

华为认证系列教程

HCIE-Security

实验指导手册

版本：3.0



华为技术有限公司

版权所有 © 华为技术有限公司 2025。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址：深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址：<https://e.huawei.com>

华为认证体系介绍

华为认证是华为公司基于“平台+生态”战略，围绕“云-管-端”协同的新ICT技术架构，打造的覆盖ICT（Information and Communications Technology，信息通信技术）全技术领域的认证体系，包含ICT基础设施认证、基础软硬件认证、云平台及云服务认证三类认证。

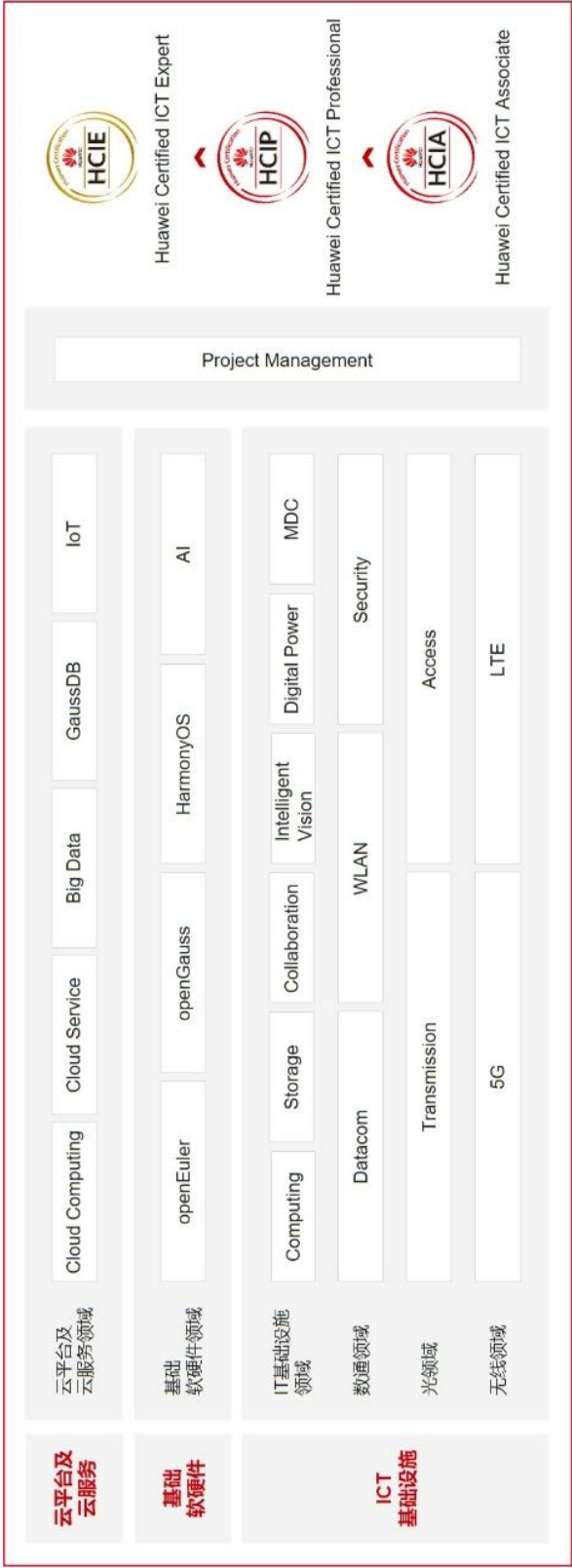
根据ICT从业者的学习和进阶需求，华为认证分为工程师级别、高级工程师级别和专家级别三个认证等级。

华为认证覆盖ICT全领域，符合ICT融合的技术趋势，致力于提供领先的人才培养体系和认证标准，培养数字化时代新型ICT人才，构建良性ICT人才生态。

HCIE-Security (Huawei Certified ICT Expert-Security，华为认证网络专家级工程师-安全方向)，主要面向华为公司办事处、代表处一线工程师，以及其他希望学习华为Security产品的技术人士。HCIE-Security认证涵盖华为网络安全、内容安全、终端接入安全的内容。

华为职业认证全景图

华为职业认证覆盖ICT全领域，致力于提供领先的人才培养体系和认证标准，培养数字化时代的新型ICT人才，构建良性的ICT人才生态。



简介

本书为 HCIE-Security v3.0 认证培训实验指导教程，适用于希望了解 Security 基础知识、虚拟系统、双机热备、用户认证、VPN 技术、内容安全、入侵防御、园区安全组网设计和运维管理等内容以及相关技术部署的读者。

内容描述

本实验指导书共包含 14 个实验，从网络安全设备基础配置开始，逐一介绍了防火墙虚拟化技术、高可靠性技术、交换安全、路由安全、网络准入控制、VPN 技术、网络攻击与防御、DDoS 攻击与防御、入侵防御系统、APT 攻击检测与防御，安全态势感知、Web 安全、智能安全运维和网络安全故障排查的配置实践。

- 实验一为防火墙综合实验，通过实验的操作与配置，帮助读者熟悉防火墙的基本安全功能，理解虚拟系统的工作原理。
 - 实验二为高可靠性实验，通过实验操作与配置演示，帮助读者掌握防火墙和入侵防御设备的双机热备部署流程。
 - 实验三为交换安全实验，通过实验的操作与配置，帮助读者掌握二层网络的安全防护功能。
 - 实验四为路由安全实验，重点讲解数通设备控制平面和转发平面的安全功能，为读者在安全运维管理时提供参考。
 - 实验五为终端接入安全综合实验，通过 802.1X 和 Portal 认证的操作与配置，使读者了解网络准入控制的工作原理和配置过程。
 - 实验六为 VPN 综合实验，通过演示 IPsec VPN 和 SSL VPN 的部署流程和配置细节，帮助读者全面掌握 VPN 的配置方法。
 - 实验七为 IPv6 网络安全实验，通过此实验，帮助读者掌握 NAT64 的转换原理，并了解与 IPv6 组网相关的安全技术部署。
 - 实验八为防火墙内容安全实验，通过部署 URL 过滤，邮件过滤和内容过滤，帮助读者理解内容安全的操作配置和工作原理。
 - 实验九为入侵防御和反病毒配置实验，通过在 IPS 设备上部署入侵防御和反病毒功能，帮助读者了解其工作原理和操作配置。
 - 实验十为 Anti-DDoS 配置实验，通过使用华为 Anti-DDoS 解决方案部署 DDoS 攻击防御体系，使读者掌握 Anti-DDoS 设备及 SecoManager (ATIC) 的配置及维护。
 - 实验十一为 FireHunter 配置实验，通过部署防火墙与 FireHunter 的安全联动抵御 APT 攻击，使读者了解针对未知威胁的攻击防范措施和配置流程。
-

- 实验十二为 HiSec Insight 配置实验，通过 HiSec Insight 的日志采集功能，进行数据实时分析，有效的发现网络中的潜在威胁，使读者掌握态势感知的应用。
- 实验十三为 SecoManager 运维实验，通过演示 SecoManager 控制器对防火墙和 IPS 设备的集中纳管，使读者掌握使用 SecoManager 控制器实现网络安全智能化运维的技能。
- 实验十四为故障排查实验，通过有线 802.1X 故障排查，IPSec VPN 故障排查和内容安全故障排查的过程，使读者了解故障排查的思路，为网络安全运维提供参考。

读者知识背景

本课程为华为认证专家级课程，为了更好地掌握本书内容，阅读本书的读者应首先具备以下基本条件：

- 具有基本的数通知识背景，同时熟悉华为安全设备，了解基本安全知识。

本书常用图标



实验环境说明

组网说明

本实验环境面向准备 HCIE-Security 考试的网络安全工程师。每套实验环境包括无线控制器 1 台，无线接入点 1 台，核心路由器 2 台，汇聚交换机 2 台，接入交换机 3 台，镜像交换机 2 台，防火墙 4 台，IPS 设备 2 台，Anti-DDoS 设备 2 台，Firehunter 服务器 1 台，iMaster NCE-Campus 服务器 1 台，SecoManager 服务器 1 台，HiSec Insight 服务器一台，服务器 1 台（安装 FusionCompute 用于支撑虚拟终端设备）。每套实验环境适用于 1 名学员同时上机操作。

设备介绍

为了满足 HCIE-Security 实验需要，建议每套实验环境设备采购以“HCIE-Security V3.0 实验设备采购清单.xlsx”为准。

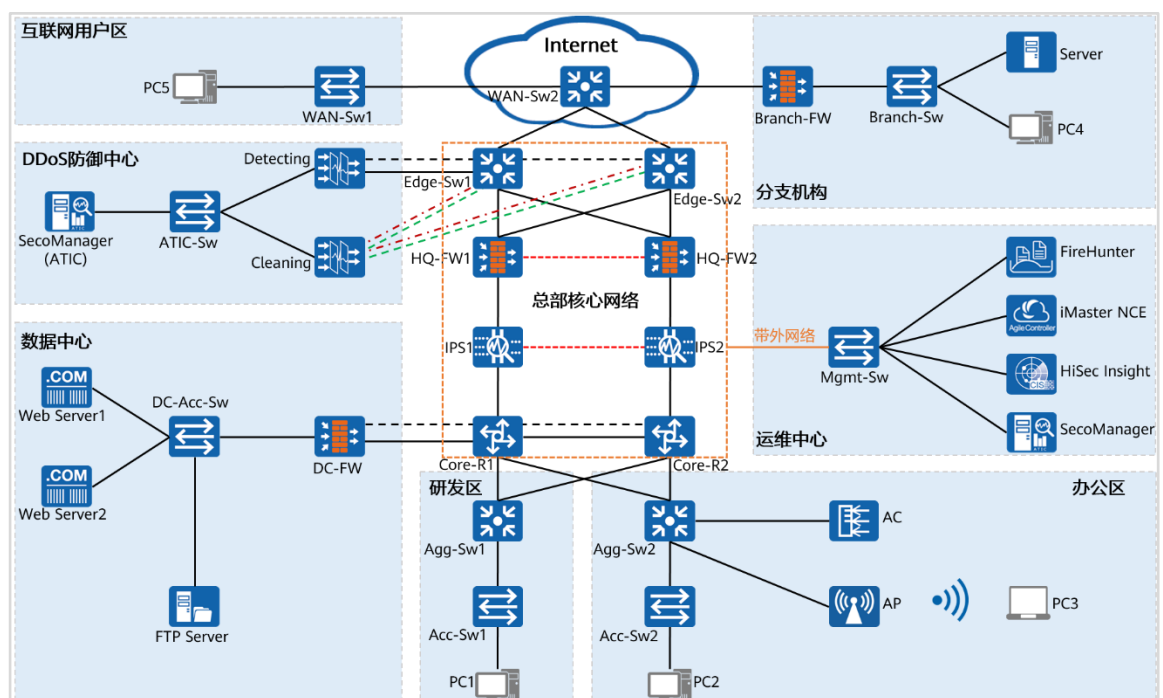
准备实验环境

检查设备

实验开始之前请每组学员检查自己的实验设备是否齐全，实验清单如下：

设备名称	数量	备注
服务器	5台	用于安装SecoManager, Firehunter, iMaster NCE-Campus和HiSec Insight等组件
USG6000F系列防火墙	4台	
华为S5700 PoE交换机	7台	
AC6508无线控制器	1台	
AirEngine5762S	1个	
AR6121E路由器	2台	
IPS6000F系列	2台	
Anti-DDoS1900系列	2台	
双绞线, 串口线	若干	

实验拓扑



终端地址

终端名称	终端地址	服务器名称	服务器地址
PC1	192.168.11.X/24 (通过DHCP获取地址)	Web Server1	192.168.16.107/24

PC2	192.168.12.X/24 (通过DHCP获取地址)	Web Server2	192.168.16.108/24
PC3	192.168.51.X/24 (通过DHCP获取地址)	FTP Server	192.168.16.110/24
PC4	192.168.14.104/24	Branch Server	192.168.13.106/24
PC5	100.1.15.105/24		

恢复环境

实验时，为避免残余配置对实验的影响，在实验完成后，需清空设备的配置信息；同时，在实验开始时，确保设备从预配置文件启动，否则需指定下次启动时的配置文件，并重启设备（通常由讲师完成）。

登陆设备需要输入密码，本实验手册中设备的登录密码为“Huawei@123”。

```

Login authentication
Password:                //输入设备登录密码
<USG6000F> startup saved-configuration hda1:/pre_config.zip
Info: Succeeded in setting the configuration for booting system.
<USG6000F> reboot fast
System will reboot! Continue ? [y/n]: y
Info: system is rebooting ,please wait...

```

目录

前 言	3
简介	3
内容描述	3
读者知识背景	4
实验环境说明	4
准备实验环境	5
1 防火墙综合实验	13
1.1 实验介绍	13
1.1.1 关于本实验	13
1.1.2 实验组网介绍	13
1.1.3 实验规划	13
1.2 实验配置任务	14
1.2.1 配置思路	14
1.2.2 配置步骤 - CLI	14
1.2.3 配置步骤 - Web	17
1.3 结果验证	34
1.3.1 PC4 访问 Branch Server	34
1.3.2 PC5 访问 Branch Server	34
1.4 配置参考（仅展示本实验相关配置）	35
1.4.1 Branch-FW 的配置	35
1.5 思考题	38
2 高可靠性实验	39
2.1 实验介绍	39
2.1.1 关于本实验	39
2.1.2 实验组网介绍	39
2.1.3 实验规划	40
2.2 实验配置任务	41
2.2.1 配置思路	41
2.2.2 配置步骤	42
2.3 结果验证	56
2.3.1 防火墙双机热备配置查看	56
2.3.2 IPS 双机热备配置查看	57
2.3.3 SLB 配置查看	58
2.4 配置参考（仅展示本实验相关配置）	59
2.4.1 HQ-FW1 的配置	59
2.4.2 HQ-FW2 的配置	61
2.4.3 IPS1 的配置	62
2.4.4 IPS2 的配置	63
2.4.5 DC-FW 的配置	65

2.5 思考题	66
3 交换安全实验	67
3.1 实验介绍	67
3.1.1 关于本实验	67
3.1.2 实验组网介绍	67
3.1.3 实验规划	67
3.2 实验配置任务	68
3.2.1 配置思路	68
3.2.2 配置步骤	68
3.3 结果验证	69
3.3.1 查看 MAC 地址漂移的配置信息	69
3.3.2 查看端口安全的配置信息	70
3.3.3 查看 DHCP-Snooping 的配置结果	70
3.4 配置参考（仅展示本实验相关配置）	71
3.4.1 AGG-SW1 的配置	71
3.4.2 ACC-SW1 的配置	71
3.5 思考题	71
4 路由安全实验	73
4.1 实验介绍	73
4.1.1 关于本实验	73
4.1.2 实验组网介绍	74
4.1.3 实验规划	74
4.2 实验配置任务	75
4.2.1 配置思路	75
4.2.2 配置步骤	75
4.3 结果验证	77
4.3.1 PC4 登录 vFW2	77
4.3.2 OSPF 邻居关系查看	79
4.4 配置参考（仅展示本实验相关配置）	81
4.4.1 HQ-FW1 的配置	81
4.4.2 HQ-FW2 的配置	82
4.4.3 DC-FW 的配置	82
4.4.4 Branch-FW 的配置	82
4.4.5 Core-R1 的配置	83
4.4.6 Core-R2 的配置	83
4.4.7 AGG-SW1 的配置	83
4.4.8 AGG-SW2 的配置	83
4.5 思考题	84
5 终端接入安全综合实验	85
5.1 实验介绍	85
5.1.1 关于本实验	85
5.1.2 实验组网介绍	85
5.1.3 实验规划	85
5.2 实验配置任务	86

5.2.1 配置思路.....	86
5.2.2 配置步骤（802.1X 认证）.....	86
5.2.3 配置步骤（Portal 认证）.....	96
5.3 结果验证.....	107
5.3.1 802.1X 认证.....	107
5.3.2 Portal 认证.....	113
5.4 配置参考（仅展示本实验相关配置）.....	119
5.4.1 ACC-SW1 的配置.....	119
5.4.2 AGG-SW2 的配置.....	119
5.4.3 AC 的配置.....	120
5.5 思考题.....	123
6 VPN 综合实验.....	124
6.1 实验介绍.....	124
6.1.1 关于本实验.....	124
6.1.2 实验组网介绍.....	124
6.1.3 实验规划.....	125
6.2 实验配置任务.....	125
6.2.1 配置思路.....	125
6.2.2 配置步骤-IPSec VPN（CLI）.....	126
6.2.3 配置步骤-IPSec VPN（Web）.....	130
6.2.4 配置步骤-SSL VPN（CLI）.....	135
6.2.5 配置步骤-SSL VPN（Web）.....	137
6.3 结果验证.....	142
6.3.1 IPSec VPN 验证.....	142
6.3.2 SSL VPN 验证.....	143
6.4 配置参考（仅展示本实验相关配置）.....	149
6.4.1 HQ-FW1 的配置.....	149
6.4.2 DC-FW 的配置.....	151
6.4.3 Branch-FW 的配置.....	152
6.4.4 Core-R1 的配置.....	153
6.5 思考题.....	153
7 IPv6 网络安全实验.....	154
7.1 实验介绍.....	154
7.1.1 关于本实验.....	154
7.1.2 实验组网介绍.....	155
7.1.3 实验规划.....	155
7.2 实验配置任务.....	156
7.2.1 配置思路.....	156
7.2.2 配置步骤.....	156
7.3 结果验证.....	161
7.3.1 IPv6 终端地址获取情况.....	161
7.3.2 NAT64 业务联通性测试.....	162
7.4 配置参考（仅展示本实验相关配置）.....	163
7.4.1 DC-FW 的配置.....	163

7.4.2 Core-R1 的配置.....	164
7.4.3 Core-R2 的配置.....	164
7.4.4 AGG-SW1 的配置.....	165
7.4.5 ACC-SW1 的配置.....	166
7.5 思考题	167
8 防火墙内容安全实验.....	168
8.1 实验介绍	168
8.1.1 关于本实验	168
8.1.2 实验组网介绍.....	168
8.1.3 实验规划.....	168
8.2 实验配置任务	169
8.2.1 配置思路.....	169
8.2.2 配置步骤（内容过滤）	169
8.2.3 配置步骤（URL 过滤）	175
8.3 结果验证.....	180
8.3.1 内容过滤验证.....	180
8.3.2 URL 过滤验证	181
8.4 配置参考（仅展示本实验相关配置）	182
8.4.1 HQ-FW1 的配置	182
8.4.2 DC-FW 的配置.....	183
8.5 思考题	184
9 入侵防御与反病毒实验.....	185
9.1 实验介绍	185
9.1.1 关于本实验	185
9.1.2 实验组网介绍.....	185
9.1.3 实验规划.....	185
9.2 实验配置任务	187
9.2.1 配置思路.....	187
9.2.2 配置步骤.....	187
9.3 结果验证.....	198
9.4 配置参考（仅展示本实验相关配置）	199
9.4.1 IPS1 的配置	199
9.5 思考题	201
10 Anti-DDoS 配置实验.....	202
10.1 实验介绍.....	202
10.1.1 关于本实验	202
10.1.2 实验组网介绍	202
10.1.3 实验规划	203
10.2 实验配置任务.....	204
10.2.1 配置思路	204
10.2.2 配置步骤	204
10.3 结果验证.....	225
10.4 配置参考（仅展示本实验相关配置）	227
10.4.1 Anti-DDoS-Detect 的配置	227

10.4.2 Anti-DDoS-Clean 的配置	232
10.5 思考题	241
11 FireHunter 配置实验	242
11.1 实验介绍	242
11.1.1 关于本实验	242
11.1.2 实验组网介绍	242
11.1.3 实验规划	243
11.2 实验配置任务	243
11.2.1 配置思路	243
11.2.2 配置步骤	244
11.3 结果验证	255
11.4 配置参考（仅展示本实验相关配置）	258
11.4.1 HQ-FW1 的配置	258
11.4.2 DC-FW 的配置	259
11.5 思考题	260
12 HiSec Insight 配置实验	261
12.1 实验介绍	261
12.1.1 关于本实验	261
12.1.2 实验组网介绍	261
12.1.3 实验规划	261
12.2 实验配置任务	262
12.2.1 配置思路	262
12.2.2 配置步骤	262
12.3 结果验证	280
12.4 配置参考（仅展示本实验相关配置）	282
12.4.1 HQ-FW1 的配置	282
12.4.2 HQ-FW2 的配置	282
12.4.3 DC-FW 的配置	283
12.5 思考题	284
13 SecoManager 运维实验	285
13.1 实验介绍	285
13.1.1 关于本实验	285
13.1.2 实验组网介绍	285
13.1.3 实验规划	286
13.2 实验配置任务	287
13.2.1 配置思路	287
13.2.2 配置步骤	287
13.3 结果验证	306
13.3.1 设备监控	306
13.3.2 策略管理	309
13.3.3 策略调优	310
13.3.4 安全联动	312
13.4 配置参考（仅展示本实验相关配置）	319
13.4.1 HQ-FW1 的配置	319

13.4.2 DC-FW 的配置	322
13.4.3 IPS1 的配置	324
13.5 思考题	326
14 故障排查综合实验	327
14.1 实验介绍	327
14.1.1 关于本实验	327
14.1.2 实验组网介绍	327
14.1.3 实验规划	328
14.2 实验配置任务	328
14.2.1 配置思路	328
14.2.2 配置步骤	328
14.3 思考题	349

1

防火墙综合实验

1.1 实验介绍

1.1.1 关于本实验

防火墙设备作为三层网关部署在园区内网和 Internet 之间。内网中划分了两个独立的区域：办公区域和服务器区域。两个区域之间通过不同的虚拟防火墙隔离，二者互访需要通过虚拟防火墙进行流量控制。

服务器区域中的 Branch Server 对外提供服务，使用服务器映射技术将 Server 的私网 IP 映射到公网，Internet 用户使用公网访问 Branch Server 上的资源，办公区域的用户则通过私网 IP 访问 Branch Server 上的资源。

1.1.2 实验组网介绍

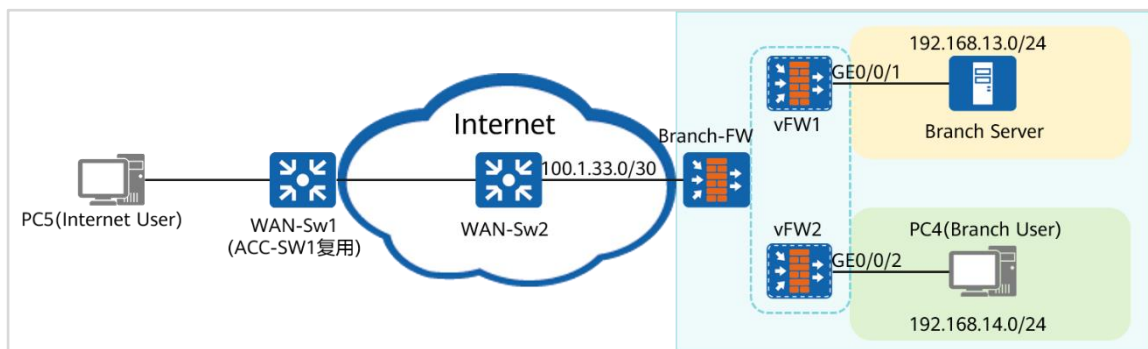


图1-1 实验拓扑图

1.1.3 实验规划

根据园区网络规划，Branch-FW 作为分支园区网络的出口设备，在 Branch-FW 上开启虚拟系统功能，部署虚拟防火墙 vFW1，用于控制访问 Branch Server 的流量。部署虚拟防火墙 vFW2，用于控制 PC4 (Branch User) 的流量。通过部署服务器映射技术将 Branch Server 的私网 IP 映射为公网 IP。

配置完成以后，实现 PC5 (Internet User) 能够通过公网访问 Branch Server，同时 PC4 (Branch User) 能够通过私网访问 Branch Server。

表1-1 端口类型及参数设计

设备	端口(安全区域/所属系统)	IP
Branch-FW	GE0/0/0(untrust/public)	100.1.33.1/30
	virtual-if0(trust/public)	/
	GE0/0/1(dmz/vFW1)	192.168.13.254/24
	virtual-if1(untrust/vFW1)	/
	GE0/0/2(trust/vFW2)	192.168.14.254/24
	virtual-if2(untrust/vFW2)	/
PC4(Branch User)	/	192.168.14.104
Branch Server	/	私网IP: 192.168.13.106 公网IP: 100.1.33.5
PC5(Internet User)	/	100.1.15.105

1.2 实验配置任务

1.2.1 配置思路

1. 所有设备上的 IP 地址已经预配，开始配置前请进行检查和测试。
2. 在 Branch-FW 上创建 vFW1 和 vFW2，并将相应接口加入到虚拟系统中，配置静态路由和安全策略，实现 PC4（Branch User）能够通过私网访问 Branch Server。
3. 在 Branch-FW 上部署服务器映射技术，将 Branch Server 的私网 IP 映射为公网 IP，配置静态路由和安全策略，使 PC5（Internet User）能够通过公网访问 Branch Server。

1.2.2 配置步骤 - CLI

步骤 1 虚拟系统配置

在 Branch-FW 上开启虚拟系统功能，创建 vFW1 和 vFW2 两个虚拟系统，并为其分配资源，添加接口。

```
< Branch-FW> system-view
Enter system view, return user view with Ctrl+Z.
[Branch-FW] vsys enable
[Branch-FW] vsys name vFW1
[Branch-FW-vsys-vFW1] assign resource-class r0
[Branch-FW-vsys-vFW1] assign interface GE0/0/1
Info: All related configurations on this interface are removed.
[Branch-FW-vsys-vFW1] quit
[Branch-FW] vsys name vFW2
[Branch-FW-vsys-vFW2] assign resource-class r0
[Branch-FW-vsys-vFW2] assign interface GE0/0/2
Info: All related configurations on this interface are removed.
[Branch-FW-vsys-vFW2] quit
```

根据规划将 Branch-FW 根系统上的接口加入相应安全区域。

```
[Branch-FW] firewall zone untrust
[Branch-FW-zone-untrust] add interface GE 0/0/0
[Branch-FW-zone-untrust] quit
[Branch-FW] firewall zone trust
[Branch-FW-zone-trust] add interface Virtual-if 0
[Branch-FW-zone-trust] quit
```

根据规划将 Branch-FW 虚拟系统上的接口加入相应安全区域并重新配置 IP 地址。

```
[Branch-FW] switch vsys vFW1
<Branch-FW-vFW1> system-view
Enter system view, return user view with Ctrl+Z.
[Branch-FW-vFW1] firewall zone untrust
[Branch-FW-vFW1-zone-untrust] add interface Virtual-if 1
[Branch-FW-vFW1-zone-untrust] quit
[Branch-FW-vFW1] firewall zone dmz
[Branch-FW-vFW1-zone-dmz] add interface GE 0/0/1
[Branch-FW-vFW1-zone-dmz] quit
[Branch-FW-vFW1] interface GE 0/0/1
[Branch-FW-vFW1-GE0/0/1] ip address 192.168.13.254 24
[Branch-FW-vFW1-GE0/0/1] service-manage ping permit
[Branch-FW-vFW1-GE0/0/1] quit
[Branch-FW-vFW1] quit
<Branch-FW-vFW1> quit
[Branch-FW] switch vsys vFW2
<Branch-FW-vFW2> system-view
Enter system view, return user view with Ctrl+Z.
[Branch-FW-vFW2] firewall zone untrust
[Branch-FW-vFW2-zone-untrust] add interface Virtual-if 2
[Branch-FW-vFW2-zone-untrust] quit
[Branch-FW-vFW2] firewall zone trust
[Branch-FW-vFW2-zone-trust] add interface g0/0/2
[Branch-FW-vFW2-zone-trust] quit
[Branch-FW-vFW2] interface GE 0/0/2
[Branch-FW-vFW2-GE0/0/2] ip address 192.168.14.254 24
[Branch-FW-vFW2-GE0/0/2] service-manage ping permit
[Branch-FW-vFW2-GE0/0/2] quit
[Branch-FW-vFW2] quit
<Branch-FW-vFW2> quit
```

步骤 2 静态路由配置

在 Branch-FW 的根系统中配置静态路由，访问 PC4（Branch User）和 Branch Server 的路由分别指向虚拟系统 vFW2 和 vFW1，同时配置缺省路由确保分支园区可访问外网。

```
[Branch-FW] ip route-static 192.168.13.0 24 vpn-instance vFW1
[Branch-FW] ip route-static 192.168.14.0 24 vpn-instance vFW2
[Branch-FW] ip route-static 0.0.0.0 0 100.1.33.2
```

在 Branch-FW 的 vFW1 虚拟系统中配置默认路由，目的虚拟路由器指向根系统 public，并配置安全策略放行 PC4（Branch User）访问 Branch Server 的流量。

```
[Branch-FW]switch vsys vFW1
<Branch-FW-vFW1> system-view
Enter system view, return user view with Ctrl+Z.
[Branch-FW-vFW1] ip route-static 0.0.0.0 0 public
[Branch-FW-vFW1] security-policy
[Branch-FW-vFW1-policy-security] rule name From_Office_to_Server
[Branch-FW-vFW1-policy-security-rule-From_Office_to_Server] source-zone untrust
[Branch-FW-vFW1-policy-security-rule-From_Office_to_Server] destination-zone dmz
[Branch-FW-vFW1-policy-security-rule-From_Office_to_Server] source-address 192.168.14.0 24
[Branch-FW-vFW1-policy-security-rule-From_Office_to_Server] destination-address 192.168.13.0 24
[Branch-FW-vFW1-policy-security-rule-From_Office_to_Server] action permit
[Branch-FW-vFW1-policy-security-rule-From_Office_to_Server] quit
[Branch-FW-vFW1-policy-security] quit
[Branch-FW-vFW1]
```

在 Branch-FW 的 vFW2 虚拟系统中配置默认路由，目的虚拟路由器指向根系统 public，并配置安全策略放行 PC4（Branch User）访问 Branch Server 的流量。

```
[Branch-FW] switch vsys vFW2
<Branch-FW-vFW2> system-view
Enter system view, return user view with Ctrl+Z.
[Branch-FW-vFW2] ip route-static 0.0.0.0 0 public
[Branch-FW-vFW2] security-policy
[Branch-FW-vFW2-policy-security] rule name From_Office_to_Server
[Branch-FW-vFW2-policy-security-rule-From_Office_to_Server] source-zone trust
[Branch-FW-vFW2-policy-security-rule-From_Office_to_Server] destination-zone untrust
[Branch-FW-vFW2-policy-security-rule-From_Office_to_Server] source-address 192.168.14.0 24
[Branch-FW-vFW2-policy-security-rule-From_Office_to_Server] destination-address 192.168.13.0 24
[Branch-FW-vFW2-policy-security-rule-From_Office_to_Server] action permit
[Branch-FW-vFW2-policy-security-rule-From_Office_to_Server] quit
[Branch-FW-vFW2-policy-security] quit
[Branch-FW-vFW2]
```

步骤 3 NAT Server 配置

在 Branch-FW 的根系统中配置服务器映射 NAT Server，将 Branch Server 的私网 IP 地址 192.168.13.106 映射为公网 IP 地址 100.1.33.5。

```
[Branch-FW] nat server 1 global 100.1.33.5 inside 192.168.13.106 no-reverse
```

配置安全策略放行 Internet 用户访问 Server 的流量。

```
[Branch-FW] security-policy
[Branch-FW-policy-security] rule name From_Internet_to_Server
[Branch-FW-policy-security-rule-From_Internet_to_Server] source-zone untrust
[Branch-FW-policy-security-rule-From_Internet_to_Server] destination-zone trust
[Branch-FW-policy-security-rule-From_Internet_to_Server] source-address 100.1.15.105 32
[Branch-FW-policy-security-rule-From_Internet_to_Server] destination-address 192.168.13.0 24
```



```
[Branch-FW-policy-security-rule-From_Internet_to_Server] action permit
[Branch-FW-policy-security-rule-From_Internet_to_Server] quit
[Branch-FW-policy-security] quit
```

在 Branch-FW 的 vFW1 虚拟系统中配置安全策略放行 Internet 用户访问 Server 的流量。

```
[Branch-FW]switch vsys vFW1
<Branch-FW-vFW1> system-view
Enter system view, return user view with Ctrl+Z.
[Branch-FW-vFW1] security-policy
[Branch-FW-vFW1-policy-security] rule name From_Internet_to_server
[Branch-FW-vFW1-policy-security-rule-From_Internet_to_server] source-zone untrust
[Branch-FW-vFW1-policy-security-rule-From_Internet_to_server] destination-zone dmz
[Branch-FW-vFW1-policy-security-rule-From_Internet_to_server] source-address 100.1.15.105 32
[Branch-FW-vFW1-policy-security-rule-From_Internet_to_server] destination-address 192.168.13.0 24
[Branch-FW-vFW1-policy-security-rule-From_Internet_to_server] action permit
[Branch-FW-vFW1-policy-security-rule-From_Internet_to_server] quit
[Branch-FW-vFW1-policy-security] quit
```

1.2.3 配置步骤 - Web

步骤 1 虚拟系统配置

登录 Branch-FW 设备 Web 管理界面（地址：<https://172.21.10.24:8443/>，账号：Webuser/Admin@123），开启虚拟系统功能，创建 vFW1 和 vFW2，并根据规划将相应接口加入到不同的虚拟系统和安全区域。

说明：设备首次登录 Web 管理页面时，系统语言默认为英语，可以点击登录页面右下角“English”切换语言为“简体中文”。

选择“系统 > 虚拟系统 > 虚拟系统”，打开虚拟系统功能，如下图。

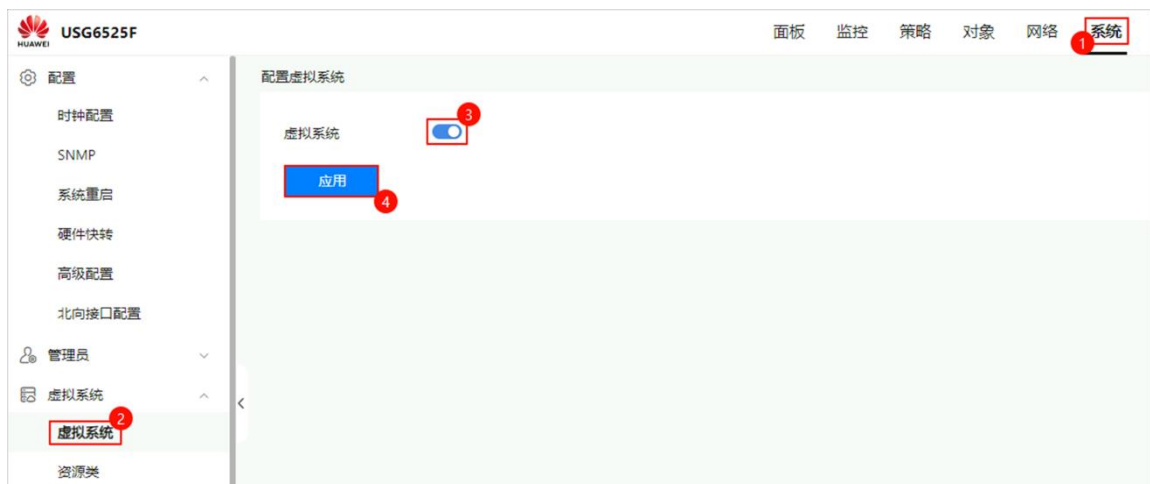


图1-2 启用虚拟系统功能

单击“新建”，创建 vFW1，并为其分配资源 r0，如下图。

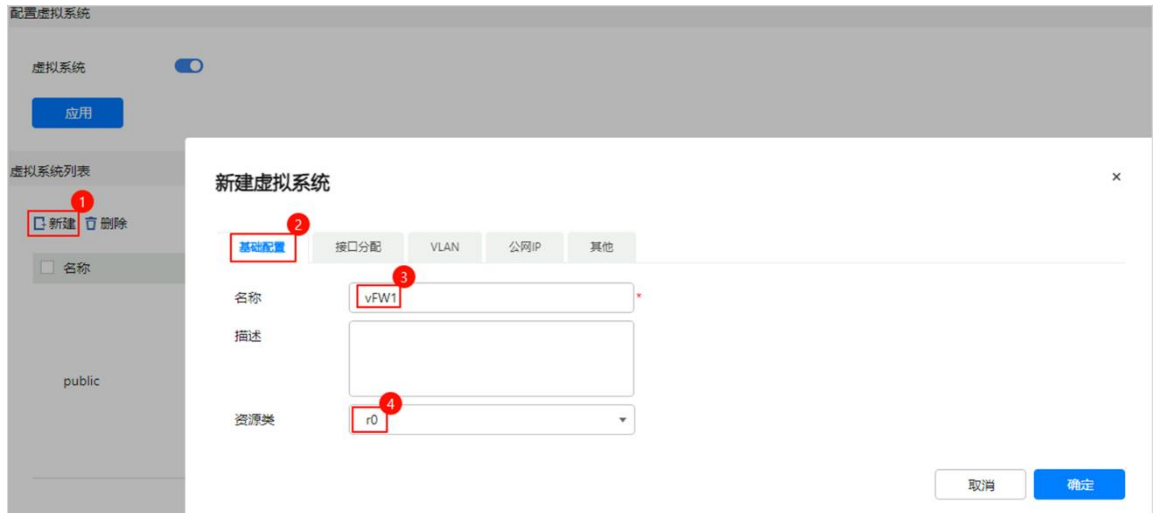


图1-3 新建 vFW1 虚拟系统

选择菜单栏中“接口分配”的条目，将 GE0/0/1 接口添加到 vFW1，并点击“确定”，如下图。



图1-4 给 vFW1 系统分配业务接口

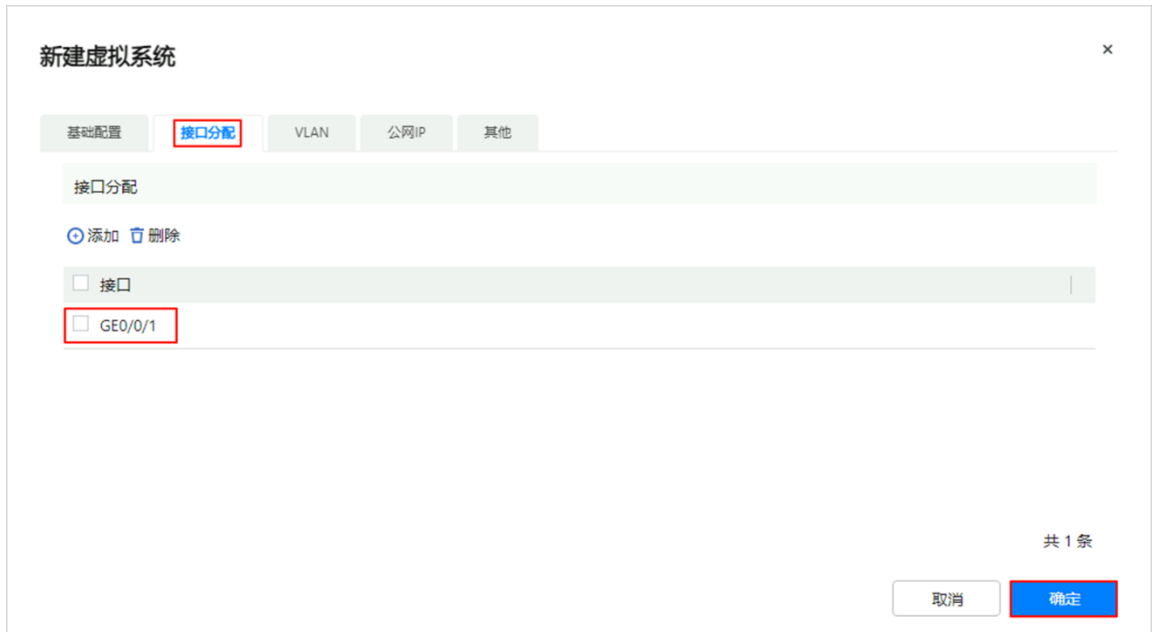


图1-5 确认 vFW1 系统业务接口分配

vFW1 创建完成后，如下图。

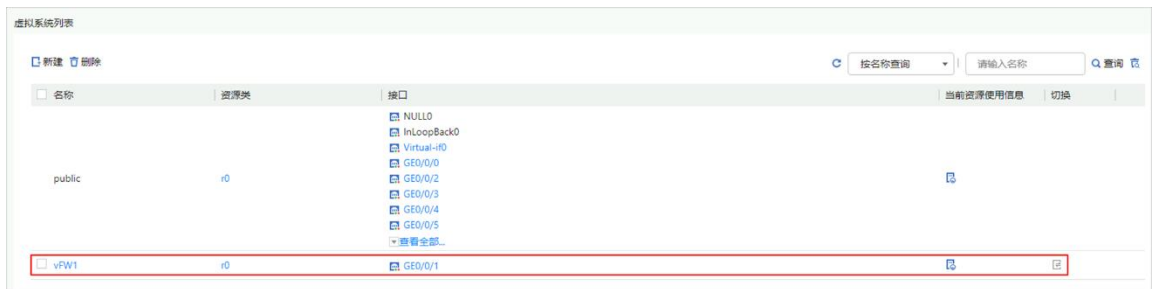


图1-6 vFW1 虚拟系统创建完成

以相同的步骤创建 vFW2，为其分配资源 r0，并将接口 GE0/0/2 添加到 vFW2 中，创建完成后，如下图。



图1-7 虚拟系统查看

Branch-FW 上相应接口的 IP 地址已经预配，根据规划，将 Branch-FW 上根系统中的接口加入相应安全区域。

选择“网络 > 接口”，点击 GE0/0/0 接口条目对应的安全区域，将接口加入 untrust 区域，如下图。

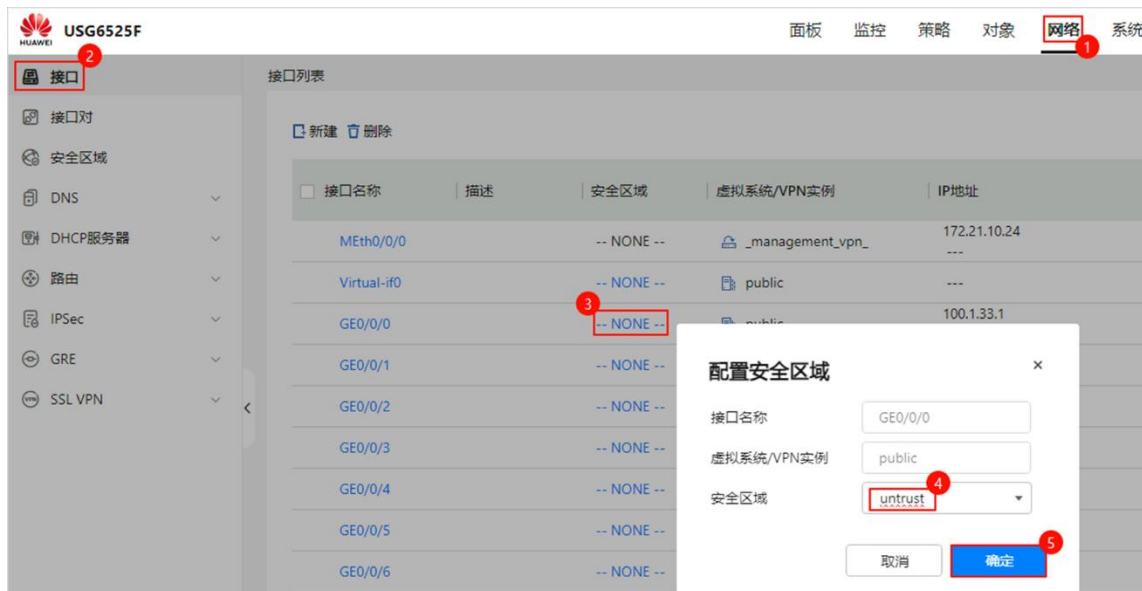


图1-8 业务接口安全区域配置

配置完成后，将 Virtual-if0 接口加入到 trust 区域，如下图。

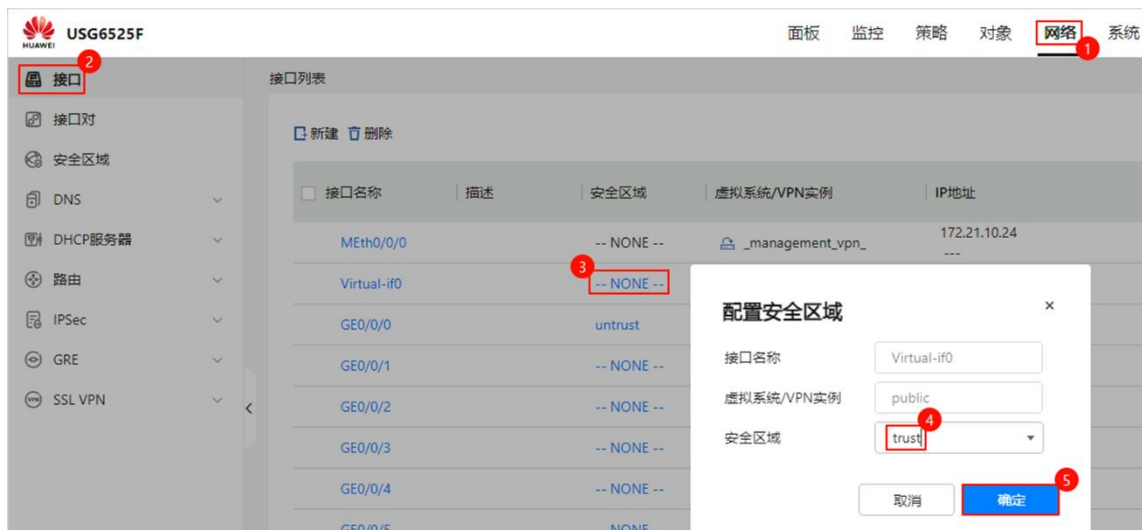


图1-9 虚拟系统接口安全区域配置

步骤 2 静态路由配置

在 Branch-FW 的根系统中配置静态路由，去往 Branch Server 网段的 192.168.13.0/24 的目的虚拟路由器为 vFW1；去往 PC4 网段的 192.168.14.0/24 的目的虚拟路由器为 vFW2，以及访问外网的缺省路由。

选择“网络 > 路由 > 静态路由”，单击“新建”，配置过程如下图。

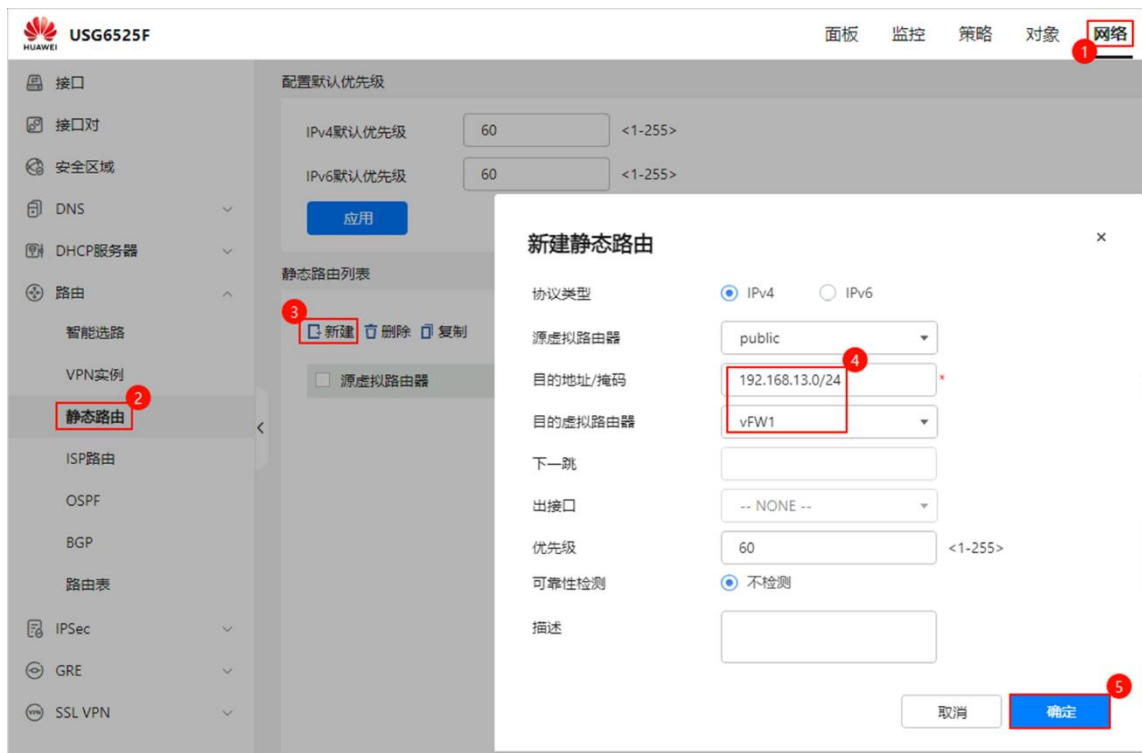


图1-10 创建访问 vFW1 系统下业务的静态路由

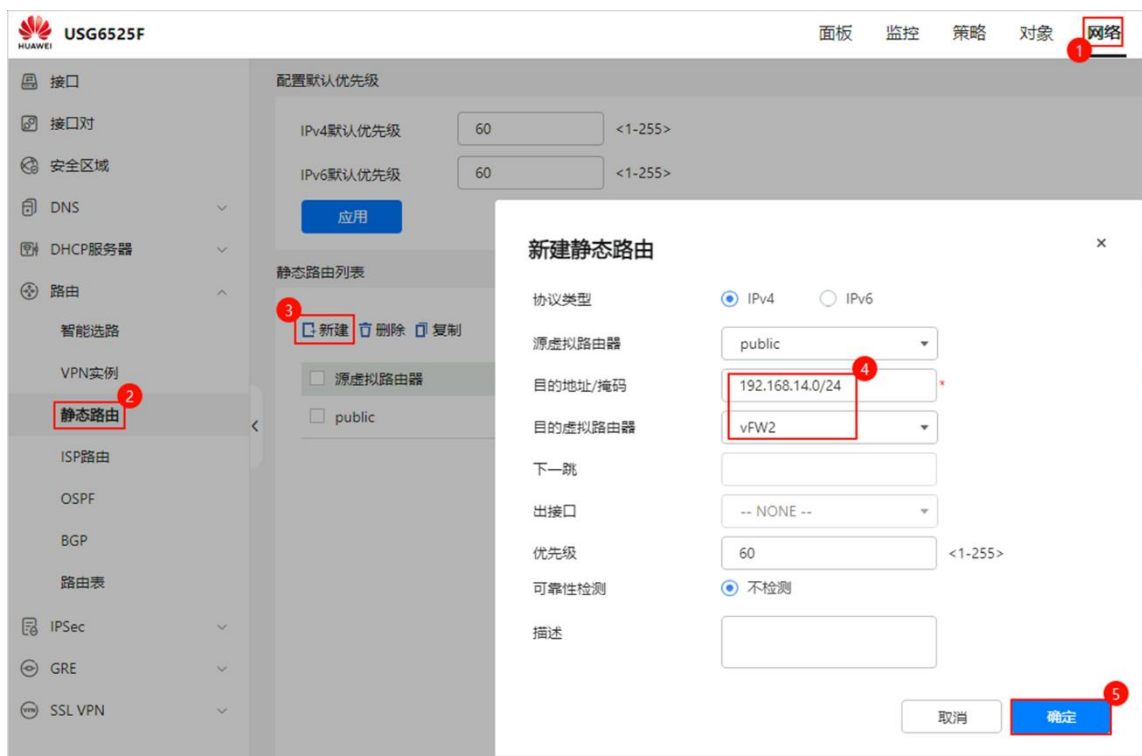


图1-11 创建访问 vFW2 系统下业务的静态路由

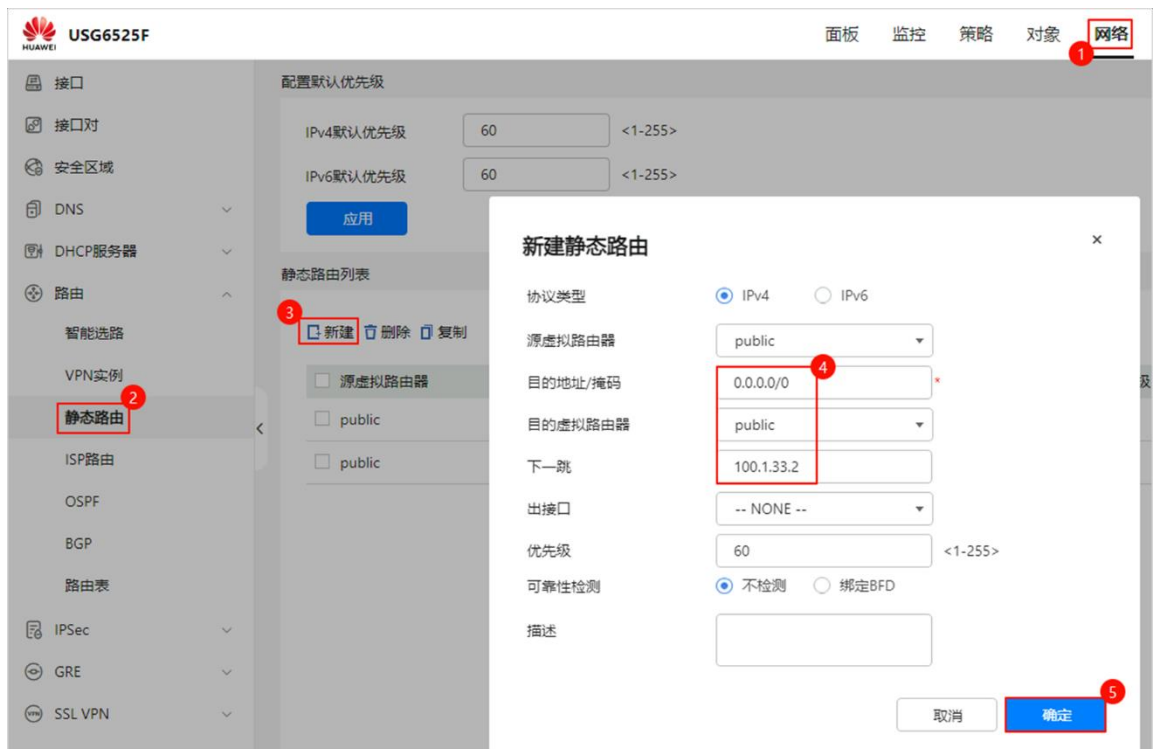


图1-12 根系统下创建访问外网的缺省路由

配置完成后，根系统中存在的静态路由条目如下图。



图1-13 静态路由查看

进入 vFW1 虚拟系统，为其接口配置 IP 地址，并将接口加入相应安全区域。

点击页面右上角“虚拟系统”的下拉菜单，选择菜单栏中的“vFW1”，如下图。



图1-14 切换 vFW1 虚拟系统

切换到 vFW1 虚拟系统后，选择“网络 > 接口”，将 GE0/0/1 加入到 DMZ 区域，并重新配置 IP 地址，如下图。



图1-15 配置 vFW1 系统下的业务接口

配置完成后，将 Virtual-if1 加入到 untrust 的安全区域，如下图。

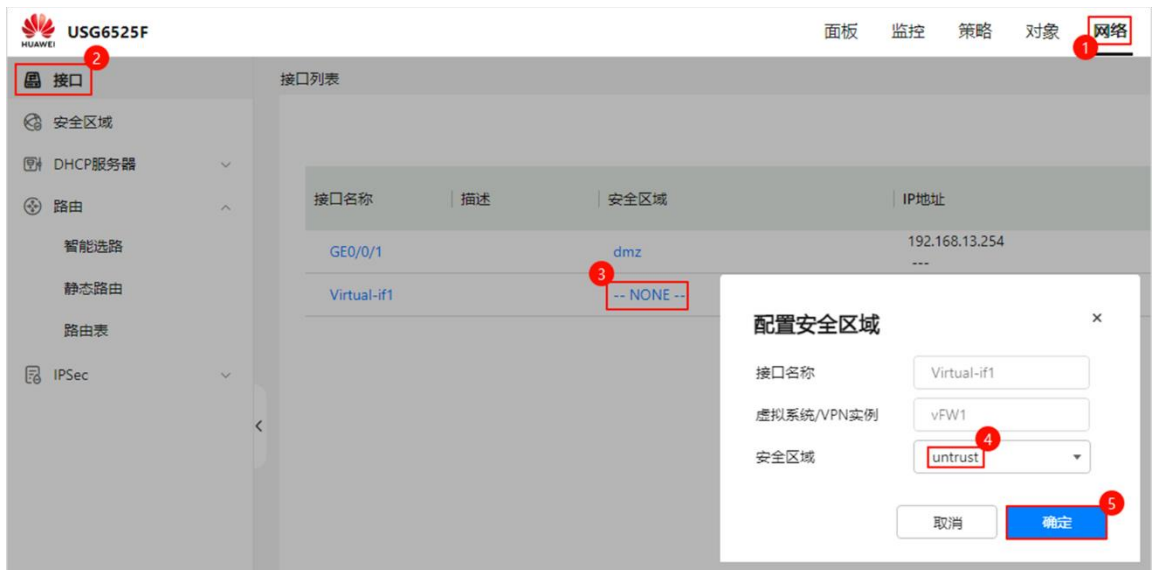


图1-16 配置 vFW1 虚拟系统接口的安全区域

vFW1 虚拟系统中的接口配置完成后，接口列表信息如下图。

接口列表					
接口名称	描述	安全区域	IP地址	连接类型	VLAN
GE0/0/1		dmz	192.168.13.254	静态IP (IPv4)	
Virtual-if1		untrust	---	静态IP (IPv6)	

图1-17 vFW1 虚拟系统下的业务接口配置信息

在 vFW1 上配置默认路由，vFW1 中产生的所有流量都通过根系统转发。

选择“网络 > 路由 > 静态路由”，单击“新建”，默认路由的目的虚拟路由器指向根系统 public，如下图。



图1-18 创建 vFW1 虚拟系统访问外部的缺省路由

配置完成后，vFW1 上的静态路由列表如下图。

静态路由列表							
源虚拟路由器	目的地址/掩码	目的虚拟路由器	下一跳	优先级	出接口	描述	配置
vFW1	0.0.0.0/0	public		60			

图1-19 vFW1 虚拟系统静态路由信息查看

在 vFW1 上配置安全策略，允许从 PC4 访问 Branch Server 的流量通过 vFW1。

选择“策略 > 安全策略 > 安全策略”，单击“新建安全策略”，配置安全策略名称为“From_Office_to_Server”，具体配置如下图。



图1-20 vFW1 创建业务安全策略

配置完成后，安全策略列表如下图。



图1-21 vFW1 查看安全策略条目

进入 vFW2 虚拟系统，为其接口配置 IP 地址，并将接口加入相应区域。

点击页面右上角“虚拟系统”的下拉菜单，选择菜单栏中的“vFW2”，如下图。



图1-22 切换至 vFW2 虚拟系统

切换到 vFW2 虚拟系统后，选择“网络 > 接口”，将 GE0/0/2 加入到 trust 区域，并重新配置 IP 地址，如下图。

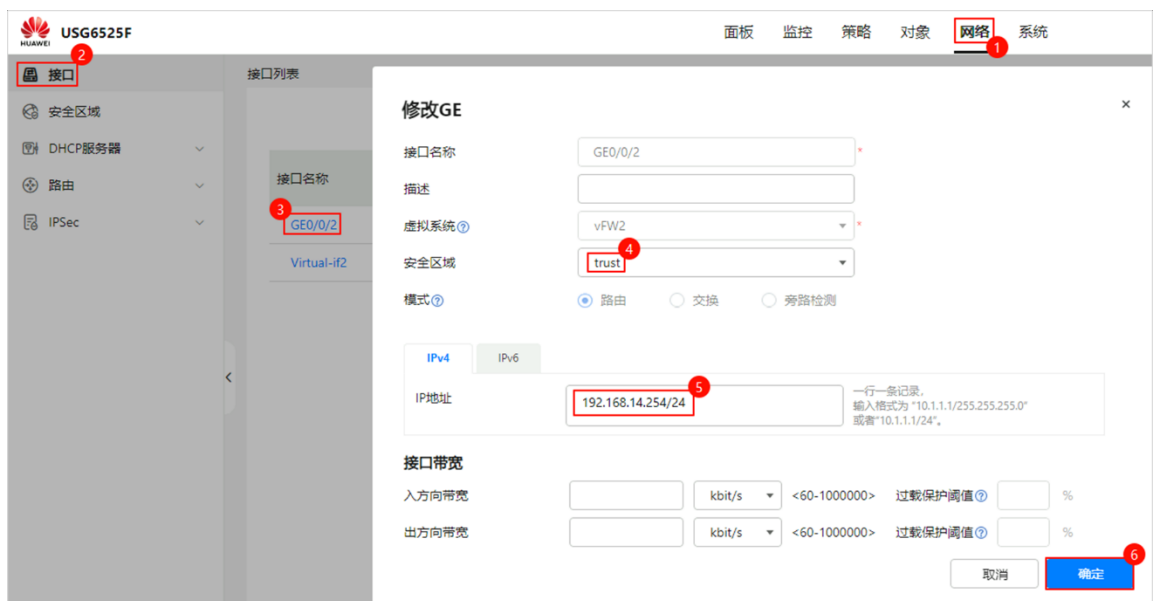


图1-23 配置 vFW2 虚拟系统业务接口

配置完成后，将 Virtual-if2 加入到 untrust 的安全区域，如下图。

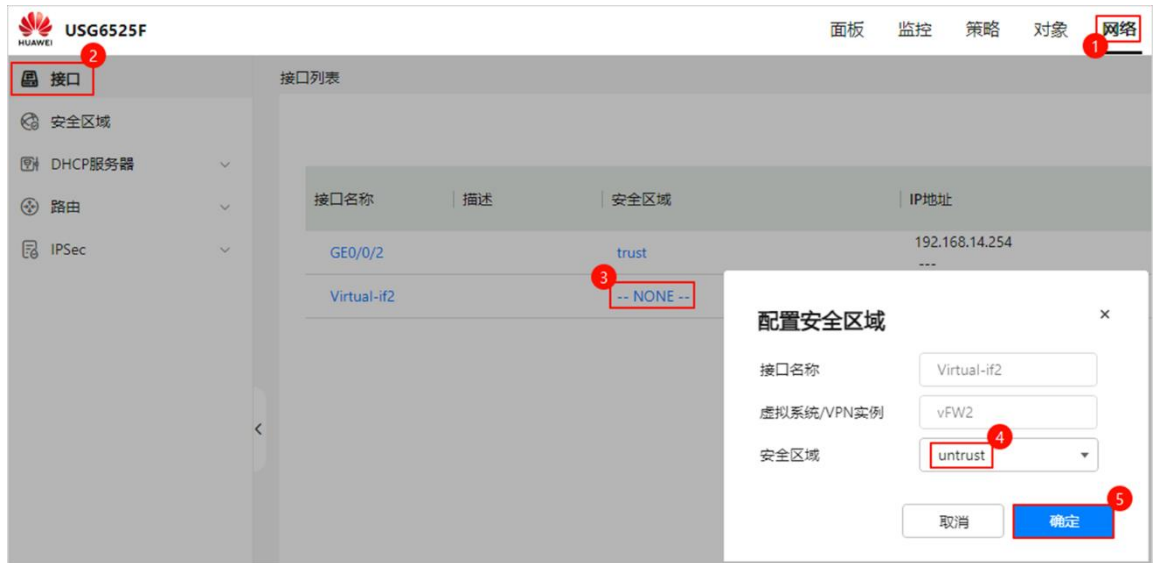


图1-24 配置 vFW2 虚拟系统接口安全区域

vFW2 虚拟系统中的接口配置完成后，接口列表信息如下图。

接口列表							
接口名称	描述	安全区域	IP地址	连接类型	VLAN	模式	状态
GE0/0/2		trust	192.168.14.254	静态IP (IPv4)		路由	↑
Virtual-if2		untrust	---	静态IP (IPv6)			↑

图1-25 vFW2 系统业务接口配置信息概览

在 vFW2 上配置默认路由，vFW2 中产生的所有流量都通过根系统转发。

选择“网络 > 路由 > 静态路由”，单击“新建”，默认路由的目的虚拟路由器指向根系统 public，如下图。

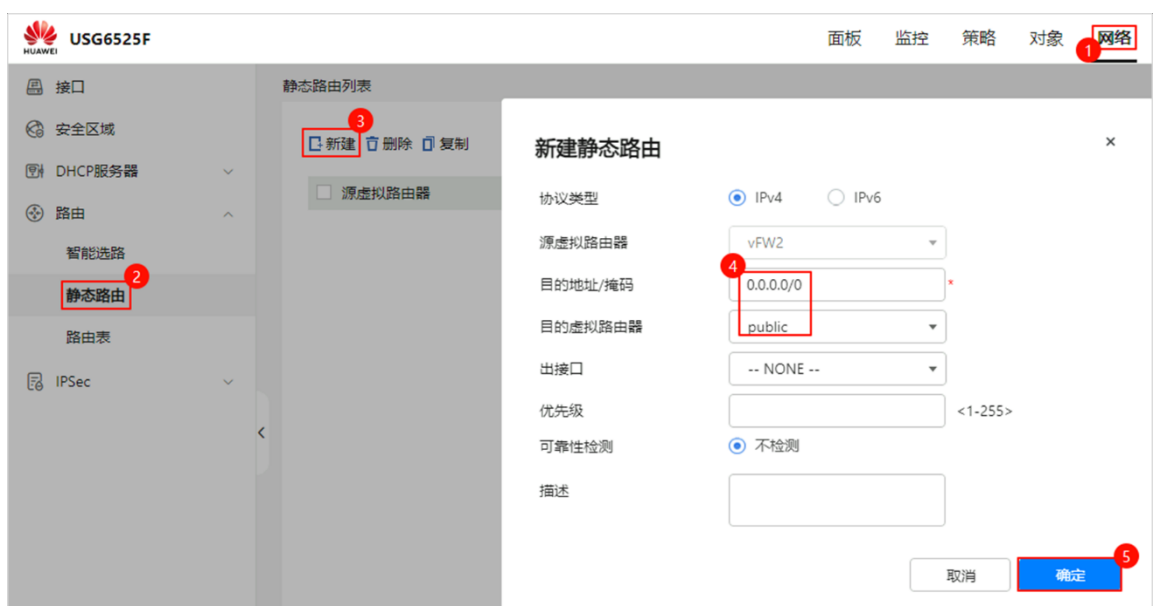


图1-26 配置 vFW2 访问外部的缺省路由

配置完成后，vFW2 上的静态路由列表如下图。



源虚拟路由器	目的地址/掩码	目的虚拟路由器	下一跳	优先级	出接口	描述	配置
vFW2	0.0.0.0/0	public	60				

图1-27 查看 vFW2 系统的静态路由配置信息

在 vFW2 上配置安全策略，允许从 PC4 访问 Branch Server 的流量通过 vFW2。

选择“策略 > 安全策略 > 安全策略”，单击“新建安全策略”，配置安全策略名称为“From_Office_to_Server”，具体配置如下图。

新建安全策略

概述

名称

From_Office_to_Server

描述

策略组

-- NONE --

条件

① 当前未加载地区识别特征库。

源

安全区域

trust

IP 地址/地区

192.168.14.0...

目的

目的类型

安全区域

安全区域

untrust

IP 地址/地区

192.168.13.0...

服务

协议

请选择服务

更多

应用/时间段/VLAN ID

动作

动作

允许

禁止

内容安全检查

反病毒/入侵防御/URL过滤/内容过滤

取消

命令预览

确定

图1-28 创建 vFW2 系统的业务安全策略

配置完成后，安全策略列表如下图。



序号	名称	源	目的	服务	应用	时间段	动作	内容安全
1	From_Office_to_Server	trust 192.168.14.0/255.255.255.0	untrust 192.168.13.0/255.255.255.0	any	any		允许	
2	default	any	any	any	any		禁止	

图1-29 查看 vFW2 系统的安全策略条目

步骤 3 NAT Server 配置

将防火墙 Branch-FW 的配置界面切换至根系统 public 中，在根系统中配置 NAT Server，将 Server 的私网 IP 地址映射为公网 IP 地址，允许 Internet 用户通过公网 IP 地址访问其资源。

选择“策略 > NAT 策略 > 服务器映射”，单击“新建”，配置 NAT Server 的名称为“Server”，公网 IP 地址为 100.1.33.5，私网 IP 地址为 192.168.13.106，如下图。



USG6525F

策略

新建服务器映射

名称: Server

安全区域:

公网地址: 100.1.33.5

私网地址: 192.168.13.106

☐ 指定协议

☐ 允许服务器使用公网地址上网

☒ 自动生成黑洞路由

提示: 为保证设备顺利转发NAT业务, 需要配置安全策略。
如需查看NAT相关日志, 请在安全策略中启用流量日志及会话日志。 (新建安全策略)

取消 确定

图1-30 配置 NAT Server

配置完成后，服务器映射列表信息如下图。



名称	公网地址	私网地址	协议	公网端口	私网端口	启用	编辑
Server	100.1.33.5	192.168.13.106				☒	

图1-31 查看 NAT Server 配置信息

选择“策略 > 安全策略 > 安全策略”，单击“新建安全策略”，配置安全策略名称为“From_Internet_to_Server”，具体配置如下图。

新建安全策略

×

概述

* 名称

From_Internet_to_Server

1

描述

策略组

-- NONE --

条件

① 当前未加载地区识别特征库。如需配置地区，请 加载地区识别特征库

源

安全区域

untrust

×

2

IP 地址/地区 ②

100.1.15.105

×

目的

目的类型

安全区域

虚拟服务

安全区域

trust

×

IP 地址/地区 ②

192.168.13.0...

×

服务 ③

协议

请选择服务

更多

应用/用户/安全组/时间段/VLAN ID

动作

动作

允许

禁止

3

内容安全检查

反病毒/入侵防御/URL过滤/内容过滤

取消

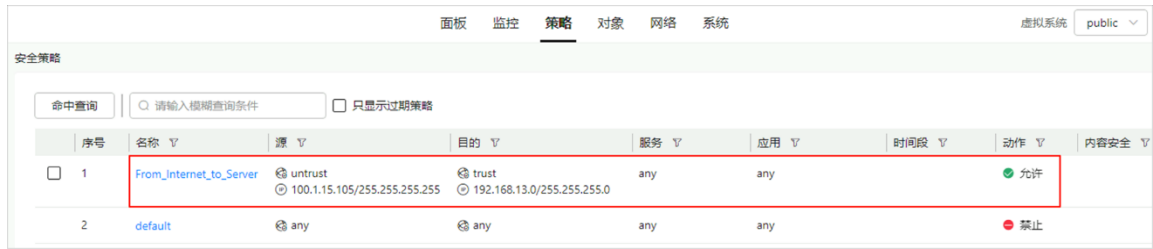
命令预览

4

确定

图1-32 根系统业务安全策略配置

配置完成后，安全策略列表如下图。



序号	名称	源	目的	服务	应用	时间段	动作	内容安全
1	From_Internet_to_Server	untrust 100.1.15.105/255.255.255.255	trust 192.168.13.0/255.255.255.0	any	any		允许	
2	default	any	any	any	any		禁止	

图1-33 根系统业务安全策略查看

上述配置完成后，将配置界面切换至 vFW1 的虚拟系统中，配置安全策略允许 PC5 访问 Branch Server。

选择“策略 > 安全策略 > 安全策略”，单击“新建安全策略”，配置安全策略名称为“From_Internet_to_Server”，方向为从 untrust 安全区域到 DMZ 区域，源 IP 地址为 PC5 的 IP 地址，目的 IP 地址为服务器网段，动作为“允许”，如下图。

新建安全策略

×

概述

* 名称

From_Internet_to_Server

1

描述

策略组

-- NONE --

条件

① 当前未加载地区识别特征库。

源

安全区域

untrust

×

2

IP 地址/地区 ②

100.1.15.105

×

目的

目的类型

安全区域

虚拟服务

安全区域

dmz

×

IP 地址/地区 ②

192.168.13.0...

×

服务 ②

协议

请选择服务

更多

应用/时间段/VLAN ID

动作

动作

允许

禁止

3

内容安全检查

反病毒/入侵防御/URL过滤/内容过滤

取消

命令预览

4

确定

图1-34 vFW1 配置业务安全策略允许访问分支服务器

配置完成后，vFW1 系统中的安全策略列表如下图。

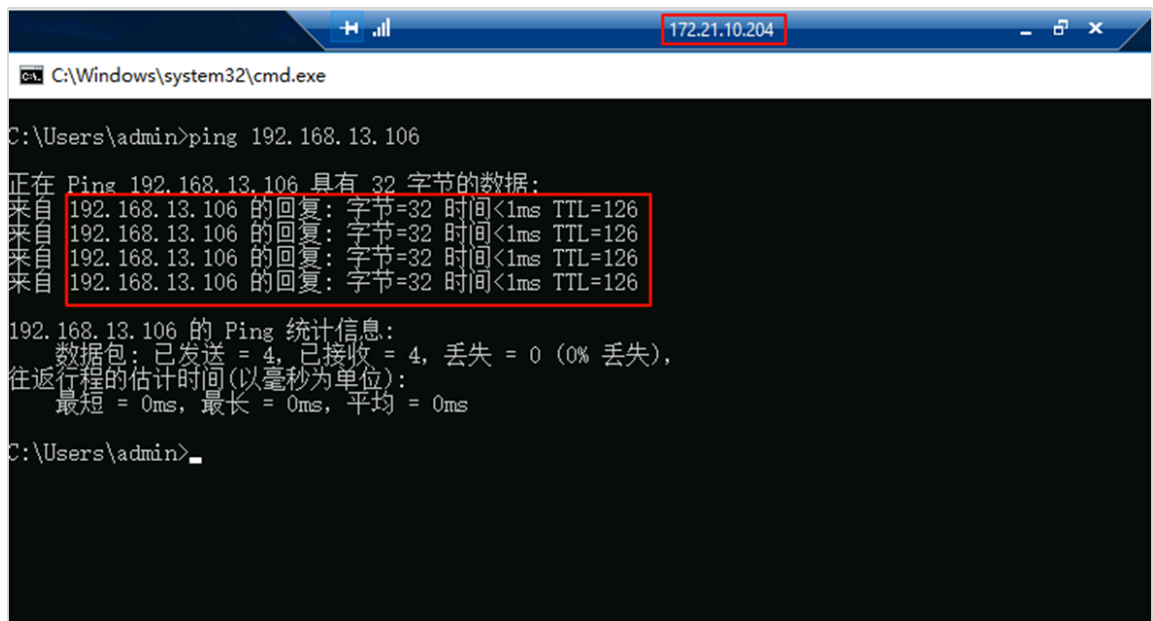
安全策略									
序号	名称	源	目的	服务	应用	时间段	动作	内容安全	
1	From_Office_to_Server	untrust 192.168.14.0/255.255.255.0	dmz 192.168.13.0/255.255.255.0	any	any		允许		
2	From_Internet_to_Server	untrust 100.1.15.105/255.255.255.255	dmz 192.168.13.0/255.255.255.0	any	any		允许		
3	default	any	any	any	any		禁止		

图1-35 vFW1 系统安全策略查看

1.3 结果验证

1.3.1 PC4 访问 Branch Server

通过远程桌面登录到 PC4，使用 ping 命令测试对 Branch Server 的访问，如下图：



```

C:\Windows\system32\cmd.exe

C:\Users\admin>ping 192.168.13.106

正在 Ping 192.168.13.106 具有 32 字节的数据:
来自 192.168.13.106 的回复: 字节=32 时间<1ms TTL=126
来自 192.168.13.106 的回复: 字节=32 时间<1ms TTL=126
来自 192.168.13.106 的回复: 字节=32 时间<1ms TTL=126
来自 192.168.13.106 的回复: 字节=32 时间<1ms TTL=126

192.168.13.106 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 0ms, 最长 = 0ms, 平均 = 0ms

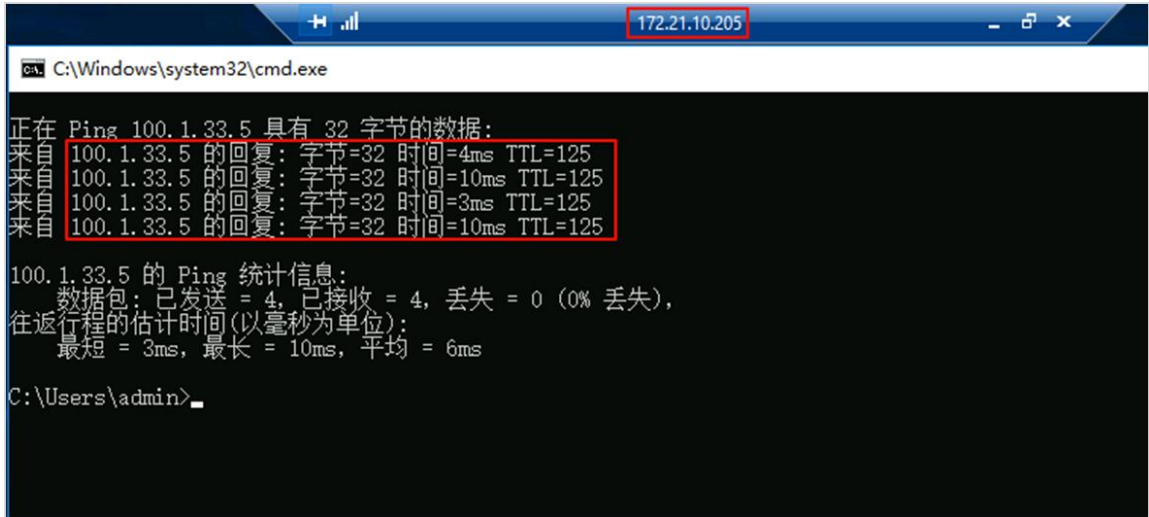
C:\Users\admin>

```

测试表明 PC4 能够访问 Branch Server，配置正确无误。

1.3.2 PC5 访问 Branch Server

通过远程桌面登录到 PC5，使用 ping 命令测试对 Branch Server 的访问，如下图：



```

C:\Windows\system32\cmd.exe
172.21.10.205

正在 Ping 100.1.33.5 具有 32 字节的数据:
来自 100.1.33.5 的回复: 字节=32 时间=4ms TTL=125
来自 100.1.33.5 的回复: 字节=32 时间=10ms TTL=125
来自 100.1.33.5 的回复: 字节=32 时间=3ms TTL=125
来自 100.1.33.5 的回复: 字节=32 时间=10ms TTL=125

100.1.33.5 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 3ms, 最长 = 10ms, 平均 = 6ms

C:\Users\admin>

```

测试表明 PC5 能够访问 Branch Server，配置正确无误。

1.4 配置参考（仅展示本实验相关配置）

1.4.1 Branch-FW 的配置

```

#
vsys enable
#
vsys name vFW1 1
  assign interface GE0/0/1
  assign resource-class r0
#
vsys name vFW2 2
  assign interface GE0/0/2
  assign resource-class r0
#
ip vpn-instance vFW1
  ipv4-family
  ipv6-family
#
ip vpn-instance vFW2
  ipv4-family
  ipv6-family
#
interface MEth0/0/0
  ip binding vpn-instance _management_vpn_
  ip address 172.21.10.24 255.255.128.0
#
interface GE0/0/0
  ip address 100.1.33.1 255.255.255.252
  service-manage ping permit

```

```
#
interface GE0/0/1
 ip binding vpn-instance vFW1
 ip address 192.168.13.254 255.255.255.0
 service-manage ping permit
#
interface GE0/0/2
 ip binding vpn-instance vFW2
 ip address 192.168.14.254 255.255.255.0
 service-manage ping permit
#
interface Virtual-if0
#
interface Virtual-if1
#
interface Virtual-if2
#
ip route-static 0.0.0.0 0.0.0.0 100.1.33.2
ip route-static 192.168.13.0 255.255.255.0 vpn-instance vFW1
ip route-static 192.168.14.0 255.255.255.0 vpn-instance vFW2
#
firewall zone trust
 set priority 85
 add interface Virtual-if0
#
firewall zone untrust
 set priority 5
 add interface GE0/0/0
#
firewall zone dmz
 set priority 50
#
nat server 1 global 100.1.33.5 inside 192.168.13.106 no-reverse
#
security-policy
 rule name From_Internet_to_Server
  source-zone untrust
  destination-zone trust
  source-address 100.1.15.105 mask 255.255.255.255
  destination-address 192.168.13.0 mask 255.255.255.0
  action permit
#
switch vsys vFW1
#
interface GE0/0/1
 ip binding vpn-instance vFW1
 ip address 192.168.13.254 255.255.255.0
 service-manage ping permit
```

```
#
interface Virtual-if1
#
ip route-static 0.0.0.0 0.0.0.0 public
#
firewall zone local
    set priority 100
#
firewall zone trust
    set priority 85
#
firewall zone untrust
    set priority 5
    add interface Virtual-if1
#
firewall zone dmz
    set priority 50
    add interface GE0/0/1
#
security-policy
    rule name From_Office_to_Server
        source-zone untrust
        destination-zone dmz
        source-address 192.168.14.0 mask 255.255.255.0
        destination-address 192.168.13.0 mask 255.255.255.0
        action permit
    rule name From_Internet_to_server
        source-zone untrust
        destination-zone dmz
        source-address 100.1.15.105 mask 255.255.255.255
        destination-address 192.168.13.0 mask 255.255.255.0
        action permit
#
switch vsys vFW2
#
interface GE0/0/2
    ip binding vpn-instance vFW2
    ip address 192.168.14.254 255.255.255.0
    service-manage ping permit
#
interface Virtual-if2
#
ip route-static 0.0.0.0 0.0.0.0 public
#
firewall zone local
    set priority 100
#
firewall zone trust
```

```
set priority 85
add interface GE0/0/2
#
firewall zone untrust
set priority 5
add interface Virtual-if2
#
firewall zone dmz
set priority 50
#
security-policy
rule name From_Office_to_Server
source-zone trust
destination-zone untrust
source-address 192.168.14.0 mask 255.255.255.0
destination-address 192.168.13.0 mask 255.255.255.0
action permit
#
```

1.5 思考题

Virtual-if 接口与虚拟防火墙之间有什么关系？

答案：Virtual-if 接口是在创建虚拟防火墙的时候，与虚拟防火墙一起自动产生的，不需要手动创建，用于虚拟防火墙之间通信。

2 高可靠性实验

2.1 实验介绍

2.1.1 关于本实验

为保障企业总部网络架构的可靠性和业务连续性，总部出口防火墙 HQ-FW1 和 HQ-FW2 设备需组建主备模式的双机热备系统，同时下游入侵防御设备 IPS1 和 IPS2 组建透明模式负载分担双机热备系统，实现入侵防御和反病毒安全功能。

为满足企业总部大量的 Web 业务，并保证 Web 业务的稳定性及可靠性，企业总部在数据中心部署了两台 Web Server，并通过 SLB 技术，将两台服务器对外呈现一个虚拟 Web Server，为企业总部用户提供 Web 业务。

2.1.2 实验组网介绍

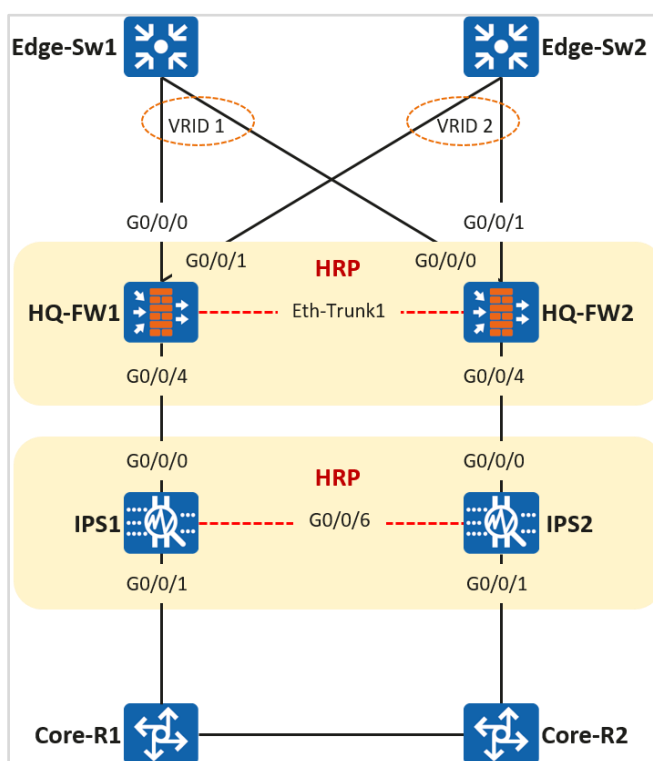


图2-1 实验拓扑图 (HRP)

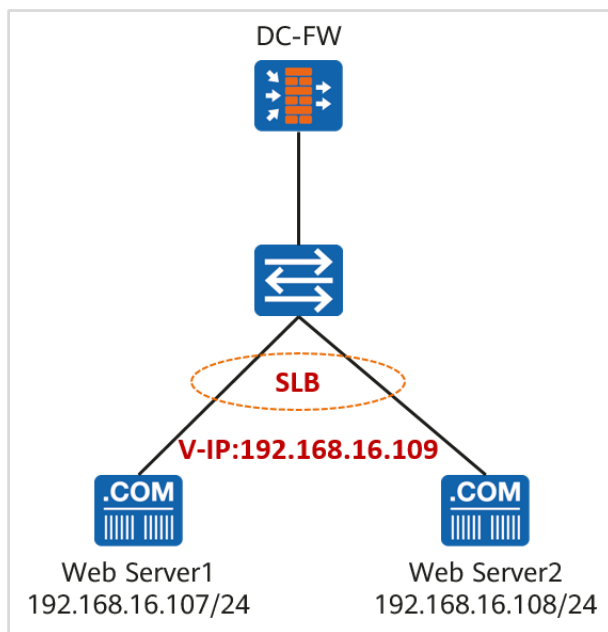


图2-2 实验拓扑图（SLB）

2.1.3 实验规划

1. 为保证企业总部网络可靠性, HQ-FW1 和 HQ-FW2 设备组建主备备份模式的双机热备系统。设备工作在路由模式, 因上下游对接的设备包含二层和三层网络设备, 故选择混合部署方式(动态路由协议&VGMP) 来实现双机热备系统, 设备心跳接口为 Eth-Trunk1。在主用防火墙 HQ-FW1 设备上配置健康检查实例, 探测上游非直连链路状态, 确保出口设备上游链路故障时, 及时切换双机主备状态, 保障业务连续。其余数据规划见下表:

表2-1 防火墙双机热备数据规划

项目	参数
认证密钥	Huawei@123
运行模式	主 (HQ-FW1) 备 (HQ-FW2)
心跳接口	Eth-Trunk1
主动抢占	启用
会话同步	开启
监控对象	接口: GE0/0/4 VRRP组: VRID1、VRID2 健康检查: FW2Edge

表2-2 健康检查数据规划

实例名称	探测接口	下一跳地址	目的地址	探测协议
FW2Edge	GE0/0/0	100.1.34.6	100.1.31.1	ICMP
	GE0/0/1	100.1.35.6	100.1.32.1	

2. 为进一步实现企业总部南北向流量的入侵防御和反病毒安全需求，在总部出口防火墙下游部署了 IPS 设备，同时为了保障企业总部网络架构的可靠性和业务韧性，需要将 IPS1 和 IPS2 设备组建为透明模式负载分担双机热备系统，具体数据规划如下：

表2-3 IPS 双机热备数据规划

项目	参数
认证密钥	Huawei@123
运行模式	负载分担
心跳接口	GE0/0/6
主动抢占	启用
监控对象	接口：GE0/0/0，GE0/0/1

3. 为保障企业总部 Web 类业务的可靠性和业务韧性，在总部数据中心部署了两台 Web Server（Web Server1 和 Web Server2），同时在 DC-FW 设备上部署 SLB 功能，将两台 Web Server 虚拟为一台 Web 服务器，对外提供 Web 服务。

表2-4 SLB 配置数据规划

项目	参数
实服务器组名称	Web_Server_Group
负载均衡算法	简单轮询
健康检查	启用
健康检查协议	ICMP
实服务器地址	192.168.16.107、192.168.16.108
虚拟服务名称	Web_Server_Group
虚拟服务器地址	192.168.16.109
负载模式	L4
源NAT功能	开启

2.2 实验配置任务

2.2.1 配置思路

防火墙双机热备部署思路：

1. 防火墙接口基础配置；
2. 创建健康检查实例；
3. 开启双机热备功能；
4. 运行模式选择主备备份；
5. 选择设备心跳接口；
6. 开启主动抢占；
7. Hello 报文周期保持默认；

图2-3 进入 G0/0/0 接口配置界面



修改GE

接口名称: GE0/0/0

描述:

虚拟系统: public

VPN实例: public

安全区域: untrust

模式: ☒ 路由 ☐ 交换 ☐ 旁路检测 ☐ 接口对

IPv4 **IPv6**

连接类型: ☒ 静态IP ☐ DHCP

IP地址: 100.1.34.1/255.255.255.248

默认网关:

接口带宽

入方向带宽: kbit/s <60-1000000> 过载保护阈值: %

出方向带宽: kbit/s <60-1000000> 过载保护阈值: %

访问控制管理

☐ HTTP ☐ HTTPS ☒ Ping ☐ SSH

取消 确定

图2-4 G0/0/0 接口基础配置

使用同样方式进入其他接口，完成如下配置：

修改GE

接口名称

GE0/0/1

描述

虚拟系统

public

VPN实例

public

安全区域

untrust

模式

路由

交换

旁路检测

接口对

IPv4

IPv6

连接类型

静态IP

DHCP

IP地址

100.1.35.1/255.255.255.248

一行一条记录。
输入格式为“10.1.1.1/255.255.255.0”
或者“10.1.1.1/24”。

默认网关

接口带宽

入方向带宽

kbit/s

<60-1000000>

过载保护阈值

%

出方向带宽

kbit/s

<60-1000000>

过载保护阈值

%

访问控制管理

HTTP

HTTPS

Ping

SSH

取消

确定

图2-5 G0/0/1 接口配置

修改GE

接口名称

GE0/0/4

描述

虚拟系统

public

VPN实例

public

安全区域

trust

模式

路由

交换

旁路检测

接口对

IPv4

IPv6

连接类型

静态IP

DHCP

IP地址

192.168.10.49/255.255.255.252

一行一条记录。
输入格式为“10.1.1.1/255.255.255.0”
或者“10.1.1.1/24”。

默认网关

取消

确定

图2-6 G0/0/4 接口配置



修改接口汇聚

接口名称: Eth-Trunk1

描述:

类型: 接口汇聚

虚拟系统: public

VPN实例: public

安全区域: dmz

模式: ☒ 路由 ☐ 交换 ☐ 旁路检测 ☐ 接口对

接口:

可选	已选
GE0/0/0	GE0/0/2
GE0/0/1	GE0/0/3
GE0/0/2	
GE0/0/3	

取消 确定

图2-7 Eth-Trunk1 接口配置

登录 HQ-FW2 设备 Web 管理界面（地址：https://172.21.10.22:8443/，账号：Webuser/Admin@123），执行与 HQ-FW1 设备同样的接口基础配置操作，此处不再演示。

步骤 2 创建健康检查实例

登录 HQ-FW1 设备 Web 管理界面（地址：https://172.21.10.21:8443/，账号：Webuser/Admin@123），选择“对象 > 健康检查 > 新建”，进入健康检查实例创建界面，执行以下操作：



USG6525F

面板 监控 策略 对象 网络 系统

健康检查列表

新建

新建健康检查

名称: FW2Edge

探测发包间隔: 5 秒

失败重试次数: 3

最小存活节点数: 1

健康检查源IP:

探测节点

新建 删除

协议	待检测目的IP/域名	端口	出接口	下一跳
☒ ICMP	100.1.32.1		GE0/0/1	100.1.35.6
☒ ICMP	100.1.31.1		GE0/0/0	100.1.34.6

取消 确定

图2-8 创建健康检查实例

健康检查实例创建成功后，效果如下：

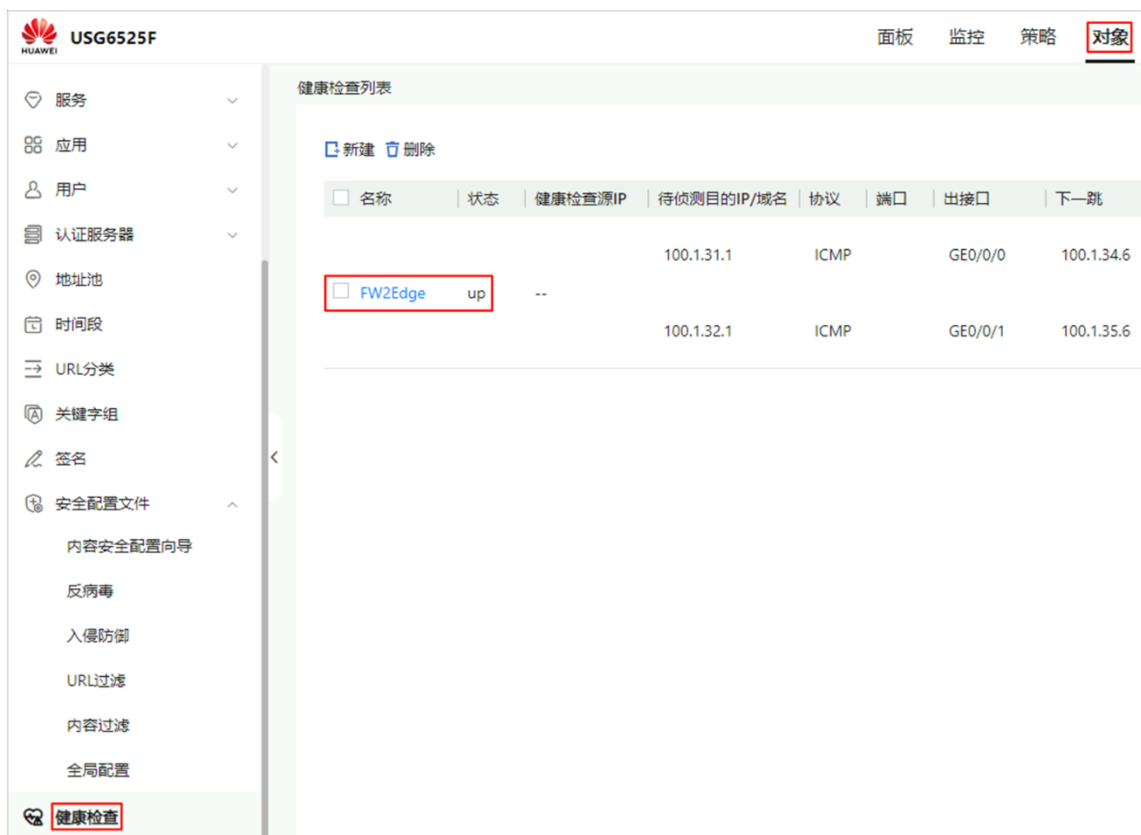


图2-9 查看健康检查实例

步骤 3 配置防火墙双机热备

登录 HQ-FW1 设备 Web 管理界面（地址：https://172.21.10.21:8443/，账号：Webuser/Admin@123），选择“系统 > 高可靠性 > 双机热备 > 配置”，进入双机热备配置界面，执行以下操作：



图2-10 进入双机热备配置界面



配置双机热备

双机热备 ☒ 1 请在组建双机设备前先查阅产品文档中的使用限制和注意事项!

认证密钥 2 Huawei@123 * <8-16> 字符

运行模式 ☒ 主备备份 ☐ 负载分担

运行角色 ☒ 主用 3 ☐ 备用

提示：双机热备的协议报文受 firewall packet-filter basic-protocol enable 命令控制。缺省情况下，需配置安全策略，允许协议报文通行。

心跳接口 4 Eth-Trunk1 * [配置] IP地址 192.168.10.17 * 对端接口IP 192.168.10.18 * +

主动抢占 ☒

静态路由由自动备份 ☒

策略路由由自动备份 ☐

Hello报文周期 1000 <500-60000> 毫秒

图2-11 双机热备基础配置



配置监控对象

☒ 接口监控 1 ☐ VRRP监控 ☐ 健康检查监控 ☐ BFD监控

提示：选择的监控接口应该是设备的业务接口。若选择VLAN，代表监控其成员接口的状态。

删除 | 接口 2 GE0/0/4 3 + 添加

接口名称 VLAN	状态	详细
GE0/0/4	✓	up

图2-12 配置接口监控对象



配置监控对象

☐ 接口监控 ☒ VRRP监控 1 ☐ 健康检查监控 ☐ BFD监控

提示：当业务接口工作在三层且连接交换机时，需要配置VRRP备份组。

新建 2 删除

VRID	接口	接口IP地址/掩码	虚拟IP地址/掩码 (可选)	角色	编辑
1	GE0/0/0	100.1.34.1/29	100.1.34.3/29	主 3	✎
2	GE0/0/1	100.1.35.1/29	100.1.35.3/29	主	✎

图2-13 配置 VRRP 监控对象

配置监控对象

接口监控 VRRP监控 健康检查监控 BFD监控

删除 FW2Edge 添加

健康检查名称	状态	目的IP/域名	出接口	下一跳
FW2Edge	up	100.1.31.1	GE0/0/0	100.1.34.6
		100.1.32.1	GE0/0/1	100.1.35.6

共 1 条 < 1 > 50条/页 前往 1 页

取消 确定

图2-14 配置健康检查联动

登录 HQ-FW2 设备 Web 管理界面（地址：<https://172.21.10.22:8443/>，账号：Webuser/Admin@123），选择“系统 > 高可靠性 > 双机热备 > 配置”，进入双机热备配置界面，执行以下操作：

配置双机热备

双机热备 ☒

认证密钥 Huawei@123 * <8-16> 字符

运行模式 ☒ 主备备份 ☐ 负载分担

运行角色 ☐ 主用 ☒ 备用

提示：双机热备的协议报文受 firewall packet-filter basic-protocol enable 命令控制。缺省情况下，需配置安全策略，允许协议报文通行。

心跳接口 Eth-Trunk1 * [配置] IP地址 192.168.10.18 * 对端接口IP 192.168.10.17 * +

主动抢占 ☒

静态路由自动备份 ☒

策略路由自动备份 ☐

Hello报文周期 1000 <500-60000> 毫秒

配置监控对象

接口监控 VRRP监控 健康检查监控 BFD监控

提示：当业务接口工作在三层且连接交换机时，需要配置VRRP备份组。

新建 删除

VRID	接口	接口IP地址/掩码	虚拟IP地址/掩码 (可选)	角色	编辑
1	GE0/0/0	100.1.34.2/29	100.1.34.3/29	备	
2	GE0/0/1	100.1.35.2/29	100.1.35.3/29	备	

取消 确定

图2-15 HQ-FW2 设备双机热备配置

步骤 4 IPS 设备接口基础配置

登录 IPS1 设备 Web 管理界面（地址：https://172.21.10.41:8443/，账号：Webuser/Admin@123），选择“网络 > 接口对”，进入接口对编辑界面，执行以下操作，删除相关接口对，手动编辑相关业务接口的 IP 地址和安全区域。

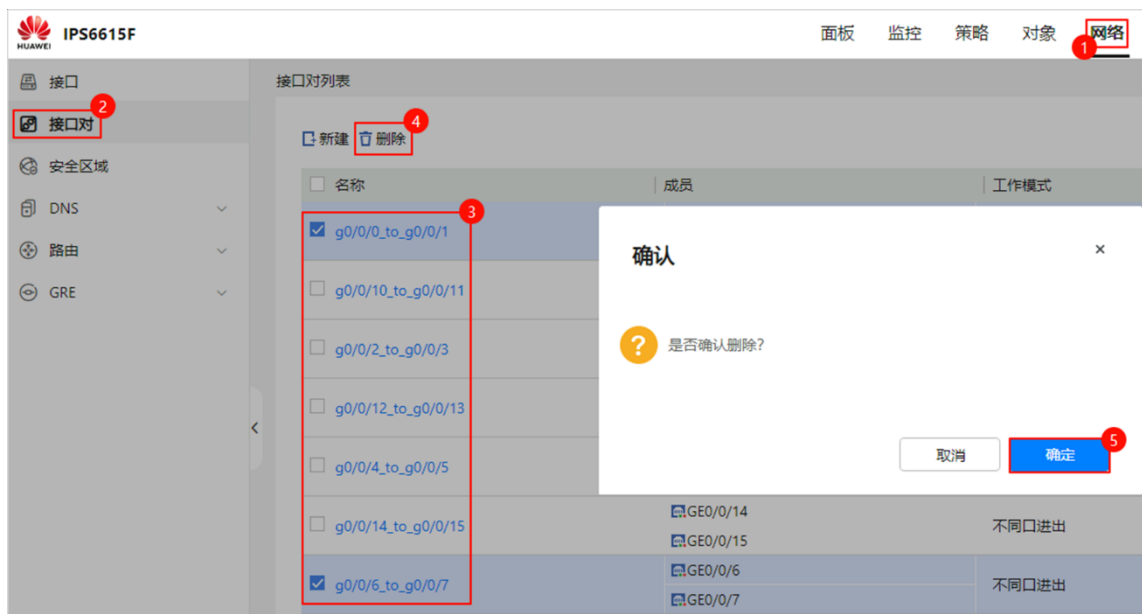


图2-16 删除接口对



图2-17 G0/0/0 接口配置

修改GE

×

接口名称

GE0/0/1

×

描述

安全区域

trust

1

▼

模式

路由

交换

旁路检测

接口对

2

连接类型

Access

Trunk

Hybrid

3

Access VLAN ID

1

<1-4094>

接口带宽

入方向带宽

kbit/s

<60-200000000>

出方向带宽

kbit/s

<60-200000000>

高级

取消

确定

4

图2-18 G0/0/1 接口配置

修改GE

×

接口名称

GE0/0/6

×

描述

虚拟系统

public

×

▼

VPN实例

public

×

▼

安全区域

dmz

1

▼

模式

路由

交换

旁路检测

接口对

2

IPv4

IPv6

IP地址

192.168.10.253/30

3

一行一条记录，

输入格式为“10.1.1.1/255.255.255.0”

或者“10.1.1.1/24”。

接口带宽

入方向带宽

kbit/s

<60-200000000>

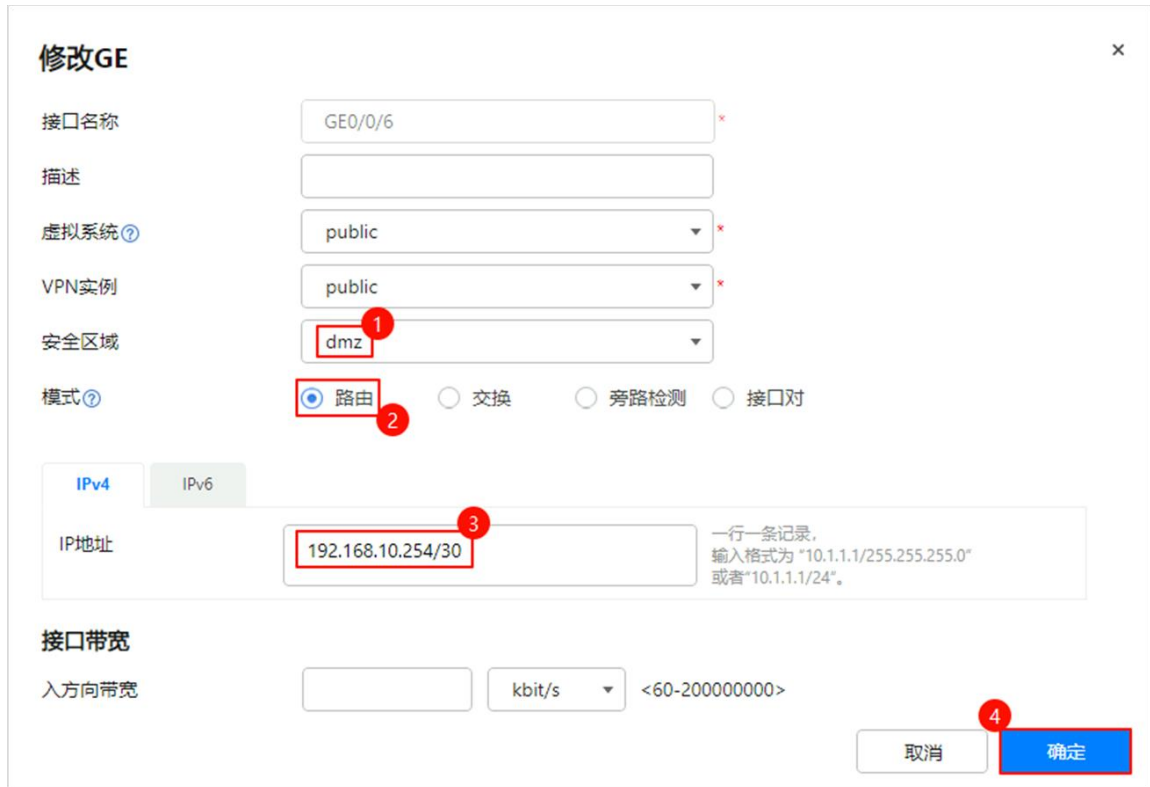
取消

确定

4

图2-19 G0/0/6 接口配置

登录 IPS2 设备 Web 管理界面（地址：https://172.21.10.42:8443/，账号：Webuser/Admin@123），执行与 IPS1 设备同样的操作，完成接口对的删除及接口 G0/0/0 和 G0/0/1 的配置，接口 G0/0/6 的配置如下：



修改GE

接口名称: GE0/0/6

描述:

虚拟系统: public

VPN实例: public

安全区域: dmz

模式: ☒ 路由 ☐ 交换 ☐ 旁路检测 ☐ 接口对

IPv4 IPv6

IP地址: 192.168.10.254/30

接口带宽

入方向带宽: kbit/s <60-200000000>

取消 确定

图2-20 IPS2 设备 G0/0/6 接口配置

步骤 5 配置 IPS 双机热备

登录 IPS1 设备 Web 管理界面（地址：https://172.21.10.41:8443/，账号：Webuser/Admin@123），选择“系统 > 高可靠性 > 双机热备 > 配置”，进入双机热备配置界面，执行以下操作：

配置双机热备

双机热备 ☒ 1

认证密钥 2 Huawei@123 * <8-16> 字符

运行模式 3 ☐ 主备备份 ☒ 负载分担 提示：默认启用会话快速备份。

提示：双机热备的协议报文受 firewall packet-filter basic-protocol enable 命令控制。缺省情况下，需配置安全策略，允许协议报文通行。

心跳接口 4 GE0/0/6 * [配置] IP地址 192.168.10.253 * 对端接口IP 192.168.10.254 *

主动抢占 ☒

静态路由由自动备份 ☐

策略路由由自动备份 ☐

Hello报文周期 1000 <500-60000> 毫秒

配置监控对象

☒ 接口监控 5 ☐ VRRP监控 ☐ 健康检查监控 ☐ BFD监控

提示：选择的监控接口应该是设备的业务接口。若选择VLAN，代表监控其成员接口的状态。

删除 | 请选择类别 | 添加

接口名称 VLAN	状态	详细
☐ GE0/0/0	✓	up 6
☐ GE0/0/1	✓	up

取消 确定 7

图2-21 IPS1 设备双机热备配置

登录 IPS2 设备 Web 管理界面（地址：https://172.21.10.42:8443/，账号：Webuser/Admin@123），选择“系统 > 高可靠性 > 双机热备 > 配置”，进入双机热备配置界面，执行以下操作：

新建实服务器组

×

* 名称

Web_Server_Group

负载均衡算法

简单轮询

实服务器繁忙策略

重新调度

IP地址类型

☒ IPv4
 ☐ IPv6

^ 健康检查

启用

☒

协议

ICMP

检查间隔

5

秒

失败次数

3

次

实服务器列表

删除

新建

☐	实服务器地址	端口	服务器状态	描述	最大连接数
☐	192.168.16.107		健康检查		
☐	192.168.16.108		健康检查		

共 2 条

取消

确定

图2-23 DC-FW 设备创建实服务器组

步骤 7 创建虚拟服务

继续在 DC-FW 设备 Web 管理界面选择“策略 > 服务器负载均衡 > 虚拟服务 > 新建”执行以下配置：

新建虚拟服务

×

* 名称

HQ_Web_Server

IP地址类型

☒ IPv4
 ☐ IPv6

* 虚拟服务器地址 ②

192.168.16.109

* 实服务器组

Web_Server_Group

会话保持

-- NONE --

负载模式

☒ 4层
 ☐ 7层

启用

☒ 启用
 ☐ 禁用

^ 高级

协议

Any

端口

Any

访问认证

☐

最大并发连接数 ②

请输入 1-4294967295 内的整数

取消

确定

图2-24 DC-FW 设备创建虚拟服务

步骤 8 配置安全策略（SLB 相关）

USG6000F 产品默认对 SLB 流量不进行安全策略过滤，但是为了严格管控各类业务流量，建议通过命令行（此功能目前仅支持命令行配置），开启针对 SLB 业务流量的安全策略管理功能。

```
[DC-FW] slb
[DC-FW-slb] security-policy enable
```

开启针对 SLB 流量的安全策略管理功能后，创建安全策略放行 SLB 业务流量，在 DC-FW 设备 Web 管理界面选择“策略 > 安全策略 > 安全策略 > 新建安全策略”创建以下安全策略：

图2-25 DC-FW 设备 SLB 安全策略配置

2.3 结果验证

2.3.1 防火墙双机热备配置查看

登录 HQ-FW1 设备 Web 管理界面（地址：<https://172.21.10.21:8443/>，账号：Webuser/Admin@123），选择“系统 > 高可靠性 > 双机热备”，进入双机热备配置查看界面，效果如下：

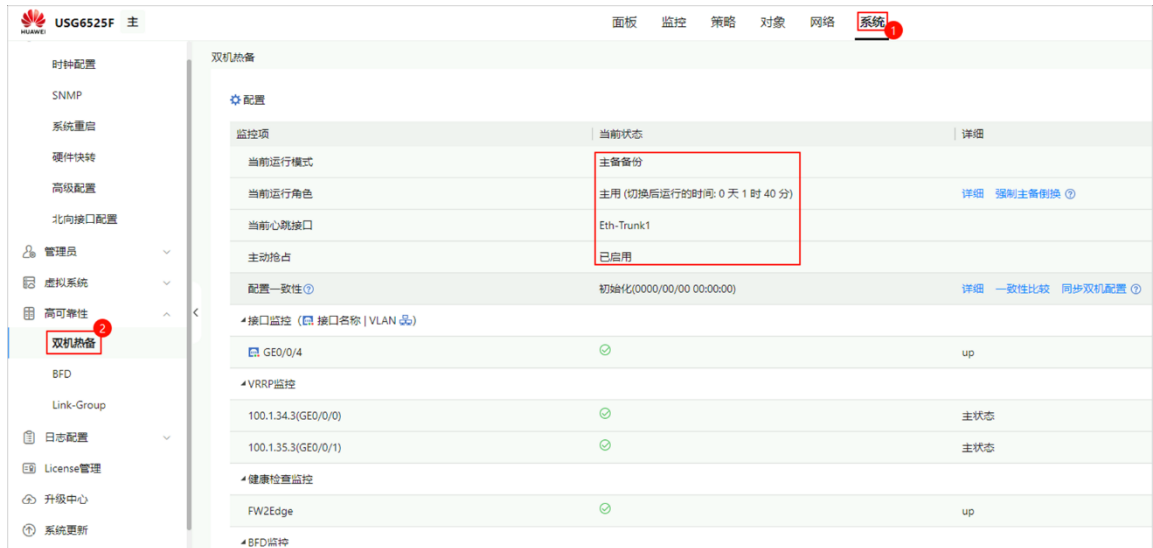


图2-26 HQ-FW1 双机热备配置

登录 HQ-FW2 设备 Web 管理界面 (地址: <https://172.21.10.22:8443/>, 账号: Webuser/Admin@123), 选择“系统 > 高可靠性 > 双机热备”, 进入双机热备配置查看界面, 效果如下:



图2-27 HQ-FW2 双机热备配置

2.3.2 IPS 双机热备配置查看

登录 IPS1 设备 Web 管理界面 (地址: <https://172.21.10.41:8443/>, 账号: Webuser/Admin@123), 选择“系统 > 高可靠性 > 双机热备”, 进入双机热备配置查看界面, 效果如下:

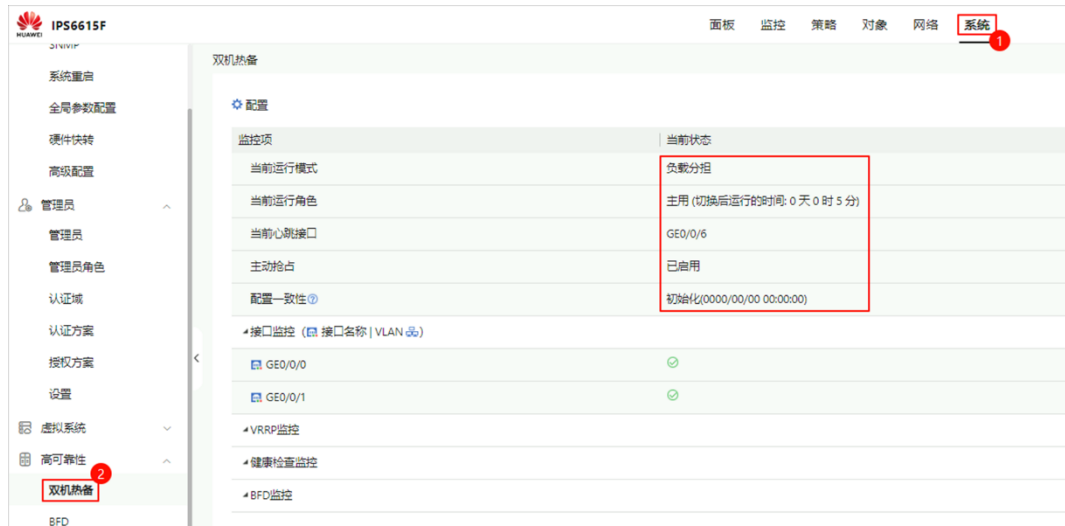


图2-28 IPS1 双机热备配置

登录 IPS2 设备 Web 管理界面（地址：<https://172.21.10.42:8443/>，账号：Webuser/Admin@123），选择“系统 > 高可靠性 > 双机热备”，进入双机热备配置查看界面，效果如下：



图2-29 IPS2 双机热备配置

2.3.3 SLB 配置查看

登录 DC-FW 设备 Web 管理界面（地址：<https://172.21.10.23:8443/>，账号：Webuser/Admin@123），选择“策略 > 服务器负载均衡 > 实服务器组”进入实服务器组列表界面，效果如下：



图2-30 SLB 实服务器组配置

继续选择“策略 > 服务器负载均衡 > 虚拟服务”查看，效果如下：

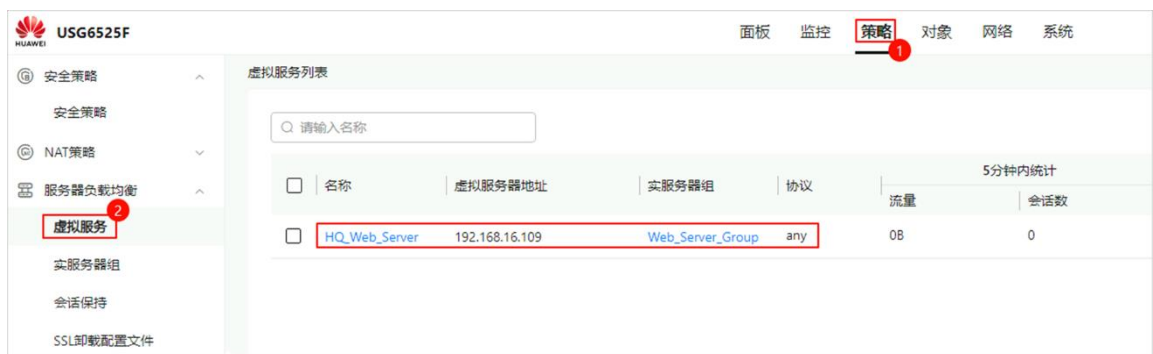


图2-31 SLB 虚拟服务配置

2.4 配置参考（仅展示本实验相关配置）

2.4.1 HQ-FW1 的配置

```
healthcheck enable
#
hrp enable
hrp auto-sync config static-route
hrp interface Eth-Trunk1 remote 192.168.10.18
hrp track healthcheck FW2Edge
hrp track interface GE0/0/4
hrp authentication-key Huawei@123
#
undo firewall packet-filter basic-protocol enable
#
interface MEth0/0/0
 ip binding vpn-instance _management_vpn_
 ip address 172.21.10.21 255.255.128.0
#
interface Eth-Trunk1
 ip address 192.168.10.17 255.255.255.252
```

```
#
interface GE0/0/0
 ip address 100.1.34.1 255.255.255.248
 vrrp vrid 1 virtual-ip 100.1.34.3 active
 service-manage ping permit
#
interface GE0/0/1
 ip address 100.1.35.1 255.255.255.248
 vrrp vrid 2 virtual-ip 100.1.35.3 active
 service-manage ping permit
#
interface GE0/0/2
 eth-trunk 1
#
interface GE0/0/3
 eth-trunk 1
#
interface GE0/0/4
 ip address 192.168.10.49 255.255.255.252
 service-manage ping permit
#
ospf 1 router-id 21.21.21.21
 default-route-advertise
 opaque-capability enable
 area 0.0.0.0
  network 192.168.10.48 0.0.0.3
#
ip route-static 0.0.0.0 0.0.0.0 100.1.34.6
ip route-static 0.0.0.0 0.0.0.0 100.1.35.6 preference 100
#
healthcheck name FW2Edge
 destination 100.1.31.1 interface GE0/0/0 next-hop 100.1.34.6 protocol icmp
 destination 100.1.32.1 interface GE0/0/1 next-hop 100.1.35.6 protocol icmp
#
firewall zone trust
 set priority 85
 add interface GE0/0/4
#
firewall zone untrust
 set priority 5
 add interface GE0/0/0
 add interface GE0/0/1
#
firewall zone dmz
 set priority 50
 add interface Eth-Trunk1
#
return
```

2.4.2 HQ-FW2 的配置

```
hrp enable
hrp device standby
hrp auto-sync config static-route
hrp interface Eth-Trunk1 remote 192.168.10.17
hrp authentication-key Huawei@123
#
undo firewall packet-filter basic-protocol enable
#
interface MEth0/0/0
 ip binding vpn-instance _management_vpn_
 ip address 172.21.10.22 255.255.128.0
#
interface Eth-Trunk1
 ip address 192.168.10.18 255.255.255.252
#
interface GE0/0/0
 ip address 100.1.34.2 255.255.255.252
#
interface GE0/0/1
 ip address 100.1.35.2 255.255.255.252
#
interface GE0/0/2
 eth-trunk 1
#
interface GE0/0/3
 eth-trunk 1
#
interface GE0/0/4
 ip address 192.168.10.65 255.255.255.252
#
interface GE0/0/5
 ip address 172.21.10.52 255.255.128.0
#
ospf 1 router-id 22.22.22.22
 default-route-advertise
 opaque-capability enable
 area 0.0.0.0
  network 192.168.10.64 0.0.0.3
#
ip route-static 0.0.0.0 0.0.0.0 100.1.34.6
ip route-static 0.0.0.0 0.0.0.0 100.1.35.6 preference 100
#
lldp enable
#
firewall zone local
 set priority 100
```

```
#
firewall zone trust
  set priority 85
  add interface GE0/0/4
#
firewall zone untrust
  set priority 5
  add interface GE0/0/0
  add interface GE0/0/1
#
firewall zone dmz
  set priority 50
  add interface Eth-Trunk1
#
return
```

2.4.3 IPS1 的配置

```
#
hrp enable
hrp mirror session enable
hrp interface GE0/0/6 remote 192.168.10.254
hrp track interface GE0/0/0
hrp track interface GE0/0/1
hrp authentication-key Huawei@123
#
interface MEth0/0/0
  ip binding vpn-instance _management_vpn_
  ip address 172.21.10.41 255.255.128.0
#
interface GE0/0/0
  portswitch
  port default vlan 1
#
interface GE0/0/1
  portswitch
  port default vlan 1
#
interface GE0/0/6
  ip address 192.168.10.253 255.255.255.252
#
firewall zone trust
  set priority 85
  add interface 10GE0/0/0
  add interface 10GE0/0/2
  add interface 10GE0/0/4
  add interface GE0/0/1
  add interface GE0/0/10
```

```
add interface GE0/0/12
add interface GE0/0/14
add interface GE0/0/2
add interface GE0/0/4
add interface GE0/0/8
#
firewall zone untrust
set priority 5
add interface 10GE0/0/1
add interface 10GE0/0/3
add interface 10GE0/0/5
add interface GE0/0/0
add interface GE0/0/11
add interface GE0/0/13
add interface GE0/0/15
add interface GE0/0/3
add interface GE0/0/5
add interface GE0/0/7
add interface GE0/0/9
#
firewall zone dmz
set priority 50
add interface GE0/0/6
#
pair-interface name g0/0/10_to_g0/0/11
pair GE0/0/10 GE0/0/11
pair-interface name g0/0/2_to_g0/0/3
pair GE0/0/2 GE0/0/3
pair-interface name g0/0/12_to_g0/0/13
pair GE0/0/12 GE0/0/13
pair-interface name g0/0/4_to_g0/0/5
pair GE0/0/4 GE0/0/5
pair-interface name g0/0/14_to_g0/0/15
pair GE0/0/14 GE0/0/15
pair-interface name g0/0/8_to_g0/0/9
pair GE0/0/8 GE0/0/9
pair-interface name 10ge0/0/0_to_10ge0/0/1
pair 10GE0/0/0 10GE0/0/1
pair-interface name 10ge0/0/2_to_10ge0/0/3
pair 10GE0/0/2 10GE0/0/3
pair-interface name 10ge0/0/4_to_10ge0/0/5
pair 10GE0/0/4 10GE0/0/5
#
return
```

2.4.4 IPS2 的配置

```
#
```

```
hrp enable
hrp mirror session enable
hrp interface GE0/0/6 remote 192.168.10.253
hrp track interface GE0/0/0
hrp track interface GE0/0/1
hrp authentication-key Huawei@123
#
interface MEth0/0/0
 ip binding vpn-instance _management_vpn_
 ip address 172.21.10.42 255.255.128.0
#
interface GE0/0/0
 portswitch
 port default vlan 1
#
interface GE0/0/1
 portswitch
 port default vlan 1
#
interface GE0/0/6
 ip address 192.168.10.254 255.255.255.252
#
firewall zone trust
 set priority 85
 add interface 10GE0/0/0
 add interface 10GE0/0/2
 add interface 10GE0/0/4
 add interface GE0/0/1
 add interface GE0/0/10
 add interface GE0/0/12
 add interface GE0/0/14
 add interface GE0/0/2
 add interface GE0/0/4
 add interface GE0/0/8
#
firewall zone untrust
 set priority 5
 add interface 10GE0/0/1
 add interface 10GE0/0/3
 add interface 10GE0/0/5
 add interface GE0/0/0
 add interface GE0/0/11
 add interface GE0/0/13
 add interface GE0/0/15
 add interface GE0/0/3
 add interface GE0/0/5
 add interface GE0/0/7
 add interface GE0/0/9
```



```
#
firewall zone dmz
  set priority 50
  add interface GE0/0/6
#
pair-interface name g0/0/10_to_g0/0/11
  pair GE0/0/10 GE0/0/11
pair-interface name g0/0/2_to_g0/0/3
  pair GE0/0/2 GE0/0/3
pair-interface name g0/0/12_to_g0/0/13
  pair GE0/0/12 GE0/0/13
pair-interface name g0/0/4_to_g0/0/5
  pair GE0/0/4 GE0/0/5
pair-interface name g0/0/14_to_g0/0/15
  pair GE0/0/14 GE0/0/15
pair-interface name g0/0/8_to_g0/0/9
  pair GE0/0/8 GE0/0/9
pair-interface name 10ge0/0/0_to_10ge0/0/1
  pair 10GE0/0/0 10GE0/0/1
pair-interface name 10ge0/0/2_to_10ge0/0/3
  pair 10GE0/0/2 10GE0/0/3
pair-interface name 10ge0/0/4_to_10ge0/0/5
  pair 10GE0/0/4 10GE0/0/5
#
return
```

2.4.5 DC-FW 的配置

```
#
slb
  security-policy enable
  group 0 Web_Server_Group
    health-check type icmp
    rserver 0 rip 192.168.16.107 status health-check
    rserver 1 rip 192.168.16.108 status health-check
  vsrver 0 HQ_Web_Server
    vip 0 192.168.16.109
    group Web_Server_Group
    protocol any
    source-nat interface-address
#
security-policy
  rule name slb
    source-zone untrust
    vsrver HQ_Web_Server
    action permit
#
```

2.5 思考题

在本实验中，部署在防火墙下游的 IPS 设备为何部署负载均衡模式的双机热备系统，而不是和上游设备保持一致，部署主备备份模式的双机热备系统？

答案：本方案中 IPS 设备上游为三层设备，运行模式需要选择负载分担，业务主备路径可依赖出口防火墙的主备模式双机热备系统控制的动态路由协议开销进行区分。若运行模式选择主备备份，备机的 VLAN 将被禁用，主备切换时，IPS 上下行设备需要一定时间重新相互学习路由，将导致业务中断。

3 交换安全实验

3.1 实验介绍

3.1.1 关于本实验

公司网络有线办公区域内设有 ACC 接入层交换机，上行连接汇聚层 AGG 交换机，下行为 PC 提供网络接入服务。为保证有线办公区内所有 PC 上网的安全性，预防设备误连线造成的环路或恶意仿冒攻击等，在交换机侧部署 MAC 地址漂移检测、端口安全以及 DHCP-Snooping 技术。

3.1.2 实验组网介绍

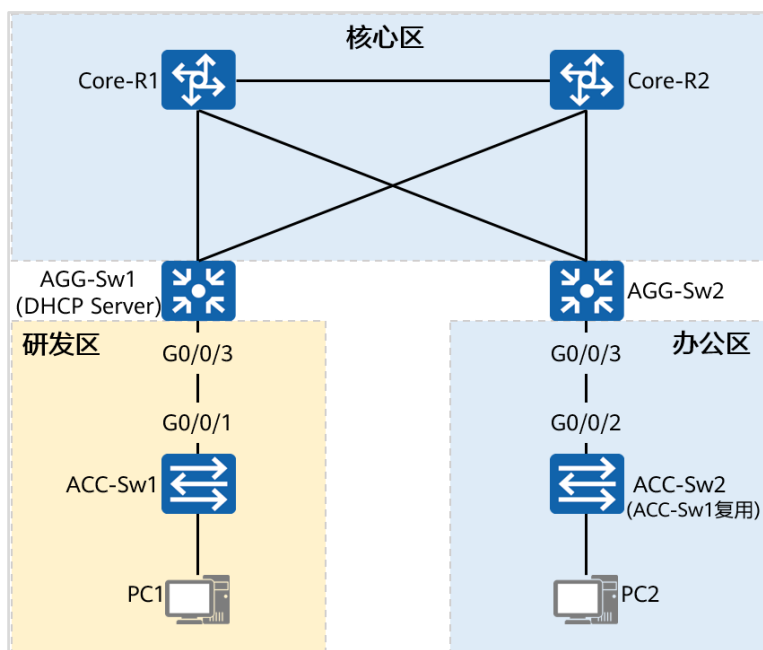


图3-1 实验拓扑图

3.1.3 实验规划

1. 总部有线办公区域部署有接入和汇聚层交换机 ACC-SW 以及 AGG-SW 为员工提供互联网访问服务。为保障研发区域内部的二层接入通信安全，需要在 AGG-SW1 与 ACC-SW1 部署交换安全技术。
2. 为防止二层环路或是仿冒攻击产生的 MAC 漂移，需在 AGG-SW1 直连 ACC-SW1 的接口上部署环路检测功能，当检测到环路发生时，接口自动关闭。

3. 研发区办公人员相对固定，为防止无关外来人员滥用接入网络资源，造成潜在安全隐患，需在 ACC-SW1 配置端口安全技术，每接口仅允许至多 5 个 MAC 接入。
4. 研发区终端由 AGG-SW1 统一分配动态 IP 地址，为实现 DHCP 攻击防范，需要在 ACC-SW1 上部署 DHCP-snooping 技术，仅接受来自 AGG-SW1 响应的 DHCP ACK、DHCP NAK 和 DHCP Offer 报文。

3.2 实验配置任务

3.2.1 配置思路

1. 总部研发区网络汇聚以及接入层交换机 AGG-SW1\ACC-SW1 间的互联配置已预配，实验前请检查，若有配置遗漏，请及时联系培训讲师，无需自行配置。
2. 公司典型组网环境中汇聚交换机通常下挂若干接入层交换机，若接入层交换机存在误连接，则容易在汇聚交换机上观察到明显的 MAC 漂移现象，极大消耗设备 CPU 资源，甚至可能导致故障点外的接入层业务受到影响，故需要在汇聚交换机 AGG-SW1 下联 ACC-SW1 的接口下配置 MAC 地址漂移检测功能。
3. 公司部分办公区域人员流动情况相对复杂，工位有线接入网口意被恶意利用发起仿冒攻击，为最大限度减少此类攻击并增加接入层安全性，需在接入交换机 ACC-SW1 直连 PC 的网口下配置端口安全功能。
4. 公司研发区终端使用由汇聚层交换机提供的 DHCP 服务获取动态地址上网，为规避 DHCP 仿冒攻击，需要在 ACC-SW1 上配置 DHCP-Snooping 功能。

3.2.2 配置步骤

步骤 1 AGG-SW1 配置 MAC 地址漂移检测

登录 AGG-SW1 并进入系统视图。

```
<AGG-SW1>system-view
```

使能 MAC 漂移检测功能。

```
[AGG-SW1] mac-address flapping detection
```

进入 G0/0/3 接口视图（此接口与下行 ACC 交换机直连）。

```
[AGG-SW1] interface g0/0/3
```

配置在 G0/0/3 接口检测到 MAC 漂移后关闭该接口。

```
[AGG-SW1-GE0/0/3] mac-address flapping action error-down  
[AGG-SW1-GE0/0/3] quit
```

步骤 2 ACC-SW1 配置端口安全

登录 ACC-SW1 并进入系统视图。

```
<ACC-SW1>system-view
```

进入 GE0/0/22 接口（此接口下行直连实验环境虚拟机）。

```
[ACC-SW1] interface g0/0/22
```

使能端口安全功能。

```
[ACC-SW1-GE0/0/22] port-security enable
```

设置该接口下 MAC 地址最大学习数量为 5。

```
[ACC-SW1-GE0/0/22] port-security max-mac-num 5
```

设置将接口学习到的 MAC 地址转化为 sticky 类型 MAC。

```
[ACC-SW1-GE0/0/22] port-security mac-address sticky
```

```
[ACC-SW1-GE0/0/22] quit
```

步骤 3 ACC-SW1 配置 DHCP snooping

登录 ACC-SW1 并进入系统视图。

```
<ACC-SW1> system-view
```

使能 DHCP 以及 DHCP snooping 功能。

```
[ACC-SW1] DHCP enable
```

```
[ACC-SW1] DHCP snooping enable
```

进入 vlan11 配置视图（PC1、ACC-SW1、AGG-SW1 使用 vlan11 互联）。

```
[ACC-SW1] vlan 11
```

在 vlan11 下使能 DHCP snooping，并指定与 AGG-SW1 互联的 g0/0/1 接口为 DHCP 报文的信任接口。

```
[ACC-SW1-vlan11] DHCP snooping enable
```

```
[ACC-SW1-vlan11] DHCP snooping trusted interface g0/0/1
```

3.3 结果验证

3.3.1 查看 MAC 地址漂移的配置信息

在 AGG-SW1 上使用命令 display mac-address flapping 查看配置结果。

```
[AGG-SW1]display mac-address flapping
```

```
MAC address Flapping Configurations :
```

```
-----
Flapping detection      : Enable
Aging time(sec)        : 300
Quit VLAN Recover time(min) : 10
Exclude VLAN list      : -
Low level VLAN list     : -
Middle level VLAN list  : 1 to 4094
High level VLAN list    : -
-----
```

3.3.2 查看端口安全的配置信息

在 ACC-SW1 上使用命令 `display mac-address sticky` 查看配置结果，可以看到共有 3 条 sticky MAC 条目。

```
[ACC-Sw1]dis mac-address sticky
```

MAC Address	VLAN/VSI/BD	Learned-From	Type
286e-d489-e012 1/-/-		GE0/0/22	sticky
e8bd-d103-cac0 1/-/-		GE0/0/22	sticky
286e-d489-95ee 11/-/-		GE0/0/22	sticky

```
Total items displayed = 3
```

3.3.3 查看 DHCP-Snooping 的配置结果

在 ACC-SW1 上使用命令 `display dhcp snooping statistics global` 查看 DHCP 报文的统计信息。

```
[ACC-Sw1]dis dhcp snooping statistics global
```

DHCP Snooping Statistics:

Client Request:

Dhcp Discover:	182325
Dhcp Request:	74
Dhcp Decline:	0
Dhcp Release:	0
Dhcp Inform:	0

Server Reply:

Dhcp Offer:	0
Dhcp Ack:	2
Dhcp Nak:	0

Drop Packet:

Dropped by mac-address check:	0
Dropped by untrust reply:	0
Dropped by request conflict:	0
Dropped by no trust port:	0

Delete DHCP snooping table:

Receive release packet:	0
Receive decline packet:	0
Lease expired:	1
User command:	0
Client transfers:	0
Interface down:	0

Arp detect:	0
Ucm notify:	0
Terminal Identity:	
Single upload count:	0
Batch get count:	0
Batch upload count:	0

3.4 配置参考（仅展示本实验相关配置）

3.4.1 AGG-SW1 的配置

```
#
sysname AGG-SW1
#
mac-address flapping detection
#
interface GE0/0/3
mac-address flapping action error-down
#
Return
```

3.4.2 ACC-SW1 的配置

```
#
sysname ACC-SW1
#
DHCP enable
#
DHCP snooping enable
#
vlan 11
DHCP snooping enable
DHCP snooping trusted interface GE0/0/1
#
interface GE0/0/22
port-security enable
port-security max-mac-num 5
port-security mac-address sticky
#
Return
```

3.5 思考题

华为可提供众多网络安全设备保障企业网络安全，为何还需要部署交换安全技术？

答：华为其他安全设备提供的安全能力主要体现在对报文和数据流二层及二层以上信息的深度检测控制，而交换安全技术主要针对二层场景，但这并不代表交换安全不重要，相反，企业内网接入层以下广播域内的安全管控是非常薄弱的，交换安全技术能在一定程度上降低接入层的安全风险。

4 路由安全实验

4.1 实验介绍

4.1.1 关于本实验

为了保障分支网络中的业务正常运行,需要创建分支用户区域安全网关 vFW2 虚拟系统管理员,进行此区域安全业务专项管理,同时为了防止基于源 IP 地址欺骗的网络攻击行为,对登录 vFW2 的流量进行 URPF 检查。

在对安全性要求较高的网络中,可以通过在路由器上配置 OSPF 报文验证来提高 OSPF 网络的安全性。本实验将在区域 0 开启 OSPF 报文验证。

4.1.2 实验组网介绍

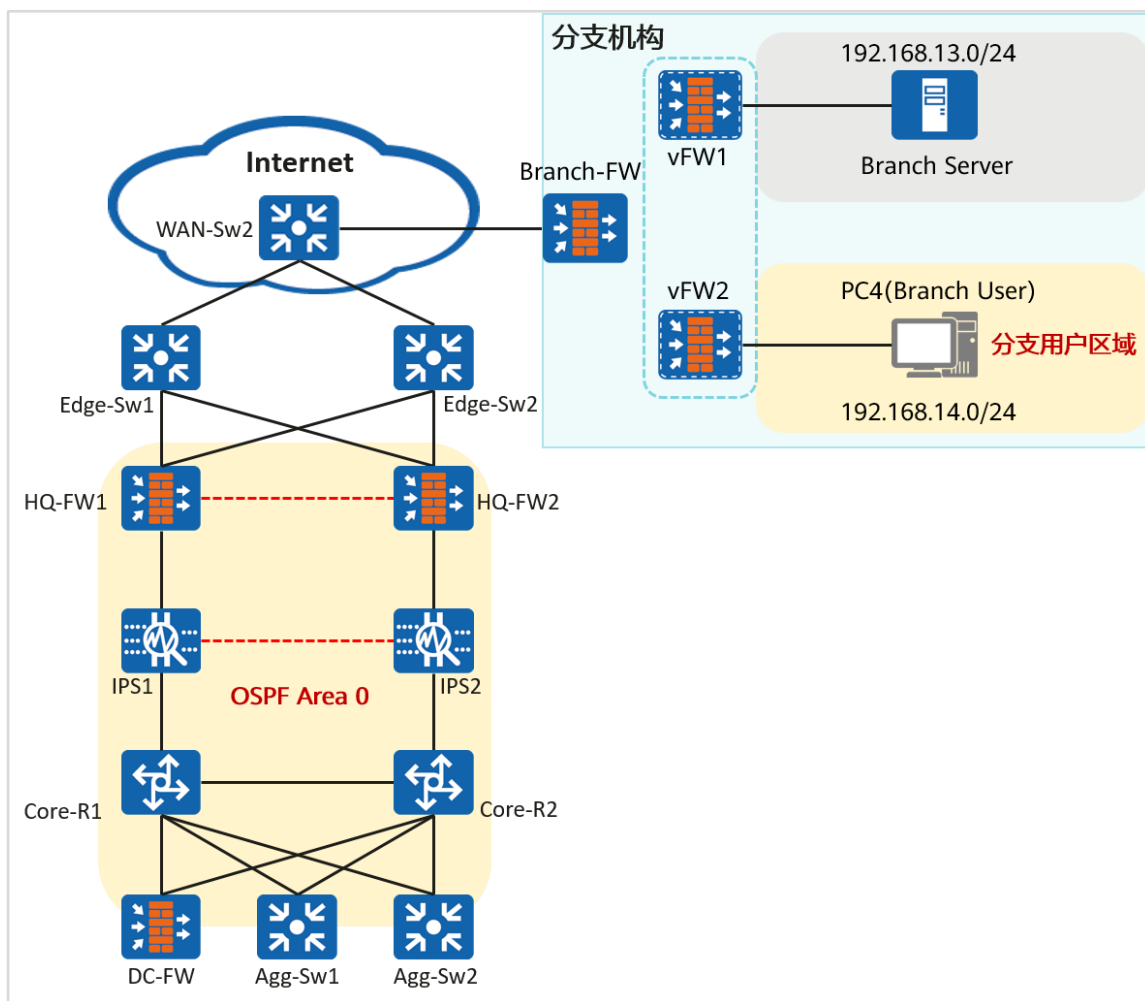


图4-1 实验拓扑图

4.1.3 实验规划

根据业务规划，在 Branch-FW 上为 vFW2 创建管理员账号。同时为了防止源 IP 地址欺骗的网络攻击行为，对登录 vFW2 的流量进行 URPF 检查，攻击流量将被丢弃。

总部网络中部署了 OSPF 进行路由学习，为保障总部网络的安全，在 OSPF 的区域 0 中开启认证，认证通过的设备才能学习路由。

表4-1 端口类型及参数设计

设备	端口(安全区域/所属系统)	IP
HQ-FW1	GE0/0/4(Trust/public)	192.168.10.49/30
HQ-FW2	GE0/0/4(Trust/public)	192.168.10.65/30
DC-FW	GE0/0/0(Trust/public)	192.168.16.254/24
	GE0/0/1(Untrust/public)	192.168.10.41/30
	GE0/0/2(Untrust/public)	192.168.10.45/30
Branch-FW	GE0/0/0(Untrust/public)	100.1.33.1/30

	Virtual-if0(Trust/public)	/
	GE0/0/2(Trust/vFW2)	192.168.14.254/24
	Virtual-if2(Untrust/public)	/
Core-R1	GE0/0/1	192.168.10.50/30
	GE0/0/2	192.168.10.53/30
	GE0/0/5	192.168.10.42/30
Core-R2	GE0/0/1	192.168.10.66/30
	GE0/0/2	192.168.10.54/30
	GE0/0/5	192.168.10.46/30
PC4	/	192.168.14.104

4.2 实验配置任务

4.2.1 配置思路

1. 在 Branch-FW 上为 vFW2 创建虚拟防火墙的管理员。
2. 在 Branch-FW 上配置 URPF 检查，防范攻击者仿冒运维管理人员接入网络。
3. 在总部网络的 OSPF 区域 0 中开启协议认证。

4.2.2 配置步骤

步骤 1 创建 vFW2 管理员账号

登录 Branch-FW (地址: <https://172.21.10.24:8443/>, 账号: Webuser/Admin@123), 单击右上角“虚拟系统”的下拉菜单, 选择“vFW2”, 切换至虚拟防火墙 vFW2, 如下图:



图4-2 切换 vFW2 虚拟系统

在 vFW2 虚拟系统 Web 管理界面选择“系统 > 管理员 > 管理员”, 单击“新建”, 创建用户名为 admin@@vFW2, 密码为“Huawei@123”的管理员账号, 角色为“系统管理员”, 允许管理员通过 Web 方式登录 vFW2, 如下图:

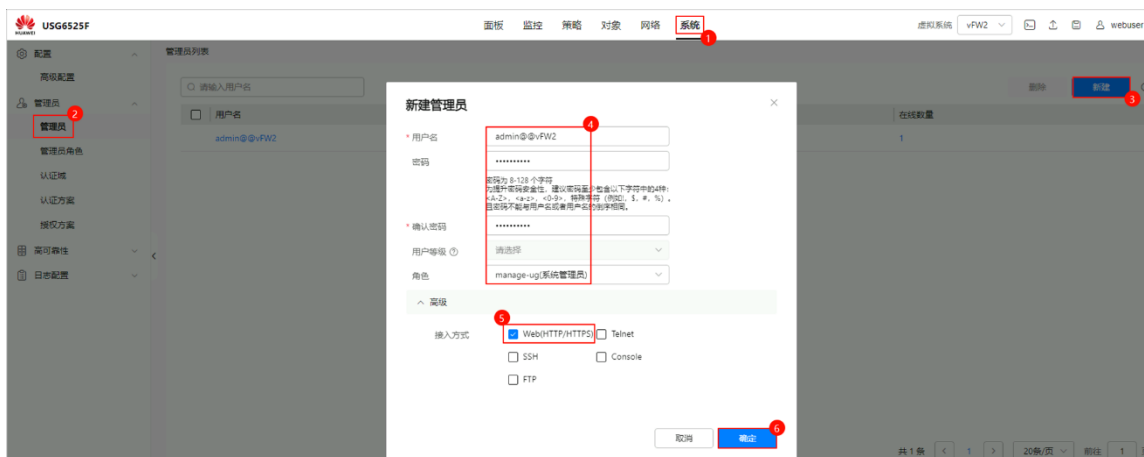


图4-3 创建 vFW2 系统管理员

管理员账号创建完成后，效果如下图：



图4-4 vFW2 管理员信息

选择“网络 > 接口”，在 GE0/0/2 接口下开启访问管理功能，开启 HTTPS 管理功能，具体操作如下图：

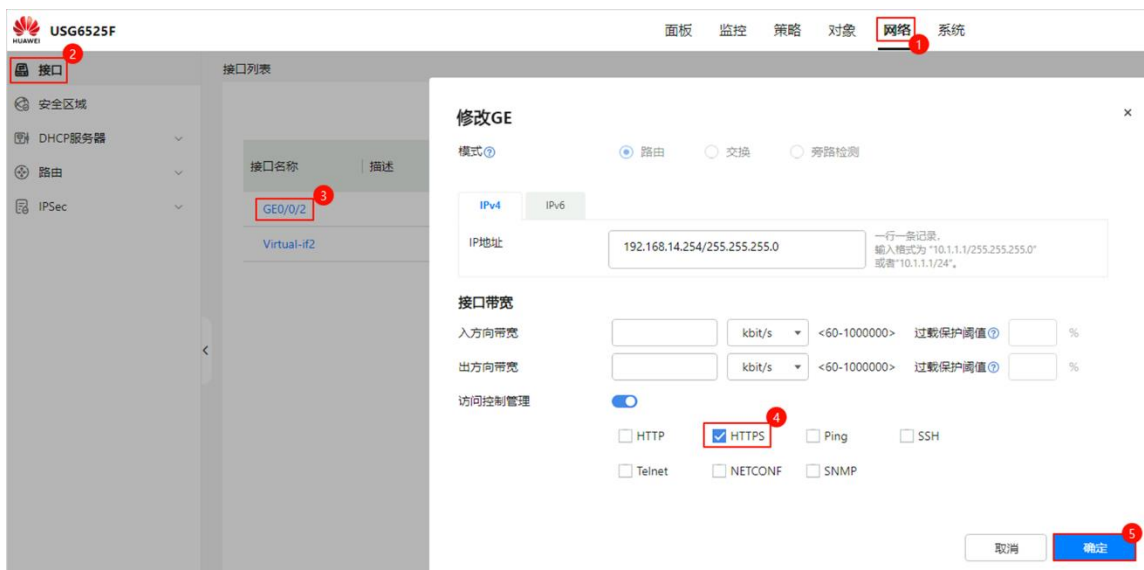


图4-5 配置 G0/0/2 接口管理功能

步骤 2 配置 URPF

本实验针对分支用户区域的业务网段(192.168.14.0/24)进行 URPF 检查,首先需要部署 ACL 筛选目标网段,之后在 Branch-FW 设备接口 GE0/0/2 下开启 URPF 检查,使运维网络的流量通过检查,配置命令如下:

```
[Branch-FW] acl 2000
[Branch-FW-acl4-basic-2000] rule permit source 192.168.14.0 0.0.0.255
[Branch-FW-acl4-basic-2000] quit
[Branch-FW] interface g0/0/2
[Branch-FW-GE0/0/2] ip urpf strict acl 2000
[Branch-FW-GE0/0/2] quit
```

步骤 3 配置协议认证

HQ-FW1 协议认证配置:

```
HRP_M[HQ-FW1] ospf 1
HRP_M[HQ-FW1-ospf-1] area 0
HRP_M[HQ-FW1-ospf-1-area-0.0.0.0] authentication-mode md5 10 cipher Huawei@123
Warning: The algorithm is not safe, and hmac-sha256 is recommended.
HRP_M[HQ-FW1-ospf-1-area-0.0.0.0] quit
HRP_M[HQ-FW1-ospf-1] quit
```

HQ-FW2、DC-FW、AGG-SW1 和 AGG-SW2 设备的协议认证配置同上。

4.3 结果验证

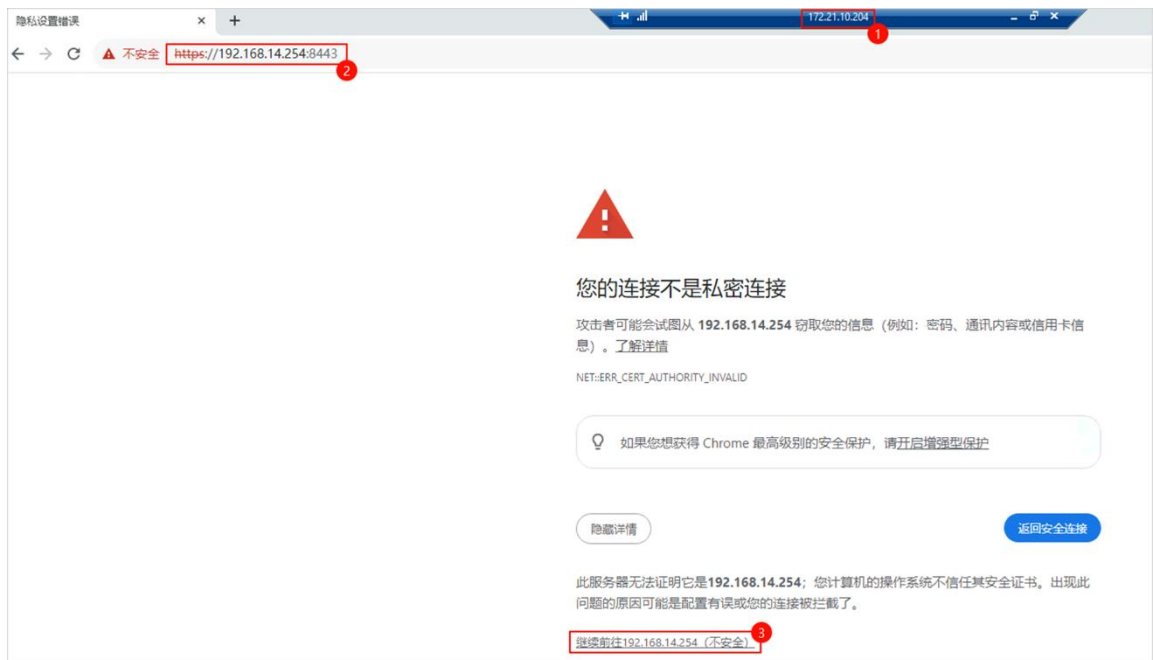
4.3.1 PC4 登录 vFW2

登录 Branch-FW (地址: <https://172.21.10.24:8443/>, 账号: Webuser/Admin@123), 在 “Public” 系统下, 选择 “系统 > 管理员 > 设置”, 进入管理员设置界面, 使能 HTTPS 服务下的 “绑定任意接口” 并点击 “应用”, 确保分支用户区域的安全管理员可通过 G0/0/2 接口登录 vFW2。



图4-6 配置 Branch-FW 设备 HTTPS 服务的绑定接口

使用 RDP 登录 PC4 (地址: 172.21.10.204, 账号: admin/Huawei123!), 模拟企业分支用户区域的安全管理员, 通过 vFW2 虚拟系统新建的管理员登录 vFW2 设备 (地址: https://192.168.14.254:8443, 账号: admin@@vFW2/Huawei@123), 效果如下:



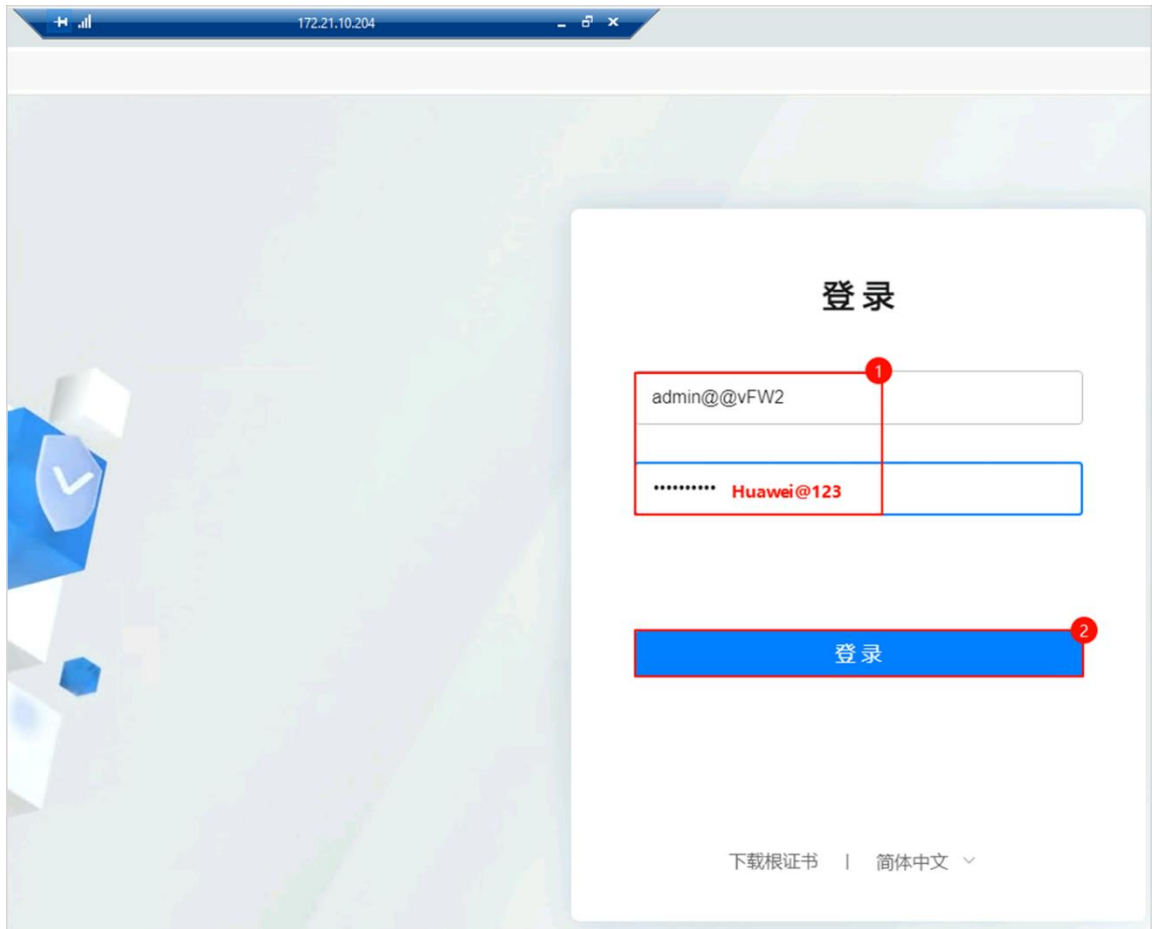


图4-7 PC4 登录 vFW2 设备

首次登录需要修改初始密码，根据设备提示完成账号密码修改后，再次登录，登录成功后选择“系统 > 管理员 > 管理员”进入管理员列表界面，可以看到之前创建的 vFW2 的系统管理员账号有 1 个在线，就是当前正在登录 vFW2 设备的管理员。



图4-8 vFW2 设备管理员信息查看

4.3.2 OSPF 邻居关系查看

HQ-FW1:

```
HRP_M[HQ-FW1]display ospf peer brief
OSPF Process 1 with Router ID 21.21.21.21
Peer Statistic Information
Total number of peer(s): 1
Peer(s) in full state: 1
```

Area Id	Interface	Neighbor id	State
0.0.0.0	GE0/0/4	11.11.11.11	Full

HQ-FW2:

```
HRP_S[HQ-FW2]display ospf peer brief
2024-12-17 17:08:12.647
OSPF Process 1 with Router ID 22.22.22.22
Peer Statistic Information
Total number of peer(s): 1
Peer(s) in full state: 1
```

Area Id	Interface	Neighbor id	State
0.0.0.0	GE0/0/4	12.12.12.12	Full

Core-R1:

```
[Core-R1-ospf-1]display ospf peer brief
```

```
OSPF Process 1 with Router ID 11.11.11.11
Peer Statistic Information
```

Area Id	Interface	Neighbor id	State
0.0.0.0	GE0/0/1	21.21.21.21	Full
0.0.0.0	GE0/0/2	12.12.12.12	Full
0.0.0.0	GE0/0/3	3.3.3.3	Full
0.0.0.0	GE0/0/4	4.4.4.4	Full
0.0.0.0	GE0/0/5	23.23.23.23	Full

```
Total Peer(s): 5
```

Core-R2:

```
[Core-R2]display ospf peer brief
```

```
OSPF Process 1 with Router ID 12.12.12.12
Peer Statistic Information
```

Area Id	Interface	Neighbor id	State
0.0.0.0	GE0/0/1	22.22.22.22	Full
0.0.0.0	GE0/0/2	11.11.11.11	Full
0.0.0.0	GE0/0/3	3.3.3.3	Full
0.0.0.0	GE0/0/4	4.4.4.4	Full
0.0.0.0	GE0/0/5	23.23.23.23	Full

```
Total Peer(s): 5
```

DC-FW:

```
[DC-FW]display ospf peer brief
```



```
OSPF Process 1 with Router ID 23.23.23.23
```

```
Peer Statistic Information
```

```
Total number of peer(s): 2
```

```
Peer(s) in full state: 2
```

Area Id	Interface	Neighbor id	State
0.0.0.0	GE0/0/1	11.11.11.11	Full
0.0.0.0	GE0/0/2	12.12.12.12	Full

```
# AGG-SW1:
```

```
[AGG-SW1]display ospf peer brief
```

```
OSPF Process 1 with Router ID 3.3.3.3
```

```
Peer Statistic Information
```

Area Id	Interface	Neighbor id	State
0.0.0.0	Vlanif58	11.11.11.11	Full
0.0.0.0	Vlanif70	12.12.12.12	Full

```
Total Peer(s): 2
```

```
# AGG-SW2:
```

```
[AGG-SW2]display ospf peer brief
```

```
OSPF Process 1 with Router ID 4.4.4.4
```

```
Peer Statistic Information
```

Area Id	Interface	Neighbor id	State
0.0.0.0	Vlanif62	11.11.11.11	Full
0.0.0.0	Vlanif74	12.12.12.12	Full

```
Total Peer(s): 2
```

4.4 配置参考（仅展示本实验相关配置）

4.4.1 HQ-FW1 的配置

```
#
ospf 1 router-id 21.21.21.21
default-route-advertise
opaque-capability enable
area 0.0.0.0
authentication-mode md5 10 cipher Huawei@123
network 192.168.10.48 0.0.0.3
#
```

4.4.2 HQ-FW2 的配置

```
#
ospf 1 router-id 22.22.22.22
default-route-advertise
opaque-capability enable
area 0.0.0.0
    authentication-mode md5 10 cipher Huawei@123
    network 192.168.10.64 0.0.0.3
#
```

4.4.3 DC-FW 的配置

```
ospf 1 router-id 23.23.23.23
opaque-capability enable
area 0.0.0.0
    authentication-mode md5 10 cipher Huawei@123
    network 192.168.10.40 0.0.0.3
    network 192.168.10.44 0.0.0.3
area 0.0.0.3
    network 192.168.16.0 0.0.0.255
```

4.4.4 Branch-FW 的配置

```
acl number 2000
    rule 5 permit source 192.168.14.0 0.0.0.255
#
interface GE0/0/2
    ip binding vpn-instance vFW2
    ip address 192.168.14.254 255.255.255.0
    service-manage http permit
    service-manage https permit
    service-manage ping permit
    ip urpf strict acl 2000
#
Web-manager server-source all-interface
#
return
#
switch vsys vFW2
#
aaa
    local-user admin@@vFW2 password irreversible-cipher Huawei@123
    local-user admin@@vFW2 service-type http
    local-user admin@@vFW2 user-group manage-ug
#
interface GE0/0/2
    ip binding vpn-instance vFW2
    ip address 192.168.14.254 255.255.255.0
```

```
service-manage http permit
service-manage https permit
```

4.4.5 Core-R1 的配置

```
ospf 1 router-id 11.11.11.11
area 0.0.0.0
 authentication-mode md5 10 cipher Huawei@123
 network 192.168.10.40 0.0.0.3
 network 192.168.10.48 0.0.0.3
 network 192.168.10.52 0.0.0.3
 network 192.168.10.56 0.0.0.3
 network 192.168.10.60 0.0.0.3
```

4.4.6 Core-R2 的配置

```
ospf 1 router-id 12.12.12.12
area 0.0.0.0
 authentication-mode md5 10 cipher Huawei@123
 network 192.168.10.44 0.0.0.3
 network 192.168.10.52 0.0.0.3
 network 192.168.10.64 0.0.0.3
 network 192.168.10.68 0.0.0.3
 network 192.168.10.72 0.0.0.3
```

4.4.7 AGG-SW1 的配置

```
ospf 1 router-id 3.3.3.3
area 0.0.0.0
 authentication-mode md5 10 cipher Huawei@123
 network 192.168.10.56 0.0.0.3
 network 192.168.10.68 0.0.0.3
area 0.0.0.1
 network 192.168.11.0 0.0.0.255
```

4.4.8 AGG-SW2 的配置

```
ospf 1 router-id 4.4.4.4
area 0.0.0.0
 authentication-mode md5 10 cipher Huawei@123
 network 192.168.10.60 0.0.0.3
 network 192.168.10.72 0.0.0.3
area 0.0.0.2
 network 192.168.12.0 0.0.0.255
 network 192.168.51.0 0.0.0.255
```

4.5 思考题

实验中配置的 URPF 模式是严格模式，在哪种情况下需要使用松散模式？

答案：松散模式下，设备仅要求 FIB 表中存在去往报文源 IP 地址的路由，不要求报文入接口与路由出接口一致。建议在不能保证对端与本端记录的路由路径一致的环境下使用松散模式。例如两个网络边界设备之间有多条路径，此时松散模式既可以有效地阻止网络攻击，又可以避免合法报文被错误丢弃。

5 终端接入安全综合实验

5.1 实验介绍

5.1.1 关于本实验

公司总部办公区用户分为有线接入用户和无线接入用户，因终端接入安全防护需要，现规划总部办公区内有线用户（PC2 模拟）接入网络时需进行 802.1X 认证，无线用户（PC3 模拟）接入网络时需进行 Portal 认证。部署在运维中心的 iMaster NCE-Campus 作为接入认证服务器。

5.1.2 实验组网介绍

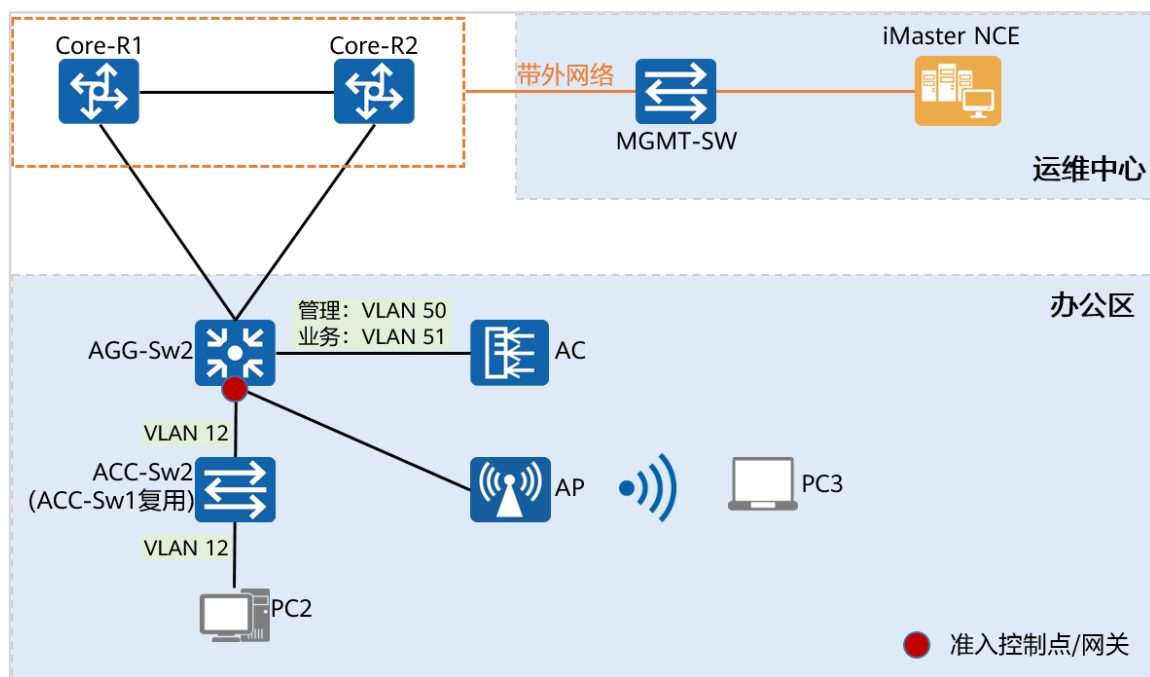


图5-1 实验拓扑图

5.1.3 实验规划

1. 总部运维管理区部署 NCE-Campus 作为认证服务器，有线办公区内 PC2 通过接入交换机 ACC-SW2 与汇聚交换机 AGG-SW2 互联；无线办公区内 AP 与同区域内 AC 控制器通过 AGG-SW2 互联。为确保总部人员访问网络资源的行为受控，需要分别为有线/无线办公区部署 802.1X 以及 Portal 认证，实现终端接入安全。

2. 有线接入用户 PC2 访问网络资源时触发 802.1X 认证，需要在操作系统内输入用户名密码上送到 AGG-SW2 以及 NCE-Campus 完成认证。
3. 无线接入用户 PC3 通过连接 AP 释放的 SSID，访问任意 URL 触发 Portal 认证，在 Web 重定向页面中完成认证后可访问 Internet。

5.2 实验配置任务

5.2.1 配置思路

802.1X 认证配置思路：

1. 在认证接入设备上配置 RADIUS 模板。
2. 在认证接入设备上配置认证和计费方案。
3. 在认证接入设备上创建 802.1X 接入模板和认证模板。
4. 在认证接入设备业务接口下启用 802.1X 认证。
5. 在认证接入设备下游二层接入设备上开启 802.1X 认证报文透传。
6. 在 NCE-Campus 上创建业务站点、准入设备、准入用户、认证规则和授权规则。

Portal 认证配置思路：

1. 在认证接入设备上配置 RADIUS 模板。
2. 在认证接入设备上配置认证和计费方案。
3. 在认证接入设备上配置 URL 认证参数。
4. 在认证接入设备上创建 Portal 服务器模板。
5. 在认证接入设备上创建认证前域资源。
6. 在认证接入设备上创建 Portal 认证模板。
7. 在认证接入设备上创建业务地址池，并配置无线业务。
8. 在 NCE-Campus 上创建准入设备、准入用户、认证规则、授权规则和 Portal 页面推送规则。

5.2.2 配置步骤（802.1X 认证）

步骤 1 配置 RADIUS 模板

在 AGG-SW2 设备上配置 RADIUS 模板与免认证规则。

```
[AGG-SW2]radius-server template Campus
[AGG-SW2-radius-Campus] radius-server shared-key cipher Huawei@123
[AGG-SW2-radius-Campus] radius-server authentication 172.21.10.78 1812 source ip-address
172.21.10.4 weight 80
Info: This operation may take a few minutes, please wait...
[AGG-SW2-radius-Campus] radius-server accounting 172.21.10.78 1813 source ip-address 172.21.10.4
weight 80
Info: This operation may take a few minutes, please wait...
```

```
[AGG-SW2-radius-Campus] radius-attribute nas-ip 172.21.10.4
[AGG-SW2-radius-Campus]radius-server authorization 172.21.10.78 shared-key cipher Huawei@123
Warning: The service listening command is not configured. Configure the radius-server authorization
server-source ip-address or radius-server authorization server-source all-interface command first.
[AGG-SW2]radius-server authorization server-source all-interface
Warning: All interface listening has security risks.
If configured, the configuration of the specified listening IP address will be removed. Continue?[Y/N]y
Info: This operation may take some time, please wait for a moment .....
[AGG-SW2]free-rule-template name default_free_rule
[AGG-SW2-free-rule-default_free_rule] free-rule 1 destination ip 172.21.10.78 mask 255.255.255.255
[AGG-SW2-free-rule-default_free_rule]quit
```

步骤 2 配置认证和计费方案

在 AGG-SW2 设备上配置认证方案和计费方案，全局 default 域内引用前文配置的 RADIUS 服务器模板和认证计费方案，并指定全局默认域为 default。

```
[AGG-SW2]aaa
[AGG-SW2-aaa] authentication-scheme radius
[AGG-SW2-aaa-authen-radius] authentication-mode radius
[AGG-SW2-aaa-authen-radius] accounting-scheme radius
[AGG-SW2-aaa-accounting-radius] accounting-mode radius
[AGG-SW2-aaa-accounting-radius] accounting realtime 15
[AGG-SW2-aaa-accounting-radius] domain default
Info: The domain default is for common users. To modify the parameters of common users domain,
perform operations in the domain default.
[AGG-SW2-aaa-domain-default] authentication-scheme radius
[AGG-SW2-aaa-domain-default] accounting-scheme radius
[AGG-SW2-aaa-domain-default] radius-server Campus
[AGG-SW2-aaa-domain-default]quit
[AGG-SW2-aaa]quit
[AGG-SW2]domain default
Info: Set the default domain success.
```

步骤 3 创建 802.1X 接入模板和认证模板

在 AGG-SW2 设备上创建 802.1X 接入模板和认证模板，并将前者调用至后者中。

```
[AGG-SW2]dot1x-access-profile name dot1x
[AGG-SW2-dot1x-access-profile-dot1x]quit
[AGG-SW2]authentication-profile name dot1x
[AGG-SW2-authen-profile-dot1x]dot1x-access-profile dot1x
[AGG-SW2-authen-profile-dot1x]quit
```

步骤 4 启用 802.1X 认证

在 AGG-SW2 设备下游业务接口下启用 802.1X 认证。

```
[AGG-SW2]interface GE0/0/3
[AGG-SW2-GE0/0/3]authentication-profile dot1x
Warning: NAC authentication cannot be enabled both on a Layer 2 Ethernet interface and the VLANIF
interface mapping the VLAN of the Ethernet interface. Otherwise, service may be interrupted.
```

```
Info: To authorize VLANs for users, ensure that the interface type is hybrid.
[AGG-SW2-GE0/0/3]quit
```

步骤 5 透传认证报文

因 802.1X 认证报文需要经过下游接入交换机，为保障认证报文的成功交互，需要在下游接入交换机 ACC-SW1 上执行如下配置，透传 802.1X 认证报文。

```
[ACC-Sw1] l2protocol-tunnel user-defined-protocol dot1x protocol-mac 0180-c200-0003 group-mac 0100-0000-0002
[ACC-Sw1-GE0/0/23] interface GE0/0/2
[ACC-Sw1-GE0/0/2] l2protocol-tunnel user-defined-protocol dot1x enable
[ACC-Sw1-GE0/0/2] interface GE0/0/23
[ACC-Sw1-GE0/0/23] l2protocol-tunnel user-defined-protocol dot1x enable
[ACC-Sw1-GE0/0/23] quit
[ACC-Sw1]undo dhcp snooping enable //为保证 802.1X 报文成功交互，可关闭前文配置的 DHCP Snooping
Warning: DHCP snooping will be disabled on the device. Continue? [Y/N]y
Info: The operation may take a few seconds. Please wait for a moment. .done.
```

步骤 6 创建站点

登录 NCE-Campus 运维界面（地址：https://172.21.10.78:18008，账号：security01/Security@123），在租户工作台首页，点击“站点”，之后点击右侧“创建”按钮，执行以下操作：



图5-2 进入站点创建界面

创建站点

×

基本信息

* 站点名称

HQ-Office

* 南向IP服务名称 ②

Public Default South Access

* 设备类型

☐ AP
☒ AR
☒ FW
☒ LSW
☒ NE
☒ WAC

站点若需要纳管Fit AP设备，请勾选WAC。站点包含WAC类型时，可以纳管WAC和Fit AP设备。

站点位置

39.904053,116.40412

配置信息

* 配置模式 ②

默认

配置文件

* 配置文件 ②

默认配置

从已有的站点克隆

更多 ∨

取消

确定

图5-3 创建站点

步骤 7 创建准入设备

登录 NCE-Campus 运维界面（地址：<https://172.21.10.78:18008>，账号：security01/Security@123）选择“准入管理 > 准入设备”，执行以下操作，创建准入设备：

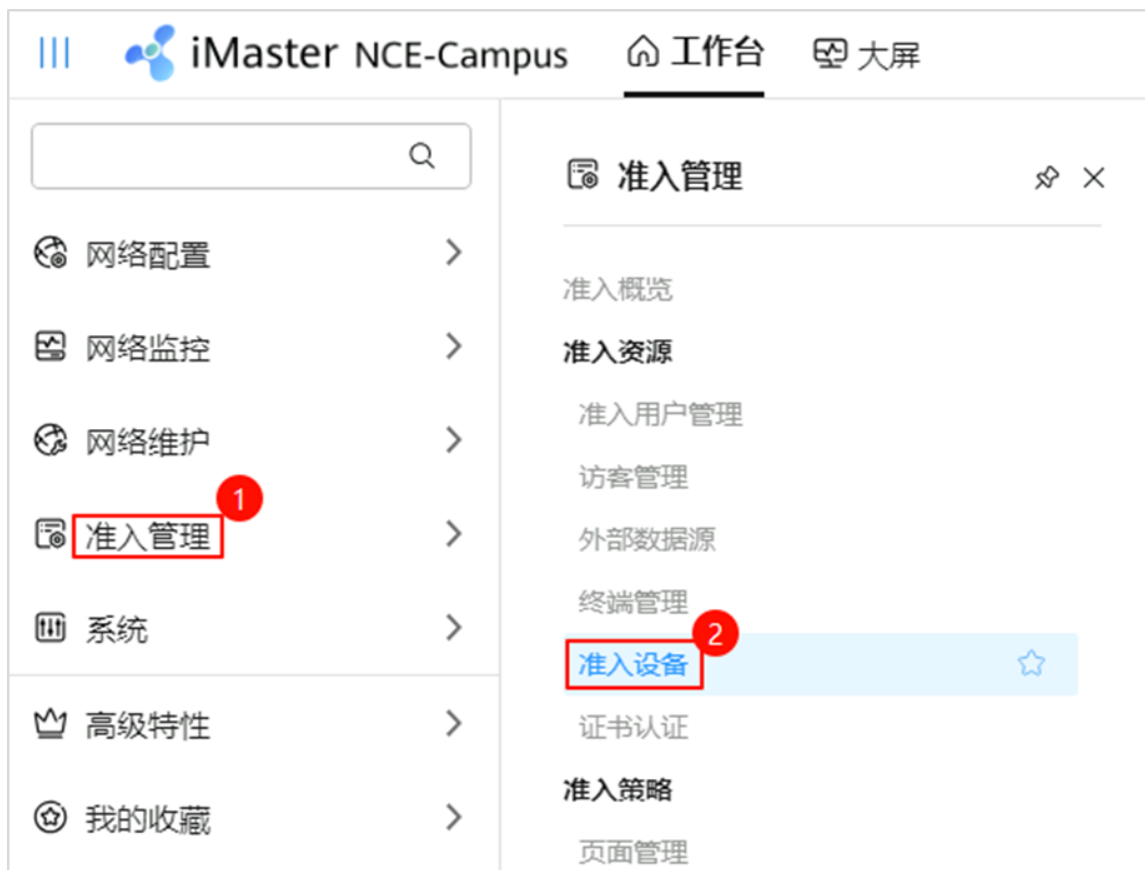


图5-4 进入准入设备创建界面

准入管理 / 准入资源 / 准入设备

准入设备管理 | 准入区域 | 准入设备模板

非云管准入设备 | 云管准入设备

创建非云管准入设备

*设备名称: AGG-SW2

描述:

*IP地址: 172.21.10.4

*准入设备组: 准入设备组

备份IP:

设备系列: Aruba OS

RADIUS认证参数:

CoA类型: 默认CoA | No CoA | Port Bounce | Reauth

CoA端口:

准入设备模板:

*认证计费密码: Huawei@123

*确认认证计费密码: Huawei@123

*授权密码: Huawei@123

*确认授权密码: Huawei@123

*计费周期(分钟): 15

图5-5 创建 802.1X 准入设备

准入设备创建完成后效果如下:

准入管理 / 准入资源 / 准入设备

准入设备管理 | 准入区域 | 准入设备模板

请输入设备名称

非云管准入设备 | 云管准入设备

请输入设备名称

高级搜索

删除 | 导出 | 导入 | 删除 | 创建

设备名称	描述	IP地址	准入设备组	备份IP	设备系列	RADIUS认证参数	Portal认证参数
AGG-SW2		172.21.10.4	准入设备组	--	Aruba OS	已配置	未配置

共1条

20 | 1 | >

图5-6 准入设备查看

步骤 8 创建准入用户

登录 NCE-Campus 运维界面（地址：https://172.21.10.78:18008，账号：security01/Security@123）选择“准入资源 > 准入用户管理”，执行以下操作：



图5-7 进入准入用户创建界面

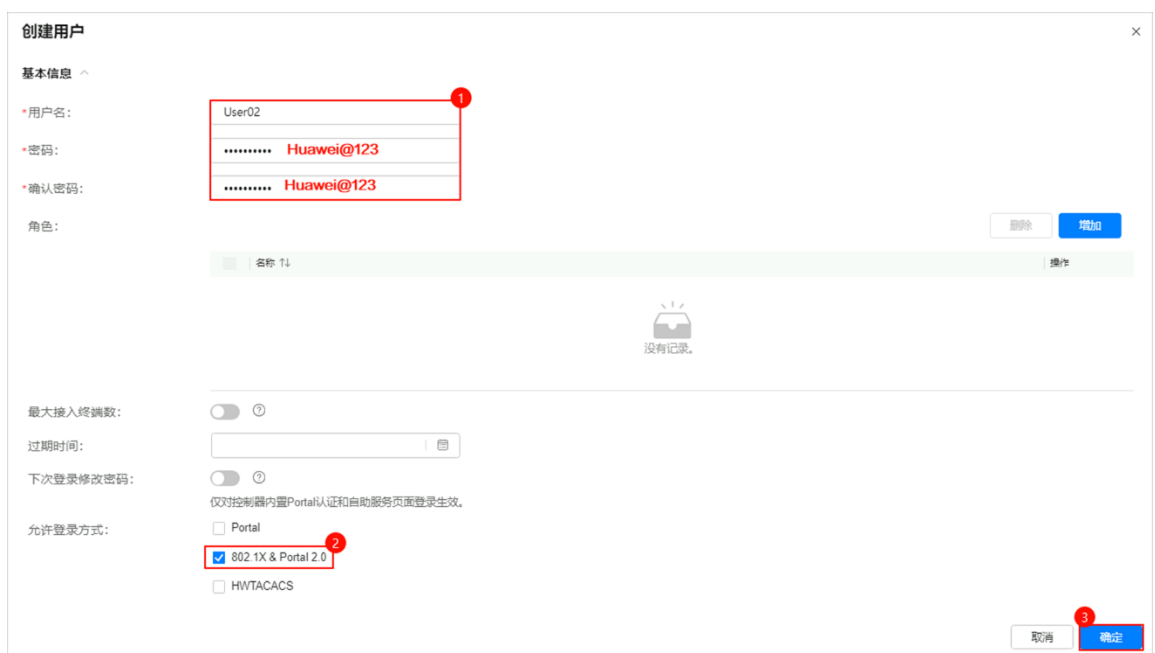


图5-8 创建 802.1X 认证用户

准入用户创建完成后效果如下：

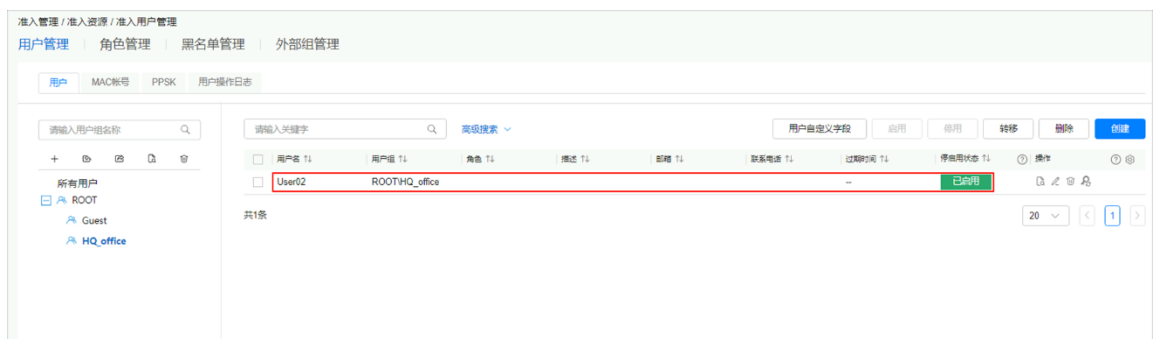


图5-9 查看 802.1X 准入认证用户

步骤 9 创建认证与授权规则

登录 NCE-Campus 运维界面（地址：https://172.21.10.78:18008，账号：security01/Security@123）选择“准入策略 > 认证授权”，执行以下操作：

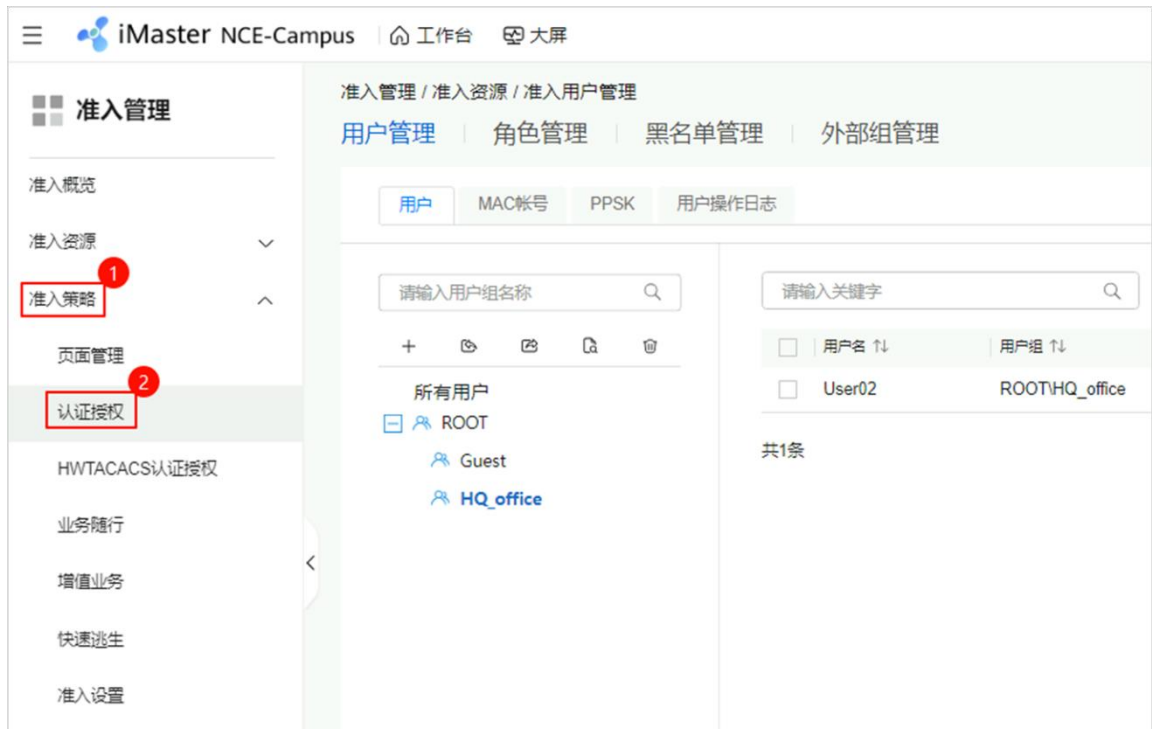


图5-10 进入认证授权规则管理界面



图5-11 创建 802.1X 认证规则（1）



图5-12 创建 802.1X 认证规则（2）

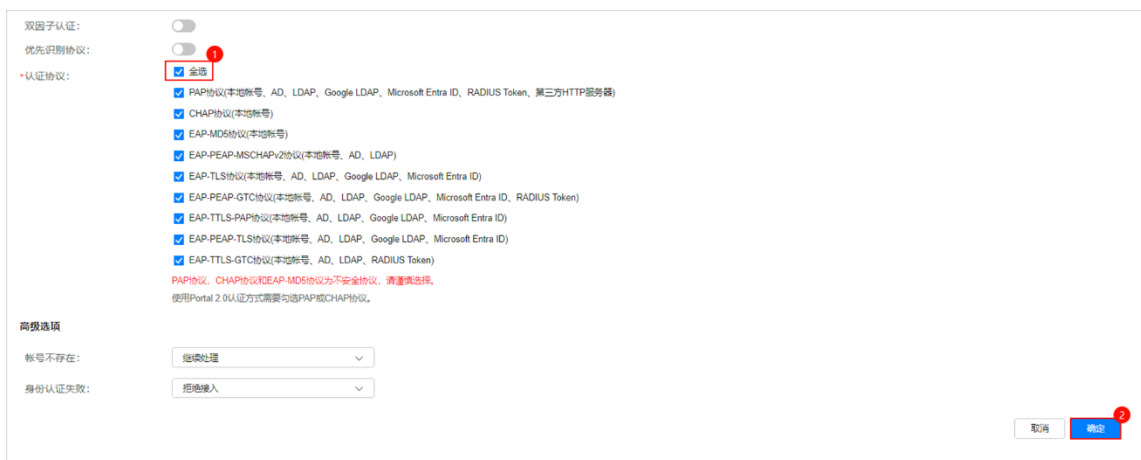


图5-13 创建 802.1X 认证规则（3）

802.1X 认证规则创建完成后效果如下：



图5-14 查看 802.1X 认证规则

在 NCE-Campus 运维界面（地址：<https://172.21.10.78:18008>，账号：security01/Security@123）选择“准入管理 > 准入策略 > 认证授权 > 授权规则”，执行以下操作，创建 802.1X 授权规则。



图5-15 进入授权规则创建界面



图5-16 创建 802.1X 授权规则（1）



图5-17 创建 802.1X 授权规则（2）

802.1X 授权规则创建完成后效果如下：



图5-18 查看 802.1X 授权规则

5.2.3 配置步骤（Portal 认证）

步骤 1 创建 RADIUS 模板

在 AC 设备上配置 RADIUS 模板，便于上送认证报文至 NCE-Campus 认证服务器。

```
[AC6508]radius-server template radius
[AC6508-radius-radius] radius-server shared-key cipher Huawei@123
[AC6508-radius-radius] radius-server authentication 172.21.10.78 1812 source ip-address 172.21.10.61
weight 80
[AC6508-radius-radius] radius-server accounting 172.21.10.78 1813 source ip-address 172.21.10.61
weight 80
[AC6508-radius-radius]quit
[AC6508]radius-server authorization 172.21.10.78 shared-key cipher Huawei@123
Warning: The service listening command is not configured. Configure the radius-server authorization
server-source ip-address or radius-server authorization server-source all-interface command first.
[AC6508]radius-server source ip-address 172.21.10.61
[AC6508]radius-server authorization server-source all-interface
Warning: All interface listening has security risks.
If configured, the configuration of the specified listening IP address will be removed. Continue?[Y/N]y
Info: This operation may take some time, please wait for a moment .....
```

步骤 2 配置认证和授权模板

在 AC 设备上配置认证方案和计费方案，全局 default 域内引用前文配置的 RADIUS 服务器模板，并指定全局默认域为 default。

```
[AC6508]aaa
[AC6508-aaa]authentication-scheme radius
[AC6508-aaa-authen-radius]authentication-mode radius
[AC6508-aaa-authen-radius]quit
[AC6508-aaa]accounting-scheme radius
[AC6508-aaa-accounting-radius]accounting-mode radius
[AC6508-aaa-accounting-radius]accounting realtime 15
[AC6508-aaa-accounting-radius]quit
[AC6508-aaa]domain default
Info: The domain default is for common users. To modify the parameters of common users domain,
perform operations in the domain default.
[AC6508-aaa-domain-default] authentication-scheme radius
[AC6508-aaa-domain-default] accounting-scheme radius
[AC6508-aaa-domain-default] radius-server radius
[AC6508-aaa-domain-default]quit
[AC6508-aaa]quit
[AC6508]domain default
Info: Set the default domain success.
```

步骤 3 配置 URL 认证参数

在 AC 设备上配置 Portal 认证 URL 地址和上报的认证参数：

```
[AC6508] url-template name nce
[AC6508-url-template-nce] url https://172.21.10.78:19008/portal
Info: Ensure that the DNS and Portal server addresses are reachable.
[AC6508-url-template-nce] url-parameter device-ip ac-ip redirect-url redirect-url ssid ssid user-ipaddress
uaddress user-mac umac
[AC6508-url-template-nce] url-parameter set device-ip 172.21.10.61
[AC6508-url-template-nce] quit
[AC6508] web-auth-server server-source all-interface
[AC6508]
```

步骤 4 配置 Portal 服务器模板

在 AC 设备上配置 Portal 服务器模板。

```
[AC6508] web-auth-server portal
[AC6508-web-auth-server-portal] server-ip 172.21.10.78
[AC6508-web-auth-server-portal] port 50100
[AC6508-web-auth-server-portal] shared-key cipher Huawei@123
Info: The shared-key configured on the device must be the same as the one configured on the portal
server. And it is strongly recommended that the shared-key be at least 16 octets to ensure a sufficiently
large range for the secret to provide protection against exhaustive search attacks.
[AC6508-web-auth-server-portal] url-template nce
[AC6508-web-auth-server-portal] source-ip 172.21.10.61
[AC6508-web-auth-server-portal] portal-access-profile name portal
[AC6508-portal-access-profile-portal] web-auth-server portal direct
Authentication profile auth_portal : done.
[AC6508-portal-access-profile-portal] quit
[AC6508]
```

步骤 5 配置认证前域资源

在 AC 设备上配置用户认证前可以访问的资源，此处必须放行 NCE-Campus 业务地址，否则用户无法访问 Portal 页面。

```
[AC6508] free-rule-template name free_rule
[AC6508-free-rule-free_rule] free-rule 1 destination ip 172.21.10.78 mask 255.255.255.255
[AC6508-free-rule-free_rule] quit
[AC6508]
```

步骤 6 配置 Portal 认证模板

在 AC 设备上配置 portal 用户认证模板，调用前文中配置的各个模板参数。

```
[AC6508] authentication-profile name auth_portal
[AC6508-authentication-profile-auth_portal] portal-access-profile portal
[AC6508-authentication-profile-auth_portal] free-rule-template free_rule
[AC-authentication-profile-auth_portal] access-domain default
[AC6508-authentication-profile-auth_portal] quit
```

步骤 7 创建业务地址池

在 AC 设备上创建 WLAN 业务地址池并调用，为无线接入终端分配业务 IP。

```
[AC6508]ip pool wlan
Info: The parameter is case insensitive. All uppercase letters in the string will be converted to lowercase letters.
[AC6508-ip-pool-wlan] gateway-list 192.168.51.254
[AC6508-ip-pool-wlan] network 192.168.51.0 mask 255.255.255.0
[AC6508-ip-pool-wlan] excluded-ip-address 192.168.51.252
[AC6508-ip-pool-wlan]interface Vlanif51
[AC6508-Vlanif51] ip address 192.168.51.254 255.255.255.0
[AC6508-Vlanif51] dhcp select global
[AC6508-Vlanif51]quit
[AC6508]
```

步骤 8 配置无线业务

在 AC 设备上按需配置无线业务，在配置无线业务前需确保 AP 已正常上线（已预配）。

```
[AC6508]wlan
[AC6508-wlan-view]security-profile name security_portal
[AC-wlan-sec-prof-security_portal]security open
Warning: This action may cause service interruption. Continue?[Y/N]:y
Info: This operation may take a few seconds, please wait.
Warning: The Open encryption algorithm is insecure. For security-sensitive scenarios, WPA2 or WPA3 is recommended.done.
[AC6508-wlan-sec-prof-security_portal]quit
[AC6508-wlan-view]ssid-profile name hq_user
[AC6508-wlan-ssid-prof-hq_user]ssid hq_user
[AC6508-wlan-ssid-prof-hq_user]quit
[AC6508-wlan-view]
[AC6508-wlan-view]vap-profile name hq_user
[AC6508-wlan-vap-prof-hq_user]forward-mode tunnel
[AC6508-wlan-vap-prof-hq_user]service-vlan vlan-id 51
[AC6508-wlan-vap-prof-hq_user]ssid-profile hq_user
[AC6508-wlan-vap-prof-hq_user]security-profile security_portal
[AC6508-wlan-vap-prof-hq_user]authentication-profile auth_portal
[AC6508-wlan-vap-prof-hq_user]quit
[AC6508-wlan-view]regulatory-domain-profile name domain1
[AC6508-wlan-regulate-domain-domain1] dca-channel 5g bandwidth 20mhz
Info: Manually trigger radio calibration, or wait for the scheduled or automatic radio calibration, to make the bandwidth configuration take effect.
Info: In 20MHz bandwidth mode, available calibration channels include channels 36,40,44,48,52,56,60,64,149,153,157,161 and 165.
[AC6508-wlan-regulate-domain-domain1] dca-channel 6g bandwidth 20mhz
Info: Manually trigger radio calibration, or wait for the scheduled or automatic radio calibration, to make the bandwidth configuration take effect.
Warning: In 20MHz bandwidth mode, no channel group is available for use. However, at least three channel groups are required. For better channel assignment, reduce the calibration bandwidth or increase the number of calibration channels.
[AC6508-wlan-regulate-domain-domain1]quit
[AC6508-wlan-view]ap-group name group1
```

```
[AC6508-wlan-ap-group-group1]radio 0
[AC6508-wlan-group-radio-group1/0] vap-profile hq_user wlan 1
[AC6508-wlan-group-radio-group1/0]radio 1
[AC6508-wlan-group-radio-group1/1]vap-profile hq_user wlan 1
[AC6508-wlan-group-radio-group1/1]quit
[AC6508-wlan-ap-group-group1]qu
[AC6508-wlan-ap-group-group1]quit
[AC6508-wlan-view]
```

步骤 9 添加 Portal 认证准入设备

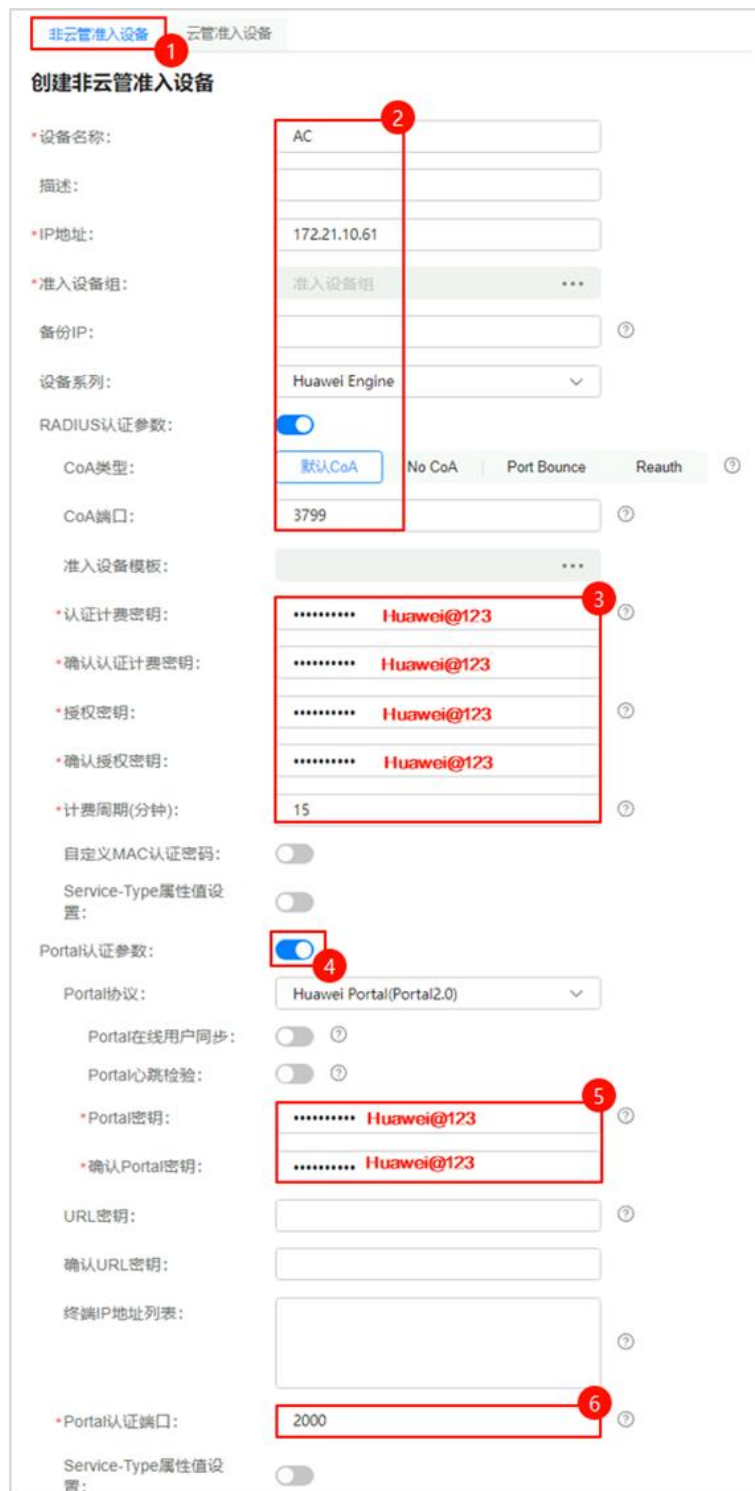
登录 NCE-Campus 运维界面（地址：https://172.21.10.78:18008，账号：security01/Security@123）选择“准入管理 > 准入设备”，执行以下操作：



图5-19 进入准入设备管理界面



图5-20 进入准入设备创建界面



创建非云管准入设备

*设备名称: AC

描述:

*IP地址: 172.21.10.61

*准入设备组: 准入设备组

备份IP:

设备系列: Huawei Engine

RADIUS认证参数:

CoA类型: 默认CoA

CoA端口: 3799

准入设备模板:

*认证计费密码: Huawei@123

*确认认证计费密码: Huawei@123

*授权密码: Huawei@123

*确认授权密码: Huawei@123

*计费周期(分钟): 15

自定义MAC认证密码:

Service-Type属性值设置:

Portal认证参数:

Portal协议: Huawei Portal(Portal2.0)

Portal在线用户同步:

Portal心跳检验:

*Portal密码: Huawei@123

*确认Portal密码: Huawei@123

URL密码:

确认URL密码:

终端IP地址列表:

*Portal认证端口: 2000

Service-Type属性值设置:

图5-21 创建 Portal 认证准入设备

Portal 认证准入设备创建完成后效果如下:

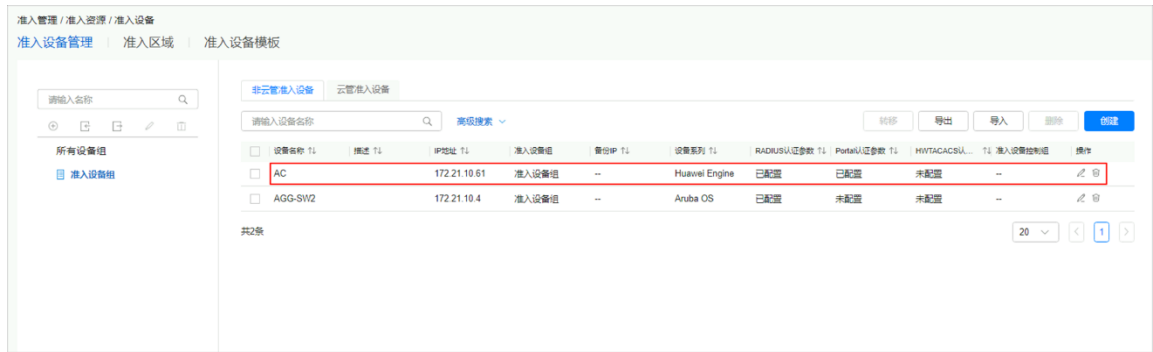


图5-22 查看 Portal 认证准入设备

步骤 10 创建 Portal 认证准入用户

登录 NCE-Campus 运维界面（地址：https://172.21.10.78:18008，账号：security01/Security@123）选择“准入管理 > 准入资源 > 准入用户管理”执行以下操作创建 Portal 认证准入用户。

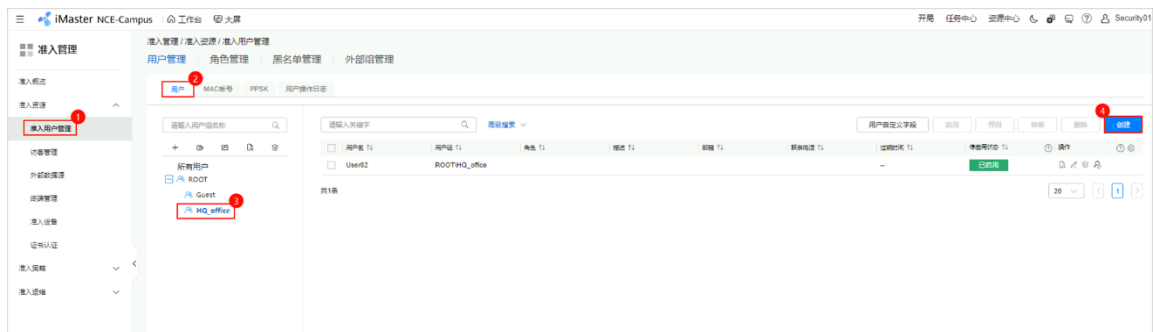


图5-23 进入准入用户创建页面

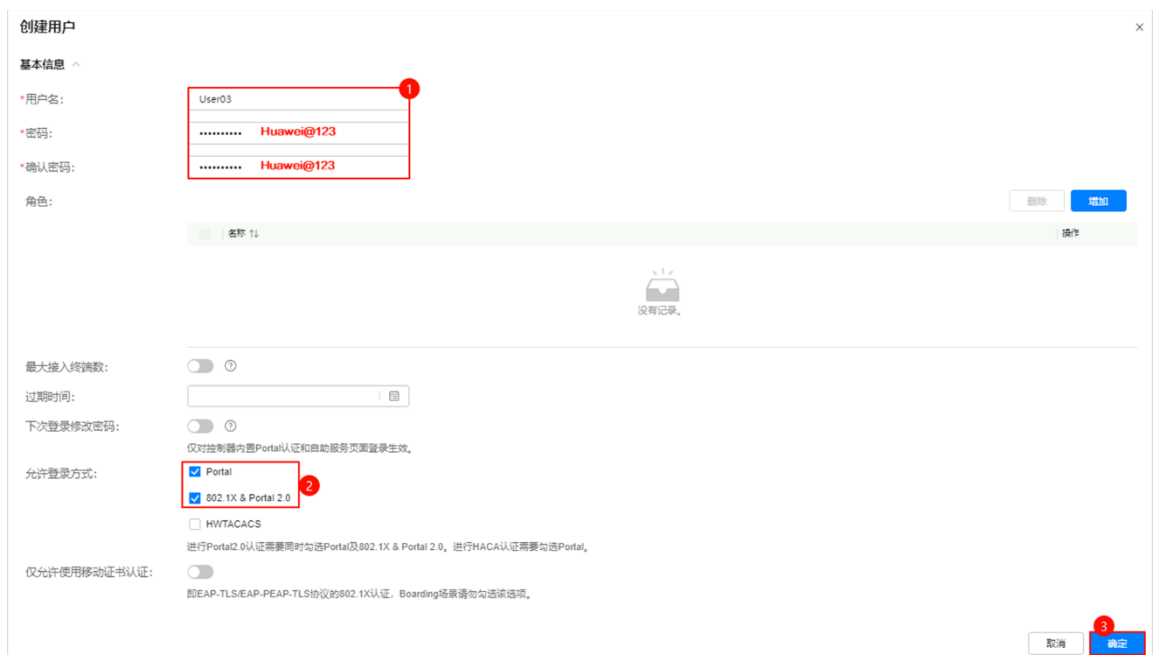


图5-24 创建 Portal 认证准入用户

Portal 认证准入用户创建完成后，效果如下：

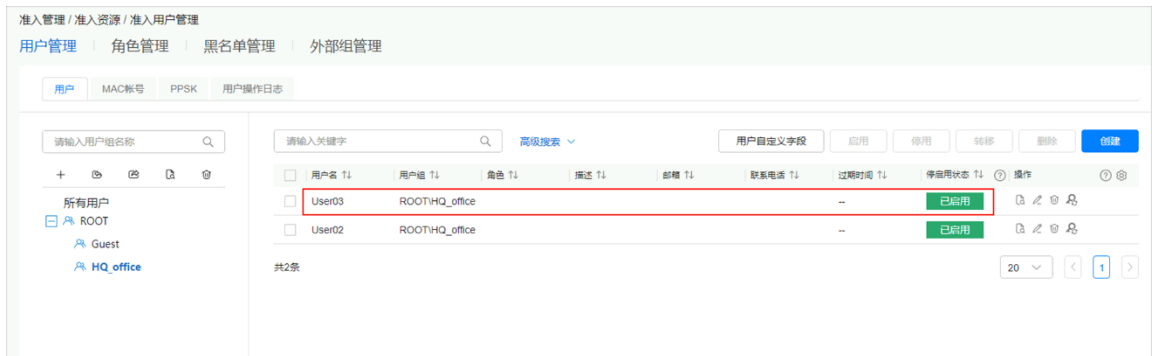


图5-25 查看 Portal 认证准入用户

步骤 11 创建认证与授权规则

登录 NCE-Campus 运维界面（地址：<https://172.21.10.78:18008>，账号：[security01/Security@123](#)）选择“准入管理 > 准入策略 > 认证授权”，执行以下操作，创建用于 Portal 认证的认证规则和授权规则。



图5-26 进入认证规则创建界面



图5-27 创建 Portal 认证规则（1）



图5-28 创建 Portal 认证规则（2）



图5-29 创建 Portal 认证规则（3）

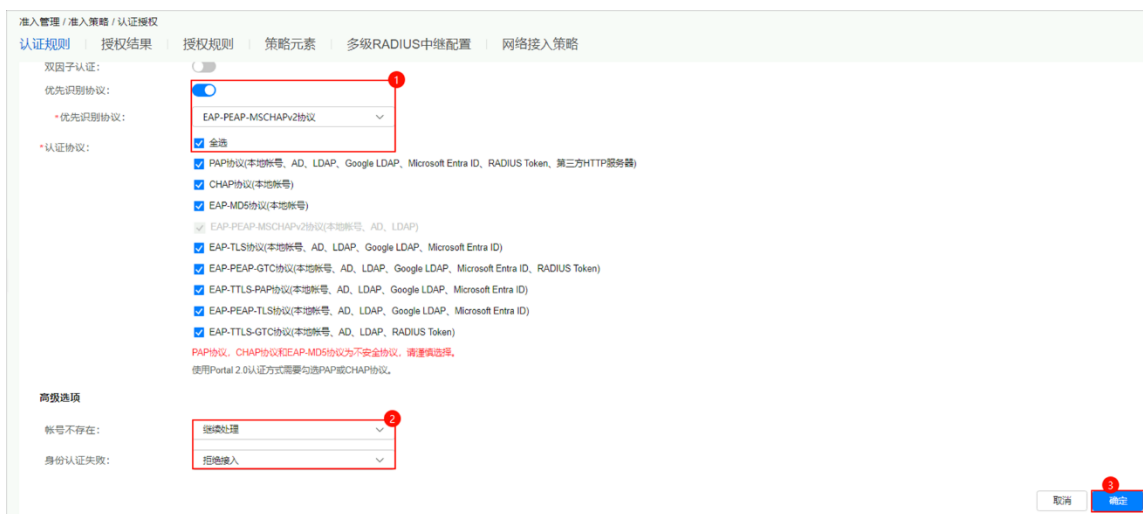


图5-30 创建 Portal 认证规则（4）

Portal 认证规则创建完成后，效果如下：



图5-31 查看 Portal 认证规则

继续在 NCE-Campus 认证授权规则创建界面选择“授权规则”，并点击右侧“创建”按钮，执行以下操作，创建 Portal 授权规则。



图5-32 进入 Portal 授权规则创建界面



图5-33 创建 Portal 授权规则（1）

图5-34 创建 Portal 授权规则（2）

图5-35 创建 Portal 授权规则（3）

Portal 授权规则创建完成后，效果如下：

优先级	名称	认证方式	接入方式	匹配条件	授权结果	描述	命中次数	由策略状态	操作
1	HQ_Office	用户接入认证	有线	账号: User02	允许接入		1	应用	编辑 删除 重置
2	HQ_WLAN	用户接入认证	WIFI	账号: User03 SSID: hq_user	允许接入		0	应用	编辑 删除 重置
N	Default	HACA Portal...	有线WIFI...		拒绝接入		0	应用	编辑 删除 重置

图5-36 查看 Portal 授权规则

步骤 12 配置 Portal 页面推送规则

登录 NCE-Campus 运维界面（地址：<https://172.21.10.78:18008>，账号：security01/Security@123）选择“准入管理 > 准入策略 > 页面管理”，执行以下操作，配置 Portal 页面推送规则。



图5-37 进入 Portal 页面推送规则管理界面



图5-38 修改 Portal 页面推送规则

5.3 结果验证

5.3.1 802.1X 认证

使用 RDP 登录 PC2 (地址: 172.21.10.202, 账号: admin/Huawei123!), 打开控制面板, 选择“网络和 Internet > 网络连接”, 进入终端设备网卡管理界面, 执行以下操作。

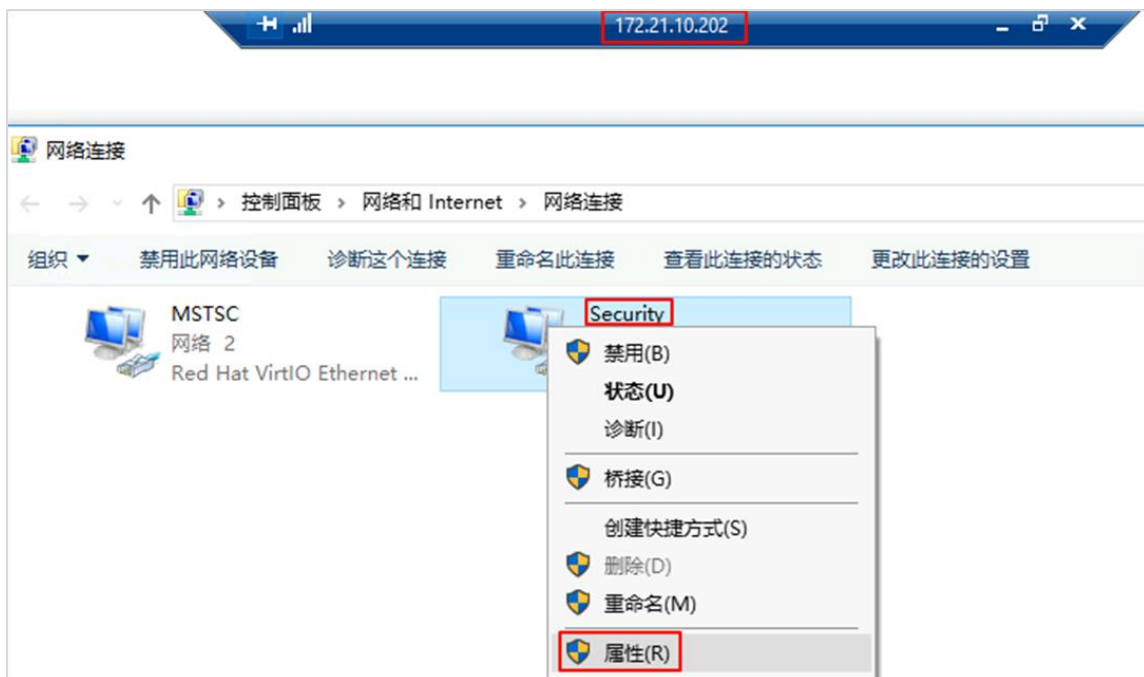


图5-39 进入 PC2 业务网卡属性界面

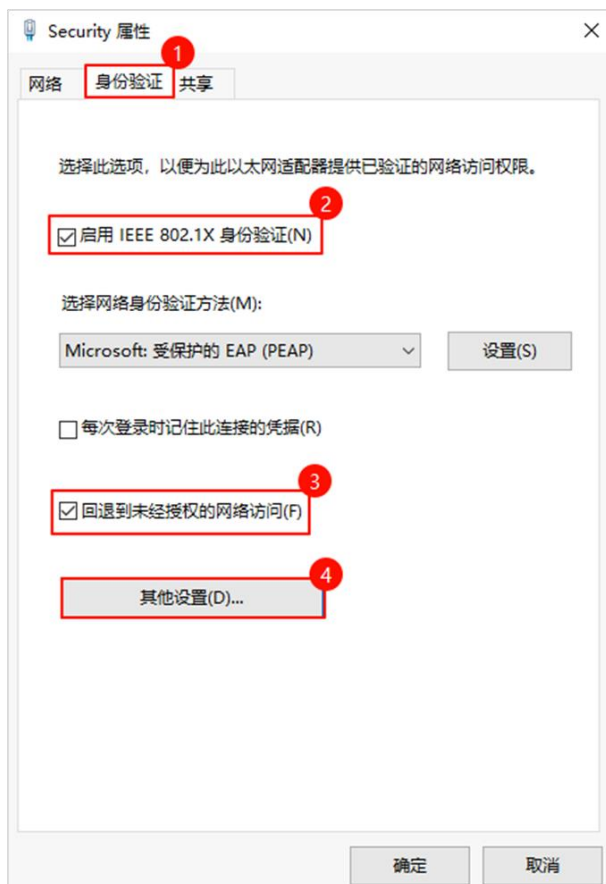


图5-40 设置网卡认证功能



图5-41 编辑网卡认证参数 (1)

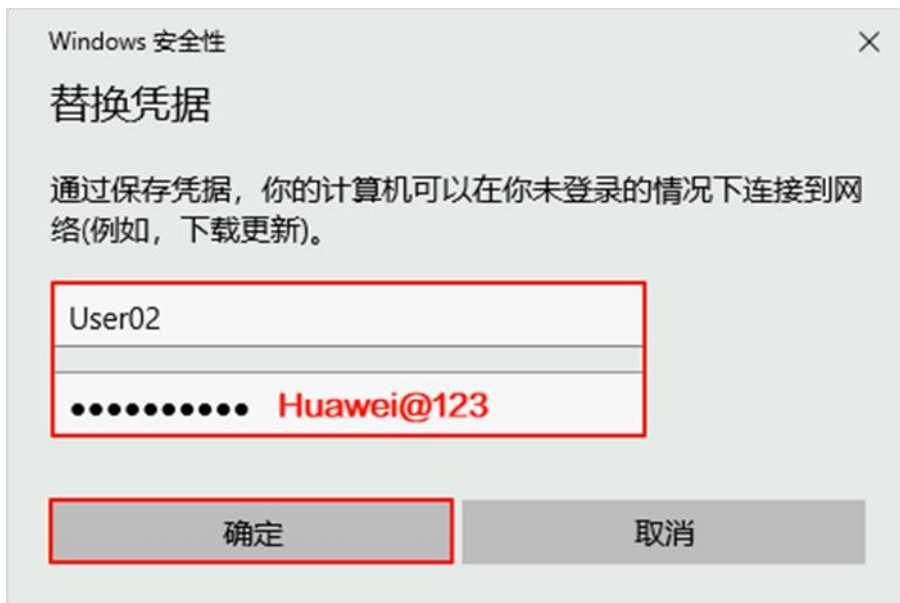


图5-42 编辑网卡认证参数（2）

完成上述操作并逐步点击“确认”后,回到终端设备网卡管理界面,双击业务网卡“Security”,可以看到以下效果,表明 PC2 设备在尝试进行 802.1X 认证。



图5-43 PC2 开始 802.1X 认证

稍等片刻后,可以发现 PC2 设备的业务网卡的“媒体状态”已切换为“已启用”,表明 802.1X 接入认证成功。



图5-44 PC2 设备 802.1X 认证成功

登录 NCE-Campus 运维界面（地址：<https://172.21.10.78:18008>，账号：security01/Security@123）选择“准入管理 > 准入概览”，进入准入管理运维主页，执行以下操作：

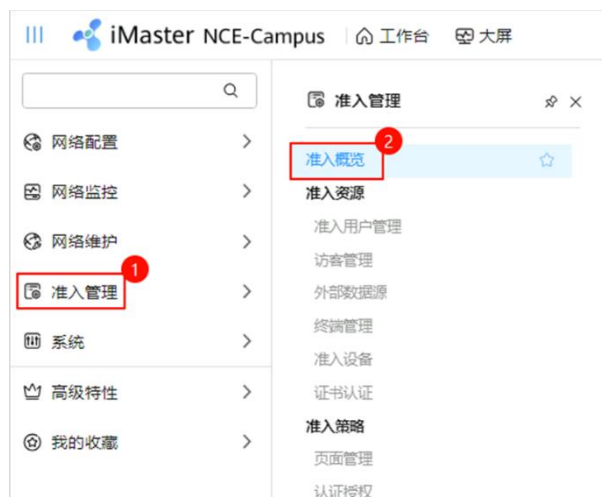


图5-45 进入转入运维管理主页

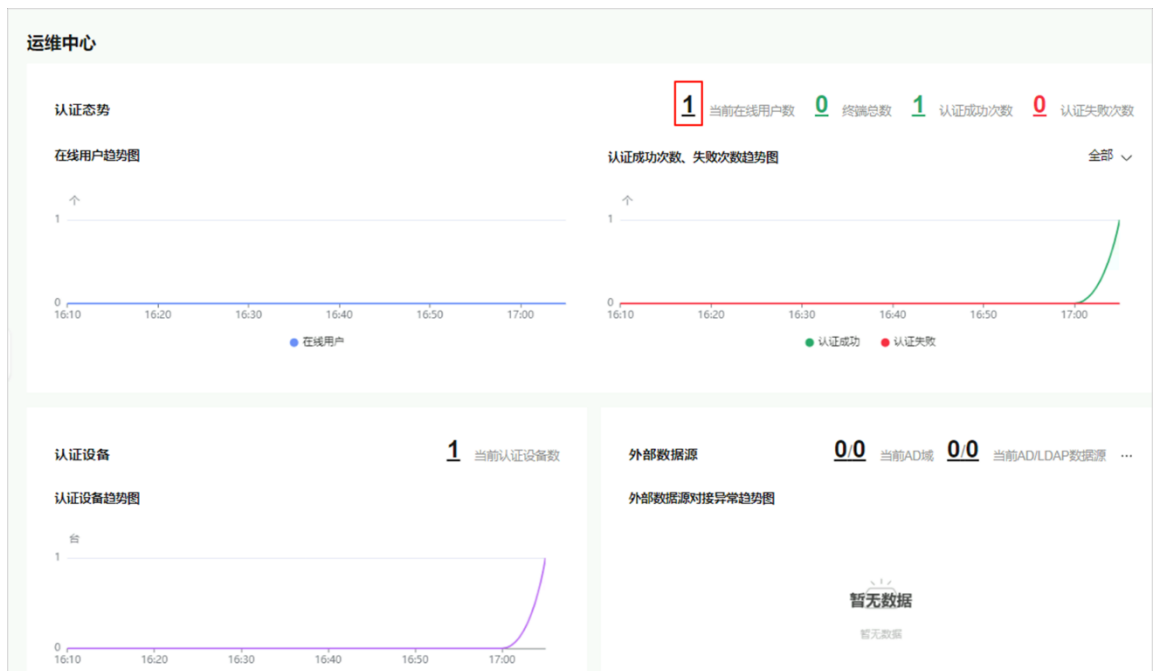


图5-46 进入在线用户查看界面



图5-47 进入在线用户详情界面



图5-48 查看在线用户 User02 详情

以上截图信息表明，PC2 通过使用 User02 的账户已成功接入网络中。

5.3.2 Portal 认证

使用 RDP 登录 PC3 (地址: 172.21.10.203, 账号: admin/Huawei123!), 打开无线网络管理并连接 “hq_user” 无线网络, 执行以下操作:

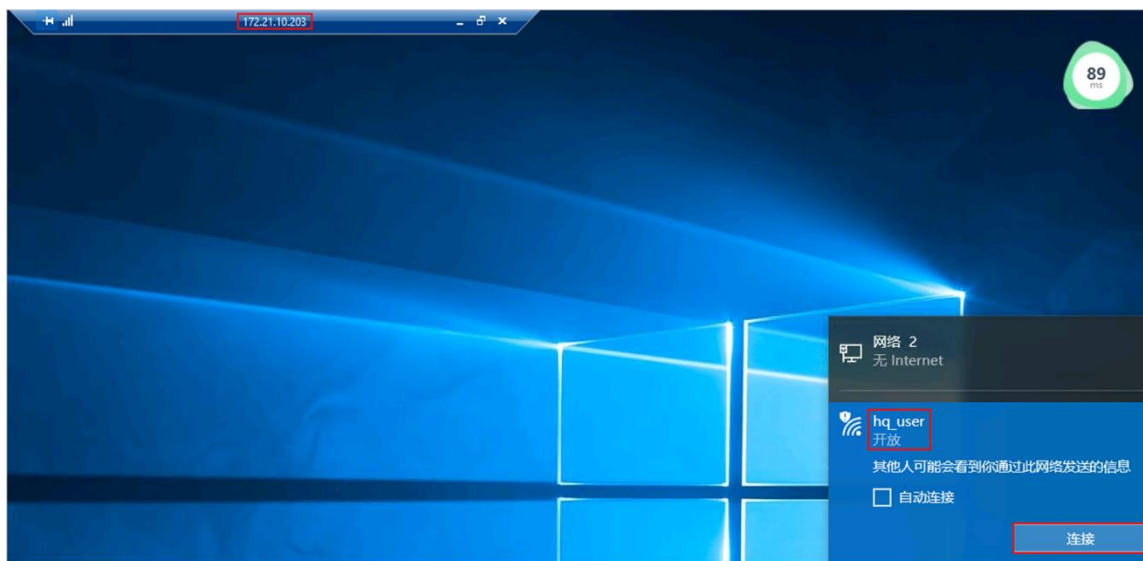


图5-49 PC3 连接无线网络



图5-50 PC3 打开浏览器访问任意 IP

浏览器访问任意 IP 后，会自动跳转到 Portal 认证界面：

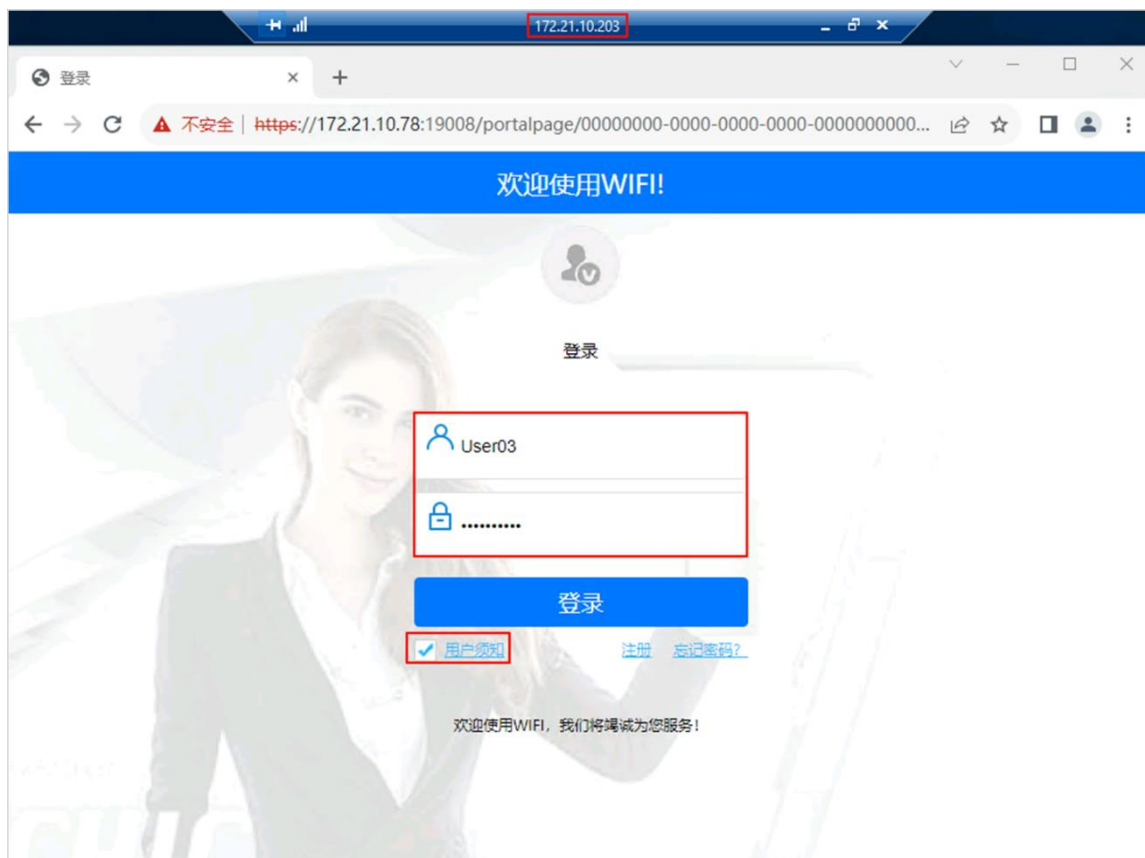


图5-51 PC3 跳转到 Portal 认证界面

输入 User03 的账户信息后，通过 Portal 认证，效果如下：

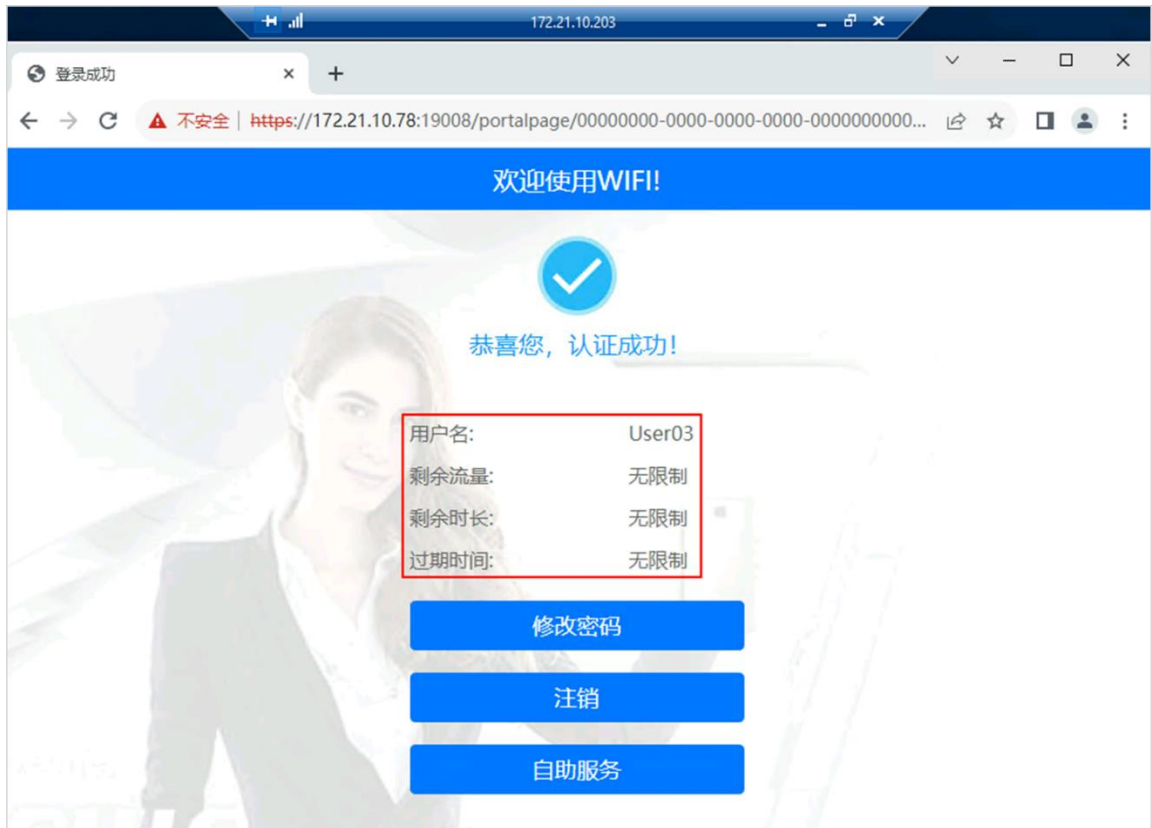


图5-52 PC3 终端 Portal 认证成功

登录 NCE-Campus 运维界面（地址：<https://172.21.10.78:18008>，账号：security01/Security@123）选择“准入管理 > 准入概览”，进入准入管理运维主页，执行以下操作：

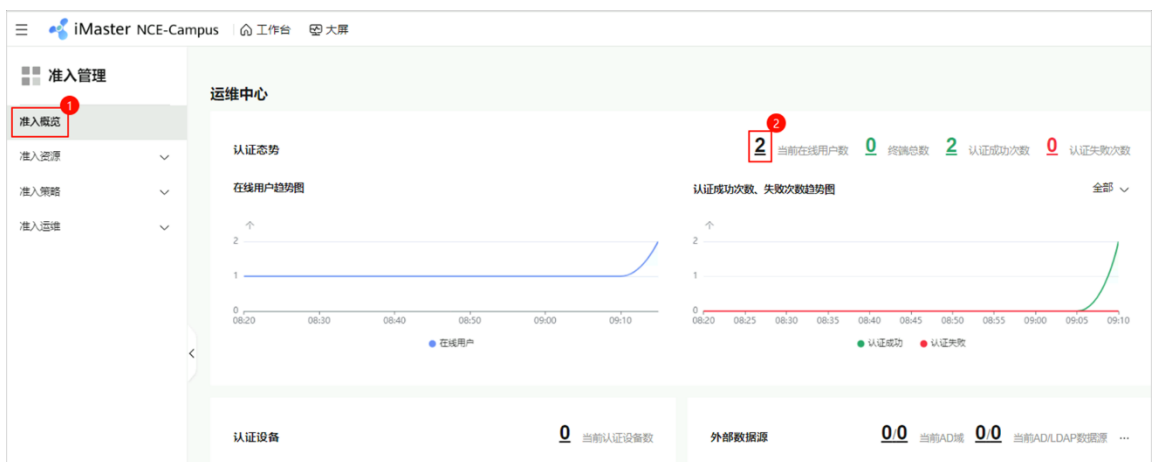


图5-53 进入在线用户管理界面



图5-54 查看 User03 用户详情

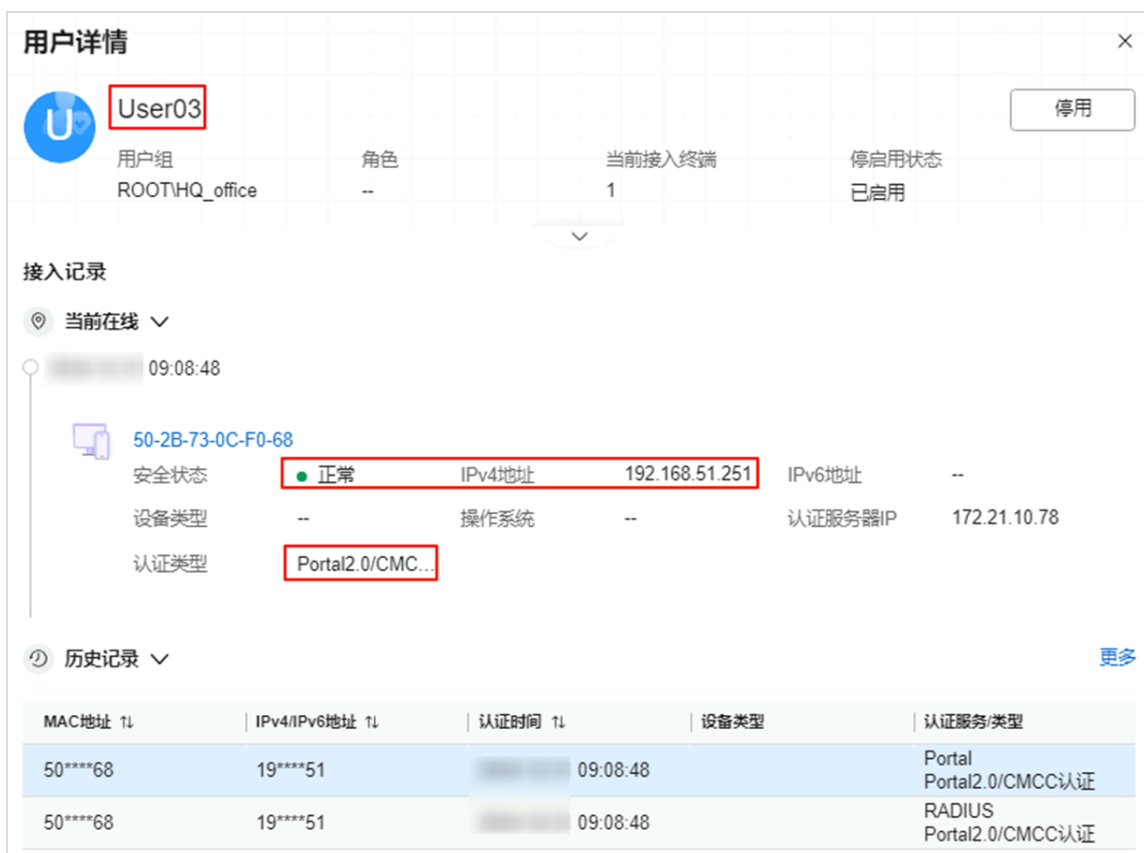


图5-55 User03 用户详情信息

可在 NCE-Campus 运维界面继续选择“准入管理 > 准入运维 > 终端认证日志”查看终端设备认证日志，效果如下：

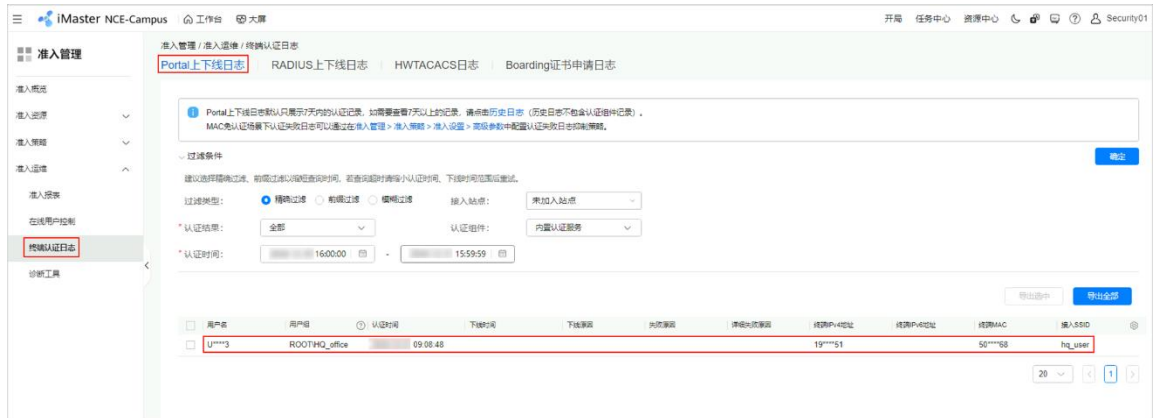


图5-56 查看 Portal 上下线日志

5.4 配置参考（仅展示本实验相关配置）

5.4.1 ACC-SW1 的配置

```
#
l2protocol-tunnel user-defined-protocol dot1x protocol-mac 0180-c200-0003 group-mac 0100-0000-0002
#
interface GE0/0/2
 port link-type access
 port default vlan 12
 l2protocol-tunnel user-defined-protocol dot1x enable
#
interface GE0/0/23
 port link-type trunk
 port trunk allow-pass vlan 11 to 33
 l2protocol-tunnel user-defined-protocol dot1x enable
#
return
```

5.4.2 AGG-SW2 的配置

```
#
radius-server template Campus
 radius-server shared-key cipher Huawei@123
 radius-server authentication 172.21.10.78 1812 source ip-address 172.21.10.4 weight 80
 radius-server accounting 172.21.10.78 1813 source ip-address 172.21.10.4 weight 80
 radius-attribute nas-ip 172.21.10.4
radius-server template default
radius-server template rd1
 radius-server shared-key cipher Huawei@123
 radius-server authentication 172.21.10.78 1812 source ip-address 172.21.10.4 weight 80
 radius-server accounting 172.21.10.78 1813 source ip-address 172.21.10.4 weight 80
 radius-attribute nas-ip 172.21.10.4
radius-server authorization 172.21.10.78 shared-key cipher Huawei@123
radius-server authorization server-source all-interface
#
free-rule-template name default_free_rule
 free-rule 1 destination ip 172.21.10.78 mask 255.255.255.255
#
portal-access-profile name portal_access_profile
#
aaa
 authentication-scheme radius
 authentication-mode radius
 accounting-scheme radius
 accounting-mode radius
 accounting realtime 15
```

```
domain default
 authentication-scheme radius
 accounting-scheme radius
 radius-server Campus
#
interface GE0/0/3
 port link-type access
 port default vlan 12
 authentication-profile dot1x
#
dot1x-access-profile name dot1x
dot1x-access-profile name dot1x_access_profile
#
return
```

5.4.3 AC 的配置

```
#
radius-server source ip-address 172.21.10.61
#
authentication-profile name auth_portal
 portal-access-profile portal
 free-rule-template free_rule
 authentication-scheme radius
 accounting-scheme radius
 radius-server radius
authentication-profile name default_authen_profile
 undo authentication ip-address in-accounting-start
authentication-profile name dot1x_authen_profile
 undo authentication ip-address in-accounting-start
authentication-profile name mac_authen_profile
 undo authentication ip-address in-accounting-start
authentication-profile name macportal_authen_profile
 undo authentication ip-address in-accounting-start
authentication-profile name portal_authen_profile
 undo authentication ip-address in-accounting-start
#
web-auth-server server-source all-interface
#
dhcp enable
#
#
radius-server template radius
 radius-server shared-key cipher %^%#U"+ATtfZoLvC]MUN8VXTGwH*>5>WZ8EdYLL*E(D$%^%#
 radius-server authentication 172.168.10.78 1812 source ip-address 172.168.10.61 weight 80
 radius-server authentication 172.21.10.78 1812 source ip-address 172.21.10.61 weight 80
 radius-server accounting 172.168.10.78 1813 source ip-address 172.168.10.61 weight 80
```



```
radius-server accounting 172.21.10.78 1813 source ip-address 172.21.10.61 weight 80
radius-server authorization 172.21.10.78 shared-key
cipher %^%#Bd4'7nAMu;sE/tVJ3X@BagM[NC@j/F{WXLHk,v8.%^%#
radius-server authorization 172.168.10.78 shared-key cipher %^%#)C=^4+\o)WZE8ZH=)e(.qNA8~vV[%-
Yj<hVTmU/A%^%#
radius-server authorization server-source all-interface
#
free-rule-template name free_rule
  free-rule 1 destination ip 172.21.10.78 mask 255.255.255.255
  free-rule 2 destination ip 172.21.10.61 mask 255.255.255.255
#
url-template name nce
  url https://172.21.10.78:19008/portal
  url-parameter device-ip ac-ip redirect-url redirect-url ssid ssid user-ipaddress uaddress user-mac umac
  url-parameter set device-ip 172.21.10.61
#
web-auth-server portal
  server-ip 172.21.10.78
  port 50100
  shared-key cipher %^%#7gv(5;G`n4"x^WXd!-^BI3C6Fz2p~;kn'W-5Ub^>%^%#
  url-template nce
  source-ip 172.21.10.61
#
portal-access-profile name portal
  web-auth-server portal direct
#
portal-access-profile name portal_access_profile
#
ip pool wlan
  gateway-list 192.168.51.254
  network 192.168.51.0 mask 255.255.255.0
  excluded-ip-address 192.168.51.252
#
aaa
  authentication-scheme radius
    authentication-mode radius
  authorization-scheme default
    authorization-mode local
  accounting-scheme default
    accounting-mode none
  accounting-scheme radius
    accounting-mode radius
    accounting realtime 15
  domain default
    authentication-scheme radius
    accounting-scheme radius
    radius-server radius
#
```

```
interface Vlanif51
 ip address 192.168.51.254 255.255.255.0
 dhcp select global
#
interface GE0/0/1
 port link-type trunk
 port trunk allow-pass vlan 50 to 51
#
wlan
 temporary-management psk %^%#%0WR@55R%0,N1s&sLotX-rTBPMR4|E7tmlTA{k;4%^%#
 ap username admin password cipher %^%#HDZ)=0~l)A<-,&]s/R~A_e:CtO5')6$B75%\k4%^%#
 traffic-profile name default
 security-profile name dot1x
 security open
 security-profile name default
 security-profile name default-wds
 security-profile name default-mesh
 security-profile name security_portal
 security open
 ssid-profile name default
 ssid-profile name hq_user
 ssid hq_user
 vap-profile name default
 vap-profile name hq_user
 forward-mode tunnel
 service-vlan vlan-id 51
 ssid-profile hq_user
 security-profile security_portal
 authentication-profile auth_portal
 wds-profile name default
 mesh-handover-profile name default
 mesh-profile name default
 regulatory-domain-profile name default
 regulatory-domain-profile name domain1
 dca-channel 5g bandwidth 20mhz
 dca-channel 6g bandwidth 20mhz
 air-scan-profile name default
 rrm-profile name default
 radio-2g-profile name default
 radio-5g-profile name default
 wids-spoof-profile name default
 wids-whitelist-profile name default
 wids-profile name default
 wireless-access-specification
 tunnel-ap-group name default
 ap-system-profile name default
 port-link-profile name default
 wired-port-profile name default
```

```
ap auth-mode no-auth
ap-group name gruo1
ap-group name group1
    regulatory-domain-profile domain1
radio 0
    vap-profile hq_user wlan 1
radio 1
    vap-profile hq_user wlan 1
ap-group name gruop1
ap-group name default
ap-id 0 type-id 187 ap-mac 28fb-aeb7-cd00 ap-sn 2102354MXJ10Q3100219
    ap-name office_ap
    ap-group group1
provision-ap
#
return
```

5.5 思考题

如果企业中 Portal 认证的主要服务对象是短期使用无线网络的外来访客，针对此类用户，提供的 Portal 认证应该具备哪些要素？

答：针对外来访客，建议在定制 Portal 页面时使用内部员工审批模板，且访客账号应存放在单独的节点内管理，并设置较短的账号过期时间，同时在审批过程中尽可能记录真实详尽的访客信息，便于出现安全问题后取证调查。

6 VPN 综合实验

6.1 实验介绍

6.1.1 关于本实验

公司网络分为总部网络和分支网络，防火墙作为出口设备部署在总部和分支网络的边界，通过在总部和分支之间部署 IPsec VPN 隧道，实现总部与分支的数据加密传输，以保障跨站点通信的安全。

同时企业总部存在出差员工，需要保障在途/出差员工可通过 Internet 访问公司总部中的 Web 资源和文件资源，通过在总部出口防火墙上部署 SSL VPN 虚拟网关，实现企业外部员工的远程安全接入。

6.1.2 实验组网介绍

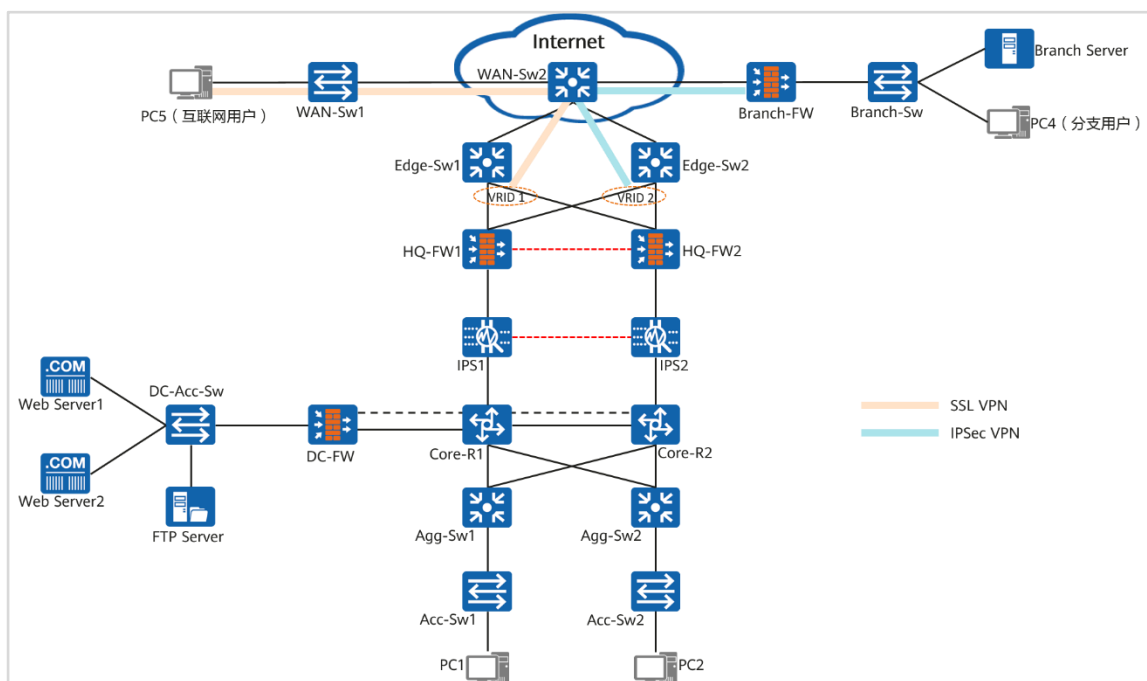


图6-1 实验拓扑图

6.1.3 实验规划

1. 为保障企业总部和分支之间的通信安全，需要在总部出口防火墙 HQ-FW 设备和企业分支出口防火墙 Branch-FW 之间部署 IPsec VPN 隧道，总部使用 HQ-FW 对接 Edge-Sw2 设备的 VRRP 备份组（VRID 2）作为 IPsec VPN 隧道端点，以此实现隧道高可用。
2. 企业总部员工出差或在途期间，为保证办公效率，公司需给在外员工提供远程接入网络的安全隧道，便于员工远程获取内网各类重要文件和资料及时满足业务需求。本实验中，总部出口防火墙 HQ-FW 设备使用对接 Edge-Sw1 设备的 VRRP 备份组（VRID 1）作为 SSL VPN 虚拟网关，以此实现 SSL VPN 的网关冗余。同时开启 SSL VPN 的网络扩展功能，并在防火墙上设置合理的安全策略和准入控制策略保障内网安全。SSL VPN 相关配置参数规划如下：

表6-1 SSL VPN 网关参数规划

网关设备	配置项	参数
HQ-FW1 HQ-FW2	网关名称	SSL_Gateway_1
	网关地址	100.1.34.3
	端口	443

表6-2 网络扩展功能参数规划

配置项	参数
保活超时时间	120
网络扩展地址池	ip_pool
地址池范围	192.168.11.220-192.168.11.250
路由模式	自适应
可访问的内网资源名称	test
可访问资源	192.168.16.0/24

表6-3 SSL VPN 角色参数规划

配置项	参数
角色名	Role1
安全组	group1
用户名	User001
登录密码	Huawei@123
可访问资源	test

6.2 实验配置任务

6.2.1 配置思路

1. IPsec VPN 配置思路：
 - （1）配置安全策略放行 IPsec 隧道协商流及业务流；

- (2) 创建高级 ACL 筛选兴趣流;
- (3) 配置 IPsec 安全提议;
- (4) 配置 IKE 安全提议;
- (5) 配置 IKE 对等体;
- (6) 配置 IPsec 策略 (模板);
- (7) 业务接口上调用 IPsec 策略;
- (8) 配置静态路由, 将去往企业分支用户的流量牵引至 Edge-Sw2 设备转发。

2. SSL VPN 配置思路:

- (1) 在出口防火墙上配置安全策略放行隧道协商流及业务流;
- (2) 在 DC-FW 上配置安全策略, 放行外部员工访问数据中心服务器的业务流量;
- (3) 在 HQ-FW1 上创建 ucl 组和用于 SSL VPN 远程接入的用户账号;
- (4) 在出口防火墙上配置内网地址池用于远程用户接入内网时获取内网地址;
- (5) 在出口防火墙上创建 SSL VPN 虚拟网关, 并设置网关名称和网关端口等参数;
- (6) 在出口防火墙上开启 SSL VPN 网络扩展功能, 并设置相关参数;
- (7) 在出口防火墙上配置 SSL VPN 的角色, 并将角色关联到 ucl 组和可访问的内网资源, 进行资源访问授权。

6.2.2 配置步骤-IPsec VPN (CLI)

步骤 1 配置安全策略 (IPsec)

在 HQ-FW1 设备上配置安全策略, 放行 IPsec VPN 隧道协商流。

```
HRP_M[HQ-FW1] security-policy
HRP_M[HQ-FW1-policy-security] rule name ipsec_ike
HRP_M[HQ-FW1-policy-security-rule-ipsec_ike] source-zone local untrust
HRP_M[HQ-FW1-policy-security-rule-ipsec_ike] destination-zone local untrust
HRP_M[HQ-FW1-policy-security-rule-ipsec_ike] source-address 100.1.35.3 32
HRP_M[HQ-FW1-policy-security-rule-ipsec_ike] source-address 100.1.33.1 32
HRP_M[HQ-FW1-policy-security-rule-ipsec_ike] destination-address 100.1.35.3 32
HRP_M[HQ-FW1-policy-security-rule-ipsec_ike] destination-address 100.1.33.1 32
HRP_M[HQ-FW1-policy-security-rule-ipsec_ike] action permit
HRP_M[HQ-FW1-policy-security-rule-ipsec_ike] quit
HRP_M[HQ-FW1-policy-security]
```

在 HQ-FW1 设备上配置安全策略, 放行总部和分支之间需要基于 IPsec VPN 隧道交互的业务流量 (本实验中要求总部 PC1 和分支 PC4 之间的流量经由 IPsec VPN 转发)。

```
HRP_M[HQ-FW1-policy-security] rule name ipsec_oa
HRP_M[HQ-FW1-policy-security-rule-ipsec_oa] source-zone trust untrust
HRP_M[HQ-FW1-policy-security-rule-ipsec_oa] destination-zone trust untrust
HRP_M[HQ-FW1-policy-security-rule-ipsec_oa] source-address 192.168.11.0 24
HRP_M[HQ-FW1-policy-security-rule-ipsec_oa] source-address 192.168.14.0 24
```

```
HRP_M[HQ-FW1-policy-security-rule-ipsec_oa] destination-address 192.168.11.0 24
HRP_M[HQ-FW1-policy-security-rule-ipsec_oa] destination-address 192.168.14.0 24
HRP_M[HQ-FW1-policy-security-rule-ipsec_oa] action permit
HRP_M[HQ-FW1-policy-security-rule-ipsec_oa] quit
HRP_M[HQ-FW1-policy-security] quit
```

以上安全策略会通过 HRP 自动同步至 HQ-FW2 设备，无需在 HQ-FW2 设备上重复配置。

在 Branch-FW 设备上配置安全策略，放行 IPSec 隧道协商流及业务流。

```
[Branch-FW] security-policy
[Branch-FW-policy-security] rule name ipsec_ike
[Branch-FW-policy-security-rule-ipsec_ike] source-zone untrust local
[Branch-FW-policy-security-rule-ipsec_ike] destination-zone untrust local
[Branch-FW-policy-security-rule-ipsec_ike] source-address 100.1.35.3 32
[Branch-FW-policy-security-rule-ipsec_ike] source-address 100.1.33.1 32
[Branch-FW-policy-security-rule-ipsec_ike] destination-address 100.1.35.3 32
[Branch-FW-policy-security-rule-ipsec_ike] destination-address 100.1.33.1 32
[Branch-FW-policy-security-rule-ipsec_ike] action permit
[Branch-FW-policy-security-rule-ipsec_ike] quit
[Branch-FW-policy-security] rule name ipsec_oa
[Branch-FW-policy-security-rule-ipsec_oa] source-zone trust untrust
[Branch-FW-policy-security-rule-ipsec_oa] destination-zone untrust trust
[Branch-FW-policy-security-rule-ipsec_oa] source-address 192.168.14.0 24
[Branch-FW-policy-security-rule-ipsec_oa] source-address 192.168.11.0 24
[Branch-FW-policy-security-rule-ipsec_oa] destination-address 192.168.14.0 24
[Branch-FW-policy-security-rule-ipsec_oa] destination-address 192.168.11.0 24
[Branch-FW-policy-security-rule-ipsec_oa] action permit
[Branch-FW-policy-security-rule-ipsec_oa] quit
[Branch-FW-policy-security] quit
[Branch-FW]
```

因 PC4 的流量受控于 vFW2 虚拟系统，所以还需要在 vFW2 虚拟系统内配置安全策略，放行 IPSec 业务流。

```
[Branch-FW] switch vsys vFW2
<Branch-FW-vFW2> sy
[Branch-FW-vFW2] security-policy
[Branch-FW-vFW2-policy-security] rule name ipsec_oa
[Branch-FW-vFW2-policy-security-rule-ipsec_oa] source-zone trust untrust
[Branch-FW-vFW2-policy-security-rule-ipsec_oa] destination-zone trust untrust
[Branch-FW-vFW2-policy-security-rule-ipsec_oa] source-address 192.168.14.0 24
[Branch-FW-vFW2-policy-security-rule-ipsec_oa] source-address 192.168.11.0 24
[Branch-FW-vFW2-policy-security-rule-ipsec_oa] destination-address 192.168.14.0 24
[Branch-FW-vFW2-policy-security-rule-ipsec_oa] destination-address 192.168.11.0 24
[Branch-FW-vFW2-policy-security-rule-ipsec_oa] action permit
[Branch-FW-vFW2-policy-security-rule-ipsec_oa] quit
[Branch-FW-vFW2-policy-security] quit
[Branch-FW-vFW2] quit
<Branch-FW-vFW2> quit
[Branch-FW]
```

步骤 2 筛选兴趣流

在 HQ-FW1 设备上创建高级 ACL 筛选 IPsec VPN 隧道业务流。

```
HRP_M[HQ-FW1] acl 3000
HRP_M[HQ-FW1-acl4-advance-3000] rule permit ip source 192.168.11.0 0.0.0.255 destination
192.168.14.0 0.0.0.255
HRP_M[HQ-FW1-acl4-advance-3000] quit
HRP_M[HQ-FW1]
```

HQ-FW2 设备会通过 HRP 自动同步，无需单独配置。

在 Branch-FW 设备上创建高级 ACL 筛选 IPsec VPN 隧道业务流。

```
[Branch-FW] acl 3000
[Branch-FW-acl4-advance-3000] rule permit ip source 192.168.14.0 0.0.0.255 destination 192.168.11.0
0.0.0.255
[Branch-FW-acl4-advance-3000] quit
[Branch-FW]
```

步骤 3 配置 IPsec、IKE 安全提议

HQ-FW1 配置 IPsec 安全提议与 IKE 安全提议。

```
HRP_M[HQ-FW1] ipsec proposal HQ
Warning: GCM/GMAC are authenticated encryption algorithms, esp authentication config is ignored.
HRP_M[HQ-FW1-ipsec-proposal-HQ] encapsulation-mode tunnel
HRP_M[HQ-FW1-ipsec-proposal-HQ] transform esp
HRP_M[HQ-FW1-ipsec-proposal-HQ] esp authentication-algorithm sha2-256
HRP_M[HQ-FW1-ipsec-proposal-HQ] esp encryption-algorithm aes-256-gcm-128
HRP_M[HQ-FW1-ipsec-proposal-HQ] quit
HRP_M[HQ-FW1] ike proposal 10
HRP_M[HQ-FW1-ike-proposal-10] authentication-method pre-share
HRP_M[HQ-FW1-ike-proposal-10] prf hmac-sha2-256
HRP_M[HQ-FW1-ike-proposal-10] encryption-algorithm aes-gcm-256
HRP_M[HQ-FW1-ike-proposal-10] dh group14
HRP_M[HQ-FW1-ike-proposal-10] integrity-algorithm hmac-sha2-256
HRP_M[HQ-FW1-ike-proposal-10] quit
```

HQ-FW2 设备会通过 HRP 自动同步上述配置，无需单独配置。

在 Branch-FW 设备上配置 IPsec 安全提议与 IKE 安全提议。

```
[Branch-FW] ipsec proposal Branch
Warning: GCM/GMAC are authenticated encryption algorithms, esp authentication config is ignored.
[Branch-FW-ipsec-proposal-Branch] encapsulation-mode tunnel
[Branch-FW-ipsec-proposal-Branch] transform esp
[Branch-FW-ipsec-proposal-Branch] esp authentication-algorithm sha2-256
[Branch-FW-ipsec-proposal-Branch] esp encryption-algorithm aes-256-gcm-128
[Branch-FW-ipsec-proposal-Branch] quit
[Branch-FW] ike proposal 10
[Branch-FW-ike-proposal-10] authentication-method pre-share
[Branch-FW-ike-proposal-10] prf hmac-sha2-256
```



```
[Branch-FW-ike-proposal-10] encryption-algorithm aes-gcm-256
[Branch-FW-ike-proposal-10] dh group14
[Branch-FW-ike-proposal-10] integrity-algorithm hmac-sha2-256
[Branch-FW-ike-proposal-10] quit
[Branch-FW]
```

步骤 4 配置 IKE 对等体

在 HQ-FW1 设备创建 IKE 对等体。

```
HRP_M[HQ-FW1] ike peer Branch
HRP_M[HQ-FW1-ike-peer-Branch] ike-proposal 10
HRP_M[HQ-FW1-ike-peer-Branch] pre-shared-key Huawei@123
HRP_M[HQ-FW1-ike-peer-Branch] quit
HRP_M[HQ-FW1]
```

HQ-FW2 设备会通过 HRP 自动同步上述配置，无需单独配置。

在 Branch-FW 设备创建 IKE 对等体。

```
[Branch-FW] ike peer HQ
[Branch-FW-ike-peer-HQ] ike-proposal 10
[Branch-FW-ike-peer-HQ] remote-address 100.1.35.3
[Branch-FW-ike-peer-HQ] pre-shared-key Huawei@123
[Branch-FW-ike-peer-HQ] quit
[Branch-FW]
```

步骤 5 配置 IPsec 策略

在 HQ-FW1 设备上创建 IPsec 策略模板，并基于模板创建 IPsec 策略。

```
HRP_M[HQ-FW1] ipsec policy-template policy1 1
HRP_M[HQ-FW1-ipsec-policy-templet-policy1-1] security acl 3000
HRP_M[HQ-FW1-ipsec-policy-templet-policy1-1] proposal HQ
HRP_M[HQ-FW1-ipsec-policy-templet-policy1-1] ike-peer Branch
HRP_M[HQ-FW1-ipsec-policy-templet-policy1-1] tunnel local 100.1.35.3
HRP_M[HQ-FW1-ipsec-policy-templet-policy1-1] quit
HRP_M[HQ-FW1] ipsec policy map1 10 isakmp template policy1
HRP_M[HQ-FW1]
```

HQ-FW2 设备会通过 HRP 自动同步上述配置，无需单独配置。

在 Branch-FW 设备上创建 IPsec 策略。

```
[Branch-FW] ipsec policy map1 10 isakmp
Info: The ISAKMP policy sequence number should be smaller than the template policy sequence number
in the policy group.Otherwise, the ISAKMP policy does not take effect.
[Branch-FW-ipsec-policy-isakmp-map1-10] security acl 3000
[Branch-FW-ipsec-policy-isakmp-map1-10] proposal Branch
[Branch-FW-ipsec-policy-isakmp-map1-10] ike-peer HQ
[Branch-FW-ipsec-policy-isakmp-map1-10] quit
[Branch-FW]
```

步骤 6 调用 IPsec 策略

在 HQ-FW1 设备的 G0/0/1 接口下调用 IPsec 策略。

```
HRP_M[HQ-FW1] interface g0/0/1
HRP_M[HQ-FW1-GE0/0/1] ipsec policy map1
HRP_M[HQ-FW1-GE0/0/1] quit
```

HQ-FW2 设备会通过 HRP 自动同步上述配置，无需单独配置。

在 Branch-FW 设备的 G0/0/0 接口下调用 IPsec 策略。

```
[Branch-FW] interface g0/0/0
[Branch-FW-GE0/0/0] ipsec policy map1
[Branch-FW-GE0/0/0] quit
```

步骤 7 静态路由引流

在 HQ-FW1 设备上配置静态路由，将去往分支 Branch-FW 设备和 PC4 的流量牵引至 Edge-SW2 设备转发。

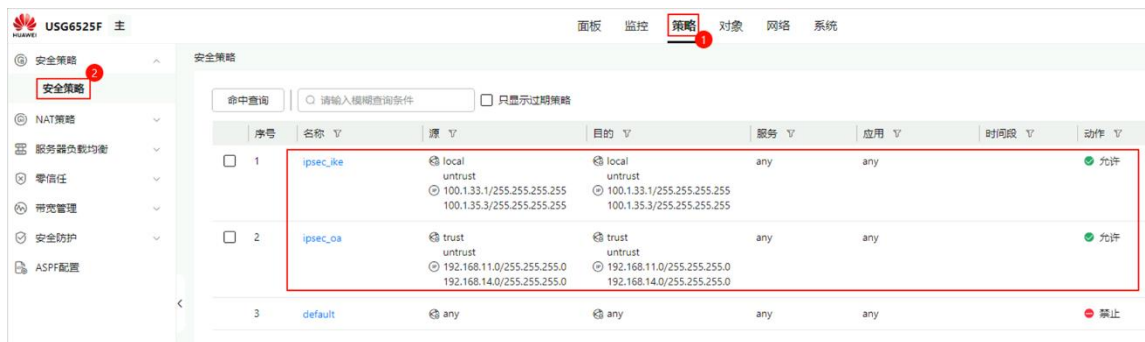
```
HRP_M[HQ-FW1] ip route-static 192.168.14.0 24 100.1.35.6
HRP_M[HQ-FW1] ip route-static 100.1.33.1 32 100.1.35.6
```

HQ-FW2 设备会通过 HRP 自动同步上述配置，无需单独配置。

6.2.3 配置步骤-IPsec VPN (Web)

步骤 1 配置安全策略 (IPsec)

登录 HQ-FW1 设备 Web 管理界面（地址：<https://172.21.10.21:8443/>，账号：Webuser/Admin@123），选择“策略 > 安全策略 > 新建安全策略”，按照 IPsec VPN 业务规划创建安全策略，创建策略细节操作可参考“1 防火墙综合实验”相关操作步骤，安全策略创建完成后效果如下：



序号	名称	源	目的	服务	应用	时间段	动作
1	ipsec_ike	local untrust 100.1.33.1/255.255.255.255 100.1.35.3/255.255.255.255	local untrust 100.1.33.1/255.255.255.255 100.1.35.3/255.255.255.255	any	any		允许
2	ipsec_oa	trust untrust 192.168.11.0/255.255.255.0 192.168.14.0/255.255.255.0	trust untrust 100.1.33.1/255.255.255.0 192.168.14.0/255.255.255.0	any	any		允许
3	default	any	any	any	any		禁止

图6-2 HQ-FW1 安全策略配置信息

登录 Branch-FW 设备 Web 管理界面（地址：<https://172.21.10.24:8443/>，账号：Webuser/Admin@123），选择“策略 > 安全策略 > 新建安全策略”，按照 IPsec VPN 业务规划创建安全策略，创建策略细节操作可参考“1 防火墙综合实验”相关操作步骤，安全策略创建完成后效果如下：

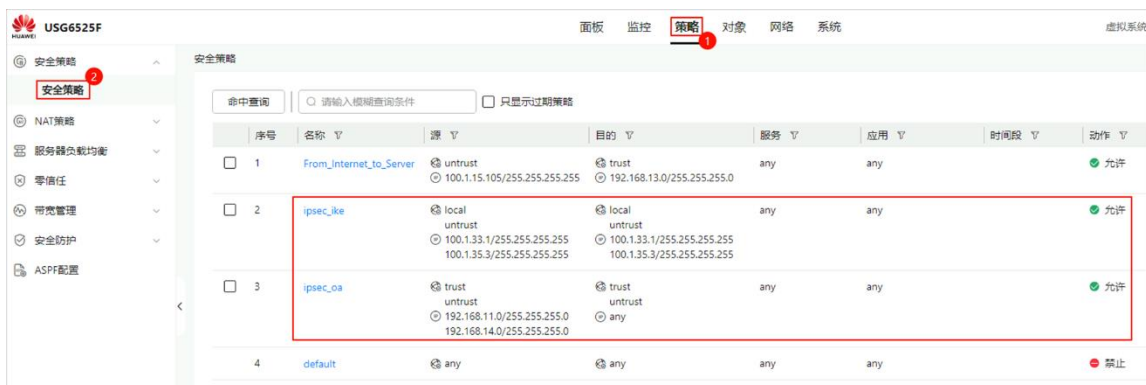


图6-3 Branch-FW 安全策略配置信息

步骤 2 配置 IPsec 策略

登录 HQ-FW1 设备 Web 管理界面（地址：<https://172.21.10.21:8443/>，账号：Webuser/Admin@123），选择“网络 > IPsec > IPsec”，进入 IPsec 策略配置界面，点击“新建”，执行以下操作：



图6-4 选择 IPsec 应用场景



图6-5 IPsec 策略基础参数配置



图6-6 定义 IPsec VPN 业务数据流

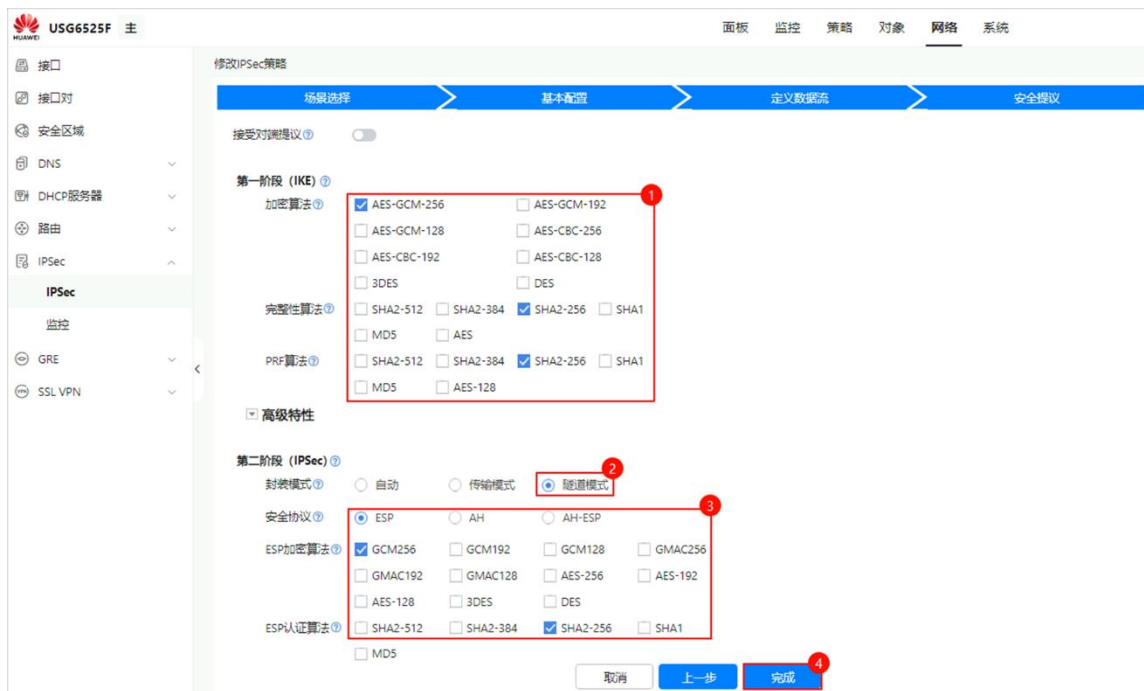


图6-7 配置 IKE 和 IPsec 安全提议并提交 IPsec 策略

上述配置在 HQ-FW2 设备上会通过 HRP 自动同步，无需单独配置。

登录 Branch-FW 设备 Web 管理界面（地址：<https://172.21.10.24:8443/>，账号：Webuser/Admin@123），选择“网络 > IPsec > IPsec”，进入 IPsec 策略配置界面，点击“新建”，执行以下操作：



图6-8 选择 IPsec 应用场景



USG6525F

修改IPsec策略

场景选择 基本配置 定义数据流 安全提议

虚拟系统: public

策略名称: map1-10

本端接口: GE0/0/0 (配置)

本端地址: 100.133.1

对端地址: 100.135.3

认证方式: 预共享密钥 RSA签名

预共享密钥: Huawei@123

本地ID: IP地址

对端ID: IP地址

协商报文路由注入: ☐

取消 上一步 下一步

图6-9 IPsec 策略基础参数配置



USG6525F

修改IPsec策略

场景选择 基本配置 定义数据流 安全提议

待加密的数据流

地址类型: ☒ IPv4 ☐ IPv6

新建 删除 插入

请输入要查询的IP 查询

源地址	目的地址	协议	源端口	目的端...	动作	编辑
192.168.14.0/255.255.255.0	192.168.11.0/255.255.255.0	any	any	any	加密	

共1条 < 1 > 50条/页 前往 1 页

反向路由注入: ☐

取消 上一步 下一步

图6-10 定义 IPSec VPN 业务数据流



图6-11 配置 IKE 和 IPSec 安全提议并提交 IPSec 策略

6.2.4 配置步骤-SSL VPN (CLI)

步骤 1 配置安全策略 (SSL)

在 HQ-FW1 设备上配置安全策略，放行 SSL VPN 隧道协商流和业务流。

```
HRP_M[HQ-FW1] security-policy
HRP_M[HQ-FW1-policy-security] rule name sslvpn_gw
HRP_M[HQ-FW1-policy-security-rule-sslvpn_gw] source-zone untrust
HRP_M[HQ-FW1-policy-security-rule-sslvpn_gw] destination-zone local
HRP_M[HQ-FW1-policy-security-rule-sslvpn_gw] source-address 100.1.15.0 mask 255.255.255.0
HRP_M[HQ-FW1-policy-security-rule-sslvpn_gw] action permit
HRP_M[HQ-FW1-policy-security-rule-sslvpn_gw] quit
HRP_M[HQ-FW1-policy-security] rule name sslvpn_oa
HRP_M[HQ-FW1-policy-security-rule-sslvpn_oa] quit
HRP_M[HQ-FW1-policy-security] rule name sslvpn_oa
HRP_M[HQ-FW1-policy-security-rule-sslvpn_oa] source-zone untrust
HRP_M[HQ-FW1-policy-security-rule-sslvpn_oa] destination-zone trust
HRP_M[HQ-FW1-policy-security-rule-sslvpn_oa] source-address 192.168.11.0 24
HRP_M[HQ-FW1-policy-security-rule-sslvpn_oa] destination-address 192.168.16.0 24
HRP_M[HQ-FW1-policy-security-rule-sslvpn_oa] service http ftp
HRP_M[HQ-FW1-policy-security-rule-sslvpn_oa] action permit
HRP_M[HQ-FW1-policy-security-rule-sslvpn_oa] quit
HRP_M[HQ-FW1-policy-security] quit
HRP_M[HQ-FW1] firewall detect ftp
```

HQ-FW2 设备会通过 HRP 自动同步上述配置，无需单独配置。

在 DC-FW 设备上配置安全策略，放行由 SSL VPN 远程接入的用户访问公司总部数据中心服务器。

```
[DC-FW] security-policy
[DC-FW-policy-security] rule name sslvpn_oa
[DC-FW-policy-security-rule-sslvpn_oa] source-zone untrust
[DC-FW-policy-security-rule-sslvpn_oa] destination-zone dmz
[DC-FW-policy-security-rule-sslvpn_oa] source-address 192.168.11.0 24
[DC-FW-policy-security-rule-sslvpn_oa] destination-address 192.168.16.0 24
[DC-FW-policy-security-rule-sslvpn_oa] service http ftp
[DC-FW-policy-security-rule-sslvpn_oa] action permit
[DC-FW-policy-security-rule-sslvpn_oa] quit
[DC-FW-policy-security] quit
[DC-FW] firewall detect ftp
```

步骤 2 创建用户和 UCL 组

```
HRP_M[HQ-FW1] ucl-group name group1
HRP_M[HQ-FW1] aaa
HRP_M[HQ-FW1-aaa] local-access-user User001
HRP_M[HQ-FW1-aaa-access-user-User001] password cipher Huawei@123
Info: After changing the rights (including the password, access type) of a local access user, the rights of
users already online do not change.The change takes effect to users who go online after the change.
Info: The password of the local access user is saved in real time, but is not saved in the saved-
configuration file.
HRP_M[HQ-FW1-aaa-access-user-User001] service-type sslvpn
HRP_M[HQ-FW1-aaa-access-user-User001] ucl-group group1
HRP_M[HQ-FW1-aaa-access-user-User001] quit
HRP_M[HQ-FW1-aaa] quit
HRP_M[HQ-FW1]
```

HQ-FW2 设备会通过 HRP 自动同步上述配置，无需单独配置。

步骤 3 创建地址池

在 HQ-FW1 设备上创建地址池，用于给通过 SSL VPN 远程接入的用户分配内网地址。

```
HRP_M[HQ-FW1] ip pool ip_pool
HRP_M[HQ-FW1-ip-pool-ip_pool] section 0 192.168.11.220 192.168.11.250
HRP_M[HQ-FW1-ip-pool-ip_pool] quit
HRP_M[HQ-FW1]
```

在 Core-R1 设备上配置针对地址池的回程静态路由，并将其重分发至 OSPF 进程中，避免远程用户通过 SSL VPN 访问内网服务器后，响应报文无法正确转发至 HQ-FW 设备上（若规划的 SSL VPN 网络扩展的地址池和内网现有业务网段重叠时，需要执行此操作，否则可略过此操作）。

```
[Core-R1] ip route-static 192.168.11.192 26 192.168.10.49
[Core-R1] ospf 1
[Core-R1-ospf-1] import-route static
```


步骤 4 创建 SSL VPN 虚拟网关

```
HRP_M[HQ-FW1] virtual-gateway SSL_Gateway_1
HRP_M[HQ-FW1-virtual-gateway-SSL_Gateway_1] service address 100.1.34.3 port 443
HRP_M[HQ-FW1-virtual-gateway-SSL_Gateway_1] service
HRP_M[HQ-FW1-virtual-gateway-SSL_Gateway_1-service] network-extension keep-alive timeout 120
HRP_M[HQ-FW1-virtual-gateway-SSL_Gateway_1-service] network-extension ip-pool ip_pool
HRP_M[HQ-FW1-virtual-gateway-SSL_Gateway_1-service] network-extension mode adapt
HRP_M[HQ-FW1-virtual-gateway-SSL_Gateway_1-service] network-extension resource test ip-subnet
192.168.16.0 255.255.255.0
HRP_M[HQ-FW1-virtual-gateway-SSL_Gateway_1-service] quit
HRP_M[HQ-FW1-virtual-gateway-SSL_Gateway_1] quit
HRP_M[HQ-FW1]
```

步骤 5 配置 SSL VPN 角色

```
HRP_M[HQ-FW1] virtual-gateway SSL_Gateway_1
HRP_M[HQ-FW1-virtual-gateway-SSL_Gateway_1] role Role1
HRP_M[HQ-FW1-virtual-gateway-SSL_Gateway_1-role-Role1] group group1
HRP_M[HQ-FW1-virtual-gateway-SSL_Gateway_1-role-Role1] resource test
HRP_M[HQ-FW1-virtual-gateway-SSL_Gateway_1-role-Role1] quit
HRP_M[HQ-FW1-virtual-gateway-SSL_Gateway_1] quit
HRP_M[HQ-FW1]
```

6.2.5 配置步骤-SSL VPN (Web)

步骤 1 配置安全策略 (SSL)

登录 HQ-FW1 设备 Web 管理界面 (地址: <https://172.21.10.21:8443/> , 账号: Webuser/Admin@123) , 选择 “策略 > 安全策略 > 安全策略 > 新建安全策略” , 创建以下安全策略, 放行 SSL VPN 隧道协商流和业务流。

序号	名称	源	目的	服务	应用	时间段	动作
1	ipsec_ike	local untrust 100.1.33.1/255.255.255.255 100.1.35.3/255.255.255.255	local untrust 100.1.33.1/255.255.255.255 100.1.35.3/255.255.255.255	any	any		允许
2	ipsec_oa	trust untrust 192.168.11.0/255.255.255.0 192.168.14.0/255.255.255.0	trust untrust 192.168.11.0/255.255.255.0 192.168.14.0/255.255.255.0	any	any		允许
3	sslvpn_gw	untrust 100.1.15.0/255.255.255.0	local any	any	any		允许
4	sslvpn_oa	untrust 192.168.11.0/255.255.255.0	trust 192.168.16.0/255.255.255.0	http ftp	any		允许
5	default	any	any	any	any		禁止

图6-12 HQ-FW1 设备 SSL VPN 相关安全策略配置

在 HQ-FW1 设备的安全策略配置界面, 继续选择 “ASPF 配置” , 执行以下配置, 开启针对 FTP 的 ASPF 功能。



图6-13 HQ-FW1 设备 FTP 服务 ASPF 功能配置

上述配置 HQ-FW2 设备会通过 HRP 自动同步，无需单独配置。

登录 DC-FW 设备 Web 管理界面（地址：<https://172.21.10.23:8443/>，账号：Webuser/Admin@123），选择“策略 > 安全策略 > 安全策略 > 新建安全策略”，创建以下安全策略，放行 SSL VPN 业务流。

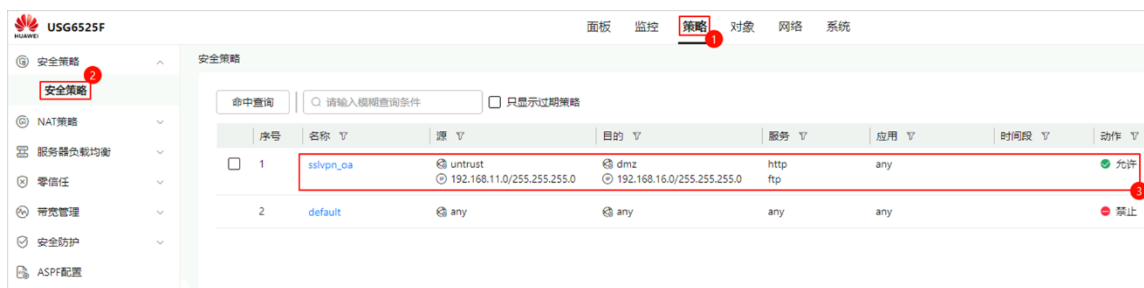


图6-14 DC-FW 设备 SSL VPN 相关安全策略配置



图6-15 DC-FW 设备 FTP 服务 ASPF 功能配置

步骤 2 创建 SSL VPN 用户

登录 HQ-FW1 设备 Web 管理界面（地址：<https://172.21.10.21:8443/>，账号：Webuser/Admin@123），选择“对象 > 用户 > 用户管理 > 安全组 > 新建”，执行以下操作：



图6-16 HQ-FW1 设备创建用户安全组

完成安全组创建后，在安全组内创建 SSL VPN 登录用户：



图6-17 HQ-FW1 设备创建 SSL VPN 用户

上述配置 HQ-FW2 设备会通过 HRP 自动同步，无需单独配置。

步骤 3 配置 SSL VPN 虚拟网关

登录 HQ-FW1 设备 Web 管理界面（地址：https://172.21.10.21:8443/，账号：Webuser/Admin@123），选择“网络 > SSL VPN > SSL VPN > 新建”，进入 SSL VPN 配置界面，执行以下操作：



图6-18 进入 SSL VPN 配置界面

修改 SSL VPN

网关配置

网络扩展

角色授权

* 网关名称

SSL_Gateway_1

* 网关地址

添加网关地址

手动配置IP地址

100.134.3

端口

443

域名

使能链路备份

网关证书

公钥算法切换为SM2将会导致使用RSA算法的VPN客户端无法登录。

RSA

SM2

* 本地证书

default (默认证书)

用户认证

认证方式

用户+密码

认证域

请选择认证域

DNS服务器

添加DNS服务器

DNS域名后缀

隧道生命周期

会话超时时间

5

<1-1440>分钟

生命周期无限制

生命周期

1440

<60-2880>分钟

最大并发用户数

<1-100>

图6-19 SSL VPN 网关基础参数配置

修改 SSL VPN

网关配置

网络扩展

角色授权

保持连接

保活超时时间

120

<60-600>秒

* IP地址池

ip_pool

代理自动配置

接入用户互访

隔离模式

接入终端路由隔离

自适应路由模式

网络扩展资源配置

请输入资源名称

删除

新建

名称	IP网段	描述
test	192.168.16.0/255.255.255.0	

取消

确定

图6-20 配置 SSL VPN 网络扩展参数

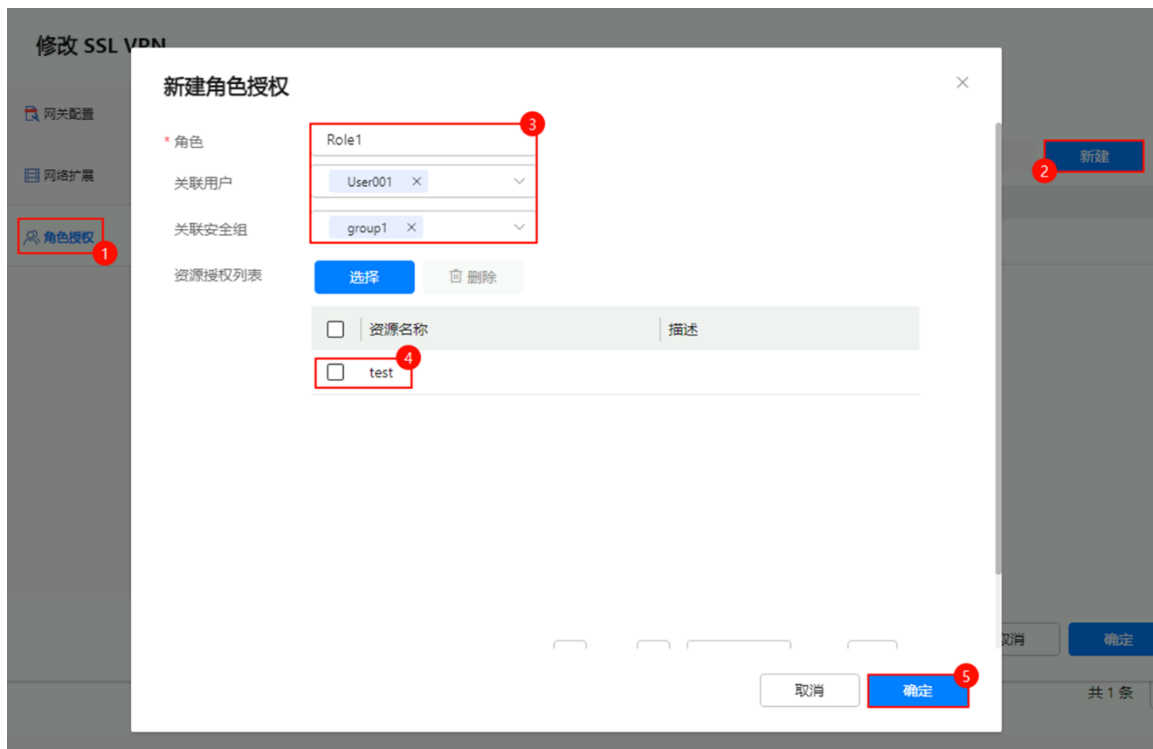


图6-21 配置 SSL VPN 角色授权

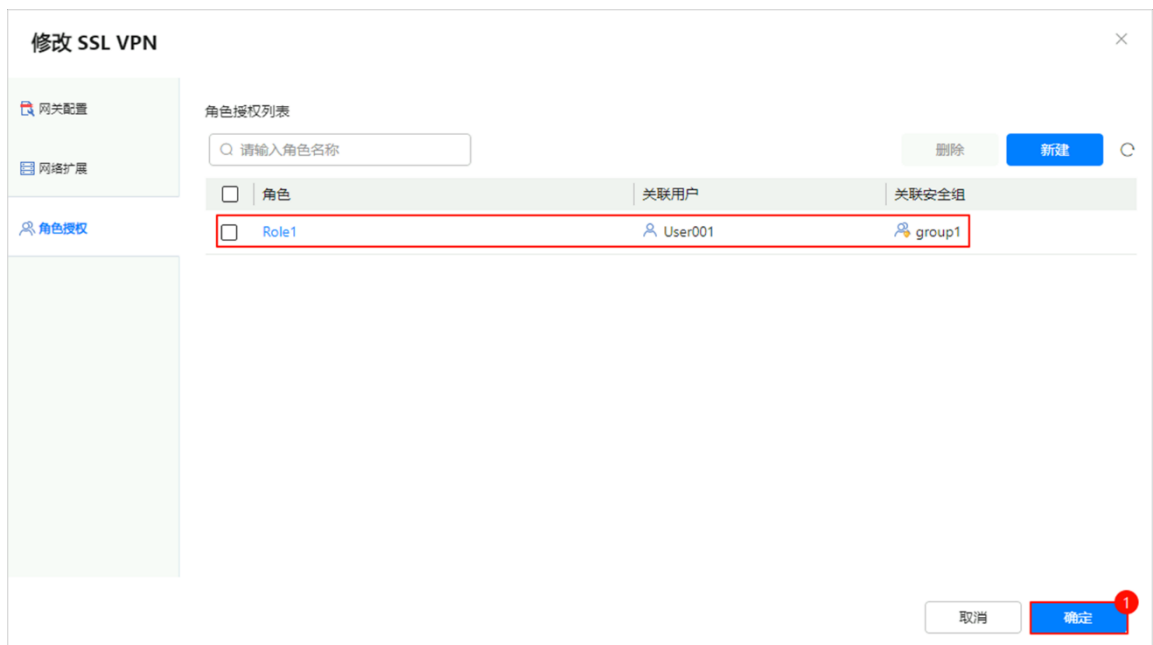


图6-22 确认 SSL VPN 配置信息并提交

在 Core-R1 设备配置针对地址池的回程静态路由，并将其重分发至 OSPF 进程中，避免远程用户通过 SSL VPN 访问内网服务器后，响应报文无法正确转发至 HQ-FW 设备上（若规划的 SSL VPN 网络扩展的地址池和内网现有业务网段重叠时，需要执行此操作，否则可略过此操作）。

```
[Core-R1] ip route-static 192.168.11.192 26 192.168.10.49
```

```
[Core-R1] ospf 1
[Core-R1-ospf-1] import-route static
```

6.3 结果验证

6.3.1 IPSec VPN 验证

登录 HQ-FW1 设备 Web 管理界面（地址：https://172.21.10.21:8443/，账号：Webuser/Admin@123），选择“网络 > IPSec > IPSec”进入 IPSec 策略列表界面，查看 IPSec 策略的配置和协商情况，效果如下：



图6-23 IPSec 策略查看

使用 RDP 登录 PC1（地址：172.21.10.201，账号：admin/Huawei123!），模拟企业总部员工，访问 PC4 业务地址（192.168.14.104），测试 IPSec VPN 隧道连通性是否正常，效果如下：



图6-24 IPSec VPN 业务连通性测试

在 HQ-FW1 设备 Web 管理界面选择“网络 > IPSec > 监控”进入 IPSec 监控界面，效果如下：



图6-25 IPSec 监控

6.3.2 SSL VPN 验证

使用 RDP 登录 PC5 (地址: 172.21.10.205, 账号: admin/Huawei123!), 模拟企业在途员工, 打开桌面“univpn”客户端, 执行以下操作:



图6-26 打开 SSL VPN 客户端并进入 SSL VPN 连接配置界面



图6-27 配置 SSL VPN 连接参数



图6-28 连接 SSL VPN 网关



图6-29 登录 SSL VPN 网关

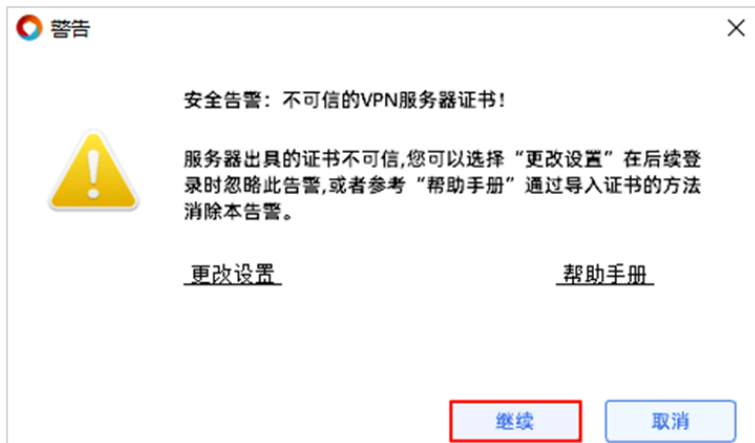


图6-30 忽略证书安全告警



图6-31 SSL VPN 连接成功

打开 PC5 命令行窗口，键入“ipconfig”查看网络参数，可以发现目前已获得内网业务地址：

```
管理员: 命令提示符
C:\Windows\system32>ipconfig

Windows IP 配置

未知适配器 本地连接:

    连接特定的 DNS 后缀 . . . . . :
    本地链接 IPv6 地址. . . . . : fe80::d8e5:8336:501e:11e9%25
    IPv4 地址 . . . . . : 192.168.11.247
    子网掩码 . . . . . : 255.255.255.255
    默认网关. . . . . :

以太网适配器 MSTSC:

    连接特定的 DNS 后缀 . . . . . :
    本地链接 IPv6 地址. . . . . : fe80::d9d8:f49d:1982:217d%11
    IPv4 地址 . . . . . : 172.21.10.205
    子网掩码 . . . . . : 255.255.128.0
    默认网关. . . . . : 172.21.10.254

以太网适配器 Security:

    连接特定的 DNS 后缀 . . . . . :
    本地链接 IPv6 地址. . . . . : fe80::3916:a280:570:4430%2
    IPv4 地址 . . . . . : 100.1.15.105
    子网掩码 . . . . . : 255.255.255.0
    默认网关. . . . . : 100.1.15.254

C:\Windows\system32>
```

图6-32 PC5 终端 SSL VPN 网络参数查看

打开 PC5 的浏览器，访问企业总部 Web 服务器（<http://192.168.16.109>），效果如下：



图6-33 PC5 通过 SSL VPN 远程访问企业总部 Web 业务

继续打开 PC 的文件资源管理器，访问企业总部数据中心 FTP（ftp://192.168.16.110），效果如下：

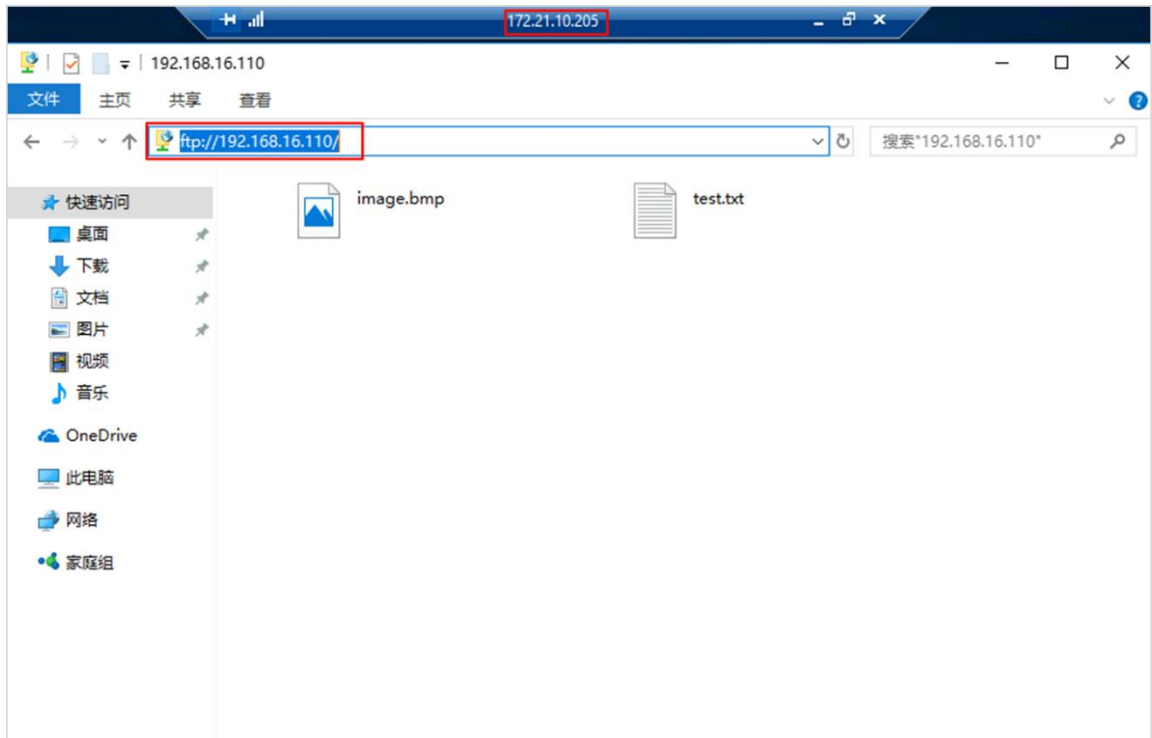


图6-34 PC5 通过 SSL VPN 访问企业总部 FTP 业务

6.4 配置参考（仅展示本实验相关配置）

6.4.1 HQ-FW1 的配置

```
#
ip pool ip_pool
 section 0 192.168.11.220 192.168.11.250
#
acl number 3000
 rule 5 permit ip source 192.168.11.0 0.0.0.255 destination 192.168.14.0 0.0.0.255
#
interface GE0/0/1
 ip address 100.1.35.1 255.255.255.248
 vrrp vrid 2 virtual-ip 100.1.35.3 active
 service-manage ping permit
 ipsec policy map1
#
ospf 1 router-id 21.21.21.21
 default-route-advertise
 import-route static
 opaque-capability enable
 area 0.0.0.0
 authentication-mode md5 10 cipher Huawei@123
 network 192.168.10.48 0.0.0.3
```

```
#
ip route-static 192.168.14.0 255.255.255.0 100.1.35.6
#
ike proposal 10
  encryption-algorithm aes-gcm-256
  dh group14
  authentication-algorithm sha2-256
  authentication-method pre-share
  integrity-algorithm hmac-sha2-256
  prf hmac-sha2-256
#
ipsec proposal HQ
  esp authentication-algorithm sha2-256
  esp encryption-algorithm aes-256-gcm-128
#
ike peer Branch
  pre-shared-key Huawei@123
  ike-proposal 10
  remote-id-type ip
  remote-id 100.1.33.1
  local-id 100.1.35.3
  dpd type periodic
#
ipsec policy-template policy1 1
  security acl 3000
  ike-peer Branch
  proposal HQ
  tunnel local 100.1.35.3
  alias policy1-1
#
ipsec policy map1 10 isakmp template policy1
#
firewall detect ftp
#
security-policy
  rule name ipsec_ike
    source-zone local
    source-zone untrust
    destination-zone local
    destination-zone untrust
    source-address 100.1.33.1 mask 255.255.255.255
    source-address 100.1.35.3 mask 255.255.255.255
    destination-address 100.1.33.1 mask 255.255.255.255
    destination-address 100.1.35.3 mask 255.255.255.255
    action permit
  rule name ipsec_oa
    source-zone trust
    source-zone untrust
```

```
destination-zone trust
destination-zone untrust
source-address 192.168.11.0 mask 255.255.255.0
source-address 192.168.14.0 mask 255.255.255.0
destination-address 192.168.11.0 mask 255.255.255.0
destination-address 192.168.14.0 mask 255.255.255.0
action permit
rule name sslvpn_gw
source-zone untrust
destination-zone local
source-address 100.1.15.0 mask 255.255.255.0
action permit
rule name sslvpn_oa
source-zone untrust
destination-zone trust
source-address 192.168.11.0 mask 255.255.255.0
destination-address 192.168.16.0 mask 255.255.255.0
service ftp
service http
action permit
#
virtual-gateway SSL_Gateway_1 0
service address 100.1.34.3 port 443
service
network-extension ip-pool ip_pool
network-extension resource test ip-subnet 192.168.16.0 255.255.255.0
role Role1 0
user User001
group group1
resource test
#
return
```

6.4.2 DC-FW 的配置

```
#
firewall detect ftp
#
security-policy
rule name sslvpn_oa
source-zone untrust
destination-zone dmz
source-address 192.168.11.0 mask 255.255.255.0
destination-address 192.168.16.0 mask 255.255.255.0
service ftp
service http
action permit
#
```

6.4.3 Branch-FW 的配置

```
#
acl number 3000
 rule 5 permit ip source 192.168.14.0 0.0.0.255 destination 192.168.11.0 0.0.0.255
#
interface GE0/0/0
 ip address 100.1.33.1 255.255.255.252
 service-manage ping permit
 ipsec policy map1
#
ike proposal 10
 encryption-algorithm aes-gcm-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ipsec proposal Branch
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike peer HQ
 pre-shared-key Huawei@123
 ike-proposal 10
 remote-id-type ip
 dpd type periodic
 remote-address 100.1.35.3
#
ipsec policy map1 10 isakmp
 security acl 3000
 ike-peer HQ
 proposal Branch
 tunnel local applied-interface
 sa trigger-mode auto
#
security-policy
 rule name ipsec_ike
 source-zone local
 source-zone untrust
 destination-zone local
 destination-zone untrust
 source-address 100.1.33.1 mask 255.255.255.255
 source-address 100.1.35.3 mask 255.255.255.255
 destination-address 100.1.33.1 mask 255.255.255.255
 destination-address 100.1.35.3 mask 255.255.255.255
 action permit
```



```
rule name ipsec_oa
  source-zone trust
  source-zone untrust
  destination-zone trust
  destination-zone untrust
  source-address 192.168.11.0 mask 255.255.255.0
  source-address 192.168.14.0 mask 255.255.255.0
  action permit
#
switch vsys vFW2
#
security-policy
  rule name ipsec_oa
    source-zone trust
    source-zone untrust
    destination-zone trust
    destination-zone untrust
    source-address 192.168.11.0 mask 255.255.255.0
    source-address 192.168.14.0 mask 255.255.255.0
    action permit
#
return
```

6.4.4 Core-R1 的配置

```
[Core-R1] ip route-static 192.168.11.192 26 192.168.10.49
[Core-R1] ospf 1
[Core-R1-ospf-1] import-route static
```

6.5 思考题

IPSec VPN 除了使用双机热备保障隧道可靠性之外，还有什么技术可以保障 IPSec VPN 隧道的高可靠性？

答案：还可通过链路冗余备份和智能选路实现 IPSec VPN 隧道高可靠。

为提高网络可靠性，企业总部可通过两条或多条链路与企业分支建立 IPSec 连接。当主物理链路失效时，其路由变为不可达，流量切换到备用链路。IPSec 隧道不需要进行重协商，可快速完成流量切换。

防火墙作为多出口企业的安全网关时，可以通过配置 IPSec 智能选路功能实现多条 IPSec 隧道动态切换。按照链路切换机制的不同可以分为两种不同场景：基于链路质量探测结果和基于路由状态变化。

7

IPv6 网络安全实验

7.1 实验介绍

7.1.1 关于本实验

防火墙 DC-FW 支持双协议栈，连接总部的 IPv6 网络和服务器区域的 IPv4 网络。从运营商处获取的 IPv6 地址段为 2001:db8::/64，NAT64 规划的 IPv6 地址前缀为 2001:db8::/96。管理员将 IPv6 前缀与服务器的 IPv4 地址进行拼接，提供给总部 IPv6 网络中的办公网络进行访问，现要求位于办公网络中的 PC 通过拼接后的 IPv6 地址能够访问到 IPv4 网络中的服务器。

总部 IPv6 网络中使用 OSPFv3 进行 IPv6 的路由学习，为保障总部网络的安全性，汇聚交换机接入核心路由器时，需要进行 OSPFv3 的协议认证；同时办公区域的 PC 通过 DHCPv6 获取 IPv6 地址，为防止 DHCPv6 攻击，需要开启 ND-Snooping。

7.1.2 实验组网介绍

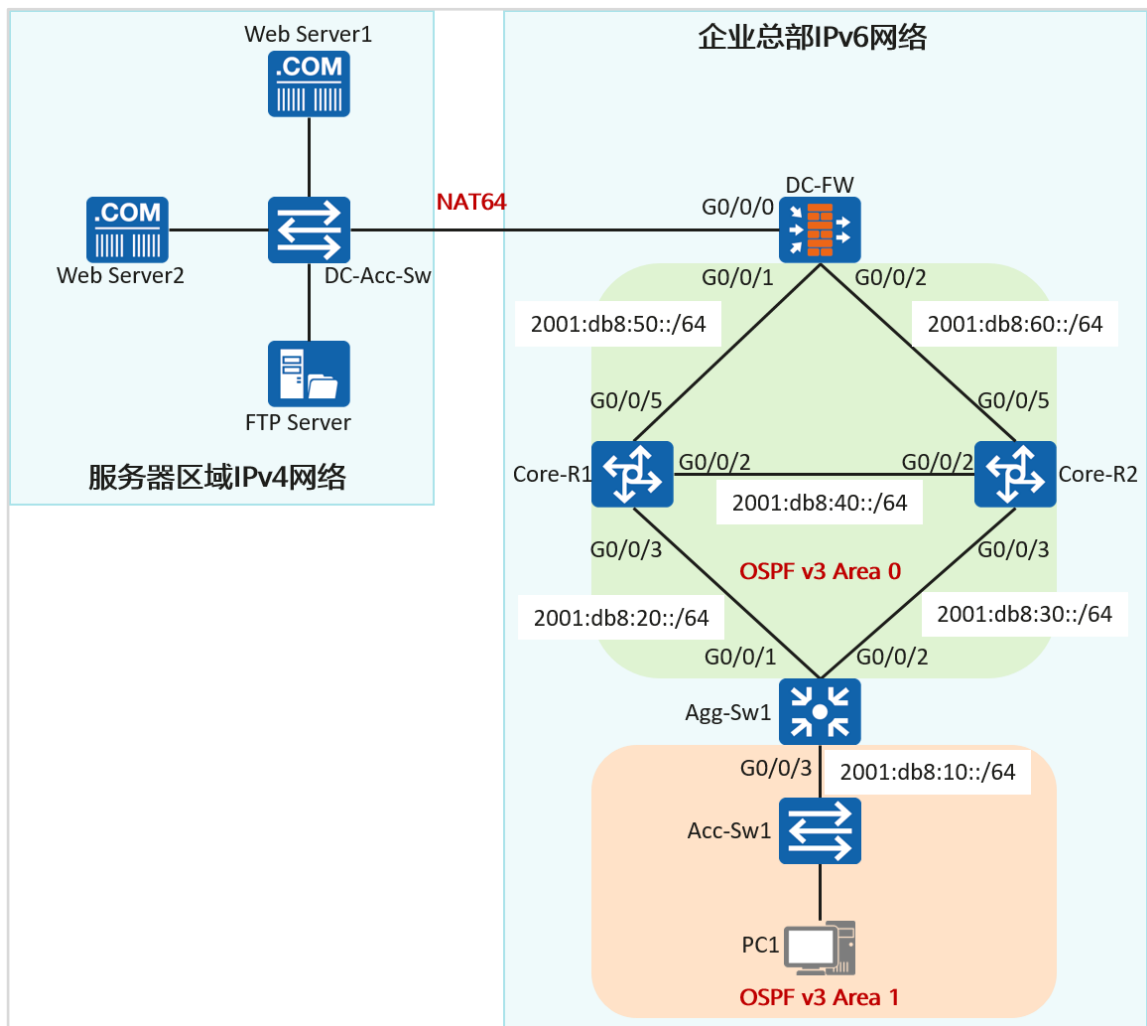


图7-1 实验拓扑图

7.1.3 实验规划

1. DC-FW 设备为总部 IPv6 网络和服务器 IPv4 网络的双栈网关设备。
2. 总部网络办公区域的用户 (PC1)使用 IPv6 地址访问服务器的 IPv4 地址时, 在 DC-FW 上进行 NAT64 的地址转换。
3. 总部网络中部署 OSPFv3 进行 IPv6 路由学习, 为保障总部网络的安全, 核心路由器和汇聚交换机之间需要配置 OSPFv3 认证。
4. 总部研发区域的 PC 通过 DHCPv6 获取 IPv6 地址, 为防御 DHCPv6 攻击, 需要配置 ND-Snooping 功能。

表7-1 端口类型及参数设计

设备	端口(安全区域)	IP
DC-FW	GE0/0/0(DMZ)	192.168.16.254/24
	GE0/0/1(Untrust)	2001:db8:50::2/64

	GE0/0/2(Untrust)	2001:db8:60::2/64
	/	NAT64前缀: 2001:db8::/96
Core-R1	GE0/0/2	2001:db8:40::1/64
	GE0/0/3	2001:db8:20::2/64
	GE0/0/5	2001:db8:50::1/64
Core-R2	GE0/0/2	2001:db8:40::2/64
	GE0/0/3	2001:db8:30::2/64
	GE0/0/5	2001:db8:60::1/64
AGG-SW1	GE0/0/1	2001:db8:20::1/64
	GE0/0/2	2001:db8:30::1/64
	GE0/0/3	2001:db8:10::1/64
PC1	/	前缀: 2001:db8:10::/64 通过DHCPv6获取地址 网关: 2001:db8:10::1/64
Web Server1	/	IPv4地址: 192.168.16.107 NAT64拼接IPv4地址: 2001:db8::c0a8:106b
Web Server2	/	IPv4地址: 192.168.16.108 NAT64拼接IPv4地址: 2001:db8::c0a8:106c
FTP Server	/	IPv4地址: 192.168.16.110 NAT64拼接IPv4地址: 2001:db8::c0a8:106e

7.2 实验配置任务

7.2.1 配置思路

1. 根据规划，在所有设备上配置 IPv6 地址。
2. 在 AGG-SW1 上配置 DHCPv6，使办公区的 PC1 获取 2001:db8:10::/64 前缀的 IPv6 地址，并在 ACC1-SW1 上开启 NP-Snooping 防御 DHCPv6 的攻击。
3. 在 AGG-SW1，Core-R1，Core-R2 和 DC-FW 上配置 OSPFv3 路由协议，进行 IPv6 路由的学习，并在 AGG-SW1，Core-R1 和 Core-R2 之间开启 OSPFv3 认证。
4. 在 DC-FW 上配置 NAT64，使用 PC1 能够通过 IPv6 地址访问到服务器的 IPv4 地址。

7.2.2 配置步骤

步骤 1 配置 IPv6 地址

在 AGG-SW1 上开启 IPv6 功能，并配置 IPv6 地址，命令如下。

```
[AGG-SW1] int vlanif 58
```

```
[AGG-SW1-Vlanif58] ipv6 enable
[AGG-SW1-Vlanif58] ipv6 address 2001:DB8:20::1/64
[AGG-SW1-Vlanif58] int vlanif 70
[AGG-SW1-Vlanif70] ipv6 enable
[AGG-SW1-Vlanif70] ipv6 address 2001:DB8:30::1/64
[AGG-SW1-Vlanif70] int vlanif 11
[AGG-SW1-Vlanif11] ipv6 enable
[AGG-SW1-Vlanif11] ipv6 address 2001:db8:10::1/64
```

在 Core-R1 上开启 IPv6 功能，并配置 IPv6 地址，命令如下。

```
[Core-R1] ipv6
[Core-R1] int g0/0/2
[Core-R1-GE0/0/2] ipv6 enable
[Core-R1-GE0/0/2] ipv6 address 2001:db8:40::1/64
[Core-R1-GE0/0/2] quit
[Core-R1] int g0/0/3
[Core-R1-GE0/0/3] ipv6 enable
[Core-R1-GE0/0/3] ipv6 address 2001:db8:20::2/64
[Core-R1-GE0/0/3] quit
[Core-R1] int g0/0/5
[Core-R1-GE0/0/5] ipv6 enable
[Core-R1-GE0/0/5] ipv6 address 2001:db8:50::1/64
[Core-R1-GE0/0/5] quit
```

在 Core-R2 上开启 IPv6 功能，并配置 IPv6 地址，命令如下。

```
[Core-R2] ipv6
[Core-R2] int g0/0/2
[Core-R2-GE0/0/2] ipv6 enable
[Core-R2-GE0/0/2] ipv6 address 2001:db8:40::2/64
[Core-R2-GE0/0/2] quit
[Core-R2] int g0/0/3
[Core-R2-GE0/0/3] ipv6 enable
[Core-R2-GE0/0/3] ipv6 address 2001:db8:30::2/64
[Core-R2-GE0/0/3] quit
[Core-R2] int g0/0/5
[Core-R2-GE0/0/5] ipv6 enable
[Core-R2-GE0/0/5] ipv6 address 2001:db8:60::1/64
[Core-R2-GE0/0/5] quit
```

在 DC-FW 上开启 IPv6 功能，并配置 IPv6 地址，命令如下。

```
[DC-FW] int g0/0/1
[DC-FW-GE0/0/1] ipv6 enable
[DC-FW-GE0/0/1] ipv6 address 2001:db8:50::2/64
[DC-FW-GE0/0/1] quit
[DC-FW] int g0/0/2
[DC-FW-GE0/0/2] ipv6 enable
[DC-FW-GE0/0/2] ipv6 address 2001:db8:60::2/64
[DC-FW-GE0/0/2] quit
```

```
[DC-FW]
```

步骤 2 配置 DHCPv6 与 ND-Snooping

在 AGG-SW1 上配置 DHCPv6 功能，为总部办公区域的客户端（PC1）分配 IPv6 地址，地址池的前缀为 2001:db8:10::/64，排除网关 IP 地址。配置发布 RA 报文，使 DHCPv6 客户端通过 RA 报文学习到 IPv6 网关的缺省路由；配置发布 RA 报文的 M 和 O 标志位，使 DHCPv6 客户端通过 DHCPv6 方式获取 IPv6 地址和其他网络参数，命令如下。

```
[AGG-SW1] DHCP enable
[AGG-SW1] DHCPv6 pool pool1
[AGG-SW1-dhcpv6-pool-pool1] address prefix 2001:db8:10::/64
[AGG-SW1-dhcpv6-pool-pool1] excluded-address 2001:db8:10::1
[AGG-SW1-dhcpv6-pool-pool1] quit
[AGG-SW1] interface Vlanif11
[AGG-SW1-Vlanif11] DHCPv6 server pool1
[AGG-SW1-Vlanif11] undo ipv6 nd ra halt
[AGG-SW1-Vlanif11] ipv6 nd autoconfig managed-address-flag
[AGG-SW1-Vlanif11] ipv6 nd autoconfig other-flag
[AGG-SW1-Vlanif11] ipv6 nd ra prefix default no-advertise
[AGG-SW1-Vlanif11] quit
```

在 ACC-SW1 上开启 ND-Snooping，在 VLAN11 内使能 ND Snooping 功能，配置接口 GE0/0/1 为 ND Snooping 信任接口，使能自动探测 ND Snooping 动态绑定表项对应用户的在线状态功能，并配置发送 NS 探测报文的探测次数，探测时间间隔和允许学习 ND Snooping 动态绑定表项的最大个数。

```
[ACC-SW1] nd snooping enable
[ACC-SW1] vlan 11
[ACC-SW1-vlan11] nd snooping enable
[ACC-SW1-vlan11] quit
[ACC-SW1] interface gigabitethernet 0/0/1
[ACC-SW1-GE0/0/1] nd snooping trusted
[ACC-SW1-GE0/0/1] quit
[ACC-SW1] nd user-bind detect enable
[ACC-SW1] nd user-bind detect retransmit 5 interval 600
[ACC-SW1] nd snooping max-user-number 200
```

步骤 3 配置 OSPFv3

在 AGG1-SW1 上开启 OSPFv3 功能，命令如下。

```
[AGG-SW1] ospfv3
[AGG-SW1-ospfv3-1] router-id 3.3.3.3
[AGG-SW1-ospfv3-1] quit
[AGG-SW1] interface Vlanif11
[AGG-SW1-Vlanif11] ospfv3 1 area 0.0.0.1
[AGG-SW1-Vlanif11] quit
[AGG-SW1] interface Vlanif58
[AGG-SW1-Vlanif58] ospfv3 1 area 0.0.0.0
```

```
[AGG-SW1-Vlanif58] quit
[AGG-SW1]interface Vlanif70
[AGG-SW1-Vlanif70] ospfv3 1 area 0.0.0.0
[AGG-SW1-Vlanif70] quit
```

在 Core-R1 上开启 OSPFv3 功能，命令如下。

```
[Core-R1] ospfv3
[Core-R1-ospfv3-1] router-id 11.11.11.11
[Core-R1-ospfv3-1] quit
[Core-R1] interface GE 0/0/2
[Core-R1-GE0/0/2] ospfv3 1 area 0.0.0.0
[Core-R1-GE0/0/2] quit
[Core-R1] interface GE 0/0/3
[Core-R1-GE0/0/3] ospfv3 1 area 0.0.0.0
[Core-R1-GE0/0/3] quit
[Core-R1] interface GE 0/0/5
[Core-R1-GE0/0/5] ospfv3 1 area 0.0.0.0
[Core-R1-GE0/0/5] quit
```

在 Core-R2 上开启 OSPFv3 功能，命令如下。

```
[Core-R2] ospfv3
[Core-R2-ospfv3-1] router-id 12.12.12.12
[Core-R2-ospfv3-1] quit
[Core-R2] interface GE 0/0/2
[Core-R2-GE0/0/2] ospfv3 1 area 0.0.0.0
[Core-R2-GE0/0/2] quit
[Core-R2] interface GE 0/0/3
[Core-R2-GE0/0/3] ospfv3 1 area 0.0.0.0
[Core-R2-GE0/0/3] quit
[Core-R2] interface GE 0/0/5
[Core-R2-GE0/0/5] ospfv3 1 area 0.0.0.0
[Core-R2-GE0/0/5] quit
```

在 DC-FW 上开启 OSPFv3 功能，命令如下。

```
[DC-FW] ospfv3
[DC-FW-ospfv3-1] router-id 23.23.23.23
[DC-FW-ospfv3-1] quit
[DC-FW] int g0/0/1
[DC-FW-GE0/0/1] ospfv3 1 area 0.0.0.0
[DC-FW-GE0/0/1] int g0/0/2
[DC-FW-GE0/0/2] ospfv3 1 area 0.0.0.0
[DC-FW-GE0/0/2] quit
```

在 AGG-SW1 与 Core-R1，Core-R2 的相连接口开启 OSPFv3 认证，认证算法为 HMAC-SHA256，密码为 Huawei@123，配置命令如下。

AGG-SW1

```
[AGG-SW1] interface Vlanif58
[AGG-SW1-Vlanif58] ospfv3 authentication-mode hmac-sha256 key-id 10 cipher Huawei@123
```

```
[AGG-SW1-Vlanif58] quit
[AGG-SW1] interface Vlanif70
[AGG-SW1-Vlanif70] ospfv3 authentication-mode hMAC-sha256 key-id 10 cipher Huawei@123
[AGG-SW1-Vlanif70] quit
```

Core-R1

```
[Core-R1] interface GE 0/0/3
[Core-R1-GE0/0/3] ospfv3 authentication-mode hMAC-sha256 key-id 10 cipher Huawei@123
[Core-R1-GE0/0/3] quit
```

Core-R2

```
[Core-R2] interface GE 0/0/3
[Core-R2-GE0/0/3] ospfv3 authentication-mode hMAC-sha256 key-id 10 cipher Huawei@123
[Core-R2-GE0/0/3] quit
```

步骤 4 配置 NAT64

在 DC-FW 设备上开启 NAT64 功能。

```
[DC-FW] nat64 enable
[DC-FW] int g0/0/1
[DC-FW-GE0/0/1] nat64 enable
[DC-FW-GE0/0/1] int g0/0/2
[DC-FW-GE0/0/2] nat64 enable
[DC-FW-GE0/0/2] quit
```

在 DC-FW 设备上配置安全策略，放行 IPv6 用户访问数据中心的业务流量。

```
[DC-FW] security-policy
[DC-FW-policy-security] rule name nat64
[DC-FW-policy-security-rule-nat64] source-zone untrust
[DC-FW-policy-security-rule-nat64] destination-zone dmz
[DC-FW-policy-security-rule-nat64] source-address 2001:db8:10:: 64
[DC-FW-policy-security-rule-nat64] action permit
[DC-FW-policy-security-rule-nat64] quit
[DC-FW-policy-security] quit
```

在 DC-FW 设备上配置 NAT64 前缀为 “2001:db8::/96”。

```
[DC-FW] nat64 prefix 2001:db8:: 96
```

在 DC-FW 设备上配置 NAT64 映射策略。

```
[DC-FW] nat-policy
[DC-FW-policy-nat] rule name nat64
[DC-FW-policy-nat-rule-nat64] source-zone untrust
[DC-FW-policy-nat-rule-nat64] destination-zone dmz
[DC-FW-policy-nat-rule-nat64] source-address 2001:db8:10:: 64
[DC-FW-policy-nat-rule-nat64] egress-interface g0/0/0
[DC-FW-policy-nat-rule-nat64] nat-type nat64
[DC-FW-policy-nat-rule-nat64] action source-nat easy-ip
[DC-FW-policy-nat-rule-nat64] quit
```


因 DC-FW 设备上配置的 NAT64 前缀并没有配置在 OSPFv3 中，所以需要在 AGG-SW1、Core-R1 和 Core-R2 设备上配置针对 NAT64 前缀的回程静态路由。

AGG-SW1

```
[AGG-SW1] ipv6 route-static 2001:DB8:: 96 2001:DB8:30::2 preference 70
[AGG-SW1] ipv6 route-static 2001:DB8:: 96 2001:DB8:20::2
```

Core-R1

```
[Core-R1] ipv6 route-static 2001:DB8:: 96 2001:DB8:50::2
```

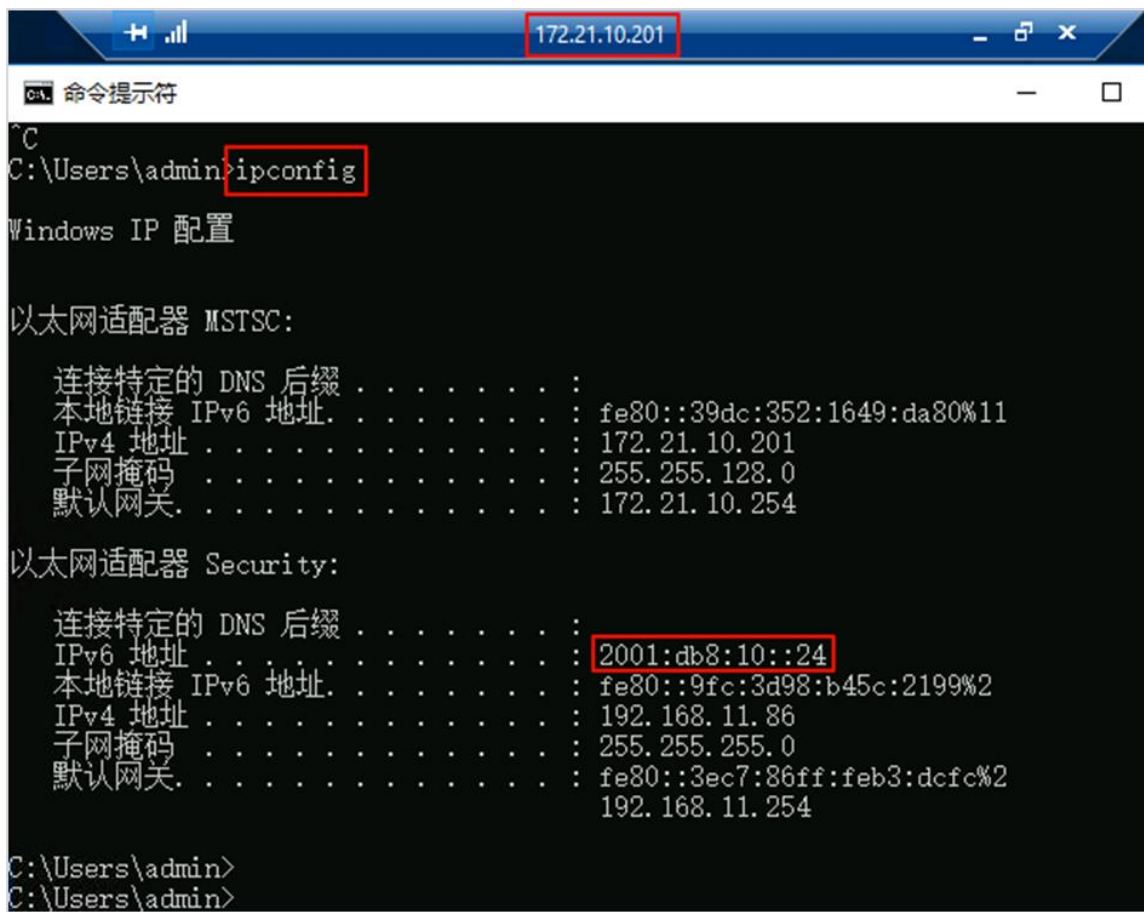
Core-R2

```
[Core-R2] ipv6 route-static 2001:DB8:: 96 2001:DB8:60::2
```

7.3 结果验证

7.3.1 IPv6 终端地址获取情况

使用 RDP 登录 PC1 (地址: 172.21.10.201, 账号: admin/Huawei123!), 打开命令行并键入 “ipconfig” 查看 IPv6 地址的获取情况:



```

C:\Users\admin>ipconfig

Windows IP 配置

以太网适配器 MSTSC:

    连接特定的 DNS 后缀 . . . . . : 
    本地连接 IPv6 地址. . . . . : fe80::39dc:352:1649:da80%11
    IPv4 地址 . . . . . : 172.21.10.201
    子网掩码 . . . . . : 255.255.128.0
    默认网关. . . . . : 172.21.10.254

以太网适配器 Security:

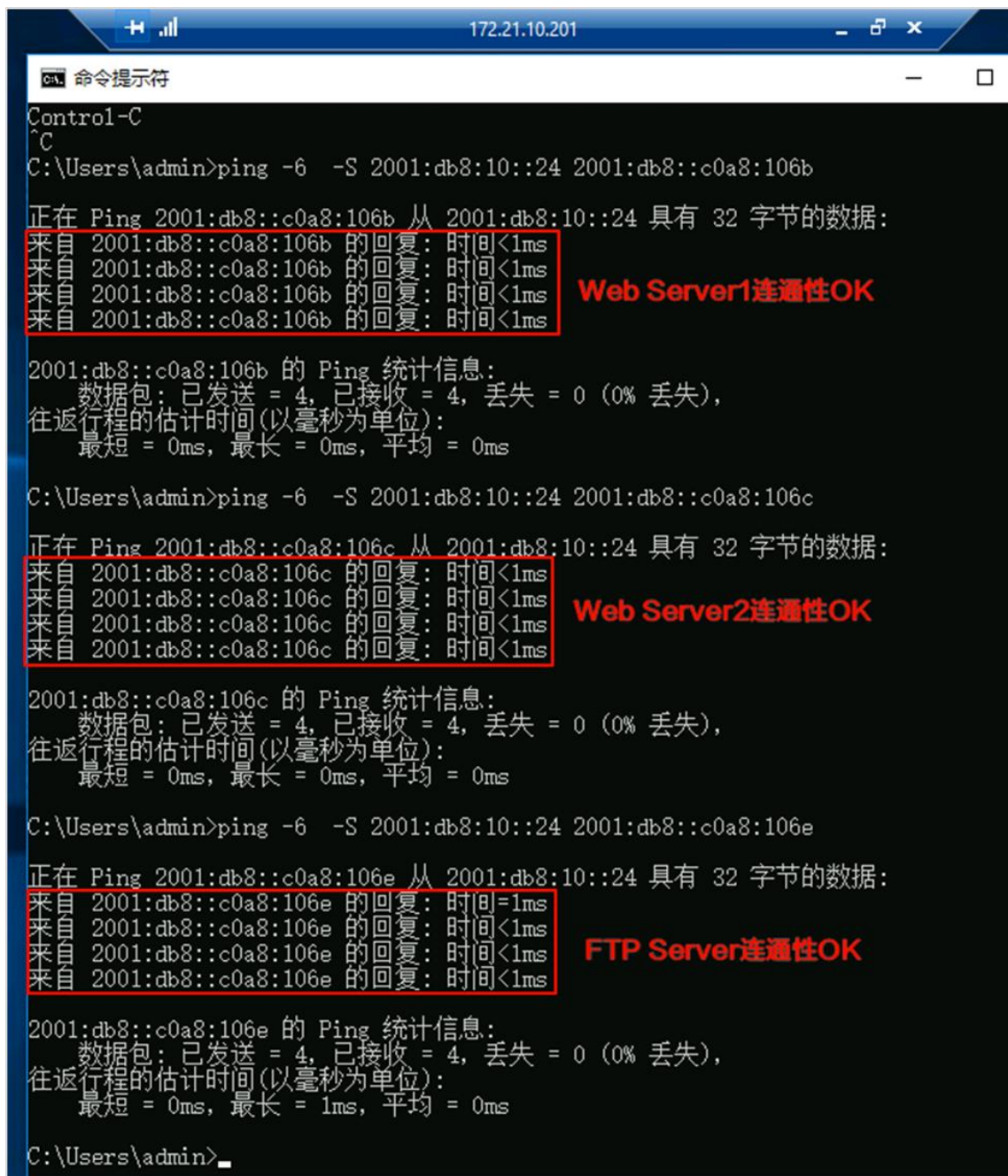
    连接特定的 DNS 后缀 . . . . . : 
    IPv6 地址 . . . . . : 2001:db8:10::24
    本地连接 IPv6 地址. . . . . : fe80::9fc:3d98:b45c:2199%2
    IPv4 地址 . . . . . : 192.168.11.86
    子网掩码 . . . . . : 255.255.255.0
    默认网关. . . . . : fe80::3ec7:86ff:feb3:dcfc%2
                        192.168.11.254

C:\Users\admin>
C:\Users\admin>
  
```

图7-2 PC1 终端 IPv6 地址获取情况

7.3.2 NAT64 业务联通性测试

使用 RDP 登录 PC1 (地址: 172.21.10.201, 账号: admin/Huawei123!), 打开命令行, 进行 NAT64 业务连通性测试, 效果如下:



```

Control-C
^C
C:\Users\admin>ping -6 -S 2001:db8:10::24 2001:db8::c0a8:106b

正在 Ping 2001:db8::c0a8:106b 从 2001:db8:10::24 具有 32 字节的数据:
来自 2001:db8::c0a8:106b 的回复: 时间<1ms
来自 2001:db8::c0a8:106b 的回复: 时间<1ms
来自 2001:db8::c0a8:106b 的回复: 时间<1ms
来自 2001:db8::c0a8:106b 的回复: 时间<1ms
2001:db8::c0a8:106b 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 0ms, 最长 = 0ms, 平均 = 0ms
C:\Users\admin>ping -6 -S 2001:db8:10::24 2001:db8::c0a8:106c

正在 Ping 2001:db8::c0a8:106c 从 2001:db8:10::24 具有 32 字节的数据:
来自 2001:db8::c0a8:106c 的回复: 时间<1ms
来自 2001:db8::c0a8:106c 的回复: 时间<1ms
来自 2001:db8::c0a8:106c 的回复: 时间<1ms
来自 2001:db8::c0a8:106c 的回复: 时间<1ms
2001:db8::c0a8:106c 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 0ms, 最长 = 0ms, 平均 = 0ms
C:\Users\admin>ping -6 -S 2001:db8:10::24 2001:db8::c0a8:106e

正在 Ping 2001:db8::c0a8:106e 从 2001:db8:10::24 具有 32 字节的数据:
来自 2001:db8::c0a8:106e 的回复: 时间=1ms
来自 2001:db8::c0a8:106e 的回复: 时间<1ms
来自 2001:db8::c0a8:106e 的回复: 时间<1ms
来自 2001:db8::c0a8:106e 的回复: 时间<1ms
2001:db8::c0a8:106e 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 0ms, 最长 = 1ms, 平均 = 0ms
C:\Users\admin>
  
```

Web Server1连通性OK

Web Server2连通性OK

FTP Server连通性OK

图7-3 NAT64 业务连通性测试

7.4 配置参考（仅展示本实验相关配置）

7.4.1 DC-FW 的配置

```
#
ospfv3 1
 router-id 23.23.23.23
 area 0.0.0.0
#
interface GE0/0/1
 ipv6 enable
 ip address 192.168.10.41 255.255.255.252
 ipv6 address 2001:DB8:50::2/64
 ospfv3 1 area 0.0.0.0
 service-manage ping permit
 nat64 enable
#
interface GE0/0/2
 ipv6 enable
 ip address 192.168.10.45 255.255.255.252
 ipv6 address 2001:DB8:60::2/64
 ospfv3 1 area 0.0.0.0
 service-manage ping permit
 nat64 enable
#
nat64 enable
nat64 prefix 2001:db8:: 96
#
firewall detect ftp
#
security-policy
 rule name nat64
  source-zone untrust
  destination-zone dmz
  source-address 2001:DB8:10:: 64
  action permit
#
nat-policy
 rule name nat64
  source-zone untrust
  destination-zone dmz
  source-address 2001:DB8:10:: 64
  nat-type nat64
  action source-nat easy-ip
```

```
#  
return
```

7.4.2 Core-R1 的配置

```
#  
ipv6  
#  
ospfv3 1  
  router-id 11.11.11.11  
#  
interface GE0/0/2  
  undo portswitch  
  ipv6 enable  
  ip address 192.168.10.53 255.255.255.252  
  ipv6 address 2001:DB8:40::1/64  
  ospfv3 1 area 0.0.0.0  
#  
interface GE0/0/3  
  undo portswitch  
  ipv6 enable  
  ip address 192.168.10.57 255.255.255.252  
  ipv6 address 2001:DB8:20::2/64  
  ospfv3 1 area 0.0.0.0  
  ospfv3 authentication-mode hmac-sha256 key-id 10 cipher Huawei@123  
#  
interface GE0/0/5  
  undo portswitch  
  ipv6 enable  
  ip address 192.168.10.42 255.255.255.252  
  ipv6 address 2001:DB8:50::1/64  
  ospfv3 1 area 0.0.0.0  
#  
ipv6 route-static 2001:DB8:: 96 2001:DB8:50::2  
#  
return
```

7.4.3 Core-R2 的配置

```
#  
ipv6  
#  
ospfv3 1  
  router-id 12.12.12.12  
#  
interface GE0/0/2  
  undo portswitch  
  ipv6 enable  
  ip address 192.168.10.54 255.255.255.252
```

```
ipv6 address 2001:DB8:40::2/64
ospfv3 1 area 0.0.0.0
#
interface GE0/0/3
undo portswitch
ipv6 enable
ip address 192.168.10.69 255.255.255.252
ipv6 address 2001:DB8:30::2/64
ospfv3 1 area 0.0.0.0
ospfv3 authentication-mode hmac-sha256 key-id 10 cipher Huawei@123
#
interface GE0/0/5
undo portswitch
ipv6 enable
ip address 192.168.10.46 255.255.255.252
ipv6 address 2001:DB8:60::1/64
ospfv3 1 area 0.0.0.0
#
ipv6 route-static 2001:DB8::96 2001:DB8:60::2
#
return
```

7.4.4 AGG-SW1 的配置

```
#
ipv6
#
dhcp enable
#
nd snooping enable
#
dhcpv6 pool pool1
address prefix 2001:DB8:10::/64
excluded-address 2001:DB8:10::1
#
ospfv3 1
router-id 3.3.3.3
#
interface Vlanif11
ipv6 enable
ip address 192.168.11.254 255.255.255.0
ipv6 address 2001:DB8:10::1/64
ipv6 nd ra prefix default no-advertise
undo ipv6 nd ra halt
ipv6 nd autoconfig managed-address-flag
ipv6 nd autoconfig other-flag
ospfv3 1 area 0.0.0.1
dhcp select interface
```

```
dhcpv6 server pool1
dhcp server gateway-list 192.168.11.254
#
interface Vlanif58
ipv6 enable
ip address 192.168.10.58 255.255.255.252
ipv6 address 2001:DB8:20::1/64
ospfv3 1 area 0.0.0.0
ospfv3 authentication-mode hmac-sha256 key-id 10 cipher Huawei@123
#
interface Vlanif70
ipv6 enable
ip address 192.168.10.70 255.255.255.252
ipv6 address 2001:DB8:30::1/64
ospfv3 1 area 0.0.0.0
ospfv3 authentication-mode hmac-sha256 key-id 10 cipher Huawei@123
#
interface GE0/0/1
port link-type access
port default vlan 58
#
interface GE0/0/2
port link-type access
port default vlan 70
#
interface GE0/0/3
port link-type access
port default vlan 11
#
ipv6 route-static 2001:DB8:: 96 2001:DB8:30::2 preference 70
ipv6 route-static 2001:DB8:: 96 2001:DB8:20::2
#
return
```

7.4.5 ACC-SW1 的配置

```
#
nd snooping enable
nd user-bind detect enable
nd user-bind detect retransmit 5 interval 600
nd snooping max-user-number 200
#
vlan 11
nd snooping enable
#
interface GE0/0/1
port link-type access
port default vlan 11
```

```
nd snooping trusted  
#  
return
```

7.5 思考题

DC-FW 设备 OSPFv3 协议建立邻居关系的时候,使用的是 2001:db8:50::/64 和 2001:db8:60::/64 地址段的地址吗? 如果不是, OSPFv3 协议建立邻居关系使用的是哪种地址? 若需配置安全策略放行 OSPFv3 交互报文, 则安全策略中的源目 IP 地址应该如何匹配?

答案: 不是, 使用 link-local 类型的 IPv6 地址建立 OSPFv3 邻居, 安全策略中应该匹配的是 link-local 的 IPv6 地址。

8

防火墙内容安全实验

8.1 实验介绍

8.1.1 关于本实验

企业总部数据中心中部署有 Web 和 FTP 服务器提供服务，为保证内外网用户访问服务器的安全性，需要在企业总部出口防火墙 HQ-FW 设备及数据中心边界防火墙 DC-FW 设备上部署内网安全过滤技术，对员工业务流量进行精细化安全管控。

8.1.2 实验组网介绍

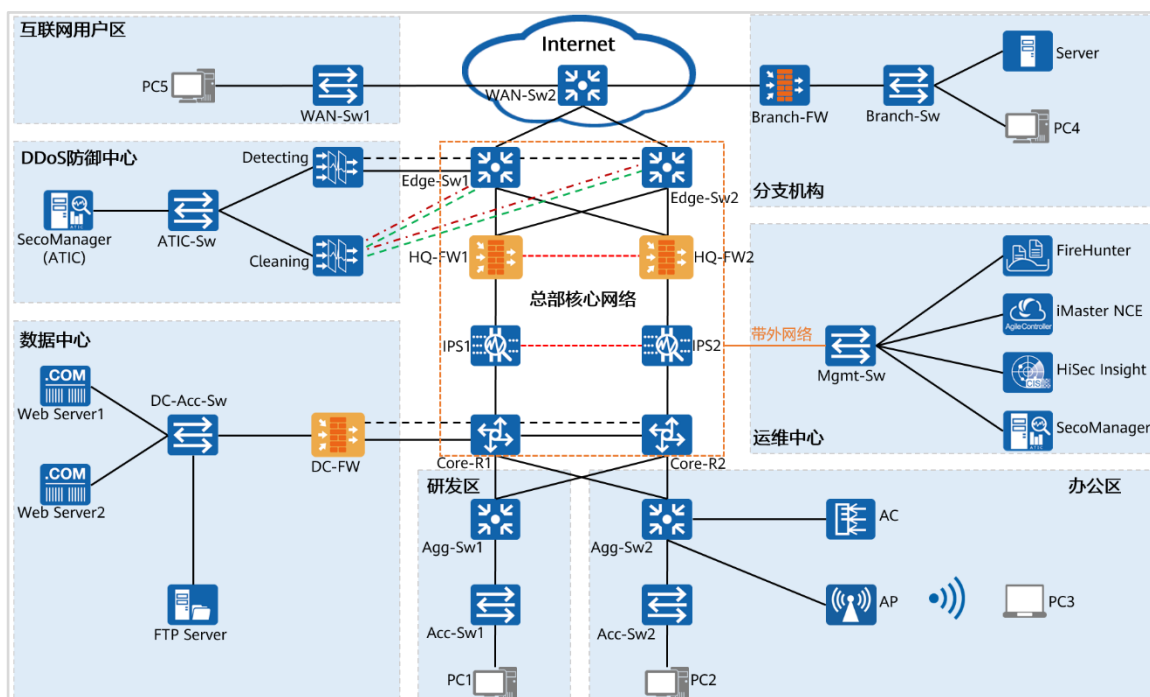


图8-1 实验拓扑图

8.1.3 实验规划

1. 在出口防火墙 HQ-FW 设备上部署内容过滤，阻断用户使用 FTP 以表格文件形式上传或下载任何有关身份证号、银行卡号以及包含关键字“Huawei”相关的信息。
2. 在数据中心边界防火墙 DC-FW 设备上部署 URL 过滤技术，阻断员工访问任何以“URL_Filter”结尾的 URL。

8.2 实验配置任务

8.2.1 配置思路

内容过滤配置思路：

1. 创建关键字组，将身份证号、银行卡号以及“Huawei”关键字定义为一个关键字组。
2. 创建内容过滤配置文件，并调用刚才创建的关键字组。
3. 在业务安全策略中调用内容过滤配置文件。
4. 提交内容过滤配置。

URL 过滤配置思路：

1. 创建 URL 过滤配置文件，将以“URL_Filter”结尾的 URL 放在黑名单。
2. 设置 URL 过滤级别为“高”。
3. 在业务安全策略中调用刚才创建的 URL 过滤配置文件。
4. 提交 URL 过滤配置。

8.2.2 配置步骤（内容过滤）

步骤 1 创建关键字组

登录 HQ-FW1 设备 Web 管理界面（地址：<https://172.21.10.21:8443/>，账号：Webuser/Admin@123），选择“对象 > 关键字组 > 新建”，进入关键字组的创建界面，执行以下操作：

新建关键字组

* 关键字组名称

关键字信息 ①

☐	关键字名称	匹配模式	文本/正则表达式	区分大小写	权重
☐	银行卡号	正则表达式			1
☐	身份证号	正则表达式			1

删除 新建

图8-2 创建关键字组（1）



新建关键字组

* 关键字组名称: word

关键字信息 ①

☐	关键字名称	匹配模式	文本/正则表达式	区分大小写
☐	银行卡号	正则表达式		
☐	身份证号	正则表达式		

删除 新建

新建自定义关键字

添加信用卡号关键字

添加社会安全号关键字

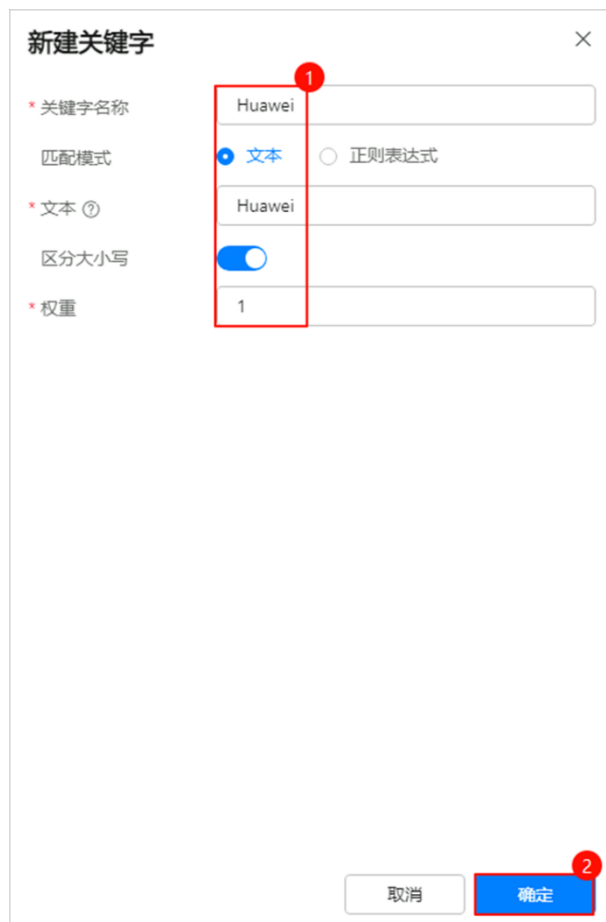
添加机密关键字

添加中国移动手机号关键字

添加中国联通手机号关键字

添加中国电信手机号关键字

图8-3 创建关键字组（2）



新建关键字

* 关键字名称: Huawei

匹配模式: ☒ 文本 ☐ 正则表达式

* 文本 ②: Huawei

区分大小写: ☒

* 权重: 1

取消 确定

图8-4 创建关键字组（3）

新建关键字组

* 关键字组名称

word

关键字信息

删除

新建

☐	关键字名称	匹配模式	文本/正则表达式	区分大小写	权重
☐	银行卡号	正则表达式			1
☐	身份证号	正则表达式			1
☐	Huawei	文本	Huawei	是	1

共 3 条

取消

确定

图8-5 创建关键字组（4）

步骤 2 创建内容过滤配置文件

继续在 HQ-FW1 设备 Web 管理界面选择“对象 > 安全配置文件 > 内容过滤 > 新建”，进入内容过滤配置文件创建界面，执行以下操作：

新建内容过滤配置文件

* 名称

Content_Filter

内容过滤规则

删除

新建

☐	规则名称	关键字组	应用	文件类型	方向	动作	告警阈值	阻断阈值
没有记录								

图8-6 创建内容过滤配置文件（1）

新建内容过滤规则

* 规则名称

Rule1

* 关键字组

word

* 应用

FTP

* 文件类型

XLSX XLS

方向

☐ 上传
☐ 下载
☒ 双向

动作

☐ 告警
☒ 阻断
☐ 按权重累计阈值

取消

确定

图8-7 创建内容过滤配置文件（2）

新建内容过滤配置文件

* 名称

Content_Filter

内容过滤规则

删除

新建

☐	规则名称	关键字组	应用	文件类型	方向	动作	告警阈值	阻断阈值
☐	Rule1	word	FTP	XLSX XLS	双向	阻断	-	-

共 1 条

取消

确定

图8-8 创建内容过滤配置文件（3）

步骤 3 调用内容过滤配置文件

继续在 HQ-FW1 设备 Web 管理界面选择“策略 > 安全策略 > 安全策略”，进入安全策略界面，选择业务相关的安全策略“ipsec_oa”和“sslvpn_oa”进行二次编辑，调用刚才创建的内容过滤配置文件，以“ipsec_oa”安全策略为例演示操作流程：

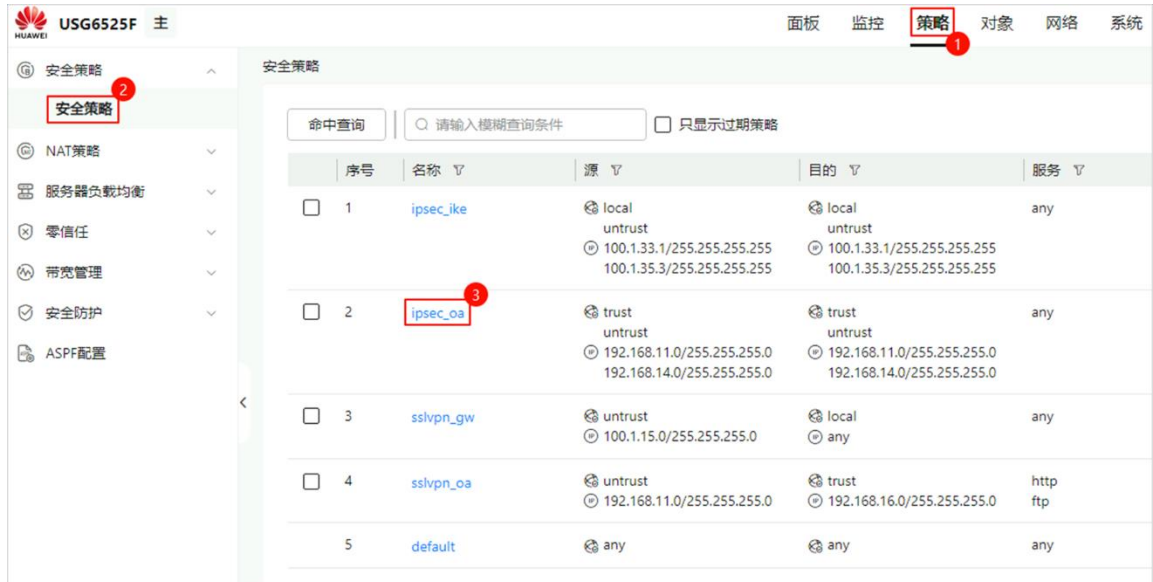


图8-9 进入“ipsec_oa”安全策略编辑界面

修改安全策略

×

概述

* 名称

ipsec_oa

描述

策略组

-- NONE --

条件

ⓘ 当前未加载地区识别特征库。如需配置地区，请[加载地区识别特征库](#)

源

安全区域

trust ×

untrust ×

IP 地址/地区 ⓘ

192.168.11.0... ×

192.168.14.0... ×

目的

1↓

目的类型

☒ 安全区域

☐ 虚拟服务

安全区域

trust ×

untrust ×

IP 地址/地区 ⓘ

192.168.11.0... ×

192.168.14.0... ×

服务 ⓘ

协议

any

更多 ▾

应用/用户/安全组/时间段/VLAN ID

动作

动作

☒ 允许

☐ 禁止

内容安全检查 ⓘ

ⓘ 引用安全配置文件会导致设备性能一定程度的下降。

反病毒

-- NONE --

入侵防御

-- NONE --

URL过滤

-- NONE --

内容过滤

Content_Filter

其他

取消

命令预览

确定

图8-10 调用内容过滤配置文件

使用同样方式在“sslvpn_oa”安全策略中同样调用之前创建的内容过滤配置文件，完成后效果如下：

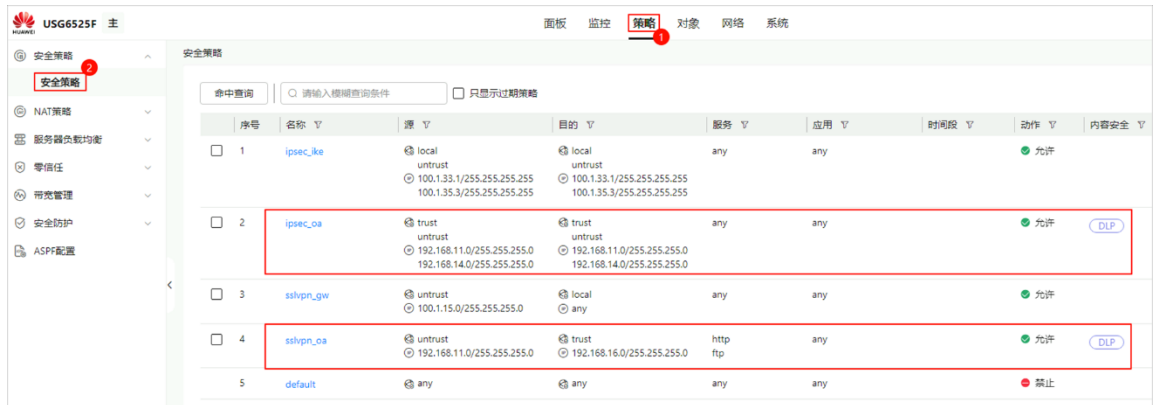


图8-11 内容过滤配置文件调用概览

步骤 4 提交配置（内容过滤）

在 HQ-FW1 设备 Web 管理界面右上角点击配置提交按钮，完成内容过滤相关配置的提交。

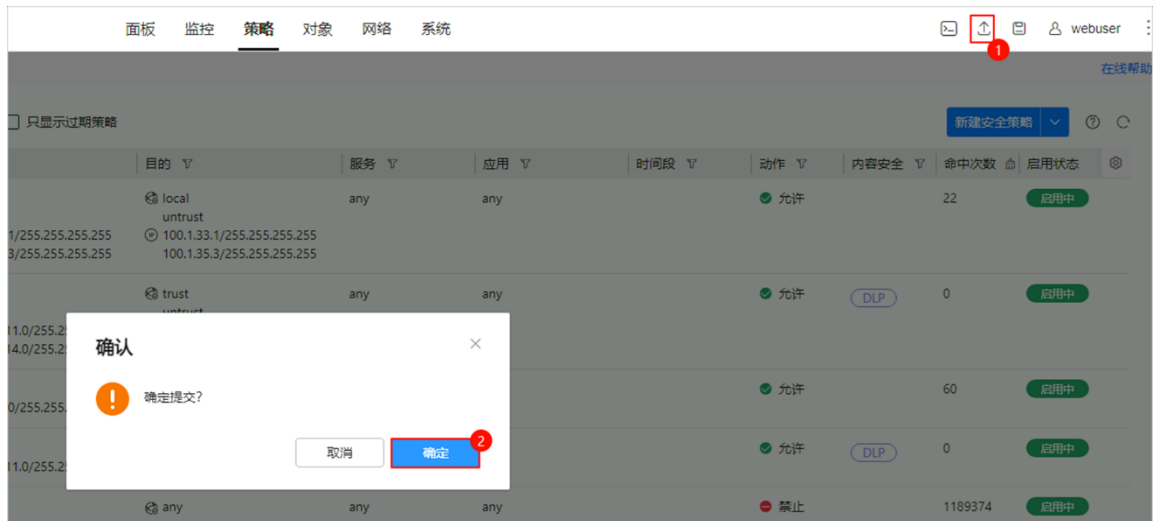


图8-12 提交内容过滤配置



图8-13 配置提交成功

8.2.3 配置步骤（URL 过滤）

步骤 1 创建 URL 过滤配置文件

登录 DC-FW 设备 Web 管理界面（地址：https://172.21.10.23:8443/，账号：Webuser/Admin@123），选择“对象 > 安全配置文件 > URL 过滤 > 新建”，进入 URL 过滤配置文件创建界面，执行以下操作：

新建URL过滤配置文件

* 名称: URL_Filter

缺省动作: 允许

加密流量过滤: ☐ 启用该功能后，可以对不解密的HTTPS流量进行URL过滤。

类型	白名单	黑名单
URL	白名单的优先级高于黑名单	* /URL_Filter
Host	白名单的优先级高于黑名单	白名单的优先级高于黑名单

URL过滤级别

☒ 高: 对所有成人网站，非法活动，社交网络，视频共享等网站进行严格的限制。

☐ 中: 对所有成人网站和非法网站进行控制。

取消 确定

图8-14 创建 URL 过滤配置文件

步骤 2 调用 URL 过滤配置文件

继续在 DC-FW 设备 Web 管理界面选择“策略 > 安全策略 > 安全策略”，进入安全策略界面，选择业务相关的安全策略“sslvpn_oa”、“nat64”和“slb”进行二次编辑，调用刚才创建的 URL 过滤配置文件，以“sslvpn_oa”安全策略为例演示操作流程：

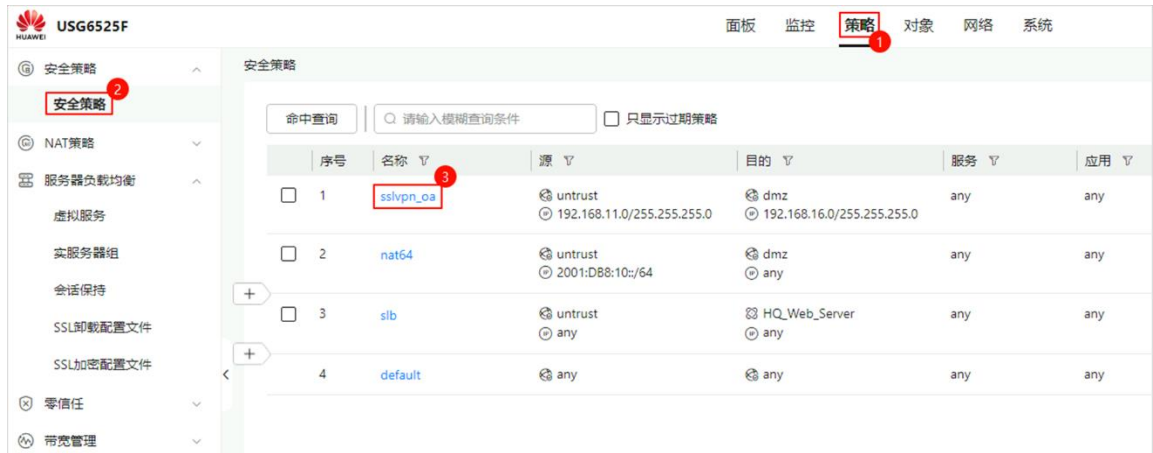


图8-15 进入“sslvpn_oa”安全策略编辑页面

修改安全策略

概述

名称

sslvpn_oa

描述

策略组

-- NONE --

条件

当前未加载地区识别特征库。如需配置地区，请[加载地区识别特征库](#)

源

安全区域

untrust

IP 地址/地区

192.168.11.0...

目的

目的类型

安全区域

虚拟服务

安全区域

dmz

IP 地址/地区

192.168.16.0...

服务

协议

any

更多

应用/用户/安全组/时间段/VLAN ID

动作

动作

允许

禁止

内容安全检查

引用安全配置文件会导致设备性能一定程度的下降。

反病毒

-- NONE --

入侵防御

-- NONE --

URL过滤

URL_Filter

内容过滤

-- NONE --

取消

命令预览

确定

图8-16 调用 URL 过滤配置文件

使用同样方式在“nat64”和“slb”安全策略中同样调用之前创建的 URL 过滤配置文件，完成后效果如下

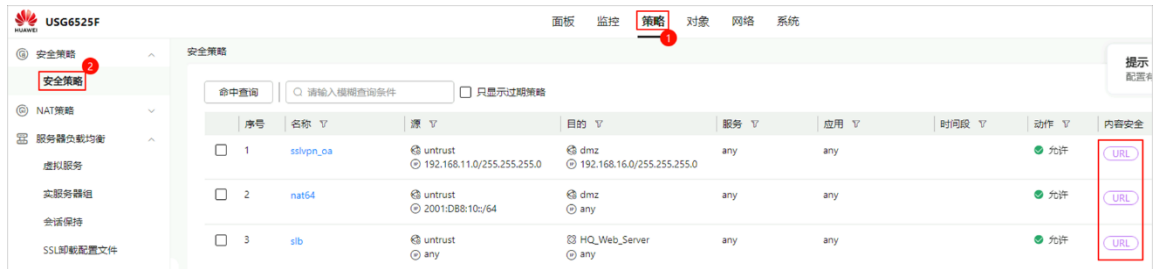


图8-17 URL 过滤配置文件调用概览

步骤 3 提交配置（URL 过滤）

在提交配置之前，为对比实验结果，可以先通过 RDP 登录 PC1（地址：172.21.10.201，账号：admin/Huawei123!），打开浏览器访问黑名单内的 URL“http://192.168.16.109/URL_Filter”，效果如下（此步骤可选）：

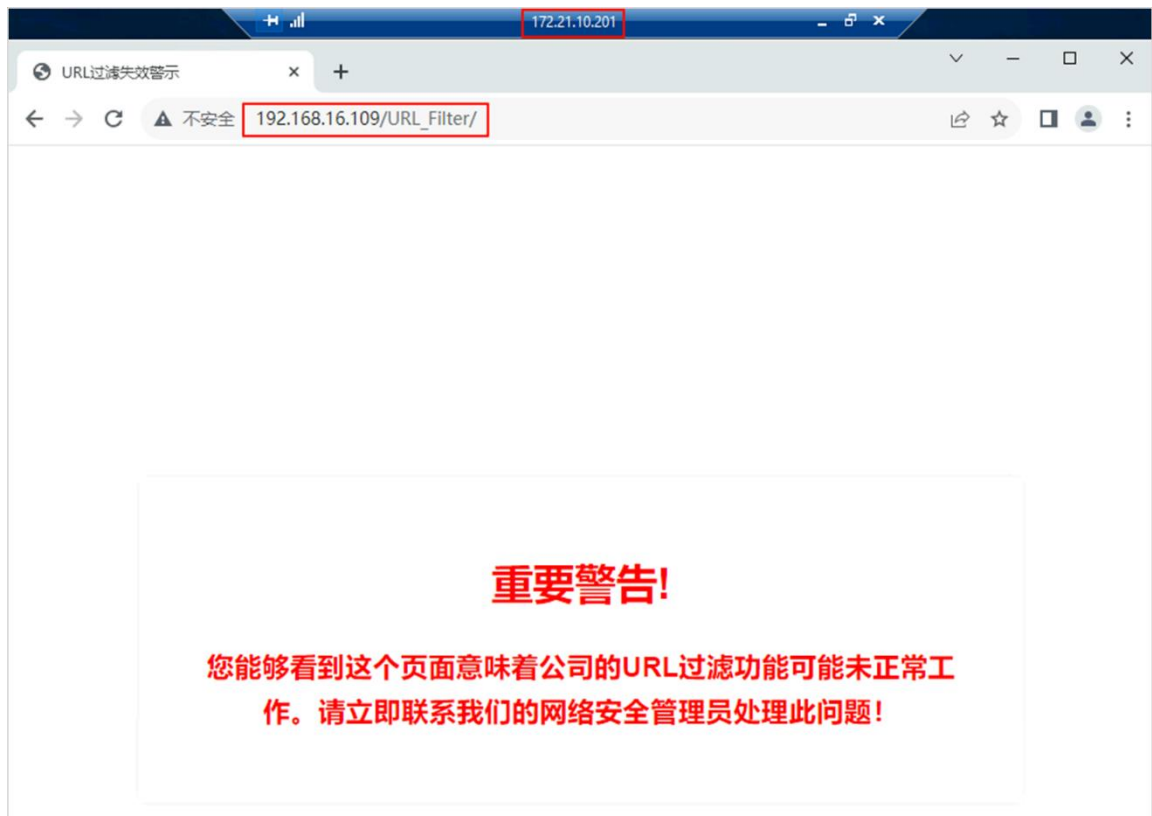


图8-18 PC1 访问黑名单 URL（URL 过滤配置提交前）

在 HQ-FW1 设备 Web 管理界面右上角点击配置提交按钮，完成 URL 过滤相关配置的提交。

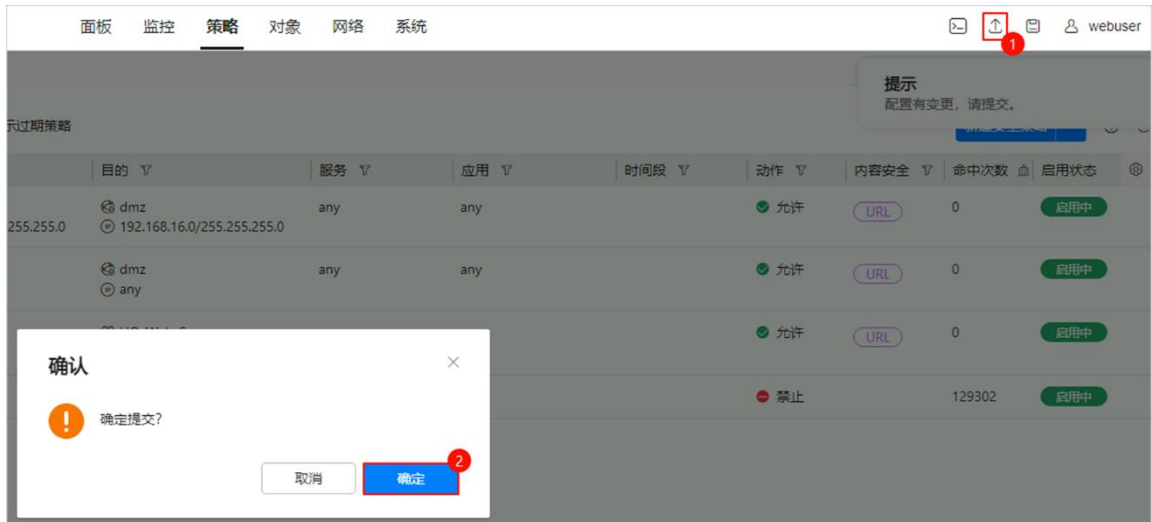


图8-19 提交 URL 过滤配置

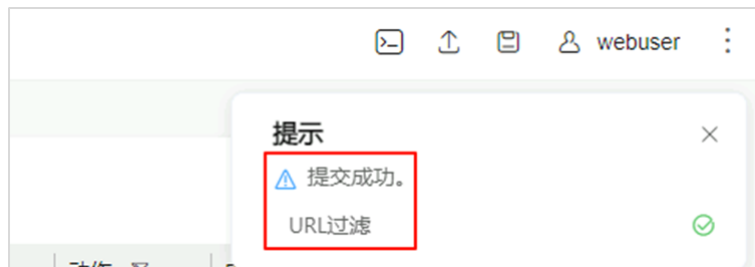


图8-20 配置提交成功

8.3 结果验证

8.3.1 内容过滤验证

使用 RDP 登录 PC5 (地址: 172.21.10.205, 账号: admin/Huawei123!), 在成功接入 SSL VPN 后, 打开资源管理器访问企业总部 FTP 服务器, 并将桌面上“内容过滤测试文件.xlsx”上传至企业总部 FTP 服务器:

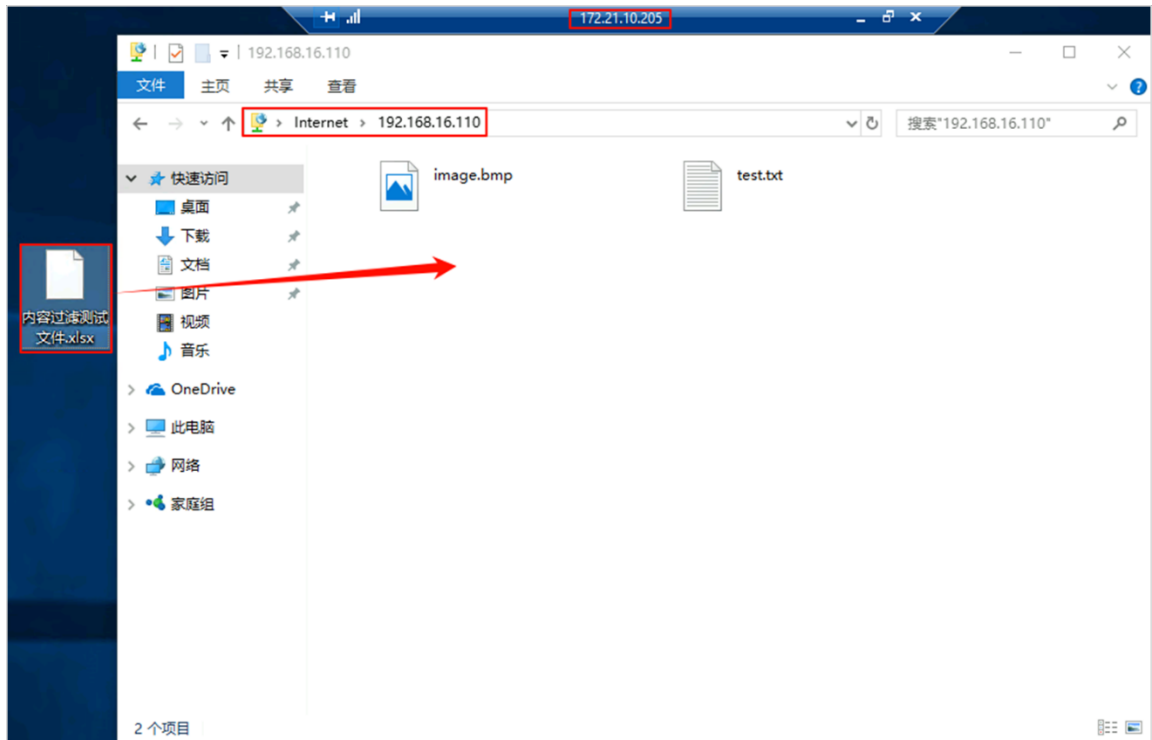


图8-21 PC5 上传内容过滤文件

执行完文件上传后, 登录 HQ-FW1 设备 Web 管理界面(地址: <https://172.21.10.21:8443/>, 账号: Webuser/Admin@123), 选择“监控 > 日志 > 内容日志”, 可以看到刚才的文件上传行为已触发了内容过滤的配置文件, 文件上传已被阻断:



图8-22 HQ-FW1 内容日志查看

8.3.2 URL 过滤验证

通过 RDP 登录 PC1 (地址: 172.21.10.201, 账号: admin/Huawei123!), 打开浏览器访问黑名单内的 URL “http://192.168.16.109/URL_Filter”, 效果如下:

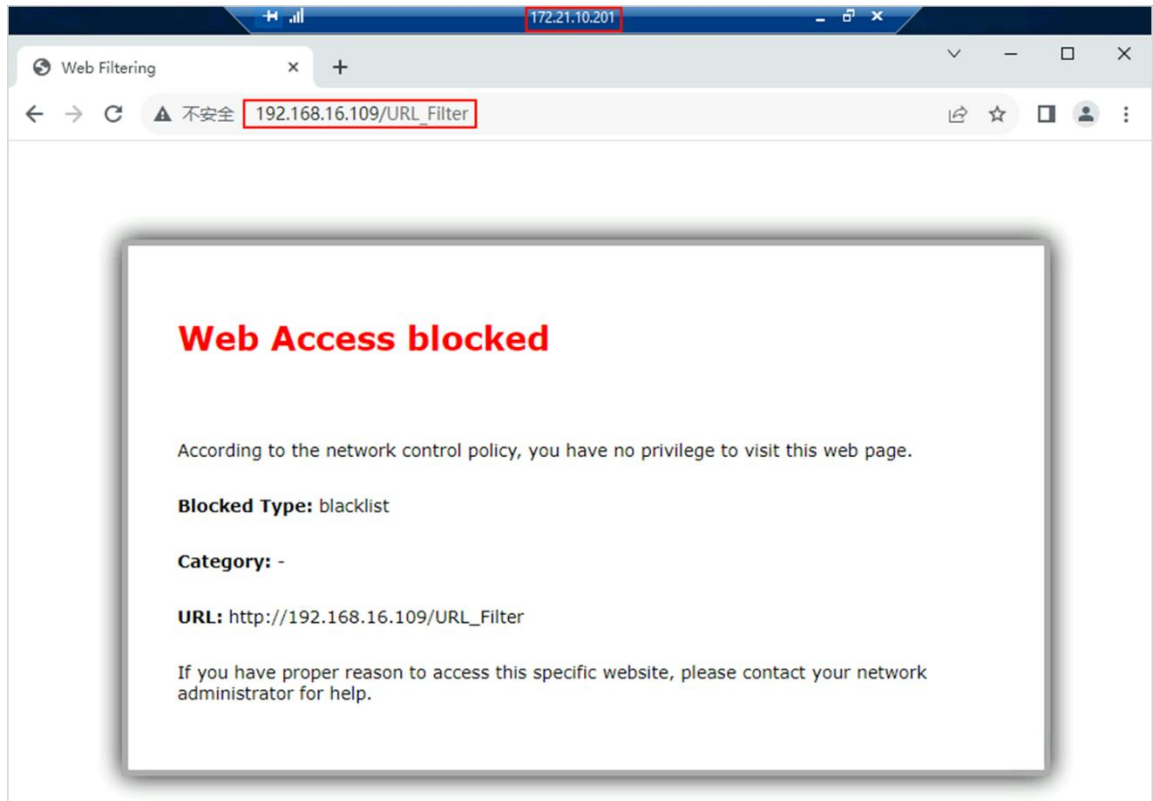


图8-23 PC1 访问黑名单 URL

8.4 配置参考（仅展示本实验相关配置）

8.4.1 HQ-FW1 的配置

```
#
security-policy
rule name ipsec_oa
source-zone trust
source-zone untrust
destination-zone trust
destination-zone untrust
source-address 192.168.11.0 mask 255.255.255.0
source-address 192.168.14.0 mask 255.255.255.0
destination-address 192.168.11.0 mask 255.255.255.0
destination-address 192.168.14.0 mask 255.255.255.0
profile data-filter Content_Filter
action permit
rule name sslvpn_oa
source-zone untrust
destination-zone trust
source-address 192.168.11.0 mask 255.255.255.0
destination-address 192.168.16.0 mask 255.255.255.0
```

```
service ftp
service http
profile data-filter Content_Filter
action permit
#
keyword-group name word
pre-defined-keyword name bank-card-number weight 1
pre-defined-keyword name id-card-number weight 1
user-defined-keyword name Huawei
expression match-mode text Huawei
#
profile type data-filter name Content_Filter
rule name Rule1
direction both
keyword-group name word
undo application type http imap nfs pop3 smb smtp
undo file-type name c cpp cxx doc docx h hpp html java ppt pptx txt
action block
#
return
```

8.4.2 DC-FW 的配置

```
#
profile type url-filter name URL_Filter
add blacklist url */url_filter
category pre-defined control-level high
#
security-policy
rule name sslvpn_oa
source-zone untrust
destination-zone dmz
source-address 192.168.11.0 mask 255.255.255.0
destination-address 192.168.16.0 mask 255.255.255.0
profile url-filter URL_Filter
action permit
rule name nat64
source-zone untrust
destination-zone dmz
source-address 2001:DB8:10:: 64
profile url-filter URL_Filter
action permit
rule name slb
source-zone untrust
vserver HQ_Web_Server
profile url-filter URL_Filter
action permit
#
```

8.5 思考题

内容安全除了介绍的 URL 过滤和内容过滤功能外, 还有哪些功能可以使用? 使用场景是什么?

答案:

反病毒 (AV): 反病毒特性用于保护内网的用户和服务端免受病毒威胁。

入侵防御 (IPS): 入侵防御是一种安全机制。设备通过分析网络流量来检测入侵, 并通过一定的响应方式实时地中止入侵行为。

DNS 过滤: DNS (Domain Name System) 过滤可以对用户访问的域名进行控制, 允许或禁止用户访问某些网站, 达到规范上网行为的目的。

文件过滤: 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。

应用行为控制: 应用行为控制功能可以对常见的 HTTP 行为、FTP 行为和 IM 行为进行精细化控制。

云接入安全感知: 云接入安全感知特性用于对企业云应用进行精细化和差异化的控制。

9 入侵防御与反病毒实验

9.1 实验介绍

9.1.1 关于本实验

企业总部网络中部署有 Web 和 FTP 服务器提供网络服务，为保证用户访问服务器的安全性，在总部网络出口防火墙下游部署了 IPS 设备对用户的访问进行检查，若发现入侵行为或者病毒文件，IPS 将阻断访问流量并告警。

9.1.2 实验组网介绍

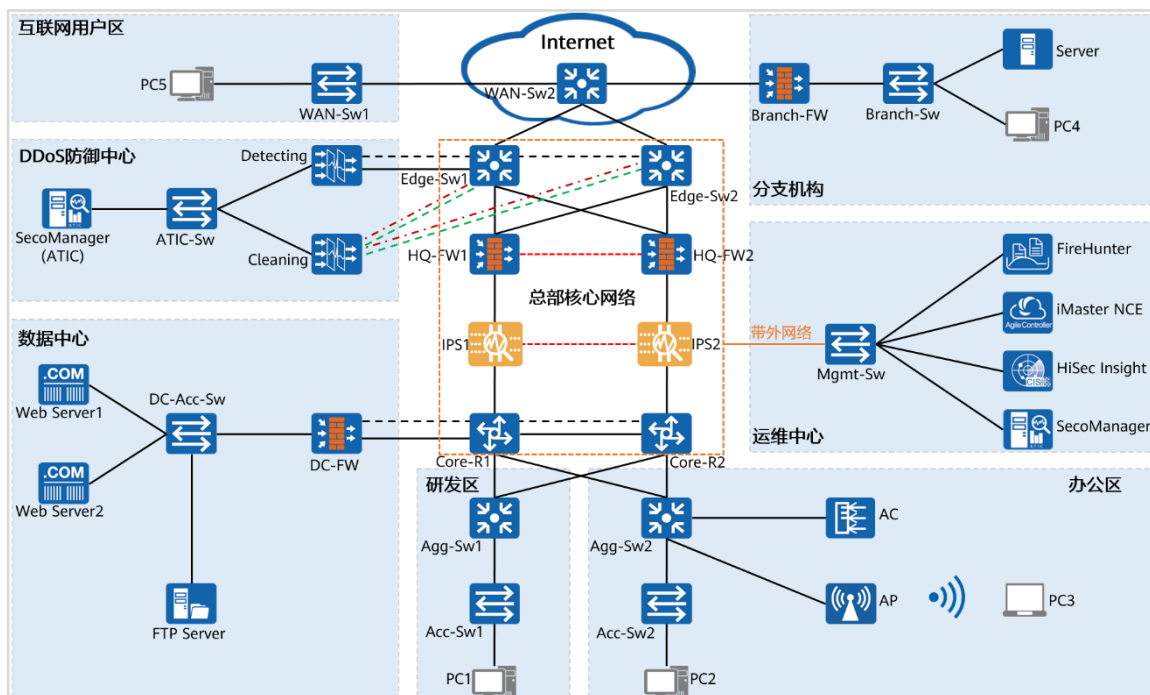


图9-1 实验拓扑图

9.1.3 实验规划

本实验中 IPS 设备以二层透明直路方式部署在防火墙下游，主要用于检测各类网络入侵和病毒攻击并及时阻断，作为防火墙安全策略防护的补充。

华为 IPS 设备支持即插即用，也即默认预设了安全规则，且调用了内容安全配置文件，本身具备了一部分入侵防御及反病毒的能力。

为了使入侵防御和反病毒安全功能更具有针对性，本实验将基于总部出口防火墙的业务安全策略在 IPS 设备上部署相对应的业务安全策略，并合理调用入侵防御配置文件和反病毒配置文件，实现针对性安全防护。

入侵防御部署规划如下：

表9-1 入侵防御配置参数规划

服务器	入侵防御配置	
	配置项	参数
总部Web Server	入侵防御配置文件名	Web_Server
	签名过滤器名	Web_Server
	防御目标操作系统	Windows
	防御协议	网络服务类协议
	威胁类别	木马、广告软件、CGI攻击、跨站脚本攻击、注入攻击、Webshell
	响应动作	阻断
总部FTP Server	入侵防御配置文件名	FTP_Server
	签名过滤器名	FTP_Server
	防御目标操作系统	所有
	防御协议	全部
	威胁类别	全部
	响应动作	阻断

反病毒部署规划如下：

表9-2 反病毒配置参数规划

服务器	反病毒配置	
	配置项	参数
总部Web Server	反病毒配置文件名	Web_Server
	检测协议	HTTP
	检测方向	双向
	检测动作	阻断
总部FTP Server	反病毒配置文件名	FTP_Server
	检测协议	FTP
	检测方向	双向
	检测动作	阻断

9.2 实验配置任务

9.2.1 配置思路

1. 基于总部出口防火墙业务安全策略，在 IPS 设备上部署相应的业务安全策略。
2. 基于规划在 IPS 设备上创建入侵防御配置文件和反病毒配置文件。
3. 在 IPS 业务安全策略中合理调用刚才创建的入侵防御配置文件和反病毒配置文件。
4. 提交配置，使能入侵防御和反病毒配置文件。

9.2.2 配置步骤

步骤 1 配置安全策略

登录 IPS1 设备 Web 管理界面（地址：<https://172.21.10.41:8443/>，账号：Webuser/Admin@123），选择“策略 > 安全策略 > 安全策略 > 新建安全策略”，进入安全策略创建页面，执行以下操作：



图9-2 进入 IPS1 设备安全策略创建界面

新建安全策略

×

* 名称

FTP_Server

描述

策略组

-- NONE --

^ 条件

源

安全区域

untrust

IP 地址

请选择地址

目的

安全区域

trust

IP 地址

192.168.16.110

服务

ftp

更多

应用/时间段/VLAN ID

^ 动作

动作

允许

禁止

取消

命令预览

确定

图9-4 创建针对 FTP 服务器的安全策略

新创建的安全策略优先级在 IPS 设备默认的安全策略“ips_default”之后，所以需要调整安全策略优先级，具体操作如下：

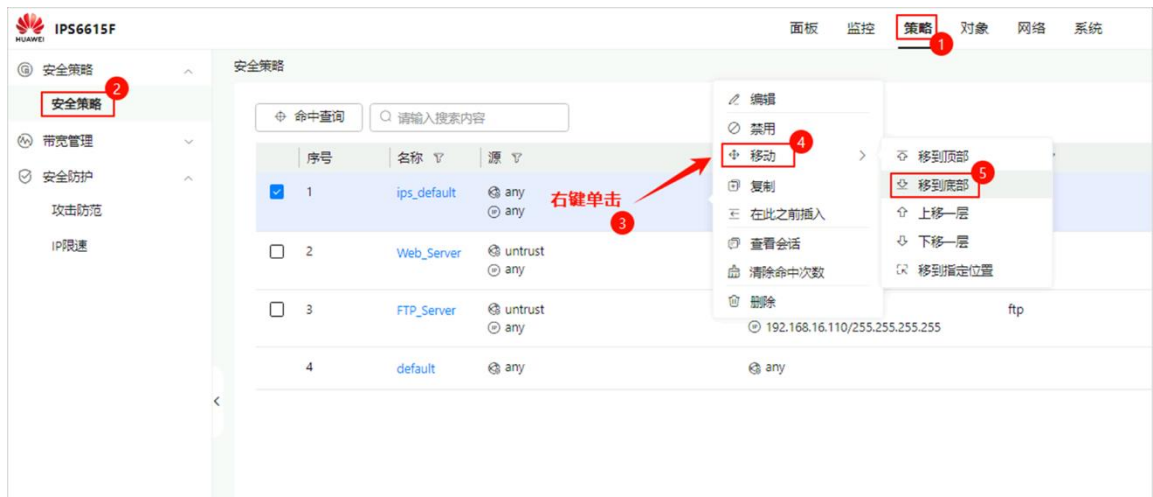


图9-5 调整 IPS 设备安全策略优先级

安全策略优先级调整完成后，效果如下：

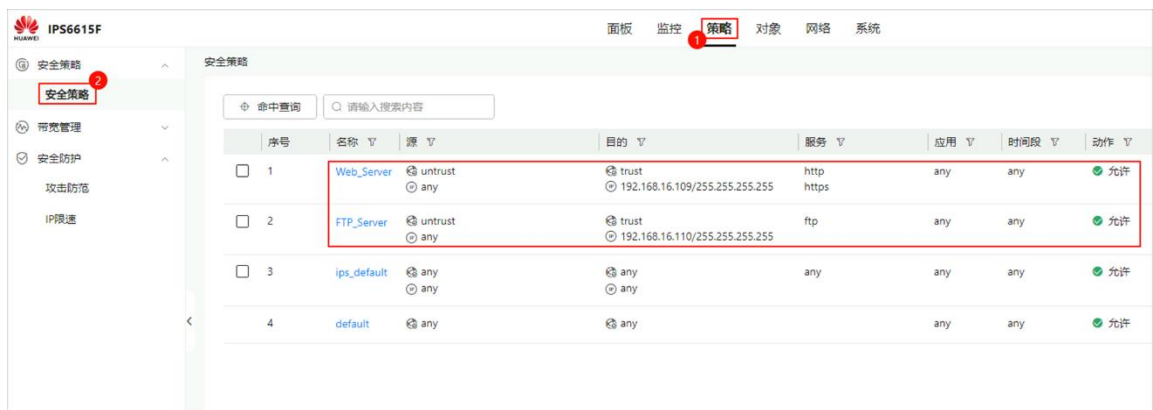


图9-6 IPS1 安全策略概览

步骤 2 创建入侵防御配置文件

登录 IPS1 设备 Web 管理界面（地址：<https://172.21.10.41:8443/>，账号：Webuser/Admin@123），选择“对象 > 安全配置文件 > 入侵防御 > 新建”，进入入侵防御配置文件创建界面，执行以下操作：

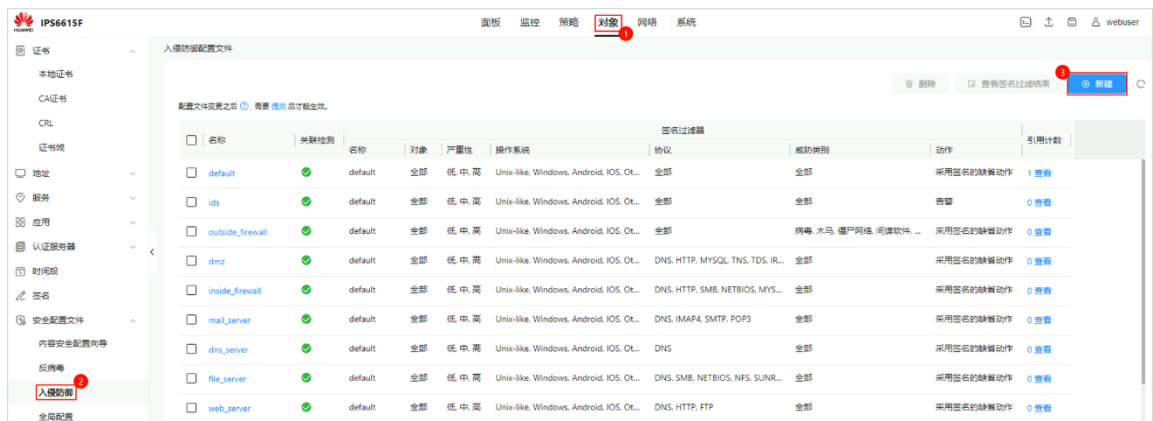


图9-7 进入 IPS 配置文件创建界面

图9-8 创建 Web_Server 入侵防御配置文件

图9-9 创建签名过滤器



图9-10 完成 Web_Server 入侵防御配置文件创建

使用同样配置方式继续创建针对 FTP 服务器的入侵防御配置文件：



图9-11 创建针对 FTP 服务器的入侵防御配置文件

步骤 3 创建反病毒配置文件

登录 IPS1 设备 Web 管理界面 (地址: <https://172.21.10.41:8443/>, 账号: Webuser/Admin@123), 选择“对象 > 安全配置文件 > 反病毒 > 新建”, 进入反病毒配置文件创建界面, 执行以下操作:

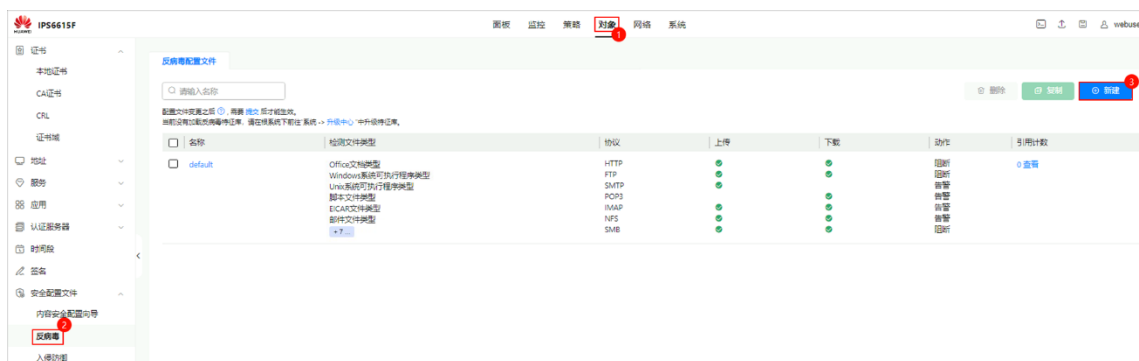


图9-12 进入反病毒配置文件创建界面

新建反病毒配置文件

基础配置

* 名称

FTP_Server

检测文件类型

Office文档类型 × Windows系统... × Unix系统可执... × 脚本文件类型 × EICAR文件类型 × 邮件文件类型 × Flash文件类型 × + 6...

检测协议

协议	检测开关	检测方向	检测动作
HTTP	☐	双向	阻断
FTP	☒	双向	阻断
SMTP	☐	上传	告警
POP3	☐	下载	告警
IMAP	☐	双向	告警
NFS	☐	双向	告警
SMB	☐	双向	阻断

病毒例外

请输入病毒名称

添加

删除

☐	名称
--------------------------	----

取消

确定

图9-14 创建针对 FTP 服务器的反病毒配置文件

步骤 4 调用配置文件

登录 IPS1 设备 Web 管理界面（地址：<https://172.21.10.41:8443/>，账号：Webuser/Admin@123），选择“策略 > 安全策略 > 安全策略”，进入安全策略列表界面，选择之前创建的业务安全策略“Web_Server”和“FTP_Server”进行二次编辑，以“Web_Server”安全策略为例，演示配置文件的调用过程：

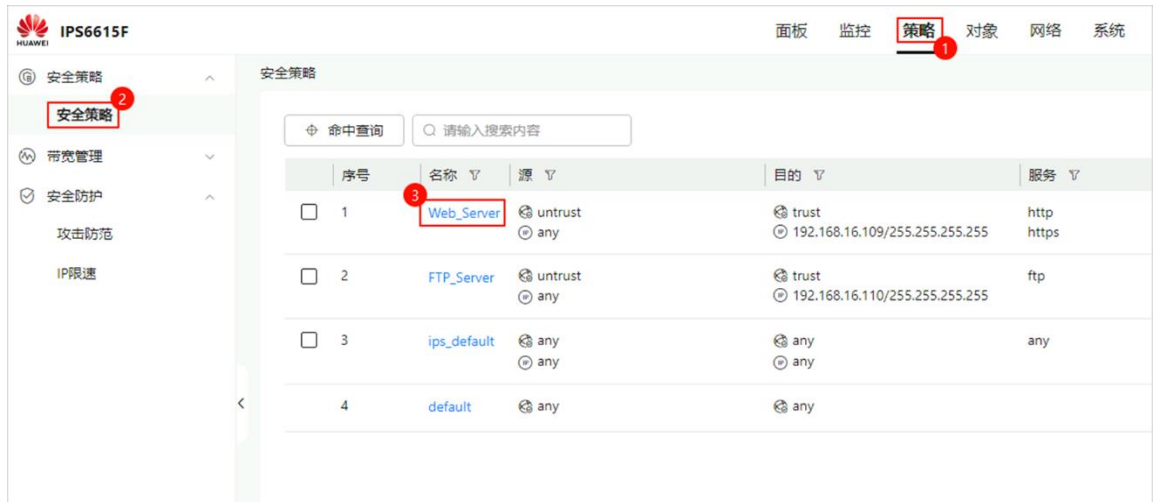


图9-15 进入“Web_Server”安全策略编辑界面

修改安全策略

概述

* 名称

Web_Server

描述

策略组

-- NONE --

条件

动作

允许

禁止

内容安全检查

反病毒

Web_Server

入侵防御

Web_Server

其他

取消

命令预览

确定

图9-16 在“Web_Server”安全策略下调用入侵防御及反病毒配置文件

使用同样操作方式在“FTP_Server”安全策略下调用对应的入侵防御配置文件和反病毒配置文件，调用完成后效果如下：

IPS6615F

面板

监控

策略

对象

网络

系统

安全策略

安全策略

命中查询

请输入搜索内容

序号	名称	源	目的	服务	应用	时间段	动作	内容安全
1	Web_Server	untrust any	trust 192.168.16.109/255.255.255.255	http https	any	any	允许	AV IPS
2	FTP_Server	untrust any	trust 192.168.16.110/255.255.255.255	ftp	any	any	允许	AV IPS
3	ips_default	any any	any any	any	any	any	允许	IPS
4	default	any	any		any	any	允许	

图9-17 配置文件调用概览

步骤 5 提交配置

登录 IPS1 设备 Web 管理界面（地址：https://172.21.10.41:8443/，账号：Webuser/Admin@123），在页面右上角点击提交配置按钮，完成入侵防御及反病毒相关配置的提交：

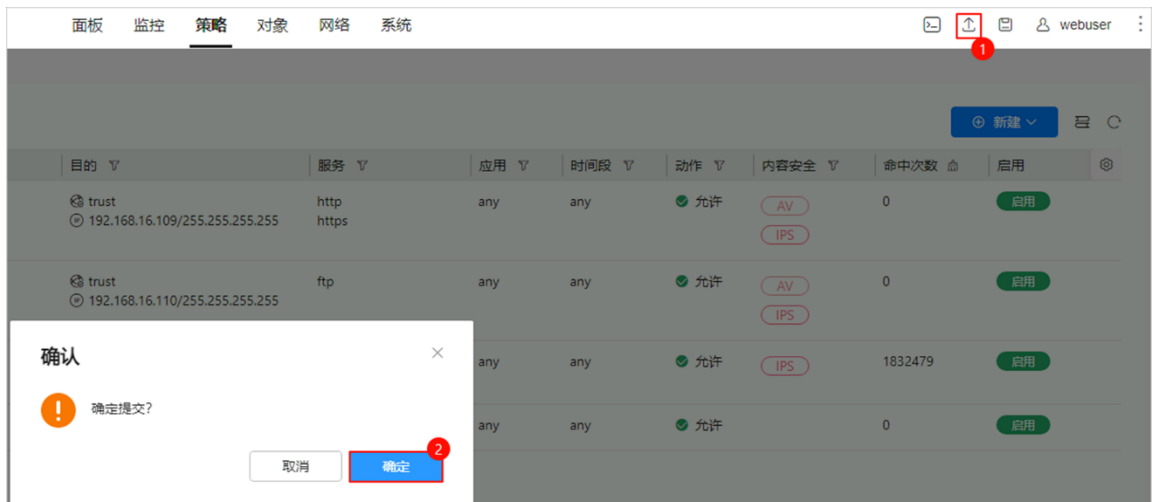


图9-18 提交内容安全配置



图9-19 配置提交成功

上述所有配置 IPS2 设备均会通过 HRP 自动同步，无需单独配置。

9.3 结果验证

使用 RDP 登录 PC5（地址：172.21.10.205，账号：admin/Huawei123!），在成功接入 SSL VPN 后，打开资源管理器连接企业总部 FTP 服务器，并将桌面上的“入侵防御测试文件”文件上传至企业总部 FTP 服务器。

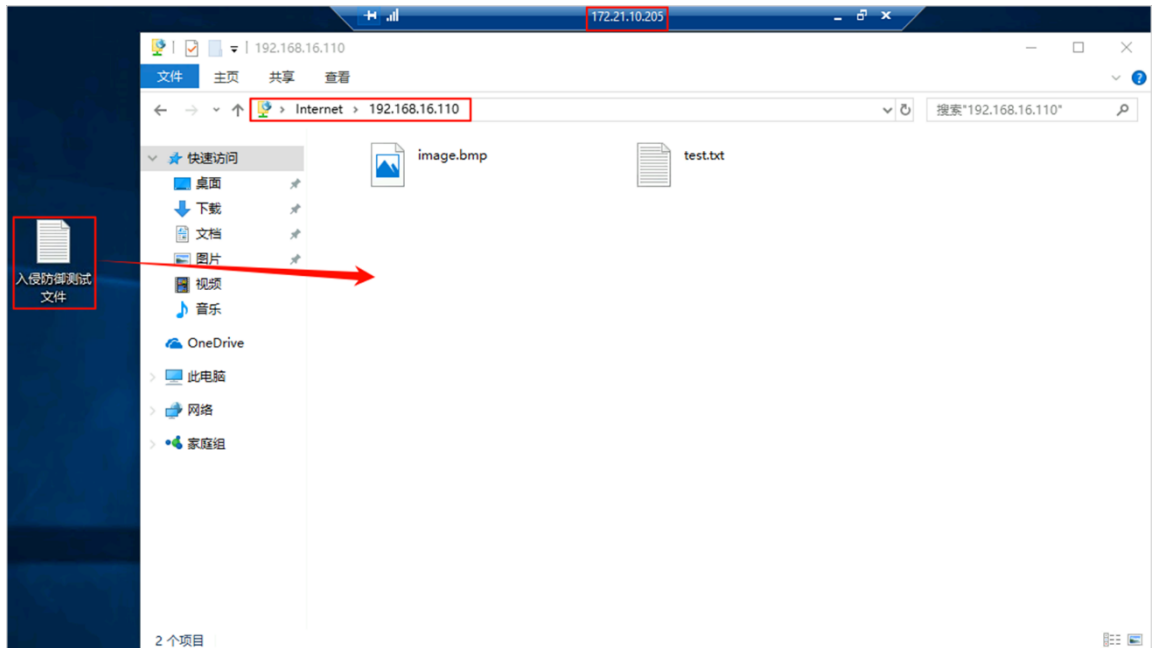


图9-20 PC5 上传入侵防御测试文件

执行完上述操作后，回到 IPS1 设备 Web 管理界面，选择“监控 > 日志 > 威胁日志”，可以发现刚才的文件传输行为已经触发了威胁日志的产生：

说明：此处威胁日志条目数和执行文件传输的次数有关，存在威胁日志即可，无需关注数量。



图9-21 IPS1 设备产生的入侵防御威胁日志

9.4 配置参考（仅展示本实验相关配置）

9.4.1 IPS1 的配置

```
#
profile type ips name Web_Server
undo assoc-check enable
signature-set name Web_Server
action block
os windows
target both
severity low medium high information
protocol DNS HTTP ICMP TFTP FTP
```

```
category Trojan Adware CGI XSS Injection Webshell
profile type ips name FTP_Server
undo assoc-check enable
signature-set name FTP_Server
action block
os unix-like windows android ios other
target both
severity low medium high information
protocol all
category all
#
profile type av name Web_Server
undo ftp-detect enable
undo smtp-detect enable
undo pop3-detect enable
undo imap-detect enable
undo nfs-detect enable
undo smb-detect enable
profile type av name FTP_Server
file-type av all
undo http-detect enable
undo smtp-detect enable
undo pop3-detect enable
undo imap-detect enable
undo nfs-detect enable
undo smb-detect enable
#
security-policy
default action permit
rule name Web_Server
source-zone untrust
destination-zone trust
destination-address 192.168.16.109 mask 255.255.255.255
service http
service https
profile av Web_Server
profile ips Web_Server
action permit
rule name FTP_Server
source-zone untrust
destination-zone trust
destination-address 192.168.16.110 mask 255.255.255.255
service ftp
profile av FTP_Server
profile ips FTP_Server
action permit
rule name ips_default
profile ips default
```



```
action permit  
#
```

9.5 思考题

USG 设备本身已包含了 IPS 设备的绝大部分功能,为何还需要在企业网络中单独部署 IPS 设备?

答案: 尽管华为 USG 设备具备 IPS 的大部分功能,但在企业网络中单独部署 IPS 设备仍有必要。这主要是因为特定的 IPS 设备能更专注于入侵检测和防御,提供针对高级威胁的深度包检查,以及针对新型和复杂攻击的专用签名。例如,华为曾发现其 HG532 设备存在未知漏洞(CVE-2017-17215), 此类漏洞需要依赖 CheckPoint 的 IPS 保护模块进行针对性防御,确保网络的安全。单独的 IPS 设备能有效弥补设备原生安全功能的不足,提供额外的安全能力补充,尤其是在面对 0 day 漏洞时,能提供即时的保护。

10 Anti-DDoS 配置实验

10.1 实验介绍

10.1.1 关于本实验

公司总部网络部署 Web 服务器对内外网的用户提供服务，为保障内外网用户访问服务器的稳定性，避免因发生 DDoS 攻击造成公司 Web 类服务中断，公司总部在网络出口部署了 Anti-DDoS 设备，并通过 SecoManager 控制器对 Anti-DDoS 设备进行集中管理、策略下发和日志分析等工作。

10.1.2 实验组网介绍

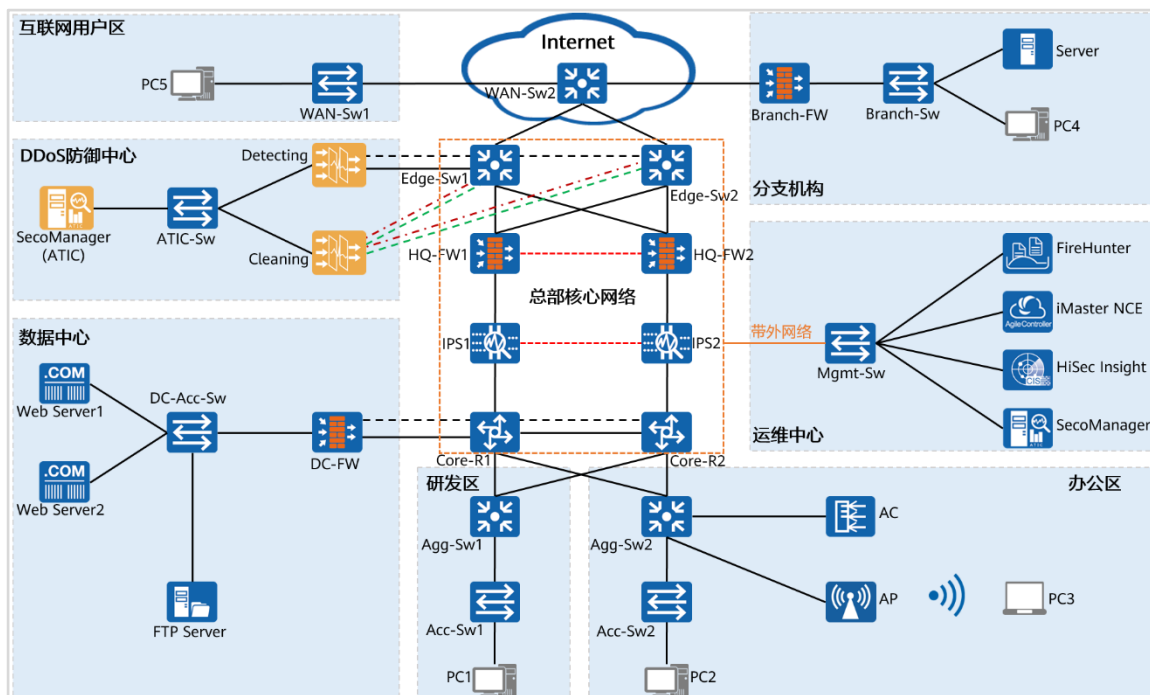


图10-1 实验拓扑图

10.1.3 实验规划

总部网络出口部署了 2 台 Anti-DDoS 设备，1 台作为检测设备，另 1 台 Anti-DDoS 设备作为清洗设备。当发现 DDoS 攻击时，检测设备上报 SecoManager，SecoManager 下发防御策略到清洗设备，清洗设备根据防御策略进行清洗。

网络参数规划如下：

表10-1 Anti-DDoS 系统网络参数规划

设备	端口	用途	地址
SecoManager (ATIC)	eth1	业务对接	172.21.10.73/17
Detecting	Meth0/0/0	管理口，对接 SecoManager	172.21.10.31/17
	G0/0/0	日志口，对接 SecoManager	172.21.10.33/17
	G0/0/1	流量检测端口（主）	/
	G0/0/2	流量检测端口（备）	/
Cleaning	Meth0/0/0	管理口，对接 SecoManager	172.21.10.32/17
	G0/0/0	日志口，对接 SecoManager	172.21.10.34/17
	G0/0/1	引流地址（主）	192.168.10.26/30
	G0/0/2	引流地址（备）	192.168.10.34/30
	G0/0/3	回注地址（主）	192.168.10.30/30
	G0/0/4	回注地址（备）	192.168.10.38/30
Edge-Sw1	G0/0/1 (VLANIF 31)	镜像端口	100.1.31.1/30
	G0/0/4 (VLANIF 31)	观察端口	/
	G0/0/5	引流端口	192.168.10.25/30
	G0/0/6	回注端口	192.168.10.29/30
Edge-Sw2	G0/0/1 (VLANIF 32)	镜像端口	100.1.32.1/30
	G0/0/4 (VLANIF 32)	观察端口	/
	G0/0/5	引流端口	192.168.10.33/30
	G0/0/6	回注端口	192.168.10.37/30

Anti-DDoS 设备对接 SecoManager 设备时的 SNMP 及 STelnet 参数规划：

表10-2 SNMP 参数规划

配置项	参数
协议版本	SNMP v3

用户名	atic
认证算法	SHA2-256
加密算法	AES256
认证密钥	Security@123
鉴权密钥	Security@123

表10-3 STelnet 参数规划

配置项	参数
用户名	aticuser
认证密码	HCIE@Security12#\$
RSA密钥长度	3072

10.2 实验配置任务

10.2.1 配置思路

1. 基于拓扑规划，合理配置 Anti-DDoS 设备的工作模式及业务接口。
2. 在企业总部出口设备 Edge-Sw 设备上部署端口镜像，将进入企业总部的业务流量镜像至 Detecting 设备。
3. 在 Edge-Sw 设备和 Cleaning 设备之间部署 BGP 协议，建立 IBGP 邻居关系，AS 号为 100，并将到达防护对象（Web Server）的可疑流量从 Edge-Sw 引流至 Cleaning 设备。
4. 完成流量清洗后，Cleaning 设备通过 PBR 方式将流量回注至 Edge-Sw 设备。
5. 在 Detecting 设备和 Cleaning 设备上部署 SNMP 和 STelnet 功能，便于对接 SecoManager。
6. 登录 SecoManager 纳管 Detecting 设备和 Cleaning 设备，并配置防护对象和防御策略。
7. 为保证防护阈值设置合理，需在 SecoManager 侧配置基线学习功能，实时优化防御阈值，避免误判。

10.2.2 配置步骤

步骤 1 配置工作模式及业务接口

修改检测设备的工作模式，并重启。

```
[Anti-DDoS-Detect]firewall ddos detect-spu slot 0 cpu 0
[Anti-DDoS-Detect]quit
<Anti-DDoS-Detect>save
Warning: The current configuration will be written to the device.Continue? [Y/N]:y
Now saving the current configuration to the slot 0 .
Info: Save the configuration successfully.
<Anti-DDoS-Detect>reboot
```

```

MPU 0:
Next startup system software: flash:/Anti-DDoS1900_V600R022C00SPC100.cc
Next startup saved-configuration file: flash:/1.cfg
Next startup paf file: default
Next startup patch package: flash:/Anti-DDoS1900_V600R022SPH150.PAT
Warning: The system will reboot.Continue? [Y/N]:y

```

说明：

表10-4 不同型号 Anti-DDoS 设备工作模式修改命令及说明

设备型号	模式修改	备注
Anti-DDoS1905 系列	firewall ddos 命令用来指定 CPU 为检测或者 flow 检测。 undo firewall ddos 命令用来删除 CPU 检测或 flow 检测类型。	缺省情况下，CPU 为清洗功能，用户需通过命令指定某 CPU 为检测或 flow 检测功能。
Anti-DDoS1908 系列	firewall ddos detect-spu 命令用来指定 CPU 为检测。 undo firewall ddos detect-spu 命令用来删除 CPU 检测。	缺省情况下，CPU 为清洗功能，用户需要通过命令指定某 CPU 为检测功能。

等待 Detecting 设备重启完成后，开始配置设备业务接口及安全区域。

Detecting 设备安全区域配置。

```

[Anti-DDoS-Detect]firewall zone trust
[Anti-DDoS-Detect-zone-trust] add interface GE0/0/0
[Anti-DDoS-Detect-zone-trust]quit
[Anti-DDoS-Detect]firewall zone untrust
[Anti-DDoS-Detect-zone-untrust]add interface GE0/0/1
[Anti-DDoS-Detect-zone-untrust]add interface GE0/0/2
[Anti-DDoS-Detect-zone-untrust]quit
[Anti-DDoS-Detect]

```

Cleaning 设备安全区域配置。

```

[Anti-DDoS-Clean]firewall zone trust
[Anti-DDoS-Clean-zone-trust]add interface G 0/0/0
[Anti-DDoS-Clean-zone-trust]add interface G 0/0/3
[Anti-DDoS-Clean-zone-trust]add interface G 0/0/4
[Anti-DDoS-Clean-zone-trust]quit
[Anti-DDoS-Clean]firewall zone untrust
[Anti-DDoS-Clean-zone-untrust] add interface G 0/0/1
[Anti-DDoS-Clean-zone-untrust] add interface G 0/0/2
[Anti-DDoS-Clean-zone-untrust]quit
[Anti-DDoS-Clean]

```

Detecting 设备业务接口配置。

```

[Anti-DDoS-Detect]interface GE0/0/0

```

```
[Anti-DDoS-Detect-GE0/0/0] undo service-manage enable
[Anti-DDoS-Detect-GE0/0/0] anti-ddos detect enable
[Anti-DDoS-Detect-GE0/0/0] quit
[Anti-DDoS-Detect]interface GE0/0/1
[Anti-DDoS-Detect-GE0/0/1] portswitch
[Anti-DDoS-Detect-GE0/0/1] port link-type trunk
[Anti-DDoS-Detect-GE0/0/1] port trunk allow-pass vlan 1 to 4094
Info: Some VLANs are not created.Please create them to make the configuration take effect.
[Anti-DDoS-Detect-GE0/0/1] anti-ddos flow-statistic enable
[Anti-DDoS-Detect-GE0/0/1] anti-ddos detect enable
[Anti-DDoS-Detect-GE0/0/1] quit
[Anti-DDoS-Detect]interface GE0/0/2
[Anti-DDoS-Detect-GE0/0/2] portswitch
[Anti-DDoS-Detect-GE0/0/2] port link-type trunk
[Anti-DDoS-Detect-GE0/0/2] port trunk allow-pass vlan 1 to 4094
Info: Some VLANs are not created.Please create them to make the configuration take effect.
[Anti-DDoS-Detect-GE0/0/2] anti-ddos flow-statistic enable
[Anti-DDoS-Detect-GE0/0/2] anti-ddos detect enable
[Anti-DDoS-Detect-GE0/0/2] quit
[Anti-DDoS-Detect]
```

Cleaning 设备业务接口配置。

```
[Anti-DDoS-Clean] interface G 0/0/0
[Anti-DDoS-Clean-GE0/0/0] undo service-manage enable
[Anti-DDoS-Clean-GE0/0/0] quit
[Anti-DDoS-Clean] interface G 0/0/1
[Anti-DDoS-Clean-GE0/0/1] undo service-manage enable
[Anti-DDoS-Clean-GE0/0/1] anti-ddos clean enable
[Anti-DDoS-Clean-GE0/0/1] anti-ddos flow-statistic enable
[Anti-DDoS-Clean-GE0/0/1]quit
[Anti-DDoS-Clean] interface G 0/0/2
[Anti-DDoS-Clean-GE0/0/2] undo service-manage enable
[Anti-DDoS-Clean-GE0/0/2] anti-ddos clean enable
[Anti-DDoS-Clean-GE0/0/2] anti-ddos flow-statistic enable
[Anti-DDoS-Clean-GE0/0/2] quit
[Anti-DDoS-Clean] interface G 0/0/3
[Anti-DDoS-Clean-GE0/0/3] undo service-manage enable
[Anti-DDoS-Clean-GE0/0/3] quit
[Anti-DDoS-Clean] interface G 0/0/4
[Anti-DDoS-Clean-GE0/0/4] undo service-manage enable
[Anti-DDoS-Clean-GE0/0/4] quit
[Anti-DDoS-Clean]
```

完成 Detecting 设备及 Cleaning 设备的安全区域及业务接口的配置后，需要配置安全策略，放行业务流量。

Detecting 设备安全策略配置。

```
[Anti-DDoS-Detect]security-policy
[Anti-DDoS-Detect-policy-security]default action permit
```

```
Warning:Setting the default packet filtering to permit poses security risks.You are advised to configure
the security policy based on the actual data flows.Are you sure you want to continue?Please select
[Y/N]:y
[Anti-DDoS-Detect-policy-security]quit
```

Cleaning 设备安全策略配置同上。

步骤 2 配置端口镜像

```
[Edge-Sw1] observe-port 1 interface g0/0/4
[Edge-Sw1] interface GE0/0/1
[Edge-Sw1-GE0/0/1] port-mirroring to observe-port 1 inbound
[Edge-Sw1-GE0/0/1] quit
[Edge-Sw1]
```

Edge-Sw2 设备端口镜像配置同上。

步骤 3 配置 BGP

在 Cleaning 设备上部署 BGP 协议，与 Edge-Sw 设备建立 IBGP 邻居关系，用于 DDoS 引流。

```
[Anti-DDoS-Clean] route-policy 1 permit node 10
Info: This sequence is being overridden.
[Anti-DDoS-Clean-route-policy] apply community no-advertise
[Anti-DDoS-Clean-route-policy] quit
[Anti-DDoS-Clean] bgp 100
[Anti-DDoS-Clean-bgp] router-id 32.32.32.32
[Anti-DDoS-Clean-bgp] peer 192.168.10.25 as-number 100
[Anti-DDoS-Clean-bgp] peer 192.168.10.33 as-number 100
[Anti-DDoS-Clean-bgp] import-route ospf
[Anti-DDoS-Clean-bgp] ipv4-family unicast
[Anti-DDoS-Clean-bgp-af-ipv4] peer 192.168.10.25 route-policy 1 export
[Anti-DDoS-Clean-bgp-af-ipv4] peer 192.168.10.25 advertise-community
[Anti-DDoS-Clean-bgp-af-ipv4] peer 192.168.10.33 route-policy 1 export
[Anti-DDoS-Clean-bgp-af-ipv4] peer 192.168.10.33 advertise-community
[Anti-DDoS-Clean-bgp-af-ipv4] quit
[Anti-DDoS-Clean-bgp] quit
[Anti-DDoS-Clean] firewall ddos bgp-next-hop 192.168.10.29
[Anti-DDoS-Clean] firewall ddos bgp-next-hop fib-filter
```

在 Edge-Sw1 和 Edge-Sw2 设备上配置 BGP 协议，与 Cleaning 设备建立 IBGP 邻居关系。

Edge-Sw1

```
[Edge-Sw1] bgp 100
[Edge-Sw1-bgp] router-id 21.21.21.21
[Edge-Sw1-bgp] peer 192.168.10.26 as-number 100
[Edge-Sw1-bgp] quit
[Edge-Sw1]
```

Edge-Sw2

```
[Edge-Sw2] bgp 100
```

```
[Edge-Sw2-bgp] router-id 22.22.22.22
[Edge-Sw2-bgp] peer 192.168.10.34 as-number 100
[Edge-Sw2-bgp] quit
[Edge-Sw2]
```

步骤 4 配置策略路由

在 Cleaning 设备上配置策略路由，将清洗后的业务流量回注至业务网络中。

```
[Anti-DDoS-Clean] policy-based-route
[Anti-DDoS-Clean-policy-pbr] rule name traffic_injection_sw1
[Anti-DDoS-Clean-policy-pbr-rule-traffic_injection_sw1] ingress-interface GE 0/0/1
[Anti-DDoS-Clean-policy-pbr-rule-traffic_injection_sw1] action pbr egress-interface GE 0/0/3 next-hop
192.168.10.29
[Anti-DDoS-Clean-policy-pbr-rule-traffic_injection_sw1] quit
[Anti-DDoS-Clean-policy-pbr] rule name traffic_injection_sw2
[Anti-DDoS-Clean-policy-pbr-rule-traffic_injection_sw2] ingress-interface GE 0/0/2
[Anti-DDoS-Clean-policy-pbr-rule-traffic_injection_sw2] action pbr egress-interface GE 0/0/4 next-hop
192.168.10.37
[Anti-DDoS-Clean-policy-pbr-rule-traffic_injection_sw2] quit
[Anti-DDoS-Clean-policy-pbr] quit
[Anti-DDoS-Clean]
```

为避免回注流量被再次送往 Cleaning 设备产生环路，需要在出口设备 Edge-Sw 设备上部署策略路由，将回注流量强行转发至下游出口防火墙。

Edge-Sw1

```
[Edge-Sw1] traffic classifier injection
[Edge-Sw1-classifier-injection] if-match inbound-interface GigabitEthernet 0/0/6
[Edge-Sw1-classifier-injection] quit
[Edge-Sw1-classifier-injection] traffic behavior injection
[Edge-Sw1-behavior-injection] redirect ip-nexthop 100.1.34.3
[Edge-Sw1-behavior-injection] quit
[Edge-Sw1-behavior-injection] traffic policy injection
[Edge-Sw1-trafficpolicy-injection] classifier injection behavior injection
[Edge-Sw1-trafficpolicy-injection] quit
[Edge-Sw1] traffic-policy injection global inbound
```

Edge-Sw2

```
[Edge-Sw2] traffic classifier injection
[Edge-Sw2-classifier-injection] if-match inbound-interface GigabitEthernet 0/0/6
[Edge-Sw2-classifier-injection] quit
[Edge-Sw2-classifier-injection] traffic behavior injection
[Edge-Sw2-behavior-injection] redirect ip-nexthop 100.1.35.3
[Edge-Sw2-behavior-injection] quit
[Edge-Sw2-behavior-injection] traffic policy injection
[Edge-Sw2-trafficpolicy-injection] classifier injection behavior injection
[Edge-Sw2-trafficpolicy-injection] quit
[Edge-Sw2] traffic-policy injection global inbound
```


步骤 5 配置 SNMP 与 STelnet

在 Detecting 设备和 Cleaning 设备上部署 SNMP 和 STelnet 功能,便于对接 SecoManager。

Detecting 设备

```
[Anti-DDoS-Detect]snmp-agent
[Anti-DDoS-Detect]snmp-agent sys-info version v3
[Anti-DDoS-Detect]snmp-agent mib-view included mib2view iso
[Anti-DDoS-Detect]snmp-agent group v3 secomanager privacy read-view mib2view write-view
mib2view notify-view mib2view
[Anti-DDoS-Detect]snmp-agent usm-user v3 atic
Warning: Configuring a security algorithm is recommended, because the noauthentication or
authentication mode is insecure.
[Anti-DDoS-Detect]snmp-agent usm-user v3 atic group secomanager
Warning: Configuring a security algorithm is recommended, because the noauthentication or
authentication mode is insecure.
[Anti-DDoS-Detect]snmp-agent usm-user v3 atic authentication-mode sha2-256
Please configure the authentication password (8-255)
Enter Password: //Security@123
Confirm Password: //Security@123
Warning: Configuring a security algorithm is recommended, because the noauthentication or
authentication mode is insecure.
[Anti-DDoS-Detect]snmp-agent usm-user v3 atic privacy-mode aes256
Please configure the privacy password (8-255)
Enter Password: //Security@123
Confirm Password: //Security@123
Warning: The privacy and authentication passwords are the same, which is insecure.It is recommended
that the privacy and authentication passwords are different.
[Anti-DDoS-Detect] snmp-agent protocol source-status all-interface
Warning: It will allow all accessible network to access the device.
[Anti-DDoS-Detect] snmp-agent trap enable
[Anti-DDoS-Detect] snmp-agent trap source G 0/0/0
[Anti-DDoS-Detect] aaa
[Anti-DDoS-Detect-aaa]local-user aticuser password irreversible-cipher HCIE@Security12#$
Info: After changing the rights (including the password, access type, FTP directory, and HTTP directory)
of a local user, the rights of users already online do not change.The change takes effect to users who go
online after the change.
[Anti-DDoS-Detect-aaa] local-user aticuser privilege level 3
Warning: This operation may affect online users and will change the user privilege level, Continue?
[Y/N]:y
[Anti-DDoS-Detect-aaa] local-user aticuser service-type ssh
Info: After changing the rights (including the password, access type, FTP directory, and HTTP directory)
of a local user, the rights of users already online do not change.The change takes effect to users who go
online after the change.
[Anti-DDoS-Detect-aaa] local-aaa-user password policy administrator
[Anti-DDoS-Detect-aaa-lupp-admin] undo password alert original
[Anti-DDoS-Detect-aaa-lupp-admin] password expire 0
Warning: Password expire time configured as zero, there is a security risk.
[Anti-DDoS-Detect-aaa-lupp-admin] quit
[Anti-DDoS-Detect-aaa] undo local-aaa-user wrong-password
```

```
Warning: All blocked users will unblock.Continue? [Y/N]: y
[Anti-DDoS-Detect-aaa] quit
[Anti-DDoS-Detect] ssh user aticuser
Info: Succeeded in adding a new SSH user.
[Anti-DDoS-Detect] ssh user aticuser authentication-type all
[Anti-DDoS-Detect] ssh user aticuser service-type all
[Anti-DDoS-Detect] snetconf server enable
Info: Succeeded in starting the SNETCONF server on SSH port 22.
Warning: After configuring the source interface or source address, the IPV6 listening socket will be
created.
[Anti-DDoS-Detect] netconf
[Anti-DDoS-Detect-netconf] protocol inbound ssh ipv4 port 830
Info: Succeeded in starting the ssh port 830 service.
[Anti-DDoS-Detect-netconf] nacm
[Anti-DDoS-Detect-netconf-nacm] nacm enable
[Anti-DDoS-Detect-netconf-nacm] group-name nacm-group
[Anti-DDoS-Detect-netconf-nacm-nacm-group-nacm-group] user-name aticuser
[Anti-DDoS-Detect-netconf-nacm-nacm-group-nacm-group] quit
[Anti-DDoS-Detect-netconf-nacm] execute-default permit
[Anti-DDoS-Detect-netconf-nacm] quit
[Anti-DDoS-Detect-netconf] quit
[Anti-DDoS-Detect]rsa local-key-pair create
The key name will be:Host
% RSA keys defined for Host_Host already exist.
Warning: Replace the host key, Continue? [Y/N]: y
The range of public key size is (2048, 4096).
NOTE: Key pair generation will take a short while.
Please input the modulus [default = 3072]:
[Anti-DDoS-Detect] user-interface vty 0 4
[Anti-DDoS-Detect-ui-vty0-4] authentication-mode aaa
[Anti-DDoS-Detect-ui-vty0-4] user privilege level 3
[Anti-DDoS-Detect-ui-vty0-4] protocol inbound ssh
[Anti-DDoS-Detect-ui-vty0-4] quit
[Anti-DDoS-Detect] stelnet server enable
[Anti-DDoS-Detect] ssh user aticuser
[Anti-DDoS-Detect] ssh user aticuser authentication-type password
[Anti-DDoS-Detect] ssh user aticuser service-type stelnet
[Anti-DDoS-Detect] ssh server-source all-interface
Warning: SSH server source configuration will take effect in the next login.Continue? [Y/N]:y
Warning: It expands the range of accessed IP.
[Anti-DDoS-Detect] sftp server enable
Info: Succeeded in starting the SFTP server.
Warning: After configuring the source interface or source address, the IPV6 listening socket will be
created.
[Anti-DDoS-Detect] ssh user aticuser service-type all
[Anti-DDoS-Detect] ssh user aticuser sftp-directory flash:/
```

Cleaning 设备配置同上。

步骤 6 设备纳管

登录 SecoManager 运维界面（地址：https://172.21.10.73:31943，账号：admin/Security@123），选择“设备管理 > 设备”进入设备管理配置界面，执行以下操作：



图10-2 进入设备管理界面



图10-3 进入设备 SSH 指纹策略配置界面



图10-4 配置设备 SSH 指纹验证策略



图10-5 进入设备添加配置界面



SecoManager

监控 攻击防御 报表分析 设备管理 系统管理

网络配置

设备管理 > 网络配置 > 设备

1. 扫描规则定义了IP地址段和使用的协议(SNMP或Netconf), SecoManager根据扫描规则发现设备。
2. 请先导入设备的公钥指纹, 如果不导入请打开[设备SSH指纹策略](#), 打开“信任首次学习的指纹”。

* 设备发现协议类型: SNMP

1. 设置规则

位置: + 选择

设备厂商:

* 管理IP地址: 172.21.10.31
172.21.10.32

< 选择模板 保存模板

SNMPv3

1. 鉴权协议SHA和MD5由于协议本身的限制, 其安全性不高, 建议选择安全性更高的SHA2类型的鉴权协议。
CBC_DES和AES-128安全性不高, 建议使用安全性更高的AES_256加密算法以提升安全性。

* 用户名: atic

* 鉴权协议: SHA2-256

* 加密算法: AES-256

* 端口: 161

* 重复次数(次): 3

* 鉴权密钥: Security@123

* 加密密钥: Security@123

* 超时时间(毫秒): 4000

图10-6 配置设备扫描参数(1)



NETCONF

* 用户名: aticuser

* 密码: HCIE@Security12#\$

* 端口: 830

STELNET

1. STELNET协议为AntiDDoS设备特有参数。
纳管AntiDDoS1800/8000设备时需要开启数据维护中的兼容AntiDDoS1800/8000设备算法开关。

* 用户名: aticuser

* 密码: HCIE@Security12#\$

公钥:

1.如果填写了公钥, 使用STELNET协议访问设备时对设备进行公钥认证。2.为了保证数据传输的安全性, 建议填写公钥。

日志

* 日志密码: HCIE@Security12#\$

其他设置

虚拟系统容量:

开始扫描

图10-7 配置设备扫描参数（2）

设备管理 > 网络配置 > 设备

1、扫描规则定义了IP地址段和使用的协议(SNMP或Netconf)，SecoManager根据扫描规则发现设备。
2、请先导入设备的公钥指纹，如果不导入请打开设备SSH指纹策略，打开“信任首次学习的指纹”。

* 设备发现协议类型： SNMP

1、设置规则 ✓

2、添加设备

扫描网段： 172.21.10.31; 172.21.10.32

扫描进度： 100% 扫描成功： 2 扫描失败： 0 重设规则

扫描成功列表 | 扫描失败列表

全选 全不选 添加 已选择： 2

☒	设备名称	IP地址	版本
☒	Anti-DDoS-Clean	172.21.10.32	
☒	Anti-DDoS-Detect	172.21.10.31	

共2条

返回

确认

发现设备完成，请进行设备添加！

确定

设备管理 > 网络配置 > 设备

1、扫描规则定义了IP地址段和使用的协议(SNMP或Netconf)，SecoManager根据扫描规则发现设备。
2、请先导入设备的公钥指纹，如果不导入请打开设备SSH指纹策略，打开“信任首次学习的指纹”。

* 设备发现协议类型： SNMP

1、设置规则 ✓

2、添加设备

扫描网段： 172.21.10.31; 172.21.10.32

扫描进度： 100% 扫描成功： 2 扫描失败： 0 重设规则

扫描成功列表 | 扫描失败列表

全选 全不选 添加 已选择： 2

☒	设备名称	IP地址	版本
☒	Anti-DDoS-Clean	172.21.10.32	
☒	Anti-DDoS-Detect	172.21.10.31	

共2条

返回

确认

发现设备完成，请进行设备添加！

确定

图10-8 设备扫描成功并添加

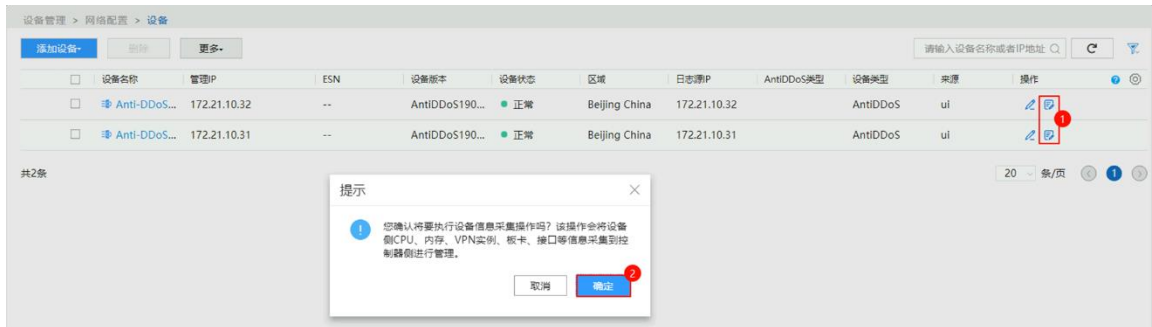


图10-9 采集 Anti-DDoS 设备信息



图10-10 进入采集器配置界面

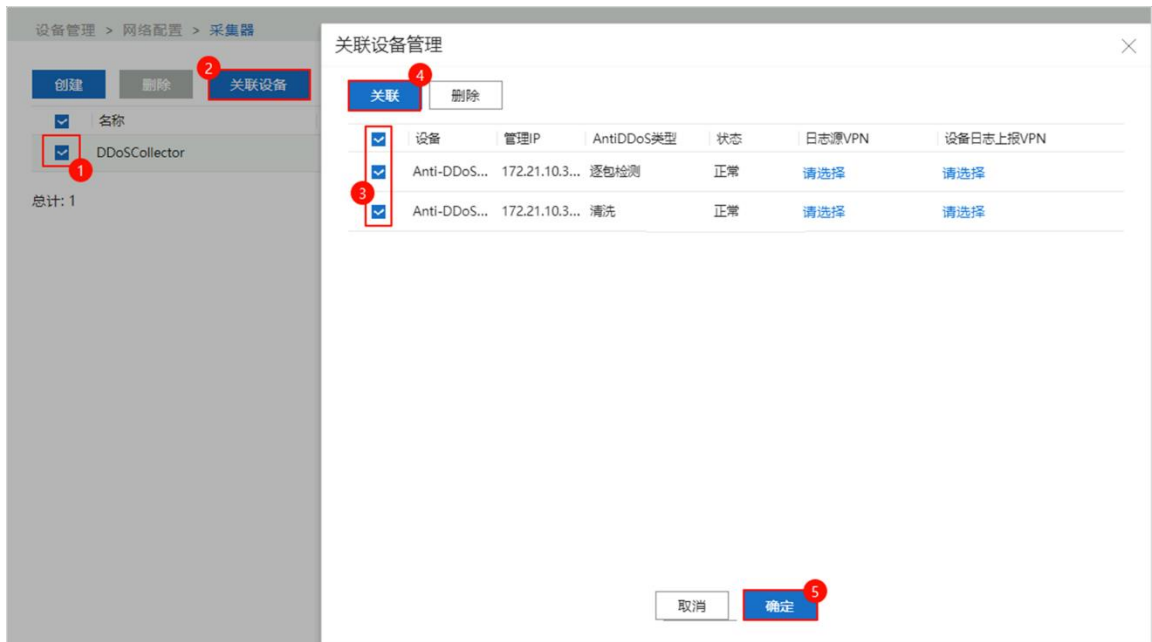


图10-11 采集器关联 Anti-DDoS 设备

完成上述 Anti-DDoS 设备扫描、设备添加以及设备信息采集的操作后，需要在企业总部出口防火墙 HQ-FW 设备上部署 NAT Server，将企业总部 Web 服务器地址映射为一个公网地址，提供给互联网用户访问，并配置相关的业务安全策略，放行对应的访问流量。

登录 HQ-FW1 设备 Web 管理界面（地址：<https://172.21.10.21:8443/>，账号：Webuser/Admin@123），选择“策略 > 安全策略 > 安全策略 > 新建安全策略”，创建以下安全策略，放行互联网用户对企业总部 Web 服务器的访问流量。

图10-12 HQ-FW1 设备创建针对总部 Web 服务器的安全策略

完成安全策略创建后，继续在 HQ-FW1 设备的 Web 管理界面选择“策略 > NAT 策略 > 服务器映射 > 新建”，创建针对企业总部 Web 服务器的 NAT Server。



图10-13 HQ-FW1 创建针对企业总部 Web 服务器的 NAT Server

上述配置会通过 HRP 自动同步至 HQ-FW2 设备。

由于 HQ-FW 设备上部署的 NAT Server 的公网地址对于 WAN-Sw2 和 Edge-Sw 设备都是未知网段，为保证互联网用户（使用 PC5 模拟）可以正常访问企业总部 Web 服务器的对外公网地址（100.1.36.1），需要在 WAN-Sw2 设备配置静态路由，具体操作如下：

WAN-SW2

```
[WAN-SW2] ip route-static 100.1.36.1 32 100.1.31.1
[WAN-SW2] ip route-static 100.1.36.1 32 100.1.32.1 pre 70
```

步骤 7 配置防护对象

登录 SecoManager 运维界面（地址：https://172.21.10.73:31943，账号：admin/Security@123），选择“攻击防御 > 防御对象”进入防御对象配置页面，执行以下操作：

说明：防护对象的参数并非固定，实际部署时可根据业务防护需求合理设置，本实验配置的防护对象参数仅做演示。



图10-14 进入防护对象创建页面



图10-15 创建防护对象



图10-16 设置防护对象参数（1）

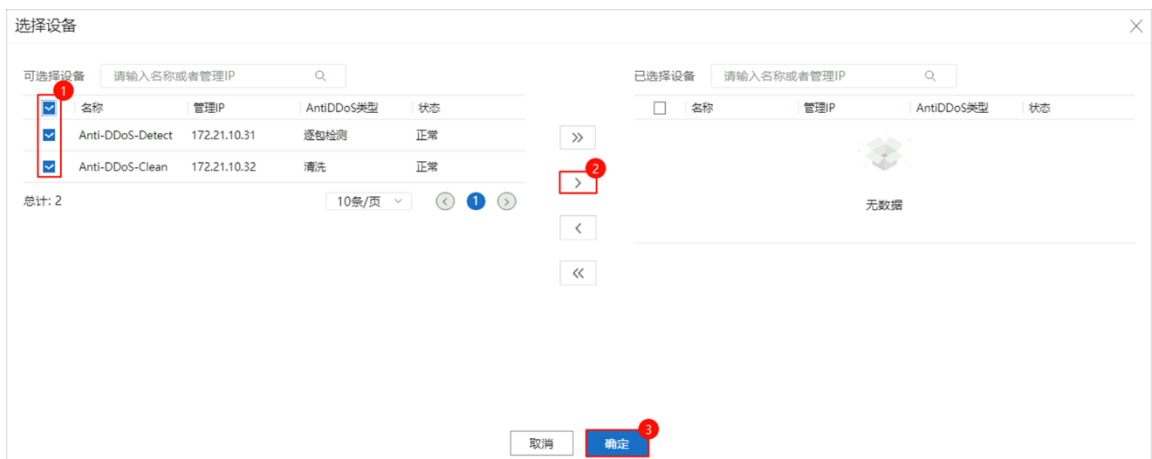


图10-17 设置防护对象参数（2）



图10-18 设置防护对象参数（3）

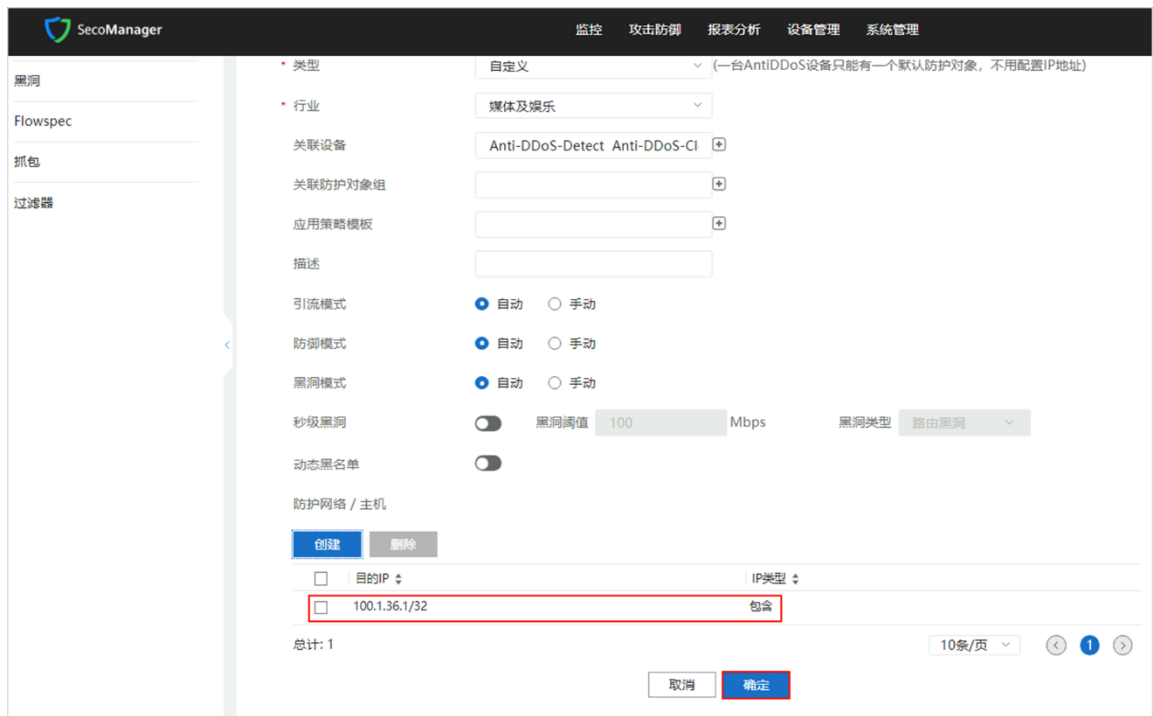


图10-19 确认防护对象参数并提交

防护对象创建完成后效果如下：



图10-20 防护对象创建完成

步骤 8 配置防御策略

登录 SecoManager 运维界面（地址：https://172.21.10.73:31943，账号：admin/Security@123），选择“攻击防御 > 防御对象”进入防御对象配置页面，执行以下操作：



图10-21 进入防御策略编辑界面

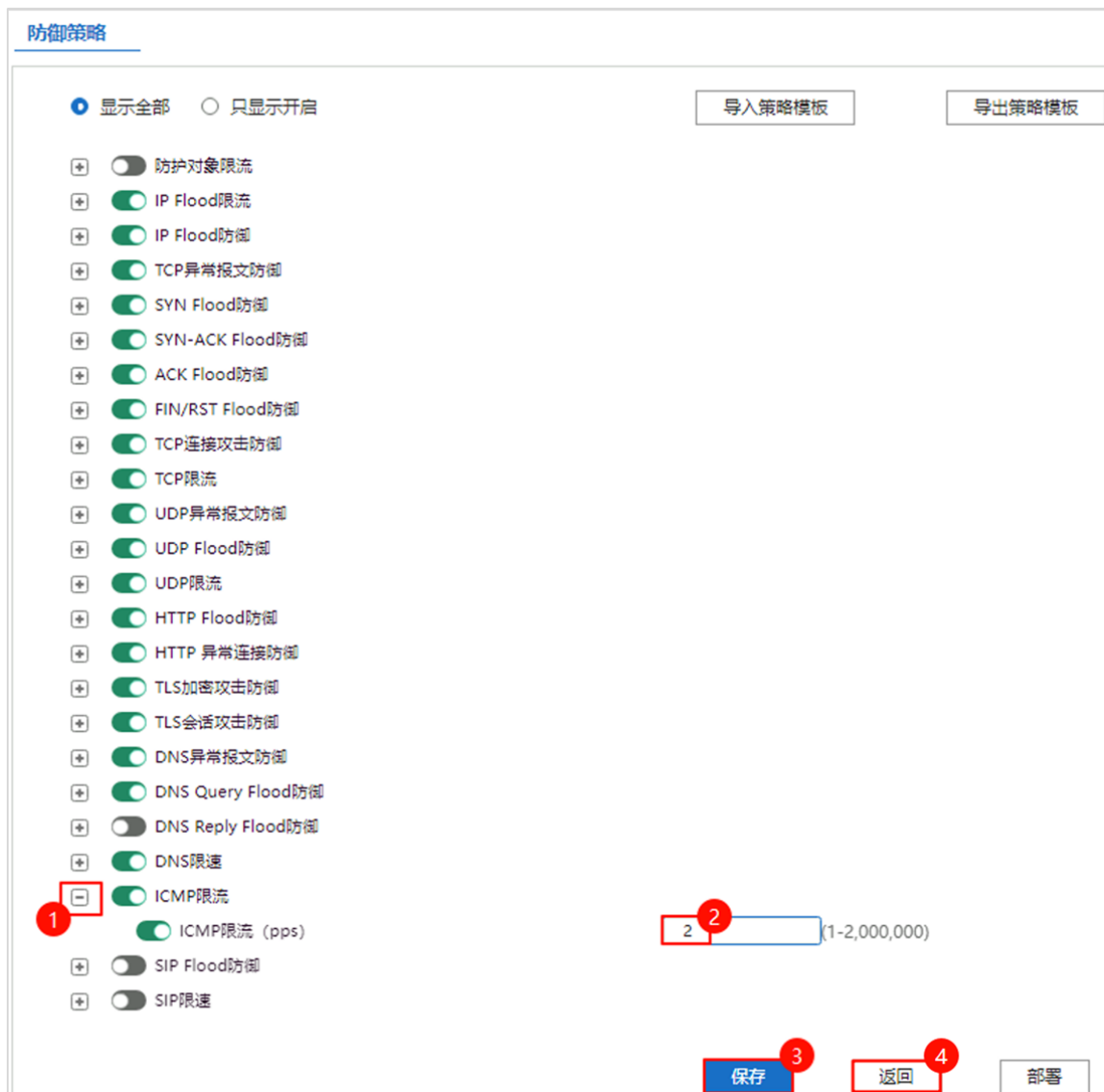


图10-22 设置防御策略

说明：此处为便于触发 Anti-DDoS 系统的防御效果，将 ICMP 限流参数设置为 2pps（Detecting 和 Cleaning 均需配置），实际部署时需根据业务防护需求合理设置。



图10-23 部署防护对象



图10-24 防护对象部署成功

步骤 9 配置基线学习

为保证防护阈值设置合理，需在 SecoManager 侧配置基线学习功能，实时优化防御阈值，避免误判。

登录 SecoManager 运维界面（地址：https://172.21.10.73:31943，账号：admin/Security@123），选择“攻击防御 > 策略管理 > 防护对象”，在防护对象列表界面执行以下操作：

10.3 结果验证

使用 RDP 登录 PC5 (地址: 172.21.10.205, 账号: admin/Huawei123!), 打开 5 个命令行窗口, 对总部 Web 服务器进行不间断并发 Ping 测试 (ping 100.1.36.1 -t), 模拟来自互联网用户的 DDoS 流量:

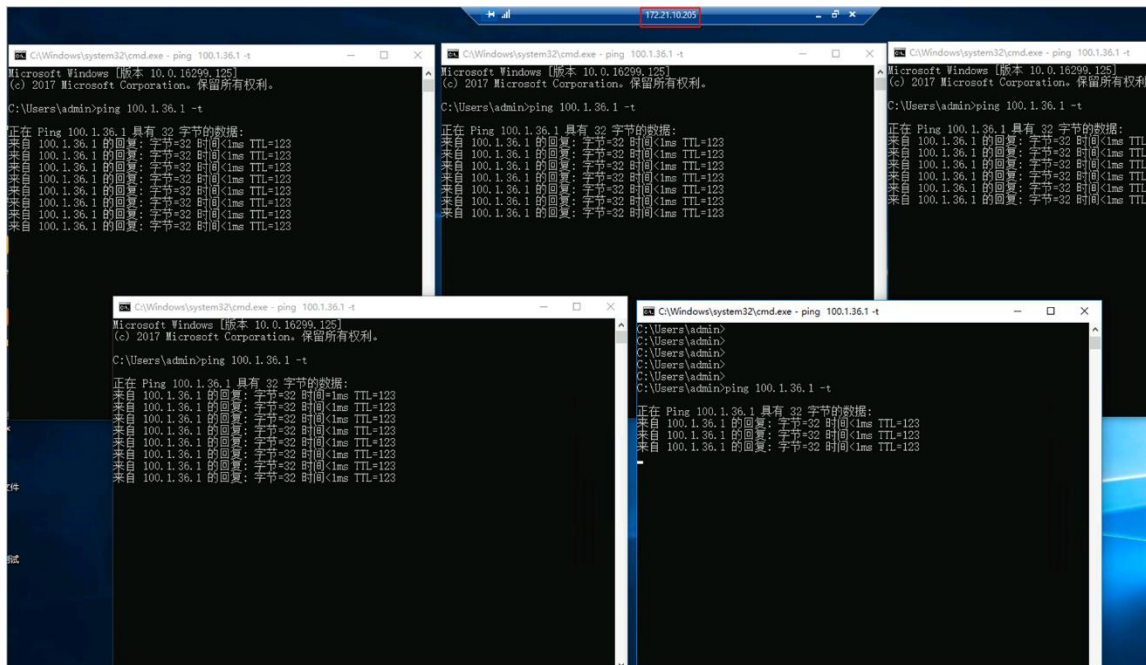


图10-29 PC5 模拟 DDoS 攻击流量

登录 SecoManager 运维界面 (地址: https://172.21.10.73:31943, 账号: admin/Security@123), 选择“攻击防御 > 防御对象”进入防御对象页面, 可以发现防护对象的状态已经变为“异常”, 且引流状态已切换为“引流中”。



图10-30 检测到 DDoS 攻击后防护对象的状态

在 SecoManager 运维界面选择“监控 > 告警管理 > 当前告警”, 查看系统告警信息, 可以发现存在以下告警:



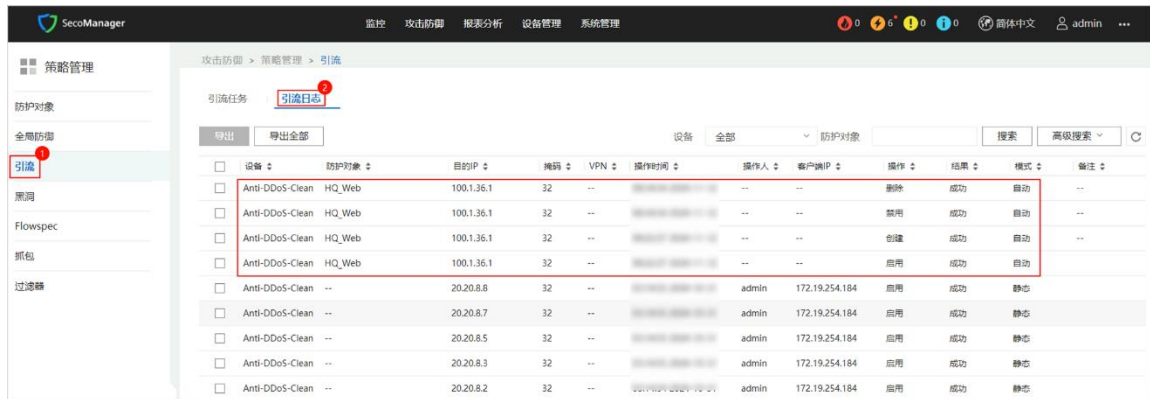
图10-31 查看当前告警

点击“防护对象状态异常”的告警条目，可以看到以下告警详情：



图10-32 查看防护对象异常的告警详情

在 SecoManager 运维界面选择“攻击防御 > 策略管理 > 引流”，查看引流日志，可以看到以下信息：



设备	防护对象	目的IP	掩码	VPN	操作时间	操作人	客户端IP	操作	结果	模式	备注
Anti-DDoS-Clean	HQ_Web	100.1.36.1	32	--	2020-08-08 10:00:00	--	--	删除	成功	自动	--
Anti-DDoS-Clean	HQ_Web	100.1.36.1	32	--	2020-08-08 10:00:00	--	--	禁用	成功	自动	--
Anti-DDoS-Clean	HQ_Web	100.1.36.1	32	--	2020-08-08 10:00:00	--	--	创建	成功	自动	--
Anti-DDoS-Clean	HQ_Web	100.1.36.1	32	--	2020-08-08 10:00:00	--	--	启用	成功	自动	--
Anti-DDoS-Clean	--	20.20.8.8	32	--	2020-08-08 10:00:00	admin	172.19.254.184	应用	成功	静态	--
Anti-DDoS-Clean	--	20.20.8.7	32	--	2020-08-08 10:00:00	admin	172.19.254.184	应用	成功	静态	--
Anti-DDoS-Clean	--	20.20.8.5	32	--	2020-08-08 10:00:00	admin	172.19.254.184	应用	成功	静态	--
Anti-DDoS-Clean	--	20.20.8.3	32	--	2020-08-08 10:00:00	admin	172.19.254.184	应用	成功	静态	--
Anti-DDoS-Clean	--	20.20.8.2	32	--	2020-08-08 10:00:00	admin	172.19.254.184	应用	成功	静态	--

图10-33 查看引流日志

10.4 配置参考（仅展示本实验相关配置）

10.4.1 Anti-DDoS-Detect 的配置

说明：以下配置包含控制器下发的内容，请勿直接复制输入，建议参考上文流程进行配置。

```
#
firewall ddos detect-spu slot 0 cpu 0
#
firewall ddos log-local-ip 172.21.10.31
firewall ddos log-server-ip 172.21.10.73
#
rsa peer-public-key 172.21.10.32
public-key-code begin
3082018A
02820181
009ABC07 5483733C 8A0D3833 1F7DE032 16018DA8 CBF500F9 8CFFC12C 821D6655
1A782ADF 29BFDB06 3D5174B1 44DC06FA D885361E 1EF28BE5 8A65134C 02714755
D2D91064 3826CBA0 E05706DC 8957CCD0 60F79FF7 3D0DCD78 C4AD428A B888BFAF
ECDDFFF5 6BA807BB C1467945 4EDC9622 D1952B2D 9003AF08 7DE04B09 81FC3DBE
88C51162 8D4DDCC0 9FC7684B 5966CD1B 231F0ABA 2631BF28 576014D8 8F02065A
CB92C156 90FA30B9 587127A5 77A5F091 81B8821D 160CD40F 132D08A5 AB53D7E0
E17A860A 13E2AC73 8B7DC984 B3F4B045 A719CEA3 5AB82624 F08C5F4A 0DE7AE08
18183272 93F71296 1889A30C 393B5E6C 299BD5F0 240A0FD4 104F6EFA 600E884D
DF392F8D B5FBEA3D 9ED1CA2B B4D3D65A 7A3DBF1A C375AF08 80DCE8A2 6AEAEDF7
7972A780 DC042FDA 84108CB4 576373A7 117F1399 7319E8F3 4BF11157 B084DF6D
96F478CC 1A1B1C02 0A1A0FF4 DFE171CB 43525553 3D464085 1C319B10 3A87F579
DB592DE7 BDADCF4C 3D0E375F 70B78773 C30968F0 DF285204 85BF5701 3DC12DAE
17
0203
010001
public-key-code end
peer-public-key end
```

```
#
arp learning on-different-segment disable
#
telnet ipv6 server disable
telnet server-source all-interface
undo telnet ipv6 server-source all-interface
#
diffserv domain default
#
ip vpn-instance _management_vpn_
  ipv4-family
#
time-range worktime 08:00 to 18:00 working-day
#
aaa
  local-aaa-user password policy administrator
    undo password alert original
    password expire 0
  undo local-aaa-user wrong-password
  local-user aticuser password irreversible-cipher Security@123
  local-user aticuser privilege level 3
  local-user aticuser service-type ssh
  local-user secomanager password irreversible-cipher HCIE@Security12#$
  local-user secomanager privilege level 3
  local-user secomanager service-type ssh
#
interface GE0/0/0
  ip address 172.21.10.33 255.255.128.0
  undo service-manage enable
  anti-ddos detect enable
#
interface GE0/0/1
  portswitch
  port link-type trunk
  port trunk allow-pass vlan 1 to 4094
  anti-ddos flow-statistic enable
  anti-ddos detect enable
#
interface GE0/0/2
  portswitch
  port link-type trunk
  port trunk allow-pass vlan 1 to 4094
  anti-ddos flow-statistic enable
  anti-ddos detect enable
#
snmp-agent
snmp-agent local-engineid 800007DB03F4E451DE28DF
#
```

```
snmp-agent sys-info version v3
snmp-agent group v3 secomanager privacy read-view mib2view write-view mib2view notify-view mib2view
#
snmp-agent mib-view included ddos iso
snmp-agent mib-view included mib2view iso
snmp-agent usm-user v3 atic
snmp-agent usm-user v3 atic group secomanager
snmp-agent usm-user v3 atic authentication-mode sha2-256 cipher Security@123
snmp-agent usm-user v3 secomanager privacy-mode aes256 cipher Security@123
#
snmp-agent trap source GE0/0/0
#
snmp-agent protocol source-status all-interface
undo snmp-agent protocol source-status ipv6 all-interface
#
undo snmp-agent proxy protocol source-status all-interface
undo snmp-agent proxy protocol source-status ipv6 all-interface
#
snmp-agent trap enable
#
stelnet server enable
sftp server enable
snetconf server enable
ssh server rsa-key min-length 3072
ssh user aticuser
ssh user aticuser authentication-type password
ssh user aticuser service-type all
ssh user aticuser sftp-directory flash:/
ssh user secomanager
ssh user secomanager authentication-type password
ssh user secomanager service-type stelnet
ssh server-source all-interface
undo ssh ipv6 server-source all-interface
ssh authorization-type default aaa
#
ssh server cipher aes256_gcm aes128_gcm aes256_ctr aes192_ctr aes128_ctr
ssh server hmac sha2_512 sha2_256
ssh server key-exchange dh_group_exchange_sha256
#
ssh server publickey rsa_sha2_256 rsa_sha2_512
#
ssh server dh-exchange min-len 3072
#
ssh client first-time enable
ssh client peer 172.21.10.32 assign rsa-key 172.21.10.32
#
ssh client publickey rsa_sha2_256 rsa_sha2_512
```

```
#
ssh client cipher aes256_gcm aes128_gcm aes256_ctr aes192_ctr aes128_ctr
ssh client hmac sha2_512 sha2_256
ssh client key-exchange dh_group_exchange_sha256
#
netconf
protocol inbound ssh ipv4 port 830
#
nacm
nacm enable
execute-default permit
group-name nacm-group
user-name atic
#
anti-ddos filter name test type dns
filter-id 10
#
ddos-zone name zone_11
zone-id 11
ip address 100.1.100.1 32
anti-ddos destination-ip session-limit protocol tcp max-speed 400000
anti-ddos destination-ip session-limit protocol udp max-speed 10000
anti-ddos destination-ip session-limit protocol other max-speed 10000
bandwidth-limit destination-ip type udp max-speed 50000
bandwidth-limit destination-ip type icmp max-speed 500
bandwidth-limit destination-ip type tcp-fragment max-speed 10000
bandwidth-limit destination-ip type udp-fragment max-speed 10000
bandwidth-limit destination-ip type other max-speed 100000
anti-ddos rst-flood session-check
anti-ddos syn-flood source-detect mode advanced
anti-ddos tcp-abnormal-flood alert-rate 500
anti-ddos syn-flood source-limit max-number 50 duration 3
anti-ddos dns format-check alert-rate 500
anti-ddos dns-request-flood source-detect
anti-ddos ack-flood session-check
anti-ddos ack-flood source-rate-check 500
anti-ddos udp-flood fingerprint-learn enable
anti-ddos udp-malformed-flood alert-rate 500
anti-ddos udp-flood defend alert-speed 500
anti-ddos https-flood defend alert-rate 20000
anti-ddos https-flood ssl-defend illegal-session-num 3 interval 5
anti-ddos https-flood ssl-defend incomplete-negotiation enable
anti-ddos tls-flood large-resource resource-size 100 illegal-ratio 90 min-number 50 interval 5
anti-ddos tls-flood fixed-resource illegal-ratio 90 min-number 20 interval 5
anti-ddos tls-flood concurrent-connection alert-number 10000
anti-ddos http-flood defend alert-request 5000
anti-ddos http-flood detect-uri source-statistic illegal-ratio 90 min-number 20 interval 5
anti-ddos http-flood detect-uri index 1 uri / full-matching
```

```
anti-ddos http-flood slow-attack-check content-length 1000
anti-ddos http-flood large-resource resource-size 100 illegal-ratio 90 min-number 50 interval 5
anti-ddos http-flood illegal-session-check
anti-ddos http-flood illegal-session-check null-method-check enable
anti-ddos http-flood illegal-session-check range-header-check enable
anti-ddos http-flood illegal-session-check multi-method-check enable
anti-ddos http-flood concurrent-connection alert-number 10000
anti-ddos tcp-connection-flood alert-number 20000
anti-ddos tcp-connection-flood alert-rate 5000
anti-ddos tcp-connection-flood illegal-session-check packet-min-number 1 interval 5
anti-ddos tcp-connection-flood illegal-session-check illegal-session-num 3 interval 5
anti-ddos dns-request-limit source-ip other max-rate 200
anti-ddos first-packet-check tcp
anti-ddos first-packet-check udp interval upper-limit 2000
anti-ddos first-packet-check dns interval upper-limit 5000
anti-ddos first-packet-check syn interval lower-limit 500 upper-limit 4000
anti-ddos first-packet-check syn-ack interval lower-limit 500 upper-limit 4000
anti-ddos filter attack alert-rate 1000
anti-ddos source-port statistic enable
#
ddos-zone name zone_14
zone-id 14
ip address 100.1.36.1 32
anti-ddos destination-ip session-limit protocol tcp max-speed 400000
anti-ddos destination-ip session-limit protocol udp max-speed 10000
anti-ddos destination-ip session-limit protocol other max-speed 10000
bandwidth-limit destination-ip type udp max-speed 50000
bandwidth-limit destination-ip type icmp max-speed 2
bandwidth-limit destination-ip type tcp-fragment max-speed 10000
bandwidth-limit destination-ip type udp-fragment max-speed 10000
bandwidth-limit destination-ip type other max-speed 100000
anti-ddos rst-flood session-check
anti-ddos syn-flood source-detect mode advanced
anti-ddos tcp-abnormal-flood alert-rate 500
anti-ddos syn-flood source-limit max-number 50 duration 3
anti-ddos dns format-check alert-rate 500
anti-ddos dns-request-flood source-detect
anti-ddos ack-flood session-check
anti-ddos ack-flood source-rate-check 500
anti-ddos udp-flood fingerprint-learn enable
anti-ddos udp-malformed-flood alert-rate 500
anti-ddos udp-flood defend alert-speed 500
anti-ddos https-flood defend alert-rate 20000
anti-ddos https-flood ssl-defend illegal-session-num 3 interval 5
anti-ddos https-flood ssl-defend incomplete-negotiation enable
anti-ddos tls-flood large-resource resource-size 100 illegal-ratio 90 min-number 50 interval 5
anti-ddos tls-flood fixed-resource illegal-ratio 90 min-number 20 interval 5
anti-ddos tls-flood concurrent-connection alert-number 10000
```

```
anti-ddos http-flood defend alert-request 5000
anti-ddos http-flood detect-uri source-statistic illegal-ratio 90 min-number 20 interval 5
anti-ddos http-flood detect-uri index 1 uri / full-matching
anti-ddos http-flood slow-attack-check content-length 1000
anti-ddos http-flood large-resource resource-size 100 illegal-ratio 90 min-number 50 interval 5
anti-ddos http-flood illegal-session-check
anti-ddos http-flood illegal-session-check null-method-check enable
anti-ddos http-flood illegal-session-check range-header-check enable
anti-ddos http-flood illegal-session-check multi-method-check enable
anti-ddos http-flood concurrent-connection alert-number 10000
anti-ddos tcp-connection-flood alert-number 20000
anti-ddos tcp-connection-flood alert-rate 5000
anti-ddos tcp-connection-flood illegal-session-check packet-min-number 1 interval 5
anti-ddos tcp-connection-flood illegal-session-check illegal-session-num 3 interval 5
anti-ddos dns-request-limit source-ip other max-rate 200
anti-ddos first-packet-check tcp
anti-ddos first-packet-check udp interval upper-limit 2000
anti-ddos first-packet-check dns interval upper-limit 5000
anti-ddos first-packet-check syn interval lower-limit 500 upper-limit 4000
anti-ddos first-packet-check syn-ack interval lower-limit 500 upper-limit 4000
anti-ddos filter attack alert-rate 1000
anti-ddos source-port statistic enable
#
firewall zone trust
set priority 85
add interface GE0/0/0
#
firewall zone untrust
set priority 5
add interface GE0/0/1
add interface GE0/0/2
#
security-policy
default action permit
#
return
```

10.4.2 Anti-DDoS-Clean 的配置

说明：以下配置包含控制器下发的内容，请勿直接复制输入，建议参考上文流程进行配置。

```
#
firewall ddos log-local-ip 172.21.10.32
firewall ddos log-server-ip 172.21.10.73
firewall ddos bgp-next-hop fib-filter
firewall ddos bgp-next-hop 192.168.10.29

#
rsa peer-public-key 172.21.10.31
```



```
public-key-code begin
3082018A
02820181
00AC0E08 C9963721 528AE9D2 3686ECEC C406804F 6D9565DA 520A66E4 4EF294AA
8D1C970D 0B3137AD 8245F514 1FC5D98C 94A186DF F9501D92 AA815F76 46842138
45D2753D D5E8D129 1684B60C DE1B463F 83DF2C08 F2A001C4 5595D09C 4D38BD9D
D15348BC 866E0C75 1BB3CC9F 1D243F09 DABBA541 C68F6B89 4FFD30D0 58CDA95A
88D8A21F 91EE36F4 C0BC7CE2 12869296 67277C26 6A927471 3BDC643F B98C833F
20E7A46C FC60A7AF 3DE6F7DA 331DD03E 51F18A31 A947C11C BFA0F022 F7B41E9F
5F6D30BD 235713E4 3F2DDDA 67764455 871B175D 7F752322 F2CD79AF 1C92BAA8
99C7B71E 62CEA696 60A8CCFB F9EB89E6 03625F2C 70897887 7D76CA59 80706999
C3C6CD77 B86A3552 FB1F21F9 39B83CFB 4FF3F62D EA1A8B93 E375C266 042CC3E3
6E01DEE0 1570B5CC A35A5D5A 12EF5F9F 0706B8A0 5054A008 6653BC8D D17067C7
CBF51704 8E331AEE 8D5137ED 33BFF71F EC68361C 917CBE43 127F39B1 1E4DCDF7
7F1D056C 5546D4FA 185D1B9B 4107B471 2FBFEFE29 DFA6322E A74DE4EB B10B3364
5D
0203
010001
public-key-code end
peer-public-key end
#
aaa
local-aaa-user password policy administrator
undo password alert original
password expire 0
undo local-aaa-user wrong-password
local-user aticuser password irreversible-cipher HCIE@Security12#$
local-user aticuser privilege level 3
local-user aticuser service-type ssh
#
interface GE0/0/0
ip address 172.21.10.34 255.255.128.0
undo service-manage enable
#
interface GE0/0/1
ip address 192.168.10.26 255.255.255.252
undo service-manage enable
anti-ddos flow-statistic enable
anti-ddos clean enable
#
interface GE0/0/2
ip address 192.168.10.34 255.255.255.252
undo service-manage enable
anti-ddos flow-statistic enable
anti-ddos clean enable
#
interface GE0/0/3
description ztp
```

```
ip address 192.168.10.30 255.255.255.252
undo service-manage enable
dhcp client request option-list 7 43 66 67 143 150
#
interface GE0/0/4
ip address 192.168.10.38 255.255.255.252
undo service-manage enable
#
bgp 100
router-id 32.32.32.32
private-4-byte-as enable
peer 192.168.10.25 as-number 100
peer 192.168.10.33 as-number 100
#
ipv4-family unicast
import-route ospf
peer 192.168.10.25 enable
peer 192.168.10.25 route-policy 1 export
peer 192.168.10.25 advertise-community
peer 192.168.10.33 enable
peer 192.168.10.33 route-policy 1 export
peer 192.168.10.33 advertise-community
#
route-policy 1 permit node 10
apply community no-advertise
#
snmp-agent
snmp-agent local-engineid 800007DB03F4E451DE25BA
#
snmp-agent sys-info version v3
snmp-agent group v3 secomanager privacy read-view mib2view write-view mib2view notify-view
mib2view
#
snmp-agent mib-view included ddos iso
snmp-agent mib-view included mib2view iso
snmp-agent usm-user v3 atic
snmp-agent usm-user v3 atic group secomanager
snmp-agent usm-user v3 atic authentication-mode sha2-256 cipher Security@123
snmp-agent usm-user v3 atic privacy-mode aes256 cipher Security@123
#
snmp-agent trap source GE0/0/0
#
snmp-agent protocol source-status all-interface
undo snmp-agent protocol source-status ipv6 all-interface
#
undo snmp-agent proxy protocol source-status all-interface
undo snmp-agent proxy protocol source-status ipv6 all-interface
#
```

```
snmp-agent trap enable
#
stelnet server enable
sftp server enable
snetconf server enable
ssh server rsa-key min-length 3072
ssh user aticuser
ssh user aticuser authentication-type password
ssh user aticuser service-type all
ssh user aticuser sftp-directory flash:/
ssh user secomanager
ssh user secomanager authentication-type password
ssh user secomanager service-type stelnet
ssh server-source all-interface
undo ssh ipv6 server-source all-interface
ssh authorization-type default aaa
#
ssh server cipher aes256_gcm aes128_gcm aes256_ctr aes192_ctr aes128_ctr
ssh server hmac sha2_512 sha2_256
ssh server key-exchange dh_group_exchange_sha256
#
ssh server publickey rsa_sha2_256 rsa_sha2_512
#
ssh server dh-exchange min-len 3072
#
ssh client first-time enable
ssh client peer 172.21.10.31 assign rsa-key 172.21.10.31
#
ssh client publickey rsa_sha2_256 rsa_sha2_512
#
ssh client cipher aes256_gcm aes128_gcm aes256_ctr aes192_ctr aes128_ctr
ssh client hmac sha2_512 sha2_256
ssh client key-exchange dh_group_exchange_sha256
#
netconf
  protocol inbound ssh ipv4 port 830
#
nacm
  nacm enable
  execute-default permit
  group-name nacm-group
  user-name atic
#
anti-ddos filter name test type dns
  filter-id 10
#
ddos-zone name zone_11
  zone-id 11
```

```
ip address 100.1.100.1 32
anti-ddos destination-ip session-limit protocol tcp max-speed 400000
anti-ddos destination-ip session-limit protocol udp max-speed 10000
anti-ddos destination-ip session-limit protocol other max-speed 10000
bandwidth-limit destination-ip type udp max-speed 50000
bandwidth-limit destination-ip type icmp max-speed 1
bandwidth-limit destination-ip type tcp-fragment max-speed 10000
bandwidth-limit destination-ip type udp-fragment max-speed 10000
bandwidth-limit destination-ip type other max-speed 100000
anti-ddos rst-flood session-check
anti-ddos syn-flood source-detect mode advanced
anti-ddos tcp-abnormal-flood alert-rate 500
anti-ddos syn-flood source-limit max-number 50 duration 3
anti-ddos dns format-check alert-rate 500
anti-ddos dns-request-flood source-detect
anti-ddos ack-flood session-check
anti-ddos ack-flood source-rate-check 500
anti-ddos udp-flood fingerprint-learn enable
anti-ddos udp-malformed-flood alert-rate 500
anti-ddos udp-flood defend alert-speed 500
anti-ddos https-flood defend alert-rate 20000
anti-ddos https-flood ssl-defend illegal-session-num 3 interval 5
anti-ddos https-flood ssl-defend incomplete-negotiation enable
anti-ddos tls-flood large-resource resource-size 100 illegal-ratio 90 min-number 50 interval 5
anti-ddos tls-flood fixed-resource illegal-ratio 90 min-number 20 interval 5
anti-ddos tls-flood concurrent-connection alert-number 10000
anti-ddos http-flood defend alert-request 5000
anti-ddos http-flood detect-uri source-statistic illegal-ratio 90 min-number 20 interval 5
anti-ddos http-flood detect-uri index 1 uri / full-matching
anti-ddos http-flood slow-attack-check content-length 1000
anti-ddos http-flood large-resource resource-size 100 illegal-ratio 90 min-number 50 interval 5
anti-ddos http-flood illegal-session-check
anti-ddos http-flood illegal-session-check null-method-check enable
anti-ddos http-flood illegal-session-check range-header-check enable
anti-ddos http-flood illegal-session-check multi-method-check enable
anti-ddos http-flood concurrent-connection alert-number 10000
anti-ddos tcp-connection-flood alert-number 20000
anti-ddos tcp-connection-flood alert-rate 5000
anti-ddos tcp-connection-flood illegal-session-check packet-min-number 1 interval 5
anti-ddos tcp-connection-flood illegal-session-check illegal-session-num 3 interval 5
anti-ddos dns-request-limit source-ip other max-rate 200
anti-ddos first-packet-check tcp
anti-ddos first-packet-check udp interval upper-limit 2000
anti-ddos first-packet-check dns interval upper-limit 5000
anti-ddos first-packet-check syn interval lower-limit 500 upper-limit 4000
anti-ddos first-packet-check syn-ack interval lower-limit 500 upper-limit 4000
anti-ddos filter attack alert-rate 1000
anti-ddos source-port statistic enable
```

```
#
ddos-zone name zone_12
zone-id 12
ip address 20.20.9.0 24
anti-ddos destination-ip session-limit protocol tcp max-speed 400000
anti-ddos destination-ip session-limit protocol udp max-speed 10000
anti-ddos destination-ip session-limit protocol other max-speed 10000
bandwidth-limit destination-ip type udp max-speed 50000
bandwidth-limit destination-ip type icmp max-speed 500
bandwidth-limit destination-ip type tcp-fragment max-speed 10000
bandwidth-limit destination-ip type udp-fragment max-speed 10000
bandwidth-limit destination-ip type other max-speed 100000
anti-ddos rst-flood session-check
anti-ddos syn-flood source-detect mode advanced
anti-ddos tcp-abnormal-flood alert-rate 500
anti-ddos syn-flood source-limit max-number 50 duration 3
anti-ddos dns format-check alert-rate 500
anti-ddos dns-request-flood source-detect
anti-ddos ack-flood session-check
anti-ddos ack-flood source-rate-check 500
anti-ddos udp-flood fingerprint-learn enable
anti-ddos udp-malformed-flood alert-rate 500
anti-ddos udp-flood defend alert-speed 500
anti-ddos https-flood defend alert-rate 20000
anti-ddos https-flood ssl-defend illegal-session-num 3 interval 5
anti-ddos https-flood ssl-defend incomplete-negotiation enable
anti-ddos tls-flood large-resource resource-size 100 illegal-ratio 90 min-number 50 interval 5
anti-ddos tls-flood fixed-resource illegal-ratio 90 min-number 20 interval 5
anti-ddos tls-flood concurrent-connection alert-number 10000
anti-ddos http-flood defend alert-request 5000
    anti-ddos http-flood detect-uri source-statistic illegal-ratio 90 min-number 20 interval 5
anti-ddos http-flood detect-uri index 1 uri / full-matching
anti-ddos http-flood slow-attack-check content-length 1000
anti-ddos http-flood large-resource resource-size 100 illegal-ratio 90 min-number 50 interval 5
anti-ddos http-flood illegal-session-check
anti-ddos http-flood illegal-session-check null-method-check enable
anti-ddos http-flood illegal-session-check range-header-check enable
anti-ddos http-flood illegal-session-check multi-method-check enable
anti-ddos http-flood concurrent-connection alert-number 10000
anti-ddos tcp-connection-flood alert-number 20000
anti-ddos tcp-connection-flood alert-rate 5000
anti-ddos tcp-connection-flood illegal-session-check packet-min-number 1 interval 5
anti-ddos tcp-connection-flood illegal-session-check illegal-session-num 3 interval 5
dynamic-blacklist-mode auto
anti-ddos dns-request-limit source-ip other max-rate 200
apply anti-ddos filter name test preference 1
anti-ddos first-packet-check tcp
anti-ddos first-packet-check udp interval upper-limit 2000
```

```
anti-ddos first-packet-check dns interval upper-limit 5000
anti-ddos first-packet-check syn interval lower-limit 500 upper-limit 4000
anti-ddos first-packet-check syn-ack interval lower-limit 500 upper-limit 4000
anti-ddos filter attack alert-rate 1000
anti-ddos feature-log enable
anti-ddos source-port statistic enable
#
ddos-zone name zone_13
zone-id 13
ip address 20.20.8.0 24
anti-ddos destination-ip session-limit protocol tcp max-speed 400000
anti-ddos destination-ip session-limit protocol udp max-speed 10000
anti-ddos destination-ip session-limit protocol other max-speed 10000
bandwidth-limit destination-ip type udp max-speed 50000
bandwidth-limit destination-ip type icmp max-speed 500
bandwidth-limit destination-ip type tcp-fragment max-speed 10000
bandwidth-limit destination-ip type udp-fragment max-speed 10000
bandwidth-limit destination-ip type other max-speed 100000
anti-ddos rst-flood session-check
anti-ddos syn-flood source-detect mode advanced
anti-ddos tcp-abnormal-flood alert-rate 500
anti-ddos syn-flood source-limit max-number 50 duration 3
anti-ddos dns format-check alert-rate 500
anti-ddos dns-request-flood source-detect
anti-ddos ack-flood session-check
anti-ddos ack-flood source-rate-check 500
anti-ddos udp-flood fingerprint-learn enable
anti-ddos udp-malformed-flood alert-rate 500
anti-ddos udp-flood defend alert-speed 500
anti-ddos https-flood defend alert-rate 20000
anti-ddos https-flood ssl-defend illegal-session-num 3 interval 5
anti-ddos https-flood ssl-defend incomplete-negotiation enable
anti-ddos tls-flood large-resource resource-size 100 illegal-ratio 90 min-number 50 interval 5
anti-ddos tls-flood fixed-resource illegal-ratio 90 min-number 20 interval 5
anti-ddos tls-flood concurrent-connection alert-number 10000
anti-ddos http-flood defend alert-request 5000
anti-ddos http-flood detect-uri source-statistic illegal-ratio 90 min-number 20 interval 5
anti-ddos http-flood detect-uri index 1 uri / full-matching
anti-ddos http-flood slow-attack-check content-length 1000
anti-ddos http-flood large-resource resource-size 100 illegal-ratio 90 min-number 50 interval 5
anti-ddos http-flood illegal-session-check
anti-ddos http-flood illegal-session-check null-method-check enable
anti-ddos http-flood illegal-session-check range-header-check enable
anti-ddos http-flood illegal-session-check multi-method-check enable
anti-ddos http-flood concurrent-connection alert-number 10000
anti-ddos tcp-connection-flood alert-number 20000
anti-ddos tcp-connection-flood alert-rate 5000
anti-ddos tcp-connection-flood illegal-session-check packet-min-number 1 interval 5
```

```
anti-ddos tcp-connection-flood illegal-session-check illegal-session-num 3 interval 5
dynamic-blacklist-mode auto
anti-ddos dns-request-limit source-ip other max-rate 200
apply anti-ddos filter name test preference 1
anti-ddos first-packet-check tcp
anti-ddos first-packet-check udp interval upper-limit 2000
anti-ddos first-packet-check dns interval upper-limit 5000
anti-ddos first-packet-check syn interval lower-limit 500 upper-limit 4000
anti-ddos first-packet-check syn-ack interval lower-limit 500 upper-limit 4000
anti-ddos filter attack alert-rate 1000
anti-ddos host-traffic-overflow alert-speed 500
anti-ddos feature-log enable
anti-ddos source-port statistic enable
#
ddos-zone name zone_14
zone-id 14
ip address 100.1.36.1 32
anti-ddos destination-ip session-limit protocol tcp max-speed 400000
anti-ddos destination-ip session-limit protocol udp max-speed 10000
anti-ddos destination-ip session-limit protocol other max-speed 10000
bandwidth-limit destination-ip type udp max-speed 50000
bandwidth-limit destination-ip type icmp max-speed 2
bandwidth-limit destination-ip type tcp-fragment max-speed 10000
bandwidth-limit destination-ip type udp-fragment max-speed 10000
bandwidth-limit destination-ip type other max-speed 100000
anti-ddos rst-flood session-check
anti-ddos syn-flood source-detect mode advanced
anti-ddos tcp-abnormal-flood alert-rate 500
anti-ddos syn-flood source-limit max-number 50 duration 3
anti-ddos dns format-check alert-rate 500
anti-ddos dns-request-flood source-detect
anti-ddos ack-flood session-check
anti-ddos ack-flood source-rate-check 500
anti-ddos udp-flood fingerprint-learn enable
anti-ddos udp-malformed-flood alert-rate 500
anti-ddos udp-flood defend alert-speed 500
anti-ddos https-flood defend alert-rate 20000
anti-ddos https-flood ssl-defend illegal-session-num 3 interval 5
anti-ddos https-flood ssl-defend incomplete-negotiation enable
anti-ddos tls-flood large-resource resource-size 100 illegal-ratio 90 min-number 50 interval 5
anti-ddos tls-flood fixed-resource illegal-ratio 90 min-number 20 interval 5
anti-ddos tls-flood concurrent-connection alert-number 10000
anti-ddos http-flood defend alert-request 5000
anti-ddos http-flood detect-uri source-statistic illegal-ratio 90 min-number 20 interval 5
anti-ddos http-flood detect-uri index 1 uri / full-matching
anti-ddos http-flood slow-attack-check content-length 1000
anti-ddos http-flood large-resource resource-size 100 illegal-ratio 90 min-number 50 interval 5
anti-ddos http-flood illegal-session-check
```

```
anti-ddos http-flood illegal-session-check null-method-check enable
anti-ddos http-flood illegal-session-check range-header-check enable
anti-ddos http-flood illegal-session-check multi-method-check enable
anti-ddos http-flood concurrent-connection alert-number 10000
anti-ddos tcp-connection-flood alert-number 20000
anti-ddos tcp-connection-flood alert-rate 5000
anti-ddos tcp-connection-flood illegal-session-check packet-min-number 1 interval 5
anti-ddos tcp-connection-flood illegal-session-check illegal-session-num 3 interval 5
anti-ddos dns-request-limit source-ip other max-rate 200
anti-ddos first-packet-check tcp
anti-ddos first-packet-check udp interval upper-limit 2000
anti-ddos first-packet-check dns interval upper-limit 5000
anti-ddos first-packet-check syn interval lower-limit 500 upper-limit 4000
anti-ddos first-packet-check syn-ack interval lower-limit 500 upper-limit 4000
anti-ddos filter attack alert-rate 1000
anti-ddos source-port statistic enable
#
firewall zone trust
set priority 85
add interface GE0/0/0
add interface GE0/0/3
add interface GE0/0/4
#
firewall zone untrust
set priority 5
add interface GE0/0/1
add interface GE0/0/2
#
security-policy
default action permit
#
policy-based-route
rule name traffic_injection
ingress-interface GE0/0/1
action pbr egress-interface GE0/0/3 next-hop 192.168.10.29
rule name traffic_injection_sw2
ingress-interface GE0/0/2
action pbr egress-interface GE0/0/4 next-hop 192.168.10.37
rule name traffic_injection_sw1
ingress-interface GE0/0/1
action pbr egress-interface GE0/0/3 next-hop 192.168.10.29
#
return
```


10.5 思考题

除了使用 BGP 协议进行引流以外, 还可以使用什么技术进行引流? 二者在实现机制上有什么区别?

答案: 还可以使用策略路由进行引流。策略路由引流是指在企业出口路由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。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。

11

FireHunter 配置实验

11.1 实验介绍

11.1.1 关于本实验

沙箱技术是防御 APT 的有效手段之一。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，则与沙箱联动的安全设备根据检测结果，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。

为避免 APT 攻击入侵导致公司数据泄露，关键业务停摆。公司总部所有防火墙均与管理中心 FireHunter 设备对接，便于及时检测各类可疑文件，识别网络中传输的恶意文件和 C&C 攻击，有效避免未知威胁攻击的扩散和企业核心信息资产损失。

11.1.2 实验组网介绍

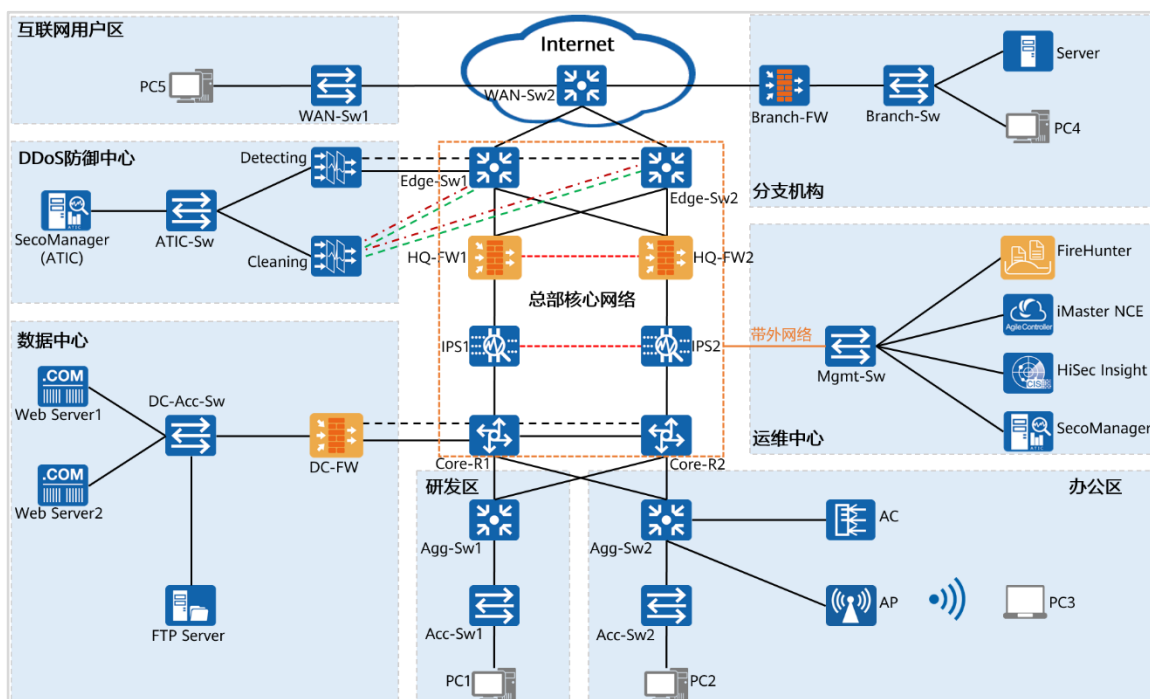


图11-1 实验拓扑图

11.1.3 实验规划

企业总部出口防火墙及数据中心边界防火墙均与运维中心 FireHunter 设备进行安全联动，便于及时检测各类可疑文件，识别网络中传输的恶意文件和 C&C 攻击，有效避免未知威胁攻击的扩散和企业核心信息资产损失。

本实验中，防火墙和沙箱之间采用带外管理网（已预配）对接，具体网络参数如下：

表11-1 基础网络参数规划

设备	配置项	数据
HQ-FW1	对接接口	GE0/0/5
	IP地址	172.21.10.51/17
HQ-FW2	对接接口	GE0/0/5
	IP地址	172.21.10.52/17
DC-FW	对接接口	GE0/0/5
	IP地址	172.21.10.53/17
FireHunter	对接接口	ETH1
	IP地址	172.21.10.74/17

本实验需用到 Web 管理方式配置设备，具体设备相关的 Web 登录参数如下表所示：

表11-2 设备登录参数

设备	登录地址	账号信息	说明
HQ-FW1	https://172.21.10.21:8443	Webuser/Admin@123	——
HQ-FW2	https://172.21.10.22:8443	Webuser/Admin@123	——
DC-FW	https://172.21.10.23:8443	Webuser/Admin@123	——
FireHunter	https://172.21.10.74:32229	admin/Security@123	业务面
	https://172.21.10.74:32230	admin/Security@123	运维面

11.2 实验配置任务

11.2.1 配置思路

1. 登录沙箱 Web 管理界面，配置沙箱对接参数（API Key 和设备证书），便于防火墙与沙箱对接。
2. 配置安全策略，确保本地沙箱和防火墙可以正常通信。
3. 防火墙配置本地沙箱参数，完成与本地沙箱对接。
4. 防火墙中配置 APT 防御配置文件，将特定类型的文件上送至沙箱检测。
5. 配置在安全策略中调用 APT 防御配置文件，激活 APT 防御配置文件。

11.2.2 配置步骤

步骤 1 配置对接参数

登录 FireHunter 运维面（地址：https://172.21.10.74:32230/，账号：admin/Security@123），选择“运维 > 通信 API Key”。API Key 用于 FireHunter 校验联动设备的身份，管理员需要在联动设备上设置相同的 API Key。原 API Key 为：“Huawei12#\$FireHunter”，本案例设置为：“Huawei@FireHunter@123”。

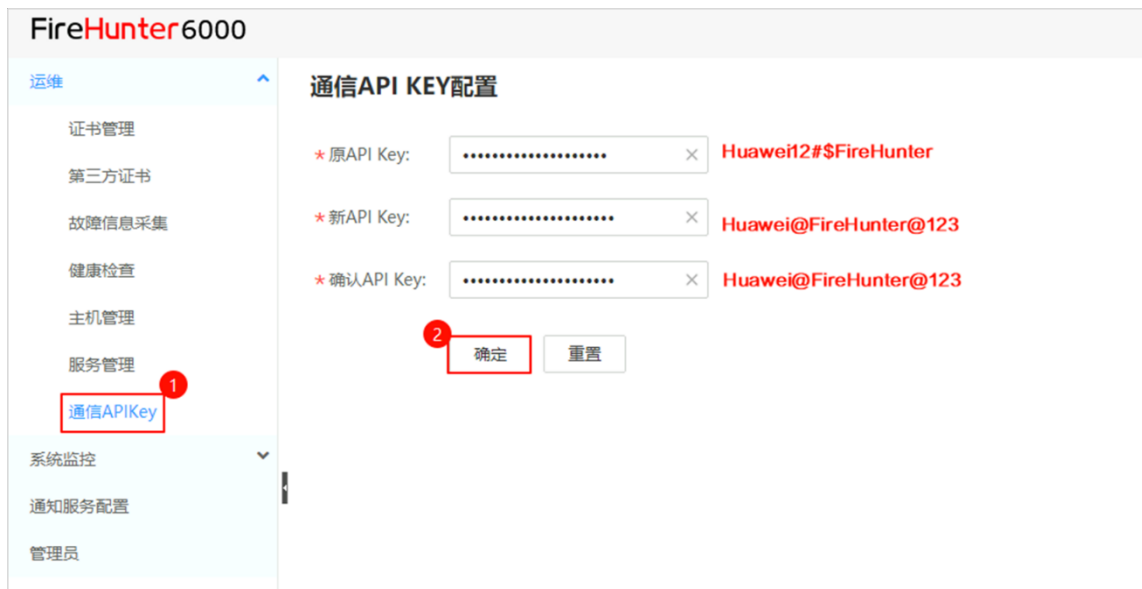


图11-2 配置通信 API KEY

选择“运维 > 证书管理”，单击“导出 > cer”，将 FireHunter 的服务证书下载到本地（实验跳板机），具体如下所示。当配置防火墙与 FireHunter 联动的设备时，需要导入 FireHunter 的服务证书（浏览器有安全提示时，需手动确定保留证书文件）。



图11-3 导出证书

步骤 2 配置检测内容

登录 FireHunter 业务面（地址：<https://172.21.10.74:32229/>，账号：admin/Security@123）选择“配置 > 检测策略”。按实际业务需求配置检测参数，具体如下所示。

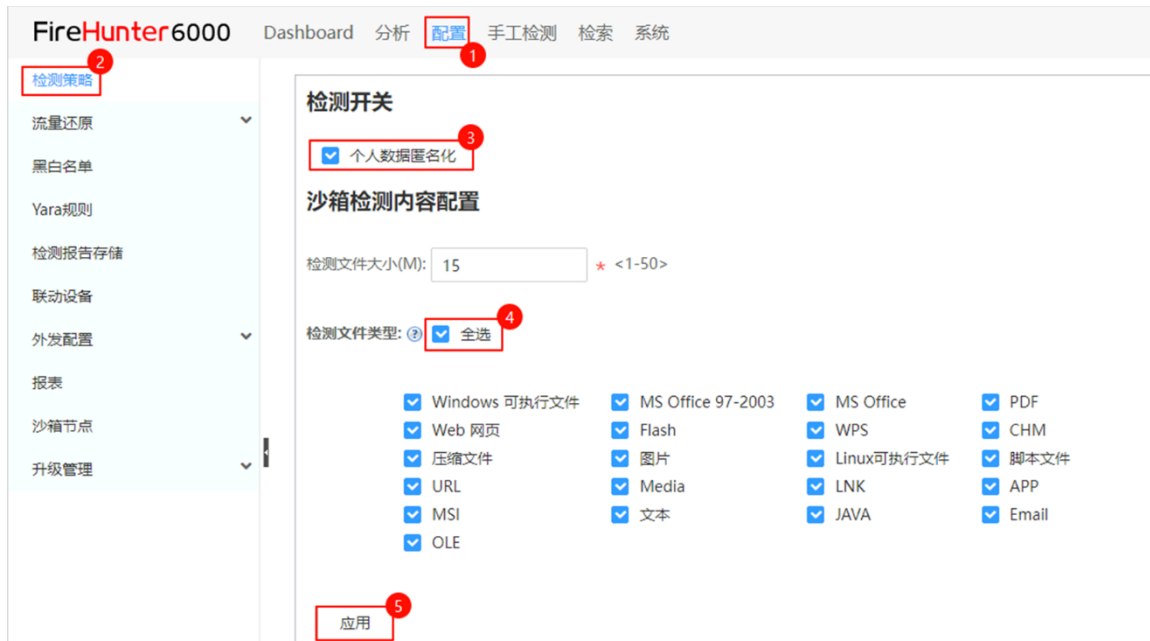


图11-4 配置检测内容

FireHunter 支持设置待检测文件的大小，支持对多种类型的文件进行检测，管理员可以根据现网实际环境选择要检测的文件类型。完成后点击“应用”。

在“文件解压密码配置模块”新增一个文件解压密码“Huawei@123”（实际生产场景中，可根据实际情况自行添加文件解压口令），具体操作如下：

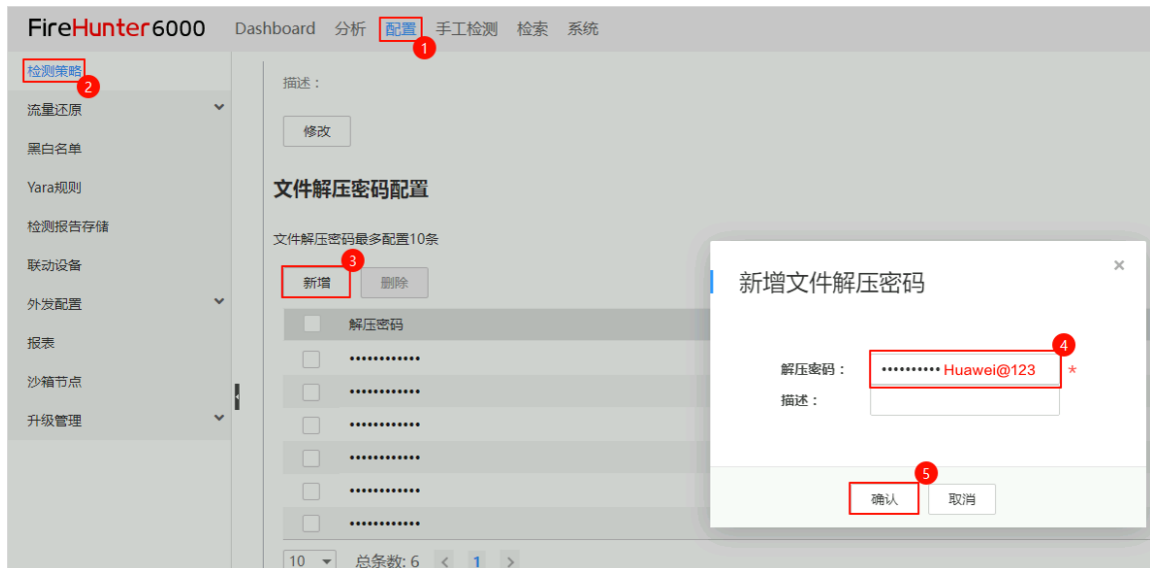


图11-5 新增文件解压密码

步骤 3 添加联动设备

登录 FireHunter 业务面（地址：<https://172.21.10.74:32229/>，

账号：admin/Security@123）选择“配置 > 联动设备”。单击“添加”，之后输入 HQ-FW1 的对接 IP 地址，具体如下所示：

添加 HQ-FW1



图11-6 添加联动设备

添加 HQ-FW2 和 DC-FW 步骤同上，对接地址参考“基础网络参数规划表”，添加完成后如下：



图11-7 联动设备列表

步骤 4 防火墙安全策略

在出口防火墙与数据中心边界防火墙上配置安全策略放行防火墙与沙箱的双向流量，确保沙箱和防火墙可以联动成功。

登录 HQ-FW1 设备 Web 管理界面（地址：https://172.21.10.21:8443/，账号：Webuser/Admin@123），选择“策略 > 安全策略 > 安全策略 > 新建安全策略”，进入安全策略创建页面，执行如下操作：

新建安全策略

概述

* 名称: sandbox

描述:

策略组: -- NONE --

条件

① 当前未加载地区识别特征库。如需配置地区，请 加载地区识别特征库

源

安全区域: mgmt_zone × local ×

IP 地址/地区 ②: 172.21.10.51 × 172.21.10.52 × 172.21.10.74 ×

目的

目的类型: ☒ 安全区域 ☐ 虚拟服务

安全区域: mgmt_zone × local ×

IP 地址/地区 ②: 172.21.10.51 × 172.21.10.52 × 172.21.10.74 ×

服务 ②

协议: 请选择服务

更多 ▾ 应用/用户/安全组/时间段/VLAN ID

动作

动作: ☒ 允许 ☐ 禁止

内容安全检查 ▾ 反病毒/入侵防御/URL过滤/内容过滤

取消 命令预览 确定

图11-8 HQ-FW1 创建与沙箱对接的安全策略

HQ-FW2 设备会通过 HRP 自动同步安全策略，无需单独配置。

登录 DC-FW 设备 Web 管理界面（地址：<https://172.21.10.23:8443/>，账号：Webuser/Admin@123），选择“策略 > 安全策略 > 安全策略 > 新建安全策略”，进入安全策略创建页面，执行如下操作：

图11-9 DC-FW 创建与沙箱对接的安全策略

步骤 5 配置防火墙侧对接参数

登录 HQ-FW1 设备 Web 管理界面（地址：https://172.21.10.21:8443/，账号：Webuser/Admin@123），选择“对象 > 安全配置文件 > 反病毒 > 沙箱联动配置 > 本地沙箱”。输入沙箱地址并导入沙箱 CA 证书，证书详见“步骤 1”。

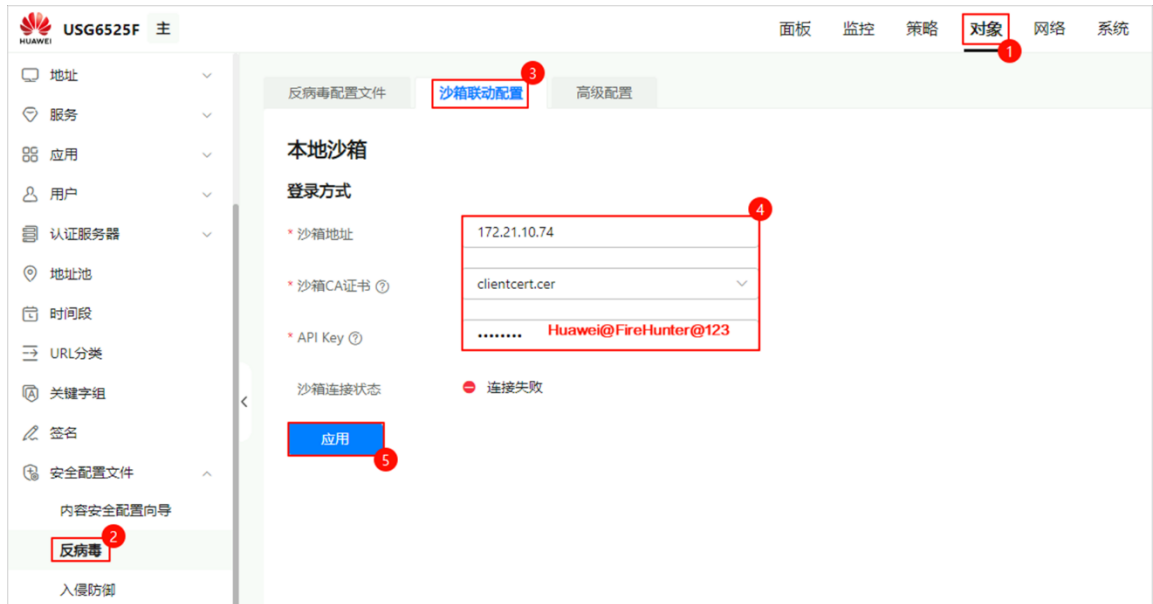


图11-10 HQ-FW1 本地沙箱对接参数配置

说明：若此处沙箱 CA 证书已经上传至防火墙设备本地，则直接选择即可，无需二次上传。
完成上述参数配置后，点击“应用”，稍等片刻后，可发现沙箱连接状态会切换为“连接成功”。

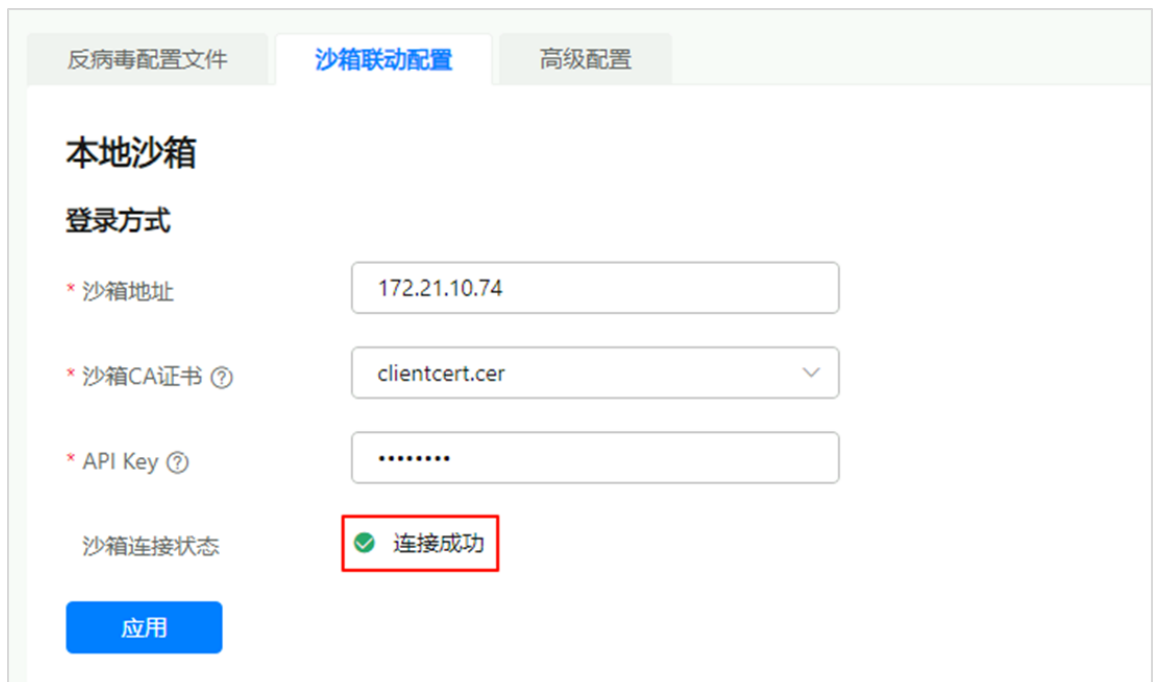


图11-11 沙箱连接成功

DC-FW 执行上述相同操作，确保与沙箱对接成功。
完成防火墙设备侧沙箱对接参数的配置后，返回登录 FireHunter 业务面（地址：<https://172.21.10.74:32229/>，
账号：admin/Security@123），选择“配置 > 联动设备”。可以看到之前添加的防火墙设备，连接状态已经 OK。



图11-12 设备联动结果

步骤 6 创建 APT 防御配置文件

登录 HQ-FW1 设备 Web 管理界面（地址：<https://172.21.10.21:8443/>，账号：Webuser/Admin@123），选择“对象 > 安全配置文件 > 反病毒 > 反病毒配置文件 > 新建”，进入反病毒配置文件创建界面，执行以下操作：



图11-13 HQ-FW1 创建 APT 防御配置文件

上述配置文件创建完成后, 效果如下:



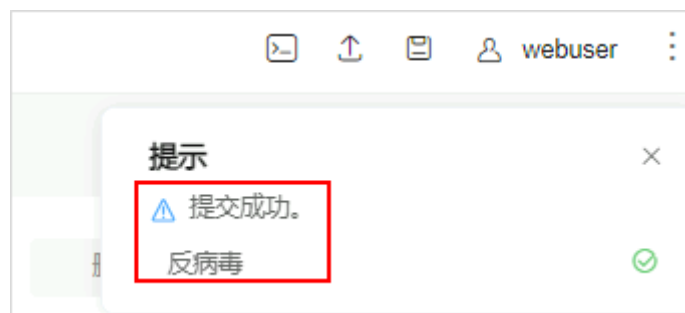
图11-14 反病毒配置文件查看

新的反病毒配置文件创建完成后，需要根据系统提示，在页面右上角提交反病毒配置：



提交反病毒配置文件

点击提交按钮后，在系统提示消息上选择“确认”并等待提交成功，提交成功后效果如下：



反病毒配置文件提交成功

HQ-FW2 设备会通过 HRP 自动同步上述配置，无需单独配置。

登录 DC-FW 设备 Web 管理界面（地址：https://172.21.10.23:8443/，账号：Webuser/Admin@123），执行上述相同操作。

步骤 7 引用 APT 防御配置文件

登录 HQ-FW1 设备 Web 管理界面（地址：https://172.21.10.21:8443/，账号：Webuser/Admin@123），选择“策略 > 安全策略”，进入安全策略查看页面，在所有业务安全策略（“ipsec_oa”、“sslvpn_oa”、“HQ_Web_Server”）中调用刚才创建的“Local_Sandbox”反病毒配置文件。

以“ipsec_oa”安全策略的操作为例演示 APT 防御配置文件的调用。在 HQ-FW1 设备安全策略查看页面点击“ipsec_oa”安全策略进行策略编辑，调用“Local_Sandbox”反病毒配置文件。

序号	名称	源	目的	服务
1	ipsec_ike	local untrust 100.1.33.1/255.255.255.255 100.1.35.3/255.255.255.255	local untrust 100.1.33.1/255.255.255.255 100.1.35.3/255.255.255.255	any
2	ipsec_oa	trust untrust 192.168.11.0/255.255.255.0 192.168.14.0/255.255.255.0	trust untrust 192.168.11.0/255.255.255.0 192.168.14.0/255.255.255.0	any
3	sslvpn_gw	untrust 100.1.15.0/255.255.255.0	local any	any

图11-15 进入“ipsec_oa”安全策略修改界面

动作

动作 1 允许 禁止

内容安全检查 ^

引用安全配置文件会导致设备性能一定程度的下降。

反病毒 2 Local_Sandbox

入侵防御 -- NONE --

URL过滤 -- NONE --

内容过滤 Content_Filter

取消 命令预览 3 确定

图11-16 “ipsec_oa”安全策略调用APT防御配置文件

在 HQ-FW1 设备的“sslvpn_oa”和“HQ_Web_Server”安全策略中均执行上述操作，调用反病毒配置文件“Local_Sandbox”。执行完成后效果如下：

序号	名称	源	目的	服务	应用	时间域	动作	内容安全
1	ipsec_ike	local untrust 100.1.33.1/255.255.255.255 100.1.35.3/255.255.255.255	local untrust 100.1.33.1/255.255.255.255 100.1.35.3/255.255.255.255	any	any		允许	
2	ipsec_oa	trust untrust 192.168.11.0/255.255.255.0 192.168.14.0/255.255.255.0	trust untrust 192.168.11.0/255.255.255.0 192.168.14.0/255.255.255.0	any	any		允许	AV DLP
3	sslvpn_gw	untrust 100.1.15.0/255.255.255.0	local any	any	any		允许	
4	sslvpn_oa	untrust 192.168.11.0/255.255.255.0	trust 192.168.16.0/255.255.255.0	http	any		允许	AV DLP
5	HQ_Web_Server	untrust any	trust 192.168.16.109/255.255.255...	any	any		允许	AV
6	sandbox	local mgmt_zone 172.21.10.51/255.255.255.255 172.21.10.42/24	local mgmt_zone 172.21.10.51/255.255.255.255 172.21.10.42/24	any	any		允许	

图11-17 HQ-FW1 设备反病毒配置文件调用情况概览

HQ-FW2 设备会通过 HRP 自动同步上述配置，无需单独配置。

登录 DC-FW 设备 Web 管理界面（地址：<https://172.21.10.23:8443/>，账号：Webuser/Admin@123），执行上述相同操作，DC-FW 设备上涉及到的业务安全策略有：“sslvpn_oa”、“nat64”和“slb”。执行完成后效果如下：

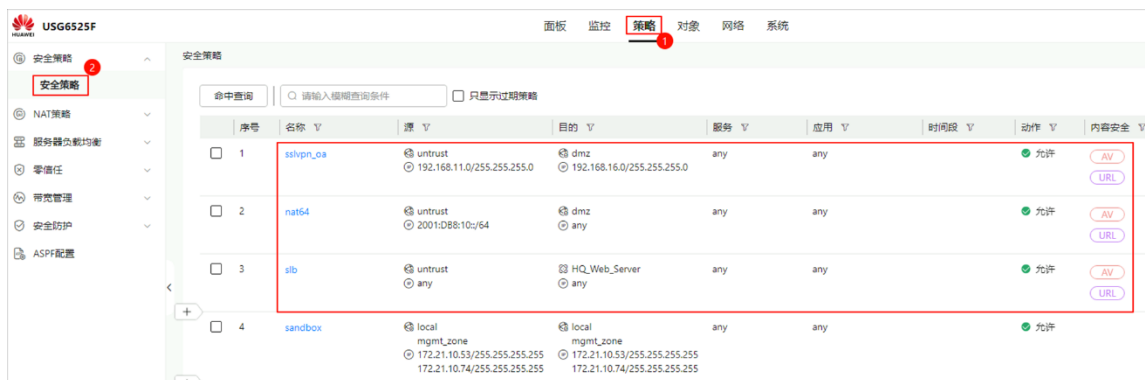


图11-18 DC-FW 设备反病毒配置文件调用情况概览

11.3 结果验证

使用 RDP 登录 PC5 (地址: 172.21.10.205, 账号: admin/Huawei123!), 在成功接入 SSL VPN 后, 打开资源管理器连接企业总部 FTP 服务器, 并将桌面上的“沙箱测试文件”压缩包上传至企业总部 FTP 服务器:

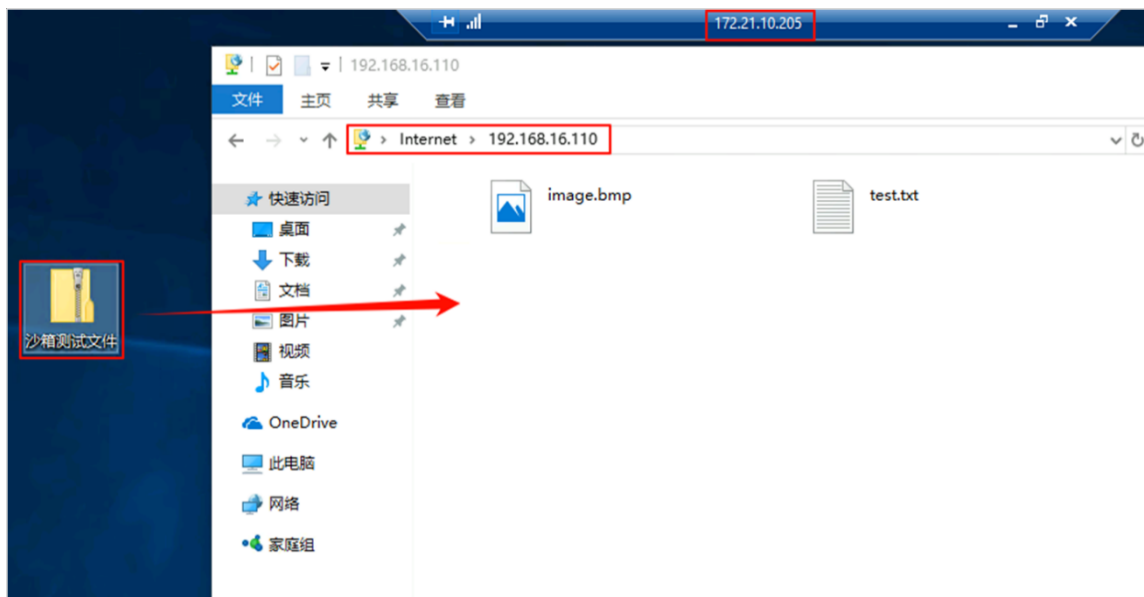


图11-19 PC5 通过 FTP 传输沙箱测试文件

完成上述文件传输操作后, 登录 FireHunter 业务面 (地址: [https:// 172.21.10.74:32229/](https://172.21.10.74:32229/), 账号: admin/Security@123) 选择“配置 > 联动设备”进入联动设备查看界面, 可以发现, 已有设备提交了检测任务:

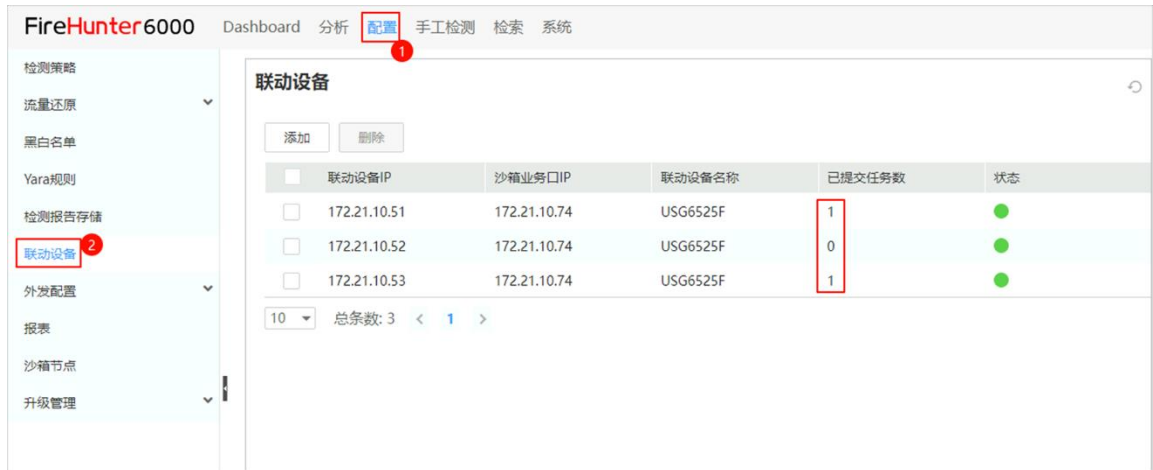


图11-20 查看联动设备提交任务数

继续在 FireHunter 业务面选择“分析 > 文件检测”查看文件检测结果：

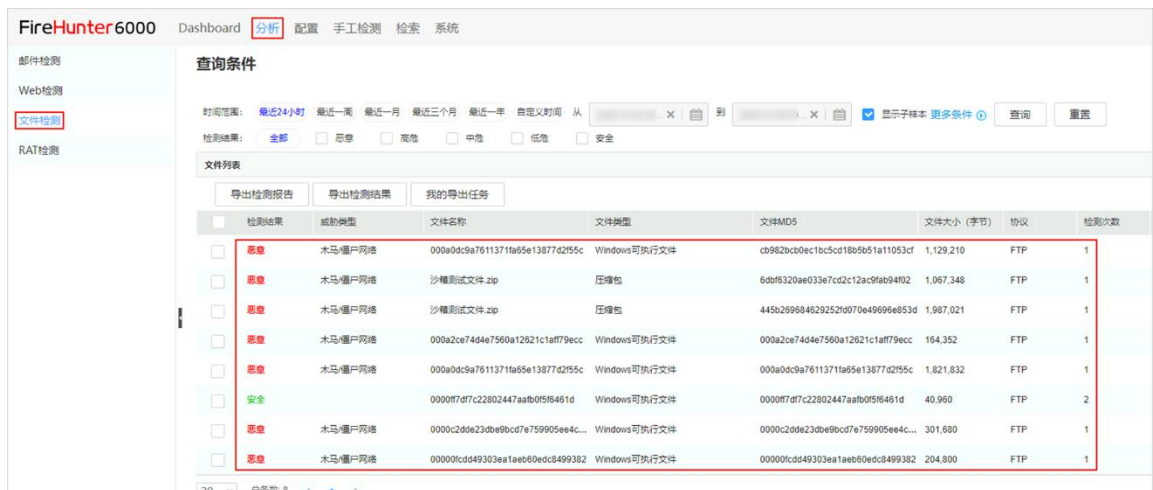


图11-21 查看文件检结果

在 FireHunter 业务面选择“Dashboard > 检测”查看检测统计信息：

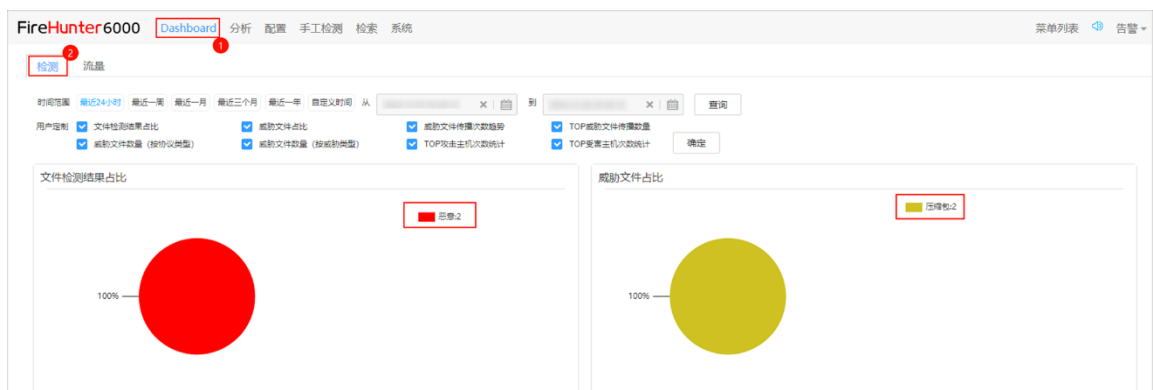


图11-22 查看检测分析结果统计信息

选择一个提交了检测任务的安全联动设备，登录其 Web 管理界面，查看威胁日志，本实验以 HQ-FW1 设备为例演示操作。

登录 HQ-FW1 设备 Web 管理界面（地址：https://172.21.10.21:8443/，账号：Webuser/Admin@123），选择“监控 > 日志 > 威胁日志”，查看设备威胁日志：



The screenshot displays the Huawei USG6525F Web Management Interface. The top navigation bar includes '面板', '监控' (highlighted with a red circle 1), '策略', '对象', '网络', and '系统'. The left sidebar shows the '日志' (Logs) section, with '威胁日志' (Threat Log) highlighted (red circle 2). The main area shows the '威胁日志列表' (Threat Log List) with a table containing one entry. A red circle 3 highlights the '查看' (View) icon for this entry.

The '威胁日志详情' (Threat Log Details) window is open, showing the following information:

威胁		源	目的
威胁类型	沙箱	安全区域	untrust
威胁名称	沙箱测试文件.zip	地址	192.168.11.245 192.168.16.110
威胁ID		端口	50706 49888
次数	1	NAT地址	
配置文件	Local_Sandbox	NAT端口	
动作	告警	源用户	
文件名称	沙箱测试文件.zip	XFF	
文件类型	zip		
攻击阶段			
访问内容			
文件MD5	445b269684629252fd070e49696e853d		

The '日志公共字段' (Log Common Fields) section shows the following details:

日志公共字段	值
时间	20:31:06
应用类别	
应用子类别	
应用	FTP
安全策略	sslvpn_oa

The '关闭' (Close) button is located at the bottom right of the details window.

图11-23 查看 HQ-FW1 设备威胁日志

11.4 配置参考（仅展示本实验相关配置）

11.4.1 HQ-FW1 的配置

```
#
profile type av name Local_Sandbox
  sandbox-detect enable
  file-reputation-detect enable
#
security-policy
  rule name ipsec_oa
    source-zone trust
    source-zone untrust
    destination-zone trust
    destination-zone untrust
    source-address 192.168.11.0 mask 255.255.255.0
    source-address 192.168.14.0 mask 255.255.255.0
    destination-address 192.168.11.0 mask 255.255.255.0
    destination-address 192.168.14.0 mask 255.255.255.0
    profile av Local_Sandbox
    profile data-filter Content_Filter
    action permit
  rule name sslvpn_oa
    source-zone untrust
    destination-zone trust
    source-address 192.168.11.0 mask 255.255.255.0
    destination-address 192.168.16.0 mask 255.255.255.0
    service ftp
    service http
    profile av Local_Sandbox
    profile data-filter Content_Filter
    action permit
  rule name HQ_Web_Server
    source-zone untrust
    destination-zone trust
    destination-address 192.168.16.109 mask 255.255.255.255
    profile av Local_Sandbox
    action permit
  rule name sandbox
    source-zone local
    source-zone mgmt_zone
    destination-zone local
    destination-zone mgmt_zone
    source-address 172.21.10.51 mask 255.255.255.255
    source-address 172.21.10.52 mask 255.255.255.255
    source-address 172.21.10.74 mask 255.255.255.255
    destination-address 172.21.10.51 mask 255.255.255.255
```

```
destination-address 172.21.10.52 mask 255.255.255.255
destination-address 172.21.10.74 mask 255.255.255.255
action permit
#
security-telemetry
collect apt-file
destination-group sandbox
ca-certificate clientcert.cer
ipv4-address 172.21.10.74 port 5002
sensor-group sandbox
select apt-file
subscription sandbox
destination-group sandbox
sensor-group sandbox
api-key Huawei@FireHunter@123
#
return
```

11.4.2 DC-FW 的配置

```
#
profile type av name Local_Sandbox
sandbox-detect enable
file-reputation-detect enable
#
security-policy
rule name sslvpn_oa
source-zone untrust
destination-zone dmz
source-address 192.168.11.0 mask 255.255.255.0
destination-address 192.168.16.0 mask 255.255.255.0
profile av Local_Sandbox
profile url-filter URL_Filter
action permit
rule name nat64
source-zone untrust
destination-zone dmz
source-address 2001:DB8:10:: 64
profile av Local_Sandbox
profile url-filter URL_Filter
action permit
rule name slb
source-zone untrust
vserver HQ_Web_Server
profile av Local_Sandbox
profile url-filter URL_Filter
action permit
rule name sandbox
```

```
source-zone local
source-zone mgmt_zone
destination-zone local
destination-zone mgmt_zone
source-address 172.21.10.53 mask 255.255.255.255
source-address 172.21.10.74 mask 255.255.255.255
destination-address 172.21.10.53 mask 255.255.255.255
destination-address 172.21.10.74 mask 255.255.255.255
actionn permit
#
security-telemetry
collect apt-file
destination-group sandbox
ca-certificate clientcert.cer
ipv4-address 172.21.10.74 port 5002
sensor-group sandbox
select apt-file
subscription sandbox
destination-group sandbox
sensor-group sandbox
api-key Huawei@FireHunter@123
#
return
```

11.5 思考题

FireHunter 设备通常会部署在哪些位置，起到什么作用？

答案：

互联网边界出口：重点防范来自互联网的恶意邮件、恶意 Web 流量攻击等。

分支接入边界：避免恶意文件在外联接入区域扩散，在分支总部之间任意扩散。

核心部门边界：防范内网恶意文件传播、共享，防止横向感染核心部门。

数据中心边界：重点保护服务器等核心资产，防范内网潜伏的攻击、恶意扫描，渗透等。

12 HiSec Insight 配置实验

12.1 实验介绍

12.1.1 关于本实验

HiSec Insight 是基于大数据的 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，实现组织内部的全网安全态势感知。

12.1.2 实验组网介绍

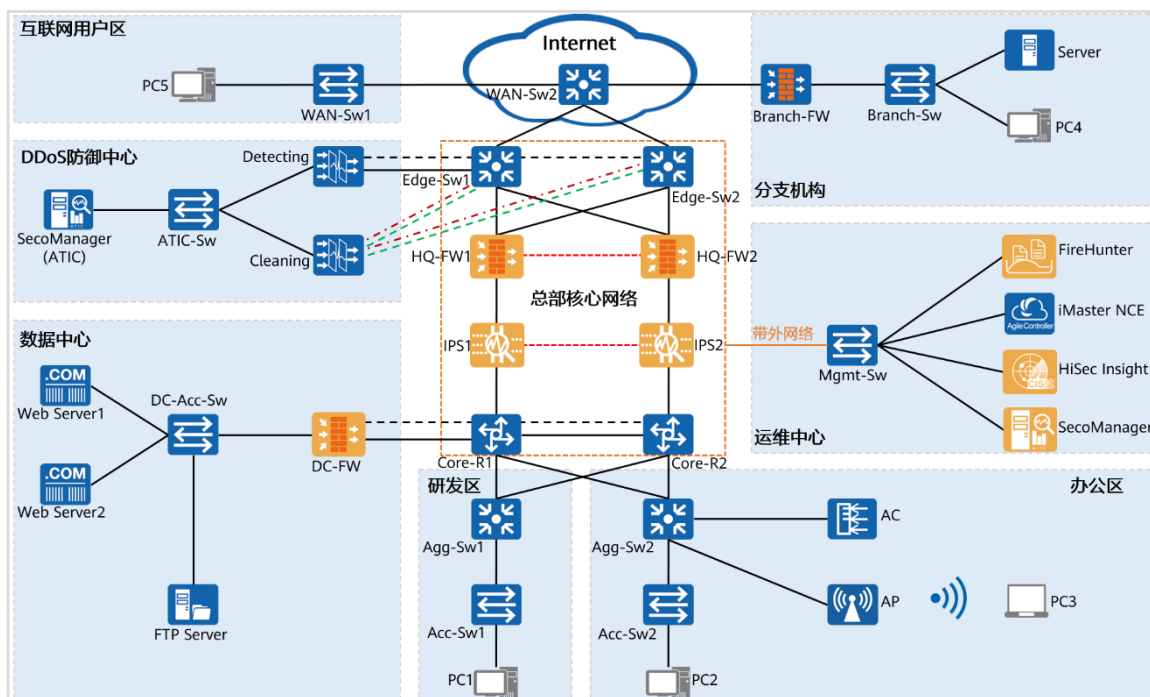


图12-1 实验拓扑图

12.1.3 实验规划

本实验通过可视化/流探针/采集器三合一主机形式部署 HiSec Insight，并通过带外管理网络和其余网络安全设备对接，详细规划如下：

1. 所有企业总部的防火墙将 Dataflow 日志发送给 HiSec Insight 采集器，HiSec Insight 采集器对日志做预处理，并上报给 HiSec Insight 分析模块进行分析检测。
2. FireHunter 将威胁日志发送给 HiSec Insight，用于大数据安全分析和威胁展示等。
3. 当 HiSec Insight 分析并判定威胁事件后，会根据策略调用 SecoManager 的北向接口，通过 SecoManager 实现对恶意流量的阻断或隔离，实现安全联动和响应。

表12-1 对接网络参数设计

设备	配置项	数据
HQ-FW1	对接接口	GE0/0/5
	IP地址	172.21.10.51/17
HQ-FW2	对接接口	GE0/0/5
	IP地址	172.21.10.52/17
DC-FW	对接接口	GE0/0/5
	IP地址	172.21.10.53/17
FireHunter	对接接口	ETH2
	IP地址	172.21.10.74/17
SecoManager	对接接口	ETH2
	IP地址	172.21.10.71/17
HiSec Insight	对接接口	ETH2
	IP地址	172.21.10.80/17

12.2 实验配置任务

12.2.1 配置思路

1. 配置总部所有防火墙设备的日志外发参数，并配置安全策略放行日志外发。
2. 设置 FireHunter 日志外发参数。
3. 在 HiSec Insight 侧创建针对防火墙和 FireHunter 设备的日志接收任务。
4. 配置 SecoManager 与 HiSec Insight 安全联动。

12.2.2 配置步骤

步骤 1 防火墙日志输出设置

登录 HQ-FW1 设备 Web 管理界面（地址：<https://172.21.10.21:8443>，账号：Webuser/Admin@123），选择“系统 > 日志配置 > 日志配置”，进入日志配置页面，执行如下操作：

说明：日志加密传输的密码统一设置为“Huawei@123”。



图12-2 HQ-FW1 日志输出设置

登录 HQ-FW2 设备 Web 管理界面（地址：<https://172.21.10.22:8443>，账号：Webuser/Admin@123），选择“系统 > 日志配置 > 日志配置”，进入日志配置页面，执行如下操作：

说明：若处在双机热备系统的备份设备 HQ-FW2 无法进行此项配置，可以通过命令“hrp standby config enable”开启备机的配置功能，再执行以下操作。



图12-3 HQ-FW2 日志输出设置

登录 DC-FW 设备 Web 管理界面（地址：<https://172.21.10.23:8443>，账号：Webuser/Admin@123），选择“系统 > 日志配置 > 日志配置”，进入日志配置页面，执行如下操作：



图12-4 DC-FW 日志输出设置

步骤 2 防火墙安全策略配置

登录 HQ-FW1 设备 Web 管理界面（地址：https://172.21.10.21:8443，账号：Webuser/Admin@123），选择“策略 > 安全策略 > 安全策略 > 新建安全策略”，进入安全策略创建页面，执行如下操作：

新建安全策略

^ 概述

* 名称: HiSecInsight

描述:

策略组: -- NONE --

^ 条件

① 当前未加载地区识别特征库。如需配置地区，请 加载地区识别特征库

源

安全区域: local, mgmt_zone

IP 地址/地区: 172.21.10.51, 172.21.10.52, 172.21.10.80

目的

目的类型: ☒ 安全区域 ☐ 虚拟服务

安全区域: mgmt_zone, local

IP 地址/地区: 172.21.10.51, 172.21.10.52, 172.21.10.80

服务

协议: 请选择服务

更多 > 应用/用户/安全组/时间段/VLAN ID

^ 动作

动作: ☒ 允许 ☐ 禁止

内容安全检查 > 反病毒/入侵防御/URL过滤/内容过滤

取消 命令预览 确定

图12-5 HQ-FW1 创建与 HiSec Insight 对接的安全策略

HQ-FW2 设备会通过 HRP 自动同步上述安全策略，无需单独配置。

登录 DC-FW 设备 Web 管理界面（地址：https://172.21.10.23:8443，账号：Webuser/Admin@123），选择“策略 > 安全策略 > 新建 > 新建安全策略”，进入安全策略创建页面，执行如下操作：

新建安全策略

概述

* 名称

HiSecinsight

描述

策略组

-- NONE --

条件

① 当前未加载地区识别特征库。如需配置地区，请 加载地区识别特征库

源

安全区域

mgmt_zone local

IP 地址/地区 ②

172.21.10.53 172.21.10.80

目的

1↓

目的类型

☒ 安全区域 ☐ 虚拟服务

安全区域

local mgmt_zone

IP 地址/地区 ②

172.21.10.53 172.21.10.80

服务 ③

协议

请选择服务

更多

应用/用户/安全组/时间段/VLAN ID

动作

动作

☒ 允许 ☐ 禁止

内容安全检查

反病毒/入侵防御/URL过滤/内容过滤

取消

命令预览

确定

图12-6 DC-FW 创建与 HiSec Insight 对接的安全策略

步骤 3 FireHunter 日志输出设置

登录 FireHunter 业务面（地址：<https://172.21.10.74:32229/>，

账号：admin/Security@123）选择“配置 > 外发配置 > 检测日志外发”，执行如下操作：

FireHunter 6000 Dashboard 分析 **配置** 手工检测 检索 系统

检测策略
流量还原
黑白名单
Yara规则
检测报告存储
联动设备
外发配置
检测日志外发
邮件告警外发
报表
沙箱节点
升级管理

检测日志外发

本系统与日志服务器连接的加密方式由服务端决定，选择TLSv1.2加密连接时，需要确保服务端提供了TLSv1.2安全

⚠️ 启用日志外发功能前请先确认日志服务器地址配置合法合规

日志外发：☒ 启用

服务器IP: 172.21.10.80 * 服务器端口: 514 * (1-65535)

日志格式: 采集器格式 * 使用协议: UDP * 选择证书:

威胁级别:
☒ 全选
☒ 低危 ☒ 中危 ☒ 高危 ☒ 恶意

应用

图12-7 FireHunter 日志输出设置

步骤 4 创建防火墙日志接收任务

登录 HiSec Insight 的运维面（地址：<https://172.21.10.80:31943>，账号：admin/Security@123），点击“数据接入 > 日志接入 > 日志接入管理 > 创建”，进入日志接入任务创建界面，执行如下操作：

HiSec Insight

[首页](#)
[安全态势](#)
[威胁分析](#)
[检索](#)
[报告与处置](#)
[资产管理](#)
[数据接入](#)

数据接入

日志接入

规则集

采集器管理

流量接入

元数据

选择来源

配置任务基本参数, Syslog格式日志编码格式需为UTF-8。

接入方式:

UDP TCP

任务名称:

USG

只能输入大小写英文字母、数字、下划线和连接符, 且必须以大小写字母开头, 长度不超过50个字符

端口:

9002

范围: 514或者1024~65535

日志源IP:

172.21.10.51,172.21.10.52,172.21.11

172.21.10.51,172.21.10.52,172.21.10.53

示例: 10.1.1.1,10.1.1.2-10.1.1.255

长时间未收到日志发送告警

下一步

图12-8 选择日志来源

UDP/TCP REST

返回

选择来源

输入设置

检查

规则集:

选择规则集作为解析数据的依据。

规则集:

Firewall_Dataflow x

密码:

..... Huawei@123

密码长度: 8~32个字符

选择目标采集器

选择将数据发送到的采集器

采集器IP	运行状态
172.21.10.80	运行

上一步

下一步

图12-9 选择规则集与目标采集器

! UDP通道数据明文传输，存在信息泄露以及篡改的风险，建议优先采用TCP协议接收数据，并设置TLS双向认证。

检查

检查任务基本参数配置

接入方式:	UDP
端口:	9002
日志源IP:	172.21.10.51,172.21.10.52,172.21.10.53
任务名称:	USG
规则集:	Firewall_Dataflow
采集器IP:	172.21.10.80
密码:	*****

上一步
提交

图12-10 检查信息并提交

确认
×

i

创建任务成功，是否启动？确认启动，采集器将根据规则集从设备上报的日志中提取信息。日志中可能包含邮箱名、邮件正文、手机号等个人数据。如必须使用这些数据，请根据当地法律妥善收集处理。

取消
确认

图12-11 确认提交

提交日志接收任务后，在日志接收任务列表启动日志接收任务（如果日志接收任务自动启动，则不需要此步骤）：



图12-12 启动日志接收任务

步骤 5 创建沙箱日志接收任务

登录 HiSec Insight 的运维面（地址：<https://172.21.10.80:31943>，账号：admin/Security@123），点击“数据接入 > 日志接入 > 日志接入管理 > 创建”，进入日志接入任务创建界面，执行如下操作：



图12-13 选择日志来源

UDP/TCP
REST

返回

✓

选择来源

○

输入设置

!

UDP通道数据明文传输，存在信息泄露以及篡改的风险，建议优先采用TCP协议接收数据，并设置TLS双向认证。

规则集:

选择规则集作为解析数据的依据。

规则集:

FireHunter x

选择目标采集器

选择将数据发送到的采集器

✓

采集器IP

运行状态

✓

172.21.10.80

运行

上一步

下一步

图12-14 选择规则集与目标采集器

返回

✓

选择来源

✓

输入设置

○

检查

!

UDP通道数据明文传输，存在信息泄露以及篡改的风险，建议优先采用TCP协议接收数据，并设置TLS双向认证。

检查

检查任务基本参数配置

接入方式:

UDP

端口:

514

日志源IP:

172.21.10.74

任务名称:

FireHunter

规则集:

FireHunter

采集器IP:

172.21.10.80

上一步

提交

图12-15 检查信息并提交

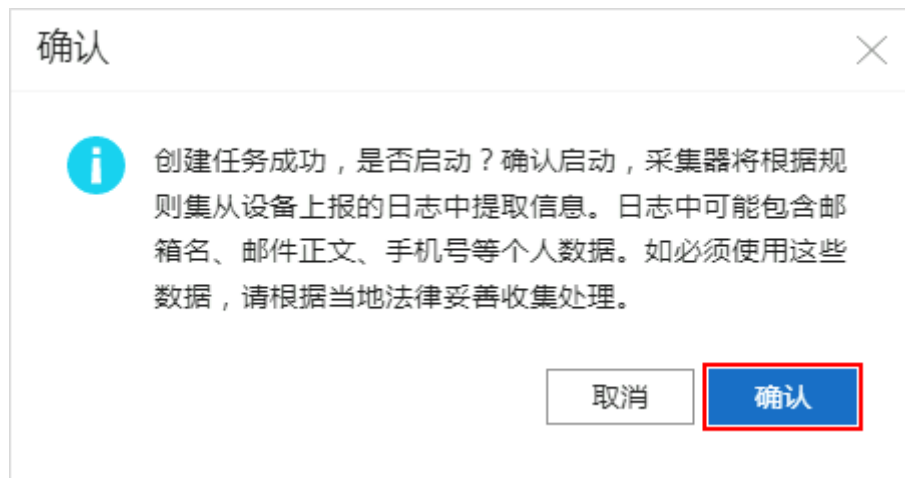


图12-16 确认提交

创建完成后在“数据接入 > 日志接入 > 日志接入管理 > 任务列表”模块应看到如下效果：

图12-17 日志接入任务列表

步骤 6 创建北向用户

登录 SecoManager 系统 Web 管理界面（地址：<https://172.21.10.71:31943/>，账号：admin/Security@123），选择“系统管理 > 用户管理 > 用户管理”，点击“用户”页签，之后点击右边“创建”按钮，执行如下操作：

默认工作组

创建用户

基本信息 所属用户组 选择角色 选择管理对象 访问控制

类型: ① 本地 三方系统接入 远端

* 用户名: ① admin@system.com

用户全名:

* 密码: ① Security@123

* 确认密码: Security@123

手机号码: 国家码/地区码

电子邮箱:

登录欢迎信息:

取消 完成 下一步

默认工作组

创建用户

基本信息 所属用户组 选择角色 选择管理对象 访问控制

请选择所属用户组, 单击 [这里](#) 创建新用户组。

已选用户组 (0)

请输入用户... 刷新

用户组名 描述

暂无数据

取消 完成 上一步 下一步

默认工作组

创建用户

基本信息 所属用户组 选择角色 选择管理对象 访问控制

已选操作/最大可选操作: 1/20

请输入角色名称 收缩 请输入角色名称 清空 删除

角色

☐ Auditor

☐ Deploy Administrator

☐ Design Administrator

☒ Northbound Interface Operator

☐ Operator

☐ Safe Auditor

☐ System Administrator

☐ Tenant Administrator

Northbound Interface Operator

取消 完成 上一步 下一步

创建用户

基本信息 所属用户组 选择角色 选择管理对象 访问控制

管理级别：
租户 设备
* 租户：
+ 选择 选择所属最大资源： 选择

取消 完成 上一步 下一步

创建用户

基本信息 所属用户组 选择角色 选择管理对象 访问控制

请选择登录时间控制策略：

请输入时间策略名 刷新 创建

时间策略	描述	起止日期	每日起止时间	星期
默认策略	默认策略不限制任何时间登录。		00:00 ~ 23:59	星期日, 星期一, 星期二, 星期三, 星期四, 星期五, 星期六

总计: 1 10条/页 1

请选择登录IP地址控制策略：

公共策略 个人策略

登录IP地址控制策略范围: 使用所有登录IP地址控制策略 使用指定登录IP地址控制策略

请输入IP地址 刷新 创建

允许访问的IP地址区间 描述

取消 完成 上一步

图12-18 创建北向对接用户

步骤 7 获取 SecoManager 证书

在 SecoManager 系统 Web 管理界面选择“系统管理 > 证书与 License > 控制器证书管理”，在左侧导航栏选择“服务证书管理”进入证书服务列表页面，选择“APIGWService”。



图12-19 选择服务证书

在 APIGWService 证书列表页面，选择“身份证书”，将“server_chain”证书链导出至本地（实验跳板机）：



图12-20 导出证书链

步骤 8 导入 SecoManager 证书

登录 HiSec Insight 的运维面（地址：https://172.21.10.80:31943，账号：admin/Security@123），点击“系统 > 系统设置 > 证书管理 > 服务证书管理”，在“服务列表”界面，选择“HiSiSOARMgmtService”服务，之后在“HiSiSOARMgmtService 证书列表”界面，选择“信任证书”页签，将上一步导出的证书链进行导入并确认。

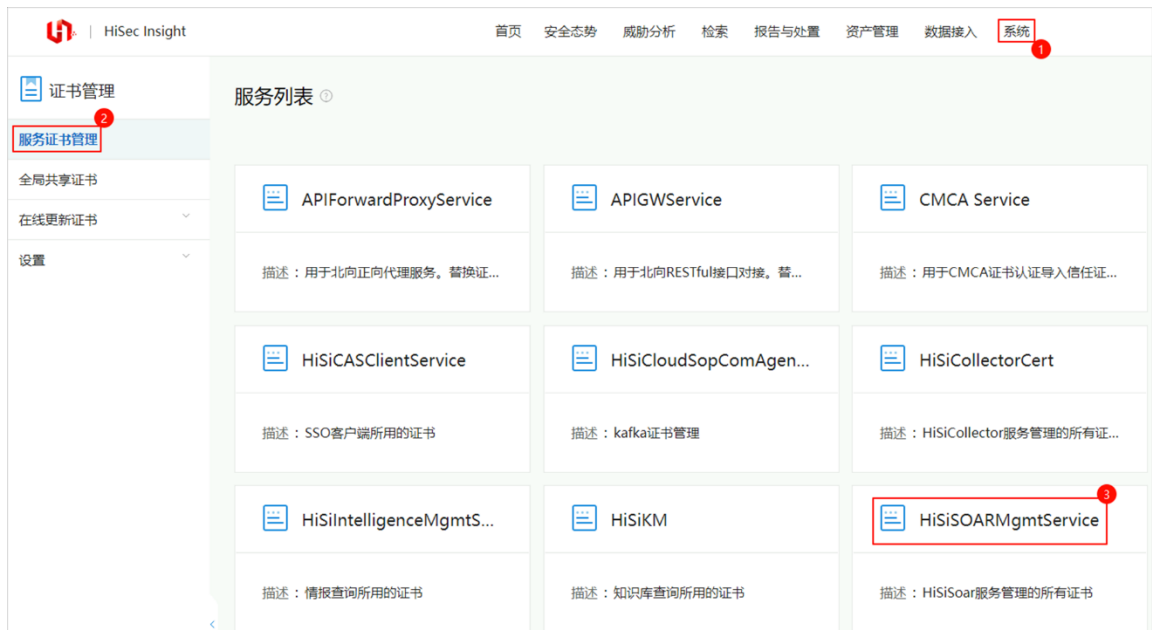


图12-21 进入“HiSiSOARMgmtService”证书管理页面



图12-22 导入 SecoManager 证书

证书导入完成后效果如下：



图12-23 “HiSiSOARMgmtService”信任证书列表

步骤 9 联动 SecoManager

在 HiSec Insight 基础运维界面选择“报告与处置 > 响应编排 > 设备”，选择“设备”页签，单击“创建”，将 SecoManager 添加为联动设备。

← 设备信息

设备基本信息

* 名称:

SecoManager

* 设备类型:

华为SecoManager控制器

* IP:

172.21.10.71

* 端口:

18002

* 联动协议:

☒ HTTPS ☐ HTTP

* 设备认证方式:

☒ 证书认证 ☐ 免证书认证

* 安全加密:

☒ ②

描述:

认证配置信息

* 认证链接:

/controller/v2/tokens

* 用户名:

admin@system.com

* 密码:

..... Security@123

提交

测试连通性

取消

图12-24 配置联动参数

提示

i

是否开始测试设备连通性？

取消

确认



图12-25 测试联动性

设备连通后在原先界面点击“提交”并确认即可。

←

设备信息

* 联动协议:

☒ HTTPS
 ☐ HTTP

* 设备认证方式:

☒ 证书认证
 ☐ 免证书认证

* 安全加密:

☒ ①

描述:

认证配置信息

* 认证链接:

/controller/v2/tokens

* 用户名:

admin@system.com

* 密码:

.....

提交

测试连通性

取消

图12-26 提交 SecoManager 联动配置

步骤 10 设置联动策略

在 HiSec Insight 基础运维界面选择“报告与处置 > 响应编排 > 快速处置管理”。单击处置策略“快速处置_SecoManager 创建阻断策略”对应的“创建”，之后在弹出的窗口中配置联动策略。



图12-27 进入联动策略创建页面



图12-28 配置联动策略

触发事件选项在实际部署时需根据业务需求合理配置,此处勾选了全部事件。

12.3 结果验证

使用 RDP 登录 PC5 (地址: 172.21.10.205, 账号: admin/Huawei123!), 在成功接入 SSL VPN 后, 打开资源管理器连接企业总部 FTP 服务器, 并将桌面上的“沙箱测试文件”、“内容过滤测试文件”和“入侵防御测试文件”一并上传至企业总部 FTP 服务器:

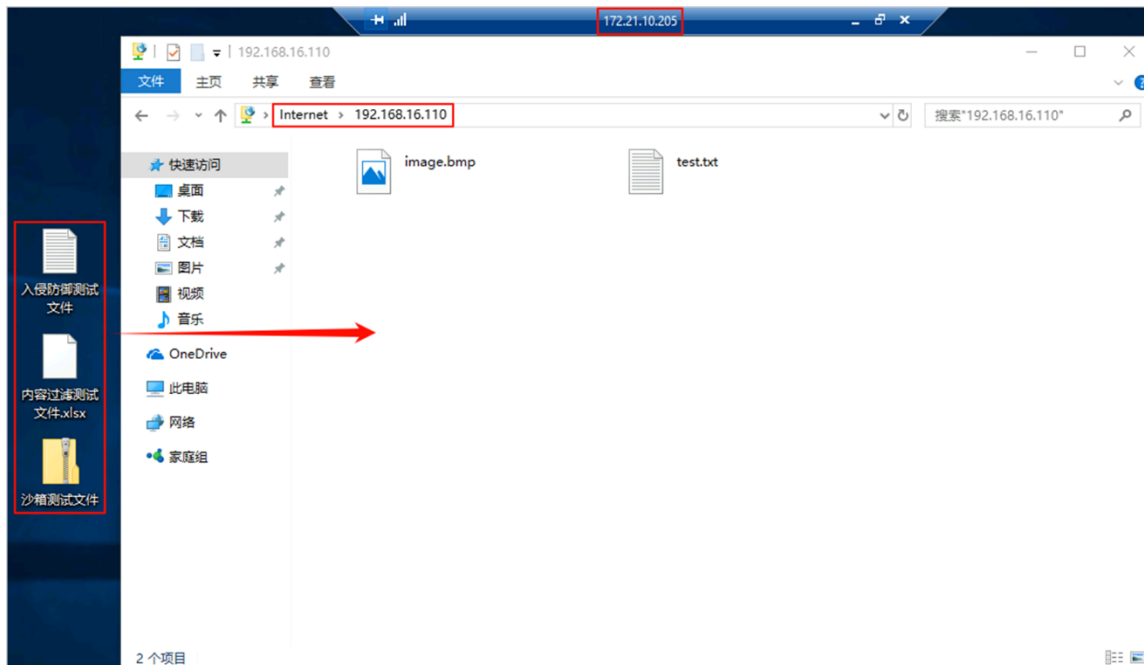


图12-29 PC5 上传测试文件至企业总部 FTP 服务器

完成文件上传后, 可回到 HiSec Insight 基础运维界面选择“检索 > 智能检索 > 原始事件”并点击查询按钮, 效果如下:

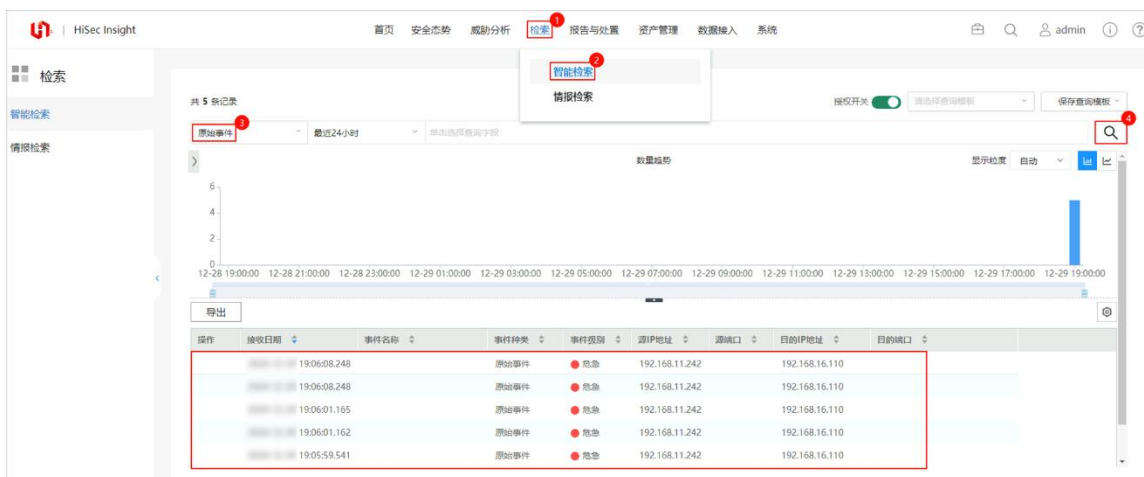


图12-30 HiSec Insight 查看原始事件

继续在 HiSec Insight 基础运维界面选择“威胁分析 > 威胁事件”, 查看 HiSec Insight 分析出来的安全威胁:



图12-31 HiSec Insight 查看威胁事件

在 HiSec Insight 基础运维界面选择“安全态势 > 综合安全态势”可通过安全态势感知大屏直观阅览网络安全状态：

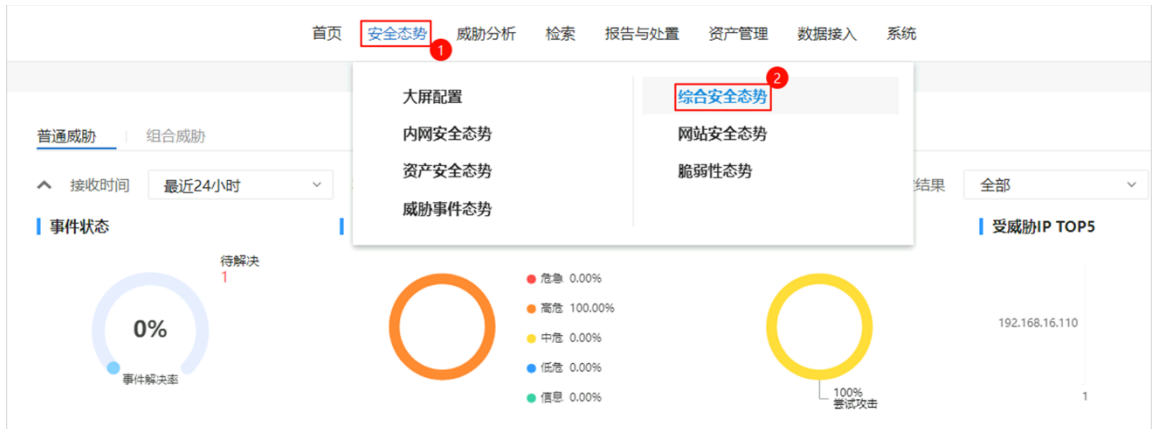


图12-32 进入 HiSec Insight 安全态势感知大屏



图12-33 HiSec Insight 安全态势感知大屏

12.4 配置参考（仅展示本实验相关配置）

12.4.1 HQ-FW1 的配置

```
#
info-center loghost source GE0/0/5
info-center loghost 172.21.10.80
#
log type policy enable
#
log type traffic enable
#
log type traffic-report enable
#
dataflow enable
#
firewall log source 172.21.10.51 1617
firewall log host 1 172.21.10.80 9002
firewall log password Huawei@123
firewall log encrypt-algorithm aes256-gcm
firewall log session filter nat enable
#
security-policy
 rule name HiSecInsight
   source-zone local
   source-zone mgmt_zone
   destination-zone local
   destination-zone mgmt_zone
   source-address 172.21.10.51 mask 255.255.255.255
   source-address 172.21.10.52 mask 255.255.255.255
   source-address 172.21.10.80 mask 255.255.255.255
   destination-address 172.21.10.51 mask 255.255.255.255
   destination-address 172.21.10.52 mask 255.255.255.255
   destination-address 172.21.10.80 mask 255.255.255.255
   action permit
#
return
```

12.4.2 HQ-FW2 的配置

```
#
info-center loghost source GE0/0/5
info-center loghost 172.21.10.80
#
log type policy enable
#
log type traffic enable
#
```

```
log type traffic-report enable
#
dataflow enable
#
firewall log source 172.21.10.52 1617
firewall log host 1 172.21.10.80 9002
firewall log password Huawei@123
firewall log encrypt-algorithm aes256-gcm
firewall log session filter nat enable
#
security-policy
rule name HiSecInsight
source-zone local
source-zone mgmt_zone
destination-zone local
destination-zone mgmt_zone
source-address 172.21.10.51 mask 255.255.255.255
source-address 172.21.10.52 mask 255.255.255.255
source-address 172.21.10.80 mask 255.255.255.255
destination-address 172.21.10.51 mask 255.255.255.255
destination-address 172.21.10.52 mask 255.255.255.255
destination-address 172.21.10.80 mask 255.255.255.255
action permit
#
return
```

12.4.3 DC-FW 的配置

```
#
info-center loghost source GE0/0/5
info-center loghost 172.21.10.80
#
log type policy enable
#
log type traffic enable
#
log type traffic-report enable
#
dataflow enable
#
firewall log source 172.21.10.53 1617
firewall log host 1 172.21.10.80 9002
firewall log password Huawei@123
firewall log encrypt-algorithm aes256-gcm
#
security-policy
rule name HiSecInsight
source-zone local
```

```
source-zone mgmt_zone
destination-zone local
destination-zone mgmt_zone
source-address 172.21.10.53 mask 255.255.255.255
source-address 172.21.10.80 mask 255.255.255.255
destination-address 172.21.10.53 mask 255.255.255.255
destination-address 172.21.10.80 mask 255.255.255.255
action permit
#
return
```

12.5 思考题

HiSec Insight 除了采集日志的功能以外，还有哪些功能，使用场景是什么？

答案：

1. 已知/高级威胁检测：

发现外部渗透：通过上网流量检测包含恶意附件的恶意邮件。

发现被入侵主机：通过上网流量发现进行 C&C 通信的内部主机。

发现数据外发：通过上网流量发现隐蔽通道异常。

2. 全网安全态势感知：

全网感知安全态势并可视化，直观洞察企业面临的威胁。

3. 调查取证分析：

基于日志+流量+情报的快速检索，辅助快速确认攻击事件。

可疑流量 PCAP 报文获取，辅助事件确认调查分析。

4. 安全联动防护：

联动安全设备和园区控制器执行防护动作，如阻断 C&C 外联，阻断隐蔽通道外发、隔离内部主机等行为。

13

SecoManager 运维实验

13.1 实验介绍

13.1.1 关于本实验

企业总部运维中心部署 SecoManager 控制器，使用 SecoManager 控制器统一管理防火墙、IPS 等安全设备，可实现安全策略的统一编排和管理，从单点防御到全网协防，抵御各类网络威胁。

同时 SecoManager 可与运维中心态势感知系统 HiSec Insight 进行安全联动，当 HiSec Insight 基于网络数据分析出安全威胁事件时，可通过调用 SecoManager 北向接口，下发安全策略编排任务，并由 SecoManager 给执行层安全设备下发安全策略，实现威胁处置闭环。

13.1.2 实验组网介绍

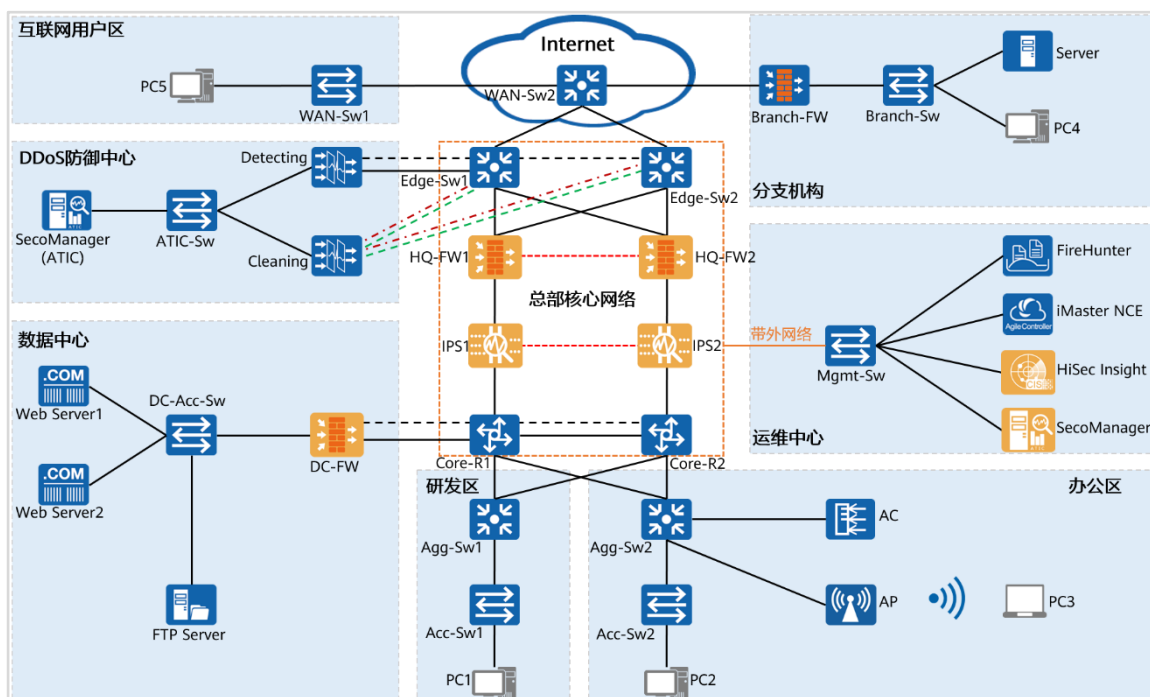


图13-1 实验拓扑图

13.1.3 实验规划

SecoManager 进行设备集中管理时，需先在设备侧预配基础网络参数、SNMP 和 NETCONF 相关的配置，并确保设备和控制器之间路由可达，之后在控制器侧进行设备扫描和设备添加操作从而完成设备纳管。

本方案中，安全设备和控制器之间采用带外管理网（已预配）对接，具体网络参数如下：

表13-1 基础网络参数规划

设备	配置项	数据
HQ-FW1	对接接口	GE0/0/5
	IP地址	172.21.10.51/17
HQ-FW2	对接接口	GE0/0/5
	IP地址	172.21.10.52/17
DC-FW	对接接口	GE0/0/5
	IP地址	172.21.10.53/17
IPS1	对接接口	Meth 0/0/0
	IP地址	172.21.10.41/17
IPS2	对接接口	Meth 0/0/0
	IP地址	172.21.10.42/17
SecoManager	对接接口	ETH2
	IP地址	172.21.10.71/17
HiSec Insight	对接接口	ETH2
	IP地址	172.21.10.80/17

用于设备扫描发现的 SNMP 协议配置数据规划如下：

表13-2 SNMP 参数规划

配置项	数据
SNMP版本	v3
安全用户名	SecoManager
认证密码	Hello@123
加密密码	User@87654321

用于控制器下发配置的 NETCONF 配置数据规划如下：

表13-3 NETCONF 参数规划

配置项	数据
用户名	netconf-admin
密码	Hello@123
NETCONF端口	830

13.2 实验配置任务

13.2.1 配置思路

1. 配置安全策略，放行防火墙与控制器之间的交互报文。
2. 完成 SNMP 协议配置，确保控制器可正常扫描到安全设备。
3. 完成 NETCONF 协议配置，确保控制器可下发配置到安全设备。
4. 控制器侧扫描并添加安全设备，完成设备纳管。
5. 控制器侧执行数据同步，确保双机热备系统主备之间、控制器与设备之间的配置同步。

13.2.2 配置步骤

步骤 1 配置安全策略

登录 HQ-FW1 设备 Web 管理界面（地址：<https://172.21.10.21:8443>，账号：Webuser/Admin@123），选择“策略 > 安全策略 > 新建 > 新建安全策略”，进入安全策略创建页面，进行以下操作，放行 HQ-FW1/2 设备至 SecoManager 侧的双向流量。

新建安全策略

×

概述

名称

SecoManager

1

描述

策略组

-- NONE --

条件

① 当前未加载地区识别特征库。如需配置地区，请 加载地区识别特征库

源

安全区域

local × mgmt_zone ×

2

IP 地址/地区 ②

172.21.10.51 × 172.21.10.52 × 172.21.10.71 ×

目的

11

目的类型

安全区域

虚拟服务

安全区域

mgmt_zone × local ×

IP 地址/地区 ②

172.21.10.51 × 172.21.10.52 × 172.21.10.71 ×

服务 ②

协议

请选择服务

更多

应用/用户/安全组/时间段/VLAN ID

动作

动作

允许

禁止

3

内容安全检查

反病毒/入侵防御/URL过滤/内容过滤

取消

命令预览

确定

4

图13-2 HQ-FW1 创建对接 SecoManager 的安全策略

HQ-FW2 设备可通过 HRP 自动同步上述安全策略配置，无需单独配置。

登录 DC-FW 设备 Web 管理界面（地址：<https://172.21.10.23:8443>，账号：Webuser/Admin@123），选择“策略 > 安全策略 > 新建 > 新建安全策略”，进入安全策略创建页面，进行以下操作，放行 DC-FW 设备至 SecoManager 侧的双向流量。

在 HQ-FW2、DC-FW、IPS1 和 IPS2 设备上同样按照上述操作关闭黑名单锁。

若处在双机热备系统的备份设备无法进行配置,可以通过命令“hrp standby config enable”开启备机的配置功能。

登录 HQ-FW1 设备 Web 管理界面 (地址: <https://172.21.10.21:8443>, 账号: Webuser/Admin@123), 选择“系统 > 配置 > SNMP”, 执行如下配置:

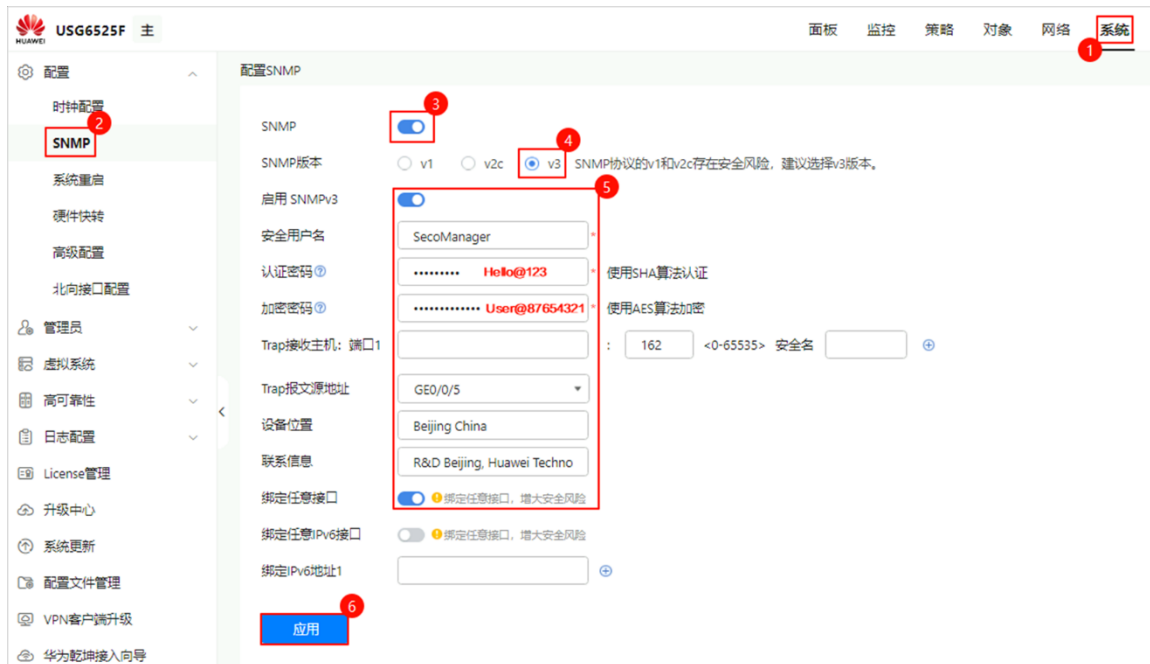


图13-4 HQ-FW1 配置 SNMP

HQ-FW2、DC-FW 设备 SNMP 配置同上。

登录 IPS1 设备 Web 管理界面 (地址: <https://172.21.10.41:8443>, 账号: Webuser/Admin@123), 选择“系统 > 配置 > SNMP”, 执行如下配置:

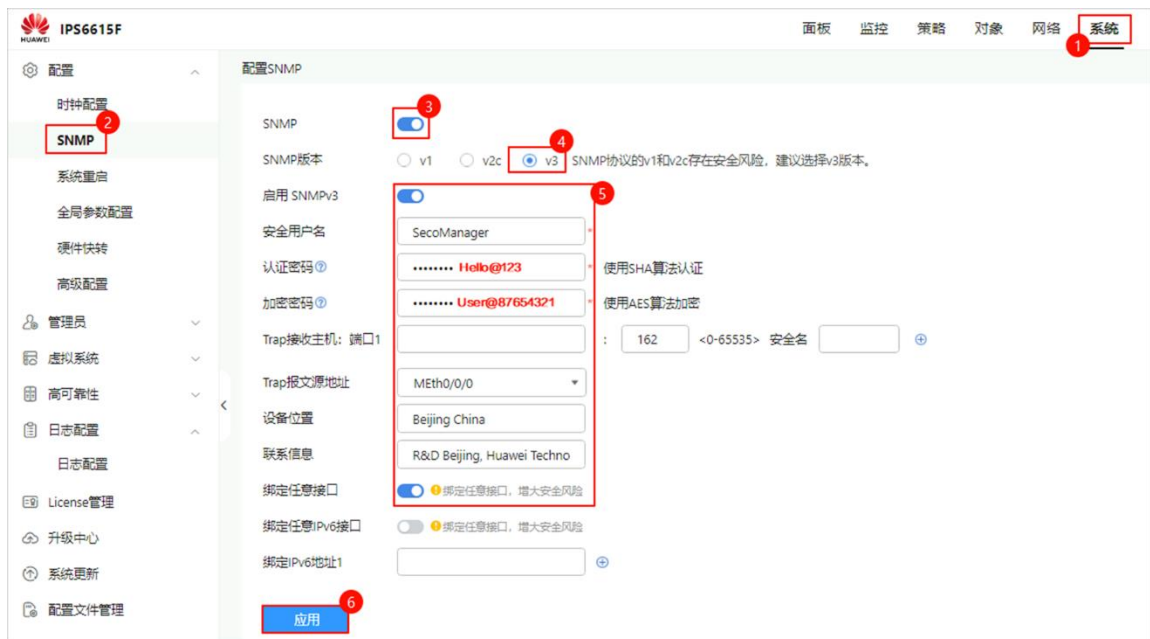


图13-5 IPS1 配置 SNMP

IPS2 设备 SNMP 配置同上。

步骤 3 配置 NETCONF

在 HQ-FW1 设备上创建管理员，选择“系统 > 管理员 > 管理员”，单击“新建”。配置管理员以及对应的服务类型和认证类型。



图13-6 创建管理员

管理员相关配置 HQ-FW2 设备会通过 HRP 自动同步，无需单独配置。

DC-FW 和 IPS1 设备的管理员创建操作同上。

在 HQ-FW1 设备 Web 管理界面选择“网络 > 接口”，选择对接控制器的 G0/0/5 接口，并开启接口下对应的管理功能：

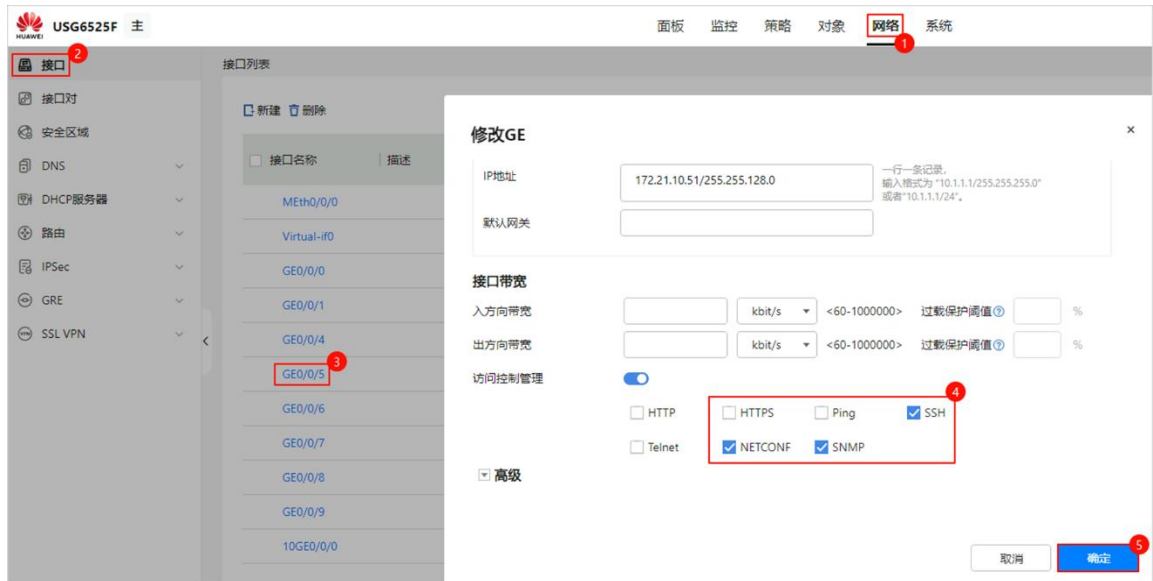


图13-7 开启接口管理功能

HQ-FW2、DC-FW 接口管理功能的配置同上。

在 HQ-FW1 设备 Web 管理界面选择“系统 > 管理员 > 设置”，选择“SSH 配置”。开启 SSH 服务及绑定服务的端口。

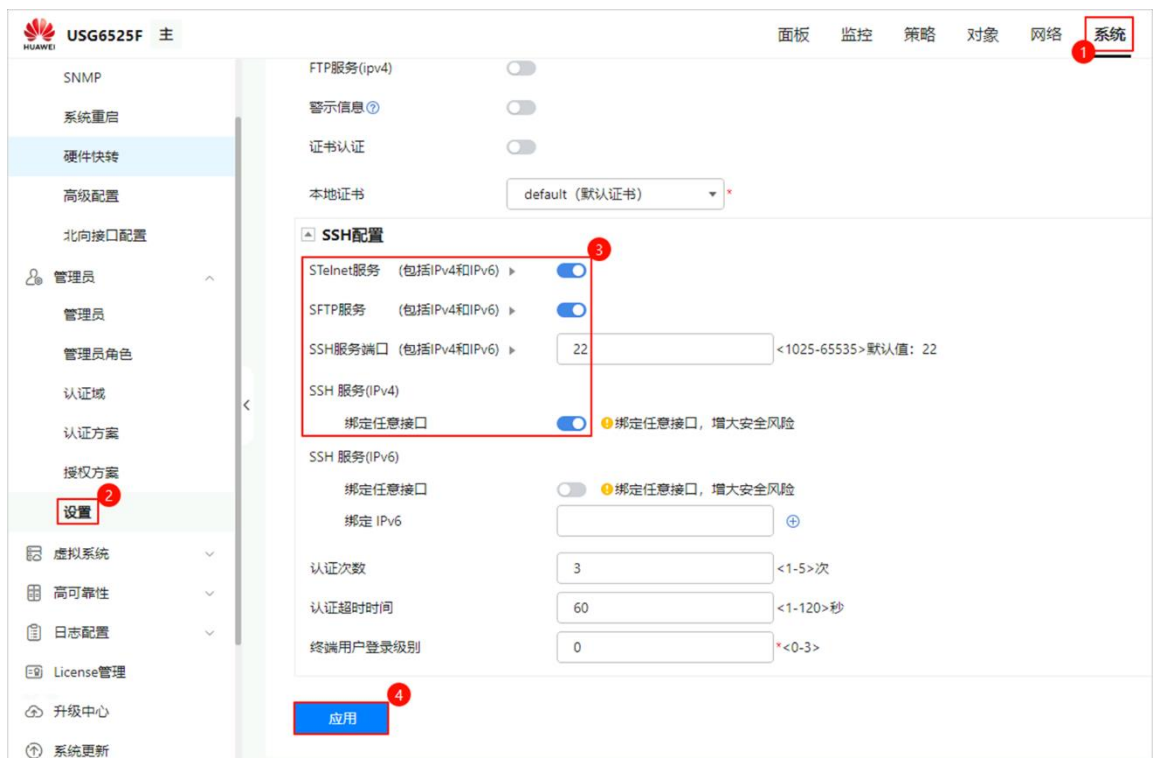


图13-8 HQ-FW1 启用 SSH 服务

HQ-FW2 和 DC-FW 设备的 SSH 相关配置步骤同上。

在 HQ-FW1 设备 Web 管理界面选择“系统 > 配置 > 北向接口配置”，点击开启。



图13-9 开启北向接口

HQ-FW2 和 DC-FW 设备的北向接口相关配置步骤同上。

登录 IPS1 设备 Web 管理界面（地址：https://172.21.10.41:8443，账号：Webuser/Admin@123），选择“系统 > 管理员 > 设置”按照如下操作开启 IPS 设备的 SSH 服务器和北向接口：



图13-10 IPS1 设备开启 SSH 服务及北向接口

IPS2 设备的 SSH 服务及北向接口相关配置同上。

步骤 4 添加设备

在 SecoManager 中发现设备后，需要和设备建立 SSH 连接，设备才能正常使用。在建立 SSH 连接时，SecoManager 会判断设备的 SSH 公钥指纹是否可信。公钥指纹是指公钥长度较长，

通过对其进行加密散列计算，将其变成一个短的指纹，方便比对。如果设备的 SSH 公钥指纹可信，则校验通过，才能成功建立 SSH 连接。

SecoManager 可通过如下两种方式判断设备的 SSH 公钥指纹是否可信：

1. 信任首次学习的指纹。
2. 批量导入 SSH 公钥指纹，使用导入的 SSH 公钥指纹对设备的 SSH 公钥指纹进行校验。

本方案采用第一种方式进行演示，具体操作如下：

登录 SecoManager 的 Web 管理界面（地址：<https://172.21.10.71:31943/>，账号：admin/Security@123），选择“设备管理 > 设备 > 设备”，在“更多”的下拉框中，单击“设备 SSH 指纹策略”。



图13-11 进入设备 SSH 指纹策略配置页面

点击开启“信任首次学习的指纹”选项，因本操作属高危操作，需要手动点击“确认”，具体操作如下图（选择首次信任，但不要锁定首次学习的指纹）：



图13-12 配置设备 SSH 指纹校验策略

完成上述设备 SSH 指纹校验策略的配置后，点击“返回”，正式开始添加设备，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”。



图13-13 进入发现设备配置页面

选择“设备发现协议类型”为“SNMP”，根据规划数据填写鉴权和加密密钥，点击“开始扫描”。

设备管理 / 设备 / 设备

1

1、扫描规则定义了IP地址段和使用的协议(SNMP或Netconf)，SecoManager根据扫描规则发现设备。
2、请先导入设备的公钥指纹，如果不导入请打开设备SSH指纹策略，打开“信任首次学习的指纹”。

* 设备发现协议类型:

SNMP

1

1、设置规则

位置:

+ 选择

设备厂商:

* 管理IP地址:

2

172.21.10.41
172.21.10.42
172.21.10.51
172.21.10.52
172.21.10.53

选择模板

保存模板

SNMPv3

1

鉴权协议SHA和MD5由于协议本身的限制，其安全性不高，建议选择安全性更高的SHA2类型的鉴权协议。
CBC_DES和AES-128安全性不高，建议使用安全性更高的AES_256加密算法以提升安全性。

* 用户名:

SecoManager

* 鉴权协议:

SHA2-256

* 鉴权密钥:

..... Hello@123

* 加密算法:

AES-256

* 加密密钥:

.....
User@87654321

* 端口:

161

* 超时时间 (毫秒):

4000

* 重复次数 (次):

3

NETCONF

* 用户名:

netconf-admin

* 密码:

..... Hello@123

* 端口:

830

STELNET

1

STELNET协议为AntiDDoS设备特有参数。
纳管AntiDDoS1800/8000设备时需要开启数据维护中的兼容AntiDDoS1800/8000设备算法开关。

其他设置

虚拟系统容量:

4

开始扫描

图13-14 设置参数并扫描发现设备

在“扫描成功列表”页签选择需要添加的设备，单击“添加”，将设备添加到 SecoManager。

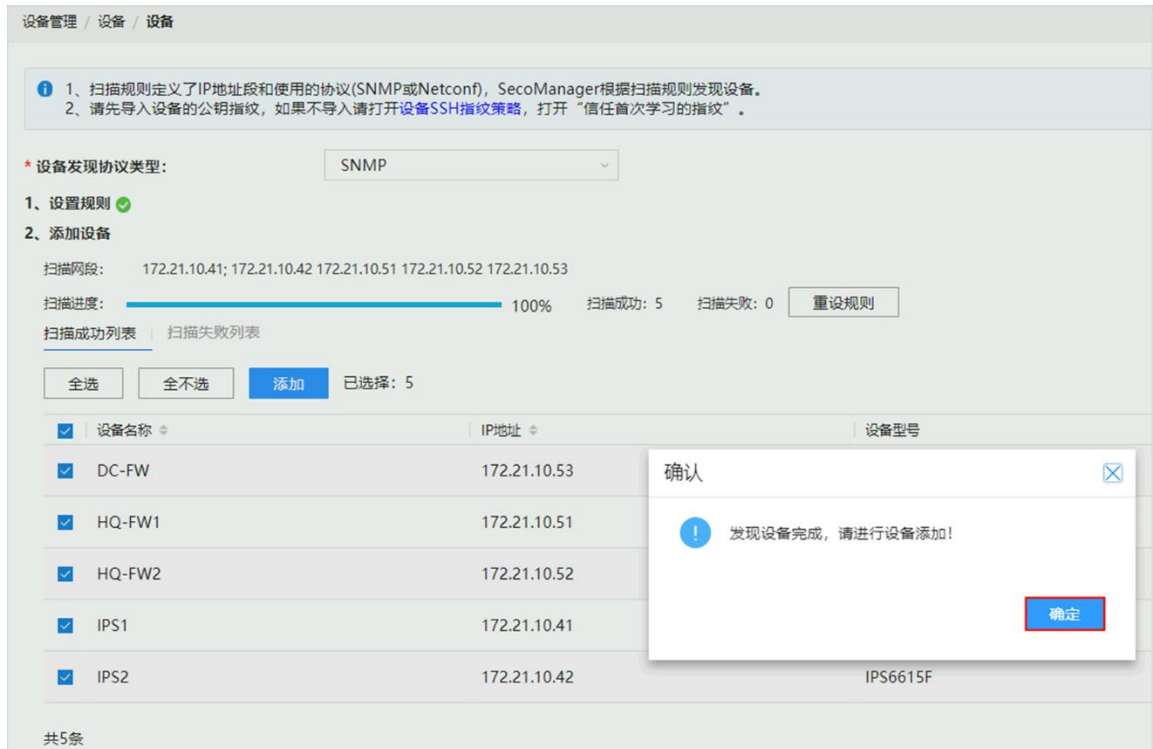


图13-15 发现设备

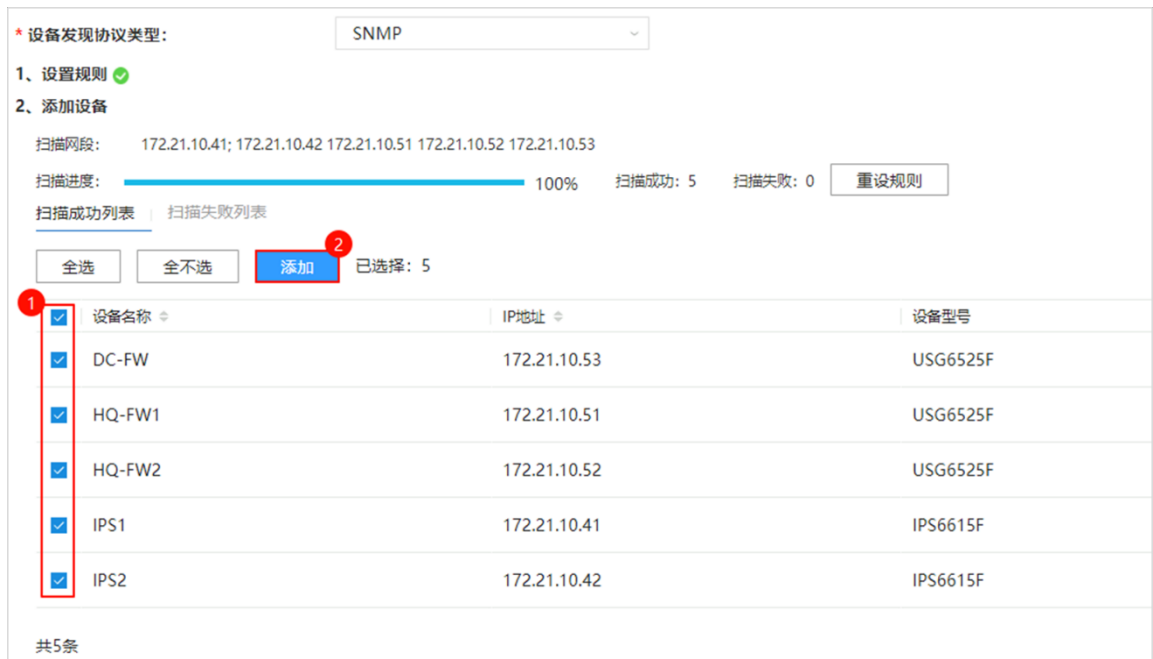
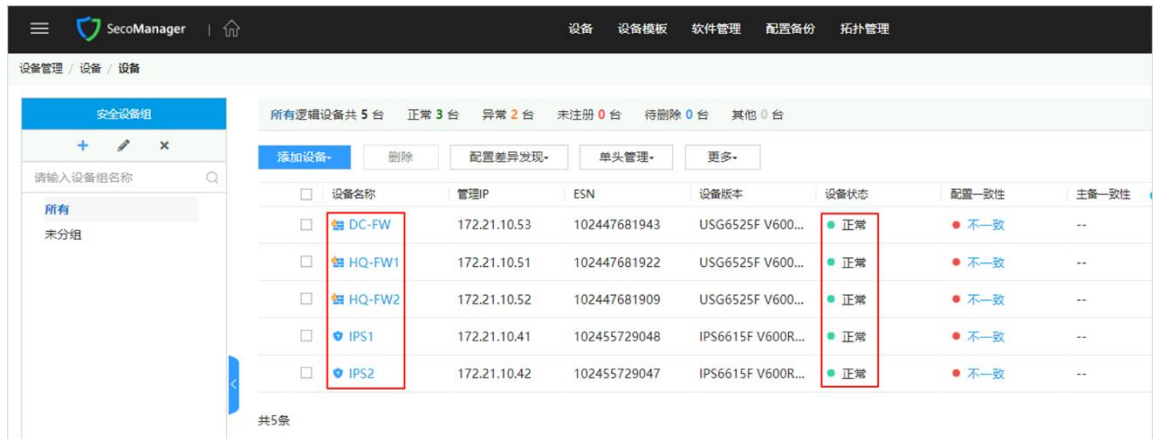


图13-16 添加设备

设备添加完成后如下图所示：



设备名称	管理IP	ESN	设备版本	设备状态	配置一致性	主备一致性
DC-FW	172.21.10.53	102447681943	USG6525F V600...	正常	不一致	--
HQ-FW1	172.21.10.51	102447681922	USG6525F V600...	正常	不一致	--
HQ-FW2	172.21.10.52	102447681909	USG6525F V600...	正常	不一致	--
IPS1	172.21.10.41	102455729048	IPS6615F V600R...	正常	不一致	--
IPS2	172.21.10.42	102455729047	IPS6615F V600R...	正常	不一致	--

图13-17 纳管成功设备列表

步骤 5 创建双机热备组

为便于管理安全设备，在控制器上需根据实际组网结构创建双机热备组，选择“设备管理 > 设备 > 设备 > 添加设备 > 创建双机热备组”。



设备名称	管理IP	ESN	设备版本	设备状态
W	172.21.10.53	102447681943	USG6525F V600...	正常
W1	172.21.10.51	102447681922	USG6525F V600...	正常
W2	172.21.10.52	102447681909	USG6525F V600...	正常
IPS1	172.21.10.41	102455729048	IPS6615F V600R...	正常
IPS2	172.21.10.42	102455729047	IPS6615F V600R...	正常

图13-18 进入双击热备组创建页面

输入双机热备组名称并添加双机热备组成员。

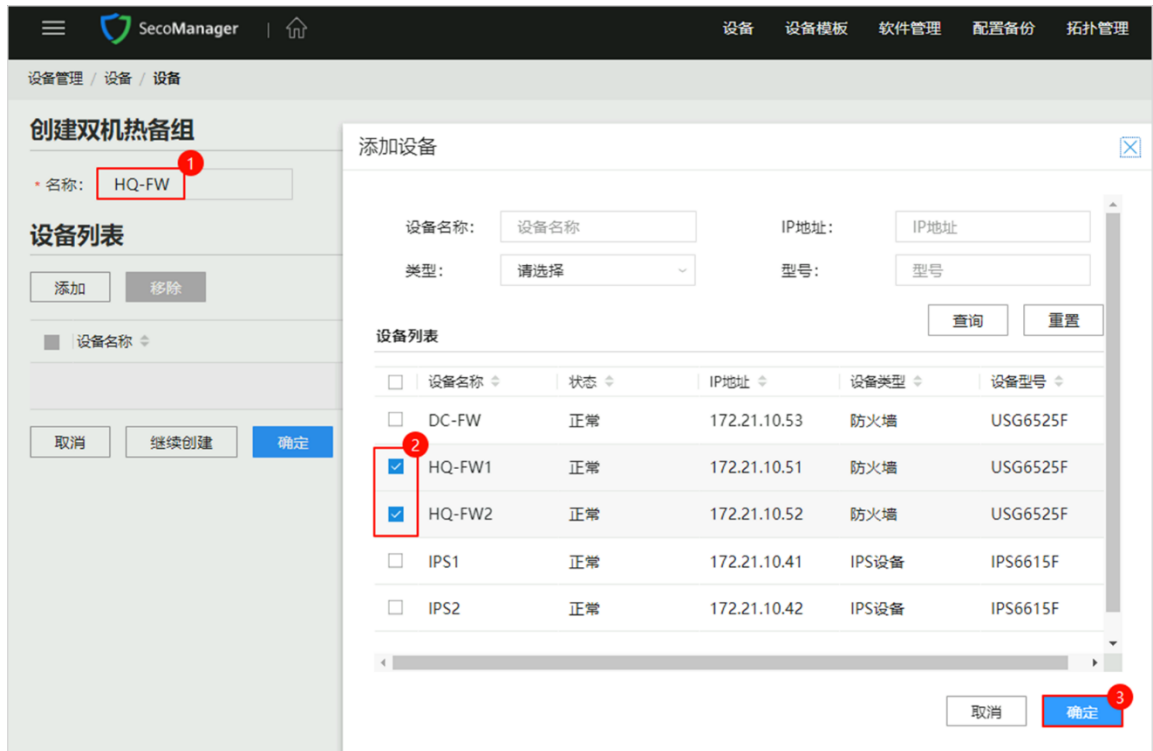


图13-19 创建总部出口防火墙双机热备组

勾选“继续创建”，进一步创建总部 IPS 双机热备组。

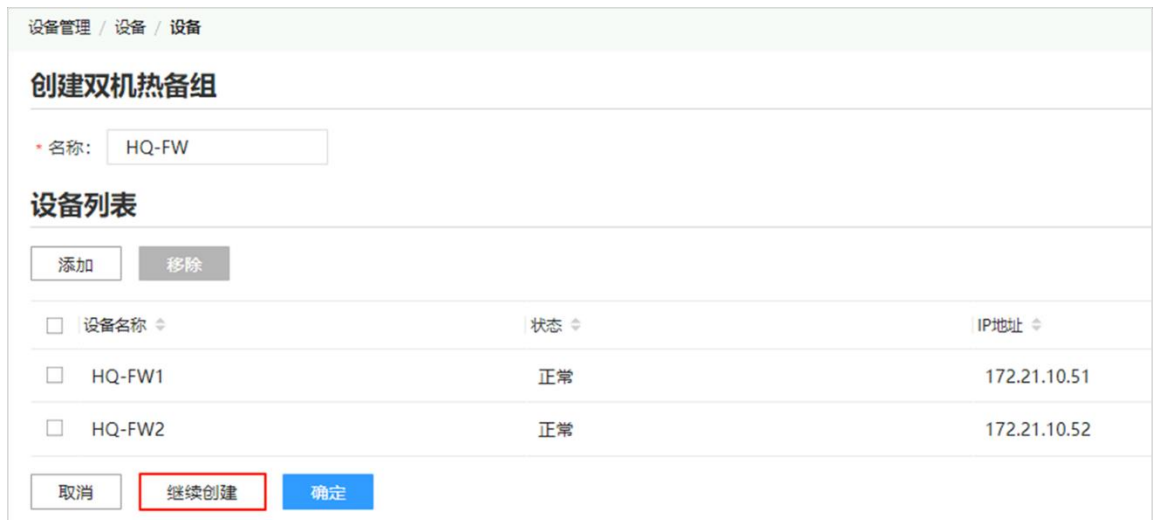


图13-20 继续创建双机热备组

使用相同的操作步骤，输入双机热备组名称并添加双机热备组成员。

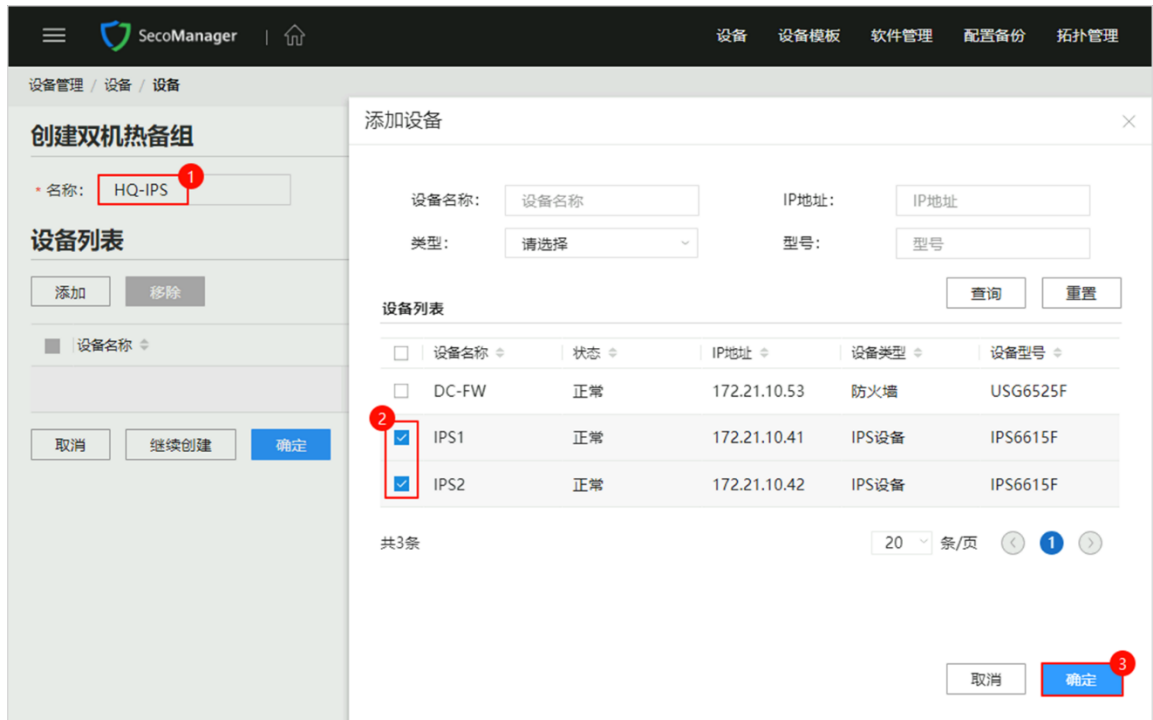


图13-21 创建总部 IPS 双机热备组



图13-22 确认双机热备组成员设备

所有双机热备组创建完成后，可以看到如下效果：



	设备名称	管理IP	ESN	设备版本	设备状态	配置一致性	主备一致性
☐	DC-FW	172.21.10.53	102447681943	USG6525F V600...	正常	不一致	--
> ☐	HQ-FW	172.21.10.51	--	USG6525F V600...	正常	不一致	一致
> ☐	HQ-IPS	172.21.10.41	--	IPS6615F V600R...	正常	不一致	一致

图13-23 双机热备组列表

步骤 6 数据同步

为保证设备侧和控制器侧的配置数据一致，需在控制器执行数据同步操作，在控制器上选择“设备管理 > 设备 > 设备”，进入设备管理列表，可发现“配置一致性”下方提示配置不一致，可点击“不一致”，查看设备侧与控制器侧配置差异。



	设备名称	管理IP	ESN	设备版本	设备状态	配置一致性
☐	DC-FW	172.21.10.53	102447681943	USG6525F V600...	正常	不一致
> ☐	HQ-FW	172.21.10.51	--	USG6525F V600...	正常	不一致
> ☐	HQ-IPS	172.21.10.41	--	IPS6615F V600R...	正常	不一致

图13-24 查看数据中心防火墙配置差异

查看“差异发现结果”后，可根据业务需求，选择需要同步的配置内容，本案例以“同步全部”为例进行演示。

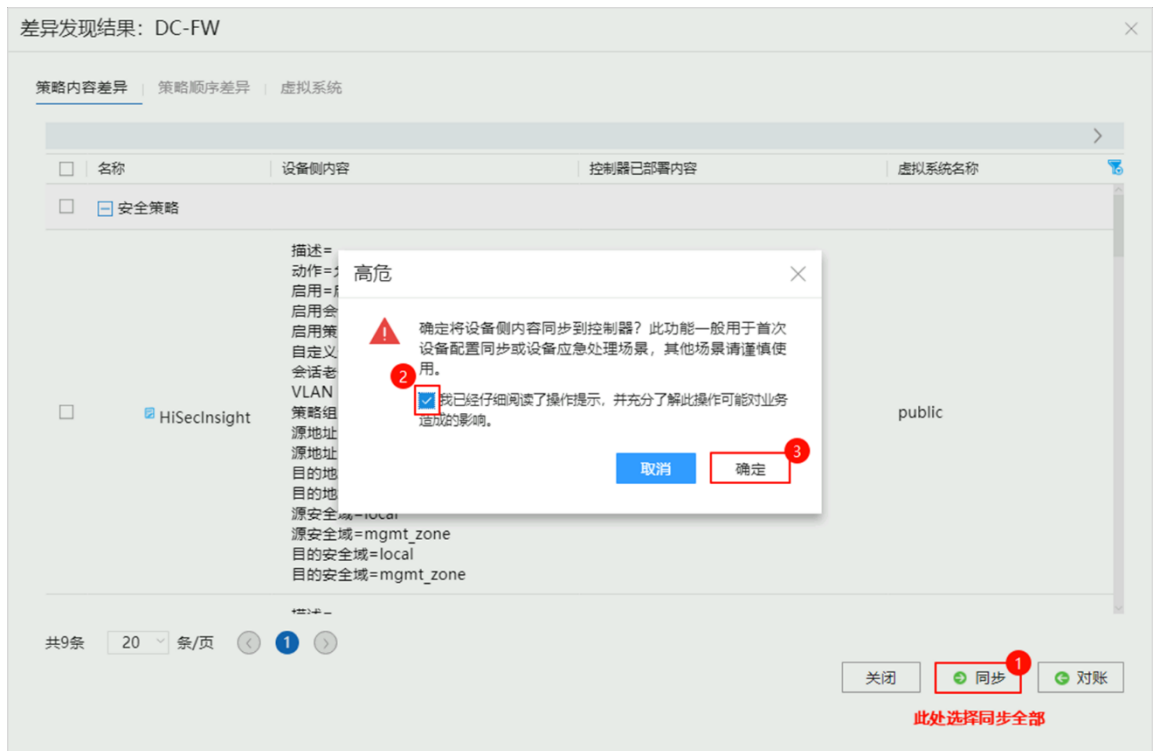


图13-25 同步数据中心防火墙配置

对“HQ-FW”和“HQ-IPS”双机热备组执行上述同样操作，完成配置同步，完成后结果如下：

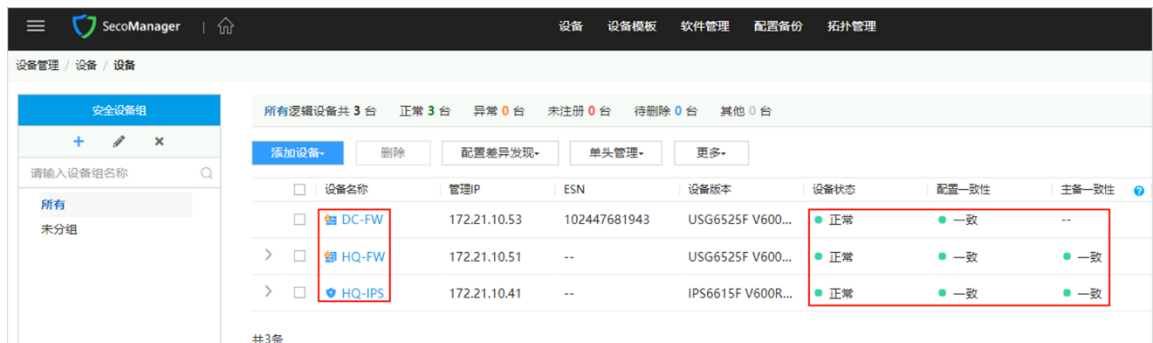


图13-26 数据同步结果

为避免手动重复性执行配置同步操作，可设置“定时差异发现”进行周期性自动差异发现。点击“配置差异发现 > 设置定时差异发现”。



图13-27 设置定时差异发现

根据业务实际需求及组网需求，选择合适的差异发现周期，本案例以 120 分钟为例演示。



图13-28 创建定时任务

步骤 7 收集告警

前提条件：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。需在 SecoManager 上开启 SNMP Trap 服务，开启后 SecoManager 才能接收设备发送的告警。相关配置参数规划如下：

表13-4 告警收集数据规划

项目		数据	说明
Trap 服务	接收私有VB	不开启	控制器选择是否接收携带扩展的私有VB的Trap报文。
	协议版本	v3	-
	端口	1200	-
SNMPv3 安全参数	用户名	ACTrap_fw	控制器向设备下发的安全参数，用于设备上报告警时的认证和加密。
	鉴权协议	HMAC_SHA2_256	
	鉴权密钥	Hello@123	
	加密算法	AES_256	
	加密密钥	User@87654321	

在“系统管理”APP 的菜单中选择“系统设置 > 南向协议”，选择“SNMP 配置”，开启 Trap 服务，单击“应用”。



图13-29 进入南向协议配置页面



图13-30 配置 Trap 服务

在“SNMPv3 安全参数”区域，单击“创建”，参考相关数据规划完成 SNMP 安全参数的配置。

创建

X

i

鉴权协议HMAC_SHA和HMAC_MD5由于协议本身的限制，其安全性不高，建议选择安全性更高的HMAC_SHA2_512鉴权协议(选择SHA2以上鉴权协议，请检测纳管的设备是否支持该协议，否则会导致配置下发失败)；CBC_DES安全性不高，建议使用安全性更高的AES_256加密算法以提升安全性。

* 用户名：

ACTrap_

Security

* 鉴权协议：

HMAC_SHA2_256

* 鉴权密钥：

..... Hello@123

* 加密算法：

AES_256

* 加密密钥：

..... User@87654321

取消

确认

图13-31 配置 SNMPv3 安全参数

完成上述操作后，控制器侧即可接收设备侧告警。

13.3 结果验证

13.3.1 设备监控

在 SecoManager “监控” APP 的菜单中选择“全局监控”，可以看到所有纳管设备的统计信息，了解安全设备全局情况。



图13-32 进入全局监控界面

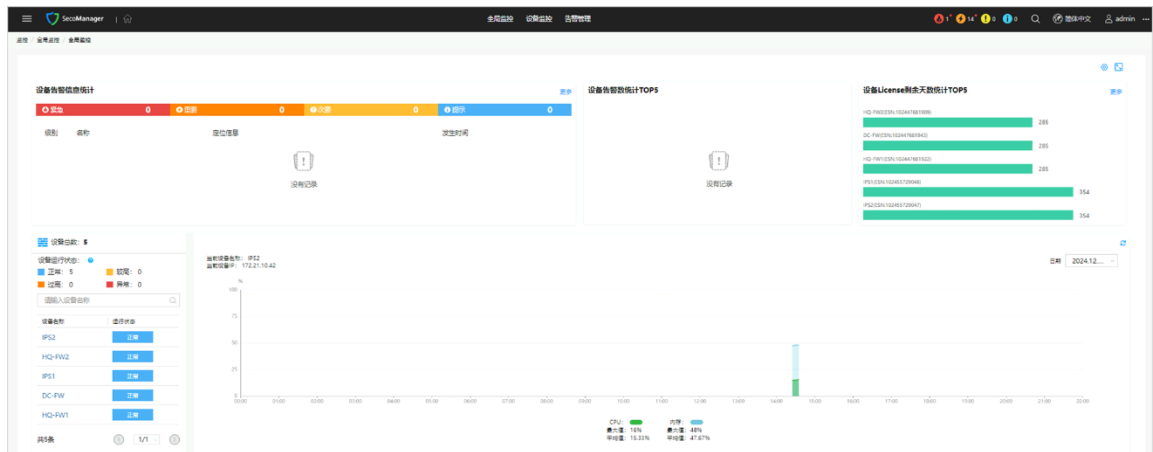


图13-33 全局监控

在“监控”APP的菜单中选择“设备监控”，并选择需要监控的安全设备。

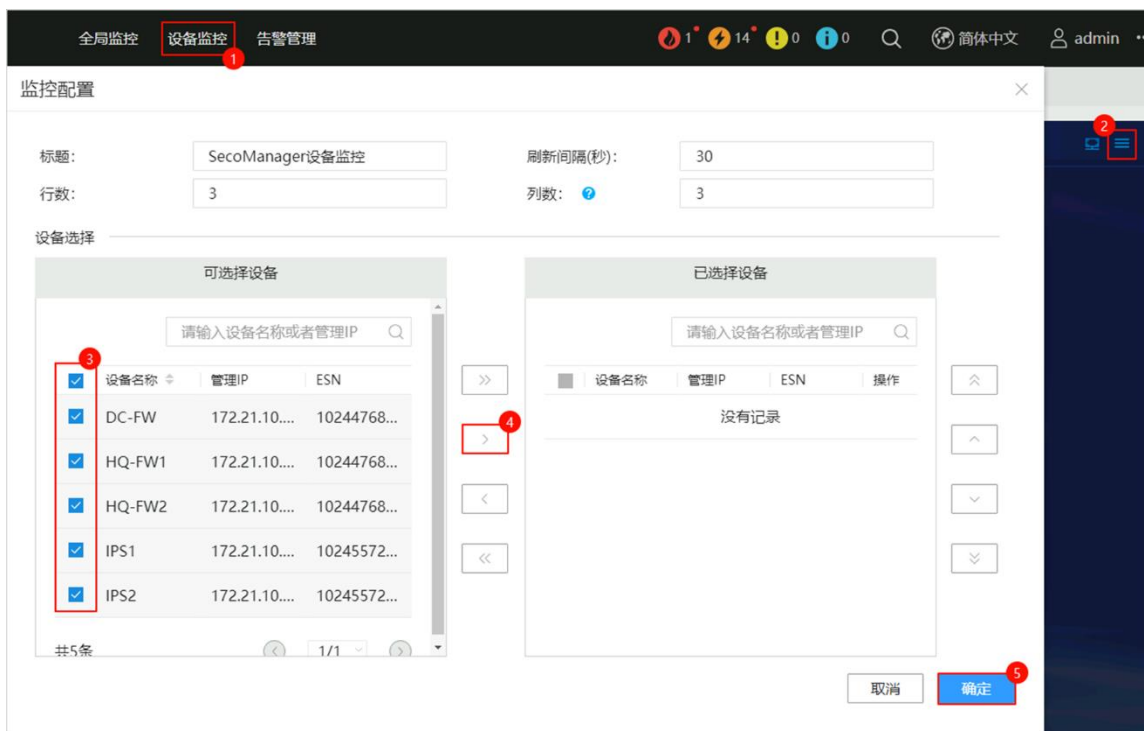


图13-34 进入设备监控配置页面并选择监控设备

设备监控配置完成后效果如下：



图13-35 设备监控主页面

点击设备监控主页面中单个设备右上角详情按钮，可进入对应设备的详细监控页面，以 HQ-FW1 设备为例：



图13-36 进入 HQ-FW1 设备监控详细页面

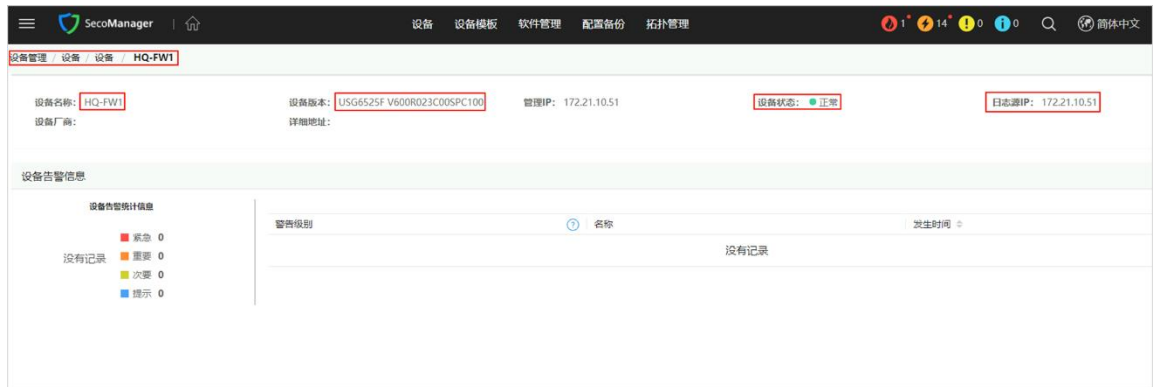


图13-37 HQ-FW1 设备监控详情

13.3.2 策略管理

在 SecoManager 系统 Web 管理界面选择“网元策略 > 策略配置 > 安全策略”，可对所有安全设备的安全策略进行集中查看和管理，避免策略的分布式配置和运维，提高安全策略维护和管理效率。



图13-38 进入安全策略管理界面



图13-39 安全策略管理界面

除安全策略外，NAT 策略、带宽策略和服务映射规则均可在 SecoManager 控制器上集中查看和管理，实际业务场景中可按需使用。



图13-40 策略配置功能呈现

13.3.3 策略调优

SecoManager 系统支持对纳管设备进行策略冗余性分析并调优，精简设备安全策略，优化冗余配置，本实验以 DC-FW 设备为例演示。

在 SecoManager 系统 Web 管理界面选择“监控 > 设备监控 > 设备监控”，进入设备监控主页面，并点击特定设备右上角监控详情按钮，进入设备监控详情页面：



图13-41 进入 DC-FW 设备监控详情页

在 DC-FW 设备监控详情页点击“策略调优”，按照系统提示准备进行冗余分析。

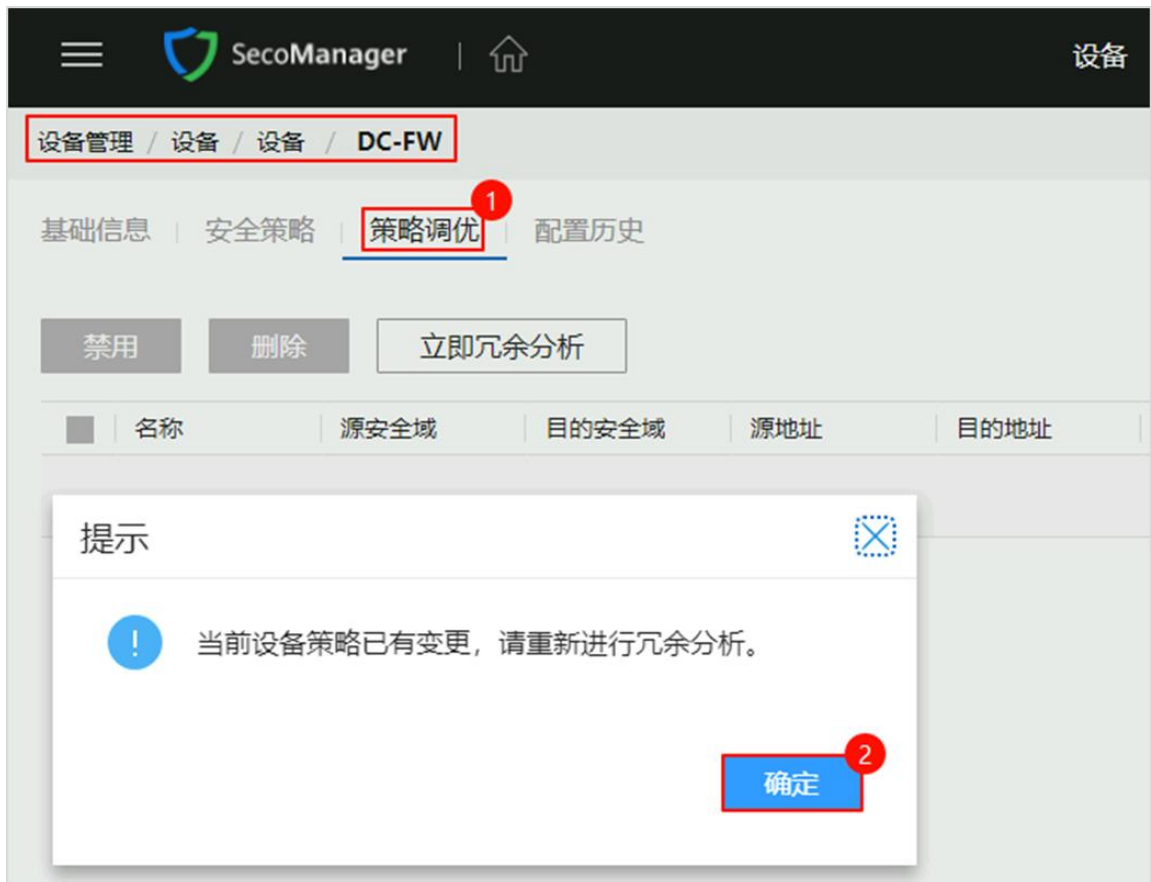


图13-42 准备进行冗余分析

之后点击“立即冗余分析”开始对 DC-FW 设备进行策略冗余分析。



图13-43 开始进行冗余分析

冗余分析任务完成后，系统会将安全设备所有安全策略的冗余情况输出，DC-FW 设备的安全策略冗余情况如下：

设备管理 / 设备 / DC-FW														
基础信息 安全策略 策略调优 配置历史														
禁用 删除 立即冗余分析														
请输入策略名称 所有 搜索														
☐	名称	源安全域	目的安全域	源地址	目的地址	服务	应用	时间域	动作	应用	上一次分析...	冗余情况	被覆属于	策略名称
☐	sslvpn_oa	untrust	dmz	192.168.11.0/24	192.168.16.0/24	any	any	any	允许	启用	2024-12-3...	不冗余	sslvpn_oa	安全策略
☐	nat64	untrust	dmz	2001::DB8:10::/48	any	any	any	any	允许	启用	2024-12-3...	部分冗余	sslvpn_oa	安全策略
☐	slb	untrust	any	any	any	any	any	any	允许	启用	2024-12-3...	部分冗余	sslvpn_oa	安全策略
☐	sandbox	local_mgmt_zone	local_mgmt_zone	172.21.10.74/24	172.21.10.53/24	any	any	any	允许	启用	2024-12-3...	不冗余	sandbox	安全策略
☐	HiSecInsight	local_mgmt_zone	local_mgmt_zone	172.21.10.80/24	172.21.10.80/24	any	any	any	允许	启用	2024-12-3...	部分冗余	sandbox	安全策略
☐	SecoManager	local_mgmt_zone	local_mgmt_zone	172.21.10.53/24	172.21.10.53/24	any	any	any	允许	启用	2024-12-3...	部分冗余	sandbox	安全策略
☒	default	any	any	any	any	any	any	any	禁止	启用	2024-12-3...	部分冗余	sslvpn_oa	安全策略
共7条														
20 条/页														

图13-44 DC-FW 设备策略冗余性分析结果

经过分析可以发现，DC-FW 设备的个别安全策略存在“部分冗余”的情况，针对“部分冗余”的安全策略，建议基于业务实际情况进行二次评估，切勿直接禁用，否则会影响正常业务或者控制流的交互，本案例中，系统判定的“部分冗余”的安全策略条目是用于放行多种不同的管理流，故不做处理。实际业务场景中，若对实际业务不是非常了解，针对“部分冗余”的策略建议不做修改。

13.3.4 安全联动

本方案中，SecoManager 与 HiSec Insight 已实现对接（实验 12 中已经配置），当 HiSec Insight 分析并判定威胁事件后，会调用 SecoManager 的北向接口，通过 SecoManager 对安全设备下发相关策略，实现对恶意流量的阻断或隔离，实现安全联动和响应。

SecoManager 要进行安全策略编排和下发时，需要获取安全设备的保护网段，可以手动创建保护网段或基于发现的网络拓扑自动学习保护网段。本案例以手动创建为例演示。

登录 SecoManager 的 Web 管理界面（地址：<https://172.21.10.71:31943/>，账号：admin/Security@123），在“业务策略”APP 的菜单中选择“安全服务 > 编排配置”，在“设备配置”页签下，单击“添加”，之后勾选特定设备进行配置。



图13-45 进入编排配置界面

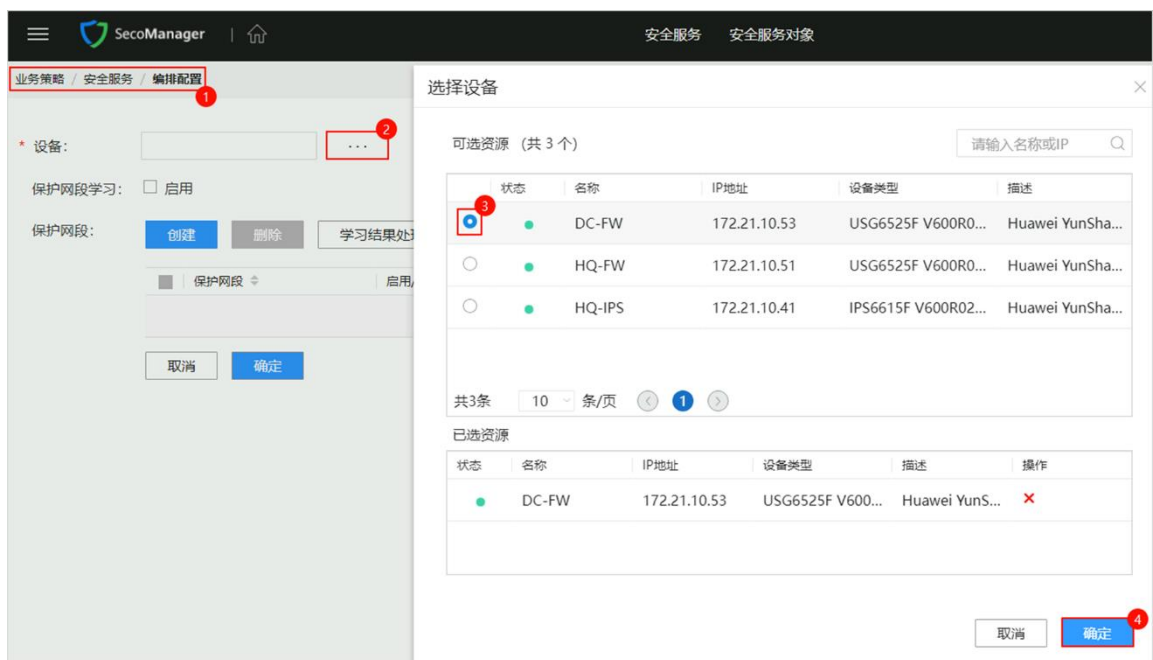


图13-46 选择数据中心防火墙配置保护网段

完成设备选择后，在保护网段右侧点击“创建”，将园区内部核心资产所在的业务网段手动添加为保护网段。



图13-47 手动添加保护网段

完成上述操作后，点击“确认”，完成数据中心防火墙的保护网段创建工作。

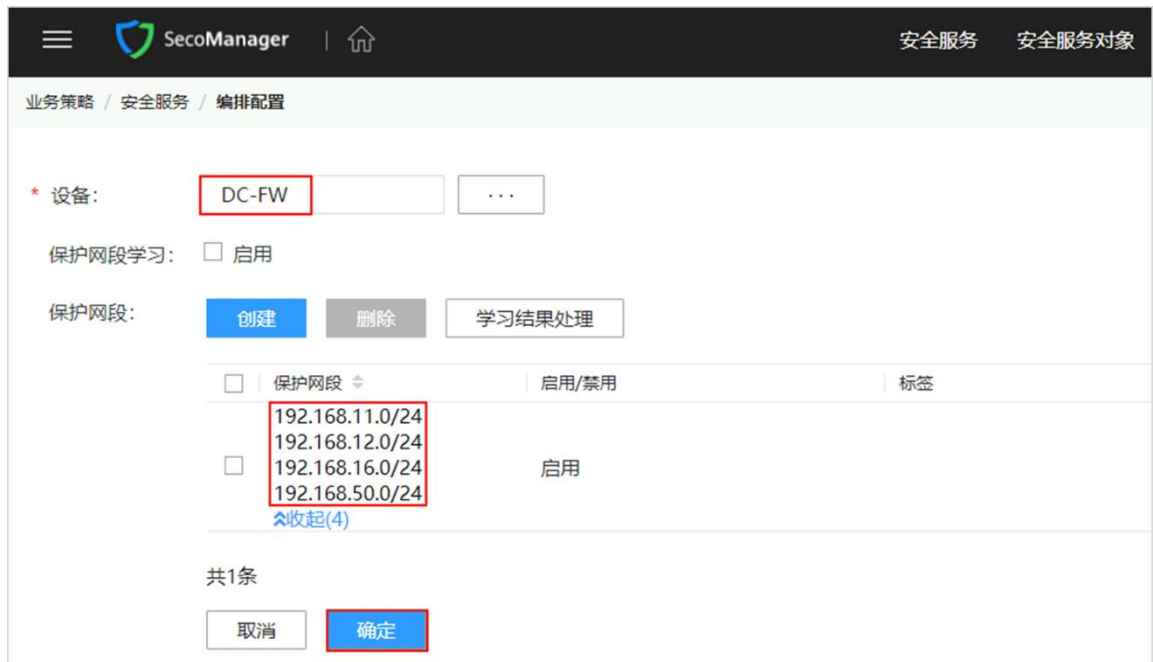


图13-48 确认创建保护网段

使用相同方式为企业总部出口防火墙及 IPS 双机热备组配置保护网段，完成后效果如下：



图13-49 设备编排配置结果查看

完成 SecoManager 侧安全设备的保护网段配置后，登录 HiSec Insight 的运维面（地址：<https://172.21.10.80:31943>，账号：admin/Security@123），点击“威胁分析 > 威胁事件”，进入威胁事件管理界面。

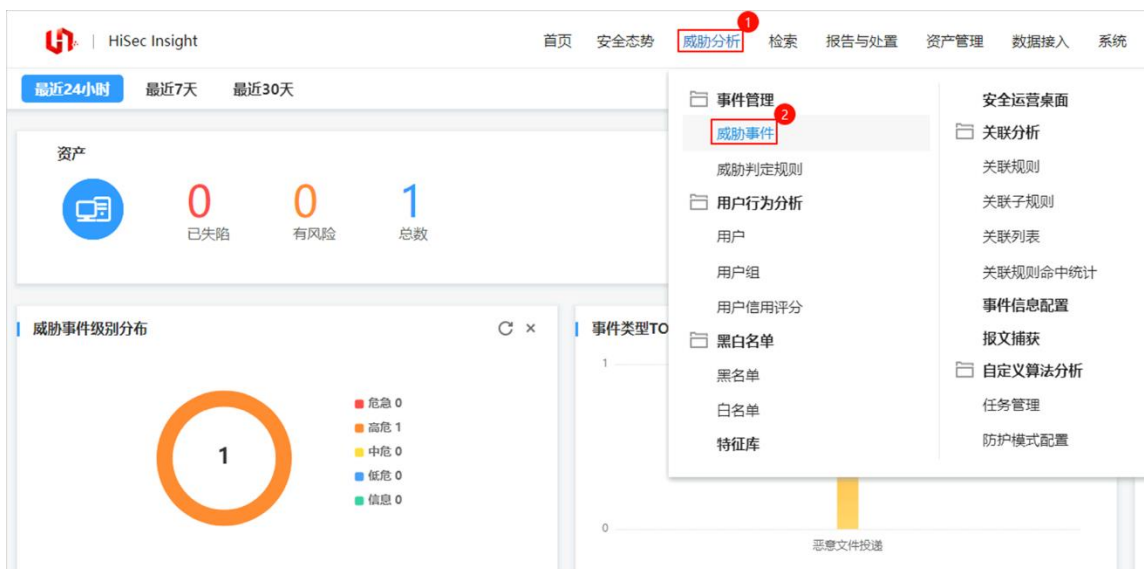


图13-50 进入威胁事件管理界面

在威胁事件管理界面，可以查看到存在恶意文件传输的威胁事件，此次威胁事件也是在“实验 12”中执行结果验证时触发的，此处以这个威胁事件演示安全威胁处置相关操作（如果此处没有出现威胁事件，可以按照“12.3 结果验证”相关步骤再执行一遍，确保触发威胁事件）。



图13-51 查看并处置威胁事件

在威胁事件处置界面可以看到 HiSec Insight 系统与 SecoManager 已完成安全联动，点击“操作”列下面“处置”按钮，对威胁事件进行处置。

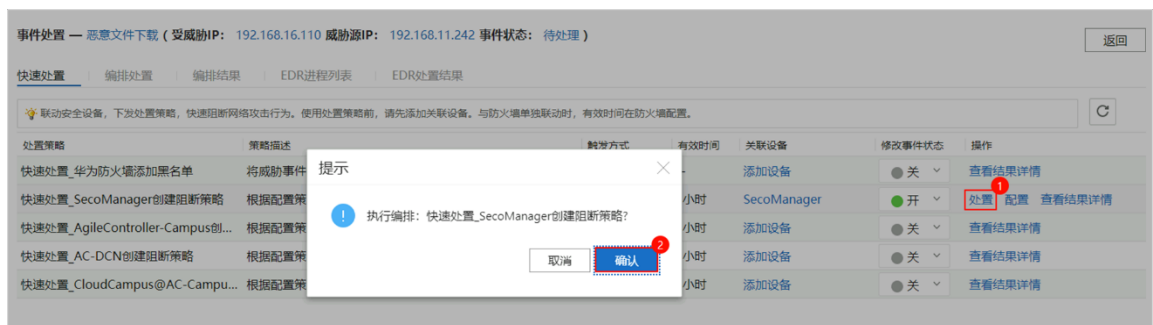


图13-52 处置威胁事件

执行完上述操作后，在 HiSec Insight 威胁处置界面点击“编排结果”，查看编排任务的执行结果：



图13-53 查看编排结果

完成上述操作后, 登录 SecoManager 的 Web 管理界面(地址: <https://172.21.10.71:31943/> , 账号: admin/Security@123) , 选择“网元策略 > 部署任务 > 部署任务”进入安全策略编排任务界面。



图13-54 进入安全策略编排任务界面

在 SecoManager 安全策略编排任务列表中可以看到由 HiSec Insight 系统联动触发的安全策略编排任务, 点击任务右侧“操作”列下面的详情按钮, 查看编排任务详细信息。



图13-55 查看编排任务详情

在安全任务编排详情页面, 可以看到 SecoManager 已给所纳管的三个逻辑设备下发了针对威胁事件的安全阻断策略, 且已部署成功。

设备名称	ESN/IP	部署状态	部署成功 (策略: 2; 对象: 0; 策略组: 0; 策略移动: 2; 系统模板: 0)	部署失败 (策略: 0; 对象: 0; 策略组: 0; 策略移动: 0; 系统模板: 0)	部署时间: 2s
DC-FW	10244768194...	部署成功	部署成功 (策略: 2; 对象: 0; 策略组: 0; 策略移动: 2; 系统模板: 0)	部署失败 (策略: 0; 对象: 0; 策略组: 0; 策略移动: 0; 系统模板: 0)	部署时间: 2s
HQ-FW	10244768192...	部署成功	部署成功 (策略: 2; 对象: 0; 策略组: 0; 策略移动: 2; 系统模板: 0)	部署失败 (策略: 0; 对象: 0; 策略组: 0; 策略移动: 0; 系统模板: 0)	部署时间: 2s
HQ-IPS	10245572904...	部署成功	部署成功 (策略: 2; 对象: 0; 策略组: 0; 策略移动: 2; 系统模板: 0)	部署失败 (策略: 0; 对象: 0; 策略组: 0; 策略移动: 0; 系统模板: 0)	部署时间: 2s

图13-56 编排任务部署结果查询

为进一步确认安全策略是否部署到执行层安全设备上，可分别登录 HQ-FW1、IPS1、和 DC-FW 设备，选择“策略 > 安全策略”查看设备上的安全策略是否有新增的由 SecoManager 下发的安全策略。设备登录信息如下：

HQ-FW1（地址：https://172.21.10.21:8443，账号：Webuser/Admin@123）；

IPS1（地址：https://172.21.10.41:8443，账号：Webuser/Admin@123）；

DC-FW（地址：https://172.21.10.23:8443，账号：Webuser/Admin@123）。

序号	名称	源	目的	服务	应用	时间段	动作
1	CIS_202412301507033	any 192.168.11.242/255.255.255...	any any	any	any		禁止
2	CIS_202412301507043	any any	any 192.168.11.242/255.255.255...	any	any		禁止
3	ipsec_ike	local untrust 100.1.33.1/255.255.255.255 100.1.35.3/255.255.255.255	local untrust 100.1.33.1/255.255.255.255 100.1.35.3/255.255.255.255	any	any		允许

图13-57 HQ-FW1 安全策略查看

序号	名称	源	目的	服务	应用	时间段	动作
1	CIS_202412301507033	any 192.168.11.242/255.255.255...	any any	any	any		禁止
2	CIS_202412301507043	any any	any 192.168.11.242/255.255.255...	any	any		禁止
3	sslvpn_oa	untrust 192.168.11.0/255.255.255.0	dmz 192.168.16.0/255.255.255.0	any	any		允许
4	nat64	untrust 2001::DB8:10::64	dmz any	any	any		允许

图13-58 DC-FW 安全策略查看

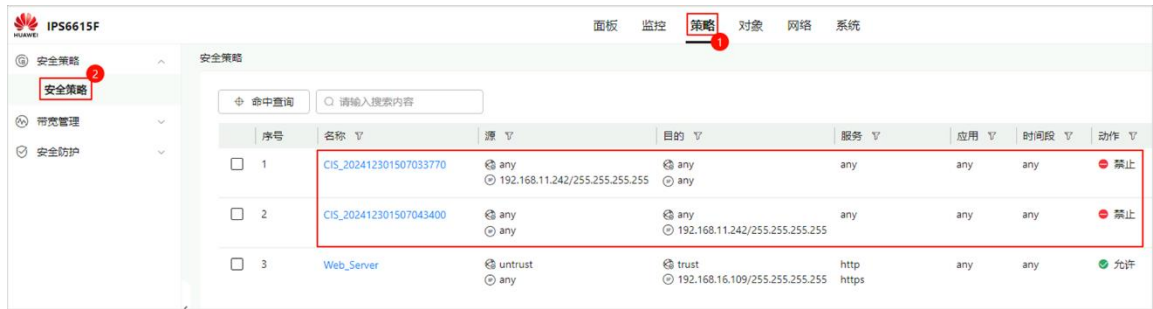


图13-59 IPS1 安全策略查看

可以看到底层安全设备上均已部署了由 SecoManager 下发的安全策略，已经实现了对应威胁事件的安全策略部署与执行，完成了安全联动和响应。

完成上述操作后，再次登录 HiSec Insight 的运维面（地址：<https://172.21.10.80:31943>，账号：admin/Security@123），点击“威胁分析 > 威胁事件”，进入威胁事件管理界面，查看原始威胁事件，可以发现其状态已切换为“已解决”。



图13-60 威胁事件处置结果查看

13.4 配置参考（仅展示本实验相关配置）

13.4.1 HQ-FW1 的配置

```
#
snmp-agent
snmp-agent local-engineid 800007DB03148C4AE9217A
#
snmp-agent sys-info version v3
snmp-agent group v3 ACTRAP noauthentication read-view iso notify-view iso
snmp-agent group v3 ACTRAP privacy read-view iso notify-view iso
snmp-agent group v3 v3group privacy read-view v3view write-view v3view notify-view v3view
snmp-agent target-host host-name ACController trap address udp-domain 172.21.10.71 udp-port 1200
params securityname ACTrap_Security v3 privacy
```

```
#
snmp-agent mib-view included iso iso
snmp-agent mib-view included v3view iso
snmp-agent usm-user v3 SecoManager
snmp-agent usm-user v3 SecoManager group v3group
snmp-agent usm-user v3 SecoManager authentication-mode sha2-256
cipher %+%##!!!!!!!"!!!!!!!"!!!!!!!"2'(C#ViSyM#A"Cl.\2,6lQ4{Vn[![FQud,>!!!!2jp5!!!!!!!"5W|bKIDZzD0x4a6vf
--'LA-20vD/DP9+gMU!!!!!!%+%#
snmp-agent usm-user v3 SecoManager privacy-mode aes256
cipher %+%##!!!!!!!"!!!!!!!"!!!!!!!"2'(C#ViSyM|U%#/{=!O>:(dVLSWLk"SqVHG!!!!2jp5!!!!!!!">!!!!^68mGC%-
+,Vh,l%WptSMrAE4U>mZ]DyA}cOZakU:%+%#
snmp-agent usm-user v3 ACTrap_Security
snmp-agent usm-user v3 ACTrap_Security group ACTRAP
snmp-agent usm-user v3 ACTrap_Security authentication-mode sha2-256
cipher %+%##!!!!!!!"!!!!!!!"!!!!!!!"2'(C#ViSyMr%T;V$:W,"spdA#FU>o0CPMM8!!!!2jp5!!!!!!!"e3`B8caEgCx8F
^OHTqJ~MuSSpK4l/@UDl<!!!!!!%+%#
snmp-agent usm-user v3 ACTrap_Security privacy-mode aes256
cipher %+%##!!!!!!!"!!!!!!!"!!!!!!!"2'(C#ViSyM9Hrd8NDqa=D"41!i$f5U2n`]Q!!!!2jp5!!!!!!!">!!!!wA}xU%2qC+\#
Uj4T`(Q$R.7G1wV0l%vwDv)4pV;L%+%#
#
snmp-agent trap source GE0/0/5
#
snmp-agent blacklist ip-block disable
snmp-agent blacklist user-block disable
#
snmp-agent protocol source-status all-interface
undo snmp-agent protocol source-status ipv6 all-interface
#
undo snmp-agent proxy protocol source-status all-interface
undo snmp-agent proxy protocol source-status ipv6 all-interface
#
snmp-agent trap enable
#
aaa
local-user netconf-admin password irreversible-cipher
$1d$x|\EYGNKz+J<)CF8$'wft*HuYu(<L(JL}5>;..{~E%Q4-AFo2m-#q5@b!$
local-user netconf-admin privilege level 3
local-user netconf-admin service-type ssh
#
interface GE0/0/5
ip address 172.21.10.51 255.255.128.0
service-manage netconf permit
service-manage snmp permit
service-manage ssh permit
#
stelnet server enable
sftp server enable
ssh server rsa-key min-length 3072
ssh user netconf-admin
```



```
ssh user netconf-admin authentication-type password
ssh user netconf-admin service-type all
ssh user netconf-admin sftp-directory flash:
ssh server-source all-interface
undo ssh ipv6 server-source all-interface
ssh authorization-type default aaa
#
ssh server cipher aes256_gcm aes128_gcm aes256_ctr aes192_ctr aes128_ctr
ssh server hmac sha2_512 sha2_256
ssh server key-exchange dh_group_exchange_sha256
#
ssh server publickey ecc rsa_sha2_256 rsa_sha2_512
#
ssh server dh-exchange min-len 3072
#
ssh client publickey ecc rsa_sha2_256 rsa_sha2_512
#
ssh client cipher aes256_gcm aes128_gcm aes256_ctr aes192_ctr aes128_ctr
ssh client hmac sha2_512 sha2_256
ssh client key-exchange dh_group_exchange_sha256
#
netconf
 protocol inbound ssh ipv4 port 830
 callhome root
#
security-policy
 rule name CIS_202412311537015270
  source-address 192.168.11.242 mask 255.255.255.255
  policy logging
  action deny
 rule name CIS_202412311537020980
  destination-address 192.168.11.242 mask 255.255.255.255
  policy logging
  action deny
 rule name SecoManager
  source-zone local
  source-zone mgmt_zone
  destination-zone local
  destination-zone mgmt_zone
  source-address 172.21.10.51 mask 255.255.255.255
  source-address 172.21.10.52 mask 255.255.255.255
  source-address 172.21.10.71 mask 255.255.255.255
  destination-address 172.21.10.51 mask 255.255.255.255
  destination-address 172.21.10.52 mask 255.255.255.255
  destination-address 172.21.10.71 mask 255.255.255.255
  action permit
#
return
```

13.4.2 DC-FW 的配置

```
#
aaa
 local-user netconf-admin password irreversible-cipher $1d$qH&Q3joJ-
X`X0p'Q$]eoW@[9kl/)_~ZK>7A%9iN\T}gtz+GWgP=2e^.P$
 local-user netconf-admin privilege level 3
 local-user netconf-admin service-type ssh
#
interface GE0/0/5
 ip address 172.21.10.53 255.255.128.0
 service-manage netconf permit
 service-manage snmp permit
 service-manage ssh permit
#
snmp-agent
snmp-agent local-engineid 800007DB03148C4AE922BF
#
snmp-agent sys-info version v3
snmp-agent group v3 ACTRAP noauthentication read-view iso notify-view iso
snmp-agent group v3 ACTRAP privacy read-view iso notify-view iso
snmp-agent group v3 v3group privacy read-view v3view write-view v3view notify-view v3view
snmp-agent target-host host-name ACController trap address udp-domain 172.21.10.71 udp-port 1200
params securityname ACTrap_Security v3 privacy
#
snmp-agent mib-view included iso iso
snmp-agent mib-view included v3view iso
snmp-agent usm-user v3 SecoManager
snmp-agent usm-user v3 SecoManager group v3group
snmp-agent usm-user v3 SecoManager authentication-mode sha2-256
cipher %+%##!!!!!!!"!!!!!"!!!!*!!!!L7LG%PT+oLst'LOlv%{3(}Lg8fJq61DB`|B!!!!2jp5!!!!!!;IVx:Ry\'6%i@>A[]
sDL^e8YS3[T#M[])a;!!!!%+%#
snmp-agent usm-user v3 SecoManager privacy-mode aes256
cipher %+%##!!!!!!!"!!!!!"!!!!*!!!!L7LG%PT+oLHT]:(%2^_6+OjYNI]O_J3k3mP!!!!2jp5!!!!!!>!!!!;mf<O^,Bp<&z
me+f<Wx!lgx{X:KI=)drL=6z9Q";%+%#
snmp-agent usm-user v3 ACTrap_Security
snmp-agent usm-user v3 ACTrap_Security group ACTRAP
snmp-agent usm-user v3 ACTrap_Security authentication-mode sha2-256
cipher %+%##!!!!!!!"!!!!!"!!!!*!!!!L7LG%PT+oLloZFUFfOl:wUFsGetmB6IZ7$Z!!!!2jp5!!!!!!>!!!!1/sYMRHN%$9
V=.LqrLA&F[zP1nO[DVjRd~!!!!%+%#
snmp-agent usm-user v3 ACTrap_Security privacy-mode aes256
cipher %+%##!!!!!!!"!!!!!"!!!!*!!!!L7LG%PT+oLG$O@FR5(eFAs6M1S"Kh~{J5xB!!!!2jp5!!!!!!>!!!!5*2a)u:@%):3
IKJMHY`59oGL4~X(9Lb'1e>qw,;"%+%#
#
snmp-agent trap source GE0/0/5
#
snmp-agent blacklist ip-block disable
snmp-agent blacklist user-block disable
#
snmp-agent protocol source-status all-interface
```

```
undo snmp-agent protocol source-status ipv6 all-interface
#
undo snmp-agent proxy protocol source-status all-interface
undo snmp-agent proxy protocol source-status ipv6 all-interface
#
snmp-agent trap enable
#
stelnet server enable
sftp server enable
ssh server rsa-key min-length 3072
ssh user netconf-admin
ssh user netconf-admin authentication-type password
ssh user netconf-admin service-type all
ssh user netconf-admin sftp-directory flash:
ssh server-source all-interface
undo ssh ipv6 server-source all-interface
ssh authorization-type default aaa
#
ssh server cipher aes256_gcm aes128_gcm aes256_ctr aes192_ctr aes128_ctr
ssh server hmac sha2_512 sha2_256
ssh server key-exchange dh_group_exchange_sha256
#
ssh server publickey ecc rsa_sha2_256 rsa_sha2_512
#
ssh server dh-exchange min-len 3072
#
ssh client publickey ecc rsa_sha2_256 rsa_sha2_512
#
ssh client cipher aes256_gcm aes128_gcm aes256_ctr aes192_ctr aes128_ctr
ssh client hmac sha2_512 sha2_256
ssh client key-exchange dh_group_exchange_sha256
#
netconf
  protocol inbound ssh ipv4 port 830
  callhome root
#
security-policy
  rule name CIS_202412311537015270
    source-address 192.168.11.242 mask 255.255.255.255
    policy logging
    action deny
  rule name CIS_202412311537020980
    destination-address 192.168.11.242 mask 255.255.255.255
    policy logging
    action deny
  rule name SecoManager
    source-zone local
    source-zone mgmt_zone
```

```
destination-zone local
destination-zone mgmt_zone
source-address 172.21.10.53 mask 255.255.255.255
source-address 172.21.10.71 mask 255.255.255.255
destination-address 172.21.10.53 mask 255.255.255.255
destination-address 172.21.10.71 mask 255.255.255.255
action permit
#
return
```

13.4.3 IPS1 的配置

```
#
aaa
 local-user netconf-admin password irreversible-cipher
 $1d$[rAv+Hr",L;uNbR#$pPvqA(@tZ63jElDm@ow"m`:QI7[=;JiqSwNP=6}1$
 local-user netconf-admin privilege level 3
 local-user netconf-admin service-type ssh
#
snmp-agent
snmp-agent local-engineid 800007DB03F4E451DE2F6E
#
snmp-agent sys-info version v3
snmp-agent group v3 ACTRAP noauthentication read-view iso notify-view iso
snmp-agent group v3 ACTRAP privacy read-view iso notify-view iso
snmp-agent group v3 v3group privacy read-view v3view write-view v3view notify-view v3view
snmp-agent target-host host-name ACController trap address udp-domain 172.21.10.71 udp-port 1200
params securityname ACTrap_Security v3 privacy
#
snmp-agent mib-view included iso iso
snmp-agent mib-view included v3view iso
snmp-agent usm-user v3 SecoManager
snmp-agent usm-user v3 SecoManager group v3group
snmp-agent usm-user v3 SecoManager authentication-mode sha2-256
cipher %+%##!!!!!!"!!!!!!"!!!!!!*!!!!!!3>YL.gB*dLtR0j%vL5scw|~S`8MMOfj$F!!!!!!2jp5!!!!!!"!!!!!!WS)p=V`\\MNT2\\hX
C_#b/YrzJI&{Y~25quv0!!!!!!%+%#
snmp-agent usm-user v3 SecoManager privacy-mode aes256
cipher %+%##!!!!!!"!!!!!!"!!!!!!*!!!!!!3>YL.gB*\uJ-
P[h;3="U,L2F:EU8c3F!!!!!!2jp5!!!!!!>!!!!XE&z8i_r@FVEKfj39MJ$YZi^Y@\\H09W)cn)*P"gN%+%#
snmp-agent usm-user v3 ACTrap_Security
snmp-agent usm-user v3 ACTrap_Security group ACTRAP
snmp-agent usm-user v3 ACTrap_Security authentication-mode sha2-256
cipher %+%##!!!!!!"!!!!!!"!!!!!!*!!!!!!3>YL.gB*8u[7Fi7h*Xe{hw;9_cU1+9u>H!!!!!!2jp5!!!!!!"!!!!!!v2:18>+f:{Qe2Hzpw
_O#|B4>C>{(,zl=rO!!!!!!%+%#
snmp-agent usm-user v3 ACTrap_Security privacy-mode aes256
cipher %+%##!!!!!!"!!!!!!"!!!!!!*!!!!!!3>YL.gB*y<&yUjZN!8l#k.^YyQT_1""~!!!!!!2jp5!!!!!!>!!!!e0ntDnab#Oz~t08$
zkCuYXy1/6H[.Q:gF']J]O%+%#
#
snmp-agent trap source MEth0/0/0
#
```

```
snmp-agent blacklist ip-block disable
snmp-agent blacklist user-block disable
#
snmp-agent protocol source-status all-interface
undo snmp-agent protocol source-status ipv6 all-interface
#
undo snmp-agent proxy protocol source-status all-interface
undo snmp-agent proxy protocol source-status ipv6 all-interface
#
snmp-agent trap enable
#
stelnet server enable
sftp server enable
ssh server rsa-key min-length 3072
ssh user netconf-admin
ssh user netconf-admin authentication-type password
ssh user netconf-admin service-type all
ssh user netconf-admin sftp-directory flash:
ssh server-source all-interface
undo ssh ipv6 server-source all-interface
ssh authorization-type default aaa
#
ssh server cipher aes256_gcm aes128_gcm aes256_ctr aes192_ctr aes128_ctr
ssh server hmac sha2_512 sha2_256
ssh server key-exchange dh_group_exchange_sha256
#
ssh server publickey rsa_sha2_256 rsa_sha2_512
#
ssh server dh-exchange min-len 3072
#
ssh client publickey rsa_sha2_256 rsa_sha2_512
#
ssh client cipher aes256_gcm aes128_gcm aes256_ctr aes192_ctr aes128_ctr
ssh client hmac sha2_512 sha2_256
ssh client key-exchange dh_group_exchange_sha256
#
netconf
  protocol inbound ssh ipv4 port 830
#
security-policy
  default action permit
  rule name CIS_202412311537015270
    source-address 192.168.11.242 mask 255.255.255.255
    policy logging
    action deny
  rule name CIS_202412311537020980
    destination-address 192.168.11.242 mask 255.255.255.255
    policy logging
```

```
    action deny  
#  
return
```

13.5 思考题

SecoManager 除了设备和安全策略的集中管理外, 还有哪些功能可以用于安全设备的运维中?

答案: SecoManager 还支持对安全域、地址集、服务和日志等对象的集中规划管理。

14 故障排查综合实验

14.1 实验介绍

14.1.1 关于本实验

为防止非公司员工接入总部网络，办公区域的用户（PC2 模拟）只有通过 802.1X 认证后，才能访问公司总部的网络资源。

公司网络分为总部网络和分支网络，防火墙作为出口设备部署在总部和分支网络的边界，通过配置防火墙的 IPsec VPN 技术，实现总部与分支的数据加密传输，以保障通信的安全。

总部网络中部署有 Web 和 FTP 服务器提供网络服务，为保证分支网络用户访问服务器的安全性，在服务器前端部署了防火墙设备对用户的访问进行检查，如果发现威胁风险，防火墙将阻断访问流量。

由于公司网络中的需求繁杂，安全技术多样，因此，本实验通过梳理各种安全技术的故障排查流程，为公司管理员提供运维参考。

14.1.2 实验组网介绍

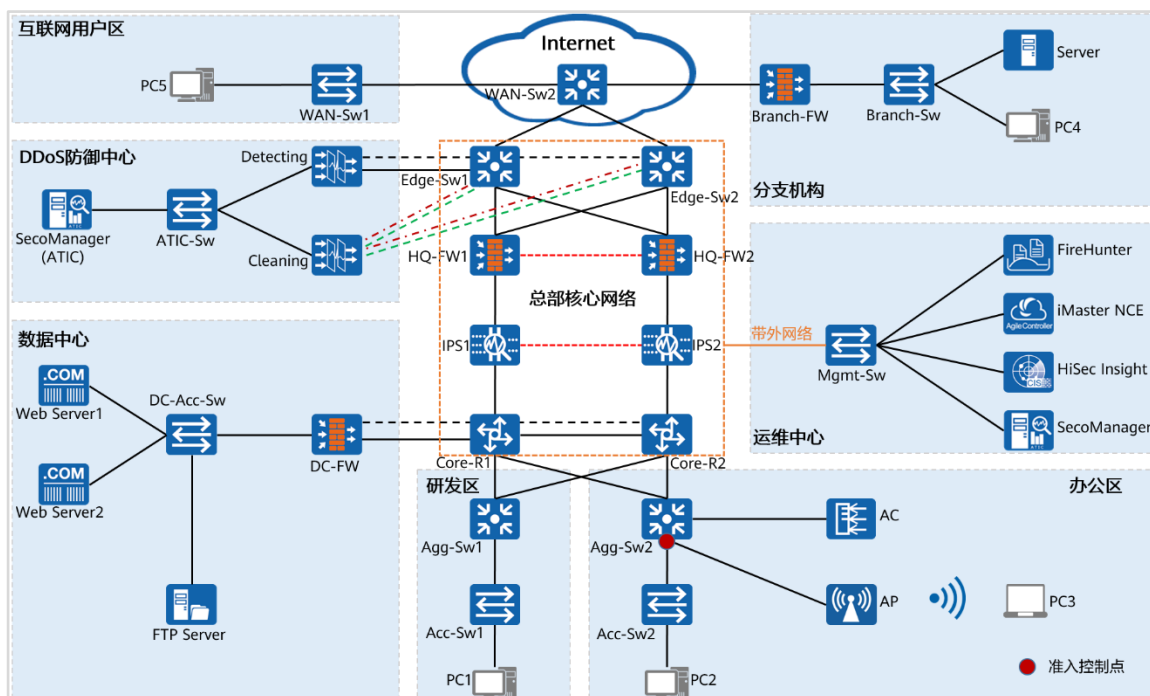


图14-1 实验拓扑图

14.1.3 实验规划

1. 由于办公区域用户只有通过 802.1X 认证才能接入总部网络，首先介绍准入控制的故障排查思路。
2. 为保障总部网络与分支网络的通信安全，需要在总部出口防火墙 HQ-FW1 和 HQ-FW2 设备与分支出口的 Branch-FW 设备上部署 IPsec VPN 技术，加密站点间通信数据。为了保障总部和分支的正常互访，管理员需要掌握 IPsec VPN 技术的部署和排障。
3. 总部服务器前端部署了防火墙 DC-FW 设备，并配置了内容安全过滤技术，用于检查访问服务器的流量，为保障内容安全技术的正确规划和部署，最后将介绍内容安全的故障排查技巧。

14.2 实验配置任务

14.2.1 配置思路

1. 有线 802.1X 认证技术请参考“实验 5 终端安全接入综合实验”进行配置部署，本实验不再赘述，只介绍故障排查的思路和过程。
2. IPsec VPN 技术请参考“实验 6 VPN 综合实验”进行配置部署，本实验不再赘述，只介绍故障排查的思路和过程。
3. 内容安全技术请参考“实验 8 防火墙内容安全实验”进行配置部署，本实验不再赘述，只介绍故障排查的思路和过程。

14.2.2 配置步骤

步骤 1 有线 802.1X 认证故障排查

有线 802.1X 认证的排查思路如下图，根据思路脑图，进行逐步排查。



图14-2 802.1X 故障排查流程

以 Windows 客户端为例，使用 Windows 系统的认证功能，需要开启“Wired AutoConfig”和“WLAN AutoConfig”两个服务，在 Windows 系统中使用 Windows+R 打开终端，或者搜索命令提示符打开终端，输入“services.msc”，确定即可，如下图：

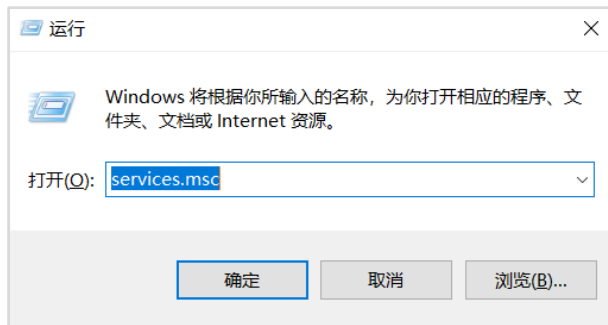


图14-3 进入 Windows 服务控制界面

查看服务列表中的“Wired AutoConfig”和“WLAN AutoConfig”服务是否为“正在运行”的状态。如果不是，双击这两个服务的名称，进入属性配置窗口启动服务，并将“启动类型”改为自动，如下图：

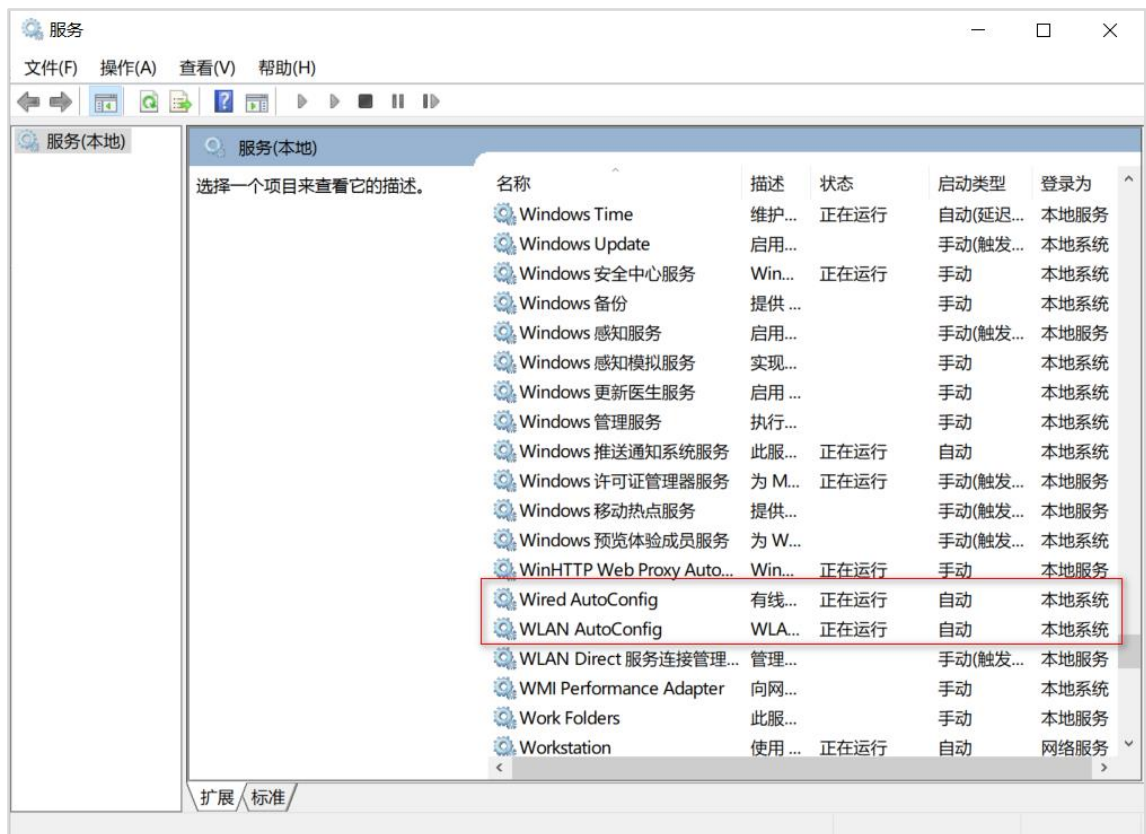


图14-4 确认“Wired AutoConfig”和“WLAN AutoConfig”服务运行状态

在用户的终端设备 PC2 上查看 IP 地址是否正常。如果使用 DHCP 获取地址，查看 IP 地址和网关等信息获取是否正确，打开 CMD 窗口，使用“ipconfig”命令，查看 IP 地址，如下图。

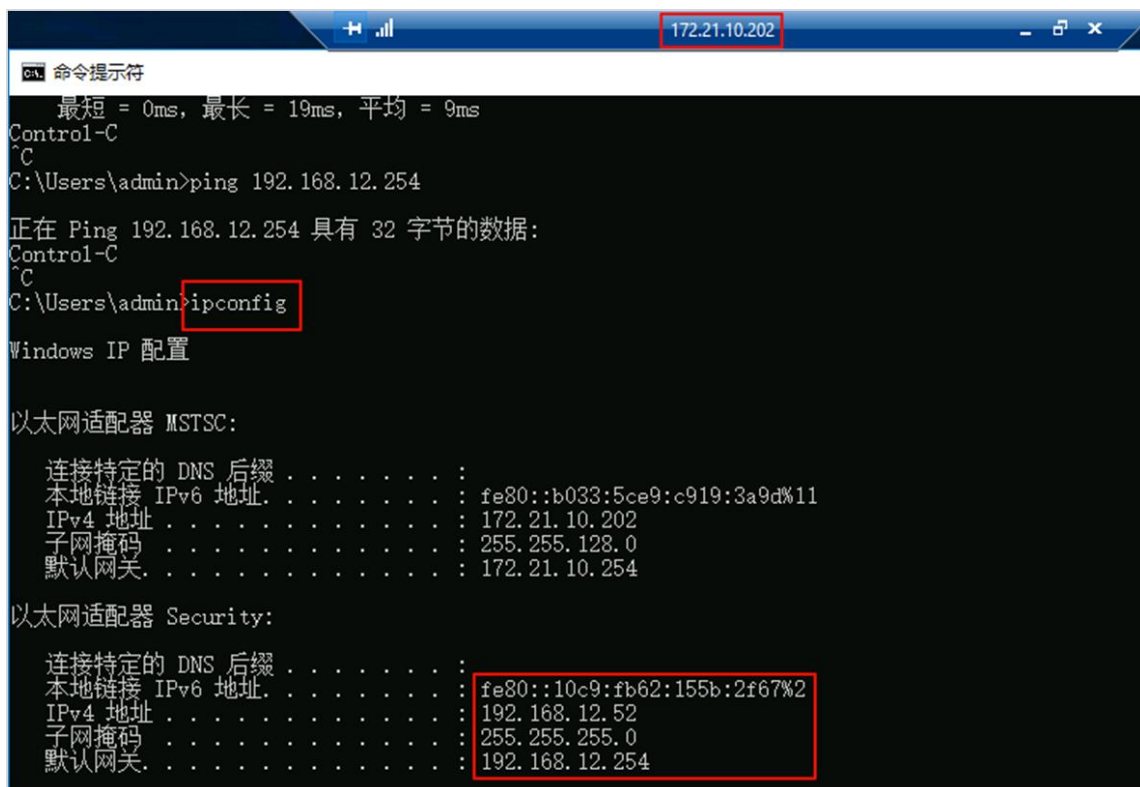


图14-5 查看 PC2 地址获取情况

排查无误后，在 Window 客户端上输入用户名密码进行登录测试，打开“控制面板 > 网络和 Internet > 网络连接”，右键单机“Security”网卡，选择“属性”，如下图。

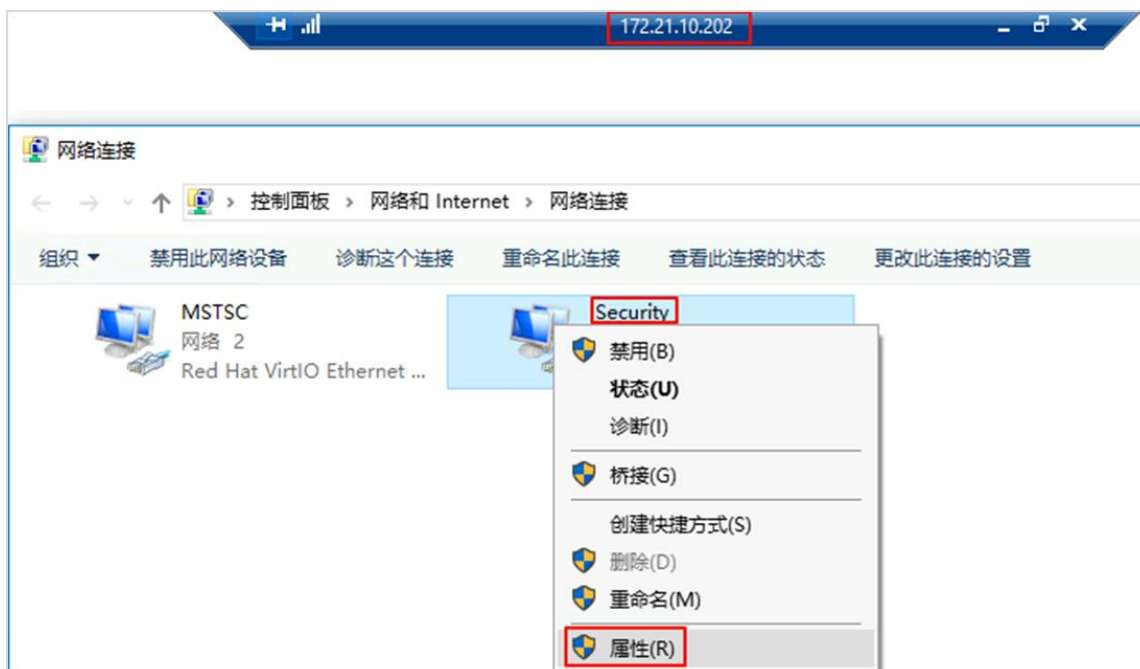


图14-6 进入“Security”网卡属性界面

在“身份验证”窗口单击“其他设置”，在弹出的“802.1X 设置”窗口单击“替换凭证”，如下图。

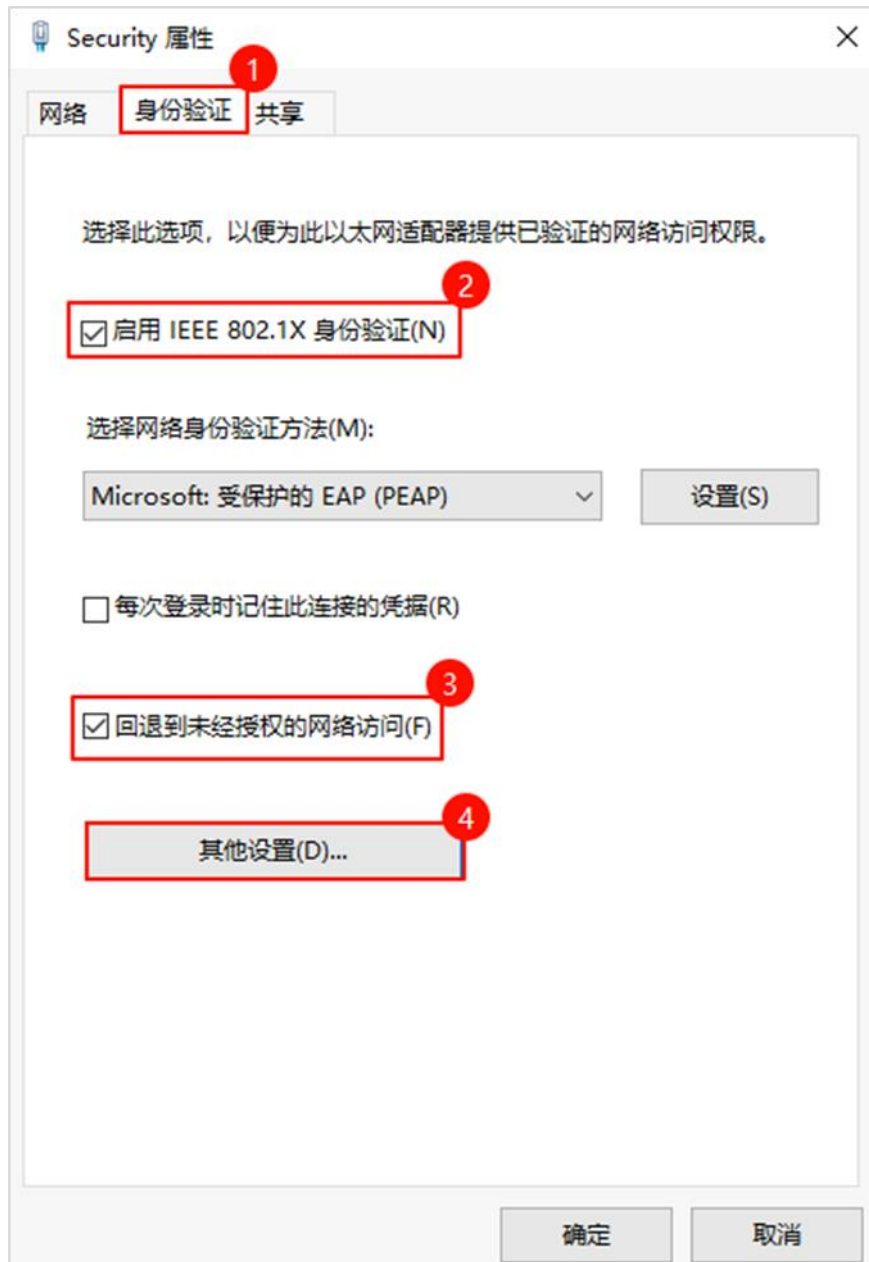




图14-7 替换认证凭据

重新输入用户名和密码进行认证，认证成功后，网络连接正常，如下图。

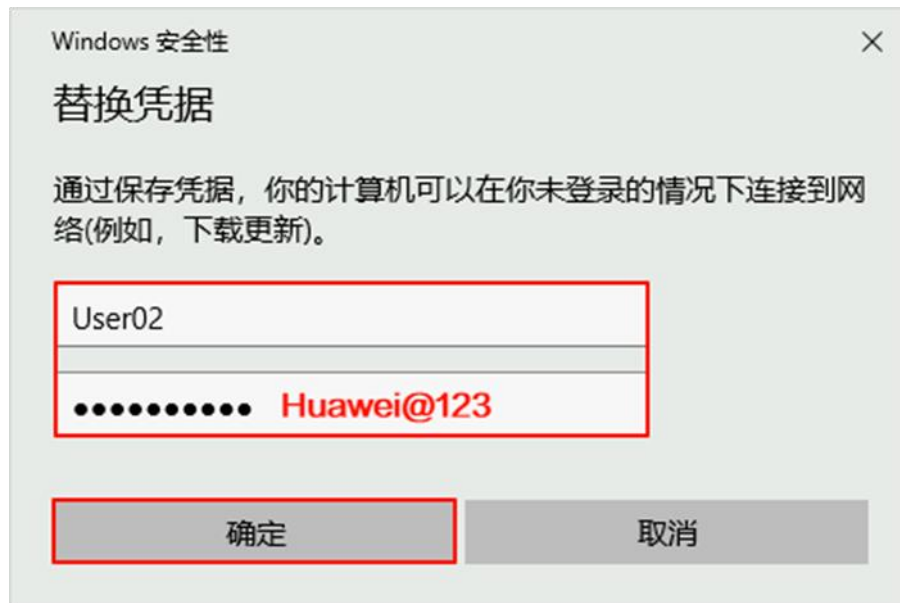


图14-8 编辑认证凭据

客户端故障排查完成后，登录准入控制设备排查故障。

以交换机为准入控制设备为例，查看准入控制设备上的认证服务器模板配置是否正确，使用命令“display radius-server configuration template Campus”，如下图。

```
<AGG-SW2>display radius-server configuration template Campus
-----
Server-template-name           : Campus
Server-template-index          : 2
Protocol-version               : standard
Traffic-unit                   : B
Shared-secret-key              : *****
Group-filter                   : class
Timeout-interval(in second)    : 2
Retransmission                 : 5
EndPacketSendTime              : 3
Dead time(in minute)           : 5
Domain-included                : Original
NAS-IP-Address                 : 172.21.10.4
Calling-station-id MAC-format  : xxxx-xxxx-xxxx
Called-station-id MAC-format   : XX-XX-XX-XX-XX-XX
NAS-Port-ID format             : New
Service-type                   : -
NAS-IPv6-Address               : ::
Server algorithm               : master-backup based-user
Detect-interval(in second)     : 60
Detect up-server(in second)    : 0
Detect timeout(in second)      : 3
Chargeable-user-identity       : Not Support
CUI Not reject                 : No
Enable framed-ip-address       : No
```

```

Enable IPv4 traffic-statistics encapsulation : No
Authentication Server 1                : 172.21.10.78    Port:1812  Weight:80  [up]
                                         Vrf:- LoopBack:NULL Vlanif:NULL
                                         Source IP: 172.21.10.4
Accounting Server 1                    : 172.21.10.78    Port:1813  Weight:80  [up]
                                         Vrf:- LoopBack:NULL Vlanif:NULL
                                         Source IP: 172.21.10.4
-----

```

查看认证计费模板配置是否使用了 RADIUS 协议，如下图。

```
<AGG-SW2>display authentication-scheme radius
```

```

Authentication-scheme-name      : radius
Authentication-method           : RADIUS
Radius authentication-type of admin : PAP(all)
Server no-response accounting    : NO
Server no-response authorization : NO
Location after radius reject     : None

```

```
<AGG-SW2>display accounting-scheme radius
```

```

Accounting-scheme-name          : radius
Accounting-method               : RADIUS
Realtime-accounting-switch      : Enabled
Realtime-accounting-interval(min) : 15
Start-accounting-fail-policy    : Offline
Realtime-accounting-fail-policy : Online
Realtime-accounting-failure-retries : 3

```

查看认证域配置是否正确，如下图。

```
<AGG-SW2>display domain name default
```

```

Domain-name                     : default
Domain-index                    : 0
Domain-state                    : Active
Authentication-scheme-name      : radius
Accounting-scheme-name          : radius
Authorization-scheme-name       : -
Service-scheme-name             : -
RADIUS-server-template          : Campus
Accounting-copy-RADIUS-template : -
HWTACACS-server-template        : -
HACA-server-template            : -
Push-url-address                : -
Flow-statistic                  : -

```

查看认证 profile 配置是否使用了 default 域，如下图。

```
<AGG-SW2>display authentication-profile configuration name dot1x
```

```

Profile name                    : dot1x

```

Dot1x access profile name	: dot1x
Mac access profile name	: -
Portal access profile name	: -
Free rule template	: -
Force domain	: -
Dot1x force domain	: -
Mac-authen force domain	: -
Portal force domain	: -
Default domain	: -
Dot1x default domain	: -
Mac-authen default domain	: -
Portal default domain	: -
Permit domain	: -
Authentication handshake	: Enable
Authentication handshake period	: 300s
Auth-fail re-auth period	: 60s
Pre-auth re-auth period	: 60s
Auth-fail aging time	: 82800s
Pre-auth aging time	: 82800s
Author-keep aging time	: 0s
Dot1x-mac-bypass	: Disable
Mac authen before 802.1X authen	: Disable
Single-access	: Disable
Device-type authorize service-scheme	: -
Iconnect device authorize service-scheme	: -
Mac move detect enable	: Enable
Authentication mode	: multi-authen
Authen-fail authorize service-scheme	: -
Authen-server-down authorize service-scheme	: -
Authen-server-down authorize keep	: -
Authen-server-noreply authorize keep	: -
Authen-server-down close re-authen	: N
Pre-authen authorize service-scheme	: -
Security-name-delimiter	: -
Domain-name-delimiter	: -
Domain-location	: -
Domainname-parse-direction	: -
SVF flag	: Disable
Ip-static-user	: Disable
Roam-realtime-accounting	: Enable
Update-IP-realtime-accounting	: Enable
IP-address in-accounting-start	: Enable
IPv4-address in-accounting-start mandatory	: Enable
Linkdown offline delay time	: 10
Termination action	: -
Control direction	: Inbound
Redirect ACL original url	: Disable
Update-Info-realtime-accounting	: Enable

```
IPv6 Control Flag           : N
No IP Check Flag           : N
IP Conflict Check Flag     : Y
Authentication no-replace dot1x : -
Lldp sensor-ap authentication disable : Disable
```

使用 test-aaa 命令，测试配置的认证模板 Campus 能够认证通过，如下图。

```
<AGG-SW2>test-aaa User02 Huawei@123 radius-template Campus pap
Info: Account test succeeded.
```

认证通过表明模板配置没有问题，认证不通过，请根据错误提示的修改配置。

如果用户终端通过二层交换机与准入控制设备交互认证报文，检查二层交换机上是否配置了 EAP 报文透传功能，如下图。

```
[ACC-Sw1]display l2protocol-tunnel group-MAC all
Protocol          EncapType ProtocolType Protocol-MAC   Group-MAC      Pri
-----
stp               llc          dsap 0x42      0180-c200-0000 0100-0ccd-cdd0 0
                  ssap 0x42
dot1x             -            -              0180-c200-0003 0100-0000-0002 0
```

准入控制设备上的故障排查完成后，登录 NCE-Campus 排查故障。

登录 NCE-Campus，选择“准入管理 > 准入资源 > 准入用户管理”，在创建的用户组“HQ_Office”中，查看 user02 账号是够存在，状态是否为“启用”，如下图。

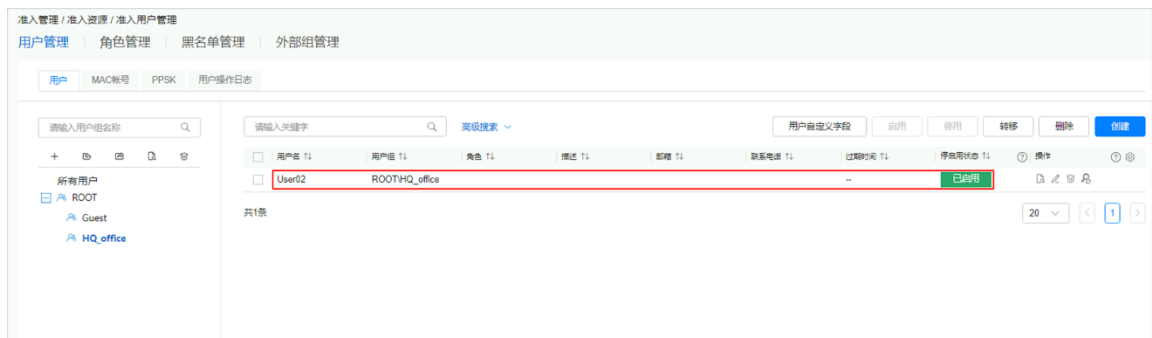


图14-9 查看 802.1X 认证账户信息

查看准入控制设备是否添加，选择“准入管理 > 准入资源 > 准入设备”，查看添加的设备 IP 地址是否正确，RADIUS 认证是否开启。

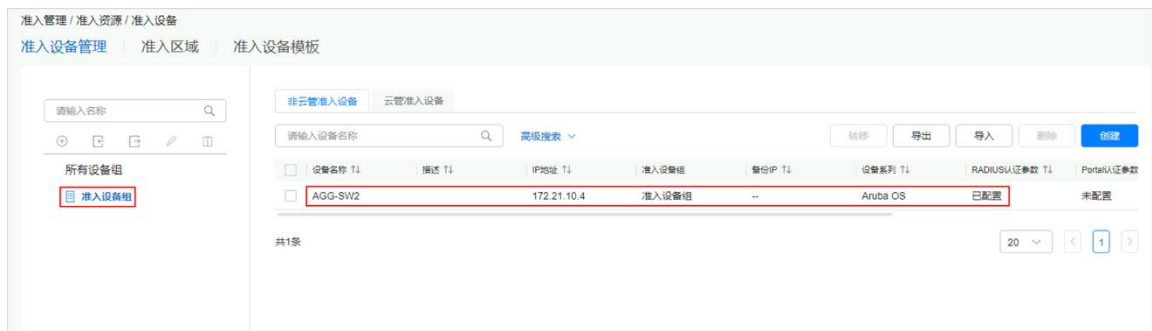


图14-10 查看 802.1X 准入认证设备

查看认证授权规则，选择“策略>准入>准入策略>认证授权”，分别查看认证规则，授权结果和授权规则，如下图。



图14-11 查看认证规则



图14-12 查看授权规则

确认无误后，查看运维中心，了解具体的认证过程。选择“准入管理 > 准入概览”，查看认证信息概览，如下图。



图14-13 查看认证信息概览

若页面上存在“认证失败次数”，则单击“认证失败次数”，会出现“认证日志”，选择“RADIUS 认证日志”，则会展示详细的认证信息，如下图。

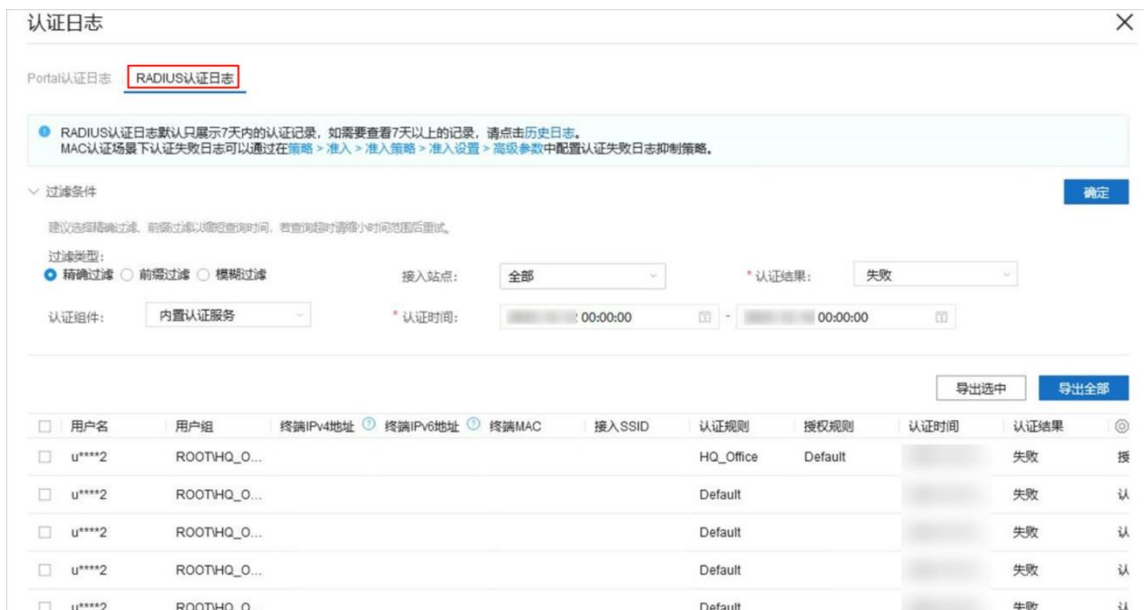


图14-14 查看 RADIUS 认证日志

单击认证日志最右侧的“查看详情”，则可以查看详细的认证失败原因排查故障，如下图。

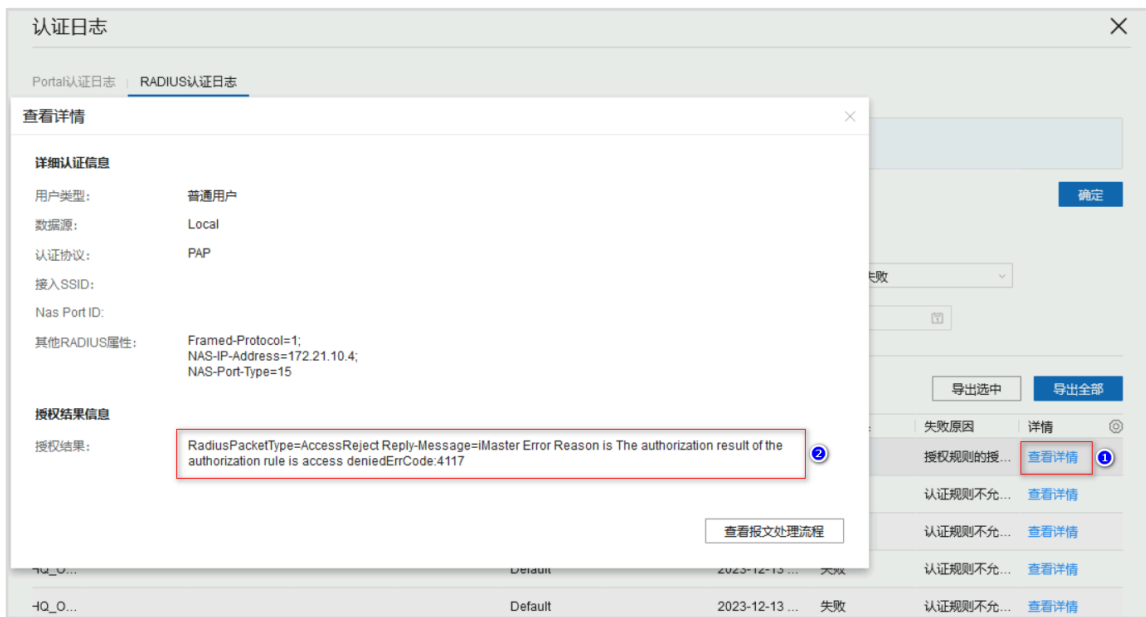


图14-15 查看日志详情

单击“查看报文处理流程”，则可以查看认证报文的交互过程，如下图。



图14-16 查看报文处理流程

步骤 2 IPsec VPN 故障排查

IPsec VPN 故障的排查思路如下图，根据思路脑图，进行逐步排查。



图14-17 IPsec VPN 故障排查思路

由于 HQ-FW1 和 HQ-FW2 是总部的出口设备，并且运行了双机热备功能，HQ-FW1 作为主设备负责流量的转发，所以登录 HQ-FW1 进行 IPsec VPN 故障排查。

登录 HQ-FW1 设备 Web 管理界面，查看 IKE 对等体路由是否可达，选择“网络 > IPsec > IPsec”，单击 IPsec 策略的“诊断”，使用 IPsec 策略的自动诊断功能。



图14-18 进入 IPsec 策略自动诊断界面



图14-19 开始 IPsec 策略自动化诊断

等待 IPsec 策略自动诊断完成后, 效果如下:

IPSec诊断

×

策略名称

policy1-1

本端接口

GE0/0/1

诊断方式

☐ 本端主动发起协商 (仅点到点场景、且对端地址固定时支持此方式)

☒ 接收对端协商报文 (对端是点到多点时不适用此方式)

对端地址

100.1.33.1

诊断

导出

诊断项	诊断结果
阶段1协商结果:	⊗ 超时。对端不返回协商失败信息(可能原因:协商模式、协商版本、封装模式、加密算法、认证算法、DH组、完整性算法中有配置不匹配)或者路由不可达。

共 1 条

关闭

图14-20 IPSec 策略诊断结果

按照设备提示消息进行排查处理，确保对等体可达后，在 HQ-FW1 设备 Web 管理界面选择“策略 > 安全策略 > 安全策略”，查看安全策略是否放行了 IKE 的协商报文，如下图。

USG6525F 主

面板 监控 **策略** 对象 网络 系统

安全策略

命中查询 ☐ 只显示过期策略

	序号	名称	源	目的	服务	应用	时间段	动作
☐	1	ipsec_ike	local untrust 100.1.33.1/255.255.255.255 100.1.35.3/255.255.255.255	local untrust 100.1.33.1/255.255.255.255 100.1.35.3/255.255.255.255	any	any		允许
☐	2	ipsec_oa	trust untrust 192.168.11.0/255.255.255.0 192.168.14.0/255.255.255.0	trust untrust 192.168.11.0/255.255.255.0 192.168.14.0/255.255.255.0	any	any		允许
☐	3	sslvpn_gw	untrust 100.1.15.0/255.255.255.0	local any	any	any		允许
☐	4	sslvpn_oa	untrust 192.168.11.0/255.255.255.0	trust 192.168.16.0/255.255.255.0	http ftp	any		允许
☐	5	HQ_Web_Server	untrust any	trust 192.168.16.109/255.255.255...	any	any		允许

图14-21 查看 HQ-FW1 设备关于 IPSec 协商流的安全策略

安全策略排查完成后，选择“网络 > IPsec > IPsec”，单击 IPsec 策略的“编辑”按钮，在 IPsec 策略中单击“安全提议”中查看 HQ-FW1 上的 IKE 参数是否与 Branch-FW 上的一致，如下图。



图14-22 查看 HQ-FW1 设备 IKE 参数

IKE SA 建立失败的故障排查完成后，排查 IPSec SA 建立失败的原因。

在 IPSec 策略边界界面，单击“安全提议”，查看 HQ-FW1 上的 IPSec 参数是否与 Branch-FW 上的一致，如下图。



图14-23 查看 HQ-FW1 设备 IPSec 参数

排查完成后，排查 HQ-FW1 上的待加密的数据流（即感兴趣流量）与 Branch-FW 上是否互为镜像，在 HQ-FW1 和 Branch-FW 上分别查看，如下图。

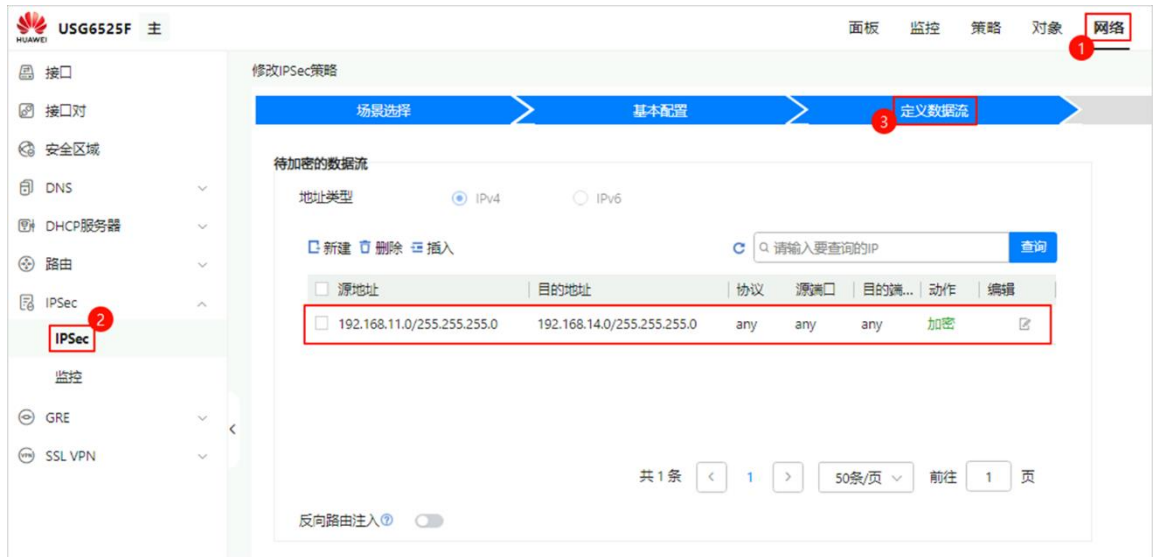


图14-24 查看 HQ-FW1 设备 IPsec VPN 待加密业务流

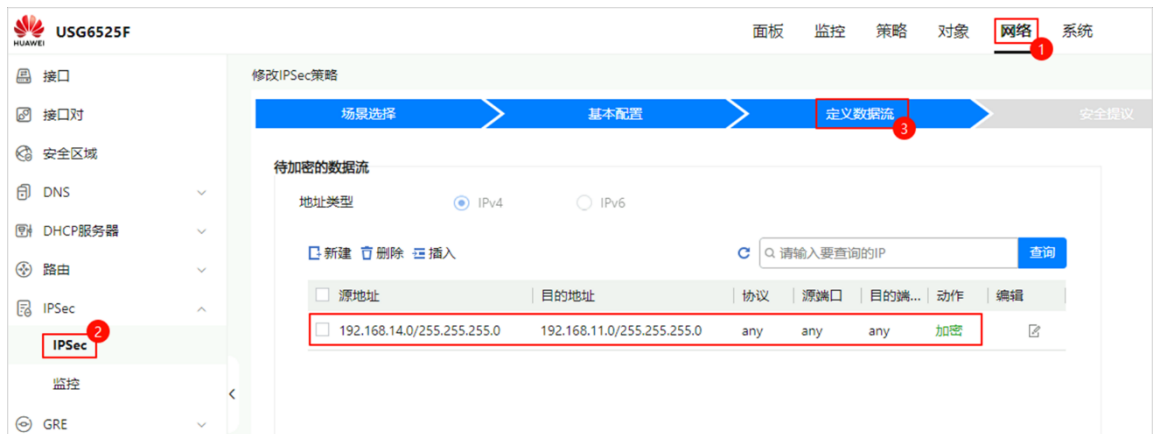


图14-25 查看 Branch-FW 设备 IPsec VPN 待加密业务流

排查完成后，以 HQ-FW1 为例，查看 IPsec 策略是否调用在了正确的接口上，如下图。



图14-26 查看 HQ-FW1 设备 IPsec 策略基本配置

IKE SA 和 IPsec SA 的故障排查完成后，IPsec 隧道就行够正常建立，在 HQ-FW1 设备 Web 管理界面，单机 IPsec 策略列表中的“详情”按钮，可以查看到具体协商的信息，如下图。



图14-27 进入 IPsec 策略详情界面

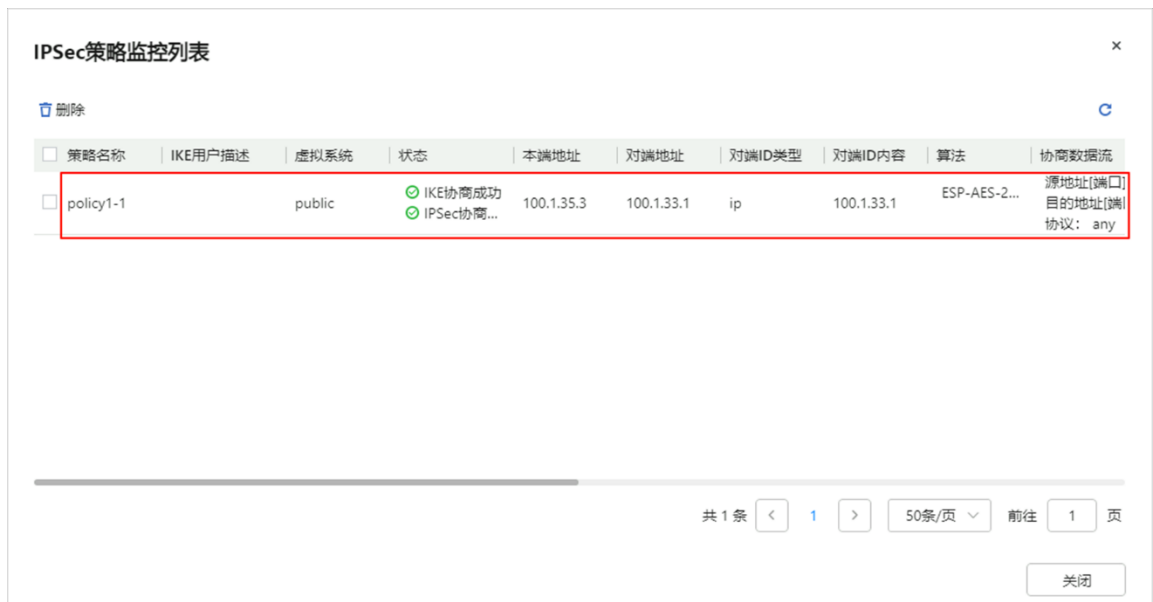


图14-28 查看 HQ-FW1 设备 IPsec 策略协商详情

上述排查工作完成后，使用终端进行连通性测试，如果不成功，查看安全策略是否放行了 IPsec 策略中匹配的感兴趣流量（业务流量）。

在 HQ-FW1 设备 Web 管理界面选择“策略 > 安全策略 > 安全策略”，查看安全策略是否放行了 IPsec VPN 业务流量，如下图。

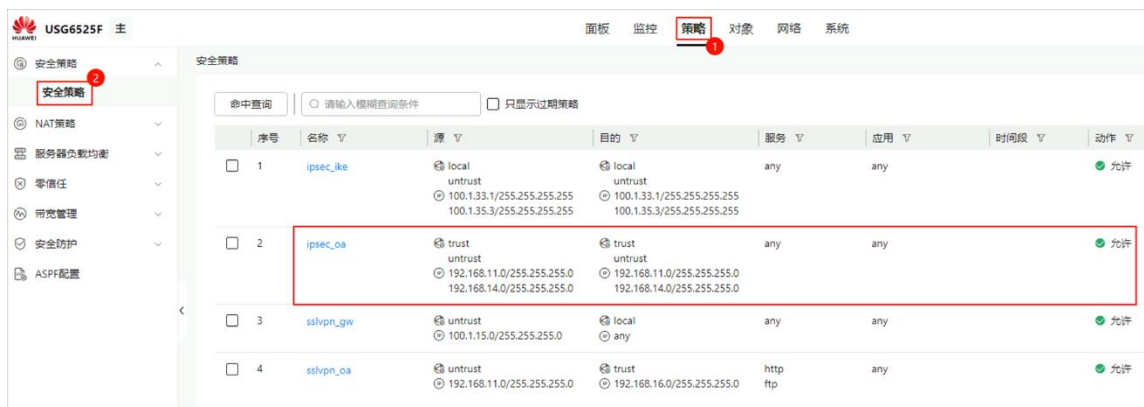


图14-29 查看 HQ-FW1 设备针对 IPsec VPN 业务流量的安全策略

如果总部在 HQ-FW1 和 HQ-FW2 上部署了源 NAT 策略，还需要排查是否配置了 No-NAT 的策略进行 NAT 穿越，对感兴趣流量不做转换，本套实验暂不涉及。

步骤 3 内容安全故障排查

内容安全的排查思路如下图，根据思路脑图，进行逐步排查。

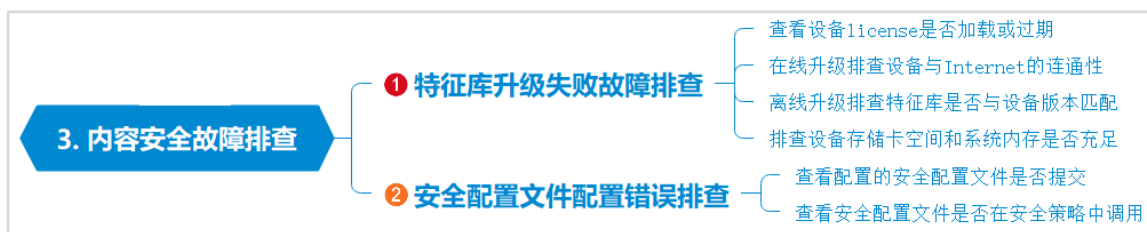


图14-30 内容安全故障排查思路

由于总部网络中在服务器前端部署了 DC-FW 用于进行访问服务器的流量检查，因此在 DC-FW 上部署了内容安全的功能，如 URL 过滤和内容过滤等。

如果运维过程中，发现配置的内容安全功能未生效，首先排查设备的 License 是否导入或者过期，在 DC-FW 设备 Web 管理界面上选择“系统 > License 管理”，查看 License 的过期时间和授权的功能等信息，如下图。



图14-31 查看 DC-FW 设备的 License 信息

License 处于过期或者未授权的状态时，请登录华为官网申请 License。

升级设备的特征库，选择“系统 > 升级中心”，查看特征库的升级版本，如果不是最新的特征库，通过在线或离线方式升级，如下图。



图14-32 查看 DC-FW 设备特征库升级信息

在线升级前，请 DC-FW 测试与升级中心地址的连通性，如果不能通过 Internet 连接升级中心，请使用离线升级，如下图。



图14-33 测试 DC-FW 设备与升级中心的连通性

采用离线升级时，需要先获取 DC-FW 的版本信息，选择“系统 > 系统更新”，查看“当前版本”，如下图。

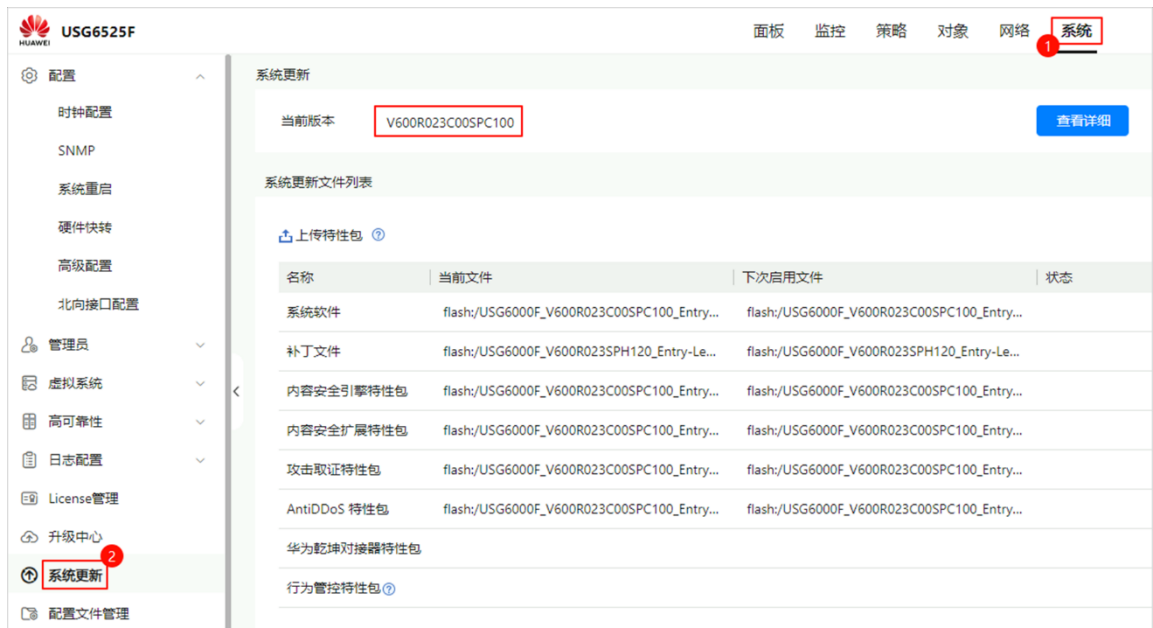


图14-34 查看 DC-FW 设备系统软件当前版本

登录华为升级中心网站 sec.huawei.com，在“特征库升级 > 下载特征库与组件包”页面搜索对应产品版本，下载对应的特征库和组件包，如下图。

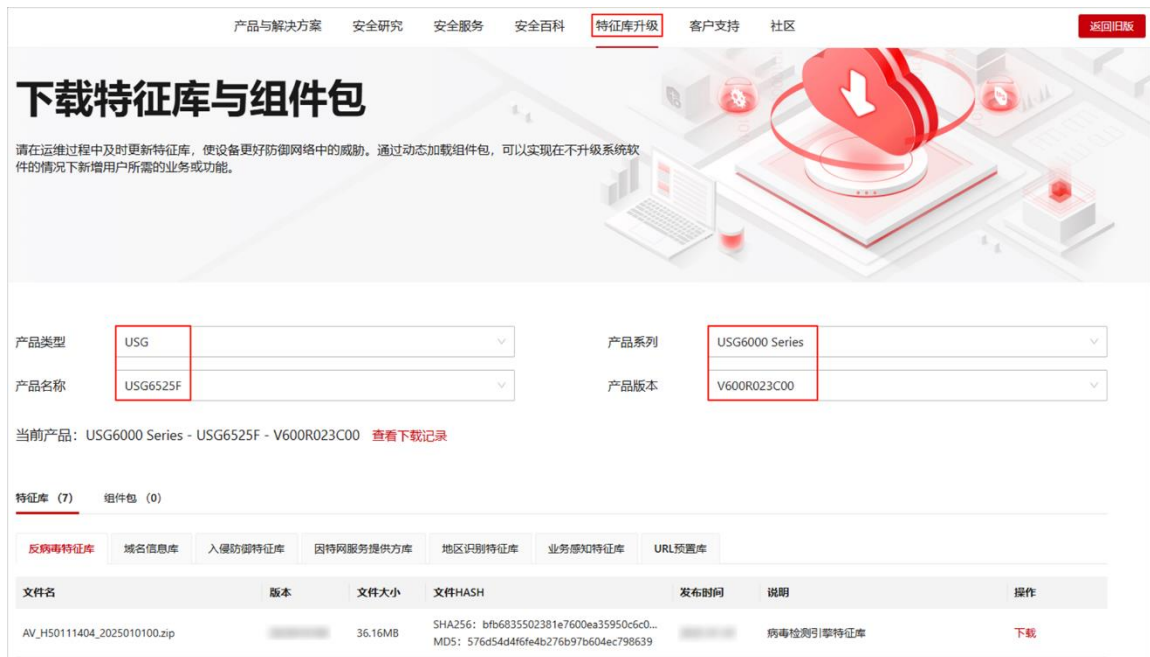


图14-35 查询设备所需特征库和组件包

特征库升级前，查看 DC-FW 的内存空间是否充足，选择“面板 > 设备信息”，查看设备的资源使用情况，如下图。

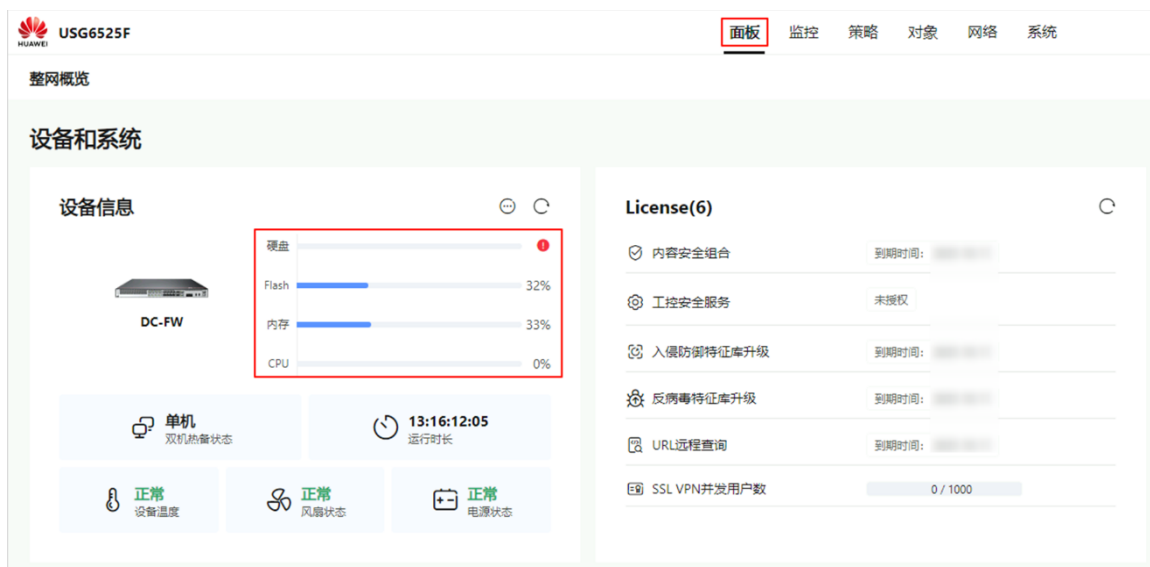


图14-36 查看 DC-FW 设备资源使用情况

特征库升级成功后，排查安全配置文件的配置参数，确认配置参数正确后，DC-FW 的右上角会出现如下提示，提交后配置才能生效，如下图。



图14-37 设备配置文件提交提示

安全配置文件提交后，确认其在安全策略中调用，以 URL 过滤为例，选择“对象 > 安全配置文件 > URL 过滤”，在 URL 过滤配置文件列表中查看引用次数。单击引用次数中的“查看”，可以看到引用该配置文件的安全策略名称，如下图。



图14-38 进入 URL 过滤配置文件的引用详情界面



图14-39 DC-FW 设备 URL 过滤配置文件的引用详情

14.3 思考题

请简单列举故障排查的顺序？

答案：参考 TCP/IP 模型，可以从低层到高层排查，也可以从高层到低层排查，即可以从物理层到应用层的排查，也可以是从应用层到物理层的排查。或者基于某一安全功能的配置步骤进行逐步排查。