

华为认证系列教程

HCIP-Security

实验指导手册

版本：V4.0



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，信息技术）全技术领域的认证体系，包含ICT技术架构与应用认证、云服务与平台认证两类认证。

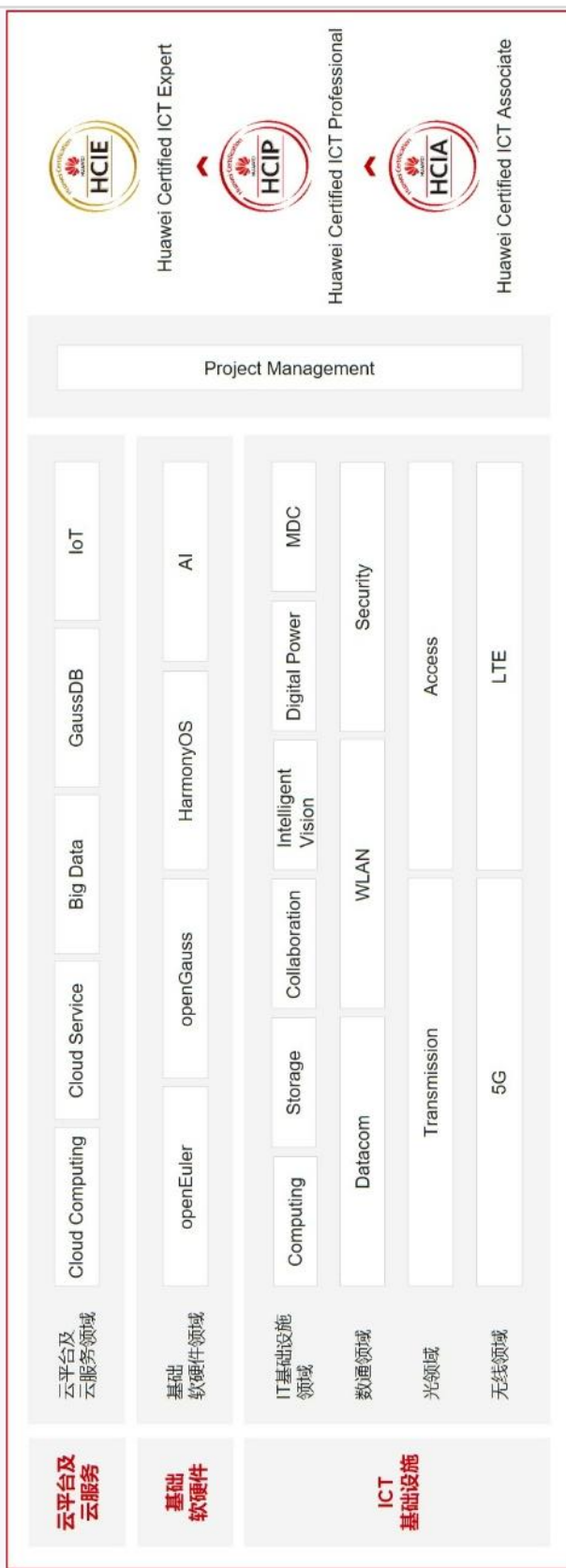
根据ICT从业者的学习和进阶需求，华为认证分为工程师级别、高级工程师级别和专家级别三个认证等级。

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。

HCIP-Security(Huawei Certified ICT Professional-Security，华为认证网络高级工程师安全方向)，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。HCIP-Security认证涵盖华为网络安全、内容安全、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。



前言

简介

本手册主要面向准备参加 HCIP-Security 考试的学员，同时也适合希望深入了解 Security 基础知识及相关技术的读者。内容涵盖虚拟系统、流量管理、用户认证、VPN 技术与故障排除、内容安全、攻击防护、园区组网设计与搭建和园区网络安全技术的配置与部署。

内容描述

本实验指导书共包含 14 个实验，从网络安全设备双机热备技术开始，逐一介绍了防火墙虚拟系统、流量管理、智能选路、IPSec VPN、SSL VPN、DDoS 攻击防御、内容安全、漏洞与威胁防范、802.1x 无线认证以及 Portal 无线认证的配置实践。同时模拟双机热备、IPSec VPN、SSL VPN 以及 Portal 无线认证故障，进行排错实践。

本实验指导书共包含如下实验：

- 实验一为双机热备实验，帮助读者掌握主备模式双机热备系统配置以及双机热备系统与链路高可靠性技术的安全联动部署，保障企业出口架构可靠性和业务连续性。
 - 实验二为双机热备故障排除实验，模拟双机热备开局及维护过程中可能遇到的问题，进行有效的排错，帮助读者了解并掌握双机热备故障的排查思路。
 - 实验三为虚拟系统实验，帮助读者了解虚拟系统的应用场景和基础配置，掌握虚拟系统间互访的配置方法。
 - 实验四为流量管理实验，重点讲解基于 IP 地址的带宽管理，使读者掌握防火墙上基于 IP 地址进行带宽管理配置方法。
 - 实验五为智能选路实验，通过在防火墙上部署出站智能选路，使出口防火墙可以根据链路负载情况选择最佳出口进行流量转发，保障业务交互质量。
 - 实验六为 IPSec 点到多点应用实验，通过在防火墙上配置点到多点 IPSec VPN，帮助读者了解 IPSec VPN 点到多点的配置方式，保障站点间通信的安全性。
 - 实验七为 IPSec VPN 故障排除实验，模拟 IPSec VPN 点到多点场景在开局及维护过程中可能遇到的问题，进行有效的排错，帮助读者了解并掌握 IPSec VPN 故障的排查思路。
 - 实验八为 SSL VPN 部署实验，通过在防火墙上部署 SSL VPN 虚拟网关，并开启网络扩展功能，满足企业员工远程接入企业内网的需求，使学员掌握 SSL VPN 的部署流程。
 - 实验九为 DDoS 攻击防御实验，通过在企业出口部署 Anti-DDoS 设备，对 Internet 访问企业内网的流量进行检查，并对威胁进行实时阻断。通过本章实验，使读者掌握 Anti-DDoS 设备的使用逻辑和配置方法。
 - 实验十为内容安全过滤实验，在出口防火墙部署 URL 过滤功能禁止企业员工访问游戏门户网站。部署文件过滤功能阻断下载可执行文件以降低内网感染病毒的风险。部署内容过
-

滤功能，对包含机密信息的文件或应用进行过滤，降低公司机密泄露的风险。通过上述操作帮助读者理解并掌握防火墙内容安全配置方法。

- 实验十一为入侵防御实验，在 IPS（入侵防御系统）上配置入侵防御功能，防范 Internet 用户对企业内网的 Web 服务器发起的 SQL 注入攻击。帮助读者理解并掌握 IPS（入侵防御系统）的使用方法。
- 实验十二为 802.1x 认证实验，在企业中部署 WLAN 为员工提供无线办公环境，使用 802.1x 认证技术对接入用户进行身份认证，帮助学员掌握 802.1x 认证相关配置。
- 实验十三为 Portal 认证实验，在企业中部署 WLAN 为员工提供无线办公环境，使用 Portal 认证技术对接入用户进行身份认证，帮助学员掌握 Portal 认证相关配置。
- 实验十四为 Portal 认证故障排除实验，模拟 Portal 无线认证在开局及维护过程中可能遇到的问题，进行有效的排错，帮助读者了解并掌握 Portal 无线认证故障的排查思路。

说明：不同实验章节之间业务参数规划彼此独立，建议学员在操作时，首先清除实验相关设备的残余配置并导入设备初始预配，之后再开始每个章节的实验操作，避免因设备残留配置导致实验结果出错。

读者知识背景

本课程为华为认证资深工程师级课程，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：

- 具有基本的计算机操作能力
 - 熟悉 TCP/IP 协议栈工作原理
 - 熟悉防火墙、以太网交换机、路由器、WLAN 基本工作原理
 - 具备 HCIA-Security 课程所描述的知识技能
-

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 HCIP-Security 考试的网络安全工程师。每套实验环境包括防火墙 3 台，企业出口路由器 2 台，互连交换机 4 台，无线控制器（AC）1 台，无线接入点（AP）1 台，Anti-DDoS 设备 2 台，Anti-DDoS 管理中心（SecoManager）1 套，入侵防御&检测系统（IPS）1 台，各类功能服务器 4 台，及若干 PC 和笔记本电脑。

设备介绍

为了满足 HCIP-Security 实验需要，建议每套实验环境采用以下配置：

设备名称、型号与版本的对应关系如下：

设备名称	设备型号	软件版本
防火墙	USG6525F	V600R024C00SPC100
企业出口路由器	AR6121E	V300R019C13SPC200
互连交换机	S5735-S24T4X-X	V200R021C01SPC200
无线控制器	AirEngine 9700-M1	V200R023C00SPC100
无线接入点	AirEngine5760-51	V200R021C00SPC100
Anti-DDoS	AntiDDoS1905	V600R022C00SPC100
Anti-DDoS管理中心	SecoManager	V500R023C00SPC100

入侵防御&检测系统	IPS6615F	V600R023C00SPC100
认证服务器	iMaster NCE-Campus	V300R023C00SPC110

注：本书所有设备的端口信息、显示信息以及配置信息等全部按照推荐拓扑中的设备给出，不同的实验环境可能有所不同。互连交换机使用支持三层功能的交换机即可，型号并不做强制要求。

使用说明

学员需具备基本的数通技术能力和 HCIA-Security 技术能力，为减轻学员在数通和基础配置上的配置压力，在 HCIP-Security 实验指导手册中的实验更多聚焦在关键设备及关键技术的配置部署上，实验拓扑中互连设备的基础配置会在每个实验章节最后以“预配置”的形式展现。

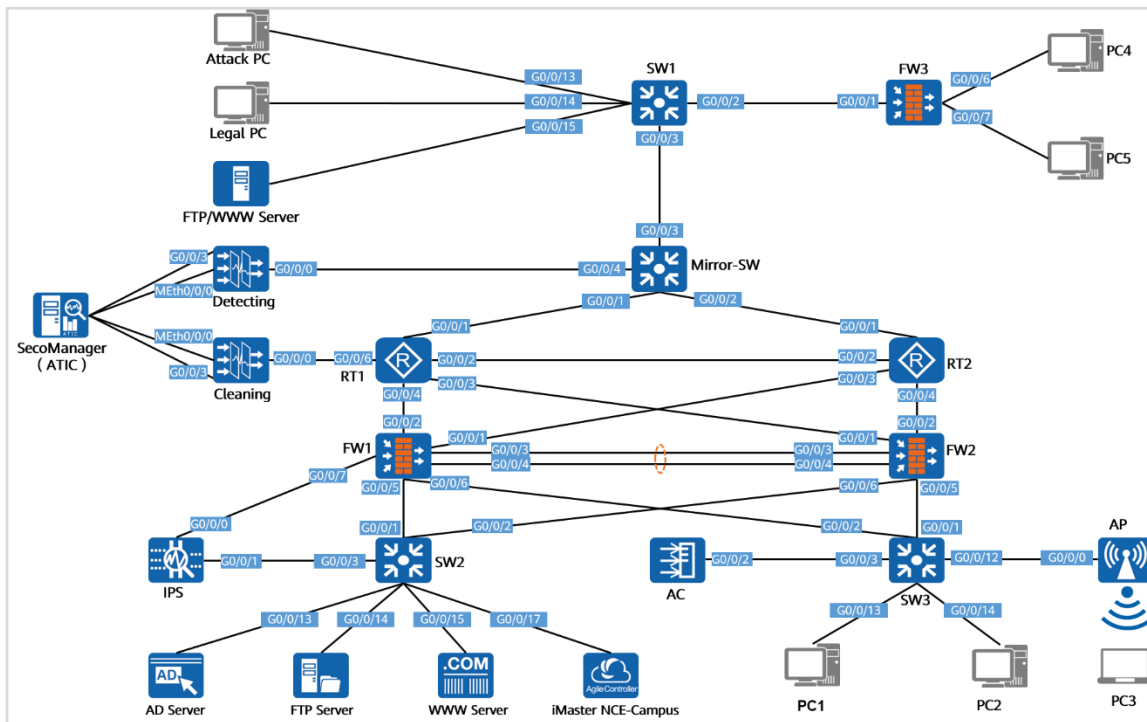
准备实验环境

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
USG6525F防火墙	每组3台	
AR6121E路由器	每组2台	
华为S5735交换机	每组4台	
AirEngine 9700-M1无线控制器	每组1台	
AirEngine5760-51无线接入点	每组1个	
Anti-DDoS1905	每组2台	
SecoManager	每组1台	
IPS6615F	每组1台	
iMaster NCE-Campus	每组1台	
虚拟主机	7台	其中PC3终端要有无线网卡
虚拟服务器	5台	
双绞线	若干	

实验拓扑



组网拓扑搭建说明：

本实验拓扑模拟了一个中型企业网络。RT1 与 RT2 作为企业出口设备连接 Internet，FW1 与 FW2 部署为主备模式双机热备系统，保障企业网络架构可靠性与稳定性。

在企业内网部署了终端用户和服务器资源，并由 Anti-DDoS 设备和 IPS 设备监控和防御网络入侵。同时企业内部部署了 WLAN 为无线终端提供网络服务。

FW3 设备连接的网络站点模拟企业分支机构，分支机构中存在两个不同部门，需要在 FW3 设备上部署虚拟防火墙技术，对分支机构两个不同的部门进行独立的安全管控。

SW1、Legal PC、Attack PC 与 FTP/WWW Server 模拟 Internet 网络资源。

注意点：SecoManager (ATIC) 与 Detecting、Cleaning 设备之间实际由 Mirror-SW 设备连接，为了美化拓扑，方便读者观看，特以此种形式展现。

目录

前 言	3
简介	3
内容描述	3
读者知识背景	4
本书常用图标	5
实验环境说明	5
准备实验环境	6
1 防火墙双机热备实验	16
1.1 实验介绍	16
1.1.1 关于本实验	16
1.1.2 实验目的	16
1.1.3 实验组网介绍	16
1.1.4 实验规划	17
1.2 实验任务配置	18
1.2.1 配置思路	18
1.2.2 配置步骤 - CLI	19
1.2.3 配置步骤 - Web	27
1.3 结果验证	45
1.3.1 连通性测试	45
1.3.2 路径探测	46
1.3.3 故障模拟	46
1.4 配置参考	47
1.4.1 RT1 配置	47
1.4.2 RT2 配置	48
1.4.3 FW1 配置	49
1.4.4 FW2 配置	51
1.4.5 SW1 预配置	52
1.4.6 SW2 预配置	53
1.4.7 SW3 预配置	53
1.4.8 Mirror-SW 预配置	54
1.5 思考题	54

2 防火墙双机热备故障排除实验	55
2.1 实验介绍	55
2.1.1 关于本实验	55
2.1.2 实验目的	55
2.1.3 实验组网介绍	55
2.1.4 实验规划	56
2.2 实验任务配置	57
2.2.1 配置思路	57
2.2.2 配置步骤	57
2.3 配置参考	73
2.3.1 RT1 配置	73
2.3.2 RT2 配置	74
2.3.3 FW1 配置	74
2.3.4 FW2 配置	76
2.3.5 SW1 预配置	78
2.3.6 SW2 预配置	78
2.3.7 SW3 预配置	78
2.3.8 Mirror-SW 预配置	79
2.4 思考题	79
3 防火墙虚拟系统实验	81
3.1 实验介绍	81
3.1.1 关于本实验	81
3.1.2 实验目的	81
3.1.3 实验组网介绍	81
3.1.4 实验规划	82
3.2 实验任务配置	82
3.2.1 配置思路	82
3.2.2 配置步骤 - CLI	83
3.2.3 配置步骤 - Web	87
3.3 结果验证	108
3.3.1 研发部业务测试	108
3.3.2 市场部业务测试	111
3.4 配置参考	114
3.4.1 FW3 配置	114
3.4.2 SW1 预配置	117

3.5 思考题	118
4 防火墙流量管理实验.....	119
4.1 实验介绍	119
4.1.1 关于本实验	119
4.1.2 实验目的.....	119
4.1.3 实验组网介绍.....	120
4.1.4 实验规划.....	120
4.2 实验任务配置	121
4.2.1 配置思路.....	121
4.2.2 配置步骤 - CLI	121
4.2.3 配置步骤 - Web	123
4.3 结果验证	131
4.3.1 认证前业务测试	131
4.3.2 Portal 认证测试	132
4.3.3 认证后业务测试	137
4.3.4 带宽管理测试.....	137
4.4 配置参考	138
4.4.1 FW1 配置.....	138
4.4.2 RT1 预配置	140
4.4.3 Mirror-SW 预配置.....	141
4.4.4 SW1 预配置.....	141
4.5 思考题	142
5 防火墙智能选路实验.....	143
5.1 实验介绍	143
5.1.1 关于本实验	143
5.1.2 实验目的.....	143
5.1.3 实验组网介绍.....	143
5.1.4 实验规划.....	144
5.2 实验任务配置	145
5.2.1 配置思路.....	145
5.2.2 配置步骤 - CLI	145
5.2.3 配置步骤 - Web	147
5.3 结果验证	153
5.4 配置参考	155
5.4.1 FW1 配置.....	155

5.4.2 RT1 预配置	155
5.4.3 RT2 预配置	156
5.4.4 SW1 预配置	156
5.4.5 Mirror-SW 预配置	157
5.4.6 SW3 预配置	157
5.5 思考题	158
6 IPsec 点到多点应用实验	159
6.1 实验介绍	159
6.1.1 关于本实验	159
6.1.2 实验目的	159
6.1.3 实验组网介绍	159
6.1.4 实验规划	160
6.2 实验任务配置	161
6.2.1 配置思路	161
6.2.2 配置步骤 - CLI	161
6.2.3 配置步骤 - Web	169
6.3 结果验证	193
6.3.1 业务连通性测试	193
6.3.2 隧道信息查看	196
6.4 配置参考	197
6.4.1 FW1 配置	197
6.4.2 FW2 配置	199
6.4.3 FW3 配置	201
6.4.4 RT1 预配置	203
6.4.5 RT2 预配置	203
6.4.6 SW1 预配置	204
6.4.7 Mirror-SW 预配置	205
6.4.8 SW2 预配置	205
6.4.9 SW3 预配置	205
6.5 思考题	206
7 IPsec VPN 故障排除实验	207
7.1 实验介绍	207
7.1.1 关于本实验	207
7.1.2 实验目的	207
7.1.3 实验组网介绍	207

7.1.4 实验规划.....	208
7.2 实验任务配置	209
7.2.1 配置思路.....	209
7.2.2 配置步骤.....	209
7.3 配置参考	230
7.3.1 FW1 配置	230
7.3.2 FW2 配置	232
7.3.3 FW3 配置	234
7.3.4 RT1 预配置	236
7.3.5 RT2 预配置	237
7.3.6 SW1 预配置.....	237
7.3.7 Mirror-SW 预配置.....	238
7.3.8 SW2 预配置.....	238
7.3.9 SW3 预配置.....	239
7.4 思考题	239
8 SSL VPN 部署实验	240
8.1 实验介绍	240
8.1.1 关于本实验	240
8.1.2 实验目的.....	240
8.1.3 实验组网介绍.....	241
8.1.4 实验规划.....	241
8.2 实验任务	242
8.2.1 配置思路.....	242
8.2.2 配置步骤 - CLI	243
8.2.3 配置步骤 - Web.....	245
8.3 结果验证	252
8.4 配置参考	257
8.4.1 FW2 配置	257
8.4.2 SW1 预配置.....	258
8.4.3 Mirror-SW 预配置.....	259
8.4.4 RT2 预配置	259
8.4.5 SW3 预配置.....	260
8.5 思考题	260
9 DDoS 攻击防御实验	261
9.1 实验介绍	261

9.1.1 关于本实验	261
9.1.2 实验目的.....	261
9.1.3 实验组网介绍.....	262
9.1.4 实验规划.....	263
9.2 实验任务配置	264
9.2.1 配置思路.....	264
9.2.2 配置步骤.....	265
9.3 结果验证	284
9.4 配置参考	286
9.4.1 FW1 配置	286
9.4.2 RT1 配置	287
9.4.3 Mirror-SW 配置	288
9.4.4 Detecting 配置	289
9.4.5 Cleaning 配置.....	294
9.4.6 SW1 预配置.....	299
9.4.7 SW2 预配置.....	299
9.5 思考题	300
10 内容安全过滤实验.....	301
10.1 实验介绍.....	301
10.1.1 关于本实验.....	301
10.1.2 实验目的	301
10.1.3 实验组网介绍	302
10.1.4 实验规划	302
10.2 实验任务配置.....	303
10.2.1 配置思路	303
10.2.2 配置步骤 - CLI.....	303
10.2.3 配置步骤 - Web.....	306
10.3 结果验证.....	323
10.4 配置参考.....	326
10.4.1 FW1 配置.....	326
10.4.2 SW1 预配置	328
10.4.3 Mirror-SW 预配置	328
10.4.4 RT1 预配置.....	328
10.4.5 SW3 预配置	329
10.5 思考题	329

11 入侵防御实验	330
11.1 实验介绍	330
11.1.1 关于本实验	330
11.1.2 实验目的	330
11.1.3 实验组网介绍	331
11.1.4 实验规划	332
11.2 实验任务配置	332
11.2.1 配置思路	332
11.2.2 配置步骤	333
11.3 结果验证	348
11.4 配置参考	350
11.4.1 IPS 配置	350
11.4.2 RT1 预配置	351
11.4.3 FW1 预配置	351
11.4.4 SW1 预配置	352
11.4.5 SW2 预配置	352
11.4.6 Mirror-SW 预配置	353
11.5 思考题	353
12 802.1X 认证实验	354
12.1 实验介绍	354
12.1.1 关于本实验	354
12.1.2 实验目的	354
12.1.3 实验组网介绍	354
12.1.4 实验规划	355
12.2 实验任务配置	355
12.2.1 配置思路	355
12.2.2 配置步骤	356
12.3 结果验证	371
12.4 配置参考	381
12.4.1 SW2 配置	381
12.4.2 SW3 配置	382
12.4.3 FW2 配置	382
12.4.4 AC 配置	383
12.5 思考题	385
13 Portal 认证实验	386

13.1 实验介绍.....	386
13.1.1 关于本实验.....	386
13.1.2 实验目的.....	386
13.1.3 实验组网介绍.....	386
13.1.4 实验规划.....	387
13.2 实验任务配置.....	388
13.2.1 配置思路.....	388
13.2.2 配置步骤.....	388
13.3 结果验证.....	403
13.4 配置参考.....	409
13.4.1 SW2 配置.....	409
13.4.2 SW3 配置.....	409
13.4.3 FW2 配置.....	409
13.4.4 AC 配置.....	410
13.5 思考题.....	413
14 Portal 认证故障排除实验.....	414
14.1 实验介绍.....	414
14.1.1 关于本实验.....	414
14.1.2 实验目的.....	414
14.1.3 实验组网介绍.....	414
14.1.4 实验规划.....	415
14.2 实验任务配置.....	416
14.2.1 配置思路.....	416
14.2.2 配置步骤.....	416
14.3 配置参考.....	427
14.3.1 SW2 配置.....	427
14.3.2 SW3 配置.....	428
14.3.3 FW2 配置.....	428
14.3.4 AC 配置.....	429
14.4 思考题.....	431

1

防火墙双机热备实验

1.1 实验介绍

1.1.1 关于本实验

某企业内部网络需要访问互联网，为避免网络设备及外部不可控因素导致通信线路中断，影响业务正常交互，计划在网络出口区部署防火墙双机热备系统，增加网络可靠性。

本实验将 FW1 和 FW2 两台防火墙部署为主备模式双机热备系统，作为企业出口区安全网关，两台路由器作为企业出口设备，保证了在网络通信线路单边故障的情况下，企业内网仍可与外部网络之间正常通信，业务连续性不受影响。

1.1.2 实验目的

- 掌握防火墙上行连接路由器，下行连接交换机组网的主备模式双机热备系统的部署。
- 掌握 Eth-trunk、BFD 等链路高可靠性技术和双机热备系统的安全联动。

1.1.3 实验组网介绍

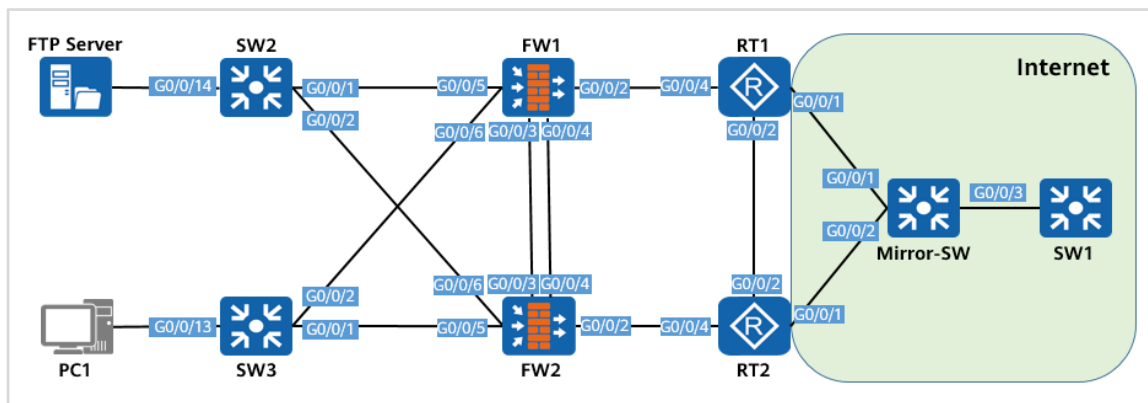


图1-1 双机热备实验拓扑

FW1 与 FW2 组建主备模式双机热备系统，PC1 和 FTP Server 的网关分别为防火墙上 VRRP1 与 VRRP2 备份组虚拟 IP。RT1、RT2 与 FW1、FW2 之间运行 OSPF 实现网络互通。RT1 与 RT2 模拟企业网络的出口设备，SW1 与 Mirror-SW 模拟 Internet，SW2 和 SW3 作为接入交换机连接内网终端，最终实现内部网络的 PC1 与 FTP Server 可以与 Internet 互通。SW1、SW2、SW3 与 Mirror-SW 设备的详细配置请参考“1.4 配置参考”，实验操作步骤中不再赘述。

1.1.4 实验规划

表1-1 设备接口规划表

设备	接口	接口性质	接口信息	说明
RT1	G0/0/1.2	三层子接口	4.4.4.2/30 终结VLAN2	网络出接口，与Mirror-SW互连
	G0/0/2	三层接口	10.1.1.1/30	与RT2互连
	G0/0/4	三层接口	10.3.1.1/30	与FW1互连
	LoopBack0	三层接口	33.33.33.1/32	OSPF Router-ID
RT2	G0/0/1.40	三层子接口	3.3.3.2/30 终结VLAN 40	网络出接口，与Mirror-SW互连
	G0/0/2	三层接口	10.1.1.2/30	与RT1互连
	G0/0/4	三层接口	10.6.1.1/30	与FW2互连
	LoopBack0	三层接口	44.44.44.1/32	OSPF Router-ID
FW1	G0/0/2	三层接口	10.3.1.2/30 安全域：untrust	上行连接RT1
	G0/0/3	Eth-trunk 0 聚合接口	10.10.10.1/24 安全域：dmz	双机热备心跳接口
	G0/0/4			
	G0/0/5	三层接口	172.16.30.2/24 安全域：trust	下行连接接入SW接口，需要配置VRRP虚拟网关
	G0/0/6	三层接口	172.16.20.2/24 安全域：trust	
	LoopBack0	三层接口	11.11.11.1/32	OSPF Router-ID
FW2	G0/0/2	三层接口	10.6.1.2/30 安全域：untrust	上行连接RT2
	G0/0/3	Eth-trunk 0 聚合接口	10.10.10.2/24 安全域：dmz	双机热备心跳接口
	G0/0/4			
	G0/0/5	三层接口	172.16.20.3/24 安全域：trust	下行连接接入SW接口，需要配置VRRP虚拟网关
	G0/0/6	三层接口	172.16.30.3/24	

			安全域: trust	
	LoopBack0	三层接口	22.22.22.1/32	OSPF Router-ID
SW1	G0/0/3	Trunk	PVID: 1 Allow-pass VLAN: 2, 40	与Mirror-SW互连
	VLANIF2	三层	4.4.4.1/30	与RT1出口地址为直连地址
	VLANIF40	三层	3.3.3.1/30	与RT2出口地址为直连地址
SW2	G0/0/1	Access	PVID: 30	上下行接口只需允许业务VLAN通过
	G0/0/2			
	G0/0/14			
SW3	G0/0/1	Access	PVID: 40	上下行接口只需允许业务VLAN通过
	G0/0/2			
	G0/0/13			
Mirror-SW	G0/0/1	Trunk	PVID: 1 Allow-pass VLAN: 2, 40	上下行接口只需允许业务VLAN通过
	G0/0/2			
	G0/0/3			
PC1	Ethernet0	网卡	172.16.20.100/24 网关: 172.16.20.1/24	终端
FTP Server	Ethernet0	网卡	172.16.30.101/24 网关: 172.16.30.1/24	终端

1.2 实验任务配置

1.2.1 配置思路

1.配置 FW1、FW2、RT1 和 RT2 设备的 IP 地址，包括防火墙接口所属的安全区域。

2.配置 FW1、FW2、RT1 和 RT2 之间的 OSPF。RT1 与 RT2 模拟企业网络的出口，SW1 模拟 Internet。在 RT1 和 RT2 上配置默认路由和 NAT，同时该条静态路由需要引入 OSPF 中，最终实现内部网络的 PC1 与 PC2 可以访问 Internet。

3.完成 FW1 与 FW2 的双机热备配置，心跳接口使用 Eth-trunk 接口，两台防火墙下行连接交换机使用 VRRP 对接。

4.按照规划配置防火墙安全策略，放行业务流量。

5.使用 BFD 技术探测防火墙非直连链路，并联动防火墙双机热备系统，在主线路出现故障时，及时进行主备切换，保障业务连续。

1.2.2 配置步骤 - CLI

步骤 1 网络基本参数配置

按照网络参数规划表配置设备接口 IP 及防火墙业务接口安全区域。其中 SW1、SW2、SW3 和 Mirror-SW 已经预配，具体可参考“1.4 配置参考”。

防火墙接口 IP 配置完成后，需要将接口划分到表格中对应的安全区域。

FW1 的配置如下：

```
[FW1] interface Eth-Trunk0
[FW1-Eth-Trunk0] ip address 10.10.10.1 255.255.255.0
[FW1-Eth-Trunk0] quit
[FW1] interface G0/0/3
[FW1-G0/0/3] eth-trunk 0
[FW1-G0/0/3] quit
[FW1] interface G0/0/4
[FW1-G0/0/4] eth-trunk 0
[FW1-G0/0/4] quit
[FW1] interface G0/0/2
[FW1-G0/0/2] ip address 10.3.1.2 255.255.255.252
[FW1-G0/0/2] quit
[FW1] interface G0/0/5
[FW1-G0/0/5] ip address 172.16.30.2 255.255.255.0
[FW1-G0/0/5] vrrp vrid 2 virtual-ip 172.16.30.1 active
[FW1-G0/0/5] quit
[FW1] interface G0/0/6
[FW1-G0/0/6] ip address 172.16.20.2 255.255.255.0
[FW1-G0/0/6] vrrp vrid 1 virtual-ip 172.16.20.1 active
[FW1-G0/0/6] quit
[FW1] interface LoopBack0
[FW1-LoopBack0] ip address 11.11.11.1 255.255.255.255
[FW1-LoopBack0] quit
[FW1] firewall zone trust
[FW1-zone-trust] add interface G0/0/5
[FW1-zone-trust] add interface G0/0/6
[FW1-zone-trust] quit
[FW1] firewall zone untrust
```

```
[FW1-zone-untrust] add interface G0/0/1
[FW1-zone-untrust] add interface G0/0/2
[FW1-zone-untrust] quit
[FW1] firewall zone dmz
[FW1-zone-dmz] add interface Eth-Trunk0
[FW1-zone-dmz] quit
[FW1]
```

FW2 的配置如下:

```
[FW2] interface Eth-Trunk0
[FW2-Eth-Trunk0] ip address 10.10.10.2 255.255.255.0
[FW2-Eth-Trunk0] quit
[FW2] interface G0/0/3
[FW2-GE0/0/3] eth-trunk 0
[FW2-GE0/0/3] quit
[FW2] interface G0/0/4
[FW2-GE0/0/4] eth-trunk 0
[FW2-GE0/0/4] quit
[FW2] interface G0/0/2
[FW2-GE0/0/2] ip address 10.6.1.2 255.255.255.252
[FW2-GE0/0/2] quit
[FW2] interface G0/0/5
[FW2-GE0/0/5] ip address 172.16.20.3 255.255.255.0
[FW2-GE0/0/5] vrrp vrid 1 virtual-ip 172.16.20.1 standby
[FW2-GE0/0/5] quit
[FW2] interface G0/0/6
[FW2-GE0/0/6] ip address 172.16.30.3 255.255.255.0
[FW2-GE0/0/6] vrrp vrid 2 virtual-ip 172.16.30.1 standby
[FW2-GE0/0/6] quit
[FW2] interface LoopBack0
[FW2-LoopBack0] ip address 22.22.22.1 255.255.255.255
[FW2-LoopBack0] quit
[FW2] firewall zone trust
[FW2-zone-trust] add interface G0/0/5
[FW2-zone-trust] add interface G0/0/6
[FW2-zone-trust] quit
[FW2] firewall zone untrust
[FW2-zone-untrust] add interface G0/0/1
[FW2-zone-untrust] add interface G0/0/2
[FW2-zone-untrust] quit
[FW2] firewall zone dmz
[FW2-zone-dmz] add interface Eth-Trunk0
[FW2-zone-dmz] quit
[FW2]
```

RT1 设备的接口 IP 配置如下:

```
[RT1] interface GigabitEthernet0/0/1
[RT1-GigabitEthernet0/0/1] undo portswitch
```

```
[RT1-GigabitEthernet0/0/1] quit
[RT1] interface GigabitEthernet0/0/1.2
[RT1-GigabitEthernet0/0/1.2] dot1q termination vid 2
[RT1-GigabitEthernet0/0/1.2] ip address 4.4.4.2 255.255.255.252
[RT1-GigabitEthernet0/0/1.2] quit
[RT1] interface GigabitEthernet0/0/2
[RT1-GigabitEthernet0/0/2] undo portswitch
[RT1-GigabitEthernet0/0/2] ip address 10.1.1.1 255.255.255.252
[RT1-GigabitEthernet0/0/2] quit
[RT1] interface GigabitEthernet0/0/4
[RT1-GigabitEthernet0/0/4] undo portswitch
[RT1-GigabitEthernet0/0/4] ip address 10.3.1.1 255.255.255.252
[RT1-GigabitEthernet0/0/4] quit
[RT1] interface LoopBack0
[RT1-LoopBack0] ip address 33.33.33.1 255.255.255.255
[RT1-LoopBack0] quit
[RT1]
```

RT2 设备的接口 IP 配置如下:

```
[RT2] interface GigabitEthernet0/0/1
[RT2-GigabitEthernet0/0/1] undo portswitch
[RT2-GigabitEthernet0/0/1] quit
[RT2] interface GigabitEthernet0/0/1.40
[RT2-GigabitEthernet0/0/1.40] dot1q termination vid 40
[RT2-GigabitEthernet0/0/1.40] ip address 3.3.3.2 255.255.255.252
[RT2-GigabitEthernet0/0/1.40] quit
[RT2] interface GigabitEthernet0/0/2
[RT2-GigabitEthernet0/0/2] undo portswitch
[RT2-GigabitEthernet0/0/2] ip address 10.1.1.2 255.255.255.252
[RT2-GigabitEthernet0/0/2] quit
[RT2] interface GigabitEthernet0/0/4
[RT2-GigabitEthernet0/0/4] undo portswitch
[RT2-GigabitEthernet0/0/4] ip address 10.6.1.1 255.255.255.252
[RT2-GigabitEthernet0/0/4] quit
[RT2] interface LoopBack0
[RT2-LoopBack0] ip address 44.44.44.1 255.255.255.255
[RT2-LoopBack0] quit
[RT2]
```

步骤 2 配置 OSPF

按规划配置 FW1、FW2、RT1、RT2 的 OSPF，OSPF 进程号设为 1，在相应接口上激活 OSPF 协议。

在 FW1 和 FW2 上关闭防火墙对基础协议报文的过滤功能，确保 OSPF 报文可以正常交互。

```
[FW1] undo firewall packet-filter basic-protocol enable
```

```
[FW2] undo firewall packet-filter basic-protocol enable
```

在 FW1 上配置 OSPF，在各三层业务接口上激活 OSPF。

```
[FW1] ospf 1 router-id 11.11.11.1
[FW1-ospf-1] area 0.0.0.0
[FW1-ospf-1-area-0.0.0.0] quit
[FW1] interface G0/0/2
[FW1-GE0/0/2] ospf enable 1 area 0.0.0.0
[FW1-GE0/0/2] quit
[FW1] interface G0/0/5
[FW1-GE0/0/5] ospf enable 1 area 0.0.0.0
[FW1-GE0/0/5] quit
[FW1] interface G0/0/6
[FW1-GE0/0/6] ospf enable 1 area 0.0.0.0
[FW1-GE0/0/6] quit
[FW1]
```

在 FW2 上配置 OSPF，在各三层业务接口上激活 OSPF。

```
[FW2]ospf 1 router-id 22.22.22.1
[FW2-ospf-1] area 0.0.0.0
[FW2-ospf-1-area-0.0.0.0] quit
[FW2]interface G0/0/2
[FW2-GE0/0/2] ospf enable 1 area 0.0.0.0
[FW2-GE0/0/2] quit
[FW2]interface G0/0/5
[FW2-GE0/0/5] ospf enable 1 area 0.0.0.0
[FW2-GE0/0/5] quit
[FW2]interface G0/0/6
[FW2-GE0/0/6] ospf enable 1 area 0.0.0.0
[FW2-GE0/0/6] quit
[FW2]
```

在 RT1 配置 OSPF，在三层业务接口上激活 OSPF。

```
[RT1] ospf 1 router-id 33.33.33.1
[RT1-ospf-1] area 0
[RT1-ospf-1-area-0.0.0.0] quit
[RT1-ospf-1] quit
[RT1] interface GigabitEthernet0/0/2
[RT1-GigabitEthernet0/0/2] ospf enable 1 area 0
[RT1-GigabitEthernet0/0/2] quit
[RT1] interface GigabitEthernet0/0/4
[RT1-GigabitEthernet0/0/4] ospf enable 1 area 0
[RT1-GigabitEthernet0/0/4] quit
```

在 RT2 配置 OSPF，在三层业务接口上激活 OSPF。

```
[RT2] ospf 1 router-id 44.44.44.1
[RT2-ospf-1] area 0
[RT2-ospf-1-area-0.0.0.0] quit
```

```
[RT2-ospf-1] quit
[RT2] interface GigabitEthernet0/0/2
[RT2-GigabitEthernet0/0/2] ospf enable 1 area 0
[RT2-GigabitEthernet0/0/2] quit
[RT2] interface GigabitEthernet0/0/4
[RT2-GigabitEthernet0/0/4] ospf enable 1 area 0
[RT2-GigabitEthernet0/0/4] quit
```

在 FW1 和 FW2 设备上检查 OSPF 邻居关系，效果如下：

```
[FW1]display ospf peer brief
OSPF Process 1 with Router ID 11.11.11.1
                Peer Statistic Information
Total number of peer(s): 3
Peer(s) in full state: 3
-----
Area Id      Interface      Neighbor id    State
0.0.0.0      GE0/0/2        33.33.33.1     Full
0.0.0.0      GE0/0/5        22.22.22.1     Full
0.0.0.0      GE0/0/6        22.22.22.1     Full
-----
```

```
[FW2] display ospf peer brief
OSPF Process 1 with Router ID 22.22.22.1
                Peer Statistic Information
Total number of peer(s): 3
Peer(s) in full state: 3
-----
Area Id      Interface      Neighbor id    State
0.0.0.0      GE0/0/2        44.44.44.1     Full
0.0.0.0      GE0/0/5        11.11.11.1     Full
0.0.0.0      GE0/0/6        11.11.11.1     Full
-----
```

可以发现防火墙的 OSPF 邻居均已正常建立。

完成上述 OSPF 基础配置后，在 RT1 上添加缺省路由到 Internet（即拓扑图中的 SW1）。

```
[RT1] ip route-static 0.0.0.0 0.0.0.0 4.4.4.1
```

在 RT2 上添加缺省路由到 Internet（即拓扑图中的 SW1）。

```
[RT2] ip route-static 0.0.0.0 0.0.0.0 3.3.3.1
```

在 SW1 上配置回程路由。

```
[SW1] ip route-static 172.16.0.0 16 4.4.4.2
[SW1] ip route-static 172.16.0.0 16 3.3.3.2 preference 70
```

RT1 上配置 Easy IP，在内网用户访问 Internet 时替换源地址。

```
[RT1] acl number 3500
[RT1-acl-adv-3500] rule 5 permit ip
[RT1-acl-adv-3500] quit
```

```
[RT1] interface GigabitEthernet 0/0/1.2
[RT1-GigabitEthernet0/0/1.2] nat outbound 3500
[RT1-GigabitEthernet0/0/1.2] quit
```

RT2 上配置 Easy IP，在内网用户访问 Internet 时替换源地址。

```
[RT2] acl number 3500
[RT2-acl-adv-3500] rule 5 permit ip
[RT2-acl-adv-3500] quit
[RT2] interface GigabitEthernet0/0/1.40
[RT2-GigabitEthernet0/0/1.40] nat outbound 3500
[RT2-GigabitEthernet0/0/1.40] quit
```

在 RT1 的 OSPF 中引入外部缺省路由。

```
[RT1] ospf 1
[RT1-ospf-1] import-route static
[RT1-ospf-1] default-route-advertise always
[RT1-ospf-1] quit
```

RT2 配置同上。

步骤 3 配置双机热备功能

在两台 FW 上配置针对上行业务接口的监控。

```
[FW1] hrp track interface G0/0/2
```

FW2 设备配置同上。

为处理不对称业务流，建议在两台 FW 上都配置会话快速备份功能。

```
[FW1] hrp mirror session enable
```

FW2 设备配置同上。

在两台 FW 上指定心跳口、配置 HRP 认证密钥（Huawei@123）并启用双机热备功能。

```
[FW1] hrp interface Eth-Trunk0 remote 10.10.10.2
[FW1] hrp authentication-key Huawei@123
[FW1] hrp enable
```

```
[FW2] hrp interface Eth-Trunk0 remote 10.10.10.1
[FW2] hrp authentication-key Huawei@123
[FW2] hrp enable
HRP_S[FW2] hrp standby config enable
```

在两台 FW 上查看 HRP 双机热备状态。

```
HRP_M[FW1] display hrp state verbose
Local role: Active, Peer role: Standby
Local priority: 0:2, Peer priority: 0:2
Connection state: succeeded
Stable time: 0 day, 0 hour, 1 minute
Configuration:
Hello interval          1000ms
```



```

Preempt                on
Track trunk member      on
Auto-Sync connection status  on
Auto-Sync configuration  on
Mirror configuration     off
Mirror session          on
Adjust OSPF-Cost         on
Adjust OSPFv3-Cost       on
Adjust BGP-Cost          on

```

Module	Fault	Robust
Total	0	2
Manual	0	0
BFD	0	0
Healthcheck	0	0
Tracked interface	0	0
VRRP	0	0
CPU	0	2
Boot sync	0	0
Dynamic BFD	0	0
Device reboot	0	0

Detail-Information:

```

ospf-cost: 0
ospfv3-cost: 0
bgp-cost: 0
GE0/0/6 vrrp vrid 1: active
GE0/0/5 vrrp vrid 2: active
GE0/0/2: up

```

```

HRP_S[FW2]display hrp state verbose
Local role: Standby, Peer role: Active
Local priority: 0:2, Peer priority: 0:2
Connection state: succeeded
Stable time: 0 day, 0 hour, 2 minutes
Configuration:
Hello interval          1000ms
Preempt                 on
Track trunk member      on
Auto-Sync connection status  on
Auto-Sync configuration  on
Mirror configuration     off
Mirror session          on
Adjust OSPF-Cost         on
Adjust OSPFv3-Cost       on
Adjust BGP-Cost          on

```

Module	Fault	Robust
Total	0	2
Manual	0	0
BFD	0	0
Healthcheck	0	0
Tracked interface	0	0
VRRP	0	0
CPU	0	2
Boot sync	0	0
Dynamic BFD	0	0
Device reboot	0	0
Detail-Information:		
	ospf-cost: 65500	
	ospfv3-cost: 65500	
	bgp-cost: 100	
	GE0/0/5 vrrp vrid 1: standby	
	GE0/0/6 vrrp vrid 2: standby	
	GE0/0/2: up	

步骤 4 配置安全策略

说明：由于 FW1 与 FW2 建立了双机热备系统，FW1 的安全策略配置会自动同步到 FW2 上，故此处仅在 FW1 上配置安全策略。

配置安全策略，允许内网用户访问外网。

```
HRP_M[FW1] security-policy
HRP_M[FW1-policy-security] rule name t2u
HRP_M[FW1-policy-security-rule-t2u] source-zone trust
HRP_M[FW1-policy-security-rule-t2u] destination-zone untrust
HRP_M[FW1-policy-security-rule-t2u] action permit
HRP_M[FW1-policy-security-rule-t2u] quit
HRP_M[FW1-policy-security] quit
HRP_M[FW1]
```

步骤 5 配置双机热备与 BFD 联动

为避免 RT1 上行链路出现故障时，双机热备系统未及时进行主备切换，导致业务中断，需要在 FW1 和 RT1 设备之间部署 BFD 进行链路周期性探测，并将 BFD 会话与双机热备系统进行安全联动，在主用业务链路故障时可以及时触发主备切换，保证业务连续。

在 FW1 上全局使能 BFD 特性，并配置 BFD 会话 1，对端 IP 地址为 4.4.4.2，本端地址为 10.3.1.2，本地标识符为 20，远端标识符为 10。

```
HRP_M[FW1] bfd
HRP_M[FW1-bfd] quit
HRP_M[FW1] bfd 1 bind peer-ip 4.4.4.2 source-ip 10.3.1.2
HRP_M[FW1-bfd-session-1] discriminator local 20
HRP_M[FW1-bfd-session-1] discriminator remote 10
HRP_M[FW1-bfd-session-1] quit
```

```
HRP_M[FW1]
```

在 RT1 上全局使能 BFD 特性，并配置 BFD 会话 1，对端 IP 地址为 10.3.1.2，本端地址为 4.4.4.2，本地标识符为 10，远端标识符为 20。

```
[RT1] bfd
[RT1] bfd 1 bind peer-ip 10.3.1.2 source-ip 4.4.4.2
[RT1-bfd-session-1] discriminator local 10
[RT1-bfd-session-1] discriminator remote 20
[RT1-bfd-session-1] commit
[RT1-bfd-session-1] quit
```

在 FW1 上配置 BFD 与双机热备联动。

```
HRP_M[FW1] hrp track bfd-session 20
```

1.2.3 配置步骤 - Web

步骤 1 网络基本参数配置

按照“表 1-1”规划数据，完成网络基本参数配置。其中 SW1、SW2、SW3、Mirror-SW 已经预配，具体可参考“1.4 配置参考”。

说明：RT1 和 RT2 设备的相关配置参考“1.2.2 配置步骤-CLI”中相关配置步骤即可，本节重点介绍 FW 设备的 Web 配置过程。

登录 FW1 设备 Web 管理界面，选择“网络 > 接口”，进入接口列表界面，配置业务接口 IP 地址及安全区域（HRP 心跳接口除外），此处以 GE0/0/2 接口为例，展示业务接口基础配置步骤。

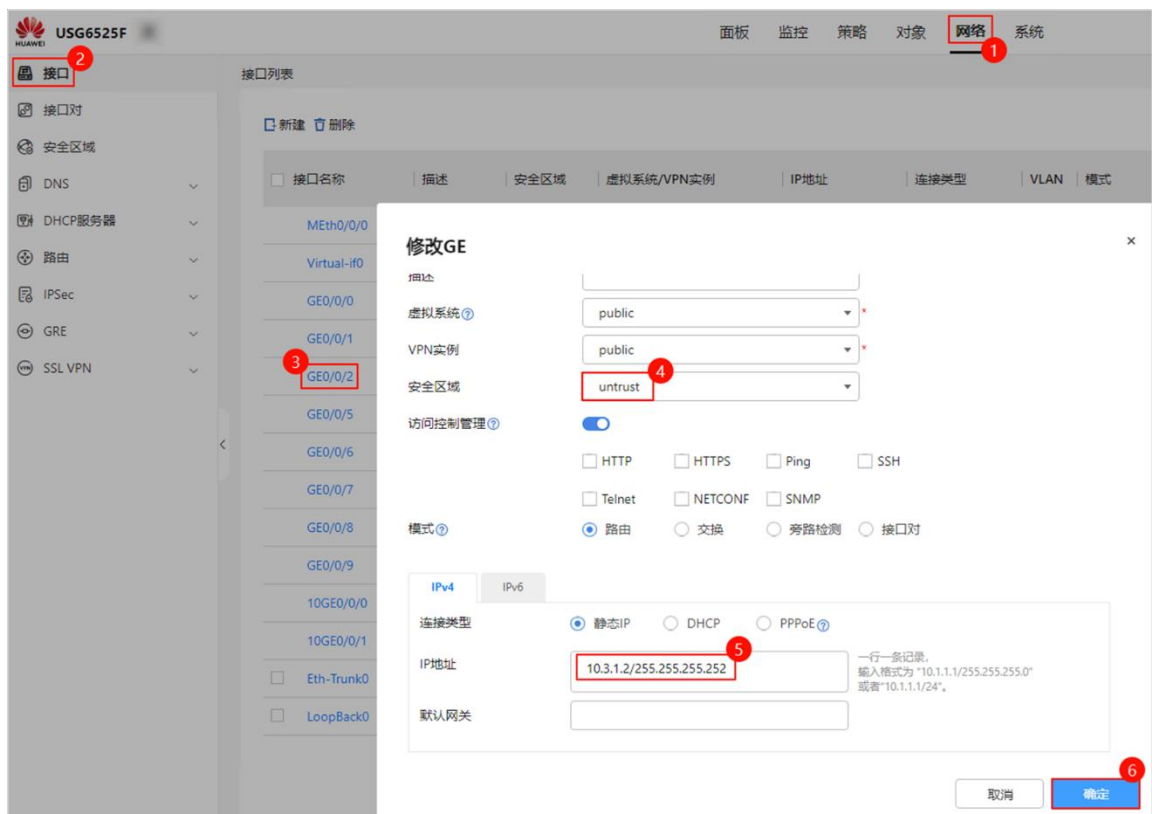


图1-2 FW1 设备 GE0/0/2 接口地址及安全区域配置

FW1 设备其余业务接口及 FW2 设备的业务接口配置均可参考上述步骤，结合“表 1-1”规划数据完成配置，此处不再赘述。

步骤 2 配置 OSPF

登录 FW1 设备 Web 管理界面，选择“网络 > 路由 > OSPF”，在“OSPF 列表”界面中点击“新建”执行以下操作。

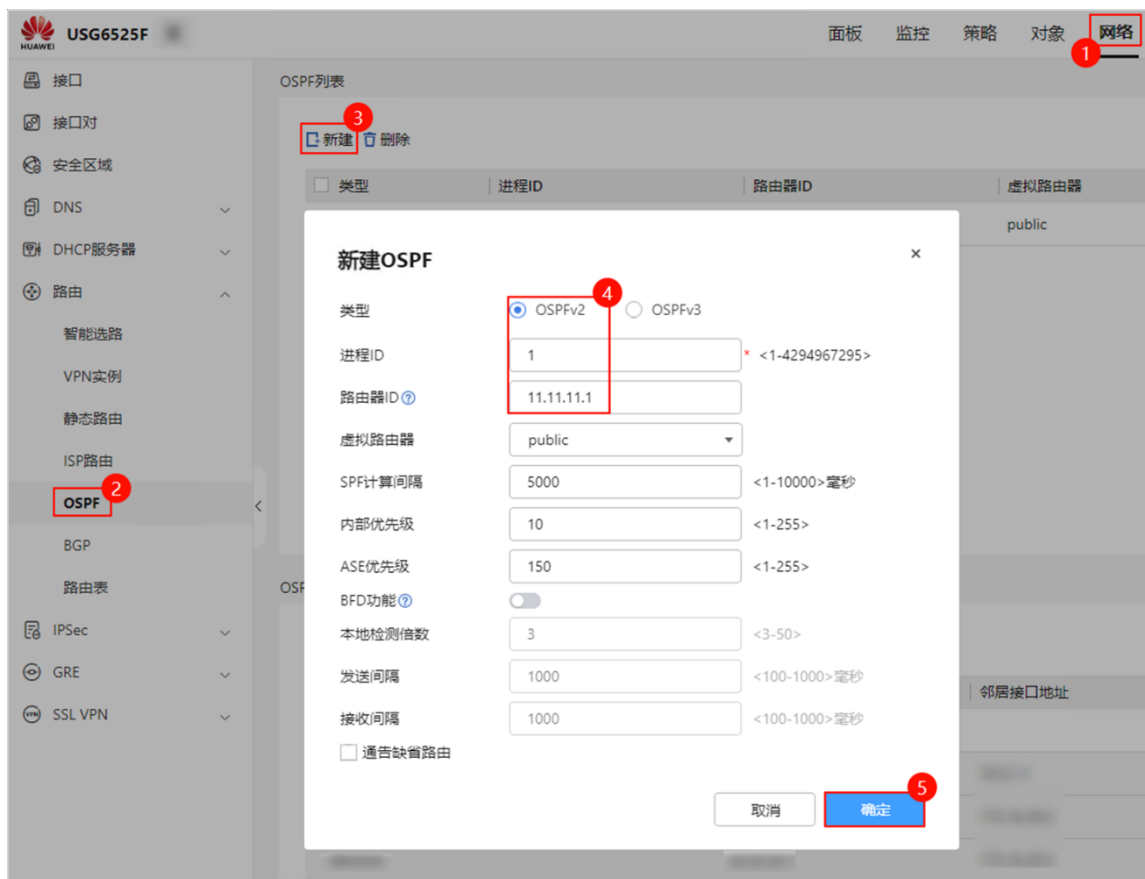


图1-3 FW1 设备上新建 OSPF 进程

在 OSPF 列表界面选择刚才新建的 OSPF 进程 1，点击最右边的“高级”按钮，继续进行 OSPF 相关配置。



图1-4 FW1 设备 OSPF 区域配置



图1-5 FW1 设备 OSPF 网络配置（1）



图1-6 FW1 设备 OSPF 网络配置（2）

登录 FW2 设备 Web 管理界面，参考 FW1 设备 OSPF 配置步骤，部署 FW2 设备的 OSPF 协议，具体操作截图如下：



图1-7 FW2 设备上新建 OSPF 进程



图1-8 FW2 设备 OSPF 区域配置



图1-9 FW2 设备 OSPF 网络配置 (1)



图1-10 FW2 设备 OSPF 网络配置 (2)

使用命令行分别登录 FW1 和 FW2 设备，并关闭防火墙对基础协议报文的过滤功能，确保 OSPF 报文可以正常交互。

```
[FW1] undo firewall packet-filter basic-protocol enable
```

```
[FW2] undo firewall packet-filter basic-protocol enable
```

也可以直接在 Web 管理界面点击命令行按钮，进入网页版命令行窗口，并键入上述命令。二者操作效果相同，以 FW1 设备为例，操作流程如下：

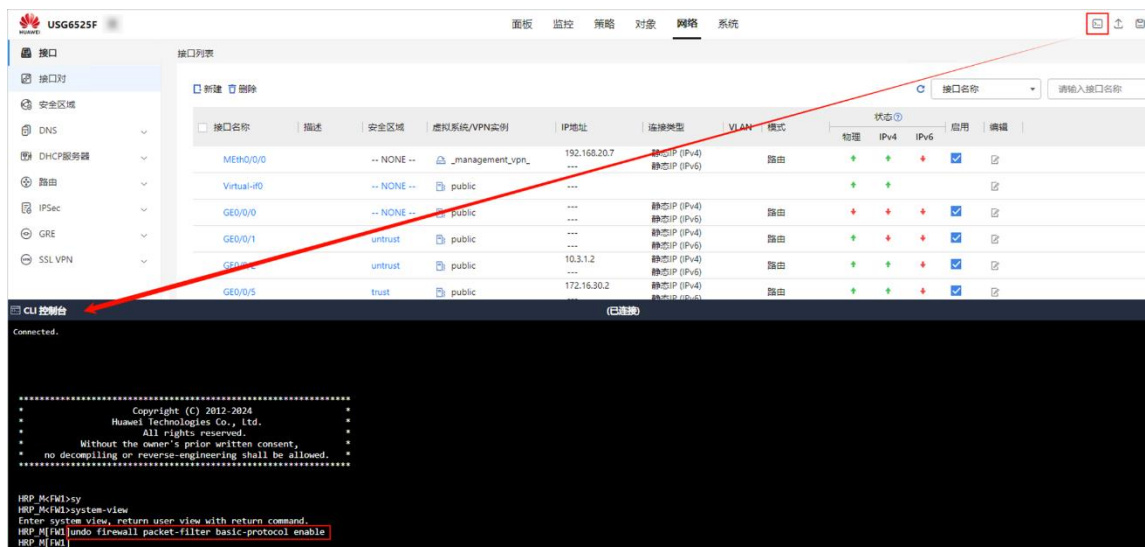


图1-11 进入 FW1 设备网页版命令行窗口并关闭基础协议报文过滤功能

FW2 设备网页版命令行窗口相关操作同上。

RT1 和 RT2 设备上关于 OSPF、缺省路由、缺省路由重发布至 OSPF 以及 NAT 的配置，均可参考“1.2.2 配置步骤-CLI”中相关配置步骤和命令完成，此处不再赘述。

完成 RT1 和 RT2 设备的上述配置后，在 FW1 设备 Web 管理界面，点击“网络 > 路由 > OSPF”进入 OSPF 列表界面，查看 OSPF 邻居状态，效果如下：

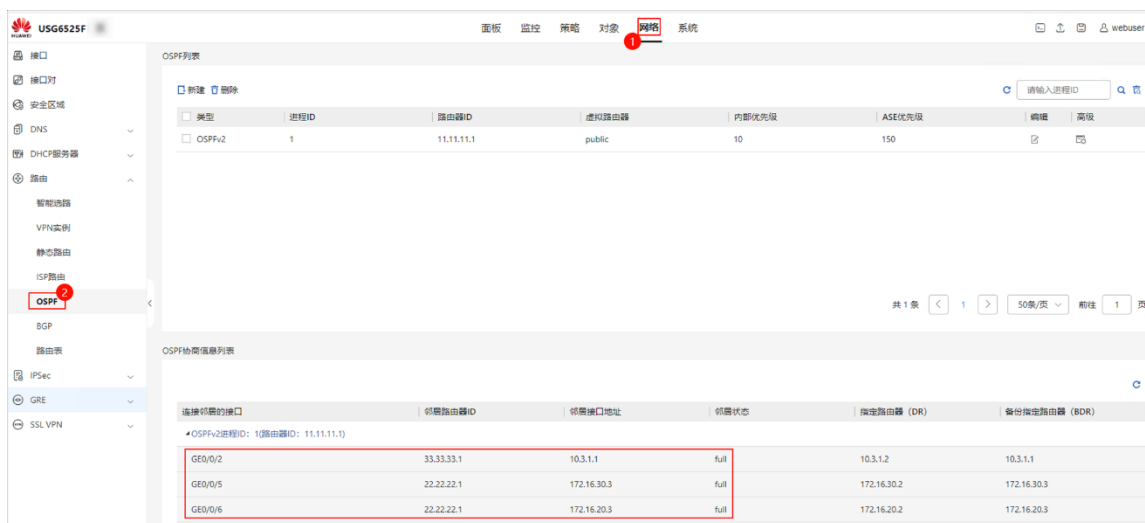


图1-12 查看 FW1 设备 OSPF 邻居状态

继续在 FW1 设备 Web 管理界面选择“网络 > 路由 > 路由表”，进入路由表查看界面，执行以下操作，查看 OSPF 路由条目：



图1-13 查看 FW1 设备 OSPF 路由条目

FW2 设备查看步骤同上。

步骤 3 配置 BFD 会话

在 FW1 设备上创建 BFD 会话，探测从 FW1 至 RT1 设备上游业务接口之间的链路可靠性。登录 FW1 设备 Web 管理界面，选择“系统 > 高可靠性 > BFD”进入 BFD 配置页面，执行以下操作：

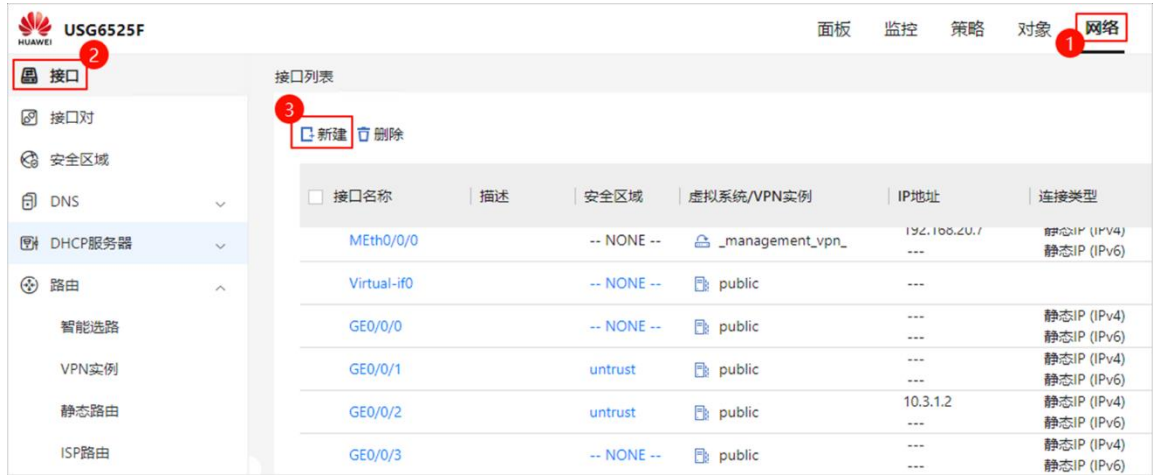


图1-14 在 FW1 设备上创建 BFD 会话

RT1 设备指向 FW1 设备的 BFD 会话的配置可参考“1.2.2 配置步骤-CLI”中相关配置。

步骤 4 配置双机热备

登录 FW1 设备 Web 管理界面，选择“网络 > 接口”进入接口列表界面，点击“新建”，执行以下操作，配置双机热备心跳接口：



USG6525F

网络

接口

接口列表

新建 删除

接口名称	描述	安全区域	虚拟系统/VPN实例	IP地址	连接类型
Meth0/0/0		-- NONE --	_management_vpn_	192.168.20.1	静态IP (IPv4) 静态IP (IPv6)
Virtual-if0		-- NONE --	public	---	静态IP (IPv4) 静态IP (IPv6)
GE0/0/0		-- NONE --	public	---	静态IP (IPv4) 静态IP (IPv6)
GE0/0/1		untrust	public	---	静态IP (IPv4) 静态IP (IPv6)
GE0/0/2		untrust	public	10.3.1.2	静态IP (IPv4) 静态IP (IPv6)
GE0/0/3		-- NONE --	public	---	静态IP (IPv4) 静态IP (IPv6)

图1-15 进入 FW1 设备接口创建界面



图1-16 配置 FW1 心跳接口基础参数

登录 FW2 设备 Web 管理界面，使用同样操作方式，配置 FW2 设备心跳接口的基础参数，具体操作如下：

新建接口

描述

类型

序号

虚拟系统

VPN实例

安全区域

访问控制管理

模式

接口

IPv4

IPv6

连接类型

IP地址

默认网关

接口汇聚

0

public

public

dmz

HTTP

HTTPS

Ping

SSH

Telnet

NETCONF

SNMP

路由

交换

旁路检测

接口对

可选

GE0/0/5

GE0/0/6

GE0/0/7

GE0/0/8

<

1

/ 1

>

已选

GE0/0/3

GE0/0/4

静态IP

DHCP

10.10.10.2/24

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"。

取消

确定

图1-17 配置 FW2 设备心跳接口基础参数

完成上述操作后，登录 FW1 设备 Web 管理界面，选择“系统 > 高可靠性 > 双机热备”，点击“配置”按钮，执行以下操作：



图1-18 FW1 双机热备配置（1）

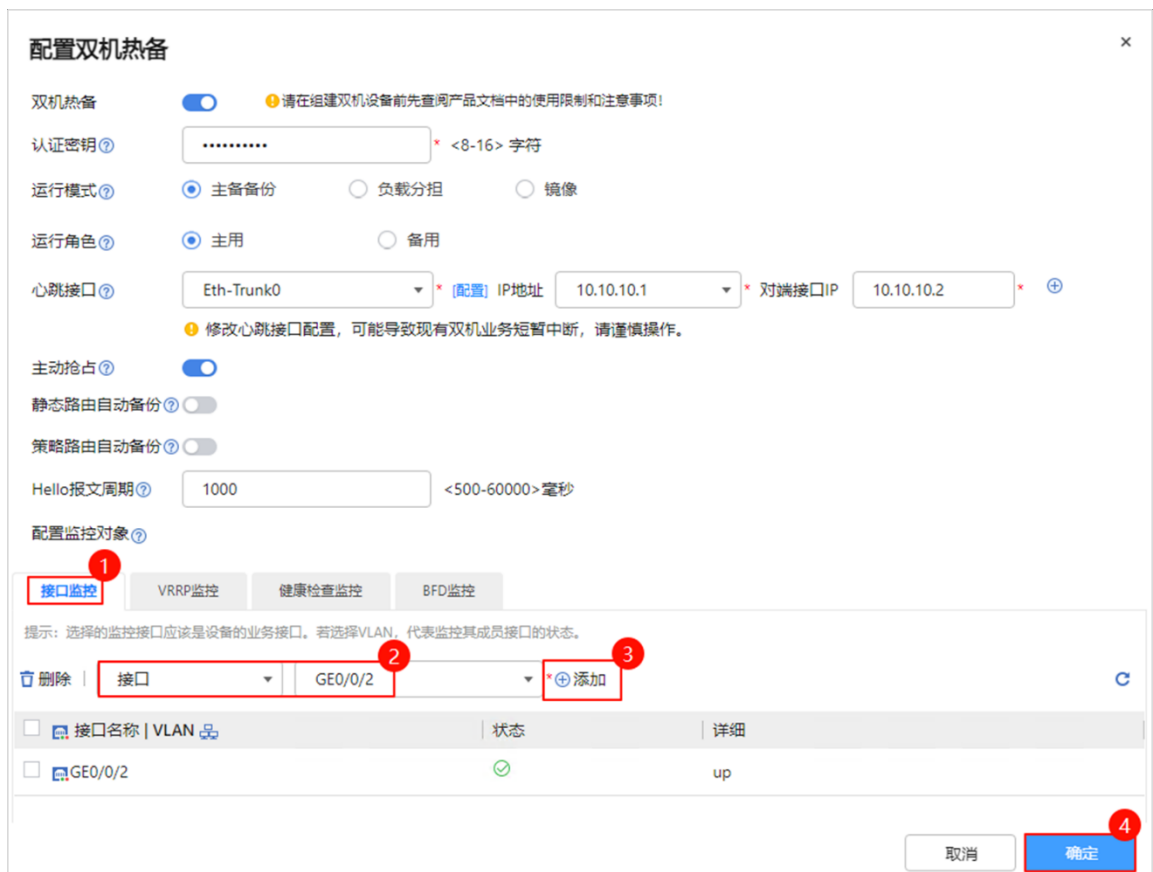


图1-19 FW1 双机热备配置（2）

配置双机热备

认证密码

<8-16> 字符

运行模式

☒ 主备备份

☐ 负载分担

☐ 镜像

运行角色

☒ 主用

☐ 备用

心跳接口

Eth-Trunk0

[配置]

IP地址

10.10.10.1

[配置]

对端接口IP

10.10.10.2

修改心跳接口配置，可能导致现有双机业务短暂中断，请谨慎操作。

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

VRRP监控

提示：当业务接口工作在三层且连接对端设备时，建议配置VRRP监控。

新建

删除

VRID

接口

新建虚拟IP地址

VRID

1

<1-255>

接口

GE0/0/6

[配置]

接口IP地址/掩码

172.16.20.2/255.255.255.0

*

虚拟IP地址/掩码（可选）

172.16.20.1

*

虚拟MAC

☐

取消

确定

图1-20 FW1 双机热备配置（3）

配置双机热备

认证密钥 * <8-16> 字符

运行模式 ☒ 主备备份 ☐ 负载分担 ☐ 镜像

运行角色 ☒ 主用 ☐ 备用

心跳接口 * [配置] IP地址 * 对端接口IP * +

修改心跳接口配置，可能导致现有双机业务短暂中断，请谨慎操作。

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 <500-60000> 毫秒

配置监控对象

接口监控

VRRP监控

提示：当业务接口工作在三层且连接对端设备时，建议配置VRRP监控。

新建

删除

VRID	接口
1	GE0/0/6

新建虚拟IP地址

VRID * <1-255>

接口 * [配置]

接口IP地址/掩码 *

虚拟IP地址/掩码 (可选) *

虚拟MAC ☐

取消

确定

图1-21 FW1 双机热备配置（4）

配置双机热备

认证密码

.....

<8-16> 字符

运行模式

主备备份

负载分担

镜像

运行角色

主用

备用

心跳接口

Eth-Trunk0

[配置]

IP地址

10.10.10.1

对端接口IP

10.10.10.2

修改心跳接口配置，可能导致现有双机业务短暂中断，请谨慎操作。

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

删除

20.1

添加

BFD名称	本地标识	对端IP	出接口	状态
1	20	4.4.4.2		up

取消

确定

图1-22 FW1 双机热备配置（5）

完成 FW1 设备的上述操作后，登录 FW2 设备 Web 管理界面，选择“系统 > 高可靠性 > 双机热备”，点击“配置”按钮，执行以下操作：

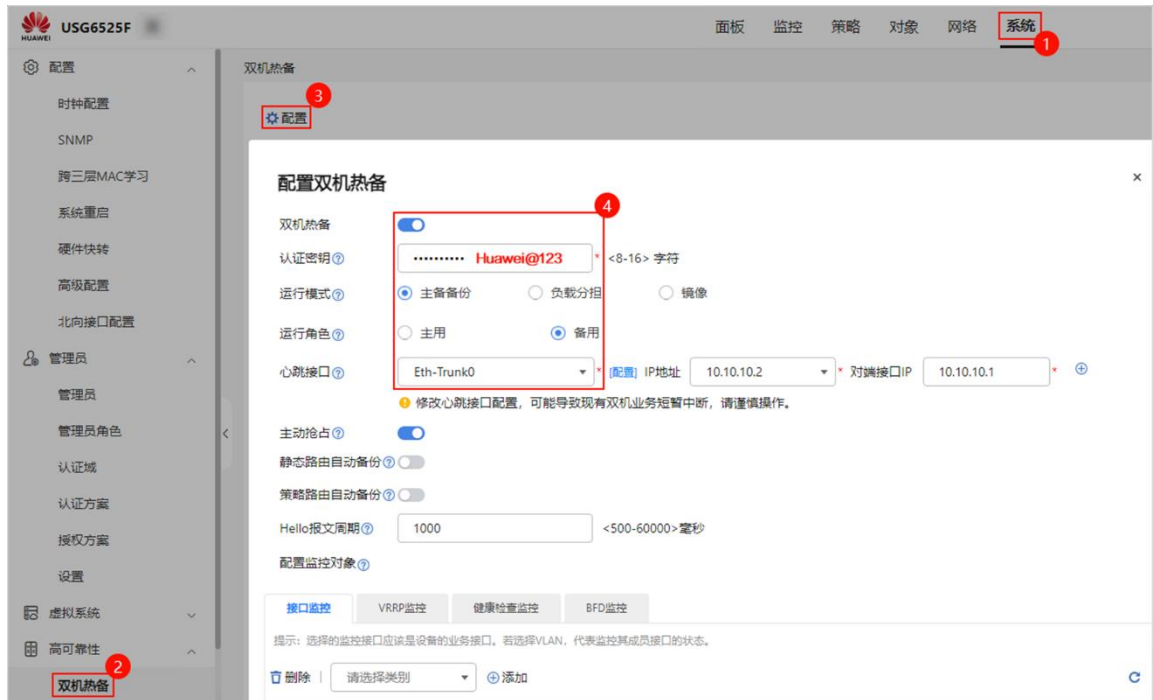


图1-23 FW2 双机热备配置（1）

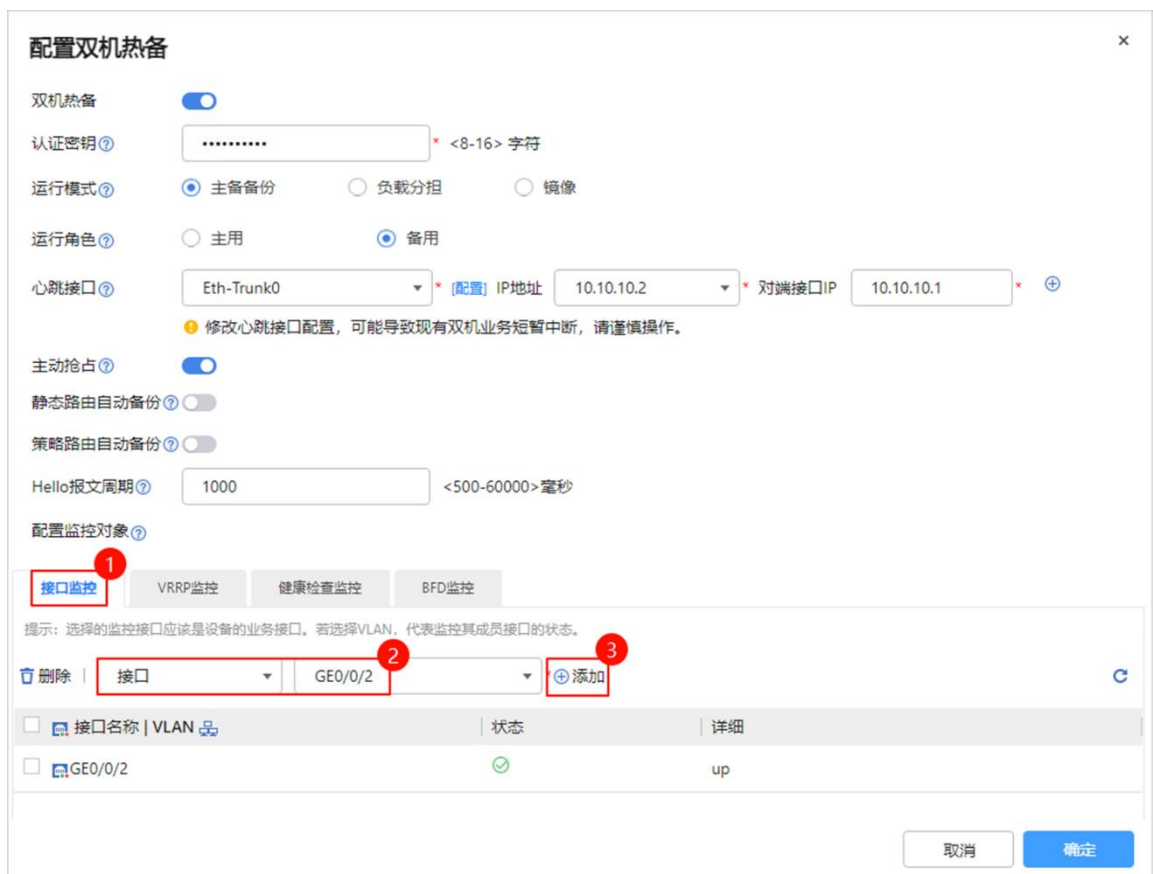


图1-24 FW2 双机热备配置（2）

配置双机热备

运行模式② ☒ 主备备份 ☐ 负载分担 ☐ 镜像

运行角色② ☐ 主用 ☒ 备用

心跳接口② * [配置] IP地址 * 对端接口IP *

⚠ 修改心跳接口配置, 可能导致现有双机业务短暂中断, 请谨慎操作。

主动抢占② ☒

静态路由由自动备份② ☐

策略路由由自动备份② ☐

Hello报文周期② <500-60000>毫秒

配置监控对象②

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。

VRID	接口	接口IP地址/掩码	虚拟IP地址/掩码 (可选)	角色	编辑
☐ 1	GE0/0/5	172.16.20.3/24	172.16.20.1/24	备	编辑
☐ 2	GE0/0/6	172.16.30.3/24	172.16.30.1/24	备	编辑

共 2 条 < 1 > 50条/页 前往 1 页

图1-25 FW2 双机热备配置（3）

完成 FW1 和 FW2 设备的双机热备配置后, 可通过 Web 界面查看双机热备配置状态。在 FW1 设备 Web 管理界面选择“系统 > 高可靠性 > 双机热备”进入双机热备查看界面, 效果如下:

USG6525F 主

面板 监控 策略 对象 网络 **系统**

配置

双机热备

配置

监控项	当前状态	详细
当前运行模式	主备备份	
当前运行角色	主用 (切换后运行的时间: 0 天 0 时 10 分)	详细 强制主备切换
当前心跳接口	Eth-Trunk0	
主动抢占	已启用	
配置一致性	初始化(0000/00/00 00:00:00)	详细 一致性比较 同步双机配置

接口监控 (接口名称 | VLAN)

GE0/0/2	up
---------	----

VRRP监控

172.16.30.1(GE0/0/5)	主状态
172.16.20.1(GE0/0/6)	主状态

健康检查监控

BFD监控

20	up
----	----

图1-26 FW1 设备双机热备配置信息查看

在 FW2 设备 Web 管理界面选择“系统 > 高可靠性 > 双机热备”进入双机热备查看界面，效果如下：

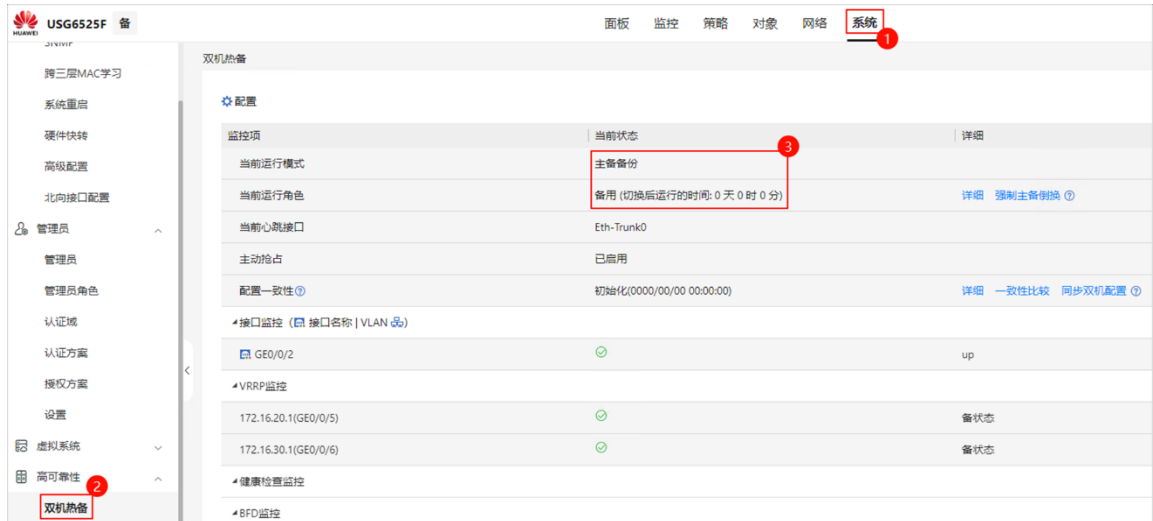


图1-27 FW2 设备双机热备配置信息查看

步骤 5 配置安全策略

说明：由于 FW1 与 FW2 建立了双机热备系统，FW1 的安全策略配置会自动同步到 FW2 上，故此处仅在 FW1 上配置安全策略。

在 FW1 设备 Web 管理界面选择“策略 > 安全策略 > 新建安全策略”，进入安全策略创建界面，执行以下操作：



图1-28 进入 FW1 设备安全策略创建界面

新建安全策略

×

* 名称

t2u

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

地址/地区 ①

any

标签

请选择

目的

目的类型

● 安全区域

○ 虚拟服务

安全区域

untrust

地址/地区 ①

any

标签

请选择

服务 ①

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 ▾

反病毒/入侵防御/URL过滤/内容过滤/文件过滤/邮件过滤/DNS过滤

▽ 其他

激活 Windows

转到“设置”以激活 Windows

取消

命令预览

确定

图1-29 在 FW1 设备创建安全策略放行业务流量

1.3 结果验证

1.3.1 连通性测试

通过 RDP 登录 FTP Server，在 FTP Server 上测试到 SW1 上 3.3.3.1 地址的连通性，效果如下：

```
C:\Users\Administrator>ping 3.3.3.1

Pinging 3.3.3.1 with 32 bytes of data:
Reply from 3.3.3.1: bytes=32 time=1ms TTL=253
Reply from 3.3.3.1: bytes=32 time<1ms TTL=253
Reply from 3.3.3.1: bytes=32 time<1ms TTL=253
Reply from 3.3.3.1: bytes=32 time<1ms TTL=253

Ping statistics for 3.3.3.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Administrator>_
```

图1-30 FTP Server 访问 Internet 资源

通过 RDP 登录 PC1，在 PC1 上测试到 SW1 上 4.4.4.1 地址的连通性，效果如下：

```
C:\Users\Security>ping 4.4.4.1

Pinging 4.4.4.1 with 32 bytes of data:
Reply from 4.4.4.1: bytes=32 time=2ms TTL=253
Reply from 4.4.4.1: bytes=32 time=1ms TTL=253
Reply from 4.4.4.1: bytes=32 time<1ms TTL=253
Reply from 4.4.4.1: bytes=32 time=1ms TTL=253

Ping statistics for 4.4.4.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 1ms

C:\Users\Security>_
```

图1-31 PC1 访问 Internet 资源

1.3.2 路径探测

通过 RDP 登录 FTP Server，在 FTP Server 上测试到 SW1 上 3.3.3.1 地址的流量路径，效果如下：

```
C:\Users\Administrator>tracert 3.3.3.1

Tracing route to 3.3.3.1 over a maximum of 30 hops

  1      8 ms      1 ms      1 ms    172.16.30.2
  2      1 ms     <1 ms     <1 ms    10.3.1.1
  3     62 ms      2 ms      3 ms    3.3.3.1

Trace complete.

C:\Users\Administrator>_
```

图1-32 FTP Server 访问 Internet 资源的流量路径（非故障）

可以发现 FTP Server 正常情况下访问 Internet 资源的流量路径是：FTP Server -> SW2 -> FW1 -> RT1 -> SW1。

通过 RDP 登录 PC1，在 PC1 上测试到 SW1 上 4.4.4.1 地址的连通性，效果如下：

```
C:\Users\Security>tracert 4.4.4.1

Tracing route to 4.4.4.1 over a maximum of 30 hops

  1      2 ms      1 ms      1 ms    172.16.20.2
  2      1 ms     <1 ms     <1 ms    10.3.1.1
  3      3 ms      4 ms      2 ms    4.4.4.1

Trace complete.

C:\Users\Security>_
```

图1-33 PC1 访问 Internet 资源的流量路径（非故障）

可以发现 PC1 正常情况下访问 Internet 资源的流量路径是：PC1 -> SW3 -> FW1 -> RT1 -> SW1。

1.3.3 故障模拟

手动关闭 FW1 的 G0/0/2 接口，在 FTP Server 上测试到 SW1 上 3.3.3.1 地址的路径，效果如下：

```
C:\Users\Administrator>tracert 3.3.3.1

Tracing route to 3.3.3.1 over a maximum of 30 hops

  1      1 ms      1 ms      <1 ms    172.16.30.3
  2      1 ms      <1 ms      1 ms    10.6.1.1
  3      4 ms      2 ms      2 ms    3.3.3.1

Trace complete.

C:\Users\Administrator>_
```

图1-34 FTP Server 访问 Internet 资源的流量路径（故障后）

可以发现 FTP Server 在主用业务路径故障后访问 Internet 资源的流量路径是：FTP Server -> SW3 -> FW2 -> RT2 -> SW1，业务流量切换至备用链路。

手动开启 FW1 的 G0/0/2 接口，并等待 1 分钟后，在 FTP Server 上测试到 SW1 上 3.3.3.1 地址的路径，效果如下：

```
C:\Users\Administrator>tracert 3.3.3.1

Tracing route to 3.3.3.1 over a maximum of 30 hops

  1      8 ms      1 ms      1 ms    172.16.30.2
  2      1 ms      <1 ms      <1 ms    10.3.1.1
  3     62 ms      2 ms      3 ms    3.3.3.1

Trace complete.

C:\Users\Administrator>_
```

图1-35 FTP Server 访问 Internet 资源的流量路径（故障恢复后）

可以发现 FTP Server 在主用业务路径故障恢复后访问 Internet 资源的流量路径是：FTP Server -> SW3 -> FW1 -> RT1 -> SW1，业务流量已切换至主用链路。

1.4 配置参考

1.4.1 RT1 配置

```
#
sysname RT1
#
acl number 3500
 rule 5 permit ip
#
bfd
```

```
#
interface GigabitEthernet0/0/1
 undo portswitch
#
interface GigabitEthernet0/0/1.2
 dot1q termination vid 2
 ip address 4.4.4.2 255.255.255.252
 nat outbound 3500
#
interface GigabitEthernet0/0/2
 undo portswitch
 ip address 10.1.1.1 255.255.255.252
 ospf enable 1 area 0.0.0.0
#
interface GigabitEthernet0/0/4
 undo portswitch
 ip address 10.3.1.1 255.255.255.252
 ospf enable 1 area 0.0.0.0
#
interface LoopBack0
 ip address 33.33.33.1 255.255.255.255
#
bfd
bfd 1 bind peer-ip 10.3.1.2 source-ip 4.4.4.2
 discriminator local 10
 discriminator remote 20
 commit
#
ospf 1 router-id 33.33.33.1
 default-route-advertise always
 area 0.0.0.0
#
ip route-static 0.0.0.0 0.0.0.0 4.4.4.1
#
return
```

1.4.2 RT2 配置

```
#
sysname RT2
#
acl number 3500
 rule 5 permit ip
#
interface GigabitEthernet0/0/1
 undo portswitch
#
interface GigabitEthernet0/0/1.40
```



```
dot1q termination vid 40
ip address 3.3.3.2 255.255.255.252
nat outbound 3500
#
interface GigabitEthernet0/0/2
undo portswitch
ip address 10.1.1.2 255.255.255.252
ospf enable 1 area 0.0.0.0
#
interface GigabitEthernet0/0/4
undo portswitch
ip address 10.6.1.1 255.255.255.252
ospf enable 1 area 0.0.0.0
#
interface LoopBack0
ip address 44.44.44.1 255.255.255.255
#
ospf 1 router-id 44.44.44.1
default-route-advertise always
area 0.0.0.0
#
ip route-static 0.0.0.0 0.0.0.0 3.3.3.1
#
return
```

1.4.3 FW1 配置

```
#
sysname FW1
#
undo firewall packet-filter basic-protocol enable
#
hrp enable
hrp device active
hrp standby config enable
hrp mirror session enable
hrp interface Eth-Trunk0 remote 10.10.10.2
hrp track bfd-session 20
hrp track interface GE0/0/2
hrp authentication-key Huawei@123
#
bfd
#
interface Eth-Trunk0
ip address 10.10.10.1 255.255.255.0
#
interface G0/0/2
undo shutdown
```

```
ip address 10.3.1.2 255.255.255.252
ospf enable 1 area 0.0.0.0
#
interface G0/0/3
undo shutdown
eth-trunk 0
#
interface G0/0/4
undo shutdown
eth-trunk 0
#
interface G0/0/5
undo shutdown
ip address 172.16.30.2 255.255.255.0
vrrp vrid 2 virtual-ip 172.16.30.1 active
ospf enable 1 area 0.0.0.0
#
interface G0/0/6
undo shutdown
ip address 172.16.20.2 255.255.255.0
vrrp vrid 1 virtual-ip 172.16.20.1 active
ospf enable 1 area 0.0.0.0
#
interface LoopBack0
ip address 11.11.11.1 255.255.255.255
#
firewall zone trust
set priority 85
add interface G0/0/5
add interface G0/0/6
#
firewall zone untrust
set priority 5
add interface G0/0/2
#
firewall zone dmz
set priority 50
add interface Eth-Trunk0
#
bfd 1 bind peer-ip 4.4.4.2 source-ip 10.3.1.2
discriminator local 20
discriminator remote 10
commit
#
ospf 1 router-id 11.11.11.1
area 0.0.0.0
#
security-policy
```

```
rule name policy_sec1
  source-zone trust
  destination-zone untrust
  action permit
#
return
```

1.4.4 FW2 配置

```
#
sysname FW2
#
undo firewall packet-filter basic-protocol enable
#
hrp enable
hrp device standby
hrp standby config enable
hrp mirror session enable
hrp interface Eth-Trunk0 remote 10.10.10.1
hrp track interface GE0/0/2
hrp authentication-key Huawei@123
#
interface Eth-Trunk0
  ip address 10.10.10.2 255.255.255.0
#
interface G0/0/2
  undo shutdown
  ip address 10.6.1.2 255.255.255.252
  ospf enable 1 area 0.0.0.0
#
interface G0/0/3
  undo shutdown
  eth-trunk 0
#
interface G0/0/4
  undo shutdown
  eth-trunk 0
#
interface G0/0/5
  undo shutdown
  ip address 172.16.20.3 255.255.255.0
  vrrp vrid 2 virtual-ip 172.16.20.1 standby
  ospf enable 1 area 0.0.0.0
#
interface G0/0/6
  undo shutdown
  ip address 172.16.30.3 255.255.255.0
  vrrp vrid 2 virtual-ip 172.16.30.1 standby
```

```
ospf enable 1 area 0.0.0.0
#
interface LoopBack0
 ip address 22.22.22.1 255.255.255.255
#
firewall zone trust
 set priority 85
 add interface G0/0/5
 add interface G0/0/6
#
firewall zone untrust
 set priority 5
 add interface G0/0/1
 add interface G0/0/2
#
firewall zone dmz
 set priority 50
 add interface Eth-Trunk0
#
ospf 1 router-id 22.22.22.1
 area 0.0.0.0
#
security-policy
 rule name policy_sec1
  source-zone trust
  destination-zone untrust
  action permit
#
return
```

1.4.5 SW1 预配置

```
#
sysname SW1
#
vlan batch 2 40
#
interface vlanif2
 ip address 4.4.4.1 255.255.255.252
#
interface vlanif40
 ip address 3.3.3.1 255.255.255.252
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 2 40
#
ip route-static 172.16.0.0 16 4.4.4.2
```

```
ip route-static 172.16.0.0 16 3.3.3.2 preference 70
#
return
```

1.4.6 SW2 预配置

```
#
sysname SW2
#
vlan batch 30
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 30
#
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 30
#
interface GigabitEthernet0/0/14
 port link-type access
 port default vlan 30
#
return
```

1.4.7 SW3 预配置

```
#
sysname SW3
#
vlan batch 40
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 40
#
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 40
#
interface GigabitEthernet0/0/13
 port link-type access
 port default vlan 40
#
return
```

1.4.8 Mirror-SW 预配置

```
#
sysname Mirror-SW
#
vlan batch 2 40
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 2 40
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 2 40
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 2 40
#
return
```

1.5 思考题

防火墙主备备份模式的双机热备系统和负载分担模式的双机热备系统的区别是什么？

参考答案：

主备备份：两台防火墙一主一备。正常情况下业务流量由主用设备处理。当主用设备故障时，备用设备接替主用设备处理业务流量，保证业务不中断。

负载分担：两台防火墙互为主备。正常情况下两台设备共同分担整网的业务流量。当其中一台设备故障时，另外一台设备会承担其业务，保证原本通过该设备转发的业务不中断。

2 防火墙双机热备故障排除实验

2.1 实验介绍

2.1.1 关于本实验

本实验将 FW1 和 FW2 两台防火墙部署为主备模式双机热备系统，作为企业出口区安全网关，两台路由器作为企业出口设备，保证了在网络通信线路单边故障的情况下，企业内网仍可与外部网络之间正常通信，业务连续性不受影响。

鉴于学员在部署双机热备时，可能会遇到一些故障类问题。本实验以预配置脚本的方式，设置双机热备故障点，供学员排错练习。

2.1.2 实验目的

- 理解主备备份模式双机热备工作原理。
- 掌握双机热备关键配置。
- 掌握双机热备故障排查思路和操作步骤。

2.1.3 实验组网介绍

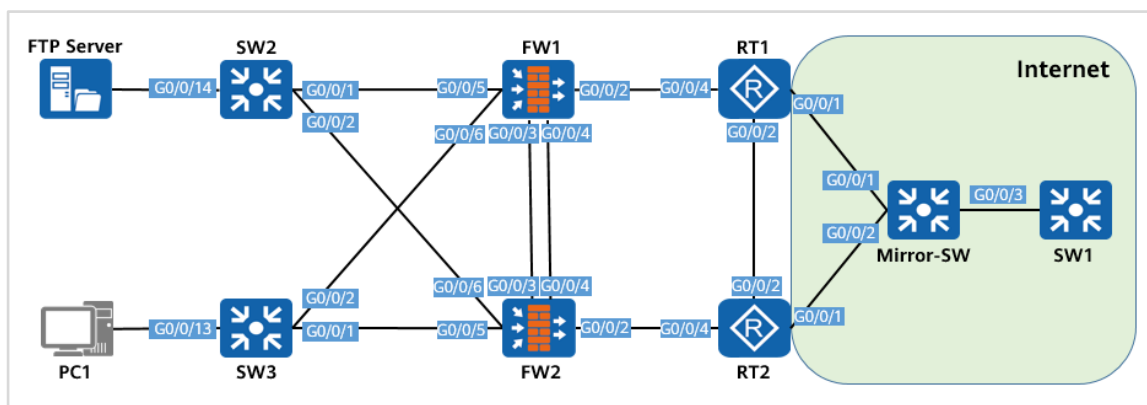


图2-1 双机热备故障排除实验拓扑

FW1 与 FW2 组建主备模式双机热备系统，PC1 和 FTP Server 的网关分别为防火墙上 VRRP1 与 VRRP2 备份组虚拟 IP。RT1、RT2 与 FW1、FW2 之间运行 OSPF 实现网络互通。RT1 与 RT2 模拟企业网络的出口设备，SW1 与 Mirror-SW 模拟 Internet，SW2 和 SW3 作为接入交换机连接内网终端，最终实现内部网络的 PC1 与 FTP Server 可以与 Internet 互通。

2.1.4 实验规划

表2-1 设备接口规划表

设备	接口	接口性质	接口信息	说明
RT1	G0/0/1.2	三层子接口	4.4.4.2/30 终结VLAN2	网络出接口，与Mirror-SW互连
	G0/0/2	三层接口	10.1.1.1/30	与RT2互连
	G0/0/4	三层接口	10.3.1.1/30	与FW1互连
	LoopBack0	三层接口	33.33.33.1/32	OSPF Router-ID
RT2	G0/0/1.40	三层子接口	3.3.3.2/30 终结VLAN40	网络出接口，与Mirror-SW互连
	G0/0/2	三层接口	10.1.1.2/30	与RT1互连
	G0/0/4	三层接口	10.6.1.1/30	与FW1互连
	LoopBack0	三层接口	44.44.44.1/32	OSPF Router-ID
FW1	G0/0/2	三层接口	10.3.1.2/30 安全域：untrust	上行连接RT1接口
	G0/0/3	Eth-trunk 0 聚合接口	10.10.10.1/24 安全域：dmz	双机热备心跳接口
	G0/0/4			
	G0/0/5	三层接口	172.16.30.2/24 安全域：trust	下行连接接入SW接口，需要配置VRRP虚拟网关
	G0/0/6	三层接口	172.16.20.2/24 安全域：trust	
	LoopBack0	三层接口	11.11.11.1/32	OSPF Router-ID
FW2	G0/0/2	三层接口	10.6.1.2/30 安全域：untrust	上行连接RT2接口
	G0/0/3	Eth-trunk 0 聚合接口	10.10.10.2/24 安全域：dmz	双机热备心跳接口
	G0/0/4			
	G0/0/5	三层接口	172.16.20.3/24 安全域：trust	下行连接接入SW接口，需要配置VRRP虚拟网关
	G0/0/6	三层接口	172.16.30.3/24	

			安全域: trust	
	LoopBack0	三层接口	22.22.22.1/32	OSPF Router-ID
SW1	G0/0/3	Trunk	PVID: 1 Allow-pass VLAN: 2, 40	互连接口
	VLANIF2	三层	4.4.4.1/30	与RT1出口地址为直连
	VLANIF40	三层	3.3.3.1/30	与RT2出口地址为直连
SW2	G0/0/1	Access	PVID: 30	上下行接口只需允许业务VLAN通过
	G0/0/2			
	G0/0/14			
SW3	G0/0/1	Access	PVID: 40	上下行接口只需允许业务VLAN通过
	G0/0/2			
	G0/0/13			
Mirror-SW	G0/0/1	Trunk	PVID: 1 Allow-pass VLAN: 2, 40	上下行接口只需允许业务VLAN通过
	G0/0/2			
	G0/0/3			
PC1	Ethernet0	网卡	172.16.20.100/24 网关: 172.16.20.1/24	终端
FTP Server	Ethernet0	网卡	172.16.30.101/24 网关: 172.16.30.1/24	终端

2.2 实验任务配置

2.2.1 配置思路

- 1.将预配置刷入对应设备。
- 2.按照实验规划检查业务是否正常，并逐一排错。

2.2.2 配置步骤

步骤 1 导入预配

在对应设备中刷入对应的预配置脚本，完成实验预配。

RT1

```
#
sysname RT1
#
acl number 3500
rule 5 permit ip
#
bfd
#
interface GigabitEthernet0/0/1
undo portswitch
#
interface GigabitEthernet0/0/1.2
dot1q termination vid 2
ip address 4.4.4.2 255.255.255.252
nat outbound 3500
#
interface GigabitEthernet0/0/2
undo portswitch
ip address 10.1.1.1 255.255.255.252
ospf enable 1 area 0.0.0.0
#
interface GigabitEthernet0/0/4
undo portswitch
ip address 10.3.1.1 255.255.255.252
ospf enable 1 area 0.0.0.0
#
interface LoopBack0
ip address 33.33.33.1 255.255.255.255
#
bfd 1 bind peer-ip 10.3.1.2 source-ip 4.4.4.2
discriminator local 10
discriminator remote 20
commit
#
ospf 1 router-id 33.33.33.1
default-route-advertise always
area 0.0.0.0
#
ip route-static 0.0.0.0 0.0.0.0 4.4.4.1
#
return
```

RT2

```
#
sysname RT2
```

```
#
acl number 3500
  rule 5 permit ip
#
interface GigabitEthernet0/0/1
  undo portswitch
#
interface GigabitEthernet0/0/1.40
  dot1q termination vid 40
  ip address 3.3.3.2 255.255.255.252
  nat outbound 3500
#
interface GigabitEthernet0/0/2
  undo portswitch
  ip address 10.1.1.2 255.255.255.252
  ospf enable 1 area 0.0.0.0
#
interface GigabitEthernet0/0/4
  undo portswitch
  ip address 10.6.1.1 255.255.255.252
  ospf enable 1 area 0.0.0.0
#
interface LoopBack0
  ip address 44.44.44.1 255.255.255.255
#
ospf 1 router-id 44.44.44.1
  default-route-advertise always
  area 0.0.0.0
#
ip route-static 0.0.0.0 0.0.0.0 3.3.3.1
#
return
```

FW1

```
#
sysname FW1
#
undo firewall packet-filter basic-protocol enable
#
hrp enable
hrp device active
hrp standby config enable
hrp mirror session enable
hrp interface Eth-Trunk0 remote 10.10.10.2
hrp track bfd-session 20
hrp track interface GE0/0/2
hrp authentication-key Huawei@123
#
```

```
bfd
#
interface Eth-Trunk0
 ip address 10.10.10.1 255.255.255.0
#
interface G0/0/2
 undo shutdown
 ip address 10.3.1.2 255.255.255.252
 ospf enable 1 area 0.0.0.0
#
interface G0/0/3
 undo shutdown
 eth-trunk 0
#
interface G0/0/4
 undo shutdown
 eth-trunk 0
#
interface G0/0/5
 undo shutdown
 ip address 172.16.30.2 255.255.255.0
 vrrp vrid 2 virtual-ip 172.16.30.1 active
 ospf enable 1 area 0.0.0.0
#
interface G0/0/6
 undo shutdown
 ip address 172.16.20.2 255.255.255.0
 vrrp vrid 1 virtual-ip 172.16.20.1 active
 ospf enable 1 area 0.0.0.0
#
interface LoopBack0
 ip address 11.11.11.1 255.255.255.255
#
firewall zone trust
 set priority 85
 add interface G0/0/5
 add interface G0/0/6
#
firewall zone untrust
 set priority 5
 add interface G0/0/1
 add interface G0/0/2
#
firewall zone dmz
 set priority 50
 add interface Eth-Trunk0
#
bfd 1 bind peer-ip 4.4.4.2 source-ip 10.3.1.2
```

```
discriminator local 20
discriminator remote 10
commit
#
ospf 1 router-id 11.11.11.1
area 0.0.0.0
#
security-policy
rule name policy_sec1
source-zone trust
destination-zone untrust
action permit
#
return
```

FW2

```
#
sysname FW2
#
undo firewall packet-filter basic-protocol enable
#
hrp enable
hrp device standby
hrp standby config enable
hrp mirror session enable
hrp interface Eth-Trunk0 remote 10.10.10.1
hrp track interface GE0/0/2
hrp authentication-key Huawei@123
#
interface Eth-Trunk0
ip address 10.10.10.2 255.255.255.0
#
interface G0/0/2
undo shutdown
ip address 10.6.1.2 255.255.255.252
ospf enable 1 area 0.0.0.0
#
interface G0/0/3
undo shutdown
eth-trunk 0
#
interface G0/0/4
undo shutdown
eth-trunk 0
#
interface G0/0/5
undo shutdown
ip address 172.16.20.3 255.255.255.0
```

```
vrp vrid 2 virtual-ip 172.16.20.1 standby
ospf enable 1 area 0.0.0.0
#
interface G0/0/6
undo shutdown
ip address 172.16.30.3 255.255.255.0
vrp vrid 2 virtual-ip 172.16.30.1 active
ospf enable 1 area 0.0.0.0
#
interface LoopBack0
ip address 22.22.22.1 255.255.255.255
#
firewall zone trust
set priority 85
add interface G0/0/5
add interface G0/0/6
#
firewall zone untrust
set priority 5
add interface G0/0/1
add interface G0/0/2
#
firewall zone dmz
set priority 50
#
ospf 1 router-id 22.22.22.1
area 0.0.0.0
#
security-policy
rule name policy_sec1
source-zone trust
destination-zone untrust
action permit
#
return
```

SW1

```
#
sysname SW1
#
vlan batch 2 40
#
interface vlanif2
ip address 4.4.4.1 255.255.255.252
#
interface vlanif40
ip address 3.3.3.1 255.255.255.252
#
```

```
interface GigabitEthernet0/0/3
  port link-type trunk
  port trunk allow-pass vlan 2 40
#
ip route-static 172.16.0.0 16 4.4.4.2
ip route-static 172.16.0.0 16 3.3.3.2 preference 70
#
return
```

SW2

```
#
sysname SW2
#
vlan batch 30
#
interface GigabitEthernet0/0/1
  port link-type access
  port default vlan 30
#
interface GigabitEthernet0/0/2
  port link-type access
  port default vlan 30
#
interface GigabitEthernet0/0/14
  port link-type access
  port default vlan 30
#
return
```

SW3

```
#
sysname SW3
#
vlan batch 40
#
interface GigabitEthernet0/0/1
  port link-type access
  port default vlan 40
#
interface GigabitEthernet0/0/2
  port link-type access
  port default vlan 40
#
interface GigabitEthernet0/0/13
  port link-type access
  port default vlan 40
#
return
```

Mirror-SW

```
#
sysname Mirror-SW
#
vlan batch 2 40
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 2 40
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 2 40
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 2 40
#
return
```

步骤 2 故障排查

本案例中双机热备为下行连接交换机，上行连接路由器的主备备份模式双机热备组网。心跳接口是 GigabitEthernet0/0/3 和 GigabitEthernet0/0/4 捆绑的链路聚合接口，正确的配置逻辑为：

1. 监控上下行业务接口状态。
2. 配置下行连接交换机的 VRRP 备份组。
3. 配置上行连接路由器的动态路由。
4. 确保心跳接口路由可达。
5. 指定心跳接口、配置 HRP 认证密钥并启用双机热备功能。

按照上述配置思路，逐一排查问题。

刷入预配置后，检查 FW1 和 FW2 的双机热备状态。

```
HRP_M[FW1]display hrp state
Local role: Active, Peer role: Unknown
Local priority: 0:2, Peer priority: 0:0
Connection state: failed
Stable time: 0 day, 0 hour, 0 minute
Last state change information: The HRP link changes to down due to "Heartbeat packet timeout". local device ID is 14-8c-4a-e9-22-30, peer device ID is 60-9b-b4-ef-e1-e0.
```

```
HRP_M[FW2]display hrp state
Local role: Active, Peer role: Unknown
Local priority: 0:2, Peer priority: 0:0
Connection state: failed
```



```
Stable time: 0 day, 0 hour, 0 minute
Last state change information: The HRP core state changed due to "HRP hello packet negotiation failed". (old_state=standby, new_state=active, local_fault_indicator=0, local_robustness_indicator=2, peer_fault_indicator=0, peer_robustness_indicator=0)
```

经过检查发现，FW1 和 FW2 各自认为自己是双机热备的主设备，且不知道对端设备的状态，需要按照配置思路排查问题。

首先检查 FW1 和 FW2 监控上行接口的配置是否正确。

```
HRP_M[FW1] dis cu | in hrp track
hrp track bfd-session 20
hrp track interface GE0/0/2
HRP_M[FW1]
```

```
HRP_M[FW2] dis cu | in hrp track
hrp track interface GE0/0/2
HRP_M[FW2]
```

可以发现设备针对上行业务接口的监控命令已正常配置。

继续检查设备业务接口状态。

```
HRP_M[FW1] display interface brief
PHY: Physical
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
(b): BFD down
(e): ETHOAM down
(d): Dampening Suppressed
(p): port alarm down
(dl): DLDAP down
(c): CFM down
(ed): error down
InUti/OutUti: input utility rate/output utility rate
```

Interface	PHY	Protocol	InUti	OutUti	inErrors	outErrors
10GE0/0/0	down	down	0%	0%	0	0
10GE0/0/1	down	down	0%	0%	0	0
Eth-Trunk0	up	up	0.01%	0.01%	0	0
GE0/0/3	up	up	0.01%	0.01%	0	0
GE0/0/4	up	up	0%	0%	0	0
GE0/0/0	down	down	0%	0%	0	0
GE0/0/1	up	down	0.01%	0%	0	0
GE0/0/2	up	up	0.01%	0.01%	0	0
GE0/0/5	up	up	0.01%	0.01%	0	0
GE0/0/6	up	up	0.01%	0.01%	0	0
GE0/0/7	up	down	0%	0%	0	0
GE0/0/8	down	down	0%	0%	0	0
GE0/0/9	down	down	0%	0%	0	0

LoopBack0	up	up(s)	--	--	0	0
MEth0/0/0	up	up	0.01%	0.01%	0	0
NULL0	up	up(s)	0%	0%	0	0
Virtual-if0	up	up(s)	0%	0%	0	0

```
HRP_M[FW2]display interface brief
```

```
PHY: Physical
```

```
*down: administratively down
```

```
^down: standby
```

```
(l): loopback
```

```
(s): spoofing
```

```
(b): BFD down
```

```
(e): ETHOAM down
```

```
(d): Dampening Suppressed
```

```
(p): port alarm down
```

```
(dl): DLDP down
```

```
(c): CFM down
```

```
(ed): error down
```

```
InUti/OutUti: input utility rate/output utility rate
```

Interface	PHY	Protocol	InUti	OutUti	inErrors	outErrors
10GE0/0/0	down	down	0%	0%	0	0
10GE0/0/1	down	down	0%	0%	0	0
Eth-Trunk0	up	up	0.01%	0.01%	0	0
GE0/0/3	up	up	0.01%	0.01%	0	0
GE0/0/4	up	up	0%	0%	0	0
GE0/0/0	down	down	0%	0%	0	0
GE0/0/1	up	down	0.01%	0%	0	0
GE0/0/2	up	up	0.01%	0.01%	0	0
GE0/0/5	up	up	0.01%	0.01%	0	0
GE0/0/6	up	up	0.01%	0.01%	0	0
GE0/0/7	down	down	0%	0%	0	0
GE0/0/8	down	down	0%	0%	0	0
GE0/0/9	down	down	0%	0%	0	0
LoopBack0	up	up(s)	--	--	0	0
MEth0/0/0	up	up	0.01%	0.01%	0	0
NULL0	up	up(s)	0%	0%	0	0
Virtual-if0	up	up(s)	0%	0%	0	0

由以上信息可以发现，两台防火墙业务接口状态均正常。

继续检查两台 FW 设备的业务接口 IP 地址配置情况。

```
HRP_M[FW1]display ip interface brief
```

```
*down: administratively down
```

```
!down: FIB overload down
```

```
^down: standby
```

```
(l): loopback
```

```
(s): spoofing
```

```
(d): Dampening Suppressed
```

(ed): error down

The number of interface that is UP in Physical is 10

The number of interface that is DOWN in Physical is 5

The number of interface that is UP in Protocol is 8

The number of interface that is DOWN in Protocol is 7

Interface	IP Address/Mask	Physical	Protocol	VPN
10GE0/0/0	unassigned	down	down	--
10GE0/0/1	unassigned	down	down	--
Eth-Trunk0	10.10.10.1/24	up	up	--
GE0/0/0	unassigned	down	down	--
GE0/0/1	unassigned	up	down	--
GE0/0/2	10.3.1.2/30	up	up	--
GE0/0/5	172.16.30.2/24	up	up	--
GE0/0/6	172.16.20.2/24	up	up	--
GE0/0/7	unassigned	up	down	--
GE0/0/8	unassigned	down	down	--
GE0/0/9	unassigned	down	down	--
LoopBack0	11.11.11.1/32	up	up(s)	--
MEth0/0/0	192.168.20.7/24	up	up	_management...
NULL0	unassigned	up	up(s)	--
Virtual-if0	unassigned	up	up(s)	--

HRP_M[FW2]display ip interface brief

*down: administratively down

!down: FIB overload down

^down: standby

(l): loopback

(s): spoofing

(d): Dampening Suppressed

(ed): error down

The number of interface that is UP in Physical is 9

The number of interface that is DOWN in Physical is 6

The number of interface that is UP in Protocol is 8

The number of interface that is DOWN in Protocol is 7

Interface	IP Address/Mask	Physical	Protocol	VPN
10GE0/0/0	unassigned	down	down	--
10GE0/0/1	unassigned	down	down	--
Eth-Trunk0	10.10.10.2/24	up	up	--
GE0/0/0	unassigned	down	down	--
GE0/0/1	unassigned	up	down	--
GE0/0/2	10.6.1.2/30	up	up	--
GE0/0/5	172.16.20.3/24	up	up	--
GE0/0/6	172.16.30.3/24	up	up	--
GE0/0/7	unassigned	down	down	--
GE0/0/8	unassigned	down	down	--
GE0/0/9	unassigned	down	down	--
LoopBack0	22.22.22.1/32	up	up(s)	--

Meth0/0/0	192.168.20.6/24	up	up	_management...
NULL0	unassigned	up	up(s)	--
Virtual-if0	unassigned	up	up(s)	--

由以上信息发现，两台 FW 设备在本实验用到的业务接口的 IP 地址均已正常配置。

继续检查 FW 设备的安全区域配置。

```
HRP_M[FW1]display zone
local
  priority is 100
  interface of the zone is (0):
#
trust
  priority is 85
  interface of the zone is (2):
    GE0/0/5
    GE0/0/6
#
untrust
  priority is 5
  interface of the zone is (2):
    GE0/0/1
    GE0/0/2
#
dmz
  priority is 50
  interface of the zone is (1):
    Eth-Trunk0
#
```

```
HRP_M[FW2]display zone
local
  priority is 100
  interface of the zone is (0):
#
trust
  priority is 85
  interface of the zone is (2):
    GE0/0/5
    GE0/0/6
#
untrust
  priority is 5
  interface of the zone is (2):
    GE0/0/1
    GE0/0/2
#
dmz
```

```
priority is 50
interface of the zone is (0):
#
```

由以上信息可以发现，FW2 设备上没有将心跳接口 Eth-Trunk0 规划进安全区域。需要执行以下操作修正配置。

```
HRP_M[FW2]firewall zone dmz
HRP_M[FW2-zone-dmz]add interface Eth-Trunk 0
HRP_M[FW2-zone-dmz]quit
HRP_M[FW2]
```

完成上述修改后，可以发现双机热备系统依旧是双主状态，需要继续排查故障，接下来检查 FW 设备下游接口的 VRRP 配置。

```
HRP_M[FW1]dis cu interface g0/0/5
#
interface GE0/0/5
ip address 172.16.30.2 255.255.255.0
vrrp vrid 2 virtual-ip 172.16.30.1 active
ospf enable 1 area 0.0.0.0
#
return
HRP_M[FW1]dis cu interface g0/0/6
#
interface GE0/0/6
ip address 172.16.20.2 255.255.255.0
vrrp vrid 1 virtual-ip 172.16.20.1 active
ospf enable 1 area 0.0.0.0
#
return
```

```
HRP_M[FW2]dis cu interface g0/0/5
#
interface GE0/0/5
ip address 172.16.20.3 255.255.255.0
vrrp vrid 1 virtual-ip 172.16.20.1 standby
ospf enable 1 area 0.0.0.0
#
return
HRP_M[FW2]dis cu interface g0/0/6
#
interface GE0/0/6
ip address 172.16.30.3 255.255.255.0
vrrp vrid 2 virtual-ip 172.16.30.1 active
ospf enable 1 area 0.0.0.0
#
return
```

由以上信息可以发现，FW2 设备下游 G0/0/6 业务接口的 VRRP 备份组状态配置与网络规划不一致，需要执行以下操作修正。

```
HRP_M[FW2]interface g0/0/6
HRP_M[FW2-GE0/0/6]vrrp vrid 2 virtual-ip 172.16.30.1 standby
HRP_M[FW2-GE0/0/6]quit
HRP_M[FW2]
```

完成上述修改后，可以发现双机热备系统依旧是双主状态，需要继续排查故障，接下来检查防火墙 OSPF 邻居关系。

```
HRP_M[FW1]display ospf peer brief
OSPF Process 1 with Router ID 11.11.11.1
      Peer Statistic Information
Total number of peer(s): 3
Peer(s) in full state: 3
```

Area Id	Interface	Neighbor id	State
0.0.0.0	GE0/0/2	33.33.33.1	Full
0.0.0.0	GE0/0/5	22.22.22.1	Full
0.0.0.0	GE0/0/6	22.22.22.1	Full

```
HRP_M[FW2]display ospf peer brief
OSPF Process 1 with Router ID 22.22.22.1
      Peer Statistic Information
Total number of peer(s): 3
Peer(s) in full state: 3
```

Area Id	Interface	Neighbor id	State
0.0.0.0	GE0/0/2	44.44.44.1	Full
0.0.0.0	GE0/0/5	11.11.11.1	Full
0.0.0.0	GE0/0/6	11.11.11.1	Full

由以上信息可以发现，FW 设备上 OSPF 邻居关系均正常，继续排查两台 FW 设备之间心跳接口的路由可达性。

```
HRP_M[FW1]interface Eth-Trunk 0
HRP_M[FW1-Eth-Trunk0]service-manage ping permit
HRP_M[FW1-Eth-Trunk0]quit
HRP_M[FW1]security-policy
HRP_M[FW1-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
HRP_M[FW1-policy-security]ping 10.10.10.2
  PING 10.10.10.2: 56 data bytes, press CTRL_C to break
    Reply from 10.10.10.2: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from 10.10.10.2: bytes=56 Sequence=2 ttl=255 time=1 ms
```

```
Reply from 10.10.10.2: bytes=56 Sequence=3 ttl=255 time=1 ms
Reply from 10.10.10.2: bytes=56 Sequence=4 ttl=255 time=1 ms
Reply from 10.10.10.2: bytes=56 Sequence=5 ttl=255 time=1 ms

--- 10.10.10.2 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 1/1/1 ms

HRP_M[FW1-policy-security]default action deny
Warning: Setting the default interzone packet filtering to deny may affect actual data traffic. You are
advised to configure the security policy based on the actual services. Are you sure you want to continue?
Please select [Y/N]:y
HRP_M[FW1-policy-security]quit
HRP_M[FW1]
```

```
HRP_M[FW2]interface Eth-Trunk 0
HRP_M[FW2-Eth-Trunk0]service-manage ping permit
HRP_M[FW2-Eth-Trunk0]quit
HRP_M[FW2]security-policy
HRP_M[FW2-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
HRP_M[FW2-policy-security]ping 10.10.10.1
  PING 10.10.10.1: 56 data bytes, press CTRL_C to break
    Reply from 10.10.10.1: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from 10.10.10.1: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 10.10.10.1: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 10.10.10.1: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 10.10.10.1: bytes=56 Sequence=5 ttl=255 time=1 ms

--- 10.10.10.1 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 1/1/1 ms

HRP_M[FW2-policy-security] default action deny
Warning: Setting the default interzone packet filtering to deny may affect actual data traffic. You are
advised to configure the security policy based on the actual services. Are you sure you want to continue?
Please select [Y/N]:y
HRP_M[FW2-policy-security]quit
HRP_M[FW2]
```

由以上信息可以发现，两台 FW 设备之间的心跳接口是路由可达的，但双机热备系统目前依旧是双主状态，需要继续排查 HRP 心跳接口配置及 HRP 认证密钥配置。

```
HRP_M[FW1]dis cu | in hrp interface
hrp interface Eth-Trunk0 remote 10.10.10.2
HRP_M[FW1]dis cu | in hrp au
HRP_M[FW1]dis cu | in hrp authentication
hrp authentication-key %+%######!"!!#!!*!!7LTnVOK_g:3WLNlJ!At9l-
8AQDlO/OF64j/!!!!2jp5!!!!<!!!!9ZHQAzXvyO=m7w<ZR@2R#@f~>J_}00H_AV+!!!!%+%#
```

```
HRP_M[FW2]dis cu | in hrp interface
hrp interface Eth-Trunk0 remote 10.10.10.1
HRP_M[FW2]dis cu | in hrp authentication
hrp authentication-
key %+%######!"!!#!!*!!7LTnVOK_g:f@Bf)^Pq]7$fDN<NmsWRfh8IU!!!!2jp5!!!!;!!!!Y42dJU3ENCd\{c0
nT509/3jbQJE+0/rX77!!!!%+%#
HRP_M[FW2]
```

由以上信息可以发现，两台 FW 设备的心跳接口相关配置无误，但 HRP 认证密钥显示出来的散列字符串并不一致，由此可以推断出两台 FW 设备的 HRP 认证密钥不一致，需要为两台 FW 设备重新配置 HRP 认证密钥，此处统一设置为“Huawei@123”。

```
HRP_M[FW1]hrp authentication-key Huawei@123
Warning: This command affects the setup of the hot standby connection. A hot standby connection can
be set up only when the configurations on both ends are consistent. Continue?Please select [Y/N]:y
HRP_M[FW1]
```

```
HRP_M[FW2]hrp authentication-key Huawei@123
Warning: This command affects the setup of the hot standby connection. A hot standby connection can
be set up only when the configurations on both ends are consistent. Continue?Please select [Y/N]:y
HRP_M[FW2]
```

完成上述配置后，可以发现 FW2 设备的 HRP 系统提示已经变更为备份设备，再检查两台设备 HRP 状态。

```
HRP_M[FW1]display hrp state
Local role: Active, Peer role: Standby
Local priority: 0:2, Peer priority: 0:2
Connection state: succeeded
Stable time: 0 day, 0 hour, 1 minute
Last state change information: 20**-02-25 09:14:48 The HRP core state changed due to "Local priority
changed". (old_state=standby, new_state=active, local_fault_indicator=0, local_robustness_indicator=2,
peer_fault_indicator=0, peer_robustness_indicator=2)
HRP_M[FW1]
```

```
HRP_S[FW2]display hrp state
Local role: Standby, Peer role: Active
Local priority: 0:2, Peer priority: 0:2
Connection state: succeeded
Stable time: 0 day, 0 hour, 2 minutes
```



```
Last state change information: 20**-02-25 09:16:56 The HRP core state changed due to "Peer priority changed". (old_state=active, new_state=standby, local_fault_indicator=0, local_robustness_indicator=2, peer_fault_indicator=0, peer_robustness_indicator=2)
HRP_S[FW2]
```

由以上信息可以发现两台 FW 设备的 HRP 状态已正常，至此双机热备故障排除实验完成。

2.3 配置参考

2.3.1 RT1 配置

```
#
sysname RT1
#
acl number 3500
 rule 5 permit ip
#
bfd
#
interface GigabitEthernet0/0/1
 undo portswitch
#
interface GigabitEthernet0/0/1.2
 dot1q termination vid 2
 ip address 4.4.4.2 255.255.255.252
 nat outbound 3500
#
interface GigabitEthernet0/0/2
 undo portswitch
 ip address 10.1.1.1 255.255.255.252
 ospf enable 1 area 0.0.0.0
#
interface GigabitEthernet0/0/4
 undo portswitch
 ip address 10.3.1.1 255.255.255.252
 ospf enable 1 area 0.0.0.0
#
interface LoopBack0
 ip address 33.33.33.1 255.255.255.255
#
bfd 1 bind peer-ip 10.3.1.2 source-ip 4.4.4.2
 discriminator local 10
 discriminator remote 20
 commit
#
ospf 1 router-id 33.33.33.1
 default-route-advertise always
```

```
area 0.0.0.0
#
ip route-static 0.0.0.0 0.0.0.0 4.4.4.1
#
return
```

2.3.2 RT2 配置

```
#
 sysname RT2
#
acl number 3500
 rule 5 permit ip
#
interface GigabitEthernet0/0/1
 undo portswitch
#
interface GigabitEthernet0/0/1.40
 dot1q termination vid 40
 ip address 3.3.3.2 255.255.255.252
 nat outbound 3500
#
interface GigabitEthernet0/0/2
 undo portswitch
 ip address 10.1.1.2 255.255.255.252
 ospf enable 1 area 0.0.0.0
#
interface GigabitEthernet0/0/4
 undo portswitch
 ip address 10.6.1.1 255.255.255.252
 ospf enable 1 area 0.0.0.0
#
interface LoopBack0
 ip address 44.44.44.1 255.255.255.255
#
ospf 1 router-id 44.44.44.1
 default-route-advertise always
 area 0.0.0.0
#
ip route-static 0.0.0.0 0.0.0.0 3.3.3.1
#
return
```

2.3.3 FW1 配置

```
#
sysname FW1
#
```

```
undo firewall packet-filter basic-protocol enable
#
hrp enable
hrp device active
hrp standby config enable
hrp mirror session enable
hrp interface Eth-Trunk0 remote 10.10.10.2
hrp track bfd-session 20
hrp track interface GE0/0/2
hrp authentication-key Huawei@123
#
bfd
#
interface Eth-Trunk0
 ip address 10.10.10.1 255.255.255.0
#
interface G0/0/2
 undo shutdown
 ip address 10.3.1.2 255.255.255.252
 ospf enable 1 area 0.0.0.0
#
interface G0/0/3
 undo shutdown
 eth-trunk 0
#
interface G0/0/4
 undo shutdown
 eth-trunk 0
#
interface G0/0/5
 undo shutdown
 ip address 172.16.30.2 255.255.255.0
 vrrp vrid 2 virtual-ip 172.16.30.1 active
 ospf enable 1 area 0.0.0.0
#
interface G0/0/6
 undo shutdown
 ip address 172.16.20.2 255.255.255.0
 vrrp vrid 1 virtual-ip 172.16.20.1 active
 ospf enable 1 area 0.0.0.0
#
interface LoopBack0
 ip address 11.11.11.1 255.255.255.255
#
firewall zone trust
 set priority 85
 add interface G0/0/5
 add interface G0/0/6
```

```
#
firewall zone untrust
  set priority 5
add interface G0/0/2
#
firewall zone dmz
  set priority 50
  add interface Eth-Trunk0
#
bfd 1 bind peer-ip 4.4.4.2 source-ip 10.3.1.2
  discriminator local 20
  discriminator remote 10
  commit
#
ospf 1 router-id 11.11.11.1
  area 0.0.0.0
#
security-policy
  rule name policy_sec1
    source-zone trust
    destination-zone untrust
    action permit
#
return
```

2.3.4 FW2 配置

```
#
sysname FW2
#
undo firewall packet-filter basic-protocol enable
#
hrp enable
hrp device standby
hrp standby config enable
hrp mirror session enable
hrp interface Eth-Trunk0 remote 10.10.10.1
hrp track interface GE0/0/2
hrp authentication-key Huawei@123
#
interface Eth-Trunk0
  ip address 10.10.10.2 255.255.255.0
#
interface G0/0/2
  undo shutdown
  ip address 10.6.1.2 255.255.255.252
  ospf enable 1 area 0.0.0.0
#
```

```
interface G0/0/3
 undo shutdown
 eth-trunk 0
#
interface G0/0/4
 undo shutdown
 eth-trunk 0
#
interface G0/0/5
 undo shutdown
 ip address 172.16.20.3 255.255.255.0
 vrrp vrid 2 virtual-ip 172.16.20.1 standby
 ospf enable 1 area 0.0.0.0
#
interface G0/0/6
 undo shutdown
 ip address 172.16.30.3 255.255.255.0
 vrrp vrid 2 virtual-ip 172.16.30.1 standby
 ospf enable 1 area 0.0.0.0
#
interface LoopBack0
 ip address 22.22.22.1 255.255.255.255
#
firewall zone trust
 set priority 85
 add interface G0/0/5
 add interface G0/0/6
#
firewall zone untrust
 set priority 5
 add interface G0/0/1
 add interface G0/0/2
#
firewall zone dmz
 set priority 50
 add interface Eth-Trunk0
#
ospf 1 router-id 22.22.22.1
 area 0.0.0.0
#
security-policy
 rule name policy_sec1
 source-zone trust
 destination-zone untrust
 action permit
#
return
```

2.3.5 SW1 预配置

```
#
sysname SW1
#
vlan batch 2 40
#
interface Vlanif2
 ip address 4.4.4.1 255.255.255.252
#
interface Vlanif40
 ip address 3.3.3.1 255.255.255.252
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 2 40
#
ip route-static 172.16.0.0 16 4.4.4.2
ip route-static 172.16.0.0 16 3.3.3.2 preference 70
#
return
```

2.3.6 SW2 预配置

```
#
sysname SW2
#
vlan batch 30
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 30
#
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 30
#
interface GigabitEthernet0/0/14
 port link-type access
 port default vlan 30
#
return
```

2.3.7 SW3 预配置

```
#
sysname SW3
#
```

```
vlan batch 40
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 40
#
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 40
#
interface GigabitEthernet0/0/13
 port link-type access
 port default vlan 40
#
return
```

2.3.8 Mirror-SW 预配置

```
#
sysname Mirror-SW
#
vlan batch 2 40
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 2 40
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 2 40
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 2 40
#
return
```

2.4 思考题

两台防火墙组件双机热备系统的设备系统要求是什么？

参考答案：

组成双机热备的两台设备的型号必须相同。两台设备的硬盘配置可以不同。例如，一台设备安装硬盘，另一台设备不安装硬盘，不会影响双机热备的运行。但未安装硬盘的设备日志存储量将远低于安装了硬盘的设备，而且部分日志功能不可用。

组成双机热备的两台设备的系统软件版本、系统补丁版本、特征库版本必须相同；对于 USG6700F 系列设备，HASH 选择 CPU 模式以及 HASH 因子建议相同，如果不相同，则主备切换的时候，可能会出现端口预分配、源 NAT 等业务受损情况。

3 防火墙虚拟系统实验

3.1 实验介绍

3.1.1 关于本实验

某大型企业分支机构使用防火墙作为网络出口（也即整体拓扑图中 FW3 设备），企业内部有研发部和市场部两个部门（分别用图中 PC4 和 PC5 模拟），现需要使用防火墙虚拟系统功能，将研发部与市场部的网络区分管理，实现部门与部门之间、部门到 Internet 之间访问权限的精细化管理，在满足业务需求的同时，保证网络的安全。

3.1.2 实验目的

- 学会创建虚拟系统并完成虚拟系统资源分配。
- 掌握虚拟系统到根系统之间的互通配置。
- 掌握虚拟系统到虚拟系统之间的互通配置。
- 实现企业内网研发部和市场部可以共用根系统同一个公网地址访问 Internet。

3.1.3 实验组网介绍

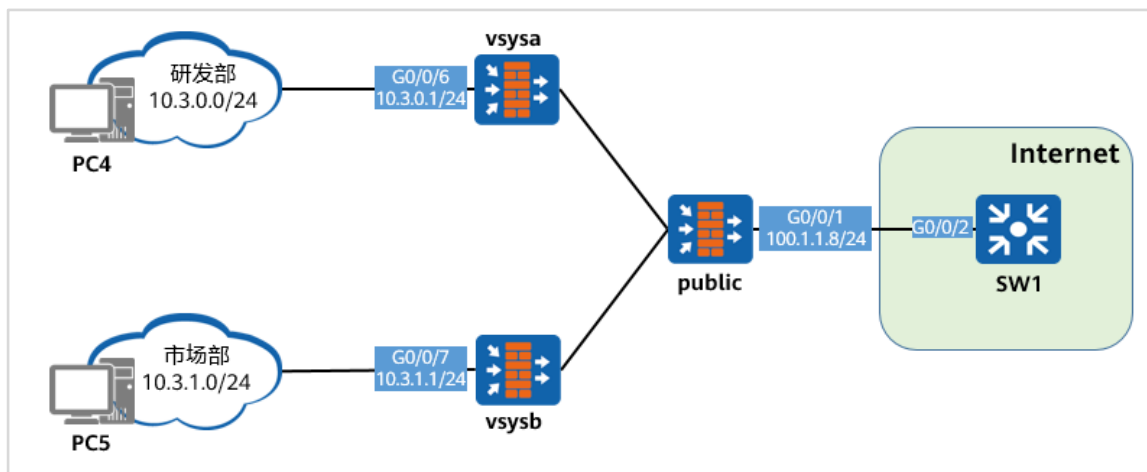


图3-1 防火墙虚拟系统实验拓扑图

在 FW3 上创建虚拟系统 vsysa 和 vsysb，GE0/0/6 属于虚拟系统 vsysa，GE0/0/7 属于虚拟系统 vsysb，GE0/0/1 属于防火墙 public。SW1 模拟 Internet，相关配置已预配，具体可参考“3.4 配置参考”。

3.1.4 实验规划

表3-1 设备接口规划表

设备	接口	接口性质	接口信息	说明
FW3	G0/0/1	三层接口	100.1.1.8/24 安全区域: Public/untrust	企业出接口, 连接Internet
	G0/0/6	三层接口	10.3.0.1/24 安全区域: vsysa/trust	虚拟系统vsysa的内联口
	G0/0/7	三层接口	10.3.1.1/24 安全区域: vsysb/trust	虚拟系统vsysb的内联口
	Virtual-if0	三层接口	172.16.0.1/24 安全区域: Public/trust	public防火墙的虚拟接口, 连接虚拟系统vsysa、vsysb
	Virtual-if1	三层接口	172.16.1.1/24 安全区域: vsysa/untrust	虚拟系统vsysa的虚拟接口, 连接public防火墙
	Virtual-if2	三层接口	172.16.2.1/24 安全区域: vsysb/untrust	虚拟系统vsysb的虚拟接口, 连接public防火墙
SW1	G0/0/2	Access	PVID: 1	连接防火墙
	VLANIF1	三层接口	100.1.1.1/24	模拟Internet, 公网地址
PC4	Ethernet0	网卡	10.3.0.100/24 网关: 10.3.0.1/24	终端
PC5	Ethernet0	网卡	10.3.1.100/24 网关: 10.3.1.1/24	终端

3.2 实验任务配置

3.2.1 配置思路

- 1.开启防火墙虚拟系统功能。
- 2.根据业务需求配置资源类, 并在根系统下创建虚拟系统 vsysa 和 vsysb, 为虚拟系统分配资源。
- 3.在根系统、虚拟系统 vsysa 和虚拟系统 vsysb 下分别配置接口, 并将接口加入安全区域。

- 4.在根系统、虚拟系统 vsysa 和虚拟系统 vsysb 下分别配置路由，对研发部和市场部下用户主机访问 Internet 的流量进行引流。
- 5.在根系统、虚拟系统 vsysa 和虚拟系统 vsysb 下根据业务需求分别配置安全策略，放行研发部中 10.3.0.100 ~ 10.3.0.110 和市场部下所有用户主机访问 Internet 的相关流量。
- 6.在根系统下配置源 NAT 策略，将从内网发往 Internet 的报文的源地址转换为根系统公网接口的 IP 地址。
- 7.在根系统为研发部与市场部互访的员工配置路由。

3.2.2 配置步骤 - CLI

步骤 1 网络基本参数配置

按照“表 3-1”数据规划，完成网络基本参数配置。其中 SW1 已经预配，具体可参考“3.4 配置参考”中 SW1 的预配。

```
[FW3]interface g0/0/1
[FW3-GE0/0/1]ip address 100.1.1.8 24
[FW3-GE0/0/1]quit
[FW3]firewall zone untrust
[FW3-zone-untrust]add interface g0/0/1
[FW3-zone-untrust]quit
[FW3]
```

其余业务接口在创建完虚拟系统后配置。

步骤 2 开启虚拟系统功能

开启虚拟系统。

```
[FW3] vsys enable
```

步骤 3 配置资源类

```
[FW3] resource-class r1
[FW3-resource-class-r1] resource-item-limit session reserved-number 10000 maximum 50000
[FW3-resource-class-r1] resource-item-limit policy reserved-number 300
[FW3-resource-class-r1] resource-item-limit bandwidth 20 entire
[FW3-resource-class-r1] quit
```

步骤 4 创建虚拟系统

创建虚拟系统 vsysa，并为其分配资源。

```
[FW3] vsys name vsysa
[FW3-vsys-vsysa] assign resource-class r1
[FW3-vsys-vsysa] assign interface G0/0/6
Warning: All configurations related to this interface will be removed. Continue?Please select [Y/N]:y
Info: All related configurations on this interface are removed.
[FW3-vsys-vsysa] quit
[FW3]
```

创建虚拟系统 vsysb，并为其分配资源。

```
[FW3]vsys name vsysb
[FW3-vsys-vsysb]assign resource-class r1
[FW3-vsys-vsysb]assign interface G0/0/7
Warning: All configurations related to this interface will be removed. Continue?Please select [Y/N]:y
Info: All related configurations on this interface are removed.
[FW3-vsys-vsysb]quit
[FW3]
```

步骤 5 根系统业务接口配置

```
[FW3] firewall zone trust
[FW3-zone-trust] add interface Virtual-if 0
[FW3-zone-trust] quit
[FW3]
```

步骤 6 根系统路由配置

配置根系统到 Internet 的路由，对研发部与市场部下的用户主机访问 Internet 的流量进行引流。

```
[FW3] ip route-static 0.0.0.0 0.0.0.0 100.1.1.1
```

步骤 7 根系统安全策略配置

配置根系统下的安全策略，放行研发部与市场部中的用户主机访问 Internet 的流量。

```
[FW3] security-policy
[FW3-policy-security] rule name trust_to_untrust
[FW3-policy-security-rule-trust_to_untrust] source-zone trust
[FW3-policy-security-rule-trust_to_untrust] destination-zone untrust
[FW3-policy-security-rule-trust_to_untrust] source-address 10.3.0.0 24
[FW3-policy-security-rule-trust_to_untrust] source-address 10.3.1.0 24
[FW3-policy-security-rule-trust_to_untrust] action permit
[FW3-policy-security-rule-trust_to_untrust] quit
[FW3-policy-security] quit
```

步骤 8 根系统 NAT 配置

配置根系统下的源 NAT 策略，将从研发部与市场部发往 Internet 的报文的源地址转换为根系统下的公网接口 GE0/0/1 的 IP 地址。

```
[FW3] nat-policy
[FW3-policy-nat] rule name nat1
[FW3-policy-nat-rule-nat1] source-zone trust
[FW3-policy-nat-rule-nat1] egress-interface G0/0/1
[FW3-policy-nat-rule-nat1] source-address 10.3.0.0 24
[FW3-policy-nat-rule-nat1] source-address 10.3.1.0 24
[FW3-policy-nat-rule-nat1] action source-nat easy-ip
[FW3-policy-nat-rule-nat1] quit
[FW3-policy-nat] quit
```

```
[FW3]
```

步骤 9 虚拟系统 vsysa 配置

配置虚拟系统 vsysa 下的接口 IP 并将其加入安全区域。

```
[FW3]switch vsys vsysa
<FW3-vsysa> system-view
[FW3-vsysa]interface G0/0/6
[FW3-vsysa-GE0/0/6] ip address 10.3.0.1 255.255.255.0
[FW3-vsysa-GE0/0/6]quit
[FW3-vsysa]firewall zone trust
[FW3-vsysa-zone-trust] add interface G0/0/6
[FW3-vsysa-zone-trust] quit
[FW3-vsysa]firewall zone untrust
[FW3-vsysa-zone-untrust] add interface Virtual-if1
[FW3-vsysa-zone-untrust] quit
[FW3-vsysa]
```

配置虚拟系统 vsysa 到根系统的路由，将研发部中的用户主机访问 Internet 的流量引入根系统。

```
[FW3-vsysa] ip route-static 0.0.0.0 0.0.0.0 public
```

配置虚拟系统 vsysa 下的安全策略，允许研发部中 10.3.0.100~10.3.0.110 网段的用户主机访问 Internet。

```
[FW3-vsysa] security-policy
[FW3-vsysa-policy-security] rule name to_internet_allow
[FW3-vsysa-policy-security-rule-to_internet_allow] source-zone trust
[FW3-vsysa-policy-security-rule-to_internet_allow] destination-zone untrust
[FW3-vsysa-policy-security-rule-to_internet_allow] source-address range 10.3.0.100 10.3.0.110
[FW3-vsysa-policy-security-rule-to_internet_allow] action permit
[FW3-vsysa-policy-security-rule-to_internet_allow] quit
[FW3-vsysa-policy-security]quit
[FW3-vsysa]
```

配置虚拟系统 vsysa 下的安全策略，允许研发部中所有用户主机访问市场部用户主机。

```
[FW3-vsysa]security-policy
[FW3-vsysa-policy-security]rule name to_market_allow
[FW3-vsysa-policy-security-rule-to_market_allow]source-zone trust
[FW3-vsysa-policy-security-rule-to_market_allow]destination-zone untrust
[FW3-vsysa-policy-security-rule-to_market_allow]destination-address 10.3.1.0 24
[FW3-vsysa-policy-security-rule-to_market_allow]action permit
[FW3-vsysa-policy-security-rule-to_market_allow]quit
[FW3-vsysa-policy-security]quit
[FW3-vsysa]
```

步骤 10 虚拟系统 vsysb 配置

配置虚拟系统 vsysb 下的接口 IP 并将其加入安全区域。

```
[FW3-vsysa]quit
<FW3-vsysa>quit
[FW3]switch vsys vsysb
<FW3-vsymb>system-view
[FW3-vsymb]interface GE0/0/7
[FW3-vsymb-GE0/0/7] ip address 10.3.1.1 255.255.255.0
[FW3-vsymb-GE0/0/7] quit
[FW3-vsymb]firewall zone trust
[FW3-vsymb-zone-trust] add interface GE0/0/7
[FW3-vsymb-zone-trust] quit
[FW3-vsymb]firewall zone untrust
[FW3-vsymb-zone-untrust]add interface Virtual-if2
[FW3-vsymb-zone-untrust]quit
[FW3-vsymb]
```

配置虚拟系统 vsymb 到根系统的路由，将市场部中的用户主机访问 Internet 的流量引入根系统。

```
[FW3-vsymb] ip route-static 0.0.0.0 0.0.0.0 public
```

配置虚拟系统 vsymb 下的安全策略，允许市场部的所有用户主机访问 Internet。

```
[FW3-vsymb]security-policy
[FW3-vsymb-policy-security]rule name to_internet_allow
[FW3-vsymb-policy-security-rule-to_internet_allow]source-zone trust
[FW3-vsymb-policy-security-rule-to_internet_allow]destination-zone untrust
[FW3-vsymb-policy-security-rule-to_internet_allow]action permit
[FW3-vsymb-policy-security-rule-to_internet_allow]quit
[FW3-vsymb-policy-security]quit
[FW3-vsymb]
```

步骤 11 虚拟系统互访配置

在根系统为研发部与市场部互访的员工配置路由，配置虚拟系统 vsysa、vsymb 的安全策略，使研发部与市场部员工可以相互访问。

```
[FW3-vsymb] quit
<FW3-vsymb> quit
[FW3] ip route-static vpn-instance vsymb 10.3.0.0 255.255.255.0 vpn-instance vsysa
[FW3] ip route-static vpn-instance vsysa 10.3.1.0 255.255.255.0 vpn-instance vsymb
```

进入虚拟系统 vsysa 配置安全策略，允许虚拟系统 vsymb 的主机访问虚拟系统 vsysa 的主机。

```
[FW3]switch vsys vsysa
<FW3-vsysa>system-view
[FW3-vsysa] security-policy
[FW3-vsysa-policy-security]rule name vsymb_to_vsysa
[FW3-vsysa-policy-security-rule-vsymb_to_vsysa] source-zone untrust
[FW3-vsysa-policy-security-rule-vsymb_to_vsysa] destination-zone trust
[FW3-vsysa-policy-security-rule-vsymb_to_vsysa] source-address 10.3.1.0 24
[FW3-vsysa-policy-security-rule-vsymb_to_vsysa] destination-address 10.3.0.0 24
```

```
[FW3-vsypa-policy-security-rule-vsypb_to_vsypa] action permit
[FW3-vsypa-policy-security-rule-vsypb_to_vsypa] quit
[FW3-vsypa-policy-security]quit
[FW3-vsypa]
```

进入虚拟系统 vsypb 配置安全策略，允许虚拟系统 vsypa 的主机访问虚拟系统 vsypb 的主机。

```
[FW3]switch vsys vsypb
<FW3-vsypb>system-view
[FW3-vsypb]security-policy
[FW3-vsypb-policy-security] rule name vsypa_to_vsypb
[FW3-vsypb-policy-security-rule-vsypa_to_vsypb]source-zone untrust
[FW3-vsypb-policy-security-rule-vsypa_to_vsypb]destination-zone trust
[FW3-vsypb-policy-security-rule-vsypa_to_vsypb]source-address 10.3.0.0 24
[FW3-vsypb-policy-security-rule-vsypa_to_vsypb]destination-address 10.3.1.0 24
[FW3-vsypb-policy-security-rule-vsypa_to_vsypb]action permit
[FW3-vsypb-policy-security-rule-vsypa_to_vsypb]quit
[FW3-vsypb-policy-security] quit
[FW3-vsypb]
```

3.2.3 配置步骤 - Web

步骤 1 开启虚拟系统功能

登录 FW3 设备 Web 管理界面，选择“系统 > 虚拟系统 > 虚拟系统”，执行以下操作，启用虚拟系统功能。



图3-2 FW3 启用虚拟系统功能

步骤 2 配置资源类

在 FW3 设备 Web 管理界面选择“系统 > 虚拟系统 > 资源类”，单击“新建”执行以下操作。

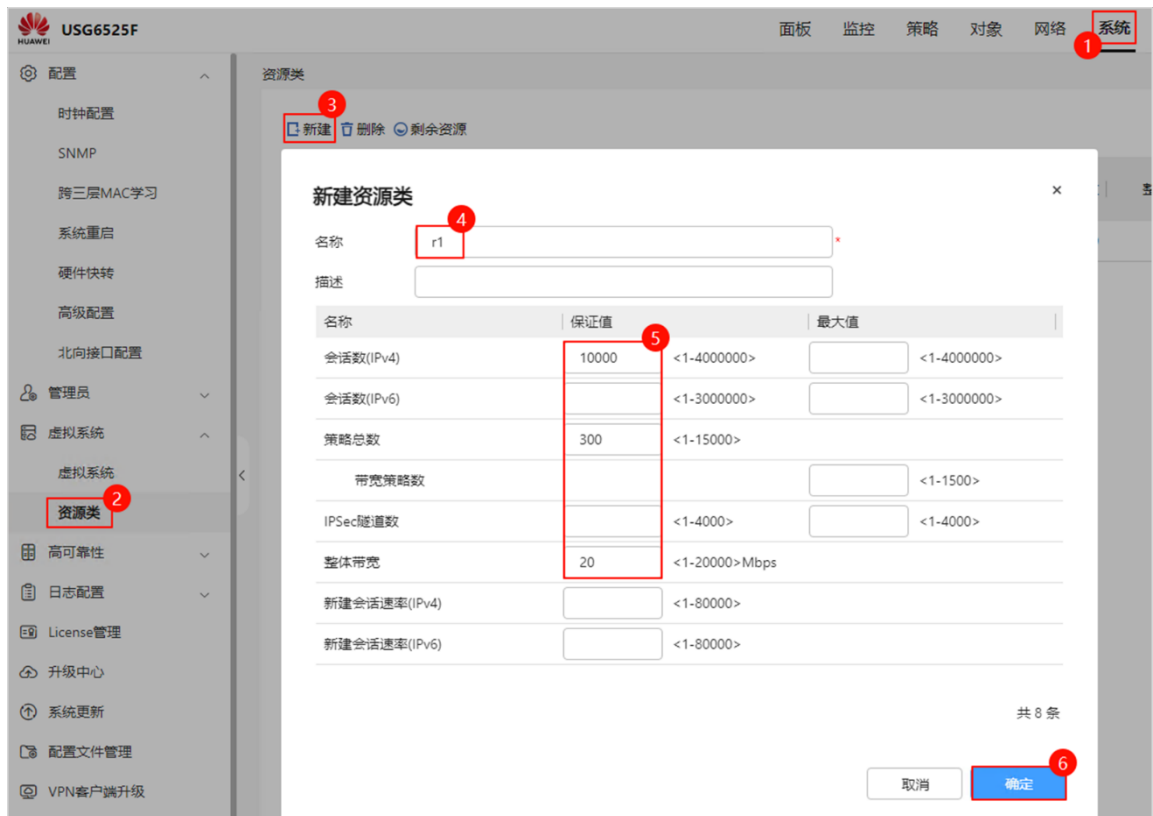


图3-3 创建虚拟系统资源类

步骤 3 创建虚拟系统

在 FW3 设备 Web 管理界面选择“系统 > 虚拟系统 > 虚拟系统”，在虚拟系统列表界面内单击“新建”，执行以下操作。



图3-4 创建虚拟系统 vsysa (1)



图3-5 创建虚拟系统 vsysa (2)

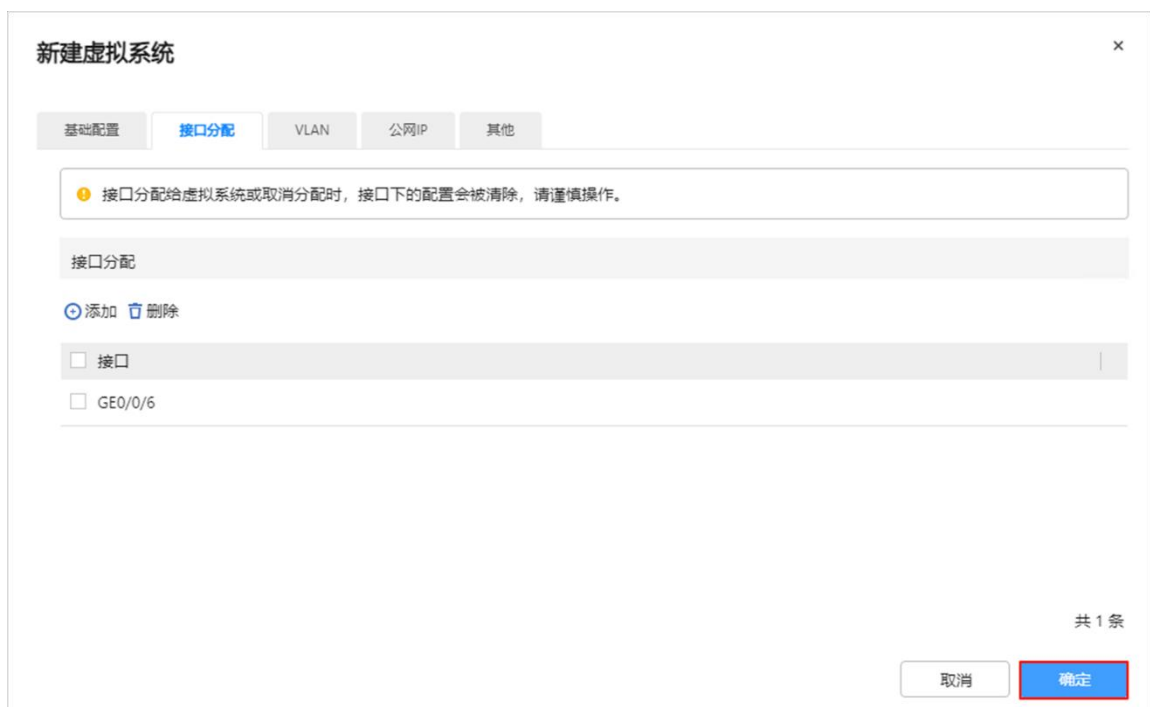


图3-6 创建虚拟系统 vsysa (3)



图3-7 创建虚拟系统 vsysb (1)

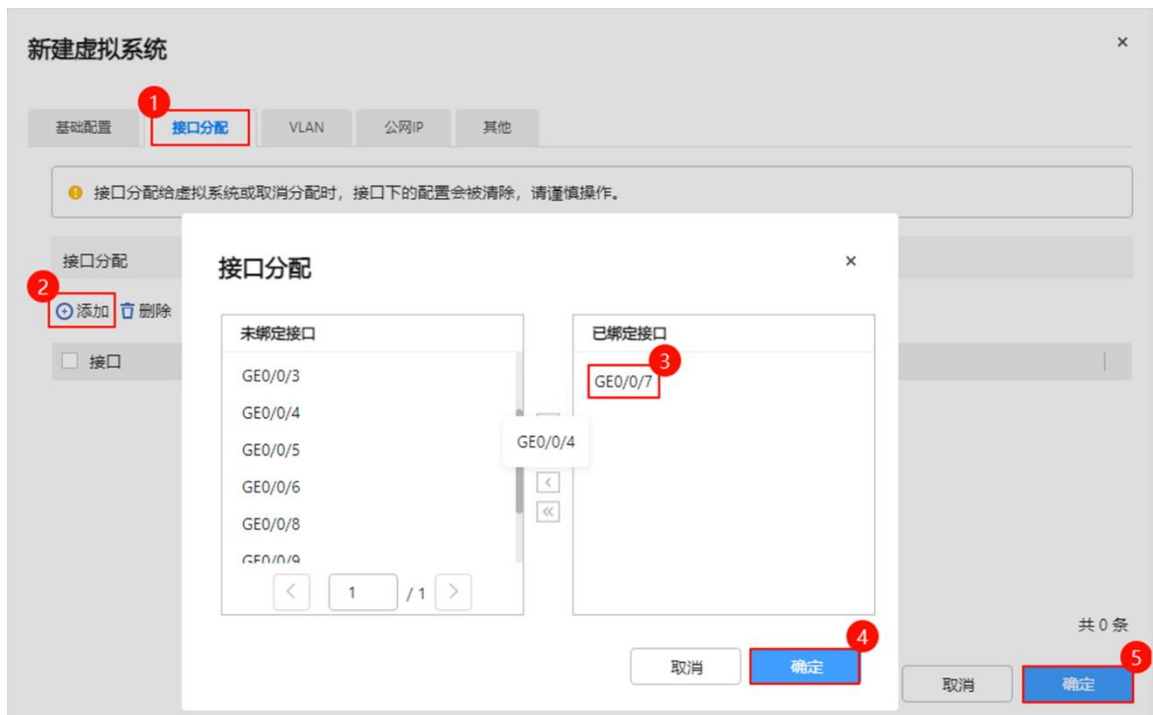


图3-8 创建虚拟系统 vsysb (2)

步骤 4 根系统业务接口配置

在根系统下配置业务接口 IP 地址，并将其加入安全区域。

在 FW3 设备 Web 管理界面选择“网络 > 接口”，进入接口列表界面，执行以下操作：

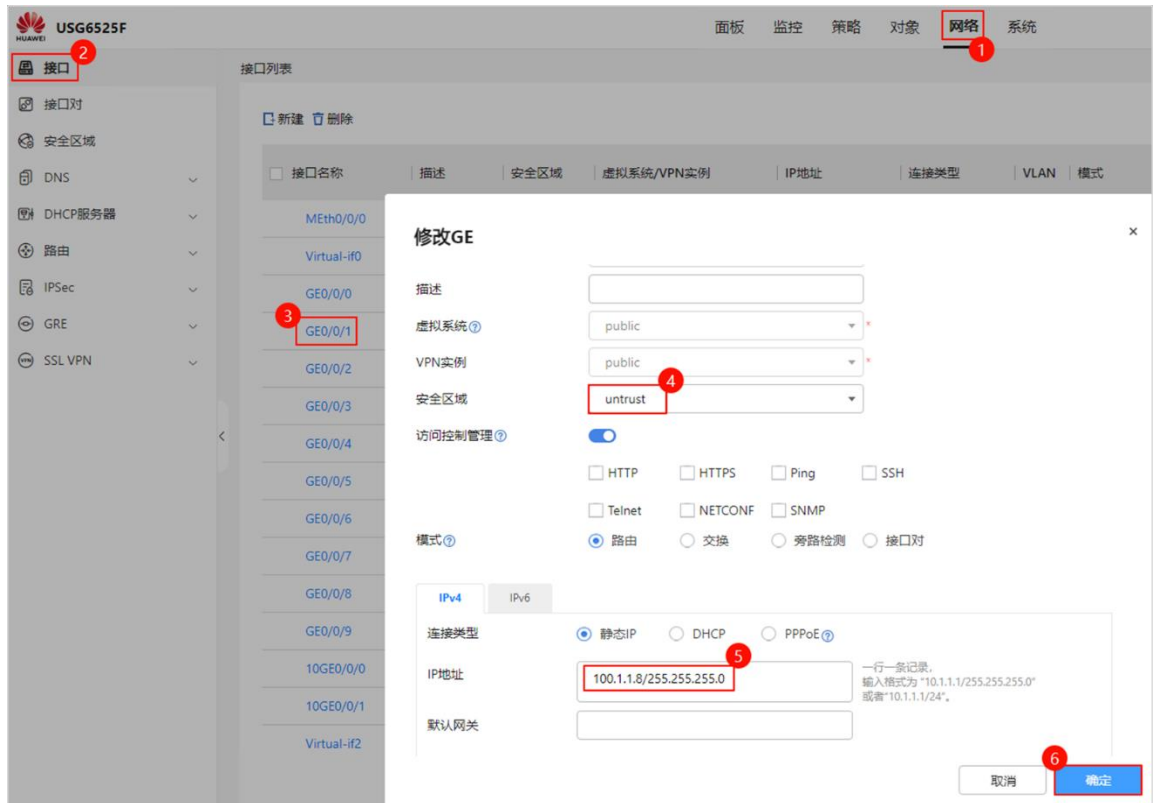


图3-9 根系统 GE0/0/1 接口配置

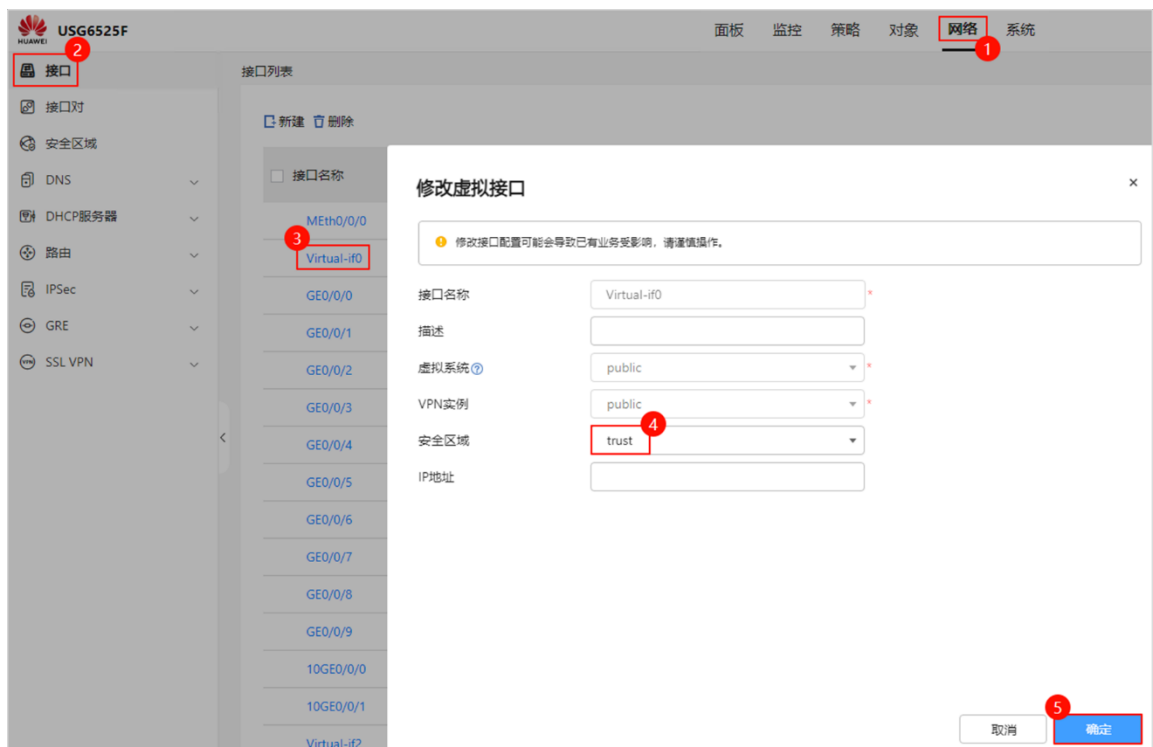


图3-10 根系统 Virtual-if0 接口配置

步骤 5 配置根系统访问 Internet 的路由

在 FW3 设备 Web 管理界面选择“网络 > 路由 > 静态路由”，单击“新建”，执行以下操作，配置根系统访问 Internet 的路由。

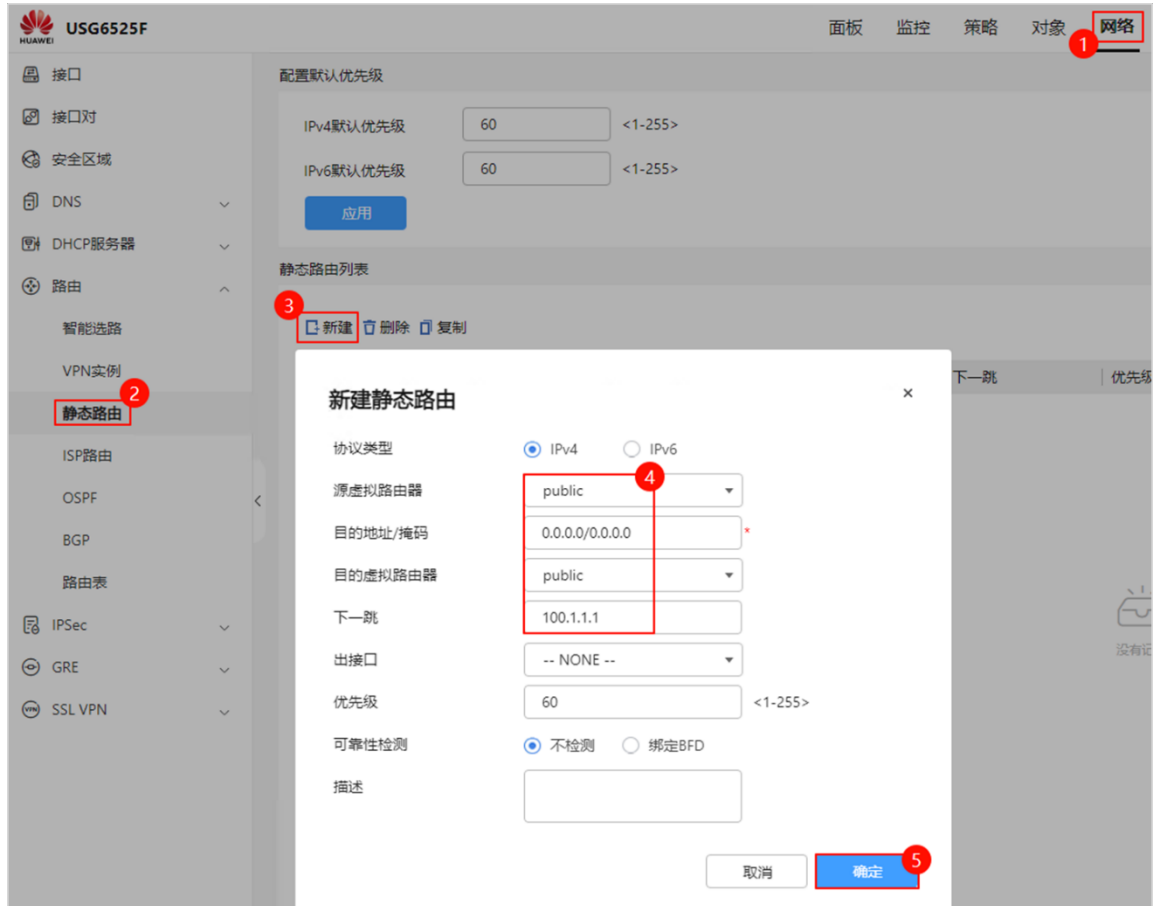


图3-11 配置根系统访问 Internet 的路由

步骤 6 配置根系统安全策略

在 FW3 设备 Web 管理界面选择“策略 > 安全策略 > 安全策略”，单击“新建安全策略”，执行以下操作，放行研发部与市场部中的用户主机访问 Internet 的流量。

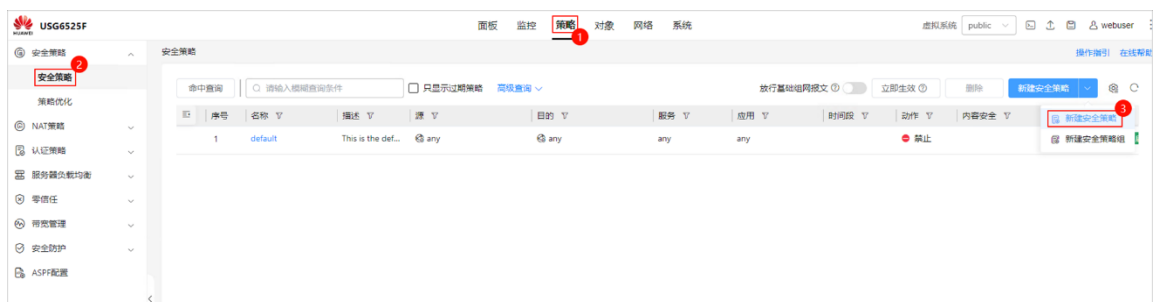


图3-12 进入根系统安全策略配置界面



图3-13 配置根系统安全策略放行内网用户访问 Internet 的流量

步骤 7 配置根系统源 NAT 策略

在 FW3 设备 Web 管理界面选择“策略 > NAT 策略 > NAT 策略”，执行以下操作配置源 NAT 策略，将从研发部与市场部发往 Internet 的报文的源地址转换为根系统下的公网接口 GE0/0/1 的 IP 地址。



图3-14 进入 NAT 策略配置界面

新建NAT策略

×

功能介绍

名称nat1

描述

NAT类型☒ NAT ☐ NAT64 ☐ NAT66

转换模式仅转换源地址

时间段请选择时间段

原始数据包

源安全区域trust

目的类型☐ 目的安全区域 ☒ 出接口

GEO/0/1

源地址10.3.0.0/24 × 10.3.1.0/24 ×

目的地址请选择或输入地址

服务请选择或输入服务

转换后的数据包

源地址转换为☐ 地址池中的地址 ☒ 出接口地址

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3-15 配置源 NAT 策略

步骤 8 虚拟系统 vsysa 配置

在 FW3 设备 Web 管理界面右上角的“虚拟系统”下拉菜单中选择“vsysa”，进入 vsysa 虚拟系统。



图3-16 进入 vsysa 虚拟系统

在 vsysa 虚拟系统 Web 管理界面选择“网络 > 接口”，执行以下操作，完成 vsysa 系统内业务接口的基础配置：

说明：虚拟系统配套的虚拟接口（Virtual-if）的编号并非固定，可能会因多次删除和创建虚拟系统导致虚拟接口（Virtual-if）编号错乱，实际操作时，以虚拟系统实际产生的虚拟接口编号为准。



图3-17 vsysa 系统 GE0/0/6 接口配置

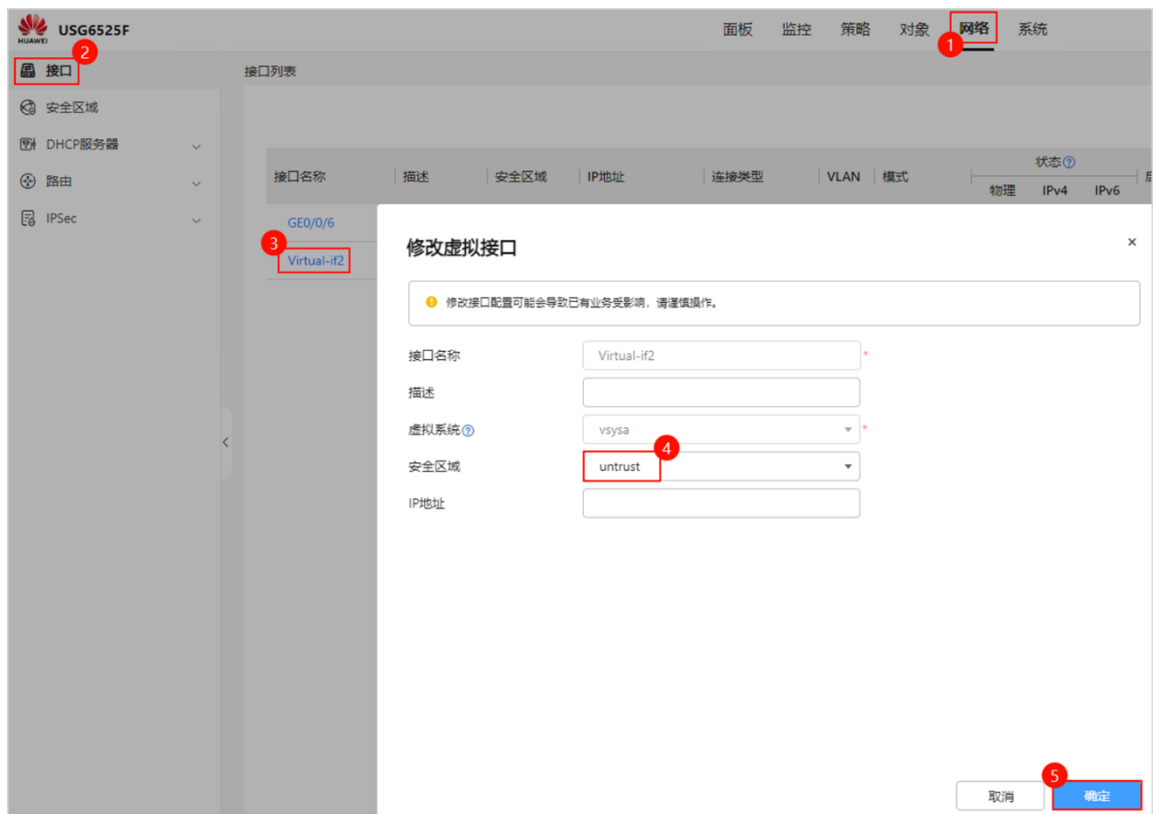


图3-18 vsysa 系统虚拟接口配置

完成接口基础配置后，继续在 vsysa 虚拟系统 Web 管理界面选择“网络 > 路由 > 静态路由”，单击“新建”，配置虚拟系统 vsysa 到根系统的路由，将研发部中的用户主机访问 Internet 的流量引入根系统。



图3-19 配置 vsysa 系统静态路由

在 vsysa 虚拟系统 Web 管理界面选择“策略 > 安全策略 > 安全策略”，单击“新建安全策略”，配置虚拟系统 vsysa 下的安全策略，允许研发部中 10.3.0.100~10.3.0.110 网段的用户主机访问 Internet；允许研发部中所有用户主机访问市场部用户主机。

新建安全策略

×

概述

* 名称

to_internet_allow

描述

策略组

-- NONE --

条件

ⓘ 当前未加载地区识别特征库。

源

安全区域

trust

地址/地区

10.3.0.100-1...

目的

10.3.0.100-10.3.0.110

目的类型

安全区域

虚拟服务

安全区域

untrust

地址/地区

any

服务

any

更多

应用/用户/安全组/时间段/VLAN ID

动作

3

允许

禁止

内容安全检查

反病毒/入侵防御/URL过滤/内容过滤/文件过滤/邮件过滤/DNS过滤

确定

命令预览

取消

图3-20 配置 vsysa 系统安全策略放行访问 Internet 的流量



新建安全策略

概述

* 名称: to_market_allow

描述:

策略组: -- NONE --

条件

当前未加载地区识别特征库。

源

安全区域: trust

地址/地区: 10.3.0.0/24

目的

目的类型: ☒ 安全区域 ☐ 虚拟服务

安全区域: untrust

地址/地区: 10.3.1.0/24

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: 反病毒/入侵防御/URL过滤/内容过滤/文件过滤/邮件过滤/DNS过滤

取消 命令预览 确定

图3-21 配置 vsysa 系统访问 vsysb 系统的流量

步骤 9 虚拟系统 vsysb 配置

在 FW3 设备 Web 管理界面右上角的“虚拟系统”下拉菜单中选择“vsysb”，进入 vsysb 虚拟系统。

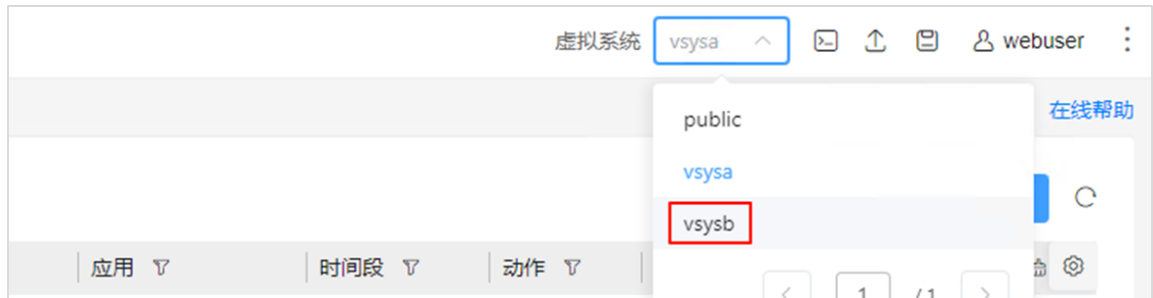


图3-22 进入 vsysb 虚拟系统

在 vsysb 虚拟系统 Web 管理界面选择“网络 > 接口”，执行以下操作，完成 vsysb 系统内业务接口的基础配置：

说明：虚拟系统配套的虚拟接口（Virtual-if）的编号并非固定，可能会因多次删除和创建虚拟系统导致虚拟接口（Virtual-if）编号错乱，实际操作时，以虚拟系统实际产生的虚拟接口编号为准。



图3-23 vsysb 系统 GE0/0/7 接口配置

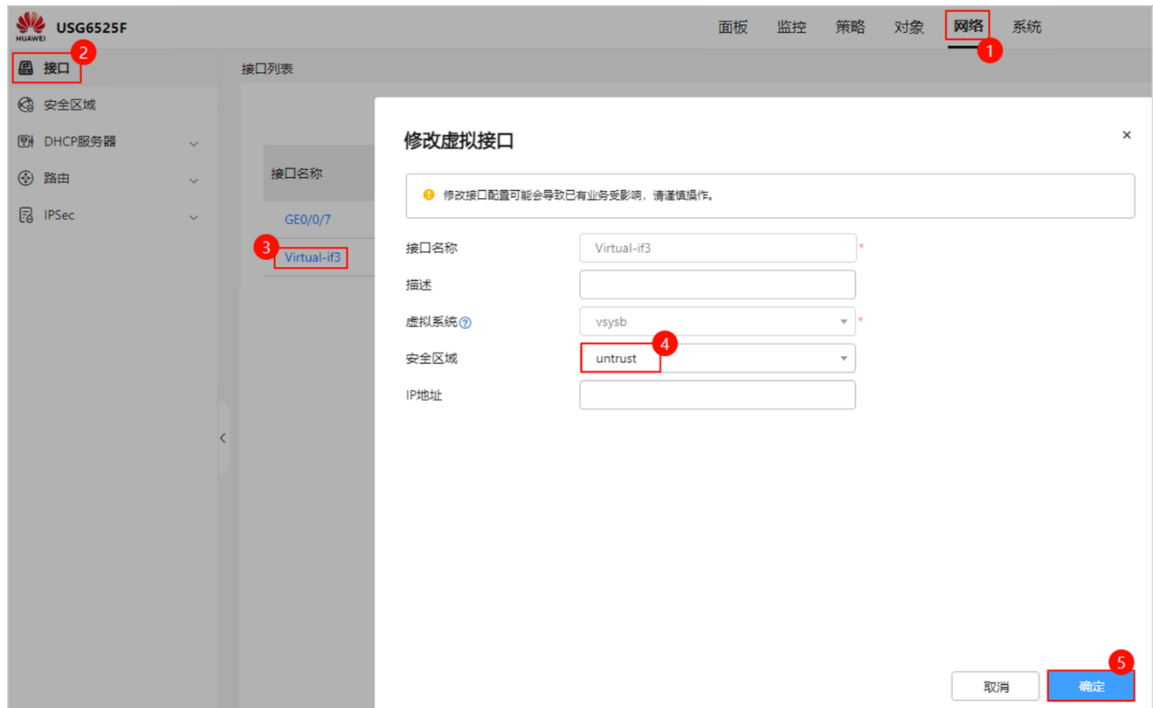


图3-24 vsysb 系统虚拟接口配置

完成接口基础配置后，继续在 vsysb 虚拟系统 Web 管理界面选择“网络 > 路由 > 静态路由”，单击“新建”，配置虚拟系统 vsysb 到根系统的路由，将研发部中的用户主机访问 Internet 的流量引入根系统。



图3-25 配置 vsysb 系统静态路由

在 vsysb 虚拟系统 Web 管理界面选择“策略 > 安全策略 > 安全策略”，单击“新建安全策略”，配置虚拟系统 vsysb 下的安全策略，允许市场部所有用户访问 Internet；允许市场部中所有用户访问研发部。



新建安全策略

概述

* 名称: to_internet_allow

描述:

策略组: -- NONE --

条件

当前未加载地区识别特征库。

源

安全区域: trust

地址/地区: 10.3.1.0/24

目的

目的类型: ☒ 安全区域 ☐ 虚拟服务

安全区域: untrust

地址/地区: any

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: 反病毒/入侵防御/URL过滤/内容过滤/文件过滤/邮件过滤/DNS过滤

取消 命令预览 确定

图3-26 配置 vsysb 系统安全策略放行访问 Internet 的流量

步骤 10 虚拟系统互访配置

在根系统为研发部与市场部互访配置静态路由；配置虚拟系统 vsysa、vsysb 的安全策略，使研发部与市场部员工可以相互访问。

在界面右上角的“虚拟系统”下拉菜单中选择“public”，进入根系统。

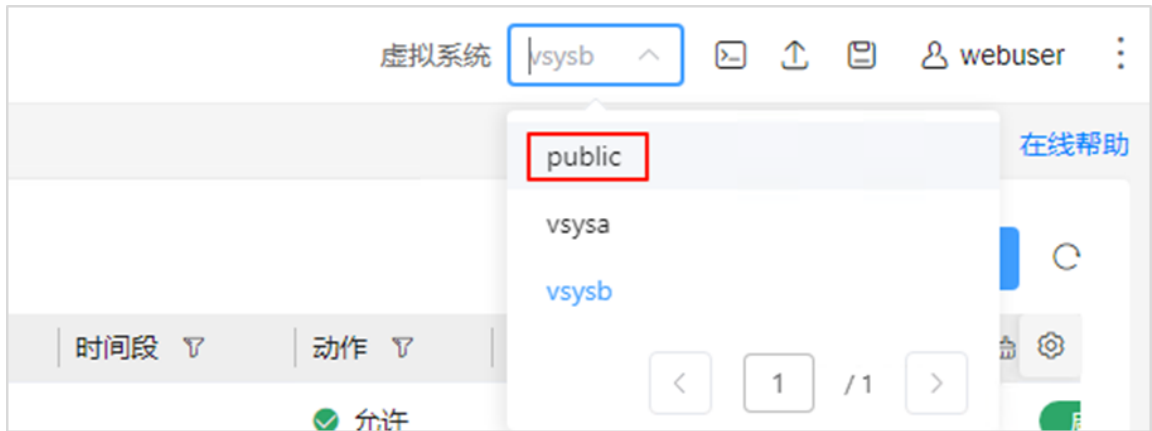


图3-27 进入 FW3 设备根系统

在根系统 Web 管理界面选择“网络 > 路由 > 静态路由”，单击“新建”，执行以下操作。

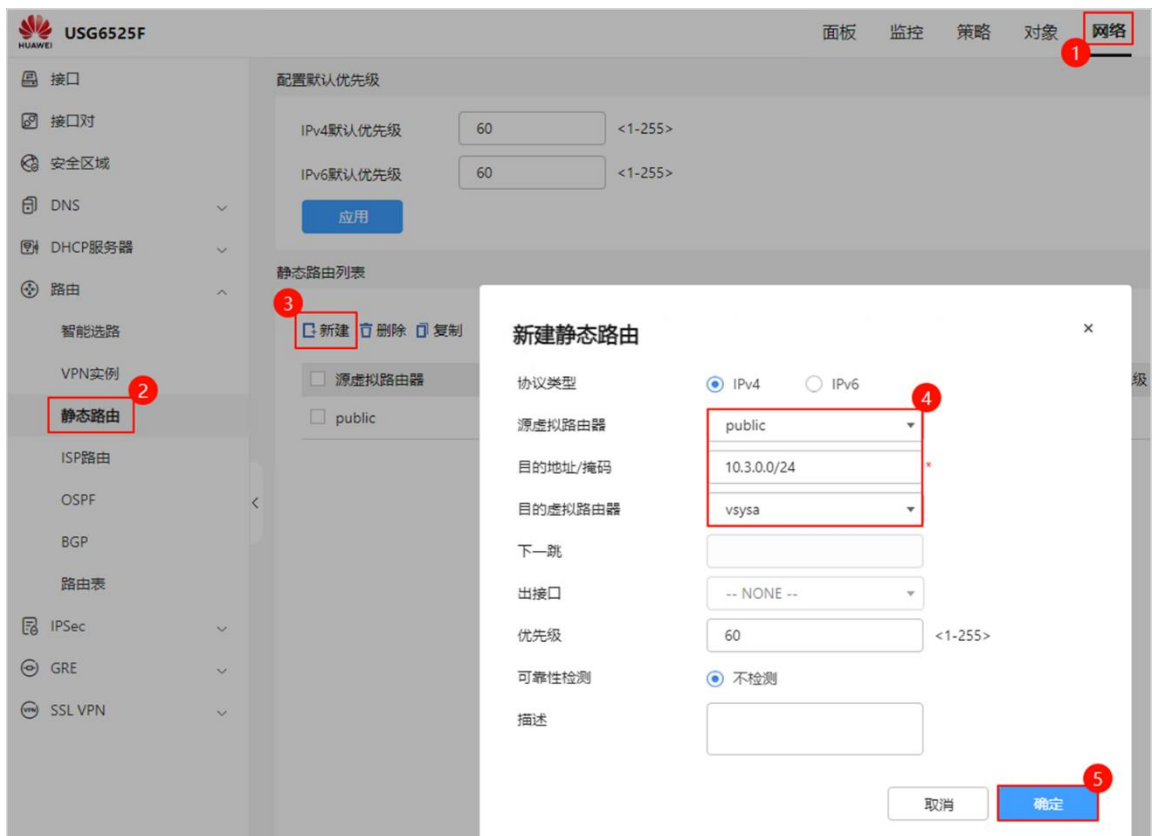


图3-28 配置根系统去往 vsysa 系统的静态路由

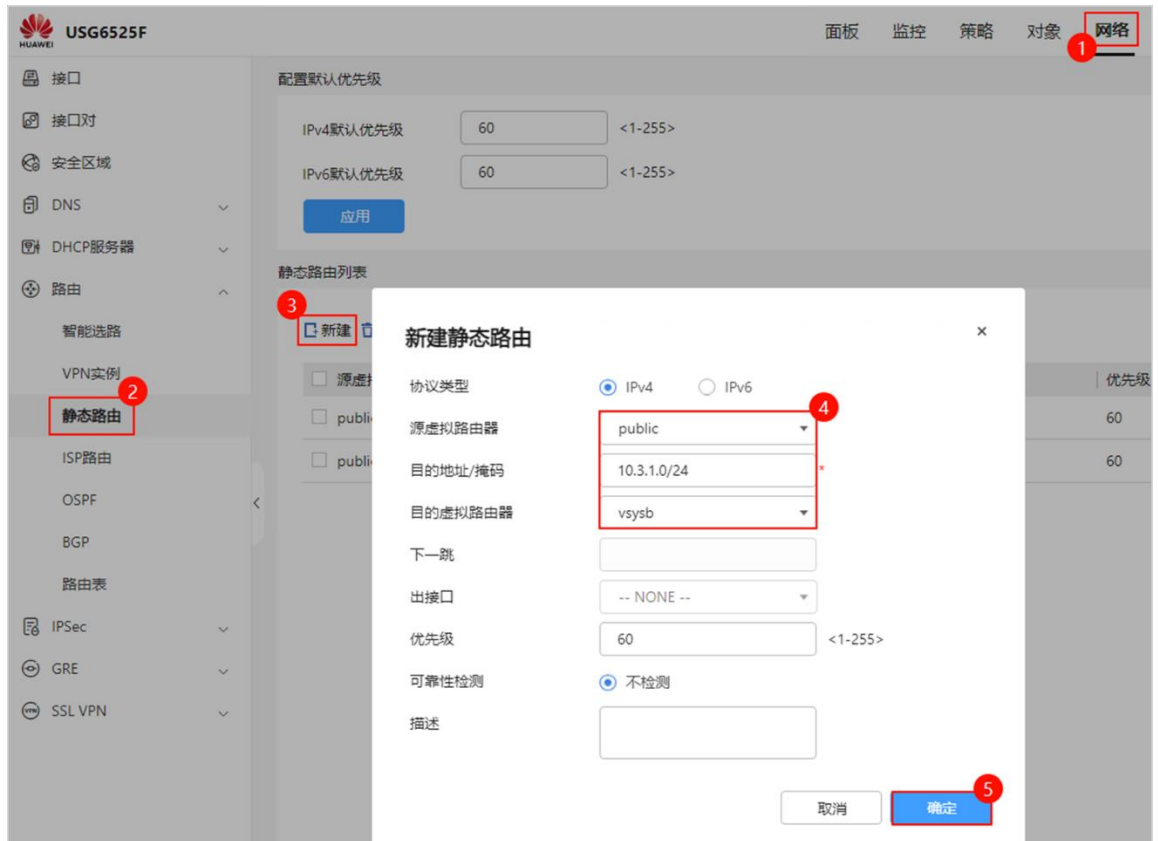


图3-29 配置根系统去往 vsysb 系统的静态路由

进入虚拟系统 vsysa 配置安全策略。允许虚拟系统 vsysb 主机访问虚拟系统 vsysa 主机。



图3-30 进入 vsysa 系统



新建安全策略

^ 概述

* 名称 b2a

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

地址/地区 ② 10.3.1.0/24

目的

目的类型 ☒ 安全区域 ☐ 虚拟服务

安全区域 trust

地址/地区 ② 10.3.0.0/24

服务 ②

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 反病毒/入侵防御/URL过滤/内容过滤/文件过滤/邮件过滤/DNS过滤

取消 命令预览 确定

图3-31 配置安全策略允许 vsysb 系统访问 vsysa 系统

进入虚拟系统 vsysb 配置安全策略。允许虚拟系统 vsysa 主机访问虚拟系统 vsysb 主机。



图3-32 进入 vsysb 系统

新建安全策略

^ 概述

* 名称
a2b

描述

策略组
-- NONE --

^ 条件

当前未加载地区识别特征库。

源

安全区域
untrust

地址/地区
10.3.0.0/24

目的

目的类型
安全区域 虚拟服务

安全区域
trust

地址/地区
10.3.1.0/24

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 反病毒/入侵防御/URL过滤/内容过滤/文件过滤/邮件过滤/DNS过滤

取消 命令预览 确定

图3-33 配置安全策略允许 vsysa 系统访问 vsysb 系统

3.3 结果验证

3.3.1 研发部业务测试

将研发部中的主机（PC4）业务网卡的 IP 地址配置为 10.3.0.100/24，网关设置为 10.3.0.1/24，测试到达 Internet（SW1 设备的 100.1.1.1 地址）的连通性，效果如下：

```
C:\Users\Security>ipconfig

Windows IP Configuration

Ethernet adapter mgmt:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::596b:4507:e712:6f11%13
    IPv4 Address. . . . . : 192.168.20.113
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.20.254

Ethernet adapter servcie:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::7de3:5163:7ca0:37a5%11
    IPv4 Address. . . . . : 10.3.0.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.3.0.1

Tunnel adapter isatap.{D8FCA672-EF4F-476C-97EB-C2BBF3906A5A}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Tunnel adapter isatap.{C67F2CCD-0648-4907-8C6A-E55B241DC2CC}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Users\Security>ping 100.1.1.1

Pinging 100.1.1.1 with 32 bytes of data:
Reply from 100.1.1.1: bytes=32 time=1ms TTL=253
Reply from 100.1.1.1: bytes=32 time=1ms TTL=253
Reply from 100.1.1.1: bytes=32 time<1ms TTL=253
Reply from 100.1.1.1: bytes=32 time<1ms TTL=253

Ping statistics for 100.1.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Security>
```

图3-34 研发部访问 Internet（允许的主机范围内）

将研发部中的主机（PC4）业务网卡的 IP 地址配置为 10.3.0.120/24，网关设置为 10.3.0.1/24，测试到达 Internet（SW1 设备的 100.1.1.1 地址）的连通性，效果如下：

```
C:\Users\Security>ipconfig

Windows IP Configuration

Ethernet adapter mgmt:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::596b:4507:e712:6f11%13
    IPv4 Address. . . . . : 192.168.20.113
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.20.254

Ethernet adapter servcie:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::7de3:5163:7ca0:37a5%11
    IPv4 Address. . . . . : 10.3.0.120
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.3.0.1

Tunnel adapter isatap.{D8FCA672-EF4F-476C-97EB-C2BBF3906A5A}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Tunnel adapter isatap.{C67F2CCD-0648-4907-8C6A-E55B241DC2CC}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Users\Security>ping 100.1.1.1

Pinging 100.1.1.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 100.1.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Security>_
```

图3-35 研发部访问 Internet（允许的主机范围外）

继续使用研发部主机（PC4）测试到达市场部主机（PC5）的连通性，效果如下：

```
C:\Users\Security>ipconfig

Windows IP Configuration

Ethernet adapter mgmt:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::596b:4507:e712:6f11%13
    IPv4 Address. . . . . : 192.168.20.113
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.20.254

Ethernet adapter servcie:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::7de3:5163:7ca0:37a5%11
    IPv4 Address. . . . . : 10.3.0.120
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.3.0.1

Tunnel adapter isatap.{D8FCA672-EF4F-476C-97EB-C2BBF3906A5A}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Tunnel adapter isatap.{C67F2CCD-0648-4907-8C6A-E55B241DC2CC}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Users\Security>ping 10.3.1.100

Pinging 10.3.1.100 with 32 bytes of data:
Reply from 10.3.1.100: bytes=32 time<1ms TTL=126
Reply from 10.3.1.100: bytes=32 time<1ms TTL=126
Reply from 10.3.1.100: bytes=32 time<1ms TTL=126
Reply from 10.3.1.100: bytes=32 time<1ms TTL=126

Ping statistics for 10.3.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

图3-36 研发部访问市场部

3.3.2 市场部业务测试

将市场部中的主机（PC5）业务网卡的 IP 地址修改为 10.3.1.100/24，网关设置为 10.3.1.1/24，测试到达 Internet（SW1 设备的 100.1.1.1 地址）的连通性，效果如下：

```
C:\Users\Security>ipconfig

Windows IP Configuration

Ethernet adapter mgmt:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::5079:59b5:fbf4:a16e%13
    IPv4 Address. . . . . : 192.168.20.114
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.20.254

Ethernet adapter service:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::7546:23ec:6f35:66c4%11
    IPv4 Address. . . . . : 10.3.1.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.3.1.1

Tunnel adapter isatap.{D8FCA672-EF4F-476C-97EB-C2BBF3906A5A}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Tunnel adapter isatap.{C67F2CCD-0648-4907-8C6A-E55B241DC2CC}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Users\Security>ping 100.1.1.1

Pinging 100.1.1.1 with 32 bytes of data:
Reply from 100.1.1.1: bytes=32 time=1ms TTL=253
Reply from 100.1.1.1: bytes=32 time=1ms TTL=253
Reply from 100.1.1.1: bytes=32 time=1ms TTL=253
Reply from 100.1.1.1: bytes=32 time<1ms TTL=253

Ping statistics for 100.1.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

图3-37 市场部访问 Internet

使用市场部主机（PC5）测试到达研发部主机（PC4）的连通性，效果如下：


```
C:\Users\Security>ipconfig

Windows IP Configuration

Ethernet adapter mgmt:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::5079:59b5:fbf4:a16e%13
    IPv4 Address. . . . . : 192.168.20.114
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.20.254

Ethernet adapter service:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::7546:23ec:6f35:66c4%11
    IPv4 Address. . . . . : 10.3.1.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.3.1.1

Tunnel adapter isatap.{D8FCA672-EF4F-476C-97EB-C2BBF3906A5A}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Tunnel adapter isatap.{C67F2CCD-0648-4907-8C6A-E55B241DC2CC}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Users\Security>ping 10.3.0.120

Pinging 10.3.0.120 with 32 bytes of data:
Reply from 10.3.0.120: bytes=32 time<1ms TTL=126
Reply from 10.3.0.120: bytes=32 time<1ms TTL=126
Reply from 10.3.0.120: bytes=32 time<1ms TTL=126
Reply from 10.3.0.120: bytes=32 time<1ms TTL=126

Ping statistics for 10.3.0.120:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

图3-38 市场部访问研发部

3.4 配置参考

3.4.1 FW3 配置

```
#
vsys enable
resource-class r1
  resource-item-limit session reserved-number 10000 maximum 50000
  resource-item-limit bandwidth 20 entire
  resource-item-limit policy reserved-number 300
#
vsys name vsysa 1
  assign interface GE0/0/6
  assign resource-class r1
#
vsys name vsysb 2
  assign interface GE0/0/7
  assign resource-class r1
#
ip vpn-instance default
  ipv4-family
#
ip vpn-instance vsysa
  ipv4-family
  ipv6-family
#
ip vpn-instance vsysb
  ipv4-family
  ipv6-family
#
#
interface GE0/0/1
  undo shutdown
  ip address 100.1.1.8 255.255.255.0
  service-manage http permit
  service-manage https permit
  service-manage ping permit
  service-manage ssh permit
  service-manage snmp permit
  service-manage telnet permit
  service-manage netconf permit
#
interface GE0/0/6
```

```
undo shutdown
ip binding vpn-instance vsysa
ip address 10.3.0.1 255.255.255.0
service-manage http permit
service-manage https permit
service-manage ping permit
service-manage ssh permit
service-manage telnet permit
#
interface GE0/0/7
undo shutdown
ip binding vpn-instance vsysb
ip address 10.3.1.1 255.255.255.0
service-manage http permit
service-manage https permit
service-manage ping permit
service-manage ssh permit
service-manage telnet permit
#
firewall zone local
set priority 100
#
firewall zone trust
set priority 85
add interface Virtual-if0
#
firewall zone untrust
set priority 5
add interface GE0/0/1
#
firewall zone dmz
set priority 50
#
ip route-static 0.0.0.0 0.0.0.0 100.1.1.1
ip route-static vpn-instance vsysa 10.3.1.0 255.255.255.0 vpn-instance vsysb
ip route-static vpn-instance vsysb 10.3.0.0 255.255.255.0 vpn-instance vsysa
#
security-policy
rule name trust_to_untrust
source-zone trust
destination-zone untrust
source-address 10.3.0.0 mask 255.255.255.0
source-address 10.3.1.0 mask 255.255.255.0
action permit
#
nat-policy
rule name nat1
source-zone trust
```

```
egress-interface GE0/0/1
source-address 10.3.0.0 mask 255.255.255.0
source-address 10.3.1.0 mask 255.255.255.0
action source-nat easy-ip
#
switch vsys vsysa
#
interface GE0/0/6
undo shutdown
ip binding vpn-instance vsysa
ip address 10.3.0.1 255.255.255.0
service-manage http permit
service-manage https permit
service-manage ping permit
service-manage ssh permit
service-manage telnet permit
#
firewall zone local
set priority 100
#
firewall zone trust
set priority 85
add interface GE0/0/6
#
firewall zone untrust
set priority 5
add interface Virtual-if1
#
firewall zone dmz
set priority 50
#
security-policy
rule name to_internet_allow
source-zone trust
destination-zone untrust
source-address address-set 10.3.0.100-10.3.0.110
action permit
rule name to_market_allow
source-zone trust
destination-zone untrust
destination-address 10.3.1.0 mask 255.255.255.0
action permit
rule name vsysb_to_vsysa
source-zone untrust
destination-zone trust
source-address 10.3.1.0 mask 255.255.255.0
destination-address 10.3.0.0 mask 255.255.255.0
action permit
```

```
#
ip route-static 0.0.0.0 0.0.0.0 public
#
switch vsys vsysb
#
interface GE0/0/7
undo shutdown
ip binding vpn-instance vsysb
ip address 10.3.1.1 255.255.255.0
service-manage http permit
service-manage https permit
service-manage ping permit
service-manage ssh permit
service-manage telnet permit
#
firewall zone local
set priority 100
#
firewall zone trust
set priority 85
add interface GE0/0/7
#
firewall zone untrust
set priority 5
add interface Virtual-if2
#
firewall zone dmz
set priority 50
#
security-policy
rule name to_internet_allow
source-zone trust
destination-zone untrust
action permit
rule name vsysa_to_vsysb
source-zone untrust
destination-zone trust
source-address 10.3.0.0 mask 255.255.255.0
destination-address 10.3.1.0 mask 255.255.255.0
action permit
#
ip route-static 0.0.0.0 0.0.0.0 public
#
```

3.4.2 SW1 预配置

```
#
interface vlanif1
```

```
ip address 100.1.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
port link-type access
#
```

3.5 思考题

防火墙的根系统与虚拟系统中配置 Virtual-if 接口的作用是什么？

参考答案：虚拟接口是创建虚拟系统时系统自动为其创建的一个逻辑接口，作为虚拟系统自身与其他虚拟系统之间通信的接口。

4 防火墙流量管理实验

4.1 实验介绍

4.1.1 关于本实验

某企业将防火墙作为出口网关部署在网络边界，使内部网络中的用户可以访问 Internet。在办公环境中，为了提高企业员工的工作效率，企业考虑为每个员工分配固定的上下行带宽速率，并通过防火墙对接入网络的用户进行本地 Portal 认证。

4.1.2 实验目的

- 学会配置带宽策略，限制内网 PC 上传/下载带宽。
 - 实现对企业员工进行本地 Portal 认证。
-

4.1.3 实验组网介绍

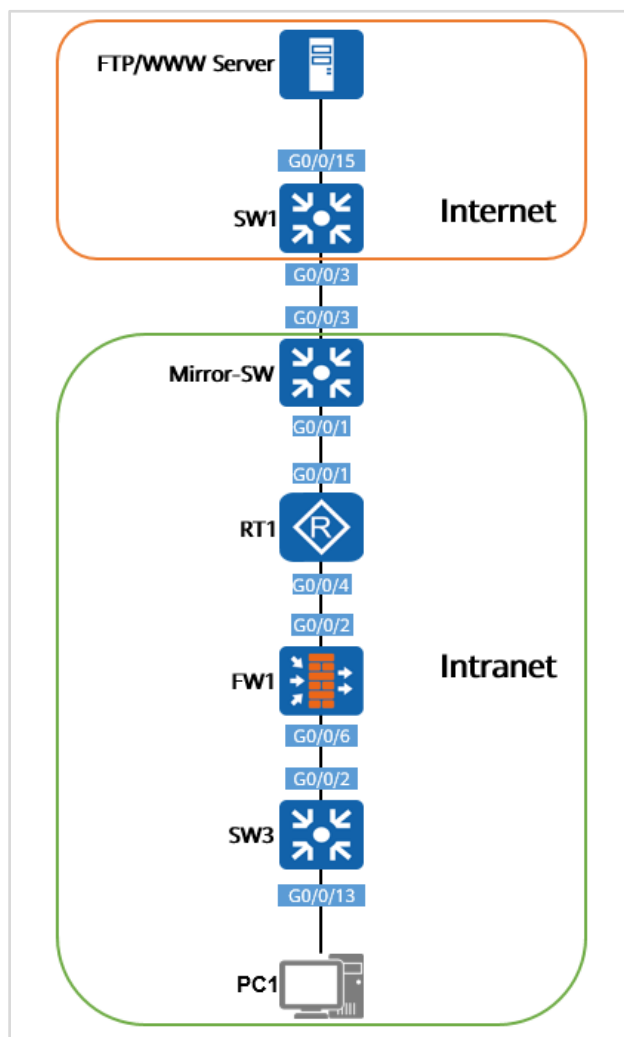


图4-1 流量管理实验拓扑

SW3、Mirror-SW 负责二层互联，RT1 与 SW1 之间需要路由可达。SW3、Mirror-SW 、RT1 与 SW1 的配置在实验步骤中未做体现，具体可参考“4.4 配置参考”中的预配置，本实验重点介绍 FW1 上关键配置。

4.1.4 实验规划

表4-1 设备接口规划表

设备	接口	接口性质	接口信息	说明
FW1	G0/0/2	三层接口	10.3.1.2/30 安全区域: untrust	网络上行口出接口， 与RT1互连
	G0/0/6	三层接口	172.16.20.2/24 安全区域: trust	与SW3互连

RT1	G0/0/1.2	三层接口	4.4.4.2/30 终结VLAN 2	与Mirror-SW互连
	G0/0/4	三层接口	10.3.1.1/30	与FW1互连
SW1	G0/0/3	Trunk	PVID: 1 Allow-pass VLAN: 2	与RT1互连
	G0/0/15	Access	PVID: 300	连接FTP/WWW Server
	VLANIF2	三层接口	4.4.4.1/30	与RT1接口组成直连网段
	VLANIF300	三层接口	100.20.1.1/24	FTP/WWW Server网关
Mirror-SW	G0/0/2	Trunk	PVID: 1 Allow-pass VLAN: 2	互连接口
	G0/0/3			
SW3	G0/0/2	Access	PVID: 40	连接终端
	G0/0/13			与FW2互连
PC1	Ethernet0	网卡	172.16.20.100/24 网关: 172.16.20.1/24	内网测试终端
FTP/WWW Server	Ethernet0	网卡	100.20.1.2/24 网关: 100.20.1.1/24	Internet服务器

4.2 实验任务配置

4.2.1 配置思路

- 1.网络基础参数配置（接口地址、安全区域）。
- 2.配置安全策略、静态路由、NAT 策略，允许内网用户访问 Internet。
- 3.配置带宽策略，对内网用户上传下载的速率进行限制。
- 4.配置用户身份验证，用户访问 Internet 需要先完成 Portal 认证。

4.2.2 配置步骤 - CLI

步骤 1 网络基本参数配置

FW1 设备基础网络参数的配置可复用“1.2.2 配置步骤-CLI”中步骤 1 相关配置，此处无需再次配置。

步骤 2 配置安全策略

FW1 设备业务安全策略的配置可复用“1.2.2 配置步骤-CLI”中步骤 4 相关配置，此处无需再次配置。

但是因为本实验有 FTP 业务模拟，需要开启针对 FTP 业务的 ASPF 功能。

```
HRP_M[FW1]firewall detect ftp
```

步骤 3 路由配置

FW1 设备路由配置可复用“1.2.2 配置步骤-CLI”中步骤 2 相关配置，此处无需再次配置。

步骤 4 NAT 策略配置

RT1 设备 NAT 策略配置可复用“1.2.2 配置步骤-CLI”中步骤 2 相关配置，此处无需再次配置。

步骤 5 带宽通道配置

为上网用户配置相应的带宽通道。

```
HRP_M[FW1]bandwidth-policy
HRP_M[FW1-policy-bandwidth] profile name ftp
HRP_M[FW1-policy-bandwidth-profile-ftp] bandwidth maximum-bandwidth whole downstream 20000
HRP_M[FW1-policy-bandwidth-profile-ftp] bandwidth maximum-bandwidth per-ip downstream 2000
HRP_M[FW1-policy-bandwidth-profile-ftp] quit
HRP_M[FW1-policy-bandwidth]
```

步骤 6 带宽策略配置

针对上网用户配置带宽策略。

```
HRP_M[FW1-policy-bandwidth]rule name ftp
HRP_M[FW1-policy-bandwidth-rule-ftp] source-zone trust
HRP_M[FW1-policy-bandwidth-rule-ftp] destination-zone untrust
HRP_M[FW1-policy-bandwidth-rule-ftp] source-address 172.16.20.0 mask 255.255.255.0
HRP_M[FW1-policy-bandwidth-rule-ftp] action qos profile ftp
Warning: Using this feature will affect performance, please enable it with caution.
HRP_M[FW1-policy-bandwidth-rule-ftp] quit
HRP_M[FW1-policy-bandwidth]quit
HRP_M[FW1]
```

步骤 7 Portal 认证配置

启用 Portal 认证并配置本地 Portal 服务器。

```
HRP_M[FW1] identity-management
HRP_M[FW1-identity-management]portal
HRP_M[FW1-identity-management-portal] portal enable
```

```
Warning: The IP address is not specified, which expands the range of accessed IP.
HRP_M[FW1-identity-management-portal] server https ip 172.16.20.2 port 8887
HRP_M[FW1-identity-management-portal] quit
HRP_M[FW1-identity-management]quit
HRP_M[FW1]
```

创建安全组与用户，用于本地认证。

```
HRP_M[FW1]ucl-group name staff
HRP_M[FW1]aaa
HRP_M[FW1-aaa] local-access-user user1
HRP_M[FW1-aaa-access-user-user1] 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[FW1-aaa-access-user-user1] service-type portal
Warning: If the service type of local access users is configured multiple times, the new configuration
overwrites the previous one. The new configuration may cause local access users unable to go online.
Continue? [Y/N]: y
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.
HRP_M[FW1-aaa-access-user-user1]ucl-group staff
HRP_M[FW1-aaa-access-user-user1] quit
HRP_M[FW1-aaa]quit
HRP_M[FW1]
```

配置 Portal 认证策略。

```
HRP_M[FW1]auth-policy
HRP_M[FW1-policy-auth]rule name policy_auth_01
HRP_M[FW1-policy-auth-rule-policy_auth_01]source-zone trust
HRP_M[FW1-policy-auth-rule-policy_auth_01]source-address 172.16.20.0 24
HRP_M[FW1-policy-auth-rule-policy_auth_01]action portal
HRP_M[FW1-policy-auth-rule-policy_auth_01]quit
HRP_M[FW1-policy-auth]quit
HRP_M[FW1]
```

配置安全策略，放通 trust 到 local 的安全策略，确保认证报文可正常交互。

```
HRP_M[FW1]security-policy
HRP_M[FW1-policy-security]rule name trust-local
HRP_M[FW1-policy-security-rule-trust-local] source-zone trust
HRP_M[FW1-policy-security-rule-trust-local] destination-zone local
HRP_M[FW1-policy-security-rule-trust-local] action permit
HRP_M[FW1-policy-security-rule-trust-local] quit
HRP_M[FW1-policy-security]quit
HRP_M[FW1]
```

4.2.3 配置步骤 - Web

步骤 1 网络基本参数配置

FW1 设备基础网络参数的配置可复用“1.2.3 配置步骤-Web”中步骤 1 相关配置，此处无需再次配置。

步骤 2 安全策略配置

FW1 设备业务安全策略的配置可复用“1.2.3 配置步骤-Web”中步骤 5 相关配置，此处无需再次配置。

但是因为本实验有 FTP 业务模拟，需要开启针对 FTP 业务的 ASPF 功能。

在 FW1 设备 Web 管理界面选择“策略 > ASPF 配置”进入 ASPF 配置界面，执行以下操作：

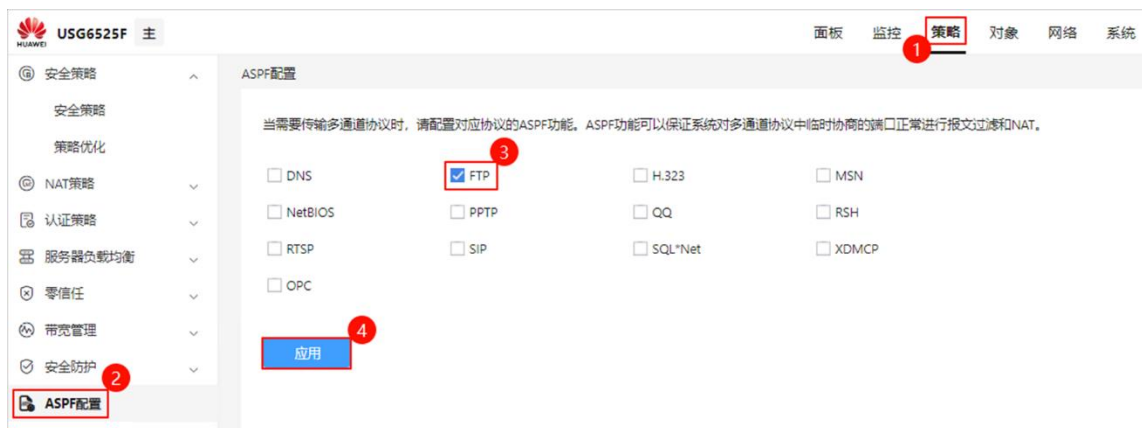


图4-2 FW1 开启针对 FTP 的 ASPF 功能

步骤 3 路由配置

FW1 设备路由配置可复用“1.2.3 配置步骤-Web”中步骤 2 相关配置，此处无需再次配置。

步骤 4 NAT 策略配置

RT1 设备 NAT 策略配置可复用“1.2.2 配置步骤-CLI”中步骤 2 相关配置，此处无需再次配置。

步骤 5 带宽管理配置

在 FW1 设备 Web 管理界面选择“策略 > 带宽管理 > 带宽通道”新建带宽通道，为上网用户配置带宽通道。



USG6525F 主

面板 监控 **策略**

④ 安全策略 ^

安全策略

策略优化

④ NAT策略 v

认证策略 v

服务器负载均衡 v

零信任 v

带宽管理 ^

带宽策略

带宽通道

安全防护 v

带宽通道列表

3 新建 删除

名称	整体限流		
	最大带宽	保证带宽	最大连接数



图4-5 配置带宽策略

步骤 6 Portal 认证配置

在 FW1 设备 Web 管理界面选择“对象 > 用户 > 上网方式”配置用户上网方式为“Portal 认证”。

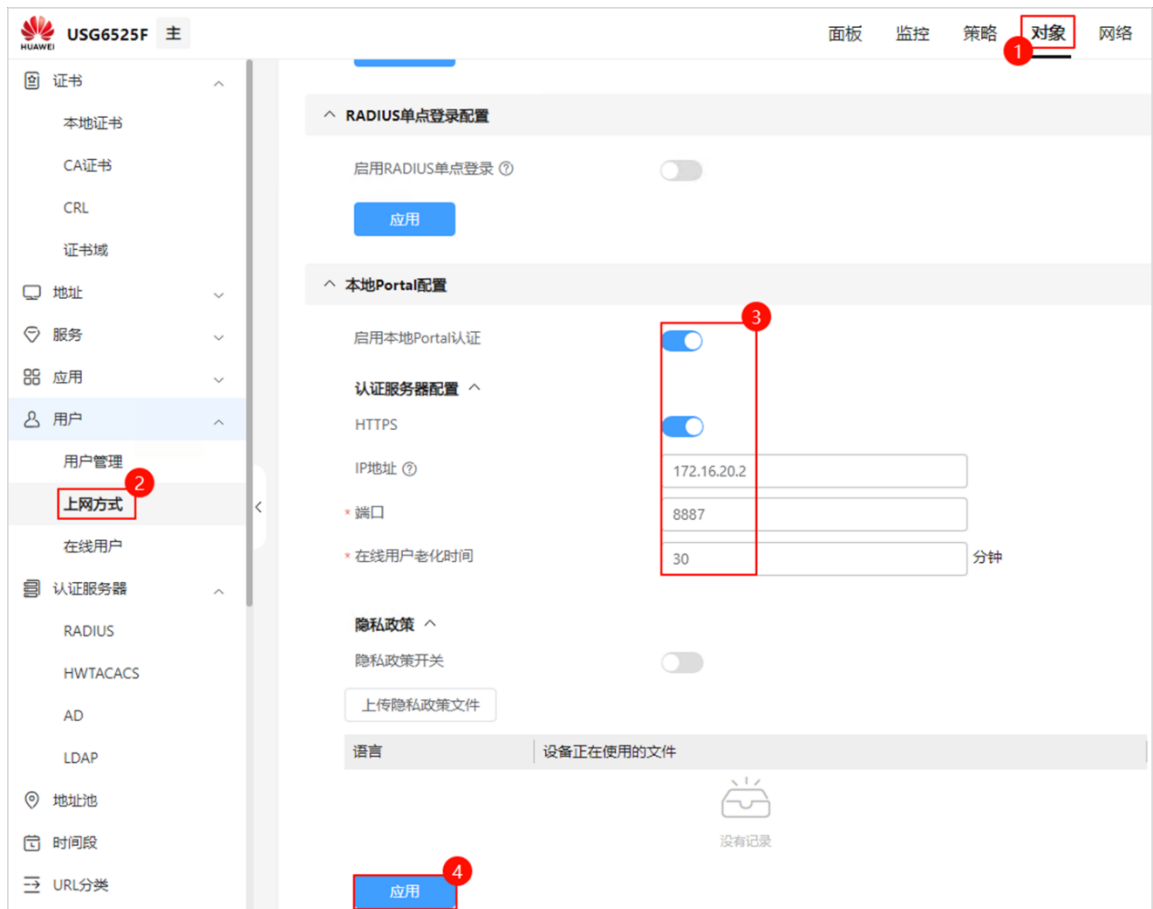


图4-6 本地 Portal 认证全局配置

选择“对象 > 用户 > 用户管理”创建本地用户安全组 and 用户，用于 Portal 认证。



图4-7 新建用户安全组

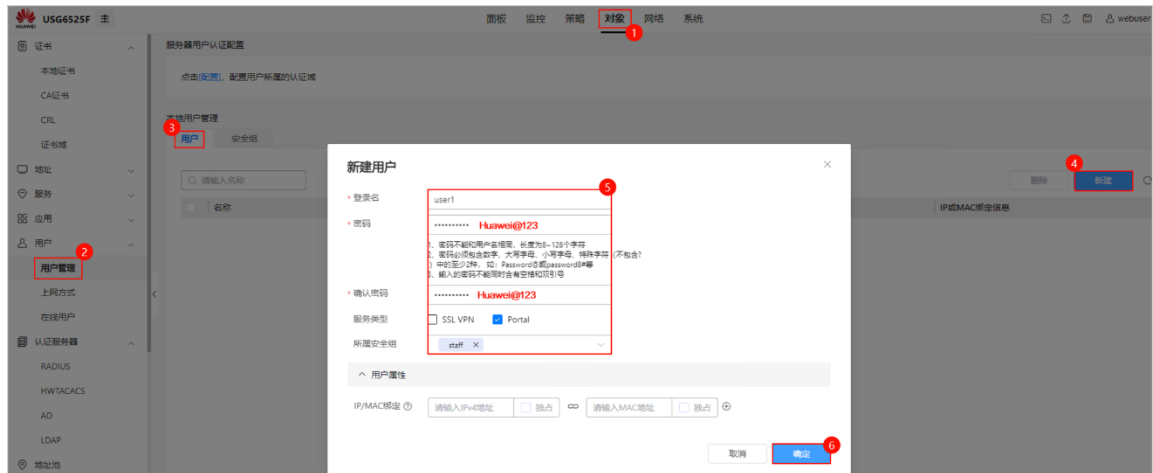


图4-8 新建本地 Portal 认证用户

选择“策略 > 认证策略”，新建认证策略，要求用户从 trust 区域访问 untrust 区域时，均需要先经过 Portal 认证。

新建认证策略

概述

* 名称

Portal

描述

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

trust

IP 地址/地区 ②

any

目的

安全区域

untrust

IP 地址/地区 ②

any

服务 ②

协议

any

动作

认证动作

不认证 ②

免认证 ②

SDP准入认证

Portal认证

TSM在线用户同步

取消

命令预览

确定

图4-9 新建认证策略

选择“策略 > 安全策略 > 新建安全策略”，创建安全策略，放行 trust 到 local 的安全策略，确保证据报文可正常交互。



新建安全策略

概述

名称: trust_local

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

地址/地区: any

标签: 请选择

目的

目的类型: ☒ 安全区域 ☐ 虚拟服务

安全区域: local

地址/地区: any

标签: 请选择

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: 反病毒/入侵防御/URL过滤/内容过滤/文件过滤/邮件过滤/DNS过滤

转到“设置”以激活 Windows。

取消 命令预览 确定

图4-10 创建安全策略保障 Portal 认证报文正常交互

4.3 结果验证

4.3.1 认证前业务测试

使用 RDP 登录 PC1 终端，在进行 Portal 认证前打开命令行，测试到达 FTP/WWW Server 的连通性。

```
C:\Users\Security>ping 100.20.1.2

Pinging 100.20.1.2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 100.20.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

图4-11 PC1 访问 Internet（认证前）

可以发现在用户进行 Portal 认证前，无法访问 Internet 资源。

4.3.2 Portal 认证测试

打开 PC1 终端浏览器，输入：“https://172.16.20.2:8887”，访问 Portal 认证界面。

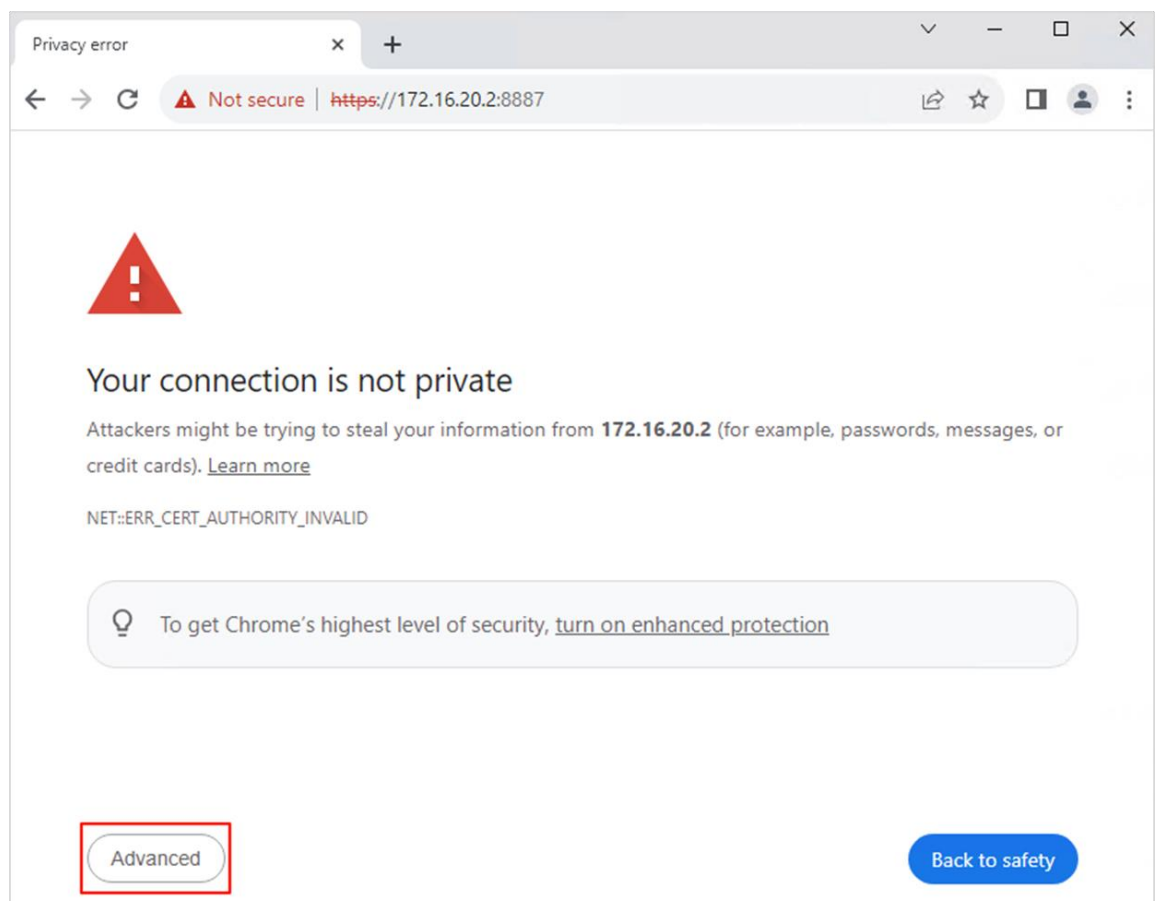


图4-12 PC1 访问 Portal 认证界面 (1)

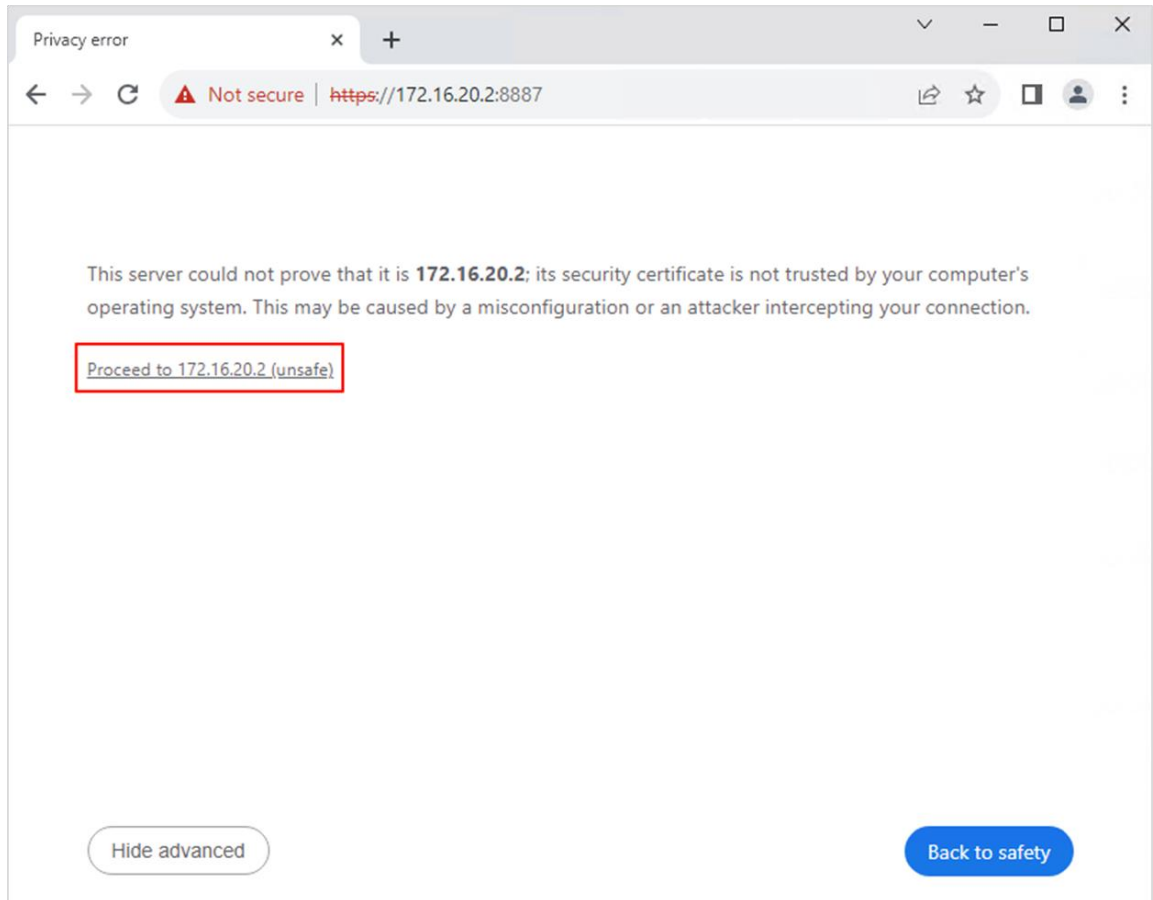


图4-13 PC1 访问 Portal 认证界面 (2)

进入 Portal 认证界面后，输入之前在 FW1 设备本地创建的用户信息（user1/Huawei@123）。

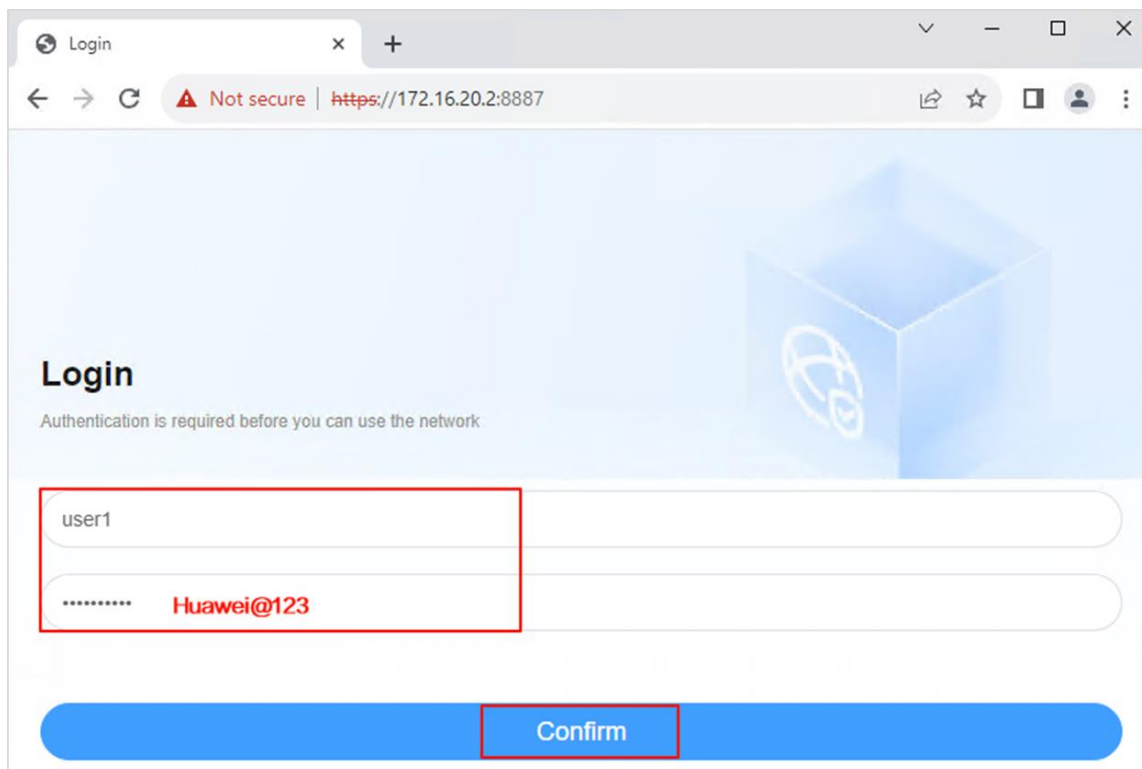
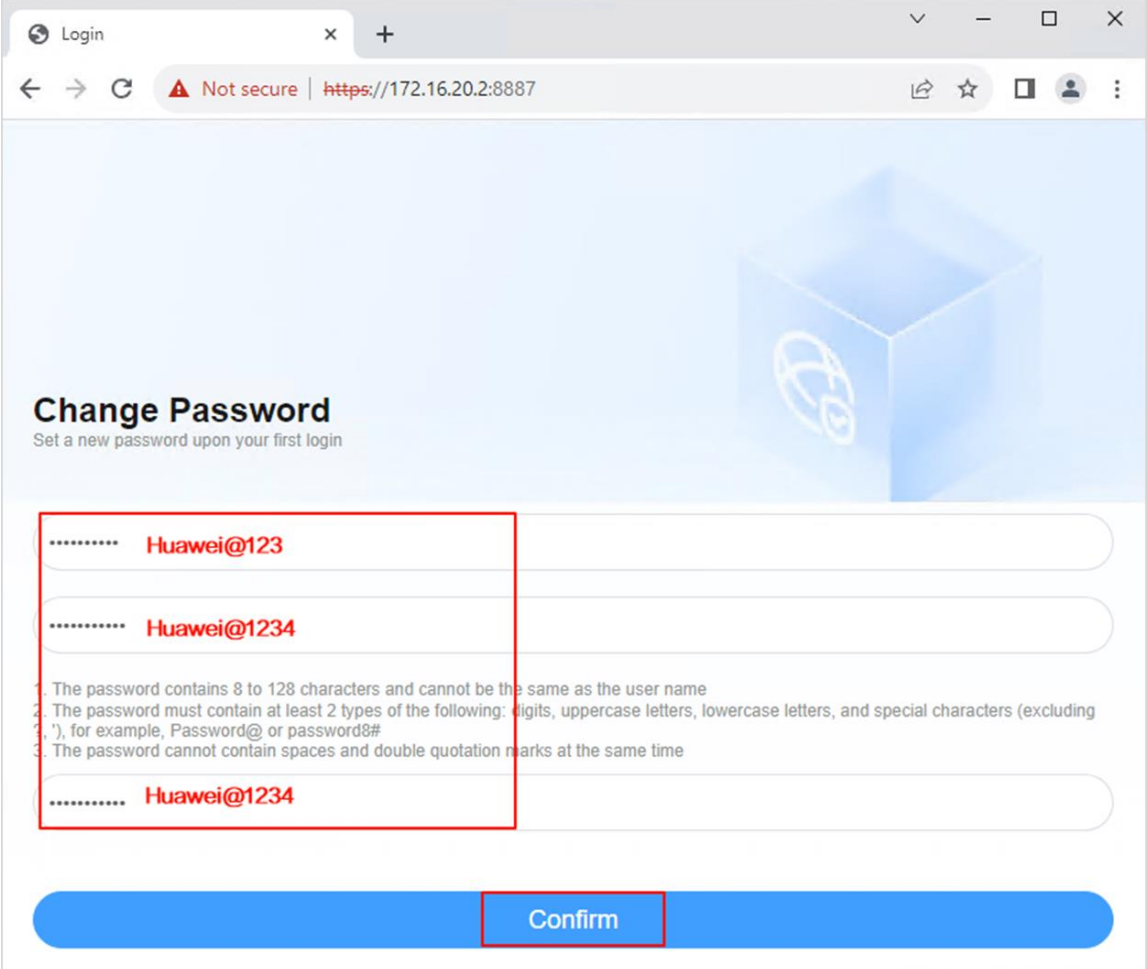


图4-14 PC1 进行 Portal 认证

用户首次进行 Portal 认证时，设备会强制要求修改初始密码。



Login

Not secure | https://172.16.20.2:8887

Change Password

Set a new password upon your first login

..... Huawei@123

..... Huawei@1234

1. The password contains 8 to 128 characters and cannot be the same as the user name
2. The password must contain at least 2 types of the following: digits, uppercase letters, lowercase letters, and special characters (excluding '), for example, Password@ or password8#
3. The password cannot contain spaces and double quotation marks at the same time

..... Huawei@1234

Confirm

图4-15 PC1 修改 Portal 认证密码

密码修改完成后，按照提示再次进行 Portal 认证。

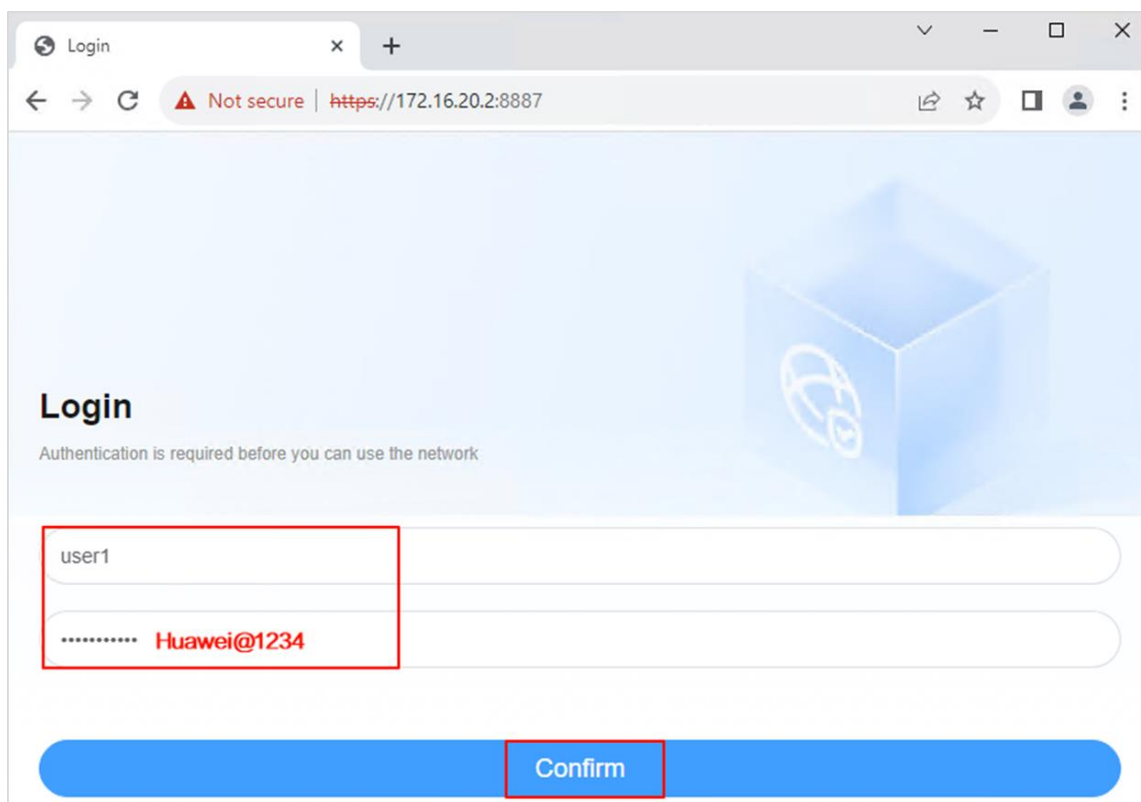


图4-16 PC1 执行 Portal 认证（初始密码修改后）

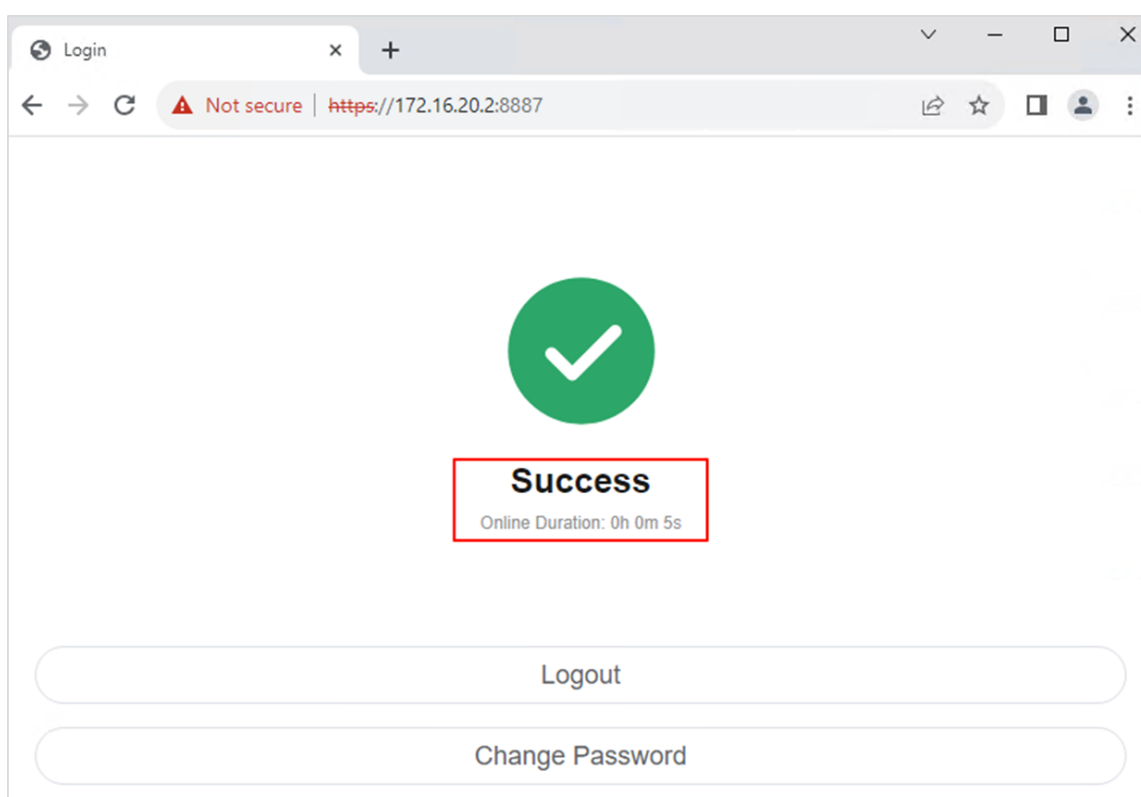


图4-17 PC1 认证成功

4.3.3 认证后业务测试

使用 RDP 登录 PC1 终端，打开命令行，测试到达 FTP/WWW Server 的连通性。

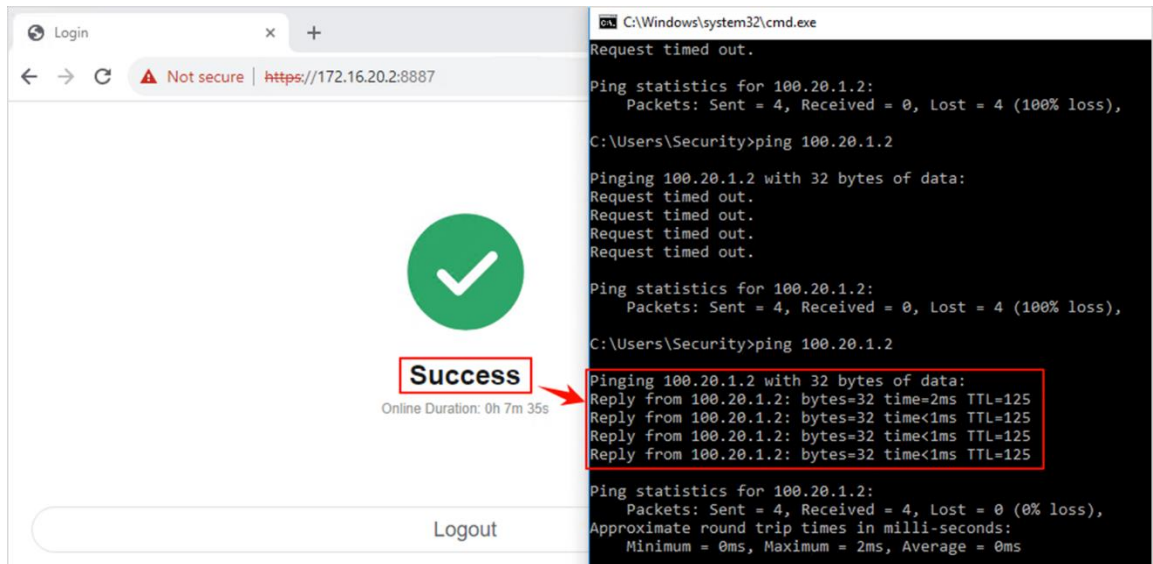


图4-18 PC1 访问 Internet（认证后）

可以发现在用户进行 Portal 认证后，可以正常访问 Internet 资源。

4.3.4 带宽管理测试

在 PC1 桌面上打开“MobaXterm”软件，执行以下操作，访问 FTP/WWW Server 的 FTP 服务。

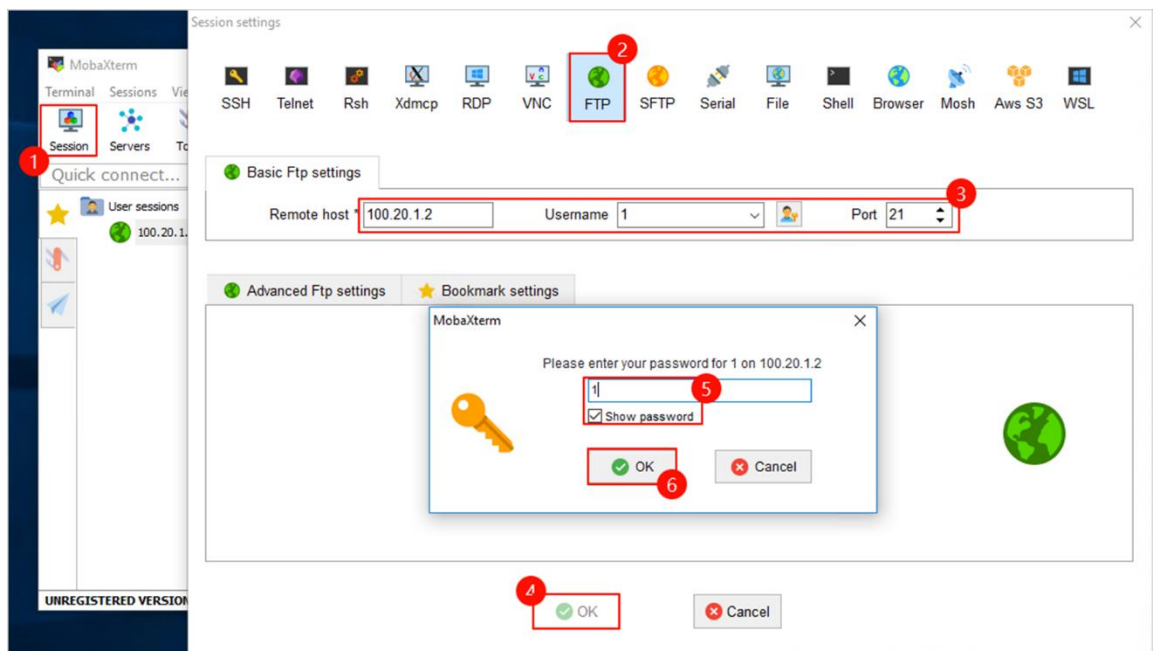


图4-19 PC1 建立 FTP 会话（1）

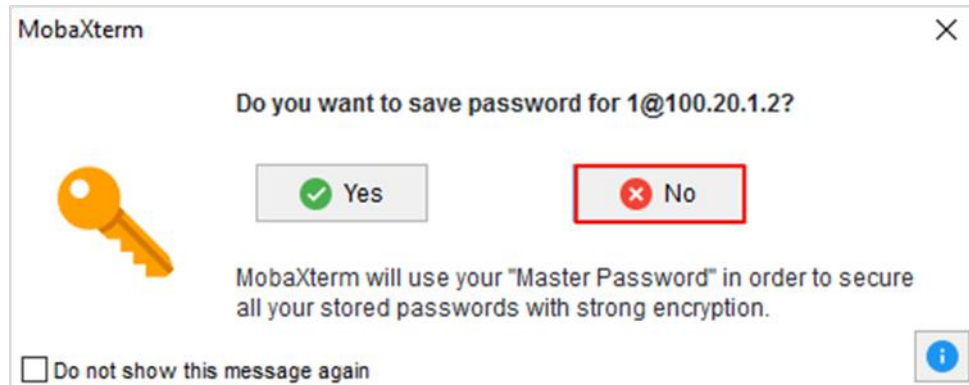


图4-20 PC1 建立 FTP 会话（2）

成功建立 FTP 会话后，将 FTP 服务器上“PixPin_10.0.9.1.exe”文件拖拽至 PC1 桌面，进行文件下载，此时将鼠标悬停在文件下载进度条，可以发现文件下载速率始终维持在设定的阈值之下，表明带宽管理配置生效。

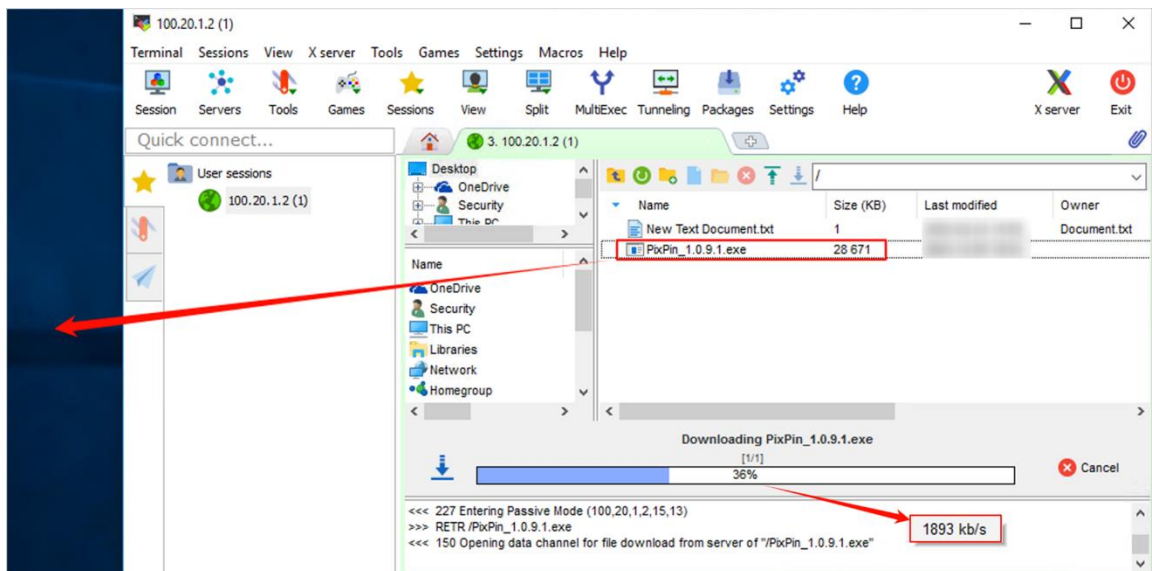


图4-21 PC1 文件传输测试

4.4 配置参考

4.4.1 FW1 配置

```
#
sysname FW1
#
interface GE0/0/2
 ip address 10.3.1.2 255.255.255.252
 ospf enable 1 area 0.0.0.0
```

```
service-manage ping permit
#
interface GE0/0/6
 ip address 172.16.20.2 255.255.255.0
 vrrp vrid 1 virtual-ip 172.16.20.1 active
 ospf enable 1 area 0.0.0.0
#
ospf 1 router-id 11.11.11.1
 opaque-capability enable
 area 0.0.0.0
  network 10.3.1.2 0.0.0.0
  network 172.16.20.0 0.0.0.255
  network 172.16.30.0 0.0.0.255
#
firewall zone local
 set priority 100
#
firewall zone trust
 set priority 85
 add interface GE0/0/5
 add interface GE0/0/6
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
 add interface GE0/0/2
#
firewall zone dmz
 set priority 50
 add interface Eth-Trunk0
#
firewall detect ftp
#
security-policy
 rule name t2u
  source-zone trust
  destination-zone untrust
  action permit
 rule name trust-local
  source-zone trust
  destination-zone local
  action permit
#
bandwidth-policy
 profile name ftp
  bandwidth maximum-bandwidth whole downstream 20000
  bandwidth maximum-bandwidth per-ip downstream 2000
 rule name ftp
```

```
source-zone trust
destination-zone untrust
source-address 172.16.20.0 mask 255.255.255.0
action qos profile ftp
#
auth-policy
rule name policy_auth_01
source-zone trust
source-address 172.16.20.0 mask 255.255.255.0
action portal
#
identity-management
sso-radius
sso-tsm
portal
server https ip 172.16.20.2 port 8887
portal enable
#
return
```

4.4.2 RT1 预配置

```
#
sysname RT1
#
acl number 3500
rule 5 permit ip
#
bfd
#
interface GigabitEthernet0/0/1
undo portswitch
#
interface GigabitEthernet0/0/1.2
dot1q termination vid 2
ip address 4.4.4.2 255.255.255.252
nat outbound 3500
#
interface GigabitEthernet0/0/2
undo portswitch
ip address 10.1.1.1 255.255.255.252
ospf enable 1 area 0.0.0.0
#
interface GigabitEthernet0/0/4
undo portswitch
ip address 10.3.1.1 255.255.255.252
ospf enable 1 area 0.0.0.0
#
```

```
interface LoopBack0
 ip address 33.33.33.1 255.255.255.255
#
bfd 1 bind peer-ip 10.3.1.2 source-ip 4.4.4.2
 discriminator local 10
 discriminator remote 20
 commit
#
ospf 1 router-id 33.33.33.1
 default-route-advertise always
 area 0.0.0.0
#
ip route-static 0.0.0.0 0.0.0.0 4.4.4.1
#
return
```

4.4.3 Mirror-SW 预配置

```
#
sysname Mirror-SW
#
vlan batch 2 40
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 2 40
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 2 40
#
return
```

4.4.4 SW1 预配置

```
#
sysname SW1
#
vlan batch 2 40 300
#
interface vlanif2
 ip address 4.4.4.1 255.255.255.252
#
interface vlanif40
 ip address 3.3.3.1 255.255.255.252
#
interface vlanif300
 ip address 100.20.1.1 255.255.255.0
```

```
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 2 40
#
interface GigabitEthernet 0/0/15
 port link-type access
 port default vlan 300
#
ip route-static 172.16.0.0 16 4.4.4.2
ip route-static 172.16.0.0 16 3.3.3.2 preference 70
#
return
```

4.5 思考题

带宽通道中设置的整体保证带宽和最大带宽的区别？

参考答案：

整体的保证带宽是指进入带宽通道的流量可获得的最小带宽资源，整体的最大带宽是指进入带宽通道的流量可获得的最大带宽资源。

流量进入带宽通道后，设备将当前流量与带宽通道中设置的保证带宽/最大带宽进行比较，采取不同的处理方式：

- 如果流量小于保证带宽，这部分流量在出接口发送环节能够确保被转发。
- 如果流量大于最大带宽，则直接丢弃超出最大带宽的流量。
- 超出保证带宽的流量，在接口收发时，由设备随机丢包。

5 防火墙智能选路实验

5.1 实验介绍

5.1.1 关于本实验

某企业分别从 ISP1 和 ISP2 租用了一条链路，ISP1 链路的带宽为 50 M，ISP2 链路的带宽为 100 M。企业希望流量按照带宽比例分担到 ISP1 和 ISP2 链路上，保证带宽资源得到充分利用。当其中一条 ISP 链路过载时，后续流量将通过另一条 ISP 链路传输，提高访问的可靠性。本实验通过在防火墙部署基于链路带宽负载分担的全局选路策略方式，实现企业需求。

5.1.2 实验目的

- 了解防火墙智能选路的方式。
- 掌握防火墙智能选路方式的配置方法。

5.1.3 实验组网介绍

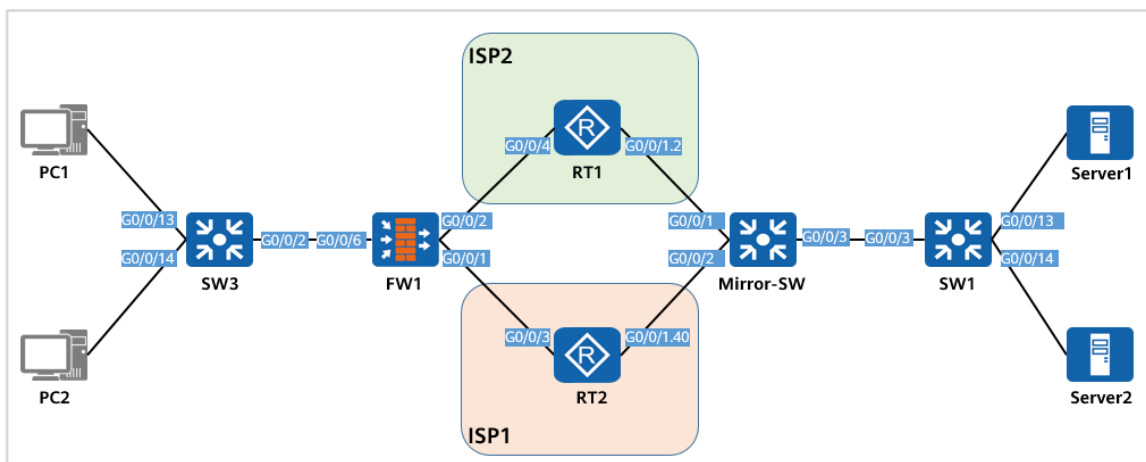


图5-1 防火墙智能选路实验拓扑图

FW1 作为企业出口网关，通过双链路分别连接 ISP1 和 ISP2，RT1、RT2 模拟 Internet。上图中 Server1 为全量拓扑中的 Attack PC，Server2 为全量拓扑中的 Legal PC，SW3、RT1、RT2、Mirror-SW 和 SW1 相关配置在实验配置步骤中未体现，请参考“5.4 配置参考”完成预配置，本实验重点介绍 FW1 上关键配置。

5.1.4 实验规划

表5-1 设备接口规划表

设备	接口	接口性质	接口信息	说明
FW1	G0/0/1	三层接口	10.5.1.2/30 安全区域: untrust	连接ISP1的出接口， 与RT2互连
	G0/0/2	三层接口	10.3.1.2/30 安全区域: untrust	连接ISP2的出接口， 与RT1互连
	G0/0/6	三层接口	172.16.20.2/24 安全区域: trust	与SW3互连，承载 终端网关
RT1	G0/0/1.2	三层子接口	4.4.4.2/30 终结VLAN2	与SW1的VLANIF2 组成直连网段
	G0/0/4	三层接口	10.3.1.1/30	与FW1互连
RT2	G0/0/1.40	三层子接口	3.3.3.2/30 终结VLAN40	与SW1的VLANIF40 组成直连网段
	G0/0/3	三层接口	10.5.1.1/30	与FW1互连
SW1	VLANIF2	三层接口	4.4.4.1/30	与RT1接口组成直连 网段
	VLANIF40	三层接口	3.3.3.1/30	与RT2接口组成直连 网段
	G0/0/3	Trunk	Allow-pass VLAN： 2， 40	与Mirror-SW互连
	G0/0/13	Access	PVID： 1000	连接Server1
	G0/0/14	Access	PVID： 2000	连接Server2
	VLANIF1000	三层接口	100.30.1.1/24	Server1的网关地址
	VLANIF2000	三层接口	100.40.1.1/24	Server2的网关地址
Mirror-SW	G0/0/1	Trunk	PVID： 1	互连接口
	G0/0/2		Allow-pass VLAN： 2， 40	
	G0/0/3			
SW3	G0/0/2	Access	PVID： 40	与FW互连

	VLANIF40	三层接口	172.16.20.100/24	对接FW
	G0/0/13	Access	PVID: 34	连接PC1
	G0/0/14	Access	PVID: 35	连接PC2
	VLANIF34	三层接口	172.17.10.1/24	PC1网关
	VLANIF35	三层接口	172.17.20.1/24	PC2网关
PC1	Ethernet0	网卡	172.17.10.100/24 网关: 172.17.10.1/24	内网终端
PC2	Ethernet0	网卡	172.17.20.100/24 网关: 172.17.20.1/24	内网终端
Server1 (Attack PC)	Ethernet0	网卡	100.30.1.2/24 网关: 100.30.1.1/24	外网终端
Server2 (Legal PC)	Ethernet0	网卡	100.40.1.2/24 网关: 100.40.1.1/24	外网终端

5.2 实验任务配置

5.2.1 配置思路

- 1.配置健康检查功能，分别为 ISP1 和 ISP2 链路配置健康检查实例。
- 2.配置防火墙接口的 IP 地址、安全区域、网关地址、带宽和过载保护阈值。
- 3.配置全局选路策略，配置智能选路方式为根据链路带宽负载分担、调用健康检查实例，并指定 FW1 和 ISP1、ISP2 网络直连的出接口作为智能选路成员接口。
- 4.配置安全策略和 NAT 策略，允许企业内网用户访问外网资源。

5.2.2 配置步骤 - CLI

步骤 1 网络基本参数配置

参照“表 5-1”数据规划，完成网络基本参数配置。其中 SW3、RT1、RT2、Mirror-SW 和 SW1 设备已预配，具体可参考“5.4 配置参考”。

FW1 设备的上游连接 RT2 设备的业务接口 GE0/0/1，需要配置 IP 地址，开启 OSPF，并添加进 Untrust 区域。

```
HRP_M[FW1]interface GE0/0/1
HRP_M[FW1-GE0/0/1] ip address 10.5.1.2 255.255.255.252
HRP_M[FW1-GE0/0/1]ospf enable 1 area 0.0.0.0
```

```
HRP_M[FW1-GE0/0/1]quit
HRP_M[FW1]firewall zone untrust
HRP_M[FW1-zone-untrust] add interface GE0/0/1
HRP_M[FW1-zone-untrust]quit
HRP_M[FW1]
```

步骤 2 配置健康检查功能

在 FW1 上配置健康检查功能。

```
HRP_M[FW1]healthcheck enable
HRP_M[FW1]healthcheck name isp-healthcheck
HRP_M[FW1-healthcheck-isp-healthcheck] destination 100.30.1.2 interface GE0/0/1 protocol icmp
HRP_M[FW1-healthcheck-isp-healthcheck] destination 100.40.1.2 interface GE0/0/2 protocol icmp
HRP_M[FW1-healthcheck-isp-healthcheck] quit
HRP_M[FW1]
```

步骤 3 配置接口

配置接口所在链路的带宽和过载保护阈值，并开启上行业务接口的 ping 测试功能，确保健康检查报文可正常交互。

```
HRP_M[FW1] interface GE0/0/1
HRP_M[FW1-GE0/0/1] gateway 10.5.1.1
HRP_M[FW1-GE0/0/1] bandwidth ingress 50000 threshold 90
Warning: Using this feature will affect performance, please enable it with caution.
HRP_M[FW1-GE0/0/1] bandwidth egress 50000 threshold 90
Warning: Using this feature will affect performance, please enable it with caution.
HRP_M[FW1-GE0/0/1] service-manage ping permit
HRP_M[FW1-GE0/0/1] quit
HRP_M[FW1] interface GE 0/0/2
HRP_M[FW1-GE0/0/2] gateway 10.3.1.1
HRP_M[FW1-GE0/0/2] bandwidth ingress 100000 threshold 95
Warning: Using this feature will affect performance, please enable it with caution.
HRP_M[FW1-GE0/0/2] bandwidth egress 100000 threshold 95
Warning: Using this feature will affect performance, please enable it with caution.
HRP_M[FW1-GE0/0/2] service-manage ping permit
HRP_M[FW1-GE0/0/2] quit
HRP_M[FW1]
```

步骤 4 配置全局选路策略

配置全局选路策略，流量根据链路带宽负载分担。

```
HRP_M[FW1]multi-interface
HRP_M[FW1-multi-inter]mode proportion-of-bandwidth
HRP_M[FW1-multi-inter]healthcheck isp-healthcheck
HRP_M[FW1-multi-inter]add interface GE0/0/1
HRP_M[FW1-multi-inter]add interface GE0/0/2
HRP_M[FW1-multi-inter]quit
HRP_M[FW1]
```

步骤 5 配置安全策略

FW1 设备业务安全策略的配置可复用“1.2.2 配置步骤-CLI”中步骤 4 相关配置，此处无需再次配置。

步骤 6 配置 NAT 策略

配置出接口方式的源 NAT 策略，使内网用户直接借用防火墙 FW1 的公网 IP 地址来访问 Internet。

```
HRP_M[FW1]nat-policy
HRP_M[FW1-policy-nat]rule name trust-untrust
HRP_M[FW1-policy-nat-rule-trust-untrust]source-zone trust
HRP_M[FW1-policy-nat-rule-trust-untrust]destination-zone untrust
HRP_M[FW1-policy-nat-rule-trust-untrust]action source-nat easy-ip
Warning: Services will be interrupted after an active/standby switchover due to the different public IP
addresses of the devices. Therefore, the address pool configuration mode is recommended.
HRP_M[FW1-policy-nat-rule-trust-untrust]quit
HRP_M[FW1-policy-nat]quit
HRP_M[FW1]
```

5.2.3 配置步骤 - Web

步骤 1 网络基本参数配置

参照“表 5-1”数据规划，完成网络基本参数配置。其中 SW3、RT1、RT2、Mirror-SW 和 SW1 设备已预配，具体可参考“5.4 配置参考”。

在 FW1 设备 Web 管理界面选择“网络 > 接口”，进入接口列表界面，执行以下操作，完成业务接口基础配置。

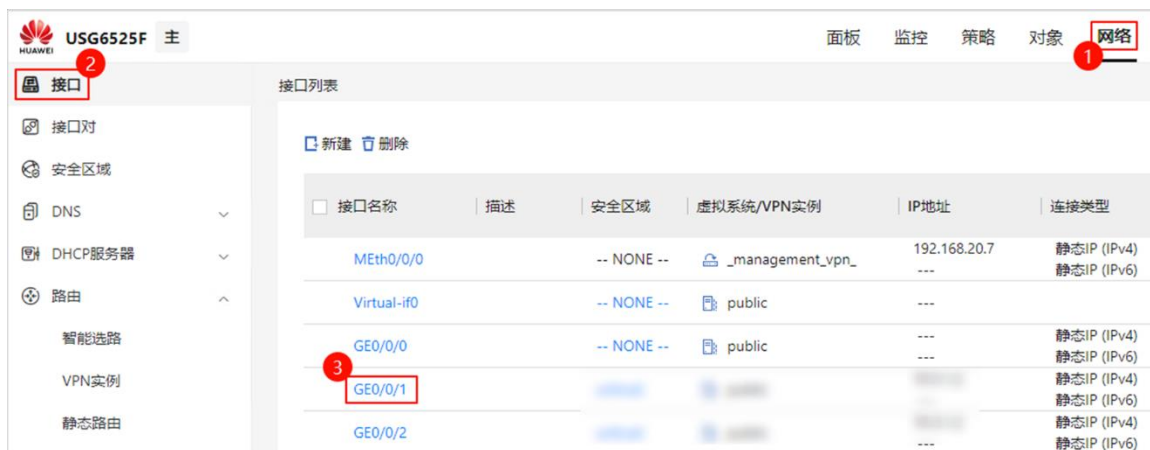


图5-2 进入 GE0/0/1 接口配置界面

修改GE

修改接口配置可能会导致已有业务受影响，请谨慎操作。

接口名称

GE0/0/1

描述

虚拟系统

public

VPN实例

public

安全区域

untrust

访问控制管理

HTTP

HTTPS

Ping

SSH

Telnet

NETCONF

SNMP

模式

路由

交换

旁路检测

接口对

IPv4

IPv6

连接类型

静态IP

DHCP

PPPoE

IP地址

10.5.1.2/255.255.255.252

默认网关

10.5.1.1

多出口选项

缺省路由

源进源出路由控制

接口带宽

入方向带宽

出方向带宽

高级

取消

确定

图5-3 GE0/0/1 接口基础配置

使用同样方式进入 GE0/0/2 接口配置界面，完成 GE0/0/2 接口基础配置。

确定

图5-4 GE0/0/2 接口基础配置

步骤 2 配置健康检查功能

开启防火墙的健康检查功能，并针对 ISP1 和 ISP2 出口链路新建一个健康检查实例。假设 ISP1 网络的目的地址网段为 100.20.1.0/24，ISP2 网络的目的地址网段为 100.40.1.0/24。

在 FW1 设备 Web 管理界面选择“对象 > 健康检查”，在“健康检查列表”区域单击“新建”执行以下操作：



图5-5 配置健康检查

步骤 3 配置全局选路策略

配置防火墙的全局选路策略，流量根据链路带宽负载分担，将 GE0/0/1 和 GE0/0/2 加入出接口列表，并调用之前创建的健康检查实例。

在 FW1 设备 Web 管理界面选择“网络 > 路由 > 智能选路”，在“全局选路策略列表”区域，单击“配置”执行以下操作。

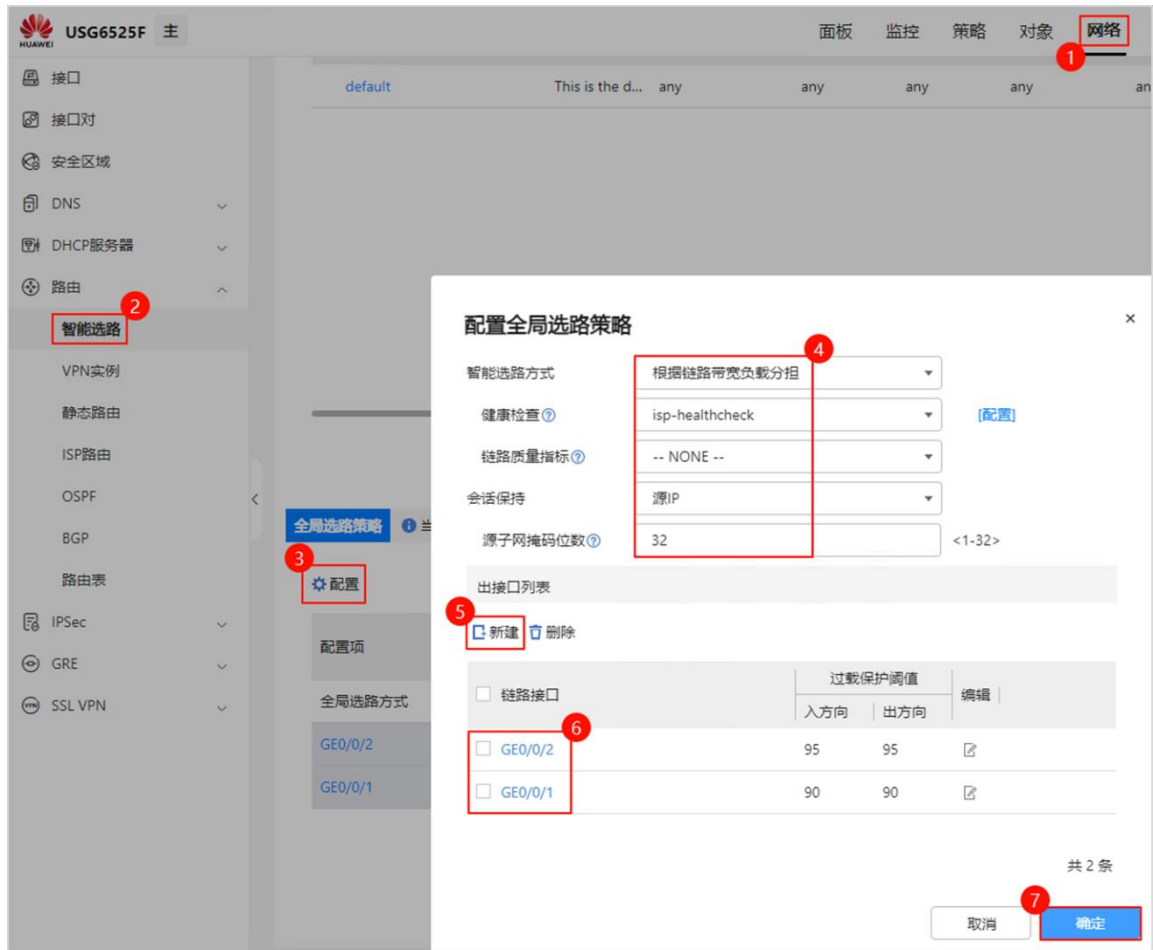


图5-6 配置全局选路策略

步骤 4 配置安全策略

FW1 设备业务安全策略的配置可复用“1.2.2 配置步骤-CLI”中步骤 4 相关配置，此处无需再次配置。

步骤 5 配置 NAT 策略

配置出接口方式的源 NAT 策略，使内网用户直接借用防火墙 FW 的公网 IP 地址来访问 Internet。

在 FW1 设备 Web 管理界面选择“策略 > NAT 策略 > NAT 策略”，单击“新建”进入 NAT 策略配置界面，执行以下操作。



USG6525F 主

面板 监控 **策略**

③ 安全策略

安全策略

策略优化

③ NAT策略

NAT策略

服务器映射

④ 认证策略

服务器负载均衡

④ 零信任

NAT策略

源转换地址池 目的转换地址池

④ 新建 删除 复制 移动 插入 清除全部命中次数 启用 禁用 批量生成安全策略

请输入要查询的内容 添加查询项

名称	描述	NAT类型	转换模式	时间段
default	This is the defau...		不做转换	

图5-7 进入 NAT 策略配置界面

新建NAT策略

×

[功能介绍]

名称

trust-untrust

描述

NAT类型

☒ NAT
☐ NAT64
☐ NAT66

转换模式

仅转换源地址

时间段

请选择时间段

原始数据包

源安全区域

trust

[多选]

目的类型

☒ 目的安全区域
☐ 出接口

untrust

[多选]

源地址?

请选择或输入地址

目的地址?

请选择或输入地址

服务?

请选择或输入服务

转换后的数据包

源地址转换为

☐ 地址池中的地址
☒ 出接口地址

⚠

由于主机和备机转换后的公网地址不一样，双机热备切换将导致业务中断需重连，建议改为地址池配置方式。

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5-8 配置源 NAT 策略

5.3 结果验证

为避免“实验 4”中部署的本地 Portal 认证影响本实验的业务验证，可以先将 FW1 设备上部署的认证策略删除，之后再行本实验的业务验证。

```
HRP_M[FW1]auth-policy
HRP_M[FW1-policy-auth]undo rule name Portal
```

```
HRP_M[FW1-policy-auth]quit
HRP_M[FW1]
```

使用 RDP 登录 PC1 终端和 PC2 终端，打开命令行，通过 ping 命令测试到 Server1（Attack PC）和 Server2（Legal PC）的连通性，以此模拟内网访问 Internet 的业务流量。

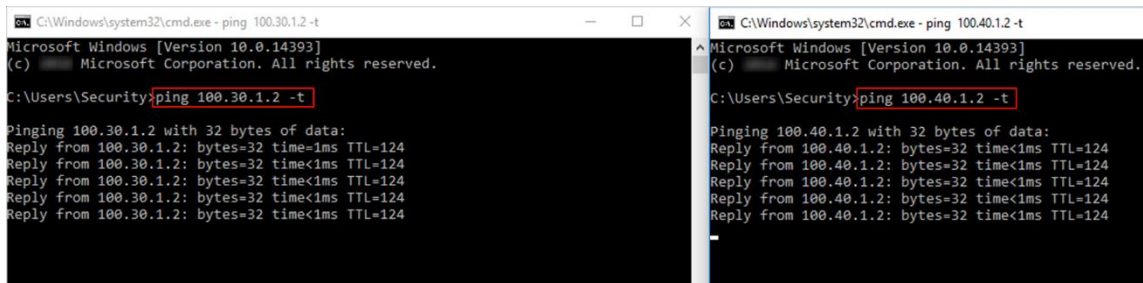


图5-9 PC1 业务流量模拟

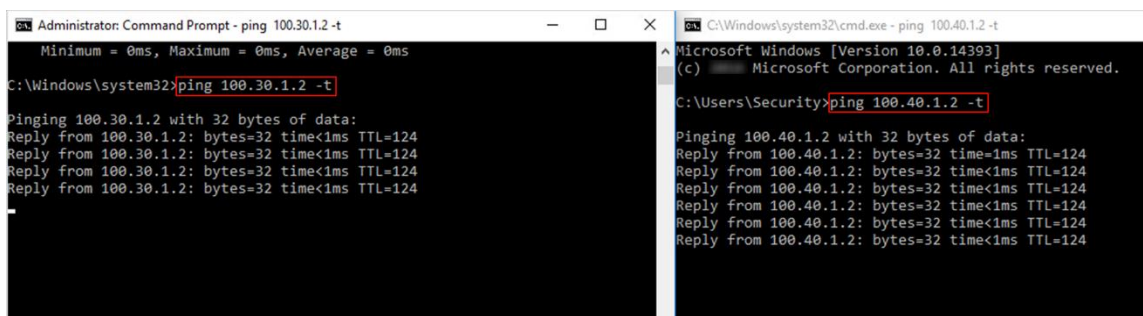


图5-10 PC2 业务流量模拟

上述业务模拟可以执行多次，模拟不同的内网访问 Internet 的业务流量，之后在 FW1 设备上执行以下操作，查看 FW1 设备两个上游业务接口的会话数占比，可以发现两个业务接口所承载的会话数量的比值大致为 1:2，符合业务接口的带宽比值。

说明：具体会话数占比会随着业务会话数的上涨无限接近理论值，因实验环境中无法模拟大量的业务流，所以实际会话数占比可能会和理论值有偏差，属正常现象。

```
HRP_M[FW1]display firewall session table interface ge 0/0/1
Current Total Sessions : 3
Slot: 0 CPU: 0
ICMP VPN: public --> public 10.5.1.2:63775 --> 100.30.1.2:2048
ICMP VPN: public --> public 172.17.10.100:1[10.3.1.2:2049] --> 100.30.1.2:2048
ICMP VPN: public --> public 172.17.20.100:1[10.3.1.2:2050] --> 100.40.1.2:2048
HRP_M[FW1]display firewall session table interface ge 0/0/2
Current Total Sessions : 5
Slot: 0 CPU: 0
ICMP VPN: public --> public 172.17.10.100:1[10.3.1.2:2049] --> 100.40.1.2:2048
udp VPN: public --> public 10.3.1.2:49172 --> 4.4.4.2:4784
ICMP VPN: public --> public 172.17.20.100:1[10.3.1.2:2050] --> 100.30.1.2:2048
ICMP VPN: public --> public 10.3.1.2:64141 --> 100.40.1.2:2048
ICMP VPN: public --> public 172.17.20.100:1[10.3.1.2:2049] --> 100.40.1.1:2048
HRP_M[FW1]
```

5.4 配置参考

5.4.1 FW1 配置

```
#
sysname FW1
#
healthcheck enable
healthcheck name isp-healthcheck
  destination 100.30.1.2 interface GE0/0/1 protocol icmp
  destination 100.40.1.2 interface GE0/0/2 protocol icmp
#
interface GE0/0/1
  undo shutdown
  ip address 10.5.1.2 255.255.255.252
  gateway 10.5.1.1
  bandwidth ingress 50000 threshold 90
  bandwidth egress 50000 threshold 90
#
interface GE0/0/2
  undo shutdown
  ip address 10.3.1.2 255.255.255.252
  gateway 10.3.1.1
  bandwidth ingress 100000 threshold 95
  bandwidth egress 100000 threshold 95
#
firewall zone untrust
  set priority 5
  add interface GE0/0/1
  add interface GE0/0/2
#
multi-interface
mode proportion-of-bandwidth
  healthcheck isp-healthcheck
  add interface GE0/0/1
  add interface GE0/0/2
#
nat-policy
  rule name trust-untrust
    source-zone trust
    destination-zone untrust
    action source-nat easy-ip
#
```

5.4.2 RT1 预配置

```
#
```

```
sysname RT1
#
interface GigabitEthernet0/0/1
 undo portswitch
#
interface GigabitEthernet0/0/1.2
 dot1q termination vid 2
 ip address 4.4.4.2 255.255.255.252
#
interface GigabitEthernet0/0/4
 undo portswitch
 ip address 10.3.1.1 255.255.255.252
#
ip route-static 0.0.0.0 0.0.0.0 4.4.4.1
#
```

5.4.3 RT2 预配置

```
#
sysname RT2
#
interface GigabitEthernet0/0/1
 undo portswitch
#
interface GigabitEthernet0/0/1.40
 dot1q termination vid 40
 ip address 3.3.3.2 255.255.255.252
#
interface GigabitEthernet0/0/3
 undo portswitch
 ip address 10.5.1.1 255.255.255.252
 ospf enable 1 area 0.0.0.0
#
ip route-static 0.0.0.0 0.0.0.0 3.3.3.1
#
```

5.4.4 SW1 预配置

```
#
sysname SW1
#
vlan batch 2 40 1000 2000
#
interface vlanif2
 ip address 4.4.4.1 255.255.255.252
#
interface vlanif40
 ip address 3.3.3.1 255.255.255.252
```

```
#
interface vlanif1000
 ip address 100.30.1.1 255.255.255.0
#
interface vlanif2000
 ip address 100.40.1.1 255.255.255.0
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 2 40
#
ip route-static 10.3.1.0 255.255.255.252 4.4.4.2
ip route-static 10.5.1.0 255.255.255.252 4.4.4.2
ip route-static 172.17.0.0 16 4.4.4.2
ip route-static 172.17.0.0 16 3.3.3.2 preference 70
#
interface GigabitEthernet0/0/13
 port link-type access
 port default vlan 1000
#
interface GigabitEthernet0/0/14
 port link-type access
 port default vlan 2000
#
```

5.4.5 Mirror-SW 预配置

```
#
sysname Mirror-SW
#
vlan batch 2 40
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 2 40
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 2 40
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 2 40
#
```

5.4.6 SW3 预配置

```
#
```

```
interface Vlanif34
 ip address 172.17.10.1 255.255.255.0
 ospf enable 1 area 0.0.0.0
#
interface Vlanif35
 ip address 172.17.20.1 255.255.255.0
 ospf enable 1 area 0.0.0.0
#
interface Vlanif40
 ip address 172.16.20.100 255.255.255.0
 ospf enable 1 area 0.0.0.0
#
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 40
#
interface GigabitEthernet0/0/13
 port link-type access
 port default vlan 34
#
interface GigabitEthernet0/0/14
 port link-type access
 port default vlan 35
#
```

5.5 思考题

如果现在需要根据链路权重将流量在出口链路上进行负载分担，如何实现？

参考答案：与基于带宽实现负载分担的配置思路不同的是，在配置全局选路策略时，配置智能选路方式为根据链路权重负载分担，指定 FW 设备与不同 ISP 网络直连的出接口作为智能选路成员接口，并为接口设置权重值。

6 IPsec 点到多点应用实验

6.1 实验介绍

6.1.1 关于本实验

某企业网络由总部和两个分部组成，出口网关均为防火墙，但是位于不同的地理区域。总部与分部之间需要跨 Internet 互访。为保证数据的安全性，现需要在总部和分部 1、分部 2 之间建立 IPsec VPN，用于加密不同站点间交互的业务数据。

6.1.2 实验目的

- 掌握 IPsec VPN 应用场景及点到多点部署流程。
- 掌握在 IPsec VPN 组网方案下，防火墙安全策略的配置细节。

6.1.3 实验组网介绍

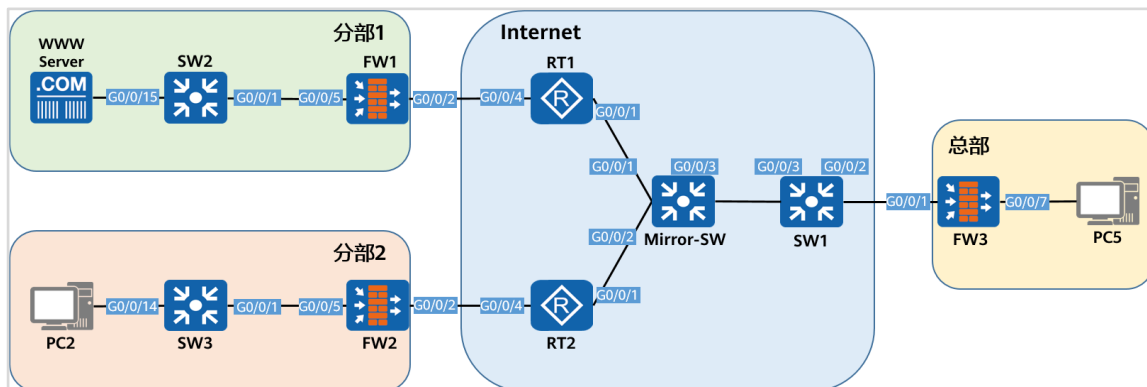


图6-1 IPsec VPN 点到多点应用实验拓扑

FW1 为企业分部 1 的出口网关，FW2 为企业分部 2 的出口网关，FW3 为企业总部的出口网关，使用 RT1、RT2、Mirror-SW 和 SW1 模拟 Internet。SW2 和 SW3 是接入层交换机，WWW Server、PC2 和 PC5 均为站点内终端设备。

分部网络规划：在 SW2 和 SW3 中，上下行端口采用 Access 的类型，将 PC 划分到对应的 VLAN。在 FW1 上配置 WWW Server 的网关、在 FW2 上配置 PC2 的网关。

Internet 区域网络规划：RT1、RT2 与 SW1 之间是三层网络（部署 OSPF），通过静态路由指向各站点出口 FW 设备，实现对站点内网络的访问，并将静态路由引入至 OSPF。

总部网络规划：PC5 业务网关部署在出口设备 FW3 上。

RT1、RT2、Mirror-SW、SW1、SW2 和 SW3 相关配置在本实验配置步骤中未体现，具体可参考“6.4 配置参考”相关设备预配置，本实验重点介绍 FW1、FW2 和 FW3 设备上关键配置。

6.1.4 实验规划

表6-1 设备接口规划表

设备	接口	接口性质	接口信息	说明
FW1	GE0/0/2	三层接口	10.3.1.2/30 安全区域: untrust	连接Internet的出接口， 与RT1互连
	GE0/0/5	三层接口	172.16.30.2/24 安全区域: trust	与SW2互连
FW2	GE0/0/2	三层接口	10.6.1.2/30 安全区域: untrust	连接Internet的出接口， 与RT1互连
	GE0/0/5	三层接口	172.16.40.2/24 安全区域: trust	与SW3互连
FW3	GE0/0/1	三层接口	100.1.1.8/24 安全区域: untrust	连接Internet的出接口， 与SW1互连
	GE0/0/7	三层接口	100.100.1.1/24 安全区域: trust	连接PC5
RT1	G0/0/1.2	三层子接口	4.4.4.2/30 终结VLAN2	与SW1的VLANIF2组成 直连网段
	G0/0/4	三层接口	10.3.1.1/30	与FW1互连
RT2	G0/0/1.40	三层子接口	3.3.3.2/30 终结VLAN40	与SW1的VLANIF40组成 直连网段
	G0/0/4	三层接口	10.6.1.1/30	与FW2互连
SW1	G0/0/2	Access	PVID: 1	与FW3互连
	G0/0/3	Trunk	PVID: 1 Allow-pass VLAN: 2, 40	与Mirror-SW互连
	VLANIF1	三层接口	100.1.1.1/24	与FW3接口组成直连网 段

	VLNAIF2	三层接口	4.4.4.1/30	与RT1接口组成直连网段
	VLNAIF40	三层接口	3.3.3.1/30	与RT2接口组成直连网段
SW2	G0/0/1	Access	PVID: 30	与FW1互连
	G0/0/15	Access	PVID: 30	连接WWW Server
SW3	G0/0/1	Access	PVID: 40	与FW2互连
	G0/0/14	Access	PVID: 40	连接PC2
Mirror-SW	G0/0/1	Trunk	PVID: 1	互连接口
	G0/0/2		Allow-pass VLAN:	
	G0/0/3		2, 40	
WWW Server	Ethernet0	三层	172.16.30.10/24 网关: 172.16.30.2/24	终端
PC2	Ethernet0	三层	172.16.40.10/24 网关: 172.16.40.2/24	终端
PC5	Ethernet0	三层	100.100.1.10/24 网关: 100.100.1.1/24	终端

6.2 实验任务配置

6.2.1 配置思路

- 1.设备基础 IP 地址配置，FW1、FW2、FW3 接口的 IP 地址和安全域请参考上表配置，WWW Server、PC2 和 PC5 地址及网关请参考上表配置，SW1、SW2、SW3、Mirror-SW、RT1 和 RT2 的配置请参考章节末的“6.4 配置参考”中的预配。
- 2.配置 untrust 和 local 区域间的双向互通安全策略，确保 IPsec VPN 协商报文可正常交互。
- 3.配置总部与分部之间的 IPsec 相关参数，建立分部与总部的 IPsec VPN。
- 4.配置分部与总部间业务安全策略，允许 WWW Server、PC2 和 PC5 间互访。

6.2.2 配置步骤 - CLI

步骤 1 网络基本参数配置

参考“表 6-1”规划数据，完成网络基本参数配置。其中 RT1、RT2、SW1、SW2、SW3 和 Mirror-SW 已预配，具体可参考“6.4 配置参考”。终端设备的网络参数按照“表 6-1”数据规划配置即可。

因在之前的“实验 1”已将 FW1 和 FW2 部署为主备模式的双机热备系统，需要拆除双机热备系统，并关闭本实验暂时用不到的业务接口，同时删除之前在 FW1 和 FW2 设备上部署的 OSPF。

```
HRP_M[FW1]undo hrp enable
Warning: Disabling the hot standby function will interrupt related services. Are you sure you want to
continue? [Y/N]:y
[FW1]int Eth-Trunk 0
[FW1-Eth-Trunk0]shutdown
Warning: This interface is configured as HRP heartbeat interface.
Continue? [Y/N]:y
[FW1-Eth-Trunk0]quit
[FW1]int g0/0/6
[FW1-GE0/0/6]shutdown
[FW1-GE0/0/6]quit
[FW1]int g0/0/1
[FW1-GE0/0/1]shutdown
[FW1-GE0/0/1]quit
[FW1]undo ospf 1
Warning: The OSPF process will be deleted. Continue? [Y/N]:y
[FW1]
```

```
HRP_M[FW2]undo hrp enable
Warning: Disabling the hot standby function will interrupt related services. Are you sure you want to
continue? [Y/N]:y
[FW2]int Eth-Trunk 0
[FW2-Eth-Trunk0]shutdown
Warning: This interface is configured as HRP heartbeat interface.
Continue? [Y/N]:y
[FW2-Eth-Trunk0]quit
[FW2]int g0/0/6
[FW2-GE0/0/6]shutdown
[FW2-GE0/0/6]quit
[FW2]int g0/0/1
[FW2-GE0/0/1]shutdown
[FW2-GE0/0/1]quit
[FW2]undo ospf 1
Warning: The OSPF process will be deleted. Continue? [Y/N]:y
[FW2] [FW2]interface ge0/0/5
[FW2-GE0/0/5]ip add 172.16.40.2 24
[FW2-GE0/0/5]quit
[FW2]
```

完成上述操作后，剩余基础网络配置可以直接复用之前在“实验 1”中配置的 FW1 和 FW2 设备业务接口的基础配置，此处无需再次配置。

因之前“实验 3”中在 FW3 设备上部署了虚拟系统相关配置，需要删除之前创建的虚拟系统，并重新配置业务接口的 IP 地址和安全区域。

```
[FW3]undo vsys name vsysa
Warning: All related configurations will be deleted.Please select [Y/N]:y
[FW3]undo vsys name vsysb
Warning: All related configurations will be deleted.Please select [Y/N]:y
[FW3]int g0/0/7
[FW3-GE0/0/7]ip add 100.100.1.1 24
[FW3-GE0/0/7]quit
[FW3]
[FW3]firewall zone trust
[FW3-zone-trust]ad interface g0/0/7
[FW3-zone-trust]quit
[FW3]
```

完成上述操作后，剩余基础网络配置可以直接复用之前在“实验 3”中配置的 FW3 设备业务接口的基础配置，此处无需再次配置。

步骤 2 防火墙路由配置

配置 FW1、FW2 和 FW3 到 Internet 的缺省路由。

```
[FW1] ip route-static 0.0.0.0 0.0.0.0 10.3.1.1
```

```
[FW2] ip route-static 0.0.0.0 0.0.0.0 10.6.1.1
```

```
[FW3] ip route-static 0.0.0.0 0.0.0.0 100.1.1.1
```

步骤 3 配置安全策略

配置 FW1、FW2 和 FW3 设备的域间安全策略，放行 local 和 untrust 区域之间的双向流量，确保 IPSec VPN 协商报文可正常交互。

```
[FW1] security-policy
[FW1-policy-security] rule name untrust-local
[FW1-policy-security-rule-untrust-local] source-zone untrust
[FW1-policy-security-rule-untrust-local] source-zone local
[FW1-policy-security-rule-untrust-local] destination-zone untrust
[FW1-policy-security-rule-untrust-local] destination-zone local
[FW1-policy-security-rule-untrust-local] action permit
[FW1-policy-security-rule-untrust-local] quit
[FW1-policy-security] quit
```

```
[FW2]security-policy
[FW2-policy-security]rule name untrust-local
```

```
[FW2-policy-security-rule-untrust-local] source-zone untrust
[FW2-policy-security-rule-untrust-local] source-zone local
[FW2-policy-security-rule-untrust-local] destination-zone untrust
[FW2-policy-security-rule-untrust-local] destination-zone local
[FW2-policy-security-rule-untrust-local] action permit
[FW2-policy-security-rule-untrust-local] quit
[FW2-policy-security]quit
[FW2]
```

```
[FW3]security-policy
[FW3-policy-security]rule name untrust-local
[FW3-policy-security-rule-untrust-local] source-zone untrust
[FW3-policy-security-rule-untrust-local] source-zone local
[FW3-policy-security-rule-untrust-local] destination-zone untrust
[FW3-policy-security-rule-untrust-local] destination-zone local
[FW3-policy-security-rule-untrust-local] action permit
[FW3-policy-security-rule-untrust-local] quit
[FW3-policy-security]quit
[FW3]
```

步骤 4 配置 IPsec VPN

本案例中有多个分部，因此在总部出口设备 FW3 上采用模板的方式建立 IPsec VPN，在两个分部出口设备 FW1 和 FW2 上使用 ISAKMP 方式建立 IPsec VPN。

在 FW1 上创建 ACL 3500 匹配分部 FW1 到总部 FW3 的感兴趣流。

```
[FW1]acl number 3500
[FW1-acl4-advance-3500] rule permit ip source 172.16.30.0 0.0.0.255 destination 100.100.1.0 0.0.0.255
[FW1-acl4-advance-3500] quit
[FW1]
```

在 FW1 上创建 IPsec 安全提议。

```
[FW1] ipsec proposal 1
Warning: GCM/GMAC are authenticated encryption algorithms, esp authentication config is ignored.
[FW1-ipsec-proposal-1] esp authentication-algorithm sha2-256
[FW1-ipsec-proposal-1] esp encryption-algorithm aes-256-gcm-128
[FW1-ipsec-proposal-1] quit
```

在 FW1 上配置 IKE 安全提议。

```
[FW1] ike proposal 1
[FW1-ike-proposal-1] encryption-algorithm aes-gcm-256
[FW1-ike-proposal-1] dh group14
[FW1-ike-proposal-1] authentication-algorithm sha2-256
[FW1-ike-proposal-1] authentication-method pre-share
[FW1-ike-proposal-1] integrity-algorithm hmac-sha2-256
[FW1-ike-proposal-1] prf hmac-sha2-256
[FW1-ike-proposal-1] quit
```

在 FW1 上配置 IKE 对等体。

```
[FW1] ike peer 1
[FW1-ike-peer-1] pre-shared-key Huawei@123
[FW1-ike-peer-1] remote-address 100.1.1.8
[FW1-ike-peer-1] ike-proposal 1
[FW1-ike-peer-1] quit
[FW1]
```

配置 IPsec 策略。

```
[FW1] ipsec policy 1 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.
[FW1-ipsec-policy-isakmp-1-10] ike-peer 1
[FW1-ipsec-policy-isakmp-1-10] proposal 1
[FW1-ipsec-policy-isakmp-1-10] security acl 3500
[FW1-ipsec-policy-isakmp-1-10] quit
[FW1]
```

在 FW1 的出接口调用 IPsec 策略。

```
[FW1] interface GE 0/0/2
[FW1-GE0/0/2] ipsec policy 1
[FW1-GE0/0/2] quit
[FW1]
```

在 FW2 上创建 ACL 3500 匹配分部 FW2 到总部 FW3 的感兴趣流。

```
[FW2]acl number 3500
[FW2-acl4-advance-3500] rule permit ip source 172.16.40.0 0.0.0.255 destination 100.100.1.0 0.0.0.255
[FW2-acl4-advance-3500] quit
[FW2]
```

在 FW2 上创建 IPsec 安全提议。

```
[FW2]ipsec proposal 1
Warning: GCM/GMAC are authenticated encryption algorithms, esp authentication config is ignored.
[FW2-ipsec-proposal-1] esp authentication-algorithm sha2-256
[FW2-ipsec-proposal-1] esp encryption-algorithm aes-256-gcm-128
[FW2-ipsec-proposal-1] quit
[FW2]
```

在 FW2 上配置 IKE 安全提议。

```
[FW2]ike proposal 1
[FW2-ike-proposal-1] encryption-algorithm aes-gcm-256
[FW2-ike-proposal-1] dh group14
[FW2-ike-proposal-1] authentication-algorithm sha2-256
[FW2-ike-proposal-1] authentication-method pre-share
[FW2-ike-proposal-1] integrity-algorithm hmac-sha2-256
[FW2-ike-proposal-1] prf hmac-sha2-256
[FW2-ike-proposal-1] quit
[FW2]
```

在 FW2 上配置 IKE 对等体。

```
[FW2] ike peer 1
[FW2-ike-peer-1] pre-shared-key Huawei@123
[FW2-ike-peer-1] remote-address 100.1.1.8
[FW2-ike-peer-1] ike-proposal 1
[FW2-ike-peer-1] quit
[FW2]
```

配置 IPsec 策略。

```
[FW2] ipsec policy 1 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.
[FW2-ipsec-policy-isakmp-1-10] ike-peer 1
[FW2-ipsec-policy-isakmp-1-10] proposal 1
[FW2-ipsec-policy-isakmp-1-10] security acl 3500
[FW2-ipsec-policy-isakmp-1-10] quit
[FW2]
```

在 FW2 的出接口调用 IPsec 策略。

```
[FW2] interface GE 0/0/2
[FW2-GE0/0/2] ipsec policy 1
[FW2-GE0/0/2] quit
[FW2]
```

在 FW3 上创建 ACL 3500 匹配总部 FW3 到分部 FW1、FW2 的感兴趣流。

```
[FW3] acl number 3500
[FW3-acl-adv-3500] rule permit ip source 100.100.1.0 0.0.0.255 destination 172.16.30.0 0.0.0.255
[FW3-acl-adv-3500] rule permit ip source 100.100.1.0 0.0.0.255 destination 172.16.40.0 0.0.0.255
[FW3-acl-adv-3500] quit
```

在 FW3 上创建 IPsec 安全提议。

```
[FW3] ipsec proposal 1
Warning: GCM/GMAC are authenticated encryption algorithms, esp authentication config is ignored.
[FW3-ipsec-proposal-1] esp authentication-algorithm sha2-256
[FW3-ipsec-proposal-1] esp encryption-algorithm aes-256-gcm-128
[FW3-ipsec-proposal-1] quit
[FW3]
```

在 FW3 上配置 IKE 安全提议。

```
[FW3] ike proposal 1
[FW3-ike-proposal-1] encryption-algorithm aes-gcm-256
[FW3-ike-proposal-1] dh group14
[FW3-ike-proposal-1] authentication-algorithm sha2-256
[FW3-ike-proposal-1] authentication-method pre-share
[FW3-ike-proposal-1] integrity-algorithm hmac-sha2-256
[FW3-ike-proposal-1] prf hmac-sha2-256
[FW3-ike-proposal-1] quit
[FW3]
```

在 FW3 上配置 IKE 对等体。

```
[FW3] ike peer 1
[FW3-ike-peer-1] pre-shared-key Huawei@123
[FW3-ike-peer-1] ike-proposal 1
[FW3-ike-peer-1] quit
[FW3]
```

配置 IPsec 模板，在模板中调用感兴趣流、IPsec 安全提议和 IKE 对等体。

```
[FW3] ipsec policy-template map1 10
[FW3-ipsec-policy-templet-map1-10] security acl 3500
[FW3-ipsec-policy-templet-map1-10] ike-peer 1
[FW3-ipsec-policy-templet-map1-10] proposal 1
[FW3-ipsec-policy-templet-map1-10] quit
[FW3]
```

配置策略模板方式的 IPsec 策略。

```
[FW3] ipsec policy 1 10 isakmp template map1
```

在 FW3 的出接口调用 IPsec 策略。

```
[FW3] interface GE0/0/1
[FW3-GE0/0/1] ipsec policy 1
[FW3-GE0/0/1] quit
[FW3]
```

步骤 5 配置业务安全策略

配置 FW1、FW2 和 FW3 设备的域间安全策略，放行站点间交互的业务流量。

配置 FW1 中 trust 区域与 untrust 区域的安全策略。

```
[FW1] security-policy
[FW1-policy-security] rule name IPSec_OA
[FW1-policy-security-rule-IPSec_OA] source-zone trust untrust
[FW1-policy-security-rule-IPSec_OA] destination-zone untrust trust
[FW1-policy-security-rule-IPSec_OA] source-address 172.16.30.0 mask 255.255.255.0
[FW1-policy-security-rule-IPSec_OA] source-address 100.100.1.0 mask 255.255.255.0
[FW1-policy-security-rule-IPSec_OA] destination-address 100.100.1.0 mask 255.255.255.0
[FW1-policy-security-rule-IPSec_OA] destination-address 172.16.30.0 mask 255.255.255.0
[FW1-policy-security-rule-IPSec_OA] action permit
[FW1-policy-security-rule-IPSec_OA] quit
[FW1-policy-security] quit
[FW1]
```

```
[FW2] security-policy
[FW2-policy-security] rule name IPSec_OA
[FW2-policy-security-rule-IPSec_OA] source-zone trust untrust
[FW2-policy-security-rule-IPSec_OA] destination-zone untrust trust
[FW2-policy-security-rule-IPSec_OA] source-address 172.16.40.0 mask 255.255.255.0
[FW2-policy-security-rule-IPSec_OA] source-address 100.100.1.0 mask 255.255.255.0
[FW2-policy-security-rule-IPSec_OA] destination-address 100.100.1.0 mask 255.255.255.0
```

```
[FW2-policy-security-rule-IPSec_OA] destination-address 172.16.40.0 mask 255.255.255.0
[FW2-policy-security-rule-IPSec_OA] action permit
[FW2-policy-security-rule-IPSec_OA] quit
[FW2-policy-security] quit
[FW2]
```

```
[FW3] security-policy
[FW3-policy-security] rule name IPSec_OA
[FW3-policy-security-rule-IPSec_OA] source-zone trust untrust
[FW3-policy-security-rule-IPSec_OA] destination-zone untrust trust
[FW3-policy-security-rule-IPSec_OA] source-address 172.16.40.0 mask 255.255.255.0
[FW3-policy-security-rule-IPSec_OA] source-address 172.16.30.0 mask 255.255.255.0
[FW3-policy-security-rule-IPSec_OA] source-address 100.100.1.0 mask 255.255.255.0
[FW3-policy-security-rule-IPSec_OA] destination-address 100.100.1.0 mask 255.255.255.0
[FW3-policy-security-rule-IPSec_OA] destination-address 172.16.40.0 mask 255.255.255.0
[FW3-policy-security-rule-IPSec_OA] destination-address 172.16.30.0 mask 255.255.255.0
[FW3-policy-security-rule-IPSec_OA] action permit
[FW3-policy-security-rule-IPSec_OA] quit
[FW3-policy-security] quit
[FW3]
```

步骤 6 配置 NAT 穿越

因之前的实验在 FW 设备上均有部署 NAT 策略，为避免 NAT 转换影响 IPSec VPN 业务正常交互，需要针对 IPSec VPN 交互的业务流量进行免 NAT 转换的操作。

```
[FW1]nat-policy
[FW1-policy-nat]rule name no-nat
[FW1-policy-nat-rule-no-nat]source-zone trust
[FW1-policy-nat-rule-no-nat]source-address 172.16.30.0 24
[FW1-policy-nat-rule-no-nat]destination-zone untrust
[FW1-policy-nat-rule-no-nat]destination-address 100.100.1.0 24
[FW1-policy-nat-rule-no-nat]action no-nat
[FW1-policy-nat-rule-no-nat]quit
[FW1-policy-nat]rule move no-nat top
[FW1-policy-nat]quit
[FW1]
```

```
[FW2]nat-policy
[FW2-policy-nat]rule name no-nat
[FW2-policy-nat-rule-no-nat]source-zone trust
[FW2-policy-nat-rule-no-nat]source-address 172.16.40.0 24
[FW2-policy-nat-rule-no-nat]destination-zone untrust
[FW2-policy-nat-rule-no-nat]destination-address 100.100.1.0 24
[FW2-policy-nat-rule-no-nat]action no-nat
[FW2-policy-nat-rule-no-nat]quit
[FW2-policy-nat]rule move no-nat top
```



```
[FW2-policy-nat]quit
[FW2]
```

```
[FW3]nat-policy
[FW3-policy-nat]rule name no-nat
[FW3-policy-nat-rule-no-nat]source-zone trust
[FW3-policy-nat-rule-no-nat]source-address 100.100.1.0 24
[FW3-policy-nat-rule-no-nat]destination-zone untrust
[FW3-policy-nat-rule-no-nat]destination-address 172.16.40.0 24
[FW3-policy-nat-rule-no-nat]destination-address 172.16.30.0 24
[FW3-policy-nat-rule-no-nat]action no-nat
[FW3-policy-nat-rule-no-nat]quit
[FW3-policy-nat]rule move no-nat top
[FW3-policy-nat]quit
[FW3]
```

6.2.3 配置步骤 - Web

步骤 1 网络基本参数配置

按照“表 6-1”中的规划数据，完成网络基本参数配置。其中 RT1、RT2、SW1、SW2、SW3 和 Mirror-SW 设备已预配，具体可参考“6.4 配置参考”。

登录 FW1 设备 Web 管理界面，选择“网络 > 接口”进入接口列表界面，执行以下操作，完成设备业务接口基础配置。



USG6525F

面板 监控 策略 对象 **网络** 系统

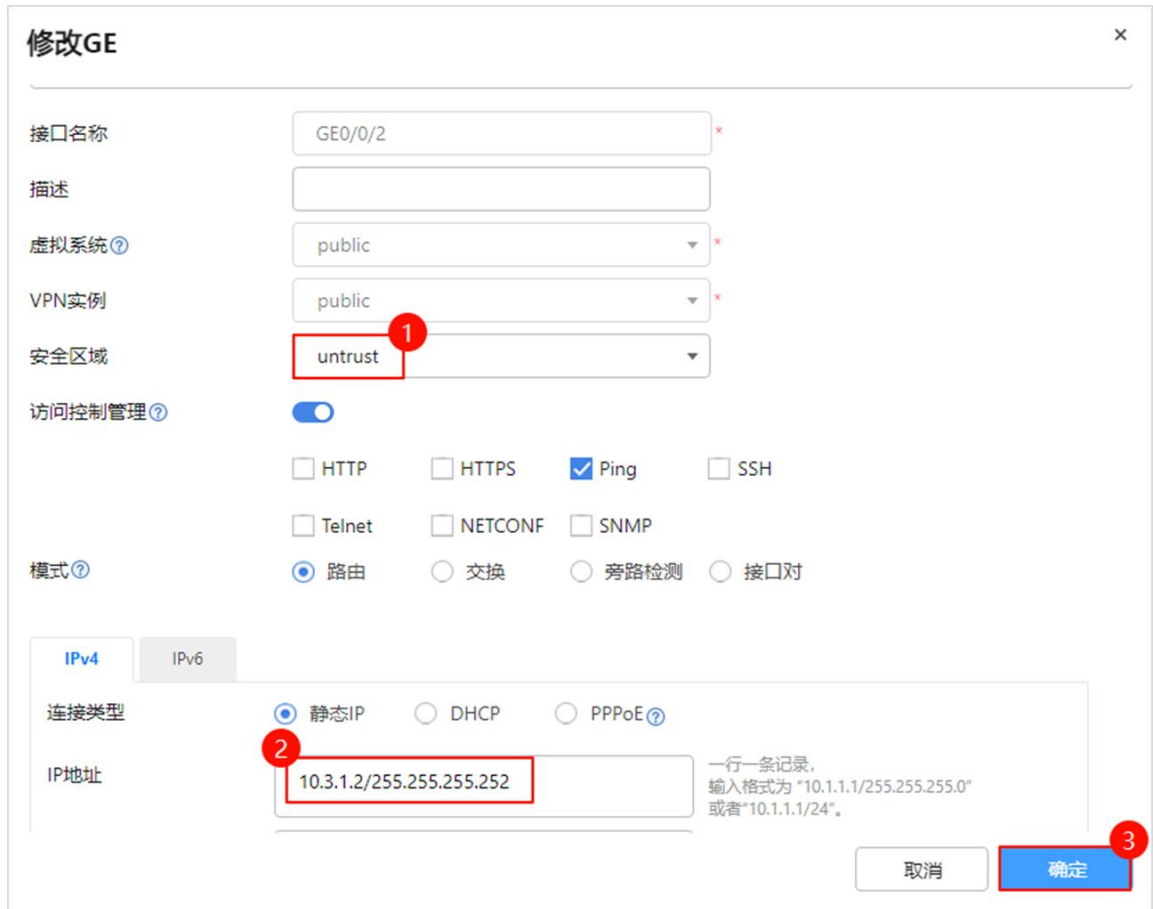
接口

接口列表

新建 删除

接口名称	描述	安全区域	虚拟系统/VPN实例	IP地址
MEth0/0/0		-- NONE --	_management_vpn_	192.168.20.7
Virtual-if0		-- NONE --	public	---
GE0/0/0		-- NONE --	public	---
GE0/0/1				
GE0/0/2				
GE0/0/5				
GE0/0/6				

图6-2 进入 FW1 设备 GE0/0/2 接口配置界面



修改GE

接口名称: GE0/0/2

描述:

虚拟系统: public

VPN实例: public

安全区域: untrust

访问控制管理: ☒

HTTP ☐ HTTPS ☐ Ping ☒ SSH ☐

Telnet ☐ NETCONF ☐ SNMP ☐

模式: ☒ 路由 ☐ 交换 ☐ 旁路检测 ☐ 接口对

IPv4 IPv6

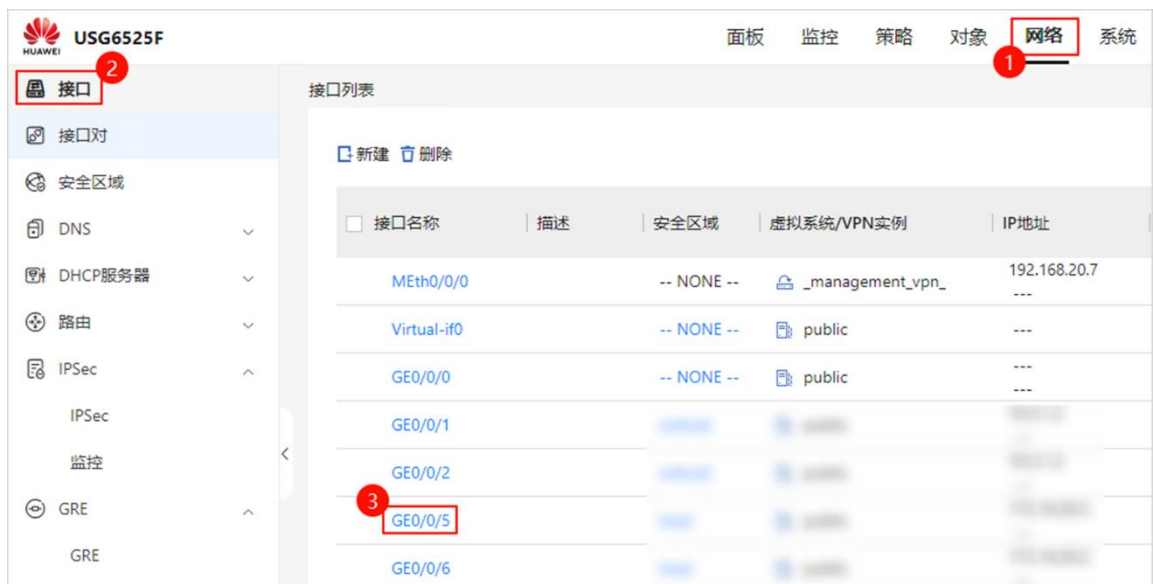
连接类型: ☒ 静态IP ☐ DHCP ☐ PPPoE

IP地址: 10.3.1.2/255.255.255.252

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"。

取消 确定

图6-3 FW1 设备 GE0/0/2 接口基础配置



USG6525F

面板 监控 策略 对象 网络 系统

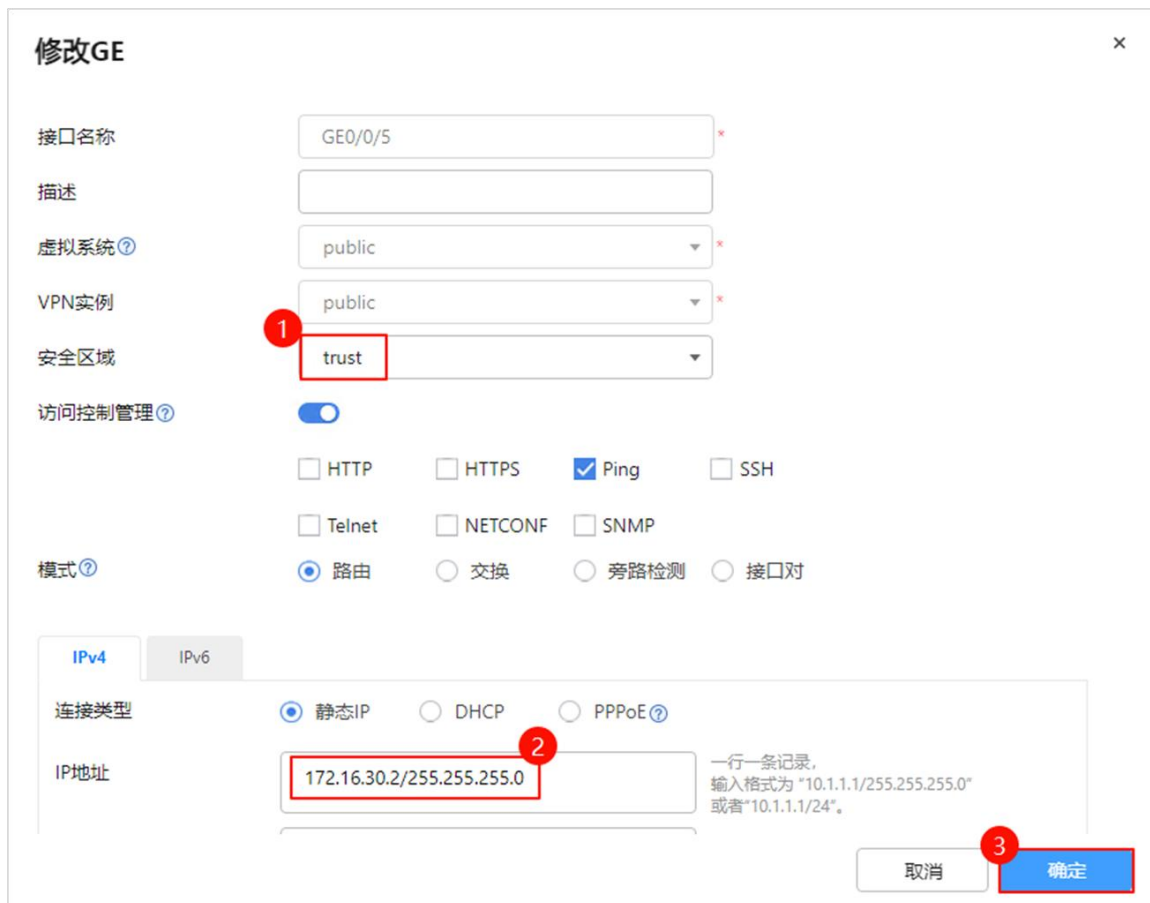
接口

接口列表

新建 删除

接口名称	描述	安全区域	虚拟系统/VPN实例	IP地址
MEth0/0/0		-- NONE --	_management_vpn_	192.168.20.7
Virtual-if0		-- NONE --	public	---
GE0/0/0		-- NONE --	public	---
GE0/0/1				
GE0/0/2				
GE0/0/5				
GE0/0/6				

图6-4 进入 FW1 设备 GE0/0/5 接口配置界面



修改GE

接口名称: GE0/0/5

描述:

虚拟系统: public

VPN实例: public

安全区域: trust

访问控制管理: ☒

☐ HTTP
 ☐ HTTPS
 ☒ Ping
 ☐ SSH

☐ Telnet
 ☐ NETCONF
 ☐ SNMP

模式: ☒ 路由 ☐ 交换 ☐ 旁路检测 ☐ 接口对

IPv4 IPv6

连接类型: ☒ 静态IP ☐ DHCP ☐ PPPoE

IP地址: 172.16.30.2/255.255.255.0

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"。

取消 确定

图6-5 FW1 设备 GE0/0/5 接口基础配置

FW2 和 FW3 设备业务接口配置步骤同上，配置参数详见“表 6-1”，此处不再赘述。

步骤 2 防火墙路由配置

在 FW1 设备 Web 管理界面选择“网络 > 路由 > 静态路由”，执行以下操作，创建到 Internet 的缺省路由。



图6-6 FW1 设备缺省路由配置

使用同样操作步骤为 FW2 和 FW3 设备创建缺省路由。

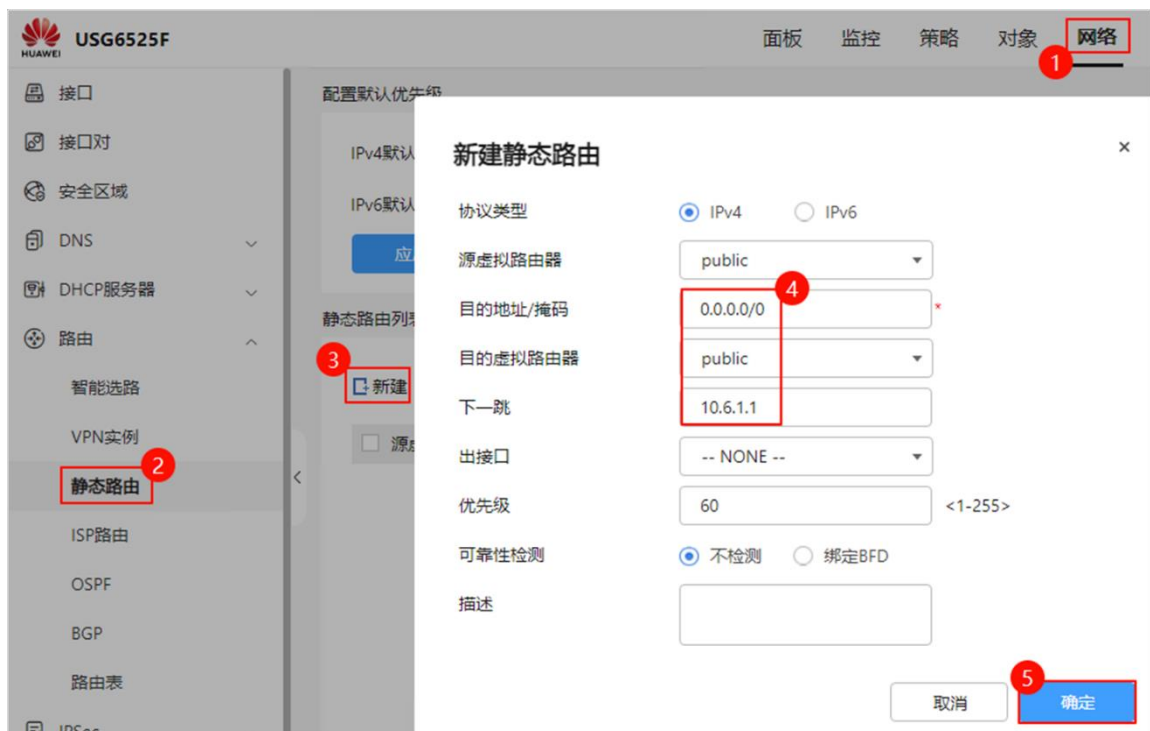


图6-7 FW2 设备缺省路由配置

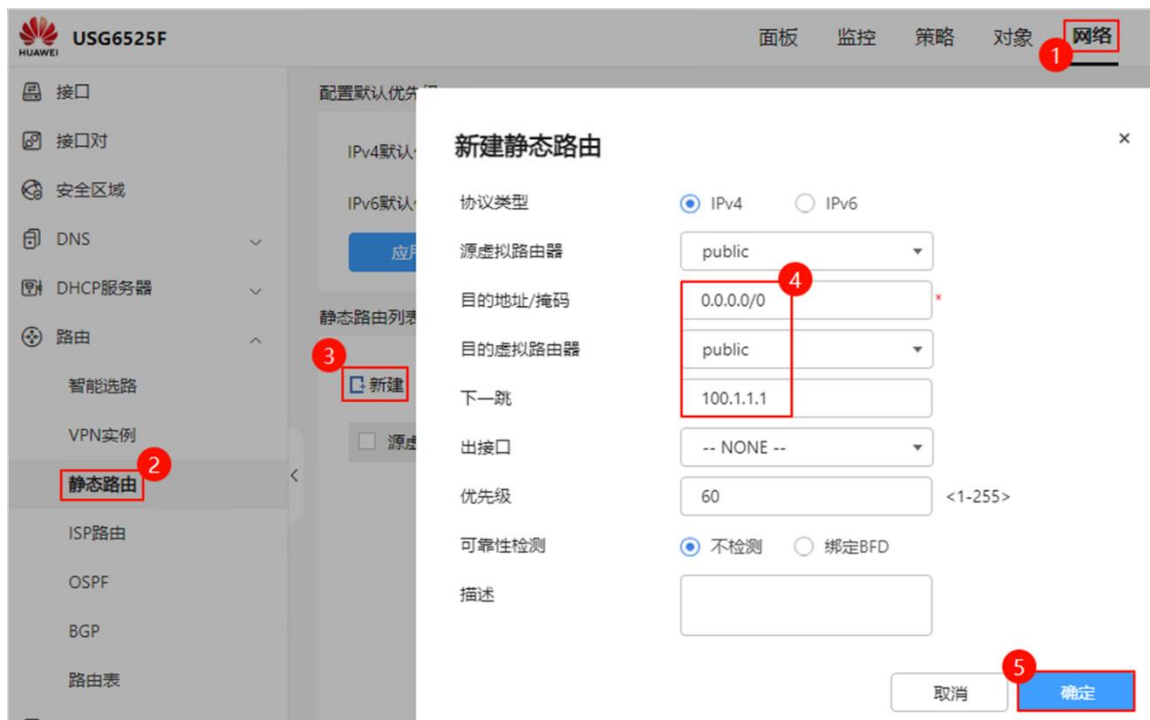


图6-8 FW3 设备缺省路由配置

步骤 3 配置安全策略

配置 FW1、FW2 和 FW3 设备的域间安全策略，放行 local 和 untrust 区域之间的双向流量，确保 IPsec VPN 协商报文可正常交互。

在 FW1 设备 Web 管理界面选择“策略 > 安全策略 > 安全策略”，新建如下安全策略。

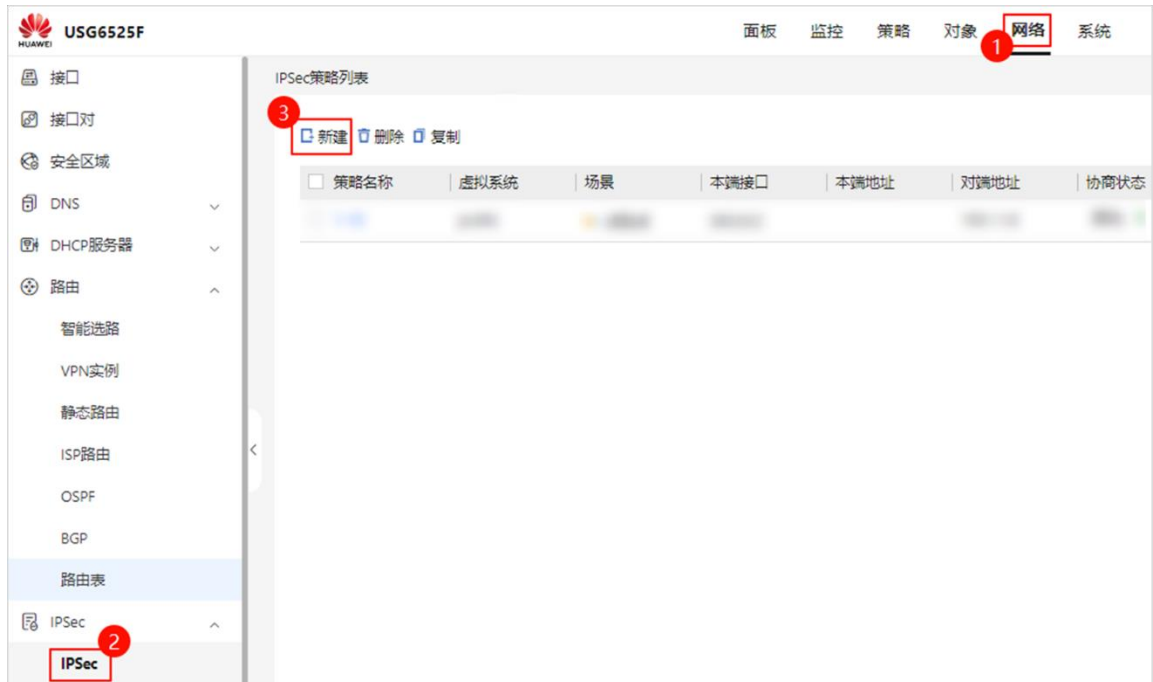


图6-10 进入 FW1 设备 IPsec 策略配置界面



图6-11 FW1 设备选择 IPSec 策略场景

场景选择

基本配置

定义数据流

安全提议

虚拟系统

策略名称

本端接口

本端地址

对端地址

认证方式

预共享密钥

本端ID

对端ID

协商报文路由注入

public

1-10

GE0/0/2

10.3.1.2

100.1.1.8

正在检查路由

提示：如果修改了本端或对端地址，需要同步调整安全策略配置，以保证IPSec隧道可以正常协商。

预共享密钥

RSA签名

..... Huawei@123

IP地址

接受任意对端ID

取消

上一步

下一步

图6-12 FW1 设备 IPsec 基础参数配置

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

1

新建

删除

插入

查询

☐	源地址	目的地址	协议	源端口	目的端...	动作	编辑
☐	172.16.30.0/255.255.255.0	100.100.1.0/255.255.255.0	any	any	any	加密	

2
 |

共 1 条

<

1

>

50条/页

前往

1

页

反向路由注入
☐

取消

上一步

3

下一步

图6-13 FW1 设备 IPsec 加密数据流配置



场景选择 > 基本配置 > 定义数据流 > 安全提议

第一阶段 (IKE)

加密算法 ☒ AES-GCM-256 ☐ AES-GCM-192
☐ AES-GCM-128 ☐ AES-CBC-256
☐ AES-CBC-192 ☐ AES-CBC-128
☐ 3DES ☐ DES

完整性算法 ☐ SHA2-512 ☐ SHA2-384 ☒ SHA2-256 ☐ SHA1
☐ MD5 ☐ AES

PRF算法 ☐ SHA2-512 ☐ SHA2-384 ☒ SHA2-256 ☐ SHA1
☐ MD5 ☐ AES-128

☒ 高级特性

第二阶段 (IPSec)

封装模式 ☐ 自动 ☐ 传输模式 ☒ 隧道模式

安全协议 ☒ ESP ☐ AH ☐ AH-ESP

ESP加密算法 ☒ GCM256 ☐ GCM192 ☐ GCM128 ☐ GMAC256
☐ GMAC192 ☐ GMAC128 ☐ AES-256 ☐ AES-192
☐ AES-128 ☐ 3DES ☐ DES

ESP认证算法 ☐ SHA2-512 ☐ SHA2-384 ☒ SHA2-256 ☐ SHA1
☐ MD5

取消 上一步 完成

图6-14 FW1 设备安全提议配置

在 FW2 设备 Web 管理界面选择“网络 > IPsec > IPsec > 新建”，执行以下操作，完成 IPsec VPN 相关配置。

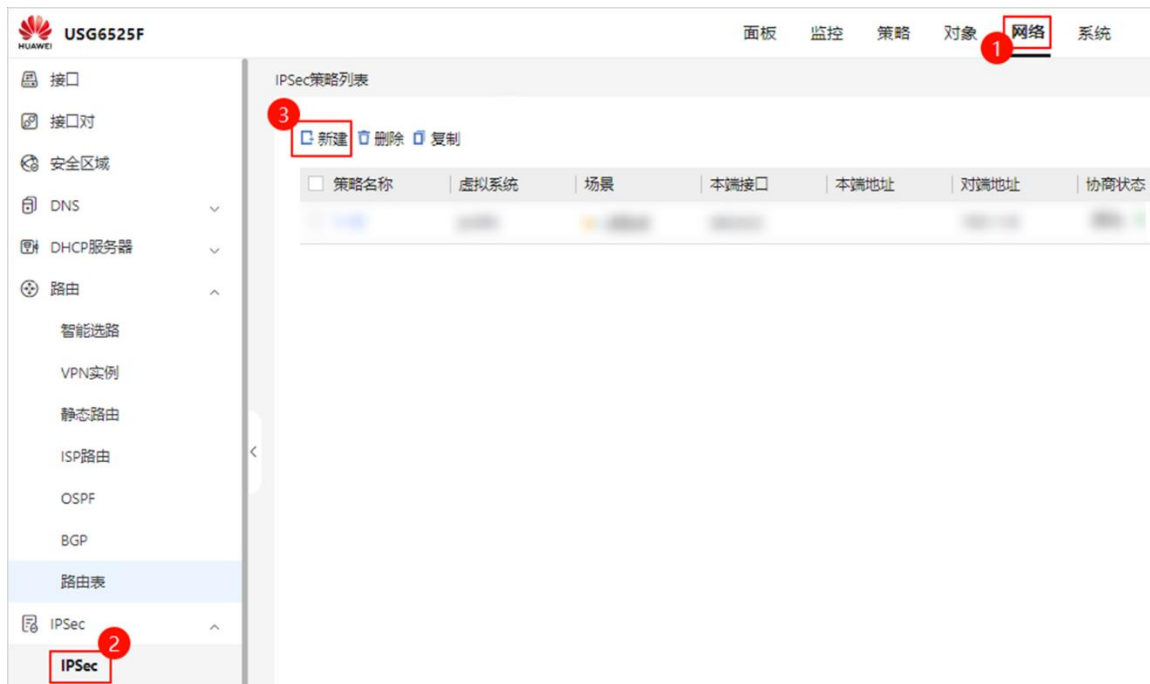


图6-15 进入 FW2 设备 IPsec 策略配置界面



图6-16 FW2 设备选择 IPSec 策略场景

场景选择

基本配置

定义数据流

安全提议

虚拟系统

策略名称

本端接口 ?

本端地址 ?

对端地址

认证方式

预共享密钥

本端ID ?

对端ID

协商报文路由注入 ?

public

1-10

GE0/0/2

10.6.1.2

100.1.1.8

☒ 预共享密钥 ☐ RSA签名

..... Huawei@123

IP地址

接受任意对端ID

☐

正在检查路由

提示: 如果修改了本端或对端地址, 需要同步调整安全策略配置, 以保证IPSec隧道可以正常协商。

取消

上一步

下一步

图6-17 FW2 设备 IPSec 基础参数配置

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

1

新建

删除

插入

C

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
☐ 172.16.40.0/255.255.255.0	100.100.1.0/255.255.255.0	any	any	any	2 加密	

共1条

<

1

>

50条/页

前往

1

页

反向路由注入?

☐

取消

上一步

3 下一步

图6-18 FW2 设备 IPsec 加密数据流配置

场景选择 > 基本配置 > 定义数据流 > 安全提议

第一阶段 (IKE)

加密算法 ☒ AES-GCM-256 ☐ AES-GCM-192
☐ AES-GCM-128 ☐ AES-CBC-256
☐ AES-CBC-192 ☐ AES-CBC-128
☐ 3DES ☐ DES

完整性算法 ☐ SHA2-512 ☐ SHA2-384 ☒ SHA2-256 ☐ SHA1
☐ MD5 ☐ AES

PRF算法 ☐ SHA2-512 ☐ SHA2-384 ☒ SHA2-256 ☐ SHA1
☐ MD5 ☐ AES-128

☒ 高级特性

第二阶段 (IPSec)

封装模式 ☐ 自动 ☐ 传输模式 ☒ 隧道模式

安全协议 ☒ ESP ☐ AH ☐ AH-ESP

ESP加密算法 ☒ GCM256 ☐ GCM192 ☐ GCM128 ☐ GMAC256
☐ GMAC192 ☐ GMAC128 ☐ AES-256 ☐ AES-192
☐ AES-128 ☐ 3DES ☐ DES

ESP认证算法 ☐ SHA2-512 ☐ SHA2-384 ☒ SHA2-256 ☐ SHA1
☐ MD5

取消 上一步 完成

图6-19 FW2 设备安全提议配置

在 FW3 设备 Web 管理界面选择“网络 > IPsec > IPsec > 新建”，执行以下操作，完成 IPsec VPN 相关配置。

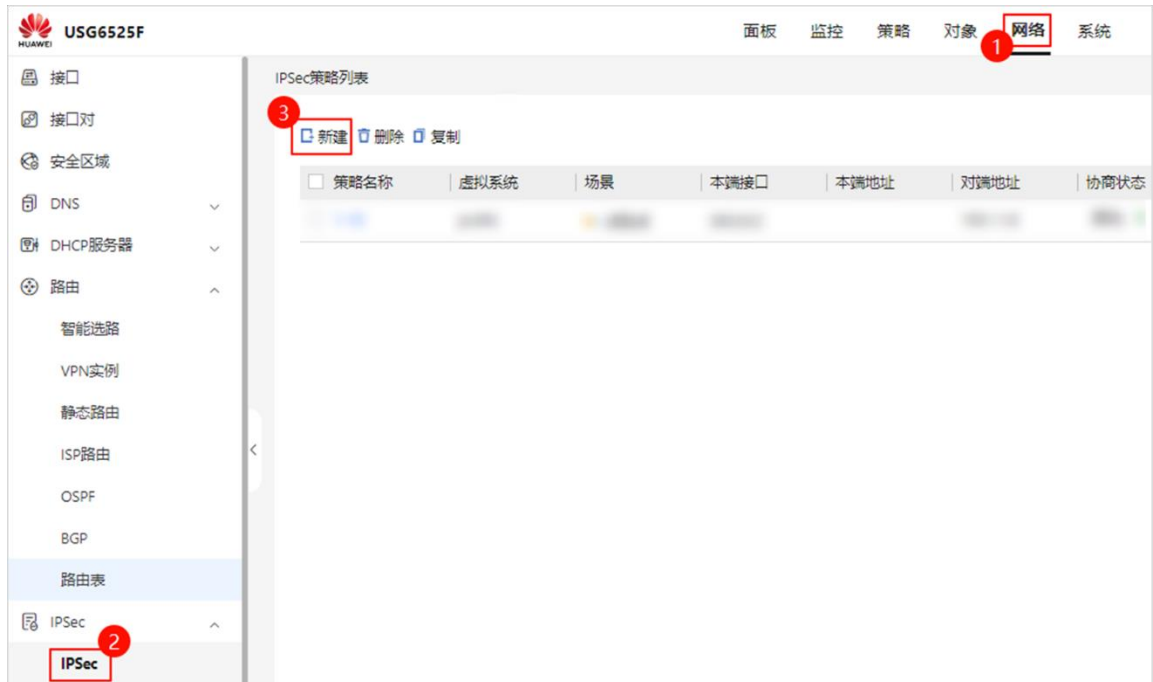


图6-20 进入 FW3 设备 IPsec 策略配置界面



图6-21 FW3 设备选择 IPSec 策略场景

场景选择

基本配置

定义数据流

安全提议

虚拟系统

策略名称

本端接口 ?

本端地址 ?

对端地址

认证方式

密钥类型

预共享密钥

本端ID ?

对端ID

协商报文路由注入 ?

public

map1-10

GEO/0/1

100.1.1.8

提示: 如果修改了本端或对端地址, 需要同步调整安全策略配置, 以保证IPSec隧道可以正常协商。

☒ 预共享密钥 ☐ RSA签名

☒ 单密钥 ☐ 多密钥

..... Huawei@123

IP地址

接受任意对端ID

取消

上一步

下一步

图6-22 FW3 设备 IPSec 基础参数配置

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

1

新建 删除 插入

Q 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
☐	100.100.1.0/255.255.255.0	172.16.30.0/255.255.255.0	any	any	any	加密	+ [编辑]
☐	100.100.1.0/255.255.255.0	172.16.40.0/255.255.255.0	any	any	any	加密	+ [编辑]

共 2 条

< 1 >

50条/页

前往 1 页

反向路由注入?

☐

取消

上一步

3 下一步

图6-23 FW3 设备 IPsec 加密数据流配置

图6-24 FW3 设备安全提议配置

步骤 5 配置业务安全策略

配置 FW1、FW2 和 FW3 设备的域间安全策略，放行站点间交互的业务流量。

分别登录 FW1、FW2 和 FW3 设备的 Web 管理界面，选择“策略 > 安全策略 > 安全策略 > 新建安全策略”，执行以下操作，创建用于站点业务交互的安全策略。

^ 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

地址/地区 100.100.1.0/... 172.16.30.0/...

标签 请选择

目的

目的类型 安全区域 虚拟服务

安全区域 trust untrust

地址/地区 100.100.1.0/... 172.16.30.0/...

标签 请选择

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 反病毒/入侵防御/URL过滤/内容过滤/文件过滤/邮件过滤/DNS过滤

转到“设置”以激活 Windows。

取消 命令预览 确定

图6-25 FW1 设备安全策略配置（针对业务流）

^ 概述

* 名称IPSec_OA

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trust × untrust ×

地址/地区 ①100.100.1.0/... × 172.16.40.0/... ×

标签请选择

目的

目的类型安全区域 虚拟服务

安全区域trust × untrust ×

地址/地区 ①100.100.1.0/... × 172.16.40.0/... ×

标签请选择

服务 ②

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 反病毒/入侵防御/URL过滤/内容过滤/文件过滤/邮件过滤/DNS过滤

转到“设置”以激活 Windows。

取消 命令预览 确定

图6-26 FW2 设备安全策略配置（针对业务流）



^ 概述

* 名称

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

地址/地区 ①

标签

目的

目的类型 ☒ 安全区域 ☐ 虚拟服务

安全区域

地址/地区 ①

标签

服务 ②

协议

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/文件过滤/邮件过滤/DNS过滤

转到“设置”以激活 Windows。

图6-27 FW3 设备安全策略配置（针对业务流）

步骤 6 配置 NAT 策略

因之前的实验在 FW 设备上均有部署 NAT 策略，为避免 NAT 转换影响 IPSec VPN 业务正常交互，需要针对 IPSec VPN 交互的业务流量进行免 NAT 转换的操作。

在 FW1 设备 Web 管理界面选择“策略 > NAT 策略 > NAT 策略 > 新建”，执行以下操作，部署 IPsec VPN 场景下的 NAT 穿越。



图6-28 进入 FW1 设备的 NAT 策略配置界面



图6-29 FW1 配置免 NAT 策略



图6-30 调整 NAT 策略优先级

使用同样配置步骤，在 FW2 和 FW3 设备上均配置免 NAT 策略并调整 NAT 策略优先级。

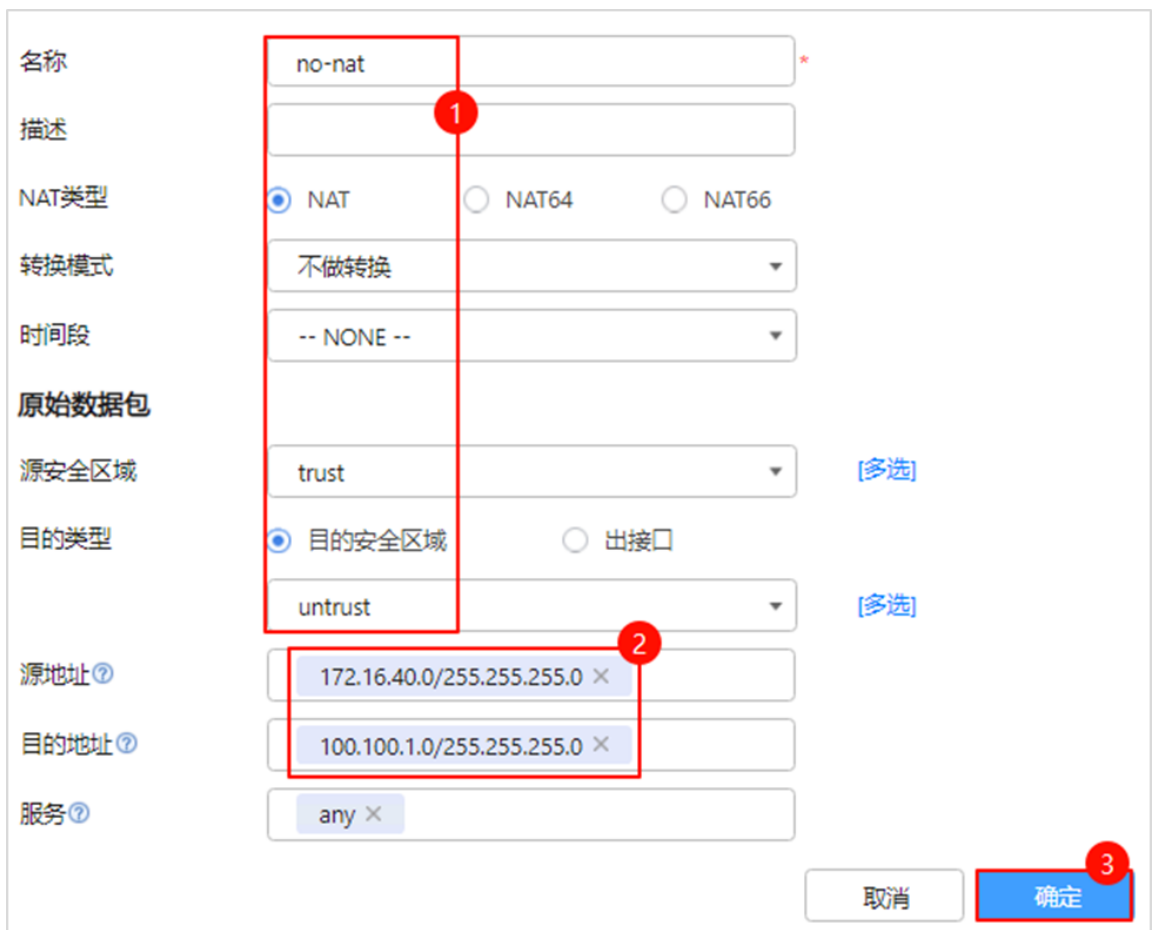


图6-31 FW2 配置免 NAT 策略



图6-32 FW2 调整 NAT 策略优先级

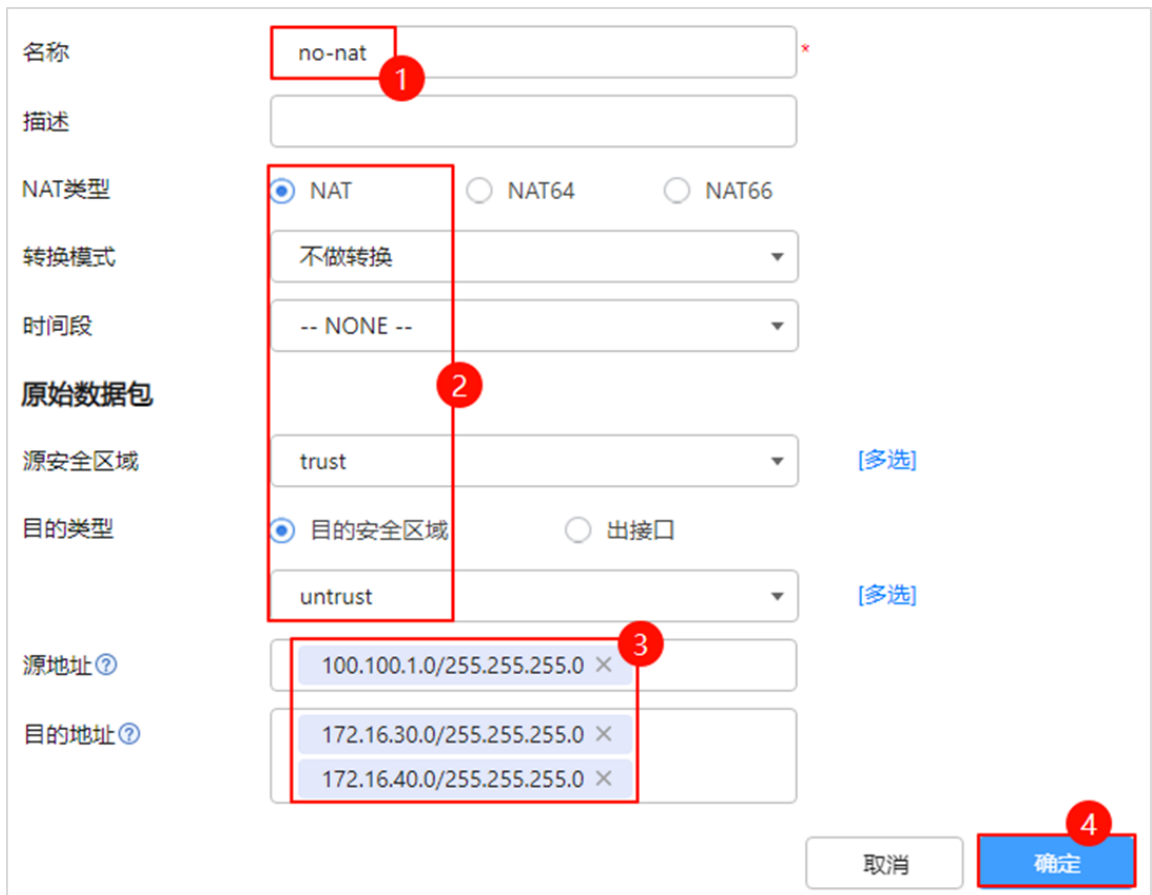


图6-33 FW3 配置免 NAT 策略



图6-34 FW3 调整 NAT 策略优先级

6.3 结果验证

6.3.1 业务连通性测试

使用 RDP 登录 WWW Server，打开命令行，测试分部 1 到达总部业务终端 PC5 的连通性。

```
C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter service:

    Connection-specific DNS Suffix . : 
    Link-local IPv6 Address . . . . . : fe80::adb2:d4d4:aefb:74f7%13
    IPv4 Address. . . . . : 172.16.30.10
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 172.16.30.2

Ethernet adapter mgmt:

    Connection-specific DNS Suffix . : 
    Link-local IPv6 Address . . . . . : fe80::2169:beba:a1d1:3fa1%12
    IPv4 Address. . . . . : 192.168.20.107
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.20.254

Tunnel adapter isatap.{CE306785-F74E-4E9C-9D2A-C55461647F7C}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . : 

Tunnel adapter isatap.{8157AE65-456B-4427-A7E1-B96ED4CB300A}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . : 

C:\Users\Administrator>ping 100.100.1.10

Pinging 100.100.1.10 with 32 bytes of data:
Reply from 100.100.1.10: bytes=32 time=1ms TTL=126
Reply from 100.100.1.10: bytes=32 time<1ms TTL=126
Reply from 100.100.1.10: bytes=32 time<1ms TTL=126
Reply from 100.100.1.10: bytes=32 time<1ms TTL=126

Ping statistics for 100.100.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Administrator>_
```

图6-35 分部1 访问总部连通性测试

使用 RDP 登录 PC2，打开命令行，测试分部 2 到达总部业务终端 PC5 的连通性。

```

Ethernet adapter service:

Connection-specific DNS Suffix  . : 
Link-local IPv6 Address . . . . . : fe80::490d:d3a9:e1d2:249a%11
IPv4 Address. . . . . : 172.16.40.10
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 172.16.40.2

Tunnel adapter isatap.{D8FCA672-EF4F-476C-97EB-C2BBF3906A5A}:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix  . : 

Tunnel adapter isatap.{C67F2CCD-0648-4907-8C6A-E55B241DC2CC}:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix  . : 

C:\Users\Security>ping 100.100.1.10

Pinging 100.100.1.10 with 32 bytes of data:
Reply from 100.100.1.10: bytes=32 time=1ms TTL=126
Reply from 100.100.1.10: bytes=32 time<1ms TTL=126
Reply from 100.100.1.10: bytes=32 time<1ms TTL=126
Reply from 100.100.1.10: bytes=32 time<1ms TTL=126

Ping statistics for 100.100.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Security>_

```

图6-36 分部2 访问总部连通性测试

使用 RDP 登录 PC5，打开命令行，分别测试总部到分部 1 业务终端 WWW Server 和分部 2 业务终端 PC2 的连通性。

```
Ethernet adapter service:

Connection-specific DNS Suffix  . : 
Link-local IPv6 Address . . . . . : fe80::7546:23ec:6f35:66c4%11
IPv4 Address. . . . . : 100.100.1.10
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 100.100.1.1

Tunnel adapter isatap.{D8FCA672-EF4F-476C-97EB-C2BBF3906A5A}:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix  . : 

Tunnel adapter isatap.{C67F2CCD-0648-4907-8C6A-E55B241DC2CC}:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix  . : 

C:\Users\Security>ping 172.16.30.10

Pinging 172.16.30.10 with 32 bytes of data:
Reply from 172.16.30.10: bytes=32 time=1ms TTL=126
Reply from 172.16.30.10: bytes=32 time<1ms TTL=126
Reply from 172.16.30.10: bytes=32 time<1ms TTL=126
Reply from 172.16.30.10: bytes=32 time<1ms TTL=126

Ping statistics for 172.16.30.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Security>ping 172.16.40.10

Pinging 172.16.40.10 with 32 bytes of data:
Reply from 172.16.40.10: bytes=32 time=1ms TTL=126
Reply from 172.16.40.10: bytes=32 time<1ms TTL=126
Reply from 172.16.40.10: bytes=32 time<1ms TTL=126
Reply from 172.16.40.10: bytes=32 time<1ms TTL=126

Ping statistics for 172.16.40.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Security>
```

图6-37 总部访问分部业务连通性测试

6.3.2 隧道信息查看

分别登录 FW1、FW2 和 FW3 设备 Web 管理界面，选择“网路 > IPSec > 监控”，进入 IPSec 监控列表界面，查看 IPSec 隧道协商状态及具体信息。



图6-38 FW1 设备 IPsec VPN 隧道信息



图6-39 FW2 设备 IPsec VPN 隧道信息



图6-40 FW3 设备 IPsec VPN 隧道信息

6.4 配置参考

6.4.1 FW1 配置

```
#
sysname FW1
#
```

```
acl number 3500
 rule 5 permit ip source 172.16.30.0 0.0.0.255 destination 100.100.1.0 0.0.0.255

#
interface GE0/0/2
 ip address 10.3.1.2 255.255.255.252
 service-manage ping permit
 ipsec policy 1
#
interface GE0/0/5
 ip address 172.16.30.2 255.255.255.0
 service-manage ping permit
#
ip route-static 0.0.0.0 0.0.0.0 10.3.1.1
#
ike proposal 1
 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 1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256-gcm-128
#
ike peer 1
 pre-shared-key Huawei@123
 ike-proposal 1
 remote-address 100.1.1.8
#
ipsec policy 1 10 isakmp
 security acl 3500
 ike-peer 1
 proposal 1
#
firewall zone trust
 set priority 85
 add interface GE0/0/5
 add interface GE0/0/6
#
firewall zone untrust
 set priority 5
 add interface GE0/0/1
 add interface GE0/0/2
#
security-policy
```

```
rule name untrust-local
  source-zone local
  source-zone untrust
  destination-zone local
  destination-zone untrust
  action permit
rule name IPSec_OA
  source-zone trust
  source-zone untrust
  destination-zone trust
  destination-zone untrust
  source-address 100.100.1.0 mask 255.255.255.0
  source-address 172.16.30.0 mask 255.255.255.0
  destination-address 100.100.1.0 mask 255.255.255.0
  destination-address 172.16.30.0 mask 255.255.255.0
  action permit
#
nat-policy
rule name no-nat
  source-zone trust
  destination-zone untrust
  source-address 172.16.30.0 mask 255.255.255.0
  destination-address 100.100.1.0 mask 255.255.255.0
  action no-nat
rule name trust-untrust
  source-zone trust
  destination-zone untrust
  action source-nat easy-ip
#
return
```

6.4.2 FW2 配置

```
#
sysname FW2
#
acl number 3500
  rule 5 permit ip source 172.16.40.0 0.0.0.255 destination 100.100.1.0 0.0.0.255
#
interface GE0/0/2
  ip address 10.6.1.2 255.255.255.252
  service-manage ping permit
  ipsec policy 1
#
interface GE0/0/5
  ip address 172.16.40.2 255.255.255.0
  service-manage ping permit
#
```

```
ip route-static 0.0.0.0 0.0.0.0 10.6.1.1
#
ike proposal 1
  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 1
  esp authentication-algorithm sha2-256
  esp encryption-algorithm aes-256-gcm-128
#
ike peer 1
  pre-shared-key Huawei@123
  ike-proposal 1
  remote-address 100.1.1.8
#
ipsec policy 1 10 isakmp
  security acl 3500
  ike-peer 1
  proposal 1
#
firewall zone trust
  set priority 85
  add interface GE0/0/5
  add interface GE0/0/6
#
firewall zone untrust
  set priority 5
  add interface GE0/0/1
  add interface GE0/0/2
#
security-policy
  rule name untrust-local
    source-zone local
    source-zone untrust
    destination-zone local
    destination-zone untrust
    action permit
  rule name IPSec_OA
    source-zone trust
    source-zone untrust
    destination-zone trust
    destination-zone untrust
    source-address 100.100.1.0 mask 255.255.255.0
    source-address 172.16.40.0 mask 255.255.255.0
```



```
destination-address 100.100.1.0 mask 255.255.255.0
destination-address 172.16.40.0 mask 255.255.255.0
action permit
#
nat-policy
rule name no-nat
source-zone trust
destination-zone untrust
source-address 172.16.40.0 mask 255.255.255.0
destination-address 100.100.1.0 mask 255.255.255.0
action no-nat
rule name trust-untrust
source-zone trust
destination-zone untrust
action source-nat easy-ip
#
return
```

6.4.3 FW3 配置

```
#
sysname FW3
#
acl number 3500
rule 5 permit ip source 100.100.1.0 0.0.0.255 destination 172.16.30.0 0.0.0.255
rule 10 permit ip source 100.100.1.0 0.0.0.255 destination 172.16.40.0 0.0.0.255
#
interface GE0/0/1
ip address 100.1.1.8 255.255.255.0
service-manage ping permit
ipsec policy 1
#
interface GE0/0/7
ip address 100.100.1.1 255.255.255.0
service-manage ping permit
#
ip route-static 0.0.0.0 0.0.0.0 100.1.1.1
#
ike proposal 1
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 1
esp authentication-algorithm sha2-256
```

```
esp encryption-algorithm aes-256-gcm-128
#
ike peer 1
pre-shared-key Huawei@123
ike-proposal 1
#
ipsec policy-template map1 10
security acl 3500
ike-peer 1
proposal 1
alias map1-10
#
ipsec policy 1 10 isakmp template map1
#
firewall zone trust
set priority 85
add interface GE0/0/7
#
firewall zone untrust
set priority 5
add interface GE0/0/1
#
security-policy
rule name untrust-local
source-zone local
source-zone untrust
destination-zone local
destination-zone untrust
action permit
rule name IPSec_OA
source-zone trust
source-zone untrust
destination-zone trust
destination-zone untrust
source-address 100.100.1.0 mask 255.255.255.0
source-address 172.16.30.0 mask 255.255.255.0
source-address 172.16.40.0 mask 255.255.255.0
destination-address 100.100.1.0 mask 255.255.255.0
destination-address 172.16.30.0 mask 255.255.255.0
destination-address 172.16.40.0 mask 255.255.255.0
action permit
#
nat-policy
rule name no-nat
source-zone trust
destination-zone untrust
source-address 100.100.1.0 mask 255.255.255.0
destination-address 172.16.30.0 mask 255.255.255.0
```

```
destination-address 172.16.40.0 mask 255.255.255.0
action no-nat
rule name nat1
source-zone trust
egress-interface GE0/0/1
source-address 10.3.0.0 mask 255.255.255.0
source-address 10.3.1.0 mask 255.255.255.0
action source-nat easy-ip
#
return
```

6.4.4 RT1 预配置

```
#
sysname RT1
#
interface GigabitEthernet0/0/1
undo portswitch
#
interface GigabitEthernet0/0/1.2
dot1q termination vid 2
ip address 4.4.4.2 255.255.255.252
#
interface GigabitEthernet0/0/4
undo portswitch
ip address 10.3.1.1 255.255.255.252
#
ospf 1 router-id 33.33.33.1
import-route direct
import-route static
area 0.0.0.0
network 4.4.4.0 0.0.0.3
#
ip route-static 172.16.30.0 24 10.3.1.2
#
return
```

6.4.5 RT2 预配置

```
#
sysname RT2
#
interface GigabitEthernet0/0/1
undo portswitch
#
interface GigabitEthernet0/0/1.40
dot1q termination vid 40
ip address 3.3.3.2 255.255.255.252
```

```
#
interface GigabitEthernet0/0/4
 undo portswitch
 ip address 10.6.1.1 255.255.255.252
#
ospf 1 router-id 33.33.33.2
 import-route direct
 import-route static
 area 0.0.0.0
  network 3.3.3.0 0.0.0.3
#
ip route-static 172.16.40.0 24 10.6.1.2
#
return
```

6.4.6 SW1 预配置

```
#
sysname SW1
#
vlan batch 2 40
#
interface vlanif1
 ip address 100.1.1.1 255.255.255.0
#
interface vlanif2
 ip address 4.4.4.1 255.255.255.252
#
interface vlanif40
 ip address 3.3.3.1 255.255.255.252
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 2 40
#
ospf 1 router-id 33.33.33.3
 import-route direct
 import-route static
 area 0.0.0.0
  network 3.3.3.0 0.0.0.3
  network 4.4.4.0 0.0.0.3
#
ip route-static 100.100.1.0 24 100.1.1.8
#
return
```

6.4.7 Mirror-SW 预配置

```
#
sysname Mirror-SW
#
vlan batch 2 40
#
interface GigabitEthernet0/0/1
port link-type trunk
port trunk allow-pass vlan 2 40
#
interface GigabitEthernet0/0/2
port link-type trunk
port trunk allow-pass vlan 2 40
#
interface GigabitEthernet0/0/3
port link-type trunk
port trunk allow-pass vlan 2 40
#
return
```

6.4.8 SW2 预配置

```
#
sysname SW2
#
vlan batch 30
#
interface GigabitEthernet0/0/1
port link-type access
port default vlan 30
#
interface GigabitEthernet0/0/15
port link-type access
port default vlan 30
#
interface GigabitEthernet0/0/13
shutdown
#
interface GigabitEthernet0/0/14
shutdown
#
return
```

6.4.9 SW3 预配置

```
#
sysname SW3
```

```
#
vlan batch 40
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 40
#
interface GigabitEthernet0/0/14
 port link-type access
 port default vlan 40
#
return
```

6.5 思考题

完成本实验所有配置后，两个企业分部之间是否可以互访？为什么？

参考答案：无法互访，因为两个分部之间并未部署 IPsec VPN 隧道，分部互访的业务流并未添加进 IPsec VPN 的感兴趣流，相关安全策略也并未放行。

7 IPsec VPN 故障排除实验

7.1 实验介绍

7.1.1 关于本实验

某中大型企业新增两个分部，企业总部与两个分部在不同的城市，总部与分部之间需要跨 Internet 交互业务数据。因此需要在总部与分部 1、分部 2 之间建立 IPsec VPN 隧道；同时在分部 1 与分部 2 之间部署 IPsec VPN 隧道，用于站点间交互业务数据的加密。

本实验以预配置脚本的模式，模拟开局过程中可能遇到的问题，学员需要尝试排查故障、解决问题，满足企业不同站点间业务交互需求。

7.1.2 实验目的

- 掌握 IPsec VPN 的配置方式。
- 掌握 IPsec VPN 在 NAT 场景下的配置要点。
- 掌握 IPsec VPN 的排错方法。

7.1.3 实验组网介绍

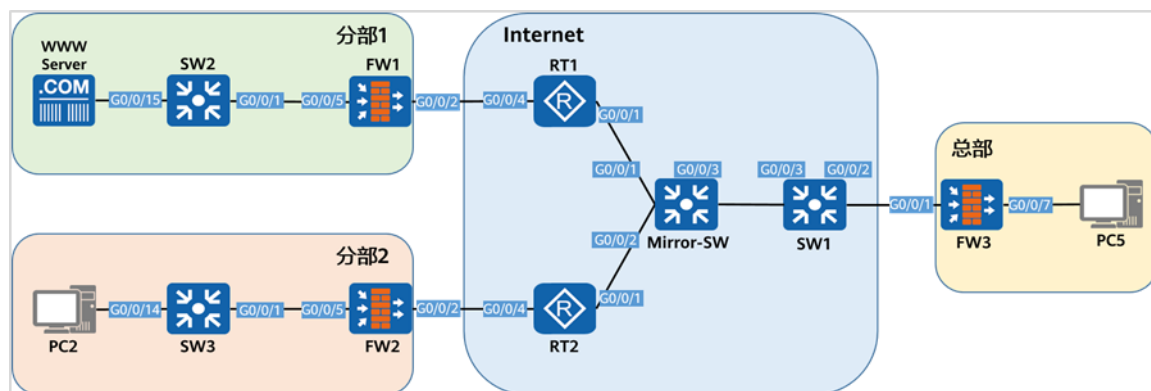


图7-1 IPsec VPN 故障排除实验拓扑

FW1 为企业分部 1 的出口网关，FW2 为企业分部 2 的出口网关，FW3 为企业总部的出口网关，使用 RT1、RT2、Mirror-SW 和 SW1 模拟 Internet。SW2 和 SW3 是接入层交换机，WWW Server、PC2 和 PC5 均为站点内终端设备。

分部网络规划：在 SW2 和 SW3 中，上下行端口采用 Access 的类型，将 PC 划分到对应的 VLAN。在 FW1 上配置 WWW Server 的网关、在 FW2 上配置 PC2 的网关。

Internet 区域网络规划：RT1、RT2 与 SW1 之间是三层网络（部署 OSPF），通过静态路由指向各站点出口 FW 设备，实现对站点内网络的访问，并将静态路由引入至 OSPF。

总部网络规划：PC5 业务网关部署在出口设备 FW3 上。

业务规划：

1. 分部 1 的出口设备 FW1 需要与总部出口设备 FW3 建立 IPsec VPN，分部 1 内的 WWW Server 需要访问互联网。
2. 分部 2 的出口设备 FW2 需要与总部出口设备 FW3 建立 IPsec VPN，分部 2 内的 PC 禁止访问互联网，分部 2 的 PC2 需要与总部 PC5 互通。
3. 分部 1 与分部 2 之间需要相互访问，出于安全考虑，总部要求分部之间的数据需要经过总部转发。

RT1、RT2、Mirror-SW、SW1、SW2 和 SW3 相关配置在本实验配置步骤中未体现，具体可参考“7.3 配置参考”相关设备预配置，本实验重点介绍 FW1、FW2 和 FW3 设备上关键配置。

7.1.4 实验规划

表7-1 设备接口规划表

设备	接口	接口性质	接口信息	说明
FW1	GE0/0/2	三层接口	10.3.1.2/30 安全区域：untrust	连接Internet的出接口，与RT1互连
	GE0/0/5	三层接口	172.16.30.2/24 安全区域：trust	与SW2互连
FW2	GE0/0/2	三层接口	10.6.1.2/30 安全区域：untrust	连接Internet的出接口，与RT1互连
	GE0/0/5	三层接口	172.16.40.2/24 安全区域：trust	与SW3互连
FW3	GE0/0/1	三层接口	100.1.1.8/24 安全区域：untrust	连接Internet的出接口，与SW1互连
	GE0/0/7	三层接口	100.100.1.1/24 安全区域：trust	连接PC5
RT1	G0/0/1.2	三层子接口	4.4.4.2/30 终结VLAN2	与SW1的VLANIF2组成直连网段
	G0/0/4	三层接口	10.3.1.1/30	与FW1互连
RT2	G0/0/1.40	三层子接口	3.3.3.2/30	与SW1的VLANIF40组

			终结VLAN40	成直连网段
	G0/0/4	三层接口	10.6.1.1/30	与FW2互连
SW1	G0/0/2	Access	PVID: 1	与FW3互连
	G0/0/3	Trunk	PVID: 1 Allow-pass VLAN: 2, 40	与Mirror-SW互连
SW2	G0/0/1	Access	PVID: 30	与FW1互连
	G0/0/15	Access	PVID: 30	连接WWW Server
SW3	G0/0/1	Access	PVID: 40	与FW2互连
	G0/0/14	Access	PVID: 40	连接PC2
Mirror-SW	G0/0/1	Trunk	PVID: 1 Allow-pass VLAN: 2, 40	互连接口
	G0/0/2			
	G0/0/3			
WWW Server	Ethernet0	三层	172.16.30.10/24 网关: 172.16.30.2/24	终端
PC2	Ethernet0	三层	172.16.40.10/24 网关: 172.16.40.2/24	终端
PC5	Ethernet0	三层	100.100.1.10/24 网关: 100.100.1.1/24	终端

7.2 实验任务配置

7.2.1 配置思路

- 1.将预配置刷入对应设备。
- 2.按照实验规划检查业务是否正常，并逐一排错。

7.2.2 配置步骤

步骤 1 完成设备预配置

完成 FW1 的预配置。

```
#
sysname FW1
```

```
#
acl number 3500
 rule 5 permit ip source 172.16.30.0 0.0.0.255 destination 100.100.1.0 0.0.0.255
#
ipsec proposal 1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256
#
ike proposal 1
 encryption-algorithm aes-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer 1
 pre-shared-key Admin@123
 ike-proposal 1
 remote-address 100.1.1.8
 rsa encryption-padding oaep
 rsa signature-padding pss
 local-id-preference certificate enable
#
ipsec policy 1 10 isakmp
 security acl 3500
 ike-peer 1
 proposal 1
 tunnel local applied-interface
 sa trigger-mode auto
#
interface GE0/0/2
 undo shutdown
 ip address 10.3.1.2 255.255.255.252
 service-manage ping permit
 ipsec policy 1
#
interface GE0/0/5
 undo shutdown
 ip address 172.16.30.2 255.255.255.0
 service-manage http permit
#
firewall zone local
 set priority 100
#
firewall zone trust
 set priority 85
 add interface GE0/0/5
```

```
#
firewall zone untrust
 set priority 5
 add interface GE0/0/2
#
firewall zone dmz
 set priority 50
#
ip route-static 0.0.0.0 0.0.0.0 10.3.1.1
#
security-policy
 rule name untrust-local
  source-zone untrust
  source-zone local
  destination-zone untrust
  destination-zone local
  action permit
 rule name trust-untrust
  source-zone trust
  destination-zone untrust
  source-address 172.16.30.0 mask 255.255.255.0
  destination-address 100.100.1.0 mask 255.255.255.0
  action permit
 rule name untrust-trust
  source-zone untrust
  destination-zone trust
  source-address 100.100.1.0 mask 255.255.255.0
  destination-address 172.16.30.0 mask 255.255.255.0
  action permit
#
nat-policy
 rule name nat
  source-zone local
  source-zone trust
  destination-zone untrust
  action source-nat easy-ip
#
return
```

完成 FW2 的预配置。

```
#
sysname FW2
#
acl number 3500
 rule 5 permit ip source 172.16.40.2 0.0.0.0 destination 100.100.1.0 0.0.0.255
#
ipsec proposal 1
 transform ah
```

```
ah authentication-algorithm sha2-256
#
ike proposal 1
  encryption-algorithm aes-256
  dh group14
  authentication-algorithm sha2-256
  authentication-method pre-share
  integrity-algorithm hmac-sha2-256
  prf hmac-sha2-256
#
ike peer 1
  pre-shared-key Huawei@123
  ike-proposal 1
  remote-address 100.100.1.1
  remote-address 100.1.1.8
  rsa encryption-padding oaep
  rsa signature-padding pss
  local-id-preference certificate enable
  ikev2 authentication sign-hash sha2-256
#
ipsec policy 1 1 isakmp
  security acl 3500
  ike-peer 1
  proposal 1
#
interface GE0/0/2
  undo shutdown
  ip address 10.6.1.2 255.255.255.252
  service-manage ping permit
  ipsec policy 1
#
interface GE0/0/5
  undo shutdown
  ip address 172.16.40.2 255.255.255.0
  service-manage ping permit
#
firewall zone local
  set priority 100
#
firewall zone trust
  set priority 85
  add interface GE0/0/5
#
firewall zone untrust
  set priority 5
  add interface GE0/0/2
#
firewall zone dmz
```

```
set priority 50
#
ip route-static 0.0.0.0 0.0.0.0 10.6.6.1
#
security-policy
 rule name untrust-local
   source-zone untrust
   source-zone local
   destination-zone untrust
   destination-zone local
   action permit
 rule name trust-untrust
   source-zone trust
   destination-zone untrust
   source-address 172.16.40.0 mask 255.255.255.0
   destination-address 100.100.1.0 mask 255.255.255.0
   action permit
 rule name untrust-trust
   source-zone untrust
   destination-zone trust
   source-address 100.100.1.0 mask 255.255.255.0
   destination-address 172.16.40.0 mask 255.255.255.0
   action permit
#
return
```

完成 FW3 的预配置。

```
#
sysname FW3
#
acl number 3500
 rule 5 permit ip source 100.100.1.0 0.0.0.255 destination 172.16.30.0 0.0.0.255
 rule 10 permit ip source 100.100.1.0 0.0.0.255 destination 172.16.40.0 0.0.0.255
#
ipsec proposal 1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256
#
ike proposal 1
 encryption-algorithm aes-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer 1
 pre-shared-key Huawei@123
```

```
ike-proposal 1
rsa encryption-padding oaep
rsa signature-padding pss
local-id-preference certificate enable
ikev2 authentication sign-hash sha2-256
#
ipsec policy-template map1 10
security acl 3500
ike-peer 1
proposal 1
#
ipsec policy 1 1 isakmp template map1
#
interface GE0/0/1
undo shutdown
ip address 100.1.1.8 255.255.255.0
service-manage ping permit
ipsec policy 1
#
interface GE0/0/7
undo shutdown
ip address 100.100.1.1 255.255.255.0
service-manage ping permit
#
firewall zone local
set priority 100
#
firewall zone trust
set priority 85
add interface GE0/0/7
#
firewall zone untrust
set priority 5
add interface GE0/0/1
#
firewall zone dmz
set priority 50
#
ip route-static 0.0.0.0 0.0.0.0 100.1.1.1
#
security-policy
rule name untrust-local
source-zone untrust
source-zone local
destination-zone untrust
destination-zone local
action permit
rule name trust-untrust
```

```
source-zone trust
destination-zone untrust
source-address 100.100.1.0 mask 255.255.255.0
destination-address 172.16.30.0 mask 255.255.255.0
destination-address 172.16.40.0 mask 255.255.255.0
action permit
rule name untrust-trust
source-zone untrust
destination-zone trust
source-address 172.16.30.0 mask 255.255.255.0
source-address 172.16.40.0 mask 255.255.255.0
destination-address 100.100.1.0 mask 255.255.255.0
action permit
#
return
```

RT1、RT2、Mirror-SW、SW1、SW2 和 SW3 相关配置在本实验配置步骤中未体现，具体可参考“7.3 配置参考”相关设备预配置。同时参考“表 7-1”数据规划完成 WWW Server、PC2、PC5 的业务网卡参数的配置。

步骤 2 检查分部 1 与总部的业务

两台防火墙之间需要建立 IPsec VPN 的前提是连接 Internet 的接口路由可达。所以首先检查路由可达性。

```
<FW1> ping 100.1.1.8
PING 100.1.1.8: 56 data bytes, press CTRL_C to break
Reply from 100.1.1.8: bytes=56 Sequence=1 ttl=253 time=22 ms
Reply from 100.1.1.8: bytes=56 Sequence=2 ttl=253 time=4 ms
Reply from 100.1.1.8: bytes=56 Sequence=3 ttl=253 time=56 ms
Reply from 100.1.1.8: bytes=56 Sequence=4 ttl=253 time=5 ms
Reply from 100.1.1.8: bytes=56 Sequence=5 ttl=253 time=54 ms
--- 100.1.1.8 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 4/28/56 ms
```

以上信息显示分部 1 与总部出口防火墙的公网接口路由可达，之后继续检测业务连通性，在 FW1 上用业务网关 ping 总部的业务网关。

```
<FW1> ping -a 172.16.30.2 100.100.1.1
PING 100.100.1.1: 56 data bytes, press CTRL_C to break
Request time out
Request time out
Request time out
Request time out
Request time out
--- 100.100.1.1 ping statistics ---
5 packet(s) transmitted
```

```
0 packet(s) received
100.00% packet loss
```

测试发现业务之间不互通。继续检查 FW1 上是否建立了 IKE SA 和 IPSec SA。

```
<FW1> display ike sa
```

```
<FW1> display ipsec sa
```

经过检查未发现 IKE SA 和 IPSec SA，说明 IPSec VPN 没有建立成功，此时需要先将 IKE SA 建立起来，重点排查一阶段 IKE 相关配置。

查看 IKE 协商失败的原因。

```
[FW1] display ike error-info verbose
current info Num :17
Ike error information:
current ike Error-info number :17

-----
Peer      : 100.1.1.8
Port      : 500
version   : v2
Reason    : authentication fail
Detail    : rcv peer auth fail notification(pre-share-key)
Error-time : 20XX-XX-XX
```

经上述信息可以发现 IKE 协商失败的具体原因是预共享密钥认证失败。

检查 FW1 的 IKE 一阶段的相关预配置。

```
#
ike proposal 1
 encryption-algorithm aes-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer 1
 pre-shared-key Admin@123
 ike-proposal 1
 remote-address 100.1.1.8
 rsa encryption-padding oaep
 rsa signature-padding pss
 local-id-preference certificate enable
#
```

检查 FW2 的 IKE 一阶段的相关预配置。

```
ike proposal 1
 encryption-algorithm aes-256
 dh group14
```



```

authentication-algorithm sha2-256
authentication-method pre-share
integrity-algorithm hmac-sha2-256
prf hmac-sha2-256
#
ike peer 1
pre-shared-key Huawei@123
ike-proposal 1
remote-address 100.100.1.1
remote-address 100.1.1.8
rsa encryption-padding oaep
rsa signature-padding pss
local-id-preference certificate enable
ikev2 authentication sign-hash sha2-256
#

```

对比发现 FW1 的 ike peer 与 FW2 的 ike peer 中预共享密钥配置的不一致。

修改 FW1 的 ike peer 密钥。

```

[FW1] ike peer 1
[FW1-ike-peer-1] pre-shared-key Huawei@123
[FW1-ike-peer-1] quit

```

完成上述操作后，在 FW1 上再次使用业务网关 ping 总部的业务网关。

```

<FW1> ping -a 172.16.30.2 100.100.1.1
PING 100.100.1.1: 56 data bytes, press CTRL_C to break
Request time out
Request time out
Request time out
Request time out
Request time out
Request time out
--- 100.100.1.1 ping statistics ---
5 packet(s) transmitted
0 packet(s) received
100.00% packet loss

```

测试发现业务之间仍不互通。

继续检查 FW1 上的 IKE SA 和 IPsec SA。

```

<FW1> display ike sa
IKE SA information :

```

Conn-ID	Peer	VPN	Flag(s)	Phase	RemoteType	RemoteID
55	100.1.1.8/500		RD ST A	v2:2	IP	100.1.1.8
54	100.1.1.8/500		RD ST A	v2:1	IP	100.1.1.8

```

Number of IKE SA : 2

```

```

<FW1> display ipsec sa

```

```

ipsec sa information:
=====
Interface: GigabitEthernet0/0/2
=====

-----
IPSec policy name: "1"
Sequence number : 10
Acl group       : 3500/IPv4
Acl rule        : 10
Mode            : ISAKMP
-----

Connection ID   : 45
Encapsulation mode: Tunnel
Holding time    : 0d 0h 0m 45s
Tunnel local    : 10.3.1.2/500
Tunnel remote   : 100.1.1.8/500
Flow source     : 172.16.30.0/255.255.255.0 0/0-65535
Flow destination : 100.100.1.0/255.255.255.0 0/0-65535

[Outbound ESP SAs]
SPI: 187369605 (0xb2b0885)
Proposal: ESP-ENCRYPT-AES-256 ESP-AUTH-SHA2-256-128
SA remaining soft duration (kilobytes/sec): 17825792/1397
SA remaining hard duration (kilobytes/sec): 20971520/1936
Max sent sequence-number: 13
UDP encapsulation used for NAT traversal: N
SA encrypted packets (number/bytes): 5/720

[Inbound ESP SAs]
SPI: 187186009 (0xb283b59)
Proposal: ESP-ENCRYPT-AES-256 ESP-AUTH-SHA2-256-128
SA remaining soft duration (kilobytes/sec): 18035507/1433
SA remaining hard duration (kilobytes/sec): 20971520/1936
Max received sequence-number: 12288
UDP encapsulation used for NAT traversal: N
SA decrypted packets (number/bytes): 5/720
Anti-replay : Enable
Anti-replay window size: 1024

```

排查发现 FW1 上存在 IKE SA 和 IPsec SA，但是业务不通，接下来查看 ACL 3500 是否正确筛选业务流量。

```

<FW1> display acl all
Advanced ACL 3500, 1 rule ( Reference counter 1 )
Acl's step is 5
rule 10 permit ip source 172.16.30.0 0.0.0.255 destination 100.100.1.0 0.0.0.255 (0 times matched)

```

排查发现 ACL 3500 配置无误，但命中计数并未增加，由此判断出流量没有经过 IPsec 模块处理。根据防火墙处理报文流程，报文会先经过 NAT 处理，然后再由 IPsec 模块匹配处理，

且分部 1 有访问 Internet 的需求，需要部署源 NAT 策略。因此需要排查 FW1 设备 NAT 配置。

```
[FW1]nat-policy
[FW1-policy-nat]display this
#
nat-policy
 rule name nat
   source-zone local
   source-zone trust
   destination-zone untrust
   action source-nat easy-ip
#
return
```

以上 NAT 配置表示 FW1 的 local 区域和 trust 区域的流量访问 untrust 区域的资源时，将全部进行源地址转换，FW1 上路由出接口为 G0/0/2，所以到达 IPSec 模块处理时源地址为 10.3.1.2，无法匹配到 ACL 3500，进而无法触发 IPSec 相关处理流程。

修改 FW1 设备 NAT 配置。

```
[FW1] nat-policy
[FW1-policy-nat] undo rule name nat
[FW1-policy-nat] rule name IPSec-deny
[FW1-policy-nat-rule-IPSec-deny] destination-address 100.100.1.0 mask 255.255.255.0
[FW1-policy-nat-rule-IPSec-deny] source-zone local
[FW1-policy-nat-rule-IPSec-deny] source-zone trust
[FW1-policy-nat-rule-IPSec-deny] destination-zone untrust
[FW1-policy-nat-rule-IPSec-deny] action no-nat
[FW1-policy-nat-rule-IPSec-deny] quit
[FW1-policy-nat] rule name nat
[FW1-policy-nat-rule-nat] source-zone local
[FW1-policy-nat-rule-nat] source-zone trust
[FW1-policy-nat-rule-nat] destination-zone untrust
[FW1-policy-nat-rule-nat] action source-nat easy-ip
[FW1-policy-nat-rule-nat] quit
[FW1-policy-nat] quit
```

完成上述配置后，在 FW1 设备上再次用业务网关 ping 总部的业务网关。

```
[FW1] ping -a 172.16.30.2 100.100.1.1
PING 100.100.1.1: 56 data bytes, press CTRL_C to break
 Reply from 100.100.1.1: bytes=56 Sequence=1 ttl=255 time=4 ms
 Reply from 100.100.1.1: bytes=56 Sequence=2 ttl=255 time=2 ms
 Reply from 100.100.1.1: bytes=56 Sequence=3 ttl=255 time=2 ms
 Reply from 100.100.1.1: bytes=56 Sequence=4 ttl=255 time=1 ms
 Reply from 100.100.1.1: bytes=56 Sequence=5 ttl=255 time=2 ms
 --- 100.100.1.1 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
```

```
round-trip min/avg/max = 1/2/4 ms
5 packet(s) transmitted
0 packet(s) received
100.00% packet loss
```

继续使用分部 1 的业务终端 WWW Server 测试到达总部业务终端 PC5 的连通性。

```
C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter service:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::adb2:d4d4:aefb:74f7%13
    IPv4 Address. . . . . : 172.16.30.10
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 172.16.30.2

Ethernet adapter mgmt:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::2169:beba:a1d1:3fa1%12
    IPv4 Address. . . . . : 192.168.20.107
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.20.254

Tunnel adapter isatap.{CE306785-F74E-4E9C-9D2A-C55461647F7C}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Tunnel adapter isatap.{8157AE65-456B-4427-A7E1-B96ED4CB300A}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Users\Administrator>ping 100.100.1.10

Pinging 100.100.1.10 with 32 bytes of data:
Reply from 100.100.1.10: bytes=32 time=1ms TTL=126
Reply from 100.100.1.10: bytes=32 time<1ms TTL=126
Reply from 100.100.1.10: bytes=32 time<1ms TTL=126
Reply from 100.100.1.10: bytes=32 time<1ms TTL=126

Ping statistics for 100.100.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Administrator>
```

图7-2 分部 1 与总部之间的业务测试

可以发现分部 1 与总部之间的业务已可以正常交互，分部 1 至总部的 IPsec VPN 排障完成。

步骤 3 检查分部 2 与总部的业务

参照步骤 2 中排查思路，首先检查公网接口之间的路由可达性。

```
<FW2> ping 100.1.1.8
PING 100.1.1.8: 56 data bytes, press CTRL_C to break
Request time out
```

```
Request time out
Request time out
Request time out
Request time out
--- 100.1.1.8 ping statistics ---
5 packet(s) transmitted
0 packet(s) received
100.00% packet loss
```

经排查发现，公网接口之间路由不可达，继续查看 FW2 设备的安全策略配置。

```
security-policy
rule name untrust-local
source-zone untrust
source-zone local
destination-zone untrust
destination-zone local
action permit
```

经排查发现，安全策略配置无误，继续查看路由表，未发现 FW2 设备去往 Internet 的缺省路由。

```
<FW2> display ip routing-table
Proto: Protocol          Pre: Preference
Route Flags: R - relay, D - download to fib, T - to vpn-instance, B - black hole route
-----
Routing Table : _public_
          Destinations : 11          Routes : 11

Destination/Mask    Proto   Pre  Cost   Flags NextHop         Interface
-----
10.6.1.0/30         Direct  0    0       D   10.6.1.2         GE0/0/2
10.6.1.2/32         Direct  0    0       D   127.0.0.1        GE0/0/2
10.6.1.3/32         Direct  0    0       D   127.0.0.1        GE0/0/2
22.22.22.1/32       Direct  0    0       D   127.0.0.1        LoopBack0
127.0.0.0/8         Direct  0    0       D   127.0.0.1        InLoopBack0
127.0.0.1/32        Direct  0    0       D   127.0.0.1        InLoopBack0
127.255.255.255/32  Direct  0    0       D   127.0.0.1        InLoopBack0
172.16.40.0/24      Direct  0    0       D   172.16.40.2      GE0/0/5
172.16.40.2/32      Direct  0    0       D   127.0.0.1        GE0/0/5
172.16.40.255/32    Direct  0    0       D   127.0.0.1        GE0/0/5
255.255.255.255/32  Direct  0    0       D   127.0.0.1        InLoopBack0
```

查看缺省路由的配置。

```
<FW2> display current-configuration | include route-static
ip route-static 0.0.0.0 0.0.0.0 10.6.6.1
```

发现缺省路由的下一跳配置错误，需要修改为 10.6.1.1。

```
[FW2]ip route-static 0.0.0.0 0.0.0.0 10.6.1.1
```

完成上述配置后，再次测试 FW2 是否可以 ping 通 FW3 的 G0/0/1 接口。可以发现分部 2 出口设备与总部出口设备之间路由可达。

```
<FW2> ping 100.1.1.8
PING 100.1.1.8: 56 data bytes, press CTRL_C to break
Reply from 100.1.1.8: bytes=56 Sequence=1 ttl=253 time=2 ms
Reply from 100.1.1.8: bytes=56 Sequence=2 ttl=253 time=3 ms
Reply from 100.1.1.8: bytes=56 Sequence=3 ttl=253 time=33 ms
Reply from 100.1.1.8: bytes=56 Sequence=4 ttl=253 time=2 ms
Reply from 100.1.1.8: bytes=56 Sequence=5 ttl=253 time=2 ms
--- 100.1.1.8 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 2/8/33 ms
```

继续在 FW2 设备上用业务网关访问总部的业务网关，可以发现无法访问。

```
<FW2> ping -a 172.16.40.2 100.100.1.1
PING 100.100.1.1: 56 data bytes, press CTRL_C to break
Request time out
Request time out
Request time out
Request time out
Request time out
--- 100.100.1.1 ping statistics ---
5 packet(s) transmitted
0 packet(s) received
100.00% packet loss
```

下一步继续检查 FW2 设备上是否建立了 IKE SA 和 IPsec SA。

```
<FW2> display ike sa
IKE SA information :
Conn-ID    Peer      VPN      Flag(s)   Phase    RemoteType RemoteID
-----
14         100.1.1.8/500 RD|ST|A   v2:1      IP       100.1.1.8
Number of IKE SA : 1
```

```
<FW2> dis ipsec sa
```

经检查发现 IKE SA 协商正常，但是不存在 IPsec SA，说明 IKE 一阶段协商成功，二阶段协商失败，这种情况通常是配置的对接参数不一致导致的。

检查 FW2、FW3 设备上 IPsec 安全提议的配置。

```
[FW2] ipsec proposal 1
[FW2-ipsec-proposal-1] display this
#
ipsec proposal 1
transform ah
```

```
ah authentication-algorithm sha2-256
#
```

```
[FW3]ipsec proposal 1
[FW3-ipsec-proposal-1]display this
#
ipsec proposal 1
  esp authentication-algorithm sha2-256
  esp encryption-algorithm aes-256-gcm-128
#
```

检查发现 FW2 设备上的 IPSec 安全提议的封装协议为 AH，但 FW3 设备上 IPSec 安全提议的封装协议为 ESP，二者配置不一致。

将 FW2 上 IPSec 安全提议修改为如下配置。

```
[FW2] ipsec proposal 1
[FW2-ipsec-proposal-1] transform esp
[FW2-ipsec-proposal-1] esp authentication-algorithm sha2-256
[FW2-ipsec-proposal-1] esp encryption-algorithm aes-256
[FW2-ipsec-proposal-1] quit
```

完成上述配置后，在 FW2 设备上再次用业务网关 ping 总部的业务网关。

```
<FW2> ping -a 172.16.40.2 100.100.1.1
PING 100.100.1.1: 56 data bytes, press CTRL_C to break
Request time out
Reply from 100.100.1.1: bytes=56 Sequence=2 ttl=255 time=3 ms
Reply from 100.100.1.1: bytes=56 Sequence=3 ttl=255 time=1 ms
Reply from 100.100.1.1: bytes=56 Sequence=4 ttl=255 time=2 ms
Reply from 100.100.1.1: bytes=56 Sequence=5 ttl=255 time=2 ms
--- 100.100.1.1 ping statistics ---
 5 packet(s) transmitted
 4 packet(s) received
20.00% packet loss
round-trip min/avg/max = 1/2/3 ms
```

可以发现业务网关可以 ping 通，说明 IKE SA 和 IPSec SA 协商成功。

继续测试分部 2 业务终端至总部业务终端之间的连通性。

```
C:\Users\Security>ping 100.100.1.10

Pinging 100.100.1.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 100.100.1.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\Security>
```

图7-3 分部2 访问总部业务测试（不可达）

两台 FW 设备的业务网关地址可以互通，但是真实的业务不通，此时需要检查业务终端的网络参数的配置是否正确（本实验终端设备网络参数默认无误），以及 FW2 设备用于筛选 IPSec VPN 业务流的 ACL 配置是否正确。

检查 ACL 是否有命中计数更新。

```
<FW2> display acl all
Advanced ACL 3500, 1 rule ( Reference counter 1 )
Acl's step is 5
rule 5 permit ip source 172.16.40.2 0.0.0.0 destination 100.100.1.0 0.0.0.255 (5 times matched)
```

检查发现 ACL 命中计数在 PC2 访问 PC5 的后计数仍然为 5，命中次数无增长。且 ACL 3500 的源地址未包含分部 2 的整个业务网段。

修改 FW2 上 ACL 3500 的配置。

```
[FW2] acl number 3500
[FW2-acl-adv-3500] rule permit ip source 172.16.40.0 0.0.0.255 destination 100.100.1.0 0.0.0.255
[FW2-acl-adv-3500] undo rule 5
[FW2-acl-adv-3500] quit
```

完成上述配置后，继续使用分部 2 的 PC2 访问总部的 PC5。


```

Ethernet adapter service:

Connection-specific DNS Suffix  . : 
Link-local IPv6 Address . . . . . : fe80::490d:d3a9:e1d2:249a%11
IPv4 Address. . . . . : 172.16.40.10
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 172.16.40.2

Tunnel adapter isatap.{D8FCA672-EF4F-476C-97EB-C2BBF3906A5A}:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix  . : 

Tunnel adapter isatap.{C67F2CCD-0648-4907-8C6A-E55B241DC2CC}:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix  . : 

C:\Users\Security>ping 100.100.1.10

Pinging 100.100.1.10 with 32 bytes of data:
Reply from 100.100.1.10: bytes=32 time=1ms TTL=126
Reply from 100.100.1.10: bytes=32 time<1ms TTL=126
Reply from 100.100.1.10: bytes=32 time<1ms TTL=126
Reply from 100.100.1.10: bytes=32 time<1ms TTL=126

Ping statistics for 100.100.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Security>_

```

图7-4 分部 2 访问总部业务测试

可以发现分部 2 与总部之间的业务已可以正常交互，分部 2 至总部的 IPsec VPN 排障完成。

步骤 4 检查分部 1 与分部 2 的业务

分部之间相互通信需要经过总部转发，数据走向为：

WWW Server↔FW1↔FW3↔FW2↔PC2，这种方式分部之间无需建立 IPsec VPN，分部 1 的 WWW Server 访问分部 2 的 PC2 的数据到达分部 1 的出口 FW1 时，FW1 将报文封装进 IPsec VPN 转发到 FW3，FW3 通过 IPsec VPN 将报文转发给 FW2，反向转发逻辑一致。

首先测试分部之间的业务连通性，使用分部 1 业务终端 WWW Server 访问分部 2 的 PC2。

```
C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter service:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::adb2:d4d4:aefb:74f7%13
    IPv4 Address. . . . . : 172.16.30.10
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 172.16.30.2

Ethernet adapter mgmt:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::2169:beba:a1d1:3fa1%12
    IPv4 Address. . . . . : 192.168.20.107
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.20.254

Tunnel adapter isatap.{CE306785-F74E-4E9C-9D2A-C55461647F7C}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Tunnel adapter isatap.{8157AE65-456B-4427-A7E1-B96ED4CB300A}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Users\Administrator>ping 172.16.40.10

Pinging 172.16.40.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.16.40.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

图7-5 分部1 访问分部2 业务测试（不可达）

测试发现分部1 与分部2 之间业务不可达。

首先查看分部1 出口设备 FW1 的 ACL 是否筛选了访问分部2 的业务流量。

```
<FW1> display acl all
Advanced ACL 3500, 2 rules ( Reference counter 1 )
Acl's step is 5
rule 10 permit ip source 172.16.30.0 0.0.0.255 destination 100.100.1.0 0.0.0.255 (13 times matched)
```

可以发现 FW1 设备上的 ACL 没有配置 WWW Server 网段到 PC2 网段的感兴趣流，需要补充。

在 FW1 上的 ACL 3500 添加 WWW Server 网段到 PC2 网段的感兴趣流。

```
[FW1] acl number 3500
[FW1-acl-adv-3500] rule permit ip source 172.16.30.0 0.0.0.255 destination 172.16.40.0 0.0.0.255
[FW1-acl-adv-3500] quit
```

同理，FW2 和 FW3 的感兴趣流也需要继续补充完善。

在 FW2 的 ACL 3500 添加 PC2 网段到 WWW Server 网段的感兴趣流。

```
[FW2] acl number 3500
[FW2-acl-adv-3500] rule permit ip source 172.16.40.0 0.0.0.255 destination 172.16.30.0 0.0.0.255
[FW2-acl-adv-3500] quit
```

在 FW3 的 ACL 3500 添加 WWW Server 网段到 PC2 网段、PC2 网段到 PC1 网段的感兴趣流。

```
[FW3] acl number 3500
[FW3-acl-adv-3500] rule permit ip source 172.16.30.0 0.0.0.255 destination 172.16.40.0 0.0.0.255
[FW3-acl-adv-3500] rule permit ip source 172.16.40.0 0.0.0.255 destination 172.16.30.0 0.0.0.255
[FW3-acl-adv-3500] quit
```

完成上述操作后，分部 1 业务终端 WWW Server 依旧无法访问分部 2 业务终端 PC2。

```
C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter service:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::adb2:d4d4:aefb:74f7%13
    IPv4 Address. . . . . : 172.16.30.10
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 172.16.30.2

Ethernet adapter mgmt:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::2169:beba:a1d1:3fa1%12
    IPv4 Address. . . . . : 192.168.20.107
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.20.254

Tunnel adapter isatap.{CE306785-F74E-4E9C-9D2A-C55461647F7C}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Tunnel adapter isatap.{8157AE65-456B-4427-A7E1-B96ED4CB300A}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Users\Administrator>ping 172.16.40.10

Pinging 172.16.40.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.16.40.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

图7-6 分部 1 访问分部 2 业务测试（不可达）

继续查看分部 1 出口设备 FW1 的 ACL 命中次数。

```
<FW1> display acl all
Advanced ACL 3500, 2 rules ( Reference counter 1 )
Acl's step is 5
rule 5 permit ip source 172.16.30.0 0.0.0.255 destination 100.100.1.0 0.0.0.255 (13 times matched)
```

```
rule 10 permit ip source 172.16.30.0 0.0.0.255 destination 172.16.40.0 0.0.0.255 (0 times matched)
```

可以发现分部 1 至分部 2 的 ACL 规则并未命中，根据之前的经验，如果流量没有被 IPSec VPN 的感兴趣流筛选，可能是数据优先被 NAT 处理。

检查 FW1 的 NAT 配置。

```
[FW1]nat-policy
[FW1-policy-nat]dis this
#
nat-policy
rule name IPSec-deny
source-zone local
source-zone trust
destination-zone untrust
destination-address 100.100.1.0 mask 255.255.255.0
action no-nat
rule name nat
source-zone local
source-zone trust
destination-zone untrust
action source-nat easy-ip
#
```

可以发现 FW1 上的 NAT 策略转换了 WWW Server 访问 PC2 流量的源地址。

修改 FW1 的 NAT 配置。

```
[FW1] nat-policy
[FW1-policy-nat] rule name IPSec-deny
[FW1-policy-nat-rule-IPSec-deny] destination-address 172.16.40.0 mask 255.255.255.0
[FW1-policy-nat-rule-IPSec-deny] quit
[FW1-policy-nat] quit
```

完成上述配置后，继续检查 FW1 的安全策略配置。

```
[FW1]security-policy
[FW1-policy-security]dis this
#
security-policy
rule name untrust-local
source-zone untrust
source-zone local
destination-zone untrust
destination-zone local
action permit
rule name trust-untrust
source-zone trust
destination-zone untrust
source-address 172.16.30.0 mask 255.255.255.0
destination-address 100.100.1.0 mask 255.255.255.0
action permit
```

```
rule name untrust-trust
 source-zone untrust
 destination-zone trust
 source-address 100.100.1.0 mask 255.255.255.0
 destination-address 172.16.30.0 mask 255.255.255.0
 action permit
#
```

可以发现 untrust 与 trust 之间的安全策略未放通 172.16.40.0/24 网段。

修改 FW1 的安全策略。

```
[FW1] security-policy
[FW1-policy-security] rule name trust-untrust
[FW1-policy-security-rule-trust-untrust] destination-address 172.16.40.0 mask 255.255.255.0
[FW1-policy-security-rule-trust-untrust] rule name untrust-trust
[FW1-policy-security-rule-untrust-trust] source-address 172.16.40.0 mask 255.255.255.0
[FW1-policy-security-rule-untrust-trust] quit
[FW1-policy-security] quit
```

同理修改 FW2 的安全策略。

```
[FW2] security-policy
[FW2-policy-security] rule name trust-untrust
[FW2-policy-security-rule-trust-untrust] destination-address 172.16.30.0 mask 255.255.255.0
[FW2-policy-security-rule-trust-untrust] rule name untrust-trust
[FW2-policy-security-rule-untrust-trust] source-address 172.16.30.0 mask 255.255.255.0
[FW2-policy-security-rule-untrust-trust] quit
[FW2-policy-security] quit
```

完成上述配置后，使用分部 1 的业务终端 WWW Server 测试到达分部 2 业务终端 PC2 的连通性。

```
C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter service:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::adb2:d4d4:aefb:74f7%13
    IPv4 Address. . . . . : 172.16.30.10
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 172.16.30.2

Ethernet adapter mgmt:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::2169:beba:a1d1:3fa1%12
    IPv4 Address. . . . . : 192.168.20.107
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.20.254

Tunnel adapter isatap.{CE306785-F74E-4E9C-9D2A-C55461647F7C}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Tunnel adapter isatap.{8157AE65-456B-4427-A7E1-B96ED4CB300A}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Users\Administrator>ping 172.16.40.10

Pinging 172.16.40.10 with 32 bytes of data:
Reply from 172.16.40.10: bytes=32 time=3ms TTL=125
Reply from 172.16.40.10: bytes=32 time=1ms TTL=125
Reply from 172.16.40.10: bytes=32 time=1ms TTL=125
Reply from 172.16.40.10: bytes=32 time=1ms TTL=125

Ping statistics for 172.16.40.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 3ms, Average = 1ms
```

图7-7 分部 1 访问分部 2 业务测试

可以发现分部 1 与分部 2 之间的业务已可以正常交互，分部 1 至分部 2 的 IPsec VPN 排障完成。

7.3 配置参考

7.3.1 FW1 配置

```
#
sysname FW1
#
acl number 3500
 rule 10 permit ip source 172.16.30.0 0.0.0.255 destination 100.100.1.0 0.0.0.255
 rule 15 permit ip source 172.16.30.0 0.0.0.255 destination 172.16.40.0 0.0.0.255
#
```

```
ipsec proposal 1
  esp authentication-algorithm sha2-256
  esp encryption-algorithm aes-256
#
ike proposal 1
  encryption-algorithm aes-256
  dh group14
  authentication-algorithm sha2-256
  authentication-method pre-share
  integrity-algorithm hmac-sha2-256
  prf hmac-sha2-256
#
ike peer 1
  pre-shared-key Huawei@123
  ike-proposal 1
  remote-address 100.1.1.8
  rsa encryption-padding oaep
  rsa signature-padding pss
  local-id-preference certificate enable
#
ipsec policy 1 10 isakmp
  security acl 3500
  ike-peer 1
  proposal 1
  tunnel local applied-interface
  sa trigger-mode auto
#
interface GE0/0/2
  undo shutdown
  ip address 10.3.1.2 255.255.255.252
  service-manage ping permit
  ipsec policy 1
#
interface GE0/0/5
  undo shutdown
  ip address 172.16.30.2 255.255.255.0
  service-manage http permit
#
firewall zone local
  set priority 100
#
firewall zone trust
  set priority 85
  add interface GE0/0/5
#
firewall zone untrust
  set priority 5
  add interface GE0/0/2
```

```
#
firewall zone dmz
 set priority 50
#
ip route-static 0.0.0.0 0.0.0.0 10.3.1.1
#
security-policy
 rule name untrust-local
  source-zone untrust
  source-zone local
  destination-zone untrust
  destination-zone local
  action permit
 rule name trust-untrust
  source-zone trust
  destination-zone untrust
  source-address 172.16.30.0 mask 255.255.255.0
  destination-address 100.100.1.0 mask 255.255.255.0
  destination-address 172.16.40.0 mask 255.255.255.0
  action permit
 rule name untrust-trust
  source-zone untrust
  destination-zone trust
  source-address 100.100.1.0 mask 255.255.255.0
  source-address 172.16.40.0 mask 255.255.255.0
  destination-address 172.16.30.0 mask 255.255.255.0
  action permit
#
nat-policy
 rule name IPSec-deny
  source-zone local
  source-zone trust
  destination-zone untrust
  destination-address 100.100.1.0 mask 255.255.255.0
  destination-address 172.16.40.0 mask 255.255.255.0
  action no-nat
 rule name nat
  source-zone local
  source-zone trust
  destination-zone untrust
  action source-nat easy-ip
#
return
```

7.3.2 FW2 配置

```
#
sysname FW2
```



```
#
acl number 3500
 rule 5 permit ip source 172.16.40.0 0.0.0.255 destination 100.100.1.0 0.0.0.255
 rule 5 permit ip source 172.16.40.0 0.0.0.255 destination 172.16.30.0 0.0.0.255
#
ipsec proposal 1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256
#
ike proposal 1
 encryption-algorithm aes-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer 1
 pre-shared-key Huawei@123
 ike-proposal 1
 remote-address 100.100.1.1
 remote-address 100.1.1.8
 rsa encryption-padding oaep
 rsa signature-padding pss
 local-id-preference certificate enable
 ikev2 authentication sign-hash sha2-256
#
ipsec policy 1 1 isakmp
 security acl 3500
 ike-peer 1
 proposal 1
#
interface GE0/0/2
 undo shutdown
 ip address 10.6.1.2 255.255.255.252
 service-manage ping permit
 ipsec policy 1
#
interface GE0/0/5
 undo shutdown
 ip address 172.16.40.2 255.255.255.0
 service-manage ping permit
#
firewall zone local
 set priority 100
#
firewall zone trust
 set priority 85
```

```
add interface GE0/0/5
#
firewall zone untrust
set priority 5
add interface GE0/0/2
#
firewall zone dmz
set priority 50
#
ip route-static 0.0.0.0 0.0.0.0 10.6.1.1
#
security-policy
rule name untrust-local
source-zone untrust
source-zone local
destination-zone untrust
destination-zone local
action permit
rule name trust-untrust
source-zone trust
destination-zone untrust
source-address 172.16.40.0 mask 255.255.255.0
destination-address 100.100.1.0 mask 255.255.255.0
destination-address 172.16.30.0 mask 255.255.255.0
action permit
rule name untrust-trust
source-zone untrust
destination-zone trust
source-address 100.100.1.0 mask 255.255.255.0
source-address 172.16.30.0 mask 255.255.255.0
destination-address 172.16.40.0 mask 255.255.255.0
action permit
#
return
```

7.3.3 FW3 配置

```
#
sysname FW3
#
acl number 3500
rule 5 permit ip source 100.100.1.0 0.0.0.255 destination 172.16.30.0 0.0.0.255
rule 10 permit ip source 100.100.1.0 0.0.0.255 destination 172.16.40.0 0.0.0.255
rule 15 permit ip source 172.16.30.0 0.0.0.255 destination 172.16.40.0 0.0.0.255
rule 20 permit ip source 172.16.40.0 0.0.0.255 destination 172.16.30.0 0.0.0.255
#
ipsec proposal 1
esp authentication-algorithm sha2-256
```

```
    esp encryption-algorithm aes-256
#
ike proposal 1
    encryption-algorithm aes-256
    dh group14
    authentication-algorithm sha2-256
    authentication-method pre-share
    integrity-algorithm hmac-sha2-256
    prf hmac-sha2-256
#
ike peer 1
    pre-shared-key Huawei@123
    ike-proposal 1
    rsa encryption-padding oaep
    rsa signature-padding pss
    local-id-preference certificate enable
    ikev2 authentication sign-hash sha2-256
#
ipsec policy-template map1 10
    security acl 3500
    ike-peer 1
    proposal 1
#
ipsec policy 1 1 isakmp template map1
#
interface GE0/0/1
    undo shutdown
ip address 100.1.1.8 255.255.255.0
    service-manage ping permit
    ipsec policy 1
#
interface GE0/0/7
    undo shutdown
ip address 100.100.1.1 255.255.255.0
    service-manage ping permit
#
firewall zone local
    set priority 100
#
firewall zone trust
    set priority 85
add interface GE0/0/7
#
firewall zone untrust
    set priority 5
    add interface GE0/0/1
#
firewall zone dmz
```

```
set priority 50
#
ip route-static 0.0.0.0 0.0.0.0 100.1.1.1
#
security-policy
rule name untrust-local
source-zone untrust
source-zone local
destination-zone untrust
destination-zone local
action permit
rule name trust-untrust
source-zone trust
destination-zone untrust
source-address 100.100.1.0 mask 255.255.255.0
destination-address 172.16.30.0 mask 255.255.255.0
destination-address 172.16.40.0 mask 255.255.255.0
action permit
rule name untrust-trust
source-zone untrust
destination-zone trust
source-address 172.16.30.0 mask 255.255.255.0
source-address 172.16.40.0 mask 255.255.255.0
destination-address 100.100.1.0 mask 255.255.255.0
action permit
#
return
```

7.3.4 RT1 预配置

```
#
sysname RT1
#
interface GigabitEthernet0/0/1
undo portswitch
#
interface GigabitEthernet0/0/1.2
dot1q termination vid 2
ip address 4.4.4.2 255.255.255.252
#
interface GigabitEthernet0/0/4
undo portswitch
ip address 10.3.1.1 255.255.255.252
#
ospf 1 router-id 33.33.33.1
import-route direct
import-route static
area 0.0.0.0
```

```
network 4.4.4.0 0.0.0.3
#
ip route-static 172.16.30.0 24 10.3.1.2
#
return
```

7.3.5 RT2 预配置

```
#
sysname RT2
#
interface GigabitEthernet0/0/1
undo portswitch
#
interface GigabitEthernet0/0/1.40
dot1q termination vid 40
ip address 3.3.3.2 255.255.255.252
#
interface GigabitEthernet0/0/4
undo portswitch
ip address 10.6.1.1 255.255.255.252
#
ospf 1 router-id 33.33.33.2
import-route direct
import-route static
area 0.0.0.0
network 3.3.3.0 0.0.0.3
#
ip route-static 172.16.40.0 24 10.6.1.2
#
return
```

7.3.6 SW1 预配置

```
#
sysname SW1
#
vlan batch 2 40
#
interface vlanif1
ip address 100.1.1.1 255.255.255.0
#
interface vlanif2
ip address 4.4.4.1 255.255.255.252
#
interface vlanif40
ip address 3.3.3.1 255.255.255.252
#
```

```
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 2 40
#
ospf 1 router-id 33.33.33.3
 import-route direct
 import-route static
 area 0.0.0.0
  network 3.3.3.0 0.0.0.3
  network 4.4.4.0 0.0.0.3
#
ip route-static 100.100.1.0 24 100.1.1.8
#
return
```

7.3.7 Mirror-SW 预配置

```
#
sysname Mirror-SW
#
vlan batch 2 40
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 2 40
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 2 40
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 2 40
#
return
```

7.3.8 SW2 预配置

```
#
sysname SW2
#
vlan batch 30
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 30
#
interface GigabitEthernet0/0/15
```

```
port link-type access
port default vlan 30
#
interface GigabitEthernet0/0/13
shutdown
#
interface GigabitEthernet0/0/14
shutdown
#
return
```

7.3.9 SW3 预配置

```
#
sysname SW3
#
vlan batch 40
#
interface GigabitEthernet0/0/1
port link-type access
port default vlan 40
#
interface GigabitEthernet0/0/14
port link-type access
port default vlan 40
#
return
```

7.4 思考题

本实验规划中，分部之间需要通过 IPSec VPN 互访，总部防火墙的安全策略需要如何设置？

参考答案：因分部互访的业务流量对于总部出口防火墙来说，并未跨越安全区域，所以无需配置相关的安全策略放行分部互访的流量。

8

SSL VPN 部署实验

8.1 实验介绍

8.1.1 关于本实验

某企业出口为防火墙设备，企业在途员工（Legal PC）需要使用 SSL VPN 的“网络拓展”功能访问企业总部内网的业务（PC1）。

本实验通过在企业出口防火墙 FW2 设备上部署 SSL VPN 虚拟网关，并配置网络扩展功能，满足企业在途员工访问企业内网的需求。

8.1.2 实验目的

- 掌握 SSL VPN 基本配置方法。
 - 实现企业在途员工对总部内网业务的访问。
-

8.1.3 实验组网介绍

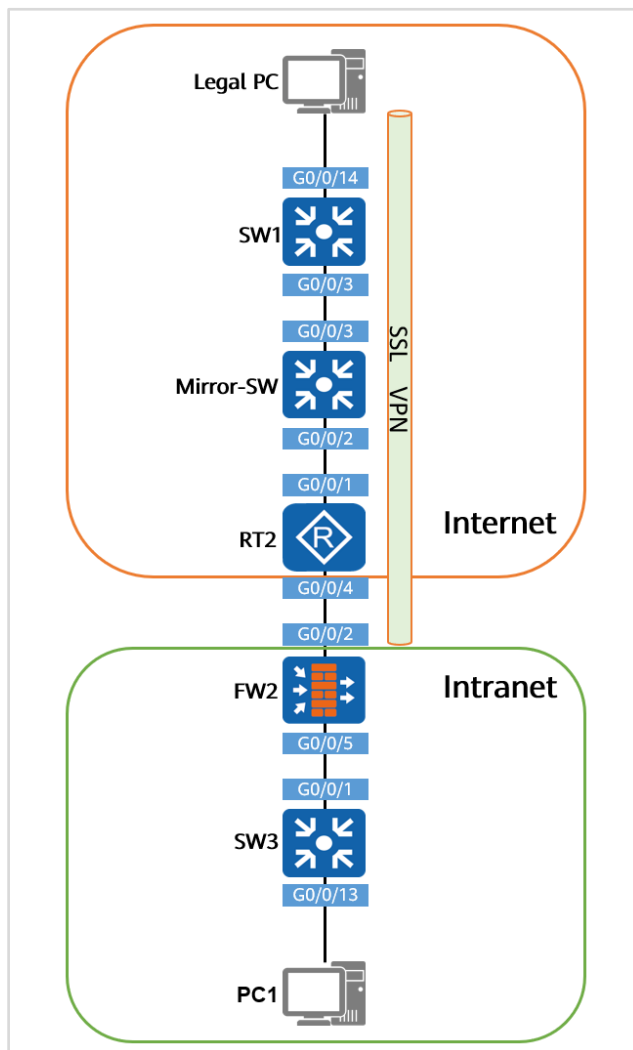


图8-1 SSL VPN 故障排除实验拓扑

FW2 作为企业出口安全设备，承载 SSL VPN 虚拟网关，企业在途用户（Legal PC）与 FW2 建立 SSL VPN 隧道，并通过 SSL VPN 网络扩展功能访问企业内网业务（PC1）。

SW3、RT2、Mirror-SW 和 SW1 设备已预配，具体配置在本实验步骤中不体现，详细配置可参考“8.4 配置参考”中相关设备的预配置，本实验重点介绍 FW2 设备上关键配置。

8.1.4 实验规划

表8-1 设备接口规划表

设备	接口	接口性质	接口信息	说明
SW1	G0/0/3	Trunk	PVID: 1 Allow-pass VLAN: 40	与Mirror-SW互连

	VLANIF40	三层接口	3.3.3.1/30	与RT2设备 GE0/0/1.40接口三层 互联
	G0/0/14	Access	PVID: 1000	连接Legal PC
	VLANIF1000	三层接口	100.20.1.1/24	Legal PC的网关
Mirror-SW	G0/0/2	Trunk	PVID: 1	互连接口
	G0/0/3		Allow-pass VLAN: 40	
SW3	G0/0/1	Access	PVID: 40	与FW2互连
	G0/0/13	Access	PVID: 40	连接PC1
FW2	GE0/0/2	三层接口	10.6.1.2/30 安全区域: untrust	Internet出接口, 与 RT2互连
	GE0/0/5	三层接口	172.16.10.1/24 安全区域: trust	PC1网关
RT2	GE0/0/1.40	三层子接口	3.3.3.2/30 终结VLAN40	与SW1设备VLANIF40 接口三层互连
	GE0/0/4	三层接口	10.6.1.1/30	与FW2互连
Legal PC	Ethernet0	网卡	100.20.1.2/24 网关: 100.20.1.1	终端
PC1	Ethernet0	网卡	172.17.10.2/24 网关: 172.17.10.1	终端

8.2 实验任务

8.2.1 配置思路

- 1.完成业务接口基础配置，并配置安全策略放行隧道协商流及业务流。
- 2.创建 UCL 组和用于 SSL VPN 远程接入的用户账号。
- 3.配置内网地址池用于远程用户接入内网时获取内网地址。
- 4.创建 SSL VPN 虚拟网关，并设置网关名称和网关端口等参数。
- 5.开启 SSL VPN 网络扩展功能，并设置相关参数。
- 6.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。

8.2.2 配置步骤 - CLI

步骤 1 接口基础配置

配置 FW2 设备业务接口 IP 地址及安全区域。

```
[FW2]interface GE0/0/2
[FW2-GE0/0/2] ip address 10.6.1.2 255.255.255.252
[FW2-GE0/0/2] service-manage ping permit
[FW2-GE0/0/2]quit
[FW2]interface GE0/0/5
[FW2-GE0/0/5] ip address 172.16.10.1 255.255.255.0
[FW2-GE0/0/5] service-manage ping permit
[FW2-GE0/0/5]quit
[FW2]firewall zone trust
[FW2-zone-trust] add interface GE0/0/5
[FW2-zone-trust]quit
[FW2]firewall zone untrust
[FW2-zone-untrust] add interface GE0/0/2
[FW2-zone-untrust]quit
[FW2]
```

步骤 2 配置安全策略

在防火墙 FW2 设备上配置安全策略，允许 SSL VPN 隧道协商流量及企业在途用户远程访问企业内网的业务流量。

```
[FW2]security-policy
[FW2-policy-security]rule name ssl_gw
[FW2-policy-security-rule-ssl_gw]source-zone untrust
[FW2-policy-security-rule-ssl_gw]destination-zone local
[FW2-policy-security-rule-ssl_gw]destination-address 10.6.1.2 32
[FW2-policy-security-rule-ssl_gw]action permit
[FW2-policy-security-rule-ssl_gw]quit
[FW2-policy-security]rule name ssl_oa
[FW2-policy-security-rule-ssl_oa]source-zone untrust
[FW2-policy-security-rule-ssl_oa]destination-zone trust
[FW2-policy-security-rule-ssl_oa]destination-address 172.16.10.0 24
[FW2-policy-security-rule-ssl_oa]action permit
[FW2-policy-security-rule-ssl_oa]quit
[FW2-policy-security]quit
[FW2]
```

步骤 3 创建 UCL 组和用户

创建 UCL 组（group1）和用于 SSL VPN 远程接入的用户账号（User001/Huawei@123）。

```
[FW2]acl-group name group1
[FW2]aaa
```

```
[FW2-aaa] local-access-user User001
[FW2-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.
[FW2-aaa-access-user-User001]service-type sslvpn
Warning: If the service type of local access users is configured multiple times, the new configuration
overwrites the previous one. The new configuration may cause local access users unable to go online.
Continue? [Y/N]:y
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.
[FW2-aaa-access-user-User001]ucl-group group1
[FW2-aaa-access-user-User001]quit
[FW2-aaa]quit
[FW2]
```

步骤 4 创建地址池

配置内网地址池（172.16.10.200-250），用于远程用户接入内网时，为其分配内网地址。

```
[FW2] ip pool ip_pool
[FW2-ip-pool-ip_pool] section 0 172.16.10.200 172.16.10.250
[FW2-ip-pool-ip_pool] quit
[FW2]
```

步骤 5 配置 SSL VPN 虚拟网关

创建 SSL VPN 虚拟网关，并设置网关名称和网关端口等参数，同时开启 SSL VPN 网络扩展功能，并设置相关参数。

```
[FW2] virtual-gateway SSL_Gateway_1
Warning: The SSL VPN function affects the performance of the entire system. Pay attention to the traffic
and CPU usage of the device.
[FW2-virtual-gateway-SSL_Gateway_1] service address 10.6.1.2 port 443
[FW2-virtual-gateway-SSL_Gateway_1] service
[FW2-virtual-gateway-SSL_Gateway_1-service] network-extension keep-alive timeout 120
[FW2-virtual-gateway-SSL_Gateway_1-service] network-extension ip-pool ip_pool
[FW2-virtual-gateway-SSL_Gateway_1-service] network-extension mode adapt
[FW2-virtual-gateway-SSL_Gateway_1-service] network-extension resource test ip-subnet 172.16.10.0
255.255.255.0
[FW2-virtual-gateway-SSL_Gateway_1-service] quit
[FW2-virtual-gateway-SSL_Gateway_1] quit
[FW2]
```

步骤 6 配置 SSL VPN 用户角色

配置 SSL VPN 的角色，并将角色关联到 UCL 组和允许访问的内网资源，进行资源访问授权。

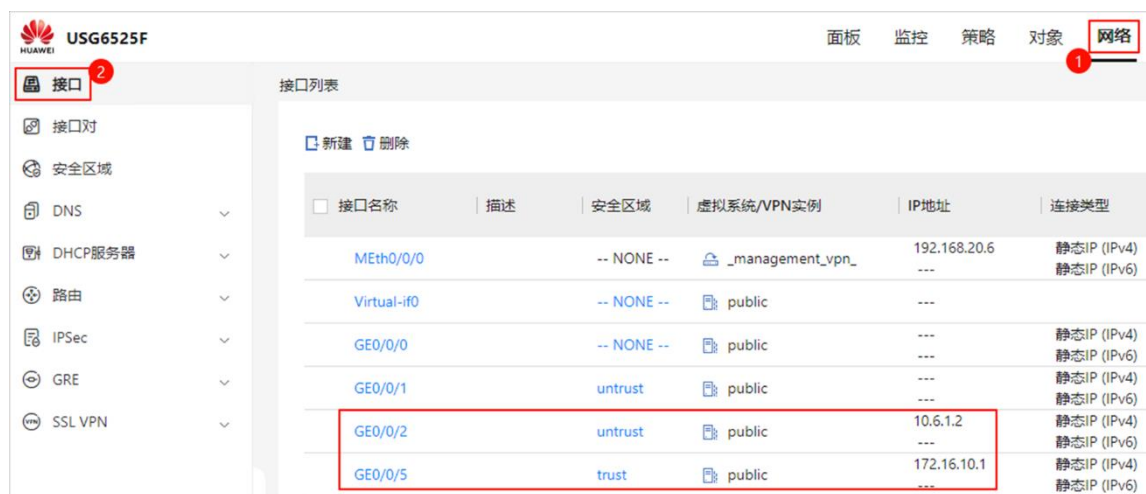
```
[FW2] virtual-gateway SSL_Gateway_1
[FW2-virtual-gateway-SSL_Gateway_1] role Role1
```

```
[FW2-virtual-gateway-SSL_Gateway_1-role-Role1] group group1
[FW2-virtual-gateway-SSL_Gateway_1-role-Role1] resource test
[FW2-virtual-gateway-SSL_Gateway_1-role-Role1] quit
[FW2-virtual-gateway-SSL_Gateway_1] quit
[FW2]
```

8.2.3 配置步骤 – Web

步骤 1 接口基础配置

在 FW2 设备 Web 管理界面选择“网络 > 接口”，进入接口列表配置界面，基于“6.2.3 配置步骤 - Web”中配置步骤，参考“表 8-1”数据规划，完成 FW2 设备业务接口的地址和安全区域的配置，配置完成后效果如下：



接口名称	描述	安全区域	虚拟系统/VPN实例	IP地址	连接类型
MEth0/0/0		-- NONE --	_management_vpn_	192.168.20.6	静态IP (IPv4)
Virtual-if0		-- NONE --	public	---	静态IP (IPv6)
GE0/0/0		-- NONE --	public	---	静态IP (IPv4)
GE0/0/0		-- NONE --	public	---	静态IP (IPv6)
GE0/0/1		untrust	public	---	静态IP (IPv4)
GE0/0/1		untrust	public	---	静态IP (IPv6)
GE0/0/2		untrust	public	10.6.1.2	静态IP (IPv4)
GE0/0/2		untrust	public	---	静态IP (IPv6)
GE0/0/5		trust	public	172.16.10.1	静态IP (IPv4)
GE0/0/5		trust	public	---	静态IP (IPv6)

图8-2 FW2 设备业务接口基础配置

步骤 2 配置安全策略

在 FW2 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”进入安全策略配置界面，执行以下操作，创建安全策略，放行 SSL VPN 隧道协商流量及远程用户访问企业内网的业务流量。

^ 概述

* 名称 ssl_gw

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 X

地址/地区 ① any

标签 请选择

目的

目的类型 ☒ 安全区域 ☐ 虚拟服务

安全区域 local X

地址/地区 ① 10.6.1.2/255.... X

标签 请选择

服务 ①

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 反病毒/入侵防御/URL过滤/内容过滤/文件过滤/邮件过滤/DNS过滤

转到“设置”以激活 Windows。

取消 命令预览 确定

图8-3 FW2 安全策略配置（SSL VPN 协商流）



^ 概述

* 名称

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

地址/地区

标签

目的

目的类型 ☒ 安全区域 ☐ 虚拟服务

安全区域

地址/地区

标签

服务

协议

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/文件过滤/邮件过滤/DNS过滤

转到“设置”以激活 Windows。

取消 命令预览 确定

图8-4 FW2 安全策略配置（SSL VPN 业务流）

步骤 3 创建 UCL 组和用户

在 FW2 设备 Web 管理界面选择“对象 > 用户 > 用户管理”，进入本地用户管理界面，执行以下操作，创建 UCL 组和本地用户，用于 SSL VPN 接入用户认证。

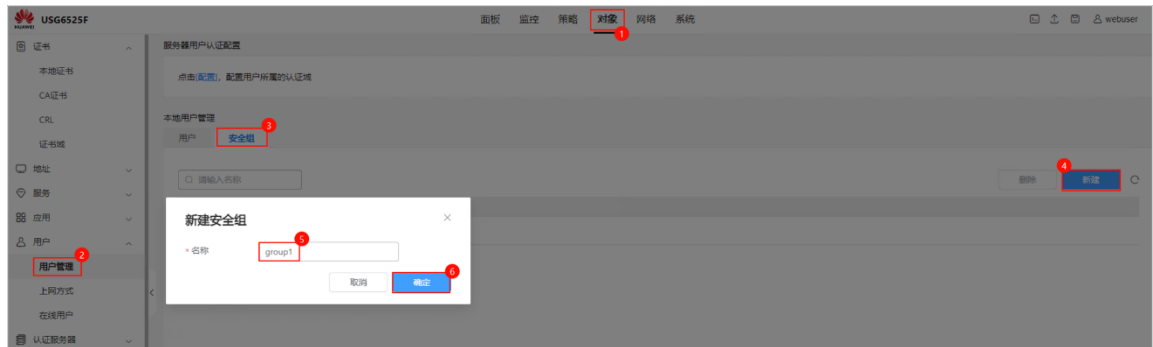


图8-5 创建 UCL 组

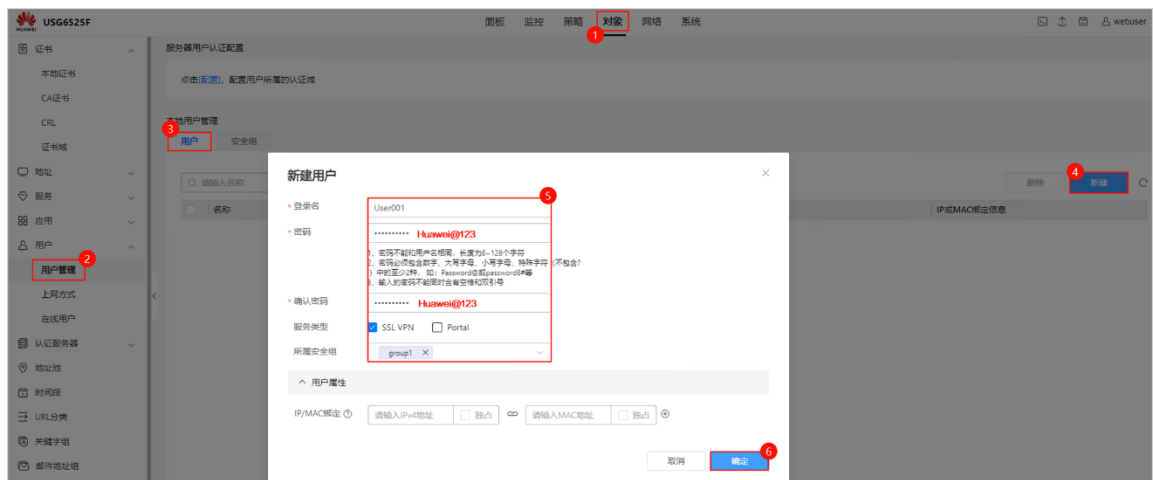


图8-6 创建本地 SSL VPN 用户

步骤 4 创建地址池

在 FW2 设备 Web 管理界面选择“对象 > 地址池 > 新建”，进入地址池配置界面，执行以下操作，创建内网地址池用于远程用户接入内网时获取内网地址。

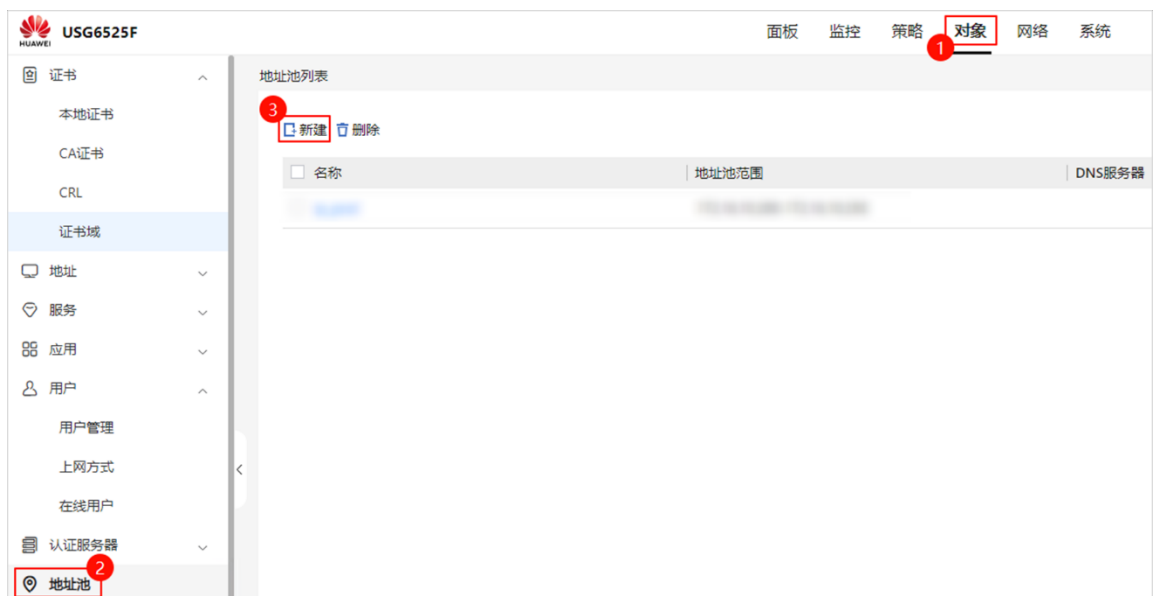


图8-7 进入地址池配置界面



图8-8 创建内网地址池

步骤 5 配置 SSL VPN 虚拟网关

在 FW2 设备 Web 管理界面选择“网络 > SSL VPN > SSL VPN > 新建”，进入 SSL VPN 网关配置界面，执行以下操作，配置 SSL VPN 虚拟网关并部署网络扩展功能，满足企业在途员工远程接入企业内网的需求。

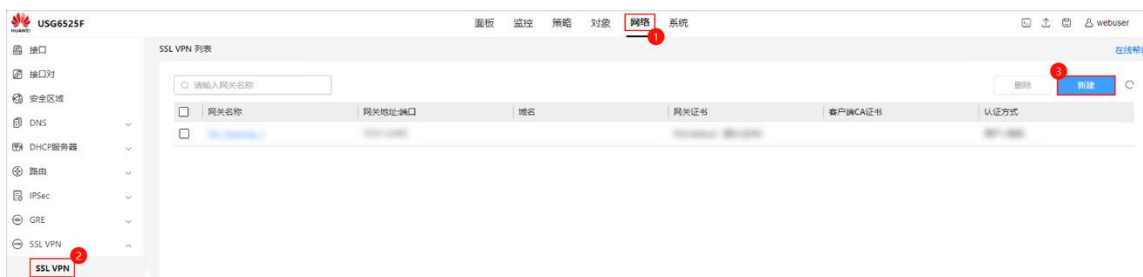


图8-9 进入 SSL VPN 虚拟网关配置界面



图8-10 SSL VPN 虚拟网关基础参数配置



图8-11 SSL VPN 网络扩展参数配置



图8-12 进入 SSL VPN 角色创建界面



图8-13 配置 SSL VPN 角色授权



图8-14 确定 SSL VPN 虚拟网关参数并提交配置

8.3 结果验证

使用 RDP 登录 Legal PC，模拟企业在途员工，打开桌面“univpn”客户端，执行以下操作：

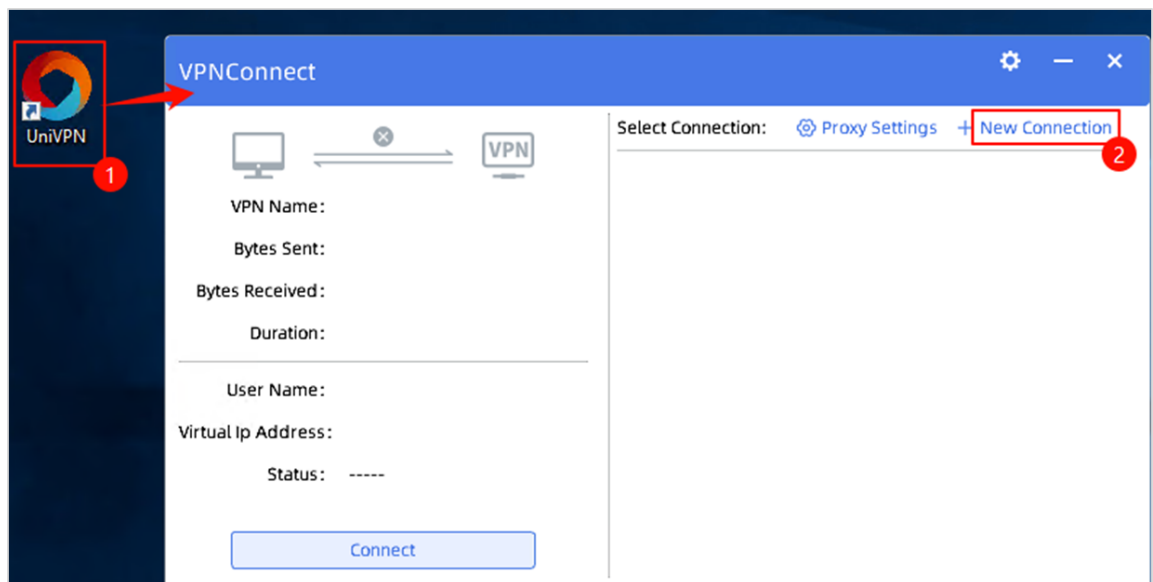
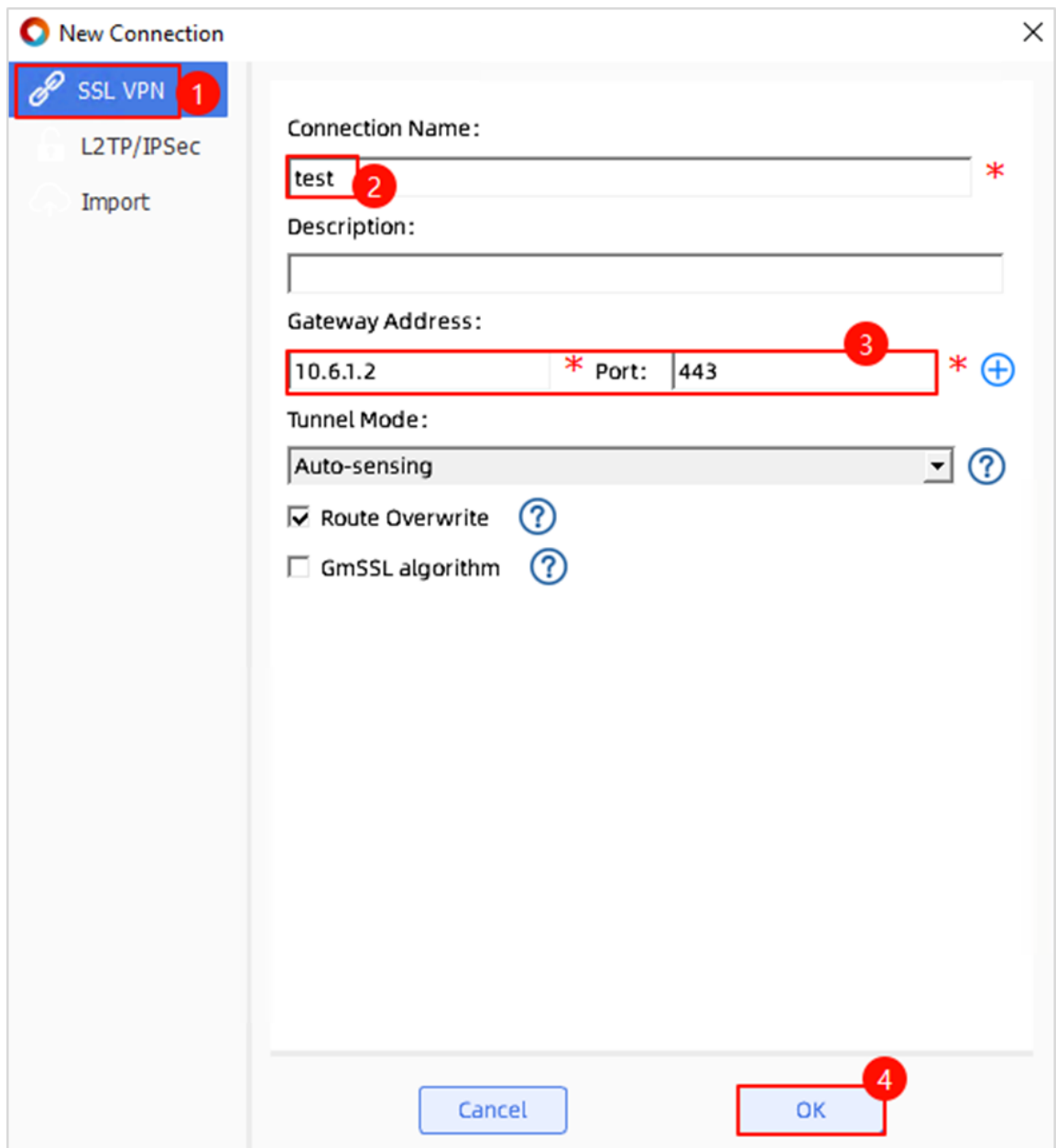


图8-15 打开 SSL VPN 客户端并进入 SSL VPN 连接配置界面



The image shows a 'New Connection' dialog box with a sidebar on the left and a main configuration area on the right. The sidebar contains three options: 'SSL VPN' (highlighted with a red box and a red circle '1'), 'L2TP/IPSec', and 'Import'. The main area contains the following fields and controls:

- Connection Name:** A text box containing 'test' (highlighted with a red box and a red circle '2'). A red asterisk '*' is to the right of the box.
- Description:** An empty text box.
- Gateway Address:** A text box containing '10.6.1.2' (highlighted with a red box and a red circle '3'). To its right is a label '* Port:' followed by a text box containing '443' (highlighted with a red box and a red circle '3'). A red asterisk '*' and a blue plus icon '+' are to the right of the port box.
- Tunnel Mode:** A dropdown menu showing 'Auto-sensing' (highlighted with a red box and a red circle '3'). A blue question mark icon '?' is to the right of the dropdown.
- Route Overwrite:** A checked checkbox with a blue question mark icon '?' to its right.
- GmSSL algorithm:** An unchecked checkbox with a blue question mark icon '?' to its right.

At the bottom of the dialog, there are two buttons: 'Cancel' and 'OK' (highlighted with a red box and a red circle '4').

图8-16 配置 SSL VPN 连接参数

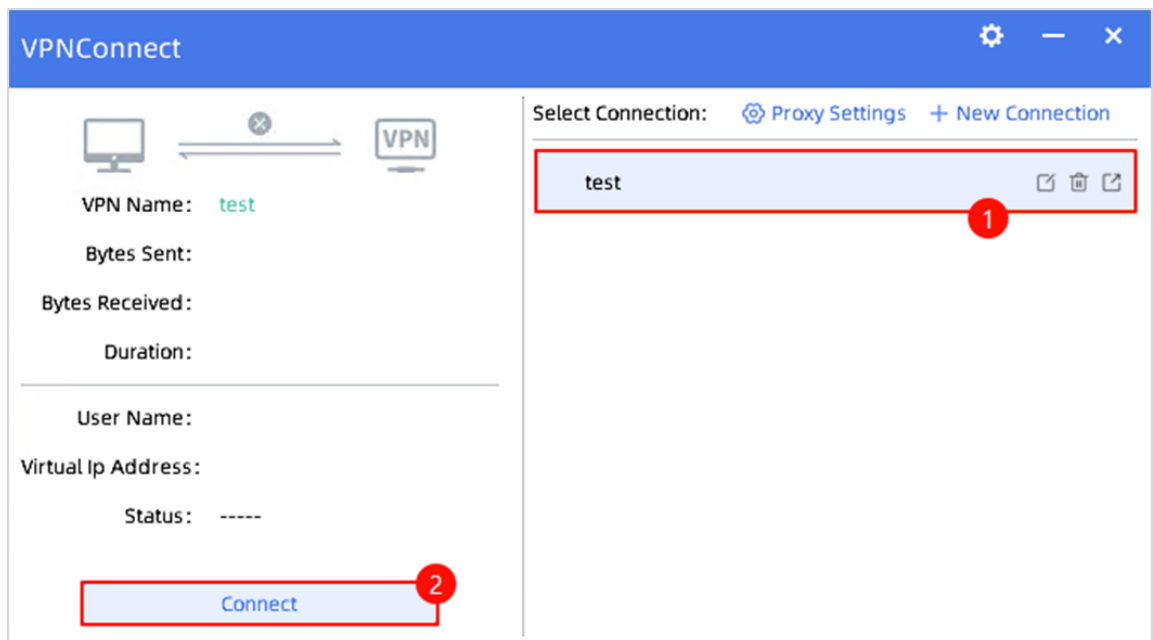


图8-17 连接 SSL VPN 网关

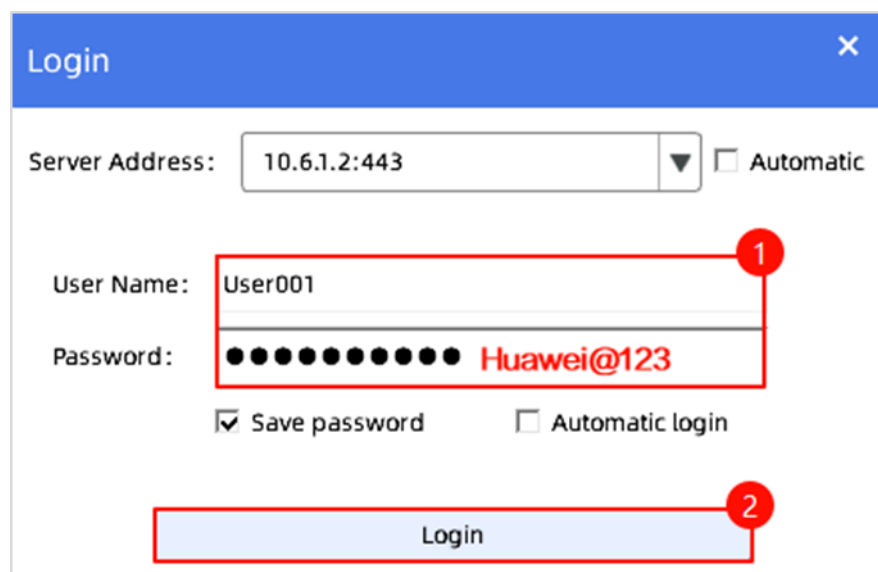


图8-18 登录 SSL VPN 网关

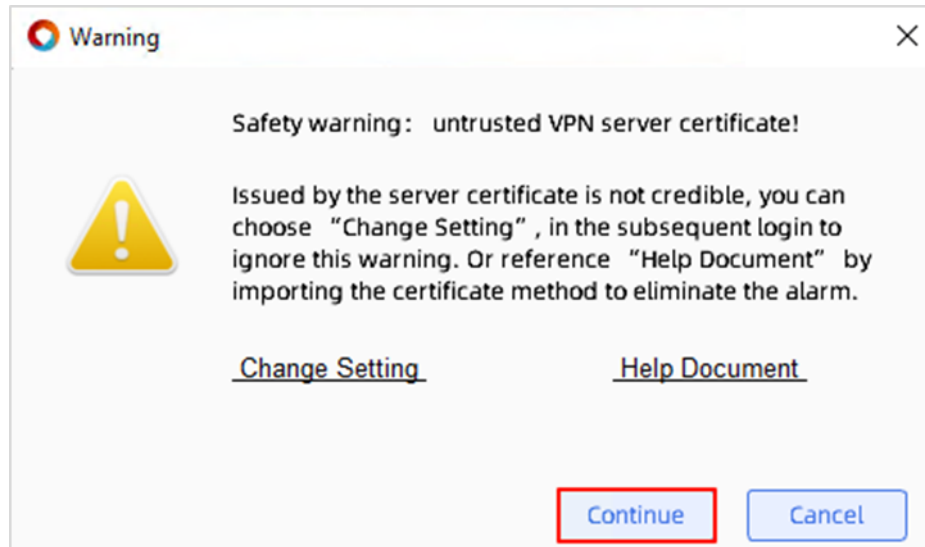


图8-19 忽略证书安全告警

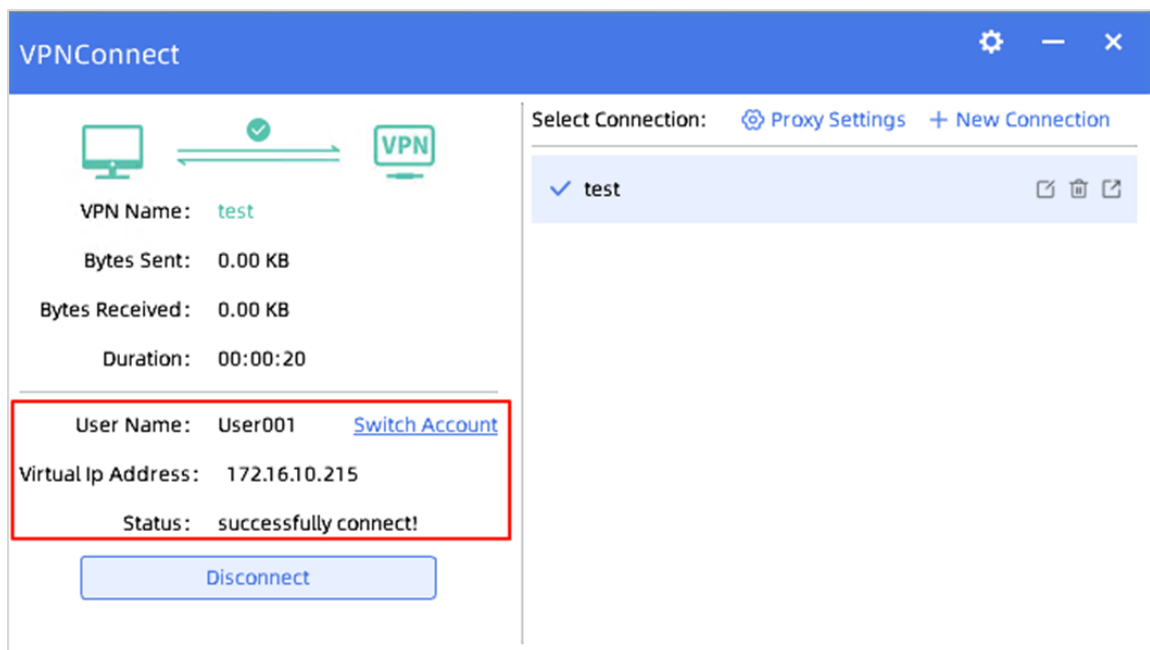


图8-20 SSL VPN 连接成功

打开 Legal PC 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：

```
C:\Users\Security>ipconfig

Windows IP Configuration

Unknown adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::7c5d:bc72:4e03:b46e%21
    IPv4 Address. . . . . : 172.16.10.215
    Subnet Mask . . . . . : 255.255.255.255
    Default Gateway . . . . . : 

Ethernet adapter mgmt:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::55a1:7a81:d1ef:8070%13
    IPv4 Address. . . . . : 192.168.20.109
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.20.254

Ethernet adapter service:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::4437:1c74:a79d:93e4%11
    IPv4 Address. . . . . : 100.20.1.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 100.20.1.1

Tunnel adapter isatap.{D8FCA672-EF4F-476C-97EB-C2BBF3906A5A}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Tunnel adapter isatap.{C67F2CCD-0648-4907-8C6A-E55B241DC2CC}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :
```

图8-21 Legal PC 查看网络参数

使用 Legal PC 访问企业内网 PC1，效果如下：


```
C:\Users\Security>ping 172.16.10.2

Pinging 172.16.10.2 with 32 bytes of data:
Reply from 172.16.10.2: bytes=32 time=2ms TTL=127
Reply from 172.16.10.2: bytes=32 time=1ms TTL=127
Reply from 172.16.10.2: bytes=32 time=1ms TTL=127
Reply from 172.16.10.2: bytes=32 time=1ms TTL=127

Ping statistics for 172.16.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\Users\Security>_
```

图8-22 Legal PC 访问企业内网 PC1

8.4 配置参考

8.4.1 FW2 配置

```
#
sysname FW2
#
ucl-group name group1
#
ip pool ip_pool
    section 0 172.16.10.200 172.16.10.250
#
aaa
    local-access-user User001
        service-type sslvpn
        ucl-group group1
    y
#
interface GE0/0/2
    ip address 10.6.1.2 255.255.255.252
    service-manage ping permit
#
interface GE0/0/5
    ip address 172.16.10.1 255.255.255.0
    service-manage ping permit
#
ip route-static 0.0.0.0 0.0.0.0 10.6.1.1
#
firewall zone trust
```

```
add interface GE0/0/5
#
firewall zone untrust
add interface GE0/0/2
#
security-policy
rule name ssl_gw
source-zone untrust
destination-zone local
destination-address 10.6.1.2 mask 255.255.255.255
action permit
rule name ssl_oa
source-zone untrust
destination-zone trust
destination-address 172.16.10.0 mask 255.255.255.0
action permit
#
virtual-gateway SSL_Gateway_1 0
service address 10.6.1.2 port 443
service
network-extension ip-pool ip_pool
network-extension resource test ip-subnet 172.16.10.0 255.255.255.0
role Role1 0
group group1
resource test
#
return
```

8.4.2 SW1 预配置

```
#
sysname SW1
#
vlan batch 40 1000
#
interface vlanif40
ip address 3.3.3.1 255.255.255.252
#
interface vlanif1000
ip address 100.20.1.1 255.255.255.0
#
interface GigabitEthernet0/0/3
port link-type trunk
port trunk allow-pass vlan 40
#
interface GigabitEthernet0/0/14
port link-type access
port default vlan 1000
```

```
#
ospf 1 router-id 33.33.33.3
import-route direct
area 0.0.0.0
network 3.3.3.0 0.0.0.3
#
return
```

8.4.3 Mirror-SW 预配置

```
#
sysname Mirror-SW
#
vlan 40
#
interface GigabitEthernet0/0/2
port link-type trunk
port trunk allow-pass vlan 40
#
interface GigabitEthernet0/0/3
port link-type trunk
port trunk allow-pass vlan 40
#
return
```

8.4.4 RT2 预配置

```
#
sysname RT2
#
interface GigabitEthernet0/0/1
undo portswitch
#
interface GigabitEthernet0/0/1.40
dot1q termination vid 40
ip address 3.3.3.2 255.255.255.252
#
interface GigabitEthernet0/0/4
undo portswitch
ip address 10.6.1.1 255.255.255.252
#
ospf 1 router-id 33.33.33.2
import-route direct
area 0.0.0.0
network 3.3.3.0 0.0.0.3
#
return
```

8.4.5 SW3 预配置

```
#
sysname SW3
#
vlan batch 40
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 40
#
interface GigabitEthernet0/0/13
 port link-type access
 port default vlan 40
#
return
```

8.5 思考题

防火墙部署了 SSL VPN 虚拟网关后，还能否复用为 IPSec VPN 网关？

参考答案：

可以复用，但是当防火墙设备既做 IPSec VPN 网关，也做 SSL VPN 网关时需要注意：

1. IPSec VPN 保护的内网流量和 SSL VPN 保护的内网流量不能重叠。
2. SSL VPN 外层隧道的流量不能在 IPSec 保护流量的范围内。

9 DDoS 攻击防御实验

9.1 实验介绍

9.1.1 关于本实验

为避免大规模 DDoS 攻击造成业务中断，企业在出口区部署 Anti-DDoS 设备，并通过 SecoManager 控制器对 Anti-DDoS 设备进行集中管理和策略下发。

9.1.2 实验目的

- 学会使用 SecoManager 管理中心纳管 Anti-DDoS 设备。
 - 掌握 SecoManager 管理中心使用方法。
 - 掌握使用 BGP 进行动态引流的配置方法。
 - 掌握通过 SecoManager 控制器对 Anti-DDoS 设备下发策略并阻断威胁流量的操作。
-

9.1.3 实验组网介绍

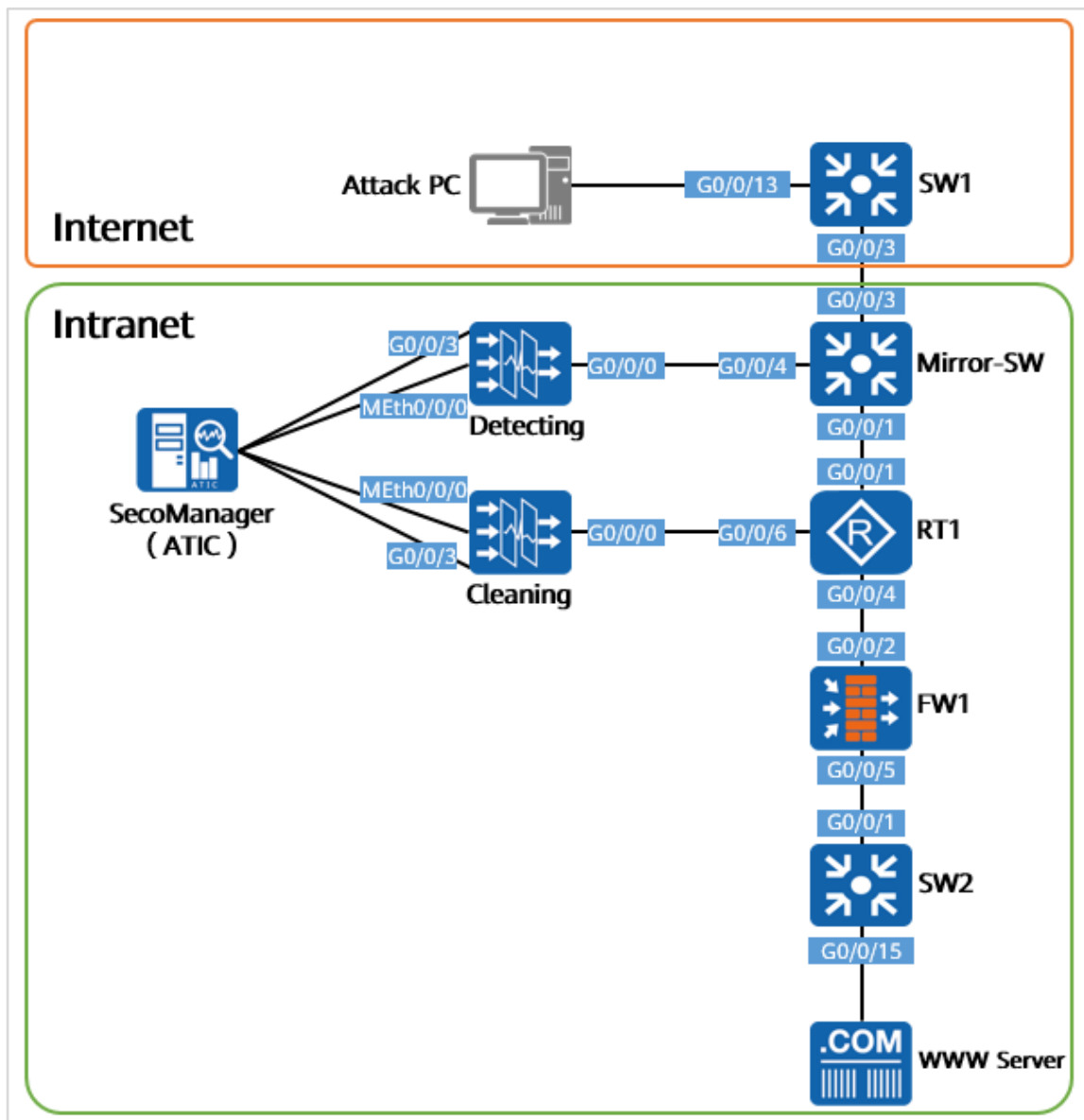


图9-1 DDoS 攻击防御实验拓扑

Attack PC 模拟 DDoS 攻击源，RT1 为企业出口路由器，在出口路由器上游部署了一台镜像交换机与 Anti-DDoS 检测设备对接，实现流量检测，企业内网部署了对外网提供服务的 Web 服务器（WWW Server）。

说明：SecoManager（ATIC）与 Detecting、Cleaning 设备之间实际由 Mirror-SW 设备连接，为了美化拓扑，方便读者观看，特以此种形式展现。SW1 和 SW2 设备已预配，具体配置可参考“9.4 配置参考”。

网络规划细节如下：

1. Internet 部分：Attack PC 的网关在 SW1 上。

2. 企业出口：最外侧为镜像交换机，负责将 Internet 访问企业总部内网的流量镜像到 Anti-DDoS 检测设备进行威胁检测。出口路由器与 Anti-DDoS 清洗设备之间通过部署 BGP 将 Internet 访问企业内网的恶意流量引流至 Anti-DDoS 清洗设备中清洗。
3. Anti-DDoS 系统：SecoManager 负责纳管 Anti-DDoS 检测设备、Anti-DDoS 清洗设备，并下发对应的检测和清洗策略。
4. 企业内网：Web 服务器需要对 Internet 提供服务，网关在 FW1 上。

9.1.4 实验规划

表9-1 设备接口规划表

设备	端口	接口性质	接口信息	说明
SW1	G0/0/3	Trunk	PVID: 1 Allow-pass VLAN: 2	与Mirror-SW互连
	G0/0/13	Access	PVID: 30	连接Attack PC
	VLANIF30	三层接口	20.20.20.1/24	Attack PC网关
	VLNAIF2	三层接口	4.4.4.1/30	与RT1三层互联
SW2	G0/0/1	Access	PVID: 30	与FW1互连
	G0/0/15	Access	PVID: 30	连接WWW Server
Mirror-SW	G0/0/1	Trunk	PVID: 1 Allow-pass VLAN: 2	与RT1互连
	G0/0/3			镜像端口
	G0/0/4	Access	PVID: 1	默认配置，观察端口
RT1	G0/0/1.2	三层子接口	4.4.4.2/30 终结VLAN2	与SW1互连
	G0/0/4	三层接口	10.3.1.1/30	与FW1互连
	G0/0/6	Trunk	PVID: 1 Allow-pass VLAN: 10 20	与Anti-DDoS清洗设备互连
	VLANIF10	三层接口	1.1.1.1/24	引流接口，与Anti-DDoS清洗设备 G0/0/0.1接口对接
	VLANIF20	三层接口	2.2.2.1/24	回注接口，与Anti-DDoS清洗设备

				G0/0/0.2接口对接
FW1	G0/0/2	三层接口	10.3.1.2/30 安全区域: untrust	与RT1互连
	G0/0/5	三层接口	172.16.30.2/24 安全区域: trust	与SW2互连, WWW Server网关
Detecting	MEth0/0/0	三层接口	vpn instance: _management_vpn_ 192.168.2.10/24	管理接口
	G0/0/0	Access	PVID: 1	检测接口, 与Mirror-SW互连
	G0/0/3	三层接口	192.168.2.13/24	日志发送接口
Cleaning	MEth0/0/0	三层接口	vpn instance: _management_vpn_ 192.168.2.12/24	管理接口
	G0/0/0	Trunk	PVID: 1 Allow-pass VLAN: 10 20	与RT1设备互联
	VLANIF10	三层接口	1.1.1.2/24	引流接口
	VLANIF20	三层接口	2.2.2.2/24	回注接口
	G0/0/3	三层接口	192.168.2.14/24	日志发送接口
SecoManager (ATIC)	ETH1	网卡	192.168.2.200/24	控制器业务对接
Attack PC	Ethernet0	网卡	20.20.20.2/24 网关: 20.20.20.1/24	终端
WWW Server	Ethernet0	网卡	172.16.30.10/24 网关: 172.16.30.2/24	终端

9.2 实验任务配置

9.2.1 配置思路

- 1.完成防火墙设备业务接口基础配置及安全策略配置。
- 2.基于拓扑规划, 合理配置 Anti-DDoS 设备的工作模式及业务接口。

- 3.在企业出口设备 Mirror-SW 设备上部署端口镜像，将进入企业内网的业务流量镜像至 Detecting 设备。
- 4.在 RT1 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（WWW Server）的可疑流量从 RT1 引流至 Cleaning 设备。
- 5.完成流量清洗后，Cleaning 设备通过 PBR 方式将流量回注至 RT1 设备。
- 6.在 Detecting 设备和 Cleaning 设备上部署 SNMP 和 STelnet 功能，用于对接 SecoManager。
- 7.登录 SecoManager 纳管 Detecting 设备和 Cleaning 设备，并配置防护对象和防御策略。

9.2.2 配置步骤

步骤 1 网络基本参数配置

按照“表 9-1”数据规划，完成网络基本参数配置。其中 SW1 和 SW2 设备已经预配，具体可参考“9.4 配置参考”。

Mirror-SW 设备作为企业出口镜像交换机，同时复用为 SecoManager（ATIC）控制器与 Anti-DDoS 设备之间的二层互联设备，需要完成相关接口的基础配置。

```
[Mirror-SW]vlan batch 2 43
[Mirror-SW]interface GigabitEthernet0/0/1
[Mirror-SW-GigabitEthernet0/0/1] port link-type trunk
[Mirror-SW-GigabitEthernet0/0/1] port trunk allow-pass vlan 2
[Mirror-SW-GigabitEthernet0/0/1]interface GigabitEthernet0/0/3
[Mirror-SW-GigabitEthernet0/0/3] port link-type trunk
[Mirror-SW-GigabitEthernet0/0/3] port trunk allow-pass vlan 2
[Mirror-SW-GigabitEthernet0/0/3]interface GigabitEthernet0/0/5
[Mirror-SW-GigabitEthernet0/0/5] port link-type access
[Mirror-SW-GigabitEthernet0/0/5] port default vlan 43
[Mirror-SW-GigabitEthernet0/0/5]interface GigabitEthernet0/0/6
[Mirror-SW-GigabitEthernet0/0/6] port link-type access
[Mirror-SW-GigabitEthernet0/0/6] port default vlan 43
[Mirror-SW-GigabitEthernet0/0/6]interface GigabitEthernet0/0/7
[Mirror-SW-GigabitEthernet0/0/7] port link-type access
[Mirror-SW-GigabitEthernet0/0/7] port default vlan 43
[Mirror-SW-GigabitEthernet0/0/7]interface GigabitEthernet0/0/8
[Mirror-SW-GigabitEthernet0/0/8] port link-type access
[Mirror-SW-GigabitEthernet0/0/8] port default vlan 43
[Mirror-SW-GigabitEthernet0/0/8]interface GigabitEthernet0/0/9
[Mirror-SW-GigabitEthernet0/0/9] port link-type access
[Mirror-SW-GigabitEthernet0/0/9] port default vlan 43
[Mirror-SW-GigabitEthernet0/0/9]quit
[Mirror-SW]
```

RT1 设备为企业出口设备，需要基于“表 9-1”数据规划完成业务接口基础配置。

```
[RT1]vlan batch 10 20
[RT1]interface GigabitEthernet0/0/1
```

```
[RT1-GigabitEthernet0/0/1] undo portswitch
[RT1-GigabitEthernet0/0/1]interface GigabitEthernet0/0/1.2
[RT1-GigabitEthernet0/0/1.2] dot1q termination vid 2
[RT1-GigabitEthernet0/0/1.2] ip address 4.4.4.2 255.255.255.252
[RT1-GigabitEthernet0/0/1.2]interface GigabitEthernet0/0/4
[RT1-GigabitEthernet0/0/4] undo portswitch
[RT1-GigabitEthernet0/0/4] ip address 10.3.1.1 255.255.255.252
[RT1-GigabitEthernet0/0/4]interface GigabitEthernet0/0/6
[RT1-GigabitEthernet0/0/6]portswitch
[RT1-GigabitEthernet0/0/6]port link-type trunk
[RT1-GigabitEthernet0/0/6]port trunk allow-pass vlan 10 20
[RT1-GigabitEthernet0/0/6]quit
[RT1]int vlan 10
[RT1-Vlanif10]ip add 1.1.1.1 24
[RT1-Vlanif10]int vlan 20
[RT1-Vlanif20]ip add 2.2.2.1 24
[RT1-Vlanif20]quit
[RT1]
```

FW1 设备为企业出口安全网关，需要基于“表 9-1”数据规划完成业务接口地址及安全区域配置。

```
[FW1]interface GE0/0/2
[FW1-GE0/0/2] ip address 10.3.1.2 255.255.255.252
[FW1-GE0/0/2]quit
[FW1]interface GE0/0/5
[FW1-GE0/0/5] ip address 172.16.30.2 255.255.255.0
[FW1-GE0/0/5]quit
[FW1]firewall zone trust
[FW1-zone-trust] add interface GE0/0/5
[FW1-zone-trust]quit
[FW1]firewall zone untrust
[FW1-zone-untrust] add interface GE0/0/2
[FW1-zone-untrust]quit
[FW1]
```

步骤 2 安全策略配置

在企业出口防火墙 FW1 设备上部署安全策略，允许 Internet 用户访问企业内网 WWW Server。

```
[FW1] security-policy
[FW1-policy-security] rule name to_www
[FW1-policy-security-rule-to_www] source-zone untrust
[FW1-policy-security-rule-to_www] destination-zone trust
[FW1-policy-security-rule-to_www] destination-address 172.16.30.10 mask 255.255.255.255
[FW1-policy-security-rule-to_www] action permit
[FW1-policy-security-rule-to_www] quit
[FW1-policy-security] quit
[FW1]
```

步骤 3 路由配置

在 FW1 和 RT1 设备之间部署 OSPF 协议，在 RT1 设备上配置缺省路由，用于访问 Internet，并将缺省路由发布在 OSPF 协议中。

```
[RT1]ip route-static 0.0.0.0 0.0.0.0 4.4.4.1
[RT1]ospf 1 router-id 33.33.33.1
[RT1-ospf-1] default-route-advertise always
[RT1-ospf-1] area 0.0.0.0
[RT1-ospf-1-area-0.0.0.0] network 10.3.1.0 0.0.0.3
[RT1-ospf-1-area-0.0.0.0]quit
[RT1-ospf-1]quit
[RT1]
```

```
[FW1] ospf 1 router-id 11.11.11.1
[FW1-ospf-1] import-route op-route
[FW1-ospf-1] area 0.0.0.0
[FW1-ospf-1-area-0.0.0.0] network 10.3.1.0 0.0.0.3
[FW1-ospf-1-area-0.0.0.0] network 172.16.30.0 0.0.0.255
[FW1-ospf-1-area-0.0.0.0] quit
[FW1-ospf-1] quit
[FW1]
```

步骤 4 NAT Server 配置

因企业内网 Web 服务器需要对 Internet 用户提供服务，所以需要为其配置 NAT Server，对 Internet 用户暴露公网地址，此处对外的公网地址设置为 100.100.100.100。

```
[FW1]nat server www global 100.100.100.100 inside 172.16.30.10 no-reverse route
```

步骤 5 工作模式及业务接口配置

修改检测设备的工作模式，并重启。

```
[Detecting]firewall ddos detect-spu slot 0 cpu 0
[Detecting]quit
<Detecting>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.
<Detecting>reboot fast
MPU 0:
Next startup system software: flash:/AntiDDoS1900_V600R022C00SPC100.cc
Next startup saved-configuration file: flash:/config.cfg
Next startup paf file: default
Next startup patch package: flash:/AntiDDoS1900_V600R022SPH150.PAT
Warning: The system will reboot. Continue? [Y/N]:y
System preprocessing has started, 100% completed.
System preprocessing succeeded.
```

等待 Detecting 设备重启完成后，检查当前设备工作模式，可以发现 Detecting 设备目前工作模式已切换为检测模式。

```
[Detecting] display ddos slot
Slot ID  CPU ID  Config  Register      Status
-----
0          0      detect  Registered    detect
-----
```

根据拓扑规划，配置 Detecting 设备接口安全区域。

```
[Detecting] firewall zone untrust
[Detecting-zone-untrust] add interface GE0/0/0
[Detecting-zone-untrust] quit
[Detecting] firewall zone trust
[Detecting-zone-trust] add interface GE0/0/3
[Detecting-zone-trust] quit
[Detecting]
```

根据拓扑规划，配置 Cleaning 设备接口安全区域。

```
[Cleaning] vlan batch 10 20
[Cleaning] interface Vlanif10
[Cleaning-Vlanif10] undo service-manage enable
[Cleaning-Vlanif10] quit
[Cleaning] interface Vlanif20
[Cleaning-Vlanif20] undo service-manage enable
[Cleaning-Vlanif20] quit
[Cleaning] interface GE0/0/0
[Cleaning-GE0/0/0] portswitch
[Cleaning-GE0/0/0] port link-type trunk
[Cleaning-GE0/0/0] port trunk allow-pass vlan 10 20
[Cleaning-GE0/0/0] quit
[Cleaning] firewall zone trust
[Cleaning-zone-trust] add interface GE0/0/3
[Cleaning-zone-trust] add interface Vlanif20
[Cleaning-zone-trust] quit
[Cleaning] firewall zone untrust
[Cleaning-zone-untrust] add interface Vlanif10
[Cleaning-zone-untrust] quit
[Cleaning] firewall zone dmz
[Cleaning-zone-dmz] add interface GE0/0/0
[Cleaning-zone-dmz] quit
[Cleaning]
```

Detecting 设备业务接口配置。

```
[Detecting] vlan 1
[Detecting-vlan1] interface GE0/0/3
[Detecting-GE0/0/3] ip address 192.168.2.13 24
[Detecting-GE0/0/3] undo service-manage enable
[Detecting-GE0/0/3] quit
```

```
[Detecting]interface GE0/0/0
[Detecting-GE0/0/0] portswitch
[Detecting-GE0/0/0] port link-type access
[Detecting-GE0/0/0] port default vlan 1
[Detecting-GE0/0/0] anti-ddos flow-statistic enable
[Detecting-GE0/0/0] anti-ddos detect enable
[Detecting-GE0/0/0] quit
[Detecting]
```

Cleaning 设备业务接口配置。

```
[Cleaning]interface G0/0/3
[Cleaning-GE0/0/3] ip address 192.168.2.14 24
[Cleaning-GE0/0/3] undo service-manage enable
[Cleaning-GE0/0/3] quit
[Cleaning]interface Vlanif10
[Cleaning-Vlanif10] ip address 1.1.1.2 255.255.255.0
[Cleaning-Vlanif10]quit
[Cleaning]interface Vlanif20
[Cleaning-Vlanif20] ip address 2.2.2.2 255.255.255.0
[Cleaning-Vlanif20]quit
[Cleaning]interface g0/0/0
[Cleaning-GE0/0/0]anti-ddos flow-statistic enable
[Cleaning-GE0/0/0]anti-ddos clean enable
[Cleaning-GE0/0/0]quit
[Cleaning]
```

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。

```
[Detecting]security-policy
[Detecting-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
[Detecting-policy-security]quit
[Detecting]
```

Cleaning 设备安全策略配置同上。

步骤 6 端口镜像配置

```
[Mirror-SW]observe-port 1 interface G0/0/4
[Mirror-SW]interface G0/0/3
[Mirror-SW-GigabitEthernet0/0/3]port-mirroring to observe-port 1 inbound
[Mirror-SW-GigabitEthernet0/0/3]quit
[Mirror-SW]
```

步骤 7 BGP 配置

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。

```
[Cleaning]route-policy 1 permit node 10
Info: New Sequence of this List
[Cleaning-route-policy]apply community no-advertise
[Cleaning-route-policy]quit
[Cleaning]bgp 100
[Cleaning-bgp]router-id 32.32.32.32
[Cleaning-bgp]peer 1.1.1.1 as-number 100
[Cleaning-bgp]import-route ospf
[Cleaning-bgp]ipv4-family unicast
[Cleaning-bgp-af-ipv4] peer 1.1.1.1 route-policy 1 export
[Cleaning-bgp-af-ipv4] peer 1.1.1.1 advertise-community
[Cleaning-bgp-af-ipv4] quit
[Cleaning-bgp]quit
[Cleaning]firewall ddos bgp-next-hop 2.2.2.1
[Cleaning]firewall ddos bgp-next-hop fib-filter
[Cleaning]
```

在 RT1 设备上配置 BGP 协议，与 Cleaning 设备建立 IBGP 邻居关系。

```
[RT1]bgp 100
[RT1-bgp]router-id 21.21.21.21
[RT1-bgp]peer 1.1.1.2 as-number 100
[RT1-bgp]quit
[RT1]
```

步骤 8 策略路由配置

在 Cleaning 设备上配置策略路由，将清洗后的业务流量回注。

```
[Cleaning]policy-based-route
[Cleaning-policy-pbr]rule name traffic_injection
[Cleaning-policy-pbr-rule-traffic_injection] ingress-interface vlanif10
[Cleaning-policy-pbr-rule-traffic_injection] action pbr egress-interface vlanif20 next-hop 2.2.2.1
[Cleaning-policy-pbr-rule-traffic_injection] quit
[Cleaning-policy-pbr]quit
[Cleaning]
```

为避免回注流量被再次送往 Cleaning 设备产生环路，需要在 RT1 设备上部署策略路由，将回注流量强行转发至下游防火墙设备。

```
[RT1]traffic classifier injection
[RT1-classifier-injection]if-match inbound-interface GigabitEthernet 0/0/6
[RT1-classifier-injection]quit
[RT1]traffic behavior injection
[RT1-behavior-injection] redirect ip-nexthop 10.3.1.2
[RT1-behavior-injection] quit
[RT1] traffic policy injection
[RT1-trafficpolicy-injection] classifier injection behavior injection
```

```
[RT1-trafficpolicy-injection] quit
[RT1]interface GigabitEthernet 0/0/6
[RT1-GigabitEthernet0/0/6]traffic-policy injection inbound
[RT1-GigabitEthernet0/0/6]quit
[RT1]
```

步骤 9 SNMP 与 STelnet 配置

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

```
[Detecting]snmp-agent
Info: It will create the SNMP listening socket after the source interface or source address is configured.
[Detecting]snmp-agent sys-info version v3
[Detecting]snmp-agent mib-view included mib2view iso
[Detecting]snmp-agent group v3 secomanager privacy read-view mib2view write-view mib2view notify-view mib2view
[Detecting]snmp-agent usm-user v3 atic
Warning: Configuring a security algorithm is recommended, because the noauthentication or authentication mode is insecure.
[Detecting]snmp-agent usm-user v3 atic group secomanager
Warning: Configuring a security algorithm is recommended, because the noauthentication or authentication mode is insecure.
[Detecting]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.
[Detecting]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.
[Detecting]snmp-agent protocol source-status all-interface
Warning: It will allow all accessible network to access the device.
[Detecting] snmp-agent trap enable
[Detecting] snmp-agent trap source G0/0/3
[Detecting]aaa
[Detecting-aaa]local-user aticuser password irreversible-cipher HCIP@Security12#$
[Detecting-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
[Detecting-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.
[Detecting-aaa] local-aaa-user password policy administrator
[Detecting-aaa-lupp-admin] undo password alert original
```

```
Warning: Original password alert has been disabled, there is a security risk.
[Detecting-aaa-lupp-admin]password expire 0
[Detecting-aaa-lupp-admin] quit
[Detecting-aaa] undo local-aaa-user wrong-password
Warning: All blocked users will unblock. Continue? [Y/N]:y
[Detecting-aaa] quit
[Detecting] ssh user aticuser
Info: Succeeded in adding a new SSH user.
[Detecting] ssh user aticuser authentication-type all
[Detecting] ssh user aticuser service-type all
[Detecting] snetconf server enable
Info: Succeeded in starting the SNETCONF server on SSH port 22.
Warning: After configuring the source interface or source address, the IPV4/IPV6 listening socket will be
created.
[Detecting] netconf
[Detecting-netconf]protocol inbound ssh ipv4 port 830
Info: Succeeded in starting the ssh port 830 service.
Warning: After configuring the source interface or source address, the IPV4 listening socket will be
created.
[Detecting-netconf]
[Detecting-netconf] nacm
[Detecting-netconf-nacm] nacm enable
[Detecting-netconf-nacm]group-name nacm-group
[Detecting-netconf-nacm-nacm-group-nacm-group] user-name aticuser
[Detecting-netconf-nacm-nacm-group-nacm-group] quit
[Detecting-netconf-nacm] execute-default permit
[Detecting-netconf-nacm]quit
[Detecting-netconf] quit
[Detecting]rsa local-key-pair create
The key name will be:Host
The range of public key size is (2048, 4096).
NOTE: Key pair generation will take a short while.
Please input the modulus [default = 3072]:
[Detecting] user-interface vty 0 4
[Detecting-ui-vty0-4]authentication-mode aaa
[Detecting-ui-vty0-4]user privilege level 3
[Detecting-ui-vty0-4]protocol inbound ssh
[Detecting-ui-vty0-4] quit
[Detecting] stelnet server enable
Info: Succeeded in starting the STelnet server.
Warning: After configuring the source interface or source address, the IPV4/IPV6 listening socket will be
created.
[Detecting] ssh user aticuser
Info: The SSH user aticuser already exist.
[Detecting] ssh user aticuser authentication-type password
[Detecting] ssh user aticuser service-type stelnet
[Detecting] 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.
[Detecting] 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.
[Detecting] ssh user aticuser service-type all
[Detecting] ssh user aticuser sftp-directory flash:/
[Detecting]
```

Cleaning 设备配置同上。

步骤 10 设备纳管

登录 SecoManager 业务平面选择“设备管理 > 设备”进入设备管理配置界面，执行以下操作：



图9-2 进入设备管理界面



图9-3 进入设备 SSH 指纹策略配置界面

设备SSH指纹校验策略配置

① 为保证自动发现的设备是可信的，需要进行指纹配置，有以下两种方式：

方式1：在控制器中导入设备的SSH公钥指纹，在控制器和设备建立SSH连接时，对设备返回的公钥指纹和导入的指纹进行匹配，如果不匹配则无法和设备建立连接。

方式2：选择信任首次学习的指纹，在信任该指纹的前提下，用户也可以对该指纹进行锁定，如果相同管理IP的设备指纹发生变化，则控制器无法再对该设备建立连接。

信任设备SSH指纹

信任首次学习的指纹

① 开关打开，控制器和设备建立连接的过程中会自动获取设备的SSH公钥指纹，并存储；开关关闭，需要用户导入设备的SSH公钥指纹。

☒

锁定首次学习的指纹

① 开关打开，控制器锁定首次学习到的指纹，如果设备SSH公钥指纹发生变化，则控制器无法连接设备；开关关闭，控制器不锁定首次学习到的SSH公钥指纹，如果设备SSH公钥指纹发生变化，控制器自动更新存储的公钥指纹。

☐

导入设备SSH指纹

① 1、一次最多只能导入500条数据。

2、查看已导入设备SSH指纹请打开“系统管理 > 系统设置 > 南向协议 > SSH客户端配置”。

下载模板：[模板.xls](#)

上传文件：

...

上传

返回

图9-4 配置设备 SSH 指纹验证策略

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

添加设备

删除

更多

自动发现

创建Flow集群

名称	管理IP	ESN	设备版本	设备状态

图9-5 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

特征库升级管理

采集器

防御组

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: 192.168.2.10
192.168.2.12

选择模板 保存模板

SNMPv3

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

* 超时时间(毫秒): 4000

图9-6 配置设备扫描参数(1)



NETCONF

* 用户名: aticuser

* 密码: HCIP@Security12#\$

* 端口: 830

STELNET

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: HCIP@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: HCIP@Security12#\$

其他设置

虚拟系统容量:

开始扫描

图9-8 设备扫描成功

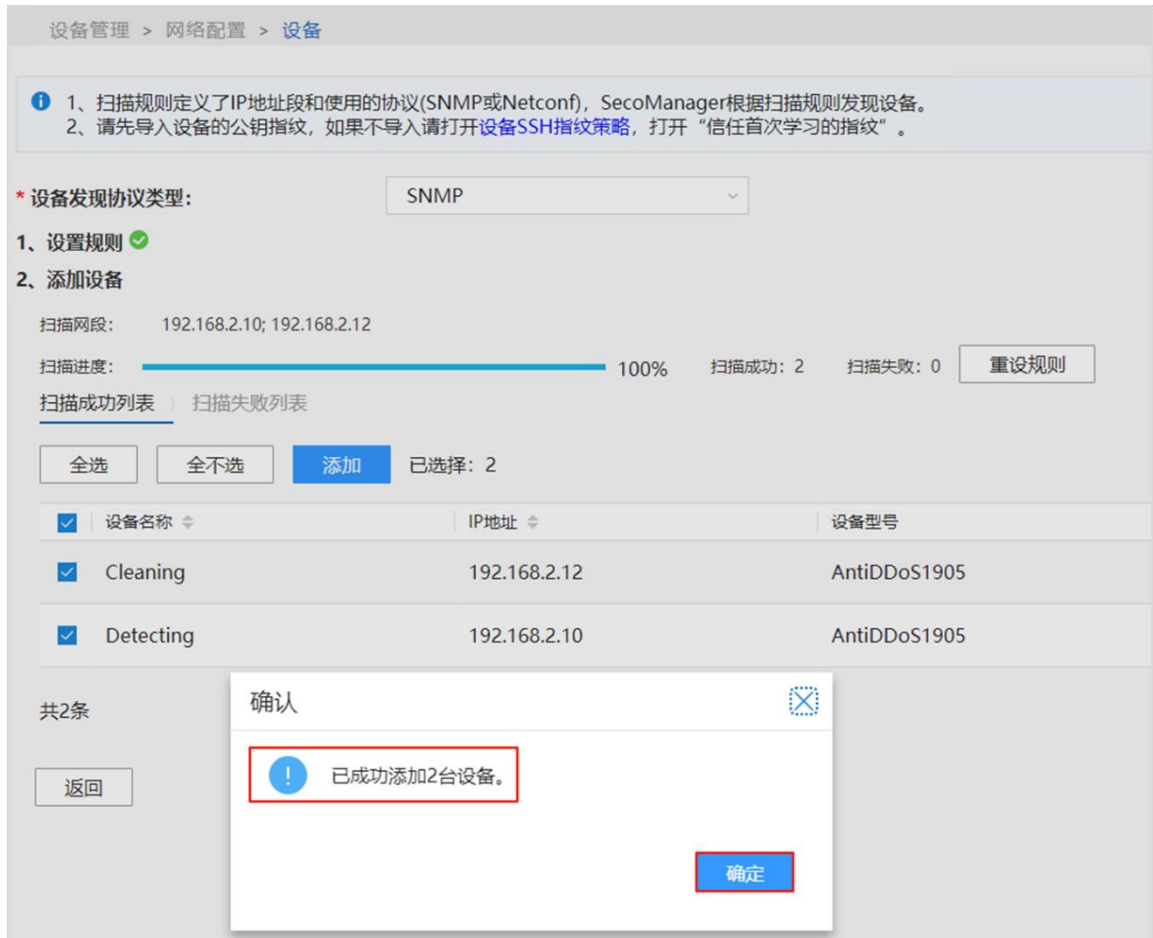


图9-9 设备成功添加

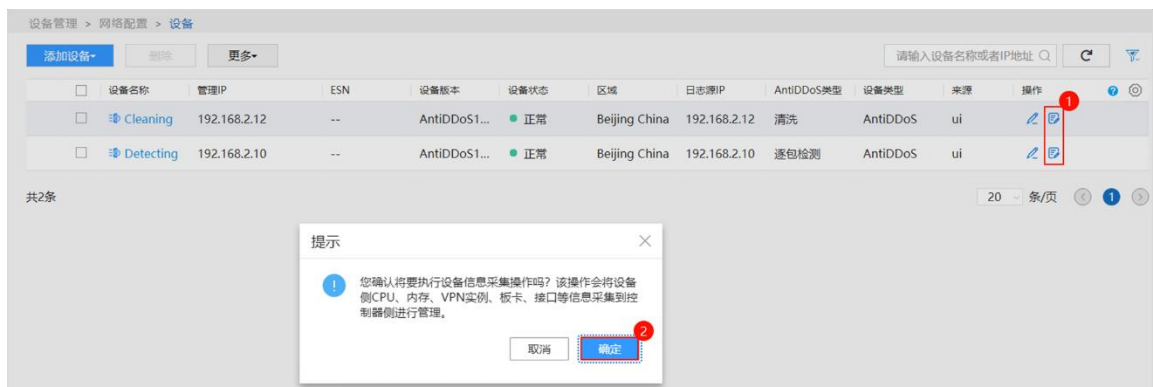


图9-10 采集 Anti-DDoS 设备信息



图9-11 进入采集器配置界面

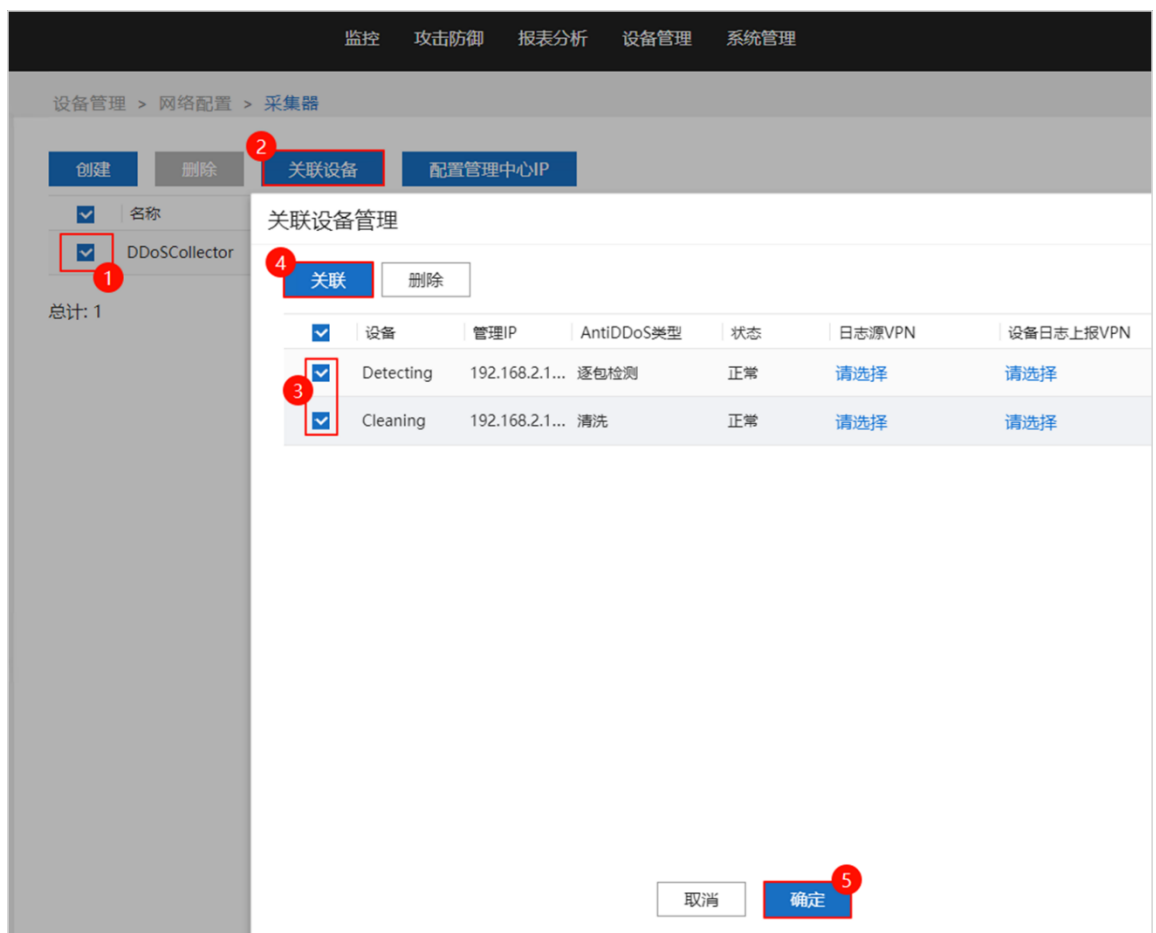


图9-12 采集器关联 Anti-DDoS 设备

步骤 11 防护对象配置

在 SecoManager 业务平面选择“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作参考。



图9-13 进入防护对象创建页面



图9-14 创建防护对象



图9-15 设置防护对象参数（1）



图9-16 设置防护对象参数（2）

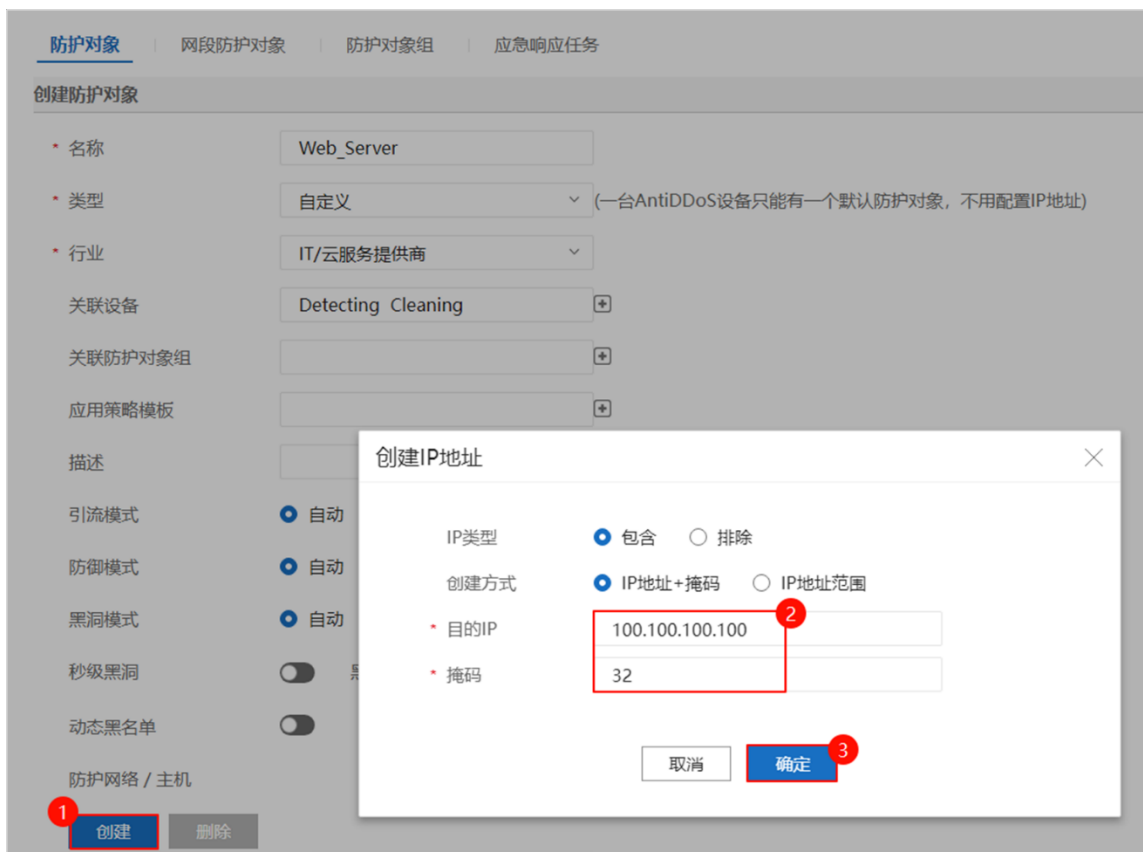


图9-17 设置防护对象参数（3）

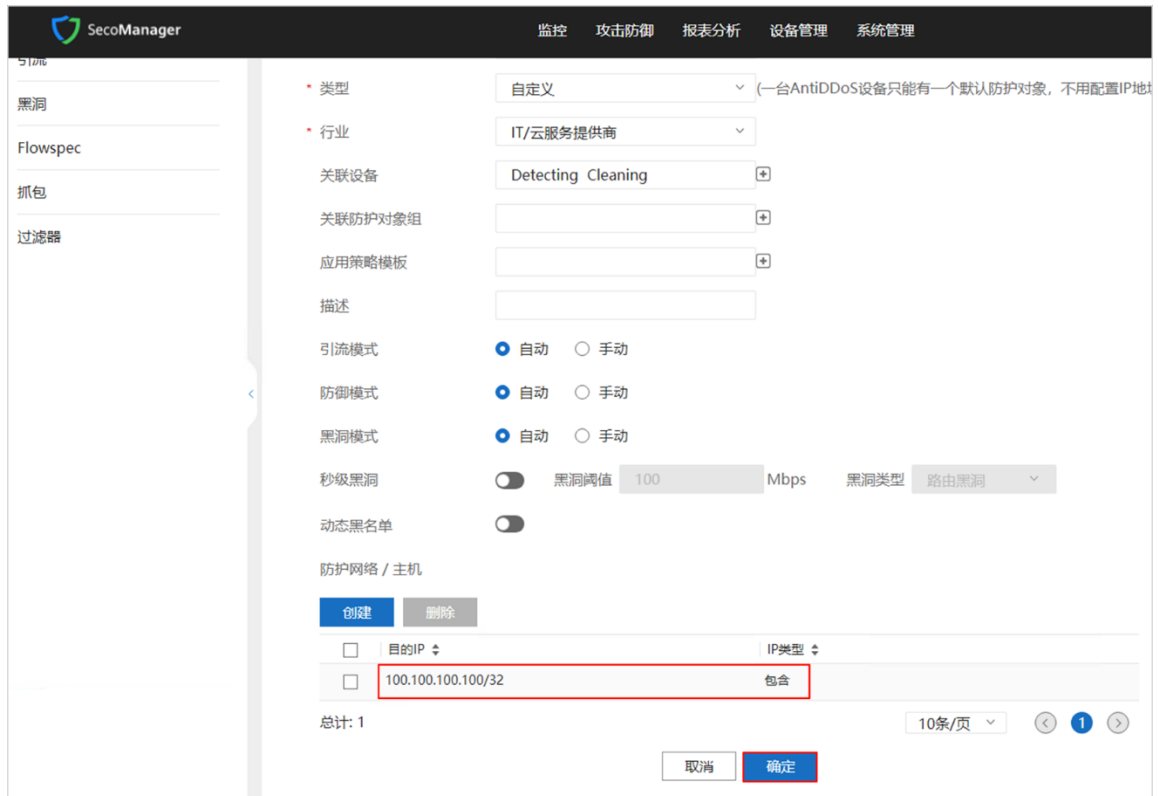


图9-18 确认防护对象参数并提交

防护对象创建完成后效果如下：



防护对象	基线学习	异常状态	防御状态	引流状态	部署状态	防御...	过滤器
Web_Server	未学习	正常	--	未引流	未部署		0

图9-19 防护对象创建完成

步骤 12 防御策略配置

登录 SecoManager 业务平面选择“攻击防御 > 防御对象”进入防御对象配置页面，执行以下操作：

防护对象 | 网段防护对象 | 防护对象组 | 应急响应任务

创建 部署 迁移 拆除 删除 基线学习 设置告警分级 导入/导出

支持输入星号模糊查询 高级查询

☐	防护对象	基线学习	异常状态	防御状态	引流状态	部署状态	防御...	过滤器	位置...	黑名单	白名单	告警...	应用模板	① 操作
☒	Web_Server	未学习	正常	--	未引流	未部署		0	0	0	0		--	编辑 删除
名称	IP策略	TCP策略	UDP策略	ICMP策略	HTTP策略	TLS策略	DNS策略	SIP策略	防护对象策略	操作	应用模板			
Detecting	限流 防御	限流 防御	限流 防御	限流	防御	防御	限流 防御	未配置	未配置	编辑 删除	不涉及			
Cleaning	限流 防御	限流 防御	限流 防御	限流	防御	防御	限流 防御	未配置	未配置	编辑 删除	不涉及			

总计: 1

10条/页

图9-20 进入防御策略编辑界面

防御策略

☒ 显示全部
☐ 只显示开启

导入策略模板

导出策略模板

+

防护对象限流

+

IP Flood限流

+

IP Flood防御

+

TCP异常报文防御

+

SYN Flood防御

+

SYN-ACK Flood防御

+

ACK Flood防御

+

FIN/RST Flood防御

+

TCP连接攻击防御

+

TCP限流

+

UDP异常报文防御

+

UDP Flood防御

+

UDP限流

+

HTTP Flood防御

+

HTTP 异常连接防御

+

TLS加密攻击防御

+

TLS会话攻击防御

+

DNS异常报文防御

+

DNS Query Flood防御

+

DNS Reply Flood防御

+

DNS限速

1

+

ICMP限流

+

ICMP限流 (pps)

+

SIP Flood防御

+

SIP限速

2

1

(1-2,000,000)

3

保存

4

返回

部署

图9-21 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 1 pps（Detecting 和 Cleaning 设备均需配置），实际部署时需根据业务防护需求合理设置。



图9-22 部署防护对象



图9-23 防护对象部署成功

9.3 结果验证

使用 RDP 登录 Attack PC，打开多个命令行窗口，对企业 Web 服务器进行不间断并发 Ping 测试（ping 100.100.100.100 -t），模拟来自互联网用户的 DDoS 流量：

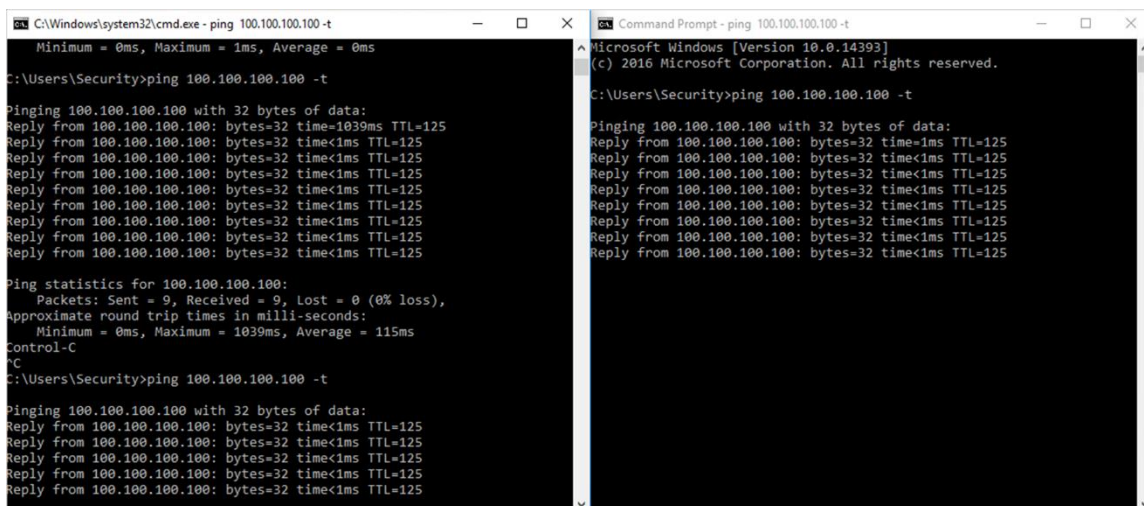


图9-24 Attack PC 模拟 DDoS 攻击流量

登录 SecoManager 业务平面，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9-25 检测到 DDoS 攻击后防护对象的状态

在 SecoManager 业务平面选择“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9-26 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：

告警详情

[告警详情和处理建议](#) | 最近2个月处理记录

基本信息

名称:	防护对象状态异常	首次发生时间:	11:18:40
最近发生时间:	11:18:40	次数:	1
告警ID:	0x000493ea	级别:	提示
类型:	通信告警	附加信息:	防护对象名称=Web_Server; 攻击详情= 攻击类型: ICMP Flood 阈值: 1pps/- 入流量: 1pps/- 目的端口: -; 设备名称=Detecting; 防御模式=auto

定位信息: 防护对象IP=100.100.100.100;
方向=inbound;

备注

单击编辑备注信息。

清除 确认 关闭

图9-27 查看防护对象异常的告警详情

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

SecoManager

监控 攻击防御 报表分析 设备管理 系统管理

攻击防御 > 策略管理 > 引流

引流任务 [引流日志](#)

导出 导出全部

设备	防护对象	目的IP	掩码	VPN	操作时间	操作人	客户源IP	操作	结果	模式	备注
Cleaning	Web_Server	100.100.100.100	32	--	11:18:40	--	--	创建	成功	自动	--
Cleaning	Web_Server	100.100.100.100	32	--	11:18:40	--	--	启用	成功	自动	--

总计: 2

20条/页

图9-28 查看引流日志

9.4 配置参考

说明：Detecting 设备和 Cleaning 设备包含控制器下发的内容，请勿直接复制配置脚本输入设备，建议参考上文流程进行配置。

9.4.1 FW1 配置

```
#  
sysname FW1  
#  
interface GE0/0/2
```

```
ip address 10.3.1.2 255.255.255.252
service-manage ping permit
#
interface GE0/0/5
ip address 172.16.30.2 255.255.255.0
service-manage ping permit
#
ospf 1 router-id 11.11.11.1
import-route ospf
opaque-capability enable
area 0.0.0.0
network 10.3.1.0 0.0.0.3
network 172.16.30.0 0.0.0.255
#
firewall zone trust
set priority 85
add interface GE0/0/5
#
firewall zone untrust
set priority 5
add interface GE0/0/2
#
nat server www global 100.100.100.100 inside 172.16.30.10 no-reverse route
#
security-policy
rule name to_www
source-zone untrust
destination-zone trust
destination-address 172.16.30.10 mask 255.255.255.255
action permit
#
return
```

9.4.2 RT1 配置

```
#
sysname RT1
#
vlan batch 10 20
#
traffic classifier injection operator or
if-match inbound-interface GigabitEthernet0/0/6
#
traffic behavior injection
redirect ip-nexthop 10.3.1.2
#
traffic policy injection
classifier injection behavior injection precedence 5
```

```
#
interface Vlanif10
 ip address 1.1.1.1 255.255.255.0
#
interface Vlanif20
 ip address 2.2.2.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 undo portswitch
#
interface GigabitEthernet0/0/1.2
 dot1q termination vid 2
 ip address 4.4.4.2 255.255.255.252
#
interface GigabitEthernet0/0/4
 undo portswitch
 ip address 10.3.1.1 255.255.255.252
#
interface GigabitEthernet0/0/6
 port link-type trunk
 port trunk allow-pass vlan 10 20
 traffic-policy injection inbound
#
bgp 100
 router-id 21.21.21.21
 peer 1.1.1.2 as-number 100
#
ipv4-family unicast
 undo synchronization
 peer 1.1.1.2 enable
#
ospf 1 router-id 33.33.33.1
 default-route-advertise always
 area 0.0.0.0
 network 10.3.1.0 0.0.0.3
#
ip route-static 0.0.0.0 0.0.0.0 4.4.4.1
#
return
```

9.4.3 Mirror-SW 配置

```
#
sysname Mirror-SW
#
vlan batch 2 43
#
observe-port 1 interface GigabitEthernet0/0/4
```



```
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 2
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 2
 port-mirroring to observe-port 1 inbound
#
interface GigabitEthernet0/0/5
 port link-type access
 port default vlan 43
#
interface GigabitEthernet0/0/6
 port link-type access
 port default vlan 43
#
interface GigabitEthernet0/0/7
 port link-type access
 port default vlan 43
#
interface GigabitEthernet0/0/8
 port link-type access
 port default vlan 43
#
interface GigabitEthernet0/0/9
 port link-type access
 port default vlan 43
#
return
```

9.4.4 Detecting 配置

```
#
sysname Detecting
#
firewall defend action discard
#
firewall ddos detect-spu slot 0 cpu 0
#
undo firewall session link-state check
#
undo firewall ipv6 session link-state check
#
firewall fragment-forward enable
#
firewall ipv6 fragment-forward enable
```

```
#
firewall ddos log-local-ip 192.168.2.13
firewall ddos log-server-ip 192.168.2.200
anti-ddos packet-capture
key %+%###!!!!!!"!!!!"!!!!!!od9{R[&0UBVNzBX;$'m&:k%q;Tjdx:qRKSC!!!!2jp5!!!!q!!!!]q9-.Wj0|YrIFREy+2
u5jk&j+ZGz)X#:QqHc0`\+n0weB^czo3@!N`F@3unX3gXXPFPeO>]wZ"d*dbSm](7=EHYdM1y#f62BP\,%+
%#
#
undo firewall packet-filter basic-protocol enable
#
arp learning on-different-segment disable
#
telnet server disable
telnet ipv6 server disable
undo telnet server-source all-interface
undo telnet ipv6 server-source all-interface
#
diffserv domain default
#
ip vpn-instance _management_vpn_
  ipv4-family
#
vlan 1
#
aaa
  authentication-scheme default
    authentication-mode local
  authorization-scheme default
    authorization-mode local
  accounting-scheme default
    accounting-mode none
  local-aaa-user password policy administrator
    password history record number 0
    undo password alert original
    password expire 0
  domain default
    authentication-scheme default
    accounting-scheme default
  undo local-aaa-user wrong-password
  local-aaa-user user-name complexity-check disable
  local-user admin password irreversible-cipher $1d$oee6NSc}_UE8-
~T]$]T2ULmz[I"C,vkAg5^+39en&YbT8zBZO>L2ie&s0$
  local-user admin password-force-change disable
  local-user admin privilege level 3
  local-user admin service-type telnet terminal ssh http
  local-user admin1 password irreversible-cipher
$1d$sr*RD"$ubT,%^D"H$24IP/,2qb(_Z"6BKYXvM8@HP~3a.[~u{+>P%J9FI$
  local-user admin1 password-force-change disable
```

```
local-user admin1 privilege level 3
local-user admin1 service-type telnet terminal ssh http
local-user aticuser password irreversible-cipher $1d$w[fpT`vl]#|Q-
f=n$]=xUM^hs|E7$@6Tq{;3DzEAbM>z(K8_)]|Q"/.6O$
local-user aticuser privilege level 3
local-user aticuser service-type ssh
#
interface MEth0/0/0
ip binding vpn-instance _management_vpn_
ip address 192.168.2.10 255.255.255.0
#
interface GE0/0/0
portswitch
port default vlan 1
anti-ddos flow-statistic enable
anti-ddos detect enable
#
interface GE0/0/3
ip address 192.168.2.13 255.255.255.0
undo service-manage enable
#
snmp-agent
snmp-agent local-engineid 800007DB03F4E451DE31AD
#
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 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 %+%##!!!!!!!"!!!!!"!!!!*!!!!od9{R[&0UBmbh=e{K,*SKE/T{im~$BVJb"!!!!2jp5!!!!!=!!!!r\y%*w>yB<qC^6
/BvfdVL4K2JA$dEUD5.f!!!!%+%#
snmp-agent usm-user v3 atic privacy-mode aes256
cipher %+%##!!!!!!!"!!!!!"!!!!*!!!!od9{R[&0UBSISQ%F(+w=R-
n"=Mng/ND$c6~!!!!2jp5!!!!!=!!!!NV6X%FZ/g/Q/9G-bl/3~aC%A.]W)y*j#5.$!!!!%+%#
#
snmp-agent trap source GE0/0/3
#
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
#
```

```
lldp 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 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
#
user-interface vty 0 4
 authentication-mode aaa
 user privilege level 3
 protocol inbound ssh
#
netconf
 protocol inbound ssh ipv4 port 830
#
nacm
 nacm enable
 execute-default permit
 group-name nacm-group
 user-name aticuser
#
ddos-zone name zone_11
 zone-id 11
 ip address 100.100.100.100 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
#
firewall zone trust
set priority 85
add interface GE0/0/3
```

```
#
firewall zone untrust
  set priority 5
  add interface GE0/0/0
#
firewall zone dmz
  set priority 50
#
security-policy
  default action permit
#
return
```

9.4.5 Cleaning 配置

```
#
sysname Cleaning
#
firewall defend action discard
#
undo firewall session link-state check
#
undo firewall ipv6 session link-state check
#
firewall fragment-forward enable
#
firewall ipv6 fragment-forward enable
#
firewall ddos log-local-ip 192.168.2.14
firewall ddos log-server-ip 192.168.2.200
firewall ddos bgp-next-hop fib-filter
firewall ddos bgp-next-hop 2.2.2.1
anti-ddos packet-capture
key %+%##!!!!!!"!!!!"!!!!*!!!!c9TGTa3D0G09F4!jA!9:@ZDKW4z23>v}f7:!!!!2jp5!!!!!!q!!!!=-
75/6&w3!T_1e!}*WE&DHpu)*{-
$B+EkOjhR;$LYr0VXUONQp0:j*AEILMxy;q%xj'N(LD.hK3E=~E$=H&BS](`WMF{:*7rUGF%+%#
#
undo firewall packet-filter basic-protocol enable
#
vlan batch 10 20
#
ip vpn-instance _management_vpn_
  ipv4-family
#
aaa
  authentication-scheme default
    authentication-mode local
  authorization-scheme default
```

```
authorization-mode local
accounting-scheme default
accounting-mode none
local-aaa-user password policy administrator
password history record number 0
undo password alert original
password expire 0
domain default
authentication-scheme default
accounting-scheme default
undo local-aaa-user wrong-password
local-aaa-user user-name complexity-check disable
local-user admin password irreversible-cipher $1d$B>Wt;=M~N~*Cl<O$U%_<&-"">6Pp8-
D7TtYHr6bh=q]-0D)js\'\'6z4F$
local-user admin password-force-change disable
local-user admin privilege level 3
local-user admin service-type telnet terminal ssh http
local-user admin1 password irreversible-cipher $1d$S2QW29^V59S#LX+m$7dfLRB],s-
16eO.*2{%WLaNgO)3K}Pc/RS>o12PN$
local-user admin1 password-force-change disable
local-user admin1 privilege level 3
local-user admin1 service-type telnet terminal ssh http
local-user aticuser password irreversible-cipher
$1d$J+3o=U/yZ"ubm;Mh$Xi+nA.O2%DuoUC~wv5V34ztq""jfp+qi3)~;*t1!$
local-user aticuser privilege level 3
local-user aticuser service-type ssh
#
interface Vlanif10
ip address 1.1.1.2 255.255.255.0
undo service-manage enable
#
interface Vlanif20
ip address 2.2.2.2 255.255.255.0
undo service-manage enable
#
interface GE0/0/0
portswitch
port link-type trunk
port trunk allow-pass vlan 10 20
anti-ddos flow-statistic enable
anti-ddos clean enable
#
interface GE0/0/3
ip address 192.168.2.14 255.255.255.0
undo service-manage enable
#
bgp 100
router-id 32.32.32.32
```

```
private-4-byte-as enable
peer 1.1.1.1 as-number 100
#
ipv4-family unicast
import-route ospf-1
peer 1.1.1.1 enable
peer 1.1.1.1 route-policy 1 export
peer 1.1.1.1 advertise-community
#
route-policy 1 permit node 10
apply community no-advertise
#
snmp-agent
snmp-agent local-engineid 800007DB03F4E451DE3054
#
snmp-agent sys-info version v3
snmp-agent group v3 secmananager privacy read-view mib2view write-view mib2view notify-view
mib2view
#
snmp-agent mib-view included mib2view iso
snmp-agent usm-user v3 atic
snmp-agent usm-user v3 atic group secmananager
snmp-agent usm-user v3 atic authentication-mode sha2-256
cipher %+%##!!!!!!!"!!!!!"!!!!!"!!!!!"c9TGTa3D0GvHQFTcl(q4DN<:<]"`TO3+gN+!!!!2jp5!!!!!!=!!!!UK4@>;}X=O;{:
1E,t7rPvuZz.=T;UL#w17~!!!!!"%+%#
snmp-agent usm-user v3 atic privacy-mode aes256
cipher %+%##!!!!!!!"!!!!!"!!!!!"!!!!!"c9TGTa3D0Go,J*jhbO4Az0s%>w"t2kz`^0!!!!2jp5!!!!!!=!!!!g4p21H6g44cL_w
Q!tUY&DWxPWDiCS#xg+/&!!!!!"%+%#
#
snmp-agent trap source GE0/0/3
#
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
#
lldp 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 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
#
user-interface vty 0 4
 authentication-mode aaa
 user privilege level 3
 protocol inbound ssh
#
netconf
 protocol inbound ssh ipv4 port 830
#
nacm
 nacm enable
 execute-default permit
 group-name nacm-group
 user-name aticuser
#
ddos-zone name zone_11
 zone-id 11
 ip address 100.100.100.100 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
#
firewall zone trust
set priority 85
add interface GE0/0/3
add interface Vlanif20
#
firewall zone untrust
set priority 5
add interface Vlanif10
#
firewall zone dmz
set priority 50
add interface GE0/0/0
```

```
#
security-policy
  default action permit
#
policy-based-route
  rule name traffic_injection
    ingress-interface Vlanif10
    action pbr egress-interface Vlanif20 next-hop 2.2.2.1
#
return
```

9.4.6 SW1 预配置

```
#
sysname SW1
#
vlan batch 2 30
#
interface vlanif2
  ip address 4.4.4.1 255.255.255.252
#
interface vlanif30
  ip address 20.20.20.1 255.255.255.0
#
interface GigabitEthernet0/0/3
  port link-type trunk
  port trunk allow-pass vlan 2
#
interface GigabitEthernet0/0/13
  port link-type access
  port default vlan 30
#
ip route-static 100.100.100.0 255.255.255.0 4.4.4.2
#
return
```

9.4.7 SW2 预配置

```
#
sysname SW2
#
interface GigabitEthernet0/0/1
  port link-type access
  port default vlan 30
#
interface GigabitEthernet0/0/15
  port link-type access
  port default vlan 30
```

#

9.5 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？

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，将访问防护对象的流量引导至清洗设备。

10

内容安全过滤实验

10.1 实验介绍

10.1.1 关于本实验

企业为规范员工上网行为，通过在出口防火墙部署 URL 过滤、文件过滤和内容过滤功能，实现如下需求：

- 1.通过 URL 过滤功能禁止企业员工访问游戏门户网站。
- 2.阻断来自互联网的可执行文件的下载，以降低信息泄露和内网感染病毒的风险。
- 3.通过内容过滤功能对包含机密信息的文件或应用进行过滤，降低公司机密泄露的风险。

10.1.2 实验目的

- 掌握防火墙 URL 过滤、文件过滤和内容过滤功能的配置方式。
-

10.1.3 实验组网介绍

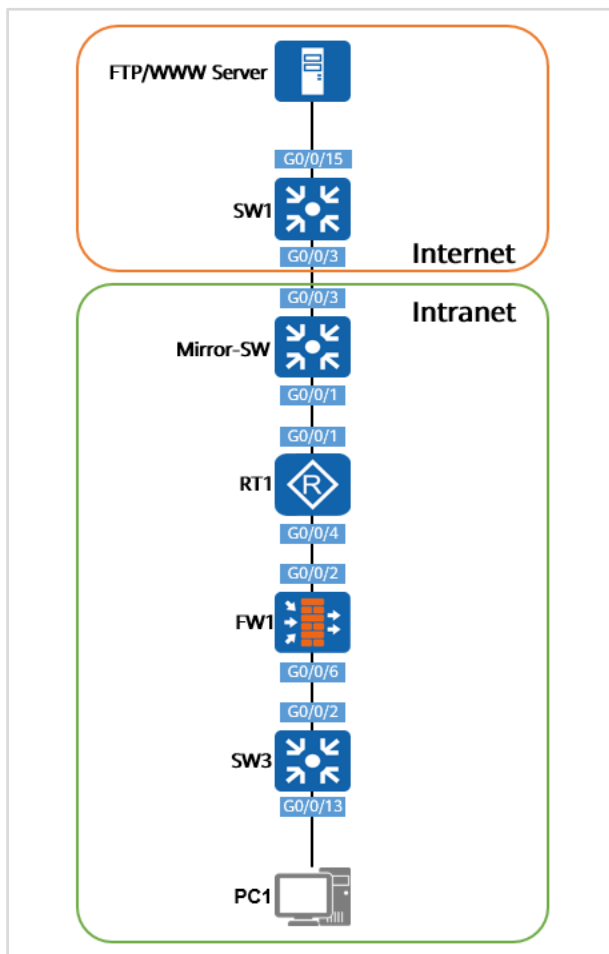


图10-1 内容安全综合实验拓扑图

SW1 模拟 Internet，FW1 作为企业安全网关，针对内网用户执行内容安全过滤来保证企业信息安全。

SW1、SW3、Mirror-SW 和 RT1 设备已预配，具体配置在本实验步骤中不体现，详细配置可参考“10.4 配置参考”中相关设备的预配置，本实验重点介绍 FW1 设备上关键配置。

10.1.4 实验规划

表10-1 设备接口规划表

设备	接口	接口性质	接口信息	说明
FW1	G0/0/2	三层接口	10.3.1.2/30 安全区域: untrust	与RT1互连
	G0/0/6	三层接口	172.16.20.2/24 安全区域: trust	与SW3互连, PC1的网关

RT1	G0/0/1.2	三层接口	4.4.4.2/30	与Mirror-SW互连
	G0/0/4	三层接口	10.3.1.1/30	与FW1互连
SW1	G0/0/15	Access	PVID: 300	连接FTP/WWW Server
	VLANIF300	三层接口	172.17.100.1/24	FTP/WWW Server网关
	G0/0/3	Trunk	PVID: 1 Allow-pass VLAN: 2	与Mirror-SW互连
	VLANIF2	三层接口	4.4.4.1/30	与RT1接口组成直连网段
Mirror-SW	G0/0/1	Trunk	PVID: 1 Allow-pass VLAN: 2	互连接口
	G0/0/3			
SW3	G0/0/2	Access	PVID: 40	与FW1互连
	G0/0/13	Access	PVID: 40	连接PC1
FTP/WWW Server	Ethernet 0	网卡	172.17.100.10/24 网关: 172.17.100.1/24	终端
PC1	Ethernet 0	网卡	172.16.20.10/24 网关: 172.16.20.2/24	终端

10.2 实验任务配置

10.2.1 配置思路

- 1.配置接口 IP 地址和安全区域，完成网络基本参数配置。
- 2.配置 URL 过滤安全配置文件，设置缺省动作，设置自定义 URL 分类动作。
- 3.配置安全策略，调用 URL 过滤安全配置文件。
- 4.配置文件过滤安全配置文件，设置文件类型、策略方向和策略动作。
- 5.配置内容过滤关键字组，设置匹配类型、关键字和权重。
- 6.配置内容过滤安全配置文件，设置关键字组、方向和动作。
- 7.配置安全策略，调用文件过滤安全配置文件和内容过滤安全配置文件。

10.2.2 配置步骤 - CLI

步骤 1 网络基本参数配置

按照“表 10-1”数据规划，完成网络基本参数配置。其中 SW1、SW3、Mirror-SW 和 RT1 已经预配，具体可参考“10.4 配置参考”。

完成 FW1 设备业务接口地址、安全区域和路由配置。

```
[FW1]interface GE0/0/2
[FW1-GE0/0/2] ip address 10.3.1.2 255.255.255.252
[FW1-GE0/0/2]quit
[FW1]interface GE0/0/6
[FW1-GE0/0/6] ip address 172.16.20.2 255.255.255.0
[FW1-GE0/0/6]quit
[FW1]firewall zone trust
[FW1-zone-trust] add interface GE0/0/6
[FW1-zone-trust]quit
[FW1]firewall zone untrust
[FW1-zone-untrust] add interface GE0/0/2
[FW1-zone-untrust]quit
[FW1] ospf 1 router-id 11.11.11.1
[FW1-ospf-1] area 0.0.0.0
[FW1-ospf-1-area-0.0.0.0] network 10.3.1.0 0.0.0.3
[FW1-ospf-1-area-0.0.0.0] network 172.16.20.0 0.0.0.255
[FW1-ospf-1-area-0.0.0.0] quit
[FW1-ospf-1] quit
[FW1] undo firewall packet-filter basic-protocol enable
[FW1] firewall detect ftp
```

步骤 2 创建 URL 过滤配置文件

```
[FW1]profile type url-filter name game
[FW1-profile-url-filter-game]default action allow
[FW1-profile-url-filter-game]category pre-defined control-level high
[FW1-profile-url-filter-game]add blacklist url 172.17.100.10/game
[FW1-profile-url-filter-game]quit
[FW1]
```

步骤 3 调用 URL 过滤配置文件

```
[FW1]security-policy
[FW1-policy-security]rule name game_filter
[FW1-policy-security-rule-game_filter] source-zone trust
[FW1-policy-security-rule-game_filter] destination-zone untrust
[FW1-policy-security-rule-game_filter] source-address 172.16.20.0 24
[FW1-policy-security-rule-game_filter] profile url-filter game
Warning: When the device performs content security detection or application identification on traffic,
the performance of the device is affected. Therefore, configure the function as required.
[FW1-policy-security-rule-game_filter] action permit
[FW1-policy-security-rule-game_filter]quit
[FW1-policy-security]quit
[FW1]
```


步骤 4 配置 NAT 策略

配置源 NAT 策略，将内网客户端源地址转换成防火墙 FW1 出接口地址访问 Internet。

```
[FW1] nat-policy
[FW1-policy-nat] rule name trust-untrust
[FW1-policy-nat-rule-trust-untrust] source-zone trust
[FW1-policy-nat-rule-trust-untrust] destination-zone untrust
[FW1-policy-nat-rule-trust-untrust] action source-nat easy-ip
[FW1-policy-nat-rule-trust-untrust] quit
[FW1-policy-nat] quit
[FW1]
```

步骤 5 创建文件过滤配置文件

```
[FW1]profile type file-block name exe
[FW1-profile-file-block-exe]rule name exe
[FW1-profile-file-block-exe-rule-exe]file-type pre-defined name EXE MSI RPM OCX A ELF DLL PE SYS
[FW1-profile-file-block-exe-rule-exe]application all
[FW1-profile-file-block-exe-rule-exe]direction download
[FW1-profile-file-block-exe-rule-exe]action block
[FW1-profile-file-block-exe-rule-exe]quit
[FW1-profile-file-block-exe]quit
[FW1]
```

步骤 6 创建内容过滤关键字组

```
[FW1] keyword-group name secret
[FW1-keyword-group-secret] user-defined-keyword name secret
[FW1-keyword-group-secret-keyword-secret] expression match-mode text secret
[FW1-keyword-group-secret-keyword-secret] weight 1
[FW1-keyword-group-secret-keyword-secret] quit
[FW1-keyword-group-secret] quit
[FW1]
```

步骤 7 创建内容过滤配置文件

```
[FW1] profile type data-filter name secret
[FW1-profile-data-filter-secret] rule name secret
[FW1-profile-data-filter-secret-rule-secret] keyword-group name secret
[FW1-profile-data-filter-secret-rule-secret] file-type all
[FW1-profile-data-filter-secret-rule-secret] application all
[FW1-profile-data-filter-secret-rule-secret] action block
[FW1-profile-data-filter-secret-rule-secret] quit
[FW1-profile-data-filter-secret] quit
[FW1]
```

步骤 8 调用文件过滤/内容过滤

在原有安全策略中调用刚才创建的文件过滤配置文件和内容过滤配置文件。

```
[FW1]security-policy
[FW1-policy-security]rule name game_filter
[FW1-policy-security-rule-game_filter]profile data-filter secret
[FW1-policy-security-rule-game_filter]profile file-block exe
[FW1-policy-security-rule-game_filter]quit
[FW1-policy-security]quit
[FW1]
```

步骤 9 提交配置

```
[FW1]engine configuration commit
Info: The operation may last several minutes, please wait. Try "display engine information" for detail.
```

10.2.3 配置步骤 - Web

步骤 1 网络基本参数配置

按照“表 10-1”数据规划，完成网络基本参数配置。其中 SW1、SW3、Mirror-SW 和 RT1 已经预配，具体可参考“10.4 配置参考”。

登录 FW1 设备 Web 管理界面，选择“网络 > 接口”，参考“5.2.3 配置步骤 - Web”相关配置步骤，基于“表 10-1”数据规划完成 FW1 设备业务接口的基础配置，配置完成后效果如下：



接口名称	描述	安全区域	虚拟系统/VPN实例	IP地址	连接类型	VLAN
MEth0/0/0		-- NONE --	_management_vpn_	192.168.20.7	静态IP (IPv4)	---
Virtual-if0		-- NONE --	public	---	静态IP (IPv6)	---
GE0/0/0		-- NONE --	public	---	静态IP (IPv4)	---
GE0/0/1		-- NONE --	public	---	静态IP (IPv6)	---
GE0/0/2		untrust	public	10.3.1.2	静态IP (IPv4)	---
GE0/0/5		-- NONE --	public	---	静态IP (IPv6)	---
GE0/0/6		trust	public	172.16.20.2	静态IP (IPv4)	---
GE0/0/7		-- NONE --	public	---	静态IP (IPv6)	---

图10-2 FW1 设备业务接口基础配置信息

在 FW1 设备 Web 管理界面选择“网络 > 路由 > OSPF > 新建”，进入 OSPF 配置界面，参考“1.2.3 配置步骤 - Web”相关配置步骤完成 FW1 设备的 OSPF 配置，配置完成后效果如下：



图10-3 FW1 设备 OSPF 配置信息

步骤 2 创建 URL 过滤配置文件

在 FW1 设备 Web 管理界面选择“对象 > 安全配置文件 > URL 过滤 > 新建”，执行以下操作，创建 URL 过滤配置文件。



图10-4 进入 URL 配置文件创建界面



* 名称

加密流量过滤 ☐ 启用该功能后，可以通过不解密的方式对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	172.17.100.10/game
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

分类过滤

缺省动作 ☒ 允许 ☐ 告警 ☐ 阻断

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。

☐ 低 对色情网站进行控制。

☐ 自定义

名称	☐ 允许	☐ 告警	☐ 阻断
> IT相关	☐	☐	☐
> P2P	☐	☐	☒
> 博彩	☐	☐	☒

激活 Windows
转到“设置”以激活 Windows。

取消 确定

图10-5 创建 URL 过滤配置文件

步骤 3 调用 URL 过滤

在 FW1 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”，进入安全策略创建界面，执行以下操作，创建业务安全策略，用于后续调用各类内容安全配置文件。

^ 概述

* 名称
game_filter

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

地址/地区 ⓘ
172.16.20.0/...

标签
请选择

目的

目的类型
☒ 安全区域 ☐ 虚拟服务

安全区域
untrust

地址/地区 ⓘ
any

标签
请选择

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 ∨ 反病毒/入侵防御/URL过滤/内容过滤/文件过滤/邮件过滤/DNS过滤

转到“设置”以激活 Windows。

取消 命令预览 确定

图10-6 创建业务安全策略



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 1 game ▾

内容过滤 ▾

文件过滤 ▾

邮件过滤 ▾

DNS过滤 ▾

▽ 其他

激活 Windows
转到“设置”以激活 Windows。

取消 命令预览 2 确定

图10-7 调用 URL 过滤配置文件

步骤 4 配置 NAT 策略

配置源 NAT 策略，将内网客户端源地址转换成防火墙 FW1 出接口地址访问 Internet。

在 FW1 设备 Web 管理界面选择“策略 > NAT 策略 > NAT 策略 > 新建”，执行以下操作，在 FW1 设备上创建源 NAT 策略。



USG6525F

面板 监控 **策略** 对象 网络 系统

3 NAT策略 源转换地址池 目的转换地址池

4 新建 删除 复制 移动 插入 清除全部命中次数 启用 禁用 批量生成安全策略

请输入要查询的内容 添加查询项

名称	描述	NAT类型	转换模式	时间段	源安全区域
default	This is the default...		不做转换		any

图10-8 进入 NAT 策略配置界面

[功能介绍]

名称
trust-untrust

描述

NAT类型
☒ NAT
☐ NAT64
☐ NAT66

转换模式
仅转换源地址

时间段
-- NONE --

原始数据包

源安全区域
trust

目的类型
☒ 目的安全区域
☐ 出接口

源地址
any

目的地址
any

服务
any

转换后的数据包

源地址转换为
☐ 地址池中的地址
☒ 出接口地址

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。

取消
确定

图10-9 创建源 NAT 策略

步骤 5 创建文件过滤配置文件

在 FW1 设备 Web 管理界面选择“对象 > 安全配置文件 > 文件过滤 > 新建”，执行以下操作，创建文件过滤配置文件。



图10-10 进入文件过滤配置文件创建界面



图10-11 创建文件过滤配置文件（1）

* 规则名称

exe

* 应用

全部

文件类型

全部 ×

自定义扩展名

每行可配置一个自定义扩展名，行之间用回车分隔

方向

☐ 上传

☒ 下载

☐ 全部

动作

☐ 告警

☒ 阻断

说明：POP3、SMTP、IMAP和NFS不支持阻断动作，将对其执行告警动作。

激活 Windows

转到“设置”以激活 Windows。

取消

确定

图10-12 创建文件过滤配置文件（2）



图10-13 创建文件过滤配置文件（3）

步骤 6 创建关键字组

在 FW1 设备 Web 管理界面选择“对象 > 关键字组 > 新建”，执行以下操作，创建关键字组，用于后续创建内容过滤配置文件。



图10-14 进入关键字组创建界面

关键字组名称 secret 1

关键字信息 ①

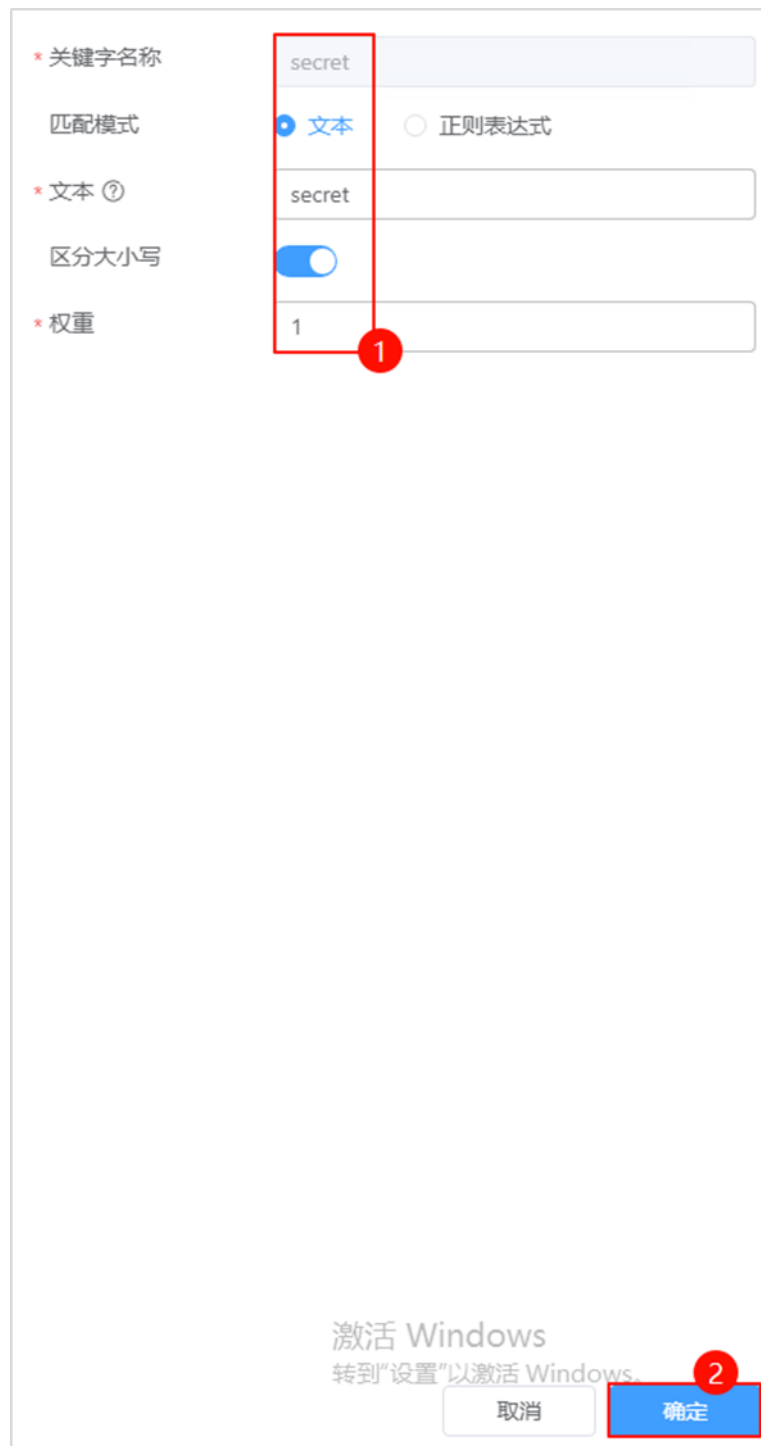
☐ 关键字名称 匹配模式 文本/正则表达式 区分大小写

☐ 2 3 新建自定义关键字

删除 新建

- 添加银行卡号关键字
- 添加信用卡号关键字
- 添加社会安全号关键字
- 添加身份证号关键字
- 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10-15 新建关键字组（1）



* 关键字名称

secret

匹配模式

☒ 文本 ☐ 正则表达式

* 文本 ②

secret

区分大小写

☒

* 权重

1

激活 Windows
转到“设置”以激活 Windows。

取消 确定

图10-16 新建关键字组（2）

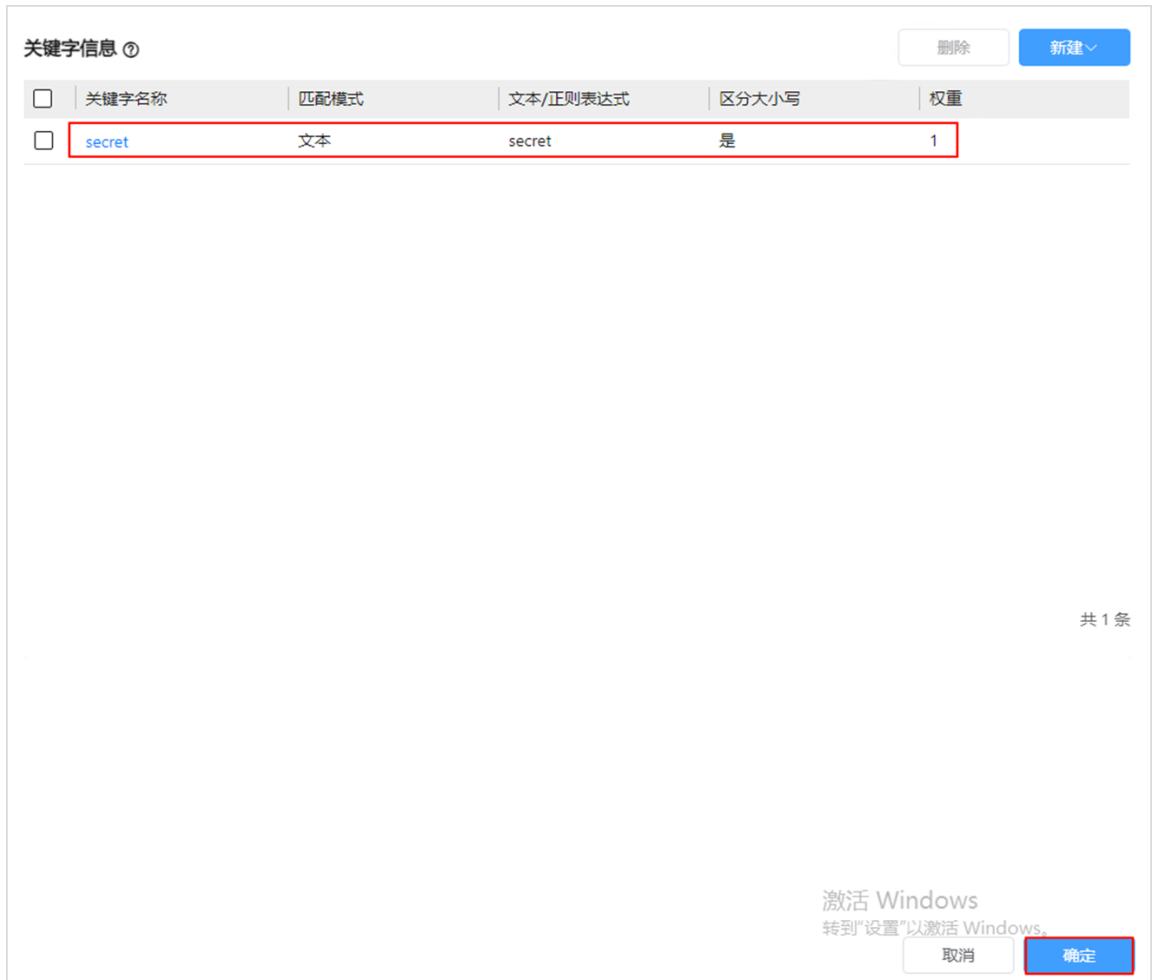


图10-17 新建关键字组（3）

步骤 7 创建内容过滤配置文件

在 FW1 设备 Web 管理界面选择“对象 > 安全配置文件 > 内容过滤 > 新建”，执行以下操作，创建内容过滤配置文件。

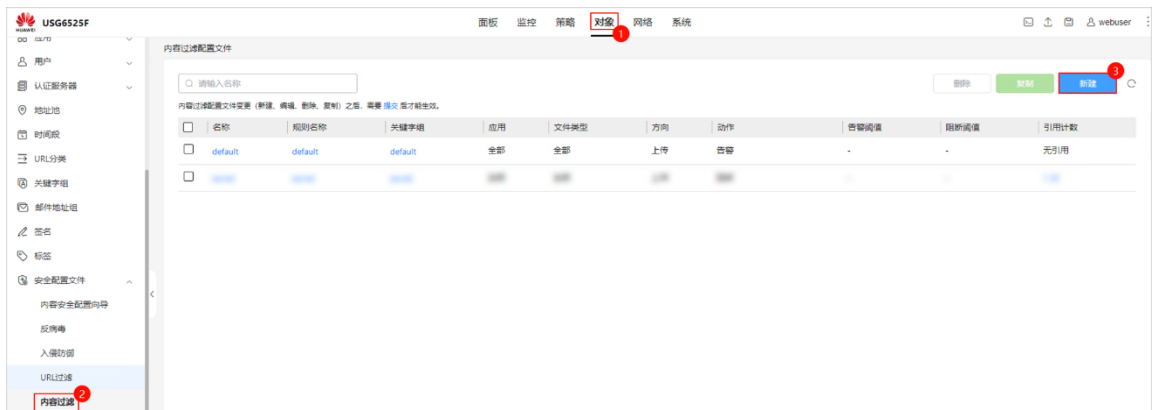


图10-19 新建内容过滤配置文件（1）



* 规则名称

* 关键字组

* 应用

* 文件类型

方向 ☒ 上传 ☐ 下载 ☐ 双向

动作 ☐ 告警 ☒ 阻断 ☐ 按权重累计阈值 ②

说明：NFS、POP3、SMTP、IMAP不支持阻断动作，将对其执行告警动作。

激活 Windows
转到“设置”以激活 Windows。

取消 确定

图10-20 新建内容过滤配置文件（2）

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
☐	secret	secret	全部	全部	上传	阻断	-	-

共 1 条

激活 Windows

转到“设置”以激活 Windows。

取消 确定

图10-21 新建内容过滤配置文件（3）

步骤 8 调用配置文件

在 FW1 设备 Web 管理界面选择“策略 > 安全策略 > 安全策略”，选择之前创建的业务安全策略“game_filter”进行二次编辑，调用之前创建的文件过滤和内容过滤配置文件。

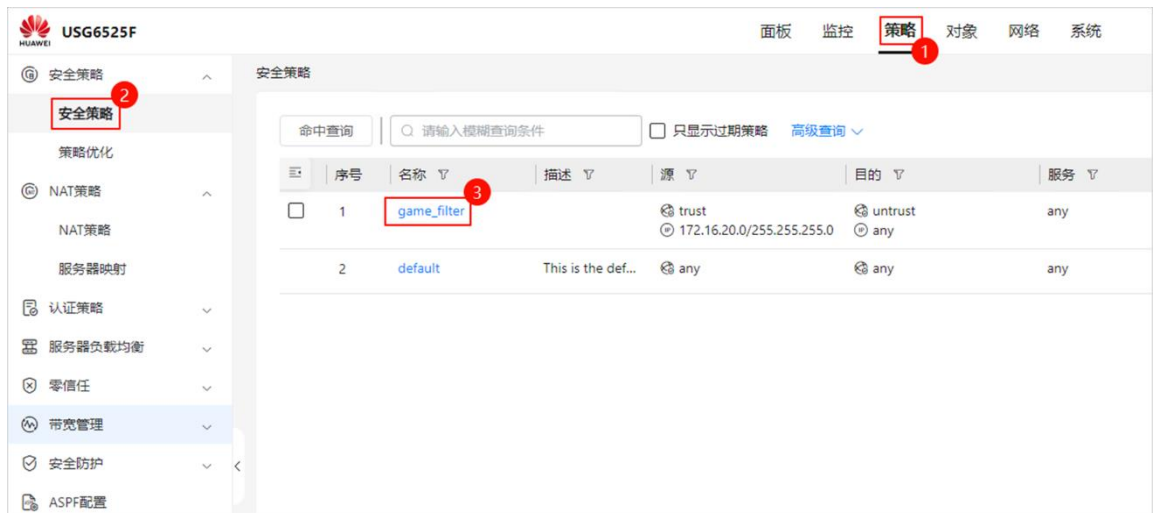


图10-22 进入“game_filter”安全策略修改界面

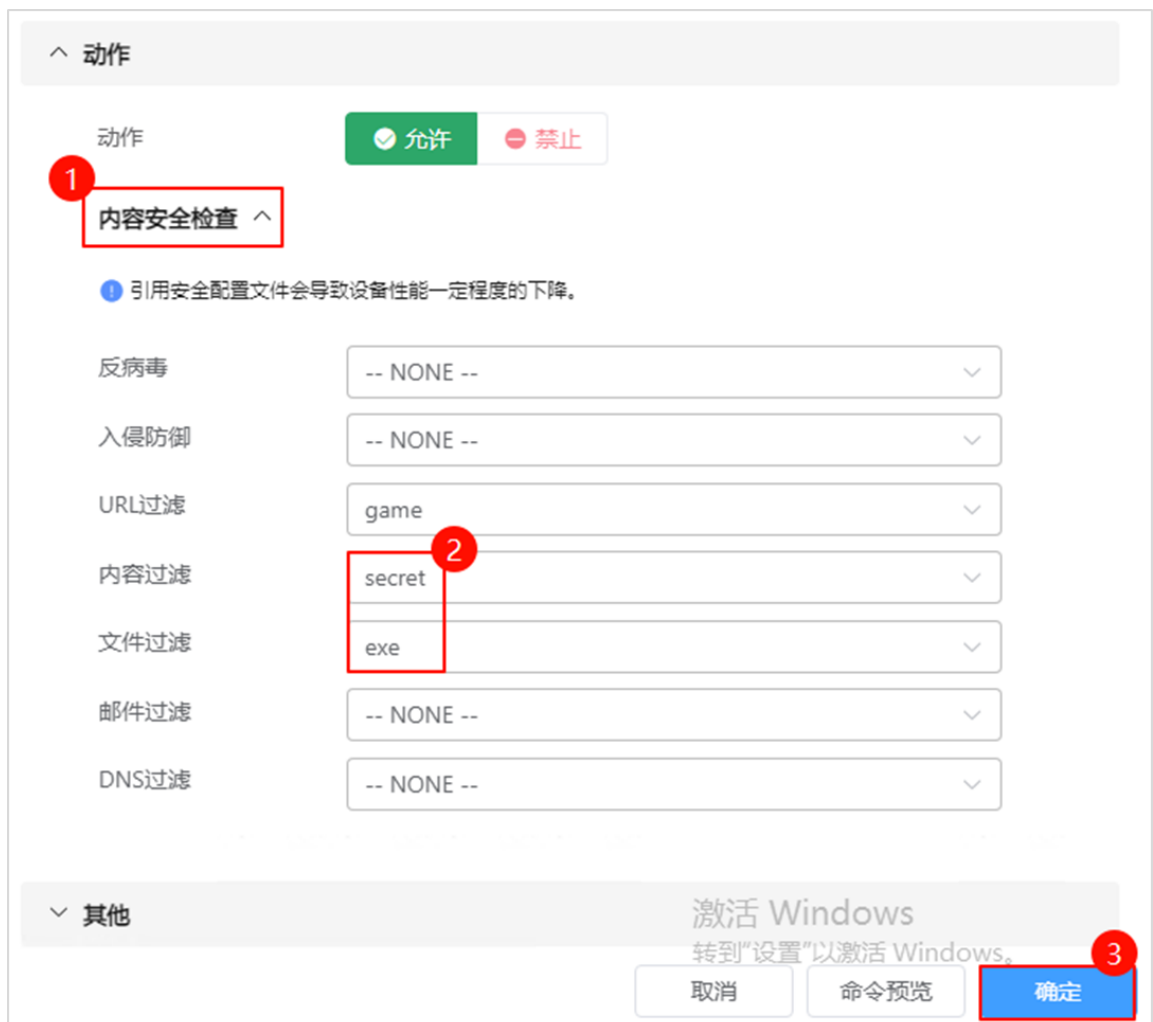


图10-23 调用内容安全配置文件

步骤 9 提交配置

在 FW1 设备 Web 管理界面右上角点击配置提交按钮，使内容安全相关配置生效。

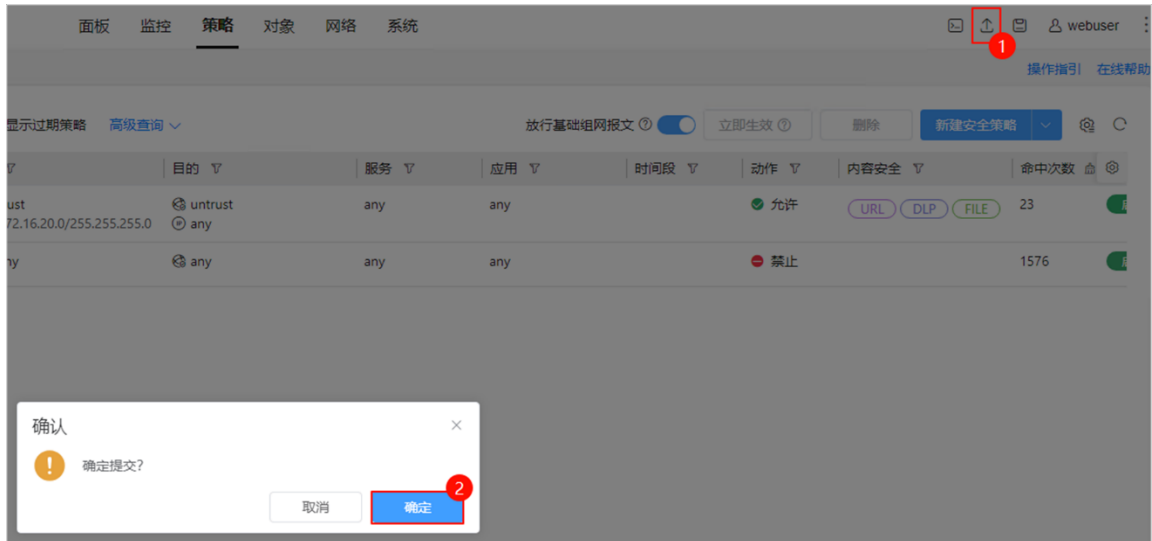


图10-24 提交配置

10.3 结果验证

使用 RDP 登录 PC1，打开浏览器输入“https://172.17.100.10/game”尝试访问游戏网页，效果如下：

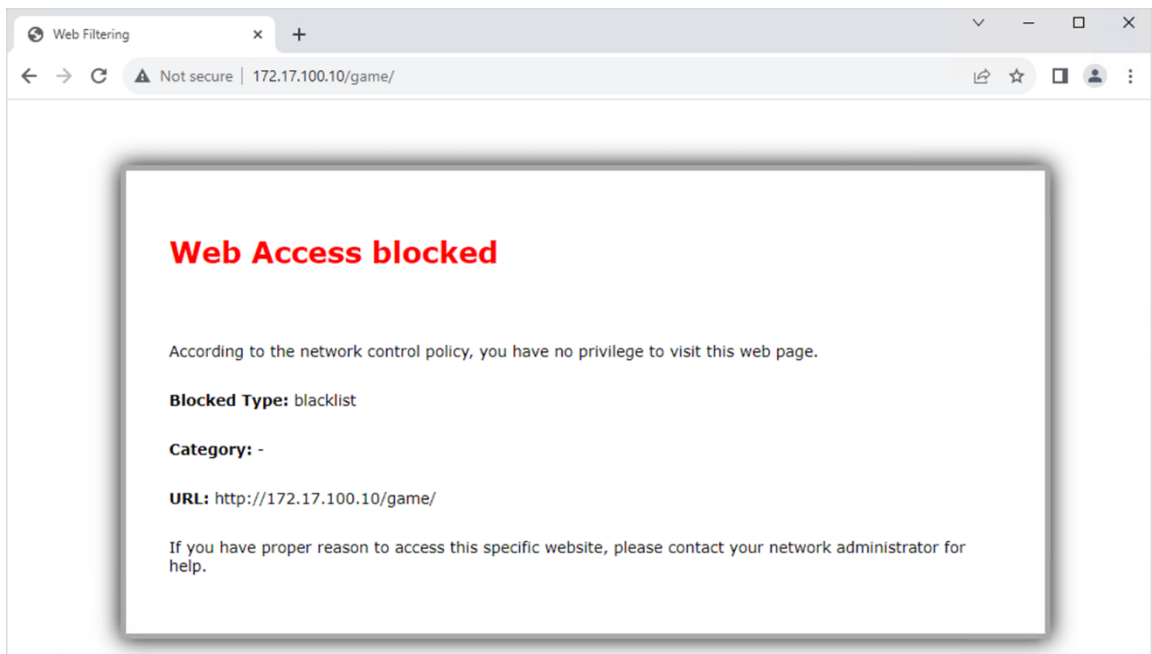


图10-25 PC1 访问游戏业务阻断效果

登录 FW1 设备 Web 管理界面，选择“监控 > 日志 > URL 日志”查看 URL 过滤日志。

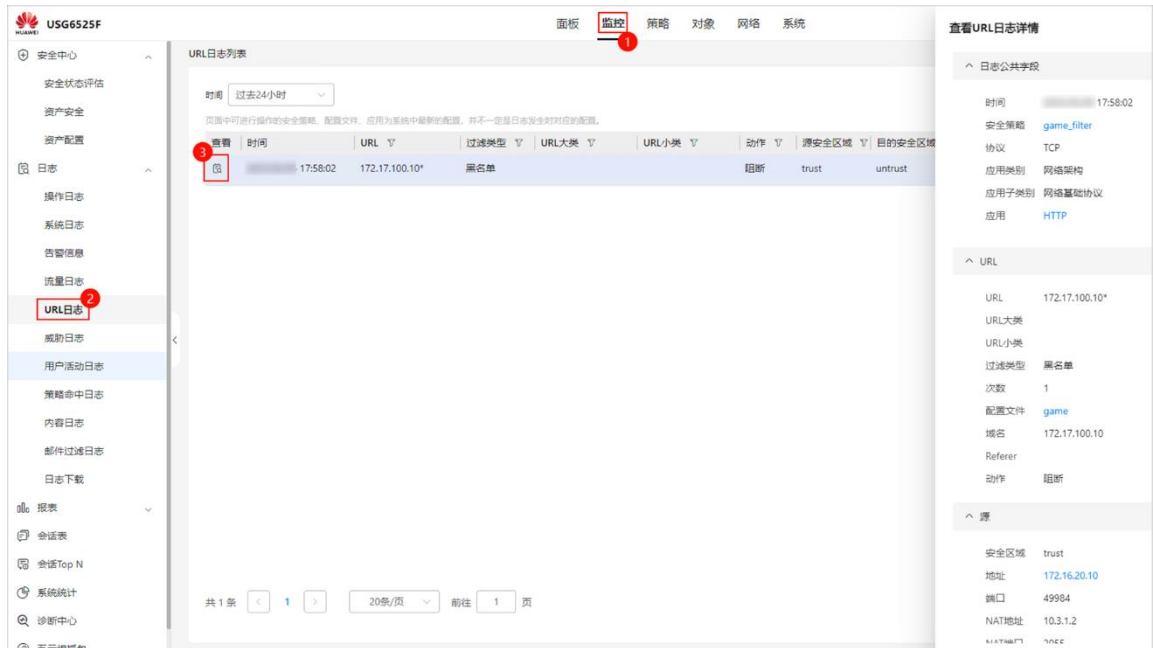


图10-26 查看 URL 过滤日志

打开 PC1 文件资源管理器，输入“ftp://172.17.100.10”尝试访问 FTP 业务，FTP 服务器设置了登录账号（用户名和密码均为“1”），连接到 FTP 服务器以后，尝试下载 FTP 服务器上的 exe 文件“PixPin_1.0.9.1.exe”。

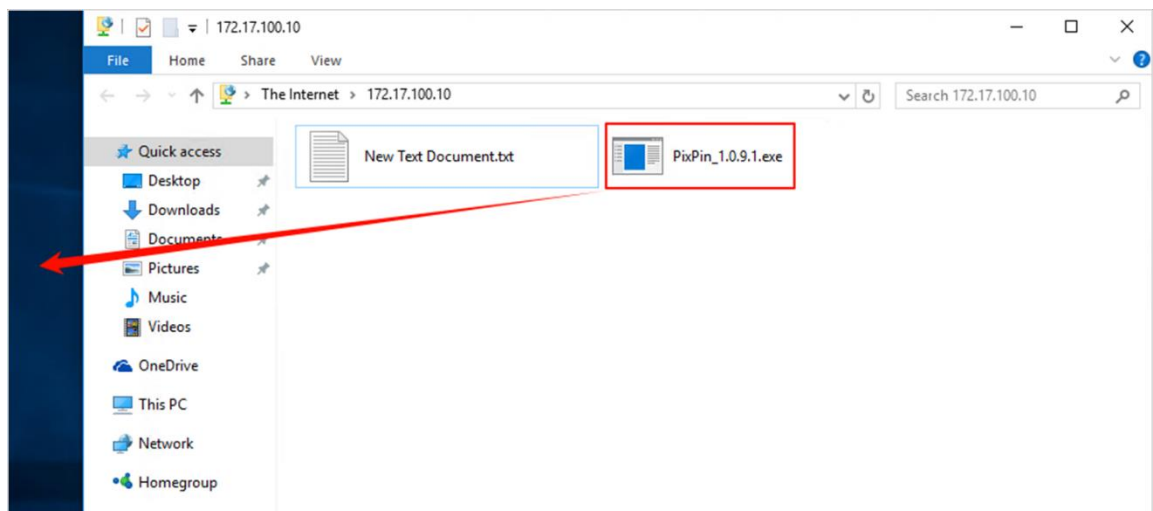


图10-27 尝试下载可执行文件

打开 FW1 设备 Web 管理界面，选择“监控 > 日志 > 内容日志”查看文件过滤日志。

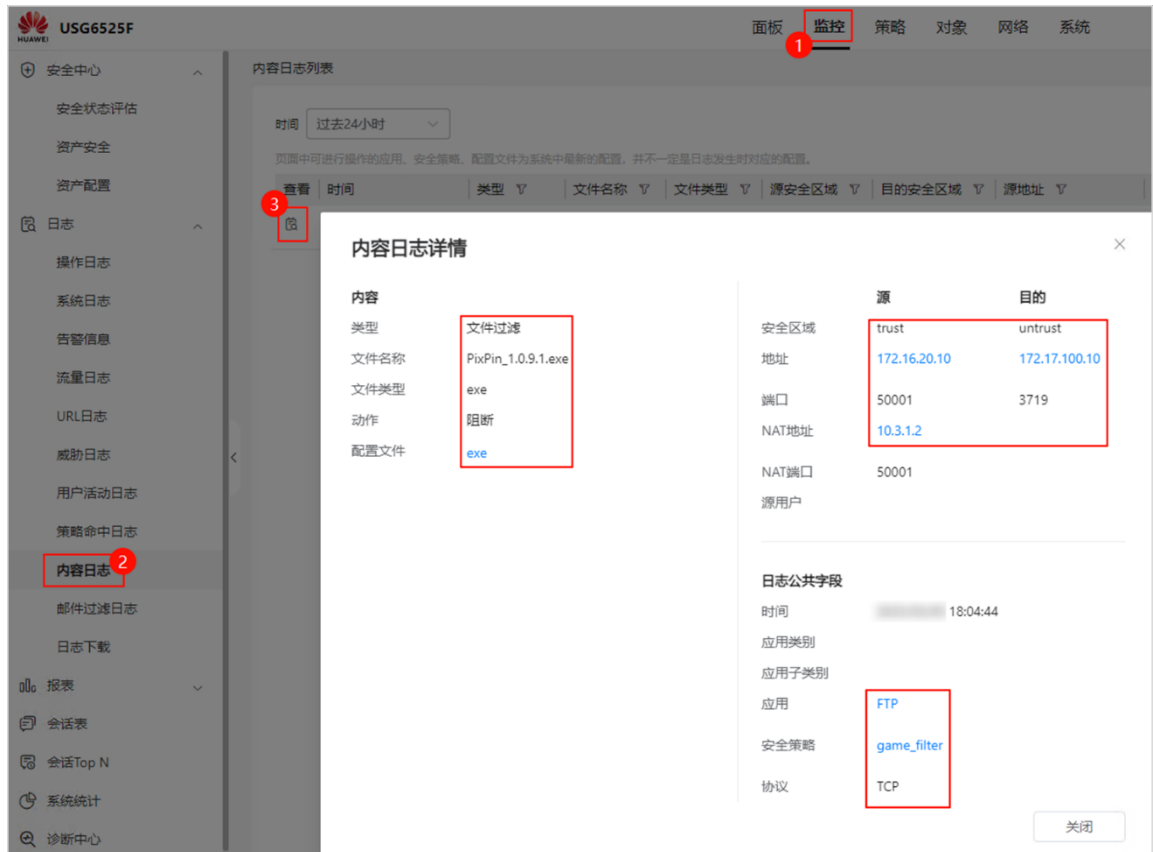


图10-28 查看文件过滤日志

在 PC1 桌面新建一个文本文档“secret.txt”，编辑内容需包含“secret”关键字，模拟企业机密文件，新建完成后，尝试上传至 FTP 服务器。

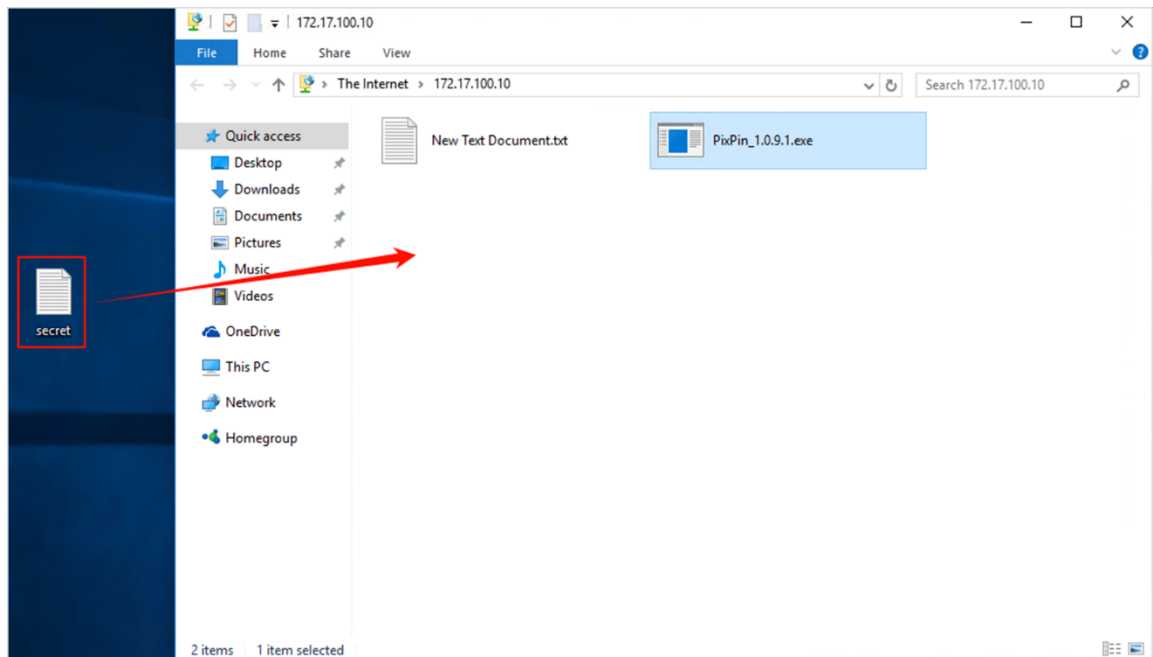


图10-29 尝试外发企业机密信息

打开 FW1 设备 Web 管理界面，选择“监控 > 日志 > 内容日志”查看内容过滤日志。

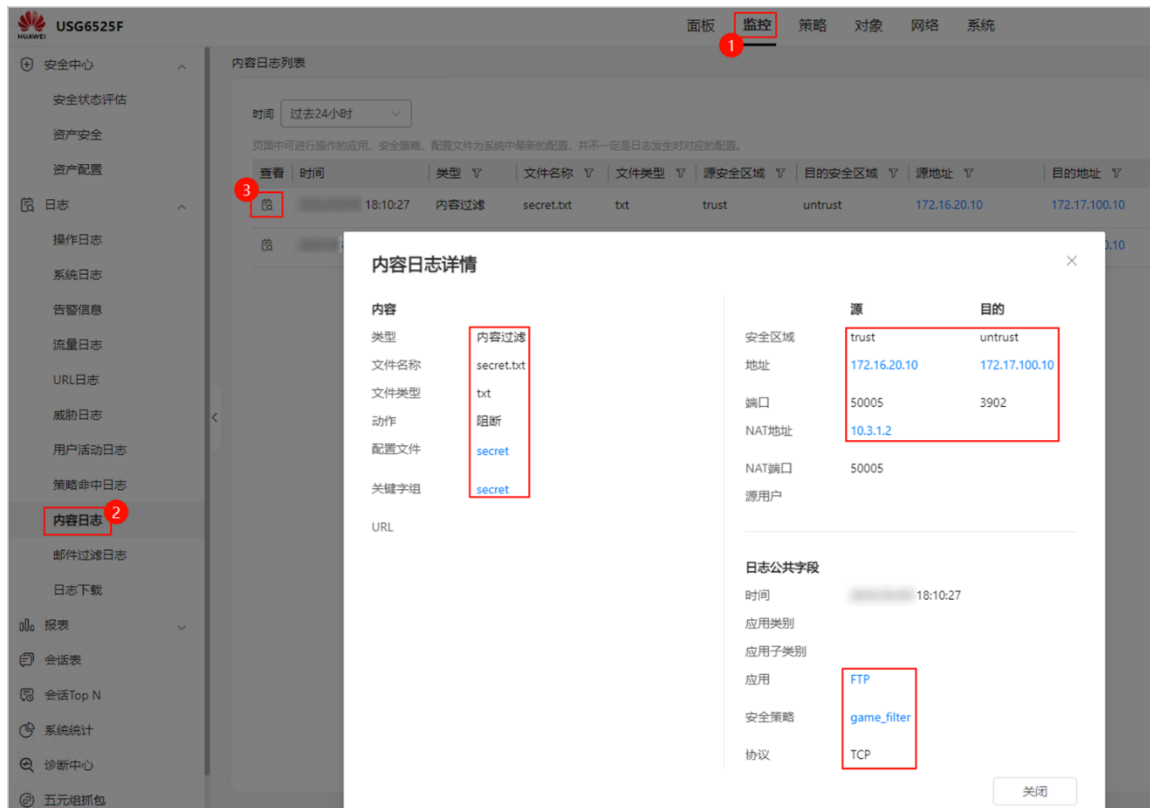


图10-30 查看内容过滤日志

10.4 配置参考

10.4.1 FW1 配置

```
#
sysname FW1
#
interface GE0/0/2
 ip address 10.3.1.2 255.255.255.252
 service-manage ping permit
#
interface GE0/0/6
 ip address 172.16.20.2 255.255.255.0
 service-manage ping permit
#
ospf 1 router-id 11.11.11.1
 opaque-capability enable
 area 0.0.0.0
```

```
network 10.3.1.0 0.0.0.3
network 172.16.20.0 0.0.0.255
#
firewall zone trust
add interface GE0/0/6
#
firewall zone untrust
add interface GE0/0/2
#
profile type url-filter name game
add blacklist url 172.17.100.10/game
category pre-defined control-level high
#
keyword-group name secret
user-defined-keyword name secret
expression match-mode text secret
#
profile type data-filter name secret
rule name secret
keyword-group name secret
action block
#
profile type file-block name exe
rule name exe
direction download
action block
#
firewall detect ftp
#
security-policy
rule name game_filter
source-zone trust
destination-zone untrust
source-address 172.16.20.0 mask 255.255.255.0
profile url-filter game
profile data-filter secret
profile file-block exe
action permit
#
nat-policy
rule name trust-untrust
source-zone trust
destination-zone untrust
action source-nat easy-ip
#
return
```

10.4.2 SW1 预配置

```
#
sysname SW1
#
vlan batch 2 300
#
interface Vlanif2
 ip address 4.4.4.1 255.255.255.252
#
interface Vlanif300
 ip address 172.17.100.1 255.255.255.0
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 2
#
interface GigabitEthernet0/0/15
 port link-type access
 port default vlan 300
#
ip route-static 10.3.1.0 255.255.255.252 4.4.4.2
#
```

10.4.3 Mirror-SW 预配置

```
#
sysname Mirror-SW
#
vlan batch 2
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 2
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 2
#
```

10.4.4 RT1 预配置

```
#
sysname RT1
#
interface GigabitEthernet0/0/1
 undo portswitch
#
```

```
interface GigabitEthernet0/0/1.2
  dot1q termination vid 2
  ip address 4.4.4.2 255.255.255.252
#
interface GigabitEthernet0/0/4
  undo portswitch
  ip address 10.3.1.1 255.255.255.252
#
ospf 1 router-id 33.33.33.1
  default-route-advertise always
  area 0.0.0.0
    network 10.3.1.0 0.0.0.3
#
ip route-static 0.0.0.0 0.0.0.0 4.4.4.1
#
```

10.4.5 SW3 预配置

```
#
sysname SW3
#
vlan batch 40
#
interface GigabitEthernet0/0/2
  port link-type access
  port default vlan 40
#
interface GigabitEthernet0/0/13
  port link-type access
  port default vlan 40
#
```

10.5 思考题

在双机热备组网环境下部署 URL 过滤功能时，对双机热备系统的工作模式是否有强制要求？

参考答案：要求双机热备必须工作在主备备份模式下，因为在报文来回路径不一致的组网环境中，设备无法接收到一条数据流的所有报文，URL 过滤功能不可用。

11 入侵防御实验

11.1 实验介绍

11.1.1 关于本实验

某企业部署了对外提供服务的 Web 服务器，但可能面临非法外网用户利用 SQL 注入漏洞，在未经授权的情况下访问网站后台数据库中的数据，盗取用户的隐私以及个人信息，造成企业的信息泄露。

本实验在 IPS 设备上配置入侵防御功能，用于防范 Internet 用户对企业内网的 Web 服务器发起的 SQL 注入攻击。

11.1.2 实验目的

- 通过使用 DVWA 理解 PHP 中 SQL 注入漏洞产生的原理及利用方法。
 - 掌握配置 IPS 入侵防御功能进行威胁防范。
-

11.1.3 实验组网介绍

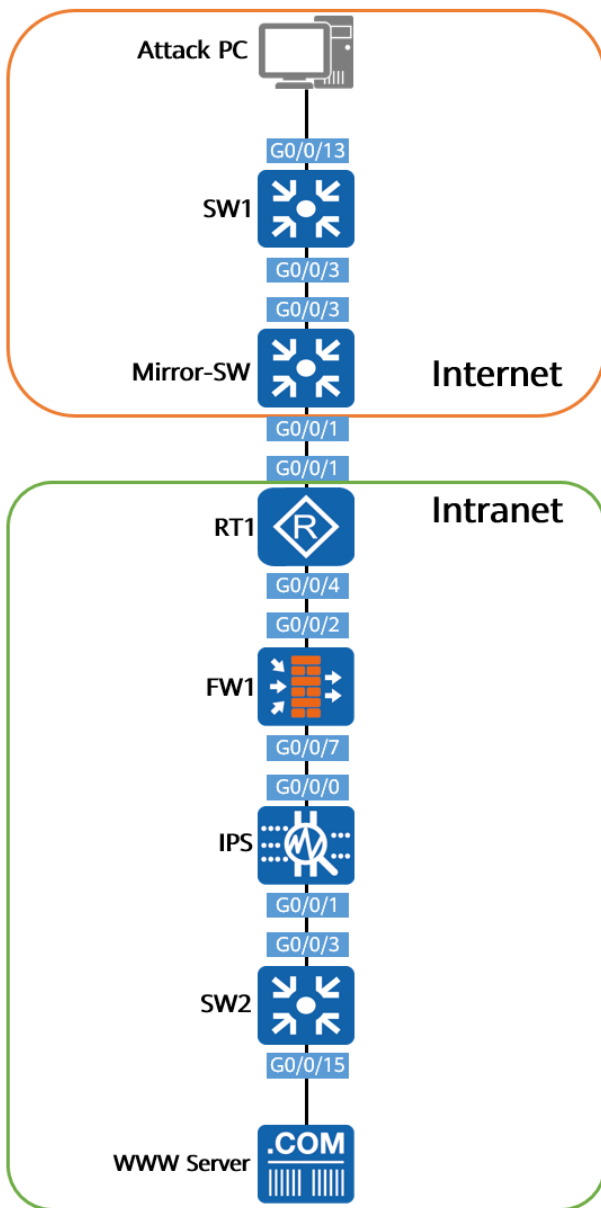


图11-1 漏洞与威胁防范实验拓扑图

FW1 作为企业出口安全网关，上连 RT1 出口路由器，下连 IPS 入侵防御设备。SW1、Mirror-SW 和 SW2 均为二层交换设备，Attack PC 模拟攻击者，对内网 Web 服务器发起 SQL 注入攻击。通过在 IPS 上配置签名过滤器和入侵防御配置文件防止攻击。

SW1、Mirror-SW、SW2、RT1 和 FW1 的相关配置在本实验配置步骤中未体现，具体配置可参考“11.4 配置参考”。

11.1.4 实验规划

表11-1 设备接口规划表

设备	接口	接口性质	IP地址	说明
FW1	G0/0/2	三层接口	10.1.3.2/30 安全区域: untrust	与RT1互连
	G0/0/7	三层接口	172.16.30.1/24 安全区域: trust	与IPS互连, WWW Server网关
RT1	G0/0/1	三层接口	20.20.20.1/24	Attack PC网关
	G0/0/4	三层接口	10.3.1.1/30	与FW1互连
IPS	G0/0/0	二层接口	安全区域: untrust	与FW1互连
	G0/0/1	二层接口	安全区域: trust	与SW2互连
SW1	G0/0/3	Access	PVID: 30	连接Attack PC
	G0/0/13	Access	PVID: 30	与Mirror-SW互连
Mirror-SW	G0/0/3	Access	PVID: 40	与SW1互连
	G0/0/1	Access	PVID: 40	与RT1互连
SW2	G0/0/3	Access	PVID: 30	与IPS互连
	G0/0/15	Access	PVID: 30	连接WWW Server
Attack PC	Ethernet0	网卡	20.20.20.2/24 网关: 20.20.20.1/24	终端
WWW Server	Ethernet0	网卡	172.16.30.10/24 网关: 172.16.30.1/24	终端

11.2 实验任务配置

11.2.1 配置思路

- 1.完成网络基本参数配置, 保证 Attack PC 与 WWW Server 可以通信。
- 2.使用 SQL 语句测试是否有注入点并验证注入类型。
- 3.使用 SQL 语句查询数据库信息与版本。
- 4.创建入侵防御配置文件, 配置签名过滤器。

5.配置业务安全策略，调用入侵防御配置文件。

说明：底层网络配置请参考“11.4 配置参考”，本实验只演示 SQL 漏洞测试与入侵防御的相关操作步骤。

11.2.2 配置步骤

步骤 1 禁用缺省策略

登录 IPS 设备 Web 管理界面，选择“策略 > 安全策略 > 安全策略”，执行以下操作，禁用 IPS 设备缺省的安全策略，避免影响后续对靶机的操作。

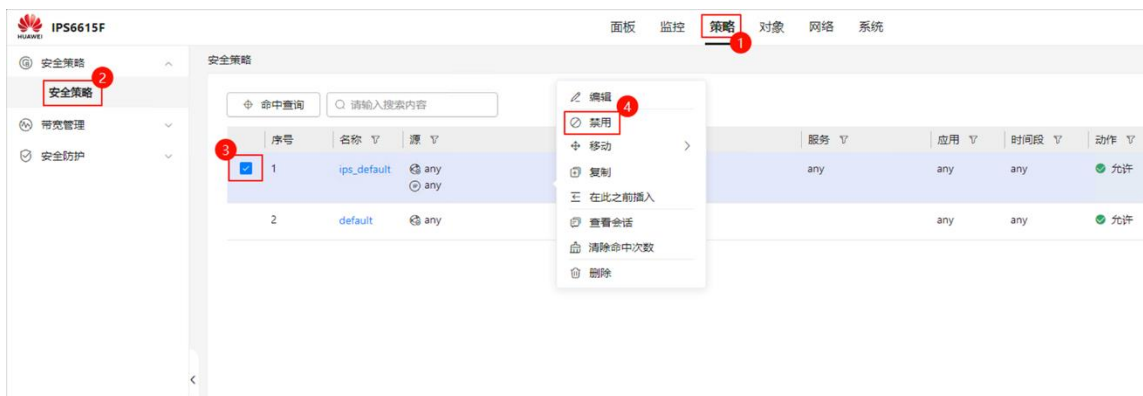


图11-2 禁用 IPS 缺省安全策略

步骤 2 登录靶场

使用 RDP 登录 Attack PC，打开浏览器输入“http://172.16.30.10:8080”，打开 DVWA，输入用户名“admin”，密码“password”，成功登录靶场环境，如下图所示：

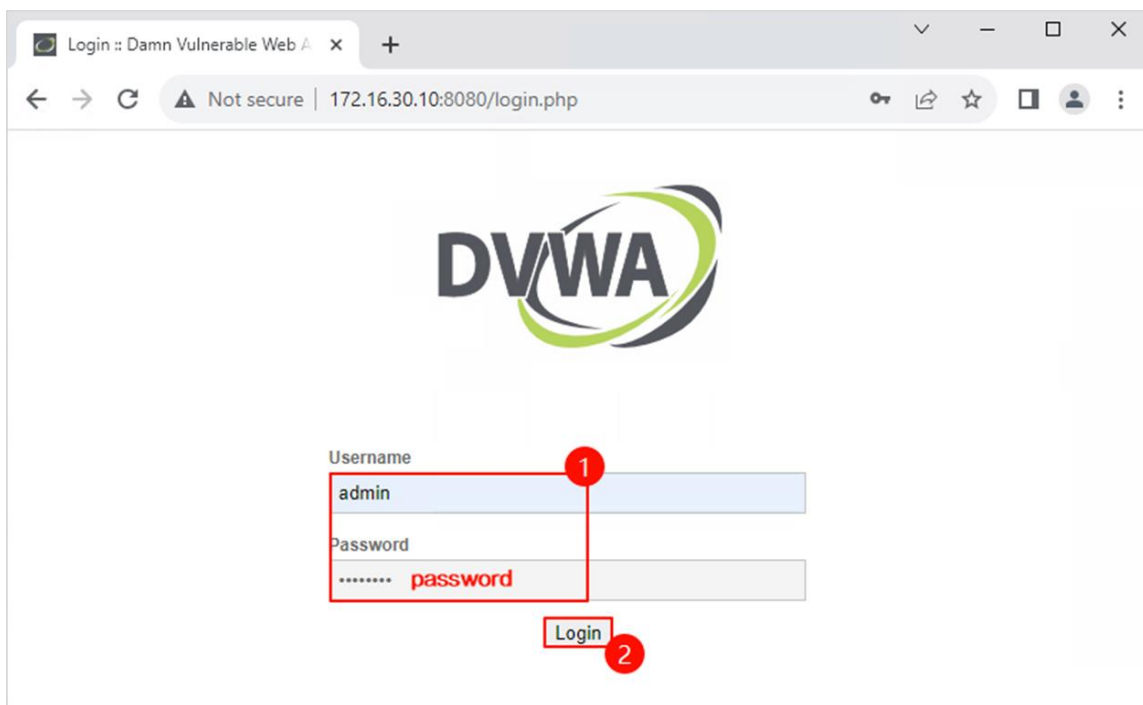


图11-3 登录靶场

步骤 3 调整安全级别

登录后，执行以下操作，将 DVWA 的安全级别调整为“low”。

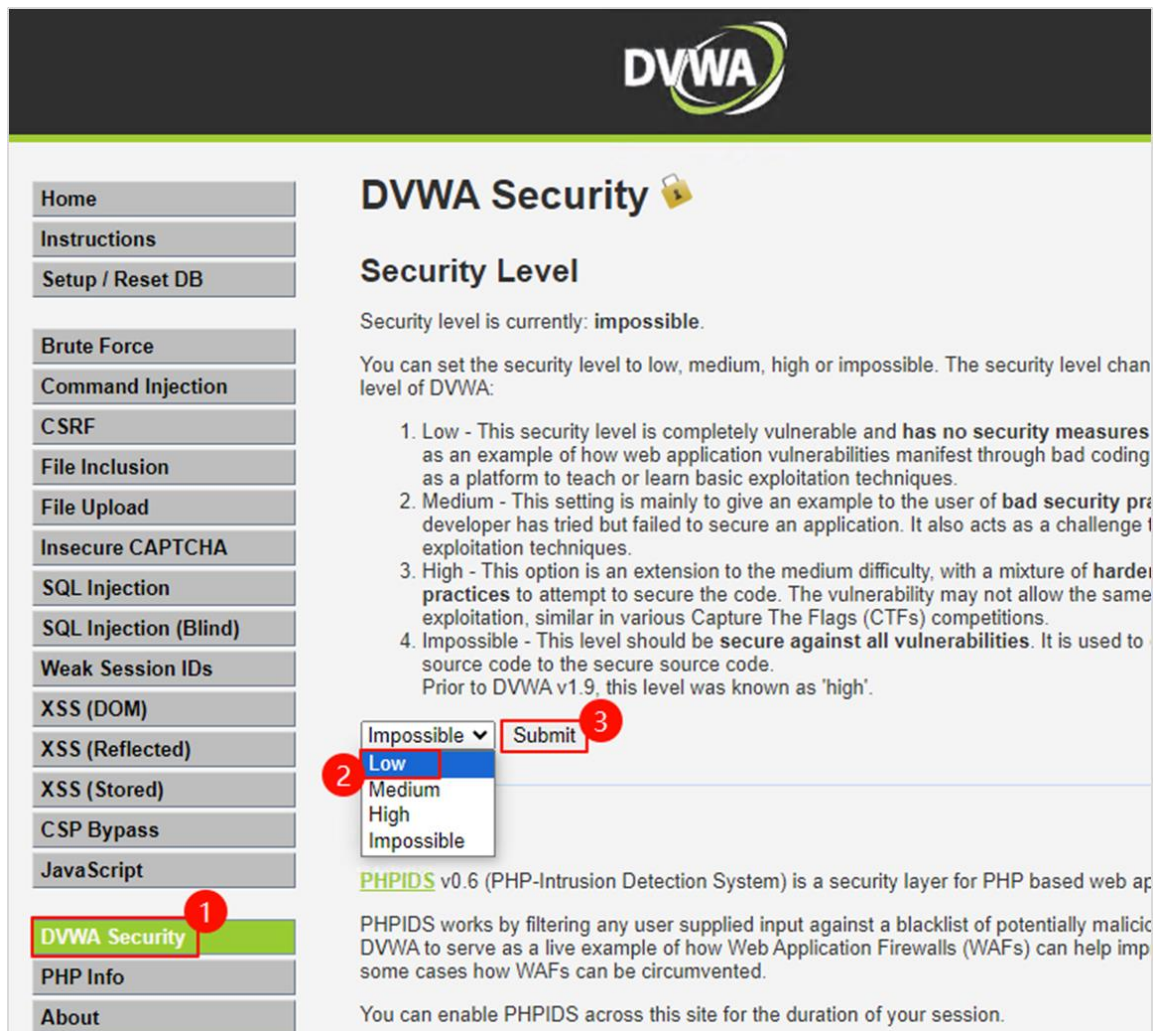


图11-4 调整 DVWA 安全级别

步骤 4 执行 ID 查询

说明：为避免 SQL 命令与双引号混淆，后续 SQL 相关命令均使用括号隔离。

输入 User ID，输入正确的 ID（1），然后提交，显示 ID，First name，Surname 信息。

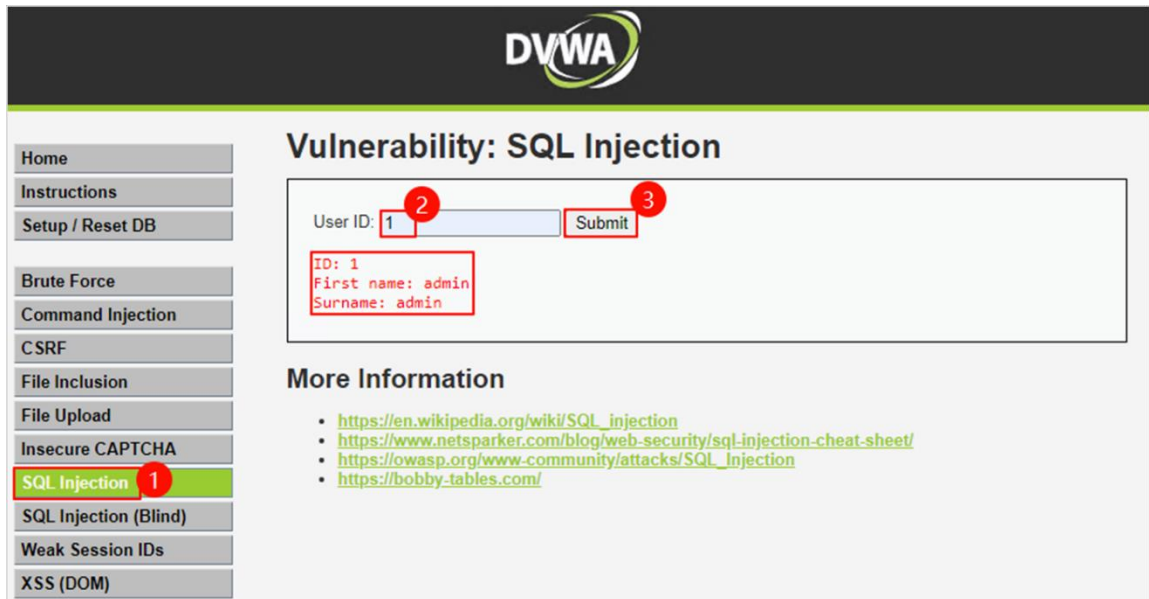


图11-5 执行 ID 查询

步骤 5 检测 SQL 注入漏洞

输入 User ID (1)，能够正常返回用户名和密码，在 1 后面尝试加上英文单引号 (')。

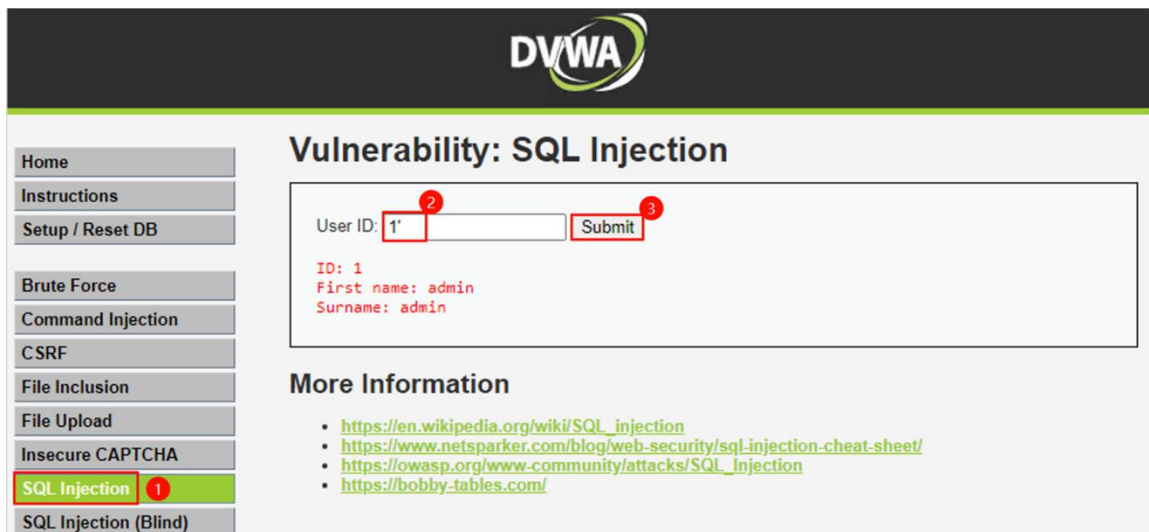


图11-6 检查 SQL 注入漏洞

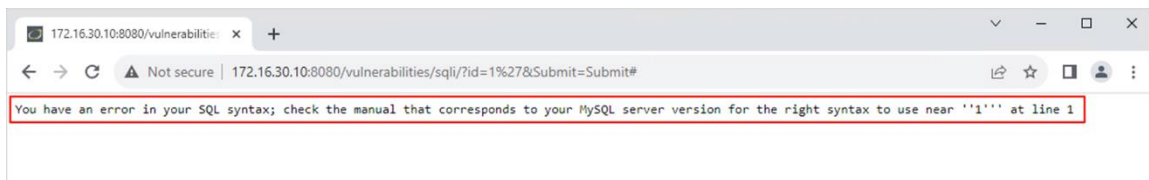


图11-7 查询结果报错

查询结果报错，说明此处存在注入点。

步骤 6 判断 SQL 注入类型

在注入点尝试输入（1 and 1=1）。

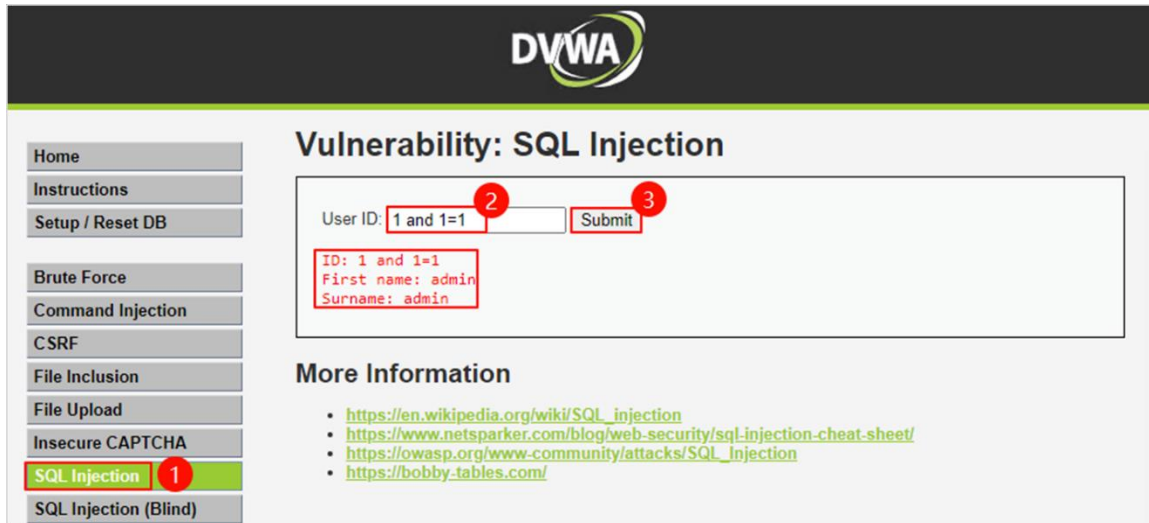


图11-8 判断是否为数字型注入（1）

成功返回数据，再次在注入点尝试输入（1 and 1=2）。

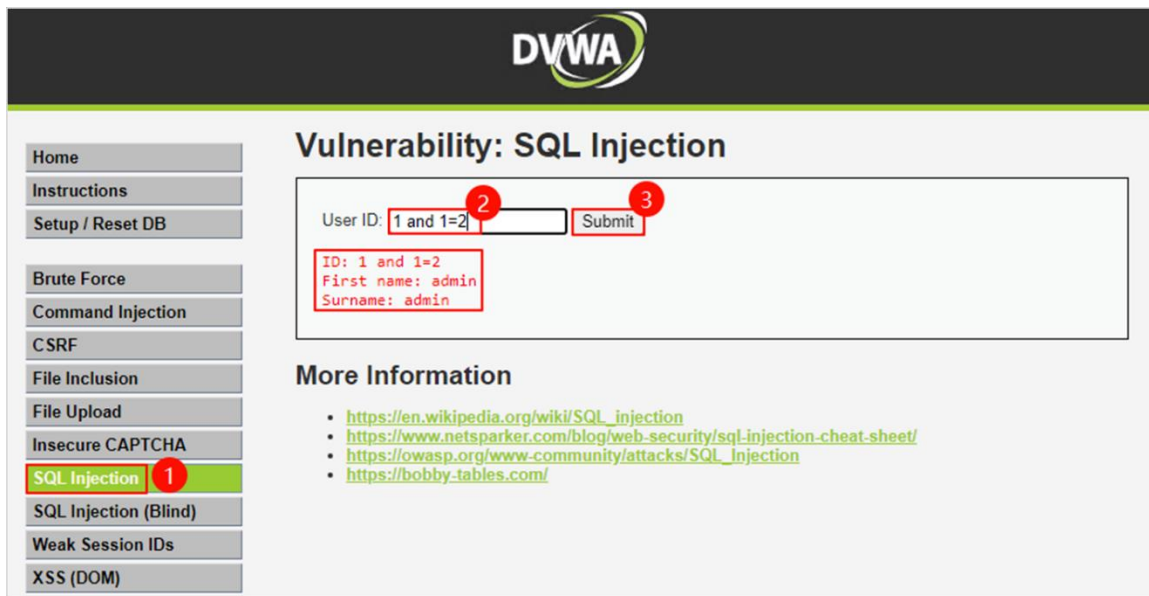


图11-9 判断是否为数字型注入（2）

结果依然成功返回数据，说明不是数字型注入，因为返回值没有受到数字的影响。

接下来判断是否为字符型注入，再次在注入点尝试输入（0' or 1#）。

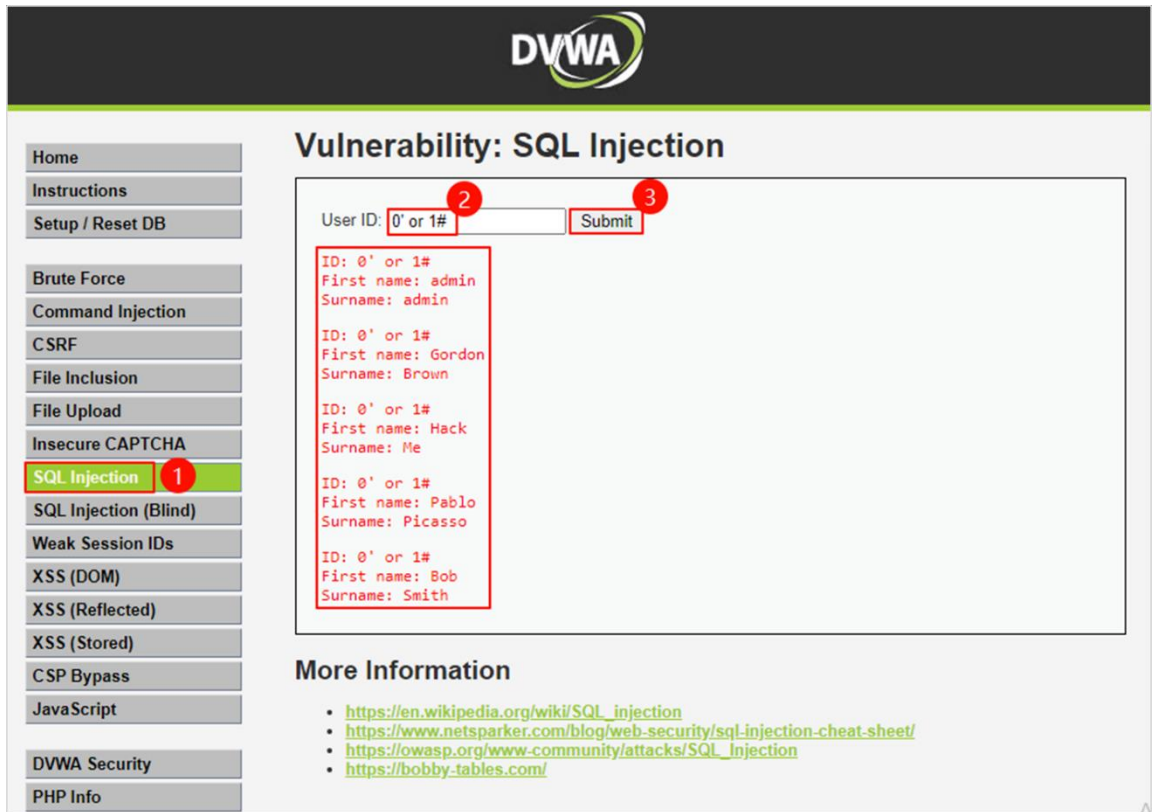


图11-10 判断是否为字符型注入

结果可以查到数据库中所有内容，说明是字符型注入。

步骤 7 查询信息列表长度

利用 order by [num]语句来测试查询信息列表长度，修改 num 的值，首先尝试输入（ 1' order by 1# ）。

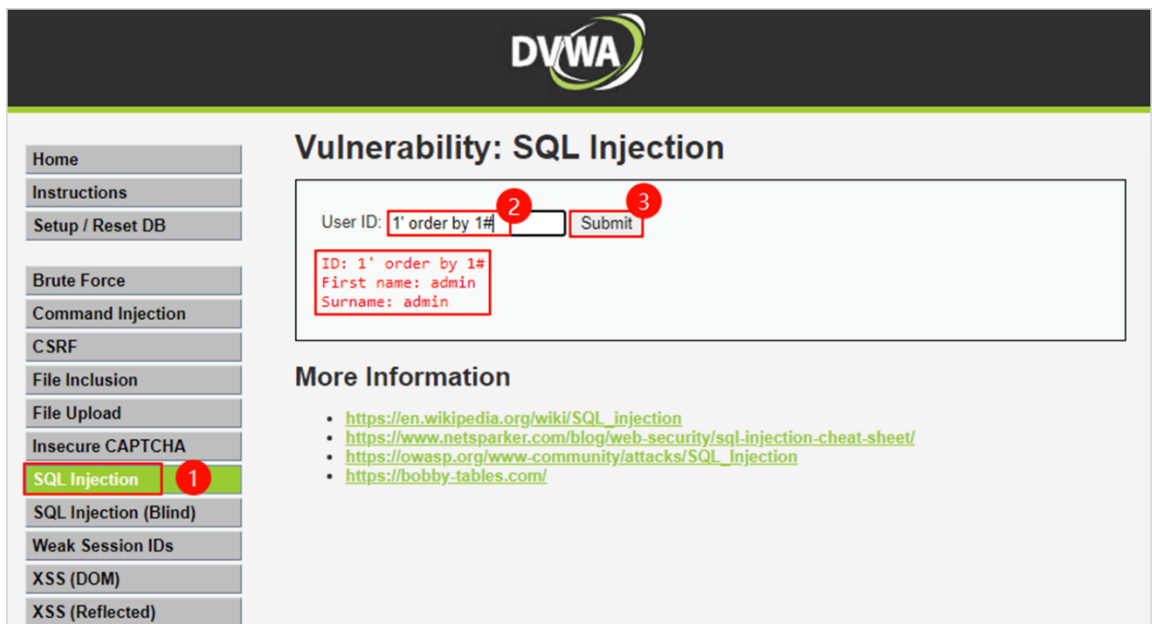


图11-11 查询信息列表长度（1）

结果页面正常显示数据，继续尝试输入（1' order by 2#）。

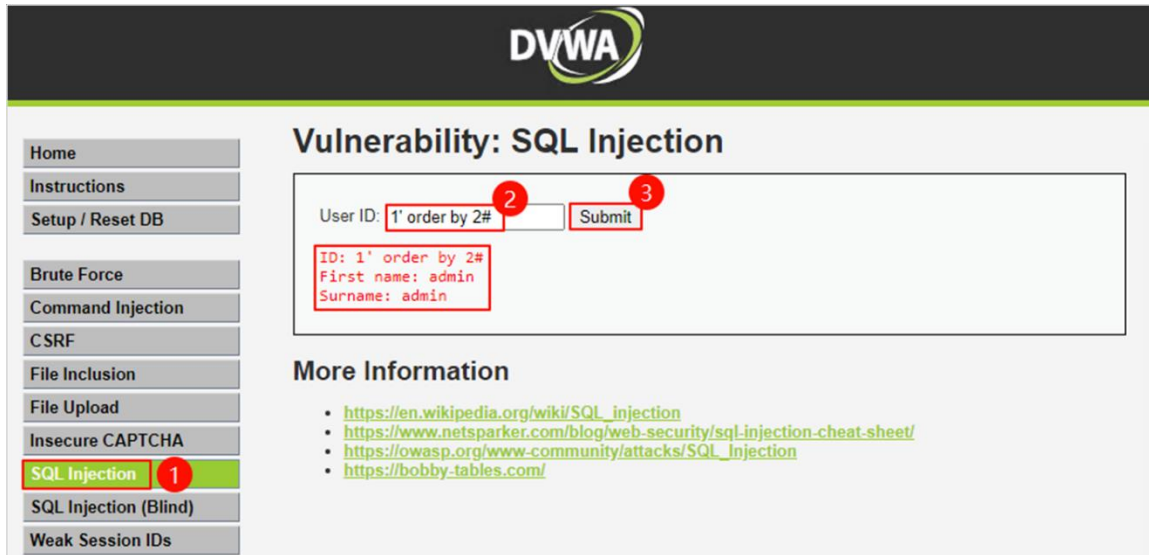


图11-12 查询信息列表长度（2）

结果页面正常显示数据，继续尝试输入（1' order by 3#）。

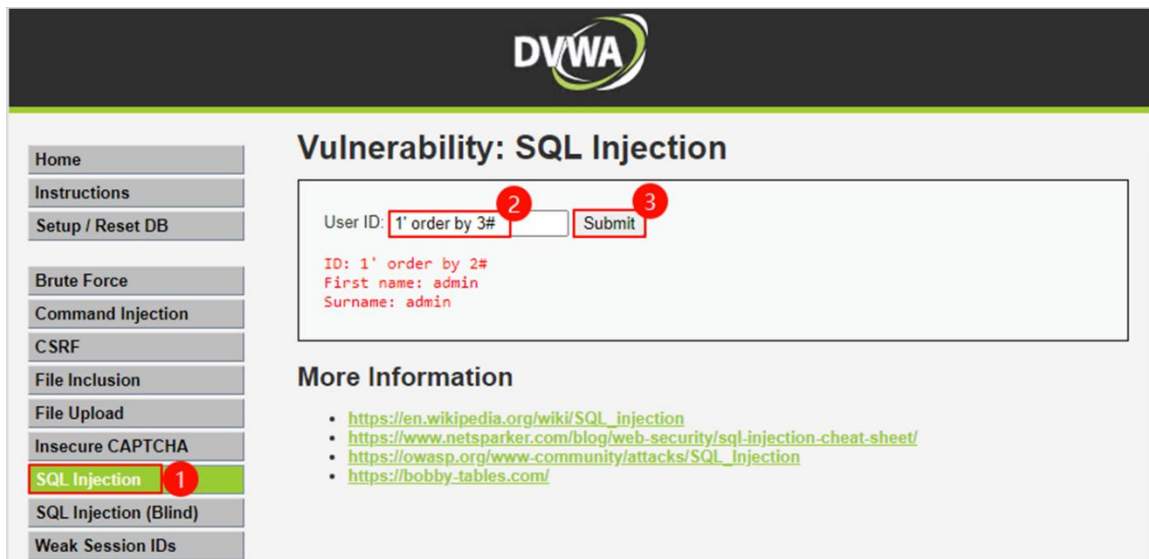


图11-13 查询信息列表长度（2）



图11-14 查询结果报错

当输入 num 取值为“3”时页面报错，由此我们判断表的尺寸为2列。

步骤 8 查询数据库用户和数据库名

构造联合查询语句（' union select user(),database()# ）查询当前数据库用户和数据库名。



图11-15 查询数据库用户和数据库名

基于回显信息可知数据库用户为“root@localhost”，数据库名为“dvwa”。

步骤 9 查询当前数据库版本

构造联合查询语句（'1' and 1=2 union select version(),database()# ）查询当前数据库版本信息。

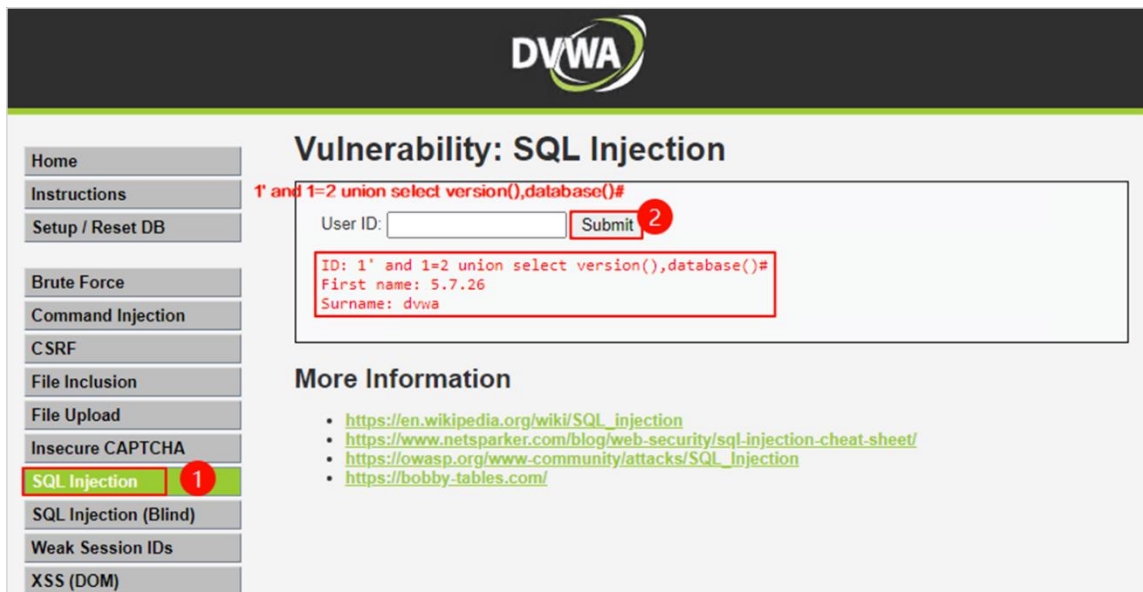


图11-16 查询数据库版本信息

基于回显信息可知数据库版本信息为“5.7.26”。

攻击者利用 SQL 注入漏洞，在未经授权的情况下，可以访问数据库中的数据，盗取用户的隐私以及个人信息，造成用户的信息泄露。SQL 注入漏洞作为出现频率最高，危害程度极大的安全漏洞，具有广泛性、隐蔽性、危害性、操作方便等特点，因此我们需要防范注入攻击，保障企业以及用户的信息安全。

步骤 10 配置 IPS 业务接口

本实验中，将 IPS 设备进行直路二层透明部署。需要设置上下游接口的工作模式和安全区域。

在 IPS 设备 Web 管理界面选择“网络 > 接口对”，执行以下操作，删除“g0/0/0_to_g0/0/1”接口对，并重新配置相关业务接口。

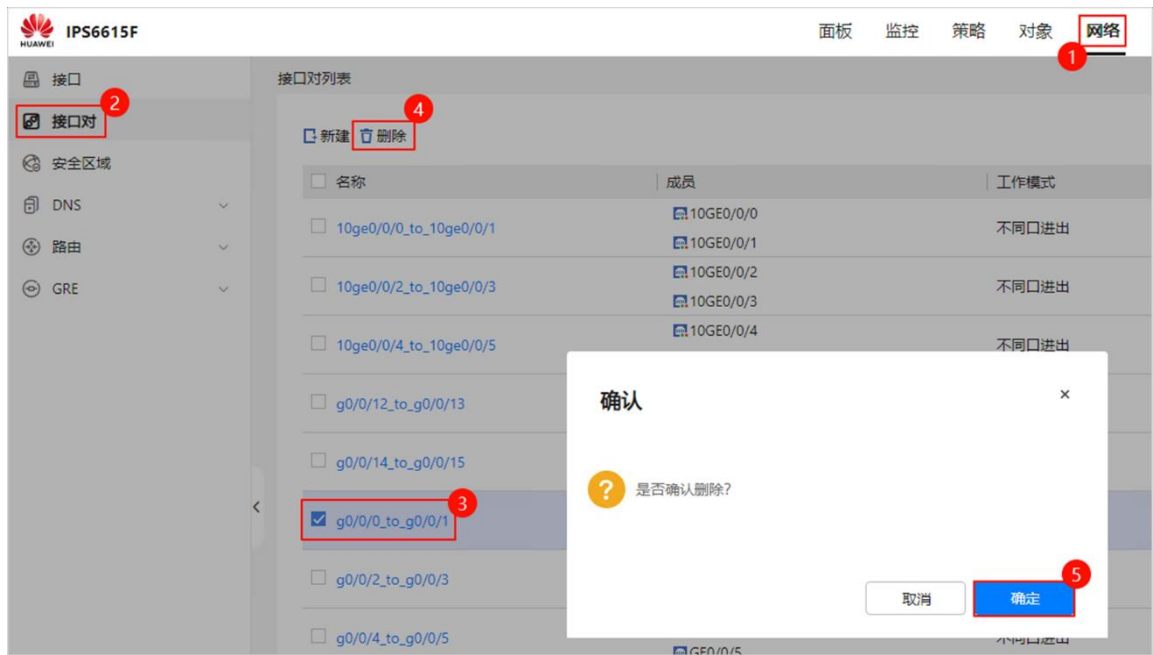


图11-17 删除原有接口对



图11-18 G0/0/0 接口基础配置



图11-19 G0/0/1 接口基础配置

步骤 11 配置 IPS 的工作模式

在 IPS 设备 Web 管理界面选择“系统 > 配置 > 全局参数配置”，执行以下操作，将 IPS 设备的工作模式设置为“防护模式”。



图11-20 设置 IPS 设备工作模式

步骤 12 创建入侵防御配置文件

在 IPS 设备 Web 管理界面选择“对象 > 安全配置文件 > 入侵防御”，执行以下操作，创建入侵防御配置文件。

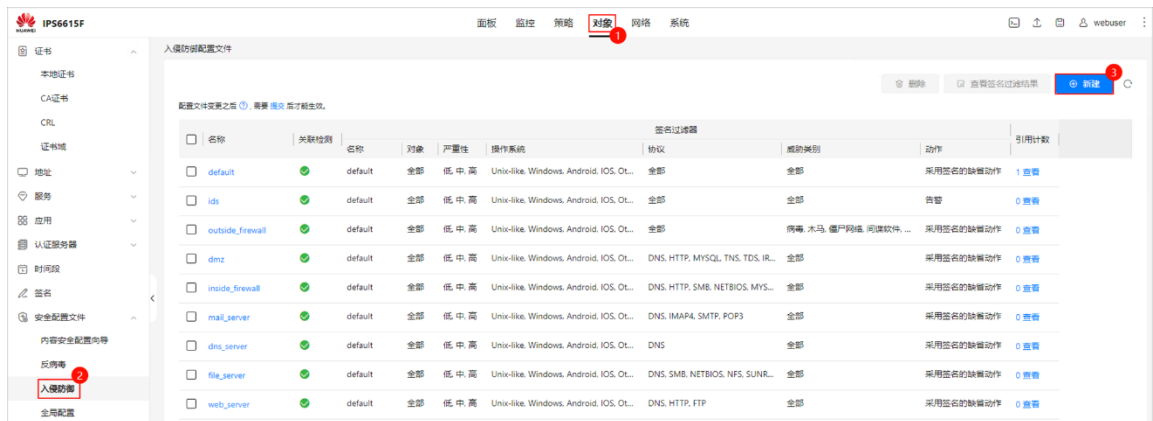


图11-21 进入入侵防御配置文件创建界面



图11-22 创建入侵防御配置文件（1）

新建签名过滤器

×

配置一个签名过滤器，可以方便的获得多个签名。通过选择对象、严重性、协议等签名的属性，系统会筛选出具有这些属性的签名。
如果不设定筛选属性默认为全部签名。

* 名称 SQL 1

对象 ☒ 服务端 ☒ 客户端

严重性 ☒ 高 ☒ 中 ☒ 低 ☒ 提示

操作系统 ☒ Windows ☒ Unix-like ☒ Android ☒ IOS ☒ Other

协议

☒ 全部

- ☒ 网络文件类协议
- ☒ 网络服务类协议
- ☒ 邮件类协议
- ☒ 聊天类协议
- ☒ 数据库类协议
- ☒ 其他类型

威胁类别

☐ 间谍软件
☐ 广告软件
☐ CGI攻击
☐ 跨站脚本攻击
☒ 注入攻击 2
☐ 目录遍历
☐ 信息泄露
☐ 远程文件包含攻击

动作

☐ 采用签名的缺省动作
☐ 告警
☒ 阻断 3

激活 Windows

转到“设置”以激活 Windows

预览签名过滤结果

取消

确定 4

图11-23 创建入侵防御配置文件（2）

新建入侵防御配置文件

×

* 名称

SQL

关联检测

☐

关联检测一般用于检测暴力破解类攻击，如果经过设备的流量已做过IP地址转换，需要关闭此功能，避免误报。

签名过滤器

例外签名

删除

新建

☐	名称	签名过滤结果	对象	严重性	操作系统	协议	威胁类别
☐	SQL	查看签名过滤结果	全部	高, 中, 低 提示	Windows, Unix-like, ...	全部	注入攻击

激活 Windows

转到“设置”以激活 Windows

取消

确定

图11-24 创建入侵防御配置文件（3）

完成上述配置后，在 IPS 设备 Web 管理界面右上角点击“提交”按钮，使相关配置生效。

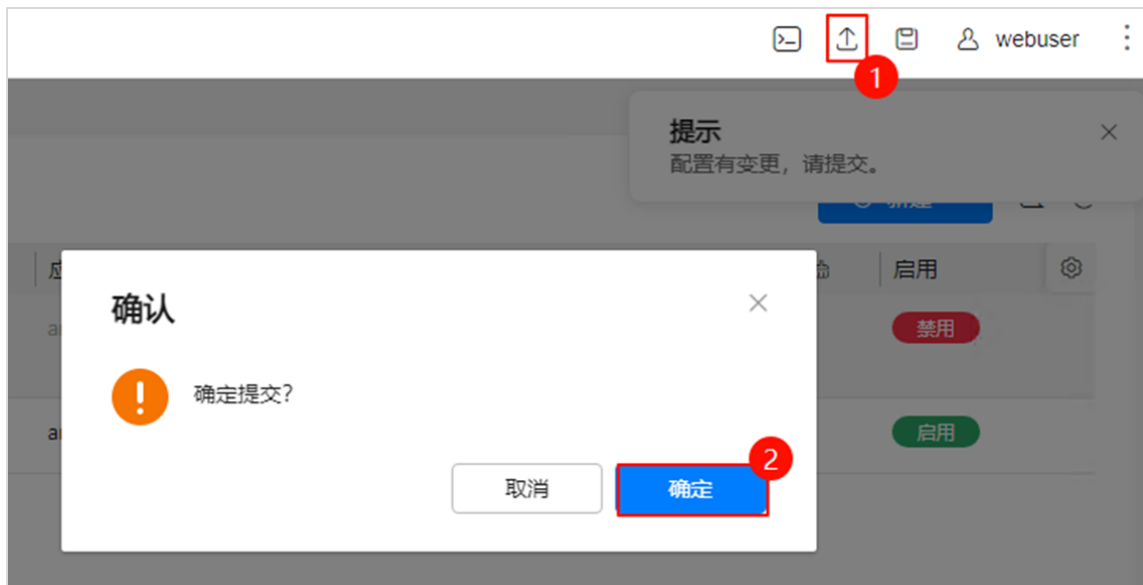


图11-25 提交配置

步骤 13 调用入侵安全配置文件

在 IPS 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”，进入安全策略配置界面，执行以下操作，创建业务安全策略，并调用之前创建的入侵防御配置文件。



图11-26 进入安全策略配置界面

新建安全策略

×

概述

* 名称

IPS_SQL

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 ?

172.16.30.0/...

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

取消

命令预览

确定

图11-27 配置业务安全策略



图11-28 调用入侵防御配置文件

11.3 结果验证

在 Attack PC 上访问 DVWA 页面，再次使用（ ' union select user(),database()# ）联合查询语句，尝试查询当前数据库用户和数据库名。

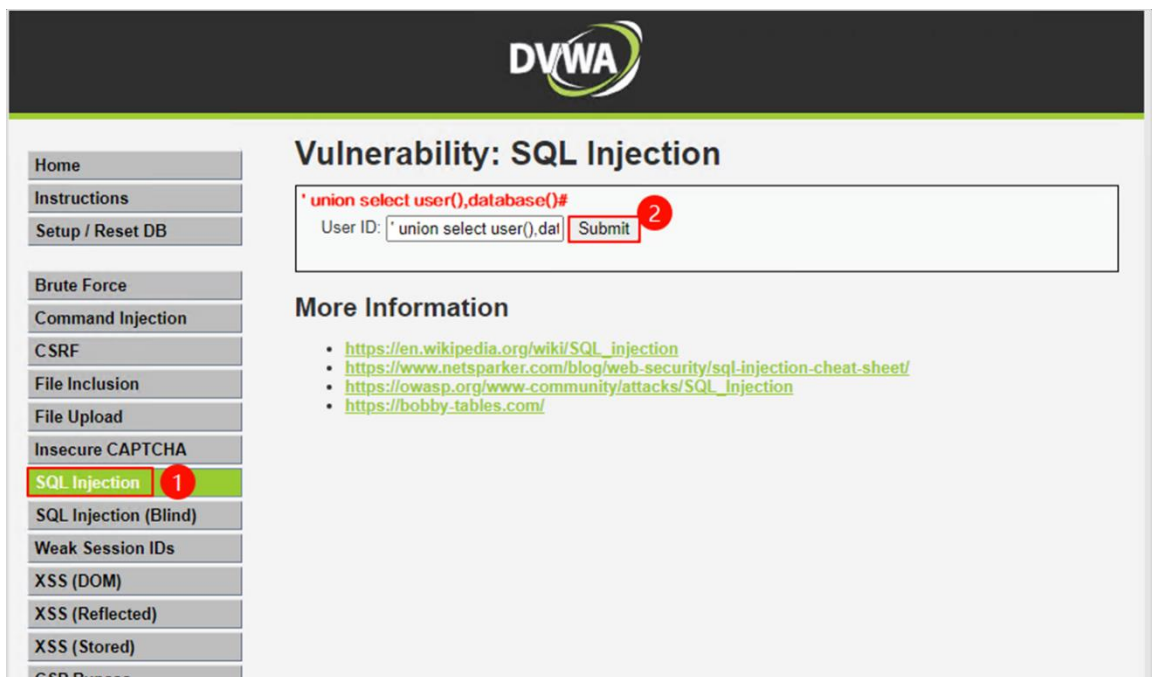


图11-29 尝试查询当前数据库用户和数据库名

发现页面被 IPS 设备阻断，如下图所示：

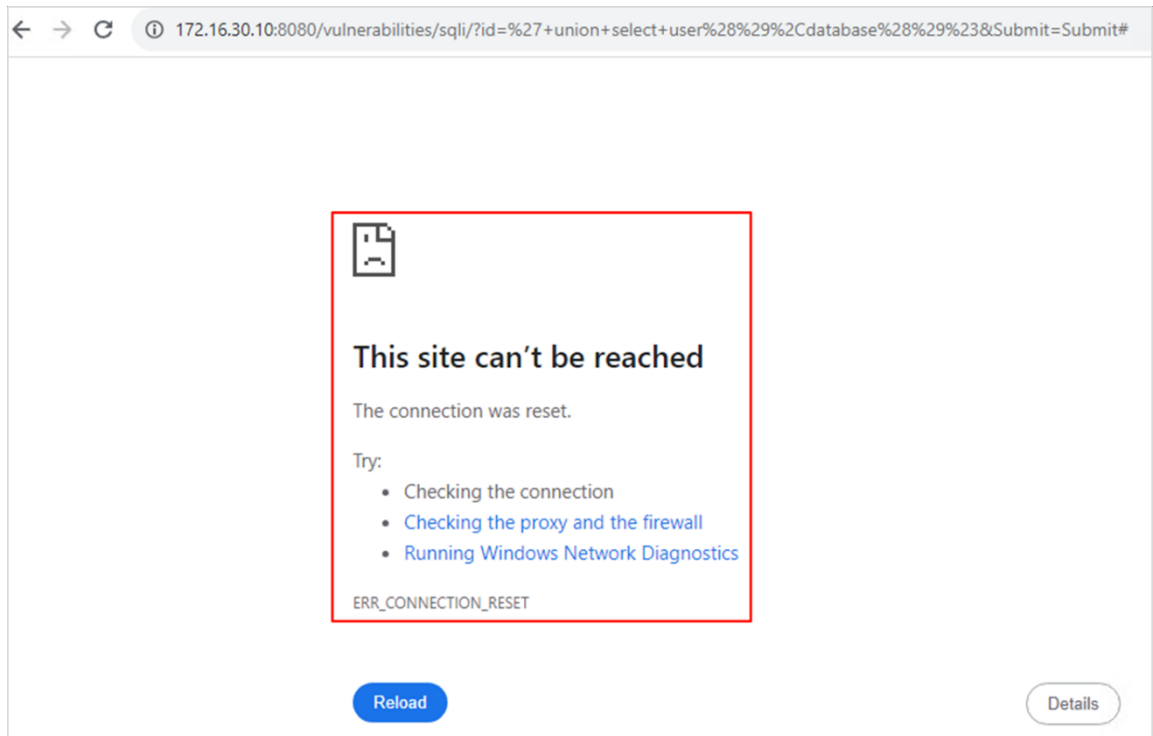


图11-30 DVWA 页面被阻断

登录 IPS 设备 Web 管理界面，选择“监控 > 日志 > 威胁日志”，执行以下操作，查看 IPS 设备的威胁日志。

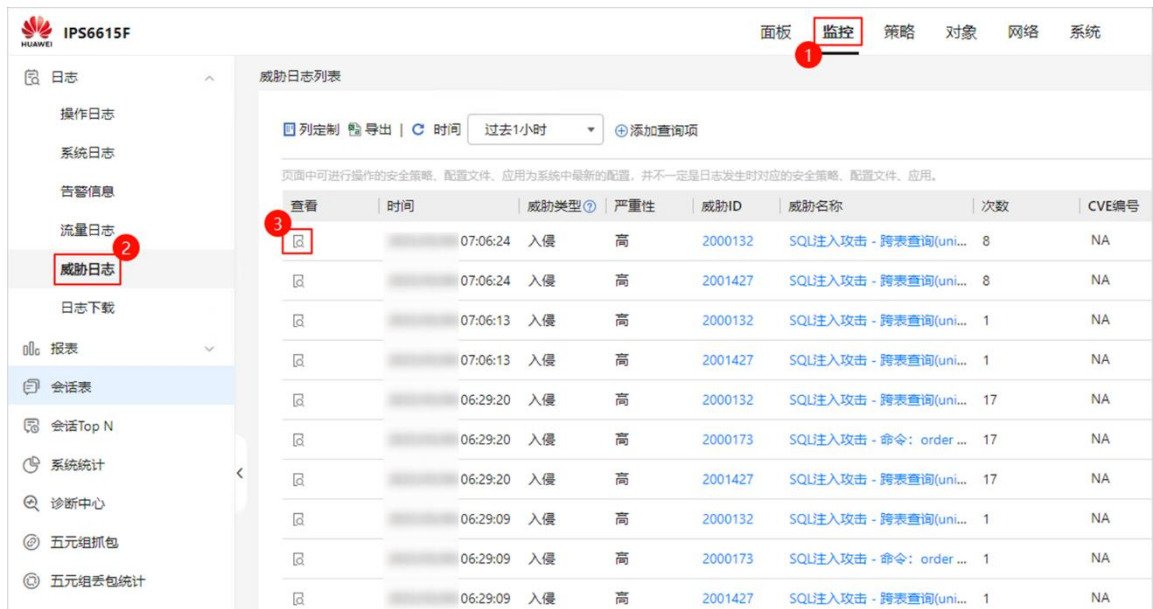


图11-31 查看 IPS 设备威胁日志（1）

查看威胁日志详情

日志公共字段

时间:

07:06:24

协议:

TCP

安全策略:

IPS_SQL

应用类别:

网络架构

应用子类别:

网络基础协议

应用:

HTTP

威胁

威胁类型:

入侵

入侵子类型:

攻击入侵

威胁名称:

SQL注入攻击 - 跨表查询(union ...

威胁ID:

2000132

次数:

8

配置文件:

SQL

动作:

阻断

源

源安全区域:

untrust

源地址:

20.20.20.2

源端口:

0

NAT源地址:

NAT源端口:

目的

目的安全区域:

trust

目的地址:

172.16.30.10

目的端口:

8080

NAT目的地址:

NAT目的端口:

关闭

图11-32 查看 IPS 设备威胁日志（2）

11.4 配置参考

11.4.1 IPS 配置

```
#
sysname IPS
#
profile type ips name SQL
undo assoc-check enable
signature-set name SQL
action block
os unix-like windows android ios other
target both
severity low medium high information
protocol all
category Injection
#
interface GE0/0/0
portswitch
```

```
port default vlan 1
#
interface GE0/0/1
portswitch
port default vlan 1
#
firewall zone trust
add interface GE0/0/1
#
firewall zone untrust
add interface GE0/0/0
#
security-policy
default action permit
rule name ips_default
disable
profile ips default
action permit
rule name IPS_SQL
source-zone untrust
destination-zone trust
destination-address 172.16.30.0 mask 255.255.255.0
profile ips SQL
action permit
#
return
```

11.4.2 RT1 预配置

```
#
sysname RT1
#
interface GigabitEthernet0/0/1
undo portswitch
ip address 20.20.20.1 255.255.255.0
#
interface GigabitEthernet0/0/4
undo portswitch
ip address 10.3.1.1 255.255.255.252
#
ip route-static 172.16.30.0 255.255.255.0 10.3.1.2
#
```

11.4.3 FW1 预配置

```
#
sysname FW1
#
```

```
interface GE0/0/2
 ip address 10.3.1.2 255.255.255.252
#
interface GE0/0/7
 ip address 172.16.30.1 255.255.255.0
#
firewall zone trust
 add interface GE0/0/7
#
firewall zone untrust
 add interface GE0/0/2
#
security-policy
 rule name u2t
  source-zone untrust
  destination-zone trust
  destination-address 172.16.30.0 mask 255.255.255.0
  action permit
#
ip route-static 0.0.0.0 0.0.0.0 10.3.1.1
#
```

11.4.4 SW1 预配置

```
sysname SW1
#
vlan batch 30
#
interface GigabitEthernet0/0/3
 port default vlan 30
#
interface GigabitEthernet0/0/13
 port default vlan 30
#
```

11.4.5 SW2 预配置

```
sysname SW2
#
vlan batch 30
#
interface GigabitEthernet0/0/3
 port default vlan 30
#
interface GigabitEthernet0/0/15
 port default vlan 30
#
```

11.4.6 Mirror-SW 预配置

```
sysname Mirror-SW
#
vlan batch 40
#
interface GigabitEthernet0/0/1
 port default vlan 40
#
interface GigabitEthernet0/0/3
 port default vlan 40
#
```

11.5 思考题

一个签名过滤器中设定的多个过滤条件之间的关系是什么？

参考答案：一个签名必须同时满足所有过滤条件才能加入签名过滤器。也即签名过滤器设定的多个过滤条件之间是“与”的关系。

12 802.1X 认证实验

12.1 实验介绍

12.1.1 关于本实验

某企业部署了 WLAN 为员工提供无线办公环境，出于安全考虑，企业计划使用 802.1X 认证技术对用户执行准入认证，且由于员工人数较多，需要使用 RADIUS 服务器（iMaster NCE-Campus）统一管理员工的账号和权限。

12.1.2 实验目的

- 掌握无线 AC 基础配置。
- 掌握 WLAN 模板配置。
- 掌握 WLAN 802.1X 认证配置。

12.1.3 实验组网介绍

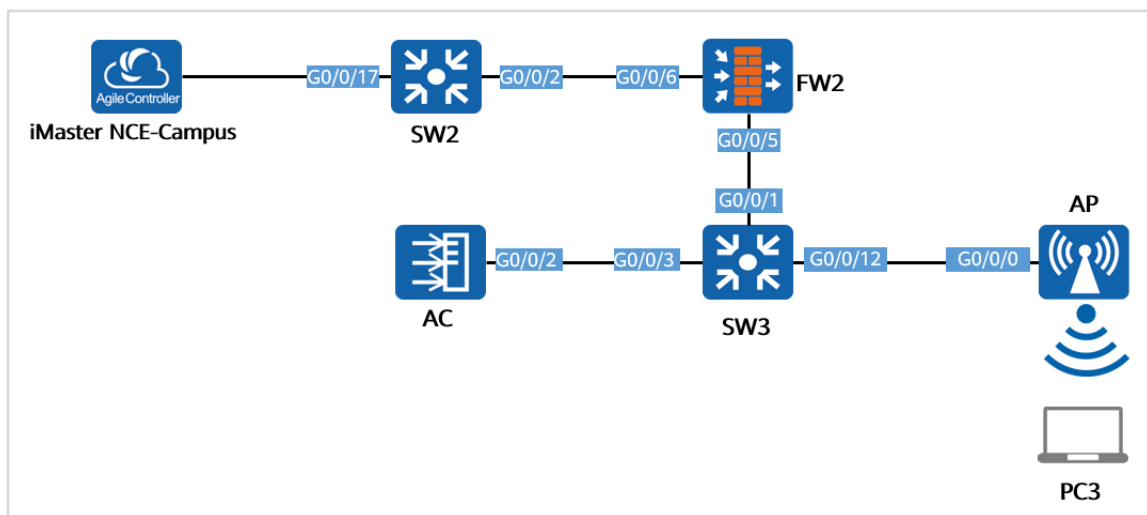


图12-1 802.1x 认证实验拓扑

- 1.使用外置电源给 AP 供电，iMaster NCE-Campus 作为 RADIUS 服务器。
- 2.AP 与 AC 之间为二层组网，AP 和终端的 DHCP 服务器均部署在 AC 上。
- 3.AC 与 RADIUS 服务器之间为二层组网，无线终端的 AAA 认证由 RADIUS 服务器执行。

12.1.4 实验规划

表12-1 设备接口规划表

设备	接口	接口性质	接口信息	说明
SW2	G0/0/2	Trunk	PVID: 1 Allow-pass VLAN: 10	与FW2互连
	G0/0/17	Access	PVID: 10	连接iMaster NCE-Campus
SW3	G0/0/1	Trunk	PVID: 1 Allow-pass VLAN: 10	与FW2互连
	G0/0/3	Trunk	PVID: 1 Allow-pass VLAN: 10, 4000, 4001	与AC互连
	G0/0/12	Trunk	PVID: 4000 Allow-pass VLAN: 4000	与AP互连
FW2	GE0/0/5	Trunk	PVID: 1 Allow-pass VLAN: 10	与SW3互连
	GE0/0/6	Trunk	PVID: 1 Allow-pass VLAN: 10	与SW2互连
AC	GE0/0/2	Trunk	PVID: 1 Allow-pass VLAN: 10, 4000, 4001	与SW3互连
AP	GE0/0/0	/	保持默认无需配置	与SW3互连
iMaster NCE-Campus	Ethernet0	网卡	192.168.2.201/24	服务器接口IP

12.2 实验任务配置

12.2.1 配置思路

- 1.底层网络配置，实现 AC 到 AP 之间互通。
- 2.配置 AC 的 DHCP Server 功能，为 AP 分配管理地址，为无线终端分配业务地址。
- 3.配置 AP 上线。

- 4.在 AC 上配置对接 RADIUS 认证服务器的参数。
- 5.在 iMaster NCE-Campus 上配置 RADIUS 功能。
- 6.完成 SSID 等模板及 WLAN 802.1x 认证相关配置。

12.2.2 配置步骤

步骤 1 设备基础配置

按照“表 12-1”数据规划，完成 AC、SW3、AP 之间二层网络的配置，完成 SW3、FW2、SW2 之间的二层网络的配置。

配置 AC 的 GigabitEthernet0/0/2 接口。

```
[AC] vlan batch 10 4000 4001
[AC] interface GigabitEthernet0/0/2
[AC-GigabitEthernet0/0/2] port link-type trunk
[AC-GigabitEthernet0/0/2] undo port trunk allow-pass vlan 1
[AC-GigabitEthernet0/0/2] port trunk allow-pass vlan 10 4000 4001
[AC-GigabitEthernet0/0/2] quit
```

配置 SW3 的 G0/0/3、G0/0/12 和 G0/0/1 接口。

```
[SW3] vlan batch 10 4000 4001
[SW3] interface GigabitEthernet0/0/3
[SW3-G0/0/3] port link-type trunk
[SW3-G0/0/3] port trunk allow-pass vlan 10 4000 4001
[SW3-G0/0/3] quit
[SW3] interface GigabitEthernet0/0/12
[SW3-G0/0/12] port link-type trunk
[SW3-G0/0/12] port trunk pvid vlan 4000
[SW3-G0/0/12] port trunk allow-pass vlan 4000
[SW3-G0/0/12] quit
[SW3] interface GigabitEthernet0/0/1
[SW3-G0/0/1] port link-type trunk
[SW3-G0/0/1] port trunk allow-pass vlan 10
[SW3-G0/0/1] quit
```

配置 FW2 的 GE0/0/5 和 GE0/0/6 接口，并将接口加入安全区域。

```
[FW2] vlan 10
[FW2] interface GE0/0/5
[FW2-GE0/0/5] portswitch
[FW2-GE0/0/5] port link-type trunk
[FW2-GE0/0/5] undo port trunk allow-pass vlan 1
[FW2-GE0/0/5] port trunk allow-pass vlan 10
[FW2-GE0/0/5] quit
[FW2] interface GE0/0/6
[FW2-GE0/0/6] portswitch
[FW2-GE0/0/6] port link-type trunk
[FW2-GE0/0/6] undo port trunk allow-pass vlan 1
```

```
[FW2-GE0/0/6] port trunk allow-pass vlan 10
[FW2-GE0/0/6] quit
[FW2] firewall zone trust
[FW2-zone-trust] add interface GE0/0/5
[FW2-zone-trust] add interface GE0/0/6
[FW2-zone-trust] quit
```

配置 SW2 的 G0/0/2、G0/0/17 接口。

```
[SW2] vlan 10
[SW2] interface GigabitEthernet 0/0/2
[SW2-G0/0/2] port link-type trunk
[SW2-G0/0/2] undo port trunk allow-pass vlan 1
[SW2-G0/0/2] port trunk allow-pass vlan 10
[SW2-G0/0/2] quit
[SW2] interface GigabitEthernet 0/0/17
[SW2-G0/0/17] port link-type access
[SW2-G0/0/17] port default vlan 10
[SW2-G0/0/17] quit
```

步骤 2 配置 DHCP

AC 需要为 AP 提供管理地址，同时为无线用户（PC3）提供业务地址，本实验配置 VLAN4000 为管理网段，配置 VLAN4001 为业务网段。

开启 AC 的 DHCP 功能。

```
[AC] dhcp enable
```

配置 AP 管理网段的网关，并选择全局 DHCP 地址池。

```
[AC] interface vlanif4000
[AC-VLANIF4000] ip address 10.10.1.1 255.255.255.0
[AC-VLANIF4000] dhcp select global
[AC-VLANIF4000] quit
```

配置 AP 管理网段的 DHCP 地址池。

```
[AC] ip pool vlan4000
[AC-ip-pool-vlan4000] gateway-list 10.10.1.1
[AC-ip-pool-vlan4000] network 10.10.1.0 mask 255.255.255.0
[AC-ip-pool-vlan4000] option 43 sub-option 3 ascii 10.10.1.1
[AC-ip-pool-vlan4000] quit
```

配置无线业务网段的网关，并选择全局 DHCP 地址池。

```
[AC] interface vlanif4001
[AC-VLANIF4001] ip address 10.20.1.1 255.255.255.0
[AC-VLANIF4001] dhcp select global
[AC-VLANIF4001] quit
```

配置无线用户网段的 DHCP 全局地址池。

```
[AC] ip pool vlan4001
[AC-ip-pool-vlan4001] gateway-list 10.20.1.1
```

```
[AC-ip-pool-vlan4001] network 10.20.1.0 mask 255.255.255.0
[AC-ip-pool-vlan4001] quit
```

配置无线用户认证地址，与 RADIUS 认证服务器（iMaster NCE-Campus）通信。

```
[AC] interface vlanif10
[AC-VLANIF10] ip address 192.168.2.100 255.255.255.0
[AC-VLANIF10] quit
```

步骤 3 配置 AP 上线

创建 AP 组，用于将相同配置的 AP 都加入同一 AP 组中，并配置免认证。

```
[AC] wlan
[AC-wlan-view] ap-group name ap-group1
[AC-wlan-ap-group-ap-group1] quit
[AC-wlan-view] ap auth-mode no-auth
[AC-wlan-view] ap-mac 28fb-aeb7-d580 //MAC 地址并非固定，需要基于实验环境中 AP 的真实 MAC 调整
[AC-wlan-ap-0] ap-group ap-group1
```

创建域管理模板，在域管理模板下配置 AC 的国家码并在 AP 组下引用域管理模板。

```
[AC-wlan-view] regulatory-domain-profile name domain1
[AC-wlan-regulate-domain-domain1] country-code cn
Info: The current country code is same with the input country code.
[AC-wlan-regulate-domain-domain1] quit
[AC-wlan-view] ap-group name ap-group1
[AC-wlan-ap-group-ap-group1] regulatory-domain-profile domain1
Warning: This configuration change will clear the channel and power configurations of radios, and may
restart APs. Continue?[Y/N]:y
[AC-wlan-ap-group-ap-group1] quit
[AC-wlan-view] quit
[AC]
```

配置 AC 的源接口。

```
[AC] capwap source interface vlanif4000
Set the DTLS PSK(contains 8-32 plain-text characters, or 48 or 68 cipher-text characters that must be a
combination of at least two
of the following: lowercase letters a to z, uppercase letters A to Z, digits, and special characters): //配
置 DTLS 加密的 PSK
Confirm PSK: //重复输入 DTLS 加密的 PSK，两次输入保持一致
Configuring the new PSK, waiting...
Info: Deliver DTLS PSK to devices using CAPWAP connections. It may take a few minutes.
-----
CAPWAP DTLS PSK deliver result
Deliver Number : 0
Success Number : 0
Failed Number : 0
-----done.
Set the DTLS inter-controller PSK(contains 8-32 plain-text characters, or 48 or 68 cipher-text characters
that must be a combination
```

```

of at least two of the following: lowercase letters a to z, uppercase letters A to Z, digits, and special
characters): //配置 AC 间 DTLS 加密的 PSK
Confirm PSK: //重复输入 AC 间 DTLS 加密的 PSK, 两次输入保持一致
Configuring the new PSK, waiting.....done.
Set the user name for FIT APs(The value is a string of 4 to 31 characters, which can contain letters,
underscores, and digits, and m
ust start with a letter):admin //统一配置 FIT AP 的登录用户名
Set the password for FIT APs(plain-text password of 8-128 characters or cipher-text password of 48-188
characters that must be a combina
tion of at least three of the following: lowercase letters a to z, uppercase letters A to Z, digits, and
special characters): //统一配置 FIT AP 的登录密码
Confirm password: //重复输入 FIT AP 的登录密码, 两次输入保持一致
Set the global temporary-management psk(contains 8-63 plain-text characters, or 48-108 cipher-text
characters that must be a combina
tion of at least two of the following: lowercase letters a to z, uppercase letters A to Z, digits, and special
characters): //配置全局离线管理 VAP 的接入密码
Confirm PSK: //重复输入全局离线管理 VAP 的接入密码, 两次输入保持一致
Warning: Ensure that the management VLAN and service VLAN are different. Otherwise, services may be
interrupted.
Warning: Before an added device goes online for the first time, enable DTLS no-auth if it runs a version
earlier than V200R021C00 or
enable DTLS certificate-mandatory-match if it runs V200R021C00 or later.
[AC] capwap dtls no-auth enable //V200R021C00 版本开始, AC 默认开启 CAPWAP 控制隧道的 DTLS 加
密功能。添加 AP 时 AP 会上线失败, 此时需要先开启 CAPWAP DTLS 不认证方式让 AP 上线, 以便 AP 获取
安全凭证, AP 上线后应及时关闭该功能 (undo capwap dtls no-auth enable), 避免未授权 AP 上线
Warning: This operation allows for device access in non-DTLS encryption mode even when DTLS is
enabled and brings security risks. Af
ter the device goes online for the first time, disable this function to prevent security risks.
Continue?[Y/N]:y
[AC]

```

执行命令 display ap all 查看到 AP 的 “State” 字段为 “nor” 时, 表示 AP 正常上线。

```

[AC-wlan-ap-0]display ap all
Total AP information:
nor : normal [1]
ExtraInfo : Extra information
-----
ID MAC Name Group IP Type State STA
Uptime ExtraInfo
-----
0 28fb-aeb7-d580 28fb-aeb7-d580 ap-group1 10.10.1.187 AirEngine5761-12 nor 0 5S -
-----
Total: 1

```

步骤 4 RADIUS 服务器对接参数配置

在 AC 上创建 RADIUS 服务器模板。

```

[AC] radius-server template t1
[AC-radius-wlan-t1] radius-server authentication 192.168.2.201 1812

```

```
[AC-radius-wlan-t1] radius-server accounting 192.168.2.201 1813
[AC-radius-wlan-t1] radius-server shared-key cipher Huawei@123
[AC-radius-wlan-t1] quit
```

在 AC 上配置与 RADIUS 服务器通信的源地址为 192.168.2.100。

```
[AC] radius-server source ip-address 192.168.2.100
```

创建 RADIUS 方式的认证方案。

```
[AC] aaa
[AC-aaa] authentication-scheme HCIP-Security
Info: Create a new authentication scheme.
[AC-aaa-authen-HCIP-Security] authentication-mode radius
[AC-aaa-authen-HCIP-Security] quit
[AC-aaa]quit
[AC]
```

步骤 5 802.1x 认证和 SSID 相关配置

创建名为“HCIP-Security”的 802.1X 接入模板，配置认证方式为 EAP 中继模式。

```
[AC] dot1x-access-profile name HCIP-Security
[AC-dot1x-access-profile-HCIP-Security] dot1x authentication-method eap
[AC-dot1x-access-profile-HCIP-Security] quit
```

创建名为“HCIP-Security”的认证模板，并引用 802.1X 接入模板、认证方案和 RADIUS 服务器模板。

```
[AC] authentication-profile name HCIP-Security
[AC-authentication-profile-HCIP-Security] dot1x-access-profile HCIP-Security
[AC-authentication-profile-HCIP-Security] authentication-scheme HCIP-Security
[AC-authentication-profile-HCIP-Security] radius-server t1
[AC-authentication-profile-HCIP-Security] quit
```

创建名为“HCIP-Security”的安全模板，并配置安全策略。

```
[AC] wlan
[AC-wlan-view] security-profile name HCIP-Security
[AC-wlan-sec-prof-HCIP-Security] security wpa-wpa2 dot1x aes
[AC-wlan-sec-prof-HCIP-Security] quit
```

创建名为“HCIP-Security”的 SSID 模板，并配置 SSID 名称为“HCIP-Security”。

```
[AC-wlan-view] ssid-profile name HCIP-Security
[AC-wlan-ssid-prof-HCIP-Security] ssid HCIP-Security
[AC-wlan-ssid-prof-HCIP-Security] quit
```

创建名为“HCIP-Security”的 VAP 模板，配置业务数据转发模式、业务 VLAN，并引用安全模板、认证模板和 SSID 模板。

```
[AC-wlan-view] vap-profile name HCIP-Security
[AC-wlan-vap-prof-HCIP-Security] forward-mode tunnel
[AC-wlan-vap-prof-HCIP-Security] service-vlan vlan-id 4001
[AC-wlan-vap-prof-HCIP-Security] security-profile HCIP-Security
[AC-wlan-vap-prof-HCIP-Security] authentication-profile HCIP-Security
```



```
[AC-wlan-vap-prof-HCIP-Security] ssid-profile HCIP-Security
[AC-wlan-vap-prof-HCIP-Security] quit
```

配置 AP 组引用 VAP 模板，AP 上射频 0 和射频 1 都使用 VAP 模板“HCIP-Security”的配置。

```
[AC-wlan-view] ap-group name ap-group1
[AC-wlan-ap-group-ap-group1] vap-profile HCIP-Security wlan 1 radio 0
[AC-wlan-ap-group-ap-group1] vap-profile HCIP-Security wlan 1 radio 1
[AC-wlan-ap-group-ap-group1] quit
[AC-wlan-view] quit
[AC]
```

配置认证后域的用户组“group1”，只允许用户组成员访问 10.10.10.0/24 网段的网络资源。

```
[AC] acl 3001
[AC-acl-adv-3001] rule 1 permit ip destination 10.10.10.0 0.0.0.255
[AC-acl-adv-3001] rule 2 deny ip destination any
[AC-acl-adv-3001] quit
[AC] user-group group1
[AC-user-group-group1] acl-id 3001
[AC-user-group-group1] quit
```

步骤 6 配置 RADIUS Server

本实验将 iMaster NCE-Campus 作为 RADIUS 服务器，使用租户管理员账号登录 iMaster NCE-Campus 进行配置。

在配置 RADIUS 认证前需要在 iMaster NCE-Campus 上添加 AC 控制器，配置计费 and 授权密钥，该密钥需要与 AC 设备上 RADIUS 服务器模板中配置的密钥保持一致。

在 iMaster NCE-Campus 租户管理界面选择“准入管理 > 准入资源 > 准入设备”，新建准入控制设备 AC，并将计费和授权密钥均配置为“Huawei@123”。

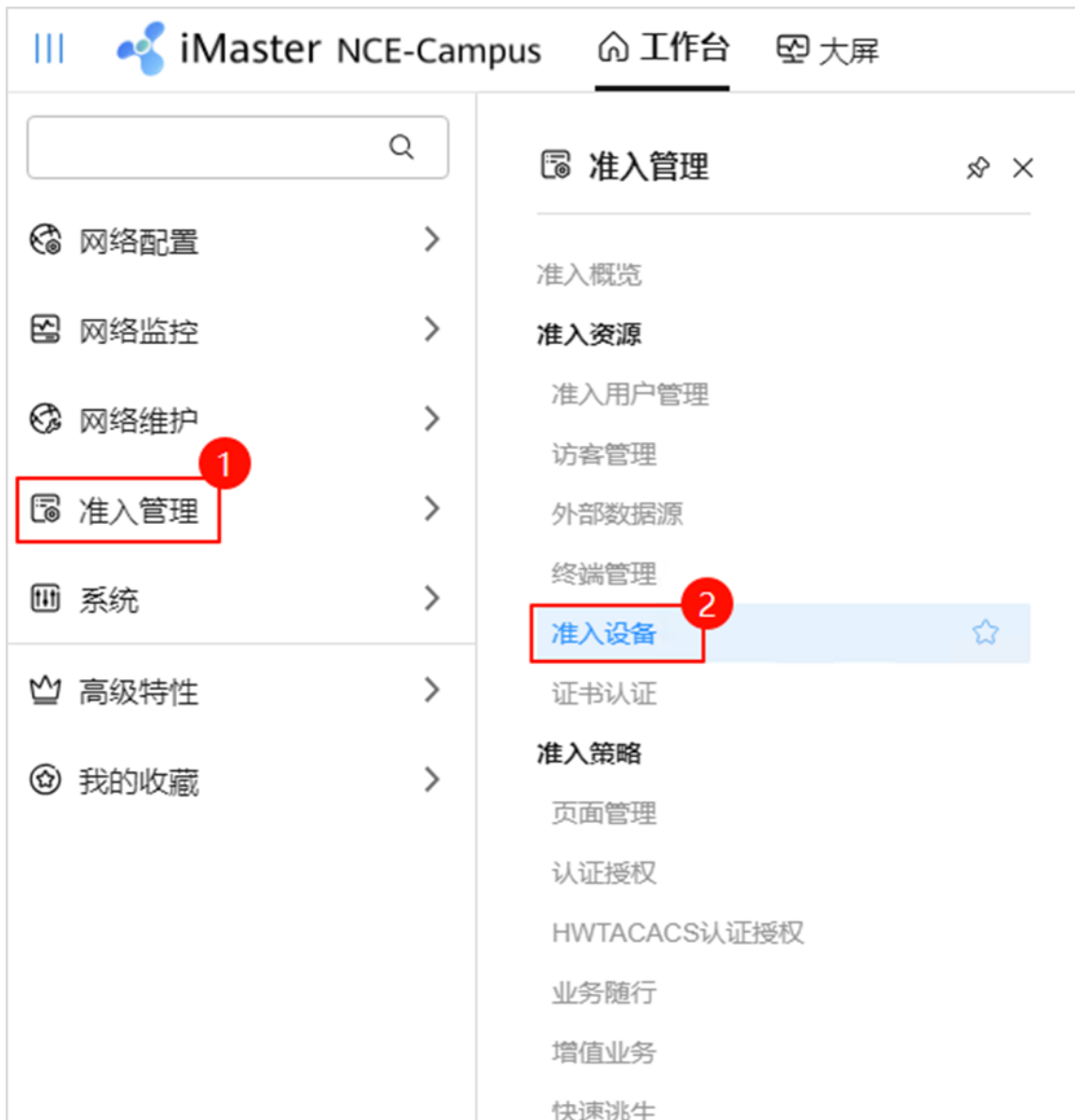


图12-2 进入准入设备资源管理界面



图12-3 进入准入设备创建界面

图12-4 创建准入设备

准入设备创建完成后，效果如下：

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	PortA认证参数	HWTACACS...	准入设备模板	操作
AC		192.168.2.100	准入设备组	--	Huawei NAC	已配置	未配置	未配置	--	编辑

图12-5 准入设备创建完成效果

继续在准入管理界面选择“用户管理 > Guest > 创建”，执行以下操作，创建准入用户账号。



图12-6 进入用户账号创建界面

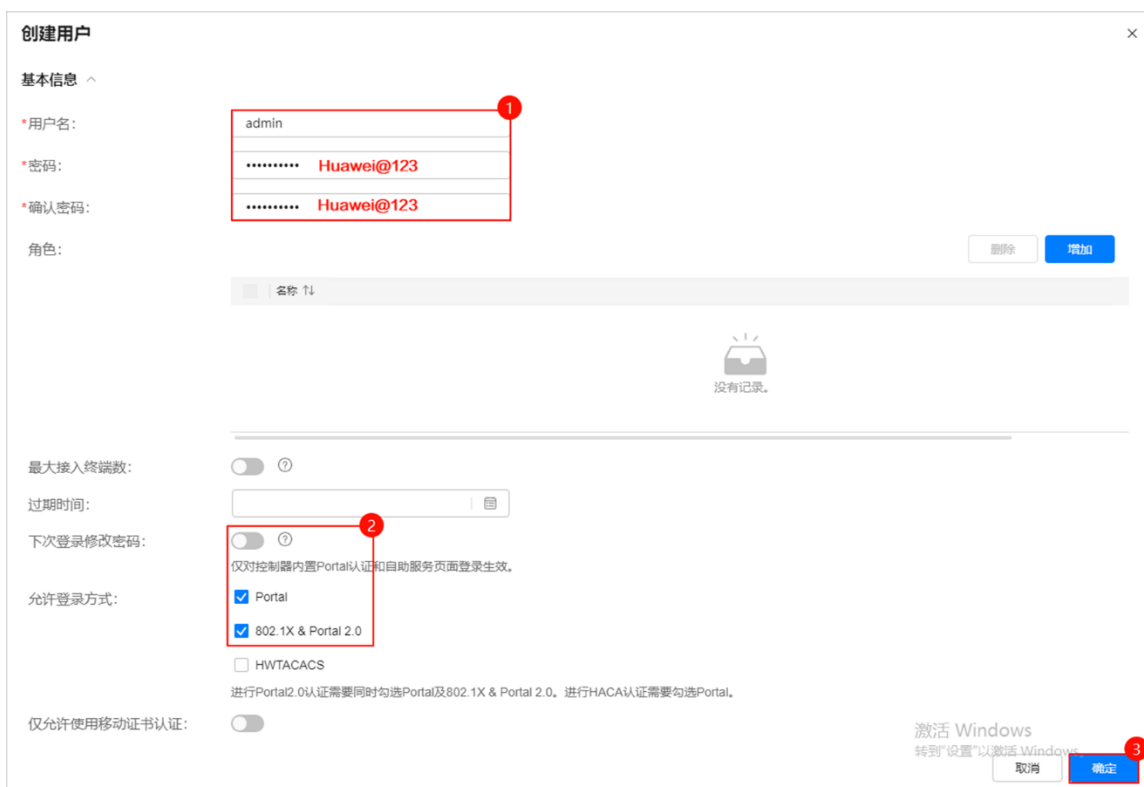


图12-7 创建 802.1X 准入用户账号

在 iMaster NCE-Campus 租户管理界面选择“准入管理 > 准入策略 > 认证授权”，执行以下操作，创建认证与授权规则。

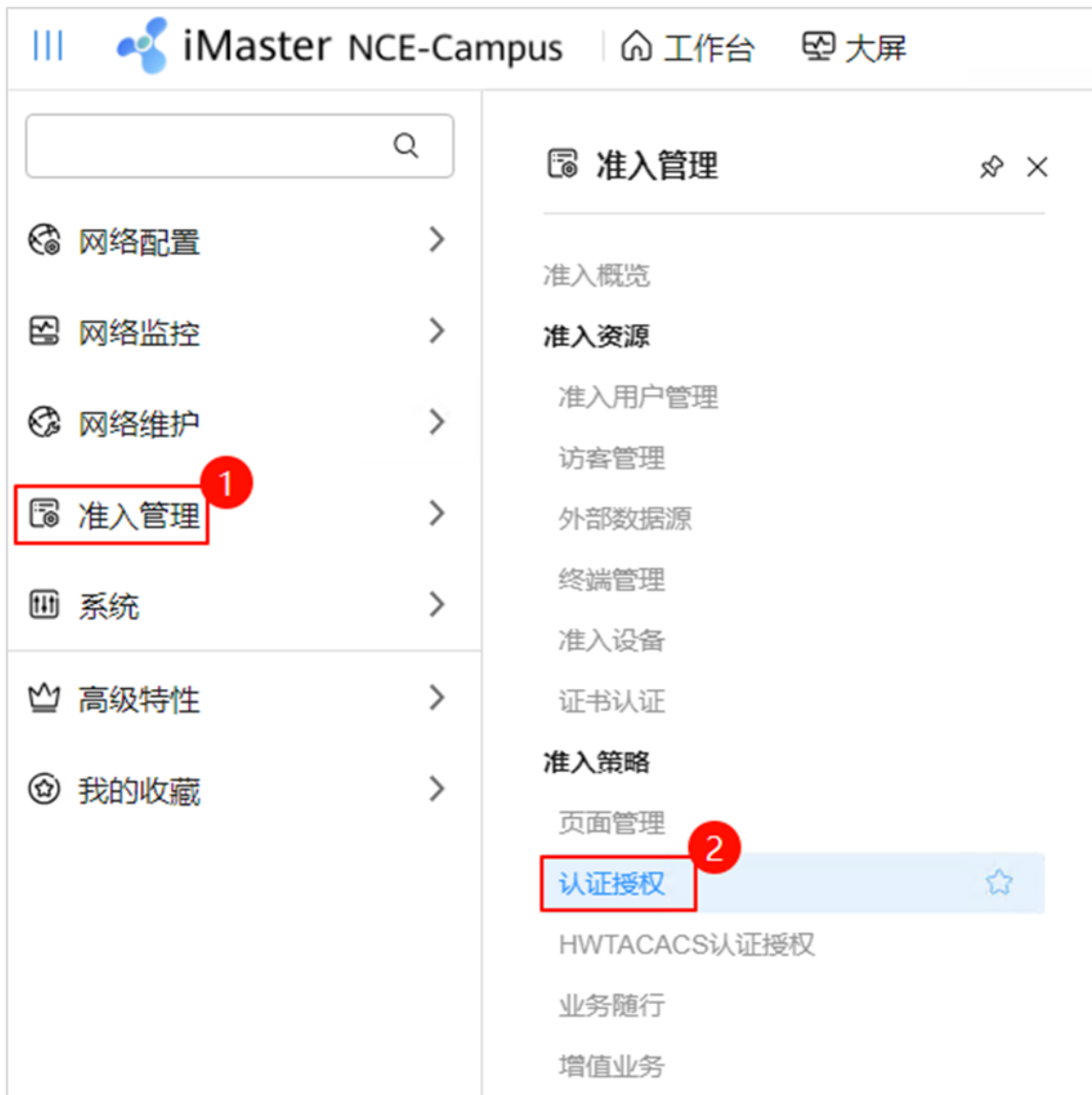


图12-8 进入认证授权管理界面



图12-9 进入认证规则创建界面



准入管理 / 准入策略 / 认证授权

认证规则 | 授权结果 | 授权规则 | 策略元素 | 多级RADIUS中继配置 | 网络接入策略

*名称: 802.1X

描述:

认证方式: 用户接入认证 MAC认证 设备管理认证

启用Portal-HACA协议: ☐

接入方式: WIFI 有线 蜂窝网络

用户信息

用户组信息匹配: ☐

帐号信息匹配: ☒

*帐号:

删除 增加

帐号	帐号类型	用户组	操作

图12-10 创建 802.1X 认证规则（1）



选择帐号

待选

用户组: 所有用户

用户 请输入帐号

☐	帐号类型	帐号	用户组
☒	用户	admin	ROOT\Guest
☐	用户	~anonymous	ROOT

共2条

已选

请输入帐号

没有记录。

>> > < <<

取消 确定

图12-11 创建 802.1X 认证规则（2）



认证信息

RADIUS中继: ☐

接入参数: ☐

*数据源:

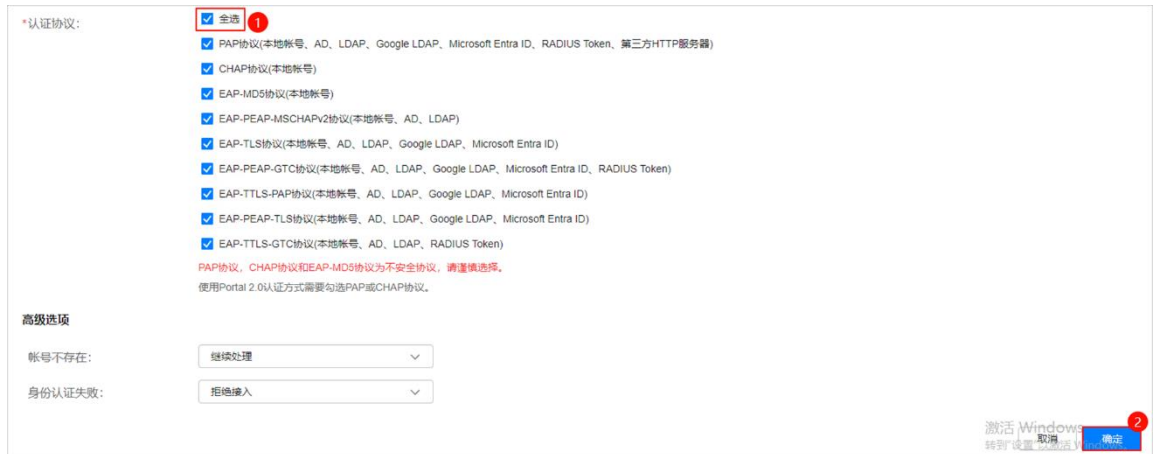
☐	优先级	名称	类型	操作
☒	1	本地数据源	本地数据源	

共1条

删除 增加

20 < 1 >

图12-12 创建 802.1X 认证规则（3）



*认证协议:

- ☒ 全选
- ☒ PAP协议(本地帐号、AD、LDAP、Google LDAP、Microsoft Entra ID、RADIUS Token、第三方HTTP服务器)
- ☒ CHAP协议(本地帐号)
- ☒ EAP-MD5协议(本地帐号)
- ☒ EAP-PEAP-MSCHAPv2协议(本地帐号、AD、LDAP)
- ☒ EAP-TLS协议(本地帐号、AD、LDAP、Google LDAP、Microsoft Entra ID)
- ☒ EAP-PEAP-GTC协议(本地帐号、AD、LDAP、Google LDAP、Microsoft Entra ID、RADIUS Token)
- ☒ EAP-TTLS-PAP协议(本地帐号、AD、LDAP、Google LDAP、Microsoft Entra ID)
- ☒ EAP-PEAP-TLS协议(本地帐号、AD、LDAP、Google LDAP、Microsoft Entra ID)
- ☒ EAP-TTLS-GTC协议(本地帐号、AD、LDAP、RADIUS Token)

PAP协议、CHAP协议和EAP-MD5协议为不安全协议，请谨慎选择。
使用Portal 2.0认证方式需要勾选PAP或CHAP协议。

高级选项

帐号不存在:

身份认证失败:

图12-13 创建 802.1X 认证规则（4）

在认证授权管理界面选择“授权结果 > 创建”，执行以下操作，配置用户授权结果。



准入管理 / 准入策略 / 认证授权

认证规则 | **授权结果** | 授权规则 | 策略元素 | 多级RADIUS中继配置 | 网络接入策略

请输入关键字

名称	业务类型	描述	VIP用户	ACL	IPv6 ACL	授权用户组	安全组	VLAN	下行流量(Mb/s)	上行流量(Mb/s)	DSCP	操作
允许接入	全部	允许接入为...	否	--	--	--	--	--	0	0	--	[编辑]
拒绝接入	全部	拒绝接入为...	否	--	--	--	--	--	0	0	--	[编辑]

共2条

图12-14 进入授权结果创建界面



准入管理 / 准入策略 / 认证授权

认证规则 | **授权结果** | 授权规则 | 策略元素 | 多级RADIUS中继配置 | 网络接入策略

创建

*名称:

配置名称标识:

描述:

策略

设备管理业务: ☐

VIP用户: ☐

ACL:

当配置结果名称长度超过31位时，该属性必填，将使用配置名称标识作为设备上相关属性名称进行配置下发。
仅支持云管设备AP和LSW，不支持非云管准入设备。
支持AP、LSW、AR，仅支持有ACL编号的ACL，不支持编号为编号段的ACL。其中无线用户使用3001~3031，有线用户使用3001~3988。

图12-15 创建用户授权结果（1）

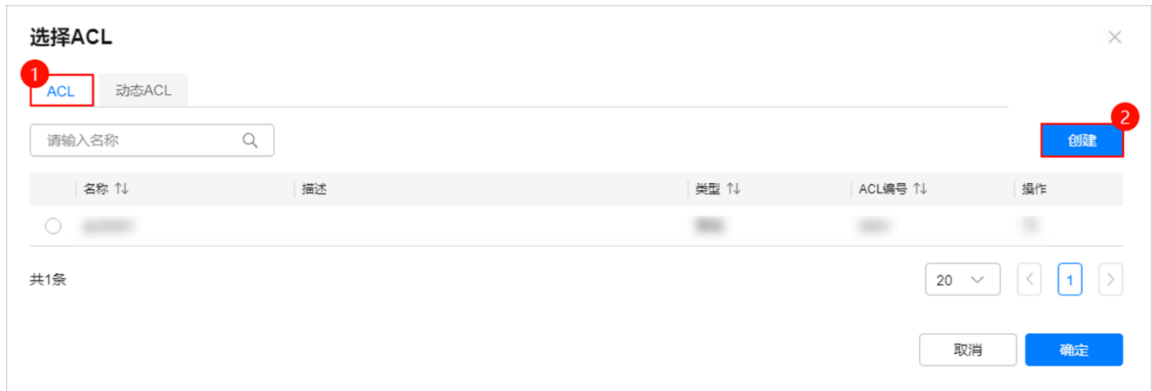


图12-16 创建用户授权结果（2）

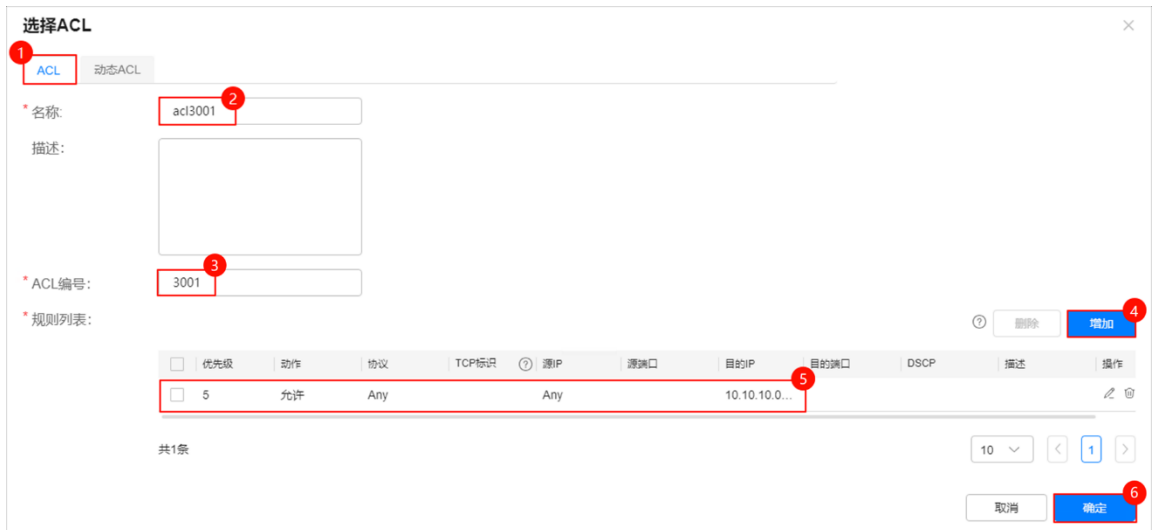


图12-17 创建用户授权结果（3）



图12-18 创建用户授权结果（4）

在认证授权管理界面选择“授权规则 > 创建”，执行以下操作，配置用户授权规则。



图12-19 进入授权规则创建界面



图12-20 创建用户授权规则（1）



图12-21 创建用户授权规则（2）

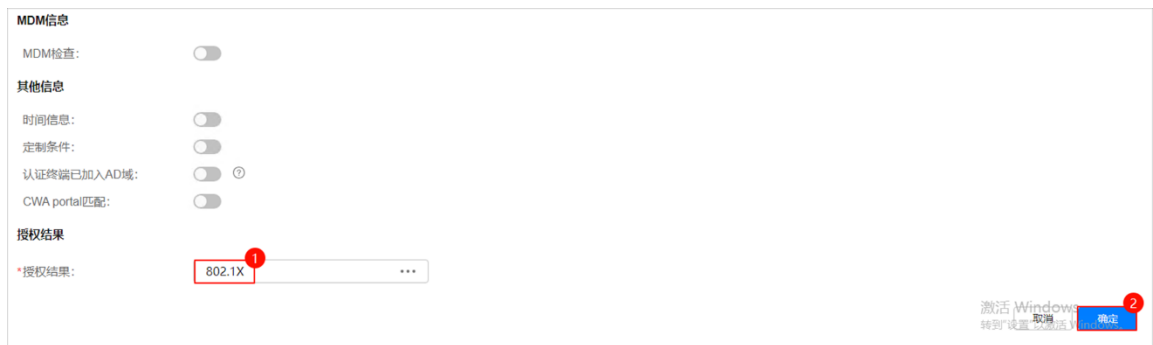


图12-22 创建用户授权规则（3）

继续执行相同操作，创建针对认证点 AC 设备的授权规则（此步骤可选）。



图12-23 创建 AC 设备授权规则（1）

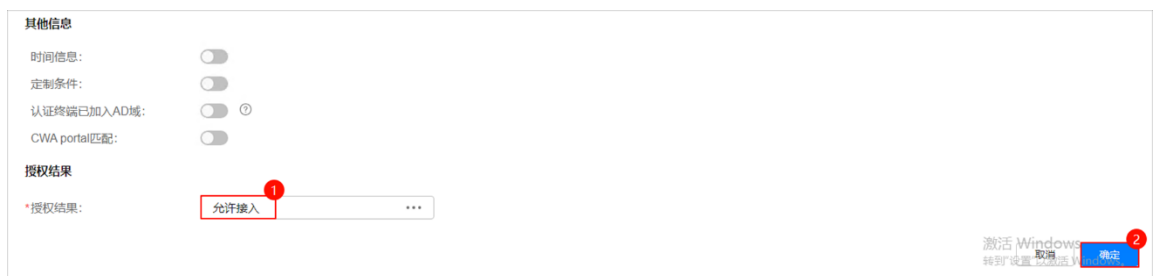


图12-24 创建 AC 设备授权规则（2）

上述授权规则创建完成后效果如下：



图12-25 授权规则创建结果

12.3 结果验证

使用 RDP 登录 PC3，打开“控制面板”，执行以下操作，手动配置无线网络，并设置 802.1X 认证凭据。

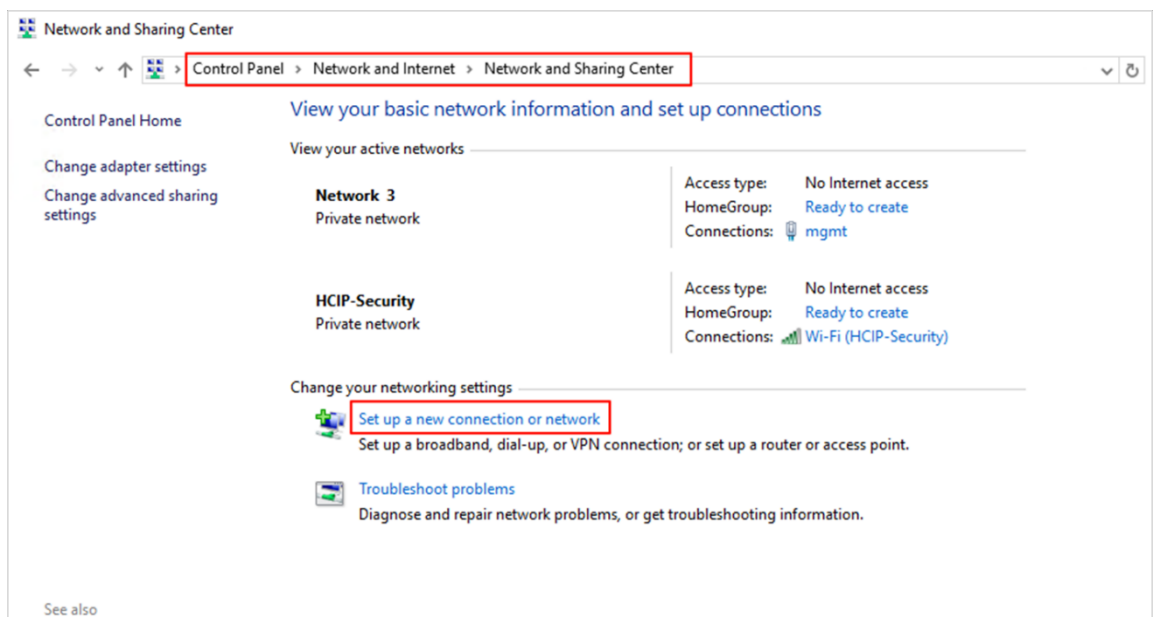


图12-26 设置新的连接或网络

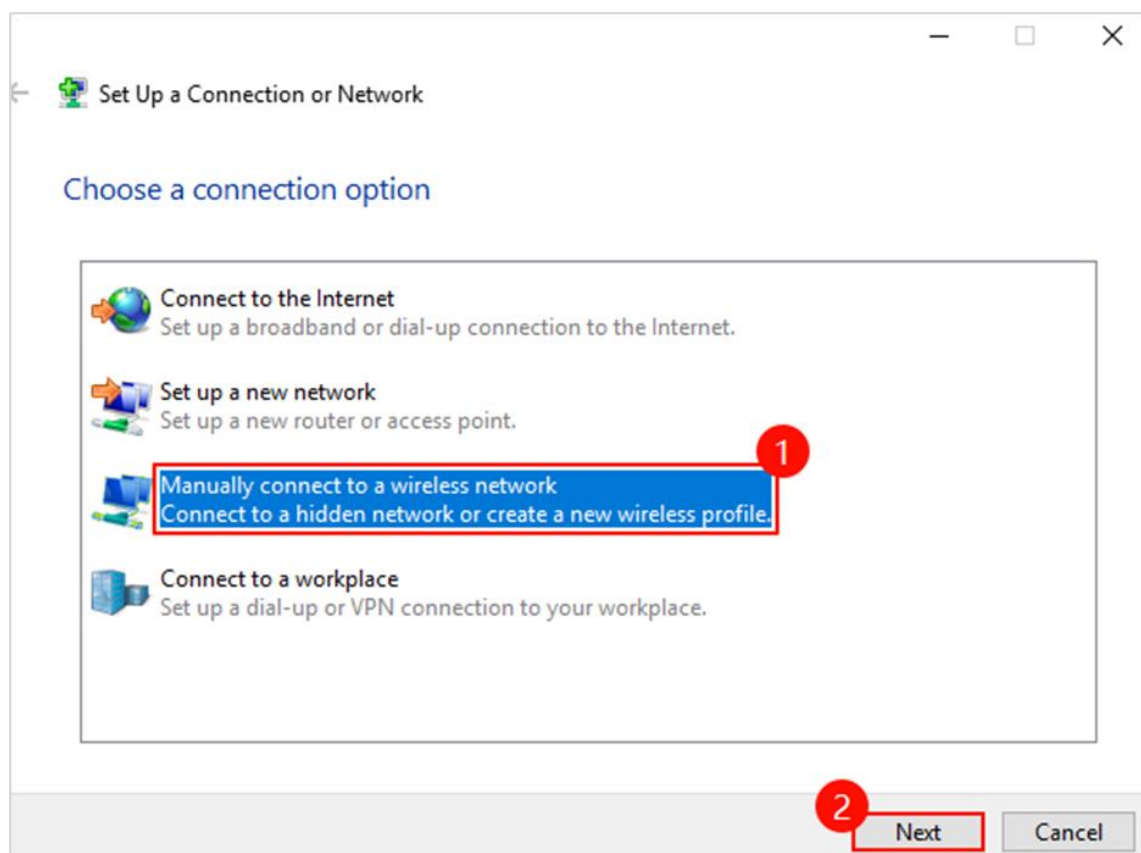
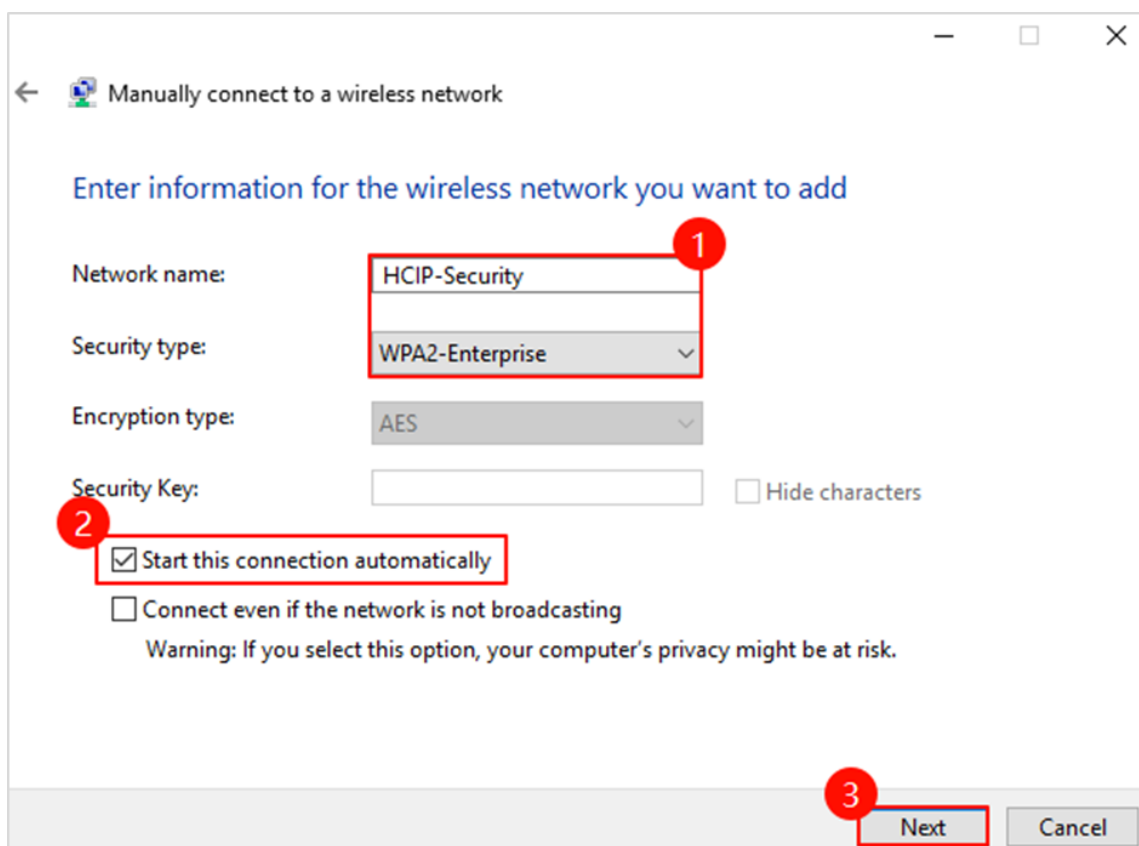


图12-27 手动连接到无线网络



←  Manually connect to a wireless network

Enter information for the wireless network you want to add

Network name:

Security type:

Encryption type:

Security Key: ☐ Hide characters

☒ Start this connection automatically

☐ Connect even if the network is not broadcasting

Warning: If you select this option, your computer's privacy might be at risk.

图12-28 设置无线网络基础参数

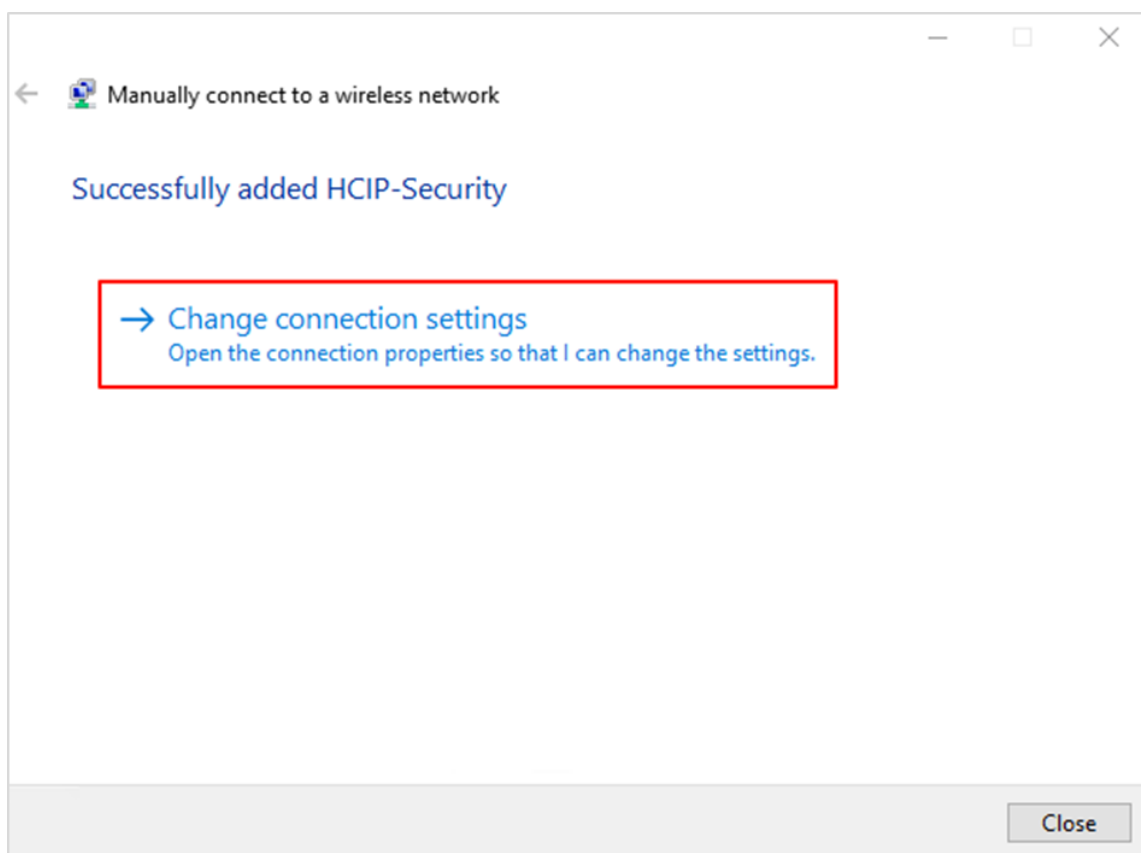


图12-29 更改连接设置

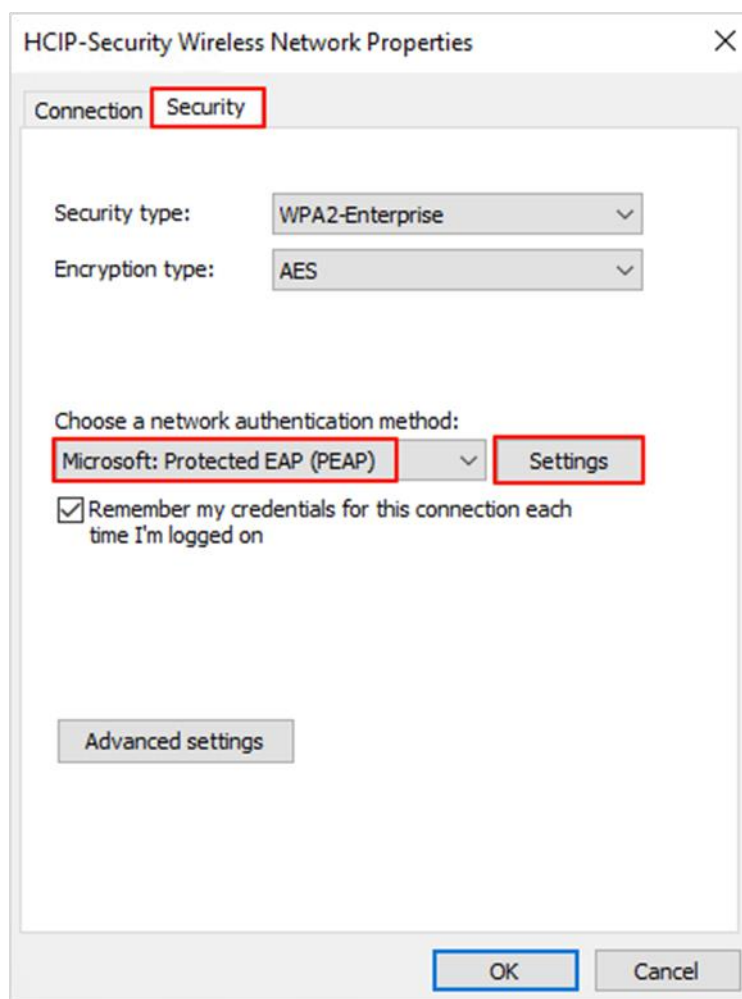


图12-30 设置无线网络安全属性

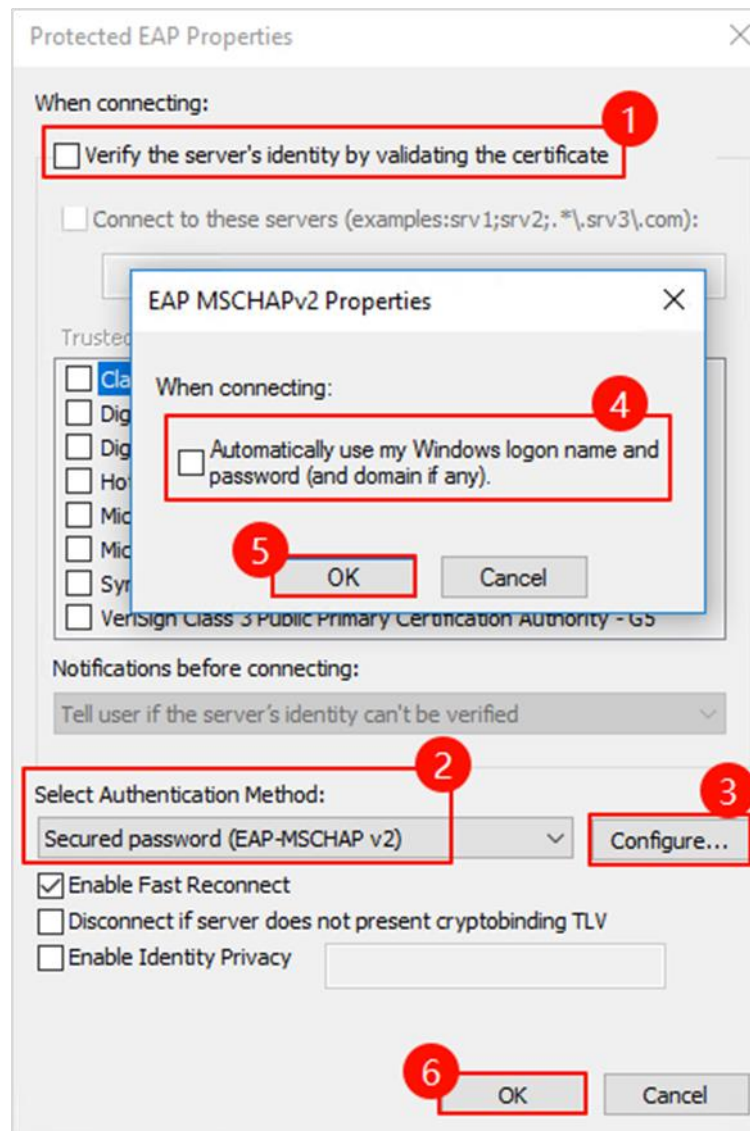


图12-31 设置受保护的 EAP 属性

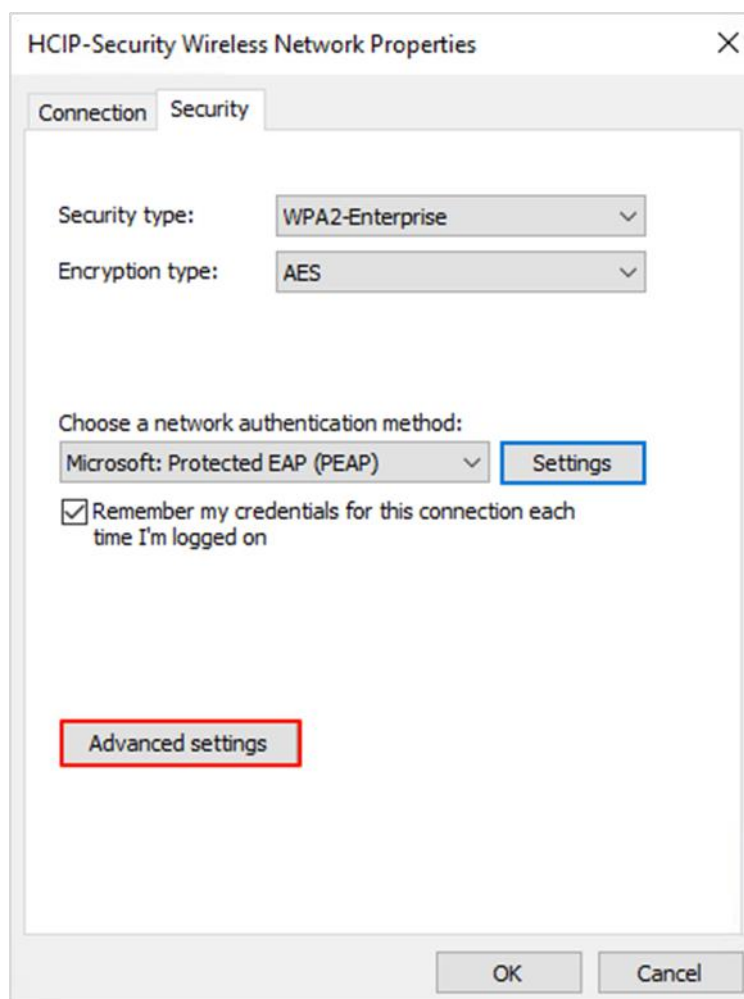


图12-32 进入网络安全属性高级配置界面

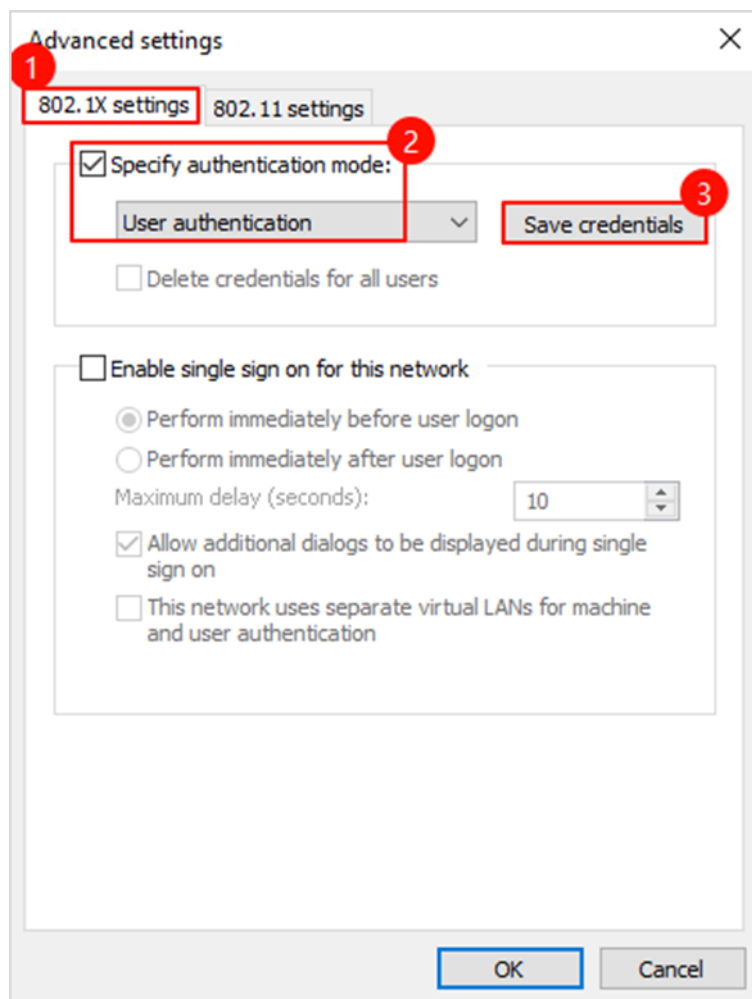


图12-33 指定 802.1X 身份验证模式

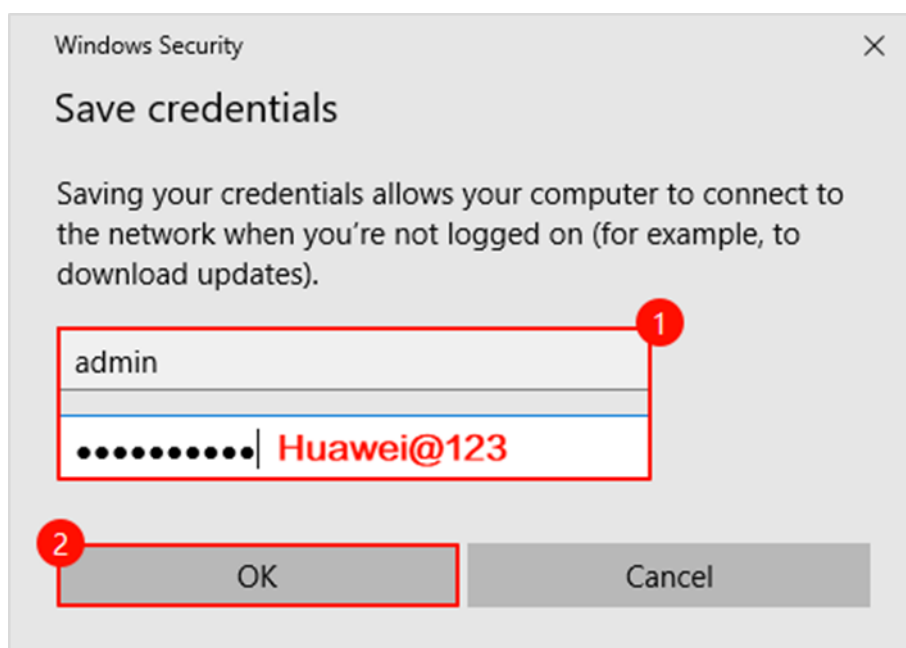


图12-34 设置 802.1X 认证凭据

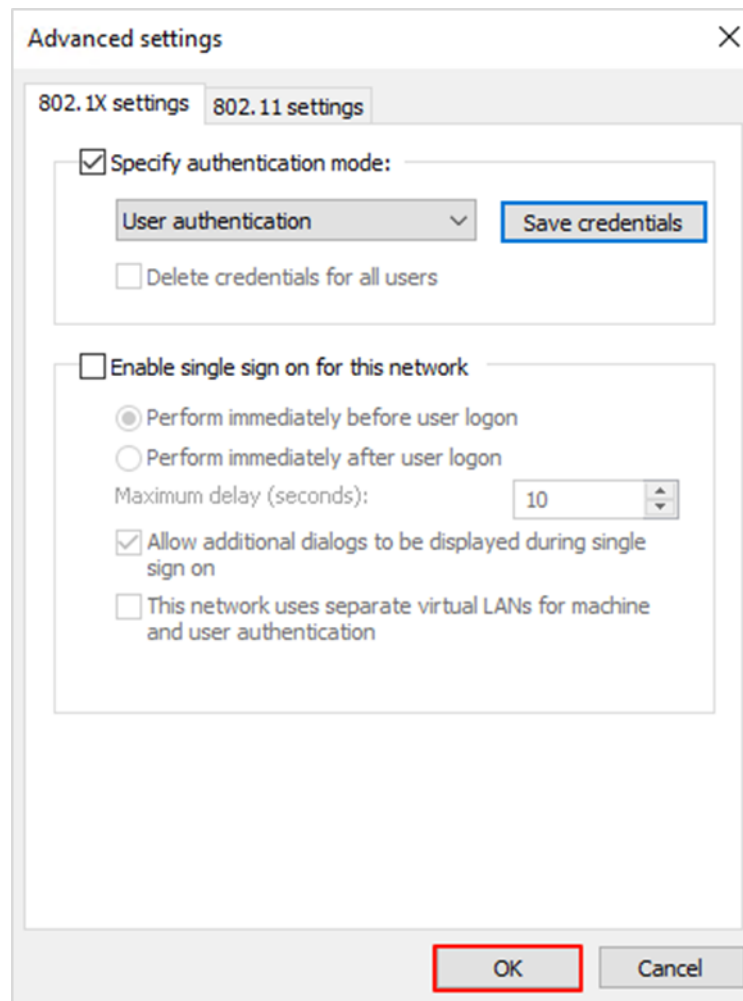


图12-35 完成无线网络安全属性高级设置

执行完上述操作后，点击 PC3 无线网卡，连接“HCIP-Security”无线网络。

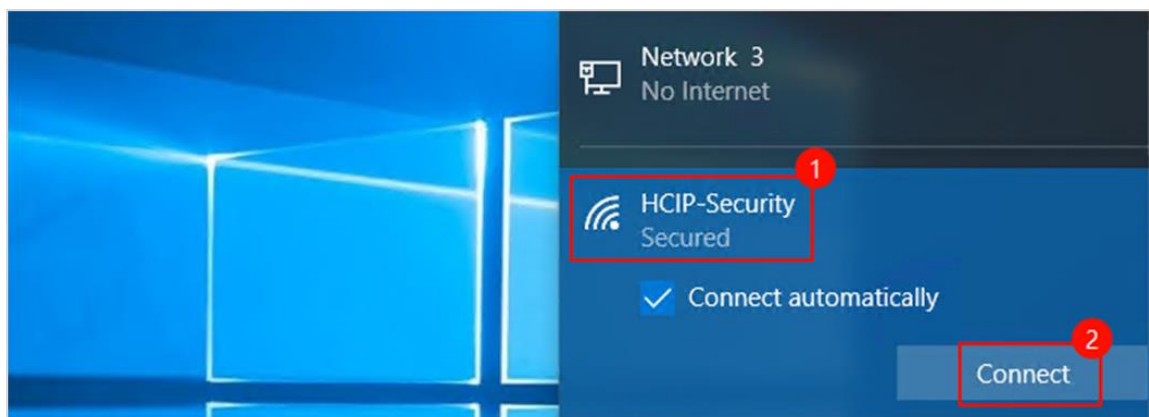


图12-36 连接无线网络

无线网络连接完成后，打开 PC3 网络适配器设置，右键单击“WiFi”网卡，并选择“Status”查看无线网卡连接状态。

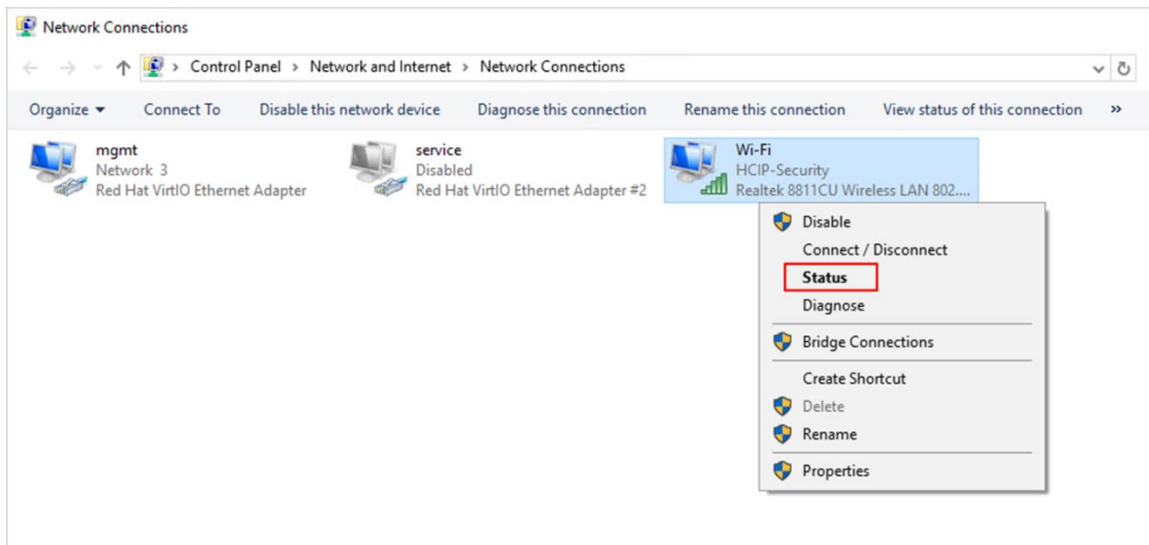


图12-37 查看无线网卡连接状态

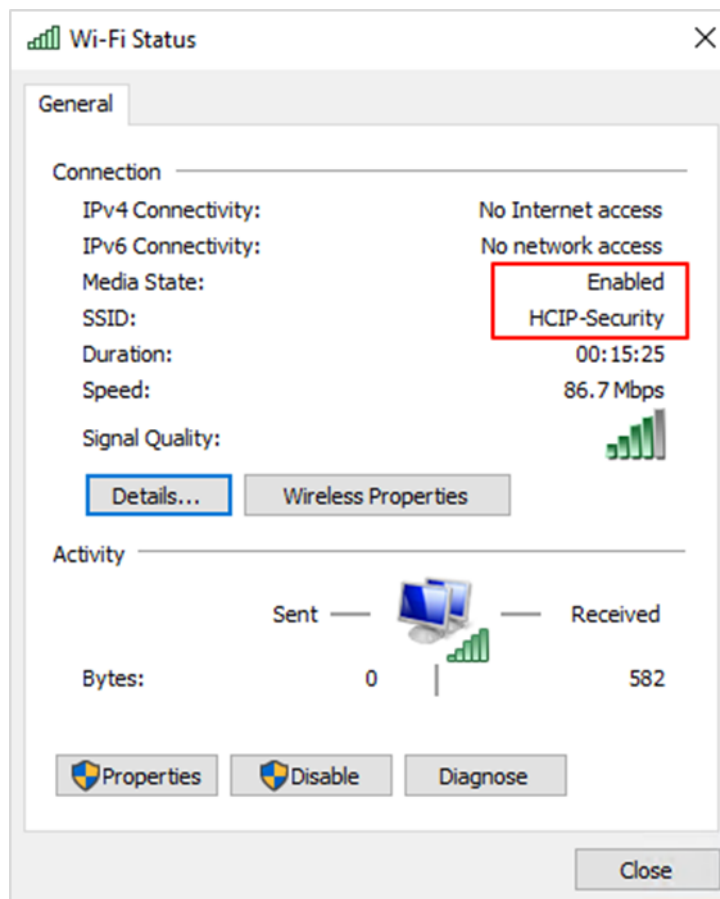


图12-38 无线网络正常连接

使用租户账号登录 iMaster NCE-Campus 管理界面，选择“准入管理 > 准入运维 > 终端认证日志 > RADIUS 上下线日志”，查看用户上线日志。



图12-39 查看用户上线日志

点击用户上线日志最右侧“查看详情”，查看用户上线日志详情。

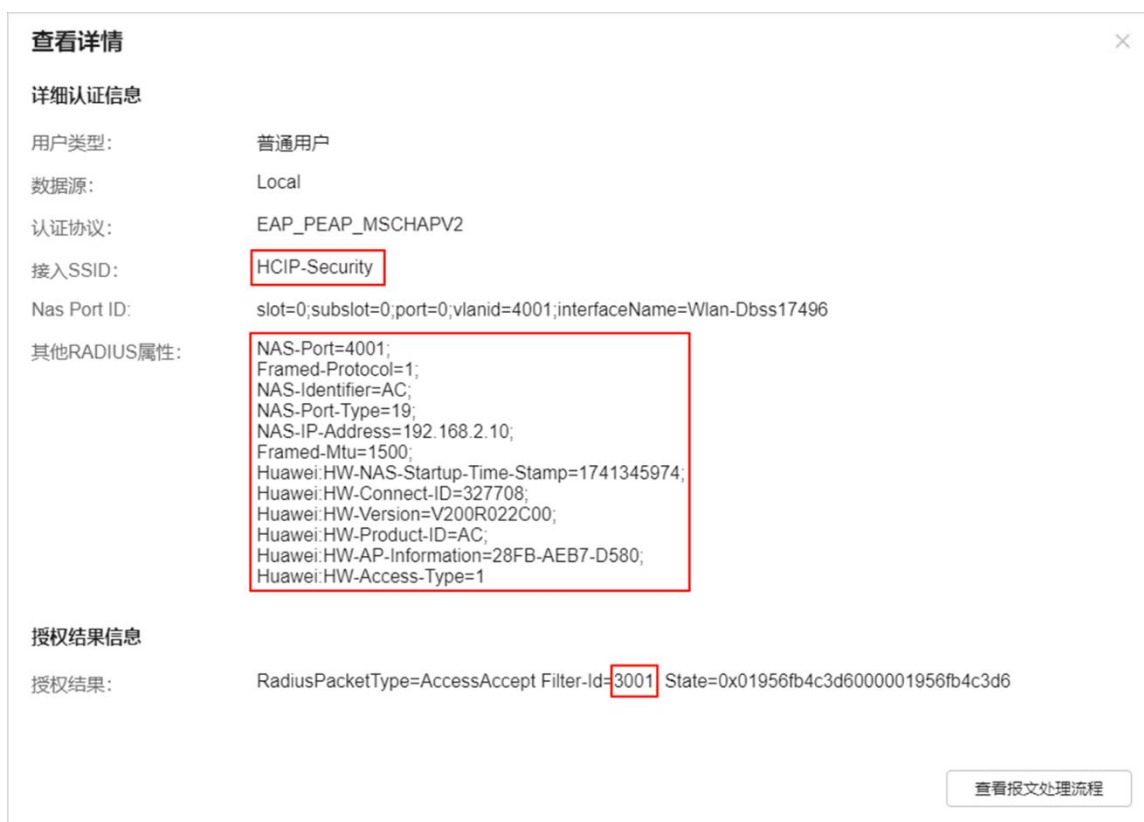


图12-40 查看用户上线日志详情

12.4 配置参考

12.4.1 SW2 配置

```
#
sysname SW2
#
vlan batch 10
```

```
#
interface GigabitEthernet0/0/2
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/17
 port link-type access
 port default vlan 10
#
```

12.4.2 SW3 配置

```
#
sysname SW3
#
vlan batch 10 4000 4001
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 10 4000 4001
#
interface GigabitEthernet0/0/12
 port link-type trunk
 port trunk pvid vlan 4000
 port trunk allow-pass vlan 4000
#
```

12.4.3 FW2 配置

```
#
sysname FW2
#
vlan batch 10
#
interface GE0/0/5
 portswitch
 undo shutdown
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 10
#
interface GE0/0/6
 portswitch
```

```
undo shutdown
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 10
#
firewall zone trust
set priority 85
add interface GE0/0/5
add interface GE0/0/6
#
```

12.4.4 AC 配置

```
#
sysname AC
#
vlan batch 10 4000 to 4001
#
authentication-profile name HCIP-Security
dot1x-access-profile HCIP-Security
authentication-scheme HCIP-Security
radius-server t1
#
radius-server source ip-address 192.168.2.100
#
dhcp enable
#
radius-server template t1
radius-server shared-key cipher %^%#P&81!R"6z-4x~C~knm!Zkbs~@xljSAe/3K+9|i*8%^%#
radius-server authentication 192.168.2.201 1812 weight 80
radius-server accounting 192.168.2.201 1813 weight 80
#
acl number 3001
rule 1 permit ip destination 10.10.10.0 0.0.0.255
rule 2 deny ip
#
user-group group1
acl-id 3001
#
ip pool vlan4000
gateway-list 10.10.1.1
network 10.10.1.0 mask 255.255.255.0
option 43 sub-option 3 ascii 10.10.1.1
#
ip pool vlan4001
gateway-list 10.20.1.1
network 10.20.1.0 mask 255.255.255.0
#
```

```
aaa
 authentication-scheme HCIP-Security
 authentication-mode radius
#
interface Vlanif10
 ip address 192.168.2.100 255.255.255.0
#
interface Vlanif4000
 ip address 10.10.1.1 255.255.255.0
 dhcp select global
#
interface Vlanif4001
 ip address 10.20.1.1 255.255.255.0
 dhcp select global
#
interface GigabitEthernet0/0/2
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 10 4000 to 4001
#
capwap source interface vlanif4000
capwap dtls psk %^%#0!>x<g+._rk[GCUShe(g8nk)PbOuQ1NTz1-Tr=%%^%#
capwap dtls inter-controller psk %^%#qcmB:/J!ABiwjHg@@VMf!eYSj/:z5l`DP7rl"*0%^%#
capwap dtls no-auth enable
#
wlan
 temporary-management psk %^%#~/5'B_l~4M8#xg$(R;z7~p[P(#zzc>&V*%'6[Tn(%^%#
 ap username admin password cipher %^%#Kc98l|*gB-S5ATHdbGK@c$3x4!O<8.OKsA@nnT~K%^%#
 traffic-profile name default
 security-profile name default
 security-profile name default-wds
 security-profile name default-mesh
 security-profile name HCIP-Security
 security wpa-wpa2 dot1x aes
 ssid-profile name default
 ssid-profile name HCIP-Security
 ssid HCIP-Security
 vap-profile name HCIP-Security
 forward-mode tunnel
 service-vlan vlan-id 4001
 ssid-profile HCIP-Security
 security-profile HCIP-Security
 authentication-profile HCIP-Security
 regulatory-domain-profile name domain1
 dca-channel 5g bandwidth 20mhz
 ap-group name ap-group1
 regulatory-domain-profile domain1
 radio 0
```



```
vap-profile HCIP-Security wlan 1
radio 1
vap-profile HCIP-Security wlan 1
ap-id 0 type-id 187 ap-mac 28fb-aeb7-d580 ap-sn 2102354MXJ10Q3100287
ap-group ap-group1
ap-id 1 ap-mac 28fb-aeb7-d581
provision-ap
#
dot1x-access-profile name HCIP-Security
#
return
```

12.5 思考题

同一个 RADIUS 服务器同时配置在多个 RADIUS 服务器模板下时，有什么注意事项？

参考答案：

- 1.如果不同 RADIUS 服务器模板下的共享密钥不同，则需要在每个 RADIUS 服务器模板视图下分别配置。
- 2.如果所有 RADIUS 服务器模板下的共享密钥相同，则可以在系统视图下配置。配置命令为 radius-server ip-address { ipv4-address | ipv6-address } shared-key cipher key-string。
- 3.RADIUS 服务器模板视图下和系统视图下都配置 RADIUS 服务器的密钥时，系统视图下配置的 RADIUS 服务器密钥优先生效。

13 Portal 认证实验

13.1 实验介绍

13.1.1 关于本实验

某企业部署了 WLAN 为员工提供无线办公环境，出于安全考虑，企业计划使用 Portal 方式对用户执行准入认证，且由于员工人数较多，需要使用 RADIUS 服务器（iMaster NCE-Campus）统一管理员工的账号和权限。

13.1.2 实验目的

- 掌握无线 AC 基础配置。
- 掌握 WLAN 模板配置。
- 掌握 Portal 认证配置。

13.1.3 实验组网介绍

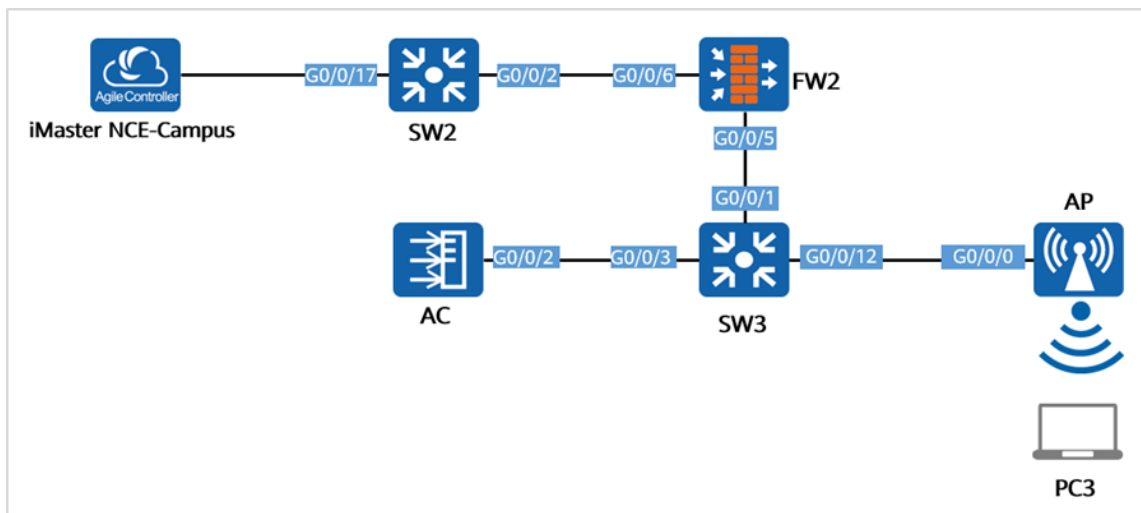


图13-1 Portal 认证实验拓扑

- 1.使用外置电源给 AP 供电，iMaster NCE-Campus 作为 RADIUS 服务器。
- 2.AP 与 AC 之间为二层组网，AP 和终端的 DHCP 服务器均部署在 AC 上。
- 3.AC 与 RADIUS 服务器之间为二层组网，无线终端的 AAA 认证由 RADIUS 服务器执行。

4.用户连接“HCIP_Sec_Portal”无线网络时，需要通过 Portal 认证，Portal 页面由 RADIUS 服务器推送。

13.1.4 实验规划

表13-1 设备接口规划表

设备	接口	接口性质	接口信息	说明
SW2	G0/0/2	Trunk	PVID: 1 Allow-pass VLAN: 10	与FW2互连
	G0/0/17	Access	PVID: 10	连接iMaster NCE-Campus
SW3	G0/0/1	Trunk	PVID: 1 Allow-pass VLAN: 10	与FW2互连
	G0/0/3	Trunk	PVID: 1 Allow-pass VLAN: 10, 4000, 4001	与AC互连
	G0/0/12	Trunk	PVID: 4000 Allow-pass VLAN: 4000	与AP互连
FW2	GE0/0/5	Trunk	PVID: 1 Allow-pass VLAN: 10	与SW3互连
	GE0/0/6	Trunk	PVID: 1 Allow-pass VLAN: 10	与SW2互连
AC	GE0/0/2	Trunk	PVID: 1 Allow-pass VLAN: 10, 4000, 4001	与SW3互连
AP	GE0/0/0	/	保持默认无需配置	与SW3互连
iMaster NCE-Campus	Ethernet0	网卡	192.168.2.201/24	服务器接口IP

13.2 实验任务配置

13.2.1 配置思路

- 1.底层网络配置，实现底层网络互通。
- 2.配置 AC 的 DHCP Server 功能，为 AP 分配管理地址，为无线终端分配业务地址。
- 3.配置 AP 上线。
- 4.在 AC 上配置对接 RADIUS 认证服务器的参数。
- 5.在 AC 上配置 SSID 等模板及 WLAN Portal 认证相关配置。
- 6.在 iMaster 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。

13.2.2 配置步骤

步骤 1 设备基础配置

按照“表 13-1”数据规划，完成 AC、SW3、AP 之间二层网络的配置，完成 SW3、FW2、SW2 之间的二层网络的配置。

配置 AC 的 GigabitEthernet0/0/2 接口。

```
[AC] vlan batch 10 4000 4001
[AC] interface GigabitEthernet0/0/2
[AC-GigabitEthernet0/0/2] port link-type trunk
[AC-GigabitEthernet0/0/2] undo port trunk allow-pass vlan 1
[AC-GigabitEthernet0/0/2] port trunk allow-pass vlan 10 4000 4001
[AC-GigabitEthernet0/0/2] quit
```

配置 SW3 的 G0/0/3、G0/0/12 和 G0/0/1 接口。

```
[SW3] vlan batch 10 4000 4001
[SW3] interface GigabitEthernet0/0/3
[SW3-G0/0/3] port link-type trunk
[SW3-G0/0/3] port trunk allow-pass vlan 10 4000 4001
[SW3-G0/0/3] quit
[SW3] interface GigabitEthernet0/0/12
[SW3-G0/0/12] port link-type trunk
[SW3-G0/0/12] port trunk pvid vlan 4000
[SW3-G0/0/12] port trunk allow-pass vlan 4000
[SW3-G0/0/12] quit
[SW3] interface GigabitEthernet0/0/1
[SW3-G0/0/1] port link-type trunk
[SW3-G0/0/1] port trunk allow-pass vlan 10
[SW3-G0/0/1] quit
```

配置 FW2 的 GE0/0/5 和 GE0/0/6 接口，并将接口加入安全区域。

```
[FW2] vlan 10
```

```
[FW2] interface GE0/0/5
[FW2-GE0/0/5] portswitch
[FW2-GE0/0/5] port link-type trunk
[FW2-GE0/0/5] undo port trunk allow-pass vlan 1
[FW2-GE0/0/5] port trunk allow-pass vlan 10
[FW2-GE0/0/5] quit
[FW2] interface GE0/0/6
[FW2-GE0/0/6] portswitch
[FW2-GE0/0/6] port link-type trunk
[FW2-GE0/0/6] undo port trunk allow-pass vlan 1
[FW2-GE0/0/6] port trunk allow-pass vlan 10
[FW2-GE0/0/6] quit
[FW2] firewall zone trust
[FW2-zone-trust] add interface GE0/0/5
[FW2-zone-trust] add interface GE0/0/6
[FW2-zone-trust] quit
```

配置 SW2 的 G0/0/2、G0/0/17 接口。

```
[SW2] vlan 10
[SW2] interface GigabitEthernet 0/0/2
[SW2-G0/0/2] port link-type trunk
[SW2-G0/0/2] undo port trunk allow-pass vlan 1
[SW2-G0/0/2] port trunk allow-pass vlan 10
[SW2-G0/0/2] quit
[SW2] interface GigabitEthernet 0/0/17
[SW2-G0/0/17] port link-type access
[SW2-G0/0/17] port default vlan 10
[SW2-G0/0/17] quit
```

步骤 2 配置 DHCP

AC 需要为 AP 提供管理地址，同时为无线用户（PC3）提供业务地址，本实验配置 VLAN4000 为管理网段，配置 VLAN4001 为业务网段。

开启 AC 的 DHCP 功能。

```
[AC] dhcp enable
```

配置 AP 管理网段的网关，并选择全局 DHCP 地址池。

```
[AC] interface vlanif4000
[AC-VLANIF4000] ip address 10.10.1.1 255.255.255.0
[AC-VLANIF4000] dhcp select global
[AC-VLANIF4000] quit
```

配置 AP 管理网段的 DHCP 地址池。

```
[AC] ip pool vlan4000
[AC-ip-pool-vlan4000] gateway-list 10.10.1.1
[AC-ip-pool-vlan4000] network 10.10.1.0 mask 255.255.255.0
[AC-ip-pool-vlan4000] option 43 sub-option 3 ascii 10.10.1.1
[AC-ip-pool-vlan4000] quit
```

配置无线业务网段的网关，并选择全局 DHCP 地址池。

```
[AC] interface vlanif4001
[AC-VLANIF4001] ip address 10.20.1.1 255.255.255.0
[AC-VLANIF4001] dhcp select global
[AC-VLANIF4001] quit
```

配置无线用户网段的 DHCP 全局地址池。

```
[AC] ip pool vlan4001
[AC-ip-pool-vlan4001] gateway-list 10.20.1.1
[AC-ip-pool-vlan4001] network 10.20.1.0 mask 255.255.255.0
[AC-ip-pool-vlan4001] quit
```

配置无线用户认证地址，与 RADIUS 认证服务器（iMaster NCE-Campus）通信。

```
[AC] interface vlanif10
[AC-VLANIF10] ip address 192.168.2.100 255.255.255.0
[AC-VLANIF10] quit
```

步骤 3 配置 AP 上线

创建 AP 组，用于将相同配置的 AP 都加入同一 AP 组中，并配置免认证。

```
[AC] wlan
[AC-wlan-view] ap-group name ap-group1
[AC-wlan-ap-group-ap-group1] quit
[AC-wlan-view] ap auth-mode no-auth
[AC-wlan-view] ap-mac 28fb-aeb7-d580 //MAC 地址并非固定，需要基于实验环境中 AP 的真实 MAC 调整
[AC-wlan-ap-0] ap-group ap-group1
```

创建域管理模板，在域管理模板下配置 AC 的国家码并在 AP 组下引用域管理模板。

```
[AC-wlan-view] regulatory-domain-profile name domain1
[AC-wlan-regulate-domain-domain1] country-code cn
Info: The current country code is same with the input country code.
[AC-wlan-regulate-domain-domain1] quit
[AC-wlan-view] ap-group name ap-group1
[AC-wlan-ap-group-ap-group1] regulatory-domain-profile domain1
Warning: This configuration change will clear the channel and power configurations of radios, and may
restart APs. Continue?[Y/N]:y
[AC-wlan-ap-group-ap-group1] quit
[AC-wlan-view] quit
[AC]
```

配置 AC 的源接口。

```
[AC] capwap source interface vlanif4000
Set the DTLS PSK(contains 8-32 plain-text characters, or 48 or 68 cipher-text characters that must be a
combination of at least two
of the following: lowercase letters a to z, uppercase letters A to Z, digits, and special characters): //配
置 DTLS 加密的 PSK
Confirm PSK: //重复输入 DTLS 加密的 PSK，两次输入保持一致
Configuring the new PSK, waiting...
```

```

Info: Deliver DTLS PSK to devices using CAPWAP connections. It may take a few minutes.
-----
CAPWAP DTLS PSK deliver result
Deliver Number : 0
Success Number : 0
Failed Number : 0
-----done.
Set the DTLS inter-controller PSK(contains 8-32 plain-text characters, or 48 or 68 cipher-text characters
that must be a combination
of at least two of the following: lowercase letters a to z, uppercase letters A to Z, digits, and special
characters): //配置 AC 间 DTLS 加密的 PSK
Confirm PSK: //重复输入 AC 间 DTLS 加密的 PSK，两次输入保持一致
Configuring the new PSK, waiting.....done.
Set the user name for FIT APs(The value is a string of 4 to 31 characters, which can contain letters,
underscores, and digits, and m
ust start with a letter):admin //统一配置 FIT AP 的登录用户名
Set the password for FIT APs(plain-text password of 8-128 characters or cipher-text password of 48-188
characters that must be a com
bination of at least three of the following: lowercase letters a to z, uppercase letters A to Z, digits, and
special characters): //统一配置 FIT AP 的登录密码
Confirm password: //重复输入 FIT AP 的登录密码，两次输入保持一致
Set the global temporary-management psk(contains 8-63 plain-text characters, or 48-108 cipher-text
characters that must be a combina
tion of at least two of the following: lowercase letters a to z, uppercase letters A to Z, digits, and special
characters): //配置全局离线管理 VAP 的接入密码
Confirm PSK: //重复输入全局离线管理 VAP 的接入密码，两次输入保持一致
Warning: Ensure that the management VLAN and service VLAN are different. Otherwise, services may be
interrupted.
Warning: Before an added device goes online for the first time, enable DTLS no-auth if it runs a version
earlier than V200R021C00 or
enable DTLS certificate-mandatory-match if it runs V200R021C00 or later.
[AC] capwap dtls no-auth enable //V200R021C00 版本开始，AC 默认开启 CAPWAP 控制隧道的 DTLS 加
密功能。添加 AP 时 AP 会上线失败，此时需要先开启 CAPWAP DTLS 不认证方式让 AP 上线，以便 AP 获取
安全凭证，AP 上线后应及时关闭该功能（undo capwap dtls no-auth enable），避免未授权 AP 上线
Warning: This operation allows for device access in non-DTLS encryption mode even when DTLS is
enabled and brings security risks. Af
ter the device goes online for the first time, disable this function to prevent security risks.
Continue?[Y/N]:y
[AC]

```

执行命令 display ap all 查看到 AP 的“State”字段为“nor”时，表示 AP 正常上线。

```

[AC-wlan-ap-0]display ap all
Total AP information:
nor : normal [1]
ExtraInfo : Extra information
-----
ID MAC Name Group IP Type State STA
Uptime ExtraInfo
-----

```

```
0      28fb-aeb7-d580 28fb-aeb7-d580 ap-group1 10.10.1.187 AirEngine5761-12 nor    0    55    -
-----
Total: 1
```

步骤 4 RADIUS 服务器对接参数配置

在 AC 上创建 RADIUS 服务器模板。

```
[AC] radius-server template t1
[AC-radius-wlan-t1] radius-server authentication 192.168.2.201 1812
[AC-radius-wlan-t1] radius-server accounting 192.168.2.201 1813
[AC-radius-wlan-t1] radius-server shared-key cipher Huawei@123
[AC-radius-wlan-t1] quit
```

在 AC 上配置与 RADIUS 服务器通信的源地址为 192.168.2.100。

```
[AC] radius-server source ip-address 192.168.2.100
```

说明：以上四个配置步骤与“实验 12”完全相同，可直接复用，无需二次配置。

步骤 5 配置认证与授权模板

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。

```
[AC]aaa
[AC-aaa]authentication-scheme radius
[AC-aaa-authen-radius]authentication-mode radius
[AC-aaa-authen-radius]quit
[AC-aaa]accounting-scheme radius
Info: Create a new accounting scheme.
[AC-aaa-accounting-radius]accounting-mode radius
[AC-aaa-accounting-radius]accounting realtime 15
[AC-aaa-accounting-radius]quit
[AC-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.
[AC-aaa-domain-default] authentication-scheme radius
[AC-aaa-domain-default] accounting-scheme radius
[AC-aaa-domain-default] radius-server t1
[AC-aaa-domain-default]quit
[AC-aaa]quit
[AC]domain default
Info: Set the default domain success.
```

步骤 6 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。

```
[AC]url-template name nce
[AC-url-template-nce] url https://192.168.2.201:19008/portal
Info: Ensure that the DNS and Portal server addresses are reachable.
```



```
[AC-url-template-nce] url-parameter device-ip ac-ip redirect-url redirect-url ssid ssid user-ipaddress
uaddress user-mac umac
[AC-url-template-nce] url-parameter set device-ip 192.168.2.100
[AC-url-template-nce] quit
[AC]web-auth-server 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
[AC]
```

步骤 7 配置 Portal 服务器模板

在 AC 设备上配置 Portal 服务器模板。

```
[AC]web-auth-server portal
[AC-web-auth-server-portal]server-ip 192.168.2.201
[AC-web-auth-server-portal]port 50100
[AC-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.
[AC-web-auth-server-portal]url-template nce
[AC-web-auth-server-portal]source-ip 192.168.2.100
[AC-web-auth-server-portal]portal-access-profile name portal
[AC-portal-access-profile-portal] web-auth-server portal direct
[AC-portal-access-profile-portal] quit
[AC]
```

步骤 8 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。

```
[AC]free-rule-template name free_rule
[AC-free-rule-free_rule]free-rule 1 destination ip 192.168.2.201 mask 255.255.255.255
[AC-free-rule-free_rule]quit
[AC]
```

步骤 9 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。

```
[AC]authentication-profile name auth_portal
Authentication profile auth_portal : done.
[AC-authentication-profile-auth_portal]portal-access-profile portal
Info: This operation may take a few minutes, please wait...
Authentication profile auth_portal : done.
[AC-authentication-profile-auth_portal]free-rule-template free_rule
[AC-authentication-profile-auth_portal]access-domain default
[AC-authentication-profile-auth_portal]quit
[AC]
```

步骤 10 配置无线业务

创建名为“security_portal”的安全模板，并配置安全策略。

```
[AC-wlan-view]security-profile name security_portal
[AC-wlan-sec-prof-security_portal]security open
[AC-wlan-sec-prof-security_portal]quit
```

创建 SSID 模板，并配置 SSID 名称。

```
[AC-wlan-view]ssid-profile name HCIP_Sec_Portal
[AC-wlan-ssid-prof-HCIP_Sec_Portal]ssid HCIP_Sec_Portal
Info: This operation may take a few seconds, please wait.done.
[AC-wlan-ssid-prof-HCIP_Sec_Portal]quit
[AC-wlan-view]
```

创建 VAP 模板，配置业务数据转发模式、业务 VLAN，并引用安全模板、认证模板和 SSID 模板。

```
[AC-wlan-view]vap-profile name HCIP_Sec_Portal
[AC-wlan-vap-prof-HCIP_Sec_Portal]forward-mode tunnel
Info: This operation may take a few seconds, please wait.done.
[AC-wlan-vap-prof-HCIP_Sec_Portal]service-vlan vlan-id 4001
Info: This operation may take a few seconds, please wait.done.
[AC-wlan-vap-prof-HCIP_Sec_Portal]ssid-profile HCIP_Sec_Portal
Info: This operation may take a few seconds, please wait.done.
[AC-wlan-vap-prof-HCIP_Sec_Portal]security-profile security_portal
Info: This operation may take a few seconds, please wait.done.
[AC-wlan-vap-prof-HCIP_Sec_Portal]authentication-profile auth_portal
Info: This operation may take a few seconds, please wait.done.
[AC-wlan-vap-prof-HCIP_Sec_Portal]quit
```

配置 AP 组引用 VAP 模板，AP 上射频 0 和射频 1 都使用新建的 VAP 模板。

```
[AC-wlan-view]ap-group name ap-group1
[AC-wlan-ap-group-ap-group1] radio 0
[AC-wlan-group-radio-ap-group1/0] vap-profile HCIP_Sec_Portal wlan 3
Info: This operation may take a few seconds, please wait.done.
[AC-wlan-group-radio-ap-group1/0] radio 1
[AC-wlan-group-radio-ap-group1/1] vap-profile HCIP_Sec_Portal wlan 3
Info: This operation may take a few seconds, please wait.done.
[AC-wlan-group-radio-ap-group1/1]quit
[AC-wlan-ap-group-ap-group1]quit
[AC-wlan-view]quit
[AC]
```

步骤 11 添加 Portal 认证准入设备

使用租户账号登录 NCE-Campus 管理界面，选择“准入管理 > 准入设备”，执行以下操作：



图13-2 进入准入设备管理界面

此处可复用“实验 12”中已添加的准入设备，但需按照以下操作，调整部分参数。

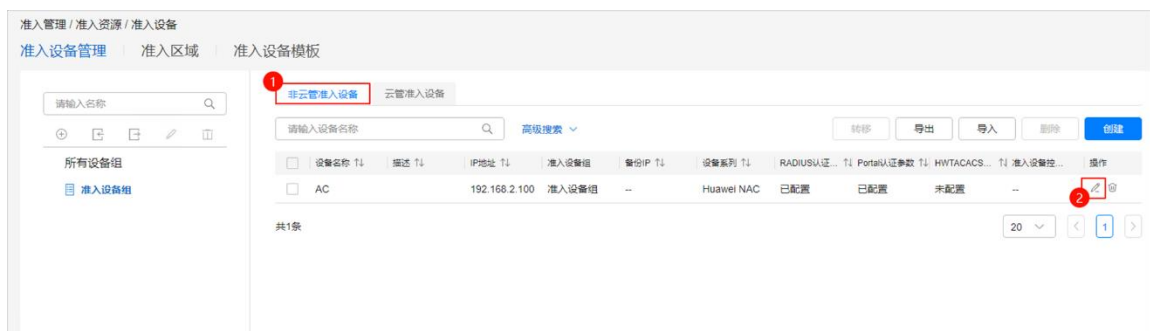


图13-3 进入准入设备配置参数修改界面

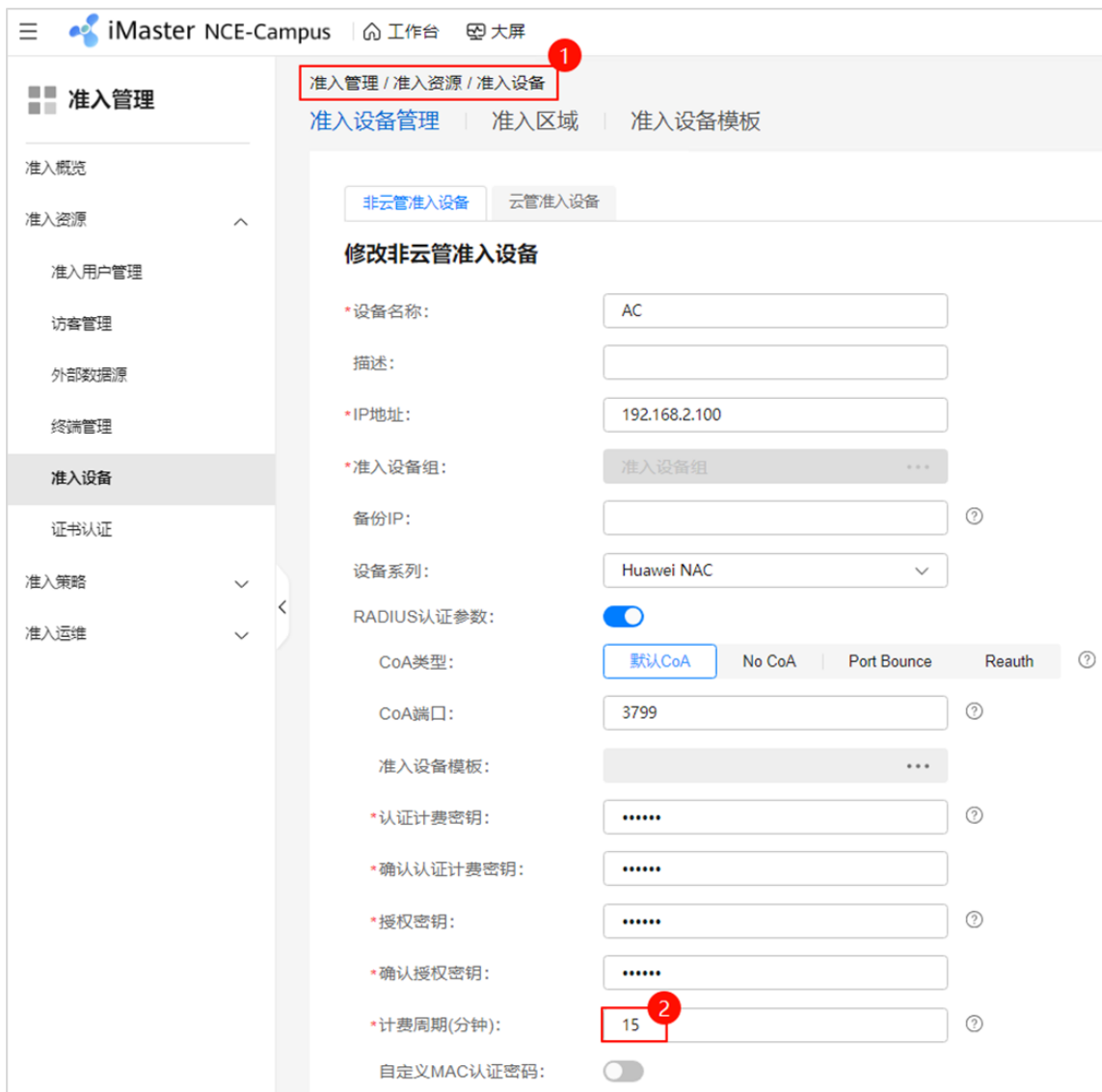


图13-4 准入设备参数修改（1）

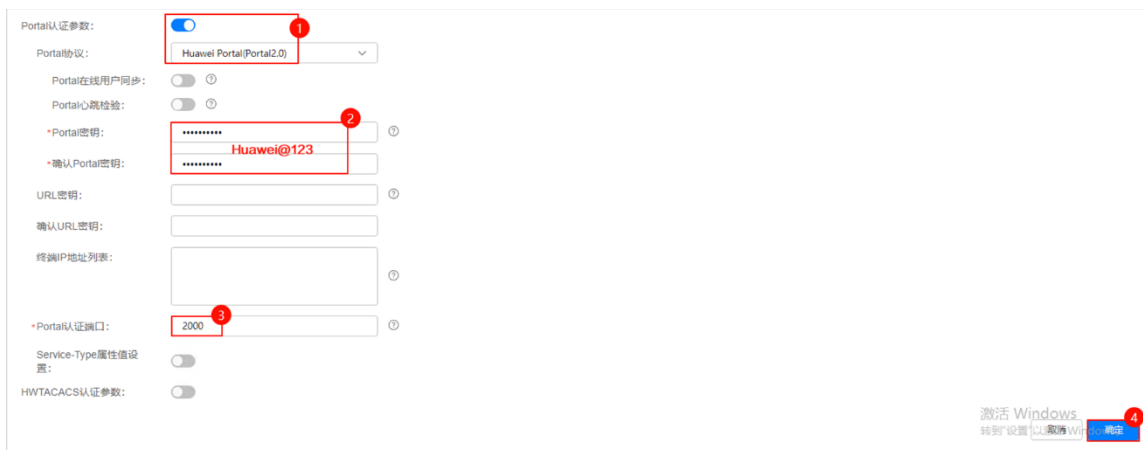


图13-5 准入设备参数修改（2）

步骤 12 创建 Portal 认证准入用户

使用租户账号登录 NCE-Campus 管理界面，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13-6 进入准入用户创建页面

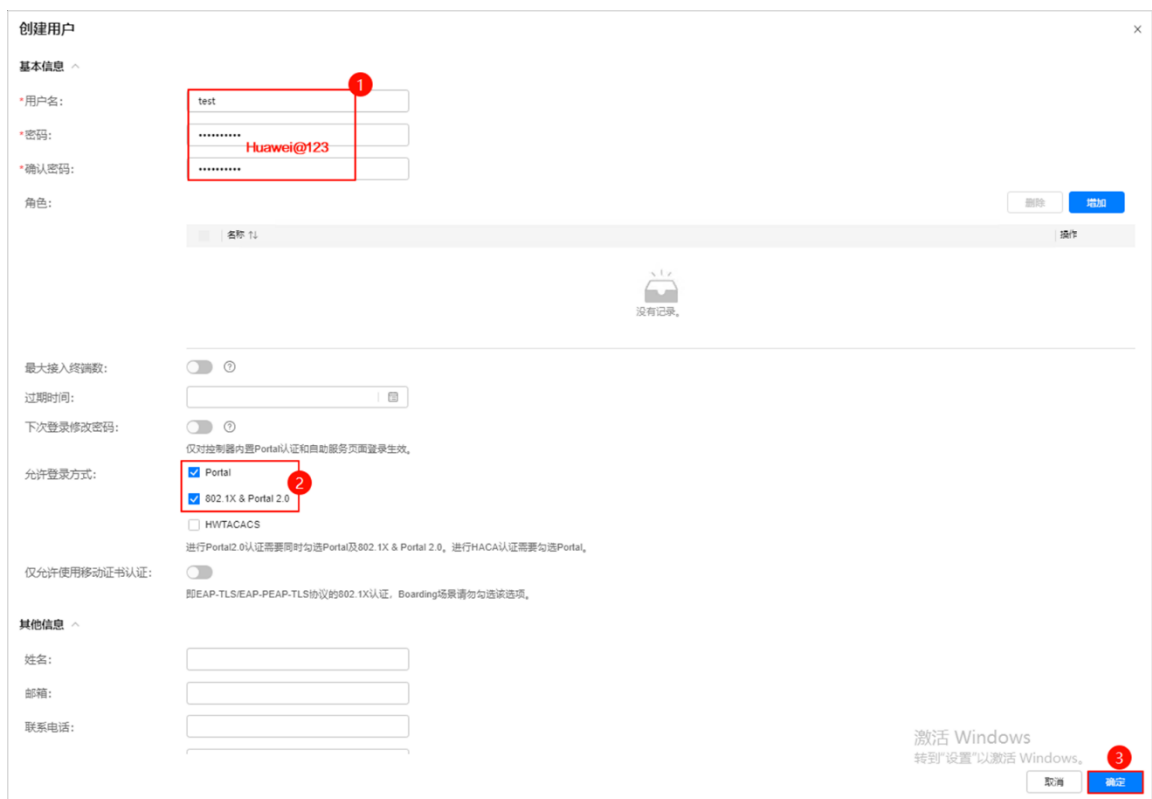


图13-7 创建 Portal 认证准入用户

Portal 认证准入用户创建完成后，效果如下：

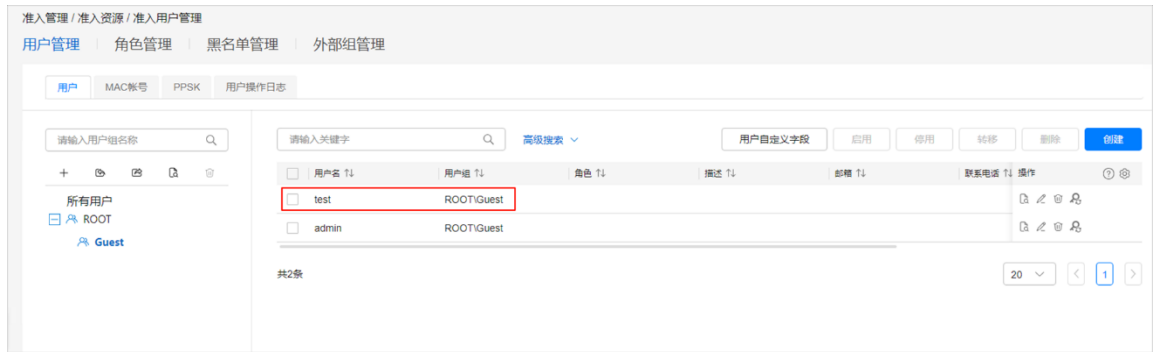


图13-8 查看 Portal 认证准入用户

步骤 13 创建认证与授权规则

使用租户账号登录 NCE-Campus 管理界面，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13-9 进入认证规则创建界面

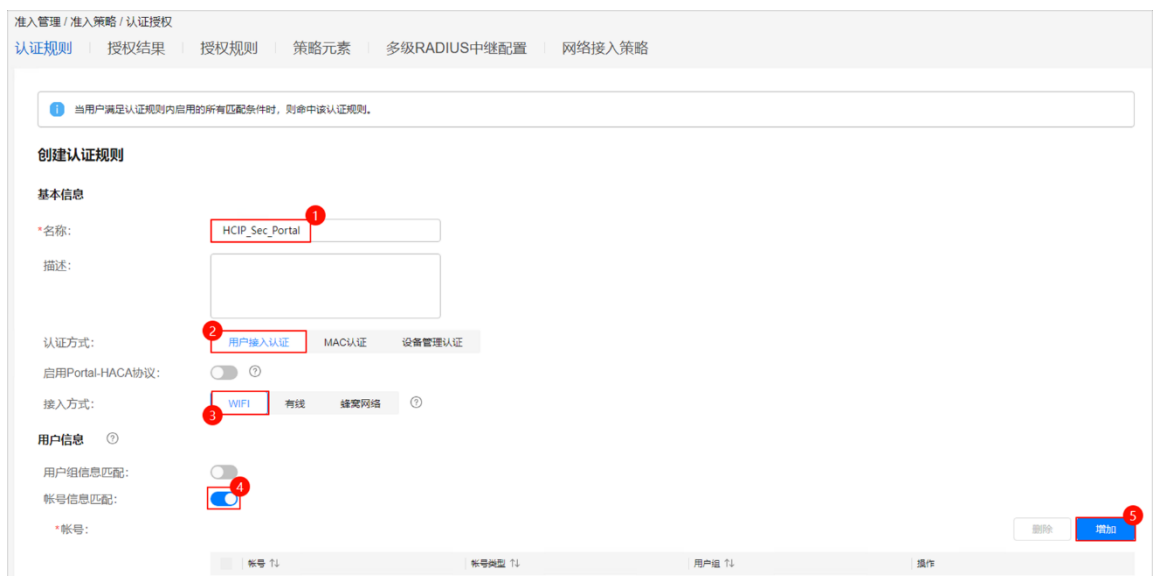


图13-10 创建 Portal 认证规则（1）

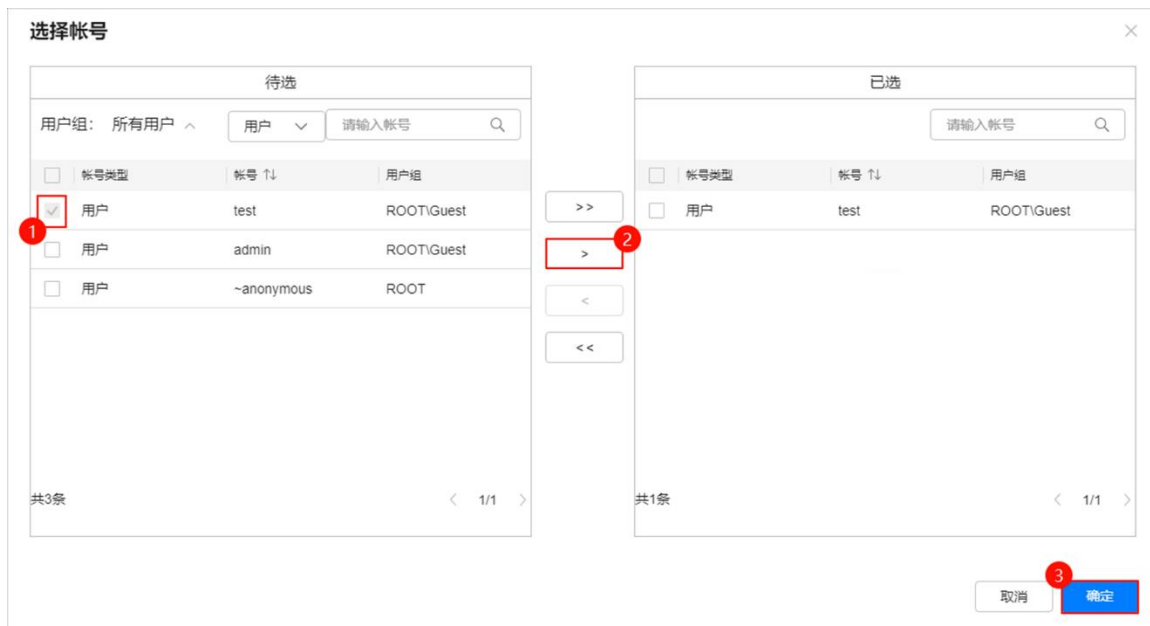


图13-11 创建 Portal 认证规则（2）

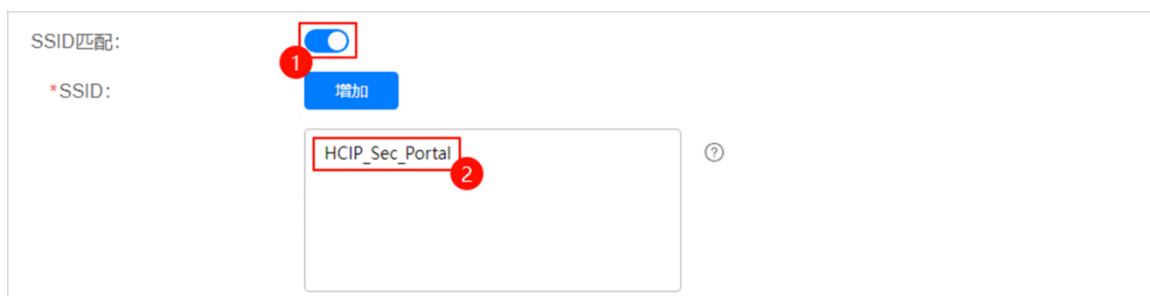


图13-12 创建 Portal 认证规则（3）

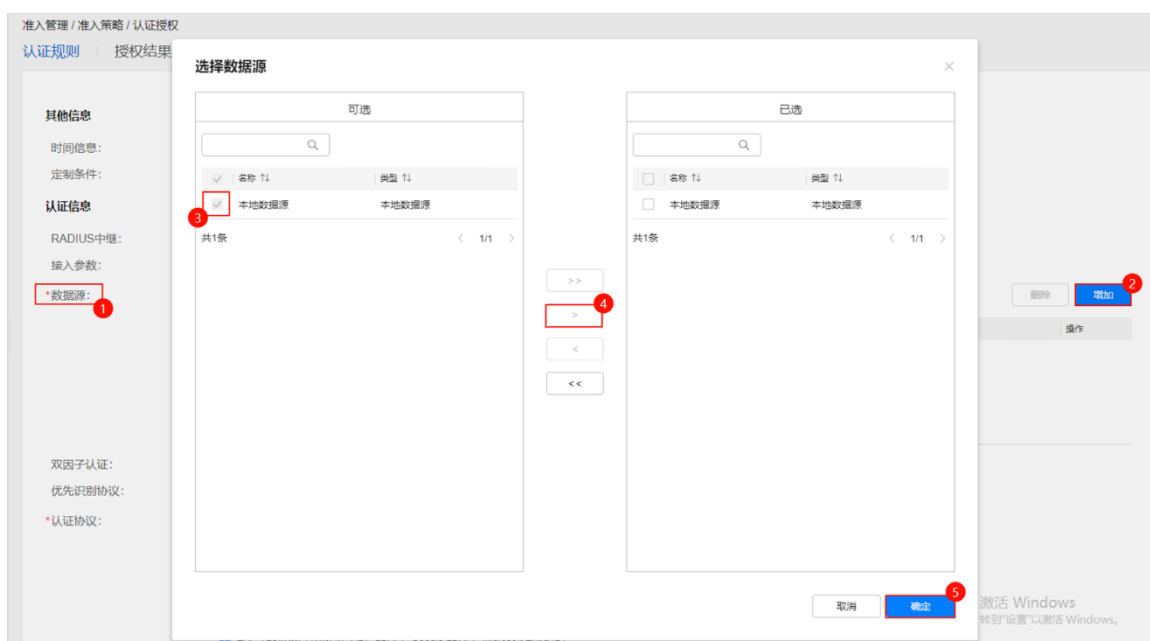


图13-13 创建 Portal 认证规则（4）

图13-13展示了创建Portal认证规则的配置界面。在“认证协议”部分，选择了“EAP-PEAP-MSCHAPv2”。在“高级选项”部分，配置了“帐号不存在”和“身份认证失败”的处理方式。最后，点击了“创建”按钮。

图13-14 创建 Portal 认证规则（5）

Portal 认证规则创建完成后，效果如下：

优先级	名称	认证方式	接入方式	匹配条件	数据源	认证协议	命中次数	接入参数	自停用状态	操作
1	802.1X	用户接入认证	WiFi	帐号: admin	<数据源>	PAP协议(...)	12	--	应用	删除
2	HCIP_Sec...	用户接入认证	WiFi	帐号: test SSID: HCIP_Sec_Portal	<数据源>	PAP协议(...)	0	--	应用	删除
N	Default	HACA Port...	有线/WiFi/...		<数据源>	EAP-TLS...	2	--	应用	删除

图13-15 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。

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	自停用状态	操作
1	802.1X	用户接入认证	WiFi	帐号: admin	802.1X		7	应用	删除
2	802.1X_A...	用户接入认证	有线	帐号: admin	允许接入		0	应用	删除
N	Default	HACA Port...	有线/WiFi/...		拒绝接入		0	应用	删除

图13-16 进入 Portal 授权规则创建界面



图13-17 创建 Portal 授权规则（1）



图13-18 创建 Portal 授权规则（2）

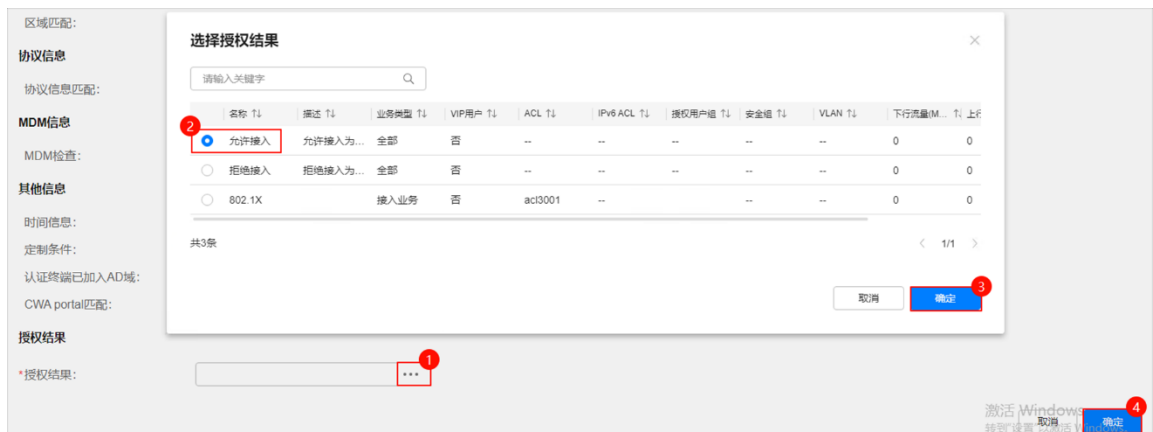


图13-19 创建 Portal 授权规则（3）

Portal 授权规则创建完成后，效果如下：



图13-20 查看 Portal 授权规则

步骤 14 配置 Portal 页面推送规则

使用租户账号登录 NCE-Campus 管理界面，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13-21 进入 Portal 页面推送规则管理界面



图13-22 修改 Portal 页面推送规则（1）



图13-23 修改 Portal 页面推送规则（2）

13.3 结果验证

使用 RDP 登录 PC3，打开无线网络管理并连接“HCIP_Sec_Portal”无线网络，执行以下操作：

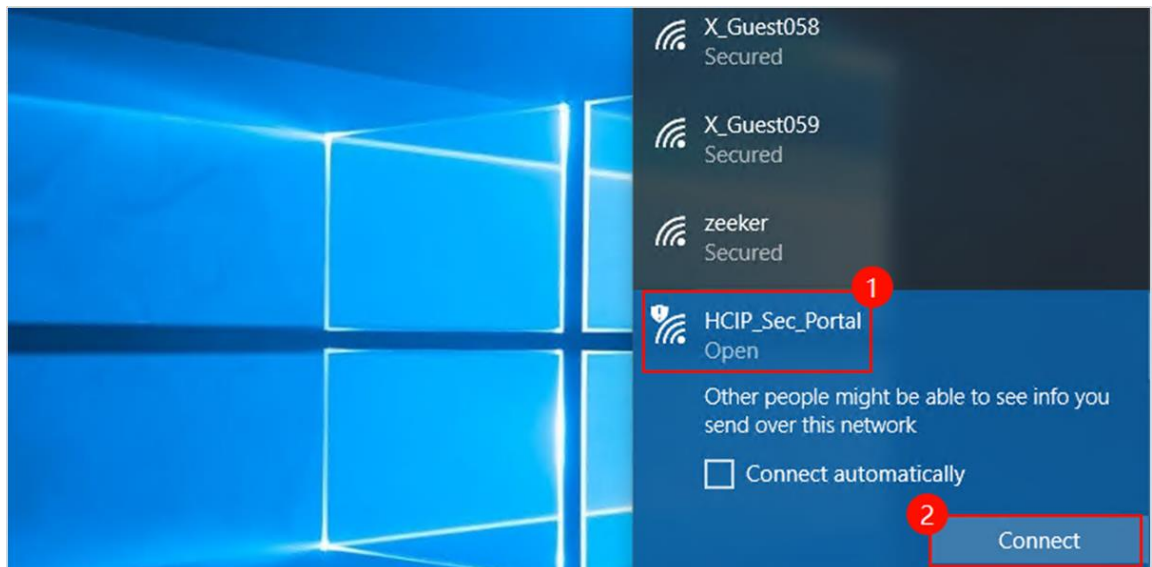


图13-24 PC3 连接无线网络

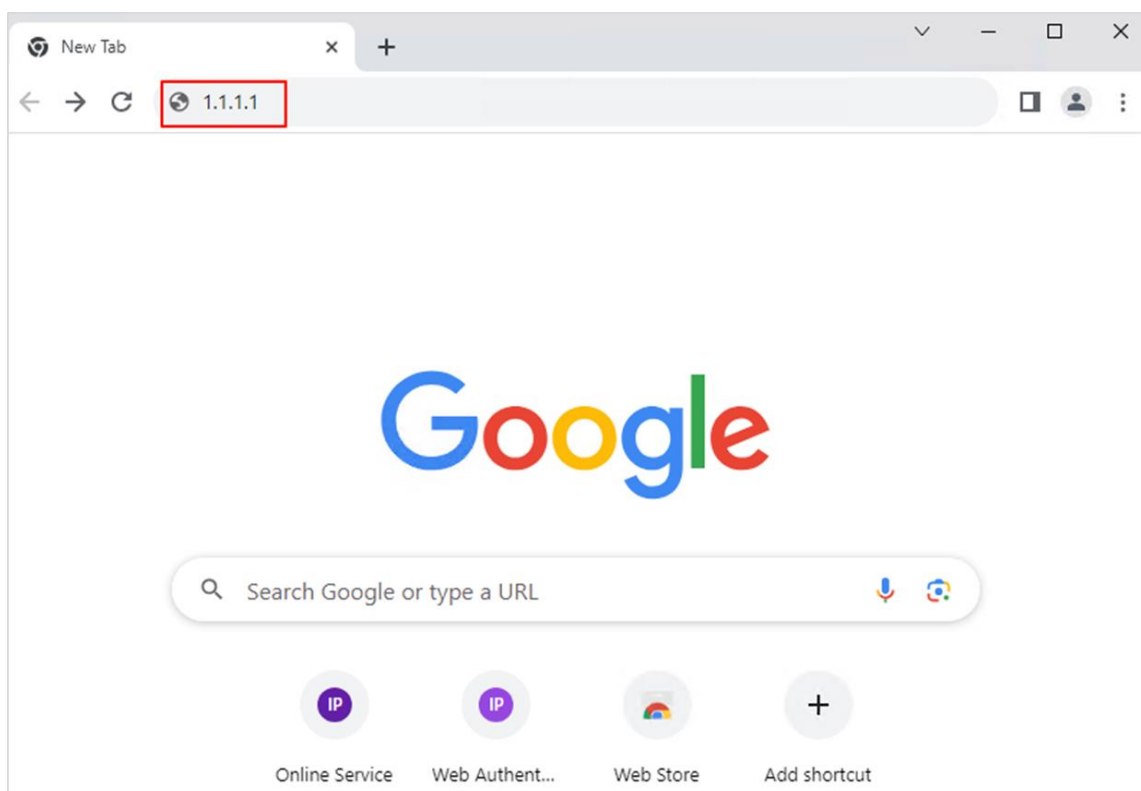


图13-25 PC3 打开浏览器访问任意 IP

浏览器访问任意 IP 后，会自动跳转到 Portal 认证界面：

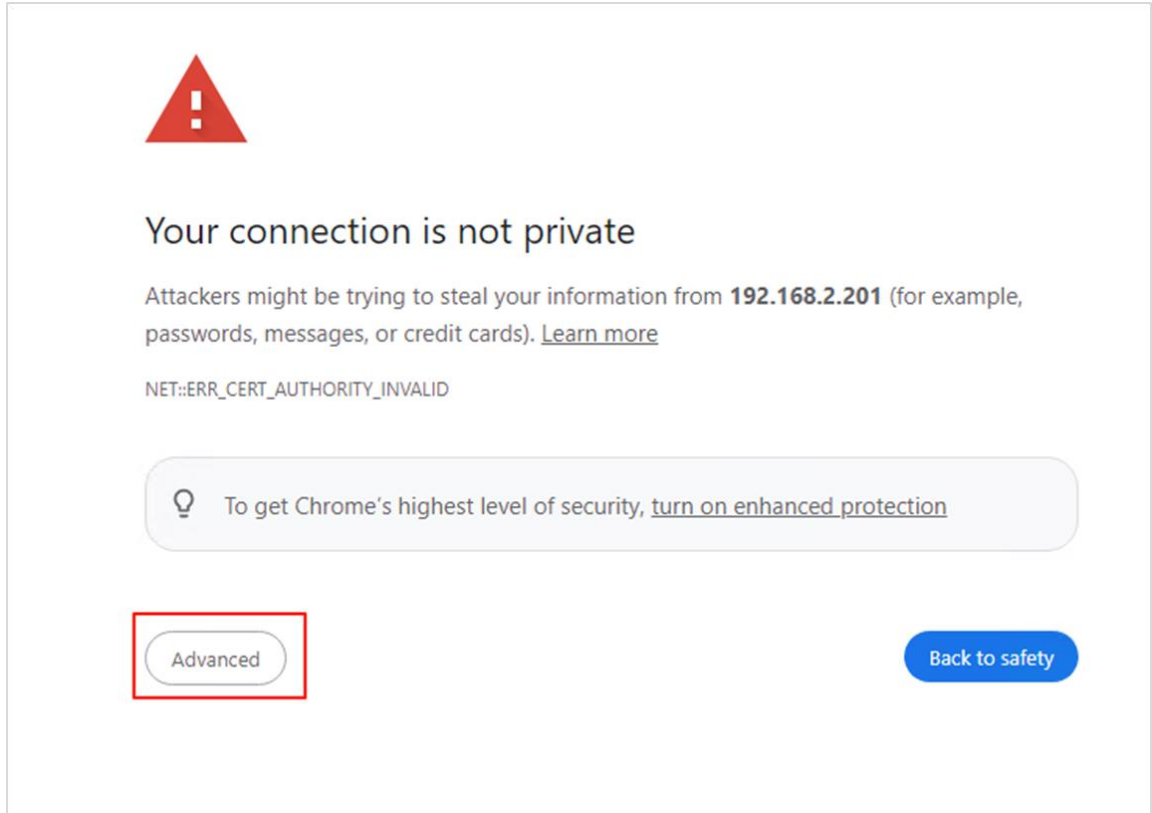


图13-26 忽略安全告警

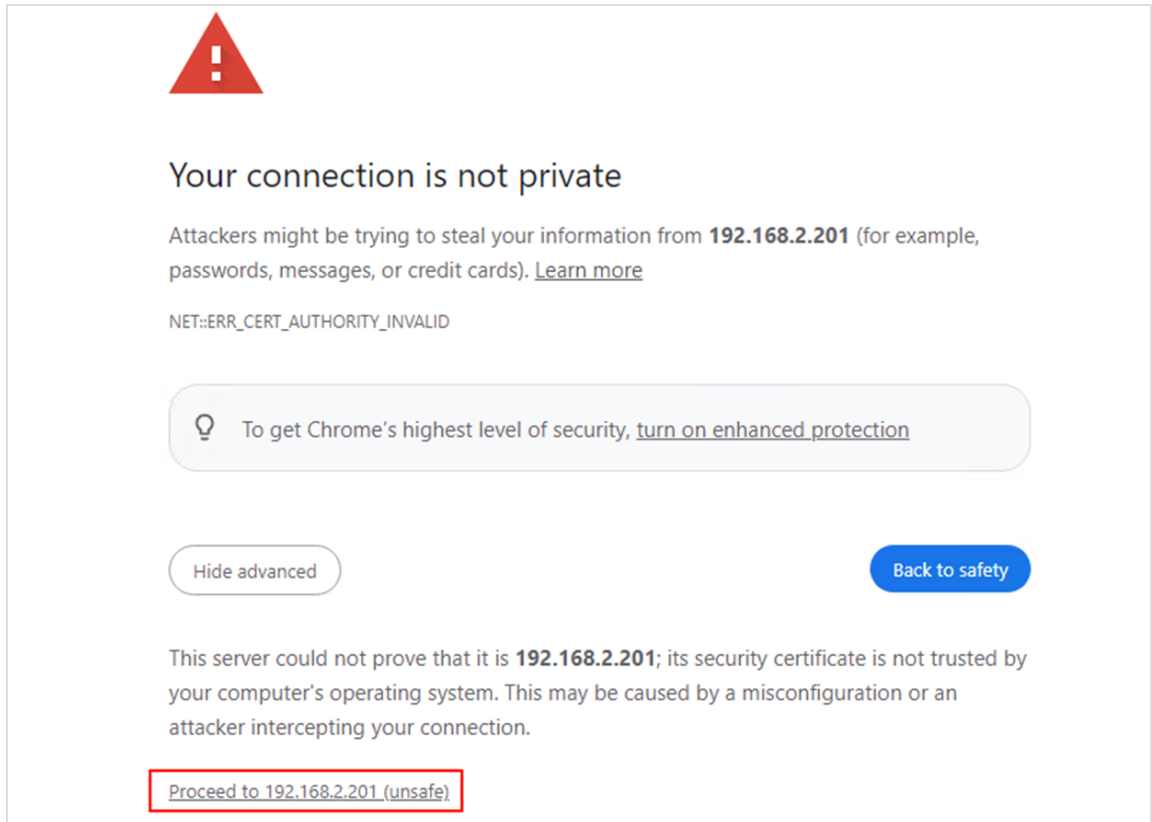


图13-27 继续访问跳转页面

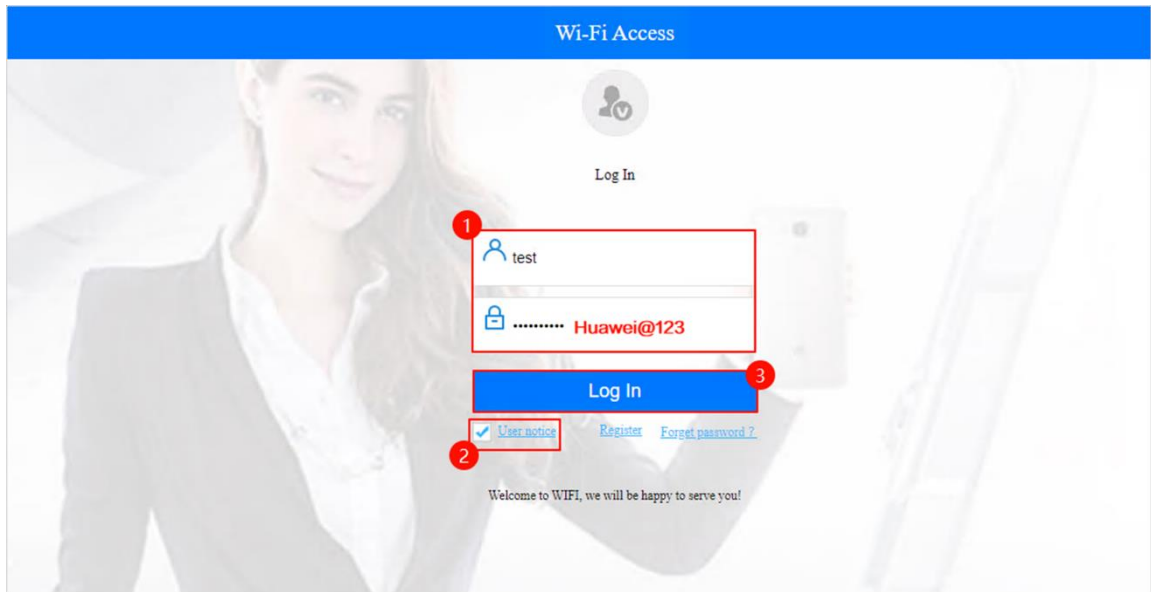


图13-28 PC3 跳转到 Portal 认证界面

输入“test/Huawei@123”的账户信息后，通过 Portal 认证，效果如下：

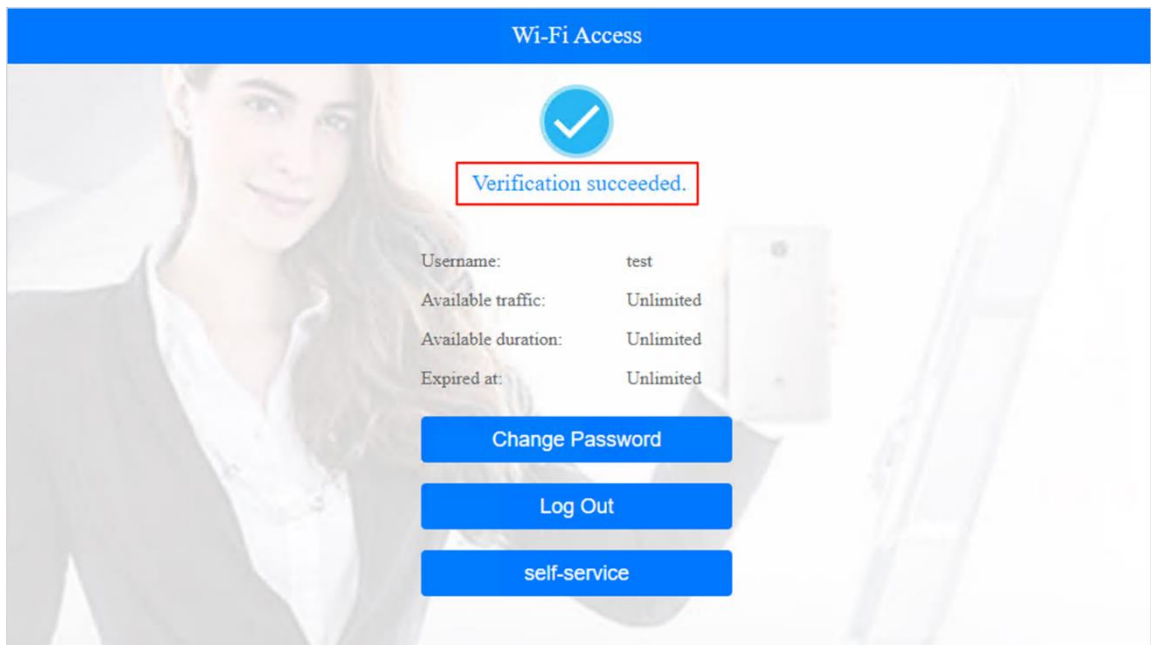


图13-29 PC3 终端 Portal 认证成功

使用租户账号登录 NCE-Campus 管理界面，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：

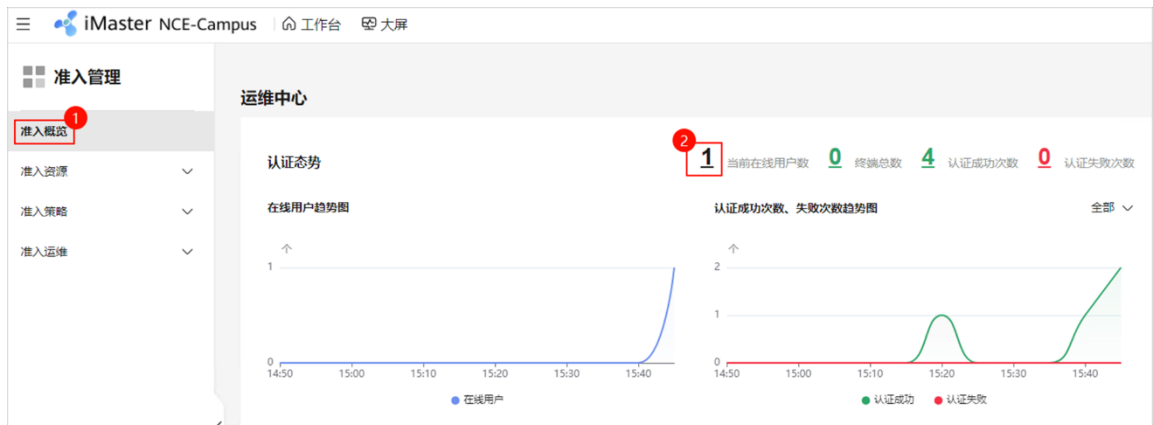


图13-30 进入在线用户管理界面



图13-33 查看 Portal 上下线日志

13.4 配置参考

13.4.1 SW2 配置

```
#
sysname SW2
#
vlan batch 10
#
interface GigabitEthernet0/0/2
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/17
 port link-type access
 port default vlan 10
#
```

13.4.2 SW3 配置

```
#
sysname SW3
#
vlan batch 10 4000 4001
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 10 4000 4001
#
interface GigabitEthernet0/0/12
 port link-type trunk
 port trunk pvid vlan 4000
 port trunk allow-pass vlan 4000
#
```

13.4.3 FW2 配置

```
#
sysname FW2
```

```
#
vlan batch 10
#
interface GE0/0/5
 portswitch
 undo shutdown
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 10
#
interface GE0/0/6
 portswitch
 undo shutdown
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 10
#
firewall zone trust
 set priority 85
 add interface GE0/0/5
 add interface GE0/0/6
#
```

13.4.4 AC 配置

```
#
 sysname AC
#
radius-server source ip-address 192.168.2.100
#
vlan batch 10 4000 to 4001
#
authentication-profile name auth_portal
 portal-access-profile portal
 free-rule-template free_rule
 access-domain default
#
web-auth-server server-source all-interface
#
dhcp enable
#
radius-server template t1
 radius-server shared-key cipher %^%#P&81!R"6z-4x~C~knm!Zkbs~@xljSAe/3K+9|i*8%^%#
 radius-server authentication 192.168.2.201 1812 weight 80
 radius-server accounting 192.168.2.201 1813 weight 80
#
free-rule-template name free_rule
 free-rule 1 destination ip 192.168.2.201 mask 255.255.255.255
```

```
#
url-template name nce
url https://192.168.2.201:19008/portal
url-parameter device-ip ac-ip redirect-url redirect-url ssid ssid user-ipaddress uaddress user-mac umac
url-parameter set device-ip 192.168.2.100
#
web-auth-server portal
server-ip 192.168.2.201
port 50100
shared-key cipher %^%#X[0m,<YOfG~sOx#mZV9YT+]>U;C~{+R0ZEY.Wrw>%^%#
url-template nce
source-ip 192.168.2.100
#
portal-access-profile name portal
web-auth-server portal direct
#
portal-access-profile name portal_access_profile
#
ip pool vlan4000
gateway-list 10.10.1.1
network 10.10.1.0 mask 255.255.255.0
option 43 sub-option 3 ascii 10.10.1.1
#
ip pool vlan4001
gateway-list 10.20.1.1
network 10.20.1.0 mask 255.255.255.0
#
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 t1
#
interface Vlanif10
ip address 192.168.2.100 255.255.255.0
#
interface Vlanif4000
ip address 10.10.1.1 255.255.255.0
dhcp select global
#
interface Vlanif4001
ip address 10.20.1.1 255.255.255.0
dhcp select global
```

```
#
interface GigabitEthernet0/0/2
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 10 4000 to 4001
#
capwap source interface vlanif4000
capwap dtls psk %^%#0!>x<g+._rk[GCUShe(g8nk)PbOuQ1NTz1-Tr=%^%#
capwap dtls inter-controller psk %^%#qcmB:/J!ABiwjjHg@@VMf!eYSj/:z5l`DP7rl"*0%^%#
capwap dtls no-auth enable
#
wlan
 temporary-management psk %^%#~/5'B_l~4M8#xg$(R;z7~p[P(#zzc>&V*%'6[Tn(%^%#
 ap username admin password cipher %^%#Kc98l|*gB-S5ATHdbGK@c$3x4!O<8.OKsA@nnT~K%^%#
 security-profile name security_portal
 security open
 ssid-profile name HCIP_Sec_Portal
 ssid HCIP_Sec_Portal
 vap-profile name HCIP-Security
 forward-mode tunnel
 service-vlan vlan-id 4001
 ssid-profile HCIP-Security
 security-profile HCIP-Security
 authentication-profile HCIP-Security
 vap-profile name HCIP_Sec_Portal
 forward-mode tunnel
 service-vlan vlan-id 4001
 ssid-profile HCIP_Sec_Portal
 security-profile security_portal
 authentication-profile auth_portal
 regulatory-domain-profile name domain1
 dca-channel 5g bandwidth 20mhz
 ap-group name ap-group1
 regulatory-domain-profile domain1
 radio 0
 vap-profile HCIP_Sec_Portal wlan 3
 radio 1
 vap-profile HCIP_Sec_Portal wlan 3
 ap-id 0 type-id 187 ap-mac 28fb-aeb7-d580 ap-sn 2102354MXJ10Q3100287
 ap-group ap-group1
 ap-id 1 ap-mac 28fb-aeb7-d581
 provision-ap
#
return
```

13.5 思考题

Portal 认证配置过程中，为何需要配置 free-rule？

参考答案：用户认证成功之前，为满足用户基本的网络服务，需要用户认证成功前就能获取部分网络访问权限。可在 free-rule 模板中配置 free-rule 规则，满足用户在认证成功前的网络访问需求。

14 Portal 认证故障排除实验

14.1 实验介绍

14.1.1 关于本实验

某企业部署了 WLAN 为员工提供无线办公环境，出于安全考虑，企业计划使用 Portal 方式对用户执行准入认证，且由于员工人数较多，需要使用内网中原有的 AD 认证服务器，完成对员工身份的认证。

本实验通过设置无线 Portal 认证开局及使用过程中常见的故障，带领学员学会常规的 Portal 故障排查思路，让学员掌握华为无线 AC 设备对接 AD 服务器认证相关配置。

14.1.2 实验目的

- 了解 Portal 认证流程。
- 掌握 AC 对接 AD 服务器的配置流程。
- 掌握常规 Portal 认证故障排查思路。

14.1.3 实验组网介绍

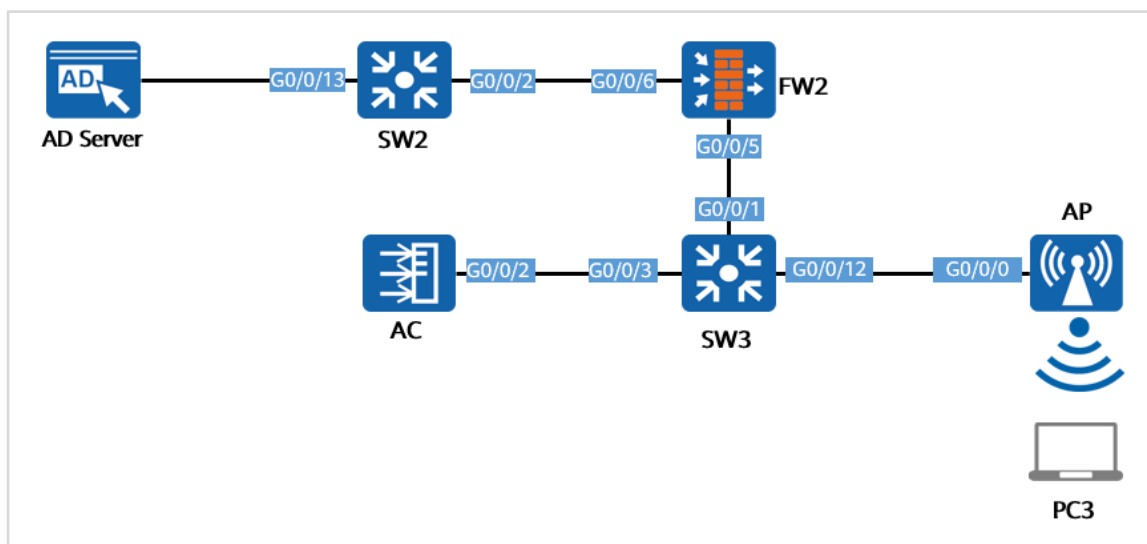


图14-1 Portal 无线认证实验拓扑

1.使用外置电源给 AP 供电。

- 2.AP 与 AC 之间为二层组网，AP 和终端的 DHCP 服务器均部署在 AC 上。
- 3.AC 与 AD 服务器之间为二层组网，无线终端的认证由 AD 服务器执行。
- 4.用户连接“Portal_AD”无线网络时，需要通过 Portal 认证，认证页面使用 AC 本地 Portal 页面。

14.1.4 实验规划

表14-1 设备接口规划表

设备	接口	接口性质	接口信息	说明
SW2	G0/0/2	Trunk	PVID: 1 Allow-pass VLAN: 10	与FW2互连
	G0/0/13	Access	PVID: 10	连接AD认证服务器
SW3	G0/0/1	Trunk	PVID: 1 Allow-pass VLAN: 10	与FW2互连
	G0/0/3	Trunk	PVID: 1 Allow-pass VLAN: 10, 4000, 4001	与AC互连
	G0/0/12	Trunk	PVID: 4000 Allow-pass VLAN: 4000	与AP互连
FW2	GE0/0/5	Trunk	PVID: 1 Allow-pass VLAN: 10	与SW3互连
	GE0/0/6	Trunk	PVID: 1 Allow-pass VLAN: 10	与SW2互连
AC	GE0/0/2	Trunk	PVID: 1 Allow-pass VLAN: 10, 4000, 4001	与SW3互连
AP	GE0/0/0	/	保持默认，无需配置	与SW3互连
AD Server	Ethernet0	网卡	172.16.30.100/24	服务器IP

14.2 实验任务配置

14.2.1 配置思路

- 1.将预配置导入对应设备。
- 2.按照实验规划检查业务是否正常，并逐一排错。

14.2.2 配置步骤

步骤 1 完成设备预配置

完成 SW2 的预配置。

```
#
sysname SW2
#
vlan batch 10
#
interface GigabitEthernet0/0/2
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/13
port link-type access
port default vlan 10
#
```

完成 SW3 的预配置。

```
#
sysname SW3
#
vlan batch 10 4000 4001
#
interface GigabitEthernet0/0/1
port link-type trunk
port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/3
port link-type trunk
port trunk allow-pass vlan 10 4000 4001
#
interface GigabitEthernet0/0/12
port link-type trunk
port trunk pvid vlan 4000
port trunk allow-pass vlan 4000
#
```


完成 FW2 的预配置。

```
#
sysname FW2
#
vlan batch 10
#
interface GigabitEthernet0/0/5
 portswitch
 undo shutdown
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/6
 portswitch
 undo shutdown
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 10
#
firewall zone trust
 set priority 85
 add interface GigabitEthernet0/0/5
 add interface GigabitEthernet0/0/6
#
```

完成 AC 的预配置。

```
#
sysname AC
#
http secure-server ssl-policy default_policy
http secure-server server-source -i all
Y
http server enable
#
portal local-server ip 10.20.1.1
portal local-server http port 8080
#
portal https-redirect tls1.1 enable
Y
#
vlan batch 10 4000 4001
#
dns resolve
dns proxy enable
Y
#
```

```
dhcp enable
#
interface vlanif10
 ip address 172.16.30.10 255.255.255.0
#
interface vlanif4000
 ip address 10.10.1.1 255.255.255.0
 dhcp select global
#
interface vlanif4001
 ip address 10.20.1.1 255.255.255.0
 dhcp select global
#
ad-server template t1
 ad-server authentication 172.16.30.100 88 no-ssl
Y
 ad-server authentication base-dn dc=huawei,dc=cn
 ad-server authentication manager cn=Administrator,cn=users Huawei@123
 ad-server authentication host-name WIN-Q2QSOCUE8QT.huawei.cn
 ad-server authentication ldap-port 389
 ad-server user-filter sAMAccountName
 ad-server group-filter ou
 ad-server cipher-suite aes256-hmac-sha1
#
portal-access-profile name Portal-AD
 portal http-proxy-redirect enable
#
ip pool vlan4001
 gateway-list 10.20.1.1
 network 10.20.1.0 mask 255.255.255.0
#
ip pool vlan4000
 gateway-list 10.10.1.1
 network 10.10.1.0 mask 255.255.255.0
 option 43 sub-option 3 ascii 10.10.1.1
#
aaa
 authentication-scheme Portal-AD
  authentication-mode ad
 authorization-scheme AD
  authorization-mode ad
#
authentication-profile name Portal-AD
 authentication-scheme Portal-AD
 authorization-scheme AD
 ad-server t1
#
interface GigabitEthernet0/0/2
```

```

port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 10 4000 4001
#
wlan
security-profile name Portal-AD
security open
Y
Y
ssid-profile name Portal-AD
ssid Portal-AD
vap-profile name Portal-AD
forward-mode tunnel
service-vlan vlan-id 4001
ssid-profile Portal-AD
security-profile Portal-AD
Y
ap-group name ap-group1
radio 0
vap-profile Portal-AD wlan 3
radio 1
vap-profile Portal-AD wlan 3
radio 2
vap-profile Portal-AD wlan 3
ap-id 1 type-id 130 ap-mac 14ab-0228-5f80 ap-sn 2102353GES6RN5008931
ap-name a5760
Y
ap-group ap-group1
Y
#

```

在 AC 上配置 capwap 隧道的源接口，同时需要配置对应密码，参考如下加粗的配置。

```

[AC] capwap source interface vlanif 4000
Set the DTLS inter-controller PSK(contains 8-32 plain-text characters, or 48 or 68 cipher-text characters
that must be a combination of at least two of the following: lowercase letters a to z, uppercase letters A
to Z, digits, and special characters):Huawei@123
Confirm PSK:Huawei@123
Configuring the new PSK, waiting.....done.

Info: Deliver DTLS PSK to devices using CAPWAP connections. It may take a few minutes.

-----
CAPWAP DTLS PSK deliver result
Deliver Number : 0
Success Number : 0
Failed Number : 0
-----.....done.

Set the user name for FIT APs(The value is a string of 4 to 31 characters, which can contain letters,
underscores, and digits, and must start with a letter):admin

```

Set the password for FIT APs(plain-text password of 8-128 characters or cipher-text password of 48-188 characters that must be a combination of at least three of the following: lowercase letters a to z, uppercase letters A to Z, digits, and special characters): **Huawei@123**

Confirm password: **Huawei@123**

Set the global temporary-management psk(contains 8-63 plain-text characters, or 48-108 cipher-text characters that must be a combination of at least two of the following: lowercase letters a to z, uppercase letters A to Z, digits, and special characters): **Huawei@123**

Confirm PSK: **Huawei@123**

Warning: Ensure that the management VLAN and service VLAN are different. Otherwise, services may be interrupted.

Warning: Before an added device goes online for the first time, enable DTLS no-auth if it runs a version earlier than V200R021C00 or enable DTLS certificate-mandatory-match if it runs V200R021C00 or later.

步骤 2 检查无线终端连接情况

使用 RDP 登录 PC3，打开无线网络管理，发现无法搜索到名为“Portal-AD”的无线网络。

在 AC 上检查 AP 是否上线。

```
[AC] display ap all
Total AP information:
idle : idle          [1]
ExtraInfo : Extra information

-----
ID      MAC           Name  Group    IP Type           State STA  Uptime ExtraInfo
-----
1       14ab-0228-5f80 a5760 ap-group1 - AirEngine5760-51 idle  0  -    -
-----
Total: 1
```

发现 AP 没有上线，但 AP 上线配置无误，此处考虑到 AC 对接 V200R021C00 及之后版本的 AP 时，可能因为没有 DTLS 凭证导致无法上线，尝试以下操作。

使能 CAPWAP 的 DTLS 会话使用预置证书认证方式。

```
[AC] capwap dtls cert-mandatory-match enable
Warning: This operation allows for device access using the preset certificate when DTLS is enabled and brings security risks. After the device goes online for the first time, disable this function to prevent security risks. Continue?[Y/N]:Y
```

说明：增加对接 V200R021C00 及之后版本的 AP 时，避免 AP 无法上线，可以先开启该功能允许 AP 以预置证书认证方式进行 DTLS 会话，使 AP 上线。AP 上线后会获取新的 DTLS 凭证，重新以安全方式进行 DTLS 会话和上线。为确保网络安全，在 AP 重新上线后，应立即关闭该功能，避免未授权 AP 接入网络。

完成上述操作后，再次检查 AP 上线情况，发现 AP 已正常上线。

```
[AC] display ap all
Total AP information:
nor   : normal       [1]
ExtraInfo : Extra information

-----
ID      MAC           Name  Group    IP      Type           State STA  Uptime ExtraInfo
-----
```

```

-----
1      14ab-0228-5f80 a5760 ap-group1 10.10.1.131 AirEngine5760-51 nor    0    24S    -
-----

```

Total: 1

回到 PC3，再次尝试连接 “Portal-AD” 无线网络，发现可以正常连接。

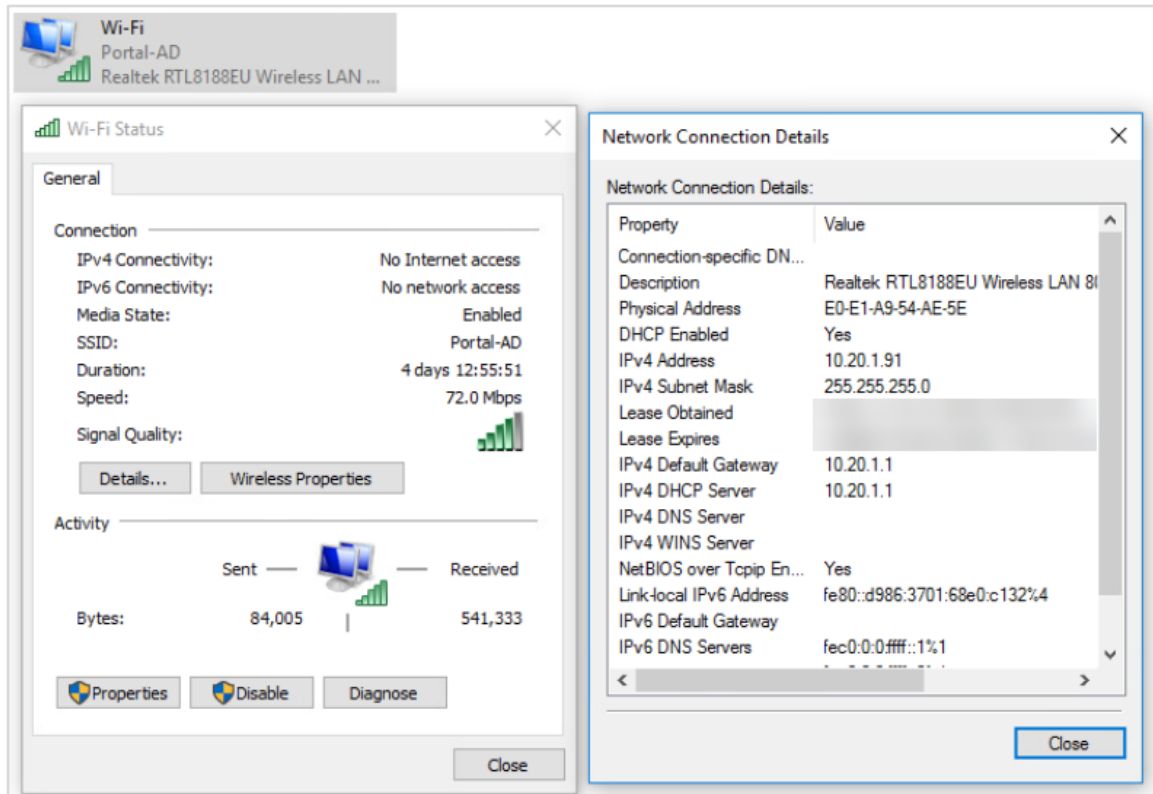


图14-2 PC3 正常连接 “Portal_AD” 无线网络

步骤 3 检查 Portal 页面弹出情况

PC3 成功连接无线网络以后，在 PC3 的浏览器中随意输入一个 IP 地址并回车，发现没有 Portal 认证页面弹出。

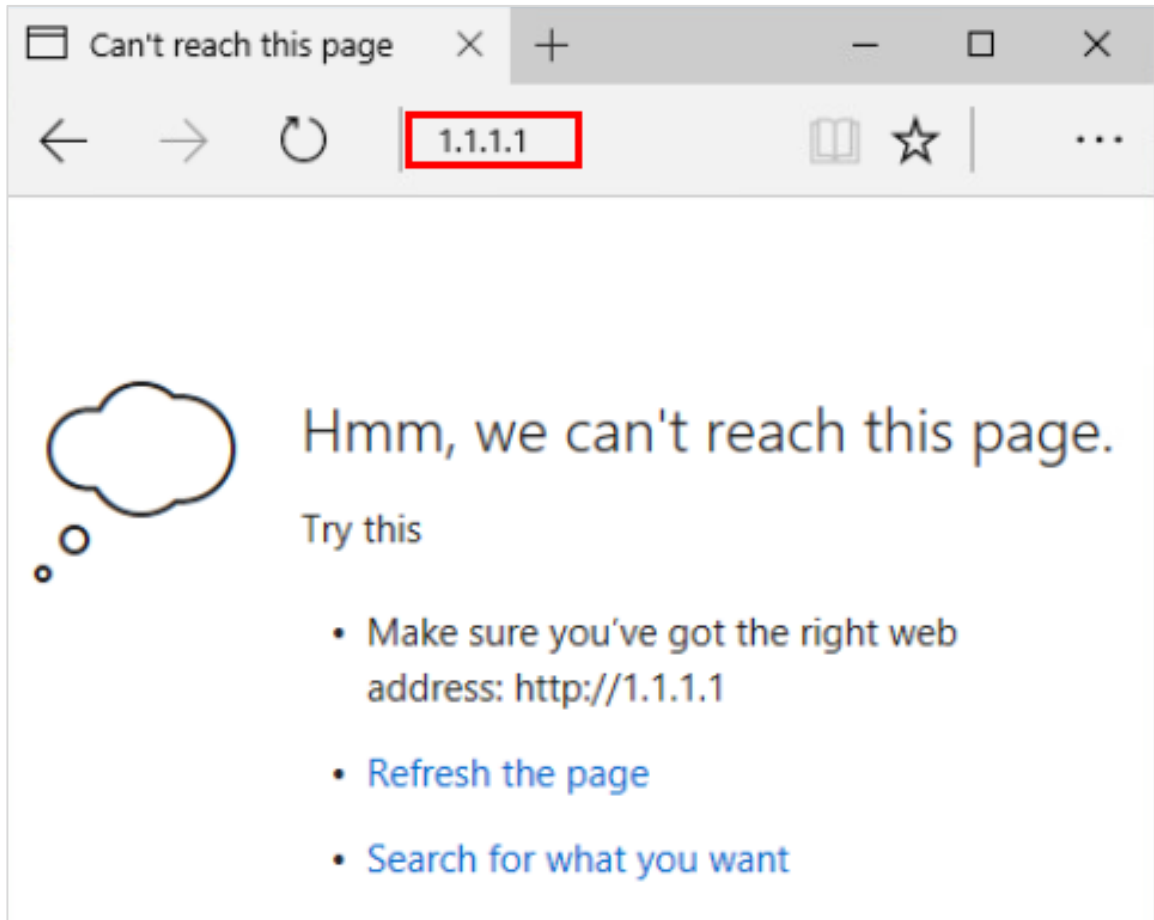


图14-3 Portal 认证页面未正常弹出

以上现象表示 AC 本地的 Portal 页面未响应，可能是 PC3 与 AC 之间不互通、Portal 认证配置问题、AC 本地 Portal 页面配置参数等问题，需要逐一排查。

首先检查网络连通性，发现 PC3 可以 ping 通 AC，表明底层网络无问题。

```
C:\Users\Security>ping 10.20.1.1

Pinging 10.20.1.1 with 32 bytes of data:
Reply from 10.20.1.1: bytes=32 time=27ms TTL=255
Reply from 10.20.1.1: bytes=32 time=36ms TTL=255
Reply from 10.20.1.1: bytes=32 time=7ms TTL=255
Reply from 10.20.1.1: bytes=32 time=11ms TTL=255

Ping statistics for 10.20.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 7ms, Maximum = 36ms, Average = 20ms
```

图14-4 PC3 与 AC 之间连通性测试

之后再检查 Portal 认证相关配置。

#

```
authentication-profile name Portal-AD
 authentication-scheme Portal-AD
 authorization-scheme AD
 ad-server t1
#
```

从上述 AC 的配置可以发现，认证模板中调用了认证模式、授权模式，但是没有调用 Portal 接入模板。

继续检查 Portal 接入模板配置。

```
#
portal-access-profile name Portal-AD
 portal http-proxy-redirect enable
#
```

可以发现 Portal 接入模板配置与本实验规划有出入，实验规划使用 AC 本地的 portal 页面，该配置有误。

修改 Portal 接入模板配置，使用内置 Portal 服务器。

```
[AC] portal-access-profile name Portal-AD
[AC-portal-access-profile-Portal-AD] undo portal http-proxy-redirect enable
[AC-portal-access-profile-Portal-AD] portal local-server enable
[AC-portal-access-profile-Portal-AD] quit
```

之后在认证模板中调用 Portal 接入模板。

```
[AC] authentication-profile name Portal-AD
[AC-authentication-profile-Portal-AD] portal-access-profile Portal-AD
[AC-authentication-profile-Portal-AD] quit
```

完成上述配置后，使用 PC3 再次测试，发现依旧无法跳转至 Portal 页面。

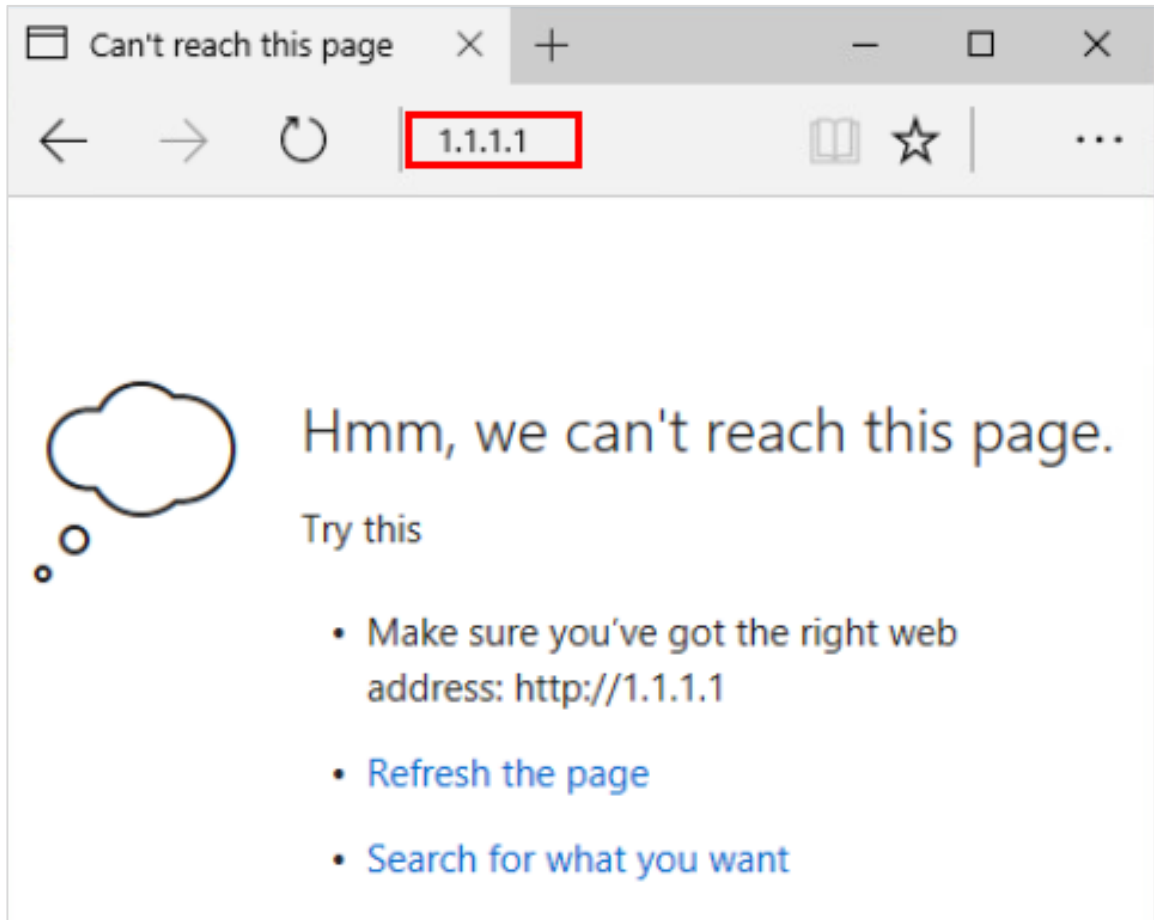


图14-5 Portal 认证页面未正常弹出

继续排查，按照配置逻辑，Portal 接入模板需要在认证模板中调用，认证模板需要在 vap-profile 视图下调用。

接下来查看 vap-profile 视图下配置。

```
[AC] wlan
[AC-wlan-view] vap-profile name Portal-AD
[AC-wlan-vap-prof-Portal-AD] display this
#
forward-mode tunnel
service-vlan vlan-id 4001
ssid-profile Portal-AD
security-profile Portal-AD
#
```

由以上配置信息发现，在 vap-profile 视图下未调用认证模板。

完善 vap-profile 视图下的配置。

```
[AC] wlan
[AC-wlan-view] vap-profile name Portal-AD
[AC-wlan-vap-prof-Portal-AD] authentication-profile Portal-AD
Warning: This action may cause service interruption. Continue?[Y/N]Y
Info: This operation may take a few seconds, please wait.done.
```



```
[AC-wlan-vap-prof-Portal-AD] quit
```

完成上述配置后，再次使用 PC3 测试，发现浏览器可以正常跳转 AC 内置的 portal 页面。

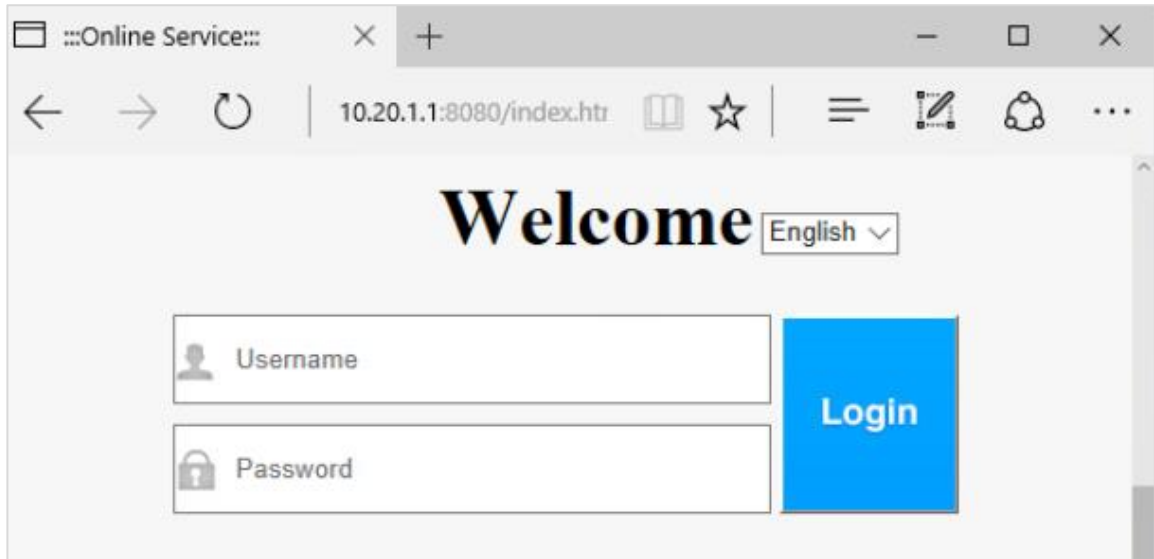


图14-6 正常跳转 Portal 认证页面

步骤 4 检查 AD 认证

在 Portal 认证页面中输入 AD 服务器中的用户账号（test/Huawei@123）测试。

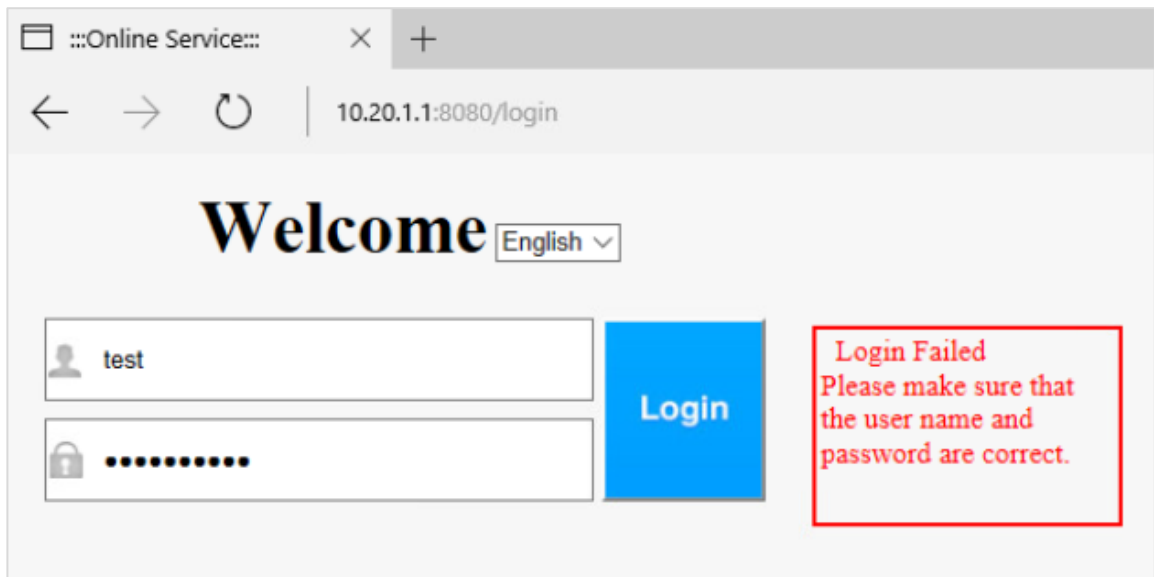


图14-7 尝试 Portal 认证

发现用户认证失败，用户输入用户名密码提交认证请求时，报文得先经过 AC 转发，然后由 AD 认证服务器校验。

在 AC 上检查 authentication-scheme Portal-AD 中的配置。

```
[AC] aaa
[AC-aaa] authentication-scheme Portal-AD
[AC-aaa-authen-Portal-AD] display this
```

```
#
authentication-scheme Portal-AD
authentication-mode ad
#
```

发现认证模式为 AD，配置正确。

在 AC 上检查 authorization-scheme Portal-AD 中的配置。

```
[AC] aaa
[AC-aaa] authorization-scheme Portal-AD
[AC-aaa-author-Portal-AD] display this
#
authorization-scheme Portal-AD
authorization-mode ad
#
```

授权模式为 AD，配置正确。

在 AC 上检查 AD 服务器配置。

```
[AC] ad-server template t1
[AC-ad-t1] display this
#
ad-server template t1
ad-server authentication 172.16.30.100 88 no-ssl
ad-server authentication base-dn dc=huawei,dc=cn
ad-server authentication manager cn=Administrator,cn=users %^%#fBzRQc;\y6xPILX`G#*~Kku#.Wch~-
flrN4WjNM#%^%#
ad-server authentication host-name WIN-Q2QSOCUE8QT.huawei.cn
ad-server authentication ldap-port 389
ad-server user-filter sAMAccountName
ad-server group-filter ou
ad-server cipher-suite aes256-hmac-sha1
#
```

配置参数正确。

在 AC 上测试用户名密码与 AD 服务器是否对接正常。

```
[AC] test-aaa test Huawei@123 ad-template t1
Info: Server detection succeeded.
```

回显信息说明 AC 与 AD 之间的对接正常，用户名及密码无误，由此推断，故障点在无线终端 PC3 与 AC 侧。

在 AC 上开启调试命令，之后在 PC3 浏览器上再次输入用户名密码登录。

```
<AC> debugging portal event
<AC> debugging portal message
<AC> terminal debugging
<AC> terminal monitor
<AC> Aug 15 20** 01:29:06.804.1+00:00
AC %01WEBS/4/USER_ACCESSRESULT(l)[0]:[WEBS_USER_ONLINEFAIL]USERNAME:test;IPADDRESS:10.
20.1.202;MAC:-;ERRCODE:303;
```

调试回显信息中的“ERRCODE 303”代表 Portal 服务器认证失败。Portal 认证支持 AD/LDAP 认证，但是需要将认证方式配置为 PAP，内置 Portal 默认采用 CHAP，需要通过 portal local-server authentication-method { chap | pap }命令手动配置认证方式为 PAP。

配置 AC 内置 Portal 采用 PAP 认证方式。

```
[AC] portal local-server authentication-method pap
```

完成上述配置后，在 PC3 浏览器 Portal 认证页面中输入 AD 服务器中的用户名密码（test/Huawei@123），再次进行 Portal 认证测试。

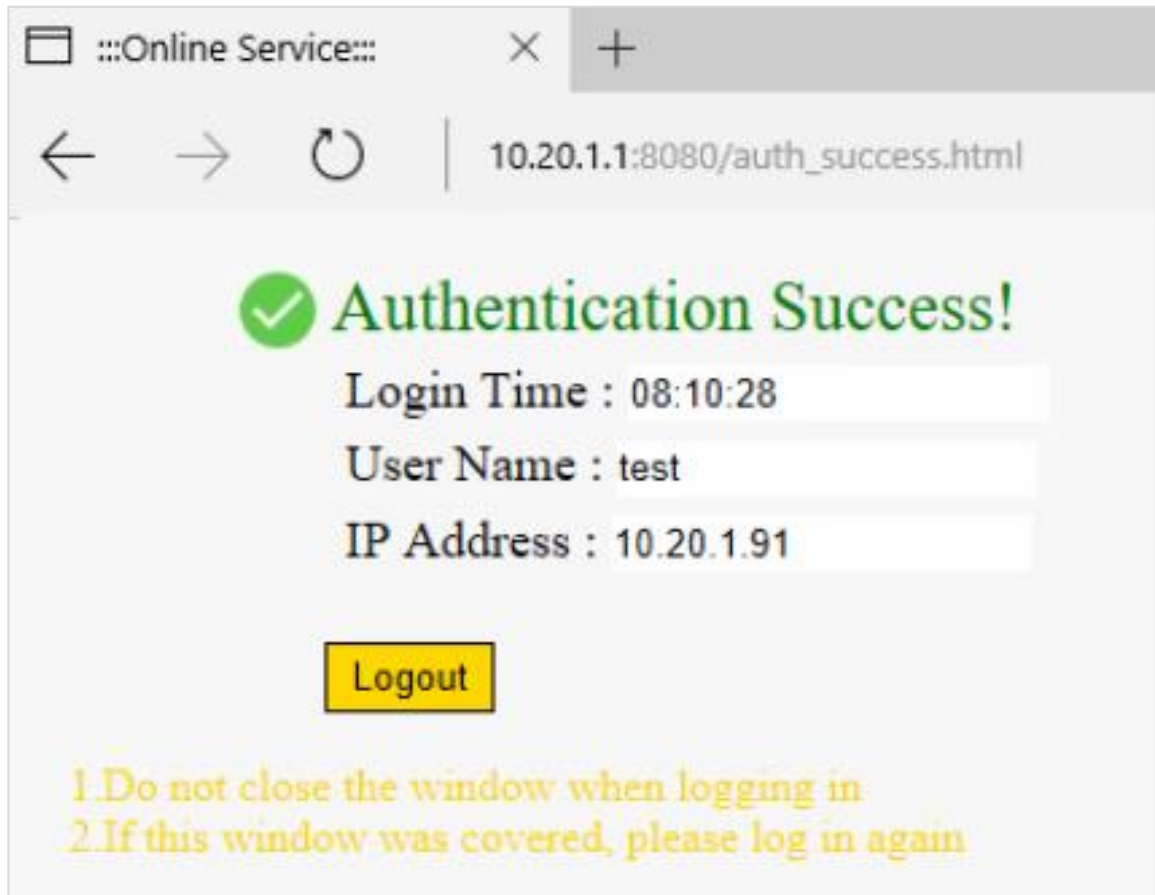


图14-8 Portal 认证成功

由以上信息可以发现 PC3 的 Portal 认证已正常，至此 Portal 认证故障排除实验完成。

14.3 配置参考

14.3.1 SW2 配置

```
#
sysname SW2
#
vlan batch 10
```

```
#
interface GigabitEthernet0/0/2
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/13
 port link-type access
 port default vlan 10
#
```

14.3.2 SW3 配置

```
#
sysname SW3
#
vlan batch 10 4000 4001
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 10 4000 4001
#
interface GigabitEthernet0/0/12
 port link-type trunk
 port trunk pvid vlan 4000
 port trunk allow-pass vlan 4000
#
```

14.3.3 FW2 配置

```
#
sysname FW2
#
vlan batch 10
#
interface GigabitEthernet0/0/5
 portswitch
 undo shutdown
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/6
 portswitch
```

```
undo shutdown
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 10
#
firewall zone trust
set priority 85
add interface GigabitEthernet0/0/5
add interface GigabitEthernet0/0/6
#
```

14.3.4 AC 配置

```
#
sysname AC
#
http secure-server ssl-policy default_policy
http secure-server server-source -i all
http server enable
#
portal local-server ip 10.20.1.1
portal local-server authentication-method pap
portal local-server http port 8080
#
portal https-redirect tls1.1 enable
#
portal pass dns enable
#
vlan batch 10 4000 4001
#
dns resolve
dns proxy enable
#
dhcp enable
#
ad-server template t1
ad-server authentication 172.16.30.100 88 no-ssl
ad-server authentication base-dn dc=huawei,dc=cn
ad-server authentication manager cn=Administrator,cn=users %^%#fBzRQc;\y6xPILX`G#*~Kku#.Wch~-firN4WjNM#%^%#
ad-server authentication host-name WIN-Q2QSOCUE8QT.huawei.cn
ad-server authentication ldap-port 389
ad-server user-filter sAMAccountName
ad-server group-filter ou
ad-server cipher-suite aes256-hmac-sha1
#
portal-access-profile name Portal-AD
portal local-server enable
```

```
#
ip pool vlan4001
 gateway-list 10.20.1.1
 network 10.20.1.0 mask 255.255.255.0
#
ip pool vlan4000
 gateway-list 10.10.1.1
 network 10.10.1.0 mask 255.255.255.0
 option 43 sub-option 3 ascii 10.10.1.1
#
aaa
 authentication-scheme Portal-AD
 authentication-mode ad
 authorization-scheme AD
 authorization-mode ad
#
authentication-profile name Portal-AD
portal-access-profile Portal-AD
 authentication-scheme Portal-AD
 authorization-scheme AD
 ad-server t1
#
interface vlanif10
 ip address 172.16.30.10 255.255.255.0
#
interface vlanif4000
 ip address 10.10.1.1 255.255.255.0
 dhcp select global
#
interface vlanif4001
 ip address 10.20.1.1 255.255.255.0
 dhcp select global
#
interface GigabitEthernet0/0/2
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 10 4000 4001
#
capwap source interface vlanif4000
#
wlan
 security-profile name Portal-AD
 security open
 ssid-profile name Portal-AD
 ssid Portal-AD
 vap-profile name Portal-AD
 forward-mode tunnel
 service-vlan vlan-id 4001
```

```
ssid-profile Portal-AD
security-profile Portal-AD
authentication-profile Portal-AD
ap-group name ap-group1
radio 0
    vap-profile Portal-AD wlan 3
radio 1
    vap-profile Portal-AD wlan 3
radio 2
    vap-profile Portal-AD wlan 3
ap-id 1 type-id 130 ap-mac 14ab-0228-5f80 ap-sn 2102353GES6RN5008931
ap-name a5760
ap-group ap-group1
#
```

14.4 思考题

在 AC+FIT AP 组网场景中，AP 无法上线的原因可能有哪些？

参考答案：

- 1.物理设备故障：AP 故障、AC 故障、中间网络设备故障、线缆故障等。
- 2.供电故障：交换机供电不足、供电模式错误等。
- 3.网络配置故障：DHCP 配置错误 AP 无法获取地址、AP 与 AC 网络不可达、AP 认证配置错误、CAPWAP 源地址配置错误、AC 上黑白名单配置错误等。
- 4.软件版本故障：AP 与 AC 软件版本不匹配、版本升级失败等。
- 5.License 原因：AC 未加载 License 或 License 满载。