

华为认证 Security 系列教程

HCIA-Security

实验指导手册

版本：4.0



华为技术有限公司

版权所有 © 华为技术有限公司 2024。保留一切权利。

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

商标声明



和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

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

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

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： <https://e.huawei.com>

华为认证体系介绍

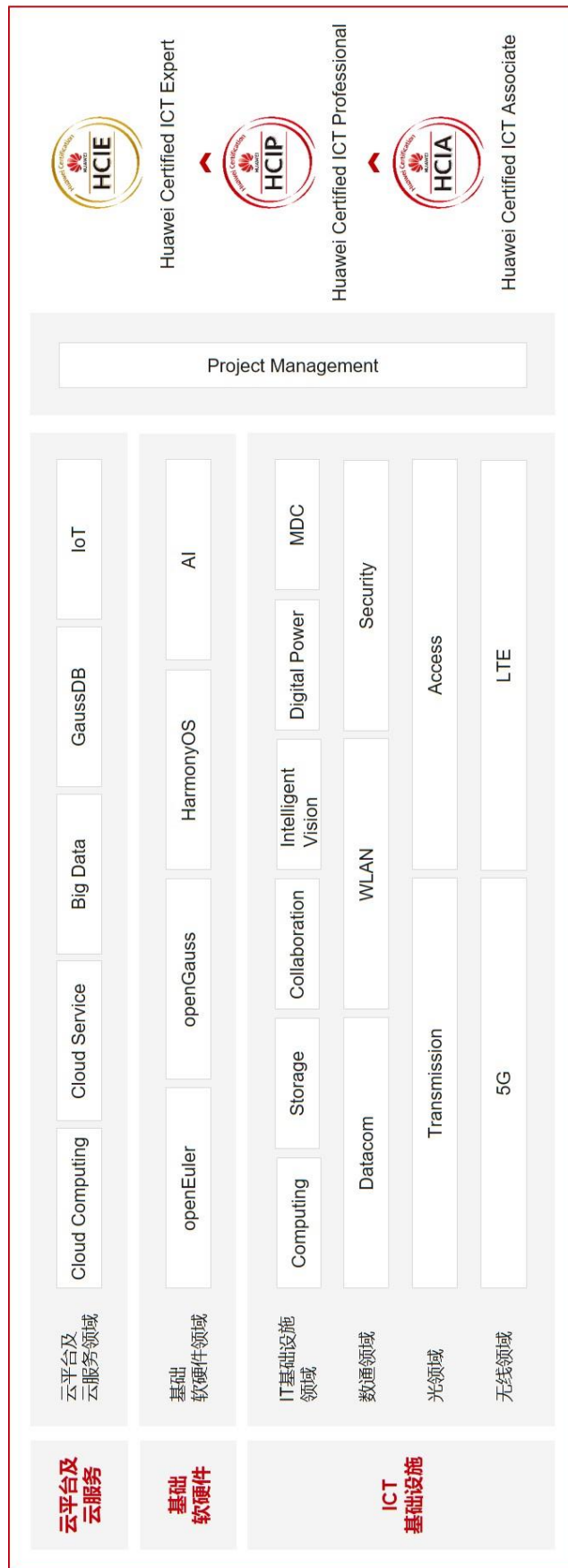
华为认证是华为公司基于“平台+生态”战略，围绕“云-管-端”协同的新ICT技术架构，打造的覆盖ICT（Information and Communications Technology，信息通信技术）全技术领域的认证体系，包含ICT技术架构与应用认证、云服务与平台认证两类认证。

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。

HCIA-Security（Huawei Certified ICT Associate-Security，华为认证网络通信工程师安全方向）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安全产品和网络安全的技术人士。HCIA-Security认证在内容上涵盖信息安全域安全概述、网络安全基础、加解密原理与应用等内容。

华为认证协助您打开行业之窗，开启改变之门，屹立在网络安全领域的潮头浪尖！



前言

简介

本书为 HCIA-Security 认证培训教程，适用于准备参加 HCIA-Security 考试的学员或者希望了解信息安全概念及规范、常见的网络安全威胁及防范、网络安全基础知识、防火墙网络安全防范技术、用户管理技术、加解密原理与加密技术应用等相关技术的读者。

内容描述

本实验指导书共包含 7 个实验，从设备基本操作配置开始，逐一介绍了登陆防火墙的基础操作、安全策略、NAT、双机热备、用户管理、IPSec VPN、SSL VPN 的配置与实现。

- 实验一为防火墙登陆实验，通过介绍登陆防火墙的常规方式，帮助读者熟悉防火墙管理方式，掌握基础调试能力。
- 实验二为防火墙安全策略实验，通过基本的组网配置，帮助读者掌握防火墙安全区域与区域间转发控制逻辑等关键技术能力。
- 实验三为防火墙 NAT Server & 源 NAT 实验，重点讲解源 NAT 转换和目的 NAT 转换技术，通过此实验，使读者掌握在 NAT 场景下防火墙的调试方法，熟悉防火墙作为出口设备的应用场景。
- 实验四为防火墙双机热备实验，通过此实验，帮助读者掌握如何使用防火墙对业务实现冗余，以及在防火墙单机故障情况下如何保证业务正常运行等技术能力。
- 实验五为点到点 IPSec VPN 实验，通过此实验，帮助读者掌握不同网络跨互联网相互通信的基本方法。
- 实验六为 SSL VPN 实验，本实验可以实现移动办公用户在互联网上随时访问企业内网，帮助读者理解 SSL VPN 的原理与配置。

读者知识背景

本课程为华为认证基础课程，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：

- 具有基本的网络安全知识背景，同时熟悉华为路由交换设备，了解基本数通知识。

本书常用图标



Firewall



Switch



以太网线缆



PC



Server



调试串口线缆

实验环境说明

组网说明

本实验环境面向准备 HCIA-Security 考试的网络安全工程师。每套实验环境包括防火墙 2 台，交换机 2 台，PC 主机 4 台。每套实验环境适用于 4 名学员同时上机操作。

设备介绍

为了满足 HCIA-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
交换机	S5735-S24T4X	V200R021C00SPC100
防火墙	USG6525F	V600R022C00SPC100

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型号给出，不同的实验环境中，以上信息可能有所不同，学员需要注意。

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
S5735交换机	每组2台	
USG6525F防火墙	每组2台	

笔记本或台式机	每组4台	
双绞线	每组8条	长度至少2米
Console线	每组1条	

每组学员检查自己的设备列表如下：

- S5735 交换机 2 台；
- USG6525F 防火墙 2 台；
- 笔记本或台式机 4 台；
- 双绞线 8 条；
- Console 线 1 条。

清空防火墙配置

实验时，为避免残余配置对实验的影响，要求学生在实验完成后，关闭设备之前需要清空设备保存的配置信息。实验开始时，确认设备从空配置启动，否则执行配置清空，并重启设备。

登录防火墙需要输入用户名及密码，本实验配置的用户名为：admin，密码为 Admin@123，交换机操作方式方法一致，以防火墙为例说明如下：

```
Login authentication
Username:admin
Password:
<FW> reset saved-configuration
This will delete the configuration in the flash memory.
The device configurations will be erased to reconfigure.
Are you sure? (y/n)[n]:y
Clear the configuration in the device successfully.
```

重启防火墙的命令是：

```
<FW> reboot
Info: The system is comparing the configuration, please wait.
Warning: All the configuration will be saved to the next startup configuration.
Continue ? [y/n]:n
System will reboot! Continue ? [y/n]:y
Info: system is rebooting ,please wait...
```

目录

前 言	3
简介	3
内容描述	3
读者知识背景	3
本书常用图标	4
实验环境说明	4
准备实验环境	4
1 如何登录防火墙	10
1.1 通过 Console 口登录设备 (PuTTY)	10
1.1.1 实验介绍	10
1.1.2 实验任务配置	11
1.1.3 结果验证	12
1.1.4 思考题	12
1.2 熟悉命令行 (PuTTY)	13
1.2.1 实验介绍	13
1.2.2 实验任务配置	14
1.2.3 思考题	16
1.3 通过 Telnet 登录设备	16
1.3.1 实验介绍	16
1.3.2 实验任务配置	17
1.3.3 结果验证	22
1.3.4 思考题	22
1.4 通过 SSH 登录设备	23
1.4.1 实验介绍	23
1.4.2 实验任务配置	23
1.4.3 结果验证	26
1.4.4 思考题	26
1.5 通过默认 Web 方式登录设备	27
1.5.1 实验介绍	27
1.5.2 实验任务配置	27
1.5.3 结果验证	28

1.5.4 思考题	29
1.6 通过 Web 方式登录设备	30
1.6.1 实验介绍	30
1.6.2 实验任务配置	30
1.6.3 结果验证	34
1.6.4 思考题	35
2 防火墙安全策略实验	36
2.1 实验介绍	36
2.1.1 关于本实验	36
2.1.2 实验目的	36
2.1.3 实验组网介绍	36
2.1.4 实验规划	36
2.2 实验任务配置	37
2.2.1 配置思路	37
2.2.2 配置步骤 - CLI	37
2.2.3 配置步骤 - Web	38
2.3 结果验证	40
2.4 思考题	41
3 防火墙 NAT Server & 源 NAT 实验	42
3.1 实验介绍	42
3.1.1 关于本实验	42
3.1.2 实验目的	42
3.1.3 实验组网介绍	42
3.1.4 实验规划	42
3.1.5 配置思路	43
3.1.6 配置步骤 - CLI	43
3.1.7 配置步骤 - Web	44
3.1.8 结果验证	49
3.1.9 思考题	50
3.2 实验任务配置（NAT Server & 源 NAT 实验）	50
3.2.1 配置思路	50
3.2.2 配置步骤 - CLI	50
3.2.3 配置步骤 - Web	52
3.2.4 结果验证	57
3.2.5 思考题	58

4 防火墙双机热备实验	59
4.1 实验介绍	59
4.1.1 关于本实验	59
4.1.2 实验目的	59
4.1.3 实验组网介绍	59
4.1.4 实验规划	59
4.2 实验任务配置	60
4.2.1 配置思路	60
4.2.2 配置步骤 - CLI	60
4.2.3 配置步骤 - Web	63
4.3 结果验证	70
4.4 配置参考	73
4.4.1 FW1 的配置	73
4.4.2 FW2 的配置	75
4.5 思考题	76
5 点到点 IPsec VPN 实验	77
5.1 实验介绍	77
5.1.1 关于本实验	77
5.1.2 实验目的	77
5.1.3 实验组网介绍	77
5.1.4 实验规划	77
5.2 实验任务配置	78
5.2.1 配置思路	78
5.2.2 配置步骤 - Web	78
5.3 结果验证	84
5.4 配置参考	84
5.4.1 FW1 的配置	84
5.4.2 FW2 的配置	86
5.5 思考题	88
6 SSL VPN 实验	89
6.1 实验介绍	89
6.1.1 关于本实验	89
6.1.2 实验目的	89
6.1.3 实验组网介绍	89
6.1.4 实验规划	89

6.2 实验任务配置	90
6.2.1 配置思路.....	90
6.2.2 配置步骤 - Web	90
6.3 结果验证	96
6.4 配置参考	100
6.4.1 FW 的配置	100
6.5 思考题	102

1 如何登录防火墙

1.1 通过 Console 口登录设备（PuTTY）

1.1.1 实验介绍

1.1.1.1 关于本实验

本实验通过配置出厂空配置下的防火墙，使用 PC 终端通过 Console 口登录设备，了解并熟悉设备的管理和配置。

1.1.1.2 实验目的

- 掌握 PC 终端通过设备 Console 口登录并管理设备的方法；
- 掌握一些常见的命令行配置；
- 掌握使用命令行在线帮助的方法；
- 掌握如何撤销命令；
- 掌握如何使用命令行快捷键。

1.1.1.3 实验组网介绍

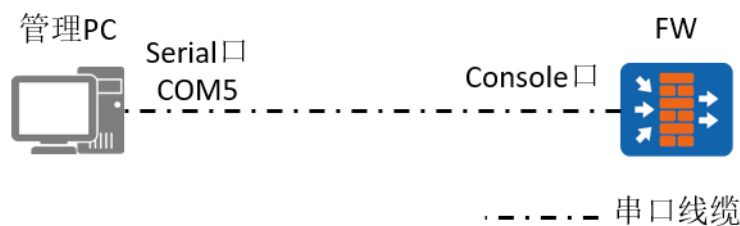


图1-1 通过 Console 口登录设备拓扑图

1.1.1.4 实验背景

如组网图所示，FW 是一台全新无配置的防火墙，PC 通过串口线缆连接到 FW 的 Console 口，需要对 FW 进行一些初始化操作。

1.1.1.5 实验规划

管理 PC 使用串口线缆连接设备的 Console 口，管理 PC 通过 PuTTY 软件登录设备。

表1-1 设备端口及参数说明

设备	端口	端口类型	说明
管理PC	COM5	串口	串口线缆在管理PC端是USB接口或者串口，电脑上需要安装驱动，查看并使用对应的端口号。
防火墙设备	Console	Console口	设备面板有Console接口标识。

1.1.2 实验任务配置

1.1.2.1 配置思路

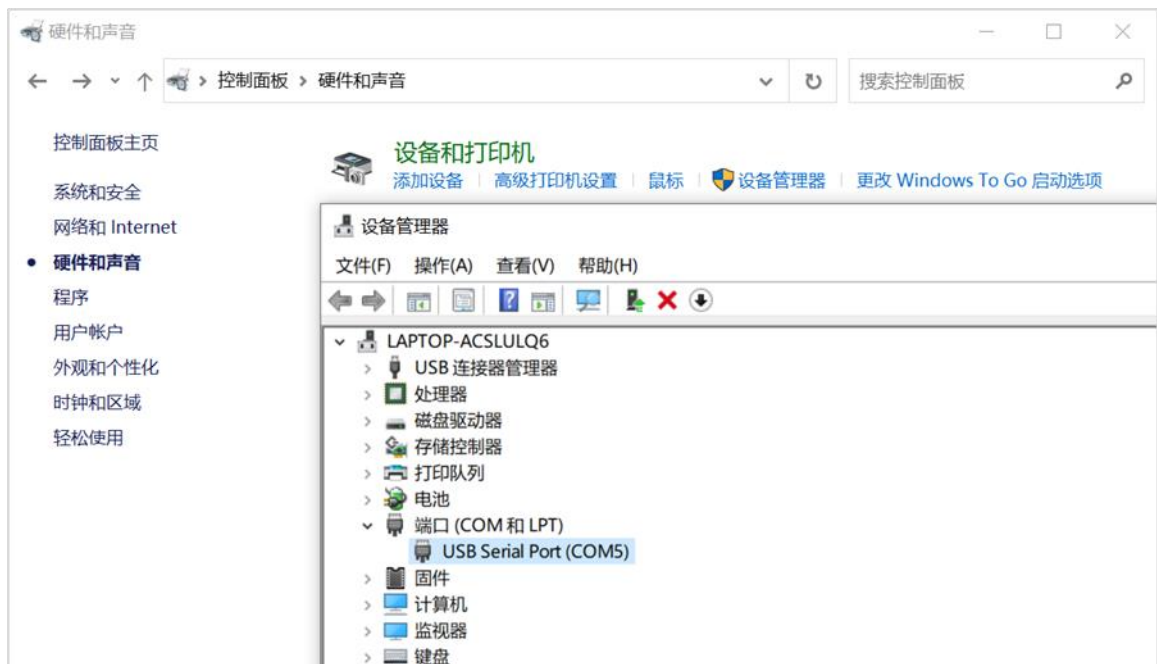
- 1.使用串口线缆连接管理 PC 的串口（或者 USB 接口）和设备的 Console 口。
- 2.在管理 PC 上配置 PuTTY 软件的连接参数，登录设备。

1.1.2.2 配置步骤

步骤 1 完成设备建立连接后，将所有设备上电，并且保证设备运行正常。

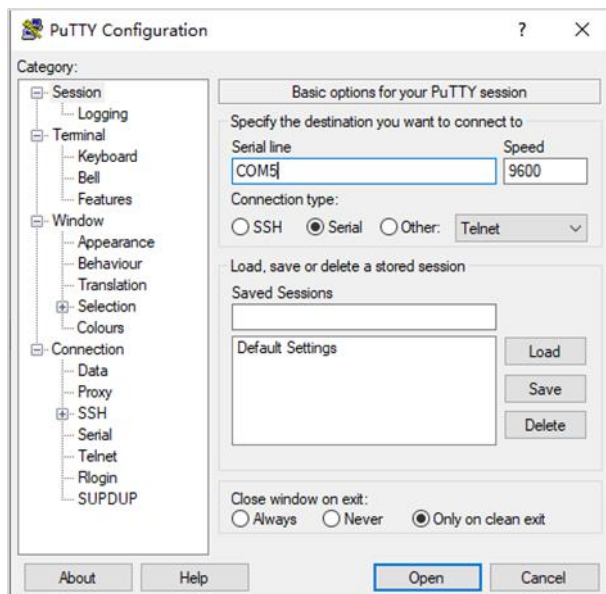
步骤 2 查看管理 PC 连接设备所使用的 Serial COM 的端口号。

选择“控制面板 > 硬件和声音 > 设备和打印机 > 设备管理器 > 端口”，查看 Serial Port 的端口号。



步骤 3 在管理 PC 上运行 PuTTY 并配置参数。

选择“Session”，Connection type 协议为“Serial”，Serial line 处配置端口，端口为步骤二查询到的 Serial COM 端口 COM5，其余参数按照如图所示配置。



1.1.3 结果验证

按下回车键在 PuTTY 上出现以下内容时，说明通过 Console 口登录设备成功。



1.1.4 思考题

在管理 PC 上插上 Console 线，但是在管理 PC 的“控制面板 > 硬件和声音 > 设备和打印机 > 设备管理器 > 端口”中未查看到 Serial Port 的端口号，可能有哪些原因？有哪些对应的解决办法？

参考答案：

- 1.管理 PC 未安装 Console 线的驱动。尝试扫描驱动并安装即可，注意不同 Console 线需要安装的驱动可能不同，建议先排除驱动安装问题。
- 2.Console 线有问题。尝试替换其他 Console 线缆。
- 3.电脑接口接触不良。尝试重新插拔调试线缆，或者更换新的调试线缆。

1.2 熟悉命令行（PuTTY）

1.2.1 实验介绍

1.2.1.1 关于本实验

在设备出厂配置下，PC 终端通过 Console 口登录设备，可以对设备进行命令行的基本操作。

1.2.1.2 实验目的

通过本实验，熟悉命令行的基本操作。

1.2.1.3 实验组网介绍

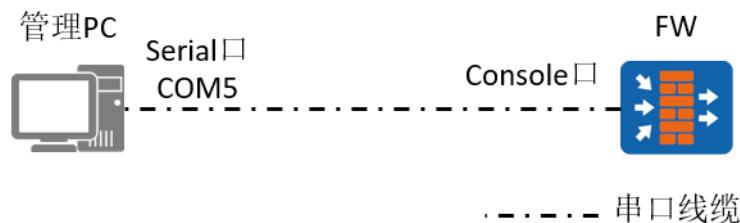


图1-2 通过 Console 口登录设备拓扑图

1.2.1.4 实验背景

如组网图所示，FW 是一台全新无配置的防火墙，网络管理员在拿到该设备后，需要对防火墙做一些调试，了解防火墙命令行操作等，故需要使用 PC 通过串口线缆连接到 FW 的 Console 口，使用 PuTTY 软件登陆设备，并对 FW 进行一些初始化操作。

1.2.1.5 实验规划

管理 PC 使用串口线缆连接设备的 Console 口，管理 PC 通过 PuTTY 软件登录设备。

表1-2 设备端口及参数说明

设备	端口	端口类型	说明
管理PC	COM5	以太网口	串口线缆在管理PC端是USB接口或者串口，电脑上需要安装驱动，查看并使用对应的端口号。
防火墙设备	Console	Console口	设备面板有Console接口标识。

1.2.2 实验任务配置

1.2.2.1 配置思路

- 1.通过 Console 口登录设备。
- 2.对设备进行基本的命令行配置。

1.2.2.2 配置步骤

步骤 1 通过 Console 口登录设备。

步骤 2 进入系统视图。

系统将命令行接口划分为若干个命令视图，系统的所有命令都注册在某个（或某些）命令视图下，只有在相应的视图下才能执行该视图下的命令。与防火墙建立连接后需要输入用户名和初始密码，并修改为新密码。大部分命令需要在系统视图下进行配置，所以配置之前需要先从用户视图进入系统视图，命令如下：

```
Press ENTER to get started.
Login authentication
Username:admin
Password:
The password needs to be changed. Change now? [Y/N]: Y
Please enter old password:
Please enter new password:
Please confirm new password:

Info: Your password has been changed. Save the change to survive a reboot.
*****
*          Copyright (C) 2014-2020 Huawei Technologies Co., Ltd.          *
*                               All rights reserved.                       *
*          Without the owner's prior written consent,                     *
*          no decompiling or reverse-engineering shall be allowed.         *
*****
<FW> system
[FW]
```

步骤 3 进入接口视图。

在系统视图下，可以键入不同的配置命令进入相应的协议、接口等视图。以进入接口视图为例，命令如下：

```
[FW] interface GigabitEthernet 0/0/1
[FW-GigabitEthernet0/0/1]
```

步骤 4 在线帮助。

“?” 为 VRP 平台提供的在线帮助之一（注意：输入时必须使用英文输入法）。在系统视图下直接键入问号，系统便会列出在系统视图下可以配置的命令参数，或者在参数后键入空格，

然后再键入问号，便可获得该参数后可以使用的参数列表，如果是键入一段字符串，其后紧接键入问号，则系统会列出以该字符串开头的所有命令。如：

```
[FW] interface ?  
Cellular          Cellular interface  
Dialer            Dialer interface  
Eth-Trunk         Ethernet-Trunk interface  
GigabitEthernet  GigabitEthernet interface  
LoopBack         LoopBack interface  
NULL             NULL interface  
Nve              Nve interface  
Tunnel           Tunnel interface  
Vbdif            Vbdif interface  
Virtual-Template Virtual-Template interface
```

Tab 键也是 VRP 平台提供的在线帮助之一。输入命令的某个关键字的前几个字母，按下 <TAB> 键，可以显示出完整的关键字，也可以在符合该字母的所有命令之间进行切换。

```
[FW] inter //键入“Tab”  
[FW] interface
```

步骤 5 退出视图。

当完成某项配置，需要回退到上一视图时，可以使用“quit”命令，以退出接口视图为例：

```
[FW-GigabitEthernet0/0/1] quit  
[FW]
```

步骤 6 回到用户视图。

当需要从其他视图回到用户视图时，可以使用“return”命令，如：

```
[FW-GigabitEthernet0/0/1] return  
<FW>
```

步骤 7 查看设备版本。

可以在任意视图下查看设备版本，命令为“display version”，如：

```
<FW> display version  
Huawei Versatile Routing Platform Software  
VRP (R) Software, Version 5.170 (USG6500 V600R007C20)  
Copyright (C) 2014-2020 Huawei Technologies Co., Ltd.
```

步骤 8 保存配置。

保存设备所有配置，使用“save”命令，需要在用户视图下执行该命令：

```
<FW> save  
The current configuration will be written to hda1:/fw2.zip.  
Are you sure to continue?[Y/N]Y  
Now saving the current configuration to the slot 0..  
Jan 19 2022 10:13:19 FW %%01CFM/4/SAVE(s)[0]:The user chose Y when deciding whether to save the  
configuration to the device.....
```

```
Save the configuration successfully.
```

步骤 9 查看配置。

查看当前视图下的配置，在当前视图下使用命令“display this”，以接口视图为例：

```
[FW-GigabitEthernet0/0/0] display this
#
interface GigabitEthernet0/0/0
undo shutdown
ip address 192.168.0.1 255.255.255.0
#
Return
```

查看当前所有配置，包括当前未被保存的配置，可以在任意视图执行该命令，使用命令如下：

```
[FW] display current-configuration
```

查看当前已保存的配置，可以在任意视图执行该命令，使用命令如下：

```
[FW] display saved-configuration
```

1.2.3 思考题

通过 PuTTY 登录设备后，在配置命令过程中，偶尔会出现乱码，应该如何解决？

参考答案：

检查 PuTTY 的字符编码是否为 UTF-8 格式，若非此格式，请重新设置 PuTTY 软件的字符编码格式。

1.3 通过 Telnet 登录设备

1.3.1 实验介绍

1.3.1.1 关于本实验

网络管理员在维护网络过程中，经常需要登录很多设备，通过 Console 口登录每台设备比较困难，为方便维护与调试设备，通过在设备上配置远程登录功能，使远程管理员能够通过 Telnet 方式远程登录到设备上进行管理。

1.3.1.2 实验目的

通过本实验，掌握配置设备 Telnet 远程登录功能的基本方法。

1.3.1.3 实验组网介绍

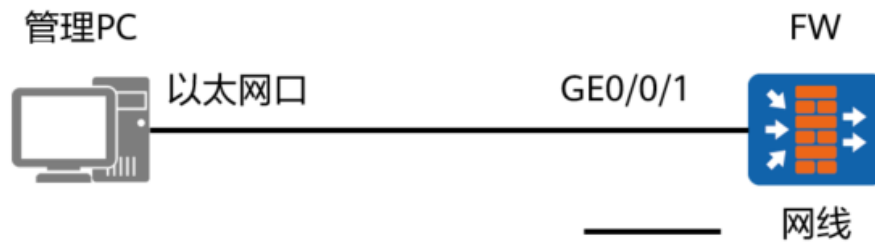


图1-3 通过 Telnet 方式登录设备拓扑图

1.3.1.4 实验规划

管理 PC 使用普通网线连接设备的 GE0/0/1 口，管理 PC 通过 PuTTY 软件远程登录设备。

表1-3 设备端口及参数说明

设备	端口	端口类型	地址
管理PC	以太网接口	以太网口	10.1.2.100/24
防火墙设备	GE0/0/1	以太网口	10.1.2.1/24

1.3.2 实验任务配置

1.3.2.1 配置思路

- 1.使用其他方式登录到设备上（如 Console 登录）。
- 2.在设备上配置 Telnet 功能。
- 3.在管理 PC 上登录测试。

1.3.2.2 配置步骤 – CLI

步骤 1 通过其他方式登录到设备上（如 Console 登录，具体方法参照实验 1.1 通过 Console 口登录设备）。

步骤 2 在设备上开启 Telnet 功能。

```
<FW> system-view
[FW] telnet server enable
```

步骤 3 配置登录接口。

配置接口的 IP 地址用于登录。

```
[FW] interface GigabitEthernet 0/0/1
[FW-GigabitEthernet0/0/1] ip address 10.1.2.1 24
```

配置接口的访问控制功能。

```
[FW-GigabitEthernet0/0/1] service-manage enable
```

```
[FW-GigabitEthernet0/0/1] service-manage telnet permit
[FW-GigabitEthernet0/0/1] quit
```

配置接口加入安全区域。

```
[FW] firewall zone trust
[FW-zone-trust] add interface GigabitEthernet0/0/1
[FW-zone-trust] quit
```

配置安全策略，允许管理 PC 访问防火墙的 GE0/0/1。

```
[FW] security-policy
[FW-policy-security] rule name trust-local
[FW-policy-security-rule-trust-local] source-zone trust
[FW-policy-security-rule-trust-local] destination-zone local
[FW-policy-security-rule-trust-local] action permit
```

备注：如使用防火墙 MGMT 口进行远程登录，则不需要配置步骤三。

步骤 4 配置管理员信息。

配置 VTY 管理员认证方式为 AAA。

```
[FW] user-interface vty 0 4
[FW-ui-vty0-4] authentication-mode aaa
[FW-ui-vty0-4] protocol inbound telnet
[FW-ui-vty0-4] user privilege level 3
[FW-ui-vty0-4] quit
```

配置 Telnet 管理员。

```
[FW] aaa
[FW-aaa] manager-user telnetuser
[FW-aaa-manager-use-telnetuser] password cipher (Enter password)
[FW-aaa-manager-use-telnetuser] service-type telnet
[FW-aaa-manager-use-telnetuser] level 3
[FW-aaa-manager-use-telnetuser] quit
```

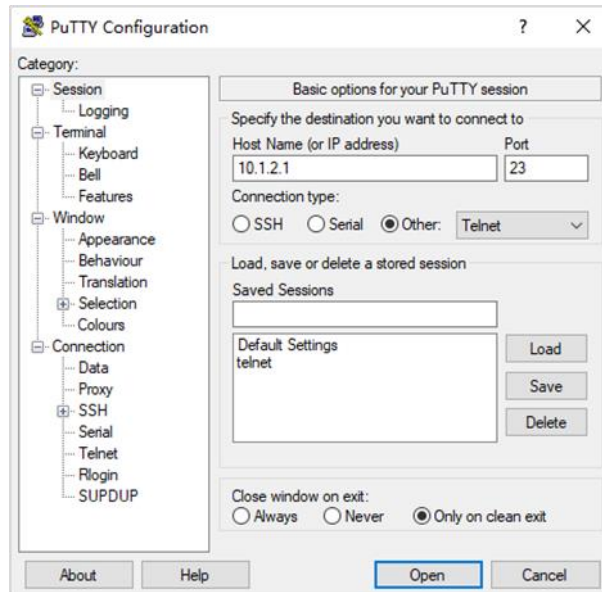
为管理员绑定角色（可选，仅防火墙支持）。

```
[FW-aaa] bind manager-user telnetuser role system-admin
```

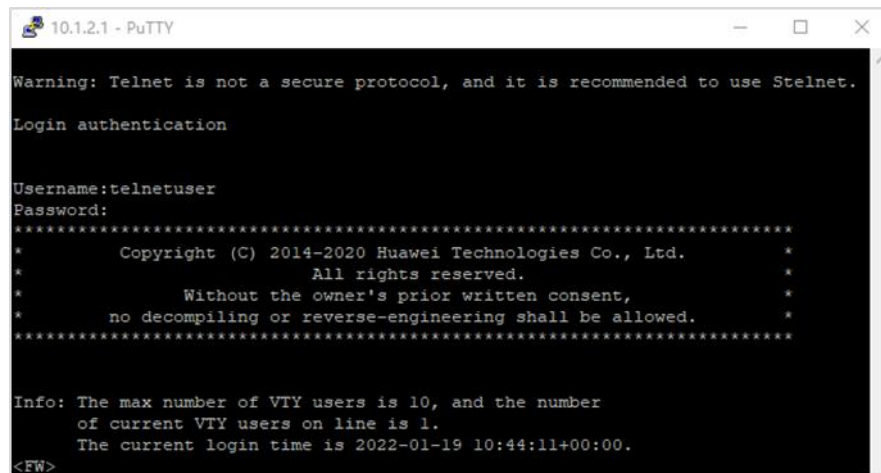
步骤 5 登录设备。

在管理 PC 上配置地址为 10.1.2.100/24，运行 PuTTY，填写设备 Telnet 参数，登录设备。

选择“Session”，Connection type 协议选择“Telnet”，Host Name (or IP address)填写“10.1.2.1”，其余参数按照如图所示配置。



点击“Open”连接，出现如下现象，表示成功使用 Telnet 方式登录设备。



1.3.2.3 配置步骤 – Web（仅防火墙支持）

步骤 1 通过默认 Web 方式登录到设备上（具体方法参照实验 1.5 通过默认 Web 方式登录设备）。

步骤 2 开启 Telnet 服务。

选择“系统 > 管理员 > 设置”，勾选 Telnet 服务复选框。

步骤 3 配置登录接口。

配置用于登录的接口进行配置。选择“网络 > 接口 > GE0/0/1”，点击“编辑”。

配置接口的 IP 地址、安全区域、访问控制功能。

修改GE

接口名称

GE0/0/1

描述

虚拟系统?

public

VPN实例

public

安全区域

trust

模式?

☒ 路由
☐ 交换
☐ 旁路检测
☐ 接口对

IPv4

IPv6

连接类型

☒ 静态IP
☐ DHCP

IP地址

10.1.2.1/24

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".

默认网关

接口带宽

入方向带宽

kbit/s

<60-1000000>

过载保护阈值?

%

出方向带宽

kbit/s

<60-1000000>

过载保护阈值?

%

访问控制管理

☒ HTTP
☒ HTTPS
☒ Ping
☒ SSH
☒ Telnet
☒ NETCONF
☒ SNMP

高级

自协商

☒

IPv4 MTU?

1500

<46-9550>字节

IPv6 MTU?

1500

<1280-9550>字节

ARP严格学习

☐

取消

确定

备注：如使用防火墙 MGMT 口进行远程登录，则不需要配置步骤三。

步骤 4 配置管理员信息。

选择“系统 > 管理员 > 管理员”，单击“新建”。



配置 Telnet 用户名为 telnetuser，密码为 Admin@123，管理员角色为“系统管理员”，并勾选 Telnet 服务类型。

新建管理员

* 用户名

telnetuser

密码

.....

密码为 8-128 个字符
 为提升密码安全性，建议密码至少包含以下字符中的4种：
 <A-Z>，<a-z>，<0-9>，特殊字符（例如!，\$，#，%）。
 且密码不能与用户名或者用户名的倒序相同。

* 确认密码

.....

用户等级 ①

请选择

* 角色

manage-ug(系统管理员)

高级

接入方式

☒ Web(HTTP/HTTPS)
 ☒ Telnet
 ☐ SSH
 ☐ Console
 ☐ FTP

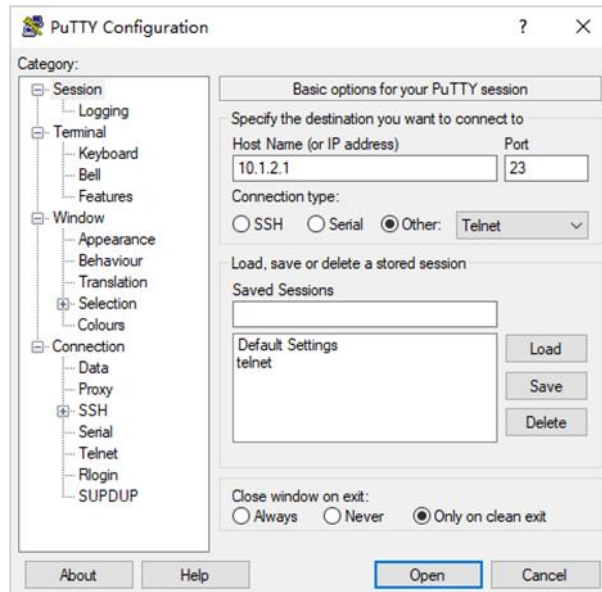
取消

确定

步骤 5 登录设备。

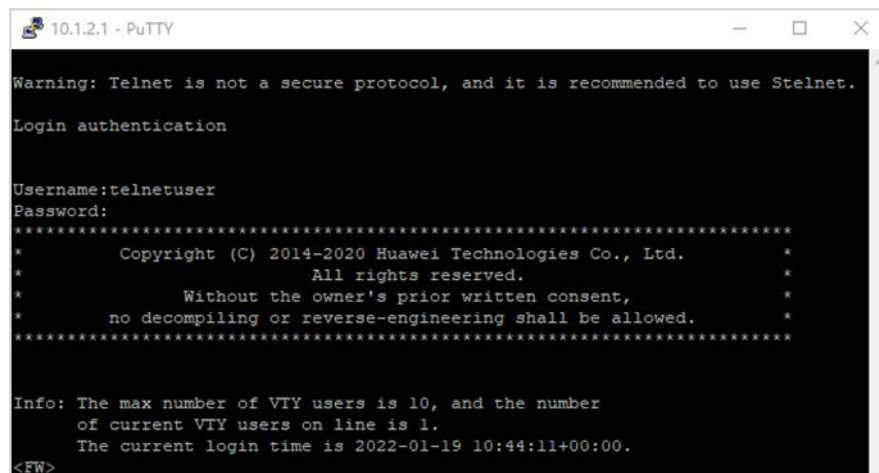
在管理 PC 上配置地址为 10.1.2.100/24，运行 PuTTY，填写设备 Telnet 参数，登录设备。

选择“Session”，Connection type 协议选择“Telnet”，Host Name (or IP address)填写“10.1.2.1”，其余参数按照如图所示配置。



1.3.3 结果验证

点击步骤 5 的“Open”连接，按下回车键，输入用户名 telnetuser，密码 Admin@123，当 PuTTY 界面上出现以下信息时，说明 Telnet 登录设备成功。



1.3.4 思考题

Telnet 登录设备使用的端口号是 TCP 23，Telnet 登录方式是否可以更改为其他端口号？如果可以修改，对应的命令是什么？修改完成以后，查看当前 Telnet 连接端口号的命令是什么？

参考答案：

- 1.可以使用 telnet server port *port-number* 命令行设置 Telnet 服务器的侦听端口号。
- 2.Telnet 侦听端口号修改完成以后，可以使用 display telnet server status 命令行查看当前 Telnet 服务器正在使用的侦听端口号。

1.4 通过 SSH 登录设备

1.4.1 实验介绍

1.4.1.1 关于本实验

网络管理员在维护网络过程中，经常需要登录很多设备，通过 Console 口登录每台设备比较困难，且 Telnet 远程登录设备的报文是明文，为更加安全，通过在设备上配置 SSH 功能，使远程管理员能够通过 SSH 方式登录到设备上进行管理。

1.4.1.2 实验目的

通过本实验，掌握配置设备 SSH 远程登录功能的基本方法。

1.4.1.3 实验组网介绍

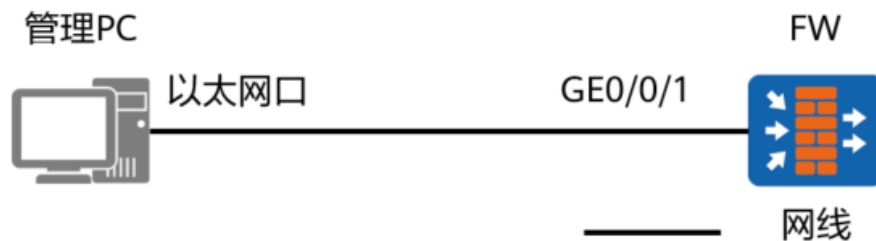


图1-4 通过 SSH 方式登录设备拓扑图

1.4.1.4 实验规划

管理 PC 使用普通网线连接设备的 GE0/0/1 口，管理 PC 通过 PuTTY 软件远程登录设备。

表1-4 设备端口及参数说明

设备	端口	端口类型	地址
管理PC	电脑网口	以太网口	10.1.2.100/24
防火墙设备	GE0/0/1	以太网口	10.1.2.1/24

1.4.2 实验任务配置

1.4.2.1 配置思路

- 1.使用其他方式登录到设备上（如 Console 登录）。
- 2.在设备上配置 SSH 功能。
- 3.在管理 PC 上登录测试。

1.4.2.2 配置步骤 – CLI

步骤 1 通过其他方式登录到设备上（如 Console 登录，具体方法参照实验 1.1 通过 Console 口登录设备）。

步骤 2 在设备上开启 SSH 功能。

```
<FW> system-view
[FW] stelnet server enable
```

步骤 3 配置登录接口。

配置接口的 IP 地址用于登录。

```
[FW] interface GigabitEthernet 0/0/1
[FW-GigabitEthernet0/0/1] ip address 10.1.2.1 24
```

配置接口的访问控制功能。

```
[FW-GigabitEthernet0/0/1] service-manage enable
[FW-GigabitEthernet0/0/1] service-manage ssh permit
[FW-GigabitEthernet0/0/1] quit
```

配置接口加入安全区域。

```
[FW] firewall zone trust
[FW-zone-trust] add interface GigabitEthernet0/0/1
[FW-zone-trust] quit
```

配置安全策略，允许管理 PC 访问防火墙的 GE0/0/1。

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

备注：如使用防火墙 MGMT 口进行远程登录，则不需要配置步骤三。

步骤 4 配置管理员信息。

配置 VTY 管理员认证方式为 AAA。

```
[FW] user-interface vty 0 4
[FW-ui-vty0-4] authentication-mode aaa
[FW-ui-vty0-4] protocol inbound ssh
[FW-ui-vty0-4] user privilege level 3
[FW-ui-vty0-4] quit
```

创建 SSH 管理员账号 sshuser，指定认证方式为 password，并配置密码为 Admin@123，服务方式为 SSH。

```
[FW] aaa
[FW-aaa] manager-user sshuser
```

```
[FW-aaa-manager-use-sshuser] password cipher (Enter password)
[FW-aaa-manager-use-sshuser] service-type ssh
[FW-aaa-manager-use-sshuser] level 3
[FW-aaa-manager-use-sshuser] quit
```

为管理员绑定角色（可选，仅防火墙支持）。

```
[FW-aaa] bind manager-user sshuser role system-admin
```

配置 SSH 用户。

```
[FW] ssh user sshuser
[FW] ssh user sshuser authentication-type password
[FW] ssh user sshuser service-type stelnet
```

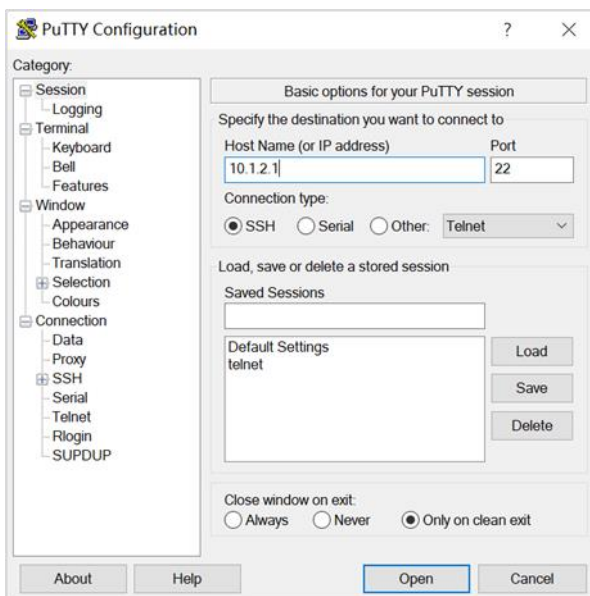
步骤 5 生成本地密钥对。

```
[FW] rsa local-key-pair create
The key name will be: FW_Host
The range of public key size is (512 ~ 2048).
NOTES: A key shorter than 1024 bits may cause security risks.
       The generation of a key longer than 512 bits may take several minutes.
Input the bits in the modulus[default = 2048]:
Generating keys...
...+++++++
..+++++++
.....+++++++
.....+++++++
```

步骤 6 登录设备。

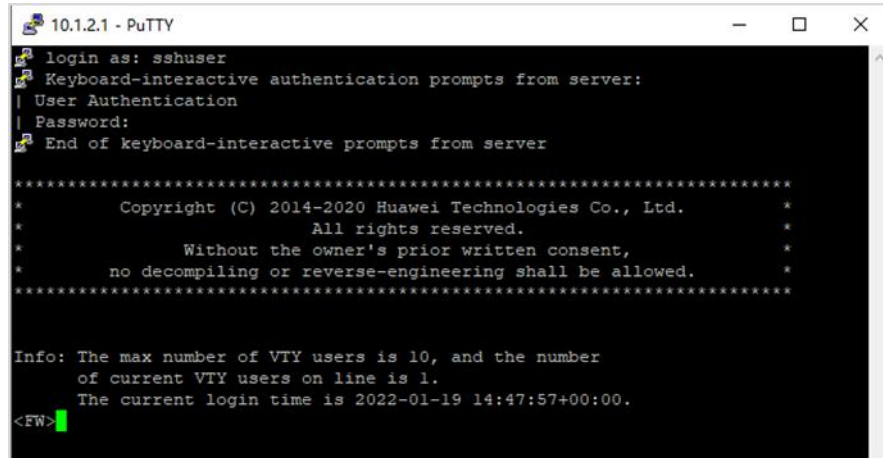
在管理 PC 上配置地址为 10.1.2.100/24，运行 PuTTY，填写设备 SSH 参数，登录设备。

选择“Session”，Connection type 协议选择“SSH”，Host Name (or IP address)填写“10.1.2.1”，其余参数按照如图所示配置。



1.4.3 结果验证

点击步骤 6 的“Open”连接，按下回车键，输入用户名 sshuser，密码 Admin@123，当 PuTTY 界面上出现以下信息时，说明 SSH 登录设备成功。



```
10.1.2.1 - PuTTY
login as: sshuser
Keyboard-interactive authentication prompts from server:
| User Authentication
| Password:
| End of keyboard-interactive prompts from server

*****
*      Copyright (C) 2014-2020 Huawei Technologies Co., Ltd.      *
*      All rights reserved.                                       *
*      Without the owner's prior written consent,                *
*      no decompiling or reverse-engineering shall be allowed.    *
*****

Info: The max number of VTY users is 10, and the number
      of current VTY users on line is 1.
      The current login time is 2022-01-19 14:47:57+00:00.
<FW>
```

1.4.4 思考题

本实验 SSH 登录设备属于哪种类型？是否还有其他形式的 SSH 安全登录形式？如果有，请举例并列举安全验证登录的关键步骤。

参考答案：

1. 本实验是 SSH 基于口令的安全验证方式。

2. SSH 安全验证分为：基于口令的安全验证和基于密钥的安全验证。

3. SSH 基于口令的安全验证登录步骤：

- 用户发起登陆请求；
- 远程主机将自己的公钥返回给请求主机；
- 请求主机使用公钥对用户输入的密码进行加密；
- 请求主机将加密后的密码发送给远程主机；
- 远程主机使用私钥对密码进行解密；
- 最后，远程主机判断解密后的密码是否与用户密码一致，如果一致则登录成功。

4. SSH 基于密钥的安全验证登录步骤：

- 用户主机生成密钥对，并将公钥导入远程主机；
- 用户发起登陆请求；
- 远程主机向用户返回一个随机串；
- 用户所在主机使用私钥对这个随机串进行加密，并将加密后的随机串返回至远程主机；
- 最后，远程主机使用导入进来的公钥对加密随机串进行解密。如果解密成功，就证明用户的登陆信息是正确的，则允许登陆。

1.5 通过默认 Web 方式登录设备

1.5.1 实验介绍

1.5.1.1 关于本实验

工程师在拿到一台全新的防火墙时，往往希望使用 Web 页面的方式来调试设备。在设备出厂配置下，PC 终端可以通过防火墙管理口 MGMT 登录设备，可实现对设备的管理和配置。

1.5.1.2 实验目的

通过本实验，掌握 PC 终端通过默认 Web 方式登录防火墙的方法。

1.5.1.3 实验组网介绍

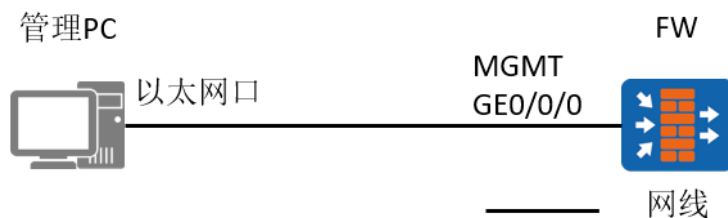


图1-5 通过默认 Web 方式登录设备拓扑图

1.5.1.4 实验规划

管理 PC 使用普通网线连接设备的 MGMT 网口，管理 PC 通过 Web 浏览器登录设备。

表1-5 设备端口及参数说明

设备	端口	端口类型	IP地址
管理PC	电脑网口	以太网口	192.168.0.2/24
防火墙设备	GigabitEthernet0/0/0	以太网口	192.168.0.1/24

1.5.2 实验任务配置

1.5.2.1 配置思路

- 1.使用双绞线连接管理 PC 的以太网口和设备的 MGMT 接口。
- 2.在管理 PC 上使用浏览器访问防火墙。

1.5.2.2 配置步骤

- 步骤 1 设备建立连接后，将所有设备上电，并且保证设备运行正常。将管理员 PC 网口与设备的管理口（MEth 0/0/0）通过网线或者二层交换机相连。
- 步骤 2 将管理员 PC 的 IP 地址设置为与设备管理口 IP 地址同一网段。设备管理口缺省 IP 地址是 192.168.0.1，设置 PC 为 192.168.0.2 ~ 192.168.0.254 范围内的 IP 地址。

步骤 3 在浏览器中输入地址：https://ip-address:8443。ip-address 为设备管理口 IP 地址。输入地址登录后，浏览器会给出证书不安全的告警提示，此时可以选择继续浏览。

步骤 4 浏览器无法验证设备提供的默认证书，因此会有安全告警提示，登录后可以更换设备证书，消除告警。

步骤 5 如果是首次登录设备，设备会弹出创建管理员帐号界面。按照系统提示输入用户名、密码、确认密码，然后单击“创建”，即可完成 Web 管理员帐号的创建。

（注意：缺省情况下，设备管理口 Meth0/0/0 的 IP 地址是 192.168.0.1，并开启了 HTTPS 管理。对于 USG6510F-D、USG6510F-DK、USG6510F-DL、USG6530F-D、USG6530F-DL 使用 GE0/0/0 作为管理接口。）



The image shows a web form titled "创建帐号" (Create Account). It contains three input fields: the first is labeled "admin", the second and third are masked with dots. Below the input fields is a blue button labeled "创建" (Create).

1.5.3 结果验证

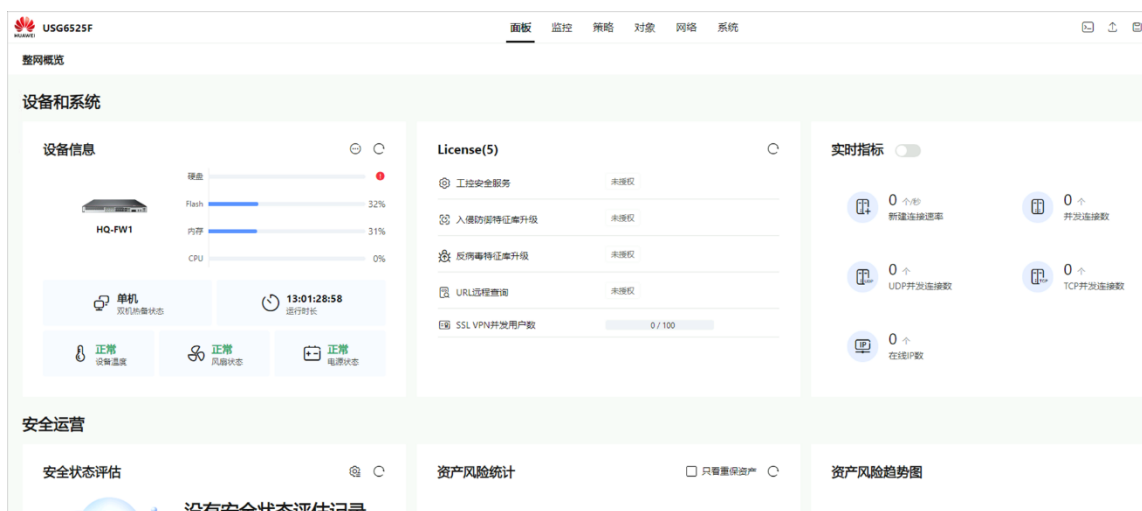
输入用户名 admin，密码 Admin@123，点击“登录”。

登录

6pb65

[下载根证书](#) | [简体中文](#)

在浏览器界面上出现以下信息，说明登录防火墙成功。



1.5.4 思考题

缺省情况下，默认 Web 方式登录设备的接口是哪一个？是否需要通过命令行方式手动开启 Web 服务？

参考答案：

缺省情况下，设备管理口 Meth0/0/0 的 IP 地址是 192.168.0.1，并开启了 HTTPS 管理。对于 USG6510F-D、USG6510F-DK、USG6510F-DL、USG6530F-D、USG6530F-DL 使用 GE0/0/0 作为管理接口，无需手动开启 Web 服务，无需配置安全策略放通。

1.6 通过 Web 方式登录设备

1.6.1 实验介绍

1.6.1.1 关于本实验

防火墙加入网络后，工程师希望通过管理 PC 登录防火墙的管理页面，此时管理口 MGMT 未接入网络，PC 终端通过防火墙业务口以 Web 方式登录设备，可实现对设备的管理和配置。

1.6.1.2 实验目的

通过本实验，掌握 PC 终端通过 Web 方式登录防火墙的方法。

1.6.1.3 实验组网介绍

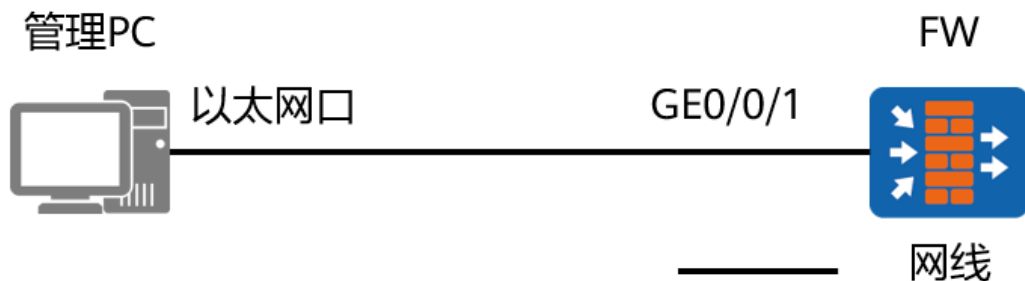


图1-6 通过 Web 方式登录设备拓扑图

1.6.1.4 实验规划

管理 PC 使用网线连接设备的 GE0/0/1 口，管理 PC 通过 Web 浏览器登录设备。

表1-6 设备端口及参数说明

设备	端口	端口类型	IP地址	说明
管理PC	网口	以太网口	10.1.2.100/24	
防火墙设备	GE0/0/1	以太网口	10.1.2.1/24	设备业务口默认不支持Web方式登录，所以需要开启Web功能以及配置Web登录的账号密码等。

1.6.2 实验任务配置

1.6.2.1 配置思路

- 1.使用双绞线连接管理 PC 的以太网口和设备的业务接口。
- 2.配置设备的 Web 登录功能。
- 3.在管理 PC 上进行登录测试。

1.6.2.2 配置步骤 - CLI

步骤 1 设备建立连接后，将所有设备上电，并且保证设备运行正常。

步骤 2 通过其他方式登录到设备上（如 Console，Telnet，SSH 等，详情请参照实验 1.1，1.2 和 1.3）。

步骤 3 检查是否已经启动 Web 服务器功能。如未启动，使用如下命令开启。

```
[FW] web-manager security enable
```

备注：执行 web-manager security enable 命令，表示开启 HTTPS 设备管理。若配置命令为 web-manager enable，表示开启 HTTP 设备管理。不容许 HTTPS 和 HTTP 设备管理使用相同的端口，否则会导致端口冲突。

步骤 4 配置登录接口。

配置接口 IP 地址以及接口的访问控制功能。

```
[FW] interface GigabitEthernet 0/0/1
[FW-GigabitEthernet0/0/1] ip address 10.1.2.1 24
[FW-GigabitEthernet0/0/1] service-manage enable
[FW-GigabitEthernet0/0/1] service-manage https permit
[FW-GigabitEthernet0/0/1] quit
```

配置接口加入安全区域。

```
[FW] firewall zone trust
[FW-zone-trust] add interface GigabitEthernet 0/0/1
[FW-zone-trust] quit
```

配置安全策略，允许管理 PC 访问防火墙的 GE0/0/1。

```
[FW] security-policy
[FW-policy-security] rule name trust-local
[FW-policy-security-rule-trust-local] source-zone trust
[FW-policy-security-rule-trust-local] destination-zone local
[FW-policy-security-rule-trust-local] action permit
```

步骤 5 配置管理员信息。

```
[FW] aaa
[FW-aaa] manager-user webuser
[FW-aaa-manager-use-webuser] password cipher (Enter password)
[FW-aaa-manager-use-webuser] level 3
[FW-aaa-manager-use-webuser] service-type web
[FW-aaa-manager-use-webuser] quit
```

为管理员绑定角色（可选，仅防火墙支持）。

```
[FW-aaa] bind manager-user webuser role service-admin
```

步骤 6 配置 PC 的 IP 地址为 10.1.2.100/24。PC 的浏览器访问 https://10.1.2.1:8443。

1.6.2.3 配置步骤 - Web

步骤 1 设备建立连接后，将所有设备上电，并且保证设备运行正常。

步骤 2 通过默认 Web 方式登录到设备上（详情请参照实验 1.5）。

步骤 3 开启 HTTPS 服务。

选择“系统 > 管理员 > 设置”，检查 HTTPS 服务复选框是否打开。



The screenshot shows the '配置设备服务' (Configure Device Services) page for a Huawei USG6525F. The left sidebar has '配置' (Configuration) expanded, with '设置' (Settings) selected under '管理员' (Admin). The main area shows the 'HTTPS 服务' (HTTPS Service) configuration. The 'HTTPS 服务' toggle is turned on. Below it, 'HTTPS 服务端口' (HTTPS Service Port) is set to 8443. '绑定任意接口' (Bind Any Interface) is disabled. '绑定接口' (Bind Interface) is set to MEth0/0/0. '绑定 IP' (Bind IP) is empty. 'Web 登录验证码' (Web Login Verification) is disabled. 'Web 服务超时时间' (Web Service Timeout) is 1440. 'Web 最大在线管理员数' (Web Max Online Admins) is 200. '用户名复杂度检查' (User Name Complexity Check) is enabled. '本地用户密码策略' (Local User Password Policy) shows '密码复杂度检查' (Password Complexity Check) with 4 types of characters selected, '密码最小长度' (Password Min Length) as 8, and '密码有效期' (Password Validity) as 0. '用户名密码相似性检查' (User Name Password Similarity Check) is enabled. '本地用户锁定策略' (Local User Lock Policy) is disabled. '服务器用户锁定策略' (Server User Lock Policy) is enabled. '连续登录失败时间间隔' (Continuous Login Failure Time Interval) is 5.

配置用于登录的接口进行配置。选择“网络 > 接口 > GE0/0/1”，点击“编辑”，配置接口的 IP 地址、安全区域、访问控制功能。

修改GE

接口名称

GE0/0/1

描述

虚拟系统?

public

VPN实例

public

安全区域

trust

模式?

☒ 路由
☐ 交换
☐ 旁路检测
☐ 接口对

IPv4

IPv6

连接类型

☒ 静态IP
☐ DHCP

IP地址

10.1.2.1/24

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".

默认网关

接口带宽

入方向带宽

kbit/s

<60-1000000>

过载保护阈值?

%

出方向带宽

kbit/s

<60-1000000>

过载保护阈值?

%

访问控制管理

☒ HTTP
☒ HTTPS
☒ Ping
☒ SSH
☒ Telnet
☒ NETCONF
☒ SNMP

高级

自协商

☒

IPv4 MTU?

1500

<46-9550>字节

IPv6 MTU?

1500

<1280-9550>字节

ARP严格学习

☐

取消

确定

配置管理员信息。

选择“系统 > 管理员 > 管理员”，单击“新建”，配置 Web 用户名为 webuser，密码为 Admin@123，管理员角色为“系统管理员”。

1.6.4 思考题

通过非管理接口登录设备 Web 页面需要哪些关键配置？

参考答案：

- 1.接口下需要开启 HTTPS 访问服务，并加入安全区域。
- 2.接口所属安全区域到 local 区域的安全策略需要放通。
- 3.开启全局 HTTPS 服务。

2 防火墙安全策略实验

2.1 实验介绍

2.1.1 关于本实验

在开局及维护网络过程中，希望使用防火墙对网络进行一定的防护，本实验介绍了安全区域与安全策略等重点概念，本实验通过在防火墙上部署安全策略，保证 trust 区域主机能够主动访问 untrust 区域的主机。

2.1.2 实验目的

- 理解安全策略原理；
- 理解不同安全区域之间的关系；
- 掌握通过命令行和 Web 方式配置防火墙安全策略。

2.1.3 实验组网介绍

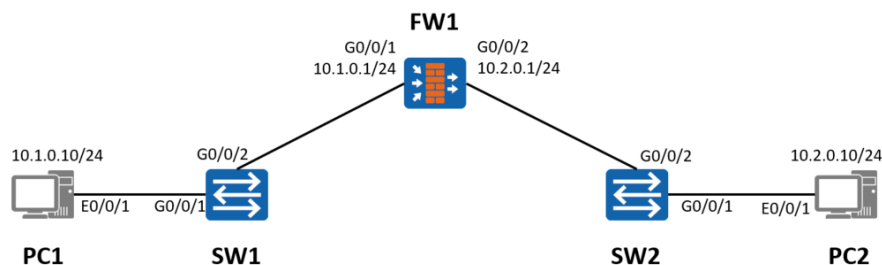


图2-1 防火墙安全策略实验拓扑图

2.1.4 实验规划

FW1 被部署在两个网络之间。其中上下行设备均是交换机，且 FW1 上下行业务接口工作在三层。

表2-1 端口地址和区域划分

设备	接口	IP地址	安全区域
FW1	GigabitEthernet0/0/1	10.1.0.1/24	trust
	GigabitEthernet0/0/2	10.2.0.1/24	untrust

PC1	Eth0/0/1	10.1.0.10/24	trust
PC2	Eth0/0/1	10.2.0.10/24	untrust

2.2 实验任务配置

2.2.1 配置思路

- 1.配置基本的 IP 地址和所属安全区域。
- 2.配置域间安全策略。
- 3.PC1 与 PC2 的网关需要配置为防火墙对应同网段的接口 IP 地址。

2.2.2 配置步骤 - CLI

步骤 1 完成 FW1 上下行业务接口的配置。配置各接口 IP 地址并加入相应安全区域。

```
[FW1] interface G0/0/1
[FW1-GigabitEthernet0/0/1] ip address 10.1.0.1 255.255.255.0
[FW1-GigabitEthernet0/0/1] quit
[FW1] interface G0/0/2
[FW1-GigabitEthernet0/0/2] ip address 10.2.0.1 255.255.255.0
[FW1-GigabitEthernet0/0/2] quit
[FW1] firewall zone trust
[FW1-zone-trust] add interface G0/0/1
[FW1-zone-trust] quit
[FW1] firewall zone untrust
[FW1-zone-untrust] add interface G0/0/2
[FW1-zone-untrust] quit
```

步骤 2 配置 trust 区域和 untrust 区域的域间转发策略。

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

步骤 3 配置 Switch。

分别将两台 Switch 的两个接口加入同一个 VLAN，缺省 VLAN 即可，如需配置请参考交换机的相关文档。

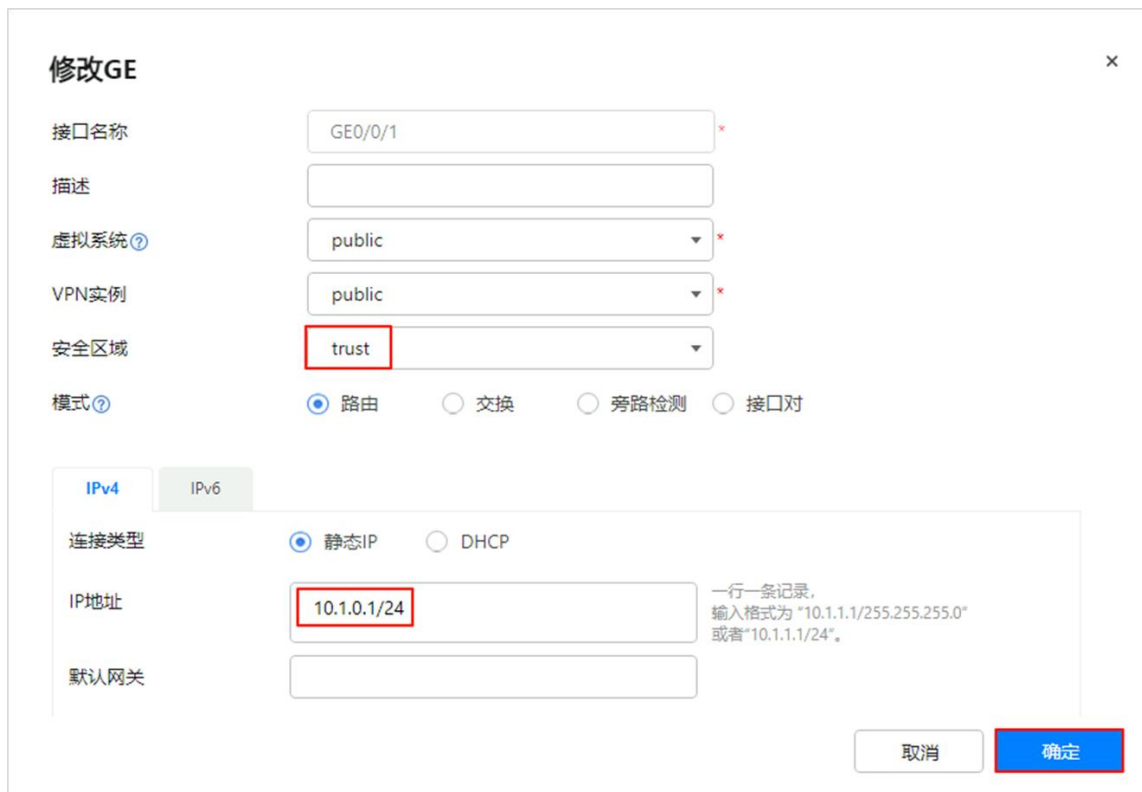
步骤 4 配置 PC。

配置 PC1 的 IP 地址为 10.1.0.10/24，网关为 10.1.0.1；配置 PC2 的 IP 地址为 10.2.0.10/24，网关为 10.2.0.1。

2.2.3 配置步骤 - Web

步骤 1 完成 FW1 防火墙接口配置。

选择“网络 > 接口”，单击需要配置接口后面的配置按钮。依次选择或输入各项参数，单击“确定”。完成 GigabitEthernet0/0/1 接口配置如图所示：



修改GE

接口名称: GE0/0/1

描述:

虚拟系统: public

VPN实例: public

安全区域: trust

模式: ☒ 路由 ☐ 交换 ☐ 旁路检测 ☐ 接口对

IPv4 | IPv6

连接类型: ☒ 静态IP ☐ DHCP

IP地址: 10.1.0.1/24

默认网关:

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**

选择“网络 > 接口”，单击需要配置接口后面的配置按钮。依次选择或输入各项参数，单击“确定”。完成 GigabitEthernet0/0/2 接口配置如图所示：

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

模式?

☒ 路由
☐ 交换
☐ 旁路检测
☐ 接口对

IPv4

IPv6

连接类型

☒ 静态IP
☐ DHCP

IP地址

10.2.0.1/24

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"。

默认网关

取消

确定

步骤 2 完成 FW1 防火墙域间转发策略配置。

trust 与 untrust 间转发策略：选择“策略 > 安全策略 > 安全策略”。在“安全策略列表”中，单击“新建”。依次输入或选择各项参数。单击“确定”。完成 trust 与 untrust 间转发策略如图所示：


```
PC> ping 10.2.0.10
Ping 10.2.0.10: 32 data bytes, Press Ctrl_C to break
From 10.2.0.10: bytes=32 seq=1 ttl=127 time=16 ms
From 10.2.0.10: bytes=32 seq=2 ttl=127 time=16 ms
From 10.2.0.10: bytes=32 seq=3 ttl=127 time=15 ms
From 10.2.0.10: bytes=32 seq=4 ttl=127 time<1 ms
From 10.2.0.10: bytes=32 seq=5 ttl=127 time=16 ms
--- 10.2.0.10 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 0/12/16 ms
```

通过 display firewall session table 命令可以查看防火墙的会话表。

```
[FW1] display firewall session table
Current Total Sessions : 1
icmp VPN: public --> public 10.1.0.10:49569 --> 10.2.0.10:2048
```

2.4 思考题

在本实验的基础上，请尝试使用 PC2 访问 PC1，并说明无法 ping 通的原因。

参考答案：

由于本实验中的安全策略仅放通 PC1 主动访问 PC2 的权限，并未放通 PC2 主动访问 PC1 的权限，所以 PC2 主动向 PC1 发起访问，报文会被防火墙默认安全策略丢弃。

3 防火墙 NAT Server & 源 NAT 实验

3.1 实验介绍

3.1.1 关于本实验

某企业出口设备为一台防火墙，目前该企业内部员工需要通过防火墙访问互联网，并且该企业内部网络中有一台服务器对互联网用户提供服务。

通过在出口防火墙上配置 NAT 技术，可以实现位于企业内网中的多个用户使用少量的公网地址同时访问 Internet，也可以使外网用户通过特定 IP 地址访问内网服务器。

3.1.2 实验目的

- 理解源 NAT 应用场景及原理；
- 理解 NAT Server 应用场景及原理；
- 掌握通过命令行和 Web 方式配置防火墙 NAT Server & 源 NAT 命令。

3.1.3 实验组网介绍

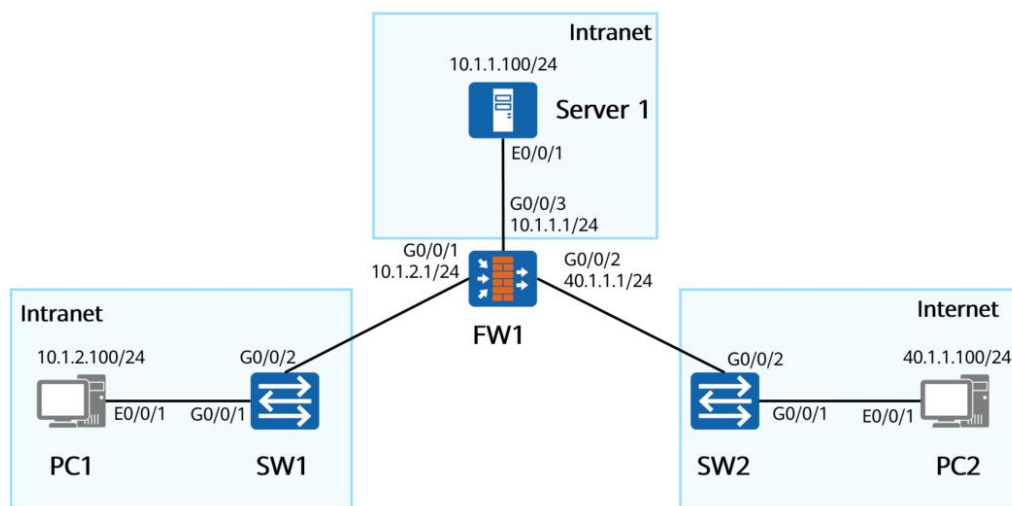


图3-1 防火墙 NAT Server & 源 NAT 实验拓扑图

3.1.4 实验规划

FW1 部署在网络的出口。其中上、下行设备均是交换机。

表3-1 端口地址和区域划分

设备	接口	IP地址	安全区域
FW1	GigabitEthernet0/0/1	10.1.2.1/24	trust
	GigabitEthernet0/0/2	40.1.1.1/24	untrust
	GigabitEthernet0/0/3	10.1.1.1/24	dmz
PC1	Eth0/0/1	10.1.2.100/24	trust
PC2	Eth0/0/1	40.1.1.100/24	untrust
Server 1	Eth0/0/1	10.1.1.100/24	dmz

实验任务配置（源 NAT 实验）

3.1.5 配置思路

- 1.配置基本的 IP 地址和所属安全区域，并且配置对应安全策略。
- 2.配置 NAT 地址池。
- 3.配置 NAT 策略。

3.1.6 配置步骤 - CLI

步骤 1 完成 FW1 上、下行业务接口的配置。配置各接口 IP 地址并加入相应安全区域。

配置 FW1 上、下行业务接口的 IP 地址。

```
<FW1> system-view
[FW1] interface G0/0/1
[FW1-GigabitEthernet0/0/1] ip address 10.1.2.1 255.255.255.0
[FW1-GigabitEthernet0/0/1] quit
[FW1] interface G0/0/2
[FW1-GigabitEthernet0/0/2] ip address 40.1.1.1 255.255.255.0
[FW1-GigabitEthernet0/0/2] quit
[FW1] interface G0/0/3
[FW1-GigabitEthernet0/0/3] ip address 10.1.1.1 255.255.255.0
[FW1-GigabitEthernet0/0/3] quit
```

将 FW1 的接口加入到相应安全区域。

```
[FW1] firewall zone trust
[FW1-zone-trust] add interface G0/0/1
[FW1-zone-trust] quit
[FW1] firewall zone untrust
[FW1-zone-untrust] add interface G0/0/2
[FW1-zone-untrust] quit
[FW1] firewall zone dmz
[FW1-zone-dmz] add interface G0/0/3
```

```
[FW1-zone-dmz] quit
```

步骤 2 配置 trust 区域和 untrust 区域的域间转发策略。

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

步骤 3 配置 NAT 地址池，公网地址范围为 2.2.2.2-2.2.2.5。

```
[FW1] nat address-group natpool
[FW1-address-group-natpool] section 2.2.2.2 2.2.2.5
```

步骤 4 配置 NAT 策略。

```
[FW1] nat-policy
[FW1-policy-nat] rule name source_nat
[FW1-policy-nat-rule-source_nat] destination-zone untrust
[FW1-policy-nat-rule-source_nat] source-zone trust
[FW1-policy-nat-rule-source_nat] action source-nat address-group natpool
```

步骤 5 配置 Switch。

分别将两台 Switch 的两个接口加入同一个 VLAN，缺省 VLAN 即可，如需配置请参考交换机的相关文档。

3.1.7 配置步骤 - Web

步骤 1 完成 FW1 防火墙接口配置。

选择“网络 > 接口”，单击需要配置接口后面的配置按钮。依次选择或输入各项参数，单击“确定”。完成 GigabitEthernet0/0/1 接口配置，如下图所示：

修改GE

接口名称

GE0/0/1

描述

虚拟系统

public

VPN实例

public

安全区域

trust

模式

☒ 路由
☐ 交换
☐ 旁路检测
☐ 接口对

IPv4

IPv6

连接类型

☒ 静态IP
☐ DHCP

IP地址

10.1.2.1/24

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”。

默认网关

取消

确定

选择“网络 > 接口”，单击需要配置接口后面的配置按钮。依次选择或输入各项参数，单击“确定”。完成 GigabitEthernet0/0/2 接口配置，如下图所示：

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

模式

☒ 路由
☐ 交换
☐ 旁路检测
☐ 接口对

IPv4

IPv6

连接类型

☒ 静态IP
☐ DHCP

IP地址

40.1.1.1/24

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”。

默认网关

取消

确定

选择“网络 > 接口”，单击需要配置接口后面的配置按钮。依次选择或输入各项参数，单击“确定”。完成 GigabitEthernet0/0/3 接口配置，如下图所示：

修改GE

接口名称

GE0/0/3

描述

虚拟系统

public

VPN实例

public

安全区域

dmz

模式

☒ 路由
☐ 交换
☐ 旁路检测
☐ 接口对

IPv4

IPv6

连接类型

☒ 静态IP
☐ DHCP

IP地址

10.1.1.1/24

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"。

默认网关

取消

确定

步骤 2 完成 FW1 防火墙域间转发策略配置。

选择“策略 > 安全策略 > 安全策略”，在“安全策略列表”中，单击“新建”，依次输入或选择各项参数，单击“确定”。完成 trust 与 untrust 区域的域间转发策略，如下图所示：

新建安全策略

×

* 名称

policy_sec

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

IP 地址/地区 ②

any

目的

1↓

目的类型

☒ 安全区域
 ☐ 虚拟服务

安全区域

untrust

IP 地址/地区 ②

any

服务 ②

协议

请选择服务

更多

应用/用户/安全组/时间段/VLAN ID

^ 动作

动作

☒ 允许
 ☐ 禁止

内容安全检查

反病毒/入侵防御/URL过滤/内容过滤

^ 其他

取消

命令预览

确定

步骤 3 配置 NAT 地址池。公网地址范围为 2.2.2.2-2.2.2.5。

选择“策略 > NAT 策略”。选择“源转换地址池”页签。在“源转换地址池”中单击  新建地址池，配置完成后单击“确定”。具体配置如下图所示：

新建源转换地址池

* 地址池名称

natpool

IP地址类型

☒ IPv4
 ☐ IPv6

* IP地址范围

2.2.2.2-2.2.2.5

每行可输入一个地址范围或单个IP，行之间用回车分隔，示例：

- 10.10.1.2
- 10.10.1.1-10.10.1.2

自动生成黑洞路由 ?

☐

允许端口地址转换

☒

高级

取消

确定

步骤 4 配置 NAT 策略。

选择“策略 > NAT 策略”。选择“NAT 策略”页签。在“NAT 策略列表”中单击  新建 NAT 策略，配置完成后单击“确定”。具体配置如下图所示：

新建NAT策略

×

[\[功能介绍\]](#)

名称

source_nat

*

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

源转换地址池

natpool

▼

*

[配置]

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

3.1.8 结果验证

从 PC1 ping PC2 地址。

```
PC> ping 40.1.1.100
```

```
Ping 40.1.1.100: 32 data bytes, Press Ctrl_C to break
From 40.1.1.100: bytes=32 seq=1 ttl=127 time=16 ms
From 40.1.1.100: bytes=32 seq=2 ttl=127 time=16 ms
From 40.1.1.100: bytes=32 seq=3 ttl=127 time<1 ms
From 40.1.1.100: bytes=32 seq=4 ttl=127 time=15 ms
From 40.1.1.100: bytes=32 seq=5 ttl=127 time=16 ms
```

```
--- 40.1.1.100 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 0/12/16 ms
```

在 FW1 上使用 display firewall session table 命令查看 NAT 转换情况，如下所示：

```
[FW1] display firewall session table
Current Total Sessions : 5
icmp  VPN: public --> public  10.1.2.100:56279[2.2.2.5:2057] -->40.1.1.100:2048
icmp  VPN: public --> public  10.1.2.100:55255[2.2.2.5:2053] -->40.1.1.100:2048
icmp  VPN: public --> public  10.1.2.100:56023[2.2.2.5:2056] -->40.1.1.100:2048
icmp  VPN: public --> public  10.1.2.100:55767[2.2.2.5:2055] -->40.1.1.100:2048
icmp  VPN: public --> public  10.1.2.100:55511[2.2.2.5:2054] -->40.1.1.100:2048
```

可以看到，防火墙将源地址 10.1.2.100 转换成了 NAT 地址池中的 2.2.2.5 与 PC2 进行通信。

3.1.9 思考题

源 NAT 中 NAT 与 NAT No-PAT 的区别在哪里？分别适用于什么场景？

参考答案：

NAPT 是一种同时转换 IP 地址和端口的转换技术，能够实现多个私网地址共用一个或多个公网地址访问公网资源。适用于公网地址数量少，同时上网的私网用户数量大的场景。

NAT No-PAT 是一种仅转换 IP 地址，不转换端口的转换技术，可实现私网地址到公网地址一对一的地址转换。适用于上网用户较少，且公网地址数与同时上网的用户数相同的场景。

3.2 实验任务配置（NAT Server & 源 NAT 实验）

3.2.1 配置思路

- 1.配置基本的 IP 地址和所属安全区域，并且配置对应的安全策略。
- 2.配置 NAT Server。
- 3.配置 NAT 地址池。
- 4.配置 NAT 策略。

3.2.2 配置步骤 - CLI

步骤 1 完成 FW1 上、下行业务接口的配置。配置各接口 IP 地址并加入相应安全区域。

配置 FW1 上、下行业务接口的 IP 地址。

```
<FW1> system-view
```

```
[FW1] interface G0/0/1
[FW1-GigabitEthernet0/0/1] ip address 10.1.2.1 255.255.255.0
[FW1-GigabitEthernet0/0/1] quit
[FW1] interface G0/0/2
[FW1-GigabitEthernet0/0/2] ip address 40.1.1.1 255.255.255.0
[FW1-GigabitEthernet0/0/2] quit
[FW1] interface G0/0/3
[FW1-GigabitEthernet0/0/3] ip address 10.1.1.1 255.255.255.0
[FW1-GigabitEthernet0/0/3] quit
```

步骤 2 配置 untrust 区域和 dmz 区域的域间转发策略。

```
[FW1] security-policy
[FW1-policy-security] rule name bidectinal_nat
[FW1-policy-security-rule-policy_sec] source-zone untrust
[FW1-policy-security-rule-policy_sec] destination-zone dmz
[FW1-policy-security-rule-policy_sec] action permit
[FW1-policy-security-rule-policy_sec] service ftp
[FW1-policy-security-rule-policy_sec] quit
```

步骤 3 配置 NAT Server。

```
[FW1] nat server ftpserver protocol tcp global 40.1.1.2 ftp inside 10.1.1.100 ftp
```

步骤 4 配置 NAT 地址池。

```
[FW1] nat address-group natpool2
[FW1-address-group-natpool] section 10.1.1.10 10.1.1.20
```

步骤 5 在 dmz 与 untrust 区域间应用 NAT ALG 功能，使服务器可以正常对外提供 FTP 服务。缺省情况下已经在全局启用了 NAT ALG 功能，该步骤可以省略。

```
[FW1] firewall interzone dmz untrust
[FW1 -interzone-dmz-untrust] detect ftp
[FW1 -interzone-dmz-untrust] quit
```

步骤 6 创建 dmz 和 untrust 区域之间的 NAT 策略，确定进行 NAT 转换的源地址范围，并且将其与 natpool2 进行绑定。

```
[FW1] nat-policy
[FW1-policy-nat] rule name source_nat
[FW1-policy-nat-rule-source_nat] destination-zone dmz
[FW1-policy-nat-rule-source_nat] source-zone untrust
[FW1-policy-nat-rule-source_nat] source-address 40.1.1.0 24
[FW1-policy-nat-rule-source_nat] action nat address-group natpool2
```

步骤 7 配置 Switch。

分别将两台 Switch 的两个接口加入同一个 VLAN，缺省 VLAN 即可，如需配置请参考交换机的相关文档。

3.2.3 配置步骤 - Web

步骤 1 完成 FW1 防火墙接口配置。

选择“网络 > 接口”，单击需要配置接口后面的配置按钮。依次选择或输入各项参数，单击“确定”。完成 GigabitEthernet0/0/1 接口配置，如下图所示：



修改GE

接口名称: GE0/0/1

描述:

虚拟系统: public

VPN实例: public

安全区域: trust

模式: ☒ 路由 ☐ 交换 ☐ 旁路检测 ☐ 接口对

IPv4 | IPv6

连接类型: ☒ 静态IP ☐ DHCP

IP地址: 10.1.2.1/24

默认网关:

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

选择“网络 > 接口”，单击需要配置接口后面的配置按钮。依次选择或输入各项参数，单击“确定”。完成 GigabitEthernet0/0/2 接口配置，如下图所示：

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

模式

☒ 路由
☐ 交换
☐ 旁路检测
☐ 接口对

IPv4

IPv6

连接类型

☒ 静态IP
☐ DHCP

IP地址

40.1.1.1/24

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”。

默认网关

取消

确定

选择“网络 > 接口”，单击需要配置接口后面的配置按钮。依次选择或输入各项参数，单击“确定”。完成 GigabitEthernet0/0/3 接口配置，如下图所示：

修改GE

接口名称

GE0/0/3

描述

虚拟系统

public

VPN实例

public

安全区域

dmz

模式

☒ 路由
☐ 交换
☐ 旁路检测
☐ 接口对

IPv4

IPv6

连接类型

☒ 静态IP
☐ DHCP

IP地址

10.1.1.1/24

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”。

默认网关

取消

确定

步骤 2 完成 FW1 防火墙域间转发策略配置。

选择“策略 > 安全策略 > 安全策略”，在“安全策略列表”中，单击“新建”。依次输入或选择各项参数。单击“确定”。完成 untrust 与 dmz 间转发策略，如下图所示：

新建安全策略

概述

名称

bidirectal_nat

描述

策略组

-- NONE --

条件

当前未加载地区识别特征库。如需配置地区，请加载地区识别特征库

源

安全区域

untrust

IP 地址/地区

any

目的

目的类型

安全区域

虚拟服务

安全区域

dmz

IP 地址/地区

any

服务

协议

ftp

更多

应用/用户/安全组/时间段/VLAN ID

动作

动作

允许

禁止

内容安全检查

反病毒/入侵防御/URL过滤/内容过滤

取消

命令预览

确定

步骤 3 配置 NAT Server。

选择“策略 > NAT 策略> 服务器映射”，在“服务器映射列表”中单击新建，配置完成后单击“确定”。具体配置如下图所示：

新建服务器映射

×

[\[功能介绍\]](#)

名称

ftpserver

*

安全区域?

▼

公网地址?

40.1.1.2

*

-

私网地址?

10.1.1.100

*

-

☒ 指定协议

协议

TCP

▼

*

公网端口

21

*

-

<1-65535>

私网端口

21

*

-

<1-65535>

☒ 允许服务器使用公网地址上网?

☒ 自动生成黑洞路由?

提示: 为保证设备顺利转发NAT业务, 需要配置安全策略。

如需查看NAT相关日志, 请在安全策略中启用流量日志及会话日志。 [\[新建安全策略\]](#)

取消

确定

步骤 4 配置 NAT 地址池。

#选择“策略 > NAT 策略”。选择“源转换地址池”页签。在“源转换地址池”中单击  新建地址池，配置完成后单击“确定”。具体配置如下图所示：

新建源转换地址池

×

* 地址池名称

natpool2

IP地址类型

☒ IPv4
 ☐ IPv6

* IP地址范围

10.1.1.10-10.1.1.20

每行可输入一个地址范围或单个IP，行之间用回车分隔，示例：

- 10.10.1.2
- 10.10.1.1-10.10.1.2

自动生成黑洞路由 ?

☐

允许端口地址转换

☒

高级

取消

确定

步骤 5 配置 NAT 策略。

选择“策略 > NAT 策略”。选择“NAT 策略”页签。在“NAT 策略列表”中单击  新建 NAT 策略，配置完成后单击“确定”。具体配置如下图所示：

新建NAT策略

×

[功能介绍]

名称

source_nat2

*

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

untrust

▼

[多选]

目的类型

☒ 目的安全区域
☐ 出接口

dmz

▼

[多选]

源地址②

40.1.1.0/24 ×

目的地址②

请选择或输入地址

服务②

ftp ×

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

源转换地址池

natpool2

▼

*

[配置]

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

3.2.4 结果验证

在防火墙上查看相关信息，如下所示：

```
[FW1] display nat server
Server in private network information:
  Total    1 NAT server(s)
server name    : ftpserver
id             : 0
zone           : ---
global-start-addr : 40.1.1.2
global-end-addr   : 40.1.1.2
inside-start-addr : 10.1.1.100
inside-end-addr   : 10.1.1.100
global-start-port : 21(ftp)
global-end-port   : 21
```

inside-start-port : 21(ftp)	inside-end-port : 21
globalvpn : public	insidevpn : public
vsys : public	protocol : tcp
vrrp : ---	no-revers : 0
interface : ---	vrrp-bind-interface: ---
unr-route : 1	description : ---
nat-disable : 0	

3.2.5 思考题

当外网用户通过特定 IP 地址访问内网服务器时，报文到达防火墙的处理步骤依次有哪些？

参考答案：

首包到达防火墙 > 匹配 NAT Server 进行目的地址转换 > 查找路由表 > 匹配安全策略 > 创建会话。

4 防火墙双机热备实验

4.1 实验介绍

4.1.1 关于本实验

某企业的业务需持续提供服务，为避免网络设备及外部不可控因素导致线路中断，希望在网络出口增加冗余以增加网络的可靠性。

本实验通过在网络出口位置部署两台防火墙作为网关，保证了在单机故障的情况下内部网络与外部网络之间的通信畅通。

4.1.2 实验目的

- 理解双机热备的基本原理；
- 理解 VGMP 和 HRP 协议；
- 掌握通过命令行和 Web 方式配置防火墙双机热备。

4.1.3 实验组网介绍

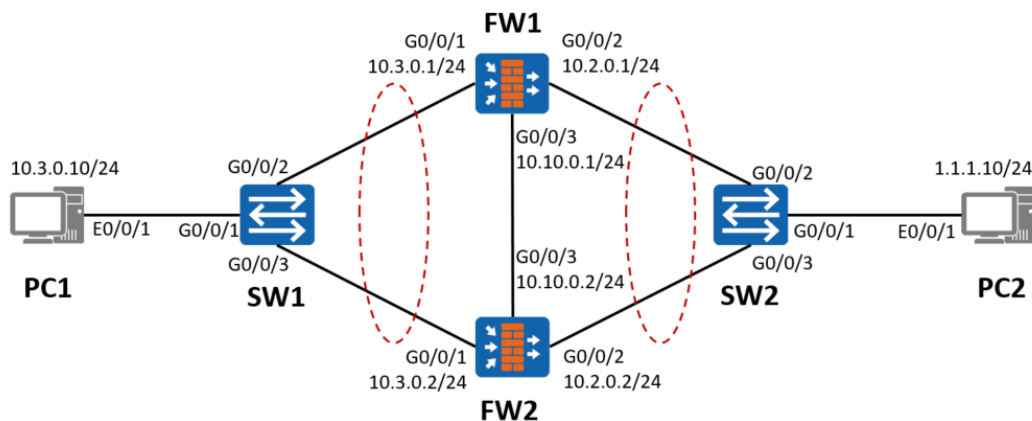


图4-1 防火墙双机热备实验拓扑图

4.1.4 实验规划

FW 作为安全设备被部署在网络出口位置。其中上、下行设备均是交换机，FW1、FW2 以主备备份方式工作。

表4-1 端口地址和区域划分

设备	接口	IP地址	安全区域
FW1	GigabitEthernet0/0/1	10.3.0.1/24	trust
	GigabitEthernet0/0/2	10.2.0.1/24	untrust
	GigabitEthernet0/0/3	10.10.0.1/24	dmz
FW2	GigabitEthernet0/0/1	10.3.0.2/24	trust
	GigabitEthernet0/0/2	10.2.0.2/24	untrust
	GigabitEthernet0/0/3	10.10.0.2/24	dmz
PC1	Eth0/0/1	10.3.0.10/24	trust
PC2	Eth0/0/1	1.1.1.10/24	untrust
SW1	G0/0/1 G0/0/2 G0/0/3	Access	PVID: VLAN 10
SW2	G0/0/1 G0/0/2 G0/0/3	Access	PVID: VLAN 10

4.2 实验任务配置

4.2.1 配置思路

- 1.在 FW1、FW2 上配置基本的 IP 地址和所属安全区域，并且放行对应的安全策略。
- 2.进行双机热备配置，备份方式为主备备份，FW1 为主，FW2 为备。

4.2.2 配置步骤 - CLI

步骤 1 完成 FW1 和 FW2 上、下行业务接口的配置。配置各接口 IP 地址并加入相应安全区域。

配置 FW1 上、下行业务接口的 IP 地址。

```
<FW1> system-view
[FW1] interface GigabitEthernet0/0/1
[FW1-GigabitEthernet0/0/1] ip address 10.3.0.1 255.255.255.0
[FW1-GigabitEthernet0/0/1] quit
[FW1] interface GigabitEthernet0/0/2
```

```
[FW1-GigabitEthernet0/0/2] ip address 10.2.0.1 255.255.255.0
[FW1-GigabitEthernet0/0/2] quit
```

配置 FW1 接口 GigabitEthernet0/0/1 的 VRRP 备份组 1，并加入到状态为 Active 的 VGMP 管理组。

```
[FW1] interface GigabitEthernet0/0/1
[FW1-GigabitEthernet0/0/1] vrrp vrid 1 virtual-ip 10.3.0.3 255.255.255.0 active
[FW1-GigabitEthernet0/0/1] quit
```

配置 FW1 接口 GigabitEthernet0/0/2 的 VRRP 备份组 2，并加入到状态为 Active 的 VGMP 管理组。

```
[FW1] interface GigabitEthernet0/0/2
[FW1-GigabitEthernet0/0/2] vrrp vrid 2 virtual-ip 1.1.1.1 255.255.255.0 active
[FW1-GigabitEthernet0/0/2] quit
```

将 FW1 上、下行业务接口加入安全区域。

```
[FW1] firewall zone trust
[FW1-zone-trust] add interface GigabitEthernet0/0/1
[FW1-zone-trust] quit
[FW1] firewall zone untrust
[FW1-zone-untrust] add interface GigabitEthernet0/0/2
[FW1-zone-untrust] quit
```

配置 FW2 上、下行业务接口的配置。

```
<FW2> system-view
[FW2] interface GigabitEthernet0/0/1
[FW2-GigabitEthernet0/0/1] ip address 10.3.0.2 255.255.255.0
[FW2-GigabitEthernet0/0/1] quit
[FW2] interface GigabitEthernet0/0/2
[FW2-GigabitEthernet0/0/2] ip address 10.2.0.2 255.255.255.0
[FW2-GigabitEthernet0/0/2] quit
```

配置 FW2 接口 GigabitEthernet0/0/1 的 VRRP 备份组 1，并加入到状态为 Standby 的 VGMP 管理组。

```
[FW2] interface GigabitEthernet0/0/1
[FW2-GigabitEthernet0/0/1] vrrp vrid 1 virtual-ip 10.3.0.3 255.255.255.0 standby
[FW2-GigabitEthernet0/0/1] quit
```

配置 FW2 接口 GigabitEthernet0/0/2 的 VRRP 备份组 2，并加入到状态为 Standby 的 VGMP 管理组。

```
[FW2] interface GigabitEthernet0/0/2
[FW2-GigabitEthernet0/0/2] vrrp vrid 2 virtual-ip 1.1.1.1 255.255.255.0 standby
[FW2-GigabitEthernet0/0/2] quit
```

将 FW2 上、下行业务接口加入安全区域。

```
[FW2] firewall zone trust
[FW2-zone-trust] add interface GigabitEthernet 0/0/1
[FW2-zone-trust] quit
[FW2] firewall zone untrust
```

```
[FW2-zone-untrust] add interface GigabitEthernet 0/0/2
[FW2-zone-untrust] quit
```

步骤 2 完成 FW1、FW2 的心跳线配置。

配置 FW1 心跳接口 GigabitEthernet0/0/3 的 IP 地址。

```
[FW1] interface GigabitEthernet0/0/3
[FW1-GigabitEthernet0/0/3] ip address 10.10.0.1 255.255.255.0
[FW1-GigabitEthernet0/0/3] quit
```

配置 FW2 心跳接口 GigabitEthernet0/0/3 的 IP 地址。

```
[FW2] interface GigabitEthernet0/0/3
[FW2-GigabitEthernet0/0/3] ip address 10.10.0.2 255.255.255.0
[FW2-GigabitEthernet0/0/3] quit
```

配置 FW1 心跳接口 GigabitEthernet0/0/3 加入 dmz 安全区域。

```
[FW1] firewall zone dmz
[FW1-zone-dmz] add interface GigabitEthernet0/0/3
[FW1-zone-dmz] quit
```

配置 FW2 心跳接口 GigabitEthernet0/0/3 加入 dmz 安全区域。

```
[FW2] firewall zone dmz
[FW2-zone-dmz] add interface GigabitEthernet0/0/3
[FW2-zone-dmz] quit
```

配置 FW1 心跳接口认证密钥并启用双机热备功能。

```
[FW1] hrp interface GigabitEthernet0/0/3 remote 10.10.0.2
[FW1] hrp authentication-key Admin@123
[FW1] hrp enable
```

配置 FW2 心跳接口认证密钥并启用双机热备功能。

```
[FW2] hrp interface GigabitEthernet0/0/3 remote 10.10.0.1
[FW2] hrp authentication-key Admin@123
[FW2] hrp enable
```

步骤 3 在 FW1 上配置安全策略，允许业务报文通过。双机热备状态成功建立后，FW1 的安全策略配置会自动备份到 FW2 上。

配置 FW1 上 trust 区域和 untrust 区域的域间转发策略。

```
HRP_M[FW1] security-policy
HRP_M[FW1-policy-security] rule name trust_to_untrust
HRP_M[FW1-policy-security-rule-trust_to_untrust] source-zone trust
HRP_M[FW1-policy-security-rule-trust_to_untrust] destination-zone untrust
HRP_M[FW1-policy-security-rule-trust_to_untrust] source-address 10.3.0.0 24
HRP_M[FW1-policy-security-rule-trust_to_untrust] action permit
HRP_M[FW1-policy-security-rule-trust_to_untrust] quit
HRP_M[FW1-policy-security] quit
```

步骤 4 在 FW1 上配置 NAT 策略。双机热备状态成功建立后，FW1 的 NAT 策略配置会自动备份到 FW2 上。

配置 NAT 策略，当内网用户访问 Internet 时，将源地址由 10.3.0.0/24 网段转换为地址池中的地址（1.1.1.2-1.1.1.5）。

```
HRP_M[FW1] nat address-group group1
HRP_M[FW1-address-group-group1] section 0 1.1.1.2 1.1.1.5
HRP_M[FW1-address-group-group1] quit
HRP_M[FW1] nat-policy
HRP_M[FW1-policy-nat] rule name policy_nat1
HRP_M[FW1-policy-nat-rule-policy_nat1] source-zone trust
HRP_M[FW1-policy-nat-rule-policy_nat1] destination-zone untrust
HRP_M[FW1-policy-nat-rule-policy_nat1] source-address 10.3.0.0 24
HRP_M[FW1-policy-nat-rule-policy_nat1] action source-nat address-group group1
```

步骤 5 配置 Switch。

分别将 SW1、SW2 的三个接口加入 VLAN 10，如需配置请参考交换机的配置文档。

4.2.3 配置步骤 - Web

步骤 1 完成 FW1 和 FW2 上、下行业务接口的配置。配置各接口 IP 地址并加入相应安全区域。

完成 FW1 防火墙接口配置。选择“网络 > 接口”，单击需要配置的接口后边的配置按钮 。依次选择或输入各项参数，单击“确定”。完成 GigabitEthernet0/0/1 接口配置，如下图所示：

修改GE

接口名称

GE0/0/1

描述

虚拟系统?

public

VPN实例

public

安全区域

trust

模式?

☒ 路由
☐ 交换
☐ 旁路检测
☐ 接口对

IPv4

IPv6

连接类型

☒ 静态IP
☐ DHCP

IP地址

10.3.0.1/24

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"。

默认网关

取消

确定

FW1 的 GigabitEthernet0/0/2 和 GigabitEthernet0/0/3，FW2 的 GigabitEthernet0/0/1、GigabitEthernet0/0/2 和 GigabitEthernet0/0/3 的接口配置类似，不再赘述。

步骤 2 完成 FW1、FW2 的心跳线配置。

修改GE

接口名称

GE0/0/3

描述

虚拟系统?

public

VPN实例

public

安全区域

-- NONE --

模式?

☒ 路由
☐ 交换
☐ 旁路检测
☐ 接口对

IPv4

IPv6

连接类型

☒ 静态IP
☐ DHCP

IP地址

10.10.0.1/24

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"。

默认网关

取消

确定

FW2 的 GigabitEthernet0/0/3 接口配置类似，此处省略。

步骤 3 配置 FW1 和 FW2 防火墙双机热备相关配置。

FW1 配置如下（认证密钥：Huawei@123）：

配置双机热备

双机热备

认证密钥

运行模式

运行角色

心跳接口

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

配置监控对象

请在组建双机设备前先查阅产品文档中的使用限制和注意事项！

<8-16> 字符

主备备份

负载分担

主用

备用

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

GE0/0/3

[配置] IP地址

10.10.0.1

对端接口IP

10.10.0.2

1000

<500-60000>毫秒

接口监控

VRRP监控

健康检查监控

BFD监控

提示：当业务接口工作在三层且连接交换机时，需要配置VRRP备份组。

新建

删除

VRID	接口	接口IP地址/掩码	虚拟IP地址/掩码（可选）	角色	编辑
1	GE0/0/1	10.3.0.1/24	10.3.0.3/24	主	
2	GE0/0/2	10.2.0.1/24	1.1.1.1/24	主	

共 2 条 1 50条/页 前往 1 页

取消

确定

FW2 配置如下（认证密钥：Huawei@123）：

配置双机热备

双机热备

认证密钥 * <8-16> 字符

运行模式 ☒ 主备备份 ☐ 负载分担

运行角色 ☐ 主用 ☒ 备用

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

心跳接口 * [配置] IP地址 * 对端接口IP *

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

健康检查监控

BFD监控

提示：当业务接口工作在三层且连接交换机时，需要配置VRRP备份组。

新建

删除

VRID	接口	接口IP地址/掩码	虚拟IP地址/掩码 (可选)	角色	编辑
☐ 1	GE0/0/1	10.3.0.2/24	10.3.0.3/24	备	编辑
☐ 2	GE0/0/2	10.2.0.2/24	1.1.1.1/24	备	编辑

共 2 条 < 1 > 50条/页 前往 1 页

取消

确定

步骤 4 在双机热备的配置界面可以查看双机热备的状态信息。

FW1 双机热备状态如下：

USG6525F 主		面板	监控	策略	对象	网络	系统				
配置		双机热备									
配置		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 11 分)	详细 强制主备切换							
		当前心跳接口	GE0/0/3								
		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 (按 接口名称 VLAN 过滤)									
		VRRP监控									
		10.3.0.3(GE0/0/1)	✓	主状态							
		1.1.1.1(GE0/0/2)	✓	主状态							
		健康检查监控									
		BFD监控									

FW2 双机热备状态如下：



步骤 5 配置 FW1 和 FW2 的域间转发策略。

在 FW1 上配置安全策略，允许业务报文通过。双机热备状态成功建立后，FW1 的安全策略配置会自动备份到 FW2 上。

选择：“策略 > 安全策略 > 安全策略”。在“安全策略列表”中，单击“新建”，依次输入或选择各项参数，单击“确定”。完成 trust 与 untrust 间转发策略，如下图所示：

新建安全策略

×

概述

名称

trust_to_untrust

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 ×

IP 地址/地区 ②

10.3.0.0/24 ×

目的

11

目的类型

☒ 安全区域

☐ 虚拟服务

安全区域

untrust ×

IP 地址/地区 ②

any

服务 ②

请选择服务

更多

应用/用户/安全组/时间段/VLAN ID

动作

动作

☒ 允许

☐ 禁止

内容安全检查

反病毒/入侵防御/URL过滤/内容过滤

取消

命令预览

确定

步骤 6 在 FW1 上配置 NAT 策略。双机热备状态成功建立后，FW1 的 NAT 策略配置会自动备份到 FW2 上。

#选择：“策略 > NAT 策略 > NAT 策略 > 源转换地址池 > 新建”配置 NAT 地址池。

新建源转换地址池 ✕

* 地址池名称

group1

IP地址类型

☒ IPv4 ☐ IPv6

* IP地址范围

1.1.1.2-1.1.1.5

每行可输入一个地址范围或单个IP，行之间用回车分隔，示例：

- 10.10.1.2
- 10.10.1.1-10.10.1.2

自动生成黑洞路由 ?

☐

允许端口地址转换

☒

高级

取消

确定

选择：“策略 > NAT 策略 > NAT 策略 > 新建”配置 NAT 策略，当内网用户访问 Internet 时，将源地址由 10.3.0.0/24 网段转换为地址池中的地址（1.1.1.2-1.1.1.5）。

新建NAT策略

×

[\[功能介绍\]](#)

名称

policy_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

▼

[多选]

目的类型

☒ 目的安全区域
☐ 出接口

untrust

▼

[多选]

源地址?

10.0.3.0/24 ×

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

源转换地址池

group1

▼

*

[配置]

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

步骤 7 配置 Switch。

分别将 SW1、SW2 的三个接口加入 VLAN 10，如需配置请参考交换机的配置文档。

4.3 结果验证

在 FW1 上执行 **display vrrp** 命令，检查 VRRP 组内接口的状态信息。

```
HRP_M<FW1> display vrrp
GigabitEthernet0/0/1 | Virtual Router 1
State : Master
```

```
Virtual IP : 10.3.0.3
Master IP : 10.3.0.1
PriorityRun : 120
PriorityConfig : 100
MasterPriority : 120
Preempt : YES    Delay Time : 0 s
TimerRun : 60 s
TimerConfig : 60 s
Auth type : NONE
Virtual MAC : 0000-5e00-0101
Check TTL : YES
Config type : vgmp-vrrp
Backup-forward : disabled
```

GigabitEthernet0/0/2 | Virtual Router 2

```
State : Master
Virtual IP : 1.1.1.1
Master IP : 10.2.0.1
PriorityRun : 120
PriorityConfig : 100
MasterPriority : 120
Preempt : YES    Delay Time : 0 s
TimerRun : 60 s
TimerConfig : 60 s
Auth type : NONE
Virtual MAC : 0000-5e00-0102
Check TTL : YES
Config type : vgmp-vrrp
Backup-forward : disabled
```

在 FW2 上执行 **display vrrp** 命令，检查 VRRP 组内接口的状态信息。

```
HRP_S<FW2>display vrrp
```

GigabitEthernet0/0/1 | Virtual Router 1

```
State : Backup
Virtual IP : 10.3.0.3
Master IP : 10.3.0.1
PriorityRun : 120
PriorityConfig : 100
MasterPriority : 120
Preempt : YES    Delay Time : 0 s
TimerRun : 60 s
TimerConfig : 60 s
Auth type : NONE
Virtual MAC : 0000-5e00-0101
Check TTL : YES
Config type : vgmp-vrrp
Backup-forward : disabled
```

```
GigabitEthernet0/0/2 | Virtual Router 2
State : Backup
Virtual IP : 1.1.1.1
Master IP : 0.0.0.0
PriorityRun : 120
PriorityConfig : 100
MasterPriority : 0
Preempt : YES    Delay Time : 0 s
TimerRun : 60 s
TimerConfig : 60 s
Auth type : NONE
Virtual MAC : 0000-5e00-0102
Check TTL : YES
Config type : vgmp-vrrp
Backup-forward : disabled
```

在 FW1 执行 **display hrp state verbose** 命令，检查当前 VGMP 组的状态。

```
HRP_M< FW1>display hrp state verbose
Role: active, peer: standby
Running priority: 45000, peer: 45000
Backup channel usage: 0.00%
Stable time: 0 days, 0 hours, 46 minutes
Last state change information: 17:18:08 HRP core state changed, old_state = abnormal(active),
new_state = normal, local_priority = 45000, peer_priority = 45000.

Configuration:
hello interval:          1000ms
preempt:                  60s
mirror configuration:     off
mirror session:           off
track trunk member:      on
auto-sync configuration:  on
auto-sync connection-status: on
adjust ospf-cost:         on
adjust ospfv3-cost:       on
adjust bgp-cost:          on
nat resource:             off

Detail information:
    GigabitEthernet0/0/1 vrrp vrid 1: active
    GigabitEthernet0/0/2 vrrp vrid 2: active
                                ospf-cost: +0
                                ospfv3-cost: +0
                                bgp-cost: +0
```

在 FW2 上执行 **display hrp state verbose** 命令，检查当前 VGMP 组的状态。

```
HRP_S<FW2>display hrp state verbose
```

```
Role: standby, peer: active
Running priority: 45000, peer: 45000
Backup channel usage: 0.00%
Stable time: 0 days, 0 hours, 41 minutes
Last state change information: 17:18:08 HRP core state changed, old_state = abnormal(standby),
new_state = normal, local_priority = 45000, peer_priority = 45000.
```

Configuration:

```
hello interval:          1000ms
preempt:                  60s
mirror configuration:     off
mirror session:           off
track trunk member:      on
auto-sync configuration:  on
auto-sync connection-status: on
adjust ospf-cost:         on
adjust ospfv3-cost:       on
adjust bgp-cost:          on
nat resource:             off
```

Detail information:

```
GigabitEthernet0/0/1 vrrp vrid 1: standby
GigabitEthernet0/0/2 vrrp vrid 2: standby
                        ospf-cost: +65500
                        ospfv3-cost: +65500
                        bgp-cost: +100
```

在 trust 区域的 PC1 能够 ping 通 untrust 区域的 PC2，并分别在 FW1 和 FW2 上执行命令 **display firewall session table** 检查会话，如下所示：

```
HRP_M<FW1> display firewall session table
```

```
Current Total Sessions : 1
```

```
icmp VPN: public --> public 10.3.0.10:53419[1.1.1.4:2049] --> 1.1.1.10:2048
```

```
HRP_S<FW2> display firewall session table
```

```
Current Total Sessions : 1
```

```
icmp VPN: public --> public 10.3.0.10:53419[1.1.1.4:2049] --> 1.1.1.10:2048
```

4.4 配置参考

4.4.1 FW1 的配置

```
#
sysname FW1
#
hrp enable
```

```
hrp interface GigabitEthernet0/0/3 remote 10.10.0.2
hrp authentication-key Admin@123
#
interface GigabitEthernet0/0/1
ip address 10.3.0.1 255.255.255.0
vrrp vrid 1 virtual-ip 10.3.0.3 255.255.255.0 active
#
interface GigabitEthernet0/0/2
ip address 10.2.0.1 255.255.255.0
vrrp vrid 2 virtual-ip 1.1.1.1 255.255.255.0 active
#
interface GigabitEthernet0/0/3
ip address 10.10.0.1 255.255.255.0
#
firewall zone trust
set priority 85
add interface GigabitEthernet0/0/1
#
firewall zone untrust
set priority 5
add interface GigabitEthernet0/0/2
#
firewall zone dmz
set priority 50
add interface GigabitEthernet0/0/3
#
ip route-static 0.0.0.0 0.0.0.0 1.1.1.10
#
nat address-group group1
section 0 1.1.1.2 1.1.1.5
#
security-policy
rule name trust_to_untrust
source-zone trust
destination-zone untrust
source-address 10.3.0.0 24
action permit
#
nat-policy
rule name policy_nat1
source-zone trust
destination-zone untrust
source-address 10.3.0.0 24
action source-nat address-group group1
#
```

4.4.2 FW2 的配置

```
#
sysname FW2
#
hrp enable
hrp interface GigabitEthernet0/0/3 remote 10.10.0.1
hrp authentication-key Admin@123
#
interface GigabitEthernet0/0/1
ip address 10.3.0.2 255.255.255.0
vrrp vrid 1 virtual-ip 10.3.0.3 255.255.255.0 standby
#
interface GigabitEthernet0/0/2
ip address 10.2.0.2 255.255.255.0
vrrp vrid 2 virtual-ip 1.1.1.1 255.255.255.0 standby
#
interface GigabitEthernet0/0/3
ip address 10.10.0.2 255.255.255.0
#
firewall zone trust
set priority 85
add interface GigabitEthernet0/0/1
#
firewall zone untrust
set priority 5
add interface GigabitEthernet0/0/2
#
firewall zone dmz
set priority 50
add interface GigabitEthernet0/0/3
#
ip route-static 0.0.0.0 0.0.0.0 1.1.1.10
#
nat address-group group1
section 0 1.1.1.2 1.1.1.5
#
security-policy
rule name trust_to_untrust
source-zone trust
destination-zone untrust
source-address 10.3.0.0 24
action permit
#
nat-policy
rule name policy_nat1
source-zone trust
destination-zone untrust
```

```
source-address 10.3.0.0 24
action source-nat address-group group1
#
```

4.5 思考题

心跳接口之间交互的 HRP 报文是否受安全策略控制？

参考答案：

心跳接口之间交互 HRP 报文是否受安全策略限制与设备型号与版本有关系，本实验手册环境中，心跳接口之间交互 HRP 报文不受安全策略限制。

在新版本中，HRP 报文是否受安全策略控制决定于 firewall packet-filter basic-protocol enable 命令的配置。缺省情况下，firewall packet-filter basic-protocol enable 处于开启状态，即 HRP 报文受安全策略控制，需要在心跳接口所在安全区域与 local 区域之间配置安全策略，允许 HRP 报文通过。

5 点到点 IPSec VPN 实验

5.1 实验介绍

5.1.1 关于本实验

企业 A 与企业 B 之间需要跨互联网相互访问业务，由于业务涉及公司机密，希望通过保密的方式进行业务互访。

本实验以网络 A 与网络 B 模拟企业 A 与企业 B，网络 A 和网络 B 通过 FW1 和 FW2 连接到 Internet。通过组网实现 FW1 和 FW2 之间建立 IKE 方式的 IPSec 隧道，网络 A 和网络 B 的用户可通过 IPSec 隧道互相访问，访问过程中在互连网的报文被 IPSec VPN 的加密，达到保密需求。

5.1.2 实验目的

- 理解 IPSec VPN 的基本原理；
- 掌握点到点 IPSec VPN 应用场景的配置。

5.1.3 实验组网介绍

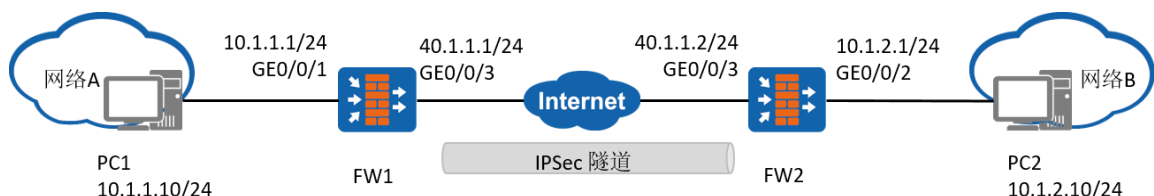


图5-1 点到点 IPSec VPN 实验拓扑图

5.1.4 实验规划

网络 A 属于 10.1.1.0/24 子网，PC1 为网络 A 中的一台主机，FW1 为网络 A 的网关；
网络 B 属于 10.1.2.0/24 子网，PC2 为网络 B 中的一台主机，FW2 为网络 B 的网关；
FW1 与 FW2 出口连接互联网，FW1 与 FW2 出口路由可达，FW1 与 FW2 之间建立 IPSec 隧道。

表5-1 端口地址和区域划分

设备	接口	IP地址	安全区域
----	----	------	------

FW1	GigabitEthernet0/0/3	40.1.1.1/24	untrust
	GigabitEthernet0/0/1	10.1.1.1/24	trust
FW2	GigabitEthernet0/0/3	40.1.1.2/24	untrust
	GigabitEthernet0/0/2	10.1.2.1/24	trust
PC1	Eth0/0/1	10.1.1.10/24	trust
PC2	Eth0/0/1	10.1.2.10/24	trust

5.2 实验任务配置

5.2.1 配置思路

- 1.配置各接口的 IP 地址。
- 2.配置域间安全策略。
- 3.配置 IPSec/IKE 安全提议。
- 4.配置并应用 IPSec 策略。

5.2.2 配置步骤 - Web

步骤 1 配置各接口的 IP 地址。

在防火墙上配置各自接口的 IP 地址，并将接口加入对应安全区域。以 FW1 的配置为例，FW2 的配置参照 FW1。

#在 FW1 选择“网络 > 接口” 单击 GigabitEthernet 0/0/1 和 GigabitEthernet 0/0/3 对应的 ，按照如下参数进行配置：

修改GE

接口名称

GE0/0/1

描述

虚拟系统?

public

VPN实例

public

安全区域

trust

模式?

☒ 路由
☐ 交换
☐ 旁路检测
☐ 接口对

IPv4

IPv6

连接类型

☒ 静态IP
☐ DHCP

IP地址

10.1.1.1/255.255.255.0

一行一条记录。
输入格式为 "10.1.1.1/255.255.255.0"
或者"10.1.1/24"。

默认网关

取消

确定

修改GE

接口名称

GE0/0/3

描述

虚拟系统?

public

VPN实例

public

安全区域

untrust

模式?

☒ 路由
☐ 交换
☐ 旁路检测
☐ 接口对

IPv4

IPv6

连接类型

☒ 静态IP
☐ DHCP

IP地址

40.1.1.1/24

一行一条记录。
输入格式为 "10.1.1.1/255.255.255.0"
或者"10.1.1/24"。

默认网关

取消

确定

FW2 设备接口配置步骤同上，此处不再赘述。

步骤 2 配置 FW1 与 FW2 上安全策略。

在防火墙上配置安全策略 ipsec 允许网络 A 和网络 B 网段互访，同时放行 IPSec 协议协商流，以 FW1 的配置为例进行说明，FW2 的配置参照 FW1，不再赘述。

在 FW1 上选择“策略 > 安全策略 > 安全策略”，单击“新建”安全策略，允许网段 10.1.1.0/24 和 10.1.2.0/24 间的流量互访。

新建安全策略

概述

名称

ipsec

描述

策略组

-- NONE --

条件

当前未加载地区识别特征库。如需配置地区，请加载地区识别特征库

源

安全区域

trust × untrust ×

IP 地址/地区 ①

10.1.1.0/24 × 10.1.2.0/24 ×

目的

目的类型

安全区域

虚拟服务

安全区域

trust × untrust ×

IP 地址/地区 ①

10.1.1.0/24 × 10.1.2.0/24 ×

服务 ②

协议

请选择服务

更多

应用/用户/安全组/时间段/VLAN ID

动作

动作

允许

禁止

内容安全检查

反病毒/入侵防御/URL过滤/内容过滤

取消

命令预览

确定

在 FW1 上选择“策略 > 安全策略 > 安全策略”，单击“新建”安全策略，允许防火墙 local 区域与 untrust 区域之间相互访问，为建立 IPSec VPN 提供前提条件。

新建安全策略

×

概述

* 名称

untrust_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

untrust ×

local ×

IP 地址/地区 ⓘ

any

目的

目的类型

☒ 安全区域

☐ 虚拟服务

安全区域

local ×

untrust ×

IP 地址/地区 ⓘ

any

服务 ⓘ

协议

请选择服务

更多 ▾

应用/用户/安全组/时间段/VLAN ID

动作

动作

☒ 允许

☐ 禁止

内容安全检查 ▾

反病毒/入侵防御/URL过滤/内容过滤

取消

命令预览

确定

步骤 3 配置 IPSec 策略。

在 FW1 上选择“网络 > IPSec > IPSec”，单击“新建”，选择“场景”为“点到点”。在“基础配置”中设置 IPSec 相关参数，包括预共享密钥“Test!123”、本端及对端地址等。







在 FW2 上执行相同操作，需要注意的是，感兴趣流的配置需要与 FW1 设备侧互为镜像。

5.3 结果验证

PC1 用 ping 命令测试 PC2 的连通性。

```
C:\Users\admin>ping 10.1.2.10
Pinging 10.1.2.10 with 32 bytes of data:
Reply from 10.1.2.10: bytes=32 time=2ms TTL=126
Reply from 10.1.2.10: bytes=32 time<1ms TTL=126
Reply from 10.1.2.10: bytes=32 time<1ms TTL=126
Reply from 10.1.2.10: bytes=32 time<1ms TTL=126
Ping statistics for 10.1.2.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms
```

5.4 配置参考

5.4.1 FW1 的配置

```
#
acl number 3000
 rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
#
ipsec proposal prop16217151963
```

```
encapsulation-mode auto
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 ike162171519631
  exchange-mode auto
  pre-shared-key %^%#Tw^J,\TJzTtF8tRRu6K#DD"zU-1`OI*(Em%lTb['%^%#
  ike-proposal 1
  remote-id-type none
  dpd type periodic
  remote-address 40.1.1.2
  rsa encryption-padding oaep
  rsa signature-padding pss
  local-id-preference certificate enable
  ikev2 authentication sign-hash sha2-256
#
ipsec policy ipsec1621715194 1 isakmp
  security acl 3000
  ike-peer ike162171519631
  proposal prop16217151963
  tunnel local applied-interface
  alias 1
  sa trigger-mode auto
  sa duration traffic-based 5242880
  sa duration time-based 3600
#
interface GigabitEthernet0/0/3
  undo shutdown
  ip address 40.1.1.1 255.255.255.0
  ipsec policy ipsec1621715194
#
interface GigabitEthernet0/0/1
  undo shutdown
  ip address 10.1.1.1 255.255.255.0
#
firewall zone trust
  set priority 85
  add interface GigabitEthernet0/0/2
#
firewall zone untrust
```

```
set priority 5
add interface GigabitEthernet0/0/3
#
ip address-set 10.1.1.0/24 type object
description 网络 A 地址段
address 0 10.1.1.0 mask 24
#
ip address-set 10.1.2.0/24 type object
description 网络 B 地址段
address 0 10.1.2.0 mask 24
#
security-policy
rule name ipsec1
description 网络 A-网络 B
source-zone trust
destination-zone untrust
source-address address-set 10.1.1.0/24
destination-address address-set 10.1.2.0/24
action permit
rule name ipsec2
description 网络 B-网络 A
source-zone untrust
destination-zone trust
source-address address-set 10.1.2.0/24
destination-address address-set 10.1.1.0/24
action permit
rule name untrust-local
source-zone local
source-zone untrust
destination-zone local
destination-zone untrust
action permit
#
```

5.4.2 FW2 的配置

```
#
acl number 3000
rule 5 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
#
ipsec proposal prop16217202185
encapsulation-mode auto
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 ike162172021857
exchange-mode auto
pre-shared-key %^%#-"i1,QFGvWsErbOB@ph98G-PW*QI_1W-{Z~58>0.%^%#
ike-proposal 1
remote-id-type none
dpd type periodic
remote-address 40.1.1.1
rsa encryption-padding oaep
rsa signature-padding pss
local-id-preference certificate enable
ikev2 authentication sign-hash sha2-256
#
ipsec policy ipsec1621720216 1 isakmp
security acl 3000
ike-peer ike162172021857
proposal prop16217202185
tunnel local applied-interface
alias 1
sa trigger-mode auto
sa duration traffic-based 5242880
sa duration time-based 3600
#
interface GigabitEthernet0/0/3
undo shutdown
ip address 40.1.1.2 255.255.255.0
ipsec policy ipsec1621720216
#
interface GigabitEthernet0/0/2
undo shutdown
ip address 10.1.2.1 255.255.255.0
#
firewall zone trust
set priority 85
add interface GigabitEthernet0/0/2
#
firewall zone untrust
set priority 5
add interface GigabitEthernet0/0/1
#
ip route-static 0.0.0.0 0.0.0.0 40.1.1.1
#
ip address-set 10.1.1.0/24 type object
description 网络 A 地址段
```

```
address 0 10.1.1.0 mask 24
#
ip address-set 10.1.2.0/24 type object
description 网络 B 地址段
address 0 10.1.2.0 mask 24
#
security-policy
rule name ipsec1
description 网络 A-网络 B
source-zone trust
destination-zone untrust
source-address address-set 10.1.1.0/24
destination-address address-set 10.1.2.0/24
action permit
rule name ipsec2
description 网络 B-网络 A
source-zone untrust
destination-zone trust
source-address address-set 10.1.2.0/24
destination-address address-set 10.1.1.0/24
action permit
rule name untrust-local
source-zone local
source-zone untrust
destination-zone local
destination-zone untrust
action permit
#
```

5.5 思考题

如果企业 A 与企业 B 各自的员工都有访问互联网的需求，在防火墙出口配置 NAT 时需要注意什么？

参考答案：

企业 A 与企业 B 之间的流量在防火墙上会先查找路由找到出接口，此时在出接口的报文匹配顺序是先 NAT、后 IPSec。如果出口配置 NAT，一定要拒绝企业 A 与企业 B 之间的流量进行地址转换。

6 SSL VPN 实验

6.1 实验介绍

6.1.1 关于本实验

如下图所示的企业网络中，使用防火墙本地认证对各部门的员工进行用户认证，通过认证的用户能够获得接入企业内部网络的权限，未通过认证的用户则无法接入企业内网。

现希望某个用户组（group1）的移动办公用户出差时也能够获得一个内网 IP 地址，像在局域网一样访问企业内部的各种资源。另外为了增强安全性，采用用户名和密码结合的本地认证方式对移动办公用户的身份进行认证。

6.1.2 实验目的

- 掌握 SSL VPN 虚拟网关的配置方法；
- 了解 SSL VPN 使用场景和组网规划。

6.1.3 实验组网介绍

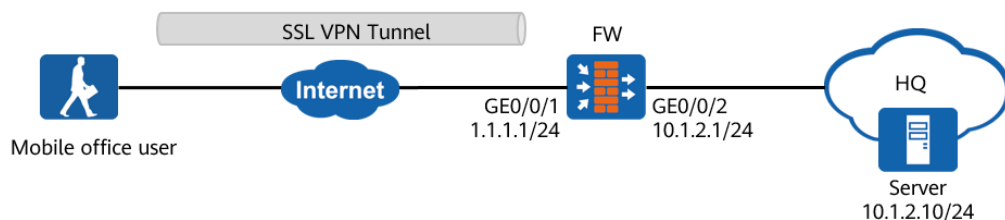


图6-1 SSL VPN 实验拓扑图

6.1.4 实验规划

表6-1 端口地址和区域划分

设备	接口	IP地址	安全区域
FW	GigabitEthernet0/0/1	1.1.1.1/24	untrust
	GigabitEthernet0/0/2	10.1.2.1/24	trust
Server	Eth0/0/1	10.1.2.10/24	trust

移动办公用户	Eth0/0/1	连接公网即可	untrust
--------	----------	--------	---------

6.2 实验任务配置

6.2.1 配置思路

- 1.配置各接口的 IP 地址，将各接口加入对应的安全区域。
- 2.配置用户和认证。
- 3.配置 SSL VPN 网关。
- 4.配置 SSL 协议等参数。
- 5.配置安全策略。

6.2.2 配置步骤 - Web

步骤 1 配置接口。

在 FW 上选择“网络 > 接口” 单击 GigabitEthernet 0/0/1 对应的 ，按照如下参数进行配置：

修改GE

接口名称

GE0/0/1

描述

虚拟系统?

public

VPN实例

public

安全区域

untrust

模式?

☒ 路由
☐ 交换
☐ 旁路检测
☐ 接口对

IPv4

IPv6

连接类型

☒ 静态IP
☐ DHCP

IP地址

1.1.1.1/24

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”。

默认网关

取消

确定

在 FW 上选择“网络 > 接口” 单击 GigabitEthernet 0/0/2 对应的 ，按照如下参数进行配置：

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

trust

模式

☒ 路由
☐ 交换
☐ 旁路检测
☐ 接口对

IPv4

IPv6

连接类型

☒ 静态IP
☐ DHCP

IP地址

10.1.2.1/255.255.255.0

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”。

默认网关

取消

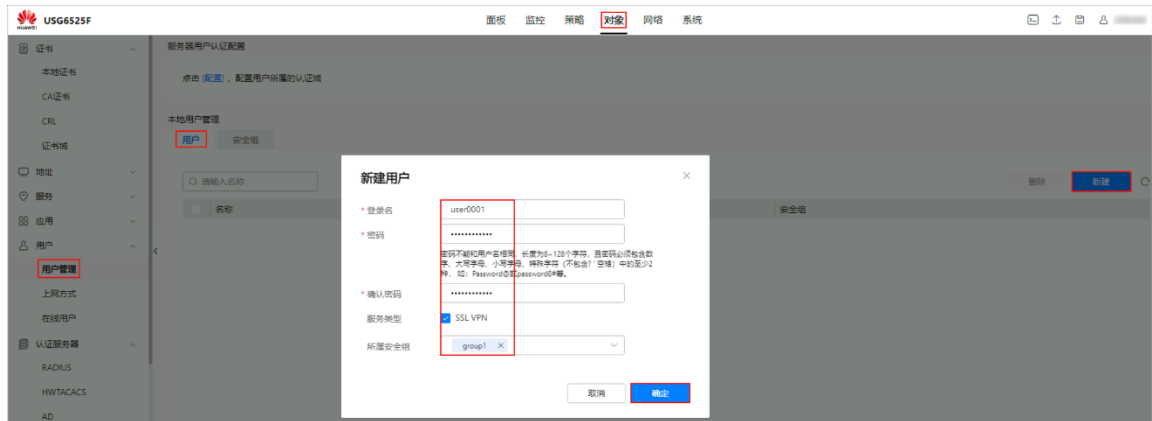
确定

步骤 2 配置用户和认证。

选择“对象 > 用户 > default”，按如下参数配置。

用户 user0001 所属的用户组为“/default/group1”，“认证类型”为本地认证，“密码”为 Password@123（需要注意，在新建用户 user0001 之前，应先新建安全组“/default/group1”，这样才能在新建用户时引用已创建好的用户安全组）。





步骤 3 配置 SSL VPN 网关。

选择“网络 > SSL VPN > SSL VPN”，单击“新建”，按照如下参数配置，配置完成后单击“下一步”。

新建 SSL VPN

1 网关配置

2 网络扩展

3 角色授权

* 网关名称

gateway

* 网关地址

添加网关地址

GE0/0/1

[接口IP]

端口 443 <1024-50000> 或查 443

域名 ①

使能链路备份

网关证书

公钥算法

RSA SM2

* 本地证书

default (默认证书)

用户认证

认证方式 ②

用户+密码

认证域

请选择认证域

DNS服务器 ②

添加DNS服务器

DNS域名后缀

隧道生命周期

会话超时时间

5 <1-1440>分钟

生命周期无限制

生命周期

1440 <60-2880>分钟

最大并发用户数

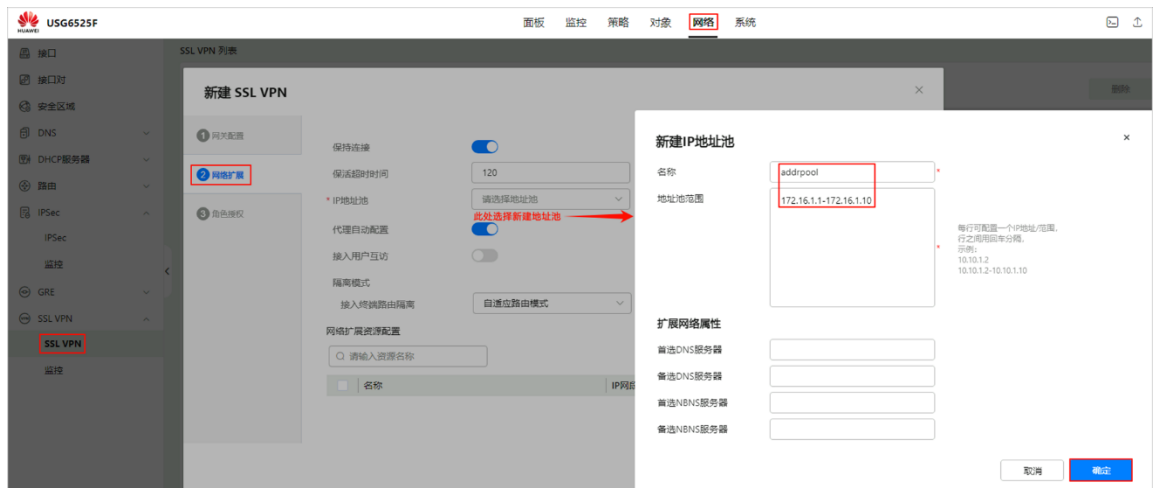
10 <1-100>

取消

< 上一步

下一步 >

在“网络扩展”模块新建地址池用于给远程接入的用户分配内网地址。完成后单击“下一步”。



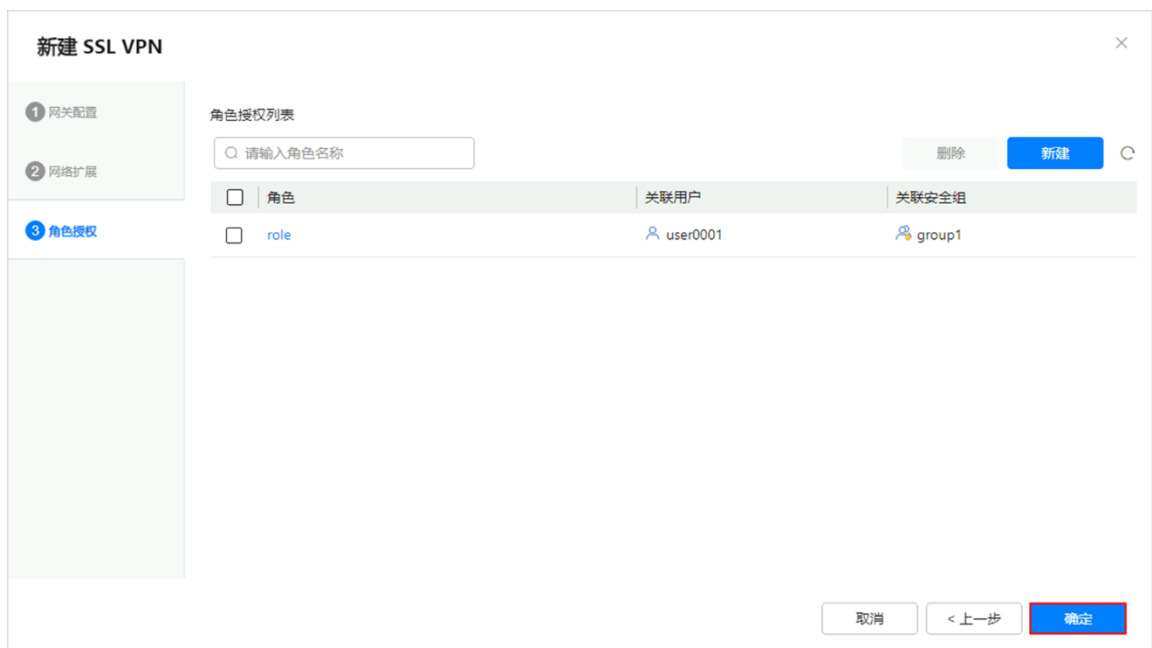
继续创建 SSL VPN 远程接入用户可以访问的内网资源。



配置 SSL VPN 的角色授权/用户。在“角色授权列表”中，单击“新建”，按下图配置角色授权参数。配置完成后单击“确定”。



返回“角色授权/用户”配置界面，单击“确定”。



步骤 4 配置安全策略。

配置从 Internet 到 FW 的安全策略，允许出差员工登录 SSL VPN 网关。选择“策略 > 安全策略 > 安全策略”。单击“新建”，按照如下参数配置安全策略 policy01。

新建安全策略

×

概述

名称

policy01

描述

策略组

-- NONE --

条件

ⓘ 当前未加载地区识别特征库。如需配置地区，请 [加载地区识别特征库](#)

源

安全区域

untrust

IP 地址/地区 ⓘ

any

目的

目的类型

安全区域

虚拟服务

安全区域

local

IP 地址/地区 ⓘ

1.1.1.1

服务 ⓘ

协议

请选择服务

更多

应用/用户/安全组/时间段/VLAN ID

动作

允许

禁止

内容安全检查

反病毒/入侵防御/URL过滤/内容过滤

取消

命令预览

确定

配置 FW 到内网的安全策略，允许出差员工访问总部资源。选择“策略 > 安全策略 > 安全策略”。单击“新建”，按照如下参数配置安全策略 policy02。

新建安全策略

概述

* 名称

policy02

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

IP 地址/地区 ①

172.16.1.0/24

目的

1

目的类型

安全区域

虚拟服务

安全区域

trust

IP 地址/地区 ①

10.1.2.0/24

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

取消

命令预览

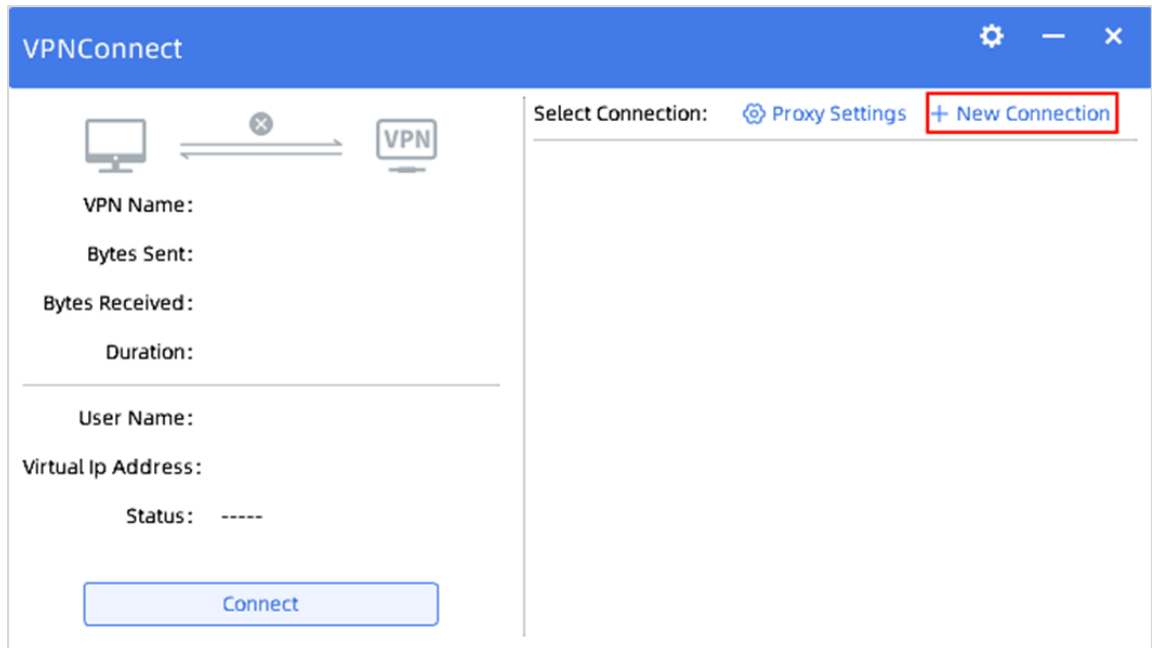
确定

总部 Server 的 IP 地址配置为 10.1.2.10/24，网关为 10.1.2.1，此处省略。

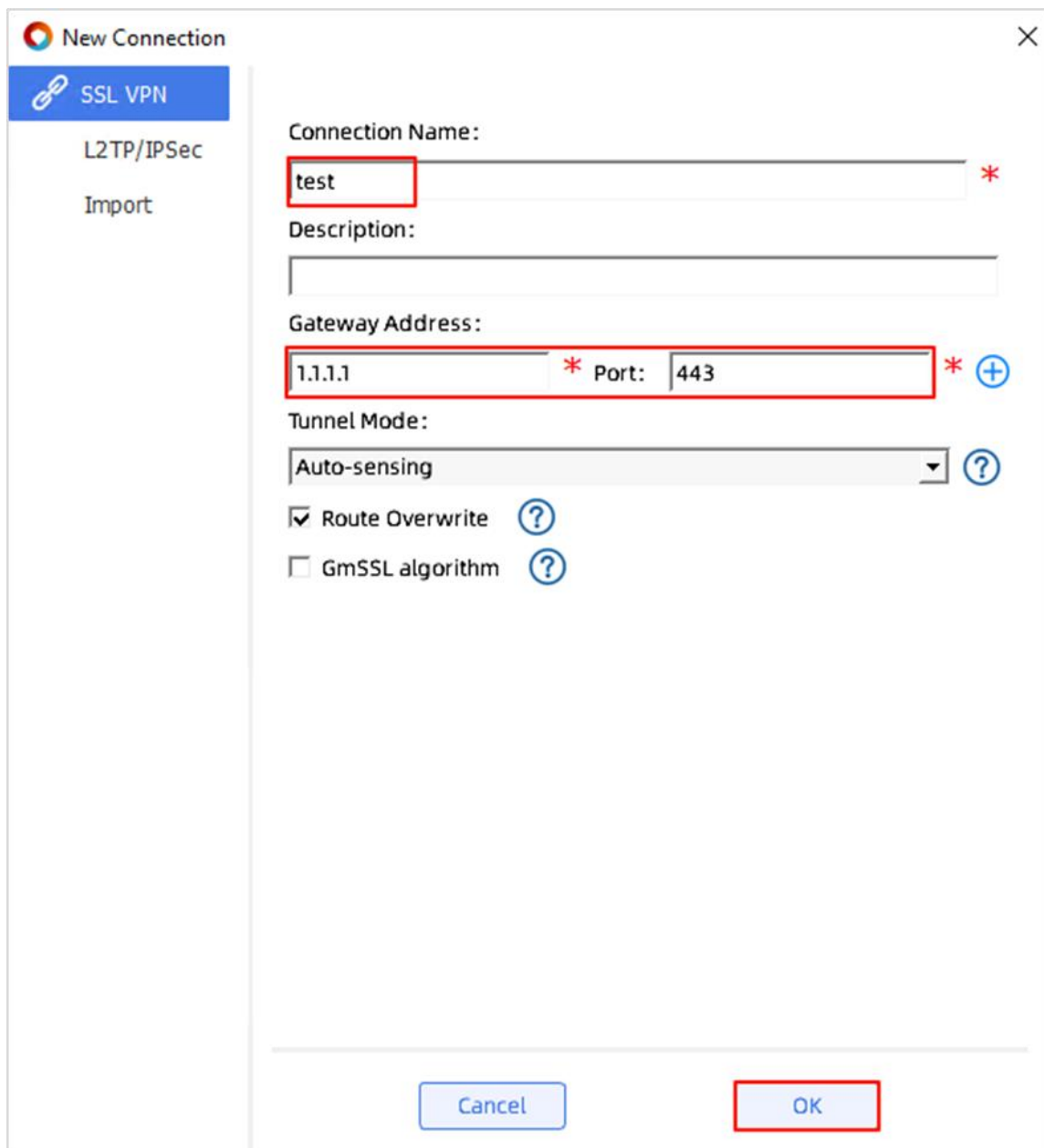
6.3 结果验证

在移动办公人员电脑终端打开“UniVPN”客户端，参考下图执行 SSL VPN 接入操作。

新建 SSL VPN 连接：



编辑 SSL VPN 连接参数:

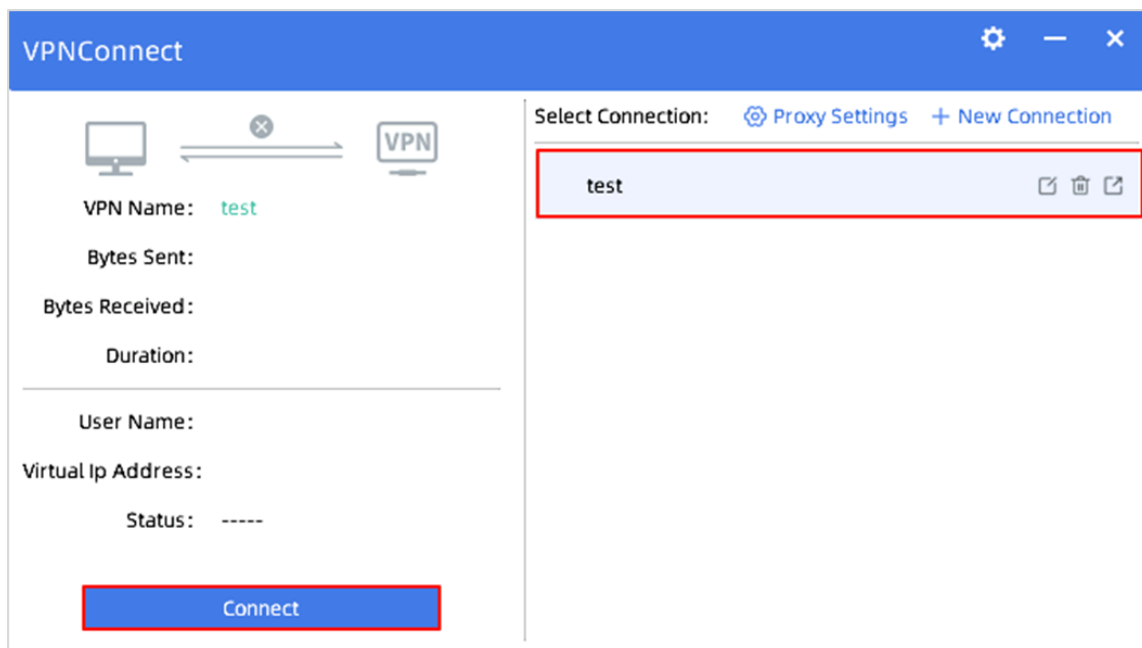


The image shows a 'New Connection' dialog box with a sidebar on the left containing three options: 'SSL VPN' (highlighted in blue), 'L2TP/IPSec', and 'Import'. The main area contains the following fields and controls:

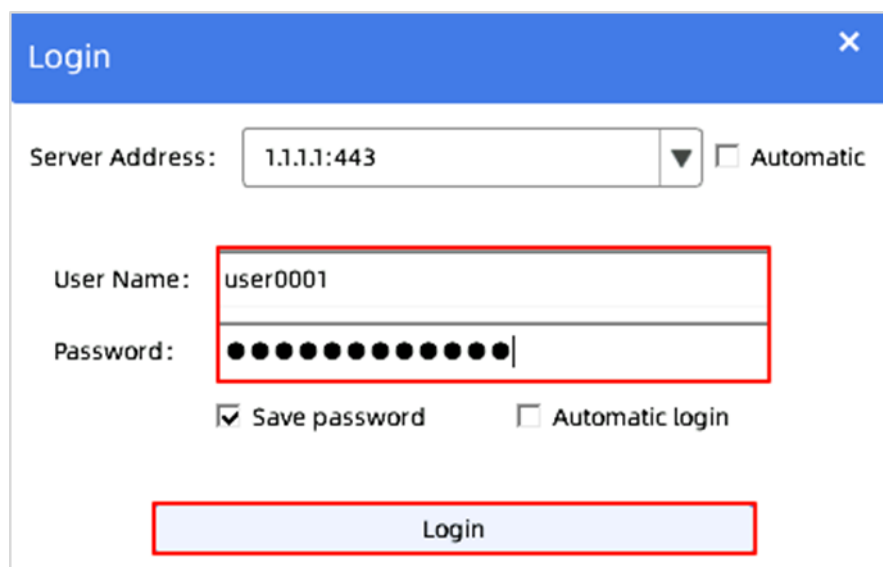
- Connection Name:** A text input field containing 'test', with a red asterisk (*) to its right.
- Description:** An empty text input field.
- Gateway Address:** A text input field containing '1.1.1.1', followed by a red asterisk (*), the label 'Port:', a text input field containing '443', another red asterisk (*), and a blue plus icon (+).
- Tunnel Mode:** A dropdown menu showing 'Auto-sensing' with a blue question mark icon (?) to its right.
- 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 are two buttons: 'Cancel' and 'OK' (which is highlighted with a red border).

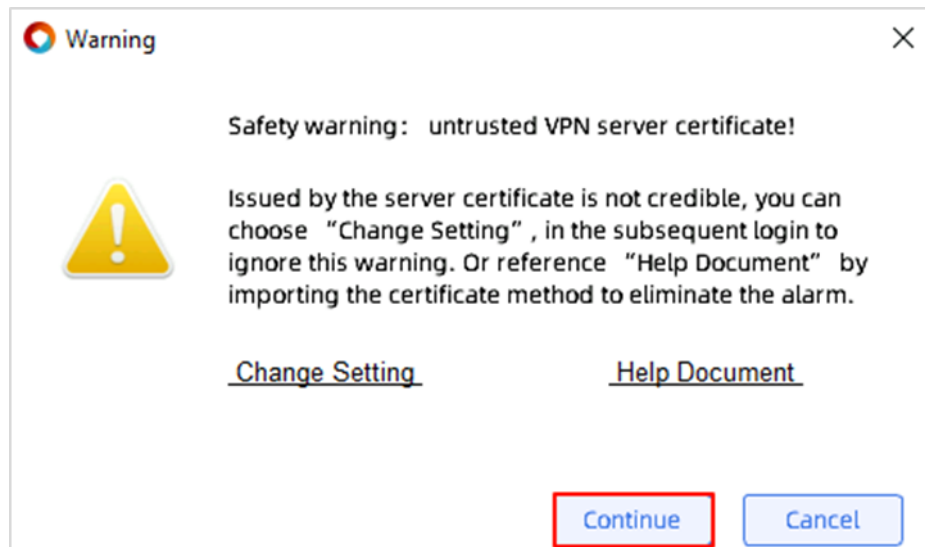
启动 SSL VPN 连接:



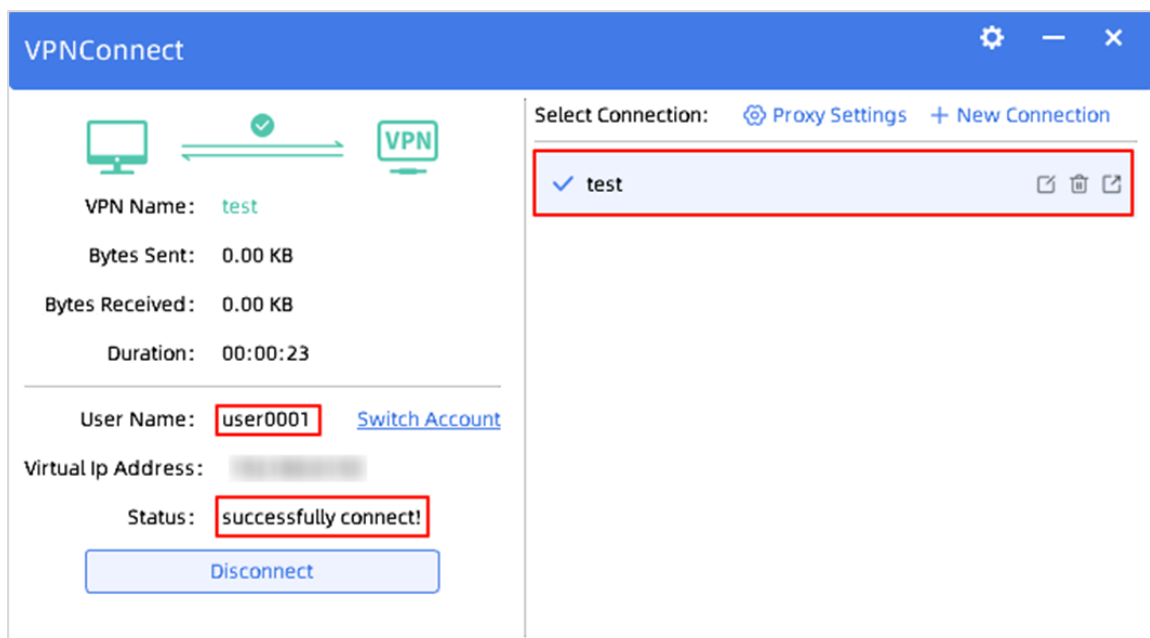
执行 SSL VPN 用户认证:



忽略证书告警:



SSL VPN 连接成功:



6.4 配置参考

6.4.1 FW 的配置

```
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 service-type ssl-vpn
```

```
internet-access mode password
reference user current-domain
#
interface GigabitEthernet0/0/1
undo shutdown
ip address 1.1.1.1 255.255.255.0
#
interface GigabitEthernet0/0/2
undo shutdown
ip address 10.1.2.1 255.255.255.0
#
firewall zone trust
set priority 85
add interface GigabitEthernet0/0/2
#
firewall zone untrust
set priority 5
add interface GigabitEthernet0/0/1
#
v-gateway gateway interface GigabitEthernet0/0/1 private
v-gateway gateway alias gateway
#
*****BEGIN***gateway**1****#
v-gateway gateway
basic
ssl version tlsv12
ssl timeout 5
ssl lifecycle 1440
ssl public-key algorithm rsa
ssl ciphersuit custom aes256-sha non-des-cbc3-sha aes128-sha
service
network-extension enable
network-extension keep-alive enable
network-extension keep-alive interval 120
network-extension netpool 172.16.1.1 172.16.1.10 255.255.255.0
netpool 172.16.1.1 default
network-extension mode manual
network-extension manual-route 10.1.2.0 255.255.255.0
security
policy-default-action permit vt-src-ip
certification cert-anonymous cert-field user-filter subject cn group-filter subject cn
certification cert-anonymous filter-policy permit-all
certification cert-challenge cert-field user-filter subject cn
certification user-cert-filter key-usage any
undo public-user enable
hostchecker
cachedcleaner
vpndb
```

```
group /default
group /default/group1
role
role default
role default condition all
role role
role role condition all
role role network-extension enable
****END****
#
ip address-set 10.1.1.0/24 type object
address 0 10.1.1.0 mask 24
#
ip address-set 10.1.2.0/24 type object
address 0 10.1.1.0 mask 24
#
ip address-set 1.1.1.1/24 type object
address 0 1.1.1.0 mask 24
#
ip address-set 172.16.1.0/24 type object
address 0 172.16.1.0 mask 24
#
security-policy
default action permit
rule name policy01
source-zone untrust
destination-zone local
destination-address address-set 1.1.1.1/24
service https
action permit
rule name policy02
source-zone untrust
destination-zone trust
source-address address-set 172.16.1.0/24
destination-address address-set 10.1.2.0/24
action permit
rule name pass
action permit
#
```

6.5 思考题

在完成 SSL VPN 接入后，远程接入电脑的 CMD 中路由表和 IP 地址会有什么变化？

参考答案：

CMD 中输入 route print 命令查看 IPv4 路由表，可以看到下发的 10.1.2.0/24 的路由；

CMD 中输入 ipconfig 命令查看本地网卡信息，可以看到网卡被分配了 172.16.1.1/24-172.16.1.10/24 中的某一个 IP 地址。