华为认证安全系列教程

HCNA-Security

实验指导手册

版本:2.5

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

目录

1 手册说明

1.1 适用范围

本手册适用于指导学员学习 HCNA-Security 中涉及的实验内容。主要实验设备为华为下一代防火墙，包括：USG6300&6500&6600 V100R001。

1.2 防火墙产品描述

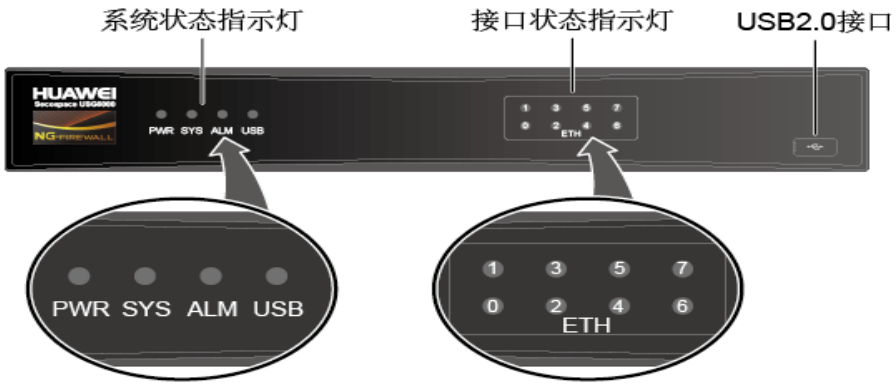
1.2.1 USG6320 产品描述

- **设备概述**

USG6320 为桌面型盒式 1U 设备，采用一体化机箱的结构设计，标配固定接口，内置风扇模块，不支持接口扩展，外接电源适配器供电。其一体化机箱尺寸为 300mm×220mm×44.5mm（宽×深×高），可以安装在 19 英寸标准机柜中。

- **前面板**

USG6320 前面板上提供 USB 2.0 接口、系统状态指示灯和接口状态指示灯。USG6320 前面板如下图所示。

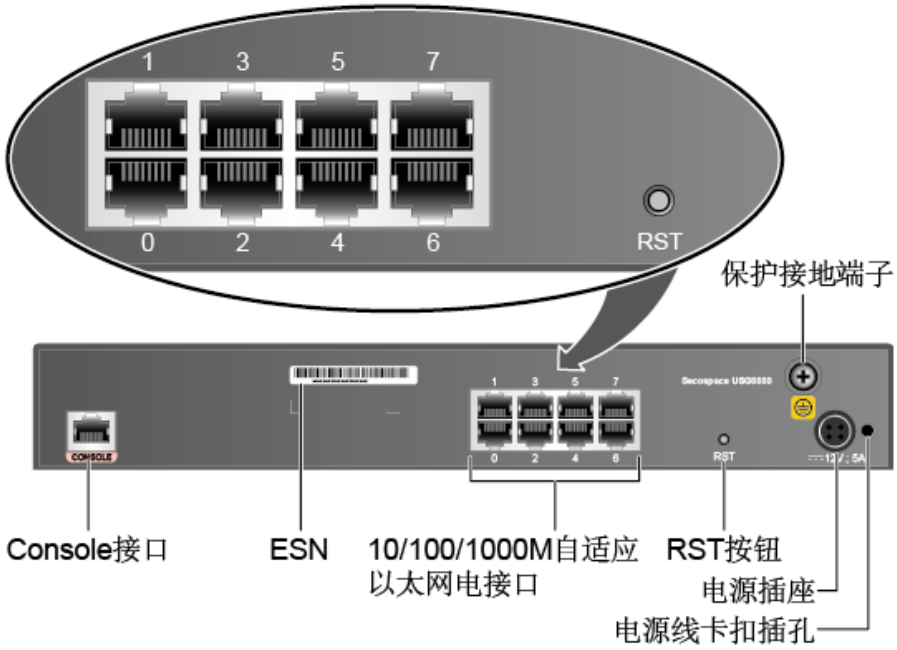


名称	描述
USB2.0	·插接 U 盘，通过 U 盘升级设备的系统软件等

接口状态指示灯 0-7（绿色）		·常亮：链路已经连通 ·每秒闪 8 次（8Hz）：有数据收发 ·常灭：链路没有连通
系统状态指示灯	PWR 指示灯（绿色）	·常亮：电源工作正常 ·常灭：电源故障或没有连接
	SYS 指示灯（绿色）	·常亮：系统处于上电加载或复位启动状态 ·每 2 秒闪 1 次（0.5Hz）：系统处于正常运行状态 ·每秒闪 2 次（2Hz）：系统处于启动中 ·每秒闪 8 次（8Hz）：系统软件或配置文件正在升级 ·常灭：系统故障
	ALM 指示灯（红色）	·常亮：系统运行出现故障 ·常灭：系统运行正常
	USB 指示灯（绿色）	·常亮：USB 2.0 接口已经连接。 ·常灭：USB 2.0 接口没有连接

- **后面板**

USG6320 后面板上提供多种固定接口、保护接地端子、RST 按钮和电源插座等。USG6320 后面板如下图所示。



名称	描述
Console 接口（RJ45）	Console 接口用于连接控制台，实现本地配置功能。
ESN	唯一标识设备的数字序列号。申请 License 文件时需要提供设备 ESN 信息。
0-7 （RJ45）	8 个 10/100/1000M 自适应以太网电接口，接口编号为 GigabitEthernet0/0/0～GigabitEthernet0/0/7。GigabitEthernet

	0/0/0 是带内管理口，默认 IP 地址为 192.168.0.1。
RST 按钮	当设备正常运行时，按下 RST 按钮将重新启动设备。建议按 RST 按钮前保存当前配置。
保护接地端子	用于连接保护地线的 M4 OT 端子，将保护地线连接到机柜、工作台、墙体的接地点或者机房中的接地排上。
电源插座	用于连接电源适配器的 4PIN 插头端。
电源线卡扣插孔	用于安装电源线卡扣。该卡扣用来绑定电源线，防止电源线松脱。

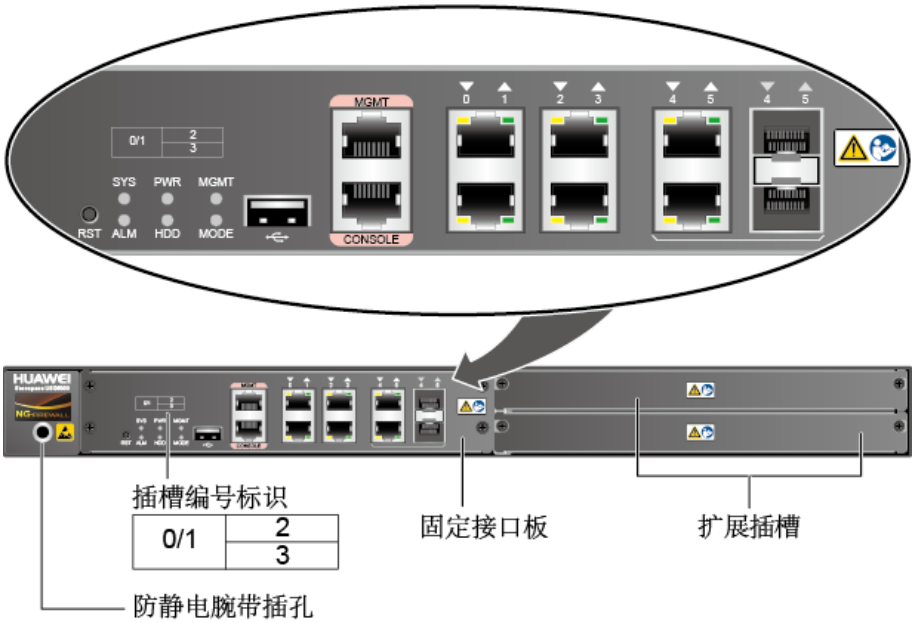
1.2.2 USG6330 产品描述

- **设备概述**

USG6330/6350/6360 采用一体化机箱的结构设计，由固定接口板、电源模块、内置风扇模块组成，并且支持选配硬盘、双电源和多种扩展卡来提升系统可靠性和接口的扩展能力。其一体化机箱尺寸为 442mm×421mm×44.4mm（宽×深×高），可以安装在 19 英寸标准机柜中。

- **前面板**

USG6330 前面板上提供固定接口板、防静电腕带插孔和多个扩展槽位。USG6330 前面板如下图所示。

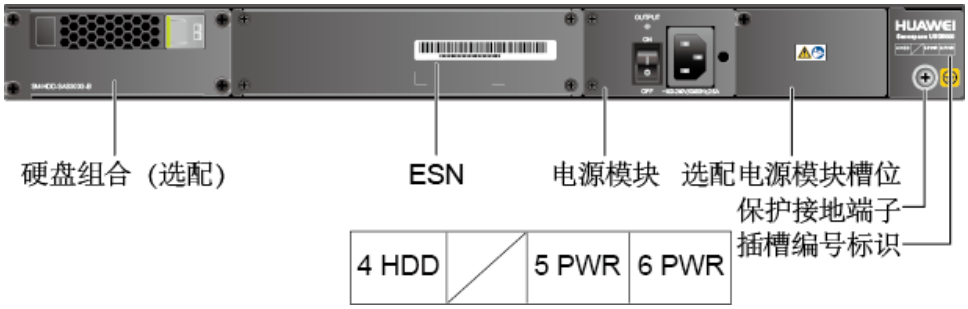


名称		描述
插槽号标识		标识设备支持的槽位类型及其槽位编号，0 代表带外管理口所在的槽位号，1 代表固定接口板所在的槽位号，2-3 代表 WSIC 槽位及其编号。
固定	MGMT 接口	带外管理口，10/100/1000M 自适应以太网接口。
	Console 接口	用于连接控制台，实现本地配置功能。

接口板	USB2.0 接口	插接 U 盘，通过 U 盘升级设备的系统软件等。
	0-3 （RJ45）	10/100/1000M 自适应以太网电接口。
	4-5（RJ45+SFP）	光电互斥接口，Combo 接口缺省工作在电接口状态。
扩展插槽		提供 2 个 WSIC 插槽。
防静电腕带插孔		用于插接防静电腕带（要求接地端子已连接好保护地线）。

- **后面板**

USG6330 后面板上提供电源模块、保护接地端子等，并提供硬盘插槽用于选购硬盘组合。USG6330 后面板如下图所示。



名称	描述
插槽标号标识	标识槽位号及其槽位上插接的模块类型。
电源模块	为设备提供电源输入和电源分配。标配单电源，支持选配双电源，组成 1+1 冗余备份。
硬盘组合	硬盘组合主要用于实时记录日志和报表。
ESN	唯一标识设备的数字序列号。
保护接地端子	用于连接保护地线的 M4 OT 端子，将保护地线连接到机柜、工作台的接地点或者机房中的接地排上。

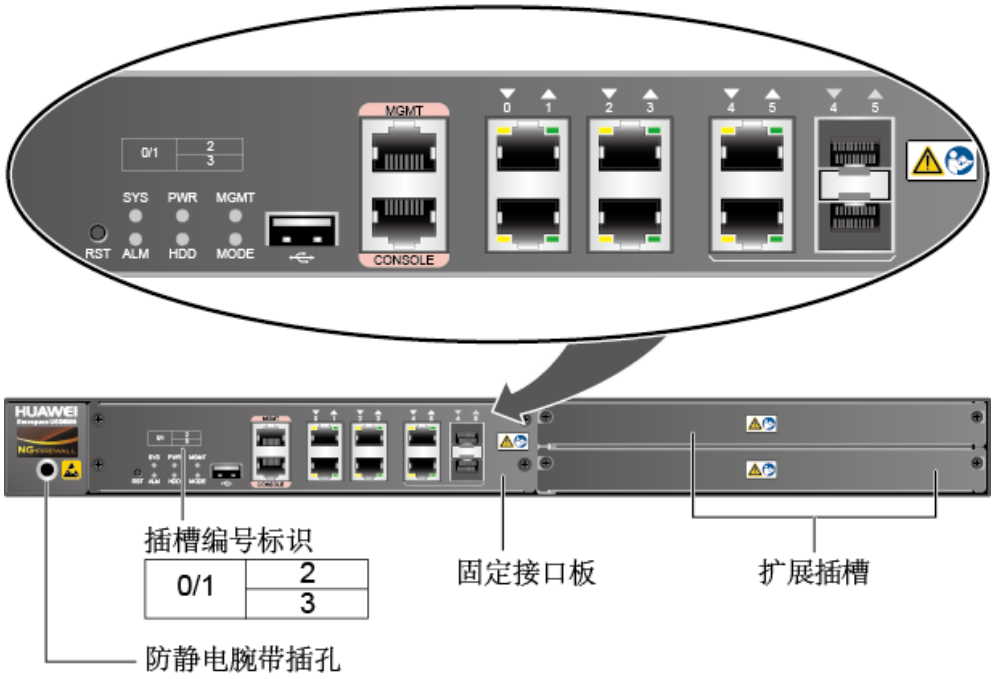
1.2.3 USG6530 产品描述

- **设备概述**

USG6530 采用一体化机箱的结构设计，由固定接口板、电源模块、内置风扇模块组成，并且支持选配硬盘、双电源和多种扩展卡来提升系统可靠性和接口的扩展能力。其一体化机箱尺寸为 442mm×421mm×44.4mm（宽×深×高），可以安装在 19 英寸标准机柜中。

- **前面板**

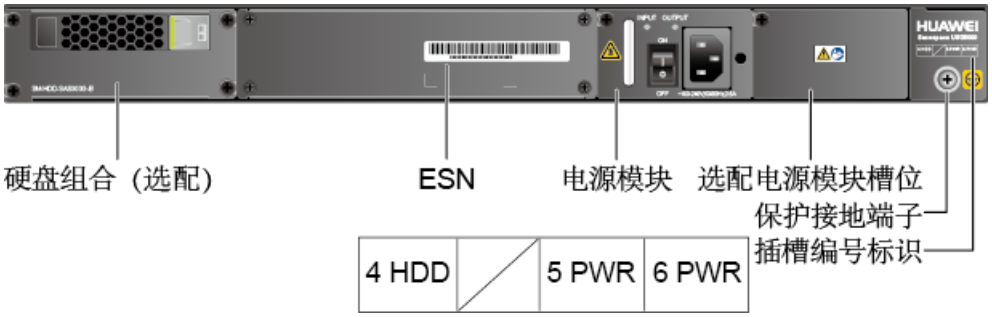
USG6530 前面板上提供固定接口板、防静电腕带插孔和多个扩展槽位。其前面板如下图所示。



名称		描述
插槽号标识		标识设备支持的槽位类型及其槽位编号，0 代表带外管理口所在的槽位号，1 代表固定接口板所在的槽位号，2-3 代表 WSIC 槽位及其编号。
固定接口板	MGMT 接口	带外管理口，10/100/1000M 自适应以太网接口。
	Console 接口	用于连接控制台，实现本地配置功能。
	USB2.0 接口	插接 U 盘，通过 U 盘升级设备的系统软件等。
	0-3 （RJ45）	10/100/1000M 自适应以太网电接口。
	4-5（Combo）	Combo 接口是一个逻辑接口，一个 Combo 接口对应面板上一个电接口和一个光接口，而在设备内部只有一个转发接口。
扩展插槽		提供 2 个 WSIC 插槽。
防静电腕带插孔		用于插接防静电腕带（要求接地端子已连接好保护地线）。

- **后面板**

USG6530 后面板上提供电源模块、保护接地端子等，并提供硬盘插槽用于选购硬盘组合。其后面板如下图所示。



名称	描述
插槽标号标识	标识槽位号及其槽位上插接的模块类型。
电源模块	为设备提供电源输入和电源分配。标配单电源，支持选配双电源，组成 1+1 冗余备份。
硬盘组合	硬盘组合 SM-HDD-SAS300G-B 由硬盘插卡和硬盘单元 SM-HDD-SAS300G-A 组成，主要用于实时记录日志和报表。
ESN	唯一标识设备的数字序列号。
保护接地端子	用于连接保护地线的 M4 OT 端子，将保护地线连接到机柜、工作台的接地点或者机房中的接地排上。

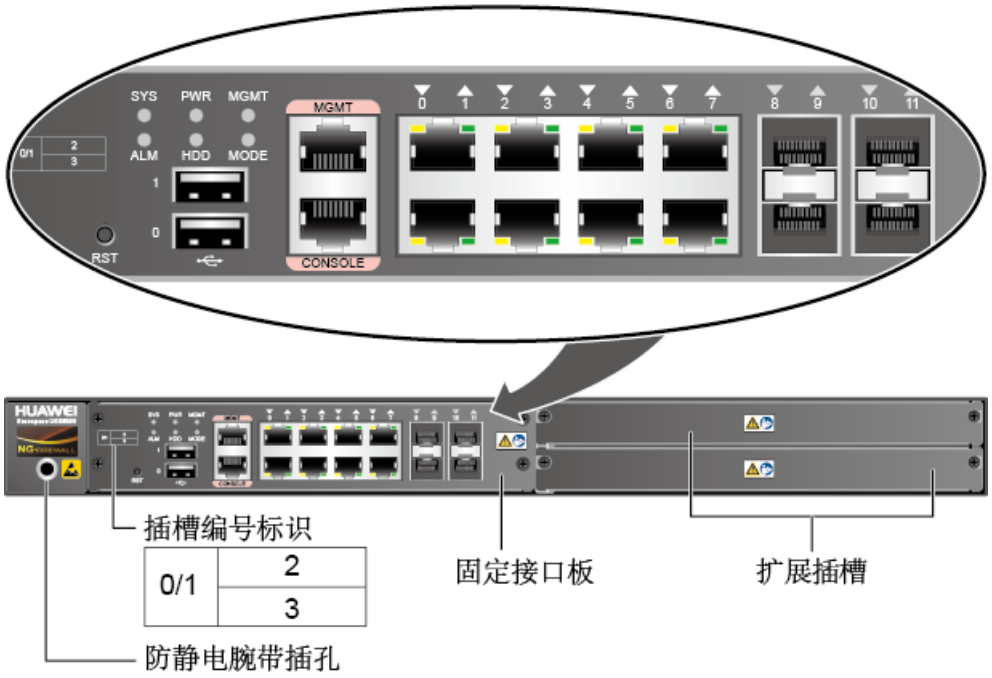
1.2.4 USG6550 产品描述

- **设备概述**

USG6550 采用一体化机箱的结构设计，由固定接口板、电源模块、内置风扇模块组成，并且支持选配硬盘、双电源和多种扩展卡来提升系统可靠性和接口的扩展能力。其一体化机箱尺寸为 442mm×421mm×44.4mm（宽×深×高），可以安装在 19 英寸标准机柜中。

- **前面板**

USG6550 前面板上提供固定接口板、防静电腕带插孔和多个扩展槽位。其前面板如下图所示。

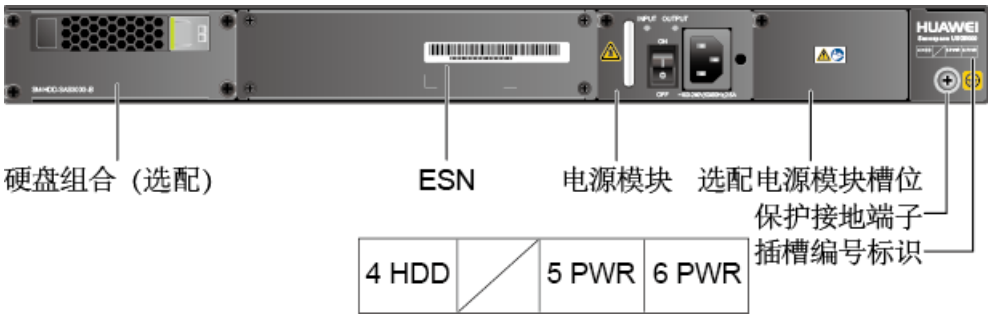


名称	描述
插槽号标识	标识设备支持的槽位类型及其槽位编号，0 代表带外管理口所在的槽位号，1 代表固定接口板所在的槽位号，2-3 代表

		WSIC 槽位及其编号。
固定接口板	MGMT 接口	带外管理口，10/100/1000M 自适应以太网接口。
	Console 接口	用于连接控制台，实现本地配置功能。
	USB2.0 接口	插接 U 盘，通过 U 盘升级设备的系统软件等。
	0-7 （RJ45）	10/100/1000M 自适应以太网电接口。
	8-11（SFP）	千兆以太网光接口。
扩展插槽		提供 2 个 WSIC 插槽。
防静电腕带插孔		用于插接防静电腕带（要求接地端子已连接好保护地线）。

- **后面板**

USG6550 后面板上提供电源模块、保护接地端子等，并提供硬盘插槽用于选购硬盘组合。其后面板如下图所示。



名称	描述
插槽标号标识	标识槽位号及其槽位上插接的模块类型。
电源模块	为设备提供电源输入和电源分配。标配单电源，支持选配双电源，组成 1+1 冗余备份。
硬盘组合	硬盘组合 SM-HDD-SAS300G-B 由硬盘插卡和硬盘单元 SM-HDD-SAS300G-A 组成，主要用于实时记录日志和报表。
ESN	唯一标识设备的数字序列号。
保护接地端子	用于连接保护地线的 M4 OT 端子，将保护地线连接到机柜、工作台的接地点或者机房中的接地排上。

1.2.5 物理接口编号方法

为便于对接口进行配置和维护，设备按照“接口类型 A/B/C”编号形式，并遵循如下的编号原则对接口进行编号：

- A 为槽位号，即接口卡所在槽位的编号。
- B 为子卡号（目前都没有子卡，此号为 0）。
- C 为接口序号，按照从下到上、从左到右的顺序依次编号，即“A/B/0～A/B/x”，x 为接口个数减 1。

例如，USG 的 2 号槽位安装了 5FSW 接口卡，那么各接口的编号为：Ethernet2/0/0、Ethernet2/0/1、Ethernet2/0/2、Ethernet2/0/3、Ethernet2/0/4。

1.3 终端安全产品描述

1.3.1 Agile controller 产品概述

Agile Controller 是华为最新研制的基于用户和应用的网络资源自动化控制系统。该系统定位是智慧的园区大脑，在 SDN 集中化控制思想的指导下，动态调配整个园区的网络与安全资源，让网络更敏捷的为业务服务。

Agile Controller 系统包括三部分：业务管理器（Service Manager，SM）、业务控制器（Service Controller，SC）、安全态势管理器（Security View，SV）以及 AnyOffice 客户端，网络接入设备作为方案的组成部分与 Agile Controller 服务器联动实现基于用户的接入控制和业务随行。

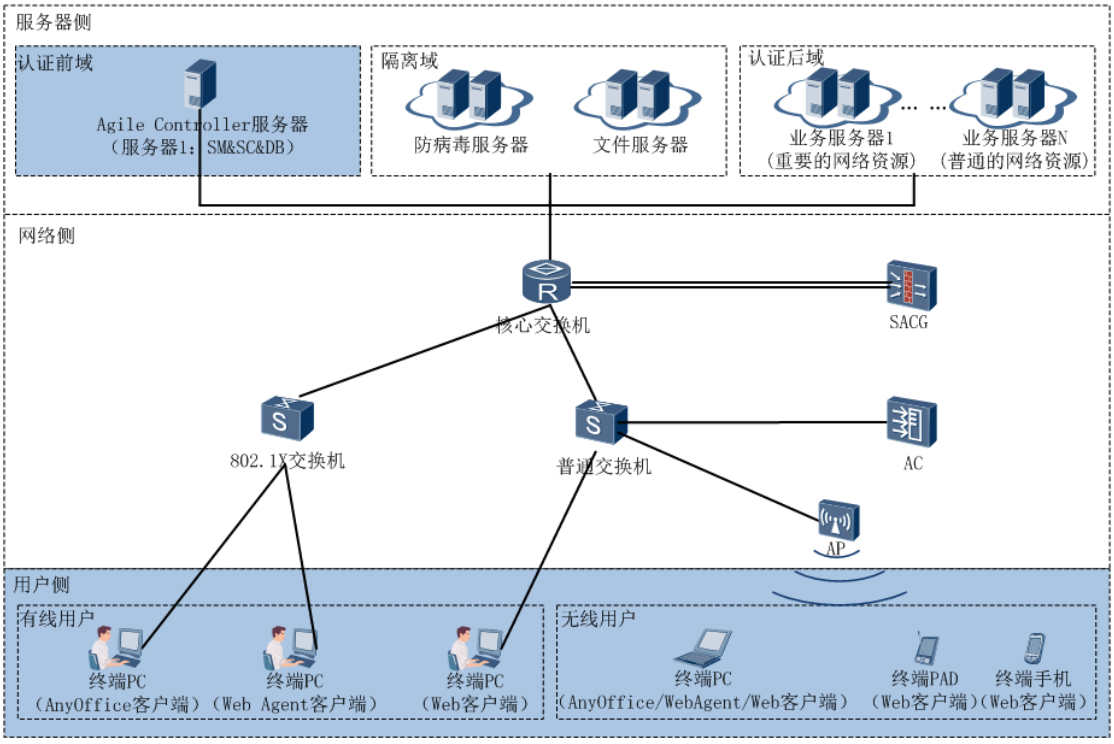
1.3.2 Agile Controller 系统部署

Agile Controller 的组网部件采用 C/S 和 B/S 两种架构。服务器侧组网部件包括：管理中心（MC）、业务管理器（SM）、业务控制器（SC）、安全态势管理器（SV）和日志采集与管理分析器（iRadar）。用户侧包括 AnyOffice 客户端、Web Agent 插件客户端和 Web 客户端。

名称	描述

管理中心 （MC）	Agile Controller 的管理中心，制定准入控制的总体策略，并将策略下发给各 SM 节点。
管理服务器 （SM）	Agile Controller 的管理入口，包括策略配置、部署的入口。SM 管理各个 SC，向已连接的 SC 发送实时指令，完成各种业务。
控制服务器 （SC）	Agile Controller 的功能控制中心，集成 AuthServer 服务器、Portal 服务器、RADIUS 服务器、Network 服务器，与网络接入设备联动实现基于用户的网络访问控制策略。
AnyOffice 客户端	Agile Controller 系统提供有 AnyOffice 准入认证客户端，用户可选择通过 AnyOffice 客户端进行网络接入认证，也可以选择使用标准 802.1x 客户端或主流浏览器进行认证。
网络接入设备	Agile Controller 系统支持多种类型的网络接入控制设备，包括 WLAN 的 AC/AP 设备、华为的 Portal 交换机、通用的标准 802.1X 交换机，以及华为的 SACG 网络接入控制网关等。

根据不同的网络特点、规模、带宽及质量，终端管理数量，控制服务器失效转移等要求，Agile Controller 的部署方式可分为集中式、分布式和分级式。对于小规模、终端数量小于 2000 个的网络一般采用集中式部署 Agile Controller。单服务器集中式部署方案如下图所示。



1.3.3 Agile Contoller 性能指标

- 服务器性能指标

性能项目	指标
RADIUS 服务器-本地账号	100 次认证/秒

Portal 服务器-本地账号	40 次认证/秒
终端识别性能（非扫描）	1000 个/分钟
最大终端数	10 万
管理的最大设备数量	2000

- AnyOffice 客户端（Windows 平台）性能指标

性能项目	指标
内存占用	40-50M
认证时间（非 802.1X）	<=3 秒
认证时间（802.1X）	<=10 秒
认证时间（802.1X 证书）	<=15 秒

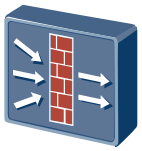
注：采用配置为 CPU-2GHz，内存-4G，操作系统-Win7

1.4 图示

Internet

PC终端

网络云图



USG系列防火墙

便携PC终端

通用路由器

无线基站

服务器

1.5 安全声明

1.5.1 加密算法的声明

目前设备采用的加密算法包括 DES、3DES、AES、RSA，验证算法包括 SHA1、SHA2、MD5，具体采用哪种加密算法请根据场景而定。请优先采用我们的建议，否则会造成无法满足您安全防御的要求。

- 对称加密算法建议使用 AES（128 位及以上密钥）
- 非对称加密算法建议使用 RSA（2048 位及以上密钥）
- 哈希算法建议使用 SHA2（256 及以上密钥）
- HMAC（基于哈希算法的消息验证码）算法建议使用 HMAC-SHA2
- DES、3DES、RSA 和 AES 加密算法是可逆的。对于协议对接类的应用场景，存储在本地的密码必须使用可逆加密算法。
- SHA1、SHA2 和 MD5 加密算法是不可逆的。对于管理员类型的密码，必须采用不可逆加密算法。

1.5.2 特性使用的声明

- 设备支持通过 FTP、TFTP、SFTPv1&v2 及 FTPS 传输文件。使用 FTP、TFTP、SFTP v1 协议存在安全风险，建议您使用 SFTPv2 或 FTPS 方式进行文件操作。
- 设备支持通过 Telnet 协议和 STelnetv1&v2 协议登录。使用 Telnet 和 STelnetv1 协议存在安全风险，建议您使用 STelnetv2 登录设备。

2 如何登录防火墙设备

2.1 通过 Console 口登录设备（Putty）

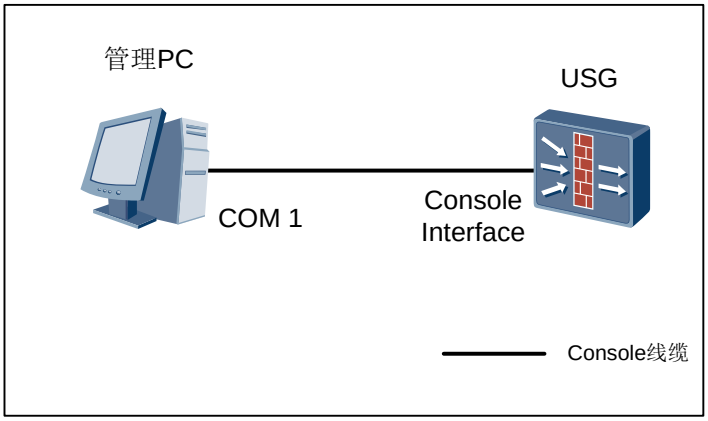
实验目的

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

组网设备

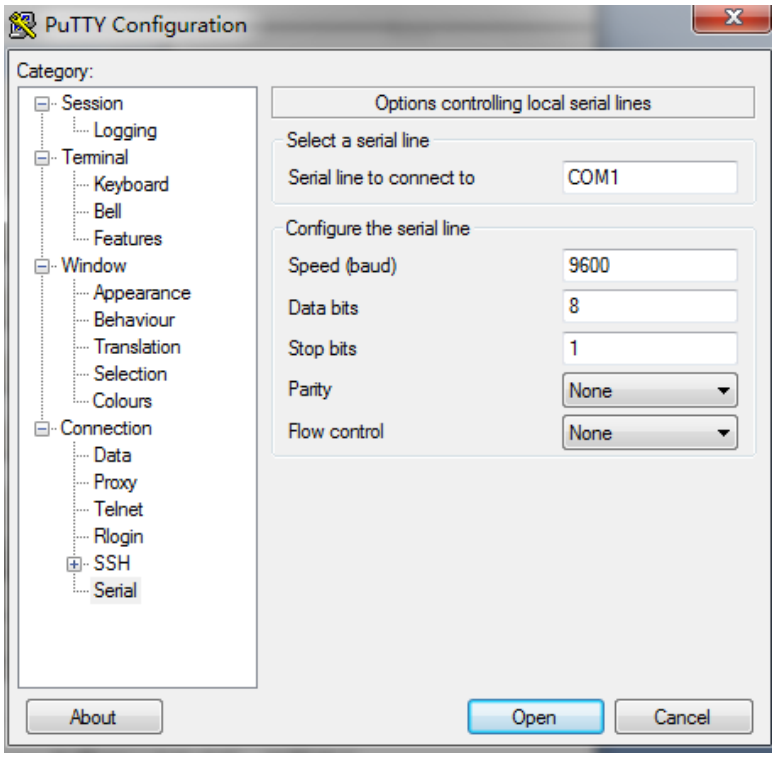
USG 防火墙 1 台，PC 机 1 台。

实验拓扑图

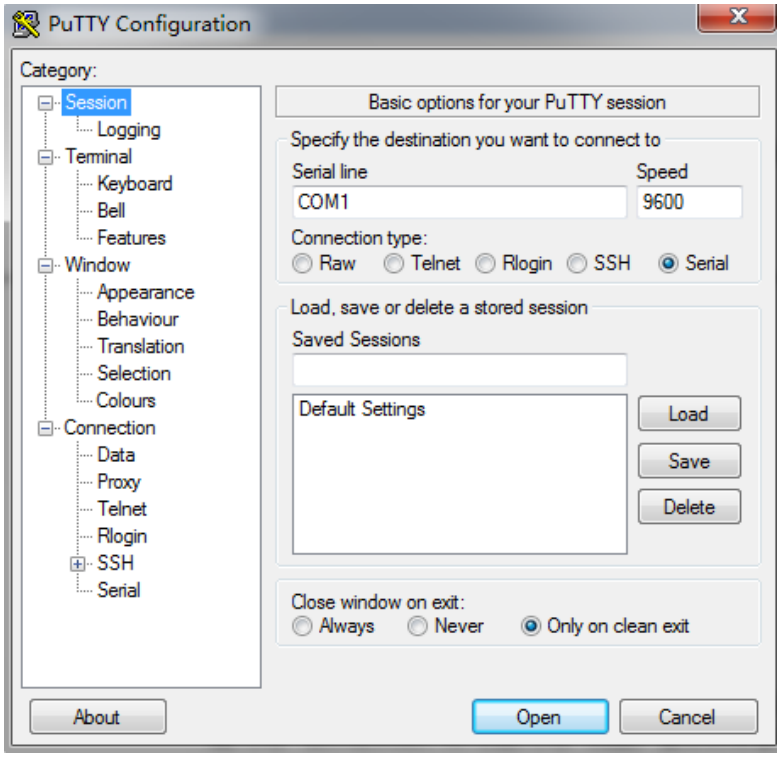


实验步骤

Step 1 下载 Putty 软件到本地并双击运行该软件。配置管理 PC 连接设备的 COM 口参数。具体参数配置如图所示。



Step 2 单击“Open”，即可进入命令行配置界面。



Step 3 在 PC 仿真终端上，首先按下“Enter”键，然后按照提示输入用户名和密码，即可进入用户视图，登录到设备上。

验证结果

```
**********************************************************
```

```
*                  All rights reserved 2013-2014                  *
*           Without the owner's prior written consent,            *
* no decompiling or reverse-engineering shall be allowed. *
* Notice:                                                          *
*          This is a private communication system.                 *
*     Unauthorized access or use may lead to prosecution. *
************************************************************
```

2.2 通过 Web 方式登录设备（默认方式登录）

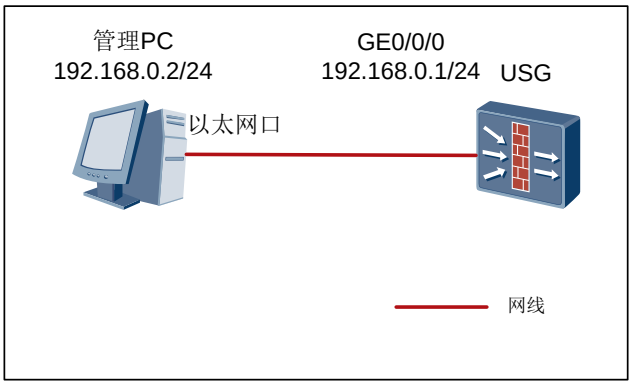
实验目的

在出厂配置下，管理 PC 通过 MGMT 口登录设备，可实现对设备的管理和配置。

组网设备

USG 防火墙 1 台，PC 机 1 台。

实验拓扑图



实验步骤

Step 1 设备物理连接后，将所有设备上电，并且保证设备运行正常。

Step 2 管理 PC 网卡和 USG 防火墙 GE0/0/0 接口正常连接网线。

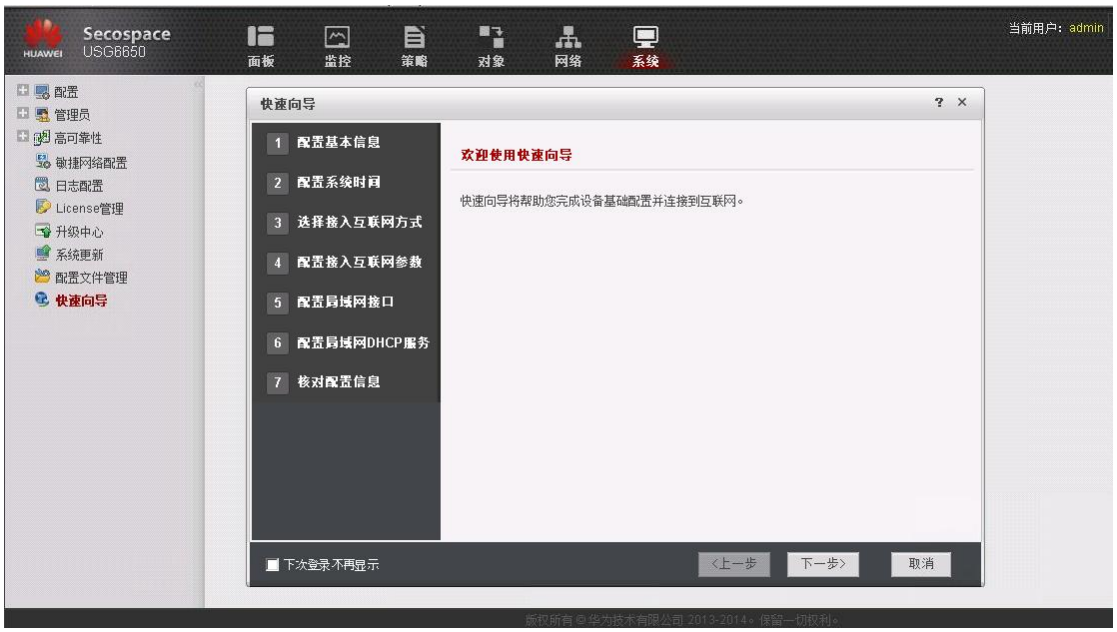
Step 3 配置管理 PC 的 IP 地址为 192.168.0.2/24。

Step 4 管理 PC 通过浏览器访问 https://192.168.0.1:8443，输入用户名 admin，密码 Admin@123，检查是否可以登录设备。如果成功登录则表示配置成功，否则请检查配置。

Step 5 修改缺省管理员账号的密码后，单击“确定”，进入 Web 界面。

Note：缺省情况下，设备的 GE0/0/0 的 IP 地址是 192.168.0.1，并开启 HTTPS 管理。用户可以通过用户名 admin，密码 Admin@123 登录。

验证结果



2.3 配置 Telnet 登录设备

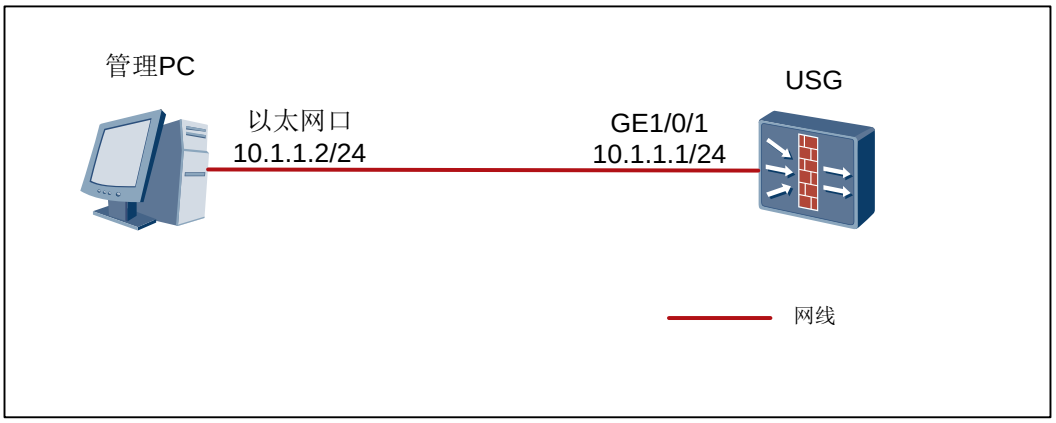
实验目的

通过配置使终端通过 Telnet 方式登录设备，实现对设备的配置和管理。

组网设备

USG 防火墙 1 台，PC 机 1 台。

实验拓扑图



实验步骤 - CLI

Step 1 通过 Console 口登录 USG 防火墙。（参见 2.1 章节，通过 Console 方式登录设备。）

Step 2 开启 Telnet 服务。

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

Step 3 配置登录接口。

以下面的情况为例进行配置：本地用户通过 Telnet 方式接入到 USG 防火墙的 GE1/0/1 接口，该接口的 IP 地址为 10.1.1.1，子网掩码为 255.255.255.0。（如使用管理口 GE0/0/0，则无需执行此步骤。）

a. 配置接口 IP 地址以及接口的访问控制功能，允许管理员通过接口 Telnet 登录设备

```
[USG] interface GigabitEthernet 1/0/1
[USG-GigabitEthernet1/0/1] ip address 10.1.1.1 24
[USG-GigabitEthernet1/0/1] service-manage enable
[USG-GigabitEthernet1/0/1] service-manage telnet permit
[USG-GigabitEthernet1/0/1] quit
```

b. 配置接口加入安全区域。

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

Step 4 配置用户信息。

a. 配置 VTY 管理员认证方式为 AAA。

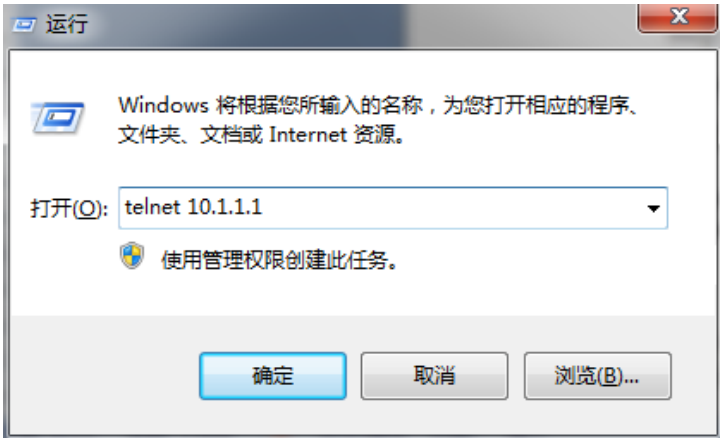
```
[USG] user-interface vty 0 4
[USG-ui-vty0-4] authentication-mode aaa
[USG-ui-vty0-4] quit
```

b. 配置 Telnet 管理员。新建管理员，用户名为 telnetuser，密码为 Admin@123，级别为 level3。

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

Step 5 管理 PC 的配置。

在 PC 上选择“开始 > 运行”，显示“运行”窗口，在“打开”中输入 telnet 10.1.1.1 如图所示，单击“确定”，开始连接 USG。



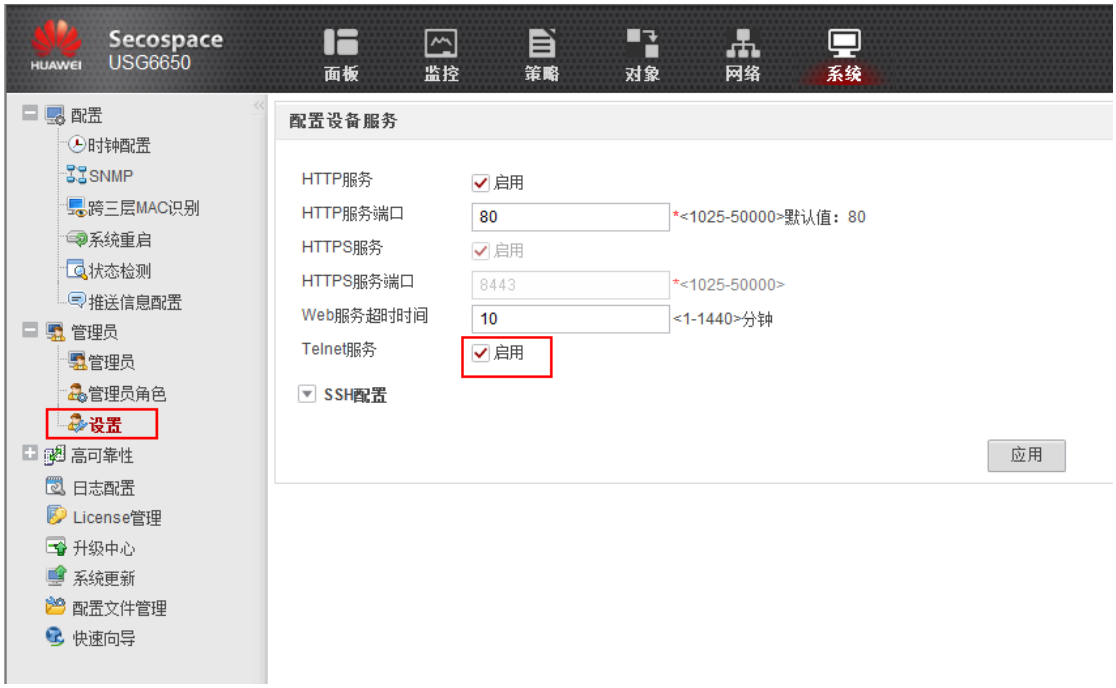
Step 6 按照提示输入用户名和密码，即可进入用户视图，登录到设备上。

实验步骤 - Web

Step 1 通过 Web 进入 USG 用户视图。 （参见 2.2 通过 Web 方式登录设备。）

Step 2 开启 Telnet 服务.

选择“系统 > 管理员 > 设置”，勾选 Telnet 服务复选框。

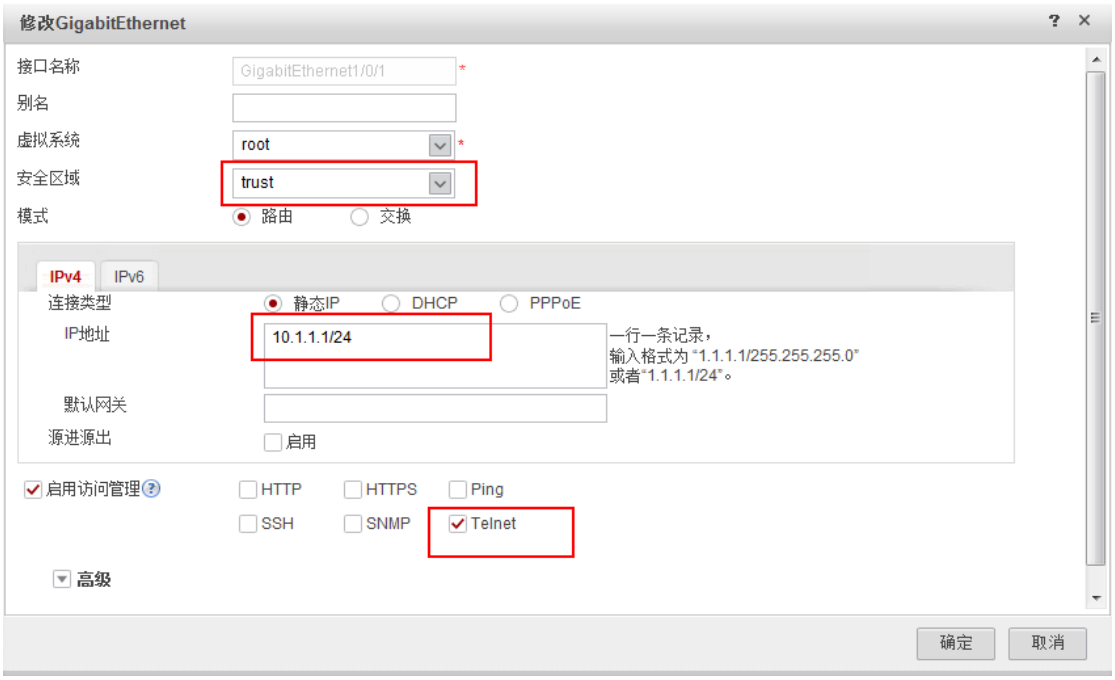


Step 3 配置登录接口.

以下面的情况为例进行配置：本地用户通过 Telnet 方式接入到 USG 防火墙的 GE1/0/1 接口，接口的 IP 地址为 10.1.1.1，子网掩码为 255.255.255.0。

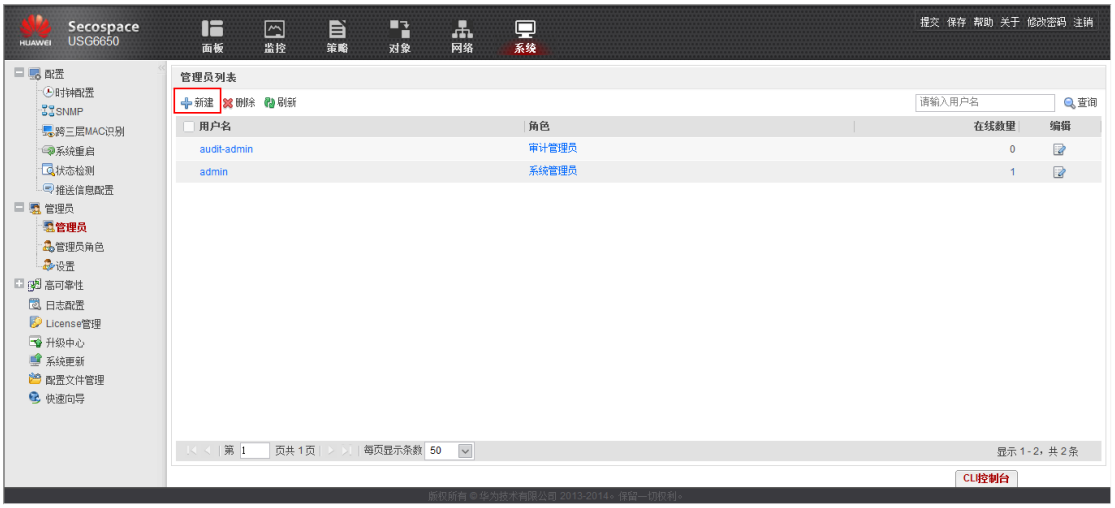
a. 选择“网络>接口>GE1/0/1”

b. 配置接口加入 Trust 区域、接口 IP、接口允许 Telnet 管理

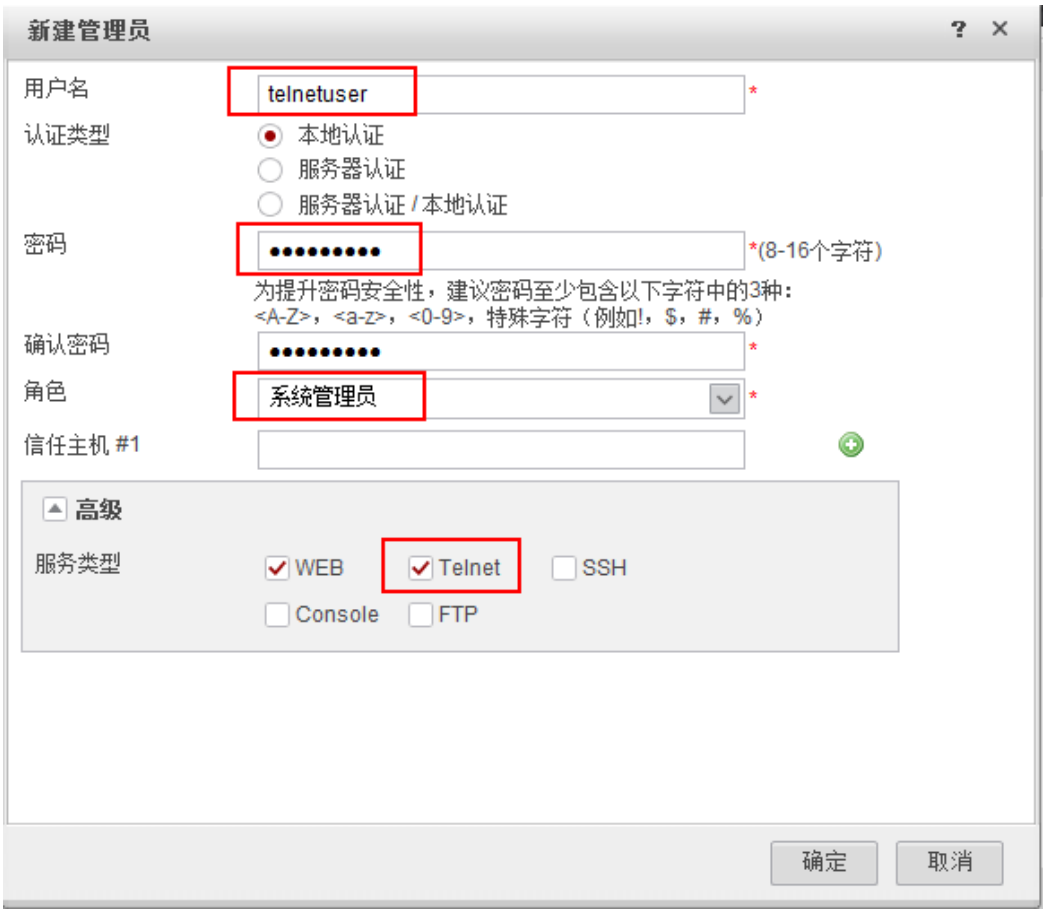


Step 4 配置登 Telnet 管理员.

a. 选择“系统>管理员>管理员”，单击“新建”。

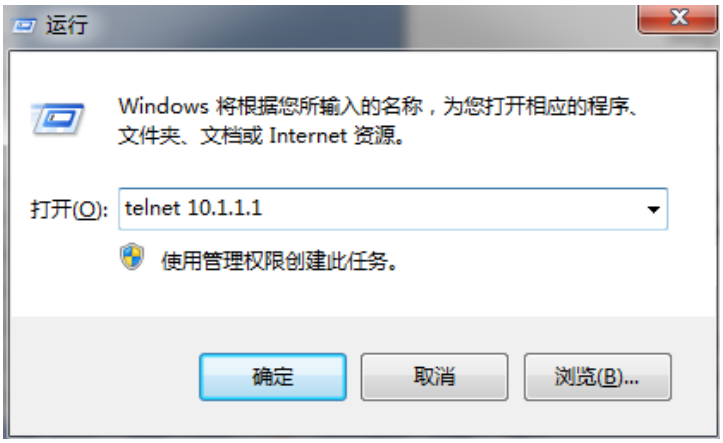


b. 配置 Telnet 用户名为 telnetuser，密码为 Admin@123、管理员角色为“系统管理员”，并勾选 Telnet 服务类型。



Step 5 本地管理员 PC 上的配置。

在 PC 上选择“开始 > 运行”，显示“运行”窗口，在“打开”中输入 telnet 10.1.1.1 如图所示，单击“确定”，开始连接 USG。



Step 6 按照提示输入用户名和密码，即可进入用户视图，登录到设备上。

验证结果

```
**************************************************************
*                  All rights reserved 2013-2014                  *
```

```
*            Without the owner's prior written consent,          *
* no decompiling or reverse-engineering shall be allowed. *
* Notice:                                                          *
*          This is a private communication system.                 *
*     Unauthorized access or use may lead to prosecution. *
************************************************************
```

2.4 配置 Web 方式登录设备

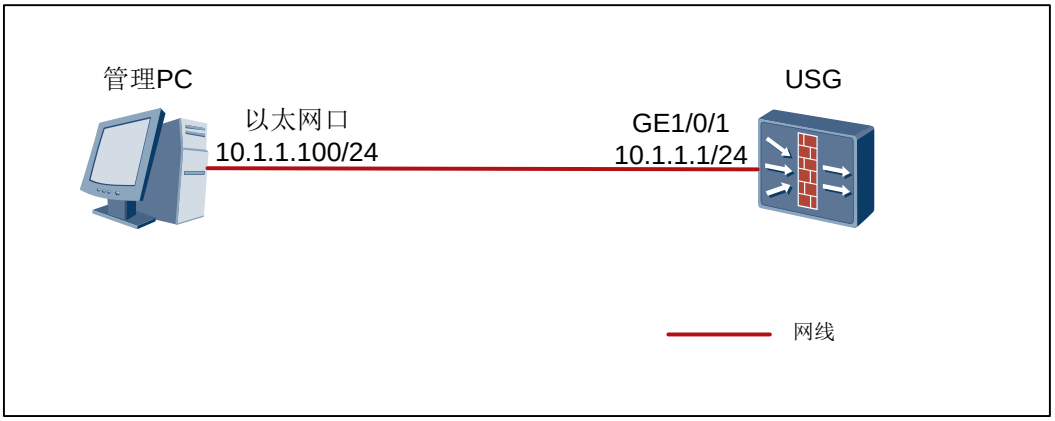
实验目的

掌握基于 Web 方式管理 USG 防火墙设备的方法。

组网设备

USG 防火墙 1 台，PC 机 1 台。

实验拓扑图



实验步骤 - CLI

Step 1 设备物理连接后，将所有设备上电，并且保证设备运行正常。

Step 2 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
```

Note:

1. 执行 Security 参数，则开启 Https 管理；如不执行 Security 参数，则是开启 Http 设备管理。

2. 不允许 Https 和 Http 管理使用相同的端口，这样配置会导致端口冲突。

Step 3 配置登录接口。

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 10.1.1.1 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
```

Step 4 配置 Web 用户。

```
[USG] aaa
[USG-aaa] manager-user webuser
[USG-aaa-manager-use-webuser] password
Enter Password:
Confirm Password:
[USG-aaa-manager-use-webuser] level 3
[USG-aaa-manager-use-webuser] service-type web
[USG-aaa-manager-use-webuser] quit
```

Step 5 配置管理 PC 的 IP 地址为 10.1.1.100/24。管理 PC 通过浏览器访问 https://10.1.1.1:8443。

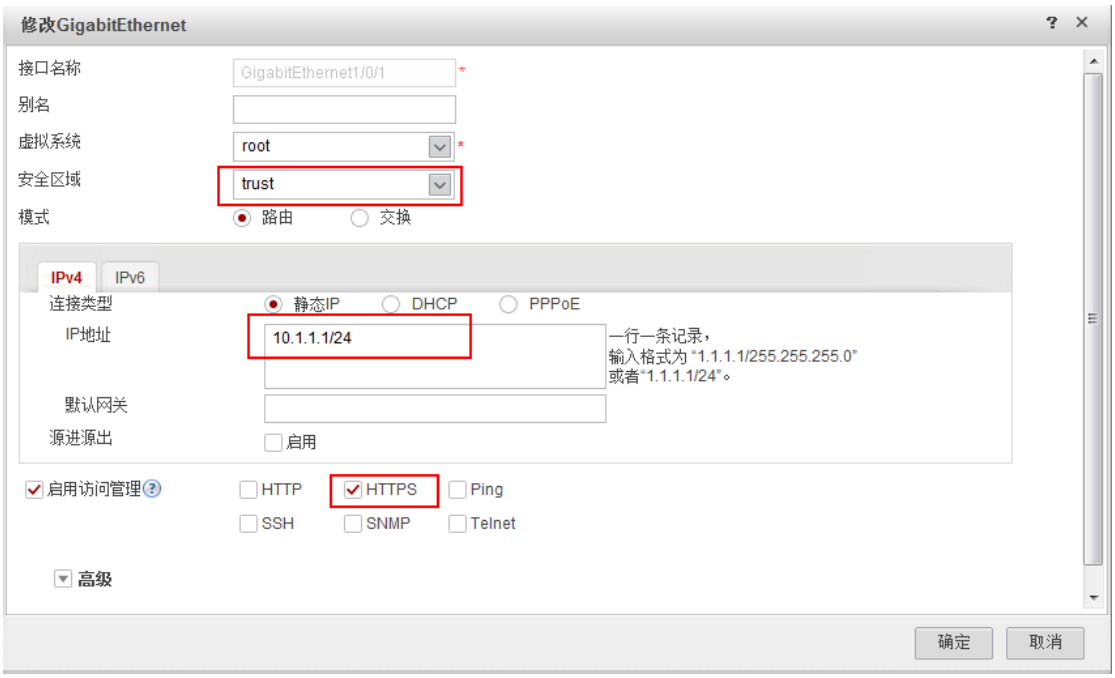
实验步骤 - Web

Step 1 Web 登录设备建立连接后，将所有设备上电，并且保证设备运行正常。

Step 2 配置登录接口。

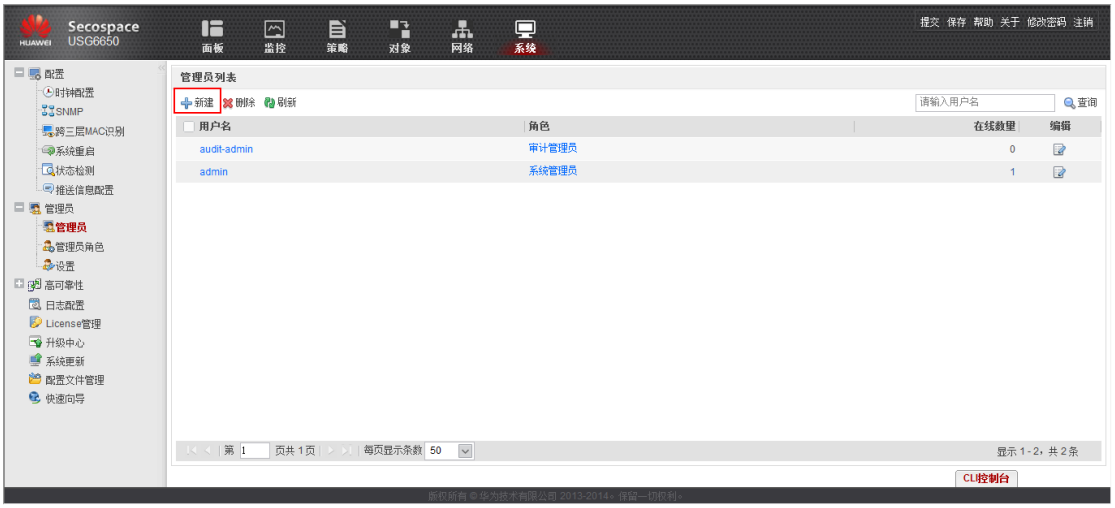
a. 选择“网络>接口>GE1/0/1”。

b. 配置接口加入 Trust 区域，配置接口 IP，启用接口 Https 管理功能。

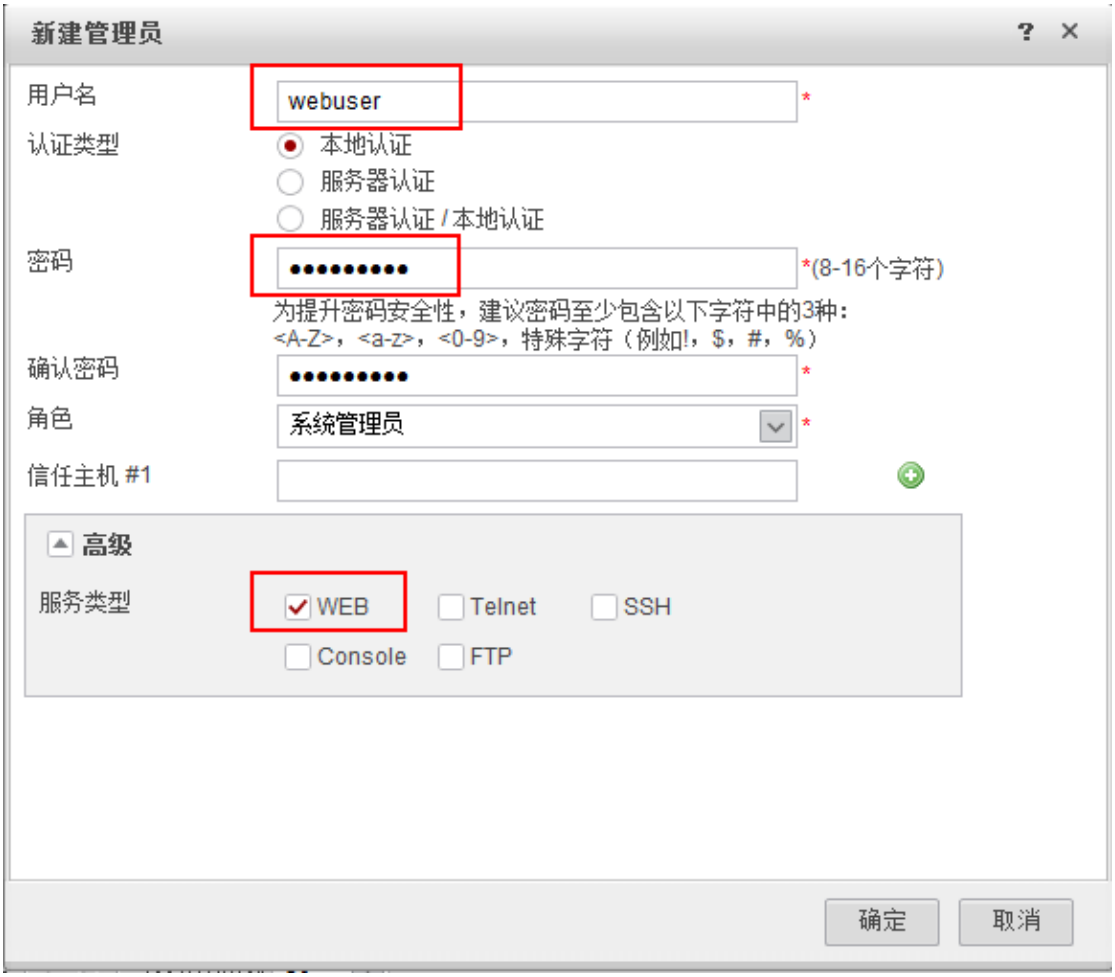


Step 3 创建管理员

a. 选择“系统>管理员>管理员”，单击“新建”。



b. 配置 Web 用户名为 webuser，密码为 Admin@123，管理员角色为“系统管理员”，服务类型为“WEB”。



Step 4 启动 Web 管理功能

选择“系统 > 管理员 > 设置”，勾选“HTTPS 服务”复选框。

Step 5 配置管理 PC 的 IP 地址为 10.1.1.100/24。 管理 PC 通过浏览器访问 https://10.1.1.1:8443。

验证结果

提示安全证书警告，选择”继续浏览此网站”。

2.5 配置 SSH 方式登录设备

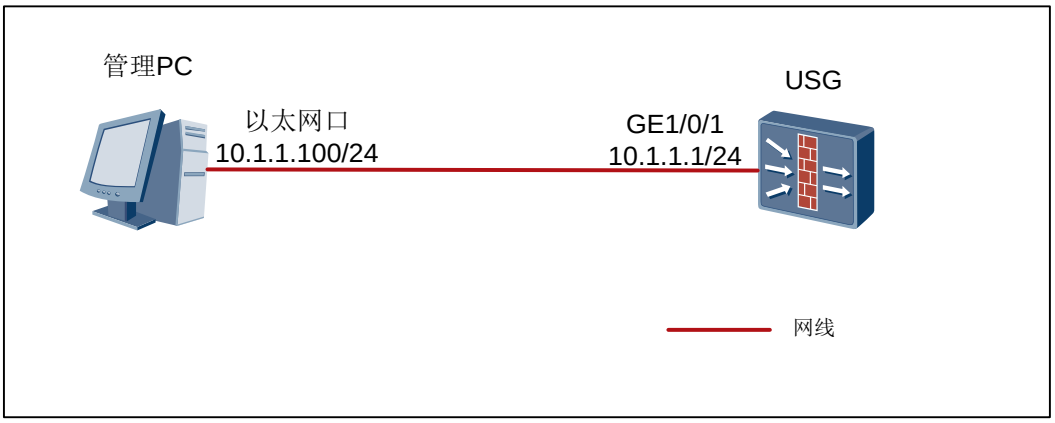
实验目的

掌握基于 SSH 方式管理 USG 防火墙设备的方法。

组网设备

USG 防火墙 1 台，PC 机 1 台。

实验拓扑图



实验步骤 - CLI

Step 1 设备物理连接后，将所有设备上电，并且保证设备运行正常。

Step 2 启用 STelnet 服务。

```
[USG] stelnet server enable
```

Step 3 配置登录接口。

a. 配置接口 GE1/0/1 接口的 IP 地址为 10.1.1.1/24。（略）

b. 启用 SSH 服务以及接口的访问控制功能。

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

c. 将 GE1/0/1 接口加入安全区域。（略）

Step 4 配置 VTY 用户界面。

```
[USG] user-interface vty 0 4
[USG-ui-vty0-4] authentication-mode aaa
[USG-ui-vty0-4]quit
```

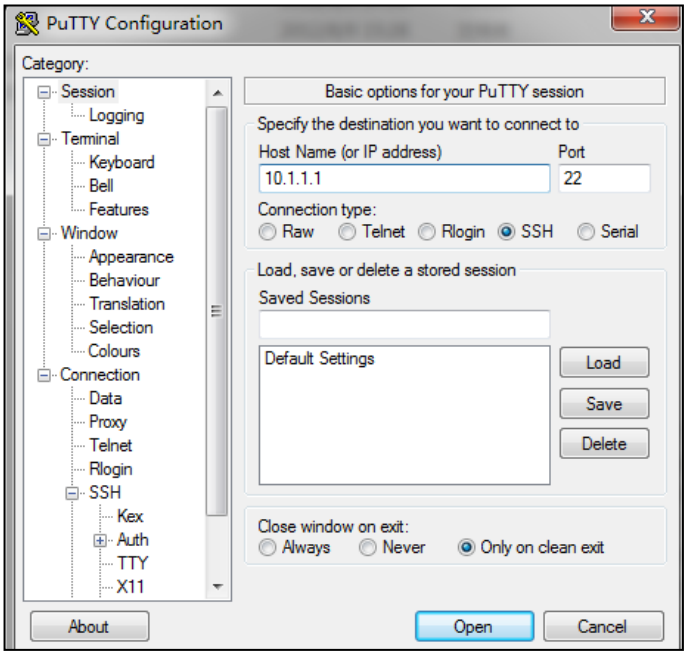
Step 5 创建 SSH 管理员账号。

```
[USG] aaa
[USG-aaa] manager-user sshuser
[USG-aaa-manager-use-sshuser] service-type ssh
[USG-aaa-manager-use-sshuser] level 3
[USG-aaa-manager-use-sshuser] ssh authentication-type password
[USG-aaa-manager-use-sshuser] password
Enter Password:
Confirm Password:
[USG-aaa-manager-use-sshuser] ssh service-type telnet
[USG-aaa-manager-use-sshuser] quit
```

Step 6 生成本地密钥对。

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

Step 7 配置管理 PC 的 IP 地址为 10.1.1.100/24。管理 PC 通过 Putty SSH 访问 USG 防火墙设备。



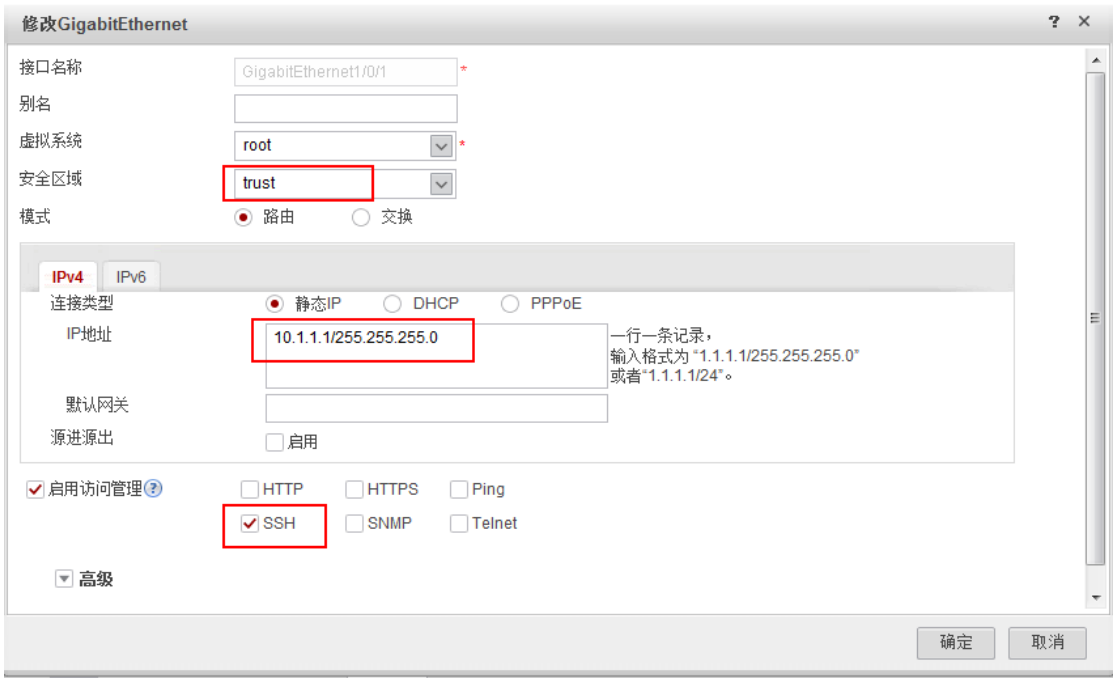
实验步骤 - Web

Step 1 设备物理连接后，将所有设备上电，并且保证设备运行正常。

Step 2 配置登录接口

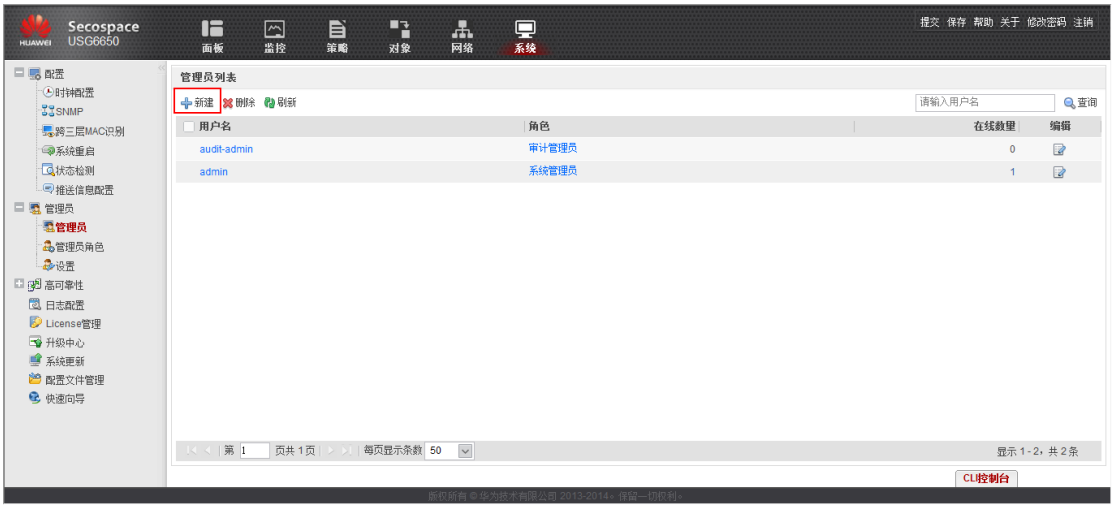
a. 选择“网络>接口>GE1/0/1”。

b. 配置接口加入 Trust 区域，配置接口的 IP 地址，开启接口 SSH 管理功能。

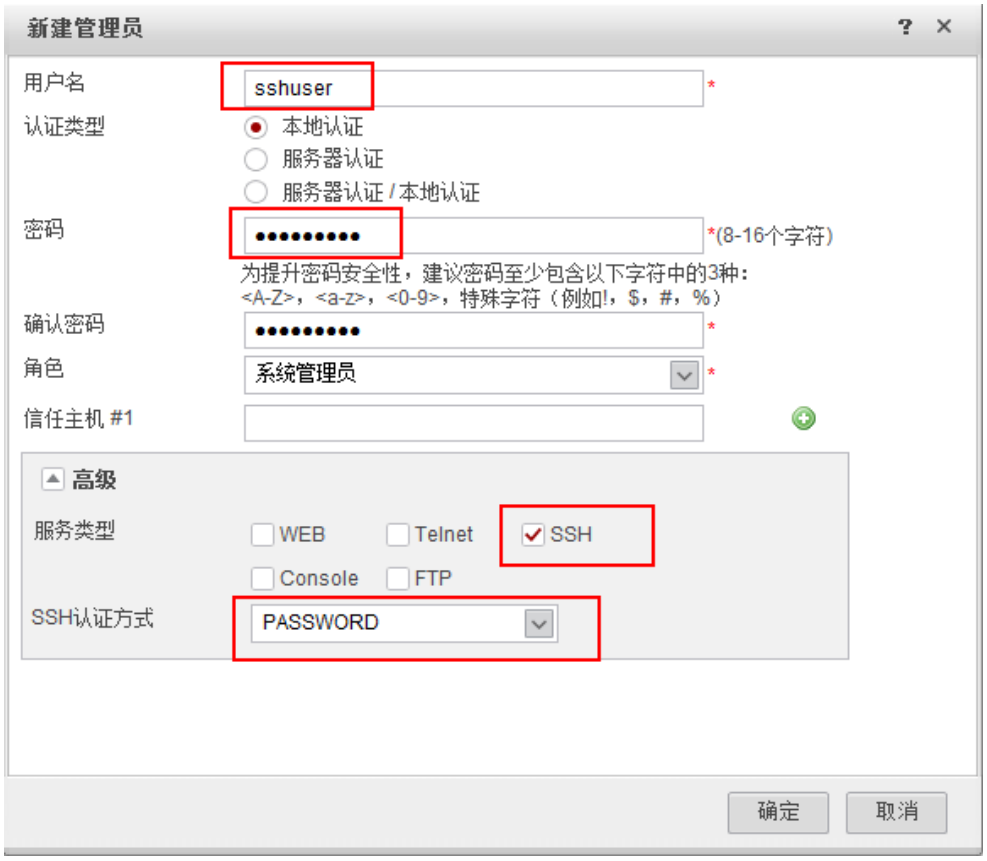


Step 3 配置 SSH 管理员。

a. 选择“系统>管理员>管理员”，单击“新建。

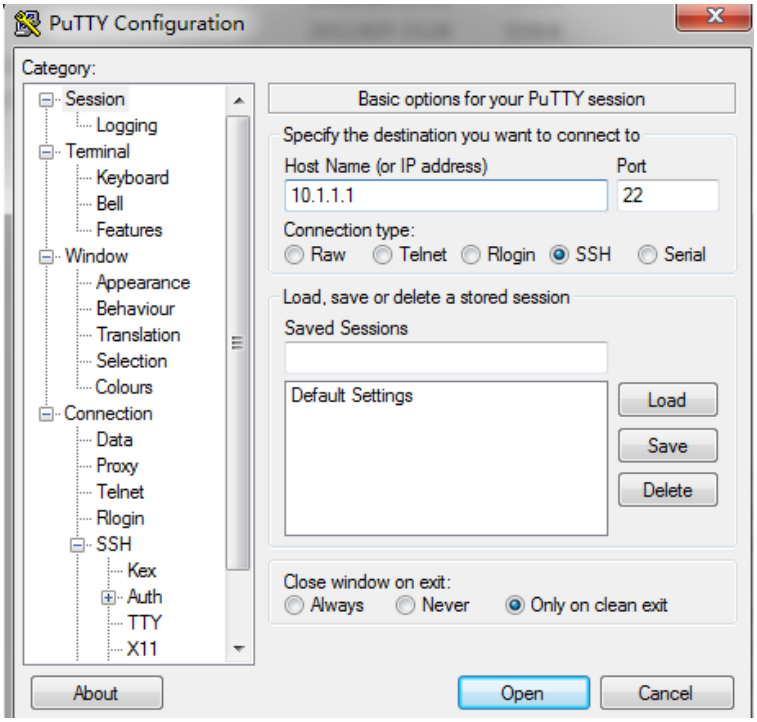


b. 配置 SSH 用户的用户名和密码，并勾选“SSH”服务类型，认证方式为 PASSWORD。



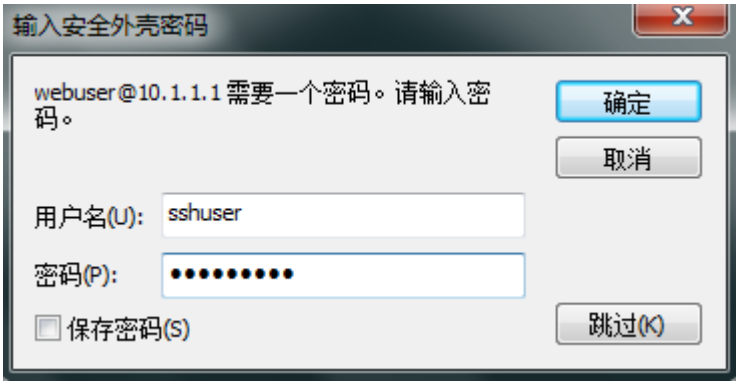
Step 4 配置 SSH 用户的服务方式为 STelnet，并启用 STelnet 服务。

Step 5 配置管理 PC 的 IP 地址为 10.1.1.100/24。 管理 PC 通过 Putty SSH 访问设备。



验证结果

输入用户名 sshuser 密码 Admin@123，可以成功登录设备



3 防火墙基础配置

3.1 系统管理

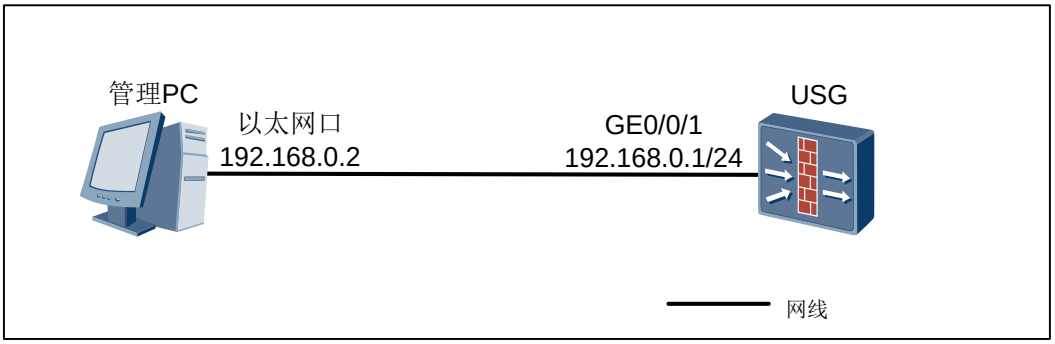
实验目的

掌握配置设备主机名、配置时间、配置 SNMP 服务器、配置日志服务器、配置 License、配置文件的备份和恢复的方法。

组网设备

USG 防火墙 1 台，PC 机 1 台。

实验拓扑图



实验步骤 - CLI

Step 1 设备物理连接后，将所有设备上电，并且保证设备运行正常。

Step 2 通过 Console，Telnet，SSH 等管理方式，登录到设备中（参考 2.1-2.5 章节）。

Step 3 配置设备主机名。

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

Step 4 配置时间。

```
<USG> clock datetime 0:0:0 2009/01/01
```

Step 5 配置 SNMP V2c 服务器。SNMP 服务器是 192.168.1.2

```
<USG> system-view
[USG] snmp-agent sys-info version v2c          //设置 SNMP 版本号 V2c
[USG] snmp-agent community read public         //设置 SNMP 只读团体字 public
[USG] snmp-agent community write admin         //设置 SNMP 读写团体字 admin
[USG] snmp-agent trap enable     //设置 SNMP trap 功能
[USG] snmp-agent target-host trap address udp-domain 192.168.1.2 params
securityname swebUser v2c   //设置 SNMP trap 服务器
```

思考：Snmp Agent Trap 的作用是什么?

配置管理设备主动向网管服务器发送告警。如果不配置 Snmp Trap，Snmp 网管服务将只是周期性向被管理设备发送各种查询报文，设备返回查询数据。

Step 6 配置日志服务器。

查看信息中心是否使能，使能后才能记录日志信息，默认是使能的。

```
[USG] display info-center
Information Center:enabled
```

开启信息中心。

```
[USG] info-center enable
```

配置日志服务器 IP 地址和发送日志信息的源接口。

```
[USG] info-center loghost 192.168.1.10
[USG] info-center loghost source GE0/0/1
```

Step 7 配置 License

```
[USG] license file hda1:/license.dat
```

Step 8 配置备份和恢复

设备做 FTP Server 的方式

//配置网络连接、IP 地址、接口安全区域及包过滤。（略）

//开启设备的 FTP 功能并配置 FTP 用户名、密码及 FTP 路径。

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

//从管理 PC 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管理 PC。

在管理 PC 中:“开始 > 运行”，输入 **cmd** 后单击“确定”。

```
C:\Documents and Settings\Administrator> ftp 192.168.0.1
Connected to 192.168.0.1.
220 FTP service ready.
User （192.168.0.1:（none））: ftpuser
331 Password required for ftpuser.
Password:
230 User logged in.
ftp> get vrpcfg.cfg
200 Port command okay.
150 Opening ASCII mode data connection for vrpcfg.cfg.
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.
ftp>
```

恢复：

恢复的步骤和备份的步骤类似，但是有两点不同点。

//恢复使用 **Put** 命令将文件上传到设备上。

```
ftp> put vrpcfg.cfg
200 Port command okay.
150 Opening ASCII mode data connection for vrpcfg.cfg.
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。

```
<sysname> startup saved-configuration vrpcfg.cfg
```

实验步骤 - Web

Step 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。

Step 2 通过 Web 管理方式，登录到设备中（参考 2.4 章节）。

Step 3 配置设备主机名 USG_A。

选择“面板 > 系统信息 > 设备名称”，单击“更改”。

Step 4 配置时间。

选择“系统 > 配置 > 时钟配置”。

Step 5 配置 SNMP V2c 服务器。SNMP 服务器是 192.168.1.2。

选择“系统 > 配置 > SNMP”。设置如图所示：

Step 6 配置日志服务器。

//查看信息中心是否使能，使能后才能记录日志信息，默认是使能的。

选择“日志 > 日志配置 > 信息中心”。

//配置日志服务器 IP 地址和发送日志信息的源接口。

选择“系统 > 日志配置 > 配置 Syslog”。设置源接口 GE1/0/1,日志主机 192.168.1.10。

Step 7 配置 License。

选择导入管理 PC 本地的 License 文件，并选择激活。License 具体的信息可以在“系统 > License 管理”中查看。

Step 8 配置备份和恢复

通过 Web 备份和恢复配置

备份：

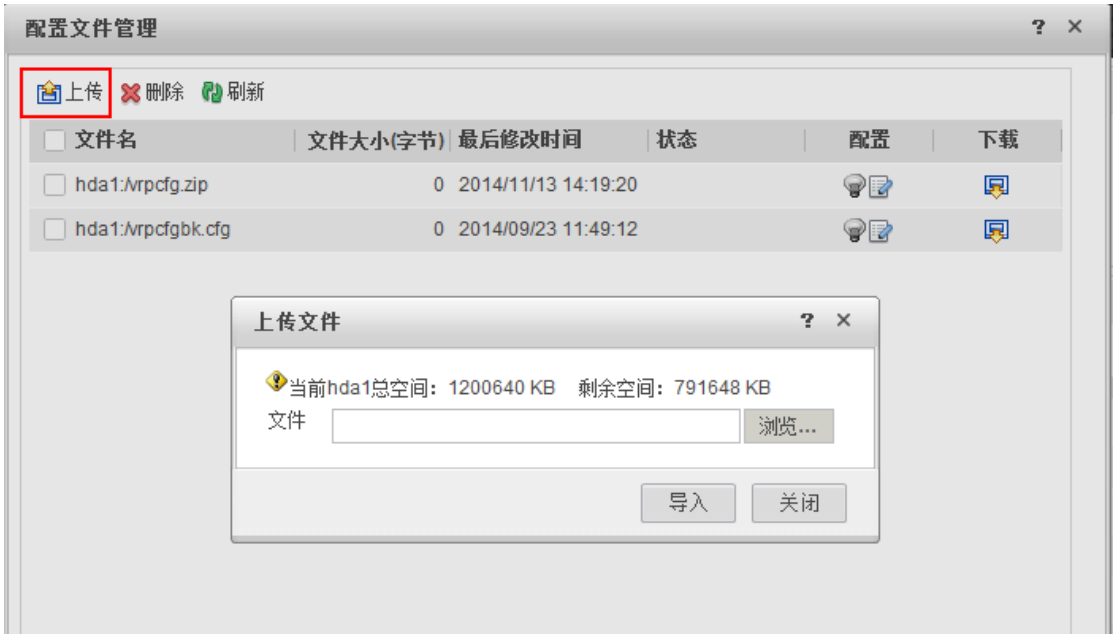
//在菜单导航树中选择“系统 > 配置文件管理”进入配置管理界面。单击“选择”按钮，进入配置文件管理界面：

//单击待备份的配置文件对应的下载图标：

 此配置文件当前正在使用，点击  下载配置文件到本地。

恢复：

//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。



//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  。

//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。

验证结果

选择“系统 > 维护 > 配置管理”查看下一次启动的配置文件。


Secospace
USG6650
面板
监控
策略
对象
网络
系统
配置
时钟配置
SNMP
跨三层MAC识别
IDS联动
系统重启
状态检测
推送信息配置
管理员
高可靠性
敏捷网络配置
日志配置
License管理
升级中心
系统更新
配置文件管理
配置文件信息
当前配置文件
hda1:/vrpcfg.zip
恢复出厂配置
下次启动配置文件
hda1:/vrpcfg.zip
选择
当前配置
刷新
查询
导出
比较
保存
10:38:01 2015/03/13
#
l2tp domain suffix-separator @
#
info-center source AUDIT channel 0 log state off
info-center source DLP channel 0 log state off

4 防火墙安全转发策略

4.1 基于 IP 地址的转发策略

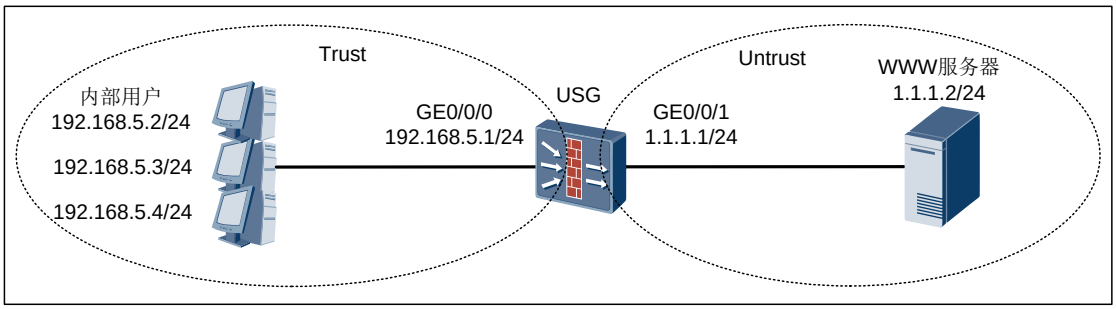
实验目的

掌握基于 IP 地址控制访问的配置方法。

组网设备

USG 防火墙 1 台，PC 机 3 台，WWW 服务器 1 台。

实验拓扑图



实验步骤 - CLI

Step 1 配置各个接口的 IP 地址，并加入相应的安全区域。

```
<USG>system-view
[USG] interface GigabitEthernet 0/0/0
[USG-GigabitEthernet0/0/0] ip address 192.168.5.1 24
[USG-GigabitEthernet0/0/0] quit
[USG]interface GigabitEthernet 0/0/1
[USG-GigabitEthernet0/0/1] ip address 1.1.1.1 24
[USG-GigabitEthernet0/0/1] quit
[USG] firewall zone trust
```

```
[USG-zone-trust] add interface GigabitEthernet 0/0/0
[USG-zone-trust] quit
[USG] firewall zone untrust
[USG-zone-untrust] add interface GigabitEthernet0/0/1
[USG-zone-untrust] quit
```

Step 2 配置名称为 ip_deny 的地址集，将几个不允许上网的 IP 地址加入地址集。

```
[USG] ip address-set ip_deny type object
[USG-object-address-set-ip_deny] address 192.168.5.2 0
[USG-object-address-set-ip_deny] address 192.168.5.3 0
[USG-object-address-set-ip_deny] address 192.168.5.6 0
[USG-object-address-set-ip_deny] quit
```

Step 3 创建拒绝特殊的几个 IP 地址访问 Internet 的转发策略。

```
[USG] security policy
[USG-policy-security] rule name policy_deny
[USG-policy-security-rule-policy_deny] source-address address-set ip_deny
[USG-policy-security-rule-policy_deny] action deny
[USG-policy-security-rule-policy_deny tbound-0] quit
```

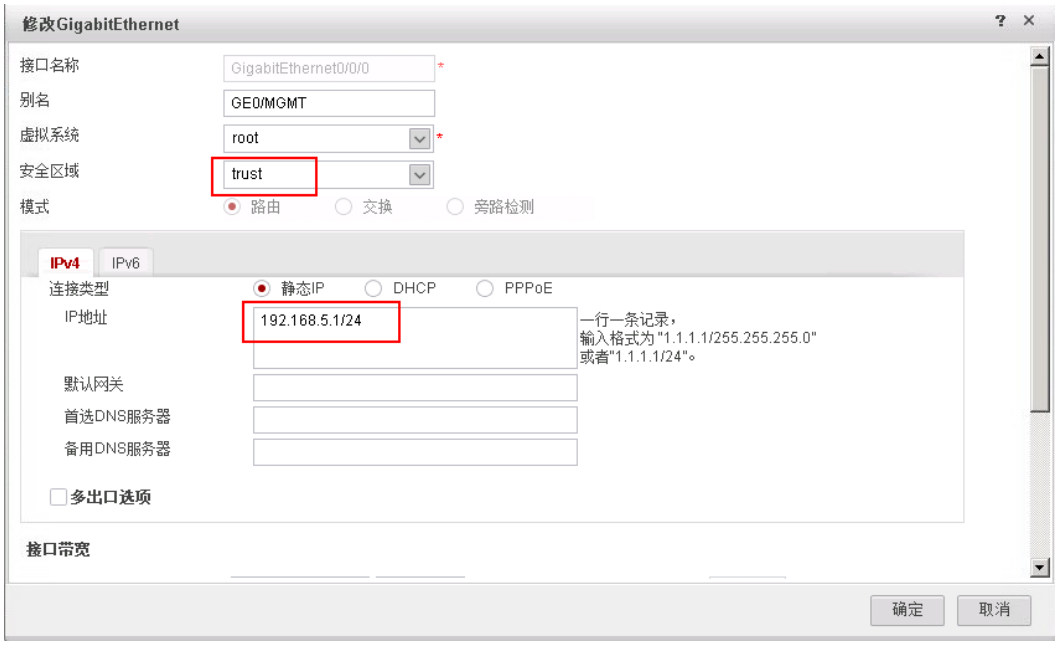
Step 4 创建允许其他属于 192.168.5.0/24 这个网段的 PC 访问 Internet 的转发策略。

```
[USG] security policy
[USG-policy-security] rule name policy_permit
[USG-policy-security-rule-policy_permit] source-address 192.168.5.0 24
[USG-policy-security-rule-policy_permit] action permit
[USG-policy-security-rule-policy_permit] quit
```

实验步骤 - Web

Step 1 配置各个接口的 IP 地址，并加入相应的安全区域。如图所示：

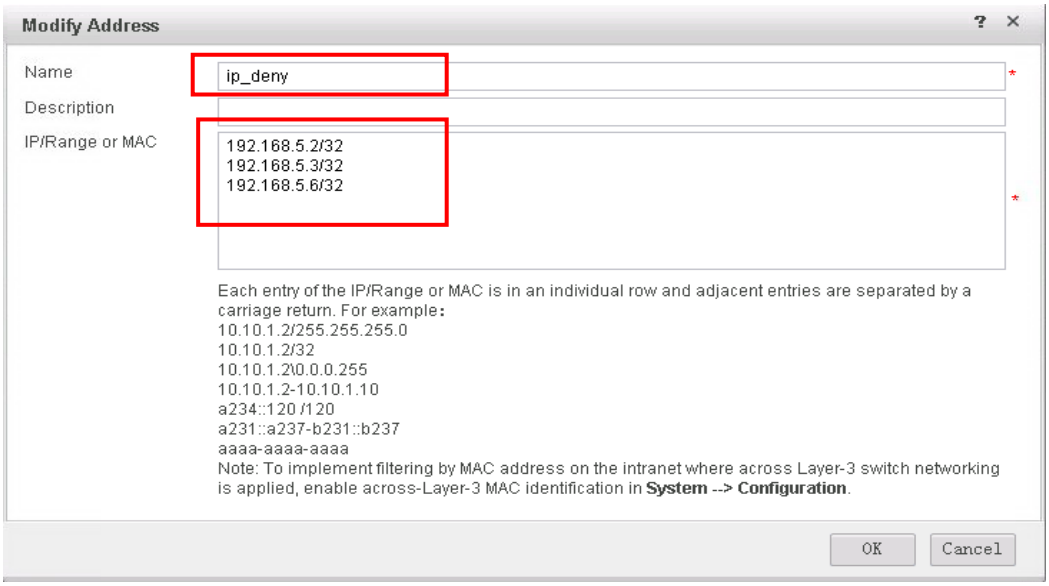
选择“网络>接口>GE0/0/0”，配置接口 IP 地址，并加入到 Trust 区域。



重复上述步骤配置接口 GE0/0/1 的 IP 地址并加入 Untrust 区域。（略）

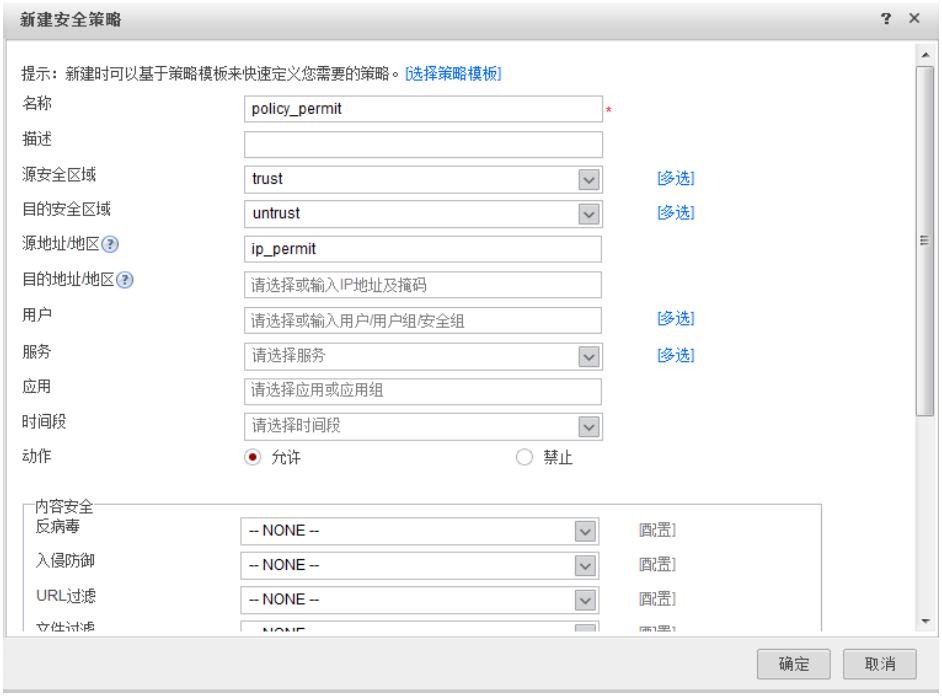
Step 2 配置名称为 ip_deny 的地址集，将几个不允许上网的 IP 地址加入地址集。

1. 选择“对象 > 地址 > 地址”，单击“新建”，配置地址的各项参数。



Step 3 创建拒绝特殊的几个 IP 地址访问 Internet 的转发策略。 选择“策略 > 安全策略 > 安全策略”，单击“新建”，并输入各项参数。

Step 4 创建允许 192.168.5.0/24 这个网段访问 Internet 的转发策略。



验证结果

经过验证，发现 192.168.5.2、192.168.5.3 和 192.168.5.6 这 3 台 PC 无法访问 Internet；而 192.168.5.0/24 中的其他 IP 地址可以正常访问 Internet。

5 网络地址转换实验

5.1 源 NAT 实验

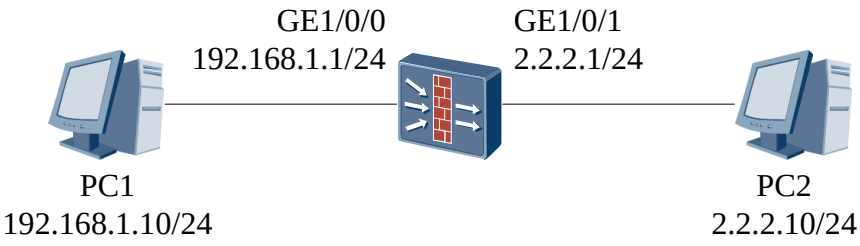
实验目的

掌握 NAT 的配置方法。

组网设备

USG 防火墙 1 台，PC 机 2 台。

实验拓扑图



实验步骤 - CLI

Step 1 配置 PC1 和 PC2 的 IP 地址分别为 192.168.1.10/24 和 2.2.2.10/24。

Step 2 设置防火墙 GE1/0/0 和 GE1/0/1 的 IP 地址。

```
[USG]interface GigabitEthernet 1/0/0
[USG-GigabitEthernet1/0/0]ip address 192.168.1.1 255.255.255.0
[USG-GigabitEthernet1/0/0]quit
[USG]interface GigabitEthernet 1/0/1
[USG-GigabitEthernet1/0/1]ip address 2.2.2.1 255.255.255.0
[USG-GigabitEthernet1/0/1]quit
```

Step 3 将接口加入防火墙安全区域。（GE0/0/0 加入 Trust 区域，GE0/0/1 加入 Untrust 区域）

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

Step 4 配置域间包过滤策略。

```
[USG] security-policy
[USG-policy-security] rule name source_nat
[USG-policy-security-rule-source_nat] source-addresss 192.168.1.0 24
[USG-policy-security-rule-source_nat] source-zone trust
[USG-policy-security-rule-source_nat] destination-zone untrust
[USG-policy-security-rule-source_nat] action permit
```

Step 5 配置 NAT 地址池，公网地址范围为 2.2.2.2—2.2.2.5。

```
[USG] nat address-group 1
[USG-nat-address-group-1] section 2.2.2.2 2.2.2.5
```

Step 6 配置 NAT policy。

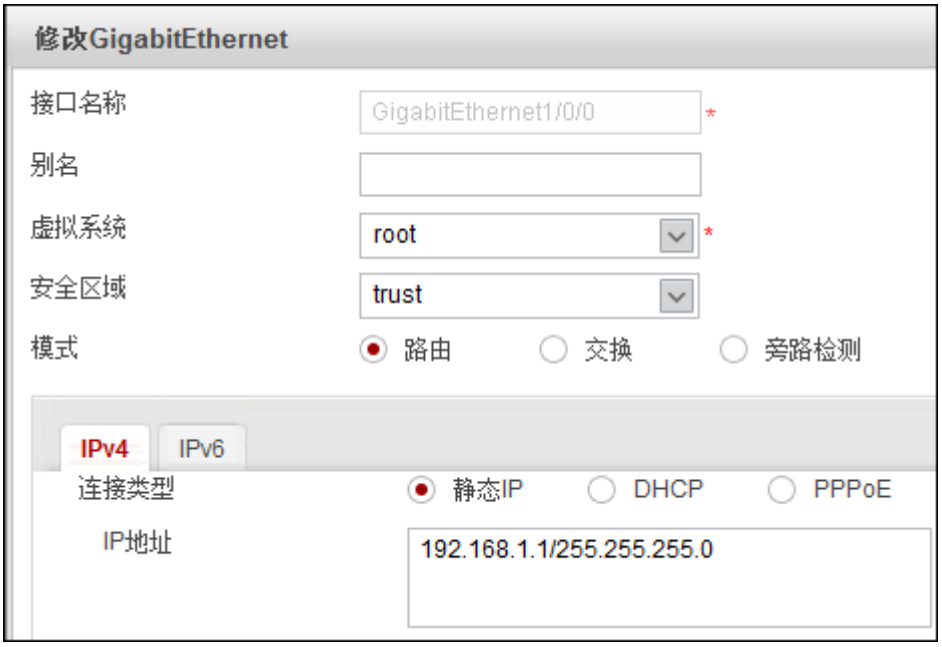
```
[USG] nat-policy
[USG-policy-nat] rule name source_nat
[USG-policy-nat-rule-source_nat] destination-address 2.2.2.10 24
[USG-policy-nat-rule-source_nat] source-address 192.168.1.0 24
[USG-policy-nat-rule-source_nat] source-zone trust
[USG-policy-nat-rule-source_nat] destination-zone untrust
[USG-policy-nat-rule-source_nat] action nat address-group 1
```

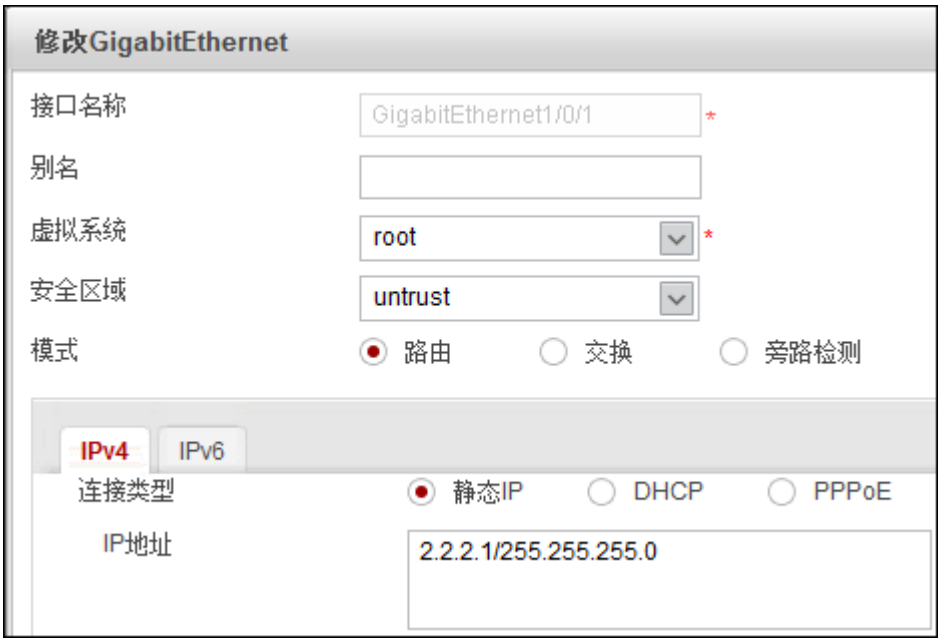
实验步骤 - Web

Step 1 配置 PC1 和 PC2 的 IP 地址分别为 192.168.1.10/24 和 2.2.2.10/24。

Step 2 设置防火墙 GE1/0/0 和 GE1/0/1 的 IP 地址。

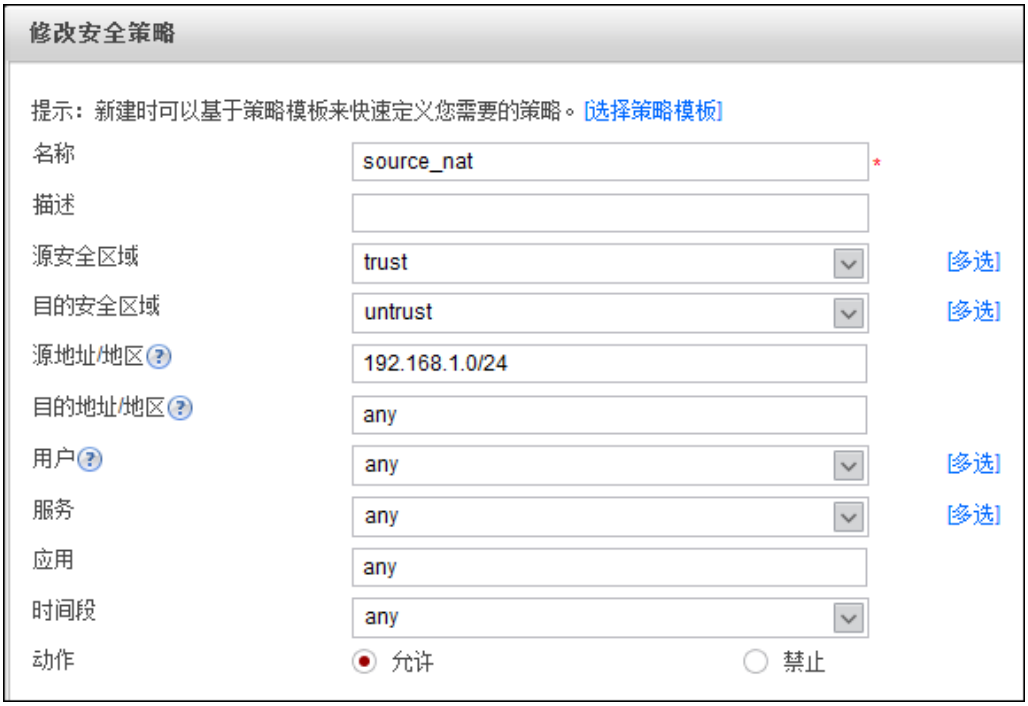
选择“网络 > 接口”。在“接口列表”中单击各接口对应的 。配置如下图所示：配置完成后单击“确定”。





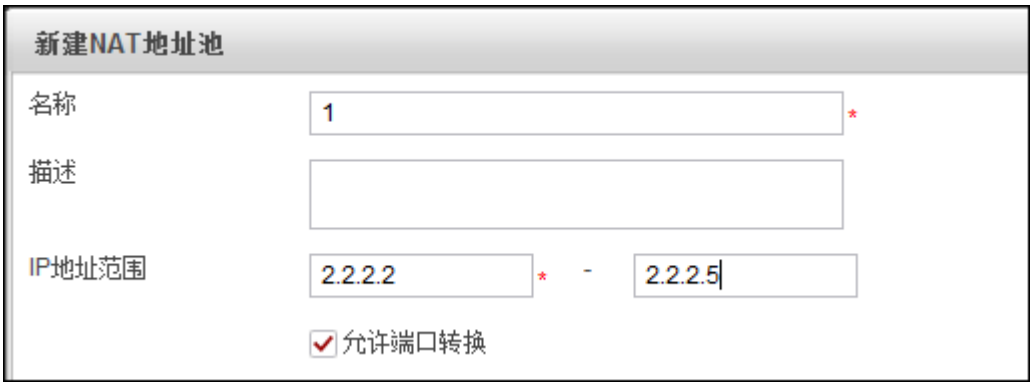
Step 3 配置域间包过滤策略。选择“策略 > 安全策略”。

在“安全策略列表”中单击 。配置如下图所示：配置完成后单击“确定”。



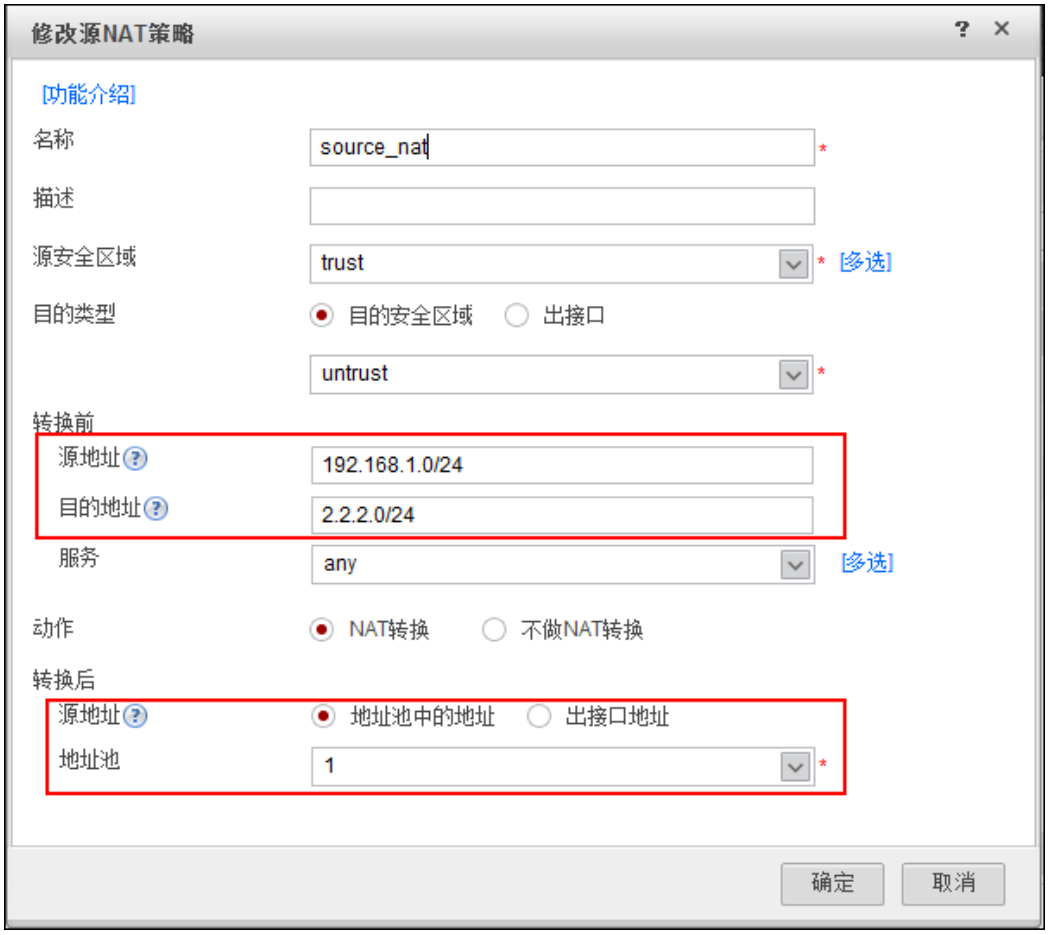
Step 4 配置 NAT 地址池，公网地址范围为 2.2.2.2—2.2.2.5。

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”。



Step 5 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”。



验证结果

从 PC1 ping PC2 地址

```
PC1>ping 2.2.2.10
Ping 2.2.2.10: 32 data bytes, Press Ctrl_C to break
From 2.2.2.10: bytes=32 seq=1 ttl=127 time=79 ms
From 2.2.2.10: bytes=32 seq=2 ttl=127 time=31 ms
From 2.2.2.10: bytes=32 seq=3 ttl=127 time=94 ms
From 2.2.2.10: bytes=32 seq=4 ttl=127 time=62 ms
From 2.2.2.10: bytes=32 seq=5 ttl=127 time=94 ms
--- 2.2.2.10 ping statistics ---
  5 packet（s） transmitted
  5 packet（s） received
  0.00% packet loss
  round-trip min/avg/max = 31/72/94 ms
```

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

```
[USG]display firewall session table
Current Total Sessions : 15
icmp    VPN:public --> public 192.168.1.10:45346[2.2.2.5:45346]-->2.2.2.10:2048
```

```
icmp    VPN:public --> public 192.168.1.10:45602[2.2.2.5:45602]-->2.2.2.10:2048
icmp    VPN:public --> public 192.168.1.10:45858[2.2.2.5:45858]-->2.2.2.10:2048
icmp    VPN:public --> public 192.168.1.10:46114[2.2.2.5:46114]-->2.2.2.10:2048
icmp    VPN:public --> public 192.168.1.10:46370[2.2.2.5:46370]-->2.2.2.10:2048
```

可以看到，防火墙将源地址 192.168.1.10 转换成了 NAT 地址池中的 2.2.2.5 与 PC2 进行通信。

5.2 NAT Server & 源 NAT 实验

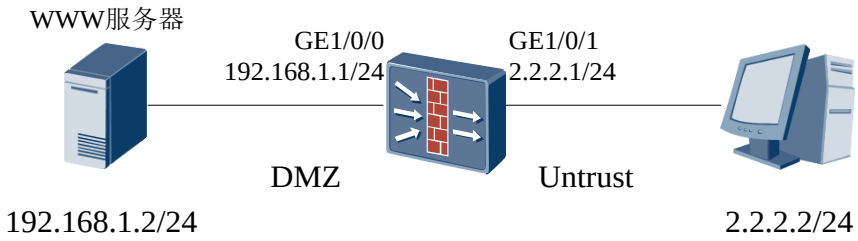
实验目的

通过本实验,让学员掌握配置 NAT Server 和源 NAT 的方法。

组网设备

USG 防火墙 1 台，PC 机 1 台，WWW 服务器 1 台。

实验拓扑图



实验步骤 - CLI

Step 1 设置 WWW 服务器和 PC 的地址。

Step 2 设置防火墙 GE1/0/0 和 GE1/0/1 的 IP 地址。

```
[USG]interface GigabitEthernet 1/0/0
[USG-GigabitEthernet1/0/0]ip address 192.168.1.1 255.255.255.0
[USG-GigabitEthernet1/0/0]quit
[USG]interface GigabitEthernet 1/0/1
[USG-GigabitEthernet1/0/1]ip address 2.2.2.1 255.255.255.0
[USG-GigabitEthernet1/0/1]quit
```

Step 3 将接口加入防火墙安全区域。（GE0/0/0 加入 DMZ 区域，GE0/0/1 加入 Untrust 区域）

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

Step 4 配置域间包过滤策略。

```
[USG] security-policy
[USG-policy-security] rule name bidectinal_nat
[USG-policy-security-rule-bidectinal_nat] source-zone untrust
[USG-policy-security-rule-bidectinal_nat] destination-zone dmz
[USG-policy-security-rule-bidectinal_nat] destination-address 192.168.1.2 32
[USG-policy-security-rule-bidectinal_nat] service ftp
[USG-policy-security-rule-bidectinal_nat] action permit
```

Step 5 配置 NAT Server。

```
[USG] nat server ftpserver protocol tcp global 2.2.2.4 ftp inside 192.168.1.2 ftp
```

Step 6 配置 NAT 地址池。

```
[USG] nat address-group 2
[USG-nat-address-group-2] section 192.168.1.10 192.168.1.20
```

Step 7 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 NAT ALG 功能，该步骤可以省略。

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

Step 8 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。

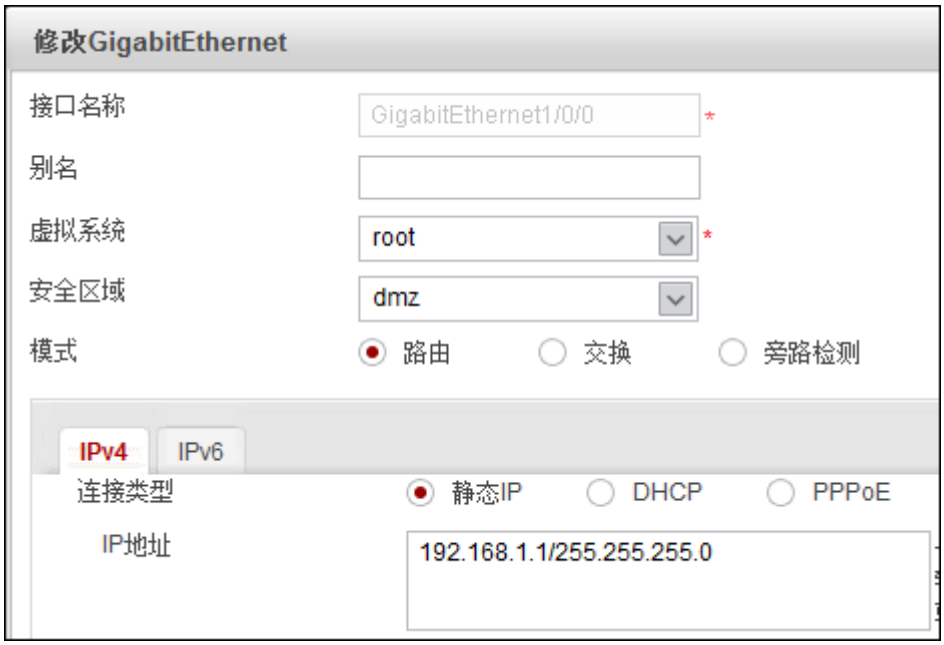
```
[USG] nat-policy
[USG-policy-nat] rule name biderectinal_nat
[USG-policy-nat-rule-biderectinal_nat] source-zone untrust
[USG-policy-nat-rule-biderectinal_nat] destination-zone dmz
[USG-policy-nat-rule-biderectinal_nat] source-address 2.2.2.0 24
[USG-policy-nat-rule-biderectinal_nat] action nat address-group 2
```

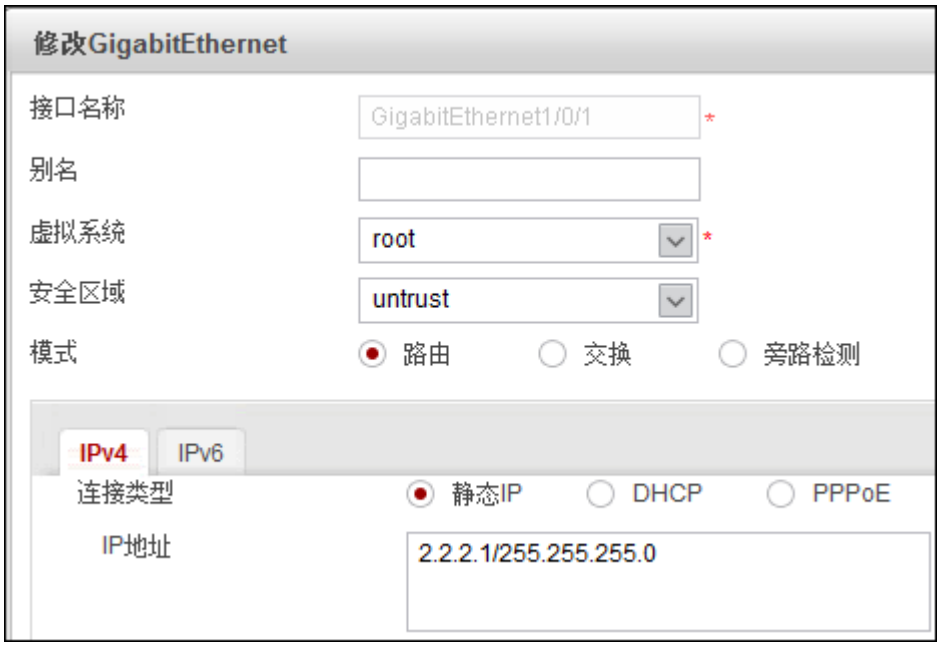
实验步骤 – Web

Step 1 设置 WWW 服务器和 PC 的 IP 地址。

Step 2 设置防火墙 GE1/0/0 和 GE1/0/1 的 IP 地址。

选择“网络 > 接口”。在“接口列表”中单击各接口对应的。配置如下图所示：配置完成后单击“确定”。





Step 3 配置域间包过滤策略。

选择“策略 > 安全策略”。在“转发策略列表”中单击 。配置如下图所示：配置完成后单击“确定”。

Step 4 配置 NAT Server。

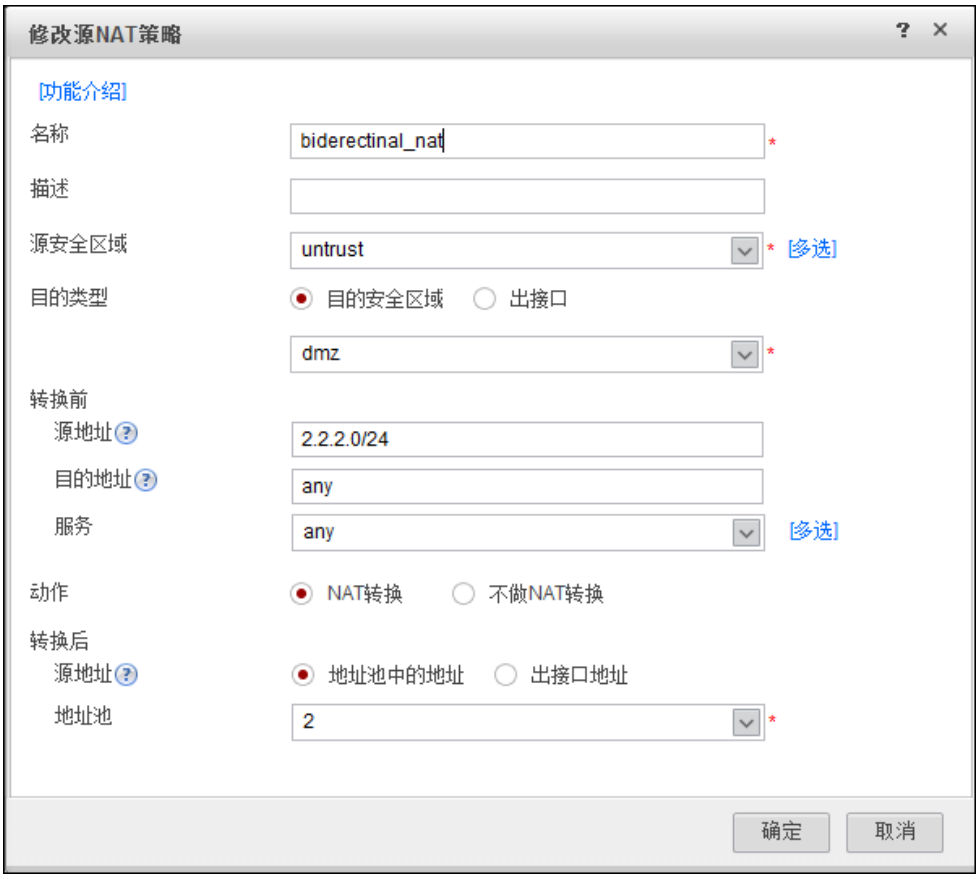
选择“策略 ＞NAT 策略＞ 服务器映射”。在“服务器映射列表”中单击 。配置如图所示：配置完成后单击“确定”。

Step 5 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：

Step 6 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：



验证结果

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

```
<USG>display nat server
Server in private network information:
 name                  : ftpserver
 zone                  : ---
 interface             : ---
 global-start-addr : 2.2.2.4                global-end-addr     : ---
 inside-start-addr : 192.168.1.2            inside-end-addr     : ---
 global-start-port : 21（ftp）                global-end-port     : ---
 insideport            : 21（ftp）
 globalvpn             : public             insidevpn           : public
 protocol              : tcp                vrrp                : ---
 no-reverse            : no

  Total     1 NAT servers
```

6 防火墙双机热备实验

6.1 防火墙双机热备实验

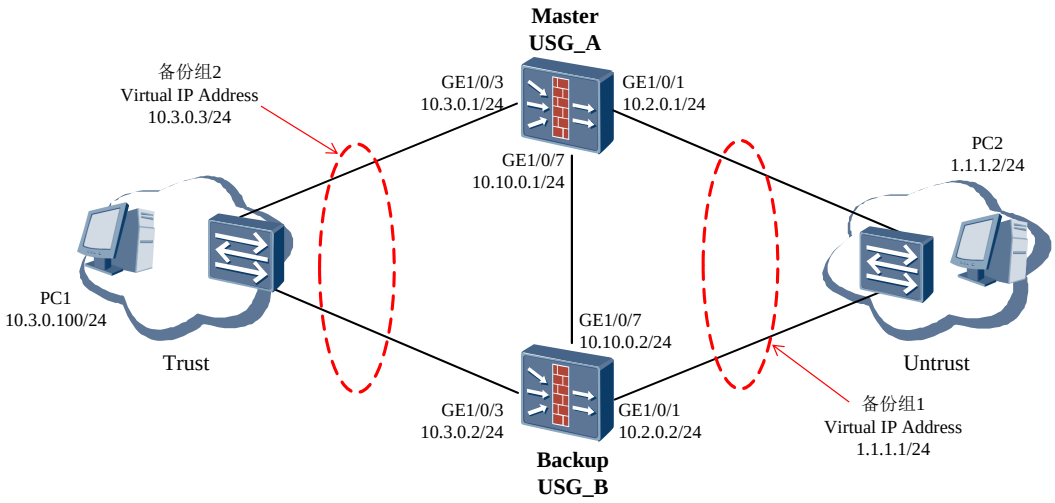
实验目的

掌握基于命令行和 Web 两种方式配置防火墙双机热备。

组网设备

USG 防火墙 2 台（相同型号），交换机 2 台，PC 机 2 台。

实验拓扑图



实验步骤 - CLI

Step 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_A> system-view
[USG_A] interface GigabitEthernet 1/0/1
[USG_A-GigabitEthernet1/0/1] ip address 10.2.0.1 255.255.255.0
[USG_A-GigabitEthernet1/0/1] quit
[USG_A] interface GigabitEthernet 1/0/3
[USG_A-GigabitEthernet1/0/3] ip address 10.3.0.1 255.255.255.0
[USG_A-GigabitEthernet1/0/3] quit
[USG_A] firewall zone trust
```

```
[USG_A-zone-trust] add interface GigabitEthernet 1/0/3
[USG_A-zone-trust] quit
[USG_A] firewall zone untrust
[USG_A-zone-untrust] add interface GigabitEthernet 1/0/1
[USG_A-zone-untrust] quit
```

配置接口 GE1/0/1 的 VRRP 备份组 1，并加入到状态为 Active 的 VGMP 管理组。

```
[USG_A] interface GigabitEthernet 1/0/1
[USG_A-GigabitEthernet1/0/1] vrrp vrid 1 virtual-ip 1.1.1.1 255.255.255.0 active
[USG_A-GigabitEthernet1/0/1] quit
```

配置接口 GE1/0/3 的 VRRP 备份组 2，并加入到状态为 Active 的 VGMP 管理组。

```
[USG_A] interface GigabitEthernet 1/0/3
[USG_A-GigabitEthernet1/0/3] vrrp vrid 2 virtual-ip 10.3.0.3    255.255.255.0 active
[USG_A-GigabitEthernet1/0/3] quit
```

Step 2 完成 USG_A 的心跳线配置。

配置 GE1/0/7 的 IP 地址。

```
[USG_A] interface GigabitEthernet1/0/7
[USG_A-GigabitEthernet1/0/7] ip address 10.10.0.1 255.255.255.0
[USG_A-GigabitEthernet1/0/7] quit
```

配置 GE1/0/7 加入 DMZ 区域。

```
[USG_A] firewall zone dmz
[USG_A-zone-dmz] add interface GigabitEthernet1/0/7
[USG_A-zone-dmz] quit
```

指定 GE1/0/7 为心跳口。

```
[USG_A] hrp interface GigabitEthernet1/0/7
```

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

Step 4 启用 HRP 备份功能。

```
[USG_A] hrp enable
```

Step 5 配置 USG_B。

USG_B 和上述 USG_A 的配置基本相同，不同之处在于：

1. USG_B 各接口的 IP 地址与 USG_A 各接口的 IP 地址不相同。
2. USG_B 的业务接口 GE1/0/1 和 GE1/0/3 加入状态为 Standby 的 VGMP 管理组。

Step 6 配置 Switch。

分别将 2 台 Switch 的三个接口加入同一个 VLAN，缺省 VLAN 即可。如需配置请参考交换机的相关文档。

实验步骤 – Web

Step 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 GE1/0/1 接口配置如图所示：

GE1/0/3 和 GE1/0/7 配置类似

Step 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：

Step 3 完成 USG_A 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：

USG_B 防火墙配置与 USG_A 防火墙基本一致，具体配置略。

验证结果

在 USG_A 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<USG_A>display vrrp
  GigabitEthernet1/0/1 | Virtual Router 1
    VRRP Group : Active
    state : Active
    Virtual IP : 1.1.1.1
    Virtual MAC : 0000-5e00-0101
    Primary IP : 10.2.0.1
    PriorityRun : 120
    PriorityConfig:100
    ActivePriority : 120
    Preempt : YES      Delay Time : 0
    Advertisement Timer : 1
    Auth Type : NONE
    Check TTL : YES

  GigabitEthernet1/0/3 | Virtual Router 2
    VRRP Group : Active
    state : Active
    Virtual IP : 10.3.0.3
    Virtual MAC : 0000-5e00-0102
    Primary IP : 10.3.0.1
    PriorityRun : 120
```

```
    PriorityConfig:100
    ActivePriority : 120
    Preempt : YES     Delay Time : 0
    Advertisement Timer : 1
    Auth Type : NONE
    Check TTL : YES
```

在 USG_A 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<USG_A>display hrp state
The firewall's config state is: ACTIVE
  Current state of virtual routers configured as active:
                GigabitEthernet1/0/3       vrid     2 : active
                GigabitEthernet1/0/1       vrid     1 : active
```

在处于 Trust 区域的 PC1 端 ping VRRP 组 2 的虚拟 IP 地址 10.3.0.3，在 USG_A 上检查会话。

```
HRP_A<USG_A>display firewall session table
Current Total Sessions : 1
  icmp    VPN:public --> public 10.3.0.100:1-->10.3.0.3:2048
```

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 USG_A 和 USG_B 上检查会话。

```
HRP_A<USG_A>display firewall session table
Current Total Sessions : 1
  icmp    VPN:public --> public 10.3.0.100:1-->1.1.1.2:2048


HRP_S<USG_B>display firewall session table
Current Total Sessions : 1
  icmp    VPN:public --> public      Remote 10.3.0.100:1-->1.1.1.2:2048
```

可以看出 USG_B 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 1.1.1.2 –t ，然后将 USG_A 防火墙 GE1/0/1 接口网线拔出，观察防火墙状态切换及 Ping 包丢包情况；再将 USG_A 防火墙 GE1/0/1 接口网线恢复，观察防火墙状态切换及 Ping 包丢包情况。

7 防火墙用户管理

7.1 上网用户认证（免认证和密码认证）

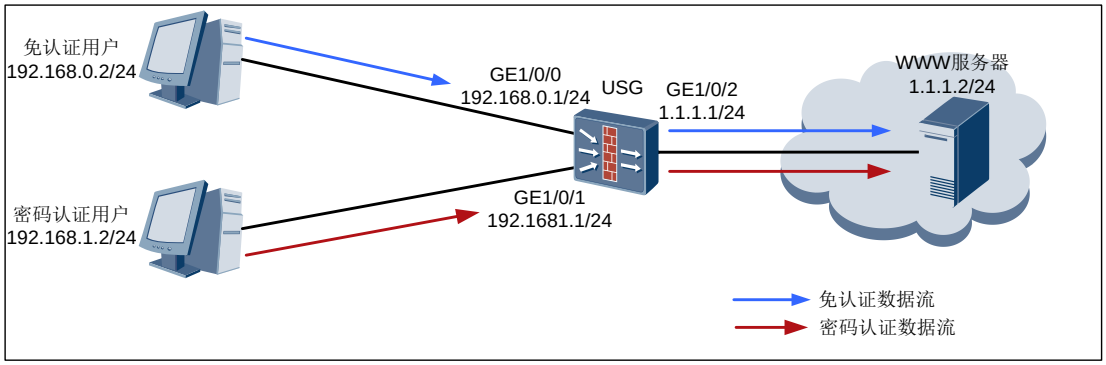
实验目的

掌握免认证和密码认证的应用场景及配置方法。

组网设备

USG 防火墙 1 台，WWW 服务器 1 台，PC 机 2 台。

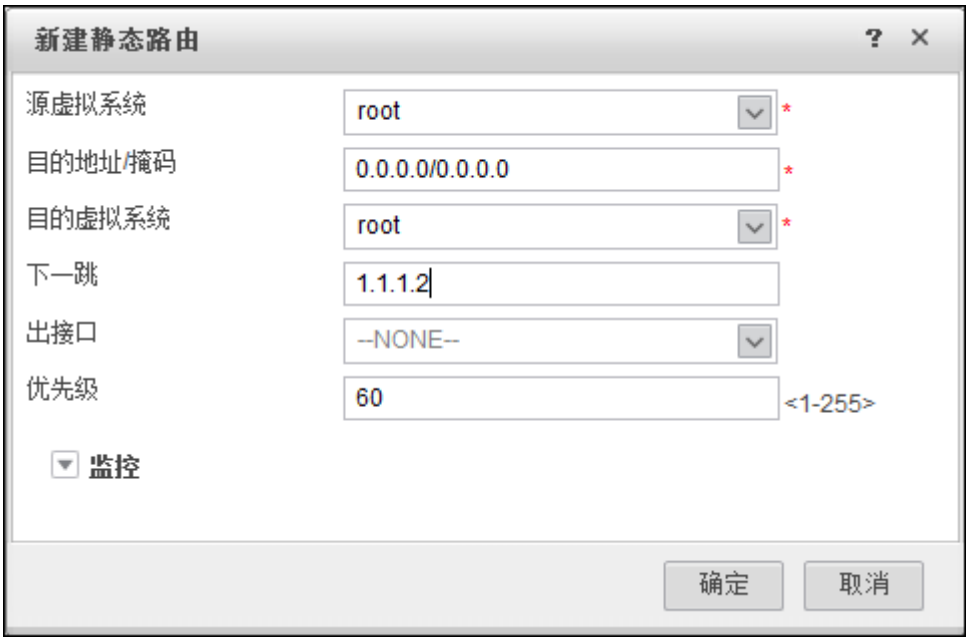
实验拓扑图



实验步骤 - Web

Step 1 配置 USG 相关接口的基本参数，并加入安全域。GE1/0/0 加入 Guest 区域,GE1/0/1 加入 Trust,GE1/0/2 加入 Untrust。具体步骤略。

Step 2 配置缺省路由，其下一跳地址为 1.1.1.2。

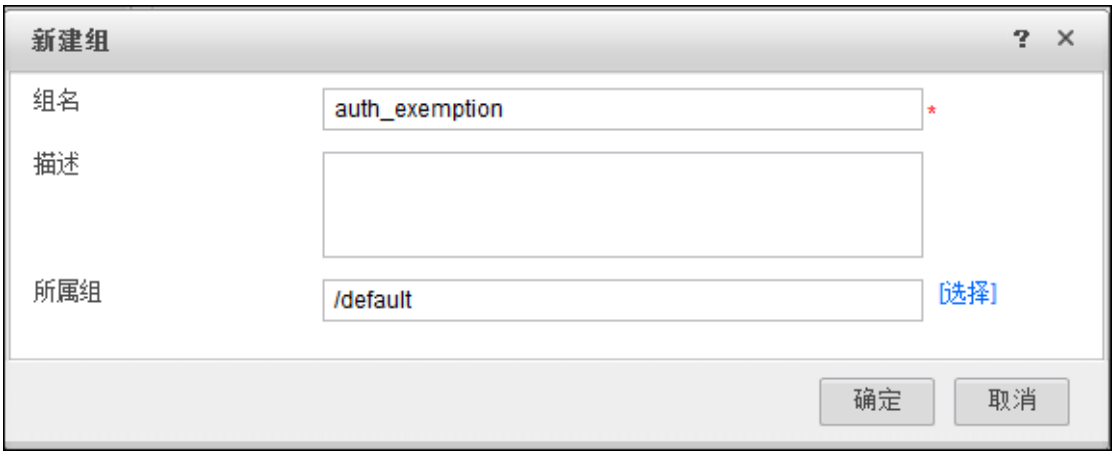


Step 3 创建免认证用户组。

选择“对象 > 用户 > 用户/组”。

在“组织结构”中，选择“default”。

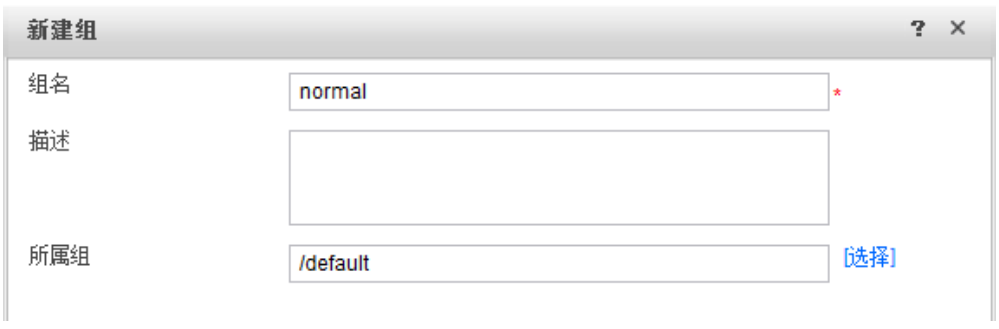
在“成员管理”中单击“新建”，选择“新建组”，组名：auth_exemption。



Step 4 创建网段 192.168.0.0/24 对应的用户认证策略：guest。

Step 5 创建密码认证用户组和用户。

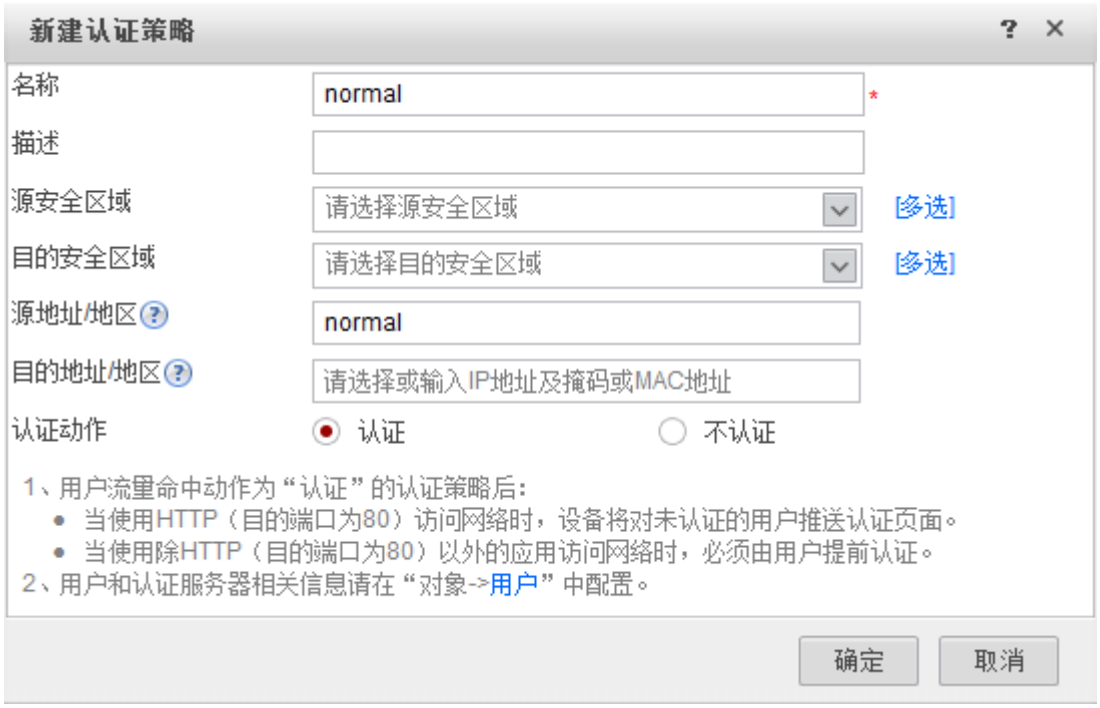
选择“对象 > 用户 > 用户/组”。
在“组织结构”中，选择“default”。
在“成员管理”中单击“新建”，选择“新建组”，组名：normal。



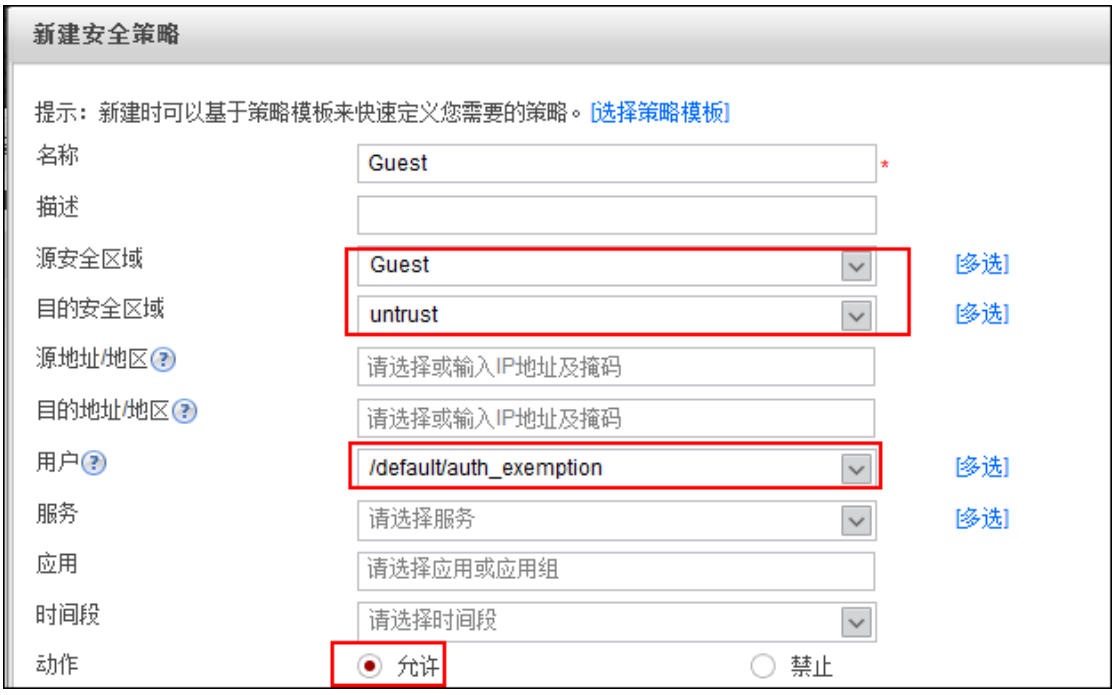
在“组织结构”中，选择“normal”。

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

Step 6 创建网段 192.168.1.0/24 对应的用户认证策略：normal。



Step 7 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 auth_exemption，动作为 Permit。



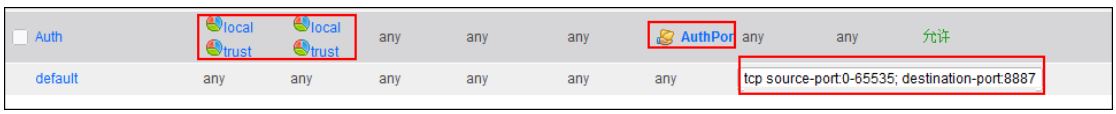
Step 8 为密码认证用户创建转发策略。

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。

Step 9 配置上网认证推送页面。

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。

Step 10 配置 Local 区域的安全策略，允许 8887 端口流量通过防火墙，使认证页面成功推送。



验证结果

临时用户不需要输入用户名密码，即可以访问 Internet。
普通用户通过 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 VPN 技术实验

8.1 L2TP VPN 实验（Client-Initialized VPN）

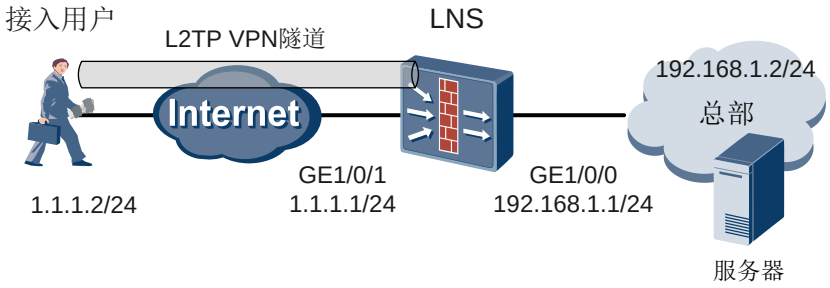
实验目的

掌握基于 Client-Initialized 方式建立本地认证的 L2TP 的配置方法。

组网设备

USG 防火墙 1 台，服务器 1 台，PC 机 1 台。

实验拓扑图



实验步骤 - CLI

Step 1 配置 LNS 端，设置接口 IP 地址并配置域间包过滤策略。

```
<USG> system-view
[USG] sysname LNS
[LNS] interface GigabitEthernet 1/0/1
[LNS-GigabitEthernet1/0/1] ip address 1.1.1.1 255.255.255.0
[LNS-GigabitEthernet1/0/1] quit
[LNS] interface GigabitEthernet 1/0/0
[LNS-GigabitEthernet1/0/0] ip address 192.168.1.1 255.255.255.0
[LNS-GigabitEthernet1/0/0] quit
```

Step 2 创建虚拟模板 Virtual-Template 并配置相关信息。

```
[LNS] interface virtual-template 1
[LNS-Virtual-Template1] ip address 192.168.0.1 255.255.255.0
[LNS-Virtual-Template1] ppp authentication-mode chap
[LNS-Virtual-Template1] quit
```

Step 3 开启 L2TP。

```
[LNS] l2tp enable
```

Step 4 创建并配置 L2TP 组。

```
[LNS] l2tp-group 1
[LNS-l2tp1] tunnel name LNS
[LNS-l2tp1] allow l2tp virtual-template 1 remote client1
[LNS-l2tp1] tunnel authentication
[LNS-l2tp1] tunnel password cipher Huawei@123
```

Step 5 配置给用户分配的地址池。并设置用户名及密码（应与出差员工侧的设置一致）。

```
[LNS] user-manage user vpdnuser
[LNS-localuser-pc1] password Admin@123
[LNS-localuser-pc1] parent-group /default
[LNS]aaa
[LNS-aaa] domain default
[LNS-aaa-domain-default] ip pool 1 192.168.0.2 192.168.0.100
[LNS-aaa-domian-default] quit
```

Step 6 配置为对端接口分配 IP 地址池中的地址。

```
[LNS] interface virtual-template 1
[LNS-Virtual-Template1] remote address pool 1
[LNS-Virtual-Template1] quit
```

Step 7 将接口加入安全区域，并配置域间包过滤。

```
[LNS]firewall zone trust
[LNS-zone-trust]add interface GigabitEthernet 1/0/0
[LNS-zone-trust]add interface virtual-template 1
[LNS-zone-trust]quit
[LNS]firewall zone untrust
[LNS-zone-untrust]add interface GigabitEthernet 1/0/1
[LNS-zone-untrust]quit
[LNS]security-policy
[LNS-policy-security]rule name trust_untrust
[LNS-policy-security-rule-trust_untrust]source-zone trust
[LNS-policy-security-rule-trust_untrust]destination-zone untrust
[LNS-policy-security-rule-trust_untrust]source-address 192.168.1.0 24
[LNS-policy-security-rule-trust_untrust]action permit
[LNS-policy-security-rule-trust_untrust]quit
[LNS-policy-security]rule name untrust_trust
[LNS-policy-security-rule-untrust_trust]source-zone untrust
[LNS-policy-security-rule-untrust_trust]destination-zone trust
[LNS-policy-security-rule-untrust_trust]destination-address 192.168.1.0 24
[LNS-policy-security-rule-untrust_trust]quit
[LNS-policy-security]rule name local_untrust
[LNS-policy-security-rule-local_untrust]source-zone local
[LNS-policy-security-rule-local_untrust]destination-zone untrust
[LNS-policy-security-rule-local_untrust]source-address 1.1.1.1 24
[LNS-policy-security-rule-local_untrust]quit
[LNS-policy-security]rule name untrust_local
[LNS-policy-security-rule-untrust_local]source-zone untrust
```

```
[LNS-policy-security-rule-untrust_local]destination-zone local
[LNS-policy-security-rule-untrust_local]destination-address1.1.1.1 24
[LNS-policy-security-rule-untrust_local]quit
```

Step 8 配置 LAC 客户端。

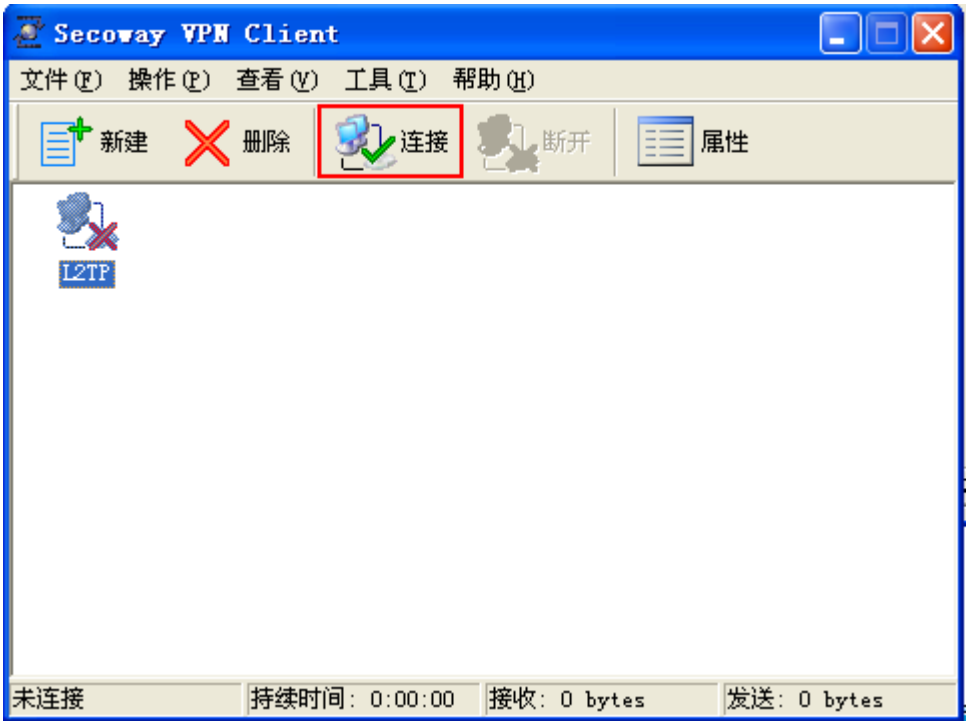
在 LAC 主机上安装华为 Secoway VPN Client。点击 

创建一个新的连接。选择”通过输入参数创建连接”，单击”下一步”。

Step 9 输入服务器地址，即 LNS 端地址，用户名/密码（vpdnuser/Admin@123），完成后单击”下一步”。

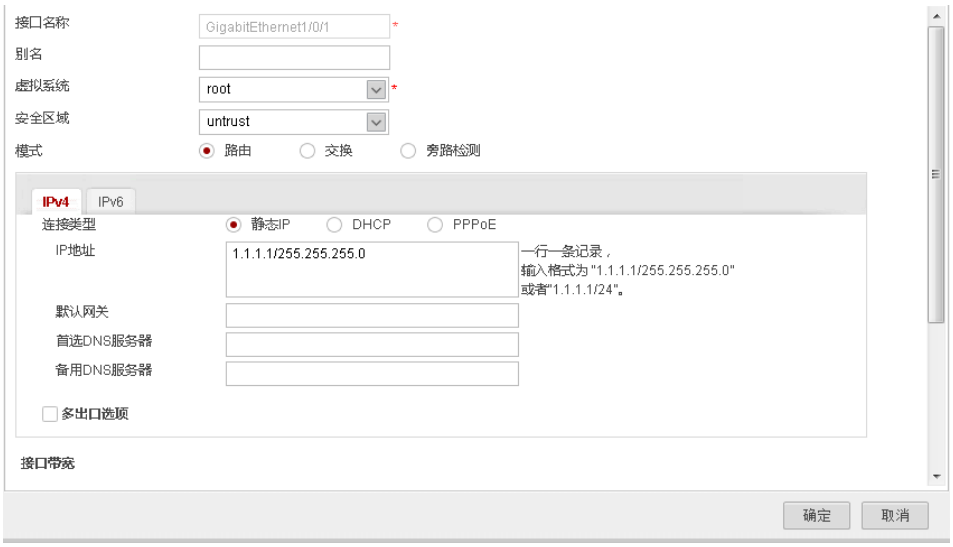
Step 10 输入隧道名称（client1）和认证模式（CHAP）。勾选”启用隧道验证功能”，并输入隧道验证密码（Huawei@123）。单击”完成”。

Step 11 点击创建好的 L2TP 连接，单击”连接”。

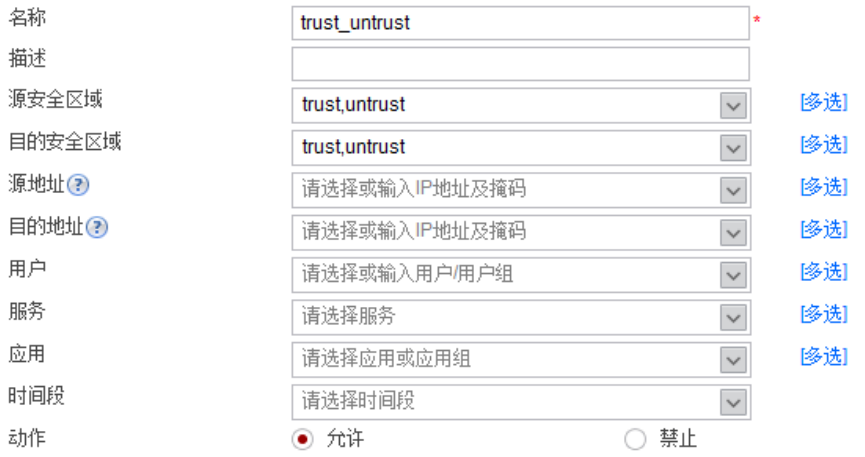


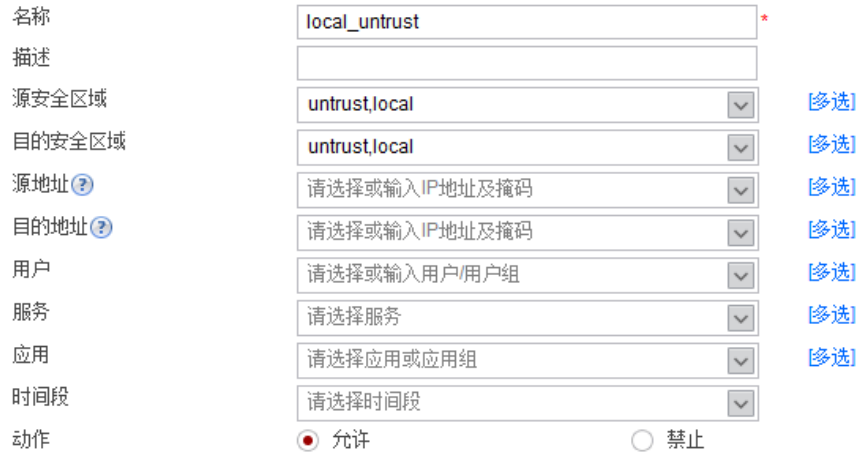
实验步骤 - Web

Step 1 配置 LNS 端，设置接口 IP 地址并配置域间包过滤策略。选择“网络 > 接口”。在“接口列表”中，单击 GE1/0/1 对应的 。配置如图所示：

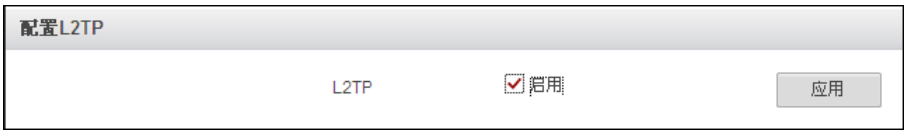


Step 2 选择“策略 > 安全策略”。在“转发策略列表”中，单击“新建”，创建策略。



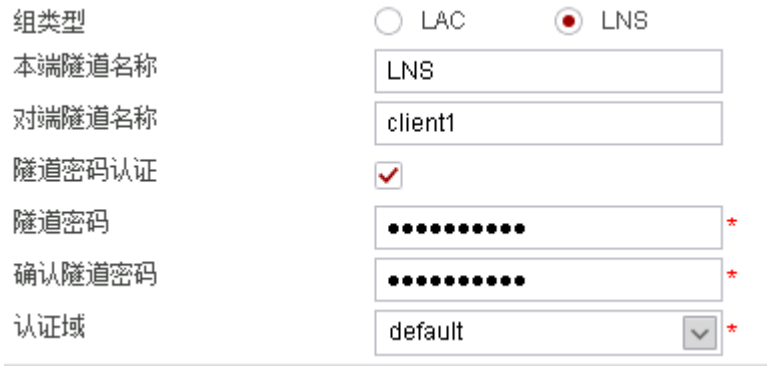


Step 3 配置 L2TP 参数。选择“网络 > L2TP > L2TP”。在“配置 L2TP”中，勾选 L2TP 后的“启用”按钮，并单击“应用”。

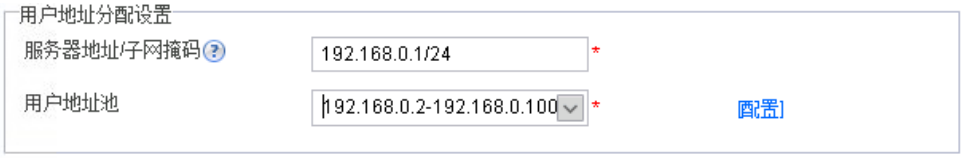


Step 4 选择“对象>用户>用户/组”。选中“default”认证域，在“成员管理”中，单击“新建”，并选择“新建用户”，按如下参数配置。

Step 5 配置其余 L2TP 参数。“对端隧道名称”要和 LAC 端配置的“本端隧道名称”一致。对端隧道名称为 client1/Huawei@123，如图所示。



Step 6 设置服务器地址及地址池段。如图所示，最后“应用”保存配置。



Step 7 配置 LAC 客户端。该步骤与 CLI 方式配置中 LAC 客户端配置一致，请参考 CLI 配置中 Step 8 – Step11。

验证结果

配置成功后，当有 VPN 用户上线时，分别在 LAC 和 LNS 上执行 display l2tp tunnel 命令可发现隧道建立成功。以 LNS 侧的显示为例：

```
[LNS] display l2tp tunnel
 Total tunnel = 1
 LocalTID RemoteTID RemoteAddress      Port     Sessions RemoteName
 2        22        1.1.1.2            1701     1        client1
```

LAC 执行 display l2tp session 命令可看到会话连接建立情况。以 LNS 侧的显示为例：

```
[LNS] display l2tp session
```

```
Total session = 1
LocalSID    RemoteSID    LocalTID
1           1            2
```

在使用 Web 界面进行配置时，选择网络 > L2TP > 监控，查看建立起的 L2tp 会话信息。

8.2 GRE VPN 实验

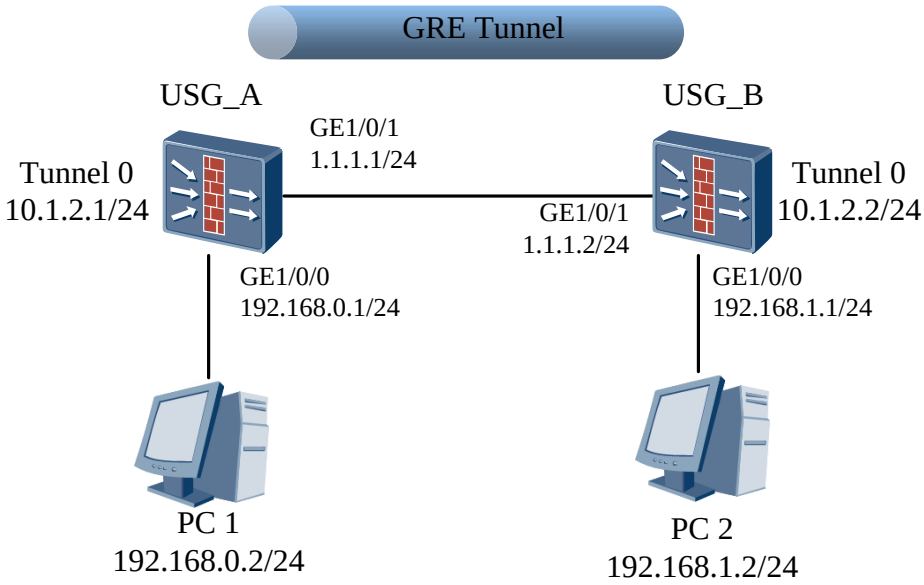
实验目的

掌握 GRE VPN 的应用场景及配置方法。

组网设备

USG 防火墙 2 台，PC 机 2 台。

实验拓扑图



实验步骤 - CLI

Step 1 配置主机 IP 地址，步骤省略。

Step 2 配置防火墙接口 IP 地址。

配置 USG_A：

```
[USG_A]interface GigabitEthernet 1/0/0
[USG_A-GigabitEthernet1/0/0]ip address 192.168.0.1 24
[USG_A-GigabitEthernet1/0/0]quit
[USG_A]interface GigabitEthernet 1/0/1
[USG_A-GigabitEthernet1/0/1]ip address 1.1.1.1 24
```

配置 USG_B：

```
[USG_B]interface GigabitEthernet 1/0/0
[USG_B-GigabitEthernet1/0/0]ip address 192.168.1.1 24
[USG_B-GigabitEthernet1/0/0]quit
[USG_B]interface GigabitEthernet 1/0/1
[USG_B-GigabitEthernet1/0/1]ip address 1.1.1.2 24
```

Step 3 配置接口安全区域并配置域间包过滤策略。

配置 USG_A：

```
[USG_A]firewall zone trust
[USG_A-zone-trust]add interface GigabitEthernet 1/0/0
[USG_A-zone-trust]quit
[USG_A]firewall zone untrust
[USG_A-zone-untrust]add interface GigabitEthernet 1/0/1
[USG_A-zone-untrust]quit
[USG_A]security-policy
[USG_A-policy-security]rule name policy_sec
[USG_A-policy-security-rule-policy_sec]source-zone trust untrust local
[USG_A-policy-security-rule-policy_sec]destination-zone trust untrust local
[USG_A-policy-security-rule-policy_sec]action permit
[USG_A-policy-security-rule-policy_sec]quit
```

配置 USG_B：

```
[USG_B]firewall zone trust
[USG_B-zone-trust]add interface GigabitEthernet 1/0/0
[USG_B-zone-trust]quit
[USG_B]firewall zone untrust
[USG_B-zone-untrust]add interface GigabitEthernet 1/0/1
[USG_B-zone-untrust]quit
[USG_B]security-policy
[USG_B-policy-security]rule name policy-sec
[USG_B-policy-security-rule-policy_sec]source-zone trust untrust local
[USG_B-policy-security-rule-policy_sec]destination-zone trust untrust local
[USG_B-policy-security-rule-policy_sec]action permit
[USG_B-policy-security-rule-policy_sec]quit
```

Step 4 配置 Tunnel 接口。并将 Tunnel 接口加入 Untrust 区域。

配置 USG_A：

```
[USG_A]interface Tunnel 0
[USG_A-Tunnel0]tunnel-protocol gre
[USG_A-Tunnel0]ip address 10.1.2.1 24
[USG_A-Tunnel0]source 1.1.1.1
[USG_A-Tunnel0]destination 1.1.1.2
[USG_A-Tunnel0]quit
[USG_A]firewall zone untrust
[USG_A-zone-untrust]add interface Tunnel 0
[USG_A-zone-untrust]quit
```

配置 USG_B：

```
[USG_B]interface Tunnel 0
[USG_B-Tunnel0]tunnel-protocol gre
[USG_B-Tunnel0]ip address 10.1.2.2 24
[USG_B-Tunnel0]source 1.1.1.2
[USG_B-Tunnel0]destination 1.1.1.1
[USG_B-Tunnel0]quit
[USG_B]firewall zone untrust
[USG_B-zone-untrust]add interface Tunnel 0
[USG_B-zone-untrust]quit
```

Step 5 配置静态路由。

配置 USG_A：

```
[USG_A]ip route-static 192.168.1.0 24 Tunnel 0
```

配置 USG_B：

```
[USG_B]ip route-static 192.168.0.0 24 Tunnel 0
```

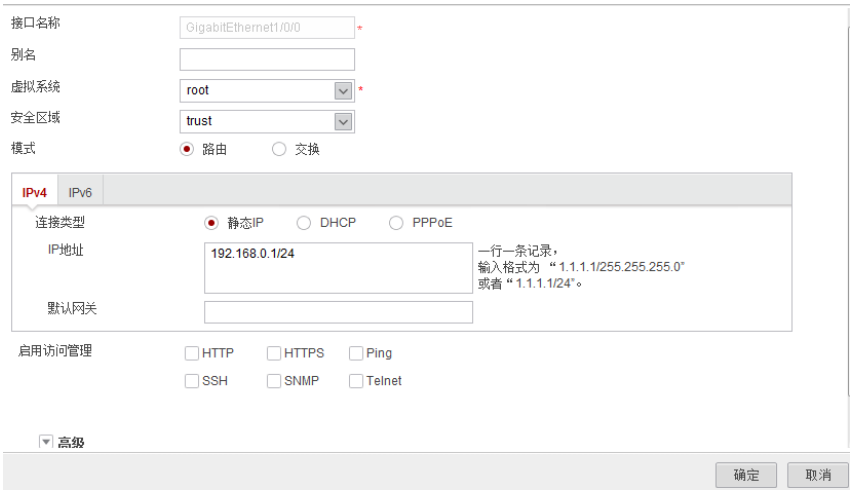
实验步骤 – Web

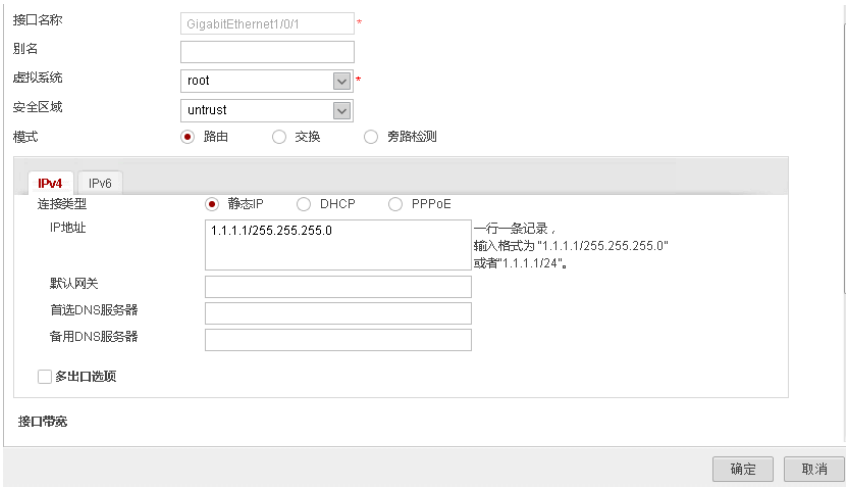
Step 1 配置 PC 的 IP 地址，配置步骤略。

Step 2 配置防火墙接口 IP 地址。选择“网络 > 接口”。在“接口列表”中单击各接口对应的 。配置如下图所示：配置完成后单击“应用”。

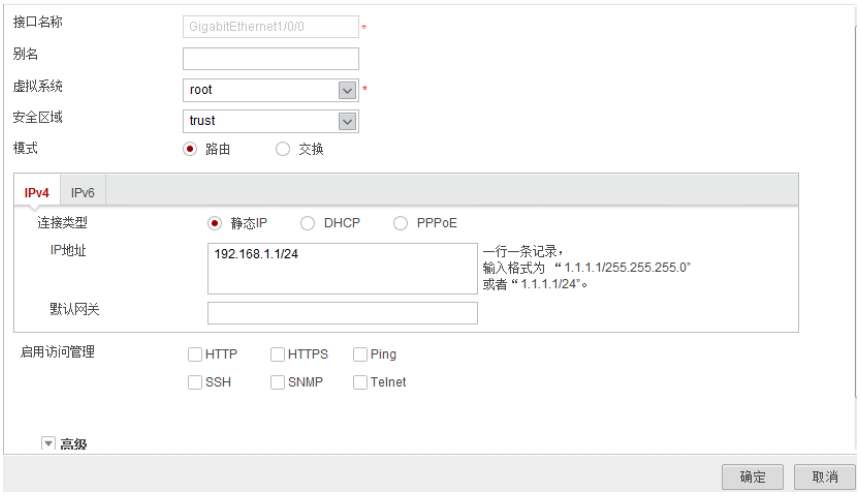
Step 3 防火墙接口配置。

配置 USG_A：


接口名称
GigabitEthernet1/0/0
别名
虚拟系统
root
安全区域
trust
模式
路由
交换
IPv4
IPv6
连接类型
静态IP
DHCP
PPPoE
IP地址
192.168.0.1/24
一行一条记录，
输入格式为 “1.1.1.1/255.255.255.0”
或者“1.1.1.1/24”。
默认网关
启用访问管理
HTTP
HTTPS
Ping
SSH
SNMP
Telnet
高级
确定
取消


接口名称
GigabitEthernet1/0/1
别名
虚拟系统
root
安全区域
untrust
模式
路由
交换
旁路检测
IPv4
IPv6
连接类型
静态IP
DHCP
PPPoE
IP地址
1.1.1.1/255.255.255.0
一行一条记录，
输入格式为“1.1.1.1/255.255.255.0”
或者“1.1.1.1/24”。
默认网关
首选DNS服务器
备用DNS服务器
多出口选项
接口带宽
确定
取消

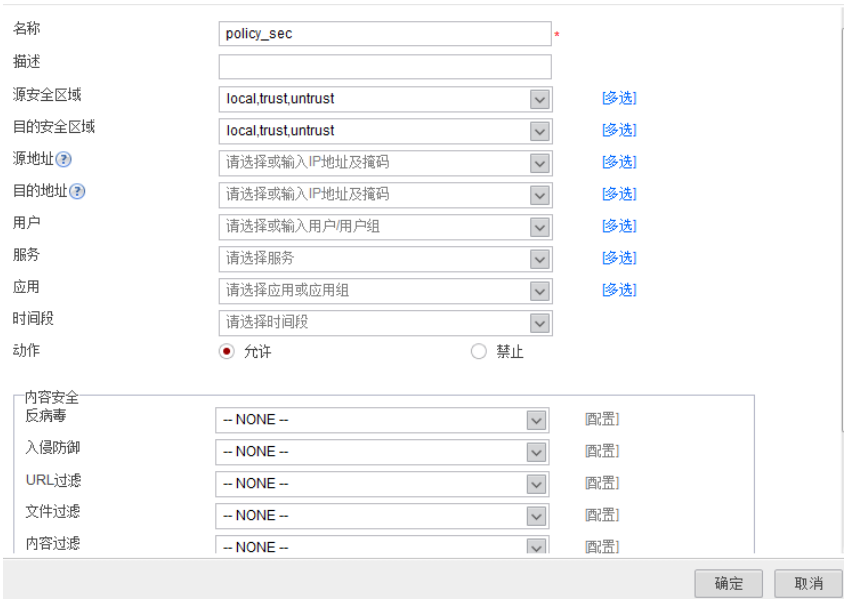
配置 USG_B：


接口名称
GigabitEthernet1/0/0
别名
虚拟系统
root
安全区域
trust
模式
路由
交换
IPv4
IPv6
连接类型
静态IP
DHCP
PPPoE
IP地址
192.168.1.1/24
一行一条记录，
输入格式为 “1.1.1.1/255.255.255.0”
或者“1.1.1.1/24”。
默认网关
启用访问管理
HTTP
HTTPS
Ping
SSH
SNMP
Telnet
高级
确定
取消

Step 4 配置域间包过滤策略。

选择“策略 > 安全策略”。在“安全策略列表”中单击 。配置如下图所示：配置完成后单击“应用”。

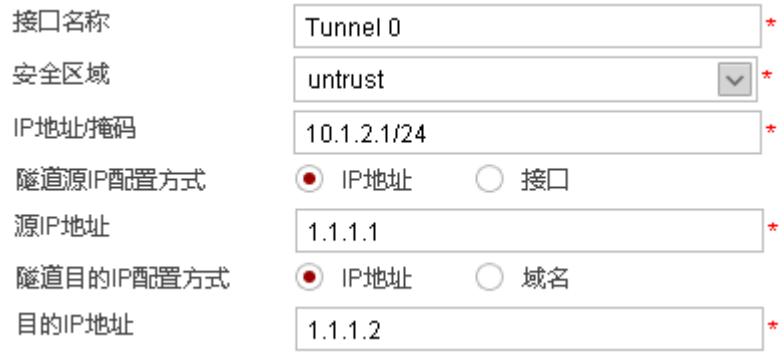
配置 USG_A：



防火墙 B 配置的配置与 A 相同。

Step 5 配置 Tunnel 接口。并将 Tunnel 接口加入 Untrust 区域。选择“网络 > GRE > GRE”。在“GRE 接口列表”中，单击“新建”。配置 GRE 隧道接口参数，配置如下图所示：

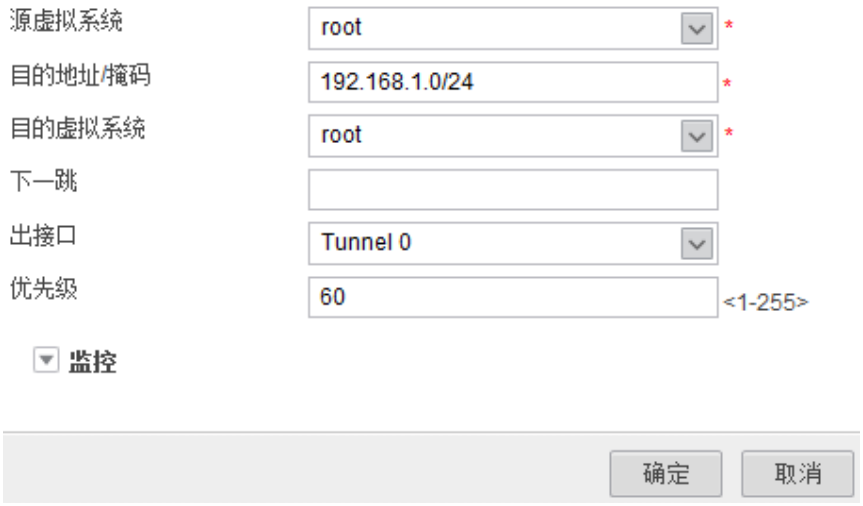
配置 USG_A：



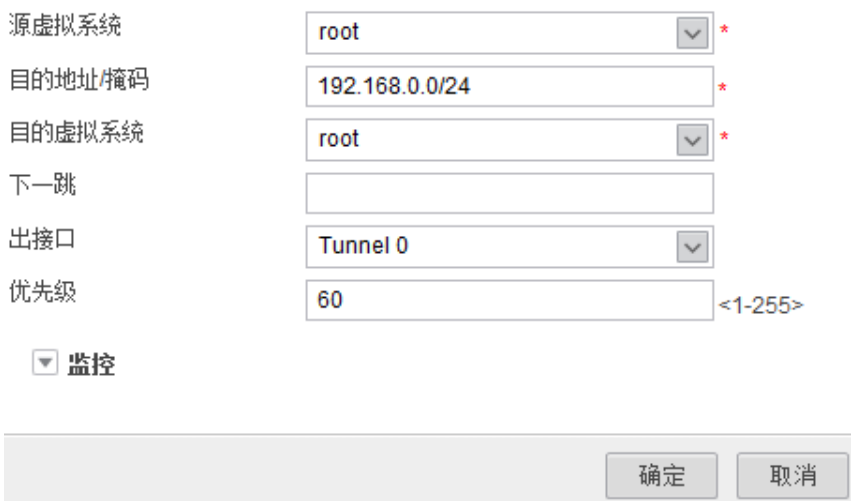
配置 USG_B：

Step 6 配置静态路由。选择“网络 > 路由 > 静态路由”。在“静态路由列表”中，单击“新建”。在“新建静态路由”界面中，配置如下图所示：

配置 USG_A：



配置 USG_B：



验证结果

PC1 和 PC2 之间能够相互 Ping 通。

9 IPSec VPN 实验

9.1 点到点的 IPSec 隧道实验

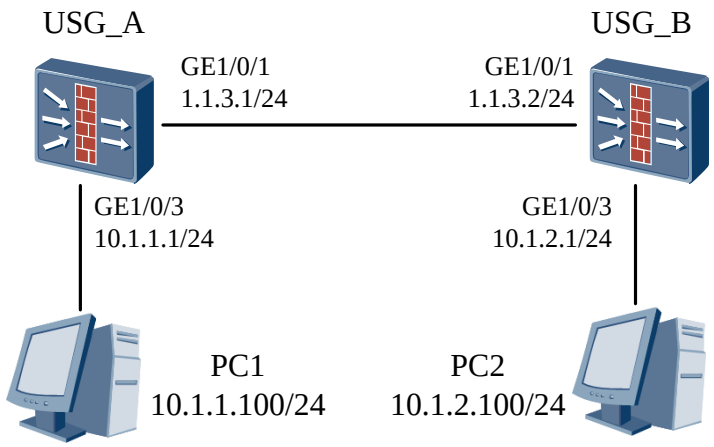
实验目的

掌握点对点方式，两端 VPN 设备公网 IP 地址固定场景下 IPSec VPN 的基本配置方法。

组网设备

USG 防火墙 2 台，PC 机 2 台。

实验拓扑图



实验步骤 - CLI

配置 USG_A：

Step 1 基础配置。（略）

Step 2 配置域间过滤规则。

```
[USG_A]security-policy
[USG_A-policy-security]rule name policy_sec1
```

```
[USG_A-policy-security-rule-policy_sec1]source-zone trust untrust
[USG_A-policy-security-rule-policy_sec1]destination-zone trust untrust
[USG_A-policy-security-rule-policy_sec1]source-address 10.1.1.0 24
[USG_A-policy-security-rule-policy_sec1]source-address 10.1.2.0 24
[USG_A-policy-security-rule-policy_sec1]destination-address 10.1.1.0 24
[USG_A-policy-security-rule-policy_sec1]destination-address 10.1.2.0 24
[USG_A-policy-security-rule-policy_sec1]action permit
[USG_A-policy-security-rule-policy_sec1]quit
[USG_A-policy-security]rule name policy_sec2
[USG_A-policy-security-rule-policy_sec2]source-zone local untrust
[USG_A-policy-security-rule-policy_sec2]destination-zone local untrust
[USG_A-policy-security-rule-policy_sec2]source-address 1.1.3.0 24
[USG_A-policy-security-rule-policy_sec2]destination-address 1.1.3.0 24
[USG_A-policy-security-rule-policy_sec2]action permit
[USG_A-policy-security-rule-policy_sec2]quit
```

Step 3 配置 USG_A 的 ACL，定义要保护的数据流。

```
[USG_A]acl 3000
[USG_A-acl-adv-3000]rule permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
[USG_A-acl-adv-3000]quit
```

Step 4 配置到对端私网地址段的静态路由

```
[USG_A] ip route-static 10.1.2.0 255.255.255.0 1.1.3.2
```

Step 5 配置 IPSec 安全提议。

```
[USG_A] ipsec proposal tran1
[USG_A-ipsec-proposal-tran1]quit
```

Step 6 配置 IKE 安全提议。

```
[USG_A] ike proposal 10
[USG_A-ike-proposal-10] quit
```

Step 7 配置 IKE peer。

```
[USG_A]ike peer b
[USG_A-ike-peer-b]ike-proposal 10
[USG_A-ike-peer-b]remote-address 1.1.3.2
[USG_A-ike-peer-b]pre-shared-key huawei
[USG_A-ike-peer-b]quit
```

Step 8 配置安全策略。

```
[USG_A] ipsec policy map1 10 isakmp
[USG_A-ipsec-policy-isakmp-map1-10] security acl 3000
```

```
[USG_A-ipsec-policy-isakmp-map1-10] proposal tran1
[USG_A-ipsec-policy-isakmp-map1-10] ike-peer b
[USG_A-ipsec-policy-manual-map1-10] quit
```

Step 9 在接口上引用安全策略。

```
[USG_A] interface GigabitEthernet 1/0/1
[USG_A-GigabitEthernet1/0/1] ipsec policy map1
```

配置 USG_B：

Step 10 基础配置。（略）

Step 11 配置域间过滤规则。

```
[USG_B]security-policy
[USG_B-policy-security]rule name policy_sec1
[USG_B-policy-security-rule-policy_sec1]source-zone trust untrust
[USG_B-policy-security-rule-policy_sec1]destination-zone trust untrust
[USG_B-policy-security-rule-policy_sec1]source-address 10.1.1.0 24
[USG_B-policy-security-rule-policy_sec1]source-address 10.1.2.0 24
[USG_B-policy-security-rule-policy_sec1]destination-address 10.1.1.0 24
[USG_B-policy-security-rule-policy_sec1]destination-address 10.1.2.0 24
[USG_B-policy-security-rule-policy_sec1]action permit
[USG_B-policy-security-rule-policy_sec1]quit
[USG_B-policy-security]rule name policy_sec2
[USG_B-policy-security-rule-policy_sec2]source-zone local untrust
[USG_B-policy-security-rule-policy_sec2]destination-zone local untrust
[USG_B-policy-security-rule-policy_sec2]source-address 1.1.3.0 24
[USG_B-policy-security-rule-policy_sec2]destination-address 1.1.3.0 24
[USG_B-policy-security-rule-policy_sec2]action permit
[USG_B-policy-security-rule-policy_sec2]quit
```

Step 12 配置 USG_B 的 ACL，定义要保护的数据流。

```
[USG_B]acl 3000
[USG_B-acl-adv-3000]rule permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0
0.0.00.255
[USG_B-acl-adv-3000]quit
```

Step 13 配置到对端私网网段的静态路由

```
[USG_B] ip route-static 10.1.1.0 255.255.255.0 1.1.3.1
```

Step 14 配置 IPSec 安全提议。

```
[USG_B] ipsec proposal tran1
[USG_B-ipsec-proposal-tran1]quit
```

Step 15 配置 IKE 安全提议。

```
[USG_B] ike proposal 10
[USG_B-ike-proposal-10] quit
```

Step 16 配置 IKE peer。

```
[USG_B]ike peer a
[USG_B-ike-peer-b]ike-proposal 10
[USG_B-ike-peer-b]remote-address 1.1.3.1
[USG_B-ike-peer-b]pre-shared-key huawei
[USG_B-ike-peer-b]quit
```

Step 17 配置安全策略。

```
[USG_B] ipsec policy map1 10 isakmp
[USG_B-ipsec-policy-isakmp-map1-10] security acl 3000
[USG_B-ipsec-policy-isakmp-map1-10] proposal tran1
[USG_B-ipsec-policy-isakmp-map1-10] ike-peer a
[USG_B-ipsec-policy-manual-map1-10] quit
```

Step 18 接口上引用安全策略。

```
[USG_B] interface GigabitEthernet 1/0/1
[USG_B-GigabitEthernet1/0/1] ipsec policy map1
```

实验步骤 – Web

配置 USG_A：

Step 1 基础配置。（略）

Step 2 配置 Trust 域与 Untrust 域的域间过滤规则和 Local 安全区域和 Untrust 安全区域之间的安全策略。

USG_A=10.1.1.0/24 USG_B=10.1.2.0/24
LOCAL_A=1.1.3.0/24 LOCAL_B=1.1.3.0/24

Step 3 配置到对端私网网段的静态路由。

Step 4 配置 USG_A 的 IPSec 隧道，选择“网络>IPSec>IPSec”，单击“新建”，选择“场景”为“点到点”。配置 IPSec 策略基本信息，并指定对端网关，预共享秘钥为 huawei。

Step 5 在“待加密的数据流”中单击“新建”，按如下数据增加一条数据流规则。

Step 6 展开“安全提议”中的“高级”，按如下参数配置 IPSec 安全提议，本例中所使用的安全提议参数全部为缺省配置。

USG_B 的配置与 USG_A 类似，仅需要修改静态路由、对端网关 IP 和需要 IPSec 隧道保护的数据流相应的 IP 地址即可，具体实验步骤略。

验证结果

配置成功后，从 PCA 可以 Ping 通 PCB，分别在 USG_A 和 USG_B 上执行 **display ike sa**、**display ipsec sa** 会显示安全联盟的建立情况。以 USG_B 为例，出现以下显示信息说明 IKE 安全联盟、IPSec 安全联盟建立成功。

```
<USG_B> display ike sa
current ike sa number: 2
  ------------------------------------------------------------------------------
    conn-id        peer                flag            phase       vpn
  ------------------------------------------------------------------------------
    101            1.1.3.1             RD              v2:2        public
    100            1.1.3.1             RD              v2:1        public

  flag meaning
  RD--READY       ST--STAYALIVE    RL--REPLACED          FD--FADING
  TO--TIMEOUT     TD--DELETING     NEG--NEGOTIATING      D--DPD
```

9.2 点到多点 IPSec 隧道实验

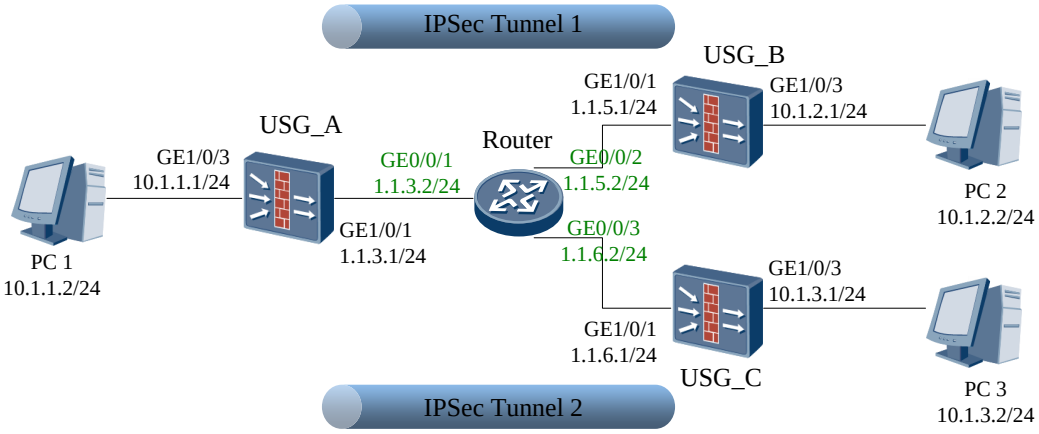
实验目的

掌握点到多点（总部到多个分支机构组网），分支机构 IP 地址不固定的场景下，总部通过 IKE 安全策略模板方式，分支机构通过 IKE 安全策略方式建立 IPSec 隧道的配置方法。

组网设备

USG 防火墙 3 台，路由器或三层交换机 1 台，PC 机 3 台。

实验拓扑图



注：USG_B 和 USG_C 所在分支机构公网 IP 地址为动态获取。本实验中为方便组网，均配置固定 IP 地址。

实验步骤 - CLI

配置 USG_A：

Step 1 基础配置。（略）

Step 2 配置到达分支机构的静态路由，此处假设下一跳地址为 1.1.3.2。

```
[USG_A] ip route-static 0.0.0.0 0.0.0.0 1.1.3.2
```

Step 3 定义被保护的数据流。

```
[USG_A] acl 3000
[USG_A-acl-adv-3000] rule permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
[USG_A-acl-adv-3000] rule permit ip source 10.1.1.0 0.0.0.255 destination 10.1.3.0 0.0.0.255
[USG_A-acl-adv-3000] quit
```

Step 4 配置名称为 tran1 的 IPSec 安全提议。（第 2 条命令开始为缺省配置可以不用配置）

```
[USG_A] ipsec proposal tran1
[USG_A-ipsec-proposal-tran1] encapsulation-mode tunnel
[USG_A-ipsec-proposal-tran1] transform esp
[USG_A-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
[USG_A-ipsec-proposal-tran1] esp encryption-algorithm aes
[USG_A-ipsec-proposal-tran1] quit
```

Step 5 配置序号为 10 的 IKE 安全提议。（第 2 条命令开始为缺省配置可以不用配置）

```
[USG_A] ike proposal 10
[USG_A-ike-proposal-10] authentication-method pre-share
[USG_A-ike-proposal-10] authentication-algorithm sha2-256
[USG_A-ike-proposal-10] quit
```

Step 6 配置名称为 b 的 IKE Peer。

```
[USG_A] ike peer b
[USG_A-ike-peer-b] ike-proposal 10
[USG_A-ike-peer-b] pre-shared-key huawei
[USG_A-ike-peer-b] quit
```

Step 7 配置名称为 map_temp 序号为 1 的 IPSec 安全策略模板。

```
[USG_A] ipsec policy-template map_temp 1
[USG_A-ipsec-policy-templet-map_temp-1] security acl 3000
[USG_A-ipsec-policy-templet-map_temp-1] proposal tran1
[USG_A-ipsec-policy-templet-map_temp-1] ike-peer b
[USG_A-ipsec-policy-templet-map_temp-1] quit
```

Step 8 在 IPSec 安全策略 map1 中引用安全策略模板 map_temp。

```
[USG_A] ipsec policy map1 10 isakmp template map_temp
```

Step 9 在接口 GigabitEthernet 1/0/1 上应用安全策略 map1。

```
[USG_A] interface GigabitEthernet 1/0/1
[USG_A-GigabitEthernet1/0/2] ipsec policy map1
[USG_A-GigabitEthernet1/0/2] quit
```

配置 USG_B：

Step 10 基础配置。（略）

Step 11 配置到达总部和其他私网的静态路由，下一跳地址为 1.1.5.2。

```
[USG_B] ip route-static 0.0.0.0 0.0.0.0 1.1.5.2
```

Step 12 定义被保护的数据流。

```
[USG_B] acl 3000
[USG_B-acl-adv-3000] rule permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.255.255
[USG_B-acl-adv-3000] quit
```

Step 13 配置名称为 tran1 的 IPSec 安全提议。（第 2 条命令开始为缺省配置可以不用配置）

```
[USG_B] ipsec proposal tran1
[USG_B-ipsec-proposal-tran1] encapsulation-mode tunnel
[USG_B-ipsec-proposal-tran1] transform esp
[USG_B-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
[USG_B-ipsec-proposal-tran1] esp encryption-algorithm aes
[USG_B-ipsec-proposal-tran1] quit
```

Step 14 配置序号为 10 的 IKE 安全提议。（第 2 条命令开始为缺省配置可以不用配置）

```
[USG_B] ike proposal 10
[USG_B-ike-proposal-10] authentication-method pre-share
[USG_B-ike-proposal-10] authentication-algorithm sha2-256
[USG_B-ike-proposal-10] quit
```

Step 15 配置 IKE Peer。

```
[USG_B] ike peer a
[USG_B-ike-peer-a] ike-proposal 10
[USG_B-ike-peer-a] remote-address 1.1.3.1
[USG_B-ike-peer-a] pre-shared-key huawei
[USG_B-ike-peer-a] quit
```

Step 16 配置名称为：map1，序号为：10 的 IPSec 安全策略。

```
[USG_B] ipsec policy map1 10 isakmp
[USG_B-ipsec-policy-isakmp-map1-10] security acl 3000
[USG_B-ipsec-policy-isakmp-map1-10] proposal tran1
[USG_B-ipsec-policy-isakmp-map1-10] ike-peer a
[USG_B-ipsec-policy-isakmp-map1-10] quit
```

Step 17 在 GE1/0/1 接口上应用安全策略 map1。

```
[USG_B] interface GigabitEthernet 1/0/1
[USG_B-GigabitEthernet1/0/1] ipsec policy map1
[USG_B-GigabitEthernet1/0/1] quit
```

配置 USG_C：

Step 18 基础配置。（略）

Step 19 配置到达总部和其他私网的静态路由，下一跳地址为 1.1.6.2。

```
[USG_C] ip route-static 0.0.0.0 0.0.0.0 1.1.6.2
```

Step 20 定义被保护的数据流。

```
[USG_C] acl 3000
[USG_C-acl-adv-3000] rule permit ip source 10.1.3.0 0.0.0.255 destination 10.1.1.0 0.0.255.255
[USG_C-acl-adv-3000] quit
```

Step 21 配置名称为 tran1 的 IPSec 安全提议。（第 2 条命令开始为缺省配置可以不用配置）

```
[USG_C] ipsec proposal tran1
[USG_C-ipsec-proposal-tran1] encapsulation-mode tunnel
[USG_C-ipsec-proposal-tran1] transform esp
[USG_C-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
[USG_C-ipsec-proposal-tran1] esp encryption-algorithm aes
[USG_C-ipsec-proposal-tran1] quit
```

Step 22 配置序号为 10 的 IKE 安全提议。（第 2 条命令开始为缺省配置可以不用配置）

```
[USG_C] ike proposal 10
[USG_C-ike-proposal-10] authentication-method pre-share
[USG_C-ike-proposal-10] authentication-algorithm sha2-256
[USG_C-ike-proposal-10] quit
```

Step 23 配置 IKE Peer。

```
[USG_C] ike peer a
[USG_C-ike-peer-a] ike-proposal 10
[USG_C-ike-peer-a] remote-address 1.1.3.1
[USG_C-ike-peer-a] pre-shared-key huawei
```

```
[USG_C-ike-peer-a] quit
```

Step 24 配置名称为 map1 序号为 10 的 IPSec 安全策略。

```
[USG_C] ipsec policy map1 10 isakmp
[USG_C-ipsec-policy-isakmp-map1-10] security acl 3000
[USG_C-ipsec-policy-isakmp-map1-10] proposal tran1
[USG_C-ipsec-policy-isakmp-map1-10] ike-peer a
[USG_C-ipsec-policy-isakmp-map1-10] quit
```

Step 25 在 GigabitEthernet 1/0/1 接口上应用安全策略 map1。

```
[USG_C] interface GigabitEthernet 1/0/1
[USG_C-GigabitEthernet1/0/1] ipsec policy map1
[USG_C-GigabitEthernet1/0/1] quit
```

Step 26 配置路由器接口地址（略）。

实验步骤 - Web

配置 USG_A：

Step 1 基础配置。（略）

Step 2 配置 Trust 域与 Untrust 域的域间过滤规则和 Local 安全区域和 Untrust 安全区域之间的安全策略。

USG_A=10.1.1.0/24 USG_B=10.1.2.0/24 USG_C=10.1.3.0/24
LOCAL_A=1.1.3.0/24 LOCAL_B=1.1.5.0/24 LOCAL_C=1.1.6.0/24

Step 3 配置到对端私网网段的缺省静态路由。

Step 4 配置 USG_A 的 IPSec 隧道，选择“网络>IPSec>IPSec”，在“IPSec 策略列表”下单击“新建”，选择“场景”为“点到多点”，“对端接入类型”选择“分支网关”，按如下参数配置“基本配置”，总部此时为了让多个网关接入，不指定对端网关的详细信息，预共享秘钥为 huawei。

Step 5 勾选“待加密的数据流”中的“反向路由注入”，表示总部自动生成到分支私网的路由。

Step 6 勾选“安全提议”中的“接受对端提议”，表示由分支网关来提议 IPSec 协议和算法。

Step 7 单击“应用”，完成 USG_A 配置。

USG_B 配置：

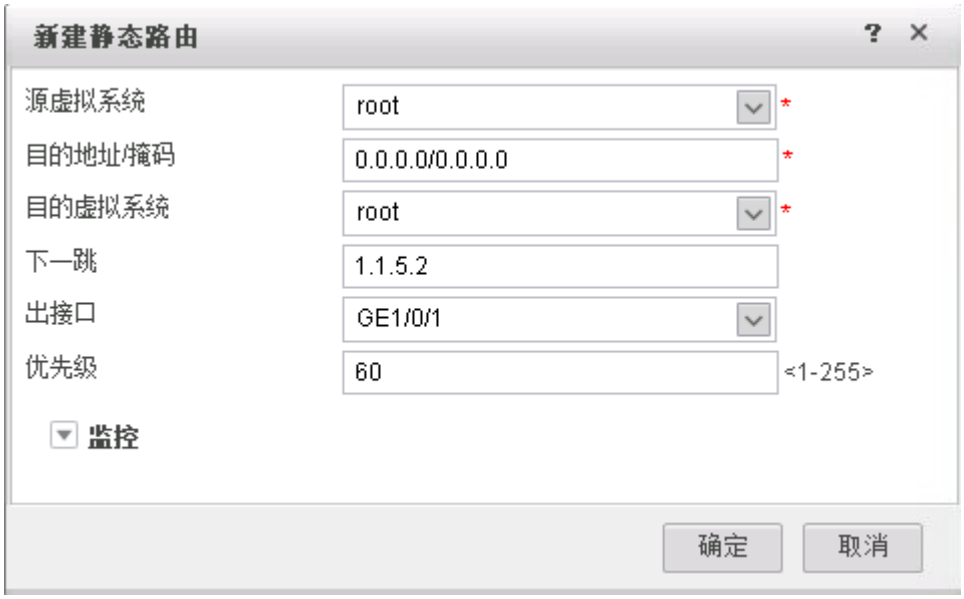
Step 8 基础配置。（略）

Step 9 配置 Trust 域与 Untrust 域的域间缺省过滤规则和 Local 安全区域和 Untrust 安全区域之间的安全策略。

USG_A=10.1.1.0/24 USG_B=10.1.2.0/24

LOCAL_A=1.1.3.0/24 LOCAL_B=1.1.5.0/24

Step 10 配置到对端私网网段的静态路由



Step 11 配置 USG_B 的 IPSec 隧道。选择“网络>IPSec>IPSec”，单击“新建”，选择“场景”为“点到点”。配置 IPSec 策略基本信息，并指定对端网关，预共享秘钥为 huawei。

Step 12 在“待加密的数据流”中单击“新建”，按如下数据增加一条数据流规则。

Step 13 展开“安全提议”中“高级”，本例中所使用的安全提议参数全部为缺省配置。

USG_C 配置与 USG_B 类似，仅需要修改静态路由和需要 IPSec 隧道保护的数据流相应的 IP 地址即可，具体实验步骤略。

Step 14 配置路由器接口地址（同命令行方式）。

验证结果

在 PC2 和 PC3 上分别 Ping PC1，都可以 Ping 通。

分别在 USG_A、USG_B 和 USG_C 上执行 **display ike sa**、**display ipsec sa**，显示安全

联盟的建立情况。

以 USG_B 为例，出现以下显示说明 IKE 安全联盟、IPSec 安全联盟建立成功。

```
<USG_B> display ike sa
current ike sa number: 2
  ------------------------------------------------------------------------------
    conn-id        peer                 flag            phase       vpn
  ------------------------------------------------------------------------------
    101            1.1.3.1        RD|ST          v2:2          public
    100            1.1.3.1        RD|ST          v2:1          public

  flag meaning
  RD--READY       ST--STAYALIVE    RL--REPLACED          FD--FADING
  TO--TIMEOUT     TD--DELETING     NEG--NEGOTIATING      D--DPD
<USG_B> display ipsec sa
  ----------------------------
  IPsec policy name: "map1"
  sequence number: 10
  mode: isakmp
  vpn: public
  ----------------------------
    connection id: 4
    rule number: 0
    encapsulation mode: tunnel
    tunnel local : 1.1.5.1        tunnel remote: 1.1.3.1
    flow          source: 10.1.2.0-10.1.2.255 0-65535 0
    flow destination: 10.1.1.0-10.1.1.255 0-65535 0

    [inbound ESP SAs]
      spi: 7519344  (0x72bc70)
      vpn: public          said: 8    cpuid: 0x0000
      proposal: ESP-ENCRYPT-AES ESP-AUTH-SHA2-256
      sa remaining key duration  (bytes/sec) : 1887436044/3572
      max received sequence-number: 9
      udp encapsulation used for nat traversal: N

    [outbound ESP SAs]
      spi: 5365969  (0x51e0d1)
      vpn: public          said: 9    cpuid: 0x0000
      proposal: ESP-ENCRYPT-AES ESP-AUTH-SHA2-256
      sa remaining key duration  (bytes/sec) : 1887435576/3572
      max sent sequence-number: 10
```

udp encapsulation used for nat traversal: N

10 SSL VPN 综合实验

10.1 SSL VPN 综合实验

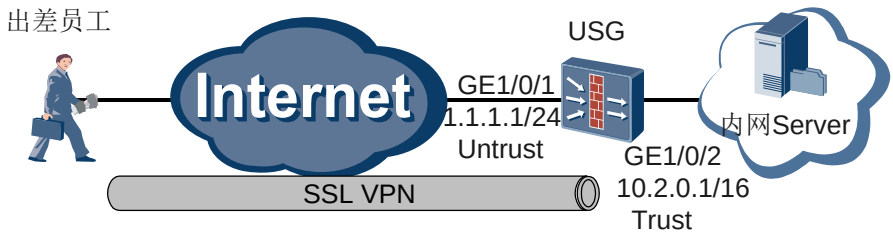
实验目的

掌握 SSL VPN 的相关应用及配置方法。

组网设备

USG 防火墙 1 台，服务器 1 台，PC 机 1 台。

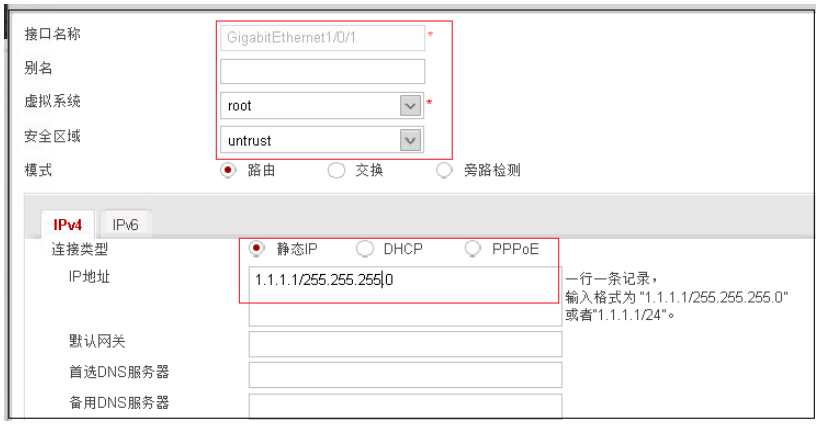
实验拓扑图



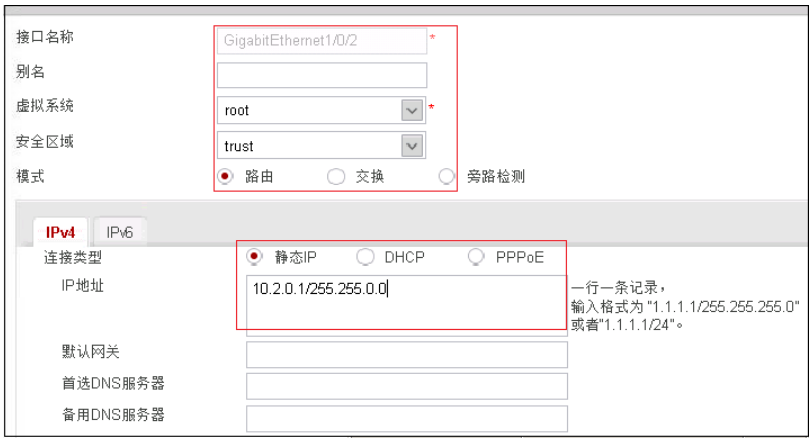
实验步骤

Step 1 配置接口。

选择“网络 > 接口”。 单击 GE1/0/1，按如下参数配置。



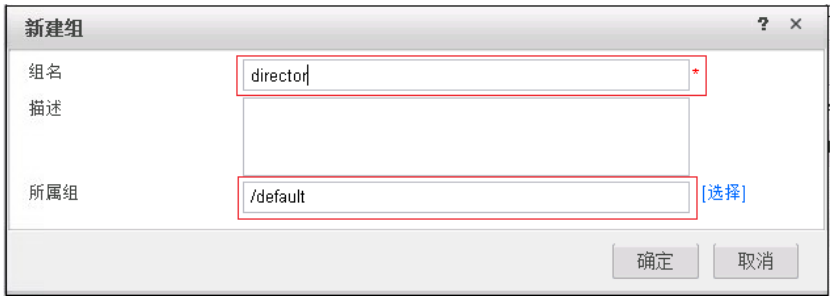
Step 2 参考上述步骤按如下参数配置 GE1/0/2 接口。



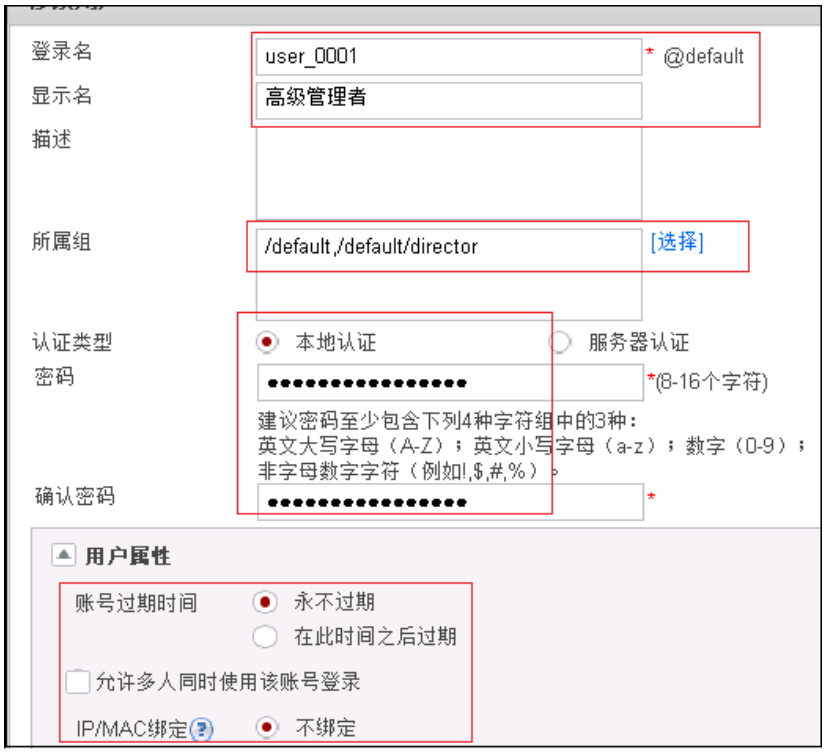
Step 3 配置用户和认证。

创建高级管理者对应的组和用户。 选择“对象 > 用户 > 用户/组”。 选中 default。

在“成员管理”中，单击“新建”，选择“新建组”，按如下参数配置。



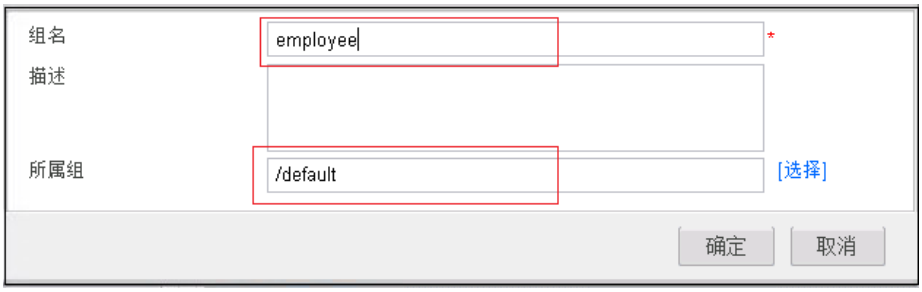
Step 4 在“成员管理”中，单击“新建”，选择“新建用户”，按如下参数配置。



Step 5 创建普通员工对应的组和用户。

选择“对象 > 用户 > 用户/组”。 选中”default”。

在“成员管理”中，单击“新建”，选择“新建组”，按如下参数配置。



Step 6 在“成员管理”中，单击“新建”，选择“新建用户”，按如下参数配置。

Step 7 配置认证域。

选择“对象 > 用户 > 认证域”。 单击“default”，按如下参数配置。

Step 8 配置 SSL VPN 网关。包括：网关地址、用户认证、最大并发用户数。

选择“网络 > SSL VPN > SSL VPN”。 单击“新建”，按如下参数配置 SSL VPN 网关。

配置完成后单击“下一步”。

Step 9 SSL 配置。

采用缺省配置即可，单击“下一步”。

Step 10 选择需要开启的业务。

选择“Web 代理”、“网络扩展”、“文件共享”、“端口转发”。 单击“下一步”。

Step 11 配置 Web 代理。

在“Web 代理资源”中，单击“新建”。 按如下参数添加 Web 代理资源 Webmail。

参考上述步骤按如下参数添加 Web 代理资源，资源名：ERP。

Step 12 配置网络扩展。

按如下参数配置可分配 IP 地址池范围。

在“可访问内网网段列表”中，单击“新建”。 按如下参数配置可访问的内网网段。

Step 13 启用文件共享服务。

配置文件共享。 勾选“启用”，并应用该设置。

在**文件共享资源管理**列表中，点击 新建 创建文件共享资源列表并应用。

Step 14 启用端口转发服务。

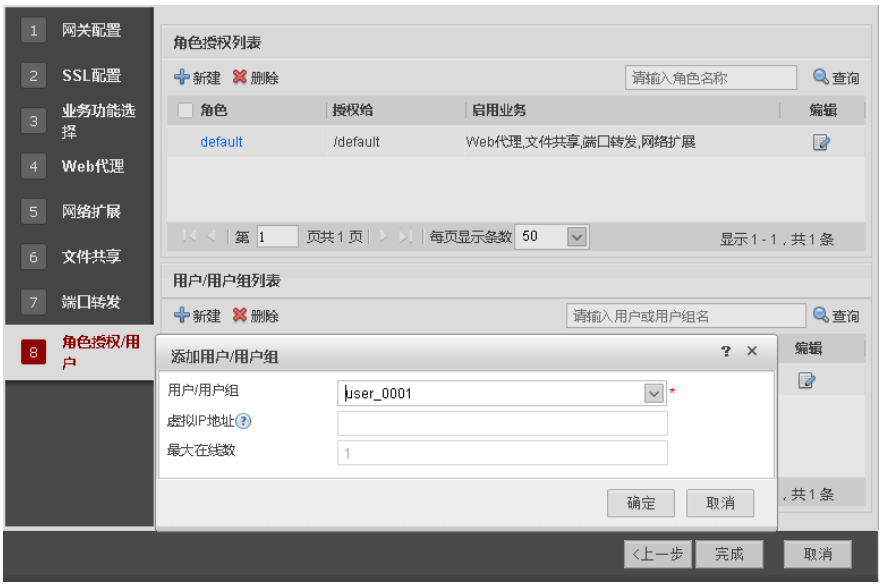
配置**端口转发**。启用端口转发服务并应用。

在**端口转发资源列表**中， 点击 新建 添加新的端口转发资源并应用设置。

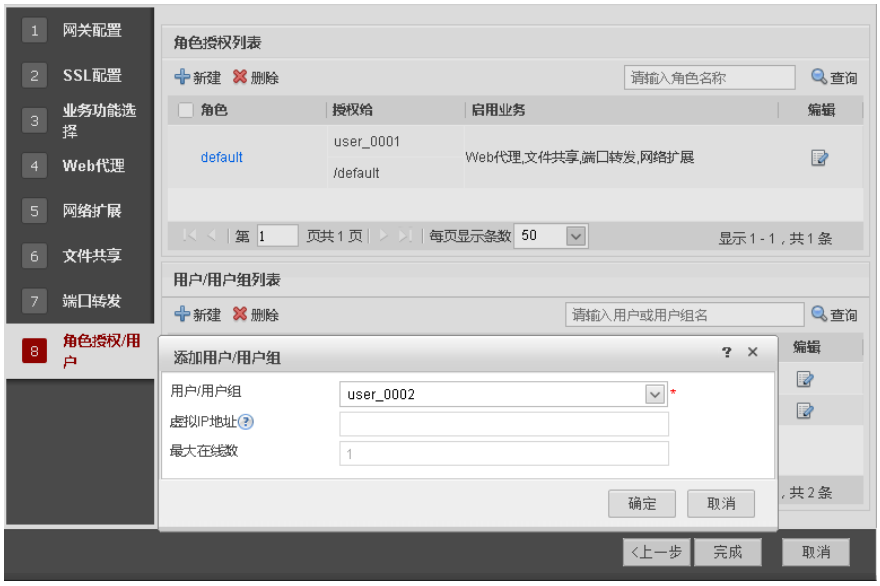
Step 15 配置 SSL VPN 的角色授权/用户。

在“用户/用户组列表”中，单击“新建”。

将使用 SSL VPN 业务的用户都加入用户列表，按如下参数配置 user_0001。



参考上述步骤按如下参数配置 user_0002。



在“角色授权列表”中，单击“新建”。 将 director 组加入角色并关联相应权限。

将 employee 组加入角色并关联相应权限。

Step 16 配置安全策略，允许用户使用 SSL VPN 业务。

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：policy_sslvpn_1。

参考上述步骤按照如下参数配置安全策略：policy_sslvpn_2。

验证结果

假设出差员工 user_0001 属于 director，那么他能够使用 Webmail 和 ERP， 通过网络扩展功能可以获得内网的 IP 地址，查看并下载文件共享资源，以及实现端口转发。验证步骤如下：

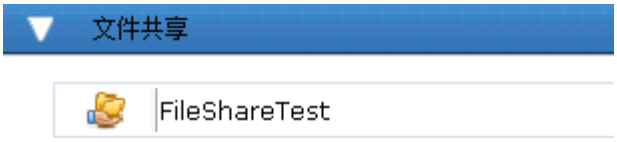
1. 在电脑的浏览器中输入"**https://1.1.1.1"**后，单击回车键。

2. 在弹出的安全警报中选择"是"。

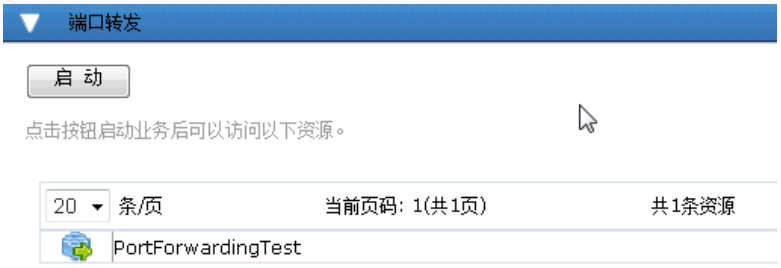
3. 在 SSL VPN 网关登录界面输入用户名和密码后，单击"登录"。登录成功后，你将会看到之前所配置的 Web 代理、文件共享、端口转发和网络扩展服务。

4. 在 SSL VPN 网关界面上显示 Web 代理资源"Webmail"和"ERP"，单击 "Webmail"或"ERP"即可使用相应的业务。

5. 在 SSL VPN 网关界面上显示文件共享资源"Study"，单击"Study"，输入文件服务器的用户名和密码后，即可查看并下载文档。



6. 在 SSL VPN 网关界面上显示端口转发资源。



7. 通过网络扩展功能可以获得内网的 IP 地址。 并且在 SSL VPN 网关界面上会显示网络扩展功能。单击"启动"后，自动安装的虚拟网卡会获取虚拟 IP 地址，用户就像在局域网一样能够访问各种业务。

11 UTM 实验

11.1 UTM 病毒库、IPS 签名库升级

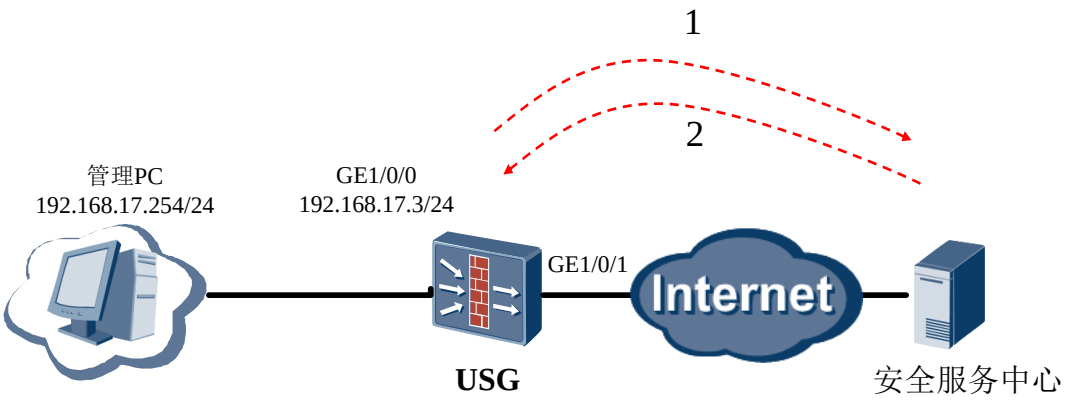
实验目的

掌握 UTM 病毒库升级及 IPS 签名库升级的配置方法。

组网设备

USG 防火墙 1 台，要求防火墙能够连接互联网，PC 机 1 台。

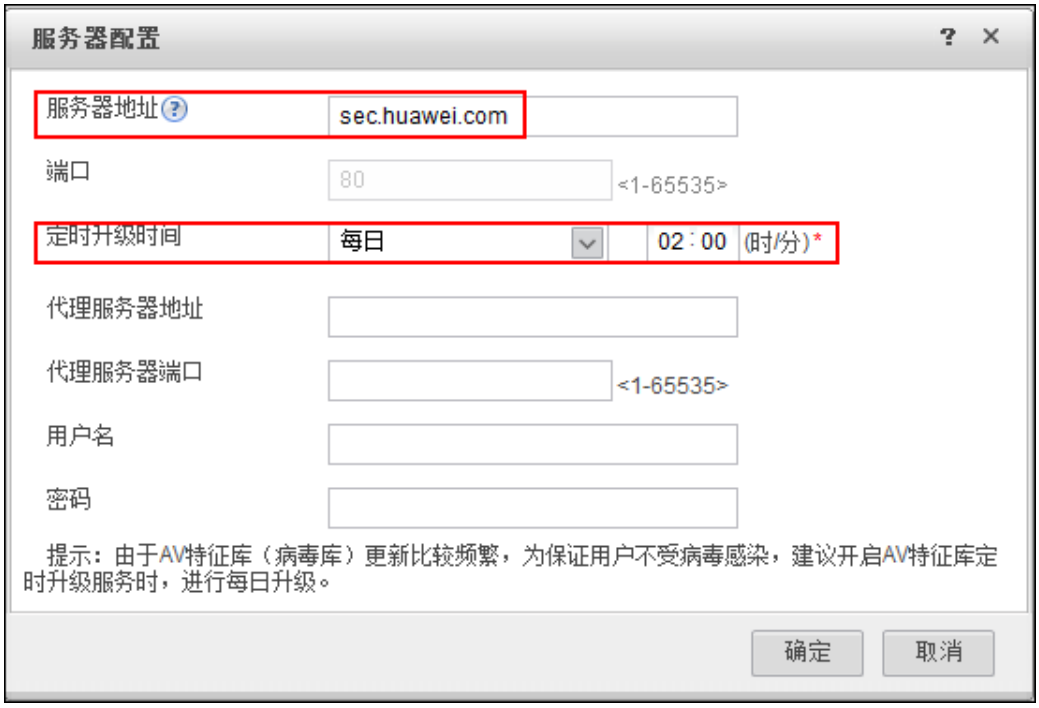
实验拓扑图



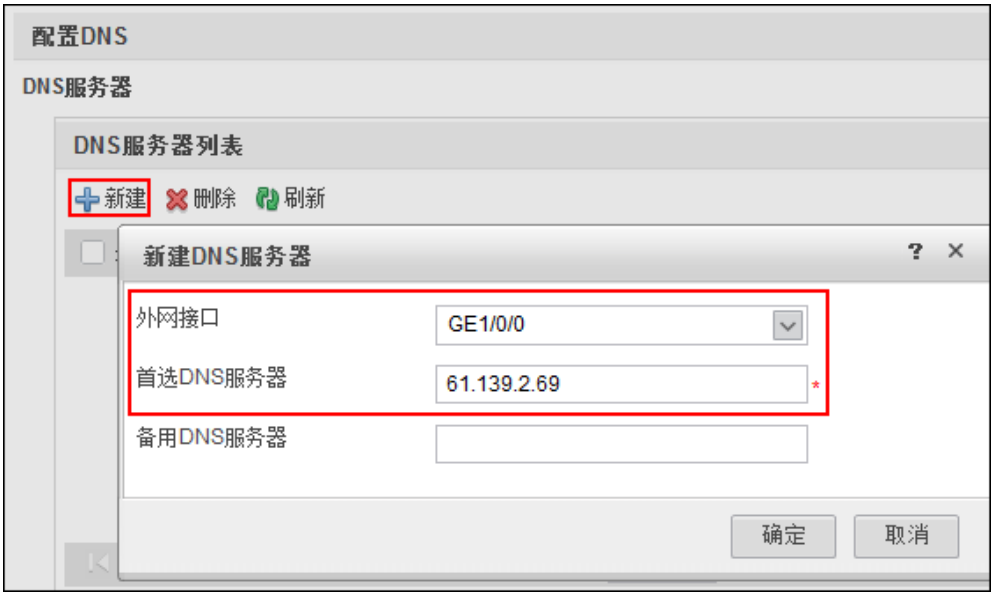
项目	设备	数据
（1）	USG（待升级签名库和病毒库设备）	接口号：GE1/0/0 IP 地址：192.168.17.3/24 安全区域：Trust 接口 GE1/0/1 能够连接互联网
（2）	内网管理 PC	管理 PC IP 地址：192.168.17.254/24

实验步骤 – Web

Step 1 配置安全服务中心。选择“系统 >升级中心”。点击“服务器地址”配置安全服务中心相关信息。在“安全服务中心域名”中，输入需配置的安全服务中心的域名：sec.huawei.com，并设定升级时间为每天 02：00。



Step 2 添加 DNS 服务器。选择“网络 > DNS > DNS”。在“DNS 服务器列表”的文本框新建 DNS 服务器。 单击“确定”。



验证结果

实验结果：

1），执行命令 **display update configuration**，查看内网升级的相关信息。

```
<USG>display update configuration
11:49:24  2015/05/06
Update Configuration Information:
-------------------------------------------------------------
  Update Server                    : sec.huawei.com
  Update Port                      : 80
  Proxy Server                     : -
  Proxy Port                       : -
  Proxy User                       : -
  Proxy Password                   : -
  IPS-SDB:
    Application Confirmation   : Disable
    Schedule Update                : Enable
    Schedule Update Frequency : Daily
    Schedule Update Time         : 02:00
  AV-SDB:
    Application Confirmation   : Disable
    Schedule Update                : Enable
    Schedule Update Frequency : Daily
    Schedule Update Time         : 02:00
  SA-SDB:
    Application Confirmation   : Disable
    Schedule Update                : Enable
    Schedule Update Frequency : Daily
    Schedule Update Time         : 02:00
-------------------------------------------------------------
```

2），执行命令 **display version ips-sdb** 和 **display version av-sdb**，可查看升级后的签名库或病毒库的版本。如果升级后的版本符合要求，表明升级成功。

```
<USG>display version ips-sdb
14:02:35  2015/05/06
IPS SDB Update Information List:
-----------------------------------------------------------------
  Current Version:
    Signature Database Version      : 2014082604
    Signature Database Size（byte） : 1849702
    Update Time                          : 13:44:29 2015/03/31
    Issue Time of the Update File : 15:15:43 2014/08/26

  Backup Version:
    Signature Database Version      :
```

```
    Signature Database Size（byte） : 0
    Update Time                     : 00:00:00 0000/00/00
    Issue Time of the Update File : 00:00:00 0000/00/00
-------------------------------------------------------------
IPS Engine Information List:
-------------------------------------------------------------
  Current Version:
    IPS Engine Version          : V200R001C10SPC225
    IPS Engine Size（byte）       : 3145728
    Update Time                 : 13:44:28 2015/03/31
    Issue Time of the Update File : 10:51:45 2014/09/21

  Backup Version:
    IPS Engine Version          :
    IPS Engine Size（byte）       : 0
    Update Time                 : 00:00:00 0000/00/00
    Issue Time of the Update File : 00:00:00 0000/00/00
-------------------------------------------------------------

<USG>display version av-sdb
14:03:42  2015/05/06
AV SDB Update Information List:
-------------------------------------------------------------
  Current Version:
    Signature Database Version  : 2014091500
    Signature Database Size（byte） : 115294666
    Update Time                 : 13:44:29 2015/03/31
    Issue Time of the Update File : 01:50:47 2014/09/15
  Backup Version:
    Signature Database Version  :
    Signature Database Size（byte） : 0
    Update Time                 : 00:00:00 0000/00/00
    Issue Time of the Update File : 00:00:00 0000/00/00
-------------------------------------------------------------
```

11.2 UTM 入侵防御实验

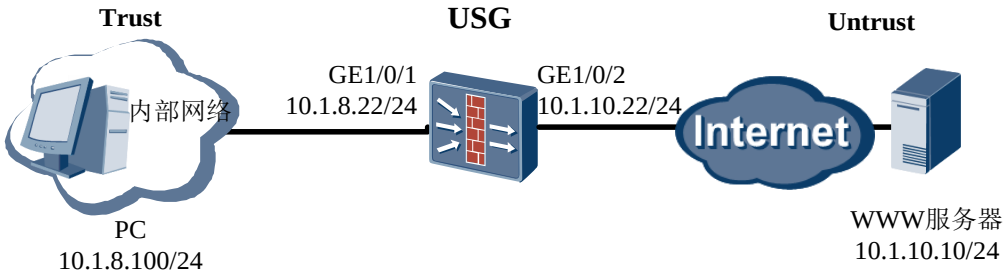
实验目的

掌握在 USG 设备上配置 UTM 入侵防御的方法。

组网设备

USG 防火墙 1 台，WWW 服务器一台，PC1 台。

实验拓扑图

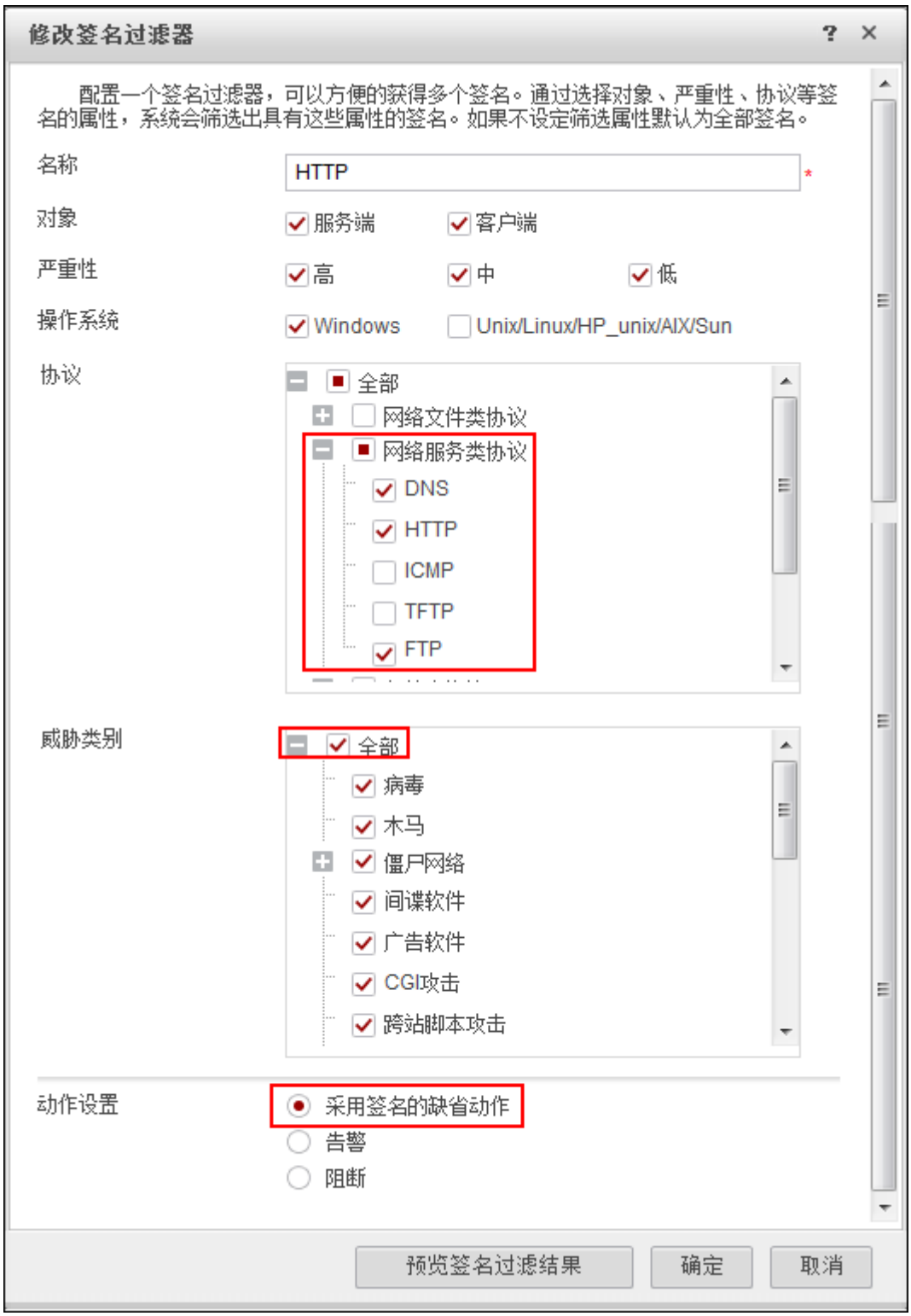


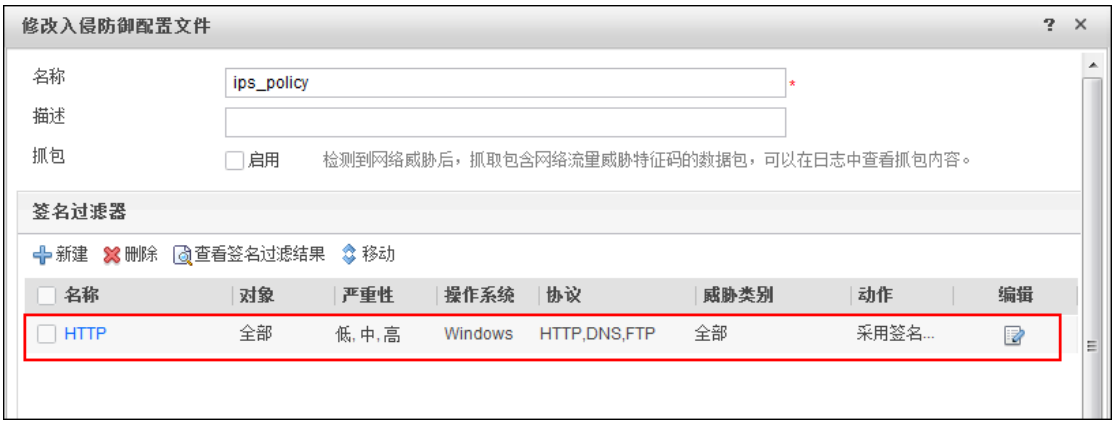
实验步骤 - Web

Step 1 完成防火墙基础配置（略）

Step 2 配置入侵防御策略。选择“对象 > 安全配置文件 > 入侵防御”。 单击“新建”。 创建名为“IPS_Policy”的入侵防御策略。

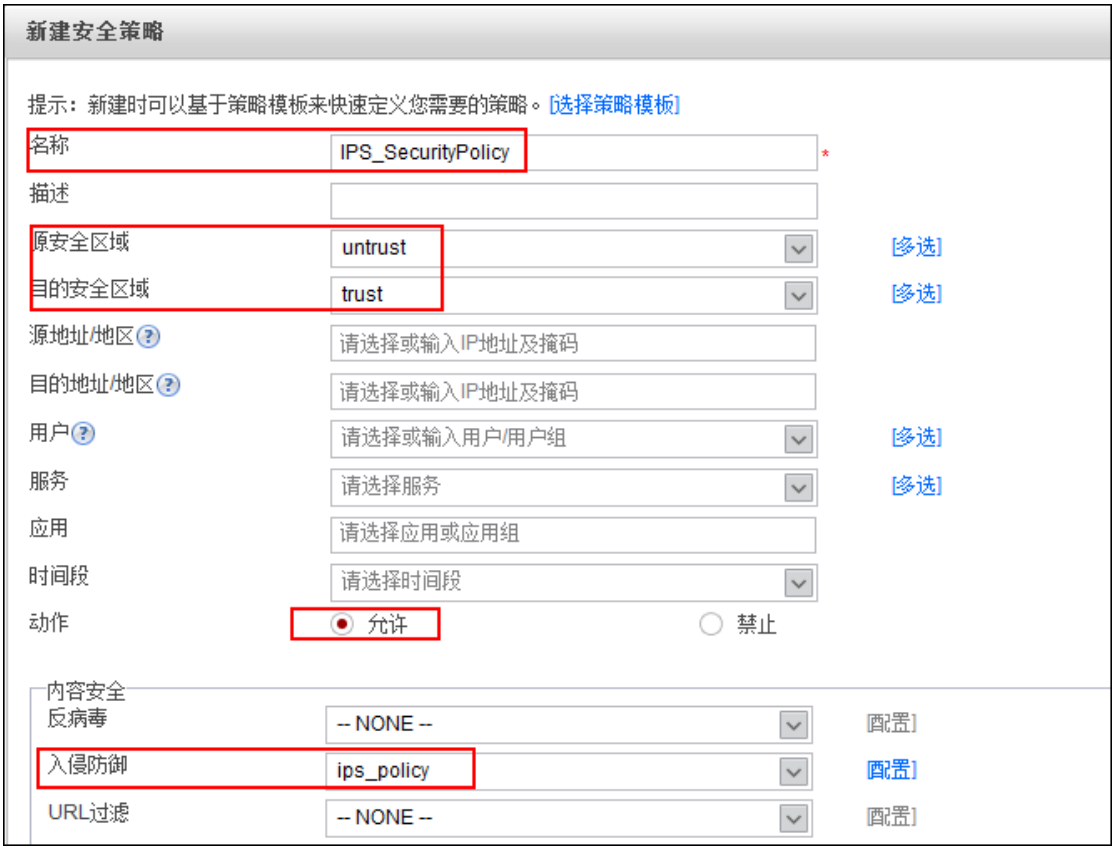
Step 3 在该入侵防御策略下，创建签名过滤器。阻断来自 HTTP 的入侵。


修改签名过滤器
配置一个签名过滤器，可以方便的获得多个签名。通过选择对象、严重性、协议等签名的属性，系统会筛选出具有这些属性的签名。如果不设定筛选属性默认为全部签名。
名称
HTTP
对象
服务端
客户端
严重性
高
中
低
操作系统
Windows
Unix/Linux/HP_unix/AIX/Sun
协议
全部
网络文件类协议
网络服务类协议
DNS
HTTP
ICMP
TFTP
FTP
威胁类别
全部
病毒
木马
僵尸网络
间谍软件
广告软件
CGI攻击
跨站脚本攻击
动作设置
采用签名的缺省动作
告警
阻断
预览签名过滤结果
确定
取消



Step 4 点击“提交”对配置的 IPS 策略进行编译。

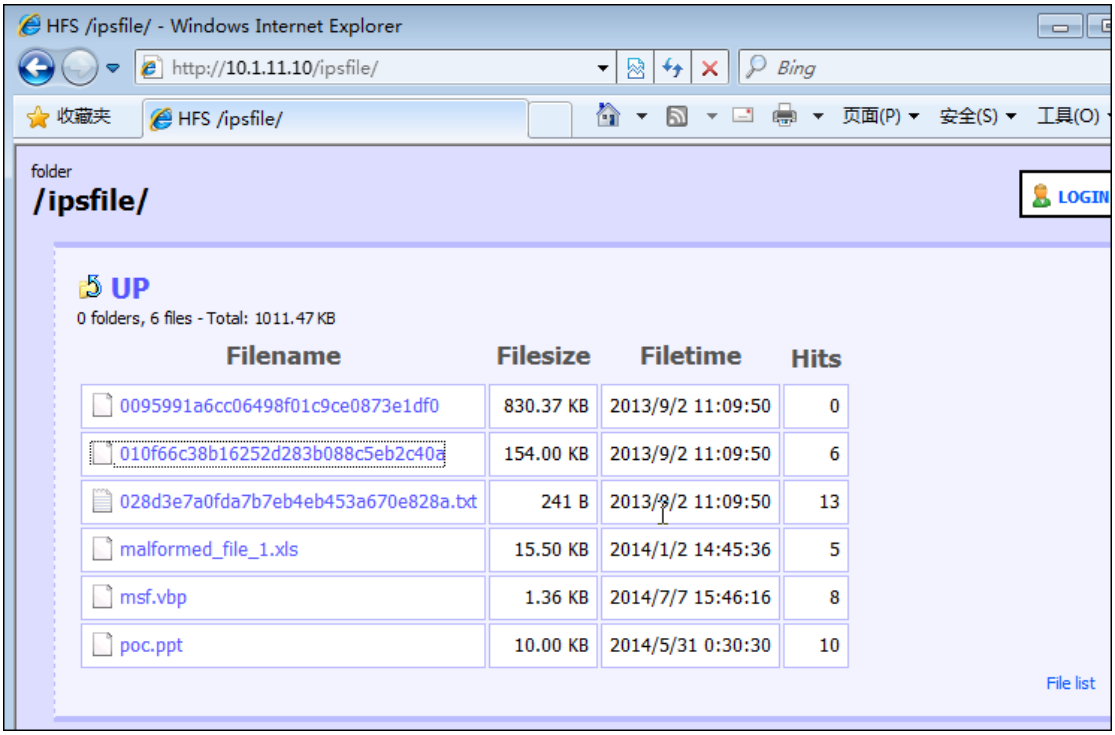
Step 5 配置安全策略，将入侵防御策略应用到该安全策略下。



验证结果

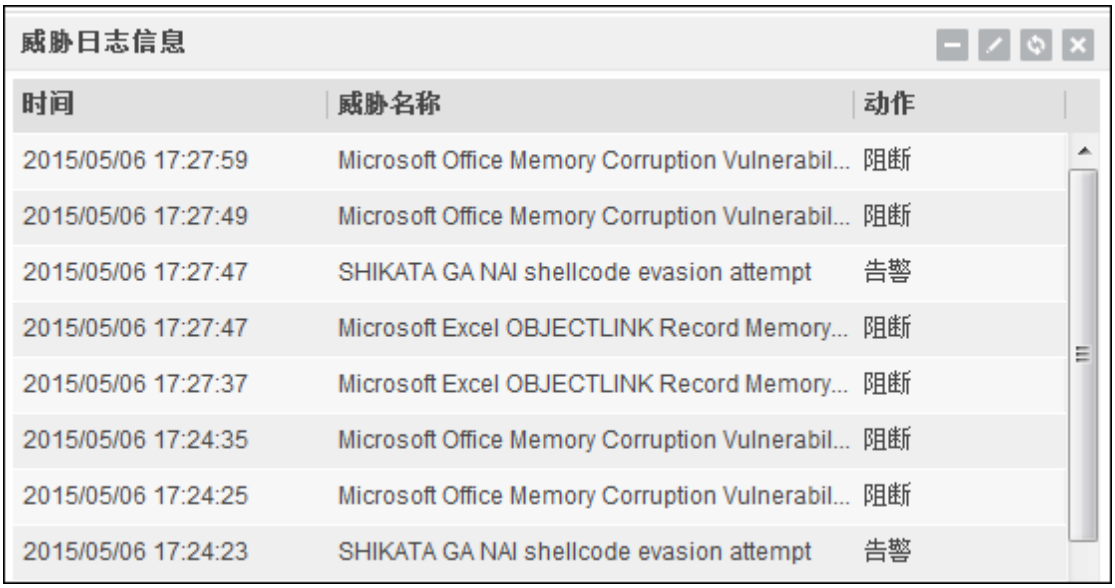
实验结果：

a. 在客户端上点击 IPS 测试文件



b. 当用户下载到恶意攻击文件时，连接将会被阻断。

c. 在设备主面板中查看威胁防护的阻断日志。



11.3 UTM AV 防病毒实验

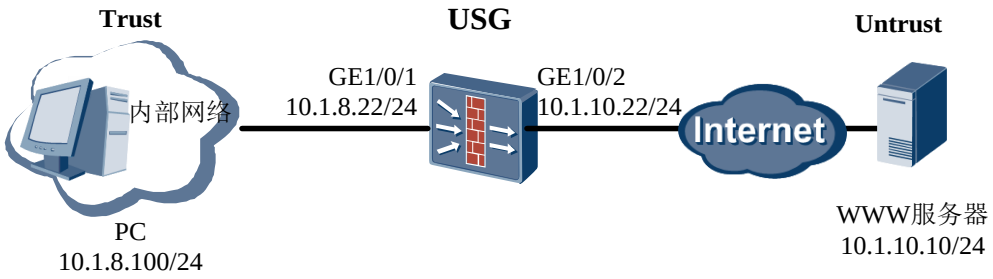
实验目的

掌握在 USG 设备上配置 UTM AV 防病毒的方法。

组网设备

USG 防火墙 1 台，WWW 服务器 1 台，PC 机 1 台。

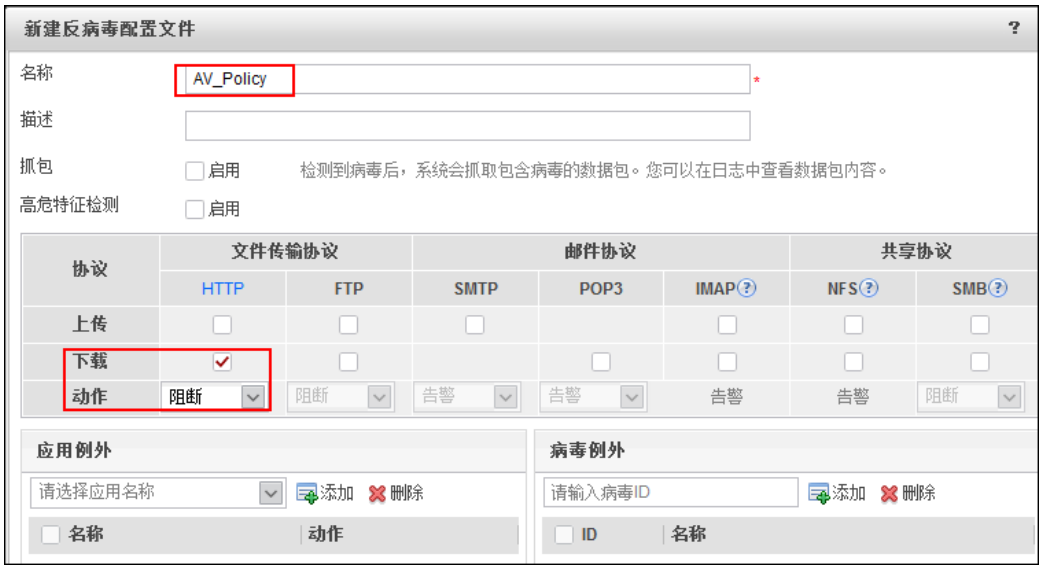
实验拓扑图



实验步骤

Step 1 配置 USG 相关接口的基本参数（略）。

Step 2 配置反病毒策略。选择“对象 > 安全配置文件 > 反病毒”。 单击“新建”。 创建名为“AV_Policy”的反病毒策略。在 HTTP 上下载文件时对其进行阻断。

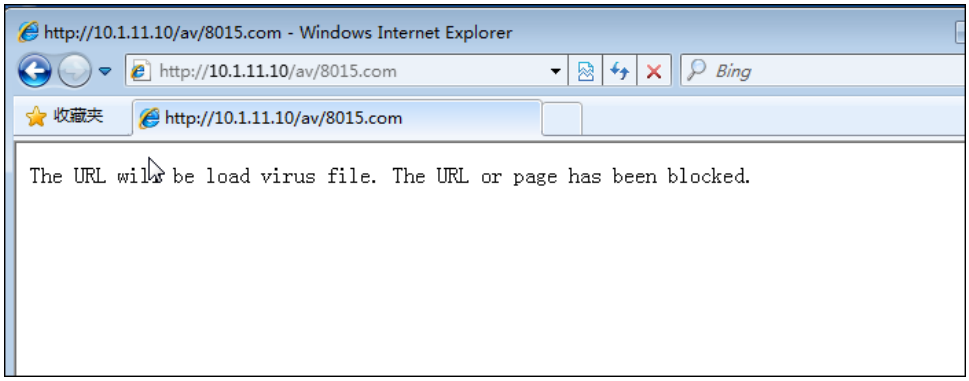


Step 3 配置安全策略，将反病毒策略应用到该安全策略下。

验证结果

实验结果：

1. 当用户访问带病毒的 Web 页面时，USG 防火墙会阻断连接。



2. 在设备主面板可以查看到相关的威胁日志。