Security 上机指导书

1 手册说明

本手册用于指导学员学习华为安全产品的配置和部署技术,学员可以通过教材的实验说明，掌握本手册中的实验内容。

1.1 适用范围

适用于华为系统安全工程师培训安全课程中涉及的实验内容。

适用防火墙系列包括:

- USG2200&5100 V300R001

1.2 防火墙产品描述

1.2.1 USG2200 产品描述

- 机箱尺寸

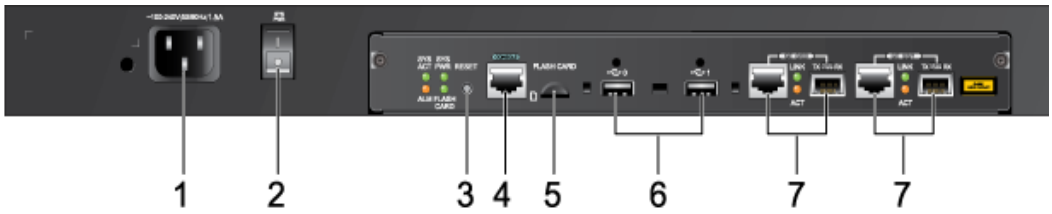
USG2200 由一体化机箱、扩展接口卡组成。其一体化机箱尺寸为 442mm×414mm×43.6mm（宽×深×高），可以安装在 19 英寸标准机柜中。

- 前面板

USG2200 的电源和风扇采用内置式，因此从外观上看不到电源和风扇。USG2200 包括 USG2210、USG2220、USG2230、USG2250 四种型号。这四种型号都支持交流机型，其中 USG2250 还有支持直流电源的机型。如下图所示。

USG2200 前面板（直流机型）

USG2200 前面板（交流机型）



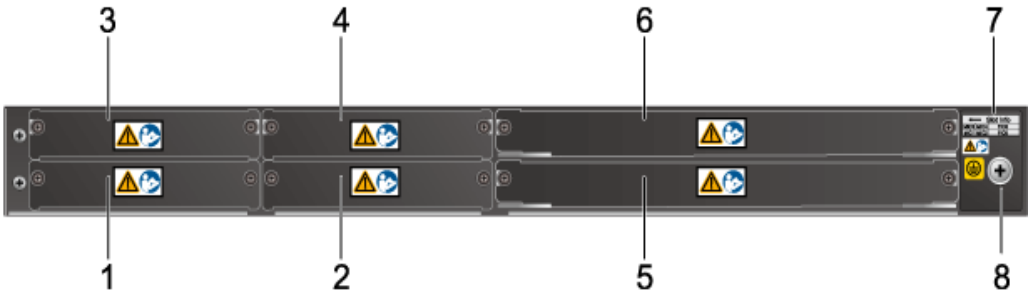
1. 交流/直流电源插座	2. 交流/直流电源开关	3. 系统复位键
4. Console 接口	5. 闪存接口	6. USB2.0 接口

7. GE ombo 接口		

- 后面板

USG2210、USG2220、USG2230、USG2250 后面板布局相同，如下图所示，左侧和中间是 4 个 MIC 插槽，右侧为 2 个 FIC 插槽。

USG2200 后面板



1. MIC1/DMIC1 插槽	2. MIC2/DMIC2 插槽	3. MIC3 插槽
4. MIC4 插槽	5. FIC5/DFIC5 插槽	6. FIC6 插槽
7.槽位标识	8. 接地端子	

- 槽位分布和排列顺序

FIC5 可插入一个 DFIC 接口卡。如下图所示。

USG2200 槽位编号及排列顺序示意图

MIC3	MIC4	FIC6
MIC1	MIC2	FIC5

提示：MIC1 和 MIC3 两个槽位可以插入两个 MIC 接口卡或插入一个 DMIC 接口卡；

MIC2 和 MIC4 两个槽位可以插入两个 MIC 接口卡或插入一个 DMIC 接口卡；

1.2.2 USG5120 产品描述

- 机箱尺寸

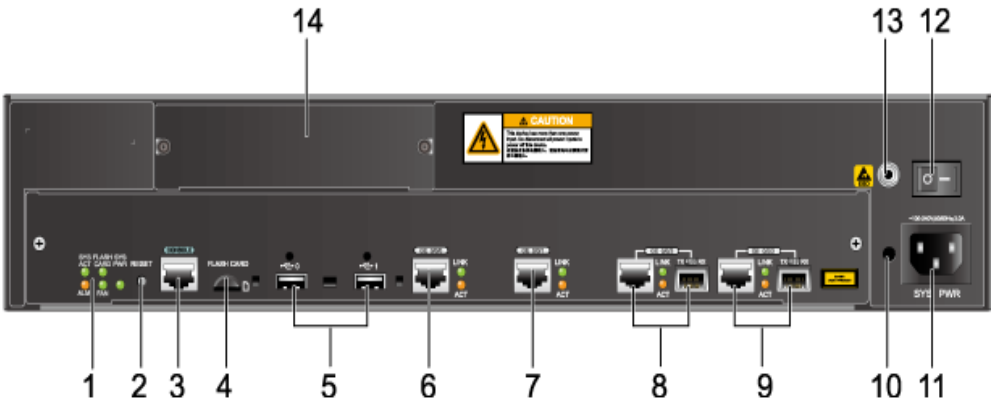
USG5120 由一体化机箱、扩展接口卡组成。其一体化机箱尺寸为 442mm×414mm×86.1mm（宽×深×高），可以安装在 19 英寸标准机柜中。

- 前面板

USG5120 有交流和直流两种机型。USG5120 的前面板如下图所示。

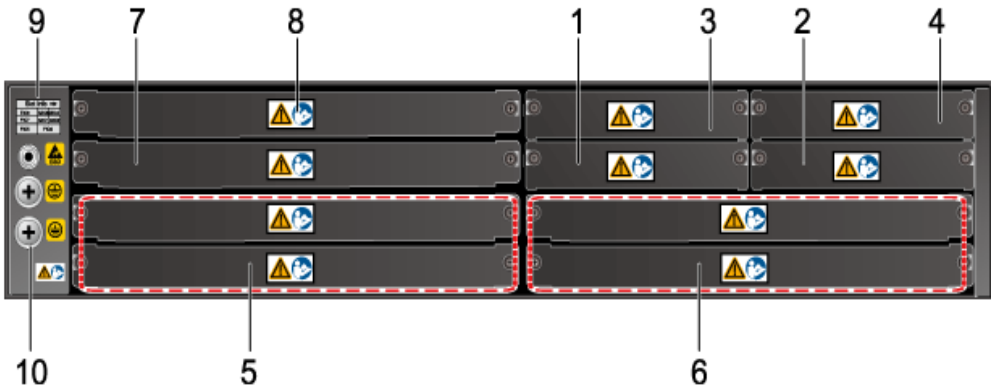
USG5120 前面板（直流机型）

USG5120 前面板（交流机型）



1.指示灯	2.系统复位键	3. Console 接口
4.闪存接口	5. USB2.0 接口	6. 10/100/1000M 以太网接口
7. 10/100/1000M 以太网品	8. GE Combo 接口 2	9. GE Combo 接口 3
10. 卡扣插孔	11. 交流/直流电源插座	12. 交流/直流电源开关
13. 防静电手腕带插孔	14. 防尘面板	

- 后面板



1. MIC1/DMIC1 插
2. MIC2/DMIC2 插槽
3. MIC3 插槽
4. MIC4 插槽
5. FIC5/DFIC5 插槽
6. FIC6/DFIC6 插槽
7. FIC7 插槽
8. FIC8 插槽
9. 槽位标识
10. 接地端子

- 槽位分布和排列顺序

USG5120 的 FIC5 和 FIC6 槽位除了可插入一个 DFIC 接口卡外，还可只在下半部分插入一个 FIC 接口卡。此时，为了防尘需要在 DFIC 槽位的上半部分安装一个假面板，以封闭后面板。FIC7 可插入一个 DFIC 接口卡。如下图所示。

USG5120 槽位编号及排列顺序示意图

FIC8	MIC3	MIC4
FIC7	MIC1	MIC2
FIC5	FIC6	

1.2.3 USG5150 产品描述

- 机箱尺寸

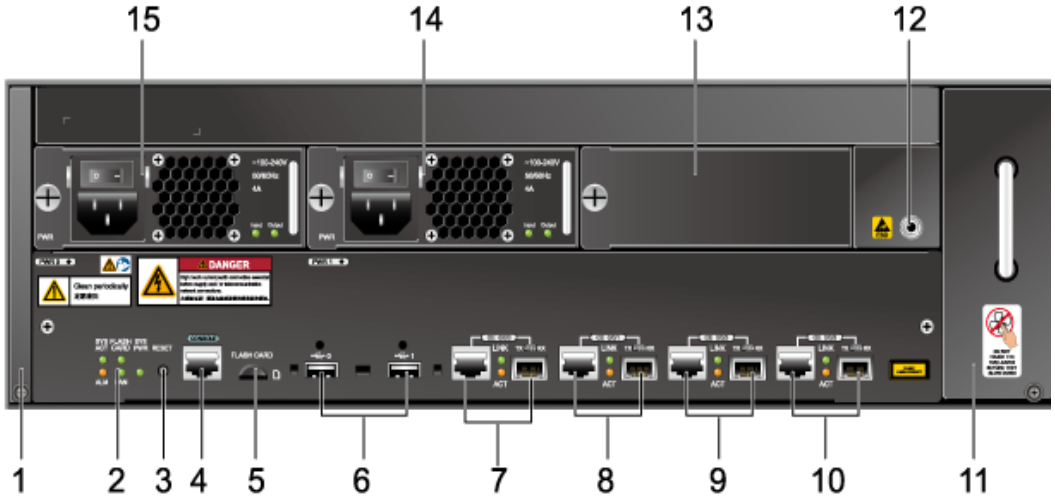
USG5150 由一体化机箱、扩展接口卡组成。其一体化机箱尺寸为 442mm×414mm×130.5mm（宽×深×高），可以安装在 19 英寸标准机柜中。

- 前面板

USG5150 的电源和风扇模块均可热插拔，其前面板如下图所示。

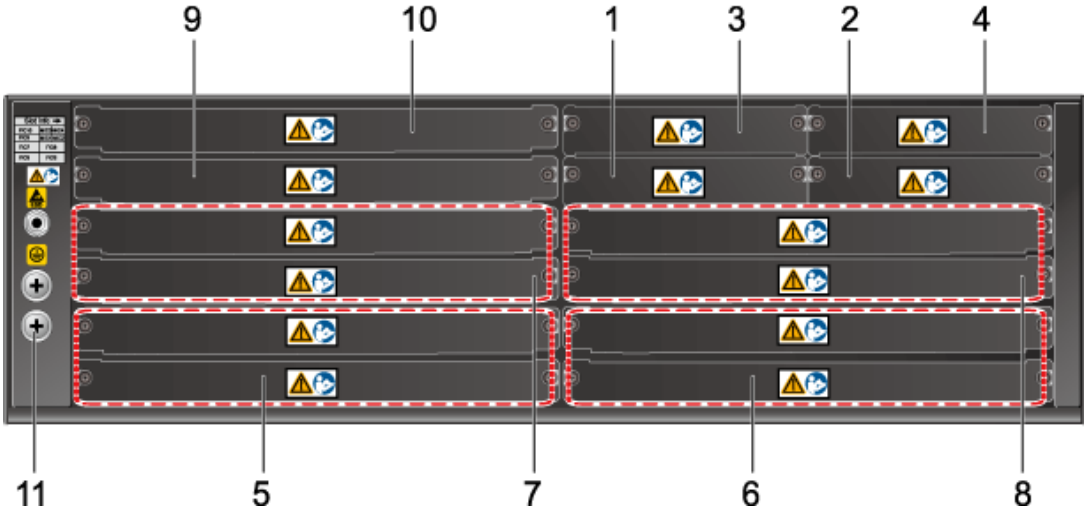
USG5150 前面板（直流机型）

USG5150 前面板（交流机型）



1.防尘网	2. 指示灯	3.系统复位键
4. Console 接口	5. 闪存接口	6. USB2.0 接口
7. GE Combo 接口 0	8. GE Combo 接口 1	9. GE Combo 接口 2
10. GE Combo 接口 3	11. 风扇框	12. ESD 防静电插孔
13. 防尘挡板	14. 交流/直流电源模块 1	15.交流/直流电源模块 0

- 后面板



1. MIC1/DMIC1 插槽	2. MIC2/DMIC2 插槽	3. MIC3 插槽
4. MIC4 插槽	5. FIC5/DFIC5 插槽	6. FIC6/DFIC6 插槽
7. FIC7/DFIC7 插槽	8. FIC8/DFIC8 插槽	9. FIC9 插槽
10. FIC10 插槽	11. 接地端子	

- 槽位分布和排列顺序

USG5150 的 FIC5、FIC6、FIC7 和 FIC8 槽位除了可插入一个 DFIC 接口卡外，还可只在下半部分插入一个 FIC 接口卡。此时，为了防尘需要在 DFIC 槽位的上半部分安装一个假面板，以封闭后面板。如下图所示。

USG5150 槽位编号及排列顺序示意图

FIC10	MIC3	MIC4
FIC9	MIC1	MIC2
FIC7	FIC8	
FIC5	FIC6	

提示：FIC9 和 FIC10 两个槽位可以插入两个 FIC 接口卡，但不可以使用 DFIC 接口卡；FIC9 和 FIC10 两个槽位不支持 1GE 接口卡、4GE 接口卡、1GPON 接口卡、16POTS 接口卡和 32POTS 接口卡；

1.2.4 物理接口编号方法

设备物理接口采用的编号原则如下：

各接口按照从下到上，从左到右的顺序依次编号。物理接口编号为 interface-type X/0/Y，interface-type 为接口类型（如 Ethernet 等），X 表示槽位号，0 为板卡号，目前支持的接口卡没有子卡，所以此位均为 0。Y 表示接口序号。主板的槽位号为 0。

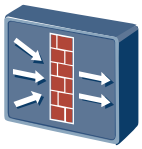
例如，USG 的 2 号槽位安装了 5FSW 接口卡，那么各接口的编号为：Ethernet2/0/0、Ethernet2/0/1、Ethernet2/0/2、Ethernet2/0/3、Ethernet2/0/4。

1.3 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

2 如何登陆防火墙设备

2.1 通过Console口登录设备(超级终端)

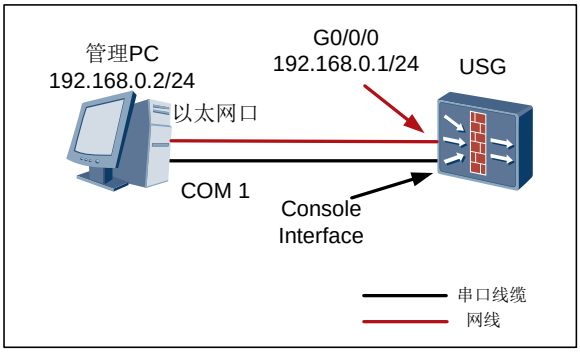
实验目的

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

组网设备

USG 防火墙一台，PC 机一台。

实验拓扑图



实验步骤

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。

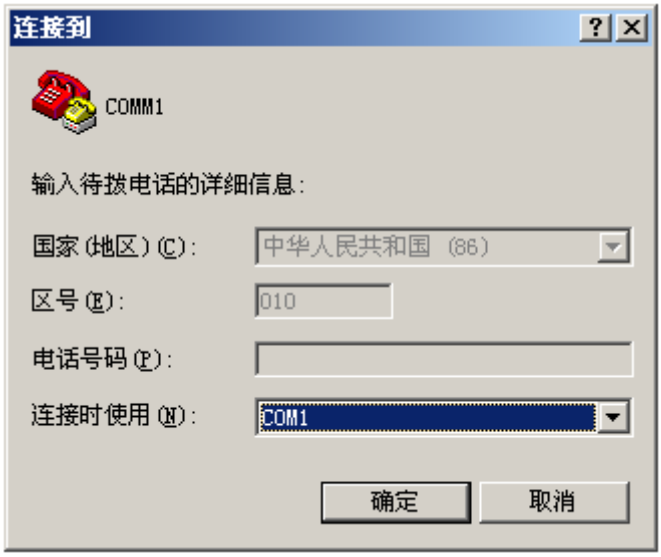
Step 2 在 PC 上运行终端仿真程序（以 Windows XP 的超级终端为例），选择“开始 > 程序 > 附件 > 通讯 > 超级终端”，显示“连接描述”对话框。

Step 3 在“名称”中输入 PC 与 USG 的连接名称，例如 COMM1；并在“图标”中选择任一图标，如图所示。

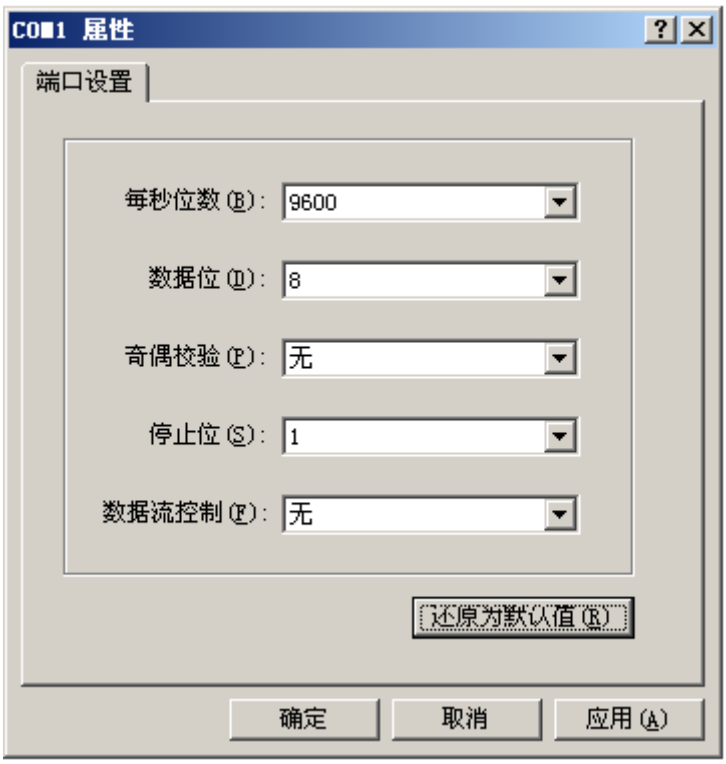
“连接描述”对话框（通过 Console 口登录）

Step 4 单击“确定”，显示“连接到”对话框。

Step 5 在“连接时使用”中选择 PC 与 USG 连接时使用的串口，例如 COM1，如图所示。



Step 6 单击“确定”，显示“COM1 属性”对话框。设置端口的通信参数，如图所示。



Step 7 单击“确定”或“还原为默认值（R）”。

Step 8 在 PC 仿真终端上，单击“Enter”，通过 USG 配置的认证方式后，按照提示输入用户名和密码后，即可进入用户视图，登录到设备上。

验证结果

```
**************************************************************************
*         Copyright(C) 2008-2012 Huawei Technologies Co., Ltd.           *
*                         All rights reserved                            *
*              Without the owner's prior written consent,                *
*         no decompiling or reverse-engineering shall be allowed.        *
**************************************************************************

User interface con0 is available
Please Press ENTER.
```

2.2 通过Web方式登录设备（默认方式登录）

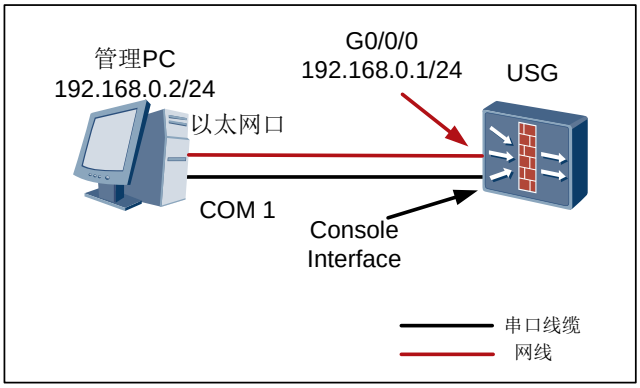
实验目的

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

组网设备

USG 防火墙一台，PC 机一台。

实验拓扑图



实验步骤

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 PC 网卡和 USG G0/0/0 接口正常连接网线。

Step 3 配置 PC 的 IP 地址为 192.168.0.2/24。

Step 4 PC 的浏览器访问 http://192.168.0.1，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。

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

验证结果


Huawei
Eudemon200E-C
系统
面板
状态
配置
管理员
维护
高可靠性
虚拟防火墙
选择
设备资源信息
CPU
7
Memory
48
Flash
93
CPU使用率：7%
内存使用率：48%
Flash使用率：93%

3 防火墙基础配置

3.1 系统管理

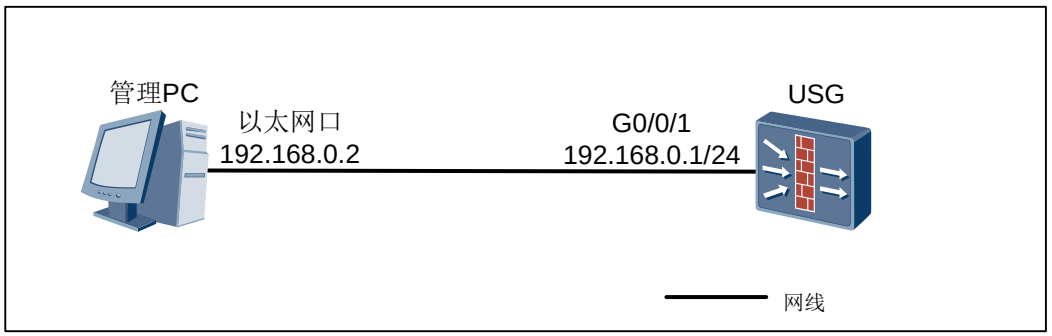
实验目的

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

组网设备

USG 防火墙一台，PC 机一台。

实验拓扑图



实验步骤（CLI）

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 Console,Telnet,SSH 等管理方式,登录到设备中。实验步骤参考 1.1-1.6（略）。

Step 3 配置设备主机名

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

Step 4 配置时间

```
<sysname>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。

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

开启信息中心。

```
[sysname]info-center enable
```

配置日志服务器 IP 地址和发送日志信息的源接口。

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

Step 7 配置 License

```
[sysname]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。

```
<sysname>system-view
[sysname]ftp server enable
Info:Start FTP server
[sysname]aaa
[sysname-aaa]local-user ftpuser password cipher Ftppass#
[sysname-aaa]local-user ftpuser service-type ftp
[sysname-aaa]local-user ftpuser level 3
[sysname-aaa]local-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 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
```

4 防火墙安全转发策略

4.1 基于IP地址的转发策略

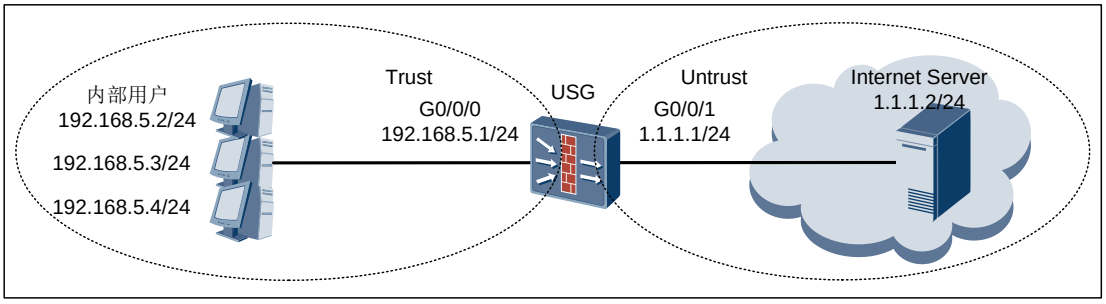
实验目的

介绍最基本的通过 IP 地址控制访问权限的举例。

组网设备

USG 防火墙一台，PC 机两台。

实验拓扑图



实验步骤 - CLI

Step 1 配置各个接口的 IP，并加入相应的安全区域。

```
<USG>system-view
[USG]interface GigabitEthernet 0/0/0
[USG-GigabitEthernet0/0/2]ip address 192.168.5.1 24
[USG-GigabitEthernet0/0/2]quit
[USG]interface GigabitEthernet 0/0/1
[USG-GigabitEthernet0/0/3]ip address 1.1.1.1 24
[USG-GigabitEthernet0/0/3]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]policy interzone trust untrust outbound
[USG-policy-interzone-trust-untrust-outbound]policy 0
[USG-policy-interzone-trust-untrust-outbound-0]policy source address-set
ip_deny
[USG-policy-interzone-trust-untrust-outbound-0]action deny
[USG-policy-interzone-trust-untrust-outbound-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-policy-interzone-trust-untrust-outbound]policy 1
[USG-policy-interzone-trust-untrust-outbound-1]policy source 192.168.5.0 mask
24
[USG-policy-interzone-trust-untrust-outbound-1]action permit
[USG-policy-interzone-trust-untrust-outbound-1]quit
[USG-policy-interzone-trust-untrust-outbound]quit
```

Step 5 关闭缺省包过滤。

```
[USG] firewall packet-filter default deny interzone trust untrust
```

思考：为何要将缺省包过滤关闭，如果不关闭会有怎样的结果。

验证结果

验证 192.168.5.2、192.168.5.3 和 192.168.5.6 这 3 台 PC 访问 Internet 是否被拒绝。
验证 192.168.5.0/24 中的其他 IP 地址是否可以正常访问 Internet。

5 网络地址转换实验

5.1 NAT Outbound实验

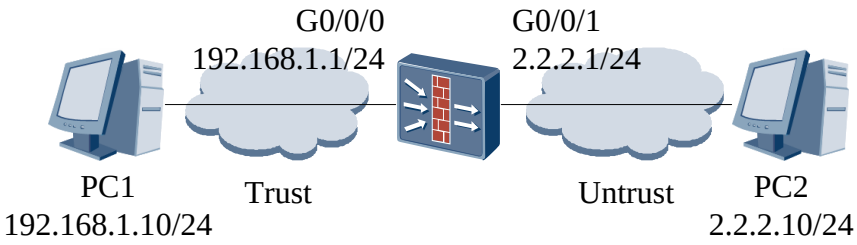
实验目的

通过本实验，你将了解 NAT outbound 的工作原理及详细配置。

组网设备

USG 防火墙一台，PC 机两台。

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 GE0/0/0 和 GE0/0/1 的 IP 地址。

```
[USG]interface GigabitEthernet 0/0/0
[USG-GigabitEthernet0/0/0]ip address 192.168.1.1 255.255.255.0
[USG-GigabitEthernet0/0/0]quit
[USG]interface GigabitEthernet 0/0/1
[USG-GigabitEthernet0/0/1]ip address 2.2.2.1 255.255.255.0
[USG-GigabitEthernet0/0/1]quit
[USG]
```

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 0/0/0
```

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

Step 4 配置域间包过滤策略。

```
[USG]policy interzone trust untrust outbound
[USG-policy-interzone-trust-untrust-outbound-0]policy 0
[USG-policy-interzone-trust-untrust-outbound-0]action permit
[USG-policy-interzone-trust-untrust-outbound-0]policy source 192.168.1.0 mask
24
```

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 2.2.2.2 2.2.2.5
```

Step 6 配置 NAT policy。

```
[USG]nat-policy interzone trust untrust outbound
[USG-nat-policy-interzone-trust-untrust-outbound]policy 1
[USG-nat-policy-interzone-trust-untrust-outbound-1]action source-nat
[USG-nat-policy-interzone-trust-untrust-outbound-1]policy destination 2.2.2.10 0
.0.0.255
[USG-nat-policy-interzone-trust-untrust-outbound-1]address-group 1
[USG-nat-policy-interzone-trust-untrust-outbound-1]policy source 192.168.1.10
0.0.0.255
[USG-nat-policy-interzone-trust-untrust-outbound-1]quit
[USG-nat-policy-interzone-trust-untrust-outbound]quit
```

验证结果

查看 nat-policy 配置

```
[USG]dis nat-policy interzone trust untrust outbound
nat-policy interzone trust untrust outbound
 policy 1 (0 times matched)
   action source-nat
   policy service service-set ip
   policy source 192.168.1.0 0.0.0.255
   policy destination 2.2.2.0 0.0.0.255
   address-group 1
```

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]dis 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 & NAT Inbound实验

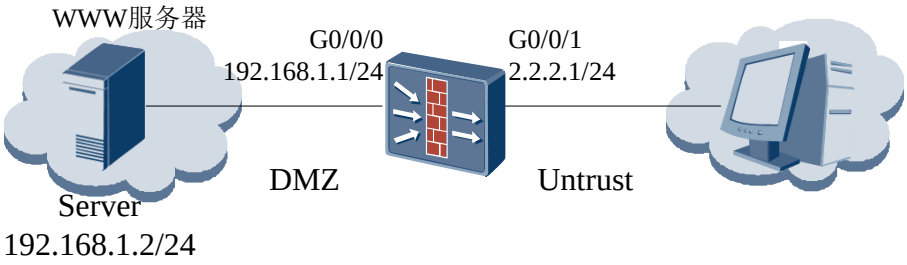
实验目的

学会配置 NAT Server 和 NAT inbound.

组网设备

USG 防火墙一台，PC 机一台，服务器一台。

实验拓扑图



实验步骤 - CLI

Step 1 设置 server 地址和 PC 地址。

Step 2 设置防火墙 GE0/0/0 和 GE0/0/1 的 IP 地址。

```
[USG]interface GigabitEthernet 0/0/0
[USG-GigabitEthernet0/0/0]ip address 192.168.1.1 255.255.255.0
[USG-GigabitEthernet0/0/0]quit
[USG]interface GigabitEthernet 0/0/1
[USG-GigabitEthernet0/0/1]ip address 2.2.2.1 255.255.255.0
[USG-GigabitEthernet0/0/1]quit
[USG]
```

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

Step 4 配置域间包过滤策略。

```
[USG]policy interzone dmz untrust inbound
[USG-policy-interzone-dmz-untrust-inbound]policy 0
```

```
[USG-policy-interzone-dmz-untrust-inbound-0]policy destination 192.168.1.2
0.0.0.255
[USG-policy-interzone-dmz-untrust-inbound-0]policy service service-set ftp
[USG-policy-interzone-dmz-untrust-inbound-0]action permit
```

Step 5 配置 NAT server。

```
[USG] nat server 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 1 192.168.1.10 192.168.1.20
```

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。

```
[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 1 进行绑定。

```
[USG] nat-policy interzone dmz untrust inbound
[USG-nat-policy-interzone-dmz-untrust-inbound] policy 0
[USG-nat-policy-interzone-dmz-untrust-inbound-0] policy source 2.2.2.0
0.0.0.255
[USG-nat-policy-interzone-dmz-untrust-inbound-0] action source-nat
[USG-nat-policy-interzone-dmz-untrust-inbound-0] address-group 1
[USG-nat-policy-interzone-dmz-untrust-inbound-0] quit
[USG-nat-policy-interzone-dmz-untrust-inbound] quit
```

验证结果

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

```
[USG]dis nat server
Server in private network information:
 id                  : 0
 zone                : ---
 interface           : ---
 global-start-addr : 2.2.2.4              global-end-addr    : ---
 inside-start-addr : 192.168.1.20         inside-end-addr    : ---
 global-start-port : ---                  global-end-port    : ---
 insideport          : ---
 globalvpn           : public             insidevpn          : public
 protocol            : ---                vrrp               : ---
```

```
no-reverse              : no

  Total     1 NAT servers
```

5.3 双出口NAT实验(基于zone的NATserver+双出口)

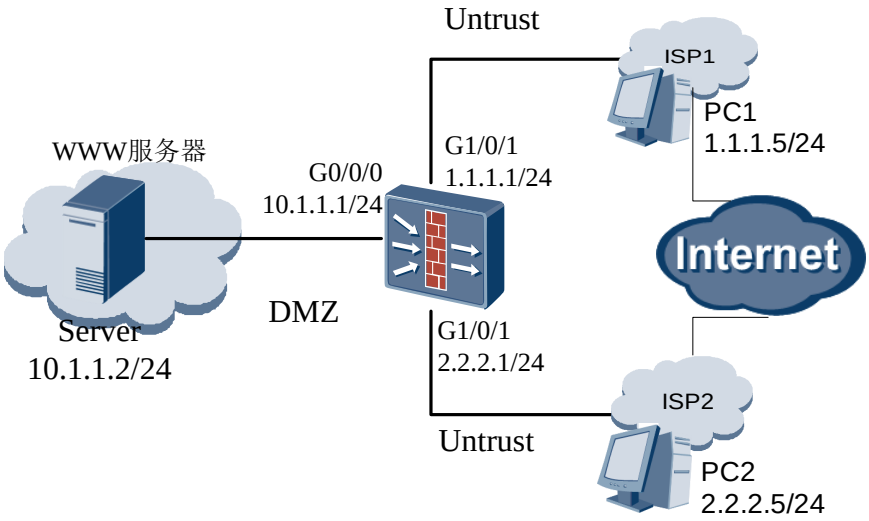
实验目的

学会配置双出口 NAT.学会配置基于 zone 的 NAT server。

组网设备

WWW server 一台，PC 机两台，USG 防火墙一台。

实验拓扑图



实验步骤 -CLI

Step 1 配置 PC1、PC2 和 WWW 服务器的 IP 地址。具体步骤省略。

Step 2 配置防火墙接口地址。

```
[USG]interface GigabitEthernet 0/0/0
[USG-GigabitEthernet0/0/0]ip address 10.1.1.1 255.255.255.0
[USG-GigabitEthernet0/0/0]quit
[USG]interface GigabitEthernet 0/0/1
[USG-GigabitEthernet0/0/1]ip address 1.1.1.1 255.255.255.0
[USG-GigabitEthernet0/0/1]quit
[USG]interface GigabitEthernet 0/0/2
[USG-GigabitEthernet0/0/2]ip address 2.2.2.1 255.255.255.0
[USG-GigabitEthernet0/0/2]quit
[USG]firewall zone dmz
```

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

Step 3 创建两个新的安全区域并将 GE0/0/1 和 GE0/0/2 加入相应的安全区域。

```
[USG]firewall zone name ISP1
[USG-zone-isp1]set priority 10
[USG-zone-isp1]add int GigabitEthernet 0/0/1
[USG-zone-isp1]quit
[USG]firewall zone name ISP2
[USG-zone-isp2]set priority 15
[USG-zone-isp2]add int GigabitEthernet 0/0/2
[USG-zone-isp2]quit
```

Step 4 配置相应的域间包过滤策略。

```
[USG] policy interzone dmz isp1 inbound
[USG-policy-interzone-dmz-isp1-inbound] policy 0
[USG-policy-interzone-dmz-isp1-inbound-0] policy destination 10.1.1.2 0
[USG-policy-interzone-dmz-isp1-inbound-0] policy service service-set http
[USG-policy-interzone-dmz-isp1-inbound-0] action permit
[USG-policy-interzone-dmz-isp1-inbound-0] quit
[USG-policy-interzone-dmz-isp1-inbound] quit
[USG] policy interzone dmz isp2 inbound
[USG-policy-interzone-dmz-isp2-inbound] policy 0
[USG-policy-interzone-dmz-isp2-inbound-0] policy destination 10.1.1.2 0
[USG-policy-interzone-dmz-isp2-inbound-0] policy service service-set http
[USG-policy-interzone-dmz-isp2-inbound-0] action permit
[USG-policy-interzone-dmz-isp2-inbound-0] quit
[USG-policy-interzone-dmz-isp2-inbound] quit
```

Step 5 配置内部服务器，对不同的安全区域发布不同的公网 IP 地址。

```
[USG] nat server zone isp1 protocol tcp global 1.1.1.2 inside 10.1.1.2
[USG] nat server zone isp2 protocol tcp global 2.2.2.2 inside 10.1.1.2
```

验证结果

查看 NAT Server.

```
[USG]display nat server
Server in private network information:
 id                    : 0
 zone                  : isp1
 interface             : ---
 global-start-addr : 1.1.1.2                  global-end-addr     : ---
```

```
inside-start-addr : 10.1.1.2                inside-end-addr    : ---
global-start-port : 0(any)                  global-end-port    : ---
insideport             : 0(any)
globalvpn              : public             insidevpn          : public
protocol               : tcp                vrrp               : ---
no-reverse             : no

id                     : 1
zone                   : isp2
interface              : ---
global-start-addr : 2.2.2.2                 global-end-addr    : ---
inside-start-addr : 10.1.1.2                inside-end-addr    : ---
global-start-port : 0(any)                  global-end-port    : ---
insideport             : 0(any)
globalvpn              : public             insidevpn          : public
protocol               : tcp                vrrp               : ---
no-reverse             : no
Total     2 NAT servers
```

使用 display firewall session table 查看 nat server 转换情况：

```
[USG]dis firewall session table
09:29:38    2013/05/22
 Current Total Sessions : 11
   icmp    VPN:public --> public 10.1.1.1:52651-->10.1.1.2:2048
   icmp    VPN:public --> public 1.1.1.1:52907-->1.1.1.2:2048
   icmp    VPN:public --> public 2.2.2.1:53163-->2.2.2.2:2048
   icmp    VPN:public --> public 2.2.2.2:256-->10.1.1.2:2048
   icmp    VPN:public --> public 1.1.1.2:256-->10.1.1.2:2048
   http    VPN:public --> public 1.1.1.2:2053-->10.1.1.2:80
   http    VPN:public --> public 2.2.2.2:2050-->10.1.1.2:80
   http    VPN:public --> public 2.2.2.2:2051-->10.1.1.2:80
   http    VPN:public --> public 2.2.2.2:2052-->10.1.1.2:80
   http    VPN:public --> public 2.2.2.2:2053-->10.1.1.2:80
   http    VPN:public --> public 1.1.1.2:2054-->10.1.1.2:80
```

6 防火墙双机热备实验

6.1 防火墙双机热备实验

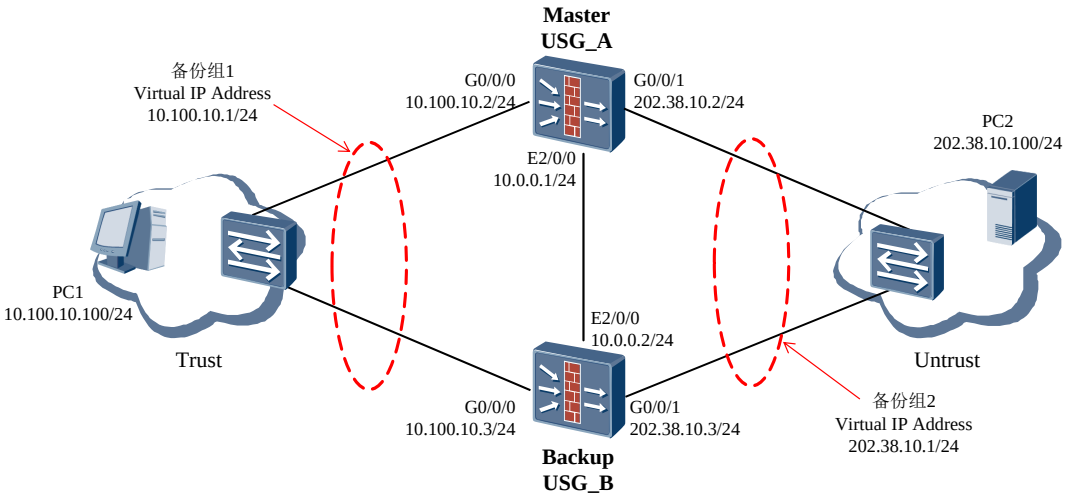
实验目的

熟悉通过命令行和 web 方式配置防火墙双机热备，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、USG_B 以主备备份方式工作，且上下行业务接口工作在三层。

组网设备

1. 两台同型号的 USG2200 或两台同型号的 USG5000 防火墙，2 台交换机，两台 PC
2. 防火墙至少有三个业务接口

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 0/0/0
[USG_A-GigabitEthernet0/0/0] ip address 10.100.10.2 24
[USG_A-GigabitEthernet0/0/0] quit
[USG_A] interface GigabitEthernet 0/0/1
```

```
[USG_A-GigabitEthernet0/0/3] ip address 202.38.10.2 24
[USG_A-GigabitEthernet0/0/3] quit
[USG_A] firewall zone trust
[USG_A-zone-trust] add interface GigabitEthernet 0/0/0
[USG_A-zone-trust] quit
[USG_A] firewall zone untrust
[USG_A-zone-untrust] add interface GigabitEthernet 0/0/1
[USG_A-zone-untrust] quit
```

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

```
[USG_A] interface GigabitEthernet 0/0/0
[USG_A-GigabitEthernet0/0/1] vrrp vrid 1 virtual-ip 10.100.10.1 master
[USG_A-GigabitEthernet0/0/1] vrrp virtual-mac enable
[USG_A-GigabitEthernet0/0/1] quit
```

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

```
[USG_A] interface GigabitEthernet 0/0/1
[USG_A-GigabitEthernet0/0/3] vrrp vrid 2 virtual-ip 202.38.10.1 master
[USG_A-GigabitEthernet0/0/3] vrrp virtual-mac enable
[USG_A-GigabitEthernet0/0/3] quit
```

Step 2 配置心跳线与防火墙之间的安全策略。

```
[USG] firewall packet-filter default permit interzone local dmz
```

Step 3 完成 USG_A 的心跳线配置。

配置 Ethernet2/0/0 的 IP 地址。

```
[USG_A] interface Ethernet2/0/0
[USG_A-GigabitEthernet0/0/2] ip address 10.0.0.1 24
[USG_A-GigabitEthernet0/0/2] quit
```

配置 Ethernet2/0/0 加入 DMZ 区域。

```
[USG_A] firewall zone dmz
[USG_A-zone-dmz] add interface Ethernet2/0/0
[USG_A-zone-dmz] quit
```

指定 Ethernet2/0/0 为心跳口。

```
[USG_A] hrp interface Ethernet2/0/0
```

Step 4 启用 HRP 备份功能。

```
[USG_A] hrp enable
```

Step 5 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_M[USG_A] policy interzone trust untrust outbound
```

```
HRP_M[USG_A-policy-interzone-trust-untrust-outbound] policy 1
HRP_M[USG_A-policy-interzone-trust-untrust-outbound-1] policy source
10.100.10.0 0.0.0.255
HRP_M[USG_A-policy-interzone-trust-untrust-outbound-1] action permit
HRP_M[USG_A-policy-interzone-trust-untrust-outbound-1] quit

HRP_M[USG_A-policy-interzone-trust-untrust-outbound] quit
```

Step 6 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 GigabitEthernet0/0/0 和 GigabitEthernet0/0/1 加入状态为 Slave 的 VGMP 管理组。

Step 7 配置 Switch。

分别将两台 Switch 的三个接口加入同一个 VLAN，具体配置命令请参考交换机的相关文档。

Step 8 配置静态路由。

在内网中的 PC 上配置静态路由，将 VRRP 备份组的虚拟 IP 地址作为到达其他网段的下一跳地址。

实验结果

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_M<USG_A>dis vrrp
16:12:02   2013/06/08
  GigabitEthernet0/0/1 | Virtual Router 2
    VRRP Group : Master
    state : Master
    Virtual IP : 202.38.10.1
    Virtual MAC : 0000-5e00-0102
    Primary IP : 202.38.10.2
    PriorityRun : 120
    PriorityConfig : 100
    MasterPriority : 120
    Preempt : YES     Delay Time : 0
    Advertisement Timer : 1
    Auth Type : NONE
    Check TTL : YES
```

```
GigabitEthernet0/0/0 | Virtual Router 1
    VRRP Group : Master
    state : Master
    Virtual IP : 10.100.10.1
    Virtual MAC : 0000-5e00-0101
    Primary IP : 10.100.10.2
    PriorityRun : 120
    PriorityConfig : 100
    MasterPriority : 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_M<USG_A>dis hrp state
16:15:31   2013/06/08
 The firewall's config state is: MASTER

 Current state of virtual routers configured as master:
                GigabitEthernet0/0/1      vrid     2 : master
                GigabitEthernet0/0/0      vrid     1 : master
```

在处于 Trust 区域的 PC1 端 ping VRRP 组 1 的虚拟 IP 地址 10.100.10.1，在 USG_A 上检查会话。

```
HRP_M<USG_A>display firewall session table
16:17:36   2013/06/08
 Current Total Sessions : 1
  icmp    VPN:public --> public 10.100.10.100:1-->10.100.10.1:2048
```

可以看出 VRRP 组配置正确后，在 PC1 端能够 ping 通 VRRP 组 1 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_M<USG_A>display firewall session table
16:19:42   2013/06/08
 Current Total Sessions : 1
  icmp    VPN:public --> public 10.100.10.100:1-->202.38.10.100:2048


HRP_S<USG_B>display firewall session table
16:03:19   2013/06/08
 Current Total Sessions : 1
```

```
  icmp    VPN:public --> public      Remote 10.100.10.100:1-->202.38.10.100:2048
```

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 202.38.10.100 –t ,然后将 USG_A 防火墙 G0/0/0 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 G0/0/0 接口网线恢复，观察防火墙状态切换及 ping 包丢包情况。