防火墙/SD-WAN

命令行手册

手册版本　V5.0

产品版本　V2.6.5.0

资料状态　发行

目录

1 系统管理

系统管理是对系统进行管理维护的一种重要手段，通过系统管理可以了解设备的基本用法，比如怎样对设备进行管理，如何上传下载配置文件，如何升级系统，以及如何获得帮助等。

1.1 TSOS操作系统概述

TSOS 是防火墙/SD-WAN 设备使用的操作系统。可以通过命令行配置，也可以通过图形界面进行配置。其中命令行配置除了可以通过 console 口连接，也可以通过 SSH，Telnet 客户端连接，图形界面采用的 B/S 模式，可以通过 HTTPS 和 HTTP 进行连接。本手册只介绍通过命令行的方式进行配置管理。

1.1.1 命令行特性

这一节主要讲述当您进入命令行进行配置时所要进行的步骤。请仔细阅读本节以及后边几节中关于使用命令行接口的详细信息。

使用命令行接口（CLI），请按照以下步骤：

第 1 步：当进入命令行接口出现命令提示符后，请确认您有相应的权限。大多数配置命令都需要用户您有管理员权限。

第 2 步：键入命令名称。


注意

TSOS 命令行中的所有命令和关键字都是小写。

如果命令不含需要用户输入的参数，那么请直接跳到第 3 步。如果命令含需要用户输入的参数，那么继续以下步骤：

1）如果命令需要一个参数值，请输入一个参数值。在输入参数值时，可能要输入关键字。

2）命令的参数值部分一般指定了您应该输入什么样的参数，是某范围内的数值，或者字符串或者 IP 地址。关键字是指命令中要操作的对象。

3）如果命令需要多个参数值，请按命令的提示依次输入关键字和每个参数值。直到提示信息中出现让您按回车键信息为止。

第 3 步：输入完整的命令后，请按回车键。

例如：

“exit” 是一个不含参数和关键字的命令。命令名称为 exit；

“ip address A.B.C.D/M” 是一个含有参数和关键字的命令。其中命令名称为 ip，关键字为 address，参数值为 A.B.C.D/M。

1.1.2 语法帮助

命令行接口内置有语法帮助。如果您对某个命令的语法不是很确定，请输入该命令中您所知道的部分，然后输入“?”或“空格加 ？”。命令行会提示您已经输入的部分命令后剩余部分的可能的命令清单。

1.1.3 使用语法帮助补齐命令

TSOS 提供用户输入“Tab”键后，对命令进行补齐的功能。当您输入了一部分命令后，再输入“Tab”键，如果匹配的命令有多个，则列出可能的命令清单，如果匹配的命令只有一个，那么命令行会自动把用户输入的那部分命令补齐，并把光标移至最后。

1.1.4 命令中的符号

您可能会在命令语法中看到各种符号，这些符号只是说明您该如何输入该命令，但是不是命令本身的一个部分。下表对这些符号进行了概要说明。

表 1-1 命令行中的符号

符号	描述
大写字母	大写字母表示该命令的该部分必须输入一个字符串参数。例如命令： usergroup NAME firewall 中您必须在NAME那个位置输入一个合法的用户组的名字作为您所创建的用户组的名字。
A.B.C.D和A.B.C.D/M	A.B.C.D表示IP地址，M表示掩码。例如命令： ip route A.B.C.D/M (A.B.C.D|INTERFACE)
圆括号 ( )和竖直线 |	圆括号一般和竖直线配合使用。圆括号括起来的部分表示这部分命令有几个用竖直线分隔开的可选项，您必须选择输入其中一项。 例如命令： timezone (utc|cst) 中圆括号内包含由竖直线分隔的两个可选项，您必须输入utc 和cst其中的一个。
中括号 [ ]	中括号表示里面的参数可输入或可不输入。 例如命令： show access-user [USERNAME] 中第二个参数如果输入表示有要显示指定用户名称的接入用户信息，如果不输入表示显示所有接入用户的信息
尖括号和数值范围	尖括号和数值范围表示输入的参数的取值范围在那两个数值之间的某个数。 例如命令：policy <1-5000> 中配置到设备上的策略ID可以是1至5000中的任何一个。

1.1.5 命令简写

命令简写是指您可以只输入命令单词或关键字的前边部分字母，只要那部分字母不会造成歧义，就可以直接回车执行该命令。但需要用户输入的参数如 PPPoE 模板的名字等，要完整输入。例如：

```
ip address 192.168.1.1/16
```

可以简写成：`ip add 192.168.1.1/16`

注意

当使用命令简写时，您必须输入足够多的字母，以确保在众多命令中不会造成歧义。

1.1.6 命令模式

设备支持丰富的命令模式，下表列出了所有的命令模式。

表 1-2 设备支持的所有命令模式

命令模式	提示符	进入方法
普通模式	FW>	系统引导起来后，输入密码
特权模式	FW #	在普通模式下输入密码
全局配置模式	FW (config)#	在特权模式下输入 configure terminal
以太网接口配置模式	FW (config-ge1/0)#	在全局配置模式下输入 interface IFNAME，例如：interface ge1/0
VLAN配置模式	FW (config-vlan1000)#	在配置模式下输入 interface VLANNAME

1.1.7 常用命令介绍

表 1-3 普通模式下的常用命令介绍

命令	描述
enable	进入特权模式，可以对设备进行配置和写操作
exit	退出当前模式，返回到上一级模式。
ping -c <1-10000> -s <0-65507> -w <0-10> WORD	网络连通性基本检测工具，WORD为对方主机地址。-c表示ping包的个数，-s表示包的大小，-w是等待相应的时间。
list	显示当前模式下可用的命令
show running-config	显示当前的配置信息（可以是没有保存的）
show startup-config	显示已经保存的启动配置信息
show version	显示版本信息

1.2 实现系统配置的途径

您可以通过以下途径对设备进行管理：

- 使用终端（或者仿终端软件）连接到设备的串口（Console）从而访问设备的命令行接口（CLI）
- 使用 Telnet 管理设备
- 使用 SSH 管理设备
- 通过 Web 进行管理

1.2.1 通过串口实现系统配置

- 波特率 ：9600
- 数据位 ：8
- 奇偶校验 ：无
- 停止位 ：1

- 流量控制 ：无

正确设置完 Console 的参数并将设备加电，可以看到设备的登录提示信息。

1.2.2 通过Telnet实现系统配置

任何一个有 Telnet 功能的工作站都能通过 TCP/IP 网络连接到设备。可以通过以下步骤 Telnet 登录到设备：

通过 Console 口用管理员用户的帐号登录到设备。进入接口配置模式。

然后给设备某个接口配置 IP 地址。给接口配置 IP 地址可以使用以下命令：

ip address A.B.C.D/M

配置接口允许 Telnet 登录，可以使用下面的命令：

allow access telnet

此后可以从该接口上以该接口的 IP 地址 Telnet 登录到设备命令行接口。

1.2.3 通过SSH方式实现系统配置

网络被攻击，很多情况是由于服务器提供了 Telnet 服务引起的。Telnet 服务有一个致命的弱点——它以明文的方式传输用户名及口令，所以，很容易被别有用心的人窃取口令。目前，一种有效代替 Telnet 服务的有用工具就是 SSH 服务。SSH 客户端与服务器端通讯时，用户名及口令均进行了加密，有效防止了对口令的窃听。设备支持以 SSH 的方式对设备的管理。

任何一个有 SSH 功能的工作站都能通过 TCP/IP 网络连接到设备。可以通过以下步骤登录到设备：

通过 Console 口用管理员用户的帐号登录到设备。进入接口配置模式。

然后给设备某个接口配置 IP 地址。给接口配置 IP 地址可以使用以下命令：

ip address A.B.C.D/M

配置接口允许 SSH 登录，可以使用下面的命令：

allow access ssh

此后可以从该接口上以该接口的 IP 地址通过 SSH 命令登录到设备命令行接口。

1.3 系统文件管理

系统文件的管理是指对于配置文件、系统应用程序文件的维护和管理。对于系统文件的管理，在没有特别指明的时候，都是在特权模式下操作。

1.3.1 copy命令使用

copy 命令的格式如下：

copy tftp A.B.C.D RemoteFile (version|config| license| applib)

具体参数解释如下

version ： 表示更新版本文件

config ： 表示配置文件

license ： 表示授权文件

applib ： 表示特征库文件

1.3.2 保存配置文件

每一次修改了设备的配置后，必须将配置保存到设备中，重新启动后，配置才能保持不变。

配置文件保存的步骤如下所述：

方法 1：

步骤1	write memory	将配置文件保存到系统中

方法 2：

步骤1	write file	将配置文件保存到系统中

1）以上两个命令作用相同，都实现保存配置文件的功能。

2）startup-config 表示系统启动时的配置项，而 running-config 表示系统启动后当前的配置项，操作员更改后的配置项反映在 running-config 中，系统刚启动时，running-config 就是 startup-config。

1.3.3 多配置文件

多配置文件备份步骤如下所述：

步骤1	copy (running-config|startup-config) backup-config	将运行配置或者启动配置备份

为配置文件添加描述信息：

步骤1	write (startup-config|backup-config) (default|<0-9>) description .DESCRIPTION	为配置文件添加描述信息

将某一个配置文件作为下次启动的配置:

步骤1	Copy backup-config startup-config	将某一个配置文件作为下次启动的配置:

1.3.4 配置文件的上传与下载

用户还可以把一份好的配置文件保存到文本文件中，在需要的时候（例如不小心把设备配置搞乱了，不知道怎样把配置恢复到以前的状态时）再把配置文件下载到设备中。通过使用下面的命令完成配置文件的下载：

copy tftp A.B.C.D RemoteFile config

配置导出的命令：

copy (running-config|startup-config) tftp A.B.C.D RemoteFile

1.3.5 系统升级

用户还可以把一份版本文件下载到设备中。通过使用下面的命令完成系统文件的下载：

copy tftp A.B.C.D RemoteFile version

1.4 常用系统管理命令

1.4.1 开启Telnet服务

开启 Telnet 服务的步骤：

步骤1	allow access telnet	开启Telnet服务，执行该命令后将允许其他机器Telnet到设备

1.4.2 开启SSH服务

开启 SSH 服务的步骤：

步骤1	allow access ssh	开启SSH服务，执行该命令后将允许其他机器SSH到设备

1.4.3 查看谁在系统上

who 命令显示当前有哪些操作员登录进系统。

1.4.4 清除登录用户

如果有多个操作员登录进系统，而有些操作员出现了异常，某个管理员可以把其他管理员踢出系统，可以通过 clear user 命令完成这个功能。

操作步骤：

步骤1	clear user USERNAME address A.B.C.D time TIME	根据输入的用户名，地址，时间清除对应的用户。

1.4.5 查看系统的版本

show version 命令可以查看系统的版本信息，包括所有物理接口，以及接口的 MAC 地址，系统的版本信息。例如：

```
FW# show version
Serial number: 00100000000000001308065216
TBOS                          : V0206R0100B20161209
Compile time                  : Dec  9 2016 15:00:24
Copyright 2013-2017 Networks Corp.

mgt:     e1000e v2.1.4-NAPI MAC address: 00:e0:4c:08:2e:68
ge0/0:   e1000e v2.1.4-NAPI MAC address: 00:e0:4c:08:2e:6a
ge0/1:   e1000e v2.1.4-NAPI MAC address: 00:e0:4c:08:2e:6b
ge0/2:   e1000e v2.1.4-NAPI MAC address: 00:e0:4c:08:2e:69
```

ge0/3: e1000e v2.1.4-NAPI MAC address: 00:e0:4c:08:2e:6c

2 系统的引导

软件系统的引导依靠一个独立的软件模块，称之为 bootLoader。bootLoader 包含以下两个功能：

1. 系统硬件的初始化和软件系统的引导。
2. 系统版本的下载升级。

2.1 bootLoader概述

bootLoader 环境是一个包含初始化过程和系统引导以及版本下载功能的独立软件模块。一般来说，当设备的系统软件由于故障无法启动的情况下，可以进入该软件环境进行系统的升级和修复。在一般正常的情况下，无需进入该软件环境。

该模块属于高级功能，一般用户请谨慎使用该模块。

2.2 配置bootLoader

2.2.1 进入bootLoader

如果需要进入 bootLoader 环境，要将 console 电缆接到 PC 机的 COM 口，并设置 PC 机超级终端的参数为：波特率 9600，数据位 8，停止位 1，流控无。

启动设备，超级终端会打印：

Press Ctrl+c to stop auto-boot.

3 seconds left.

此时按 Ctrl+c 可以进入 bootLoader 环境，如果 3 秒钟内没有任何输入，则会自动启动系统软件。按 Ctrl+c 后，系统会进入如下环境：

```
********************************************************************************
*                                                                              *
*                          BOOT MENU:                                          *
*   1. Configure network parameters.                                           *
*   2. Download version image by ethernet port to disk.                        *
*   3. Download version image by serial port to disk.                          *
*   4. Download version image from USB device to disk.                         *
*   5. Misc functions.                                                         *
*   6.Reboot.                                                                  *
*                                                                              *
********************************************************************************
```

2.2.2 bootLoader功能1 配置网络参数

该功能用于，通过网口下载软件版本时所需的网络参数。缺省的网络参数见表 2-1

表2-1 设备下载网口的缺省设置信息

内容	缺省设置	备注
下载网口	eth0	不能更改设置
系统软件的文件名 (Startup image)	tsos.bin	可更改设置
本地IP地址 (Startup local)	192.168.1.176	可更改设置
本地IP地址掩码 (Startup mask)	24	可更改设置
服务器IP地址 (Startup server)	192.168.31.177	可更改设置
网关IP地址 (Startup gateway)	192.168.31.1	可更改设置

下载版本需要做的准备工作有，将存有版本文件的 PC 机的网口和设备的下载网口（下载网口见表 2-1 ）相连；在 PC 机上启动 TFTP server 软件并指向版本文件。

配置网络参数通过 bootLoader 菜单的功能
1. Configure network parameters.
来实现，选择 1 配置网络参数：

```
Please input your choice:1
Do you want to edit startup script - continue (y/n)? y
Startup image: tsos.bin
Startup local: 192.168.31.176
Startup mask: 24
Startup server: 192.168.31.177
Startup gateway: 192.168.1.1
Are you sure to store the parameters above - continue (y/n)? Y
```

上述参数的含义如下：

Startup gateway：如果 PC 机和设备直连或处在一个局域网内，可不需要配置此参数（建议采取这种模式）。如果 PC 机和设备处在不同的局域网内，这个地址用来设置设备的网关地址。

Startup local：下载版本时设备所使用的 IP 地址。

Startup mask：下载版本时设备所使用的 IP 地址掩码。

Startup server：PC 机的 IP 地址。

Startup image：版本文件文件名。

2.2.3 bootLoader功能2 网络下载版本

在**错误!未找到引用源。**所描述的网络参数设置正确的情况下，选择
2. Download version image by ethernet port to disk.
可以将版本文件下载并安装到设备的磁盘中。下载和安装信息如下：

Downloading tsos.bin.....

Download success, vsos.bin length:26800640

Begain to install files.....

Install /boot/kernel.img.....success!

Install /boot/rootfs.img.....success!

Install /boot/sign_rul.gz.....success!

Install /boot/security.gz.....success!

Install /boot/av_lib.gz.....success!

Install /boot/ips_ver.....success!

Install /boot/av_ver.....success!

Finish to install version file!

下载完毕后重启设备，系统就可以进入更新后的 VSOS 版本。

2.2.4 bootLoader功能3 串口下载版本

串口下载版本指通过 console 口使用 XMODEM 协议下载版本文件。请选择
3. Download version image by serial port to disk.
例如：

Please input your choice:4

Please change baudrate to 115200 and transfer file by XMODEM protocol.

看到上述提示后，请将 windows 超级终端的波特率设置为 115200（为了加快下载速度），并重新连接，然后用超级终端的“发送文件”按钮，选择 XMODEM 协议，选择正确的版本文件，并按发送。文件传输即开始。

文件传输结束，系统会打印：

Download complete, please change baudrate to 9600.

看到上述提示后，请将 windows 超级终端的波特率设置为 9600。

下载完毕后重启设备，系统就可以进入更新后的软件版本。

2.2.5 bootLoader功能4 USB下载版本

设备插入 U 盘并启动后，可以在 bootLoader 菜单中选择
4. Download version image from USB device to disk.
注意 U 盘中必须存储有版本文件 tsos.bin。系统会把版本文件从 U 盘中读出并存储到本地磁盘中。

下载完毕后重启设备，系统就可以进入更新后的软件版本。

2.2.6 bootLoader功能5 杂项功能

选择
5. Misc functions.
会进入杂项功能子菜单，系统会打印出子菜单选项：

```
************************************************************
*                                                          *
*              MISC FUNCTIONS MENU:                        *
*   1. Clear current configure file.                       *
*   2. Recover backup configure file.                      *
*   3. Modify system clock.                                *
*   4. Reset administrator passowrd.                       *
*   5. Fix CF card file system (EXT2)                      *
*   6. Fix hard disk file system (EXT2/EXT3)               *
*   7. Exit.                                               *
*                                                          *
************************************************************
```

各个选项功能如下：

1.Clear current configure file.

清除当前系统的配置文件，该操作无法恢复，请谨慎使用！

2.Recover backup configure file.

将当前配置文件恢复为备份配置，该操作无法恢复，请谨慎使用！

3.Modify system clock.

修改硬件系统时钟。选择该选项，系统会逐一提示，如下所示：

```
Do you want to Modify system clock - continue (y/n)? y
 Year:    2008
 Month:   2
 Day:     20
 Hour:    6
 Minute:  39
 Second:  17
Current time: 2008/02/20 06:39:17. Are you sure - continue (y/n)? y
```

确认后，系统时间被修改。

4.Reset administrator passowrd.

该选项可在下次启动时将管理员口令恢复为缺省口令，该功能只在下一次启动生效，再次启动还是需要输入合法的管理员口令。

5.Fix CF card file system (EXT2)

该选项检查并修复 CF 卡的文件系统。

6.Fix hard disk file system (EXT2/EXT3)

该选项检查并修复硬盘的文件系统。

7.Exit.

该项退回到上一级菜单。

2.2.7 bootLoader功能6 重启设备

选择
6.Reboot
可以重启设备。

3 系统监控

3.1 概述

系统监控是指监控系统某一资源，当其情况到达指定阈值后，进行告警。

3.2 系统监控

系统监控是指监控系统 CPU、内存、温度和连接数资源，当其情况到达指定阈值后，进行告警。

3.2.1 配置监控CPU利用率

监控步骤：

步骤1	查看系统当前cpu使用状况
	FW# show cpu usage Core 1Min 5Min 15Min BOS 0.07% 0.10% 0.10% App1 0.85% 0.86% 0.86%
步骤2	查看当前cpu监控值
	FW# show sysmon monitor cpu sysres cpu 90
步骤3	进入监控配置节点
	FW(config)# sysmon
步骤4	配置监控系统CPU利用率
	FW(sysmon)# sysres cpu 85 表示配置系统 CPU 利用率阈值为 85%，系统默认监控阈值为 90%。
步骤5	取消用户自己配置的cpu监控值，恢复系统默认值
	FW(sysmon)# no sysres cpu 表示取消用户自己配置的CPU监控阈值，恢复系统默认监控阈值90%。

3.2.2 配置监控内存利用率

监控步骤：

步骤1	查看系统当前内存使用状况
	FW# show memory Memory total : 3903 MB memory free : 950 MB Shared memory Total: 2046 MB Shared Used: 563 MB Total Hugepages: 1023 Free Hugepages: 731 FW# show memory usage BOS Mem Usage : 48.79% Shared Mem Usage: 27.545% (563 MB)
步骤2	查看当前内存监控值

	FW# show sysmon monitor memory sysres memory 90
步骤3	进入监控配置节点
	FW(config)# sysmon
步骤4	配置监控系统内存利用率
	FW(sysmon)# sysres memory 85 表示配置系统内存利用率监控阈值为 85%,系统默认监控阈值为 90%
步骤5	取消用户自己配置的内存监控值，恢复系统默认值
	FW(sysmon)# no sysres memory 表示取消用户自己配置的memory监控阈值，恢复系统默认监控阈值90%。

3.2.3 配置监控CPU温度

监控步骤：

步骤1	查看系统当前cpu温度阈值
	FW# show sysmon monitor cpu_temperature sysres cpu_temperature 90
步骤2	进入监控配置节点
	FW(config)# sysmon
步骤3	配置监控系统CPU温度阈值
	FW(sysmon)# sysres cpu_temperature 80 表示配置设备 CPU 温度用阈值为 80，系统默认值为 90
步骤4	取消用户自己配置的cpu温度监控值，恢复系统默认值
	FW(sysmon)# no sysres cpu_temperature 表示取消用户自己配置的CPU温度监控阈值，恢复系统默认监控阈值90。

3.2.4 配置监控系统连接数

监控步骤：

步骤1	查看系统当前连接数监控阈值
	FW# show sysmon monitor session sysres session 10000
步骤2	进入监控配置节点
	FW(config)# sysmon
步骤3	配置监控系统连接数
	FW(sysmon)# sysres session 20000 表示配置系统连接数监控阈值为 20000 条,系统默认监控阈值为 10000
步骤4	取消用户自己配置的系统连接数监控值，恢复系统默认值
	FW(sysmon)# no sysres session 表示取消用户自己配置的系统连接数监控阈值，恢复系统默认监控阈值10000。

3.3 流量监控

3.3.1 配置流量监控

监控步骤：

步骤1	进入监控配置节点
	FW(config)# sysmon
步骤2	配置流量监控

	FW(sysmon)# sysres flow 1024000 表示配置流量监控，如果系统流量大于 1024000 则告警。
步骤3	取消流量监控
	FW(sysmon)# no sysres flow

3.4 报文监控

3.4.1 配置报文监控

监控步骤：

步骤1	进入监控配置节点
	FW(config)# sysmon
步骤2	配置报文监控
	FW(sysmon)# sysres packet 1000 表示配置报文监控，如果系统报文占用空间大于 1000 则告警。
步骤3	取消报文监控
	FW(sysmon)# no sysres packet

3.5 NAT连接数监控

3.5.1 配置NAT连接数监控

监控步骤：

步骤1	进入监控配置节点
	FW(config)# sysmon
步骤2	配置nat连接数监控
	FW(sysmon)# sysres nat-session 1000 表示配置 nat 连接数监控，如果 nat 规则并发连接数总和大于 1000 则告警。
步骤3	取消nat连接数监控
	FW(sysmon)# no sysres nat-session

3.6 日志空间监控

3.6.1 配置日志空间监控

监控步骤：

步骤1	进入监控配置节点
	FW(config)# sysmon
步骤2	配置日志空间监控
	FW(sysmon)# sysres log_space 90 表示配置日志空间监控，如果日志空间占用硬盘大于 90%则告警。
步骤3	取消日志空间监控
	FW(sysmon)# no sysres log_space

3.7 系统监控告警方式

3.7.1 配置系统监控告警方式

命令说明：log (net|cpu|memory|cpu_temperature|session|flow|packet| nat-session) (local|syslog|email)

关键字和参数	说明
(net|cpu|memory|cpu_temperature|session|flow|packet| nat-session|log_space)	net表示网络监控 cpu表示系统CPU利用率监控 memory表示系统内存利用率监控 cpu_temperature表示CPU温度监控 session表示系统连接数监控 flow表示流量监控 packet表示报文占用空间（即报文长度） nat-session表示nat规则并发连接数总和 log_space表示日志硬盘的占用率
(local|syslog|email)	local表示把告警信息发送到本地日志 syslog表示把告警信息发送到SYSLOG服务器 email表示把告警信息发送到所配置的邮件地址

3.8 显示系统监控配置信息

3.8.1 显示系统监控配置信息

显示步骤：

步骤1	显示系统监控配置
	FW# show sysmon config sysmon log net syslog log net enail log cpu local log cpu syslog log memory local log memory syslog log cpu_temperature local log cpu_temperature syslog log session local log session syslog log nat-session local log nat-session syslog sysres cpu 85 sysres cpu_temperature 85 sysres memory 85 sysres session 15000 sysres flow 1024000 sysres nat-session 1000 Sysres log_space 90 !

3.9 配置案例

3.9.1 告警配置

在命令行设置系统监控：

```
FW(config)# sysmon
FW(sysmon)# sysres cpu 85
FW(sysmon)# sysres cpu_temperature 85
FW(sysmon)# sysres memory 85
FW(sysmon)# sysres session 20000
FW(sysmon)# sysres flow 1024000
FW(sysmon)# log net syslog
FW(sysmon)# log net enail
FW(sysmon)# log cpu local
FW(sysmon)# log cpu syslog
FW(sysmon)# log cpu_temperature local
FW(sysmon)# log cpu_temperature syslog
FW(sysmon)# log memory local
FW(sysmon)# log memory syslog
FW(sysmon)# log session local
FW(sysmon)# log session syslog
FW(sysmon)# log log_space syslog
```

查看系统监控的结果，需要登陆 web 页面，进入**日志>系统日志>系统事件**，查看日志。

4 配置会话管理

4.1 会话管理概述

会话管理原理：

会话管理功能，即基于状态的资源控制，用于保护 FW 资源。

对 FW 产品来说，资源是十分宝贵的，当受到外来的 DDOS 一类攻击时，设备内部的资源大量被攻击流所占用，此时正常的报文必然会受到影响。

启动会话管理服务后，设备会对所建流进行监控，将这些流区分为全连接和半连接：当有新建连接长时间未得到应答就会一直处于半连接状态，直至得到正确应答才会转成全连接状态。当设备内的半连接超过限制时，就判断有可能是遭受到了攻击，这时设备将会做相应的处理。

会话管理主要功能：

- 连接数管理
- 连接老化时间控制
- 连接监控
- 连接删除
- 基于源/目的 IP/目的端口的连接统计
- 协议管理

相关术语解释：

- 系统连接总数：所有协议的连接总数之和。
- 系统半连接总数：所有协议的半连接总数之和。
- 系统半连接速率总数：所有协议的半连接速率总数之和。
- 协议连接总数：该协议当前建流数，包括全连接和半连接。
- 协议半连接总数：该协议当前所建流中仍处于半连接状态的流数。
- 协议半连接速率总数：该协议当前一分钟内所建流中仍处于半连接状态的流数。

4.2 配置会话管理

4.2.1 缺省配置信息

表 4-1 会话管理缺省配置信息

内容	缺省设置	备注
使能/禁止状态（enable/disable）	enable	可更改设置
TCP SYNSENT状态老化时间	20	可更改设置
TCP SYNRECV状态老化时间	10	可更改设置
TCP ESTABLISHED状态老化时间	3600	可更改设置
TCP TIMEWAIT状态老化时间	5	可更改设置
TCP LASTACK状态老化时间	5	可更改设置

TCP FINWAIT状态老化时间	5	可更改设置
TCP CLOSE状态老化时间	5	可更改设置
TCP CLOSEWAIT状态老化时间	5	可更改设置
UDP HALFOPEN状态老化时间	10	可更改设置
UDP STREAM状态老化时间	30	可更改设置
ICMP老化时间	10	可更改设置
GRE半连接老化时间	10	可更改设置
GRE STREAM状态老化时间	30	可更改设置
其它协议老化时间	30	可更改设置

4.2.2 关闭/启动会话管理服务

配置步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	no ip inspect service	停止会话管理服务
步骤3	exit	退出全局配置模式

使用 ip inspect service 可以重新启动会话管理服务，使其恢复到缺省配置。

停止会话管理服务后，各协议的老化时间会切换到另一组默认时间：

TCP SYNSENT状态老化时间	120
TCP SYNRECV状态老化时间	60
TCP ESTABLISHED状态老化时间	43200
TCP TIMEWAIT状态老化时间	120
TCP LASTACK状态老化时间	30
TCP FINWAIT状态老化时间	120
TCP CLOSE状态老化时间	10
TCP CLOSEWAIT状态老化时间	60
UDP HALFOPEN状态老化时间	30
UDP STREAM状态老化时间	180
ICMP老化时间	30
GRE半连接老化时间	30
GRE STREAM状态老化时间	180
其它协议老化时间	600

4.2.3 配置会话管理老化时间

配置步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	ip inspect idletime tcp synsent-time <0-1728000>	配置TCP SYNSENT状态老化时间
步骤3	ip inspect idletime tcp synrecv-time <0-1728000>	配置TCP SYNRECV状态老化时间
步骤4	ip inspect idletime tcp finwait-time <0-1728000>	配置TCP FINWAIT状态老化时间
步骤5	ip inspect idletime tcp closewait-time<0-1728000>	配置TCP TIMEWAIT状态老化时间
步骤6	ip inspect idletime tcp timewait-time <0-1728000>	配置TCP CLOSEWAIT状态老化时间

步骤7	ip inspect idletime tcp close-time <0-1728000>	配置TCP CLOSE状态老化时间
步骤8	ip inspect idletime tcp established-time <0-1728000>	配置TCP ESTABLISHED状态老化时间
步骤9	ip inspect idletime tcp lastack-time <0-1728000>	配置TCP LASTACK状态老化时间
步骤10	ip inspect idletime udp halfopen <0-3600>	配置UDP HALFOPEN状态老化时间
步骤11	ip inspect idletime udp stream <0-1728000>	配置UDP STREAM状态老化时间
步骤12	ip inspect idletime gre timeout <0-3600>	配置GRE半连接老化时间
步骤13	ip inspect idletime gre stream <0-1728000>	配置GRE STREAM状态老化时间
步骤21	ip inspect idletime (tcp-idletime|udp-idletime|icmp-idletime|generic-idletime) <0-1728000>	配置各协议老化时间
步骤22	no ip inspect idletime tcp all	TCP各状态老化时间全部恢复为默认值
步骤23	no ip inspect idletime udp all	UDP各状态老化时间全部恢复为默认值
步骤24	no ip inspect idletime gre all	GRE各状态老化时间全部恢复为默认值
步骤26	no ip inspect idletime (tcp-idletime|udp-idletime|icmp-idletime|generic-idletime|all)	各协议老化时间恢复为默认值
步骤27	exit	退出全局配置模式
步骤28	show ip inspect idletime all	显示当前IP INSPECT老化时间配置

以上命令均可使用 no 命令取消对各个命令的设置，使其恢复到缺省配置。

参数说明：

参数	说明	缺省配置
<0-1728000>	老化时间，单位为秒	无
(tcp-idletime|udp-idletime|icmp-idletime|generic-idletime|all)	各协议老化时间，tcp和udp为全连接老化时间。	无

4.2.4 配置协议管理

网络设备对不同协议的连接都有超时删除功能，以保护设备的连接资源。在 FW 中，对 TCP 协议的全连接，默认超时时间是 1 小时，UDP 协议为 30 秒。

有些应用程序在全连接建立后，报文只会根据实际的数据进行交互，而没有保活机制，往往会导致连接超时删除，后续的数据无法通过设备。

协议管理功能提供了设置特定服务超时时间的功能，可以解决这种需要长时间空闲连接的问题。

配置步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	protocol manage NAME	配置一项协议管理并进入协议管理节点
步骤3	description LINE	配置描述

步骤4	protocol <TCP | UDP>	配置协议
步骤5	port <1-65535>	配置目的端口
步骤6	timeout <1-65535>	配置超时时间，单位为分钟

配置协议管理后，不会影响已经建立的连接，对新建的连接配置才会生效。

4.3 会话监控与维护

4.3.1 查看会话计数值

步骤1	show ip inspect count

```
host# show ip inspect count
System
    Connect sum count:              38441
    Complete connect count:         38418
    Connect rate count:             6298
```

4.3.2 查看会话默认老化时间

步骤1	show ip inspect idletime all

```
host# show ip inspect idletime all
TCP syn sent time: 20 seconds
TCP syn rec time: 10 seconds
TCP idletime: 3600 seconds
TCP fin wait time: 5 seconds
TCP close wait time: 5 seconds
TCP last ack time: 5 seconds
TCP wait time: 5 seconds
TCP close time: 5 seconds
UDP Halfopen time: 10 seconds
UDP idletime: 30 seconds
ICMP idletime: 10 seconds
GRE idletime: 10 seconds
GRE stream idletime: 30 seconds
Other idletime: 30 seconds
```

4.3.3 查看设备当前连接

步骤1	show ip connection all [<1-1000>]

```
host# show ip connection all
  Protocol:TCP   PolicyID:122                    State:Complete                  Expire: 00:00:04
                 SrcIP:20.20.2.2                 DstIP:12.1.1.22                 Existed:00:00:03
                 SrcPort:26386                   DstPort:21                      CoreId:1
                 (RouteCacheOrigi)Outif:vlan201  Nexthop:00:15:2a:6e:5d:36  HHCache:14
                 (RouteCacheReply)Outif:vlan21   Nexthop:50:12:13:05:15:00  HHCache:14
                 Application:ftp
```

步骤2	show ip connection protocol (tcp|udp|icmp|generic|all) ip source (IPADDRESS | any) dest (IPADDRESS | any) port (DESTPORT|any) state (complete|halfopen|all) [<1-1000>]

```
host# show ip connection protocol all ip source 20.20.2.2 dest any port any state all
Protocol:TCP   PolicyID:122                    State:Complete                Expire: 00:00:04
  SrcIP:20.20.2.2                              DstIP:12.1.1.22               Existed:00:00:03
  SrcPort:26386                                DstPort:21                    CoreId:1
  (RouteCacheOrigi)Outif:vlan201               Nexthop:00:15:2a:6e:5d:36     HHCache:14
  (RouteCacheReply)Outif:vlan21                Nexthop:50:12:13:05:15:00     HHCache:14
  Application:ftp
```

参数说明：

参数	说明	缺省配置
[<1-1000>]	最大显示连接数	无
(tcp|udp|icmp|generic|all)	按协议匹配显示	无
(IPADDRESS | any)	按IP地址匹配显示	Any
(DESTPORT|any)	按目的端口匹配显示	Any
(complete|halfopen|all)	按连接状态匹配显示	无

IPADDRESS 可以输入 IP 地址/范围/掩码 3 种形式
DESTPORT 可以输入端口号/范围 2 种形式

4.3.4 删除设备当前连接

步骤1	clear ip connection all

删除当前设备所有连接。

4.3.5 统计设备当前连接

步骤1	show ip connection statistic (source-ip|dest-ip) [IPADDRESS]
	host# show ip connection statistic dest-ip dest-ip 207.46.113.221 count 3 dest-ip 207.46.120.32 count 2 dest-ip 207.46.108.15 count 1 dest-ip 65.54.195.185 count 1 dest-ip 192.168.31.103 count 1 dest-ip 207.46.26.127 count 1
步骤2	show ip connection statistic port [DESTPORT]
	host # show ip connection statistic port dest-port 1863 count 2 dest-port 80 count 1 dest-port 53 count 1 dest-port 1940 count 1

参数说明：

参数	说明	缺省配置
(source-ip|dest-ip)	按源IP还是目的IP统计	无
[IPADDRESS]	IP地址	所有IP地址
[DESTPORT]	目的端口	所有端口

IPADDRESS 可以输入 IP 地址/范围/掩码 3 种形式
DESTPORT 可以输入端口号/范围 2 种形式

5 接口

5.1 配置以太网端口

5.1.1 以太网端口概述

通过配置以太网端口可以实现更改端口的带宽设置、双工模式以及端口速率等设置功能。对于端口的命名，如果是 1000M 网卡，则名称前缀为 ge，比如 ge0/0，ge1/0 等等；如果是 10000M 网卡，则名称前缀为 xge，比如 xge1/1 等等。设备的所有端口缺省状态下是打开的。

5.1.2 配置以太网端口

1. 缺省配置

表1-1 端口缺省设置信息

内容	缺省设置	备注
端口自协商配置（auto-negotiate on/off）	on	可以更改设置
端口MTU(mtu)	1500	可以更改设置
端口管理状态(shutdown/no shutdown)	no shutdown	可以更改设置

2. 启用自协商功能

默认情况下，端口参数是自协商的，在自协商模式下，端口的所有参数都是自动协商出来的，不能设置端口的参数。

启用端口自协商功能的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface IFNAME	进入某一个interface
步骤3	auto-negotiate on	启用端口的自协商功能
步骤4	end	退到特权模式下
步骤5	write terminal	显示配置

3. 禁用自协商功能

默认情况下，端口参数是自协商的。禁用自协商功能后，可以对端口参数进行配置。

禁用端口自协商功能的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface IFNAME	进入某一个interface
步骤3	auto-negotiate off	禁用端口的自协商功能
步骤4	end	退到特权模式下
步骤5	write terminal	显示配置

缺省情况下端口的自协商功能是打开的，用户必须关闭端口的自协商功能后才能对端口的其他参数进行配置。

4. 双工设置

双工就是在相对的方向上可以同时传输信息。半双工可以实现双向的通信，但不能在两个方向上同时进行，必须轮流交替地进行。与共享式 HUB 相连时，应置以太网口为半双工方式；与交换式 LAN SWITCH 相连时，一般置以太网口为全双工方式。

配置端口双工模式的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface IFNAME	进入某一个interface
步骤3	duplex (full|half)	配置端口的双工模式
步骤4	end	退到特权模式下
步骤5	write terminal	显示配置

参数说明：

duplex (full|half)：

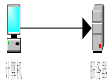
参数	说明	缺省配置
full	全双工	这是缺省设置
half	半双工	非缺省设置

5. 速率设置

端口速率表示了端口收发数据包的速率，通常为1000M，千兆设备端口速率为10M 、100M和 1000M。要使网络互联设备可以正常工作，必须保证相互连接的两个端口配置有相同的速率。

端口速率设置的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface IFNAME	进入某一个interface
步骤3	speed (10|100|1000|10000)	配置端口的速率
步骤4	end	退到特权模式下
步骤5	write terminal	显示配置



百兆端口不能设置 1000M 速率。

6. 关闭端口

端口关闭后将不再收发数据，主要用于系统故障的发现和诊断，但是通常情况下不需要这样做。

关闭端口的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface IFNAME	进入某一个interface
步骤3	shutdown	关闭端口
步骤4	end	退到特权模式下
步骤5	write terminal	显示配置

7. 配置接口 IP 地址

端口的 IP 地址可以通过两种方式配置：

1、 静态配置：静态指定 IP 地址

2、 DHCP 方式获取：通过 DHCP 方式从 DHCP 服务器获取 IP 地址，同时也能取到网关

和 DNS 设置

每个端口都能分别配置不同的 IP 地址方式，但每次只能配置一种方式。下面分别介绍这两种不同：

1、静态 IP

配置端口静态 IP 的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface IFNAME	进入某一个interface
步骤3	ip address A.B.C.D/M	静态指定接口IP地址，A.B.C.D/M为接口IP地址和掩码长度
步骤4	end	退到特权模式下
步骤5	write terminal	显示配置

2、DHCP 方式

配置端口通过 DHCP 方式获取地址的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface IFNAME	进入某一个interface
步骤3	ip address dhcp metric <1-255> gw (reset|default) dns (reset|default)	配置接口通过DHCP获取IP地址
步骤4	end	退到特权模式下
步骤5	write terminal	显示配置

参数说明：

ip address dhcp：

参数	说明	缺省配置
metric <1-255>	配置通过DHCP获取地址的权重，范围<1-255>	无
gw (reset|default)	配置网关的获取方式，reset为使用DHCP服务器指定的网关，default为使用系统原有的网关	默认不勾选
dns (reset|default)	配置DNS的获取方式，reset为使用DHCP服务器指定的DNS，default为使用系统原有的DNS	默认不勾选

使用 no ip address 可以删除当前接口的 IP 地址设置；

使用 no ip address dhcp 可以取消接口的 dhcp client 设置；

8. 配置接口 MTU

接口的 MTU 用于控制接口的最大报文发送长度。

关闭端口的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface IFNAME	进入某一个interface
步骤3	mtu <68-1500>	设置端口最大发送报文长度，缺省为1500
步骤4	end	退到特权模式下
步骤5	write terminal	显示配置

9. 配置端口管理访问

端口的管理访问是用来控制通过该端口访问和管理设备的权限。通过配置端口的管理

访问可以限制对端口的某类访问，保护设备的安全运行。

配置端口管理访问的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface IFNAME	进入某一个interface
步骤3	allow (http|https|ping|telnet|ssh)	配置端口管理访问
步骤4	end	退到特权模式下
步骤5	write terminal	显示配置

参数说明：

allow access：

参数	说明	缺省配置
http	允许或者禁止通过HTTP方式管理设备	
https	允许或者禁止通过HTTPs方式管理设备	
telnet	允许或者禁止通过Telnet方式管理设备	
ssh	允许或者禁止通过ssh方式管理设备	
ping	允许或者禁止外面设备Ping设备	

以上这些权限在同一个端口上可以同时打开多个，可以组合使用。

10. 配置端口别名

设备在出厂的时候每个端口的名字和设备面板上的名字是一致的，在设备的使用过程中，为了便于理解和记住端口的用处，需要把接口改成比较直观的名字。通过 aliasname 命令可以给每个端口取一个个直观的别名。

修改端口别名的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface IFNAME	进入某一个interface
步骤3	aliasname NAME	配置端口别名，NAME为端口的别名
步骤4	end	退到特权模式下
步骤5	write terminal	显示配置

5.1.3 配置案例

案例描述

将端口 ge0 的速率设置为 100Mbps，双工模式设置为全双工，关闭端口 ge0。

配置步骤：

步骤1	进入以太网端口配置模式
	host(config)# interface ge0
步骤2	关闭自协商
	host (config-if)# no auto
步骤3	配置端口ge0的带宽为100Mbps
	host (config-if)# speed 100
步骤4	配置端口ge0为全双工工作模式

	host (config-if)# duplex full
步骤5	关闭端口ge0
	host (config-if)# shutdown

5.1.4 以太网端口监控与维护

1. 显示端口的信息

显示某个端口信息的步骤：

步骤1	显示某个端口的信息
	USG_A# show interface eth0 eth0 Link status is up,Admin status is up aliasname eth0 mtu 1500 HWaddr: 00:92:25:26:00:08 auto negotiate: ON speed: 100 duplex: UFLL inet addr: 192.168.0.10 Bcast: 192.168.0.255 Mask:255.255.255.0 UP BROADCAST PHYUP RUNNING MULTICAST MTU:1500 Metric:1 RX packets:8738 errors:0 dropped:0 overruns:0 frame:0 TX packets:6556 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 RX rate: 2 packets/s 370 bytes/s TX rate: 0 packets/s 0 bytes/s

Show interface 命令不指定具体端口则显示所有端口的信息。

5.1.5 故障分析

用如下方法测试以太网端口是否正常工作：

在网络负载小时，从 PC 机（PC 机与设备位于同一局域网内）Ping 设备的以太网口，观察是否能正确返回全部报文；

在网络负载大时，查看连接双方(如设备和交换机)的端口统计信息，观察接收到错帧的统计数量是否快速增加。

如果这两项测试中有任何一项不能通过，则可以断定设备的以太网口工作不正常。

在确认以太网有故障之后可按如下步骤进行排错：

查看物理设备连接是否正常

在物理设备连接正常的情况下，网线两端端口对应的 Link 指示灯应点亮。

查看连接双方速率设置是否一致

如果一方工作于 1000Mbps 模式，而另一方工作于 100Mbps 模式时，端口也不会正常工作。故障表现为：配置为 1000Mbps 模式的一方显示为端口 down；配置为 100Mbps 模式的一方则显示为端口 UP。对于这种故障，只要使用 speed 命令把连接双方的速率配成一致即可。

查看连接双方是否处于同一网络

连接双方必须处于同一网络，即二者的网络地址一样而主机地址不同，如果二者网络地址不一样，请用 ip address 命令正确设置 IP 地址。

查看连接双方的双工模式是否一致（其中一方为设备）

当双工模式不一致，即一方工作于全双工模式，而另一方工作于半双工模式，故障表现为：

网络流量增大时，配置为半双工模式的一方显示冲突频繁（如连接共享式 Hub 则整个网络段上所有其它机器都显示冲突严重），配置为全双工模式的一方则显示接收到大量错包，同时，双方丢包严重。

可用 show interface [IFNAME]命令查看以太网收发包的错误率，冲突现象一般可以通过网口状态指示灯观察到；

在连接共享式 Hub 时，应该以半双工模式工作；在连接 Lanswitch 时，一般使用全双工模式工作。

5.2 配置VLAN接口

本节涉及设备 VLAN 的配置，内容主要包括：

VLAN 概述

配置接口封装的链路层协议为 VLAN

5.2.1 VLAN概述

在一个物理局域网内，通过对端口的划分，将局域网内的设备分割为几个各自独立的群组，群组内部的设备之间可以自由地通讯，而当分属不同群组的设备要进行通讯时，必须进行三层的路由转发。通过这种方式，一个物理局域网就如同被划分为几个相互隔离的局域网，这些不同的群组就称为虚拟局域网（VLAN）。加入到 VLAN 中的接口分两种方式：tag 与 untag，tag 的方式启用 802.1q 协议并能处理协议报文，untag 方式则只能处理不带 vlan 标签的普通以太报文。

VLAN 支持 STP 协议，STP（Spanning Tree Protocol）是生成树协议的英文缩写。该协议可应用于环路网络，通过一定的算法实现路径冗余，同时将环路网络修剪成无环路的树型网络，从而避免报文在环路网络中的增生和无限循环。

5.2.2 创建VLAN接口

VLAN ID 值的说明：

设备的 VLAN ID 值的范围是 1-4094，这个值是通过使用 vlan vlanid 指令设定的，例如，如果创建了一个 VLAN ID 为 10 的 VLAN，则命令为 vlan 10。

配置接口封装的链路层协议为 VLAN 的步骤:

步骤1	vlan <1-4094>	用于创建VLAN，<1-4094>为VLAN ID。
步骤2	Interface VLANNAME	设置端口的IP地址等

5.2.3 将接口加入VLAN中

以 untag 的方式将接口加入 VLAN 的步骤：

步骤1	interface NAME	进入一个端口
步骤2	untag VLANNAME	以untag的方式将本端口加入一个VLAN，同时该端口的所有IP地址将被删除

以 tag 的方式将接口加入 VLAN 的步骤：

步骤1	interface NAME	进入一个端口
步骤2	tag VLANNAME	以tag的方式将本端口加入一个VLAN，同时该端口的所有IP地址将被删除

5.2.4 配置信息的显示

VLAN 配置信息显示命令:

步骤1	show interface	显示接口信息

1）将一个端口加入一个 VLAN 时该端口的所有 IP 地址将被删除。
2）已加入聚合链路的端口不能加入 VLAN。
3）同一个端口只能 untag 到一个 VLAN。
4）同一个端口不能既 tag 又 untag 到同一个 VLAN 中。

5.2.5 配置网桥STP

STP（Spanning Tree Protocol）是生成树协议的英文缩写。该协议可应用于环路网络，通过一定的算法实现路径冗余，同时将环路网络修剪成无环路的树型网络，从而避免报文在环路网络中的增生和无限循环。

创建新的桥接口，开启关闭 STP 功能

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	vlan <1-4094>	进入VLAN接口配置
步骤3	bridge stp (enable|disable)	选择开启货关闭STP功能

配置网桥优先级

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	vlan <1-4094>	进入桥接口配置
步骤3	bridge priority <0-61440>	配置桥接口优先级

参数说明：

参数	说明	缺省配置
priority	桥接口优先级值，范围0-61440	32768

配置网桥发送 bpdu hello 时间

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	vlan <1-4094>	进入桥接口配置
步骤3	bridge hello-time <1-10>	配置发送bpdu hello时间

参数说明：

参数	说明	缺省配置
hello-time	发送hello bpdu时间间隔，范围1-10	2

配置网桥 STP 最大老化时间

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	vlan <1-4094>	进入桥接口配置
步骤3	bridge max-age <6-40>	配置STP最大老化时间

参数说明：

参数	说明	缺省配置
max-age	STP最大老化时间，范围6-40	20

配置网桥端口状态转换时延

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	vlan <1-4094>	进入桥接口配置
步骤3	bridge forward-delay <4-30>	配置端口状态转换时延

参数说明：

参数	说明	缺省配置
forward-delay	端口状态转换时延，范围4-30	15

注意

要选择性能较高、位置较靠中心的桥的优先级最高。

提示

端口转换时间是指：开启 STP 后，端口从 listening 到 learning 到 forwarding 变化的时间间隔。

5.2.6 常见故障分析

VLAN 无法正常工作

故障现象	在VLAN的两个端口之间数据无法转发
分析与解决	1）是否将正确的端口加入网桥 2）链路是否正常 3）端口状态是否正常（该端口Admin状态是否是up）

5.3 配置VXLAN接口

本节涉及设备 VXLAN 的配置，内容主要包括：
VXLAN 概述、如何配置和使用 VXLAN

5.3.1 VXLAN概述

VXLAN（Virtual eXtensible Local Area Network，虚拟扩展局域网），是由 IETF 定义的 NVO3（Network Virtualization over Layer 3）标准技术之一，是对传统 VLAN 协议的一

种扩展。VXLAN 的特点是将 L2 的以太帧封装到 UDP 报文（即 L2 over L4）中，并在 L3 网络中传输。

VXLAN 本质上是一种隧道技术，在源网络设备与目的网络设备之间的 IP 网络上，建立一条逻辑隧道，将用户侧报文经过特定的封装后通过这条隧道转发。从用户的角度来看，接入网络的服务器就像是连接到了一个虚拟的二层交换机的不同端口上，可以方便地通信。

5.3.2 创建VXLAN接口

VNI 值的说明：

VXLAN Network Identifier，VXLAN 网络标识符，例如，如果创建了一个 VNI 为 10 的 VXLAN，则命令为 vxlan 10。

配置 VXLAN 的步骤:

步骤1	configure terminal	进入配置模式
步骤2	interface vxlan < 0-16777215 >	用于创建VXLAN，<0-16777215>为Vni
步骤3	remote A.B.C.D	设置vxlan隧道的目的地址
步骤4	local A.B.C.D	设置vxlan隧道的源地址

5.3.3 配置信息的显示

VXLAN 配置信息显示命令:

步骤1	show interface	显示接口信息

5.3.4 VXLAN fdb表显示

VXLAN 配置信息显示命令:

步骤1	show vxlan < 0-16777214> fdb	Vxlan fdb table

5.4 配置透明桥

本节涉及设备桥接口的配置，内容主要包括：

透明桥概述

配置桥接口

5.4.1 透明概述

透明网桥功能最初是由 DEC 公司提出，并被 802.1 委员会采纳并标准化。透明网桥实现网络报文链路层转发，使用方便，易于安装。透明桥支持 STP 协议，STP（Spanning Tree Protocol）是生成树协议的英文缩写。该协议可应用于环路网络，通过一定的算法实现路径冗余，同时将环路网络修剪成无环路的树型网络，从而避免报文在环路网络中的增生和无限循环。

5.4.2 创建桥接口

新建透明桥接口步骤:

步骤1	Interface bvi <0-255>	用于创建桥接口，<0-255>为桥组号。
步骤2	Interface BVINAME	设置桥接口的IP地址等

5.4.3 将接口加入透明桥中

物理接口加入到透明桥的步骤：

步骤1	interface NAME	进入一个端口
步骤2	bridge-group <0-255>	将端口加入到某个桥组号的透明桥，同时该端口的所有IP地址将被删除

5.4.4 配置信息的显示

透明桥配置信息显示命令:

步骤1	show bridge-group <0-255>	显示透明桥信息

1）将一个端口加入一个透明桥时该端口的所有 IP 地址将被删除。

2）已加入聚合链路的端口不能加入透明桥。

3）已加入到透明桥或 VLAN 的端口不能加入透明桥。

5.4.5 配置网桥STP

STP（Spanning Tree Protocol）是生成树协议的英文缩写。该协议可应用于环路网络，通过一定的算法实现路径冗余，同时将环路网络修剪成无环路的树型网络，从而避免报文在环路网络中的增生和无限循环。

创建新的桥接口，开启关闭 STP 功能

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	Interface bvi<0-255>	进入桥接口配置
步骤3	bridge stp (enable|disable)	选择开启货关闭STP功能

配置网桥优先级

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	Interface bvi<0-255>	进入桥接口配置
步骤3	bridge priority <0-61440>	配置桥接口优先级

参数说明：

参数	说明	缺省配置
priority	桥接口优先级值，范围0-61440	32768

配置网桥发送 bpdu hello 时间

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	Interface bvi<0-255>	进入桥接口配置

步骤3	bridge hello-time <1-10>	配置发送bpdu hello时间

参数说明：

参数	说明	缺省配置
hello-time	发送hello bpdu时间间隔，范围1-10	2

配置网桥 STP 最大老化时间

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	Interface bvi<0-255>	进入桥接口配置
步骤3	bridge max-age <6-40>	配置STP最大老化时间

参数说明：

参数	说明	缺省配置
max-age	STP最大老化时间，范围6-40	20

配置网桥端口状态转换时延

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	Interface bvi<0-255>	进入桥接口配置
步骤3	bridge forward-delay <4-30>	配置端口状态转换时延

参数说明：

参数	说明	缺省配置
forward-delay	端口状态转换时延，范围4-30	15

要选择性能较高、位置较靠中心的桥的优先级最高。

端口转换时间是指：开启 STP 后，端口从 listening 到 learning 到 forwarding 变化的时间间隔。

5.4.6 常见故障分析

透明桥无法正常工作

故障现象	在透明桥的两个端口之间数据无法转发
分析与解决	1）是否将正确的端口加入网桥 2）链路是否正常 3）端口状态是否正常（该端口Admin状态是否是up）

5.5 配置链路聚合Trunk接口

5.5.1 链路聚合Trunk概述

链路聚合 Trunk 是通过组合多个链路成为一个逻辑的网络链路，用于提高带宽。在使用快速以太网和千兆以太网技术，通过链路聚合提高了设备之间通讯通道的容量和可用性。两个或多个百兆或千兆以太网连接捆绑在一起来提高带宽的容量和连接的冗余性。链路聚合也提供了负载均衡的方式来处理通讯负荷，使得通讯负荷均分在几个链路中，不会有单独一个链路超负载。通过链路聚合，用户可以在许多应用中得到实际的益处：更高的可靠性、更高的带宽，使用现有的设备，节约成本（不需要更新设备来获取更高的带宽）。

5.5.2 配置链路聚合Trunk接口

创建新的 Trunk 接口，将物理接口加入 Trunk 中

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	Interface tvi0	创建Trunk接口tvi0
步骤3	Interface eth0 trunk-group 0 Interface eth1 trunk-group 0	物理口eth0、eth1加入到trunk 0组

参数说明：

参数	说明	缺省配置
Trunk组号	0-255	

配置 Trunk 的聚合模式

配置步骤

步骤1	configure terminal	进入配置模式
步骤2	Interface tvi0	进入Trunk接口tvi0
步骤3	trunk lacp disable	配置Trunk接口tvi0聚合模式为手工聚合模式
步骤3	trunk lacp enable	配置Trunk接口tvi0聚合模式为LACP协议聚合模式

参数说明：

参数	说明	缺省配置
手工聚合模式	所有加入到Trunk接口的物理子接口平行，都可以接收报文，并且在发送报文时，轮询发送，即从第一个物理子接口到最后一个物理子接口依次发送	手工模式
LACP聚合模式	所有加入到Trunk的物理子接口上都开启LACP协议，将与对端的物理接口进行LACP协商，符合聚合条件者可以聚合在一起	

配置 Trunk 接口 untag 到 VLAN

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	Interface bvi0	进入桥接口配置
步骤3	Interface tvi0	进入Trunk接口配置
步骤4	untag vlan1	untag到VLAN

配置 Trunk 接口 tag 到 VLAN

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	Interface tvi0	进入Trunk接口配置
步骤3	tag vlan 1	tag到VLAN

参数说明：

参数	说明	缺省配置
Trunk的vlan ID	vlan ID与物理接口vlan ID相同	

5.5.3 常见故障分析

故障现象 1：Trunk 接口不收发报文

现象	Trunk 接口不能接收报文也不能发送报文
分析	可能是Trunk链路聚合协商不成功，导致其下端口inactive
解决	检查对端设备 trunk 口配置，使 Trunk 两端聚合协商成功

5.6 配置GRE接口

5.6.1 GRE概述

GRE（Generic Routing Encapsulation，通用路由封装）协议是对网络层协议的数据报文进行封装，使这些被封装的数据报文能够在另一个网络层协议中传输。GRE 采用了 Tunnel（隧道）技术，是 VPN（Virtual Private Network）的第三层隧道协议。通过 GRE 接口配合路由配置，可以将流量引入 GRE 隧道传输。

5.6.2 配置GRE接口

创建新的 GRE 接口

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	Interface gre0	创建GRE接口gre0

参数说明：

参数	说明	缺省配置
GRE组号	0-255	

配置 GRE 参数

配置步骤

步骤1	configure terminal	进入配置模式
步骤2	Interface gre0	进入GRE接口gre0
步骤3	source (A.B.C.D|INTERFACE_NAME)	配置GRE隧道的源，IP地址或者接口名称
步骤3	destination (A.B.C.D|dynamic)	配置GRE隧道的目的，IP地址或动态模式
步骤4	key <1-9999>	配置GRE隧道的key
步骤5	ttl <1-255>	配置GRE报文的TTL
步骤6	keepalive <1-86400> <1-1000>	配置GRE隧道的keepalive

参数说明：

参数	说明	缺省配置
GRE隧道的源	GRE隧道的源，具体IP地址或者是接口名称（以太网接口、桥接口、vlan接口、trunk接口等）	
GRE隧道的目的	GRE隧道的目的，具体IP地址或者动态模式，动态模式必须由隧道对端主动连接	
GRE隧道的key	标示GRE隧道，范围1-9999	
GRE隧道的TTL	GRE 隧道封装 IP 报文的 TTL	
GRE隧道的keepalive	GRE隧道保活报文的发送间隔与重试次数	默认间隔10秒，重试3次

5.6.3 常见故障分析

故障现象 1：GRE 接口不收发报文

现象	GRE 接口不能接收报文也不能发送报文
分析	可能是GRE隧道两端的key值不同
解决	检查隧道对端设备 GRE 接口与本端 key 值相同

5.7 配置接口联动组

接口联动可以通过配置接口联动组的方式，把多个物理接口绑定在一起，实现同一联动组内接口之间链路状态保持一致的功能。

首先新建一个接口联动组，然后用 include 命令向接口联动组中添加需要做联动的物理接口。一般一个接口联动组中至少需要配置两个接口进行相互联动，如果联动组中的接口配置少于两个则没有意义。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	bind-interface-group NAME	进入名为NAME的接口联动组
步骤3	include interface IF_NAME	将名为IF_NAME的接口加入该联动组中
步骤4	show bind-interface	显示接口联动组配置信息

使用 no include interface IF_NAME 可以删除接口联动组中通过 include interface 命令添

加的接口。

参数说明：

命令（1）：bind-interface-group NAME

参数	说明	缺省配置
<NAME>	接口联动组名称	无

命令（2）：include interface IF_NAME

参数	说明	缺省配置
<IF_NAME>	物理接口名称	无

5.7.1 配置案例: 添加接口到接口联动组中

案例描述：配置两个接口到指定的联动组中。

配置步骤：

步骤1	开启接口联动总开关
	host(config)# bind-interface enable
步骤2	创建一个接口联动组
	host(config)#bind-interface-group group1
步骤3	在这个接口联动组中添加两个接口
	host(config-zone)# include interface ge0/0
	host(config-zone)# include interface ge0/3

使用 show 命令查看配置结果：

host# show bind-interface

bind-interface enable

bind-interface-group group1

include-interface ge0/0

include-interface ge0/3

5.7.2 故障现象

现象	接口联动组中无法加入某个物理接口。
分析	当一个接口正在被其它接口联动组引用时，就不能再加入到其它接口联动组中。
解决	可以先把这个接口从其他接口联动组中删除，再添加到需要加入的联动组中。

5.8 配置接口镜像

5.8.1 接口镜像概述

接口镜像功能通过将一个或多个源接口的数据流量转发到某一个指定接口来实现对网络的监听，可以通过镜像接口对网络的流量进行监控分析。支持接口镜像的接口类型有物理接口与 GRE 接口。

5.8.2 配置接口镜像

启用接口镜像

配置步骤：

步骤1	configure terminal	进入配置模式

步骤3	mirror NAME1 (inbound|outbound|both) to NAME2	配置名为NAME1的接口流量镜像到NAME2

参数说明：

参数	说明	缺省配置
inbound	镜像接口的接收流量	
outbound	镜像接口的发送流量	
both	镜像接口的接收、发送流量	

取消接口镜像

配置步骤：

步骤1	configure terminal	进入配置模式
步骤3	no mirror NAME	取消名为NAME1的接口镜像

5.8.3 故障现象

现象	某个接口不能配置接口镜像。
分析	只有物理接口、gre接口可以配置接口镜像，目的镜像接口，不能配置为源镜像接口。
解决	取消接口作为目镜像接口，重新配置该接口为源镜像接口。

6 配置安全域

6.1 安全域概述

域就是接口组，可以在一个域中加入多个接口，但是一个接口只能属于一个域。如果一个接口被包含在某个域中，就不能单独对该接口进行配置。

6.2 配置向域中添加接口

可以用 include 命令向域中添加一个接口。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	zone NAME	进入名为NAME的域模式
步骤3	include interface IF_NAME	将名为IF_NAME的接口加入该域中
步骤4	show zone NAME	显示域配置信息

使用 no include interface IF_NAME 可以删除接口组中通过 include interface 命令添加的接口。

参数说明：

命令（1）：zone NAME

参数	说明	缺省配置
<NAME>	域名称	无

命令（2）：include interface IF_NAME

参数	说明	缺省配置
<IF_NAME>	接口名称	无

6.3 配置区域内接口互访

可以用 allow intrazone 命令来配置区域内接口互访

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	zone NAME	进入名为NAME的域模式
步骤3	allow intrazone	允许区域内接口互访

6.4 配置案例

6.4.1 配置案例: 添加接口到域中

案例描述

配置一个接口到指定的域中。

配置步骤：

步骤1	创建一个域

	host(config)#zone all
步骤2	在这个于中添加一个接口
	host(config-zone)# include interface eth0

配置结果：

```
host# show running-config
!
zone all
    include interface eth0
!
```

6.5 安全域监控与维护

6.5.1 查看域信息

查看某个域的步骤：

步骤1	显示某个域信息
	host # show zone all ! zone all include interface eth0 *host* # all是域名称; eth0是被加到域中的接口名称。

6.6 常见故障分析

6.6.1 故障现象：

现象	执行no zone NAME以后，该域仍然存在。
分析	当一个域正在被引用时，就不能通过no命令删除。
解决	可以先撤销其它配置对该域的引用，确定其没有被引用之后再用no命令删除该节点。

现象	安全域无法添加接口。
分析	安全域需要添加的接口在其它安全域或其它防火墙策略中被引用
解决	查看需要添加的接口是否被其它安全域或防火墙策略引用。如果被引用，去掉接口在其它冲突位置的引用后再添加到该安全域，或者重新选择可配置的接口，加入到安全域中。

7 配置 IPv6

7.1 IPv6概述

IPv6（Internet Protocol Version 6，因特网协议版本6）是网络层协议的第二代标准 协议，也被称为IPng（IP Next Generation，下一代因特网），它是IETF（Internet Engineering Task Force，Internet 工程任务组）设计的一套规范，是IPv4 的升级 版本。IPv6 和IPv4 之间最显著的区别为IP 地址的长度从32 比特增加到128 比特。

7.1.1 IPv6协议特点

1. 简化的报文头格式

通过将IPv4 报文头中的某些字段裁减或移入到扩展报文头，减小了IPv6 基本报文 头的负载，从而简化了转发设备对 IPv6 报文的处理，提高了转发效率。尽管 IPv6 地址长度是IPv4 地址长度的四倍，但IPv6 基本报文头的长度只有40 字节，为IPv4 报文头长度（不包括选项字段）的两倍。

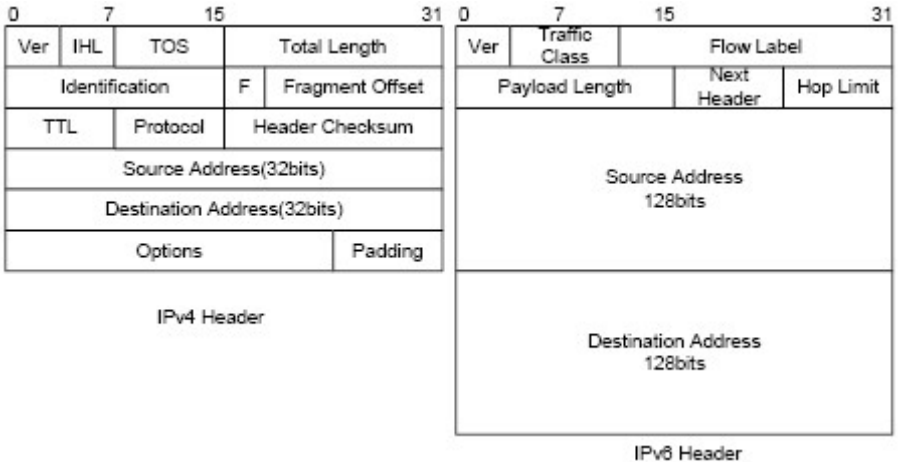


图7-1 IPv4报文头和IPv6基本报文头格式比较

2. 充足的地址空间

IPv6 的源地址与目的地址长度都是128 比特（16 字节）。它可以提供超过3.4×10^{38} 种可能的地址空间，完全可以满足多层次的地址划分需要，以及公有网络和机构内 部私有网络的地址分配。

3. 层次化的地址结构

IPv6 的地址空间采用了层次化的地址结构，有利于路由快速查找，同时可以借助路 由聚合，有效减少IPv6 路由表占用的系统资源。

4. 地址自动配置

为了简化主机配置，IPv6 支持有状态地址配置和无状态地址配置：

- 有状态地址配置是指从服务器（如DHCP 服务器）获取IPv6 地址及相关信息；
- 无状态地址配置是指主机根据自己的链路层地址及路由器发布的前缀信息自动配置IPv6 地址及相关信息。

同时，主机也可根据自己的链路层地址及默认前缀（FE80::/64）形成链路本地地址， 实现与本链路上其他主机的通信。

5. 内置安全性

IPv6 将IPSec 作为它的标准扩展头，可以提供端到端的安全特性。这一特性也为解 决网络安全问题提供了标准，并提高了不同IPv6 应用之间的互操作性。

6. 支持QoS

IPv6 报文头的流标签（Flow Label）字段实现流量的标识，允许设备对某一流中的 报文进行识别并提供特殊处理。

7. 增强的邻居发现机制

IPv6 的邻居发现协议就是一组 ICMPv6（Internet Control Message Protocol for IPv6，IPv6 的因特网控制报文协议）消息，管理着邻居节点间（即同一链路上的节 点）信息的交互。它代替了ARP（Address Resolution Protocol，地址解析协议）、 ICMPv4 路由器发现和ICMPv4 重定向消息，并提供了一系列其他功能。

8. 灵活的扩展报文头

IPv6 取消了 IPv4 报文头中的选项字段，并引入了多种扩展报文头，在提高处理效 率的同时还大大增强了IPv6 的灵活性，为IP 协议提供了良好的扩展能力。IPv4 报 文头中的选项字段最多只有40 字节，而IPv6 扩展报文头的大小只受到IPv6 报文大 小的限制。

7.1.2 IPv6地址介绍

1. IPv6 地址表示方式

IPv6 地址被表示为以冒号（:）分隔的一连串16 比特的十六进制数。每个IPv6 地址 被分为8 组，每组的16 比特用4 个十六进制数来表示，组和组之间用冒号隔开，比 如：2001:0000:130F:0000:0000:09C0:876A:130B。

为了简化IPv6 地址的表示，对于IPv6 地址中的“0”可以有下面的处理方式：

- 每组中的前导“0”可以省略，即上述地址可写为2001:0:130F:0:0:9C0:876A:130B。
- 如果地址中包含连续两个或多个均为0 的组，则可以用双冒号“::”来代替， 即上述地址可写为2001:0:130F::9C0:876A:130B。

注意：
在一个IPv6 地址中只能使用一次双冒号“::”，否则当设备将“::”解析为0 以恢复128 位地址时，就无法确定“::”所代表的0 的个数。

IPv6 地址由两部分组成：地址前缀与接口标识。其中，地址前缀相当于 IPv4 地址中的网络号码字段部分，接口标识相当于IPv4 地址中的主机号码部分。 地址前缀的表示方式为：IPv6 地址/前缀长度。其中，IPv6 地址是前面所列出的任一形式，而前缀长度是一个十进制数，表示IPv6 地址最左边多少位为地址前缀。

2. IPv6 的地址分类

IPv6 主要有三种类型的地址：单播地址、组播地址和任播地址。

- 单播地址：用来唯一标识一个接口，类似于 IPv4 的单播地址。发送到单播地址的数据报文将被传送给此地址所标识的接口。
- 组播地址：用来标识一组接口（通常这组接口属于不同的节点），类似于IPv4 的组播地址。发送到组播地址的数据报文被传送给此地址所标识的所有接口。
- 任播地址：用来标识一组接口（通常这组接口属于不同的节点）。发送到任播地址的数据报文被传送给此地址所标识的一组接口中距离源节点最近（根据使用的路由协议进行度量）的一个接口。

说明：
IPv6 中没有广播地址，广播地址的功能通过组播地址来实现。

IPv6 地址类型是由地址前面几位（称为格式前缀）来指定的，主要地址类型与格式前缀的对应关系如表7-1所示。

表7-1　地址类型与格式前缀的对应关系

地址类型		格式前缀（二进制）	IPv6 前缀标识
单播地址	未指定地址	00...0　(128 bits)	::/128
	环回地址	00...1　(128 bits)	::1/128
	链路本地地址	1111111010	FE80::/10
	站点本地地址	1111111011	FEC0::/10
	全球单播地址	其他形式	-
组播地址		11111111	FF00::/8
任播地址		从单播地址空间中进行分配，使用单播地址的格式	

3. 单播地址的类型

IPv6 单播地址的类型可有多种，包括全球单播地址、链路本地地址和站点本地地址 等。

- 全球单播地址等同于 IPv4 公网地址，提供给网络服务提供商。这种地址类型 的结构允许路由前缀的聚合，从而限制了全球路由表项的数量。
- 链路本地地址用于邻居发现协议和无状态自动配置中本地链路上节点之间的通信。使用链路本地地址作为源或目的地址的数据报文不会被转发到其他链路 上。
- 站点本地地址与 IPv4 中的私有地址类似。使用站点本地地址作为源或目的地 址的数据报文不会被转发到本站点（相当于一个私有网络）外的其它站点。
- 环回地址：单播地址0:0:0:0:0:0:0:1（简化表示为::1）称为环回地址，不能分 配给任何物理接口。它的作用与在 IPv4 中的环回地址相同，即节点用来给自 己发送 IPv6 报文。
- 未指定地址：地址::称为未指定地址，不能分配给任何节点。在节点获得有效 的 IPv6 地址之前，可在发送的IPv6 报文的源地址字段填入该地址，但不能作 为IPv6 报文中的目的地址。

4. 组播地址

表7-2所示的组播地址，是预留的特殊用途的组播地址。

表7-2　预留的IPv6 组播地址列表

地址	应用
FF01::1	节点本地范围所有节点组播地址
FF02::1	链路本地范围所有节点组播地址
FF01::2	节点本地范围所有路由器组播地址
FF02::2	链路本地范围所有路由器组播地址
FF05::2	站点本地范围所有路由器组播地址

另外，还有一类组播地址：被请求节点（Solicited-Node）地址。该地址主要用于获取同一链路上邻居节点的链路层地址及实现重复地址检测。每一个单播或任播IPv6 地址都有一个对应的被请求节点地址。其格式为：

FF02:0:0:0:0:1:FFXX:XXXX

其中，FF02:0:0:0:0:1:FF 为104 位固定格式；XX:XXXX 为单播或任播IPv6 地址的 后24 位。

5. IEEE EUI-64 格式的接口标识符

IPv6 单播地址中的接口标识符用来标识链路上的一个唯一的接口。目前 IPv6 单播 地址基本上都要求接口标识符为64 位。IEEE EUI-64 格式的接口标识符是从接口的 链路层地址（MAC 地址）变化而来的。IPv6 地址中的接口标识符是64 位，而MAC 地址是48 位，因此需要在MAC 地址的中间位置（从高位开始的第24 位后）插入 十六进制数FFFE（1111111111111110）。为了确保这个从MAC 地址得到的接口 标识符是唯一的还要将Universal/Local (U/L)位从高位开始的第7 位设置为“1”。最后得到的这组数就作为EUI-64 格式的接口标识符。

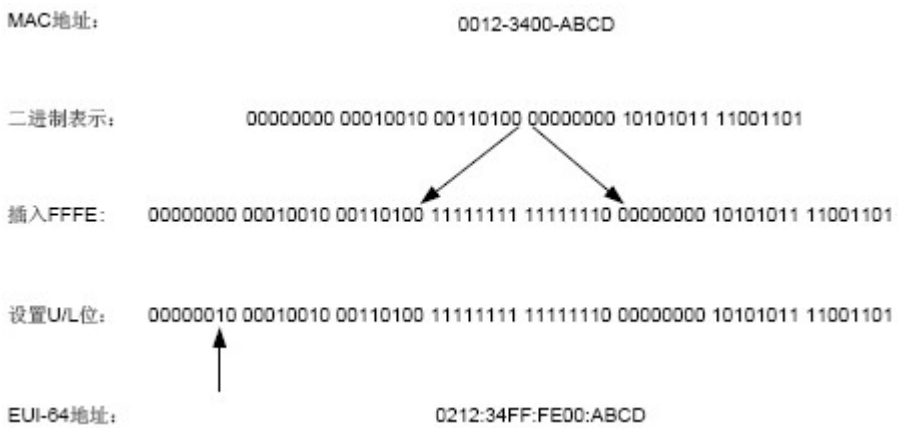


图7-2 MAC地址到EUI-64格式的接口标识符的转换过程

7.1.3 IPv6邻居发现协议介绍

IPv6 邻居发现协议使用五种类型的ICMPv6 消息，实现下面一些功能：地址解析、 验证邻居是否可达、重复地址检测、路由器发现/前缀发现及地址自动配置、重定向 等功能。

邻居发现协议使用的ICMPv6 消息的类型及作用如表7-3所示。

表7-3 邻居发现协议使用的ICMPv6 消息类型及作用

ICMPv6 消息	作用
邻居请求消息 NS（Neighbor Solicitation）	获取邻居的链路层地址
	验证邻居是否可达
	进行重复地址检测
邻居通告消息 NA（Neighbor Advertisement）	对 NS 消息进行响应
	节点在链路层变化时主动发送 NA 消息，向邻居节点通告本节点的变化信息
地路由器请求消息 RS（Router Solicitation）	主机启动后，通过 RS 消息向路由器发出请求，请求前缀和 其他配置信息，用于主机的自动配置
路由器通告消息 RA（Router Advertisement）	对 RS 消息进行响应
	在没有抑制 RA 消息发布的条件下，路由器会周期性地发布 RA 消息，其中包括前缀和一些标志位的信息
重定向消息（Redirect）	当满足一定的条件时，缺省网关通过向源主机发送重定向消 息，使主机重新选择正确的下一跳地址进行后续报文的发送

邻居发现协议提供的主要功能如下：

1. 地址解析

获取同一链路上邻居节点的链路层地址（与IPv4 的ARP功能相同），通过邻居请求 消息NS和邻居通告消息NA实现。如图7-3所示，节点A要获取节点B的链路层地址。

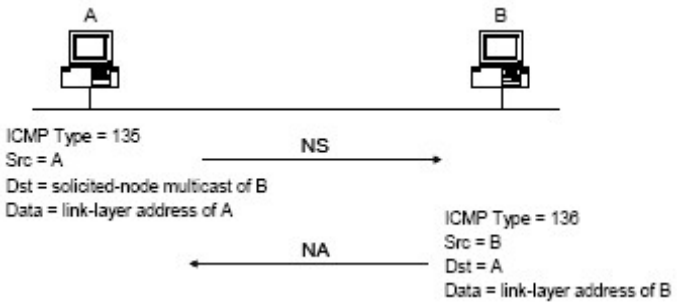


图7-3 地 址 解 析 示 意 图

(1) 节点A 以组播方式发送NS 消息。NS 消息的源地址是发送NS 消息的节点A 的接口IPv6 地址，目的地址是节点B 的被请求节点组播地址，消息内容中包 含了节点A 的链路层地址。

(2) 节点B 收到NS 消息后，判断报文的目的地址是否为自己的IPv6 地址对应的 被请求节点组播地址。如果是，则以单播方式返回NA 消息，其中包含了自己 的链路层地址。

(3) 节点A 从收到的NA 消息中就可获取到节点B 的链路层地址之后双方即可通 信。

2. 验证邻居是否可达

在获取到邻居节点的链路层地址后，通过邻居请求消息 NS 和邻居通告消息 NA 可 以验证邻居节点是否可达。

(1) 节点发送NS 消息，其中目的地址是邻居节点的IPv6 地址。

(2) 如果收到邻居的确认报文，则认为邻居可达；否则，认为邻居不可达。

3. 重复地址检测

当节点获取到一个IPv6 地址后，需要使用重复地址检测功能确定该地址是否已被其 他节点使用（与IPv4 的免费ARP功能相似）。通过邻居请求消息NS和邻居通告消息 NA实现，如图7-4所示。

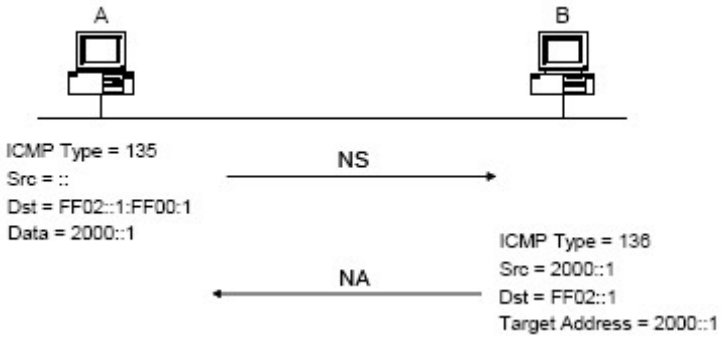


图7-4 重 复 地 址 检 测 示 意 图

(1) 节点A 发送NS 消息，NS 消息的源地址是未指定地址::，目的地址是想要检测 的IPv6 地址对应的被请求节点组播地址，消息内容中包含了想要检测的IPv6 地址。

(2) 如果节点B 已经使用这个IPv6 地址，则会返回NA 消息。其中包含了自己的IPv6 地址。

(3) 节点A 收到节点B 发来的NA 消息，就知道该IPv6 地址已被使用。反之，则 说明该地址未被使用，节点A 就可使用此IPv6 地址。

4. 路由器发现/前缀发现及地址自动配置

路由器发现及前缀发现是指主机从收到的 RA 消息中获取邻居路由器及所在网络的前缀，以及其他配置参数。

地址无状态自动配置是指主机根据路由器发现/前缀发现所获取的信息，自动配置

IPv6 地址。

路由器发现/前缀发现通过路由器请求消息RS 和路由器通告消息RA 来实现，具体 过程如下：

(1) 主机启动时，通过RS 消息向路由器发出请求，请求前缀和其他配置信息，以 便用于主机的配置。

(2) 路由器返回RA 消息，其中包括前缀和一些标志位的信息（路由器也会周期性 地发布RA 消息）。

(3) 主机利用路由器返回的RA 消息中的地址前缀及其他配置参数，自动配置接口 的IPv6 地址及其他信息。

5. 重定向功能

当主机启动时，它的路由表中可能只有一条到缺省网关的缺省路由。当满足一定的 条件时，缺省网关会向源主机发送ICMPv6 重定向消息，通知主机选择更好的下一 跳进行后续报文的发送（与IPv4 的ICMP 重定向消息的功能相同）。

设备在满足下列条件时会发送对主机重定向的ICMPv6 重定向报文：

- 接收和转发数据报文的接口是同一接口；
- 被选择的路由本身没有被ICMPv6 重定向报文创建或修改过；
- 被选择的路由不是缺省路由；
- 被转发的IPv6 数据报文中不包含路由扩展头。

7.1.4 IPv6 PMTU发现

报文从源端到目的端的传输路径中所经过的链路可能具有不同的MTU。在IPv6 中， 当报文的长度大于链路的MTU 时，报文的分片将在源端进行，从而减轻中间转发设 备的处理压力，合理利用网络资源。

PMTU（Path MTU，路径MTU）发现机制的目的就是要找到从源端到目的端的路径 上最小的MTU。PMTU发现的工作过程如图7-5所示。

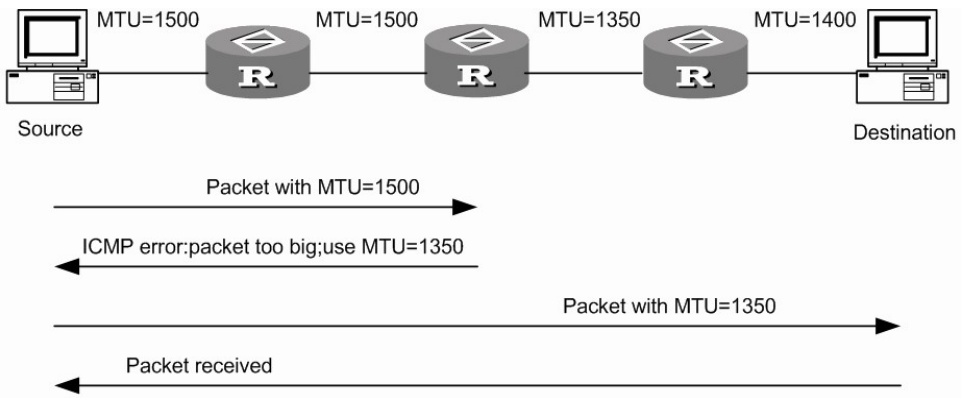


图7-5 PMTU 发现的工作过程

(1) 源端主机使用自己的MTU 对报文进行分片，之后向目的主机发送报文。

(2) 中间转发设备接收到该报文进行转发时，如果发现转发报文的接口支持的MTU 值小于报文长度，则会丢弃报文，并给源端返回一个ICMPv6 差错报文， 其中包含了转发失败的接口的MTU。

(3) 源主机收到该差错报文后，将使用报文中所携带的MTU 重新对报文进行分片 并发送。

(4) 如此反复，直到目的端主机收到这个报文，从而确定报文从源端到目的端路径 中的最小MTU。

7.1.5 IPv6过渡技术简介

随着Internet 的日益膨胀,现有的IPv4 地址已经十分紧缺,虽然使用分配临时IPv4 地址或NAT（Network Address Translator,网络地址转换）等技术,在一定程度上 缓解了IPv4 地址不足的状况,但也增加了地址解析和处理方面的开销,同时导致某 些高层应用失效,而且仍然无法回避IPv4 地址即将被分配殆尽这个问题。采用128 位地址长度的IPv6 协议,彻底解决了IPv4 地址不足的难题，并且在地址容量、安 全性、网络管理、移动性以及服务质量等方面有明显的改进，是下一代互联网络协 议采用的核心标准之一。IPv6 与IPv4 不兼容，但它同所有的TCP / IP 协议族中的 其他协议兼容，即IPv6 完全可以取代IPv4。

在IPv6 成为主流协议之前,首先使用IPv6 协议栈的网络希望能与当前仍被IPv4 支 撑着的Internet 进行正常通信，因此必须开发出IPv4 和IPv6 互通技术以保证IPv4 能够平稳过渡到IPv6。此外，互通技术应该对信息传递做到高效无缝。国际上IETF 组建了专门的NGTRANS 工作组，开展对IPv4 和IPv6 过渡问题和高效无缝互通问 题的研究。目前已经出现了多种过渡技术和互通方案，这些技术各有特点，用于解 决不同过渡时期、不同环境的通信问题。

目前解决过渡问题的基本技术主要有 3 种：双协议栈（RFC2893），隧道技术（RFC2893）和NAT-PT(RFC2766)。

说明：

本设备支持双协议栈和隧道技术。

对于IPv6 节点来说,兼容IPv4 的最直接有效的办法就是保留一个完整的IPv4 协议 栈。同时支持IPv4 协议和IPv6 协议的网络节点即成为双协议栈节点。当双协议栈 节点配置IPv4 地址和IPv6 地址后，就可以在相应接口上转发IPv4 和IPv6 报文。

当一个上层的应用支持IPv4 和IPv6 协议时,根据协议要求可以选用TCP或UDP作为 传输层的协议，但在选择网络层协议时，它会优先选择IPv6 协议栈。图 7-6所示为 IPv4 单协议栈和IPv4/IPv6 双协议栈的结构图。

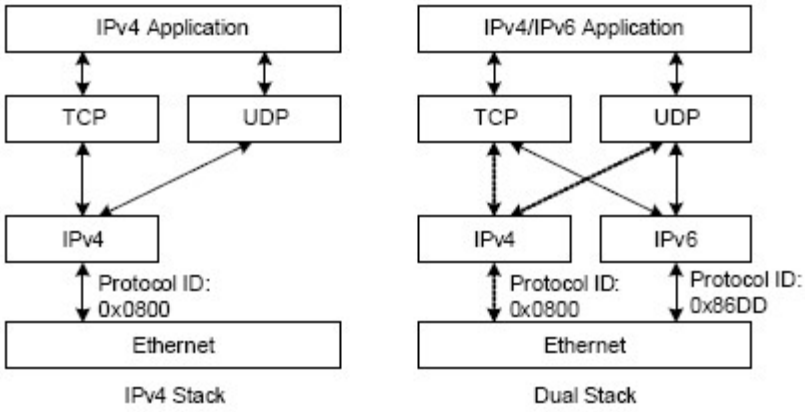


图7-6

7.1.6 IPv6隧道技术简介

Tunnel（隧道）技术是VPN（Virtual Private Network）中广泛采用的一种第三层隧 道协议。Tunnel 是一个虚拟的点对点的连接，在实际应用中仅支持点对点连接的虚 拟接口为Tunnel 接口。一个Tunnel 提供了一条使封装的数据报文能够传输的通路， 并且在一个Tunnel 的两端可以分别对数据报进行封装及解封装。

本设备支持配置IPv6 in IPv4 隧道。

1、 IPv6 in iPv4 隧道原理

IPv6 in IPv4 隧道机制是将IPv6 数据报文封装上IPv4 的报文头，通过隧道（Tunnel） 使IPv6 报文穿越IPv4 网络，实现隔离的IPv6 网络的互通，如图7-7所示。

注意：

IPv6 in IPv4 隧道两端的设备必须支持IPv4/IPv6 双协议栈。

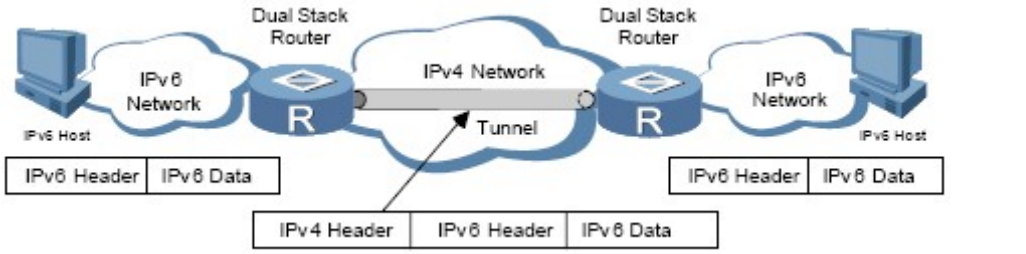


图7-7 IPv6 in IPv4 隧道原理图

IPv6 in IPv4 隧道对报文的处理过程如下：

- IPv6 网络中的设备发送IPv6 报文，到达隧道的源端设备；
- 隧道的源端设备根据路由表判定该报文要通过隧道进行转发，将会在 IPv6 报 文前封装上IPv4 的报文头，通过隧道的实际物理接口将报文转发出去；
- 封装报文通过隧道到达隧道目的端设备，目的端设备判断该封装报文的目的地 是

本设备后，将对报文进行解封装。

2、 ◆ 目的端设备根据解封装后的 IPv6 报文的目的地址将报文进行转发；如果目的地就是本设备，则将IPv6 报文转给上层协议处理。IPv6 in IPv4 隧道模式

IPv6 in iPv4 隧道可以建立在主机-主机、主机-设备、设备-主机、设备-设备之间。 隧道的终点可能是IPv6 报文的最终目的地，也可能需要进一步转发。

根据隧道终点的IPv4 地址的获取方式不同，隧道分为“配置隧道”及“自动隧道”。

- 如果隧道的终点不是IPv6 报文的最终目的地，当IPv6 报文通过隧道到达隧道 终点后，隧道终点设备（通常为路由器）会对封装的 IPv6 报文进行解封装， 并转发IPv6 报文到最终目的地。在这种情况下，不能从IPv6 报文的目的地址 中自动获取到隧道终点的IPv4 地址，需要进行手工配置。这样的隧道即为“配置隧道”。
- 如果隧道的终点就是IPv6 报文的最终目的地，则可以采用内嵌IPv4 地址的特 殊 IPv6 地址形式，实现从 IPv6 报文的目的地址中自动获取隧道终点的 IPv4 地址。这样的隧道即为 “自动隧道”。

根据对IPv6 报文的封装方式的不同，IPv6 in IPv4 隧道分为以下几种模式：

- 手动隧道
- 6to4 隧道
- ISATAP（Intra-Site Automatic Tunnel Addressing Protocol，站点内自动隧道 寻址协议）隧道

在上面列出的隧道模式中，手动隧道为配置隧道；IPv4 兼容 IPv6 自动隧道、6to4隧道及ISATAP 隧道为自动隧道。

1）. 手动隧道

手动隧道是点到点之间的链路，一条链路就是一个单独的隧道。主要用于边缘路由 器-边缘路由器或主机-边缘路由器之间定期安全通信的稳定连接，可实现与远端 IPv6 网络的连接。

2）. 6to4 隧道

6to4 隧道是点到多点的自动隧道，主要用于将多个IPv6 孤岛通过IPv4 网络连接到 IPv6 网络。6to4 隧道通过IPv6 报文的目的地址中嵌入的IPv4 地址，可以自动获取 隧道的终点。6to4 隧道采用特殊的地址：6to4 地址，其格式为：2002:abcd:efgh: 子网号::接口ID/64，其中abcd:efgh 表示该6to4 隧道对应的32 位IPv4 源地址，用 16 进制表示（如1.1.1.1 可以表示为0101:0101）。通过这个嵌入的IPv4 地址可以 自动确定隧道的终点，使隧道的建立非常方便。

由于 6to4 地址的 64 位地址前缀中的 16 位子网号可以由用户自定义，前缀中的前 48 位已由固定数值、隧道起点或终点设备的IPv4 地址确定，使IPv6 报文通过隧道 进行转发成为可能。6to4 隧道可以实现 IPv6 网络的互连，克服了 IPv4 兼容 IPv6 自动隧道使用的局限性。

3）. ISATAP 隧道

随着IPv6 技术的推广现有的IPv4 网络中将会出现越来越多的IPv6 主机，ISATAP 隧道技术为这种应用提供了一个较好的解决方案。ISATAP 隧道是点到点的自动隧 道技术，通过在IPv6 报文的目的地址中嵌入的IPv4 地址，可以自动获取隧道的终 点。使用 ISATAP 隧道时，IPv6 报文的目的地址和隧道接口的 IPv6 地址都要采用 特殊的地址：ISATAP 地址。ISATAP 地址格式为：Prefix(64bit):0:5EFE:ip-address。 ip-address 形式为a.b.c.d 或者abcd:efgh，其中abcd:efgh 表示32 位IPv4 源地址。 通过这个嵌入的 IPv4 地址就可以自动建立隧道，完成 IPv6 报文的传送。ISATAP 隧道主要用于在IPv4 网络中IPv6 路由器-IPv6 路由器、主机-路由器的连接。

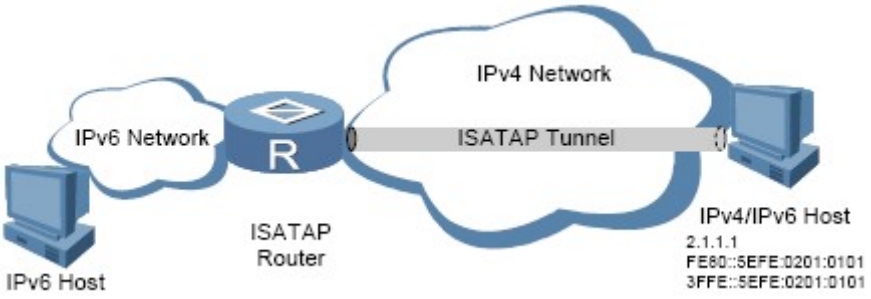


图 7-8 ISATAP 隧道

7.2 配置IPv6

7.2.1 配置IPv6单播地址

IPv6 站点本地地址和全球单播地址可以通过下面两种方式配置：

- 采用EUI-64 格式形成当配置采用EUI-64 格式形成IPv6 地址时接口的IPv6 地址的前缀是所配置的前缀，而接口标识符则由接口的链路层地址转化而来。
- 手工配置：用户手工配置IPv6 站点本地地址或全球单播地址。

IPv6 的链路本地地址可以通过两种方式获得：

- 自动生成：设备根据链路本地地址前缀（FE80::/64）及接口的链路层地址， 自动为接口生成链路本地地址；
- 手动指定：用户手工配置IPv6 链路本地地址。

说明：

- 当接口配置了 IPv6 站点本地地址或全球单播地址后，同时会自动生成链路本地地址。且与采用**ipv6 address auto link-local** 命令生成的链路本地地址相同。 此时如果手工指定接口的链路本地地址，则手工指定的有效。如果删除手工指定 的链路本地地址，则接口的链路本地地址恢复为系统自动生成的地址。
- 配置链路本地地址时，手工指定方式的优先级高于自动生成方式。即如果先采用自动生成方式，之后手工指定，则手工指定的地址会覆盖自动生成的地址；如果 先手工指定，之后采用自动生成的方式，则自动配置不生效，接口的链路本地地 址仍是手工指定的.此时如果想要改为自动配置,则必须先删除手工指定的地址， 再配置采用自动生成的方式。
- 在 LoopBack 接口视图下配置 IPv6 站点本地地址或全球单播地址时，只能配置 128 位的前缀长度。

注意：

1）本设备只支持手动配置 IPv6 全球单播地址或站点本地地址 IPv6 地址；

2）本设备自动生成接口的 IPv6 链路本地地址，无需配置。

表7-5 配置IPv6 单播地址

操作	命令	说明
进入配置模式	**configure terminal**	
进入接口模式	**interface** *interface-type interface-number*	

配置IPv6 全球单播地址或站点本地地址	手工指定IPv6 地址	**ipv6 address** *ipv6-address/prefix-length*	二者必选其一 缺省情况下，接口没有配置站点本地地址和全球单播地址
	采用EUI-64 格式形成IPv6 地址	**ipv6 address** *ipv6-address/prefix-length* **eui-64**	
配置IPv6 链路本地地址	配置自动生成链路本地地址	**ipv6 address** *ipv6-address* **link-local**	可选 缺省情况下，当接口配置了IPv6 站点本地地址或全球单播地址后，同时会自动生成链路本地
	手工指定接口的链路本地地址	**ipv6 address auto link-local**	

7.2.2 配置IPv6邻居发现协议

用户可以根据实际情况，配置接口是否发送RA消息及发送RA消息的时间间隔，同 时可以配置RA消息中的相关参数以通告给主机。当主机接收到RA消息后，就可以 采用这些参数进行相应操作。可以配置的RA消息中的参数及含义如表1-8所示。

表7-6 RA 消息中的参数及描述

参数	描述
前缀信息（Prefix Information）	在同一链路上的主机收到设备发布的前缀信息后，可以进行无状态 自动配置等操作
被管理地址配置标志位（M flag）	用于确定主机是否采用有状态自动配置获取IPv6 地址 如果设置该标志位为1，主机将通过有状态自动配置（例如DHCP 服务器）来获取IPv6 地址；否则，将通过无状态自动配置获取IPv6 地址，即根据自己的链路层地址及路由器发布的前缀信息生成IPv6 地址
其他配置标志位（O flag）	用于确定主机是否采用有状态自动配置获取除IPv6 地址外的其他信息 如果设置其他配置标志位为1，主机将通过有状态自动配置（例如DHCP 服务器）来获取除IPv6 地址外的其他信息；否则，将通过无 状态自动配置获取其他信息
路由器生存时间（**ra-lifetime**）	用于设置发布RA 消息的路由器作为主机的默认路由器的时间，主 机根据接收到的RA 消息中的路由器生存时间参数值，就可以确定 是否将发布该RA 消息的路由器作为默认路由器
邻居请求消息重传时间间隔（**ra-interval**）	设备发送NS 消息后，如果未在指定的时间间隔内收到响应，则会 重新发送NS 消息
保持邻居可达状态的时间（**reachable-time**）	当通过邻居可达性检测确认邻居可达后，在所设置的可达时间内， 设备认为邻居可达；超过设置的时间后，如果需要向邻居发送报文， 会重新确认邻居是否可达

说明：

在接口上配置的邻居请求消息重传时间间隔及保持邻居可达状态的时间，既可作为 RA 消息中的信息发布给主机也可作为本接口发送邻居请求消息的时间间隔及保持 邻居可达状态的时间。

注意：

RA 消息发布的最大间隔时间应该小于或等于RA 消息中路由器的生存时间。

表7-7 配置RA 消息的相关参数

操作	命令	说明
进入配置模式	**configure terminal**	-
进入接口视图	**interface** *interface-type interface-number*	-
取消对RA 消息发布的抑制	**ipv6 nd send-ra**	必选 缺省情况下，抑制发布RA 消息
配置RA 消息发布的时间间隔	**ipv6 nd ra-interval SECONDS**	可选 缺省情况下，RA 消息发布最大时间间隔为600 秒，最小时间间隔为200 秒 RA 消息周期性发布时，相邻两次的时间间隔是在最大时间间隔与最小时间间隔之间随机选取一个值作为周期性发布RA 消息的时间间隔 配置的最小时间间隔应该小于等于最大时间间隔的0.75 倍；RA 消息发布的最大实际间隔应该小于或等于RA 消息中路由器的生存时间
配置RA 消息中的前缀信息	**ipv6 nd prefix-advertisement IPV6PREFIX VALID PREFERRED [onlink] [autoconfig]**	可选 缺省情况下,没有配置RA 消息中的前缀信息，此时将使用发送RA 消息的接口IPv6 地址作为RA 消息中的前缀信息
配置被管理地址配置标志位为1	**ipv6 nd managed-config-flag**	可选 缺省情况下被管理地址标志位为0，即主机通过无状态自动配置获取IPv6 地址
配置其他配置标志位为1	**ipv6 nd other-config-flag**	可选 缺省情况下，其他配置标志位为 0，即主机通过无状态自动配置获取其他信息
配置RA 消息中路由器的生存时间	**ipv6 nd ra-lifetime SECONDS**	可选 缺省情况下，RA 消息中路由器的生存时间为1800 秒 RA 消息中路由器的生存时间应该大于或等于RA 消息的发布时间间隔
配置邻居请求消息重传时间间隔	**ipv6 nd ra-interval SECONDS**	可选 缺省情况下,接口发送NS 消息的间间隔为1000 毫秒，接口发布的RA 消息中Retrans Timer 字段的

配置保持邻居可达状态的时间	**ipv6 nd reachable-time MILLISECONDS**	可选 缺省情况下接口保持邻居可达状 态的时间为30000 毫秒，接口发布的RA 消息中Reachable Timer 字段的值为0

7.2.3 配置IPv6静态路由

表7-8 配置IPv6 静态路由

操作	命令	说明
进入配置模式	**configure terminal**	
配置 IPv6 静态路由	**ipv6 route X:X::X:X/M (X:X::X:X |INTERFACE_NAME) [<1-255> <1-100>]**	
取消 IPv6 静态路由配置	**no ipv6 route X:X::X:X/M (X:X::X:X |INTERFACE_NAME)**	
显示 IPv6 路由表	**show ipv6 route**	

7.2.4 配置IPv4/IPv6双协议栈

为了实现双协议栈功能,必须先使能IPv6 功能。否则即使配置了接口的IPv6 地址，仍无法转发IPv6 的报文。

表7-9 配置双协议栈

操作	命令	说明
进入配置模式	**configure terminal**	
使能IPv6 功能	**ipv6 enable**	必选 缺省情况下，IPv6 功能处于关闭状态
进入接口视图	interface interface-type interface-number	-
配置接口的 IPv4 地址	ip address ip-address ip-address/prefix-length	必选 缺省情况下，接口没有配置IPv4 地址
配置接口的 IPV6 地址	ipv6 address ipv6-address/prefix-length	缺省情况下，接口没有配置 IPv6 站点本地地址和

		全球单播地址

8 配置 ARP

8.1 ARP概述

IP 数据包常通过以太网发送。以太网设备并不识别 32 位 IP 地址：它们是以 48 位以太网地址(MAC 地址)传输以太网数据包的。因此，IP 驱动器必须把 IP 地址转换成 MAC 地址。在这两种地址之间存在着某种静态的或算法的映射，常常需要查看一张表。地址解析协议(Address Resolution Protocol，ARP)就是用来确定这些映象的协议。

通常设备的 arp 表是动态从网络中获得，但有很多场景需要在无法获得外界 arp 的情况下向外发生数据，这就需要静态 ARP 功能来完成。静态 ARP 是强制绑定某 IP 地址与某 MAC 地址的功能，通过该功能可以完成黑洞路由、直接发送 IP 数据等功能。

8.2 添加静态ARP

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	arp static A.B.C.D HH-HH-HH-HH-HH-HH	配置静态ARP
步骤3	end	回到特权模式

8.3 删除静态ARP

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	no arp static A.B.C.D HH-HH-HH-HH-HH-HH	删除指定的静态ARP
步骤3	end	回到特权模式

8.4 常见故障分析

8.4.1 故障现象：

现象	添加静态 ARP 对端网络不通
分析	可能是静态ARP IP地址与对端网络IP相同导致冲突

解决	删除静态 ARP，直接使用对端网络中 IP 地址

9 配置 DHCP 服务器

9.1 DHCP服务概述

本设备提供两种 DHCP 服务功能：DHCP 服务器和 DHCP Relay。

9.1.1 DHCP 服务器概述

DHCP 的全称是动态主机配置协议（Dynamic Host Configuration Protocol）。设备可以作为 DHCP Server，用于实现对网络中 IP 地址的动态分配和集中管理。动态分配是指当 DHCP 客户端第一次从 DHCP Server 租用到 IP 地址后，并非永久的使用该地址，只要租约到期，客户端就要释放(Release)这个 IP 地址以给其它工作站使用。为了实现 IP 地址的动态分

配，必须设置 DHCP Server 拥有一个 IP 地址范围，用来分配给用户，这个用来分配给客户端的地址范围也叫 IP 地址池（IP Pool）。

下图反映了 DHCP 客户端从 DHCP 服务器申请 IP 地址的过程。主机 A（客户端）先广播 DHCPDISCOVER 包寻找网络上的 DHCP 服务器，DHCP 服务器向客户端单播包含配置参数的 DHCPOFFER 消息。

图9-1 DHCP 客户端从 DHCP 服务器申请 IP 地址

- 当客户端第一次登录到网络时，它会向网络广播一个 DHCPDISCOVER 消息，此时由于客户端还不知道自己属于哪一个网路，所以封包的来源地址为 0.0.0.0，目的地址则为 255.255.255.255。
- 由于网络上可能不止一个 DHCP 服务器，凡是具有有效 IP 地址信息的 DHCP 服务器均从各自还没有租出的地址中选择一个空闲 IP，然后将该提议回应给客户端。
- 客户端从接收到的第一个提议中选定 IP 地址信息，并广播一条租用地址的消息请求。由发出该提议的 DHCP 服务器响应该消息，确认已接受请求并开始租用。
- 客户端收到确认后开始使用此地址

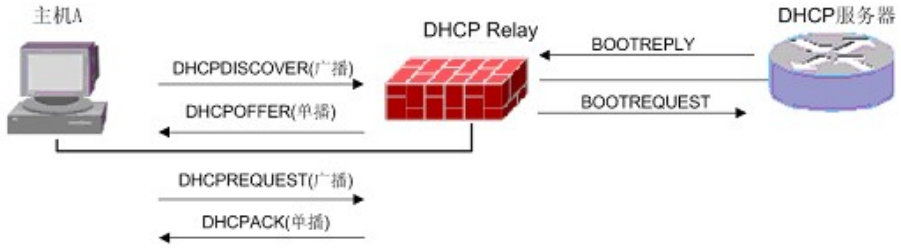
注意

DHCP 客户端可以接收多个 DHCP 服务器的消息，自己从中选一个 DHCP 服务器，同时也暗示它拒绝了其它 DHCP 服务器应答的配置参数。

9.1.2 DHCP Relay概述

DHCP Relay 是用来将一个网段的 DHCP 请求转发给其它网段的 DHCP Server，由其它网段的 DHCP Server 分配 IP 地址。DHCP Relay 存在的原因是因为 DHCP 客户端还没有 IP 环境设定，这时由 DHCP Relay 来接管客户的 DHCP 请求然后将 DHCP 消息传递给 DHCP Server，再将 DHCP 服务器的应答消息传给客户端，客户端获得 IP 地址。当然也可以在每一个网段之中安装 DHCP Server 但这样的话设备成本会增加而且管理上面也比较分散。DHCP Relay 的工作原理如下图所示：

图9-2 DHCP 客户端通过 Relay 从 DHCP 服务器申请 IP 地址



9.2 配置DHCP Server

图 16-3 反映了 DHCP 客户端从 DHCP 服务器申请 IP 地址的过程。主机 A（客户端）先广播 DHCPDISCOVER 包寻找网络上的 DHCP 服务器，DHCP 服务器向客户端单播包含配置参数的 DHCPOFFER 消息。

图9-3 DHCP 客户端从 DHCP 服务器申请 IP 地址

- 当客户端第一次登录到网络时，它会向网络广播一个 DHCPDISCOVER 消息，此时由于客户端还不知道自己属于哪一个网络，所以封包的来源地址为 0.0.0.0，目的地址则为 255.255.255.255。
- 由于网络上可能不止一个 DHCP 服务器，凡是具有有效 IP 地址信息的 DHCP 服务器均从各自还没有租出的地址中选择一个空闲 IP，然后将该提议回应给客户端。
- 客户端从接收到的第一个提议中选定 IP 地址信息，并广播一条租用地址的消息请求。由发出该提议的 DHCP 服务器响应该消息，确认已接受请求并开始租用。
- 客户端收到确认后开始使用此地址。


注意

DHCP 客户端可以接收多个 DHCP 服务器的消息，自己从中选一个 DHCP 服务器，同时也暗示它拒绝了其它 DHCP 服务器应答的配置参数。

9.2.2 在接口上指定DHCP Server服务

配置步骤

步骤1	(config)# interface IFNAME	进入相应接口
步骤2	(config-if)# dhcpserver enable	在该接口上指定DHCP Server
步骤3	(config-if)# no dhcpserver enable	在该接口上取消DHCP Server


注意

只有在该接口上指定了 DHCPServer 服务，DHCP Server 才会处理该接口的 DHCP 请求。系统初始时 DHCP Server 不处理所有接口的 DHCP 请求。

DHCP SERVER 支持物理接口，VLAN 接口和 trunk 接口。

9.2.3 配置DHCP Server服务子网

配置步骤

步骤1	(config)# dhcp	进入DHCP配置模式
步骤2	(config-dhcp)# share-net NAME subnet A.B.C.D/M	增加子网及其SUBNET
步骤3	(config-dhcp)# no share-net NAME subnet	删除子网SUBNET
步骤4	(config-dhcp)# no share-net NAME	删除子网所有配置

9.2.4 配置DHCP Server地址池及其租约

配置步骤

步骤1	(config-dhcp)# share-net NAME A.B.C.D E.F.G.H infinite	增加子网的地址池,其租约为无限
步骤2	(config-dhcp)# share-net NAME A.B.C.D A.B.C.D <0-100> days <0-23> hours <0-59> mins	增加子网的地址池,其租约为所配置的时间
步骤3	(config-dhcp)# no share-net NAME A.B.C.D E.F.G.H	删除子网的地址池

注意

每个子网只可以有 1 个地址池。 infinite 意味租约期为无限。若租约不为 infinte，则其取值范围为 5 分钟至 100 天。

9.2.5 配置DHCP 子网缺省网关

配置步骤

步骤1	(config-dhcp)# share-net NAME router A.B.C.D	配置子网的缺省网关
步骤2	(config-dhcp)# no share-net NAME router	取消子网的缺省网关

9.2.6 配置DHCP 子网DNS服务器

配置步骤

步骤1	(config-dhcp)# share-net NAME dns A.B.C.D [E.F.G.H]	配置子网的DNS服务器
步骤2	(config-dhcp)# no share-net NAME dns	取消子网的DNS服务器

9.2.7 配置DHCP 子网WINS服务器

配置步骤

步骤1	(config-dhcp)# share-net NAME wins A.B.C.D [E.F.G.H]	配置子网的WINS服务器
步骤2	(config-dhcp)# no share-net NAME wins	取消子网的WINS服务器

9.2.8 配置DHCP 子网域名

配置步骤

步骤1	(config-dhcp)# share-net NAME domain NAME	配置子网的域名
步骤2	(config-dhcp)# no share-net NAME domain	取消子网的域名

9.2.9 配置DHCP 地址绑定

DHCP Server 可以设置指定的 IP 地址与指定的 MAC 地址捆绑，指定的 MAC 地址与 IP 地址一一对应，并且关联对应 DHCP 服务器，每条绑定项都有指定的绑定名称。

配置步骤

步骤1	(config-dhcp)# bind NAME HH-HH-HH-HH-HH-HH A.B.C.D NAME	设置地址绑定
步骤2	(config-dhcp)# no bind NAME	取消地址绑定

9.2.10 配置DHCP 地址排除

DHCP Server 可以设置保留的地址范围，这些保留的地址将不会分配给 DHCP 客户端。

配置步骤

步骤1	(config-dhcp)# exclude 10.0.0.0 10.0.0.11	设置地址排除
步骤2	(config-dhcp)# no exclude 10.0.0.0 10.0.0.11	取消地址排除

9.3 DHCP服务监控

9.3.1 DHCP Debug

步骤1 显示当前 DHCP 的 debug 情况

```
FW# show dhcp debug
```

步骤2 打开 DHCP debug 开关

```
FW# debug dhcp event
FW# debug dhcp packet detail
FW# show debug
DHCP debugging status:
  DHCP event debugging is on
  DHCP packet debugging is on
```

步骤3 关闭 dhcp debug

```
FW# no debug dhcp
FW# show dhcp debug
```

9.3.2 显示DHCP Server配置信息

步骤1 显示当前 DHCP 的配置及开关情况

```
FW# show dhcp config
```

```
dhcp
exclude 10.0.0.2 10.0.0.3
 exclude 10.0.0.5 10.0.0.10
 bind aaa 11:22:33:44:55:66 1.1.1.1 server-1
 bind bindtable 00:16:76:65:30:9c 192.168.6.169 server-2
 share-net aaa subnet 10.0.0.0/24
 share-net aaa 10.0.0.3 10.0.0.10 7 days 3 hours 5 mins
 share-net aaa router 10.0.0.1
 share-net aaa dns 203.196.0.3
 share-net aaa wins 10.0.0.1
 share-net bbb subnet 192.168.6.1/24
 share-net bbb 192.168.6.171 192.168.6.173 infinite
 share-net bbb router 192.168.6.1
 share-net bbb dns 203.196.0.3
 share-net bbb wins 192.168.0.1
```

9.3.3 显示DHCP Server地址分配信息

步骤1 显示当前的地址租约以及客户端信息

```
FW# show dhcp ip active
------------------------------
ipaddr:       192.168.2.4
macaddr:      00-0d-60-78-81-75
start_time:    2007-01-01 05:22:43
end_time:     2007-01-01 05:27:43
interface:    bvi2
FW# show dhcp ip free
------------------------------
ipaddr:       192.168.2.3
macaddr:      00-16-76-65-3b-3c
start_time:    2007-01-01 05:17:49
end_time:     2007-01-01 05:22:49
interface:    bvi2
FW# show dhcp ip summary

  General Statistics
    Active IP      :   1
    Abandoned IP   :   0
    Expired Leases :   1

  Usage by Network :
    Network      Netmask     Active  Abandoned  Expired
```

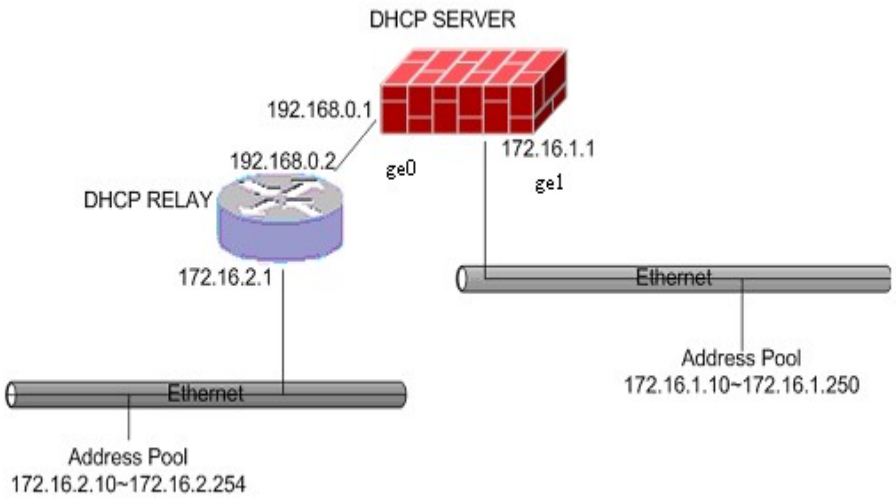
	192.168.2.1	255.255.255.0	1	0	1

9.4 配置案例

案例描述：

配置设备（DHCP Server）给两个子网分配 IP 地址，如下图所示，172.16.1.0/16 为直接相连的子网，172.16.2.0/16 为通过另一台设备（DHCP Relay）连接的子网。

图9-4 DHCP 服务配置案例组网图



配置步骤：

步骤**1**	配置图中DHCP SERVER所在的设备上接口IP地址
	FW_A(config) interface ge0
	FW_A (config- ge0) ip address 192.168.0.1/24
	FW_A (config- ge0) dhcpserver enable
	FW_A (config) interface ge1
	FW_A (config- ge1) ip address 172.16.1.1/24
	FW_A (config- ge1) dhcpserver enable
	FW_A (config) exit
	FW_A (config) ip route 172.16.2.0/24 192.168.0.2
	FW_A (config) exit
步骤**2**	配DHCP相关参数

	FW_A (config)dhcp
	FW_A (config-dhcp)share-net ge1 subnet 172.16.1.0/24
	FW_A (config-dhcp)share-net ge1 router 172.16.1.1
	FW_A (config-dhcp)share-net ge1 dns 202.99.16.1
	FW_A (config-dhcp)share-net ge1 172.16.1.10 172.16.1.250 infinite
	FW_A (config-dhcp)share-net ForRelay subnet 172.16.2.0/24
	FW_A (config-dhcp)share-net ForRelay 172.16.2.10 172.16.2.254 infinite
	FW_A (config-dhcp)exit
步骤3	配置dhcp relay
	FW_A (config)# interface ge1
	FW_A (config-ge1)# dhcprelay 192.168.0.1
	FW_A (config-ge1)# exit
	FW_A(config)# policy 1 any any any any any always permit
	FW_A(config-policy)# enable
	FW_A(config-policy)# exit

10 配置静态路由

10.1 静态路由概述

静态路由是在路由器中人工配置的固定路由条目。除非网络管理员干预，否则静态路由不会发生变化。由于静态路由不能对网络的改变作出反映，一般用于网络规模不大、拓扑结构固定的网络中。静态路由的优点是简单、高效、可靠。在所有的路由中，静态路由优先级最高。

设备静态路由支持对路由的健康检查，通过配置健康检查策略，支持对静态路由状态进行监测。当健康检查失败后，会将路由状态置为失效，从而避免数据转发到不可用的下一跳上。

10.2 配置静态路由

静态路由是由用户配置的路由。当用户确信到达某个网段应该先转发到某个地址时，可以通过 ip route 命令配置这个静态路由，同时可以配置该静态路由的权重(1-100)，用于负载分担。静态路由支持健康检查。当健康检查对象失效以后，使对应的静态路由无效。

配置静态路由的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	ip route A.B.C.D/M (A.B.C.D|INTERFACE) [monitor MONITOR] [<distance> <weight>]	配置静态路由
步骤3	exit	退出配置模式
步骤4	show ip route	显示静态路由信息

参数说明：

ip route：

参数	说明	缺省配置
A.B.C.D/M	目的地址	无
(A.B.C.D|INTERFACE)	路由网关地址或者出接口	无
MONITOR	引用健康检查模板，当前支持tcp和icmp两种类型，检查路由下一跳的健康状态	无，缺省不进行健康检查
<distance>	路由优先级，范围<1-255>	1
<weight>	路由权重，范围1-100	1

10.3 配置缺省路由

有一类特殊的路由称为默认路由（或缺省路由），即目的地址和掩码为 0.0.0.0/0 的路由。它可以匹配任何目的地址，所以每个找不到对应路由的报文都将按默认路由转发。通常默认路由都是在用户认为有必要时通过静态路由配置的。在网络有一个唯一出口连接到其他网络时，配置默认路由是很有用的，它可以使设备所需要的路由数量大大降低。

配置缺省路由的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	ip route 0.0.0.0/0 (A.B.C.D|INTERFACE) [monitor MONITOR] [<distance> <weight>]	配置缺省路由
步骤3	end	退出配置模式

10.4 配置信息显示命令

表 10-1 显示静态路由信息

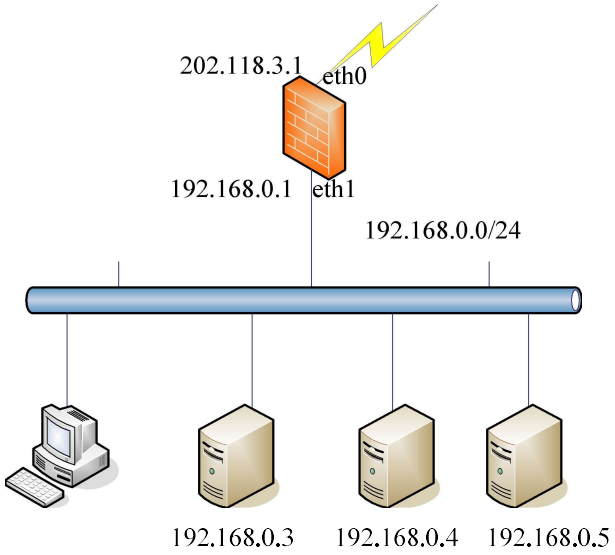
命令	解释
show ip route	显示路由信息

10.5 配置案例

10.5.1 配置缺省路由

案例描述：

配置缺省路由，把每个没有对应路由的报文转发到公网地址 202.118.3.2



配置案例：

步骤1	配置缺省路由
	FW_A(config)# ip route 0.0.0.0/0 202.118.3.2
步骤2	配置接口参数
	FW_A(config)# interface eth0 FW_A(config-eth0)#ip address 202.118.3.1/24 FW_A(config)# interface eth1 FW_A(config-eth1)#ip address 192.168.0.1/24
步骤3	查看路由表
	FW_A# show ip route Codes: K - kernel route, C - connected, S - static, I - ISP, R - RIP, O - OSPF, D - DHCP, P - PPPOE, > - selected route, * - FIB route C>* 127.0.0.0/8 is directly connected, lo weight: 0 K>* 127.0.0.1/32 is directly connected, lo weight: 0 C>* 192.168.0.0/24 is directly connected, eth1 weight: 0 K>* 192.168.0.1/32 is directly connected, eth1 weight: 0 C>* 202.118.3.0/24 is directly connected, eth0 weight: 0 K>* 202.118.3.1/32 is directly connected, eth0 weight: 0

10.6 常见故障

10.6.1 路由状态为失效状态

故障现象	配置了静态路由后，路由状态显示为失效状态

分析	若静态路由没有配置健康检查，从以下几点分析： 1. 路由配置的下一跳地址对应出接口down。 2. 依据路由配置的下一跳地址查找不到出接口。 3. 相同路由情况下，有管理距离更优的路由。 若静态路由配置了健康检查，除了上述内容外，还需要从以下几点分析： 1. 检查健康检查日志，是否由于路由健康检查失败导致的静态路由失效。 2. 检查是否健康检查模板覆盖IP地址配置了非下一跳的IP地址。 3. 检查是否健康检查的配置的超时时间和重试次数过短，健康检查报文在超时时间内没有返回则认为健康检查失败。
解决	检查上面分析中的配置是否正确。

11 配置管理路由

11.1 管理路由概述

管理路由是在路由器中人工配置的固定路由条目。除非网络管理员干预，否则管理路由不会发生变化。由于管理路由等同于静态路由，不能对网络的改变作出反映，一般用于网络规模不大、拓扑结构固定的网络中。管理路由的作用域为管理员的管理数据流量，对业务流量无效，所以被称之为管理路由。管理路由的特点是只对从管理接口进入的管理流量起作用。

11.2 配置管理路由

管理路由是由用户配置的路由。当用户确信到达某个管理员网段应该先转发到某个地址时，可以通过 mangement route 命令配置这个管理路由。

配置静态路由的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	management route A.B.C.D/M A.B.C.D	配置管理路由
步骤3	exit	退出配置模式
步骤4	show ip fib route	显示管理路由信息

参数说明：

management route：

参数	说明	缺省配置
A.B.C.D/M	目的地址	无
(A.B.C.D|INTERFACE)	路由网关地址或者出接口	无

11.3 配置管理接口

管理接口是由用户配置指定的管理流量的出入口。

配置缺省路由的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface IFNAME	进入某一个interface
步骤3	port type mgt	指定当前接口为管理接口
步骤4	end	退到特权模式下
步骤5	show run interface	显示配置

11.4 配置信息显示命令

表 10-2 显示管理路由信息

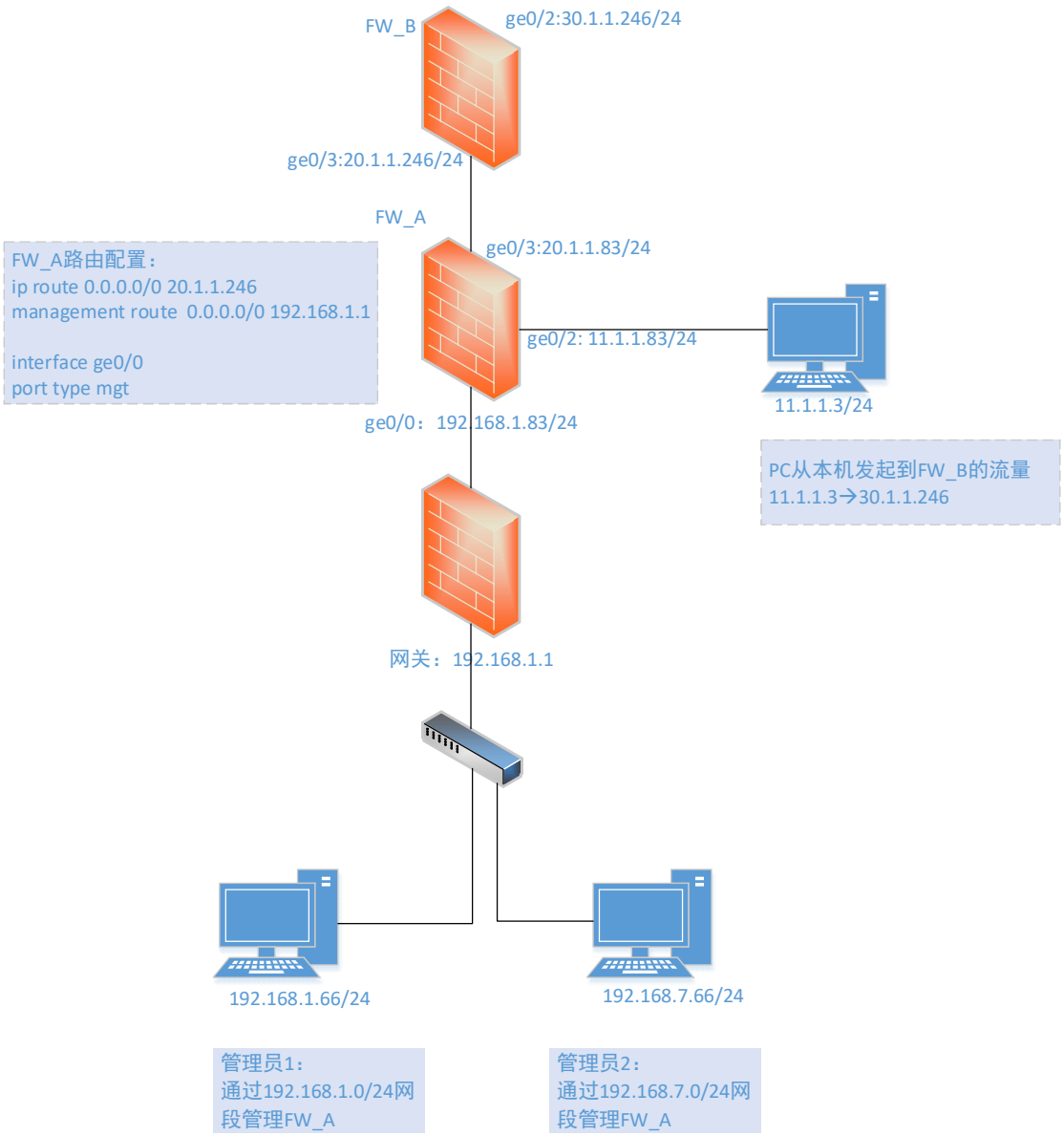
命令	解释
show ip fib route	显示路由信息

11.5 配置案例

11.5.1 配置管理路由

案例描述：

用户希望通过网关 FW_A 上的默认路由来访问 FW_B 后的资源；同时，不同网络的管理员，能够通过管理口访问管理 FW_A 设备，两者互不影响。此案例我们可通过管理路由隔离功能来实现。



配置案例：

步骤1	配置管理路由
	FW_A(config)# management route 0.0.0.0/0 192.168.1.1
步骤2	配置接口参数
	FW_A(config)# interface ge0/0
	FW_A(config-ge0/0)#ip address 192.168.1.83/24
	FW_A(config-ge0/0)#port type mgt
	FW_A(config)# interface ge0/2
	FW_A(config- ge0/2)#ip address 11.1.1.83/24
	FW_A(config)# interface ge0/3
	FW_A(config- ge0/3)#ip address 20.1.1.83/24

步骤3	查看路由表
	FW_A# show ip fib route Table 1, 0.0.0.0/0 gate 192.168.1.1 oif ge0/0 Table 1, 192.168.1.0/24 gate 192.168.1.83 oif ge0/0 Table 254, 127.0.0.0/8 gate 127.0.0.1 oif lo Table 254, 20.1.1.0/24 gate 20.1.1.83 oif ge0/3 Table 254, 11.1.1.0/24 gate 11.1.1.83 oif ge0/2 Table 255, 127.0.0.1/32 oif lo Table 255, 20.1.1.83/32 oif ge0/3 Table 255, 11.1.1.83/32 oif ge0/2 Table 255, 192.168.1.83/32 oif ge0/0

11.6 常见故障

11.6.1 路由状态为失效状态

故障现象	配置了管理路由后，show ip fib route没有显示配置的管理路由
分析	从以下几点分析： 1. 路由配置的下一跳地址对应出接口down。 2. 依据路由配置的下一跳地址查找不到出接口。 3. 路由配置的下一跳地址对应的出接口没有配置为管理接口。
解决	检查上面分析中的配置是否正确。

12 配置 RIP

12.1 RIP协议概述

RIP 协议是基于 D-V 算法（又称为 Bellman-Ford 算法）的内部动态路由协议，简称 IGP（Interior Gateway Protocol）,它通过 UDP 数据报文交换路由信息。D-V 算法又称为距离向量算法,这种算法在 ARPARNET 早期就用于计算机网络的路由的计算。RIP 协议在目前已成为路由器、主机路由信息传递的标准之一，是最广泛使用的 IGP 之一，被大多数 IP 路由器商业卖主广泛使用。RIP 协议被设计用于使用同种技术的中型网络，因此适应于大多数的校园网和使用速率变化不是很大的连续线的地区性网络。对于更复杂的环境，一般不使用 RIP 协议。

RIP 协议使用跳数来衡量到达信宿机的距离称为路由权，RIP 协议使用两种形式的报文：路径信息请求报文和路径信息响应报文。在路由器端口第一次启动时，将会发送请求报文。路径信息响应报文包含了实际的路由信息，以每 30 秒的间隔发送给相邻端口。在 RIP 协议中，还使用了水平分割、毒性逆转机制来防止路由环的形成，并且使用触发更新和路由超时机制确保路由的正确性。

12.2 配置RIP

12.2.1 缺省配置信息

防火墙设备关于 RIP 的缺省设置信息如以下表格所示：

表 12-1 RIP 缺省配置信息

内容	缺省设置	备注
使能/禁止状态（enable/disable）	disable	可更改设置
接口认证类型（none/text/md5）	none	可更改设置
版本	2	可更改设置
定时更新时间	30秒	建议采用缺省设置
超时时间	180秒	建议采用缺省设置
垃圾收集时间	120秒	建议采用缺省设置

12.2.2 配置启用RIP路由协议功能

启用 rip 路由协议，在此基础上才能对 rip 路由功能作进一步配置

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router rip	启用rip功能并进入rip配置节点

在配置模式下使用 no router rip 可以取消对 rip 的设置，使其恢复到缺省配置。

参数说明：

命令（1）：router NAME

参数	说明	缺省配置
NAME	路由协议类型	无


注意

只有在启用 rip 以后才能对 rip 其他功能作进一步配置。

12.2.3 配置RIP版本

RIP 的版本配置，在接口没有做出版本配置的情况下控制 RIP 协议收发报文的版本信息。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router rip	启用rip功能并进入rip配置模式
步骤3	version 1	配置收发报文版本为1
步骤4	end	回到enable模式
步骤5	show running-config	show命令

使用 no version 可以取消对 version 的设置，使其恢复到缺省配置 2。

参数说明：

命令（1）：version <1-2>

参数	说明	缺省配置
<1-2>	Rip版本	2

12.2.4 配置RIP发布的网络

把系统所在的直连网络发布出去，使其他路由器能够学到到达本地网络的路由。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router rip	启用rip功能并进入rip配置模式

步骤3	network 202.38.168.1/24	配置向外发布网络202.38.168.1/24
步骤4	end	回到enable模式
步骤5	show ip rip	show命令

使用 no network 202.38.168.1/24 可以取消对 202.38.168.1/24 的设置，使其不发布 202.38.168.1/24 的路由。

参数说明：

命令（1）：network <A.B.C.D/M>

参数	说明	缺省配置
<A.B.C.D/M>	需要发布的网络	无

12.2.5 配置RIP发布缺省路由

配置一条 0.0.0.0/0 的路由发布出去。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router rip	启用rip功能并进入rip配置模式
步骤3	default-information originate	配置发布缺省路由
步骤4	end	回到enable模式
步骤5	show ip rip	show命令

使用 no default-information originate 可以取消发布缺省路由的设置。

12.2.6 配置RIP默认的重发布度量

重发布某种类型时如果没有配置本身的重发布度量，就是用默认的度量值。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router rip	启用rip功能并进入rip配置模式
步骤3	default-metric 3	配置默认的重发布度量为3
步骤4	end	回到enable模式
步骤5	show ip rip	show命令

使用 no default-metri 可以取消对默认度量的设置，使其恢复到默认值 1。

参数说明：

命令（1）：default-metric <1-16>

参数	说明	缺省配置
<1-16>	默认的重发布度量值	1

12.2.7 配置RIP定时器触发时间

RIP 会根据定时更新时间周期的向外发布整个路由表，如果超时时间到达时还没有收到某条路由的更新，就把这条路由从内核路由表中删除，并把 metric 置为 16 向外发布，并设置垃圾收集定时器；垃圾收集时间到达时，把这条路由在 rip 路由表中删除。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router rip	启用rip功能并进入rip配置模式
步骤3	timers basic 5 30 20	配置定时器触发时间为5 30 20秒
步骤4	end	回到enable模式
步骤5	show ip rip	show命令

使用 no timers basic 可以取消对定时器触发时间的设置，使其恢复到默认值 30 秒 180 秒 120 秒。

参数说明：

命令（1）：timers basic <5- 2147483647> <5- 2147483647> <5- 2147483647>

参数	说明	缺省配置
<5- 2147483647>	定时更新时间	30秒
<5- 2147483647>	超时时间	180秒
<5- 2147483647>	垃圾收集时间	120秒

12.2.8 配置RIP定时器触发时间

重发布路由可以把例如静态、直连、ospf 的路由引入到 rip 中向外发布。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router rip	启用rip功能并进入rip配置模式
步骤3	redistribute connected metric 3	配置重发布直连路由，度量为3
步骤4	end	回到enable模式
步骤5	show ip rip	show命令

使用 no redistribute connected 可以取消直连路由的重发布。

参数说明：

命令（1）：redistribute （connected|static|ospf）[metric <1-16>]

参数	说明	缺省配置
（connected|static|ospf）	路由类型	无
<1-16>	重发布度量	1

12.2.9 配置RIP接口收发报文版本

对每个接口设置特有的收发报文版本。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router rip	启用rip功能并进入rip配置模式
步骤3	ip rip eth1 send version 1	配置接口eth1的发送版本为1
步骤4	end	回到enable模式
步骤5	show ip rip	show命令

使用 no ip rip eth1 send version 可以取消对接口 eth1 发送版本的配置，使其恢复到默认值。

参数说明：

命令（1）：ip rip NAME (send|receive) version <1-2>

参数	说明	缺省配置
NAME	接口名	无
(send|receive)	动作类型	无
<1-2>	版本	2

12.2.10 配置RIP接口的认证类型

对每个接口设置特有的收发报文认证。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router rip	启用rip功能并进入rip配置模式
步骤3	ip rip eth1 authentication md5 12345	配置接口eth1为md5认证，认证密码为12345
步骤4	end	回到enable模式
步骤5	show running-config	show命令

使用 no ip rip eth1 authentication 可以取消对接口 eth1 认证的配置，使其恢复到默认值无认证。

参数说明：

命令（1）：ip rip NAME authentication (md5|text) NAME

参数	说明	缺省配置
NAME	接口名	无
(md5|text)	认证类型	无
NAME	认证密码	无

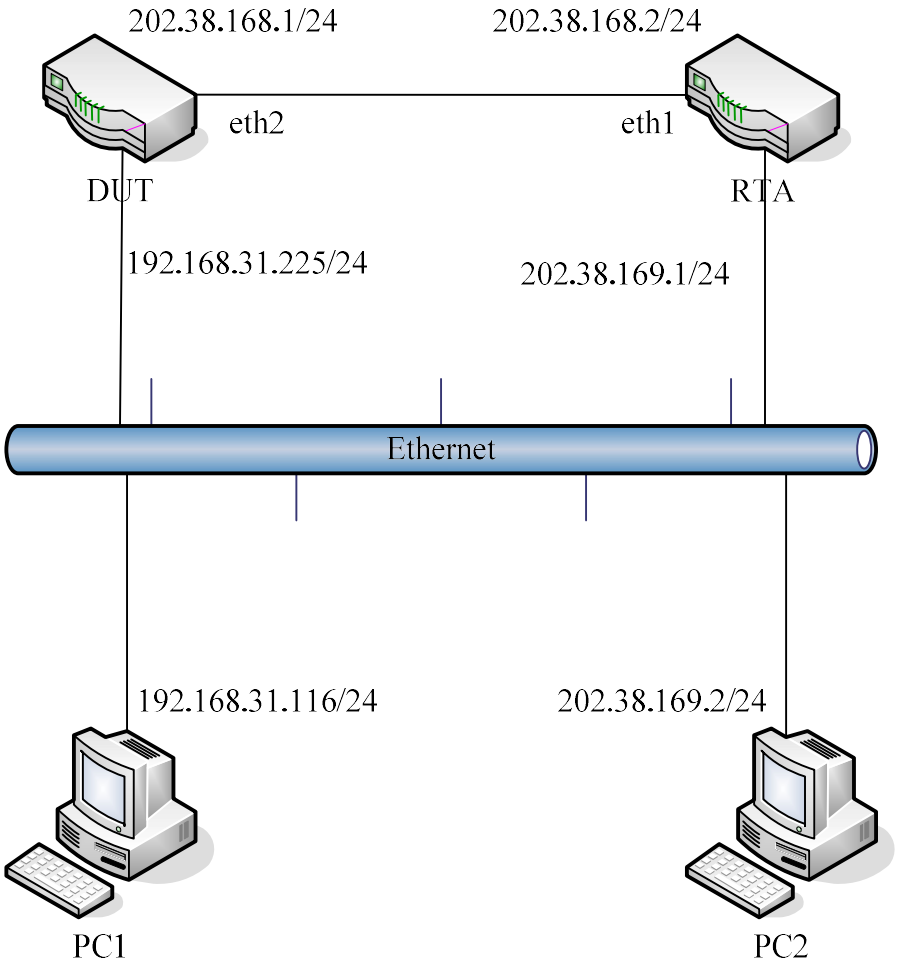
12.3 配置案例

12.3.1 配置案例：两台USG设备通过RIP路由协议互通

案例描述

DUT 和 RTA 都为防火墙设备，IP 地址配置如图，DUT 在 eth0 和 eth2 接口上启用了 RIP，RTA 在接口 eth0 和 eth1 上启用了 RIP，两个设备的互连的接口收发报文的版本都设置为 2。

案例组网图



配置步骤：

步骤1	DUT的配置
	FW# configure terminal FW(config)# router rip FW(router-rip)# network 202.38.168.1/24 FW(router-rip)# network 192.168.31.225/24 FW(router-rip)# ip rip eth2 send version 2 FW(router-rip)# ip rip eth2 receive version 2 FW(router-rip)# end FW#

步骤2	RTA的配置

```
FW# configure terminal
FW(config)# router rip
FW(router-rip)# network 202.38.168.2/24
FW(router-rip)# network 202.38.169.1/24
FW(router-rip)# ip rip eth1 send version 2
FW(router-rip)# ip rip eth1 receive version 2
FW(router-rip)# end
FW#
```

步骤3	DUT执行show running-config

步骤4	RTA执行show running-config

配置结果：

DUT 的 show running-config 信息

router rip

network 202.38.168.1/24

network 192.168.31.225/24

ip rip eth2 send version 2

ip rip eth2 receive version 2

!

RTA 的 show running-config 信息

router rip

network 202.38.168.2/24

network 202.38.169.1/24

ip rip eth1 send version 2

ip rip eth1 receive version 2

12.4 RIP监控与维护

12.4.1 查看 RIP路由表

介绍常用的 show 命令的使用

查看 RIP 路由表的步骤：

步骤1	显示rip路由表

```
FW# show ip route rip
Codes: R - RIP, C - connected, O - OSPF, B - BGP
```

```
(n) - normal, (s) - static, (d) - default, (r) - redistribute,
(i) - interface
     Network          Next Hop         Metric From          Time
R(s) 0.0.0.0/0        0.0.0.0             1 self
C(r) 192.168.31.0/24  0.0.0.0             1 self
C(i) 202.38.168.0/24  0.0.0.0             1 self
FW#
```

可以看出RIP路由表中有三条路由，两个直连路由192.168.31.0/24和192.168.31.0/24，度量为1，还有一个默认路由。

12.4.2 查看 RIP配置

介绍常用的 show 命令的使用

查看 RIP 配置的步骤：

步骤1 察看RIP的配置

```
Routing Protocol is "rip"
  Sending updates every 5 seconds with +/-50%, next due in 2 seconds
  Timeout after 30 seconds, garbage collect after 20 seconds
  Default redistribution metric is 1
  Redistributing: connected
  Default version control: send version 2, receive version 2
    Interface        Send  Recv
    eth2             2     2
  Routing for Networks:
    202.38.168.1/24
  Routing Information Sources:
    Gateway          BadPackets BadRoutes  Distance Last Update
  Distance: (default is 120)
FW#
```

可以看出定时器时间设置为5秒30秒和20秒，默认重发布路由度量为1，重发布了直连路由，接口2的收发版本都为2，配置网络202.38.168.1/24向外发布。

12.4.3 查看调试信息

debug rip events

debug rip packet

debug rip packet (send | revc)

debug rip zebra

应用环境

给出何时需要使用该调试命令。

debug rip events 可以查看 RIP 运行时各个事件

debug rip packet 可以查看 RIP 收发报文的信息

debug rip zebra 可以查看陆由变更时发生的事件

调试实例

给出使用该调试命令显示的信息。重要的显示信息用**黑体字**标识。

```
FW# debug rip packet
FW# debug rip events
update timer fire!
SEND UPDATE to eth2 ifindex 3
multicast announce on eth2
update routes on interface eth2 ifindex 3
SEND to socket 11 port 520 addr 224.0.0.9
SEND RESPONSE version 2 packet size 44
   0.0.0.0/0 -> 0.0.0.0 family 2 tag 0 metric 1
   192.168.31.0/24 -> 0.0.0.0 family 2 tag 0 metric 3

Rip_read!
ignore packet comes from myself, 202.38.168.1
update timer fire!
SEND UPDATE to eth2 ifindex 3
multicast announce on eth2
update routes on interface eth2 ifindex 3
SEND to socket 11 port 520 addr 224.0.0.9
SEND RESPONSE version 2 packet size 44
   0.0.0.0/0 -> 0.0.0.0 family 2 tag 0 metric 1
   192.168.31.0/24 -> 0.0.0.0 family 2 tag 0 metric 3

Rip_read!
ignore packet comes from myself, 202.38.168.1
```

结果分析：

对以上调试实例进行必要的分析，当出现不是预期情况的处理方法。

■ RIP 会定时在各个接口发布更新报文，也会收到其他设备发送来的更新报文。

只有高级用户才可以使用此命令，由于此命令会在命令行上打印大量信息，占用很多 CPU 资源因此强烈建议用户，当调试结束时，一定要用 no debug rip (events|packet|zebra)命令禁用此功能。

12.5 常见故障分析

12.5.1 故障现象：两台设备不能正常通信

现象	两台设备不能正常通信
分析	互连接口收发版本不匹配，认证类型不匹配，接口配置是否正确
解决	检查接口配置，修改接口配置

13 配置 OSPF

13.1 OSPF协议概述

OSPF(Open Shortest Path First)是动态路由协议,其功能是实现网际间的路由。

OSPF 是一个自治系统内部路由协议，用于在单一自治系统(autonomous system,AS)内计算产生路由。与 RIP 等距离向量路由协议不同的是，OSPF 是基于链路状态的路由协议。它能够在网络链路变化时快速产生新路由，并能够管理比 RIP 范围更大的网络自治系统。

OSPF 是自治系统内部使用的链路状态路由协议，OSPF 通过路由器之间通告链路状态信息（LSA），来建立链路状态数据库，然后就可以根据 SPF 算法计算出到每个结点的最短路径树了，进而可计算出路由。它的工作方式与我们熟悉的 RIP 和 IGRP 协议不同，OSPF 只须发送当前结点到相邻结点的路由结构信息，而 RIP 和 IGRP 需要结点把自己保留的路由表或路由表的一部分全部发送到相邻结点，相邻结点根据这些信息更新自己的路由表，显然 OSPF 协议发送的信息量少，而 RIP 发送的信息量较多。在通告的链路状态结构中，OSPF 协议支持 IP 子网结构。

OSPF 向相邻的路由器定期发送一个 hello 报文，并接收邻居路由器发来的 hello 报文。这个 hello 报文不但可以帮助路由器在初始工作时了解相邻结构，而且可以在运行中了解相邻路由器的工作情况，如果相邻的路由器关机了，或链路不通了，就不会从相应邻居那里收到 hello 报文了，从而能够很快知道哪些路由器不能工作了，能够对网络拓扑结构的变化做到快速反应。

如果网络支持多个路由器，可以实现在一个网段的诸多 OSPF 路由器中选择一个指定路由器 DR 和一个备份指定路由器 BDR，在进行链路数据库同步时，由指定路由器向整个网络发送 LSA，以减少流量开销。

13.2 配置OSPF

13.2.1 缺省配置信息

防火墙设备关于 OSPF 的缺省设置信息如以下表格所示：

表 13-1 OSPF 缺省配置信息

内容	缺省设置	备注
使能/禁止状态（enable/disable）	disable	可更改设置
OSPF区域认证类型（none/text/md5）	不认证	可更改设置
接口认证类型（none/text/md5）	不认证	可更改设置
发布缺省路由	不发布	可更改设置
OSPF路由的优先级	110	可更改设置
spf-delay值和spf-holdtime值	spf-delay：5秒 spf-holdtime：10秒	建议采用缺省设置
兼容rfc1583	不兼容	可更改设置

LSA重传时间	5秒	建议采用缺省设置
LSA发送延迟	1秒	建议采用缺省设置
Hello-interval值	10秒	可更改设置
Dead-interval值	4 * Hello-interval	可更改设置
接口选举DR的优先级	1	可更改设置
OSPF区域路由聚合	不聚合	可更改设置
重发布其他路由协议路由的路由类型	第2类外部路由	可更改设置

13.2.2 配置启用OSPF路由协议功能

启用 OSPF 路由协议，在此基础上才能对 OSPF 路由功能作进一步配置

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router ospf	启用OSPF功能并进入OSPF配置节点

在配置模式下使用 no router OSPF 可以取消对 OSPF 的设置，使其恢复到缺省配置。

参数说明：

命令（1）：router NAME

参数	说明	缺省配置
NAME	路由协议类型	无

注意

只有在启用 OSPF 以后才能对 OSPF 其他功能作进一步配置。

13.2.3 配置OSPF路由器Router-ID

OSPF 协议需要路由器的 Router-ID，作为本路由器在自治系统中的唯一标识。一般在协议任务启动后，会自动选出一个 Router-ID。通常路由器先挑选 IP 地址最大的环回地址。若无环回地址，则选择状态 up 的接口地址大的作为本路由器的 Router-ID，也可以指定一个 Router-ID。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router ospf	启用OSPF功能并进入OSPF配置模式
步骤3	router-id 1.1.1.1	配置路由器Router-ID
步骤4	end	回到enable模式
步骤5	show ip ospf	show命令

使用 no router-id 可以取消对 router-id 的设置， router-id 将会重新自动选举。

参数说明：

命令（1）：router-id A.B.C.D

参数	说明	缺省配置
A.B.C.D	OSPF Router-ID	

13.2.4 配置运行OSPF的接口

配置运行 OSPF 的接口以及其所属的区域。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router ospf	启用OSPF功能并进入OSPF配置模式
步骤3	network 10.0.1.0/24 area 0	从属于10.0.1.0/24接口上启用OSPF,其所属的区域为0
步骤4	end	回到enable模式
步骤5	show ip ospf	show命令

使用 no network 10.0.1.0/24 area 0 可以取消设置。

参数说明：

命令（1）：network A.B.C.D/M area (A.B.C.D|<0-4294967295>)

参数	说明	缺省配置
<A.B.C.D/M>	接口所属的网段	无
(A.B.C.D|<0-4294967295>)	区域ID	无

13.2.5 配置OSPF区域认证方式

OSPF 支持在同一区域内进行认证。一个区域中所有的路由器的认证类型必须一致（不认证、明文认证、MD5 密文认证）。认证提供基于密码的保护，防止未经授权对区域进行的访问。在配置区域认证时，必须对区域的所有接口单独配置认证密码。当接口的认证方式和接口所在区域的认证不一致时，优先考虑接口配置的认证方式。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router ospf	启用OSPF功能并进入OSPF配置模式
步骤3	area 0 authentication	配置区域0的认证方式为明文认证
步骤4	end	回到enable模式
步骤5	show ip ospf	show命令

使用 no area (A.B.C.D|<0-4294967295>) authentication 可以取消区域认证的设置，恢复为默认值不认证。

参数说明：

命令（1）：area (A.B.C.D|<0-4294967295>) authentication [message-digest]

参数	说明	缺省配置
(A.B.C.D|<0-4294967295>)	区域ID	无
message-digest	密文认证方式	没有这个参数表示明文认证

13.2.6 配置OSPF NSSA

自治系统外的ASE路由不可以进入到NSSA区域中，但是NSSA区域内的路由器引入的ASE路由可以在NSSA中传播并发送到区域之外。由于是作为OSPF标准协议的一种扩展属性，应尽量减少与不支持该属性的路由器协调工作时的冲突和兼容性问题。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router ospf	启用OSPF功能并进入OSPF配置模式
步骤3	area 1 nssa translate-candidate	配置区域1为nssa区域，并且该设备参与是否将7类lsa转为5类的选举
步骤4	end	回到enable模式
步骤5	show ip ospf	show命令

使用 no area 1 nssa 可以取消该区域的 nssa 属性设置。

参数说明：

命令（1）：area (A.B.C.D|<0-4294967295>) nssa (translate-candidate|translate-never|translate-always) [no-summary]

参数	说明	缺省配置
(A.B.C.D|<0-4294967295>)	区域ID	无
(translate-candidate|translate-never|translate-always)	NSSA区域的ABR是否进行7转5操作。非ABR该参数无意义。	缺省为translate-candidate，表示从ABR中选出一个来进行7转5操作。
[no-summary]	配置该参数的话，ABR会将3类LSA也过滤掉不传入NSSA区域	可选配置。

注意

1、 如果某个区域内的路由器配置了该属性，该区域内的所有路由器都要配置该属性。

2、 在改变该属性时，需要重新启动 ospf

13.2.7 配置OSPF区域间路由聚合

区域间的路由聚合是为了减少区域间路由数量，它使 ABR 通告一条聚合的域间路由到其他区域，而被聚合的路由不被宣告出去。在 OSPF 中，ABR 向其他区域发送路由信息时，以网段为单位生成 Type 3 LSA。如果该区域中存在一些连续的网段，则可以配置 ABR 将这些连续的网段聚合成一个网段。这样 ABR 只发送一条聚合后的 LSA，所有落入本命令指定的聚合网段范围的 LSA 将不再会被单独发送出去，这样可减少其他区域中链路状态数据库（LSDB）的规模。如果该网段范围用关键字 not-advertise 限定，则到这一个网段路由的聚合路由将不会被广播出去。这个网段是由 IP 地址/掩码的方式说明的。接收聚合网段和对网段的限定，可减少区域间路由信息的交流量。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router ospf	启用OSPF功能并进入OSPF配置模式
步骤3	area 0 range 10.0.0.0/16	设置聚合路由通告的区域和地址范围
步骤4	end	回到enable模式
步骤5	show running-config ospf	show命令

使用 no area (A.B.C.D|<0-4294967295>) range A.B.C.D/M.可以设置。

参数说明：

命令（1）：area (A.B.C.D|<0-4294967295>) range A.B.C.D/M [not-advertise]

参数	说明	缺省配置
(A.B.C.D|<0-4294967295>)	进行聚合的区域ID	
A.B.C.D/M	地址范围	
[not-advertise]	不宣告聚合后的路由	

命令（2）：area (A.B.C.D|<0-4294967295>) range A.B.C.D/M advertise cost <0-16777215>

参数	说明	缺省配置
(A.B.C.D|<0-4294967295>)	进行聚合的区域ID	
A.B.C.D/M	地址范围	
<0-16777215>	聚合路由的宣告Metric	

命令（3）：area (A.B.C.D|<0-4294967295>) range A.B.C.D/M substitute A.B.C.D/M

参数	说明	缺省配置
(A.B.C.D|<0-4294967295>)	进行聚合的区域ID	1
A.B.C.D/M	地址范围	
A.B.C.D/M	将地址范围替换成该地址宣告	

可以使用 no area (A.B.C.D|<0-4294967295>) range A.B.C.D/M advertise cost 取消路由聚合宣告的 cost。

13.2.8 配置OSPF路由重分布

为了能够使得多个路由协议同时运作，可以将一种路由协议的信息引入到另一种路由协议中，这个过程可以称为路由重分布。运行 OSPF 的自治系统可以引入自治系统外部的其他路由协议的路由或者静态路由以达到路由信息共享。当路由器运行 OSPF 且还运行其他路由协议，若要引入外部路由信息，需要配置路由重分布。

OSPF 使用 4 类不同的路由，按优先级由高到低排列如下：

区域内路由

区域间路由

第一类外部路由

第二类外部路由

区域内和区域间路由描述自治系统内部的网络结构；外部路由则描述了如何选择到自治系统以外的路由。第一类外部路由是指接收的是 IGP 路由（例如 RIP、STATIC），由于这类路由的可信程度较高，所以，计算出的外部路由的花费与自治系统内部的路由花费的数量级相同，并且与 OSPF 自身路由的花费具有可比性，即到第一类外部路由的花费值＝本路由器到相应的 ASBR 的花费值＋ASBR 到该路由目的地址的花费值。第二类外部路由器是指接收的是 EGP 路由，由于这类路由的可信度比较低，所以 OSPF 协议认为，从 ASBR 到自治系统之外的花费远远大于在自治系统之内到达 ASBR 的花费，计算路由花费时主要考虑前者。即第二类外部路由的花费值＝ASBR 到该路由目的地址的花费值。如果该值相等，再考虑本路由器到相应的 ASBR 的花费值。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router ospf	启用OSPF功能并进入OSPF配置模式

步骤3	redistribute connected metric 11 metric-type 1	配置重发布值直连路由，Metric为11，第一类外部路由
步骤4	end	回到enable模式
步骤5	show running-config ospf	show命令

使用 no redistribute (connected|static|rip)可以取消路由重发布的设置。

参数说明：

命令（1）：redistribute (connected|static|rip) metric <1-16777214> metric-type (1|2)

参数	说明	缺省配置
(connected|static|rip)	重发布路由的类型	无
<1-16777214>	重发布的路由的Metric	无
(1|2)	重发布路由的类型	第二类外部路由

13.2.9 配置OSPF重发布路由缺省Metric

配置 OSPF 重发布外部路由时的缺省 Metric。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router ospf	启用OSPF功能并进入OSPF配置模式
步骤3	default-metric 100	配置重发布路由的缺省Metric为100
步骤4	end	回到enable模式
步骤5	show running-config ospf	show命令

使用 no default-metric 可以取消该设置。

参数说明：

命令（1）：default-metric <1-16777214>

参数	说明	缺省配置
<1-16777214>	重发布路由的默认Metric	无

13.2.10 配置OSPF重发布默认路由

一旦配置了路由重分布，路由器就自动成为自治系统边界路由器。但是缺省情况下，不会发布缺省路由，可以强制自治系统边界路由器发布缺省路由。但这时路由器表中必须包含缺省路由。如果路由表中没有缺省路由，而要强制自治系统边界路由器产生缺省路由，使用 always 参数。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router ospf	启用OSPF功能并进入OSPF配置模式
步骤3	default-information originate metric 100 metric-type 1	配置重发布默认路由，Metric为100，类型为第一类外部路由
步骤4	end	回到enable模式
步骤5	show running-config ospf	show命令

使用 no default-information originate 可以取消该项配置，使其恢复到默认值。

参数说明：

命令（1）：default-information originate metric <1-16777214> metric-type (1|2)

参数	说明	缺省配置
<1-16777214>	重发布默认路由的Metric。	无
(1|2)	重发布默认路由的类型	第二类外部路由

命令（2）：default-information originate always metric <1-16777214> metric-type (1|2)

参数	说明	缺省配置
always	强制发布默认路由，即使路由表中没有默认路由。	无
<1-16777214>	重发布默认路由的Metric。	无
(1|2)	重发布默认路由的类型	第二类外部路由

13.2.11 配置OSPF协议优先级

一个协议的优先级指的是一个路由信息来源的可信度等级。优先级是一个 1 到 255 的整数，通常情况下，值越高可信度越低。值为 255 就意味着路由信息源根本不可信，应该被忽略。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router ospf	启用OSPF功能并进入OSPF配置模式
步骤3	distance <1-255>	配置OSPF的管理距离（协议优先级）
步骤4	end	回到enable模式
步骤5	show running-config ospf	show命令

使用 no distance 可以取消配置，使其恢复到默认值 110。

参数说明：

命令（1）：distance <1-255>

参数	说明	缺省配置
<1-255>	接口名	无

命令（2）：distance ospf intra-area <1-255> inter-area <1-255> external <1-255>

参数	说明	缺省配置
<1-255>	域内路由的OSPF优先级	110
<1-255>	域间路由的OSPF优先级	110
<1-255>	AS外部路由的OSPF优先级	110

13.2.12 配置OSPF兼容RFC1583

配置路由器计算外部到 ASBR 的路径时是否兼容 RFC1583 的规定，当有多条到达 ASBR 的 AS 内部路径时：

兼容 RFC1583，直接判断多条路由的距离值

不兼容 RFC1583，始终优先选择非骨干区域的区域内路径。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router ospf	启用OSPF功能并进入OSPF配置模式
步骤3	compatible rfc1583	设置兼容rfc1583
步骤4	end	回到enable模式
步骤5	show ip ospf	show命令

使用 no compatible rfc1583 可以取消兼容 rfc1583 的配置，使其恢复到默认值不兼容 rfc1583。

13.2.13 配置OSPF路由计算定时器

配置 ospf 接收拓扑结构改变之后和启动最短路径优先（OSPF）之间的延迟时间和配置连续两次 SPF 计算之间的时间。

配置步骤：

步骤1	configure terminal	进入配置模式

步骤2	router ospf	启用OSPF功能并进入OSPF配置模式
步骤3	timers spf 10 20	设置spf-delay为10秒，设置spf-holdtime为20秒
步骤4	end	回到enable模式
步骤5	show ip ospf	show命令

使用 no timers spf 可以取消该配置，使其恢复到默认值 spf-delay 为 5 秒，spf-holdtime 为 10 秒。

参数说明：

命令（1）：timers spf <0-4294967295> <0-4294967295>

参数	说明	缺省配置
<0-4294967295>	spf-delay值	5秒
<0-4294967295>	spf-holdtime值	10秒

13.2.14 配置OSPF接口认证方式

OSPF 支持接口间的邻居在建立邻居关系的时候进行认证，防止非法设备接入网络。OSPF 支持两种认证模式：明文认证和 MD5 认证。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	interface ge0	进入接口ge0进行OSPF配置
步骤3	ip ospf authentication	设置接口认证方式为明文认证
步骤4	end	回到enable模式
步骤5	show running-config	show命令

使用 no ip ospf authentication 可以取消该配置，使其恢复到默认值不认证。

参数说明：

命令（1）：ip ospf authentication [message-digest]

参数	说明	缺省配置
[message-digest]	不用该参数表示明文认证，使用该参数表示密文认证	不认证

13.2.15 配置OSPF接口明文认证密钥

配置 OSPF 接口上用于明文认证的密钥。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	interface ge0	进入接口ge0进行OSPF配置
步骤3	ip ospf authentication-key aaa	设置接口明文认证密钥
步骤4	end	回到enable模式
步骤5	show running-config	show命令

使用 no ip ospf authentication-key 可以取消该配置，删除该认证密钥。

参数说明：

命令（1）：ip ospf authentication-key AUTH_KEY

参数	说明	缺省配置
AUTH_KEY	配置用于明文认证的密钥	不认证

13.2.16 配置OSPF接口密文认证密钥

配置 OSPF 接口上用于密文认证的密钥。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	interface ge0	进入接口ge0进行OSPF配置
步骤3	ip ospf message-digest-key 1 md5 aaa	设置接口认证方式为明文认证
步骤4	end	回到enable模式
步骤5	show running-config	show命令

使用no ip ospf message-digest-key <1-255>可以取消该配置，删除该认证密钥。

参数说明：

命令（1）：ip ospf message-digest-key <1-255> md5 KEY

参数	说明	缺省配置
<1-255>	配置key-ID	无
KEY	密文认证的密钥	无

13.2.17 配置OSPF接口的优先级

网络支持多个路由器，可以实现在一个网段的诸多 OSPF 路由器中选择一个指定路由器 DR 和一个备份指定路由器 BDR，在进行链路数据库同步时，由指定路由器向整个网络发送 LSA，以减少流量开销。

路由器接口的优先级决定了该接口在选举 DR 时所具有的资格，优先级高的在选举权发生冲突时首先考虑。DR 不是人为指定的，而是由本网段中所有的路由器共同选举出来的。本网段内优先级大于 0 的路由器都可以作为“候选人”。在所有自称是 DR 的路由器中选取优先级最大的；若两台路由器的优先级相等，则选 Router ID 最大的为 DR。在选举 DR 的同时也选举出 BDR，BDR 也和本网段内的所有路由器建立邻接关系并交换路由信息。当 DR 失效后，BDR 会立即成为 DR，由于不需要重新选举，并且邻接关系事先已经建立，所以这个过程是非常短暂的。这个时候还需要再重新选举出一个新的 BDR，虽然一样需要较长的时间，但并不会影响路由的计算。网段中的 DR 并不一定是 priority 最大的路由器；同理，BDR 也并不一定就是 priority 第二大的路由器。

DR 是指某个网段中的概念，是针对路由器的接口而言的。某台路由器在一个接口上可能是 DR，在另一个接口上可能是 BDR，或者是 DRother。

只有在广播或者 NBMA 类型接口时才会选举 DR，在点到点或者点到多点类型的接口上不需要选举 DR。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	interface ge0	进入接口ge0进行OSPF配置
步骤3	ip ospf priority <0-255>	设置接口的优先级
步骤4	end	回到enable模式
步骤5	show running-config ospf	show命令

使用 no ip ospf priority 可以取消该配置，使其恢复到默认值。

参数说明：

命令（1）：ip ospf priority <0-255>

参数	说明	缺省配置
<0-255>	接口优先级	无

13.2.18 配置OSPF接口发送报文的开销

用户可以指定接口发送报文的开销，否则 OSPF 会根据当前的接口自动计算开销。

配置步骤：

步骤1	configure terminal	进入配置模式

步骤2	interface ge0	进入接口ge0进行OSPF配置
步骤3	ip ospf cost <1-65535>	设置接口发送报文开销
步骤4	end	回到enable模式
步骤5	show ip ospf interface	show命令

使用 no ip ospf cost 可以取消该配置。

参数说明：

命令（1）：ip ospf cost <1-65535>

参数	说明	缺省配置
<1-65535>	接口发送报文的开销	无

13.2.19 配置OSPF接口LSA重传间隔

当一台路由器向他的邻居发送一条 LSA 后，需要等待对方的确认报文。若在规定的时间内没有收到对方的确认报文，就会重传这条 LSA。用户可以对 retransmit-internal 的值进行配置。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	interface ge0	进入接口ge0进行OSPF配置
步骤3	ip ospf retransmit-interval <3-65535>	设置接口LSA重传间隔
步骤4	end	回到enable模式
步骤5	show ip ospf interface	show命令

使用 no ip ospf retransmit-interval 可以取消该配置，使其恢复到默认值 5 秒。

参数说明：

命令（1）：ip ospf retransmit-interval <3-65535>

参数	说明	缺省配置
<3-65535>	LSA重传间隔时间	5秒

13.2.20 配置OSPF接口LSA发送延迟

在发送链路状态更新报文（LSU）时，对报文中 LSA 的老化时间增加 transmit-delay 秒。该参数的配置主要考虑到接口上发送报文的所需的时间。LSA 在本路由器的“链路状态数据库”（LSDB）中会随着时间老化（age 每秒钟加 1），但在网络的传输过程中却不会。所以有必要在发送之前将老化时间增加

transmit?-delay 秒，这一点对于低速网络更为重要。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	interface ge0	进入接口ge0进行OSPF配置
步骤3	ip ospf transmit-delay <1-65535>	设置接口LSA发送延迟
步骤4	end	回到enable模式
步骤5	show ip ospf interface	show命令

使用 no ip ospf transmit-delay 可以取消该配置，使其恢复到默认值。

参数说明：

命令（1）：ip ospf transmit-delay <1-65535>

参数	说明	缺省配置
<1-65535>	接口LSA发送延迟	1秒

13.2.21 配置OSPF接口Hello报文定时器

Hello 报文是最常用的一种报文，它周期性地被发送至邻居路由器，用于发现与维护邻居关系，选举 DR 与 BDR。用户可以对发送 Hello 报文的时间间隔 Hello-interval 的值进行配置。值越小，网络的变化将被越快的发现，但将花费更多的网络的传输。同一网段的路由器的 Hello-interval 必须相同。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	interface ge0	进入接口ge0进行OSPF配置
步骤3	ip ospf hello-interval <1-65535>	设置接口Hello报文发送定时器
步骤4	end	回到enable模式
步骤5	show ip ospf interface	show命令

使用 no ip ospf hello-interval 可以取消该配置，使其恢复到默认值 10 秒。

参数说明：

命令（1）：ip ospf hello-interval <1-65535>

参数	说明	缺省配置
<1-65535>	Hello报文发送间隔时间	10秒

13.2.22 配置OSPF接口邻居失效定时器

相邻路由器间的失效时间是指在该时间间隔内若未收到对方的 hello 报文，则认为对端路由器失效。用户可以对邻居路由器的失效时间 Dead-interval 的值进行配置。Dead-interval 的值至少是 Hello-interval 值的 4 倍，同一网段的路由器的 Dead-interval 也必须相同。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	interface ge0	进入接口ge0进行OSPF配置
步骤3	ip ospf dead-interval <1-65535>	设置接口邻居失效间隔时间
步骤4	end	回到enable模式
步骤5	show ip ospf interface	show命令

使用 no ip ospf dead-interval 可以取消该配置，使其恢复到默认值 40 秒。

参数说明：

命令（1）：ip ospf dead-interval <1-65535>

参数	说明	缺省配置
<1-65535>	邻居失效间隔时间	40秒

13.2.23 配置接口的OSPF网络类型

缺省情况下，按不同介质可划分成下列三种网络：广播网络（以太网，令牌环网、FDDI），非广播多路访问网络（帧中继、X.25），点到点网络（HDLC、PPP）。对以上任一类网络都可以进行 OSPF 配置。可以不考虑缺省的介质类型，选择配置 OSPF 网络类型。利用这一点，可将非广播多路访问网络配置为广播网络，如 X.25 和帧中继允许 OSPF 在其上以广播型运行，这就不用再去配置邻居。可将广播网络配置为非广播多路访问网络，例如当网络中有不支持组播传送地址的路由器时。对于不具有广播和组播能力的网络，必须配置对端邻居来指定发送 hello 报文，并可以指定邻居的优先级和轮询时间间隔。

点到多点是具有一个或者多个邻居的编号的点到点接口，它建立多主机路由。与非广播多路访问和点到点网络相比，点到多点网络具有以下优点：一到多接口更易于配置，因为它不需要配置邻居命令，只需要一个 IP 子网，所以不必分配路由选择。不需要全网络拓扑结构，开销较小。

USG 支持 OSPF 网络类型有广播型和点对点型。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	interface ge0	进入接口ge0进行OSPF配置

步骤3	ip ospf network (broadcast |point-to-point)	设置接口OSPF网络类型
步骤4	end	回到enable模式
步骤5	show ip ospf interface	show命令

使用 no ip ospf network 可以取消该配置。

参数说明：

命令（1）：ip ospf network (broadcast |point-to-point)

参数	说明	缺省配置
broadcast	设置接口OSPF网络类型为广播型网络。	
point-to-point	设置接口OSPF网络类型为点对点型网络。	

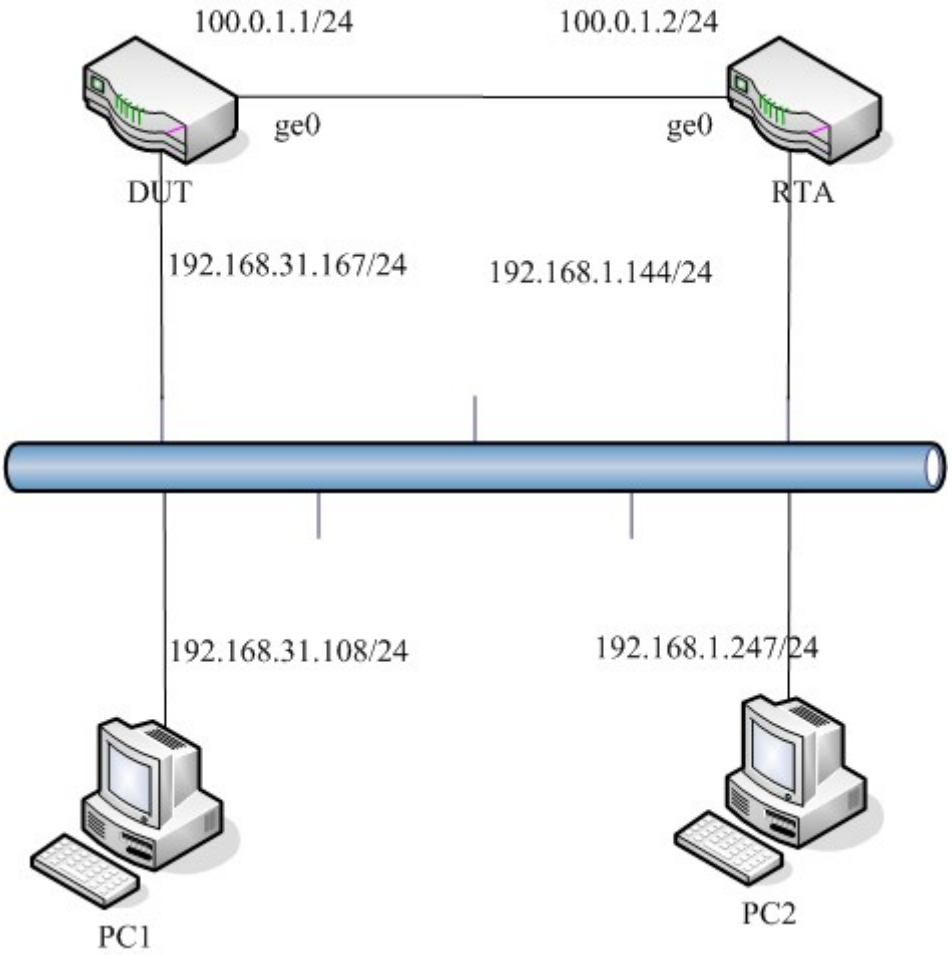
13.3 配置案例

13.3.1 配置案例：两台USG设备通过OSPF路由协议互通

案例描述

DUT 和 RTA 都为防火墙设备，IP 地址配置如图，通过在两台设备上使用 OSPF，DUT 设备能学到 192.168.1.0/24 网段的路由，RTA 能学到 192.168.31.0/24 网段的路由。

案例组网图



配置步骤：

步骤1	DUT的配置
	DUT# configure terminal DUT (config)# router ospf DUT (router- ospf)# network 192.168.31.0/24 area 0 DUT (router- ospf)# network 100.0.1.0/24 area 0 DUT (router- ospf)# end DUT#

步骤2	RTA的配置
	RTA# configure terminal RTA (config)# router ospf RTA (router-ospf)# network 192.168.1.0/24 area 0 RTA (router-ospf)# network 100.0.1.0/24 area 0 RTA (router-ospf)# end RTA#

步骤3	DUT#show ip route
步骤4	RTA#show ip route

配置结果：

DUT 的 show running-config ospf 信息：

```
router ospf
 network 100.0.1.0/24 area 0
 network 192.168.31.0/24 area 0
```

RTA 的 show running-config ospf

```
router ospf
 network 100.0.1.0/24 area 0
 network 192.168.1.0/24 area 0
```

13.4 OSPF监控与维护

13.4.1 查看 OSPF路由表

介绍常用的 show 命令的使用

查看 OSPF 路由表的步骤：

步骤1	显示OSPF路由表
	RTA# show ip route ospf N 100.0.1.0/24 [10] area: 0.0.0.0 directly attached to ge0 N 192.168.1.0/24 [10] area: 0.0.0.0 directly attached to ge1 N 192.168.31.0/24 [20] area: 0.0.0.0 via 100.0.1.1, ge0

13.4.2 查看OSPF信息

介绍常用的 show 命令的使用

查看 OSPF 信息的步骤：

步骤1	察看OSPF的信息
	RTA# show ip ospf OSPF Routing Process, Router ID: 200.0.0.1 Supports only single TOS (TOS0) routes This implementation conforms to RFC2328 RFC1583 Compatibility flag is disabled

```
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Refresh timer 10 secs
Number of external LSA 0
Number of areas attached to this router: 1

Area ID: 0.0.0.0 (Backbone)
   Number of interfaces in this area: Total: 2, Active: 2
   Number of fully adjacent neighbors in this area: 1
   Area has no authentication
   SPF algorithm executed 3 times
   Number of LSA 3
```

13.4.3 查看OSPF邻居信息

介绍常用的 show 命令的使用

查看 OSPF 邻居信息：

步骤1 察看OSPF邻居信息

```
RTA#  Neighbor  ID          Pri       State                 Dead  Time       Address
Interface                 RXmtL RqstL DBsmL
200.0.0.2                   1       Full/BDR              00:00:36         100.0.1.1
ge0:100.0.1.2             0       0       0
```

13.4.4 查看OSPF LSA数据库

介绍常用的 show 命令的使用

查看 OSPF LSA 数据库信息

步骤1 察看OSPF邻居信息

```
RTA# show ip ospf  database

                OSPF Router with ID (200.0.0.1)

                Router Link States (Area 0.0.0.0)
Link ID         ADV Router      Age  Seq#       CkSum  Link count
200.0.0.1       200.0.0.1       32 0x80000007 0x3e1f 2
200.0.0.2       200.0.0.2       10 0x80000006 0x251a 2

                Net Link States (Area 0.0.0.0)
Link ID         ADV Router      Age  Seq#       CkSum
100.0.1.2       200.0.0.1       32 0x80000003 0x7022
```

13.4.5 查看OSPF接口信息

介绍常用的 show 命令的使用

查看 OSPF 接口信息

步骤1	察看OSPF邻居信息
	RTA# show ip ospf interface ge0
	ge0 is up, line protocol is up Internet Address 100.0.1.2/24,Area 0.0.0.0 Router ID 200.0.0.1, Network Type BROADCAST, Cost: 10 Transmit Delay is 1 sec, State DR, Priority 1 Designated Router (ID) 200.0.0.1,Interface Address 100.0.1.2 Backup Designated Router (ID) 200.0.0.2,Interface Address 100.0.1.1 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5 Hello due in 00:00:05 Neighbor Count is 1, Adjacent neighbor count is 1

13.4.6 查看调试信息

debug ospf events

debug ospf packet (hello|dd|ls-request|ls-update|ls-ack|all)

debug ospf packet (hello|dd|ls-request|ls-update|ls-ack|all) (send|recv)

debug ospf packet (hello|dd|ls-request|ls-update|ls-ack|all) detail

debug ospf lsa (generate|flooding|install|refresh)

debug ospf ism (status|events|timers)

debug ospf nsm (status|events|timers)

debug ospf zebra (interface|redistribute)

应用环境

给出何时需要使用该调试命令。

debug ospf events 可以查看 OSPF 运行时各个事件

debug ospf packet (hello|dd|ls-request|ls-update|ls-ack|all)可以查看 OSPF 收发各类报文的信息

debug ospf packet (hello|dd|ls-request|ls-update|ls-ack|all) (send|recv)查看 OSPF 接收或者发送报文的信息。

debug ospf packet (hello|dd|ls-request|ls-update|ls-ack|all) detail 查看 OSPF 协议报文的详细必须 debug ospf packet (hello|dd|ls-request|ls-update|ls-ack|all) 或者 debug ospf packet (hello|dd|ls-request|ls-update|ls-ack|all) (send|recv)配

合使用才有效。

debug ospf lsa (generate|flooding|install|refresh)查看 LSA 各个阶段的情况。

debug ospf ism (status|events|timers)查看接口状态机的状态、事件和定时器情况。

debug ospf nsm (status|events|timers)查看邻居状态及的状态、事件和定时器的情况。

debug ospf zebra (interface|redistribute)查看接口状态和路由变更信息。

调试实例

DUT#debug ospf event
DUT#debug ospf packet hello
DUT# debug ospf packet hello detail
make_hello: options: 2, int: ge0:100.0.1.1
------------------------Dump Sent Packet Begin.----------------------------
Header
  Version 2
  Type 1 (Hello)
  Packet Len 48
  Router ID 200.0.0.2
  Area ID 0.0.0.0
  Checksum 0xa292
  AuType 0
Hello
  NetworkMask 255.255.255.0
  HelloInterval 10
  Options 2 (*|-|-|-|-|-|E|*)
  RtrPriority 1
  RtrDeadInterval 40
  DRouter 100.0.1.1
  BDRouter 100.0.1.2
  # Neighbors 1
    Neighbor 200.0.0.1
Hello sent to [224.0.0.5] via [ge0:100.0.1.1].
------------------------Dump Sent Packet End.----------------------------
------------------------Dump Received Packet Begin.----------------------------
Header
  Version 2
  Type 1 (Hello)
  Packet Len 48
  Router ID 200.0.0.1
  Area ID 0.0.0.0
  Checksum 0x0
  AuType 2
  Cryptographic Authentication
  Key ID 1
  Auth Data Len 16
  Sequence number 709641
Hello
  NetworkMask 255.255.255.0
  HelloInterval 10
  Options 2 (*|-|-|-|-|-|E|*)
  RtrPriority 1
  RtrDeadInterval 40
  DRouter 100.0.1.1
  BDRouter 100.0.1.2
  # Neighbors 1
    Neighbor 200.0.0.2

结果分析：

可以看到接收的 Hello 报文和发送的 Hello 报文的认证类型不一致，会导致邻接关系丢失。应该检查配置，使两边的认证类型统一。

只有高级用户才可以使用此命令，由于此命令会在命令行上打印大量信息，占用很多 CPU 资源因此强烈建议用户，当调试结束时，一定要用 no debug ospf 命令禁用此功能。

13.5 常见故障分析

13.5.1 故障现象1：两台设备不能建立邻接关系

现象	两台设备不能建立邻接关系
分析	1、 区域ID不匹配 2、 认证类型不匹配 3、 密钥不匹配 4、 网段（网络掩码匹配） 5、 Hello-interval不匹配 6、 Dead-interval不匹配 7、 两台设备间是否需要建立邻接关系
解决	1、 检查接口上OSPF参数的配置 2、 是否应该和邻居路由器建立一个邻接关系，满足下列条件中的一个或者多个，那么将建立邻接关系： A、 网络类型是点对点的 B、 网络类型是点到多点的 C、 网络类型是虚链路 D、 本地路由器是邻接路由器所在网络的 DR E、 本地路由器是邻接路由器所在网络的 BDR F、 邻居路由器是 DR G、 邻居路由器是 BDR

14 配置 BGP

14.1 BGP协议概述

BGP（Border Gateway Protocol）是一种不同自治系统的路由器之间进行通信的外部网关协议(Exterior Gateway Protocol，EGP)，其主要功能是在不同的自治系统(Autonomous Systems，AS)之间交换网络可达信息，并通过协议自身机制来消除路由环路。

BGP 使用 TCP 协议作为传输协议，通过 TCP 协议的可靠传输机制保证 BGP 的传输可靠性。

运行 BGP 协议的 Router 称为 BGP Speaker，建立了 BGP 会话连接(BGP Session)的 BGP Speakers 之间被称作对等体(BGP Peers)。 BGP speaker 之间建立对等体的模式有两种 ：IBGP(Internal BGP) 和 EBGP(External BGP)。IBGP 是指在相同 AS 内建立的 BGP 连接，EBGP 是指在不同 AS 之间建立的 BGP 连接。二者的作用简而言之就是：EBGP 是完成不同 AS 之间路由信息的交换，IBGP 是完成路由信息在本 AS 内的过渡。

本产品支持的是版本是 BGP-4，具有如下特点：

- 支持配置 router-id
- 支持手动指定 BGP 对等体
- 支持 BGP 对等体组
- 支持使用 Loopback 接口
- 支持多跳跃 EBGP 连接
- 支持接收路由数量限制
- 支持过滤私有 AS 号
- 支持定时器设置
- 支持 BGP 和 IGP 交互
- 支持 BGP 路由聚合
- 支持 BGP 路由衰减
- 支持 BGP 路由反射器
- 支持 AS 联盟
- 支持管理距离配置
- 支持 BGP 软复位

- 支持 BGP 的监控和维护

支持的路由属性主要有以下十种：

- ORIGN
- AS_PATH
- NEXT_HOP
- MULTI_EXIT_DISC
- LOCAL-PREFERENCE
- ATOMIC_AGGREGATE
- AGGREGATOR
- COMMUNITY
- ORIGINATOR_ID
- CLUSTER_LIST

除此而外，还支持对接收和发布的路由实施策略，支持 AS 路径列表过滤，访问列表(access list)、前缀列表(prifex list)、分发控制列表(distribute-list)和路由映射(Route map)过滤器。

14.2 配置BGP

14.2.1 缺省配置信息

防火墙关于 BGP 的缺省设置信息如以下表格所示：

表14-1 BGP 缺省配置信息

内容	缺省设置	备注
路由器ID	如果配置了lookback接口，就从lookback接口中选择最大的，否则就从物理接口中选择最大的。	可更改设置
缺省路由生成	不生成	可更改设置
EBGP多跳	关闭/255	可更改设置
发布缺省路由	不发布	可更改设置
TCP MD5认证	不认证	不可更改设置
Keepalive Time值	60秒	建议采用缺省设置

Holdtime 值	180秒	可更改设置
ConnectRetry time	120秒	不可更改设置
AdvIntelval（IBGP）	15秒	建议采用缺省设置
Advintelval(EBGP)	30秒	建议采用缺省设置
Bgp scan time	60秒	可更改设置
MED值	0	可更改设置
Local_pref值	100	可更改设置
路由聚合	关闭	可更改设置
路由衰减	关闭	可更改设置
Suppress limit	2000	可更改设置
Half-life-time	15minutes	可更改设置
Reuse limit	750	可更改设置
Max-suppress time	4*half-life-time	可更改设置
管理距离	EBGP 20	
	IBGP 200	
	Local 200	
IGP 路由检查	不检查	可更改设置

14.2.2 配置启用BGP路由协议功能

启用 BGP 路由协议，在此基础上才能对 BGP 路由功能作进一步配置

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router bgp <1-4294967295>	启用bgp功能并进入bgp配置节点

在配置模式下使用 no router bgp <1-4294967295>可以取消对 bgp 的设置，使其恢复到缺省配置。

参数说明：

命令（1）：router NAME

参数	说明——Table Heading	缺省配置
NAME	路由协议类型	无

注意

只有在启用 bgp 以后才能对 bgp 其他功能作进一步配置。每一台设备同时只能配置一个 bgp 实例。

自治系统：AS 是拥有同一选路策略，在同一技术管理部门下运行的一组路由器。它的范围是<1-4294967295>。

14.2.3 配置BGP路由器Router-ID

BGP 协议需要路由器的 Router-ID，作为本路由器在自治系统中的唯一标识。一般在协议任务启动后，会自动选出一个 Router-ID。通常路由器先挑选 IP 地址最大的环回地址。若无环回地址，则选择状态 up 的接口地址大的作为本路由器的 Router-ID.也可以指定一个 Router-ID。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router bgp <1-4294967295>	启用BGP功能并进入BGP配置模式
步骤3	bgp router-id 1.1.1.1	配置路由器Router-ID
步骤4	end	回到enable模式
步骤5	show ip bgp	show命令

使用 no bgp router-id 可以取消对 router-id 的设置，router-id 将会重新自动选举。

参数说明：

命令（1）：bgp router-id A.B.C.D

参数	说明——Table Heading	缺省配置
A.B.C.D	bgp Router-ID	

14.2.4 配置指定BGP对等体

BGP 的运行需要手动指定对等体。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router bgp <1-4294967295>	启用bgp功能并进入bgp配置模式
步骤3	neighbor 1.1.1.1 remote-as 100	指定对等体的ip地址为1.1.1.1 所属AS为AS100
步骤4	end	回到enable模式
步骤5	show run bgp	show命令

使用no neighbor 1.1.1.1 remote-as 100可以取消设置。

参数说明：

命令（1）：neighbor A.B.C.D remote-as <1-4294967295>

参数	说明——Table Heading	缺省配置
A.B.C.D	对等体的地址	无

<1-4294967295>	对等体所属自治系统的自治系统号	无

14.2.5 配置BGP对等体组

对 BGP Speaker 来说，许多对等体的配置信息(包括执行的路由策略等)都相同，为了简化配置，提高效率，推荐使用 BGP 对等体组。。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router bgp <1-4294967295>	启用bgp功能并进入bgp配置模式
步骤3	neighbor WORD peer-group	创建对等体组。
步骤4	neighbor A.B.C.D peer-group WORD	向对等体组中添加成员
步骤5	end	回到enable模式
步骤6	show run bgp	show命令

使用no neighbor peer-group WORD可以取消对等体组设置，恢复为默认值不认证。

参数说明：

命令（1）：neighbor WORD peer-group
neighbor A.B.C.D peer-group WORD

参数	说明——Table Heading	缺省配置
A.B.C.D	对等体组的地址	无
WORD	对等体组的名字	

14.2.6 配置回环接口作为BGP邻居

BGP 使用到达一个邻居的最优本地地址作为发送更新报文的源。该地址通常是具有到邻居的最佳路径的接口的 IP 地址。当有多条链路可用于连接到一个邻居时，这通常在 IBGP 拓扑中出现，通常使用一个回送接口作为本地路由器的 BGP 邻居，并且可用性很强。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router bgp <1-4294967295>	启用bgp功能并进入bgp配置模式
步骤3	neighbor 1.1.1.1 remote-as 100	指定对等体的ip地址为1.1.1.1 所属AS为AS100
步骤4	neighbor 1.1.1.1 update-source lo1	配置lo1作为作为邻居的源端口

步骤5	end	回到enable模式

使用 no neighbor A.B.C.D update-source lo1 可以撤销设置。

参数说明：

命令（1）：neighbor A.B.C.D update-source lo<1-255>

参数	说明——Table Heading	缺省配置
A.B.C.D	对等体IP地址	无
lo<1-255>	Lookback接口地址	无

14.2.7 EBGP多跳配置

EBGP 缺省的 TTL 值是 1 跳，要求是直连的。如果不是直连的，就需要配置 EBGP 多跳并配置跳数<1-255>。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router bgp <1-4294967295>	启用bgp功能并进入bgp配置模式
步骤3	neighbor A.B.C.D ebgp-multihop <1-255>	配置EBGP多跳并配置跳数
步骤4	End	回到enable模式
步骤5	show running-config bgp	show命令

使用 no neighbor 1.1.1.1 ebgp-multihop <1-255> 取消设置。

参数说明：

命令（1）：neighbor A.B.C.D ebgp-multihop <1-255>

参数	说明——Table Heading	缺省配置
A.B.C.D	邻居IP地址	无
<1-255>	跳数	1

14.2.8 配置与指定对等体（组）建立连接的keepalive和holdtime值

配置与指定的 BGP 对等体(组)建立连接时使用的 Keepalive 和 Holdtime 时间值。

keepalive 的范围（1 ～ 65535 seconds），缺省 60seconds；holdtime 的范围（1 ～ 65535 seconds），缺省 180seconds。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router bgp <1-4294967295>	启用bgp功能并进入bgp配置模式
步骤3	neighbor{A.B.C.D | peer-group-name} times <0-65535> <0-65535>	配置keepalive和holdtime值
步骤4	end	回到enable模式
步骤5	show running-config bgp	show命令

使用 no neighbor {A.B.C.D | peer-group-name} times <0-65535> <0-65535>可以取消该设置。

参数说明：

命令（1）：neighbor{A.B.C.D | peer-group-name} times keepalive holdtime

参数	说明——Table Heading	缺省配置
A.B.C.D	邻居IP地址	无
peer-group-name	组名	无
<0-65535>	Keepalive	60s
<0-65535>	Holdtime	180s

14.2.9 配置路由更新的时间间隔

BGP 默认的 IBGP 对等体缺省的时间间隔是 15s，EBGP 是 30s。可以根据需要认为的设定针对邻居的路由更新时间间隔。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router bgp <1-4294967295>	启用bgp功能并进入bgp配置模式
步骤3	neighbor{A.B.C.D | peer-group-name} advertisement-interval <0-600>	设置路由更新时间
步骤4	end	回到enable模式
步骤5	show running-config bgp	show命令

使用 no neighbor{A.B.C.D | peer-group-name} advertisement-interval <0-600>可以取消该项配置，使其恢复到默认值。

参数说明：

命令（1）：neighbor{A.B.C.D | peer-group-name} advertisement-interval <0-600>

参数	说明——Table Heading	缺省配置
A.B.C.D	邻居IP地址	无
peer-group-name	组名	无
<0-600>	时间间隔	IBGP 15s，EBGP 30s

14.2.10 配置向BGP对等体发送缺省路由

有的时候需要向 BGP 对等体发送一条下一跳为自己的缺省路由。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router bgp <1-4294967295>	启用bgp功能并进入bgp配置模式
步骤3	neighbor{A.B.C.D | peer-group-name} default-originate	向邻居发送缺省路由
步骤4	end	回到enable模式
步骤5	show running-config bgp	show命令

使用 no neighbor{A.B.C.D | peer-group-name} default-originate 可以取消配置。

参数说明：

命令（1）： neighbor{A.B.C.D | peer-group-name} default-originate

参数	说明——Table Heading	缺省配置
A.B.C.D	邻居IP地址	无
peer-group-name	组名	无

14.2.11 配置更改路由下一跳为自己

BGP 路由在 IBGP 之间传递时不更改下一跳，这样的话有时候会造成路由不可达。为了保证路由的可达，一般会配置 next-hop-self，即在把路由向外宣告时把该路由的下一跳强制改成自己的接口 IP 地址。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router bgp <1-4294967295>	启用bgp功能并进入bgp配置模式
步骤3	neighbor{A.B.C.D | peer-group-name} next-hop-self	更改下一跳为自己

步骤4	end	回到enable模式
步骤5	show ip bgp	show命令

使用no neighbor{A.B.C.D | peer-group-name} next-hop-self可以取消的配置。

参数说明：

命令（1）：neighbor{A.B.C.D | peer-group-name} next-hop-self

参数	说明——Table Heading	缺省配置
A.B.C.D	邻居IP地址	无
peer-group-name	组名	无

14.2.12 配置删除私有AS号

在 RFC4271 中规定 AS 号的 64512 到 65535 为私有 AS 号不能在公网上传播。所以有的时候需要向对等体宣告路由的时候去掉私有的 AS 号。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router bgp <1-4294967295>	启用bgp功能并进入bgp配置模式
步骤3	neighbor{A.B.C.D | peer-group-name} remove-private-AS	删除私有AS号
步骤4	end	回到enable模式
步骤5	show ip bgp	show命令

使用no neighbor{A.B.C.D | peer-group-name} remove-private-AS，可以取消该配置。

参数说明：

命令（1）：neighbor{A.B.C.D | peer-group-name} remove-private-AS

参数	说明——Table Heading	缺省配置
A.B.C.D	邻居IP地址	无
peer-group-name	组名	无

14.2.13 配置允许发送团体属性

BGP 默认是不向对等体发送团体属性的，有的时候采用团体属性做路由过滤的时候，需要开启向邻居发送团体属性。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router bgp <1-4294967295>	启用bgp功能并进入bgp配置模式
步骤3	neighbor{A.B.C.D | peer-group-name} send-community	开启发送团体属性
步骤4	end	回到enable模式
步骤5	show running-config	show命令

使用 no neighbor{A.B.C.D | peer-group-name} send-community 可以取消该配置

参数说明：

命令（1）：neighbor{A.B.C.D | peer-group-name} send-community

参数	说明——Table Heading	缺省配置
A.B.C.D	邻居IP地址	无
peer-group-name	组名	无

14.2.14 配置限制接收的路由数量

不同的设备性能是不一样的，有的时候为了保护设备，就需要限制接收路由的数量。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router bgp <1-4294967295>	启用bgp功能并进入bgp配置模式
步骤3	neighbor{A.B.C.D | peer-group-name} maximum-prefix <1-4294967295>	配置限制接收路由的数量
步骤4	end	回到enable模式
步骤5	show running-config	show命令

使用 no neighbor{A.B.C.D | peer-group-name} maximum-prefix <1-4294967295>可以取消该配置。

参数说明：

命令（1）：neighbor{A.B.C.D | peer-group-name} maximum-prefix <1-4294967295>

参数	说明——Table Heading	缺省配置
A.B.C.D	邻居IP地址	无

peer-group-name	组名	无
<1-4294967295>	路由数量	无

14.2.15 配置保留对等体路由信息

保存邻居发来的路由信息，当 bgp 重新建立对等体时，不需要要邻居直接发送路由信息，这样对内存要求比较高，一般情况下不建议这样配置。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router bgp <1-4294967295>	启用bgp功能并进入bgp配置模式
步骤3	neighbor{A.B.C.D | peer-group-name} soft-reconfiguration inbound	配置保留对等体路由信息
步骤4	end	回到enable模式
步骤5	show running-config	show命令

使用no neighbor{A.B.C.D | peer-group-name} soft-reconfiguration inbound 可以取消该配置。

参数说明：

命令（1）：neighbor{A.B.C.D | peer-group-name} soft-reconfiguration inbound

参数	说明——Table Heading	缺省配置
A.B.C.D	邻居IP地址	无
peer-group-name	组名	无

14.2.16 配置关闭对等体

有的时候配置一些路由策略而需要临时关闭 BGP 对等体。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router bgp <1-4294967295>	启用bgp功能并进入bgp配置模式
步骤3	neighbor{A.B.C.D | peer-group-name} shutdown	关闭BGP对等体
步骤4	end	回到enable模式
步骤5	show running-config bgp	show命令

使用no neighbor {A.B.C.D | peer-group-name} shutdown可以取消该配置。

参数说明：

命令（1）：neighbor{A.B.C.D | peer-group-name} shutdown

参数	说明——Table Heading	缺省配置
A.B.C.D	邻居IP地址	无
peer-group-name	组名	无

14.2.17 配置IGP和BGP路由交互

通过和 IGP 协议的交互，从 IGP 注入路由信息。BGP 将注入的路由发布给自己的邻居。要通过 network 命令手工注入 BGP Speaker 要向其 BGP Speaker 公告的网络信息。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router bgp <1-4294967295>	启用bgp功能并进入bgp配置模式
步骤3	network A.B.C.D/M [backdoor]	宣告路由
步骤4	end	回到enable模式
步骤5	show ip bgp	show命令

使用 no network A.B.C.D/M 可以取消该配置。

参数说明：

命令（1）：network A.B.C.D/M [backdoor]

参数	说明——Table Heading	缺省配置
A.B.C.D/M	路由/掩码	无

注意

1.如果不加掩码，就按默认的 A、B、C 类

2、如果要确保通告的路由为本地存在的路由，还需要配置 bgp network import-check 坚持这条路由是否在当前的 IP 路由表中，如果不在的话就不把这条路由作为 BGP 路由

14.2.18 配置重发布IGP路由到BGP

将 IGP 产生的路由重发布到 BGP 的路由中，重发布的路由可以是直连路由、静态路由和动态路由协议产生的路由。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router bgp <1-4294967295>	启用bgp功能并进入bgp配置模式
步骤3	redistribute [connected | ospf | rip | static]	重发布路由
步骤4	end	回到enable模式
步骤5	show ip bgp	show命令

使用 no redistribute [connected | ospf | rip | static]可以取消该配置

参数说明：

命令（1）：redistribute [connected | ospf | rip | static]

参数	说明——Table Heading	缺省配置
Connected	直连路由	无
Ospf	Ospf产生的路由	无
Rip	Rip产生的路由	无
Static	静态路由	无

14.2.19 配置BGP的定时器

BGP 使用 Keepalive 定时器来维持和对等体的有效连接，使用 Holdtime 定时器来判断对等体是否有效。缺省情况下，Keepalive 定时器的值为 60S，Holdtime 定时器的值 180S。当 BGP Speakers 之间建立 BGP 连接时，双方将对 Holdtime 进行协商，值更小的 Holdtime 将被选择，而 Keepalive 定时器值的选择将基于协商后的 Holdtime 的 1/3 和配置的 Keepalive 的值得较小者。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router bgp <1-4294967295>	启用bgp功能并进入bgp配置模式
步骤3	timers bgp <0-65535> <0-65535>	设置Holdtime、keepalive定时器
步骤4	end	回到enable模式
步骤5	show run bgp	show命令

使用 no timers bgp <0-65535> <0-65535>可以取消该配置。

参数说明：

命令（1）：timers bgp <0-65535> <0-65535>

参数	说明——Table Heading	缺省配置
<0-65535>	Keepalive	60秒
<0-65535>	Holdtime	180秒

注意

设置了定时器后必须执行 clear 命令，有关 clear 命令下面会讲到使用。

14.2.20 配置BGP的软复位

无论什么时候只要路由策略发送了变化，必须提供有效的方法使得新的路由策略生效，传统的方法是先关掉 BGP 再建立连接。本产品支持 BGP 的软复位，在不关闭 BGP 会话的基础上有效的实施新的路由策略。

为了方便 BGP 软复位描述，下面我们称影响输入路由信息的路由策略为输入路由策略(如 In-route-map、In-dist-list 等)，影响输出路由信息的路由策略为输出路由策略(如 Out-route-map、Out-dist-list 等)。

如果输出路由策略发生变化，那么在 BGP 配置模式下执行：

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router bgp <1-4294967295>	启用bgp功能并进入bgp配置模式
步骤3	clear ip bgp {* | neighbor address | peer-group peer-group-name | external} soft in	软复位BGP连接，不需要重启BGP Session，同时激活路由策略的实施。
步骤4	end	回到enable模式
步骤5	show run bgp	show命令

如果输入路由策略发生变化，其操作将比输出路由策略变化更复杂。这是因为输出路由策略是实施在本 BGP Speaker 的路由信息表上。而输入路由策略是实施在从 BGP Peer 接收来的路由信息上，出于节约内存考虑，本地 BGP Speaker 并不保留原始的从 BGP Peer 接收来的路由信息。

如果确实修改了输入路由策略，常用做法是通过命令 neighbor soft-reconfiguration inbound 为指定的每个 BGP 对等体在本 BGP Speaker 上保存一份原始的路由信息，为随后修改输入路由策略提供原始路由信息依据。

目前存在一种称为“路由刷新性能”的标准实现方式，支持在不保存原始路由信息的条件下，修改路由策略并能得到实施。本产品支持路由刷新性能。

如果输入路由策略发生变化，那么在 BGP 配置模式下执行：

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router bgp <1-4294967295>	启用bgp功能并进入bgp配置模式
步骤3	neighbor{A.B.C.D.| WORD} soft-reconfiguration inbound	如果双方都支持路由刷新就不需要配置这个命令
步骤4	end	回到enable模式
步骤5	show ip bgp neighbors	show命令

参数说明：

命令（1）：neighbor{A.B.C.D.| WORD} soft-reconfiguration inbound

参数	说明——Table Heading	缺省配置
*	所有的BGP对等体执行	无
A.B.C.D	对这个对等体执行	无
WORD	对等体组	无

注意

对不支持路由刷新功能的配置neighbor{A.B.C.D.| WORD} soft-reconfiguration inbound 会消耗大量的内存。

提示

路由策略发送改变了必须实施新的路由策略。

14.2.21 配置BGP路由策略

BGP 可以灵活运用路由策略来控制路由，本产品支持 access-list、prefix-list、as-path-list 路径列表和 route-map。有关些路由策略的详细配置详见后面路由协议无关章节配置。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router bgp <1-4294967295>	启用bgp功能并进入bgp配置模式
步骤3	neighbor{A.B.C.D.| WORD} distribute-list access-list-name {in | out}	配置access-list
步骤4	end	回到enable模式
步骤5	show ip bgp neighbors	show命令

除此而外，还有neighbor{A.B.C.D.| WORD} route-map WORD {in | out}、

neighbor {A.B.C.D.|WORD} filter-list path-list-name {in | out} 和 neighbor { A.B.C.D.| WORD}} prefix-list prefix-list-name {in | out}这三个路由策略工具。

使用 no 取消配置。

参数说明：

命令（1）：neighbor {A.B.C.D.| WORD} distribute-list access-list-name {in | out}

参数	说明——Table Heading	缺省配置
A.B.C.D.	对等体地址	无
WORD	组名	无

14.2.22 配置AS-PATH属性

AS-PATH 属性是 BGP 的一个重要属性，主要用来防止环路，通过配置 AS-PATH-LIST 来实施路由策略也是很有效地一种方式。

防火墙支持基于正则表达式的 AS-PATH-LIST。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router bgp <1-4294967295>	启用bgp功能并进入bgp配置模式
步骤3	ip as-path access-list path-list-name {permit |deny} as-regular-expression	配置AS-PATH-LIST列表
步骤4	end	回到enable模式
步骤5	show run bgp	show命令

使用no ip as-path access-list path-list-name {permit |deny} as-regular-expression 可以取消该配置。

支持的正则表达式主要如下：

.*	匹配所有的路径信息(其实就是没有过滤)
^$	匹配本地 AS 发起的更新
^200$	匹配所有以 AS200 开始和结束的路径，也就是说，仅仅匹配由 AS200 发起的路由或由 AS200 发出的更新(没有 AS 前置并且没有中间 AS)。E.g，它不匹配 200 200
_200$	匹配所有由 AS200 发起的路由，包括那些添加在 200

	前的路径
^200	匹配任何从邻居 AS200 收到的更新，e.g，200、200 100、200 300 100、2001 等
_200_	AS_PATH 包括 AS200(穿过 AS200 的前缀，但不是由 AS 200 发起的或直接从 AS200 收到的前缀)，e.g 200、200 100、300 200 100 等
^100（_100）*（_400）*$	匹配从 AS100 和它紧接着的邻居 AS400 来的路径，e.g 100、100 100、100 400、100 400

参数说明：

命令(1)：ip as-path access-list path-list-name {permit |deny} as-regular-expression

参数	说明——Table Heading	缺省配置
path-list-name	路径列表名字	
as-regular-expressio	正则表达式	

注意

按照标准(RFC4271)实现，BGP 进行最优路径选举时并不考虑 AS 路径长度。但一般情况下，AS 路径长度越短，路径优先级应该越高，所以我们在进行最优路径选举时考虑了 AS 路径的长度。您可以在根据实际情况确定在选举最优路径时是否考虑 AS 路径长度。

如果您希望选举最优路径时不考虑 AS 路径长度，在 BGP 配置模式下执行：bgp bestpath as-path ignore 就可以忽略 AS-PATH 的长度。

14.2.23 配置MED属性

BGP 使用 MED 值作为从 EBGP Peers 学习到的路径进行优先级比较的依据之一，

MED 值越小，路径优先级越高。

缺省情况下，选举最优路径时，只对来自同一 AS 的对等体的路径才比较 MED 值，

如果您希望允许比较来自不同 AS 的对等体的路径的 MED 值，在 BGP 配置模式

下执行：

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router bgp <1-4294967295>	启用bgp功能并进入bgp配置模式
步骤3	bgp always-compare-med	允许来自不同AS 的路径的MED值能进行比较。
步骤4	end	回到enable模式
步骤5	show run bgp	show命令

缺省情况下，选举最优路径时，对来自 AS 联盟内部其他子 AS 的对等体的路径是不进行 MED 比较的，如果您希望来自 AS 联盟内部对等体的路径允许比较 MED 值，在 BGP 配置模式下执行：

步骤1	configure terminal	进入配置模式
步骤2	router bgp <1-4294967295>	启用bgp功能并进入bgp配置模式
步骤3	bgp bestpath med confed	允许来自联盟内部其他子AS的对等体的路径的MED值能进行比较。
步骤4	end	回到enable模式
步骤5	show run bgp	show命令

缺省情况下，如果接收到未设置 MED 属性的路径，该路径的 MED 值被认为是 0 根据 MED 值越小，路径优先级越高，所以该路径的 MED 达到了最高的优先级。

如果您希望未设置 MED 属性的路径的 MED 属性优先级为最低，在 BGP 配置模式

下执行：

步骤1	configure terminal	进入配置模式
步骤2	router bgp <1-4294967295>	启用bgp功能并进入bgp配置模式
步骤3	bgp bestpath med missing-as-worst	将未设置MED属性的路径的优先级设置为最低。
步骤4	end	回到enable模式
步骤5	show run bgp	show命令

缺省情况下，选举最优路径时，将根据接收到的路径的顺序进行比来自相同 AS 的对等体的路径先比较，在 BGP 配置模式下执行：

步骤1	configure terminal	进入配置模式
步骤2	router bgp <1-4294967295>	启用bgp功能并进入bgp配置模式
步骤3	bgp deterministic-med	允许来自相同AS的对等体的路径先比较，缺省情况下将按照路径接收顺序比较，后接收的路径先比较。
步骤4	end	回到enable模式
步骤5	show run bgp	show命令

使用no 取消设置。

14.2.24 配置LOCAL_PREF属性

BGP 使用 LOCAL_PREF 作为从 IBGP Peers 学习到的路径进行优先级比较的依据之一，LOCAL_PREF 值越大优先级越高。

BGP Speaker 将接收到的外部路由发送给 IBGP Peers 时添加本地优先级属性， 如果需要修改本地优先级属性，在 BGP 配置模式下执行：

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router bgp <1-4294967295>	启用bgp功能并进入bgp配置模式
步骤3	bgp default local-preference <0-4294967295>	修改localpref的值
步骤4	end	回到enable模式
步骤5	show run bgp	show命令

使用no bgp default local-preference <0-4294967295>可以取消该配置，恢复到默认的100。

参数说明：

命令（1）：bgp default local-preference <0-4294967295>

参数	说明——Table Heading	缺省配置
<0-4294967295>	Local_pref值	100

除此之外也可以通 route-map 进行修改。

14.2.25 配置COMMUNITY Attribute

COMMUNITY Attribute(团体属性)是能控制路由信息分发的又一种方式。

团体是一组目的地的集合， 定义团体属性的作用是为了方便实施基于团体的路由策略，从而简化在 BGP Speaker 上控制路由信息分发的配置。

每个目的地可以属于多个团体，自治系统管理员可以定义一个目的地属于哪些团体。

缺省情况下，所有的目的地都属于 Internet 团体，携带在路径的团体属性中。

目前共预定义了四个公共的团体属性值：

- Internet：表示 Internet 团体，所有的路径都属于该团体。
- no-export：表示本路径不发布给 EBGP peers。

- no-advertise：表示本路径不发布任何一个 BGP peers。
- local-as：表示本路径不发布到本 AS 外部，当配置联盟时，本路径不发布给其它的自治系统或子自治系统。

通过团体属性，您可以控制路由信息的接收，优先权和分发。

BGP Speaker 可以在学习、发布或者重分发路由时，设置、添加或者修改团体属性值。在进行路由聚合时，聚合后的路径将包含所有被聚合的路径的团体属性值。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router bgp <1-4294967295>	启用bgp功能并进入bgp配置模式
步骤3	Ip community-list standard community-list-name {permit | deny} community-number	创建团体列表。 community-list-name 团体列表的名字 community-number 团体列表的具体值，可以是您指定的一个值 (1 ～4,294,967,200)， 也可以是知名的团体属性（internet、local-AS、no-advertise、no-export）
步骤4	end	回到enable模式
步骤5	show run bgp	show命令

使用no 命令可以取消该配置

参数说明：

命令（1）：ip as-path access-list path-list-name {permit |deny} as-regular-expression

参数	说明——Table Heading	缺省配置
path-list-name	路径列表名字	
as-regular-expressio	正则表达式	

注意

配置团体属性的同时必须打开发送团体属性。

14.2.26 配置比较router-id

缺省情况下，在选举最优路径过程中，如果接收到两条从不同 EBGP Peers 接收来的所有路径属性都相同的路径，我们是根据接收的顺序选举最优路径。您可以通过配置如下命令，选举 Router ID 更小的路径为最优路径。

配置步骤：

步骤1	configure terminal	进入配置模式

步骤2	router bgp <1-4294967295>	启用bgp功能并进入bgp配置模式
步骤3	bgp bestpath compare-routerid	允许BGP进行最优路径选择时比较router ID。
步骤4	end	回到enable模式
步骤5	show run bgp	show命令

使用no bgp bestpath compare-routerid可以取消该配置。

14.2.27 配置BGP聚合路由

BGP-4 支持 CIDR，所以允许创建聚合表项，以减小 BGP 路由表的大小。当然，只有当聚合范围内存在有效的路径时，才将 BGP 聚合表项添加到 BGP 路由表中。本产品支持手动聚合和自动聚合。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router bgp <1-4294967295>	启用bgp功能并进入bgp配置模式
步骤3	aggregate-address A.B.C.D/M	配置聚合路由
步骤4	aggregate-address A.B.C.D/M as-set	添加AS号
步骤5	aggregate-address A.B.C.D/M summary-only	不发送聚合精细路由
步骤6	end	回到enable模式
步骤5	show run bgp	show命令

使用no 可以取消该配置。

参数说明：

命令（1）：aggregate-address A.B.C.D/M [as-set summary-only]

参数	说明——Table Heading	缺省配置
A.B.C.D/M	聚合路由	

命令（2）：aggregate-address A.B.C.D Aggregate mask A.B.C.D [as-set summary-only]

参数	说明——Table Heading	缺省配置
A.B.C.D	聚合地址	
A.B.C.D	聚合掩码	

注意

路由聚合对设备的性能要求很高的，应在充分考虑设备性能后再考虑使用路由聚合。

14.2.28 配置BGP路由反射器

为了加快路由信息的收敛，通常一个 AS 内的所有 BGP Speaker 将建立全连接关系(BGP Speaker 两两建立邻接关系)。当 AS 内的 BGP Speaker 数量过多，将增加 BGP Speaker 的资源开销，同时也给网络管理员增加了配置任务的工作量和复杂度，降低了网络的扩张性能。

对此，提出了路由反射器和 AS 联盟两种方法来减少 AS 内 IBGP 对等体的连接数量。

路由反射器是一种减少自治系统内 IBGP 对等体连接数量的方法。将一台 BGP Speaker 设置为路由反射器，其将本自治系统内的 IBGP 对等体分为两类：客户端和非客户端。

在 AS 内实现路由反射器，其规则如下：

- 配置路由反射器，并指定其客户端，路由反射器和其客户端形成一个群。路由反射器和客户端之间将建立连接关系。
- 一个群内路由反射器的客户端不应该同群外的其他 BGP Speaker 建立连接关系。
- 在 AS 内，非客户端的 IBGP 对等体之间建立完全连接关系，这里的非客户端的 IBGP 对等体包括以下几种情况：一个群内的多个路由反射器之间；群内的路由反射器和群外不参与路由反射器功能的 BGP Speaker(通常这些 BGP Speaker 不支持路由反射器功能)；群内的路由反射器和其他群的路由反射器之间。

路由反射器接收到一条路由的处理规则如下：

- 从 EBGP Speaker 接收到的路由更新，将发送给所有的客户端和非客户端；
- 从客户端接收到的路由更新，将发送其他客户端和所有非客户端；
- 从 IBGP 非客户端接收到的路由更新，将发送给其所有客户端。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router bgp <1-4294967295>	启用bgp功能并进入bgp配置模式
步骤3	neighbor{A.B.C.D | WORD} route-reflector-client	配置本产品为路由反射器，并指定其客户端。
步骤4	end	回到enable模式
步骤5	show run bgp	show命令

通常一个群只配置一个路由反射器，在这种情况下，可以使用路由反射器的 Router ID 标识这个群。为了增加冗余，您可以在群内设置多个路由反射器，在这种情况下，您必须配置群 ID，以便一个路由反射器可以识别来自于群内其他路由反射器的路由更新。

配置群 ID：

步骤1	configure terminal	进入配置模式
步骤2	router bgp <1-4294967295>	启用bgp功能并进入bgp配置模式
步骤3	bgp cluster-id A.B.C.D	配置群ID
步骤4	end	回到enable模式
步骤5	show run bgp	show命令

通常情况下，群内的路由反射器的客户端之间并不需要建立连接关系，路由反射器将反射客户端之间的路由。但是，如果所有客户端之间都已经建立了全连接关系，可以取消路由反射器反射客户端路由的功能。

使用no 可以取消该配置。

参数说明：

命令（1）：neighbor{A.B.C.D | WORD} route-reflector-client

参数	说明——Table Heading	缺省配置
A.B.C.D	对等体地址	
WORD	组名	

14.2.29 配置BGP联盟

联盟是另一种减少自治系统内 IBGP 对等体连接数量的方法。

将一个自治系统划分为多个子自治系统，并通过设置一个统一的联盟 ID(即联盟 AS 号)将这些子自治系统组成一个联盟。对联盟外部来说，整个联盟仍然认为是一个 AS，且只有联盟的 AS 号对外可见。在联盟内部，子自治系统内部的 BGP Speakers 之间仍然建立完全 IBGP 对等体连接，子自治系统间的 BGP Speaker 之间建立 EBGP 连接。虽然在子自治系统的 BGP Speakers 之间建立的是 EBGP 连接，但交换信息时，对于 NEXT_HOP、MED 以及 LOCAL_PREF 等路径属性信息仍然保持不变。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router bgp <1-4294967295>	启用bgp功能并进入bgp配置模式
步骤3	bgp confederation identifier <1-4294967295>	配置 AS 联盟号
步骤4	bgp confederation peers <1-4294967295>	配置在 AS 联盟内的其他子 AS 号
步骤5	end	回到enable模式

步骤6	show run bgp	show命令

使用no可以取消该配置。

参数说明：

命令（1）：bgp confederation identifier <1-4294967295>

参数	说明——Table Heading	缺省配置
<1-4294967295>	联盟号	无

14.2.30 配置BGP的管理距离

管理距离表示一个路由信息源的可信度，其范围是从 1～255，管理距离的值越大，其可信度越低。BGP 对所学习到的路由信息的不同来源设定不同的管理距离，分为 External-distance、Internal-distance 和 Local-distance 三类：

- External-distance：从 EBGP Peers 学习到路由的管理距离
- Internal-distance：从 IBGP Peers 学习到路由的管理距离
- Local-distance：从 Peers 学习到，但被认为存在可以从 IGP 学习到更优的路由的管理距离，通常这些路由通过 Network Backdoor 命令表示。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router bgp <1-4294967295>	启用bgp功能并进入bgp配置模式
步骤3	distance bgp <1-255> <1-255> <1-255>	配置 管理距离
步骤4	end	回到enable模式
步骤5	show run bgp	show命令

使用no可以取消该配置。

参数说明：

命令（1）：distance bgp <1-255> <1-255> <1-255>

参数	说明——Table Heading	缺省配置
<1-255>	External-distance	20
<1-255>	Internal-distance	200
<1-255>	Local-distance	200

注意 一般不建议修改管理距离。

14.2.31 BGP扫描时间配置

BGP 进程会对 bgp rib 路由表进行周期性的扫描，以确定是否应该删除前缀和属性，以及是否应该刷新路由映射或者过滤缓存。也可以扫描 IP rib 以确保所有的下一跳是否仍然有效。如果下一跳不可达，那么所有使用该下一跳的地址的 BGP 表项都会从 BGP RIB 中被清除。BGP 衰减信息也会在每个周期内被更新。通常，每 60 秒扫描一次。也可以更改扫描时间。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router bgp <1-4294967295>	启用bgp功能并进入bgp配置模式
步骤3	bgp scan-time <5-60>	修改扫描周期时间
步骤4	end	回到enable模式
步骤5	show run bgp	show命令

使用no可以取消该配置。

参数说明：

命令（1）：bgp scan-time <5-60>

参数	说明——Table Heading	缺省配置
<5-60>	扫描周期	60s

14.2.32 配置BGP的路由衰减

路由在被认为有效和无效之间来回变化时，称为路由振荡。路由振荡常引起不稳定的路由在网上传播，从而引起了网络的不稳定性。BGP 路由衰减是一种减少路由振荡的方法，其通过监控来自 EBGP Peer 的路由信息从而减少可能的路由振荡。

BGP 的路由衰减使用如下术语：

- 路由振荡：Route Flap，路由在有效和无效之间来回变化。
- 惩罚值：Penalty，每一次路由振荡，启动路由衰减的 BGP Speaker 为该路由增加一次惩罚值，该值累计直到超过抑制上限。
- 抑制上限：Suppress Limit，当路由的惩罚值超过该值时，路由被抑制。
- 半衰期：Half-life-time，惩罚值减为一半的所经过的时间。
- 重新启用值：Reuse Limit，当路由的惩罚值低于该值时，路由抑制解除。
- 最大抑制时间：Max-suppress-time，路由能被抑制的最长时间。

路由衰减处理的简单描述：对每一次路由振荡，BGP Speaker 对该路由进行一次惩罚(累加到惩罚值中)，当惩罚值达到抑制上限，路由将被抑制。在半衰期到达时，惩罚值减为一半，当惩罚值减到重新启用值时，路由重新被激活。路由被抑制的最长时限为最大抑制时间值。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	router bgp <1-4294967295>	启用bgp功能并进入bgp配置模式
步骤3	bgp dampening	启动bgp衰减
步骤4	bgp dampening <1-45> <1-20000> <1-20000> <1-255>	配置路由衰减的参数值
步骤4	end	回到enable模式
步骤5	show run bgp	show命令

使用no可以取消该配置。

参数说明：

命令（1）：bgp dampening <1-45> <1-20000> <1-20000> <1-255>

参数	说明——Table Heading	缺省配置
<1-45>	半衰期	15minutes
<1-20000>	重新启用值	750
<1-20000>	抑制上限	2000
<1-255>	最大抑制时间	4*half-life-time

14.2.33 BGP的维护和监控

BGP 的监控和维护主要包括 debug 和 show 显示。

Debug bgp 打开 bgp debug 开关

Debug bgp events 打开 bgp 事件 debug

Debug bgp as4 打开 4 字节 as

Debug bgp filters 打开过滤

Debug bgp fsm 打开状态机

Debug bgp keepalives 打开 keepalive

Debug bgp update {in|out} 打开 update 报文

Debug bgp zebra 打开 zebra

Show 显示命令：

show ip bgp 显示全部 BGP 路由信息。

show ip bgp A.B.C.D 显示指定目的地的 BGP 路由信息。

show ip bgp prefix-list prefix-list-name 显示匹配前缀列表的指定目的地 BGP 路由信息。

show ip bgp community-list community-lister-number 显示匹配指定团体列表的 BGP 路由信息。

show ip bgp filter-list path-list-number 显示匹配指定 AS 路径列表的 BGP 路由信息。

show ip bgp regexp as-regular-expression 显示 AS 路径属性匹配指定正则表达式的 BGP 路由信息。

show ip bgp dampening flap-statistics 显示所有振荡记录的路由的振荡统计信息。

show ip bgp neighbors [address] [received-routes | routes | advertised-routes] 显示 BGP 对等体的信息。

show ip bgp summary 梗概显示 BGP Router 本身的配置和对等体的信息。

show ip bgp peer-group [peer-group-name] 显示 BGP 对等体组的配置信息

show bgp memory 显示 bgp 使用的内存

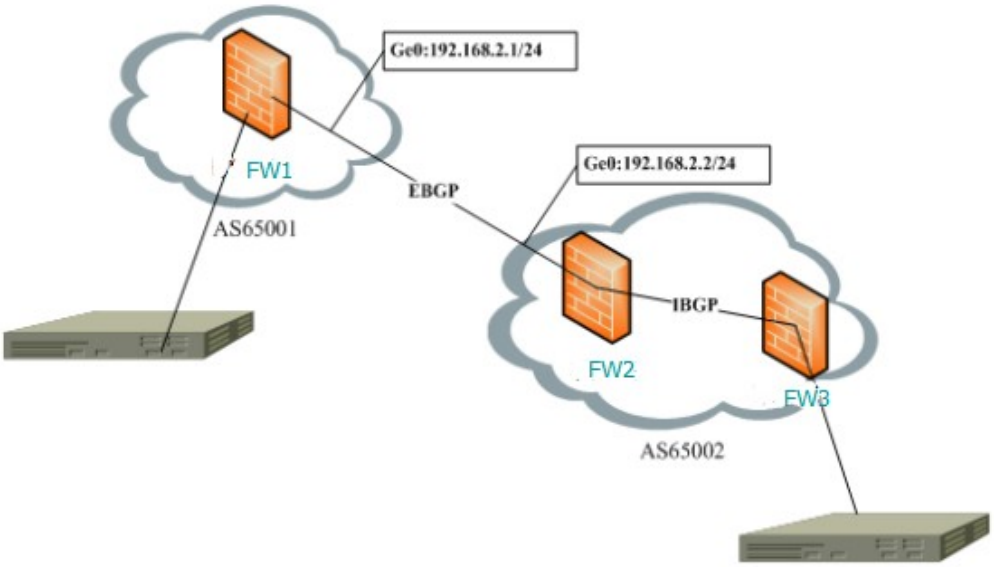
14.3 配置案例

14.3.1 配置案例1：两台防火墙设备通过BGP路由协议互通

案例描述

AS65001 有一台 FW1，AS65002 有 2 台 FW,分别是 FW2 、FW3，FW1 、FW2 之间是 EBGP 连接，FW2 、FW3 之间是 IBGP。

案例组网图



配置步骤：

步骤1	FW1的配置
	FW11# configure terminal FW1 (config)# router bgp 65001 FW1(router- bgp)# neighbor 192.168.2.2 remote-as 65002 FW1(router- bgp)# bgp router-id 1.1.1.1 FW1(router- bgp)# network 1.1.1.1 FW1#end

步骤2	FW2的配置
	FW2# configure terminal FW2 (config)# router bgp 65002 FW2(router- bgp)# neighbor 192.168.2.1 remote-as 65001 FW2(router- bgp)# neighbor 192.168.31.107 remote-as 65002 FW2(router- bgp)# bgp router-id 2.2.2.2 FW2(router- bgp)# network 2.2.2.2 FW2#end

步骤3	FW3的配置
	FW3# configure terminal FW3 (config)# router bgp 65002 FW3(router- bgp)# neighbor 192.168.31.106 remote-as 65002 FW3(router- bgp)# bgp router-id 3.3.3.3 FW3(router- bgp)# network 3.3.3.3 FW3#end

步骤4	

配置结果：

FW1 show running-config bgp 信息：

```
router bgp 65001
 bgp router-id 1.1.1.1
 network 1.0.0.0/8
 neighbor 192.168.2.2 remote-as 65002
!
```

FW2 的 show running-config bgp

```
router bgp 65002
 bgp router-id 2.2.2.2
 network 2.0.0.0/8
 neighbor 192.168.2.1 remote-as 65001
 neighbor 192.168.31.107 remote-as 65002
!
```

FW3 的 show running-config bgp

```
router bgp 65002
 bgp router-id 3.3.3.3
 network 3.0.0.0/8
 neighbor 192.168.31.106 remote-as 65002
!
```

14.4 BGP监控与维护

14.4.1 查看 BGP路由表

介绍常用的 show 命令的使用

查看 bgp 路由表的步骤：

步骤1	显示bgp路由表

```
FW1# sh ip bgp
BGP table version is 0, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 1.0.0.0/8        0.0.0.0                  0         32768 i
```

*> 2.0.0.0/8	192.168.2.2	0	0 65002 i
*> 3.0.0.0/8	192.168.2.2		0 65002 i

Total number of prefixes 3

14.4.2 查看信息

介绍常用的 show 命令的使用

查看 bgp 信息的步骤：

步骤1 察看bgp的信息

FW1# sh ip bgp summary

BGP router identifier 1.1.1.1, local AS number 65001

RIB entries 5, using 480 bytes of memory

Peers 1, using 4528 bytes of memory

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
192.168.2.2	4	65002	40	48	0	0	0	00:10:37	2

Total number of neighbors 1

14.4.3 查看bgp邻居信息

介绍常用的 show 命令的使用

查看 bgp 邻居信息：

步骤1 察看bgp邻居信息

FW1# sh ip bgp neighbors

BGP neighbor is 192.168.2.2, remote AS 65002, local AS 65001, external link

BGP version 4, remote router ID 2.2.2.2

BGP state = Established, up for 00:13:44

Last read 19:46:26, hold time is 180, keepalive interval is 60 seconds

Neighbor capabilities:

4 Byte AS: advertised and received

Route refresh: advertised and received(old & new)

Message statistics:

Inq depth is 0

Outq depth is 0

	Sent	Rcvd
Opens:	7	3
Notifications:	2	2
Updates:	1	3
Keepalives:	41	36
Route Refresh:	0	0
Capability:	0	0
Total:	51	44

Minimum time between advertisement runs is 30 seconds

For address family: IPv4 Unicast

Community attribute sent to this neighbor(both)

1 accepted prefixes

Connections established 5; dropped 4

Last reset 00:13:56, due to User reset

Local host: 192.168.2.1, Local port: 179

Foreign host: 192.168.2.2, Foreign port: 57455

Nexthop: 192.168.2.1

14.4.4 查看bgp 内存使用情况

介绍常用的 show 命令的使用

查看 bgp 内存使用情况

步骤1	察看bgp内存使用情况
	FW1# sh bgp memory 9 RIB nodes, using 864 bytes of memory 2 BGP routes, using 112 bytes of memory 1 Static routes, using 48 bytes of memory 1 Adj-Out entries, using 40 bytes of memory

3 BGP attributes, using 168 bytes of memory
2 BGP extra attributes, using 112 bytes of memory
2 BGP AS-PATH entries, using 48 bytes of memory
1 BGP AS-PATH segments, using 24 bytes of memory
2 peers, using 9056 bytes of memory
21 hash tables, using 840 bytes of memory
5 hash buckets, using 120 bytes of memory

14.5 常见故障分析

14.5.1 故障现象1：两台设备不能建立邻接关系

现象	两台设备不能建立邻接关系
分析	8、 两边peer地址路由不可达 9、 对等体IP地址或者AS号配置错误 10、Open报文协商不成功 11、配置lookback接口路由不可达 12、Igp之间网络不通 13、Router-id冲突
解决	3、 检查接口配置 4、 打开debug开关 5、 通过抓包分析

15 配置 BFD

15.1 BFD概述

BFD(Bidirectional Forwarding Detection，双向转发检测)协议提供一种轻负载、快速检测两台邻接路由器之间转发路径连通状态的方法。协议邻居通过该方式可以快速检测到转发路径的连通故障，加快启用备份转发路径，提升现有网络性能。

15.2 配置BFD

15.2.1 配置BFD会话参数

BFD 需要双向使能，即互为 BFD 邻居的设备都需要做 BFD 配置。

配置步骤:

步骤1	configure terminal	进入配置模式
步骤2	Interface ifname	进入某个接口
步骤3	bfd interval milliseconds min_rx milliseconds multiplier interval-multiplier	配置BFD参数

参数说明：

参数	说明	缺省配置
milliseconds	配置最小发送间隔，单位毫秒	750
milliseconds	配置最小接收间隔，单位毫秒	500
interval-multiplier	配置检测超时倍数	3

15.2.2 配置BFD被动模式

在被动模式下,BFD 不会主动向会话的对端发送 BFD 控制报文,只有等收到 BFD 控制报文后才会向对端发送 BFD 控制报文。

配置步骤:

步骤1	configure terminal	进入配置模式
步骤2	Interface ifname	进入某个接口
步骤3	bfd passive	开启bfd被动模式

如果想关闭被动模式，使用 no bfd passive 命令。

15.2.3 配置BFD与BGP联动

BGP 协议在对等体之间建立了 BGP 连接后，便周期性地发送 KEEPLIVE 报文以保持连接的活跃性，若在指定时间没有收到报文，会认为此条路由不再生效，这种方式不能快速响应链路故障。在 BGP 上启动 BFD 检测后，将会为 BGP 对等体建立 BFD 会话，一旦 BFD 检测到邻居失效，BGP 路由将直接进入失效状态，不再参与路由转发。

配置步骤:

步骤1	configure terminal	进入配置模式
步骤2	router bgp 100	进入bgp模式
步骤3	neighbor A.B.C.D fall-over bfd	配置BFD与BGP联动

如果想删除配置，使用命令 no neighbor A.B.C.D fall-over bfd

15.2.4 配置BFD与OSPF联动

OSPF 协议在建立邻居之后，便周期性地发送 Hello 报文以保持连接的活跃性，若在指定时间没有收到报文，会认为此条路由不再生效，这种方式不能快速响应链路故障。在 OSPF 上启动 BFD 检测后，将会为 OSPF 邻居间建立 BFD 会话，一旦 BFD 检测到邻居失效，OSPF 路由将直接进入失效状态，不再参与路由转发。

配置步骤:

步骤1	configure terminal	进入配置模式
步骤2	interface ifname	进入某个接口
步骤3	ip ospf bfd enable	配置BFD与OSPF联动

如果想删除配置，使用命令 no ip ospf bfd enable .

15.2.5 配置BFD与静态路由联动

静态路由在下一跳失效时，此条静态路由会在一定时间内被置于失效状态，这种方式不能快速响应链路故障。在静态路由上启动 BFD 检测后，将会为静态路由下一跳建立 BFD 会话，一旦 BFD 检测到下一跳失效，静态路由将直接进入失效状态。

配置步骤:

步骤1	configure terminal	进入配置模式
步骤2	ip route static bfd ifname A.B.C.D A.B.C.D	配置BFD与静态路由联动

如果想删除配置，使用命令 no ip route static bfd ifname A.B.C.D A.B.C.D.

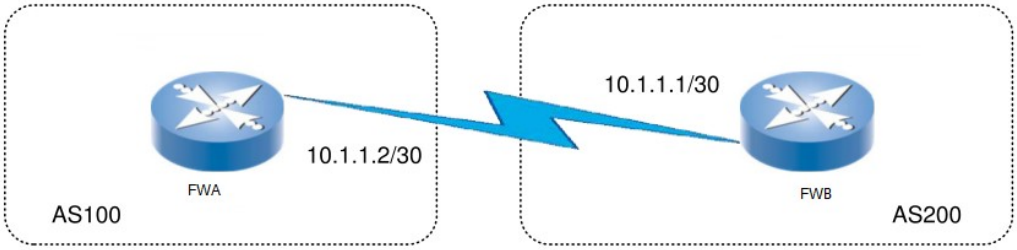
15.3 配置案例

15.3.1 BFD与BGP联动

案例描述：

两台设备建立 BGP 连接，为了能快速发现链路故障，在 BGP 连接上启用 BFD 检测功能，当链路出现故障的时候，能够快速检测，加快路由收敛。

案例组网图



配置步骤：

步骤1	配置FW_A
	FW_A(config)# router-bgp 100
	FW_A(router-bgp)# neighbor 10.1.1.1 remote-as 200
	FW_A(router-bgp)# neighbor 10.1.1.1 fall-over bfd

步骤2	配置FW_B
	FW_B# configure router-bgp 200
	FW_B(router-bgp)# neighbor 10.1.1.2 remote-as 100
	FW_B(router-bg)#neighbor 10.1.1.2 fall-over bfd
步骤3	配置FW_A BFD参数
	FW_A(config)# interface ge0/0
	FW_A(config)#bfd interva 200 min_rx 200 multiplier 3
步骤4	配置FW_B BFD参数
	FW_A(config)# interface ge0/0
	FW_A(config)#bfd interva 200 min_rx 200 multiplier 3

FWA 的配置：

!

bfd interval 200 min_rx 200 multiplier 3

!

!!

router bgp 100

```
 network 10.1.1.0/24
 neighbor 10.1.1.1 remote-as 200
 neighbor 10.1.1.1 fall-over bfd
!
```

FWB 的配置：

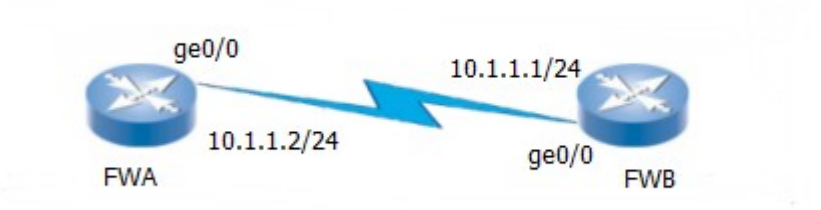
```
!
 bfd interval 200 min_rx 200 multiplier 3
 !

!!
router bgp 200
 network 10.1.1.0/24
 neighbor 10.1.1.2 remote-as 100
 neighbor 10.1.1.2 fall-over bfd
!
```

15.3.2 BFD与OSPF联动

案例描述：

两台设备建立 OSPF 邻居，为了能快速发现链路故障，在 OSPF 连接上启用 BFD 检测功能，当链路出现故障的时候，能够快速检测，加快路由收敛。



配置步骤：

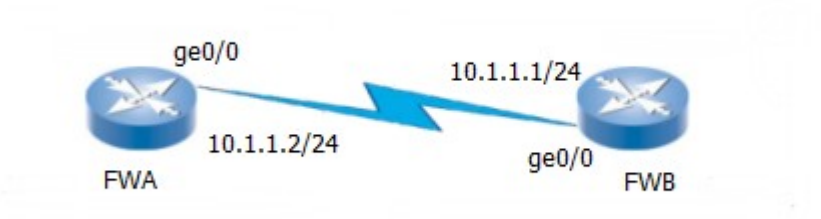
步骤1	配置FW_A
	FW_A(config)# router-ospf FW_A(router-ospf)# network 10.1.1.0/0 area 0
步骤2	配置FW_B
	FW_B(config)# router-ospf FW_B(router-ospf)# network 10.1.1.0/0 area 0
步骤3	配置FW_A BFD参数 FW_A(config-ge0/0)# interface ge0/0 FW_A(config-ge0/0)#ip ospf bfd enable
步骤4	配置FW_B BFD参数

FW_B(config-ge0/0)# interface ge0/0 FW_B(config-ge0/0)#ip ospf bfd enable

15.3.3 BFD与静态路由联动

案例描述：

设备配置一条静态路由，下一跳指向另一台设备，为了能快速发现下一跳是否出现故障，在静态路由上启用 BFD 检测功能，当链路出现故障的时候，能够快速检测。



配置步骤：

步骤1	配置FW_A
	FW_A(config)# ip route 100.1.1.0/24 10.1.1.1 FW_A(router)# ip route static bfd ge0/0 10.1.1.2 10.1.1.1
步骤2	配置FW_B
	FW_B(router)# ip route static bfd ge0/0 10.1.1.1 10.1.1.2

FW_A 配置结果：

!!

ip route 100.1.1.0/24 10.1.1.1

!

!

ip route static bfd ge/0 10.1.1.2 10.1.1.1

!

FW_B 配置结果：

!

ip route static bfd ge/0 10.1.1.1 10.1.1.2

!

15.4 BFD会话监控与维护

15.4.1 查看 BFD邻居

步骤1	显示BFD邻居				
	FWA# show bfd neighbors				
	OutAddr	NeighAddr	LD/RD	Holdown(mult)	State
	10.1.1.2	10.1.1.1	3/1	2250(3)	UP

15.5 故障分析

15.5.1 BFD邻居建立失败

现象	两端配置bfd，但是bfd邻居建立失败
分析	● bfd邻居地址是否配置错误 ● 接口地址是否配置错误 ● bgp联动bfd时，查看bgp邻居是否建立成功

15.6 常用调试功能

调试实例：

```
FWA# terminal monitor
FWA# debug bfd fsm
FWA# debug bfd zebra
[ZEBRA] rcvd: ipv4_bfd_cneigh_add <raddr=136.136.1.254/32, laddr=136.136.1.1/32, ifindex=16, flags=0>
bfd_neightbl_raddr_adddel:(raddr) adding new neighborbfd_neightbl_ldisc_add:(ldisc) Assign: neighp->ldisc=6
bfd_neigh_add: starting bfd session <local IP:136.136.1.1 disc:0x00000006(6)<==>remote IP:136.136.1.254 disc:0x00000000(0)>
[FSM] (bfd_fsm_neigh_add) Add l:136.136.1.1, r:136.136.1.254/ldisc:6, rdisc:0
```

结果分析：

收到了 BFD 的报文，但是状态机并没有 UP，检查 BFD 的配置是否错误。

16 配置策略路由

16.1 策略路由概述

策略路由，也叫做基于策略的路由，是指一个 IPv4 或 IPv6 类型的 IP 包在决定下一跳转发地址时，不是简单的根据目的或源 IP 地址来决定，而是综合考虑多种因素决定。这些因素可以是源地址、目的地址、入接口、服务、用户、应用、域名、时间表等的组合。策略路由支持轮询、加权轮询、源 IP 哈希、源 IP 和端口哈希等选择下一跳的算法，并支持根据健康检查的结果决定下一跳的可用状态。策略路由是一种更加灵活的路由机制，其优先级高于路由选路。

16.2 配置策略路由

16.2.1 创建策略路由

配置策略路由的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	policy-route <1-512> (IF_IN|any) (SIP|any) (DIP|any) (SEV|any) (USER|any) (APP|any) (DONAME|any) (TR|always) (rr|sh|sip_port|wrr)	配置策略路由，将匹配策略的数据包转发至下一跳，具体配置参数见下方的参数说明。
步骤3	nexthop A.B.C.D <1-100> [<1-255>] [TEMPLATE_NAME] [TEMPLATE_NAME] out-interface INTERFACE_NAME [<1-255>] <1-100> [TEMPLATE_NAME] [TEMPLATE_NAME]	配置下一跳地址或者出接口及其对应的权重、优先级、主健康检查模板（可选）、备健康检查模板（可选）。若有多个下一跳，则在该视图下继续添加即可。
步骤4	policy enable	启用策略路由，默认启用，可不配置
步骤5	end	返回特权模式
步骤6	show policy-route [<1-512>]	查看策略路由当前配置

参数说明：

参数	说明	缺省配置
<1-512>	策略路由ID	无
(IF_IN|any)	报文入接口，any表示所有接口	无

(SIP|any)	源地址对象，any表示所有源地址	无
(DIP|any)	目的地址对象，any表示所有目的地址	无
(SEV|any)	服务对象，any表示所有服务	无
(USER|any)	用户对象，any表示所有用户	无
(APP|any)	应用对象，any表示所有应用	无
(DONAME|any)	域名对象，any表示所有域名	无
(TR|always)	时间对象，always表示全部时间	无
(rr|sh|sip_port|wrr)	配置下一跳算法，rr为轮询、sh为源IP哈希、sip_port为源IP和端口哈希、wrr为加权轮询	无

注意

1. 策略路由优先级高于普通路由选路。
2. 策略路由依据接口、源地址、目标地址等作为冲突检查。如果配置重叠或者出现冲突，则会提示配置错误。
3. 优先级越高下一跳越优，高优先级链路健康检查失败后，会自动切换到低优先级下一跳转发。当高优先级故障恢复后，则再次切换到高优先级下一跳转发。
4. 健康检查对象若为非下一跳地址，注意设备要有到该地址的路由，且下一跳为策略路由配置的下一跳地址。
5. 对于设备直连的路由网段不匹配策略路由转发而是查直连路由转发。

16.2.2 创建IPv6策略路由

配置 IPv6 策略路由的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	policy-route-ipv6 <1-512> (IF_IN|any) (SIP|any) (DIP|any) (SEV|any) (APP|any) (TR|always) (rr|sh|sip_port|wrr)	配置IPv6策略路由，将匹配策略的数据包转发至下一跳，具体配置参数见下方的参数说明。
步骤3	nexthop X:X::X:X [<1-255>] <1-100> [TEMPLATE_NAME] [TEMPLATE_NAME] out-interface INTERFACE_NAME [<1-255>] <1-100> [TEMPLATE_NAME] [TEMPLATE_NAME]	配置下一跳地址或者出接口及其对应的权重、优先级、主健康检查模板（可选）、备健康检查模板（可选）。若有多个下一跳，则在该视图下继续添加即可。
步骤4	policy enable	启用策略路由，默认启用，可不配置
步骤5	end	返回特权模式
步骤6	show policy-route-ipv6 [<1-512>]	查看策略路由当前配置

16.2.3 修改策略路由

依据策略路由 ID 进入到策略路由配置视图进行修改。

配置步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	policy-route <1-512>	输入需要修改的策略路由的ID
步骤3	source-interface (IF_IN|any)	修改策略路由的入接口
步骤4	source-addres (SIP|any)	修改策略路由的源地址对象
步骤5	destination-address (SIP|any)	修改策略路由的目的地址对象
步骤6	service (SEV|any)	修改策略路由的服务对象
步骤7	user (USER|any)	修改策略路由的用户对象
步骤8	app (APP|any)	修改策略路由的应用对象
步骤9	domain-name (DONAME|any)	修改策略路由的域名对象
步骤10	Timerange (TR|always)	修改策略路由的时间对象
步骤11	algorithm (rr|sh|sip_port|wrr)	修改策略路由的负载均衡算法
步骤12	exit	返回特权模式

16.2.4 删除策略路由

删除策略路由，配置步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	no policy-route <1-512>	删除指定ID的策略路由条目
步骤3	exit	返回特权模式

删除策略路由下一跳，配置步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	policy-route <1-512>	输入需要删除指定下一跳的策略路由的ID
步骤3	no nexthop A.B.C.D	删除指定下一跳地址
步骤4	exit	返回特权模式

删除策略路由出接口，配置步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	policy-route <1-512>	输入需要删除指定出接口的策略路由的ID
步骤3	no out-interface INTERFACE_NAME	删除指定出接口
步骤4	exit	返回特权模式

16.2.5 调整策略路由的顺序

用 policy-route move 命令可以调整策略路由的顺序，从而使位置在前的策略优先匹配。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	policy-route move <1-512> before <1-512>	移动一条策略路由到指定的策略路由之前
步骤3	policy-route move <1-512> after <1-512>	移动一条策略路由到指定的策略路由之后
步骤4	end	退出到特权模式

16.2.6 插入策略路由

用 insert 命令可以创建一条新的策略路由，并插入到指定的策略路由之前或者之后。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	policy-route insert <1-512> (IF_IN|any) (SIP|any) (DIP|any) (SEV|any) (APP|any) (DONAME|any) (TR|always) (rr|sh|sip_port|wrr) before <1-512>	插入一条新的策略路由到指定的策略路由之前
步骤3	policy-route insert <1-512> (IF_IN|any) (SIP|any) (DIP|any) (SEV|any) (USER|any) (APP|any) (DONAME|any) (TR|always) (rr|sh|sip_port|wrr) after <1-512>	插入一条新的策略路由到指定的策略路由之后
步骤4	end	退出到特权模式

16.2.7 策略路由启用禁用

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	policy-route <1-512>	输入需要配置的策略路由的ID
步骤3	policy (enable|disable)	启用或禁用策略路由
步骤4	end	退出到特权模式

16.3 配置案例

案例描述：

某企业财务部门在工作时间需要通过电信专线访问外网，财务部门 IP 地址范围 192.168.0.10 – 192.168.0.20。

配置步骤：

步骤1	创建一个地址对象：finance_department
	fw40(config)# address finance_department
步骤2	在这个地址对象中添加财务部门地址范围
	fw40(config-addr)# range-address 192.168.0.10 192.168.0.20
步骤3	将应用对象电子邮件和办公软件等办公类应用添加到应用组中
	fw40(config-app-profile)#member category email fw40(config-app-profile)#member category office-software
步骤4	创建一个时间对象，将工作时间加入到时间对象中
	fw40(config)# schedule recurring work_time fw40(config)# periodic 08:00:00 12:00:00 monday tuesday wednesday thursday friday null null fw40(config)# periodic 13:00:00 18:00:00 monday tuesday wednesday thursday friday null null
步骤5	创建icmp健康检查模板
	fw40(config)# healthcheck icmp icmp
步骤6	创建策略路由，引用对应的地址对象、应用组和时间对象等，下一跳地址配置引用健康检查模板
	fw40(config)#policy-route 2 any finance_department any any any any any work_time rr fw40(config-policy-route)# nexthop 10.1.1.1 1 10 icmp

配置结果：

fw40# show running-config

address finance_department

range-address 192.168.0.10 192.168.0.20

!

schedule recurring work_time

periodic 08:00:00 12:00:00 monday tuesday wednesday thursday friday null null

periodic 13:00:00 18:00:00 monday tuesday wednesday thursday friday null null

!

healthcheck icmp icmp

interval 16

```
 maxretrys 3
 timeout 5
policy-route 1 any finance_department any any any any any work_time rr
 policy enable
 session-persist disable
 nexthop 10.1.1.1 1 10 icmp!
!
!
```

16.4 常见故障分析

16.4.1 策略路由不生效

现象	配置策略路由后没有按照策略路由配置转发到对应下一跳
分析	分析可能为以下几种情况： 1. 策略路由没有启用。 2. 匹配上了比本条策略路由优先级更高的策略路由。 3. 检查策略路由下一跳是否配置正确，该下一跳是否有直连路由。 4. 检查策略路由下一跳健康检查是否成功。 5. 检查源IP或者目的IP地址是否在地址对象中添加了排除。 6. 检查访问的目的网段是否在设备上有直连路由。 7. 检查匹配策略路由的报文是否为反向报文。 8. 依据会话信息，检查连接是否为配置开启策略路由之前的连接。 9. 查看命中策略路由的报文是否通过设备进行二层转发。
解决	1. 将策略路由启用。 2. 可以根据需求修改策略路由或者改变策略路由的顺序。 3. 若依据下一跳地址查不到直连路由，则不会从该下一跳出，顺序向下匹配其他策略路由。 4. 检查健康检查失败原因，是否下一跳地址不可达或者链路出现故障。 5. 将IP地址从排除地址中删除。 6. 有直连路由情况下，会匹配直连路由转发，不再匹配策略路由，故对设备上有直连路由的网段配置策略路由无效。 7. 策略路由是基于流的匹配，正向报文匹配策略路由转发，反向报文不会匹配策略路由策略，而是按照路由查找转发，同时遵循路径一致性的原则。 8. 为了避免连接断开，策略路由不会影响已建流的流量转发。可以通过重新发起一个连接来确认策略路由是否正确匹配。 9. 只有三层转发的报文才会进策略路由的匹配流程。

17 配置 NAT

17.1 NAT概述

NAT 即网络地址转换，最初是由 RFC1631(目前已由 RFC3022 替代)定义，用于私有地址向公有地址的转换，以解决公有 IP 地址短缺的问题。后来随着 NAT 技术的发展及应用的不断深入，NAT 更被证明是一项非常有用的技术，可用于多种用途，如：提供了单向隔离，具有很好的安全特性；可用于目标地址的映射，使公有地址可访问配置私有地址的服务器；另外还可用于服务器的负载均衡和地址复用等。

NAT 分为源 NAT 和目的 NAT。源 NAT 是基于源地址的 NAT，可细分为动态 NAT、PAT 和静态 NAT。动态 NAT 和 PAT 是一种单向的针对源地址的映射，主要用于内网访问外网，减少公有地址的数目，隐藏内部地址。动态 NAT 指动态地将源地址转换映射到一个相对较小的地址池中，对于同一个源 IP，不同的连接可能映射到地址池中不同的地址；PAT 是指将所有源地址都映射到同一个地址上，通过端口的映射实现不同连接的区分，实现公网地址的共享。静态 NAT 是一种一对一的双向地址映射，主要用于内部服务器向外提供服务的情况。在这种情况下，内部服务器可以主动访问外部，外部也可以主动访问这台服务器，相当于在内、外网之间建立了一条双向通道。

基于目标地址的 NAT，我们称为目的 NAT，可分为目标地址映射、目标端口映射、服务器负载均衡等。基于目标地址的 NAT 也称为反向 NAT 或地址映射。目的 NAT 是一种单向的针对目标地址的映射，主要用于内部服务器向外部提供服务的情况，它与静态 NAT 的区别在于它是单向的。外部可以主动访问内部，内部却不可以主动访问外部。另外，可使用目的 NAT 实现负载均衡的功能，即可以将一个目标地址转换为多个内部服务器地址。也可以通过端口的映射将不同的端口映射到不同的机器上。

另外，掌握 NAT 的基本原理之后，NAT 不仅仅可用于公有地址和私有地址之间的转换，还可用于公有地址与公有地址之间、私有地址与私有地址之间的转换。


注意

NAT 的负载均衡功能只是将一个目标地址均衡转换到不同的内部主机地址上，它并不检测内部主机是否运行正常。它仅仅是一种特殊的地址转换功能，并不是真正意义上的负载均衡。

17.2 配置NAT

系统中把 NAT 的配置分为： Static、Source、Destination 三种基本类型，另外

还有一种同时可以配置源和目的转换的双向 NAT。

每条 NAT 规则都是和某个特定的接口相关联的，需要注意的是，Source NAT 是在离开接口时进行转换的，Destination NAT 是在进入接口时进行转换的，所以配置 Source NAT 的时候必须和对应的出接口关联，而配置 Destination NAT 的时候需要和对应的入接口关联。双向 Nat 是一条规则里同时配置 Source NAT 和 Destination NAT，匹配流量既做源地址转换，也要做目的地址转换。

17.2.1 配置地址池(NAT POOL)

地址池中存放供动态 NAT 使用的地址范围的集合。地址池的使用支持轮转方式和非轮转方式，同时支持地址池分段。

在进行地址转换后，报文的真实地址将被转换为地址池中的地址。

配置地址池的步骤:

步骤1	configure terminal	进入配置模式
步骤2	ip nat pool POOLNAME	进入地址池节点
步骤3	ip address A.B.C.D A.B.C.D	配置一段地址池
步骤4	rotary	轮询
步骤5	sip_sticky	源地址保持
步骤6	check method	配置SNAT地址检查类型
	dns	地址池检查类型为dns
	icmp	地址池检查类型为icmp
	tcp	地址池检查类型为tcp
步骤7	nexthop address A.B.C.D	SNAT地址池检查下一跳地址
步骤8	check address A.B.C.D	SNAT地址池检查，目标地址
步骤9	check dport <1-65535>	SNAT地址池检查，TCP类型目的端口

使用 no ip nat pool POOLNAME 命令可以删除一个地址池。

使用 no ip address A.B.C.D A.B.C.D 命令可以删除一段地址范围。

使用 no rotary 命令可以禁用轮询。

使用 no sip_sticky 命令可以禁用源地址保持。

使用 no check address 命令可以关闭 SNAT 地址池检查。

注意

不能删除正被 NAT 规则引用的地址池;结束地址不能小于起始地址；池段范围不能出现重叠现象。

17.2.2 配置static NAT

静态 NAT 是一对一的双向地址映射。在这种情况下，被映射的内部主机可以主动访问外部，外部也可以主动访问这台内部主机，相当于在内、外网之间建立了一条双向通道。

配置 static NAT 的步骤:

步骤1	configure terminal	进入配置模式
步骤2	ip nat static INTERFACE A.B.C.D A.B.C.D [log] [ID]	配置一条静态NAT规则

使用 no ip nat ID 命令可以删除一条静态 NAT 规则。


注意

建议在配置 NAT 规则时不指定 ID，系统会自动进行选择。

17.2.3 配置source NAT

源 NAT 是一种单向的针对源地址的映射，主要用于内网访问外网，减少公有地址的数目，隐藏内部地址。

配置 source NAT 的步骤:

步骤1	configure terminal	进入配置模式
步骤2	ip nat source [except] INTERFACE (ADDR_OBJ | any) (ADDR_OBJ | any) (SRV_OBJ|any) (POOL|interface|ip A.B.C.D) [log] [ID]	配置一条源NAT规则。可以指定已经定义的地址池，也可以用interface关键字，表明使用出接口的接口地址，也可以直接配置ip

使用 no ip nat ID 命令可以删除一条源 NAT 规则。

使用关键字“except”，配置 NAT 排除规则，匹配规则的流量不做 NAT 转换。


注意

建议在配置 NAT 规则时不指定 ID，系统会自动进行选择。

17.2.4 配置destination NAT

目的 NAT 根据应用场合不同，可以分为以下三种：

服务器地址、端口映射：实现外网地址和内部地址的单向映射或同时实现转换端口；

服务器业务分流：根据访问的业务不同，系统把目的地址转换为内部不同的服务器地址；

服务器负载分担：把一个外部 IP 映射到内部的一个地址池中，即一到多的映射功能；

配置 destination NAT 的步骤:

步骤1	configure terminal	进入配置模式
步骤2	ip nat destination [except] (INTERFACE|any) (ADDR_OBJ | any) (ADDR_OBJ | any) (SRV_OBJ|any) (POOL| ip A.B.C.D) [service <1-65535>] [log] [ID]	配置一条目的NAT规则。可以指定已经定义的地址池，也可以直接配置ip。

使用 no ip nat ID 命令可以删除一条目的 NAT 规则。

使用关键字“except”，配置 NAT 排除规则，匹配规则的流量不做 NAT 转换。

使用关键字“service”，配置转换后的目的端口。


注意

建议在配置 NAT 规则时不指定 ID，系统会自动进行选择。

17.2.5 配置双向NAT

双向 NAT 是一条规则里，同时配置源 NAT 和目的 NAT。

配置双向 NAT 的步骤:

步骤1	configure terminal	进入配置模式
步骤2	ip nat destination （INTERFACE|any） (ADDR_OBJ | any) (ADDR_OBJ | any) (SRV_OBJ|any) (POOL| ip A.B.C.D) [service <1-65535>] src-translate-to (POOL| ip A.B.C.D) [log] [ID]	配置一条双向NAT规则。

使用 no ip nat ID 命令可以删除一条双向 NAT 规则。

17.2.6 其他NAT配置

1.2.6.1 源端口保持

步骤1	configure terminal	进入配置模式
步骤2	ip nat <1-65535> keep-sport enable [strict]	配置NAT规则的源端口保持。Strict表示严格保持。

使用 ip nat <1-65535> keep-sport disable 取消源端口保持。默认是随机选择。

1.2.6.2 启用

步骤1	configure terminal	进入配置模式
步骤2	ip nat <1-65535> enable	启用NAT规则。

使用 ip nat <1-65535> disable 取消启用。

1.2.6.3 描述信息

步骤1	configure terminal	进入配置模式
步骤2	ip nat <1-65535> description .LINE	配置NAT规则的描述信息。

使用 no ip nat <1-65535> description 取消描述信息。

1.2.6.4 HA 单元 ID

步骤1	configure terminal	进入配置模式
步骤2	ip nat <1-65535> unit-id <1-2>	配置NAT规则的单元id。

1.2.6.5 移动 NAT 规则

步骤1	configure terminal	进入配置模式
步骤2	ip nat move <1-65535> (before|after) <1-65535>	改变nat规则配置顺序。

17.3 端口管理

17.3.1 设置服务端口号

针对服务器有时会改变或者添加所提供服务对应的监听端口号的情况，设备需要改变或添加预置的服务端口号，使设备能正确识别报文中端口号所对应的服务类型。

例如，某个 FTP 服务器除了开放 21 端口监听请求之外，也开放了 1000 端口监听 FTP 请求；当设备接收到一个报文的目的端口号为 1000 时，要识别出该报文为一个 FTP 相关报文，这样就需要设备对服务的端口进行一定的处理。


注意

协议对应的默认端口号无法改变或删除。

配置步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	ip nat service (ftp|tftp|sip) <1-65535>	添加协议对应的端口号(目前仅支持ftp、tftp和sip协议)
步骤3	end	退到特权模式下

步骤4	write terminal	显示配置

使用 no ip nat service (ftp|tftp|sip) <1-65535> 命令可以删除一条服务端口。

注意	每个协议，除了默认端口，最多可以添加 7 个端口号。所有协议最多只能存在 10 条记录。

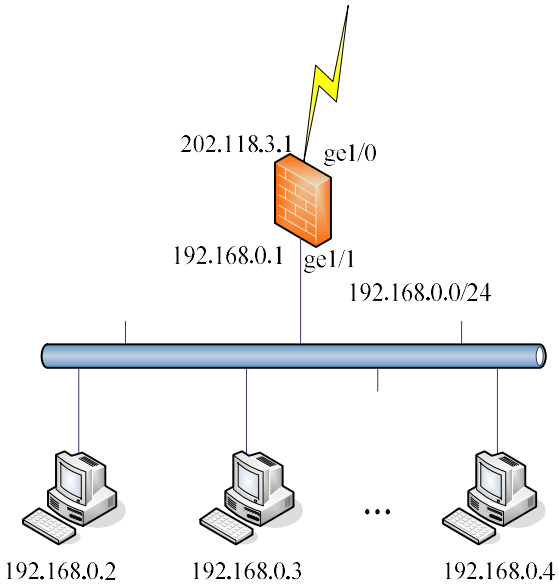
17.4 配置案例

17.4.1 配置source NAT

案例描述：

公司需要通过防火墙共享上网。内网地址为 192.168.0.0/24 网段，公网地址为 202.118.3.11

图17-1 Source NAT 配置案例组网图



配置步骤：

步骤1	建立一个地址对象
	host(config)# address inside-net host(config-addr)# net-address 192.168.0.0/24 host(config-addr)#exit host(config)#
步骤2	配置一个地址池

```
host(config)#ip nat pool pub-pool
host(ip-nat-pool)#ip address 202.118.3.11 202.118.3.11
host(ip-nat-pool)# exit
host(config)#
```

步骤3 配置一条source NAT规则

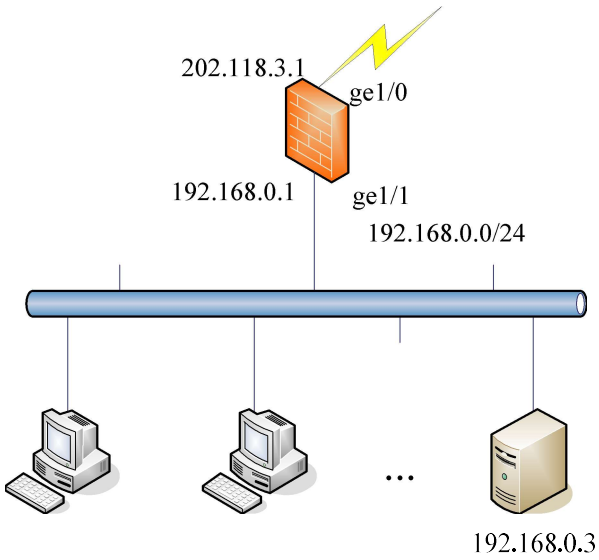
```
host(config)#ip nat source ge1/0 inside-net any any any pub-pool
```

17.4.2 配置static NAT

案例描述：

内网有一台服务器对外提供服务，服务器的内网地址为 192.168.0.3，映射的公网地址为 202.118.3.11。

图 15-2Static NAT 配置案例组网图



配置步骤：

步骤1 配置一条static NAT规则

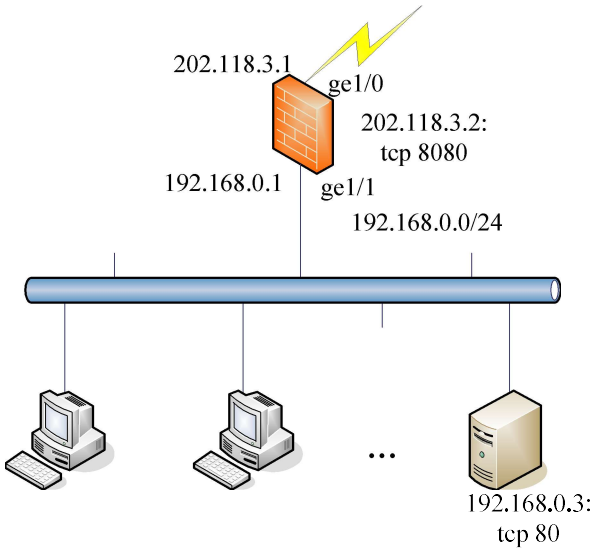
```
host(config)#ip nat static ge1/0 192.168.0.3 202.118.3.11
```

17.4.3 配置destination NAT——服务器地址、端口映射

案例描述：

内网有一台服务器对外提供 HTTP 服务，内网地址为 192.168.0.3，服务端口为 tcp 80，对外开放的地址为 202.118.3.2，对外开放的服务端口为 tcp 8080

图 15-3 配置 destination NAT 案例组网图



配置步骤：

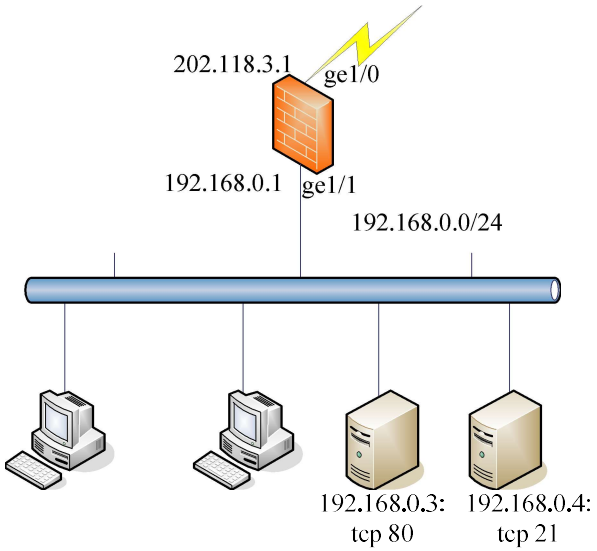
步骤1	建立一个地址对象
	host(config)# address http-pub host(config-addr)# address 202.118.3.2 host(config-addr)#exit host(config)#
步骤2	配置一个服务对象
	host(config)#service http8080 host(config-sev)# tcp dest 8080 source 1 65535 host(config-sev)#exit host(config)#
步骤3	配置一个地址池
	host(config)#ip nat pool web-server host(ip-nat-pool)#ip address 192.168.0.3 192.168.0.3 host(ip-nat-pool)# exit host(config)#
步骤4	配置一条destination NAT规则
	host(config)ip nat destination ge1/0 any http-pub http8080 web-server service 80

17.4.4 配置destination NAT——服务器业务分流

案例描述：

内网有 HTTP、FTP 服务器各一台，内网地址分别为 192.168.0.3 和 192.168.0.4，对外采用同一个公网 IP——202.118.3.1，根据访问的业务自动映射到这两台服务器，实现业务分流。

图 15-4 配置 destination NAT 案例组网图 a



配置步骤：

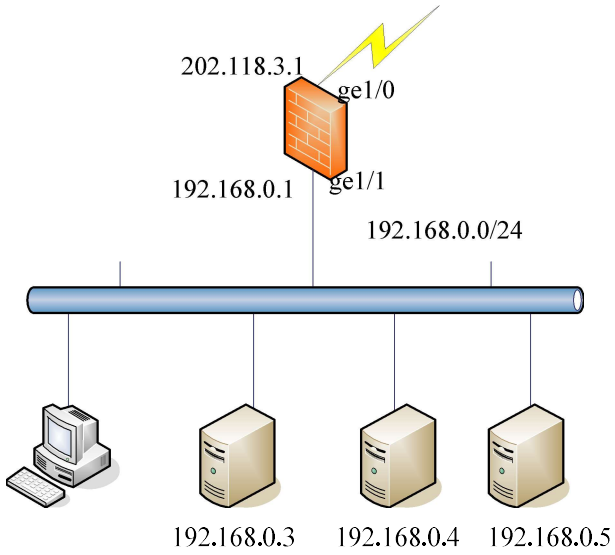
步骤1	建立一个地址对象
	host(config)# address serv-pub host(config-addr-obj)# address 202.118.3.1 host(config-addr-obj)#exit host(config)#
步骤2	配置两个地址池
	host(config)#ip nat pool web-server host(ip-nat-pool)#ip address 192.168.0.3 192.168.0.3 host(ip-nat-pool)# exit host(config)#ip nat pool ftp-server host(ip-nat-pool)#ip address 192.168.0.4 192.168.0.4 host(ip-nat-pool)# exit host(config)#
步骤3	配置两条destination NAT规则
	host(config)#ip nat destination ge1/0 any serv-pub http web-server host(config)#ip nat destination ge1/0 any serv-pub ftp ftp-server

17.4.5 配置destination NAT——服务器负载分担

案例描述：

内网采用三台服务器进行负载分担，内网地址分别为 192.168.0.3、 192.168.0.4 和 192.168.0.5，对外采用同一个公网 IP——202.118.3.1。

图 15-5 配置 destination NAT 案例组网图 a



配置步骤：

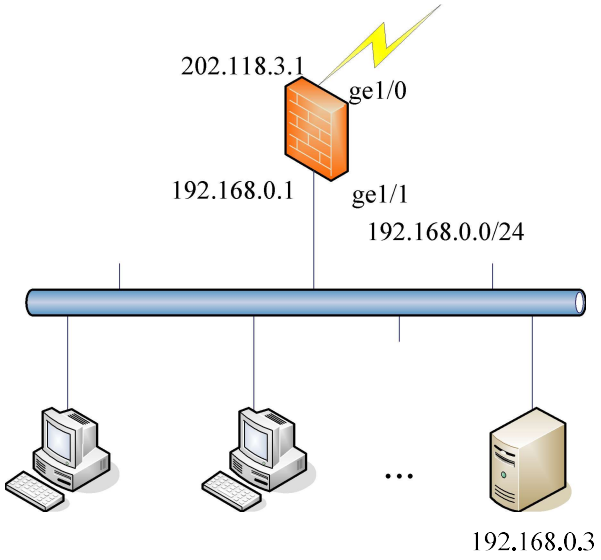
步骤1	建立一个地址对象
	host(config)# address serv-pub host(config-addr-obj)# address 202.118.3.1 host(config-addr-obj)#exit host(config)#
步骤2	配置一个地址池
	host(config)#ip nat pool servers host(ip-nat-pool)#ip address 192.168.0.3 192.168.0.5 host(ip-nat-pool)# rotary host(ip-nat-pool)# exit host(config)#
步骤3	配置一条destination NAT规则
	host(config)ip nat destination ge1/0 any serv-pub any servers

17.4.6 配置双向 NAT

案例描述：

内网有一台服务器对外和对内提供服务，服务器的内网地址为 192.168.0.3，映射的公网地址为 202.118.3.11。

图 15-5 配置 destination NAT 案例组网图 a



配置步骤：

步骤1	建立一个地址对象
	host(config)# address serv-pub host(config-addr-obj)# address 202.118.3.11 host(config-addr-obj)#exit host(config)#
步骤2	配置一个地址池
	host(config)#ip nat pool servers host(ip-nat-pool)#ip address 192.168.0.3 192.168.0.3 host(ip-nat-pool)# exit host(config)#
步骤3	配置一条双向NAT规则，转换后的源地址为192.168.0.100
	host(config)# ip nat destination any any serv-pub any servers src-translate-to ip 192.168.0.100

17.4.7 配置服务端口

案例描述：

内网中包含一台 FTP 服务器，该服务器在 100 端口上监听 FTP 请求。

配置步骤：

步骤1	进入congfig模式
	host# configure terminal

步骤2	添加FTP的端口号100
	host (config-if)# ip nat service ftp 100

命令 no ip nat service ftp 100 可以删除添加的端口号 100。


注意

不同的协议添加的 ALG 端口可以相同。

17.5 NAT监控与维护

17.5.1 查看NAT配置信息

步骤1	查看NAT地址池和NAT规则信息
	host# show ip nat pool ip nat pool pub_net ip address 202.118.3.11 202.118.3.11 ip nat pool inside_net ip address 192.168.0.3 192.168.0.3 显示系统中配置了两个地址池 host# show ip nat rule ip nat source ge1/0 any any any interface 1 ip nat 1 unit-id 1 ip nat 1 keep-sport enable ip nat fail-time: 2231 显示系统中配置了一条源NAT规则，此规则的源端口保持，以及选址失败次数。 host# show ip nat statistics ip nat statistics: static nat rule counts: 0 source nat rule counts: 1 destination nat rule counts: 0 translation entry counts: 12 显示系统中NAT规则数及当前NAT转换的条目数

17.5.2 查看NAT转换信息

步骤1	查看全部NAT转换的信息
	host# show ip nat translations
步骤2	查看前n条NAT转换的信息
	host# show ipv4 nat translations [<1-1000>]
步骤3	查看前n条符合特定条件的NAT转换的信息
	host# show ipv4 nat translations protocol (tcp|udp|icmp|generic|all) ip source (IPADDRESS | any) dest (IPADDRESS | any) port (DESTPORT|any) [<1-1000>]

17.5.3 清除NAT转换条目

步骤1	清除系统中的所有转换条目
	host# clear ip nat translations 该命令同时会清除系统中的所有流信息

17.5.4 查看NAT转化过程信息

步骤1	查看NAT转换过程的调试信息
	host# debug ip nat

17.5.5 查看NAT地址池使用情况

步骤1	查看NAT地址池使用率
	host# show ip nat pool usage host# show ip nat pool NAME detail usage

17.5.6 查看NAT规则选址失败次数

步骤1	查看NAT规则选址失败次数
	host# show ip nat rule 1 ip nat source ge0/0 any any http interface 1 ip nat 1 unit-id 1 ip nat fail-time: 380 host# show ip nat rule
步骤2	查看ipv6规则和跨协议转换规则选址失败次数
	host# show ipv6 nat rule ipv6 nat source tvi2 any any any interface 1

ipv6 nat 1 unit-id 1 ipv6 nat fail-time: 28295 ! host# show ipv6 nat rule 1 host# show ipv6 nat rule 1 ipv6 nat source tvi2 any any any interface 1 ipv6 nat 1 unit-id 1 ipv6 nat fail-time: 28295 host# show (nat46|nat64) rule 1

17.5.7 清除NAT规则选址失败次数

步骤1	清除NAT规则选址失败次数
	host# clear ip nat fail-time 1 host# clear ipv6 nat fail-time 1 host# clear (nat64|nat46) fail-time 1

17.6 常见故障分析

17.6.1 连接时通时断

故障现象	做了NAT之后，经过NAT Ping另外网络的机器，时通时断；或刚开始是通的，一会儿又断了；或一直不通
分析与解决	1)转换后的地址有冲突，别人已经使用。有些地址可能Ping不通，但不能排除地址已被使用的可能，因为对方可以禁止了Ping包。 2)可以查看被Ping的机器中的ARP表项，NAT转换后的地址对应的MAC是否为设备的MAC地址，如不是，证明有其它机器使用了此IP。使用无人使用的地址作为NAT转换后的地址。

18 NAT 地址池检查

18.1 NAT地址池检查概述

NAT 地址池检查功能用于检查 NAT 地址池中 NAT 地址的可用性。开启该功能后，在做源 NAT 时排除掉 NAT 地址池中不可用的 NAT 地址，NAT 地址池检查的参数有默认配置。

18.2 NAT地址池配置检查功能

步骤1	configure terminal	进入配置模式
步骤2	ip nat pool POOLNAME	进入地址池节点
步骤3	check address A.B.C.D	配置地址池节点中的探测地址
步骤4	nexthop address A.B.C.D	配置地址池探测的下一跳地址

使用 no check address 命令可以关闭地址池探测功能。

18.3 配置NAT地址池探测参数:

步骤1	configure terminal	进入配置模式
步骤2	snat-pool-check interval <1-60>	修改NAT地址池检查间隔
步骤3	snat-pool-check allow-failtime <1-30>	修改NAT地址池检查允许失败次数
步骤4	snat-pool-check domain NAME	修改NAT地址池检查域名
步骤5	snat-pool-check dport <1-65535>	修改NAT地址池检查目的端口
步骤6	snat-pool-check sportrange <1024-65535>	修改NAT地址池检查源端口号轮巡范围

在特权模式下可以通过 show snat-pool-check 命令查看 NAT 地址池探测参数，与默认值相同的参数不显示。

19 配置 IPSec VPN

19.1 IPSec VPN概述

IPSec 使用加密和认证机制，为数据在公共网络环境中的传输提供安全保障。它能够为数据传输提供了以下安全服务：

数据的机密性——IPSec 使用 ESP 安全协议为数据传输提供加密保护。

数据的完整性——IPSec 使用 ESP 或 AH 安全协议为数据的传输提供完整性保护。这使得数据接收方可以及时地发现数据是否在传输的过程中被修改过。

数据源的认证——IPSec 接收方验证数据的来源。

抗重播——IPSec 的接收方可以检测到重播的 IP 包并丢弃。

通常，一个 IPSec 系统实现主要由以下部分组成：

安全协议——包括“封装安全载荷协议（以下简称 ESP）”和“认证头协议（以下简称 AH）”协议。ESP 可以提供数据的完整性、机密性和抗重播服务；AH 协议可以提供数据源认证、完整性和抗重播保护。

安全策略库（以下简称 SPDB）和安全关联库（以下简称 SADB）——安全策略库决定了对哪些 IP 报文进行处理，如何进行处理（丢弃、绕过、IPSec 处理）；安全关联库决定了对那些需要进行 IPSec 处理的 IP 报文的处理细节，如使用什么安全协议，加密算法，认证算法等。

密钥管理协议——用于协商建立、更新、删除 SA，包括 ISAKMP SA 和 IPSec SA。通常 IPSec 系统实现使用 IKE 密钥管理协议协商建立 SA。

相关术语解释：

认证头协议（AH）：用于验证数据包的安全协议。

封装安全载荷协议（ESP）： 用于加密和验证数据包的安全协议；可与 AH 配合工作可也以单独工作。

加密算法：ESP 所使用的加密算法

验证算法：AH 或 ESP 用来验证对方的验证算法

密钥管理协议：用于完成共享密钥的建立、更新和删除。其中，IKE（Internet 密钥交换协议）是 IPSec 默认使用的密钥交换协议

构建 VPN 是 IPSec 的典型应用。本章主要详细介绍使用 IPSec 构建 VPN 的过程，并给出典型案例。单独使用 USG 集成的 IPSec VPN 子系统可以为网关之间、使用 VPN 客户端的主机和网关之间的数据传输提供安全保障。USG 集成的 IPSec VPN 子系统具有以下功能：

支持路由模式和桥模式使用 IPSec。

支持隧道模式和传输模式。

支持 IKEv1、IKEv2、国密。

使用 IKE 协议建立、更新、删除 SA。

IKE 阶段 1 协商支持预共享密钥认证方法、证书认证方法。
主模式协商和野蛮模式协商。
使用预共享密钥认证方法时，支持使用 IPv4 地址、FQDN、USER_FQDN 类型的 ID。
支持静态接入（通过指定对端网关为静态 IP 或域名的方式）和动态接入（通过指定对端网关为动态 IP 的方式）。
支持丰富的加密算法和认证算法。
支持 DH 组 2、组 5、组 14、组 22、组 23、组 24。
支持 DPD 探测。
支持 NAT 穿越。
支持 PFS。

19.2 配置IPSec VPN

19.2.1 缺省配置信息

表 18-1 IPSec VPN 缺省配置信息

内容	缺省设置	备注
密钥协商时协商双方的身份标识	预共享密钥方式默认为IKE协商使用的接口的IP地址；证书方式默认为证书的主题	采用预共享密钥认证方式时，可更改为FQDN、USER_FQDN
密钥协商验证对方的方式	预共享密钥(pre-shared)	可更改为证书
ISAKMP SA的生存期	86400秒	可更改设置
IPSec SA的生存期（时间方式）	10800秒	可更改设置
安全协议的工作方式	隧道模式	可更改为传输模式
加密算法	AES128	可更改设置
验证算法	MD5	可更改设置
密钥协商模式	主模式	可更改野蛮模式
DPD对等体检测功能	不启用	可更改为启用

19.2.2 配置IKEv1阶段1

在全局配置模式下配置 IKEv1（Internet Key Exchange version 1）阶段 1 的相关参数。IKEv1 协商发起方利用这些参数发起协商，通过与对对端协商建立 ISAKMP SA，从而为 IPSec SA 的协商建立安全环境。

配置步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	edit gateway NAME	进入阶段1的配置

步骤3	authentication (pre-share|rsa-sig)	设置认证方法
步骤4	set localid address A.B.C.D	配置本端使用的IP地址
步骤5	set mode {main | aggressive}	设置阶段1的协商模式
步骤6	set remotegw A.B.C.D |dynamic	设置对端网关的地址
步骤7	set preshared-key KEY	使用预共享密钥认证方式时设置预共享密钥值
	set local-cert NAME	使用证书认证方式时设置本地证书
	group (1|2|5|14|22|23|24)	设置密钥交换所采用的DH组，默认为group2。
步骤8	lifetime <1200-86400>	配置ISAKMP SA的生存期。默认是86400秒
步骤9	set policy <1-3>	配置算法（可配置最多3套算法）
步骤10	encrypt (3des|des|aes128|aes192|aes256)	设置加密算法，默认是AES128
步骤11	hash (md5|sha|sha2_256|sha2_384|sha2_512)	设置HASH算法，默认是MD5认证
步骤12	exit	退出当前设置
步骤13	set dpd <30-120>	设置对等体检测
步骤14	set nat <10-900>	设置NAT穿越的保活时间
步骤15	set id (local|peer) ID	设置本方|对端ID
步骤16	exit	退出当前设置

以上命令均可使用 no 命令取消对各个命令的设置，使其恢复到缺省配置。

参数说明：

edit gateway NAME：

参数	说明	缺省配置
NAME	阶段1的名称	缺省无设置

set mode {main|aggressive}：

参数	说明	缺省配置
{main|aggressive}	设置阶段1的协商方式	缺省是主模式

set remotegw A.B.C.D| dynamic

参数	说明	缺省配置
{A.B.C.D| dynamic}	设置对端网关的方式	缺省是IP地址

set preshared-key KEY

参数	说明	缺省配置
KEY	密钥值。在设置认证方式为预共享密钥时有效。	无

set local-cert NAME

参数	说明	缺省配置
NAME	本地证书名称。在设置认证方式为rsa签名。	无

group (1|2|5|14|22|23|24)

参数	说明	缺省配置
(1|2|5|14|22|23|24)	Diff-Hellmen数组	默认group2

lifetime TIME

参数	说明	缺省配置
TIME	配置isakmp sa的生存期	默认是86400秒

set policy <1-3>

参数	说明	缺省配置
<1-3>	配置算法，最多可以配置三组算法组合	缺省指定一套，policy 1

encrypt (3des|des|aes128|aes192|aes256)

参数	说明	缺省配置
(3des|des|aes128|aes192|aes256)	设置加密算法	默认是AES128加密。

hash (md5|sha1|sha2_256|sha2_384|sha2_512)

参数	说明	缺省配置
(md5|sha|sha2_256|sha2_384|sha2_512)	设置HASH认证算法	默认是MD5认证。

set dpd <30-120>

参数	说明	缺省配置
<30-120>	设置对等体检测	缺省是30秒，功能不启用

set nat <10-900>

参数	说明	缺省配置
<10-900>	设置NAT穿越的保活时间	缺省是10秒

set id (local|peer) ID

参数	说明	缺省配置
ID	设置本端和对端的协商时的身份标识	预共享密钥方式默认为IKE协商使用的接口的IP地址；证书方式默认为证书的主题

用户可以配置多条 IKE 策略，当 FW 设备进行 IKE 协商时试图协商到两端设备相同的 IKE 策略 。

19.2.3 配置IKEv2阶段1

在全局配置模式下配置 IKEv2（Internet Key Exchange version 2）阶段 1 的相关参数。IKEv2 协商发起方利用这些参数发起协商，通过与对对端协商建立 ISAKMP SA，从而为 IPSec SA 的协商建立安全环境。

配置步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	edit gateway-ikev2 NAME	进入阶段1的配置
步骤3	authentication (pre-share|rsa-sig)	设置认证方法
步骤4	set localid address A.B.C.D	配置本端使用的IP地址
	set local-interface	
步骤5	set remotegw A.B.C.D |dynamic	设置对端网关的地址
步骤6	set preshared-key KEY	使用预共享密钥认证方式时设置预共享密钥值
	set local-cert NAME	使用证书认证方式时设置本地证书
	group (1|2|5|14|22|23|24)	设置密钥交换所采用的DH组，默认为group2。
步骤7	lifetime <1200-86400>	配置ISAKMP SA的生存期。默认是86400秒
步骤8	set policy <1-3>	配置IKE策略
步骤9	encrypt (3des|des|aes128|aes192|aes256)	设置加密算法，默认是3DES
步骤10	hash (md5|sha|sha2_256|sha2_384|sha2_512)	设置HASH算法，默认是MD5认证
步骤11	exit	退出当前设置
步骤12	set nat <10-900>	设置NAT穿越的保活时间
步骤13	set id (local|peer) ID	设置本方|对端ID
步骤14	exit	退出当前设置

以上命令均可使用 no 命令取消对各个命令的设置，使其恢复到缺省配置。

参数说明：

edit gateway-ikev2 NAME：

参数	说明	缺省配置
NAME	阶段1的名称	缺省无设置

set remotegw A.B.C.D| dynamic

参数	说明	缺省配置
{A.B.C.D| dynamic}	设置对端网关的方式	缺省是IP地址

set preshared-key KEY

参数	说明	缺省配置
KEY	密钥值。在设置认证方式为预共享密钥时有效。	无

set local-cert NAME

参数	说明	缺省配置
NAME	本地证书名称。在设置认证方式为rsa签名时有效。	无

group (1|2|5|14|22|23|24)

参数	说明	缺省配置
(1|2|5|14|22|23|24)	Diff-Hellmen数组	默认group2

lifetime TIME

参数	说明	缺省配置
TIME	配置isakmp sa的生存期	默认是86400秒

set policy <1-3>

参数	说明	缺省配置
<1-3>	配置IKE 策略，最多可以配置三组算法组合	缺省指定一套，policy 1

encrypt (3des|des|aes128|aes192|aes256)

参数	说明	缺省配置
(3des|des|aes128|aes192|aes256)	设置加密算法	默认是3DES加密。

hash (md5|sha1|sha2_256|sha2_384|sha2_512)

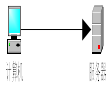
参数	说明	缺省配置
(md5|sha1|sha2_256|sha2_384|sha2_512)	设置HASH认证算法	默认是MD5认证。

set nat <10-900>

参数	说明	缺省配置
<10-900>	设置NAT穿越的保活时间	缺省是10秒

set id (local|peer) ID

参数	说明	缺省配置
ID	设置本端和对端的协商时的身份标识	预共享密钥方式默认为IKE协商使用的接口的IP地址；证书方式默认为证书的主题



用户可以配置多条 IKE 策略，当 FW 设备进行 IKE 协商时试图协商到两端设备相同的 IKE 策略 。

19.2.4 配置国密阶段1

在全局配置模式下配置国密阶段 1 的相关参数。国密协商发起方利用这些参数发起协商，通过与对对端协商建立 ISAKMP SA，从而为 IPSec SA 的协商建立安全环境。

配置步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	edit gateway-gb NAME	进入阶段1的配置
步骤3	set localid address A.B.C.D	配置本端使用的IP地址
步骤4	set remotegw A.B.C.D |dynamic	设置对端网关的地址
步骤5	set local-cert NAME	使用证书认证方式时设置本地证书
步骤6	lifetime <1200-86400>	配置ISAKMP SA的生存期。默认是86400秒
步骤7	set policy-gb <1-2>	配置IKE策略
步骤8	encrypt-gb (sm1|sm4)	设置加密算法，默认是sm4
步骤9	hash-gb (sm3)	设置HASH算法
步骤10	exit	退出当前设置
步骤11	set dpd <30-120>	设置对等体检测
步骤12	set nat <10-900>	设置NAT穿越的保活时间
步骤13	exit	退出当前设置

以上命令均可使用 no 命令取消对各个命令的设置，使其恢复到缺省配置。

参数说明：

edit gateway-gb NAME：

参数	说明	缺省配置
NAME	阶段1的名称	缺省无设置

set remotegw A.B.C.D| dynamic

参数	说明	缺省配置
{A.B.C.D| dynamic}	设置对端网关的方式	缺省是IP地址

set local-cert NAME

参数	说明	缺省配置
NAME	本地证书名称。在设置认证方式为rsa签名。	无

lifetime TIME

参数	说明	缺省配置
TIME	配置isakmp sa的生存期	默认是86400秒

set policy-gb <1-2>

参数	说明	缺省配置
<1-2>	配置IKE 策略，最多可以配置两组算法组合	缺省指定一套，policy 1

encrypt-gb (sm1|sm4)

参数	说明	缺省配置
(sm1|sm4)	设置加密算法	默认是sm4加密。

hash-gb(sm3)

参数	说明	缺省配置
(sm3)	设置HASH认证算法	默认是sm3认证。

set dpd <30-120>

参数	说明	缺省配置
<30-120>	设置对等体检测	缺省是30秒，功能不启用

set nat <10-900>

参数	说明	缺省配置
<10-900>	设置NAT穿越的保活时间	缺省是10秒

注意

用户可以配置多条 IKE 策略，当 FW 设备进行 IKE 协商时试图协商到两端设备相同的 IKE 策略 。

19.2.5 配置IKEv1、IKEv2阶段2

配置步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	vpn ipsec phase2	进入阶段2的配置
步骤3	edit tunnel NAME	编辑阶段2隧道的名称
步骤4	set peer GATEWAY	配置阶段1的名称
步骤5	set propasal1 (esp-3des-md5|esp-3des-null|esp-3des-sha1||esp-3des-sha2_256|esp-3des-sha2_384|esp-3des-sha2_512|esp-aes128-md5|esp-aes128-null|esp-aes128-sha1|esp-aes128-sha2_256|esp-aes128-sha2	设置阶段2的交互方案，交互方案是可接受的安全协议和算法组合。两端FW设备通过协商达成共识使用某个相同的交互方案进行IPSec通信（ikev2不支持AH相关算法）

	_384|esp-aes128-sha2_512|esp-aes192-md5|esp-aes192-sha2_256|esp-aes192-sha2_384|esp-aes192-sha2_512|esp-aes192-null|esp-aes192-sha1|esp-aes256-md5|esp-aes256-null|esp-aes256-sha1|esp-aes256-sha2_256|esp-aes256-sha2_384|esp-aes256-sha2_512| ah-md5-hmac|ah-sha-hmac|ah-sha2_256-hmac|ah-sha2_384-hmac|ah-sha2_512-hmac|esp-des-md5|esp-des-null|esp-des-sha1|esp-des-sha2_256|esp-des-sha2_384|esp-des-sha2_512)	
步骤6	mode (tunnel | transport)	配置协商IPSec SA的模式
步骤7	pfs (1|2|5|14)	配置pfs所使用的Diffle-Hellmen数组，缺省是disable
步骤8	set lifetime seconds <120-86400>	配置IPSec SA时间的生存期，缺省是10800秒
步骤9	exit	退出IPSec策略配置模式

以上命令均可使用 no 命令取消对各个命令的设置，使其恢复到缺省配置。

参数说明：

edit tunnel NAME：

参数	说明	缺省配置
NAME	编辑阶段2的名称	无

set peer GATEWAY：

参数	说明	缺省配置
GATEWAY	阶段1的名称	无

set （propasal1| propasal2| propasal3 ）
esp-3des-md5|esp-3des-null|esp-3des-sha1||esp-3des-sha2_256|esp-3des-sha2_384|esp-3des-sha2_512|esp-aes128-md5|esp-aes128-null|esp-aes128-sha1|esp-aes128-sha2_256|esp-aes128-sha2_384|esp-aes128-sha2_512|esp-aes192-md5|esp-aes192-sha2_256|esp-aes192-sha2_384|esp-aes192-sha2_512|esp-aes192-null|esp-aes192-sha1|esp-aes256-md5|esp-aes256-null|esp-aes256-sha1|esp-aes256-sha2_256|esp-aes256-sha2_384|esp-aes256-sha2_512|ah-md5-hmac|ah-sha-hmac|ah-sha2_256-hmac|ah-sha2_384-hmac|ah-sha2_512-hmac|esp-des-md5|esp-des-null|esp-des-sha1|esp-des-sha2_256|esp-des-sha2_384|esp-des-sha2_512)

参数	说明	缺省配置
(esp-3des-md5|esp-3des-null|esp-3des-sha1||esp-3des-sha2_256|esp-3des-sha2_384|esp-3des-sha2_512|esp-aes128-md5|esp-aes128-null|esp-aes128-sha1|esp-aes128-sha2_256|esp-aes128-sha2_384|esp-aes128-sha2_512|esp-aes192-md5|esp-aes192-sha2_256|esp-aes192-sha2_384|esp-aes192-sha2_512|esp-aes192-null|esp-aes192-sha1|esp-aes256-md5|esp-aes256-null|esp-aes256-sha1|esp-aes256-sha2_256|esp-aes256-sha2_384|esp-aes256-sha2_512| ah-md5-hmac|ah-sha-hmac|ah-sha2_256-hmac| ah-sha2_384-hmac|ah-sha2_512-hmac|esp-des-md5|esp-des-null|esp-des-sha1|esp-des-sha2_256|esp-des-sha2_384|esp-des-sha2_512)	设置封装算法（ikev2不支持AH相关算法）	缺省是esp-aes128-md5。

pfs (1|2|5)

参数	说明	缺省配置
(1|2|5|14)	配置pfs所使用的Diffle-Hellmen数组	缺省无设置

mode (tunnel | transport)

参数	说明	缺省配置
(tunnel | transport)	配置隧道的工作模式是隧道模式或传输模式	缺省隧道模式

set lifetime seconds <600-86400>

参数	说明	缺省配置
<120-86400>	配置IPSec SA时间的生存期	缺省是10800秒

19.2.6 配置国密阶段2

配置步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	edit tunnel-gb NAME	进入阶段2的配置
步骤3	set peer GATEWAY	配置阶段1的名称
步骤4	set propasal1 (esp-sm4-sm3|esp-sm1-sm3|ah-sm3-hmac)	设置阶段2的交互方案，交互方案是可接受的安全协议和算法组合。两端FW设备通过协商达成共识使用某个相同的交互方案进行IPSec通信
步骤5	mode (tunnel | transport)	配置协商IPSec SA的模式
步骤6	set lifetime seconds <120-86400>	配置IPSec SA时间的生存期，缺省是10800秒
步骤7	exit	退出IPSec策略配置模式

以上命令均可使用 no 命令取消对各个命令的设置，使其恢复到缺省配置。

参数说明：

edit tunnel-gb NAME：

参数	说明	缺省配置
NAME	编辑阶段2的名称	

set peer GATEWAY：

参数	说明	缺省配置
GATEWAY	阶段1的名称	

set （propasal1| propasal2）(esp-sm4-sm3|esp-sm1-sm3|ah-sm3-hmac)

参数	说明	缺省配置
(esp-sm4-sm3|esp-sm1-sm3|ah-sm3-hmac)	设置封装算法	缺省是esp-sm4-sm3。

set lifetime seconds <120-86400>

参数	说明	缺省配置
<120-86400>	配置IPSec SA时间的生存期	缺省是10800秒

19.2.7 配置IPsec策略

配置步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	edit ipsec-policy NAME	编辑手工配置隧道的名字
步骤4	set subnet A.B.C.D/E A.B.C.D/E	设置保护子网的地址
步骤5	set peer port <0-65535>	设置保护流量目的端口（根据需要配置）
步骤6	set local port <0-65535>	设置保护流量源端口（根据需要配置）
步骤7	set protocol <0-255>	设置保护流量协议号（根据需要配置）
步骤8	set tunnel NAME	设置阶段二隧道
步骤9	set policy enable	使能策略
步骤10	set auto-connect enable	自动触发建立隧道（可选）
步骤11	exit	退出IPSec策略配置模式

以上命令均可使用 no 命令取消对各个命令的设置，使其恢复到缺省配置。

参数说明：

set subnet A.B.C.D/E A.B.C.D/E：

参数	说明	缺省配置
A.B.C.D/E	IPSec要保护的本地和对端子网	无

set peer port <0-65535>

参数	说明	缺省配置
<0-65535>	设置保护流量的目的端口	无

set local port <0-65535>

参数	说明	缺省配置
<0-65535>	设置保护流量的源端口	无

set protocol <0-255>

参数	说明	缺省配置
<0-255>	设置保护流量协议号	无

set tunnel NAME

参数	说明	缺省配置
NAME	设置第二阶段隧道的名称	无

set auto-connect (enable|disable)

参数	说明	缺省配置
enable|disable	是否自动发起协商	disable

19.3 配置案例

注意

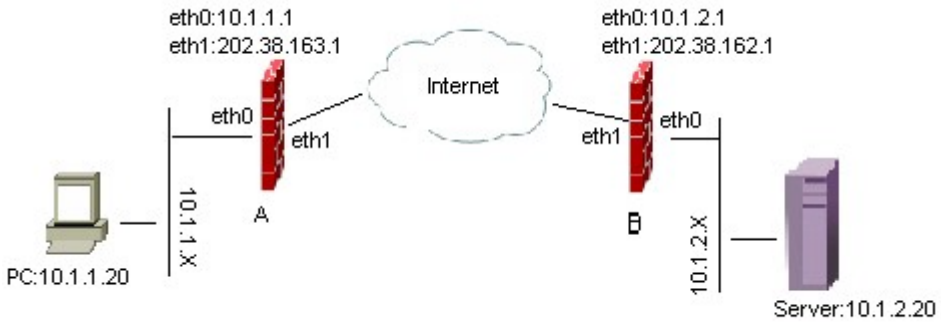
配置时，首先进入特权模式

19.3.1 配置案例1：基本IPSEC VPN应用

案例描述

假定网络环境如下图所示，PC 机到 Server 的流量需要经过各自的 FW 设备后在 Internet 上传输，为了保证流量在 Internet 传输过程中的安全性，有必要在 FW_A 和 FW_B 之间建立 IPSec 的 VPN 隧道以保障通信安全。

案例组网图



配置步骤：

FW_A 的配置：

步骤1	配置接口
	FW_A#configure terminal
	FW_A(config)# interface eth0
	FW_A(config-eth0)# ip address 10.1.1.1/24
	FW_A(config-eth0)# exit
	FW_A(config)# interface eth1
	FW_A(config-eth1)# ip address 202.38.163.1/24
	FW_A(config-eth1)# exit
步骤2	配置阶段1

```
FW_A(config)# edit gateway FW
FW_A(config-phase1-gateway)# set mode main
FW_A(config-phase1-gateway)# set remotegw 202.38.162.1
FW_A(config-phase1-gateway)#set localid address 202.38.163.1
FW_A(config-phase1-gateway)# authentication pre-share
FW_A(config-phase1-gateway)# set preshared-key 123456
FW_A(config-phase1-gateway)# lifetime 10800
FW_A(config-phase1-gateway)# group 2
FW_A(config-phase1-gateway)# set policy 1
FW_A(config-phase1-gateway-policy)# encrypt 3des
FW_A(config-phase1-gateway-policy)# hash md5
FW_A(config-phase1-gateway-policy)# exit
FW_A(config-phase1-gateway)# exit
```

步骤3 配置阶段2

```
FW_A(config)# vpn ipsec phase2
FW_A(config-phase2)# edit tunnel FW_A
FW_A(config-phase2-tunnel)# set peer FW
FW_A(config-phase2-tunnel)# mode tunnel
FW_A(config-phase2-tunnel)# set lifetime seconds 3600
FW_A(config-phase2-tunnel)# set propasal1 esp-3des-md5
FW_A(config-phase2-tunnel)# exit
```

步骤4 配置IPSec策略

```
FW_A(config)# edit ipsec-policy FW_A
FW_A(config-ipsec-policy)# set subnet 10.1.1.0/24 10.1.2.0/24
FW_A(config-ipsec-policy)# set tunnel FW_A
FW_A(config-policy)# exit
```

FW_B 的配置：

步骤1 配置接口

```
FW_B(config)# interface eth0
FW_B(config-eth0)# ip address 10.1.2.1/24
FW_B(config-eth0)# exit
FW_B(config)# interface eth1
FW_B(config-eth1)# ip address 202.38.162.1/24
FW_B(config-eth1)# exit
```

步骤2 配置阶段1

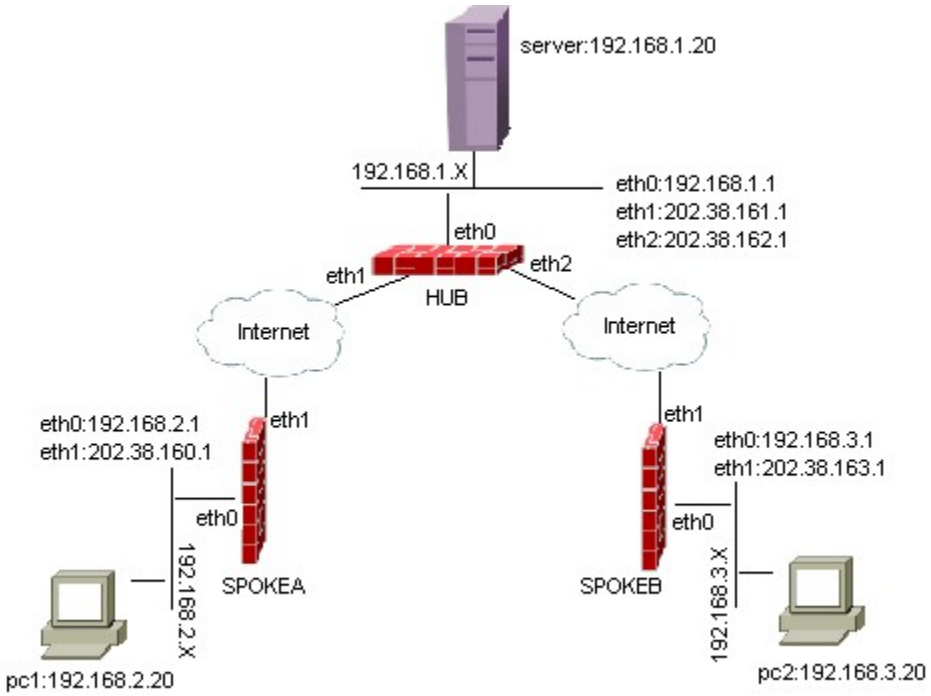
	FW_B(config)# edit gateway FW
	FW_B(config-phase1-gateway)# set mode main
	FW_B(config-phase1-gateway)# set remotegw 202.38.163.1
	FW_B(config-phase1-gateway)# set localid address 202.38.162.1
	FW_B(config-phase1-gateway)# authentication pre-share
	FW_B(config-phase1-gateway)# set preshared-key 123456
	FW_B(config-phase1-gateway)# lifetime 10800
	FW_B(config-phase1-gateway-policy)# group 2
	FW_B(config-phase1-gateway)# set policy 1
	FW_B(config-phase1-gateway-policy)# encrypt 3des
	FW_B(config-phase1-gateway-policy)# hash md5
	FW_B(config-phase1-gateway-policy)# exit
	FW_B(config-phase1-gateway)# exit
步骤3	配置阶段2
	FW_B(config)# vpn ipsec phase2
	FW_B(config-phase2)# edit tunnel FW_B
	FW_B(config-phase2-tunnel)# set peer FW
	FW_B(config-phase2-tunnel)# mode tunnel
	FW_B(config-phase2-tunnel)# set lifetime seconds 3600
	FW_B(config-phase2-tunnel)# set propasall esp-3des-md5
	FW_B(config-phase2-tunnel)# exit
步骤4	配置IPSec策略
	FW_A(config)# edit ipsec-policy FW_B
	FW_A(config-ipsec-policy)# set subnet 10.1.2.0/24 10.1.1.0/24
	FW_A(config-ipsec-policy)# set tunnel FW_B
	FW_A(config-policy)# exit

19.3.2 配置案例2：HUB-SPOKE组网应用

案例描述

假定网络环境如下图所示 SPOKEA 想要访问 SPOKEB，但是他们之间没有网络连接。必须通过 HUB 进行转发。

案例组网图



配置步骤：

HUB 的配置

步骤1	配置接口
	HUB#configure terminal
	HUB(config)# interface eth0
	HUB(config-eth0)# ip address 192.168.1.1/24
	HUB(config-eth0)# exit
	HUB(config)# interface eth1
	HUB(config-eth1)# ip address 202.38.161.1/24
	HUB(config-eth1)# exit
	HUB(config)# interface eth2
	HUB(config-eth2)# ip address 202.38.162.1/24
	HUB(config-eth2)# exit
步骤2	配置阶段1

```
HUB(config)# edit gateway spoke1
HUB(config-phase1-gateway)# set mode main
HUB(config-phase1-gateway)# set remotegw 202.38.160.1
HUB(config-phase1-gateway)# set localid address 202.38.161.1
HUB(config-phase1-gateway)# authentication pre-share
HUB(config-phase1-gateway)# set preshared-key spoke1
HUB(config-phase1-gateway)# lifetime 10800
HUB(config-phase1-gateway)# group 2
HUB(config-phase1-gateway)# set policy 1
HUB(config-phase1-gateway-policy)# encrypt 3des
HUB(config-phase1-gateway-policy)# hash md5
HUB(config-phase1-gateway-policy)# exit
HUB(config-phase1-gateway)# exit
HUB(config)# edit gateway spoke2
HUB(config-phase1-gateway)# set mode main
HUB(config-phase1-gateway)# set remotegw 202.38.163.1
HUB(config-phase1-gateway)# set localid address 202.38.162.1
HUB(config-phase1-gateway)# authentication pre-share
HUB(config-phase1-gateway)# set preshared-key spoke2
HUB(config-phase1-gateway)# lifetime 10800
HUB(config-phase1-gateway)# group 2
HUB(config-phase1-gateway)# set policy 1
HUB(config-phase1-gateway-policy)# encrypt 3des
HUB(config-phase1-gateway-policy)# hash md5
HUB(config-phase1-gateway-policy)# exit
HUB(config-phase1-gateway)# exit
```

步骤3 配置阶段2

```
HUB(config)# vpn ipsec phase2
HUB(config-phase2)# edit tunnel HUB_TO_SP1
HUB(config-phase2-tunnel)# set peer spoke1
HUB(config-phase2-tunnel)# mode tunnel
HUB(config-phase2-tunnel)# set lifetime seconds 3600
HUB(config-phase2-tunnel)# set propasal1 esp-3des-md5
HUB(config-phase2-tunnel)# exit
HUB(config)# vpn ipsec phase2
HUB(config-phase2)# edit tunnel HUB_TO_SP2
HUB(config-phase2-tunnel)# set peer spoke2
HUB(config-phase2-tunnel)# mode tunnel
HUB(config-phase2-tunnel)# set lifetime seconds 3600
HUB(config-phase2-tunnel)# set propasal1 esp-3des-md5
HUB(config-phase2-tunnel)# exit
```

步骤4 配置IPSec策略

```
HUB(config)# edit ipsec-policy HUB_TO_SP1_1
HUB(config-ipsec-policy)# set subnet 192.168.3.0/24 192.168.2.0/24
HUB(config-ipsec-policy)# set tunnel HUB_TO_SP1
HUB(config-ipsec-policy)# set policy enable
HUB(config-policy)# exit
HUB(config)# edit ipsec-policy HUB_TO_SP1_2
HUB(config-ipsec-policy)# set subnet 192.168.1.0/24 192.168.2.0/24
HUB(config-ipsec-policy)# set tunnel HUB_TO_SP1
HUB(config-ipsec-policy)# set policy enable
HUB(config-policy)# exit
HUB(config)# edit ipsec-policy HUB_TO_SP2_1
HUB(config-ipsec-policy)# set subnet 192.168.2.0/24 192.168.3.0/24
HUB(config-ipsec-policy)# set tunnel HUB_TO_SP2
HUB(config-ipsec-policy)# set policy enable
HUB(config-policy)# exit
HUB(config)# edit ipsec-policy HUB_TO_SP2_2
HUB(config-ipsec-policy)# set subnet 192.168.1.0/24 192.168.3.0/24
HUB(config-ipsec-policy)# set tunnel HUB_TO_SP2
HUB(config-ipsec-policy)# set policy enable
HUB(config-policy)# exit
```

SPOKEA 的配置

步骤1 配置接口

```
SPOKEA# configure terminal
SPOKEA(config)# interface eth0
SPOKEA(config-eth0)# ip address 192.168.2.1/24
SPOKEA(config-eth0)# exit
SPOKEA(config)# interface eth1
SPOKEA(config-eth1)# ip address 202.38.160.1/24
SPOKEA(config-eth1)# exit
```

步骤2 配置阶段 1

```
SPOKEA(config)# edit gateway spoke1
SPOKEA(config-phase1-gateway)# set mode main
SPOKEA(config-phase1-gateway)# set remotegw 202.38.161.1
SPOKEA(config-phase1-gateway)# set localid address 202.38.160.1
SPOKEA(config-phase1-gateway)# authentication pre-share
SPOKEA(config-phase1-gateway)# set preshared-key spoke1
SPOKEA(config-phase1-gateway)# lifetime 10800
SPOKEA(config-phase1-gateway)# group 2
SPOKEA(config-phase1-gateway)# set policy 1
SPOKEA(config-phase1-gateway-policy)# encrypt 3des
SPOKEA(config-phase1-gateway-policy)# hash md5
SPOKEA(config-phase1-gateway-policy)# exit
SPOKEA(config-phase1-gateway)# exit
```

步骤3 配置阶段 2

```
SPOKEA(config)# vpn ipsec phase2
SPOKEA(config-phase2)# edit tunnel SP1_TO_HUB
SPOKEA(config-phase2-tunnel)# set peer spoke1
SPOKEA(config-phase2-tunnel)# mode tunnel
SPOKEA(config-phase2-tunnel)# set lifetime seconds 3600
SPOKEA(config-phase2-tunnel)# set propasal1 esp-3des-md5
SPOKEA(config-phase2-tunnel)# exit
```

步骤4 配置 IPSec 策略

```
SPOKEA(config)# edit ipsec-policy SP1_TO_HUB_1
SPOKEA(config-ipsec-policy)# set subnet 192.168.2.0/24 192.168.1.0/24
SPOKEA(config-ipsec-policy)# set tunnel SP1_TO_HUB
SPOKEA(config-ipsec-policy)# set policy enable
SPOKEA(config-policy)# exit
SPOKEA(config)# edit ipsec-policy SP1_TO_HUB _2
SPOKEA(config-ipsec-policy)# set subnet 192.168.2.0/24 192.168.3.0/24
SPOKEA(config-ipsec-policy)# set tunnel SP1_TO_HUB
SPOKEA(config-ipsec-policy)# set policy enable
HUB(config-policy)# exit
```

SPOKEB 的配置

步骤1 配置接口

```
SPOKEB# configure terminal
SPOKEB(config)# interface eth0
SPOKEB(config-eth0)# ip address 192.168.3.1/24
SPOKEB(config-eth0)# exit
SPOKEB(config)# interface eth1
SPOKEB(config-eth1)# ip address 202.38.163.1/24
SPOKEB(config-eth1)# exit
```

步骤2	配置阶段 1
	SPOKEB(config)# edit gateway spoke2
	SPOKEB(config-phase1-gateway)# set mode main
	SPOKEB(config-phase1-gateway)# set remotegw 202.38.162.1
	SPOKEB(config-phase1-gateway)# set localid address 202.38.163.1
	SPOKEB(config-phase1-gateway)# authentication pre-share
	SPOKEB(config-phase1-gateway)# set preshared-key spoke2
	SPOKEB(config-phase1-gateway)# lifetime 10800
	SPOKEB(config-phase1-gateway)# group 2
	SPOKEB(config-phase1-gateway)# set policy 1
	SPOKEB(config-phase1-gateway-policy)# encrypt 3des
	SPOKEB(config-phase1-gateway-policy)# hash md5
	SPOKEB(config-phase1-gateway-policy)# exit
	SPOKEB(config-phase1-gateway)# exit
步骤3	配置阶段 2
	SPOKEB(config)# vpn ipsec phase2
	SPOKEB(config-phase2)# edit tunnel SP2_TO_HUB
	SPOKEB(config-phase2-tunnel)# set peer spoke2
	SPOKEB(config-phase2-tunnel)# mode tunnel
	SPOKEB(config-phase2-tunnel)# set lifetime seconds 3600
	SPOKEB(config-phase2-tunnel)# set propasal1
	esp-3des-md5SPOKEB(config-phase2-tunnel)# exit
步骤4	配置 IPSec 策略
	SPOKEB(config)# edit ipsec-policy SP2_TO_HUB _1
	SPOKEB(config-ipsec-policy)# set subnet 192.168.3.0/24 192.168.1.0/24
	SPOKEB(config-ipsec-policy)# set tunnel SP2_TO_HUB
	SPOKEB(config-ipsec-policy)# set policy enable
	SPOKEB(config-policy)# exit
	SPOKEB(config)# edit ipsec-policy SP2_TO_HUB _2
	SPOKEB(config-ipsec-policy)# set subnet 192.168.3.0/24 192.168.2.0/24
	SPOKEB(config-ipsec-policy)# set tunnel SP2_TO_HUB
	SPOKEB(config-ipsec-policy)# set policy enable
	SPOKEB(config-policy)# exit

19.4 IPSec VPN监控与维护

19.4.1 查看阶段1的SA是否建立

查看ISAKMP SA的建立

```
USG#show crypto isakmp sa
total: 1,   established: 1
  dst            src              state       expires   id  name
200.0.0.2      200.0.0.3        STATE_MAIN_I4   3560     1 tunnel1
```

可以看到总共建立了1条ISAKMP SA。本端地址是200.0.0.3，本端作为发起者与对端地址是200.0.0.2的VPN设备之间协商好的ISAKMP SA，SA距离到期重协商的时间还剩3560秒，id是1，连接的名称是tunnel1

19.4.2 查看阶段2的SA是否建立

查看IPSec SA的建立

```
USG#show crypto ipsec sa
total: 1,   established: 1
tunnel name: "tunnel1"  state: STATE_QUICK_I2 type 2
serial-id: 2
local: 200.0.0.3 peer: 200.0.0.2
local client (addr/mask/prot/port): 200.0.0.0/24/0/0
remote client (addr/mask/prot/port): 192.168.1.0/24/0/0

ESP SAs:
SA life(seconds): 2300/2400
SA life(kilobytes): 0(in) 0(out)/5120
inbound SPI: 0xEA0D2F18
outbound SPI: 0xEE0CADF1
proposal: ESP_3DES AUTH_ALGORITHM_HMAC_MD5
encapsulation: ENCAPSULATION_MODE_TUNNEL
Dead Peer Detection enable
```

可以看到建立了一条IPSec通道，该通道保护的数据流是源地址是200.0.0.0/24到目的地址是192.168.1.0/24。采用的是ESP封装，封装的加密算法是3DES，加密认证算法是MD5，工作模式是隧道模式

19.4.3 查看SA的协商过程

（列举非隐含模式下的常用 Debug 命令，应用环境，给出使用 Debug 命令后显

示的信息，并对该信息进行必要的解释与分析）

应用环境

当用户协商不成功时可以通过 ***debug ike*** 命令了解协商失败的原因，供有经验的管理员或技术人员分析。

调试实例

给出使用该调试命令显示的信息。重要的显示信息用黑体字标识。

```
USG#debug ike
"test1" #452: received Vendor ID payload [Openswan (this version) 2.6.49 ]
"test1" #452: received Vendor ID payload [Dead Peer Detection]
"test1" #452: received Vendor ID payload [RFC 3947] method set to=115
"test1" #452: enabling possible NAT-traversal with method RFC 3947
(NAT-Traversal)
"test1" #452: transition from state STATE_MAIN_I1 to state STATE_MAIN_I2
IKE : sending 228 bytes for STATE_MAIN_I1 through vlan192:500 to 192.168.31.4:500
(using #452) fd 48
"test1" #452: STATE_MAIN_I2: sent MI2, expecting MR2
initiate on demand from 192.168.32.217:0 to 192.168.100.26:0 proto=0 state:
fos_start because: acquire
packet from 192.168.31.4:4500: Informational Exchange is for an unknown
(expired?) SA with MSGID:0x8f024764
packet from 192.168.31.4:4500: Informational Exchange is for an unknown
(expired?) SA with MSGID:0x56b5245e
"test1" #452: NAT-Traversal: Result using draft-ietf-ipsec-nat-t-ike (MacOS X):
both are NATed
"test1" #452: transition from state STATE_MAIN_I2 to state STATE_MAIN_I3
IKE : sending 76 bytes for STATE_MAIN_I2 through vlan192:4500 to
192.168.31.4:4500 (using #452) fd 49
"test1" #452: STATE_MAIN_I3: sent MI3, expecting MR3
"test1" #452: received Vendor ID payload [CAN-IKEv2]
"test1" #452: Main mode peer ID is ID_IPV4_ADDR: '192.168.6.254'
"test1" #452: we require peer to have ID '192.168.31.4', but peer declares
'192.168.6.254'
"test1" #452: sending encrypted notification INVALID_ID_INFORMATION to
192.168.31.4:4500
IKE : sending 76 bytes for notification packet through vlan192:4500 to
192.168.31.4:4500 (using #452) fd 49
"test1" #452: Informational Exchange message must be encrypted
```

结果分析

对以上调试实例进行必要的分析，当出现不是预期情况的处理方法。

显示对端身份没有通过验证。

这时您需要确认：

两端的 ID 设置是否一致

19.4.4 常见故障分析

故障现象：不能建立隧道

	安全联盟协商不成功，不能建立 SA，在命令 show crypto ipsec sa 中看不到相关信息
	1）查看两端设备的相应的安全策略配置是否对称 2）阶段 1 的协商策略、验证密钥是否一致 3）阶段 2 的转换集是否一致
	1）如果安全策略配置不对称，则修改成对称 2）阶段 1 或者阶段 2 的协商策略不一致，则修改成一致

20 配置 SSL 接入管理

20.1 SSLVPN概述

SSLVPN 指的是使用者利用 SSL 协议封包处理功能，利用公司内部 SSLVPN 网关，通过网络封包转向的方式，让使用者可以在远程计算机执行应用程序，读取公司内部服务器数据。它采用标准的安全套接层（SSL）对传输中的数据包进行加密，从而在应用层保护了数据的安全性。高质量的 SSL VPN 解决方案可保证企业进行安全的全局访问。在不断扩展的互联网 Web 站点之间、远程办公室、传统交易大厅和客户端间，SSLVPN 克服了 IPSec VPN 的不足，用户可以轻松实现安全易用、无需客户端安装且配置简单的远程访问，从而降低用户的总成本并增加远程用户的工作效率。而同样在这些地方，设置传统的 IPSec VPN 非常困难，甚至是不可能的，这是由于必须更改网络地址转换（NAT）和防火墙设置。

SSLVPN 分为两种工作模式：

- Web 模式。也叫做代理 Web 页面。它将来自远端浏览器的页面请求（采用 HTTPS 协议）转发给 Web 服务器，然后将服务器的响应回传给终端用户。
- Tunnel 模式。需要、下载运行的客户端支持。客户端和 USG 设备建立 SSL 隧道后，USG 为客户端分配 IP。客户端通过建立的虚接口直接通过 SSL 隧道连接到内部网络。该种方式可支持各种应用。

20.2 配置SSLVPN

20.2.1 缺省配置信息

内容	缺省设置	备注
用户超时时间(idletime)	3600秒	可更改设置
Sslvpn服务开启(enable)	disable	可更改设置
Sslvpn服务端口(port)	10443	可更改设置

20.2.2 配置超时时间

用户登录后，在配置的超时时间内没有新的访问请求，用户将超时下线。

超时时间的配置步骤

步骤	执行命令	说明
1	configure terminal	进入全局配置模式
2	sslvpn	进入sslvpn配置模式
3	idletime [60-86400]	配置超时时间。单位为秒。范围是[60-86400]，

		默认3600秒。

使用 `no idletime` 命令恢复默认值。

20.2.3 启用SSLVPN

启用 SSLVPN 的步骤：

步骤	执行命令	说明
1	configure terminal	进入全局配置模式
2	sslvpn	进入sslvpn配置模式
3	enable	启用SSLVPN。默认为不启用

使用 no enable 禁用 SSLVPN

20.2.4 启用数据压缩

启用 SSLVPN 隧道模式数据压缩的步骤：

步骤	执行命令	说明
1	configure terminal	进入全局配置模式
2	sslvpn	进入sslvpn配置模式
3	compress enable	启用数据压缩。默认为不启用

使用 no compress enable 禁用数据压缩

20.2.5 启用客户端认证

启用 SSLVPN 客户端认证的步骤：

步骤	执行命令	说明
1	configure terminal	进入全局配置模式
2	sslvpn	进入sslvpn配置模式
3	verify-client-cert CA	启用客户端认证，配置认证的CA证书。默认为不启用

使用 no verify-client-cert 禁用客户端认证

20.2.6 启用用户唯一性检查

启用 SSLVPN 用户唯一性检查的步骤：

步骤	执行命令	说明
1	configure terminal	进入全局配置模式
2	sslvpn	进入sslvpn配置模式
3	user-exclusive	启用客户端唯一性检查。默认为不启用

使用 no user-exclusive 禁用用户唯一性检查

20.2.7 配置SSLVPN服务端口

客户端通过配置的 SSLVPN 服务端口来访问 SSLVPN 服务。

步骤：

步骤	执行命令	说明
1	configure terminal	进入全局配置模式
2	sslvpn	进入sslvpn配置模式
3	port <1-65536>	默认服务端口为：10443

使用 no port 来恢复为默认端口。

配置的端口不能与本机打开的其他端口冲突。如 web server 的默认端口 443。

20.2.8 定制SSL登录信息

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	sslvpn	进入sslvpn节点
步骤3	linkman xiaoming phone 010-89656545 email xiaoming@163.com portal-msg “welcome to use SSL-VPN”	配置联系人、电话、email、门户信息

20.2.9 删除SSL登录信息

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	sslvpn	进入sslvpn节点
步骤3	no linkman no phone no email no portal-msg	删除联系人、电话、email、门户信息

20.2.10 配置IP地址范围

此命令配置 TUNNEL 模式分配给客户端的 ip 地址范围

步骤	执行命令	说明
1	configure terminal	进入全局配置模式
2	sslvpn	进入sslvpn配置模式
3	ip-range A.B.C.D A.B.C.D	配置ip地址范围

使用 `no ip-range` 清除 ip 地址范围。


注意

起始地址不能大于结束地址

地址范围不能超过 65535

起始地址将被分配给 USG4.1 设备。

20.2.11 配置可访问的私有网络

此命令配置 TUNNEL 模式用户可以访问的私有网络，USG4.1 将为 SSLVPN 客户端添加到此网络的网段路由。

步骤	执行命令	说明
1	configure terminal	进入全局配置模式
2	sslvpn	进入sslvpn配置模式
3	private-net A.B.C.D/M	配置TUNNEL模式用户可以访问的私有网络

使用 `no private-net` 清除此配置。


注意

私有网络必须是 USG4.1 设备可以路由的。

20.2.12 配置分配给用户的DNS

此命令配置 TUNNEL 模式配置分配给用户的 DNS，USG4.1 将把 dns 配置推送给 SSLVPN 客户端。

步骤	执行命令	说明
1	configure terminal	进入全局配置模式
2	sslvpn	进入sslvpn配置模式
3	dns A.B.C.D	配置TUNNEL模式配置分配给用户的DNS

使用 `no dns` 清除此配置。

20.2.13 配置分配给用户的WINS

此命令配置 TUNNEL 模式配置分配给用户的 WINS，USG4.1 将把 WINS 配置推送给 SSLVPN 客户端。

步骤	执行命令	说明
1	configure terminal	进入全局配置模式
2	sslvpn	进入sslvpn配置模式
3	wins A.B.C.D	配置TUNNEL模式配置分配给用户的wins

使用 no wins 清除此配置。

20.2.14 配置需要过滤的HTTP方法

此命令配置 Web 访问模式 HTTP 方法过滤功能

步骤	执行命令	说明
1	configure terminal	进入全局配置模式
2	sslvpn	进入sslvpn配置模式
3	block-http-method(get|post|put|head|connect|trace|purge|options|delete|propfind|proppatch|mkcol|copy|move|lock|unlock|bmove|bdelete|bpropfind|bproppatch|bcopy|search|subscribe|unsubscribe|poll|report|other)	配置Web访问模式HTTP方法过滤功能过滤的HTTP方法

使用 no block-http-method 清除此配置。

20.2.15 启用HTML重写功能

此命令开启 Web 访问模式 HTML 重写功能

步骤	执行命令	说明
1	configure terminal	进入全局配置模式
2	sslvpn	进入sslvpn配置模式
3	html-rewrite-enable	开启sslvpn的Web访问模式的HTML重写功能

使用 no html-rewrite-enable 清除此配置。

20.2.16 配置特殊改写功能

此命令开启 Web 访问模式 HTML 的特殊改写

步骤	执行命令	说明
1	configure terminal	进入全局配置模式

2	sslvpn	进入sslvpn配置模式
3	special-rewrite	配置特殊改写的内容

20.2.17 配置SSLVPN认证用户组和用户

步骤	执行命令	说明
1	configure terminal	进入全局配置模式
2	usergroup NAME sslvpn mode (tunnel|web|all) [imprint-clean] [access-security (all-check|os-check| task-check) rule (deny|access-limit)]	配置sslvpn认证用户组 Imprint_clien为是否要清除客户端痕迹 access-security可以配置需要检查操作系统和运行进程；rule指定检查时失败时的处理方法：deny为禁止访问，access-limit 访问限制资源。
3	user access USER group GROUP	将认证的用户加入用户组

配置用户和用户组参看用户管理章节。

20.2.18 配置可访问资源

此命令配置 sslvpn 用户通过 web 模式或 agent 模式可以访问的网络资源。

Web 模式可访问：web，ftp，fileshare ,owa 资源。

步骤	执行命令	说明
1	configure terminal	进入全局配置模式
2	sslvpn	进入sslvpn配置模式
3	`resource TITLE server A.B.C.D port PORT type （web |ftp|fileshare|owa） description （null | DESCRIPTION） [enable]`	配置sslvpn用户通过web 模式或agent模式可以访问的网络资源。

使用 `no resource TITLE` 清除此配置。

20.2.19 配置可访问资源组

此命令配置 sslvpn 用户通过 web 模式或 agent 模式可以访问的网络资源组。

步骤	执行命令	说明
1	configure terminal	进入全局配置模式

2	sslvpn	进入sslvpn配置模式
3	resource-group TITLE usergrouplimit description (null | DESCRIPTION) [client-check-free]	配置sslvpn用户通过web 模式或agent模式可以访问的网络资源组。

使用 no resource-group TITLE 清除此配置。

20.2.20 配置将资源加入资源组

此命令配置将资源加入资源组。

步骤	执行命令	说明
1	configure terminal	进入全局配置模式
2	sslvpn	进入sslvpn配置模式
3	resource TITLE group TITLE	将资源加入资源组

使用 no resource TITLE group TITLE 将资源从资源组中删除。

20.2.21 配置用户组可以访问资源组

此命令配置可以访问资源组的用户组。只有资源组和用户组邦定在一起，相关用户组的用户才可以访问此资源组的资源。

步骤	执行命令	说明
1	configure terminal	进入全局配置模式
2	sslvpn	进入sslvpn配置模式
3	#resource-group TITLE group USERGROUP	配置可以访问此资源组的用户组

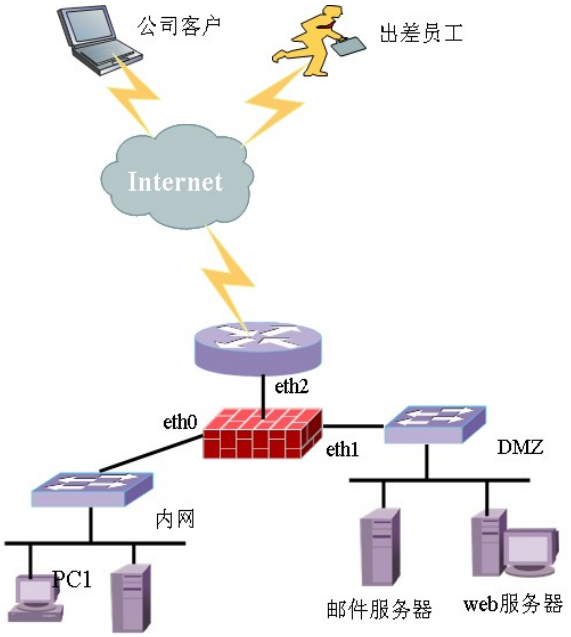
使用 no resource-group TITLE 清除此配置。

20.3 配置案例

20.3.1 配置案例1

案例描述：公司客户通过 SSLVPN web 模式，访问内网 DMZ 区域 web server。

案例组网图：



配置步骤：

步骤1	启用SSLVPN
	USG4.1(config)sslvpn USG4.1(sslvpn)enable
步骤2	配置用户和用户组
	USG4.1(config) usergroup clientgroup sslvpn mode web USG4.1(config) user access client1 local password USG4.1(config) user access client1 group clientgroup

20.3.2 配置案例2

案例描述：出差员工通过 SSLVPN TUNNEL 模式，访问内网 DMZ 区域 MAIL SERVER。

案例组网图：如案例 1 图

配置步骤：

步骤1	启用SSLVPN
	USG4.1(config)sslvpn USG4.1(sslvpn)enable
步骤2	配置分配给 sslvpn 客户端地址范围
	USG4.1(sslvpn) ip-range 30.0.0.1 30.0.0.255
步骤3	配置 tunnel 模式可访问的私有网络（dmz）
	USG4.1(sslvpn) private-net 192.168.1.0/24
步骤4	配置用户和用户组
	USG4.1(config) usergroup employeegroup sslvpn mode tunnel USG4.1(config) user access employee1 local password USG4.1(config) user access employee1 group employeegroup
步骤5	配置安全策略放通隧道流量
	USG4.1(config)# address dmz USG4.1(config-addr)# net-address 192.168.1.0/24 USG4.1(config)# address sslvpnip USG4.1(config-addr)# net-address 30.0.0.0/24 USG4.1(config) firewall policy 1 USG4.1(config-fw-policy) action permit USG4.1(config-fw-policy) enable USG4.1(config-fw-policy) src-zone tunssl USG4.1(config-fw-policy) dst-zone any USG4.1(config-fw-policy) src-addr sslvpnip USG4.1(config-fw-policy) dst-addr dmz

20.4 SSLVPN监控与维护

20.4.1 显示SSLVPN调试信息

查看步骤：

步骤	执行命令	说明
1	[no] debug sslvpn (all|event|proxy|session|tunnel)	开启/关闭调试SSLVPN模块

```
USG4.1# debug sslvpn session
check user login failed:
ip=33.0.0.2cookie=__utma=190263273.1998659089.1175739823.1175739823.1175741024.2;__utmz=190263273.1175739823.1.1.utmccn=(direct)|utmcsr=(direct)|utmcmd=(none)
check user login failed:
ip=33.0.0.2cookie=__utma=190263273.1998659089.1175739823.1175739823.1175741024.2;__utmz=190263273.1175739823.1.1.utmccn=(direct)|utmcsr=(direct)|utmcmd=(none)
logout failed :no match user SrcIP=33.0.0.2 cookie=__utma=190263273.1998659089.1175739823.1175739823.1175741024.2;__utmz=1
90263273.1175739823.1.1.utmccn=(direct)|utmcsr=(direct)|utmcmd=(none)
%sslvpn aaa auth :user=test  group=vpn
% handle sslvpn aaa auth respond...
%generage user cookie=3esu22ef99shindk38c3ctq99ut7zy42
%SrcIP=33.0.0.2 UserName=test@vpn mode=3 Content="auth ok"
```

20.4.2 查看SSLVPN用户信息

显示登录用户信息，包括用户名，ip，登录时间等。

步骤	执行命令	说明
1	show sslvpn-session	查看SSLVPN登录用户信息

```
USG4.1# show sslvpn-session
user-name      cookie      login-ip       tunnel-ip
login-time   idle  in/out
test@vpn                   2xxas2rr          202.106.0.111
10 Apr 13:27 5       0K/0K
```

20.5 常见故障分析

20.5.1 故障现象1：用户登录失败。

现象	用户登录失败。
分析	可能用户输入错误（本地认证的用户无需@用户组）
解决	输入正确的用户名（格式：username），密码。

20.5.2 故障现象2：登录用户不能访问内网

现象	用户登录成功后，不能通过 web 或 tunnel 模式访问内网
分析	可能策略不匹配，或策略没有绑定该用户所在的sslvpn用户组。
解决	检查策略配置，看是否匹配用户访问请求。检查策略是否绑定该用户所在的 sslvpn 用户组。

20.5.3 故障现象3：Tunnel模式隧道不能建立

现象	用户登录成功通过客户端软件建立隧道失败。
分析	该用户所在的用户组，没有用tunnel模式使用权限。
解决	为用户组开启 `tunnel` 模式使用权限

21 配置 L2TP

21.1 L2TP概述

PPP 定义了一种通过二层（L2）点对点连接传输多协议报文的封装机制。典型情况下，一个用户通过某种接入技术（如 ISDN，ADSL 拨号等）获得一个到网络接入服务器（NAS）的二层连接，并在该连接上进行 PPP 会话。在这样的配置中，二层终节点和 PPP 会话的终节点位于同样的物理设备上（也就是说，NAS）。

L2TP（Layer Two Tunneling Protocol）是一种二层隧道协议，它扩展了 PPP 的模型，通过二层隧道将 PPP 会话的终点延伸到另一个通过分组交换网互连的不同设备上，而不是二层接入的终节点。从而将 PPP 会话从二层终结的限制中解脱出来，扩大了 PPP 的应用范围。

L2TP 包括 LAC 和 LNS 两种功能：

- LAC（L2TP Access Concentrator）：L2TP 访问集中器。是 L2TP 隧道的一个端点，是 L2TP 网络服务器（LNS）的对等体（peer）。LAC 负责在一个 LNS 和一个远地系统之间转发 PPP 报文，并维护 LAC 和 LNS 之间的隧道（TUNNEL）和会话（SESSION）连接。
- LNS（L2TP Network Server）：L2TP 网络服务器。是 L2TP 隧道的一个端点，是 LAC 的对等体。负责维护与远地系统之间的 PPP 连接，为远地系统提供对内部网的访问服务。

L2TP 隧道给远程拨号用户提供了连接到 VPN 网关的解决方案，拨号 VPN 又称为 VPDN(virtual private dial network)。在这种应用中，由 VPN 网关提供 LNS 功能，如果拨号用户本身支持 L2TP，则可以采用自愿隧道模式直接连接到 LNS；如果拨号用户本身不支持 L2TP，则可以通过当地 ISP 提供的 LAC 功能采用强制隧道模式连接到 LNS。

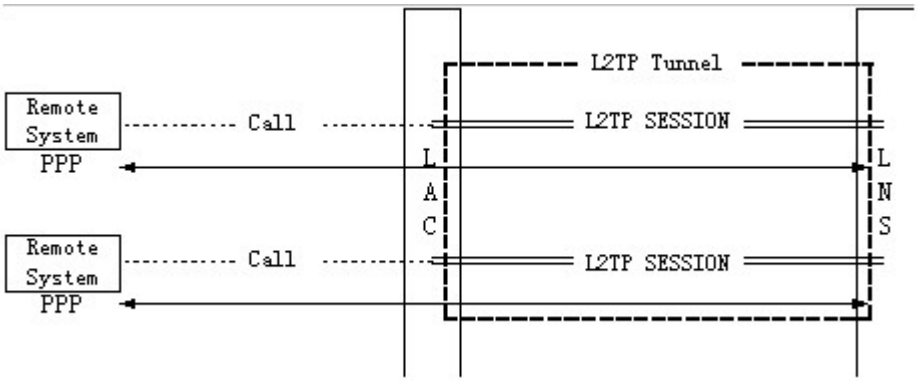
这两种连接方式的拓扑结构如下所示：

（1）L2TP 客户端直接接入 LNS

（2）拨号用户通过 LAC 远程接入 LNS

在一个 LNS 和 LAC 对之间存在着两种类型的连接，一种是隧道（tunnel）连接，它定义了一个 LNS 和 LAC 对；另一种是会话（session）连接，它复用在隧道连接之上，用于表示承载在隧道连接中的每个 PPP 会话过程。

隧道透传 PPP 帧



L2TP 连接的维护以及 PPP 数据的传送都是通过 L2TP 报文的交换来完成的，这些报文封装在 UDP 报文里从而在承载在 TCP/IP 上。

L2TP 报文可以分为两种类型，一种是控制报文，另一种是数据报文。控制报文用于隧道连接和会话连接的建立与维护。控制报文的传输是可靠的，使用了报文编号确认，滑动窗口，超时重传，隧道保活检测等机制保证控制报文的传输。数据报文则用于承载用户的 PPP 会话数据包。数据报文本身不保证可靠传输，应

该根据上层应用由上层协议保证数据报文的可靠投递。

21.2 配置L2TP

设备目前只支持 L2TP 的 LNS 功能，不支持 LAC 功能，而且 LNS 只是监听接口的 L2TP 连接请求，不会主动发起 L2TP 连接请求。

21.2.1 配置L2TP模板

设备只能配置一个 L2TP 模板，包括配置地址池，用户认证组名。设备默认没有监听地址，只要在接口上配置了启用 L2TP，都可以拨号到此接口。

配置步骤:

步骤1	configure terminal	进入配置模式
步骤2	l2tp ip A.B.C.D A.B.C.D Usergroup	配置L2TP模板

使用 no l2tp ip 可以取消对 L2TP 模板的设置，使其恢复到缺省配置。

参数说明：

命令（2）：

参数	说明	缺省配置
A.B.C.D	地址池的起始地址	无
A.B.C.D	地址池的结束地址	无
Usergroup	认证用户组名称	无

地址池地址是用来分配给拨号客户端的地址，每个拨号客户端分配一个，当分配完后，将不允许客户端再拨上来，除非某个已经拨上来的客户端释放地址。此地址不能与内网地址和其他接口地址在同一网段，以防止地址冲突。

在配置 12tp 模板前，必须先配置认证用户组，否则无法配置模版。

地址池中的第一个地址分配给服务器的 12tp 接口，不可用做分配地址。

21.2.2 配置L2TP DNS

当配置了 L2TP dns 地址，则在与客户端拨号协商时，会将此地址发给客户端，如果协商成功，客户端会将此地址设置为拨号连接的主 dns。这里不支持 second dns。

配置步骤:

步骤1	configure terminal	进入配置模式
步骤2	l2tp dns 100.1.1.102	配置L2TP DNS

如果想删除 12tp dns，使用 no 12tp dns 命令。

21.2.3 配置L2TP WINS

当配置了 L2TP wins 地址，则在与客户端拨号协商时，会将此地址发给客户端，如果协商成功，客户端会将此地址设置为拨号连接的主 wins。这里不支持 second wins。

配置步骤:

步骤1	configure terminal	进入配置模式
步骤2	l2tp wins 100.1.1.101	配置L2TP WINS

如果想删除 wins 配置，使用命令 no l2tp wins

21.2.4 配置启动L2TP功能

启动 L2TP 后，才能与拨号客户端进行通信。否则，不响应拨号客户端拨号请求。

配置步骤:

步骤1	configure terminal	进入配置模式
步骤2	l2tp enable	启动L2TP功能

使用 no l2tp enable 停止 L2TP 服务器功能。

21.2.5 配置L2TP UNIQUE

用户唯一性检查配置，若配置了此选项，在同一个时刻，同一个用户只能登陆一次。

配置步骤:

步骤1	configure terminal	进入配置模式
步骤2	l2tp unique	配置L2TP UNIQUE

如果想取消该限制，使用命令 no l2tp unique。

21.2.6 删除在线用户

在服务器端删除在线用户。

配置步骤:

步骤1	L2tp delete username[A.B.C.D]	删除某一在线用户

用户 ip 为可选输入，指的是隧道 ip。

若删除全部在线用户可以使用命令 l2tp delete all。

21.3 配置案例

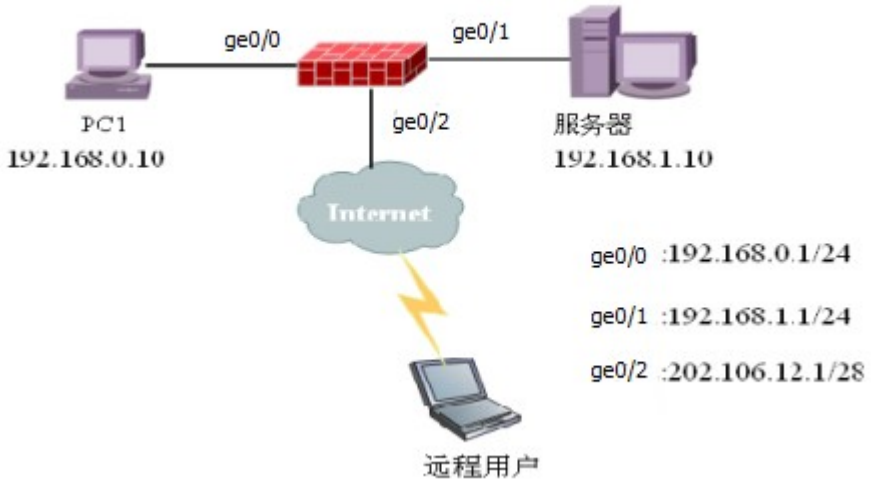
21.3.1 L2TP客户端直接连接到LNS

案例描述：

远程用户希望访问本地局域网，由于本地局域网使用的是私有地址，从 INTERNET 上不能直接访问。如果用户有 L2TP 客户端，则可以使用 L2TP 客户端远程拨入本地 VPN 网关上的 LNS，建立 L2TP 隧道，然后通过 PPP 协商由本地 VPN 网关对远程用户进行认证，并给他分配一个本地的私网地址，从而在远程用户和 LNS 之间建立一条基于 L2TP 的 VPDN 连接，使远程用户可以像本地用户一样访问本地局域网。

这里远程用户通过公网，拨号到 LNS 的 ge0/2 接口。拨号成功后，便可以像内网用户一样访问 192.168.0.0/24 和 192.168.1.0/24 两个网段了。

案例组网图



配置步骤：

步骤1	配置认证用户组
	FW_A(config)# user access test_user local test123 FW_A(config)# usergroup test_group FW_A(config)# user access test_user group test_group FW_A(config)#
步骤2	配置拨号接口
	FW_A# configure terminal FW_A(config)# interface ge0/2 FW_A(config-if)# allow l2tp FW_A(config-if)#

步骤3	配置L2TP模板
	FW_A(config)# l2tp ip 100.1.1.10 100.1.1.100 test_group
	FW_A(config)#
步骤4	启动L2TP服务
	FW_A(config)# l2tp enable
	FW_A(config)#

配置结果：

```
!
user access test_user local test123
usergroup test_group
user access test_user group test_group
 !
l2tp ip 100.1.1.10 100.1.1.100 test_group
l2tp enable
!
!
interface ge0/2
 ip address 202.106.12.1/28
 allow http
 allow l2tp
 allow telnet
!
!
```

21.4 L2TP监控与维护

21.4.1 查看 L2TP地址池配置

步骤1	显示L2TP地址池配置信息
	USG_A# show l2tp pool
	100.1.1.11 100.1.1.100 90 90
	Free addresses:
	100.1.1.11
	100.1.1.12
	100.1.1.13
	100.1.1.14

。 。 。 。 。

100.1.1.100

可以看到，可用的地址池地址从100.1.1.11到100.1.1.100。

上面的两个90分别表示地址池地址总数和可用的地址数。

21.4.2 查看 L2TP会话信息

步骤1 显示L2TP会话信息

```
USG_A# show l2tp session
user-name     login-ip        tunnel-ip       login-time      idle   in/out(kb)
test_user     202.106.12.1    100.1.1.12      18 Jul 15:06    0      7.99/2.34
```

可以看到登录用户名，用户登录地址，隧道地址、登录日期、空闲时间、流量流入流出统计等信息。

21.5 故障分析

21.5.1 L2TP客户端拨号，无法建立连接

现象	L2TP客户端直接拨号到LNS，无法建立连接。
分析	有可能是以下几种情况导致客户端无法建立连接 ● 客户端的用户名密码错误，确认一下用户名和密码。 ● 客户端指定的连接地址不是LNS拨号接口配置的地址。 ● 查看服务端配置的地址池地址是否已分配完全，是否还有可用地址。 ● L2TP接口是否执行allow l2tp.

21.5.2 L2TP建立连接后，出现异常断开

现象	L2TP客户端直接连接到LNS，出现异常断开连接。
分析	有可能是以下几种情况导致客户端无法建立连接 ● 由于网络故障导致L2TP隧道的hello报文没有应答，设备断开隧道连接。请确认网络线路没有故障，而且L2TP服务器接口正常工作。

21.6 常用调试功能

21.6.1 debug l2tp packet

应用环境:

拨号客户端请求后，服务器没有响应。

调试实例：

```
USG_A# terminal monitor
USG_A# debug l2tp packet
L2TP Rcv Packet: <- type=SCCRQ, tid=0, sid=0, Nr=0, Ns=0
L2TP Rcv Packet: <- type=SCCRQ, tid=0, sid=0, Nr=0, Ns=0
```

结果分析：

本地接收到了拨号客户端的请求报文，但是没有发送应答报文。可以查看 l2tp 配置信息，看是否执行了 l2tp enable 命令。

22 配置 DNS 代理

22.1 DNS代理概述

DNS 代理模块，主要功能是解析内网用户访问外网资源时的 DNS 请求，根据配置控制 DNS 请求的处理方法，包括转发、代理、或者本地解析。

1. 转发：直接转发 DNS 请求
2. 代理：将符合配置条件的 DNS 请求，发送到指定 DNS 服务器，支持负载均衡、会话保持和健康检查。
3. 本地解析：指定 DNS 请求的返回 IP 地址，支持轮询算法。

通过 DNS 代理模块，可以根据探测结果和预先设定的策略，将 DNS 请求转发到不同的服务器，用户就会得到比较理想的 DNS 请求结果，从而实现对带宽资源的合理利用。

22.2 配置DNS代理

22.2.1 配置DNS代理全局配置

参数	说明	缺省配置
步骤1	config terminal	进入配置模式
步骤2	dns-proxy	进入DNS代理模式
步骤3	enable/disable	启用和关闭DNS代理功能
步骤4	all-vlan enable/disable	入接口类型选项。所有接口/自定义接口
	alloc-vlan NAME	配置DNS代理自定义接口
	no alloc-vlan NAME	取消DNS代理自定义接口
	dns-proxy ip A.B.C.D port <1-65535>	配置监听地址和监听端口
	algorithm (priority rr wrr)	配置算法
	src-net NAME	配置代理内网网段
	policy (enable/disable)	启用/关闭DNS代理策略
	persist-profile NAME	配置会话保持类型

	persist-profile mask A.B.C.D	配置会话保持掩码
	persist-profile timeout <1-4294967295>	配置会话保持超时时间
步骤5	health-monitor (enable/disable)	开启/关闭健康检查
	health-monitor-domain NAME	配置健康检查域名
	health-monitor-interval <1-86400>	配置健康检查间隔
	health-monitor-maxretrys <1-10>	配置健康检查最大重试次数
步骤6	dns-server A.B.C.D nexthop A.B.C.D	配置DNS全局配置引用的DNS服务器

22.2.2 配置DNS服务器

参数	说明	缺省配置
步骤1	config terminal	进入配置模式
步骤2	dns-proxy	进入DNS代理模式
步骤3	Server A.B.C.D nexthop A.B.C.D priority <1-100>	配置DNS服务器

22.2.3 配置DNS代理策略

1，配置 DNS 代理策略

参数	说明	缺省配置
步骤1	config terminal	进入配置模式
步骤2	dns-proxy	进入DNS代理模式
步骤3	policy <1-9999> src-net NAME dst-net NAME domain NAME (permit|deny|local-query)	配置DNS代理策略
步骤4	enable/disable	启用/关闭DNS代理策略
步骤5	dns-server A.B.C.D nexthop A.B.C.D	DNS代理策略中配置dns服务器
	address ip A.B.C.D ttl <1-86400>	DNS本地解析配置IP和TTL时间

2，修改 DNS 代理策略

参数	说明	缺省配置
步骤1	config terminal	进入配置模式

步骤2	dns-proxy	进入DNS代理模式
步骤3	policy <1-9999>	进入DNS代理策略模式
步骤4	enable/disable	启用/关闭DNS代理策略
步骤5	dns-server A.B.C.D nexthop A.B.C.D	DNS代理策略中配置dns服务器
	address ip A.B.C.D ttl <1-86400>	DNS本地解析配置ip和ttl

22.3 DNS代理监控与调试

22.3.1 查看DNS代理配置信息

参数	说明	缺省配置
步骤1	enable	进入特权模式
步骤2	show dns-proxy config	查看DNS代理配置信息
步骤3	show running-config	查看正在运行的DNS代理配置

22.3.2 查看DNS代理调试信息

参数	说明	缺省配置
步骤1	enable	进入特权模式
步骤2	debug dns-proxy (event|cfg)	查看DNS代理调试信息

23 配置 DNS

23.1 DNS概述

DNS 为其他需要域名解析的模块提供域名解析客户端功能：向配置的 DNS 服务器发送域名解析请求，并接受 DNS 服务器的响应，最后将解析后的地址发送给各个使用 DNS 的模块。

23.2 配置DNS

缺省配置信息

容	缺省设置	备注
重试次数	2	不可更改设置
超时时间	5秒	不可更改设置

配置主DNS服务器

DNS 客户端首先向 DNS 主服务器请求域名解析。

步骤	执行命令	说明
1	configure terminal	进入全局配置模式。
2	ip name-server master A.B.C.D	配置主DNS服务器。

使用 no ip name-server master 清除主 DNS 服务器。

配置从DNS服务器

如果 DNS 主服务器解析失败或超时，客户端首先向 DNS 从服务器请求域名解析。

步骤	执行命令	说明
1	configure terminal	进入全局配置模式。
2	ip name-server backup A.B.C.D	配置从DNS服务器。

使用 no ip name-server backup 清除 从 DNS 服务器。

DNS查询

进行域名解析。

步骤	执行命令	说明
1	dns-lookup NAME	域名解析。

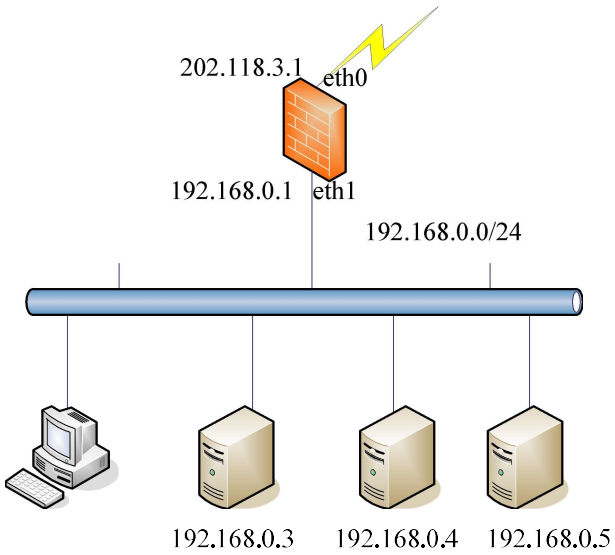
23.3 DNS监控与调试

查看DNS调试信息

步骤	执行命令	说明
1	[no] debug dnsclient	开启/关闭调试DNS模块
	host# debug dnsclient host # dns-lookup www.sina.com.cn %res_nmkquery :n=33 %Res_query: query is id-54017 qr-0 opcode-0 aa-0 tc-0 rd-1 ra-0 unused-0 rcode-0 qdcount-256 ancou nt-0 nscount-0 arcount-0 ,string length is 33 %Connect to dns server 1.1.1.1 FD:468 %connect to dns server ok %send dns request to dns server ok %res_nmkquery :n=33 %Res_query: query is id-54017 qr-0 opcode-0 aa-0 tc-0 rd-1 ra-0 unused-0 rcode-0 qdcount-256 ancou nt-0 nscount-0 arcount-0 ,string length is 33 dns lookup:www.sina.com.cn : 202.108.33.32	

23.4 配置案例

配置案例:



案例描述

DNS 服务器地址为 202.118.3.2，备份 DNS 服务器地址为 202.118.3.3。在设备上配置 DNS 服务后可以向配置的 DNS 服务器发送域名解析请求，并接受 DNS 服务器的响应，来进行域名解析。

配置步骤：

步骤1	创建一个域。
	host (config)# ip name-server master 202.118.3.2 host (config)# ip name-server backup 202.118.3.3
步骤2	查看配置信息。
	host # show running-config ! ip name-server master 202.118.3.2 ip name-server backup 202.118.3.3

23.5 常见故障分析

故障现象1：DNS解析失败

现象	DNS 解析失败。
分析	DNS服务器配置错误，或没有到DNS服务器的路由。
解决	配置正确的DNS服务器地址或添加到DNS服务器网络的路由。

24 系统参数

24.1 系统参数概述

协议管理：网络设备对不同协议的连接都有超时删除功能，以保护设备的连接资源。在本产品中，对 TCP 协议的全连接，默认超时时间是 1 小时，UDP 协议为 30 秒。有些应用程序在全连接建立后，报文只会根据实际的数据进行交互，而没有保活机制，往往会导致连接超时删除，后续的数据无法通过设备。协议管理功能提供了设置特定服务超时时间的功能，可以解决这种需要长时间空闲连接的问题。

TCP 状态管理：链接数统计时，根据此链接的 tcp 状态，决定是否统计此链接。

参数管理：一些模块功能的控制开关，统一置于此处，方便操作。

24.2 配置协议管理

配置步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	protocol manage NAME	配置一项协议管理并进入协议管理节点
步骤3	description LINE	配置描述
步骤4	protocol <TCP | UDP>	配置协议
步骤5	port <1-65535>	配置目的端口
步骤6	timeout <1-65535>	配置超时时间，单位为分钟
步骤7	end	退出到特权模式
步骤8	show protocol manage	查看配置

使用 no protocol manage NAME 命令可以删除已配置的协议管理项。

配置协议管理后，不会影响已经建立的连接，对新建的连接配置才会生效。

24.3 配置TCP状态管理

24.3.1 配置TCP全连接状态统计

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	tcp full-connect-state (established|all-connect)	配置TCP全连接状态统计
步骤3	end	返回特权模式
步骤4	show tcp full-connect-state	查看当前配置

参数说明：

参数	说明	缺省配置
established	只统计全连接	统计全部连接
all-connect	统计全部链接，全连接加上半连接	统计全部连接

24.3.2 TCP状态检查

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	ip inspect check loose	配置TCP宽松检查
步骤3	end	返回特权模式

使用”no ip inspect check loose”可以取消配置。

24.4 配置参数管理

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	app check (enable|disable)	应用识别
步骤3	ips check (enable|disable)	入侵检测
步骤4	av check (enable|disable)	病毒检测
步骤5	h323_check (enable | disable) ftp_check (enable | disable) sip_check (enable | disable) rtsp_check (enable | disable)	多链接管理
步骤6	global-path-consistency (enable|disable)	来回路径一致性
步骤7	global-path-consistency-without-route (enable | disable)	路径一致不查路由

Config terminal 节点下

使用” show expect-check”可以查看多链接管理配置。

使用” show app-global”可以查看应用识别、病毒检测、入侵检测配置。

应用识别，病毒检测，入侵检测配置默认开启，执行 show app-global 的时候，不显示，当把上述功能关闭后，再执行 show app-global 可以正确显示配置。

25 路由跟踪

25.1 路由跟踪概述

为了了解数据包在设备中的详细流程，方便用户配置和管理，设备中提供了路由跟踪功能。通过配置路由跟踪，用户能模拟一个数据包在设备中进行全流程处理，并根据相应的结果定位问题，方便用户调整配置，了解设备处理概况。

路由跟踪的输出结果主要包含：模拟的数据包经过的功能模块及处理结果。

目前支持的功能模块主要包括：安全策略的匹配，地址池的调用，会话控制策略的匹配，防护策略的匹配，用户认证策略的匹配，流量或连接数限制检查结果，NAT 地址转换，路由查询结果。

路由跟踪只显示数据包经过的功能模块。

25.2 配置路由跟踪

25.2.1 配置TCP(或UDP)协议类型的路由跟踪

协议类型为 TCP(或 UDP)的路由跟踪，需要指定源端口和目的端口参数。

配置步骤：

步骤1	packet-trace input INTERFACE_NAME (udp|tcp) A.B.C.D <0-65535> A.B.C.D <0-65535> [detail]	配置协议类型为TCP(或UDP)的路由跟踪

参数说明：

命令（1）：packet-trace input INTERFACE_NAME (udp|tcp) A.B.C.D <0-65535> A.B.C.D <0-65535> [detail]

参数	说明	缺省配置
INTERFACE_NAME	入接口	无
(udp|tcp)	协议类型	无
A.B.C.D	源IP	无
<0-65535>	源端口	无
A.B.C.D	目的IP	无
<0-65535>	目的端口	无

25.2.2 配置ICMP协议类型的路由跟踪

协议类型为 ICMP 的路由跟踪，需要指定类型、代码。

配置步骤：

步骤1	packet-trace input INTERFACE_NAME icmp A.B.C.D A.B.C.D <0-18> <0-15> [detail]	配置协议类型为ICMP的路由跟踪

参数说明：

命令（1）：packet-trace input INTERFACE_NAME icmp A.B.C.D A.B.C.D <0-18> <0-15> [detail]

参数	说明	缺省配置
INTERFACE_NAME	入接口	无
A.B.C.D	源IP	无
A.B.C.D	目的IP	无
<0-18>	类型	无
<0-15>	代码	无

25.2.3 配置ip协议类型的路由跟踪

配置协议类型为 IP 的路由跟踪，需要指定协议参数。

配置步骤：

步骤1	packet-trace input INTERFACE_NAME ip A.B.C.D A.B.C.D NUMBER [detail]	配置协议类型为IP的路由跟踪

参数说明：

命令（1）：packet-trace input INTERFACE_NAME ip A.B.C.D A.B.C.D NUMBER [detail]

参数	说明	缺省配置
INTERFACE_NAME	入接口	无
A.B.C.D	源IP	无
A.B.C.D	目的IP	无
NUMBER	协议参数	无

25.3 配置案例

25.3.1 配置案例1：配置IPv4路由跟踪

案例描述

配置 IPv4 的路由跟踪，模拟 2.1.1.4 ping 1.1.1.2 的数据包。

配置步骤：

步骤1	配置路由跟踪
	800C_3# packet-trace input vlan10 icmp 2.1.1.4 1.1.1.2 8 0 detail

配置结果：

Phase : 0

Type : CONNTRACK

Action : FORWARD

Result : success

Detail : Skb 2.1.1.4->1.1.1.2 Init conntrack, i_dev:vlan10

Conntrack 1: 2.1.1.4 -> 1.1.1.2

Phase : 1

Type : ROUTE-LOOKUP

Action : FORWARD

Result : success

Detail : Route success, odev is ge2/5, nexthop is 3.1.1.2

Phase : 2

Type : POLICY-MATCH

Action : FORWARD

Result : success

Detail : Packet matched policy, policy ID : 4, mode : permit

Phase : 3

Type : PROTECT-POLICY-MATCH

Action : FORWARD

Result : success

Detail : Packet matched protect policy, protect policy ID : 1

Phase : 4

Type : NAT-TRANS

Action : FORWARD

Result : success

Detail : Packet do SNAT, nat rule id is 1

NAT: 1 2.1.1.4 -> 1.1.1.2 >> 3.1.1.10 -> 1.1.1.2

25.3.2 配置案例2：配置Ipv6路由跟踪

案例描述

配置 IPv6 的路由跟踪，模拟 2011::2 访问 2014::2 的 80 端口的数据包。

配置步骤：

步骤1	配置路由跟踪
	800C_3# packet-trace input vlan10 tcp 2011::2 52341 2014::2 80 detail

配置结果：

Phase : 0

Type : CONNTRACK

Action : FORWARD

Result : success

Detail : Skb 2011:0000:0000:0000:0000:0000:0000:0002->2014:0000:0000:0000:0000:0000:0000:0002 Init conntrack, i_dev:vlan10

Conntrack 6: 2011:0000:0000:0000:0000:0000:0000:0002 52341 -> 2014:0000:0000:0000:0000:0000:0000:0002 80

Phase : 1

Type : ROUTE-LOOKUP

Action : FORWARD

Result : success

Detail : Route success, odev is vlan20, nexthop is 2013:0000:0000:0000:0000:0000:0000:0003

Phase : 2

Type : POLICY-MATCH

Action : FORWARD

Result : success

Detail : Packet matched policy, policy ID : 1, mode : permit

Phase : 3

Type : PROTECT-POLICY-MATCH

Action : FORWARD

Result : success

Detail : Packet matched protect policy, protect policy ID : 1

Phase : 4

Type : NAT-TRANS

Action : FORWARD

Result : success

Detail : Packet do SNAT, nat rule id is 1

NAT: 6 2011:0000:0000:0000:0000:0000:0000:0002:52341 ->
2014:0000:0000:0000:0000:0000:0000:0002:80 >>
2013:0000:0000:0000:0000:0000:0000:0001:1189 ->
2014:0000:0000:0000:0000:0000:0000:0002:80

26 SDWAN 策略

26.1 SDWAN策略概述

SDWAN 策略，是指在 SDWAN 组网环境下，符合指定条件的报文，在多出口链路的情况下，根据链路的实时质量选择出口下一跳。根据 SDWAN 策略选路的优先级和策略路由相同，高于路由选路。

链路质量检查用来探测 SDWAN 策略的下一跳的链路质量。

链路质量检查通过周期性主动发送 ICMP 探测报文的方式获得 SDWAN 策略各下一跳的延迟、抖动、丢包率等信息，以便 SDWAN 策略能够选择出更优质可靠的链路发送数据。

配置链路质量检查前，请确保被探测的目的 IP 能够正常回复 ICMP 报文。

26.2 配置SDWAN策略

26.2.1 创建SDWAN策略

配置策略路由的步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	policy-route <1-512> (IF_IN|any) (SIP|any) (DIP|any) (SEV|any) (USER|any)(APP|any)(DONAME|any)(TR|always) sdwan(min_delay|min_jitter|min_loss_rate|rr|sh|sip_port|wrr|link_replication)	配置SDWAN策略路由，将匹配策略的数据包转发至下一跳，具体配置参数见下方的参数说明。
步骤3	nexthop A.B.C.D <1-100> [<1-255>] [TEMPLATE_NAME] out-interface INTERFACE_NAME <1-100> [<1-255>] [TEMPLATE_NAME] out-ipsec-tunnel NAME<1-100> [<1-255>] [TEMPLATE_NAME]	配置下一跳地址或者出接口及其对应的权重、优先级、链路质量检查模板（可选）。若有多个下一跳，则在该视图下继续添加即可。
步骤4	policy enable	启用SDWAN策略，默认启用，可不配置
步骤5	end	返回特权模式
步骤6	show policy-route [<1-512>]	查看SDWAN策略当前配置

参数说明：

参数	说明	缺省配置
<1-512>	策略路由ID	无
(IF_IN|any)	报文入接口，不能配置为any	无
(SIP|any)	源地址对象，any表示所有源地址	无
(DIP|any)	目的地址对象，any表示所有目的地址	无
(SEV|any)	服务对象，any表示所有服务	无
(USER|any)	用户对象，any表示所有用户	无
(APP|any)	应用对象，any表示所有应用	无
(DONAME|any)	域名对象，any表示所有域名	无
(TR|always)	时间对象，always表示全部时间	无
(min_delay|min_jitter|min_loss_rate|rr|sh|sip_port|wrr|link_replication)	配置下一跳算法，min_delay为最小延迟、min_jitter为最小抖动、min_loss_rate为最小丢包率、rr为轮询、sh为源IP哈希、sip_port为源IP和端口哈希、wrr为加权轮询、link_replication为链路复制	无

注意

6. SDWAN 策略选路的优先级和策略路由相同，高于普通路由选路。
7. SDWAN 策略依据接口、源地址、目标地址等作为冲突检查。如果配置重叠或者出现冲突，则会提示配置错误。
8. 优先级越高下一跳越优，高优先级链路的链路状态都不可用后，会自动切换到低优先级下一跳转发。当高优先级故障恢复后，则再次切换到高优先级下一跳转发。
9. 链路质量检查对象若为非下一跳地址，注意设备要有到该地址的路由。
10. 对于设备直连的路由网段不匹配 SDWAN 策略转发而是查直连路由转发。
11. WOC 加速模板、链路复制算法，都是只有当下一跳为 GRE 接口或 IPSEC 隧道的情况下，才会生效。
12. 当使用最小延迟、最小抖动和最小丢包率算法时，下一跳必须引用链路质量检查模板才能获取到链路质量值并依据算法调度。

26.2.2 修改SDWAN策略

依据策略路由 ID 进入到 SDWAN 策略配置视图进行修改。

配置步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	policy-route <1-512>	输入需要修改的SDWAN策略的ID
步骤3	source-interface (IF_IN)	修改SDWAN策略的入接口
步骤4	source-addres (SIP|any)	修改SDWAN策略的源地址对象
步骤5	destination-address (SIP|any)	修改SDWAN策略的目的地址对象
步骤6	service (SEV|any)	修改SDWAN策略的服务对象
步骤7	user (USER|any)	修改SDWAN策略的用户对象
步骤8	app (APP|any)	修改SDWAN策略的应用对象
步骤9	domain-name (DONAME|any)	修改SDWAN策略的域名对象
步骤10	timerange (TR|always)	修改SDWAN策略的时间对象
步骤11	algorithm (min_delay|min_jitter|min_loss_rate|rr|sh|sip_port|wrr|link_replication)	修改SDWAN策略的负载均衡算法
步骤12	exit	返回特权模式

26.2.3 删除SDWAN策略

删除 SDWAN 策略，配置步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	no policy-route <1-512>	删除指定ID的SDWAN策略条目
步骤3	exit	返回特权模式

删除 SDWAN 策略下一跳，配置步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	policy-route <1-512>	输入需要删除指定下一跳的SDWAN策略的ID
步骤3	no nexthop A.B.C.D	删除指定下一跳地址
步骤4	exit	返回特权模式

删除 SDWAN 策略出接口，配置步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	policy-route <1-512>	输入需要删除指定出接口的SDWAN策略的ID
步骤3	no out-interface INTERFACE_NAME	删除指定出接口
步骤4	exit	返回特权模式

删除 SDWAN 策略出口 IPSEC 隧道，配置步骤：

步骤1	configure terminal	进入全局配置模式

步骤2	policy-route <1-512>	输入需要删除指定出接口的SDWAN策略的ID
步骤3	no out-ipsec-tunnel NAME	删除指定出口IPSEC隧道
步骤4	exit	返回特权模式

26.2.4 调整SDWAN策略的顺序

用 policy-route move 命令可以调整 SDWAN 策略的顺序，从而使位置在前的策略优先匹配。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	policy-route move <1-512> before <1-512>	移动一条SDWAN策略到指定的策略之前
步骤3	policy-route move <1-512> after <1-512>	移动一条SDWAN策略到指定的策略之后
步骤4	end	退出到特权模式


注意

流量匹配 SDWAN 策略时，按照顺序向下匹配，命中后不再进行后续策略匹配。当所有的 SDWAN 策略都无法匹配时，则匹配路由转发。

26.2.5 插入SDWAN策略

用 insert 命令可以创建一条新的 SDWAN 策略，并插入到指定的 SDWAN 策略之前或者之后。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	policy-route insert <1-512> (IF_IN|any) (SIP|any) (DIP|any) (SEV|any) (APP|any) (DONAME|any) (TR|always) sdwan (min_delay|min_jitter|min_loss_rate|rr|sh|sip_port|wrr|link_replication) before <1-512>	插入一条新的SDWAN策略到指定的策略之前
步骤3	policy-route insert <1-512> (IF_IN|any)(SIP|any) (DIP|any) (SEV|any)(USER|any) (APP|any) (DONAME|any) (TR|always) sdwan (min_delay|min_jitter|min_loss_rate|rr|	插入一条新的SDWAN策略路由到指定的策略之后

	sh|sip_port|wrr|link_replication) after <1-512>	
步骤4	end	退出到特权模式

26.2.6 SDWAN策略启用禁用

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	policy-route <1-512>	输入需要配置的SDWAN策略的ID
步骤3	policy (enable|disable)	启用或禁用SDWAN策略
步骤4	end	退出到特权模式

26.2.7 配置链路质量检查

可以用 healthcheck 命令添加链路质量检查模板。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	healthcheck NAME for_link_quality	创建链路质量检查模板
步骤3	end	退出到特权模式

通过以上配置可以创建一条最简单的链路质量检查配置，若需要对链路质量检查的参数进行配置，在进入链路质量检查模板后，可参考下表对应参数项进行修改。

参数说明：

参数	说明	缺省配置
detect interval<1-60>	链路质量检查发送探测包的间隔时间，单位为100毫秒。	1
maxretrys<1-10>	当报文连续超时次数达到最大重试次数时，认为当前链路质量探测失败。	3
detect link-delay<0-1000>	延时阈值，链路质量检查结果中的链路延时值超过延时阈值时认为此链路不可用，单位毫秒。	5
detect link-jitter<0-1000>	抖动阈值，链路质量检查结果中的链路抖动值超过抖动阈值时认为此链路不可用，单位毫秒。	20
detect loss-rate <0-100>	丢包阈值，链路质量检查结果中的链路丢包值超过丢包阈值时认为此链路不可用。	100
detect timeout <1-10>	发送的链路质量探测包在此时间内	1

	如果没收到回应包，则判定此报文未收到回复，单位为秒。	
detect period <10-1024>	每周期发送探测报文的个数。	60
real ipA.B.C.D	指定链路质量检查探测包的目的IPv4地址。	无
real ipv6A:B:C:D:E:F	指定链路质量检查探测包的目的IPv6地址。	无
real domain DOMAIN_NAME	链路质量检查会解析此域名并将其解析结果作为链路质量检查的目的IP。	无
source ipA.B.C.D	指定链路质量检查探测包的源IP地址。	无

注意

1. 当下一跳类型为接口或者 IPSecVPN 隧道时，必须配置源 IP、目的 IP 或覆盖域名，否则会导致链路质量检查失败。
2. 链路质量检查配置源 IP 时，源 IP 地址必须在接口上存在，否则会导致链路质量检查失败。

26.3 配置案例

案例描述：

某企业，上海分公司内网地址段 40.1.1.0/24，出口部署 FW1，北京总部内网地址段 50.1.1.0/24，出口部署 FW2，分公司员工需要直接通过内网地址访问总部的 HTTP 服务器。

上海分公司有两条出口链路，分别属于电信、网通，电信的出口公网地址为 10.10.10.10；网通出口的公网地址为 11.11.11.11。

北京总部也有两条出口链路，分别属于电信、网通，电信的出口公网地址为 20.10.10.20；网通出口的公网地址为 21.11.11.12。

上海和北京的两条出口分别使用 gre 和 ipsec 隧道打通，分部和总部之间访问时，选择延时最小的隧道进行通信。

配置步骤：

步骤1	创建两个地址对象并添加地址范围：
	fw40(config)# address shanghai
	fw40(config-addr)# net-address 40.1.1.0/24
	fw40(config)# address beijing
	fw40(config-addr)# net-address 50.1.1.0/24

步骤2	在上海分公司创建两个链路质量检查模板： fw40(config)# healthcheck GRE sh for_link_quality fw40 (config-healthcheck)# real ip 20.10.10.20 fw40 (config-healthcheck)# source ip 10.10.10.10 fw40(config)# healthcheck ipsec-sh for_link_quality fw40 (config-healthcheck)# real ip 21.11.11.12 fw40 (config-healthcheck)# source ip 11.11.11.11
步骤3	创建SDWAN策略，引用对应的地址对象、服务对象等，指定出口隧道和选路算法，引用链路质量检查模板
	fw40(config)#policy-route 1 ge0/2 shanghai beijing http any any any always sdwan min_delay fw40(config-policy-route)# out-interface gre 1 10 GREsh fw40(config-policy-route)# out-ipsec-tunnelipsec 1 10 ipsec-sh

配置结果：

fw40# show running-config

address shanghai

net-address 40.1.1.0/24

address beijing

net-address 50.1.1.0/24

!

healthcheck GRE-sh for_link_quality

detect interval 1

maxretrys 3

detect loss-rate 5

detect link-delay 100

detect link-jitter 20

detect timeout 1

detect period 10

real ip 20.10.10.20

source ip 10.10.10.10

healthcheck ipsec-sh for_link_quality

detect interval 1

maxretrys 3

detect loss-rate 5

detect link-delay 100

detect link-jitter 20

detect timeout 1

detect period 10

real ip 21.11.11.12

source ip 11.11.11.11

policy-route 1 ge0/2 shanghai beijinghttp any any any always sdwan min_delay

policy enable

session-persist disable

out-interface gre 1 10 GREsh

out-ipsec-tunnel ipsec 1 10 ipsec-sh

!

!

26.4 常见故障分析

26.4.1 SDWAN策略不生效

现象	配置SDWAN策略后没有按照SDWAN策略配置转发到对应下一跳
分析	分析可能为以下几种情况： 10. SDWAN策略没有启用。 11. 匹配上了比本条SDWAN策略优先级更高的SDWAN策略。 12. 检查SDWAN策略下一跳是否配置正确，该下一跳是否有直连路由。 13. 检查SDWAN策略下一跳链路状态检查结果是否为可用。 14. 检查源IP或者目的IP地址是否在地址对象中添加了排除。 15. 检查访问的目的网段是否在设备上有直连路由。 16. 反向报文匹配SDWAN策略，该策略中下一跳对应的出接口是否包含正向报文的入接口。 17. 依据会话信息，检查连接是否为配置开启SDWAN策略之前的连接。 18. 查看命中SDWAN策略的报文是否通过设备进行二层转发。
解决	10. 将SDWAN策略启用。 11. 可以根据需求修改SDWAN策略或者改变SDWAN策略的顺序。 12. 若依据下一跳地址查不到直连路由，则不会从该下一跳出，顺序向下匹配其他SDWAN策略。 13. 检查链路状态不可用的原因，是否下一跳地址不可达，或者链路的延迟、抖动、丢包率大于阈值，或者链路出现故障。 14. 将IP地址从排除地址中删除。 15. 有直连路由情况下，会匹配直连路由转发，不再匹配SDWAN策略，故对设备上有直连路由的网段配置SDWAN策略无效。 16. SDWAN策略的正反向报文分别匹配策略路由选路，但反向报文选路时遵循路径一致性的原则。

17. 为了避免连接断开，SDWAN策略不会影响已建流的流量转发。可以通过重新发起一个连接来确认SDWAN策略是否正确匹配。
18. 只有三层转发的报文才会进SDWAN策略的匹配流程。

27 WOC 模板

27.1 woc模板概述

WOC 有两个主要功能：双边加速和压缩，采用双边部署的方式，对 VPN 隧道的传输进行加速。在网络状况不佳的情况下，通信双方因为丢包、延迟等问题，会存在极差的网络体验。双边加速功能，使用传输协议优化技术，基于快速重传确认、选择重传等报文级别的控制，发送冗余数据缓解丢包造成的降速，使数据快速可靠的传输。压缩功能，将 IP 报文的数据部分进行压缩，节约了带宽和流量，缩短下载时间。WOC 功能的应用于网络质量不佳的链路上，能加速和优化数据传输，提升用户体验。

27.2 配置woc模板

27.2.1 配置woc模板

woc 模板可配置压缩，双边加速。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	woc-profile NAME	配置woc模板
步骤3	compress (enable|disable)	开启压缩
步骤4	accelerate (enable|disable)	开启双边加速
步骤5	end	返回特权模式
步骤6	show woc-profile [NAME]	显示woc模板配置

使用 no woc-profile NAME 可以删除已经配置的 woc 模板。

参数说明：

命令（1）：woc-profile NAME

参数	说明	缺省配置
<NAME>	woc模板的名称	无

命令（2）：compress (enable|disable)

参数	说明	缺省配置
enable	开启压缩	无
disable	关闭压缩	无

命令（3）：accelerate (enable|disable)

参数	说明	缺省配置
enable	开启双边加速	无
disable	关闭双边加速	无

27.3 配置案例

27.3.1 添加woc模板

案例描述

配置一个 woc 模板，名称为 woc_pub，开起压缩和双边加速。

配置步骤：

步骤1	创建一个woc模板
	host(config)# woc-profile woc_pub
步骤2	在这个模板中开启压缩
	host(config-woc)# compress enable
步骤3	在这个模板中开启双边加速
	host(config-woc)# accelerate enable
步骤4	显示添加信息
	host# show woc-profile woc-profile woc_pub compress enable accelerate enable host#

27.4 常见故障分析

27.4.1 故障现象1：

现象	执行no woc-profile NAME以后，该woc模板仍然存在。
分析	当一个woc模板为预定义或正在被引用时，就不能通过no命令删除。
解决	可以先撤销其它配置对该woc模板的引用，再用no命令删除该节点。

28 防火墙策略

28.1 防火墙策略概述

为了对数据流进行统一控制，方便用户配置和管理，防火墙引入了防火墙策略的概念。

通过配置防火墙策略能够对经过设备的数据流进行有效的控制和管理。当设备收到数据报文时，把该报文的方向、源地址、目的地址、协议、端口等信息和用户配置的策略匹配，决定是否建立这条数据流，并且把这条流和匹配的策略关联起来，从而确定如何处理该流的后续报文，实现允许、丢弃，决定哪些用户和数据能进出，以及它们进出的时间和地点。

防火墙策略可以配置所属策略组，方便对策略进行分组匹配和管理。策略按页面策略组前后顺序和组内规则的排列顺序进行匹配。对通过设备的数据包进行处理，对于到设备本身的数据包和设备本身发出的数据包不进行限制。

28.2 配置策略组

28.2.1 配置策略组

用 firewall policy group 命令来配置一个策略组。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	firewall policy group (ipv4|ipv6) NAME	配置一个ipv4或者ipv6策略组
步骤3	end	返回特权模式
步骤4	show (ipv4|ipv6) firewall policy group	查看ipv4或者ipv6策略组的配置

28.2.2 插入策略组

用 insert 命令可以创建一个新的策略组，并插入到指定的策略组之前。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	firewall policy group (ipv4|ipv6) NAME insert before NAME	插入一个ipv4或者ipv6策略组
步骤3	end	返回特权模式
步骤4	show (ipv4|ipv6) firewall policy group	查看ipv4或者ipv6策略组的配置

28.2.3 移动策略组

用 move 命令可以调整策略组的顺序，从而使位置在前的策略组优先匹配。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	firewall policy group (ipv4|ipv6) move NAME before NAME	移动一个策略组到指定的策略组之前
步骤3	firewall policy group (ipv4|ipv6) move NAME after NAME	移动一个策略组到指定的策略组之后
步骤4	end	退出到特权模式
步骤5	show (ipv4|ipv6) firewall policy group	查看ipv4或者ipv6策略组的配置

28.2.4 删除策略组

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	no firewall policy group (ipv4|ipv6) NAME type (move-subpolicy|del-subpolicy)	删除一个策略组，并且指定策略组下策略的处理动作：移动或者删除。
步骤3	end	退出到特权模式
步骤4	show (ipv4|ipv6) firewall policy group	查看ipv4或者ipv6策略组的配置

move-subpolicy： 删除策略组时，将策略组下策略移动到“default”策略组。

del-subpolicy：删除策略组时，将策略组下策略一起删除。

28.3 配置防火墙策略

28.3.1 配置防火墙策略

防火墙策略的基本要素是匹配条件和动作。匹配条件包括数据流的方向、源地址、目的地址、用户、服务、应用和策略生效的时间范围。其中，数据流的方向通过指定入接口、出接口、源地址和目的地址来确定，服务、应用和时间范围都可以直接引用已定义的对象。

策略的动作有 PERMIT，DENY，不同的动作下又有不同的可选配置，从而决定对符合匹配条件的数据流实现哪些业务。

用 firewall policy 命令来配置一条策略，在策略模式下指定该策略的基本要素。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	firewall policy <1-30000>	配置一条防火墙策略，ID范围为

		<1-30000>，如果不指定，系统会自动分配一个ID
步骤3	src-zone (IF_IN|any)	配置数据流的流入接口，可以指定某个接口或安全域，any表示所有接口
步骤4	dst-zone (IF_IN|any)	配置数据流的流出接口，可以指定某个接口或安全域，any表示所有接口
步骤5	src-addr (SADDR|any)	配置数据流的源地址，可以引用已定义的某个地址对象或地址对象组，any表示源地址为所有地址对象
步骤6	dst-addr (DADDR|any)	配置数据流的目的地址，可以引用已定义的某个地址对象或地址对象组，any表示目的地址为所有地址对象
步骤7	service (ah|aol|bgp|bootpc|bootps|daytime|dhcp|dns||esp||finger|ftp|gopher|gre|h323|hostname|http|https|icmp|igmp|ike|imap|info_adress|info_request|irc|internet-locator- service|l2tp|ldap|mysql|netmeeting|netbios-ns|netbios-dgm|netbios-ssn|nfs|nicname|nntp|ntp|onc-rpc|osf|pc-anywhere|pim|ping|ping6|pop2|pop3|pptp|printer|quake|radius|radius-acct|raudio||rexec|rip|rlogin|rsh|samba|sccp|sip|sip-man messenger|shell|smtp|smux|snmp|socks|aquid|ssh|syslog|talk|tcp|telnet|tftp|time|timestamp|tproxy|udp|uucp|vdolive|wais|webcache|winframe|who|x-windows|SRV_OBJ|any)	配置数据流的服务属性，包括协议、源端口和目的端口，可以引用系统预定义服务、自定义的服务对象或服务对象组，any表示为所有服务
步骤8	app (APP|any)	指定数据流的应用属性，可以引用已定义的某个应用对象或应用对象组，any表示为所有应用
步骤9	user (USER|any)	指定数据流的用户属性，可以引用已定义的某个用户对象或用户组,any表示为所有用户
步骤10	timerange (TR|always)	指定策略生效的时间，可以引用已配置的时间对象TR，always表示所有时间范围
步骤11	action (permit|deny)	配置策略的模式，允许或拒绝
步骤12	name NAME	配置策略的名称，策略名称不能重复，可选配置，不配置时名称为空
步骤13	end	返回特权模式

步骤14	show running-config firewall policy	查看策略的当前配置

使用 no firewall policy <1-30000>可以删除这条策略。


注意

1、 策略 ID 是防火墙策略的唯一标识。
2、 创建一条策略时，默认动作是 permit。
3、 命令行配置支持基于五元组创建策略，创建一条策略时，必须至少指定源地址、目的地址、服务属性，策略才为挂载可匹配的状态，其他属性（如用户、应用等）可不配置，不配置的属性表示对应项任何对象都可以匹配，相当于 any。

28.3.2 启用防火墙策略

防火墙策略缺省是不启用的，配置好一个防火墙策略之后用 enable 命令可以启用该策略，使其生效。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	firewall policy <1-30000>	对于一条已经配置好的防火墙策略，可以用该命令进入策略模式
步骤3	enable	启用该策略
步骤4	end	退出到特权模式
步骤5	show running-config firewall policy	查看防火墙策略的当前配置

使用 no enable 可以恢复缺省配置，即不启用该防火墙策略。

28.3.3 描述防火墙策略

用 description 命令可以描述一条防火墙策略的功能信息。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	firewall policy <1-30000>	对于一条已经配置好的防火墙策略，可以用该命令进入策略模式
步骤3	description LINE	为该策略添加描述信息
步骤4	end	退出到特权模式
步骤5	show running-config firewall policy	查看防火墙策略的当前配置

使用 no description 可以清除该策略的描述信息

28.3.4 移动防火墙策略

用 move 命令可以调整防火墙策略的顺序，从而使位置在前的策略优先匹配。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	firewall policy move <1-30000> before<1-30000>	移动一条策略到指定的策略之前
步骤3	firewall policy move <1-30000> after<1-30000>	移动一条策略到指定的策略之后
步骤4	end	退出到特权模式
步骤5	show running-config firewall policy	查看防火墙策略的当前配置

28.3.5 插入防火墙策略

用 insert 命令可以创建一条新的防火墙策略，并插入到指定的策略之前。

步骤1	config terminal	进入配置模式
步骤2	firewall policy insert before <1-30000>	插入一条新策略到指定的策略之前，策略ID由系统自动分配
步骤3	end	退出到特权模式
步骤4	show running-config firewall policy	查看防火墙策略的当前配置

28.3.6 配置防火墙策略的日志

用 log 命令可以启用 syslog 功能。在模式为 deny 的防火墙策略中，匹配该策略的数据流被阻断的信息被发往 syslog 服务器，在模式为 permit 的防火墙策略中，匹配该策略的数据流创建和拆除的信息被发往 syslog 服务器，日志的优先级为 LOG_INFO。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	firewall policy <1-30000>	对于一条已经配置好的防火墙策略，可以使用该命令进入策略模式
步骤3	log (policy |session-end| session-start）	启用策略的syslog功能。log policy只有当策略动作为deny时可配置，Log session-end 和 log session-start只有当策略动作为permit时可配置。
步骤4	end	退出到特权模式
步骤5	show running-config firewall policy	查看防火墙策略的当前配置

使用 no log (policy |session-end| session-end）可以停用 syslog 功能

28.3.7 配置防火墙策略的流量统计

在模式为 permit 的防火墙策略中，用 flowstat 命令可以启用流量统计功能，统计匹配该策略的数据流量。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	firewall policy <1-30000>	对于一条已经配置好的防火墙策略，可以使用该命令进入策略模式
步骤3	flowstat	启用流量统计功能
步骤4	end	退出到特权模式
步骤5	show running-config firewall policy	查看防火墙策略的当前配置

使用 no flowstat 可以停用流量统计功能


注意

只有模式为 permit 的防火墙策略才能配置流量统计功能。

28.3.8 配置防火墙策略的会话超时时间

在模式为 permit 的防火墙策略中，用 timeout 命令可以配置匹配策略的会话的超时时间，不配置时，为会话的协议默认超时时间。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	firewall policy <1-30000>	对于一条已经配置好的防火墙策略，可以使用该命令进入策略模式
步骤3	timeout <1-65535> [min]	配置匹配策略的会话的超时时间，单位默认为秒，可以配置分钟
步骤4	end	退出到特权模式
步骤5	show running-config firewall policy	查看防火墙策略的当前配置

使用 no timeout 可以恢复会话的协议默认超时时间


注意

只有模式为 permit 的防火墙策略才能配置会话超时时间。

28.3.9 配置防火墙策略所属的策略组

配置策略所属的策略组，便于对策略实行分组管理。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	firewall policy <1-30000>	对于一条已经配置好的防火墙策略，可以使用该命令进入策略模式
步骤3	firewall-policy-group NAME	配置策略所属的策略组
步骤4	end	退出到特权模式
步骤5	show running-config firewall policy	查看防火墙策略的当前配置

系统预定义"default"策略组，策略默认属于“default”策略组。

使用 show (ipv4|ipv6) firewall policy group detail NAME，可以查看策略组下包含策略数。

28.3.10 配置防火墙策略匹配的默认动作

设置防火墙策略的匹配的默认动作，当匹配不到防火墙策略的时候，执行设置的默认动作。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	default-policy action (accept|drop)	将默认的动作设置为permit或者deny
步骤4	end	退出到特权模式
步骤5	show default-policy action	查看防火墙策略的默认动作

28.3.11 配置防火墙策略全局匹配

通过匹配模块的设置可以开启或者关闭整个匹配的流程

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	policy-match (enable|disable)	开启或者关闭整个策略匹配的流程
步骤4	end	退出到特权模式
步骤5	show policy-match switch	查看安全匹配模块的开启关闭状态

28.3.12 配置防火墙策略预编译

通过防火墙策略预编译的设置可以切换防火墙策略的匹配方式，在大量防火墙策略配置下，开启预编译匹配方式可以提高性能。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	policy-precompile (enable|disable)	开启或者关闭策略预编译
步骤3	policy-precompile start	预编译当前防火墙策略配置
步骤4	policy-precompile-auto (enable|disable)	开启或者关闭自动预编译
步骤5	policy-precompile-auto interval <1-86400>	调整自动预编译时间间隔，默认30s
步骤6	show policy-precompile-auto interval	查看自动预编译时间间隔，默认配置不显示
步骤7	show policy-precompile status	查看策略预编译的开启关闭状态

28.4 配置案例

28.4.1 案例1：创建防火墙策略允许区域互访

案例描述

设备的 vlan1 连接内网，配置策略允许内网用户在非工作时间访问外网。

配置步骤：

步骤1	创建地址对象Intranet t
	(config)# address Intranet
	(config-addr)# net-address 10.1.1.0/24
	(config-addr)# exit
步骤2	配置时间对象Non-working
	(config)# schedule recurring Non-working
	(config-schd)# absolute 00-01-01 00:00:00 99-01-01 00:00:00
	(config- schd)# periodic 08:30:00 17:30:00 null null null null null saturday sunday
步骤3	配置防火墙策略，允许非工作时间内网访问外网
	(config-fw-policy)#firewall policy 1
	(config-fw-policy)#src-zone vlan1
	(config-fw-policy)#dst-zone any
	(config-fw-policy)#src-addr Intranet
	(config-fw-policy)#dst-addr any
	(config-fw-policy)#service any
	(config-fw-policy)#timerange Non-working
	(config-fw-policy)#app any
	(config-fw-policy)#user any
	(config-fw-policy)#action permit
步骤4	启用配置的策略
	(config)#firewall policy 1
	(config-fw-policy)#enable
步骤4	查看防火墙策略配置
	host#show firewall policy 1

28.5 防火墙策略监控与维护

28.5.1 查看防火墙策略的配置

查看某防火墙策略配置信息的步骤

步骤1	显示某条防火墙策略的配置信息

	(config)#show firewall policy 1 action permit enable match statistic: 0 status: mount firewall-policy-group default src-zone vlan1 dst-zone any src-addr Intranet dst-addr any service any timerange Non-working user any app any 可以看到策略1的配置信息，所属策略组为deault，指定了入接口为vlan1，出接口为any，源地址为定义的地址对象Intranet，目的地址为定义的地址对象any，服务对象为any，应用对象为any，时间为定义好的周期时间对象，状态为enable，即该策略生效，动作为permit，即匹配上前几个要素的数据流防火墙允许通过。

28.5.2 查看数据流和防火墙策略的匹配情况

查看某防火墙策略配置信息的步骤

当数据包的方向、源地址、目的地址、协议、端口等信息和某条策略中配置的要素都相符却无法执行相应动作的时候，为了在终端显示该调试信息，需要执行命令 terminal monitor。

步骤1	显示调试信息
	(config)# terminal monitor (config)# debug policy packet

注意	由于此命令会在命令行上打印大量的信息，占用很多 CPU 资源，所以在调试结束的时候，一定要用 no debug policy packet 命令禁用此功能。

28.6 常见故障分析

28.6.1 匹配上某条策略的数据流没有执行相应的动作

现象	匹配上某条策略的数据流没有执行相应的动作（阻断、放行）

分析	有可能是以下几种情况导致该策略无法生效： 1、 策略匹配没有开启，请查看策略匹配的状态是否为enable。 2、 该策略没有启用，请检查策略状态是否为enable。 3、 由于策略按页面顺序进行匹配，数据流可能匹配到前面的某条策略，请检查配置是否冲突。 4、 配置的防火墙策略是针对到设备本地的访问。 5、 检查是否开启了策略预编译，且开启后有过策略修改。
解决	1、 启用策略匹配，修改策略匹配状态为enable。 2、 启用策略，修改该策略状态为enable。 3、 依据需求调整策略顺序。 4、 防火墙策略只对转发流量生效，不对到设备本地的流入或流出流量进行控制。 5、 若开启了策略预编译后策略进行了修改没有重新预编译还是会按照以前的策略匹配执行，可将预编译开关关闭或重新执行策略预编译，再验证策略匹配。

29 本地安全策略

29.1 本地安全策略概述

通过配置本地安全策略，能够对访问本机的数据流进行有效的控制和管理。当设备收到数据报文时，把该报文的入接口、源地址、目的地址以及服务与用户配置的策略匹配，决定是否建立这条数据流，并且把这条流和匹配的策略关联起来，从而确定如何处理该流的后续报文，实现允许、丢弃，决定哪些用户和数据能够访问本机。

29.2 配置本地安全策略

29.2.1 创建本地安全策略

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	local-policy <1-512> (IF_IN|any) (SIP|any) (DIP|any) ("SRV_OBJ|any") (permit|deny)	创建一条本地安全策略，ID范围为<1-512>，匹配条件包含入接口、源地址、目的地址和服务，动作为permit和deny。
步骤13	end	返回特权模式
步骤14	show local-policy	查看策略的当前配置

使用 no local-policy <1-512>可以删除这条策略。

29.2.2 启用本地安全策略

本地安全策略缺省是不启用的，配置好一个本地安全策略之后用 enable 命令可以启用该策略，使其生效。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	local-policy <1-512>	对于一条已经配置好的本地安全策略，可以用该命令进入策略模式
步骤3	enable	启用该策略
步骤4	end	退出到特权模式
步骤5	show local-policy	查看本地安全策略的当前配置

使用 no enable 可以恢复缺省配置，即不启用该本地安全策略。

29.2.3 描述本地安全策略

用 description 命令可以描述一条本地安全策略的功能信息。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	local-policy <1-512>	对于一条已经配置好的本地安全策略，可以用该命令进入策略模式
步骤3	description .LINE	描述该策略
步骤4	end	退出到特权模式
步骤5	show local-policy	查看本地安全策略的当前配置

使用 no description 可以清除该策略的描述信息

29.2.4 移动本地安全策略

用 move 命令可以调整本地安全策略的顺序，从而使位置在前的策略优先匹配。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	local-policy move <1-512> before <1-512>	移动一条策略到指定的策略之前
步骤3	local-policy move <1-512> after <1-512>	移动一条策略到指定的策略之后
步骤4	end	退出到特权模式
步骤5	show local-policy	查看本地安全策略的当前配置

29.2.5 插入本地安全策略

用 insert 命令可以创建一条新的本地安全策略，并插入到指定的策略之前。

步骤1	config terminal	进入配置模式
步骤2	local-policy insert <1-512> (IF_IN|any) (SIP|any) (DIP|any) ("SRV_OBJ|any ") (permit|deny) before <1-512>	插入一条新策略到指定的策略之前
步骤3	end	退出到特权模式
步骤4	show local-policy	查看本地安全策略的当前配置

29.2.6 配置本地安全策略的日志

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	local-policy <1-512>	对于一条已经配置好的本地安全策略，可以用该命令进入策略模式
步骤3	log	启用日志
步骤4	end	退出到特权模式
步骤5	show local-policy	查看本地安全策略的当前配置

使用 no log 可以关闭日志功能

29.2.7 配置本地安全策略匹配的默认动作

设置本地安全策略的匹配的默认动作，当匹配不到本地安全策略的时候，执行设置的默认动作。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	default-local-policy action (accept|drop)	将默认的动作设置为accept或者deny
步骤3	end	退出到特权模式
步骤4	show default-local-policy action	查看本地安全策略的默认动作

29.2.8 配置本地安全策略全局匹配

通过匹配模块的设置可以开启或者关闭整个匹配的流程

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	local-policy-match (enable|disable)	开启或者关闭整个策略匹配的流程
步骤3	end	退出到特权模式
步骤4	show local-policy-match switch	查看本地安全匹配模块的开启关闭状态

29.3 配置案例

29.3.1 案例：阻断不安全用户访问设备

案例描述

阻断某些不安全用户访问设备。

配置步骤：

步骤1	创建地址对象 nosecurity
	(config)# address nosecurity (config-addr)# net-address 10.1.1.0/24 (config-addr)# exit
步骤2	配置本地安全策略，阻断不安全用户访问设备
	(config)# local-policy 1 any nosecurity any any deny
步骤3	启用策略
	(config)# local-policy 1 (config)#enable
步骤4	查看策略配置
	(config)#show local-policy 1

29.4 本地安全策略监控与维护

29.4.1 查看本地安全策略的配置

查看某条本地安全策略配置信息的步骤

步骤1	显示某条本地安全策略的配置信息
	(config)#show local-policy 1 local-policy 1 any nosecurity any any deny enable log description nosecurity match statistic: 0 可以看到策略1的配置信息，指定了入接口为any，源地址为定义的地址对象nosecurity，目的地址对象any，服务对象为any，状态为enable，即该策略生效，动作为deny，即匹配上前几个要素的数据流被阻断。

29.4.2 查看数据流和本地安全策略的匹配情况

当数据包的方向、源地址、目的地址、协议、端口等信息和某条策略中配置的要素都相符却无法执行相应动作的时候，为了在终端显示该调试信息，需要执行命令 terminal monitor。

步骤1	显示调试信息
	(config)# terminal monitor (config)# debug local-policy packet

由于此命令会在命令行上打印大量的信息，占用很多 CPU 资源，所以在调试结束的时候，一定要用 no debug local-policy packet 命令禁用此功能。

30 配置防护策略

30.1 安全防护策略概述

为了防止网络设备受到恶意攻击，防火墙加入了攻击防护功能。

通过配置安全防护策略能够对经过设备的数据流进行有效的监控，并判断是否受到了恶意攻击。若设备开启了安全防护功能，设备会将收到数据报文的源地址、目的地址、协议、服务等信息和用户配置的安全防护策略进行匹配，判断此报文是否需要判断攻击，如果需要则把这条流与匹配的攻击策略关联起来，且省略该流的后续报文匹配策略的动作，而符合策略的报文则根据配置的某种防护功能（包括攻击防护、入侵防护、病毒防护、web 防护、威胁情报）对报文进行处理，从而决定哪些数据包能进出、哪些数据包需要丢弃。

在没有配置任何攻击防护策略的情况下，对于经过设备的所有数据包，其缺省为不开启策略匹配。

安全防护策略在 IPv4 或 IPv6 配置相同入接口时，按照从上往下的匹配原则，只对通过设备的数据包进行处理，对于设备本身发出的数据包不进行限制。

30.2 配置安全防护策略

防护策略的基本要素是匹配条件和动作。匹配条件包括数据流的方向、源地址、目的地址、用户、服务和策略生效的时间范围。其中，数据流的方向通过指定入接口、源地址、目的地址来确定，用户、服务和时间范围都可以直接引用已定义的对象。

攻击防护策略按 IPv4 或 IPv6 从上往下匹配的原则，只对通过防火墙的数据包进行处理，对于设备本身发出的数据包不进行限制。

30.2.1 缺省配置信息

防火墙设备关于攻击防护的防护策略的缺省设置信息如以下表格所示：

表30-1 攻击防护的缺省配置信息

内容	缺省设置	备注
防护策略使能	disable	可更改设置
日志过滤	disable	可更改设置

30.2.2 创建防护策略

步骤：

步骤1	configure terminal	进入配置模式
步骤2	protect-policy id dev src dst sev user tr	配置一个攻击防护策略，并进入攻击防护策略配置节点

参数说明：

命令：protect-policy id dev src dst sev user tr

参数	说明	缺省配置
<id >	攻击防护策略id号	无
<dev>	入接口	any
<src>	源地址	any
<dst>	目的地址	any
<sev>	服务	any
<user>	用户组	any
<tr>	时间表	always

30.2.3 攻击防护策略引用威胁情报

步骤：

步骤1	configure terminal	进入配置模式
步骤2	protect-policy id dev src dst sev user tr	配置一个攻击防护策略，并进入攻击防护策略配置节点
步骤3	threat-intelligence-profile NAME	引用威胁情报策略

参数说明：

命令：threat-intelligence-profile NAME

参数	说明	缺省配置
<NAME>	威胁情报名称	无

使用 no threat-intelligence-profile 可以取消对威胁情报策略的引用。

30.2.4 插入攻击防护策略

步骤：

步骤1	configure terminal	进入配置模式
步骤2	protect-policy insert 2 any any any x-windows user always before 1	将攻击策略2插入到攻击策略1之前

30.2.5 移动攻击防护策略顺序

步骤：

步骤1	configure terminal	进入配置模式
步骤2	protect-policy move 1 before 2	移动攻击防护策略1到2之前
	protect-policy move 1 after 2	移动攻击防护策略1到2之后

30.2.6 启用攻击防护策略

步骤：

步骤1	configure terminal	进入配置模式
步骤2	protect-policy id	进入攻击防护配置节点
步骤3	enable	启用攻击防护策略

使用 no enable 命令可以取消启用攻击防护策略。

30.3 配置案例

30.3.1 配置一条攻击防护策略

案例描述

配置一个入接口为 ge0/3,源地址为 any,目的地址为 any,服务为 http,时间表为 anytime 的攻击防护策略，引用的威胁情报为 test1，并开启攻击防护策略。

步骤1	进入配置模式
	host# config terminal
步骤2	创建攻击防护策略
	host(config)# protect-policy 11 ge0/3 any any any any always
步骤3	引用威胁情报test1
	host(config-protect-policy)# threat-intelligence-profile test1
步骤4	使能这个攻击防护策略
	host(config-protect-policy)# enable
步骤5	开启威胁情报日志
	log threat-intelligence-profile

配置结果：

host# show protect-policy 11

protect-policy 11 ge0/3 any any any always

enable

match statistic: 0

threat-intelligence-profile test1

log threat-intelligence-profile

30.4 防扫描监控与维护

30.4.1 查看防护策略配置

查看防护策略配置的步骤：

步骤	进入enable模式执行show running-config protect-policy

查看配置结果：

host#

host# show running-config protect-policy

!!

protect-policy 11 ge0/3 any any any any always

enable

threat-intelligence-profile test1

log threat-intelligence-profile

!

protect-policy-match enable

!

kernel-tcp-syncookies enable

!

host# 11是防护策略id号; *ge0/3*是防护策略配置的入接口名称,enable表示启用这条防护策略，test1是这条攻击防护策略引用的威胁情报的名称。

30.5 常见故障分析

30.5.1 故障现象：某些应该匹配上某条策略的数据流没有匹配上该策略

现象	匹配上某条策略的数据流没有受到相应的限制。某些应该匹配上某条策略的数据流没有匹配上该策略。
分析	有可能是以下几种情况导致该策略无法生效： 1.该策略没有启用，请检查策略状态是否为启用； 2.由于策略在IPv4或IPv6有相同入接口时按从上往下的原则进行匹配，数据流可能匹配到前面的某条策略，请检查配置是否冲突。
解决	启用该策略，如果和其他策略的配置冲突，可以根据需求修改策略或者改变策略的顺序。

31 配置攻击防护

31.1 攻击防护概述

攻击防护是防 FLOOD 攻击和防扫描安全功能的配置模版。攻击防护功能需要在安全防护策略中引用才能起作用。符合策略的报文则根据攻击防护中的配置实现告警、丢弃、syncookie 等动作，从而决定哪些数据包能进出、哪些数据包需要丢弃。

31.2 配置攻击防护

攻击防护需要在防护策略中引用。

31.2.1 缺省配置信息

防火墙设备关于攻击防护缺省设置信息如以下表格所示：

表31-1 攻击防护的缺省配置信息

内容	缺省设置	备注
防Flood模块使能	disable	可更改设置
防TCP Flood攻击	disable	可更改设置
防UDP Flood攻击	disable	可更改设置
防ICMP Flood攻击	disable	可更改设置
防Scan模块使能	disable	可更改设置
防TCP Scan攻击	disable	可更改设置
防UDP Scan攻击	disable	可更改设置
防Ping Sweep攻击	disable	可更改设置
扫描识别门限	1000	可更改设置
对源主机的阻断时间	20	可更改设置

31.2.2 创建攻击防护

步骤：

步骤1	configure terminal	进入配置模式
步骤2	protect-profile NAME	配置一个攻击防护，并进入攻击防护配置节点

使用 no protect-profile NAME 可以删除一个攻击防护。

31.2.3 配置攻击防护的描述

可以对配置的攻击防护进行简短的说明以描述相关功能。描述信息最多支持 128 个字符(64 个中文)。

步骤：

步骤1	description DESC	配置攻击防护的描述信息

使用 no 命令可以取消相关配置。

31.2.4 配置防TCP Flood

选择启用 TCP 协议的防 Flood 攻击功能。TCP Flood 即 SYN Flood 攻击，是众多攻击形式的一种方式。SYN Flood 利用 TCP 协议的缺陷，向服务器端发送大量伪造的 TCP 连接请求之后，自身不再做出应答，使得服务器端的资源迅速耗尽，从而无法及时处理其它正常的服务请求，严重的时候甚至会导致服务器系统的崩溃。

防火墙的防 SYN Flood 攻击采用了业界最新的 syncookie 技术，在很少占用系统资源的情况下，可以有效地抵御 SYN Flood 对受保护服务器的攻击。

限制类型：每主机报文速率限制(源 IP)、每主机报文速率限制(目的 IP)、总报文速率限制。

识别门限：配置 syn 报文个数的阈值，即防 TCP Flood 攻击的启动门限，缺省配置为 100。

动作：阻断、告警、syncookie。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	protect-proflie test	配置一个名为test的攻击防护
步骤3	antiflood enable	使能防flood功能
步骤4	antiflood syn (src-host|dest-host|total) packet-rate <1-10000>	选择限制类型。同时配置1秒钟限制的报文个数。
步骤5	antiflood syn action (alarm|drop|syncookie)	选择动作
步骤6	end	返回特权模式
步骤7	show protect-profile test	显示配置的安全防护表信息

no antiflood syn (src-host|dest-host|total)可以取消相关配置，使其恢复到缺省配置。

31.2.5 配置防UDP Flood

选择启用 UDP 协议的防 Flood 攻击功能。

限制类型：每主机报文速率限制(源 IP)、每主机报文速率限制(目的 IP)、总报文速率限制。

识别门限：配置 UDP 报文个数的阈值，即防 UDP Flood 攻击的启动门限，缺省配置为 100。

动作：阻断、告警

与配置防 TCP Flood 相似步骤，配置防 UDP Flood。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	protect-proflie testudp	配置一个名为testudp的攻击防护
步骤3	antiflood enable	使能防flood功能
步骤4	antiflood udp (src-host|dest-host|total) packet-rate <1-10000>	选择限制类型。同时配置1秒钟限制的报文个数。
步骤5	antiflood udp action (alarm|drop)	选择动作
步骤6	end	返回特权模式
步骤7	show protect-profile testudp	显示配置的安全防护表信息

no antiflood udp (src-host|dest-host|total)可以取消相关配置，使其恢复到缺省配置。

31.2.6 配置防ICMP Flood

选择启用 ICMP 协议的防 Flood 攻击功能。

限制类型：每主机报文速率限制(源 IP)、每主机报文速率限制(目的 IP)、总报文速率限制。

识别门限：配置 ICMP 报文个数的阈值，即防 ICMP Flood 攻击的启动门限，缺省配置为 100。

动作：阻断、告警

与配置防 TCP Flood 相似步骤，配置防 ICMP Flood。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	protect-proflie testicmp	配置一个名为testicmp的攻击防护
步骤3	antiflood enable	使能防flood功能
步骤4	antiflood icmp (src-host|dest-host|total) packet-rate <1-10000>	选择限制类型。同时配置1秒钟限制的报文个数。
步骤5	antiflood icmp action (alarm|drop)	选择动作
步骤6	end	返回特权模式
步骤7	show protect-profile testicmp	显示配置的安全防护表信息

no antiflood icmp (src-host|dest-host|total)可以取消相关配置，使其恢复到缺省配置。

31.2.7 配置防TCP Scan

根据实际网络情况，当受到 tcp scan 扫描攻击时，可以配置防 tcp 扫描攻击。

当一个源 IP 地址在 1 秒内将含有 tcp Syn 片段的 IP 封包发送给位于相同目标 IP 地址的不同端口数量或不同目标的同一个端口大于配置的门限值时,即认为其进行了端口扫描，系统将其标记为 tcp scan，并在配置的阻断时间内拒绝来自于该台源主机的所有其它 tcp Syn 包。

启用防 tcp scan 扫描攻击，可能会占用比较多的内存。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	protect-proflie test	配置一个名为test的攻击防护
步骤3	antiscan enable	使能防scan功能
步骤4	antiscan tcp	配置防TCP Scan攻击
步骤5	end	返回特权模式
步骤6	show protect-profile	显示配置的安全防护表信息

使用 no antiflood tcp 可以取消对防 TCP Scan 的设置，使其恢复到缺省配置。

31.2.8 配置防UDP Scan

根据实际网络情况，当受到 udp scan 扫描攻击时，可以配置防 udp scan 扫描攻击。当一个源 IP 地址在 1 秒内将含有 udp 的 IP 封包发送给位于相同目标 IP 地址的不同端口数量或不同目标的同一个端口大于配置的门限值时，即进行了一次端口扫描，系统将其标记为 udp scan，并在配置的阻断时间内拒绝来自于该台源主机的所有其它 udp 包。

启用防 UDP Scan 扫描攻击，可能会占用比较多的内存。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	protect-proflie test	配置一个名为test的攻击防护
步骤3	antiscan enable	使能防scan功能
步骤4	antiscan udp	配置防UDP Scan攻击
步骤5	end	返回特权模式
步骤6	show protect-profile	显示配置的安全防护表信息

使用 no antiflood udp 可以取消对防 UDP Scan 的设置，使其恢复到缺省配置。

31.2.9 配置防Ping sweep

根据实际网络情况，当受到 Ping sweep 扫描攻击时，可以配置防 Ping sweep 扫描攻击。当一个源 IP 地址在 1 秒内发送给不同主机的 ICMP 封包超过门限值时，即进行了一次地址扫描。此方案的目的是将 ICMP 封包(通常是应答请求) 发送给各个主机，以期获得至少一个回复，从而查明目标地址。设备在

内部记录从某一远程源地点发往不同地址的 ICMP 封包数目。当某个源 IP 被标记为地址扫描攻击，则系统在配置的阻断时间内拒绝来自该主机的其它更多 ICMP 封包。

启用防 Ping sweep 扫描攻击，可能会占用比较多的内存。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	protect-proflie test	配置一个名为test的攻击防护
步骤3	antiscan enable	使能防scan功能
步骤4	antiscan ping	配置防PING Sweep攻击
步骤5	end	返回特权模式
步骤6	show protect-profile	显示配置的安全防护表信息

使用 no antiflood ping 可以取消对防 Ping sweep 的设置，使其恢复到缺省配置。

31.2.10 配置扫描识别门限

用 threshold 可以配置防扫描功能的扫描识别门限，超过门限值时，该源 IP 被标记为扫描攻击，来自于该台源主机的所有其它攻击包都被阻断。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	protect-proflie test	配置一个名为test的攻击防护
步骤3	antiscan enable	使能防scan功能
步骤4	antiscan threshold <10-65535>	配置扫描识别门限
步骤5	end	返回特权模式
步骤6	show protect-profile	显示配置的安全防护表信息

使用 no antiscan threshold 可以取消对扫描识别门限的设置，使其恢复到缺省配置。

31.2.11 配置对源主机的阻断时间

用 block-time 命令可以设置阻断时间，当系统检测到扫描攻击时，在配置的阻断时间内拒绝来自于该台源主机的所有其它攻击包。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	protect-proflie test	配置一个名为test的攻击防护
步骤3	antiscan enable	使能防scan功能
步骤4	antiscan block-time <1-65535>	配置防扫描的阻断时间
步骤5	end	返回特权模式

步骤6	show protect-profile	显示配置的安全防护表信息

使用 no antiscan block-time 可以取消对防扫描阻断时间的设置，使其恢复到缺省配置。

31.2.12 攻击防护策略引用安全防护表

步骤：

步骤1	configure terminal	进入配置模式
步骤2	protect-policy id	进入指定id的防护策略配置节点
步骤3	protect-profile NAME	防护策略引用攻击防护
步骤4	log-profile	使能攻击防护日志功能

使用 no protect-policy id 命令删除该攻击防护策略。

31.3 配置案例

31.3.1 攻击防护中配置防Flood

案例描述

配置一个名为 test1 的攻击防护，表中 1）开启防 TCP Flood 中的限制每主机报文速率功能（源 ip），限制个数为 1100，动作选择 syncookie。2）开启防 UDP Flood 中的限制每主机报文速率功能（目的 ip），限制个数为 1200，动作选择丢包。3）开启防 ICMP Flood 中的限制总报文速率限制功能，限制个数为 1300，动作选择告警。4）开启日志功能

配置步骤：

步骤1	进入配置模式
	host# config terminal
步骤2	创建一个名字为test1的攻击防护
	host(config)# protect-profile test1
步骤3	防Flood功能使能
	host(config-profile)# antiflood enable
步骤4	开启防TCP Flood中的限制每主机报文速率功能（源ip），限制个数为1100
	host(config-profile)# antiflood syn src-host packet-rate 1100
步骤5	配置Tcp Flood的动作为syn_cookies
	host(config-profile)# antiflood syn action syn_cookies
步骤6	开启防UDP Flood中的限制每主机报文速率功能（目的ip），限制个数为1200
	host(config-profile)# antiflood udp dest-host packet-rate 1200
步骤7	配置Udp Flood的动作为丢弃
	host(config-profile)# antiflood udp action drop
步骤6	开启防ICMP Flood中的限制总报文速率功能，限制个数为1300
	host(config-profile)# antiflood icmp total packet-rate 1300

步骤7	配置ICMP Flood的动作为告警
	host(config-profile)# antiflood icmp action alarm

配置结果：

```
host# show protect-profile test1
protect-profile test1
 antiflood enable
 antiflood syn src-host packet-rate 1100
 antiflood syn action syn_cookies
 antiflood udp dest-host packet-rate 1200
 antiflood udp action drop
 antiflood icmp total packet-rate 1300
 antiflood icmp action alarm
```

31.3.2 安全防护表中配置防Scan

案例描述

在名为 test1 的安全防护表中使能防扫描功能，并开启 TCP 协议扫描，扫描识别阀值设置为 200，主机抑制时长设置为 40

步骤1	进入配置模式
	host# config terminal
步骤2	进入安全防护表test1
	host(config)# protect-profile test1
步骤3	使能防扫描功能
	host(config-profile)#antiscan enable
步骤4	开始TCP协议扫描功能
	host(config-profile)# antiscan tcp
步骤5	设置扫描识别阀值
	host(config-profile)# antiscan threshold 200
步骤6	设置主机抑制时长
	host(config-profile)# antiscan block-time 40

配置结果：

```
host# show protect-profile test1
protect-profile test1
 antiscan enable
 antiscan tcp
 antiscan block-time 40
 antiscan threshold 200
```

31.4 防扫描监控与维护

31.4.1 查看安全防护表配置

查看安全防护表配置的步骤：

步骤	用show protect-profile NAME 查看名为NAME的安全防护表的配置 用show protect-profile 查看所有安全防护表的配置

查看配置结果：

```
host# show protect-profile test1
!!
protect-profile test1
 antiflood enable
 antiflood syn src-host packet-rate 1100
 antiflood syn action syn_cookies
 antiscan enable
 antiscan tcp
 antiscan block-time 40
 antiscan threshold 200
!
```

test1是安全防护表的名字，可以看出名为test1的安全防护表开启了日志，防Flood功能使能，开启了TCP协议防Flood功能，源主机目标的门限值为1100，动作为syncookie。没有开启防UDP Flood和防ICMP Flood。防扫描功能使能，开启的是防TCP协议扫描，主机阻断时间为40s，扫描识别阀值为200.

31.4.2 查看被防扫描阻断的源IP

查看被防扫描阻断的源 IP 的步骤：

步骤	用show protect-policy-antiscan block-ip 查看被防扫描阻断的源IP

查看配置结果：

```
host# show protect-policy-antiscan block-ip
ip 128.1.1.6      protect-policy test
ip 128.1.1.5      protect-policy test
ip 128.1.1.4      protect-policy test
```

上面列出了被攻击策略test阻断的源IP地址

31.5 常见故障分析

31.5.1 故障现象：防flood功能不能正常工作

现象	防flood功能不能正常工作。

分析	若策略匹配成功，但是防flood功能不起作用，有可能是以下几种情况导致防flood功能无法生效： ● 检查安全防护对象中的防flood总开关是否勾选； ● 由于防flood中分为syn flood、udp flood、icmp flood，检查报文类型是否选对 ● 检查所配置的门限值是否过大 ● 检查所配置的防flood的动作是否正确
解决	修改原有配置，以保证防flood功能能正常工作。

31.5.2 故障现象：配置防扫描后没有报警，没有拒包

现象	通过抓包或流收集后，确定确实受到了扫描攻击，而此时设备没有报警，没有拒包。
分析	可能是以下几种情况导致： ● 扫描识别门限设置得太大，导致扫描计数还没有达到门限值。 ● 同时配置了防扫描、防Syn Flood和会话管理中的TCP半连接数目限制，三者功能有重叠，可能导致防扫描功能未起作用
解决	检查配置，如果是因为门限值设置得太大，根据实际需求修改到合适的值。

32 配置病毒防护

32.1 病毒防护概述

针对内外网入口处进行实时的病毒扫描，将外来病毒隔离在内网之外，实现工作站被动防御病毒之外的主动病毒防御。同时还提供文件扫描功能，可以对特定的文件类型进行扫描。我们可以在诸如 HTTP、FTP、IMAP、POP3、SMTP 等应用协议时进行文件扫描。

32.2 配置病毒防护模板

32.2.1 新建病毒防护模板

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	av-profile NAME protocol PROTONAME action (permit|deny)	新建或者修改病毒防护模板
步骤3	end	返回特权模式
步骤4	show av profile [NAME]	查看病毒防护模板当前配置

使用 no av-profile NAME 可以删除病毒防护模板。

参数说明：

参数	说明	缺省配置
NAME	模板名称	无
PROTONAME	匹配的应用协议，包括 HTTP、FTP、IMAP、POP3、SMTP	无
permit	配置模板的模式为放行	无
deny	配置模板的模式为阻断	无

32.2.2 防护策略引用病毒防护模板

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	protect-policy <1-9999>	对于一条已经配置好的防护策略，可以使用该命令进入策略模式
步骤3	av-profile NAME	引用病毒防护模板
步骤4	log av-profile	开启病毒防护日志

步骤5	end	退出到特权模式
步骤6	show protect-policy	查看防护策略的当前配置

使用 no av-profile 取消引用的病毒防护模板，使用 no log av-profile 关闭日志。

只有防护策略引用了病毒防护模板，才能够配置日志。
取消引用病毒防护模板，日志也会关闭。

32.3 配置扫描文件类型

32.3.1 扫描方式配置

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	av-file any enable	扫描一切文件类型
步骤3	end	退出到特权模式
步骤4	show av-file cfg	查看扫描方式

使用 av-file any disable 取消扫描一切文件类型，改为扫描指定文件类型方式。

32.3.2 新增文件类型

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	av-file EXPR (enable|disable)	若文件类型已存在，修改启用与不启用；不存在，新增文件类型，并配置启用不启用
步骤3	end	退出到特权模式
步骤4	show av-file	查看文件类型配置

使用 no av-file EXPR 删除文件类型。

32.3.3 指定文件类型的全部启用与禁用

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	av-file all enable	启用全部的指定文件类型
步骤3	end	退出到特权模式
步骤4	show av-file	查看文件类型配置

使用 av-file all disable 禁用全部的指定文件类型。

32.4 病毒防护监控

32.4.1 查看命中情况

查看数据包是否命中病毒模板，为了在终端显示该调试信息，需要执行命令 terminal monitor。

步骤1	显示调试信息
	host# terminal monitor host# debug av check


注意

由于此命令会在命令行上打印大量的信息，占用很多 CPU 资源，所以在调试结束的时候，一定要用 no debug av check 命令禁用此功能。

33 配置入侵防护

33.1 入侵防护概述

随着互联网的飞速发展，网络环境也变得越来越复杂，恶意攻击、木马、蠕虫病毒等混合威胁不断增大，单一的防护措施已经无能为力，企业需要对网络进行多层、深层的防护来有效保证其网络安全，而入侵防御系统(IPS)则是提供深层防护体系的保障。

防火墙设备入侵防御利用事件特征可以检测到特定的网络行为，并可以选择放行、阻断、阻断源 ip 等动作，以达到保护网络的功能。 防火墙设备入侵防御的事件特征库可以动态升级，以实时跟踪最新的网络威胁，保护网络的安全。

33.2 配置入侵防护事件集

33.2.1 新建事件集

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	ips set NAME	新建事件集
步骤3	end	返回特权模式
步骤4	show ips set [NAME]	查看事件集的当前配置

使用 no ips set NAME 可以删除事件集。

33.2.2 配置描述

用 description 命令可以描述一个事件集的功能信息。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	ips set NAME	对于一个已经配置好的事件集，可以用该命令进入事件集模式
步骤3	description .LINE	配置描述
步骤4	end	退出到特权模式
步骤5	show ips set [NAME]	查看事件集的当前配置

使用 no description 可以取消描述。

33.2.3 配置自动更新

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	ips set NAME	对于一个已经配置好的事件集，可以用该命令进入事件集模式
步骤3	update-with-ips (enable|disable)	配置该事件集是否随特征库的更新而更新
步骤4	end	退出到特权模式
步骤5	show ips set [NAME]	查看事件集的当前配置

33.2.4 配置防护级别

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	ips set NAME	对于一个已经配置好的事件集，可以用该命令进入事件集模式
步骤3	level (high|middle|low)	配置防护级别
步骤4	end	退出到特权模式
步骤5	show ips set [NAME]	查看事件集的当前配置

使用 no level 可以恢复到默认级别，默认级别为低。

33.2.5 配置事件集抓包

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	ips set NAME	对于一个已经配置好的事件集，可以用该命令进入事件集模式
步骤3	ips-set capture (enable|disable)	配置事件集抓包是否启用
步骤4	ips-set capture deal_num <1-20>	配置单条流抓包个数，仅对扩展抓包生效
步骤5	end	退出到特权模式
步骤6	show ips set [NAME]	查看事件集的当前配置

33.2.6 防护策略引用事件集

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	protect-policy <1-9999>	对于一条已经配置好的防护策略，可以使用该命令进入策略模式
步骤3	ips-set NAME	引用事件集

步骤4	log ips	开启ips日志
步骤5	end	退出到特权模式
步骤6	show protect-policy	查看防护策略的当前配置

使用 no ips-set 取消引用的事件集，使用 no log ips 关闭日志。

只有防护策略引用了入侵防护事件集，才能够配置日志。取消引用事件集，日志也会关闭。

33.3 配置基于事件的安全类别ID的过滤

配置步骤：

步骤1	show ips filter sec-id all	查看安全ID与类别的对应关系
步骤2	config terminal	进入配置模式
步骤3	ips filter sec-id ("IPS_SEC_ID") disable	对相应的类别进行过滤
步骤4	end	退出到特权模式
步骤5	show ips filter sec-id disable	查看被过滤掉的类型

使用 ips filter sec-id ("IPS_SEC_ID") enable 取消过滤。

33.4 全局配置-阻断源ip时间

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	ips timeout <0-9999>	阻断源ip时间，单位分钟
步骤3	end	退出到特权模式
步骤4	show ips timeout	查看阻断时间

33.5 全局配置-事件集自动更新配置

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	ips add-custom-level level-low (y|n) level-mid (y|n) level-high (y|n) level-serious (y|n)	需要更新到自定义事件集中的事件等级，分别为：低级事件、中级事件、高级事件、严重事件。
步骤3	ips add-custom-action (no-change|pass)	需要更新到自定义事件集中的事件动作：不变、放行。
步骤4	end	退出到特权模式
步骤5	show ips customset-update-cfg	查看阻断时间

33.6 全局配置-配置IPS抓包

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	ips capture type (base|extend)	配置抓包方式
步骤3	ips capture timeout <1-720>	配置抓包时间
步骤4	ips capture rate <0-1000>	配置抓包速率
步骤5	ips capture once_catch <0-10>	配置事件抓包次数
步骤6	ips capture (enable|disable)	启用/禁用在线抓包
步骤7	end	退出到特权模式
步骤8	show ips capture cfg	查看当前ips抓包的配置

33.7 入侵防护监控

33.7.1 查看事件的命中情况

查看数据包是否命中事件，为了在终端显示该调试信息，需要执行命令 terminal monitor。

步骤1	显示调试信息
	# terminal monitor # debug ips check

注意

由于此命令会在命令行上打印大量的信息，占用很多 CPU 资源，所以在调试结束的时候，一定要用 no debug ips check 命令禁用此功能。

33.7.2 查看抓包信息

查看数据包抓包信息，为了在终端显示该调试信息，需要执行命令 terminal monitor。

步骤1	显示调试信息
	# terminal monitor # debug ips capture

注意

由于此命令会在命令行上打印大量的信息，占用很多 CPU 资源，所以在调试结束的时候，一定要用 no debug ips capture 命令禁用此功能。

34 配置 Web 防护

34.1 Web防护概述

Web 防护策略防护的攻击有两种，分别是 XSS 攻击和 SQL 注入攻击。XSS 是一种经常出现在 web 应用中的计算机安全漏洞，它允许恶意 web 用户将代码植入到提供给其它用户使用的页面中，这些代码包括 HTML 代码和客户端脚本。SQL 注入攻击也是黑客对数据库进行攻击的常用手段之一，该攻击针对相当大一部分代码没有对用户输入数据的合法性进行判断的现状，通过提交一段数据库查询代码，根据程序返回的结果，获得某些数据。

本模块基于特征库的方式对两种攻击进行防御，针对两种攻击采用特征匹配的方式，对通过 HTTP 提交的信息采用模式匹配的方式进行检查，发现符合 xss/sql 特征的攻击，即提交日志，并根据预设的动作阻断或者放行连接。

34.2 配置Web防护

34.2.1 缺省配置信息

防火墙设备关于 Web 防护的缺省设置信息如以下表格所示：

表34-1 Web 防护的缺省配置信息

内容	缺省设置	备注
SQL注入	disable	可更改设置
动作	deny	可更改设置
XSS攻击	disable	可更改设置
动作	deny	可更改设置

34.2.2 新建Web防护策略

根据命令行提示创建 Web 防护策略。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	web-security-profile NAME (sql-enable|sql-disable) (permit|deny) (xss-enable|xss-disable) (permit|deny)	配置Web防护相关的过滤信息
步骤3	End	返回特权模式
步骤4	show web-security-profile	显示所有Web防护策略配置

NAME：Web 防护策略名称。

(sql-enable|sql-disable)：sql 注入防护是否启用。

(permit|deny) ：对符合匹配条件的数据流执行的动作。

(xss-enable|xss-disable)：xss 攻击防护是否启用。

(permit|deny) ：对符合匹配条件的数据流执行的动作。

34.2.3 删除Web防护策略

根据策略名称删除指定的 Web 防护策略。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	no web-security-profile NAME	删除指定名字的Web防护策略
步骤3	end	返回特权模式
步骤4	show web-security-profile	显示所有Web防护策略配置

34.2.4 修改某一策略的匹配信息

根据策略的名字，进入到策略内部对匹配信息进行修改。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	web-security-profile NAME (sql-enable|sql-disable) (permit|deny) (xss-enable|xss-disable) (permit|deny)	配置sql注入和xss攻击防护的规则

34.2.5 查询Web防护策略的配置

根据命令查看所有 Web 防护策略配置或指定策略名称的策略配置。

配置步骤：

步骤1	show web-security-profile	显示所有Web防护策略配置
步骤2	show web-security-profile NAME	显示指定名称的策略配置

35 配置威胁情报

35.1 威胁情报概述

威胁情报防护通过查询离线库和云端平台得到 IP 地址和域名的威胁情况，对用户访问的目的 IP 地址和域名进行威胁等级检查，如果发现有 IP 地址或者域名的威胁情况超过策略中设置的防护等级，即提交日志，并根据预设的动作阻断或者放行。

35.2 配置威胁情报

35.2.1 新建威胁情报策略

根据命令行提示创建威胁情报策略。

配置步骤

步骤1	configure terminal	进入配置模式
步骤2	threat-intelligence NAME	配置威胁情报名称
步骤3	desc DESC	配置威胁情报描述
步骤4	threat-type (any|ransomware|mining-software|e-bank-trojan|steal-trojan|hacking-tools|backdoor-software|botnet|regular-trojan|dga|dark-industry|scanning-detection|covert-tracking|suspicious-threat|directed-attack|worm-virus|apt-attack|other-control)	配置威胁类型
步骤5	check (all | ip | domain)	配置查询类型
步骤6	protect-level (high | middle | low)	配置防护等级
步骤7	action (permit | deny)	配置动作
步骤8	end	返回特权模式
步骤9	show threat-intelligence	显示所有威胁情报策略配置

参数说明：

参数	说明	缺省配置
NAME	威胁情报策略名称	无
DESC	威胁情报策略描述	无
(any|ransomware|mining-software|e-bank-trojan|steal-trojan|hacking-tools|backdoor-software|botnet|regular-trojan|dga|dark-industry|scanning-detection|covert-tracking|suspicious-threat|directed-attack|worm-virus|apt-attack|other-control)	威胁情报策略匹配的威胁类型	无
(all | ip | domain)	进行威胁情报检查的类型	无
(high | middle | low)	威胁情报策略的防护等级	无
(permit|deny)	对符合匹配条件的数据流执行的动作	无

35.2.2 删除威胁情报策略

根据策略名称删除指定的威胁情报策略。

配置步骤

步骤1	configure terminal	进入配置模式
步骤2	no threat-intelligence NAME	删除指定名字的威胁情报策略
步骤3	end	返回特权模式
步骤4	show threat-intelligence	显示所有威胁情报策略配置(默认配置不显示)

35.2.3 修改威胁情报策略

根据策略名称，进入到策略内部对匹配信息进行修改。

配置步骤

步骤1	configure terminal	进入配置模式
步骤2	threat-intelligence NAME	进入该策略配置模式
步骤3	desc DESC	配置威胁情报描述
步骤4	threat-type (any|ransomware|mining-software|e-bank-trojan|steal-trojan|hacking-tools|backdoor-software|botnet|regular-trojan|dga	配置威胁类型

	|dark-industry|scanning-detection|covert-tracking|suspicious-threat|directed-attack|worm-virus|apt-attack|other-control)	
步骤5	check (all | ip | domain)	配置查询类型
步骤6	protect-level (high | middle | low)	配置防护等级
步骤7	action (permit | deny)	配置动作
步骤8	end	返回特权模式

35.2.4 修改威胁情报防护等级

配置步骤

步骤1	configure terminal	进入配置模式
步骤2	threat-intelligence protect-level low <0-100> middle <0-100> high <0-100>	配置防护等级的威胁阈值
步骤3	end	返回特权模式

注意

威胁情报的防护等级设置必须保证低等级的威胁阈值最高，高等级的威胁阈值最低。

35.2.5 修改云端查询配置

配置步骤

步骤1	configure terminal	进入配置模式
步骤2	threat-intelligence cloud-check (enable|disable)	开启/关闭云端查询
步骤3	threat-intelligence cloud-server http://www.test.com	配置指定云端查询服务器
步骤3	end	返回特权模式

35.2.6 修改情报库在线升级配置

配置步骤

步骤1	configure terminal	进入配置模式
步骤2	threat-intelligence auto-update (enable|disable)	开启/关闭情报库自动在线升级

步骤3	threat-intelligence auto-update-time hour <0-23> minute <0-59>	配置情报库每天自动在线升级的时间点
步骤4	end	返回特权模式

35.2.7 查询威胁情报的配置

配置步骤

步骤1	show threat-intelligence	显示所有威胁情报策略配置

36 配置防 DOS 攻击

36.1 防DOS攻击概述

作为一款防火墙产品，需要同时具备防止攻击和保证正常数据通过的功能。当设备遇到大量攻击时，如果所有的连接资源都被攻击所占用，则正常数据就无法通过设备。

防 DOS(Denial of Service)攻击设计的目标就是要使设备能够阻止外部的恶意攻击，同时还能使内网正常地与外界通信。不仅保护设备，更要保护内网。当遭受到攻击时，向用户进行报警提示。

常见的 DOS 攻击主要包括 ping-of-death、tear-drop、jolt2、syn-flag、land-base、winnuke、smurf 等。

36.2 配置防DOS攻击

36.2.1 缺省配置

内容	缺省设置	备注
防ping of death攻击	disable	可更改设置
防tear drop攻击	disable	可更改设置
防jolt2攻击	disable	可更改设置
防land-based攻击	disable	可更改设置
防winnuke攻击	disable	可更改设置
防syn flag攻击	disable	可更改设置
防smurf攻击	disable	可更改设置

36.2.2 配置防ping-of-death攻击功能

ping-of-death 攻击是通过向目的主机发送长度超过 65535 的 icmp 报文，使目的主机发生处理异常而崩溃。

配置了防 ping-of-death 攻击功能后，设备可以检测出 ping-of-death 攻击，丢弃攻击报文并输出告警日志信息。

配置步骤

步骤1	`configure terminal`	进入配置模式
步骤2	`ip defend attack ping-of-death`	打开防ping-of-death攻击

使用 no 命令可以关闭该功能。

36.2.3 配置防tear-drop攻击功能

tear-drop 攻击通过向目的主机发送报文偏移重叠的分片报文，使目的主机发生处理异常而崩溃。

配置了防 tear-drop 攻击功能后，设备可以检测出 tear-drop 攻击，并输出告警日志信息。因为正常报文传送也有可能出现报文重叠，因此设备不会丢弃该报文，而是采取裁减、重新组装报文的方式，发送出正常的报文。

配置步骤

步骤1	configure terminal	进入配置模式
步骤2	ip defend attack tear-drop	打开防tear-drop攻击

使用 no ip defend attack tear-drop 命令可以关闭该功能。

36.2.4 配置防jolt2攻击功能

jolt2 攻击通过向目的主机发送报文偏移加上报文长度超过 65535 的报文，使目的主机处理异常而崩溃。

配置了防 jolt2 攻击功能后，设备可以检测出 jolt2 攻击，丢弃攻击报文并输出告警日志信息。

配置步骤

步骤1	configure terminal	进入配置模式
步骤2	ip defend attack jolt2	打开防jolt2攻击

使用 no ip defend attack jolt2 命令可以关闭该功能。

36.2.5 配置防land-base攻击功能

land-base 攻击通过向目的主机发送目的地址和源地址相同的报文，使目的主机消耗大量的系统资源，从而造成系统崩溃或死机。

配置了防 land-base 攻击功能后，设备可以检测出 land-base 攻击，丢弃攻击报文并输出告警日志信息。

配置步骤

步骤1	configure terminal	进入配置模式
步骤2	ip defend attack land-base	打开防land-base攻击

使用 no ip defend land-base 命令可以关闭该功能。

36.2.6 配置防winnuke攻击功能

winnuke 攻击通过向目的主机的 139、138、137、113、53 端口发送 TCP 紧急标识位 urg 为 1 的带外数据报文，使系统处理异常而崩溃。

配置了防 winnuke 攻击功能后，设备可以检测出 winnuke 攻击报文，将报文中

的 TCP 紧急标志位为 0 后转发报文，并可以输出告警日志信息。

配置步骤

步骤1	configure terminal	进入配置模式
步骤2	ip defend attack winnuke	打开防winnuke攻击

使用 no ip defend attack winnuke 命令可以关闭该功能。

36.2.7 配置防syn-flag攻击功能

syn-flag 攻击通过向目的主机发送错误的 tcp 标识组合报文，浪费目的主机资源。

配置了防 syn-flag 攻击功能后，设备可以检测出 syn-flag 攻击，丢弃攻击报文并输出告警日志信息。

配置步骤

步骤1	configure terminal	进入配置模式
步骤2	ip defend attack syn-flag	打开防syn-flag攻击

使用 no 命令可以关闭该功能。

36.2.8 配置防smurf攻击

Smurf 攻击结合使用了 IP 欺骗和 ICMP 回复方法使大量网络传输充斥目标系统，引起目标系统拒绝为正常系统进行服务。Smurf 攻击通过使用将回复地址设置成受害网络的广播地址的 ICMP 应答请求(ping)数据包，来淹没受害主机，最终导致该网络的所有主机都对此 ICMP 应答请求做出答复，导致网络阻塞。

防火墙设备的防 smurf 攻击可以检测出 smurf 攻击，可以有效地丢弃攻击报文并输出告警日志信息。

配置步骤

步骤1	configure terminal	进入配置模式
步骤2	ip defend attack smurf	打开防smurf攻击

使用 no ip defend smurf 命令可以关闭该功能。

36.3 配置案例

36.3.1 案例1：配置防DOS攻击

案例描述：

当网络上出现大量的攻击报文时，可通过抓包或查看流信息判断是否受到攻击。攻击报文将会占用大量的资源，影响我们所保护主机的性能，也影响设备的性能。

这时要通过抓包或查看流信息来查看受到了何种攻击，并启用对应的防攻击，从而保护内网和设备。若设备收到目的地址和源地址相同的报文，则触发设备的 Land-Base 攻击防护功能，设备将攻击报文丢弃，并发出告警信息。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	ip defend attack land-base	打开防land-base攻击

36.4 防DOS攻击的监控与维护

36.4.1 查看配置信息

步骤1	Show ip defend attack
	host# show ip defend attack ip defend attack informations: ip defend attack ping-of-death:disable ip defend attack tear-drop:disable ip defend attack jolt2:disable ip defend attack land-base:disable ip defend attack winnuke:disable ip defend attack syn-flag:disable ip defend attack smurf:enble

36.4.2 查看防DOS攻击的debug信息

步骤1	debug ip defend attack
	host#debug ip defend attack 打开该命令时，系统会向控制台打印检测到的攻击信息。

36.5 常见故障分析

36.5.1 防Dos攻击防御失效

现象	防Dos的攻击防御失效。
分析	SYN Flood攻击防御失效的原因可能有以下几个：防Dos攻击的服务没有启动或者防Dos攻击有很多种类型，可能选择防Dos攻击类型错误。
解决	防Dos攻击服务是否启动，可以用show ip defend attack命令查看。如果未启动，启动防Dos攻击服务。

37 配置防 ARP 攻击

37.1 ARP攻击防御概述

在局域网中，通信前必须通过 ARP 协议将 IP 地址转换为 MAC 地址。ARP 协议对网络安全具有重要的意义，但是当初 ARP 方式的设计没有考虑到过多的安全问题，留下很多隐患，使得 ARP 攻击成为当前网络环境中遇到的一个非常典型的安全威胁。

通过伪造 IP 地址和 MAC 地址实现 ARP 欺骗，能够在网络中产生大量的 ARP 通信量使网络阻塞，攻击者只要持续不断的发出伪造的 ARP 响应包就能更改目标主机 ARP 缓存，造成网络中断或中间人攻击。

受到 ARP 攻击后会出现无法正常上网、ARP 包爆增、不正常或错误的 MAC 地址、一个 MAC 地址对应多个 IP、IP 冲突等情况。

ARP 攻击因为技术门槛低，易于实现，在现今的网络中频频出现，有效防范 ARP 攻击已成为确保网络畅通的必要条件。

防 ARP 攻击功能能有效识别 ARP 欺骗攻击和 ARP flood 攻击，对疑似攻击的行为告警，并配合 IP-MAC 绑定、主动保护发包及关闭 ARP 学习等功能有效防范 ARP 攻击造成的损害。

37.2 配置ARP攻击防御

37.2.1 缺省配置信息

ARP 攻击防御功能默认不启用。缺省设置信息如下表所示：

表37-1 ARP 攻击防御功能缺省配置信息

内容	缺省设置	备注
使能/禁止状态ARP欺骗攻击防御	不启用	可更改设置
使能/禁止主动保护发包	不启用	可更改设置
主动发包保护时间间隔	1秒	可更改设置
主动发包保护	空	可添加列表
使能/禁止ARP学习	不启用	可更改设置

37.2.2 配置启用ARP攻击防御功能

启用 ARP 攻击防御功能，启用后对检测到的 ARP 攻击告警

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	anti-arp spoof service	启用ARP攻击防御
步骤3	exit	回到enable模式

使用 no anti-arp spoof service 命令，可以关闭 ARP 攻击防御

37.2.3 配置启用主动保护发包

启用主动保护发包功能，每隔规定的时间间隔就对主动保护列表上的端口和 IP 发免费 ARP 报文。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	anti-arp broadcast service	启用ARP主动保护发包
步骤3	anti-arp broadcast interface INTERFACE_NAME list A.B.C.D HH-HH-HH-HH-HH-HH	配置添加保护列表，使得设备在端口INTERFACE_NAME 发送 IP 为A.B.C.D ，MAC 为HH-HH-HH-HH-HH-HH的免费ARP报文
步骤4	anti-arp broadcast interface INTERFACE_NAME	配置添加保护接口，使得设备在端口INTERFACE_NAME发送其配置的所有IP
步骤5	anti-arp broadcast interval <1-10>	配置ARP主动保护发包间隔时间
步骤6	exit	回到enable模式

使用 no anti-arp broadcast service 可以关闭 ARP 主动保护发包

使用 no anti-arp broadcast interface INTERFACE_NAME list A.B.C.D HH-HH-HH-HH-HH-HH 可以删除主动保护列表的已配置项

使用 clear anti-arp broadcast interface INTERFACE_NAME list 可以清除接口 INTERFACE_NAME 上已配置的所有列表项

使用 no anti-arp broadcast interface INTERFACE_NAME 可以关闭删除已配置的保护接口

参数说明：

参数	说明	缺省配置
INTERFACE_NAME	设备当前可用接口名	空
A.B.C.D	IP地址	空
HH-HH-HH-HH-HH-HH	MAC地址	空
<1-10>	时间间隔	空

注意

启用主动保护发包一定要在开启了 ARP 攻击防御功能以后才有作用。


提示

配置完成后，可以在 ENABLE 节点下使用命令：

show anti-arp broadcast interface 查看设备当前有哪些接口已配置了接口保护

show anti-arp broadcast interface list 查看当前配置的保护列表

37.2.4 配置关闭ARP学习

关闭 ARP 学习功能后，IP-MAC 对应关系不在 IP-MAC 绑定表内的报文将不能通过设备

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	anti-arp study-arp	关闭ARP学习功能
步骤3	exit	回到enable模式

使用 no anti-arp study-arp 可以重新开启 ARP 学习功能。


注意

关闭 ARP 学习一定要在开启了 ARP 攻击防御功能以后才有作用。

此功能可能影响网络使用，请慎重使用。

强烈建议在使用前绑定所用可能使用的 IP-MAC

37.2.5 配置防ARP flood攻击

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	anti-arp flood service	开启防ARP flood攻击功能
步骤3	anti-arp flood block-time <10-65535>	设置ARP flood攻击主机阻断时间
步骤4	anti-arp flood threshold <1-10000>	设置ARP flood攻击门限值
步骤5	exit	回到enable模式

使用 no anti-arp flood service 可以关闭防 ARP flood 攻击功能。

参数说明：

参数	说明	缺省配置
<10-65535>	阻断时间	空
<1-10000>	ARP flood攻击门限值	空

37.3 监控与维护

37.3.1 查看ARP 攻击抑制主机列表

查看 ARP 攻击抑制主机列表：

步骤	配置
	host# show anti-arp flood list anti-arp flood block-list: IP: MAC: TIME 172.16.10.254 78-E3-B5-A9-E2-F3 23 172.16.10.254 78-E3-B5-A9-E2-F4 23 172.16.10.254 78-E3-B5-A9-E2-F7 0 172.16.10.254 78-E3-B5-A9-E2-F3 23表明IP地址为172.16.10.254，MAC地址为78-E3-B5-A9-E2-F3的报文为ARP Flood 攻击报文，该主机被设备阻断时长还有23秒。 Time为0时，对应的主机不被阻断。

37.3.2 查看DEBUG信息

步骤	配置
	host# debug anti-arp

使用 no debug anti-arp命令关闭debug信息

37.4 配置案例

37.4.1 配置案例：配置防ARP欺骗

案例描述：

配置防 ARP 欺骗和防 ARP Flood，检测网络中是否有 ARP 攻击

配置步骤：

步骤	配置
	host# configure terminal
	host(config)# anti-arp spoof service
	host(config)# anti-arp broadcast service
	host(config)# anti-arp broadcast interval 10
	host(config)# anti-arp broadcast interface vlan1000
	host(config)# anti-arp broadcast interface vlan1000 list 172.16.10.254 78-e3-b5-a9-e2-f7
	host(config)# anti-arp flood service
	host(config)# anti-arp flood block-time 30
	host(config)# anti-arp flood threshold 100

配置结果：

show show anti-arp 信息

anti-arp spoof service

anti-arp broadcast service

anti-arp broadcast interval 10

anti-arp flood service

anti-arp flood block-time 30

anti-arp flood threshold 100

anti-arp broadcast interface vlan1000

anti-arp broadcast interface vlan1000 list 172.16.10.254 78-E3-B5-A9-E2-F7

打开 ARP 攻击防护 debug 信息，当有 ARP 攻击时会有日志产生

host# debug anti-arp

host# terminal monitor

ARP 欺骗日志

host# [Core 1][5417358498] SrcIP=172.16.10.254 SrcPort=vlan1000 SMAC=78:E3:B5:A9:E2:F3 Content="Packet in conflict with MAC 78:E3:B5:A9:E2:F7 in ARP table"

ARP Flood 日志

[Core 1][5417358682] arp flood: SrcIP(172.16.10.254) SrcMAC(78:e3:b5:a9:e2:f4) attacking DstIP(172.16.10.1) DstMAC(00:00:00:00:00:00)

37.5 常见故障分析

37.5.1 故障现象：PC无法上网

现象	配置反ARP欺骗后无法上网
分析	配置关闭了ARP学习，又没有在IP-MAC绑定表中加入PC
解决	在绑定表中加入PC

38 配置 IP-MAC 绑定

38.1 IP-MAC绑定概述

Address Resolution Protocol (ARP)是寻找 IP 地址所对应的 MAC 地址的一种协议。

为什么需要寻找 IP 地址对应的 MAC 地址呢？我们知道，在以太网中，对于处于同一子网的两个通信实体来说，他们的一次 IP 通信过程大致如下：

当源端发送一个 IP 包之前，它必须知道目的端的以太网地址才可以完成封装，可是此时源端只能知道目的端的 IP 地址（通过用户的事先配置或者查路由表），这样就必须依靠 ARP 协议来完成目的端以太网地址的解析。因此源端发送一个包含目的 IP 地址的 ARP 请求，目的端收到后向源端返回 ARP 应答，通告自己的 MAC 地址，源端获得目的端 MAC 地址后才可以将 IP 包封装在以太网头中发送出去。

由于网络中可能存在一些攻击软件仿冒某台主机上网，逃过跟踪。为了避免这种情况，本设备实现了 IP-MAC 绑定功能，把用户的 MAC 和 IP 绑定起来。配置了 IP-MAC 绑定后，通过设备的报文的 MAC 和 IP 必须严格一致，否则报文将被丢弃。

38.2 配置IP-MAC绑定

38.2.1 配置IP-MAC绑定

添加一项 IP-MAC 绑定，需要输入绑定名称、IP 地址、MAC 地址、是否进行唯一性检查(unique-ip 或 multi-ip)

步骤	执行命令	说明
1	configure terminal	进入全局配置模式
2	ipmac NAME A.B.C.D HH-HH-HH-HH-HH-HH (unique-ip|multi-ip)	配置一条IP-MAC绑定，唯一性检查选择unique-ip，非唯一性检查选择multi-ip

使用 **no ipmac NAME** 清除一条绑定项。

38.2.2 查看ARP列表

步骤	执行命令	说明
1	show arp	显示当前ARP列表

38.2.3 清除ARP列表

步骤	执行命令	说明
1	clear arp	清除ARP列表

38.3 配置案例

案例描述

把张三的主机 192.168.31.118 和 00-16-41-59-3E-AF 绑定起来，并且是唯一性的。

配置步骤

步骤1	添加IP-MAC绑定
	configure terminal ipmac zhangsan 192.168.31.118 00-16-41-59-3E-AF unique-ip 通过添加名称为 zhangsan 的 IP-MAC 绑定项，使得 zhangsan 的主机 IP 与 MAC 唯一绑定，其他的 IP 地址与 MAC 地址没有按照该绑定项对应的报文不能通过。

38.4 常见故障分析

网关无法上网

现象	对网关进行了IP-MAC绑定后，无法上网。
分析	对网关进行IP-MAC绑定，选择了唯一性检查(unique-ip)，导致了网络只能和网关相通，其他主机则不通。
解决	将网关IP-MAC绑定设置为非唯一性检查(multi-ip)。

39 配置 IP 黑名单

39.1 IP黑名单概述

用户发现有可疑流量时，可在防火墙中配置 IP 黑名单进行防护。流经防火墙的流量命中 IP 黑名单配置的过滤条件时，在设定时间内可以精确阻断该流量。

IP 黑名单支持 IPv4、IPv6、用户区域及 ISP 四种类型，创建时需要配置阻断方向、加入分组、阻断的类型及地址和设定超时时间，其中用户区域及 ISP 类型超时时间设置为永久。按照阻断方向匹配 IP 黑名单地址的报文在生效时间段内不再进行投递，直接做丢弃处理。

所有 IP 黑名单均被进行分组管理，可通过 IP 黑名单组对其下黑名单进行整组启停和设定超时时间。系统内置名为 default、non_manually_addition_block、abnormal_assets_block 三个默认组，用于分组管理手动添加、非手动阻断生成及资产黑名单。

39.2 配置IP黑名单组

39.2.1 配置IP黑名单组

可以根据需要，配置 IP 黑名单组，设置是否启用以及设定时间

黑名单组无时间设定配置步骤：

步骤1	config terminal	进入配置模式
步骤2	blacklist-group NAME (enable|disable)	配置黑名单组，无时间配置，enable:组启用 disable:组停止启用
步骤3	end	返回特权模式
步骤4	show running-config blacklist-group	显示IP黑名单组配置

黑名单组有效时间配置步骤：

步骤1	config terminal	进入配置模式
步骤2	blacklist-group NAME (enable|disable) valid_time_type (min|day|month) timeout <0-9999> configtime YY-MM-DD HH:NN:SS	配置黑名单组，有效时间配置
步骤3	end	返回特权模式
步骤4	show running-config blacklist-group	显示IP黑名单组配置

参数说明：

参数	说明	缺省配置
(enable|disable)	enable:组启用 disable:组停止启用	
(min|day|month)	生效时间单位可设置为分钟 <0-9999> 、 天 <0-9999> 或 月 <0-600>	默认5分钟
YY-MM-DD HH:NN:SS	黑名单组有效时间设置的配置时间，格式为年月日 时分秒	

黑名单组绝对时间配置步骤：

步骤1	config terminal	进入配置模式
步骤2	blacklist-group NAME (enable|disable) starttime YY-MM-DD HH:NN:SS endtime YY-MM-DD HH:NN:SS	配置黑名单组，绝对时间配置，enable:组启用 disable:组不启用
步骤3	end	返回特权模式
步骤4	show running-config blacklist-group	显示IP黑名单组配置

参数说明：

参数	说明	缺省配置
(enable|disable)	enable:组启用 disable:组停止启用	
YY-MM-DD HH:NN:SS	黑名单组绝对时间设置的开始时间，格式为年-月-日 时:分:秒	
YY-MM-DD HH:NN:SS	黑名单组绝对时间设置的结束时间，格式为年-月-日 时:分:秒	

使用 no blacklist-group NAME 删除黑名单组及组下全部黑名单成员。

39.2.2 修改IP黑名单组启停状态

可以根据需要，启用或关闭 IP 黑名单组。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	blacklist-group NAME state (enable|disable)	修改黑名单组的启停状态，enable:组启用 disable:组不启用
步骤3	end	返回特权模式
步骤4	show running-config blacklist-group	显示IP黑名单组配置

39.2.3 修改IP黑名单组名称

可以根据需要，修改 IP 黑名单组名称

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	blacklist-group NAME blacklist-group-new NAME	修改IP黑名单组名称
步骤3	end	返回特权模式
步骤4	show running-config blacklist-group	显示IP黑名单组配置

39.2.4 查看IP黑名单组配置

配置步骤：

步骤1	show blacklist-group all	显示所有IP黑名单组配置

39.2.5 查看IP黑名单组数量

配置步骤：

步骤1	show blacklist-group count	显示IP黑名单组的数量

39.3 配置IP黑名单

39.3.1 配置IP黑名单阻断方向

可以根据需要，配置 IP 黑名单的阻断方向进行防护。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	blacklist match type (sip|sip-or-dip)	配置IP黑名单阻断方向， sip:源IP阻断 sip-or-dip:源或目的IP阻断
步骤3	end	返回特权模式
步骤3	show running-config blacklist	显示IP黑名单配置

39.3.2 配置ipv4类型IP黑名单

可以根据实际网络情况，配置 ipv4 类型 IP 黑名单进行防护。

IP 黑名单有效时间配置步骤：

步骤1	config terminal	进入配置模式

步骤2	blacklist-ip (A.B.C.D|A.B.C.D/M|A.B.C.D-A.B.C.H) valid_time_type (min|day|month) timeout <0-9999> blacklist-group NAME	配置ipv4类型有效时间IP黑名单
步骤3	end	返回特权模式
步骤3	show running-config blacklist	显示IP黑名单配置

参数说明：

参数	说明	缺省配置
(A.B.C.D|A.B.C.D/M|A.B.C.D-A.B.C.H)	ipv4类型源地址，掩码M可为(1-32)	
(min|day|month|forever)	生效时间单位可设置为分钟<0-9999>、天<0-9999>或月<0-600>，forever为永久时间设定	默认5分钟
NAME	黑名单所属组名称	

IP 黑名单绝对时间配置步骤：

步骤1	config terminal	进入配置模式
步骤2	blacklist-ip (A.B.C.D|A.B.C.D/M|A.B.C.D-A.B.C.H) starttime YY-MM-DD HH:NN:SS endtime YY-MM-DD HH:NN:SS blacklist-group NAME	配置ipv4类型绝对时间IP黑名单
步骤3	end	返回特权模式
步骤3	show running-config blacklist	显示IP黑名单配置

参数说明：

参数	说明	缺省配置
(A.B.C.D|A.B.C.D/M|A.B.C.D-A.B.C.H)	ipv4类型源地址，掩码M可为(1-32)	
YY-MM-DD HH:NN:SS	黑名单绝对时间设置的开始时间，格式为年-月-日 时:分:秒	
YY-MM-DD HH:NN:SS	黑名单绝对时间设置的结束时间，格式为年-月-日 时:分:秒	
NAME	黑名单所属组名称	

使用 no blacklist-ip (A.B.C.D|A.B.C.D/M|A.B.C.D-A.B.C.H) blacklist-group NAME 可以删除所在组下对应地址的 IP 黑名单配置。

使用 blacklist-del-all 可以删除全部 IP 黑名单配置。

39.3.3 配置ipv6类型IP黑名单

可以根据实际网络情况，配置 ipv6 类型 IP 黑名单进行防护。

IPv6 黑名单有效时间配置步骤：

步骤1	config terminal	进入配置模式
步骤2	blacklist-ipv6 (X:X::X:X|X:X::X:X/M|X:X::X:X-X:X::X:X) valid_time_type (min|day|month) timeout <0-9999> blacklist-group NAME	配置ipv6类型有效时间IP黑名单
步骤3	end	返回特权模式
步骤3	show running-config blacklist	显示IP黑名单配置

参数说明：

参数	说明	缺省配置
(X:X::X:X|X:X::X:X/M|X:X::X:X-X:X::X:X)	IPv6或IPv6/掩码类型地址，掩码可取(128|112|96|80|64)	
(min|day|month|forever)	生效时间单位可设置为分钟<0-9999>、天<0-9999>或月<0-600>，forever为永久时间设定	
NAME	黑名单所属组名称	

IPv6 黑名单绝对时间配置步骤：

步骤1	config terminal	进入配置模式
步骤2	blacklist-ipv6 (X:X::X:X|X:X::X:X/M|X:X::X:X-X:X::X:X) starttime YY-MM-DD HH:NN:SS endtime YY-MM-DD HH:NN:SS blacklist-group NAME	配置ipv6类型绝对时间IP黑名单
步骤3	end	返回特权模式
步骤3	show running-config blacklist	显示IP黑名单配置

参数说明：

参数	说明	缺省配置
(X:X::X:X|X:X::X:X/M|X:X::X:X-X:X::X:X)	IPv6或IPv6/掩码类型地址，掩码可取(128|112|96|80|64)	
YY-MM-DD HH:NN:SS	黑名单绝对时间设置的开始时间，格式为年-月-日 时:分:秒	
YY-MM-DD HH:NN:SS	黑名单绝对时间设置的结束时间，格式为年-月-日 时:分:秒	
NAME	黑名单所属组名称	

使用 no blacklist-ipv6 (X:X::X:X|X:X::X:X/M|X:X::X:X-X:X::X:X) blacklist-group NAME 删除所在组下对应地址的 IP 黑名单配置。

使用 blacklist-del-all 可以删除全部 IP 黑名单配置。

39.3.4 配置用户区域类型IP黑名单

可以根据实际网络情况，配置用户区域类型 IP 黑名单进行防护。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	blacklist-region province NAME valid_time_type (forever) blacklist-group NAME	配置用户区域类型IP黑名单
步骤3	end	返回特权模式
步骤3	show running-config blacklist	显示IP黑名单配置

参数说明：

参数	说明	缺省配置
< NAME >	34个区域名称之一，命令行需支持中文编码格式	
(forever)	生效时间，用户区域类型为永久时间设定	

使用 no blacklist-region province NAME blacklist-group NAME 可以删除所在组下对应用户区域名称的 IP 黑名单配置。

使用 blacklist-del-all 可以删除全部 IP 黑名单配置。

39.3.5 配置ISP类型IP黑名单

可以根据实际网络情况，配置 ISP 类型 IP 黑名单进行防护。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	blacklist-isp NAME valid_time_type (forever) blacklist-group NAME	配置用户区域类型IP黑名单
步骤3	end	返回特权模式
步骤3	show running-config blacklist	显示IP黑名单配置

参数说明：

参数	说明	缺省配置
< NAME >	ISP地址库的名称	
(forever)	生效时间，ISP类型为永久时间设定	

使用 no blacklist-isp NAME blacklist-group NAME 可以删除所在组下对应 ISP 名称的 IP 黑名单配置。

使用 blacklist-del-all 可以删除全部 IP 黑名单配置。

39.3.6 配置IP黑名单全局开关

可以根据需要，配置开启或关闭 IP 黑名单阻断防护功能。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	blacklist (disable|enable)	IP黑名单全局开关，disable:关闭IP黑名单阻断防护功能 enable:开启IP黑名单阻断防护功能
步骤3	end	返回特权模式
步骤3	show running-config blacklist	显示IP黑名单配置

39.3.7 配置IP黑名单超时自动删除开关

可以根据需要，配置开启或关闭 IP 黑名单超时自动删除。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	blacklist (timeout-del-off|timeout-del-on)	IP黑名单超时自动删除开关， timeout-del-off:关闭超时自动删除 timeout-del-on:开启超时自动删除
步骤3	end	返回特权模式
步骤3	show running-config blacklist	显示IP黑名单配置

39.3.8 配置IP黑名单删除全部超时

可以根据需要，配置手动将超时 IP 黑名单条目删除。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	blacklist-del-all-timeout	手动将超时IP黑名单条目删除
步骤3	end	返回特权模式
步骤3	show running-config blacklist	显示IP黑名单配置

39.3.9 配置IP黑名单清除全部命中数

可以根据需要，配置清除全部 IP 黑名单的命中数。

配置步骤：

步骤1	config terminal	进入配置模式

步骤2	blacklist-clear-all-statistic	清除全部IP黑名单的命中数
步骤3	end	返回特权模式
步骤3	show running-config blacklist	显示IP黑名单配置

39.4 IP黑名单监控与维护

介绍常用的 show 命令的使用

39.4.1 查看IP黑名单阻断方向

配置步骤:

步骤1	enable	进入使能模式
步骤2	show blacklist match type	查看IP黑名单阻断方向

39.4.2 查看IP黑名单配置

配置步骤:

步骤1	enable	进入使能模式
步骤2	show blacklist table all [<1-1000>]	查看全部黑名单表，最多显示1000条
步骤2	show blacklist table ipv4 (IPADDRESS | any) [<1-1000>]	查看IPv4类型黑名单表，最多显示1000条
步骤2	show blacklist table ipv6 (IPADDRESS | any) [<1-1000>]	查看IPv6类型黑名单表，最多显示1000条
步骤2	show blacklist table region (REGIONNAME | any) [<1-1000>]	查看用户区域类型黑名单表，最多显示1000条
步骤2	show blacklist table isp (ISPNAME| any) [<1-1000>]	查看ISP类型黑名单表，最多显示1000条

39.4.3 查看IP黑名单规格

配置步骤:

步骤1	enable	进入使能模式
步骤2	show blacklist max-num	查看当前IP黑名单规格数

39.4.4 查看IP黑名单数量

配置步骤:

步骤1	enable	进入使能模式
步骤2	show blacklist count	查看当前IP黑名单统计总数和超时个数

39.4.5 查看IP黑名单全局开关状态

配置步骤:

步骤1	enable	进入使能模式
步骤2	show blacklist switch global-state	查看黑名单开关，全局启停状态

39.4.6 查看IP黑名单超时自动删除开关状态

配置步骤:

步骤1	enable	进入使能模式
步骤2	show blacklist switch timeout-del	查看黑名单开关，超时后删除状态

39.5 配置案例

39.5.1 配置IP黑名单

如果流信息中有大量非正常的同一源 ip 地址请求，可以认为受到了攻击，这时我们可以通过对 IP 黑名单进行配置以保护内网和设备，对可疑源 ip 地址的请求进行拦截阻断。

配置步骤：

步骤1	查看网络数据分析结果，确定是否受到同一源ip地址的攻击
步骤2	配置IP黑名单以及生效时间

```
host(config)# blacklist match type sip
host(config)#blacklist-ip 201.163.43.13 valid_time_type min timeout 0 blacklist-group default
host(config)# end
host #
```

配置结果：

host # show running-config blacklist

!!

blacklist enable

blacklist timeout-del-off

blacklist match type sip

blacklist-ip 201.163.43.13 valid_time_type min timeout 0 blacklist-group default configtime 22-11-01 19:10:15

!

39.6 常见故障分析

39.6.1 配置IP黑名单后没有拒包

现象	通过抓包或流收集后，确定确实有从已配置IP黑名单中的阻断ip地址发出的包经过设备，没有拒包。
分析	可能是以下情况导致： ● IP黑名单配置已超过了生效时间，不再生效。
解决	检查配置，可以根据实际需求修改，刷新IP黑名单的生效时间，或者将其直接配置成永久生效。

40 白名单防护

40.1 白名单概述

开启白名单功能后，流经防火墙的流量在匹配到白名单配置的过滤条件后，在设定时间内会将该流量绕过防火墙策略、IP 黑名单等安全策略检查，做放行处理。

白名单仅对 IP 地址进行匹配，匹配方向可为源 IP、源或目的 IP。白名单支持 IPv4、IPv6、用户区域及 ISP 类型的地址配置。在 web 页面中，支持对白名单进行手动添加、编辑添加等添加方式。导入和导出功能，方便对大量的白名单地址进行配置和备份操作。白名单首页根据未超时白名单的命中数从大到小进行 TOP100 展示。

40.2 配置白名单匹配方向

进入**策略>安全防护>白名单**，选择**匹配方向配置**，设置白名单的放行方向，如下图：

源 IP：选择流经报文的源 IP 进行白名单匹配命中。

源或目的 IP：对流经报文先进行源 IP 的白名单匹配，若未命中，再进行目的 IP 的白名单匹配。

40.3 配置白名单

40.3.1 配置白名单

进入**策略>安全防护>白名单**，选择**配置**，如下图：

地址：白名单所放行的 IP 地址或用户区域、ISP 名称所包含的 IP 地址。

配置添加时间 ：白名单配置创建时的系统时间。

生效时间：白名单生效的时间，单位为分钟。

剩余放行时长：白名单剩余的生效时间，单位为秒。

添加方式：白名单的添加方式。

命中：流经设备流量匹配到白名单地址的命中计数

配置步骤：

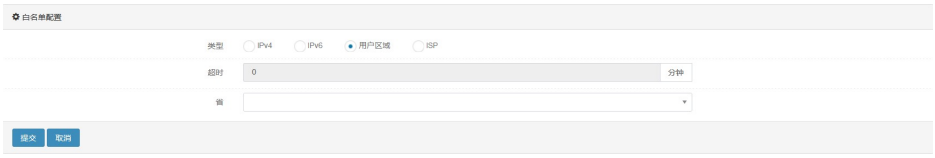
1. 点击**新建**按钮创建白名单，如下图：

参数说明：

类型：白名单有 IPv4、IPv6、用户区域和 ISP 四种类型，新建的时候任选其一。

源 IP：白名单所放行的 ipv4 或者 ipv6 地址。

超时：配置白名单超时时间，允许配置范围为 0-9999，单位为分钟。默认为 5 分钟，配置成‘0’表示永久生效。

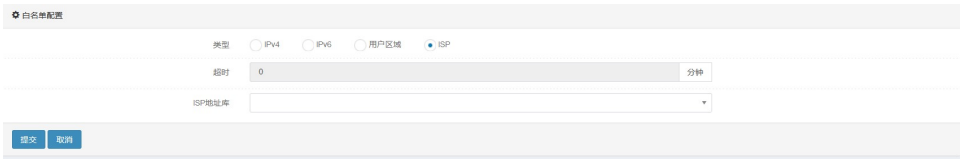


参数说明：

类型：用户区域类型。

超时：用户区域类型白名单超时时间设定为永久生效。

省：以 34 个中国省级行政区域名称区分不同的 IP 归属。



参数说明：

类型：ISP 类型。

超时：ISP 类型白名单超时时间设定为永久生效。

ISP 地址库：以 ISP 地址库名称区分不同的 IP 归属。

2. 配置完毕后，点击**提交**。

白名单规格为 10000 条。

配置白名单放行的 IP 时要与白名单的类型对应上。

白名单放行的 IP 地址不能配置成广播地址和全 0 地址。

白名单 Pv4 类型配置子网地址时支持掩码为 1~32，IPv6 类型仅支持 64、80、96、112、128 位掩码配置。

40.3.2 编辑创建白名单

配置步骤：

1. 进入**策略>安全防护>白名单**，点击**编辑**批量创建白名单，如下图：

参数说明：

编辑窗口：输入 IPv4 或 IPv4/掩码，支持批量粘贴操作。

重置：清空编辑窗口已有内容。

关闭 ：取消白名单编辑创建操作。

2. 编辑完毕后，点击**确定，**白名单创建并提示成功编辑添加的条数，如下图：

3. 点击**关闭，**完成白名单编辑创建。

提示

通过编辑创建的白名单生效时间均为永久。

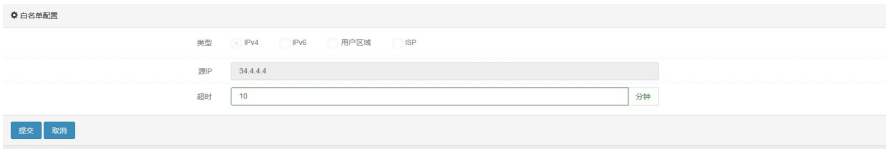
编辑窗口的白名单规格为 2048 条。

40.3.3 修改白名单

配置步骤：

1. 进入**策略>安全防护>白名单**，对于某条白名单，点击白名单前面的序号进入修改界面。

2. 可以对白名单表项内可修改时间进行修改，修改完毕后点击**提交**。



注意

编辑修改白名单时，类型和 IP 不能改变。

用户区域及 ISP 类型白名单无可修改内容。

40.3.4 删除白名单

配置步骤：

1. 进入**策略>安全防护>白名单**，选择**配置**，如下图：

2. 点击 删除某条白名单配置或者点击 删除全部白名单配置。

40.3.5 重置白名单命中数

配置步骤：

1. 进入**策略>安全防护>白名单**，选择**配置**，如下图：

2. 点击 重置某条白名单已有命中数。

注意

设备重启后白名单命中数均重置。

白名单超时后，已有命中数统计值保留。

40.3.6 全局开关白名单

配置步骤：

1. 进入**策略>安全防护>白名单**，选择**配置**，如下图：

2. 打开 白名单全局开关： 开 开关按钮，白名单模块对流经设备流量进行匹配放行处理。

注意

系统默认白名单全局开关状态为关闭。

40.3.7 查询白名单

配置步骤：

1. 进入**策略>安全防护>白名单**，选择**配置**，如下图：

2. 输入需要查找的白名单 IP 地址，点击 进行查找，如下图：

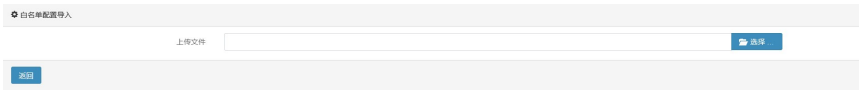
40.4 白名单配置导入导出

进入**策略>安全防护>白名单**，选择**配置**，如下图：

40.4.1 白名单导入

导入：可导入包含白名单配置的文本文件，系统会读取文件中的配置并执行下发。

点击选择，选择需要导入的白名单配置文件，如下图：



白名单导入配置须如下：

- **IPv4 类型**

whitelist-ip (x.x.x.x|x.x.x.x/x|x.x.x.0-x.x.x.255) timeout x configtime x-x-x x:x:x

x.x.x.x|x.x.x.x/x|x.x.x.0-x.x.x.255 ： IPv4 或 IPv4/掩码类型地址或 IP 范围，掩码可取(1~32)；

x：生效时间（分钟）；

x-x-x x:x:x ：配置起始的年-月-日 时：分：秒。

- **纯 IPv4**

x.x.x.x

x.x.x.x/x

纯 IPv4 或 IPv4/掩码类型地址，掩码可取值 1~32；

- **IPv6 类型**

whitelist-ipv6 (x:x::x:x|x:x::x:x/x) timeout x configtime x-x-x x:x:x

x:x::x:x|x:x::x:x/x ： IPv6 或 IPv6/掩码类型地址或 IP 范围，掩码可取(128|112|96|80|64)；

x ：生效时间（分钟）；

x-x-x x:x:x ：配置生效时的年-月-日 时：分：秒。

- **用户区域类型**

whitelist-region province NAME timeout 0 configtime x-x-x x:x:x

NAME：区域名称，34个区域名称之一；

x-x-x x:x:x ：配置生效时的年-月-日 时：分：秒。

- **ISP 类型**

whitelist-isp NAME timeout 0 configtime x-x-x x:x:x

NAME：ISP 地址库名称；

x-x-x x:x:x ：配置生效时的年-月-日 时：分：秒。

注意

导入文件如果有用户区域白名单类型，导入文档需使用 GB2312 编码。

40.4.2 白名单导出

导出：可将白名单的配置导出至一个文本文件中。

点击**导出**，如下图：

参数说明：

类型：支持两种白名单导出方式：导出全部白名单配置和只导出永久白名单配置。

选择类型点击**导出**按钮，设备根据导出类型及导出时间生成已命名的文档后，可操作页面弹窗保存至本地路径。

注意

导出文件如果有用户区域白名单类型，导出文档需用 GB2312 编码显示。

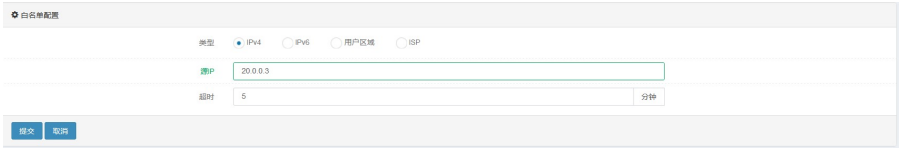
白名单导出前需先对当前配置进行保存。

40.5 配置案例

40.5.1 案例1：创建白名单

配置步骤：

1. 进入**策略>安全防护>白名单**，选择**配置**，点击**新建**按钮进入配置页面，配置源 IP 为 20.0.0.3 的白名单，如下图：



2. 点击**提交**，完成配置。

41 配置域名黑名单防护

41.1 域名黑名单概述

用户发现有对可疑站点的请求流量时，可在防火墙中配置域名黑名单来进行防护。流经防火墙的 DNS 请求报文命中域名黑名单配置的过滤条件时，在设定时间表内可以精确阻断该 DNS 请求。

域名黑名单支持两种类型的域名格式，一种是带点的域名格式（如：qq.com、www.baidu.com），另一种是不带点的格式（如：google、github），所配置的域名长度不应超过 255，且对大小写不敏感。

41.2 配置域名黑名单

41.2.1 配置域名黑名单

可以根据实际网络情况，配置域名黑名单进行防护。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	domain-blacklist table DOMAIN (TR|always)	配置域名黑名单
步骤3	end	返回特权模式
步骤3	show running-config domain-blacklist	显示域名黑名单配置

参数说明：

命令：domain-blacklist table DOMAIN (TR|always)

参数	说明	缺省配置
DOMAIN	域名地址	无
TR	时间对象	always

使用 no domain-blacklist table DOMAIN 可以删除域名地址是 DOMAIN 的黑名单配置。

使用 no domain-blacklist table 可以删除全部域名黑名单配置。

41.3 配置案例

41.3.1 案例1：禁止员工访问博彩站点

某博彩站点（www.lottery.com）可能会有挂马行为，为了公司内部网络安全，可以通过配置域名黑名单来阻断对该站点的访问。

配置步骤：

步骤1	开启域名黑名单功能
	host(config)# domain-blacklist enable
步骤2	配置域名黑名单
	host(config)# domain-blacklist table www.lottery.com always host(config)# end host #

配置结果：

!!

domain-blacklist enable

domain-blacklist table www.lottery.com always

!

41.3.2 案例2：禁止员工在上班期间访问游戏站点

公司上班时间为早九晚六，在这期间不希望员工访问 game.com 站点来玩游戏，可以通过配置域名黑名单来阻断对该站点的访问。

配置步骤：

步骤1	开启域名黑名单功能
	host(config)# domain-blacklist enable
步骤2	配置时间对象： 每周（星期一、星期二、星期三、星期四、星期五） 开始时间（09:00:00） 结束时间（18:00:00）
	host(config)# schedule recurring working host(config-schd)# periodic 09:00:00 18:00:00 monday tuesday wednesday thursday friday null null host(config-schd)# end host #
步骤3	配置域名黑名单
	host(config)# domain-blacklist table game.com working host(config)# end host #

配置结果：

!!

domain-blacklist enable

domain-blacklist table game.com working

!

41.4 域名黑名单监控与维护

介绍常用的 show 命令的使用以及其他内部命令

41.4.1 查看域名黑名单配置

查看单条域名黑名单：

步骤1	执行 host# show domain-blacklist table game.com
	domain-blacklist table game.com working 0 可以看到对应域名黑名单的详细信息；配置的阻断域名地址是game.com；引用的时间对象是working；命中数是0；在生效时间内，对[*.]game.com的DNS请求报文全部被阻断。

查看所有域名黑名单：

步骤1	执行 host# show domain-blacklist table
	domain-blacklist table www.lottery.com always 0 domain-blacklist table game.com working 0 可以看到所有域名黑名单的详细信息。

41.4.2 查看域名黑名单规格

查看域名黑名单当前规格数：

步骤1	执行host# show domain-blacklist max-num
	domain-blacklist max-num is 10000 可以看到当前域名黑名单规格数为1万条。

41.4.3 扩展域名黑名单规格

扩展域名黑名单规格数：

步骤1	执行host# domain-blacklist max-num <10000-100000>
	域名黑名单规格数初始为1万条，可通过该命令进行扩展，最多10万条；该功能只在vtysh命令行中支持，一般不建议在防火墙设备内存不足的情况下使用。

41.4.4 查看域名黑名单数量

查看域名黑名单统计总数：

步骤1	执行host# show domain-blacklist count
	domain-blacklist count is 5

可以看到当前黑名单总数为5。

41.4.5 查看域名黑名单后缀匹配开关

查看域名黑名单后缀匹配开关：

步骤1 执行host# show domain-blacklist suffix-match

domain-blacklist suffix-match is disable

可以看到域名黑名单后缀匹配功能默认是关闭状态。

41.4.6 开启域名黑名单后缀匹配功能

开启域名黑名单后缀匹配功能：

步骤1 执行host(config)# domain-blacklist suffix-match enable

开启域名黑名单后缀匹配功能后，将会对DNS请求报文中的域名的常见后缀也进行匹配。

41.4.7 关闭域名黑名单后缀匹配功能

关闭域名黑名单后缀匹配功能：

步骤1 执行host(config)# domain-blacklist suffix-match disable

关闭域名黑名单后缀匹配功能后，将不会对DNS请求报文中的域名的常见后缀进行匹配，默认是关闭状态。

41.5 常见故障分析

41.5.1 配置域名黑名单后没有阻断DNS请求报文

现象	通过抓包或流收集后，发现本该被域名黑名单模块阻断的DNS请求报文，却没有被阻断。
分析	可能是以下情况导致： ● DNS请求报文是否命中了白名单 ● 域名黑名单模块全局开关是否开启 ● 域名黑名单的时间表是否过了生效期
解决	● 删除对应的白名单条目 ● 开启域名黑名单全局开关 ● 修改域名黑名单时间表的生效期

42 配置口令防护

42.1 口令防护概述

口令防护分为两个模块：弱口令检查、防口令暴力破解。

弱口令(weak password) 没有严格和准确的定义，通常认为容易被别人猜测到或被破解工具破解的口令均为弱口令。弱口令指的是仅包含简单数字和字母的口令，例如“123”、“abc”等，因为这样的口令很容易被别人破解，从而使用户的互联网账号受到他人控制，因此不推荐用户使用。

弱口令检查通过审计报文中的用户名和密码以及登陆状态，利用规则匹配的方式对密码进行检查，将检测到的弱口令进行日志上报。

口令暴力破解的意思是利用所有可能的字符组密码，尝试破解登录口令。这是最原始，粗暴的破解方法，根据运算能力，如果能够承受的起时间成本的话，最终一定会爆破出密码。而防口令暴力破解就是对此种攻击方式进行预防。

防口令暴力破解通过统计登录失败次数，来判断某个 IP 是否进行了口令暴力破解。一旦某个 IP 被认为是进行了暴力破解，则可以针对这个 IP 进行告警、阻断、精准阻断。

口令防护功能目前支持的协议有 FTP，POP3，IMAP，SMTP，HTTP，TELNET。

42.2 配置口令防护模版

口令防护模版需要在防护策略中引用。

42.2.1 缺省配置信息

防火墙设备关于口令防护缺省设置信息如以下表格所示：

口令防护的缺省配置信息

内容	缺省设置	备注
弱口令检测	disable	可更改设置
检查等级	低	可更改设置
防口令暴力破解	disable	可更改设置
允许连续失败次数	3次/每分钟	可更改设置
动作	告警	可更改设置
阻断时间	1min	可更改设置

42.2.2 创建口令防护对象

步骤：

步骤1	configure terminal	进入配置模式

步骤2	password-check-profile NAME	配置一个口令防护模版，并进入口令防护配置节点

使用 no password-check-profile NAME 可以删除一个攻击防护。

42.2.3 配置弱口令检查

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	password-check-profile test	配置一个名为test的口令防护
步骤3	weak-password (enable|disable)	开启/关闭弱口令检查功能
步骤4	weak-password check-level (low|middle|high)	配置弱口令检查等级
步骤5	end	返回特权模式
步骤6	show running-config password-check-profile test	显示配置的口令防护对象信息

参数说明：

参数	说明	缺省配置
(enable|disable)	开启/关闭弱口令检查功能	关闭
(low|middle|high)	检查等级低/中/高	低

42.2.4 配置防口令暴力破解检查

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	password-check-profile test	配置一个名为test的口令防护
步骤3	brute-force-check (enable|disable)	开启/关闭防口令暴力破解功能
步骤4	brute-force-check retry (3-60) block-action (alarm|ct-drop|src-drop) [block-time (0-3600)]	配置防口令暴力破解的连续失败次数、动作、阻断时间
步骤5	end	返回特权模式
步骤6	show running-config password-check-profile test	显示配置的口令防护对象信息

参数说明：

参数	说明	缺省配置
(enable|disable)	开启/关闭防口令暴力破解功能	关闭
(alarm|ct-drop|src-drop)	动作为告警、精准阻断、阻断源ip	告警
block-time (0-3600)	当动作为精准阻断或者阻	无

断ip时，需要配置阻断时间

使用 clear brute-force-check-stat-list 命令清空统计链表上的所有信息。

使用 clear brute-force-check-block-list 命令清空精准阻断链表上的所有信息。

42.2.5 攻击防护策略引用口令防护

步骤：

步骤1	configure terminal	进入配置模式
步骤2	protect-policy id	进入指定id的防护策略配置节点
步骤3	password-check-profile NAME	防护策略引用攻击防护
步骤4	log check-password-profile	使能口令防护日志功能

使用 no password-check-profile NAME 命令删除该口令防护策略。

42.3 配置案例

42.3.1 攻击防护中配置口令防护

案例描述

配置一个名为 test1 的口令防护模版，开启弱口令检查，设置弱口令检查等级为高。开启防口令暴力破解，设置允许连续失败次数为每分钟 5 次，动作为精准阻断，阻断时间为 3 分钟。在攻击防护策略 5 中引用该口令防护并开启日志功能。

配置步骤：

步骤1	进入配置模式
	host# config terminal
步骤2	创建一个名字为test1的口令防护
	host(config)# password-check-profile test1
步骤3	弱口令检查功能使能
	host(config-password-check)# weak-password enable
步骤4	设置弱口令检查等级为高
	host(config-password-check)# weak-password check-level high
步骤5	防口令暴力破解功能使能
	brute-force-check enable
步骤6	设置允许连续失败次数为每分钟5次，动作为精准阻断，阻断时间为3分钟
	brute-force-check retry 5 block-action ct-drop block-time 3
步骤7	新建一个攻击防护策略test
步骤8	在攻击防护策略test中引用口令防护test1
	password-check-profile test1
步骤9	开启口令防护日志

log check-password-profile

配置结果：

host# show password-check-profile test1

password-check-profile test1

weak-password enable

weak-password check-level high

brute-force-check enable

brute-force-check retry 5 block-action ct-drop block-time 3

host# show protect-policy 5

protect-policy 5 any any any pop3 any always

match statistic: 0

password-check-profile test1

log check-password-profile

43 配置应用控制

43.1 应用控制概述

应用控制是对安全策略功能增强，不再局限于简单地匹配 IP、端口进行分析控制，而是进一步对报文的数据内容进行协议分析、特征识别，识别出流量所属的具体应用，进而完成对某些具体应用流量的过滤、审计等功能。

应用控制策略的配置，主要包括：

- 应用，用来审计的目标应用。详细参照“应用对象”一章，目前防火墙可以识别的应用有 1000 多种，覆盖了当前流行的绝大多数应用。
- 应用行为，应用所表现出来的动作，如登录、注销、下载文件等等。
- 应用行为参数，应用行为的具体内容。如登录的用户名，下载的文件名等等。

应用控制策略的匹配顺序遵循规则：

a) 同一个应用的不同策略，匹配顺序和页面排列顺序一致；页面支持调整策略顺序

b) 不同应用的不同策略没有顺序关系，流量先匹配应用；

c) 既有单个应用，又有应用组对象，应用组对象包含该应用，则按照页面顺序进行匹配。

应用控制策略支持放行、阻断两种处理动作，可以配置是否开启日志记录，。

43.2 配置应用控制

43.2.1 缺省配置信息

防火墙设备关于应用控制的缺省设置信息如以下表格所示：

表43-1 应用控制的缺省配置信息

内容	缺省设置	备注
启用	disable	可更改设置
地址对象	any	可更改设置
用户	Any	可更改设置
应用	any	可更改设置
应用行为	any	可更改设置
行为参数	any	可更改设置

关键字	any	可更改设置
匹配类型	include	可更改设置
时间表	always	可更改设置
处理动作	permit	可更改设置
日志	disable	可更改设置

43.2.2 新建应用控制策略

根据命令行提示创建应用控制策略。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	app-policy-profile <1-1000> (SIP|any) (USER|any) (APP|any) (ACTION|any) (permit|deny) (TR|always)	配置应用控制应用相关的过滤信息
步骤3	policy-match-content (CONTENT|any) (include|exclude) (KEYOWRD|any)	配置匹配应用内容的规则
步骤4	enable	启用策略
步骤5	End	返回特权模式
步骤6	show app-policy-profile	显示所有应用控制策略配置

<1-1000>：应用控制的策略 ID 范围。

(SIP|any)：源地址或默认的地址对象 any。

(USER|any)：用户、用户组或默认的 any。

(APP|any)：应用、应用组或应用大类的名字，any 代表所有应用

(ACTION|any)：应用所表现出来的动作，如登录、注销、下载文件等等，any 表示所有应用行为。

(permit|deny)：对符合匹配条件的数据流执行的动作，允许为允许，拒绝为拒绝。

(TR|always)：策略生效的时间，TR 代表已配置的时间对象，always 表示所有时间。

(CONTENT|any)：应用行为的具体内容。如登录的用户名，下载的文件名等等。any 表示应用行为的所有参数。

(include|exclude)：匹配类型分别包含和不包含两种。

(KEYOWRD|any)：根据所配置的行为参数获取到的内容进行匹配(大小写敏感)。any 代表匹配任何内容。

43.2.3 删除应用控制策略

根据策略 ID 删除指定的应用控制策略。

配置步骤：

步骤1	config terminal	进入配置模式

步骤2	no app-policy-profile <1-1000>	删除指定ID的应用控制策略
步骤3	end	返回特权模式
步骤4	show app-policy-profile	显示所有应用控制策略配置

43.2.4 修改某一策略的匹配信息

根据策略的 ID 号，进入到策略内部对匹配信息进行修改。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	app-policy-profile <1-1000>	根据策略ID，进入策略内
步骤3	policy-match-content (CONTENT|any) (include|exclude) (KEYOWRD|any)	配置匹配应用内容的规则，可以配置多条
步骤4	no policy-match-content (CONTENT|any) (include|exclude) (KEYOWRD|any)	可以将配置好的匹配信息删除
步骤5	log enable	启用日志
步骤6	no log enable	关闭日志
步骤7	enable	启用策略
步骤8	no enable	关闭策略

43.2.5 查询应用控制策略的配置

根据命令查看所有应用控制策略配置或指定策略 ID 的策略配置。

配置步骤：

步骤1	show app-policy-profile	显示所有应用控制策略配置
步骤2	show app-policy-profile <1-1000>	显示指定ID的策略配置

43.2.6 移动应用控制策略的匹配顺序

以某个应用控制策略为基准，可以配置将目标策略移动到基准策略之前或之后。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	app-policy-profile move <1-1000> before <1-1000>	将前者ID对应的策略移动到后者ID对应的策略之前
步骤3	app-policy-profile move <1-1000> after <1-1000>	将前者ID对应的策略移动到后者ID对应的策略之后
步骤4	end	返回特权模式

步骤5	show app-policy-profile	显示所有应用控制策略配置

43.3 配置案例

43.3.1 阻断QQ号中包含“12456”的用户登陆

PC 通过防火墙设备访问外网。配置应用控制规则阻断 QQ 号中包含“123456”的用户登陆。

1. 配置步骤：

步骤2	配置应用控制策略
	FW_A(config)# app-policy-profile 1 any any qq Login deny always
	FW_A(config)# policy-match-content audit_username include deny_123456
	FW_A(config)# enable
	FW_A(config)# end
	FW_A #

2. 配置结果：

```
!!
app-policy-profile 1 any any qq Login deny always
 enable
 no log enable
 policy-match-content audit_username include deny_123456
!
```

以上关键参数说明如下：

qq：应用名。（内置）

enable： 使能策略

Login：应用行为，登陆。（内置）

audit_username：行为参数，审计的行为参数为用户名。（内置）

deny_123456：在 web 页面配置的关键字对象，内容为“123456”。（关键字内容配置不支持命令行）

3. 配置验证：

登陆 QQ 号中含“123456”的用户登陆，如果登陆失败，则证明策略阻断成功。

43.3.2 拒绝接收所有电子邮件

PC 通过防火墙设备访问外网。配置应用控制规则拒绝接收所有电子邮件。

1. 配置步骤：

步骤2	配置应用控制策略
	FW_A(config)# app-policy-profile 1 any any email Email_receive deny always
	FW_A(config)# policy-match-content any include any
	FW_A(config)# enable
	FW_A(config)# end
	FW_A #

2. 配置结果：

!!

app-policy-profile 1 any any email Email_receive deny always

enable

no log enable

policy-match-content any include any

!

以上关键参数说明如下：

email ：应用名称：电子邮件。

Email_receive：邮件接收。

3. 配置验证：

通过查看 web 页面该策略是否被命中，或者确认用户能发送邮件但是不能接收到电子邮件。

44 配置 Web 控制

44.1 Web控制概述

Web 访问控制审计功能可以对用户在某网站发布信息或者发布含有特定关键字信息的行为进行控制，并能对发布行为进行日志记录。例如，阻止用户在社区论坛类网站发布含有关键字“暴力”的信息，并记录发布行为日志。网络管理员可以针对不同用户、不同时间、不同信息发布行为制定适合的 Web 外发信息规则，系统将会对与规则相匹配的网络流量根据配置进行处理。

44.2 配置Web控制

44.2.1 缺省配置信息

防火墙设备关于 Web 控制的缺省设置信息如以下表格所示：

表44-1 Web 控制的缺省配置信息

内容	缺省设置	备注
启用	disable	可更改设置
入接口	any	可更改设置
源地址	any	可更改设置
用户	any	可更改设置
URL分类	any	可更改设置
文件类型	any	可更改设置
时间表	always	可更改设置
网页关键字	any	可更改设置
匹配类型	include	可更改设置
处理动作	permit	可更改设置
日志	disable	可更改设置

44.2.2 新建Web控制策略

根据命令行提示创建 Web 控制策略。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	web-filter-policy <1-100> (SIP|any) (USER|any) (IF_IN|any)	配置Web控制相关的过滤信息
步骤3	filter-rule <1-20> (URL|any)	配置url过滤规则

	(TYPE|any) (enable|disable) (TR|always) (permit|deny) (log|no-log) (enable|disable)	
步骤4	filter-rule <1-20> keyword (KEYOWRD|any) (include|exclude)	添加网页关键字过滤规则
步骤5	enable	启用策略
步骤6	End	返回特权模式
步骤7	show web-filter-policy	显示所有Web控制策略配置

<1-100>：Web 控制的策略 ID 范围。

(SIP|any)：源地址或默认的地址对象 any。

(USER|any)：用户、用户组或默认的 any。

(IF_IN|any)：入接口、vlan、安全域或默认的 any。

<1-20>：Web 控制的策略里规则的 ID 范围。

(URL|any)：URL 分类，any 代表所有 url。

(TYPE|any)：文件类型引用的关键字，any 表示所有文件类型。

(enable|disable)：是否启用匹配列表。

(TR|always)：策略生效的时间，TR 代表已配置的时间对象，always 表示所有时间。

(permit|deny)：对符合匹配条件的数据流执行的动作，允许为允许，拒绝为拒绝。

(log|no-log) ：是否启用该条规则日志上报功能。

(enable|disable)：是否启用该条规则。

<1-20>：此 ID 为 web 控制策略规则里已创建的 ID。

(KEYOWRD|any)：网页引用的关键字，any 代表任意关键字。

(include|exclude)：包含或不包含的匹配类型。

44.2.3 删除Web控制策略

根据策略 ID 删除指定的 Web 控制策略。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	no web-filter-policy <1-100>	删除指定ID的Web控制策略
步骤3	end	返回特权模式
步骤4	show web-filter-policy	显示所有Web控制策略配置

44.2.4 修改某一策略的匹配信息

根据策略的 ID 号，进入到策略内部对匹配信息进行修改。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	web-filter-policy <1-100>	根据策略ID，进入策略内
步骤3	filter-rule <1-20> (URL|any) (TYPE|any) (enable|disable) (TR|always) (permit|deny) (log|no-log) (enable|disable)	配置匹配url分类内容的规则，可以配置多条
步骤4	no filter-rule <1-20>	可以将配置好的规则删除
步骤5	no filter-rule <1-20> keyword KEYWORD	可以将配置好的规则里网页关键字匹配删除
步骤6	enable	启用策略
步骤7	no enable	关闭策略

44.2.5 查询Web控制策略的配置

根据命令查看所有 Web 控制策略配置或指定策略 ID 的策略配置。

配置步骤：

步骤1	show web-filter-policy	显示所有Web控制策略配置
步骤2	show web-filter-policy <1-100>	显示指定ID的策略配置

44.2.6 移动Web控制策略的匹配顺序

以某个 Web 控制策略为基准，可以配置将目标策略移动到基准策略之前或之后。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	web-filter-policy move <1-100> before <1-100>	将前者ID对应的策略移动到后者ID对应的策略之前
步骤3	web-filter-policy move <1-100> after <1-100>	将前者ID对应的策略移动到后者ID对应的策略之后
步骤4	end	返回特权模式
步骤5	show web-filter-policy	显示所有Web控制策略配置

44.3 配置案例

44.3.1 拒绝所有游戏网页并提示该网络禁止访

PC 通过防火墙设备访问外网。配置阻断所有新闻网页并提示该网络禁止访问新闻。

配置步骤：

步骤2	配置Web控制策略
	FW_A(config)# web-filter-policy 3 any any any
	FW_A(config)# filter-rule 1 game any enable always permit no-log enable
	FW_A(config)# filter-rule 1 keyword any include
	FW_A(config)# enable
	FW_A(config)# end
	FW_A #

配置结果：

```
!!
web-filter-policy 3 any any any
 enable
 filter-rule 1 game any enable always permit no-log enable
 filter-rule 1 keyword any include
!
```

Game：URL 分类游戏类型。

配置验证：

通过查看 web 页面该策略被命中，访问游戏网页被拒绝。

45 配置 QoS 策略

45.1 QoS概述

QoS 为英文 Quality of Service 缩写，即服务质量。简单地说，QoS 能够对穿过设备的数据包进行合理的排队，对其中特定的数据包赋以较高的优先级，从而加速传输的过程，以实现实时交互。

由于每种应用系统对网络的要求有所不同，这使得带宽本身并不能解决网络拥塞的问题。QoS 所追求的传输质量在于：数据包不仅要到达其欲传输的目的地址，而且要保证数据包的顺序性、完整性和实时性。通过 QoS 网络可以按照业务的类型或级别加以区分，并能够依次对各级别进行处理。

防火墙设备可以对策略中指定的流进行服务质量保证。

45.2 QoS线路配置

45.2.1 创建线路策略

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	tc-policy line NAME	创建线路策略
步骤3	show tc-policy	查看策略的当前配置

使用 no tc-policy line NAME 命令可以删除指定线路策略。

注意

1、创建线路策略成功后，会默认生成一条“def_NAME”的流控策略；

2、会将线路策略最大带宽设置成默认值（1000000）；

3、默认控制 egress 方向；

45.2.2 启用线路策略

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	tc-policy line NAME	对于一条已经配置好的线路策略，可以用该命令进入策略模式
步骤3	enable	启用这条线路策略

使用 disable 命令可以禁用这条策略，默认启用。

45.2.3 绑定接口

用 match interface INTERFACE_NAME 命令可以为线路策略绑定一个接口，对从该接口进入或者发出的数据流进行相应的控制。

配置步骤：

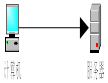
步骤1	configure terminal	进入配置模式
步骤2	tc-policy line NAME	对于一条已经配置好的线路策略，可以用该命令进入策略模式
步骤3	match interface INTERFACE_NAME	为策略绑定接口
步骤4	show tc-policy	查看策略的当前配置

参数说明：

match interface：

参数	说明	缺省配置
INTERFACE_NAME	绑定的接口，可以是物理口，也可以是vlan，trunk口。	无

使用 no match interface 命令可以取消线路策略绑定的接口。



1、一个接口只能被一条线路策略绑定；

2、要想修改线路绑定的接口，必须先解绑，然后再去绑定新的接口；

45.2.4 设置控制方向

用 limit (ingress|egress|both)命令可以设置控制方向。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	tc-policy line NAME	对于一条已经配置好的线路策略，可以用该命令进入策略模式
步骤3	limit (ingress|egress|both)	设置控制方向
步骤5	show tc-policy	查看策略的当前配置

参数说明：

limit：

参数	说明	缺省配置
(ingress|egress|both)	接口入方向|接口出方向|接口出入两个方向	接口出方向

45.2.5 配置最大带宽

用 maxbandwidth (ingress|egress) <8-100000000>命令可以配置出/入方向的最大带宽，对匹配该策略的流量按方向限速。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	tc-policy line NAME	对于一条已经配置好的线路策略，可以用该命令进入策略模式
步骤3	maxbandwidth (ingress|egress) <8-100000000>	配置出/入方向的最大带宽
步骤4	show tc-policy	查看策略的当前配置

参数说明：

maxbandwidth：

参数	说明	缺省配置
(ingress|egress)	接口的入/出方向	
<8-100000000>	最大带宽取值范围 8-100000000，单位kbps	

45.3 QoS流控策略

45.3.1 创建流控策略

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	tc-policy channel NAME parent NAME	创建流控策略
步骤3	show tc-policy	查看策略的当前配置

使用 no tc-policy channel NAME 命令可以删除指定流控策略。

参数说明：

tc-policy channel：

参数	说明	缺省配置
NAME（1）	流控策略的名称	无
NAME（2）	流控策略的父策略（上一级策略）	无

注意

1、创建一条流控策略成功后，会生成默认的最大带宽，保证带宽和生效的保证带宽。

2、删除一条流控策略，它及其下面的流控策略都会被删除。

45.3.2 启用流控策略

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	tc-policy channel NAME	进入流控策略
步骤3	enable	启用这条线路策略

使用 disable 命令可以禁用这条策略，默认启用。

45.3.3 设置流控策略优先级

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	tc-policy channel NAME	进入流控策略
步骤2	priority (high|medium|low)	设定策略优先级
步骤3	show tc-policy	查看策略当前配置

优先级默认为低。

45.3.4 配置匹配条件

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	tc-policy channel NAME	进入流控策略
步骤3	match (SIP|any) (DIP|any) ("CMD_GROUP_SERVICE") (USER|any) (APP|any) (TR|always)	设定策略匹配条件
步骤4	show running-config tc-policy	查看策略当前配置

参数说明：

参数	说明	缺省配置
(SIP|any)	数据流的源地址，可以引用已定义的某个地址对象或地址对象组，any表示源地址为任意。	无
(DIP|any)	数据流的目的地址，可以引用已定义的某个地址对象或地址对象组，any表示目的地址为任意。	无
(ah|aol|bgp|bootpc|bootps|daytime|dhcp|dns|discard|esp||finger|ftp|gopher|	数据流的服务属性，包括协议、源端口和目的端口，可以引用系统预定义服务、自	无

gre|h323|hostname|http|https|icmp|igmp|ike|imap|info_adress|info_request|irc|internet-locator-service|l2tp|ldap|mysql|netmeeting|netbios-ns|netbios-dgm|netbios-ssn|nfs|nicname|nntp|ntp|onc-rpc|osp f|pc-anywhere|pim|ping|ping6|pop2|pop3|pptp|printer|quake|radius|radius acct|raudio||rexec|rip|rlogin|rsh|samba|sccp|sip|sipmanmessenger|shell|smtp|smux|snmp|socks|aquid|ssh|syslog|talk|tcp|telnet|tftp|time|timestamp|tproxy|udp|uucp|vdolive|wais|webcache|winframe|who|x-windows|SRV_OBJ|any)	定义的服务对象或服务对象组，any表示服务为任意。	
(USER|any)	数据流的用户属性，可以引用已定义的某个用户对象或用户对象组，any表示用户为任意。	无
(APP|any)	数据流的应用属性，可以引用已定义的某个应用对象或应用对象组，any表示应用为任意。	
(TR|always)	策略生效的时间，可以引用已配置的时间对象TR，always表示所有时间。	无

45.3.5 配置最大带宽

用 maxbandwidth (ingress|egress)命令可以配置出/入方向的最大带宽，对匹配该策略的流量按方向限速。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	tc-policy channel NAME	对于一条已经配置好的流控策略，可以用该命令进入策略模式

步骤3	maxbandwidth <8-100000000>	(ingress|egress)	配置出/入方向的最大带宽
步骤4	show tc-policy		查看策略的当前配置

参数说明：

maxbandwidth：

参数	说明	缺省配置
(ingress|egress)	接口的入/出方向	
<8-100000000>	最大带宽取值范围 8-100000000，单位kbps	

注意

1、最大带宽不能大于上一级的最大带宽，不能小于下一级的最大带宽

45.3.6 配置保证带宽

用 bandwidth (ingress|egress)命令可以配置出/入方向的保证带宽，对匹配该策略的流量按方向进行保证。

配置步骤：

步骤1	configure terminal		进入配置模式
步骤2	tc-policy channel NAME		对于一条已经配置好的流控策略，可以用该命令进入策略模式
步骤3	bandwidth <8-100000000>	(ingress|egress)	配置出/入方向的保证带宽
步骤4	show tc-policy		查看策略的当前配置

参数说明：

bandwidth：

参数	说明	缺省配置
(ingress|egress)	接口的入/出方向	
<8-100000000>	保证带宽取值范围 8-100000000，单位kbps	

注意

1、保证带宽不能大于最大带宽。

2、保证带宽不能大于上一级的保证带宽。

3、配置完保证带宽后，会按照比例生成生效的保证带宽。

45.3.7 配置主机带宽

用 perip (ingress|egress)命令可以配置出/入方向的主机带宽，对匹配该策略的流量按方向进行每源 ip 限速。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	tc-policy channel NAME	对于一条已经配置好的流控策略，可以用该命令进入策略模式
步骤3	perip (ingress|egress) <8-100000000>	配置出/入方向的主机带宽
步骤4	show running-config tc-policy	查看策略的当前配置

使用 no perip (ingress|egress)可以取消主机限速。

参数说明：

perip：

参数	说明	缺省配置
(ingress|egress)	接口的入/出方向	
<8-100000000>	主机带宽取值范围 8-100000000，单位kbps	

45.3.8 移动策略顺序

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	tc-policy channel NAME	对于一条已经配置好的流控策略，可以用该命令进入策略模式
步骤3	move (top|bottom|up|down)	移动策略的顺序
步骤4	show tc-policy	查看策略的当前配置

参数说明：

move：

参数	说明	缺省配置
(top|bottom|up|down)	（顶端|底端|上移|下移）	

注意

只有同级的策略才能移动顺序。

45.3.9 开启策略日志

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	tc-policy channel NAME	对于一条已经配置好的流控策略，可以用该命令进入策略模式
步骤3	log	开启日志
步骤4	show running-config tc-policy	查看策略的当前配置

使用 no log 可以关闭日志。

45.4 策略的监控与维护

45.4.1 查看统计结果

查看流控配置的统计结果

步骤1	查看流控配置的统计结果
	show tc-policy statistics --- INPKTS INOCTS INbps INdrops EPKTS EOCT Ebps Edrops --- 统计结果显示了 入方向：通过报文个数；通过字节数；通过比特数/秒；丢弃的报文数 出方向：通过报文个数；通过字节数；通过比特数/秒；丢弃的报文数

45.4.2 查看数据流的匹配情况和丢包情况

查看数据流的匹配情况和丢包情况，为了在终端显示该调试信息，需要执行命令 terminal monitor。

步骤1	显示调试信息
	terminal monitor debug tc-policy match debug tc-policy drop

注意	由于此命令会在命令行上打印大量的信息，占用很多 CPU 资源，所以在调试结束的时候，一定要用 no debug tc-policy all 命令禁用此功能。

45.5 配置案例

案例描述

公司互联网出口带宽 10M，都通过网卡 eth0 连接到 internet，配置策略分别给

不同部门分配相应带宽。

配置步骤：

步骤1	创建地址对象Product和Administrative和Sale
	(config)# address Product
	(config-addr)# net-address 10.1.1.0/24
	(config-addr)# exit
	(config)# address Administrative
	(config-addr)# net-address 10.1.2.0/24
	(config-addr)# exit
	(config)# address Sale
	(config-addr)# net-address 10.1.3.0/24
	(config-addr)# exit
步骤2	创建线路策略 Company
	(config)# tc-policy line Company
	(config-tc-Company)#match interface eth0
	(config-tc-Company)#maxbandwidth ingress 10000
	(config-tc-Company)#maxbandwidth egress 10000
步骤3	创建流控策略CL-product
	(config)# tc-policy channel CL-product parent Company
	(config-tc-Product)#maxbandwidth ingress 2000
	(config-tc-Product)#maxbandwidth egress 2000
	(config-tc-Product)#bandwidth ingress 1000
	(config-tc-Product)#bandwidth egress 1000
	(config-tc-Product)#match Product any any any any always
步骤4	创建流控策略CL-administrative
	(config)# tc-policy channel CL-administrative parent Company
	(config-tc-Product)#maxbandwidth ingress 4000
	(config-tc-Product)#maxbandwidth egress 4000
	(config-tc-Product)#bandwidth ingress 2000
	(config-tc-Product)#bandwidth egress 2000
	(config-tc-Product)#match Administrative any any any any always
步骤5	创建流控策略CL-sales
	(config)# tc-policy channel CL-sales parent Company
	(config-tc-Product)#maxbandwidth ingress 5000
	(config-tc-Product)#maxbandwidth egress 5000
	(config-tc-Product)#bandwidth ingress 4000
	(config-tc-Product)#bandwidth egress 4000
	(config-tc-Product)#match Sales any any any any always

步骤6	查看策略配置
	(config)# show tc-policy

46 配置会话控制策略

46.1 会话控制概述

用户可以针对连接会话，进行新建或者并发的控制，从而保护连接表不被攻击填满，并且能够在一定程度上限制一些服务或应用的带宽。

会话控制支持根据入接口、源地址、目的地址、时间、服务、用户和应用的组合去进行控制。会话控制功能包括了源主机连接限制、源主机连接速率限制、目的主机连接限制、目的主机连接速率限制、总连接限制和总连接速率限制六种限制方式。

通过配置会话控制策略可以对经过设备的数据流进行有效的控制。当设备收到数据报文时，把该报文的源地址、目的地址、服务等信息和用户配置的会话控制策略匹配，决定是否对这条数据流进行限制，并且把这条流和匹配的会话控制策略关联起来，从而确定如何处理该流的后续报文。

会话控制策略按 IPv4 或 IPv6 从上往下匹配的原则，只对通过防火墙的数据包进行处理，对于设备本身发出的数据包不进行限制。

46.2 配置会话控制

46.2.1 缺省配置

内容	缺省设置	备注
源主机连接限制	不限制	可更改设置
源主机连接速率限制	不限制	可更改设置
目的主机连接限制	不限制	可更改设置
目的主机连接速率限制	不限制	可更改设置
总连接限制	不限制	可更改设置
总连接速率限制	不限制	可更改设置

46.2.2 创建会话控制

步骤：

步骤1	configure terminal	进入配置模式
步骤2	policy-session id IF_IN SIP DIP SRV_OBJ USER USER APP TR	配置一个会话控制策略，并进入会话控制配置节点

参数说明：

命令：policy-session id IF_IN SIP DIP SRV_OBJ USER APP TR

参数	说明	缺省配置
<id >	会话控制策略id号	无
< IF_IN >	入接口	any
<SIP>	源地址	any
< DIP >	目的地址	any
< SRV_OBJ >	服务	any
<USER>	用户	any
< APP >	应用	any
< TR >	时间表	always

46.2.3 进入会话控制策略配置节点

步骤：

步骤1	configure terminal	进入配置模式
步骤2	policy-session id	进入指定id的会话控制配置节点

使用 no policy-session id 命令可以删除对应 id 的会话控制策略。

46.2.4 开启会话控制策略日志

在会话控制策略中开启日志

步骤：

步骤1	configure terminal	进入配置模式
步骤2	policy-session id	进入会话控制配置节点
步骤3	log session policy	开启策略日志

使用 no log session policy 命令可以关闭会话控制策略的日志。

46.2.5 配置限制方式

在会话控制策略中配置限制方式。

步骤：

步骤1	configure terminal	进入配置模式
步骤2	policy-session id	进入会话控制配置节点
步骤3	session rate-limit per-sip x	配置源主机连接速率限制
	session rate-limit per-dip x	配置目的主机连接速率限制

	session rate-limit x	配置总连接速率限制
	session sum-limit per-sip x	配置源主机连接限制
	session sum-limit per-dip x	配置目的主机连接限制
	session sum-limit x	配置总连接限制

参数说明：

命令（1）：session rate-limit per-sip x

参数	说明	缺省配置
<x>	源主机连接速率限制值	缺省为0个/秒，表示不限制

命令（2）：session sum-limit per-sip x

参数	说明	缺省配置
<x>	源主机连接限制值	缺省为0个，表示不限制

使用如下命令可以取消相关限制：

no session rate-limit per-sip 取消源主机连接速率限制

no session rate-limit per-dip 取消目的主机连接速率限制

no session rate-limit 取消总连接速率限制

no session sum-limit per-sip 取消源主机连接限制

no session sum-limit per-dip 取消目的主机连接限制

no session sum-limit 取消总连接限制

46.2.6 移动会话控制策略顺序

步骤：

步骤1	configure terminal	进入配置模式
步骤2	policy-session move id1 after id2	移动会话控制策略id1到id2之后
	policy-session move id2 before id1	移动会话控制策略id2到id1之前

46.2.7 启用会话控制策略

步骤：

步骤1	configure terminal	进入配置模式
步骤2	policy-session id	进入会话控制配置节点
步骤3	enable	启用会话控制策略

使用 no enable 命令可以取消启用会话控制策略。

46.3 配置案例

46.3.1 配置案例: 配置一条会话控制策略进行会话控制

案例描述

为用户 user1 配置一个入接口为 ge/3,源地址为 any,目的地址为 any,服务为 http,应用为 any,时间表为 anytime 的会话控制策略，将总连接数限制为 1000 个，源 ip 总连接速率限制为 10 个/秒。

配置步骤：

步骤1	进入配置模式
	host# config terminal
步骤2	创建一个用户组test
	usergroup test
步骤3	创建一个用户user1
	user access user1 local 111111
步骤4	将上述用户加入到用户组
	user access user1 group test
步骤5	创建一个会话控制策略
	host(config)# policy-session 1 ge0/3 any any http user1 any always
步骤6	配置总连接数限制为1000个
	host(session-policy)# session sum-limit 1000
步骤7	配置源ip总连接速率限制为10个/秒
	host(session-policy)# session rate-limit per-sip 10
步骤8	启用会话控制策略
	host(session-policy)# enable

46.4 会话控制监控与维护

46.4.1 查看会话控制信息

查看会话控制的步骤：

步骤	进入enable模式执行show running-config policy-session

查看配置结果：

host# show running-config policy-session

ftp_check enable

sip_check disable

h323_check disable

rtsp_check disable

```
!
!!
policy-session 1 ge0/3 any any http user1 any always
 session rate-limit per-sip 10
 session sum-limit 1000
 enable
!
!
```

host# 1是会话控制策略id号；*ge0/3*是会话控制策略配置的入接口名称,enable表示启用这条会话控制策略。

46.5 常见故障分析

46.5.1 故障现象：

现象	匹配上某条策略的某些数据流没有受到相应的限制
分析	有可能是以下几种情况导致该策略无法生效： ● 该策略没有启用，请检查策略状态是否为启用； ● 由于策略在IPv4或IPv6有相同入接口时按从上往下的原则进行匹配，数据流可能匹配到前面的某条策略，请检查配置是否冲突。
解决	启用该策略，如果和其他策略的配置冲突，可以根据需求修改策略或者改变策略的顺序。

47 配置 Web 认证策略

47.1 Web认证策略概述

配置 Web 认证策略前需要先配置认证用户组和认证服务器。配置认证用户时，既可以选择配置单个用户，也可以选择配置用户组。但是在 Web 认证策略中只能配置用户组。Web 认证策略将过滤掉没有经过认证的用户报文，对应经通过认证的报文进行转发。。

47.2 配置Web认证策略

在配置 Web 认证策略前，需要先配置用户及用户组。在配置用户时，既可以选择配置认证用户也可以选择配置静态绑定用户。

47.2.1 缺省配置信息

防火墙设备关于 Web 认证策略的缺省设置信息如以下表格所示：

表47-1 Web 认证策略的缺省配置信息

内容	缺省设置	备注
Web认证策略使能	disable	可更改设置

47.2.2 创建用户组

步骤：

步骤1	configure terminal	进入配置模式
步骤2	1)user access username local password	配置一个本地用户
	2)user access username ldap servername	配置一个ldap认证用户
	3)user access username radius servername	配置一个radius认证用户
	4)user access username static[disable]	配置一个静态用户
步骤3	usergroup name	创建用户组
步骤4	user access username group groupname	将用户添加到用户组中

参数说明：

参数	说明	缺省配置
<local >	本地认证	无
< ldap >	ldap服务器认证	无

< radius >	radius服务器认证	无
< static >	配置静态用户	无
< user >	用户	无
< usergroup >	用户组	无

47.2.3 创建Web认证策略

步骤：

步骤1	configure terminal	进入配置模式
步骤2	webauth-policy id if_in if_out src dst tr action	配置一个Web认证策略，并进入Web认证策略配置节点

参数说明：

命令：webauth-policy id if_in if_out src dst tr [permit| webauth]

参数	说明	缺省配置
<id >	Web认证策略id号	无
< if_in >	入接口	any
< if_out >	出接口	any
<src>	源地址	any
<dst>	目的地址	any
<tr>	时间表	always
<permit >	Web认证策略动作为允许	无
<webauth>	Web认证策略动作为认证用户	无

47.2.4 将用户组添加到Web认证策略中

步骤：

步骤1	configure terminal	进入配置模式
步骤2	webauth-policy id	配置一个Web认证策略，并进入Web认证策略配置节点
步骤3	webauth-group groupname	将用户组挂到Web认证策略下

47.2.5 移动Web认证策略顺序

步骤：

步骤1	configure terminal	进入配置模式
步骤2	webauth-policy move 1 before 2	移动web认证策略1到2之前
	webauth-policy move 1 after 2	移动web认证策略1到2之后

47.2.6 启用Web认证策略

步骤：

步骤1	configure terminal	进入配置模式
步骤2	webauth-policy id	进入Web认证配置节点
步骤3	enable	启用Web认证策略

使用 no enable 命令可以取消启用 Web 认证策略。

47.3 配置案例

47.3.1 配置一条挂有用户组的Web认证策略

案例描述

配置一个入接口为 ge0/3,出接口为 ge0/0,源地址为 any,目的地址为 any,时间表为 anytime,动作为 webauth 的 Web 认证策略，引用的用户组为 test1，并开启 Web 认证策略。

步骤1	进入配置模式
	host# config terminal
步骤2	配置用户
	host(config)#user access user111 local 111111
步骤3	配置用户组
	usergroup test1
步骤4	将用户挂到用户组中
	user access user111 group test1
步骤5	创建Web认证策略
	host(config)#webauth-policy 11 ge0/3 ge0/0 any any always webauth
步骤6	引用用户组test1
	host(config-webauth-policy)# webauth-group test1
步骤7	使能这个Web认证策略
	host(config-webauth-policy)# enable

配置结果：

host# show webauth-policy 11

webauth-policy 11 ge0/3 ge0/0 any any always webauth
 enable
 match statistic: 0
webauth-group test1
!

47.3.2 查看web认证策略配置

查看 web 认证策略配置的步骤：

步骤	进入enable模式执行show running-config webauth-policy
	查看配置结果： host# show running-config webauth-policy !! protect-policy 11 ge0/3 ge0/0 any any always webauth enable webauth-group test1 ! 11是Web认证策略id号; *ge0/3*是Web认证策略配置的入接口名称, *ge0/0*是Web认证策略配置的出接口名称,，enable表示启用这条策略，test1是这条Web认证策略引用用户组的名称。

47.4 常见故障分析

47.4.1 故障现象：认证用户进行认证时失败

现象	认证用户进行认证时失败。
分析	（1） 密码错误 （2） 用户已经禁用 （3） 本地不保存用户名的认证用户认证时所在的组没有加入RADIUS服务器 （4） RADIUS/LDAP服务器配置错误（比如：共享密钥，IP等） （5） RADIUS/LDAP服务器连接不上（比如：PING不通） （6） RADIUS/LDAP服务器上没有这个用户
解决	（2） 检查用户密码，输入正确的用户名和密码 （3） 解禁用户 （4） 为该用户认证时所在的组添加RADIUS/LDAP服务器 （5） 修改该RADIUS/LDAP服务器的配置 （6） 首先确保防火墙USG和RADIUS/LDAP服务器能通讯，能PING通

	（7） 为该RADIUS/LDAP服务器添加该用户

53 配置地址对象

48.1 地址对象、域名地址和地址对象组概述

为了方便用户配置和管理，防火墙设备中引入了地址对象的概念。地址对象分为地址节点、域名地址和地址组，地址组是地址节点和域名地址的集合。在其它功能的配置中，可以引用地址对象来定义配置生效的条件。

48.2 配置地址对象和地址组

地址对象分为 IPV4 类型，IPV6 类型，MAC 类型以及 IP+MAC 类型。其中 IPV4 类型的地址对象中可以指定确定的 IP 地址，也可以用网络掩码的形式指定 IP 范围，还可以通过起止 IP 地址的形式确定 IP 范围，或者添加 ISP 地址库。

IPV6 类型的地址对象中可以指定确定的 IP 地址，也可以用网络掩码的形式指定 IP 范围，还可以通过起止 IP 地址的形式确定 IP 范围。MAC 类型的地址对象中可以指定多个 MAC 地址。IP+MAC 类型的地址对象中，可以将一个 IP 地址与一个 MAC 地址作为地址对来进行管理。

48.2.1 配置IPV4类型的地址对象

■ 创建地址对象

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	address NAME	创建名为NAME的地址对象
步骤3	show address NAME	显示地址对象的配置信息

使用 no address NAME 可以删除指定地址对象。

■ 向地址对象中添加地址成员（主机，子网，范围，isp 地址库）

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	address NAME	进入名为NAME的地址对象模式
步骤3	description LINE	描述该地址对象
步骤4	host-address A.B.C.D	将指定的IP地址加入该地址对象中
步骤5	no host-address A.B.C.D	将指定的IP地址从地址对象中删除
步骤6	net-address A.B.C.D/M	将一个网络掩码加入该地址对象中
步骤7	no net-address A.B.C.D/M	将指定的网络地址从地址对象中删除

步骤8	range-address A.B.C.D E.F.G.H	用起止与终止IP地址表示范围，并添加到该地址对象中
步骤9	no range-address A.B.C.D E.F.G.H	将指定的地址范围从地址对象中删除
步骤10	isp-address NAME	将一个ISP地址库加入地址对象
步骤11	no isp-address NAME	将指定的ISP地址库从地址对象中删除
步骤12	show address NAME	显示地址对象的配置信息

■ 向地址对象中添加排除地址成员（子网，范围）

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	address NAME	进入名为NAME的地址对象模式
步骤3	net-address-exp A.B.C.D/M	将指定的排除IP网络掩码加入该地址对象中
步骤4	no net-address-exp A.B.C.D/M	将排除IP网络掩码从该地址对象中删除
步骤5	range-exp-address A.B.C.D E.F.G.H	将指定的排除IP地址范围加入该地址对象中
步骤6	no range-exp-address A.B.C.D E.F.G.H	将排除IP地址范围从该地址对象中删除
步骤7	show address NAME	显示地址对象的配置信息

48.2.2 配置IPV6类型的地址节点

■ 创建 IPV6 地址对象

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	address-v6 NAME	创建名为NAME的IPV6类型地址对象
步骤3	show address-v6 NAME	显示地址对象的配置信息

使用 no address-v6 NAME 可以删除指定 IPV6 地址对象。

■ 向地址对象中添加 IPV6 地址成员（主机，子网，范围）

步骤1	configure terminal	进入配置模式
步骤2	address-v6 NAME	进入名为NAME的地址对象模式
步骤3	description LINE	描述该地址对象
步骤4	host-v6 X:X::X:X	将指定的IPV6地址加入该地址对象中
步骤5	no host-address X:X::X:X	将指定的IPV6地址从地址对象中删除
步骤6	net-v6 X:X::X:X/M	将一个网络掩码加入该地址对象中
步骤7	no net-v6 X:X::X:X/M	将指定的网络地址从地址对象中删除
步骤8	range-v6 X:X::X:X X:X::X:X	用起止与终止IP地址表示范围，并添加到该地址对象中
步骤9	no range-v6 X:X::X:X X:X::X:X	将指定的地址范围从地址对象中删除

步骤10	show address-v6 NAME	显示地址对象的配置信息

48.2.3 配置MAC类型的地址节点

■ 创建地址对象：

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	address-mac NAME	创建名为NAME的MAC类型地址对象
步骤3	description LINE	描述该地址对象
步骤4	show address-mac NAME	显示地址对象的配置信息

使用 no address-mac NAME 可以删除指定 MAC 地址对象

■ 向地址对象中添加 mac 地址成员

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	address-mac NAME	进入名为NAME的MAC类型地址对象
步骤3	mac-address FF-FF-FF-FF-FF-FF	将指定的MAC地址加入地址对象
步骤6	show address-mac NAME	显示地址对象的配置信息

使用 no mac-address FF-FF-FF-FF-FF-FF 可以将指定的 MAC 地址从地址对象中删除

必须在系统->配置->DNS 中，配置好首选 DNS 服务器，域名地址才能解析到对应的 IP 地址，自动添加为该域名地址对象的成员。

48.2.4 配置IP+MAC类型的地址节点

■ 创建地址对象：

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	address-ip-mac NAME	创建名为NAME的IP+MAC类型地址对象
步骤3	description LINE	描述该地址对象
步骤4	show address-mac NAME	显示地址对象的配置信息

使用 no address-ip-mac NAME 可以删除指定的 IP+MAC 地址对象

■ 向地址对象中添加 IP+MAC 地址成员

配置步骤：

步骤1	configure terminal	进入配置模式

步骤2	address-ip-mac NAME	进入名为NAME的IP+MAC类型地址对象
步骤4	bind A.B.C.D FF-FF-FF-FF-FF-FF	将指定的IP地址与MAC地址对加入地址对象
步骤5	show address-ip-mac NAME	显示地址对象的配置信息

使用 no bind A.B.C.D FF-FF-FF-FF-FF-FF ，将指定的 IP 地址与 MAC 地址对从地址对象中删除

48.2.5 配置地址组

地址对象组是地址对象的集合，一个地址对象组中可以包括多个地址对象。

可以用 address-object 命令向地址对象组中添加一个地址对象。

- 创建地址组：

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	address-group NAME	创建名为NAME的地址组
步骤3	description .LINE	为地址组添加描述
步骤4	show address-group NAME	显示地址对象组的配置信息

使用 no address-group NAME 可以删除指定的地址组

- 向地址组中添加地址对象成员

步骤1	configure terminal	进入配置模式
步骤2	address-group NAME	进入名为NAME的地址对象组模式
步骤3	address-object ADDRESS	将指定的地址节点添加到该地址组中
步骤4	show address-group NAME	显示地址对象组的配置信息

使用 no address-object ADDRESS 命令可以删除地址对象组中通过 address-object 命令添加的地址对象。

48.2.6 配置域名地址

域名地址是一种特殊的地址组，地址组名称定义为域名地址，地址组成员是由配置域名解析到的 IP 地址集合，解析分为主动探测及被动探测两种解析方式。

- 创建主动+被动解析方式域名地址：

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	address-domain DOMAIN	创建名为DOMAIN的主动+被动解析域名地址

步骤3	end	推出配置模式
步骤4	show address-domain	显示域名地址的配置和成员信息

使用 no address-domain DOMAIN 可以删除指定的域名地址

■ 创建仅被动解析方式域名地址：

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	address-domain-passive DOMAIN	创建名为DOMAIN的仅被动解析域名地址
步骤3	end	推出配置模式
步骤4	show address-domain	显示域名地址的配置和成员信息

使用 no address-domain-passive DOMAIN 可以删除指定的域名地址

■ 域名地址对象解析时间间隔配置：

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	address-domain-timer set <10-7200>	设置域名地址对象解析时间间隔
步骤3	end	推出配置模式
步骤4	show address-domain timer	查看域名地址对象解析时间间隔

使用 no address-domain timer 可以取消域名地址对象解析间隔设置(默认 20s)

■ 域名地址对象每次解析数量配置：

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	address-domain-up-num set <1-200>	设置域名地址对象每次解析数量
步骤3	end	推出配置模式
步骤4	show address-domain-up-num	查看域名地址对象每次解析数量

使用 no address-domain-up-num 可以取消域名地址对象每次解析数量设置(默认 20 条)

■ 解析到成员的自动淘汰时间配置：

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	address-domain-member-rtt set <0-3600>	设置成员的自动淘汰时间，0为关闭成员自动淘汰机制
步骤3	end	推出配置模式
步骤4	show address-domain-member-rtt	查看成员的自动淘汰时间

使用 no address-domain-member-rtt 可以取消设置成员的自动淘汰时间设置(默认 3600s)

48.3 配置案例

48.3.1 配置案例：添加地址对象与地址对象组

案例描述

配置一个地址对象和一个地址对象组并且将这个地址对象放入地址对象组里。

配置步骤：

步骤1	创建一个地址对象
	USG_A(config)# address dev
步骤2	在这个地址对象中添加一个主机地址
	USG_A(config-addr)# host-address 192.168.10.100
步骤3	创建一个地址对象组
	USG_A(config)# address dev-group
步骤4	将地址对象(dev)添加到这个地址对象组里
	USG_A(config-addrgrp)# address-object dev
步骤5	显示添加信息
	USG_A(config)# show address-group address-group dev-group address-object dev !

配置结果：

```
USG_A# show running-config
address dev
    host-address 192.168.10.100
!
address-group dev-group
    address-object dev
!
```

48.4 地址对象与地址对象组监控与维护

48.4.1 查看地址对象

查看某个地址对象的步骤：

步骤1 显示某个地址对象信息

```
USG_A# show address dev
address dev
    host-address 192.168.10.100
!
USG_A#
```

dev是地址对象名称; 192.168.10.100是主机IP地址。

48.4.2 查看地址对象组

查看某个地址对象组的步骤：

步骤1 显示某个地址对象组信息

```
USG_A# show address-group dev-group
Address-group dev-group
    address-object dev
!
USG_A#
```

dev-group是地址对象组名称; dev是地址对象。

48.4.3 查看域名地址

查看域名地址的步骤：

步骤1 显示所有域名地址的配置和成员信息

```
host# show address-domain
address-domain www.baidu.com
  dnsresolve: 110.242.68.4
  dnsresolve: 110.242.68.3
address-domain-passive baidu
!
host#
```

	www.sina.com是域名地址的名称；dnsresolve中显示的从解析到的IP地址。

查看域名地址成员数量的步骤：

步骤1	显示所有域名地址成员数量
	host# show address-domain member num domain member num all: 2

48.5 常见故障分析

48.5.1 故障现象1：

现象	执行no address|address-group NAME以后，该对象或对象组仍然存在。
分析	当一个对象或对象组正在被引用时，就不能通过no命令删除。
解决	可以先撤销其它配置对该对象或对象组的引用，确定其没有被引用之后再用no命令删除该节点。

48.5.2 故障现象2：

现象	新建域名地址后，查看域名地址列表，成员为空。
分析	检查系统的DNS服务器是否已经配置并且能够正常访问。
解决	为系统配置有效的DNS服务器。

54 配置服务对象

49.1 服务对象和服务对象组概述

为了方便用户配置和管理，防火墙设备中引入了服务对象的概念。在其它功能的配置中，可以引用服务对象来定义配置生效的条件。

49.2 配置服务对象和服务对象组

服务对象中包含了协议和协议属性。

49.2.1 配置向服务对象中添加TCP|UDP服务

可以用 tcp|udp 命令向 Service 中添加 tcp|udp 服务。对于 TCP 和 UDP 来讲，服务对象包含协议、源端口和目标端口信息。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	service NAME	进入名为NAME的服务对象模式，如果不存在就创建新的服务对象。
步骤3	(tcp|udp) dest <1-65535> [<1-65535>] [source <1-65535> [<1-65535>]]	添加一个tcp|udp服务，需要指定目标端口或范围，也可以指定源端口或范围
步骤4	show service NAME	显示服务对象NAME的配置信息

使用 no (tcp|udp) dest <1-65535> [<1-65535>] [source <1-65535> [<1-65535>]] 可以取消对服务对象的设置。

参数说明：

命令（1）：service NAME

参数	说明	缺省配置
<NAME>	服务对象的名称	无

命令（2）：(tcp|udp) dest <1-65535> [<1-65535>] [source <1-65535> [<1-65535>]]

参数	说明	缺省配置
<dest>	目标端口	无
<1-65535>	目标起止端口	无

<1-65535>	目标终止端口	无
<source>	源端口	无
<1-65535>	源起止端口	无
<1-65535>	源终止端口	无

49.2.2 配置向服务对象中添加ICMP服务

可以用 icmp 命令向 Service 中添加 icmp 服务。对于 ICMP，服务对象包含协议、type、code 信息。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	service NAME	进入名为NAME的服务对象模式，如果不存在就创建新的服务对象。
步骤3	icmp <0-255> [<0-255>]	添加一个icmp服务，需要指定type，可以指定code
步骤4	show service NAME	显示服务对象NAME的配置信息

参数说明：

命令（1）：icmp <0-255> [<0-255>]

参数	说明	缺省配置
<0-225>	ICMP type	无
<0-225>	ICMP code	无

49.2.3 配置向服务对象中添加IP服务

可以用 ip 命令向 Service 中添加 ip 服务。对于 IP，服务对象包含协议类型信息。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	service NAME	进入名为NAME的服务对象模式，如果不存在就创建新的服务对象。
步骤3	ip <1-255>	添加一个ip服务，需要指定protocol
步骤4	show service NAME	显示服务对象NAME的配置信息

参数说明：

命令（1）：ip <0-255>

参数	说明	缺省配置
<0-225>	Protocol type	无

49.2.4 配置向服务对象组中添加服务对象

服务对象组是服务对象的集合，一个服务对象组中可以包括多个服务对象。

可以用 service-object 命令向服务对象组中添加一个服务对象，可以是系统预定义服务，也可以是用户自定义的服务。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	service-group NAME	进入名为NAME的服务对象组模式，如果不存在就创建新的服务对象组。
步骤3	service-object ("CMD_GROUP_SERVICE")	将指定的预定义服务或自定义服务或any添加到该服务对象组中
步骤4	show service-group NAME	显示服务对象NAME的配置信息

参数说明：

命令（1）：service-object ("CMD_GROUP_SERVICE")

参数	说明	缺省配置
<"CMD_GROUP_SERVICE ">	系统支持的预定义服务或者自定义服务或any	无

使用 no service-object ("CMD_GROUP_SERVICE")命令可以删除服务对象组中通过 service-object 命令添加的服务对象。

"CMD_GROUP_SERVICE" 是 " CMD_GROUP_SERVICEX "|SRV_OBJ|any", CMD_GROUP_SERVICEX是系统预定义的服务，分别有 ah|aol|bgp|bootpc|bootps|daytime|dh cp|dns||esp||finger|ftp|gopher|gre|h323| hostname|http|https|icmp|igmp|ike|imap| info_adress|info_request|irc|interne t-locator- service|l2tp|ldap|mysql|ne tmeeting|netbios-ns|netbios-dgm| netbios-ssn|nfs|nicname|nntp|ntp| onc-rpc|osf|pc-anywhere|pim|ping| ping6|pop2|pop3|pptp|printer|quake|rad ius|radius-acct|raudio||rexec|rip|rlo

	gin|rsh|samba|sccp|sip|sip-man messenger|shell|smtp|smux|snmp|s ocks|aquid|ssh|syslog|talk|tcp|telne t|tftp|time|timestamp|tproxy|udp|uucp|vdol ive|wais|webcache|winframe|who|x-windows ，SRV_OBJ 是用户自定义的服务名称，any 为任意服务。

49.3 配置案例

49.3.1 配置案例1: 添加服务对象与服务对象组

案例描述

配置一个服务对象和一个服务对象组并且将这个服务对象放入服务对象组里。

配置步骤：

步骤1	创建一个服务对象
	USG_A(config)# service svc
步骤2	在这个地址对象中添加TCP服务
	USG_A(config-sev)# tcp dest 80
步骤3	创建一个服务对象组
	USG_A(config)# service-group svc-group
步骤4	将服务对象(svc)添加到这个服务对象组里
	USG_A(config-sevgrp)# service-object svc
步骤5	显示添加信息
	USG_A(config)# show service-group service-group svc-group service-object svc ! USG_A(config)#

配置结果：

```
USG_A# show running-config
service svc
    tcp dest 80
!
service-group svc-group
    service-object svc
```

!

49.3.2 配置案例2:配置服务对象

案例描述

配置一个服务对象，其中包含 tcp 协议，目标端口分别为 23，源端口的范围是 1~65535。

配置步骤：

步骤1	创建一个服务对象
	USG_A(config)# service telnet
步骤2	向服务对象中添加端口范围
	USG_A(config-sev-obj)# tcp 23 source 1 65535

49.4 服务对象与服务对象组监控与维护

49.4.1 查看服务对象

查看某个地址对象的步骤：

步骤1	显示某个地址对象信息
	USG_A# show service svc service svc tcp dest 80 ! USG_A# svc是服务对象名称; 80是目标端口。

49.4.2 查看服务对象组

查看某个地址对象组的步骤：

步骤1	显示某个地址对象组信息
	USG_A # show service-group svc-group service-group svc-group service-object svc ! USG_A # svc-group是服务对象组名称; svc是服务对象名称。

49.5 常见故障分析

49.5.1 故障现象1：

现象	执行no service|service-group NAME以后，该对象或对象组仍然存在。
分析	当一个对象或对象组正在被引用时，就不能通过no命令删除。
解决	可以先撤销其它配置对该对象或对象组的引用，确定其没有被引用之后再用no命令删除该节点。

55 配置应用对象

50.1 应用对象概述

为了方便用户配置和管理，防火墙设备中引入了应用对象的概念。在其它功能的配置中，可以引用应用对象来定义配置生效的条件。

应用对象主要包括：

- 预定义应用：具体的用户应用，如下载软件、即时通信软件，目前有 20 大类 1000 多种应用，通过应用于特征库更新，不需要用户配置。
- 自定义应用：需要用户自行配置。
- 应用组：需要用户自行配置，可引用预定义应用和自定义应用。

50.2 配置应用对象

50.2.1 配置自定义应用

自定义应用可配置协议类型、源地址、目的地址、源端口和目标端口信息。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	app-custom NAME	配置自定义应用
步骤3	custom protocol (tcp|udp)	选择协议类型
步骤4	custom (src-ip NAME| src-port <1-65535>| dst-ip NAME| dst-port <1-65535>)	配置源地址、源端口、目的地址、目的端口。
步骤5	end	返回特权模式
步骤6	show app-custum	显示自定义应用配置

使用 no custom (protocal|src-ip|dst-ip|src-port|dst-port)可以取消对自定义应用的设置。

参数说明：

命令（1）：app-custom NAME

参数	说明	缺省配置
<NAME>	自定义应用的名称	无

命令（2）：custom (src-ip NAME| src-port <1-65535>| dst-ip NAME| dst-port <1-65535>)

参数	说明	缺省配置
<src-ip>	源地址	无
<NAME>	地址对象的名称	无
<src-port>	源端口	无
<1-65535>	源端口	无
<dst-ip>	目的地址	无
<NAME>	地址对象的名称	无
<dst-port>	目的端口	无
<1-65535>	目的止端口	无

50.2.2 配置应用组

实际使用中，一个策略经常需要引用多个应用，将需要引用的应用配置到应用组中，引用该应用组即可。可引用预定义应用和自定义应用。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	app-group NAME	配置应用组
步骤3	desc DESC	设置应用组描述
步骤4	member (app| category) NAME	引用应用或者应用分类
步骤5	end	返回特权模式
步骤6	show app-group	显示应用组配置

使用 no member (app| category) NAME 可以删除应用组对应用的引用。

参数说明：

命令（1）：app- group NAME

参数	说明	缺省配置
<NAME>	应用组的名称	无

命令（2）：member (app| category) NAME

参数	说明	缺省配置
<app>	引用预定义应用或者自定义应用	无
<category>	引用应用分类	无
<NAME>	应用或者应用分类的名称	无

50.3 配置案例

50.3.1 添加自定义应用与应用组

案例描述

配置一个协议类型为 tcp、源地址引用地址对象名称是 123 的自定义应用和一个应用组，并且将这个自定义应用放入应用组里。

配置步骤：

步骤1	创建一个自定义应用
	FW_A(config)# app-custom c1
步骤2	在这个自定义应用中配置协议类型
	FW_A(config-app-custom)#custom protocol tcp
步骤3	在这个自定义应用中配置源地址
	FW_A(config-app-custom)#custom src-ip 123
步骤3	创建一个应用组
	FW_A(config)# app-group g1
步骤4	将自定义应用(c1)添加到这个应用组里
	FW_A(config-app-profile)#member app c1
步骤5	显示添加信息
	FW_A(config)# show app-group g1 member app c1 FW_A(config)#

配置结果：

```
FW_A# show running-config
app-custom c1
 custom protocol tcp
 custom src-ip 123
! app-group g1
 member app c1
!
```

50.4 应用与应用组监控与维护

50.4.1 查看自定义应用

查看某个自定义应用的步骤：

步骤1	显示某个自定义应用信息	
	FW_A# show app-custom c1	
	app-custom c1	app-id:10006 ref:3

	custom protocol tcp custom src-ip 123 FW_A# c1是自定义名称; 123是地址对象名称。

50.4.2 查看应用组

查看某个应用组的步骤：

步骤1	显示某个应用组的信息
	FW_A# show app-group g1 member app c1 FW_A# g1是应用组的名称; c1是应用的名称。

50.5 常见故障分析

50.5.1 故障现象1：

现象	执行no app-custom|app-group NAME以后，该自定义应用或应用组仍然存在。
分析	当一个自定义应用或应用组正在被引用时，就不能通过no命令删除。
解决	可以先撤销其它配置对该自定义应用或应用组的引用，确定其没有被引用之后再用no命令删除该节点。

56 用户对象

51.1 用户对象概述

用户对象中包括两个成员：用户及用户组。用户的配置包括：用户类型、认证用户服务器类型。用户类型可分为认证用户及静态绑定用户两种。

认证用户：配置认证用户时需要配置相应的认证方式，可以是本地认证，也可以是 LDAP 服务器认证，或者 RADIUS 服务器认证。

- 本地认证：需要配置相应的认证密码。
- LDAP 服务器认证：需要指定相应的 LDAP 服务器。
- RADIUS 服务器认证：需要指定相应的 RADIUS 服务器。

静态绑定用户：配置静态绑定用户时，需要配置相应的绑定 IP。可以一个 IP 地址，也可以是一个 IP 地址范围。

所有的用户都可以选择启用或者不启用。

在新建用户组时需要配置的内容包括:用户组名称,用户成员及认证服务器成员。其中用户成员及认证服务器成员可以为空。

51.2 配置用户

配置步骤：

	configure terminal	进入配置模式
	user access *USERNAME* enable	新建用户并使能或者用户使能
	user access *USERNAME* disable	新建用户并去使能或者用户去使能
	user access *USERNAME* group *GROUPNAME*	若用户存在则将用户加入已经存在的用户组中。若用户不存在则新建用户同时将用户加入到用户组中
	user access *USERNAME* [ldap|radius] *SEVERNAME*	新建服务器认证用户，并指定认证该用户的服务器

	user access *USERNAME* local *PASSWORD*	新建本地认证用户，并指定认证密码。
	user access *USERNAME* static (config-user-static)# host-address *IP*	新建静态绑定用户，并指定一个单独IP
	user access *USERNAME* static (config-user-static)# range-address *BEGIN-IP END-IP*	新建静态绑定用户，并指定IP范围

参数说明：

参数	说明	缺省配置
< USERNAME >	用户名称	无
<GROUPNAME>	用户加入的已经存在的用户组名称	无
<SEVERNAME>	指定的用户服务器名称	无
< PASSWORD >	本地认证用户的认证密码	无
< IP>	静态绑定IP	无
< BEGIN-IP >	静态绑定IP范围的起始IP	无
< END-IP >	静态绑定IP范围的结束IP	无

51.3 配置用户组

配置步骤：

	configure terminal	进入配置模式
	usergroup *NAME*	新建用户组

参数说明：

参数	说明	缺省配置
< NAME >	用户组名称	无

51.4 配置案例

51.4.1 配置案例: 配置认证用户并加入用户组中

案例描述

配置一个名为 test1 的本地认证用户，认证密码为 12341234。配置一个名为 test2 的 LDAP 认证用户，指定其 LDAP 认证服务器的名称为 myldap。配置一个静态认证用户 test3，其静态绑定 IP 为 10.1.1.2。最后将这 3 个用户加入到用户组 testgroup 中。

配置步骤：

	host(config)# stated enable	使能设备信息记录功能
	host(config)# usergroup testgroup	新建用户组testgroup
	host(config)# user access test1 local 12341234	新建本地认证用户
	host(config)# user access test2 ldap myldap	新建LDAP认证用户
	host (config)# user access test3 static host (config-user-static)# host-address 10.1.1.2	新建静态认证用户 绑定IP
	host (config)#user access test1 enable host (config)#user access test2 enable host (config)#user access test3 enable	使能3个用户
	host(config)# user access test1 group testgroup host(config)# user access test2 group testgroup host(config)# user access test3 group testgroup	将3个用户加入到 testgroup用户组中

配置结果显示：

```
host# show access-user
Access User Name    User Type   User Status    Password/Radius-Server    Reference Count
test1               local       enable         12341234                  1
test2               ldap        enable         myldap                    1
test3               static      enable                                   1
Total users : 3
host#
```

host # show usergroup

Usergroup Name	Usergroup_Type	Refer_Count
testgroup	local	0

Total usergroups : 1

57 认证服务器

52.1 认证服务器概述

防火墙支持使用 RADIUS 服务器、LDAP 服务器的用户认证。（1）可以添加一个 RADIUS 服务器对象，以允许用户使用选定的 RADIUS 服务器进行认证。（2）可以添加一个 LDAP 服务器对象，以允许用户使用选定的 LDAP 服务器进行认证。在 web 认证与管理员认证中，可以选择配置的服务器对象进行远程认证。

52.2 配置说明

52.2.1 配置RADIUS认证服务器对象

配置步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	radius-server NAME A.B.C.D SECRET [PORT]	指定radius服务器名称、IP地址、密码、端口号
步骤3	end	退出全局模式

使用 no radius-server NAME命令删除已创建的radius服务器对象。

52.2.2 配置LDAP认证服务器对象

配置步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	ldap NAME	指定ldap服务器名称，进入ldap配置命令结点
步骤3	ldap A.B.C.D [PORT]	配置ldap服务器的IP地址、端口号
步骤4	dn DN	配置ldap服务器区别名dn
步骤5	bindtype regular user NAME passwd PASSWORD	配置ldap服务器管理员、密码
步骤6	end	退出ldap命令结点，退出全局模式

使用 no ldap NAME命令删除已创建的ldap服务器对象。

52.2.3 查看认证服务器对象

配置步骤：

步骤1	show radius-server	查看radius服务器对象列表
步骤2	show ldapserver	查看ldap服务器对象流表

52.2.4 配置案例

案例一

radius 服务器地址为 1.1.1.1，配置 radius 服务器供用户和管理员使用

配置步骤：

步骤1	进入配置模式
	host# config terminal
步骤2	创建radius服务器
	radius-server radius 1.1.1.1 secret 111111 1812

案例二：

ldap 服务器地址为 1.1.1.2，配置 ldap 服务器供用户和管理员使用

配置步骤：

步骤1	进入配置模式
	host# config terminal
步骤2	创建ldap服务器
	host(config)# ldap ldap_test
步骤3	配置ldap服务器的ip地址和端口号
	host(config-ldap)# ldap 1.1.1.2 389
步骤4	配置区别名
	host(config-ldap)# dn dc=test,dc=com
步骤5	配置用户名密码
	host(config-ldap)# bindtype regular user cn=admin,cn=users,dc=test,dc=com passwd 111111

52.3 AD域同步

52.3.1 AD域同步概述

使用 AD 域同步策略可以将 LDAP 服务器上的用户组同步到设备上，方便用户使用。

52.3.2 配置AD域同步

配置步骤：

	configure terminal	进入配置模式
	ad POLICY_NAME SERVER DN	配置同步策略
	ad POLICY_NAME sync	立即同步某条策略

使用 no ad POLICY_NAME 命令可以删除某条策略。

参数说明：

命令（1）：添加同步策略：ad POLICY_NAME SERVER DN

参数	说明	缺省配置
< POLICY_NAME >	同步策略名称	无
< SERVER >	需要同步的LDAP服务器名称	无
< DN >	同步信息在LDAP服务器上的路径	无

命令（2）：执行同步命令：ad POLICY_NAME sync

参数	说明	缺省配置
< POLICY_NAME >	同步策略名称	无

52.3.3 配置案例: 配置设备信息记录功能

案例描述

配置同步策略 aaa，需要同步的 LDAP 服务器为 myldap，需要同步的分支的 DN 为 dc=king，dc=com。立即同步该策略。

配置步骤：

	host(config)# ad aaa myldap dc=king,dc=com	配置同步策略
	host(config)# ad aaa sync	立即同步该策略

配置结果：

host# show ad

Policy Name	*Ldap Server*	*DN*
aaa	*myldap*	*dc=king,dc=com*

查看同步过来的用户：

acc# show usergroup

Usergroup Name	Usergroup_Type	Refer_Count
adc	local	0
aab	local	0
aaa	local	0
03	ldapsync	0
04	ldapsync	0
05	ldapsync	0
06	ldapsync	0
07	ldapsync	0
08	ldapsync	0
09	ldapsync	0
10	ldapsync	0
a	ldapsync	0
b	ldapsync	0

Total usergroups : 14

58 配置 URL 分类

53.1 URL分类概述

为了方便用户配置和管理，防火墙设备中引入了 URL 分类的概念。在其它功能的配置中，可以引用 URL 分类来定义配置生效的条件。

URL 分类主要包括：

- 预定义 URL 分类：将常见的 URL 进行分类，例如娱乐、金融理财、互联网门户等，通过 URL 特征库更新，不需要用户配置。
- 自定义 URL 分类：需要用户自行配置。
- URL 组：需要用户自行配置，可引用预定义 URL 分类和自定义 URL 分类。

53.2 配置URL分类

53.2.1 配置自定义URL分类

自定义 URL 分类可配置分类描述。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	url-custom NAME	配置自定义URL分类
步骤3	desc DESC	配置自定义URL分类描述
步骤4	end	返回特权模式
步骤5	show url-custum	显示自定义URL分类配置

使用 no desc 可以取消对自定义 URL 分类描述的设置。

参数说明：

命令（1）：url-custom NAME

参数	说明	缺省配置
<NAME>	自定义URL分类的名称	无

命令（2）：desc DESC

参数	说明	缺省配置
<DESC>	描述的内容	无

53.2.2 配置URL组

实际使用中，一个策略经常需要引用多个 URL 分类，将需要引用的 URL 分类配置到 URL 组中，引用该 URL 组即可。可引用预定义 URL 分类和自定义 URL 分类。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	url-group NAME	配置URL组
步骤3	desc DESC	设置URL组描述
步骤4	member url NAME	引用URL分类
步骤5	end	返回特权模式
步骤6	show url-group	显示URL组配置

使用 no member url NAME 可以删除 URL 组对 URL 分类的引用。

参数说明：

命令（1）：url- group NAME

参数	说明	缺省配置
<NAME>	URL组的名称	无

命令（2）：member url NAME

参数	说明	缺省配置
<NAME>	URL分类的名称	无

53.3 配置案例

53.3.1 添加URL组

案例描述

配置一个 URL 组，并且将名为“娱乐”的预定义 URL 分类加入 URL 组里。

配置步骤：

步骤1	创建一个URL组
	FW_A(config)# url-group g1
步骤2	将预定义URL分类(entertainment)添加到这个应用组里
	FW_A(config-url-group)#member url entertainment
步骤3	返回特权模式
	FW_A(config-url-group)#end
步骤4	显示添加信息

```
FW_A(config)# show url-group g1
 member url entertainment
FW_A(config)#
```

配置结果：

```
FW_A# show running-config
! url-group g1
 member url entertainment
!
```

53.4 URL分类与URL组监控与维护

53.4.1 查看预定义URL分类

查看预定义 URL 分类的步骤：

步骤1 显示预定义URL分类信息

```
FW_A# show url-class
======url-class======
 1 => entertainment      娱乐      提供综合性娱乐、影视的网站。
 2 => game               游戏      提供各种电子游戏的网站。
 3 => shopping   购物      提供网络购物站点的网站。
 4 => financial-planning          金融理财          提供各种类型金融理财的网站。
 5 => life-inquiry       生活查询          提供涉及日常生活的综合资讯或服务的网站。
 6 => interests  兴趣爱好          提供各种类别的兴趣爱好相关的网站。
 7 => education  教育      提供各类教育资讯或提供相关服务信息的网站。
 8 => sociality  社交      提供建立社会性网络的互联网应用服务的网站。
 9 => news       新闻      提供综合型新闻、资讯的网站。
 10 => email     邮件      用于电子手段提供信息交换的通信方式的网站。
```

53.4.2 查看自定义URL分类

查看自定义 URL 分类的步骤：

步骤1 显示自定义URL分类信息

```
FW_A# show url-custom
url-custom custom10   url_id: 1999          ref: 0
 str-num 1
```

53.4.3 查看URL组

查看某个 URL 组的步骤：

步骤1	显示某个URL组的信息
	FW_A# show url-group g1 member url entertainment FW_A# g1是应用组的名称; entertainment是应用的名称。

53.5 常见故障分析

53.5.1 故障现象1：

现象	执行no url-custom|url-group NAME以后，该自定义URL分类或URL组仍然存在。
分析	当一个自定义URL分类或URL组正在被引用时，就不能通过no命令删除。
解决	可以先撤销其它配置对该自定义URL分类或URL组的引用，确定其没有被引用之后再用no命令删除该节点。

59 配置域名对象

54.1 应用对象概述

为了方便用户配置和管理，防火墙设备中引入了域名对象的概念。在其它功能的配置中，可以引用域名对象来定义配置生效的条件。

应用对象主要包括：

- 自定义域名：需要用户自行配置。
- 域名组：需要用户自行配置，可引用自定义应用。

54.2 配置域名对象

54.2.1 配置自定义域名

自定义域名可配置域名、描述等信息。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	domian-custom NAME	配置自定义域名
步骤3	domian (include|string) STRING	配置自定义域名字符串
步骤4	desc DESC	配置自定义域名描述
步骤5	end	返回特权模式
步骤6	show domian-custum	显示自定义应用配置

使用 no domain 可以取消对自定义域名字符串的设置。

参数说明：

命令（1）：domain-custom NAME

参数	说明	缺省配置
<NAME>	自定义域名的名称	无

命令（2）：domain (include|string) STRING

参数	说明	缺省配置
<include>	包含	无
<string>	完全匹配	无
<STRING>	自定义域名字符串	无

54.2.2 配置域名组

实际使用中，一个策略经常需要引用多个域名对象，将需要引用的域名配置到域名组中，引用该域名组即可。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	domain-group NAME	配置域名组
步骤3	desc DESC	设置域名组描述
步骤4	member domain NAME	引用自定义域名
步骤5	end	返回特权模式
步骤6	show domain-group	显示域名组配置

使用 no member domain NAME 可以删除域名组对自定义域名的引用。

参数说明：

命令（1）：domain- group NAME

参数	说明	缺省配置
<NAME>	域名组的名称	无

命令（2）：member domain NAME

参数	说明	缺省配置
<domain>	引用自定义域名	无
<NAME>	自定义域名的名称	无

54.3 配置案例

54.3.1 添加自定义域名与域名组

案例描述

配置一个自定义域名和一个域名组，并且将这个自定义域名放入域名组里。

配置步骤：

步骤1	创建一个自定义域名
	FW_A(config)# domain-custom c1
步骤2	在这个自定义应用中配置域名字符串
	FW_A(config-domain-custom)#domain include 123
步骤3	创建一个域名组
	FW_A(config)# domain-group g1
步骤4	将自定义域名(c1)添加到这个域名组里
	FW_A(config-domain-group)#member domain c1
步骤5	显示添加信息

```
FW_A(config)# show domain-group g1
 member domain c1
FW_A(config)#
```

配置结果：

```
FW_A# show running-config
domain-custom c1
 domain include 123
!
domain-group g1
 member domain c1
!
```

54.4 自定义域名与域名组监控与维护

54.4.1 查看自定义域名

查看某个自定义域名的步骤：

步骤1	显示某个自定义域名信息

```
FW_A# show domain-custom c1
domain-custom c1                    id:1 ref:3
 desc desc1
 domain include 123
```

c1是自定义名称；desc1是自定义域名描述；123是域名字符串。

54.4.2 查看应用组

查看某个域名组的步骤：

步骤1	显示某个域名组的信息

```
FW_A# show domain-group g1
 domain-group g1
 desc desc1
 member domain qq
```

g1是域名组的名称；desc1是域名组描述；c1是自定义域名的名称。

54.5 常见故障分析

54.5.1 故障现象

现象	执行no domain-custom|domain-group NAME以后，该自定义域名或域名组仍然存在。
分析	当一个自定义域名或域名组正在被引用时，就不能通过no命令删除。
解决	可以先撤销其它配置对该自定义域名或域名组的引用，确定其没有被引用之后再用no命令删除该对象。

60 配置时间对象

55.1 绝对时间和周期时间概述

为了方便用户配置和管理，防火墙设备中引入了时间对象概念，时间对象分为绝对时间和周期时间。在其它功能的配置中，可以引用时间对象来定义配置生效的条件。

绝对时间：配置服务在指定的时间内生效。

周期时间：配置服务在指定的时间范围内在指定的周期（星期一~星期日）执行。

55.1.1 配置在绝对时间中配置有效时间范围

绝对时间中只能配置一个有效时间范围

配置步骤：

步骤1	Configure terminal	进入配置模式
步骤2	schedule onetime NAME	进入名为NAME的绝对时间模式，如果不存在就创建新的时间对象。
步骤3	absolute YY-MM-DD HH:NN:SS YY-MM-DD HH:NN:SS	配置有效时间范围。年、月、日、小时、分钟、秒为一个时间单位，设置时间表的起始和终止时间。

使用 no absolute 删除绝对时间中的有效时间范围。

参数说明：

命令（1）：schedule onetime NAME

参数	说明	缺省配置
<NAME>	时间对象的名称	无

命令（2）：absolute YY-MM-DD HH:NN:SS YY-MM-DD HH:NN:SS

参数	说明	缺省配置
<YY-MM-DD>	时间表起止日期（年，月，日）	无
<HH:NN:SS>	时间表起止时间（时，分，秒）	无
<YY-MM-DD>	时间表终止日期（年，月，日）	无
<HH:NN:SS>	时间表终止时间（时，分，	无

秒）	

55.1.2 配置在周期时间中配置有效时间范围

周期时间中可以定义有效时间范围和有效时间段。有效时间范围只能有一个，而有效时间段可以有多个。有效时间段之间是或的关系，满足其中一个即可；有效时间范围和有效时间段之间是与的关系，都满足才生效。

可以用 absolute 命令向周期时间中添加一个有效时间范围。

配置步骤：

步骤1	Configure terminal	进入配置模式
步骤2	schedule recurring NAME	进入名为NAME的周期时间模式，如果不存在就创建新的时间对象。
步骤3	absolute YY-MM-DD HH:NN:SS YY-MM-DD HH:NN:SS	配置有效时间范围。年、月、日、小时、分钟、秒为一个时间单位，设置时间表的起始和终止时间。
步骤4	show schedule recurring NAME	显示周期表NAME配置信息

参数说明：

命令（1）：schedule recurring NAME

参数	说明	缺省配置
<NAME>	循环时间表名称	无

命令（2）：absolute YY-MM-DD HH:NN:SS YY-MM-DD HH:NN:SS

参数	说明	缺省配置
<YY-MM-DD>	周期表起止日期（年，月，日）	无
<HH:NN:SS>	周期表起止时间（时，分，秒）	无
<YY-MM-DD>	周期表终止日期（年，月，日）	无
<HH:NN:SS>	周期表终止时间（时，分，秒）	无

55.1.3 配置在周期时间中配置有效时间段

可以用 periodic 命令向周期时间中添加多个有效时间段。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	schedule recurring NAME	进入名为NAME的时间对象模式，如果不存在就创建新的时间对象。
步骤3	periodic HH:NN:SS HH:NN:SS (monday|null)…(sunday|null)	配置周期时间段。可配置每天的时间范围，支持离散的星期配置。
步骤4	show schedule recurring NAME	显示周期表NAME配置信息

参数说明：

命令（1）：schedule recurring NAME

参数	说明	缺省配置
<NAME>	周期表名称	无

命令（2）：periodic HH:NN:SS HH:NN:SS (monday|null)…(sunday|null)

参数	说明	缺省配置
<HH:NN:SS >	周期表起止时间（时，分，秒）	无
<HH:NN:SS>	周期表终止时间（时，分，秒）	无
<monday|null>	星期一或者null	无
<tuesday|null>	星期二或者null	无
<wednesday|null>	星期三或者null	无
<.thursday|null>	星期四或者null	无
<friday|null>	星期五或者null	无
<saturday|null>	星期六或者null	无
<sunday|null>	星期日或者null	无

Periodic HH:NN:SS HH:NN:SS (nmonday|null)…(Sunday|null)命令中星期一到星期日必须要填写如果不要设置可以用 null 代替

55.2 配置案例

55.2.1 配置案例:配置时间表

案例描述

配置一个时间对象，其中绝对时间范围从 2007 年 1 月 1 日 0 点到 2007 年 2 月 2 日 0 点，周期时间段是每周六和周日早上 8 点半到下午 5 点半。

配置步骤：

步骤1	创建一个时间表
	USG_A(config)# schedule recurring backup
步骤2	在时间对象中配置有效时间范围
	USG_A(config-tr-obj)# absolute 07-01-01 00:00:00 07-02-02 00:00:00
步骤3	在时间对象中配置时间段
	periodic 08:30:00 17:30:00 null null null null null saturday sunday

配置结果：

UTM# show running-config

schedule recurring backup

absolute 07-01-01 00:00:00 07-02-02 00:00:00

periodic 08:30:00 17:30:00 null null null null null saturday sunday

!

55.3 绝对时间与周期时间监控与维护

55.3.1 查看周期表与绝对时间的步骤：

步骤1	显示某个周期时间表
	USG_A# show schedule recurring backup schedule recurring backup absolute 07-01-01 00:00:00 07-02-02 00:00:00 periodic 08:30:00 17:30:00 null null null null null saturday sunday USG_A# backup是时间表名称;。07-01-01 00:00:00 07-02-02 00:00:00 是绝对时间 08:30:00 17:30:00 null null null null null saturday sunday 是周期时间

55.4 常见故障分析

55.4.1 故障现象1：

现象	执行no schedule recurring NAME以后，该时间表仍然存在。
分析	当一个对象或对象组正在被引用时，就不能通过no命令删除。
解决	可以先撤销其它配置对时间表的引用，确定其没有被引用之后再用no命令删除该节点。

61 配置健康检查

56.1 健康检查概述

健康检查用来对路由下一跳或远端设备进行探测，来获取路由下一跳或远端设备的健康状况。一旦发现链路或设备故障，将不再往该链路上进行流量分担。

支持的健康检查方式包括 ICMP，TCP，UDP，HTTP，HTTPS，RADIUS，LDAP，FTP，POP3，SMTP 等等，除了使用 ICMP 能够对连通性监控外，对具体的服务可以使用相应的检查方式提供更准确的监控。

56.2 配置健康检查模板

可以用 healthcheck 命令添加健康检查模板。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	healthcheck NAME（dns|ftp|http|https|icmp|ldap|mssql|mysql|oracle|pop3|radius|smtp|snmp|tcp|tcphalfopen|udp）	创建健康检查模板，配置需要创建的健康检查类型
步骤3	end	退出到特权模式

通过以上配置可以创建一条最简单的健康检查配置，若需要对健康检查的参数进行配置，在进入健康检查模板后，可参考下表对应参数项进行修改。

参数说明：

ICMP 类型健康检查配置参数：

参数	说明	缺省配置
interval <1-86400>	健康检查发送状态探测包的间隔时间，单位为秒	16
maxretrys <1-10>	健康检查探测包探测失败后的重试次数	3
timeout <1-86400>	发送的健康检查探测包在此时间内如果没有收到回应包，则此次健康检查探测失败，单位为秒。	5
real ip A.B.C.D	用于配置模板检查真实去探测的IP地址，当引用对象的健康状况依赖于	无，默认检查引用对象的地址

	其他IP的主机或链路时填写此项。	
source ip A.B.C.D	指定发送健康检查探测包的源IP地址，当健康检查源IP地址需要指定时填写此项。	无，默认自动选择发送的源IP地址

UDP 类型健康检查配置参数：

参数	说明	缺省配置
interval <1-86400>	健康检查发送状态探测包的间隔时间，单位为秒	16
maxretrys <1-10>	健康检查探测包探测失败后的重试次数	3
timeout <1-86400>	发送的健康检查探测包在此时间内如果没有收到回应包，则此次健康检查探测失败，单位为秒。	5
real ip A.B.C.D	用于配置模板检查真实去探测的IP地址，当引用对象的健康状况依赖于其他IP的主机或链路时填写此项。	无，默认检查引用对象的地址
real port <1-65535>	用于配置模板检查真实去探测的端口。当引用对象的健康状况依赖于其他端口时填写此项，此时覆盖IP必须配置。	无
sendstring LINE	UDP报文中的发送内容	无

TCP 类型健康检查配置参数：

参数	说明	缺省配置
interval <1-86400>	健康检查发送状态探测包的间隔时间，单位为秒	16
maxretrys <1-10>	健康检查探测包探测失败后的重试次数	3
timeout <1-86400>	发送的健康检查探测包在此时间内如果没有收到回应包，则此次健康检查探测失败，单位为秒。	5
real ip A.B.C.D	用于配置模板检查真实去探测的IP地址，当引用对象的健康状况依赖于其他IP的主机或链路时填写此项。	无，默认检查引用对象的地址
real port <1-65535>	用于配置模板检查真实去探测的端口。当引用对象的健康状况依赖	无

	于其他端口时填写此项，此时覆盖IP必须配置。	
sendstring LINE	TCP报文中的发送内容	无
recvstring LINE	接收到报文中应含的内容。当接收到的内容不包含此内容时，状态为DOWN。	无

TCP HALF OPEN 类型健康检查配置参数：

参数	说明	缺省配置
interval <1-86400>	健康检查发送状态探测包的间隔时间，单位为秒	16
maxretrys <1-10>	健康检查探测包探测失败后的重试次数	3
timeout <1-86400>	发送的健康检查探测包在此时间内如果没有收到回应包，则此次健康检查探测失败，单位为秒。	5
real ip A.B.C.D	用于配置模板检查真实去探测的IP地址，当引用对象的健康状况依赖于其他IP的主机或链路时填写此项。	无，默认检查引用对象的地址
real port <1-65535>	用于配置模板检查真实去探测的端口。当引用对象的健康状况依赖于其他端口时填写此项，此时覆盖IP必须配置。	无

同 TCP 类型健康检查相比，TCP HALF OPEN 类型健康检查在设备和服务器之间不建立连接，减少了报文交互。

FTP 类型健康检查配置参数：

参数	说明	缺省配置
interval <1-86400>	健康检查发送状态探测包的间隔时间，单位为秒	16
maxretrys <1-10>	健康检查探测包探测失败后的重试次数	3
timeout <1-86400>	发送的健康检查探测包在此时间内如果没有收到回应包，则此次健康检查探测失败，单位为秒。	5

username USERNAME	FTP认证的用户名	无
password PASSWORD	FTP用户的密码	无
real ip A.B.C.D	用于配置模板检查真实去探测的IP地址，当引用对象的健康状况依赖于其他IP的主机或链路时填写此项。	无，默认检查引用对象的地址
real port <1-65535>	用于配置模板检查真实去探测的端口。当引用对象的健康状况依赖于其他端口时填写此项，此时覆盖IP必须配置。	无

HTTP/HTTPS 类型健康检查配置参数：

参数	说明	缺省配置
interval <1-86400>	健康检查发送状态探测包的间隔时间，单位为秒	16
maxretrys <1-10>	健康检查探测包探测失败后的重试次数	3
timeout <1-86400>	发送的健康检查探测包在此时间内如果没有收到回应包，则此次健康检查探测失败，单位为秒。	5
sendstring LINE	HTTP/HTTPS报文中的发送的请求行。	无
requestbody LINE	HTTP/HTTPS报文中的发送的请求体。	无
recvstring LINE	接收到报文中应含的内容。当接收到的内容不包含此内容时，状态为DOWN。	无
username USERNAME	HTTP/HTTPS认证的用户名。	无
password PASSWORD	HTTP/HTTPS用户的密码。	无
real ip A.B.C.D	用于配置模板检查真实去探测的IP地址，当引用对象的健康状况依赖于其他IP的主机或链路时填写此项。	无，默认检查引用对象的地址
real port <1-65535>	用于配置模板检查真实去探测的端口。当引用对象的健康状况依赖于其他端口时填写此项，此时覆盖IP必须配置。	无

SNMP 类型健康检查配置参数：

参数	说明	缺省配置
interval <1-86400>	健康检查发送状态探测包的间隔时间，单位为秒	16
maxretrys <1-10>	健康检查探测包探测失败后的重试次数	3
timeout <1-86400>	发送的健康检查探测包在此时间内如果没有收到回应包，则此次健康检查探测失败，单位为秒。	5
community COMMUNITY	SNMP代理认证的密码。	public
agent type （UCD|windows）	可以选择UCD(linux)和windows两种类型。	UCD
cpu max <1-100> %	cpu使用率阈值,超过此值认为服务器不可用。	80%
cpu weight <0-255>	cpu,内存，磁盘三者参与负载计算时所占的权重比例。	3
mem max <1-100> %	内存使用率阈值，超过此值认为服务器不可用。	70%
mem weight <0-255>	cpu,内存，磁盘三者参与负载计算时所占的权重比例。	2
disk max <1-100> %	磁盘使用率阈值，超过此值认为服务器不可用。	90%
disk weight <0-255>	cpu,内存，磁盘三者参与负载计算时所占的权重比例。	4

DNS 类型健康检查配置参数：

参数	说明	缺省配置
interval <1-86400>	健康检查发送状态探测包的间隔时间，单位为秒	16
maxretrys <1-10>	健康检查探测包探测失败后的重试次数	3
timeout <1-86400>	发送的健康检查探测包在此时间内如果没有收到回应包，则此次健康检查探测失败，单位为秒。	5
domain DOMAIN_NAME	去DNS服务器上解析的域名。	无
dns-type （a|a6|aaaa|any|cname|h	设置域名记录类型	A

info|mx|ns|ptr|soa|txt）		
recvstring LINE	接收到报文中应含的内容。当接收到的内容不包含此内容时，则此次健康检查失败。	无
real ip A.B.C.D	用于配置模板检查真实去探测的IP地址，当引用对象的健康状况依赖于其他IP的主机或链路时填写此项。	无，默认检查引用对象的地址
real port <1-65535>	用于配置模板检查真实去探测的端口。当引用对象的健康状况依赖于其他端口时填写此项，此时覆盖IP必须配置。	无

RADIUS 类型健康检查配置参数：

参数	说明	缺省配置
interval <1-86400>	健康检查发送状态探测包的间隔时间，单位为秒	16
maxretrys <1-10>	健康检查探测包探测失败后的重试次数	3
timeout <1-86400>	发送的健康检查探测包在此时间内如果没有收到回应包，则此次健康检查探测失败，单位为秒。	5
username USERNAME	RADIUS认证用户名称。	无
password PASSWORD	RADIUS用户密码。	无
secret SECRET	和RADIUS服务器的协商密钥。	无
real ip A.B.C.D	用于配置模板检查真实去探测的IP地址，当引用对象的健康状况依赖于其他IP的主机或链路时填写此项。	无，默认检查引用对象的地址
real port <1-65535>	用于配置模板检查真实去探测的端口。当引用对象的健康状况依赖于其他端口时填写此项，此时覆盖IP必须配置。	无

LDAP 类型健康检查配置参数：

参数	说明	缺省配置
interval <1-86400>	健康检查发送状态探测包的间隔时间，单位为秒	16
maxretrys <1-10>	健康检查探测包探测失败后的重	3

	试次数	
timeout <1-86400>	发送的健康检查探测包在此时间内如果没有收到回应包，则此次健康检查探测失败，单位为秒。	5
username USERNAME	LDAP用户名称。	无
password PASSWORD	LDAP用户密码。	无
real ip A.B.C.D	用于配置模板检查真实去探测的IP地址，当引用对象的健康状况依赖于其他IP的主机或链路时填写此项。	无，默认检查引用对象的地址
real port <1-65535>	用于配置模板检查真实去探测的端口。当引用对象的健康状况依赖于其他端口时填写此项，此时覆盖IP必须配置。	无

SMTP 类型健康检查配置参数：

参数	说明	缺省配置
interval <1-86400>	健康检查发送状态探测包的间隔时间，单位为秒	16
maxretrys <1-10>	健康检查探测包探测失败后的重试次数	3
timeout <1-86400>	发送的健康检查探测包在此时间内如果没有收到回应包，则此次健康检查探测失败，单位为秒。	5
real ip A.B.C.D	用于配置模板检查真实去探测的IP地址，当引用对象的健康状况依赖于其他IP的主机或链路时填写此项。	无，默认检查引用对象的地址
real port <1-65535>	用于配置模板检查真实去探测的端口。当引用对象的健康状况依赖于其他端口时填写此项，此时覆盖IP必须配置。	无

POP3 类型健康检查配置参数：

参数	说明	缺省配置
interval <1-86400>	健康检查发送状态探测包的间隔时间，单位为秒	16
maxretrys <1-10>	健康检查探测包探测失败后的重试次数	3

timeout <1-86400>	发送的健康检查探测包在此时间内如果没有收到回应包，则此次健康检查探测失败，单位为秒。	5
username USERNAME	POP3用户名称。	无
password PASSWORD	POP3用户密码。	无
real ip A.B.C.D	用于配置模板检查真实去探测的IP地址，当引用对象的健康状况依赖于其他IP的主机或链路时填写此项。	无，默认检查引用对象的地址
real port <1-65535>	用于配置模板检查真实去探测的端口。当引用对象的健康状况依赖于其他端口时填写此项，此时覆盖IP必须配置。	无

SMTP 类型健康检查配置参数：

参数	说明	缺省配置
interval <1-86400>	健康检查发送状态探测包的间隔时间，单位为秒	16
maxretrys <1-10>	健康检查探测包探测失败后的重试次数	3
timeout <1-86400>	发送的健康检查探测包在此时间内如果没有收到回应包，则此次健康检查探测失败，单位为秒。	5
real ip A.B.C.D	用于配置模板检查真实去探测的IP地址，当引用对象的健康状况依赖于其他IP的主机或链路时填写此项。	无，默认检查引用对象的地址
real port <1-65535>	用于配置模板检查真实去探测的端口。当引用对象的健康状况依赖于其他端口时填写此项，此时覆盖IP必须配置。	1521

MSSQL 类型健康检查配置参数：

参数	说明	缺省配置
interval <1-86400>	健康检查发送状态探测包的间隔时间，单位为秒	16
maxretrys <1-10>	健康检查探测包探测失败后的重试次数	3
timeout <1-86400>	发送的健康检查探测包在此时间	5

	内如果没有收到回应包，则此次健康检查探测失败，单位为秒。	
real ip A.B.C.D	用于配置模板检查真实去探测的IP地址，当引用对象的健康状况依赖于其他IP的主机或链路时填写此项。	无，默认检查引用对象的地址
real port <1-65535>	用于配置模板检查真实去探测的端口。当引用对象的健康状况依赖于其他端口时填写此项，此时覆盖IP必须配置。	1433

MYSQL 类型健康检查配置参数：

参数	说明	缺省配置
interval <1-86400>	健康检查发送状态探测包的间隔时间，单位为秒	16
maxretrys <1-10>	健康检查探测包探测失败后的重试次数	3
timeout <1-86400>	发送的健康检查探测包在此时间内如果没有收到回应包，则此次健康检查探测失败，单位为秒。	5
real ip A.B.C.D	用于配置模板检查真实去探测的IP地址，当引用对象的健康状况依赖于其他IP的主机或链路时填写此项。	无，默认检查引用对象的地址
real port <1-65535>	用于配置模板检查真实去探测的端口。当引用对象的健康状况依赖于其他端口时填写此项，此时覆盖IP必须配置。	3306

56.3 修改健康检查模板

可以用 healthcheck NAME 命令来修改指定的健康检查模板

配置步骤：

步骤**1**	configure terminal	进入配置模式
步骤**2**	healthcheck NAME（dns|ftp|htp|https|icmp|ldap|mssql|mysql|oracle|pop3|radius|smtp|snmp|tcp|tcphalfopen|udp）	进入名为NAME的健康检查
步骤**3**	interval <1-86400>	修改健康检查发送状态探测包的间隔时间，单位为秒。

步骤4	maxretrys <1-10>	修改健康检查探测包探测失败后的重试次数，单位为秒。
步骤5	timeout <1-86400>	修改发送的健康检查探测包在此时间内如果没有收到回应包，则此次健康检查探测失败，单位为秒。
步骤6	real ip A.B.C.D	修改模板检查真实去探测的IP地址。

56.4 删除健康检查模板

可以用 no healthcheck NAME 命令来修改指定的健康检查模板

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	no healthcheck NAME（dns|ftp|htp|https|icmp|ldap|mssql|mysql|oracle|pop3|radius|smtp|snmp|tcp|tcphalfopen|udp）	删除名为NAME的健康检查，健康检查模板没有被其他模块引用的情况下才可以删除

56.5 配置案例

新建一个 ICMP 类型的健康检查模板，然后在策略路由中引用此模板。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	fw40(config)# healthcheck icmp icmp	添加icmp健康检查模板
步骤3	fw40(config-healthcheck)# exit	退出到配置模式
步骤4	fw40(config)# policy-route 1 any any any any any always rr	创建一条策略路由
步骤5	fw40(config-policy-route)#nexthop 10.1.1.1 10 10 icmp	配置引用icmp健康检查模板

配置结果：

healthcheck icmp icmp

interval 16

maxretrys 3

timeout 5

!

policy-route 1 vlan10 any any any any always rr

policy disable

session-persist disable

nexthop 10.1.1.1 10 10 icmp

56.6 常见故障分析

56.6.1 故障现象

现象	健康检查不成功
分析	当没有路由能够到达要探测的地址时，健康检查报文发送失败。
解决	设备上添加对应的路由。

62 配置 PKI

57.1 PKI协议概述

PKI（公钥基础设施）技术采用证书管理公钥，通过第三方的可信任机构--认证中心 CA(Certificate Authority)，把用户的公钥和用户的其他标识信息（如名称、e-mail、身份证号等）捆绑在一起，在 Internet 网上验证用户的身份。目前，通用的办法是采用建立在 PKI 基础之上的数字证书，通过把要传输的数字信息进行加密和签名，保证信息传输的机密性、真实性、完整性和不可否认性，从而保证信息的安全传输。

设备上的 PKI 本地证书功能是：当设备作为 PKI 客户端时，选择本地证书作为本设备的身份标识，并且验证从其他主机接收到的证书的合法性。这相当于 IE 浏览器中的证书项功能。主要包含三项配置：导入用户证书、导入第三方 CA 证书、导入第三方 CA 的 CRL。这三个功能是相对独立又相互联系，即可以根据具体需要，导入不同的本地证书、不同的 CA 证书、不同的 CRL，但要验证某个终端证书时，需要导入该终端证书的 CA 证书、CRL，以便对该终端证书进行验证。

57.2 配置PKI

对设备所要使用的客户端证书、第三方 CA 证书、第三方 CRL 进行导入导出配置，并且可以生成一个证书请求，向第三方 CA 申请签发。

57.2.1 本地证书的导出

配置本地证书的导出。本地证书根据状态分为两种：本地生成的证书请求和本地证书。导出本地生成的证书请求导出的是证书请求文件；本地证书导出的证书文件。本地证书根据存放位置又分为两种：本地存放和 USBKEY。两种证书都能导出。

配置步骤：

步骤1	由1.2.1所示命令进入PKI配置节点　　进入PKI配置模式
步骤2	certificate local export tftp A.B.C.D CERTIFICATE_NAME

参数说明：

命令（1）：certificate local export tftp A.B.C.D CERTIFICATE_NAME

参数	说明	缺省配置
A.B.C.D	Tftp服务器地址	无

CERTIFICATE_NAME	证书名称	无

57.2.2 PKCS12格式证书的导入

导入 PKCS12 格式的证书。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	certificate local pkcs12 import (local|usb) tftp A.B.C.D CERTIFICATE_NAME [PASSWORD]	导入PKCS12格式的证书。
步骤3	show certificate local [CERTIFICATE_NAME]	显示证书信息

使用 no certificate local CERTIFICATE_NAME，删除由 CERTIFICATE_NAME 指定的证书。

参数说明：

命令（1）：certificate local pkcs12 import (local|usb) tftp A.B.C.D CERTIFICATE_NAME [PASSWORD]

参数	说明	缺省配置
(local|usb)	证书存入的位置：local表示存放在USG设备中；usb表示证书存入USBKEY。	无
A.B.C.D	Tftp服务器地址	无
CERTIFICATE_NAME	证书名称	无
PASSWORD	加密PKCS12文件的密钥	无

57.2.3 证书私钥文件的导入

证书和私钥文件的导入。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	certificate local cert_key import (local|usb) tftp A.B.C.D CERTIFICATE_NAME KEYFILE_NAME [PASSWORD]	导入证书和私钥文件。

步骤3	show certificate local [CERTIFICATE_NAME]	显示证书信息

使用 no certificate local CERTIFICATE_NAME，删除由 CERTIFICATE_NAME 指定的证书。

参数说明：

命令（1）：certificate local cert_key import (local|usb) tftp A.B.C.D CERTIFICATE_NAME KEYFILE_NAME [PASSWORD]

参数	说明	缺省配置
(local|usb)	证书存入的位置：local表示存放在USG设备中；usb表示证书存入USBKEY。	无
A.B.C.D	Tftp服务器地址	无
CERTIFICATE_NAME	证书文件名	无
KEYFILE_NAME	私钥文件名	无
PASSWORD	加密私钥文件的密钥	无

57.2.4 CA证书的导出

CA 证书的导出。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	certificate ca export tftp A.B.C.D CERTIFICATE_NAME	导出CA证书
步骤3	show certificate ca [CERTIFICATE_NAME]	显示证书信息

参数说明：

命令（1）：certificate ca export tftp A.B.C.D CERTIFICATE_NAME

参数	说明	缺省配置
A.B.C.D	Tftp服务地址	无
CERTIFICATE_NAME	CA证书名称	无

57.2.5 CA证书的导入

导入 CA 证书，作为验证从其他终端接收过来的用户证书进行签名验证的依据，该导入的 CA 证书是作为可信证书使用的，必须要保证该 CA 证书的安全性。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	certificate ca import tftp A.B.C.D CERTIFICATE_NAME	导入CA证书。
步骤3	show certificate ca [CERTIFICATE_NAME]	显示证书信息

使用 no certificate ca CERTIFICATE_NAME 删除由 CERTIFICATE_NAME 指定的 CA 证书。

参数说明：

命令（1）：certificate ca import tftp A.B.C.D CERTIFICATE_NAME

参数	说明	缺省配置
A.B.C.D	Tftp服务器地址	无
CERTIFICATE_NAME	证书文件名称	无

57.2.6 CRL的导出

导出 CRL。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	certificate crl export tftp A.B.C.D CERTIFICATE_NAME	导出CRL。
步骤3	show certificate crl [CERTIFICATE_NAME]	显示CRL信息

使用 certificate crl CERTIFICATE_NAME 删除由 CERTIFICATE_NAME 指定的 CRL。

参数说明：

命令（1）：certificate crl export tftp A.B.C.D CERTIFICATE_NAME

参数	说明	缺省配置
A.B.C.D	Tftp服务器地址	无
CERTIFICATE_NAME	CRL名称	无

57.2.7 CRL导入

导入第三方 CA 的 CRL，在对从其他终端接收过来的证书进行验证时，要查找导入的 CRL，从而确定该终端用户证书是否被撤销。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	certificate crl import tftp A.B.C.D CERTIFICATE_NAME	
步骤3	show certificate crl [CERTIFICATE_NAME]	显示CRL信息

使用 no certificate crl CERTIFICATE_NAME 删除由 CERTIFICATE_NAME 指定的 CRL。

参数说明：

命令（1）：certificate crl import tftp A.B.C.D CERTIFICATE_NAME

参数	说明	缺省配置
A.B.C.D	Tftp服务器地址	无
CERTIFICATE_NAME	CRL文件名称	无

57.3 配置案例

57.3.1 配置案例1：导入本地证书

案例描述

本地根据用户的个人信息在页面生成证书请求文件，经 CA 签发后再将该证书导入设备。

配置步骤：

步骤1	导出证书请求
	FW_A# configure terminal FW_A(config)#certificate local export tftp 192.168.31.126 vpn
步骤2	导入经CA签发后的证书
	FW_A# configure terminal FW_A(config)#certificate local cert import tftp 192.168.31.126 vpn.crt
步骤3	查看导入证书的详细信息

```
FW_A#show certificate local vpn
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 44 (0x2c)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=CN, ST=BeiJing, O=Ven, OU=R&D,
CN=zhu/emailAddress=zhu_zhiwei@test.com
        Validity
            Not Before: Jan 24 04:48:38 2008 GMT
            Not After : Jan 23 04:48:38 2009 GMT
        Subject: C=CN, ST=BeiJing, L=BeiJing, O=testTech, OU=R&D,
CN=www.testtech.com.cn/emailAddress=master@testtech.com.cn
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:e3:b6:41:05:8e:52:90:1a:01:97:26:11:6b:91:
                    6b:84:b5:57:c8:3d:4f:8e:7a:af:d9:5d:b1:84:3e:
                    a0:a3:e8:a4:8a:4d:fc:c3:b4:8a:da:9d:e9:ab:83:
                    08:a2:f7:6e:ce:00:76:06:0a:87:2c:86:50:37:95:
                    5c:f1:fd:ee:ce:f6:37:a6:94:dd:f5:17:06:24:4e:
                    7e:49:66:ae:21:a6:f0:f9:39:e0:5d:24:77:1c:67:
                    07:40:b7:f1:78:cb:3c:87:04:29:28:27:65:42:b9:
                    b7:0b:8c:3f:ca:9c:ba:f2:c9:67:29:b5:8c:cd:04:
                    45:18:25:b4:bf:29:2e:ef:3f
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:

08:4C:16:FA:59:38:D9:0E:98:43:4C:37:77:DE:5E:BA:27:C8:B2:67
            X509v3 Authority Key Identifier:

keyid:9D:F5:86:2B:37:4A:DC:4C:E8:F5:0B:01:C0:D2:3D:A5:35:2C:E1:F3

    Signature Algorithm: sha1WithRSAEncryption
        68:2d:4c:20:55:b2:8f:9e:d9:90:31:4b:c9:79:a7:42:2f:72:
        23:ff:08:c1:10:96:b3:86:1f:3c:bd:41:a1:9b:26:fd:23:1e:
        6d:2e:17:03:35:17:92:db:28:63:26:f7:7d:b8:58:e8:01:55:
        3c:0f:3a:e6:2d:1b:79:c1:1a:6f:3d:cf:12:39:59:5d:0e:d4:
        eb:15:d7:12:74:07:40:1e:c4:f4:41:12:06:e3:cb:d4:f1:57:
        0b:74:26:3a:ac:d9:ff:88:53:4c:01:55:03:a7:89:4b:ed:0d:
        06:d5:1d:60:61:ef:bc:4d:45:0b:1a:af:14:03:05:76:5f:03:
        ef:c1
```

配置结果：

57.4 PKI监控与维护

57.4.1 查看本地证书信息

查看本地证书信息步骤：

步骤1	显示PKI本地证书信息

```
FW_A# show certificate local
Name       subject                          location     status       reference
ccccc1111                                   Local        Request      0
testclient C=CN, ST=BJ, L=BJ, O=test, OU=   Local        Certificate  0
pkcs_2     C=CN, ST=BJ, L=BJ, O=test, OU=   Local        Certificate  0
pkcs_3     C=CN, ST=BJ, L=BJ, O=test, OU=   Local        Certificate  0
pkcs_4     C=CN, ST=BJ, L=BJ, O=test, OU=   Local        Certificate  0
pkcs_5     C=CN, ST=BJ, L=BJ, O=test, OU=   Local        Certificate  0
pkcs_6     C=CN, ST=BJ, L=BJ, O=test, OU=   Local        Certificate  0
client     C=CN, ST=bj, L=bj, O=testtech,   Local        Certificate  0
 Total (13) local files, (12) local certificate files, (1) local certificate request file
```

Name表示证书的名称；subject表示证书主题；location表示证书存放的位置：Local表示存放在设备中，USBKEY表示存放在USBKEY中；status表示是证书请求或者是证书。reference表示的是该证书引用的次数，引用次数大于1不能被删除。

步骤2	显示PKI本地某个证书详细信息

```
FW_A# show certificate local client
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number: 1 (0x1)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C=CN, ST=bj, L=bj, O=testtech, OU=testtech,
CN=testca/emailAddress=root@testtech.com
        Validity
            Not Before: Jan 10 09:56:21 2008 GMT
            Not After : Jan  9 09:56:21 2009 GMT
        Subject: C=CN, ST=bj, L=bj, O=testtech, OU=testtech,
CN=usg1/emailAddress=root@testtech.com.cn
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
```

```
                                00:a0:c4:71:1c:d9:d2:6a:03:f4:d1:49:42:31:6c:
                                c5:3c:e9:66:b6:57:7b:e3:d3:2c:a7:4e:ad:3e:99:
                                81:a6:3a:af:c3:80:31:f0:05:dc:6b:f4:20:9e:bf:
                                77:a2:ac:4b:fc:ea:e5:58:47:4e:01:76:4e:04:d3:
                                33:d3:ec:d7:f8:0b:2f:56:9b:24:63:74:0d:17:d1:
                                dc:bc:ef:e2:37:95:29:1b:3a:13:cb:03:38:b7:73:
                                8c:75:f3:3d:8b:c2:4e:b6:88:98:db:b7:f0:42:ac:
                                5a:17:04:0d:8c:06:2d:43:83:11:8b:79:c5:43:d4:
                                5e:2c:00:11:c5:f2:1b:60:6b
                            Exponent: 65537 (0x10001)
                    Signature Algorithm: md5WithRSAEncryption
                        91:c8:97:a4:87:1f:5b:1d:10:9c:19:51:af:a2:d0:da:a7:ec:
                        3f:f4:e8:4b:ce:20:eb:37:3a:bf:39:ed:b9:8e:a0:58:a3:62:
                        59:bb:bb:0c:8a:94:84:4d:95:98:87:0e:29:31:fc:66:28:d1:
                        46:cf:a8:0b:2d:0c:d4:6d:96:78:88:71:9f:83:4b:13:b8:be:
                        42:c5:b7:a7:9d:c3:23:fc:98:50:19:17:bf:79:10:bc:3b:f7:
                        c0:78:9a:e2:60:3d:d6:97:99:1b:88:3a:1b:c9:4f:71:69:b3:
                        09:4f:a2:c8:77:bd:63:bf:8e:ac:9e:0b:3b:90:4f:11:6f:48:
                        8e:3d
```

57.4.2 查看CA证书信息

查看 CA 证书信息的步骤：

步骤1	察看CA证书信息
	FW_A# Name subject CA_Cert_1 C=cn, ST=beijing, L=haidian, O=testtech, OU=testca, CN=test, CA_Cert_2 C=cn, ST=beijing, L=haidian, O=testtech, OU=testca, CN=test, CA_Cert_3 C=cn, ST=beijing, L=haidian, O=testtech, OU=testca, CN=test, CA_Cert_4 C=cn, ST=beijing, L=haidian, O=testtech, OU=testca, CN=test, CA_Cert_5 C=cn, ST=beijing, L=haidian, O=testtech, OU=testca, CN=test, CA_Cert_6 C=cn, ST=beijing, L=haidian, O=testtech, OU=testca, CN=test, Total (6) CA certificate files Name表示CA证书的名称；subject表示证书的主题。
步骤1	察看CA某个证书详细信息
	FW_A# show certificate ca CA_Cert_1 Certificate: Data: Version: 3 (0x2) Serial Number: 0 (0x0)

Signature Algorithm: md5WithRSAEncryption

Issuer: C=cn, ST=beijing, L=haidian, O=testtech, OU=testca, CN=test/emailAddress=testca@testtech.com.cn

Validity

Not Before: Dec 13 05:58:40 2007 GMT

Not After : Dec 10 05:58:40 2017 GMT

Subject: C=cn, ST=beijing, L=haidian, O=testtech, OU=testca, CN=test/emailAddress=testca@testtech.com.cn

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (1024 bit)

Modulus (1024 bit):

00:bd:8e:24:09:4f:34:23:51:84:4b:ef:36:4c:02:
ec:93:bb:37:29:c6:97:a0:0e:13:1d:e9:9b:cf:b7:
34:8e:b7:5b:5c:52:79:41:a5:fb:1b:1f:a8:3d:e7:
89:87:75:12:1e:44:8f:bc:10:c6:f9:87:b0:d5:59:
9e:f4:46:24:d9:1e:0a:e2:98:7c:47:9d:bd:85:f7:
be:0c:11:ab:b8:1c:63:7d:18:07:bb:af:38:7b:cc:
f6:4e:e3:08:82:82:be:42:6b:95:0f:c2:d6:81:73:
3b:54:22:3c:13:24:16:f3:ab:77:90:d8:52:6c:f9:
97:cd:06:8f:80:77:0b:59:09

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Subject Key Identifier:

B2:A3:71:FF:4F:E3:FE:42:2D:3E:46:7C:FE:F6:17:1E:F2:94:C1:2D

X509v3 Authority Key Identifier:

keyid:B2:A3:71:FF:4F:E3:FE:42:2D:3E:46:7C:FE:F6:17:1E:F2:94:C1:2D

DirName:/C=cn/ST=beijing/L=haidian/O=testtech/OU=testca/CN=test/emailAddress=testca@testtech.com.cn

serial:00

X509v3 Basic Constraints:

CA:TRUE

Signature Algorithm: md5WithRSAEncryption

51:22:95:d5:aa:fe:c3:f0:eb:d6:20:c2:46:fe:02:38:d1:a9:
1b:ec:4d:a1:20:fa:41:66:42:b7:c7:56:ae:f0:ba:3f:19:a9:
d4:3e:4b:d4:a2:85:c6:48:95:4e:11:e5:1a:e8:33:c1:c9:4b:
2d:95:79:ef:84:07:52:66:38:a4:e6:c6:af:0f:1e:4a:bc:05:
77:7e:11:26:29:d8:8f:86:23:b5:2a:5c:6a:ff:f0:d6:15:55:

```
ac:af:a8:00:ec:2a:9a:2a:c3:72:41:68:5f:ff:11:2e:fd:b7:
f0:35:07:18:9e:42:f5:b6:01:76:fc:38:e7:90:92:2a:d0:ba:
ef:d1
```

57.4.3 查看CRL信息

查看 CRL 信息的步骤：

步骤1 察看CRL信息

```
FW_A# Name                    issuer
CRL_1          /C=CN/ST=jilin/L=changchun/O=CNC/OU=CNCCA/CN=CHINA
NETCOM CLASS
CRL_2          /C=CN/ST=jilin/L=changchun/O=CNC/OU=CNCCA/CN=CHINA
NETCOM CLASS
CRL_3          /C=CN/ST=jilin/L=changchun/O=CNC/OU=CNCCA/CN=CHINA
NETCOM CLASS
CRL_4          /C=CN/ST=jilin/L=changchun/O=CNC/OU=CNCCA/CN=CHINA
NETCOM CLASS
CRL_5          /C=CN/ST=jilin/L=changchun/O=CNC/OU=CNCCA/CN=CHINA
NETCOM CLASS
  Total (5) CRL    files
```

步骤1 察看某个CRL详细信息

```
Certificate Revocation List (CRL):
        Version 2 (0x1)
        Signature Algorithm: md5WithRSAEncryption
        Issuer:
/C=CN/ST=jilin/L=changchun/O=CNC/OU=CNCCA/CN=CHINA        NETCOM
CLASS1 CA
        Last Update: Dec 19 22:00:01 2007 GMT
        Next Update: Dec 20 22:00:01 2007 GMT
        CRL extensions:
            X509v3 CRL Number:
                1
            X509v3 Authority Key Identifier:

keyid:C1:83:B3:82:87:1A:3B:6C:19:3E:35:4E:23:D8:9B:75:44:67:96:E4

Revoked Certificates:
    Serial Number: 24E0
        Revocation Date: Aug 14 06:42:53 2006 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
```

```
                Certificate Hold
        Serial Number: 246F
            Revocation Date: Aug 14 06:54:11 2006 GMT
            CRL entry extensions:
                X509v3 CRL Reason Code:
                    Certificate Hold
        Serial Number: 2281
            Revocation Date: Aug 14 09:10:00 2006 GMT
            CRL entry extensions:
                X509v3 CRL Reason Code:
                    Key Compromise
        Serial Number: 2281
            Revocation Date: Aug 14 09:10:00 2006 GMT
            CRL entry extensions:
                X509v3 CRL Reason Code:
                    Key Compromise
        Serial Number: 24B5
            Revocation Date: Aug 14 09:38:46 2006 GMT
            CRL entry extensions:
                X509v3 CRL Reason Code:
                    Key Compromise
        Serial Number: 24B5
            Revocation Date: Aug 14 09:38:46 2006 GMT
            CRL entry extensions:
                X509v3 CRL Reason Code:
                    Key Compromise
        Serial Number: 24B5
            Revocation Date: Aug 14 09:40:50 2006 GMT
            CRL entry extensions:
                X509v3 CRL Reason Code:
                    Key Compromise
```

57.5 常见故障分析

57.5.1 故障现象1：导入USBKEY的证书无法通过验证

现象	导入USBKEY的证书使用中无法通过验证
分析	1. 写入USBKEY失败。 2. 证书中的publicExponent和USBKEY设定的publicExponent不一致。

	3. 写入的modulus和privateExponent长度不一致。 4. 写入的modulus和私钥文件中的modulus不一致
解决	1. 重新写入 USBKEY。 2. 设备中生成的公司钥对使用的 publicExponent 为 65537。应该和 USBKEY 中使用的 publicExponent 一致。 3. 写入的 modulus 和 privateExponent 长度一致 4. 写入的 modulus 与私钥文件中的 modulus、证书中的 modulus 要一致。

63 配置 PKI CA

58.1 PKI协议概述

CA 即证书管理机构，受委托发放数字证书的第三方组织或公司。数字证书是用来建立数字签名和公-私(public-private)密钥对的。CA 在这个过程中所起的作用就是保证获得这一独特证书的人就是被授权者本人。在数据安全和电子商务中，CA 是一个非常重要的组成部分，因为它们确保信息交换各方的身份。

CA 中心提供管理 CA 证书、签发并管理用户证书、管理 CRL 三大功能。在使用时，首先生成 CA 证书（颁发机构证书），并用该 CA 证书的私钥来为用户证书签名。用户证书可以根据用户的信息（如国家、地区、单位等）生成一个用户证书请求，然后对此请求进行签发，生成一个具有公私钥对的证书，颁发给具体用户，作为该用户的身份标识使用。对有些已经不安全的用户证书可以进行撤销操作，并根据撤销理由生成 CRL，将 CRL 颁发给用户，来作为验证证书是否安全有效的一个依据。

CA 中心的主要用途在于：签发用户证书、签发 CRL，在签发用户证书与 CRL 前，首先要确定 CA 根证书。

58.2 配置PKI CA

配置设备 CA 中心，主要包括配置管理 CA 证书、配置管理用户证书、配置管理 CRL 三个方面。需要注意的是，用户证书与 CRL 都是由 CA 证书（根证书）来签发，因此确定好 CA 证书后，如果没有安全因患（如 CA 私钥泄露）不要轻易改变 CA 证书。

58.2.1 生成CA证书

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	cacenter ca new CERTIFICATE_NAME	配置CA证书。
步骤3	show cacenter ca cacert	显示CA证书信息

参数说明：

参数	说明	缺省配置
CERTIFICATE_NAME	证书请求名称	无

58.2.2 配置证书信息－位置

配置证书的可选信息－位置（城市）。

配置步骤：

步骤1	由1.2.1所示命令进入PKI CA配置节点	进入PKI CA配置模式
步骤2	city CITY_NAME	配置位置（城市）

参数说明：

命令（1）：city CITY_NAME

参数	说明	缺省配置
CITY_NAME	位置（城市）名称	无

注意

只有在启用PKI CA以后才能对PKI CA其他功能作进一步配置。

58.2.3 配置证书信息－国家或地区

配置证书可选信息－国家或地区，使用 GB。

配置步骤：

步骤1	由1.2.1所示命令进入PKI CA配置节点	进入PKI CA配置模式
步骤2	country COUNTRY_NAME	配置国家代码

参数说明：

命令（1）：country COUNTRY_NAME

参数	说明	缺省配置
COUNTRY_NAME	国家或地区名称的两位代码。	

58.2.4 配置证书信息－组织

配置运行 PKI 的接口以及其所属的区域。

配置步骤：

步骤1	由1.2.1所示命令进入PKI CA配置节点	进入PKI CA配置模式
步骤2	organization ORGANIZATION_NAME	配置证书信息组织名称。

参数说明：

命令（1）：organization ORGANIZATION_NAME

参数	说明	缺省配置
ORGANIZATION_NAME	组织名称	无

58.2.5 配置证书信息－州/省

配置证书信息－州/省。

配置步骤：

步骤1	由1.2.1所示命令进入PKI CA配置节点	进入PKI CA配置模式
步骤2	state STATE_NAME	配置证书信息－州/省

参数说明：

命令（1）：state STATE_NAME

参数	说明	缺省配置
STATE_NAME	州/省名称	无

58.2.6 配置证书信息－部门

配置证书信息－部门。

配置步骤：

步骤1	由1.2.1所示命令进入PKI CA配置节点	进入PKI CA配置模式
步骤2	unit UNIT_NAME	配置证书信息－部门

参数说明：

命令（1）：unit UNIT_NAME

参数	说明	缺省配置
UNIT_NAME	部门名称。	

58.2.7 配置证书信息－EMAIL

配置证书信息－EMAIL。

配置步骤：

步骤1	由1.2.1所示命令进入PKI CA配置节点	进入PKI CA配置模式
步骤2	email EMAIL	启用PKI功能并进入PKI配置模式

参数说明：

命令（1）：email EMAIL

参数	说明	缺省配置
EMAIL	EMAIL地址	无

58.2.8 配置证书信息－密钥长度

配置证书信息－密钥长度。

配置步骤：

步骤1	由1.2.1所示命令进入PKI CA配置节点	进入PKI CA配置模式
步骤2	keylength (1024|2048)	启用PKI功能并进入PKI配置模式

参数说明：

命令（1）：keylength (1024|2048)

参数	说明	缺省配置
1024	密钥长度为1024	无
2048	密钥长度为2048	无

58.2.9 配置证书信息－有效期

配置证书信息－有效期。

配置步骤：

步骤1	由1.2.1所示命令进入PKI CA配置节点	进入PKI CA配置模式

步骤2	days DAYS	启用PKI功能并进入PKI配置模式

参数说明：

命令（1）：days DAYS

参数	说明	缺省配置
DAYS	有效期天数	365

58.2.10 CA证书的导出

导出 CA 证书也分为两种格式，一种是 pem 格式，单导出 CA 证书文件。另一种是 pkcs12 格式文件，是将证书与密钥打包在一起导出。需要注意的是，导出 CA 证书为 pkcs12 格式时，会将 CA 私钥一同导出，仅做对 CA 证书的备份功能使用，不能给用户使用。给用户使用的 CA 证书要导出为 PEM 格式。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	cacenter ca cacert export tftp A.B.C.D (pem|p12) [PASSWORD]	

参数说明：

命令（1）：cacenter ca cacert export tftp A.B.C.D (pem|p12) [PASSWORD]

参数	说明	缺省配置
A.B.C.D	Tftp服务器地址	无
(pem|p12)	导出ca证书的格式	
PASSWORD	导出为p12格式时的密码	

58.2.11 CA证书导入

导入 CA 证书功能，可以将上级 CA 所颁发的证书导入到设备中去，使设备的 CA 中心作为一个子 CA 来管理用户证书与 CRL。导入 CA 证书分为两种格式：一种是 CA 证书与 CA 私钥打包在一起的 pkcs12 格式的文件；一种是 CA 证书与私钥分开存储，都为 PEM 格式的证书。

从第三方 CA 签发的证书导入 pkcs12 格式：

配置步骤：

步骤1	configure terminal	进入配置模式

步骤2	cacenter ca cacert import pkcs12 tftp A.B.C.D CERTIFICATE_NAME [PASSWORD]	导入第三方CA所签发的pkcs12格式证书，包含了CA私钥
步骤3	show cacenter ca cacert	显示证书信息

参数说明：

命令（1）：cacenter ca cacert import pkcs12 tftp A.B.C.D CERTIFICATE_NAME [PASSWORD]

参数	说明	缺省配置
A.B.C.D	Tftp服务器地址。	无
CERTIFICATE_NAME	证书名称。	无
PASSWORD	Pkcs12格式文件的密码	

从第三方 CA 签发的证书导入 pem 格式：

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	cacenter ca cacert import pem tftp A.B.C.D CERTIFICATE_NAME KEYFILE_NAME [PASSWORD]	导入第三方CA所签发的pem格式证书，证书文件与私钥文件分开
步骤3	show cacenter ca cacert	显示证书信息

参数说明：

命令（1）：cacenter ca cacert import pem tftp A.B.C.D CERTIFICATE_NAME KEYFILE_NAME [PASSWORD]

参数	说明	缺省配置
A.B.C.D	Tftp服务器地址。	无
CERTIFICATE_NAME	证书名称。	无
KEYFILE_NAME	密钥名称	
PASSWORD	密钥文件的密码	

58.2.12 CRL配置

对 CA 中心的 CRL 进行配置管理，并且可以向 CA 用户提供自动下载 CRL 文件功能，同时可以根据配置的 CRL 周期自动更新 CRL。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	cacenter ca crl config period <1-65535> url URL	配置CRL服务

参数说明：

命令（1）：cacenter ca crl config period <1-65535> url URL

参数	说明	缺省配置
<1-65535>	Crl本次更新与下次更新的时间间隔，单位为天	30天
URL	客户端下载CRL的URL	无

CRL 下载 URL，在设备配置了多个 IP 时，可以选择一个，例如：http://192.168.31.27\cacrl.crl，后面的 cacrl.crl 不能改变

58.2.13 CRL的更新

在当前时间更新 CRL 撤销证书列表，会将自上次创建 CRL 后所撤销的证书的序列号、撤销原因更新到 CRL 列表中

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	cacenter ca crl update	更新CRL

58.2.14 CRL的导出

导出 CRL 文件，提供给 CA 的用户使用，判断所要验证证书是否已经被撤销。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	cacenter ca crl export tftp A.B.C.D	导出CRL

参数说明：

命令（1）：cacenter ca crl export tftp A.B.C.D

参数	说明	缺省配置
A.B.C.D	Tftp服务地址	无

58.2.15 签发用户证书请求

在创建用户证书时，首先要创建一个用户证书请求（生成请求文件及公私密钥对），然后用 CA 证书对该用户请求签发，生成一个用户可用的证书。生成证书后，可以对证书进行撤销、删除、导出、查看操作。

生成的用户证书时要对其进行签名，签名所用的为 CA 私钥，因此在签发用户证书时，一定要确保 CA 证书与私钥已经存在。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	cacenter ca sign NAME days DAYS password PASSWORD	签发用户证书
步骤3	show cacenter certificate NAME	显示用户证书信息

参数说明：

命令（1）：cacenter ca sign NAME days DAYS password PASSWORD

参数	说明	缺省配置
NAME	已经生成的请求的名字	无
DAYS	有效期天数	无
PASSWORD	打包成pkcs12文件的密码	

58.2.16 撤销用户证书

如果用户证书因为种种原因如私钥泄露等而不能保证其安全性，需要将用户证书进行撤销，撤销后，在进行 CRL 更新时，会将该用户证书的序列号与撤销原因保存到 CRL 中

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	cacenter ca revoke NAME REASON	
步骤3	show cacenter ca certificate	查看用户证书信息

参数说明：

命令（1）：cacenter ca revoke NAME REASON

参数	说明	缺省配置
NAME	要撤销的证书名称	无
REASON	撤销原因	无

58.2.17 导出用户证书

导出用户证书，可以将导出的用户证书拷贝到用户终端，作为用户的身份标识

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	cacenter ca certificate export tftp A.B.C.D CERTIFICATE_NAME	

参数说明：

命令（1）：cacenter ca certificate export tftp A.B.C.D CERTIFICATE_NAME

参数	说明	缺省配置
A.B.C.D	Tftp服务器地址	无
CERTIFICATE_NAME	用户证书名称	无

58.3 配置案例

58.3.1 生成用户证书

案例描述：

某公司有财务部、人力资源部、市场部三个部门，此三个部门要通过 SSL VPN 或者 IPSec 访问公司的 USG 设备，这种情况下，就需要三标识三个部门的用户证书与 CA 证书。

配置步骤

首先，要生成该公司的 CA 证书，填写该公司的名称、位置、国家、电子邮件等信息，同时也要填写希望生成的 CA 证书的有效期、密钥长度等信息。生成 CA 证书后，要创建该公司财务部证书请求，填写财务部通用信息，然后对该证书请求进行签发，最后导出到用户终端供用户使用。

步骤1	configure terminal	进入配置模式
步骤2	host(config)# cacenter ca cacert new	配置CA根证书名称为ABCcomp

	ABCcomp	
步骤3	host(config-cacert)# city BeiJing host(config-cacert)# keylength 1024 host(config-cacert)# country CN host(config-cacert)# days 365 host(config-cacert)# unit Final host(config-cacert)# exit	配置CA证书城市为BeiJing，密钥长度为1024，国家为CN，有效期为365天，部门为Final，执行exit命令后，CA证书创建完毕
步骤4	host(config)# cacenter ca request FinanceCert	创建用户证书请求FinaceCert
步骤5	host(config-request)# country CN host(config-request)# city BeiJing host(config-request)# keylength 1024 host(config-request)# unit Finance host(config-request)# exit	配置用户证书国家CN，城市BeiJing，密钥长度1024，部门 Finace，执行exit命令用户证书请求创建完毕
步骤6	host(config)# cacenter ca sign FinanceCert days 365 password 111111	签发该用户证书请求，有效期是365天，密码是111111
步骤7	host(config)# cacenter ca certificate export tftp 192.168.31.27 FinaceCert	将证书FinaceCert导出到tftp服务器中
步骤8		管理员可以将导出的用户证书拷贝到用户终端，作为用户身份标识

58.3.2 撤销用户证书

案例描述：

假如财务部按照以上步骤所生成的证书不慎将私钥泄露，因而造成财务部用户证书不能继续使用，这时需要撤销该用户证书，以免发生信息泄露等不安全事件。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	host(config)# cacenter ca revoke FinaceCert reason keyCompromise	撤销生成的财务部证书FinaceCert，撤销原因是keyCompromise
步骤3	host(config)# vpn ca crl update	更新CRL列表
步骤4	host(config)# cacenter ca crl export tftp 192.168.31.27	导出CRL列表文件到tftp服务器192.168.31.27中
步骤8		更新并导出CRL文件，将该CRL文件导入给公司的USG设备，同时拷贝给其他各部门主机，这些部门的主机应该将该CRL文件导入到IE等客户端程序，这样，在整个公司内，财务部的证书就已经撤销，如果有人冒用财务部证书，不

	会被验证通过，保证了公司通信的安全

58.4 常见故障分析

现象	导入CA证书时，提示导入证书错误
分析	导致这种错误提示的原因是：证书密码错误、证书公私钥不配对
解决	输入证书的正确密码，并保证所导入证书的公私钥配对性

64 配置日志

59.1 配置系统日志概述

防火墙设备上的日志展示一共分为七大类，包括系统事件、审计事件、VPN 事件、配置审计、SDWAN 事件、流事件和安全事件。本设备支持标准的 SYSLOG 格式，包括本地日志，以及 E-mail 日志，提供给用户掌握系统运行状况的方法。

59.2 配置说明

59.2.1 缺省配置信息

内容	缺省设置	备注
本地日志（memory）	关闭	可更改设置
E-Mail日志（email）	关闭	可更改设置
SYSLOG服务器状态（enable/disable）	disable	可更改设置
SYSLOG服务端口（port）	514	可更改设置

59.2.2 配置本地日志

本地日志，系统将各模块的日志信息记录到设备日志文件中。

59.2.3 配置模块发送日志到本地日志

配置步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	"log(antiarp|app|attack|bgp| blacklist| config|dhcp|filter|flood|ha|hm| if-info|nat|ospf|qos|rip|scan|server|se ssionpolicy|system-info|url|vrrp|war ningevent) memory upto (emergencies| alerts| critical|errors|warnings|notifications| informational)"	每个模块，每个位置对应一个优先级。最低级别为informational；

使用 "no log(antiarp|app|attack|bgp| blacklist|config|dhcp|filter|flood|ha|hm| if-info|nat|ospf|qos|rip|scan|server|sessionpolicy|system-info|url|vrrp|warningevent)", 删除对应模块的所有日志配置。

59.2.4 清除本地日志

该命令将清除本地所有日志信息

配置步骤：

步骤1	clear log memory	清除本地日志

59.2.5 配置模块发送日志到E-mail

配置步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	"log(antiarp|app|attack|bgp| blacklist| config|dhcp|filter|flood|ha|hm| if-info|nat|ospf|qos|rip|scan|server|sessionpolicy|system-info|url|vrrp|warningevent) email upto (emergencies| alerts| critical|errors|warnings)"	每个模块，每个位置对应一个优先级。最低级别为warnings。

使用 "no log(antiarp|app|attack|bgp| blacklist|config|dhcp|filter|flood|ha|hm| if-info|nat|ospf|qos|rip|scan|server|sessionpolicy|system-info|url|vrrp|warningevent)", 删除对应模块的所有日志配置。

59.2.6 配置添加SYSLOG日志服务器

SYSLOG 日志,，系统将各模块的日志信息按配置发送到 SYSLOG 服务器，最多可以配置 8 个 syslog 服务器。

配置步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	log server addr A.B.C.D port<1-65535> enable	添加syslog服务器并启用

使用 log server addr A.B.C.D port<1-65535> disable 命令关闭 SYSLOG 服务器。

59.2.7 配置删除SYSLOG服务器

配置步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	no log server addr A.B.C.D	删除syslog服务器

59.2.8 配置模块发送日志到SYSLOG服务器

配置步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	"log(antiarp|app|attack|bgp| blacklist| config|dhcp|filter|flood|ha|hm| if-info|nat|ospf|qos|rip|scan|server|se ssionpolicy|system-info|url|vrrp|war ningevent) server upto (emergencies| alerts| critical|errors|warnings|notifications| informational)"	每个模块，每个位置对应一个优先级。最低级别为informational。

使用 "no log(antiarp|app|attack|bgp| blacklist|config|dhcp|filter|flood|ha|hm| if-info|nat|ospf|qos|rip|scan|server|sessionpolicy|system-info|url|vrrp|warni ngevent)", 删除对应模块的所有日志配置。

59.3 配置案例

59.3.1 配置案例1: 配置本地日志

案例描述：

配置接口模块通知级别日志到本地日志。

配置步骤：

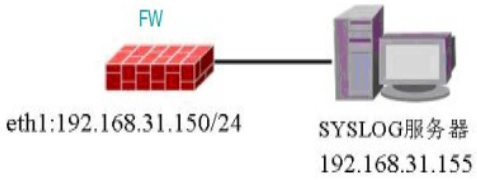
步骤1	配置接口模块内存日志等级
	FW# config terminal FW(config)# log if-info memory upto notifications FW(config)#exit
步骤2	查看配置
	FW#show log-config log if-info memory upto notifications !

59.3.2 配置案例2: 配置SYSLOG日志

案例描述：

配置 DHCP 模块信息级别日志到 SYSLOG 日志。

案例组网图：



配置步骤：

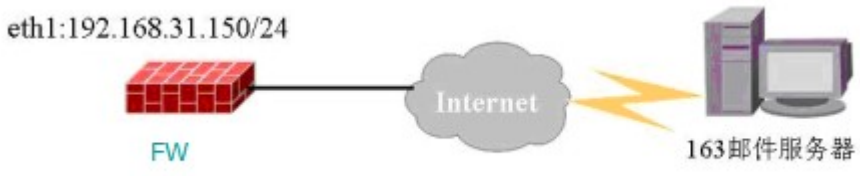
步骤1	配置DHCP模块SYSLOG日志等级
	FW# config terminal FW(config)# log dhcp server upto informational
步骤2	配置SYSLOG服务器参数
	FW(config)# log server addr 192.168.31.155 port 514 enable
步骤3	查看配置
	FW# show log-config log dhcp server upto informational log server addr 192.168.31.155 port 514 enable !

59.3.3 配置案例3: 配置E-mail日志

案例描述：

配置系统运行模块告警级别日志发送到 E-mail。

案例组网图：



配置步骤：

步骤1	配置系统运行信息模块SYSLOG日志等级

	FW# config terminal FW(config)# log run-info email upto warnings
步骤2	配置Email参数
	FW(config)# smtp-config FW(smtp-config)# server smtp.163.com FW(smtp-config)# sender david@163.com FW(smtp-config)# receiver1 jackey@163.com FW(smtp-config)# receiver2 poll@163.com FW(smtp-config)# auth enable FW(smtp-config)# username david FW(smtp-config)# passwd davidqpmz FW(smtp-config)# exit FW(config)# exit
步骤3	查看配置
	FW# show log-config log run-info email upto warnings ! FW# show smtp-config ! smtp-config server smtp.163.com sender david@163.com receiver1 jackey@163.com receiver2 poll@163.com username david passwd davidqpmz auth enable

59.4 常见故障分析

59.4.1 故障现象1：SYLOG日志失效。

现象	在SYSLOG服务器上看不到对应模块日志
分析	1）是否正确配置SYLOG服务器的地址和端口号 2）是否指定模块的日志类别和等级到SYSLOG Server
解决	1）正确配置SYSLOG服务器的地址和端口号 2）指定模块的日志类别和等级到SYSLOG Server

59.4.2 故障现象2：E-mail日志失效。

现象	没有收到对应模块信息的邮件
分析	1）是否正确配置Email配置参数 2）是否指定模块的日志类别和等级到Email日志
解决	1）正确配置Email配置参数 2）指定模块的日志类别和等级到Email日志

65 配置日志合并

60.1 日志合并概述

防火墙设备上的日志展示一共分为四大类，包括系统事件、审计事件、配置审计和安全事件。有些模块在短时间内会产生大量相同的日志，不利于用户去查看，对此，对此类日志可以按源 IP 与目的 IP 进行合并。

可以进行合并的日志包括：流量控制，防 DOS 攻击，防火墙策略，防扫描，防 flood 攻击，本地安全策略以及黑名单。合并周期默认 60 秒。

60.2 配置说明

60.2.1 缺省配置信息

内容	缺省设置	备注
合并周期	60秒	可更改设置
日志合并开关	关闭	可更改设置
日志合并数量	5000	可更改设置

60.2.2 配置日志合并

配置步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	log merge enable	配置日志合并全局开关
步骤3	log qos|attack|blacklist|filter|local-policy|flood|scan merge option OPTION	配置日志合并，合并方式option为sip或dip

使用 "no log qos|attack|blacklist|filter|local-policy|flood|scan merge option OPTION删除对应模块的日志合并配置。

使用 log merge disable关闭日志合并全局开关。

60.2.3 配置日志合并周期

合并周期默认 60 秒。

配置步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	log merge time <10-600>	配置日志合并周期

60.2.4 配置日志合并数量

默认日志合并数量 5000.

配置步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	log merge number <500-5000>	配置日志合并数量

60.2.5 配置日志总开关

配置步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	log merge all on|off	日志合并全部开启或关闭

60.2.6 日志合并调试

步骤1	debug syslog merge	查看日志合并信息
步骤2	debug syslog merge count	查看日志合并的次数

60.3 常见故障分析

60.3.1 故障现象1：日志没有进行合并。

现象	配置防护墙策略基于源IP方式合并，在本地未看到产生合并类型的日志
分析	1）未达到日志合并周期查看日志内容。 2）当前上报的日志为该源IP第一次匹配策略时上报的日志。 3）待合并的日志源IP、策略ID、策略动作三者存在一项不相同。
解决	1）配置日志合并后，合并日志是按照合并周期上报，等待周期事件后才会看到合并日志。 2）源IP第一次匹配策略时，会直接发出，不会记录日志合并，只有当这个源IP周期内再次匹配策略才会产生合并日志，日志内容为该源IP第一次匹配策略时的内容。 3）若策略存在策略ID、策略动作时，则需要策略ID和策略动作也相同才会进行日志合并。

66 流日志

61.1 流日志概述

为了方便快速查看一条数据流经过设备时的详细处理信息，流日志整合了若干模块（包括流管理、NAT 转换、防火墙策略、av、ips、威胁情报以及流量控制）的日志信息，在这条数据流拆除的时候，生成一条日志上报。设备针对长连接，会每隔 5 分钟上报一次。

61.1.1 流日志全局开关

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	ct-log (enable|disable)	开启/关闭流日志功能。

使用 show ct-log 查看开关状态。

61.1.2 流日志过滤开关

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	log conntrack (memory| server| email) upto (emergencies|alerts|critical| errors|warnings|notifications |informational)	开启流日志过滤开关，流日志级别是信息。

使用 show log-config 可以查看过滤开关开启状态。

67 配置系统

系统维护包括系统时间设置，E-mail 设置，系统相关配置的备份恢复，系统升级，诊断以及集中管理配置。

62.1 系统时间设置

62.1.1 查看系统连续运行的时间

查看步骤：

步骤1	查看系统连续运行的时间
	FW# show system uptime current time : Mon Apr 2 10:14:44 2007 system runtime : 4 minutes 表示当前时间是上午10:14，系统运行已经4分钟。

62.1.2 查看系统当前的日期和时间

查看步骤：

步骤1	查看系统当前的日期和时间
	FW# show date ABS time :1197539979 UTC time :2007-12-13 09:59:39 Local time :2007-12-13 17:59:39 UTC time表示系统当前UTC时间, Local time表示系统当前本地时间

62.1.3 查看系统当前的时区

查看步骤：

步骤1	查看系统当前的时区
	FW# show timezone timezone 57 表示当前时区为第57时区(即CST,中国时区)。

62.1.4 配置系统当前的时区

配置步骤：

步骤1	配置系统当前的时区
	FW(config)# timezone 57 表示配置当前时区为第57时区(即CST,中国时区)。

时区参数对应如下：

1 zone1=GMT-12:00 日界线西

2 zone2=GMT-11:00 中途岛 萨摩亚群岛

3 zone3=GMT-10:00 夏威夷

4 zone4=GMT-09:00 阿拉斯加

5 zone5=GMT-08:00 太平洋时间(美国和加拿大) 蒂华纳

6 zone6=GMT-07:00 山地时间(美国和加拿大)

7 zone7=GMT-07:00 亚利桑那

8 zone8=GMT-07:00 齐瓦瓦 拉巴斯 马扎特兰

9 zone9=GMT-06:00 萨斯喀彻温

10 zone10=GMT-06:00 中部时间(美国和加拿大)

11 zone11=GMT-06:00 中美州

12 zone12=GMT-06:00 瓜达拉哈拉 墨西哥城 蒙特雷

13 zone13=GMT-05:00 波哥大 利马 基多

14 zone14=GMT-05:00 东部时间(美国和加拿大)

15 zone15=GMT-05:00 印第安那州(东部)

16 zone16=GMT-04:00 大西洋时间(美国和加拿大)

17 zone17=GMT-04:00 加拉加斯 拉巴斯

18 zone18=GMT-04:00 圣地亚哥

19 zone19=GMT-03:30 纽芬兰

20 zone20=GMT-03:00 巴西利亚

21 zone21=GMT-03:00 布宜诺斯艾利斯 乔治敦

22 zone22=GMT-03:00 格陵兰

23 zone23=GMT-02:00 中大西洋

24 zone24=GMT-01:00 佛得角群岛

25 zone25=GMT-01:00 亚速尔群岛

26 zone26=GMT 格林威治 都柏林 爱丁堡 伦敦 里斯本

27 zone27=GMT 卡萨布兰卡 蒙罗维亚

28 zone28=GMT+01:00 阿姆斯特丹 柏林 伯尔尼 罗马 斯德哥尔摩 维也纳
29 zone29=GMT+01:00 贝尔格莱德 布拉迪斯拉发 布达佩斯 卢布尔雅那
30 zone30=GMT+01:00 布鲁塞尔 哥本哈根 马德里 巴黎
31 zone31=GMT+01:00 萨拉热窝 斯科普里 华沙 萨格勒布
32 zone32=GMT+01:00 中非西部
33 zone33=GMT+02:00 布加勒斯特
34 zone34=GMT+02:00 哈拉雷 比勒陀利亚
35 zone35=GMT+02:00 赫尔辛基 基辅 里加 索非亚 塔林 维尔纽斯
36 zone36=GMT+02:00 开罗
37 zone37=GMT+02:00 雅典 贝鲁特 伊斯坦布尔 明斯克
38 zone38=GMT+02:00 耶路撒冷
39 zone39=GMT+03:00 巴格达
40 zone40=GMT+03:00 科威特 利雅得
41 zone41=GMT+03:00 莫斯科 圣彼得堡 伏尔加格勒
42 zone42=GMT+03:00 内罗毕
43 zone43=GMT+03:30 德黑兰
44 zone44=GMT+04:00 阿布扎比 马斯喀特
45 zone45=GMT+04:00 巴库 第比利斯 埃里温
46 zone46=GMT+04:30 喀布尔
47 zone47=GMT+05:00 叶卡捷琳堡
48 zone48=GMT+05:00 伊斯兰堡 卡拉奇 塔什干
49 zone49=GMT+05:30 马德拉斯 孟买 加尔各答 新德里
50 zone50=GMT+05:45 加德满都
51 zone51=GMT+06:00 阿拉木图 新西伯利亚
52 zone52=GMT+06:00 阿斯塔纳 达卡
53 zone53=GMT+06:00 斯里哈亚华登尼普拉
54 zone54=GMT+06:30 仰光
55 zone55=GMT+07:00 克拉斯诺亚尔斯克
56 zone56=GMT+07:00 曼谷 河内 雅加达
57 zone57=GMT+08:00 北京 重庆 乌鲁木齐 香港特别行政区
58 zone58=GMT+08:00 吉隆坡 新加坡
59 zone59=GMT+08:00 珀斯
60 zone60=GMT+08:00 台北
61 zone61=GMT+08:00 伊尔库茨克 乌兰巴图

62 zone62=GMT+09:00 大阪 东京 札幌

63 zone63=GMT+09:00 汉城

64 zone64=GMT+09:00 雅库次克

65 zone65=GMT+09:30 阿德莱德

66 zone66=GMT+09:30 达尔文

67 zone67=GMT+10:00 布里斯班

68 zone68=GMT+10:00 符拉迪沃斯托克

69 zone69=GMT+10:00 关岛 莫尔兹比港

70 zone70=GMT+10:00 霍巴特

71 zone71=GMT+10:00 堪培拉 墨尔本 悉尼

72 zone72=GMT+11:00 马加丹 所罗门群岛 新喀里多尼亚

73 zone73=GMT+12:00 奥克兰 惠灵顿

74 zone74=GMT+12:00 斐济 堪察加半岛 马绍尔群岛

75 zone75=GMT+13:00 努库阿洛法

62.1.5 手动设置系统当前的日期和时间

命令说明：date <2006-2030> <1-12> <1-31> <0-23> <0-59> <0-59>

关键字和参数	说明
<2006-2030>	配置年份
<1-12>	配置月份
<1-31>	配置日
<0-23>	配置小时
<0-59>	配置分钟
<0-59>	配置秒

配置步骤：

步骤1	设置系统当前的日期和时间
	FW# date 2007 04 02 10 20 50
	表示设置系统时间为2007年4月2日上午10点20分50秒

62.1.6 使用ntp设置系统当前的时间

配置步骤：

步骤1	配置ntp server地址及loop间隔
	FW(config)# ntp 192.168.31.155 6
	表示配置ntp server地址为192.168.31.155, ntp loop间隔为6分钟

使用 no ntp 命令可以停止 ntp 配置。

查看步骤：

步骤1	显示ntp配置
	FW# show ntp info timezone 57 ntp master 192.168.31.155 6

62.1.7 使用ntp立即更新系统时间

步骤1	通过ntp立即更新系统时间
	FW# ntpupdate time.windows.com time update success

62.1.8 配置ntp认证密钥

配置步骤：

步骤1	配置ntp认证密钥标识及密钥密文
	FW(config)# ntp authkey key-id <keyid> key-type MD5 secret <SECRET> 表示配置ntp认证密钥的标识为keyid，密钥类型为MD5，密钥密文为SECRET

使用 no ntp authkey key-id <1-65535>命令可以删除由指定的 key-id 标识的 ntp 认证密钥。

查看步骤：

步骤1	显示ntp认证密钥配置
	FW # show ntp keys key-id 20 key-type MD5 secret HuIeRvajTTWy201E+Qi2GAeo+iih63U9aGPC/Ymnh+MUGo17j4YWr4ZGPPq Op0m length 5 ref 1

62.1.9 使用带认证的ntp设置系统当前的时间

配置步骤：

步骤1	配置主用ntp server地址、loop间隔及认证密钥标识
	FW(config)# ntp 192.168.31.155 60 key-id 20 表示配置首选ntp server地址为192.168.31.155, ntp loop间隔为60分钟，使用标识为20的ntp密钥进行认证。

使用 no ntp 命令可以停止主用 ntp 配置。

步骤2	配置备用ntp server地址、loop间隔及认证密钥标识
	FW(config)# ntp backup 192.168.31.160 60 key-id 20 表示配置备用ntp server地址为192.168.31.160, ntp loop间隔为60分钟，使用标识为20的ntp密钥进行认证。

使用 no ntp backup 192.168.31.160 key-id 20 命令可以删除地址为 192.168.31.160 使用密钥标识为 20 认证的备用 ntp 服务器配置。

62.2 E-mail设置

62.2.1 配置SMTP服务器名称或者地址

步骤	执行命令	说明
1	configure terminal	进入全局配置模式
2	smtp-config	进入SMTP配置模式
3	server NAME	配置服务器的名字或者IP
4	server address	配置服务器的名字或者IP
5	server port	配置服务器端口

使用 no server 可以删除 SMTP 服务器配置。

62.2.2 配置邮件发送者邮件地址

步骤	执行命令	说明
1	configure terminal	进入全局配置模式
2	smtp-config	进入SMTP配置模式
3	sender NAME	配置邮件发送者的地址
4	Send-interval <1-60>	发送时间间隔

使用 no sender 取消配置。

62.2.3 配置邮件接收者邮件地址

步骤	执行命令	说明
1	configure terminal	进入全局配置模式
2	smtp-config	进入SMTP配置模式
3	receiver1LONGSTRING	配置邮件接收者的地址。多个接收者地址需要使用分号“;”隔开，最多可以输入255的字符。

使用 no receiver1 取消配置。

62.2.4 配置发送邮件时是否需要认证

步骤	执行命令	说明
1	configure terminal	进入全局配置模式
2	smtp-config	进入SMTP配置模式
3	auth enable	配置邮件发送时需要认证

使用 auth disable 取消发送邮件时需要认证的配置。

62.2.5 配置发送邮件时认证使用的用户名

步骤	执行命令	说明
1	configure terminal	进入全局配置模式
2	smtp-config	进入SMTP配置模式
3	username NAME	配置邮件发送时认证使用的用户名

使用 no username 取消邮件发送时认证使用的用户名的配置。

62.2.6 配置发送邮件时认证使用的密码

步骤	执行命令	说明
1	configure terminal	进入全局配置模式
2	smtp-config	进入SMTP配置模式
3	passwd PASSWORD	配置邮件发送时认证使用的密码

使用 no passwd 取消邮件发送时认证使用的密码。

62.2.7 配置SSL加密

步骤	执行命令	说明
1	configure terminal	进入全局配置模式
2	smtp-config	进入SMTP配置模式
3	ssl enable	启用ssl加密

使用 ssl disable 取消 ssl 加密。

62.3 设备运行记录

62.3.1 设备运行记录概述

设备运行记录包括：设备运行记录配置、设备运行记录日志文件导出、系统运行记录导出。主要用于对设备运行的健康状态进行记录。

设备运行记录配置：用于对设备运行记录功能进行配置，以便形成设备运行记录日志。

设备运行记录日志文件导出：日志中记录设备的一些实时信息，包括版本信息、接口信息、流量信息等。用户可以选择性的导出日志，并导出压缩包文件。

系统运行记录导出：导出系统运行记录文件加密压缩包。

由于命令行无法导出文件，因此，只能对设备运行记录功能进行配置操作。

62.3.2 配置设备运行记录

配置步骤：

步骤	configure terminal	进入配置模式
步骤2	stated enable	设备运行记录功能使能
步骤3	stated disable	设备运行记录功能去使能
步骤4	stated interval <TIME>	配置信息记录间隔
步骤5	stated retention <DAYS>	配置日志文件保存天数

参数说明：

命令（1）：stated interval <TIME>

参数	说明	缺省配置
<TIME>	时间间隔<60-86400>	300秒

命令（2）：stated retention <DAYS>

参数	说明	缺省配置
<DAYS>	记录天数<1-7>	3天

62.3.3 配置案例

案例描述

配置设备信息记录功能，记录间隔为 60s，记录天数为 4 天。

配置步骤：

步骤1	host(config)# stated enable	使能设备信息记录功能

步骤2	host(config)# stated interval 60	修改记录间隔为60s
步骤3	host(config)# stated retention 4	修改记录天数为4天

配置结果：

host# show stated

stated enable

stated interval 60

stated retention 4

62.4 密码复杂度

密码复杂度代表了设备密码的强度，分为高、中、低三个级别，高复杂度密码必须包含特殊字符（!@#$%&`,-.）、数字（0-9）、大小写字母，并且密码的长度不得小于 8 位；中复杂度密码必须包含数字与特殊字符，并且密码的长度不得小于 8 位；低复杂度密码只要满足最小长度不低于 8 位。

配置步骤：

步骤**1**	config terminal	进入配置模式
步骤**2**	user password complexity-level<1-3>	配置密码复杂度1高2中3低

62.5 管理员密码长度配置

创建管理员时允许配置最小的密码长度，最小长度不得低于 8 位，最大不高于 63 位。

配置步骤：

步骤**1**	config terminal	进入配置模式
步骤**2**	admin password LENGTH	配置密码长度

62.6 常用系统管理命令

62.6.1 修改Telnet服务端口

修改 Telnet 服务端口：

步骤**1**	server-telnet (default|<1024-65535>)	port	修改Telnet服务端口号，执行该命令后将允许其他机器通过该端口Telnet到设备

62.6.2 修改ssh服务端口

修改 ssh 服务端口：

步骤**1**	server-ssh (default|<1024-65535>)	port	修改ssh服务端口号，执行该命令后将允许其他机器通过该端口ssh到设备

62.6.3 修改ssh服务安全性

修改 Ssh 服务端口：

步骤1	system-security-level (normal|high)	修改ssh服务的安全级别

62.7 集中管理

62.7.1 集中管理概述

集中管理功能是结合集中管理平台使用的，主要应用在设备管理 IP 在私网的环境中。设备自动注册到集中管理平台后，通过集中管理平台就能轻松管理设备了。

62.7.2 集中管理配置步骤

步骤	执行命令	说明
1	configure terminal	进入全局配置模式
2	trpa host A.B.C.D	配置集中管理平台IP
3	trpa if INTERFACE	配置集中管理接口
4	trpa key STRING	配置集中管理平台密钥
5	trpa enable	开启自动注册到集中管理平台

62.7.3 其他命令行说明

序号	执行命令	说明
1	trpa port <1-65535>	配置集中管理平台端口，默认443
2	trpa keepalive-period < 1-65535 >	发送保活报文间隔，默认600秒
3	trpa method (http |https)	设备注册时支持的协议（http或者https），默认https
5	trpa disable	关闭自动注册到集中管理平台

62.8 配置自动备份

62.8.1 配置自动备份概述

配置自动备份可以具体按每周或者每月定期备份当前配置文件，防止设备因异常导致配置文件丢失，设备最多可以备份 32 份配置文件，其中无硬盘设备备份的配置文件大小不能超过 10M，总配置文件大小不能超过 10M。

62.8.2 自动保存配置步骤

步骤	执行命令	说明
1	configure terminal	进入全局配置模式
2	config-auto-save (enable|disable)	开启配置自动备份开关
3	config-auto-save weekly (sun|null)(mon|null)(tue|null)(wed|null)(thu|null)(fri|null)(sat|null)	配置自动备份时间按每周保存
4	config-auto-save monthly <1-31>	配置自动备份时间按每月保存
5	config-auto-save time hour <0-23> minute <0-59>	配置自动备份时间具体时分

使用 no config-auto-save weekly 取消每周配置自动备份；

使用 no config-auto-save monthly 取消每月配置自动备份；

使用 no config-auto-save time 取消配置自动备份具体时分。

62.8.3 自动保存配置案例

设备按每月 1 号晚上 22:30 备份配置文件：

步骤	执行命令
1	configure terminal
2	config-auto-save enable
3	config-auto-save monthly 1
5	config-auto-save time hour 22 minute 30

62.9 命令行超时时间配置

在命令行无操作的情况下，超过该设置的时间，登录用户会自动退出。缺省为 10 分钟。

步骤	执行命令	说明
1	configure terminal	进入全局配置模式
2	vtysh timeout <1-480>	配置命令行超时时间

可以使用 no vtysh timeout 取消命令行超时时间配置。

68 配置管理员用户

本章涉及管理员用户以及用户组的配置。叙述了怎样配置管理用户以及用户组的配置。

63.1 配置管理员

防火墙设备出厂的默认配置包括一个超级管理员用户 admin，使用这个帐号，可以登录设备对设备进行配置，包括配置其它的管理员。每个管理员都有它的管理地址，以及管理权限和描述，权限是通过权限表来限制的。下面一一列举怎样进行配置。下列各项配置，如未特别说明，均指特权模式下的操作。

63.1.1 配置用户权限表

权限表是在配置管理员用户的时候使用到的。每个管理员会对应一个管理员权限表，该管理员只具有管理员权限表中规定的权限。配置步骤如下

配置用户权限表的步骤:

步骤1	configure terminal	进入全局配置模式
步骤2	authorized-table NAME	如果不存在该权限表，创建一个，并进入权限表节点，如果存在，直接进入权限表节点
步骤3	authorized (read|write) (all|system-config|log-configt|admin-user| updata|log-read|reboot|updata)	设置权限表的读写权限

参数说明：

参数	说明	缺省配置
read	表示后面的参数说明的是读权限。	无
write	表示后面的参数说明的是写权限。	无
all	表示所有功能都打开	无
system-config	具有系统配置的权限，系统配置具有下面六种权限规定以外的所有权限，且具有对象管理的权限。	无
log-config	具有日志操作的权限。	无
admin-user	具有管理员用户，授权表，在线信息的操作权限。	无
Log-read	具有日志访问权限。	无

updata	具有升级的操作权限。	无

63.1.2 配置本地用户

本地管理员用户是指用户的信息保存在防火墙设备上。配置步骤如下

配置本地用户的步骤:

步骤1	user administrator USER local PASSWORD authorized-table NAME [disable]	创建或者修改本地管理员用户的密码以及管理权限表，并可以通过disable选项使该用户暂时无效。

63.1.3 配置RADIUS管理员用户

RADIUS 管理员用户是指用户的信息保存在 RADIUS 服务器上。用户认证需要通过 RADIUS 服务器认证。配置步骤如下

配置 RADIUS 管理员用户的步骤:

步骤1	user administrator USER radius SERVER authorized-table NAME [disable]	创建或者修改RADIUS管理员对应的RADIUS服务器以及管理权限表，并可以通过disable选项使该用户暂时无效。

63.1.4 配置LDAP管理员用户

LDAP 管理员用户是指用户的信息保存在 LDAP 服务器上。用户认证需要通过 LDAP 服务器认证。配置步骤如下

配置 RADIUS 管理员用户的步骤:

步骤1	user administrator USER ldap SERVER authorized-table NAME [disable]	创建或者修改RADIUS管理员对应的LDAP服务器以及管理权限表，并可以通过disable选项使该用户暂时无效。

63.1.5 配置管理员用户的管理地址

如果需要控制登录用户的地址，可以通过配置管理员用户的授权地址来控制用户登录的地址范围。如果没有配置该地址，那么可以通过任意的 IP 地址登录。配置步骤如下：

配置管理员用户的授权地址的步骤:

步骤1	user administrator USER authorized-address (first|second|third) A.B.C.D/M	可以配置三个授权地址，该用户可以通过任意一个地址登录

管理地址也可以是网段地址：

配置管理员用户的授权地址的步骤:

步骤1	user administrator USER authorized-address (first|second|third)	可以配置三个授权地址段，该用户可以通过任意一个地址段内的地址登录

	A.B.C.D/M

参数说明：

参数	说明	缺省配置
first	表示第一个授权地址	
second	表示第二个授权地址	
third	表示第三个授权地址	

三个授权地址没有先后顺序，只是为了区分。

63.1.6 配置管理员最短口令长度

配置管理员用户的最短口令长度的步骤:

步骤1	admin password	LENGTH	管理员用户的最短口令长度

参数说明：

参数	说明	缺省配置
LENGTH	最短口令长度	6

63.2 配置信息显示命令

配置信息显示命令列表

命令	解释
show admin-user	显示当前已添加的管理员用户信息
show running-config	显示当前配置。

show local user 命令显示举例:

步骤1 在线管理员用户的显示举例:

```
FW# who
Login style     Username    IP
Console         admin       *                Mon Apr  9 10:17:19
SSH             admin       192.168.31.117   Mon Apr  9 10:21:17
Telnet          admin       192.168.31.117   Mon Apr  9 10:21:32
```

63.3 配置案例

63.3.1 配置管理员用户的权限表功能

案例描述：

配置防火墙，添加两个管理员用户 check 和 admin，其中 check 的权限表是

show-config，admin 的权限表是 system-config。Show-config 具有显示功能的权限，而 admin 具有读写所有模块的权限。结果：

用户 check 只能使用 show 命令，不能进入 CONFIG 节点；

用户 admin 可以使用系统中所有命令。

图 63-1 配置管理员用户授权功能

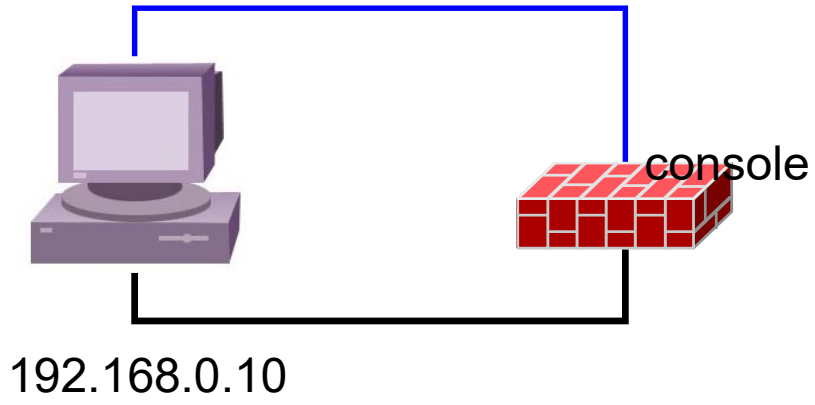


图 4-1

配置步骤：

步骤1	添加授权表
	FW# configure terminal FW(config)# authorized-table reader FW(authorized-table)# authorized read all FW(authorized-table)# exit FW(config)# FW# configure terminal FW(config)# authorized-table system-config FW(authorized-table)# authorized read all FW(authorized-table)# authorized write all FW(authorized-table)# exit FW(config)#
步骤2	添加管理员用户
	FW# configure terminal FW(config)# user administrator check local testtech authorized-table reader FW(config)# user administrator admin local testtech authorized-table system-config
步骤3	设置用户管理地址
	FW(config)# user administrator check authorized-address first 192.168.0.10

步骤4	保存配置
	FW (config)# write memory

案例达到的效果如下：

以 check 用户登录

Username: check

Password:

FW> en

FW# show admin-user

Admin User Name	User Type	User Status
admin	local	enable
check	local	enable

Total users : 2

FW# configure terminal

This user is not permited this operation

FW#

以上可以看出，当我们以 check 用户登录时，只能查看信息，但是不能进入 config 节点进行配置。

如果用户不是通过 192.168.0.10 登录设备的，会提示非法地址的错误，不让登录。

以 admin 用户登录

Username: admin

Password:

FW> en

FW# show admin-user

Admin User Name	User Type	User Status
admin	local	enable
check	local	enable

Total users : 2

FW# configure terminal

FW(config)#

以上可以看出，当我们以 admin 用户登录时，能够进入 config 节点进行配置。

63.4 故障分析

63.4.1 用户无法登录

故障现象	存在该用户，但使用这个用户名无法登录
分析与解决	1）该用户是否是管理员用户 2）是否对该用户名限制登录的IP地址范围 3）该用户是否处于封禁状态，如果是使用user administrator check local testtech authorized-table Reader 类似的命令启用。 4）用户密码存在问题，请使用user administrator check local testtech authorized-table Reader 指令重设一遍用户密码。

63.4.2 命令无法执行

故障现象	用户能够登录，但是不能执行命令
分析与解决	通过show running-config查看配置，查看用户对应的权限表中是否有对应的权限

69 配置版本管理

64.1 系统升级和相关配置备份恢复

64.1.1 手动升级及配置恢复

命令说明：**copy tftp A.B.C.D RemoteFile** (version |config |license |applib|avlib|ipslib|urllib|waflib)

关键字和参数	说明
tftp	表示采用tftp协议传输文件
A.B.C.D	表示tftp server地址
RemoteFile	表示在tftp server上该文件名
(version |config |license |applib|avlib|ipslib|urllib|waflib)	version ：表示更新软件版本 config ：表示更新系统配置文件 license ：表示更新 License 文件 applib ：表示更新应用特征库 avlib ：表示更新病毒防护特征库 ipslib ：表示更新入侵防护特征库 urllib ：表示更新 URL 分类特征库 waflib ：表示更新 WEB 应用防护特征库

命令说明：write (file|memory|terminal|backup-config|startup-config)

关键字和参数	说明
(file|memory|terminal|backup-config |startup-config)	File ：表示保存当前配置 Memory：表示缓存当前配置 Terminal：表示显示当前配置 Backup-config：表示备份当前配置 Startup-config：表示保存当前配置

64.1.2 特征库自动升级配置

步骤1	进入特征库自动升级配置模式
	FW_A(config)# auto-update (app-lib|av-lib|ips-lib|url-lib|waf-lib) FW_A(auto-update)#

步骤2	配置升级服务器
	FW_A(auto-update)# server http://192.168.1.1/update/update.asp
步骤3	配置按星期几升级
	FW_A(auto-update)# weekly sun mon null wed null fri null 表示每星期日/星期一/星期三/星期五升级
步骤4	或者配置按每月几号升级
	FW_A(auto-update)# monthly 10,20,30 表示每月10号,20号,和30号升级
步骤5	配置升级时间
	FW_A(auto-update)# time hour 3 minute 0 表示该天凌晨3点整升级
步骤6	启用自动升级配置
	FW_A(auto-update)# update enable
步骤7	关闭自动升级配置
	FW_A(auto-update)# update disable

64.1.3 系统快照

命令说明：system snapshot (auto| delete| manual| recover| show)

关键字和参数	说明
system snapshot	系统快照的命令
(auto| delete| manual| recover| show)	auto ：表示自动快照 delete ：表示删除快照 manua ：表示手动快照 recover ：表示恢复快照 show ：表示显示快照

命令	参数	说明
system snapshot auto disable		关闭自动快照开关
system snapshot auto enable		打开自动快照开关
system snapshot auto monthly	<day> <hour> <minute>	设置每月自动快照时间,<day>取值范围1-31,<hour>取值范围0-23,<minute>取值范围0-59
system snapshot auto weekly	<day> <hour> <minute>	设置每周自动快照时间, <day>取值范围1-7,<hour>取值范围0-23,<minute>取值范围0-59。
system snapshot delete	<name>	删除快照，<name>是快照的名字
system snapshot manua	<remark>	手动创建快照，< remark >是快照的备注
system snapshot recover	<name>	恢复快照，<name>是快照的名字
system snapshot show all		显示存在的快照

system snapshot show info		显示当前快照信息

64.2 系统升级案例

64.2.1 手动升级系统版本

步骤1	进入enable模式，从本地下载系统版本文件
	FW_A# copy tftp 4.4.4.10 tsos.bin version FW_A# tsos.bin 100% |**********| 72196k 0:00:00 ETA Download finish, begin to purse and install version file tsos.bin. success. FW_A#
步骤2	重启设备
	FW_A# reboot The system will be rebooted! Please enter "y/n" to confirm: y

64.2.2 手动升级应用特征库版本

步骤1	进入enable模式，从本地下载应用特征库版本文件
	FW_A# copy tftp 4.4.4.10 20160728.sig applib 20160728.sig 100% |**********| 511k 0:00:00 ETA Download finish, begin to purse and install version file 20160728.sig. success. FW_A#

64.2.3 系统快照

手动创建快照

步骤1	在config节点下，手动创建系统快照，备注名为123，可以修改
	host(config)# system snapshot manual 123 It will take some time. Please wait..... host(config)# system snapshot show all name remark V200R0400B20210517_20210608080931 123

自动创建快照操作

步骤1	在config节点下，设置自动系统快照，设置时间是每周1的2点03分自动快照

	host(config)# system snapshot auto enable Please set weekly or monthly. host(config)# system snapshot auto weekly 1 2 3 host(config)# system snapshot show info CURRENT INFO: The current system is not a snapshot system. AUTO INFO: week:1 hour:2 minute:3

删除快照操作

步骤1	在config节点下，显示存在的系统快照
	host(config)# system snapshot show all name remark V200R0400B20210517_20210608080931 123
步骤2	删除存在的快照
	host(config)# system snapshot delete V200R0400B20210517_20210608080931 host(config)# system snapshot show all name remark host(config)#

恢复快照操作

步骤1	在config节点下，显示存在的系统快照
	host(config)# system snapshot show all name remark V200R0400B20210517_20210608082913 456
步骤2	选择一个要恢复系统快照
	host(config)# system snapshot recover V200R0400B20210517_20210608082913 Restore the system snapshot, the system will automatically reboot! Please enter "y/n" to confirm: y system_snapshot:Restore system snapshot successfully! The system is going down NOW!

70 VRRP

65.1 VRRP概述

通常，同一网段内的所有主机都设置一条相同的以网关为下一跳的缺省路由。主机发往其他网段的报文将通过缺省路由发往网关，再由网关进行转发，从而实现主机与外部网络的通信。当网关发生故障时，本网段内所有以网关为缺省路由的主机将无法与外部网络通信。

缺省路由为用户的配置操作提供了方便，但是对缺省网关设备提出了很高的稳定性要求。增加出口网关是提高系统可靠性的常见方法，此时如何在多个出口之间进行选路就成为需要解决的问题。

VRRP（Virtual Router Redundancy Protocol，虚拟路由器冗余协议）将可以承担网关功能的路由器加入到备份组中，形成一台虚拟路由器，由 VRRP 的选举机制决定哪台路由器承担转发任务，局域网内的主机只需将虚拟路由器配置为缺省网关。

VRRP 是一种容错协议，在提高可靠性的同时，简化了主机的配置。在具有多播或广播能力的局域网（如以太网）中，借助 VRRP 能在某台设备出现故障时仍然提供高可靠的缺省链路，有效避免单一链路发生故障后网络中断的问题，而无需修改动态路由协议、路由发现协议等配置信息。

65.2 配置VRRP

65.2.1 设置VRRP备份组的描述

设置一个 VRRP 备份组的描述信息。

步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface ge0/0	进入接口配置模式
步骤3	vrrp 1 description DESC	找到或创建组号为1的虚拟路由器，并设置描述信息

参数说明：

参数	说明	缺省配置
vrid	备份组号	无
description	描述信息	无

65.2.2 取消VRRP备份组的描述

将一个 VRRP 备份组的描述清空。

步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface ge0/0	进入接口配置模式
步骤3	no vrrp 1 description	找到组号为1的虚拟路由器，取消描述

参数说明：

参数	说明	缺省配置
vrid	备份组号	无

65.2.3 向VRRP备份组增加一个虚拟IP

增加一个虚拟 IP 到 VRRP 备份组。

步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface ge0/0	进入接口配置模式
步骤3	vrrp 1 ip 192.168.31.1	找到或创建组号为1的虚拟路由器，将一个虚拟IP增加到备份组

参数说明：

参数	说明	缺省配置
vrid	备份组号	无
ip	虚拟IP地址	无

注意

虚拟 IP 地址不能为全零地址(0.0.0.0)、广播地址(255.255.255.255)、环回地址、非 A/B/C 类地址和其它非法 IP 地址(如 0.0.0.1)。

65.2.4 从VRRP备份组删除一个虚拟IP

删除一个备份组的虚拟 IP。

步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface ge0/0	进入接口配置模式
步骤3	no vrrp 1 ip 192.168.31.1	找到组号为1的虚拟路由器，删除一个ip

参数说明：

参数	说明	缺省配置
vrid	备份组号	无
ip	虚拟IP地址	无

65.2.5 设置VRRP备份组的优先级

设置一个 VRRP 备份组的优先级。

步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface ge0/0	进入接口配置模式
步骤3	vrrp 1 priority 120	找到或创建组号为1的虚拟路由器，并设置优先级

参数说明：

参数	说明	缺省配置
vrid	备份组号	无
priority	优先级	100

65.2.6 恢复VRRP备份组的缺省优先级

恢复一个 VRRP 备份组的缺省优先级 100。

步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface ge0/0	进入接口配置模式
步骤3	no vrrp 1 priority	找到组号为1的虚拟路由器，并恢复优先级为100

参数说明：

参数	说明	缺省配置
vrid	备份组号	无

65.2.7 启用VRRP备份组的抢占模式

启用一个 VRRP 备份组的抢占模式。

步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface ge0/0	进入接口配置模式
步骤3	vrrp 1 preempt delay 10	找到或创建组号为1的虚拟路由器，启用抢占模式并把延迟设置为10秒

参数说明：

参数	说明	缺省配置
vrid	备份组号	无
preempt delay	抢占延迟	0

65.2.8 禁用VRRP备份组的抢占模式

禁用一个 VRRP 备份组的抢占模式。

步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface ge0/0	进入接口配置模式
步骤3	no vrrp 1 preempt	找到为1的虚拟路由器，禁用抢占

参数说明：

参数	说明	缺省配置
vrid	备份组号	无

65.2.9 设置VRRP备份组的版本模式

设置一个 VRRP 备份组的版本模式。

步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface ge0/0	进入接口配置模式
步骤3	vrrp 1 version v3	找到或创建组号为1的虚拟路由器，并设置版本模式

参数说明：

参数	说明	缺省配置
vrid	备份组号	无
version	版本模式	v2

65.2.10 恢复VRRP备份组的缺省版本模式

恢复一个 VRRP 备份组的缺省版本模式。

步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface ge0/0	进入接口配置模式
步骤3	no vrrp 1 version	找到组号为1的虚拟路由器，恢复版本呢模式为v2

参数说明：

参数	说明	缺省配置
vrid	备份组号	无

65.2.11 设置VRRP备份组的认证模式

设置一个 VRRP 备份组的认证模式。

步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface ge0/0	进入接口配置模式
步骤3	vrrp 1 authentication md5 KEY	找到或创建组号为1的虚拟路由器，并设置md5认证模式和认证字

参数说明：

参数	说明	缺省配置
vrid	备份组号	无
authentication	认证模式	无

65.2.12 取消VRRP备份组的认证

取消一个 VRRP 备份组的认证。

步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface ge0/0	进入接口配置模式
步骤3	no vrrp 1 authentication	找到组号为1的虚拟路由器，并取消认证

参数说明：

参数	说明	缺省配置
vrid	备份组号	无

65.2.13 设置VRRP备份组的通告时间间隔

设置一个 VRRP 备份组的通告时间间隔。

步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface ge0/0	进入接口配置模式
步骤3	vrrp 1 timers advertise 200	找到或创建组号为1的虚拟路由器，并设置通告时间间隔，单位亚秒

参数说明：

参数	说明	缺省配置
vrid	备份组号	无
timers advertise	通告时间间隔	100

65.2.14 恢复VRRP备份组的缺省通告时间间隔

恢复一个 VRRP 备份组的通告时间间隔。

步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface ge0/0	进入接口配置模式
步骤3	no vrrp 1 timers advertise	找到组号为1的虚拟路由器，并恢复通告时间间隔为100

参数说明：

参数	说明	缺省配置
vrid	备份组号	无

65.2.15 启用VRRP备份组的虚拟IP 可Ping

启用一个 VRRP 备份组的虚拟 IP 可 Ping。

步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface ge0/0	进入接口配置模式
步骤3	vrrp 1 ping	找到或创建组号为1的虚拟路由器，并启用Ping

参数说明：

参数	说明	缺省配置
vrid	备份组号	无

65.2.16 禁用VRRP备份组的虚拟IP可Ping

禁用一个 VRRP 备份组的虚拟 IP 可 Ping。

步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface ge0/0	进入接口配置模式
步骤3	no vrrp 1 ping	找到组号为1的虚拟路由器，并禁用Ping

参数说明：

参数	说明	缺省配置
vrid	备份组号	无

65.2.17 启用VRRP备份组

启用一个 VRRP 备份组。

步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface ge0/0	进入接口配置模式
步骤3	vrrp 1 enable	找到组号为1的虚拟路由器，并启用

参数说明：

参数	说明	缺省配置
vrid	备份组号	无

65.2.18 禁用VRRP备份组

禁用一个 VRRP 备份组。

步骤：

步骤1	configure terminal	进入全局配置模式
步骤2	interface ge0/0	进入接口配置模式
步骤3	no vrrp 1 enable	找到组号为1的虚拟路由器，并禁用

参数说明：

参数	说明	缺省配置
vrid	备份组号	无

65.3 配置案例

案例描述

在接口 ge0/0 下，建立一个组号为 1，虚拟 IP 为 192.168.31.1，简单字符串认证，通告时间间隔为 2 秒的备份组。

配置步骤：

步骤1	进入congfig模式
	FW# configure terminal
步骤2	进入接口
	FW (config)# interface ge0/0
步骤3	建立虚拟IP为192.168.31.1的备份组1
	FW (config-ge0)#vrrp 1 ip 192.168.31.1
步骤4	配置备份组1为简单字符串认证模式，认证字为123
	FW (config-ge0)# vrrp 1 authentication text 123
步骤5	修改备份组1的通告时间间隔为2秒（200亚秒）
	FW (config-ge0)# vrrp 1 timers advertise 200
步骤6	启用备份组1
	FW (config-ge0)# vrrp 1 enable

65.4 监控与维护

65.4.1 查看VRRP配置

步骤：

步骤1	显示VRRP配置信息
	FW_A# show vrrp ge0-Group 1 Enabled State is Master Using VRRP protocol is version 2 Virtual IP address is 192.168.31.1 Virtual MAC address is 00:00:5E:00:01:01 Advertisement interval is 2.00 seconds Priority is 100

	Preemption enabled Ping disabled Using TEXT authentication, password: 123 Master is 192.168.31.106, priority is 100

65.5 故障分析

65.5.1 故障现象1：

现象	配置好了一个备份组，在启用后一直显示处于“Initialize”状态。
分析	备份组所属接口没有处于UP状态，或者网线没有插好。
解决	备份组所属接口必须满足： 1、 接口处于 UP 状态 2、 接口网线上能检测到载波信号 3、 接口上至少配置了一个真实 IP 地址

71 配置 HA

66.1 HA概述

高可靠性即 HA（High-Availability），是保证网络高可靠的一种技术方案，可防止网络中由于单个防火墙的设备故障或网络故障导致网络中断，保证网络服务的连续性和安全强度。支持两台防火墙设备以主-备或主-主两种工作模式运行，可以满足不同的组网需要。

在主-备工作模式下，只有状态为“主”的防火墙设备转发流量，所有流量都被主设备转发，“备”设备不工作，但保持和“主”同样的配置，同时实时监测“主”设备的运行状态，一旦检测到“主”设备出现故障，比如掉电，设备死机等。“备”设备会自动接管“主”设备承担网络流量的转发工作，以保持网络的不中断运行。

在主-主工作模式下，两台防火墙设备同时转发流量，流量的分配比例取决于相邻网络设备的路由配置，以及防火墙上的相关配置，如浮动 IP 等。在主-主工作模式下，每台设备转发和自己单元 ID 相同的流量。

两台防火墙设备通过用户设置 IP 地址发送心跳报文来检测对端防火墙的工作状态，同时防火墙产品支持另外三个附加因素可选项：“网关监控”，“接口监控”和“链路聚合监控”作为切换条件。正在工作中的防火墙设备，如果检测到自己的监控状态比对端的优先级低，则会主动使自己变为“备”状态，所有流量被另外的防火墙设备接管。在主备工作模式下，具有抢占模式，可以指定主备设备，在正常的情况下，由指定的主备配置决定主备状态。

本章涉及 HA 功能的配置，阐述了如何通过命令行配置 HA，实现 HA 功能。

66.2 配置HA

系统中 HA 的工作模式分为主备和主主模式，都可工作在路由和桥模式下，具有冗余备份，负载分担（需要其他设备分配流量）的功能。目前，只支持两台设备。为了保证切换后设备能正常工作，两台设备的硬件型号必须相同。

66.2.1 配置基本配置

HA 基本配置，用来启用 HA 的基本功能。包括：工作模式、心跳通信地址、抢占模式等等。

配置步骤:

步骤1	configure terminal	进入配置模式
步骤2	ha-group	进入HA配置节点
步骤3	enable (backup-master| master-master)	配置HA工作模式，并启动HA功能。工作模式分为主主和主备
步骤4	primary-failover self A.B.C.D peer A.B.C.D	配置首选通信地址，self为本地ip，peer为对端ip
步骤5	second-failover self A.B.C.D peer A.B.C.D	配置备选通信地址，self为本地ip，peer为对端ip
步骤6	unitID <1-2>	配置单元ID。设备的ID号，用于标识双机模式下的两台设备
步骤7	grob-style (master|backup|disable)	配置抢占模式，分为：抢占主和抢占备。默认不启用
步骤8	ha-time <1-3>	配置心跳发送间隔。取值范围1-3秒，默认配置为3秒
步骤9	float mac (enbale|disable)	配置是否启用浮动MAC

使用 disable 可以取消对步骤 3 的设置。

使用 no primary-failover 可以取消对步骤 4 的设置。

使用 no second-failover 可以取消对步骤 5 的设置。

使用 no ha-time 可以取消对步骤 8 的设置。

注意

1. 两台设备的通信地址必须成对配置，并且不能指定为接口的浮动 IP。
2. 主主模式下，两台设备的单元 ID 必须指定为不同。
3. 主备模式下，两台设备的抢占模式必须成对配置。
4. 两台设备的心跳发送间隔必须配置为相同。

66.2.1 配置配置同步

防火墙设备 HA 功能可实现配置的手动同步和自动同步，当配置完一台设备后，用户可以把本设备上的配置同步到另一台设备上，既减少了用户配置的工作量，又保证了两台设备配置相同。

配置步骤:

步骤1	configure terminal	进入配置模式
步骤2	ha-group	进入HA配置节点
步骤3	config-sync self A.B.C.D peer E.F.G.H	配置同步使用的IP地址，self为本地ip，peer为对端ip

步骤4	autosyn enable	启用自动同步
步骤5	config detect	定时探测对端配置和本地配置是否相同。默认的探测间隔为1分钟

使用 no config-sync 可以取消对步骤 3 的设置

使用 no autosyn enable 可以取消对步骤 5 的设置

使用 no config detect 可以取消对步骤 5 的设置


提示

1. 本地和对端地址可以和 HA 通信地址相同，不能指定为接口的浮动 IP。
2. 指定本地和对端地址后，可以在 HA 监控页面进行手动同步配置。
3. 启用实时监测同步状态后，可以在 HA 监控页面查看检测结果。
4. 两台设备中，只要有一台启用实时监测即可。
5. 配置同步功能，不会同步 HA 本身的配置，VRRP，动态路由，以及网络配置→接口、网络配置→设备 IP 相关的配置。
6. 自动同步和实时监测同步状态不能同时开启

66.2.2 配置连接同步

连接同步包括四层流同步，为了保证故障切换时，已经建立的连接不中断，就必须进行连接同步。

配置步骤:

步骤1	configure terminal	进入配置模式
步骤2	ha-group	进入HA配置节点
步骤3	mirroring-address self A.B.C.D peer E.F.G.H [alternate]	连接同步使用的IP地址，self为本地ip，peer为对端ip
步骤4	sync connection	启用连接同步
步骤5	fdb backup (enable | disable)	桥模式下，启用fdb的自动同步

使用 no mirroring-address [alternate] 可以取消对步骤 3 的设置

使用 no sync connection 可以取消对步骤 5 的设置

66.2.3 配置监控配置

HA 监控分网关监控、接口监控和链路聚合监控，实时监控设备上的运行状况，当出现监控故障时，会引起设备的状态切换，保证业务不中断。

配置步骤:

步骤1	configure terminal	进入配置模式
步骤2	ha-group	进入HA配置节点
步骤3	sysmon-gw A.B.C.D <1-2> HM	配置网关监控，HM为健康检查模板名称
步骤4	sysmon-interface IF_NAME timeout <0-3600>	配置接口监控
步骤5	sysmon-trunk TRUNK_NAME threshold <0-100>	配置链路聚合监控

使用 no sysmon-gw A.B.C.D 可以取消对步骤 3 的设置。

使用 no sysmon-interface IF_NAME 可以取消对步骤 3 的设置。

使用 no sysmon-trunk TRUNK_NAME 可以取消对步骤 3 的设置。

66.2.4 配置切换条件

HA 切换条件分对象故障数不等于对端时切换（对端需相同配置）、全部对象故障时切换和任意几个对象故障时切换。

配置步骤:

步骤1	configure terminal	进入配置模式
步骤2	ha-group	进入HA配置节点
步骤3	sysmon-switch default	对象故障数不等于对端时切换，设备默认配置。
步骤4	sysmon-switch all-down	全部对象故障时切换
步骤5	sysmon-switch part-down threshold <0-10000>	任意几个对象故障时切换

使用 show sysmon-switch state 可以查看设备当前配置和监控状态。

66.2.5 配置停止/激活HA功能

HA 功能启动后，有时可能想暂停 HA 状态协商的工作，让设备保持各自当前的

HA 状态不变，可用此功能。

配置步骤:

步骤1	configure terminal	进入配置模式
步骤2	ha-group	进入HA配置节点
步骤3	standby	停止HA协商功能

使用 no standby 重新激活 HA 状态协商功能。

注意

此命令只能在主设备上启用，执行后 HA 仍是启动状态，只是暂停了协商切换功能，两台设备维持状态不变。一般很少用到此命令，但比如想更换 ha 口网线时，可以先执行 standby 命令，然后更换网线，完毕后再执行 no standby 激活协商功能，这样可以避免拔掉 ha 口网线时的状态紊乱。只用于 ha 主备。

66.2.6 配置HA状态倒换功能

HA 功能启动后，使用此命令可将 HA 状态手工进行主备间切换，即主设备变成备份设备，备份设备变成主设备。

配置步骤:

步骤1	configure terminal	进入配置模式
步骤2	ha-group	进入HA配置节点
步骤3	swap	配置HA进行HA主备倒换

注意

此命令只能在主设备上启用。如果想更换主设备，或者想把主设备从网络中拿开，则可以先执行 swap 命令，把流量都转向另外一台设备，待原来的主设备变成备份设备后，再进行操作。只用于 ha 主备且没有配置抢占模式情况下。

66.3 配置案例

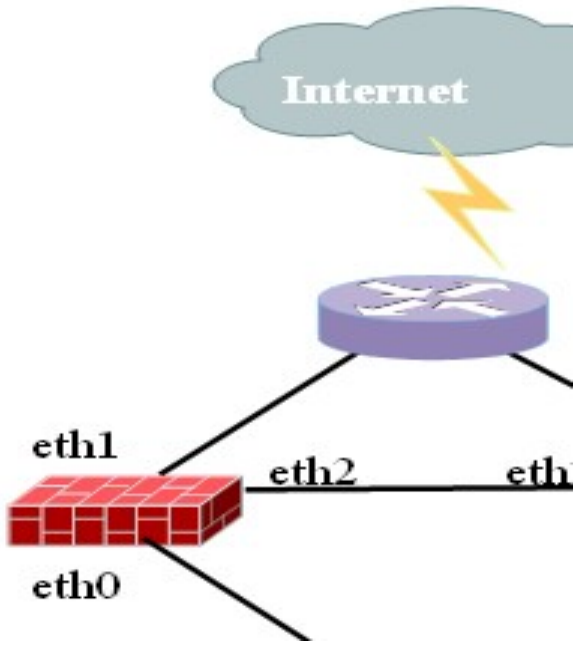
66.3.1 配置案例1：配置主备模式

案例描述：

两台防火墙，分别为 FW_A，FW_B 作为冗余设备，工作在主备模式，实现冗余备份的功能。首先把其中一台设备（假设 FW_A）接入网络，并正确连接好网线，

HA 口网线可以先不连接。连接好网线后，为设备（FW_A）加电启动，然后通过管理界面对设备（FW_A）进行 HA 配置，并启动 HA 功能。然后把另外一台设备（FW_B）加入网络中，并启动 HA 功能。这里假设设备的业务口为 eth0，eth1, HA 通信地址配置在 eth2 上。

案例组网图



配置步骤：

对设备 FW_A 的配置：

步骤1	配置FW_A 的通信地址
	FW_A(config)# ha-group
	FW_A(ha-group)# primary-failover self 3.3.3.3 peer 3.3.3.5
步骤2	配置FW_A的监控接口
	FW_A(ha-group)# sysmon-interface eth0 timeout 3
	FW_A(ha-group)# sysmon-interface eth1 timeout 3
步骤3	配置FW_A的工作模式并启动HA功能
	FW_A(ha-group)# enable backup-master

对设备 FW_B 的配置：

步骤1	配置FW_B 的HA通信地址
	FW_B (config)# ha-group
	FW_B (ha-group)# primary-failover self 3.3.3.5 peer 3.3.3.3
步骤2	配置FW_B的监控接口

	FW_B (ha-group)# sysmon-interface eth0 timeout 3 FW_B (ha-group)# sysmon-interface eth1 timeout 3
步骤3	配置FW_B的工作模式并启动HA功能，且开启浮动MAC
	FW_B (ha-group)# enable backup-master FW_B (ha-group)# float mac enbale

配置结果：

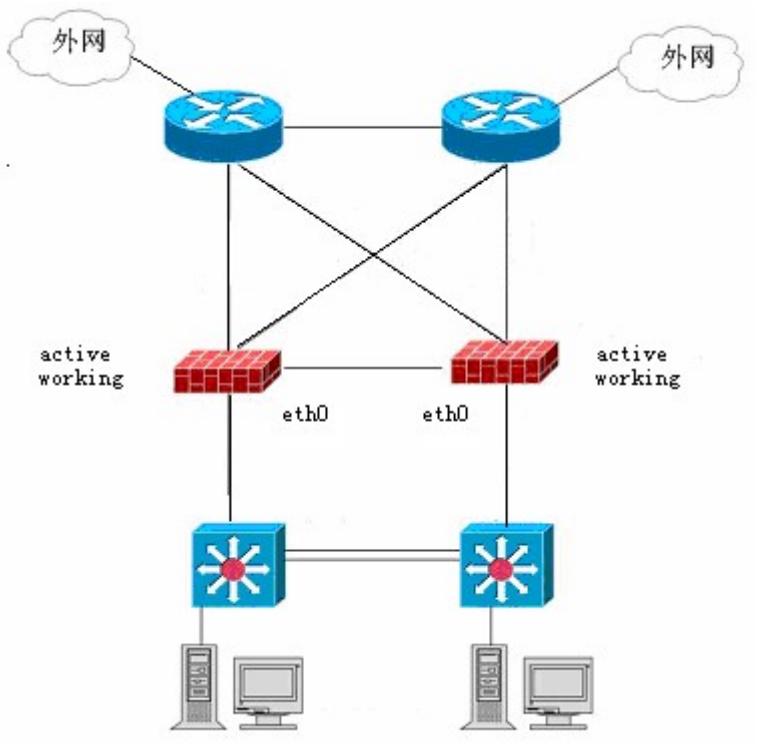
```
enable backup-master
unitID 1
primary-failover self 3.3.3.3 peer 3.3.3.5
sysmon-interface eth0 timeout 3
sysmon-interface eth1 timeout 3
float mac enbale
!
```

66.3.2 配置案例2：配置主主模式

案例描述：

两台防火墙，分别为 FW_A，FW_B 作为冗余设备，工作在主主模式，实现冗余备份的功能。首先把其中一台设备（假设 FW_A）接入网络，并正确连接好网线，HA 口网线可以先不连接。连接好网线后，为设备（FW_A）加电启动，然后通过管理界面对设备（FW_A）进行 HA 配置，并启动 HA 功能。然后把另外一台设备（FW_B）加入网络中，并启动 HA 功能。这里假设设备 HA 通信地址配置在 eth0 上。

案例组网图



配置步骤：

对设备 FW_A 的配置：

步骤1	配置FW_A 的HA接口
	FW_A(config)# ha-group
	FW_A(ha-group)# primary-failover self 3.3.3.3 peer 3.3.3.5
步骤2	配置FW_A的工作模式并启动HA功能
	FW_A(ha-group)# enable master-master

对设备 FW_B 的配置：

步骤1	配置FW_B 的HA接口
	FW_B (config)# ha-group
	FW_B (ha-group)# primary-failover self 3.3.3.5 peer 3.3.3.3
步骤2	配置FW_B的工作模式并启动HA功能
	FW_B (ha-group)# enable master-master

配置结果：

```
!
ha-group
primary-failover self 3.3.3.3 peer 3.3.3.5
enable master-master
```

66.4 HA监控与调试

66.4.1 查看 HA配置

步骤1	显示FW_A的HA配置信息
	FW_A# show ha conf workmode: backup-master Unit-id: 1 grob style: pry-self:30.1.1.40 pry-peer:30.1.1.50 sec-self:0.0.0.0 sec-peer:0.0.0.0 ha-time: 3 config-sync self:30.1.1.40 peer:30.1.1.50 config detect: OFF sync connection ON autosyn enable ON mirroring-address self 30.1.1.40 peer 30.1.1.50 fdb backup enable FW_A# 可以看到，工作模式为主备模式，通信地址配置、同步相关的配置。
步骤1	显示FW_A的HA监控信息
	FW_A#show sysmon-gw FW_A#show sysmon-interface FW_A#show sysmon-trunk 分别查看，网关、接口、聚合链路的配置情况

66.4.2 查看 HA状态

应用环境

FW_A 与 FW_B 做冗余备份，工作在主备模式下，启动 HA 并使 FW_A 成为主设备。

调试实例

步骤1	显示FW_A的HA状态信息
	FW_A# FW_A# show ha state Local : Hostname=FW_A Status=Master, Unit-id=1, Sysmon-down=0 Remote: Hostname=FW_B Status=Master, Unit-id=2, Sysmon-down=0 Config: N/A Softversion: N/A

FW_A#

这里Local显示是本地信息，包括主机名称，和ha状态。

Remote显示是对端信息，包括主机名称，和ha状态。

最后一行显示的是两台设备的各种配置是否相同。包括软件版本，以及配置信息。值为SYNC，表示相同，ASYNC表示不同，N/A或者unkown表示还没有获取到状态信息。

66.4.3 调试

通过 debug ha 命令来进行相关调试。包括：

debug ha cfg	查看配置相关调试信息
debug ha event	ha 状态相关信息
debug ha recv	接收到的 ha 报文信息
debug ha send	发送的 ha 报文信息
debug ha session	连接同步的信息

debug ha recv 调试实例：

```
FW_A# terminal monitor
FW_A# debug ha recv
FW_A# Ha rcv packet (170 bytes) workmode=backup-master ifstatus=1 type=0 mac=00-10-f3-0e-56-c2 sec=0 usec=0
I am master and receive other backup packet
I keep being master
```

结果分析：

本地状态为主，接收到了对端的备份报文，自己仍然保持主状态。对端发送报文长度为 170bytes，工作模式为主备，对端监控口状态正常。（1 表示正常，0 表示异常），类型为备份报文（0 表示为备份状态报文，1 表示为主状态报文）。

debug ha send 调试实例：

```
FW_A# terminal monitor
FW_A# debug ha send
FW_A# HA send a keep_alive packet (send bytes 170 buflen 170) status=Master type=1 ifstatus=1 secs=4098 usecs=773124
HA send a keep_alive packet (send bytes 170 buflen 170) status=Master type=1 ifstatus=1 secs=4100 usecs=633885
HA send a keep_alive packet (send bytes 170 buflen 170) status=Master type=1 ifstatus=1 secs=4101 usecs=634034
```

结果分析：

本地发送报文长度为 170bytes，自身状态为主，报文类型为主状态报文。监控口状态正常。后面的秒和毫秒表示主设备的时间值。

66.5 故障分析

66.5.1 HA无法与对端通信

现象	show ha state时只能看到Local的状态信息，没有Remote状态信息。
分析	ha口通信有问题。 ● ha口是否配置正确。确保ha口是相互直连。 ● ha口网线是否松动。
解决	给出故障的解决方案 ● show ha conf检查配置。如果不正确，更改配置。

72 配置 SNMP

67.1 SNMP协议概述

SNMP（Simple Network Management Protocol）即简单网络管理协议，是有IETF（Internet Engineeriing Task Force，互联网工程任务组）定义的一套基于SGMP（Simple Gateway Monitor Protocol，简单网关监视协议）的网络管理协议。以 SNMP 为技术的网络管理系统(NMS)中，管理工作站利用 SNMP 进行远程监控管理网络上的所有支持这种协议的设备（如计算机工作站、终端、路由器、Hub、网络打印机等），主要负责监视设备状态、修改设备配置、接受事件警告等。

SNMPv3 保持了 SNMPv1 和 SNMPv2 易于理解和实现的特性，同时还增强了网络管理的安全性能，提供了前两个版本欠缺的保密、验证和访问控制等安全管理特性。SNMPv3 正在逐渐扩充和发展，新的管理信息库还在不断增加，能够支持更多的网络应用。所以，它是建立网络管理系统的有力工具，也将推动互联网不断发展。

根据需求增加了 snmpv3 特性，实现了 snmpv3 中的用户管理机制，还添加了公司的私有 mib 库。

67.2 配置SNMP

67.2.1 缺省配置信息

防火墙设备关于 SNMP 的缺省设置信息如以下表格所示：

表 67-1 SNMP 缺省配置信息

内容		
使能/禁止状态（enable/disable）	disable	可更改设置
版本v1	启用	可更改设置
版本v2c	启用	可更改设置
版本v3	启用	可更改设置
设备位置	空	可更改设置
trap地址	空	可更改设置
团体	public	可更改设置
Usm用户	空	可添加用户

67.2.2 配置启用SNMP代理

启用设备的 SNMP 代理，启用后客户端可以访问设备的 MIB 库信息

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	snmp	进入snmp配置节点
步骤3	snmp enable	启用snmp代理

在 snmp 节点下使用 snmp disable 可以关闭 snmp 代理。

参数说明：

命令（1）：snmp NAME

enable	启用snmp代理	无
disable	关闭snmp代理	无

只有在启用 SNMP 以后才能对 SNMP 其他功能作进一步配置。

67.2.3 配置设备物理位置

配置设备物理位置的字符串信息。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	snmp	进入snmp配置节点
步骤3	syslocation abc	配置位置信息为abc
步骤4	end	回到enable模式

使用 no syslocation 可以取消对 syslocation 的设置，使其恢复到缺省配置空。

参数说明：

命令（1）：syslocation NAME

NAME	设备位置信息	空

67.2.4 配置trap地址

配置 snmp 代理发送 trap 时 trap 信息发往的 IP 地址。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	snmp	进入snmp配置节点
步骤3	trap address 192.168.31.2	增加一个trap地址为192.168.31.2
步骤4	end	回到enable模式

使用 no trap address A.B.C.D 可以删除该 trap 地址的配置。可同时添加多个 trap 地址。

参数说明：

命令（1）：trap address A.B.C.D

A.B.C.D	trap信息发送的IP地址	无

67.2.5 配置community

配置 snmp 的团体字符串。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	snmp	进入snmp配置节点
步骤3	community abc	配置团体为abc
步骤4	end	回到enable模式

使用 no community 可以取消对团体的设置，使其恢复到默认值 public。

参数说明：

命令（1）：community NAME

NAME	团体字符串信息	public

67.2.6 配置SNMP版本

配置 snmp 代理启用或关闭的版本。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	snmp	进入snmp配置节点
步骤3	version v1	启用snmp代理v1版本
步骤4	end	回到enable模式

使用 no version v1 可以关闭 snmp 代理 v1 版本。

参数说明：

命令（1）：version (v1|v2c|v3)

(v1|v2c|v3)	启用snmp代理版本	启用

67.2.7 配置SNMP USM用户

配置 snmpv3 用户以及此用户对应的认证和加密算法。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	snmp	进入snmp配置节点
步骤3	snmpv3 usm-user u1 auth-mode MD5 11111111 privacy DES 11111111	配置创建用户u1，采用MD5认证算法和DES加密算法，密钥均为11111111。
步骤4	end	回到enable模式

使用 no snmpv3 usm-user u1 可以删除用户 u1，使用 no snmpv2 usm-user 可

以删除所有用户。

参数说明：

命令（1）：snmpv3 usm-user NAME auth-mode (MD5|SHA) PASSWORD1 privacy (DES|AES) PASSWORD2

NAME	用户名	无
(MD5|SHA)	认证算法	无
PASSWORD1	认证算法密钥	无
(DES|AES)	加密算法	无
PASSWORD2	加密算法密钥	无

67.2.8 配置SNMP管理IP

配置 snmp 管理 IP，用于对发往设备的 SNMP 请求进行过滤。

配置步骤：

步骤1	configure terminal	进入配置模式
步骤2	snmp	进入snmp配置节点
步骤3	add ip address 192.168.31.2	增加一个管理IP地址192.168.31.2。
步骤4	end	回到enable模式

使用 delete ip address 192.168.31.2 可以删除管理 IP 地址 192.168.31.2。

参数说明：

命令（1）：add ip address A.B.C.D

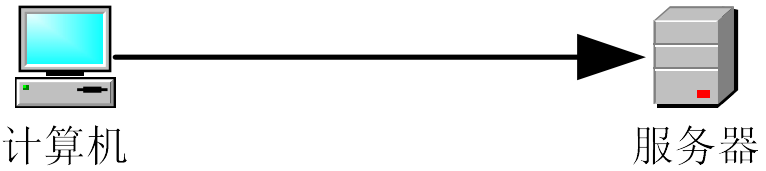
A.B.C.D	管理IP地址	无

67.3 配置案例

67.3.1 配置案例1：通过MIB Browser访问设备MIB库

案例描述

服务器为 USG 设备，实现了 snmp 代理，支持 v1、v2c、v3，计算机为 pc 机，安装了 iReasoning MIB Browser 软件作为管理站。



配置步骤：

步骤1	服务器的配置
	800C_3# configure terminal 800C_3(config)# snmp 800C_3(config-snmp)# snmp enable 800C_3(config-snmp)# syslocation abc 800C_3(config-snmp)# community public 800C_3(config-snmp)# trap address 192.168.31.2 800C_3(config-snmp)# snmpv3 usm-user u1 auth-mode MD5 11111111 privacy DES 11111111 800C_3(config-snmp)# end 800C_3#
步骤2	计算机上MIB Browser的配置

配置结果：

DUT 的 show running-config 信息

snmp

snmp enable

syslocation abc

trap address 192.168.31.2

snmpv3 usm-user u1 auth-mode MD5 secret XMrOjfrJUmSj5p7teDZnBoGy+MLHk26EnNTQfWyFPUmj2o7vvHJEaFzfpMlvuHx privacy DES secret XMrOjfrJUmSj5p7teDZnBoGy+MLHk26EnNTQfWyFPUmj2o7vvHJEaFzfpMlvuHx!

67.4 SNMP监控与维护

67.4.1 查看usm用户

查看 usm user：

步骤1	显示usm用户的配置
	800C_3(config)# snmp
	800C_3(config-snmp)# show snmpv3 usm-user
	usm-user authentication privacy
	u1 MD5 DES

total usm-user number: 1

800C_3(config-snmp)#

可以看出snmp配置一个usm用户，使用MD5认证DES加密。

67.4.2 查看调试信息

debug snmp

查看 snmp 处理过程。


注意

只有高级用户才可以使用此命令，由于此命令会在命令行上打印大量信息，占用很多 CPU 资源因此强烈建议用户，当调试结束时，一定要用 no debug snmp 命令禁用此功能。

67.5 常见故障分析

67.5.1 故障现象1：管理站不能访问代理站MIB库

现象	访问超时或提示认证失败
分析	团体字符串配置不正确或usm用户配置不正确
解决	检查并修改团体字符串和usm用户的配置

73 无线配置

68.1 无线网络概述

部分型号的防火墙添加了 Wi-Fi 功能模块和蜂窝移动网络功能模块。Wi-Fi 功能支持 802.11n 协议，能够让移动终端通过 Wi-Fi 连接到防火墙，进而实现无线网络的访问策略控制。蜂窝移动网络功能模块，通过插入运营商提供的 4G SIM 卡，可以让防火墙及其下的网络通过蜂窝网络访问互联网。通过这两项功能，能够保障企业无线网络、物联网的信息安全。

68.2 配置无线网络

68.2.1 配置Wi-Fi

配置 Wi-Fi 之前，需要配置 Wi-Fi 接口相应的 IP 地址、DHCP 服务器。

Wi-Fi 的配置选项如下：

wifi	进入Wi-Fi配置节点
ssid SSID	配置Wi-Fi热点名称
auth-mode (none|wpa-psk|wpa2-psk)	配置认证方式
passwd PASSWD	配置Wi-Fi的认证密码
band (2.4GHz | 5GHz) channel CHANNEL	选择Wi-Fi的工作频段，以及工作信道
country (China | Japan)	选择国家（目前支持中国和日本）
power (on | off)	使能/关闭Wi-Fi

注意

1. 防火墙上，Wi-Fi 所对应的物理接口为 ge_wlan。
2. 防火墙 Wi-Fi 只能工作在一种频段下。
3. 认证的密码至少需要 8 位。
4. 不同的国家或地区，可以使用的信道是不同的

68.2.2 配置蜂窝移动网络

蜂窝移动网络的配置选项如下：

lte	进入蜂窝移动网络配置节点

power	使能/关闭蜂窝移动网络

注意

1. 防火墙所支持的 SIM 卡为标准卡 Standard SIM，而非 Mini SIM、Nano SIM、Micro SIM。
2. SIM 卡不支持热插拔。请在防火墙断电的情况下，插拔 SIM 卡。
3. 防火墙上，蜂窝移动网络所对应的物理接口为 ge_lte。
4. ge_lte 接口获取运营商 IP 地址的方式为 PPPoE。

68.3 配置案例

68.3.1 无线网络配置案例

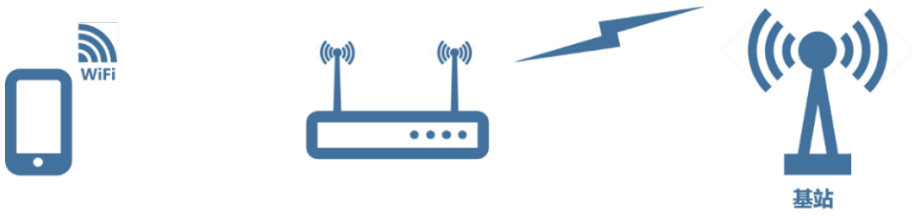
案例描述：

企业的移动终端和物联网终端需要能够访问互联网。但由于没有铺设线缆，无法通过有线网络组网。并且为了信息安全，需要一台防火墙来隔离内外网络。此时配置了无线功能模块的防火墙正好可以用来解决这个需求。

用户需求如下：

1. 企业内网的移动终端、物联网终端经过防火墙的访问控制策略，可以访问互联网。而外网试图访问企业内网的行为则被阻断。
2. 由于没有布置互联网专线，需要使用联通 4G 蜂窝网络来访问互联网。

配置案例组网图：



1. 配置 Wi-Fi

步骤1	show wifi config country: China ssid: wl_network-5G	显示Wi-Fi缺省配置

	password: wl-passwd-12345678 band: 5GHz channel: 0 auth-mode: wpa2-personal	
步骤2	configure termial	进入配置模式
步骤3	dhcp share-net server-1 subnet 192.168.0.1/24 share-net server-1 router 192.168.0.1 share-net server-1 dns 114.114.114.114 8.8.8.8 share-net server-1 192.168.0.2 192.168.0.100 infinite	配置DHCP Server
步骤3	interface ge_wlan	配置Wi-Fi接口
步骤4	ip address 192.168.0.1/24	配置接口IP地址
步骤5	dhcpserver enable	Wi-Fi接口使能dhcp server

2. 配置蜂窝网络

步骤1	configure terminal	进入配置模式
步骤2	ip nat source ge_lte any any any interface	配置一条出口为ge_lte的NAT规则
步骤3	interface ge_lte	进入接口配置节点
步骤4	ip address dhcp metric 100 gw reset dns reset	在接口上启用DHCP

3. 配置安全策略

步骤1	configure terminal	进入配置模式
步骤2	firewall policy 1 action permit name default firewall-policy-group default src-zone ge_wlan dst-zone any src-addr any dst-addr any service any timerange always user any app any enable	配置一条入口为ge_wlan的全通防火墙策略

至此，案例配置完成。移动终端可以通过 Wi-Fi 连接防火墙，经过防火墙的防护策略保护后，再通过 4G 蜂窝移动网络访问互联网。

68.4 常见故障分析

68.4.1 Wi-Fi连接失败

现象	配置Wi-Fi后，移动终端连接Wi-Fi失败。
分析	分析可能为以下几种情况： 1. Wi-Fi名称即SSID错误。 2. 移动终端不支持5G频段。 3. 移动终端不支持所设国家的信道。 4. 未配置DHCP服务器。
解决	1. 确认移动终端所连接的SSID是否正确。 2. 修改防火墙的Wi-Fi频段为2.4GHz。 3. 修改防火墙Wi-Fi的信道，使之与移动终端所支持的信道相匹配。 4. 将ge_wlan开启DHCP服务，并配置DHCP服务器。

68.4.2 移动终端无法访问互联网

现象	移动终端成功连接防火墙Wi-Fi后，却无法访问互联网。
分析	分析可能为以下几种情况： 1. 未启用蜂窝移动网络。 2. 蜂窝移动网络信号弱。 3. 所配置的其它路由与通过蜂窝网络所获得的网关冲突。 4. 未配置源NAT。 5. 防火墙策略未生效。
解决	1. 开启蜂窝网络，查看是否能正确获得运营商分配的IP地址。 2. 观察蜂窝网络的信号状态，调整防火墙的位置，以获得更好的网络信号。 3. 调整其它路由及所获得的网关距离，使蜂窝网络的网关生效。 4. 配置出接口为ge_lte，转换后源地址为出接口地址的源NAT。 5. 检查防火墙策略是否启用，匹配是否正确。

74 web 应用防护

69.1 概述

Web 应用防护可以防止 web 应用免受各种常见攻击，如 SQL 注入，跨站脚本攻击(XSS)，能够监测并过滤掉让应用遭受攻击的流量。它会在 HTTP 流量抵达应用服务器之前检测可疑访问，同时也能防止从 Web 应用获取某些未经授权的数据。

69.2 配置web应用防护策略

69.2.1 创建web应用防护策略

根据命令行提示创建 web 应用防护策略。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	waf policy <1-500> A.B.C.D <0-65535> (IF_IN|any)	配置策略相关的过滤信息
步骤3	enable	启用策略
步骤4	name NAME	配置策略名字
步骤5	action (check_no_drop | event_action)	配置策略动作
步骤6	request-body (enable | disable)	是否检测请求体
步骤7	reply-head (enable | disable)	是否检测回应头
步骤8	reply-body (enable | disable)	是否检测回应体
步骤9	log (enable | disable)	是否开启日志
步骤10	verify-profile NAME	引用HTTP合规检查模板
步骤11	set NAME	引用事件集
步骤12	End	返回特权模式
步骤13	show waf policy	显示所有WEB应用防护策略

<1-500>：策略 ID 范围。

A.B.C.D：受保护 web 服务器的 IP 地址。

<0-65535>：受保护 web 服务器的端口。

(IF_IN|any)：入接口/安全域的名称，any 表示匹配所有。

(check_no_drop|event_action)：配置 WEB 应用防护策略动作，chec_no_drop 表示”只检测不阻断”，event_action 表示”按事件动作处理”。

(enable|disable)：enable 启动表示启用该 WEB 应用防护策略，disable 表示不启用该 WEB 应用防护策略。

69.2.2 删除web应用防护策略

根据策略 ID 删除指定的 web 应用防护策略。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	no waf policy <1-500>	删除指定ID的策略
步骤3	end	返回特权模式
步骤4	show waf policy	显示所有策略

69.2.3 修改某一策略的匹配信息

根据策略的 ID 号，进入到策略内部对匹配信息进行修改。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	waf policy <1-500>	根据策略ID，进入策略内
步骤3	enable	启用策略
步骤4	no enable	关闭策略
步骤5	name NAME	配置策略名字
步骤6	no name	取消策略名字
步骤7	action (check_no_drop|event_action)	修改策略动作
步骤8	request-body (enable|disable)	是否检测请求体
步骤9	reply-head (enable|disable)	是否检测回应头
步骤10	reply-body (enable|disable)	是否检测回应体
步骤11	end	返回特权模式
步骤12	show waf policy	显示所有策略

69.2.4 查询web应用防护策略的配置

根据命令查看所有策略配置或指定策略 ID 的策略配置。

配置步骤：

步骤1	show waf policy	显示所有策略
步骤2	show waf policy <1-500>	显示指定ID的策略

69.2.5 移动web应用防护策略的匹配顺序

以某个策略为基准，可以配置将目标策略移动到基准策略之前或之后。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	waf policy move <1-500> (before|after) <1-500>	将前者ID对应的策略移动到后者ID对应的策略之前或者之后
步骤4	end	返回特权模式
步骤5	show waf policy	显示所有策略

69.2.6 插入web应用防护策略

以某个策略为基准，可以配置将目标策略新建到基准策略之前。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	waf policy insert <1-500> A.B.C.D <0-65535> (IF_IN|any) before <1-500>	将前者ID对应的策略新建到后者ID对应的策略之前

69.3 配置事件集

69.3.1 创建事件集

根据命令行提示创建事件集。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	waf set NAME	配置事件集名字
步骤3	description .LINE	配置事件集描述
步骤4	end	返回特权模式
步骤5	show waf set	显示所有事件集

69.3.2 删除事件集

根据事件集名字删除指定的事件集。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	no waf set NAME	删除指定名字的事件集
步骤3	end	返回特权模式
步骤4	show waf set	显示所有事件集

69.3.3 查询事件集

根据命令查看所有事件集配置或指定名字的事件集配置。

配置步骤：

步骤1	show waf set	显示所有事件集
步骤2	show waf set NAME	显示指定名字的事件集

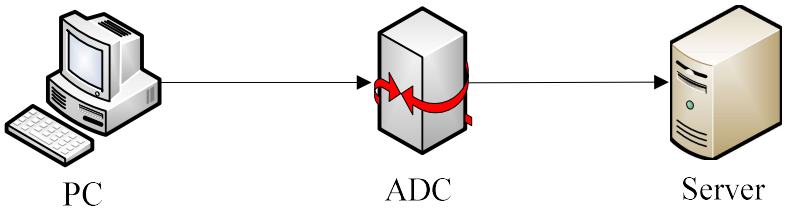
69.4 配置案例 ·

69.4.1 为服务器配置ALL事件集

案例描述

PC 通过防火墙设备访问 Web 服务器，地址为 192.168.1.2，端口为 80，引用事件集为 ALL。设策略 ID 为 100。

网络拓扑：



1. 配置步骤：

host(config)# waf policy 100 192.168.1.2 80 any

host(config-waf-policy)# enable

host(config-waf-policy)# set ALL

host(config-waf-policy)# log enable

2.配置结果

host# show waf policy 100

waf policy 100 192.168.1.2 80 any

enable

set ALL

match statistic: 0

host#

3.配置验证

触发 ALL 事件集中的事件，上报对应日志，证明配置成功。

75 资产防护

70.1 资产防护概述

资产防护的目的是探测网络中的 IP 设备或者叫资产（主要是 IOT 设备，比如打印机、摄像头等），并对这些资产起到保护作用。此类设备一般网络防护能力比较差，容易遭受攻击，通过定期去探测此类设备的指纹信息，并对比前后扫描的结果，如果发现指纹信息发生明显改变，说明 IOT 设备可能遭受到网络攻击，此时把这个设备的 ip 加入黑名单，从而保证网络的安全。

70.2 配置资产防护

70.2.1 配置防护列表

配置步骤:

步骤**1**	configure terminal	进入配置模式
步骤**2**	iot-terminal protect-task name NAME protect-mode (loose| strict)	增加一个防护任务，指定name和防护方式，然后进入资产防护节点
步骤**3**	description	配置防护任务描述
步骤4	active-detect (enable|disable)	配置主动探测开关
步骤5	passive-detect (enable|disable)	配置被动探测开关
步骤**6**	protect-net A.B.C.D/M	配置防护网段
步骤7	exclude-ip A.B.C.D	配置排除ip
步骤**8**	detect-interval < 5-30000>	配置扫描间隔（分钟）
步骤**9**	warning-level (finger|mac|manu|os|tcp|type|udp)	配置告警选项
步骤10	warning-recover (enable|disable)	配置高警自动恢复
步骤11	warning-add-blacklist (enable|disable)	配置告警自动隔离

参数说明：

参数	说明	缺省配置
name	防护任务名称	
protect-mode	防护模式，宽松模式或者严格	

	模式	
description	防护任务名称	
active-detect/ passive-detect	主动扫描（主动发包探测）/ 被动扫描（资产流量发现）	
protect-net	防护网段，最多添加8个，每个掩码最少24位	
exclude-ip	排除ip，主动探测时不探测的ip地址，最多配置32个	
detect-interval	主动探测的间隔	30分钟
warning-level	产生告警的指纹选项，配置后该参数发生变化将产生告警	mac；os；type
warning-recover	资产指纹恢复后，若有告警是否自动恢复	enable
warning-add-blacklist	资产告警后是否自动隔离，如果protect-mode是严格模式（strict），则此配置只能为模式开启，不能修改	宽松模式disble，严格模式为enable

70.2.2 配置扫描资产

审批资产配置步骤:

步骤1	configure terminal	进入配置模式
步骤2	iot-terminal A.B.C.D	进入某个资产配置试图，进入iot节点
步骤3	(no) approve	（取消）审批

参数说明：

参数	说明	缺省配置
A.B.C.D	选择一个资产进程配置	
approve	审批一个资产，即认可该资产指纹	

显示资产配置步骤:

步骤1	show iot-terminal	显示所有资产
步骤2	show iot-terminal A.B.C.D/ (un)approved/mac/type/os/online /offline/normal/warning	按条件显示资产（根据资产ip、mac、os、type、状态等）

步骤3	show iot-terminal statistic	显示资产统计值

删除资产配置步骤:

步骤1	configure terminal	进入配置模式
步骤2	no iot-terminal A.B.C.D	删除资产ip为A.B.C.D的资产

70.3 常见故障分析

资产列表为空

故障现象	防护列表配置之后，很长时间资产列表没有资产
分析与解决	1）查看防护任务的状态，如果是扫描中，需要等待扫描完； 2）如果已经扫描完，是定时等待，则需要排查网络； 3）排查扫描网段是否路由可达； 4）排查网络中是否有防扫描安全设备；

76 交换机联动

71.1 交换机联动概述

通过配置交换机联动能通过 SNMP 协议够获取指定交换机的 IP-MAC 对应关系，并添加到自己的 IP-MAC 表中。

71.2 配置交换机联动

71.2.1 配置交换机联动开关

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	iot-terminal-detect switch-linkage (on|off)	配置交换机联动开关

71.2.2 配置访问间隔

交换机联动发送 SNMP 查询数据包的间隔时间。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	iot-terminal-detect switch-linkage-interval <30-300>	配置访问间隔，单位为秒

71.2.3 配置超时时间

发送的 SNMP 查询数据包在此时间内没收到回应包，则判定此次查询失败。

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	iot-terminal-detect switch-linkage-timeout <1-10>	配置超时时间，单位为秒

71.2.4 配置snmp服务器

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	iot-terminal-detect switch-server A.B.C.D NAME [NAME]	配置snmp服务器

参数说明：

参数	说明	缺省配置
A.B.C.D	要进行联动的交换机的IP地址	
NAME	community，snmp代理认证的密码	
[NAME]	OID，SNMP代理提供的具有唯一标识的键值	1.3.6.1.2.1.3.1.1.2

71.2.5 查看通过snmp获取到的IP-MAC列表

配置步骤：

步骤1	show iot-terminal-detect ip-mac	查看IP-MAC列表

71.3 配置案例

71.3.1 交换机联动

案例描述：

防火墙设备与远端交换机设备进行联动，交换机 ip 地址为 192.168.100.2

配置步骤：

步骤1	开启交换机联动
	host(config)# iot-terminal-detect switch-linkage on
步骤2	配置snmp服务器
	host(config)# iot-terminal-detect switch-server 192.168.100.2 public 1.3.6.1.2.1.3.1.1.2
步骤3	查看交换机联动探测状态
	host# show iot-terminal-detect switch-linkage-status switch_linkage server 192.168.100.2 not in detecting.
步骤4	查看通过snmp获取到的IP-MAC列表
	host# show iot-terminal-detect ip-mac switch_linkage ip mac total count 2 : ip 192.168.100.1 mac 00-10-F3-3A-68-00 from switch 192.168.100.2 ip 192.168.100.2 mac BC-16-65-95-61-42 from switch 192.168.100.2

71.4 常见故障分析

71.4.1 未能获取到目标服务器的IP-MAC对应关系

现象	添加SNMP服务器但是未能获取到目标服务器的IP-MAC对应关系

分析	有可能是以下几种情况导致未能获取到： ● 该配置没有启用，请检查策略状态是否为启用； ● community可能不正确 ● 目的SNMP服务器不允许设备访问
解决	● 该配置没有启用，请检查配置状态是否为启用； ● 提交正确的community ● 检查要联动交换机的SNMP服务器配置，配置允许设备访问

77 指纹管理

72.1 指纹管理概述

通过配置指纹管理可以通过扫描资产列表中的资产，获取到到资产的类型、厂商和操作系统。

配置指纹管理分为预定义指纹库和自定义指纹两种配置方式。

72.2 配置预定义指纹库

72.2.1 查看预定义指纹库版本

查看步骤：

步骤1	查看预定义指纹库版本
	host# show iot-terminal-detect fingerprint-library-version Built-in fingerprint library version : V0200B20221107.

72.2.2 查看预定义指纹库指纹总数

查看步骤：

步骤1	查看预定义指纹库版本
	host# show iot-terminal-detect pre-fingerprint-library-count Pre fingerprint library count: 1881.

72.2.3 查看预定义指纹库指纹

查看步骤：

步骤1	查看预定义指纹库指纹信息
	host# show iot-terminal-detect pre-fingerprint 1 华为-防火墙1:Eudemon Server:2:防火墙:13:华为:::防火墙 2 华为-防火墙2:Modify by wangxiangguang:2:防火墙:13:华为:::防火墙 3 Canon-打印机1:Canon Http Server:3:打印机:40:Canon:::打印机 .....

72.2.4 通过tftp升级预定义指纹库

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	copy tftp A.B.C.D RemoteFile prefinger	开始升级

参数说明：

参数	说明	缺省配置
A.B.C.D	tftp服务器地址	
RemoteFile	预定义指纹库文件名	

72.2.5 通过ftp升级预定义指纹库

配置步骤：

步骤1	config terminal	进入配置模式
步骤2	copy ftp USERNAME PASSWD A.B.C.D RemoteFile prefinger	开始升级

参数说明：

参数	说明	缺省配置
USERNAME	ftp用户名	
PASSWD	ftp密码	
A.B.C.D	ftp服务器地址	
RemoteFile	预定义指纹库文件名	

72.3 配置案例

72.3.1 通过tftp升级预定义指纹库

案例描述：

tftp 服务器地址是 192.168.1.62，预定义指纹库文件是 fingerprint.zip

配置步骤：

步骤1	通过tftp升级预定义指纹库
	host# copy tftp 192.168.1.62 fingerprint.zip prefinger
步骤2	查看预定义指纹库版本
	host# show iot-terminal-detect fingerprint-library-version
	Built-in fingerprint library version : V0200B20221107.

步骤3	查看预定义指纹库指纹总数
	host# show iot-terminal-detect pre-fingerprint-library-count Pre fingerprint library count: 1881.

72.3.2 通过ftp升级预定义指纹库

案例描述：

ftp 服务器地址是 192.168.1.62，用户名是 test，密码是 123456，预定义指纹库文件是 fingerprint.zip

配置步骤：

步骤1	通过ftp升级预定义指纹库
	host# copy ftp test 123456 192.168.1.62 fingerprint.zip prefinger
步骤2	查看预定义指纹库版本
	host# show iot-terminal-detect fingerprint-library-version Built-in fingerprint library version : V0200B20221107.
步骤3	查看预定义指纹库指纹总数
	host# show iot-terminal-detect pre-fingerprint-library-count Pre fingerprint library count: 1881.

72.4 常见故障分析

72.4.1 未预定义指纹库升级失败

现象	预定义指纹库升级提示导入文件错误
分析	有可能是以下几种情况导致导入指纹失败： ● tftp或ftp服务器未启动； ● ftp用户名或密码不正确； ● 上传的文件不是zip压缩文件； ● 预定义指纹文件内容格式不对。
解决	● 启动tftp或ftp服务器； ● 输入正确的ftp用户名和密码； ● 检查上传的文件是否为zip格式； ● 检查预定义指纹文件内容的格式。

78 行为学习

73.1 行为学习监控与维护

73.1.1 查看表项

步骤1	查看学习到的被动资产和连接的详情统计
	(host)#show iot-terminal passive probe num iot terminal count: service count 10 terminal count 200 srcip count 90 service count 服务节点数量；terminal count 终端节点数量；srcip count 被动资产数量；
步骤2	查看学习到的被动资产
	(host)#show iot-terminal ipmac all
步骤3	查看被动资产的名称和状态
	(host)#terminal monitor (host)#show iot-terminal app-ip-property
步骤4	查看生效的防护网段
	(host)#show iot-terminal passive probe focus prefix

73.1.2 清除表项

步骤1	清除连接表项
	(host)#clear iot-terminal passive probe all
步骤2	清除被动资产表项
	(host)#clear iot-terminal ipmac all

73.1.3 查看行为学习过程

步骤1	查看行为学习过程的调试信息
	(host)#terminal monitor (host)#debug iot-passive-probe