



天翼云·云下一代防火墙

运维人员操作指南

天翼云科技有限公司

目 录

1	运维人员运维操作指南	1
1.1	前言	1
1.1.1	编写目的	1
1.1.2	文档范围	1
1.1.3	目标读者	1
1.2	设备日常维护操作指导	1
1.2.1	设备登录方法	1
1.3	系统升级	1
1.3.1	设备升级注意事项	1
1.3.2	设备升级方法	2
1.4	设备配置备份与恢复	2
1.4.1	备份当前配置	2
1.4.2	配置文件管理 (WebUI)	2
1.4.3	配置文件管理 (CLI)	3
1.5	单机相关操作	3
1.5.1	单机设备重启	3
1.6	双机相关操作	4
1.6.1	双机模式下主备关机	4
1.6.2	双机模式下主备设备重启	4
1.6.3	双机模式下操作系统升级	4
1.6.4	双机主备切换及切换后恢复	5
1.7	管理员创建及修改	6
1.8	创建接口	8

1.9	设备双机 HA 配置	15
1.10	路由配置	18
1.11	日志配置	19
1.12	SNMP 配置	21
1.13	NTP 配置	23
1.14	地址和服务对象	25
1.14.1	地址簿定义	25
1.14.2	服务簿定义	27
1.15	策略配置	29
1.15.1	安全策略介绍	29
1.15.2	策略规则的基本元素	29
1.15.3	策略规则及匹配顺序	30
1.15.4	配置策略规则	30
1.16	ALG 配置	32
1.17	NAT 配置	33
1.17.1	NAT 转换过程 (源 NAT)	33
1.17.2	NAT 转换过程 (目的 NAT)	34
1.18	常用诊断工具	36
1.18.1	查看系统日志	36
1.18.2	查看系统进程	36
1.18.3	查看会话情况	38
1.18.4	查看 ARP	40
1.18.5	查看路由	40
1.18.6	查看 FIB	41
1.18.7	检查连通性	42
1.19	防火墙故障排查步骤	43

1.19.1	软件部分.....	43
1.20	故障信息收集.....	45
1.20.1	CPU 异常升高.....	45
1.20.2	会话数异常升高.....	46
1.20.3	防火墙主备切换.....	47
1.20.4	丢包或者业务中断.....	47
1.21	系统调试功能.....	49
1.21.1	防火墙数据转发流程.....	49
1.21.2	DEBUG 数据流基本步骤.....	51
1.21.3	正常访问 DEBUG 信息示例.....	51
1.22	常用监控维护命令.....	53
1.23	故障信息收集.....	57

1 运维人员运维操作指南

1.1 前言

1.1.1 编写目的

运维操作指南主要为运维人员指导最终用户操作的参考文档。

1.1.2 文档范围

此文档适用于运维人员

1.1.3 目标读者

运维人员。

1.2 设备日常维护操作指导

1.2.1 设备登录方法

1. 通过 SSH 方式进行远程登陆

在 PC 机上运行 SSH 程序，输入防火墙的带外管理 IP 地址。

2. 通过 web 界面远程登录

在 PC 浏览器上面输入：<https://x.x.x.x>（管理地址）。

1.3 系统升级

1.3.1 设备升级注意事项

升级版本前，请查看设备的平台许可证是否在服务期内，长期稳定运行的设备，如非有特殊功能需求，不建议升级软件版本。

1.3.2 设备升级方法

WEB 升级方法:

点击【系统】--【升级管理】，或者直接点主页系统信息中，软件版本后的“升级”，默认选项“升级版本”，从本地上传 bin 文件，点击升级；



The image shows a web interface for upgrading a device. It has two main sections: '升级版本' (Upgrade Version) and '选择下次启动版本' (Select Next Start Version). Both sections include a warning message: '升级前建议备份配置文件，升级后请清除浏览器缓存再进行访问。' (It is recommended to back up the configuration file before upgrading, and clear the browser cache after upgrading). The '升级版本' section shows the current version as 'SG6000-M-3-5.5R2P11.bin', a file upload field, and a dropdown menu for the backup version, also set to 'SG6000-M-3-5.5R2P11.bin'. There is a checkbox for '立即重启，使新版本生效' (Restart immediately, make the new version effective) and an '应用' (Apply) button. The '选择下次启动版本' section has a similar layout with a dropdown menu for the next start version.

CLI 命令行升级:

命令行 ftp 上传: 执行模式下, import image from ftp server x.x.x.x user xxx password xxx (ftp 中的目录) SG6000-M-3-5.5R2P11.bin;

1.4 设备配置备份与恢复

1.4.1 备份当前配置

设备可以保存至多 10 份配置在设备中, 包括 current 以及 backup 0-8, current 配置会随网页配置更改随时保存, 命令行配置需要使用“save”命令保存。

可以选择【系统】--【配置文件管理】--【备份恢复】，将 current 配置备份在设备中，

设备会将最早备份的配置标记为 backup 0, 然后依次标记一直到 backup 8, 如果继续备份配置, 则自动删除 backup0, 将 backup1 变为 backup0,, 将 backup8 变为 backup 7, 当前配置保存为 backup 8。

1.4.2 配置文件管理 (WebUI)

管理员可以导入、导出或者将系统恢复出厂配置, 当前系统配置窗口提供对当前配置的

Web 方式查阅。系统能够纪录最近十次保存的起始配置信息, 用户可以根据需要导出或回退到

已保存的指定起始配置信息。

【系统】 -- 【配置文件管理】，可以导出当前或某个时间点的配置文件用来做备份。



文件名称	保存时间	大小 (字节)	软件版本	用户	备份源	描述
Startup	2018-04-25 10:39:21	90465	5.5R2	hillstone	Console	
Backup 4	2018-04-25 10:27:29	90373	5.5R2	hillstone	Console	
Backup 3	2018-04-25 09:34:01	90312	5.5R2	hillstone	Console	
Backup 2	2018-04-24 17:20:13	90312	5.5R2	autosave	---	
Backup 1	2018-03-21 22:12:25	89220	5.5R2	hillstone	SSH	
Backup 0	2018-03-21 22:11:22	89220	5.5R2	autosave	---	

1.4.3 配置文件管理 (CLI)

查看当前配置，输入以下命令：

```
show configuration
```

查看防火墙的当前起始配置信息，输入以下命令：

```
show configuration startup
```

当前起始配置信息以 “startup” 作为标记

回退起始配置信息

```
rollback configuration backup {number}
```

保存配置信息

```
save [string]
```

string - 对所保存配置信息的描述

恢复出厂配置

```
unset all
```

注意：请谨慎使用 `unset all` 命令，因为执行该命令会导致设备配置情况。

1.5 单机相关操作

1.5.1 单机设备重启

在设备运行过程中，由于各种原因，如系统文件升级等，用户需要重启设备。用户可以通过下电再重新上电重启设备，也可以通过 CLI 或者 WebUI 重启设备。

重启设备，请在执行模式下使用 `reboot` 命令重启。请参阅以下示例：

```
hostname# reboot
```

System configuration has been modified. Save? [y]/n （键入字母“y”或者敲回车键，系统将保存配置；键入字母“n”，系统将不保存配置）

```
Building configuration..
```

```
Saving configuration is finished
```

System reboot, are you sure? y/[n] （键入字母“y”，系统将重启；键入字母“n”或者敲回车键，系统将返回到执行模式）

执行 reboot 命令时，系统首先会提示用户是否保存先前所做的配置。请谨慎使用 reboot 命令，因为执行该命令会导致网络工作在短时间内中断。

1.6 双机相关操作

1.6.1 双机模式下主备关机

在设备双机模式运行过程中，由于各种原因，如需要更换其中的某台设备或全部替换，用户需要关闭设备。

1.6.2 双机模式下主备设备重启

在设备双机模式运行过程中，由于各种原因，如系统文件升级等，用户需要重启设备。用户可以通过命令行 CLI 或者 WebUI 重启设备。

- 1、先重启备设备，主墙业务不受影响，重启步骤参考 2.8.2 小节
- 2、待备墙启动完成后，再重启主设备，重启步骤参考 2.8.2 小节
- 3、备设备成为主设备接管业务，不影响业务
- 4、原主设备启动完成后成为备机（未配置抢占模式，需要恢复主备状态在主设备使用 `exec ha master switchover` 命令进行主备切换）

1.6.3 双机模式下操作系统升级

在设备双机模式运行过程中，由于各种原因，如修复版本的问题等，需要进行软件操作系统升级，为保障升级过程中业务不中断，按照下面的步骤进行：

- 1、为保证网络通讯不中断，首先对备墙进行升级，升级步骤参见 2.6 小节；
- 2、备墙升级完成后，检查 HA 配置及其他配置；
- 3、备墙配置无问题后，对主墙进行升级，升级步骤参见 2.6 小节；

- 4、主墙升级完成后会重新启动，这时备墙会接管主墙工作，保证网络通讯不中断；
- 5、原主设备升级完成后成为备机（未配置抢占模式，需要恢复主备状态在主设备使用 `exec ha master switchover` 命令进行主备切换）。

1.6.4 双机主备切换及切换后恢复

在设备双机模式运行过程中，由于各种原因，如切换测试等，需要进行主备切换操作，可参考下面两种方法：

方法一

1、备机配置抢占模式

如果将设备配置为抢占模式，一旦设备发现自己的优先级高于主设备，就会将自己升级为主设备，而原先的主设备将变为备份设备；如果将设备设置为非抢占模式，即使设备的优先级高于主设备，它也只能在主设备故障时代替主设备工作。在配置抢占模式时，用户还可以设置延迟时间，使备份设备在延迟时间过后升级为主设备。配置抢占模式，在 HA 组配置模式下使用以下命令：

```
preempt [delay-time]
```

- ◆ *delay-time* - 指定延迟时间，单位为秒。范围是 1 到 600 秒。默认值为 30 秒。

2、配置备机优先级高于主机

该命令指定的优先级用于 HA 选举。优先级高（数字小）的会被选举为主设备。为设备指定优先级，在 HA 组配置模式下使用以下命令：

```
priority number
```

- ◆ *number* - 指定优先级。范围是 1 到 254 的整数。默认值是 100。

3、进行完成主备切换

4、主机配置抢占模式

```
preempt [delay-time]
```

5、恢复原备机的优先级

6、主备状态恢复

方法二

- 1、主设备输入命令 `exec ha master switchover` 进行主备切换;
- 2、主备切换完成;
- 3、新主设备输入命令 `exec ha master switchover` 进行主备切换;
- 4、主备状态恢复;

1.7 管理员创建及修改

WEB 配置:

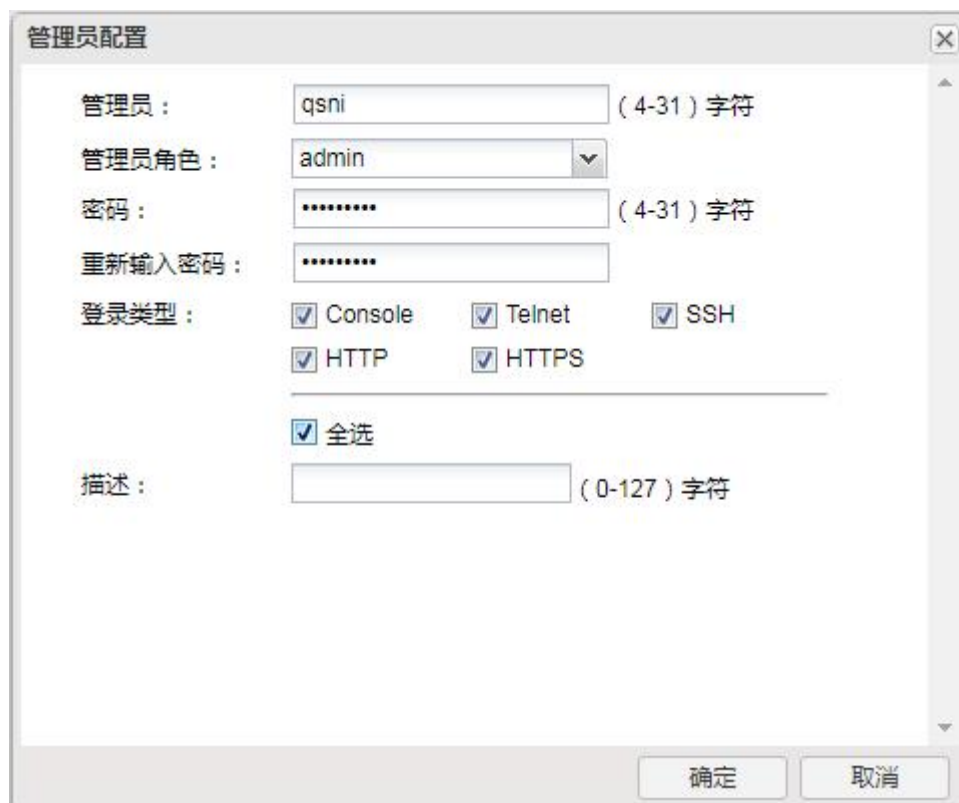
选择界面视图的【系统】--【设备管理】;



管理员	角色	Console	Telnet	SSH	HTTP	HTTPS	描述
hilstone	系统管理员	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

图 3-1 管理员配置

可以完成操作管理员的添加, 修改密码等操作;



管理员配置

管理员: (4-31) 字符

管理员角色: ▼

密码: (4-31) 字符

重新输入密码:

登录类型: Console Telnet SSH
 HTTP HTTPS

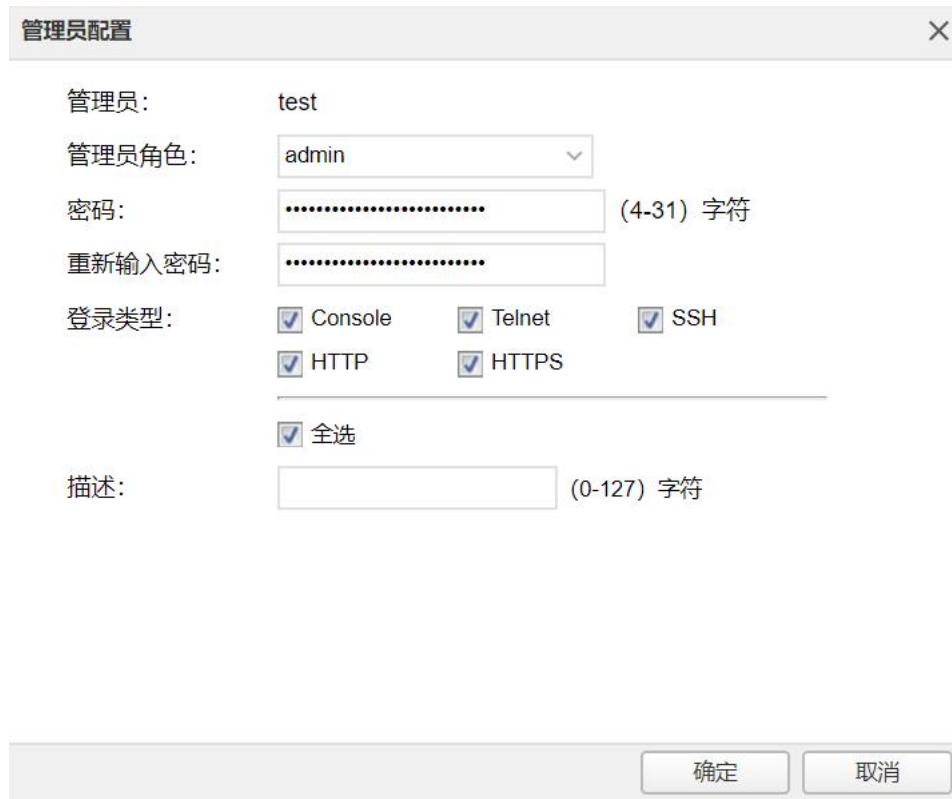
全选

描述: (0-127) 字符

确定 取消

图 3-2 管理员配置

选择系统默认超级管理员的修改项，可以重新设置用户的密码。



管理员配置

管理员: test

管理员角色: admin

密码: (4-31) 字符

重新输入密码:

登录类型: Console Telnet SSH
 HTTP HTTPS

全选

描述: (0-127) 字符

确定 取消

图 3-3 管理员配置

CLI 配置:

在全局配置模式下输入以下命令配置管理员:

```
admin user user-name
```

user-name - 指定管理员名称

在全局配置模式下使用以下命令删除指定的管理员:

```
no admin user user-name
```

在管理员配置模式下，输入以下命令配置管理员的特权:

```
role { admin | operator | auditor | admin-read-only }
```

在管理员配置模式下，输入以下命令配置管理员的密码:

```
password password
```

在管理员配置模式下，输入以下命令配置管理员的访问方式:

access {console | http | https | ssh | telnet | any}

显示系统管理员信息：

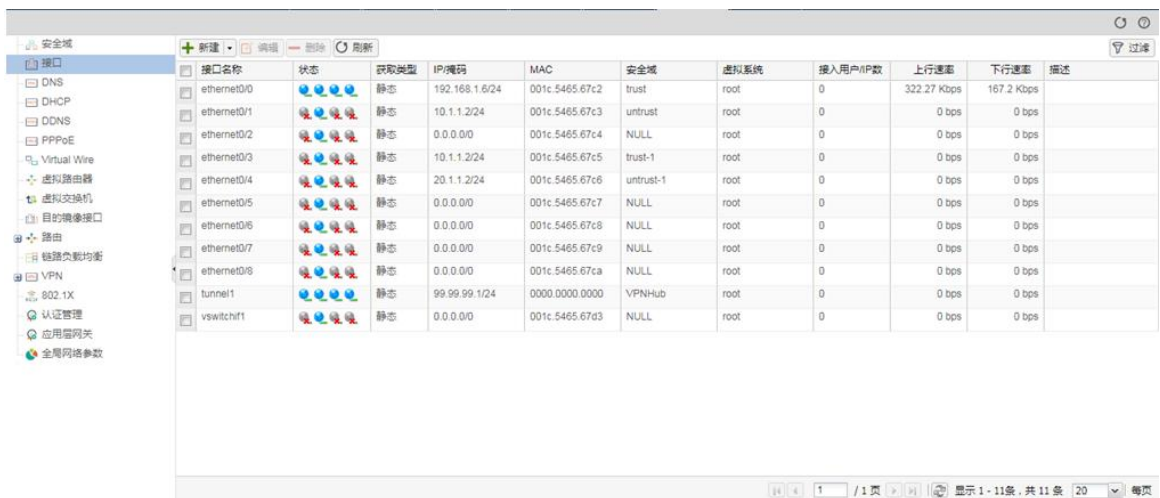
show admin user

显示系统管理员具体配置信息： show admin user user-name。

1.8 创建接口

WEB 配置：

选择【网络】--【接口】，即可进入接口配置界面。

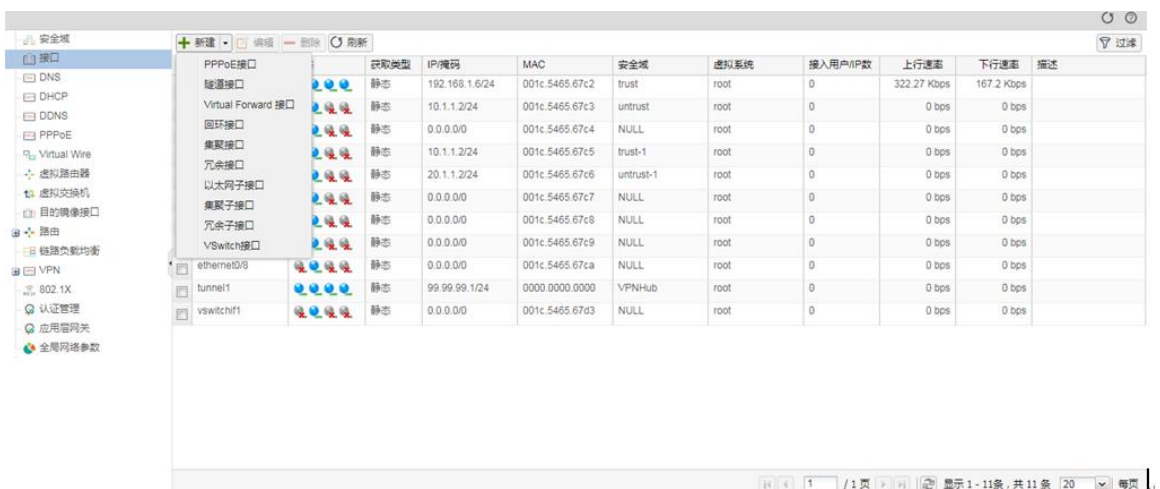


接口名称	状态	获取类型	IP/掩码	MAC	安全域	虚拟系统	接入用户/IP数	上行速率	下行速率	描述
ethernet0/0	静态	静态	192.168.1.6/24	001c.5465.67c2	trust	root	0	322.27 Kbps	167.2 Kbps	
ethernet0/1	静态	静态	10.1.1.2/24	001c.5465.67c3	untrust	root	0	0 bps	0 bps	
ethernet0/2	静态	静态	0.0.0.0/0	001c.5465.67c4	NULL	root	0	0 bps	0 bps	
ethernet0/3	静态	静态	10.1.1.2/24	001c.5465.67c5	trust-1	root	0	0 bps	0 bps	
ethernet0/4	静态	静态	20.1.1.2/24	001c.5465.67c6	untrust-1	root	0	0 bps	0 bps	
ethernet0/5	静态	静态	0.0.0.0/0	001c.5465.67c7	NULL	root	0	0 bps	0 bps	
ethernet0/6	静态	静态	0.0.0.0/0	001c.5465.67c8	NULL	root	0	0 bps	0 bps	
ethernet0/7	静态	静态	0.0.0.0/0	001c.5465.67c9	NULL	root	0	0 bps	0 bps	
ethernet0/8	静态	静态	0.0.0.0/0	001c.5465.67ca	NULL	root	0	0 bps	0 bps	
tunnel1	静态	静态	99.99.99.1/24	0000.0000.0000	VPN-Hub	root	0	0 bps	0 bps	
vswitch1	静态	静态	0.0.0.0/0	001c.5465.67d3	NULL	root	0	0 bps	0 bps	

图 3-4 接口视图

1、聚合接口配置：

选择【新建】--【集聚接口】进入集聚接口配置界面；



接口名称	状态	获取类型	IP/掩码	MAC	安全域	虚拟系统	接入用户/IP数	上行速率	下行速率	描述
PPPoe接口	静态	静态	192.168.1.6/24	001c.5465.67c2	trust	root	0	322.27 Kbps	167.2 Kbps	
隧道接口	静态	静态	10.1.1.2/24	001c.5465.67c3	untrust	root	0	0 bps	0 bps	
Virtual Forward 接口	静态	静态	0.0.0.0/0	001c.5465.67c4	NULL	root	0	0 bps	0 bps	
回环接口	静态	静态	10.1.1.2/24	001c.5465.67c5	trust-1	root	0	0 bps	0 bps	
冗余接口	静态	静态	20.1.1.2/24	001c.5465.67c6	untrust-1	root	0	0 bps	0 bps	
以太网子接口	静态	静态	0.0.0.0/0	001c.5465.67c7	NULL	root	0	0 bps	0 bps	
冗余子接口	静态	静态	0.0.0.0/0	001c.5465.67c8	NULL	root	0	0 bps	0 bps	
冗余子接口	静态	静态	0.0.0.0/0	001c.5465.67c9	NULL	root	0	0 bps	0 bps	
VSwitch接口	静态	静态	0.0.0.0/0	001c.5465.67ca	NULL	root	0	0 bps	0 bps	
ethernet0/8	静态	静态	0.0.0.0/0	001c.5465.67cb	NULL	root	0	0 bps	0 bps	
tunnel1	静态	静态	99.99.99.1/24	0000.0000.0000	VPN-Hub	root	0	0 bps	0 bps	
vswitch1	静态	静态	0.0.0.0/0	001c.5465.67d3	NULL	root	0	0 bps	0 bps	

图 3-5 集聚接口配置界面

选择填写相关参数，完成集聚接口配置；



图 3-6 集聚接口配置界面

参数配置说明：

【名称】：对聚合接口起名

【描述】：对接口进行描述

【安全域】：三层接口对应三层安全域，二层接口对应二层安全域

【聚合方式】：选择聚合方式

【ip 配置】：配置接口的互联 ip 地址

【管理方式】：选择接口的管理方式

【端口配置】：将物理接口加入聚合口

2、聚合子接口配置：

首先创建聚合接口；



图 3-7 聚合接口配置界面

参数配置说明：

【安全域】：选择无绑定

【端口配置】：将物理接口加入聚合口

创建聚合子接口：

选择【新建】--【集聚子接口】进入集聚接口配置界面；

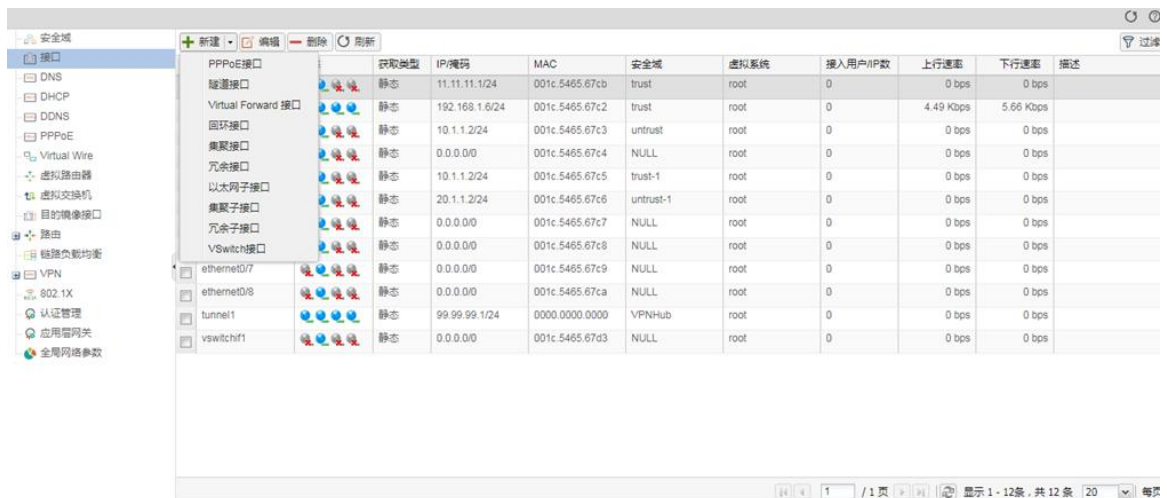


图 3-8 集聚子接口配置界面

选择填写相关参数，完成集聚接口配置；



图 3-9 集聚接口配置界面

参数配置说明：

【名称】：对聚合子接口起名【描述】：对接口进行描述

【安全域】：三层接口对应三层安全域，二层接口对应二层安全域

【ip 配置】：配置接口的互联 ip 地址

【管理方式】：选择接口的管理方式

3、配置普通物理接口

选中接口,选择【编辑】或者双击，即可配置相应接口属性；



图 3-10 接口配置视图

参数配置说明：

【描述】：对接口进行描述

【安全域】：三层接口对应三层安全域，二层接口对应二层安全域 【ip 配置】：配置接口的互联 ip 地址

【管理方式】：选择接口的管理方式

CLI 配置：

1、配置集聚接口：

在全局配置模式下输入以下命令创建聚合接口：

```
config
```

```
interface aggregate1
```

```
exit
```

在全局配置模式下使用以下命令将物理接口划入聚合接口：


```
config
```

```
interface e0/1
```

```
aggregate aggregate1
```

```
exit
```

在聚合接口配置模式下对聚合接口进行编辑：

```
config
```

```
interface aggregate1
```

```
zone trust (将接口划入 trust 安全域)
```

```
ip address 1.1.1.1/24 (配置接口 ip 地址)
```

```
manage ip 1.1.1.2 (配置设备管理接口只针对双机，也可以不配置)
```

```
description XX (对接口进行描述)
```

```
lACP enable (开启 LACP 协议)
```

```
manage http|https|telnet|ssh|ping|snmp|traceroute (开启接口的管理方式)
```

```
exit
```

显示接口信息：

```
show interface aggregate1
```

2、配置聚合子接口：

首先创建聚合接口：

在全局配置模式下输入以下命令创建聚合接口：

```
config
```

```
interface aggregate1
```

```
exit
```

在全局配置模式下使用以下命令将物理接口划入聚合接口：

```
config
```

```
interface e0/1
```

```
aggregate aggregate1
```

exit

接着创建聚合子接口并配置：

创建聚合子接口并对聚合子接口进行编辑：

config

interface aggregate1.100

zone trust （将接口划入 trust 安全域）

ip address 1.1.1.1/24 （配置接口 ip 地址）

manage ip 1.1.1.2 （配置设备管理接口只针对双机，也可以不配置）

description XX （对接口进行描述）

lACP enable （开启 LACP 协议）

manage http|https|telnet|ssh|ping|snmp|traceroute （开启接口的管理方式）

exit

显示接口信息：

show interface aggregate1.1

3、配置普通物理接口：

在全局配置模式下进入接口配置模式并对接口参数进行配置

config

interface e1/0

zone trust （将接口划入 trust 安全域）

ip address 1.1.1.1/24 （配置接口 ip 地址）

manage ip 1.1.1.2 （配置设备管理接口只针对双机，也可以不配置）

description XX （对接口进行描述）

lACP enable （开启 LACP 协议）

manage http|https|telnet|ssh|ping|snmp|traceroute （开启接口的管理方式）

exit

显示接口信息：

show interface e1/0

1.9 设备双机 HA 配置

HA 要求两台设备在软件版本、license、硬件型号、板卡数量及端口使用方面严格一一对应。

WEB 配置：

1、主防火墙配置：

选择界面视图的【系统】--【HA】；

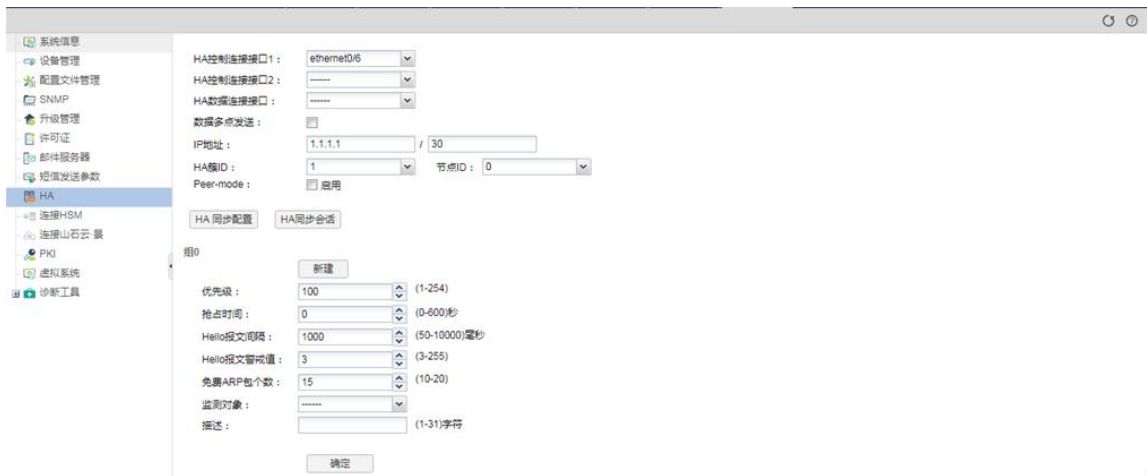


图 3-11 双机主设备配置

选择填写相关参数，完成 HA 的配置；



图 3-12 双机主设备配置

参数配置说明：

【HA 控制连接接口】：选择心跳接口，最多可以选择两个

【HA 数据连接接口】：选择心跳接口，可以使用集聚接口

【IP 地址】：配置同备机之间的心跳互联地址

【HA 簇 ID】：主备必须一样

【节点 ID】：主备分别为 0 和 1

【优先级】：默认 100，主设备建议 50，备设备 100，数值越小优先级越高

【抢占时间】：配置抢占

【检测对象】：触发检测对象后，主备进行切换

2、备防火墙配置：

选择界面视图的【系统】--【HA】；



图 3-13 双机主设备配置

选择填写相关参数，完成 HA 的配置。



图 3-14 双机主设备配置

参数配置说明：

【HA 控制连接接口】：选择心跳接口，最多可以选择两个

【IP 地址】：配置同主设备之间的心跳互联地址

【HA 簇 ID】：主备必须一样

【节点 ID】：主备分别为 0 和 1

【优先级】：默认 100，主设备建议 50，备设备 100，数值越小优先级越高

【抢占时间】：配置抢占，不建议备设备配置抢占

【检测对象】：触发检测对象后，主备进行切换

CLI 配置：

1. 主防火墙配置：

```
ha link interface ethernet0/X
ha link interface ethernet0/Y
ha link ip 1.1.1.1 255.255.255.252
ha group 0
priority 50 (优先级默认 100，越小优先级越高)
preempt
exit
ha cluster 1
```

2. 备防火墙配置：

```
ha link interface ethernet0/X
ha link interface ethernet0/Y
ha link ip 1.1.1.2 255.255.255.0
ha group 0
exit
ha cluster 1
```

1.10 路由配置

配置安全网关的缺省路由及回指路由，实现网关与其他设备通讯。

WEB 配置：

选择【网络】--【路由】--【目的路由】即可配置相应的路由条目；

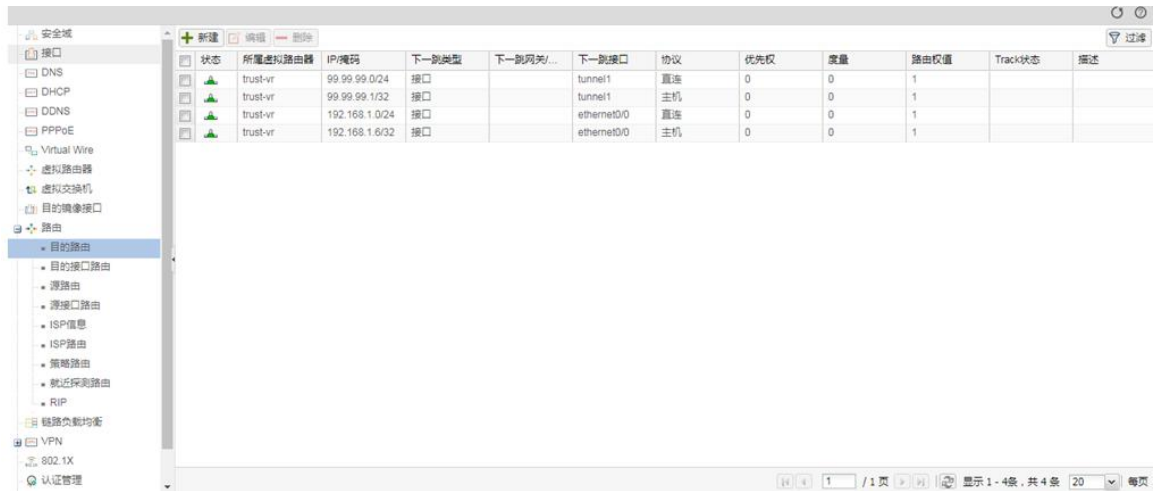


图 3-15 路由配置

选择【新建】进行路由添加或者修改。



图 3-16 路由配置

参数配置说明：

【目的地】：填写目的网段

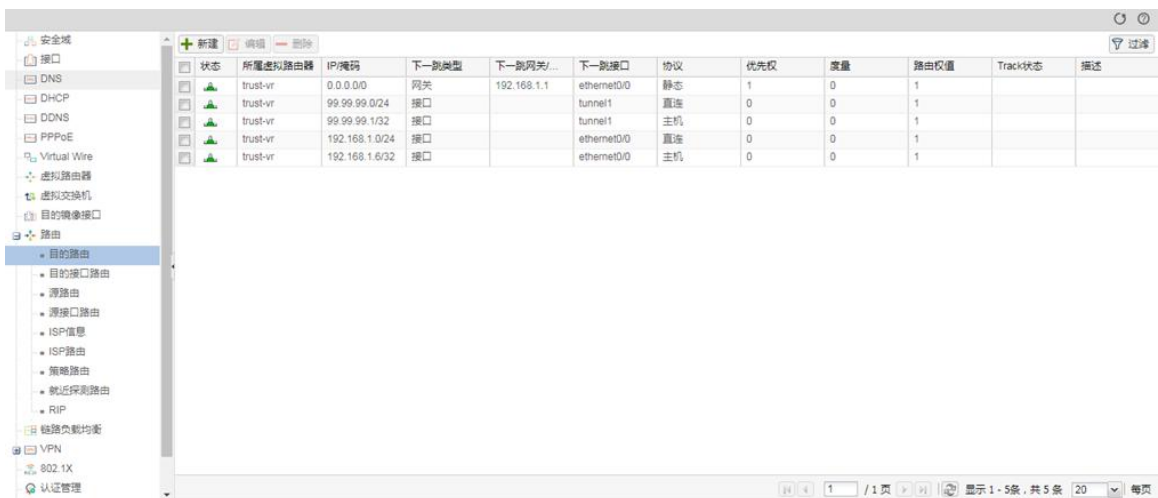
【子网掩码】：填写掩码

【下一跳】：选择路由的下一跳，没有特殊情况选择网关

【网关】：选择下一跳地址

【优先权】：优先权越小优先级越高

【路由权值】：两条等价路由按照权值分配流量



状态	所属虚拟路由器	IP掩码	下一跳类型	下一跳网关/...	下一跳接口	协议	优先权	度量	路由权值	Track状态	描述
🟢	trust-vr	0.0.0.0/0	网关	192.168.1.1	ethernet0/0	静态	1	0	1		
🟢	trust-vr	99.99.99.0/24	接口		tunnel1	直连	0	0	1		
🟢	trust-vr	99.99.99.1/32	接口		tunnel1	主机	0	0	1		
🟢	trust-vr	192.168.1.0/24	接口		ethernet0/0	直连	0	0	1		
🟢	trust-vr	192.168.1.6/32	接口		ethernet0/0	主机	0	0	1		

图 3-17 路由配置

CLI 配置：

在全局配置模式下输入以下命令进入路由配置模式：

`ip vrouter vrouter-name` vrouter-name 指定 VRouter 的名称，非特殊情况选择 trust-vr

在路由配置模式下使用以下命令创建路由：

```
ip route 10.0.0.0/8 2.2.2.2
```

使用以上命令 no 形式删除路由

```
no ip route 10.0.0.0/8 2.2.2.2
```

显示路由具体配置信息：

```
show ip route
```

1.11 日志配置

WEB 配置：

1. 日志服务器配置：

选择【监控】--【日志】--【日志管理】--【配置】--【日志服务器配置】即可进行日志服务器的配置。

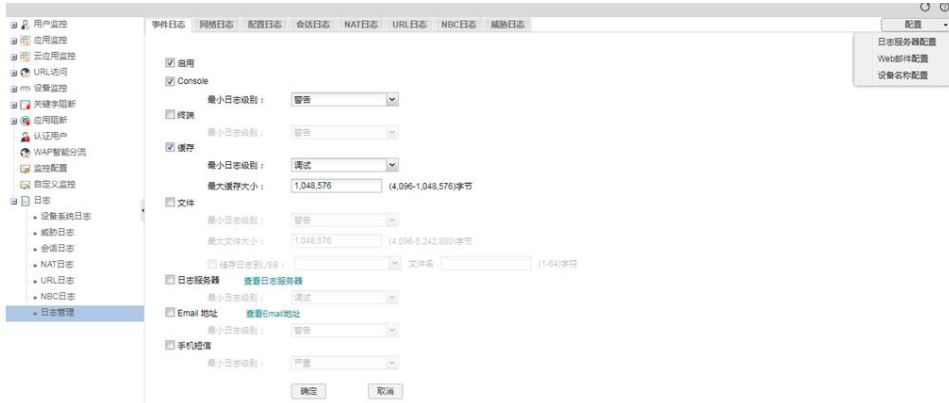


图 3-18 日志服务器配置

参数配置说明：

- 【主机名称】：填写服务器 ip 地址
- 【绑定方式】：填选择设备发送日志的出口
- 【协议】：选择日志发送使用的协议
- 【端口】：选择日志服务器开通的接口
- 【日志类型】：选择要发送的日志类型

2. 配置日志

选择【监控】--【日志】--【日志管理】选择日志的存储方式，对日志进行配置。



图 3-19 日志配置

CLI 配置:

开启或关闭相关日志功能, 在全局模式下:

开启: logging {event | security | configuration | network | traffic {session | nat | web-surfing} | debug | ips } on

关闭: no logging {event | security | configuration | network | traffic {session | nat | web-surfing} | debug | ips} on

将日志输出到相关模块, 在全局模式下:

开启: logging event to {console | remote | syslog| sms | email}

关闭: no logging event to {console | remote | syslog| sms | email}

配置日志服务器, 在全局模式下:

按 vrouter 发送:

logging syslog 40.81.208.2 vrouter "mgt-vr" udp 514 type event

按源接口发送:

logging syslog 40.81.208.2 source-interface "ethernet0/2" udp 514 type traffic session

1. 12 SNMP 配置

WEB 配置:

1. SNMP 配置:

选择【系统】--【SNMP】进入 SNMP 配置界面:



图 3-20 SNMP 配置

启用 SNMP 功能：

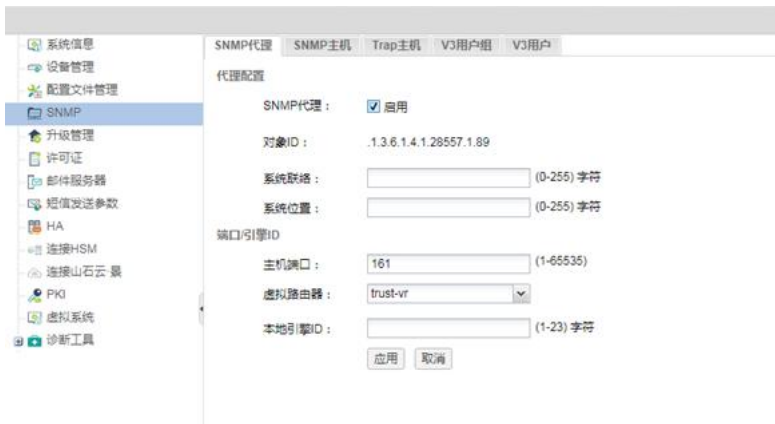


图 3-21 SNMP 功能开启配置

参数配置说明：

【SNMP】：选择启用开启 SNMP 功能

【主机端口】：选择服务端口，默认 161

2. 配置 SNMP 主机：

选择【SNMP 主机】新建 SNMP 主机，可以添加多个主机；

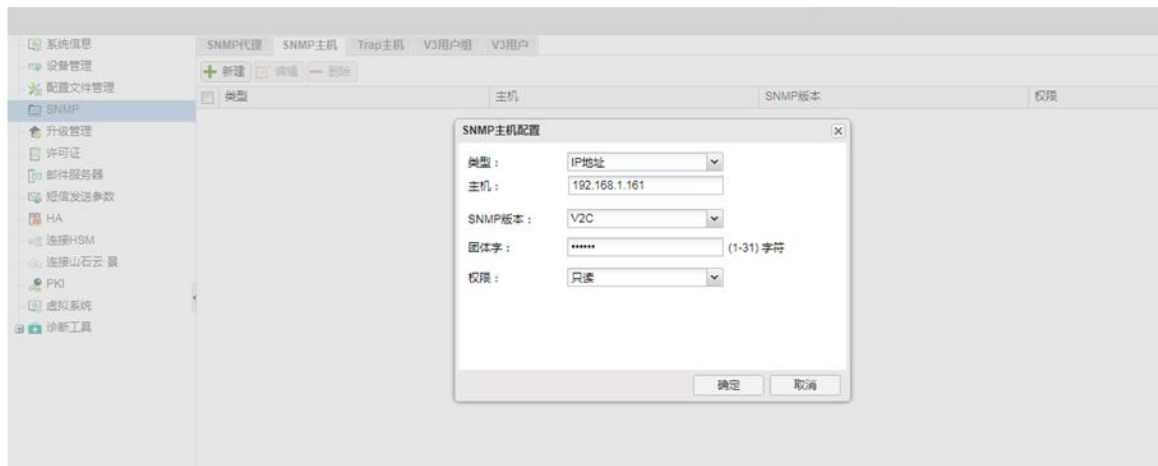


图 3-22 SNMP 主机配置

参数配置说明：

【类型】：选择 IP 地址形式

【主机】：填写 IP 地址

【SNMP 版本】：支持 V1/V2C/V3 三种版本

【团体字】：输入团体字

【权限】：有只读和只写两种权限

CLI 配置：

1. 启用 SNMP 服务，在全局模式下输入以下命令：

```
snmp-server manager
```

2. 定义 SNMP 服务端口号，在全局模式下输入以下命令：

```
snmp-server port 161
```

3. 配置 SNMP 源 vrouter：

```
snmp-server vrouter mgt-vr
```

4. 配置 SNMP 引擎 ID，在全局模式下输入以下命令：

```
snmp-server engineID ""
```

5. 指定管理主机的 IP 地址, 版本, 团体字符, 权限只读, 在全局模式下输入以下命令：

```
snmp-server host 192.168.30.4 version 2c community ro
```

6. 配置接收 SNMP trap 报文的 IP 地址, 版本, 团体字符, 端口号：

```
snmp-server trap-host 192.168.30.4 version 2c community port 162
```

1.13 NTP 配置

WEB 配置：选择【系统】--【设备管理】--【系统时间】进入 NTP 配置界面。



系统时间配置界面截图。左侧为系统管理菜单，包括系统信息、设备管理、配置文件管理、SNMP、升级管理、许可证、邮件服务器、短信发送参数、HA、连接+SM、连接山石云、PKI、虚拟系统、诊断工具。右侧为 NTP 配置区域，包含“设置系统时间”和“设置NTP”两个部分。

设置系统时间

与本地时间同步： 仅同步时间 同步时区与时间

时区：(GMT)GMT Standard Time

日期：2018/04/25

时间：14 时 37 分 25 秒

确定 取消

设置NTP

启用：

认证：

服务器	IP	密钥	虚拟路由器	源接口	操作
服务器1:	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	设置为默认服务器
服务器2:	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	设置为默认服务器
服务器3:	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	设置为默认服务器

同步间隔：5 (1-60) 分钟，缺省值：5，系统与NTP服务器同步的间隔时间

最大调整时间：10 (0-3600) 秒，缺省值：10，0表示没有时间限制

确定 取消

图 3-23 NTP 配置

启用 NTP 功能:



The screenshot shows the '设置NTP' (Configure NTP) interface. It includes a '启用' (Enable) checkbox which is checked, and an '认证' (Authentication) checkbox which is unchecked. Below these are three server configuration rows: '服务器1' (Server 1) with IP '192.168.1.161', '密钥' (Key) dropdown, '虚拟路由器' (Virtual Router) dropdown set to 'trust-vr', and '源接口' (Source Interface) dropdown set to 'ethernet0/0'. Each server row has a '设置为首选服务器' (Set as preferred server) link. At the bottom, there are fields for '同步间隔' (Sync Interval) set to '1' (1-60 minutes) and '最大调整时间' (Max Adjustment Time) set to '0' (0-3600 seconds). '确定' (OK) and '取消' (Cancel) buttons are at the bottom.

图 3-24 NTP 配置

参数配置说明:

【首选服务器】: 输入服务器地址

【密钥】: 如有需要选择密钥

【虚拟路由器】: 默认 trust-vr

【源接口】: 选择时间同步的设备接口

【启用】: 选择开启 NTP 服务 【认证】: 如有需要选择勾选

【同步间隔】: 与 NTP 服务器同步的间隔时间

【最大调整时间】: 在调整时间内可以成功进行同步, 在时间以外同步不成功

CLI 配置:

1. 启用 NTP 功能

```
ntp enable
```

2. 设置 NTP 服务器

```
ntp server x.x.x.x
```

3. 配置查询间隔

```
ntp query-interval
```

4. 配置最大调整时间

```
ntp max-adjustment 10
```

5. 配置身份验证

ntp authentication

6. 配置密钥

ntp authentication-key xx md5 xx

1.14 地址和服务对象

1.14.1 地址簿定义

地址簿是 CtyunOS 系统中用来储存 IP 地址范围与其名称的对应关系的数据库。地址簿中的 IP 地址与名称的对应关系条目被称作地址条目 (Address Entry)。地址条目的 IP 地址改变时, CtyunOS 会自动更新引用了该地址条目的模块。

WEB 配置:

选择【对象】--【地址簿】进入地址簿配置界面。



图 4-1 地址簿配置

选择【新建】建立新的地址簿。

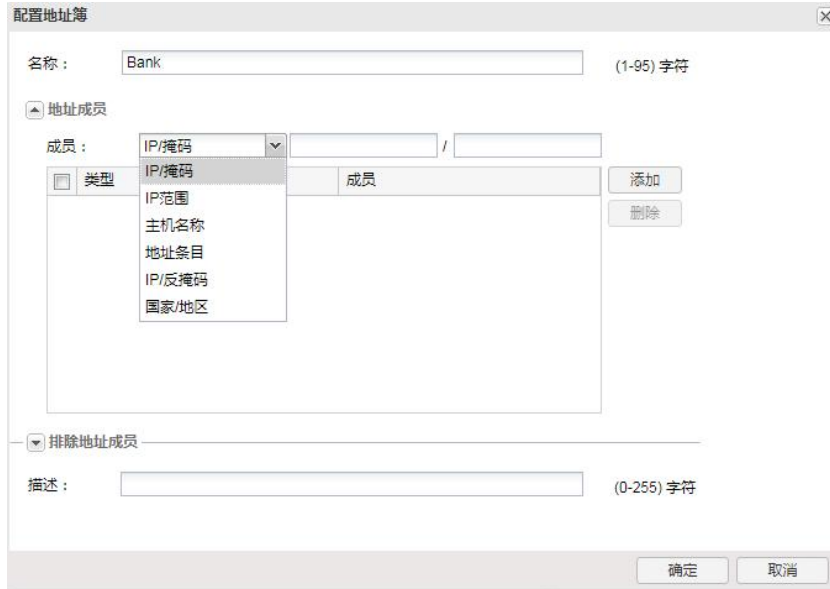


图 4-2 地址簿配置

参数配置说明：

【名称】：对所建地址簿命名

【成员】：选择地址簿成员对象，有四种方式可供选择

【描述】：对地址簿进行描述

CLI 配置：

1. 在全局配置模式，使用以下命令定义修改地址簿：

```
address address-entry
```

2. 在地址配置模式下，使用以下命令来为地址簿添加条目：

```
ip ip/netmask IP 地址段
```

```
host host-name 主机名
```

```
range min-ip [max-ip] IP 地址范围
```

```
member address-entry 地址簿成员嵌套
```

3. 在地址配置模式下，使用以下命令来为地址簿删除条目：

```
no ip ip/netmask
```

```
no host host-name
```

no range min-ip [max-ip]

no member address-entry

4. 查看地址簿信息：

show address [address-entry]

1.14.2 服务簿定义

服务 (Service)：具有协议标准的信息流。服务具有一定的特征，例如相应的协议、端口号等。

服务组：将一些服务组织到一起便组成了服务组。用户可以直接将服务组应用到防火墙策略中，这样便简化了管理。

WEB 配置：选择【对象】--【服务簿】进入服务簿配置界面

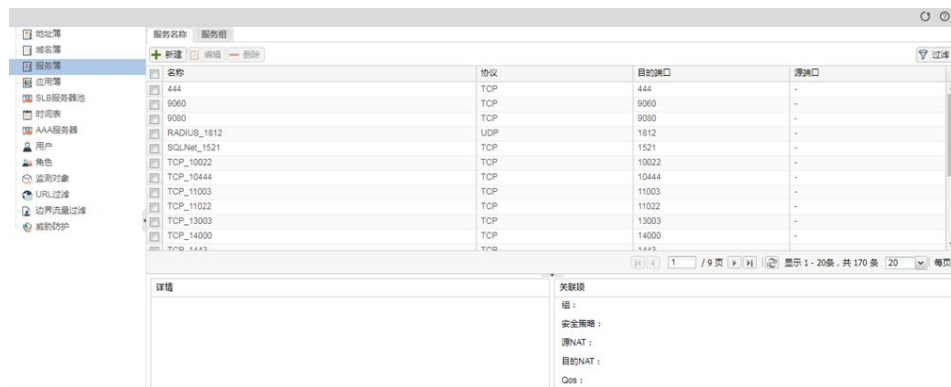


图 4-3 新建服务配置在【新建】中选择服务建立新的服务簿。

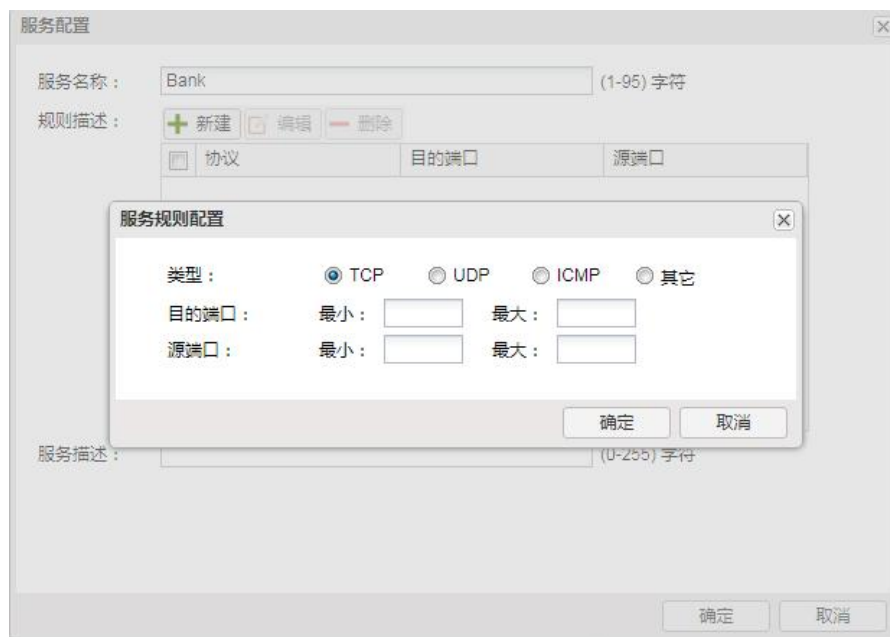


图 4-4 新建服务配置

参数配置说明：

【名称】：对所建服务命名

【成员】：选择服务的类型及端口，源端口默认 1-65535

【描述】：对地址簿进行描述

选择【对象】--【服务簿】进入地址簿配置界面。



图 4-5 服务组配置

在【新建】中选择服务建立新的服务组。

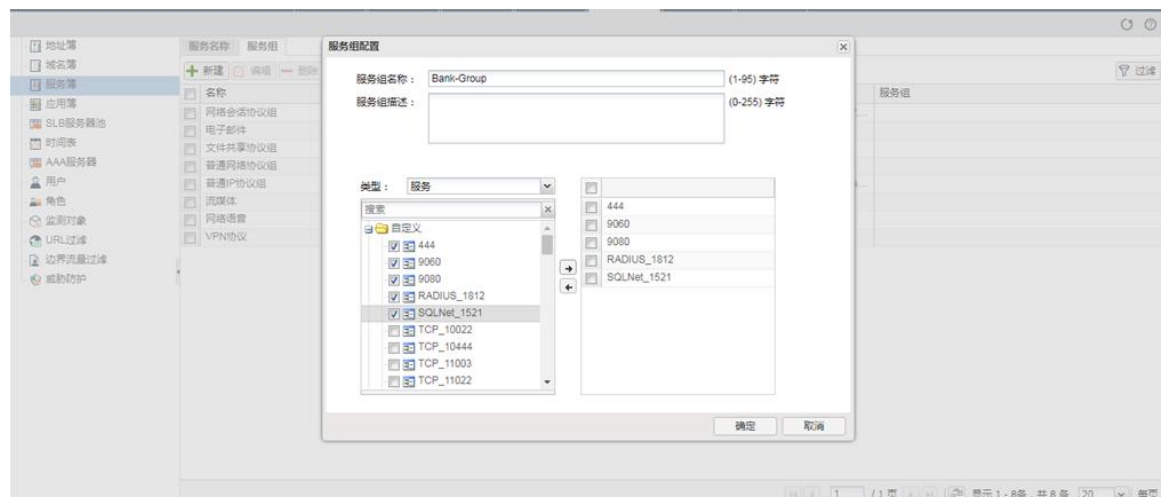


图 4-6 服务组配置

参数配置说明：

【名称】：对所建服务组命名

【成员】：选择服务加入服务组

【描述】：对服务组进行描述

CLI 配置：

1. 服务簿配置：

新建新的服务簿，在全部配置模式下输入以下命令：

service name 添加服务协议及端口，在服务簿配置模式下输入以下命令：

tcp dst-port 8000 添加 tcp 8000 端口

tcp dst-port 8010 8020 添加 tcp 8010-8020 端口

在以上命令前加 no 删除相应配置。

2. 服务组配置：

新建新的服务组，在全部配置模式下输入以下命令：

servgroup name 添加相应服务到服务组，在服务组配置模式下输入以下命令：

service HTTP 添加 HTTP 服务到服务组

service HTTPS 添加 HTTPS 服务到服务组

在以上命令前加 no 删除相应配置。

1.15 策略配置

1.15.1 安全策略介绍

策略是网络安全设备的基本功能。默认情况下，安全设备会拒绝设备上所有安全域之间的信息传输。而策略则通过策略规则（Policy Rule）决定从一个安全域到另一个安全域的哪些流量该被允许，哪些流量该被拒绝。

1.15.2 策略规则的基本元素

策略规则允许或者拒绝从一个（多个）安全域到另一个（多个）安全域/从一个地址段到另一个地址段的流量。流量的类型、流量的源安全域/源地址与目的安全域/目的地址以及行为构成策略规则的基本元素。

Source Zone/Address - 流量的源安全域/源地址。

Destination Zone/Address - 流量的目的安全域/目的地址。

Service - 流量的服务类型。

Action – 安全设备在遇到指定类型流量时所做的行为，包括允许（Permit）、拒绝（Deny）、隧道（Tunnel）、来自隧道（Fromtunnel）以及 Web 认证五个行为。

1. 15.3 策略规则及匹配顺序

策略规则分为两部分：过滤条件和行为

安全域间流量的源安全域/源地址、目的安全域/目的地址、服务类型以及角色构成策略规则的过滤条件。

对于匹配过滤条件的流量可以制定处理行为，如 Permit 或 Deny 等。

策略匹配顺序：系统查找策略顺序为由上至下，对流量按照找到的第一条与过滤条件相匹配的策略规则进行处理。

系统缺省的策略是拒绝所有流量。

1. 15.4 配置策略规则

WEB 配置：

选择【策略】--【安全策略】--【新建】创建新的策略：

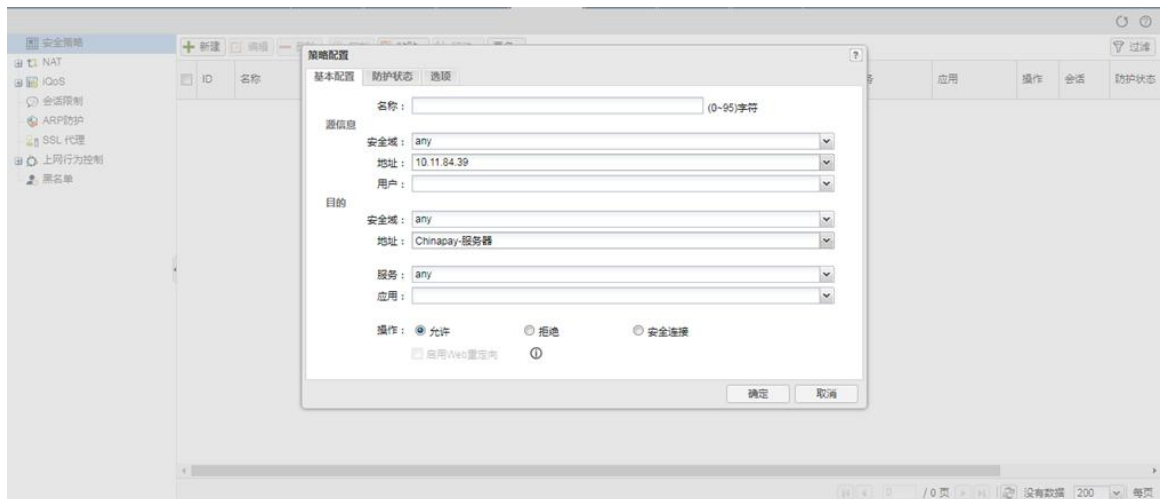


图 4-7 新建策略配置

参数配置说明：

【名称】：对所建策略命名

【源安全域】：流量流入的安全域

【目的安全域】：流量流出的安全域

【源地址】：选择地址或者地址簿，可以选择多个

【目的地址】：选择地址或者地址簿，可以选择多个

【服务簿应用簿】：选择相应的服务或者应用，不填写默认是 any

【时间表】：在时间表内策略生效，不填写默认策略没有时间限制

【行为】：选择允许或者拒绝

选择【选项】可以设置策略的优先级

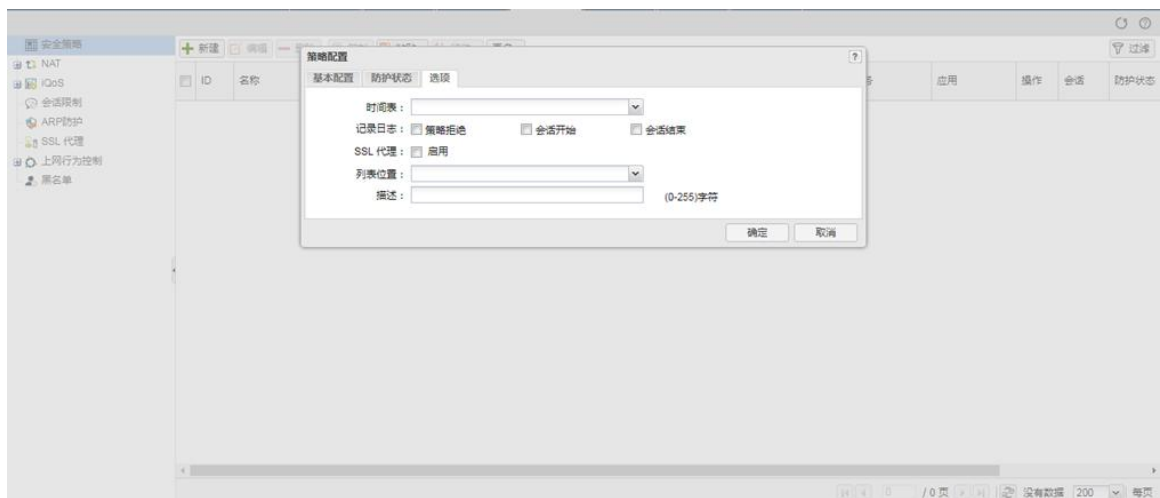


图 4-8 策略配置

参数配置说明：

【记录日志】：对命中策略的会话进行日志记录，需要开启会话日志

【列表位置】：对策略优先级进行调整，位置越靠前优先级越高

CLI 配置：

1. 进入策略配置模式，在全局配置模式下输入以下命令：

```
policy-global
```

2. 配置策略规则，在策略配置模式下输入以下命令：

```
rule id id- 指定策略规则的 ID，系统可以自动分配一个 ID；
```

```
top | before id | after id – 指定策略规则的位置；
```

默认情况下，系统会将新创建的策略规则放到所有规则的末尾；

```
src-addr – 指定策略规则的源地址条目；
```

- src-ip – 指定策略规则的源地址条目；
- dst-addr – 指定策略规则的目的地址条目；
- dst-ip – 指定策略规则的源地址条目；
- service service-name – 指定策略规则的服务名称；
- permit | deny 指定策略规则的行为；

3. 配置策略规则，在策略配置模式下输入以下命令：

```
show policy [id id] [from src-zone] [to dst-zone]
```

id id – 显示指定 ID 规则的详细信息；

from src-zone – 显示源安全域为指定域的规则的详细信息；

to dst-zone – 显示目标安全域为指定域的规则的详细信息。

4. 移动策略优先级，在策略配置模式下输入以下命令：

```
move id {top | bottom | before id | after id}
```

1.16 ALG 配置

WEB 配置：

选择【网络】--【应用层网关】：



CLI 配置：

在全局配置模式下输入以下命令开启或关闭 ALG 模块：

开启：alg XX

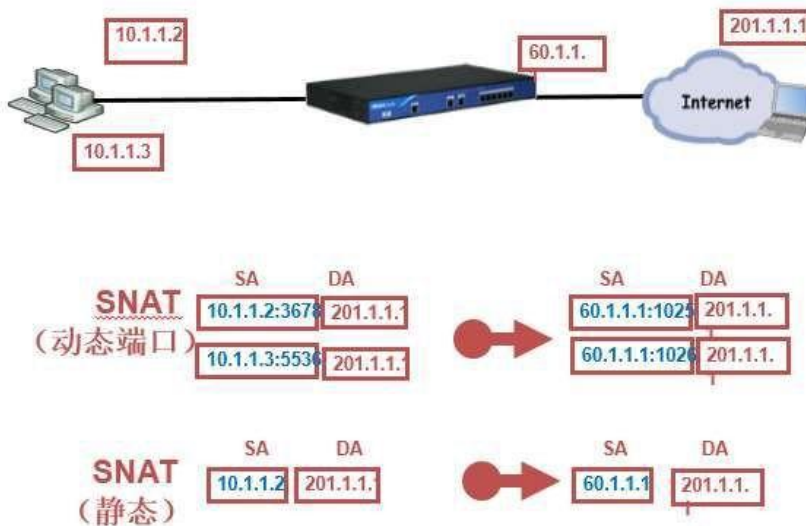
关闭: no alg xx

1.17 NAT 配置

网络地址转换 (NetworkAddressTranslation) 简称为 NAT, 是将 IP 数据包包头中的

IP 地址转换为另一个 IP 地址。当 IP 数据包通过路由器或者防火墙时, 路由器或者防火墙会把 IP 数据包的源 IP 地址和/或者目的 IP 地址进行转换。在实际应用中, NAT 主要用于私有网络访问外部网络的情况。

1.17.1 NAT 转换过程 (源 NAT)



WEB 配置:

选择【策略】--【NAT】, 点击【源 NAT】项, 点击『新建』按钮创建源 NAT 规则, 如图所示:

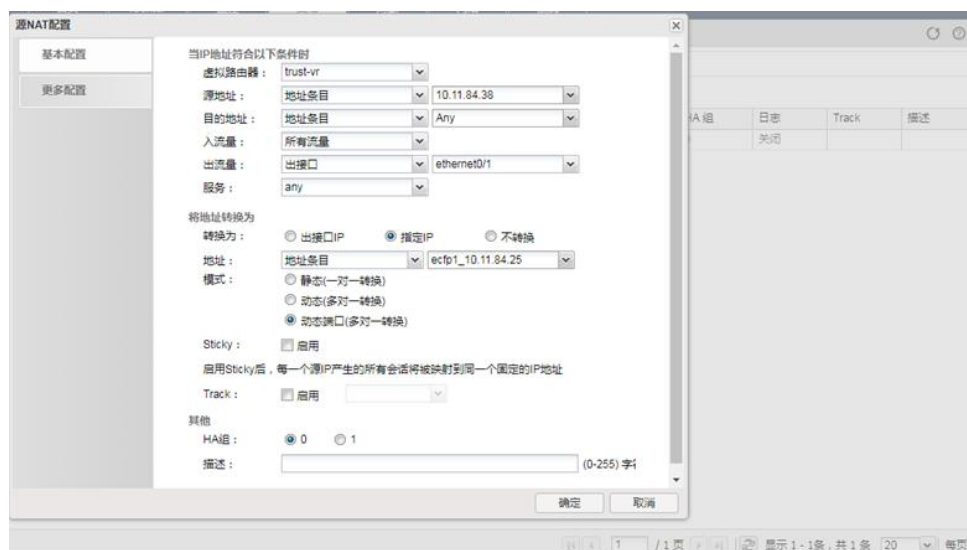


图 4-9 源 nat 转换

CLI 配置:

在 VR 配置模式下, 使用以下命令:

```
snatrule [id id] [before id | after id | top] from src-address to dst-address
[eif egress-interface] trans-to {addressbook trans-to-address | eif-ip} mode
{static | dynamicip | dynamicport [sticky]} [log]
```

id id - 为 SNAT 规则指定 ID 号。

before id | after id | top - 指定规则所在的位置

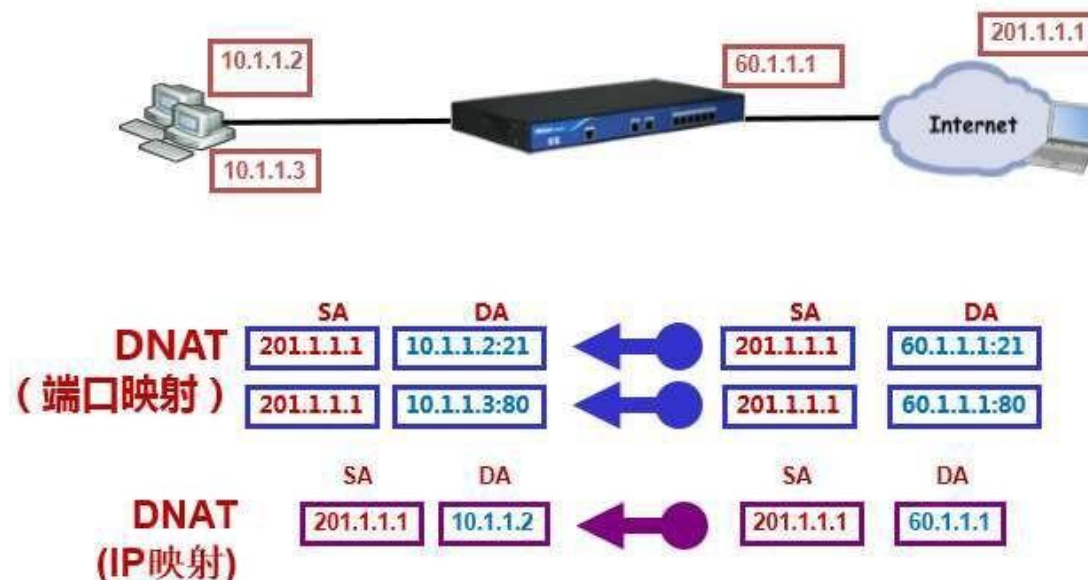
from src-address to dst-address [eif egress-interface] - 指定该规则中流量应符合的条件。

eif egress-interface - 指定流量的出接口。

addressbook trans-to-address | eif-ip - 指定 NAT 转换地址。

mode {static | dynamicip | dynamicport [sticky]} - 指定转换模式。

1. 17.2 NAT 转换过程 (目的 NAT)



WEB 配置:

选择【策略】--【NAT】, 点击【目的 NAT】项, 点击『新建』按钮创建目的 NAT 规则, 如图

所示：

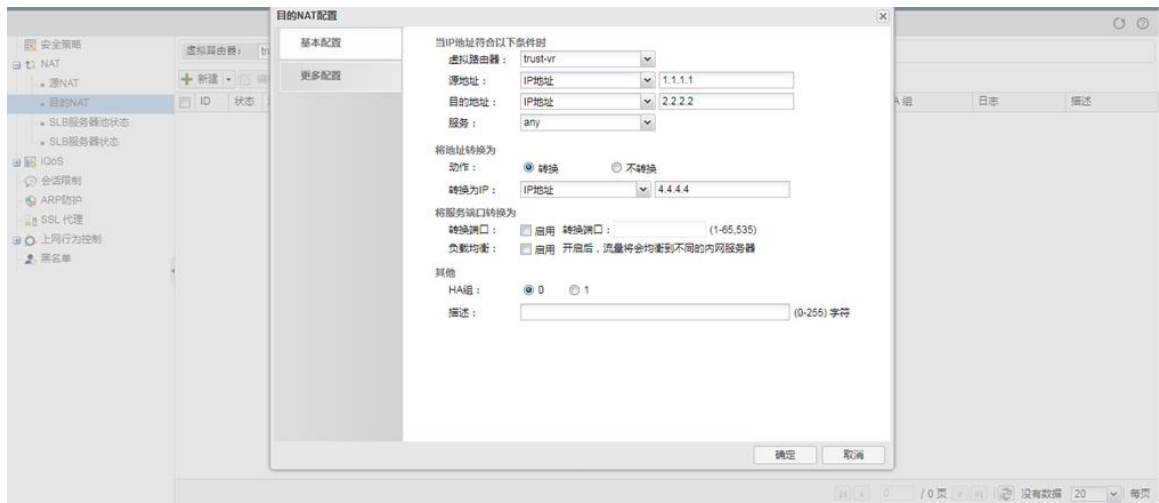


图 4-10 目的 nat 配置

CLI 配置：

在 VRouter 配置模式下，使用以下命令：

```
dnatrul [id id] [before id | after id | top] from src-address to dst-address  
[service servicename]trans-to trans-to-address [port port] [load-balance  
[ping-track]] [log]
```

NAT 规则：

NAT 分为源 NAT 和目的 NAT，源 NAT 由多条源 NAT 规则组成，目的 NAT 由多条目的 NAT 规则组成。当定义多条 NAT 规则时，需要根据需求移动 NAT 规则位置。

NAT 规则匹配顺序：

每一条 NAT 都有唯一一个 ID 号。流量进入防火墙时，防火墙对 NAT 规则进行顺序查找，然后按照查找到的相匹配的第一条规则对流量的源 IP 做 NAT 转换。ID 的大小顺序并不是规则匹配顺序。使用 showsnat/dnat 命令列出的规则顺序才是规则匹配顺序。通过移动已有的 NAT 规则从而改变规则的排列顺序。

注意：定义防火墙策略时，源和目的地址要使用 NAT 前的地址。

1.18 常用诊断工具

1.18.1 查看系统日志

云下一代防火墙安全产品提供了用于监控系统事件和网络流量的事件日志以及便于系统管理员分析和跟踪设备各种问题情况。CtyunOS 的日志信息分为七种，分别是事件 (Event) 日志信息、告警 (Alarm) 日志信息、安全 (Security) 日志信息、配置 (Configuration) 日志信息、网络 (network) 日志信息、流量 (Traffic) 日志信息和调试 (Debug) 日志信息。日志信息根据严重级别的不同，又可以分为 8 级别。

日志信息严重性级别分类：

- Emergency (紧急) 级别 0：系统不可用信息。
- Alert (警示) 级别 1：需要立即处理的信息，如设备受到攻击灯。
- Critical (关键) 级别 2：危急信息，如硬件出错。
- Error (错误) 级别 3：错误信息。
- Warning (警告) 级别 4：报警信息。
- Notification (通知) 级别 5：非错误信息，但需要特殊处理。
- Information (信息) 级别 6：通知信息。
- Debugging (调试) 级别 7：调试信息，包括正常的使用信息。

1.18.2 查看系统进程

```
hostname # show process
```

```
Tasks: 50 total, 6 running, 44 sleeping, 0 stopped
```

Pid	Process	State	Priority	Cpu(%)	Memory(%)	Runtime
1267	chassisd	R	18	1.4	0.5	0:29.47
1292	routed	S	20	0.5	0.5	2:02.91
1240	monitord	S	0	0.0	0.5	1:14.40

1268	mgd	S	20	0.0	1.0	0:17.18
1276	admind	S	20	0.0	0.4	0:00.73
1277	updated	S	20	0.0	0.5	0:00.91
1278	cloud	S	20	0.0	0.6	0:02.31
1279	dnisd	S	20	0.0	0.4	0:03.00
1280	logd	S	20	0.0	0.5	0:02.48
1281	telnetd	S	20	0.0	0.3	0:00.53
1282	ftpd	S	20	0.0	0.4	0:00.46
1283	pkid	S	20	0.0	0.5	0:01.56
1284	sshd	S	20	0.0	0.5	0:01.08
1285	pam	S	20	0.0	0.4	0:01.85
1286	lacpd	S	20	0.0	0.3	0:00.96
1287	smsspd	S	20	0.0	0.3	0:00.32
1288	netd	S	20	0.0	1.7	1:16.18
1289	rstpd	S	20	0.0	0.2	0:01.42
1290	nbcd	S	20	0.0	0.3	0:10.32
1291	nbcxd	S	20	0.0	0.4	0:00.68
1293	mrouted	S	20	0.0	0.3	0:01.64
1294	dhcpcd	S	20	0.0	0.4	0:00.53
1295	ntpd	S	20	0.0	0.4	0:00.57
1296	vpnd	S	20	0.0	0.5	0:01.99
1297	smssd	S	20	0.0	0.3	0:00.12
1299	sslvpcd	S	20	0.0	0.7	0:01.62
1300	l2tpd	S	20	0.0	0.4	0:01.68
1301	httpd	S	20	0.0	1.4	0:12.27
1303	agent	S	20	0.0	0.7	0:00.99

1305	nmagent	S	20	0.0	1.6	2:14.10
1306	pppoed	S	20	0.0	0.3	0:01.83
1307	cellulard	S	20	0.0	0.4	0:01.38
1308	ddnsd	S	20	0.0	0.4	0:00.73
1309	scheduled	S	20	0.0	0.3	0:01.63
1311	httpauth	S	20	0.0	0.4	0:00.71
1313	dot1x	S	20	0.0	0.4	0:01.34
1315	tr69	S	20	0.0	0.4	0:00.65
1316	netbiosd	S	20	0.0	0.4	0:00.76
1840	login	S	20	0.0	0.3	0:00.39
1861	httpauth	S	20	0.0	0.1	0:00.00
1862	httpauth	S	20	0.0	0.3	0:00.59
1887	d-plane	R	0	0.0	0.8	494:22.33
1888	d-plane	S	20	0.0	0.6	0:04.36
1889	d-plane	R	0	0.0	0.5	494:21.62
1890	d-plane	R	0	0.0	0.5	494:21.96
1891	d-plane	S	20	0.0	0.8	0:42.81
2032	monitord	S	20	0.0	0.3	0:00.90
2038	d-plane	S	20	0.0	0.2	0:04.98
3750	sshd	S	20	0.0	0.5	0:00.10
3751	cli	S	20	0.0	0.8	0:00.10

1. 18.3 查看会话情况

hostname # show session ?

<cr>

| Output modifiers

application	Show session by application name
core-mask	Show session by core mask
deny	Show deny session
detail	Show QoS marking and queue id cached in session
dst-addr	Show session of dstination address entry
dst-ip	Show session of destination ip
dst-port	Show session of destination port
generic	Show generic session info
h323	Show H.323 session
id	Show session by session ID
ipv4	Show session of ipv4
ipv6	Show session of ipv6
policy	Show session by policy id
protocol	Show session of protocol
src-addr	Show session of source address entry
src-ip	Show session of source ip
src-port	Show session of source port
sync	Show HA synced session
tunnel	Show tunnel session
unsync	Show HA unsynced session
vrouter	Show session of vrouter
vsys	Show session by VSYS

```
SG-6000# show session dst-ip 192.168.71.59 dst-port 3389
```

```
session: id 42, proto 6, flag 20000004, flag1 20000, created 30242, life 691192, policy  
11,app 16382(3389) flag 0x0, auth_user_id 0, reverse_auth_user_id 0
```

flow0(10(ethernet0/0)/40200810): 192.168.71.1:51193->192.168.71.59:3389

flow1(11(ethernet0/1)/200810): 10.10.10.100:3389->192.168.71.1:51193

1. 18. 4 查看 ARP

hostname # show arp

Total entries: 4

Flag: I:Authenticated ARP Driver incompatible; N:Secure Defender not installed

Protocol	Address	Age(sec)	Hardware Addr	Type	Flag	Interface/VR
Internet	10.10.10.100	255	0050.56b6.0a1c	ARPA		ethernet0/1
Internet	192.168.71.1	224	001c.5449.4c8d	ARPA		MGT0
Internet	192.168.71.51	222	000c.296a.1f49	ARPA		MGT0
Internet	192.168.71.1	195	001c.5449.4c8d	ARPA		ethernet0/0

1. 18. 5 查看路由

hostname # show ip route

Codes: K - kernel route, C - connected, S - static, I - ISP, R - RIP, O - OSPF,

B - BGP, D - DHCP, P - PPP, H - HOST, G - SCVPN, V - VPN, M - IMPORT,

Y - SYNC, L - llb outbound, > - selected first nexthop, * - FIB route, b - BFD enable

Routing Table for Virtual Router <trust-vr>

C>* 10.10.10.0/24 is directly connected, ethernet0/1

H>* 10.10.10.254/32 [0/0/1] is local address, ethernet0/1

C>* 172.16.10.0/24 is directly connected, ethernet0/2

H>* 172.16.10.254/32 [0/0/1] is local address, ethernet0/2

C>* 192.168.71.0/24 is directly connected, ethernet0/0

H>* 192.168.71.53/32 [0/0/1] is local address, ethernet0/0

Routing Table for Virtual Router <mgt-vr>

C>* 192.168.71.0/24 is directly connected, MGT0

H>* 192.168.71.52/32 [0/0/1] is local address, MGT0

1. 18. 6 查看 FIB

hostname # show fib

U-up; G-gateway; H-host; C-connected; B-blackhole; N-subnet broadcast;

P-track failed; S-switch over; I-interface; V-vrouter; L-link full

IPv4 Forwarding Table for Virutal Router <trust-vr>

Destination	Gateway	Flags	Interface	Weight
10.10.10.0/24	0.0.0.0	UC	ethernet0/1	1/1/1
10.10.10.254/32	10.10.10.254	UH	ethernet0/1	1/1/1
10.10.10.255/32	10.10.10.255	UN	ethernet0/1	1/1/1
172.16.10.0/24	0.0.0.0	UC	ethernet0/2	1/1/1
172.16.10.254/32	172.16.10.254	UH	ethernet0/2	1/1/1
172.16.10.255/32	172.16.10.255	UN	ethernet0/2	1/1/1
192.168.71.0/24	0.0.0.0	UC	ethernet0/0	1/1/1
192.168.71.53/32	192.168.71.53	UH	ethernet0/0	1/1/1
192.168.71.255/32	192.168.71.255	UN	ethernet0/0	1/1/1

IPv4 Forwarding Table for Virutal Router <mgt-vr>

Destination	Gateway	Flags	Interface	Weight
-------------	---------	-------	-----------	--------

192.168.71.0/24	0.0.0.0	UC	MGT0	1/1/1
192.168.71.52/32	192.168.71.52	UH	MGT0	1/1/1
192.168.71.255/32	192.168.71.255	UN	MGT0	1/1/1

1. 18. 7 检查连通性

```
hostname(config)# ping 10.188.9.1
```

```
Sending ICMP packets to 10.188.9.1
```

```
Seq ttl time(ms)
```

```
128 2.23
```

```
128 1.91
```

```
128 1.92
```

```
128 1.87
```

```
128 2.02
```

```
statistics: 5 packets sent, 5 received, 0% packet loss, time 4003ms rtt min/avg/max/mdev  
= 1.875/1.997/2.238/0.133 ms hostname(config)# traceroute 202.106.0.20 traceroute to  
202.106.0.20 (202.106.0.20), 30 hops max, 52 byte packets
```

```
10.188.9.1 2.367 ms 2.912 ms 2.175 ms
```

```
122.200.95.33 19.957 ms 19.943 ms 7.895 ms
```

```
172.86.100.1 7.899 ms 5.786 ms 3.579 ms
```

```
203.86.64.253 4.366 ms 5.123 ms 4.332 ms
```

```
203.86.64.150 11.439 ms 10.063 ms 26.339 ms
```

```
219.142.5.181 33.395 ms 23.490 ms *
```

```
219.141.130.65 6.215 ms 7.209 ms 6.586 ms
```

```
219.141.130.93 5.784 ms 6.029 ms 11.085 ms
```

```
202.97.57.217 7.944 ms * 202.97.57.213 5.980 ms
```

1.19 防火墙故障排查步骤

1.19.1 软件部分

1、并发会话检查

在防火墙上执行命令：`show session generic`

每个防火墙的并发会话都有一个最大值，如果超出最大值说明防火墙并发会话已经达到极、限，防火墙成为一性能瓶颈，需要升级到更高档次防火墙。

会话信息如包含 `alloc failed` 说明防火墙会话曾经达到最大值，防火墙会话建立失败，可能是防火墙性能的问题或曾经出现网络攻击现象；

```
# show session generic
```

```
VSYS 0, max 200000, allocated 0, deny session 0, free 200000, tunnel 0, alloc failed 0
```

2、CPU 利用率检查

防火墙的 CPU 主要任务为执行功能、会话、日志等管理功能，一般情况下 CPU 利用率不会太高，建议不超过 60%。防火墙 CPU 统计有 1 分钟、5 分钟、15 分钟平均值。在某一时间段 CPU 利率较高，属异常现象，可能有攻击等情况发生。CPU 利用率持续较高，说明防火墙配置错误，需要调整防火墙配置，以降低 CPU 利用率。

```
# show cpu
```

```
Average cpu utilization : 0.2%
```

```
current cpu utilization : 2.0%
```

```
Last 1 minute : 0.1%
```

```
Last 5 minutes : 0.2%
```

```
Last 15 minutes : 0.2%
```

3、内存使用率检查

在防火墙内执行 `show memory` 查看内存利用率；

```
# show memory
```

```
The percentage of memory utilization: 25%
```

```
total(kB)    used(kB)    free(kB)
```

524288 132793 391495

4、查看重要日志

云下一代防火墙安全产品提供了用于监控系统事件和网络流量的事件日志以及便于系统管理员分析和跟踪设备各种问题情况。CtyunOS 的日志信息分为七种，分别是事件 (Event) 日志信息、告警 (Alarm) 日志信息、安全 (Security) 日志信息、配置 (Configuration) 日志信息、网络 (network) 日志信息、流量 (Traffic) 日志信息和调试 (Debug) 日志信息。日志信息根据严重级别的不同，又可以分为 8 级别。

日志信息严重性级别分类：

- Emergency (紧急) 级别 0: 系统不可用信息。
- Alert (警示) 级别 1: 需要立即处理的信息，如设备受到攻击灯。
- Critical (关键) 级别 2: 危急信息，如硬件出错。
- Error (错误) 级别 3: 错误信息。
- Warning (警告) 级别 4: 报警信息。
- Notification (通知) 级别 5: 非错误信息，但需要特殊处理。
- Information (信息) 级别 6: 通知信息。
- Debugging (调试) 级别 7: 调试信息，包括正常的使用信息。

查看一些日志信息如下：

```
show logging event
```

```
show logging alarm
```

```
show logging security
```

5、路由检查

防火墙在路由模式下工作时，防火墙数据转发跟系统路由相关，检查路由设置是否正确。

```
# show ip route
```

```
Codes: K - kernel route, C - connected, S - static, I - ISP, R - RIP, O - OSPF,
```

```
        B - BGP, D - DHCP, P - PPPoE, H - HOST, G - SCVPN, V - VPN, M - IMPORT,
```

```
        > - selected route, * - FIB route
```


Routing Table for Virtual Router <trust-vr>

```
=====
=====
C>* 192.168.1.0/24 is directly connected, ethernet0/0
H>* 192.168.1.1/32 [0/0/1] is local address, ethernet0/0
=====
=====
```

6、查看系统信息

获得系统的重要信息。可将该信息提交给天翼云研发人员进行定位分析。

show tech-support

7、debug 定位分析

详见 5.4

1. 20 故障信息收集

1. 20. 1 CPU 异常升高

在设备运行过程中，当 CPU 过高影响业务时，需要收集些故障信息来进行分析定位，具体方法如下：

1、检查设备开启的功能，具体如下：

1)Show statistics-set //查看设备开启统计集,如果开启统计集较多，建议关闭一些没用的统计集。

2)查看设备是否开启 debug，并在不用时将其关闭。

Show debug //查看 debug 开启情况

Undebug all 或连续按两下 Esc //关闭 debug

3)Show session-limit // 查看设备是否开启

session-limit,查看 session-limit 是否有 drop,如有没有 drop 记录建议关闭相应 session-limit.

2、分析实际情况

1)查看设备是否有攻击。Show logging security 和 show ad zone trust/untrust statistics 查看 AD 攻击情况。

2)show statistics-set predef_rampup_ip \查看设备当前新建会话情况，看看有没有新建会话数很高的 ip。

开启此统计集方法：

```
config
```

```
statistics-set predef_rampup_ip
```

```
target-data rampup-rate record-history
```

```
group-by ip
```

```
active
```

```
exit
```

在查看完毕时可以适当关闭此统计集，方法如下：

```
no statistics-set predef_rampup_ip
```

3)比对现有配置与原配置区别。在情况允许的情况下查看配置日志，主要观察在 cpu 高之前的一些配置信息。

4)通过 show process 命令查看当前占用 CPU 较多的进程，重点关注 D_plane 之外的进程，看哪些比较高，如果都是 D_plane 进程占用的最高，基本上可以确认是性能达到了极限。设备 process 进程数很多，具体进程表示什么意思请联系厂商工程师咨询。

5)show cpu detail //查看 CPU 按时间、按 core 的分布情况，查看具体哪些 core 较高。

6)通过 show logging 查看相应的日志开启及发送情况，将不必要的日志关闭。

```
show logging //查看系统日志开启情况
```

```
no logging traffic on //关闭 traffic log
```

```
no logging alarm to console //关闭 alarm 日志发送到 console
```

7)关闭 av 检查中的 rar、zip、bzip2，并在命令行输入 av max-decompression-length 64

1. 20. 2 会话数异常升高

在设备运行过程中，当设备并发会话数过高影响业务时，需要收集些故障信息来进行分析定位，具体方法如下：

1、查看并发会话情况

```
SG-6000# show session generic
```

Device: max 100000, alloc 0, deny session 0, free 100000, tunnel 0, alloc failed 0

2、查看用户/IP 会话统计集，是否有某个 IP 会话数异常升高

SG-6000# show statistics-set predef_user_sess current

3、查看安全日志，是否有 dos 攻击导致占用大量会话数（只记录 log 没有 drop 的 ad 行为）

SG-6000# show logging security

1. 20.3 防火墙主备切换

在设备双机模式运行过程中，发现非人为切换而进行主备切换后，需要收集些故障信息来进行分析定位，具体方法如下：

在主备墙上分别查看

1、查看 alarm 日志，查看切换的时间和原因

show logging alarm

show ha group 0

2、查看本端 ha 和对端 ha 状态

3、show tech-support toconsole 命令收集大量有用信息提供给厂商

1. 20.4 丢包或者业务中断

在设备运行过程中，当出现丢包情况或者业务中断时，需要收集些故障信息来进行分析定位，具体方法如下：

1.外部接口

Show interface ex/y 查看双工、速率的协商是否正常

show controller slot 0 port x statistic 是否存在坏包，如果存在，可以尝试：更换网线；手动指定两互联设备的双工和速率

show statistics interface-counter interface ethernet0/x second 接口带宽是否已占满

2.SWITCH 是否丢包

show controller slot 0 bri statistic 中的 Tail Dropped Packet Counter:是否有丢包

3. Internal 接口

Show controller slot 0 port x statistic 查看是否有坏包，如果有可能存在硬件问题

4. CPU 和 packet buffer

show cpu/detail CPU 利用率高，一般是性能不够或者存在攻击

show cpu-cntr 查看是否有 drop、error 信息；drop 一般是性能不够，error 可能存在硬件问题

show dp-r packet-buffer:Buffer number 很少，有可能性能不足或者系统 bug 导致 packet-buffer 泄露

5. 软件

查看配置、统计集、日志等信息分析

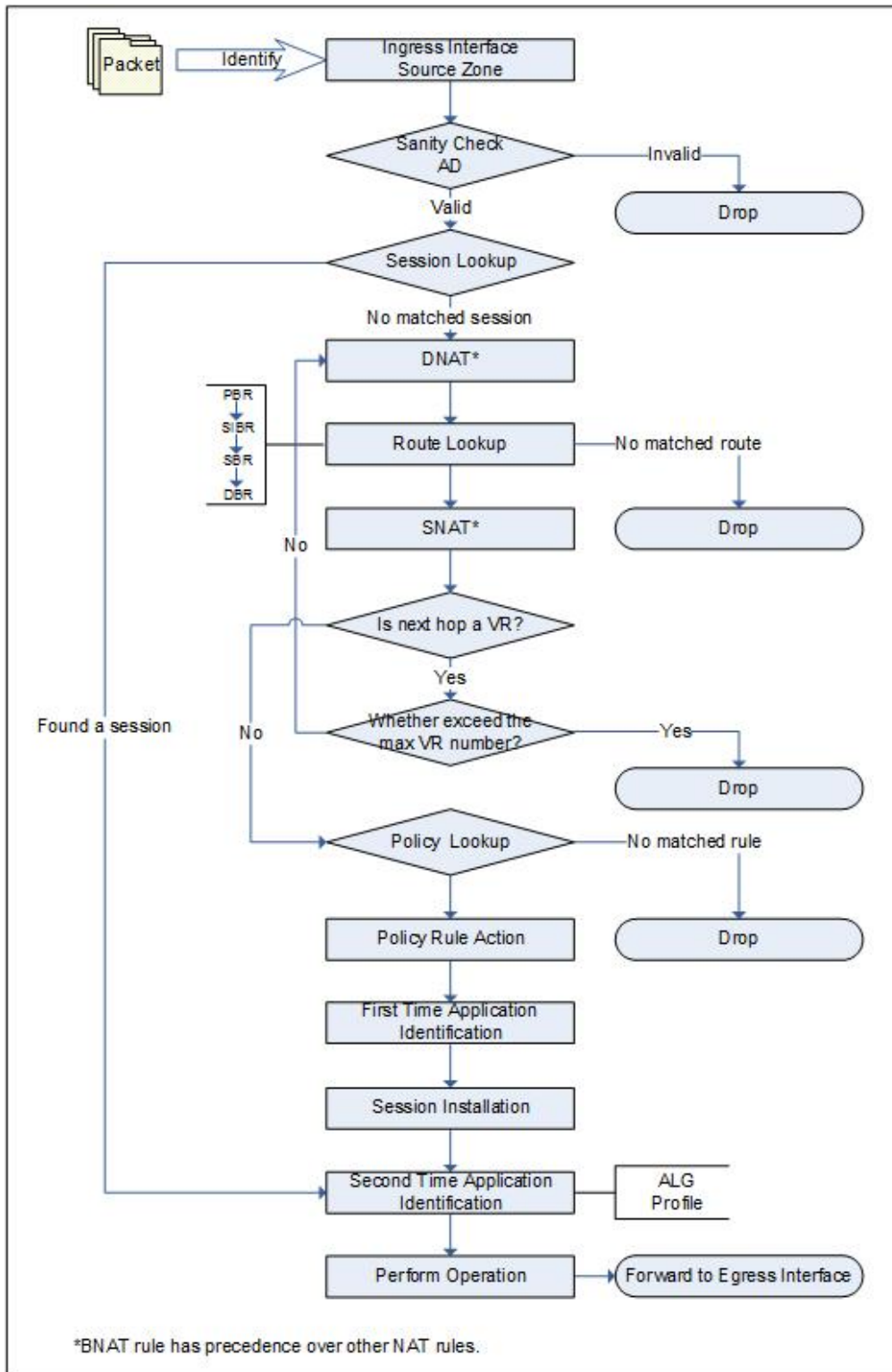
通过 debug 分析软件的丢包

6. 新增 show controller packet 和 show tech-support flow countor 查看设备的丢包情况

7、debug dp basic 查看业务在哪个模块的处理有异常，参考 5.4 章节

1.21 系统调试功能

1.21.1 防火墙数据转发流程



1. 识别数据包的逻辑入接口，可能是一般无标签接口，也可能是子接口。从而确定数据包的源安全域。

2. CtyunOS 对数据包进行合法性检查。如果源安全域配置了攻击防护功能，系统会在这一步同时进行攻击防护功能检查。

3. 会话查询。如果该数据包属于某个已建立会话，则跳过 4 到 10，直接进行第 11 步。

4. 目的 NAT (DNAT) 操作。如果能够查找到相匹配的 DNAT 规则，则为包做 DNAT 标记。因为路由查询需要 DNAT 转换的 IP 地址，所以先进行 DNAT 操作。

*如果系统配置静态一对一 BNAT 规则，那么先查找匹配的 BNAT 规则。数据包匹配了 BNAT 规则之后，按照 BNAT 的设定进行处理，不再查找普通的 DNAT 规则。

5. 路由查询。CtyunOS 的路由查询顺序从前到后依次为：策略路由 (PBR) --源接口路由 (SIBR) --源路由 (SBR) --目的路由 (DBR) --ISP 路由。此时，系统得到了数据包的逻辑出接口和目的安全域。

6. 源 NAT (SNAT) 操作。如果能够查找到相匹配的 SNAT 规则，则为包做 SNAT 标记。*如果系统配置静态一对一 BNAT 规则，那么先查找匹配的 BNAT 规则。数据包匹配了 BNAT 规则之后，按照 BNAT 的设定进行处理，不再查找普通的 DNAT 规则。

7. 下一跳 VR 查询。如果下一跳为 VR，则继续查看指定的下一跳 VR 是否超出最大 VR 数限制 (当前版本系统仅允许数据包最多通过 3 个 VR)，如果超过则丢弃数据包，如果未超过，返回 4；如果下一跳不是 VR，则继续进行下一步策略查询。

8. 策略查询。系统根据数据包的源安全域、目的安全域、源 IP 地址和端口号、目的 IP 地址和端口号以及协议，查找策略规则。如果找不到匹配的策略规则，则丢弃数据包；如果找到匹配的策略规则，则根据规则指定的行为进行处理，分别是：

允许 (Permit)：允许数据包通过。

拒绝 (Deny)：拒绝数据包通过。

隧道 (Tunnel)：将数据包转发到指定的隧道。

是否来自隧道 (Fromtunnel)：检查数据包是否来自指定的隧道，如果是，则允许通过，如果不是，则丢弃。

9. 第一次应用类型识别。系统根据策略规则中配置的端口号和服务，尝试识别应用类型。

10. 会话建立。

11. 如果需要，进行第二次应用类型识别。根据数据包的内容和流量行为再次对应用类型进行精确识别。

12. 应用层行为控制。根据确定的应用类型，系统将在此执行配置的 Profile 和 ALG 功能。
13. 根据会话中记录的信息，例如 NAT 标记等，执行相应的处理操作。
14. 将数据包转发到出接口。

1. 21. 2 DEBUG 数据流基本步骤

1. 关闭 debug 信息输出到 console

```
no logging debug to console
```

2. 设置 debug 过滤器

```
debug dp filter {src-ip | src-port | proto | dst-ip | dst-port}
```

3. 开启 debug 功能

```
debug dp basic
```

4. 清除缓存 debug 日志信息

```
clear logging debug
```

5. 发起数据流访问

6. 查看 debug 日志信息

```
show logging debug
```

7. 关闭 debug

```
undebug all 或 双击“ESC”键关闭 debug 功能
```

注意：Debug 功能占用大量 CPU 资源，建议在设备负载较高的情况下尽量避免使用 debug，如果必须使用，可设置 debug 过滤器。

Debug 过滤器提供基于 IP、端口及协议类型的过滤功能，可以降低 debug 对 CPU 资源耗费并精确定位 debug 范围。完成 debug 操作后，切记关闭 debug 功能

1. 21. 3 正常访问 DEBUG 信息示例

```
hostname(config)# sh log deb
```

```
2009-03-04 16:17:39, DEBUG@FLOW: core 0 (sys up 0x8e65ae ms):
```

001d.7294.e5f6->00

1c.5402.8c00, size 73, type 0x800, vid 0, port ethernet0/0

Switchid is 8(interface ethernet0/0) port ethernet0/0

Start I3 forward

Packet:192.168.1.12->202.106.0.20,id:8369,ipsize59,prot:17(UDP):3332

-> 53

①No session found, try to create session

//1、如某条会话已建立，则后继数据包可以直接匹配会话并转发。否则，如未匹配到现有会话，则需按检测步骤完成检测。

-----First path creating new session-----

-----VR:trust-vr start-----192.168.1.12:3332->202.106.0.20:53

②No DNAT configured for this VR

//是否匹配 DNAT 策略

③Get nexthop if_id: 10, flags: 0, nexthop: 10.188.9.1

//查询路由以确认出站接口和下一跳网关

④Found the reverse route for force revs-route setting

//是否强制回包查询逆向路由

⑤Matched source NAT: snat rule id:1

//是否匹配 SNAT 策略

Matched source NAT: source port3332->port3332

-----VR:trust-vr end-----

⑥Pak src zone trust, dst zone untrust, prot 17, dst-port 53.

Policy 1 matches, ===PERMIT===

//匹配哪条策略规则

⑦Identified as app DNS (prot=17). timeout 60.

// 识别为何种服务


```
flow0 src 192.168.1.12 --> dst 202.106.0.20 with nexthop 0.0.0.0 ifindex 0
flow1 src 202.106.0.20 --> dst 10.188.9.100 with nexthop 192.168.1.12 ifindex
8 flow0's next hop: 192.168.1.12 flow1's next hop: 10.188.9.1
crt_sess->revs_rres.nexthop: 192.168.1.12, crt_sess->revs_rres.nexthop
10.188.9.1

Application 7 hasn't been registered, don't need do ALG
APP inited for application 7

The following session is installed

@session: id 99962, prot 17, flag a, created 9332, life 60
flow0(ifid:8flowid:199924flag:801):192.168.1.12:3332->202.106.0.20:53
flow1(if id: 10 flow id: 199925 flag: 800):
202.106.0.20:53->10.188.9.100:3332 Session installed successfully
// session 创建成功

-----First path over-----@session: id 99962, prot 17, flag
4a, created 9332, life 60

//匹配到会话, 直接快速转发
flow0(ifid:8flowid:199924flag:811):192.168.1.12:3332->202.106.0.20:53
flow1(if id: 10 flow id: 199925 flag: 810):202.106.0.20:53->10.188.9.100:3332

Set fast code to fe proc

Go to fe proc directly

Got mac: ip:10.188.9.1, mac:001c.5400.1dtrust L3 forward, out if is ethernet0/2
msw_dsa_tag_encap_from_cpu:TXpacketfrominterfaceethernet0/2,vid0cos0.
```

1.22 常用监控维护命令

在设备运行过程中, 为方使用户及时了解设备运行状态及进行设备整体运行情况的监控, 需要通过一些常用命令来进行监控维护, 具体方法如下:

1、软件版本检查及运行时间检查

```
(config)# show version      /*查看版本
```

```
CtyunOS software, Version 3.5
```

```
Copyright (c) 2006-2009 by Networks, Inc.
```

```
Product name: VR5600T S/N: 0802027090006741 Assembly number: B045
```

```
Boot file is SA2000-3.5R2p4.bin from flash
```

```
Built by buildmaster2 2009/07/07 12:34:08
```

```
Uptime is 0 day 0 hour 55 minutes 46 seconds /*查看运行时间
```

2、并发会话检查

执行命令：show session generic

如果超出最大值说明防火墙并发会话已经达到极限，防火墙成为一性能瓶颈，需要升级到更高档次防火墙。

会话信息如包含 alloc failed 说明防火墙会话曾经达到最大值，防火墙会话建立失败，可能是防火墙性能的问题或曾经出现网络攻击现象；

```
(B)# show session generic    /*查看会话数
```

```
VSYS 0, max 200000, allocated 0, deny session 0, free 200000, tunnel 0, alloc failed 0
```

3、CPU 利用率检查

CPU 主要任务为执行功能、会话、日志等管理功能，一般情况下 CPU 利用率不会太高，建议不超过 60%。CPU 统计有 1 分钟、5 分钟、15 分钟平均值。在某一时间段 CPU 利率较高，属异常现象，可能有攻击等情况发生。CPU 利用率持续较高，说明防火墙配置错误，需要调整防火墙配置，以降低 CPU 利用率。

```
(B)# show cpu              /*查看 cpu 使用率
```

```
Average cpu utilization : 0.2%
```

```
current cpu utilization : 2.0%
```

```
Last 1 minute : 0.1%
```

```
Last 5 minutes : 0.2%
```

```
Last 15 minutes : 0.2%
```

4、内存使用率检查

执行 `show memory` 查看内存利用率;

```
(B)# show memory          /*查看内存
```

The percentage of memory utilization: 25%

total(kB)	used(kB)	free(kB)
524288	132793	391495

5、日志审计统计

云下一代防火墙安全产品提供了用于监控系统事件和网络流量的事件日志以及便于系统管理员分析和跟踪设备各种问题情况。CtyunOS 的日志信息分为七种，分别是事件 (Event) 日志信息、告警 (Alarm) 日志信息、安全 (Security) 日志信息、配置 (Configuration) 日志信息、网络 (network) 日志信息、流量 (Traffic) 日志信息和调试 (Debug) 日志信息。日志信息根据严重级别的不同，又可以分为 8 级别。

日志信息严重性级别分类：

- Emergency (紧急) 级别 0：系统不可用信息。
- Alert (警示) 级别 1：需要立即处理的信息，如设备受到攻击灯。
- Critical (关键) 级别 2：危急信息，如硬件出错。
- Error (错误) 级别 3： 错误信息。
- Warning (警告) 级别 4： 报警信息。
- Notification (通知) 级别 5：非错误信息，但需要特殊处理。
- Information (信息) 级别 6： 通知信息。
- Debugging (调试) 级别 7： 调试信息，包括正常的使用信息。

查看一些日志信息如下：

```
show logging event        /*查看事件日志
```

```
show logging alarm       /*查看告警日志
```

```
show logging security    /*查看安全日志
```

6、路由检查

路由模式工作时，数据转发跟系统路由相关，检查路由设置是否正确。

(B)# show ip route /*查看路由

Codes: K - kernel route, C - connected, S - static, I - ISP, R - RIP, O - OSPF,

B - BGP, D - DHCP, P - PPPoE, H - HOST, G - SCVPN, V - VPN, M - IMPORT,

> - selected route, * - FIB route

Routing Table for Virtual Router <trust-vr>

```
=====
=====
```

C>* 192.168.1.0/24 is directly connected, ethernet0/0

H>* 192.168.1.1/32 [0/0/1] is local address, ethernet0/0

```
=====
=====
```

7、查看系统信息

获得系统的一些信息。

show tech-support toconsole /*查看系统信息

8、查看 HA 状态

(M) # show ha group 0 /*查看 HA 组配置信息

HA Group id=0

state Master

priority 10 preempt 0

monitor

HA peer num 1

HA peer 0

device id 0701449100025740

ip 1.1.1.2

state Backup

priority 100

9、配置同步检查

(B)# show ha sync state config /*查看 HA 同步状态

1. 23 故障信息收集

当设备出现故障时，可以通过以下命令收集防火墙信息：

show tech-support toconsole

Show cpu detail

Show session generic

Show snat resource

Show log event | include SNAT Show logging alarm file

show log security

show environment