飞塔防火墙配置手册

FortiOS 5.0

版本	1.0
时间	2014 年 10 月
支持的版本	FortiOS v4.3.x, v5.0.x
作者	宋占军
状态	已审核
反馈	support_cn@fortinet.com

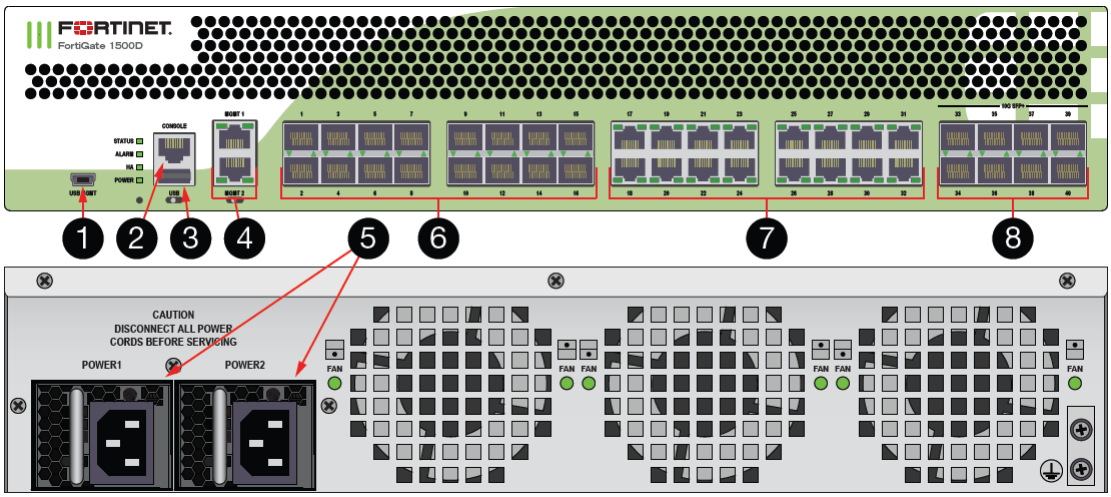
2014.10

目录

第1章.飞塔防火墙硬件介绍

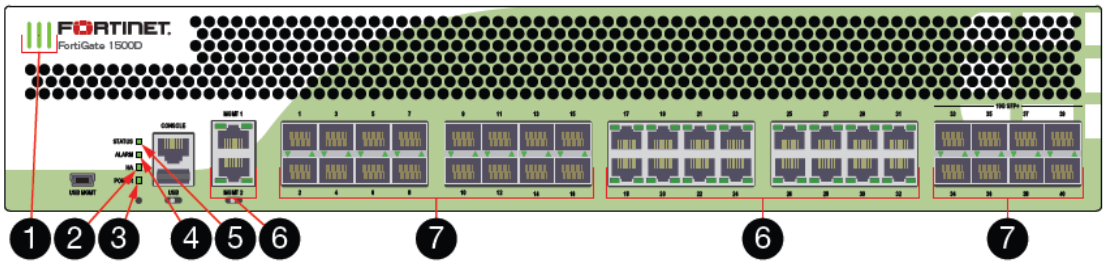
1.1. FortiGate1500D

1.1.1. 接口示意图



ID	接口	类型	描述
1	USB MGMT	USB mini-B	用户管理
2	CONSOLE	RJ-45	控制口，用于 CLI
3	USB	USB	可用于备份，3G 卡 moderm.
4	MGMT1,2	RJ-45	专用管理口，非硬件加速口
5	电源		100-240V AC, 8-4A, 50/60Hz
6	Ports1 - 16	SFP (SX or LX)	千兆 SFP 接口，支持电口和光口
7	Ports 17 - 32	RJ-45	千兆电口
8	Ports 33 - 40	SFP+	万兆 SFP 接口

1.1.2. LED 示意图



ID	LED	状态	描述
1	Logo	**绿色**	设备开启
		关	设备关闭
2	HA	绿色	正常运行 HA 模式
		红色	HA 模式故障
		关	单机模式
3	电源	**绿色**	设备开启
		关	设备关闭
4	Alarm	红色	主要告警
		琥珀色	次要告警
		关	正常运行
5	Status	绿色	**正常运行**
		绿色闪烁	**设备启动中**
		红	**严重告警**
6	**以太接口速率灯**	绿色	1G
		琥珀色	100M
		关	10M 或关闭状态
6	SFP & SFP+	绿色	活动状态

		绿色闪烁	发送和接受数据
		关	端口未使用

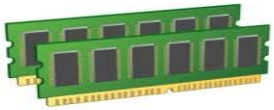
第2章.飞塔防火墙系统基础

2.1.系统介绍与基本配置

2.1.1. Flash 卡和内存

FLASH 卡有多个分区

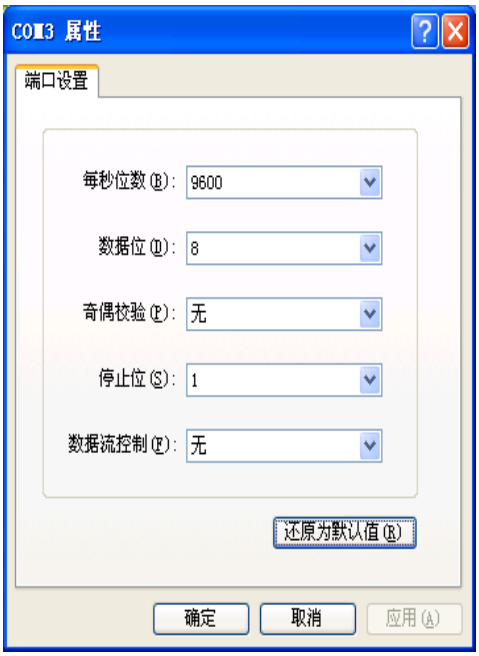
- FortiOS image 文件
- FortiOS 配置文件



内存卡

- 运行 FortiOS image
- 运行 FortiOS 配置
- 记录日志

2.1.2. Console 连接



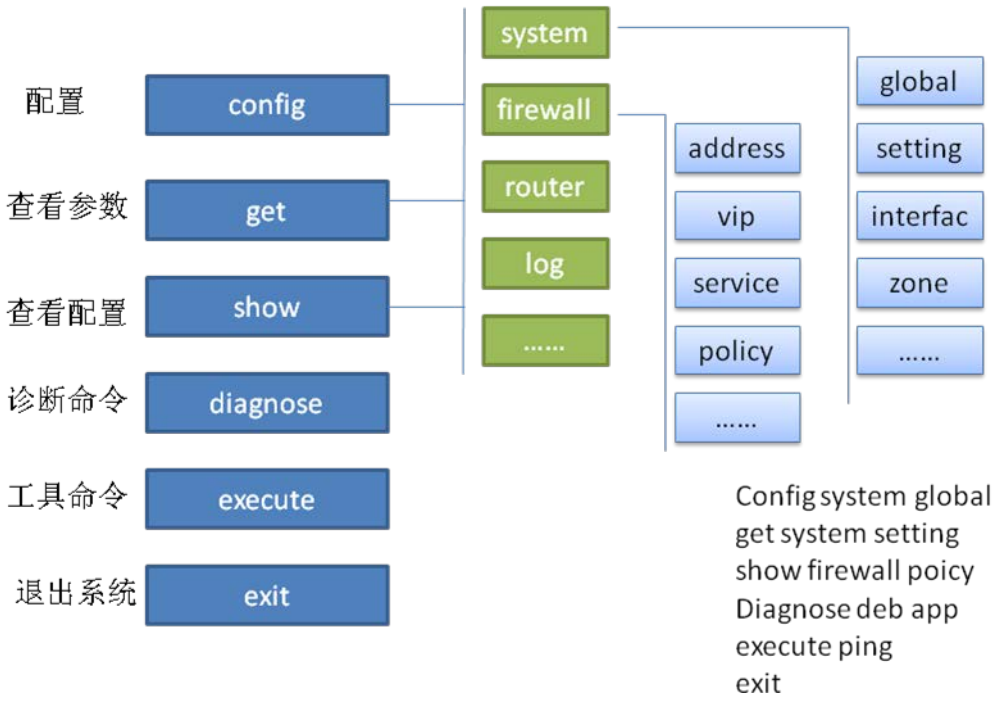
- Console 波特率设定
  - 9600 bps
  - 8 数据位
  - 1 停止位
  - 奇偶校验

Console 连接正确后,在超级终端可以看到 login 提示符

初始用户名为 admin,密码为空

2.1.3. 命令行界面

#提示符后输入?将出现命令行提示,通过 Tab 建补全命令



2.1.4. 命令行配置

设置 port2 的 IP:

310B # config system interface　　#进入接口配置

310B (interface) # edit port2　　#编辑指定接口

310B (port2) # set ip 10.0.0.99/24　　#IP 地址设定

310B (port2) # set allowaccess https ping　　#根据需要设定相应服务

310B (port2) # end　　#end 保存并退出

2.1.5. 命令行配置查看

显示设置命令

```
310B # show system interface port2
config system interface
    edit "port2"
    setvdom "root"
    setip 10.0.0.99 255.255.255.0
```

```
        setallowaccess ping https
        set type physical
next
end
```

2.1.6. 命令行参数配置查看

显示参数和当前值

```
310B # config system interface
310B (interface) # edit port2
310B (port2) # get
name                          : port2
vdom                           : root
cli-conn-status             : 0
mode                          : static
dhcp-relay-service    : disable
dhcp-relay-ip                :
dhcp-relay-type           : regular
ip                                  : 10.0.0.99 255.255.255.0
allowaccess                 : ping https
```

2.1.7. 命令行执行命令

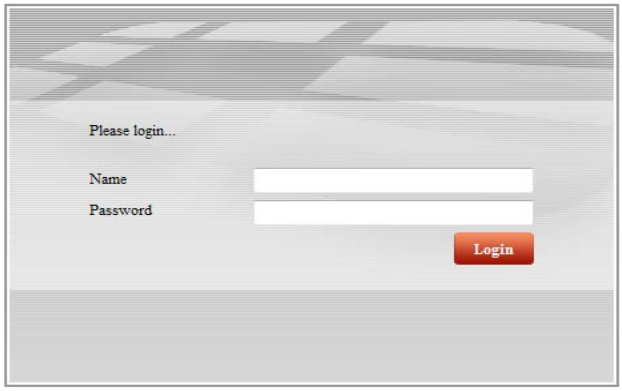
执行命令,例如:

```
executefactoryreset
execute ping
execute backup
execute date
execute time
execute reboot
execute shutdown
```

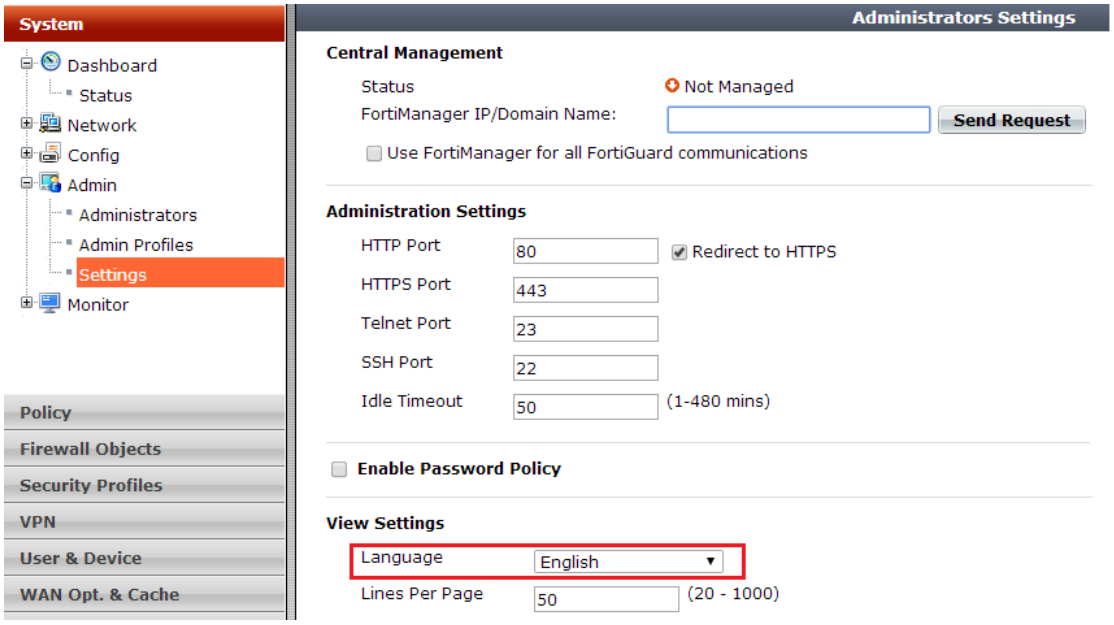
2.1.8. 登陆界面

初始登录接口 port1 或 internal，初始登录 IP 地址为 https://192.168.1.99

默认账号 admin,密码为空，建议使用最新的谷歌，火狐 3.6 以上版本或 IE8 浏览器。



初次登陆为英文界面，可以进入 System-Admin-Settings,Language 选择 Simplified Chinese



密码修改可以进入系统管理-管理员设置-管理员，选择 admin 账号进行密码修改，另在该页面可以添加信任主机,指定允许主机对 FortiGate 的访问。

命令行修改密码方法：

```
config system admin
    edit "xxx"
```

set password xxx
end
修改密码后，主备机会自动同步密码。

2.2. 配置文件管理

2.2.1. 配置备份

飞塔防火墙可以通过 web 页面或者 CLI 命令行对配置文件进行备份，同时系统也会自动保存历史配置文件，便于配置文件的恢复。

1) WE B 页面备份

打开如下页面：系统管理－面板－status－系统信息

点击“备份”按钮，将配置保存到本地计算机，选择需要保存的路径。如果配置文件需要加密保存，选择“加密配置文件”，输入密码，保存下来的文件则以加密的方式存放；恢复配置的时候需要提供相应的密码。

也可以将U盘插入设备的 USB 口，保存到U盘。

2) 命令行备份配置

Fortigate# **exec backup**

config　　备份配置文件。

disk　　备份硬盘上的 log 文件

full-config　　包括系统参数的全配置文件。

Fortigate # **exec backup config　tftp　dd.cfg 1.1.1.1**　备份文件到 1.1.1.1 的 TFTP 服务器，文件名为 dd.cfg

Fortigate # **exec backup config　usb dd.cfg**　备份到 usb 磁盘。

3)　系统自动备份

每次配置修改后，当管理员退出时系统会自动保存配置文件，可通过如下方式查看。如下图，点击修订（Revisions）

双击要查看的相关日志的历史文件。

2.2.2. 恢复配置

可以通过如下两种方法来实现配置文件的恢复。

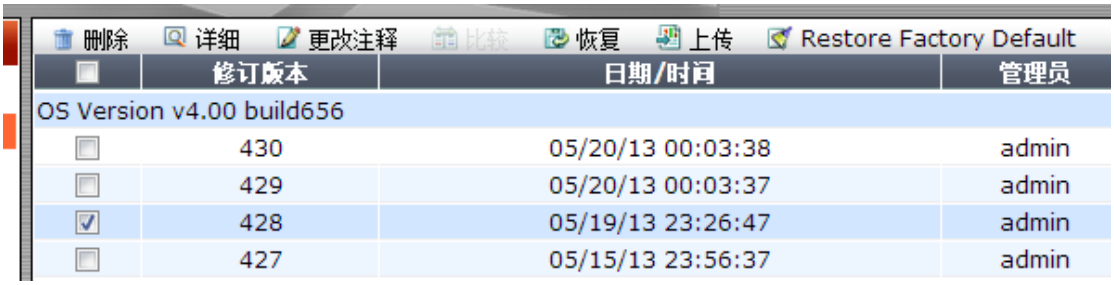
1)　恢复手动保存的配置文件

如上图，选择系统管理－面板－status－系统信息，点击还原，选择需要恢复的文件，系统会**自动重启，**加载新的配置文件。

2) 恢复系统内部自动保存配置文件

点击 Revisions

选择要还原的配置文件



点击“恢复”，系统载入相应的文件，自动重启。

2.3. 系统管理

2.3.1. 恢复出厂配置

Fortigate # execute factoryreset ，回车后选择 y。

2.3.2. 清除系统密码

密码重置步骤：

1) 连上串口并配置好；
2) 给设备加电启动（必须断电后重启）；
3) 启动完 30 秒内从串口登陆系统，用户名为：maintainer；
4) 密码： bcpb＋序列号（区分大小写）；如：bcpbFW81CM3909600364
5) 在命令行下执行如下命令重新配置“admin”的密码：

```
config system admin
  edit admin
  set password “需要配置的新密码“
end
```

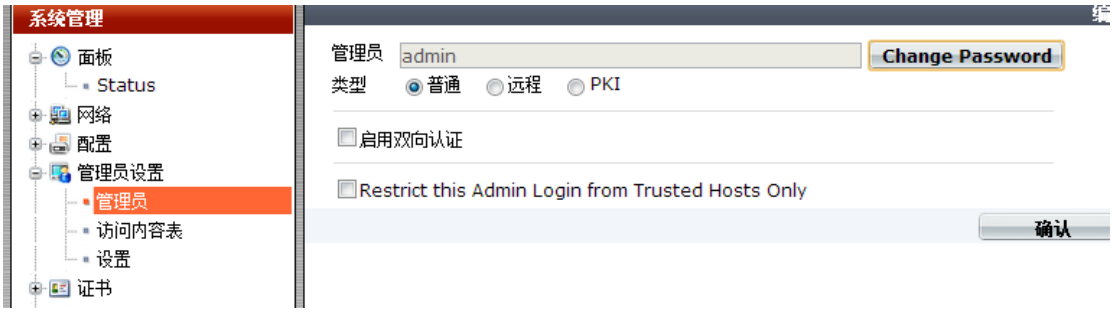
6) 用新密码从 Web 界面登陆系统。

2.3.3. 管理员管理

1) 修改管理员密码

WEB 页面：

系统管理－管理员设置－管理员，编辑 admin 用户，选择 change password，按提示操作。



命令行：

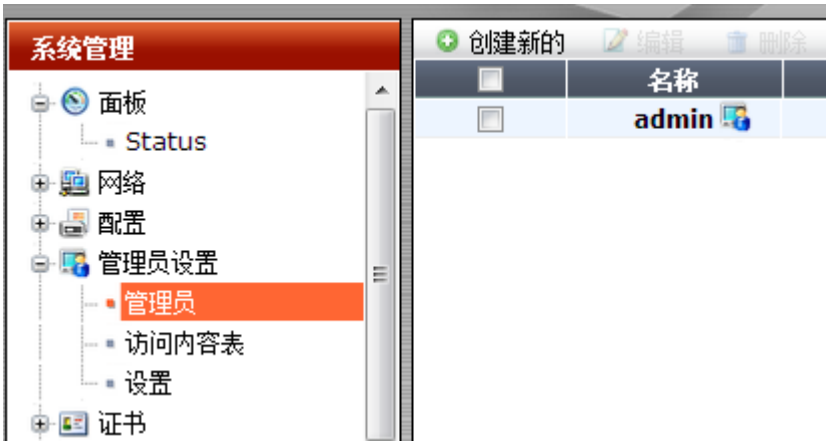
config system admin

edit admin

set password “需要配置的新密码“

end

2) 建立新的管理员



点击“创建新的“

输入用户名，密码，访问表，信任主机，双因子认证。

3) 信任主机问题

如果所有的管理账户都添加了可信主机，则只有可信主机的 IP 地址范围可以访问防火墙，**包括 PING.** 如果希望 ping 包不受限制，可以添加一个没有任何管理权限的账户，其可信主机不做任何限制。

2.3.4. NTP 服务器

配置命令：

```
config system ntp
        config ntpserver
            edit 1
                set server "11.152.8.7"
            next
        end
    set ntpsync enable
    set syncinterval 60
```

查看状态命令：

diagnose sys ntp status

诊断命令：

Fortigate # dia deb enable	开启 debug
Fortigate # dia deb application ntpd -1	查看 ntp 信息
Fortigate # dia deb application ntpd 0	关闭
Fortigate # dia deb disable	关闭 debug

2.3.5. 防火墙进程管理

1) 查看进程运行状态

dia sys top

Fortigate#get system performance top

Run Time: 0 days, 8 hours and 22 minutes

0U, 0S, 100I; 500T, 268F, 64KF

// 进程名字	ID	转态	CPU	内存//	
httpsd	99	S	0.0	5.1	//S 睡眠状态
httpsd	69	S	0.0	4.4	
cmdbsvr	33	S	0.0	4.1	
httpsd	41	S	0.0	3.6	
ipsengine	60	S <	0.0	3.3	
fgfmd	85	S	0.0	3.1	
newcli	145	R	0.0	3.1	//R 运行状态

2) 杀掉进程

diagnose sys kill <signal> <process id>

- <signal> 推荐使用 11,会产生 crashlog ,用于故障的排查。
- <process id> 进程 ID

diagnose sys kill 11 60

防火墙内部进程信息参照 6.4.2.1 小节。

2.4. 系统信息查看

2.4.1. 防火墙系统信息

查看系统的综合信息，序列号，硬件版本，软件版本，操作模式等。

FG3K9B3E10700335 # **get system status**

2.4.2. 防火墙硬件信息

FG3K9B3E10700335 # **get hardware status**

2.4.3. 防火墙 CPU 信息

Fortigate # get hardware cpu

processor : 0

vendor_id : GenuineIntel

cpu family : 6

model : 5

model name : Celeron (Covington)

stepping : 0

cpu MHz : 600.037

cache size : 64 KB

fdiv_bug : no

hlt_bug : no

f00f_bug : no

coma_bug : no

fpu : yes

fpu_exception : yes

cpuid level : 2

wp : yes

flags : fpu vme de pse tsc msr pae mce cx8 sep mtrr pge mca cmov pat c

lflush dts acpi mmx fxsr sse sse2 ss tm pbe

bogomips : 1196.03

2.4.4. 防火墙内存信息

FG3K9B3E10700335 (global) # **get hardware memory**

total: used: free: shared: buffers: cached: shm:

Mem: 12557111296 2246512640 10310598656 0 344064 950071296 970493952

Swap: 0 0 0

MemTotal: 12262804 kB

MemFree: 10068944 kB

MemShared: 0 kB

Buffers: 336 kB

Cached: 927804 kB

SwapCached: 0 kB

Active: 51936 kB

Inactive: 876356 kB

HighTotal: 0 kB

HighFree: 0 kB

LowTotal: 12262804 kB

LowFree: 10068944 kB

SwapTotal: 0 kB

SwapFree: 0 kB

2.4.5. 防火墙 NPU 板卡信息

FG3K9B3E10700335 (global) # **diagnose npu np4 list**

ID	Model	Slot	Interface
0	On-board		port1 port2 port3 port4 port5 port6 npu0-vlink0 npu0-vlink1
1	FMC-C20 //模块名称//	FMC4 //槽位//	fmc4/1 fmc4/2 fmc4/3 fmc4/4 fmc4/5 fmc4/6 fmc4/7 fmc4/8 fmc4/9 fmc4/10 fmc4/11 fmc4/12 fmc4/13 fmc4/14 fmc4/15 fmc4/16 fmc4/17 fmc4/18 fmc4/19 fmc4/20 npu1-vlink0 npu1-vlink1

2.4.6. 防火墙网络接口信息

get hardware nic port1

diagnose hardware deviceinfo nic

show system interface　查看接口配置

get system interface　简要查看接口状态。

2.4.7. 防火墙性能信息

Fortigate # get system performance status

CPU states: 0% user 1% system 0% nice 99% idle

CPU0 states: 0% user 1% system 0% nice 99% idle

Memory states: 42% used

Average network usage: 46 kbps in 1 minute, 54 kbps in 10 minutes, 99 kbps in 30 minutes

Average sessions: 24 sessions in 1 minute, 36 sessions in 10 minutes, 29 sessions in 30 minutes

Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in last 10 minutes, 0 sessions per second in last 30 minutes

Virus caught: 0 total in 1 minute

IPS attacks blocked: 0 total in 1 minute

Uptime: 0 days, 8 hours, 34 minutes

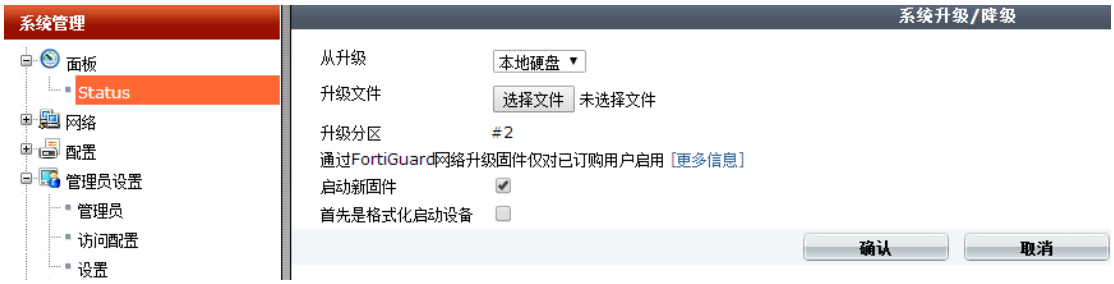
2.5. 系统 OS 维护

2.5.1. WEB 页面系统升级

打开如下页面：

1) 上传新的 OS

点击“升级”按钮，进入 OS 升级页面：



从本地电脑中选择要升级的ＯＳ文件，确定后系统会重启，并启动新的ＯＳ。

2) 使用设备中备份分区中的 OS

飞塔防火墙存在 2 个 OS 分区，点击“细节”按钮，则会列出目前系统中保存的所有ＯＳ镜像文件，选择要使用的ＯＳ，点击升级，系统会从新启动，并使用新的ＯＳ来引导。

2.5.2. TFTP 升级 OS

建议对新安装的设备，建议通过该方法写入 OS。

1) 备份好系统配置。

2) 准备好相应的 FortiOS 文件，飞塔不同型号的硬件使用不同的 OS。

3) 准备 TFTP server 软件。

4) 利用串口连接系统的 console 口，并重启动防火墙。

5) 按照屏幕提示进行如下操作。

Power on

FGT60 (19:33-06.05.2003)

Ver:03000300

Serial number:FGT-6028030xxxxx

RAM activation

Total RAM: 128MB

Enabling cache...Done.

Scanning PCI bus...Done.

Allocating PCI resources...Done.

Enabling PCI resources...Done.

Zeroing IRQ settings...Done.

Verifying PIRQ tables...Done.

Boot up, boot device capacity: 30MB.

Press any key to display configuration menu... //**此时按任意键**

. .

[G]: Get firmware image from TFTP server. //通过 TFTP 升级 OS

[F]: Format boot device. //格式化闪存。

[Q]: Quit menu and continue to boot with default firmware.　　//退出菜单，继续启动

[H]: Display this list of options.　　//帮助

Enter G,F,Q,or H:　(选择'F')

Formatting boot device...

.....

Format boot device completed.

Enter G,F,Q,or H:　(选择'G')

//此时屏幕会提示将电脑与设备的某个网络接口相连，FG3950B 和 FG3040B 为 mgmt1，FG1240B 为 39 口。这些均非硬件加速接口//

Enter TFTP server address [192.168.1.168]: 192.168.171.129　　//输入 TFTP 服务器的 IP

Enter local address [192.168.1.188]: 192.168.171.171　　//与 TFTP 服务器同网段的 IP

Enter firmware image file name [image.out]: FGT_60-v280-build219-FORTINET.out

MAC:00:09:0f:0a:1a:7c

##########

Total 10643362 bytes data downloaded.

Verifying the integrity of the firmware image.

Total 28000kB unzipped.

Save as Default firmware/Backup firmware/Run image without saving:[D/B/R]?　　(选择 'D')

Programming the boot device now.

6)　升级完成后，get system status 查看版本信息。

2.6. 设备硬件操作

2.6.1. 关闭设备

1)　通过命令行关闭设备

Fortigate # exec shutdown

This operation will shutdown the system !

Do you want to continue? (y/n)y

System is shutting down...

System is shutting down...

The system is going down NOW !!

System is shutting down...

Fortigate #

The system is halted.

2) 也可以直接关闭电源。

2.6.2. 重新启动设备

exec reboot

2.6.3. 硬盘操作

1) 查看硬盘信息：

Fortigate # exec disk list

Device S0 30.1 GB ref: 0 ATA STT_FTM32GL25H (SSD)

[Internal]

partition 1 30.1 GB ref: 1 label: 48EB731B1EBAB5A5

2) **格式化硬盘**

exec disk format 0 格式化后系统**会自动重启。**

3) 查看硬盘使用情况

Fortigate # diagnose hardware deviceinfo disk

Device S0 30.1 GB ref: 0 ATA STT_FTM32GL25H (SSD)

[Internal]

partition 1 30.1 GB ref: 1 label: 48EB731B1EBAB5A5

[dev: /dev/sda1 major: 8 minor: 1 free: 29479MB mounted: Y]

Device S* 492.0 MB ref: n/a USB DISK 2.0 (USB)

partition 1 39.1 MB ref: n/a label:

[dev: /dev/sdb1 major: 8 minor: 17 free: 10MB mounted: Y]

partition 2 39.1 MB ref: n/a label:

[dev: /dev/sdb2 major: 8 minor: 18 free: 9MB mounted: N]

partition 3 403.9 MB ref: n/a label:

[dev: /dev/sdb3 major: 8 minor: 19 free: 309MB mounted: Y]

第3章.飞塔防火墙网络配置

3.1. 物理接口

3.1.1. Web 页面

物理接口支持三种地址模式：

自定义：手动配置 ip 地址

DHCP: 从 DHCP 获取 ip 地址

PPPOE： 使用 pppoe 拨号方式。

3.1.2. 配置命令

config system interface

edit "internal"

set vdom "root" //属于 root 域

set ip 192.168.1.99 255.255.255.0 //配置 ip 地址。

set allowaccess ping https ssh http telne //配置接口管理选项

set type physical //其他类型如 vlan，802.3ad，冗余等

next

3.1.3. 接口配置多个 IP

WEB 页面：选择 附加的IP地址 按钮，选择 create new。

CLI 配置:

Config system interface

edit "internal"

set vdom "root"

set ip 192.168.1.99 255.255.255.0

```
        set allowaccess ping https ssh http telnet fgfm
        set type physical
        set secondary-IP enable                                  //允许配置 secondary IP
            config secondaryip                                   //进入配置模式
                edit 1                                           //ID，可以配置多个
                    set ip 11.0.0.1 255.255.255.0
                    set allowaccess https
                next
            end
 next
```

3.2. Vlan 接口

3.2.1. WEB 页面

3.2.2. 配置命令

FortiGate 路由模式下支持创建三层的 Vlan 接口，可以与指定物理接口关联

```
config system interface                          //配置接口
    edit "VLAN20"                                //新建接口名称
    setvdom "root"
        set ip 192.168.20.1 255.255.255.0        //vlan 接口地址
```

```
        set allowaccess ping http telnet          //vlan 接口的管理访问
        set interface "port2"                     //关联的物理接口
        setvlanid 20                              //vlan id
next
end
```

3.3. 汇聚接口

3.3.1. WEB 页面

FortiGate 链路聚合需要两个或者两个以上,最大支持到八个接口，配置链路聚合的接口必须具备以下条件:

- 接口成员为物理接口,而非 Vlan 接口；
- 接口成员必须在同一虚拟域下；
- 接口成员未定义 IP 地址,且未在策略及防火墙其他配置中被调用；
- 接口成员没有 Vlan 子接口；
- 接口成员不允许为 HA 的心跳接口；
- 接口成员不能是已有链路聚合成员。

3.3.2. 配置命令

```
edit " aggregate "
    set vdom "root"
    set ip 192.168.0.249 255.255.255.248
    set allowaccess ping https ssh telnet
    set type aggregate
        set member "port7" "port8"
 next
```

3.3.3. 查看命令

- FG5001-5050-A-5 (global) # diagnose netlink aggregate name aggregate

  LACP flags: (A|P)(S|F)(A|I)(I|O)(E|D)(E|D)

  (A|P) - LACP mode is Active or Passive

  (S|F) - LACP speed is Slow or Fast

  (A|I) - Aggregatable or Individual

  (I|O) - Port In sync or Out of sync

  (E|D) - Frame collection is Enabled or Disabled

  (E|D) - Frame distribution is Enabled or Disabled

  status: up

  distribution algorithm: L4

  LACP mode: active

  LACP speed: slow

  LACP HA: enable

  aggregator ID: 1

  ports: 2

  actor key: 17

  actor MAC address: 00:09:0f:68:35:94

partner key: 17

partner MAC address: 00:09:0f:68:37:d8

- slave: port7

  status: up

  link failure count: 3

  permanent MAC addr: 00:09:0f:68:35:94

  actor state: ASAIEE //**ASAIEE 状态正常**

  partner state: ASAIEE

  aggregator ID: 1

  slave: port8

  status: up

  link failure count: 2

  permanent MAC addr: 00:09:0f:68:35:95

  actor state: ASAIEE

  partner state: ASAIEE

  aggregator ID: 1

3.4. 冗余接口

3.4.1. WEB 页面

FortiGate 冗余接口:把两个或多个物理接口逻辑为一个接口。若其中一接口失效，则有该 redundant 组下的其他接口继续转发流量，以达到冗余的作用。

3.4.2. 配置命令

```
config system interface
        edit "redundancy"
        setvdom "root"
        setip 192.168.127.1 255.255.255.0
        setallowaccess ping https telnet
        set type redundant
        set member "port9" "port10"                    //接口成员,先加入成员为主
next
end
```

冗余接口仅在 200B 以上型号可配置。

3.4.3. 查看冗余接口的链路状态

```
ha-a-981 $ diagnose netlink redundant name redundancy
status: up                                             #冗余接口状态
npu: n
ports: 2
MAC addr: 00:09:0f:88:2c:89     #当前工作接口 MAC 地址
current slave: port9                    #当前工作接口
slave: port9
status: up
  link failure count: 3                 #端口失效计数
```

permanent MAC addr: 00:09:0f:88:2c:89
slave: port10
status: up
link failure count: 2
permanent MAC addr: 00:09:0f:88:2c:88

3.5. Zone(区)

区 zone 将 2 个或多个物理接口，vlan 接口，或冗余接口等设置在一个区域内，那么定义策略时，可以使用 zone 设定策略代替多个接口策略。

3.5.1. WEB 页面

选择所属区域

指定接口。

3.5.2. 配置命令

```
config system zone
  edit "zone"
        set interface "port5" "port6"
        set intrazone deny                    //是否屏蔽 zone 成员之间的流量
    next
end
```

配置区 zone 后，在接口中可以看见 zone 的成员，但是定义策略时，源接口将不再出现 zone 成员，而是以 zone 为单位定义策略

3.6. 命令参数

config system interface	
edit "port1"	接口名字
set vdom "root"	接口所属虚拟域
set mode static	接口地址模式：静态，pppoe,dhcp
set dhcp-relay-service disable	是否允许 DHCP 中继服务
unset dhcp-relay-ip	配置 DHCP 中继服务的 IP
set dhcp-relay-type regular	DHCP 中继服务类型，普通或者 Ipsec
set ip 11.156.224.166 255.255.255.248	IP 地址
set allowaccess ping snmp telnet	接口允访问控制选项
set fail-detect disable	是否进行接口失败检测，跟踪另外一个接口端状态
set pptp-client disable	不作为 ppptp client 拨号端
set arpforward enable	允许 arp 转发
set broadcast-forward disable	禁止广播数据的转发
set bfd global	使用全局的 bfd 配置参数
set l2forward disable	关闭 2 层数据转发
set icmp-redirect enable	开启 icmp 的路由重定向功能
set vlanforward enable	允许 vlan 转发
set stpforward disable	禁止生成树转发
set ips-sniffer-mode disable	禁止单臂模式的 IPS 检查
set ident-accept disable	关闭用户认证服务端口
set ipmac disable	接口上关闭 IP MAC 绑定
set subst disable	
set log disable	开启接口上日志记录，会降低性能，常用于排障
set fdp disable	是否允许 Fortinet Discovery Protocol (FDP)服务。

set status up	管理状态为 UP
set netbios-forward disable	允许将 netbios 转发到 wins 服务器
set wins-ip 0.0.0.0	wins 服务器的 IP 地址
set type physical	接口类型为物理接口，可以为 vlan,redandunt,aggregate 等
set sample-rate 2000	sflow 采样速率为每 2000 采样一个
set polling-interval 20	sflow 采样间隔，单位秒
set sample-direction both	sflow 监控流入和流出 2 个方向的数据
set explicit-web-proxy disable	关闭接口上的显示 web-proxy 代理
set explicit-ftp-proxy disable	关闭接口上的显示 ftp-proxy 代理
set tcp-mss 0	TCP 最大传输单元，以太网一般为 1460 字节
set inbandwidth 0	接口上的流量控制，单位 KB/s，优先策略流量整形
set outbandwidth 0	接口上的流量控制，单位 KB/s，优先策略流量整形
set spillover-threshold 0	ECMP 协议基于 usage-based 算法的时候，当发往这个接口的流量达到该值，流量就开始转发到下个接口
set weight 0	配置接口权值，仅在静态路由未设置权值时有效
set external disable	配置该接口为外部接口，用于 SIP 的 NAT
set description "	接口的描述
set alias "	配置接口别名，仅用于物理接口
set vrrp-virtual-mac disable	禁用：vrrp 生成新的 MAC 地址
set secondary-IP disable	禁用：接口上配置多个 IP 地址
set idle-timeout 0	当接口配置为 pppoe 模式的时候，空闲超时时间。
unset macaddr	是否更改接口的 MAC 地址，仅用于物理接口。
set speed auto	配置接口速率：1000full,1000halp 等
set mtu-override disable	不更改的接口 MTU
set wccp disable	禁用 WCCP：网页缓存通信协议
set sflow-sampler disable	关闭 sflow 采样

3.7. 相关诊断命令

- diagnose hardware deviceinfo nic wan1 //查看接口信息
- show system interface wan1 //查看查看接口信息接口配置
- show full-configuration system interface wan1 //查看接口全配置
- get hardware nic wan1 //查看接口信息
- get sys arp //查看 arp 表。
- exec clear system arp table //清除 arp 表
- exec ping 1.1.1.1 // ping

- exec ping-options //自定 ping 的参数

  data-size integer value to specify datagram size in bytes

  df-bit set DF bit in IP header <yes | no>

  interval integer value to specify seconds between two pings

  pattern hex format of pattern, e.g. 00ffaabb

  repeat-count integer value to specify how many times to repeat ping

  source auto | <source interface ip>

  timeout integer value to specify timeout in seconds

  tos IP type-of-service option

  ttl integer value to specify time-to-live

  validate-reply validate reply data <yes | no>

  view-settings view the current settings for ping option

- exec traceroute 8.8.8.8 // trace

第4章.飞塔防火墙路由配置

4.1. 静态路由

4.1.1. 配置页面

目的 ip/子网掩码： 路由表的目的 ip

设备： 该条路由表的关联接口，如果接口无效，路由也会失效，如果接口错误则路由条目无法工作。

网关： 下一跳 ip

注释： 注释，可选

优先级： 完全相同的 2 个条路由表，具有较低优先级的被优先使用。

管理距离： 较低管理距离的路由条目会优先被装入路由表。

4.1.2. 配置命令

```
config router static
    edit 1
        set device "port1"
        set dst 10.0.0.0 255.0.0.0
        set gateway 192.168.1.1
    next
end
```

4.1.3. 命令参数

Config router static	
edit 1	路由条目 ID
set blackhole disable	黑洞路由，所以匹配该路由的数据包将被丢弃。该条目可以被其他路由分发。
set comment "	路由条目描述
set device "port1"	该路由表转发时的端口。
set distance 10	管理距离
set dst	目标地址
set dynamic-gateway disable	device 指定的端口为 pppoe,dhcp 模式，可以自动获得默认路由。则该参数开启，则该路由条目是针对这些路由的配置。
set gateway 192.168.100.1	路由的下一跳地址
set priority 0	路由的优先级，对象相同的路由条目，管理距离相同时较低的数值优先使用。
set weight 0	路由条目的权重，与 ECMP 功能相配合，根据权重值对流量进行分配。

4.2. 策略路由

4.2.1. 配置页面

该策略路由定义所以从 port2 进入的，源地址是 192.168.118.0 255.255.255.0，目的地址是 10.0.0.0 255.0.0.0 的数据包，都会被强制由 port1 转发，转发时下一条的网关地址为 192.168.1.1.

页面内选项如下：

协议端口： 协议类型，0 为所有，可以指定 6, 17, 132 等

进入接口： 流量进入接口。

源地址掩码： 数据包的源地址

目的地址掩码： 数据包的目的地址

目的端口： 目的端口，默认为所有。从 1-65536

强制流量到： 数据包的流出接口。

网关地址： 流出接口的下一条网关地址。

4.2.2. 配置命令

```
config router policy
    edit 1
        set input-device "port2"
        set src 192.168.118.0 255.255.255.0
        set dst 10.0.0.0 255.0.0.0
        set gateway 192.168.1.1
        set output-device "port1"
    next
end
```

4.2.3. 命令参数

config router policy	
edit 1	策略路由条 ID
set input-device "port1"	数据流入的接口
set src 0.0.0.0 0.0.0.0	数据的源地址
set dst 0.0.0.0 0.0.0.0	数据的目的地址
set start-port 1	目的起始端口,仅适用于 TCP,UDP,SCTP
set end-port 65535	目的结束端口,仅适用于 TCP,UDP,SCTP
set protocol 0	协议类型，0 为所有，可以指定 6,17,132 等
set gateway 1.1.1.1	路由的下一跳地址
set output-device "port2"	数据的流出接口
set tos 0x00	是否需要匹配 TOS 字段
set tos-mask 0x00	TOS 值的掩码
next	

4.3. 路由维护

4.3.1. 查看路由表

查看全部路由表：

```
Fortigate # get router info routing-table all

Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP

       O - OSPF, IA - OSPF inter area
```

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-I

* - candidate default

S* 0.0.0.0/0 [5/0] via 192.168.118.1, wan1

C 10.10.80.0/24 is directly connected, wifi

C 11.0.0.0/24 is directly connected, internal

C 192.168.1.0/24 is directly connected, internal

C 192.168.118.0/24 is directly connected, wan1

查看某种类型的路由条目：

get router info routing-table ospf （其他可选项/bgp/static/rip/connected）

4.3.2. 查看转发表

Fortigate # get router info kernel

tab=254 vf=0 scope=253 type=1 proto=2 prio=0 0.0.0.0/0.0.0.0/0->192.168.118.0/24

pref=192.168.118.28 gwy=0.0.0.0 dev=5(wan1)

tab=254 vf=0 scope=253 type=1 proto=2 prio=0 0.0.0.0/0.0.0.0/0->10.0.0.0/24 pref

=10.0.0.1 gwy=0.0.0.0 dev=4(wan2)

4.3.3. 查看协议状态

可以查看 ospf,bgp,bfd 等协议相关信息。

Fortigate # get router info

routing-table show routing table information

protocols show routing protocols information

rip show rip information

ospf show ospf information

bgp	show router info bgp information
multicast	show routing multicast information
bfd	show BFD information
isis	show isis information
kernel	show kernel routing table
vrrp	show vrrp status
gwdetect	show gwdetect status

4.3.4. 路由协议诊断

```
Fortigate-VM64 # diagnose    ip router ospf
all           all OSPF debug
events        OSPF Events
ifsm          OSPF Interface State Machine
level         debug level
lsa           OSPF Link State Advertisement
nfsm          OSPF Neighbor State Machine
nsm           OSPF NSM information
packet        OSPF Packets
route         OSPF route information
show          show status of ospf debugging
```

第5章.飞塔防火墙策略配置

5.1. 防火墙对象

可以直接对策略内引用的地址和服务对象进行编辑。由于飞塔防火墙是面向对象的配置方法，当修改一个地址后，所有引用该对象的策略都会因为引用该对象而自动改变。

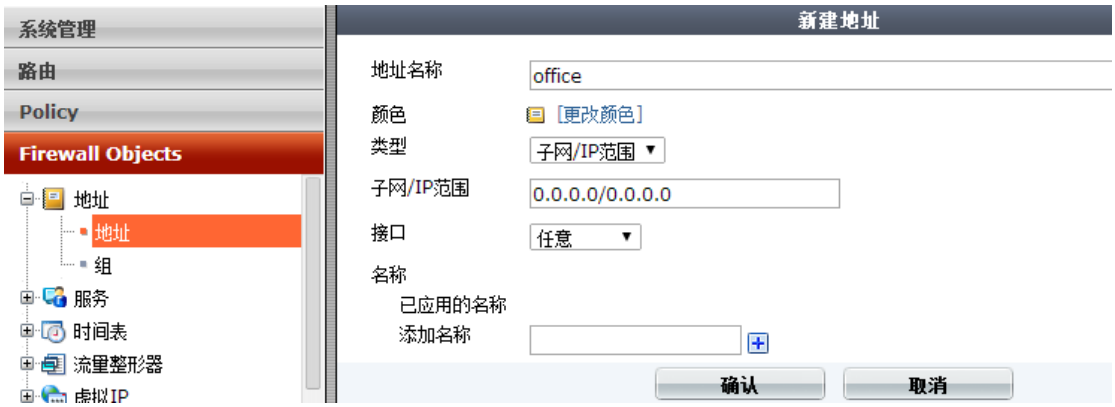
如果仅修改一条策略内的对象，则通过建立新的对象来实现。

如果想修改某个对象，来实现所有与该对象关联的配置自动更新，直接编辑对象即可。

5.1.1. 地址对象

5.1.1.1. 自定义 IP 地址

配置页面：



地址名称： 用于标识。

颜色：用于区分，归类

类型：支持如下类型

fqdn	基于域名 (www.baidu.com)
geography	根据 IP 所属地理位置 (,根据地址归属地区的数据库决定，如 China)
ipmask	地址和掩码 （10.0.0.0/8, 10.0.0.0/255.255.255.0）
iprange	地址范围 (192.168.1.[1-100])
wildcard	不规则掩码 (10.0.0.0/ 255.0.0.1)

接口：接口地址的管连接口， ‘任意’则该地址可以被基于接口的地址所引用，如果指定具体的接口，则该地址对象在策略中只能被该接口所使用。

配置命令

```
config firewall address
    edit "office"
        set subnet 192.168.1.0 255.255.255.0
    next
end
```

5.1.1.2. 定义ＩＰ地址组

配置页面：

配置命令：

```
config firewall addrgrp
    edit "group1"
        set member "IT" "insde" "office"
    next
end
```

5.1.1.3. 命令参数

config firewall address	
edit "PBX_Hqclient"	地址名称
set associated-interface "	关联接口。该对象仅关连接口可调用。不指定则为任意接口
set color 0	颜色，用于 WEB 页显示
set comment "	对象描述
set type iprange	地址类型： fqdn 基于域名 geography 根据 IP 所属地理位置 ipmask 地址和掩码 iprange 地址范围 wildcard 不规则掩码
set end-ip 11.156.141.53	结束地址
set start-ip 11.156.141.50	起始地址

next	
edit "11.156.108.EAIH_GW_IN1"	
set associated-interface "	
set color 0	
set comment "	
set type ipmask	
set subnet 11.156.108.22 255.255.255.255	地址内容
next	
edit "*.*.151.*"	
set associated-interface "	
set color 0	
set comment "	
set type wildcard	不规则掩码
set wildcard 0.0.151.0 0.0.255.0	地址内容，所有第三位是 151 的 ip 地址。 如 10.0.151.0，202.1.151.0，
next	

5.1.2. 服务对象

系统中默认对标准的服务端口进行的“预定义”，在策略中引用即可。

5.1.2.1. 自定义服务对象

配置页面如下：

每一个服务对象中可以包括多个端口，多种协议，可以直接定义端口范围。

配置命令：

config firewall service custom

```
    edit "QQ"
        set protocol TCP/UDP/SCTP
        set tcp-portrange 8000
        set udp-portrange 4000-8000
    next
end
```

5.1.2.2. 定义服务组


```
config firewall service group
    edit "offceservice"
            set member "DNS" "HTTP" "HTTPS" "POP3" "SMTP"
    next
end
```

5.1.2.3. 命令参数

config firewall service custom	
edit "TCP_6671"	服务对象名称
set protocol TCP/UDP/SCTP	协议类型： ICMP icmp 类型和代码 ICMP6 icmp6 类型和代码 IP IP 协议号 TCP/UDP/SCTP tcp/udp/sctp
set check-reset-range default	ICMP 错误信息校验使用 global 参数
set comment "	描述
set color 0	颜色，用于 WEB 页显示
set tcp-portrange 6671	TCP 端口范围
unset udp-portrange	UDP 端口范围
unset sctp-portrange	SCTP 端口范围
set tcp-halfclose-timer 0	半关闭状态超时时间

set tcp-halfopen-timer 0	半连接状态超时时间
set tcp-timewait-timer 0	Time-waiter 时间
set udp-idle-timer 0	UDP 超时时间
set session-ttl 0	会话超时时间。
next	

5.1.3. 时间表

5.1.3.1. 循环时间表


```
config firewall schedule recurring
        edit "always"                   //默认
        set day sunday monday tuesday wednesday thursday friday saturday
    next
    edit "worktime"
        set day sunday monday tuesday wednesday thursday friday saturday
        set end 18:00
        set start 09:00
    next
end
```

5.1.3.2. 单次时间表


```
config firewall schedule onetime
```

```
    edit "testoneyear"
        set end 00:00 2015/01/01
        set start 00:00 2014/01/01
    next
end
```

5.1.4. 虚拟 IP

5.1.4.1. 一对一 IP 地址映射


```
config firewall vip
    edit "webserver"
        set extip 202.0.0.167          // 映射给外部的 ip 地址，可以是范围
        set extintf "port1"
        set mappedip 192.168.0.168     //内部服务器实际的 ip 地址
    next
end
```

5.1.4.2. 一对多端口转发映射

可以将以公网 ip 的地址，分别映射到不同的内网 ip 上:

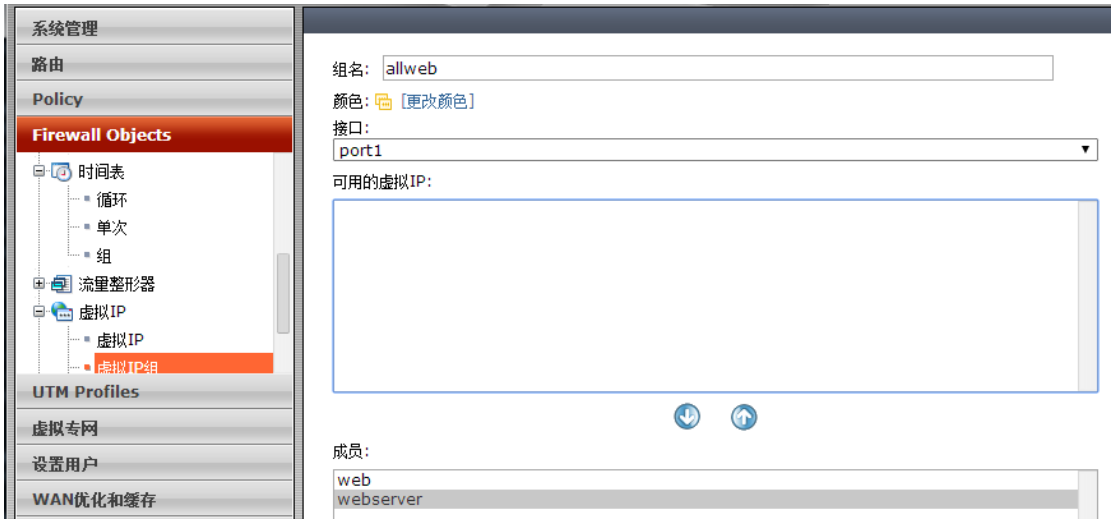
公网 ip	公网端口	内网 ip	内网端口
11.1.1.1	80----------	10.0.0.1	80
11.1.1.1	81----------	10.0.0.2	81
11.1.1.1	1443----------	10.0.0.3	443

例 1：

```
config firewall vip
    edit "web"
        set extip 11.1.1.1              //映射给外部的 ip 地址
        set extintf "port1"
        set portforward enable          //启用端口转发
        set mappedip 10.0.0.1           //内部服务器实际的 ip 地址
        set extport 80                  //映射给外部的访问端口，可以是范围
        set mappedport 80               //内部服务器实际的服务端口
    next
end

config firewall vip
    edit "web"
        set extip 11.1.1.1
        set extintf "port1"
        set portforward enable
        set mappedip 10.0.0.2
        set extport 1080-1100           //端口范围
        set mappedport 80-100           //端口范围
    next
end
```

5.1.4.3. 虚拟 ip 地址组




```
config firewall vipgrp
    edit "allweb"
        set interface "port1"
            set member "web" "webserver"          //vip 地址组成员
    next
end
```

5.1.4.4. 命令参数

config firewall vip	
edit "test"	对象名字
set id 0	ID 序号
set comment "	描述
set type static-nat	类型静态映射，或负责均衡
set extip 1.1.1.1	外部 IP
set extintf "port2"	外部接口
set arp-reply enable	是否允许 ARP 应答
set nat-source-vip disable	只允许某些 IP 地址访问该 VIP
set portforward enable	端口转发，进行端口映射
set gratuitous-arp-interval 0	为这个 VIP 发送免费 arp，0 为不发送
set color 0	颜色，用于 WEB 页显示
set mappedip 192.168.1.11	内部被映射的 IP 地址
set protocol tcp	协议类型 TCP
set extport 80	外部端口

set mappedport 1080	内部端口
next	
end	

5.2. 防火墙策略

防火墙的策略按照从上网下的顺序执行，直到数据包匹配到策略为止。

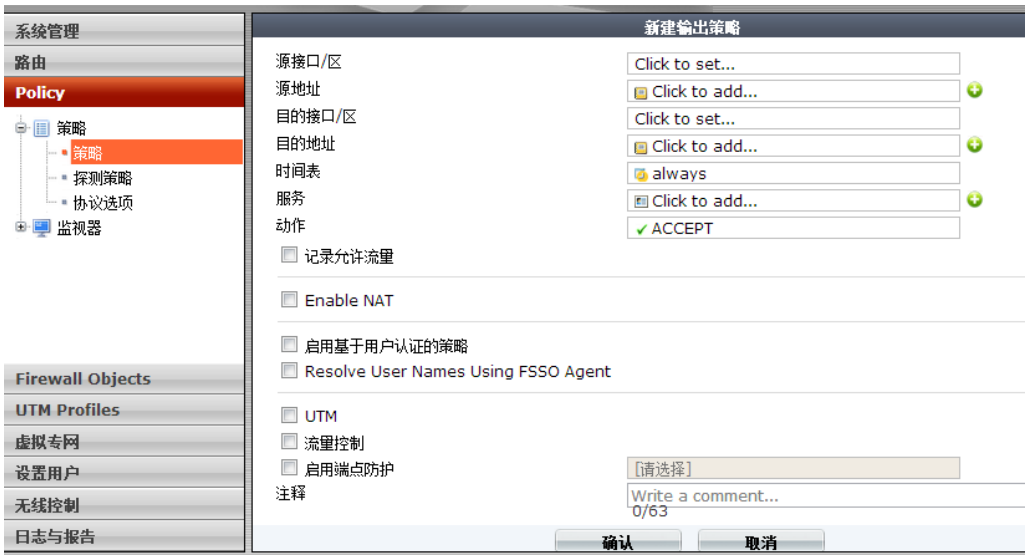
（1）源 ip，目的 ip 覆盖范围较小的放在范围较大的策略之前。

（2）匹配业务量较大的策略放在其他策略之前，减少策略匹配次数。

（3）策略尽可能的做到精确匹配，减少 any,all 等地址对象的使用。

5.2.1. 访问策略

1) WEB 页面操作：



源接口：数据包进入的接口。

源地址：源 IP 地址。

目的接口：数据包流出的接口

目的 IP：需要访问的目的 ip.

时间表：可以通过时间对策略进行控制，默认选择 always.

服务：允许访问目的地址的那些服务端口。

动作：accept, deny，ssl, ipsec 等。

Enable NAT：是否开启 NAT.

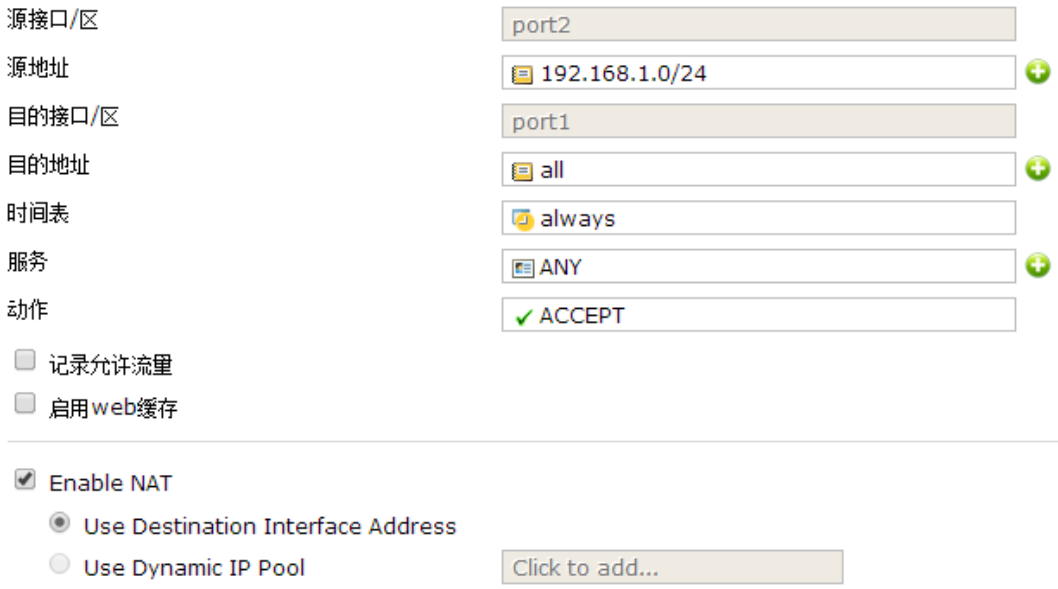
2) CLI 操作：

```
config firewall policy
    edit 1193                              //注意ID号不要重复，否则会覆盖原有配置。
        set srcintf "port2"                //源接口
        set dstintf "port1"                //目的接口
            set srcaddr "11.133.16.*"      //源IP
            set dstaddr "11.156.77.7-8"    //目的IP
        set action accept                  //动作
        set schedule "always"              //时间表
            set service "10080-10082"      //服务
    next
```

3) 克隆策略

如果要增加的新的策略与原有策略在一些参数上相同，则可直接克隆一个新的策略,然后对其进行编辑。

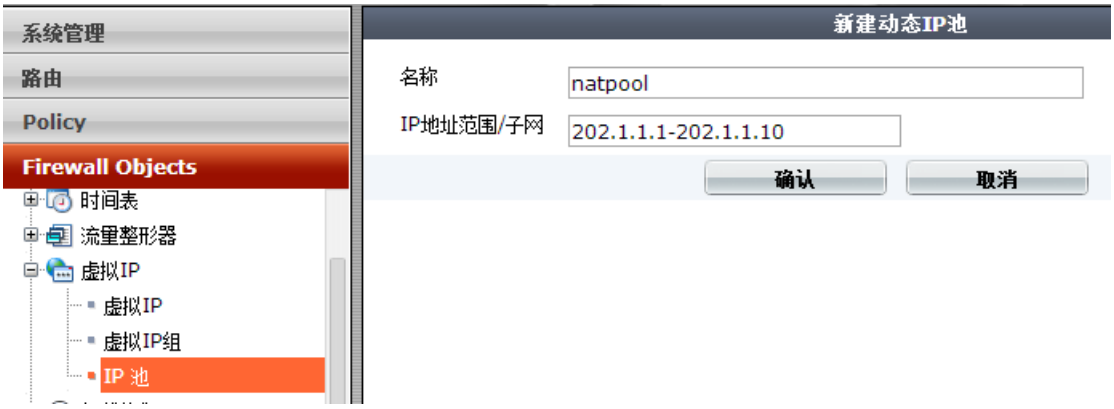
5.2.2. SNAT 策略



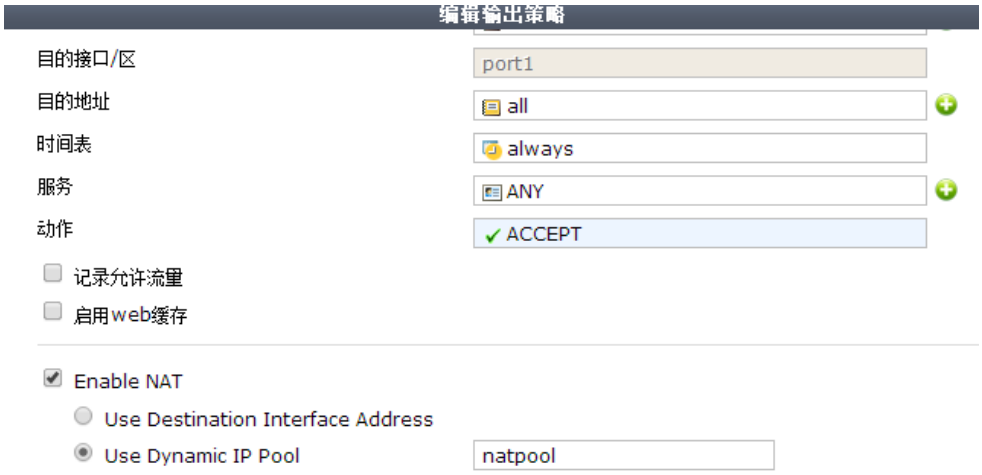
Enable NAT 有 2 个选项：

- Use Destination Interface Address：当 192.168.1.0/24 网段需要通过 port1 口进行访问的时候，会被 NAT 成接口 port1 的 ip 地址。
- Use Dynamic IP Pool：将源地址翻译成地址池内的 ip 地址。

（1）定义策略对象，ippool：



（2）配置策略：



配置命令如下：

```
config firewall ippool
    edit "natpool"
        set endip 202.1.1.10
        set startip 202.1.1.1
    next
end

config firewall policy
    edit 1
        set srcintf "port2"
        set dstintf "port1"
            set srcaddr "office"
            set dstaddr "all"
        set action accept
        set schedule "always"
            set service "ANY"
        set nat enable                          //开启 NAT
        set ippool enable                       //使用地址池
            set poolname "natpool"              //指定地址池名称
    next
end
```

5.2.3. 虚拟 IP 策略(DNAT)

主要用于将内部的服务器映射到公网：

（1）定义 VIP

参照 5.1.4.

```
config firewall vip
    edit "webserver"
```

```
        set extip 202.0.0.167              // 映射给外部的 ip 地址，可以是范围
        set extintf "port1"
        set mappedip 192.168.0.168         //内部服务器实际的 ip 地址
    next
end
```

（2）配置策略

目的地址：配置为定义好的 VIP 映射对象。

该策略允许从 por1 口进入的所有地址，访问 202.0.0.167，防火墙接收到访问该地址的数据包后，会根据 vip 映射的配置内容，将数据包的目的地址转换为 192.168.0.168，并发送给该服务器。

5.2.4. NAT 配置注意事项

防火墙策略做 NAT 的时候有 2 个选项，如下图所示，

1) use destintaion interface address:转换成策略中目的接口上所配置的ＩＰ地址.

如策略为 internal 到 wan 口的策略，internal 口地址为 192.168.1.1/24；wan 口地址为 202.0.0.1/24 则所有从匹配该策略的数据包原地址被转换为 202.0.0.1。

如果 internal 口内有一台服务器 192.168.1.100/24，被通过 vip 映射为 202.0.0.100，并配置了从 wan 到 internal 口的相关策略，则 192.168.1.100 主动访问外部网络的时候会被 NAT

成 202.0.0.100，而并不是 202.0.0.1. 因为 VIP 定义的时候与 wan 口关联，被优先选作 192.168.1.100 外出访问的转换地址。

2) use Dynamic ip Pool.使用动态地址池作为 NAT 之用

可以在 vip 页面中定义地址池，该选项使策略会优先使用地址池内定义的地址.

在转换时按如下优先顺序工作：动态地址池＞vip 映射＞外网口地址

5.2.5. CLI 批量添加策略

直接双击策略条目，进行编辑，与新建操作方法相同。

如下主要介绍如何进行批量的策略编辑。

1) 通过命令行对策略进行编辑保存为文本文件，如 policy.txt 的

2) 选择如下菜单： 从….执行脚本

3) 点击“选择文件“按钮，选择配置脚本文件，并应用。

5.2.6. VOIP 策略

对于所有 VOIP 业务，需要使用 UTM 功能内的 VOIP profile 来实现 ALG 功能。

（1） 单独为 voip 业务建立一条新策略。

```
config firewall policy
    edit 100                                    //新的策略 ID，不要与现有策略重复
```

```
        set srcintf "port1"                          //源接口
        set dstintf "port2"                          //目的接口
            set srcaddr "all"                          // 源地址
            set dstaddr "voipserver"                   //voip 服务器 ip 地址
        set action accept
        set schedule "always"
            set service "ANY"                          // 根据需要配置
        set utm-status enable                        //开启 utm 功能
        set voip-profile "default"                   // 开启 voip 脚本
        set profile-protocol-options "default"       // 协议选项
    next
end
```

其他参数根据实际网络情况配置。

（2） 将该策略移动到合适的位置，确保其可以被执行。 如下是将策略 100 移动到策略 11 前面。

```
config firewall policy
      move 100 before   11
end
```

5.3. 流量控制

飞塔的流量控制功能是基于策略实现的，即对匹配该策略的所有流量进行流控，通过策略来对用户分组，不同的策略中配置不同的流控脚本。

5.3.1. 基本配置

打开防火墙策略配置页面，可以看到配置页面下部的流量控制选项：

流量控制： 是否对该策略使用流量控制功能。

共享流量控制：

匹配该策略的所有的 IP 共享的流量，该流量是指匹配该策略的所有会话内的上行和下行流量总和。

反向流量控制：

如果希望上行和下行单独控制，则可以使用该功能。

上图中策略的方向为 internal-wan 口。 如果开启反向流量控制，那么：

共享流量控制针对从 internal-wan 方向的流量控制： 5M，

反向流量控制针对从 wan-internal 方向的流量控制： 10M。

针对每个 ip 的流量控制

匹配该策略的每个 ip 的流量控制。该参数为每个 ip 地址的上行与下行流量之和。

5.3.2. 共享流量控制

为了在策略中进行流量控制配置，需要定义好流量控制的对象脚本，然后在策略中引

用。配置页面如下

命令行：

config firewall shaper traffic-shaper

edit <shaper_name> ...

set priority {high | medium | low}

set maximum-bandwidth <rate>

set guaranteed-bandwidth <rate>

next

end

名字：自定义，用于标识。

应用控制： 设备该流控脚本如何被策略应用

每条策略： 每个使用该脚本的策略独立进行流控。

比如有 10 条策略引用了 5M 的流控脚本，那么每条策略均可以使用 5M 的带宽。

所有使用这个流量控制的策略：所有使用该脚本的策略共同进行流控。

比如有 10 条策略引用了 5M 的流控脚本，那么所有策略内的用户共同使用这 5M 的带宽，即这 10 条策略流量加起来不会超过 5M

流量优先级：

防火墙接口上定义了 6 个 FIFO 队列，0-5,0 为最高优先级，5 为最低。

0 队列用于防火墙的管理，vpn 协商等，所有由防火墙发起，或者到达防火墙的流量会自动被放入队列 0 中，最优先被转发。

对于防火墙转发的在策略中使用 traffic shaper 功能的流量，其优先级可以分为高、中、低三个级别，级别高的流量会优先被防火墙转发。分别对应于转发对队列的 1,2,3，即：

高（队列 1）、中（队列 2）、低（队列 3）

可以根据业务类型进行分类，将 VOIP 等业务设置为高优先级，http, pop3,sntp，OA 系统等配置为中优先级，其他的业务放入低优先级。

如果策略中未指定任何级别的优先级，则默认被放入高优先级。

最大带宽：

该策略所能达到的最大带宽，单位 kbps。当流量超过该闸值的时候，超过流量的数据包会被丢弃。配置为 0 ，则意味着最大带宽不受限制。

保证带宽：

该策略能够得到的保证带宽。当流量低于该值的时候，数据包会被放入到队列 0 中，也就是获得最优先的转发，保证该业务占用的最少带宽数量。不建议对非关键业务配置该参数。

当策略占用带宽介于最大带宽和保证带宽之间的时候，则按照策略内定义的优先级进行转发。

DSCP：是否使用 DSCP 差分服务代码点，其用于整个网络中配置端点到端点的 QOS 服务。

5.3.3. 每 IP 流量控制

进入如下页面进行配置：

脚本：

```
config firewall shaper per-ip-shaper
    edit "1M"
        set diffserv-forward disable
        set diffserv-reverse disable
        set max-bandwidth 1000
        set max-concurrent-session 200
    next
end
```

名字： 自定义

最大带宽：策略内的每个 ip 所能够使用的最大带宽，为上行和下行流量总和。

最大并发连接数： 匹配该策略的每个用户所能够发起的最大连接数。超过该连接数后，用户无法建立新的连接。

正向 DSCP：是否使用 DSCP 差分服务代码点，用于整个网络中配置端点到端点的 QOS 服务

反向 DSCP：是否使用 DSCP 差分服务代码点，用于整个网络中配置端点到端点的 QOS 服务

5.4. 配置 session-ttl

会话生存时间，即会话建立后无任何数据传送情况下的存活时间，默认为 3600 秒，当该会话在超时之前有任何数据匹配该会话，则该会话 ttl 计时器复位到该数值，如 3600 秒。

1) 配置全局 session-ttl

```
config system session-ttl
    set default 604800                    //300-604800 秒(最大为 7 天)
end
```

2) 全局指定服务端口 session-ttl

```
config port
    edit 1320
        set protocol 6
        set timeout 1800
        set end-port 1320                 //起始端口
        set start-port 1320               //结束端口
    next
end
```

3) 策略 session-ttl

```
config firewall policy
    edit 1
        set srcintf "internal"
        set dstintf "wan1"
            set srcaddr "all"
            set dstaddr "all"
        set action accept
        set schedule "always"
            set service "ANY"
        set session-ttl 604800
        set nat enable
    next
end
```

4) 服务对象 session-ttl

定义不同的对象，虽然同为 23 端口，可以配置指定不同的 **session-ttl** 时间。

```
config firewall service custom
    edit "telnet"
        set protocol TCP/UDP/SCT
        set tcp-portrange 23
        set session-ttl 7200
    next
    edit "telnetnew"
        set protocol TCP/UDP/SCTP
        set tcp-portrange 23
        set session-ttl 3600
    next
end
```

5) session-ttl 的优先级

低 → → 高

全局 session-ttl < 全局指定服务端口 session-ttl < 策略 session-ttl < 服务对象 session-ttl

优先级高的 session-ttl 优先被使用。

5.5. 配置 timer 计时器

可以通过 Config system global 内参数来修改防火墙的一些 timer 计时器。

1) set tcp-halfopen-timer

用于定义 tcp 半连接状态的定时器。默认为 120 秒。

相关状态：SYN_SENT, SYN & SYN/ACK

2) set tcp-halfclose-timer

用于定义 tcp 半关闭状态的定时器。默认为 120 秒。

相关状态：CLOSE_WAIT，FIN_WAIT.

3) set tcp-timewait-timer

用户定义 timer-waiter 状态后的定时器。默认为 1 秒。

定时器超时前，该会话不会被清除。参考值 30 秒。

4) set udp-idle-timer

定义 UDP 会话超时时间,默认为 180 秒。

5) ICMP 超时时间。

该参数定时器不可修改，默认为 60 秒。

5.6. 配置 ALG

飞塔支持如下协议的 ALG 配置。

序号	name	port	protocol
1	pptp	1723	6
2	h323	1720	6
3	ras	1719	17
4	tns	1521	6
5	tftp	69	17
6	rtsp	554	6
7	rtsp	7070	6
8	rtsp	8554	6
9	ftp	21	6
10	mms	1863	6
11	pmap	111	6
12	pmap	111	17
13	sip	5060	17
14	dns-udp	53	17
15	rsh	514	6
16	rsh	512	6
17	dcerpc	135	6
18	dcerpc	135	17
19	mgcp	2427	17

20	mgcp	2727	17

5.6.1. 删除 ALG

show system session-helpe
查看现有 ALG 配置
config system session-helper
edit 1
set name pptp
set port 1723
set protocol 6
next
.....more
edit 14
set name dns-udp
set port 53
set protocol 17
next
..... more
edit 20
set name mgcp
set port 2727
set protocol 17
next
end
默认配置中共 20 个。删除 DNS 的 ALG，命令如下：

config system session-helper

delele 14

end

5.6.2. 添加 ALG

如果网络中存在非标准端口的与 ALG 相关的服务，则需要手动添加，比 TCP 2021 端口的 FTP 服务。

config system session-helper
edit 21 //不要与现网 ID 重复
set name ftp
set port 2021 // FTP 协议使用的端口

set protocol 6 // 6 TCP 协议， 17UDP 协议

next

5.7. 查看会话信息

1) 查看系统会话信息

FG3K9B3E10700335 (global) # **diagnose sys session full-stat**

session table: table_size=2097152 max_depth=1 used=14

expect session table: table_size=32768 max_depth=0 used=0

misc info: **session_count=7 setup_rate=0** exp_count=0 clash=0

memory_tension_drop=0 ephemeral=0/851968 removeable=0 ha_scan=0

delete=0, flush=0, dev_down=0/0

TCP sessions:

1 in ESTABLISHED state

firewall error stat:

error1=00000000

error2=00000000

error3=00000000

error4=00000000

tt=00000000

cont=00000000

ids_recv=00000000

url_recv=00000000

av_recv=00000000

fqdn_count=00000000

tcp reset stat:

syncqf=3 acceptqf=0 no-listener=81 data=0 ses=0 ips=0

当前并发会话：session_count=7

新建会话速度：setup_rate=0

2) 会话列表查看

Fortigate # get sys session list

PROTO EXPIRE SOURCE SOURCE-NAT DESTINATION DESTINATION-NAT

tcp 3600 192.168.1.110:50299 - 192.168.1.99:22 -

tcp 32 192.168.1.110:50289 192.168.118.28:29945 173.194.72.147:443 -

tcp 101 192.168.1.110:50296 192.168.118.28:21744 112.64.234.191:12000 -

tcp 3559 192.168.1.110:50298 192.168.118.28:38130 192.168.118.8:23 -

3) 详细会话状态查看

dia sys session list 该命令输出信息较多，需要先通过 filter 进行过滤。

Fortigate # dia sys session filter

clear clear session filter

dport dest port

dst dest ip address

duration duration

expire expire

negate inverse filter

nport NAT'd source port

nsrc NAT'd source ip address

policy policy id

proto protocol number

proto-state protocol state

sport source port

src source ip address

vd index of virtual domain. -1 matches all

例：产看源地址是 192.168.1.110,目的端口是 23 的会话

Fortigate # dia sys session filter dport 23

Fortigate # dia sys session filter src 192.168.1.110

Fortigate # dia sys session list

session info: **proto=6 proto_state=07 duration=333 expire=101 timeout=3600** flags=00000000

sockflag=00000000 sockport=0 av_idx=0 use=3

origin-shaper=

reply-shaper=

per_ip_shaper=

ha_id=0 hakey=30582

policy_dir=0 tunnel=/

state=may_dirty

statistic(bytes/packets/allow_err): org=2916/70/1 reply=5389/64/1 tuples=2

orgin->sink: org pre->post, reply pre->post dev=11->5/5->11 gwy=192.168.118.8/192.168.1.110

hook=post dir=org act=snat 192.168.1.110:50298->192.168.118.8:23(192.168.118.28:38130)

hook=pre dir=reply act=dnat 192.168.118.8:23->192.168.118.28:38130(192.168.1.110:50298)

pos/(before,after) 0/(0,0), 0/(0,0)

misc=0 policy_id=1 id_policy_id=0 auth_info=0 chk_client_info=0 vd=0

serial=00005ff1 tos=ff/ff ips_view=0 app_list=0 app=0

dd_type=0 dd_rule_id=0

per_ip_bandwidth meter: addr=192.168.1.110, bps=167

total session 1

session info:

proto=6	协议类型 6 为 TCP ， 1 为 ICMP, 17 为 UDP。
proto_state=07	TCP 状态，代码为 7,close wait 状态。
duration=333	会话持续时间
expire=101	超时时间，与 proto_stat 状态相关
timeout=3600	session ttl.

4) 查看某个 IP 相关会话总数

Fortigate # dia sys session filter src 192.168.1.110 //查看源地址为 192.168.1.110 的会话

Fortigate # diagnose sys session list | grep total //根据 filtger 过滤条件查看会话总数

5) 清除会话

dia sys session filter proto 17 //所有 UDP 会话

dia sys session clear //清除会话

如果不指定 filter 则清除所有的会话，谨慎使用。

6) 查看 session-ttl

Fortigate # get sys session-ttl

default : 3600

port:

Fortigate # get sys session-info ttl

list session timeout:

Default timeout=3600

5.8. 策略配置命令

config firewall policy	
edit 1	条目 ID
set srcintf "port2"	源接口
set dstintf "port1"	目的接口
set srcaddr "all"	源地址
set dstaddr "all"	目的地址
set rtp-nat disable	对接收的 RTP 包做 NAT
set action accept	策略处理动作：accetp, deny,ssl，ipsec
set status enaable	策略状态，禁用或启用
set dynamic-profile disable	关闭动态脚本功能
unset dynamic-profile-access	设置动态脚本协议选项
set schedule "always"	配置策略时间表
set schedule-timeout disable	时间表超时后，强制清除相关会话
set service "ANY"	服务

set utm-status disable	关闭或开启 UTM 功能
set logtraffic disable	不对允许流量进行记录
set auto-asic-offload enable	启用 ASIC 芯片加速功能
set webcache disable	关闭 WAN 优化功能中的 WEB cache 功能
set session-ttl 0	配置策略的 session ttl.
set wccp disable	关闭 WCCP 功能
set fsso disable	不启用单点登录
set disclaimer disable	是否显示用户认证策略的认证界面的声明
set natip 0.0.0.0 0.0.0.0	用于 IPsec 策略，对外出的流量进行 NAT 转换
set match-vip disable	对未能匹配目标地址是 VIP 地址的策略的数据包进行匹配。用于对为匹配 vip 的流量做日志记录。
set diffserv-forward disable	QOS 选项，对 DSCP 进行处理，对转发的数据包根据配置修改 DSCP 值
set diffservcode-forward 000000	转发包的 DSCP 值范围为 000000-111111
set diffserv-reverse disable	对应答数据包进行 DSCP 处理
set diffservcode-rev 000000	应答包的 DSCP 值范围为 000000-111111
set tcp-mss-sender 0	配置发送的 TCP 最大传输单元
set tcp-mss-receiver 0	配置接收的 TCP 最大传输单元
set comments "	策略描述
set endpoint-check disable	是否启动端点检查，是否安装 forticlient
set label "	配置策略的分区视图标签（web 页面显示）
set global-label "	配置策略的全局视图标签（web 页面显示）
set replacemsg-override-group "	是否启用独立的替换信息
set identity-based disable	是否启用基于用户认证的策略
set traffic-shaper "	流量控制
set traffic-shaper-reverse "	反向流量控制
set per-ip-shaper "	针对每个 ip 的流量控制
set nat disable	是否做 NAT 转换
set client-reputation disable	是否启用用户声望系统
next	

第6章. 飞塔防火墙 HA 配置

6.1. HA 配置要求

进行飞塔 HA 的配置，硬件和 OS 系需满足如下要求：

1) 防火墙硬件型号相同;

2) 同型号硬件需要为相同的硬件版本，内存容量,CPU 型号，硬盘容量等相同;

3) 相同的 OS 版本;

4) 设备的接口不能工作在 DHCP,PPPOE 模式下。

6.2. HA 配置建议

1) 建议配置两条以上的心跳线缆，防止单心跳故障造成 HA 机群崩溃，使用独立的心跳接口，尽量避免与业务口混用。

2) 优先使用光纤接口。

3) 开启会话同步. set session-pickup enable(默认关闭)

4) 谨慎使用 override 功能。开启 override 后设备选举过程中 HA 优先级参数高于设备运行时间参数，可能造成期望成为备机的设备被选举为主设备，造成反向同步配置信息。

5) 更改默认的 HA 组的 ID，避免同一个广播域内存在多个 HA 机群，而造成接口的虚拟 MAC 冲突

6) 选择正确的监控端口和心跳端口，在开启 vdom 虚拟 cluster 时候，每个 cluster 需要单独配置。

7) 如果开启 ping server 功能，则需要再 H A 配置中添加相应的配置命令。

8) 进行 HA 环境下更换设备前，进行配置备份，防止操作失误而造成的配置丢失。

9) 建议将与飞塔防火墙相连的交换机接口配置为 fastport 模式，当发生切换时，交换机的接口可立刻进入转发状态。

6.3. HA 配置步骤

6.3.1. HA 初始配置

按照如下方法分别对要做 HA 的 2 台防火墙做如下配置。

进入系统管理>配置>高可用性页面，按下图进行配置：

对防火墙进行基础的 HA 配置需要如下几个步骤：

1 **定义工作模式**，‘主动－被动’或者‘主动－主动’，在大多数网络中会选择‘主动－被动’，即主设备进行业务处理，备机处于备份状态，当主设备发生设备故障或者接口链路故障后，则由备机继续处理业务。

2 **定义设备优先级**，优先级高的设备，优先被选为主设备。

3 **组名和密码**，使用默认即可，如设置则做 HA 的两台机器需要配置相同的参数。

4 **启用会话交接**，主墙和备墙之间实时进行会话信息的同步，当发生 HA 切换到时候，备墙上有同样的会话信息会对原来的会话进行处理，不会产生会话中断。

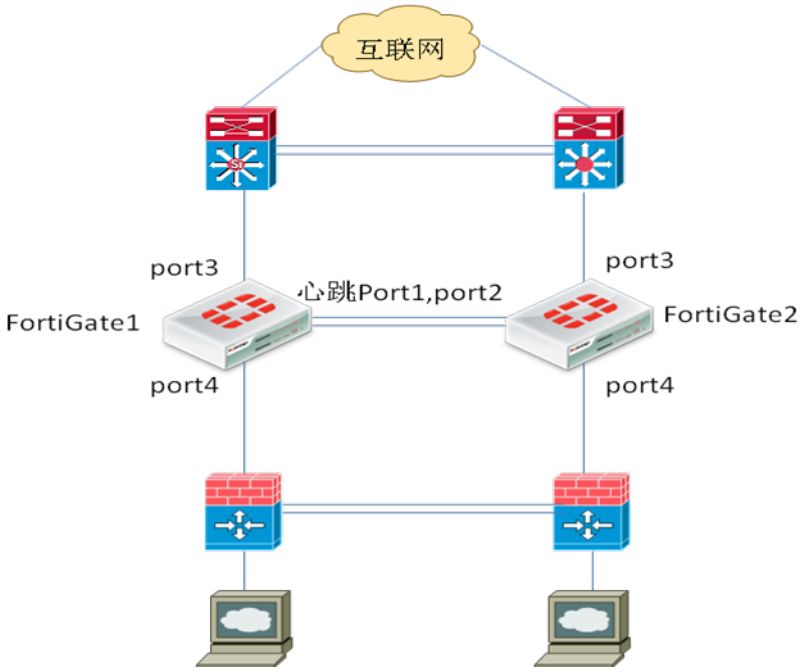
5 **定义 2 个心跳端口**，用于配置同步，会话同步，对方存活心跳检测等，为了集群的稳定建议配置 2 条或以上的线条线。

6 **定义监控端口**，业务端口需要被防火墙监控，当端口出现故障时会进行切换，具有数量多的有效监控端口的设备会作为主墙处理数据。

7 为该设备输入新名字（可选），主要是便于识别和操作方便。

6.3.2. 组建 HA 集群

按下图进行设备的连接，组建集群。



1 连接心跳线，Fortigate1 的 port1 连接 Fortigate2 的 port1，Fortigate1 的 port2 连接 Fortigate2 的 port2,

2 防火墙开始协商建立 HA 集群，此时可能会暂时失去和防火墙到连接，这是因为在 HA 协商过程中 FGCP 协议会改变防火墙接口到 MAC 地址。可以通过更新电脑的 arp 表来恢复连接，命令为 arp -d。

3 连接业务口链路。

4 组建好 HA 后，两台防火墙配置同步，具有相同的配置，通过访问主防火墙来进行业务配置，如 ip 地址，策略等。

6.4. HA 工作模式

配置的时候首先考虑到是使用a-p还是a-a模式。

```
config system ha
   set mode a-p      /a-a
end
```

6.4.1. Active-passive 模式

集群中到所有防火墙必须工作在同一个模式下。可以对运行中的H A集群进行模式的修

改，但会在成一定到延时，因为集群需要重新协商并选取新到主设备。

A-P模式提供了备机保护。HA集群中由一台主设备，和一台以上到从设备组成。从设备与主设备一样连接到网络，但不处理任何的网络会话，从设备处于备用状态。从设备会自动同步主设备到配置，并时刻监视主设备到运行状态。整个失效保护到过程是透明的，一旦主设备失效，从设备会自动接替其工作。如果设备到接口或链路出现故障，集群内会更新链路状态数据库，重新选举新的主设备。

6.4.2. Active-active 模式

A-A模式下会对UTM占用资源较多的进程进行在各个设备中进行分担。UTM需要处理协议识别、病毒扫描、ips、网页过滤、邮件过滤、数据防泄露、应用程序控制、voip内容扫描、协议保护（HTTP,HTTPS,FTP,IMAP,IMAPS,POP3,SMTP,SMTPS,IM,NNTP,SIP,SIMPLE）,SCCP协议控制等。通过对如上内容到负载均担，A-A模式可以提供更高的UTM性能。安全策略中的终端控制，流控，用户认证功能，在A-A模式下没有什么提高效果。其他非UTM功能不会进行负载分担，将由主设备进行处理。除了UTM功能外，还可以实现对TCP会话进行分担。AA模式下，集群中到主设备负责对所有通信会话的处理，然后将部分负载分发到所有从设备上。从设备可以说是活动的，因为要处理UTM的相关会话。

其他方面AA模式和AP模式是相同的。

6.5. HA 配置命令

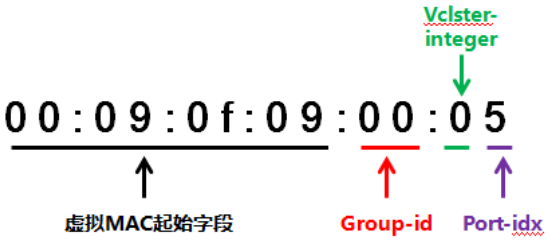
HA配置命令config system ha，如下是常用的配置命令。

1) set group-id 0

配置HA机群的组ID,一个机群内的成员必须有相同的组ID.该ID会成为生成防火墙接口的的虚拟MAC的一个组成因素，因此当同一个广播域有 2 组以上的HA机群的时候需要配置不同的组ID,防止MAC地址冲突.

接口虚拟 MAC 使用以下格式:

00-09-0f-09-<group-id_hex>-<vcluster_integer><idx>



2) set group-name "FGT-HA"

一个机群内的成员必须有相同的组名字

3) set mode standalone/a-a/a-p

HA工作模式，常用为a-p模式。AA模式下在HA状态中查看到HA的角色，有主设备及从设备,通常会被认为工作在主被模式下,实际上主主下设备虽然都在工作,仍会有一台作为集群的主设备用来控制和分配流量和会话给集群中的其他设备。AA模式默认情况下仅负载均衡UTM的流量,所以在下不使用UTM功能时建议使用AP模式。

4) set password

一个机群内的成员必须有相同的密码

5) set hbdev "port1" 50 "port2" 50

配置心跳接口。其中50为优先级，优先级高的被优先使用。

6) unset session-sync-dev

可以配置专门的心跳接口用于会话信息同步，默认和控制信息为同一心跳接口。

7) set route-ttl 10

路由转发表的存活时间。HA设备之间只同步转发表，不同步路由表。当一个备机被选举成主机后，其原有转发表的存活时间，单位秒。随后通过静态或动态路由协议生成转发表，继续工作。

8) set route-wait 0

主设备收到新的路由条目后，会等待x秒后，再同步给从设备。

9) set route-hold 10

主设备进行 2 次路由同步之间的间隔，防止路由震荡而造成反复更新路由。

10) set sync-config enable

配置文件自动同步，需要开启。

11) set encryption disable

是否允许使用AES-128和SHA1对心跳信息进行加密和完整性验证。

12) set authentication disable

是否使用SHA1算法验证心跳信息的完整性。

13) set hb-interval 2

发送心跳数据包的间隔，单位为每100ms.如配置2,则每200ms发送一个心跳信息。

14) set hb-lost-threshold 6

心跳信息连续丢失 6 个后则认为对方不再存活。

15) set helo-holddown 20

Hello状态时间。设备加入HA机群前等待的时间，防止由于未能发现所有的机群成员而造成Ha的反复协商。

16) set arps 5

设备成为主设备后，要发送免费arp来宣布自己的MAC地址，以便相连的交换机能够及时更新MAC地址表，该参数用于配置其发送的数量。

17) set arps-interval 8

发送免费arp的间隔，单位秒。

18) set session-pickup enable/disable

关闭或者开启会话同步，默认为disable。一般需要开启。

19) set session-pickup-delay{enable | disable}

仅对存活30秒以上的会话进行同步。开启后会对性能有所优化，但小于30秒的会话在HA切换的时候会丢失。默认为关闭，谨慎使用。

20) set link-failed-signal disable

防火墙上发生被监控端口失效触发HA切换的时候，是否将除心跳口外的所有端口shutdown一秒钟的时间，便于与之相连的交换机及时更新MAC表。

21) set uninterruptable-upgrade enable

是否允许无中断升级ＯＳ。系统自动分别对机群内的设备升级，并自动切换，不会造成业务的中断。

22) set ha-uptime-diff-margin 300

当进行HA选举时，启动时间为一个选举的一个参数，当 2 台设备启动时间差小于300

时则将该部分差异忽略，视为相同。

23) set override disable

默认为disable,H A 选举按如下顺序进行比较：有效接口数量>运行时间>HA优先级>设备序列号。Enable情况下，讯据顺序改变。有效接口数量> HA优先级>运行时间>设备序列号。每次设备加入或者离开机群，都会强制整个机群重新进行主设备的选举。

24) set priority 128

HA优先级，为便于管理，建议主设备200,从设备100.

25) set monitor port3 port4

配置需要被监控的端口，其有效数量多的设备成为主设备。

26) unset pingserver-monitor-interface

是否设置pingserver监控端口。

27) set pingserver-failover-threshold 0

pingserver触发的阀值，0则意味着任何的pingserver失效都会触发HA的切换。

28) set pingserver-flip-timeout 60

两次pingserver失效切换之间的间隔。如A发生失效，切换到B. 切过去之后发现B也是失效的，则需要等待60分钟的时间允许切换回A.

6.6. HA 维护命令

1) 查看 HA 配置信息

get system ha

2) 查看 HA 状态

get sys ha status

3) 管理备机

exec ha manage 0 (1)， 0 或者 1 为 HA 中的防火墙的 ID。

4) 查看 HA 是否同步

分别在主墙和备墙上执行 diagnose sys ha showcsum

FGT60B3907513417 # diagnose sys ha showcsum //查看主墙配置文件的 checksum

is_manage_master()=1, is_root_master()=1

debugzone

global: 03 c5 f2 9b a6 8e b6 15 e8 89 c3 ca 5c 29 9f e5

root: b5 e3 4c a9 60 8b e4 9e 4d 63 16 8c 90 cb 44 17

all: 65 c4 4d e9 af 9b ff c3 d5 26 ad b8 fd 29 bd 4b

checksum

global: 03 c5 f2 9b a6 8e b6 15 e8 89 c3 ca 5c 29 9f e5

root: b5 e3 4c a9 60 8b e4 9e 4d 63 16 8c 90 cb 44 17

all: 65 c4 4d e9 af 9b ff c3 d5 26 ad b8 fd 29 bd 4b

FGT60B3907513417 # exec ha manage 0 //管理备机。

FGT60B3908651894 $ diagnose sys ha showcsum // 查看备机配置文件的 checksum

is_manage_master()=0, is_root_master()=0

debugzone

global: 03 c5 f2 9b a6 8e b6 15 e8 89 c3 ca 5c 29 9f e5

root: b5 e3 4c a9 60 8b e4 9e 4d 63 16 8c 90 cb 44 17

all: 65 c4 4d e9 af 9b ff c3 d5 26 ad b8 fd 29 bd 4b

checksum

global: 03 c5 f2 9b a6 8e b6 15 e8 89 c3 ca 5c 29 9f e5

root: b5 e3 4c a9 60 8b e4 9e 4d 63 16 8c 90 cb 44 17

all: 65 c4 4d e9 af 9b ff c3 d5 26 ad b8 fd 29 bd 4b

比较两台设备的配置的 checksum 相同，则配置已经同步。

配置同步完成时，可以通过 console 观察到如下的信息：

slave succeeded to sync with master

5) HA 同步命令

exec ha synchronize start all

6) 查看 HA 运行时间差

diagnose sys ha dump 1

HA information.

vcluster id=1, nventry=2, state=work, digest=9e.70.74.a2.5e.4a...

ventry idx=0,id=1,FG50012204400045,prio=128,0,claimed=0,

override=0,flag=1,**time=0**,mon=0. //登陆的主机 time 永远为 0 //

mondev=port5,50

ventry idx=1,id=1,FG50012205400050,prio=128,-50,claimed=0,

override=0,flag=0**,time=58710**,mon=0. //time=58710*0.1 秒，意味着这台机器比登录的主机运行时间晚 5871 秒//

7) 主备切换

diagnose sys ha reset-uptime

在未开启 override 功能的时候防火墙选举主设备时，逐步比较如下参数：

- 有效的监控端口数量。
- 防火墙 HA 模式下的有效运行时间
- HA 优先级
- 防火墙序列号 SN

在防火墙接口全部正常工作的情况下，接口数相同看，运行时间为第二个要比较的参数，运行时间长的设备成为主机。

该命令用于将当前所登录的设备的 HA 主机选举参数”运行时间”复位，则其运行时间为 0,会少于备机的运行时间，触发 HA 切换，原来的备机由于运行时间长而且成为新的主机。

相关参数： set ha-uptime-diff-margin 300 （秒）

在 HA 选举过程中进行，2 台设备中运行时间差异小于 300 秒的时候则忽略不计，认为 2 台设备具有相同的运行时间。可以将该参数改小，便于 diagnose sys ha reset-uptime 的执行。

6.7. HA 模式更换备机

当 HA 模式下的防火墙，其中一个机群成员出现故障时，通常将其切换为备机状态，然后对其进行更换。

建议操作步骤如下：

1) 备份配置，防止误操作造成的配置丢失。

2) 将要更换的设备切换为备机。

3) 将事先配置好的新的备机启动，检查 HA 相关配置。
4) 关闭原有备机，拔掉网络线缆。
5) 接入新的备机，但只接入心跳线。由于具有较少的有效运行接口，新接入的备机不会被选为主设备。
6) 新的设备与原有主设备同步后，插入业务接口的线缆。
7) 进行 HA 设备切换测试，观察能否正常切换，切换过程中是否出现数据包丢失。防火墙的 HA 切换约在 1 秒之内.
8) 进行业务测试。

6.8. HA 模式设备升级

对现网中的 2 台防火墙进行更换，升级为新的飞塔防火墙。

建议操作步骤如下：

1) 割接前确认业务是否正常，并记录当前设备状态，如果 cpu,内存，会话，路由表等。
2) 关闭现网备机，断开业务链路。
3) 安装一台新的飞塔防火墙替代原有备机。
4) 新的飞塔防火墙正常启动后，插入业务线缆，同时断开旧设备的主防火墙线缆。
5) 进行链路测试,观察新上线飞塔防火墙工作是否正常;不正常且短时间内无法排除故障，则需要回退。
6) 链路正常则业务测试；不正常且短时间内无法排除故障，则需要回退。
7) 业务正常后接入第二台飞塔防火墙，先连接心跳电缆，进行 HA 同步。
8) 新的备机同步后，插入业务接口的线缆。
9) 进行 HA 设备切换测试，观察能否正常切换，切换过程中是否出现数据包丢失。飞塔防火墙的 HA 切换约在 1 秒之内.

回退步骤：

1) 恢复原防火墙主设备，同时切断新飞塔防火墙设备的电缆。
2) 链路测试
3) 恢复原防火墙备设备
4) 检测 HA 状态，HA 切换测试。

5) 业务测试。

6.9. HA 的 Ping server 配置

1) Ping server 配置

router gwdetect 是为了防止所谓端口‘假死’的问题，通过利用发送 ping 包来判断该端口链路是否可用。

config router gwdetect edit "wan2"	指定监控接口。
set failtime 3	检测数据包连续丢 3 个，认为该接口失效
set ha-priority 5	该接口 ping 检测失败后，HA 关联参数值增加 5
set interval 2	每 2 秒发送一个 ping 包
set server "8.8.8.8" "2.2.2.2	可以配置 2 个以上被检测的网关，只要有任何一个网关有回应，即认为该接口工作正常
end	

2) HA 相关联配置

如果只配置上述的配置，ping 检测失败时 H A 不会切换，只是去往该接口的路由不再有效。需要在 H A 配置中告诉防火墙 wan2 口的 pingserver 会作为 HA 切换的触发条件。

```
Config system ha
Set pingserver-monitor-interface wan2        //监视 wan2 口上的 pingserver
Set pingserver-failover-threshold 3          //ha 切换的闸值
set pingserver-flip-timeout 60               //连续 2 次 ping server 触发的 HA 切换的间隔
```

3) 参数说明

set ha-priority 5 与 pingserver-failover-threshold 3 相关联。两者相比较，当 wan2 接口 pingserver 检查失效后赋值增加 5，已经达到了闸值 3，所以触发 H A 会切换。如果 ha-priority =2，即使该接口 pingserver 检测失败，由于达不到触发的闸值，不会切换。

第7章.飞塔防火墙系统管理

7.1. 网络管理 SNMP

7.1.1. 基本配置

1) 接口上开启 SNMP 管理

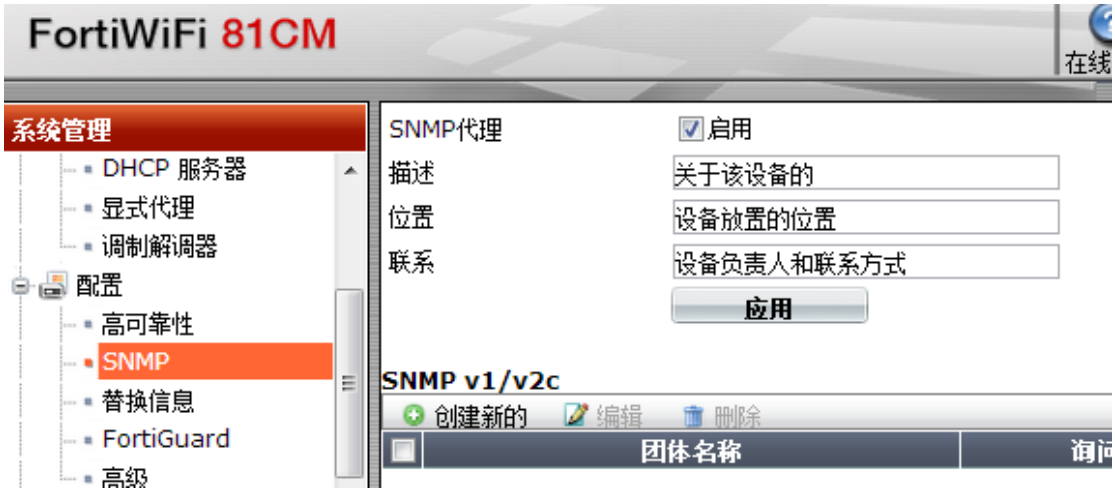
config system interface

edit "internal"

set allowaccess ping snmp //开启 SNMP 管理选项

next

2) 启用 snmp 代理，并填写相关信息

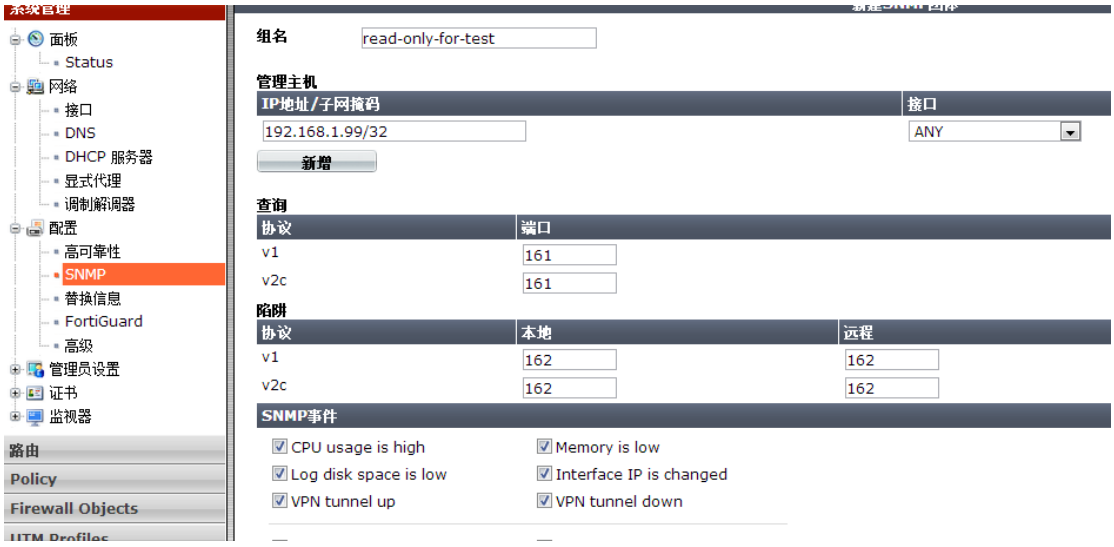


config system snmp sysinfo

set status enable

end

3) 添加 SNMP Community.



编写组名，添加管理主机的地址，选择 snmp 事件。

相关命令如下：

```
config system snmp community
    edit 1
        config hosts
            edit 1
                set ip 192.168.1.99 255.255.255.255
            next
        end
        set name "read-only-for-test"
    next
end
```

7.1.2. 诊断命令

Fortigate # dia deb en

Fortigate # dia deb application snmpd -1 /0 为关闭

Fortigate # snmpd: <msg> 59 bytes 192.168.1.110:18417 -> 192.168.1.99/192.168.1.

99:161 (itf 11.11)

snmpd: checking if community "read-only-for-test" is valid

snmpd: checking against community "read-only-for-test"

snmpd: request 1(root)/11/192.168.1.110 == comm 1/0/192.168.1.0/255.255.255.0

snmpd: matched community "read-only-for-test"

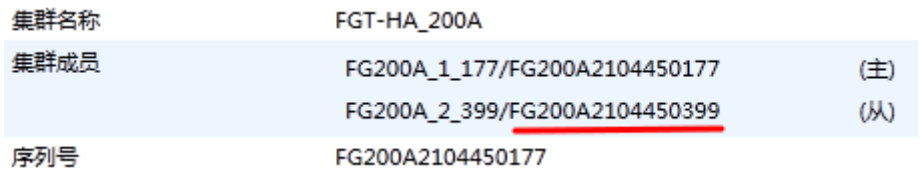
snmpd: get : fgProcessorCount.0 -> () -> 0

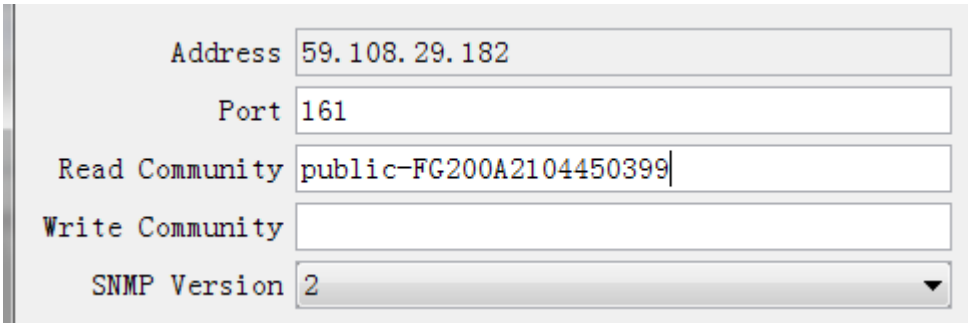
snmpd: </msg> 1

snmpd: updating cache: idx_cache

7.1.3. HA 模式带内管理

通过 SNMP 协议访问 FortiGate HA 时，访问主墙可以直接写 community；但访问各个成员时，SNMP 的 community 为:组名-序列号， 例如组名为 public，FGT200A_1 的序列号为 FGT FG200A2104450177 ，则访问 FGT200A_2 时，其通信组名为 public-FG200A2104450399.





7.1.4. HA 设备带外管理

默认情况下，HA 模式下的防火墙配置自动同步。可以按照上例进行统一管理，也可以对机群内设备进行独立管理。

1) 启用储备管理口

DMZ 接口被保留为管理接口。


```
config system ha
    set ha-mgmt-status enable
    set ha-mgmt-interface "dmz"
```

2) 为管理接口分别配置地址：

```
FGT60B3907513417 # show sys int dmz
config system interface
    edit "dmz"
        set ip 10.0.0.1 255.255.255.0
        set allowaccess ping https snmp
        set type physical
        set alias "manage"
    next
end

FGT60B3907513417 # exec ha manage 0
FGT60B3908651894 $ show sys int dmz
config system interface
    edit "dmz"
        set ip 10.0.0.2 255.255.255.0
        set allowaccess ping https snmp
```

```
            set type physical
        next
    end
```

3) 为管理口配置默认网关。

管理接口仅作为管理只用，需要配置独立的网关路由。

```
    Config system ha
      set ha-mgmt-interface-gateway 10.0.0.254
    end
```

4) 配置 SNMP

```
config system snmp    community
edit 1
                config hosts
                    edit 1
                        set ha-direct enable                    / /仅用于访问独立管理口。
                        set ip 10.0.0.100 255.255.255.255
                    next
                end
            set name "song"
        next
```

5) 对带外管理进行 ping 测试

exec enter vsys_hamgmt ， 再执行 exec ping 命令测试。

exec enter root 退出带外管理虚拟域，返回 root 域。

7.1.5. 常用 OID 值

系统监控 OID

监控参数明细	Object	对应 OID 值	参数类别（该参

			数的单位）
主机名称	sysName.0	.1.3.6.1.2.1.1.5.0	字符串
设备序列号	fnSysSerial.0	.1.3.6.1.4.1.12356.100.1.1.1.0	字符串
系统运行时间	sysUpTime.0	.1.3.6.1.2.1.1.3.0	数字，单位：timeTicks (0.01s)
系统版本	fgsSysVersion	.1.3.6.1.4.1.12356.101.4.1.1.0	字符串
系统 CPU 数量	fgProcModProcessorCount.1	.1.3.6.1.4.1.12356.101.4.5.3.1.5.1	正整数
每个 CPU 利用率(1 分钟)	fgProcessorUsage.x	.1.3.6.1.4.1.12356.101.4.4.2.1.2.*	1-100（%）
每个 CPU 利用率(5 分钟)	fgProcessorUsage5sec.x	.1.3.6.1.4.1.12356.101.4.4.2.1.3.*	1-100（%）
多个 CPU 的总利用率	fgSysCpuUsage.0	.1.3.6.1.4.1.12356.101.4.1.3.0	1-100（%）
内存利用率	fgSysMemUsage.0	.1.3.6.1.4.1.12356.101.4.1.4.0	1-100（%）
总内存大小	fgSysMemCapacity.0	.1.3.6.1.4.1.12356.101.4.1.5.0	单位（KB）
并发连接数	fgSysSesCount.0	.1.3.6.1.4.1.12356.101.4.1.8.0	数字
每秒新建连接数（1 秒平均）	fgSysSesRate1.0	.1.3.6.1.4.1.12356.101.4.1.11.0	数字
每秒新建连接数（10 秒平均）	fgSysSesRate10.0	.1.3.6.1.4.1.12356.101.4.1.12.0	数字
每秒新建连接数（30 秒平均）	fgSysSesRate30.0	.1.3.6.1.4.1.12356.101.4.1.13.0	数字
每秒新建连接数（60 秒平均	fgSysSesRate60.0	.1.3.6.1.4.1.12356.101.4.1.14.0	数字

网络接口 OID

监控参数明细	Object	对应 OID 值.*（*为接口 ID）	参数类别（该参数的单位）
IfEntry （基础表)			
系统接口数量	ifNumber.0	.1.3.6.1.2.1.2.1.0	正整数,个
接口 ID	ifIndex	.1.3.6.1.2.1.2.2.1.1.*	1.2.3….自然数
接口 MTU	ifMtu.x	.1.3.6.1.2.1.2.2.1.4.*	正整数
接口速率	ifSpeed.x	.1.3.6.1.2.1.2.2.1.5.*	正整数,单位:bit
接口管理状态	ifAdminStatus.x	.1.3.6.1.2.1.2.2.1.7.*	INTEGER {up(1), down(2),

接口工作状态	ifOperStatus.x	.1.3.6.1.2.1.2.2.1.8.*	INTEGER {up(1), down(2), testing(3), unknown(4), dormant(5), notPresent(6), lowerLayerDown(7) }
接口流量（in）	ifInOctets.x	.1.3.6.1.2.1.2.2.1.10.*	数字(32 位计数器)，字节
接口单播包转发数（in）	ifInUcastPkts.x	.1.3.6.1.2.1.2.2.1.11.*	数字(32 位计数器)，个
接口非单播包转发数（in）	ifInNUcastPkts.x	.1.3.6.1.2.1.2.2.1.12.*	数字(32 位计数器)，个
接口丢包（in）	ifInDiscards.x	.1.3.6.1.2.1.2.2.1.13.*	数字(32 位计数器)，个
接口错包（in）	ifInErrors.x	.1.3.6.1.2.1.2.2.1.14.*	数字(32 位计数器)，个
丢弃的未知协议包	ifInUnknownProtos.x	.1.3.6.1.2.1.2.2.1.15.*	数字(32 位计数器)，个
接口流量（out）	ifOutOctets.x	.1.3.6.1.2.1.2.2.1.16.*	数字(32 位计数器)，字节
接口单播包转发数（out）	ifOutUcastPkts.x	.1.3.6.1.2.1.2.2.1.17.*	数字(32 位计数器)，个
接口非单播包转发数（out）	ifOutNUcastPkts.x	.1.3.6.1.2.1.2.2.1.18.*	数字(32 位计数器)，个
接口丢包（out）	ifOutDiscards.x	.1.3.6.1.2.1.2.2.1.19.*	数字(32 位计数器)，个
接口错包（out）	ifOutErrors.x	.1.3.6.1.2.1.2.2.1.20.*	数字(32 位计数器)，个
IfXEntry (增强表，优先使用）			
接口名字	ifName.x	.1.3.6.1.2.1.31.1.1.1.1.*	字符串
接口多播包转发数（in）	ifInMulticastPkts.x	.1.3.6.1.2.1.31.1.1.1.2.*	数字(32 位计数器)，个
接口广播包转发数（in）	ifInBroadcastPkts.x	.1.3.6.1.2.1.31.1.1.1.3.*	数字(32 位计数器)，个
接口多播包转发数（out）	ifOutMulticastPkts.x	.1.3.6.1.2.1.31.1.1.1.4.*	数字(32 位计数器)，个
接口广播包转发数（out）	ifOutBroadcastPkts.x	.1.3.6.1.2.1.31.1.1.1.5.*	数字(32 位计数器)，个

接口流量（in）64 位	ifHCInOctets.x	.1.3.6.1.2.1.31.1.1.1.6.*	数字(64 位计数器)，字节
接口单播包转发数（in）64 位	ifHCInUcastPkts.x	.1.3.6.1.2.1.31.1.1.1.7.*	数字(64 位计数器)，个
接口多播包转发数（in）64 位	ifHCInMulticastPkts.x	.1.3.6.1.2.1.31.1.1.1.8.*	数字(64 位计数器)，个
接口广播包转发数（in）64 位	ifHCInBroadcastPkts.x	.1.3.6.1.2.1.31.1.1.1.9.*	数字(64 位计数器)，个
接口流量（out）64 位	ifHCOutOctets.x	.1.3.6.1.2.1.31.1.1.1.10.*	数字(64 位计数器)，字节
接口单播包转发数（out）64 位	ifHCOutUcastPkts.x	.1.3.6.1.2.1.31.1.1.1.11.*	数字(64 位计数器)，个
接口多播包转发数（out）64 位	ifHCOutMulticastPkts.x	.1.3.6.1.2.1.31.1.1.1.12.*	数字(64 位计数器)，个
接口广播包转发数（out）64 位	ifHCOutBroadcastPkts.x	.1.3.6.1.2.1.31.1.1.1.13.*	数字(64 位计数器)，个
接口 updown 状态变化是否发送 trap	ifLinkUpDownTrapEnable.x	.1.3.6.1.2.1.31.1.1.1.14.*	1：enable, 2:其他
接口速率	ifHighSpeed.x	.1.3.6.1.2.1.31.1.1.1.15.*	正整数,单位:Mbit
EtherLike-MIB			
接口信号错误	dot3StatsSymbolErrors	1.3.6.1.2.1.10.7.2.1.18.*	数字(32 位计数器)，次

监控策略流量匹配：

策略命中字节数	fgFwPolByteCoun.x	.1.3.6.1.4.1.12356.101.5.1.2.1.1.3.1.*	数字（32 位），字节

7.1.6. SNMP 命令参数

config system snmp sysinfo	
set contact-info ''	联系信息
set description ''	设备描述
set engine-id ''	SNMP 引擎标识，适用于 v3 版本
set location ''	位置
set status disable	是否开启 FortiGate SNMP agent.
set trap-high-cpu-threshold 80	cpu 使用率过高报警闸值
set trap-log-full-threshold 90	log 设备使用率过高报警闸值
set trap-low-memory-threshold 80	low-memory（内核占用）使用率过高报警闸值
end	

config system snmp community	
edit 1	
set events cpu-high mem-low log-full intf-ip vpn-tun-up vpn-tun-down ha-switch ha-hb-failure ips-signature ips-anomaly av-virus av-oversize av-pattern av-fragmented fm-if-change ha-member-up ha-member-down ent-conf-change av-conserve av-bypass av-oversize-passed av-oversize-blocked ips-pkg-update power-supply-failure faz-disconnect amc-bypass	配置支持的 TRAP,默认为开启全部的 TRAP
set name 'snmpread'	community 字符串名字
set query-v1-port 161	版本 1 的查询端口
set query-v1-status enable	允许版本 1 查询功能
set query-v2c-port 161	版本 2 的查询端口
set query-v2c-status enable	允许版本 2 查询功能
set status enable	状态为启用
set trap-v1-lport 162	版本 1 的本地服务端口，用于发送 trap
set trap-v1-rport 162	版本 1 的远程服务端口，用于发送 trap
set trap-v1-status enable	版本 1 TRap 功能开启
set trap-v2c-lport 162	版本 2 的本地服务端口，用于发送 trap
set trap-v2c-rport 162	版本 2 的远程服务端口，用于发送 trap
set trap-v2c-status enable	版本 2 TRap 功能开启
next	

7.2. 防火墙日志管理

7.2.1. 日志存贮设备

飞塔防火墙支持如下几种方式的日志存贮：

内存：系统分配一部分的内存空间用日志存储。

可以通过如下命令更改内存分配空间

```
config log memory global-setting
    set max-size 525007
end
```

硬盘：内置硬盘或者硬盘模块。

Fortianalyzer:飞塔独立日志存贮设备

Syslog：常用的日志存储软件。

Webtrends：支持。

7.2.2. 硬盘日志配置

针对如上几种日志存储设备的配置方法基本相同，以硬盘为例。

config log disk setting

set status disable /enable 关闭或开启该日志选项。

end

config log disk filter

set traffic disable //建议关闭流量日志。

end

7.2.3. syslog 日志配置

config log syslogd setting

set status enable

```
        set server "10.1.1.1"
    end
    config log syslogd filter
        set traffic disable                //建议关闭流量日志。
    end
```

飞塔防护墙支持 3 组的 syslog 服务器，和 3 组的 Fortianalyzer 设备。每组服务器的日志的过滤需要单独配置：

Syslog 配置	日志过滤
config log syslogd setting	config log syslogd filter
config log syslogd2 setting	config log syslogd2 filter
config log syslogd3 setting	config log syslogd3 filter

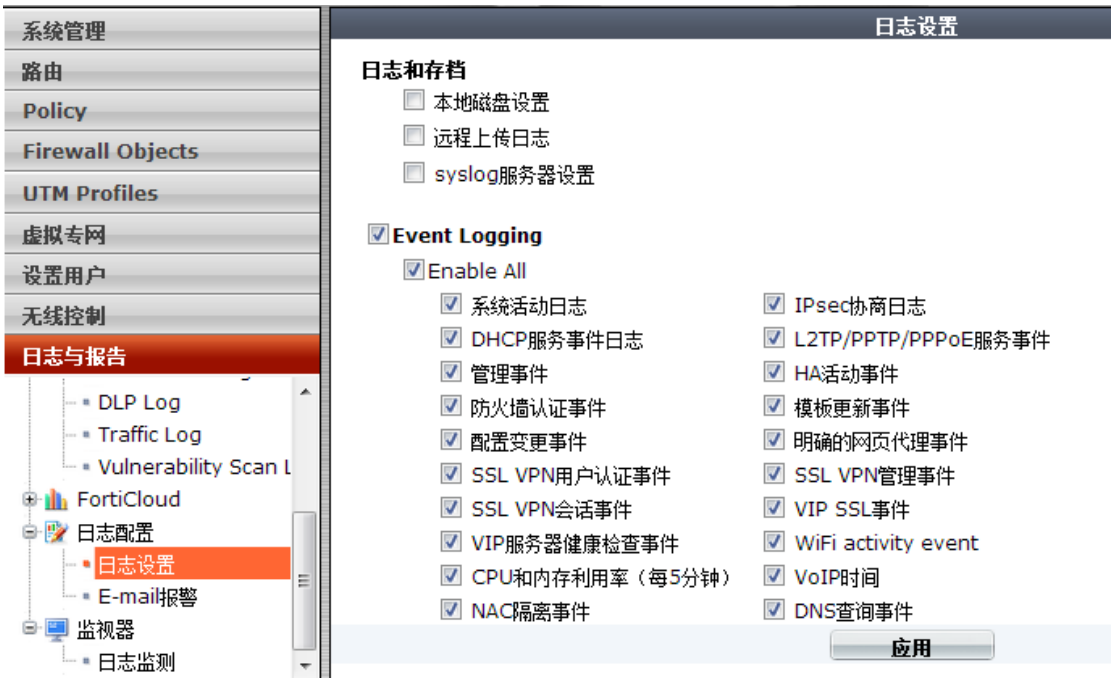
7.2.4. 日志过滤

1) 系统事件日志

所有系统相关的事件日志，可以根据事件类型对日志进行过滤。

配置系统事件日志方法如下：

Event logging:



Fortigate (eventfilter) # show full-configuration

config log eventfilter

set event enable

set admin enable

set auth enable

set config disable

set cpu-memory-usage disable

set dhcp enable

set dns disable

set ha enable

set ipsec enable

set ldb-monitor enable

set nac-quarantine enable

set pattern enable

set ppp enable

set sslvpn-log-adm enable

set sslvpn-log-auth enable

set sslvpn-log-session enable

set system enable

set vip-ssl enable

set voip enable

set wan-opt enable

set wireless-activity enable

end

7.2.5. 图形界面 GUI

访问飞塔 GUI 界面的时候，可以选择查看不同日志来源。

Fortigate # config log gui

Fortigate (gui) # set log-device ? //可选择设备如下：

memory log device memory

fortianalyzer log device FortiAnalyzer

forticloud log device FortiCloud

disk log device disk

7.2.6. CLI 查看日志

exec log list 1 查看日志文件，1 为日志类型。

exec log filter category 1 指定要查看的日志类型

exec log display 查看日志

7.2.7. 日志配置命令

config log memory setting	
set diskfull overwrite	内存日志空间用完时，覆盖现有日志
set ips-archive enable	对 IPS 进行存档
set status disable	关闭内容日志记录功能
end	

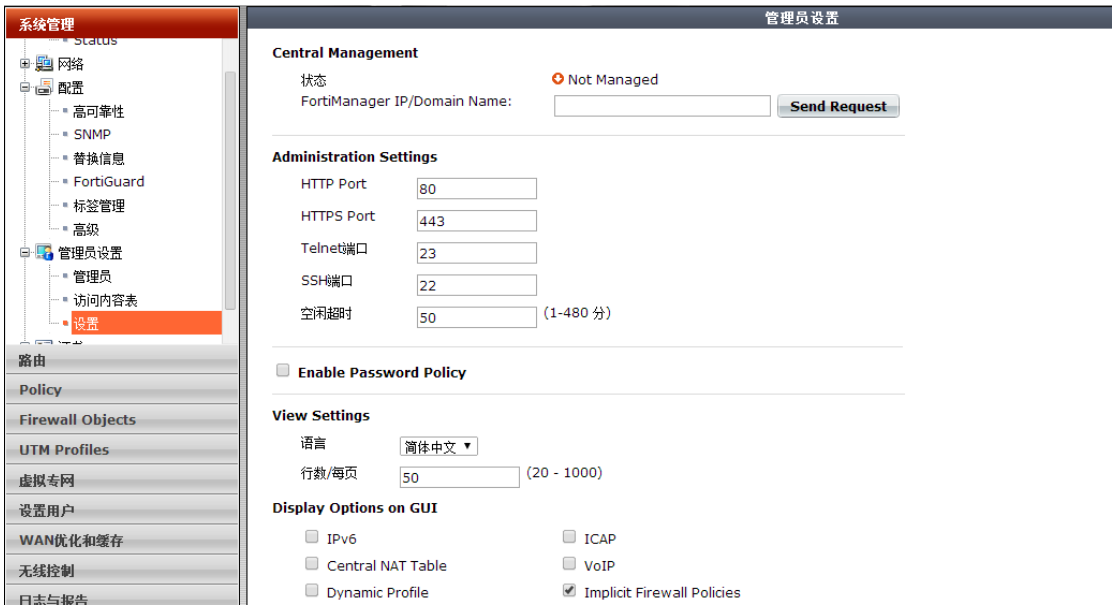
config log disk setting	
set status enable	开启硬盘记录功能
set ips-archive enable	对 IPS 进行存档
set log-quota 0	磁盘中 log 所占空间，单位 Mb
set dlp-archive-quota 0	DLP archive 所占磁盘空间
set report-quota 0	日志报告所占磁盘空间
set upload disable	是否允许将日志文件上传到 FTP 服务器
set upload-format compact	上传文件格式为压缩文件
set drive-standby-time 0	如果一段时间内无日志写入磁盘，磁盘进入休眠，0 为关闭此项功能
set full-first-warning-threshold 75	磁盘日志空间第一次告警 75%
set full-second-warning-threshold 90	磁盘日志空间第一次告警 90%
set full-final-warning-threshold 95	磁盘日志空间第一次告警 95%
set max-log-file-size 100	日志文件最大为 100M。参数可选范围 100-1000
set storage "	指定存储设别名字
set diskfull overwrite	磁盘记录空间使用完毕时，覆盖最早的日志
set sql-max-size 0	最大 SQL 数据库尺寸， 0-65536.0 则无限制
set sql-max-size-action overwrite	SQL 数据库达到最大时，覆盖最早的记录
set sql-oldest-entry 0	指定 SQL 数据库中日志中存在的最久时间，0 为无限制
set rows-per-transaction 1000	每产生 1000 条日志提交一次记录写入。
set ms-per-transaction 1000	每 1000 毫秒提交一次日志记录写入。
config sql-logging	配置 SQL 日志选项,开启后才可以生成日志报表。
set app-ctrl enable	应用控制
set attack enable	网络攻击
set dlp enable	数据防泄漏
set event enable	管理事件
set netscan enable	网络扫描
set spam enable	反垃圾邮件
set traffic enable	网络流量日志
set virus enable	反病毒
set webfilter enable	网页过滤
end	
end	
config log syslogd setting	
unset override	使用全局设置则关闭 override
set status enable	状态为开启
set server '1.1.1.1'	Syslog 服务器的地址
set reliable disable	是否使用可靠传输，如 enable 则使用 TCP
set port 514	Syslog 服务器的端口
set csv disable	产生的日志是否采用 CSV 格式
set facility local7	指定 facility 的类型

set source-ip 0.0.0.0	发送日志所使用的源 IP
end	
config log memory filter (syslog,fortianalyzer)	
set app-ctrl enable	应用控制日志(总开关)
set attack enable	攻击事件日志(总开关)
set dlp enable	防数据泄露日志(总开关)
set dlp-archive enable	防数据泄露子类－数据存档
set email enable	邮件日志(总开关)
set explicit-proxy-traffic enable	显示代理流量日志
set failed-connection enable	流量日志子类－失败的连接尝试
set netscan enable	网络扫描日志(总开关)
unset override	是否启用全局设置
set severity information	事件的等级
set traffic enable	流量日志(总开关)
set virus enable	病毒日志(总开关)
set wanopt-traffic enable	广域网优化日志(总开关)
set web enable	WEB 过滤日志(总开关)
set webcache-traffic enable	广域网优化子类－WEB 缓存
set allowed enable	流量日志子类－被策略允许的流量
set anomaly enable	Attack 子类－异常攻击
set app-ctrl-all enable	应用控制子类－允许或关闭子类日志
set blocked enable	病毒子类－被阻止的文件
set discovery enable	netscan 子类－发现事件
set dlp-all enable	防数据泄露子类
set email-log-google enable	邮件日志子类－google 邮件
set email-log-imap enable	邮件日志子类－IMAP 协议反垃圾邮件
set email-log-msn enable	邮件日志子类－MSN 邮件
set email-log-pop3 enable	邮件日志子类－POP3 协议反垃圾邮件
set email-log-smtp enable	邮件日志子类－SMTP 协议反垃圾邮件
set email-log-yahoo enable	邮件日志子类－yahoo 邮件
set extended-traffic-log enable	流量日志子类－其他流量
set ftgd-wf-block enable	WEB 过滤子类－Foritguard 中 WEB 过滤功能阻止
set ftgd-wf-errors enable	WEB 过滤子类－Foritguard 中 WEB 分类错误
set infected enable	病毒子类－病毒感染日志
set oversized enable	病毒子类－超大文件日志
set scanerror enable	病毒子类－反病毒错误日志
set signature enable	Attack 子类－基于特征库
set url-filter enable	WEB 过滤子类－url 过滤事件
set violation enable	流量日志子类－违反策略流量日志
set vulnerability enable	netscan 子类－漏洞扫描日志

set web-content enable	WEB 过滤子类－内容过滤事件
set web-filter-activex enable	WEB 过滤子类－Activex 过滤事件
set web-filter-applet enable	WEB 过滤子类－Applet 过滤事件
set web-filter-cookie enable	WEB 过滤子类－cookie 过滤事件
set web-filter-ftgd-quota enable	WEB 过滤子类－Fortiguard 配额等级
set web-filter-ftgd-quota-counting enable	WEB 过滤子类－Fortiguard 配额计数
set web-filter-ftgd-quota-expired enable	WEB 过滤子类－Fortiguard 配额超时
set web-filter-script-other enable	WEB 过滤子类－脚本等其他过滤事件
end	
config log eventfilter	
set event enable	事件信息
set admin enable	管理事件
set auth enable	认证事件
set config disable	配置修改事件
set cpu-memory-usage disable	cpu 内存使用率
set dhcp enable	DHCP 事件
set dns disable	DNS 事件
set ha enable	HA 事件
set ipsec enable	IPSEC 事件
set ldb-monitor enable	负载均衡事件
set nac-quarantine enable	NAC 隔离事件
set pattern enable	模板更新事件
set ppp enable	PPP 事件
set sslvpn-log-adm enable	SSL 管理事件
set sslvpn-log-auth enable	SSL 认证事件
set sslvpn-log-session enable	SSL 会话事件
set system enable	系统活动事件
set vip-ssl enable	VIP SSL 事件
set voip enable	Voip 事件
set wan-opt enable	广域网优化事件
set wireless-activity enable	无线事件
end	

7.3. 防火墙用户管理

7.3.1. 管理员设置



config system global

set admin-lockout-threshold 3 //admin 账户连续登陆三次失败后，锁定其 ip，使其无法进行更多的尝试

set admin-lockout-duration 60 // 锁定时间为 60 秒

set admin-port 80 // http 管理页面端口为 80

set admin-sport 443 // https 管理页面端口为 80

set admin-ssh-port 22 // ssh 管理页面端口为 80

set admin-telnet-port 23 // telnet 管理页面端口为 80

set admintimeout 5 // 管理员超时时间为 5 分钟

set language simch //简体中文管理页面

7.3.2. 管理员密码策略

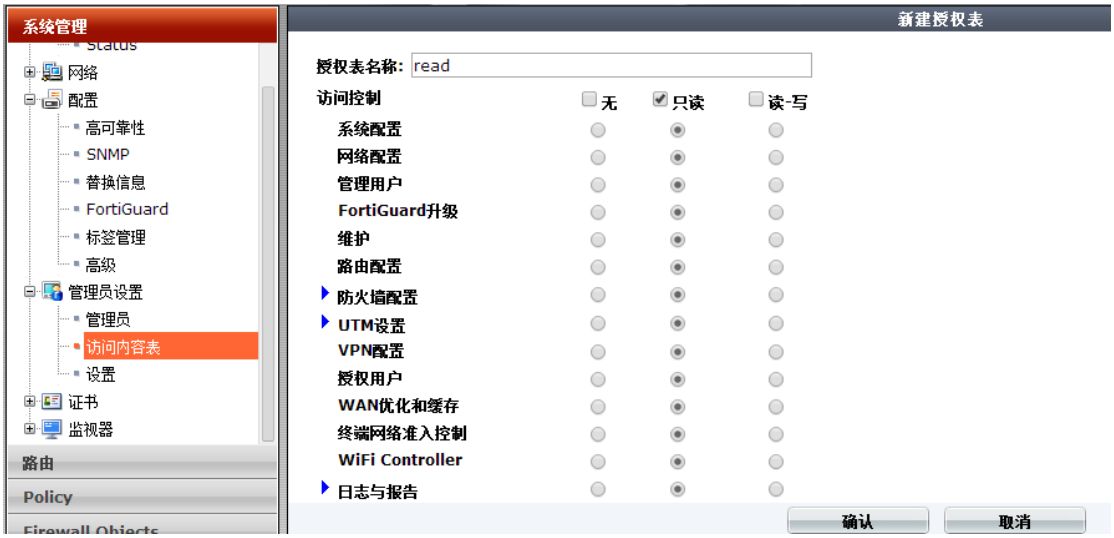
config system password-policy

set status enable //开启密码策略功能/默认关闭

set apply-to admin-password //策略应用范围是设备管理员账号，以及 ipsec 预共享密钥，可以多选。
set minimum-length 8 //密码的最小长度
set min-lower-case-letter 0 //小写字母的最小个数
set min-upper-case-letter 0 //大写字母的最小个数
set min-non-alphanumeric 0 //特殊字符的最小个数
set min-number 0 //数字的最小个数
set change-4-characters disable //每次更换密码时，新密码必须与现有密码有 4 个字符以上的差别。
set expire-status disable //开启或关闭默认密码过期选项
set expire-day 90 //密码过期时间
end

7.3.3. 管理员授权表

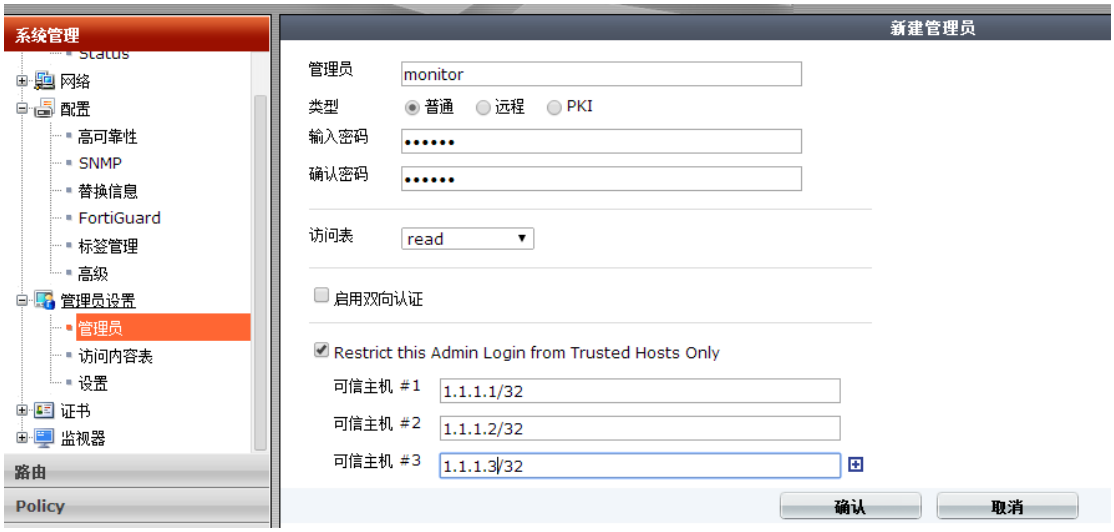
（1）建立授权表




```
config system accprofilet
    edit "read"
        set admingrp read
        set authgrp read
        set endpoint-control-grp read
        set fwgrp read
        set loggrp read
        unset menu-file
        set mntgrp read                    // 维护权限
        set netgrp read
        set routegrp read
        set sysgrp read
        set updategrp read
```

```
            set utmgrp custom
            set vpngrp read
            set wanoptgrp read
            set wifi read
                config utmgrp-permission
                    set antivirus read
                    set application-control read
                    set data-loss-prevention read
                    set ips read
                    set spamfilter read
                    set webfilter read
                end
        next
end
```

（2）为管理员分配访问权限




```
config system admin
    edit "monitor"
        set trusthost1 1.1.1.1 255.255.255.255          //信任主机
        set trusthost2 1.1.1.2 255.255.255.255
        set trusthost3 1.1.1.3 255.255.255.255
        set accprofile "read"                           // 只读权限的授权表
        set vdom "root"
        set password ENC AK1k2iA1kwvG7EOiHGA/3lYzbMwoxm0s4Uqr2ZnR2mGdyc=
    next
end
```

（3）如何建立维护账户

其他选线选择‘只读’ ，维护权限选择‘读-写’，用户可以执行 diagnose 等调试命令，便于对系统进行维护。


```
config system accprofilet
    edit "weihu"
        set admingrp read                    //其他选项均配置为 read
         ........
        set mntgrp read-write                //开启维护权限
    end
```

将该管理员授权表分配给相应的用户即可。

7.3.4. Radius 认证

（1） 配置 Radius 服务器


```
config user radius
    edit "radius"
```

```
        set secret ENC    ******
        set server "1.1.1.1"                    //主 radius 服务器
        set secondary-secret ENC ******
        set secondary-server "1.1.1.2"          //备份 radius 服务器
    next
end
```

（2） 配置用户组


```
config user group
    edit "remoteadimin"                     //组名字
        set member "radius"                 //radius 服务器名字
    next
end
```

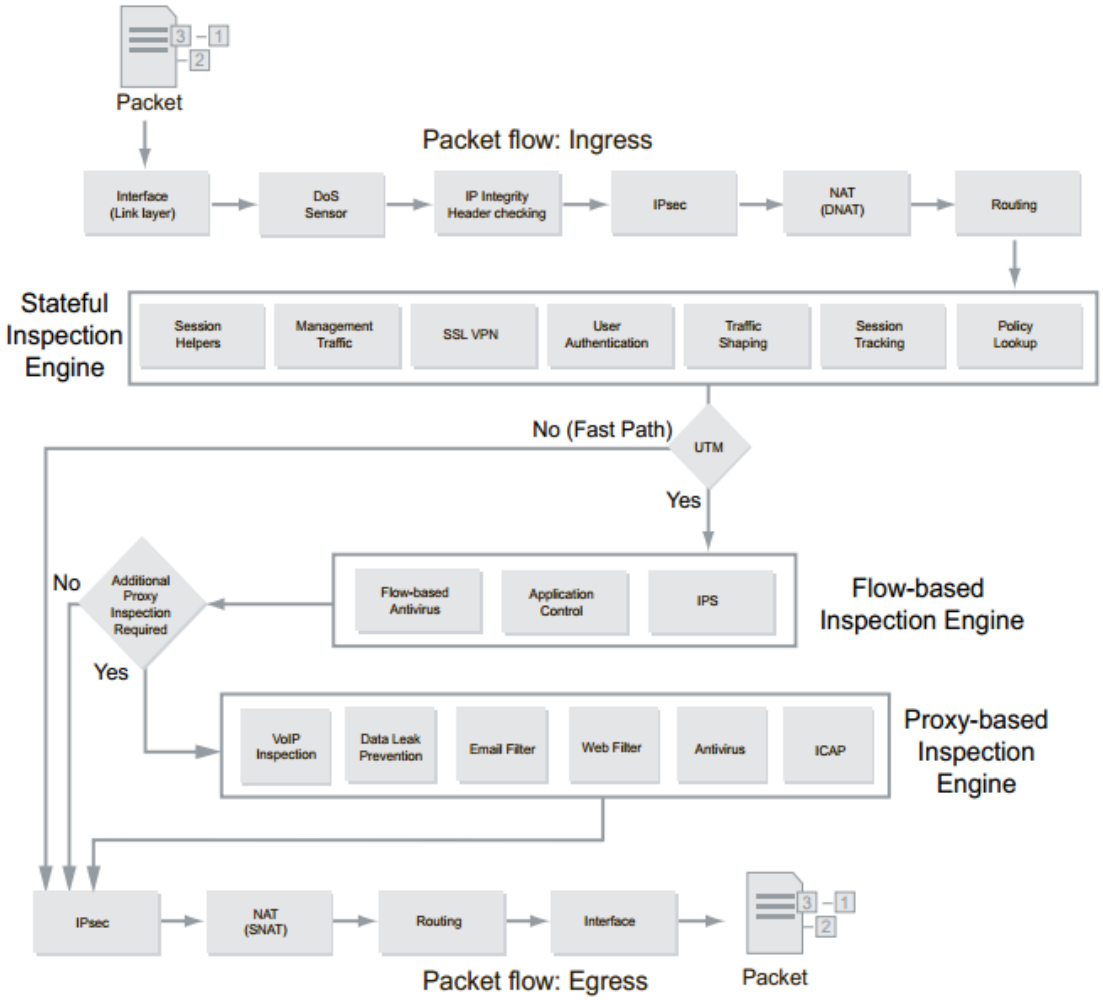
（3） 配置管理员


```
config system admin
    edit "remote"
        set remote-auth enable
        set accprofile "prof_admin"
        set vdom "root"
        set wildcard enable
        set remote-group "remoteadimin"                    //定义好的用户组名字
    next
end
```

第8章. 飞塔防火墙故障诊断

8.1. 数据包处理流程

当 FortiGate 的入接口收到数据包后，需要对其进行一系列的处理，然后由出接口发出。如下图所示：



包处理过程的各步骤如下：

1) Interface（网卡接口）

网卡接口驱动负责接数收据包，并转交给下一过程。

2) DoS Sensor（DoS 防御，默认关闭）

负责过滤 SYN flood、UDP flood、ICMP flood 等 DoS 攻击，并可针对源、目的 IP 的并发连接数进行限制。

3) IP integrity header checking（IP 头完整性校验）

检查数据包头完整性。

4) IPSec（IPSec VPN 解密，默认关闭）

如果是 FortiGate 本身的 IPSec VPN 隧道中的数据包，将对其进行解密。

5) DNAT（目标地址 NAT）

检查数据包中的目标 IP 地址，如果在 FortiGate VIP（目标地址 NAT）表中，则将其替换为映射后 IP 地址（真实 IP 地址）和端口。

6) Routing（路由）

本步骤根据数据包的目标 IP 地址确定该数据包的流出接口。

7) Stateful Inspection Engine（状态检测引擎）

状态检测引擎包含几个组件：

a) Policy lookup（策略查找）

在会话建立阶段，判断是否允许数据通过并建立会话状态，并根据 UTM 功能的开关决定数据包是否需要进入流检测引擎（Flow-based inspection engine）和代理检测引擎（Proxy-based inspection engine）。

b) Session track（会话跟踪）

维护会话表，跟踪会话状态、NAT 和其它相关功能。会话建立之后的后续数据包不再进行策略匹配，直接根据会话状态转发。

c) User authentication（用户认证，默认关闭）

对用户身份进行认证，根据用户名和用户所在组选择防火墙策略。

d) Management traffic（管理流量）

与 FortiGate 自身相关的流量处理，如 Web、SSH 管理，Syslog、SNMP 通信等。

e) SSL VPN 流量（默认关闭）

将 SSL VPN 流量解密，送至 SSL VPN 虚拟接口（通常为 ssl.root），然后查找策略。

f) Session helpers（即 ALG）

对 FTP、SIP、Oracle 等特殊应用进行处理，如动态开启策略、NAT，自动修改 payload 等，保证其正常通信。

8) Flow-based inspection engine（流检测引擎，默认关闭）

如果在防火墙策略中启用了防病毒、IPS、应用控制等流检测 UTM 功能，则会话后续数据包交由流检测引擎处理。

9) Proxy-based inspection engine（代理检测引擎，默认关闭）

如果在防火墙策略中启用了 Web 过滤、防病毒、反垃圾邮件、DLP 等应用代理检测 UTM 功能，则会话后续数据包交由代理检测引擎处理。

10)IPSec（IPSec VPN 加密，默认关闭）

如果会话匹配了 IPSec VPN 策略，此步骤将数据包加密封装

11)Source NAT（源地址 NAT）

如果策略中启用了 NAT，则将数据包的源 IP 地址和源端口替换为目标接口地址或 IP 池中的 IP 地址（通常为公网 IP 地址）。

12)Routing（路由）

最后一个路由步骤，确定数据包的流出接口，由路由引擎转发数据包。

13)Egress（流出）

由流出接口网卡将数据包发出 FortiGate。

8.2. 数据流分析工具

diagnose debug enable	开启 debug 功能
diagnose debug flow show console enable	开始 flow 的输出
diagnose debug flow filter add 119.253.62.131	定制过滤器，支持多种过滤
diagnose debug flow trace start 6	定义索要跟踪数据包的数量

例 1 ：策略允许访问 **//注释部分**

Fortigate # id=36871 trace_id=1 msg="vd-root received a packet(proto=6, 192.168. 1.110:51661->119.253.62.131:80) from internal."id=36871 trace_id=1 msg="allocate a new

session-00016920" **//internal 口收到数据，建立新会话**

id=36871 trace_id=1 msg="find a route: gw-192.168.118.1 via wan1" **//查找到路由表**

id=36871 trace_id=1 msg="find SNAT: IP-192.168.118.28, port-43333" **//检测存在 NAT 配置**

id=36871 trace_id=1 msg="Allowed by Policy-1: SNAT" **//匹配策略,ID1**

id=36871 trace_id=1 msg="SNAT 192.168.1.110->192.168.118.28:43333" **//做 NAT**

id=36871 trace_id=3 msg="vd-root received a packet(proto=6, 119.253.62.131:80->1

92.168.118.28:43333) from wan1." **// Wan1 口收到返回数据包**

id=36871 trace_id=3 msg="Find an existing session, id-00016920, reply direction"

//数据包匹配会话 id-0001692

id=36871 trace_id=3 msg="DNAT 192.168.118.28:43333->192.168.1.110:51661"

//做反向的 DNAT

id=36871 trace_id=3 msg="find a route: gw-192.168.1.110 via internal"

//查找路由，发送到 internal 口

id=36871 trace_id=5 msg="vd-root received a packet(proto=6, 192.168.1.110:51661-

>119.253.62.131:80) from internal." **//internal 口收到后续数据包**

id=36871 trace_id=5 msg="Find an existing session, id-00016920, original direction"

//匹配会话 id-0001692

id=36871 trace_id=5 msg="enter fast path" **//直接转发**

id=36871 trace_id=5 msg="SNAT 192.168.1.110->192.168.118.28:43333" **//NAT**

例 2：策略不允许访问

Fortigate # id=36871 trace_id=23 msg="vd-root received a packet(proto=6, 192.168

.1.110:51768->119.253.62.131:80) from internal."

id=36871 trace_id=23 msg="allocate a new session-00017537"

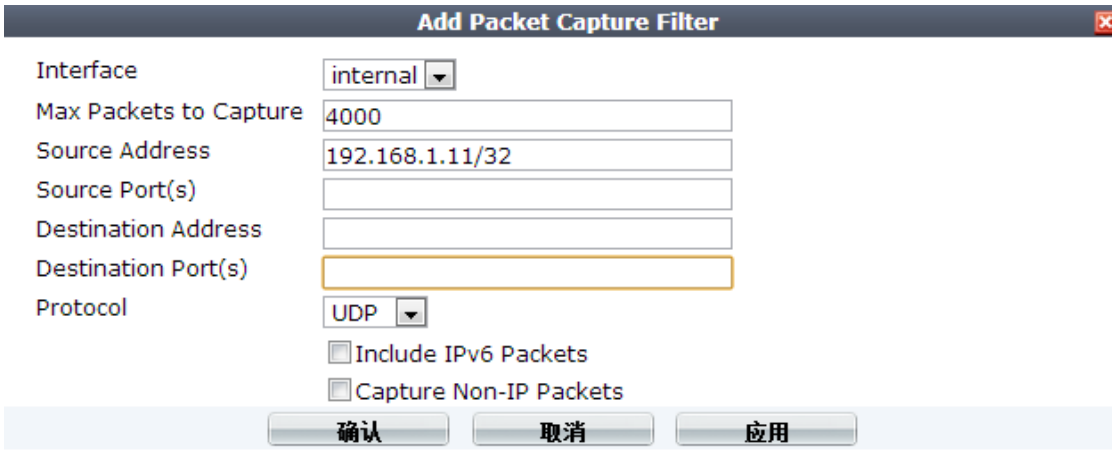
id=36871 trace_id=23 msg="find a route: gw-192.168.118.1 via wan1"

id=36871 trace_id=23 msg="Denied by forward policy check" **//直接被策略拒绝**

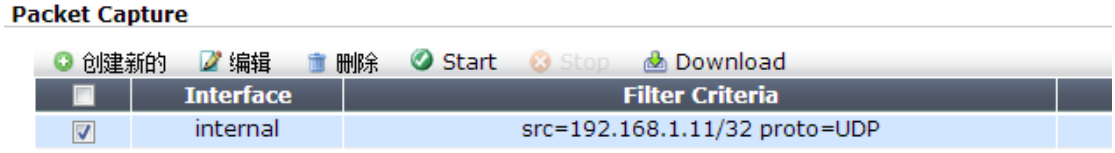
8.3. 图形界面抓包

FortiOS4.3 的图形界面下有抓取网络数据包的图形化接口。

如上图 packet capture 部分，点击‘创建新的‘即可创建一个抓包过滤器，并进行抓包。



按图填入需要抓取的过滤条件，点击确认。



点击 start 开始抓包；点击 download 将抓取的数据包保存的本地磁盘，可以用 wireshark 直接查看。

该方式的优点是方便，抓取的内容可以直接查看，不需要进行而外的转换工作，缺点是过滤选项不够丰富。

8.4. 抓包命令详解

diagnose sniffer packet <interface> <'filter'> <verbose> <count>

8.4.1. interface

<interface> 指定实际的接口名称，可以是真实的物理接口名称，也可以是 VLAN 的逻辑接口名称，当使用“any”关键字时，表示抓全部接口的数据包。 例：

＃diagnose sniffer packet port1 //表示抓物理接口为 port1 的所有数据包

＃diagnose sniffer packet any //表示抓所有接口的所有数据包

＃diagnose sniffer packet port1-v10 //当在物理接口建立一个 VLAN 子接口，其逻辑 接口名为 port1-v10，此时表示抓 port1-v10 接口的所有数据包，此处一定注意一个问题， 由于抓包命令中的空格使用来区分参数字段的，但是在逻辑接口创建时，接口名称支持空格，考虑到今后抓包分析的方便，建议在创建逻辑接口时不要带有空格。

8.4.2. verbose

<verbose> 指控制抓取数据包的内容。常用选项 4 和 6。

1: print header of packets, //只抓取 IP 的原地址、源端口、目的地址、目的端口和数据包的 Sequence numbers， 为系统缺省设置

2: print header and data from ip of packets, //抓取包括 IP、TCP 或 UDP 及其内容层的 payload。

3: print header and data from ethernet of packets) ，//抓取包括 Ether、IP、TCP 或 UDP 及其内容层的 payload。 可导出到文本文件使用专用的转换工具，转换为 Ethereal 支持文件

4:print header of packets with interface name //与第一项类似，但包括显示收发包的接口信息

5: print header and data from ip of packets with interface name //与第二项类似，但包括显示收发包的接口信息

6: print header and data from ethernet of packets (if available) with intf name //与第三项类似，但包括显示收发包的接口信息

8.4.3. count

<count> 抓取的数据包的数量。

8.4.4. filter

过滤器可以用一个表达式来表示，也可以是多个表达式进行组合;

当表达式为连续字符串，中间没有空格字符时，不需要加单引号或者双引号。

如 diagnose sniffer packet wan1 icmp 1 10；

当过滤器表达式中间存在空格，或者是由多个过滤条表达式组合的时候，则需要将整个表达式放入单引号或者双引号之内。

如：

diagnose sniffer packet any 'host 192.168.1.11' 4 2

diagnose sniffer packet wan1 'icmp and host 8.8.8.8' 1 10;

8.4.4.1.None

None 或者不写任何参数，则不做任何过滤。

Fortigate # diagnose sniffer packet wan1 none 1 3

interfaces=[wan1]

filters=[none]

0.726021 arp who-has 192.168.118.64 tell 192.168.118.1

0.726054 arp who-has 192.168.118.207 tell 192.168.118.1

0.907046 192.168.118.55.3975 -> 255.255.255.255.2654: udp 312

8.4.4.2.Tcp,udp,icmp,arp 参数

Fortigate # diagnose sniffer packet wan1 tcp 1 3

interfaces=[wan1]

filters=[tcp]

5.854756 192.168.118.28.41972 -> 74.125.31.138.443: 1918013413 ack 2189770725

10.680845 192.168.118.28.37644 -> 106.120.151.51.80: syn 1554494232

10.681300 106.120.151.51.80 -> 192.168.118.28.37644: syn 199984742 ack 1554494

3

Fortigate # diagnose sniffer packet wan1 udp 1 3

interfaces=[wan1]
filters=[udp]
0.851497 192.168.118.39.58839 -> 234.34.23.234.33674: udp 20
0.880828 192.168.118.28.38299 -> 8.8.8.8.53: udp 37
0.951063 192.168.118.55.4045 -> 255.255.255.255.2654: udp 312

Fortigate # diagnose sniffer packet wan1 icmp 1 3
interfaces=[wan1]
filters=[icmp]
5.831862 192.168.118.28 -> 119.254.12.21: icmp: echo request
5.833274 119.254.12.21 -> 192.168.118.28: icmp: echo reply
6.836748 192.168.118.28 -> 119.254.12.21: icmp: echo request

Fortigate # diagnose sniffer packet wan1 arp 1 3
interfaces=[wan1]
filters=[arp]
0.835697 arp who-has 192.168.118.211 tell 192.168.118.1
0.955753 arp who-has 192.168.118.64 tell 192.168.118.1
0.955780 arp who-has 192.168.118.207 tell 192.168.118.1

8.4.4.3.Src,dst 参数

指定源 IP　或者目的 IP。
FortiGate # diag sniffer pa any '**src 192.168.118.45 and dst 4.2.2.1**' 4
interfaces=[any]
filters=[src 192.168.118.45 and dst 4.2.2.1]
3.053283 SE in 192.168.118.45 -> 4.2.2.1: icmp: echo request
4.055621 SE in 192.168.118.45 -> 4.2.2.1: icmp: echo request
5.057185 SE in 192.168.118.45 -> 4.2.2.1: icmp: echo request
6.059751 SE in 192.168.118.45 -> 4.2.2.1: icmp: echo request

8.4.4.4.host 参数

指定主机，抓取包括该 host IP 地址的数据包，可以是源地址，也可以是目标地址。
Fortigate # diagnose sniffer　packet　wan1 '**host 8.8.8.8**' 1 10
interfaces=[wan1]
filters=[host 8.8.8.8]
5.793921 192.168.118.28 -> 8.8.8.8: icmp: echo request　　//目标地址
5.833691 8.8.8.8 -> 192.168.118.28: icmp: echo reply　　//源地址

8.4.4.5.port 参数

根据数据包源端口或者目标端口进行抓包。
Fortigate # diagnose sniffer packet wan1 '**port 80**' 1 3
interfaces=[wan1]
filters=[port 80]
5.391804 192.168.118.28.8977 -> 83.145.92.172.80: syn 3438827760
5.392339 83.145.92.172.80 -> 192.168.118.28.8977: syn 4238988927 ack 3438827761
5.392842 192.168.118.28.8977 -> 83.145.92.172.80: ack 4238988928

8.4.4.6.proto 参数

可以通过协议号进行抓包，1:ICMP, 6:TCP , 17:UDP, 89: OSPF 等。
Fortigate # diagnose sniffer packet wan1 '**proto 1**' 1 10
interfaces=[wan1]
filters=[proto 1]
5.193085 192.168.118.28 -> 8.8.8.8: icmp: echo request
5.233840 8.8.8.8 -> 192.168.118.28: icmp: echo reply
6.193968 192.168.118.28 -> 8.8.8.8: icmp: echo request
6.234911 8.8.8.8 -> 192.168.118.28: icmp: echo reply

Fortigate # diagnose sniffer packet wan1 '**proto 17**' 1 10
interfaces=[wan1]
filters=[proto 17]
1.291398 192.168.118.48.1786 -> 255.255.255.255.2654: udp 312
1.307764 192.168.118.48.1787 -> 255.255.255.255.2654: udp 322
2.813556 192.168.118.55.3735 -> 255.255.255.255.2654: udp 312
2.815426 192.168.118.55.3736 -> 255.255.255.255.2654: udp 324

8.4.4.7.and 和 or 参数

表达式连接符号 and 为“与”的关系，or 为“或”的关系。通过这个 2 参数可以将多个过滤表达式组合成一个更精确的抓包过滤器。
Fortigate # diagnose sniffer packet wan1 '**host 8.8.8.8 and udp and port 5**3’ 1 10
interfaces=[wan1]
filters=[host 8.8.8.8 and udp and port 53]
9.161057 192.168.118.28.25758 -> 8.8.8.8.53: udp 30
9.200929 8.8.8.8.53 -> 192.168.118.28.25758: udp 273

Fortigate # diagnose sniffer packet wan1 '**host 8.8.8.8 or udp**' 1 6

interfaces=[wan1]
filters=[host 8.8.8.8 or udp]
0.406682 192.168.118.28 -> 8.8.8.8: icmp: echo request
0.446384 8.8.8.8 -> 192.168.118.28: icmp: echo reply
1.408758 192.168.118.28 -> 8.8.8.8: icmp: echo request
1.447828 192.168.118.48.2345 -> 255.255.255.255.2654: udp 312
1.448329 8.8.8.8 -> 192.168.118.28: icmp: echo reply
1.467194 192.168.118.48.2346 -> 255.255.255.255.2654: udp 324

8.4.4.8. TCP 包头字段过滤

TCP 包头部

FortiGate # diag sniff packet any 'tcp[13]==2' 4 10
interfaces=[any]
filters=[tcp[13]==2]
0.566163 SE in 192.168.118.44.51011 -> 118.67.120.53.80: syn 1443461665
0.566253 port13 out 59.108.29.180.65483 -> 118.67.120.53.80: syn 1443461665
0.566476 SE in 192.168.118.44.51012 -> 118.67.120.37.80: syn 2381613524
0.566569 port13 out 59.108.29.180.65484 -> 118.67.120.37.80: syn 2381613524

TCP 包头的 13 字节内容＝＝2, 即 00**000010**。包头的第一个字节序号为 0,依次次往后数，13 就是 Flag 位置所在的字节，该字节的倒数第二位为 SYN 未，所以该命令的就是抓取所有 syn 包为 1，其他 flag 位为 0 的数据包。

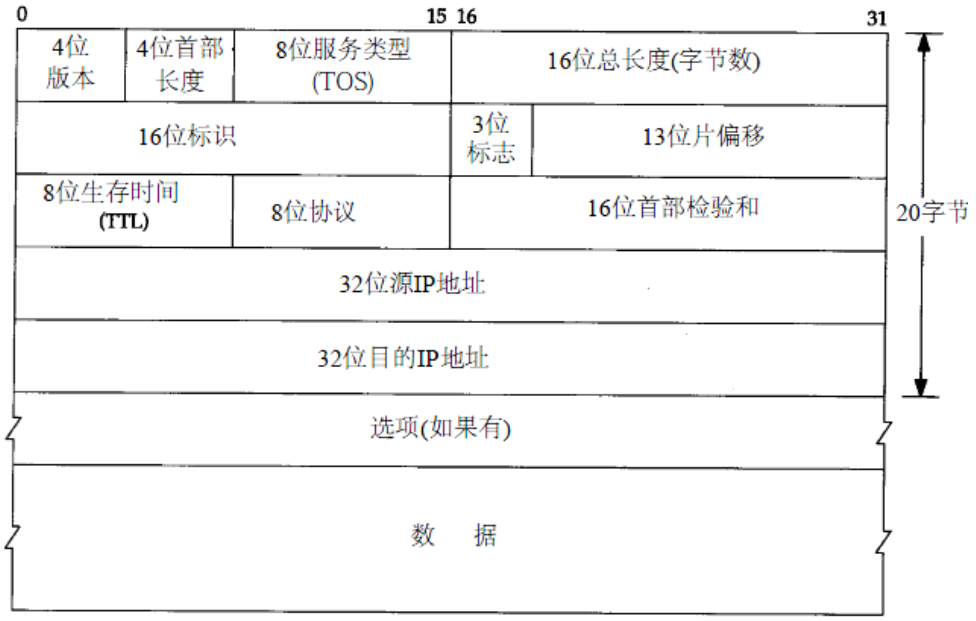
同理：diagnose sniffer packet any "tcp[13] & 4 != 0" 3 10 抓 FIN 为 1 的包。

因为 FIN 位为 1 的数据包，ACK 也置位 1,通过 tcp[13] & 4 != 0，即通过做与运算不

等于 0.也就是说只要 FIN 为 1,其他位任意。

diagnose sniffer packet any "tcp[13] & 2 != 0" 4 10　SYN 位为 1 的，其他位置可以为任意值的数据包，(SYN,SYN ACK 包)。

8.4.4.9. IP 包头字段过滤



16 进制 0x59 为十进制的 89，IP 头第 9 字节为协议字节，协议号 89 则为 OSPF.

```
Fortigate # diagnose sniffer packet any "ip[9]==0x59" 1 10
interfaces=[any]
filters=[ip[9]==0x59]
0.601194 192.168.118.28 -> 224.0.0.5:    ip-proto-89 44
11.601206 192.168.118.28 -> 224.0.0.5:    ip-proto-89 44

2 packets received by filter
0 packets dropped by kernel

Fortigate # diagnose sniffer packet any "ip[9]==89" 1 10
interfaces=[any]
filters=[ip[9]==89]
2.601194 192.168.118.28 -> 224.0.0.5:    ip-proto-89 44
12.601208 192.168.118.28 -> 224.0.0.5:    ip-proto-89 44
```

8.4.4.10. ethernet 包头字段过滤

以太网包头的第 6 字节开始的 4 个连续字节为源 MAC 地址字段位置。下面的命令为抓取所有源 MAC 地址为 0x00090fdf 的数据包。

```
FortiGate # diagnose sniffer packet SE "(ether[6:4]=0x00090fdf) and (ether[10:2]=0xe8e3)" 3 3
interfaces=[SE]
filters=[(ether[6:4]=0x00090fdf) and (ether[10:2]=0xe8e3)]
0.632650 192.168.118.45.62528 -> 192.168.118.1.22: ack 2277714159
0x0000    0009 0fcd 9f48 0009 0fdf e8e3 0800 4500          .....H........E.
0x0010    0028 2383 4000 7f06 6acd c0a8 762d c0a8          .(#.@...j...v-..
0x0020    7601 f440 0016 16b9 4e62 87c3 28ef 5010          v..@....Nb..(.P.
0x0030    3fa0 f88f 0000                                   ?.....

0.633263 192.168.118.45.62528 -> 192.168.118.1.22: ack 2277714383
0x0000    0009 0fcd 9f48 0009 0fdf e8e3 0800 4500          .....H........E.
0x0010    0028 2384 4000 7f06 6acc c0a8 762d c0a8          .(#.@...j...v-..
0x0020    7601 f440 0016 16b9 4e62 87c3 29cf 5010          v..@....Nb..).P.
0x0030    3ec0 f88f 0000                                   >.....
```

抓取目标 MAC = 00:09:0f:cd:9f:48 数据包

```
FortiGate # diagnose sniffer packet SE "(ether[0:4]=0x00090fcd) and (ether[4:2]=0x9f48)" 3 3
interfaces=[SE]
filters=[(ether[6:4]=0x00090fdf) and (ether[10:2]=0xe8e3)]
0.632650 192.168.118.45.62528 -> 192.168.118.1.22: ack 2277714159
0x0000    0009 0fcd 9f48 0009 0fdf e8e3 0800 4500          .....H........E.
0x0010    0028 2383 4000 7f06 6acd c0a8 762d c0a8          .(#.@...j...v-..
0x0020    7601 f440 0016 16b9 4e62 87c3 28ef 5010          v..@....Nb..(.P.
0x0030    3fa0 f88f 0000                                   ?.....
```

8.4.5. 数据格式转换

首先，通过该命令抓取数据包，会直接输出到屏幕上，需要通过 SecureCRT 相关工具进行抓包数据的收集。

其次，使用抓包命令的<verbose>级别为 6 时，导出的文件才能被 Wireshark 识别。

第三，要获取大量抓包信息时，SecureCRT 工具应通过远程 TELNET/SSH 连接到 FortiGate。如果使用主机串口来抓包，由于串口速率低，获取大量数据时速度非常慢。

第四，使用单独提供的脚本程序文件进行转换，主机必须提前安装 Perl 的解释程序和 Wireshark 软件，并在提供的转换脚本程序中做必要的路径指向。

8.4.5.1.SecureCRT 的配置

正常安装 SecureCRT 软件，并通过远程方式登陆到 FortiGate 网关。

1、配置 SecureCRT：File > Log Session，选择配置文件存储的路径，文件格式为*.txt

2、FortiGate 上执行抓包命令

FortiGate # diagnose sniffer packet <interface><'filter'>6<count>

其中 6 代表抓到的包输出文件支持经过转换为 Wireshark 格式文件。

8.4.5.2.下载并编辑的脚本程序文件

转换脚本程序 fgt2eth.pl 下载：

在 kb.fortinet.com 中可以搜索到 fgt2eth.pl 脚本程序。

下载的脚本文件需要使用 Wireshark 的 text2pacp.exe 程序，所以需要在脚本中指明 text2pcap.exe 的路径。text2pcap.exe 所在路径是 Wireshark 的安装路径。比如脚本第 16 行
my $text2pcapdirwin = "c:\\PROGRA~2\\Wireshark\\";

8.4.5.3.转换操作

确认正常安装 Perl 解释器，下载链接 http://www.activestate.com/activeperl/downloads 在 DOS 命令行执行将 fgt2eth.pl 和抓包文件 packet.txt 拷贝到工作目录 c:\Packets

C:\Packets>perl fgt2eth.pl -in packet.txt –out test.pacp

输出文件 test.pcap 就是抓到的包转换为 Wireshark 识别的格式文件。用 Wireshark 打开后即可进行详细分析。直接输入 perl fgt2eth.pl –help 获得帮助信息

附录：常用命令

get sys status	查看系统状态
get hardware status	查看硬件配置
get system performance status	查看性能
get sys arp	查看 arp 表
exec clear system arp table	清除 arp 表
diag debug report	生成 debug report
show sys interface show full-configuration system interface	查看接口配置
diagnose hardware deviceinfo nic port1	查看接口状态
get hard nic port1	查看接口状态
show firewall policy	查看防火墙策略
get system session list	查看会话表
diagnose sys session list	查看会话表，查看前过滤
diagnose sys session filter	会话表过滤
diagnose sys session full-stat	查看整体会话状态
get system session-info statistics	查看会话统计
diagnose sys ntp status	查看 ntp 状态
get router info routing-table all	查看路由表
get router info kernel	查看转发表
diagnose ip router	诊断路由协议
diagnose sys top	查看进程
diagnose sys kill	杀掉进程
show full-configuration system ha	查看 ha 配置
get sys ha status	查看 ha 状态
diagnose sys ha dump	查看 ha 信息
diagnose sys ha showcsum	检查配置文件是否同步
diagnose netlink redundant name	查看冗余接口状态
diagnose sys ha reset-uptime	复位 HA 计时器，进行 HA 切换
diagnose netlink aggregate name	查看聚合端口状态
exec log display	查看日志
diagnose hardware deviceinfo disk	查看硬盘状态
exec disk list	查看硬盘情况
exec disk format	格式化硬盘
diagnose firewall packet distribution	查看防火墙数据包分布情况
exec ping/ traceroute/ssh/telnet	执行常用命令
exec backup config	备份配置
exec restore config	恢复配置

diagnose deb flow	诊断数据流
diagnose sniffer packet	抓包命令