网络卫士安全网关系统

命令行手册

天融信
TOPSEC®
北京市海淀区上地东路 1 号华控大厦，100085
电话：（8610）82776666
传真：（8610）82776677
服务热线：800 810 5119
http: //www.topsec.com.cn

版权声明

本手册中的所有内容及格式的版权属于北京天融信公司（以下简称天融信）所有，未经天融信许可，任何人不得仿制、拷贝、转译或任意引用。

版权所有　不得翻印©　2011 天融信公司

商标声明

本手册中所谈及的产品名称仅做识别之用。手册中涉及的其他公司的注册商标或是版权属各商标注册人所有，恕不逐一列明。

TOPSEC® 天融信公司

信息反馈

http://www.topsec.com.cn

目　录

前言 **1**

文档目的 1
读者对象 1
相关文档 1
命令行约定 1
技术服务 2

命令行使用须知 **4**

管理员权限 4
命令分级 4
命令帮助 6

登录命令行 **6**

CONSOLE 口登录 6
SSH 远程登录 6

命令行快速指南 **7**

命令行详细说明 **8**

AAA 8
auth-map *8*
cert-accredit *14*
config *15*
onlineuser *16*
role *17*
sec-policy *24*
server *35*
server-sync *39*
sms *41*
user *42*
version *49*
ANTI-SPAM 49
blacklist *50*
greylist *51*
policy *53*
rbl *55*
reset *56*

show *56*
statistic *56*
whitelist *57*
AR 58
account *59*
apps *61*
custom *61*
dev *62*
dfi *63*
dfi-params *63*
disk *64*
flow-log *65*
flow_log_interval *65*
group_quota *66*
interface_quota *66*
ip-virus *67*
ip-virus-detail *68*
max-session *68*
monitorhost *68*
monitor-switch *69*
net-quota *70*
other-quota *70*
policy *70*
quota *72*
rules *72*
stat-object *74*
stat-object-detail *74*
tcp-quota *74*
udp-quota *75*
version *75*
virus *75*
virus-ip-top *76*
virus-group *77*
virus-domain *77*
virus-start-time *78*
DEBUG 78
filter *79*
module *81*
start *82*
clean *82*

DEFINE 82
area *83*
dns *87*
group_address *88*
group_service *92*
host *96*
query *100*
range *101*
schedule *105*
server *110*
service *114*
subnet *117*
virtual_server *121*
DPI 125
dns *126*
freemem *128*
ftp *128*
global *131*
http *134*
imap *138*
max-connection *140*
pattern *141*
policy *144*
pop3 ..... *147*
rsh *150*
rule *152*
smtp *154*
telnet *157*
webfilter *159*
FIREWALL 161
access-info *162*
enhancement *163*
group_policy *164*
policy *166*
dynamic-policy *175*
HA 176
HELPMODE 185
IDS 185
attack *186*
cc *186*

config *189*
expire-time *189*
list *190*
list-expire-time *190*
max-destination *191*
max-source *191*
packet *192*
rule *192*
sessions *195*
source-check *195*
tcp-trust-check *196*
white-list-check *196*
LOG 197
alarmevent *197*
alarmnotice *199*
log *206*
NAT 210
policy *211*
NETWORK 220
802.1X *222*
adsl *223*
anti-proxy *226*
arp *227*
arpproxy *231*
attribute *232*
attribute -group *234*
bgp *236*
bond *239*
cdp_neighbors *244*
dev *245*
dhcp *245*
dns *253*
hoststatistic *254*
interface *255*
igmp *276*
ip-probe *278*
l2tp *280*
link-backup *282*
mac-address-table *284*
mpls *286*

mroute *286*
ospf *289*
port-mirror *297*
port-statistic *301*
pptp *303*
rangstatistic *305*
reset *307*
rip *307*
route *318*
route-policy *321*
session *327*
spantree *338*
statistic *342*
subnetstatistic *344*
suitstate *345*
traffic *347*
tunnel *347*
virtual-line *350*
vlan *351*
PF 354
idbprule *354*
idsserver *355*
rule *357*
service *362*
PING 367
PKI 367
cacert *368*
clean *372*
cleancert *372*
ipseccertreq *372*
localca *374*
localcert *380*
remoteauth *382*
remotecert *383*
save *384*
sslcert *384*
sslcertreq *386*
tool *388*
usb *388*
webuicert *389*

QOS 390
config *390*
monitor *391*
rule *392*
SAVE 395
SHOW 395
SHOW_RUNNING 396
SNMP 397
managehost *397*
managesubnet *399*
set *400*
show *401*
snmpv3user *402*
start *403*
stop *403*
traphost *404*
SYSTEM 405
admin-auth-mode *406*
admininfo *407*
authset *417*
config *426*
devname *430*
flash *431*
mail-forward *431*
hd-check *432*
hd-rebuild *433*
httpd *433*
information *433*
killprocess *434*
monitord *435*
netflow *435*
netflow-filter *436*
netstat *438*
ntp *439*
probe-package *441*
probe-server-time *442*
probe-show *443*
probe-time *443*
reboot *444*
service *444*

showprocess *445*
shutdown *445*
sshd *446*
tcpdump *446*
telnetd *447*
terminal *447*
time *448*
top-policy *449*
traceroute *451*
update *451*
uptime *452*
vdcd *452*
version *453*
vs *453*
webui *454*
TELNET 457

前言

本手册向用户提供了通过本地控制台端口（console）及远程 SSH 方式对安全网关进行管理、配置的相关说明和帮助。

文档目的

本文档主要介绍如何通过命令行系统对网络卫士安全网关进行管理配置工作。

读者对象

熟悉网络卫士安全网关基本功能的资深管理员。

相关文档

《TopGate 命令行手册——IPSEC VPN 配置》
《TopGate 命令行手册——SSL VPN 配置》
《TopGate 命令行手册——防病毒配置》
《TopGate 命令行手册——IPS 配置》

命令行约定

- **基本语法**

网络卫士安全网关的命令由如下部分组成：

命令名 动作 [**选项** 参数]

命令行文字约定如下：

- 命令名一般为名词性的单词，主要说明该命令操作的对象，少数命令名为动词，直接进行动作（比如：exit、help等，其操作对象隐含）；命令名用**小写黑体**表示。
- 动作用于说明对命令所指定的对象的操作；用**小写黑体**表示。
- 选项多为名词性单词，与参数联合指定动作执行时所需要的一些信息，用**小写黑体**表示。

- 固定参数用五号Times New Roman表示，用户自定义参数用*斜体*表示。

- **分隔符**

在命令行手册中会出现以下几种分隔符号：

方括号（[]）表示可选项。

尖括号（<>）表示参数。

竖线（|）隔开多个相互独立的关键字或参数（只能选择其中一个）。

短线（-）表示数字形式的参数的范围，如 1-20

逗号分割参数（,…,…）：表示参数个数不确定的参数格式，比如向用户组添加若干个用户，每个用户间用“,”号分隔。

- **实例**

TopsecOS.define# **host add name** <*string1*> [**ipaddr** <*string2*>] [**macaddr** <*macaddress*>][**session** <*number1*>][**halfsession** <*number2*>] [**synproxy**<on|off>] [**vsid** <*number3*>][**mss** <*number4*>]

在上面的命令中 TopsecOS.define#表示当前设备名称为 TopsecOS，当前处在组件级命令 define 中。

HOST是基本命令，表示这是一个关于主机地址对象的命令；**add**是命令操作参数表示添加一个主机地址对象；**name**参数表示必选项，是添加主机地址对象时必须要设定的参数，用于表示主机地址对象的名称；**ipaddr**、**macaddr**、**session**等参数使用分隔符‘[ ]’，表示可选项；on和off关键字中间用分隔符“|”分开，表示只能选择on或off；*string1*等斜体字符是需要用户输入的参数，表示该主机地址对象的名称；

技术服务

天融信公司对于自身所有安全产品提供远程产品咨询服务，广大用户和合作伙伴可以通过多种方式获取在线文档、疑难解答等全方位的技术支持。

公司主页

http://www.topsec.com.cn/

在线技术资料

http://www.topsec.com.cn/support/down.asp

安全解决方案

http://www.topsec.com.cn/solutions/qw.asp

技术支持中心

http://www.topsec.com.cn/support/support.asp

天融信全国安全服务热线

800-810-5119

命令行使用须知

在使用命令行系统之前，请用户熟知如下信息。

管理员权限

网络卫士安全网关将登录安全设备的管理员根据权限分为三级：超级管理员、安全管理员和安全审计管理员。

- 超级管理员：可以访问所有命令行命令，管理员可以随意改变或删除配置参数。只有 superman 为唯一的超级用户，具有最高权限，而且可以修改此超级用户的名称及其口令密码。
- 安全管理员：可以访问除系统维护（例如重新启动、系统升级等）以外的所有命令，管理员可以对访问规则进行配置。但是无权分配管理员权限。
- 安全审计管理员：只能访问部分命令行命令，管理员只能查看系统配置，却无权修改现有的配置信息。

不同级别的用户提示符有所区别，超级管理员，提示符为#；安全管理员，提示符为“%”；安全审计管理员，提示符为“$”。

登录命令行系统后，若**1 分钟**内没有任何操作，则自动退出登录，以保障系统安全。如果仍然需要通过命令行管理，只能再次登录。

命令分级

网络卫士安全网关命令行分为多级，最高两级为系统级和组件级，下面分别介绍：

- 系统级

系统级为第一级，提供设备的基本管理命令。CLI 管理员登录后，直接进入该级，显示为：TopsecOS#（TopsecOS 为缺省设备名）。

在系统级下，按 tab 键，则显示出所有组件级命令。

- 组件级

组件级为第二级，提供每个安全组件（SE）所独有的管理命令。

CLI 管理员在系统级时，输入安全组件的名称并回车，即进入组件级，进行相应组

件的管理。

在组件级时，输入“exit”命令或“!”命令退出组件级，返回到系统级；

在系统级时，输入“exit”命令断开连接；

在任何一级，输入“end”命令退回系统级。

命令帮助

- 在提示符模式下，输入 “？”，显示所有下级命令列表。
- 在任何位置，按“Tab”键，如果只有唯一匹配，则补齐命令；如果有多个匹配，则显示所有匹配的命令列表，并等待管理员补充输入；如果没有匹配，则不响应。
- 任意时刻，按“↑”或“↓”键，都可选择历史命令。
- 在命令执行时，输入“Ctrl-C”中断当前命令的执行，回到系统级。
- 执行 helpmode 命令，切换命令行系统提示信息的语言（目前仅支持简体中文和英语）。

登录命令行

用户可以通过设备 Console 口或远程 SSH 两种方式对设备进行命令行配置和管理。

CONSOLE 口登录

通过设备的 Console 口进行本地管理，需要进行以下准备工作：

- 一台用于管理、配置安全设备的 PC 或笔记本
- 一条用于连接 PC 和安全设备的串口线（天融信设备随机配备）
- 配置超级终端软件（具体配置请参见安装手册的相关章节）

用户成功连接到安全网关后，依次输入默认的用户名“superman”和密码“talent”，即可登录到命令行系统。

SSH 远程登录

网络卫士安全网关在出厂默认配置中，允许用户通过 eth0 接口对安全设备进行 SSH 远程管理，eth0 口的默认管理地址是 192.168.1.254。

命令行快速指南

为了帮助用户更好地使用命令行系统，下表按照字母顺序列出了系统的所有功能组件命令：

组件级命令	功能描述
aaa	配置用户认证相关功能，包括角色、用户、认证服务器等。
anti-spam	配置管理反垃圾邮件功能
ar	配置管理 AR
avse	管理配置病毒过滤功能，具体使用请参见《TopGate 命令行手册——防病毒配置》。
debug	系统调试
define	定义系统资源，例如定义主机、子网等。
dpi	定义深度报文检测策略
firewall	设置防火墙规则，主要是 ACL 规则。
ha	高可用性设置。
helpmode	设定命令行的提示语言，目前仅支持中文或英文
ids	配置入侵检测规则
ips	配置入侵防御功能，包括入侵规则、响应动作等。具体配置请参见《TopGate 命令行手册——IPS 配置》。
log	设置日志服务器等相关参数。
nat	配置地址转换策略
network	网络设置，主要包括接口、路由、ARP、PPTP、DHCP、L2TP 等配置。
pf	包过滤规则设置
ping	发送 PING 包，验证网络连接情况。
pki	CA 管理，包括 CA 证书、VRC 用户证书等
qos	配置带宽规则，以便对网络流量进行限制。
save	保存配置
show	查看已保存配置
show_running	查看运行配置
snmp	配置使用 SNMP 相关功能，包括管理主机、陷进主机等。
sslvpn	配置 SSL VPN 隧道策略，包括 Web 转发规则、端口转发规则、全网接入规则、文件共享规则等。具体配置请参见《TopGate 命令行手册——SSLVPN 配置》。
system	系统管理，包括系统维护、备份、升级等基础管理。
telnet	远程登录命令
vpn	IPSEC VPN 配置，主要包括隧道策略、VRC 用户配置等。具体配置请参见《TopGate 命令行手册——IPSecVPN 配置》。

命令行详细说明

AAA

本模块中的命令主要用来配置用户认证的基本信息（如：本地认证数据库的配置和管理，在线用户的管理，认证服务器的配置和管理以及认证用户角色的配置和管理），以实现对用户进行多种协议、多种类型、多种方式的认证，并保证用户访问和设备之间访问的安全性。

进入本命令模块操作如下：

aaa <cr>

退出本命令模块操作如下：

end <cr>

CLI 管理员登录安全网关进入本命令模块后，可以执行相应的组件管理命令。下面将详细描述本命令模块下的所有组件管理命令。命令的实例输入格式将按已经进入本命令模块书写。

下一级命令列表

命令	功能
auth-map	设置映射策略
cert-accredit	证书授权配置
config	用户认证配置信息管理
onlineuser	管理经过认证的活动用户信息
role	用户角色信息管理和设置
sec-policy	可信接入模块设置
server	配置和管理外部认证服务器的信息。
Server-sync	LDAP 服务器同步配置信息
Sms	短信认证服务器信息配置
user	用户信息配置和管理
version	查看用户认证模块的版本信息

auth-map

对于采用外部服务器认证和证书认证的远程用户，需要先将用户按照管理员设定的属性映射到本地认证数据库的用户角色上，然后基于用户角色进行访问权限控制。该组命令用于将外部认证服务器和证书服务器上用户的按照某个属性映射到

LocalDB 的角色上，该用户的权限和 LocalDB 上对应角色的权限一致。

auth-map add server <*string1*> **mapping-type** [default|exter-mapping] [**status** [valid|invalid]] [**role-name** <*string2*>] [**attr-name** <*string3*>]

命令描述：

该命令用于添加外部服务器认证用户和证书认证用户的映射策略。

参数说明：

add	添加映射策略
server	选择外部认证服务器名。
string1	输入已经添加的外部认证服务器的名称。
mapping-type	设置组映射类型。可选项为：本地角色集合映射和外部属性映射。
defaultt|exter-mapping	Default：本地角色集合映射，表示将外部服务器上的所有用户映射到 LocalDB 中某个用户角色上。 Exter-map：外部属性映射，表示将外部认证服务器上的用户根据映射属性值映射为同名的本地用户角色，该用户的权限和 LocalDB 上对应用户角色的权限一致。
status	设置是否启用该认证策略。
valid|invalid	可选项：valid 表示是，invalid 表示否；默认值为“是”。 说明： 当选择“否”后该策略将对用户认证不产生任何作用。
role-name	可选项，仅当“mapping-type”选择“default”时需要设置该选项，设置将外部服务器上的所有用户映射到 LocalDB 中某个选定的用户角色上。
string2	输入已经添加的本地角色名称字符串。
attr-name	可选项，仅当“mapping-type”选择“exter-mapping”时需要设置该选项，设置根据此处设定的属性将认证服务器的用户映射到 LocalDB 中的同名用户角色上。
string3	输入映射依据的属性字段名。

使用说明：

当“mapping-type”选择“exter-mapping”时，将根据“attr-name”设定的属性将认证服务器的用户映射到 LocalDB 中的同名用户角色上，因此需要在本地数据库中添加同名的用户角色。

实例：

** 增加 Radius 认证服务器的映射策略，所有 Radius 认证的用户均映射为本地角色 radius-role。

auth-map add server *radius-server* **mapping-type** default **role-name** *radius-role*<cr>

auth-map add-role server <*string1*> **rolename** <*string2*>

命令描述：

该命令用于添加一个角色到认证属性规则。

参数说明：

add-role	添加一个角色到认证属性规则。
server	指定认证、授权服务器名称。
string 1	字符串，输入服务器的名称。
rolename	指定所添加的角色名称。
string2	字符串，输入角色名称。

实例：

**添加一个名为 role1 的角色到服务器 sev。

auth-map add-role server *sev* **rolename** *role1*

auth-map modify server <*string1*> **mapping-type** [default|exter-mapping] [**status** [valid|invalid]]

[**role-name** <*string2*>] [**attr-name** <*string3*>]

命令描述：

该命令用于修改映射策略。

参数说明：

modify	修改映射策略
server	选择外部认证服务器名。
string1	输入已经添加的外部认证服务器的名称。
mapping-type	设置组映射类型。可选项为：本地角色集合映射和外部属性映射。
defaultt|exter-mapping	Default：本地角色集合映射，表示将外部服务器上的所有用户映射到 LocalDB 中某个用户角色上。 Exter-mapping：外部属性映射，表示将外部认证服务器上的用户根据映射属性值映射为同名的本地用户角色，该用户的权限和 LocalDB 上对应用户角色的权限一致。
status	设置是否启用该认证策略。
valid|invalid	可选项：valid 表示是，invalid 表示否；默认值为“是”。 说明： 当选择“否”后该策略将对用户认证不产生任何作用。
role-name	可选项，仅当“mapping-type”选择“default”时需要设置该选项，设置将外部服务器上的所有用户映射到 LocalDB 中某个选定的用户角色上。
string2	输入已经添加的本地角色名称字符串。
attr-name	可选项，仅当“mapping-type”选择“exter-mapping”时需

	要设置该选项，设置根据此处设定的属性将认证服务器的用户映射到 LocalDB 中的同名用户角色上。
string3	输入映射依据的属性字段名。

实例：

** 修改 Radius 认证服务器的映射策略，不同的 Radius 认证的用户均映射为本地同名的角色。

auth-map modify server *radius-server* **mapping-type** exter-mapping **attr-name** *name*<cr>

auth-map delete server <*string*>

命令描述：

该命令用于删除指定服务器的映射策略。

参数说明：

delete	删除本地认证数据库中的指定用户。
server	指定服务器名称。
string	字符串，输入要删除的服务器的名称。

使用说明：

系统内置的 cert 和 localdb 服务器的映射策略无法删除。

实例：

** 删除 radius-server 的映射策略。

auth-map delete server *radius-server*<cr>

auth-map del-role server <*string1*> **rolename** <*string2*>

命令描述：

该命令用于从认证授权属性规则中删除一个角色。

参数说明：

del-role	从认证属性规则中删除一个角色。
server	指定认证、授权服务器名称。
string 1	字符串，输入服务器的名称。
rolename	指定所删除的角色名称。
string2	字符串，输入角色名称。

实例：

**从认证授权服务器 sev 中删除一个名为 role1 的角色。

auth-map del-role server *sev* **rolename** *role1*

auth-map clean<cr>

命令描述：

本命令用于删除管理员添加的所有映射策略。系统内置的 cert 和 localdb 服务器的映射策略无法清除。

auth-map movedown server <*string*>

命令描述：

远程用户登录安全网关设备进行认证时，检索本地数据库或外部认证服务器中是否有匹配的用户名，一旦找到匹配的用户将停止检索。检索的先后顺序由服务器映射列表中的排列顺序来决定。当多个数据库中存在同名的用户时，安全网关设备根据最先匹配的认证授权服务器的映射属性进行映射。本命令用于将指定服务器的映射策略向下移动一位。

参数说明：

movedown	下移映射策略。
server	指定要移动哪个服务器的映射策略。
string	输入服务器名。

实例：

** 将本地服务器的映射策略下移一位。

auth-map movedown server *localdb*

auth-map moveup server <*string*>

命令描述：

远程用户登录安全网关设备进行认证时，检索本地数据库或外部认证服务器中是否有匹配的用户名，一旦找到匹配的用户将停止检索。检索的先后顺序由服务器映射列表中的排列顺序来决定。当多个数据库中存在同名的用户时，安全网关设备根据最先匹配的认证授权服务器的映射属性进行映射。本命令用于将指定服务器的映射策略向上移动一位。

参数说明：

moveup	上移映射策略。
server	指定要移动哪个服务器的映射策略。
string	输入服务器名。

实例：

** 将本地服务器的映射策略上移一位。

auth-map moveup server *localdb*

auth-map movedown-num server <*string*> **num** <*number*>

命令描述：

本命令用于将指定服务器的映射策略向下移动到某一位置。

参数说明：

movedown-num	向下移动映射策略到某一位置。
server	指定要移动哪个服务器的映射策略。
string	输入服务器名。
num	指定移动的目的位置。
number	输入数字。

实例：

** 将本地服务器的映射策略移动到第四位。

auth-map moveup server *localdb* **num** 4

auth-map show [**server** <*string*>]

命令描述：

本命令用于查看所有或指定服务器的映射策略的信息。

参数说明：

show	查看映射策略的信息。
server	可选项，指定要查看哪个服务器的映射策略。
string	输入要查看的服务器名。

实例：

** 查看所有映射策略。

auth-map show<cr>

** 查看证书服务器的映射策略。

auth-map show server *cert*

auth-map clean-role server <*string*>

命令描述：

该命令用于清除认证授权属性规则中所有的角色信息。

参数说明：

clean-role	清除认证授权属性规则中所有角色信息。
server	指定认证、授权服务器的名称。
string	输入认证、授权服务器名。

实例：

** 清除服务器 sev 中认证、授权属性规则中所有角色信息。

auth-map clean-role server *sev*

cert-accredit

证书授权配置

cert-accredit add rule < *string*> **role-name** < *string*>

命令描述：

添加授权规则

参数说明：

add	添加授权规则
rule	设置条件表达式
string	字符串
role-name	设置角色名
string	字符串

cert-accredit delete index <*number*>

命令描述：

删除授权规则

cert-accredit modify index <*number*> **rule** < *string*> **role-name** < *string*>

命令描述：

修改授权规则

参数说明：

modify	添加授权规则
rule	设置条件表达式
string	字符串
role-name	设置角色名
string	字符串

cert-accredit move-up index <*number*>

命令描述：

向上移动授权规则

cert-accredit move-down index <*number*>

命令描述：

向下移动授权规则

cert-accredit show-num <cr>

命令描述：

显示授权规则的条数

cert-accredit show<cr>

命令描述：

查看授权规则

cert-accredit clean<cr>

命令描述：

清空所有授权规则

config

用户认证配置信息管理

config reset <cr>

命令描述：

本命令将所有认证配置信息恢复默认配置。

config show <cr>

命令描述：

本命令将显示当前系统的所有认证配置信息。

onlineuser

该组命令用于管理经过认证的活动用户信息，包括所有在线的用户。

onlineuser showall <cr>

命令描述：

本命令用于查看所有在线用户。

onlineuser deleteuser name <*string*> **type** < common|otp|cgi >

命令描述：

本命令用于根据用户名称删除在线用户，强迫其下线。

同一个用户能够以多个 IP 地址同时登录安全网关，执行本命令后可以强迫该用户下线，无论它以哪个 IP 地址登录安全网关。

参数说明：

deleteuser	根据用户名称删除在线用户。
name	指定用户名称。
string	字符串，输入要删除的在线用户名称。
type	指定用户类型。
common|otp|cgi	输入要删除的在线用户的用户类型：普通用户| OTP 用户|CGI 用户。

使用说明：

只有用户名称和用户类型与在线用户信息同时匹配，才能够在活动列表中删除该用户，强迫其下线。

实例：

**强迫“普通用户”“test1”下线。

onlineuser deleteuser name *test1* **type** common <cr>

onlineuser deleteaddr addr <*ipaddress*>

命令描述：

本命令用于根据 IP 地址删除在线用户信息，强迫其下线。

同一个用户能够以多个 IP 地址同时登录安全网关，执行本命令后可以强迫指定 IP 地址上登录安全网关的用户下线，但是以其它 IP 地址登录的用户仍旧处于在线活动状态。

参数说明：

deleteaddr	根据 IP 地址删除在线用户信息。
addr	指定 IP 地址。
ipaddress	标准的 IP 地址字符串，输入要删除的在线用户的 IP 地址。

实例：

** 删除 IP 地址为 192.168.83.220 的用户的在线信息。

onlineuser deleteaddr addr 192.168.83.220

role

对用户角色信息进行管理和设置。网络卫士安全网关基于角色对所有用户进行访问权限控制。对证书认证用户和外部认证服务器的用户，需要按照设定的属性将用户映射到本地数据库中的用户角色，根据本地角色来进行授权。对于本地密码认证的用户，也基于其所属的角色来进行权限分配。当一个用户属于若干个用户角色时，按照用户角色的先后顺序进行访问控制规则匹配。

role add name <*string*> [**description** <*string*>] [**nc-pool** <*string*>] [**mail** <*string*>]

[**version-control** <define|nouse>] [**version** < standard|ukey|limit|secure|ukey_limit|ukey_secure >]

[**dns1** <*ipaddress1*>] [**dns2** <*ipaddress2*>] [**wins1** <*ipaddress3*>] [**wins2** <*ipaddress4*>]

[**short-msg** <yes|no>]

命令描述：

本命令用于添加用户角色。

参数说明：

add	添加用户角色。
name	指定角色名。
string	名称字符串
description	可选项，添加对该角色必要的描述信息。
string	字符串
nc-pool	可选项，如果客户端登录安全网关后需要由安全网关为其分配 IP 地址，则需要在安全网关上设置可分配的地址范围，即地址池。为可选项。地址池可以在此处或 VRC 管理处设定，用户角色地址池设置优先于 VRC 管理处的设置。 说明： （1）使用全网接入的用户角色必须配置该选项，否则该角色的用户无法获取 DHCP 地址池中的地址。 （2）远程客户端进行全网接入时，从用户所属的第一个用户角色中相关联的地址池中分配 IP 地址。该地址池必须是 DHCP 服务器上设定的地址池中的一个。
string	输入已经设置的 DHCP 地址池的子网 IP 及掩码。
mail	设置该角色的邮箱地址。可选项。
string	邮件地址格式的字符串。
version-control	可选项，设置是否对 VRC 客户端采用的版本类型进行控制。只有当用户配置的“客户端版本控制”选择“默认”时，VRC 的版本控制才会匹配本处的设置。
define|nouse	define：“自定义”表示 VRC 客户端使用的版本应当与此处设定的版本相一致，才可以登录认证成功。 此时需要选择“客户端版本”。目前支持的客户端版本类型有：标准版、安全版、限制版，UKEY、安全版＋UKEY、限制版＋UKEY。 nouse：“不使用”表示对该 VRC 客户端不使用版本控制。此时客户端的版本控制信息还要查看 VRC 管理处关于“客户端版本控制”的设置。
version	可选项，当“客户端版本控制”设置为“自定义”时需要设置该项，用于限制 VRC 客户端使用的版本类型，只有符合规定版本的 VRC 用户才可以登录认证成功。
standard|ukey|limit|secure|ukey_limit|ukey_secure	目前支持的客户端版本类型有：standard 表示标准版、secure 表示安全版、limit 表示限制版，ukey 表示 UKEY 版、ukey_secure 表示安全版＋UKEY、ukey_limit 表示限制版＋UKEY。
dns1	可选项，安全网关可以通过 DNS 服务器设置选项来设置客户端虚拟网卡的 DNS 地址。此处设置首选 DNS 服务器的 IP 地址。
ipaddress1	标准的 IP 地址字符串。
dns2	可选项，设置备选 DNS 服务器的 IP 地址。
ipaddress2	标准的 IP 地址字符串。
wins1	可选项，设置客户端虚拟网卡的内部首选 WINS 服务器地址。
ipaddress3	IP 地址字符串
wins2	可选项，设置客户端虚拟网卡的内部备用 WINS 服务器地址。
ipaddress4	IP 地址字符串

short-msg	设置是否进行强制短信认证
yes|no	是/否

实例：

** 添加名称为 cert-role 的用户角色信息。

role add name *cert-role*

role clean<cr>

命令描述：

本命令用于删除所有用户角色。

role cleanuser name <*string*>

命令描述：

本命令用于删除指定用户角色中的所有用户。

参数说明：

cleanuser	删除指定用户角色中的所有用户。
name	指定用户角色名称。
string	字符串，输入要清空所有用户的角色名称。

role delete name <*string*> **by-admin-name** <*string*>

命令描述：

本命令用于删除指定用户角色。

参数说明：

delete	删除指定用户角色。
name	指定用户角色名称。
string	字符串，输入角色名称。
by-admin-name	指定分级管理员名称。
string	字符串。

role deluser name <*string*> **username** <*string*>

命令描述：

本命令用于删除指定用户角色中的某个用户。

参数说明：

deluser	删除指定用户角色中的某个用户。
name	指定用户角色名称。

string	字符串，输入角色名称。
username	指定要删除的用户名。
string	字符串，输入用户的名称。

实例：

**删除用户角色 radius_server 中的用户 lisi。

role deluser name *radius_server* **username** *lisi*

role modify name <*string*> [**description** <*string*>] [**nc-pool** <*string*>] [**mail** <*string*>] [**version-control** <define|nouse>] [**version** < standard|ukey|limit|secure|ukey_limit|ukey_secure >] [**dns1** <*ipaddress1*>] [**dns2** <*ipaddress2*>] [**wins1** <*ipaddress3*>] [**wins2** <*ipaddress4*>] [**short-msg** <yes|no>]

命令描述：

本命令用于修改已添加的用户角色的属性。

参数说明：

modify	修改已添加的用户角色的属性。
name	指定角色名。
string	名称字符串
description	可选项，添加对该角色必要的描述信息。
string	字符串
nc-pool	可选项，如果客户端登录安全网关后需要由安全网关为其分配 IP 地址，则需要在安全网关上设置可分配的地址范围，即地址池。为可选项。地址池可以在此处或 VRC 管理处设定，用户角色地址池设置优先于 VRC 管理处的设置。 说明： （1）使用全网接入的用户角色必须配置该选项，否则该角色的用户无法获取 DHCP 地址池中的地址。 （2）远程客户端进行全网接入时，从用户所属的第一个用户角色中相关联的地址池中分配 IP 地址。该地址池必须是 DHCP 服务器上设定的地址池中的一个。
string	输入已经设置的 DHCP 地址池的子网 IP 及掩码。
mail	设置该角色的邮箱地址。可选项。
string	邮件地址格式的字符串。
version-control	可选项，设置是否对 VRC 客户端采用的版本类型进行控制。只有当用户配置的“客户端版本控制”选择“默认”时，VRC 的版本控制才会匹配本处的设置。
define|nouse	define：“自定义”表示 VRC 客户端使用的版本应当与此处设定的版本相一致，才可以登录认证成功。此时需要选择“客户端版本”。目前支持的客户端版本类型有：标准版、安全版、限制版，UKEY、安全版＋UKEY、限制版＋UKEY。

	nouse:“不使用”表示对该 VRC 客户端不使用版本控制。此时客户端的版本控制信息还要查看 VRC 管理处关于“客户端版本控制”的设置。
version	可选项，当“客户端版本控制”设置为“自定义”时需要设置该项，用于限制 VRC 客户端使用的版本类型，只有符合规定版本的 VRC 用户才可以登录认证成功。
standard|ukey|limit|secure|ukey_limit|ukey_secure	目前支持的客户端版本类型有：standard 表示标准版、secure 表示安全版、limit 表示限制版，ukey 表示 UKEY 版、ukey_secure 表示安全版＋UKEY、ukey_limit 表示限制版＋UKEY。
dns1	可选项，安全网关可以通过 DNS 服务器设置选项来设置客户端虚拟网卡的DNS地址。此处设置首选DNS服务器的 IP 地址。
ipaddress1	标准的 IP 地址字符串。
dns2	可选项，设置备选 DNS 服务器的 IP 地址。
ipaddress2	标准的 IP 地址字符串。
wins1	可选项，设置客户端虚拟网卡的内部首选 WINS 服务器地址。
ipaddress3	IP 地址字符串
wins2	可选项，设置客户端虚拟网卡的内部备用 WINS 服务器地址。
ipaddress4	IP 地址字符串
short-msg	设置是否进行强制短信认证
yes|no	是/否

role num<cr>

命令描述：

本命令用于获得所有用户角色的数目。

role search key-word [name |mail| description] **key-value** <*string*>

命令描述：

本命令用于查找用户角色。

参数说明：

search	查找用户角色
key-word	指定查找字段。
name |mail| description	姓名|邮箱|描述信息。
key-value	指定查找关键字
string	字符串，输入要查找的关键字。

使用说明：

只有首先指定查找字段，才能进一步指定关键字。

实例：

**查找名称为“lisi”的用户角色。

role search key-word name **key-value** *lisi* <cr>

role show [**name** <*string*>] [**from** <*number*>] [**to** <*number*>] [**by-admin-name** <*string*>]

命令描述：

本命令用于查看用户角色信息。

参数说明：

show	查看用户角色信息
name	可选项，指定查看角色名
string	字符串，输入角色名。
from	可选项，指定开始用户角色序号。
number	数值
to	可选项，指定结束用户角色序号。
number	数值
by-admin-name	指定分级管理员名称。
string	字符串。

使用说明：

不指定任何参数时显示所有角色信息。

实例：

**查看名称为“lisi”的用户角色。

role show name *lisi* <cr>

role show-refer name <*string*>

命令描述：

本命令用于查看用户角色被引用的信息。

参数说明：

show-refer	查看用户角色信息
name	指定查看角色名
string	字符串，输入角色名。

实例：

**查看名称为“lisi”的用户角色被引用的情况。

role show-refer name *lisi* <cr>

role useradd name <*string*> **username** <*string*>

命令描述：

本命令用于向用户角色添加用户信息。

参数说明：

useradd	向用户角色添加用户信息
name	指定角色名
string	字符串，输入角色名。
username	输入用户名
string	字符串

实例：

**将名称为“lisi”的用户添加到角色 radius-role 中。

role useradd name radius-role **username** *lisi* <cr>

role usershow name <*string*>

命令描述：

本命令用于查看属于某用户角色中的用户信息。

参数说明：

usershow	查看用户角色中的用户信息
name	指定查看角色名
string	字符串，输入角色名。

实例：

**查看名称为“lisi”的用户角色中的用户情况。

role usershow name *lisi* <cr>

role assign-role-add role-name <*string*> **admin-name** <*string*>

命令描述：

为分级管理员分配角色

参数说明：

assign-role-add	为分级管理员分配角色
role-name	输入角色名
string	字符串，输入已经设置的角色的名称。
admin-name	设置分级管理员名。
string	字符串，输入已经设置的分级管理员名。

role assign-role-modify role-name <*string*> **admin-name** <*string*>

命令描述：

修改分级管理员分配角色

参数说明：

assign-role- modify	修改为分级管理员分配角色
role-name	输入角色名
string	字符串，输入已经设置的角色的名称。
admin-name	设置分级管理员名。
string	字符串，输入已经设置的分级管理员名。

role assign-role-delete admin-name <*string*>

命令描述：

删除分级管理员和角色绑定关系

参数说明：

assign-role- delete	修改为分级管理员分配角色
admin-name	设置分级管理员名。
string	字符串，输入已经设置的分级管理员名。

role assign-role-show<cr>

命令描述：

显示分级管理员已分配角色

sec-policy

可信接入模块，设置认证客户端接入时要检测主机上某些安全因素是否满足，如不满足则不允许接入。

sec-policy orgadd type <user|role>**name** <*string*> [**policyname** <*string*>]

命令描述：

本命令用于设置用户或角色的安全策略，即设置对用户或角色进行安全检测的规则组。

参数说明：

orgadd	添加安全策略
type	选择为用户或角色设置安全策略
user|role	用户/角色
name	设置用户或角色的名称
string	字符串，输入已经设置的用户或角色的名称。
policyname	可选项，设置安全规则组。
string	字符串，输入已经设置的安全规则组名，可以输入一个或多个，输入多个时用引号，规则中间用逗号分隔。

使用说明：

和**orgadd-policy**命令的区别在于，此命令每次都将规则组重置，即重新设置新的规则组。而**orgadd-policy**命令可以对用户已有的策略基础上添加新的规则组。

实例：

**为用户 otpuser 设置安全规则组“secpolicy1”和“gprocess_tp”。

sec-policy orgadd type user **name** *otpuser* **policyname** ‘*secpolicy1,gprocess_tp*’

sec-policy orgadd-policy type <user|role>**name** <*string*> [**policyname** <*string*>]

命令描述：

本命令用于为用户或角色添加一个安全策略。

参数说明：

orgadd-policy	添加安全策略
type	选择为用户或角色设置安全策略
user|role	用户/角色
name	设置用户或角色的名称
string	字符串，输入已经设置的用户或角色的名称。
policyname	可选项，设置安全规则组。
string	字符串，输入已经设置的安全规则组名，可以输入一个或多个，输入多个时用引号，规则中间用逗号分隔。 说明： 输入空格字符串时将清空用户或角色的所有安全策略。

使用说明：

和**orgadd**命令的区别在于此命令可以对用户已有的策略基础上添加新的规则组。而**orgadd**命令则每次都将规则组重置。

实例：

**为用户 otpuser 设置安全规则组“secpolicy1”和“gprocess_tp”。

sec-policy orgadd-policy type user **name** *otpuser* **policyname ‘***secpolicy1,*

gprocess_tp’

sec-policy orgdel-policy type <user|role>**name** <*string*> [**policyname** <*string*>]

命令描述：

本命令用于删除用户或角色的某个安全策略。

参数说明：

orgdel-policy	删除用户或角色的某个安全策略
type	选择为用户或角色设置安全策略
user|role	用户/角色
name	设置用户或角色的名称
string	字符串，输入已经设置的用户或角色的名称。
policyname	可选项，设置安全规则组。不设置该项时清空所有安全策略。
string	字符串，输入已经设置的安全规则组名，可以输入一个或多个，输入多个时用引号，规则中间用逗号分隔。

实例：

**为用户 otpuser 删除安全规则组“secpolicy1”。

sec-policy orgdel-policy type user **name** *otpuser* **policyname** *secpolicy1*

sec-policy orgclean type <user|role>**name** <*string*>

命令描述：

本命令用于清空用户或角色的安全策略。

参数说明：

orgclean	清空安全策略
type	选择为用户或角色清空安全策略
user|role	用户/角色
name	设置用户或角色的名称
string	字符串，输入已经设置的用户或角色的名称。

实例：

**为用户 otpuser 设置清空安全规则组。

sec-policy orgclean type user **name** *otpuser*

sec-policy orgmodify type <user|role>**name** <*string*> [**policyname** <*string*>]

命令描述：

本命令用于修改用户或角色的安全策略。

参数说明：

orgmodify	修改用户或角色的安全策略
type	选择为用户或角色设置安全策略
user|role	用户/角色
name	设置用户或角色的名称
string	字符串，输入已经设置的用户或角色的名称。
policyname	可选项，设置安全规则组。
string	字符串，输入已经设置的安全规则组名，可以输入一个或多个，输入多个时用引号，规则中间用逗号分隔。

实例：

**为用户 otpuser 修改安全策略，设置其安全规则组为“secpolicy1”和“gprocess_tp”。

sec-policy orgmodify type user **name** *otpuser* **policyname ‘***secpolicy1,gprocess_tp*’

sec-policy orgshow [**type** <user|role>] [**name** <*string*>]

命令描述：

本命令用于查看用户或角色的安全策略。

参数说明：

orgshow	查看安全策略
type	可选项，选择查看类型：用户或角色
user|role	用户/角色
name	可选项，设置用户或角色的名称
string	字符串，输入已经设置的用户或角色的名称。

实例：

**查看用户 otpuser 设置的安全规则组。

sec-policy orgshow type user **name** *otpuser*

sec-policy policyadd name <*string*> [**policy** <and|or>] [**right** <must|ignore>] **rulename** <*string*>

命令描述：

本命令用于将多个安全规则进行逻辑组合，从而建立安全规则组。安全规则组就是对登录客户端进行是否可信检测的安全策略，当管理员进一步设置用户及角色的安全规则组时，设备自动将策略的各个规则按照设定的逻辑整合后，对登录客户端进行安全检测。

参数说明：

policyadd	添加安全规则组
name	指定规则组的名称
string	字符串，输入规则组名。
policy	可选项，设置该规则组中的安全规则之间的逻辑关系。默认为“与”。
and|or	And：表示“并”，当选择“and”时，客户端的检测项目必须同时满足所有安全规则设定的条件，才表示该规则组满足安全条件。 Or：表示“或”，选择“or”时，客户端的检测项目只要满足其中一项安全规则设定的条件，即表示该规则组满足安全条件。
right	可选项，设置权限为必须满足或可以忽略。 说明： 安全规则组应用于“角色”时该选项才有意义，应用于“用户”时该选项设置没有意义。
must|ignore	“must”表示必须满足；“ignore”表示可以忽略； 说明： 规则组的属性设置为“必须满足”，表示当角色设置该安全规则组时，必须满足该处设定的安全检测条件，如果不满足则拒绝登录。 规则组的属性设置为“可以忽略”，表示当角色设置该安全规则组时，如果该项不满足则不能拥有该角色的权限但是可以登录。
rulename	可选项选择该规则组中包含的安全规则。
string	字符串，输入已经设置的安全规则名，可以输入一个或多个，输入多个时用引号，规则中间用逗号分隔。

实例：

**添加名称为“secpolicy1”的安全规则组，包含安全规则 os_winxp 和 process_tp，设置为默认权限：可以忽略，安全规则之间的关系为默认的“与”。

sec-policy policyadd name *secpolicy1* **rulename ‘***os_winx, process_tp*’

sec-policy policyclean <cr>

命令描述：

本命令用于 清空所有安全规则组。

sec-policy policydel name <*string*>

命令描述：

本命令用于删除某安全规则组

参数说明：

policydel	删除某安全规则组
name	指定规则组名
string	字符串，输入规则组名。

sec-policy policymodify name <*string*> [**policy** <and|or>] [**right** <must|ignore>] [**rulename** <*string*>]

命令描述：

本命令用于修改安全规则组的属性。

参数说明：

policymodify	修改安全规则组的属性
name	指定规则组的名称
string	字符串，输入规则组名。
policy	可选项，设置该规则组中的安全规则之间的逻辑关系。默认为“与”。
and|or	And：表示“并”，当选择“and”时，客户端的检测项目必须同时满足所有安全规则设定的条件，才表示该规则组满足安全条件。 Or：表示“或”，选择“or”时，客户端的检测项目只要满足其中一项安全规则设定的条件，即表示该规则组满足安全条件。
right	可选项，设置权限为必须满足或可以忽略。 说明： 安全规则组应用于“角色”时该选项才有意义，应用于“用户”时该选项设置没有意义。
must|ignore	“must”表示必须满足；“ignore”表示可以忽略； 说明： 规则组的属性设置为“必须满足”，表示当角色设置该安全规则组时，必须满足该处设定的安全检测条件，如果不满足则拒绝登录。 规则组的属性设置为“可以忽略”，表示当角色设置该安全规则组时，如果该项不满足则不能拥有该角色的权限但是可以登录。
rulename	可选项，选择该规则组中包含的安全规则。
string	字符串，输入已经设置的安全规则名，可以输入一个或多个，输入多个时中间用逗号分隔。

实例：

**添加名称为“secpolicy1”的安全规则组，包含安全规则 os_winxp 和 process_tp，设置为默认权限：可以忽略，安全规则之间的关系为默认的“与”。

sec-policy policyadd name *secpolicy1* **rulename ‘***os_winx, process_tp*’

sec-policy policyshow [**name** <*string*>] [**begin** <*number*>] [**end** <*number*>]

命令描述：

本命令用于查看安全规则组信息。

参数说明：

policyshow	查看安全规则组信息
name	可选项，指定查看名称
string	字符串，输入规则组名。
begin	指定开始序号。
number	数值
end	指定结束序号。
number	数值

使用说明：

不指定任何参数时显示所有规则组信息。

实例：

**查看名称为“gg”的规则组属性。

sec-policy policyshow name *gg* <cr>

sec-policy rule-search [**name** <*string*>] [**check-type** < regkey|file|ver|process|port| service| system-packet| os |device|virus >] [**check-os** <all|win95|win98|winnt|win2000| winxp|win2003| vista|2008|win7>] [**description** <*string*>]

命令描述：

本命令用于查找安全规则。

参数说明：

rule-search	查看安全规则
name	可选项，指定查看名称
string	字符串，输入规则名。
check-type	可选项，指定根据检测项目的类型来查看

regkey|file|ver|process|port| service| system-packet| os|device|virus	选择检测项目类型，可选项分别对应：注册表项、文件状态、文件版本、进程、端口、服务、系统补丁、操作系统、设备、病毒。
check-os	可选项，指定根据检测的操作系统的类型来查看。
all|win95|win98|winnt|win2000|winxp |win2003|vista|2008|win7	可选项分别对应“所有”、“WIN95”、“WIN98”、“WINNT”、“WIN2000”、“WINXP”、“WIN2003”、“VISTA”、“2008”或“Windows 7”。
description	描述信息
string	字符串

使用说明：

不指定任何参数时显示所有安全规则的信息。当指定多个参数时，只会显示同时满足设定条件的查询结果。

实例：

**查找名称为“os_winxp”的规则属性。

sec-policy rule-search name *os_winxp* <cr>

sec-policy ruleadd name <*string*> **check-type** < regkey|file|ver|process|port| service| system-packet| os|device|virus > [**check-os** <all|win95|win98|winnt|win2000| winxp| win2003| vista| 2008|win7>] [**check-item** <*string*>] **[check-value** <*string*>] [**operate-code** [eq|ge|le|contain] [**description** <*string*>]

命令描述：

本命令用于添加安全规则。

参数说明：

ruleadd	添加安全规则
name	输入规则名称
string	字符串，输入规则名。
check-type	必选项，指定检测项目的类型
regkey|file|ver|process|port| service| system-packet| os|device|virus	选择检测项目类型，可选项分别对应：注册表项、文件状态、文件版本、进程、端口、服务、系统补丁、操作系统、设备、病毒。
check-os	可选项，仅当检测项目的类型选择“os”时需要设置该项。对于检测类型“check-type”不是“操作系统”的规则起作用，其作用是如果被检测机和“check

	－os”设置的系统不同则该条规则会被忽略
all|win95|win98|winnt|win2000|winxp|win2003|vista|2008|win7	可选项分别对应“所有”、“WIN95”、“WIN98”、“WINNT”、“WIN2000”、“WINXP”、“WIN2003”、“VISTA”、“2008” 或 Windows 7。
check-value	可选项，设置对客户端主机的详细检测值。设置不同的“检测类型”时，有不同的设置项目。
string	1）当检测类型选择“系统补丁”时，可选项为“SP1”、“SP2”、“SP3”、“SP4”，检测客户端主机的系统大补丁或系统小补丁是否大于等于或等于检测值。 2）当检测类型选择“操作系统”时，可选项为“是”或“不是”，检测客户端主机的操作系统是否为“检测项”处设定的值。
check-item	设置对客户端主机的详细检查项目。
string	设置不同的“检测类型”时，可选项不同： 1）当检测类型选择“系统补丁”时，可选项为“系统大补丁”、“系统小补丁”。 2）当检测类型选择“操作系统”时，可选项为“WIN95”、“WIN98”、“WINNT”、“WIN2000”、“WINXP”、“WIN2003”、“VISTA”或“2008”。
operate-code	检测类型选择“注册表项”和“文件版本”时需要设置该项。
eq|ge|le|contain	相等/大于等于/小于等于/包含
description	添加对该规则必要的描述信息
string	字符串

使用说明：

不指定任何参数时显示所有安全规则的信息。当指定多个参数时，只会显示同时满足设定条件的查询结果。

实例：

**添加名称为“os_winxp”的规则，用于检查主机的操作系统是否为 WindowsXP。

sec-policy ruleadd name *os_winxp* **check-type** *os* **check-item** *WINXP* <cr>

sec-policy ruleclean<cr>

命令描述：

本命令用于当所有安全规则均未被引用时，清空所有安全规则。如果有规则被规则组引用，则该命令不能清空规则。

sec-policy ruledel name <*string*>

命令描述：

本命令用于删除某安全规则

参数说明：

ruledel	根据名称删除某安全规则。
name	指定规则名称。
string	字符串，输入要删除的规则名称。

使用说明：

只有当安全规则未被引用时才能正确删除。

实例：

**删除安全规则 kk。

onlineuser deleteuser name *test1* **type** *common* <cr>

**删除被引用的安全规则 os_winxp

sec-policy ruledel name *os_winxp*

由于该规则属于某个规则组，则执行结果为：error -23401 : rule refer error

sec-policy rulemodify name <*string*> **check-type** < regkey|file|ver|process|port| service| system-packet| os |device|virus > [**check-os** <all|win95|win98|winnt|win2000|winxp|win2003|vista| 2008|win7>] [**check-item** <*string*>] **[check-value** <*string*>] [**operate-code** [eq|ge|le|contain] [**description** <*string*>]

命令描述：

本命令用于修改安全规则属性。

参数说明：

rulemodify	修改安全规则属性
name	输入规则名称
string	字符串，输入规则名。
check-type	必选项，指定检测项目的类型
regkey|file|ver|process|port| service| system-packet| os |device|virus	选择检测项目类型，可选项分别对应：注册表项、文件状态、文件版本、进程、端口、服务、系统补丁、操作系统、设备、病毒。
check-os	可选项，仅当检测项目的类型选择“os”时需要设置该项。用于指定检测的操作系统的类型。 说明：

	对于检测类型“check-type”不是“操作系统”的规则起作用，其作用是如果被检测机和“check－os”设置的系统不同则该条规则会被忽略
all|win95|win98|winnt|win2000|winxp|win2003|vista|2008|win7	可选项分别对应“所有”、“WIN95”、“WIN98”、“WINNT”、“WIN2000”、“WINXP”、“WIN2003”、“VISTA”、“2008”或 Windows 7。
check-value	可选项，设置对客户端主机的详细检测值。设置不同的“检测类型”时，有不同的设置项目。
string	1）当检测类型选择“系统补丁”时，可选项为“SP1”、“SP2”、“SP3”、“SP4”，检测客户端主机的系统大补丁或系统小补丁是否大于等于或等于检测值。 2）当检测类型选择“操作系统”时，可选项为“是”或“不是”，检测客户端主机的操作系统是否为“检测项”处设定的值。
check-item	设置对客户端主机的详细检查项目。
string	设置不同的“检测类型”时，可选项不同： 1）当检测类型选择“系统补丁”时，可选项为“系统大补丁”、“系统小补丁”。 2）当检测类型选择“操作系统”时，可选项为“WIN95”、“WIN98”、“WINNT”、“WIN2000”、“WINXP”、“WIN2003”、“VISTA”或“2008”。
operate-code	检测类型选择“注册表项”和“文件版本”时需要设置该项。
eq|ge|le|contain	相等/大于等于/小于等于/包含
description	添加对该规则必要的描述信息
string	字符串

实例：

**修改名称为“os_check”的规则，用于检查主机的操作系统是否为 Windows98。

sec-policy rulemodify name *os_check* **check-type** *os* **check-item** *WIN98* <cr>

sec-policy rulenum<cr>

命令描述：

本命令用于显示一共有多少条安全规则。

sec-policy ruleshow [**name** <*string*>] [**begin** <*number*>] [**end** <*number*>]

命令描述：

本命令用于查看安全规则信息。

参数说明：

ruleshow	查看安全规则信息

name	可选项，指定查看名称
string	字符串，输入规则名。
begin	指定开始序号。
number	数值
end	指定结束序号
number	数值

使用说明：

不指定任何参数时显示所有规则信息。

实例：

**查看名称为“kk”的规则属性。

sec-policy ruleshow name *kk* <cr>

server

设置外部认证服务器的相关信息。

Server add name <*string1*> **protocol** <radius|tacacs|securid |ldap|tp > **server-addr** <*ipaddress*> **port** <*number*> [**shared_sceret** <*string3*>] [**server_dn** <*string4*>] [**client-addr** <*ipaddress*>] **[mode** <chap|pap>][**admin-name** <*string4*>] [**naming-attribute** < string>] [**scope** <onelevel|subtree>] [**server-type** < ad|sun|novell|other>] [**time-out** < *number*>]

命令描述：

本命令用于添加认证服务器，认证服务器类型包括： Radius、TACACS、LDAP、域认证和 SecurID 认证。

参数说明：

add	添加认证服务器。
name	指定认证服务器的名字。
string1	字符串类型，输入认证服务器的名称。
protocol	指定使用的认证协议。
radius|tacacs|securid|ldap	输入认证使用的协议类型，包括：RADIUS 认证、TACACS 认证、SecurID 认证、LDAP 认证。
server-addr	指定认证服务器的 IP 地址。该参数值必须设置。
ipaddress	标准 IP 地址字符串。
port	指定认证服务器的服务端口。该参数值必须设置。
number	数值类型，取值范围为：0~65535。
shared_sceret	指定共享密钥。

	说明： 当认证类型为 RADIUS、TACACS、SecuID 时，该参数值必须设置；对于其它类型的认证，不能设置该参数。
string3	字符串，输入认证服务器端的共享密钥。
server_dn	可选项，设定服务器域名。 说明： 当认证类型为 LDAP 和 AD 时，该参数值必须设置；对于其它类型的认证，不能设置该参数。
string4	字符串，例如服务器域名为：www.topsec.com.cn，则该参数的输入格式为“dc=topsec,dc=com,dc=cn” 。
client-addr	可选项，设置认证客户端地址
ipaddress	仅当认证协议为 Radius 时需要设置该项，表示安全网关与 Radius 服务器连接的出接口的 IP 地址。
mode	指 Radius 认证协议的认证方法，只有认证协议选择“Radius”时需要设置该项。
chap|pap	可选值为 PAP、CHAP。
admin-name	设置 LDAP 查询用户名
string4	字符串
naming-attribute	设置 LDAP 命名属性
string	字符串
scope	设置 LDAP 查找范围
onelevel|subtree	选择查找范围
server-type	设置 LDAP 服务器类型
ad|sun|novell|other	可选项为 ad、sun、novell 或其他类型
time-out	设置保活时间(5~180)，缺省为 5 秒。
number	数值

使用说明：

各种服务器均有缺省认证端口，RADIUS 的缺省认证端口为“1812”；TACACS 的缺省认证端口为“49”；LDAP 的缺省认证端口为“389”；域认证的缺省认证端口为“389”；SecurID 的缺省认证端口为“5050”。

实例：

** 添加一个 Radius 认证服务器，认证服务器名称为“RADIUS”；认证类型为“radius”；认证服务器地址为“192.168.83.231”；认证服务器端口为“1812”；共享密钥为“topsec”；保活超时为“100s”。

server add name *radius* **protocol** radius **timeout** *100* **server_addr** *192.168.83.231* **port** *1812* **shared_sceret** *topsec*

server modify name <*sername*> **protocol** <radius|tacacs|securid |ldap > **server-addr**

<*ipaddress*> **port** <*number*> [**shared_sceret** <*string3*>] [**server_dn** <*string4*>] [**client-addr** <*ipaddress*>] [**mode** <chap|pap>][**admin-name** <*string4*>] [**naming-attribute** < string>] [**scope** <onelevel|subtree>] [**server-type** < ad|sun|novell|other>][**time-out** < *number*>]

命令描述：

本命令用于修改认证服务器参数

参数说明：

modify	修改认证服务器。
name	指定认证服务器的名字。
string1	字符串类型，输入认证服务器的名称。
protocol	指定使用的认证协议。
radius|tacacs|securid|ldap	输入认证使用的协议类型，包括：RADIUS 认证、TACACS 认证、SecurID 认证、LDAP 认证。
server-addr	指定认证服务器的 IP 地址。该参数值必须设置。
ipaddress	标准 IP 地址字符串。
port	指定认证服务器的服务端口。该参数值必须设置。
number	数值类型，取值范围为：0~65535。
shared_sceret	指定共享密钥。 说明： 当认证类型为 RADIUS、TACACS、SecuID 时，该参数值必须设置；对于其它类型的认证，不能设置该参数。
string3	字符串，输入认证服务器端的共享密钥。
server_dn	可选项，设定服务器域名。 说明： 当认证类型为 LDAP 和 AD 时，该参数值必须设置；对于其它类型的认证，不能设置该参数。
string4	字符串，例如服务器域名为：www.topsec.com.cn，则该参数的输入格式为“dc=topsec,dc=com,dc=cn” 。
client-addr	可选项，设置认证客户端地址
ipaddress	仅当认证协议为 Radius 时需要设置该项，表示安全网关与 Radius 服务器连接的出接口的 IP 地址。
mode	指 Radius 认证协议的认证方法，只有认证协议选择“Radius”时需要设置该项。
chap|pap	可选值为 PAP、CHAP。
admin-name	设置 LDAP 查询用户名
string4	字符串
naming-attribute	设置 LDAP 命名属性
string	字符串
scope	设置 LDAP 查找范围
onelevel|subtree	选择查找范围
server-type	设置 LDAP 服务器类型
ad|sun|novell|other	可选项为 ad、sun、novell 或其他类型
time-out	设置保活时间(5~180)，缺省为 5 秒。
number	数值

实例：

** 将名称为“RADIUS”的 Radius 服务器的认证服务器地址修改为“192.168.83.234”；认证服务器端口修改为“1912”；共享密钥修改为“talent”。

server modify name *RADIUS* **server_addr** *192.168.83.234* **port** *1912* **shared_secret** *talent*

server delete name <*string*>

命令描述：

本命令用于删除指定认证服务器的信息。

参数说明：

delete	删除某个认证服务器的信息。
name	指定认证服务器的名字。
string	字符串，输入认证服务器的名字。

实例：

** 删除名称为“RADIUS”的认证服务器的信息。

server delete name *RADIUS*

server show [**name** <*string*>][**protocol** < radius|tacacs|securid|ldap >]

命令描述：

本命令用于查看指定认证服务器的信息。

参数说明：

show	查看认证服务器的信息。
name	可选项，指定认证服务器的名称。
string	字符串，输入认证服务器的名称。
protocol	可选项，指定认证服务器使用的协议
radius|tacacs|securid|ldap	认证使用的协议类型，包括：RADIUS 认证、TACACS 认证、SecurID 认证、LDAP 认证和域认证。

使用说明：

指定参数时，显示指定认证服务器的信息；不指定任何参数时，显示所有认证服务器的信息。

实例：

** 查看名称为“RADIUS”的认证服务器的信息。

server show name *RADIUS*

** 查看所有认证服务器的信息。

server show<cr>

server clean [**protocol** < radius|tacacs|securid| ldap >]

命令描述：

本命令用于清空所有或指定协议的认证服务器的配置信息。

参数说明：

clean	清空认证服务器的信息。
protocol	可选项，指定认证服务器使用的协议
radius|tacacs|securid| ldap	认证使用的协议类型，包括：RADIUS 认证、TACACS 认证、SecurID 认证、LDAP 认证。

使用说明：

指定参数时，清空指定协议的认证服务器的信息；不指定任何参数时，清空所有认证服务器的信息。

实例：

** 清空协议为“radius”的认证服务器的信息。

server clean protocol *radius*

** 清空所有认证服务器的信息。

server clean<cr>

server-sync

LDAP 服务器同步配置信息

server-sync modify server-name <*string*> **auto-sync**<yes|no> **time-lag** <*number*> **sync-user** <yes|no> **hwidbind** <yes|no> **multi-login** <yes|no> **user-type** <ext|ext-cert> **user-filter** <*string*> **sync-group** <yes|no> **group-filter** <*string*> **group-attr-name** <*string*>

命令描述：

本命令用于修改 LDAP 服务器同步配置信息。

参数说明：

modify	修改 LDAP 服务器同步配置信息
server-name	认证服务器名
string	字符串

auto-sync	是否自动同步
yes|no	是/否
time-lag	设置同步时间间隔(1~180)天，缺省为 180 天
number	(1~180)天，缺省为 180 天
sync-user	是否同步帐号
yes|no	是/否
hwidbind	特征码绑定
yes|no	是/否
multi-login	多点登陆
yes|no	是/否
user-type	设置用户的认证方式。
ext|ext-cert	ext 是外部口令认证 ext-cert 是外部口令+证书
user-filter	用户过滤条件
string	字符串
sync-group	同步组
yes|no	是/否
group-filter	用户组过滤条件
string	字符串
group-attr-name	组属性名，缺省是:memberOf。
string	字符串

server-sync show server-name <*string*>

命令描述：

查看 LDAP 服务器同步配置信息。

参数说明：

show	查看 LDAP 服务器同步配置信息
server-name	认证服务器名
string	字符串

server-sync sync server-name<*string*>

命令描述：

同步 LDAP 服务器信息。

参数说明：

sync	同步 LDAP 服务器信息
server-name	认证服务器名
string	字符串

sms

短信认证服务器配置

sms modify server-addr <*ipaddress*> **port** < *port*> **shared-secret** <*string*> **id <***number***>**

[**time-out <***number***>**] [**outdate <***number***>**]

命令描述：

修改短信认证服务器配置。只有当 SMS 发送模式设置为 server 时才需要设置该项。

参数说明：

modify	修改 SMS 服务器配置
server-addr	短信认证服务器地址
ipaddress	IP 地址字符串
port	设置短信网关发送短信的端口
port	端口号，必须与短信网关设置一致。
shared-secret	认证共享通行串
string	字符串，必须与短信网关设置一致。
id	网关 ID 值
number	数值，必须与短信网关设置一致。
time-out	认证超时值
number	数值
outdate	设置发送短信数目达到此处设定的值后，密钥需要重新协商
number	数值

sms show<cr>

命令描述：

查看 SMS 服务器配置。

sms clean<cr>

命令描述：

清空 SMS 服务器配置。

sms sms-type mode <server|local>

命令描述：

根据短信网关是否直接连接安全网关，设置 SMS 发送模式。

参数说明：

sms-type mode	设置 SMS 发送模式
server|local	Server 表示短信网关连接在 PC 上，PC 再和安全网关连接； Local 表示短信网关直接连接在安全网关的 USB 口。

sms auth<cr>

命令描述：

SMS 向服务器进行认证。

sms test phone <*string*> **seqnum** < *number*>

命令描述：

SMS 发送测试。

参数说明：

phone	设置接收信息手机
string	输入电话号码
seqnum	设置发送的信息
number	数值

user

用户信息配置及管理

user add name < *string*> [**pwdtype** < plain|cipher>] **passwd** < *string* > **role** < *string* > [**multi_login** <yes|no>] [**status** <locked|unlocked>] [**description**< *string* >][**mail**< *string* >] [**phone**< *number*>] [**external_attr**< yes|no >][**cert_auth**< yes|no >] [**passwd_auth** < yes|no >][**hwidbind** < yes|no >] [**hwid** < *string*>] [**version-control** <default|define|nouse>][**version** <standard|ukey |limit |secure |ukey_limit| ukey_secure>] [**vip**< *ipaddress* >] [**uip**< *ipaddress* >] [**uipmask**< *string* >] [**starttime**< *string* >] [**endtime**< *string* >] [**encrypted-pwd** < *string* >] [**need-chg-pwd** < yes|no|>] [**forbid-chg-pwd** <yes|no|>] [**pwd-timeout** < string>] **style** < default|simple>

命令描述：

本命令用于添加用户信息。

参数说明：

add	添加用户
name	指定用户名称
string	字符串，可以是中文字符、英文字母，下划线、横杠、数字的随意组合。最长 31 个字符。如果使用了“证书认证”、“本地口令+证书认证”或“外地口令+证书认证”的认证方式，则需要添加一个与证书 SUBJECT 域名称相同的用户。
pwd_type	设置密码类型
plain|cipher	明文、密文
passwd	设定用户密码
string	最少 6 个字符，最长 31 个字符。
role	设置该用户所属的角色，则用户具有该角色的访问控制权限。当一个用户属于若干个角色时，“所属角色”中角色的前后排列顺序决定授予用户权限的顺序。一旦发现匹配用户的角色，设备将停止匹配检查，并根据最先匹配的那一个角色对用户进行授权。
string	角色名，可以输入多个，用引号括起来，并用逗号分隔。
multi_login	可选项，设置是否允许多点登录，对于 SSL VPN 用户，设置是否允许多个人使用同一帐号在不同地点登录。 说明： 当设备不包含 SSL VPN 模块时，不会显示该选项。
yes|no	是/否
status	设置该用户帐号是否允许使用，只有当选择“unlocked”时才可能允许该用户登录设备进而访问内网资源，否则即使权限允许该用户帐号也禁止使用。
locked|unlocked	启用/停止
Description	可选项，输入用户描述信息。
string	字符串
mail	指认证用户的电子邮件地址信息，为可选项。
string	邮箱地址字符串。
phone	可选项，设置该用户的手机号码。
string	字符串
external_attr	为可选项。设置外部认证属性
string	字符串
cert_auth	是否需要证书认证
yes|no	是/否
passwd_auth	需要密码认证
yes|no	是/否
hwidbind	为可选项。是否使用硬件特征码绑定功能。
yes|no	启用/关闭
hwid	可选项，设置硬件特征码。只有启用“硬件特征码绑定控制”时才可添加。

string	字符串，输入硬件特征码，32 位 16 进制数。
version-control	为可选项。设置是否对 VRC 客户端采用的版本类型进行控制。
default|define|nouse	默认、自定义、不控制。
version	为可选项。选择 VRC 客户端使用的版本号，只有在 **version-control** 处选择“define”时才需要设置该项。
standard|ukey |limit |secure |ukey_limit| ukey_secure	目前支持的客户端版本类型有：标准版、安全版、限制版、UKEY、安全版＋UKEY、限制版＋UKEY。
vip	为可选项。设置是否对该 VRC 用户上线时的虚拟 IP 地址进行严格控制。
string	IP 地址字符串
uip	为可选项。设置是否指限制用户登录设备的 IP 地址及其掩码。
string	IP 地址字符串，可以限定具体 IP 地址或输入子网地址。
uipmask	为可选项。设置是否指限制用户登录设备的 IP 地址及其掩码。
string	子网掩码字符串
starttime	为可选项。设置该用户生效时间。
string	格式为:'2006-01-01 22:00:00'
endtime	为可选项。设置该用户到期时间。
string	格式为:'2006-01-01 22:00:00'
encrypted-pwd	设置加密密钥
string	字符串
need-chg-pwd	设置下次登陆是否修改密码
yes|no	是/否
forbid-chg-pwd	是否禁止修改密码
yes|no	是/否
pwd-timeout	设置密码过期时间,时间
string	字符串，格式为：'2006-01-01 09:05:00'
style	设置 SSL VPN 界面风格
default|simple	缺省风格，简单风格

使用说明：

根据用户类型是安全网关用户、VRC 用户和 SSLVPN 用户需要设置不同的选项。

实例：

** 添加用户 test，采用密码认证方式，口令为 11111111，其属于角色 gg。

user add name *test* **passwd_auth** on **passwd** *11111111* **role** *gg*

user modify name <*string*>[**pwdtype** < plain|cipher|>] **passwd** < *string* > **role** < *string* >

[**multi_login** <yes|no>] [**status** <locked|unlocked>] [**description**< *string* >][**mail**< *string* >]

[**phone**< *number*>] [**external_attr**< yes|no >][**cert_auth**< yes|no >] [**passwd_auth** < yes|no

>][**hwidbind** < yes|no >] [**hwid** < *string*>] [**version-control** <default|define|nouse>][**version** <standard|ukey |limit |secure |ukey_limit| ukey_secure>] [**vip**< *ipaddress* >] [**uip**< *ipaddress* >] [**uipmask**< *string* >] [**starttime**< *string* >] [**endtime**< *string* >] [**encrypted-pwd** < *string* >] [**need-chg-pwd** < yes|no>] [**forbid-chg-pwd** <yes|no>] [**pwd-timeout** < string>][**style** < default|simple]

命令描述：

本命令用于修改用户信息。

参数说明：

modify	修改用户
name	指定用户名称
string	字符串，可以是中文字符、英文字母，下划线、横杠、数字的随意组合。最长 31 个字符。如果使用了“证书认证”、“本地口令+证书认证”或“外地口令+证书认证”的认证方式，则需要添加一个与证书 SUBJECT 域名称相同的用户。
pwd_type	设置密码类型
plain|cipher	明文、密文
passwd	设定用户密码
string	最少 6 个字符，最长 31 个字符。
role	设置该用户所属的角色，则用户具有该角色的访问控制权限。当一个用户属于若干个角色时，“所属角色”中角色的前后排列顺序决定授予用户权限的顺序。一旦发现匹配用户的角色，设备将停止匹配检查，并根据最先匹配的那一个角色对用户进行授权。
string	角色名，可以输入多个，用引号括起来，并用逗号分隔。
multi_login	可选项，设置是否允许多点登录，对于 SSL VPN 用户，设置是否允许多个人使用同一帐号在不同地点登录。 说明： 当设备不包含 SSL VPN 模块时，不会显示该选项。
yes|no	是/否
status	设置该用户帐号是否允许使用，只有当选择“unlocked”时才可能允许该用户登录设备进而访问内网资源，否则即使权限允许该用户帐号也禁止使用。
locked|unlocked	启用/停止
Description	可选项，输入用户描述信息。
string	字符串
mail	指认证用户的电子邮件地址信息，为可选项。
string	邮箱地址字符串。
phone	可选项，设置该用户的手机号码。
string	字符串
external_attr	为可选项。设置外部认证属性
string	字符串

cert_auth	是否需要证书认证
yes|no	是/否
passwd_auth	需要密码认证
yes|no	是/否
hwidbind	为可选项。是否使用硬件特征码绑定功能。
yes|no	启用/关闭
hwid	可选项，设置硬件特征码。只有启用“硬件特征码绑定控制”时才可添加。
string	字符串，输入硬件特征码，32 位 16 进制数。
version-control	为可选项。设置是否对 VRC 客户端采用的版本类型进行控制。
default|define|nouse	默认、自定义、不控制。
version	为可选项。选择 VRC 客户端使用的版本号，只有在 **version-control** 处选择“define”时才需要设置该项。
standard|ukey |limit |secure |ukey_limit| ukey_secure	目前支持的客户端版本类型有：标准版、安全版、限制版、UKEY、安全版＋UKEY、限制版＋UKEY。
vip	为可选项。设置是否对该 VRC 用户上线时的虚拟 IP 地址进行严格控制。
string	IP 地址字符串
uip	为可选项。设置是否指限制用户登录设备的 IP 地址及其掩码。
string	IP 地址字符串，可以限定具体 IP 地址或输入子网地址。
uipmask	为可选项。设置是否指限制用户登录设备的 IP 地址及其掩码。
string	子网掩码字符串
starttime	为可选项。设置该用户生效时间。
string	格式为:'2006-01-01 22:00:00'
endtime	为可选项。设置该用户到期时间。
string	格式为:'2006-01-01 22:00:00'
encrypted-pwd	设置加密密钥
string	字符串
need-chg-pwd	设置下次登陆是否修改密码
yes|no	是/否
forbid-chg-pwd	是否禁止修改密码
yes|no	是/否
pwd-timeout	设置密码过期时间,时间
string	字符串，格式为：'2006-01-01 09:05:00'
style	设置 SSL VPN 界面风格
default|simple	缺省风格，简单风格

user delete name <*string*>

命令描述：

本命令用于删除用户信息。

参数说明：

delete	删除用户信息
name	指定用户名称
string	字符串

user show [**name** <*string1*>][**from** <*number1*>][**to**<*number2*>][**by-admin-name** < *string2*>]

命令描述：

本命令用于查看用户信息。

参数说明：

show	查看用户信息
name	可选项，指定用户名称
string1	字符串
from	可选项，指定开始用户序号。
number1	数值
to	可选项，指定结束用户序号。
number2	数值
By-admin-name	可选项，分级管理员名字
string2	字符串

user clean <cr>

命令描述：

本命令用于清空所有用户信息。

user lock name <*string*>

命令描述：

本命令用于锁定用户。

参数说明：

lock	锁定用户
name	指定用户名称
string	字符串

user unlock name <*string*>

命令描述：

本命令用于解锁用户。

参数说明：

unlock	锁定用户
name	指定用户名称

string	字符串

user search name <*string*> **key-word** <name| mail| phone| description| status| multi-login| admin-namefullname|mail|status|multi_login|phone| external > **key-value** <*string*> [**begin**<*number*>][**end**<*number*>]

命令描述：

本命令用于查找用户。

参数说明：

search	查找用户
name	指定用户名称
string	字符串
Key-word	指定根据哪个关键字查找
name|description|mail|status|multi_login|phonename| mail| phone| description| status| multi-login| admin-name	用户名、描述信息、邮箱、用户状态、是否允许多点登录、电话。
Key-value	指定关键字
string	字符串

user clearrole username <*string*>

命令描述：

本命令用于清除用户所有角色信息。

参数说明：

clearrole	清除用户所有角色信息
username	指定用户名称
string	字符串

user export <cr>

命令描述：

本命令用于导出所有用户信息。

user num <cr>

命令描述：

本命令用于获取用户数目。

user show-refer name <*string*>

命令描述：

本命令用于查看用户被引用的信息。

参数说明：

show-refer	查看用户信息
name	指定查看用户名
string	字符串，输入用户名。

实例：

**查看名称为“lisi”的用户被引用的情况。

user show-refer name *lisi* <cr>

version

查看用户认证模块的版本信息。

version< cr >]

命令描述：

本命令用于查看用户认证模块的版本信息。

ANTI-SPAM

本模块用于设置安全网关的反垃圾邮件策略。安全网关设备通过对发件人的邮件地址及 IP 地址黑白名单检查，阻止垃圾邮件进入内部网络。

当一个邮件地址同时存在于邮件地址黑名单和邮件地址白名单时，白名单优先级较高，则邮件不会被作为垃圾邮件处理，直接放行。

进入本命令模块操作如下：

anti-spam <cr>

退出本命令模块操作如下：

end <cr>

CLI 管理员登录安全网关进入本命令模块后，可以执行相应的组件管理命令。下面将详细描述本命令模块下的所有组件管理命令。命令的实例输入格式将按已经

进入本命令模块书写。

下一级命令列表

命令	功能
blacklist	设置邮件地址及 IP 地址黑名单
greylist	灰名单设置
rbl	反垃圾邮件实时黑名单配置
reset	恢复出厂配置
show	查看反垃圾邮件设置
statistic	反垃圾邮件统计功能设置
whitlist	设置邮件地址及 IP 地址白名单

blacklist

设置邮件地址及 IP 地址黑名单。系统对接收到的邮件的发件人邮件地址和 IP 地址进行检查，如果命中邮件或 IP 地址黑名单，则被确定为垃圾邮件，则进行垃圾邮件相应的处理。

blacklist email-address clean <cr>

命令描述：

本命令用于清空所有邮件地址黑名单的信息。

blacklist email-address delete index <*number*>

命令描述：

本命令用于根据邮件地址序号删除黑名单的信息。

参数说明：

delete	删除邮件地址黑名单
index	指定序号
number	数值

blacklist email-address add <*string*>

命令描述：

本命令用于添加邮件地址到黑名单。

参数说明：

add	添加邮件地址到黑名单
number	Email 地址格式字符串

blacklist ip-address add ip<*string*>

命令描述：

本命令用于添加 IP 地址到黑名单。

参数说明：

add ip	添加 IP 地址到黑名单
string	IP 地址格式字符串

blacklist ip-address add subnet<*string*>

命令描述：

本命令用于添加子网地址到黑名单。

参数说明：

add subnet	添加子网地址到黑名单
string	子网掩码地址格式字符串，格式为：a.b.c.d/e。

blacklist ip-address clean <cr>

命令描述：

本命令用于清除所有 IP 地址黑名单的信息。

blacklist ip-address delete <*string*>

命令描述：

本命令用于根据 IP 地址删除黑名单的信息。

参数说明：

delete	删除邮件地址黑名单
string	IP 地址或子网掩码格式字符串

greylist

灰名单设置

greylist reset <cr>

命令描述：

重置灰名单设置。

greylist timeset repeat <*number*>

命令描述：

设置邮件最小重发间隔，单位：分

greylist timeset waittime <*number*>

命令描述：

设置等待邮件重发最长时间，单位：小时

greylist timeset greylisttime <*number*>

命令描述：

设置灰名单保留时间，单位：天

greylist workingenable [on|off]

命令描述：

灰名单工作模式是否开启。

greylist workingset hour1 <*number1*> **hour2** < *number 2*> **min1** < *number 3*> **min2** < *number 4*>

命令描述：

灰名单工作时间设置。

参数说明：

workingset	灰名单工作时间设置
hour1	灰名单工作起始小时
number1	数值，起始小时
hour2	灰名单工作结束小时
number2	数值，结束小时
min1	灰名单工作起始分钟
number3	数值，起始分钟数
min2	灰名单工作结束分钟
number4	数值，结束分钟数

policy

反垃圾邮件策略设置

policy add name <*string*> **white-email-list** <on|off> **black-email-list** < on|off> **white-ip-list** <on|off> **black-ip-list** <on|off> **rbl** <on|off> **rdns** <on|off> **greylist** <on|off> **log** <on|off> **spam-deal-rbl** <block|record> **spam-deal-rdns** <block|record>

命令描述：

添加反垃圾邮件策略

参数说明：

add	添加反垃圾邮件策略
name	输入名称
string	字符串
white-email-list	设置是否邮件地址白名单
on|off	启用/禁用
black-email-list	设置是否启用邮件地址黑名单
on|off	启用/禁用
white-ip-list	设置是否启用 IP 地址白名单
on|off	启用/禁用
black-ip-list	设置是否启用 IP 地址黑名单
on|off	启用/禁用
rbl	设置是否启用实时黑名单
on|off	启用/禁用
rdns	设置是否启用反向 DNS 查询
on|off	启用/禁用
greylist	设置是否启用灰名单
on|off	启用/禁用
log	设置是否记录日志信息
on|off	启用/禁用
spam-deal-rbl	设置实时黑名单模块对垃圾邮件的处理方式
block|record	阻断垃圾邮件/记录日志
spam-deal-rdns	设置反向 DNS 模块对垃圾邮件的处理方式
block|record	阻断垃圾邮件/记录日志

policy modify name <*string*> **white-email-list** <on|off> **black-email-list** < on|off> **white-ip-list** <on|off> **black-ip-list** <on|off> **rbl** <on|off> **rdns** <on|off> **greylist** <on|off> **log** <on|off> **spam-deal-rbl** <block|record> **spam-deal-rdns** <block|record>

命令描述：

修改反垃圾邮件策略

参数说明：

modify	修改反垃圾邮件策略
name	输入名称
string	字符串
white-email-list	设置是否邮件地址白名单
on|off	启用/禁用
black-email-list	设置是否启用邮件地址黑名单
on|off	启用/禁用
white-ip-list	设置是否启用 IP 地址白名单
on|off	启用/禁用
black-ip-list	设置是否启用 IP 地址黑名单
on|off	启用/禁用
rbl	设置是否启用实时黑名单
on|off	启用/禁用
rdns	设置是否启用反向 DNS 查询
on|off	启用/禁用
greylist	设置是否启用灰名单
on|off	启用/禁用
log	设置是否记录日志信息
on|off	启用/禁用
spam-deal-rbl	设置实时黑名单模块对垃圾邮件的处理方式
block|record	阻断垃圾邮件/记录日志
spam-deal-rdns	设置反向 DNS 模块对垃圾邮件的处理方式
block|record	阻断垃圾邮件/记录日志

policy delete name <*string*>

命令描述：

删除反垃圾邮件策略

参数说明：

delete	删除反垃圾邮件策略
name	输入名称
string	字符串

policy clean<cr>

命令描述：

删除反垃圾邮件策略

policy show<cr>

命令描述：

查看反垃圾邮件策略

rbl

实时黑名单设置

rbl server add name <*string*> **server-addr** <*string*> **enable** <on|off>

命令描述：

添加 RBL 服务器

参数说明：

add	添加 RBL 服务器
name	输入名称
string	字符串
server-addr	输入服务器地址
string	IP 地址
enable	设置是否启用该服务器
on|off	启用/禁用

rbl server modify name <*string*> **enable** <on|off>

命令描述：

修改 RBL 服务器参数

参数说明：

modify	修改 RBL 服务器参数
name	输入名称
string	字符串
enable	设置是否启用该服务器
on|off	启用/禁用

rbl server delete name <*string*>

命令描述：

删除 RBL 服务器

参数说明：

delete	删除 RBL 服务器

name	输入名称
string	字符串

rbl server clean<cr>

命令描述：

清空所有 RBL 服务器

rbl reset<cr>

命令描述：

实时黑名单恢复默认设置

rbl clean<cr>

命令描述：

清空所有实时黑名单设置

reset

恢复反垃圾邮件默认设置

show

查看反垃圾邮件设置

statistic

反垃圾邮件统计功能设置

statistic show <cr>

命令描述：

查看反垃圾邮件统计结果

statistic clean<cr>

命令描述：

清空反垃圾邮件统计结果

whitelist

设置邮件地址及 IP 地址白名单。系统对接收到的邮件的发件人邮件地址和 IP 地址进行检查，如果命中邮件或 IP 地址地址白名单，则此处放行，到下一步做关键字匹配。

whitelist email-address clean <cr>

命令描述：

本命令用于清空所有邮件地址白名单的信息。

whitelist email-address delete index <*number*>

命令描述：

本命令用于根据邮件地址序号删除白名单的信息。

参数说明：

delete	删除邮件地址白名单
index	指定序号
number	数值

whitelist email-address add <*string*>

命令描述：

本命令用于添加邮件地址到白名单。

参数说明：

add	添加邮件地址到白名单
number	Email 地址格式字符串

whitelist ip-address add ip<*string*>

命令描述：

本命令用于添加 IP 地址到白名单。

参数说明：

add ip	添加 IP 地址到白名单
string	IP 地址格式字符串

whitelist ip-address add subnet<*string*>

命令描述：

本命令用于添加子网地址到白名单。

参数说明：

add subnet	添加子网地址到白名单
string	子网掩码地址格式字符串，格式为：a.b.c.d/e。

whitelist ip-address clean <cr>

命令描述：

本命令用于清除所有 IP 地址白名单的信息。

whitelist ip-address delete <*string*>

命令描述：

本命令用于根据 IP 地址删除白名单的信息。

参数说明：

delete	删除邮件地址白名单
string	IP 地址或子网掩码格式字符串

AR

应用程序识别参数设置

下一级命令列表

命令	功能
account	帐号控制
apps	应用层协议的信息
custom	自定义应用层协议
dev	统计开关
dfi	深度流量统计开关

dfi-params	DFI 参数
disk	磁盘是否可用
group_quota	监控应用协议组
interface_quota	监控接口流量
ip-virus	ip 的病毒统计信息
ip-virus-detail	某一 ip 感染病毒详细信息
max-session	最大连接数
monitor-switch	显示流量监控设置
monitorhost	监控主机控制
net-quota	显示设置的流量和连接配额
other-quota	其他流量百分比设置
policy	应用层协议策略
quota	配额重置
rules	规则库升级配置
stat-object	显示监控对象流量信息
stat-object-detail	显示监控对象详细信息
tcp-quota	tcp 流量百分比设置
udp-quota	udp 流量百分比设置
version	查看 AR 版本
virus	查看病毒统计信息
virus-domain	查看病毒来源统计信息
virus-group	查看病毒种类统计信息
virus-ip-top	查看感染某个病毒的 ip 排名
virus-start-time	设置病毒统计开始时间

account

对 QQ 和 MSN 两种即时通讯软件的帐号控制功能

account add name <*string*> **type** <qq|msn> **accounts** <*string*> **access** <deny|permit> **enable** <yes|no>

命令描述：

添加帐号控制策略。

参数说明：

add	添加帐号控制策略
name	帐号控制的名字
string	字符串
type	指定协议类型
qq|msn	只支持 qq 或者 msn
accounts	要控制的帐号列表
string	字符串，写在一对单引号中，空格分隔。
access	设置权限

deny|permit	deny 表示阻止，permit 表示允许
enable	是否启用该规则
yes|no	Yes 表示启用，no 表示禁用。

account modify name <*string*> **type** <qq|msn> [**accounts** <*string*>] [**access** <deny|permit>]

[**enable** <yes|no>]

命令描述：

修改帐号控制策略。

参数说明：

modify	修改帐号控制策略
name	帐号控制的名字
string	字符串
type	指定协议类型
qq|msn	只支持 qq 或者 msn
accounts	要控制的帐号列表
string	字符串，写在一对单引号中，空格分隔。
access	设置权限
deny|permit	deny 表示阻止，permit 表示允许
enable	是否启用
yes|no	Yes 表示启用，no 表示禁用。

account delete name <*string*>

命令描述：

删除帐号控制策略。

参数说明：

delete	删除帐号控制策略
name	帐号控制的名字
string	字符串

account clean<cr>

命令描述：

清空所有帐号控制策略。

account show<cr>

命令描述：

查看所有帐号控制策略。

apps

应用层协议信息

apps total<cr>

命令描述：

本命令用于显示所有应用层协议的总数。

ar apps show<cr>

命令描述：

本命令用于显示所有应用层协议的详细信息。

custom

自定义应用程序类型，用户要设置传输层协议类型及端口号

custom add name <*string*> **ports** <*string*>

命令描述：

添加自定义应用协议类型。

参数说明：

add	添加自定义应用协议类型
name	自定义应用层协议的名字
string	字符串
ports	添加端口列表
string	用一对单引号括起来，空格分隔。每一项的格式是“协议|端口”，其中协议只支持 tcp 和 udp 两种。

custom modify name <*string*> [**ports** <*string*>]

命令描述：

修改自定义应用协议类型。

参数说明：

add	修改自定义应用协议类型
name	自定义应用层协议的名字
string	字符串
ports	指定协议端口列表
string	用一对单引号括起来，空格分隔。每一项的格式是“协议|端口”，其中协议只支持 tcp 和 udp 两种。

custom delete name <*string*>

命令描述：

删除自定义应用协议类型。

参数说明：

delete	删除自定义应用协议类型
name	自定义应用协议类型的名字
string	字符串

custom clean<cr>

命令描述：

清空所有自定义应用协议类型。

custom show<cr>

命令描述：

查看所有自定义应用协议类型。

dev

接口流量统计开关

dev statistic <on|off>

命令描述

设置是否开启接口流量统计开关

参数说明：

dev statistic	设置是否开启接口流量统计开关
on|off	On 开启，off 表示关闭。

dfi

设置是否打开 DFI 过滤开关

dfi <on|off>

命令描述：

设置是否打开 DFI 过滤开关

参数说明：

dfi	设置是否打开 DFI 过滤开关
on|off	打开、关闭

dfi show<cr>

命令描述：

查看是否打开 DFI 过滤开关

dfi-params

动态流检测参数设置

dfi-params set dst_num_limits < *string*> **activity** < *string*> **activity_limits** <*string*>

multithread_limits < *string*> **expires** < *string*> **monitor_timer** < *string*>

命令描述：

DFI 参数设置。

参数说明：

set	DFI 参数设置
dst_num_limits	连接的目的主机数限制
string	数值
activity	连接的活跃程度阀值
string	数值
activity_limits	超过活跃程度限制的连接数量
string	字符串
multithread_limits	多线程连接数的限制
string	数值
expires	设置动态策略的超时限制
string	数值，默认为 1800，单位为秒。
monitor_timer	检测时间间隔，每隔一定时间对被监测主机进行 DFI 特征

	检查。
string	数值，默认为 4，单位为秒。

dfi-params show <cr>

命令描述：

查看 DFI 参数设置

dfi-params reset <cr>

命令描述：

重置 DFI 参数设置

disk

设置是否有磁盘及是否可用的状态

disk set <on|off >

命令描述

设置状态表明设备是否有磁盘

参数说明：

disk set	设置状态表明设备是否有磁盘以及磁盘是否可用
on|off	on 表示有磁盘，off 表示没有

disk set <enable|disable>

命令描述

设置状态表明设备磁盘是否可用

参数说明：

disk set	设置状态表明设备磁盘是否可用
enable|disable	enable 表示磁盘可用，disable 表示不可用。

flow-log

AR 模块流量日志设置

flow-log set <on|off >

命令描述

设置是否记录流量日志

参数说明：

flow-log	设置是否记录流量日志
on|off	on 表示有记录，off 表示不记录

flow-log show <cr >

命令描述

显示流量日志设置

flow_log_interval

设置流量日志向 TP 服务器发送的时间间隔

flow_log_interval set <*number*>

命令描述

设置流量日志向 TP 服务器发送的时间间隔

参数说明：

flow-log_interval set	设置是否记录流量日志
number	时间间隔，以分钟为单位。

flow_log_interval show <cr>

命令描述

查看流量日志向 TP 服务器发送的时间间隔

group_quota

设置应用协议组的报警流量

group_quota set_flow name <*string*> **flow** <*number*>

命令描述

设置应用协议组的报警流量的阀值

参数说明：

group_quota set_flow	设置应用协议组的报警流量
name	要设置的协议组的名字，协议组名称可以通过 ar apps show 命令获取。
string	目前支持的是传统协议、股票交易、即时消息、流媒体、网络游戏、网络电话、网络电视、p2p 下载、反动软件、其他流量、自定义协议
flow	设置各个协议的流量报警阀值
number	数值

group_quota set_session name <*string*> **session** <*number*>

命令描述

设置应用协议组的报警连接数的阀值

参数说明：

group_quota set_session	设置应用协议组的报警连接数
name	要设置的协议组的名字，协议组名称可以通过 ar apps show 命令获取。
string	目前支持的是传统协议、股票交易、即时消息、流媒体、网络游戏、网络电话、网络电视、p2p 下载、反动软件、其他流量、自定义协议
session	设置各个协议的报警连接数
number	数值

group_quota show<cr>

显示所有应用协议组报警的阀值配置

interface_quota

设置接口流量报警阀值

interface_quota set name <*string*> **value** <*number*>

命令描述：

为指定接口设定报警流量阀值

参数说明：

interface_quota set	设置指定接口设定报警流量阀值
name	设置的接口名
string	字符串
value	设置接口的报警流量阀值
number	数值

interface_quota show<cr>

查看各个接口设定的报警流量阀值

ip-virus

查看主机病毒统计信息

ip-virus show sort <asc|des> **by** <ip|low|middle|high>

命令描述

查看感染病毒的主机排名信息

参数说明：

show	查看感染病毒的 IP 排名信息
sort	指定排方式：升序或降序排列
asc|des	asc 表示升序，des 降序。
by	指定排列依据
ip|low|middle|high	Ip 表示按照 IP 地址进行排序；low 表示低风险；middle 表示一般风险；high 表示高风险。

ip-virus clean<cr>

命令描述

清空所有感染病毒的主机排名信息

ip-virus-detail

查看某一 IP 感染病毒的详细信息

ip-virus-detail show name <*string*> **sort** <asc|des> **by** <name|dir|level|count>

命令描述

查看某一个主机感染病毒的详细信息

参数说明：

show	查看某一个主机感染病毒的详细信息
sort	指定排方式：升序或降序排列
asc|des	asc 表示升序，des 降序。
by	指定排列依据
name|dir|level|count	name 表示按照 IP 地址进行排序；dir 表示按照方向排名，上传或下载；level 表示按照风险级别进行排序，风险分为低风险、一般风险和高风险。Count 表示按照次数进行排序。

max-session

设置最大连接数

max-session set <*number*>

命令描述

设置最大连接数

参数说明：

max-session set	设置最大连接数
number	数值，范围在 10000 – 1000000 之间。

monitorhost

设置主机监控的各种参数

monitorhost show<cr>

命令描述

查看主机监控的相关设置

monitorhost showsysmax <cr>

命令描述

显示系统支持的最大监控主机数

monitorhost set range <*string*> **max** <*number*> **autoreclaim** <on|off>

命令描述

设置主机监控的相关参数

参数说明：

set	设置主机监控的相关参数
range	设置主机监控的范围
string	字符串，输入已经添加的范围地址对象。
max	设置监控主机的最大个数。
number	数值
autoreclaim	是否开启自动回收
on|off	On 表示开启，off 表示关闭。

monitor-switch

流量监控设置

monitor-switch set <on|off>

命令描述：

设置是否进行流量监控

参数说明：

monitor-switch set	设置是否进行流量监控
on|off	on 表示开启流量监控，off 表示关闭

monitor-switch show<cr>

命令描述：

查看流量监控设置

net-quota

显示对网络设置的各种流量和连接的配额

net-quota show<cr>

other-quota

设置其他流量异常的阀值

other-quota set <*number*>

命令描述：

设置其他流量异常的阀值

参数说明：

other-quota set	设置其他流量异常的阀值
number	输入其他流量占总流量的百分比，范围在 0-100 之间。

policy

设置应用识别策略

policy add name <*string***> actions** <*string*> **log** <on|off>

命令描述

添加应用识别策略

参数说明：

add	添加应用识别策略
name	输入要添加的应用识别策略的名字
string	字符串
actions	各种协议的动作。
string	字符串，用一对单引号括起来，空格分隔。每一项都是“协议|动作”的格式。协议就是目前支持的所有应用层协议名或者他们对应组别名（组名就代表该组的动作都相同）。协议目前支持接近一百种，包括 http、qq、msn、pplive 等等。动作支持允许、禁止、帐号控制（只有 qq 和 msn 支持）、带宽控制（部分支持）等。

log	是否记录日志
on|off	on 表示记录，off 表示不记录。

policy modify name <*string*> [**actions** <*string*>] [**log** <on|off>]

命令描述

修改应用识别策略

参数说明：

modify	修改应用识别策略
name	输入要修改的应用识别策略的名字
string	字符串
actions	各种协议的动作。
string	字符串，用一对单引号括起来，空格分隔。每一项都是“协议|动作”的格式。协议就是目前支持的所有应用层协议名或者他们对应组别名（组名就代表该组的动作都相同）。协议目前支持接近一百种，包括 http、qq、msn、pplive 等等。动作支持允许、禁止、帐号控制（只有 qq 和 msn 支持）、带宽控制（部分支持）等。
log	是否记录日志
on|off	on 表示记录，off 表示不记录。

policy delete name <*string*>

命令描述

删除应用识别策略

参数说明：

delete	删除应用识别策略
name	输入要删除的应用识别策略的名字
string	字符串

policy clean<cr>

命令描述

清空所有应用识别策略

policy show name <*string*>

命令描述

查看应用识别策略的内容

参数说明：

delete	查看应用识别策略的内容
name	输入要查看的应用识别策略的名字
string	字符串

quota

将 tcp-quota、udp-quota、other-quota、group_quota、max-session 命令设置的相关报警阈值全部重置。

quota reset<cr>

命令描述

重置报警阈值。

rules

规则库升级配置

rules autoupdate set dayofweek <*number*> **time** <*string*> **url** <*string*> **type** <*string*> **enable** <yes|no>

命令描述

规则库自动升级设置

参数说明：

autoupdate set	规则库自动升级设置
dayofweek	设置一周中的哪一天进行更新
number	数值，1－7 分别代表星期一到星期日。
time	设置每天的具体时间段
string	字符串
url	规则库升级的服务器 URL 地址
string	字符串，支持 http 地址和 ftp 地址，形如 http://bbb.aaa.com/ 或 ftp://user:password@xxx.yyy.com/ 形式（ftp 匿名用户可省略 user:password@字段）。
type	指定需要升级的规则库类型
string	可选项为 ips 或 ar
enable	是否开启自动升级功能
yes|no	yes 表示启用，no 表示禁用。

rules autoupdate show<cr>

命令描述

查看规则库自动升级设置

rules autoupdate reset<cr>

命令描述：

恢复升级配置到出厂状态

rules update filename <*string*> **type** <ips|ar>

命令描述：

恢复升级配置到出厂状态

rules update [**filename** <*string*> **type** <ips|ar>[**url** <*string*>]]

命令描述：

用户通过命令行手动连接服务器下载规则库文件进行升级，（1）当无参数时，会读取自动升级配置中的服务器设置和规则库类型设置进行升级。(2)只有 filename 和 type 参数时，使用设备上/tmp 目录中的文件进行升级，此功能专供 WebUI 使用，实现本地升级功能。（3）filename、type 和 url 参数都存在时，从 url 指定的服务器下载 type 指定的规则库文件 filename 进行升级。

参数说明：

update	规则库自动升级设置
filename	指定服务器上规则库文件名称
string	字符串
type	指定需要升级的规则库类型
ips|ar	ips 表示升级 IPS 规则库；ar 表示升级应用程序识别规则库。
url	规则库升级的服务器 URL 地址
string	字符串，支持 http 地址和 ftp 地址，形如 http://bbb.aaa.com/ 或 ftp://user:password@xxx.yyy.com/ 形式（ftp 匿名用户可省略 user:password@字段）。

rules timeinfo show<cr>

命令描述：

显示当前各个版本库最近一次升级时间和许可证过期时间

stat-object

显示所有监控对象的流量信息

stat-object show<cr>

stat-object-detail

显示监控对象的详细信息，可以按照特定项进行排序

stat-object-detail show name <*string*> **sort** <asc|des> **by** <ip|session |up_speed |down_speed |up_bytes |down_bytes>

命令描述

显示监控对象的详细信息，可以按照特定项进行排序

参数说明：

stat-object-detail show	显示监控对象的详细信息
name	要显示详细信息的监控对象名
string	
sort	排序方式
asc|des	asc 表示升序，dec 表示降序
by	对指定项目进行排序。支持 ip、session、up_speed、down_speed、up_bytes、down_bytes 六种。
ip|session |up_speed |down_speed |up_bytes |down_bytes	ip：按照 IP 地址进行排序；session：按照连接数进行排序；up-speed：按照上行速度排序；down-speed：按照下行速度排序；up_bytes：按照上行流量进行排序；down_bytes：按照下行流量进行排序。

tcp-quota

设置 TCP 流量异常阀值，即 tcp 流量占总流量的百分比比例，范围在 5 － 90 之间。

tcp-quota set <*number*>

命令描述

设置 TCP 流量异常阀值

参数说明：

tcp-quota set	设置 TCP 流量异常阀值
number	数值，范围在 0-100 之间。

udp-quota

设置 UDP 流量异常阀值，即 UDP 流量占总流量的百分比比例，范围在 5 – 90 之间。

udp-quota set <*number*>

命令描述

设置 UDP 流量异常阀值

参数说明：

udp-quota set	设置 UDP 流量异常阀值
number	数值，范围在 0-100 之间。

version

显示应用识别规则库版本和规则库升级到期时间

ar version<cr>

virus

查看病毒统计信息

virus show sort <asc|des> **by** <name|level|action|protocol|count|last_time|virus_src>

命令描述

查看病毒统计信息

参数说明：

sort	设置排序方式
asc|des	Asc 表示升序；desc 表示降序；
by	排序依据
name|level|action|protocol|count|last_time|virus_src	Name：按照名字排序； Level：按照危害级别排序； Action：按照处理方式排序； Protocol：按照协议类型排序； Count：按照次数排序； last_time：按照最近发现时间排序； virus_src：按照病毒来源排序；

virus clean<cr>

命令描述

清空病毒统计信息

virus-ip-top

查看感染某个病毒的主机排名

virus-ip-top show name <*string*> **sort** <asc|des> **by** <ip|dir|count>

命令描述

查看感染某个病毒的主机排名信息

参数说明：

name	指定主机名
string	字符串
sort	设置排序方式
asc|des	Asc 表示升序；desc 表示降序；
by	排序依据
ip|dir|count	Ip：按照 IP 地址排名 Dir：按照方向排名，上传或下载。 Count：按照次数排序；

virus-group

查看病毒种类统计信息

virus-group show sort <asc|des> **by** <name|count>

命令描述

查看病毒种类统计信息

参数说明：

show	查看病毒种类统计信息
sort	设置排序方式
asc|des	Asc 表示升序；desc 表示降序；
by	排序依据
name|count	name：按照病毒名称排名； Count：按照次数排序；

virus-group clean<cr>

命令描述

清空病毒种类统计信息

virus-domain

查看病毒种类排序信息

virus-domain show sort <asc|des> **by** <name|count|last_time>

命令描述

查看病毒种类排序信息

参数说明：

sort	设置排序方式
asc|des	Asc 表示升序；desc 表示降序；
by	排序依据
name|count|last_time	name：按照主机名排名 Count：按照次数排序； Last_time：按照最近发现时间进行排序；

virus-domain clean<cr>

命令描述

清空病毒种类排序信息

virus-start-time

查看病毒统计开始时间

virus-start-time show<cr>

DEBUG

本命令用来配置网络卫士安全网关中的虚拟报文截获规则，以帮助管理员对安全网关的各种功能进行调试。网络卫士安全网关在安装调试时会遇到各种网络环境，可能会碰到一些问题，安全网关的调试功能，能够帮助准确获取网络通信信息，给技术支持和程序开发人员提供分析问题的帮助。网络卫士安全网关系统提供的报文调试手段包括报文截获和报文跟踪。

进入本命令模块操作如下：

debug<cr>

退出本命令模块操作如下：

end<cr>

CLI 管理员登录安全网关并进入本命令模块后，可以执行相应的组件管理命令。下面将详细描述本命令模块下的所有组件管理命令。命令的实例输入格式将按已经进入本命令模块书写。

下一级命令列表

命令	功能
filter	制定调试信息报文过滤策略，用于过滤掉用户不想输出 debug 信息的数据包
module	模块调试功能设置
start	输出模块调试信息
clean	清除调试配置并停止输出调试信息

filter

制定报文过滤策略，用于过滤掉用户不想输出 debug 信息的数据包。根据用户定义的策略过滤数据包。为符合策略的数据包做标记，方便后面 debug 模块输出：如果数据包被标记，则输出；否则，不输出。如果存在用户定义的策略，则按照策略，给符合策略的数据包做标记。如果没有相应的策略，则默认所有的数据包都不需要输出。

filter clean<cr>

命令描述：

清除所有的报文过滤策略。

filter set interface <*string***>destination-ip1 <***ipaddress1***> destination-ip2 <***ipaddress2***>**

destination-mac <*macaddress*> **destination-port1** <*port*> **destination-port2** <*port*> **source-ip1** **<***ipaddress1***> source-ip2 <***ipaddress2***>source-mac** <*macaddress*> **source-port1** <*port1*> **source-port2** <*port2*> **l3-pro** < *string* > **protocol** <*string*> [**host-ip1** <*ipaddress*> **host-ip2** <*ipaddress*>

命令描述：

设置报文过滤规则。

参数说明：

Set	设置报文过滤规则
interface	指定接口名称。
string	字符串，表示接口名称。
destination-ip1	设置报文目的 IP 的起始地址。
ipaddress	字符串，表示 IP 地址，形为 A.B.C.D。
destination-ip2	设置报文目的 IP 的结束地址。
macaddress	字符串，表示 MAC 地址，格式为：00:00:00:00:00:00。
destination-mac	设置报文的目的 MAC 地址。
macaddress	字符串，表示 MAC 地址，格式为：00:00:00:00:00:00。
destination-port1	设置报文目的端口的起始端口（当协议类型设置为 tcp 或 udp 时需要设置该参数）。
number	数值，表示端口号。
destination-port2	设置报文目的端口的结束端口（当协议类型设置为 tcp 或 udp 时需要设置该参数）。
number	数值，表示端口号。
source-ip1	设置报文源 IP 的起始地址。

ipaddress	字符串，表示 IP 地址，形为 A.B.C.D。
source-ip2	设置报文源 IP 的结束地址。
ipaddress	字符串，表示 IP 地址，形为 A.B.C.D。
Source-mac	设置报文的源 MAC 地址。
macaddress	字符串，表示 MAC 地址，格式为：00:00:00:00:00:00。
source-port1	设置报文源端口的起始端口（当协议类型设置为 tcp 或 udp 时需要设置该参数）。
number	数值，表示端口号。
source-port2	设置报文源端口的结束端口（当协议类型设置为 tcp 或 udp 时需要设置该参数）。
number	数值，表示端口号。
l3-pro	设置 3 层协议类型。
String	输入“arp”，或三层协议号。 说明： 当用户设置为 ip 类型时，还需要设置数据报文的源/目的 IP 等信息。
protocol	设置四层协议类型，共有三个选项：tcp、udp 和 icmp。
String	可选项为 tcp|udp|icmp，或输入协议类型数值。数字范围 0~1024。 说明： tcp 表示 TCP 协议，udp 表示 UDP 协议，icmp 表示 ICMP 协议。当用户选择了 tcp 或 udp 时，还需要设置报文的源端口和目的端口；而选择 icmp 时则需要设置 ICMP 类型码。
host-ip1	设置报文源 IP 的起始地址。
ipaddress	字符串，表示 IP 地址，形为 A.B.C.D。
host-ip2	设置报文源 IP 的结束地址。
ipaddress	字符串，表示 IP 地址，形为 A.B.C.D。

实例：

** 在 eth0 口上添加一条报文过滤规则，要求该规则截获从 192.168.83.2-192.168.83.200（MAC：00:08:2E:1A:06:80）到 192.168.1.163-192.168.1.225（MAC：00:08:2D:1A:19:80）的 TCP 报文，源端口为 4000-5000，目的端口为 8000-9000。

filter set interface *eth0* **source-mac** *00:08:2E:1A:06:80* **source-mac** *00:08:2D:1A:19:80* **l3proto** ip **source-ip1** *192.168.83.2* **source-ip2** *192.168.83.200* **destination-ip1** *192.168.1.163* **destination-ip1** *192.168.1.225* **protocol** tcp **source-port1** *4000* **source-port2** *5000* **destination-port1** *8000* **destination-port2** *9000*

filter show <cr>

命令描述：

查看报文过滤规则。

filter none<cr>

命令描述：

不过滤数据包，输出所有数据包。

module

模块调试功能设置

module enable name <*string*>**timestamp** <on|off> **level**<*string*>

命令描述：

打开某个模块的调试开关，设置是否增加时间戳，并可以设定输出信息级别。时间戳默认不输出，输出级别默认为 4。

参数说明：

enable	打开某个模块的调试开关
name	指定模块名
string	字符串，必须是已经注册的模块名称，可以使用 debug module show 显示
timestamp	可选项，设置是否增加时间戳，默认为“否”
on|off	是/否
level	设置调试信息的输出级别，级别越小，调试信息重要程度越高。
number	数值，范围为 1－4。

module disble name <*string*>

命令描述：

关闭某个模块的调试开关。

参数说明：

disble	关闭某个模块的调试开关
name	指定模块名
string	字符串，必须是已经注册的模块名称，可以使用 debug module show 显示

module show <cr>

命令描述：

查看已经注册的模块名称的调试开关信息。

module clean <cr>

命令描述：

全部关闭所有模块的调试开关。

start

输出模块调试信息。

debug start <cr>

命令描述：

输出模块调试信息。

clean

清除调试配置并停止输出调试信息

debug clean <cr>

命令描述：

清除调试配置并停止输出调试信息

DEFINE

网络卫士安全网关中访问规则和地址转换策略的定义是基于对象的，用户只有在定义了所涉及的对象之后，才能根据实际安全策略要求，定义访问规则和地址转换策略。本命令用来配置网络卫士安全网关中涉及到的各种对象，包括区域、主机、子网、地址范围、服务器、服务、时间等。

进入本命令模块操作如下：

define <cr>

退出本命令模块操作如下：

end <cr>

CLI 管理员登录安全网关并进入本命令模块后，可以执行相应的组件管理命令。下面将详细描述本命令模块下的所有组件管理命令。命令的实例输入格式将按已经进入本命令模块书写。

下一级命令列表

命令	功能
area	区域资源管理
dns	设置 DNS 对象
group_address	地址组管理
group_service	服务组管理
host	主机资源管理
query	查找资源对象是否被引用
range	地址范围资源管理
schedule	时间资源管理
server	负载均衡服务器管理
service	服务资源管理
subnet	子网资源管理
virtual_server	虚拟服务器组管理，即负载均衡组管理

area

安全网关的区域对象管理，在此用户可以添加、修改或删除区域，另外还可以设定区域的默认访问权限。访问控制规则引用区域来做访问控制，如果不存在可匹配的访问控制规则，网络卫士安全网关将根据目的接口所在区域的权限处理该报文。

area add name <*string1*> [**access** <on|off>][**attribute** <*string2*>][**vsid** <*number*>][**comment** <*string3*>]

命令描述：

添加一个区域。

参数说明：

add	添加一个区域
name	指定区域名称

string1	字符串，表示区域名称
access	指定区域的访问权限
on	允许访问该区域
off	拒绝访问该区域
attribute	指定与该区域绑定新的属性或属性组
string2	字符串，可以为一个或多个已经定义的属性或属性组对象名，多个时用单引号括起来，之间用空格分割’aa bb’；属性和属性组需要在 network 模块的 attribute 和 attribute-group 中进行查看和定义。
vsid	指定虚系统的标号
number	数值，安全网关上虚系统的标号
comment	设置备注内容
string3	字符串，表示备注内容

使用说明：

所谓**区域**，就是一段具有相似安全属性的网络空间，对于网络卫士安全网关来说，访问控制规则引用区域来做访问控制。

实例：

** 为虚系统 1 添加一个与属性 eth0 绑定的区域 area_eth0，并且允许访问该区域

area add name *area_eth0* **access** on **attribute** *eth0* **vsid** *1* **comment** *comment_content*

area modify name <*string1*> [**access** <on|off>][**attribute** <*string2*>][**vsid** <*number*>][**comment** <*string3*>]

命令描述：

修改一个区域。

参数说明：

modify	修改一个区域
name	指定要修改的区域的名称
string1	字符串，表示区域名称
access	指定区域新的访问权限
on	允许访问该区域
off	拒绝访问该区域
attribute	指定与该区域绑定新的属性或属性组
string2	字符串，可以为一个或多个已经定义的属性或属性组对象名，多个时用单引号括起来，之间用空格分割’aa bb’；属性和属性组需要在 network 模块的 attribute 和 attribute-group 中进行查看和定义。
vsid	指定要修改的区域对象所在的虚拟系统标号
number	数值，安全网关上虚系统的标号

comment	设置新的备注内容 说明： 如果“comment”参数后输入的值为“none”，表示删除“comment”内容。
string3	字符串，表示备注内容

使用说明：

如果所修改的区域属于某个虚系统（带有虚系统号），修改时就必须在命令行中指定相应的虚系统号。

实例：

** 修改属于虚系统 1 的 area_eth0 区域的访问权限为 off

area modify name *area_eth0* **access** off **vsid** *1*

area delete name <*string*> [**vsid** <*number*>]

命令描述：

删除一个区域。如果该区域被规则引用，则无法删除。

参数说明：

delete	删除一个区域
name	指定要删除的区域名称
string	字符串，表示区域名称
vsid	指定要删除区域的虚系统的标号
number	数值，安全网关上虚系统的标号

使用说明：

如果所删除的区域属于某个虚系统（带有虚系统号），删除时就必须在命令行中指定相应的虚系统号。

实例：

** 删除属于虚系统 1 的区域 area_eth0

area delete name *area_eth0* **vsid** *1*

area rename oldname <*string1*> **newname** <*string2*> [**vsid** <*number*>]

命令描述：

重命名一个区域。

参数说明：

rename	重命名一个区域
oldname	指定要重新命名的区域名称
string1	字符串，表示区域名称
newname	指定新的区域名称
string2	字符串，表示区域名称
vsid	指定要重命名区域所在的虚系统的标号
number	数值，安全网关上虚系统的标号

使用说明：

如果所重命名的区域属于某个虚系统（带有虚系统号），重命名时就必须在命令行中指定相应的虚系统号。

实例：

** 将属于虚系统 1 的区域 area_eth0 重命名为 firstarea

area rename oldame *area_eth0* **newname** *firstarea* **vsid** *1*

area show [**vsid** <*number*>]

命令描述：

显示安全网关系统中的所有区域对象。

参数说明：

show	显示区域对象
vsid	指定要显示区域的虚系统的标号
number	数值，安全网关上虚系统的标号

实例：

** 显示所有区域

area show <cr>

area clean <cr>

命令描述：

清空安全网关系统中的所有未被引用的区域对象。

参数说明：

clean	清空所有未被引用的区域对象
cr	键盘回车符

实例：

** 清空所有未被引用的区域对象

area clean<cr>

dns

DNS 对象设置

dns add name < *string*> **key-word** < *string*> **comment** < *string*> **vsid** < *number*>

命令描述：

添加一个 DNS 对象。

参数说明：

add	添加 DNS 对象
name	设置对象的名称
string	字符串，表示对象的名称
key-word	设置关键字
string2	字符串
comment	输入注释信息
string	字符串
vsid	指定要在哪个虚系统上添加对象
number	数值，安全网关上虚系统的标号

dns delete name < *string*> **id** < *number*> **vsid** < *number*>

命令描述：

删除一个 DNS 对象。

参数说明：

delete	删除 DNS 对象
name	设置对象的名称
string	字符串，表示对象的名称
id	指定对象 ID 号
number	数值
vsid	指定虚系统 ID
number	数值，安全网关上虚系统的标号

dns clean vsid < *string*>

命令描述：

清除指定虚系统的所有 DNS 对象。

dns show vsid < *string*>

命令描述：

查看指定虚系统的所有 DNS 对象。

dns modify name <*string*> **key-word** < *string*> **comment** < *string*> **vsid** < *number*>

命令描述：

修改一个 DNS 对象的属性。

参数说明：

modify	修改 DNS 对象的属性
name	设置对象的名称
string	字符串，表示对象的名称
key-word	设置关键字
string2	字符串
comment	输入注释信息
string	字符串
vsid	指定虚系统 ID
number	数值，安全网关上虚系统的标号

group_address

为了方便用户定义规则，网络卫士安全网关支持将主机、子网、范围地址对象组合成一个组地址对象作为规则的源或目的。组地址对象的成员必须是一个已定义的地址对象：主机地址对象、子网地址对象、范围地址对象。

group_address add name <*string1*> [**member** <*string2*>] [**vsid** <*number*>]

命令描述：

添加一个地址组对象。

参数说明：

add	添加地址组对象
name	设置地址组对象的名称
string1	字符串，表示地址组对象的名称
member	设置地址组对象中的成员

string2	字符串，表示地址对象，可以是已经定义的主机对象、子网对象或地址范围对象
vsid	指定要在哪个虚系统上添加地址组对象
number	数值，安全网关上虚系统的标号

使用说明：

在定义地址组之前，可以先定义地址对象，关于地址对象的定义请参考相关章节。

实例：

** 添加地址组对象 groupaddr1，其成员为已定义的主机对象 host1

group_address add name *groupaddr1* **member** *host1*

group_address addmember groupname <*string1*> **member** <*string2*> [**vsid** <*number*>]

命令描述：

为已经定义好的地址组添加成员。

参数说明：

addmember	为地址组添加成员
name	指定要添加成员的地址组名称
string1	字符串，表示地址组名称
member	指定要添加哪些成员
string2	字符串，表示地址对象，可以是主机对象、子网对象或范围对象
vsid	指定要添加成员的地址组所在的虚系统的标号
number	数值，安全网关上虚系统的标号

实例：

** 为地址组 groupaddr1 添加成员 subnet1

group_address addmember groupame *groupaddr1* **member** *subnet1*

group_address rename oldname <*string1*> **newname** <*string2*> [**vsid** <*number*>]

命令描述：

重新命名地址组对象。

参数说明：

rename	重命名地址组
oldname	指定要重新命名的地址组名称
string1	字符串，表示地址组对象名称（已定义的对象名称）
newname	指定新的地址组对象名称
string2	字符串，表示地址组对象的新名称

vsid	指定要重命名的地址组所在的虚系统的标号
number	数值，安全网关上虚系统的标号

实例：

** 将地址组 goupaddr1 重命名为 groupaddr2

group_address rename oldname *groupaddr1* **newname** *groupaddr2*

group_address delete [**id** <*number1*>] [**name** <*string*>] [**vsid** <*number2*>]

命令描述：

删除一个地址组对象。如果该对象被规则引用，则无法删除。

参数说明：

delete	删除一个地址组
id	指定要删除的地址组对象对应的 ID 号
number1	数值，表示地址组对象的 ID 号
name	指定要删除的地址组的名称
string	字符串，表示地址组名称
vsid	指定要删除的地址组所在的虚系统标号
number2	数值，安全网关上虚系统的标号

使用说明：

在删除地址组对象时，既可根据地址组对象的名称来删除，又可以通过地址组对象的 id 来删除，也可以同时指定 id 和 name，但是当两者不一致时以名称为准。当不指定任何参数时，删除所有**未被引用的**地址组对象。

实例：

** 删除地址组 groupaddr1

group_addrees delete name *groupaddr1*

group_address delmember groupname <*string1*> **member** <*string2*> [**vsid** <*number*>]

命令描述：

删除地址组中的成员。

参数说明：

delmeber	删除地址组中的成员
groupname	指定要删除成员的地址组对象的名称
string1	字符串，表示地址组名称

member	指定要删除地址组中的哪个成员
string2	字符串，表示地址对象名称，可以是主机对象、子网对象或范围对象
vsid	指定要删除成员的地址组所在的虚系统标号
number	数值，安全网关上虚系统的标号

实例：

** 删除地址组 groupaddr1 中的成员 subnet1

group_address delmember groupname *groupaddr1* **member** *subnet1*

group_address clean [**vsid** <*number*>]

命令描述：

删除所有未被引用的地址组对象。

参数说明：

clean	删除所有未被引用的地址组对象
vsid	指定要删除那个虚系统上的所有地址组
number	数值，安全网关上虚系统的标号

使用说明：

当不指定虚系统号时，默认删除虚系统 0 上的所有地址组

实例：

** 清除安全网关系统上的所有未被引用的地址组对象

group_address clean <cr>

group_address cleanmember groupname <*string*> [**vsid** <*number*>]

命令描述：

删除一个地址组中的所有成员。

参数说明：

cleanmember	删除一个地址组中的所有成员
groupname	指定要删除所有成员的地址组的名称
string	字符串，表示地址组的名称
vsid	指定要删除所有成员的地址组所在的虚系统标号
number	数值，安全网关上虚系统的标号

实例：

** 清空地址组 groupaddr1 中的所有成员

group_address cleanmember groupame *groupaddr1*

group_address show [**vsid** <*number*>]

命令描述：

查看所有地址组。

参数说明：

show	查看所有地址组
vsid	指定要查看那个虚系统上的地址组
number	数值，安全网关上虚系统的标号

实例：

** 查看地址组

group_address show <cr>

group_service

安全网关的服务组对象管理，在此用户可以添加、修改或删除服务组。

group_service add name <*string1*> [**member** <*string2*>] [**vsid** <*number*>]

命令描述：

添加一个服务组对象。

参数说明：

add	添加服务组对象
name	设置服务组对象的名称
string1	字符串，表示服务组的名称
member	设置服务组中的成员（服务对象），此处的服务可以是用户自定义的服务，也可以是系统的默认服务
string2	字符串，表示服务名称
vsid	指定要在哪个虚系统上添加服务组
number	数值，安全网关上虚系统的标号

使用说明：

在定义服务组之前，可以先定义服务对象，关于服务对象的定义请参考 define

service。

实例：

** 添加服务组对象 goupservice1，并将服务 http8080 作为成员加入该服务组

goup_service add name *groupservice1* **member** *http8080*

group_service addmember groupname <*string1*> **member** <*string2*> [**vsid** <*number*>]

命令描述：

向已经存在的服务组中添加服务。

参数说明：

addmember	向服务组中添加服务
groupname	设置要添加服务的服务组的名称
string1	字符串，表示服务组名称
member	设置要添加哪些服务，此服务可以是用户自定义的服务，也可以是系统的默认服务
string2	字符串，表示服务名称
vsid	指定要向哪个虚系统上的服务组添加成员
number	数值，安全网关上虚系统的标号

实例：

** 将服务 http8000 添加到 groupservice1 服务组中

group_service addmember groupname *groupservice1* **member** *http8080*

group_service rename oldname <*string1*> **newname** <*string2*> [**vsid** <*number*>]

命令描述：

重新命名服务组对象。

参数说明：

rename	重命名服务组
oldname	指定要重新命名的服务组名称
string1	字符串，表示服务组对象名称（已定义的对象名称）
newname	指定新的服务组名称
string2	字符串，表示服务组的新名称
vsid	指定要重命名的服务组所在的虚系统的标号
number	数值，安全网关上虚系统的标号

实例：

** 将服务组对象 groupservice1 重命名为 groupservice2

group_service rename oldname *groupservice1* **newname** *groupservice2*

group_service delmember groupname <*string1*> **member** <*string2*> [**vsid** <*number*>]

命令描述：

删除服务组中的成员服务。

参数说明：

delmember	删除服务组中的成员服务
groupname	指定要删除成员服务的服务组的名称
string1	字符串，表示服务组的名称
member	指定要删除服务组中的哪个服务
string2	字符串，表示服务名称
vsid	指定要删除服务的服务组所在的虚系统标号
number	数值，安全网关上虚系统的标号

实例：

** 删除服务组 groupservice2 中的服务对象 http8000

group_service delmember groupname *groupservice2* **member** *http8000*

group_service delete [**id** <*number1*>] [**name** <*string*>] [**vsid** <*number2*>]

命令描述：

删除一个服务组对象。如果该对象被规则引用，则无法删除。

参数说明：

delete	删除一个服务组对象
id	指定要删除的服务组对应的 ID 号
number1	数值，表示服务组对象的 ID 号
name	指定要删除的服务组对象的名称
string	字符串，表示服务组名称
vsid	指定要删除的服务组所在的虚系统标号
number2	数值，安全网关上虚系统的标号

使用说明：

在删除服务组对象时，既可根据服务组对象的名称来删除，又可以通过服务组对象的 id 来删除，也可以同时指定 id 和 name，但是当两者不一致时以名称为准。

当不指定任何参数时，删除**未被引用的**服务组对象。

实例：

** 删除服务组对象 groupservice2

group_service delete name *groupservice2*

group_service cleanmember groupname <*string*> [**vsid** <*number*>]

命令描述：

清空指定服务组中的所有成员服务。

参数说明：

cleanmember	清空指定服务组中的所有成员服务
groupname	指定要清空的服务组的名称
string	字符串，表示服务组名称
vsid	指定要清空那个虚系统上的服务组
number	数值，安全网关上虚系统的标号

使用说明：

当不指定虚系统号时，默认清空虚系统 0 上的服务组

实例：

** 清空服务组 groupservice2 中的所有成员服务

group_service cleanmember groupname *groupservice2*

group_service clean [**vsid** <*number*>]

命令描述：

删除所有服务组对象。

参数说明：

clean	删除所有服务组对象
vsid	指定要删除那个虚系统上的所有服务组对象
number	数值，安全网关上虚系统的标号

使用说明：

当不指定虚系统号时，默认删除虚系统 0 上的所有服务组对象

实例：

** 清除安全网关系统上的所有服务组对象

group_service clean <cr>

group_service modify name <*string1*> [**member** <*string2*>] [**vsid** <*number*>]

命令描述：

修改一个服务组对象。

参数说明：

add	修改服务组对象
name	服务组对象的名称
string1	字符串，表示服务组的名称
member	服务组中的成员（服务对象），此处的服务可以是用户自定义的服务，也可以是系统的默认服务
string2	字符串，表示服务名称
vsid	指定要在哪个虚系统上添加服务组
number	数值，安全网关上虚系统的标号

实例：

** 修改服务组对象 goupservice1，并将服务 http8080 作为成员加入该服务组

goup_service modify name *groupservice1* **member** *http8080*

group_service show [**vsid** <*number*>]

命令描述：

查看所有服务组对象。

参数说明：

show	查看所有服务组对象
vsid	指定要查看那个虚系统上的服务组对象
number	数值，安全网关上虚系统的标号

实例：

** 查看服务组对象

group_service show <cr>

host

安全网关的主机对象管理，在此用户可以添加、修改或删除主机对象。

host add <name <*string1*>> [**ipaddr** <*string2*>] [**macaddr** <*macaddress*>][**session** <*number1*>] [**halfsession** <*number2*>] [**synproxy**<on|off>] [**vsid** <*number3*>] [**mss** < *number*>] [**dir** < src|dst>] [**session-per-second** < *number*>]

命令描述：

添加一个主机对象。

参数说明：

add	添加一个主机对象
name	设置要添加的主机对象的名称
string1	字符串，表示主机对象名称
ipaddr	设置主机对象的 IP 地址
string2	字符串，表示 IP 地址，格式为：192.168.1.6，可以为一个或多个 IP 地址，多个时用单引号括起来，之间用空格分隔’192.168.83.1 192.168.1.6’
macaddr	设置主机对象的 MAC 地址
macaddress	字符串，表示 MAC 地址，格式为：00:00:00:00:00:00
session	设置并发连接数。 说明： 用于设置在同一时刻，允许其它主机与该主机建立的最大连接数。
number1	数值，表示主机对象的并发连接数
halfsession	设置半连接数 说明： 用于设置在同一时刻，允许其它主机与该主机建立的最大半连接数。限制半连接主要是为了限制特定 IP 连续发 syn 包的个数，限制此 IP 对其他机器进行 syn 攻击。
number2	数值，表示主机对象的半连接数
synproxy	设置是否开启 SYN 代理方式保护服务器，默认开启
on|off	on：开启 SYN 代理，off：关闭 SYN 代理
vsid	指定要配置主机对象的虚拟系统号
number3	数值，安全网关上虚系统的标号
mss	最大传输大小
number	数值
dir	设置地址方向 说明： 设置对地址对象的连接数进行控制的方向。
src|dst	源/目的 说明： 当选择“src”时，表示防护主机访问其他主机时进行限制； 当选择“dst”时，表示其他主机访问防护主机时进行限制。
session-per-second	每秒新建连接数
number	范围为 0-100000

实例：

** 添加一个主机 host1，并设定其 IP 地址为 192.168.1.8

host add name *host1* **ipaddr** *192.168.1.8*

host modify name <*string1*>[**ipaddr** <*string2*>][**macaddr** <*macaddress*>][**session** <*number1*>] [**halfsession** <*number2*>][**synproxy** <on|off>][**vsid** <*number3*>] [**mss** < *number*>] [**dir** < src|dst>] [**session-per-second** < *number*>]

命令描述：

修改一个主机对象。

参数说明：

modify	修改主机对象
name	指定要修改的主机对象名称
string1	字符串，表示主机对象名称
ipaddr	指定新的 IP 地址
string2	字符串，表示 IP 地址
macaddr	指定新的 MAC 地址
macaddress	字符串，表示 MAC 地址
session	指定新的最大连接数
number1	数值，表示最大连接数
halfsession	修改半连接数
number2	数值，表示主机对象的半连接数
synproxy	指定是否开启 SYN 代理
on|off	on：开启 SYN 代理，off：关闭 SYN 代理
vsid	指定要修改的主机对象所在的虚拟系统号
number3	数值，安全网关上虚系统的标号
mss	最大传输大小
number	数值
dir	设置地址方向
src|dst	源/目的，当选择“src”时，表示防护主机访问其他主机时对连接数进行限制；当选择“dst”时，表示其他主机访问防护主机时的连接数进行限制。
session-per-second	每秒新建连接数
number	范围为 0-100000

使用说明：

使用**host modify name** <*string*> **macaddr** *00:00:00:00:00:00*可以用来解除“IP MAC绑定。相当于WEBUI上的删除。

实例：

** 修改 host1 主机对象的 IP 地址为：192.168.1.20

host modify name *host1* **ipaddr** *192.168.1.20*

host rename oldname <*string1*> **newname** <*string2*> [**vsid** <*number*>]

命令描述：

重新命名主机对象。

参数说明：

rename	重命名主机对象
oldname	指定要重新命名的主机对象名称
string1	字符串，表示主机对象名称（已定义的主机对象名称）
newname	为主机对象指定新的名称
string2	字符串，表示主机对象的新名称
vsid	指定要重命名的主机对象所在的虚系统的标号
number	数值，安全网关上虚系统的标号

实例：

** 将主机对象 host1 重命名为 host2

host rename oldname *host1* **newname** *host2*

host delete [**id** <*number1*>] [**name** <*string*>] [**vsid** <*number2*>]

命令描述：

删除一个主机对象。如果该对象被规则引用，则无法删除。

参数说明：

delete	删除一个主机对象
id	指定要删除的主机对象对应的 ID 号
number1	数值，表示主机对象的 ID 号
name	指定要删除的主机对象的名称
string	字符串，表示主机对象名称
vsid	指定要删除主机对象的虚系统的标号
number2	数值，安全网关上虚系统的标号

使用说明：

在删除主机对象时，既可根据主机对象的名称来删除，又可以通过主机地址对象的 id 来删除，也可以同时指定 id 和 name，但是当两者不一致时以名称为准。

当不指定任何参数时，删除**未被策略引用的**主机地址对象。

实例：

** 删除主机对象 host1

host delete name *host1*

host clean [**vsid** <*number*>]

命令描述：

删除所有未被引用的主机对象。

参数说明：

clean	删除所有未被引用的主机对象
vsid	指定要删除那个虚系统上的所有主机对象
number	数值，安全网关上虚系统的标号

实例：

** 清除安全网关系统上的所有未被引用的主机对象

host clean <cr>

host show [**vsid** <*number*>]

命令描述：

查看所有主机对象。

参数说明：

show	查看所有主机对象
vsid	指定要查看那个虚系统上的主机对象
number	数值，安全网关上虚系统的标号

实例：

** 查看主机对象

host show <cr>

query

查找对象是否被引用

query refered name <*string*> [**vsid** <*number*>]

命令描述：

查看对象是否被引用。

参数说明：

refered	查看对象是否被引用
name	指定要查看的对象名
string	字符串，必须是已定义的对象名。
vsid	可选项，指定虚系统 ID 号。
number	数值

实例：

** 查看对象 226 是否被引用

query refered name *226*

type	ID	name
FW-POLICY	8155	

query type-by-name name <*string*> [**vsid** <*number*>]

命令描述：

显示对象所属的类型名称。

参数说明：

type-by-name	查看对象所属的类型名称
name	指定要查看的对象名
string	字符串，必须是已定义的对象名。
vsid	可选项，指定虚系统 ID 号。
number	数值

range

安全网关的地址范围对象管理，在此用户可以添加、修改或删除地址范围。

range add name <*string1*> **ip1** <*string2*> **ip2** <*string3*> [**except** <*string4*>] [**session** <*number1*>] [**synproxy** < on|off >] [**vsid** <*number2*>][**mss** < *number*>] [**dir** < src|dst>] [**session-per-second** < *number*>]

命令描述：

添加一个地址范围对象。

参数说明：

add	添加地址范围对象
name	设置地址范围对象的名称

string1	字符串，表示地址范围对象的名称
ip1	设置地址范围的起始 IP 地址
sting2	字符串，表示 IP 地址，格式为：0.0.0.0
ip2	设置地址范围的结束 IP 地址
string3	字符串，表示 IP 地址，格式为：0.0.0.0
except	设置地址范围中的排除地址
string4	字符串，表示 IP 地址，格式为：0.0.0.0
session	设置并发连接数
number1	数值，表示并发连接数
synproxy	SYN 代理开关
on|off	开/关
vsid	指定要在哪个虚系统上添加地址范围对象
number2	数值，安全网关上虚系统的标号
mss	最大传输大小
number	数值
dir	设置地址方向
src|dst	源/目的
session-per-second	每秒新建连接数
number	范围为 0-100000

使用说明：

ip1 的参数值应不大于ip2 的参数值，否则就会出现错误提示。Except的参数值应该在*Ipaddress1*和*Ipaddress2*指定的范围内。

在网络卫士安全网关的缺省配置已经有一个范围对象 any：0.0.0.0—255.255.255.255

同一时刻，应该是地址范围内所有地址各自的连接数不能大于该并发连接数。

实例：

** 添加地址范围对象 range1，其地址范围为：172.16.1.10—172.16.1.80

range add name *range1* **ip1** *172.16.1.10* **ip2** *172.16.1.80*

range modify name <*string1***> ip1** <*string2*> **ip2** <*string3*> [**except** <*string4*>] [**session** <*number*>] [**synproxy** < on|off >] [**vsid** <*number2*>][**mss** < *number*>] [**dir** < src|dst>] [**session-per-second** < *number*>]

命令描述：

修改一个地址范围对象。

参数说明：

modify	修改地址范围对象
name	设置要修改的地址范围对象的名称

string1	字符串，表示地址范围对象的名称
ip1	设置地址范围新的起始 IP 地址
sting2	字符串，表示 IP 地址，格式为：0.0.0.0
ip2	设置地址范围新的结束 IP 地址
string3	字符串，表示 IP 地址，格式为：0.0.0.0
except	设置地址范围中新的排除地址
string4	字符串，表示 IP 地址，格式为：0.0.0.0
session	设置并发连接数
number1	数值，表示并发连接数
synproxy	SYN 代理开关
on|off	开/关
vsid	指定要修改的地址范围对象所在的虚系统标号
number2	数值，安全网关上虚系统的标号
mss	最大传输大小
number	数值
dir	设置地址方向
src|dst	源/目的
session-per-second	每秒新建连接数
number	范围为 0-100000

使用说明：

同一时刻，地址范围内各主机的连接数之和不能大于该并发连接数。

实例：

** 修改 range1 对象的 IP 地址范围为：172.16.1.10—172.16.1.90

range modify name *range1* **ip1** *172.16.1.10* **ip2** *172.16.1.90*

range rename oldname <*string1*> **newname** <*string2*> [**vsid** <*number*>]

命令描述：

重新命名地址范围对象。

参数说明：

rename	重命名地址范围对象
oldname	指定要重新命名的地址范围对象名称
string1	字符串，表示地址范围对象名称（已定义的对象名称）
newname	指定新的地址范围对象名称
string2	字符串，表示地址范围对象的新名称
vsid	指定要重命名的地址范围对象所在的虚系统的标号
number	数值，安全网关上虚系统的标号

实例：

** 将地址范围对象 range1 重命名为 range2

range rename oldname *range1* **newname** *range2*

range delete [**id** <*number1*>] [**name** <*string*>] [**vsid** <*number2*>]

命令描述：

删除一个地址范围对象。如果该对象被规则引用，则无法删除。

参数说明：

delete	删除地址范围对象
id	指定要删除的地址范围对象对应的 ID 号
number1	数值，表示地址范围对象的 ID 号
name	指定要删除的地址范围对象的名称
string	字符串，表示地址范围对象名称
vsid	指定要删除的地址范围对象所在的虚系统标号
number2	数值，安全网关上虚系统的标号

使用说明：

在删除地址范围对象时，既可根据地址范围对象的名称来删除，又可以通过地址范围对象的 id 来删除，也可以同时指定 id 和 name，但是当两者不一致时以名称为准。

当不指定任何参数时，删除**未被策略引用的**地址范围对象。

实例：

** 删除地址范围对象 range1

range delete name *range1*

range clean [**vsid** <*number*>]

命令描述：

删除所有未被引用的地址范围对象。

参数说明：

clean	删除所有未被引用的地址范围对象
vsid	指定要删除那个虚系统上的所有地址范围对象
number	数值，安全网关上虚系统的标号

使用说明：

当不指定虚系统号时，默认删除虚系统 0 上的所有地址范围对象

实例：

** 清除安全网关系统上的所有未被引用的地址范围对象

range clean <cr>

range show [**vsid** <*number*>]

命令描述：

查看所有地址范围对象。

参数说明：

show	查看所有地址范围对象
vsid	指定要查看那个虚系统上的地址范围对象
number	数值，安全网关上虚系统的标号

实例：

** 查看地址范围对象

range show <cr>

schedule

安全网关的时间对象管理，在此用户可以添加、修改或删除时间对象。

schedule add name <*string1*> [**cyctype** <weekcyc >] [**week** <*string2*>] [**stime** <*string3*>] [**etime** <*string4*>] [**vsid** <*number*>]

命令描述：

添加一个多次时间对象，多次时间对象是指该时间对象包括多个不连续但有规律的时间段，例如每周二的上午 9 点到下午 17 点。

参数说明：

add	添加时间对象
name	设置时间对象的名称
string1	字符串，表示时间对象名称
cyctype	设置时间对象的类型，有 2 种 weekcyc 和 yearcyc，前者表示多次时间对象，后者表示单次时间对象
weekcyc	表示多次时间对象，例如每周一早 8 点到晚 8 点
week	设置时间对象的包括一周中的哪几天

string2	字符串，表示星期几，格式为：1234567（分别表示周一至周日）
stime	设置每天的开始时刻
string3	字符串，表示开始时刻，格式为：小时：分钟：秒
etime	设置每天的结束时刻，结束时刻的数值应该大于开始时刻
string4	字符串，表示结束时刻，格式为：小时：分钟：秒
vsid	指定要在哪个虚系统上添加时间对象
number	数值，安全网关上虚系统的标号

使用说明：

当指定“week”参数包括多个时间段时，中间不输入任何分隔符，如 12 表示星期一、二。

实例：

** 添加时间对象 week1，其时间段为每周三上午 10 点到下午 18 点

schedule add name *week1* **cyctype** weekcyc **week** *3* **stime** *10:00:00* **etime** *18:00:00*

schedule add name <*string1*> [**cyctype** <yearcyc>] [**start** <*string2*>] [**stime** <*string3*>] [**etime** <*string4*>] [**sdate** <*string5*>] [**edate** <*string6*>] [**vsid** <*number*>]

命令描述：

添加一个单次时间对象，单次时间对象是指该时间对象只包括一个时间段，例如 2007 年 1 月 1 日 0 点到 2007 年 12 月 12 日 23 点。

参数说明：

add	添加时间对象
name	设置时间对象的名称
string1	字符串，表示时间对象名称
cyctype	设置时间对象的类型，有 2 种 weekcyc 和 yearcyc，前者表示多次时间对象，后者表示单次时间对象
yearcyc	表示单次时间对象，例如 2010 年 4 月 7 日上午 10 点到 2010 年 4 月 8 日下午 18 点
start	设置开始时间
string2	字符串，表示开始时间，默认为开始一分钟
stime	设置开始的具体时间，
string3	字符串，格式为：小时：分钟：秒，默认为 00：00：00
etime	设置结束的时间
string4	字符串，格式为：小时：分钟：秒，默认为 00：00：00
sdate	设置开始日期
string5	字符串，格式为：年-月-天
edate	设置结束日期

string6	字符串，格式为：年-月-天
vsid	指定要在哪个虚系统上添加时间对象
number	数值，安全网关上虚系统的标号

实例：

** 添加时间对象 year1，其时间段为 2010 年 4 月 7 日上午 10 点到 2010 年 4 月 8 日下午 18 点

schedule add name year1 **stime** *10:00:00* **etime** *18:00:00* **sdate***2010-04-07* **edate** *2010-04-08*

schedule modify name <*string1*> [**type** <weekcyc >] [**week** <*string2*>] **stime** <*string3*>] [**etime** <*string4*>] [**vsid** <*number*>]

命令描述：

修改一个多次时间对象，多次时间对象是指该时间对象包括多个不连续但有规律的时间段，例如每周二的上午 9 点到下午 5 点。

参数说明：

modify	修改时间对象
name	指定要修改的时间对象的名称
string1	字符串，表示时间对象名称
type	制定要修改的时间对象的类型，有 2 种 weekcyc 和 yearcyc，前者表示多次时间对象，后者表示单次时间对象
weekcyc	表示多次时间对象，例如每周一早 8 点到晚 8 点
week	修改时间对象一周中包括哪几天
string2	字符串，表示星期几，格式为：1234567（分别表示周一至周日）
stime	修改每天的开始时刻
string3	字符串，表示开始时刻，格式为：小时：分钟：秒
etime	修改每天的结束时刻
string4	字符串，表示结束时刻，格式为：小时：分钟：秒
vsid	指定要在哪个虚系统上修改时间对象
number	数值，安全网关上虚系统的标号

实例：

** 将时间对象 week1 的时间段改为每周 1 上午 9 点到下午 16 点

schedule modify name *week1* **type** weekcyc **week** *1* **stime** *09:00:00* **etime** *16:00:00*

schedule modify name <*string1*> [**cyctype** <*yearcyc*>] [**start** <*string2*>] [**stime** <*string3*>] [**etime** <*string4*>] [**sdate** <*string5*>] [**edate** <*string6*>] [**vsid** <*number*>]

命令描述：

修改一个单次时间对象，单次时间对象是指该时间对象只包括一个时间段，例如 2007 年 1 月 1 日 0 点到 2007 年 12 月 12 日 23 点。

参数说明：

add	添加时间对象
name	指定要修改时间对象的名称
string1	字符串，表示时间对象名称
cyctype	指定要修改的时间对象的类型，有 2 种 weekcyc 和 yearcyc，前者表示多次时间对象，后者表示单次时间对象
yearcyc	表示多次时间对象，例如每周一早 8 点到晚 8 点
string2	字符串，表示星期几，格式为：1234567（分别表示周一至周日）
start	指定要修改的开始时间
string2	字符串，表示开始时间，默认为开始一分钟
stime	指定要修改的开始的具体时间，
string3	字符串，格式为：小时：分钟：秒，默认为 00：00：00
etime	指定要修改的结束的时间
string4	字符串，格式为：小时：分钟：秒，默认为 00：00：00
sdate	指定要修改的开始日期
string5	字符串，格式为：年-月-天
edate	指定要修改的结束日期
string6	字符串，格式为：年-月-天
vsid	指定要在哪个虚系统上修改时间对象
number	数值，安全网关上虚系统的标号

实例：

** 将时间对象 year1 的时间段改为 2010 年 4 月 7 日 10 点至 2010 年 4 月 8 日 23 点。

schedule modify name year1**stime** *10:00:00* **etime** *23:00:00* **sdate***2010-04-07* **edate** *2010-04-08*

schedule rename oldname <*string1*> **newname** <*string2*> [**vsid** <*number*>]

命令描述：

重新命名时间对象。

参数说明：

rename	重命名时间对象

oldname	指定要重新命名的时间对象名称
string1	字符串，表示时间对象名称（已定义的对象名称）
newname	指定新的时间对象名称
string2	字符串，表示时间对象的新名称
vsid	指定要重命名的时间对象所在的虚系统的标号
number	数值，安全网关上虚系统的标号

实例：

** 将时间对象 week1 重命名为 week2

schedule rename oldname *week1* **newname** *week2*

schedule delete [**id** <*number1*>] [**name** <*string*>] [**vsid** <*number2*>]

命令描述：

删除一个时间对象。如果该对象被规则引用，则无法删除。

参数说明：

delete	删除一个时间对象
id	指定要删除的时间对象对应的 ID 号
number1	数值，表示时间址对象的 ID 号
name	指定要删除的时间对象的名称
string	字符串，表示时间对象名称
vsid	指定要删除时间对象所在的虚系统标号
number2	数值，安全网关上虚系统的标号

使用说明：

在删除时间对象时，既可根据时间对象的名称来删除，又可以通过时间对象的 id 来删除，也可以同时指定 id 和 name，但是当两者不一致时以名称为准。

当不指定任何参数时，删除**未被策略引用的**时间对象。

实例：

** 删除时间对象 week1

schedule delete name *week1*

schedule clean [**cyctype** <yearcyc|weekcyc>] [**vsid** <*number*>]

命令描述：

删除所有未被引用的时间对象。

参数说明：

clean	删除所有未被引用的时间对象
cyctype	指定要清空哪种类型的时间对象，有 2 种 weekcyc 和 yearcyc
yearcyc|weekcyc	yearcyc 表示单次时间对象，weekcyc 表示多次时间对象
vsid	指定要删除那个虚系统上的所有时间对象
number	数值，安全网关上虚系统的标号

使用说明：

当不指定虚系统号时，默认删除虚系统 0 上的所有时间对象

实例：

** 清除安全网关系统上的所有未被引用的单次时间对象

schedule clean cyctype yearcyc

schedule show [**cyctype** <yearcyc|weekcyc>] [**vsid** <*number*>]

命令描述：

查看所有时间对象。

参数说明：

show	查看所有时间对象
cyctype	指定要查看哪种类型的时间对象，有 2 种 weekcyc 和 yearcyc
yearcyc|weekcyc	yearcyc 表示单次时间对象，weekcyc 表示多次时间对象
vsid	指定要查看那个虚系统上的时间对象
number	数值，安全网关上虚系统的标号

实例：

** 查看安全网关系统上的多次时间对象

schedule show cyctype weekcyc

server

安全网关的服务器对象管理，在此用户可以添加、修改或删除服务器对象，此处的服务器对象主要用于安全网关的负载均衡功能。

server add name <*string1*> **host** <*string2*> [**weight**<*number1*>] [**probe** <none|host|service>] [**port** <*number2*>] [**vsid** <*number3*>]

命令描述：

添加一个服务器对象。

参数说明：

Add	添加服务器对象
name	设置服务器对象的名称
string1	字符串，表示服务器对象的名称
host	设置服务器使用的主机
string2	字符串，表示主机名称
weight	设置服务器的权重
number1	数值，表示服务器的权重，取值范围为 1—100
probe	设置是否要对服务器进行探测，共有三种选项：none、host 和 service
none|host|service	none 表示不作探测；host 表示进行主机探测；service 表示进行服务探测，当用户选择服务探测时还需要设置探测的端口
port	设置探测端口，只有选择了服务探测时才需要设置端口
number2	数值，表示端口号
vsid	指定要在哪个虚系统上添加服务器对象
number3	数值，安全网关上虚系统的标号

使用说明：

通过探测，可以检测服务器的工作状态，可以避免在该服务器宕机或服务异常的情况下仍旧发送流量到该服务器，造成用户请求的服务不能得到响应的情况。探测的方式可以是主机探测或服务探测，主机探测是通过简单的 PING 命令进行定时监测来确定服务器是否在线，而服务探测是根据服务器提供的服务选择相应的端口通过建立 tcp 连接进行探测，如 HTTP 的 80 端口、FTP 的 21 端口或用户自定义的特殊端口。一般来说，服务探测比较能够真实反映服务器的工作状态。

实例：

** 添加服务器对象 server1，主机为 host1，权重为 20，并设置为服务探测，探测端口 8080

server add name *server1* **host** *host1* **weight** *20* **probe** *service* **port** *8080*

server modify name <*string1*> [**host** <*string2*>] [**weight**<*number1*>] [**probe** <none|host|service>] [**port** <*number2*>] [**vsid** <*number3*>]

命令描述：

修改一个服务器对象。

参数说明：

modify	修改服务器对象
name	设置要修改的服务器对象的名称
string1	字符串，表示服务器对象的名称
host	修改服务器使用的主机
string2	字符串，表示主机名称
weight	修改服务器的权重
number1	数值，表示服务器的权重，取值范围为 1—100
probe	设置是否要对服务器进行探测，共有三种选项：none、host 和 service
none|host|service	none 表示不作探测；host 表示进行主机探测；service 表示进行服务探测，当用户选择服务探测时还需要设置探测的端口
port	修改探测端口，只有选择了服务探测时才需要端口
number2	数值，表示端口号
vsid	指定要在哪个虚系统上修改服务器对象
number3	数值，安全网关上虚系统的标号

实例：

** 修改服务器对象 server1，将主机改为 host2

server modify name *server1* **host** *host2*

server rename oldname <*string1*> **newname** <*string2*> [**vsid** <*number*>]

命令描述：

重新命名服务器对象。

参数说明：

rename	重命名服务器对象
oldname	指定要重新命名的服务器对象名称
string1	字符串，表示服务器对象名称（已定义的对象名称）
newname	为服务器对象指定新的名称
string2	字符串，表示服务器对象的新名称
vsid	指定要重命名的服务器对象所在的虚系统的标号
number	数值，安全网关上虚系统的标号

实例：

** 将服务器对象 server1 重命名为 server2

server rename oldname *server1* **newname** *server2*

server delete [**id** <*number1*>] [**name** <*string*>] [**vsid** <*number2*>]

命令描述：

删除一个服务器对象。如果该对象被规则引用，则无法删除。

参数说明：

delete	删除服务器对象
id	指定要删除的服务器对象对应的 ID 号
number1	数值，表示服务器对象的 ID 号
name	指定要删除的服务器对象的名称
string	字符串，表示服务器对象名称
vsid	指定要删除服务器对象所在的虚系统标号
number2	数值，安全网关上虚系统的标号

使用说明：

在删除服务器对象时，既可根据服务器对象的名称来删除，又可以通过服务器对象的 id 来删除，也可以同时指定 id 和 name，但是当两者不一致时以名称为准。

当不指定任何参数时，删除**未被策略引用的**服务器对象。

实例：

** 删除服务器对象 server1

server delete name *server1*

server clean [**vsid** <*number*>]

命令描述：

删除所有未被引用的服务器对象。

参数说明：

clean	删除所有未被引用的服务器对象
vsid	指定要删除那个虚系统上的所有服务器对象
number	数值，安全网关上虚系统的标号

使用说明：

当不指定虚系统号时，默认删除虚系统 0 上的所有服务器对象

实例：

** 清除安全网关系统上的所有未被引用的服务器对象

server clean <cr>

server show [**vsid** <*number*>]

命令描述：

查看所有服务器对象。

参数说明：

show	查看所有服务器对象
vsid	指定要查看那个虚系统上的服务器对象
number	数值，安全网关上虚系统的标号

实例：

** 查看服务器对象

server show <cr>

service

某些服务器采用非标准的端口来提供服务，如通过 8080 端口来提供 HTTP 服务，如果安全网关缺少这类信息，它就无法正确地对该服务进行解码。对这些特殊的服务，就需要管理员在网络卫士安全网关上自行进行定义。“Service”便提供了定义服务对象的功能，在此用户可以添加、修改或删除服务对象。

service add name <*string1*> **protocol** <*number1*> **port** <*number2*>[**port2** <*number3*>]

[**comment** <*string2*>] [**vsid** <*number4*>]

命令描述：

添加一个服务对象。

参数说明：

add	添加服务对象
name	设置服务对象的名称
string1	字符串，表示自定义服务对象的名称
protocol	设置 3 层或 4 层协议码
number1	数值，表示协议码
port	设置服务的起始端口，只有一个端口时只须设置起始端口，不用设置结束端口
number2	数值，表示起始端口号
port2	设置服务的结束端口
number3	数值，表示结束端口号
comment	设置备注内容
string2	字符串，表示备注内容

vsid	指定要在哪个虚系统上添加服务对象
number4	数值，安全网关上虚系统的标号

使用说明：

服务分为系统提供的缺省服务和用户自定义服务，对于缺省服务用户无法进行添加、删除、修改等操作。

实例：

** 添加服务对象 http8080，设置协议码为 6、端口号为 8080

service add name *http8080* **protocol** *6* **port** *8080*

service modify name <*string1*> [**protocol** <*number1*>] [**port** <*number2*>] [**port2** <*number3*>] [**comment** <*string2*>] [**vsid** <*number4*>]

命令描述：

修改一个自定义服务对象。

参数说明：

modify	修改服务对象
name	指定要修改的服务对象的名称
string1	字符串，表示自定义服务对象的名称
protocol	重新设置 3 层或 4 层协议码
number1	数值，表示协议码
port	修改服务的起始端口，只有一个端口时只须设置起始端口，不用设置结束端口
number2	数值，表示起始端口号
port2	修改服务的结束端口
number3	数值，表示结束端口号
comment	修改备注内容
string2	字符串，表示备注内容
vsid	指定要修改的服务对象所在的虚系统的标号
number4	数值，安全网关上虚系统的标号

实例：

** 将服务对象 http8080 的端口号改为 8000

service modify name *http8080* **port** *8000*

service rename oldname <*string1*> **newname** <*string2*> [**vsid** <*number*>]

命令描述：

重新命名自定义服务对象。

参数说明：

rename	重命名服务对象
oldname	指定要重新命名的服务对象名称
string1	字符串，表示服务对象名称（已定义的对象名称）
newname	指定新的服务对象名称
string2	字符串，表示服务对象的新名称
vsid	指定要重命名的服务对象所在的虚系统的标号
number	数值，安全网关上虚系统的标号

实例：

** 将服务对象 http8080 重命名为 http8000

service rename oldname *http8080* **newname** *http8000*

service delete [**id** <*number1*>] [**name** <*string*>] [**vsid** <*number2*>]

命令描述：

删除一个自定义服务对象。如果该对象被规则引用，则无法删除。

参数说明：

delete	删除服务对象
id	指定要删除的服务对象对应的 ID 号
number1	数值，表示服务对象的 ID 号
name	指定要删除的服务对象的名称
string	字符串，表示服务对象名称
vsid	指定要删除服务对象所在的虚系统标号
number2	数值，安全网关上虚系统的标号

使用说明：

在删除服务对象时，既可根据服务对象的名称来删除，又可以通过服务对象的 id 来删除，也可以同时指定 id 和 name，但是当两者不一致时以名称为准。

当不指定任何参数时，删除**未被策略引用的**服务对象。

实例：

** 删除服务对象 http8000

service delete name *http8000*

service clean [**vsid** <*number*>]

命令描述：

删除所有未被引用的自定义服务对象。

参数说明：

clean	删除所有未被引用的字定义服务对象
vsid	指定要删除哪个虚系统上的所有自定义服务对象
number	数值，安全网关上虚系统的标号

使用说明：

当不指定虚系统号时，默认删除虚系统 0 上的所有自定义服务对象

实例：

** 清除安全网关系统上的所有自定义服务对象

service clean <cr>

service show [custom|default] [**vsid** <*number*>]

命令描述：

查看所有服务对象。

参数说明：

show	查看所有服务对象
custom|default	指定要查看的服务类型，custom 表示用户自定义的服务，default 表示安全网关系统中的默认服务（无需用户定义）
vsid	指定要查看哪个虚系统上的服务对象
number	数值，安全网关上虚系统的标号

实例：

** 查看安全网关系统上的自定义服务

service show custom

subnet

安全网关的子网对象管理，在此用户可以添加、修改或删除子网。

subnet add name <*string1*> **ipaddr** <*ipaddress*> **mask** <*netmask*> [**except** <*string2*>][**session**

<*number1*>] [**synproxy** < on|off >] [**vsid** <*number2*>][**mss** < *number*>] [**dir** < src|dst>]

[**session-per-second** < *number*>]

命令描述：

添加一个子网对象。

参数说明：

add	添加子网对象
name	设置子网对象的名称
string	字符串，表示子网对象的名称
ipaddr	设置子网地址
ipaddress	字符串，表示子网地址，例如 192.168.8.0
mask	设置子网掩码
netmask	字符串，表示子网掩码，例如 255.255.255.0
except	设置子网中的排除地址
string2	字符串，表示要排除的 IP 地址，格式为：0.0.0.0
session	设置并发连接数。
number1	数值，表示并发连接数
synproxy	设置 SYN 代理开关
on|off	开/关
vsid	指定要在哪个虚系统上添加子网对象
number2	数值，安全网关上虚系统的标号
mss	最大传输大小
number	数值
dir	设置地址方向
src|dst	源/目的
session-per-second	每秒新建连接数
number	范围为 0-100000

使用说明：

同一时刻，子网内所有地址各自的连接数不能大于该并发连接数。

实例：

** 添加子网对象 subnet1，其子网地址为：192.168.10.0，掩码为：255.255.255.0

subnet add name *subnet1* **ipaddr** *192.168.10.0* **mask** *255.255.255.0*

subnet modify name <*string1*> [**ipaddr** <*ipaddress*>] [**mask** <*netmask*>] [**except** <*string2*>]

[**session** <*number1*>] [**synproxy** < on|off >] [**vsid** <*number2*>][**mss** < *number*>] [**dir** < src|dst>]

[**session-per-second** < *number*>]

命令描述：

修改一个子网对象。

参数说明：

modify	修改子网对象
name	指定要修改的子网对象的名称
string	字符串，表示子网对象的名称
ipaddr	设置新的子网地址
ipaddress	字符串，表示子网地址，例如 192.168.8.0
mask	设置新的子网掩码
netmask	字符串，表示子网掩码，例如 255.255.255.0
except	设置子网中新的排除地址
string2	字符串，表示要排除的 IP 地址，格式为：0.0.0.0
session	设置新的并发连接数。
number1	数值，表示并发连接数
synproxy	设置 SYN 代理开关
on|off	开/关
vsid	修改该子网对象所属的虚系统
number2	数值，安全网关上虚系统的标号
mss	最大传输大小
number	数值
dir	设置地址方向
src|dst	源/目的
session-per-second	每秒新建连接数
number	范围为 0-100000

使用说明：

同一时刻，子网内各主机的连接数之和不能大于该并发连接数。

实例：

** 修改 subnet1 对象的 IP 地址为：192.168.20.0

subnet modify name *subnet1* **ipaddr** *192.168.20.0*

subnet rename oldname <*string1*> **newname** <*string2*> [**vsid** <*number*>]

命令描述：

重新命名子网对象。

参数说明：

rename	重命名子网对象
oldname	指定要重新命名的子网对象名称
string1	字符串，表示子网对象名称（已定义的对象名称）
newname	指定新的子网对象名称
string2	字符串，表示子网对象的新名称
vsid	指定要重命名的子网对象所在的虚系统的标号
number	数值，安全网关上虚系统的标号

实例：

** 将子网对象 subnet1 重命名为 subnet2

subnet rename oldname *subnet1* **newname** *subnet2*

subnet delete [**id** <*number1*>] [**name** <*string*>] [**vsid** <*number2*>]

命令描述：

删除一个子网对象。如果该对象被规则引用，则无法删除。

参数说明：

delete	删除一个子网对象
id	指定要删除的子网对象对应的 ID 号
number1	数值，表示子网对象的 ID 号
name	指定要删除的子网对象的名称
string	字符串，表示子网对象名称
vsid	指定要删除的子网对象所在的虚系统标号
number2	数值，安全网关上虚系统的标号

使用说明：

在删除子网对象时，既可根据子网对象的名称来删除，又可以通过子网对象的 id 来删除，也可以同时指定 id 和 name，但是当两者不一致时以名称为准。

当不指定任何参数时，删除**未被策略引用的**子网对象。

实例：

** 删除子网对象 subnet1

subnet delete name *subnet1*

subnet clean [**vsid** <*number*>]

命令描述：

删除所有未被引用的子网对象。

参数说明：

clean	删除所有未被引用的子网对象
vsid	指定要删除那个虚系统上的所有子网对象
number	数值，安全网关上虚系统的标号

使用说明：

当不指定虚系统号时，默认删除虚系统 0 上的所有子网对象

实例：

** 清除安全网关系统上的所有子网对象

subnet clean <cr>

subnet show [**vsid** <*number*>]

命令描述：

查看所有子网对象。

参数说明：

show	查看所有子网对象
vsid	指定要查看那个虚系统上的子网对象
number	数值，安全网关上虚系统的标号

实例：

** 查看子网对象

subnet show <cr>

virtual_server

安全网关的均衡组对象管理，在此用户可以添加、修改或删除均衡组。

virtual_server add name <*string1*> [**server** <*string2*>] [**balance**<rr|wrr|lc|wlc|sh|dh>] [**backup** <*number1*>] [**vsid** <*number2*>]

命令描述：

添加一个均衡组对象。

参数说明：

add	添加均衡组对象
name	设置均衡组对象的名称
string1	字符串，表示均衡组对象的名称
server	设置均衡组中包含的服务器
string2	字符串，表示服务器名称，输入多个时用单引号括起来，之间用空格分割，例如'*server1 server2*'
balance	设置负载均衡方式，共有 6 种可选方式：rr、wrr、lc、wlc、

	sh 和 dh
rr|wrr|lc|wlc|sh|dh	“rr”表示顺序选择负载均衡组中的服务器；“wrr”表示根据权重顺序选择负载均衡服务器；“lc”表示根据连接响应时间选择服务器，响应时间最快的被优先选择；“wlc”表示根据响应时间和权重选择服务器，响应时间短、权重大的服务器被优先选择；“sh”表示根据源地址作 HASH 查找来确认被选择的服务器；“dh”则表示根据目的地址作 HASH 查找来确认选择哪个负载均衡服务器。
backup	设置备份均衡组的 ID。当本组中的所有服务器均停止服务时，负载均衡组中服务器的内容将备份到指定的负载均衡组
number1	数值，表示均衡组 ID 号
vsid	指定要在哪个虚系统上添加均衡组对象
number2	数值，安全网关上虚系统的标号

使用说明：

在通信过程中，如果从负载均衡组中删除一台服务器，已经与该服务器建立的连接并不会断开，只有重新建立连接后，负载均衡组的配置才会生效。

通信中，如果所连接的服务器断开，客户机不会自动连接到负载均衡组中的其它服务器，除非重新建立连接。

当负载均衡方式设置为带权值的算法时，连接总数按权值分配，权值并不是优先级。

“dh”和“sh”算法是根据 IP 地址来进行 HASH 查找的，只有源或目的 IP 分散的情况，连接才会均分到不同的服务器上。

在定义均衡组之前，需要先定义均衡服务器对象，关于地址对象的定义请参考 define host 命令。

实例：

** 添加均衡组对象 virtual_server1，其包含的服务器为 server1 和 server2

virtual_server add name *virtual_server1* **server** *‘server1 server2’*

virtual_server modify name <*string1*> [**server** <*string2*>] [**balance**<rr|wrr|lc|wlc|sh|dh>] [**backup** <*number1*>] [**vsid** <*number2*>]

命令描述：

修改一个均衡组对象。

参数说明：

modify	修改均衡组对象

name	指定要修改的均衡组的名称
string1	字符串，表示均衡组的名称
server	修改均衡组中包含的服务器
string2	字符串，表示服务器名称
balance	修改负载均衡方式，共有 6 种可选方式：rr、wrr、lc、wlc、sh 和 dh
rr|wrr|lc|wlc|sh|dh	“rr”表示顺序选择负载均衡组中的服务器；“wrr”表示根据权重顺序选择负载均衡服务器；“lc”表示根据连接响应时间选择服务器，响应时间最快的被优先选择；“wlc”表示根据响应时间和权重选择服务器，响应时间短、权重大的服务器被优先选择；“sh”表示根据源地址作 HASH 查找来确认被选择的服务器；“dh”则表示根据目的地址作 HASH 查找来确认选择哪个负载均衡服务器。
backup	修改备份均衡组的 ID。当本组中的所有服务器均停止服务时，负载均衡组中服务器的内容将备份到指定的负载均衡组
number1	数值，表示均衡组 ID 号
vsid	指定要在哪个虚系统上修改均衡组对象
number2	数值，安全网关上虚系统的标号

实例：

** 将均衡组对象 virtual_server1 的服务器改为 server1 和 server3

virtual_server modify name *virtual_server1* **server** *‘server1 server3’*

virtual_server rename oldname <*string1*> **newname** <*string2*> [**vsid** <*number*>]

命令描述：

重新命名均衡组对象。

参数说明：

rename	重命名均衡组对象
oldname	指定要重新命名的均衡组对象名称
string1	字符串，表示均衡组对象名称（已定义的对象名称）
newname	指定新的均衡组对象名称
string2	字符串，表示均衡组对象的新名称
vsid	指定要重命名的均衡组对象所在的虚系统的标号
number	数值，安全网关上虚系统的标号

实例：

** 将均衡组对象 virtual_server 1 重命名为 virtual_server 2

virtual_server rename oldname *virtual_server1* **newname** *virtual_server2*

virtual_server delete [**id** <*number1*>] [**name** <*string*>] [**vsid** <*number2*>]

命令描述：

删除一个均衡组对象。如果该对象被规则引用，则无法删除。

参数说明：

delete	删除均衡组对象
id	指定要删除的均衡组对象对应的 ID 号
number1	数值，表示均衡组对象的 ID 号
name	指定要删除的均衡组对象的名称
string	字符串，表示均衡组对象名称
vsid	指定要删除的均衡组对象所在的虚系统标号
number2	数值，安全网关上虚系统的标号

使用说明：

在删除均衡组对象时，既可根据均衡组对象的名称来删除，又可以通过均衡组对象的 id 来删除，也可以同时指定 id 和 name，但是当两者不一致时以名称为准。

当不指定任何参数时，删除**未被策略引用的**均衡组对象。

实例：

** 删除均衡组对象 virtual_server1

virtual_server delete name *virtual_server1*

virtual_server clean [**vsid** <*number*>]

命令描述：

删除所有未被引用的均衡组。

参数说明：

clean	删除所有未被引用的均衡组
vsid	指定要删除那个虚系统上的所有均衡组
number	数值，安全网关上虚系统的标号

使用说明：

当不指定虚系统号时，默认删除虚系统 0 上的所有均衡组对象

实例：

** 清除安全网关系统上的所有均衡组

virtual_server clean <cr>

virtual_server show [**vsid** <*number*>]

命令描述：

查看所有均衡组对象。

参数说明：

show	查看所有均衡组
vsid	指定要查看那个虚系统上的均衡组对象
number	数值，安全网关上虚系统的标号

实例：

** 查看均衡组对象

virtual_server show <cr>

DPI

深度报文检测模块。

网关可以通过 DPI 对应用层的访问进行应用层内容过滤，从而实施更细粒度的访问控制。目前网关支持的 DPI 包括： FTP，HTTP, POP3, SMTP，RSH，IMAP，TELNET 和 DNS。

要使此处定义的应用层内容过滤规则生效还必须使用 filewall policy 策略来引用。DPI 实行第一匹配原则，即当两条或以上的策略策略源、策略目的、服务均相同时，只有第一条策略的 DPI 生效。

进入本命令模块操作如下：

#dpi<cr>

退出本命令模块操作如下：

#end<cr>

CLI 管理员登录网关进入本命令模块后，可以执行相应的组件管理命令。下面将详细描述本命令模块下的所有组件管理命令。命令的实例输入格式将按已经进入本命令模块书写。

下一级命令列表

命令	功能
dns	DNS 过滤策略设置
freemem	查看系统空闲内存
ftp	FTP 协议内容过滤规则设置

global	DPI 全局参数设置
http	HTTP 协议内容过滤规则设置
imap	IMAP 协议内容过滤规则设置
max-connection	设置最大连接数
pattern	关键字对象定义
policy	应用协议端口绑定设置
pop3	POP3 协议内容过滤规则设置
rsh	RSH 协议内容过滤规则设置
rule	保护内容表设置
smtp	SMTP 协议内容过滤规则设置
telnet	Telnet 协议内容过滤规则设置
webfilter	WEB 过滤策略设置

dns

网络卫士安全网关的 DNS 策略用于对通过的 DNS 查询请求进行域名过滤。通过定义 DNS 关键字，并在保护内容表中引用该关键字对象，当通过设备的 DNS 查询报文匹配选中的关键字对象时，根据关键字对象的权限对域名查询进行过滤或转发处理；否则系统将按照与关键字权限相反的权限对数据进行处理。

dns add name <*string*> [**domain-name** <*keyword*>] [**log** [on|off]]

命令描述：

添加一条 DNS 过滤策略。

参数说明：

add	添加一条 DNS 过滤策略
name	设置策略的名称
string	字符串，表示策略的名称
domain-name	可选项，选择已经定义的 DNS 协议的关键字对象，设置进行 DNS 域名过滤的报文具备的特征。当通过设备的 DNS 查询报文匹配选中的关键字对象时，根据关键字对象的权限对命令进行处理。
keyword	字符串，必须是已经定义的 DNS 协议的关键字对象。
log	可选项，当有符合该规则的数据报文被截获时是否在系统日志中作相关记录。默认不作记录。
on|off	做记录/不做记录

使用说明：

同一个策略中最多能引用 16 个关键字对象。

实例：

** 添加 DNS 过滤策略 mail，匹配的关键字为 topsec，默认权限为“允许”，且不记录日志信息。

dns add name *mail* **domain-name** *topsec*

dns clean <cr>

命令描述：

清除所有 DNS 策略。

dns delete name <*string*>

命令描述：

删除一条 DNS 策略。

参数说明：

delete	删除一条 DNS 策略
name	DNS 策略名称
string	字符串

实例：

**删除一条 DNS 策略

dns delete name *dns深度过滤*

dns modify name <*string*> [**domain-name** <*keyword*>] [**log** [on|off]]

命令描述：

修改一条 DNS 过滤策略。

参数说明：

modify	修改一条 DNS 过滤策略
name	设置策略的名称
string	字符串，表示策略的名称
domain-name	可选项，选择已经定义的 DNS 协议的关键字对象，设置进行 DNS 域名过滤的报文具备的特征。当通过设备的 DNS 查询报文匹配选中的关键字对象时，根据关键字对象的权限对命令进行处理。
keyword	字符串，必须是已经定义的 DNS 协议的关键字对象。
log	可选项，当有符合该规则的数据报文被截获时是否在系统日志中作相关记录。默认不作记录。
on|off	做记录/不做记录

dns show [**name**<*string*>]

命令描述：

显示所有或指定的 DNS 策略。

参数说明：

show	显示所有或指定 DNS 策略
name	策略名称
string	字符串

使用说明：

指定对象名时，显示指定对象的属性；不指定对象名时，显示所有 DNS 对象。

实例：

**显示所有 DNS 策略

dns show <cr>

freemem

查看系统空闲内存，单位为 KB。

freemem show<cr>

命令描述：

显示空闲内存大小，单位为 KB。。

ftp

FTP 策略配置。

定义访问控制规则时，管理员可以以一个 FTP 策略作为过滤条件，来控制使用 FTP 协议对文件的上传下载。这里的 FTP 策略的组成要素有：文件名控制、FTP 默认权限、登陆标题、是否记录日志等信息。其中文件名是指一组定义了权限的关键字对象，在进行 FTP 传输时的目标文件名称中如果包含该 FTP 策略中的关

键字将按照定义的权限处理。否则系统将按照与关键字权限相反的权限对数据进行处理。

ftp add name <*string1*> [**filename** <*string*>] [**access** <rwxn>] [**banner** <*string2*>][**log** <on|off>] [**cmd** < *string*>]

命令描述：

添加一条 FTP 策略。

参数说明：

add	添加一条 FTP 策略
name	FTP 策略名
string1	字符串
filename	可选项，引用的关键字对象名称，默认为空。
string	可以为多个字符串
access	可选项，设定访问权限，默认为 rw。
rwxn	字符串，只能是 r（读）、w（写）、x（执行）、n（没有任何权限）的组合，例如 rw 分别表示 ftp 下载、上传权限。
banner	可选项，替换 FTP 服务器向客户端返回的登录标题信息，保护服务器的版本信息不被暴露。默认为空。
string2	字符串
log	可选项，当有符合该规则的数据报文被截获时是否在系统日志中作相关记录。默认为空。
on|off	做记录/不做记录
cmd	可选项，设置禁止传输的 FTP 命令
string	字符串，可选项为 STOR、RETR、APPE、 DELE、RNFR、LIST、MKD 和 RMD，输入时可以不区分大小写。可以通过**#ftp cmd show**<cr>查看。 说明： STOR: 上传 RETR: 下载 APPE: 追加 DELE: 删除文件 RNFR: 重命名 LIST: 列表 MKD: 创建目录 RMD: 删除目录

实例：

**添加一条 FTP 策略

ftp add name *ftp深度过滤* **filename** *禁止rar文件类型* **access** rw **log** on

ftp clean <cr>

命令描述：

清除所有 ftp 策略。

ftp cmd show <cr>

命令描述：

显示支持过滤的 ftp 命令。

ftp delete name <*string*>

命令描述：

删除一条 ftp 策略。

参数说明：

delete	删除一条 ftp 策略
name	ftp 策略名称
string	字符串

实例：

**删除一条 ftp 策略

ftp delete name *ftp深度过滤*

ftp modify name <*string1*> **filename** <*string*> [**access** <rwxn>] [**banner** <*string2*>][**log** <on|off>][**cmd** < *string*>]

命令描述：

修改一条 FTP 策略。

参数说明：

modify	修改一条 FTP 策略
name	FTP 策略名
string1	字符串
filename	引用的关键字对象名称
string	可以为多个字符串
access	设定访问权限
rwxn	字符串，只能是 r（读）、w（写）、x（执行）、n（没有任何权限）的组合，例如 rw 分别表示 ftp 下载、上传权限。

banner	替换 FTP 服务器向客户端返回的登录标题信息，保护服务器的版本信息不被暴露。
string2	字符串
log	当有符合该规则的数据报文被截获时是否在系统日志中作相关记录。
on|off	做记录/不做记录
cmd	可选项，设置禁止传输的 FTP 命令
string	字符串

实例：

**修改一条 FTP 策略的权限为只允许下载，禁止上传。

ftp modify name *ftp深度过滤* **filename** *‘禁止rar文件类型’* **access** r **log** on

ftp show [**name**<*string*>]

命令描述：

显示所有或指定的 ftp 策略。

参数说明：

show	显示所有或指定 ftp 策略
name	ftp 策略名称
string	字符串

使用说明：

指定对象名时，显示指定对象的属性；不指定对象名时，显示所有 ftp 对象。

实例：

**显示所有 ftp 策略

ftp show <cr>

global

DPI 全局参数设置。网络卫士安全网关检查通过设备接收和发送的邮件，当邮件匹配 SMTP DPI 策略、POP3 DPI 策略时，根据策略设置，可能丢弃该邮件的全部或其附件，也可能将原邮件转发到指定人员。丢弃邮件处理时，安全网关系统将向指定人员发送替换邮件，替换邮件的主题和内容可以使用系统默认设置，管理员也可以进行更改。将原邮件转发到指定的收件人时，需要管理员设置收件人、发件人的地址信息，邮件帐户名和密码信息，以及该帐户的 SMTP 服务器地址。

global mail-warning reset<cr>

命令描述：

将邮件告警的相关参数恢复默认配置。

global mail-warning body<*string*> [**subject** <*string*>]

命令描述：

设置告警邮件的主题及邮件内容。

参数说明：

body	设置邮件内容
string	字符串，
subject	可选项，设置邮件主题。默认为“此邮件违反了安全策略”。
string	字符串。长度小于 64 个字符。

实例：

**修改告警邮件的内容

global mail-warning body *‘请注意，您已违反本公司安全策略！’*

global mail-warning show<cr>

命令描述：

查看邮件告警的相关参数配置。

global webfilter-update local filename <*string***> server-ip <***ipaddress***>**

命令描述：

分类库本地升级相关配置。

参数说明：

local	分类库本地升级
filename	设置升级文件名
string	字符串
server-ip	设置服务器 IP 地址。
ipaddress	字符串。

global webfilter-update remote<cr>

命令描述：

分类库远程升级 URL 恶意库。

global webfilter-update set time <*string*>

命令描述：

分类库每日自动更新时间。

参数说明：

set	分类库设置
time	设置每日自动更新时间
string	字符串，格式为 hh:mm；

global webfilter-update set host <*string*>

命令描述：

分类库远程升级主机设置。

参数说明：

set	分类库远程升级主机设置
host	设置主机 IP 或域名
string	字符串

global webfilter-update show<cr>

命令描述：

显示分类库信息

global webfilter-update reset<cr>

命令描述：

重置分类库更新设置。

global webfilter-update agent clean<cr>

命令描述：

清空现有分类库文件。

global webfilter-update agent restart<cr>

命令描述：

重启分类库代理。

global webfilter-update agent stop<cr>

命令描述：

停止分类库代理。

global tcp-splice enable <on|off>

命令描述：

设置 TCP 粘合参数。

参数说明：

tcp-splice	设置 TCP 粘合参数
enable	是否启用
on|off	启用/禁用

global show<cr>

命令描述：

查看 TCP 粘合设置。

global reset<cr>

命令描述：

TCP 粘合设置恢复出厂配置。

http

HTTP 过滤策略配置。

主要是针对 web 页面中的 Url、关键字、java/vb 脚本，applet 脚本、activex 脚本进行过滤，对 http 访问进行认证，可以用于控制用户访问网页或网站，以及禁止脚本或 Java 程序。Script、activex、applet 的开关默认是开启的。

http add name <*string1* > [**auth** <on|off>] [**url** <*string2*>] [**header** <*string3*>][**keyword** <*string4*>][**script** < allow |forbid >] [**activex** < allow |forbid>] [**applet** < allow |forbid >] [**redirect**<*string5*> [**timeout**<*number*>]][**banner**<*string6*>] [**log** <on|off >] [**spoof** <permit|deny>] [**url-maxlen** <*number*>]

命令描述：

添加一条 HTTP 策略。

参数说明：

add	添加一条 HTTP 策略
name	对象名
String1	字符串
auth	可选参数，设定是否开启会话认证，默认不开启。
on|off	是/否
url	可选参数，设定引用的文件对象资源名，默认为空。
String2	字符串，为已定义的文件对象名
header	可选参数，选择 DPI header 对象，默认为空。
string3	字符串，为已经定义的对象名
keyword	可选参数，设定关键字对象
String4	字符串，为已定义的模式集合对象名
script	可选参数，设定是否开启脚本过滤
allow|forbid	允许/禁止
activex	可选参数，设定是否开启 ACTIVEX 控件过滤
allow|forbid	允许/禁止
applet	可选参数，设定是否开启 APPLET 过滤
allow|forbid	允许/禁止
redirect	可选参数，指定重定向地址
string5	字符串
timeout	可选参数，当指定重定向地址时才需要设置，用于指定重定向超时时间，默认为 1800 秒。
number	数值。
banner	可选项，替换 HTTP 服务器向客户端返回的登录标题信息，保护服务器的版本信息不被暴露。默认为空。
String6	字符串
log	可选参数，当有符合该规则的数据报文被截获时是否在系统日志中作相关记录，默认不作记录。
on|off	做记录/不做记录
spoof	设置是否允许伪装 HTTP 连接通过
permit|deny	允许/拒绝
url-maxlen	设置 URL 最大长度
number	单位字节，范围 0－4096。

使用说明：

如果将 HTTP 认证功能设置为 on，则不需要再配置内容过滤关键字，如以下实例。

实例：

** 添加一条名为“http_policy”的 http 策略。

http add name *http_policy* **auth** off **header** *‘http_pattern’* **keyword** *‘http_pattern’*

script forbid **activex** forbid **applet** forbid **redirect** *http://192.168.1.39* **timeout** *300*

log on

** 添加一条 HTTP 认证策略。

http add name *http_auth* **auth** on

http clean <cr>

命令描述：

清除所有 HTTP 策略。

http delete name <*string*>

命令描述：

删除一条 HTTP 策略。

参数说明：

delete	删除一条 HTTP 策略
name	HTTP 策略名称
string	字符串

实例：

**删除一条名为“http_policy”的 HTTP 策略。

http delete name *http_policy*

http modify name <*string1* > **auth** <on|off> **url** <*string2*> **header** <*string3*>**keyword** <*string4*> **script** < allow |forbid > **activex** < allow |forbid> **applet** < allow |forbid > **redirect**<*string5*> **timeout**<*number*> **banner**<*banner*> **log** <on|off >

命令描述：

修改一条 HTTP 策略。

参数说明：

modify	修改一条 HTTP 策略

name	对象名
String1	字符串
auth	设定是否开启会话认证
on|off	是/否
url	设定引用的文件对象资源名
String2	字符串，为已定义的文件对象名
header	选择 DPI header 对象
string3	字符串，为已经定义的对象名
keyword	设定模式集合对象
String4	字符串，为已定义的模式集合对象名
script	设定是否开启脚本过滤
allow|forbid	允许/禁止
activex	设定是否开启 ACTIVEX 控件过滤
allow|forbid	允许/禁止
applet	设定是否开启 APPLET 过滤
allow|forbid	允许/禁止
redirect	指定重定向地址
string5	字符串
timeout	指定重定向超时时间
number	数值
banner	可选项，替换 HTTP 服务器向客户端返回的登录标题信息，保护服务器的版本信息不被暴露。默认为空。
string2	字符串
log	当有符合该规则的数据报文被截获时是否在系统日志中作相关记录
on|off	做记录/不做记录

http show [**name**<*string*>]

命令描述：

显示所有或指定的 HTTP 策略。

参数说明：

show	显示所有 HTTP 策略
name	HTTP 策略名称
string	字符串

使用说明：

无

实例：

**显示所有 HTTP 策略

http show <cr>

http url-forbidden show<cr>

命令描述：

查看 HTTP 禁止 URL 统计

http url-forbidden clean<cr>

命令描述：

清空所有 HTTP 禁止 URL 统计结果

imap

IMAP 过滤策略配置。

定义访问控制规则时，管理员可以通过增加一条包括该 DPI 的访问策略，用于控制受控网络内电子邮件的接收。IMAP 策略中包含了对发件人、收件人、主题、附件和正文的关键字过滤。如果匹配关键字，则按照关键字的权限进行处理，否则系统将按照与关键字权限相反的权限对数据进行处理。

imap add name < *string1*> [**subject** <*string2*>] [**attach** < *string3*>] [**send** < *string4*>] [**recv**< *string5*>] [**content**< *string6*>][**banner** <*string7*>][**log** <on|off>]

命令描述：

添加一条 IMAP 策略。

参数说明：

add	添加一条 IMAP 策略
name	对象名
string1	字符串
subject	可选项，设定主题匹配规则，默认为空。
string2	选定所包含的关键字对象名
attach	可选项，设定附件匹配规则，默认为空。
string3	选定所包含的关键字对象名
send	可选项，设定发件人，默认为空。
string4	选定所包含的关键字对象名
recv	可选项，设定收件人，默认为空。
string5	选定所包含的关键字对象名
content	可选项，设定邮件正文，默认为空。
string6	选定所包含的关键字对象名

banner	可选项，替换 IMAP 服务器向客户端返回的登录标题信息，保护服务器的版本信息不被暴露，默认为空。
string7	选定所包含的登录标题名
log	可选项，当有符合该规则的数据报文被截获时是否在系统日志中作相关记录，默认不作记录。
on|off	做记录/不做记录

使用说明：

在定义了 IMAP 策略后，还需要在保护内容表模块中引用该策略。

实例：

** 添加一条名为“imap_policy”的策略。

imap add name *imap_policy* **subject** *‘imap_pattern’* **attach** *‘imap_pattern’*

content *‘imap_pattern’* **banner** *banner1* **log** on

imap clean <cr>

命令描述：

清除所有 IMAP 策略。

imap delete name <*string*>

命令描述：

删除一条 IMAP 策略。

参数说明：

delete	删除一条 IMAP 策略
name	IMAP 策略名称
string	字符串

实例：

** 删除一条名为“imap_policy”的 POP3 策略。

imap delete name *imap_policy*

imap modify name < *string1*> [**subject** <*string2*>] [**attach** < *string3*>] [**send** < *string4*>] [**recv**< *string5*>] [**content**< *string6*>][**banner** <*string7*>][**log** <on|off>]

命令描述：

修改一条 IMAP 策略。

参数说明：

modify	修改一条 IMAP 过滤策略
name	对象名
string1	字符串
subject	可选项，设定主题匹配规则，默认为空。
string2	选定所包含的关键字对象名
attach	可选项，设定附件匹配规则，默认为空。
string3	选定所包含的关键字对象名
send	可选项，设定发件人，默认为空。
string4	选定所包含的关键字对象名
recv	可选项，设定收件人，默认为空。
string5	选定所包含的关键字对象名
content	可选项，设定邮件正文，默认为空。
string6	选定所包含的关键字对象名
banner	可选项，替换 SMTP 服务器向客户端返回的登录标题信息，保护服务器的版本信息不被暴露，默认为空。
string7	选定所包含的登录标题名
log	可选项，当有符合该规则的数据报文被截获时是否在系统日志中作相关记录，默认不作记录。
on|off	做记录/不做记录

imap show [**name**<*string*>]

命令描述：

显示所有或指定的 IMAP 策略。

参数说明：

show	显示所有 IMAP 策略
name	IMAP 策略名称
string	字符串

实例：

**显示所有 IMAP 策略

imap show <cr>

max-connection

设置/显示 DPI 最大连接数

max-connection set <*number*>

命令描述：

设置 DPI 最大连接数

参数说明：

set	设置 DPI 最大连接数
number	数值，范围为 1-65535。

实例：

**设置 DPI 最大连接数为 10

max-connection set *10*

max-connection show <cr>

命令描述：

查看 DPI 最大连接数

pattern

本命令用来定义与过滤内容相关的关键字对象。关键字的设置是其他 DPI 设置的基础，在定义其他 DPI 时，都要用到关键字对象。

pattern add name <*string1*> [**regular** <*string2*>]| [**case-sensitive** <yes|no>] | [**prot** <http|ftp|mail|rsh|telnet|dns>] | [**access**<rwxn>]

pattern add name <*string1*> [**url**<*string2*>] | [**access**<rwxn>]

pattern add name <*string1*> [**banner** <*string2*>]

命令描述：

添加一个关键字对象、URL 对象或者是登录标题对象。

参数说明：

add	添加一个关键字对象
name	关键字对象名
string1	字符串
regular	关键字，支持通配符“*”和“？”。
string2	字符串
case-sensitive	是否区分大小写
yes|no	区分/不区分大小写
prot	选择协议类型
http|ftp|mail|rsh|telnet|dns	用于 http|ftp|mail|rsh|telnet|dns 策略的关键字对象
access	读写权限控制

rwxn	可读、可写、可执行
banner	登录标题
String2	字符串
url	不区分大小写的 URL 表达式
String2	字符串

使用说明：

1) 添加一个关键字对象需要选择协议类型和是否区分大小写、添加 URL 对象或登录标题对象不需要设置。

2) URL 关键字设置不支持“？”和“*”通配符，不需要输入协议名称前缀（http://），在定义 DPI 策略时支持从头匹配，即前面匹配即可。

3）登录标题关键字用于替换指定网络服务所发送的登录标题，屏蔽服务器软件名称、版本、运行环境等标题信息。主要用于网络服务程序保护，防止收集服务器信息，客户端一般不可见。

实例：

** 添加一个名为“禁止”的关键字对象，包括的关键字为“*.zip”， 用于 FTP 策略，不区分大小写。

#**pattern add name** *禁止* **regular** ‘*.*zip*’ **case-sensitive** *no* **prot** *ftp* **access** rw

**添加一个名为“禁止访问”的 URL 对象，包括的关键字为“www.sina.com.cn”。

#**pattern add name** *禁止访问***url** *‘www.sina.com.cn’* **access** *rw*

**添加一个名为“http 登录标题”的登录标题对象，包括的关键字为“topsec”。

#**pattern add name** *http登录标题* **banner** ‘*topsec*’

pattern delete <regular|url|banner> **name** <*string*>

命令描述：

删除一个关键字对象。

参数说明：

delete	删除一个关键字对象
regular|url|banner	关键字类型，关键字|url|登录标题
name	指定对象名
string	字符串

使用说明：

不能删除已经被引用的关键字对象。

实例：

** 删除名为“禁止“的关键字对象

pattern delete regular **name** *禁止*

pattern show <regular|url|banner> [**name**<*string*>]

命令描述：

查看指定类型的关键字对象

参数说明：

show	查看指定类型的关键字对象
regular|url|banner	关键字|url|登录标题
name	已定义的关键字对象的名称
string	字符串

实例：

** 查看当前系统的所有 url 关键字对象

pattern show url

** 查看名为“禁止访问”的 url 关键字对象

pattern show url **name** *禁止访问*

pattern clean <regular|url|banner>

命令描述：

清除指定类型的关键字对象。

参数说明：

clean	清除所有关键字对象
regular|url|banner	关键字|url|登录标题

使用说明：

不能清除已经被引用的关键字对象。

实例：

** 清除当前系统的 url 关键字对象

pattern clean url

pattern modify name <*string1*> [**regular** <*string2*>]| [**case-sensitive** <yes|no>] | [**prot**< http|ftp |mail|rsh|telnet|dns >] | [**access**<rwxn>]

pattern modify name <*string1*> [**url**<*string2*>] | [**access**<rwxn>]

pattern modify name <*string1*> [**banner** <*string2*>]

命令描述：

修改关键字对象、URL 对象或登录标题对象的属性。

参数说明：

modify	修改关键字对象属性
name	关键字对象名
string1	字符串
regular	关键字，支持对*，？的匹配。**需要注意的是：**通配符 * 和 ？只可以出现关键字中间，关键字首尾不可以配置通配符 * 和 ？”。
string2	字符串
case-sensitive	是否区分大小写
yes|no	区分/不区分大小写
prot	选择协议类型
http|ftp|mail|rsh|telnet|dns	用于 http|ftp|mail|rsh|telnet|dns 策略的关键字对象
access	读写权限控制
rwxn	可读、可写、可执行
banner	登录标题
String2	字符串
url	不区分大小写的 URL 表达式
String2	字符串

实例：

** 在名为“禁止”的关键字对象中增加关键字“*.exe”。

#pattern modify name *禁止* **regular** *‘*.zip *.exe’* **case-sensitive** no **prot** ftp **access** rw

policy

自定义应用协议端口绑定策略。

下表列出的标准端口是系统默认的。

应用协议名	默认端口号	协议类型	所使用协议号
sip	5060	UDP	17
FTP	21	TCP	6
SMTP	25	TCP	6
TFTP	69	UDP	17

HTTP	80	TCP	6
IMAP	143	TCP	6
TELNET	23	TCP	6
POP3	110	TCP	6
SUN ONE RPC	111	TCP	6
MS DCE RPC	135	TCP	6
SQLNET	1521	TCP	6
RTSP	554	TCP	6
H225	1720	TCP	6
H225ras	1719	UDP	17
MMS	1755	TCP	6

policy add name <ftp|smtp|tftp|http|pop3|sun_rpc|ms_rpc|sqlnet|rtsp|h225| h225ras| mms|sip| pptp| rsh|imap|telnet > **net** <*string1*> **mask** <*string2*> **protocol** <udp|tcp> **port** <*number*>[**enable** < yes|no>]

命令描述：

自定义一条应用协议端口绑定策略。

参数说明：

add	增加一条应用协议端口绑定策略
name	字符串，指定要重新定义端口的协议名
<ftp|smtp|tftp|http|pop3|sun_rpc| ms_rpc|sqlnet|rtsp|h225|h225ras| mms|sip| pptp| rsh |imap|telnet >	选定其中一项
net	指定子网地址
string1	标准 IP 地址字符串
mask	指定子网掩码
string2	标准地址掩码字符串
protocol	指定所使用的协议名称
udp|tcp	选定使用 UDP 或 TCP 协议
port	自定义该协议的服务端口
number	服务端口号
enable	可选项，设置是否启用该规则
yes|no	是、否

实例：

** 将发往子网 192.168.0.0/255.255.0.0 的 http 协议数据包的目的端口绑定为 8080

policy add name http **net** *192.168.0.0* **mask** *255.255.0.0* **protocol** tcp **port** *8080*

policy clean <cr>

命令描述：

清除所有应用协议端口绑定策略。

policy delete id <*number*>

命令描述：

删除一条应用协议端口绑定策略。

参数说明：

delete	删除一条应用协议端口绑定策略
id	策略 ID
number	数值

使用说明：

可以使用 policy SHOW 命令来查看策略 ID 号。

实例：

**删除 ID 为 8547 的一条应用协议端口绑定策略

policy delete id *8547*

policy modify id <*number1*>**name** < ftp|smtp|tftp|http|pop3|sun_rpc|ms_rpc|sqlnet|rtsp|h225| h225ras| mms|sip| pptp| rsh|imap|telnet >**net** <*string1*> **mask** <*string2*>**protocol** <udp|tcp> **port** <*number2*> **enable** < yes|no>

命令描述：

修改一条应用协议端口绑定策略。

参数说明：

modify	修改一条应用协议端口绑定策略
id	要修改的策略 ID 号
Number1	数值
name	字符串，指定要重新定义端口的协议名
< ftp|smtp|tftp|http|pop3|sun_rpc| ms_rpc|sqlnet|rtsp|h225| h225ras| mms|sip| pptp| rsh|imap|telnet >	选定其中一项
net	指定子网地址
string1	标准 IP 地址字符串
mask	指定子网掩码
string2	标准地址掩码字符串
protocol	指定所使用的协议名称
udp|tcp	选定使用 UDP 或 TCP 协议
port	自定义该协议的服务端口
number	端口号
enable	可选项，设置是否启用该规则

yes|no	是、否

使用说明：

可以使用 policy SHOW 命令来查看策略 ID 号。

实例：

** 将 ID 为 8182 的端口绑定策略中的 FTP 协议数据的端口号改为 2121

policy modify id *8182* **name** ftp **net** *0.0.0.0* **mask** *0.0.0.0* **protocol** tcp **port** *2121*

policy show <cr>

命令描述：

显示所有应用协议端口绑定策略。

policy reset <cr>

命令描述：

恢复默认的应用协议端口。

pop3

POP3 过滤策略配置。

定义访问控制规则时，管理员可以通过增加一条包括该 DPI 的访问策略，用于控制受控网络内电子邮件的接收。POP3 策略中包含了对发件人、收件人、主题、附件和正文的关键字过滤。如果匹配关键字，则按照关键字的权限进行处理，否则系统将按照与关键字权限相反的权限对数据进行处理。

pop3 add name < *string1*> [**subject** <*string2*>] [**attach** < *string3*>] [**send** < *string4*>] [**recv**< *string5*>] [**content**< *string6*>][**banner** <*string7*>][**log** <on|off>][**forbidden-mail-forward** <on|off>]

命令描述：

添加一条 POP3 策略。

参数说明：

add	添加一个 POP3 过滤策略
name	对象名
string1	字符串
subject	可选项，设定主题匹配规则，默认为空。
string2	选定所包含的关键字对象名
attach	可选项，设定附件匹配规则，默认为空。
string3	选定所包含的关键字对象名
send	可选项，设定发件人，默认为空。
string4	选定所包含的关键字对象名
recv	可选项，设定收件人，默认为空。
string5	选定所包含的关键字对象名
content	可选项，设定邮件正文，默认为空。
string6	选定所包含的关键字对象名
banner	可选项，替换 POP3 服务器向客户端返回的登录标题信息，保护服务器的版本信息不被暴露，默认为空。
string7	选定所包含的登录标题名
log	可选项，当有符合该规则的数据报文被截获时是否在系统日志中作相关记录，默认不作记录。
on|off	做记录/不做记录
forbidden-mail-forward	可选项，设置是否转发不符合安全规则的邮件
on|off	转发/不转发

使用说明：

POP3 策略中，最多允许添加 16 个 pop3 对象，在 subjectdefault、attachdefault、sendefault、recvdefault、contentdefault 属性项<allow|forbid>上，默认都是 allow 属性。

在定义了 POP3 策略后，还需要在 FIREWALL 模块中启用该策略。

实例：

** 添加一条名为“pop3_policy”的策略。

pop3 add name *pop3_policy* **subject** ‘*pop3_pattern*’ **attach** ‘*pop3_pattern*’ **content** ‘*pop3_pattern*’ **banner** *banner1* **log** on

pop3 clean <cr>

命令描述：

清除所有 POP3 策略。

pop3 delete name <*string*>

命令描述：

删除一条 POP3 策略。

参数说明：

delete	删除一条 POP3 策略
name	POP3 策略名称
string	字符串

实例：

** 删除一条名为“pop_policy”的 POP3 策略。

pop3 delete name *pop_policy*

pop3 modify name < *string1*> < [**subject** <*string2*>] [**subjectdefault** <allow|deny>] [**attach** < *string3*>] [**attachdefault** <allow|deny>] [**send** < *string4*>] [**senddefault** <allow|deny>] [**recv**< *string5*>] [**recvdefault** <allow|deny>] [**content**< *string6*>] [**contentdefault** <allow|deny>]>[**banner** <*string7*>]|[**log** <on|off>]

命令描述：

修改一条 POP3 策略。

参数说明：

modify	修改一条 POP3 过滤策略
name	对象名
string1	字符串
subject	可选项，设定主题匹配规则，默认为空。
string2	选定所包含的关键字对象名
attach	可选项，设定附件匹配规则，默认为空。
string3	选定所包含的关键字对象名
send	可选项，设定发件人，默认为空。
string4	选定所包含的关键字对象名
recv	可选项，设定收件人，默认为空。
string5	选定所包含的关键字对象名
content	可选项，设定邮件正文，默认为空。
string6	选定所包含的关键字对象名
banner	可选项，替换 POP3 服务器向客户端返回的登录标题信息，保护服务器的版本信息不被暴露，默认为空。
string7	选定所包含的登录标题名
log	可选项，当有符合该规则的数据报文被截获时是否在系统日志中作相关记录，默认不作记录。
on|off	做记录/不做记录
forbidden-mail-forward	可选项，设置是否转发不符合安全规则的邮件
on|off	转发/不转发

pop3 show [**name**<*string*>]

命令描述：

显示所有或指定的 POP3 策略。

参数说明：

show	显示所有 POP3 策略
name	POP3 策略名称
string	字符串

实例：

**显示所有 POP3 策略

pop3 show <cr>

rsh

RSH 系列工具（rsh、rlogin）可以实现在远程系统上执行命令，并把结果显示到客户端系统中。网络卫士安全网关的 RSH 策略用于对通过 RSH 传输的用户命令进行关键字过滤。管理员可以定义 RSH 过滤的关键字对象，并在保护内容表中引用该关键字对象，则当通过安全网关传输的数据匹配关键字时，按照关键字的权限（允许或拒绝）进行处理；否则系统将按照与关键字权限相反的权限对数据进行处理。

rsh add name <*string1*> [**command** <*string2*>] [**log** <on|off>]

命令描述：

添加一条 RSH 过滤策略

参数说明：

add	添加一条 RSH 过滤策略
name	策略名
string1	字符串
command	可选项，引用的 RSH 协议关键字对象的名称，默认为空。
string2	可以为多个字符串
log	可选项，当有符合该规则的数据报文被截获时是否在系统日志中作相关记录。默认为空。
on|off	做记录/不做记录

rsh clean <cr>

命令描述：

清除所有 RSH 策略。

rsh delete name <*string*>

命令描述：

删除一条 RSH 策略。

参数说明：

delete	删除一条 RSH 策略
name	策略名称
string	字符串

实例：

** 删除一条名为“rsh_policy”的 RSH 策略。

rsh delete name *rsh_policy*

rsh modify name <*string1*> **command** <*string2*> **log** <on|off>

命令描述：

修改一条 RSH 过滤策略

参数说明：

modify	修改一条 RSH 过滤策略
name	策略名
string1	字符串
command	可选项，引用的 RSH 协议关键字对象的名称，默认为空。
string2	可以为多个字符串
log	可选项，当有符合该规则的数据报文被截获时是否在系统日志中作相关记录。默认为空。
on|off	做记录/不做记录

rsh show [**name**<*string*>]

命令描述：

显示所有或指定的 RSH 策略。

参数说明：

show	显示所有或指定 RSH 策略
name	RSH 策略名称

string	字符串

使用说明：

指定对象名时，显示指定对象的属性；不指定对象名时，显示所有 RSH 对象。

实例：

**显示所有 RSH 策略

rsh show <cr>

rule

设置保护内容表

rule add name <*string*> [**ar** <*string*>] [**as** < on|off>] [**av-protocol** <*string*>] [**dns** <*string*>] [**ftp** <*string*>] [**http** <*string*>] [**imap** <*string*>] [**pop3** <*string*>] [**rsh** <*string*>] [**smtp** <*string*>] [**webfilter** <*string*>] [**telnet** < *string*>] [**commentary** <*string*>]

命令描述：

添加保护内容表。

参数说明：

add	添加保护内容表
name	对象名
string	字符串
ar	可选项，指定应用程序识别策略
string	字符串
as	可选项，反垃圾邮件开关。
on|off	开、关
av-protocol	可选项，指定开启反病毒检测的协议类型
string	http|ftp|smtp|pop3|imap
dns	可选项，指定 DNS 识别策略
string	字符串，为已添加的 DNS 过滤策略名
ftp	可选项，指定 FTP 过滤策略
string	字符串，为已添加的 FTP 过滤策略名
http	可选项，指定 HTTP 过滤策略
string	字符串，为已添加的 HTTP 过滤策略名
imap	可选项，指定 IMAP 过滤策略
string	字符串，为已添加的 IMAP 过滤策略名
pop3	可选项，指定 POP3 过滤策略
string	字符串，为已添加的 RSH 过滤策略名

rsh	可选项，指定 RSH 过滤策略
string	字符串，为已添加的 RSH 过滤策略名
smtp	可选项，指定 SMTP 过滤策略
string	字符串，为已添加的 SMTP 过滤策略名
webfilter	可选项，指定 WEB 过滤策略
string	字符串，为已添加的 WEB 过滤策略名
telnet	可选项，指定 TELNET 过滤策略
string	字符串，为已添加的 TELNET 过滤策略名
commentary	可选项，输入描述信息
string	字符串，最大长度 63 字符。

rule clean <cr>

命令描述：

清除所有保护内容表对象。

rule delete name <*string*>

命令描述：

删除一个对象。

参数说明：

delete	删除一个对象
name	对象名称
string	字符串

rule modify name <*string*> [**ar** <*string*>] [**as** < on|off>] [**av-protocol** <*string*>] [**dns** <*string*>] [**ftp** <*string*>] [**http** <*string*>] [**imap** <*string*>] [**pop3** <*string*>] [**rsh** <*string*>] [**smtp** <*string*>] [**webfilter** <*string*>] [**telnet** < *string*>] [**commentary** <*string*>]

命令描述：

修改保护内容表。

参数说明：

modify	修改保护内容表
name	对象名
string	字符串
ar	可选项，指定应用程序识别策略
string	字符串
av-protocol	可选项，指定开启反病毒检测的协议类型
string	http|ftp|smtp|pop3|imap
dns	可选项，指定 DNS 识别策略
string	字符串，为已添加的 DNS 过滤策略名

ftp	可选项，指定 FTP 过滤策略
string	字符串，为已添加的 FTP 过滤策略名
http	可选项，指定 HTTP 过滤策略
string	字符串，为已添加的 HTTP 过滤策略名
imap	可选项，指定 IMAP 过滤策略
string	字符串，为已添加的 IMAP 过滤策略名
pop3	可选项，指定 POP3 过滤策略
string	字符串，为已添加的 RSH 过滤策略名
rsh	可选项，指定 RSH 过滤策略
string	字符串，为已添加的 RSH 过滤策略名
smtp	可选项，指定 SMTP 过滤策略
string	字符串，为已添加的 SMTP 过滤策略名
webfilter	可选项，指定 WEB 过滤策略
string	字符串，为已添加的 WEB 过滤策略名
telnet	可选项，指定 TELNET 过滤策略
string	字符串，为已添加的 TELNET 过滤策略名
commentary	可选项，输入描述信息
string	字符串，最大长度 63 字符。

rule show [**name**<*string*>]

命令描述：

显示所有或指定的保护内容表。

参数说明：

show	显示所有或指定保护内容表
name	指定对象名称
string	字符串

使用说明：

指定对象名时，显示指定对象的属性；不指定对象名时，显示所有对象。

smtp

SMTP 过滤策略配置。

定义访问控制规则时，管理员可以通过增加一条包括该 DPI 的访问策略，来控制电子邮件的发送。当发送一封发件人、收件人、主题、附件、内容中之一违规的邮件时，网关会按照策略中指定的方式进行处理。如果匹配关键字，则按照关键字的权限进行处理，否则系统将按照与关键字权限相反的权限对数据进行处理。

smtp add name < *string1*> [**subject** <*string2*>] [**attach** < *string3*>] [**send** < *string4*>] [**recv**< *string5*>] [**content**< *string6*>][**banner** <*string7*>][**log** <on|off>][**forbidden-mail-forward** <on|off>]

命令描述：

添加一条 SMTP 策略。

参数说明：

add	添加一个 SMTP 过滤策略
name	对象名
string1	字符串
subject	可选项，设定主题匹配规则，默认为空。
string2	选定所包含的关键字对象名
attach	可选项，设定附件匹配规则，默认为空。
string3	选定所包含的关键字对象名
send	可选项，设定发件人，默认为空。
string4	选定所包含的关键字对象名
recv	可选项，设定收件人，默认为空。
string5	选定所包含的关键字对象名
content	可选项，设定邮件正文，默认为空。
string6	选定所包含的关键字对象名
banner	可选项，替换 SMTP 服务器向客户端返回的登录标题信息，保护服务器的版本信息不被暴露，默认为空。
string7	选定所包含的登录标题名
log	可选项，当有符合该规则的数据报文被截获时是否在系统日志中作相关记录，默认不作记录。
on|off	做记录/不做记录
forbidden-mail-forward	可选项，设置是否转发不符合安全规则的邮件
on|off	转发/不转发

使用说明：

SMTP 策略中，在 subjectdefault、attachdefault、sendefault、recvdefault、contentdefault 属性项<allow|forbid>上，默认都是 allow 属性。

在定义了 SMTP 策略后，还需要在 FIREWALL 模块中启用该策略。

实例：

** 添加一条名为“smtp_policy”的策略。

smtp add name *smtp_policy* **subject** ‘*smtp_pattern’* **attach** ‘*smtp_pattern’* **content** ‘*smtp_pattern’* **banner** *banner1* **log** on

**在保护内容表中启用该策略。

#**dpi rule add name** *smtp_filter* **smtp** ‘*smtp_policy’*

smtp clean <cr>

命令描述：

清除所有 SMTP 策略。

smtp delete name <*string*>

命令描述：

删除一条 SMTP 策略。

参数说明：

delete	删除一条 SMTP 策略
name	SMTP 策略名称
string	字符串

实例：

**删除一条 SMTP 策略

smtp delete name *smtp_policy*

smtp modify name < *string1*> [**subject** <*string2*>] [**attach** < *string3*>] [**send** < *string4*>] [**recv**< *string5*>] [**content**< *string6*>][**banner** <*string7*>][**log** <on|off>][**forbidden-mail-forward** <on|off>]

命令描述：

修改一条 SMTP 策略。

参数说明：

modify	修改一条 SMTP 过滤策略
name	对象名
string1	字符串
subject	可选项，设定主题匹配规则，默认为空。
string2	选定所包含的关键字对象名
attach	可选项，设定附件匹配规则，默认为空。
string3	选定所包含的关键字对象名
send	可选项，设定发件人，默认为空。
string4	选定所包含的关键字对象名
recv	可选项，设定收件人，默认为空。
string5	选定所包含的关键字对象名
content	可选项，设定邮件正文，默认为空。
string6	选定所包含的关键字对象名

banner	可选项，替换 SMTP 服务器向客户端返回的登录标题信息，保护服务器的版本信息不被暴露，默认为空。
string7	选定所包含的登录标题名
log	可选项，当有符合该规则的数据报文被截获时是否在系统日志中作相关记录，默认不作记录。
on|off	做记录/不做记录
forbidden-mail-forward	可选项，设置是否转发不符合安全规则的邮件
on|off	转发/不转发

smtp show [**name**<*string*>]

命令描述：

显示所有或指定的 SMTP 策略。

参数说明：

show	显示所有 SMTP 策略
name	SMTP 策略名称
string	字符串

实例：

**显示所有 SMTP 策略

smtp show <cr>

telnet

TELNET 策略配置。

定义访问控制规则时，管理员可以选择该 DPI 的策略。

telnet add name <*string1*> **banner** <*string2*> **command** <*string3*> [**log** <on|off>]

命令描述：

添加一条 TELNET 策略。

参数说明：

add	添加一条 TELNET 策略
name	TELNET 策略名
String1	字符串
banner	引用的登录标题对象名称，替换 telnet 服务器向客户端返回的 banner 信息，保护服务器的版本信息不被暴露。
String2	可以为多个字符串

command	引用的关键字对象的名称
string3	字符串
log	可选项，当有符合该规则的数据报文被截获时是否在系统日志中作相关记录，默认不做记录。
on|off	做记录/不做记录

实例：

** 添加一条名为“telnet_policy”的 TELNET 策略。

telnet add name *telnet_policy* **banner** *‘http登录标题’* **log** on

telnet clean <cr>

命令描述：

清除所有 TELNET 策略。

telnet delete name <*string*>

命令描述：

删除一条 TELNET 策略。

参数说明：

delete	删除一条 TELNET 策略
name	TELNET 策略名称
string	字符串

实例：

**删除一条名为“telnet_policy”的 TELNET 策略

telnet delete name *telnet_policy*

telnet modify name <*string1*> **banner** <*string2*> **command** <*string3*> **log** <on|off>

命令描述：

修改一条 TELNET 策略。

参数说明：

modify	修改一条 TELNET 策略
name	TELNET 策略名
String1	字符串
banner	引用的登录标题对象名称，替换 telnet 服务器向客户端

	返回的 banner 信息，保护服务器的版本信息不被暴露。
String2	可以为多个字符串
command	引用的关键字对象的名称
string3	字符串
log	当有符合该规则的数据报文被截获时是否在系统日志中作相关记录。
on|off	做记录/不做记录

telnet show [**name**<*string*>]

命令描述：

显示所有或指定的 TELNET 策略。

参数说明：

show	显示所有 TELNET 策略
name	TELNET 策略名称
string	字符串

实例：

**显示所有 TELNET 策略

telnet show <cr>

webfilter

WEB 过滤策略设置

webfilter add name <*string*> **url-type** <*string*> [**log** <on|off>] [**ignore-malice** <on|off>]

[**warning-page** <on|off>]

命令描述：

添加 WEB 过滤策略。

参数说明：

add	添加 WEB 过滤策略
name	策略名称
string	字符串
url-type	指定被操作的 URL 分类
string	字符串，管理员可以利用命令 **webfilter support-type-show** 查看。
log	设置是否记录日志信息
on|off	是/否

ignore-malice	恶意网站允许跳过开关
on|off	开/关
warning-page	警告页面发送开关
on|off	开/关

webfilter clean <cr>

命令描述：

清除所有 WEB 过滤策略。

webfilter delete name <*string*>

命令描述：

删除 WEB 过滤策略。

参数说明：

modify	删除 WEB 过滤策略
name	策略名称
string	字符串

webfilter modify name <*string*> [**url-type** <*string*>] [**log** <on|off>] [**ignore-malice** <on|off>]

[**warning-page** <on|off>]

命令描述：

修改 WEB 过滤策略。

参数说明：

modify	修改 WEB 过滤策略
name	策略名称
string	字符串
url-type	指定被操作的 URL 分类
string	字符串
log	设置是否记录日志信息
on|off	是/否
ignore-malice	恶意网站允许跳过开关
on|off	开/关
warning-page	警告页面发送开关
on|off	开/关

webfilter show [**name** <*string*>]

命令描述：

查看 WEB 过滤策略。

参数说明：

show	查看 WEB 过滤策略
name	策略名称，可选项，不指定时查看所有。
string	字符串

webfilter support-type-show <cr>

命令描述：

查看 WEB 过滤分类库明细。

FIREWALL

网关访问控制规则定义模块。

用户可以通过设置访问控制规则实现灵活、强大的三到七层的访问控制。系统不但可以从区域、VLAN、地址、用户、连接、时间等多个层面对数据报文进行判别和匹配，而且还可以针对多种应用层协议进行深度内容检测和过滤。

与包过滤策略相同，访问控制规则也是顺序匹配的，但与其不同，访问控制规则没有默认规则。也就是说，如果没有在访问控制规则列表的末尾添加一条全部拒绝的规则的话，系统将根据目的接口所在区域的缺省属性（允许访问或禁止访问）处理该报文。

进入本命令模块操作如下：

#firewall<cr>

退出本命令模块操作如下：

#end<cr>

CLI 管理员登录网关进入本命令模块后，可以执行相应的组件管理命令。下面将详细描述本命令模块下的所有组件管理命令。命令的实例输入格式将按已经进入本命令模块书写。

下一级命令列表

命令	功能
access-info	设置防火墙访问记录规则
enhancement	开启 “访问控制策略重叠检查”功能
group-policy	访问控制组配置管理
policy	定义防火墙访问控制规则
dynamic-policy	动态策略设置

access-info

设置防火墙访问记录功能

access-info clean<cr>

命令描述：

清空所有访问记录。

access-info show<cr>

命令描述：

查看所有访问记录。

access-info show-config<cr>

命令描述：

显示访问记录配置。

access-info sort-show<cr>

命令描述：

显示排序设置。

access-info sort-set sort-key [srcip|dstip|protocol|dport|stat] **sort-type** [asc|desc]<cr>

命令描述：

访问记录排序设置。

参数说明：

sort-set	开启或关闭冲突检查功能
sort-key	设置排序关键字
srcip|dstip|protocol|dport|stat	源 IP/目的 IP/协议/目的端口/状态
sort-type	可选项，设置按照升序或降序排列。
asc|desc	升序/降序

实例：

**设置访问记录按照源 IP 降序排列

access-info sort-set sort-key srcip **sort-type** desc

access-info start<cr>

命令描述：

启用访问控制记录功能。

access-info stop<cr>

命令描述：

停止访问控制记录功能。

access-info refresh<cr>

命令描述：

刷新访问控制记录。

enhancement

开启 “访问控制策略重叠检查”功能。

enhancement switch [**accelerate** <on|off>][**overlap-exam** <on|off>]

命令描述：

开启或关闭冲突检查功能。

参数说明：

switch	开启或关闭冲突检查功能
accelerate	可选项，设置是否开启匹配加速功能，默认关闭。
on|off	开启或关闭
overlap-exam	可选项，设置是否开启策略重叠检查开关，默认关闭。
on|off	on 表示开启；off 表示关闭；

enhancement show <cr>

命令描述：

查看冲突检查功能相关设置。

group_policy

访问控制组配置管理。对于定义的访问控制规则，系统提供对规则的分组管理功能，不同组之间的前后顺序和组内规则的排列顺序共同决定访问控制规则的匹配顺序。

group_policy add name <*string*> [**before** < *number* >] [**vsid** <*number*>]

命令描述：

添加一条访问控制规则组。

参数说明：

add	添加一条访问控制规则组
name	设置规则组名称
string	字符串
before	可选项，设置在某规则组之前插入一条规则组。
number	输入已经添加的 ACL 规则组的 ID 号。
vsid	可选项，设置虚系统号。默认属于虚系统 0。
number	数值。范围为 0-254。

实例：

**在 ACL 规则组 8108 前插入规则组 subnat83 中。

group_policy add name *subnat83* **before** *8108*

group_policy clean [**vsid** <*number*>]

命令描述：

清空访问控制规则组。

参数说明：

clean	清空访问控制规则组
vsid	可选项，设置虚系统号。默认查看虚系统 0。
Number	数值。范围为 0-254。

实例：

**清空虚系统 0 的访问控制规则组。

group_policy clean<cr>

group_policy delete [id <*number*> **|name** <*string*>] [**vsid** <*number*>]

命令描述：

根据 ID 或名称删除某访问控制规则组。

参数说明：

delete	根据 ID 或名称删除某访问控制规则组
id	指定规则组 ID 号
number	数值
name	设置规则组名称
string	字符串
vsid	可选项，设置虚系统号。默认属于虚系统 0。
Number	数值。范围为 0-254。

实例：

**删除规则组 subnat83。

group_policy delete name *subnat83*

group_policy rename oldname<*string*> **newname** <*string*> [**vsid** <*number*>]

命令描述：

为访问控制规则组重新命名

参数说明：

rename	为访问控制规则组重新命名
oldname	设置规则组旧的名称
string	字符串
newname	设置规则组新的名称
string	字符串
vsid	可选项，设置虚系统号。默认属于虚系统 0。
Number	数值。范围为 0-254。

group_policy show [**vsid** <*number*>]

命令描述：

查看清空访问控制规则组。

参数说明：

show	查看访问控制规则组
vsid	可选项，设置虚系统号。默认查看虚系统 0。

Number	数值。范围为 0-254。

实例：

**查看虚系统 0 的访问控制规则组。

group_policy show <cr>

group_policy move <*string1***>** [**before** <*string2*> | **after** <*string3*>]

命令描述：

移动访问控制规则组。

参数说明：

move	移动访问控制规则组。
string1	字符串，表示待移动的规则组的名称
before	移动到指定的规则组之前。
string2	字符串，表示参照物规则组的名称
after	移动到指定规则组之后。
string3	字符串，表示参照物规则组的名称

实例：

** 将名为“test10”的规则组移动到名为“test2”的规则组之前。

group_policy move *test10* **before** *test2*

policy

本命令用来定义网关的访问控制规则，包括对访问控制规则的添加、修改、清除、删除、查看和移动。

policy add action <accept|deny|collect > [**srcarea** <*string1*>] [**dstarea** <*string2*>] [**srcvlan** <*string3*>][**dstvlan** <*string4*>] [**src** <*string5*>] [**dst** <*string6*>] [**service** <*string7*>] [**schedule** <*string8*>][**sport** <*string9*>] [**orig_dst** <*string10*>] [**dpi** <*string11*>] [**permanent** <on|off>] [**log** <on|off| alarm>] [**enable**<yes|no>][**before** <*number1*>] [**vsid** <*number2*>] [**comment** < *string*>] [**srcrole** <*string*>] [**group-name** < *string*>] [**max-active-session** < *string*>] [**ids** < *string*>] [**original-dscp** < *string*>] [**target-dscp** <*string*>] [**cos** <*number*>] [**anti-proxy** <on|off>] [**qos** < *string*>] [**ips-up** < *string*>] [**ips-down** < *string*>] [**traffic-statistic** < on|off>] [**dns** <

string>]

命令描述：

添加一条访问控制规则。

参数说明：

add	添加一条访问控制规则
action	设定访问权限，即允许或禁止匹配该规则的报文通过网关。
accept|deny|collect	允许/禁止/收集
srcarea	设定源区域
string	字符串，必须为已定义的区域资源名，可以有一个或多个，需用单引号’‘括起来，多个区域名之间用空格分隔即可，例如'area_eth0 area_eth1'。
dstarea	设定目标区域
string	字符串，为已定义的区域资源名，可以有一个或多个，需用单引号’‘括起来，多个区域名之间用空格分隔即可，例如'area_eth0 area_eth1'。
srcvlan	设定源 VLAN
string	字符串，为已定义 VLAN 号。
dstvlan	设定目标 VLAN
string	字符串，为已定义 VLAN 号。
src	源地址对象
string	字符串，为已定义的地址对象名。可以输入多个，格式为’aa ll’，用单引号，中间用空格分隔。
dst	目的地址对象
string6	字符串，为已定义的地址对象名，可以输入多个，格式为’aa ll’，用单引号，中间用空格分隔。
service	设定服务资源
string	字符串，必须是系统缺省服务或自定义服务的名称，可以输入多个，格式为’IP ICMP’，用单引号，中间用空格分隔。名称的大小写必须与系统定义相一致，如’IP’。查看服务资源请使用命令#define service show default<cr>查看。
schedule	选择时间资源，必须在前面 define 模块已经定义。
string	对象名称。
sport	指定源端口服务资源。
string	字符串，必须是系统已经定义的服务资源名。
orig_dst	指定地址转换前的目标地址对象。
string	字符串，必须是系统已经定义的地址对象名。
dpi	可选项，设定内容过滤策略。默认为空，表示不对报文内容进行过滤。
string	对象名称，必须在前面DPI模块已经定义，**只能选一个。**
permanent	可选项，长连接开关，默认为关闭状态，即为普通连接。一般来说，网关对通信空闲一定时间的连接将自动断开，以提高安全性和释放通信资源，但某些应用所建立的连接需要长时期保持，即使处于空闲状态。例如 ATM 机器必须和处理中心的

	服务器一直保持着连接，这个连接必须设置为长连接。
on|off	开/关，分别表示长连接和普通连接。
log	可选项，设置当数据报文匹配规则时，是否在日志中记录还是进行报警提示，默认不做记录。
on|off|alarm	做日志/不做日志/报警
enable	可选项，是否启用这条规则，默认启用该规则
yes|no	启用/不启用
before	可选项，增加访问控制规则时可以选择规则位置在那条规则之前。默认新添加的规则置于最后。
number1	数值，为已经添加的访问控制规则 ID 号。
vsid	可选项，虚系统 ID 号，默认为 0
number	数值
comment	可选项，输入规则描述
string	字符串
Srcrole	设定源角色
string1	字符串，必须为已定义的用户角色名，可以有一个或多个，需用单引号’‘括起来，多个区域名之间用空格分隔即可，例如'cert_role ,radius_role’。
group-name	可选项，指定策略组。不指定时表示默认组
string	策略组对象名
max-active-session	指定本条策略所允许的最大活动连接数。
string	数值
ids	选择已经设置的 IDS 规则对象，匹配到本条访问控制规则的数据包将根据相应的 IDS 对象对其进行处理。
string	字符串
original-dscp	设定是否检测 IP 报文的 DSCP 值，为可选项。如果设定了该值，则对于匹配 ACL 规则的 IP 报文，只有其 DSCP 值与该处设定的值匹配时，才修改为“目标 DSCP 值”设定的数值。如果不设定，则设备不检测报文的 DSCP 值，直接修改 DSCP 值。
string	字符串
target-dscp	对于匹配 ACL 规则的报文，设置是否重新标记报文的 DSCP 优先级。网络卫士安全网关在转发时提供优先级标记服务，用来为下游的交换机或路由器等网络设备提供 DiffServ 体系的支持。
string	字符串
cos	设置对于匹配 ACL 规则的报文，是否重新标记报文的 COS 值。 说明： 1．对于带有 802.1Q 标签头的以太网数据包，标签头中有 3 位优先级字段，用于指明数据包的优先级。网络卫士安全网关可以根据此处设定的 COS 值对优先级字段进行修改，供下游设备对数据流量进行管理。 2．该选项只有当数据报文的出接口为 Trunk 口时该选项有效。
number	数值

anti-proxy	是否启用防代理上网
on|off	是/否
qos	对符合规则的数据流进行流量监管，可以通过简单的设置下行限制带宽来进行流量监管，也可以通过勾选“高级”选项，选择设定的“QoS 对象”来设置更为细致的流量策略。 说明： 1）上行限制带宽：限制从 ACL 规则设定的源到目的传输数据时，带宽的最大值； 2）下行限制带宽：限制从目的到源传输数据时，带宽的最大值； 3）QoS 对象：选择已经添加的 QoS 对象，根据 QoS 对象的参数进行流量管理；要保证某些连接的传输带宽，必须设置出接口的总带宽；而且必须在 ACL 规则中设置数据出接口的区域，即对于“下行”的数据必须设置“源区域”。
string	字符串
ips-up	设置 IPS 上行策略对象
string	字符串
ips-down	设置 IPS 下行策略对象
string	字符串
traffic-statistic	可选项，设置是否开启流量统计开关
on|off	是、否
dns	可选项，选择设定的 DNS 资源对象名称
string	字符串

实例：

** 添加一条访问控制规则

policy add action accept srcarea *‘area_eth0’* **src** *‘any’* **service** *IP* **dpi** *‘http_policy’*

ar *‘msn’* **av** on **log** on **enable** yes **vsid** *0*

policy modify id <*number1*> [**action** <accept|deny|collect >] [**srcarea** <*string1*>] [**dstarea** <*string2*>] [**srcvlan** <*string3*>][**dstvlan** <*string4*>] [**src** <*string5*>] [**dst** <*string6*>] [**service** <*string7*>] [**schedule** <*string8*>][**sport** <*string9*>] [**orig_dst** <*string10*>] [**dpi** <*string11*>] [**permanent** <on|off>] [**log** <on|off| alarm>] [**enable**<yes|no>] [**vsid** <*number2*>] [**comment** < *string*>] [**srcrole** <*string*>] [**before** <*number1*>][**group-name** < *string*>] [**max-active-session** < *string*>] [**ids** < *string*>] [**original-dscp** < *string*>] [**target-dscp** <*string*>] [**cos** <*number*>] [**anti-proxy** <on|off>] [**qos** < *string*>] [**ips-up** < *string*>] [**ips-down** < *string*>][**traffic-statistic** < on|off>] [**dns** < *string*>]

命令描述：

修改一条已添加的访问控制规则。

参数说明：

modify	修改网关访问规则
id	已设定的访问规则 ID
number1	数值
action	设定访问权限，即允许或禁止匹配该规则的报文通过网关。
accept|deny|collect	允许/禁止/收集
srcarea	设定源区域
string	字符串，必须为已定义的区域资源名，可以有一个或多个，需用单引号’‘括起来，多个区域名之间用空格分隔即可，例如'area_eth0 area_eth1'。
dstarea	设定目标区域
string	字符串，为已定义的区域资源名，可以有一个或多个，需用单引号’‘括起来，多个区域名之间用空格分隔即可，例如'area_eth0 area_eth1'。
srcvlan	设定源 VLAN
string	字符串，为已定义 VLAN 号。
dstvlan	设定目标 VLAN
string	字符串，为已定义 VLAN 号。
src	源地址对象
string	字符串，为已定义的地址对象名。可以输入多个，格式为’aa ll’，用单引号，中间用空格分隔。
dst	目的地址对象
string6	字符串，为已定义的地址对象名，可以输入多个，格式为’aa ll’，用单引号，中间用空格分隔。
service	设定服务资源
string	字符串，必须是系统缺省服务或自定义服务的名称，可以输入多个，格式为’IP ICMP’，用单引号，中间用空格分隔。名称的大小写必须与系统定义相一致，如’IP’。查看服务资源请使用命令#define service show default<cr>查看。
schedule	选择时间资源，必须在前面 define 模块已经定义。
string	对象名称。
sport	指定源端口服务资源。
string	字符串，必须是系统已经定义的服务资源名。
orig_dst	指定地址转换前的目标地址对象。
string	字符串，必须是系统已经定义的地址对象名。
dpi	可选项，设定内容过滤策略。默认为空，表示不对报文内容进行过滤。
string	对象名称，必须在前面DPI模块已经定义，**只能选一个。**
permanent	可选项，长连接开关，默认为关闭状态，即为普通连接。一般来说，网关对通信空闲一定时间的连接将自动断开，以提高安全性和释放通信资源，但某些应用所建立的连接需要长时期保持，即使处于空闲状态。例如 ATM 机器必须和处理中心的服务器一直保持着连接，这个连接必须设置为长

	连接。
on|off	开/关，分别表示长连接和普通连接。
log	可选项，设置当数据报文匹配规则时，是否在日志中记录还是进行报警提示，默认不做记录。
on|off|alarm	做日志/不做日志/报警
enable	可选项，是否启用这条规则，默认启用该规则
yes|no	启用/不启用
vsid	可选项，虚系统 ID 号，默认为 0
number	数值
comment	可选项，输入规则描述
string	字符串
Srcrole	设定源角色
string1	字符串，必须为已定义的用户角色名，可以有一个或多个，需用单引号’‘括起来，多个区域名之间用空格分隔即可，例如'cert_role ,radius_role’。
before	可选项，增加访问控制规则时可以选择规则位置在那条规则之前。默认新添加的规则置于最后。
number1	数值，为已经添加的访问控制规则 ID 号。
group-name	可选项，指定策略组。不指定时表示默认组
string	策略组对象名
max-active-session	指定本条策略所允许的最大活动连接数。
string	数值
ids	选择已经设置的 IDS 规则对象，匹配到本条访问控制规则的数据包将根据相应的 IDS 对象对其进行处理。
string	字符串
original-dscp	设定是否检测 IP 报文的 DSCP 值，为可选项。如果设定了该值，则对于匹配 ACL 规则的 IP 报文，只有其 DSCP 值与该处设定的值匹配时，才修改为“目标 DSCP 值”设定的数值。如果不设定，则设备不检测报文的 DSCP 值，直接修改 DSCP 值。
string	
target-dscp	对于匹配 ACL 规则的报文，设置是否重新标记报文的 DSCP 优先级。网络卫士安全网关在转发时提供优先级标记服务，用来为下游的交换机或路由器等网络设备提供 DiffServ 体系的支持。
string	
cos	设置对于匹配 ACL 规则的报文，是否重新标记报文的 COS 值。 说明： 1．对于带有 802.1Q 标签头的以太网数据包，标签头中有 3 位优先级字段，用于指明数据包的优先级。网络卫士安全网关可以根据此处设定的 COS 值对优先级字段进行修改，供下游设备对数据流量进行管理。 2．该选项只有当数据报文的出接口为 Trunk 口时该选项有效。
number	
anti-proxy	是否启用防代理上网

on|off	是/否
qos	对符合规则的数据流进行流量监管，可以通过简单的设置下行限制带宽来进行流量监管，也可以通过勾选“高级”选项，选择设定的“QoS 对象”来设置更为细致的流量策略。 说明： 1）上行限制带宽：限制从 ACL 规则设定的源到目的传输数据时，带宽的最大值； 2）下行限制带宽：限制从目的到源传输数据时，带宽的最大值； 3）QoS 对象：选择已经添加的 QoS 对象，根据 QoS 对象的参数进行流量管理；要保证某些连接的传输带宽，必须设置出接口的总带宽；而且必须在 ACL 规则中设置数据出接口的区域，即对于“下行”的数据必须设置“源区域”。
string	字符串
ips-up	设置 IPS 上行策略对象
string	字符串
ips-down	设置 IPS 下行策略对象
string	字符串
traffic-statistic	可选项，设置是否开启流量统计开关
on|off	是、否
dns	可选项，选择设定的 DNS 资源对象名称
string	字符串

policy delete id <*number1*>[**vsid** <*number2*>]

命令描述：

删除一条访问控制规则。

参数说明：

delete	删除一条访问控制规则
id	指定访问控制规则 ID
number1	字符串，必须是已定义的规则 ID 值。
vsid	虚系统 ID，默认为 0。
number2	数值，虚系统号。

实例：

** 删除一条访问控制规则

policy delete id *8503* **vsid** *0*

policy move <*number1*>[**before** <*number2*>|**after** <*number3*>]

命令描述：

移动一条访问控制规则的位置。

参数说明：

move	移动一条访问控制规则的位置
number1	数值，表示待移动的规则的 ID 号。
before	设置将规则移动到指定规则之前。
number2	数值，表示参照物规则的 ID 号。
after	设置将规则移动到指定规则之后。
number3	数值，表示参照物规则的 ID 号。

实例：

**移动一条访问控制规则 8503 到规则 8490 之前

policy move *8503* **before** *8490*

policy show [**src** <*string*>] [**srcarea** <*string*>][**srcip** <*string*>] [**dst** <*string*>] [**dstarea** <*string*>] [**dstip** <*string*>] [**service** <*string*>] [**schedule** <*string*>] [**vsid** <*number2*>] [**group-name** < *string*>] [**from** < *number*>] [**to** <*number*>]

命令描述：

查看访问控制规则。

参数说明：

show	查看访问控制规则
src	可选项，指定源地址对象
string	字符串，为已定义的地址对象名。可以输入多个，格式为’aa ll’，用单引号，中间用空格分隔。
srcarea	可选项，设定源区域
string	字符串，必须为已定义的区域资源名，可以有一个或多个，需用单引号’ ‘括起来，多个区域名之间用空格分隔即可，例如'area_eth0 area_eth1'。
srcip	可选项，输入源 IP 的名称。
string	设定 IP 地址。
dst	可选项，目的地址对象
string	字符串，为已定义的地址对象名，可以输入多个，格式为’aa ll’，用单引号，中间用空格分隔。
dstarea	可选项，设定目标区域
string	字符串，为已定义的区域资源名，可以有一个或多个，需用单引号’ ‘括起来，多个区域名之间用空格分隔即可，例如'area_eth0 area_eth1'。
dstip	可选项，输入目的 IP 地址。
string	字符串，为已定义 VLAN 号。
service	可选项，设定服务资源
string	字符串，必须是系统缺省服务或自定义服务的名称，可以输入多个，格式为’IP ICMP’，用单引号，中间用

	空格分隔。名称的大小写必须与系统定义相一致，如'IP'。查看服务资源请使用命令#define service show default<cr>查看。
schedule	可选项，选择时间资源，必须在前面 define 模块已经定义。
string	对象名称。
vsid	可选项，虚系统 ID 号
number	数值
group-name	可选项，指定策略组。不指定时表示默认组
string	策略组对象名
from	指定开始显示的策略 ID
number	策略 ID
to	指定结束显示的策略 ID
number	策略 ID

实例：

** 查看所有访问控制规则

policy show<cr>

**查看源区域为 area_eth0 的访问控制规则

policy show srcarea *'area_eth0'*

policy clean [vsid<number>]

命令描述：

清空所有或某个虚系统的访问控制规则。

参数说明：

clean	清空访问控制规则
vsid	可选项，虚系统 ID 号
number	数值

实例：

** 清空所有访问控制规则

policy clean<cr>

**清空虚系统 1 的访问控制规则

policy clean vsid *1*

policy total [**dst** <*string*>] [**dstarea** <*string*>] [**dstip** <*string*>][**service** <*string*>][**src** <*string*>]

[**srcarea** <*string*>] [**srcip** <*string*>][**vsid** <*string*>] [**schedule** <*string*>] [**group-name** <*string*>]

命令描述：

根据对象统计访问控制规则的数量。

参数说明：

total	根据对象统计访问控制规则的数量
dst	可选项，设置查看某个目的地址对象相关的 ACL 规则总数。
string	地址对象字符串。
dstarea	可选项，设置查看某个目的区域相关的 ACL 规则总数。
string	字符串，输入区域名。
dstip	可选项，设置查看某个目的 IP 地址相关的 ACL 规则总数。
number	IP 地址字符串。
service	可选项，设置查看某个服务相关的 ACL 规则总数。
string	服务名称字符串。
src	可选项，设置查看某个源地址对象相关的 ACL 规则总数。
string	地址对象字符串。
srcarea	可选项，设置查看某个源区域相关的 ACL 规则总数。
string	字符串，输入区域名。
srcip	可选项，设置查看某个源 IP 地址相关的 ACL 规则总数。
string	IP 地址字符串。
vsid	可选项，设置查看某个虚系统的 ACL 规则总数。
string	字符串，输入虚系统 ID 号。
schedule	可选项，设置选择时间资源，必须在前面 define 模块已经定义。
string	对象名称。
group-name	可选项，指定策略组。不指定时表示默认组
string	策略组对象名

实例：

*查看虚系统 0 的访问控制规则总数

policy total vsid *0*

dynamic-policy

动态策略设置

dynamic-policy show [**src** < *ipaddress*>] [**dst** < *ipaddress*>]

命令描述：

显示动态策略。

参数说明：

show	显示动态策略
src	可选项，指定源 IP
ipaddress	IP 地址
dst	可选项，指定目的 IP
ipaddress	IP 地址

dynamic-policy delete [**src** < *ipaddress*>] [**dst** < *ipaddress*>]

命令描述：

删除动态策略。

参数说明：

delete	删除动态策略
src	可选项，指定源 IP
ipaddress	IP 地址
dst	可选项，指定目的 IP
ipaddress	IP 地址

dynamic-policy total<cr>

命令描述：

查看动态策略的总数

HA

配置高可用性参数。默认 HA 为停止状态。最好先设定 HA 的工作模式为 AA、AS 或 SP，然后再进行参数设定，否则在设置参数时可能提示错误信息。

为保证网络不间断的正常通信，可以采用两台网络卫士安全网关并联使用的方法，称为网络卫士安全网关的双机热备。在进行双机热备配置时，需要将两台网络卫士安全网关各通过一个物理接口相连，用于两台安全网关之间的状态信息的同步。本命令模块用于配置网络卫士安全网关的双机热备参数。

进入本命令模块操作如下：

ha<cr>

退出本命令模块操作如下：

end<cr>

下面将详细描述本命令模块下的所有管理命令。

ha check peer-config [detail]

命令描述：

设置 HA 对端设置是否和本地一致。输入 detail 时显示详细信息。

ha local <*ipaddress*>

命令描述：

设置 HA 接口的本地地址。

参数说明：

local	设置 HA 接口的本地地址。
ipaddress	IP 地址。

实例：

** 设置 HA 的本地地址为 192.168.10.1。

ha local *192.168.10.1*

ha local-seond-link <*ipaddress*>

命令描述：

设置 HA 心跳接口的二级连接地址。VRRPD 进程每隔 0.5s 检测一次心跳口的健康状况，如果检测到心跳口出现异常，则检测是否配置了心跳口二级连接，如果配置了二级连接，则通过二级连接进行 VRRP 报文的发送。二级心跳口之间只同步状态信息，不同步连接和配置信息。

参数说明：

local	设置 HA 心跳接口的二级连接地址
ipaddress	IP 地址。

ha peer <*ipaddress*>

命令描述：

设置 HA 接口的对端地址。

参数说明：

peer	设置 HA 接口的对端地址。
ipaddress	IP 地址。

实例：

** 设置 HA 的对端地址为 192.168.11.1。

ha peer *192.168.11.1*

ha no <local|peer>

命令描述：

清除 HA 接口的本地地址/对端地址。

参数说明：

no	清除 HA 的某些配置。
local|peer	本地地址/对端地址。

实例：

** 清除 HA 接口的本地地址。

ha no local

** 清除 HA 接口的对端地址。

ha no peer

ha no <local-second-link>

命令描述：

清除 HA 心跳口的二级连接地址

ha no vrid <*number*>

命令描述：

删除备份组的配置。

参数说明：

no	删除备份组的配置。
vrid	vrid 标示的备份组。
number	数值。

实例：

** 删除 vrid 为 2 的备份组的配置。

ha no vrid *2*

ha show [<configuration|status|metric>]

命令描述：

查看 HA 的配置信息。

参数说明：

show	查看 HA 的配置信息。
configuration	查看当前 HA 的参数配置。
status	查看本设备 HA 的运行状态。
metric	查看 VRID 组的优先级

实例：

** 查看当前 HA 参数配置。

ha show configuration

ha enable <cr>

命令描述：

启动 HA。HA 默认为停止状态，需要手工启动。

ha disable <cr>

命令描述：

停用 HA。

ha clean<cr>

命令描述：

清除 HA 的配置信息。

ha sync <from-peer|to-peer>

命令描述：

HA 同步（从对端机上同步配置/同步配置到对端机上）。

参数说明：

sync	HA 同步。
from-peer	从对端机上同步配置。
to-peer	同步配置到对端机上。

使用说明：

同步配置要在双机热备模式下。

实例：

** 从对端机上同步配置。

ha sync from-peer

** 同步配置到对端机上。

ha sync to-peer

ha mode <aa|as|sp>

命令描述：

HA 模式配置。

参数说明：

mode	HA 模式配置。
aa|as|sp	双机热备模式/负载均衡模式/连接保护模式。

实例：

** 配置 HA 模式为负载均衡模式。

ha mode aa

** 配置 HA 模式为双机热备模式。

ha mode as

ha rtosync ack <enable|disable>

命令描述：

动态数据同步应答开关。

参数说明：

rtosync	设置动态数据同步应答开关。
enable|disable	开/关。

ha rtosync ack time-out <*number*>

命令描述：

设置 HA 同步报文应答超时时间。

参数说明：

ack time-out	设置 HA 同步报文应答超时时间。
number	数值。 取值范围：10-500 毫秒；默认：10 毫秒。

ha rtosync ack resend-count <*number*>

命令描述：

设置 HA 同步报文重发次数。

参数说明：

ack resend-count	设置 HA 同步报文重发次数。
number	数值。 取值范围：0-5；默认：2。

ha rtosync statistic show <*cr*>

命令描述：

查看 HA 数据同步统计信息。

ha rtosync statistic reset <*cr*>

命令描述：

重置 HA 数据同步统计。

ha rtconfig-sync <enable|disable>

命令描述：

HA 配置实时同步开关。

参数说明：

rtconfig-sync	HA 配置实时同步开关
enable|disable	启动|停止

ha as-vrid <*number*>|<default>

命令描述：

设置 AS 模式下的 VRID。

参数说明：

as-vrid	设置 AS 模式下的 VRID 组。
number	AS 模式下的 VRID（1-254）。
default	AS 模式默认的 VRID 为 100。

ha vrid <*number1*> **priority** <*number2*>

命令描述：

备份组优先级设置。用户应当首先设定 HA 的工作模式，然后再设置备份组优先级参数，否则会有错误提示信息。

参数说明：

vrid	HA 备份组 ID。
number1	数值。
priority	HA 优先级设置。
number2	数值，如果 HA 模式为 AA，则范围为 1-255；如果 HA 模式为 AS，则必须设定为 100 或 254。

实例：

** 设置备份组优先级。

ha vrid *1* **priority** *2*

ha vrid <*number1*> **preempt** <enable|disable>

命令描述：

备份组抢占配置。用户应当首先设定 HA 的工作模式，然后再设置该参数，否则会有错误提示信息。

参数说明：

vrid	HA 备份组 ID。
number1	ID 号。
preempt	HA 抢占设置。
enable|disable	抢占/不抢占。

实例：

** 设置备份组抢占。

ha vrid *1* **preempt** enable

ha vrid <*number1*> **hold-down-time** < *number*>

命令描述：

HA 备份组接口故障抑制时间

参数说明：

vrid	HA 备份组 ID。
number1	ID 号。
hold-down-time	HA 备份组接口故障抑制时间
number	数值，范围为 0-10s。

ha vrid <*number1*> **priority** < *number*>

命令描述：

HA 优先级设置

参数说明：

vrid	HA 备份组 ID。
number1	ID 号。
priority	HA 优先级设置，
number	数值，AA 模式下范围为 1-255,AS 模式下为 100 或 254。

ha hello-interval <*number*>|<default>

命令描述：

设置 HA 心跳间隔。

参数说明：

hello-interval	设置报文发送间隔。
number	Hello 报文发送的间隔，以秒计（1-3）。
default	Hello 报文发送的默认间隔，1 秒。

实例：

** 设置 HA 心跳间隔为 2 秒。

ha hello-interval *2*

** 设置 HA 心跳间隔为默认。

ha hello-interval default

ha gratuitous-arp <*number*>

命令描述：

设置免费 ARP 个数。

参数说明：

gratuitous-arp	设置 VRID 组发送的免费 ARP 个数。
number	范围为 0-65535，0 表示无限个。

ha ip-probe < enable|disable >

命令描述：

设置 HA IP 探测开关。

参数说明：

ip-probe	设置 HA IP 探测开关
enable|disable	启用/禁用

ha ip-probe add probeid< *number*>

命令描述：

设置 HA IP 探测项目。

参数说明：

add	增加探测链路
probe-id	输入链路 ID
number	范围为 100-104。

ha ip-probe delete probeid< *number*>

命令描述：

删除 HA IP 探测项目。

参数说明：

delete	删除探测链路
probe-id	输入链路 ID
number	范围为 100-104。

ha ip-probe clean<cr>

命令描述：

清空所有 IP 探测项目。

HELPMODE

设置系统的提示语言

helpmode <chinese|english>

命令描述：

设置系统的提示语言。

参数说明：

helpmode	设置系统的提示语言。
chinese	信息文字采用中文显示。
english	信息文字采用英文显示。

实例：

** 设置系统的提示语言为中文。

helpmode chinese

IDS

本命令用来设置入侵检测的相关参数

进入本命令模块操作如下：

ids<cr>

退出本命令模块操作如下：

exit<cr>

CLI 管理员登录安全网关进入本命令模块后，可以执行相应的组件管理命令。下面将详细描述本命令模块下的所有组件管理命令。命令的实例输入格式将按已经进入本命令模块书写。

下一级命令列表

命令	功能
attack	显示或清除攻击统计信息
cc	CC 防护规则配置

config	显示 IDS 的当前配置信息
expire-time	设置或显示地址超时时间
list	名单列表
list-expire-time	设置或显示黑（白）名单超时时间
max-destination	设置或显示最大目的地址数
max-source	设置或显示最大源地址数
packet	设置或显示每个可信连接包含的报文数
rule	入侵检测规则配置
sessions	设置或显示连接数
source-check	配置源地址检查
tcp-trust-check	检测 tcp 首包是否可信
white-list-check	白名单

attack

显示或清除攻击统计信息。

attack show <cr>

命令描述：

显示当前系统受攻击状态。

参数说明：

show	显示当前系统受攻击状态。
cr	回车换行符。

attack clear <cr>

命令描述：

清除攻击统计信息。

参数说明：

clear	清除攻击统计信息。
cr	回车换行符。

cc

IDC CC 攻击防护规则相关设置。

cc add name <*string1*> **ipaddr** <*ipaddress*> **port** <*number1*> **url** <*string2*> **quota**<*number2*>

命令描述：

添加 CC 防护规则。

参数说明：

add	添加受保护主机。
name	规则名称。
string1	字符串。
ipaddr	受保护主机 IP 地址。
ipaddress	字符串。
port	受保护端口。
number1	数值，断口值。
url	URL 匹配对象名称。
string2	字符串。
quota	触发日志或报警的阀值。
number2	字符串，范围 1-65535，缺省 10。

使用说明：

URL 匹配对象必须事先添加，使用 **dpi pattern add url** 命令添加。

实例：

** 添加一则 CC 防护规则。

cc add name *cc_topsec_doc* **ipaddr** *192.168.1.54* **port** *80* **url** *topsecdoc* **quota** *500*

cc show<cr>

命令描述：

显示 CC 防护规则。

实例：

** 显示 CC 防护规则。

cc show<cr>

ID 8132 ids cc add name cc_topsec_doc ipaddr 192.168.1.54 port 80 url topsecdoc quota 500

cc modify name <*string1*> < [**ipaddr** <*ipaddress*>] [**port** <*number1*>] [**url** <*string2*>] [**quota**<*number2*>] >

命令描述：

修改 CC 防护规则。

参数说明：

modify	修改 CC 防护规则。
name	规则名称。
string1	字符串。
ipaddr	受保护主机 IP 地址。
ipaddress	字符串。
port	受保护端口。
number1	数值，端口值。
url	URL 匹配对象名称。
string2	字符串。
quota	触发日志或报警的阀值。
number2	字符串，范围 1-65535，缺省 10。

使用说明：

URL 匹配对象必须事先添加，使用 **dpi pattern add url** 命令添加。

实例：

** 修改名称为 cc_topsec_doc 的规则中受保护端口为 8080。

cc modify name *cc_topsec_doc* **port** *8080*

cc delete [< **name**<*string1*> **| id** <*string2*> >] <cr>

命令描述：

删除 CC 防护规则。

参数说明：

delete	删除 CC 防护规则。
name	规则名称。
string1	字符串。
id	规则 ID 编号。
string2	字符串。

使用说明：

不设置任何参数时，将删除所有 CC 防护规则。

实例：

** 删除 ID 为“8132”的 CC 防护规则。

cc delete id *8132*

cc clean<cr>

命令描述：

清除所有 CC 防护规则。

config

显示 IDS 的配置信息。

config show<cr>

命令描述：

显示 IDS 的配置信息。

实例：

config show<cr>

expire-time

设置或显示非处于待检测状态（不是在黑名单也不在白名单）的源地址的记录的超时时间。

expire-time set <*number*>

命令描述：

设置非处于待检测状态（不是在黑名单也不在白名单）的源地址的记录的超时时间。

参数说明：

set	设置非处于待检测状态（不是在黑名单也不在白名单）的源地址的记录的超时时间。
number	数字。 单位：秒；取值范围：1-3600 秒。

expire-time show <cr>

命令描述：

显示非处于待检测状态（不是在黑名单也不在白名单）的源地址的记录的超时时间。

参数说明：

show	显示非处于待检测状态（不是在黑名单也不在白名单）的源地址的记录的超时时间。
cr	回车换行符。

list

配置名单列表。

list address-set address <*string*> [initial|white|black]

命令描述：

设置某地址的状态。

参数说明：

address-set	设置某地址的状态
address	IPV4 地址信息
string	IPV4 地址格式
initial|white|black	初始状态|白名单|黑名单

list show [white|black]

命令描述：

显示当前黑名单或白名单的列表。

参数说明：

show	显示当前黑名单或白名单的列表
white|black	显示白名单的列表|显示黑名单的列表

list-expire-time

设置或显示黑/白名单超时时间。

list-expire-time set <*number*>

命令描述：

设置黑/白名单超时时间。

参数说明：

set	设置黑/白名单超时时间
number	数值。 取值范围：1-60 分钟。

list-expire-time show <cr>

命令描述：

显示黑/白名单超时时间。

max-destination

设置或显示 ids 保护的地址的个数上限值。

max-destination set <*number*>

命令描述：

设置 ids 保护的地址的个数上限值。

参数说明：

set	设置 ids 保护的地址的个数上限值
number	数值。 取值范围：1-100000。

max-destination show <cr>

命令描述：

显示 ids 保护的地址的个数上限值。

max-source

设置或显示系统记录的源地址个数的上限值。

max-source set <*number*>

命令描述：

设置系统记录的源地址个数的上限值。

参数说明：

set	设置系统记录的源地址个数的上限值。
number	数值。 取值范围：1-100000。

max-source show <cr>

命令描述：

显示系统记录的源地址个数的上限值。

packet

设置或显示每个可信连接包含的报文数。

packet set <*number*>

命令描述：

设置每个可信连接包含的报文数。

参数说明：

set	设置每个可信连接包含的报文数。
number	数值。 取值范围：0-65535。

packet show <cr>

命令描述：

显示每个可信连接包含的报文数。

rule

入侵检测规则同访问策略一样，用于控制通过安全网关的数据流。安全网关判断一个数据包是否可以通过时，首先查询入侵检测规则，然后使用访问策略来匹配。

rule add name <*string*> **synflood** <*numbe*> **udpflood** <*number*> **icmpflood** <*number*> **ipsweep** <*number*> **portscan** <*number*> **abntype** <*string*> **stattype** <*string*> **log**<on|off|>

命令描述：

添加 IDS 规则。

参数说明：

add	添加 IDS 规则
name	输入规则名
string	字符串。
synflood	synflood 类型攻击，触发日志或警报阀值。
numbe	数值，范围 1-65535，缺省 500。
udpflood	udpflood 类型攻击，触发日志或警报阀值。
number	数值，范围 1-65535，缺省 1000。
icmpflood	icmpflood 类型攻击，触发日志或警报阀值。
number	数值，范围 1-65535，缺省 1000。
ipsweep	ipsweep 类型攻击，触发日志或警报阀值。
number	数值，范围 1-65535，缺省 10。
portscan	portscan 类型攻击，触发日志或警报阀值。
number	数值，范围 1-65535，缺省 10。
abntype	异常攻击
string	字符串，可以设定 Land、smurf、pingofdeath、winnuke、teardrop、targa3、tcp_sscan|ip_option、ipspoof、icmpredrt 中的一个或多个，设定多个时格式举例： ’land smurf’。
stattype	统计型攻击
string	字符串，可以设定 synflood、udpflood、icmpflood、portscan、ipsweep 中的一个或多个，设定多个时格式举例： ’ synflood udpflood’
log	是否记录日志
on|off	是/否

实例：

**添加一则入侵过滤规则。

rule add name ids_t*opsec_doc* **synflood** *300* **udpflood** *500* **icmpflood** *700* **ipsweep** *20* **portscan** *15*

rule show<cr>

命令描述：

显示入侵检测规则。

rule show name <string>

命令描述：

显示某一条入侵检测规则。

rule modify name<*string*> **synflood** <*numbe*> **udpflood** <*number*> **icmpflood** <*number*>

ipsweep <*number*> **portscan** <*number*> **abntype** <*string*> **stattype** <*string*> **log** <on|off|>

命令描述：

修改 IDS 规则。

参数说明：

modify	修改 IDS 规则
name	输入规则名
string	字符串。
synflood	synflood 类型攻击，触发日志或警报阀值。
numbe	数值，范围 1-65535，缺省 500。
udpflood	udpflood 类型攻击，触发日志或警报阀值。
number	数值，范围 1-65535，缺省 1000。
icmpflood	icmpflood 类型攻击，触发日志或警报阀值。
number	数值，范围 1-65535，缺省 1000。
ipsweep	ipsweep 类型攻击，触发日志或警报阀值。
number	数值，范围 1-65535，缺省 10。
portscan	portscan 类型攻击，触发日志或警报阀值。
number	数值，范围 1-65535，缺省 10。
abntype	异常攻击
string	字符串，可以设定 Land、smurf、pingofdeath、winnuke、teardrop、targa3、tcp_sscan|ip_option、ipspoof、icmpredrt 中的一个或多个，设定多个时格式举例： ’land smurf’。
stattype	统计型攻击
string	字符串，可以设定 synflood、udpflood、icmpflood、portscan、ipsweep 中的一个或多个，设定多个时格式举例： ’ synflood udpflood’
log	是否记录日志
on|off	是/否

rule delete id <*string*>

命令描述：

删除入侵检测规则。

参数说明：

delete	删除入侵检测规则。

id	入侵检测规则 ID 编号。
string	字符串。

实例：

** 删除 ID 为“8127”的入侵检测规则。

rule delete id *8127*

rule clean<cr>

命令描述：

清除所有入侵检测规则。

sessions

设置或显示连接数。

sessions set <*number*>

命令描述：

设置加入白名单必须建立的可信连接的个数。

参数说明：

set	设置加入白名单必须建立的可信连接的个数。
number	数值。 取值范围：1-65535。

sessions show <cr>

命令描述：

显示加入白名单必须建立的可信连接的个数。

source-check

配置源地址检查。

source-check [on|off]

命令描述：

开启或者关闭源地址检查功能。

参数说明：

source-check	源地址检查开关。
on|off	On 表示开启；off 表示|关闭；

source-check show <cr>

命令描述：

查看源地址检查功能的状态。

tcp-trust-check

TCP 首包可信检测

tcp-trust-check <on|off>

命令描述：

开启或者关闭 TCP 首包可信检测功能。

参数说明：

source-check	TCP 首包可信检测开关。
on|off	on 表示开启；off 表示关闭。

tcp-trust-check show <cr>

命令描述：

查看 TCP 首包可信检测开关的状态。

white-list-check

配置白名单检查。

white-list-check [on|off]

命令描述：

允许或者关闭白名单功能。

参数说明：

white-list-check	白名单开关。
on|off	允许|关闭

white-list-check show <cr>

命令描述：

查看白名单功能状态。

LOG

本命令主要用来配置网络卫士安全网关的日志服务器、报警规则、报警方式等内容和参数。

进入本命令模块操作如下：

log<cr>

退出本命令模块操作如下：

end<cr>

CLI 管理员登录安全网关并进入本命令模块后，可以执行相应的组件管理命令。下面将详细描述本命令模块下的所有组件管理命令。命令的实例输入格式将按已经进入本命令模块书写。

下一级命令列表

命令	功能
alarmevent	报警规则配置
alarmnotice	报警方式配置
log	日志和日志服务器配置

alarmevent

安全网关的报警规则管理，在此用户可以设置对指定类型的事件采用指定的报警

方式进行报警。

alarmevent set <manage|system|security|policy|communication|hardware|recover|noticetest|all> **noticeid** <*number*> | **noticename** <*string*> | **notice** <empty>

命令描述：

根据类别设置事件的报警方式。

参数说明：

set	设置事件的报警方式。
manage|system|security|policy|communication|hardware|recover|noticetest|all	manage 表示管理系统时报警，system 表示系统报警，security 表示安全报警，policy 表示策略报警，communication 表示通信报警，hardware 表示硬件报警，recover 表示恢复报警，noticetest 表示测试报警，all 表示所有事件都报警。
noticeid	设置报警方式的 ID 号。
number	数值，表示报警方式 ID 号。
noticename	设置报警方式的名称。
string	字符串，表示报警方式名称。
notice	设置报警方式中不含报警事件规则，去掉所有的报警事件。
empty	表示不报警。

实例：

** 设置报警规则，当硬件发生变化时，采用 beep1 报警（beep1 是定义的声音报警方式）。

alarmevent set hardware **noticename** *beep1*

alarmevent show <manage|system|security|policy|communication|hardware|recover|noticetestall>

命令描述：

查看某报警事件。

参数说明：

show	查看某报警事件。
manage|system|security|policy|communication|hardware|recover|noticetest|all	manage 表示管理系统时报警，system 表示系统报警，security 表示安全报警，policy 表示策略报警，communication 表示通信报警，hardware 表示硬件报警，recover 表示恢复报警，noticetest 表示测试报警，all 表示查看所有报警事件。

实例：

** 查看安全报警事件。

alarmevent show security<cr>

log alarmevent set security noticeid '9044 9039'

alarmevent show<cr>

命令描述：

查看系统中所有的报警事件。

实例：

** 查看系统中所有的报警事件。

alarmevent show<cr>

log alarmevent set system noticeid '9044'

log alarmevent set security noticeid '9044 9039'

log alarmevent set policy noticeid '9039'

log alarmevent set communication noticeid '9044'

log alarmevent set recover noticeid '9044 9039'

alarmnotice

安全网关的报警方式管理。网络卫士安全网关可以根据预先定义的策略及安全报警事件自动触发报警，可以通过扬声器、邮件、控制台、SNMP、NETBIOS 网络信使报警等方式向管理员发出报警信息。在此用户可以设置各种报警方式下的相关参数。

alarmnotice add <beep> **name** <*string*> [<default>] | [**freq** <*number1*> **length** <*number2*> **reps** <*number3*> **delay** <*number4*>]

命令描述：

添加一个声音报警。

参数说明：

add	添加一个声音报警。
beep	表示报警方式为声音报警。

name	设置报警名称。
string	字符串，表示报警名称。
default	使用声音报警的默认值，选择此项后不再需要设置下面的参数。
freq	设置声音输出频率。
number1	数值，表示声音输出频率，单位为 HZ，范围为 1-1000HZ。
length	设置声音长度。
number2	数值，表示声音长度，单位为微秒，范围为 1-1000 微秒。
reps	设置声音的重复次数。
number3	数值，表示声音重复次数，单位为次，范围为 1-100 次。
delay	设置两次发声的间隔。
number4	数值，表示发声间隔，单位为微秒，范围为 1-1000 微秒。

使用说明：

声音报警属性设为 default 时，各参数默认值见下表。

freq	440HZ
length	200 微秒
reps	5 次
delay	100 微秒

实例：

** 添加一个缺省的声音报警 beep1。

alarmnotice add beep **name** *beep1* default

alarmnotice add <mail> **name** <*string1*> **srvaddr** <*ipaddress*> **srvport** <*number*> **mailaddr** <*string2*> **auth** <on|off> [**username** <*string*> **password** <*string*>] **subject** <*string*>

命令描述：

添加一个邮件报警。

参数说明：

add	添加一个邮件报警。
mail	表示报警方式为邮件报警。
name	设置报警名称。
string1	字符串，表示报警名称。
srvaddr	设置要使用的发送邮件的 SMTP 服务器的 IP 地址。
ipaddress	字符串，表示 IP 地址，格式为 192.168.83.6。
srvport	设置 SMTP 发件服务器的端口。
number	数值，表示端口号。
mailaddr	设置接收报警邮件的邮件帐户。
string2	字符串，表示电子邮件地址，例如 abc@topsec.com.cn。
auth	设置邮件服务器要求进行认证
on|off	on 表示是，off 表示否。

username	当邮件服务器需要认证时，输入用户名。当“auth”设置为 off 时不需要设置该项。
string	字符串
password	当邮件服务器需要认证时，输入用户密码。当“auth”设置为 off 时不需要设置该项。
string	字符串
subject	设置报警邮件的主题。
string3	字符串，表示邮件主题。

实例：

** 添加一个发送到 user@topsec.com.cn的邮件报警mail1，SMTP邮件服务器的IP地址为 192.168.1.2，端口为 25，设置报警邮件主题为“邮件报警”。

alarmnotice add mail **name** *mail1* **srvaddr** *192.168.1.2* **srvport** *25* **mailaddr** *user@topsec.com.cn* **auth** off **subject** *邮件报警*

alarmnotice add <netbios> **name** <*string1*> **hostname** <*string2*> [**ipaddr** <*ipaddress*>]

命令描述：

添加一个 netbios 报警。

参数说明：

add	添加一个 netbios 报警。
netbios	表示报警方式为 netbios 报警。
name	设置报警名称。
string1	字符串，表示报警名称。
hostname	设置接收报警信息的主机名称。
string2	字符串，表示 netbios 主机名称。netbios 主机命名必须符合规范，只能由数字、字母、下划线“_”和中横线“-”组成，其他字符均为非法字符。
ipaddr	设置接收报警信息的主机 IP 地址。
ipaddress	字符串，表示 IP 地址，格式为 192.168.83.6。

实例：

** 添加一个发送到 host1（IP：192.168.1.6）的 netbios 报警 netbios1 。

alarmnotice add netbios **name** *netbios1* **hostname** *host1* **ipaddr** *192.168.1.6*

alarmnotice add <console|snmp> **name** <*string*>

命令描述：

添加一个控制台或 SNMP 报警。

参数说明：

add	添加一个报警。
console|snmp	表示报警方式为控制台报警或 SNMP 报警。
name	设置报警名称。
string	字符串，表示报警名称。

实例：

** 添加一个控制台报警 console1。

alarmnotice add console **name** *console1*

alarmnotice modify <beep> **name** <*string*> [<default>] | [**freq** <*number1*> **length** <*number2*>

reps <*number3*> **delay** <*number4*>]

命令描述：

修改一个声音报警。

参数说明：

modify	修改一个声音报警。
beep	表示报警方式为声音报警。
name	指定要修改的报警名称。
string	字符串，表示报警名称。
default	使用声音报警的默认值，选择此项后不再需要修改下面的参数。
freq	设置声音输出频率。
number1	数值，表示声音输出频率，单位为 HZ，范围为 1-1000HZ。
length	设置声音长度。
number2	数值，表示声音长度，单位为微秒，范围为 1-1000 微秒。
reps	设置声音的重复次数。
number3	数值，表示声音重复次数，单位为次，范围为 1-100 次。
delay	设置两次发声的间隔。
number4	数值，表示发声间隔，单位为微秒，范围为 1-1000 微秒。

使用说明：

声音报警属性设为 default 时，各参数默认值见下表。

freq	440HZ
length	200 微秒
reps	5 次
delay	100 微秒

实例：

** 将 beep1 报警的参数修改为不使用默认值，而使用以下的指定值。

alarmnotice modify beep **name** *beep1* **freq** *10* **length** *100* **reps** *5* **delay** *80*

alarmnotice modify <mail> **name** <*string1*> **srvaddr** <*ipaddress*> **srvport** <*number*> **mailaddr** <*string2*> [**subject** <*string3*>]

命令描述：

修改一个邮件报警的相关参数。

参数说明：

modify	修改一个邮件报警。
mail	表示报警方式为邮件报警。
name	指定要修改的报警的名称。
string1	字符串，表示报警名称。
srvaddr	修改要使用的发送邮件的 SMTP 服务器的 IP 地址。
ipaddress	字符串，表示 IP 地址，格式为 192.168.83.6。
srvport	修改 SMTP 发件服务器的端口。
number	数值，表示端口号。
mailaddr	修改接收报警邮件的邮件帐户。
string2	字符串，表示电子邮件地址，例如 abc@topsec.com.cn。
subject	修改报警邮件的主题。
string3	字符串，表示邮件主题。

实例：

** 将邮件报警 mail1 修改为发送到 user2@topsec.com.cn。

alarmnotice modify mail **name** *mail1* **srvaddr** *192.168.1.2* **srvport** *25* **mailaddr** *user2@topsec.com.cn* **subject** *邮件报警*

alarmnotice modify <mail> **name** <*string1*> **auth** <on|off> **username** <*string2*> **password** <*string3*>

命令描述：

修改邮件报警方式的认证属性：服务器是否要求认证。

参数说明：

modify	修改邮件报警。
mail	表示报警方式为邮件报警。
name	指定要修改的报警的名称。
string1	字符串，表示报警名称。
auth	设置邮件报警的邮件服务器是否需要认证。
on|off	off 表示不需要认证，选择此项时不需要设置下面的参数；on 表示需要认证。

username	邮件服务器认证的用户名。
string2	字符串，表示用户名。
password	邮件服务器认证的密码。
string3	字符串，表示用户密码。

实例：

** 将邮件报警 mail1 修改为需要认证，认证的用户名/密码为：user/user。

alarmnotice modify mail **name** *mail1* **auth** on **username** *user* **password** *user*

alarmnotice modify <netbios> **name** <*string1*> **hostname** <*string2*> [**ipaddr** <*ipaddress*>]

命令描述：

修改一个 netbios 报警。

参数说明：

modify	修改一个 netbios 报警。
netbios	表示报警方式为 netbios 报警。
name	指定需要修改的报警的名称。
string1	字符串，表示报警名称。
hostname	修改接收报警信息的主机名称。
string2	字符串，表示主机名称。
ipaddr	修改接收报警信息的主机 IP 地址。
ipaddress	字符串，表示 IP 地址，格式为 192.168.83.6。

实例：

** 将 netbios1 报警的接收主机 IP 地址修改为：192.168.1.8。

alarmnotice modify netbios **name** *netbios1* **hostname** *host1* **ipaddr** *192.168.1.8*

alarmnotice delete name <*string*> **| id** <*number*>

命令描述：

删除一个报警。

参数说明：

delete	删除一个报警。
name	指定要删除的报警的名称。
string	字符串，表示报警名称。
id	指定要删除的报警的 ID 号。
number	数值，表示 ID 号。

使用说明：

只有当该报警规则的报警事件为空时才可以删除，否则会提示错误信息。

实例：

** 删除报警 beep1。

alarmnotice delete name *beep1*

alarmnotice clean<cr>

命令描述：

清除所有报警规则。只有当报警规则中包含的报警事件均为空时才可以操作成功。

alarmnotice show [**name** <*string*>] **|** [**id** <*number*>]

命令描述：

查看报警。

参数说明：

show	查看报警。
name	指定要查看的报警的名称。
string	字符串，表示报警名称。
id	指定要查看的报警的 ID 号。
number	数值，表示 ID 号。

实例：

** 查看名称为 mail1 的报警。

alarmnotice show name *mail1*

** 查看所有的报警。

alarmnotice show<cr>

alarmnotice test<cr>

命令描述：

测试报警。

使用说明：

为了方便用户，网络卫士安全网关提供了报警测试功能。成功添加报警方式和设置触发报警的安全事件后，用户可以通过测试来验证报警规则的有效性。

log

安全网关的日志管理，在此用户可以设置将安全网关的日志传输到日志服务器进行查看和存储，也可以直接在安全网关上对部分日志进行查看和检索。

log clean <cr>

命令描述：

清空所有日志类型缓存。

实例：

** 清空所有日志类型缓存。

log clean <cr>

Total log clean

log clean type <mix|ips|av>

命令描述：

清空日志类型缓存。

log set ipaddr <*ipaddress*> [**port** <*string*>][**logtype** <syslog|welf>] [**trans**<enable|disable>]

命令描述：

设置日志服务器。

参数说明：

set	设置日志服务器。
ipaddr	设置日志服务器的 IP 地址。
ipaddress	字符串，表示 IP 地址。
port	设置日志服务器的端口。
string	字符串，表示端口号，格式为 tcp:80 或 udp:80。
logtype	设置日志传输格式，有 2 种：syslog 和 welf。
syslog|welf	缺省为 syslog。
trans	设置是否传输日志。
enable|disable	enable 表示传输日志，disable 表示不传输日志。

使用说明：

网络卫士安全网关生成的日志信息，需要配置日志服务器来管理。缺省时日志服务器的 IP 地址为 192.168.1.253，所用协议及端口号为 udp：514，日志传输格式为 syslog，不传输日志。

实例：

** 设置日志服务器为 192.168.1.25，端口为 TCP：524，日志传输类型为 syslog，并允许传输日志。

log set ipaddr *192.168.1.25* **port** tcp:*524* **logtype** syslog **trans** enable

log count <cr>

命令描述：

查看日志总数目。

实例：

** 查看日志总数目。

log count<cr>

Total log : 351

log count type < mix|ips|av >

命令描述：

查看日志类型。

log level_set <*number***>**

命令描述：

设置哪些级别的日志传输到日志服务器。

参数说明：

level_set	设置要传输到日志服务器的日志的级别。
number	数值，表示日志级别，范围为 0—8，其中 0 表示造成系统不可用的严重错误，1 表示警报信息，2 表示造成系统某些功能不可用的错误，3 表示一般的错误信息，4 表示所有的攻击行为以及非授权访问（除通信日志外），5 表示管理员的操作记录，6 表示普通的事件记录，7 表示开发人员调试信息，

	8 表示诊断日志。

实例：

** 设置向日志服务器传输 5 级及以下级别日志。

log level_set *5*

log log_key set <*string*>

命令描述：

设置日志加密传输时的加密口令。

参数说明：

log_key	设置加密口令。
set	设置口令。
string	字符串，表示加密口令，长度必须为 8 位字符。

实例：

** 设置日志加密传输时的加密口令为：talentpw。

log log_key set *talentpw*

log type_set add < avse|mgmt|system|pf| conn|ac|secure|dpi|stat| user_auth|ips|asse|ar | sv_system| sv_wf | sv_netacc| sv_cifs | sv_pf |vpn|none >

命令描述：

添加传输到日志服务器的日志类型。

参数说明：

type_set	设置日志类型。
add	设置要添加的传输到日志服务器的日志类型。
avse|mgmt|system|pf| conn|ac|secure|dpi|stat| user_auth|ips|asse|ar | sv_system|sv_wf| sv_netacc| sv_cifs | sv_pf |vpn|none	avse（防病毒）、mgmt（配置管理）、system（系统运行）、pf（阻断策略）、conn（连接）、ac（访问控制）、secure（防攻击）、dpi（深度内容检测）、stat（端口流量）、user_auth（用户认证）、ips（入侵防御）、vpn（虚拟专网）、asse（防垃圾邮件）、sv_system（SSLVPN 的系统）、sv_wf（SSLVPN 的 Web 转发）、sv_netacc（SSLVPN 的全网介入）、sv_cifs（SSLVPN 的文件共享）、sv_pf（SSLVPN 的端口转发）、或 none（全不选）。

实例：

** 将 vpn 类型的日志传输到日志服务器。

log type_set add vpn

log type_set delete < avse|mgmt|system|pf| conn|ac|secure|dpi|stat| user_auth|ips|asse|ar |

sv_system| sv_wf | sv_netacc| sv_cifs | sv_pf |vpn|none >

命令描述：

删除传输到日志服务器的日志类型。

参数说明：

type_set	设置日志类型。
delete	设置要删除的传输到日志服务器的日志类型。
avse|mgmt|system|pf| conn|ac|secure|dpi|stat| user_auth|ips|asse|ar | sv_system|sv_wf| sv_netacc| sv_cifs | sv_pf |vpn|none	avse（防病毒）、mgmt（配置管理）、system（系统运行）、pf（阻断策略）、conn（连接）、ac（访问控制）、secure（防攻击）、dpi（深度内容检测）、stat（端口流量）、user_auth（用户认证）、ips（入侵防御）、vpn（虚拟专网）、asse（防垃圾邮件）、sv_system（SSLVPN 的系统）、sv_wf（SSLVPN 的 Web 转发）、sv_netacc（SSLVPN 的全网介入）、sv_cifs（SSLVPN 的文件共享）、sv_pf（SSLVPN 的端口转发）、或 none（全不选）。

实例：

** 在传输到日志服务器的日志类型中，删除 vpn 类型。

log type_set delete vpn

log log_crypt <enable|disable>

命令描述：

设置传输到日志服务器的日志是否加密。

参数说明：

log_crypt	设置传输日志是否加密。
enable|disable	enable 表示加密，disable 表示不加密。

实例：

** 设置将加密后的日志传输到日志服务器。

log log_crypt enable

log set_show<cr>

命令描述：

查看日志服务器的配置信息。

log show from<*number1*> **to** <*number2*> [**keyword** <*string*>] **type** <mix|ips|av>

命令描述：

查看日志信息。

参数说明：

show	查看日志信息。
from	设置从第几条日志开始查看。
number1	数值，表示日志的序号。
to	设置查看到第几条日志。
number2	数值，表示日志的序号。
keyword	可选项，设置要查看的日志中的关键字。
string	字符串，表示关键字。
type	设置要查看的日志类型。
mix|ips|av	混合|IPS|AV

实例：

** 查看第 10 条到第 100 条中的包含字符串 log 的日志信息。

log show from *10* **to** *100* **keyword** *log*

NAT

本模块中的命令主要用来进行地址转换策略的相关配置。

进入本命令模块操作如下：

nat<cr>

退出本命令模块操作如下：

end<cr>

CLI 管理员登录网关进入本命令模块后，可以执行相应的组件管理命令。下面将详细描述本命令模块下的所有组件管理命令。命令的实例输入格式将按已经进入本命令模块书写。

下一级命令列表

命令	功能
policy	配置地址转换策略。

policy

该组命令用于配置地址转换策略。当数据包通过网关时，网关将按照地址转换策略的排列顺序检索地址转换策略表，逐一与数据包匹配。一旦存在一条匹配的地址转换策略，网关将停止检索，并按所定义的策略处理数据包。如果没有可匹配的地址转换策略，网关将按照缺省策略，即“不做转换”方式，不修改数据包的任何信息，直接转发。

policy add [**srcarea** <*srcarea_nam*>] [**dstarea** <*dstarea_nam*>] [**srcvlan** <*srcvlan_no*>] [**dstvlan** <*dstvlan_no*>] [**orig_src** <*src_addr1*>] [**orig_dst** <*dst_addr1*>] [**orig_sport** <*sport_id*>] [**orig_service** <*ser_id*>] [**trans_src** < src_addr2>] [**trans_dst** <*dst_addr2*>] [**trans_service** <*ser_obj*>] [**vsid** <*number1*>] [**pat** <yes|no>] [**enable** <yes|no>] [**before** <*number2*>] [**comment** <*string*>]

命令描述：

本命令用于增加地址转换策略。

参数说明：

add	增加地址转换策略。
srcarea	设定源区域。
srcarea_nam	字符串，输入源区域资源名称。 说明： 该参数值必须是已经定义的区域资源名称，可以输入一个或多个区域资源的名称，输入多个时用单引号括起来，并用空格隔开，如’area1 area2’。
dstarea	设定目标区域。
dstarea_nam	字符串，输入目的区域资源名称。 说明： （1）该参数值必须是已经定义的区域资源名称，可以输入一个或多个区域资源的名称，输入多个时用单引号括起来，并用空格隔开，如’area1 area2’。 （2）添加目的地址转换策略时，不能设定该参数值。
srcvlan	设定源 VLAN。
srcvlan_no	字符串，输入源 VLAN 的名称。 说明： 该参数值必须是已经定义的 VLAN 名称，可以输入一个或多个 VLAN 的名称，输入多个时用单引号括起来，并

	用空格隔开，如’vlan.0001 vlan.0002’。
dstvlan	设定目的 VLAN。
dstvlan_no	字符串，输入目的 VLAN 的名称。 说明： （1）该参数值必须是已经定义的 VLAN 名称，，可以输入一个或多个 VLAN 的名称，输入多个时用单引号括起来，并用空格隔开，如’ vlan.0001 vlan.0002’。 （2）添加目的地址转换策略时，不能设定该参数值。
orig_src	设定原始报文的源对象。
src_addr1	字符串，输入原始报文的源对象名称。 说明： （1）该参数值必须是已经定义的地址对象名称。 （2）可以同时输入多个地址对象，输入格式为’test1 test2’。地址对象用单引号括起来，并且中间用空格分隔。
orig_dst	设定原始报文的目的对象。
dst_addr1	字符串，输入原始报文的目的对象名称。 说明： （1）该参数值必须是已经定义的地址对象名称。 （2）可以同时输入多个地址对象，输入格式为’test1 test2’。地址对象用单引号括起来，并且中间用空格分隔。
orig_sport	设定原始报文的源端口对象。
sport_id	字符串，输入原始报文的源端口对象名称。 说明： （1）该参数值必须是已经定义的服务资源名称。 （2）可以同时输入多个服务资源，输入格式为’server1 server2’。服务资源用单引号括起来，并且中间用空格分隔。
orig_service	设定原始报文的服务资源。
ser_id	字符串，输入原始报文的服务资源名称。 说明： （1）该参数值必须是已经定义的服务资源名称。 （2）可以同时输入多个服务资源，输入格式为’server1 server2’。服务资源用单引号括起来，并且中间用空格分隔。
trans_src	设定转换后的源对象。
src_addr2	字符串，输入转换后的源对象名称。 说明： （1）该参数值必须是已经定义的地址对象或属性名称。 （2）只能输入一个对象。 （3）添加源地址转换策略时，该参数值必须设置。
trans_dst	设定转换后的目的对象。
dst_addr2	字符串，输入转换后的目的对象名称。 说明： （1）该参数值必须是已经定义的主机地址对象或均衡组对象名称。 （2）只能输入一个对象名。 （3）添加目的地址转换策略时，该参数值必须设置。
trans_service	设定转换后的服务资源。
ser_obj	数值类型，输入转换后的服务资源的名称。 说明：

	该参数值必须是 define 模块已经定义的名称。
vsid	设定虚拟系统的 ID。
number1	数值类型，输入该地址转换策略所属的虚拟系统的 ID。
pat	设定源端口转换开关。
yes|no	yes 表示对源端口进行端口转换；no 表示不对源端口进行端口转换。 说明： 默认值为“yes”。
enable	设定地址转换策略开关。
yes|no	yes 表示启用这条地址转换策略；no 表示暂时禁用这条地址转换策略。 说明： 默认值为“yes”。
before	设定这条地址转换策略位于某条策略之前。
number2	数值类型，输入这条地址转换策略之后的下一个地址转换策略的 ID。 说明： （1）该参数值必须是已经添加的地址转换策略的 ID。 （2）查看系统缺省服务资源的 ID 使用如下命令：TopsecOS# define service show default<cr>；查看系统缺省服务资源的 ID 使用如下命令：TopsecOS# define service show default<cr>。
comment	可选项，添加必要的描述信息
string	字符串

使用说明：

1. 定义目的地址转换策略时，不能指定目的区域和目的 VLAN。

2. 系统默认情况下，在源地址转换同时也会转换源端口。

3. 未做接口绑定的属性资源不能作为地址转换策略的转换后地址。

实例：

** 在虚系统 0 中增加并启用一条源地址转换策略，使内网中的主机 A 通过网关访问公网时，使用公网地址“201.10.10.1”，并使该策略应用在 ID 为 8144 的地址转换策略之前。已知：（1）主机 A 的 IP 地址为“10.10.10.22”（地址对象名称为“10.22”）；（2）主机 A 转换后的公网地址为“201.10.10.1”（地址对象名称为“公网地址 1”）；（3）网关的 eth0 连接内网，eth1 连接公网（区域资源名称分别为“area_eth0”和“area_eth1”）。

policy add srcarea *area_eth0* **dstarea** *area_eth1* **orig_src** *10.22* **trans_src** *公网地址 1* **vsid** *0* **enable** yes **before** *8144*

** 在虚系统 0 中增加并启用一条目的地址转换策略，当公网 Internet 用户通过网

关访问 WEB 服务器时，为了隐藏服务器在内网中的真实地址 172.168.1.2（地址对象名称为“web_server1”），使用公网地址 202.99.27.201（地址对象名称为“nat_address1”）作为用户的访问地址。

policy add orig_dst *nat_address1* **orig_service** HTTP **trans_dst** *web_server1* **vsid** *0* **enable** yes

** 在虚系统 0 中增加并启用一条双向地址转换策略，以便内网用户 A 通过网关访问内网的 WEB 服务器。已知：（1）用户 A 的 IP 地址为“192.168.83.220/24”（地址对象名称为“83.220”），转换后地址为“10.10.10.20”（地址对象名称为“nat_address2”）；（2）WEB 服务器的 IP 地址为“192.168.83.234/24”（地址对象名称为“83.234”），转换后地址为“10.10.10.23”（地址对象名称为“nat_address3”）；（3）WEB 服务器通过自定义的 8080 端口提供 WEB 服务（自定义服务资源名称为“HTTP-8080”）。

policy add orig_src *83.220* **orig_dst** *83.234* **orig_service** HTTP **trans_src** *nat_address2* **trans_dst** *nat_address3* **trans_service** *HTTP-8080* **vsid** *0* **enable** yes

policy modify id <*number1*> [**srcarea** <*srcarea_nam*>] [**dstarea** <*dstarea_nam*>] [**srcvlan** <*srcvlan_no*>] [**dstvlan** <*dstvlan_no*>] [**orig_src** <*src_addr1*>] [**orig_dst** <*dst_addr1*>] [**orig_sport** <*sport_id*>] [**orig_service** <*ser_id*>] [**trans_src** < src_addr2>] [**trans_dst** <*dst_addr2*>] **[trans_service** <*ser_obj*>] [**vsid** <*number2*>] [**pat** <yes|no>] [**enable** <yes|no>] [**comment** <*string*>]

命令描述：

本命令用于修改地址转换策略。

参数说明：

modify	修改地址转换策略。
id	设定需要修改的策略 ID。
number1	数值类型，输入需要修改的策略 ID。
srcarea	修改源区域。
srcarea_nam	字符串，输入修改后的源区域资源名称。 说明： 该参数值必须是已经定义的区域资源名称，可以输入一个或多个区域资源的名称，输入多个时用单引号括起来，并用空格隔开，如’area1 area2’。

dstarea	修改目标区域。
dstarea_nam	字符串，输入修改后的目的区域资源名称。 说明： （1）该参数值必须是已经定义的区域资源名称，可以输入一个或多个区域资源的名称，输入多个时用单引号括起来，并用空格隔开，如’area1 area2’。。 （2）对于目的地址转换策略，不能设定该参数值。
srcvlan	修改源 VLAN。
srcvlan_no	字符串，输入修改后的源 VLAN 的名称。 说明： 该参数值必须是已经定义的 VLAN 名称，可以输入一个或多个 VLAN 的名称，输入多个时用单引号括起来，并用空格隔开，如’ vlan.0001 vlan.0002’。
dstvlan	修改目的 VLAN。
dstvlan_no	字符串，输入修改后的目的 VLAN 的名称。 说明： （1）该参数值必须是已经定义的 VLAN 名称，可以输入一个或多个 VLAN 的名称，输入多个时用单引号括起来，并用空格隔开，如’ vlan.0001 vlan.0002’。 （2）对于目的地址转换策略，不能设定该参数值。
orig_src	修改原始报文的源对象。
src_addr1	字符串，输入修改后的原始报文的源对象名称。 说明： （1）该参数值必须是已经定义的地址对象名称。 （2）可以同时输入多个地址对象，输入格式为’test1 test2’。地址对象用单引号括起来，并且中间用空格分隔。
orig_dst	修改原始报文的目的对象。
dst_addr1	字符串，输入修改后的原始报文的目的对象名称。 说明： （1）该参数值必须是已经定义的地址对象名称。 （2）可以同时输入多个地址对象，输入格式为’test1 test2’。地址对象用单引号括起来，并且中间用空格分隔。
orig_sport	修改原始报文的源端口对象。
sport_id	字符串，输入修改后的原始报文的源端口对象名称。 说明： （1）该参数值必须是已经定义的服务资源名称。 （2）可以同时输入多个服务资源，输入格式为’server1 server2’。服务资源用单引号括起来，并且中间用空格分隔。
orig_service	修改原始报文的服务资源。
ser_id	字符串，输入修改后的原始报文的服务资源名称。 说明： （1）该参数值必须是已经定义的服务资源名称。 （2）可以同时输入多个服务资源，输入格式为’server1 server2’。服务资源用单引号括起来，并且中间用空格分隔。
trans_src	修改转换后的源对象。
src_addr2	字符串，输入转换后的源对象名称。 说明： （1）该参数值必须是已经定义的地址对象或属性名称。

	（2）只能输入一个对象。 （3）添加源地址转换策略时，该参数值必须设置。
trans_dst	修改转换后的目的对象。
dst_addr2	字符串，输入转换后的目的对象名称。 说明： （1）该参数值必须是已经定义的主机地址对象或均衡组对象名称。 （2）只能输入一个对象名。 （3）添加目的地址转换策略时，该参数值必须设置。
trans_service	修改转换后的服务资源。
ser_obj	数值类型，输入转换后的服务资源的名称。 说明： 该参数值必须是 define 模块已经定义的名称。
vsid	修改虚拟系统的 ID。
number2	数值类型，输入修改后的虚拟系统 ID。
pat	修改源端口转换开关。
yes|no	yes 表示对源端口进行端口转换；no 表示不对源端口进行端口转换。 说明： 默认值为“yes”。
enable	修改地址转换策略开关。
yes|no	yes 表示启用这条地址转换策略；no 表示禁用这条地址转换策略。 说明： 默认值为“yes”。
comment	可选项，添加必要的描述信息
string	字符串

实例：

** 修改虚系统 0 中 id 为 8144 的目的地址转换策略，将转换后地址修改为“10.10.10.22”（地址对象为“10.22”）。

policy modify id *8144* **vsid** *0* **trans_dst** *10.22*

policy delete id <*number1*> [**vsid** <*number2*>]

命令描述：

本命令用于删除一条地址转换策略。

参数说明：

delete	删除一条地址转换策略。
id	指定地址转换策略的 ID。
number1	数值类型，输入要删除的地址转换策略的 ID。
vsid	指定该策略所属的虚系统 ID。
number2	数值类型，输入要删除的地址转换策略所属的虚系统 ID。

实例：

** 删除虚系统 0 中 ID 为 8144 的地址转换策略。

policy delete id *8144* **vsid** *0*

policy show [**vsid** <*number*>] [**dstarea** <*string*>] [**orig_dst** <*string*>][**orig_src** <*string*>] [**srcarea** <*string*>][**orig_service** <*string*>] [**from** < *number*>] [**to** <*number*>]

命令描述：

本命令用于查看对象相关的地址转换策略。

参数说明：

show	查看地址转换策略。
vsid	可选项，指定要显示的地址转换策略所属的虚系统 ID。
number	数值类型，输入要显示的地址转换策略所属的虚系统 ID。 说明：如果不设定该参数值，将显示所有虚系统中的地址转换策略。
dstarea	可选项，设定查看哪个目标区域的 NAT 策略。
string	字符串，输入目的区域资源名称。 说明： 该参数值必须是已经定义的区域资源名称，可以输入一个或多个区域资源的名称，输入多个时用单引号括起来，并用空格隔开，如’area1 area2’。
orig_dst	可选项，设定根据原始报文的目的对象查看 NAT 规则。
string	字符串，输入修改后的原始报文的目的对象名称。 说明： （1）该参数值必须是已经定义的地址对象名称。 （2）可以同时输入多个地址对象，输入格式为’test1 test2’。地址对象用单引号括起来，并且中间用空格分隔。
orig_src	可选项，设定根据原始报文的源对象查看 NAT 规则。
string	字符串，输入修改后的原始报文的源对象名称。 说明： （1）该参数值必须是已经定义的地址对象名称。 （2）可以同时输入多个地址对象，输入格式为’test1 test2’。地址对象用单引号括起来，并且中间用空格分隔。
srcarea	设定源区域。
string	字符串，输入源区域资源名称。 说明： 该参数值必须是已经定义的区域资源名称，可以输入一个或多个区域资源的名称，输入多个时用单引号括起来，并用空格隔开，如’area1 area2’。
orig_service	可选项，根据原始报文使用的服务查看相关的 NAT 策略。
string	字符串，输入修改后的原始报文的服务资源名称。 说明： （1）该参数值必须是已经定义的服务资源名称。

	（2）可以同时输入多个服务资源，输入格式为’server1 server2’。服务资源用单引号括起来，并且中间用空格分隔。
from	指定开始显示的策略 ID
number	策略 ID
to	指定结束显示的策略 ID
number	策略 ID

实例：

** 显示虚系统 0 中的所有地址转换策略。

policy show vsid *0*

** 显示网关中所有的地址转换策略。

policy show<cr>

policy clean [**vsid** <*number*>]

命令描述：

本命令用于清除地址转换策略。

参数说明：

clean	清除地址转换策略。
vsid	指定要清除的地址转换策略所属的虚系统 ID。
number	数值类型，输入要清除的地址转换策略所属的虚系统 ID。 说明：如果不设定该参数值，将清除根虚系统（vsid0）中的地址转换策略。

实例：

** 清除虚系统 1 中的所有地址转换策略。

policy clean vsid *1*

** 清除网关中根系统 vsid0 的所有的地址转换策略。

policy clean<cr>

policy move <*number1*> [<**before** <*number2*>|**after** <*number3*>]

命令描述：

本命令用于移动地址转换策略的位置。地址转换策略遵循顺序匹配的原则，移动地址转换策略可以改变策略的匹配优先级。

参数说明：

move	移动地址转换策略的位置。
number1	数值类型，输入要移动的地址转换策略 ID。
before	设定地址转换策略移动到某个策略 ID 之前。
number2	数值类型，输入策略 ID。 说明： 参数“before”和参数“after”的值不能同时设置。
after	设定地址转换策略移动到某个策略 ID 之后。
number3	数值类型，输入策略 ID。 说明： 参数“before”和参数“after”的值不能同时设置。

使用说明：

参数“before”和参数“after”的值不能同时设置。

实例：

** 将 ID 为 8144 的策略移动到 ID 为 8146 的策略之前。

policy move *8144* **before** *8146*

** 将 ID 为 8144 的策略移动到 ID 为 8126 的策略之后。

policy move *8144* **after** *8126*

policy total [**vsid** <*number*>] [**dstarea** <*string*>] [**orig_dst** <*string*>][**orig_src** <*string*>] [**srcarea** <*string*>][**orig_service** <*string*>]

命令描述：

本命令用于统计对象相关的地址转换策略的总数。

参数说明：

total	统计地址转换策略的总数。
vsid	可选项，指定要统计哪个虚系统的地址转换策略。
number	数值类型，输入要显示的地址转换策略所属的虚系统 ID。
dstarea	可选项，设定统计哪个目标区域的 NAT 策略。
string	字符串，输入目的区域资源名称。 说明： 该参数值必须是已经定义的区域资源名称，可以输入一个或多个区域资源的名称，输入多个时用单引号括起来，并用空格隔开，如’area1 area2’。
orig_dst	可选项，设定根据原始报文的目的对象统计 NAT 规则。
string	字符串，输入修改后的原始报文的目的对象名称。 说明： （1）该参数值必须是已经定义的地址对象名称。

	（2）可以同时输入多个地址对象，输入格式为’test1 test2’。地址对象用单引号括起来，并且中间用空格分隔。
orig_src	可选项，设定根据原始报文的源对象统计 NAT 规则。
string	字符串，输入修改后的原始报文的源对象名称。 说明： （1）该参数值必须是已经定义的地址对象名称。 （2）可以同时输入多个地址对象，输入格式为’test1 test2’。地址对象用单引号括起来，并且中间用空格分隔。
srcarea	设定源区域进行统计。
string	字符串，输入源区域资源名称。 说明： 该参数值必须是已经定义的区域资源名称，可以输入一个或多个区域资源的名称，输入多个时用单引号括起来，并用空格隔开，如’area1 area2’。
orig_service	可选项，根据原始报文使用的服务统计相关的 NAT 策略。
string	字符串，输入修改后的原始报文的服务资源名称。 说明： （1）该参数值必须是已经定义的服务资源名称。 （2）可以同时输入多个服务资源，输入格式为’server1 server2’。服务资源用单引号括起来，并且中间用空格分隔。

使用说明：

如果不设定任何参数值，将统计所有虚系统中的地址转换策略的总数。

实例：

** 统计虚系统 0 中的所有地址转换策略。

policy total vsid *0*

NETWORK

本命令用来配置网络卫士安全网关的网络连接功能，如 ADSL 链路配置、ARP 功能配置、接口地址和属性配置、接口流量统计功能配置、MAC 地址表配置、路由表配置和管理、PPTP 和 L2TP 链路配置、动态路由功能配置等。

进入本命令模块操作如下：

#network<cr>

退出本命令模块操作如下：

#end<cr>

CLI 管理员登录安全网关进入本命令模块后，可以执行相应的组件管理命令。下

面将详细描述本命令模块下的所有组件管理命令。命令的实例输入格式将按已经进入本命令模块书写。

下一级命令列表

命令	功能
802.1X	802.1X 认证设置
adsl	ADSL 配置管理
anti-proxy	防代理上网配置
arp	ARP 配置管理
arpproxy	ARP 代理配置管理
attribute	接口属性配置
attribute_group	接口属性组配置
bgp	BGP 路由协议设置
bond	端口聚合功能设置
cdp_neighbors	CDP 邻居信息管理
dev	安全网关流量统计
dhcp	安全网关作为 DHCP 客户端、服务器和中继的相关配置。
dns	DNS 配置
hoststatistic	主机地址对象流量统计
interface	设备接口管理
igmp	IGMP 组管理协议设置
ip-probe	IP 探测管理
l2tp	L2TP 拨入配置
link-backup	链路备份
mac-address-table	Mac 地址表配置管理
mpls	设置是否开启 MPLS 透传功能
mroute	多播路由配置管理
ospf	OSPF 动态路由协议配置
port-mirror	端口镜像设置
port-statistics	设置端口流量统计功能
pptp	PPTP 拨入配置
rangstatistic	范围地址对象流量统计
reset	网络配置初始化
rip	RIP 动态路由协议配置
route	路由表配置管理
route-policy	安全网关策略路由配置管理
session	连接设置
spantree	生成树协议配置管理
statistic	流量统计相关设置
subnetstatistic	子网地址对象流量统计
suitstate	接口联动设置
traffic	查看接口的流量信息
tunnel	GRE 通道配置管理
virtual-line	虚拟线路配置管理
vlan	VLAN 配置管理

802.1X

设置 802.1X 认证相关参数

8021x set interface <*string*>

命令描述：

设置运行 802.1X 认证的接口。

参数说明：

set	设置运行 802.1X 认证的接口
interface	指定物理接口
string	字符串，指定物理接口名称，如 eth0

8021x start <cr>

命令描述：

启动 802.1X 认证。

8021x stop <cr>

命令描述：

停止 802.1X 认证。

8021x status <cr>

命令描述：

查看 802.1X 认证状态。

8021x show-interface <cr>

命令描述：

查看 802.1X 认证接口。

8021x save<cr>

命令描述：

保存 802.1X 认证设置。

adsl

网络卫士安全网关可以外接 ADSL Modem，通过拨号与外网（如 Internet）建立通信链路。ADSL 拨号成功后，自动将 ppp0 口绑定到与其连接的一个以太网口，自动分配 IP 地址，并使系统默认网关指向 ppp0。本命令进行 ADSL 账号的管理，包括 ADSL 链路属性的设置、开始/停止 ADSL 拨号、ADSL 链路属性查看。

adsl set dev <*string*>**username <***string***> passwd <***string***> attribute** <adsl|adsl1|adsl2|adsl3> [**demand** <yes|no>] [**idle** <*number*>] [**mtu** <*number*>] [**localip**<*ipaddress*>] [**metric** <*number*>] [**weight**<*number*>] [**bandwidth**<*string*>] [**description <***string***>**] [**debug** <yes|no>]

命令描述：

设置 ADSL 拨号链路的属性参数，包括必选参数：物理接口、用户帐号名/密码。可选参数：启动模式、最大空闲时间、最大传输单元、PPPoE 接口绑定的属性、PPPoE 接口静态 IP 地址、描述信息、是否调试。

参数说明：

set	设置 ADSL 拨号链路的属性
dev	指定与 ADSL modem 连接的相关物理接口
string1	字符串，指定物理接口名称，如 eth0
username	设定 ADSL 拨号连接的用户帐号名，由电话局提供
string2	字符串，指定用户帐号名
passwd	设定 ADSL 拨号连接的用户密码字符串，由电话局提供
string3	字符串，指定用户帐号对应的密码
attribute	选择拨号属性
adsl|adsl1|adsl2|adsl3	为内置属性 adsl、adsl1、adsl2 或 adsl3。
demand	参数为可选项，设定 ADSL 链路的启动模式： 是否自动按需拨号/手工启动。默认为手工启动模式。
yes	自动按需拨号： 当有数据报文通过安全网关上与 ADSL Modem 绑定的以太网接口转发时自动启动 ADSL 通信链路。此模式下，当网络链路空闲时间（由参数 **idle** 设置）内无任何流量的时候，安全网关将自动断开 ADSL 链路，待网络再有流量访问 Internet 时自动触发。
no	手工启动模式： 需要执行**#ADSL START** 命令启动 ADSL 通信链路。此模式下，当 ADSL 链路启动后异常掉线以后，安全网关也会无限次重复尝试连接，直到链路恢复正常。
idle	参数为可选项，仅当 **demand** 的参数为 yes 时该参数才有意义。当 **demand** 参数为 no 时该参数自动设定为默认值。 修改默认的允许 ADSL 链路空闲时间，若超过设定时间

	依然没有数据传输，则自动断开 ADSL 连接。默认为 300 秒
number1	数值，单位为（秒）。
mtu	参数为可选项，用于修改接口的最大传输单元，默认为 1492
number2	数值，单位为 byte，必须在 1000-1492 之间。
localip	参数为可选项，设定静态 PPPoe 接口的 IP 地址，当 ADSL 服务提供商要求使用静态 IP 地址时设定此项。
ipaddress	IP 地址字符串，如果 ADSL 服务提供商要求使用静态 IP 地址，则在本选项处需要输入此 IP 地址。否则为空即可。
metric	设置该链路拨号成功后添加的默认路由的 Metric 值。 说明： 1）Metric 值越小，静态路由的优先级越高。 2）如果静态路由表中存在多个“Metric”相同的下一跳，则根据权重值做权重负载均衡，选择下一跳；如果权重值也相等，则采取轮询方式选择下一跳，即依次通过各条路径发送，从而实现网络的负载分担。 3）如果管理员需要指定部分用户使用某条固定的链路连接外网，则需要设置 ADSL 静态路由。
number	默认为 1，取值范围为 1-65535。
weight	设置该链路拨号成功后添加的默认路由的权重值。 说明： 1）权重值越大，静态路由的优先级越高。 2）如果静态路由表中存在多个“Metric”相同的下一跳，则根据权重值做权重负载均衡，选择下一跳；如果权重值也相等，则采取轮询方式选择下一跳，即依次通过各条路径发送，从而实现网络的负载分担。 3）如果管理员需要指定部分用户使用某条固定的链路连接外网，则需要设置 ADSL 静态路由。
number	默认为 1，取值范围为 1-128。
bandwidth	设置分配给该条 ADSL 链路的保证带宽。
string	表示带宽，范围为 1-1024M，单位可以为 K 或 M，默认为 KBps。
description	设置描述信息
string	字符串
debug	参数为可选项，设置是否将调试信息输出至日志，默认为否。
yes	是
no	否

使用说明：

1) 在ADSL拨号环境下，需要在区域中绑定拨号物理接口和ADSL属性，绝对不可以用命令 **# network interface** *eth0* **attribute add** *adsl* 将物理接口和adsl属性对象绑定。

2) 如果要实现内网用户通过ADSL拨号上网，还需要在NAT转换策略中，添加将

内网用户的源地址转换为“ADSL属性”的源地址转换策略。

实例：

** 设定在安全网关的 eth1 口启动 ADSL 链路，帐号名/密码为 B22612345/82771234，采用自动按需拨号方式启动 ADSL 链路，链路空闲时间为 200 秒，最大传输单元为 1292 字节，ADSL 链路的 PPPoE 接口和内置属性 adsl 绑定。

adsl set dev *eth1* **username** *B22612345* **passwd** *82771234* **demand** yes **idle** *200* **mtu** *1292* **attribute** adsl <cr>

** 设定在安全网关的 eth1 口启动 ADSL 链路，帐号名/密码为 B22612345/82771234，采用手动启动 ADSL 链路方式，则链路空闲时间为默认值 300 秒，无须设置。最大传输单元为默认值 1492 字节，ADSL 链路的 PPPoE 接口和内置属性 adsl 绑定。

adsl set dev *eth1* **username** *B22612345* **passwd** *82771234* **demand** no **attribute** adsl <cr>

adsl clean attribute < adsl|adsl1|adsl2|adsl3>

命令描述：

清除 ADSL 链路属性设置。

adsl show<running | status>

命令描述：

查看 ADSL 链路的属性设置或状态信息。可以提供给用户 ADSL 连接的当前状态，包含以下信息：当前连接状态（UP or DOWN）,，本端 IP，对端 IP，发送和接收到的报文数目，连接维持的时间，配置信息。

参数说明：

show	查看 ADSL 属性设置
running	查看 ADSL 链路的属性设置和是否启动。
status	查看 ADSL 链路的运行状态

实例：

**查看 ADSL 链路的属性设置

adsl show running <cr>

**查看 ADSL 链路的状态信息

adsl show status <cr>

adsl start attribute <adsl|adsl1|adsl2|adsl3>

命令描述：

手工启动 ADSL 链路，开始向 ADSL Modem 拨号连接。

参数说明：

start	启动 ADSL 链路
attribute	指定具体链路
adsl|adsl1|adsl2|adsl3	选择属性

adsl stop attribute <adsl|adsl1|adsl2|adsl3>

命令描述：

停止 ADSL 拨号。

参数说明：

stop	停止 ADSL 拨号
attribute	指定具体链路
adsl|adsl1|adsl2|adsl3	选择属性

anti-proxy

设置防代理上网功能

anti-proxy alarm <on|off>

命令描述：

开启或者关闭防代理报警开关

参数说明：

alarm	开启或者关闭防代理报警开关
on|off	开启/关闭

anti-proxy blacklist-handle <on|off>

命令描述：

开启或者关闭防代理黑名单开关

参数说明：

blacklist-handle	开启或者关闭防代理黑名单开关
on|off	开启/关闭

anti-proxy blacklist-timeout <*string*>

命令描述：

设置黑名单被禁用时间

参数说明：

blacklist-timeout	设置黑名单被禁用时间
string	范围为 1-3600*24*365 秒，默认缺省值为 3600 秒

anti-proxy tolerate-time <*string*>

命令描述：

设置 IP-id 发生两次回环的时间间隔

参数说明：

tolerate -time	设置 IP-id 发生两次回环的时间间隔
string	范围为 1-60 秒，默认缺省值为 10 秒

anti-proxy reset<cr>

命令描述：

防代理上网参数恢复默认值

anti-proxy show<cr>

命令描述：

显示防代理上网的状态

arp

网络卫士安全网关内部维护了一张 ARP 表，维护了网络卫士安全网关所学习到的主机 IP 和 MAC 地址的对应关系条目。当网络卫士安全网关转发数据报文时，会首先查看 ARP 表，如目的 IP 已经在 ARP 表中，网络卫士安全网关则不必再发

送 ARP 广播就获取了目的设备的 MAC 地址。用户可以手工添加静态 ARP 条目、清空 ARP、从 ARP 表中添加同名主机地址对象。

arp add<*ipaddress*> <*macaddress*> <*string*>

命令描述：

添加一个静态 arp 表项。

参数说明：

add	添加一个静态 arp 表项
ipaddress	标准 IP 地址字符串，指定 IP 地址。
macaddress	标准 Mac 地址字符串，格式为 aa:bb:cc:dd:ee:ff。
string	指定物理接口或 VLAN 虚接口名，如 eth0。

使用说明：

在某个接口添加静态 ARP 表项时，要求该物理接口或 VLAN 虚接口的 IP 地址已经设定好。

无实例：

** 增加eth0 口的ARP表项，IP地址为 10.10.10.2 MAC地址为*00:50:43:c0:d3:13*

arp add *10.10.10.2 00:50:43:c0:d3:13 eth0* <cr>

arp clean<cr>

命令描述：

清空所有 ARP 表项。

arp delete <*ipaddress*>

命令描述：

删除指定 IP 在 ARP 缓存表中的相关记录。

参数说明：

delete	删除指定 IP 在 ARP 缓存表中的相关记录
ipaddress	为已有 ARP 表项的 IP 地址字符串，否则会显示错误信息。

使用说明：

无

实例：

** 删除 IP 地址为 10.10.10.2 的 ARP 表项

arp delete *10.10.10.2*

arp limit <*number* | off| show>

命令描述：

设定是否限制 ARP 请求个数，及个数的上限值。系统默认不限制 ARP 请求的个数。

参数说明：

limit	设定是否限制 ARP 请求个数及个数的上限值。
number	设定允许 ARP 请求的上限值，范围为 10-2000。
off	不对 ARP 表项的个数进行限制。
show	查看 ARP 限制属性。

实例：

** 关闭限制 ARP 请求，即不对静态 ARP 表项的个数进行限制。

arp linit off<cr>

**对 ARP 请求数目限制为 40，同时开启 ARP 请求。

arp limit *40* <cr>

**查看 ARP 限制属性

arp limit show <cr>

如果关闭 ARP 限制请求，则显示为 network arp limit off

arp reverse-path [on|off]

命令描述：

是否开启 ARP 反向路径查询

参数说明：

reverse-path	是否开启 ARP 反向路径查询
on|off	开启/关闭

arp show [static | dynamic | *ipaddress*]

命令描述：

查看 ARP 表项，可以查看所有的内容，也可以根据参数来查看静态、动态或某 IP 地址的 ARP 表项。

参数说明：

show	查看 arp 表项
static	查看静态 ARP 表项
dynamic	查看动态 ARP 表项
ipaddress	标准 IP 地址字符串，指定 IP 地址

使用说明：

指定参数时显示相应类型的 ARP 表项，不指定参数时显示所有 ARP 表项。

实例：

**查看所有 ARP 表项的内容。

arp show<cr>

**查看静态 ARP 表项的内容。

arp show ststic<cr>

arp show [**complete**]< cr>

命令描述：

查看完整的 arp 项。

arp show interface <string>

命令描述：

查看接口名称。

arp detect ip <*ipaddress*> **interface** <*string*> [**from** <*ipaddress1*>] [**to** <*ipaddress2*>]

命令描述：

根据设定的接口和地址范围进行 ARP 探测。

参数说明：

detect	探测 ARP 信息
ip	探测主机 IP 地址。
ipaddress	IP 地址，标准 IP 地址字符串
interface	设置通过哪个接口进行 ARP 探测
string	接口名称，如 eth0
from	设置探测范围的起始 IP 地址
ipaddress1	起始 IP 地址，标准 IP 地址字符串

to	设置探测范围的终止 IP 地址
ipaddress2	终止 IP 地址，标准 IP 地址字符串

使用说明：

指定 ARP 探测的接口时，可以指定设备的物理接口、Vlan 口、子接口或 bond 口。

实例：

**通过 eth0 口探测 192.168.83.22-192.168.83.89 之间的 ARP 信息。

arp detect interface eth0 **from** *192.168.83.22* **to** *192.168.83.39* <cr>

arpproxy

网络卫士安全网关提供 ARP 代理功能。也就是说，当一个 ARP 请求是发往一个不同子网的主机地址的时候，如果该目的主机位于被代理的区域，网络卫士安全网关作为中间设备，可以代为回答该 ARP 请求。这样 ARP 请求端会把网络卫士安全网关的物理接口的 MAC 地址当成目的主机的 MAC 地址，使它认为网络卫士安全网关就是目的主机，从而达到保护目的主机的作用。

arpproxy add <*ipaddress1*> <*ipaddress2*> [static | dynamic]

命令描述：

添加一条 ARP 代理，代理可以分为两种类型：静态 ARP 代理和动态 ARP 代理。如果选择代理类型为静态，则设置的 ARP 代理将被保存；如果设置为动态，设备重启后，需要重新配置 ARP 代理。

参数说明：

add	添加一条 ARP 代理
ipaddress1	标准 IP 地址字符串，指定 IP 地址范围下限。
ipaddress2	标准 IP 地址字符串，指定 IP 地址范围上限。要大于或等于下限 IP 地址。
static	添加静态 ARP 代理
dynamic	添加动态 ARP 代理

实例：

**为 IP 地址为 10.10.10.2 到 10.10.10.22 范围内的主机添加一个静态 ARP 代理。

arpproxy add *10.10.10.2 10.10.10.22* static

arpproxy delete <*ipaddress1*> <*ipaddress2*>

命令描述：

删除某个 IP 地址范围内的静态 ARP 代理

参数说明：

delete	删除一个静态 ARP 代理
ipaddress1	标准 IP 地址字符串，指定 IP 地址范围下限。
ipaddress2	标准 IP 地址字符串，指定 IP 地址范围上限。要大于或等于下限 IP 地址。

使用说明：

要删除某静态 ARP 代理，参数起始 IP 地址和终止 IP 地址必须完全匹配，否则无法删除。

实例：

**删除 IP 地址为 10.10.10.2 到 10.10.10.22 范围内 ARP 代理。正确输入方法为：

arpproxy delete *10.10.10.2 10.10.10.22*

若参数输入为# **arpproxy delete *10.10.10.2 10.10.10.11*则会提示error -12406 : can not find matched entry.

arpproxy show <cr>

命令描述：

查看所有 ARP 代理信息。

arpproxy clean <cr>

命令描述：

清空静态 ARP 代理选项。

attribute

属性对象是为了映射逻辑概念（如区域）和物理概念（如接口、链路等）而设计

的一个对象，通过区域 ——属性（属性组）——接口（或链路）的映射，用户可以更加灵活地划分安全区域，同时解决 L2TP、ADSL 等动态链路的访问控制问题。

属性分为三类：

（1）内置属性对象。为方便用户配置，设备出厂时内置在安全网关中，无法修改和删除，包括属性 eth0、eth1、eth2、adsl、ipsec、wan、lan、ssn、ppp、l2tp、pptp。其中属性 eth0、eth1、eth2 已自动和物理接口 eth0、eth1、eth2 绑定，无须用户设置；部分属性可以动态的根据链路状态进行绑定，同样无须用户设置，如 L2TP、PPTP 等；其他属性以及用户自定义的属性，需要用户手工绑定到物理接口，如 adsl、ssn、lan 等。

用于描述功能属性，加入到区域中，最终应用于访问控制规则。

属性来源 ：

(1) 物理属性 "eth0","eth1",...等。 自动绑定到物理接口 eth0, eth1。

(2) 动态属性 "l2tp", "ppp", "ipsec"。

(3) 用户定义的属性 "网通" ,"电信", "测试", "研发"等。

可在 adsl 配置，隧道配置，l2tp 配置等之中使用。将接口和属性绑定。从已定义的属性对象中选择属于该接口的属性，一个接口可以同时具有多个属性，系统自动为接口“eth0”, “eth1”…等绑定属性“eth0”, “eth1”。

attribute add name <*string*>

命令描述：

添加一个属性对象。

参数说明：

add	添加一个属性对象。
name	指定属性名
string	字符串，注意不能为与内置的属性对象相同的字符串。

使用说明：

新添加属性不能与已有的属性对象重名，否则不能添加。

实例：

**添加属性 intranet：

attribute add name *intranet*

attribute delete name <*string*>

命令描述：

删除某个自定义的属性

参数说明：

delete	删除某个自定义的属性
name	指定属性名
string	字符串注意不能为与内置的属性对象相同的字符串。

使用说明：

安全网关内置的属性对象不能删除。

实例：

**删除属性 intranet：

attribute delete name *intranet*

若参数输入为# **attribute delete *eth0*则会提示error -12158 : can not delete native interface attribute。

attribute show <cr>

命令描述：

查看所有属性信息。

attribute clean<cr>

命令描述：

清空所有自定义属性对象。

attribute -group

把几个属性对象组合在一个属性组中。

attribute -group add name <*string1*> **attribute** <*string2*>

命令描述：

添加一个属性组对象。

参数说明：

add	添加一个属性组对象。
name	为属性组命名
string1	字符串，注意不能为与内置的属性组对象相同的字符串。
attribute	指定属性组中所包含的属性对象，可以指定一个或多个，应当使用单引号，并且多个属性对象之间用空格隔开。如’eth0 eth1’。
string2	字符串，必须为在network-attribute中定义的属性对象名。

使用说明：

新添加属性组不能与已有的属性组对象重名，否则不能添加。

实例：

**添加属性组对象 g0，包含属性对象 eth0 和 eth1。

attribute -group add name *g0* **attribute** ‘*eth0 eth1’*

attribute -group modify name <*string1*> **attribute** <*string2*>

命令描述：

修改一个属性组对象的属性。

参数说明：

modify	修改一个属性组对象的属性。
name	指定属性组名
string1	字符串，应当为已有的属性组对象名。
attribute	指定属性组中所包含的属性对象，可以指定一个或多个，应当使用单引号，并且多个属性对象之间用空格隔开。如’eth0 eth1’。
string2	字符串，必须为在network-attribute中定义的属性对象名。

实例：

**修改属性组对象 g0 的属性，其包含属性对象 eth0、eth1 和 l2tp。

attribute -group modify name *g0* **attribute** *‘eth0 eth1 l2tp’*

attribute -group delete name <*string1*>

命令描述：

删除一个属性组对象。

参数说明：

delete	删除一个属性组对象。
name	指定属性组名
string1	字符串，应当为已有的属性组对象名。

实例：

**删除属性组对象 g0。

attribute -group delete name *g0*

attribute -group clean <cr>

命令描述：

清除所有属性组对象。

attribute -group show <cr>

命令描述：

查看所有属性组对象的属性。

bgp

网络卫士安全网关提供对 BGP 的支持。BGP 的主要功能是与其它自治域的 BGP 交换网络可达信息。各个自治域可以运行不同的内部网关协议。BGP 更新信息包括网络号 / 自治域路径的成对信息。自治域路径包括到达某个特定网络须经过的自治域串，这些更新信息通过 TCP 传送出去，以保证传输的可靠性。本模块设置 BGP 动态路由协议的相关参数。

bgp aggregate-address <*string*> **as-set** <yes|no> **summary-only** <yes|no>

命令描述：

设置进行地址聚合的网段地址及其子网掩码。“地址聚合”用于配置 BGP 的路由聚合功能，就是把各段路由综合到一个或多个聚合或 CIDR 中，以便把路由表中的路由数目减到最小。

参数说明：

aggregate-address	设置进行地址聚合的网段地址及其子网掩码。

string	字符串，格式为 a.b.c.d/x。
as-set	设置是否为带有自治区号的路由进行聚合。
yes|no	是/否，默认为“是”。
summary-only	设置是否只发送聚合路由而略去原路由。
yes|no	设置为“yes”时将只发送聚合路由略去原路由；设置为“no”时将聚合路由和原详细路由都通告给对等体。

bgp neighbor <*ipaddress*> **remote-as** <*number*>

命令描述：

用于设置邻居信的 IP 地址和 AS 号。

参数说明：

neighbor	设置邻居 IP 地址。
string	IP 地址格式字符串。
remote-as	设置是否为带有自治区号的路由进行聚合。
number	是/否，默认为“是”。

bgp neighbor <*ipaddress*> **password** <*string*>

命令描述：

设置邻居之间在建立 TCP 连接时进行 MD5 认证的密码。如果认证失败，则不能建立 TCP 连接。

参数说明：

neighbor	设置邻居 IP 地址。
string	IP 地址格式字符串。
password	设置认证密码。
string	字符串。

bgp neighbor <*string*> **default-originate**<cr>

命令描述：

设置缺省路由宣告属性，设置同伴组是否引入默认路由，缺省不引入。

参数说明：

neighbor	设置邻居 IP 地址。
string	IP 地址格式字符串。
default-originate	设置引入默认路由。

bgp neighbor <*string*> **next-hop-self**<cr>

命令描述：

用于设置配置在发布路由时是否将自身地址作为下一跳。BGP 路由器向对等体组发布路由时，可使用自身地址作为下一跳。缺省情况下，本地路由器向对等体组发布路由时不把自身地址作为下一跳。

参数说明：

neighbor	设置邻居 IP 地址。
string	IP 地址格式字符串。
next-hop-self	设置使用自身地址作为下一跳。

bgp route-id <*string*>

命令描述：

设置 BGP 协议要通告的网络路由号，用于标识本地路由器将与之建成立的对等路由器。

参数说明：

route-id	BGP 协议要通告的网络路由号
string	IP 地址格式字符串。

bgp network <*string*>

命令描述：

设置 BGP 要通告哪个网段的网络路由。

参数说明：

network	BGP 协议要通告的网络路由号
string	IP 地址及其掩码格式字符串，格式为 a.b.c.d/x。

实例：

**设置要通告网段 10.10.10.0/24 的路由。

bgp network *10.10.10.0/24*

bgp show <running|summary|neighbor>

命令描述：

查看 BGP 相关设置信息。

参数说明：

show	查看 BGP 相关设置信息
running|summary|neighbor	运行信息/统计信息/邻居信息。

bgp show network <string>

命令描述：

查看 BGP 相关路由设置信息。

bgp start as <*number*>

命令描述：

启动 BGP 进程。

参数说明：

start	启动 BGP 进程。
as	设置 BGP 协议的本地自治系统号。
number	数值，范围为 0 到 65535。

bgp stop <cr>

命令描述：

停止 BGP 进程。

bgp redistribute[static|connected|rip|ospf] [**metric** <*number*>]

命令描述：

设置是否引入静态、直连、RIP 或者 OSPF 的路由信息到 RIP 路由协议中，并设置路由引入后的 metric 值。

参数说明：

redistribute	设置路由重发布信息。
static|connected|rip|ospf	选择引入的路由类型，分别对应静态路由、直连路由、RIP 协议路由和 OSPF 协议路由。
metric	设置路由引入后的 metric 值。
number	数值，范围为 0-16777214。

bond

网络卫士安全网关支持端口聚合功能，将多个物理接口聚合成一个逻辑端口，聚合后的端口称为一条聚合链路，其性能接近各个网口的速率总和，可大大提高端口间的通信速度。网络卫士安全网关的端口聚合功能采用 802.3ad 的工作模式，

聚合链路可以通过预先设置的负载均衡算法将流量分配给聚合链路内不同的物理接口，实现链路级的负载均衡功能，也可防止单条链路转发速率过低而出现丢包的现象。

bond add id <*number*> **load-balance** < per-packet|src-mac|dst-mac|src-dst-mac|src-ip|dst-ip|src-dst-ip|src-port|dst-port|src-dst-port|quinary >

命令描述：

增加一个 bond 接口，同时指定发送算法。

参数说明：

add	增加一个 bond 接口
id	指定接口 ID 号
number	数值，范围为 0－3。
load-balance	指定负载均衡算法，将流量分配给聚合链路内不同的物理接口。
per-packet|src-mac|dst-mac|src-dst-mac|src-ip|dst-ip|src-dst-ip|src-port|dst-port|src-dst-port|quinary	可选项为： 1）Src-mac：表示对发送的报文的源 MAC 地址进行哈希计算，决定将数据分配给聚合端口内哪个 slave 接口。 2）dst-mac：表示对发送的报文的目的 MAC 地址进行哈希计算，决定将数据分配给聚合端口内哪个 slave 接口。 3）src-dst-mac：表示对发送的报文的源和目的 MAC 地址进行哈希计算，决定将数据分配给聚合端口内哪个 slave 接口。 4）Src-ip：表示对发送的报文的源 IP 地址进行哈希计算决定将数据分配给聚合端口内哪个 slave 接口。 5）dst-ip：表示对发送的报文的目的 IP 地址进行哈希计算决定将数据分配给聚合端口内哪个 slave 接口。 6）src-dst-ip：表示对发送的报文的源和目的 IP 地址进行哈希计算决定将数据分配给聚合端口内哪个 slave 接口。 7）Src-port：表示对发送的报文的源端口进行哈希计算决定分配给聚合端口内哪个 slave 接口。 8）dst-port：表示对发送的报文的目的端口进行哈希计算决定分配给聚合端口内哪个 slave 接口。 9）src-dst-port：表示对发送的报文的源和目的端口进行哈希计算决定分配给聚合端口内哪个 slave 接口。 10）Quinary：表示根据源地址、目的地址、源端口、目的端口和 IP 协议类型进行哈希计算决定将数据分配给聚合端口内哪个 slave 接口。 11）Per-packet：表示发送数据时进行轮询，依次使用从第一个到最后一个可用的 slave 接口。

使用说明：

1）一个物理接口只能属于一个 bond 接口。

2）支持在 bond 接口上做 GRE（但是反过来不行，GRE 是虚接口，不可以把 GRE 接口加入端口聚合）。

3）当物理接口加入 bond 成为 slave 接口后，不能对它再进行 IP 层以上的配置，即禁止设置 slave 设备的 ip 地址、MAC 地址、MTU 值、mss-adjust 值、子接口，禁止设置 slave 设备为交换口。只能启用/禁用接口，配置接口 speed、配置 MTU 值。

实例：

**添加 ID 号为 1 的聚合端口，采用轮询算法进行负载均衡。

bond add id *1* **load_blance** per-packet

bond delete id <*number*>

命令描述：

删除一个 bond 接口。

参数说明：

delete	删除一个 bond 接口
id	指定接口 ID 号
number	数值，范围为 0－3。

实例：

**删除 ID 号为 1 的聚合端口。

bond delete id *1*

bond join id <*number*> **dev** <*string*>

命令描述：

把物理接口加入到 bond 接口。

参数说明：

join	把物理接口加入到 bond 接口
id	指定接口 ID 号
number	数值，范围为 0－3。

dev	指定物理接口
string	字符串，指定接口名。

使用说明：

加入到 bond 接口的物理接口必须满足如下条件：

1）不是交换模式

2）还没有加入其他 bond

3）没有子接口

4）在静态 arp 表里没有对应项

实例：

**将接口 eth0 加入到 ID 号为 1 的聚合端口。

bond join id *1* **dev** *eth0*

bond leave id <*number*> **dev** <*string*>

命令描述：

把物理接口从 bond 接口删除。

参数说明：

leave	把物理接口从 bond 接口删除
id	指定接口 ID 号
number	数值，范围为 0－3。
dev	指定物理接口
string	字符串，指定接口名。

实例：

**将接口 eth0 从 ID 号为 1 的聚合端口删除。

bond leave id *1* **dev** *eth0*

bond modify id <*number*> **load-balance** < per-packet|src-mac|dst-mac|src-dst-mac|src-ip|dst-ip|src-dst-ip|src-port|dst-port|src-dst-port|quinary >

命令描述：

修改一个 bond 接口的属性。

参数说明：

modify	修改一个 bond 接口的属性
id	指定接口 ID 号
number	数值，范围为 0－3。
load-balance	指定负载均衡算法，将流量分配给聚合链路内不同的物理接口。
per-packet|src-mac|dst-mac|src-dst-mac|src-ip|dst-ip|src-dst-ip|src-port|dst-port|src-dst-port|quinary	可选项为： 1）Src-mac：表示对发送的报文的源 MAC 地址进行哈希计算，决定将数据分配给聚合端口内哪个 slave 接口。 2）dst-mac：表示对发送的报文的目的 MAC 地址进行哈希计算，决定将数据分配给聚合端口内哪个 slave 接口。 3）src-dst-mac：表示对发送的报文的源和目的 MAC 地址进行哈希计算，决定将数据分配给聚合端口内哪个 slave 接口。 4）Src-ip：表示对发送的报文的源 IP 地址进行哈希计算决定将数据分配给聚合端口内哪个 slave 接口。 5）dst-ip：表示对发送的报文的目的 IP 地址进行哈希计算决定将数据分配给聚合端口内哪个 slave 接口。 6）src-dst-ip：表示对发送的报文的源和目的 IP 地址进行哈希计算决定将数据分配给聚合端口内哪个 slave 接口。 7）Src-port：表示对发送的报文的源端口进行哈希计算决定分配给聚合端口内哪个 slave 接口。 8）dst-port：表示对发送的报文的目的端口进行哈希计算决定分配给聚合端口内哪个 slave 接口。 9）src-dst-port：表示对发送的报文的源和目的端口进行哈希计算决定分配给聚合端口内哪个 slave 接口。 10）Quinary：表示根据源地址、目的地址、源端口、目的端口和 IP 协议类型进行哈希计算决定将数据分配给聚合端口内哪个 slave 接口。 11）Per-packet：表示发送数据时进行轮询，依次使用从第一个到最后一个可用的 slave 接口。

实例：

**修改 ID 号为 1 的聚合端口的负载均衡算法为 dst-ip，对发送的报文的目的 IP 地址进行哈希计算决定将数据分配给聚合端口内哪个 slave 接口。

bond modify id *1* **load_blance** dst-ip

bond show <cr>

命令描述：

显示 bond 接口配置。

bond clean <cr>

命令描述：

清空所有 bond 接口

cdp_neighbors

网络卫士安全网关可以接受 CDP（Cisco Discovery Protocol）消息，并可自动发现并识别出相邻的思科设备。此功能需要对端也同时开启该协议。

cdp_neighbors set cdp_thru <on | off>

命令描述：

设置是否允许 CDP 数据报文通过。

参数说明：

Set cdp_thru	设置是否允许 CDP 数据报文通过
on | off	是/否

使用说明：

无。

实例：

cdp_neighbors setcdp_thru on

cdp_neighbors show [detail]

命令描述：

查看相邻的思科设备信息。

参数说明：

show	查看相邻的 CDP 设备信息。
detail	为可选项，选择该参数时查看详细信息，不选择该参数时显示简单信息。

使用说明：

不指定任何参数时查看相邻的思科设备的简单信息，指定参数 detail 时查看详细

信息。

dev

设置安全网关物理接口的流量统计功能

dev statistic <cr>

命令描述：

查看通过安全网关设备的各个协议(包括 TCP 协议、UDP 协议和 ICMP 协议)的流量统计数据。

dhcp

网络卫士安全网关全面支持 DHCP 功能。网络卫士安全网关既可以作为 DHCP 客户端，从 DHCP 服务器动态的获得 IP 地址，也可以作为 DHCP 服务器分配 IP 地址，或者作为 DHCP 中继协助 DHCP 服务器提供动态地址租借服务。为第二级组件级命令。

进入本命令模块操作如下：

TopsecOS.network# **dhcp**<cr>

命令执行结果为：

TopsecOS.network.dhcp#

退出本命令模块至根目录下操作如下：

TopsecOS.network.dhcp# **end**<cr>

命令执行结果为：

TopsecOS#

返回上一级目录操作如下：

TopsecOS.network.dhcp# **exit**<cr>

命令执行结果为：

TopsecOS..network #

CLI 管理员登录安全网关进入本命令模块后，可以执行相应的组件管理命令。下面将详细描述本命令模块下的所有组件管理命令。命令的实例输入格式将按已经进入本命令模块书写。

client

网络卫士安全网关可以作为 DHCP 客户端，接口可以自动获取某个 IP 地址。在这种情况下，网络卫士安全网关的某些接口或全部接口将由 DHCP 服务器动态分配 IP 地址。

client start on <*string*>

命令描述：

在安全网关接口启动 DHCP 客户端。

参数说明：

start	启动 DHCP 客户端
on	指定接口名
string	字符串，指定客户端所在接口，可以是物理接口或 VLAN 虚接口名。如 eth0、vlan.0001，多个接口间需要使用逗号“,”进行分隔。

使用说明：

1）如果安全网关的接口为交换模式，必须在相应虚接口启动 DHCP 客户服务，否则会提示错误。

2）安全网关可以在多个接口同时启用 DHCP CLIENT 的服务。

3）另外还需要对 DHCP 服务器开放相关接口的 DHCP 服务。

实例：

**接口 eth0 作为 DHCP 客户端。

client start on *eth0*<cr>

**同时在接口 eth0 和 VLAN 虚接口 vlan.0001 启动 DHCP 客户服务。

client start on *eth0,vlan.0001*<cr>

client stop<cr>

命令描述：

停止 DHCP 客户端。

使用说明：

将所有接口的 DHCP 客户端停止，不能停止某个接口的 DHCP 客户端。

relay

当 DHCP 服务器和 DHCP 客户机不在同一子网内（一个广播域）时，网络卫士安全网关可以作为 DHCP 中继代理使用，从客户端接收 DHCP 请求报文，并将该报文转发给指定 DHCP 服务器，当收到 DHCP 服务的回应，安全网关将该回应再转发给发起请求的客户端主机。

relay start on <*string*> **dhcp_server** <*ipaddress*>

命令描述：

在安全网关接口启动 DHCP 中继。

参数说明：

start	启动 DHCP 中继
on	指定接口名
string	字符串，指定客户端所在接口，还有接受 server 回应的接口。可以是物理接口或 VLAN 虚接口名。如 eth0、vlan.0001，多个接口间需要使用逗号“,”进行分隔。
dhcp_server	指定网络上的 DHCP 服务器地址
ipaddress	指定服务器的 IP 地址值

使用说明：

1）如果安全网关的接口为交换模式，必须在相应虚接口启动 DHCP 中继服务，否则会提示错误。

2）中继服务需要同时开放服务器和客户机所属区域的 DHCP 服务。

3）中继服务需要同时选中与服务器和客户机物理连接的接口（或虚接口）。

4）如果 DHCP 服务器的默认网关不是安全网关的接口（虚接口）地址，必须在该服务器上添加一条静态路由（目的地址为 DHCP 作用域的网段、网关为安全网关与服务器端连接的接口），否则客户机无法正确获取 IP。

实例：

**接口 eth0 和 eth1 口启动 DHCP 中继服务，并设定 DHCP 服务器的 IP 地址为 192.168.83.234。

relay start on *eth0,eth1* **dhcp_server** *192.168.83.234*

relay stop<cr>

命令描述：

停止 DHCP 中继服务。

server

网络卫士安全网关可以作为 DHCP 服务器给指定防火区的主机分配 IP 地址，同时也给内部主机提供 DNS、默认网关等地址，如需使用此功能，需要利用 pf 模块对相应地址对象开放 DHCP 服务。

server add_host name <*string*> **macaddr** <*macaddress*>**ipaddr** <*ipaddress*>

命令描述：

DHCP 服务器给指定 MAC 分配绑定的 IP 地址。

参数说明：

Add_host	DHCP 服务器给指定 MAC 分配绑定的 IP 地址
name	设定地址绑定规则名称
string	字符串，范围是 1~31 个字节。
macaddr	指定 MAC 地址
macaddress	MAC 地址，格式为 XX:XX:XX:XX:XX:XX
ipaddr	指定要绑定的 IP 地址
ipaddress	IP 地址字符串

使用说明：

如果管理员把某 MAC 地址的主机与 IP 地址绑定，则 DHCP 服务器将分配给此主机固定 IP。另外还必须添加地址池，否则无法启动安全网关上的 DHCP 服务器进程。

实例：

**给 MAC 地址为 00:50:04:c3:b0:31　的主机分配 IP 地址 10.10.10.25

#server add_host　name *绑定 10.10.10.25* **macaddr** *00:50:04:c3:b0:31* **ipaddr** *10.10.10.25*

server add_subnet subnet <*ipaddress1*> **submask** < *ipaddress2*> **sub_start** < *ipaddress* > **sub_end** < *ipaddress*> [**gateway** <*ipaddress5*>] [**pri_dns** < *ipaddress*>] [**sec_dns** < *ipaddress*>] [**domain**　<*string*>] [**def-lease-day** <*number1*>] [**def-lease-hour** <*number2*>] [**def-lease-min** <*number3*>] [**max-lease-day** <*number4*>] [**max-lease-hour** <*number5*>] [**max-lease-min** <*number6*>] [**vci** <*string*>] [**vendor-specific** < *string*>]

命令描述：

添加一个 DHCP 服务器地址池，即可用来分配动态 IP 的地址范围。

参数说明：

Add_subnet	添加一个 DHCP 服务器地址池
subnet	必选项，设置为哪个子网创建 DHCP 作用域。
ipaddress1	IP 地址字符串
submask	必选项，设置子网掩码。
ipaddress2	子网掩码字符串。
sub_start	必选项，设置地址池起始地址。
ipaddress3	IP地址字符串，应小于*ipaddress4*设定的地址。
sub_end	必选项，设置地址池结束地址。
ipaddress4	IP地址字符串，应大于*ipaddress3*设定的地址。
gateway	可选项，设置网关地址，如果 DHCP 服务器设定了网关地址，则客户端主机在获取 IP 地址的同时按照该设置设定其网关地址。默认为空。
ipaddress5	IP 地址字符串
pri_dns	可选项，如果 DHCP 服务器设定了网关地址，则客户端主机在获取 IP 地址的同时按照该设置设定主/次 DNS 服务器地址。默认为空。
ipaddress6	IP 地址字符串
sec_dns	可选项，如果 DHCP 服务器设定了网关地址，则客户端主机在获取 IP 地址的同时按照该设置设定主/次 DNS 服务器地址。默认为空。
ipaddress7	IP 地址字符串
def-lease-day	可选项，设置缺省租用期的天数。默认为 1 天。
number1	数值，单位为天，范围为 0-3650。
def-lease-hour	可选项，设置缺省租用期的小时数。默认为 0 小时。
number2	数值，单位为小时，范围为 0-23。
def-lease-min	可选项，设置缺省租用期的分钟数。默认为 0 分钟。
number3	数值，单位为分钟，范围为 0-59。
max-lease-day	可选项，设置最大租用期的天数。默认为 7 天。
number4	数值，单位为天，范围为 0-3650。
max-lease-hour	可选项，设置最大租用期的小时数。默认为 0 小时。
number5	数值，单位为小时，范围为 0-23。

max-lease-min	可选项，设置最大租用期的分钟数。默认为 0 分钟。
number6	数值，单位为分钟，范围为 0-59。
vci	指定客户端类型
string	字符串
vendor-specific	指定供应商详情
string	字符串

使用说明：

1）配置安全网关作为 DHCP 服务器，需要首先配置地址池，才能在相应接口运行 DHCP 服务器。

2）缺省租用期表示 DHCP 服务器向 DHCP 客户端租借地址的期限。到期后如果客户端要继续使用该地址则必须续订。默认为 1 天。

最大租用期表示租约到期后在服务器端为客户保留地址的最长期限。这个宽限期在出现以下情况时保护客户端租约：客户端和服务器处于不同的时区、个别计算机的时钟没有同步、在租约过期时客户端从网络上断开。默认为 7 天。

实例：

*为子网 10.1.1.0/24 设置 DHCP 地址池，范围为 10.1.1.22-10.1.1.45。

#server add_subnet subnet *10.1.1.0* **submask** *255.255.255.0* **sub_start** *10.1.1.22* **sub_end** *10.1.1.45*

server del_host name <*string*>

命令描述：

删除地址绑定对象。

参数说明：

del_host	删除地址绑定对象
name	地址绑定对象名称
string	字符串，为已经设定的地址绑定对象名。

使用说明：

无。

实例：

**删除地址绑定对象*绑定 10.10.10.25*。

#server del_host name *绑定 10.10.10.25*

server del_subnet subnet<*ipaddress*>

命令描述：

删除地址池。

参数说明：

del_subnet	删除地址池
subnet	地址池所在子网
ipaddress	IP 地址，为已经设定的地址池所在子网 IP。

使用说明：

无。

实例：

**删除子网 10.1.1.0 的地址池。

#server del_subnet subnet *10.1.1.0.*

server start on <*string*>

命令描述：

在安全网关某接口启动 DHCP 服务器。

参数说明：

start on	在安全网关某接口启动 DHCP 服务器
string	字符串，可以是物理接口、虚接口或子接口名。

使用说明：

配置安全网关作为 DHCP 服务器，需要首先配置地址池，才能在相应接口运行 DHCP 服务器。

实例：

**在安全网关 eth0 口启动 DHCP 服务器。

#server start on *eth0*

server stop <cr>

命令描述：

在安全网关上停止 DHCP 服务器。

使用说明：

无。

实例：

**在安全网关 eth0 口停止 DHCP 服务器。

#server stop <cr>

show

查看所有 DHCP 功能相关配置。

show <status | config| binded>

命令描述：

查看 DHCP 功能相关配置、运行状态、运行结果。

参数说明：

show	查看 DHCP 功能相关配置、运行状态、运行结果
status| config	binded	查看正在运行配置/查看所有 DHCP 配置规则/显示已分配 IP 地址情况

使用说明：

选择一个参数查看相关配置信息。。

实例：

**查看所有 DHCP 配置规则，包括安全网关作为 DHCP 客户端、服务器和中继的配置规则。

dhcp show config <cr>

**显示正在运行配置

dhcp show status<cr>

**查看安全网关作为 DHCP 服务器已分配的 IP 情况

dhcp show binded<cr>

dns

网络卫士安全网关提供了 DNS 服务器的设定功能，实现域名地址与 IP 地址的映射，并保证主机域名地址在因特网中唯一。

dns relay <on|off>

命令描述：

设置 DNS 中继服务。

dns set dns1 <*ipaddress1*> [**dns2** <*ipaddress2*>] [**dns3** <*ipaddress3*>]

命令描述：

设置域名服务器的地址，最多可设三个 DNS 服务器。

参数说明：

set	设置域名服务器的地址
dns1	设置主域名服务器的地址
ipaddress1	IP 地址字符串
dns2	可选项，设置第二域名服务器的地址
ipaddress2	IP 地址字符串
dns3	可选项，设置第三域名服务器的地址
ipaddress3	IP 地址字符串

使用说明：

DNS 服务器设置多个时，当主 DNS 服务器失效时，采用第二域名服务器，当前两个域名服务器均失效时采用第三域名服务器。

dns clean < cr>

命令描述：

清除域名服务器的设置。

dns show < cr>

命令描述：

查看域名服务器的设置。

hoststatistic

配置主机流量统计功能。

hoststatistic set name< *string* >

命令描述：

添加主机地址对象到流量统计地址对象列表中，设置对地址对象的流量统计功能。

参数说明：

set	添加统计对象
name	设置统计对象名称
string	字符串，应当是已经添加的主机地址对象的名称。

使用说明：

1) 如果设置的地址对象不是已经定义的主机地址对象，则命令执行会提示错误信息。

2）查看已经定义的主机地址对象信息在 define 组件下的 host 命令下查看。

hoststatistic clean [**name**< *string* >]

命令描述：

从统计列表中删除某主地址对象，从而停止对该主机地址对象的流量统计功能。

参数说明：

clean	从统计列表中删除主机地址对象
name	可选项，指定统计对象名称，不指定时从统计列表中删除所有统计对象。
string	字符串，应当是从统计列表中已经添加的主机对象的名称。

使用说明：

1) 如果设置的地址对象不是已经定义的主机地址对象，则命令执行会提示错误信息。

2）不指定任何参数时将已添加的所有主机地址对象从统计列表中删除。

hoststatistic show< cr >

命令描述：

查看对主机地址对象的流量统计结果。

使用说明：

如果没有设置对地址对象的流量统计功能，则显示结果没有任何信息。

interface

设置安全网关指定物理接口或 VLAN 虚接口的属性对，包括安全网关接口的激活和停用、接口速率、接口的 IP 地址、接口作为交换接口或路由接口的具体属性设置。为第二级组件命令。

进入物理接口本命令模块操作如下：

TopsecOS.network# **interface** *eth0*<cr>

则系统提示符变为：

TopsecOS.network.interface eth0#

TopsecOS.network# **interface** *vlan.0007*<cr>

则系统提示符变为：

TopsecOS.network.interface vlan.0007#

退出本命令模块至根目录下操作如下：

TopsecOS.network. interface vlan.0007# **end**<cr>

命令执行结果为：

TopsecOS#

返回上一级目录操作如下：

TopsecOS.network. interface vlan.0007# **exit**<cr>

命令执行结果为：

TopsecOS..network #

CLI 管理员登录安全网关进入本命令模块后，可以执行相应的组件管理命令。下面将详细描述本命令模块下的所有组件管理命令。命令的实例输入格式将按已经进入本命令模块书写。

attribute

将接口和属性绑定。从已定义的属性对象中选择属于该接口的属性，一个接口可以同时具有多个属性，系统自动为接口“eth0”,“eth1”…等绑定属性“eth0”,“eth1”。

attribute default <cr>

命令描述：

清空接口的其余属性，只留默认属性，即接口 eth0、eth1、eth2 分别只和内置属性 eth0、eth1、eth2 绑定。

attribute add <*string*>

命令描述：

将该接口和非默认属性绑定。

参数说明：

add	将该接口和非默认属性绑定。
string	字符串，必须为在network-attribute中查看到的属性对象名。

bandwidth

接口带宽限制

bandwidth <*string*>

命令描述：

设置接口带宽限制。

参数说明：

bandwidth	设置接口带宽限制
string	“数值+单位”格式字符串，例如 100K。

description

为该接口添加必要的描述信息。

description <*string*>

命令描述：

为该接口添加必要的描述信息。

参数说明：

description	为该接口添加必要的描述信息
string	字符串。若属性描述中有空格需要用单引号‘’括起来。

实例：

**为该接口添加必要的描述信息。

description ‘*this is a switvhport interface’*<cr>

dot1q-vid

只有在设置子接口时才需要设置该参数，表示该子接口所属的 VLAN ID 号，当子接口接收的报文带有 802.1q 封装时，解析报文的 802.1q 封装信息，如果封装标签与子接口的 dot1q-vid 值一致，去掉报文的 802.1q 封装头继续转发，否则丢弃报文。

当子接口发送报文时，如果子接口的 dot1q-vid 配置不为 0，先对报文做 802.1q 封装，然后再发送出去。dot1q-vid 配置为 0 时表示不对报文进行 802.1q 封装。

只有当安全网关的物理接口需要与交换机的 Trunk 口连接时需要设置该项，此时每个子接口必须设置不同的 VLAN ID 号。

dot1q-vid <*number*>

命令描述：

设置子接口所属的 VLAN ID 号。

参数说明：

dot1q-vid	设置子接口所属的 VLAN ID 号
number	数字，范围为 0-4094，为 0 时表示不对报文进行 802.1q 封装。

duplex

设定接口的工作模式：半双工/全双工/自动协商

duplex <half|full|auto>

命令描述：

设定接口的工作模式。

参数说明：

duplex	设定接口的工作模式
half|full|auto	半双工/全双工/自动协商。

实例：

**设置接口的工作模式。

duplex half<cr>

ha-metric

设置接口的 HA 度量值

ha-metric <*number*>

命令描述：

设置接口的 HA 度量值。

参数说明：

ha-metric	设置接口的 HA 度量值
number	数字，范围为 0-100。

gratuitous-arp-interval

设置网络卫士安全网关的接口是否能够防 ARP 欺骗，网络卫士安全网关将会通过指定接口定期发送免费 ARP 报文，进行 ARP 信息更新，以达到防 ARP 欺骗的目的。

network interface <*string*> **gratuitous-arp-interval** <*number*>

命令描述：

设置安全网关接口的防 ARP 欺骗功能。

参数说明：

interface	指定要启用防 ARP 欺骗功能的接口

string	字符串，表示接口名称。目前网络卫士安全网关支持在物理接口、子接口和 Vlan 虚接口上启用防 ARP 欺骗功能。
gratuitous-arp-interval	设置发送免费 ARP 报文的时间间隔。
number	数值，取值范围为 0—1800 秒，当设置为 0 时表示不发送免费 ARP 报文，即关闭了该接口的防 ARP 欺骗功能。

实例：

**开启网络卫士安全网关 eth0 口的防 ARP 欺骗功能，设置每隔 10 秒发送一次免费 ARP 报文。

network interface *eth0* **gratuitous-arp-interval** *10* <cr>

ip

可以选择该物理接口是路由接口还是交换接口，如选择该接口为路由接口，则需要为该接口配置相应的 IP 地址和子网掩码。网络卫士安全网关不支持不同的物理接口配置相同的 IP 地址或 IP 地址在同一子网内。

若接口属性为交换接口，则配置 IP 地址时会提示错误信息，应在其所属的 VLAN 虚接口上配置 IP 地址信息。

ip add <*ipaddress*> [**mask** <*netmask*>] [**label** <*number*>] [ha_static]

命令描述：

增加当前接口对应的 IP 地址。

参数说明：

add	增加某接口对应的 IP 地址
ipaddress	IP 地址字符串
mask	可选项，设置子网掩码
netmask	子网掩码字符串
label	可选项，设定 IP 地址顺序标号，必须是区别于已有标号的数值，首次添加 IP 地址时缺省 label 为 0。
number	数值
ha_static	可选项，在双机热备时使用，如果选择此选项，则该接口的 IP 地址将不会被主设备同步，而保持原 IP 地址不变。

ip delete <*ipaddress*>

命令描述：

删除当前接口对应的 IP 地址。

参数说明：

delete	删除当前接口对应的 IP 地址
ipaddress	IP 地址字符串

ip clean <cr>

命令描述：

清空当前接口所有的 IP 地址。

mac-address

修改接口的 mac 地址。

mac-address < *macaddress* >

命令描述：

修改接口的 MAC 地址。

参数说明：

mac-address	修改接口的 mac 地址
macaddress	标准 MAC 地址字符串，格式为 aa:bb:cc:dd:ee:ff。

使用说明：

恢复接口的 MAC 地址使用# **restore** mac 命令。

实例：

**修改该接口的 MAC 地址为 00:10:5c:4e:30:22。

mac-address *00:10:5c:4e:30:22*<cr>

mode-set

设置接口工作模式为 IPS 或 IDS，只有当设备具有 IPS 功能模块时需要设置。当接口工作在 IPS 模式时，对数据做检测并转发；当工作在 IDS 模式时，对数据只作检测不作转发。默认为 IPS。

mode-set <ips|ids>

参数说明：

mode-set	设置接口的工作模式
ips|ids	选择工作模式，默认为 ips。

mss-adjust

设置该接口的 MSS（Maximum Segment Size）值。VPN 的 IPSEC 虚接口或 PPP 接口需要对报文做额外的封装，MTU 都小于 1500。这样，主机发出的报文常常需要在虚接口处分片重组，影响效率。对于 TCP 的连接，我们可以用以下的方法使得主机发出得报文小于一定的值，从而不需要分片。

mss-adjust auto <cr >

命令描述：

对该接口的 MSS 值进行调整，调整的数值是接口的 MTU－60，留部分空间给可能的 IP 选项。

mss-adjust off<cr >

命令描述：

对该接口的 MSS 值不作调整。

mss-adjust <*number*>

命令描述：

指定 MSS 调整的数值（范围为 200-1460）。

mtu

修改接口的 MTU 最大传输单元值。

mtu< *number*>

命令描述：

修改接口的 MTU 最大传输单元值（系统默认为 1500）。

参数说明：

mtu	修改接口的 MTU 最大传输单元值
number	数值。系统默认为 1500。范围在 68~1500 之间.

实例：

**修改该接口的 MTU 为 1350。

mtu *1350*<cr>

no

激活接口/改变接口的工作方式（由交换模式转变为路由模式）/删除接口描述信息。

no < shutdown|switchport|description >

命令描述：

改变接口的属性：激活接口/改变接口的工作方式（由交换模式转变为路由模式）/删除接口描述信息。

参数说明：

no	改变接口的属性。
shutdown|switchport|description	激活接口/改变接口的工作方式（由交换模式转变为路由模式）/删除接口描述信息

实例：

**激活该接口。

no shutdown <cr>

**将该接口由交换模式转换为路由模式。

no switchport<cr>

**删除对该接口的描述信息。

no description<cr>

ospf

接口 OSPF 路由协议属性设置。

ospf authentication <simple|message-digest>

命令描述：

设置 OSPF 路由协议的认证模式。

参数说明：

authentication	设置 OSPF 路由协议的认证模式
simple|message-digest	明文认证|MD5 摘要认证

实例：

**设置当前接口为明文认证模式

#ospf authentication simple

ospf authentication-key <*string*>

命令描述：

设置 SAMPLE 认证字。缺省不开启 ospf 的验证功能。如果打开，路由器要先互相通过验证才能互相通告路由信息。如果选择明文口令，口令会以明文方式在网络上发送，不安全。如果选择 md5 消息摘要方式会比较安全。

参数说明：

authentication-key	设置 SAMPLE 认证字
string	字符串

ospf message-digest-key <*string*>

命令描述：

设置 OSPF 路由协议的 MESSAGE-DIGEST 认证字。

参数说明：

message-digest-key	设置 OSPF 路由协议的 MESSAGE-DIGEST 认证字
string	字符串

ospf cost<*number*>

命令描述：

设置 OSPF 协议的接口花费，通常 OSPF 是根据链路带宽计算接口花费，用户可以根据需要对接口花费（权值）进行设定。

参数说明：

cost	设置 OSPF 协议的接口花费
number	数值，范围为 1-65535。

ospf dead-interval <*number*>

命令描述：

设置 OSPF 协议的邻居老化时间，即配置接口上邻居的最大超时时间，对于已经建立的邻居，在这个时间内如果没有接收到对方的 hello 报文，则认为邻居老化，会删除该邻居。单位是秒，缺省情况下是 40 秒。

参数说明：

dead-interval	设置 OSPF 协议的邻居老化时间
number	数值，范围为 1-65535。

ospf hello- interval <*number*>

命令描述：

设置发送 HELLO 报文间隔，即配置接口 hello 报文的发送周期。OSPF 设备定期向邻接路由器发送 HELLO 数据包，以探寻相邻路由器的状态。其探寻间隔可以进行设置。单位是秒，缺省情况下是 10 秒。

参数说明：

hello - interval	设置发送 HELLO 报文间隔
number	数值，范围为 1-65535。

ospf priority <*number*>

命令描述：

配置接口的 OSPF 优先级，该优先级的值会带在 hello 报文中发送。如果优先级数值配置为该网段所有路由器中最高，该路由器将被选择为 DR，如果设置成 0，则不参与 DR 或者 BDR 的选举。缺省优先级是 1。

参数说明：

priority	设置接口的 OSPF 优先级

number	数值，范围为 0-255。

ospf retransmit-interval <*number*>

命令描述：

设置重传时间间隔。重传间隔是指链路状态的重传间隔时间。如果一个路由器向相邻路由器发送一个新的链路状态包,在没有收到对端的确认包时,将发生重传。

参数说明：

retransmit-interval	设置重传时间间隔
number	数值，范围为 3-65535。

ospf transmit-delay <*number*>

命令描述：

设置链路状态传输延时。即配置发送每个 LSA 之前的延时。

参数说明：

transmit -delay	设置链路状态传输延时
number	数值，范围为 1-65535。

restore

恢复接口的 MAC 地址。

restore mac

命令描述：

恢复接口的 MAC 地址。

参数说明：

RESTORE	恢复接口的 MAC 地址
mac	必选项

实例：

**恢复该接口的 MAC 地址为出厂配置。

restore mac<cr>

rip

接口 RIP 路由协议属性设置。

rip authentication <simple|message-digest>

命令描述：

设置 RIP 路由协议的认证模式。

参数说明：

authentication	设置 RIP 路由协议的认证模式
simple|message-digest	明文认证|MD5 摘要认证

实例：

**设置当前接口为明文认证模式

rip authentication simple

rip no authentication mode <md5|text>

命令描述：

取消接口 RIP 协议的认证模式设置。

参数说明：

no authentication mode	取消 RIP 协议的认证模式设置，恢复为默认的
md5|text	md5 摘要认证|明文认证

实例：

**取消当前接口为明文认证模式的设置

rip no authentication mode md5

rip no receive version <1|2>

命令描述：

取消接收 RIP 协议的版本设置，恢复为默认的版本 2。

参数说明：

no receive version	取消接收 RIP 协议的版本设置
1|2	版本 1|版本 2

实例：

**取消当前接口接收协议版本号为 1 的设置

rip no receive version 1

rip no send version <1|2>

命令描述：

取消发送 RIP 协议的版本设置，恢复为默认的版本 2。

参数说明：

no send version	取消发送 RIP 协议的版本设置
1|2	版本 1|版本 2

实例：

**取消当前接口发送协议版本号为 1 的设置

rip no send version 1

rip no split-horizon [poisoned-reverse]

命令描述：

该接口的 RIP 协议不执行水平分割。

参数说明：

no split-horizon	该接口的 RIP 协议不执行水平分割
poisoned-reverse	带毒性逆转

rip receive version <1|2>

命令描述：

设置接收 RIP 协议的版本，默认为版本 2。

参数说明：

rip receive version	设置接收 RIP 协议的版本
1|2	版本 1|版本 2

实例：

**设置当前接口接收协议版本号为 1

rip receive version 1

rip send version <1|2>

命令描述：

设置当前接口发送 RIP 协议的版本，默认为版本 2。

参数说明：

send version	设置发送 RIP 协议的版本
1|2	版本 1|版本 2

实例：

**设置当前接口发送协议版本号为 1

rip send version 1

rip split-horizon [poisoned-reverse]

命令描述：

该接口的 RIP 协议执行水平分割和毒性逆转。

参数说明：

split-horizon	该接口的 RIP 协议执行水平分割
poisoned-reverse	毒性逆转

route-policy

绑定一个策略路由到接口。

route-policy set <*string*>

命令描述：

将一个策略路由和指定接口进行关联，接口可以为任何接口，但是只有可以路由的接口才会起作用，可以路由的接口包括：非交换模式的物理接口、VLAN 设备、子接口以及动态接口。

参数说明：

set	绑定一个策略路由到接口
string	指定策略路由名称。

route-policy clean <*cr*>

命令描述：

解除一个策略路由和接口的绑定。

reverse-path

设置是否根据报文的源 IP 地址和进入接口进行反向路由检查，若检查不到对应的反向路由信息，则判定该报文存在 IP 地址欺骗。

reverse-path <on|off>

命令描述：

设置是否根据报文的源 IP 地址和进入接口进行反向路由检查。

参数说明：

reverse-path	设置是否根据报文的源 IP 地址和进入接口进行反向路由检查
on	开启反向路由查询功能
off	关闭反向路由查询功能

show

查看当前接口的配置和属性。

show [configuration]

命令描述：

查看当前接口的配置信息和收发数据报文的统计情况。

参数说明：

show	查看当前接口的配置和属性
configuration	可选项，不指定该参数时查看该接口的所有属性，包括配置信息和接收和发送的数据报文统计信息。指定该参数时只显示接口的配置信息。

实例：

**查看当前接口的所有属性，包括配置信息和接收和发送的数据报文统计信息。

show<cr>

**查看当前接口的详细配置属性

show configuration<cr>

shutdown

停用当前接口。

shutdown <cr.>

命令描述：

停用当前接口。

使用说明：

启用当前接口用**# no shutdown**<cr>命令。

speed

设置接口的数据传输速率。

speed <10|100|1000|auto>

命令描述：

设置接口的数据传输速率：手工设定接口的数据传输速率，或设为自动协商数据传输速率。

参数说明：

speed	设置接口的数据传输速率
10|100|1000|auto	选定接口传输速率为 10M、100M、1000Mbps 或设定为自动协商模式。

使用说明：

当设备不支持 1000M 时候（使用命令 SPEED），报错信息如下：

TopsecOS.network# interface eth2 speed 1000

error -12148 : speed or duplex not supported on this interface

实例：

**设置该接口的数据传输速率为 100Mbps。

speed *100*<cr>

subif

网络卫士安全网关的接口工作在路由模式时，一个物理接口可以在逻辑上划分为多个子接口，这些子接口和安全网关的物理接口之间没有任何关系，只是发送给逻辑子接口的数据报文要通过该物理接口来转发，新添加的逻辑子接口不会继承

原物理接口设定的规则。

subif add <[**id** <*number*>]|[**range** <*string*>]>

命令描述：

添加子接口到当前物理接口。

参数说明：

add	添加子接口到当前接口，可以根据 ID 号或范围来添加。
id	设定新增子接口的 ID 号
number	数值，范围为 0-31。
range	设定 ID 在一定范围内的子接口
string	字符串，格式为 x-y，例如 1-3

使用说明：

添加子接口到当前物理接口时，可以指定 id 号一次添加一个子接口，也可以指定 range 一次添加多个子接口。

实例：

*在当前物理接口上添加一个 ID 号为 1 的子接口。

#**subif add id** *1*<cr>

*在当前物理接口上添加 ID 号为 1 到 3 的子接口。

subif add range *1-3*<cr>

subif clean<cr>

命令描述：

清空当前物理接口的所有子接口。

subif delete<[**id** <*number*>]|[**range** <*string*>]>

命令描述：

删除当前物理接口的子接口。

参数说明：

delete	删除当前物理接口的子接口，可以根据 ID 号或范围来删除。
id	设定欲删除子接口的 ID 号
number	数值
range	设定欲删除子接口的 ID 范围
string	字符串，格式为 x-y，例如 1-3

使用说明：

删除当前物理接口的子接口时，可以指定 id 号一次删除一个子接口，也可以指定 range 一次删除多个子接口。

实例：

*在当前物理接口上删除一个 ID 号为 1 的子接口。

#subif delete id *1*<cr>

*在当前物理接口上删除 ID 号为 1 到 3 的子接口。

subif delete range *1-3*<cr>

subif show<cr>

命令描述：

查看当前物理接口的所有子接口。

switchport

设置当前接口作为交换接口的属性。交换环境中的 2 种连接类型:

1）接口工作在 access 模式：指的是接口只属于一个 VLAN,且仅向该 VLAN 转发数据帧的端口。

2）Trunk 模式：指的是能够转发多个不同 VLAN 的通信的端口

switchport <cr>

命令描述：

设置当前物理接口的工作模式为交换模式。

switchport trunk <**allowed-vlan** <*string1*>| **native-vlan** <*string2*>| **encapsulation** <isl|dotlq> >

命令描述：

设置该交换接口属于 trunk 接口（即一个接口可以同时属于多个 VLAN）时的属性，。即该 trunk 端口属于哪些 VLAN，其 native-vlan 的 ID 号，及其封装模式。

参数说明：

switchport	设置当前物理接口的工作模式为交换模式时的属性
trunk	设置该交换接口属于 trunk 接口时的属性
allowed-vlan	设置端口所属 VLAN 范围，默认情况下为 1-1000

string1	字符串，指定 VLAN 范围，格式为 1-10，表示 1 到 10；1，10 表示 ID 为 1 或 10 的两个 vlan。
native-vlan	trunk 端口的缺省 VLAN ID。由于 Trunk 端口属于多个 VLAN，所以需要设置缺省 VLAN ID，用于当该交换接口接收到没有标记的报文时，该 Trunk 端口将此报文发往缺省 VLAN ID 标识的 VLAN。该 vlan 在 trunk 中传送不带封装的帧，只在封装为 802.1q 的 trunk 生效。
string2	字符串，指定 VLAN ID 值。
encapsulation	设定 VLAN 封装模式。
isl|dotlq	思科的 ISL 封装格式 | IEEE 802.1Q 封装格式。

实例：

**设定当前物理接口为 trunk 接口时，属于 ID 号为 1 和 5 的 VLAN。

#switchport trunk allowed-vlan *1,5*<cr>

**设定当前物理接口为 trunk 接口时，属于 ID 号为 1 到 10 的 VLAN。

#switchport trunk allowed-vlan *1-10*<cr>

**设定当前物理接口为 trunk 接口时，其 native-vlan 的 ID 号为 5。

#switchport trunk native-vlan *5*<cr>

**设定当前物理接口为 trunk 接口时，其 VLAN 封装模式为 ISL。

switchport trunk encapsulation isl<cr>

switchport access-vlan<*number*>

命令描述：

设置该交换接口只属于一个 VLAN 时，指定所属的 VLAN ID 号码。

参数说明：

switchport	设置当前物理接口的工作模式为交换模式时的属性
access-vlan	设置该交换接口为 access 接口时所属的 VLAN ID 号码
number	数值，指定 VLAN ID 号。

实例：

**设置该交换接口为 access VLAN 时属于 ID 号为 2 的 VLAN。

switchport access-vlan *2*<cr>

switchport mode <access|trunk>

命令描述：

设置该交换接口为 access 接口还是 trunk 接口。

参数说明：

switchport	设置当前物理接口的工作模式为交换模式时的属性
mode	设置该交换接口的工作模式：为 access 接口还是 trunk 接口.
access|trunk	access 模式：该交换接口只属于一个 VLAN。 trunk 模式：该交换接口可以同时属于多个 VLAN。

实例：

**设置该交换接口为 access 模式。

switchport mode access<cr>

vlan-vpn

当物理接口工作在交换模式时，需要设置是否开启接口的 QinQ 特性，开启端口的 QinQ 功能后，当该端口接收到报文，无论报文是否带有 vlan tag，安全网关都会为该报文打上本端口 access vlan 的 vlan tag，如果是 trunk 口则会打上 native vlan 的 tag。这样，如果接收到的是已经带有 vlan tag 的报文，该报文就成为双 tag 的报文；如果接收到的是不带 vlan tag 的报文，该报文就成为带有端口缺省 vlan tag 的报文。

vlan-vpn <enable|disable>

命令描述：

设置是否开启接口的 QinQ 特性。

参数说明：

vlan-vpn	设置是否开启接口的 QinQ 特性
enable|disable	开启或关闭

使用说明：

只有接口工作在交换模式时，才需要开启 QinQ 特性。否则如果接口工作在路由模式，将提示错误信息。

实例：

**设置开启该接口的 QinQ 特性。

vlan-vpn enable <cr>

vlan-vpn tpid<*string*>

命令描述：

当开启接口的 QinQ 特性时，配置 QinQ 接入功能的协议类型，默认为 0x8100。

参数说明：

vlan-vpn tpid	配置 QinQ 接入功能的协议类型。
string	输入格式为 16 进制，默认为 0x8100。

使用说明：

只有接口工作在交换模式时，并开启 QinQ 特性，才需要设置该参数。

vrid

设置该接口所属的虚拟路由备份组的 ID 号。

vrid <*number*>

命令描述：

设置该接口所属的虚拟路由备份组的 ID 号。

参数说明：

vrid	设置该接口所属的虚拟路由备份组的 ID 号
number	数值，范围为 0-255。0 表示不属于任何虚拟路由备份组。

使用说明：

无。

实例：

**设置接口属于 VRID 2。

vrid *2*<cr>

vsid

设置接口所属虚系统的 ID 号。默认为 0，表示不属于任何虚系统。

vsid <*number*>

命令描述：

设置接口所属虚系统的 ID 号。

参数说明：

vsid	设置接口所属虚系统的 ID 号

number	数值，范围为 0-254。默认为 0，表示不属于任何虚系统。

实例：

**设置接口属于 VSID 2。

vsid *2*<cr>

igmp

IGMP 组管理协议设置

group

IGMP 成员关系设置

group show<cr>

命令描述：

查看 IGMP 组成员关系。

interface

IGMP 接口配置

interface show<cr>

命令描述：

查看 IGMP 组成员关系。

interface address<cr>

命令描述：

查看所有虚拟接口的地址。

interface start<*string*>

命令描述：

启动指定的 IGMP 虚拟接口。

参数说明：

start	启动指定的 IGMP 虚拟接口
string1	字符串，为物理接口或 VLAN 虚接口的名称。

interface stop<*string*>

命令描述：

停止指定的 IGMP 虚拟接口。

参数说明：

stop	停止指定的 IGMP 虚拟接口
string1	字符串，为物理接口或 VLAN 虚接口的名称。

robust-count

允许丢包个数设置

roubust-count show<cr>

命令描述：

查看允许丢包个数设置。

robust-count set interface <*string*> **count** <*number*>

命令描述：

设置允许丢包个数

参数说明：

Set	设置允许丢包个数
interface	指定接口
string	接口名称字符串
count	设置允许丢失包的最大个数
number	数值

version

设置 IGMP 协议版本

version set interface <*string*><1|2|3>

命令描述：

配置接口运行的 IGMP 协议版本

参数说明：

set	配置接口运行的 IGMP 协议版本
interface	指定接口名
string	物理接口或虚接口名成字符串
1|2|3	指定版本号

ip-probe

IP 探测管理。通过对指定的 IP 从指定接口发送 ping 包进行探测，探测链路的状态。在静态路由、HA 以及链路备份模块可以引用 IP 探测的结果。

Ip-probe add dev <*string1*> **probe-ip** <*string2*> [**interval** <*number*>][**probe-id** <*number*>]

命令描述：

添加一条 HA 探测路径，对指定的 IP 从指定接口发送 ping 包进行探测。

参数说明：

add	添加一条探测路径
dev	指定探测用的网络接口
string1	字符串，为物理接口或 VLAN 虚接口的名称,如 eth0 或 vlan.0001。
Probe-ip	探测的 IP 地址
string2	IP 地址字符串。当需要设定多个接口为探测用的网络接口时，IP 地址之间用逗号隔开，
interval	设置发送 ping 报文的时间间隔。可选项。 说明： 探测时间间隔为上次探测结束的时间和下一次探测开始之间的时间间隔。
number	数值，范围为 1 到 3600。默认为 5。单位为秒。
probe-id	设置探测路径的 ID。可选项，不设置该参数时按照添加顺序自动为链路设置 ID 号。
number	数值，范围为 100-104。

实例：

**添加一条探测路径，接口为 eth0，探测 IP 地址为 10.10.10.22。

ip-probe add dev *eth0* **probe-ip** *10.10.10.22*。

ip-probe delete probe-id<*number*>

命令描述：

根据 ID 号删除一条探测路径。

参数说明：

delete	删除一条条探测路径
probe-id	指定欲删除探测路径的 ID 号
number	数值

实例：

**删除 ID 号为 8649 的 HA IP 探测路径。

ip-probe delete probe-id *8649*<cr>

Ip-probe modify probe-ip <*string2*> [**dev** <*string1*>] [**interval** <*number*>][**probe-id** <*number*>]

命令描述：

修改一条探测路径的参数

参数说明：

modify	修改一条探测路径的参数
probe-id	指定代修改的探测路径的 ID
number	数值，范围为 100-104。
dev	指定探测用的网络接口
string1	字符串，为物理接口或 VLAN 虚接口的名称，如 eth0 或 vlan.0001。
Probe-ip	探测的 IP 地址
string2	IP 地址字符串。当需要设定多个接口为探测用的网络接口时，IP 地址之间用逗号隔开。
interval	设置发送 ping 报文的时间间隔。可选项。 说明： 探测时间间隔为上次探测结束的时间和下一次探测开始之间的时间间隔。
number	数值，范围为 1 到 3600。默认为 5。单位为秒。

ip-probe show<cr>

命令描述：

查看所有探测路径。

ip-probe clean <cr>

命令描述：

清空所有探测路径。

l2tp

网络卫士安全网关支持 L2TP 协议，远端用户可通过天融信公司提供的相应的 L2TP 客户端组件与安全网关通过 L2TP 服务建立连接，从而访问整个网络。安全网关提供的 L2TP 服务还需要如下配置：（1）在本模块配置 L2TP 相关属性。（2）在 authentication -localdb 命令中添加类型为 vpn 的远程用户；并添加 basic 服务器。（3）在提供服务的接口开放 L2TP 服务（4）在访问控制规则处定义针对于远程用户的访问控制规则。（5）对 L2TP 客户端配置与安全网关的连接参数。

l2tp clean ip-pool<cr>

命令描述：

清空 L2TP 的 IP 地址池设置。地址池是指由一个起始 IP 地址和一个终止 IP 地址组成的 IP 地址范围，当客户端使用 L2TP 服务与安全网关的某一物理接口建立连接时，安全网关将为客户端动态分配该地址池中的一个地址作为用户的 IP 地址。

参数说明：

clean	清空 L2TP 的 IP 地址池设置。
ip-pool	IP 地址池

l2tp restart <cr>

命令描述：

重新启动 L2TP 服务。如果 L2TP 服务已经启动，则修改配置参数后需要重新启动该服务才能使修改后的配置生效。

l2tp set cipher< on|off>

命令描述：

设置通信是否加密

参数说明：

set cipher	设置通信是否加密
on|off	是/否

l2tp set ip-pool local <*ipaddress1*> **min_ip** <*ipaddress2*> **max_ip** <*ipaddress3*>

命令描述：

设置 L2TP 服务的本地虚拟 IP 地址和客户端地址池属性。本地虚拟 IP 地址为安全网关内部使用，和地址池必须设置在同一个网段。L2TP 客户端与安全网关连接成功后可以查看到本地虚拟 IP 地址和为客户端分配的 IP 地址。

参数说明：

set ip-pool	设置 L2TP 服务的地址池属性
local	设置 L2TP 服务的虚拟本地 IP 地址，当 L2TP 客户端与安全网关建立连接时客户端将与此处设定的虚拟 IP 地址进行通信。
ipaddress1	IP 地址字符串。
min_ip	设置地址池的起始地址
ipaddress2	IP 地址字符串
max_ip	设置地址池的终止地址
ipaddress3	IP 地址字符串，应大于或等于起始 IP 地址。

实例：

**设置安全网关的本地虚拟 IP 地址为 172.16.100.1 ，地址池为 172.16.200.101 到 172.16.200.200。

l2tp set ip-pool local *172.16.100.1* **min_ip** *172.16.200.101* **max_ip** *172.16.200.200*。

l2tp set port<*number*>

命令描述：

设置安全网关提供 L2TP 服务的端口号，默认段口号为 1701。

参数说明：

set port	设置安全网关提供 L2TP 服务的端口号
number	端口号，默认为 1701。

l2tp show <running | status>

命令描述：

查看 L2TP 的运行信息和配置信息。

参数说明：

show	查看 L2TP 的运行信息和配置信息
running | status	运行配置（主要是服务端口、地址池信息）|链路状态（主要是隧道信息）

实例：

**查看 L2TP 的链路状态：链路数量和链路 IP 地址。

l2tp show status<cr>

**查看 L2TP 运行配置：运行端口和地址池设置。

l2tp show running<cr>

l2tp start <cr>

命令描述：

启动 L2TP 服务。

l2tp stop <cr>

命令描述：

停止 L2TP 服务。

link-backup

在安全网关的整个运行期间，无法保证设备所有接口都能长时间正常运作，或不可避免地会遇到一些可知或不可知因素造成设备某接口无法运行。网络卫士安全网关提供了“链路备份”功能来实时监视整个链路的工作情况，一旦主链路发现异常，就立即启动“链路备份”功能自动切换到另一条备用链路，以确保网络的正常通信。同时系统会不断探测主链路的通信状态，一旦检测到主链路恢复通信，系统会自动由从链路切换回主链路。另外，主链路会实时检测从链路是否可用，

并在从链路不可用时报警。

linkbak set masterid <*number*> **slaveid** <*number*>

命令描述：

链路备份参数设置。

参数说明：

set	链路备份参数设置
masterid	指定主链路
number	数值，范围为 100-104。
slaveid	指定从链路接口
number	数值，范围为 100-104。

linkbak show <cr>

命令描述：

查看链路备份的运行信息和状态信息。

linkbak start <cr>

命令描述：

启动链路备份服务。

参数说明：

start	启动链路备份服务
cr	键盘回车符

linkbak stop <cr>

命令描述：

停止链路备份服务。

linkbak clean<cr>

命令描述：

清空链路备份所有设置。

mac-address-table

MAC 地址表的配置和管理。网络卫士安全网关内部维护了 MAC 地址表，保持了网络卫士安全网关所学习到主机 MAC 地址与安全网关接口的对应表，该接口达标主机存在的方向。当网络卫士安全网关转发数据帧时，会查看 MAC 地址表，如果该目的 MAC 存在网络卫士安全网关的 MAC 地址表中，网络卫士安全网关将直接通过该 MAC 地址所对应的接口发送。

mac-address-table add static address <*macaddress*> **vlan** <*number*> **interface** <*string*>

命令描述：

添加一条静态 MAC 地址表项，只能增加虚接口 MAC 地址。设定对某 VLAN 中已知 MAC 地址的某设备的访问通过哪个物理接口。

参数说明：

add static address	添加一条静态 MAC 地址表项
macaddress	Mac 地址字符串，格式为 xx:xx:xx:xx:xx:xx
vlan	指定设备属于哪个 VLAN
number	字符串，指定 VLAN 名，格式为 vlan.xxxx
interface	指定物理接口名称
string	接口名字符串，如 eth0

mac-address-table delete static address <*macaddress*> **vlan** <*number*> **interface** <*string*>

命令描述：

删除一条静态 MAC 地址表项。

参数说明：

delete static address	删除一条静态 MAC 地址表项
macaddress	Mac 地址字符串，格式为 xx:xx:xx:xx:xx:xx
vlan	指定设备属于哪个 VLAN
number	字符串，指定 VLAN 名，格式为 vlan.xxxx
interface	指定物理接口名称
string	接口名字符串，如 eth0

mac-address-table show [type <static|dynamic>] [**address** <*macaddress*>] [**vlan** <*number*>] [**interface** <*string*>]

命令描述：

查看 MAC 地址表的内容，包括静态 MAC 地址表和动态 MAC 地址表。

参数说明：

show	查看 MAC 地址表的内容
type	指定查看类型
static|dynamic	静态 MAC 地址表|动态 MAC 地址表项
address	指定查看的 MAC 地址
macaddress	Mac 地址字符串，格式为 xx:xx:xx:xx:xx:xx
vlan	指定查看哪个 VLAN 的 MAC 地址表项
number	字符串，指定 VLAN 名，格式为 vlan.xxxx
interface	指定查看哪个物理接口的 MAC 地址表项
string	接口名字符串，如 eth0

使用说明：

指定参数时只查看相关类型的 MAC 地址表项，不指定参数时查看 MAC 地址表的统计情况。

实例：

**查看所有的 MAC 地址表的统计情况。

mac-address-table show<cr>

Total:8192 static:1 link:9 pool:8182 route:8

1 matched mac entries.

mac vlan dev static ref

00:90:0B:05:75:60 1 eth1 1 1

mac-address-table show type dynamic

Total:8192 static:2 link:9 pool:8182 route:9

0 matched mac entries.

mac-address-table clean static <cr >

命令描述：

清空静态 MAC 地址表项。

mpls

网络卫士安全网关支持 MPLS 报文透传，只有当安全网关工作在透明模式时需要开启 MPLS 透传功能，路由模式时安全网关将直接丢弃 MPLS 报文。

只有当安全网关工作在透明模式时需要开启 MPLS 透传功能，路由模式时安全网关将直接丢弃 MPLS 报文。

透明模式下，如果开启 MPLS 透传功能，则可以对通过安全网关的 MPLS 报文进行安全策略控制；如果关闭 MPLS 透传功能，安全网关将直接转发 MPLS 报文。

mpls handle <on|off>

命令描述：

开启/关闭 MPLS 报文透传功能。

参数说明：

on|off	开启/关闭 MPLS 报文透传功能，“on”表示开启，“off”表示关闭，关闭该功能后，所有接收到的 MPLS 报文都会被丢弃。

实例：

**开启网络卫士安全网关的 MPLS 报文透传功能。

mpls handle on <cr>

mroute

网络卫士安全网关允许 IP 多点广播数据报文穿越网络卫士安全网关。对于多播协议，网络卫士安全网关支持 IGMP V1 及 IGMP V2。当安全网关工作在路由模式下，如果需要转发多播数据包，管理员必须配置多播路由，如果没有配置，则认为网络卫士安全网关不参与接收和转发多播。

mroute add src <*string*> **srcdev** <*devname1*> **group** <*ipadress*> **outdev** <*devname2*>

[join_group]

命令描述：

增加一条多播路由表项。每个条目包括多播组和对应的转发接口。如果没有配置，则认为网络卫士安全网关不参与接受和转发多播。

参数说明：

add	增加一条多播路由表项
src	指定多播服务器所在的地址或地址段，可以配置为 0.0.0.0/0，则默认是所有地址。
string	字符串，表示源网络的地址/掩码位 格式为 x.x.x.x/x。
srcdev	指定接收多播报文的接口，和服务器端相连
devname1	物理接口或 VLAN 虚接口名称字符串，例如 eth0，vlan.0001。
group	指定多播组的 IP 地址
ipadress	D 类多播组 IP 地址，在 224.0.0.0 到 239.255.255.255 的 D 类地址范围内
outdev	指定转发多播报文的接口，和客户端连接。不能与 srcdev 设定为相同的接口。
devname2	物理接口或 VLAN 虚接口名称字符串，例如 eth0，vlan.0001。
join_group	可选项，指定是否向上游多播路由器发送加入报告。 a）网络卫士安全网关如果为叶子节点（即仅仅接收多播报文不转发），则不用加入。 b）如果网络卫士安全网关处于中间节点的情况下（即在目的接口有下游多播路由器，需要转发多播报文），由安全网关设备定时向上游多播路由器发送加入报告（joining report），以保证多播报文顺利转发给下游多播路由设备，维护多播树结构。则一定要选择此项。

使用说明：

多播主机利用 I G M P 通知路由器，路由器所在子网的一台计算机想加入一个特定的多播组。I G M P 是 I P 多播方案的基础。要想使它正常工作，两个多播节点之间的所有路由器都必须提供对 I G M P 的支持。例如，假定机器 A 和 B 加入了多播组 2 2 4 . 1 . 2 . 3，两者间总共存在着三个路由器。此时，三个路由器都必须具有 I G M P 能力，以保障通信的成功进行。若某个路由器不具备 I G M P 能力（即不支持 I G M P），那么收到多播数据后，会将它草草地丢弃了事。若一个应用加入了多播组，一条 I G M P “加入”命令便会发给子网上那个特殊的“所有路由器”地址（2 2 4 . 0 . 0 . 2）。该命令用于通知所有路由器，有客户机对一个特定的多播地址产生了兴趣，即它们想加入那个多播组。以后，假如路由器收到了发给那个多播地址的数据，便会将其转发给所有多播客户机。

实例：

**添加一条多播路由，由源网段 10.10.10.0/24 发送给多播组 224.1.1.24 的多播报

文经过 eth1 口接收，并经过 eth2 口转发出去。

mroute add src *10.10.1.0/24* **srcdev** *eth1* **group** *224.1.1.24* **outdev** *eth2*

mroute delete src <*string*> **srcdev** <*devname1*> **group** <*ipadress*> **outdev** <*devname2*>

[join_group]

命令描述：

根据参数删除一条多播路由表项。

参数说明：

delete	删除一条多播路由表项
src	指定多播服务器所在的地址或地址段，可以配置为 0.0.0.0/0，则默认是所有地址。
string	字符串，表示源网络的地址/掩码位 格式为 x.x.x.x/x。
srcdev	指定接收多播报文的接口，和服务器端相连
devname1	物理接口或 VLAN 虚接口名称字符串，例如 eth0，vlan.0001。
group	指定多播组的 IP 地址
ipadress	D 类多播组 IP 地址，在 224.0.0.0 到 239.255.255.255 的 D 类地址范围内
outdev	指定转发多播报文的接口，和客户端连接。不能与 srcdev 设定为相同的接口。
devname2	物理接口或 VLAN 虚接口名称字符串，例如 eth0，vlan.0001。
join_group	可选项，指定是否向上游多播路由器发送加入报告。 a）网络卫士安全网关如果为叶子节点，即没有下游多播路由器时，则安全网关仅仅接收多播报文不转发，不用加入。 b）如果网络卫士安全网关处于中间节点的情况下（即在目的接口有下游多播路由器，需要转发多播报文），由安全网关设备定时向上游多播路由器发送加入报告（joining report），以保证多播报文顺利转发给下游多播路由设备，维护多播树结构。则一定要选择此项。

实例：

**删除一条多播路由：由源网段 10.10.10.0/24 发送给多播组 224.1.1.24 的多播报文经过 eth1 口接收，并经过 eth2 口转发出去。

mroute delete src *10.10.1.0/24* **srcdev** *eth1* **group** *224.1.1.24* **outdev** *eth2*

mroute delete id <*number*>

命令描述：

根据 ID 来删除一条静态多播路由。

参数说明：

delete	删除一条静态多播路由
id	根据路由 ID 号删除
number	数值

实例：

**删除 ID 号为 2000 的多播路由。

mroute delete id *2000*<cr>

mroute clean<cr>

命令描述：

清除所有的多播路由。

mroute show<cr>

命令描述：

查看所有的静态多播路由。

ospf

OSPF 路由协议配置。OSPF 协议是一个基于链路状态的动态路由协议，其基本原理是：在一个 OSPF 网络中，每一台路由器首先与自己的邻居建立邻接关系，然后向形成邻接关系的邻居之间发送链路状态通告（LSA），链路状态通告描述了所有的链路信息，每一个路由器接收到 LSA 都会把这些通告记录在链路数据库中，并发送一个副本给他的邻居，通过 LSA 泛洪到整个区域，所有的路由器都会形成相同的链路状态数据库，当所有路由器链路状态数据库相同时，会以自己为根，通过 SPF 算法计算出一个无环的拓扑，从而计算出自己到达系统内部可达的最佳路由。

注意：

1）设置安全网关的 IP 地址时一定要将该 IP 的 label 设置为 0，方可利用该 IP 地址启动 OSPF 服务。

2）安全网关上的配置完成后，一定要重新启动接口一次。

ospf no <**router-id** | [**access-list** <*string1*> <permits|deny><*string2*>] | [**area**<string3> **authentication** <simple|message-digest>] | [**debug** <event|ism|lsa|nsm>] | [**debug packet** <dd| hello| ls-ack| ls-request|ls-update>] | [**distribute-list** <*string4*> **out** <connected|bgp|rip>] | [**default-metric** <*number2*>] | [**network** <*string5*> **area** <*number3*>] | [**redistribute** <connected|rip|static>]>[[**default-information**]]>

命令描述：

删除路由器 IP 地址设置规则。

参数说明：

no	删除设定
router-id	可选项，取消路由器 IP 地址设置
access-list	取消设置 OSPF 访问控制规则
string1	字符串，设定规则名。
permits|deny	指定允许或禁止运行 OSPF 协议
string2	设定 OSPF 协议运行网段，格式为 x.x.x.x/x
area	取消设定 OSPF 的区域 ID
string	字符串，设定区域 ID。
authentication	指定认证模式
simple|message-digest	明文认证|MD5 摘要认证
debug	设置 OSPF 协议的事件调试功能
event | ism| lsa| nsm	事件/接口状态机/链路状态通知/邻居状态机
packet	取消选择调试哪种数据报文
dd|hello|ls-ack|ls-request |ls-update	数据库描述报文/hello 报文/链路状态响应/链路状态请求/链路状态更新报文
default-metric	设置 OSPF 协议引入路由的跳数
number	设定数值，范围为 1-16。
network	取消设置运行 OSPF 协议的网段
string	设定子网地址及子网掩码，格式为 x.x.x.x/x
area	取消设定该网段所属的区域 ID
number	数值。范围为 0-4294967295。
redistribute	设置重发布哪些路由信息到 OSPF 路由中作为外部路由信息
connected|rip|static	直连路由| RIP 路由| 静态路由

使用说明：

只有启动了 OSPF 进程，才可以取消设置 OSPF 协议的相关参数。

实例：

**删除 OSPF 访问控制规则，名称为 ww，内容为禁止网段 10.10.10.0/24 运行 OSPF 协议。

ospf no access-list *ww* deny *10.10.10.0/24*<cr>

**删除路由器 IP 地址设置

ospf no route-id<cr>

ospf access-list<*string1*> <permits|deny><*string2*>

命令描述：

设置 OSPF 访问控制规则：即设定在哪个网段允许运行 OSPF 协议，哪个网段禁止运行 OSPF 协议。

参数说明：

access-list	设置 OSPF 访问控制规则
string1	字符串，设定规则名。
permits|deny	指定允许或禁止运行 OSPF 协议
string2	设定 OSPF 协议运行网段，格式为 x.x.x.x/x

使用说明：

只有启动了 OSPF 进程，才可以设置 OSPF 协议的相关参数。

实例：

**设置 OSPF 访问控制规则，名称为 ww，内容为禁止网段 10.10.10.0/24 运行 OSPF 协议。

ospf access-list *ww* deny *10.10.10.0/24*<cr>

ospf area <*string1*>**authentication** <simple|message-digest> **stub** <default|no-summary> **range** <string>

命令描述：

设定 OSPF 协议的区域，主要指：设定运行 OSPF 协议的网段属于哪个 OSPF 区域，并且设定该区域内的路由器更新路由时是否进行认证，进而采用何种认证方式。

参数说明：

area	设定 OSPF 的区域 ID
string1	字符串，设定区域 ID。
authentication	指定认证模式
simple|message-digest	明文认证|MD5 摘要认证
stub	设置 stub 模式。
default|no-summary	默认|无摘要
range	设置地址汇聚。
string2	字符串，设定地址汇聚。

使用说明：

只有启动了 OSPF 进程，才可以设置 OSPF 协议的相关参数。

实例：

**设定运行 OSPF 协议的网段属于区域 1 采用明文认证方式。

ospf area *1* **authentication** simple<cr>

ospf debug <event|ism|lsa|nsm>

命令描述：

设置 OSPF 协议的调试功能。

参数说明：

debug	设置 OSPF 协议的事件调试功能
event | ism| lsa| nsm	事件/接口状态机/链路状态通知/邻居状态机

使用说明：

只有启动了 OSPF 进程，才可以设置 OSPF 协议的相关参数。

实例：

**设置对 OSPF 协议的事件进行调试。

ospf debug event<cr>

ospf debug packet <dd|hello|ls-ack|ls-request|ls-update>

命令描述：

设置 OSPF 协议的报文调试功能。

参数说明：

debug	设置 OSPF 协议的报文调试功能
packet	选择调试哪种数据报文
dd|hello|ls-ack|ls-request|ls-update	数据库描述报文/hello 报文/链路状态响应/链路状态请求/链路状态更新报文

使用说明：

只有启动了 OSPF 进程，才可以设置 OSPF 协议的相关参数。

实例：

**设置调试 hello 报文。

ospf debug packet hello<cr>

ospf default-metric <*number*>

命令描述：

设置 OSPF 协议引入路由的跳数。

参数说明：

default-metric	设置 OSPF 协议引入路由的跳数
number	设定数值，范围为 0-16777214。

使用说明：

只有启动了 OSPF 进程，才可以设置 OSPF 协议的相关参数。

实例：

**设置 OSPF 协议引入路由的跳数为 3。

ospf default-metric *3*<cr>

ospf default-information <always|default> [**metric** <*number*>]

命令描述：

设置 OSPF 协议缺省路由重发布信息。

参数说明：

default-information	选择重新发布方式
always|default	可选项为强制发布和缺省发布两种
metric	设置路由的 metric 值，表示路由的优先级
number	设定数值，范围为 0-16777214。

使用说明：

只有启动了 OSPF 进程，才可以设置 OSPF 协议的相关参数。

实例：

**设置 OSPF 协议强制发布缺省路由信息。

ospf default-information always

ospf distribute-list <*string*> **out** <connected | bgp | static>

命令描述：

设置 OSPF 协议过滤路由更新的网段。

参数说明：

distribute-list	设置 OSPF 协议过滤路由更新的网段

string	字符串，设置名称。
out	指定哪种接口进行过滤更新。
connected | bgp | rip|static	直连网段| BGP 协议网段|RIP 协议网段 |静态路由协议网段

使用说明：

只有启动了 OSPF 进程，才可以设置 OSPF 协议的相关参数。

实例：

**设置 OSPF 协议对直连网段过滤路由更新。

ospf distribute-list *a* **out** connected <cr>

ospf network <*string*> **area** <*number*>

命令描述：

设定在哪个网段运行 OSPF 协议以及该网段属于哪个 OSPF 区域。

参数说明：

network	设置运行 OSPF 协议的网段
string	设定子网地址及子网掩码，格式为 x.x.x.x/x
area	设定该网段所属的区域 ID
number	数值。范围为 0-4294967295。

使用说明：

只有启动了 OSPF 进程，才可以设置 OSPF 协议的相关参数。

实例：

**设置在网段 10.10.10.0/24 运行 OSPF 协议，该网段属于区域 1。

ospf network *10.10.10.0/24* **area** *1* <cr>

ospf passive-interface <*string*>

命令描述：

设定在哪个接口抑制 OSPF 协议路由更新。即设置禁止哪个接口转发路由信息，则此接口将只是被动地监听路由更新信息。

参数说明：

passive-interface	设定在哪个接口抑制 OSPF 协议路由更新
string	设定物理接口或 VLAN 虚接口名。

使用说明：

只有启动了 OSPF 进程，才可以设置 OSPF 协议的相关参数。

实例：

**设置禁止在 eth0 接口接口转发路由信息，eth0 口只能被动地监听路由更新信息。

ospf passive-interface *eth0* <cr>

ospf redistribute <connected|rip|static|bgp> [**metric** <*number*>]

命令描述：

设置要引入哪些路由信息到 OSPF 路由中作为外部路由信息。网络卫士安全网关的 OSPF 协议支持将直连路由、RIP 路由、静态路由等路由信息重新发布入 OSPF 自治系统。

参数说明：

redistribute	设置重发布哪些路由信息到 OSPF 路由中作为外部路由信息
connected|rip|static|bgp	直连路由| RIP 路由| 静态路由|BGP 路由
metric	可选项，设置路由引入后的 metric 值，默认为 1 。
number	数值，范围为 0-1677721 。

使用说明：

只有启动了 OSPF 进程，才可以设置 OSPF 协议的相关参数。

实例：

**设置重发布静态路由信息到 OSPF 路由中作为外部路由信息，metric 值为默认值。

ospf redistribute static<cr>

ospf route-id <*ipaddress*>

命令描述：

手工指定 OSPF 协议的 router-id。如果不指定，OSPF 使用某个网卡的 IP 地址作为 router-id，缺点是 router-id 有可能发生变化。

参数说明：

route-id	设定路由器 IP 地址

ipaddress	IP 地址字符串，一般用设备某接口的 IP 地址。

使用说明：

只有启动了 OSPF 进程，才可以设置 OSPF 协议的相关参数。

实例：

**设置路由器 IP 地址为 10.10.10.22。

ospf route-id *10.10.10.22* <cr>

ospf show [interface|neighbor|route|debugging|running]

命令描述：

查看 OSPF 协议的相关配置信息。

参数说明：

show	查看 OSPF 协议的相关配置信息
interface| neighbor| route |debugging |running	可选项，接口信息|邻居信息|路由信息|调试信息|运行信息。不指定参数时显示所有信息。

使用说明：

只有启动了 OSPF 进程，才可以设置 OSPF 协议的相关参数。

实例：

**查看接口信息，包括接口是否激活，接口是否运行 OSPF 协议。

ospf show interface <cr>

ospf show database < asbr-summary|external |network |router |summary |max-age |self-originate>

[**adv-router**<*ipaddress*>]

命令描述：

查看 OSPF 协议的相关配置信息。

参数说明：

show database	查看 OSPF 协议的数据库信息
asbr-summary|external |network |router |summary |max-age |self-originate	在链路状态数据库中的类型 4 LSA|在链路状态数据库中的类型 5 LSA|在链路状态数据库中的类型 2 LSA|在链路状态数据库中的类型 1 LSA|在链路状态数据库中的类型 3 LSA|在 MaxAge 链表里的 LSA|自生成链路状态
adv-router	宣告路由器
ipaddress	字符串，宣告路由器的 IP 地址，格式为 0.0.0.0

实例：

**查看数据库中的类型为 1 LSA 的 router 信息。

ospf show database router <cr>

ospf start <cr>

命令描述：

启动 OSPF 服务。

使用说明：

只有启动了 OSPF 进程，才可以设置 OSPF 协议的相关参数。

ospf stop <cr>

命令描述：

停止 OSPF 服务。

port-mirror

端口映射功能设置

filter

端口映射包过滤规则设置

port-mirror filter add name <*string*> **l2protocol** <*string*> [**l3protocol**< *number* >] [**src-ip** <*string*>] [**dst-ip** <*string*>]

命令描述：

增加一条端口映射包过滤规则。

参数说明：

add	增加一条端口映射包过滤规则
name	输入规则名
string	字符串
l2protocol	数据包使用的第二层协议类型
string |0800	输入十六进制数值或 0800。0800 表示 IP 协议。
l3protocol	数据包使用的第三层协议类型，可选项，仅当二层协议设置为 IP 协议时需要设置该项。

number	输入数值。 说明： 6 表示 TCP 协议，17 表示 UDP 协议，1 表示 ICMP 协议，2 表示 IGMP 协议；
src-ip	指定源 IP 地址，可选项，仅当二层协议设置为 IP 协议时需要设置该项。
string	IP 地址字符串
dst-ip	指定目的 IP 地址，可选项，仅当二层协议设置为 IP 协议时需要设置该项。
string	IP 地址字符串

port-mirror filter clean <cr>

命令描述：

清空所有端口映射包过滤规则。

port-mirror filter delete name <*string*>

命令描述：

删除一条端口映射包过滤规则。

参数说明：

delete	删除一条端口映射包过滤规则
name	输入规则名
string	字符串

port-mirror filter show<cr>

命令描述：

查看所有端口映射包过滤规则。

group

镜像组设置

port-mirror group add name <*string*> **dst-port** <*string*>

命令描述：

添加一组镜像。

参数说明：

add	添加一组镜像

name	输入名称
string	字符串
dst-port	目的端口网卡名称
string	字符串，如:'eth0 eth1'

port-mirror group add name <*string*> **src-port** <*string*> **direction** <in|out|both>

命令描述：

添加一组镜像。

参数说明：

add	添加一组镜像
name	输入镜像组名称
string	字符串
src-port	源端口网卡名称,如:'eth0 eth1'
string	字符串
direction	镜像方向
in|out|both	进、出、双向

network port-mirror group delete name <*string*>

命令描述：

删除一组镜像。

network port-mirror group clean<cr>

命令描述：

清空所有镜像组。

network port-mirror group show<cr>

命令描述：

查看所有镜像组。

network port-mirror group start name <*string*>

命令描述：

开启指定的镜像组。

network port-mirror group start all<cr>

命令描述：

开启所有镜像组。

network port-mirror group stop name <*string*>

命令描述：

停止指定镜像组。

network port-mirror group stop all<cr>

命令描述：

停止所有镜像组。

network port-mirror group modify name <*string*> **dst-port** <*string*>

命令描述：

修改镜像组属性。

参数说明：

modify	修改一组镜像
name	输入名称
string	字符串
dst-port	目的端口网卡名称
string	字符串，如:'eth0 eth1'

network port-mirror group modify name <*string*> [**src-port** <*string*>] [**direction** <in|out|both>]

命令描述：

修改镜像组属性。

参数说明：

modify	修改一组镜像
name	输入镜像组名称
string	字符串
src-port	源端口网卡名称,如:'eth0 eth1'
string	字符串
direction	镜像方向
in|out|both	进、出、双向

network port-mirror group connect <*string*> **to** <*string* | none>

命令描述：

镜像组连接过滤器。

参数说明：

connect	镜像组连接过滤器
string	字符串，输入镜像组名称
to	指定过滤器名，
string| none	指定过滤器名称时，将连接过滤器；如果指定参数为 none 时将断开连接。

port-statistic

网络卫士安全网关可以根据应用端口对连接中的源 IP 和目的 IP 进行流量统计，包括发送/接收报文数和建立的连接数。默认情况下，网络卫士安全网关对端口 80、8080、21、20、110、25 进行流量统计，管理员可以根据情况自行设置需要统计流量的端口。

port-statistic on <cr>

命令描述：

开启网络卫士安全网关的端口流量统计功能。

port-statistic off <cr>

命令描述：

关闭网络卫士安全网关的端口流量统计功能。

port-statistic set [**statistic**<*number*>] [**send**< *number* >][**port1** <*number*>][**port2** <*number*>] [**port3** <*number*>] [**port4** <*number*>] [**port5** <*number*>] [**port6** <*number*>]

命令描述：

设置端口流量统计相关参数。默认情况下系统只对连接中的所有 IP 在 80、8080、20、21、110、25 这 6 个固定端口上的流量进行分别统计，管理员可以根据实际情况设置对其他端口进行流量统计，但是一次只能统计 6 个端口的流量信息。

参数说明：

set	设置端口流量统计相关参数。不设置参数时全部采用默认值。
statistic	可选项，设置进行流量统计的时间间隔。默认为 1800 秒。
number	数值，范围为 300-86400。
send	可选项，设置向日志服务器发送端口流量相关日志的时间间隔。默认为 1 秒。
number	数值。
port1	重新设置统计的第一个端口号。
number	数值。
Port2	重新设置统计的第二个端口号。
number	数值。
Port3	重新设置统计的第三个端口号。
number	数值。
Port4	重新设置统计的第四个端口号。
number	数值。
Port5	重新设置统计的第五个端口号。
number	数值。
Port6	重新设置统计的第六个端口号。
number	数值。

使用说明：

网络卫士安全网关向日志服务器发送端口流量统计相关报文还需要进行相关设置：**#log log type_set add** stat。

实例：

**设置端口流量统计相关参数为默认值。

port-statistic set <cr>

port-statistic show [**ip** <*string*>] [**detail** <src|dst>]<cr>

命令描述：

查看网络卫士安全网关的端口流量统计信息。

参数说明：

show	查看端口流量统计信息。
ip	可选项，设置根据 IP 地址查看端口流量统计信息。默认全部显示。
string	IP 地址字符串。
detail	可选项，设置根据来源或目的来查看端口流量统计信息。默认全部显示。
src|dst	“src”表示查看源 IP 的端口流量信息，“dst”表示查看目的 IP 的端口流量统计信息。

实例：

**查看连接中的所有源 IP 和目的 IP 的端口流量信息。

port-statistic show <cr>

pptp

网络卫士安全网关支持 PPTP 协议，远端用户可通过 Windows 自带的拨号连接组件与安全网关通过 PPTP 服务建立连接，从而访问整个网络。安全网关提供的 PPTP 服务还需要如下配置:（1）在本模块配置 PPTP 相关属性。（2）在 authentication -localdb 命令中添加类型为 vpn 的远程用户；并添加 basic 服务器。（3）在提供服务的接口开放 PPTP 服务（4）在访问控制规则处定义针对于远程用户的访问控制规则。（5）对 PPTP 客户端进行连接参数设置。

pptp clean ip-pool<cr>

命令描述：

清空 PPTP 的 IP 地址池设置。地址池是指由一个起始 IP 地址和一个终止 IP 地址组成的 IP 地址范围，当客户端使用 PPTP 服务与安全网关的某一物理接口建立连接时，安全网关将为客户端动态分配该地址池中的一个地址作为用户的 IP 地址。

参数说明：

clean	清空 PPTP 的 IP 地址池设置
ip-pool	IP 地址池

pptp restart <cr>

命令描述：

重新启动 PPTP 服务。如果 PPTP 服务已经启动，则修改配置参数后需要重新启动该服务才能使修改后的配置生效。

pptp set cipher< on|off**>**

命令描述：

设置通信是否加密

参数说明：

set cipher	设置通信是否加密
on|off	是/否

pptp set ip-pool local <*ipaddress1*> **min_ip** <*ipaddress2*> **max_ip** <*ipaddress3*>

命令描述：

设置 PPTP 服务的本地虚拟 IP 地址和客户端地址池属性。本地虚拟 IP 地址为安全网关内部使用，和地址池必须设置在同一个网段。PPTP 客户端与安全网关连接成功后可以查看到本地虚拟 IP 地址和为客户端分配的 IP 地址。

参数说明：

set ip-pool	设置 PPTP 服务的地址池属性
local	设置 PPTP 服务的虚拟本地 IP 地址，当 PPTP 客户端与安全网关建立连接时客户端将与此处设定的虚拟 IP 地址进行通信。
ipaddress1	IP 地址字符串。
min_ip	设置地址池的起始地址
ipaddress2	IP 地址字符串
max_ip	设置地址池的终止地址
ipaddress3	IP 地址字符串，应大于或等于起始 IP 地址。

实例：

**设置安全网关的本地虚拟 IP 地址为 172.16.100.1 ，地址池为 172.16.200.101 到 172.16.200.200。

pptp set ip-pool local *172.16.100.1* **min_ip** *172.16.200.101* **max_ip** *172.16.200.200*。

pptp set port<*number*>

命令描述：

设置安全网关提供 PPTP 服务的端口号，默认端口号为 1723。

参数说明：

set port	设置安全网关提供 PPTP 服务的端口号
number	端口号，默认为 1723。

实例：

**设置 PPTP 服务的端口号为 1725。

pptp set port *1725*<cr>

pptp show <running | status>

命令描述：

查看 PPTP 的配置信息和运行状态信息。

参数说明：

show	查看 PPTP 的配置信息和运行状态信息
running | status	运行配置|链路状态

实例：

**查看 PPTP 的运行配置信息：端口设置和地址池等。

pptp show running<cr>

**查看 PPTP 的当前链路状态：链路数和链路 IP 地址信息。

pptp show status<cr>

pptp start <cr>

命令描述：

启动 PPTP 服务。

pptp stop <cr>

命令描述：

停止 PPTP 服务。

rangstatistic

设置对地址范围对象进行流量统计的功能。

rangstatistic set name< *string* >

命令描述：

添加范围地址对象到流量统计地址对象列表中，设置对地址对象的流量统计功能。

参数说明：

set	添加范围类地址对象作为流量统计对象
name	设置统计对象名称
string	字符串，应当是已经添加的范围地址对象的名称。

使用说明：

1) 如果设置的地址对象不是已经定义的范围地址对象，则命令执行会提示错误信息。

2）查看已经定义的范围地址对象信息在 define 组件下的 range 命令下查看。

rangstatistic clean [**name**< *string* >]

命令描述：

从统计列表中删除某范围地址对象，从而停止对该范围地址对象的流量统计功能。

参数说明：

clean	从统计列表中删除范围地址对象
name	可选项，指定统计对象名称，不指定时从统计列表中删除所有范围类地址统计对象。
string	字符串，应当是从统计列表中已经添加的范围对象的名称。

使用说明：

1) 如果设置的地址对象不是已经定义的范围地址对象，则命令执行会提示错误信息。

2）不指定任何参数时将已添加的所有范围地址对象从统计列表中删除。

rangstatistic show < cr >

命令描述：

查看对范围地址对象的流量统计结果。

使用说明：

如果没有设置对地址对象的流量统计功能，则显示结果没有任何信息。

reset

将接口的所有属性恢复出厂配置：包括接口的 MSS 值、MTU 值、接口的工作速率和协商模式等基本属性，以及接口所绑定的属性、接口描述信息、工作模式（路由/交换）、IP 地址和 MAC 地址、接口 OSPF 路由协议属性设置、接口 RIP 路由协议属性设置等。所有的 VLAN 和 VLAN 转换组设置也都恢复出厂配置。

reset <cr>

命令描述：

清除网络接口的所有配置信息。

rip

RIP 路由协议配置。RIP（Routing Information Protocol），路由信息协议，是推出时间最长的路由协议，也是最简单的路由协议。RIP 通过广播或多播 UDP 报文来交换路由信息，每 30 秒发送一次路由信息更新，同时根据收到的 RIP 报文更新自己的路由表。RIP 提供跳跃计数(hop count)作为尺度来衡量路由距离，跳跃计数是一个包到达目标所必须经过的路由器的数目。网络卫士安全网关支持 RIP 的 v1、v2 版本。

注意：

1）设置安全网关的 IP 地址时一定要将该 IP 的 label 设置为 0，方可利用该 IP 地址启动 RIP 服务。

2）安全网关上的配置完成后，一定要重新启动接口一次。

rip no access-list <*string1*> <permits|deny> <*string2*>

命令描述：

取消 RIP 访问控制规则的设置。

参数说明：

no	取消 RIP 某些参数的设置
access-list	取消设置 RIP 访问控制规则

string1	字符串，设定规则名。
permits|deny	指定允许或禁止运行 RIP 协议
string2	设定 RIP 协议运行网段，格式为 x.x.x.x/x

使用说明：

只有启动了 RIP 进程，才可以取消设置 RIP 协议的相关参数。

实例：

**取消设置 RIP 访问控制规则，名称为 ww，内容为禁止网段 10.10.10.0/24 运行 RIP 协议。

rip no access-list *ww* **deny** *10.10.10.0/24*<cr>

rip no debug <event|packet>

命令描述：

取消 RIP 协议对事件或数据报文的调试功能。

参数说明：

no	取消 RIP 某些参数的设置
debug	设置 RIP 协议的调试功能
event | packet	取消对事件|数据报文的调试功能

使用说明：

只有启动了 RIP 进程，才可以取消设置 RIP 协议的相关参数。

实例：

**取消 RIP 协议对事件的调试功能。

rip no debug event <cr>

rip no default-metric <*number*>

命令描述：

删除 RIP 协议的默认 metric 值设置功能。表示默认引入路由的跳数。在引入路由时，如果不分别指定各类型路由的 metric 参数，则使用默认路径开销作为路由引入后的跳数。

参数说明：

no	取消 RIP 某些参数的设置
default-metric	取消默认 metric 值设置
number1	数值

使用说明：

只有启动了 RIP 进程，才可以取消设置 RIP 协议的相关参数。

实例：

**取消 RIP 协议对默认 metric 值设置。

ripno default-metric *2*<cr>

rip no distribute-list <*string1*> **<in|out>** < *string2*>

命令描述：

删除 RIP 协议分发某些参数的设置。

参数说明：

no	删除 RIP 某些参数的设置
distribute-list	删除已定义的路由分发规则
string1	指定规则名
in |out	控制方向：该接口接收的路由信息| 由该接口发送的路由信息
string2	接口名称字符串

使用说明：

只有启动了 RIP 进程，才可以取消设置 RIP 协议的相关参数。

实例：

**删除 RIP 协议在 eth0 口定义的路由分发规则 ww。

rip no distribute-list *ww* **in** *eth0*<cr>

此规则如果未定义，则会提示：

distribute list doesn't exist

rip no neighbor<*ipadddress*>

命令描述：

删除指定地址的邻居。

参数说明：

no	删除 RIP 某些参数的设置
neighbor	删除指定 IP 地址的邻居
ipadddress	IP 地址字符串

使用说明：

只有启动了 RIP 进程，才可以取消设置 RIP 协议的相关参数。

实例：

**删除 IP 地址为 10.10.10.2 的邻居。

ripno neighbor *10.10.10.2*<cr>

rip no network<*string*>

命令描述：

取消在某网段运行 RIP 协议。

参数说明：

no	取消 RIP 某些参数的设置
network	取消在某网段运行 RIP 协议
string	设定子网地址及子网掩码，格式为 x.x.x.x/x

使用说明：

只有启动了 RIP 进程，才可以取消设置 RIP 协议的相关参数。

实例：

**取消在网段 10.10.10.0/24 运行 RIP 协议。

rip no network *10.10.10.0/24*<cr>

rip no passive-interface <*string*>

命令描述：

取消在某接口抑制路由更新。表示在此接口上，如果没有指定邻居，则这个接口不发送路由更新信息。

参数说明：

no	取消 RIP 某些参数的设置
passive-interface	取消在某接口抑制路由更新
string	接口名称字符串

使用说明：

只有启动了 RIP 进程，才可以取消设置 RIP 协议的相关参数。

实例：

**取消接口 eth0 抑制路由更新。

rip no passive-interface *eth0*<cr>

rip no redistribute < connected|ospf|static > [**metric** <*number*>]

命令描述：

取消某种路由的重发布。即取消引入静态/直连/OSPF 的路由信息到 RIP 路由协议中。

参数说明：

no	取消 RIP 某些参数的设置
redistribute	取消某种路由的重发布
connected|ospf|static	直连路由/OSPF 路由/静态路由
metric	可选项，取消该种路由的 metric 值设置
number	数值

使用说明：

只有启动了 RIP 进程，才可以取消设置 RIP 协议的相关参数。

实例：

**取消静态路由的重发布。

rip no redistribute static <cr>

rip no timer basic <*number1*> <*number2*><*number3*>

命令描述：

删除定时器设置。在 RIP 中为了支持寻路操作使用了三个不同的定时器：更新定时器、超时定时器和回收定时器。

a）更新定时器：指更新路由信息的时间间隔。此定时器默认情况下设置为 30 秒，即每隔 30 秒就会向相邻的路由器广播发送路由表的内容。

b）超时定时器：指收到通往目的主机 RIP 路由信息的最长时间，默认值为 180 秒。路由器只要收到通往特定主机的路由，就对通往该主机的超时定时器初始化，如果在 180 秒内没有接收到包含该路由的 RIP 消息，该路由的度量值（即“跳数”，metric）就被设置为 16（RIP 协议支持的最大有效度量值为 15，当一条路由的度量值达到 16 后，就表示此条路由无效，并且认为对应的目的地不可达。）。

c）回收定时器：默认值为 120 秒。当超时定时器超时后，此时启动回收定时器；

当这条路由回收定时器超时，该路由将被从路由表中删除。

参数说明：

no	取消 RIP 某些参数的设置
timer basic	取消定时器设置
number1	取消更新定时器的时间间隔，恢复默认设置
number2	取消超时定时器的时间间隔，恢复默认设置
number3	取消回收定时器的时间间隔，恢复默认设置

使用说明：

只有启动了 RIP 进程，才可以取消设置 RIP 协议的相关参数。

实例：

**取消 RIP 协议的定时器设置。

rip no timer basic *50 160 100*<cr>

rip no version <1|2>

命令描述：

设置路由协议的版本。

参数说明：

no	取消 RIP 某些参数的设置
version	取消 RIP 路由协议的版本设置
1|2	RIPv1 版本/RIPv2 版本

使用说明：

只有启动了 RIP 进程，才可以设置 RIP 协议的相关参数。

实例：

**取消设置 RIP 路由协议版本为 1

rip no version 1<cr>

rip access-list<*string1*> <**permits|deny**><*string2*>

命令描述：

设置 RIP 访问控制规则：即设定在哪个网段允许运行 RIP 协议，哪个网段禁止运行 RIP 协议。

参数说明：

access-list	设置 RIP 访问控制规则

string1	字符串，设定规则名。
permits|deny	指定允许或禁止运行 RIP 协议
string2	设定 RIP 协议运行网段，格式为 x.x.x.x/x

使用说明：

只有启动了 RIP 进程，才可以设置 RIP 协议的相关参数。

实例：

**设置 RIP 访问控制规则，名称为 ww，内容为禁止网段 10.10.10.0/24 运行 RIP 协议。

rip access-list *ww* deny *10.10.10.0/24*<cr>

rip debug <events|packet>

命令描述：

设置 RIP 协议对事件或数据报文的调试功能。

参数说明：

debug	设置 RIP 协议的调试功能
event | packet	对事件|数据报文的调试功能

使用说明：

只有启动了 RIP 进程，才可以设置 RIP 协议的相关参数。

实例：

**设置 RIP 协议对事件的调试功能。

rip debug event <cr>

rip default-metric <*number*>

命令描述：

设置 RIP 协议的默认 metric 值。表示默认引入路由的跳数。在引入路由时，如果不分别指定各类型路由的 metric 参数，则使用默认路径开销作为路由引入后的跳数。

参数说明：

default-metric	设置 RIP 协议的默认 metric 值
number	数值

使用说明：

只有启动了 RIP 进程，才可以设置 RIP 协议的相关参数。

实例：

** 设置 RIP 协议对默认 metric 值。

rip default-metric *2*<cr>

rip distribute-list <*string1*> **<in|out>** < *string2*>

命令描述：

设置 RIP 协议的路由分发规则。

参数说明：

distribute-list	设置 RIP 协议路由分发规则
string1	指定规则名
in |out	控制方向：该接口接收的路由信息| 由该接口发送的路由信息
string2	接口名称字符串

使用说明：

只有启动了 RIP 进程，才可以设置 RIP 协议的相关参数。

实例：

** RIP 协议在 eth0 口定义路由分发规则 ww。

rip distribute-list *ww* **in** *eth0*<cr>

rip neighbor<*ipadddress*>

命令描述：

指定 RIP 协议的邻居地址。

参数说明：

neighbor	指定邻居的 IP 地址
ipadddress	IP 地址字符串

使用说明：

只有启动了 RIP 进程，才可以设置 RIP 协议的相关参数。

实例：

**设置 IP 地址为 10.10.10.2 的邻居。

rip neighbor *10.10.10.2*<cr>

rip network<*string*>

命令描述：

设置在哪个网段运行 RIP 协议。

参数说明：

network	设置在哪个网段运行 RIP 协议
string	设定子网地址及子网掩码，格式为 x.x.x.x/x

使用说明：

只有启动了 RIP 进程，才可以设置 RIP 协议的相关参数。

实例：

**设置在网段 10.10.10.0/24 运行 RIP 协议。

rip network *10.10.10.0/24*<cr>

rip passive-interface <*string*>

命令描述：

设置在某接口抑制路由更新。表示在此接口上，如果没有指定邻居，则这个接口不发送路由更新信息。

参数说明：

passive-interface	设置在某接口抑制路由更新
string	接口名称字符串

使用说明：

只有启动了 RIP 进程，才可以设置 RIP 协议的相关参数。

实例：

**设置在接口 eth0 抑制路由更新。

rip passive-interface *eth0*<cr>

rip redistribute <connected|ospf|static> [**metric** <*number*>]

命令描述：

设置某种路由的重发布。即引入哪种路由：静态/直连/OSPF 的路由信息到 RIP 路由协议中，以及引入时的 Metric 值。

参数说明：

redistribute	设置某种路由的重发布
connected|ospf|static	直连路由/OSPF 路由/静态路由

metric	可选项，设置该种路由的 metric 值
number	数值

使用说明：

只有启动了 RIP 进程，才可以设置 RIP 协议的相关参数。

实例：

**设置静态路由的重发布，并设 metric 值为 6。

rip redistribute static **metric** *6*<cr>

rip timer basic <*number1*> <*number2*><*number3*>

命令描述：

设置 RIP 协议的定时器。在 RIP 中为了支持寻路操作使用了三个不同的定时器：更新定时器、超时定时器和回收定时器。

a）更新定时器：指更新路由信息的时间间隔。此定时器默认情况下设置为 30 秒，即每隔 30 秒就会向相邻的路由器广播发送路由表的内容。

b）超时定时器：指收到通往目的主机 RIP 路由信息的最长时间，默认值为 180 秒。路由器只要收到通往特定主机的路由，就对通往该主机的超时定时器初始化，如果在 180 秒内没有接收到包含该路由的 RIP 消息，该路由的度量值（即“跳数”，metric）就被设置为 16（RIP 协议支持的最大有效度量值为 15，当一条路由的度量值达到 16 后，就表示此条路由无效，并且认为对应的目的地不可达。）。

c）回收定时器：默认值为 120 秒。当超时定时器超时后，此时启动回收定时器；当这条路由回收定时器超时，该路由将被从路由表中删除。

参数说明：

timer basic	设置定时器的时间间隔
number1	设置更新定时器的时间间隔
number2	设置超时定时器的时间间隔
number3	设置回收定时器的时间间隔

使用说明：

只有启动了 RIP 进程，才可以设置 RIP 协议的相关参数。

实例：

**设置 RIP 协议的定时器的时间间隔：更新定时器 50 秒，超时定时器 160 秒，回收定时器 100 秒。

rip timer basic *50 160 100*<cr>

rip version <1|2>

命令描述：

RIP 路由协议的版本设置

参数说明：

version	设置 RIP 路由协议的版本
1|2	RIPv1 版本/RIPv2 版本

使用说明：

只有启动了 RIP 进程，才可以设置 RIP 协议的相关参数。

实例：

**设置 RIP 路由协议版本为 1

rip version 1<cr>

rip show [status|debugging|running]

命令描述：

查看 RIP 协议的相关配置信息。

参数说明：

show	查看 RIP 协议的相关配置信息
status|debugging |running	可选项，状态信息|调试信息|运行信息。不指定参数时显示所有信息。

使用说明：

只有启动了 RIP 进程，才可以设置 RIP 协议的相关参数。

实例：

**查看所有配置信息。

rip show<cr>

**查看 RIP 协议的状态信息

rip show status<cr>

rip start <cr>

命令描述：

启动 RIP 服务。

rip stop <cr>

命令描述：

停止 RIP 服务。

route

安全网关路由配置。

网络卫士安全网关内部维护了一张静态路由表，由用户定义的静态路由和策略路由组成。安全网关的静态路由表只根据目的地址来进行路由，而策略路由可以目的地址、目的端口、源地址、源端口、协议进行路由。网络卫士安全网关的策略路由方式可以实现内部网络的指定对象使用特定外部线路与外部网络通信，从而进一步增强了网络的通信安全。策略路由优先于静态路由。

route add dst <*string1*> **gw** <*gwaddress*> **dev** <*string3*> [**metric** <*number1*>] [**weight** <*number1*>] [**id** <*number2*>] [**type** <static|dhcp|ipsec>] [**probeid** <*number2*>] [**attribute** <adsl|adsl1|adsl2|adsl3>]

命令描述：

添加一条静态路由。

参数说明：

add	添加一条静态路由。
dst	设定目标地址/掩码。
string1	格式为 x.x.x.x/x 的字符串，表示目标地址/掩码。
gw	设定网关地址
gwaddress	格式为 x.x.x.x 的字符串，表示网关 IP 地址。
metric	可选项，指定路由度量值，metric 值越小，路由优先级越高。默认为 1。
number1	数字字符串，默认为 1，取值范围为 1-65535。
Weight	可选项，指定路由权重值。 说明： 1）权重值越大，静态路由的优先级越高。 2）如果静态路由表中存在多个“度量值”相同的下一跳，

	则根据权重值做权重负载均衡，选择下一跳；如果权重值也相等，则采取轮询方式选择下一跳，即依次通过各条路径发送，从而实现网络的负载分担。
number1	默认为 1，取值范围为 1-128。
dev	必选项，指定转发接口。包括物理接口、虚接口和子接口。
string3	字符串，如 eth0
id	可选项，指定路由的 id 号,建议不要指定。
number2	数值，范围为 100-899，不能与已有策略 ID 相冲突。
type	可选项，指定路由的类型（static|dhcp|ipsec）
static|dhcp|ipsec	默认为 static，如果使用 dhcp，该路由不保存。
probeid	选择已经设置的探测链路的 ID 号。 说明： 如果选择的链路状态显示为“链路不可达”，则新添加的静态路由的“标记”一栏不显示“U”，表示该条路由不可用。
number	数值，必须是已经设置的探测链路的 ID 号。范围为 100-104。
attribute	指定出接口的属性
string	选择 ADSL 属性 adsl、adsl1、adsl2 或 adsl3。

实例：

** 添加一条静态路由

#route add dst *192.168.83.0/24* **gw** *192.168.83.1* **metric** *1* **type** static **dev** *eth0*

route delete dst <*string1*> **gw** <*gwaddress*> **dev** <*string3*> [**metric** <*number1*>]

[**weight**<*number1*>] [**id** <*number2*>] [**type** <static|dhcp|ipsec>] [**probeid** <*number2*>]

[**attribute** <adsl|adsl1|adsl2|adsl3>]

命令描述：

删除一条静态路由。

参数说明：

add	删除一条静态或策略路由。
dst	设定目标地址/掩码。
string1	格式为 x.x.x.x/x 的字符串，表示目标地址/掩码。
gw	设定网关地址
gwaddress	格式为 x.x.x.x 的字符串，表示网关 IP 地址。
metric	可选项，指定路由度量值，metric 值越小，路由优先级越高。默认为 1。
number1	数字字符串，默认为 1，取值范围为 1-65535。
Weight	可选项，指定路由权重值。 说明： 1）权重值越大，静态路由的优先级越高。 2）如果静态路由表中存在多个“度量值”相同的下一跳，则根据权重值做权重负载均衡，选择下一跳；如果权重值也相等，则采取轮询方式选择下一跳，即依次通过各条路径发

	送，从而实现网络的负载分担。
number1	默认为 1，取值范围为 1-128。
dev	必选项，指定转发接口。包括物理接口、虚接口和子接口。
string3	字符串，如 eth0
id	可选项，指定路由的 id 号,建议不要指定。
number2	数值，范围为 100-899，不能与已有策略 ID 相冲突。
type	可选项，指定路由的类型（static|dhcp|ipsec）
static|dhcp|ipsec	默认为 static，如果使用 dhcp，该路由不保存。
probeid	选择已经设置的探测链路的 ID 号。 说明： 如果选择的链路状态显示为“链路不可达”，则新添加的静态路由的“标记”一栏不显示“U”，表示该条路由不可用。
number	数值，必须是已经设置的探测链路的 ID 号。范围为 100-104。
attribute	指定出接口的属性
string	选择 ADSL 属性 adsl、adsl1、adsl2 或 adsl3。

route intelligent-opt <on|off>

命令描述：

开启或关闭路由智能选路功能。

参数说明：

intelligent-opt	开启或关闭路由智能选路功能
on|off	开启/关闭

route delete id <*number*>

命令描述：

根据路由 ID 号删除一条静态路由。

参数说明：

delete	删除一条静态路由
id	要删除的路由表项的 ID
number	数值，100-899

使用说明：

无。

实例：

**删除一条 ID 为 100 的策略路由。

route delete id *100*

route ip-probe <on|off>

命令描述：

设置是否开启“路由 IP 探测”功能。如果在静态路由中引用了某 IP 探测的“ID 号”，那么只有开启“路由 IP 探测”后，静态路由模块才根据 IP 探测的结果作为路由是否可用的依据。

参数说明：

ip-probe	开启或关闭路由 IP 探测功能
on|off	开启/关闭

route clean <cr>

命令描述：

清除全部静态路由。

route show [**dst** <*string1*>] [**dev**<*string2*>] [**vsid** <*number*>]

命令描述：

显示路由配置信息（不指定任何参数时显示所有的路由配置信息）。

参数说明：

show	显示所有或指定的路由配置信息。
dst	可选项，根据路由的目的地址查看路由表
string1	标准 IP 地址字符串
dev	可选项，指定接口名，包括物理接口、虚接口和子接口。
string2	字符串
vsid	可选项，指定欲查看哪个虚系统 ID 的路由表项，无须指定其他参数。
number	数值

实例：

**显示虚系统 ID 为 1 的路由配置信息。

route show vsid *1*

route-policy

策略路由不仅能够根据目的地址，而且能够根据协议类型、应用、IP 源地址或者其它的条件（源端口、目的端口等）来确定报文的转发路径。策略路由的优先级

高于普通路由。

route-policy add name <*string*>

命令描述：

添加一条空的策略路由。

参数说明：

add	添加一条空的策略路由
name	设定路由名称
string	字符串。不得与已有策略路由名相同，而且不得超过 31 个字符。

使用说明：

添加策略路由的条目之前一定要先添加好策略路由。

route-policy add-entry name <*string*> **src** <*string*>[**sport** <*number*>][**sport2** <*number*>] **dst** <*string1*>[**dport** <*number*>][**dport2** <*number*>]**protocol** <*string*> **gw** <*gwaddress*> **dev** <*string*> [**metric** <*number*>][**weight**<*number*>]

命令描述：

添加一条策略路由条目。

参数说明：

add-entry	添加一条策略路由条目
name	指定策略路由名称
string	字符串，必须是已经添加的策略路由名。
src	设定源地址/掩码。
string	格式为 x.x.x.x/x 的字符串，表示源地址/掩码。
sport	可选项，标识数据包的源端口的起始端口，如果为单个端口，则只填写起始端口即可。
number	数值
sport2	可选项，标识数据包的源端口的结束端口，如果为单个端口，可以不必填写该项，也可以填写与起始端口相同的端口号。
number	数值，应大于等于 sport 设定的端口号。
dst	用来标识 IP 包的目的地址或目的网络。需要填写目的地址转换后的真实地址。
string	格式为 x.x.x.x/x 的字符串，表示目标地址/掩码。
dport	可选项，标识数据包的目的端口的起始端口，如果为单个端口，则只填写起始端口即可。
number	数值，范围为 0－65535。
dport2	可选项，标识数据包的目的端口的结束端口，如果为单个端口，可以不必填写该项，也可以填写与起始端口相同的端口号。
number	数值，范围为 0－65535。应大于等于 dport 设定的端口号。
protocol	可选项，设置数据包使用的协议。

string	为 0－255 的数值或 TCP、UCP、ICMP 等协议名称。
gw	设定网关地址
gwaddress	格式为 x.x.x.x 的字符串，表示网关 IP 地址。
dev	必选项，指定转发接口。包括物理接口、虚接口和子接口。
string3	字符串，如 eth0
metric	可选项，指定路由度量值，metric 值越小，路由优先级越高。默认为 1。
number1	数字字符串，如 1，2
weight	设置该策略路由的权重值。 说明： 如果策略路由表中存在多个“度量值”相同的下一跳，则根据权重值做权重负载均衡，选择下一跳；如果权重值也相等，则采取轮询方式选择下一跳，即依次通过各条路径发送，从而实现网络的负载分担。
number1	默认为 1，取值范围为 1-65535。

实例：

** 添加一条策略路由条目

#route add-entry name *gg* **dev** *eth0* **src** *192.168.0.0/16* **dst** *192.168.83.0/24***gw** *192.168.83.1* **metric** *1*

route-policy clean <cr>

命令描述：

清空策略路由。

route-policy clean-entry name <*string*>

命令描述：

清空一条策略路由中的所有路由条目。

参数说明：

clean-entry	清空一条策略路由中的所有路由条目
name	指定策略路由名称
string	字符串，为已有策略路由名。

route-policy delete name <*string*>

命令描述：

删除一条策略路由。

参数说明：

delete	删除一条策略路由
name	指定策略路由名称
string	字符串，为已有策略路由名。

route-policy delete-entry name <*string*> [**src** <*string*>][**sport** <*number*>][**sport2** <*number*>] **dst** <*string1*>[**dport** <*number*>][**dport2** <*number*>]**protocol** <*string*> **gw** <*gwaddress*> **dev** <*string*> [**metric** <*number*>][**weight**<*number*>]

命令描述：

删除一条策略路由中的某一个路由条目。

参数说明：

delete-entry	清空一条策略路由中的某一个路由条目
name	指定策略路由名称
string	字符串，必须是已经添加的策略路由名。
src	设定源地址/掩码。
string	格式为 x.x.x.x/x 的字符串，表示源地址/掩码。
sport	可选项，标识数据包的源端口的起始端口，如果为单个端口，则只填写起始端口即可。
number	数值
sport2	可选项，标识数据包的源端口的结束端口，如果为单个端口，可以不必填写该项，也可以填写与起始端口相同的端口号。
number	数值，应大于等于 sport 设定的端口号。
dst	用来标识 IP 包的目的地址或目的网络。需要填写目的地址转换后的真实地址。
string	格式为 x.x.x.x/x 的字符串，表示目标地址/掩码。
dport	可选项，标识数据包的目的端口的起始端口，如果为单个端口，则只填写起始端口即可。
number	数值，范围为 0－65535。
dport2	可选项，标识数据包的目的端口的结束端口，如果为单个端口，可以不必填写该项，也可以填写与起始端口相同的端口号。
number	数值，范围为 0－65535。应大于等于 dport 设定的端口号。
protocol	可选项，设置数据包使用的协议。
string	为 0－255 的数值或 TCP、UCP、ICMP 等协议名称。
gw	设定网关地址
gwaddress	格式为 x.x.x.x 的字符串，表示网关 IP 地址。
dev	必选项，指定转发接口。包括物理接口、虚接口和子接口。
string3	字符串，如 eth0
metric	可选项，指定路由度量值，metric 值越小，路由优先级越高。默认为 1。
number1	数字字符串，如 1，2
weight	设置该策略路由的权重值。 说明： 如果策略路由表中存在多个“度量值”相同的下一跳，则根据权重值做权重负载均衡，选择下一跳；如果权重值也相等，则采取轮询方式选择下一跳，即依次通过各条路径发送，从

	而实现网络的负载分担。
number1	默认为 1，取值范围为 1-65535。

route-policy delete-entry id <*number*>

命令描述：

根据 ID 删除一条策略路由条目。

参数说明：

delete-entry	根据 ID 删除一条策略路由条目
id	需要删除的路由备份条目的 ID
number	数值

实例：

**删除一条 ID 为 10 的路由备份条目。

route-policy delete-entry id *10*

route-policy global-bind set <*string*>

命令描述：

将一个定义好的策略路由指定为全局的策略路由，任何接口收到的数据包都会查找全局的策略路由。全局的策略路由只能指定一个，后面的设置会覆盖前面的设置。如果指定的策略路由不存在则返回不存在的错误。

参数说明：

global-bind	将策略路由设置为全局策略路由
set	设置策略路由名称
string	字符串，已添加的策略路由名称。

实例：

**将名称为 gg 的策略路由设置为全局策略路由。

route-policy global-bind set *gg*

route-policy global-unbind <cr>

命令描述：

清除绑定好的全局策略路由，将全局策略路由的绑定属性置为空。因为只能有一个策略路由被指定为全局的策略路由，所以不需要指定策略路由的名称。如果全局的策略路由已经为空，再次执行清除的命令不会返回错误。

route-policy global-show <cr>

命令描述：

显示当前已经绑定好的全局策略路由和路由条目，如果当前没有绑定任何的全局策略路由则显示为空。

route-policy name <*string*>**bindclean** <cr>

命令描述：

清除策略路由的全部绑定。

route-policy name <*string*>**show**<cr>

命令描述：

查看指定策略路由及其路由条目。

route-policy move name <*string*> **id** <*number*> **<before** <*number*>**|after** <*number*>**>** **]**

命令描述：

移动策略路由条目。由于策略路由执行顺序匹配原则，即策略的顺序与策略的逻辑相关，用户应该根据网络实际情况及时调整策略路由的位置进而改变路由的执行顺序。

参数说明：

move	移动策略路由条目
name	指定策略路由名称。
string	字符串。
id	指定待移动的策略路由条目的 ID 号。
number	数值。
before	移动到某条目之前。
number	策略路由条目 ID 号
after	移动到某条目之后。
number	策略路由条目 ID 号

实例：

**移动策略路由 gg 中 ID 为 101 的路由条目到 103 之后。

route-policy move name *gg* **id** *101* **after** *103*

session

连接设置。

session count<on|off>

命令描述：

设置是否开启连接计数统计开关

参数说明：

count	设置是否开启连接计数统计开关
on|off	开启/关闭。

session count interval <*number*>

命令描述：

设置连接计数统计时间间隔

参数说明：

count	设置连接计数统计参数
interval	时间间隔
number	数值，范围为 2－30 秒，默认为 5 秒。

session icmp-redirect<on|off>

命令描述：

设定是否允许设备发送 ICMP 重定向报文。

参数说明：

icmp-redirect	设定是否允许设备发送 ICMP 重定向报文。
on|off	设定是否发送 ICMP 重定向报文，默认不允许发送。

使用说明：

有些单臂路由的环境中，通信对于安全网关会有不对称的情况，可以发送 ICMP 重定向报文来使主机间能正常通信。发送 ICMP 重定向的条件：

1、 配置允许发送，默认不允许发送。

2、 外出接口与入接口相同。下一跳（注意不是目的）地址与源在该接口的同一网段上。

实例：

** 设置允许安全网关设备发送 ICMP 重定向报文

session icmp- redirect on

session log-op default<cr>

命令描述：

将所有日志相关设置设为系统默认值。

session log-op create<on|off>

命令描述：

设置是否发送连接创建操作日志，默认不发送。

参数说明：

log-op	日志相关设置
create	设置是否发送连接创建操作日志
on|off	是/否

session log-op delete<on|off>

命令描述：

设置是否发送连接删除操作日志，默认发送。

参数说明：

log-op	日志相关设置
create	设置是否发送连接删除操作日志
on|off	是/否

session log-op statistics<on|off>

命令描述：

设置是否发送连接流量统计操作日志，默认不发送。

参数说明：

log-op	日志相关设置
statistics	设置是否发送连接流量统计操作日志
on|off	是/否

session never-expire <*number*|**default**|**show**>

命令描述：

不超时最大百分比设置。

参数说明：

never-expire	设置不超时最大百分比，默认为 20%。
number	数值，范围为 5-90。
default	设定为默认超时值。
show	查看设置

实例：

**设定不超时最大百分比为默认值 20%。

session never-expire default

**设定不超时最大百分比为 40%。

session never-expire *40*

**查看不超时最大百分比设置。

session never-expire show

session packet-checksum <on|off >

命令描述：

设定是否对数据报文的完整性进行验证。

参数说明：

packet-checksum	设定是否对数据报文的完整性进行验证。
on|off	是/否。

实例：

**设定对数据报文的完整性进行验证。

session packet-checksum on

session protocol <**add** <*number*>|**default**>

命令描述：

设置允许对哪些非默认协议建立连接。

参数说明：

protocol	设置允许对哪些非默认协议建立连接。
add	对相应的连接协议建立连接。
number	设定协议号，范围为 0-255。
default	设定为默认设置，即只对 TCP、UDP、ICMP、GRE 的报文建立连接。

使用说明：

1）网络卫士安全网关默认情况下只支持对协议 TCP、UDP、ICMP 和 GRE 建立

连接，当用户需要支持更多的 IP 协议时，则需要在此设置。

2）查看协议类型对应数值使用如下命令：**#define service show** default

实例：

** 对 IP 协议建议连接。

session protocol add *21*

** 设置只允许默认协议建立连接。

session protocol default

session quota default<cr>

命令描述：

设定 TCP 连接、UDP 连接以及其他类型协议的连接信息占总连接的百分比上限值为默认值 0。

session quota other<*number*>

命令描述：

设定其他类型协议的连接信息占总连接的百分比上限值，默认为 0。输入范围为 0－99。

参数说明：

quota	连接个数占总连接的百分比限额设置
other	设定其他类型协议的连接信息占总连接的百分比上限值
number	数值，范围为 0-99。

session quota tcp<*number*>

命令描述：

设定 TCP 协议的连接信息占总连接的百分比上限值，默认为 0。输入范围为 0－99。

参数说明：

quota	连接个数占总连接的百分比限额设置
tcp	设定 TCP 协议的连接信息占总连接的百分比上限值
number	数值，范围为 0-99。

session quota udp<*number*>

命令描述：

设定 UDP 协议的连接信息占总连接的百分比上限值，默认为 0。输入范围为 0－99。

参数说明：

quota	连接个数占总连接的百分比限额设置
other	设定 UDP 协议的连接信息占总连接的百分比上限值
number	数值，范围为 0-99。

session quota show<cr>

命令描述：

查看连接个数占总连接的百分比限额设置

session search [**daddr** <*string*>] [**dport** <*number*>] [**flags** <on|off>] [**from** <*number*>] [**num** <*number*>] [**protocol** <*number*| tcp|udp|icmp>] [**saddr** <*string*>] [**sport** <*number*>] [**vsid** <*number*>]

命令描述：

查看 IP 连接信息。

参数说明：

search	查看 IP 连接信息
daddr	可选项，根据连接中的目的 IP 地址查看
string	IP 地址字符串
dport	可选项，根据目的端口查看
number	数值，范围为 1－65535。
flags	可选项，是否显示内部标志，默认不显示
on|off	是/否
from	可选项，从第几个连接开始显示，默认从第一个连接开始显示
number	数值
num	可选项，需要显示的连接数目，最大 8000，默认 20
number	数值，最大为 8000
protocol	可选项，设置协议类型
number	数值，范围为 1-255。
tcp|udp|icmp	选择协议类型
saddr	可选项，源 IP 地址
string	IP 地址字符串
sport	可选项，源端口
number	数值，范围为 1－65535。
vsid	可选项，虚系统号
number	数值，范围为 0－254。

session session-integrity <on|off >

命令描述：

状态检测开关设置。默认开启状态检测功能，即 TOS 跟踪 TCP 连接的状态，对于 TCP 来说必须通过完整的三次握手，结束的时候完成四次结束握手或者收到 RST 数据包才行。对于 ICMP 的 echo 请求，必须是先收到 request 才会建立连接。在特殊情况下，对于某种 TCP 连接，如果建立的时候并没有经过安全网关，连接建立以后需要经过安全网关，则需要关闭状态检测开关，否则安全网关中因为没有相应的连接不会放行。

参数说明：

session-integrity	设定是否打开连接完整性的检测
on|off	开启/关闭。

实例：

**设定不进行状态检测

session session-integrity off

session show configuration <cr>

命令描述：

查看连接配置信息。

参数说明：

show	查看连接配置信息
configuration	连接配置信息

实例：

**查看连接配置信息

session show configuration<cr>

session show count<cr>

命令描述：

输出当前在线 session 数的前 5 名信息、最近 n 秒创建 session 数的前 5 名信息和历史创建 session 数的前 5 名信息。如果不足 5 条信息，则输出全部信息。

参数说明：

show	查看连接配置信息
count	显示 IP 地址对应 session 个数的 top 5 信息

实例：

**显示 IP 地址对应 session 个数的 top 5 信息

session show count<cr>

session show statistic<cr>

命令描述：

查看连接统计信息。

参数说明：

show	查看连接统计信息
statistic	查看连接统计信息：每秒新建连接数，每秒包数。

实例：

**查看连接统计信息

session show statistic<cr>

session show max-user [**from** <*number1*>] [**num** <*number2*>]

命令描述：

查看按连接数排序的 IP 用户信息。

参数说明：

show max-user	查看按连接数排序的 IP 用户信息。
from	指定从排序用户的第几个用户开始，默认为第一个。
number1	指定数值。
num	指定需要显示的用户数目，最大为 8000，默认为 100。
number2	指定数值

实例：

**查看所有按连接数排序的 IP 用户信息

session show max-user

session show latest-update[**num** <*number2*>] [**vsid**<*number1*>]

命令描述：

查看按连接数排序的 IP 用户信息。

参数说明：

show	查看按连接数排序的 IP 用户信息。
latest-update	指定从排序用户的第几个用户开始，默认为第一个。
num	指定需要显示的用户数目，最大为 8000，默认为 100。
number2	指定数值。

vsid	指定虚系统号。
number1	指定数值。

实例：

**查看所有按连接数排序的 IP 用户信息

session show latest-update

session show syn-attack<cr>

命令描述：

查看 SYN 攻击统计信息。

session show user <*ipaddress*>

命令描述：

查看特定用户的连接信息。

参数说明：

show user	查看特定用户的连接信息
ipaddress	标准 IP 地址字符串

实例：

**查看 IP 地址为 192.168.83.228 的用户的连接信息。

session show user *192.168.83.228*

session syn-reset<on|off>

命令描述：

快速连接重用设置。当源到目的的连接已经存在，源向目的发送 SYN 包时，如果不设置该选项，则 SYN 包会被丢弃。只有打开该开关时才会将已建立的连接删除并重新建立连接。

参数说明：

syn-reset	设置是否开启快速连接重用功能
on|off	开启/关闭

session tcp-reset<on|off>

命令描述：

设定是否允许设备发送 TCP Reset 报文。

参数说明：

tcp-reset	设定是否允许设备发送 TCP Reset 报文。默认不发送。
on|off	是/否。

实例：

**设置发送 TCP 复位报文

session tcp-reset on

session timeout close <*number*|default>

命令描述：

关闭时 TCP 连接超时设置。

参数说明：

timeout	连接超时设置
close	指定 TCP 关闭超时，默认为 20 秒。
number	数值，范围为 3-800。
default	设定为默认超时值。

实例：

**设定关闭时 TCP 连接超时为默认值 20 秒。

session timeout close default

**设定关闭时 TCP 连接超时为 200 秒。

session timeout close *200*

session timeout established <*number*|default>

命令描述：

已建立 TCP 连接超时设置。

参数说明：

timeout	连接超时设置
established	设定已建立 TCP 连接超时，默认为 600 秒。
number	数值，范围为 10-7200。单位为秒。
default	设定为默认超时值。

实例：

**设定已建立 TCP 连接超时为默认值 600 秒。

session timeout established default

**设定三次握手阶段 TCP 连接超时为 200 秒。

session timeout handshake *200*

session timeout handshake <*number*|default>

命令描述：

握手时连接超时设置。

参数说明：

timeout	连接超时设置
handshake	指定三次握手阶段 TCP 连接超时，默认为 100 秒。
number	数值，范围为 10-200 秒。
default	设定为默认超时值，即 200 秒。

实例：

**设定三次握手阶段 TCP 连接超时为 150 秒。

session timeout handshake *150*

session timeout other <*number*|default>

命令描述：

其他类型连接超时设置。

参数说明：

timeout	连接超时设置
other	指定其他类型连接超时，默认为 20 秒。
number	数值，范围为 10-7200。
default	设定为默认超时值。

实例：

**设定其他类型连接超时为默认值 20 秒。

session timeout other default

**设定其他类型连接超时为 200 秒。

session timeout other *200*

session timeout syn_proxy < [**quota** <*number1*> **burst** <*number2*>] | **default**>

命令描述：

SYN 代理参数设置。

参数说明：

timeout	连接设置
syn_proxy	指定 SYN 代理超时参数。
quota	设定配额，即平均每秒 SYN 代理数目，默认为 2000 个/秒。
number1	数值，设定范围为 10-200000 个/秒。
burst	设定限额值，即最大每秒 SYN 代理数目，默认值为 5000 个/秒。
number2	数值，设定范围为 10-200000 个/秒。
default	设定为默认值，即配额为 2000 个/秒，限额为 5000 个/秒。

实例：

**设定 SYN 代理参数值为默认值。

session timeout syn_proxy default

**设定 SYN 代理参数值配额 50。限额 70。

session timeout syn_proxy quota *50* **burst** *70*

session timeout udp <*number*|default>

命令描述：

UDP 连接超时设置。

参数说明：

timeout	连接超时设置
udp	指定 UDP 超时，默认为 60 秒。
number	数值，范围为 10-7200。
default	设定为默认超时值。

实例：

**设定 UDP 连接超时为默认值 60 秒。

session timeout udp default

**设定 UDP 连接超时为 200 秒。

session timeout udp *200*

session timeout default<cr>

命令描述：

将所有连接参数设置为默认值。

参数说明：

timeout	连接设置
default	设定为默认超时值。
cr	键盘回车符

实例：

**设定所有相关连接设置为默认值。

session timeout default

session delete protocol<*string1*> **saddr**<*string2*> **sport**<*number1*> **daddr**<*string3*>

dport<*number2*>**vsid**<*number3*>

命令描述：

删除连接信息。

参数说明：

delete	删除连接信息
protocol	协议类型
string1	字符串
saddr	源 IP 地址
string2	IP 地址字符串
sport	源端口
number1	端口号
daddr	目的地址
string3	IP 地址字符串
dport	目的端口
number2	端口号
vsid	指定虚系统 ID
number3	ID 号

spantree

生成树协议的配置和管理。安全网关对交换网络提供支持，交换接口的生成树功能在缺省情况下处于关闭状态。如果网络中需要通过环路设计来提供网络的冗余容错能力，而同时又需要防止产生环路，则需要开启生成树。TOS 支持的生成树协议包括 CISCO 公司的 PVST+（每个 VLAN 维护一棵生成树）及 CST（以交换

机为单位所有 VLAN 维持一个生成树）。

spantree set mode <pvst|cst|off>

命令描述：

设置生成树的模式，以及是否开启生成树。交换接口的生成树功能在缺省情况下处于关闭状态。

参数说明：

set	设定生成树
mode	模式
pvst|cst|off	pvst 模式|cst 模式|off 不使用生成树算法

使用说明：

交换接口的生成树功能在缺省情况下处于关闭状态。如果网络中需要通过环路设计来提供网络的冗余容错能力，而同时又需要防止产生环路，则需要开启生成树。当用户可以确认该交换接口连接的部分不存在环路时，也可以关闭已经打开的生成树功能。

实例：

** 设置生成树为 pvst 模式

spantree set mode pvst

spantree set vlan <*number***> <**disable|enable**>**

命令描述：

当生成树协议工作在 PVST 模式时，设定对于指定 VLAN 是否启用生成树算法。

参数说明：

set	设定生成树参数
vlan	VLAN 编号
number	数值，形为 XXXX，不能为 0。
disable|enable	否|是

实例：

** 在 pvst 模式下开启 VLAN0001

spantree set vlan *0001* **enable**

spantree set vlan <*number1*> < **portvlanpri** <*number2*> **| portvlancost**<*number3*> > **interface**

<*string*>

命令描述：

对于指定 VLAN，设置到达根端口的费用

参数说明：

set	设定生成树
vlan	VLAN 编号
number1	数值，形为 XXXX
portvlanpri	指定端口优先级
number2	数值，范围 0-255
portvlancost	指定端口费用，即到达根端口的开销
number3	数值，范围 0-65500
interface	指定接口，必须是 VLAN 所在的已定义的接口
string	字符串

使用说明：

为接口指定 VLAN 请参见命令 **switchport trunk allowed-vlan**。

实例：

** 设定 VLAN0001 的优先级为 5

spantree set vlan *0001* **portvlanpri** *5* **interface** *eth0*

** 设定 VLAN0001 的费用为 50

spantree set vlan *0001* **portvlancost** *50* **interface** *eth0*

spantree set vlan <*number1*> [**hello** <*number2*>] [**fwddelay** <*number3*>] [**maxage** <*number4*>]

[**priority** <*number5*>]

命令描述：

设定某 VLAN 的生成树参数。

参数说明：

set	设定生成树参数
vlan	VLAN 编号
number1	数值，形为 XXXX，当指定为 0 时，设置 CST 模式生成树参数，否则指定某 VLAN 的生成树参数。
hello	可选项，设置 STP 中的 hello-time 定时器，即 BPDU 发送时间间隔，默认设置为 2 秒，范围为 1～65535。注意：呼叫时间不能大于网桥的最大老化时间（Max Age）。否则，将出现错误信息。
number2	数值，范围 1-65535s
fwddelay	可选项，设置 STP 中的传输延迟 fwddelay 定时器，即 BPDU

	转发延迟时间间隔，是指交换机的端口从阻塞状态转为转发状态所用的监听时间。默认设置为 15 秒，范围为 1～65535。
number3	数值，范围 1-65535s
maxage	可选项，设置 STP 中的最大寿命 maxage 定时器，即最大老化时间，BPDU(网桥协议数据单元)的最大老化时间，默认设置为 20 秒，范围为 1～65535。
number4	数值，范围 1-65535s
priority	可选项，设置网桥优先级，数值越小级别越高。默认值为 32768。
number5	数值，范围 1-65535

实例：

** 设定 VLAN0001 生成树的参数 hello-time 定时器值为 2 秒。

spantree set vlan *0001* **hello** *2*

spantree set root [**vlan** <*number*>]

命令描述：

设置生成树的根桥。当指定CST模式下生成树的根桥时可以不指定参数**vlan**的值，或设置vlan的参数*number*为 0。当生成树工作模式为PVST时必须指定**vlan**参数。

参数说明：

set	设定生成树
root	设定某 VLAN 为根桥
vlan	设定 VLAN 编号。当生成树工作模式为 PVST 时必须指定该参数。当生成树工作模式为 CST 时可以不设定该参数，或设定该参数为 0。
number	数值，形为 XXXX

实例：

** 设定安全网关作为 VLAN0002 的生成树的根桥

spantree set root vlan *0002*

spantree set default [**vlan** <*number*>]

命令描述：

将生成树参数恢复默认设置。当指定生成树为CST模式下时可以不指定参数**vlan**的值，或设置vlan的参数*number*为 0。当生成树工作模式为PVST时必须指定**vlan**参数。

参数说明：

set	设定生成树参数
default	恢复默认设置
vlan	设置 VLAN 编号。当生成树工作模式为 PVST 时必须指定该参数。当生成树工作模式为 CST 时可以不设定该参数，或设定该参数为 0。
number	数值，形为 XXXX

实例：

** 恢复 VLAN0001 的生成树参数为默认设置

spantree set default vlan *0001*

** 恢复 CST 模式下的生成树参数为默认设置

spantree set default

spantree show [**vlan** <*number*>] [**type**<status|configuration>]

命令描述：

查看生成树的信息。

参数说明：

show	查看生成树信息
vlan	可选项，指定查看哪个 VLAN 的生成树信息。
number	数值，形为 XXXX
type	可选项，指定要查看的信息类型
status|configuration	状态信息 | 配置信息

实例：

** 显示 VLAN0001 的生成树状态信息

spantree show vlan *0001* **type** status

statistic

流量统计相关设置

statistic on<cr>

命令描述：

开启流量统计开关

statistic show [**ip** <*ipaddress*>| **top**<*number*> | **status**]

命令描述：

显示流量统计数据和状态。

参数说明：

show	显示流量统计数据
ip	显示某个 ip 的流量
ipaddress	字符串，IP 地址
top	流量前 n 名的 ip 流量
number	数值，范围 1-1000
status	显示对主机、范围、子网地址对象的流量统计功能是否开启。

实例：

** 显示 IP 为 192.168.7.154 的流量

statistic show ip *192.168.7.154*

** 显示流量前 5 名的 IP 的流量

statistic show top *5*

**查看对主机、范围、子网地址对象的流量统计功能是否开启。

statistic show status

host statistic stop

subnet statistic stop

range statistic stop

statistic off<cr>

命令描述：

关闭流量统计开关

statistic clean<cr>

命令描述：

清除流量统计数据

subnetstatistic

设置对子网对象进行流量统计的功能。

subnetstatistic set name< *string* >

命令描述：

添加子网对象到流量统计列表中，设置对子网对象的流量统计功能。

参数说明：

set	添加子网对象作为流量统计对象
name	设置统计对象名称
string	字符串，应当是已经添加的子网对象的名称。

使用说明：

1) 如果设置的地址对象不是已经定义的子网地址对象，则命令执行会提示错误信息。

2）查看已经定义的子网对象信息在 define 组件下的 subnet 命令下查看。

subnetstatistic clean [**name**< *string* >]

命令描述：

从统计列表中删除某子网对象，从而停止对该子网对象的流量统计功能。

参数说明：

clean	从统计列表中删除子网对象
name	可选项，指定统计对象名称，不指定时从统计列表中删除所有子网对象。
string	字符串，应当是从统计列表中已经添加的子网对象的名称。

使用说明：

1) 如果设置的地址对象不是已经定义的子网地址对象，则命令执行会提示错误信息。

2）不指定任何参数时将已添加的所有子网对象从统计列表中删除。

subnetstatistic show < cr >

命令描述：

查看对子网对象的流量统计结果。

使用说明：

如果没有设置子网对象流量统计功能，则显示结果没有任何信息。

suitstate

接口联动主要用于安全网关工作在流量负载均衡模式，通过把负责转发数据的设备的出接口和入接口添加到同一个联动组，实现同一个联动组中所有接口的状态始终保持一致。

suitstate add name <*string1*> **member** <*string2*>

命令描述：

添加接口联动组。

参数说明：

add	添加接口联动组
name	设置接口联动组名称
string1	字符串，接口联动组名称
member	设置接口联动组成员
string2	字符串，物理接口名称

使用说明：

接口联动组的成员只能是物理接口。

实例：

**添加接口联动组“eth1-2”，设置参与联动的物理接口为 eth1 和 eth2。

suitstate add name *eth1-2* **member** ‘*eth1 eth2*’

suitstate delete name <*string*>

命令描述：

删除接口联动组。

参数说明：

delete	删除接口联动组
name	指定要删除的接口联动组的名称

string	字符串，接口联动组名称

实例：

**删除接口联动组“eth1-2”。

suitstate delete name *eth1-2*

suitstate clean <cr>

命令描述：

删除所有接口联动组。

实例：

**删除所有接口联动组。

suitstate clean

suitstate enable <cr>

命令描述：

启用接口联功能。

suitstate disable <cr>

命令描述：

禁用接口联功能。

suitstate show <configuration|status>

命令描述：

显示接口联动的配置或状态。

参数说明：

show	显示接口联动的配置或状态
configuration	显示接口联动的配置
status	显示接口联动的状态

实例：

**查看接口联动的当前状态。

suitstate show status

traffic

查看接口的流量信息

traffic statistic [**interface** <*string*>] <cr>

命令描述：

查看接口的流量信息

参数说明：

statistic	流量统计
interface	指定要查看流量信息的接口名称，不指定时查看所有接口的流量信息。
string	字符串，接口名称。

使用说明：

目前，网络卫士安全网关只支持对物理接口和子接口进行流量统计。

实例：

**查看接口 eth0 的流量信息。

traffic statistic interface *eth0*

tunnel

GRE 通道设置。

tunnel add name <*string1*> **local** <*string2*> **remote**<*string3*> [**key** <*number1*> **csum** <on|off> **seq** <on|off> **ttl** <*number2*>]

命令描述：

增加 GRE 通道策略对象。

参数说明：

add	增加 GRE 通道策略对象

name	通道名称
string1	字符串，隧道名称必须以“gre-”作为开头
local	通道本地端封装地址
string2	字符串，IP 地址
remote	通道目的端封装地址
string3	字符串，IP 地址
key	标示通道关键字
number1	数值，范围为 0-4294967295。
csum	是否开启校验和检查
on|off	是|否
seq	是否开启序列号检查
on|off	是|否
ttl	设置通道 TTL
number2	数值，范围为 1-255。

实例：

**增加 GRE 通道策略对象

tunnel add name *gre-test* **local** *192.168.6.24* **remote***192.168.7.23* **key** *111111* **csum** on **seq** on **ttl** *111*

tunnel clean <cr>

命令描述：

清空 GRE 通道策略对象。

tunnel delete <name<*string*>| **id** <*number*>>

命令描述：

删除 GRE 通道策略对象。

参数说明：

delete	删除指定 GRE 表中的相关记录
name	指定 GRE 策略名称
string	字符串
id	指定 GRE 策略 ID 号
number	数值

实例：

** 删除名称为 gre-test 的策略

tunnel delete name *gre-test*

tunnel modify name <*string*> [**local** <*string2*> **remote**<*string3*> **key** <*number1*> **csum** <on|off> **seq** <on|off>**ttl** <*number2*>]

命令描述：

修改 GRE 通道策略对象。

参数说明：

modify	增加 GRE 通道策略对象
name	通道名称
string1	字符串，隧道名称必须以“gre-”作为开头
local	通道本地端封装地址
string2	字符串，IP 地址
remote	通道目的端封装地址
string3	字符串，IP 地址
key	标示通道关键字
number1	数值
csum	是否开启校验和检查
on|off	是|否
seq	是否开启序列号检查
on|off	是|否
ttl	设置通道 TTL
number2	数值

实例：

**修改 GRE 通道策略对象对端 IP 地址 192.168.7.36

tunnel modify name *gre-test* **remote** *192.168.7.36*

tunnel show [**name**<*string*>| **id** <*number*>]<cr>

命令描述：

显示 GRE 通道策略对象。

参数说明：

show	显示 GRE 表中的相关记录
name	指定 GRE 策略名称
string	字符串
id	指定 GRE 策略 ID 号
number	数值

实例：

** 显示名称为 gre-test 的策略

tunnel show name *gre-test*

virtual-line

虚拟线指的是在安全网关上设定一个物理接口组 AB 口，从 A 口进入安全网关后，除了目的地址为安全网关的数据报文外，均强制从 B 口进行转发，即不经过二层交换以及三层路由的检查过程就将报文直接发送出去。

virtual-line add dev1 <*string*> **dev2** <*string*>

命令描述：

添加虚拟线路。

参数说明：

add	添加虚拟线路
dev1	设置虚拟线路左端的物理接口名
string	物理接口名字符串
dev2	设置虚拟线路右端的物理接口名
string	物理接口名字符串

实例：

** 添加虚拟线路，两端分别是 eth0 口和 eth1 口。

virtual-line add dev1 *eth0* **dev2** *eth1*

virtual-line clean<cr>

命令描述：

清空所有虚拟线路。

virtual-line delete id<*number*>

命令描述：

删除某虚拟线路。

参数说明：

delete	删除虚拟线路
id	设置虚拟线路 ID 号
number	指定虚拟线路 ID

virtual-line show<cr>

命令描述：

查看所有虚拟线路。

vlan

当物理接口工作在交换模式下时，网络卫士安全网关可以很好地支持 VLAN。交换接口的工作模式包括 ACCESS 及 TRUNK 模式。

vlan add <id <*number*>**| range**<*string*>>

命令描述：

添加 VLAN 虚接口。为了给 VLAN 指定 IP 地址，需要给 VLAN 创建一个虚拟路由接口。

参数说明：

add	添加 VLAN 虚接口
id	添加指定 id 号的 VLAN 虚接口
number	数值
range	指定 vlan 的范围
string	字符串，指定 vlan 范围，格式举例：1-10 表示 1 到 10；或 1，10 表示为 1 和 10

使用说明：

安全网关出厂配置中默认有一个 vlan，id 号为 0。

实例：

** 添加 id 号为 1-10 的 VLAN 虚接口。

vlan add range *1-10*

vlan add-group <*number1*> <*number2*>

命令描述：

将两个 VLAN 设置在同一个 VLAN 转换组中。在这两个 VLAN 间的主机是可以直接通信的而不需要经过三层交换。如果某个 VLAN 加入一个 VLAN 转换组，则不能再和原有 VLAN 中主机进行通信。

参数说明：

add-group	将两个 VLAN 设置在同一个 VLAN 转换组中
number1	数值
number2	数值

实例：

** 将 id 号为 1 和 10 的 VLAN 设置在同一个虚接口组中。

vlan add-group *1 10*

vlan delete <id <*number*>| **range**<*string*>>

命令描述：

删除 VLAN 虚接口。

参数说明：

delete	删除 VLAN 虚接口
id	指定欲删除的 VLAN 虚接口 id 号
number	数值
range	指定欲删除的 VLAN 虚接口的范围
string	字符串，指定 vlan 范围，格式举例：1-10 表示 1 到 10；或 1，10 表示为 1 和 10

使用说明：

1) 安全网关出厂配置中默认有一个 vlan，id 号为 0 不能被删除。

2)指定参数 id 时一次只能删除一个，指定参数 range 时一次可以删除多个。

实例：

** 删除 id 号为 1-10 的 VLAN 虚接口。

vlan delete range *1-10*

vlan delete-group <*number1*> <*number2*>

命令描述：

删除某个 VLAN 转换组。删除后，指定的两个 VLAN 不再属于一个组，这两个 VLAN 之间的通信依然需要进行三层交换。

参数说明：

delete-group	删除某 VLAN 转换组
number1	数值
number2	数值

使用说明：

只有两个参数的值都与已有的 VLAN 虚接口组相匹配时才能删除该组。

实例：

** 解除 id 号为 1 和 10 的 VLAN 之间的虚接口组关系。

vlan delete-group *1 10*

vlan show [**id** <*number*>]

命令描述：

查看 VLAN 虚接口组。

参数说明：

show	查看 VLAN 虚接口
id	可选项，指定欲查看哪个 VLAN 虚接口的属性。
number	数值

使用说明：

不指定任何参数时查看所有 VLAN 虚接口的属性。

实例：

** 查看所有 VLAN 虚接口。

vlan show<cr>

** 查看 id 号为 1 的 VLAN 虚接口。

vlan show id *1*

vlan show-group<cr>

命令描述：

查看 VLAN 虚接口组。

参数说明：

show-group	查看 VLAN 虚接口组
cr	键盘回车符。

vlan clean <cr>

命令描述：

删除所有的 VLAN。

PF

本命令用来设定包过滤规则

对收到的 IP 包进行访问控制，将不合法或者不被规则允许的报文先过滤掉，在网关系统没有加入网关模块的情况下，能够起到一定的安全防范作用。

进入本命令模块操作如下：

pf <cr>

退出本命令模块操作如下：

exit <cr>

CLI 管理员登录网关进入本命令模块后，可以执行相应的组件管理命令。下面将详细描述本命令模块下的所有组件管理命令。命令的实例输入格式将按已经进入本命令模块书写。

下一级命令列表

命令	功能
idbprule	IDBP 规则管理
idsserver	IDS 联动服务器管理
rule	包过滤规则管理
service	服务访问控制规则管理

idbprule

IDBP 动态规则管理。动态规则为网关系统在和 IDS 联动成功并检测到攻击行为后，会在网关上自动生成的一些阻断规则。

idbprule show <cr>

命令描述：

显示 IDBP 动态规则。

idbprule clean<cr>

命令描述：

清空 IDBP 动态规则。

idbprule delete id <*number*>

命令描述：

删除一条 IDBP 动态规则

参数说明：

delete	删除 IDBP 规则编号
id	IDBP 规则编号
number	数值 s

实例：

** 删除编号为 2 的 IDBP 规则

idbprule delete id 2

idbprule log <on|off>

命令描述：

设置增加一条 idbp 规则时是否记录日志

参数说明：

log	设置增加一条 idbp 规则时是否记录日志
on|off	是|否

idbprule drop-log <on|off>

命令描述：

设置当一个报文被一条 idbp 规则阻止时是否记录日志

参数说明：

drop-log	设置当一个报文被一条 idbp 规则阻止时是否记录日志
on|off	是|否

idsserver

设置 IDS 联动规则相关参数。网关可以实现与其他厂商的入侵检测系统的联动，对用户内部网络提供了全面、高效的安全保护。

idsserver add ip <*ipaddress*> **key** <*string*>

命令描述：

添加一个 IDS 联动规则

参数说明：

add	添加 IDS 联动规则
ip	设置可以联动的 IDS 设备 IP 地址
ipaddress	IP 地址格式字符串，形为 A.B.C.D。
key	设置和 IDS 设备的共享密钥
string	字符串

使用说明：

1）此处要求网关和联动 IDS 设备的共享密钥是手工设置的。如果联动的 IDS 设备的密钥是系统自动生成的，则需要用户在 WEBUI 界面进行操作，详细设置请参考管理手册相关部分。

2）要实现网关和 IDS 设备的联动，还需要在相应区域开放 tosids 服务，具体设置请参见 pf service 命令。

实例：

idsserver add ip *192.168.1.21* **key** *topsec*

idsserver clean <cr>

命令描述：

清除所有联动 IDS 服务器。

idsserver delete id <*number*>

命令描述：

删除一个 IDS 联动规则

参数说明：

delete	删除一个 IDS 联动规则
id	指定欲删除规则的 id 号
number	数值，应当为已有规则 id 号。

实例：

idsserver delete id *8584*

idsserver modify id<*number*> <[**ip** <*ipaddress*>][**key** <*string*>]>

命令描述：

修改一个 IDS 联动规则

参数说明：

modify	修改一个 IDS 联动规则
id	指定欲修改规则的 id 号
number	数值
ip	可选项，修改 IDS 联动设备 IP 地址
ipaddress	字符串，形为 A.B.C.D。
key	修改网关和 IDS 设备的共享密钥
string	字符串

实例：

idsserver modify id *8584* **ip** *192.168.2.33* **key** TSbeijing

idsserver show <cr>

命令描述：

查看所有 IDS 联动规则。

实例：

#**idsserver show** <cr>

ID 8584 pf idsserver add ip 192.168.1.21 key topsec

rule

包过滤规则管理

rule set default action <accept|reject> **log**<yes|no>

命令描述：

设定默认包过滤规则。

参数说明：

set default action	设定默认包过滤规则

accept|reject	允许|禁止
log	指定是否在日志中记录
yes|no	是|否

实例：

** 设置默认报过滤规则为允许通过，不记录日志

rule set default action *accept* **log** no

rule add action <accept|reject> **l2protocol** <ip|0800> [**area** <*string1*>] [**log** <yes|no>] [**smac** <*string2*>] [**dmac** <*string3*>] [**l3protocol** <all|0|tcp|6|udp|17|icmp|1|igmp|2|number>] [**sip** <*string4*>] [**dip** <*string5*>] [**sport** <*number1*>] [**dport** <*number2*>] [**sport_end** <*number3*>] [**dport_end** <*number4*>] [**vsid** <*number*>] [**enable** <yes|no>]

命令描述：

增加一条 IP 协议包过滤规则。

参数说明：

add	增加一条包过滤规则
action	对符合条件的数据包的操作，是否允许通过。
accept|reject	允许|禁止
l2protocol	数据包使用的第二层协议类型
IP|0800	IP 协议
area	指定区域资源
string1	字符串，必须是已经定义的区域资源
log	是否记录日志
yes|no	是|否
smac	设定源 mac 地址
string2	标准 mac 地址字符串
dmac	设定目的 mac 地址
string3	标准 mac 地址字符串
l3protocol	数据包使用的第三层协议类型
all|0|tcp|6|udp|17|icmp|1|igmp|2|number	全部协议/全部协议/TCP 协议/TCP 协议/UDP 协议/UDP 协议/ICMP 协议/ICMP 协议/IGMP 协议/IGMP 协议/用户输入指定协议号的数值
sip	指定源地址对象，必须是已定义的地址对象
string4	字符串
dip	指定目标地址对象 ，必须是已定义的地址对象。
string5	字符串
sport	指定源的起始端口号
number1	数值
sport_end	指定源的结束端口号
number2	数值
dport	指定目的的起始端口号

number3	数值
dport_end	指定目的的结束端口号
number4	数值
vsid	设置虚系统 id。
number	数值。
enable	选择是否生效，默认生效
yes|no	是|否

实例：

** 允许源 MAC 为 00:50:04:C3:B0:31 的设备访问目的 IP 为 doc_server 目的端口为 8000 的设备

rule add action accept **smac** *00:50:04:C3:B0:31* **dip** *doc_server* **dport** *8000*

rule add action <accept|reject> **l2protocol** < ipx|8137> [**log**<yes|no>] [**area** <*string*>] [**smac** < *string 2*>] [**dmac** < *string 3*>] [**vsid** <*number*>] [**enable** <yes|no>]

命令描述：

增加一条 IPX 协议包过滤规则。

参数说明：

add	增加一条包过滤规则
action	对符合条件的数据包的操作，是否允许通过。
accept|reject	允许|禁止
l2protocol	数据包使用的第二层协议类型
arp|0806|rarp|8035|ipx|8137	ARP| ARP|RARP| RARP|IPX|IPX 协议
log	是否记录日志
yes|no	是|否
area	指定区域资源
string1	字符串，必须是已经定义的区域资源。
smac	设定源 mac 地址
string2	标准 mac 地址字符串
dmac	设定目的 mac 地址
string3	标准 mac 地址字符串
vsid	设置虚系统 id。
number	数值。
enable	选择是否生效，默认生效
yes|no	是|否

实例：

** 为区域 area_eth1 添加 arp 允许规则，并记录日志

rule add action accept **l2protocol** arp **log** yes **area** *area_eth1*

rule clean [**vsid** <*number*>]

命令描述：

清除所有/指定虚系统内所有的包过滤规则。

参数说明：

clean	删除所有包过滤规则
vsid	删除指定虚系统内所有的过滤规则
number	数值

rule delete [**vsid** <*number1*>] **id** <*number2*>

命令描述：

删除一条包过滤规则

参数说明：

delete	删除包过滤规则
vsid	删除指定虚系统内的某条规则
number1	数值
id	规则号
number2	数值

使用说明：

查看规则编号使用命令 **rule show**。

实例：

** 删除编号为 8122 的规则

rule delete id *8122*

rule modify id <*numbe1*>[**action** <accept| reject >] [**l2protocol** <ip|0800>] [**area** <*string1*>] [**log** <yes|no>] [**smac** <*string2*>] [**dmac** <*string3*>] [**l3protocol** <all|0|tcp|6|udp|17|icmp|1|igmp|2| number>] [**sip** <*string4*>] [**dip** <*string5*>] [**sport** <*number2*>] [**dport** <*number3*>] [**sport_end** <*numbe4*>] [**dport_end** <*number5*>] [**vsid** <*number6*>] [**enable** <yes|no>]

命令描述：

修改一条 IP 协议包过滤规则。

参数说明：

modify	修改一条包过滤规则
id	规则号
number1	数值
action	对符合条件的数据包的操作，是否允许通过。。
accept|reject	允许|禁止
l2protocol	数据包使用的第二层协议类型
IP|0800	IP 协议
area	指定区域资源
string1	字符串，必须是已经定义的区域资源。
log	是否记录日志
yes|no	是|否
smac	设定源 mac 地址
string2	标准 mac 地址字符串
d**mac**	设定目的 mac 地址
string3	标准 mac 地址字符串
l3protocol	数据包使用的第三层协议类型
all|0|tcp|6|udp|17|icmp|1|igmp|2|number	全部协议/全部协议/TCP 协议/TCP 协议/UDP 协议/UDP 协议/ICMP 协议/ICMP 协议/IGMP 协议/IGMP 协议/用户输入指定协议号的数值
sip	指定源地址对象，必须是已定义的地址对象。
string4	字符串
dip	指定目标地址对象 ，必须是已定义的地址对象。
string5	字符串
sport	指定源的起始端口号
number2	数值
sport_end	指定源的结束端口号
number3	数值
dport	指定目的的起始端口号
number4	数值
dport_end	指定目的的结束端口号
number5	数值
vsid	设置虚系统 id。
number6	数值。
enable	选择是否生效，默认生效
yes|no	是|否

使用说明：

由于策略执行为第一匹配原则，则策略的顺序与策略的逻辑相关，添加策略以后可以通过移动一条包过滤规则的位置来改变策略的执行序。.

实例：

** 修改规则，禁止源 MAC 为 00:50:04:C3:B0:31 的设备访问目的 IP 为 doc_server 目的端口为 8080 的设备。

rule add action reject **smac** *00:50:04:C3:B0:31* **dip** *doc_server* **dport** *8080*

rule show [**vsid** <*number*>]

命令描述：

显示所有/指定虚系统内所有的包过滤规则。

参数说明：

show	显示包过滤规则
vsid	显示指定虚系统内的包过滤规则
number	数值

rule move id <*number1*> **before** <*number2*>|**after** <*number3*> [**vsid** <*number4*>]

命令描述：

将指定规则移动到某条规则之前或之后。

参数说明：

move	移动包过滤规则
id	待移动包过滤规则的 id 号。
number1	数值
befor	将指定规则移动到哪条规则之前
number2	数值
after	将指定规则移动到哪条规则之后
number3	数值
vsid	指定虚系统号
number4	数值

service

服务访问控制规则管理（设定访问本机的规则）：为了更好的对网关进行配置管理，管理器为用户提供了一种分类管理的方法，将登录到网关的用户按 IP 地址进行分别管理。这样，网络管理员可以指定某个 IP 地址段的用户的登录网关的方式或管理级别。

service add name

<gui|webui|auth|update|monitor|snmp|ping|ssh|telnet|tosids|dhcp|ipsecvpn|rip|l2tp|pptp|ntp|sslvpn|sslvpnmgr|websv|cgi_auth|bgp> **area** <*string1*> <**addressid** <*number1*>| **addressname**

<*string2*>> [**packets** <*number*>| **newsession**<*number*>]

命令描述：

增加一条开放某服务规则。

参数说明：

add	增加一条开放某服务规则
name	选择网关开放的服务名
gui	开放 GUI 服务
webui	开放通过 WEBUI 管理网关
auth	开放认证服务
update	升级
monitor	开放监控服务
snmp	开放 SNMP 服务
ping	开放 PING 服务
ssh	开放 SSH 服务
telnet	开放 TELNET 服务
tosids	开放 IDS 服务
dhcp	开放动态主机配置服务
ipsecvpn	开放建立 IPSEC 隧道时需要开放的服务。
rip	开放 RIP 服务
l2tp	开放 L2TP 服务
pptp	开放 PPTP 服务
ntp	开放 NTP 服务
sslvpn	开放 SSLVPN 服务
sslvpnmgr	开放 SSLVPNMGR 服务
websv	开放 WEBSV 服务
cgi_auth	开放 CGI 服务
bgp	开放 BGP 服务
area	选择允许服务请求来自哪个区域，只能从现有区域中选择一个。
string1	字符串
addressid	设定允许地址对象 ID 号
number1	数值
addressname	设定允许地址对象名称
string2	字符串，必须是已经定义的主机、子网或范围地址对象。
packets	可选项，设置允许的每秒数据包数量
number	数值，范围 0-65535；0 表示不控制。
newsession	可选项，设置允许的每秒新建连接数量
number	数值，范围 0-65535；0 表示不控制。

使用说明：

参数 addressid 与 addressname 可以同时使用，但必须确认两者所指的地址对象唯一，否则将不能正确添加服务。

实例：

** 为 eth0 接口开放 webui 服务

service add name webui **area** *area_eth0* **addressname** *any* <cr>

service delete id <*number*>

命令描述：

删除一条开放服务规则。

参数说明：

delete	删除一条开放服务规则
id	选择网关开放的服务 id 号
number	数值

使用说明：

删除服务所需的 id 号，可由使用 service show 命令查得。

实例：

** 删除 id 号为 8361 的服务

service delete id *8361*

service modify id <*number*> [**name**

<gui|webui|auth|update|monitor|snmp|ping|ssh|telnet|tosids|dhcp|ipsecvpn|rip|l2tp|pptp|ntp|sslvpn|s

slvpnmgr|websv|cgi_auth |bgp>] [**area** <*string1*>] [**addressid** <*number1*>] [**addressname**

<*string2*>][**packets**<*number*>| **newsession**<*number*>]

命令描述：

修改一条开放服务规则。

参数说明：

mod**ify**	修改一条开放服务规则
id	指定规则 ID 号
number	数值，必须是已经添加的规则号。
name	选择网关开放的服务名
gui	开放 GUI 服务
webui	开放通过 WEBUI 管理网关
auth	开放认证服务
update	升级
monitor	开放监控服务
snmp	开放 SNMP 服务
ping	开放 PING 服务

ssh	开放 SSH 服务
telnet	开放 TELNET 服务
tosids	开放 IDS 服务
dhcp	开放动态主机配置服务
ipsecvpn	开放建立 IPSEC 隧道时需要开放的服务。
rip	开放 RIP 服务
l2tp	开放 L2TP 服务
pptp	开放 PPTP 服务
ntp	开放 NTP 服务
sslvpn	开放 SSLVPN 服务
sslvpnmgr	开放 SSLVPNMGR 服务
websv	开放 WEBSV 服务
cgi_auth	开放 CGI 服务
bgp	开放 BGP 服务
area	选择允许服务请求来自哪个区域，只能从现有区域中选择一个。
String1	字符串
addressid	设定允许地址对象 ID 号
number1	数值
addressname	设定允许地址对象名称
String2	字符串，必须是已经定义的主机、子网或范围地址对象。
packets	可选项，设置允许的每秒数据包数量
number	数值，范围 0-65535；0 表示不控制。
newsession	可选项，设置允许的每秒新建连接数量
number	数值，范围 0-65535；0 表示不控制。

使用说明：

一条服务规则除 ID 号不可修改外，其余内容皆可以修改。

实例：

** 修改 id 8361 服务，内容为 eth1 接口开放 gui 服务

service modify id *8361* **name** gui **area** *area_eth1* **addressname** *any* <cr>

service show [**name**

<gui|webui|auth|update|monitor|snmp|ping|ssh|telnet|tosids|dhcp|ipsecvpn|rip|l2tp|pptp|ntp|sslvpn|s

slvpnmgr|websv|cgi_auth|bgp >]

命令描述：

查看开放服务规则。

参数说明：

show	查看开放服务规则
name	选择查看的服务名

gui	开放 GUI 服务
webui	开放通过 WEBUI 管理网关
auth	开放认证服务
update	升级
monitor	开放监控服务
snmp	开放 SNMP 服务
ping	开放 PING 服务
ssh	开放 SSH 服务
telnet	开放 TELNET 服务
tosids	开放 IDS 服务
dhcp	开放动态主机配置服务
ipsecvpn	开放建立 IPSEC 隧道时需要开放的服务。
rip	开放 RIP 服务
l2tp	开放 L2TP 服务
pptp	开放 PPTP 服务
ntp	开放 NTP 服务
sslvpn	开放 SSLVPN 服务
sslvpnmgr	开放 SSLVPNMGR 服务
websv	开放 WEBSV 服务
cgi_auth	开放 CGI 服务
bgp	开放 BGP 服务

使用说明：

选定类型时显示指定服务类型的设置，不选定类型时，显示所有规则。

实例：

** 显示所有 webui 服务开放规则

service show name *webui*

service clean <cr>

命令描述：

清除所有的服务规则。

service log [on|off]

命令描述：

service 日志开关。

参数说明：

log	service 日志开关
on|off]	打开|关闭

PING

验证网络连接情况。

ping <*ipaddress*> [**interface** <*string*>] [**count** <*number*>] [**size** <*number*>]

命令描述：

验证安全网关与主机或网络设备的连接情况。

参数说明：

ping	验证安全网关与主机或网络设备的连接情况
ipaddress	IP 地址字符串，格式为 0.0.0.0
interface	数据报文传出时通过的接口名称
string	字符串，物理接口名称
count	设定发送 ping 包的个数
number	数值，表示 ping 包个数
size	设定发送 ping 包的字节长度
number	数值，单位为字节，取值范围 0-65492

实例：

**发送 100 个数据包验证安全网关与主机 10.10.10.22 的连接情况。

ping *10.10.10.22* **count** *100* <cr>

PKI

本命令用来配置和管理网关的 vpn 证书，如管理本机证书、设置客户端认证根证书、设置客户端证书等。

进入本命令模块操作如下：

#**pki**<cr>

退出本命令模块操作如下：

#**end**<cr>

cli 管理员登录网关进入本命令模块后，可以执行相应的组件管理命令。下面将详细描述本命令模块下的所有组件管理命令，命令的实例输入格式将按已经进入本命令模块的情况书写。

下一级命令列表

命令	功能

cacert	第三方 CA 根证书管理
clean	清空 PKI 的基本配置
cleancert	清空 PKI 证书
ipseccertreq	本机 IPSec 证书请求管理
localca	本地 CA 管理
localcert	本机证书管理
remoteauth	远端认证配置
remotecert	对方设备证书管理
save	保存 PKI 配置
sslcert	本机 SSL VPN 证书管理
sslcertreq	本机 SSL VPN 证书请求管理
tool	获取证书标识符
usb	设置 USBKey
webuicert	Webui 证书管理

cacert

安全网关根证书管理。如果采用第三方 CA 服务器为 vpn 设备或者移动用户签发证书，安全网关要配置维护一个 CA 根证书链和相应 CRL 链；当 vpn 设备提交证书进行认证时，安全网关根据 CA 根证书链和相应 CRL 列表完成证书认证过程。

本模块命令提供 CA 根证书链和 CRL 链维护，为第三方 CA 提供支持。包括导入 CA 根证书、手工导入或定时自动下载 CRL，定时下载时支持 http/ LDAP 协议。管理员可在此对 CA 认证系统进行管理，包括 CA 根证书和 CRL 的导入、刷新、删除，CRL 自动下载管理增加、删除、刷新、查看操作。

cacert import certfile <*string1*> [**crlfile** <*string2*>]

命令描述：

从文件中导入 CA 证书及 CRL。

参数说明：

import	从文件中导入 CA 证书及 CRL
certfile	指定证书文件名
string1	字符串, CA 证书文件名
crlfile	指定 CRL 文件名
string2	字符串，CRL 文件名，上传至/tmp 目录下，不需要全路径

cacert modifyhttpconf index <*number*> [**httpconf**<*string*>]

命令描述：

修改 CA 通过 http 协议下载 CRL 的地址。

参数说明：

modifyhttpconf	修改 CA 通过 http 协议下载 CRL 的地址
index	指定 CA 证书序号
number	数值
httpconf	指定使用 http 协议向第三方 CA 发送下载 CRL 请求时，指定指向 CA 服务器的 CRL 信息的链接。
string	字符串

cacert modifyldapconf index <*number1*> **ip** <*ipaddress*> **port** <*number2*>**basedn**

<*string1*>[**userid** <*string2*>][**passwd** <*string3*>]

命令描述：

修改 CA 通过 LDAP 协议下载 CRL 的配置。

参数说明：

modifyldapconf	修改 CA 通过 LDAP 协议下载 CRL 的配置
index	指定 CA 证书序号
number1	数值
ip	指定 LDAP 服务器的 ip 地址（或域名）
ipaddress	ip 地址字符串
port	指定 LDAP 服务器的查询端口号
number2	数值
basedn	指定 LDAP 服务器的查询根键
string1	字符串
userid	指定登录 LDAP 服务器的用户帐号
string2	字符串
passwd	指定登录 LDAP 服务器的用户密码
string3	字符串

cacert modifycrlptoro index <*number1*> **proto** <ldap|http>

命令描述：

修改 CA 下载 CRL 所使用的协议。

参数说明：

modifyhttpconf	修改 CA 的 CRL 下载协议
index	指定 CA 证书序号
number	数值

proto	指定通过哪种协议下载 CRL 文件
ldap|http	LDAP 协议|HTTP 协议

cacert show<cr>

命令描述：

查看 CA 证书及相关信息。

cacert showcrl index <*number*>

命令描述：

查看 CA 证书的 CRL 详细信息。

参数说明：

showCRL	查看 CA 证书的 CRL 详细信息
index	指定 CA 证书序号
number	数值

c**acert showcrlproto index** <*number*>[**proto** <ldap|http>]

命令描述：

查看一个 CA 的 CRL 下载配置。

参数说明：

showcrlproto	查看一个 CA 的 CRL 下载配置
index	指定 CA 证书序号
number	数值
proto	指定下载 CRL 文件所使用的协议类型
ldap|http	LDAP 协议/HTTP 协议

cacert loadcrl index <*number*> **crlfile** <*string*>

命令描述：

导入 CRL 列表。

参数说明：

loadcrl	导入 CRL 列表
index	指定 CA 证书序号
number	数值
crlfile	指定 CRL 文件名
string	字符串

cacert downcrl index <*number*>

命令描述：

手动下载 CA 的 CRL。

参数说明：

downcrl	手动下载 CA 的 CRL
index	指定 CA 证书序号
number	数值

cacert delcrl index <*number*>

命令描述：

删除一个 CA 证书的 CRL。

参数说明：

delcrl	删除一个 CA 证书的 CRL
index	指定 CA 证书序号
number	数值

cacert delete index <*number*>

命令描述：

删除一个 CA 证书及其相关信息。

参数说明：

delete	删除一个 CA 证书及其相关信息
index	指定 CA 证书序号
number	数值

cacert crltimer [**interval** <*number*>]

命令描述：

指定 CRL 信息更新周期。

参数说明：

crltimer	指定 CRL 信息更新周期
interval	指定下载间隔，单位为秒。
number	数值

cacert clean <cr>

命令描述：

清空 CA 证书及相关信息。

clean

命令描述：

清空 PKI 的所有配置信息。

cleancert

清空 PKI 证书设置

cleancert <cr>

ipseccertreq

用于生成并导出本机 IPSec VPN 证书请求，以及将根据证书请求生成的本机 IPSec VPN 证书导入到安全网关中。

createreq

生成本机 IPSec VPN 证书请求。

createreq cn <*string*> **hash** <sha1> **len** <1024|2048> [**o** <*string*> **ou** <*string*> **c** <*string*>] [**hash** <sha1>] [**s** < *string*>] [**l** < *string*>] [**mail** < string>]

命令描述：

生成本机 IPSec VPN 证书请求。

参数说明：

cn	证书名称
string	字符串
hash	指定哈希算法
sha1	sha1 算法

len	指定算法长度
1024|2048	选择算法长度为 1024 或者 2048
o	机构名称
string	字符串
ou	组织名称
string	字符串
c	国家名称
string	字符串
hash	哈希算法
sha1	输入 sha1
s	省市名称
string	字符串
l	区县名称
string	字符串
mail	邮箱
string	字符串

exportreq

导出本机 IPSec VPN 证书请求。

本命令只适用于界面调用，用户无法使用该命令将证书请求导出到本地目录中，证书请求的导出操作只能在 webui 界面中进行。

exportreq filename <*string*>

命令描述：

导出本机 IPSec VPN 证书请求。

参数说明：

filename	指定证书请求的文件名称
string	字符串

importreq

导入根据本机 IPSec VPN 证书请求生成的证书。

本命令只适用于界面调用，用户无法使用该命令将证书导入到安全网关中，证书的导入操作只能在 webui 界面中进行。

importreq filename <*string*> **format** <der|pem>

命令描述：

导入根据本机 IPSec VPN 证书请求生成的证书。

参数说明：

filename	指定证书文件的名称
string	字符串
format	设置该证书文件的证书格式
der|pem	如果证书文件为 der 格式，则此处配置为 der；如果证书文件为 pem 格式，则此处配置为 pem。

showreq

显示已经生成的本机 IPSec VPN 证书请求内容。

showreq <cr>

命令描述：

显示已经生成的本机 IPSec VPN 证书请求内容。

参数说明：

cr	回车换行符

delete

删除已经生成的本机 IPSec VPN 证书请求内容。

delete <cr>

命令描述：

删除已经生成的本机 IPSec VPN 证书请求内容。

参数说明：

cr	回车换行符

localca

管理本地客户端认证 CA 证书和客户端证书。当客户端采用本地 CA 认证，且不启用远程 LDAP 认证时，需要进行客户端证书配置，用来认证客户。可以在本模块完成此项设置：包括以文件方式或 pkcs12 文件格式导入客户端根证书、以 vpn

本机证书作为客户端根证书、生成新的客户端根证书，客户端根证书的查看、删除等，客户端证书的生成、修改、查看、删除、导出。

clientcert

内置 CA 证书管理：包括证书签发、查看、删除、清空等操作。

clientcert create name <*string*> **country**<*string*> **province**<*string*> **city**<*string*> **email** <*string*> **organization**<*string*> **unit**<*string*> **revokedate**<*string*>

命令描述：

创建客户端认证证书。

参数说明：

create	创建客户端认证根证书
name	指定证书名
string	字符串，必填项。
country	国家名称
string	字符串，仅可输入两位英文字符。
province	省或州名称。
string	字符串
city	城市名称。
string	字符串
email	电子邮件地址
string	字符串
organization	组织名称
string	字符串
unit	单位名称
string	字符串
revokedate	指定证书最后有效日期
string	字符串，格式为 yyyy/mm/dd。

clientcert show [name <*string*>**]**

命令描述：

查看客户端认证根证书。

参数说明：

show	查看客户端认证根证书
name	证书名称（客户端用户名）
string	字符串

clientcert delete name <*string*>

命令描述：

删除客户端认证根证书。

参数说明：

delete	删除客户端认证证书
name	证书名称（客户端用户名）
string	字符串

clientcert clean <cr>

命令描述：

清空客户端认证根证书。

clientcert export name<*string*> **type** <der|pem|pkcs12|tar> **password** <*string*>

命令描述：

导出客户端认证证书。

参数说明：

export	导出客户端认证证书
name	客户端证书名称
string	字符串
type	指定证书类型
der|pem|pkcs12|tar	支持四种格式导出，根据需要选择。 pkcs12：网关支持该种格式。
password	指定打开证书文件的密码
string	字符串

clientcert batch-export type <der|pem|pkcs12|tar> **password** <*string*>

命令描述：

批量导出客户端认证证书。

参数说明：

batch-export	批量导出客户端认证证书
type	指定证书类型
der|pem|pkcs12|tar	支持四种格式导出，根据需要选择。 pkcs12：网关支持该种格式。
password	指定打开证书文件的密码
string	字符串

clientcert writeukey name<*string*> **uktype** [epass1000] **pin** <*string*>

命令描述：

导出客户端认证证书至 USBKey。

参数说明：

writeukey	删除客户端认证证书
name	证书名称
string	字符串
uktype	USBKey 的类型
epass1000	目前支持 epass1000
pin	USBKey 的写入 PIN 码
string	字符串

crl

CRL 设置。

crl creat <cr>

命令描述：

创建客户端认证 CA 根证书文件撤销列表 CRL 文件。

crl export type < der|pem >

命令描述：

导出客户端认证 CA 根证书的 CRL 文件。

参数说明：

export	导出客户端认证 CA 根证书文件撤销列表 CRL 文件
type	指定证书类型
der|pem	根据需要选择。

crl show<cr>

命令描述：

查看客户端认证 CA 根证书文件撤销列表 CRL 文件。

crl revoke name <*string*> **reason** <unspecified|keycompromise|cacompromise |

affiliationchanged>

命令描述：

导出客户端认证 CA 根证书的 CRL 文件。

参数说明：

revoke	吊销客户端认证 CA 签发的客户端证书
name	证书名称
string	根据需要选择。
reason	吊销原因
unspecified|keycompromise|cacompromise|affiliationchanged	unspecified：未指定 keycompromise：密钥泄露 cacompromise：CA 密钥泄露 affiliationchanged：附属关系个改变

rootcert

内置 CA 根证书设置。

rootcert create name <*string*> **country**<*string*> **province**<*string*> **city**<*string*> **email** <*string*>

organization<*string*> **unit**<*string*> **revokedate**<*string*>

命令描述：

创建客户端认证 CA 根证书。

参数说明：

create	创建客户端认证根证书
name	指定证书名
string	字符串，必填项。
country	国家名称
string	字符串，仅可输入两位英文字符。
province	省或州名称。
string	字符串
city	城市名称。
string	字符串
email	电子邮件地址
string	字符串
organization	组织名称
string	字符串
unit	单位名称
string	字符串
revokedate	指定证书最后有效日期
string	字符串，格式为 yyyy/mm/dd。

rootcert getbyfile certfile <*string*> **keyfile** <*string*>

命令描述：

以文件方式导入客户端认证 CA 根证书。

参数说明：

getbyfile	以文件方式导入客户端认证根证书
certfile	指定证书文件名
string	字符串
keyfile	指定证书私钥文件名
string	字符串，

rootcert getbypkcs12 certfile <*string*> **[passwd**<*string*>**]**

命令描述：

以 pkcs12 文件方式导入客户端认证根证书。

参数说明：

getbypkcs12	以 pkcs12 文件方式导入客户端认证根证书
certfile	指定 pkcs12 证书文件名
string	字符串
passwd	指定打开证书文件的密码
string	字符串

rootcert getbylocal <cr>

命令描述：

以网关设备证书作为客户端认证 CA 根证书。

rootcert show <cr>

命令描述：

查看客户端认证 CA 根证书。

rootcert export type <der|pem|pkcs12> **password** <*string*>

命令描述：

导出客户端认证 CA 根证书。

参数说明：

export	导出客户端认证 CA 根证书
type	指定证书类型
der|pem|pkcs12	支持四种格式导出，根据需要选择。

password	指定打开证书文件的密码
string	字符串

localcert

管理设备本机证书。设备的证书首先须由安全管理中心 CA 下发，下发后的证书以文件形式存在磁盘或 USBKey 等存储载体中，然后需要将它从存储载体中导入到 VPN 网关设备才可以使用。

证书导入可以有 4 种方式：

普通文件导入：包括一个证书文件，一个私钥文件。

pkcs12 格式证书导入：包括一个证书文件，一个私钥文件。

打包文件方式导入：可以把上述文件打成一个.tar 的包，再导入。

usb 卡方式导入：证书存储到 USBKey 上，然后从 USBKey 导入。

localcert getbyfile certfile <*string*> **keyfile**<*string*>

命令描述：

以普通文件方式导入证书。

参数说明：

getbyfile	文件方式导入本机证书及私钥
certfile	指定证书文件名
string1	字符串，证书文件名
keyfile	指定证书私钥文件名
string2	字符串，私钥文件名，上传至/tmp 目录下，不需要全路径

使用说明：

由于只导入了证书文件和私钥文件，并未导入根证书文件，因此需要在cacert命令中单独导入根证书。

localcert getbypkcs12 certfile <*string*> [**passwd**<*string*>]

命令描述：

以 pkcs12 格式导入证书。

参数说明：

getbypkcs12	以 pkcs12 文件格式导入本机证书及私钥
certfile	指定 pkcs12 证书文件名
string	字符串，加密证书文件名，上传至/tmp 目录下，不需要全路径。
passwd	指定打开证书文件的密码
string	字符串， 密钥。

localcert getbytar certfile <*string*>

命令描述：

以 tar 文件方式导入本机证书及私钥。

参数说明：

getbytar	以 tar 文件方式导入本机证书及私钥
certfile	指定 tar 证书文件名
string	字符串，打包证书文件名，上传至/tmp 目录下，不需要全路径符串。

localcert getbyusb passwd<*string***>**

命令描述：

从 usb 中导入本机证书及私钥。

参数说明：

getbyusb	从 usb 中导入本机证书及私钥
passwd	指定 usb 密码
string	字符串，usb 密码

localcert show <cr>

命令描述：

查看本机证书。

localcert delete<cr>

命令描述：

删除本机证书。

remoteauth

对 VPN 网关的远端认证配置。当 VPN 网关采用远端认证时，网关直接向 LDAP 或 OCSP 服务器发出认证请求。

remoteauth setldap ip <*ipaddress*> **port** <*number*>**basedn** <*string*>[**userid** <*string*>][**passwd** <*string*>]

命令描述：

对 vpn 网关进行远端 LDAP 认证配置。

参数说明：

setldap	配置远端 LDAP 认证 vpn 网关
ip	指定 LDAP 服务器的 ip 地址
ipaddress	ip 地址字符串
port	指定 LDAP 服务器的端口号
number	数值
basedn	指定 LDAP 服务器进行证书查询的根域
string	字符串
userid	指定登录 LDAP 服务器的用户帐号
string	字符串
passwd	指定登录 LDAP 服务器的用户密码
string	字符串

remoteauth setocsp server <*politos*> **url** <*string*>

命令描述：

对 vpn 网关进行远端 OCSP 认证配置。

参数说明：

setocsp	配置远端 OCSP 认证 vpn 网关
server	指定 OCSP 服务器的类型
polito	目前只支持 polito 类型的服务器，所以请输入 polito
url	指定 OCSP 服务器的 url
string	字符串,url 地址

实例：

**配置 OCSP 服务器为 http://www.topsec.com/ocspsrv

#**remoteauth setocsp server** *polito* **url** *http://www.topsec.com/ocspsrv*

remoteauth enable proto <ldap|ocsp>

命令描述：

开启远端认证。

参数说明：

enable proto	开启远端认证，并指定认证协议类型
ldap|ocsp	选择 LDAP 或 OCSP

remoteauth disable proto <ldap|ocsp>

命令描述：

关闭远端认证。

参数说明：

disable proto	关闭远端认证，并指定认证协议类型
ldap|ocsp	选择 LDAP 或 OCSP

remoteauth show [**proto** <ldap|ocsp>]

命令描述：

查看远端认证配置。

参数说明：

show	查看远端认证配置
proto	指定认证协议类型
ldap|ocsp	选择 LDAP 或 OCSP

remoteauth clean<cr>

命令描述：

清空远端认证配置。

remotecert

对端设备证书管理

remotecert import certfile <*string*>

命令描述：

导入对端设备证书。

参数说明：

import	导入证书
certfile	指定证书文件
string	字符串

remotecert show index <*number*>

命令描述：

查看对端设备证书。

参数说明：

show	查看证书
index	指定证书序号
number	数字

remotecert delete index <*number*>

命令描述：

删除对端设备证书。

参数说明：

delete	删除证书
index	指定证书序号
number	数字

save

save <cr>

命令描述：

保存 PKI 各项设置。

sslcert

SSL 网关证书管理。证书导入可以有 2 种方式：

- 普通文件导入：包括一个证书文件，一个私钥文件。

- pkcs12 格式证书导入：包括一个证书文件，一个私钥文件。

sslcert getbyfile certfile <*string*> **keyfile**<*string*>

命令描述：

以普通文件方式导入证书。

参数说明：

getbyfile	文件方式导入本机证书及私钥
certfile	指定证书文件名
string1	字符串，证书文件名
keyfile	指定证书私钥文件名
string2	字符串，私钥文件名

使用说明：

由于只导入了证书文件和私钥文件，并未导入根证书文件，因此需要在cacert命令中单独导入根证书。

sslcert getbypkcs12 certfile <*string*> [**passwd**<*string*>]

命令描述：

以 pkcs12 格式导入证书。

参数说明：

getbypkcs12	以 pkcs12 文件格式导入 SSLVPN 网关证书及私钥
certfile	指定 pkcs12 证书文件名
string	字符串，加密证书文件名，上传至/tmp 目录下，不需要全路径。
passwd	指定打开证书文件的密码
string	字符串， 密钥。

sslcert getbydefault<cr>

命令描述：

SSLVPN 网关证书使用缺省证书。

sslcert show <cr>

命令描述：

查看 SSL VPN 网关证书。

sslcertreq

用于生成并导出本机 SSL VPN 证书请求，以及将根据证书请求生成的本机 SSL VPN 证书导入到安全网关中。

createreq

生成本机 SSL VPN 证书请求。

createreq cn <*string*> **hash** <sha1> **len** <1024|2048> [**o** <*string*> **ou** <*string*> **c** <*string*>]

命令描述：

生成本机 SSL VPN 证书请求。

参数说明：

cn	证书名称
string	字符串
hash	指定哈希算法
sha1	sha1 算法
len	指定算法长度
1024|2048	选择算法长度为 1024 或者 2048
o	机构名称
string	字符串
ou	组织名称
string	字符串
c	国家名称
string	字符串

exportreq

导出本机 SSL VPN 证书请求。

本命令只适用于界面调用，用户无法使用该命令将证书请求导出到本地目录中，证书请求的导出操作只能在 webui 界面中进行。

exportreq filename <*string*>

命令描述：

导出本机 SSL VPN 证书请求。

参数说明：

filename	指定证书请求的文件名称
string	字符串

importreq

导入根据本机 SSL VPN 证书请求生成的证书。

本命令只适用于界面调用，用户无法使用该命令将证书导入到安全网关中，证书的导入操作只能在 webui 界面中进行。

importreq filename <*string*> **format** <der|pem>

命令描述：

导入根据本机 SSL VPN 证书请求生成的证书。

参数说明：

filename	指定证书文件的名称
string	字符串
format	设置该证书文件的证书格式
der|pem	如果证书文件为 der 格式，则此处配置为 der；如果证书文件为 pem 格式，则此处配置为 pem。

showreq

显示已经生成的本机 SSL VPN 证书请求内容。

showreq <cr>

命令描述：

显示已经生成的本机 SSL VPN 证书请求内容。

参数说明：

cr	回车换行符

delete

删除已经生成的本机 SSL VPN 证书请求内容。

showreq <cr>

命令描述：

删除已经生成的本机 SSL VPN 证书请求内容。

参数说明：

cr	回车换行符

tool

获取证书标识符。

tool subject certfile <*string*>

命令描述：

获取证书标识符。

参数说明：

tool subject	获取证书标识符
certfile	指定证书名称
string	字符串

usb

支持利用 USBKey 来作为 PKI 数字证书的载体。本模块用于 USBKey 参数设置，包括设置是否支持从 USBKey 读取认证信息，以及 USBKey 的类型和 PIN 码等信息。系统默认不开启 USBKey 认证。

usb set uktype <epass1000|none> **pin** <string>

命令描述：

设置 USBKey 参数。

参数说明：

set	设置 USBKey 参数。
uktype	指定 USBKey 型号。
epass1000||none	网关目前支持 epass1000
pin	指定 USBKey 的 PIN 码。
string	字符串

使用说明：

1）PIN码必须正确输入。如果PIN码输入错误，在USBKey使用中将会多次尝试用错误的PIN码。当错误次数过多（一般为 16 次），USBKey将会自锁，必须对其进行初始化方能正常使用。

2）首先必须设定USBKey相关参数才可以导出客户端证书和私钥到USBKey中。导出客户端证书和私钥请参见localca clientcert的writeukey 命令。

实例：

**设置USBKey型号为epass1000，PIN码为 00000000。

usb set uktype *epass1000* **pin** *00000000*

usb show<cr>

命令描述：

查看 USBKey 参数设置。

webuicert

以 pkcs12 文件方式导入 webui 证书。

webuicert getbypkcs12 certfile <*string*> [**passwd**<*string*>]

命令描述：

以 pkcs12 文件方式导入 webui 证书。

参数说明：

getbypkcs12	以 pkcs12 文件方式导入 webui 证书
certfile	指定 pkcs12 证书文件名
string	字符串
passwd	指定打开证书文件的密码
string	字符串

QOS

通过配置 QoS 对象，并且在访问控制规则中引用该策略，网络卫士安全网关可以实现网络带宽的动态管理。对于穿过安全网关的连接，可以在数据传输的上行和下行两个方向上分别进行带宽控制。如果不设置 QoS 对象，管理员也可以通过在访问控制策略中设置“下行限制带宽”对匹配规则的流量进行简单的限制，但是无法保证带宽。

进入本命令模块操作如下：

#qos <cr>

退出本命令模块操作如下：

#end <cr>

CLI 管理员登录安全网关并进入本命令模块后，可以执行相应的组件管理命令。下面将详细描述本命令模块下的所有组件管理命令。命令的实例输入格式将按已经进入本命令模块书写。

下一级命令列表

命令	功能
config	Qos 配置信息查看
monitor	令牌桶查看
rule	带宽规则配置

config

查看 Qos 配置信息。

config aging set <*string*>

命令描述：

设置独享队列的老化时间

参数说明：

aging	独享队列的老化时间
set	设置参数
string	数值，范围为 0-43200，单位为分钟，设置为 0 时表示永不超时。

config aging show <cr>

命令描述：

查看独享队列的老化时间设置

config queuelen set <string>

命令描述：

设置 Qos 队列长度

参数说明：

queuelen	Qos 队列长度
set	设置参数
string	数值，范围为 1-100

config queuelen show <cr>

命令描述：

查看 Qos 队列长度

monitor

QoS 令牌桶查看，主要用于售后服务人员排除故障。

monitor class [**id** <*string*>]

命令描述：

查看 QoS 队列状态。

参数说明：

class	查看 QoS 队列状态
id	可选项，指定队列 ID。不指定该参数时查看所有队列。
string	输入队列 ID 字符串

monitor policy [**id** <*string*>]

命令描述：

查看访问控制规则引用 QoS 对象的情况。

参数说明：

policy	查看访问控制规则引用 QoS 对象的情况
id	可选项，指定队列 ID。不指定该参数时查看所有队列。
string	输入队列 ID 字符串

monitor rule [**name** <*string*>]

命令描述：

查看 QoS 对象运行状况。

参数说明：

rule	查看 QoS 对象运行状况
name	可选项，指定 QoS 对象名。不指定该参数时查看所有对象。
string	字符串

monitor areadev<cr>

命令描述：

查看 QoS 保证区域状况。

monitor freeid [**list**] <cr>

命令描述：

查看 QoS 空闲队列 ID 信息。

monitor idlelist<cr>

命令描述：

查看 QoS 空闲队列。

monitor status <cr>

命令描述：

查看 QoS 运行状态。

rule

安全网关的带宽规则管理，在此用户可以在带宽类下针对不同的服务设置不同的带宽规则。

rule add name <*string1***>** [**down- exclusive-limit** < *string2*>] [**down-exclusive-rate** < *string3*>]

[**down-priority** < 0|1|2|3>] [**down-share-limit** <*string4*>] [**down-share-rate** <*string5*>]

[**up-exclusive -limit <** *string6***>**] [**up-exclusive-rate** < *string7*>] [**up-priority** <0|1|2|3 >]

[**up-share-limit** <string8>] [**up-share-rate** <*string9*>] [**policy-type** < share|exclusive>]

命令描述：

添加一个 QoS 对象。

参数说明：

add	添加 QoS 对象
name	输入对象名
string1	字符串
down- exclusive-limit	下行独享限制带宽(K,M)(Bps)
string2	数值
down-exclusive-rate	下行独享保障带宽(K,M)(Bps)
string3	数值
down-priority	下行优先级
0|1|2|3	数值
down-share-limit	下行共享限制带宽(K,M)(Bps)
string4	数值
down-share-rate	下行共享保障带宽(K,M)(Bps)
string5	数值
up-exclusive -limit	上行独享限制带宽(K,M)(Bps)
string6	数值
up-exclusive-rate	上行独享保障带宽(K,M)(Bps)
string7	数值
up-priority	上行优先级
0|1|2|3	选择优先级。
up-share-limit	上行共享限制带宽(K,M)(Bps)
string8	数值
up-share-rate	上行共享保障带宽(K,M)(Bps)
string9	数值
policy-type	策略的共享属性
share|exclusive	选择共享或独享

使用说明：

设置 Qos 对象时，上行或下行至少设置一种。未指定保障带宽出口时，认为只限制不保障。

rule clean <cr>

命令描述：

清空所有 QoS 对象。

使用说明：

只有当 qos 对象没有被其它对象引用时，才会清除掉。

rule modify name <*string1***> name** <*string1*> [**down- exclusive-limit** < *string2*>] [**down-exclusive-rate** < *string3*>] [**down-priority** < 0|1|2|3 >] [**down-share-limit** <*string4*>] [**down-share-rate** <*string5*>] [**up-exclusive -limit <** *string6***>**] [**up-exclusive-rate** < *string7*>] [**up-priority** <0|1|2|3 >] [**up-share-limit** <string8>] [**up-share-rate** <*string9*>] [**policy-type** < share|exclusive>]

命令描述：

修改 QoS 对象属性。

参数说明：

modify	修改 QoS 对象属性
name	指定对象的名称
string1	字符串
name	输入对象名
string1	字符串
down-exclusive-limit	下行独享限制带宽(K,M)(Bps)
string2	数值
down-exclusive-rate	下行独享保障带宽(K,M)(Bps)
string3	数值
down-priority	下行优先级
0|1|2|3	数值
down-share-limit	下行共享限制带宽(K,M)(Bps)
string4	数值
down-share-rate	下行共享保障带宽(K,M)(Bps)
string5	数值
up-exclusive -limit	上行独享限制带宽(K,M)(Bps)
string6	数值
up-exclusive-rate	上行独享保障带宽(K,M)(Bps)
string7	数值
up-priority	上行优先级
0|1|2|3	选择优先级。
up-share-limit	上行共享限制带宽(K,M)(Bps)
string8	数值
up-share-rate	上行共享保障带宽(K,M)(Bps)
string9	数值
policy-type	策略的共享属性
share|exclusive	选择共享或独享

使用说明：

修改 Qos 对象时， 只能修改上行（下行）保障带宽、上行（下行）限制带宽、上行（下行）优先级。增大保障带宽时可能会受到限制，导致失败。

rule delete name <*string*>

命令描述：

删除一个 QoS 对象。

参数说明：

modify	删除一个 QoS 对象
name	指定要删除的 QoS 对象的名称
string	字符串

使用说明：

只有当 qos 对象没有被其它对象引用时，才能删除掉。

rule show [**name** <*string*>]

命令描述：

查看 QoS 对象。

参数说明：

show	查看 QoS 对象信息
name	可选项，指定要查看的 QoS 对象的名称。不指定该参数时显示所有对象。
string	字符串

SAVE

save <cr>

命令描述：

保存系统配置。

SHOW

显示系统已保存的配置信息。

该命令与 **system config show** 功能一致。

show [nostop]

命令描述：

显示系统已保存的配置信息。

参数说明：

show	显示系统已保存的配置。
nostop	全部输出信息，不分屏显示。

实例：

** 查看已保存的配置。

show<cr>

SHOW_RUNNING

显示系统正在运行的配置信息。

该命令与 **system config show_running** 功能一致。

show_running [nonstop]

命令描述：

显示系统正在运行的配置信息。

参数说明：

show_running	显示系统正在运行的配置。
nostop	全部输出信息，不分屏显示。

使用说明：

当用户直接回车示将分屏显示所有输出，指定 nostop 参数的时候，输出结果不待用户击键确认就全部输出，直至完毕。

实例：

** 查看运行配置。

show_running<cr>

SNMP

本模块中的命令主要用来进行 SNMP 管理的相关配置。

进入本命令模块操作如下：

snmp<cr>

退出本命令模块操作如下：

end<cr>

CLI 管理员登录安全网关进入本命令模块后，可以执行相应的组件管理命令。下面将详细描述本命令模块下的所有组件管理命令。本模块下命令实例的输入格式将按已经进入本命令模块书写。

下一级命令列表

命令	功能
managehost	配置 SNMP 管理主机对象。
managesubnet	配置 SNMP 管理子网对象。
set	设置设备的联系方式和信息。
show	查看 SNMP 配置信息
snmpv3user	配置 SNMPV3 用户对象。
start	启动设备的 SNMP 应用。
stop	停止设备的 SNMP 应用。
traphost	配置 SNMP 陷阱主机对象。

managehost

该组命令用于配置和管理 SNMP 管理主机对象。

managehost add name <*string1*> **hostip** <*ipaddress*> **community** <*string2*>

命令描述：

本命令用于增加 SNMP 管理主机对象。

参数说明：

add	增加 SNMP 管理主机对象。
name	指定 SNMP 管理主机对象的名称。
string1	字符串，输入新增 SNMP 管理主机对象的名称。
hostip	指定 SNMP 管理主机对象的 IP 地址。

ipaddress	标准的 IP 地址字符串，输入要增加的管理主机对象的 IP 地址。
community	指定 SNMP 管理主机访问安全网关时的团体名。 说明： 1. SNMP V1/V2 支持团体名认证方案，与安全网关认可的团体名不符的 SNMP 报文将被丢弃。 2. 目前系统只支持管理主机的只读访问模式，不支持设置操作。
string2	字符串，输入团体名。

使用说明：

如果需要使用 SNMP 管理网络卫士安全网关，必须对 SNMP 管理主机开放 SNMP 服务。

实例：

** 增加一个 SNMP 管理主机对象，名称为“manage_host1”，IP 地址为“192.168.83.234”，访问安全网关的团体名为“community1”。

managehost add name *manage_host1* **hostip** *192.168.83.234* **community** *community1*

managehost delete name <*string*>

命令描述：

本命令用于删除 SNMP 管理主机对象。

参数说明：

delete	删除 SNMP 管理主机对象。
name	指定 SNMP 管理主机对象的名称。
string	字符串，输入要删除的 SNMP 管理主机对象的名称。

实例：

** 删除名称为“manage_host1”的 SNMP 管理主机对象。

Managehost delete name *manage_host1*

managehost show <cr>

命令描述：

本命令用于显示所有的 SNMP 管理主机对象。

managehost clean <cr>

命令描述：

本命令用于清除所有的 SNMP 管理主机对象。

managesubnet

该组命令用于配置和管理 SNMP 管理子网对象。

managesubnet add name <*string1*> **subnet** <*string2*> **community** <*string3*>

命令描述：

本命令用于增加 SNMP 管理子网对象。

参数说明：

add	增加 SNMP 管理子网对象。
name	指定 SNMP 管理子网对象的名称。
string1	字符串，输入新增 SNMP 管理子网对象的名称。
subnet	指定 SNMP 管理子网对象的地址。
string2	设定子网地址及子网掩码，格式为 x.x.x.x/x。
community	指定 SNMP 管理子网访问安全网关时的团体名。 说明： 1. SNMP V1/V2 支持团体名认证方案，与安全网关认可的团体名不符的 SNMP 报文将被丢弃。 2. 目前系统只支持管理子网的只读访问模式，不支持设置操作。
string3	字符串，输入团体名。

使用说明：

无。

实例：

** 增加一个 SNMP 管理子网对象，名称为“manage_subnet1”，子网地址为“192.168.83.0”，子网掩码为“255.255.255.0”，访问安全网关的团体名为“community2”。

managehost add name *manage_subnet1* **subnet** *192.168.83.0/24* **community** *community2*

managesubnet delete name <*string*>

命令描述：

本命令用于删除 SNMP 管理子网对象。

参数说明：

delete	删除 SNMP 管理子网对象。
name	指定 SNMP 管理子网对象的名称。
string	字符串，输入要删除的 SNMP 管理子网对象的名称。

实例：

** 删除名称为“manage_subnet1”的 SNMP 管理子网对象。

Managesubnet delete name *manage_subnet1*

managesubnet show <cr>

命令描述：

本命令用于显示所有的 SNMP 管理子网对象。

managesubnet clean <cr>

命令描述：

本命令用于清除所有的 SNMP 管理子网对象。

set

配置联系方式。

set location <*string*>

命令描述：

设置启用了 SNMP Agent 的设备的位置。

参数说明：

location	设置启用了 SNMP Agent 的设备的位置。
string	字符串。

set contact <*string*>

命令描述：

当设备启用了 SNMP Agent 后，设置管理这个设备的联系人信息。

参数说明：

contact	当设备启用了 SNMP Agent 后，设置管理这个设备的联系人信息。
string	字符串。

set agent-dev<*string*>

命令描述：

代理地址设置

参数说明：

agent-dev	代理地址设置
string	字符串。

show

查看 SNMP 配置和运行状态信息。

show <config| status>

命令描述：

本命令用于查看 SNMP 配置和运行状态信息。

参数说明：

show	查看 SNMP 配置和运行状态信息
config	查看 SNMP 配置信息
status	查看 SNMP 运行状态信息

实例：

** 查看 SNMP 配置信息。

show config

snmpv3user

该组命令用于配置 SNMPV3 用户对象。

snmpv3user add name <*string*> **authpass** <*string*> **privpass** <*string*> **securitylevel** <authnopriv|authpriv >

命令描述：

本命令用于增加 SNMPV3 用户对象。

参数说明：

add	增加 SNMPV3 用户对象。
name	指定 SNMPV3 用户对象的名称。
string	字符串，输入新增 SNMPV3 用户对象的名称。
authpass	指定 SNMPV3 用户对象进行认证时使用的密码，加密方式为 MD5。 说明： 必须为 8 位字符。
string	字符串，输入 SNMPV3 用户对象的认证密码。
privpass	私有密码，指定消息加密时使用的密码，加密方式为 DES。 说明： 必须为 8 位字符。
string	字符串，输入消息加密使用的密码。
securitylevel	设置安全级别
authnopriv|authpriv	不加密|加密

实例：

** 增加一个 SNMPV3 用户对象，用户名称为“v3_user1”，认证密码为“11111111”，私有密码为“22222222”，加密。

snmpv3user add name *v3_user1* **authpass** *11111111* **privpass** *22222222* **securitylevel** authpriv

snmpv3user delete name <*string*>

命令描述：

本命令用于删除 SNMPV3 用户对象。

参数说明：

delete	删除 SNMPV3 用户对象。

name	指定 SNMPV3 用户对象的名称。
string	字符串，输入要删除的 SNMPV3 用户对象的名称。

实例：

** 删除名称为“v3_user1”的 SNMPV3 用户对象。

snmpv3user delete name *v3_user1*

snmpv3user show <*cr*>

命令描述：

本命令用于显示所有的 SNMPV3 用户对象。

snmpv3user clean <*cr*>

命令描述：

本命令用于清除所有的 SNMPV3 用户对象。

start

命令描述：

该命令用于启动设备的 SNMP 应用。

start <cr>

stop

命令描述：

该命令用于停止设备的 SNMP 应用。

stop<cr>

traphost

该组命令用于配置陷阱主机对象，以接收安全网关发送的 SNMP Trap 消息。当管理主机具有 Trap 接收功能时，管理主机和陷阱主机可以是同一台主机。

traphost add name <*string*> **hostip** <*ipaddress*>

命令描述：

本命令用于增加陷阱主机对象。

参数说明：

add	增加陷阱主机对象。
name	指定陷阱主机对象的名称。
string	字符串，输入要增加的陷阱主机对象的名称。
hostip	指定陷阱主机的 IP 地址。
ipaddress	标准的 IP 地址字符串，输入要要增加的陷阱主机对象的 IP 地址。

使用说明：

当管理主机具有 Trap 接收功能时，管理主机和陷阱主机可以是同一台主机。

实例：

** 增加一个陷阱主机对象，名称为“trap_host1”，陷阱主机的 IP 地址为“192.168.83.223”。

traphost add name *trap_host1* **hostip** *192.168.83.223*

traphost delete name <*string*>

命令描述：

本命令用于删除陷阱主机对象。

参数说明：

delete	删除陷阱主机对象。
name	指定陷阱主机对象的名称。
string	字符串，输入要删除的陷阱主机对象的名称。

实例：

** 删除名称为“trap_host1”的陷阱主机对象。

traphost delete name *trap_host1*

traphost show<*cr*>

命令描述：

本命令用于显示所有的陷阱主机对象。

traphost clean<*cr*>

命令描述：

本命令用于清除所有的陷阱主机对象。

SYSTEM

本命令用来配置网络卫士安全网关的基本信息，如版本显示、时钟管理、NTP 设置、系统配置管理、系统升级、认证用户管理、管理员信息、安全网关重新启动命令等。

进入本命令模块操作如下：

system <cr>

退出本命令模块操作如下：

exit <cr>

CLI 管理员登录安全网关进入本命令模块后，可以执行相应的组件管理命令。下面将详细描述本命令模块下的所有组件管理命令。命令的实例输入格式将按已经进入本命令模块书写。

下一级命令列表

命令	功能
admin-auth-mode	认证类型配置
admininfo	安全网关设备管理员配置
authset	认证参数信息设置
config	系统配置管理
devname	系统名称管理
flash	病毒库删除命令
mail-forward	全局邮件转发参数配置
hd-check	检测系统硬盘
hd-rebuild	系统硬盘重新格式化
httpd	HTTP 服务管理
information	当前设备状态信息

killprocess	结束指定进程运行
monitord	监控服务管理
netflow	netflow 对象
netflow-filter	显示 netflow 过滤条件
netstat	netstat 命令设置
ntp	安全网关设备系统时间设置
probe-package	设备探测报文配置
probe-server-time	设备探测服务器切换时间配置
probe-show	显示服务器负载均衡参数
probe-time	设备探测时间间隔配置
reboot	重新启动系统
service	安全网关系统服务配置
showprocess	显示当前进程信息
shutdown	关闭系统
sshd	SSH 服务管理
tcpdump	TCPDUMP 命令
telnetd	用于 telnet 服务管理
terminal	终端空闲超时设置
time	系统时钟管理
top-policy	top-policy 服务器配置管理
traceroute	TRACEROUTE 命令
update	系统升级
uptime	系统启动后运行的总时间
vdcd	vdcd 进程
version	系统版本信息
vs	显示虚拟系统信息
webui	WebUI 管理设置

admin-auth-mode

设置认证类型

admin-auth-mode <local|outside>

命令描述：

设置认证类型。

参数说明：

admin-auth-mode	设置认证类型
local|outside	Local：表示本地认证；outside：外部认证。

admininfo

管理员信息配置：网络卫士安全网关支持多个管理员对其进行操作管理。不同的管理员有不同的操作权限类型：安全审计、安全管理、虚系统管理员、分级管理员，以及具有模板权限的管理员。在此可以设定管理员的权限和登录密码。

admininfo add <cr>

Input manager's name:<*string*>

New password:<*string*>

Re_enter password: <*string*>

Choose manager's privilege [audit | config | vs |template |grade]:

assign the template[y/n]：<y|n>

Input the template name: <*string*>

input the comment[y/n]: <y|n>

input the comment: <*string*>

命令描述：

增加设备管理员信息：名称、密码、权限信息。

参数说明：

add	增加设备管理员
Input manager's name:	设备管理员名称
string	名称字符串
New password:	设定密码
string	密码字符串，密码由数字和小写字母组成且大于等于 8 位，小于等于 31 位。
Re_enter password:	再次输入密码
string	字符串，必须和 **New password:**后设置相同的字符串。
Choose manager's privilege:	设定管理员权限
audit|config|vs|template|grade	audit：安全审计；审计用户只有查看配置的权限，不能修改配置。 config：安全管理；管理用户是指对网络卫士安全网关具有管理权限（但不能修改管理员配置）的用户。 vs：虚拟系统管理。虚系统用户则只能登录网络卫士安全网关上指定的虚系统。还需要在 Input the vsid [1-254]:后指定所属的虚系统号

	vsid。 template：超级管理员在“管理权限”处设置的权限模板。还需要在assign the template[y/n]:后选择y或n。如果选择y，还需要在Input the template name:后输入模板名称。 grade：分级管理用户，只具备查看和修改由该管理员本身创建的用户的权限。
Input the vsid [1-254]:	指定所属的虚系统号 vsid。
string	数值，范围为 1-254.
assign the template[y/n]	仅当权限选择 template 时需要设置该参数，设置是否在此设置所属的权限模板。
y/n	是/否
Input the template name:	输入模板名称
String	字符串
input the comment[y/n]:	描述
y|n	是否描述
input the comment:	输入描述信息
string	描述内容

使用说明：

当管理员为安全管理权限时，登录命令行界面后，命令提示符为“%”。

当管理员为安全审计权限时，登录命令行界面后，命令提示符更换为“**$**”。

当管理员为虚系统管理员时，只能通过 WEBUI 界面登录，无法通过命令行界面登录。

admininfo modify <cr>

Input manager's name: *string*

Modify the name(only super admin's name can be changed)[y/n]: [y/n]

Input new name: *string*

New password: *string*

Re_enter password: *string*

Modify the privilege[y/n]: [y/n]

Choose manager's privilege[audit | config | vs | template | grade]:

Modify the vsid[y/n]: [y/n]

Input vsid[1-254]:*number*

Modify the template[y/n]：<y|n>

Input the template name: <*string*>

Modify the comment[y/n]: [y/n]

Input the comment: *string*

命令描述：

修改某系统管理员的信息：描述信息、名称、口令、权限、所属虚系统。

参数说明：

modify	修改设备管理员信息
Input manager's name:	设备管理员名称
string	名称字符串
Modify the name(only super admin's name can be changed)[y/n]:	设置是否修改用户名
y/n	是、否
Input new name:	输入新名称
string	字符串
New password:	设定密码
string	密码字符串
Re_enter password:	再次输入密码
string	字符串，必须和 **New password:**后设置相同的字符串。
Choose manager's privilege:	设定管理员权限
audit|config|vs|template|grade	audit：安全审计；审计用户只有查看配置的权限，不能修改配置。 config：安全管理；管理用户是指对网络卫士安全网关具有管理权限（但不能修改管理员配置）的用户。 vs：虚拟系统管理。虚系统用户则只能登录网络卫士安全网关上指定的虚系统。还需要在Input the vsid [1-254]:后指定所属的虚系统号vsid。 template：超级管理员在“管理权限”处设置的权限模板。还需要在assign the template[y/n]:后选择y或n。如果选择y，还需要在Input the template name:后输入模板名称。 grade：分级管理用户，只具备查看和修改由该管理员本身创建的用户的权限。
Modify the vsid[y/n]	设置是否修改虚拟系统号
y/n	是/否
Input the vsid [1-254]:	指定所属的虚系统号 vsid。
string	数值，范围为 1-254.
Modify the template[y/n]	仅当权限选择 template 时需要设置该参数，设置是否在此修改所属的权限模板。

y/n	是/否
Input the template name:	输入模板名称
String	字符串
Modify the comment[y/n]:	是否修改描述信息
y|n	是、否
input the comment:	输入描述信息
string	描述内容

使用说明：

只有超级管理员可以修改管理员名称。

admininfo delete_db_manager name <*string*>

命令描述：

删除数据库中某管理员的信息。

参数说明：

delete_db_manager	删除数据库中某管理员的信息
name	设备管理员名称
string	名称字符串

实例：

** 删除名称为 test 的管理员

admininfo delete_db_manager name *test*

admininfo password <cr>

Modify the password[y/n]:<y|n>

New password: < *string*>

Re_enter password:< *string*>

命令描述：

修改管理员口令。

admininfo showdb <cr>

命令描述：

显示数据库中管理员名称、权限、注释等。

admininfo showonline <cr>

命令描述：

显示在线管理员名称、登录地点、在线时间。

实例：

** 查看在线管理员

admininfo showonline<cr>

** 显示所有管理员信息

Manager_name	Auth_address	Privilege	Online_time(hh:mm:ss)
superman	192.168.83.231	audit/config	0:0:17
superman	127.0.0.1	audit/config	0:0:2

admininfo status-set name <*string***> status** <enable|disable>

命令描述：

设置管理员状态

参数说明：

status-set	设置管理员状态
name	设备管理员名称
string	名称字符串
status	设置是否启用该管理员
enable|disable	启用/禁用

admininfo status-show name <*string***>**

命令描述：

查看管理员状态

参数说明：

status-show	查看管理员状态
name	指定管理员名称
string	名称字符串

admininfo template-add name <*string*> [**desc** < *string*>] [**sys-setup** < read|write|disable>] [**sys-maintainance** < read|write|disable>] [**network** < read|write|disable>] [**aaa** < read|write|disable>] [**pki** < read|write|disable>] [**resource** < read|write|disable|>] [**dpi** < read|write|disable|>] [**ips** < read|write|disable>] [**policy** < read|write|disable>] [**vpn** < read|write|disable>] [**sslvpn** < read|write|disable>] [**log-config** < read|write|disable>] [**log-access** < read|write|disable>] [**anti-virus** < read|write|disable>] [**anti-spam** <read|write|disable>] [**ha** < read|write|disable>]

[**sys-moniter** < read|write|disable|>]

命令描述：

设置管理权限。

参数说明：

template-add	设置管理权限
name	输入权限名称
string	字符串
desc	可选项，输入描述信息。
string	字符串
sys-setup	系统设置权限。可选项，默认不具有该模块设置及查看权限。
read|write|disable	读/写/无。默认为无。 说明： “无”，表示不具有该模块的设置及查看权限。 “读”，表示具有查看该模块设置的权限。 “写”，表示具有该模块的设置的所有权限。
sys-maintainance	系统维护权限。可选项，默认不具有该模块设置及查看权限。
read|write|disable	读/写/无。 说明： “无”，表示不具有该模块的设置及查看权限。 “读”，表示具有查看该模块设置的权限。 “写”，表示具有该模块的设置的所有权限。
network	网络模块。可选项，默认不具有该模块设置及查看权限。
read|write|disable	读/写/无。 说明： “无”，表示不具有该模块的设置及查看权限。 “读”，表示具有查看该模块设置的权限。 “写”，表示具有该模块的设置的所有权限。
aaa	认证模块。可选项，默认不具有该模块设置及查看权限。
read|write|disable	读/写/无。 说明： “无”，表示不具有该模块的设置及查看权限。 “读”，表示具有查看该模块设置的权限。 “写”，表示具有该模块的设置的所有权限。
pki	PKI 模块。可选项，默认不具有该模块设置及查看权限。
read|write|disable	读/写/无。 说明： “无”，表示不具有该模块的设置及查看权限。 “读”，表示具有查看该模块设置的权限。 “写”，表示具有该模块的设置的所有权限。
resource	资源模块。可选项，默认不具有该模块设置及查看权限。
read|write|disable	读/写/无。 说明： “无”，表示不具有该模块的设置及查看权限。 “读”，表示具有查看该模块设置的权限。 “写”，表示具有该模块的设置的所有权限。

dpi	深度内容检测模块。可选项，默认不具有该模块设置及查看权限。
read|write|disable	读/写/无。 说明： “无”，表示不具有该模块的设置及查看权限。 “读”，表示具有查看该模块设置的权限。 “写”，表示具有该模块的设置的所有权限。
ips	IPS 模块。可选项，默认不具有该模块设置及查看权限。
read|write|disable	读/写/无。 说明： “无”，表示不具有该模块的设置及查看权限。 “读”，表示具有查看该模块设置的权限。 “写”，表示具有该模块的设置的所有权限。
policy	安全策略。可选项，默认不具有该模块设置及查看权限。
read|write|disable	读/写/无。 说明： “无”，表示不具有该模块的设置及查看权限。 “读”，表示具有查看该模块设置的权限。 “写”，表示具有该模块的设置的所有权限。
vpn	IPSecVPN 模块。可选项，默认不具有该模块设置及查看权限。
read|write|disable	读/写/无。 说明： “无”，表示不具有该模块的设置及查看权限。 “读”，表示具有查看该模块设置的权限。 “写”，表示具有该模块的设置的所有权限。
sslvpn	SSL VPN 模块。可选项，默认不具有该模块设置及查看权限。
read|write|disable	读/写/无。 说明： “无”，表示不具有该模块的设置及查看权限。 “读”，表示具有查看该模块设置的权限。 “写”，表示具有该模块的设置的所有权限。
log-config	日志设置模块。可选项，默认不具有该模块设置及查看权限。
read|write|disable	读/写/无。 说明： “无”，表示不具有该模块的设置及查看权限。 “读”，表示具有查看该模块设置的权限。 “写”，表示具有该模块的设置的所有权限。
Log-accsee	日志访问模块。可选项，默认不具有该模块设置及查看权限。
read|write|disable	读/写/无。 说明： “无”，表示不具有该模块的设置及查看权限。 “读”，表示具有查看该模块设置的权限。 “写”，表示具有该模块的设置的所有权限。
anti-virus	病毒模块。可选项，默认不具有该模块设置及查看权限。
read|write|disable	读/写/无。 说明：

	“无”，表示不具有该模块的设置及查看权限。 “读”，表示具有查看该模块设置的权限。 “写”，表示具有该模块的设置的所有权限。
anti-spam	反垃圾邮件模块。可选项，默认不具有该模块设置及查看权限。
read|write|disable	读/写/无。 说明： “无”，表示不具有该模块的设置及查看权限。 “读”，表示具有查看该模块设置的权限。 “写”，表示具有该模块的设置的所有权限。
ha	高可用性模块。可选项，默认不具有该模块设置及查看权限。
read|write|disable	读/写/无。 说明： “无”，表示不具有该模块的设置及查看权限。 “读”，表示具有查看该模块设置的权限。 “写”，表示具有该模块的设置的所有权限。
sys-moniter	系统监视模块。可选项，默认不具有该模块设置及查看权限。
read|write|disable	读/写/无。 说明： “无”，表示不具有该模块的设置及查看权限。 “读”，表示具有查看该模块设置的权限。 “写”，表示具有该模块的设置的所有权限。

admininfo template-delete name <*string*>

命令描述

删除管理权限

admininfo template-clean <cr>

命令描述

清空所有管理权限

admininfo template-show <cr>

命令描述

查看所有管理权限

admininfo template-modify [**desc** < *string*>] [**sys-setup** < read|write|disable>] [**sys-maintainance** < read|write|disable>] [**network** < read|write|disable>] [**aaa** < read|write|disable>]

[**pki** < read|write|disable>] [**resource** < read|write|disable|>] [**dpi** < read|write|disable|>] [**ips** < read|write|disable>] [**policy** < read|write|disable>] [**vpn** < read|write|disable>] [**sslvpn** < read|write|disable>] [**log-config** < read|write|disable>] [**log-access** < read|write|disable>] [**anti-virus** < read|write|disable>] [**anti-spam** <read|write|disable>] [**ha** < read|write|disable>][**sys-moniter** < read|write|disable|>]

命令描述：

修改管理权限属性。

参数说明：

template-modify	修改管理权限属性
name	输入权限名称
string	字符串
desc	可选项，输入描述信息。
string	字符串
sys-setup	系统设置权限。可选项，默认不具有该模块设置及查看权限。
read|write|disable	读/写/无。默认为无。 说明： “无”，表示不具有该模块的设置及查看权限。 “读”，表示具有查看该模块设置的权限。 “写”，表示具有该模块的设置的所有权限。
sys-maintainance	系统维护权限。可选项，默认不具有该模块设置及查看权限。
read|write|disable	读/写/无。 说明： “无”，表示不具有该模块的设置及查看权限。 “读”，表示具有查看该模块设置的权限。 “写”，表示具有该模块的设置的所有权限。
network	网络模块。可选项，默认不具有该模块设置及查看权限。
read|write|disable	读/写/无。 说明： “无”，表示不具有该模块的设置及查看权限。 “读”，表示具有查看该模块设置的权限。 “写”，表示具有该模块的设置的所有权限。
aaa	认证模块。可选项，默认不具有该模块设置及查看权限。
read|write|disable	读/写/无。 说明： “无”，表示不具有该模块的设置及查看权限。 “读”，表示具有查看该模块设置的权限。 “写”，表示具有该模块的设置的所有权限。
pki	PKI 模块。可选项，默认不具有该模块设置及查看权限。
read|write|disable	读/写/无。 说明： “无”，表示不具有该模块的设置及查看权限。 “读”，表示具有查看该模块设置的权限。

	“写”，表示具有该模块的设置的所有权限。
resource	资源模块。可选项，默认不具有该模块设置及查看权限。
read|write|disable	读/写/无。 说明： “无”，表示不具有该模块的设置及查看权限。 “读”，表示具有查看该模块设置的权限。 “写”，表示具有该模块的设置的所有权限。
dpi	深度内容检测模块。可选项，默认不具有该模块设置及查看权限。
read|write|disable	读/写/无。 说明： “无”，表示不具有该模块的设置及查看权限。 “读”，表示具有查看该模块设置的权限。 “写”，表示具有该模块的设置的所有权限。
ips	IPS 模块。可选项，默认不具有该模块设置及查看权限。
read|write|disable	读/写/无。 说明： “无”，表示不具有该模块的设置及查看权限。 “读”，表示具有查看该模块设置的权限。 “写”，表示具有该模块的设置的所有权限。
policy	安全策略。可选项，默认不具有该模块设置及查看权限。
read|write|disable	读/写/无。 说明： “无”，表示不具有该模块的设置及查看权限。 “读”，表示具有查看该模块设置的权限。 “写”，表示具有该模块的设置的所有权限。
vpn	IPSecVPN 模块。可选项，默认不具有该模块设置及查看权限。
read|write|disable	读/写/无。 说明： “无”，表示不具有该模块的设置及查看权限。 “读”，表示具有查看该模块设置的权限。 “写”，表示具有该模块的设置的所有权限。
sslvpn	SSL VPN 模块。可选项，默认不具有该模块设置及查看权限。
read|write|disable	读/写/无。 说明： “无”，表示不具有该模块的设置及查看权限。 “读”，表示具有查看该模块设置的权限。 “写”，表示具有该模块的设置的所有权限。
log-config	日志设置模块。可选项，默认不具有该模块设置及查看权限。
read|write|disable	读/写/无。 说明： “无”，表示不具有该模块的设置及查看权限。 “读”，表示具有查看该模块设置的权限。 “写”，表示具有该模块的设置的所有权限。
Log-accsee	日志访问模块。可选项，默认不具有该模块设置及查看权限。
read|write|disable	读/写/无。

	说明： “无”，表示不具有该模块的设置及查看权限。 “读”，表示具有查看该模块设置的权限。 “写”，表示具有该模块的设置的所有权限。
anti-virus	病毒模块。可选项，默认不具有该模块设置及查看权限。
read|write|disable	读/写/无。 说明： “无”，表示不具有该模块的设置及查看权限。 “读”，表示具有查看该模块设置的权限。 “写”，表示具有该模块的设置的所有权限。
anti-spam	反垃圾邮件模块。可选项，默认不具有该模块设置及查看权限。
read|write|disable	读/写/无。 说明： “无”，表示不具有该模块的设置及查看权限。 “读”，表示具有查看该模块设置的权限。 “写”，表示具有该模块的设置的所有权限。
ha	高可用性模块。可选项，默认不具有该模块设置及查看权限。
read|write|disable	读/写/无。 说明： “无”，表示不具有该模块的设置及查看权限。 “读”，表示具有查看该模块设置的权限。 “写”，表示具有该模块的设置的所有权限。
sys-moniter	系统监视模块。可选项，默认不具有该模块设置及查看权限。
read|write|disable	读/写/无。 说明： “无”，表示不具有该模块的设置及查看权限。 “读”，表示具有查看该模块设置的权限。 “写”，表示具有该模块的设置的所有权限。

authset

认证用户管理：管理员可以通过设置系统参数规定同一管理员的最大登录失败次数，以及并发管理数和管理登录地点。一旦某个管理员的登录失败次数超过设定数值，系统将对其进行登陆锁定，从而防止非法用户通过暴力破解的方式登录到网络卫士安全网关。

进入本命令模块操作如下：

authset <cr>

退出本命令模块操作如下：

exit <cr>

authfail

设置最大验证失败相关参数。

authfail set maxnum <*number*>

命令描述：

设置最大验证失败次数。

参数说明：

set maxnum	设置系统名称
number	数值，范围 1-10。

实例：

**设置最大验证失败数为 5

authfail set maxnum *5*

authfail show <cr>

命令描述：

显示最大验证失败次数。

实例：

**显示最大验证失败次数

authfail show<cr>

The max auth fail number is:5

config

config show<cr>

命令描述：

查看当前认证相关配置。

faillock

设置认证失败锁定时间相关参数。

faillock set time<*number*>

命令描述：

设置认证失败锁定时间。

参数说明：

set time	设置认证失败锁定时间
number	数值，范围 60-3600，单位：秒。

实例：

**设置认证失败锁定时间 60s

faillock set time *60*

faillock show<cr>

命令描述：

显示认证失败锁定时间。

实例：

**显示认证失败锁定时间

faillock show<cr>

The auth fail lock_time is:60

get-lostinfo

设置是否允许用户获取丢失信息

get-lostinfo set type [disable|mail|message]

命令描述：

设置用户获取丢失信息的方式

参数说明：

set type	设置用户获取丢失信息的方式

disable|mail|message	不允许/通过 Email 获取/通过消息获取

get-lostinfo show <cr>

命令描述：

查看用户获取丢失信息的设置

managermaxlogin

设置所有管理员最大并发管理数。

managermaxlogin set maxnum<*number*>

命令描述：

设置所有管理员最大并发管理数。

参数说明：

set maxnum	设置所有管理员最大并发管理数
number	数值，范围 1-32

实例：

**设置所有管理员最大并发管理数为 16

managermaxlogin set maxnum *16*

managermaxlogin Show<cr>

命令描述：

显示所有管理员最大并发管理数。

实例：

** 显示所有管理员最大并发管理数

managermaxlogin show<cr>

The max location of manager is:16

maxonlineadm

设置在线管理员的最大数目。

maxonlineadm set maxnum<*number*>

命令描述：

设置在线管理员的最大数目。

参数说明：

set maxnum	设置在线管理员的最大数目
number	数值，范围 1-256。

实例：

**设置最大在线管理员数为 8

maxonlineadm set maxnum *8*

maxonlineadm show<cr>

命令描述：

显示最大在线管理员数。

实例：

** 显示最大在线管理员数

maxonlineadm show<cr>

The max online manager number is:8

manager-login-number

管理员登录图形验证码设置

manager-login-number set status <on|off>

命令描述：

设置管理员登录时是否显示图形验证码。

manager-login-number show <cr>

命令描述：

查看管理员登录图形验证码设置

passwd-policy

口令策略管理。

passwd-policy set-user policy < weak|medium|strong> **first-login** < yes|no> **min-length** < *number*> **timeout** < *number*>

命令描述：

设置普通用户的口令策略。

参数说明：

set-user	设置普通用户的口令策略
policy	设置口令强度
weak|medium|strong	弱/中等/强
first-login	第一次登陆是否必须修改密码
yes|no	是/否
min-length	设置口令最小必须包含的字符数。可选项
number	数值，为 6 到 31。
timeout	设置口令的有效期限。
number	数值，默认为 0，输入范围为 30 到 90。0 表示永不过时。单位为天。

passwd-policy set-manager policy < weak|medium|strong> **min-length** < *number*>

命令描述：

设置管理员的口令策略。

参数说明：

set-manager	设置管理员的口令策略
policy	设置口令强度
weak|medium|strong	弱/中等/强
min-length	设置口令最小必须包含的字符数。可选项
number	数值，为 6 到 31。

passwd-policy show < cr>

命令描述：

查看口令策略。

passwd-type

设置用户密码输出类型。

passwd-type set type [plain | cipher]

命令描述：

设置用户密码类型。

参数说明：

set type	设置用户密码类型
plain	密码类型为明文
cipher	密码加密输出

实例：

**设置用户密码输出类型为加密

passwd-type set type cipher

passwd-type show<cr>

命令描述：

显示用户密码输出类型。

实例：

** 显示用户密码输出类型

passwd-type show<cr>

system authconfig passwd-type cipher

setdefault

设置所有认证参数为默认值。

setdefault <cr>

设置所有认证参数为默认值。

命令描述：

设置所有认证参数为默认值。

secpolicy-set

安全检测策略设置。安全检查用于设置可信检查的策略，即设置在认证的时候就进行可信检查，还是在认证成功后定期进行可信检查。

secpolicy-set set before <on|off> **after** <on|off> **after-timer** <*number*>

命令描述：

设置安全检测策略。

参数说明：

set	设置策略。
before	设置是否进行登录前检查，即在认证的时候就进行可信检查。
on|off	on 表示“是”；off 表示“否”；
after	设置是否在认证成功后定期进行可信检查。
on|off	on 表示“是”；off 表示“否”；
after-timer	设置定时检查的时间间隔。
number	数值

secpolicy-set show <cr>

命令描述：

查看安全检测策略设置。

timeout

设置保活超时时间。

timeout set num <*number*>

命令描述：

设置保活超时时间。

参数说明：

set num	设置保活超时时间。
number	时间长度，单位为秒，范围 10-3600。

实例：

**设置保活超时时间为 60 秒。

timeout set num *60*

timeout show<cr>

命令描述：

显示保活超时时间。

实例：

** 显示保活超时时间

timeout show<cr>

system authconfig timeout set num 100

usermaxlogin

设置同一用户最大登录相关参数。

usermaxlogin set maxnum <*number*>

命令描述：

设置同一用户最大登录数。

参数说明：

set maxnum	设置同一用户最大登录数
number	数值，范围 1-2000。

实例：

**设置同一用户最大登录数为 4

usermaxlogin set maxnum *4*

usermaxlogin show<cr>

命令描述：

显示系统设置的最大同时在线用户数。

实例：

**显示系统设置的最大同时在线用户数

usermaxlogin show<cr>

system authset usermaxlogin set maxnum 10

config

系统配置管理。

config implement [**vsid** <*number*>]

命令描述：

使系统新增加的配置立即生效。

参数说明：

implement	使系统新增加的配置立即生效
vsid	可选项，指定虚系统 ID 号，默认为 0。范围为 0-254。
number	数值。

使用说明：

本操作使新增的配置信息立即在设备上发挥作用，但并没有保存。如果下次启动安全网关时仍需应用这些配置信息，则需要进行保存配置操作。

实例：

** 使虚系统 1 系统新增加的配置生效

config implement vsid *1*

config reset<cr>

命令描述：

加载默认配置.

实例：

** 加载设备的默认配置

config reset<cr>

config save<cr>

命令描述：

保存系统当前配置。

实例：

**保存系统当前配置

config save<cr>

** 提示成功

save config success.

config show<cr>

命令描述：

显示系统以前保存的配置。

使用说明：

显示以前进行 save 操作保存后的配置信息。如果系统正在运行的某些配置信息没有进行 save 操作，该操作将无法显示此类信息。

实例：

**显示系统以前保存的配置

config show<cr>

** 显示具体配置信息

system devname set TopsecOS

network start

network reset

ID 7000 network attribute add name eth2

ID 7001 network attribute add name eth1

ID 7002 network attribute add name eth0

ID 7003 network attribute add name adsl

……

config show_running<cr>

命令描述：

显示系统当前的配置。

使用说明：

显示系统正在运行的配置信息，可以显示还未进行 save 操作的配置信息。使用

show 命令无法显示该类信息。

实例：

**显示系统当前的配置

config show_running<cr>

** 显示具体配置信息

system devname set

TopsecOS

network start

network reset

ID 7000 network attribute add name eth0

ID 7001 network attribute add name eth1

ID 7002 network attribute add name eth2

ID 7003 network attribute add name adsl

ID 7004 network attribute add name ipsec

……

config statistic [**vsid**<*number*>]

命令描述：

显示系统配置信息统计。

参数说明：

satistic	显示系统当前的配置
vsid	虚系统号
number	数值

使用说明：

填写虚系统参数后，将显示该虚系统的配置信息统计。

实例：

** 显示系统配置信息统计

config statistic <cr>

** 统计结果显示

TypeName Number

---

define 18

pf 23

dpi 38

firewall 6

nat 4

avse 0

vpn 0

config show-save-time <cr>

命令描述：

查看配置存盘时间。

config show-backup <cr>

命令描述：

查看备份配置

config show-backup-time <cr>

命令描述：

查看备份配置时间。

config cpoy-save-to-backup <cr>

命令描述：

备份配置文件。

config cpoy- backup-to-save <cr>

命令描述：

恢复备份配置。

config upload-set start host <*ipaddress*> **option** <once|perhour|perday> [**user** <*string*>]

[**password** <*string*>]

命令描述：

配置文件自动上传设置。

参数说明：

upload-set	配置文件上传设置
start	开始上传
host	指定 FTP 服务器 IP 地址
ipaddress	IP 地址字符串
option	定时选项
once|perhour|perday	单次/每小时一次/每天一次
user	可选项，设定 FTP 服务器的用户名
string	字符串
password	可选项，设定 FTP 服务器的用户密码
string	字符串

config upload-set stop<cr>

命令描述：

停止自动上传配置文件。

config upload- show<cr>

命令描述：

查看自动上传配置文件配置。

devname

安全网关的系统名称管理：设备名称在初次使用或管理员未配置时，命令提示符显示为“TopsecOS#”。经过此处配置后，将显示为配置后的设备名称。

devname set <*string*>

命令描述：

设置系统名称。

参数说明：

set	设置系统名称
string	字符串，指定新的设备名称。

实例：

** 修改系统名称为 myname

devname set *myname*

** 当前系统名称变化

myname.system#

devname show <cr>

命令描述：

显示系统名称。

实例：

** 查看当前系统名称

devname show <cr>

** 显示当前系统名称为 TopsecOS

system devname set TopsecOS

flash

病毒库删除命令

flash clean kavengine-base<cr>

mail-forward

全局邮件转发参数配置

mail-forward set account <*string*> **password** <*string*> **sender** <*string*> **server-address** <

s*tring*> **port** < *number*> **dpi-receiver** <*string*>

命令描述：

邮件转发参数设置。

参数说明：

mail-forward	邮件转发参数设置
account	设置发送警告邮件或转发邮件的帐户名。
string	设置帐户名。

password	设置发送警告邮件或转发邮件的发件人密码
string	设置帐号密码。
sender	设置发件人地址
string	设置接收违反规则的转发原邮件的发件人地址，需符合邮件地址格式。
server-address	设置发送警告邮件或转发邮件的邮件帐户的 SMTP 服务器地址或域名
string	设置转发邮件的发件人帐户的 SMTP 服务器地址或域名，地址需符合 IP 地址格式。 说明： 如果服务器配置的地址为域名，管理员一定要在 **#network dns** 处配置安全网关的 DNS 服务器，否则不可能生效。
port	设置转发邮件时的 SMTP 服务器端口号
number	数值
dpi-receiver	设置 DPI 转发邮件时的收件人地址
string	字符串

mail-forward clean <cr>

命令描述：

清除邮件转发参数设置。

mail-forward show<cr>

命令描述：

查看邮件转发参数设置。

mail-forward test-connection<cr>

命令描述：

测试邮件转发参数设置是否正确。

hd-check

检测系统硬盘

hd-check <cr>

命令描述：

检测系统硬盘。

hd-rebuild

系统硬盘重新格式化

hd-rebuild <cr>

命令描述：

系统硬盘重新格式化

httpd

HTTP 服务管理命令。

httpd start<cr>

命令描述：

启动 HTTP 服务。

httpd stop<cr>

命令描述：

停止 HTTP 服务。

information

查看当前设备运行状态信息。

information <cr>

命令描述：

查看当前设备运行状态信息。

实例：

information<cr>

Physical Memory Information:

Total 458324 KB

Free 253944 KB

Free's ratio 55.4%

Buffer 1720 KB

Cache 106116 KB

CPU Load Information:

User 47.5%

System 52.4%

Nice 0.0%

Total Used 100.0%

Idle 0.0%

Session Numbers Information:

Totalnum= 16

Speed(cps)= 1

killprocess

结束指定进程运行

killprocess <*string*>

命令描述：

结束指定进程运行

参数说明：

killprocess	结束指定进程运行
string	字符串，指定进程名。

monitord

监控服务管理命令。

monitord start<cr>

命令描述：

启动监控服务。

monitord stop<cr>

命令描述：

停止监控服务。

netflow

netflow 服务器设置。

netflow set ipaddr <*string1*> **port** <*string2*> **transfer** [enable | disable]

命令描述：

设置 netflow 服务器信息。

参数说明：

netflow set	设置 netflow 服务器信息。
ipaddr	netflow 服务器的 IP 地址，格式为 a.b.c.d
string1	字符串，表示 IP 地址
port	netflow 服务器提供服务的端口号
string2	字符串，表示端口号
transfer	设置是否将流量信息发送到 netflow 服务器
enable|disable	enable 表示发送，disable 表示不发送

实例：

**将流量信息发送到 192.168.4.6 的 netflow 服务器的 9996 端口。

netflow set ipaddr *192.168.4.6* **port** *udp:9996* **transfer** enable

netflow show <*cr*>

命令描述：

显示 netflow 服务器信息。

实例：

**显示 netflow 服务器信息

netflow show <*cr*>

netflow-filter

netflow 过滤规则设置。

netflow-filter add saddr < *string* > **sport** < *string* > **daddr** <*string*> **dport** <*string*> **direction** <client|server|double> **enable** < yes|no|>

命令描述：

添加 netflow 过滤规则。

参数说明：

add	添加 netflow 过滤规则
saddr	设置过滤规则的源地址
string1	字符串，表示源地址对应的地址资源名称。 说明：在设置此规则前，必须先设置相应的地址资源。
sport	设置过滤规则的源端口
string2	字符串，表示源端口对应的服务资源名称。 说明：在设置此规则前，必须先设置相应的服务资源。
daddr	设置过滤规则的目的地址
string3	字符串，表示目的地址对应的地址资源名称。 说明：在设置此规则前，必须先设置相应的地址资源。
dport	设置过滤规则的目的端口
string4	字符串，表示目的端口对应的服务资源名称。 说明：在设置此规则前，必须先设置相应的服务资源。
direction	设置过滤规则的数据流向。
client|server|double	“client”表示从客户端流向服务器端 “server”表示从服务器端流向客户端 “double”表示双向 建议用户通常设置为“double”
enable	是否启用该规则
yes|no	是、否

使用说明：

在设置 netflow 过滤规则之前，请先设置涉及到的地址资源和服务资源。

netflow-filter modify id *number* **saddr** *string1* **sport** *string2* **daddr** *string3* **dport** *string4*

direction [client|server|double] **enable** < yes|no|>

命令描述：

修改 netflow 过滤规则。

参数说明：

modify	修改 netflow 过滤规则
id	指定要修改的过滤规则的 id 号。
number	数值，表示过滤规则的 id 号。
saddr	设置过滤规则的源地址
string1	字符串，表示源地址对应的地址资源名称。 说明：在设置此规则前，必须先设置相应的地址资源。
sport	设置过滤规则的源端口
string2	字符串，表示源端口对应的服务资源名称。 说明：在设置此规则前，必须先设置相应的服务资源。
daddr	设置过滤规则的目的地址
string3	字符串，表示目的地址对应的地址资源名称。 说明：在设置此规则前，必须先设置相应的地址资源。
dport	设置过滤规则的目的端口
string4	字符串，表示目的端口对应的服务资源名称。 说明：在设置此规则前，必须先设置相应的服务资源。
direction	设置过滤规则的数据流向。
client|server|double	“client”表示从客户端流向服务器端 “server”表示从服务器端流向客户端 “double”表示双向 建议用户通常设置为“double”
enable	是否启用该规则
yes|no	是、否

使用说明：

在设置 netflow 过滤规则之前，请先设置涉及到的地址资源和服务资源。

netflow-filter delete id <*numbe>r*

命令描述：

删除 netflow 过滤规则。

参数说明：

modify	删除 netflow 过滤规则
id	指定要删除的过滤规则的 id 号。
number	数值，表示过滤规则的 id 号。

实例：

**删除 id 号为 9 的过滤规则

netflow-filter delete id *9<cr>*

netflow-filter show <cr>

命令描述：

查看 netflow 过滤规则。

实例：

**查看所有 netflow 过滤规则

netflow-filter show*<cr>*

netflow-filter clean <cr>

命令描述：

清空 netflow 过滤规则。

实例：

**清空所有 netflow 过滤规则

netflow-filter clean*<cr>*

netstat

NETSTAT 命令，用于显示网络连接、路由表和网络接口信息，可以 让用户得知目前都有哪些网络连接正在运作。

netstat [a|n|p]

命令描述：

显示网络连接信息。

参数说明：

netstat	显示网络连接信息
a|n|p	a：显示所有 sockets 信息 n：以数字的形式显示所有 sockets 信息 p：显示所有 sockets 的进程号和进程名称

实例：

**显示所有连接信息

netstat a

Active Internet connections (servers and established)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	*:8000	*:*	LISTEN
tcp	0	0	*:4000	*:*	LISTEN
tcp	0	0	*:3232	*:*	LISTEN
tcp	0	0	*:4001	*:*	LISTEN
tcp	0	0	*:3233	*:*	LISTEN
tcp	0	0	*:4002	*:*	LISTEN
tcp	0	0	*:4005	*:*	LISTEN

ntp

NTP（Network Time Protocol）网络时间协议提供了一种时间同步机制，网络卫士安全网关通过使用 NTP 协议并采用优化的同步算法和网络上的 NTP 服务器保持时间同步。这样，网络卫士安全网关就可以和用户网络中的应用服务器、其他安全产品及网络管理系统等保持系统时间的一致，同时为日志审计带来很大的便捷。

ntp start [**ip** <*ipaddress*>] [**ip2** <*ipaddress*>]

命令描述：

当不指定 IP 参数时，启动安全网关作为 NTP 服务器。当指定 IP 参数时，启动安全网关作为 NTP 客户端与 IP 参数设置的 NTP 服务器进行时间同步。

参数说明：

start	启动 NTP 同步
ip	可选项，当安全网关作为 NTP 客户端时，设定 NTP 服务器 IP 地址。
ipaddress	IP 地址，形为 A.B.C.D
Ip2	可选项，当安全网关作为 NTP 客户端时，设定第二个 NTP 服务器 IP 地址。
ipaddress	IP 地址，形为 A.B.C.D

实例：

**启动 NTP 服务，服务器为 172.16.1.23

ntp start ip *172.16.1.23*

**启动安全网关作为 NTP 服务器

ntp start ip <cr>

ntp show <cr>

命令描述：

显示 NTP 的配置信息和状态。

实例：

显示 NTP 的配置信息

ntp show<cr>

NTP Client mode running,ntp server IP: 172.1.1.23

ntp stop <cr>

命令描述：

停止 NTP。

实例：

停止 NTP

ntp stop <cr>

NTP Client mode running,ntp server IP: 172.1.1.23

ntp update ip <*ipaddress*>

命令描述：

安全网关上的时间和 NTP 服务器进行时间同步。

参数说明：

update	安全网关上的时间和 NTP 服务器进行时间同步。
ip	设定 NTP 服务器 IP 地址
ipaddress	IP 地址，形为 A.B.C.D

实例：

**启动 NTP 服务，服务器为 172.16.1.23

ntp update ip *172.16.1.23*

probe-package

设置安全网关向均衡组中的服务器发送探测包的个数。

probe-package set <*number*>

命令描述：

设置设备向均衡组中的服务器发送探测包的个数。

参数说明：

set	设置设备向均衡组中的服务器发送探测包的个数
number	数值，单位为个，范围为 1-8，默认为 1。

实例：

** 设置设备向均衡组中的服务器发送探测包的个数为 5 个

probe-package set *5*

package set is 5

probe-package show <cr>

命令描述：

显示设备向均衡组中的服务器发送探测包的个数。

实例：

** 显示设备向均衡组中的服务器发送 5 个探测包

probe-package show

package set is 5

probe-server-time

设置服务器均衡组之间切换的等待时间。

probe-server-time set<*number*>

命令描述：

设置服务器均衡组之间切换的等待时间。

参数说明：

set	设置服务器均衡组之间切换的等待时间
number	数值，单位为秒，范围为 1-30，默认为 3。

实例：

**设置服务器均衡组之间切换的等待时间为 20 秒

probe-server-time set *20*

probe-server-time show<cr>

命令描述：

显示服务器均衡组之间切换的等待时间。

实例：

probe-server-time show<cr>

server update time is 20

probe-show

显示服务器负载均衡参数。

probe-show<cr>

probe-time

设置探测均衡组中所有服务器状态的时间间隔。

probe-time set <*number*>

命令描述：

设置设备探测均衡组中所有服务器状态的时间间隔。

参数说明：

set	设置探测均衡组中所有服务器状态的时间间隔
number	数值，单位为秒，范围为 5-30，默认为 10。

实例：

**设置探测均衡组中所有服务器状态的时间间隔为 20 秒

probe-time set *20*

probe-time show<cr>

显示设备探测均衡组中所有服务器状态的时间间隔。

命令描述：

显示设备探测均衡组中所有服务器状态的时间间隔。

实例：

显示设备探测均衡组中所有服务器状态的时间间隔

probe-time show

time set is 20 second

reboot

安全网关重新启动。

reboot <cr>

命令描述：

重启安全网关引擎。

service

系统服务配置

service default <cr>

命令描述：

恢复系统服务默认出厂配置，默认启动所有服务。

service status <cr>

命令描述：

显示系统服务的运行状态。

实例：

service status <cr>

system sshd start

system telnetd start

system httpd start

system monitord start

dpi sip start

dpi pop3 start

dpi http start

dpi smtp start

showprocess

显示当前进程信息。

showprocess<cr>

命令描述：

显示当前进程信息。

实例：

#showprocess<cr>

Mem: 203600K used, 254724K free, 0K shrd, 1748K buff, 106332K cached

CPU states: 7.21% user 0.00% nice 6.30% system 86.49% iowait and idle

Load average: 0.00, 0.00, 0.00 (State: S=sleeping R=running, W=waiting)

PID	USER	STATUS	RSS	PPID	%CPU	%MEM	COMMAND
11361	root	R	688	11360	0.9	0.1	top
3646	root	S	12M	1	0.0	2.8	tos_configd
3647	root	S	12M	3646	0.0	2.8	tos_configd
11326	root	S	12M	3647	0.0	2.8	tos_configd
3648	root	S	12M	3647	0.0	2.8	tos_configd
3667	root	S	12M	3647	0.0	2.8	tos_configd
3672	root	S	12M	3647	0.0	2.8	tos_configd
11214	root	S	12M	3647	0.0	2.8	tos_configd

……

shutdown

关闭系统

shutdown <cr>

命令描述：

关闭系统

sshd

SSH 服务管理命令。

sshd start<cr>

命令描述：

启动 SSH 服务。

sshd stop<cr>

命令描述：

停止 SSH 服务。

tcpdump

显示从端口捕获的数据包的报文头以及简单的统计信息。用户可以使用 Ctrl+C 中断输出。本系统的 tcpdump 命令不支持一般系统上的 tcpdump 命令的各种参数。

tcpdump <cr>

命令描述：

显示从端口捕获的数据包的报文头以及简单的统计信息

使用说明：

用户可以使用 Ctrl+C 中断输出。

实例：

tcpdump <cr>

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode

listening on eth0, link-type EN10MB (Ethernet), capture size 68 bytes

01:16:51.165380 R@eth0 IP 192.168.83.231.1356 > 192.168.83.240.22: . ack

27582604 win 16312

01:16:51.165560 X@eth0 IP 192.168.83.240.22 > 192.168.83.231.1356: P 1:305(304) ack 0 win 33768

01:16:51.384130 R@eth0 IP 192.168.83.231.1356 > 192.168.83.240.22: . ack 305 win 17520

5 packets captured

11 packets received by filter

0 packets dropped by kernel

telnetd

telnet 服务管理命令。

telnetd start<cr>

命令描述：

启动 telnet 服务。

telnetd stop<cr>

命令描述：

停止 telnet 服务。

terminal

设置终端空闲超时相关参数

terminal idle-timeout < *number* >

命令描述：

设置终端空闲超时时间。

参数说明：

idle-timeout	设置终端空闲超时时间

number	数值，范围 30-3600s，设置为 0 表示永不超时。

实例：

**设置终端空闲超时时间为 60 秒

terminal idle-timeout *60*

terminal show<cr>

命令描述：

显示终端空闲超时时间

实例：

terminal show<cr>

terminal idle timeout: 60 seconds

time

设置设备时间相关参数。

time set clock <*string1*> **date**<*string2*> **timezone**<*string3*>

命令描述：

设置设备时间

参数说明：

set	设置系统时间
colck	设置时间
string1	字符串，形为 HH:MM:SS。
date	设置日期
string2	字符串，形为 YYYY-MM-DD。
timezone	设置时区
string3	字符串，形为<+|->TZ。

实例：

time set clock *12:00:00* **date** *2007-01-01* **timezone** *+8*

Set the system time ok!

time show<cr>

命令描述：

显示设备时间

实例：

time show<cr>

+08 2007-01-19 09:58:16

top-policy

设置 TopPolicy 服务器信息。网络卫士安全网关设备支持主、从 TP 服务器的工作方式，设备首先向主 TP 服务器进行身份认证并下载策略，当主 TP 服务器不能正常工作时，设备将尝试向从服务器进行身份认证并下载策略。用户在采用证书认证建立隧道时需要对主服务器设置，根据实际情况可以选择设置从服务器。

top-policy set-ip ip <*string*> **type** <master|slave> [**notify_port** <*port*>][**policy_port** <*port*>] [**local**<yes|on>]

命令描述：

根据 IP 地址来设定 TP 服务器。

参数说明：

Set-ip	根据 IP 地址来设定 TP 服务器
ip	指定服务器 IP 地址
string	IP 地址字符串
type	选定设定主服务器还是从服务器
master|slave	主/从
notify_port	设定通道端口
port	数值，范围为 0-65535，一般采用预设的缺省值 2010。
policy_port	设定策略端口
port	数值，范围为 0-65535，一般采用预设的缺省值 2010。
local	用来判断服务器是否在当前网关的内部
yse|no	是|否，缺省为否。

使用说明：

“通告端口”和“策略端口”：TP 服务器使用这两个端口用于接收网关认证注册和下载策略请求、保活通告等。TP 服务器的“通告端口”和“策略端口”一般

采用预设的缺省值 2010，当服务器的通告端口、策略端口有变化时，则必须指明服务器的相应端口。

top-policy set-dns domain-name <*string*> **type** <master|slave> [**notify_port** <*port1*>] [**policy_port** < *port2* >] [**local**<yes|on>]

命令描述：

根据域名来设定 Top-Policy 服务器。

参数说明：

set-dns	根据域名来设定 Top-Policy 服务器
domain-name	指定服务器域名
string	字符串
type	选定设定主 TopPolicy 服务器还是从 TopPolicy 服务器
master|slave	主/从
notify_port	设定通道端口
port1	数值，范围为 1-65535。
policy_port	设定策略端口
port2	数值，范围为 1-65535。
local	用来判断 TopPolicy 服务器是否在当前网关的内部
yse|no	是|否，缺省为否。

使用说明：

“通告端口”和“策略端口”：TopPolicy服务器使用这两个端口用于接收网关认证注册和下载策略请求、保活通告等。TopPolicy服务器的“通告端口”和“策略端口”一般采用预设的缺省值 2010，当TopPolicy服务器的通告端口、策略端口有变化时，则必须指明TOP-POLICY服务器的相应端口。

top-policy show <cr>

命令描述：

查看主 TopPolicy 服务器信息。

top-policy clean<cr>

命令描述：

清空 TopPolicy 服务器信息

traceroute

用来显示路由封包到达目的地址的信息。

traceroute <*string*>

命令描述：

显示路由封包到达目的地址的信息

参数说明：

string	目标 IP 地址，格式为 0.0.0.0

实例：

traceroute *192.168.83.231*

traceroute to 192.168.83.231 (192.168.83.231), 30 hops max, 40 byte packets

update

系统升级相关设置。

update filename < *string1*> **serip** <*ipaddress*> **sysdisk** < normal > [**ftp** <yes> [**ftp-user** <*sting2*>][**ftp-password** <*string3*>]]

命令描述：

设置系统升级参数

参数说明：

update	升级网络卫士安全网关
filename	升级包文件名
string1	字符串，升级包名称
serip	升级服务器 IP 地址
ipaddress	IP 地址字符串，格式为 0.0.0.0。
sysdisk	需要升级的系统
normal	正常运行的系统
ftp	通过 FTP 服务器升级，不设置时表示通过 TFTP 服务器升级
yes	确认通过 FTP 服务器升级
ftp-user	FTP 服务器上的用户名
string2	用户名字符串
frp-password	FTP 服务器上的用户密码，与 FTP 用户名对应
string3	密码字符串

使用说明：

升级过程大约 10 分钟左右，请耐心等待。避免对安全网关进行任何操作，特别是不能按键 CTRL+C。

实例：

** 通过 TFTP 服务器对系统进行升级

update filename *3.3.002.012_upt* **serip** *192.168.1.4* **sysdisk** normal

uptime

显示系统启动后运行的总时间。

uptime<cr>

命令描述：

显示系统启动后运行的总时间。

实例：

#uptime<cr>

UP 01:28

vdcd

向 TopPolicy 服务器自动注册服务。

vdcd start <cr>

命令描述：

启动自动注册服务。

实例：

**启动自动注册服务

vdcd start <cr>

version

显示系统版本信息。

version<cr>

命令描述：

显示系统版本信息。

实例：

version <cr>

Topsec Operating System

v3.3.005.030.1_more

vs

显示虚拟系统相关信息

vs show manager<cr>

命令描述：

显示虚拟系统管理员信息。

参数说明：

Show	显示虚拟系统信息
manager	管理员信息

实例：

vs show manager<cr>

virtual system 0 manager superman

virtual system 0 manager cc

virtual system 0 manager aa

virtual system 1 manager VV

vs show interface<cr>

命令描述：

显示虚拟系统接口信息。

参数说明：

show	显示虚拟系统信息
interface	接口信息

实例：

vs show interface<cr>

virtual system 0 interface lo

virtual system 0 interface eth0

virtual system 0 interface eth1

virtual system 0 interface eth2

virtual system 0 interface vlan.0002

virtual system 0 interface vlan.0003

virtual system 0 interface vlan.0004

virtual system 0 interface vlan.0005

webui

设置 WEBUI 相关参数。

webui admin-port <*number*>

命令描述：

设置管理员使用 HTTPS 协议登录 WebUI 系统时的端口号。

参数说明：

admin-port	设置管理员使用 HTTPS 协议登录 WebUI 系统时的端口号。
number	数值

webui cert restore < cr>

命令描述：

恢复 WEBUI 系统根证书。

参数说明：

cert	设置 WEBUI 系统根证书
restore	恢复根证书。

webui cert show <cr>

命令描述：

查看根证书。

参数说明：

cert	设置 WEBUI 系统根证书
show	查看根证书。

webui default <cr>

命令描述：

恢复 WEBUI 到默认配置。

webui idle-timeout <*number*>

命令描述：

设置 WEBUI 超时时间。

参数说明：

idle-timeout	设置 WEBUI 超时时间。
number	数值，表示时间间隔，取值范围为 30-3600，单位为：秒。 当设置为 0 时，表示永不超时。

实例：

**设置 WEBUI 超时时间为 60 秒

webui idle-timeout *60*

webui show<cr>

命令描述：

查看 WEBUI 设置。

使用说明：

此处主要是查看 WEBUI 的登录超时设置和认证模式设置。

webui ssl-verify-client <yes|no>

命令描述：

设置是否启用客户端认证。

参数说明：

ssl-verify-client	设置模式
yes	启用客户端认证。设置为此认证模式时，需要用户使用正确的证书和用户名/密码方能成功登录 WEBUI 系统。
no	不启用客户端认证。在此认证模式下，用户只需提供正确的用户名/密码便可登录网络卫士安全网关的 WEBUI 系统。

使用说明：

关于 WEBUI 认证相关参数的详细设置，请参考《TopGate 管理手册——基础配置》中的相关章节。

实例：

**设置 WEBUI 认证模式为客户端认证

webui ssl-verify-client yes

webui max-client <*number*>

命令描述：

设置允许同时登录 WebUI 系统的最大用户数。

参数说明：

max-client	设置允许同时登录 WebUI 系统的最大用户数。
number	数值，表示最大用户数，取值范围为 5-200。

实例：

**设置允许同时登录 WebUI 系统的最大用户数为 100

webui max-client 100

TELNET

telnet 连接命令

telnet <*string*>[**interface** <*string*>] [**port** <*number*>]

命令描述：

建立 telnet 连接

参数说明：

string	telnet 目的主机 IP 地址
interface	可选项，设置数据报文传出时通过的接口名称
string	接口名
port	可选项，设置端口
number	数值

实例：

telnet *192.168.1.23*

声明：

1. 本手册所提到的产品规格及资讯仅供参考，有关内容可能会随时更新，天融信不另行通知。

2. 本手册中提到的产品功能或性能可能因产品具体型号、配备环境、配置方法不同而有所差异，此可能产生的差异为正常现象，产品功能和性能请以产品说明书为准。

3. 本手册中没有任何关于其他同类产品的对比或比较，天融信也不对其他同类产品表达意见，如引起相关纠纷应属于自行推测或误会，天融信对此没有任何立场。

4. 本手册中提到的信息为正常公开的信息，若因本手册或其所提到的任何信息引起了他人直接或间接的资料流失、利益损失，天融信及其员工不承担任何责任。