# 网御星云

## 安全网关 PowerV

## 命令行操作手册

VERSION 1.0

声明

- 本手册所含内容若有任何改动，恕不另行通知。
- 在法律法规的最大允许范围内，北京网御星云信息技术有限公司除就本手册和产品应负的瑕疵担保责任外，无论明示或默示，不作其它任何担保，包括（但不限于）本手册中推荐使用产品的适用性和安全性、产品的适销性和适合某特定用途的担保。
- 在法律法规的最大允许范围内，北京网御星云信息技术有限公司对于您的使用或不能使用本产品而发生的任何损坏（包括，但不限于直接或间接的个人损害、商业利润的损失、业务中断、商业信息的遗失或任何其它损失），不负任何赔偿责任。
- 本手册含受版权保护的信息，未经北京网御星云信息技术有限公司书面允许不得对本手册的任何部分进行影印、复制或翻译。
- 本手册使用于网御星云 PowerV 系列防火墙和 VPN，在手册中称为安全网关。文档少部分内容视产品具体型号略有不同，请以购买的实际产品为准。
- 网御星云不承担由于本资料中的任何不准确性引起的任何责任，网御星云保留不作另行通知的情况下对本资料进行变更、修改、转换或以其他方式修订的权利！

北京网御星云信息技术有限公司
中国北京海淀区中关村南大街 6 号中电信息大厦 8 层

# 目　录

# 第1章 前 言

## 1.1 导言

《命令行操作手册》是网御安全网关 Power V 管理员手册中的一本。该手册主要介绍如何通过终端命令行的方式对网御安全网关 Power V 进行配置管理。

## 1.2 使用建议

请阅读本文档时，参考 web 界面。一级目录树排版为 web 界面左侧导航栏。二级目录树为各个左侧导航栏点击后显示在 web 界面上方的选项。

这样有助于您找到相关的使用命令行说明。

## 1.3 本书适用对象

本手册适用于负责支持、维护安全网关的安全管理员，是进行网御星云安全网关 Power V 配置管理时的必备手册。

使用本手册的读者，应掌握 TCP/IP 协议簇，ipv4，ipv6，网络拓扑等基本知识。

## 1.4 本书适合的产品

本书适合网御星云安全网关 Power V 系列产品，以后简称网御星云安全网关 Power V，不再说明。

**请注意：**对不同的产品型号，功能模块配置会有所不同，模块的具体配置参数也会有差异，比如：SSL VPN 功能对某些型号属于选配，对密码机系列产品不支持 AES，3DES 等通用算法，协商参数也有额外限制。请以产品的实际配置为准。

# 1.5 手册章节组织

本手册按照以下章节编排：

第一章：前言，描述本书适用的读者，手册章节组织及相关参考手册等。

第二章：命令行概述，描述了网御星云安全网关Power V 用命令行进行配置的常用命令使用方法，以及一些使用技巧等。

第三章：快速入门，通过举例的方式，描述了网御星云安全网关Power V命令行配置方法，及在何种情况下使用命令行配置。

第四章：系统管理，描述与安全网关管理相关的配置，包括：系统时钟设置、时钟服务器同步、集中管理、策略代理、管理员配置、模块升级、模块升级、系统配置、管理主机、管理员账号、管理员证书、管理方式、IDS产品联动等。

第五章：网络管理，描述与网络环境相关的配置，包括：网络接口属性、端口镜像、VRRP、无线配置 、UpnP、DHCP、域名服务器、高可用性等。

第六章：路由，描述基本路由、高级路由、策略路由、动态路由、ISP路由等。

第七章：流量管理，描述安全策略、带宽管理、资源定义(地址、服务、时间)、安全选项、黑名单、负载均衡设置与使用方法。

第八章：UTM，描述UTM设置与使用方法。

第九章： 用户认证，描述用户认证的配置，包括用户认证服务器的设置，用户资源以及用户在线信息查看。

第十章：会话管理，描述应用识别策略配置和URL过滤。

第十一章：VPN配置，描述VPN的配置。

第十二章：SSLVPN，描述SIG的配置。

第十三章： IPv6，描述IPv6的接口配置、安全策略、路由管理、6to4隧道、NAT-PT、资源定义(地址、服务)的设置与使用方法。

第十四章：漏洞扫描，描述各种扫描配置，以及查看扫描任务日志及报表。

第十五章：状态监控，描述如何监控系统的运行状态，包括：系统信息、网络接口状态、路由监控等。

第十六章：日志与报警，描述日志和报警信息的设置与查看。

第十七章：其他

## 1.6 相关参考手册

《网御星云安全网关 PowerV Web 界面操作手册》：介绍了如何通过 Web 界面管理网御星云安全网关 PowerV。

《网御星云安全网关 PowerV 功能使用手册》：介绍了如何使用网御星云安全网关 PowerV 的比较复杂的功能和典型应用。

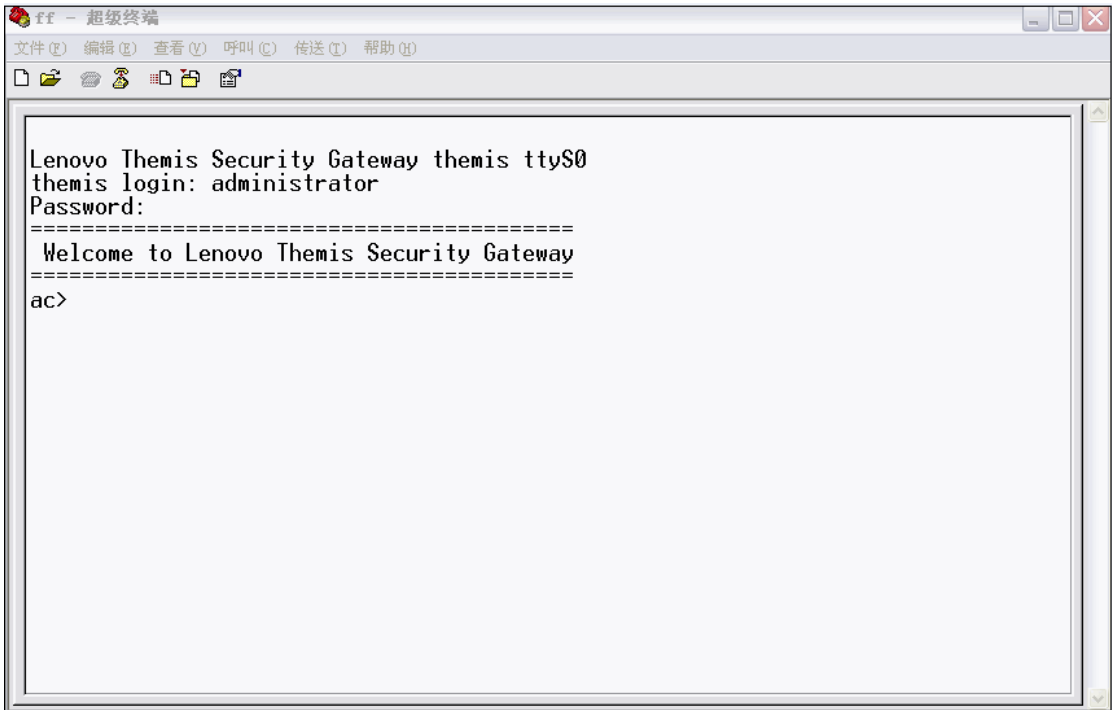
# 第2章 命令行概述

## 2.1 CLI 界面概述

CLI 界面为用户提供一个纯字符界面。它向不同级别的管理员提供不同的命令集，屏蔽管理员对文件系统的直接访问。

CLI 界面可以使用超级终端通过安全网关上的串口进入，也可以在远程使用 ssh 客户端进入，进入 CLI 界面需要提供用户名和密码。

通过超级终端进入 CLI 界面的方法如下：将管理主机的 COM 串口与安全网关的 CONSOLE 口用串口线连接，配置管理主机的超级终端，波特率为 9600 比特。以默认管理员帐号与密码登录，进入 CLI 命令行界面：




在第一次登录成功后，管理员可以按需求变更管理员帐号、管理主机、安全网关可管理 IP、管理方式或导入管理员证书。下次登录时，按变更内容进行认证与登录。

进入 CLI 界面后，会出现命令行提示符，用户可在命令行上输入、编辑命令，编辑键如下：

| | |
|---|---|
| ← | 光标前移一格 |
| → | 光标后移一格 |
| CTRL+A | 光标移到行首 |
| CTRL+E | 光标移到行尾 |
| CTRL+D | 删除光标处的单个字符 |
| CTRL+H | 删除光标前的单个字符 |

| | |
|---|---|
| CTRL+U | 清空当前命令行 |
| CTRL+C | 忽略当前命令行，在下一行显示新的命令提示符 |

用户可以使用“？”键获得上下文相关的帮助信息。
用户使用回车键提交命令。
提交过的命令会储存在历史命令列表中，通过上下箭头键调用。历史命令表可以存储 100 条命令。
用户可以使用 CTRL+C 中止正在执行的命令。
如果用户在 1800 秒内没有任何操作，CLI 界面会返回到登录提示状态。
客户端的连接、用户登录信息（成功和失败）、用户提交的命令、用户退出信息都会记录在系统日志中。

## 2.2 命令行的使用

在使用网御星云安全网关 PowerV 的命令集之前，请您参照《网御星云安全网关 PowerV Web 界面操作手册》中的安装过程，安装好安全网关，并且按照其中命令行配置的步骤进行配置和登录。

## 2.3 命令的基本结构

命令行的命令的基本结构为：“类别命令 操作类型 命令参数 1 命令参数 2 ……”
类别命令：表示想配置的项目，如：网络接口（interface）、安全规则（rule）等。
操作类型：表示对此项目进行什么样的操作，如：添加（add）、删除（del）、修改（set）、显示（show）等。
命令参数：不同的参数有不同必选或可选参数。
所有的命令和参数都是大小写敏感的。

## 2.4 基本命令行参数

以下介绍在命令行中常用的一些基本参数及其含义和格式，在没有特殊声明的情况下，都遵守这里的约定，如有特殊情况，会特殊声明。

标识：<id>
含义：序号
长度：1—5 个字符
可用字符：数字
格式：1—65535。

标识：<name>
含义：名字
长度：15 个视觉长度
可用字符：大、小写英文字母，数字，减号，下划线，合法汉字（UTF-8 编码）
格式：第一个字符必须是大、小写英文字母或数字。

备注：视觉长度为 15 个，例如：name="网御星云_leadsec-12"（个数为 15）

标识：<string>
含义：字符串
长度：0—256 个字符，或见各命令参数说明
可用字符：除制表符和问号外的任意可打印字符
格式：无

标识：<comment>
含义：注释
长度：0—255 个字符
可用字符：除制表符和问号外的任意可打印字符
格式：无

标识：<keyword>
含义：URL 过滤关键字
长度：1—255 个字符
可用字符：除制表符和问号外的任意可打印字符
格式：无

标识：<password>
含义：密码
长度：6—15 个字符
可用字符：除制表符和问号外的任意可打印字符
格式：无
备注：告警邮件密码取决于对应的邮件服务器支持格式，如果所使用的邮件服务器密码提供特殊字符支持，那么告警邮件密码也可以使用输入特殊字符设置密码（特殊字符包括：~！@#￥%……&*（）等）

标识：<email>
含义：E-Mail 地址
长度：1—64 个字符
可用字符：除制表符和问号外的任意可打印字符
格式：如 gateway@lenovo.com

标识：<filename>
含义：文件名
长度：1—254 个字符
可用字符：任意可打印字符，不包括斜线、反斜线、冒号、星号、问号、双引号、大于号、小于号、管道符、制表符
格式：无

标识：<hostname>
含义：主机名
长度：1—254 个字符

可用字符：任意可打印字符，不包括斜线、反斜线、冒号、星号、问号、双引号、大于号、小于号、管道符、制表符
格式：无

标识：<number>
含义：数字
长度：1 个以上的字符
可用字符：数字
格式：无

标识：<percent>
含义：数字
长度：1—3 个字符
可用字符：数字
格式：0—100。

标识：<ip>
含义：IP 地址
长度：7—31 个字符
可用字符：数字，句号，斜线，冒号
格式：单个 IP 地址（1.1.1.1），IP 地址/子网掩码（1.1.1.0/255.255.255.0），IP 地址段（1.1.1.10:1.1.1.20）。
备注：本说明举例为 ipv4 地址，但是使用在具体的配置下发不局限于 ipv4 地址，有可能也为 ipv6 地址，视具体情况而定。

标识：<netmask>
含义：子网掩码
长度：9—15 个字符
可用字符：数字，句号
格式： 如 255.255.255.0。

标识：<port>
含义：端口
长度：1—11 个字符
可用字符：数字，冒号
格式：单个端口（12345），端口段（1000:2000）。

标识：<mac>
含义：MAC 地址
长度：17 个字符
可用字符：A—F 大小写英文字母，数字，减号，冒号
格式：XX-XX-XX-XX-XX-XX，或 XX:XX:XX:XX:XX:XX。

标识：<date>

含义：日期
长度：8—10 个字符
可用字符：数字，减号，斜线
格式：yyyy-mm-dd，或 yyyy/mm/dd，其中 yyyy 为 2000—9999，mm 为 01—12，dd 为 01—31。

标识：<time>
含义：时间
长度：3—17 个字符
可用字符：数字，冒号，减号
格式： hh:mm:ss 或 hh:mm， hh:mm:ss-hh:mm:ss 或 hh:mm-hh:mm，其中 hh 为 00—23，mm 为 00—59，ss 为 00—59。

## 2.5 命令行使用技巧

关键字自动补全：
用户可以使用 TAB 键补全命令。
2．在线帮助：
用户可以使用？键获得上下文相关的帮助信息。
3．历史命令：
提交过的命令会储存在历史命令列表中，通过上下箭头键调用。历史命令表可以存储 100 条命令。
4．编辑功能：

| | |
|---|---|
| ← | 光标前移一格 |
| → | 光标后移一格 |
| CTRL+A | 光标移到行首 |
| CTRL+E | 光标移到行尾 |
| CTRL+D | 删除光标处的单个字符 |
| CTRL+H | 删除光标前的单个字符 |
| CTRL+U | 清空当前命令行 |
| CTRL+C | 忽略当前命令行，在下一行显示新的命令提示符 |

5．注意事项：
当输入的字符串包含空格时，必须用双引号将此字符串扩起来。
用户可以使用 CTRL+C 中止正在执行的命令。
如果用户在 1800 秒内没有任何操作，CLI 界面会返回到登录提示状态。

## 2.6 保留字

| | |
|---|---|
| any | 表示任意，如任意 IP 地址、任意服务 |
| none | 表示不使用 |

# 2.7 命令集

| 命令 | 语法 |
| --- | --- |
| Account_power | account_power { add name <name> [ commnet <comment> ] { \| [ system { none \| read \| write } ] \| [ admin { none \| read \| write } ] \| [ upgrade { none \| read \| write } ] \| [ network { none \| read \| write } ] \| [ route { none \| read \| write } ] \| [ policy { none \| read \| write } ] \| [ user { none \| read \| write } ] \| [ flow { none \| read \| write } ] \| [ holescan { none \| read \| write } ] \| [ monitor { none \| read \| write } ] [ speed { none \| read \| write } ] } \| set name <name> [ comment <comment> ] { \| [ system { none \| read \| write } ] \| [ admin { none \| read \| write } ] \| [ upgrade { none \| read \| write } ] \| [ network { none \| read \| write } ] \| [ route { none \| read \| write } ] \| [ policy { none \| read \| write } ] \| [ user { none \| read \| write } ] \| [ flow { none \| read \| write } ] \| [ holescan { none \| read \| write } ] \| [ monitor { none \| read \| write } ] [ speed { none \| read \| write } ] } \| del name <name> \| show \| startup } |
| address | address { add name <name> ip <all_ip> [ comment <comment> ] \| set name <name> { [ ip <all_ip> ] [ comment <comment> ] } \| del name <name> \| show [ name <name> ] } |
| address6 | address6 { add name <name> ip <all_ipv6> [ comment <comment> ] \| set name <name> { [ ip <all_ipv6> ] [ comment <comment> ] } \| del name <name> \| show [ name <name> ] } |
| addrgrp | addrgrp { add name <name> [ comment <comment> ] \| set name <name> { addmbr <name>+ \| delmbr <name>+ \| comment <comment> } \| del name <name> \| show [ name <name> ] } |
| Addrgrp6 | addrgrp6 { add name <name> [ comment <comment> ] \| set name <name> { comment <comment> \| addmbr <name>+ \| delmbr <name>+ } \| del name <name> \| show [ name <name> ] } |
| admacct | admacct { add name <name> password <password> powername <name> max_err_num <number> [ vmfwid <number> ] \| set { sname <name> dname <name> { [ password <password> ] \| [ powername <name> ] \| [ max_err_num <number> ] } [ vmfwid <number> ] \| multiadm { on \| off } \| passwd_rule { on \| off } upper [ on \| off lower [ on \| off number [ on \| off special ] ] ] \| unlock_style { reboot \| timeout <number> } \| idle_time <number> } \| del name <name> [ vmfwid <number> ] \| reset name <name> \| startup \| show } |
| admcert | admcert { add { cacert <filename> fwcert <filename> fwkey <filename> \| admincert <filename> } \| del admincert <filename> \| on admincert <filename> \| off admincert <filename> \| show { cacert \| fwcert \| admincert } } |
| admhost | admhost { add ip <ip> netmask <netmask> [ comment <comment> ] \| add ipv6 <net_ipv6> [ comment <comment> ] \| del ip <ip> \| del ipv6 <net_ipv6> \| show [ all \| ipv4 \| ipv6 ] } |
| admmode | admmode { on { ssh \| ppp \| telnet } \| off { ssh \| ppp \| telnet } \| show } |
| advroute | advroute { set { ospf { routerid <all_ip> [ connected { on \| off } ] [ static { on \| |

| | |
|---|---|
| | off } ] [ rip { on \| off } ] [ bgp { on \| off } ] [ defgw { on \| off } ] [ active { on \| off } ] \| area <area_ip> [ type { regular \| nssa \| stub } ] [ auth { none \| text \| md5 } ] [ virtual_link <all_ip> ] \| net <all_ip> netmask <all_ip> area <area_ip> \| port <name> [ auth { none \| text \| md5 } ] [ passwd <string> ] [ hello <number> ] [ dead <number> ] [ comment <comment> ] \| message-digest port <name> key <id> md5 <string> } \| pim sparse-mode { active { on \| off } \| port <name> dr-priority <number> rp-candidate { on \| off } rp-priority <number> } \| rip [ active { on \| off } ] [ version { v1 \| v2 } ] [ ospf { on [ ospf_metric <number> ] \| off } ] [ connected { on [ connected_metric <number> ] \| off } ] [ static { on [ static_metirc <number> ] \| off } ] [ kernel { on [ kernel_metric <number> ] \| off } ] [ bgp { on [ bgp_metric <number> ] \| off } ] [ isis { on [ isis_metric <number> ] \| off } ] [ defgw { on \| off } ] [ update <number> ] [ holddown <number> ] [ garbage <number> ] \| ripng [ active { on \| off } ] [ ospfv3 { on [ ospfv3_metric <number> ] \| off } ] [ connected { on [ connected_metric <number> ] \| off } ] [ static { on [ static_metric <number> ] \| off } ] [ kernel { on [ kernel_metric <number> ] \| off } ] [ bgp { on [ bgp_metric <number> ] \| off } ] [ defgw { on \| off } ] [ update <number> ] [ holddown <number> ] [ garbage <number> ] \| ospfv3 [ routerid <all_ip> ] [ active { on \| off } ] [ connected { on \| off } ] [ static { on \| off } ] [ ripng { on \| off } ] [ bgp { on \| off } ] [ kernel { on \| off } ] } \| add { ospf { area <area_ip> [ type { regular \| nssa \| stub } ] [ auth { none \| text \| md5 } ] [ virtual_link <all_ip> ] \| net <all_ip> netmask <all_ip> area <area_ip> \| port <name> [ auth { none \| text \| md5 } ] [ passwd <string> ] [ hello <number> ] [ dead <number> ] [ comment <comment> ] \| message-digest port <name> key <id> md5 <string> } \| pim { rp <single_ip> \| sparse-mode port <name> dr-priority <number> rp-candidate { on \| off } rp-priority <number> } \| rip { key_chain <name> keyid <number> keyword <string> start <string> { end <string> \| infinite } \| net <all_ip> netmask <all_ip> \| port <name> [ auth { none \| text [ { single_key <string> \| key_chain <name> } ] \| md5 [ { single_key <string> \| key_chain <name> } ] } ] [ send { v1 \| v2 \| both } ] [ receive { v1 \| v2 \| both } ] [ passive ] } \| ripng { port <name> active { on \| off } passive { on \| off } } \| ospfv3 { port <name> area <area_ip> } } \| del { ospf { area <area_ip> \| net <all_ip> netmask <all_ip> area <area_ip> \| port <name> \| message-digest port <name> key <id> } \| pim { rp <single_ip> \| sparse-mode port <name> } \| rip { key_chain <name> keyid <number> \| net <all_ip> netmask <all_ip> \| port <name> } \| ripng { port <name> } \| ospfv3 { port <name> area <area_ip> } } \| show { { rip \| ospf \| ripng \| ospfv3 } route } } |
| aliasip | aliasip { add { aliasid <id> if <name> ip <single_ip> status { on \| off } } \| update { aliasid <id> ip <single_ip> status { on \| off } } \| del { aliasid <id> } } |
| anti_config | anti_config -t { config { -h \| -l \| -a { anti_attack \| anti_cc } -j { on \| off } } \| attack { -h \| -l \| -a { smurf \| land \| winnuke \| queso \| sf_scan \| null_scan \| full_xmas_scan \| xmas_scan \| ipspoofing \| sroute } -j { on \| off } } \| arp { -i <name> -s <single_ip> -m <netmask> -j { on \| off } } \| ipconflict { -h \| -l \| -i <name> -s <single_ip> -m <netmask> -j { on \| off } } \| cc { -h \| -l \| -A -s <single_ip> -m <netmask> \| -U -n <id> -s <single_ip> -m <netmask> \| -D -n <id> } \| asic_syn { -h \| -l \| -c <number> [ -j { on \| off } ] \| -j { on \| off } } } |
| antiscan | antiscan { set { portscan \| hostscan } active { on \| off } value <number> log { on \| off } mail { on \| off } drop { on \| off } block { on \| off } [ blocktime <number> ] \| show { portscan \| hostscan \| whitelist } \| add whitelist { ipv4 ip <single_ip> netmask <netmask> \| ipv6 ip <single_ipv6> netmask <number> } \| del whitelist { ipv4 ip <single_ip> \| ipv6 ip <single_ipv6> } } |
| antispam | antispam { on \| off \| config show \| blackserver { add ip <single_ip> comment <comment> \| del ip <single_ip> \| import <string> \| export <string> \| on \| off } \| openrelay { on \| off } \| subjectkeywords { add keyword <string> comment <comment> \| del keyword <string> \| import <string> \| export <string> } \| spammail { add mailaddr <string> comment <comment> \| del mailaddr <string> \| import |

| | |
|---|---|
| | <string> \| export <string> } \| blocksmtpspam { on \| off } \| spamflag { on \| off \| edit <string> } \| checkspamaddress { on \| off } \| checkkeywords { on \| off } \| checkContent { on \| off } \| contentKeywords { add keyword <string> comment <comment> \| del keyword <string> \| import <string> \| export <string> } \| attachmentFilename { on \| off \| add keyword <string> comment <comment> \| del keyword <string> \| import <string> \| export <string> } \| attachmentContent { on \| off \| add keyword <string> comment <comment> \| del keyword <string> \| import <string> \| export <string> } \| whitemail { on \| off \| add mailaddr <string> comment <comment> \| del mailaddr <string> \| import <string> \| export <string> } \| attachmentFilesize { on \| off } \| max_attachment_size edit <number> \| max_all_attachment_size edit <number> \| rcpt { on \| off \| edit <number> } \| checkClient { on \| off } \| client_pop_client edit <number> \| client_pop_conn edit <number> \| client_smtp_conn edit <number> \| client_smtp_send edit <number> \| spamlog { on \| off } } |
| apc | apc { add type policy name <name> comment <comment> policyid <id> \| set type policy name <name> { group <name> \| signature <name> } [ active { on \| off } ] [ alertmail { on \| off } ] [ log { on \| off } ] \| del type policy policyid <id> \| startup \| show policy } |
| arp | Arp |
| auth | auth { server { show \| redirecturl <string> \| localport <number> log { on \| off } \| workmode { local \| ldap ip <single_ip> timeout <number> authport <number> basename <string> managername <string> managersecret <string> type <string> dnmode <string> \| radius ip <single_ip> timeout <number> authport <number> auditport <number> secret <string> type <string> \| ad ip <single_ip> managername <string> managersecret <string> realm <string> netbios <string> } } \| config { show \| forcemodify { yes \| no } pwdcomplex { none \| weak \| normal \| good \| better \| great } maxloadtimes <number> unlocktime <number> pwdperiod <number> pwdremind <number> idletime <number> } } |
| auth-policy | auth-policy { add policyname <name> [ ingress <eth> ] [ ipv4 <string> ] [ port <string> ] [ comment <comment> ] \| set policyname <name> [ ingress <eth> ] [ ipv4 <string> ] [ port <string> ] [ comment <comment> ] \| del { policyname <name> \| all } \| show { policyname <name> \| all } } |
| av | av { add type policy name <name> comment <comment> policyid <id> \| set type policy name <name> protocol <string> [ active { on \| off } ] [ log { on \| off } ] [ alertmail { on \| off } ] [ block { on \| off } ] [ resetsend { on \| off } ] [ resetrecv { on \| off } ] \| del type policy policyid <id> \| show { policy { all \| id <id> } \| avmode \| engine option \| port all } \| addsig name <name> sig <comment> \| delsig name <name> \| setsig name <name> sig <comment> \| loadsig \| addport name <name> port <all_port>+ \| delport name <name> { all \| port <all_port>+ } \| loadport \| loadpolicy \| setmode { quick \| full } \| engine [ filesize <number> ] [ blockext <string> ] [ passext <string> ] [ compress { on \| off } ] } |
| bandwidth | bandwidth { add type { parent name <name> ifname <name> [ comment <comment> ] \| child name <name> minbw <number> maxbw <number> parentname <name> priority <number> [ comment <comment> ] \| group name <name> [ comment <comment> ] } \| set type { child name <name> minbw <number> maxbw <number> parentname <name> priority <number> [ comment <comment> ] \| group name <name> { comment <comment> \| addmbr <name>+ \| delmbr <name>+ \| delallmbr } } \| del type { parent { name <name> \| all } \| child { name <name> \| all } \| group { name <name> \| all } } \| show type { parent [ name <name> ] \| child [ name <name> ] \| group [ name <name> ] } } |
| bl | bl { add { virtual <name> { pr { tcp { ip <single_ip> { port <number> { pt <number> { schd { rr \| wrr \| lc \| wlc \| dh \| sh \| lblc \| lblcr } } } } } } \| udp { ip <single_ip> { port <number> { pt <number> { schd { rr \| wrr \| lc \| wlc \| dh \| sh \| lblc \| lblcr } } } } } } } \| { real <name> { to <name> { ip <single_ip> { port <number> { |

| | |
|---|---|
| | wt <number> { gw <single_ip> } } } } } } } \| edit { virtual <name> { pt <number> { schd { rr \| wrr \| lc \| wlc \| dh \| sh } } } \| real <name> { wt <number> } } \| del { real <name> \| virtual <name> } \| on \| off \| show \| detect <number> [ dtimer <number> ] } |
| blacklist | blacklist { add [ ip <single_ip> ] [ time <number> ] [ comment <comment> ] \| del ip <single_ip> \| clean \| show } |
| Block | block { clean } |
| bw | bw { add id <id> name <name> [ sa { any \| <name> \| <ip> } ] [ sport { none \| <single_port> } ] [ da { any \| <name> \| <ip> } ] [ dport { none \| <single_port> } ] [ iif { any \| <name> } ] [ oif { any \| <name> } ] [ time { none \| <name> } ] [ level { 0 \| 1 \| 2 \| 3 } ] [ service { any \| <name> } ] bandwidthname <name> [ apc { 0 \| 512 } ] [ url { 0 \| 512 } ] [ file { 0 \| 512 } ] [ rate { 0 \| <number> } ] [ mode { srcip \| dstip } ] [ active { on \| off } ] [ comment <comment> ] \| set id <id> name <name> [ sa { any \| <name> \| <ip> } ] [ sport { none \| <single_port> } ] [ da { any \| <name> \| <ip> } ] [ dport { none \| <single_port> } ] [ iif { any \| <name> } ] [ oif { any \| <name> } ] [ time { none \| <name> } ] [ level { 0 \| 1 \| 2 \| 3 } ] [ service { any \| <name> } ] [ bandwidthname <name> ] [ apc { 0 \| 512 } ] [ url { 0 \| 512 } ] [ file { 0 \| 512 } ] [ rate { 0 \| <number> } ] [ mode { srcip \| dstip } ] [ active { on \| off } ] [ comment <comment> ] \| del { id <id> \| all } \| show [ id <id> ] \| quick_bw oif <name> minbw <number> maxbw <number> prio <number> \| apc { clear policyid <id> \| set policyid <id> groupname <name> bandwidthname <name> } \| url { clear policyid <id> \| set policyid <id> groupid <id> bandwidthname <name> } \| file { clear policyid <id> \| set policyid <id> groupid <id> bandwidthname <name> } \| easyconfig id <id> \| easyset [ level { 0 \| 1 \| 2 \| 3 } ] [ service { any \| <name> } ] bandwidthname <name> [ apc { 0 \| 512 } ] [ url { 0 \| 512 } ] [ file { 0 \| 512 } ] [ rate { 0 \| <number> } ] [ mode { srcip \| dstip } ] [ oif { any \| <name> } ] } |
| clock | clock { set <date> <single_time> \| show } |
| connect-rule | connect-rule { add rulename <name> [ client-check { version-check <string> [ proc-check <string> ] \| proc-check <string> [ version-check <string> ] } ] \| set rulename <name> [ client-check { version-check <string> [ proc-check <string> ] \| proc-check <string> [ version-check <string> ] } ] \| del { rulename <name> \| all } \| show { rulename <name> \| all } } |
| ddns | ddns { set { username <string> password <string> confirm <string> } \| show } |
| dhcpserver | dhcpserver { add { domain network <single_ip> netmask <all_ip> range <name> [ gateway <single_ip> ] [ dns <string> ] [ domainname <name> ] [ comment <comment> ] [ default_lease_time <number> ] [ max_lease_time <number> ] [ is_vpnclient { yes \| no } ] [ vpnclient_netmask <all_ip> ] \| static hostname <name> mac <mac> ip <single_ip> [ comment <comment> ] [ default_lease_time <number> ] [ max_lease_time <number> ] } \| del { domain id <number> \| static id <number> } \| set { { startup { on \| off } } \| domain id <number> [ network <single_ip> ] [ netmask <all_ip> ] [ range <name> ] [ gateway <single_ip> ] [ domainname <name> ] [ dns <string> ] [ comment <comment> ] [ default_lease_time <number> ] [ max_lease_time <number> ] [ is_vpnclient { yes \| no } ] [ vpnclient_netmask <all_ip> ] \| static id <number> [ hostname <name> ] [ mac <mac> ] [ ip <single_ip> ] [ comment <comment> ] [ default_lease_time <number> ] [ max_lease_time <number> ] } \| show \| start \| stop \| refresh } |
| Dns | dns { set { ip <single_ip> [ <single_ip> ] } \| unset \| show } |
| eim | eim { add type policy name <name> comment <comment> [ apcpolicyid <id> ] |

| | |
|---|---|
| | [ urlpolicyid <id> ] \| set type policy name <name> [ comment <comment> ] [ apcpolicyid <number> ] [ urlpolicyid <number> ] \| del type policy policyid <id> \| show policy } |
| Exit | exit |
| filterconfig | filterconfig { set { { run_mode { on \| off } \| fast_mode { on \| off } \| hardfast_mode { on \| off } \| rule_first { on \| off } \| state_check { on \| off } \| route_state_backpacket { on \| off } \| show } } \| eth { add \| del \| set \| show \| vlanfilter \| pppoefilter } <proto_name> [ <proto_value> ] [ { on \| off } ] \| show } |
| gre | gre { add name <name> local <name> remote { <single_ip> \| <name> } addr <single_ip> raddr <single_ip> \| del name <name> \| show \| set name <name> { [ local <name> ] \| [ remote { <single_ip> \| <name> } ] \| [ addr <single_ip> ] \| [ raddr <single_ip> ] } \| down name <name> \| up name <name> \| start \| stop \| restart } |
| gwarp | gwarp interface <name> { ethdstmac <mac> ethsrcmac <mac> arpop { request \| reply } arpdstaddr <single_ip> arpsrcaddr <single_ip> arpsrcmac <mac> [ repeat <string> ] [ change ] \| arpop { request \| reply } arpdstaddr <single_ip> } |
| gwmail | gwmail { set { power { on \| off } \| sender <email> receiver <string> smtp <string> password <password> [ port <single_port> ] [ log { on \| off } ] } \| unset \| show \| send [ subject <string> ] [ content <string> ] [ accessory <string> ] [ signature <string> ] } |
| ha | ha { set { ip <single_ip> netmask <all_ip> haif { on \| off } syn { on \| off } \| mode { backup \| cluster } node <number> id <number> } \| unset \| on \| off \| sync \| show { config \| status } } |
| hadetect | hadetect { on \| off \| set threshold <number> \| add { ip <single_ip> weight <number> if <name> \| if <name> } \| del { ip <single_ip> \| if <name> } \| show { config \| ip \| if \| remote_ip <single_ip> \| remote_if <single_ip> } } |
| interface | interface { add { brg if <name> [ ip <single_ip> ] [ netmask <all_ip> ] [ active { on \| off } ] [ interface_list { none \| <string> } ] [ stp { on \| off } ] [ admin { on \| off } ] [ ping { on \| off } ] [ traceroute { on \| off } ] [ ipmac_check { on \| off } ] [ ipmac_check_policy { on \| off } ] [ antispoof { on \| off } ] \| alias bind_if <name> alias_id <number> ip <single_ip> netmask <all_ip> [ active { on \| off } ] [ admin { on \| off } ] [ ping { on \| off } ] [ traceroute { on \| off } ] [ vrid <id> ] \| rd if <name> [ ip <single_ip> ] [ netmask <all_ip> ] [ active { on \| off } ] [ interface_list <string> ] [ workmode { route \| trans } ] [ ipaddr_type { static \| dhcp } ] [ dns_enable { on \| off } ] [ domain_name { none \| <string> } ] [ dhcp_relay { on \| off } ] [ dhcpserver { none \| <string> } ] [ admin { on \| off } ] [ ping { on \| off } ] [ traceroute { on \| off } ] [ ipmac_check { on \| off } ] [ ipmac_check_policy { on \| off } ] [ antispoof { on \| off } ] \| dial if <name> } \| set { phy if <name> [ ip <single_ip> ] [ netmask <all_ip> ] [ active { on \| off } ] [ mac { <mac> \| none } ] [ linkmode { auto \| full \| half } ] [ speed { 10 \| 100 \| 1000 } ] [ workmode { route \| trans \| rd } ] [ mtu <number> ] [ trunk { on \| off } ] [ ipaddr_type { static \| dhcp } ] [ dns_enable { on \| off } ] [ domain_name { none \| <string> } ] [ qos_enable { on \| off } ] [ qos_device_bw <number> ] [ dhcp_relay { on \| off } ] [ dhcpserver { none \| <string> } ] [ admin { on \| off } ] [ ping { on \| off } ] [ traceroute { on \| off } ] [ ipmac_check { on \| off } ] [ ipmac_check_policy { on \| off } ] [ antispoof { on \| off } ] \| vlan if <name> [ ip <single_ip> ] [ netmask <all_ip> ] [ active { on \| off } ] [ mac { <mac> \| none } ] [ qos_enable { on \| off } ] [ qos_device_bw <number> ] [ admin { on \| off } ] [ ping { on \| off } ] [ traceroute { on \| off } ] [ workmode { route \| trans } ] [ ipmac_check { on \| off } ] [ ipmac_check_policy { on \| off } ] [ antispoof { on \| off } ] \| brg if <name> [ ip <single_ip> ] [ netmask <all_ip> ] [ active { on \| off } ] [ interface_list { none \| <string> } ] [ stp { on \| off } ] [ admin |

| | |
|---|---|
| | { on \| off } ] [ ping { on \| off } ] [ traceroute { on \| off } ] [ ipmac_check { on \| off } ] [ ipmac_check_policy { on \| off } ] [ antispoof { on \| off } ] \| alias if <name> [ ip <single_ip> ] [ netmask <all_ip> ] [ active { on \| off } ] [ admin { on \| off } ] [ ping { on \| off } ] [ traceroute { on \| off } ] [ vrid <id> ] \| rd if <name> [ ip <single_ip> ] [ netmask <all_ip> ] [ active { on \| off } ] [ interface_list <string> ] [ workmode { route \| trans } ] [ ipaddr_type { static \| dhcp } ] [ dns_enable { on \| off } ] [ domain_name { none \| <string> } ] [ dhcp_relay { on \| off } ] [ dhcpserver { none \| <string> } ] [ admin { on \| off } ] [ ping { on \| off } ] [ traceroute { on \| off } ] [ ipmac_check { on \| off } ] [ ipmac_check_policy { on \| off } ] [ antispoof { on \| off } ] \| dial if <name> [ active { on \| off } ] [ bind_if <name> ] [ username <string> ] [ password <string> ] [ startup { on \| off } ] [ time <name> ] [ qos_enable { on \| off } ] [ qos_device_bw <number> ] [ dns_enable { on \| off } ] [ domain_name { none \| <string> } ] [ admin { on \| off } ] [ ping { on \| off } ] [ traceroute { on \| off } ] \| rdoption workmode { balance-rr \| backup \| balance-xor \| broadcast \| 802.3ad \| balance-tlb \| balance-alb } [ linkwatch <number> ] [ lacprate { slow \| fast } ] [ usr_carries { on \| off } ] } \| del { if <name> \| dial if <name> } \| show { { phy \| vlan \| brg \| vpn \| alias \| rd \| dial \| trunk \| all } \| if <name> \| rdoption } \| ipv6 { add nat { static { 6to4 \| 4to6 } <ip> <single_ipv6> \| dynamic <ip-ip:port-port> if <name> } \| set { phy if <name> [ natpt { on \| off } ] [ routeadv { on \| off } ] [ inter_time <number> ] [ route_time <number> ] [ { edit ip <net_ipv6> [ ping { on \| off } ] [ admin { on \| off } ] [ traceroute { on \| off } ] [ ipra { on \| off } ] [ valid_time <number> ] [ prefer_time <number> ] \| add ip <net_ipv6> [ ping { on \| off } ] [ admin { on \| off } ] [ traceroute { on \| off } ] [ ipra { on \| off } ] [ valid_time <number> ] [ prefer_time <number> ] \| set ip <net_ipv6> [ ping { on \| off } ] [ admin { on \| off } ] [ traceroute { on \| off } ] [ ipra { on \| off } ] [ valid_time <number> ] [ prefer_time <number> ] \| del ip <net_ipv6> ] } \| nat { prefix <prefix> \| static id <id> { 6to4 \| 4to6 } <ip> <single_ipv6> \| dynamic id <id> <ip-ip:port-port> if <name> } } \| del nat { prefix <prefix> \| static { id <id> \| all } \| dynamic { id <id> \| all } } \| show { if <name> \| nat { prefix \| static \| dynamic } } } } |
| ipmaccfg | ipmaccfg { { ipmac_log { on \| off } } \| { ipmac_check { on \| off } } \| show } |
| ips_url_trojan | ips_url_trojan { start \| stop } |
| ipsconfig | ipsconfig { add type policy name <name> comment <comment> policyid <id> \| set type policy name <name> { group <name> \| signature <name> } [ active { on \| off } ] [ log { on \| off } ] [ alertmail { on \| off } ] [ drop { on \| off } ] [ resetsend { on \| off } ] [ resetrecv { on \| off } ] [ dropsession { on \| off } ] \| del type policy policyid <id> \| show policy \| showlocal \| addlocal sip { any \| <all_ip> } sport { any \| <all_port> } dip { any \| <all_ip> } dport { any \| <all_port> } protocol { tcp \| udp } name <comment> signature <comment> [ offset <number> ] [ depth <number> ] \| setlocal <number> sip { any \| <all_ip> } sport { any \| <all_port> } dip { any \| <all_ip> } dport { any \| <all_port> } protocol { tcp \| udp } name <comment> signature <comment> [ offset <number> ] [ depth <number> ] \| activatelocal <number> \| blocklocal <number> \| dellocal <number> \| startup \| stop \| setpkt usbstorage <string> maxsize <number> packet_max <number> active { on \| off } upload { on server <string> port <number> [ username <string> ] [ password <string> ] \| off } \| showpkt { policy \| filelist } \| delpkt { id <number> \| all } \| setreasm active { on \| off } max_session <number> max_mem <number> \| showreasm \| setmode { stream \| packet } \| showmode \| loadsig } |
| isp | isp { update filename <name> id <id> \| export filename <name> id <id> \| flush ispname <name> \| insert ip <string> netmask <string> ispaddr <name> \| ispaddr <name> set [ active ] { on \| off } \| add ispaddr <name> nexthop <single_ip> dev <string> metric <id> \| set ispaddr <name> nexthop <single_ip> dev <string> metric <id> \| del ispaddr <name> } |

| | |
|---|---|
| license | license { show \| set { module { AdvRoute \| VMFW \| PolicyAgent \| ACSC \| HA \| VPN \| SSLVPN \| VPNEkey \| AV \| AVUpdate \| IPS \| IPSUpdate \| PC \| APC \| APCUpdate \| URL \| URLUpdate \| URLTrojan \| URLTrojanUpdate \| Scanner \| ScannerUpdate \| UTMLicense } active { on \| try } } \| upload <filename> } |
| linkage | linkage { set { puma { ip <single_ip>+ port <single_port> \| cert <filename> password <password> } \| nsfocus { ip <single_ip>+ port <single_port> \| cert <filename> passwd <passwd> } \| venus ip <single_ip>+ port <single_port> \| ism { ip <single_ip>+ port <single_port> \| cert <filename> password <password> } \| netpower { ip <single_ip>+ port <single_port> \| cacert <filename> consolecert <filename> consolekey <filename> } \| safemate { port <single_port> \| keyfile <filename> } \| ignoreip [ <single_ip>+ ] } \| on { puma \| nsfocus \| venus \| netpower \| safemate \| ism \| redirect redirectip <single_ip> localport <name> } \| off { puma \| nsfocus \| venus \| netpower \| safemate \| ism \| redirect } \| clean blockip \| show } |
| logserver | logserver { set ip <single_ip> port <single_port> [ protocol udp ] \| unset \| show } |
| logset | logset set { overwrite { on \| off } sendemail { on \| off } \| type [ <module> \| <help> ] \| export [ <path> \| <help> ] \| space <number> \| level <number> } |
| Macbind | macbind { detect { if <name> \| ip <single_ip> } \| { { add \| modify } ip <single_ip> mac <mac> unique { on \| off } } \| del ip <single_ip> \| show } |
| mirrorset | mirrorset { add <name> [ <name>+ ] \| set <name> \| del { all \| <name> [ <name>+ ] } \| show \| stop \| restart } |
| monitor | monitor set module <name> active { on \| off } |
| multiroute | multiroute { add ip <single_ip> ifname <string> weight <number> active { on \| off } [ detectip1 <single_ip> ] [ detectip2 <single_ip> ] \| set { routeconfig ip <single_ip> ifname <string> [ weight <number> \| active { on \| off } ] \| routestatus [ freq <number> \| active { on \| off } ] } \| show { routeconfig [ ip <single_ip> \| ifname <string> ] \| routestatus \| systemroute } \| del ip <single_ip> ifname <string> \| restart \| on \| off } |
| newconfig | newconfig { save \| reset \| import <filename> \| export <filename> [ encrypt { on \| off } ] \| import_modules <module> <filename> \| export_modules <module> <filename> [ encrypt { on \| off } ] \| extract } |
| nscanner | nscanner { dip <name> [ resultfile <name> ] [ plugin_set <number> ] [ host_num { default \| <number> } ] \| add type { 0 \| 1 } time <string> name <name> dip <name> [ plugin_set <number> ] [ host_num { default \| <number> } ] [ comment <comment> ] active { on \| off } \| edit type { 0 \| 1 } time <string> name <name> dip <name> [ plugin_set <number> ] [ host_num { default \| <number> } ] [ comment <comment> ] active { on \| off } \| del { name <name> \| all } \| enable name <name> \| disable name <name> \| scan stoptask } |
| ntopmode | ntopmode { set { on \| off } \| show } |
| ntp | ntp { set ip <single_ip> interval <number> \| unset \| on \| off \| sync \| show } |
| option | option { show \| set filter_policy { accept \| deny } |
| pc | pc { policy { add name <name> httppolicyid <number> ftppolicyid <number> smtppolicyid <number> pop3policyid <number> comment <comment> \| set name <name> httppolicyid <number> ftppolicyid <number> smtppolicyid <number> pop3policyid <number> comment <comment> \| del name <name> } \| httppolicy { add name <name> method <string> action { forbidden \| allow } urlgrpids <string> action { forbidden \| allow } urlcontentgrpid <number> action { forbidden \| allow } htmlcontentgrpid <number> action { forbidden \| allow } extgrpids <string> action { forbidden \| allow } mimegrpid <number> action { forbidden \| allow } urlmax |

| | |
|---|---|
| | <number> webmail { on \| off } advance { on \| off } log { on \| off } comment <comment> \| set name <name> method <string> action { forbidden \| allow } urlgrpids <string> action { forbidden \| allow } urlcontentgrpid <number> action { forbidden \| allow } htmlcontentgrpid <number> action { forbidden \| allow } extgrpids <string> action { forbidden \| allow } mimegrpid <number> action { forbidden \| allow } urlmax <number> webmail { on \| off } advance { on \| off } log { on \| off } comment <comment> \| del name <name> } \| ftppolicy { add name <name> method <string> action { forbidden \| allow } userid <number> action { forbidden \| allow } fileid <number> action { forbidden \| allow } upids <string> action { forbidden \| allow } downids <string> action { forbidden \| allow } banner <string> advance { on \| off } log { on \| off } comment <comment> \| set name <name> method <string> action { forbidden \| allow } userid <number> action { forbidden \| allow } fileid <number> action { forbidden \| allow } upids <string> action { forbidden \| allow } downids <string> action { forbidden \| allow } banner <string> advance { on \| off } log { on \| off } comment <comment> \| del name <name> } \| smtppolicy { add name <name> toeid <number> action { forbidden \| allow } fromeid <number> action { forbidden \| allow } subjectid <number> action { forbidden \| allow } blackaddrid <number> action { forbidden \| allow } advance { on \| off } ebomb slim <number> elim <number> time <number> ebipid <number> log { on \| off } comment <comment> \| set name <name> toeid <number> action { forbidden \| allow } fromeid <number> action { forbidden \| allow } subjectid <number> action { forbidden \| allow } blackaddrid <number> action { forbidden \| allow } advance { on \| off } ebomb slim <number> elim <number> time <number> ebipid <number> log { on \| off } comment <comment> \| del name <name> } \| pop3policy { add name <name> toeid <number> action { forbidden \| allow } fromeid <number> action { forbidden \| allow } subjectid <number> action { forbidden \| allow } log { on \| off } comment <comment> \| set name <name> toeid <number> action { forbidden \| allow } fromeid <number> action { forbidden \| allow } subjectid <number> action { forbidden \| allow } log { on \| off } comment <comment> \| del name <name> } \| content { urlgrp { add name <name> comment <comment> \| set name <name> comment <comment> \| del name <name> } \| url { add url <string> gid <number> \| set id <number> url <string> \| del id <number> } \| urlcontentgrp { add name <name> comment <comment> \| set name <name> comment <comment> \| del name <name> } \| urlcontent { add urlcontent <string> gid <number> \| set id <number> urlcontent <string> \| del id <number> } \| extgrp { add name <string> comment <comment> \| set name <string> comment <comment> \| del name <string> } \| ext { add ext <string> gid <number> \| set id <number> ext <string> \| del id <number> } \| mimegrp { add name <name> application { on \| partial \| off } video { on \| partial \| off } audio { on \| partial \| off } image { on \| partial \| off } text { on \| partial \| off } comment <comment> \| set name <name> application { on \| partial \| off } video { on \| partial \| off } audio { on \| partial \| off } image { on \| partial \| off } text { on \| partial \| off } comment <comment> \| del name <name> } \| mime add gid <number> name <name> \| usrnamegrp { add name <name> comment <comment> \| set name <name> comment <comment> \| del name <name> } \| usrname { add name <name> gid <number> \| set id <number> name <name> \| del id <number> } \| emailgrp { add name <name> comment <comment> \| set name <name> comment <comment> \| del name <name> } \| email { add email <string> gid <number> \| set id <number> email <string> \| del id <number> } \| subjectgrp { add name <name> comment <comment> \| set name <name> comment <comment> \| del name <name> } \| subject { add subject <string> gid <number> \| set id <number> subject <string> \| del id <number> } \| ipgrp { add name <name> comment <comment> \| set name <name> comment <comment> \| del name <name> } \| ip { add type <number> addr <single_ip> gid <number> \| set id <number> type <number> addr <single_ip> \| del id <number> } \| htmlcontentgrp { add name <name> comment <comment> \| set name <name> comment <comment> \| del name <name> } \| htmlcontent { add htmlcontent <string> gid <number> \| set id <number> htmlcontent <string> \| del id <number> } \| filenamegrp { add name <name> comment <comment> \| set name <name> comment |

| | |
|---|---|
| | <comment> \| del name <name> } \| filename { add filename <string> gid <number> \| set id <number> filename <string> \| del id <number> } } \| count { start \| stop \| reset \| read } \| download \| appdownload \| show { policy \| httppolicy \| ftppolicy \| smtppolicy \| pop3policy \| urlgrp [ id <number> ] \| extgrp [ id <number> ] \| mimegrp [id <number>] \| usrnamegrp [ id <number> ] \| emailgrp [ id <number> ] \| subjectgrp [ id <number> ] \| ipgrp [ id <number> ] \| urlcontentgrp [ id <number> ] \| htmlcontentgrp [ id <id> ] \| filenamegrp [ id <id> ] } } |
| permit | Permit show |
| Ping | Ping |
| pki | pki ca { ocsp client { { add \| set } config name <name> ocspurl <string> strictpolicy { on \| off } \| del config name <name> } \| scep client { getca caname <name> url <string> \| enroll caname <name> certname <name> reqname <name> url <string> interval <number> times <number> [ challenge { ip <ip> \| dns <string> \| email <string> } <string> ] \| getcrl caname <name> certname <name> url <string> \| getcert caname <name> certname <name> write <name> serial <number> url <string> } \| ipsec { show cert { ca \| local \| remote } \| del { cert { ca \| local \| remote } <name> \| crl <name> } } } |
| Pp_l2tp | pp_l2tp { pptp { add dialuser name <string> password <string> [ userip <single_ip> ] [ desc <comment> ] \| show { { dialuser { all \| <string> } } \| dialserver } \| set { { dialserver { iprange <comment> enctype { high \| low } auth { chapms \| chapms-v2 \| chap+chapms-v2 \| chapms+chapms-v2 \| chap+chapms+chapms-v2 } active { on \| off } ipserver <single_ip> portserver <single_port> } } \| { dialuser name <string> password <string> [ userip <single_ip> ] [ desc <comment> ] } } \| del dialuser { all \| <string> } } \| l2tp { add dialuser name <string> password <string> [ userip <single_ip> ] [ desc <comment> ] \| show { { dialuser { all \| <string> } } \| dialserver } \| set { { dialserver { iprange <comment> enctype { high \| low } auth { chap \| chapms \| chapms-v2 \| chap+chapms \| chapms+chapms-v2 \| chap+chapms+chapms-v2 } active { on \| off } ipserver <single_ip> portserver <single_port> } } \| { dialuser name <string> password <string> [ userip <single_ip> ] [ desc <comment> ] } } \| del dialuser { all \| <string> } } \| kick <single_ip> } |
| proxy | proxy { set { http { [ port <single_port> ] [ java { permit \| deny } ] [ javascript { permit \| deny } ] [ activex { permit \| deny } ] } \| ftp { [ port <single_port> ] [ get { permit \| deny } ] [ put { permit \| deny } ] [ multi { permit \| deny } ] } \| telnet port <single_port> \| smtp port <single_port> { [ domain <comment> ] [ server <comment> ] [ inmail <comment> ] [ insrv <comment> ] [ maxlength <number> ] [ maxreceiver <number> ] [ timespan <number> ] [ mailcount <number> ] } \| pop3 { [ port <single_port> ] [ maxlength <number> ] } \| socks port <single_port> \| dns dnsserver <single_ip> } \| add custom <name> port <single_port> \| del custom <name> \| show { default \| custom } \| on { http \| ftp \| telnet \| smtp \| pop3 \| socks \| dns \| ping \| msn \| custom <name> } \| \| off { http \| ftp \| telnet \| smtp \| pop3 \| socks \| dns \| ping \| msn \| custom <name> } } |
| psyn | psyn { set { group <id> port <string> [ action { on \| off } ] [ decision { on \| off } ] \| config [ keepalive <number> ] [ recheck <number> ] \| rungroup <id> [ group <string> ] [ active { on \| off } ] [ startup { on \| off } ] } \| show group <id> } |
| Reboot | Reboot |
| role | role { add rolename <name> normal [ time <number> ] [ always_online { on \| off } ] [ comment <comment> ] \| set rolename <name> normal [ time <number> ] [ always_online { on \| off } ] [ comment <comment> ] \| del { rolename <name> \| |

| | |
|---|---|
| | all } \| reset rolename <name> time \| show { rolename <name> \| all } } |
| route | route { table { add tablename <name> id <id> comment <comment> \| del tablename <name> } \| troute { add destip <all_ip> nexthop <single_ip> dev <name> metric <id> tablename <name> \| set destip <all_ip> nexthop <single_ip> dev <name> metric <id> tablename <name> id <id> \| del tablename <name> id <id> \| active id <id> [ on \| off ] } \| rule { add sip <all_ip> dip <all_ip> iif <name> service <name> prio <id> tablename <name> isp { on \| off } \| set sip <all_ip> dip <all_ip> iif <name> service <name> prio <id> tablename <name> id <id> isp { on \| off } \| del prio <id> } \| show \| startup \| { ipv6 troute { add destip <net_ipv6> dev <name> metric <number> [ nexthop <single_ipv6> ] \| del id <number> \| set id <number> destip <net_ipv6> dev <name> metric <number> [ nexthop <single_ipv6> ] \| active id <number> { on \| off } \| show } } } |
| rule | rule { add type { permit name <name> [ id <id> ] [ sa { any \| <name> \| <multi_ip> } ] [ sport <comment> ] [ smac <mac> ] [ da { any \| <name> \| <multi_ip> } ] [ iif { any \| <name> } ] [ oif { any \| <name> } ] [ service { any \| <name> } ] [ time { none \| <name> } ] [ avpolicy <number> ] [ ipspolicy <number> ] [ pcpolicy <number> ] [ eimpolicy <number> ] [ long { <number> \| off } ] [ log { on \| off } ] [ synflood { <number> \| off } ] [ udpflood { <number> \| off } ] [ icmpflood { <number> \| off } ] [ pingofdeath { on \| off } ] [ active { on \| off } ] [ comment <comment> ] \| ips_url_trojan name <name> [ id <id> ] [ sa { any \| <name> \| <multi_ip> } ] [ sport <comment> ] [ da { any \| <name> \| <multi_ip> } ] [ iif { any \| <name> } ] [ oif { any \| <name> } ] [ service { any \| <name> } ] [ time { none \| <name> } ] [ log { on \| off } ] [ active { on \| off } ] [ comment <comment> ] \| greennet name <name> [ id <id> ] [ sa { any \| <name> \| <multi_ip> } ] [ sport <comment> ] [ da { any \| <name> \| <multi_ip> } ] [ iif { any \| <name> } ] [ oif { any \| <name> } ] [ time { none \| <name> } ] [ long { <number> \| off } ] [ apc <number> ] [ urlblock <id> ] [ active { on \| off } ] [ comment <comment> ] \| deny name <name> [ id <id> ] [ sa { any \| <name> \| <multi_ip> } ] [ sport <comment> ] [ smac { <mac> } ] [ da { any \| <name> \| <multi_ip> } ] [ iif { any \| <name> } ] [ oif { any \| <name> } ] [ service { any \| <name> } ] [ time { none \| <name> } ] [ log { on \| off } ] [ active { on \| off } ] [ comment <comment> ] \| proxy name <name> [ id <id> ] [ sa { any \| <name> \| <multi_ip> } ] [ sport <comment> ] [ smac <mac> ] [ da { any \| <name> \| <multi_ip> } ] [ iif { any \| <name> } ] [ service <name> ] [ proxy <name> ] [ time { none \| <name> } ] [ log { on \| off } ] [ active { on \| off } ] [ comment <comment> ] \| auth name <name> [ id <id> ] [ sa { any \| <name> \| <multi_ip> } ] [ sport <comment> ] [ smac <mac> ] [ da { any \| <name> \| <multi_ip> } ] [ iif { any \| <name> } ] [ oif { any \| <name> } ] [ service { any \| <name> } ] [ time { none \| <name> } ] [ log { on \| off } ] [ synflood { <number> \| off } ] [ udpflood { <number> \| off } ] [ icmpflood { <number> \| off } ] [ pingofdeath { on \| off } ] [ active { on \| off } ] [ comment <comment> ] \| vpn name <name> [ id <id> ] [ sa { any \| <name> \| <multi_ip> } ] [ sport <comment> ] [ smac <mac> ] [ da { any \| <name> \| <multi_ip> } ] [ iif { any \| <name> } ] [ oif { any \| <name> } ] [ service { any \| <name> } ] [ time { none \| <name> } ] [ log { on \| off } ] [ synflood { <number> \| off } ] [ udpflood { <number> \| off } ] [ icmpflood { <number> \| off } ] [ pingofdeath { on \| off } ] [ active { on \| off } ] [ comment <comment> ] \| nat name <name> [ id <id> ] [ sa { any \| <name> \| <multi_ip> } ] [ sport <comment> ] sat { <name> \| <single_ip> } [ satport <comment> ] [ da { any \| <name> \| <multi_ip> } ] [ oif { any \| <name> } ] [ service { any \| <name> } ] [ log { on \| off } ] [ active { on \| off } ] [ comment <comment> ] \| masquerade name <name> [ id <id> ] [ sa { any \| <name> \| <multi_ip> } ] [ sport <comment> ] [ satport <comment> ] [ da { any \| <name> \| <multi_ip> } ] [ oif { any \| <name> } ] [ service { any \| <name> } ] [ log { on \| off } ] [ active { on \| off } ] [ comment <comment> ] \| nataccept name <name> [ id <id> ] [ sa { any \| <name> \| <multi_ip> } ] [ sport <comment> ] [ da { any \| <name> \| <multi_ip> } ] [ oif { any \| <name> } ] [ service { any \| <name> } ] [ log { on \| off } ] [ active { on \| off } ] |

| | |
|---|---|
| | [ comment <comment> ] \| portmap name <name> [ id <id> ] [ sa { any \| <name> \| <multi_ip> } ] [ sport <comment> ] [ sat { <name> \| <single_ip> \| none } ] [ pa <single_ip> ] [ ia <name> ] [ iif { any \| <name> } ] [ oif { any \| <name> } ] [ ps <name> ] [ is <name> ] [ log { on \| off } ] [ active { on \| off } ] [ hideinner { on \| off } ] [ comment <comment> ] \| portaccept name <name> [ id <id> ] [ sa { any \| <name> \| <multi_ip> } ] [ sport <comment> ] [ pa <single_ip> ] [ iif { any \| <name> } ] [ ps <name> ] [ log { on \| off } ] [ active { on \| off } ] [ comment <comment> ] \| ipmap name <name> [ id <id> ] [ sa { any \| <name> \| <multi_ip> } ] [ sat { <name> \| <single_ip> \| none } ] [ pa <single_ip> ] [ ia <name> ] [ iif { any \| <name> } ] [ oif { any \| <name> } ] [ log { on \| off } ] [ active { on \| off } ] [ hideinner { on \| off } ] [ comment <comment> ] \| ipaccept name <name> [ id <id> ] [ sa { any \| <name> \| <multi_ip> } ] [ pa <single_ip> ] [ iif { any \| <name> } ] [ log { on \| off } ] [ active { on \| off } ] [ comment <comment> ] \| antispam name <name> [ id <id> ] [ sa { any \| <name> \| <ip> } ] [ sport <port> \| none ] [ smac <mac> \| none ] [ da { any \| <name> \| <ip> } ] [ iif { any \| <interface> } ] [ time { <name> \| none } ] [ active { on \| off } ] [ comment <comment> ] \| uids name <name> [ id <id> ] [ sa { any \| <name> \| <ip> } ] [ da { any \| <name> \| <ip> } ] [ iif { any \| <name> } ] [ service { any \| <name> } ] [ time { none \| <name> } ] [ smac <mac> ] [ avpolicy <number> ] [ ipspolicy <number> ] [ active { on \| off } ] [ comment <comment> ] } \| set id <id> { [ type { permit \| deny \| proxy \| auth \| vpn \| nat \| masquerade \| nataccept \| portmap \| portaccept \| ipmap \| ipaccept \| greennet \| ips_url_trojan \| antispam \| uids } ] [ newid <id> ] [ name <name> ] [ sa { any \| <name> \| <multi_ip> } ] [ sat { <name> \| <single_ip> \| none } ] [ sport <comment> ] [ satport <comment> ] [ smac <mac> ] [ da { any \| <name> \| <multi_ip> } ] [ pa <single_ip> ] [ ia <name> ] [ iif { any \| <name> } ] [ oif { any \| <name> } ] [ service { any \| <name> } ] [ proxy <name> ] [ ps <name> ] [ is <name> ] [ time { none \| <name> } ] [ avpolicy <number> ] [ ipspolicy <number> ] [ pcpolicy <number> ] [ eimpolicy <number> ] [ long { <number> \| off } ] [ log { on \| off } ] [ synflood { <number> \| off } ] [ udpflood { <number> \| off } ] [ icmpflood { <number> \| off } ] [ pingofdeath { on \| off } ] [ active { on \| off } ] [ hideinner { on \| off } ] [ apc <number> ] [ comment <comment> ] } \| del { id <id> \| all } \| show [ id <id> ] \| refresh \| ipv6 { add type { permit name <name> [ id <id> ] [ srcip { <net_ipv6> \| ipname <name> \| any } ] [ dstip { <net_ipv6> \| ipname <name> \| any } ] [ srcport <port> ] [ smac <mac> ] [ iif { any \| <name> } ] [ oif { any \| <name> } ] [ service { any \| <name> } ] [ avpolicy <number> ] [ ipspolicy <number> ] [ pcpolicy <number> ] [ eimpolicy <number> ] [ exhah { on \| off } [ spi <string> ] [ length <string> ] [ reschk { on \| off } ] ] [ exhdst { on \| off } [ length <string> ] [ opt <string> ] ] [ exhfrag { on \| off } [ id <string> ] [ length <string> ] [ reschk { on \| off } ] [ first { on \| off } ] [ moreorlast { more \| last } ] ] [ exhhbh { on \| off } [ length <string> ] [ opt <string> ] ] [ exhmh { on \| off } [ type <string> ] ] [ exhrt { on \| off } [ type <string> ] [ segsleft <string> ] [ length <string> ] ] [ exhesp { on \| off } [ spi <string> ] ] [ active { on \| off } ] [ log { on \| off } ] [ comment <comment> ] [ time { none \| <name> } ] \| deny name <name> [ id <id> ] [ srcip { <net_ipv6> \| ipname <name> \| any } ] [ dstip { <net_ipv6> \| ipname <name> \| any } ] [ srcport <port> ] [ smac <mac> ] [ iif { any \| <name> } ] [ oif { any \| <name> } ] [ service { any \| <name> } ] [ exhah { on \| off } [ spi <string> ] [ length <string> ] [ reschk { on \| off } ] ] [ exhdst { on \| off } [ length <string> ] [ opt <string> ] ] [ exhfrag { on \| off } [ id <string> ] [ length <string> ] [ reschk { on \| off } ] [ first { on \| off } ] [ moreorlast { more \| last } ] ] [ exhhbh { on \| off } [ length <string> ] [ opt <string> ] ] [ exhmh { on \| off } [ type <string> ] ] [ exhrt { on \| off } [ type <string> ] [ segsleft <string> ] [ length <string> ] ] [ exhesp { on \| off } [ spi <string> ] ] [ active { on \| off } ] [ log { on \| off } ] [ time { none \| <name> } ] [ comment <comment> ] \| uids name <name> [ id <id> ] [ srcip { <net_ipv6> \| ipname <name> \| any } ] [ dstip { <net_ipv6> \| ipname <name> \| any } ] [ smac <mac> ] [ iif { any \| <name> } ] [ service { any \| <name> } ] [ avpolicy <number> ] [ ipspolicy <number> ] [ active { on \| off } ] [ comment <comment> ] [ time { none \| <name> } ] } \| set id <id> [ type { permit \| deny \| uids } ] [ name <name> ] [ newid <id> ] [ srcip { <net_ipv6> \| ipname <name> \| any } ] [ dstip { <net_ipv6> \| ipname <name> \| any } ] [ srcport |

| | |
|---|---|
| | <port> ] [ smac <mac> ] [ iif { any \| <name> } ] [ oif { any \| <name> } ] [ service { any \| <name> } ] [ avpolicy <number> ] [ ipspolicy <number> ] [ pcpolicy <number> ] [ eimpolicy <number> ] [ exhah { on \| off } [ spi <string> ] [ length <string> ] [ reschk { on \| off } ] ] [ exhdst { on \| off } [ length <string> ] [ opt <string> ] ] [ exhfrag { on \| off } [ id <string> ] [ length <string> ] [ reschk { on \| off } ] [ first { on \| off } ] [ moreorlast { more \| last } ] ] [ exhhbh { on \| off } [ length <string> ] [ opt <string> ] ] [ exhmh { on \| off } [ type <string> ] ] [ exhrt { on \| off } [ type <string> ] [ segsleft <string> ] [ length <string> ] ] [ exhesp { on \| off } [ spi <string> ] ] [ active { on \| off } ] [ log { on \| off } ] [ comment <comment> ] [ time { none \| <name> } ] \| del { id <id> \| all } \| show [ id <id> ] } } |
| Rz | Rz |
| sarp | sarp { show \| set <single_ip> <mac> <string20> <string20> \| del <single_ip> \| active <single_ip> \| inactive <single_ip> \| timeout <string> [ <string> ] } |
| sataddr | sataddr { add name <name> ip <sect_ip> [ comment <comment> ] \| set name <name> { [ ip <sect_ip> ] [ comment <comment> ] } \| del name <name> \| show [ name <name> ] } |
| Serveraddr | serveraddr { add name <name> ip <single_ip> [ ip <single_ip> [ ip <single_ip> [ ip <single_ip> [ ip <single_ip> [ ip <single_ip> [ ip <single_ip> [ ip <single_ip> ] ] ] ] ] ] ] ] [ comment <comment> ] \| set name <name> { [ ip <single_ip> [ ip <single_ip> [ ip <single_ip> [ ip <single_ip> [ ip <single_ip> [ ip <single_ip> [ ip <single_ip> [ ip <single_ip> ] ] ] ] ] ] ] ] [ comment <comment> ] } \| del name <name> \| show [ name <name> ] } |
| serveraddr6 | serveraddr6 { add name <name> ip <ip> [ ip <ip> [ ip <ip> [ ip <ip> [ ip <ip> [ ip <ip> [ ip <ip> [ ip <ip> ] ] ] ] ] ] ] [ comment <comment> ] \| set name <name> { [ ip <ip> [ ip <ip> [ ip <ip> [ ip <ip> [ ip <ip> [ ip <ip> [ ip <ip> [ ip <ip> ] ] ] ] ] ] ] ] [ comment <comment> ] } \| del name <name> \| show [ name <name> ] } |
| servgrp | servgrp { add name <name> [ comment <comment> ] \| set name <name> { addmbr <name>+ \| delmbr <name>+ \| comment <comment> } \| del name <name> \| show [ name <name> ] } |
| servgrp6 | servgrp6 { add name <name> [ comment <comment> ] \| set name <name> { comment <comment> \| addmbr <name>+ \| delmbr <name>+ \| delallmbr } \| del name <name> \| show [ name <name> ] } |
| service | service { add { name <name> protocol { { ftp \| h323 \| tns \| irc \| rtsp \| tftp \| mms \| xdmcp \| h323_gk \| sip } port <single_port> [ comment <comment> ] \| icmp [ type { 0 \| 3 [ code { 0 \| 1 \| 2 \| 3 \| 4 \| 5 \| 6 \| 7 \| 9 \| 10 \| 11 \| 12 \| 13 \| 14 \| 15 \| any } ] \| 4 \| 5 [ code { 0 \| 1 \| 2 \| 3 \| any } ] \| 8 \| 9 \| 10 \| 11 [ code { 0 \| 1 \| any } ] \| 12 [ code { 0 \| 1 \| any } ] \| 13 \| 14 \| 17 \| 18 } ] [ comment <comment> ] \| icmp6 [ type { 0 \| 1 [ code { 0 \| 1 \| 2 \| 3 \| 4 \| any } ] \| 2 \| 3 [ code { 0 \| 1 \| any } ] \| 4 [ code { 0 \| 1 \| 2 \| any } ] \| 127 \| 128 \| 129 \| 130 \| 131 \| 132 \| 133 \| 134 \| 135 \| 136 \| 137 \| 138 [ code { 0 \| 1 \| 255 \| any } ] \| 139 \| 140 \| 141 \| 142 \| 143 \| 144 \| 145 \| 146 \| 147 \| 148 \| 149 \| 151 \| 152 \| 153 } ] [ comment <comment> ] \| { { tcp \| udp } sp <all_port> dp <all_port> \| <number> } [ protocol { { tcp \| udp } sp <all_port> dp <all_port> \| <number> } [ protocol { { tcp \| udp } sp <all_port> dp <all_port> \| <number> } [ protocol { { tcp \| udp } sp <all_port> dp <all_port> \| <number> } [ protocol { { tcp \| udp } sp <all_port> dp <all_port> \| <number> } [ protocol { { tcp \| udp } sp <all_port> dp <all_port> \| <number> } [ protocol { { tcp \| udp } sp <all_port> dp <all_port> \| <number> } ] ] ] ] ] ] ] |

| | |
|---|---|
| | [ comment <comment> ] } } \| set name <name> { comment <comment> \| protocol { ftp port <single_port> get { allow \| deny } put { allow \| deny } multi { allow \| deny } \| { h323 \| irc \| rtsp \| tftp \| mms \| xdmcp \| h323_gk \| sip \| tns } port <single_port> \| icmp [ type { 0 \| 3 [ code { 0 \| 1 \| 2 \| 3 \| 4 \| 5 \| 6 \| 7 \| 9 \| 10 \| 11 \| 12 \| 13 \| 14 \| 15 \| any } ] \| 4 \| 5 [ code { 0 \| 1 \| 2 \| 3 \| any } ] \| 8 \| 9 \| 10 \| 11 [ code { 0 \| 1 \| any } ] \| 12 [ code { 0 \| 1 \| any } ] \| 13 \| 14 \| 17 \| 18 \| any } ] \| icmp6 [ type { 0 \| 1 [ code { 0 \| 1 \| 2 \| 3 \| 4 \| any } ] \| 2 \| 3 [ code { 0 \| 1 \| any } ] \| 4 [ code { 0 \| 1 \| 2 \| any } ] \| 127 \| 128 \| 129 \| 130 \| 131 \| 132 \| 133 \| 134 \| 135 \| 136 \| 137 \| 138 [ code { 0 \| 1 \| 255 \| any } ] \| 139 \| 140 \| 141 \| 142 \| 143 \| 144 \| 145 \| 146 \| 147 \| 148 \| 149 \| 151 \| 152 \| 153 } ] \| { tcp \| udp } sp <all_port> dp <all_port> \| <number> } [ protocol { { tcp \| udp } sp <all_port> dp <all_port> \| <number> } [ protocol { { tcp \| udp } sp <all_port> dp <all_port> \| <number> } [ protocol { { tcp \| udp } sp <all_port> dp <all_port> \| <number> } [ protocol { { tcp \| udp } sp <all_port> dp <all_port> \| <number> } [ protocol { { tcp \| udp } sp <all_port> dp <all_port> \| <number> } [ protocol { { tcp \| udp } sp <all_port> dp <all_port> \| <number> } ] ] ] ] ] ] } \| del name <name> \| show { default \| dynamic \| icmp \| icmp6 \| common \| name <name> } \| refresh } |
| sysmon | Sysmon show |
| System | System show |
| Tcpdump | Tcpdump |
| time | time { add name <name> type { once start <date> <single_time> stop <date> <single_time> [ comment <comment> ] \| week { [ sun <sect_time> ] [ mon <sect_time> ] [ tue <sect_time> ] [ wed <sect_time> ] [ thu <sect_time> ] [ fri <sect_time> ] [ sat <sect_time> ] } [ comment <comment> ] } \| set name <name> type { once { [ start <date> <single_time> stop <date> <single_time> ] [ comment <comment> ] } \| week { [ sun <sect_time> ] [ mon <sect_time> ] [ tue <sect_time> ] [ wed <sect_time> ] [ thu <sect_time> ] [ fri <sect_time> ] [ sat <sect_time> ] [ comment <comment> ] } } \| del name <name> \| show [ name <name> ] } |
| timegrp | timegrp { add name <name> [ comment <comment> ] \| set name <name> { addmbr <name>+ \| delmbr <name>+ \| delallmbr \| comment <comment> } \| del name <name> \| show [ name <name> ] } |
| Traceroute | traceroute |
| Tunnel | tunnel ipv6 { set tun6to4 { active { on \| off } \| ttl <number> local <single_ip> addr6 <all_ipv6> \| addr6 <all_ipv6> \| restart } \| add { tun6to4 ttl <number> local <single_ip> addr6 <all_ipv6> } \| del tun6to4 \| show tun6to4 } |
| Uevent | uevent { ips { active { on \| off } \| server <string> port <string> } \| av { active { on \| off } \| server <string> port <string> } \| show } |
| upgrade | Upgrade show |
| upnp | upnp { set exif <name> inif <name> \| start \| stop \| show status \| rule { add name <name> ip <all_ip> [ comment <comment> ] \| del { id <id> \| all } \| set id <id> { [ name <name> ] \| [ ip <all_ip> ] \| [ comment <comment> ] } \| show } } |

| | |
|---|---|
| urlblock | urlblock { add type policy name <name> comment <comment> policyid <id> \| set type policy name <name> signature <name> [ enabled { on \| off } ] [ log { on \| off } ] [ alertmail { on \| off } ] [ drop { on \| off } ] [ resetsend { on \| off } ] [ resetrecv { on \| off } ] [ sound { on \| off } ] \| del type policy policyid <id> \| startup \| stop \| show policy } |
| usbcli | usbcli { scan { all \| show } \| test <string> } |
| user | user { add username <name> auth-type { local-pwd pwd <string> \| local-cert \| vip \| cert-pwd pwd <string> \| dyn-pwd pwd <string> [ sn <filename> ] } [ role <string> ] [ true-name <name> ] [ bind-ip6 <single_ipv6> \| bind-ip4 <single_ip> ] [ bind-mac <mac> ] [ active { on \| off } ] [ modify-pwd-allow { on \| off } ] [ first-change-pwd { on \| off } ] [ available-period <number> ] [ pwd-available-period <number> ] [ connect-rule <name> ] [ comment <comment> ] \| set username <name> { auth-type { local-pwd pwd <string> \| local-cert \| vip \| dyn-pwd [ pwd <string> [ sn <filename> ] \| sn <filename> ] \| cert-pwd [ pwd <string> ] [ role <string> ] [ true-name <name> ] [ bind-ip6 <single_ipv6> \| bind-ip4 <single_ip> ] [ bind-mac <mac> ] [ active { on \| off } ] [ modify-pwd-allow { on \| off } ] [ first-change-pwd { on \| off } ] [ available-period <number> ] [ pwd-available-period <number> ] [ connect-rule <name> ] [ comment <comment> ] } [ role <string> ] [ true-name <name> ] [ bind-ip6 <single_ipv6> \| bind-ip4 <single_ip> ] [ bind-mac <mac> ] [ active { on \| off } ] [ modify-pwd-allow { on \| off } ] [ first-change-pwd { on \| off } ] [ available-period <number> ] [ pwd-available-period <number> ] [ connect-rule <name> ] [ comment <comment> ] \| import-sn <filename> \| syndynpass <string> dyntime <string> dynclock <string> } \| del { username <name> \| all } \| show { lock \| username <name> \| all \| online [ total \| from <number> to <number> ] } \| break username <name> \| reset username <name> { time \| password <string> } \| lock username <name> time <number> \| unlock username <name> } |
| vhq | vhq { setvq { on dir <string> http { on \| off } ftp { on \| off } smtp { on \| off } pop3 { on \| off } \| off \| del id <id> \| del all \| startup } \| sethq { on time <number> http { on \| off } ftp { on \| off } smtp { on \| off } pop3 { on \| off } \| off \| startup } } |
| vmfw | vmfw { create { vmfwname <name> \| chains [ name <name> ] } \| delete { vmfwname <name> \| interface name <name> vmfwname <name> } \| add interface name <name> type { share \| exclusive } vmfwname <name> \| show { name \| interface } |
| vpn | vpn { up { { gatewaytunnel \| clienttunnel } <name> \| all } \| down { { gatewaytunnel \| clienttunnel } <name> \| all } \| set { default [ ikelifetime <number> ] [ ipseclifetime <number> ] [ prekey <string> ] [ ipsec_active { on \| off } ] [ dhcpactive { on \| off } ] [ dhcpipaddr <ip> ] [ dhcpdevice <name> ] \| rule name <name> subnettype { subnet leftsubnet <string> rightsubnet <string> \| subnets leftsubnets <string> rightsubnets <string> } leftservicetype { defaultservice leftservice <name> \| customservice leftprotoport <string> } rightservicetype { defaultservice rightservice <name> \| customservice rightprotoport <string> } \| gatewaytunnel name <name> [ interface <name> ] [ ikename <name> ] [ rulename <name> ] [ ipsec <string> ] [ type { tunnel \| transport } ] [ phase2 { esp \| ah } ] [ pfs { yes \| no } ] [ compress { yes \| no } ] [ ipseclifetime <number> ] [ dpddelay <number> ] [ dpdtimeout <number> ] [ dpdaction { hold \| restart } ] [ initiator { start \| ignore } ] [ active { on \| off } ] \| clienttunnel name <name> [ interface <name> ] [ ikename <name> ] [ rulename <name> ] [ ipsec <string> ] [ type { tunnel \| transport } ] [ pfs { yes \| no } ] [ phase2 { esp \| ah } ] [ ipseclifetime <number> ] [ dpddelay <number> ] [ dpdtimeout <number> ] [ active { on \| off } ] \| tunnelgroup name <name> rulename <name> tunnels <string> [ comment <comment> ] \| ikeconfig { client { main { psk name <name> rightaddr <ip> [ prekey <string> ] [ ike <string> ] [ dhgroup { g1 \| g2 \| g5 } |

| | |
|---|---|
| | ] [ ikelifetime <number> ] [ idtype <number> ] [ leftid <string> ] [ rightid <string> ] [ xauth { on \| off } ] \| rsasig name <name> rightaddr <ip> leftcert <name> rightcert <name> [ idtype <number> ] [ leftid <string> ] [ rightid <string> ] [ ike <string> ] [ dhgroup { g1 \| g2 \| g5 } ] [ ikelifetime <number> ] [ xauth { on \| off } ] } \| aggr { psk name <name> rightaddr <ip> [ prekey <string> ] [ ike <string> ] [ dhgroup { g1 \| g2 \| g5 } ] [ idtype <number> ] [ leftid <string> ] [ rightid <string> ] [ ikelifetime <number> ] \| rsasig name <name> rightaddr <ip> [ idtype <number> ] [ leftid <string> ] [ rightid <string> ] leftcert <name> rightcert <name> [ ike <string> ] [ dhgroup { g1 \| g2 \| g5 } ] [ ikelifetime <number> ] [ xauth { on \| off } ] } } \| gateway { main { psk name <name> righttype <number> rightaddr <ip> [ idtype <number> ] [ leftid <string> ] [ rightid <string> ] [ prekey <string> ] [ ike <string> ] [ dhgroup { g1 \| g2 \| g5 } ] [ ikelifetime <number> ] \| rsasig name <name> righttype <number> rightaddr <ip> leftcert <name> rightcert <name> [ ike <string> ] [ dhgroup { g1 \| g2 \| g5 } ] [ ikelifetime <number> ] [ idtype <number> ] [ leftid <string> ] [ rightid <string> ] } \| aggr { psk name <name> righttype <number> rightaddr <ip> [ prekey <string> ] [ idtype <number> ] [ leftid <string> ] [ rightid <string> ] [ ike <string> ] [ dhgroup { g1 \| g2 \| g5 } ] [ ikelifetime <number> ] \| rsasig name <name> righttype <number> rightaddr <ip> [ idtype <number> ] [ leftid <string> ] [ rightid <string> ] leftcert <name> rightcert <name> [ ike <string> ] [ dhgroup { g1 \| g2 \| g5 } ] [ ikelifetime <number> ] } } } } \| add { rule name <name> subnettype { subnet leftsubnet <string> rightsubnet <string> \| subnets leftsubnets <string> rightsubnets <string> } leftservicetype { defaultservice leftservice <name> \| customservice leftprotoport <string> } rightservicetype { defaultservice rightservice <name> \| customservice rightprotoport <string> } \| gatewaytunnel name <name> interface <name> ikename <name> [ rulename <name> ] [ ipsec <string> ] [ type { tunnel \| transport } ] [ phase2 { esp \| ah } ] [ pfs { yes \| no } ] [ compress { yes \| no } ] [ ipseclifetime <number> ] [ dpddelay <number> ] [ dpdtimeout <number> ] [ dpdaction { hold \| restart } ] [ initiator { yes \| no } ] [ active { on \| off } ] \| tunnelgroup name <name> rulename <name> tunnels <string> [ comment <comment> ] \| clienttunnel name <name> interface <name> ikename <name> rulename <name> [ ipsec <string> ] [ type { tunnel \| transport } ] [ pfs { yes \| no } ] [ phase2 { esp \| ah } ] [ ipseclifetime <number> ] [ dpddelay <number> ] [ dpdtimeout <number> ] [ active { on \| off } ] \| ikeconfig { client { main { psk name <name> rightaddr <ip> [ prekey <string> ] [ ike <string> ] [ dhgroup { g1 \| g2 \| g5 } ] [ ikelifetime <number> ] [ idtype <number> ] [ leftid <string> ] [ rightid <string> ] [ xauth { on \| off } ] \| rsasig name <name> rightaddr <ip> [ idtype <number> ] [ leftid <string> ] [ rightid <string> ] leftcert <name> rightcert <name> [ ike <string> ] [ dhgroup { g1 \| g2 \| g5 } ] [ ikelifetime <number> ] [ xauth { on \| off } ] } \| aggr { psk name <name> rightaddr <ip> [ prekey <string> ] [ ike <string> ] [ dhgroup { g1 \| g2 \| g5 } ] [ idtype <number> ] [ leftid <string> ] [ rightid <string> ] [ ikelifetime <number> ] \| rsasig name <name> rightaddr <ip> [ idtype <number> ] [ leftid <string> ] [ rightid <string> ] leftcert <name> rightcert <name> [ ike <string> ] [ dhgroup { g1 \| g2 \| g5 } ] [ ikelifetime <number> ] [ xauth { on \| off } ] } } \| gateway { main { psk name <name> righttype <number> rightaddr <ip> [ idtype <number> ] [ leftid <string> ] [ rightid <string> ] [ prekey <string> ] [ ike <string> ] [ dhgroup { g1 \| g2 \| g5 } ] [ ikelifetime <number> ] \| rsasig name <name> righttype <number> rightaddr <ip> leftcert <name> rightcert <name> [ ike <string> ] [ dhgroup { g1 \| g2 \| g5 } ] [ ikelifetime <number> ] [ idtype <number> ] [ leftid <string> ] [ rightid <string> ] } \| aggr { psk name <name> righttype <number> rightaddr <ip> [ idtype <number> ] [ leftid <string> ] [ rightid <string> ] [ ike <string> ] [ dhgroup { g1 \| g2 \| g5 } ] [ ikelifetime <number> ] \| rsasig name <name> righttype <number> rightaddr <ip> [ idtype <number> ] [ leftid <string> ] [ rightid <string> ] leftcert <name> rightcert <name> [ ike <string> ] [ dhgroup { g1 \| g2 \| g5 } ] [ ikelifetime <number> ] } } } } \| show { rule { all \| <name> } \| ikeconfig { all \| <name> } \| gatewaytunnel { all \| <name> } \| clienttunnel { all \| <name> } \| tunnelgroup { all \| <name> } \| status \| default } \| del { rule { all \| <name> } \| ikeconfig { all \| <name> } \| gatewaytunnel { all \| <name> } \| clienttunnel { all \| <name> } \| tunnelgroup { all \| <name> } } \| |

| | |
|---|---|
| | version \| on \| off } |
| vrrp | Vrrp show |
| vsp | vsp { set { default_os { systemA \| systemB } } \| { get { systemA \| systemB \| backup_os \| default_os \| current_os } } \| { backup system } \| { recover { systemA \| systemB } } \| { show } } |
| wireless | wireless { on \| off \| scan \| show { station \| base \| option \| advanced } \| set { default \| { base [ mode { 11b \| 11g } ] [ channel { <number> \| auto } \| frequency { <number> \| auto } ] } \| { option [ ssid <string> ] [ hidessid { no \| yes } ] [ security_mode { disabled \| { wep [ auth { open \| share \| mixed } ] [ wep_default_key { 0 \| 1 \| 2 \| 3 } ] [ key0type { ascii \| hex } key0len { 40 \| 104 } key0 <string> ] [ key1type { ascii \| hex } key1len { 40 \| 104 } key1 <string> ] [ key2type { ascii \| hex } key2len { 40 \| 104 } key2 <string> ] [ key3type { ascii \| hex } key3len { 40 \| 104 } key3 <string> ] } \| { { wpav1 \| wpav2 } [ wpa_key <string> ] [ wpa_key_mgmt psk ] [ wpa_key_algs { TKIP \| CCMP \| mixed } ] [ wpa_gtk_rekey <number> ] [ wpa_gmk_rekey <number> ] } } } \| { advanced [ beacon_int <number> ] [ dtim_period <number> ] [ rts_threshold <number> ] [ fragm_threshold <number> ] [ shortpreamble { enable \| disable } ] [ ap_max_inactivity <number> ] [ accept_mac { <mac>+ \| none } \| deny_mac { <mac>+ \| none } ] } } |

# 第3章 快速入门

## 3.1 管理员登录

请您参照《网御星云安全网关 PowerV Web 界面操作手册》中的安装过程，安装好安全网关，并且按照第二章介绍的步骤进行配置和登录。

## 3.2 操作参考

请大家参考 web 界面左侧的顺序阅读本文档相关章节。

## 3.3 管理员退出

具体操作：执行 exit 命令

## 3.4 终端命令行配置方法

当无法通过 Web 方式登录管理界面时，通过终端命令行，按照以下步骤进行检查和处理，以恢复通过 Web 方式管理安全网关。

使用命令 interface 查看和设置网络接口的 IP 地址和管理属性；

使用命令 admhost 查看和设置管理主机 IP 地址；

使用命令 admacct 查看和设置管理员账号；

如果需要使用客户端证书的认证方式，则使用命令 admcert 查看和设置管理证书。

# 第4章 系统管理

描述与安全网关管理相关的配置，包括：系统时钟设置、时钟服务器同步、系统参数设置、模块升级、系统管理、管理主机、管理员账号、管理员证书、管理方式、IDS 产品联动、用户认证服务器、日志服务器、报警邮箱、集中管理等。

## 4.1 状态

### 4.1.1 系统信息（system）

#### 显示系统信息：

**语法：**
system show

**参数说明：**
无

**注意事项：**
无

**示例：**
ac>system show

#### 显示特征库版本信息

语法：
system show gnpatch
说明：
用来显示当前系统使用的特征码版本号、升级时间、最新下载的特征码版本号、升级时间
举例：
system show gnpatch

# 4.2 快速配置

## 4.2.1 基本配置

#### 4.2.1.1 配置桥模式

**语法：**
easyconfig set brg { on | off }

**参数说明：**
无

**注意事项：**
在 1U 平台默认配置 eth0 与 eth1 接口为透明桥模式。
在 2U 平台默认配置 eth4 与 eth5 接口为透明桥模式。

**示例：**
```
ac>easyconfig set brg on
```

#### 4.2.1.2 配置 eth3 接口 IPv4 管理接口

**语法：**
easyconfig set ipv4 ip <single_ip> mask < netmask>

**参数说明：**
<single_ip> IPv4 地址
<netmask> Ipv4 掩码

**注意事项：**
无

**示例：**
```
ac>easyconfig set ipv4 ip 10.1.5.254 mask 255.255.255.0
```

#### 4.2.1.3 配置 eth3 接口 IPv6 管理接口

**语法：**
easyconfig set ipv6 ip < single_ipv6> mask < number>

**参数说明：**
< net_ipv6> IPv6 地址

< number > Ipv6 掩码

**注意事项：**
无

**示例：**
```
ac>easyconfig set ipv6 ip 2001:288:250:2403::200 mask 64
```

#### 4.2.1.4 配置 eth3 接口 IPv4 管理主机

**语法：**
easyconfig set ipv4 adminip <single_ip> adminmask< netmask>

**参数说明：**
<single_ip> IPv4 地址
<netmask> Ipv4 掩码

**注意事项：**
无

**示例：**
```
ac>easyconfig set ipv4 adminip 10.1.5.254 adminmask 255.255.255.0
```

#### 4.2.1.5 配置 eth3 接口 IPv6 管理主机

**语法：**
easyconfig set ipv6 adminip <single_ipv6> adminmask < number>

**参数说明：**
< net_ipv6> IPv6 地址
< number > Ipv6 掩码

**注意事项：**
无

**示例：**
```
ac>easyconfig set ipv6 adminip 2001:288:250:2403::200 adminmask 64
```

#### 4.2.1.6 安全级别配置

**语法：**
easyconfig set type { utm | | fw | tc } level { high | middle | low }

**参数说明：**
无
**注意事项：**
无

**示例：**
```
ac>easyconfig set type utm level high
```

#### 4.2.1.7 显示快速配置信息

**语法：**
easyconfig show

**参数说明：**
无
**注意事项：**
无

**示例：**
```
ac>easyconfig show
```

## 4.2.2 UTM 快速配置

#### 4.2.2.1 引用策略配置

**语法：**
easyutm level { low | high | high } { avpolicy | eimpolicy | ipspolicy | pcpolicy } <id>

**参数说明：**
<id> 引用策略的 ID
**注意事项：**
无

**示例：**
```
ac>easyutm level low avpolicy 1
```

#### 4.2.2.2 配置服务开关

**语法：**
easyutm level { low | high | high } service <name> { on | off }

**参数说明：**
<name> 配置服务的名称
**注意事项：**

无

**示例：**

```
ac>easyutm level low service ftp on
```

#### 4.2.2.3 显示配置信息

**语法：**

easyutm show { low | middle | high }

**参数说明：**

无

**注意事项：**

无

**示例：**

```
ac>easyutm show low
```

## 4.2.3 流量控制快速配置

#### 4.2.3.1 新建带宽资源组

**语法：**

bw quick_bw oif <interface> minbw <number> maxbw <number> prio <number>

**参数说明：**

| | |
|---|---|
| oif | 配置网口，必选参数； |
| minbw | 配置最小带营 |
| maxbw | 配置最大带宽 |
| prio | 优先级别 |

**注意事项：**

无

**示例：**

ac> bw quick_bw oif eth0 maxbw 1000 minbw 1000 prio 5

#### 4.2.3.2 配置 apc 策略各个类别的带宽资源

**语法：**

bw apc set policyid <id> groupname <name> bandwidthname <name>

**参数说明：**

policyid <id> 配置 apc 策略的 id 号，此处为 512
groupname <name> 配置 apc 大类的名称
bandwidthname <name> 配置带宽资源组的名称

**注意事项：**

无

**示例：**

```
ac>bw apc set policyid 512 groupname p2p_download bandwidthname eth1_1000_1000_5
```

#### 4.2.3.3 配置 url 策略各个类别的带宽资源

**语法：**

bw url set policyid <id> groupid <id> bandwidthname <name>

**参数说明：**

policyid <id> 配置 url 策略的 id 号，此处为 512
groupid <id> 配置 url 大类的 id 号
bandwidthname <name> 配置带宽资源组的名称

**注意事项：**

无

**示例：**

```
ac>bw url set policyid 512 groupid 1 bandwidthname eth1_300_300_5
```

#### 4.2.3.4 配置文件类型策略各个类别的带宽资源

**语法：**

bw file set policyid <id> groupid <id> bandwidthname <name>

**参数说明：**

policyid <id> 配置文件类型策略的 id 号，此处为 256
groupid <name> 配置各文件类型的名称
bandwidthname <name> 配置带宽资源组的名称

**注意事项：**

无

**示例：**

```
ac>bw file set policyid 256 groupid 1 bandwidthname eth1_300_300_5
```

#### 4.2.3.5 配置流量控制快速配置

**语法：**

bw easyset < level { 1|2|3 } > [ service { any | <name> } ] [ bandwidthname <name> ] [ apc { 0 | 512 } ] [ url { 0 | 512 } ] [ file { 0 | 256 } ] [ rate <maxrate> ] [ mode { dstip | srcip } ] [ oif { any | <interface> } ]

**参数说明：**

level { 1|2|3 } 配置安全级别
service { any | <name> } 配置服务的名称
bandwidthname <name> 配置服务项的带宽资源组的名称
apc { 0 | 512 } 配置 apc 策略的 id 号，此处为 512
url { 0 | 512 } 配置 url 策略的 id 号，此处为 512
file { 0 | 256 } 配置文件类型策略的 id 号，此处为 256
rate <maxrate> 配置主机带宽的限制速率
mode { dstip | srcip } 配置主机带宽的控制模式
oif { any | <interface> } 配置主机带宽的输出网口

**注意事项：**

无

**示例：**

```
ac> bw easyset level 3 service FTP bandwidthname eth0_300_300_5 apc 512 url 512 file 256 rate 1000 mode dstip oif eth1
```

# 4.3 配置

## 4.3.1 日期时间

#### 4.3.1.1 时钟（clock）

## 设置系统时钟：

**语法：**

clock set <date> <time>

**参数说明：**

<date> 设置日期，格式为 yyyy/mm/dd，yyyy-mm-dd
<time> 设置时间，格式为 hh:mm:ss

**注意事项：**

不能设置系统时钟早于 2000/01/01 00:00:00

**示例：**

```
ac>clock set 2004/01/01 00:00:00
```

## 显示系统时钟：

**语法：**

clock show

**参数说明：**

无

**注意事项：**

无

**示例：**

```
ac>clock show
Clock: 2004/01/01 00:00:00
```

#### 4.3.1.2 时钟同步（ntp）

## 设置时钟同步：

**语法：**

ntp set ip <ip> interval <number>

ntp set domain <domain> interval <number>

**参数说明：**

| | |
|---|---|
| ip | 设置 NTP 时钟服务器的 IP 地址 |
| domain | 设置 NTP 时钟服务器的域名地址 |
| interval | 设置同步间隔，有效值为 1 至 65535（分钟） |

**注意事项：**

无

**示例：**

```
ac>ntp set ip 192.168.100.1 interval 60
```

## 启用时钟同步：

**语法：**
ntp on

**参数说明：**
无

**注意事项：**
无

**示例：**
ac>ntp on

## 禁用时钟同步：

**语法：**
ntp off

**参数说明：**
无

**注意事项：**
无

**示例：**
ac>ntp off

## 立即同步时钟：

**语法：**
ntp sync

**参数说明：**
无

**注意事项：**
无

**示例：**
ac>ntp sync

## 清除时钟同步设置：

**语法：**
ntp unset

**参数说明：**
无

**注意事项：**
启用时钟同步后不能清除时钟同步设置

**示例：**
```
ac>ntp unset
```

## 显示时钟同步设置：

**语法：**
ntp show

**参数说明：**
无

**注意事项：**
无

**示例：**
```
ac>ntp show
Enable: on
NTP Server: 192.168.100.1
Sync Interval(minute): 60
```

# 4.3.2 系统参数

#### 4.3.2.1 安全网关名称（hostname）

## 设置安全网关名称

**语法：**
hostname set hostname <hostname>

**参数说明：**

| | |
|---|---|
| hostname | 安全网关名称。这是一个最小长度是 1，最大长度是 20 的 ASCII 字符串，包括除制表符和问号外的任意可打印字符。 |

**注意事项：**
无

**示例：**
**ac>hostname set hostname themis**

## 显示安全网关名称

**语法：**
hostname show

**参数说明：**
无

**注意事项：**
无

**示例：**
**ac> hostname show**
Hostname: themis

# 4.3.3 集中管理 (snmp)

## 设置集中管理：

**语法：**
snmp set [snmpip <ip>] [principal <string>] [telephone <string>] [cpu <percent>] [mem <percent>] [fs <percent>] [rcomm <string>] [wcomm <string>] [comm2sec {on| off}] [trapc <string>] [comment <string>]

**参数说明：**

| | |
|---|---|
| snmpip | 设置集中管理主机 IP 地址 |
| principal | 设置负责人姓名，1 至 20 个字符 |
| telephone | 设置负责人电话，1 至 30 个字符 |
| cpu | 设置 CPU 利用率报警阈值，有效值为 1 至 100 |
| mem | 设置内存利用率报警阈值，有效值为 1 至 100 |
| fs | 设置文件系统利用率报警阈值，有效值为 1 至 100 |
| rcomm | 设置 SNMP v1&v2c 的只读团体串，1 至 32 个字符 |
| wcomm | 设置 SNMP v1&v2c 的读写团体串，1 至 32 个字符 |

| | |
|---|---|
| comm2sec | 设置是否启用 SNMP v1&v2c 团体串，有效值 on 或 off |
| trapc | 设置 SNMPv1 Trap 信息中使用的团体串 |
| comment | 设置本机备注，1 至 255 个字符 |

**示例：**

```
ac>snmp set snmpip 192.168.1.1 principal lenovo telephone 800-8108888 cpu 100 mem 90 fs 80 rcomm public wcomm private trapc public comm2sec on comment "gateway 1"
```

## 清除集中管理设置：

**语法：**

snmp unset [snmpip] [principal] [telephone] [cpu] [mem] [fs] [rcomm] [wcomm] [comm2sec] [trapc] [comment]

**参数说明：**

| | |
|---|---|
| snmpip | 清除集中管理主机 IP 地址 |
| principal | 清除负责人姓名 |
| telephone | 清除负责人电话 |
| cpu | 清除 CPU 利用率报警阈值 |
| mem | 清除内存利用率报警阈值 |
| fs | 清除文件系统利用率报警阈值 |
| rcomm | 清除 SNMP v1&v2c 的只读团体串 |
| wcomm | 清除 SNMP v1&v2c 的读写团体串 |
| comm2sec | 清除是否启用 SNMP v1&v2c 团体串 |
| trapc | 清除 SNMPv1 Trap 信息中使用的团体串 |
| comment | 清除备注 |

**示例：**

```
ac>snmp unset
```

## 添加集中管理主机：

**语法：**

```
snmp add snmpip <ip> [ <ip> ... ]
```

**参数说明：**

| | |
|---|---|
| snmpip | 添加一个或多个管理主机 IP 地址，最多同时支持 16 个 IP |

**示例：**

```
ac>snmp add snmpip 192.168.1.2  192.168.1.3
```

## 删除集中管理主机：

**语法：**

```
snmp del snmpip <ip> [ <ip> ... ]
```

**参数说明：**

| | |
|---|---|
| snmpip | 删除一个或多个管理主机 IP 地址 |

**示例：**

```
ac>snmp del snmpip 192.168.1.2  192.168.1.3
```

## 显示集中管理设置：

**语法：**

snmp show

**示例：**

```
ac>snmp show
SNMP IP: 192.168.1.1
Principal: lenovo
Telephone: 800-8108888
CPU Threshold: 100
Memory Threshold: 90
Disk Threshold: 80
Comment: gateway 1
Read Community: public
Write Community: private
Trap Community: public
Community to Security: on
```

## 设置 SNMP v3 用户：

**语法：**

snmpusm set [user <name>] [level {noauth|auth|priv}] [authproto {MD5|SHA}] [authpass <string>] [privproto {DES|AES}] [privpass <string>] [active {on|off}]

**参数说明：**

| | |
|---|---|
| user | 设置 SNMP v3 用户名 |
| level | 设置该用户的安全级别，可选值 noauth，auth 或 priv，分别代表无认证无加密，认证不加密和认证加密 |
| authproto | 设置认证协议，可选值为 MD5 或 SHA |
| authpass | 设置认证口令，8 至 32 个字符 |
| privproto | 设置加密协议，可选值为 DES 或 AES |
| privpass | 设置加密密钥，8 至 32 个字符 |
| active | 设置是否启用 SNMP v3 用户，可选值为 on 或 off |

**示例：**

```
ac> snmpusm set user lenovo level priv authproto MD5 authpass leadsec3 privproto DES
```

```
privpass lenovoai active on
```

## 显示 SNMP v3 用户：

**语法：**

snmpusm show

**示例：**

```
ac> snmpusm show
Security Name   : lenovo
Security Level  : priv
Authentication Protocol  : MD5
Authentication Passphrase: leadsec3
Privacy Protocol         : DES
Privacy Passphrase       : lenovoai
Active SNMP v3 USM       : on
```

# 4.3.4 策略代理

本节来介绍策略代理的功能和使用方法。策略代理功能是和安管平台配合使用的。所谓策略代理，就是有安管平台统一向其所管理的设备发送命令，实现对设备的资源、规则等的配置和管理功能。目前安管平台对防火墙的管理范围包括：策略配置(安全选项、安全规则、代理服务、黑名单)资源定义、VPN 管理等，防火墙端策略代理配置提供了参数配置命令，获取策略方式命令以及启停功能的命令等，具体使用方法如下：

## 基本通信参数设置

**语法：**

policyclient set server address <ip> port <port> key “key”

**参数说明：**

ip 安管平台服务器 ip 地址

port 双方通信端口

key 双方约定密钥

**注意事项：**

无

**示例：**

ac> policyclient set server address 192.168.1.1 port 8585 key admin123

## 获取策略频率设置

**语法：**

policyclient set timer retry < retry > span < span > timeout < timeout >

**参数说明：**

retry 重试次数设置

span 状态
timeout 超时值

**注意事项：**

无

**示例：**

ac> policyclient set timer retry 3 span 20 timeout 3

## 开启策略代理功能

**语法：**

policyclient up

**参数说明：**

无

**注意事项：**

无

**示例：**

ac> policyclient up

## 设置从服务器获取策略

**语法：**

policyclient net

**参数说明：**

无

**注意事项：**

无

**示例：**

ac> policyclient net

## 设置立刻从服务器获取策略

**语法：**

policyclient now

**参数说明：**

无

**注意事项：**

无

**示例：**

ac> policyclient now

## 设置本地获取策略

**语法：**

policyclient local

**参数说明：**

无

**注意事项：**

本命令的使用前须将策略文件首先放到防火墙/tmp 目录下。

**示例：**

ac> policyclient local

### 关闭策略代理功能

**语法：**

policyclient down

**参数说明：**

无

**注意事项：**

无

**示例：**

ac> policyclient down

# 4.4 管理员配置

## 4.4.1 访问权限 (account_power)

### 添加访问权限：

**语法：**

account_power add name <name> comment <comment> { [ system { none | read | write } ] | [ network { none | read | write } ] | [ route { none | read | write } ] | [ policy { none | read | write } ] | [ user { none | read | write } ] | [ flow { none | read | write } ] | [ monitor { none | read | write } ] | [ vpn { none | read | write } ] | [ utm { none | read | write } ] | [ ipv6 { none | read | write } ] | [ log { none | read | write } ] }

**参数说明：**

| | |
|---|---|
| name | 添加管理权限的名称 |
| comment | 设置管理主机的注释，必选参数，默认为空 |
| system | 系统管理权限，可选参数，默认为 none |
| network | 网络操作权限，可选参数，默认为 none |
| route | 路由操作权限，可选参数，默认为 none |
| policy | 策略操作权限，可选参数，默认为 none |
| user | 普通用户管理权限，可选参数，默认为 none |

holescan 漏洞扫描权限，可选参数，默认为 none
flow 流量管理权限，可选参数，默认为 none
monitor 系统监测权限，可选参数，默认为 none
vpn vpn 管理权限，可选参数，默认为 none
utm utm 管理权限，可选参数，默认为 none
ipv6 IPv6 管理权限，可选参数，默认为 none
log 日志管理权限，可选参数，默认为 none
none 无读写权限，可选参数，默认为 none
read 只读权限，可选参数，默认为 none
write 可读可写权限，可选参数，默认为 none

**注意事项：**
无

**示例：**
ac> account_power add name testpower comment “test power”system none network write route write policy write user write holescan write flow write monitor write vpn write utm write ipv6 write log write

## 设置访问权限：

**语法：**
account_power set name <name> comment <comment> { [ system { none | read | write } ] | [ spuer { none | read | write } ] | [ network { none | read | write } ] | [ route { none | read | write } ] | [ policy { none | read | write } ] | [ user { none | read | write } ] | [ holescan { none | read | write } ] | [ flow { none | read | write } ] | [ monitor { none | read | write } ] | [ vpn { none | read | write } ] | [ utm { none | read | write } ] | [ ipv6 { none | read | write } ] | [ log { none | read | write } ] }

**参数说明：**
name 设置管理权限的名称
comment 设置管理主机的注释，必选参数，默认为空
system 系统管理权限，可选参数，默认为 none
network 网络操作权限，可选参数，默认为 none
route 路由操作权限，可选参数，默认为 none
policy 策略操作权限，可选参数，默认为 none
user 普通用户管理权限，可选参数，默认为 none
holescan 漏洞扫描权限，可选参数，默认为 none
flow 流量管理权限，可选参数，默认为 none
monitor 系统监测权限，可选参数，默认为 none
vpn vpn 管理权限，可选参数，默认为 none
utm utm 管理权限，可选参数，默认为 none
ipv6 IPv6 管理权限，可选参数，默认为 none
log 日志管理权限，可选参数，默认为 none
none 无读写权限，可选参数，默认为 none

read 只读权限，可选参数，默认为 none
write 可读可写权限，可选参数，默认为 none

**注意事项：**
无

**示例：**
ac> account_power set name testpower comment “test power”system read network write route write policy write user write holescan write flow write monitor write vpn write utm write ipv6 write log write

## 删除访问权限：

**语法：**
account_power del name <name>

**参数说明：**
name 欲删除管理权限的名称

**注意事项：**
无

**示例：**
ac> account_power del name testpower

## 显示访问权限名称：

**语法：**
account_power show [ all | name <name> ]

**参数说明：**
all 显示所有的访问权限名,也可以省略“all”
name 显示指定的访问权限名

**注意事项：**
无

**示例：**
ac> account_power show
ID 名称 描述
1 super root account
ac>account_power show name super

名称 描 述
super root account

system: 读写
network: 读写
route: 读写
policy: 读写
user: 读写
holescan 读写
flow: 读写
speed: 读写
utm: 读写
vpn: 读写
ipv6: 读写
monitor: 读写
log: 读写

## 4.4.2 管理主机（admhost）

### 添加管理主机：

**语法：**
admhost add ip <ip> netmask <netmask> [ comment <comment> ]
admhost add ipv6 <ip/prefix> [ comment <comment> ]
**参数说明：**
ip 设置管理主机的 IP 地址
netmask 设置管理主机的子网掩码
ipv6 设置管理主机的 IPv6 地址
comment 设置管理主机的注释，可选参数，默认为空

**注意事项：**
无

**示例：**
ac>admhost add ip 192.168.1.1 netmask 255.255.255.255 comment “administration host”

ac>admhost add ipv6 2001:1::200/64 comment administration host "

### 删除管理主机：

**语法：**

admhost del ip <ip> netmask <netmask>

admhost del ipv6 <ip/prefix>

**参数说明：**

| | |
|---|---|
| ip | 指定欲删除的管理主机的 IP 地址 |
| netmask | 指定欲删除的管理主机的子网掩码 |
| ipv6 | 指定欲删除的管理主机的 IPv6 地址 |

**注意事项：**

无

**示例：**

```
ac>admhost del ip 192.168.1.1 netmask 255.255.255.255
ac>admhost del ipv6 2001:1::/64
```

## 显示管理主机：

**语法：**

admhost show

admhost show all

admhost show ipv4

admhost show ipv6

**参数说明：**

| | |
|---|---|
| all | 显示所有的管理主机地址,也可以省略“all” |
| ipv4 | 显示 IPv4 格式的管理主机地址 |
| ipv6 | 显示 IPv6 格式的管理主机地址 |

**注意事项：**

无

**示例：**

```
ac>admhost show
IP_Address        Netmask             Comment
192.168.1.1       255.255.255.255     administration host
ac>admhost show all
IP_Address      Netmask              comment
10.1.5.200      255.255.255.255       administration host
10.1.5.49       255.255.255.255       PPP administration host
10.1.6.200      255.255.255.255       administration host
------------------------------------------------------------
IP_Address/prefix_length              comment
2001:288:250:2403::200/128             administration host
2001:288:250:2403::49/128              PPP administration host
```

2001:288:250:2404::200/128 administration host

ac> admhost show ipv4
IP_Address Netmask comment
10.1.5.200 255.255.255.255 administration host
10.1.5.49 255.255.255.255 PPP administration host
10.1.6.200 255.255.255.255 administration host
ac> admhost show ipv6
IP_Address/prefix_length comment
2001:288:250:2403::200/128 administration host
2001:288:250:2403::49/128 PPP administration host
2001:288:250:2404::200/128 administration host

### 4.4.3 管理员帐号（admacct）

#### 添加管理员帐号：

**语法：**
admacct add name <name> password <password> vmfwid <id> powername <name> max_err_num <num>

**参数说明：**
name 设置管理员的名字(1 至 15 位字母或数字的组合，首位为字母)
vmfwid 设置虚拟防火墙 id（非虚拟防火墙为 0, 默认为 0，）
password 设置管理员的密码(8 至 15 位字母和数字的组合)
powername 设置管理员的权限名称，请使用“account_power show”查看可用的权限
max_err_num 设置管理员的允许最大可输入出错次数(3~10 次)

**注意事项：**
无

**示例：**
ac>admacct add name admin1 password 12345678 vmfwid 0 powername super max_err_num 5

#### 修改管理员帐号：

**语法：**
admacct { set sname <name> dname <name> [ password <password> ] | [ vmfwid <id> ] | [ powername] <name> ] | [ max_err_num <num> ] }

**参数说明：**
sname 指定欲修改前的管理员的名字

vmfwid 设置虚拟防火墙 id（非虚拟防火墙为 0, 默认为 0）
dname 指定欲修改后的管理员的名字
password 修改管理员的密码
powername 修改管理员的权限名称，请使用“account_power show”查看可用的权限
max_err_num 修改设置管理员的允许最大可输入出错次数

**注意事项：**
无

**示例：**
ac>admacct set sname admin1 dname admin2 password 12345678 powername super max_err_num 10

## 删除管理员帐号：

**语法：**
admacct del name <name> [vmfwid <id>]

**参数说明：**
name 指定欲删除的管理员的名字
vmfwid 设置虚拟防火墙 id（非虚拟防火墙为 0, 默认为 0）

**注意事项：**
不能删除超级管理员帐号 administrator

**示例：**
ac>admacct del name admin1

## 重置 ADMINISTRATOR 帐号：

**语法：**
admacct reset name administrator

**参数说明：**
无

**示例：**
ac>admacct reset name administrator

## 启用多管理员同时管理功能：

**语法：**

admacct set multiadm on

**参数说明：**
无

**注意事项：**
无

**示例：**
```
ac>admacct set multiadm on
```

## 禁用多管理员同时管理功能：

**语法：**
admacct set multiadm off

**参数说明：**
无

**注意事项：**
无

**示例：**
```
ac>admacct set multiadm off
```

## 显示管理员账号：

**语法：**
admacct show

**参数说明：**
无

**注意事项：**
无

**示例：**
```
ac>admacct  show
Name                    Powername       vmfwid  Max_err_num     Now_err_num
administrator           super           0               3               0
```

### 超时设置(帐号解锁超时)：

**语法：**

admacct set unlock_style timeout <minute>

**参数说明：**

| | |
|---|---|
| unlock_style | 帐号解锁超时方式 |
| timeout | 设置成超时解锁方式的超时时间 |

**注意事项：**

无

**示例：**

admacct set unlock_style timeout 5

## 4.4.4 管理员证书（admcert）

### 添加认证中心证书和安全网关证书：

**语法：**

admcert add cacert <filename> fwcert <filename> fwkey <filename>

**参数说明：**

| | |
|---|---|
| cacert | 设置认证中心证书文件名 |
| fwcert | 设置安全网关证书文件名 |
| fwkey | 设置安全网关密钥文件名 |

**注意事项：**

操作前要先把证书放到安全网关上，参考 rz 命令
仅支持 PEM 格式的证书文件；
会覆盖原有的认证中心证书和安全网关证书；
会自动删除不再匹配的管理员证书；
会重新启动 Web 服务器，当前的 Web 连接会被中断。

**示例：**

```
ac>admcert add cacert cacert.pem fwcert fwcert.pem fwkey fwkey.pem
```

### 添加管理员证书：

**语法：**
admcert add admincert <filename>

**参数说明：**
admincert 设置管理员证书文件名

**注意事项：**
操作前要先把证书放到安全网关上，参考 rz 命令
仅支持 PEM 格式的证书文件。

**示例：**
```
ac>admcert add admincert admin1.pem
```

## 删除管理员证书：

**语法：**
admcert del admincert <filename>

**参数说明：**
admincert 指定欲删除的管理员证书文件名

**注意事项：**
不能删除已经启用的管理员证书。

**示例：**
```
ac>admcert del admincert admin1.pem
```

## 启用管理员证书：

**语法：**
admcert on admincert <filename>

**参数说明：**
admincert 指定欲启用的管理员证书文件名

**注意事项：**
无

**示例：**
```
ac>admcert on admincert admin1.pem
```

## 禁用管理员证书：

**语法：**
admcert off admincert <filename>

**参数说明：**
admincert 指定欲禁用的管理员证书文件名

**注意事项：**
无

**示例：**
ac>admcert off admincert admin1.pem

## 显示认证中心证书：

**语法：**
admcert show cacert

**参数说明：**
无

**注意事项：**
无

**示例：**
ac>admcert show cacert
Name: cacert.pem
Description:subject=/Email=infosec@legend.com/CN=infosec/OU=infosec/O=legend/C=CN

## 显示安全网关证书：

**语法：**
admcert show fwcert

**参数说明：**
无

**注意事项：**
无

**示例：**

```
ac>admcert show fwcert
Name: fwcert.pem
Description:subject=/Email=infosec@legend.com/CN=infosec/OU=infosec/O=legend/C=CN
```

## 显示管理员证书：

**语法：**

admcert show admincert

**参数说明：**

无

**注意事项：**

无

**示例：**

```
ac>admcert show admincert
Name: admin1.pem
Status: on
Description:subject=/C=CN/O=legend/OU=infosec/CN=admin1/Email=infosec@legend.com

Name: admin2.pem
Status: off
Description:subject=/C=CN/O=legend/OU=infosec/CN=admin2/Email=infosec@legend.com
```

# 4.4.5 管理方式（admmode）

## 启用 SSH 管理方式：

**语法：**

admmode on ssh

**参数说明：**

无

**注意事项：**

无

**示例：**

```
ac>admmode on ssh
```

## 禁用 SSH 管理方式：

**语法：**

admmode off ssh

**参数说明：**

无

**注意事项：**

如果此时 PPP 方式已经打开，则也会随之关闭。

**示例：**

```
ac>admmode off ssh
```

## 启用 PPP 管理方式：

**语法：**

admmode on ppp

**参数说明：**

无

**注意事项：**

当启动 PPP 管理方式时，会同时自动打开 SSH 管理方式，并且串口登录由 COM1 变为 COM2。

**示例：**

```
ac>admmode on ppp
```

## 禁用 PPP 管理方式：

**语法：**

admmode off ppp

**参数说明：**

无

**注意事项：**

无

**示例：**

```
ac>admmode off ppp
```

## 启用 TELNET 管理方式：

**语法：**

admmode on telnet

**参数说明：**

无

**示例：**

```
ac>admmode on telnet
```

## 禁用 TELNET 管理方式：

**语法：**

admmode off telnet

**参数说明：**

无

**注意事项：**

无

**示例：**

```
ac>admmode off telnet
```

## 显示管理方式：

**语法：**

admmode show

**参数说明：**

无

**注意事项：**

无

**示例：**

```
ac>admmode show
```

# 4.5 协同联动

## 4.5.1 联动（IDS linkage）

### 设置 PUMA 联动：

**语法：**
linkage set puma ip <ip>+ port <port>

**参数说明：**

| | |
|---|---|
| ip | 设置 PUMA IDS 的 IP 地址 |
| port | 设置 PUMA IDS 的联动端口（TCP） |

**注意事项：**
如果 PUMA 联动已经启动，请先停止 PUMA 联动，再进行设置，然后再启动 PUMA 联动。

**示例：**
```
ac>linkage set puma ip 192.168.100.1 192.168.100.2 port 5000
```

### 导入 PUMA 联动证书：

**语法：**
linkage set puma cert <filename> password <password>

**参数说明：**

| | |
|---|---|
| cert | 设置 PUMA 联动证书文件名 |
| password | 设置 PUMA 联动证书的管理员口令，必须为 9 个字符 |

**注意事项：**
如果 PUMA 联动已经启动，请先停止 PUMA 联动，再导入 PUMA 联动证书，然后再启动 PUMA 联动。参考 rz 命令上传文件。

**示例：**
```
ac>linkage set puma cert puma_ids.dat password 123456789
```

### 启动 PUMA 联动：

**语法：**
linkage on puma

**参数说明：**
无

**注意事项：**
无

**示例：**
ac>linkage on puma

## 停止 PUMA 联动：

**语法：**
linkage off puma

**参数说明：**
无

**注意事项：**
无

**示例：**
ac>linkage off puma

## 设置“天阗”联动：

**语法：**
linkage set venus ip <ip>+ port <port>

**参数说明：**

| | |
|---|---|
| ip | 设置“天阗”IDS 的 IP 地址 |
| port | 设置“天阗”IDS 的联动端口（UDP） |

**注意事项：**
如果“天阗”联动已经启动，请先停止“天阗”联动，再进行设置，然后再启动“天阗”联动。
参考 rz 命令上传文件。
**示例：**
ac>linkage set venus ip 192.168.100.1 192.168.100.2 port 2000

## 启动“天阗”联动：

**语法：**
linkage on venus

**参数说明：**
无

**注意事项：**
无

**示例：**
```
ac>linkage on venus
```

## 停止“天阗”联动：

**语法：**
linkage off venus

**参数说明：**
无

**注意事项：**
无

**示例：**
```
ac>linkage off venus
```

## 设置“天眼”联动：

**语法：**
linkage set netpower ip <ip>+ port <port>

**参数说明：**

| | |
|---|---|
| ip | 设置“天眼”IDS 的 IP 地址 |
| port | 设置“天眼”IDS 的联动端口（TCP） |

**注意事项：**
如果“天眼”联动已经启动，请先停止“天眼”联动，再进行设置，然后再启动“天眼”联动。

**示例：**

```
ac>linkage set netpower ip 192.168.100.1 192.168.100.2 port 4000
```

## 导入“天眼”联动证书：

**语法：**

linkage set netpower cacert <filename> consolecert <filename> consolekey <filename>

**参数说明：**

| | |
|---|---|
| cacert | 设置 CA 证书文件名 |
| consolecert | 设置控制台证书文件名 |
| consolekey | 设置控制台密钥文件名 |

**注意事项：**

如果“天眼”联动已经启动，请先停止“天眼”联动，再导入“天眼”联动证书，然后再启动“天眼”联动。

参考 rz 命令上传文件。

**示例：**

```
ac>linkage set netpower cacert cacert.pem consolecert con_cert.pem consolekey con_key.pem
```

## 启动“天眼”联动：

**语法：**

linkage on netpower

**参数说明：**

无

**注意事项：**

无

**示例：**

```
ac>linkage on netpower
```

## 停止“天眼”联动：

**语法：**

linkage off netpower

**参数说明：**

无

**注意事项：**

无

**示例：**

```
ac>linkage off netpower
```

## 设置 SafeMate 联动：

**语法：**

linkage set safemate port <port>

**参数说明：**

port 设置 SafeMate IDS 的联动端口（UDP）

**注意事项：**

如果 SafeMate 联动已经启动，请先停止 SafeMate 联动，再设置 SafeMate 联动，然后再启动 SafeMate 联动。

**示例：**

```
ac>linkage set safemate port 2001
```

## 导入 SafeMate 联动密钥文件：

**语法：**

linkage set safemate keyfile <filename>

**参数说明：**

keyfile 设置密钥文件名

**注意事项：**

如果 SafeMate 联动已经启动，请先停止 SafeMate 联动，再导入 SafeMate 联动密钥文件，然后再启动 SafeMate 联动。

**示例：**

```
ac>linkage set safemate keyfile safemate_ids.dat
```

## 启动 SafeMate 联动：

**语法：**

linkage on safemate

**参数说明：**
无

**注意事项：**
无

**示例：**
ac>linkage on safemate

## 停止 SafeMate 联动：

**语法：**
linkage off safemate

**参数说明：**
无

**注意事项：**
无

**示例：**
ac>linkage off safemate

## 设置绿盟联动：

**语法：**
linkage set nsfocus ip <ip>+ port <port>

**参数说明：**

| | |
|---|---|
| ip | 设置 NSFOCUS IDS 的 IP 地址 |
| port | 设置 NSFOCUS IDS 的联动端口（TCP） |

**注意事项：**
如果绿盟联动已经启动，请先停止绿盟联动，再进行设置，然后再启动绿盟联动。

**示例：**
ac>linkage set nsfocus ip 192.168.100.1 192.168.100.2 port 5000

## 导入绿盟联动证书：

**语法：**

linkage set nfocus cert <filename> password <password>

**参数说明：**

| | |
|---|---|
| cert | 设置 NSFOCUS 联动证书文件名 |
| password | 设置 NSFOCUS 联动证书的管理员口令，必须为 9 个字符 |

**注意事项：**

如果 NSFOCUS 联动已经启动，请先停止 NSFOCUS 联动，再导入 NSFOCUS 联动证书，然后再启动 NSFOCUS 联动。

参考 rz 命令上传文件。

**示例：**

```
ac>linkage set nsfocus cert nsfocus_ids.dat password 123456789
```

## 启动绿盟联动：

**语法：**

linkage on nsfocus

**参数说明：**

无

**注意事项：**

无

**示例：**

```
ac>linkage on nsfocus
```

## 停止绿盟联动：

**语法：**

linkage off nsfocus

**参数说明：**

无

**注意事项：**

无

**示例：**

```
ac>linkage off nsfocus
```

## 设置忽略联动阻断的 IP 地址：

**语法：**
linkage set ignoreip <ip>

**参数说明：**
ignoreip 设置忽略联动阻断的 IP 地址

**注意事项：**
无

**示例：**
ac>linkage set ignoreip 192.168.1.1 192.168.1.2

## 清除忽略联动阻断的 IP 地址：

**语法：**
linkage set ignoreip

**参数说明：**
无

**注意事项：**
无

**示例：**
ac>linkage set ignoreip

## 清除联动阻断的 IP 地址：

**语法：**
linkage clean blockip

**参数说明：**
无

**注意事项：**
无

**示例：**
ac>linkage clean blockip

## 显示联动设置：

**语法：**
linkage show

**参数说明：**
无

**注意事项：**
请不要将联动的端口设置为同一个，如果每个联动的端口都相同，则实际启用的联动系统，为用户最后一个启用的联动系统。

**示例：**
```
ac>linkage show
PUMA: on
PUMA IP: 192.168.100.1
PUMA Port: 5000
PUMA Password: 123456789
Venus: on
Venus IP: 192.168.100.2
Venus Port: 2000
Netpower: on
Netpower IP: 192.168.100.3
Netpower Port: 4000
SafeMate: on
SafeMate IP: 192.168.100.4
SafeMate Port: 2001
Ignored IP: 192.168.1.1, 192.168.1.2
```

# 4.5.2 联动（ISM linkage）

## 设置 ISM 联动：

**语法：**
linkage set ism ip <ip>+ port <port>

**参数说明：**
ip 设置 ISM 的 IP 地址

port 设置 ISM 的联动端口（TCP）

**注意事项：**
如果 ISM 联动已经启动，请先停止 ISM 联动，再进行设置，然后再启动 ISM 联动。

**示例：**
```
ac>linkage set ism ip 192.168.100.1 192.168.100.2 port 5000
```

## 导入 ISM 联动证书：

**语法：**
linkage set ism cert <filename> password <password>

**参数说明：**
cert 设置 ISM 联动证书文件名
password 设置 ISM 联动证书的管理员口令，必须为 9 个字符

**注意事项：**
如果 ISM 联动已经启动，请先停止 ISM 联动，再导入 ISM 联动证书，然后再启动 ISM 联动。
参考 rz 命令上传文件。
**示例：**
```
ac>linkage set ism cert ism_ids.dat password 123456789
```

## 启动 ISM 联动：

**语法：**
linkage on ism

**参数说明：**
无

**注意事项：**
ISM 联动不可以和 IDS 联动同时开启，只能开启其中一个。

**示例：**
```
ac>linkage on ism
```

## 停止 ISM 联动：

**语法：**
linkage off ism

**参数说明：**
无

**注意事项：**
无

**示例：**
ac>linkage off ism

## 启用网页重定向：

**语法：**
linkage on redirect redirectip <ip> localport <localport>
**参数说明：**

| | |
|---|---|
| ip | 设置 ISM 客户端下载服务器的 ip 地址 |
| localport | 设置和 ISM 客户端下载服务器相连的防火墙接口 |

**注意事项：**
无

**示例：**
ac>linkage on redirect redirectip 2.2.2.2 localport eth0

## 关闭网页重定向：

**语法：**
linkage off redirect

**参数说明：**
无

**注意事项：**
无

**示例：**
ac>linkage off redirect

## 清除白名单：

**语法：**
permit clean

**参数说明：**
无

**注意事项：**

无

**示例：**

```
ac>permit clean
```

# 4.6 虚拟防火墙配置

## 4.6.1 添加虚拟防火墙

语法：

vmfw create vmfwname <name>

说明：name 为虚拟防火墙的名称

举例：

vmfw create vmfwname "vmfw1"

## 4.6.2 删除虚拟防火墙

语法：

vmfw delete vmfwname <name>

说明：name 为虚拟防火墙的名称

举例：

vmfw delete vmfwname "vmfw1"

## 4.6.3 添加网络接口

语法：

vmfw add interface name <name1> type <share| exclusive> vmfwname <name2>

说明：

name1 为网口的名称，比如为 eth3。

name2 为虚拟防火墙的名称。

type 为 share 表示多个虚拟墙可以同时包含此接口，为 exclusive 只能被一个虚拟墙包含

举例：

vmfw add interface name eth3 type share vmfwname vmfw1

## 4.6.4 删除网络接口

语法：

vmfw delete interface name <name1> vmfwname <name2>
说明：
name1 为网口的名称，比如为 eth3。
name2 为虚拟防火墙的名称。
举例：
vmfw delete interface name eth3 vmfwname vmfw1

### 4.6.5 添加管理员

语法：
admacct add name <name1> password <pass> manager off policyer off auditor off vmfwid <id>
说明：
name1 管理员名称
pass 为管理员密码
id 为虚拟防火墙的 id 号
举例：
admacct add name "vmadmin" password "vmadmin123" manager off policyer off auditor off vmfwid 1000

### 4.6.6 删除管理员

同删除非虚拟防火墙管理员完全一致，不再描述。请参见相关章节。

# 4.24688 维护

## 4.24688.1 备份与恢复（newconfig）

### 保存系统配置

**语法：**
newconfig save

**参数说明：**
无

**注意事项：**
无

**示例：**

```
ac>newconfig save
```

## 恢复出厂配置

**语法：**

newconfig reset

**参数说明：**

无

**注意事项：**

所有当前配置都会丢失，需要重新启动安全网关

**示例：**

```
ac>newconfig reset
Please reboot system.
```

## 导出系统配置

**语法：**

newconfig export <filename> [ encrypt { on | off } ]

**参数说明：**

| | |
|---|---|
| <filename> | 指定导出系统配置的文件名 |
| encrypt | 指定是否对导出的系统配置文件进行加密，可选参数，默认为进行加密 |

**注意事项：**

导出的系统配置为上一次保存的系统配置。

必须使用支持 ZMODEM 协议的终端登录，如 Windows 超级终端，SecureCRT 等。

导出的文件自动下载到管理主机，下载文件的存放位置必须事先在终端程序里指定。

**示例：**

```
ac>newconfig export fw.cfg encrypt on
```

## 导出模块配置

**语法：**

newconfig export_modules <module1,module2,...> <filename> { [ encrypt <on|off> ]}

**参数说明：**

<module1,module2,...> 模块名称列表，以逗号分开
<filename> 指定导出系统配置的文件名
encrypt 指定是否对导出的系统配置文件进行加密，可选参数，默认为进行加密

**注意事项：**
导出的系统配置为上一次保存的系统配置。
必须使用支持 ZMODEM 协议的终端登录，如 Windows 超级终端，SecureCRT 等。
导出的文件自动下载到管理主机，下载文件的存放位置必须事先在终端程序里指定。

**示例：**
```
ac>newconfig export_modules rule rule.cfg encrypt on
```

## 导入系统配置

**语法：**
newconfig import <filename>

**参数说明：**
<filename> 指定欲导入的系统配置文件名

**注意事项：**
导入前先要把配置文件上传到安全网关，见 rz 命令。导入后需要重新启动安全网关，新的配置才能生效。注意：导出的配置文件带有安全网关软硬件版本的信息，不能导入到别的版本安全网关中。而且如果同样的配置文件被导入到不同安全网关中，且这些安全网关位于同一网络时，可能会引起配置冲突，如 IP 地址，MAC 地址等。

**示例：**
```
ac>newconfig import fw.cfg
Please reboot system.
```

## 导入模块配置

**语法：**
newconfig import_modules <module1,module2,...> <filename>

**参数说明：**
<module1,module2,...> 模块名称列表，以逗号分开
<filename> 指定欲导入的系统配置文件名(使用绝对路径)

**注意事项：**
导入前先要把配置文件上传到安全网关，见 rz 命令。导入后需要重新启动安全网关，新的配置才能生效。注意：导出的配置文件带有安全网关软硬件版本的信息，不能导入到别的版本安全网关中。而且如果同样的

配置文件被导入到不同安全网关中，且这些安全网关位于同一网络时，可能会引起配置冲突，如 IP 地址，MAC 地址等。

**示例：**

```
ac>newconfig import rule /tmp/upload/rule.cfg
Please reboot system.
```

## 4.24688.2 系统升级（upgrade）

### 升级安全网关

**语法：**

upgrade package <filename>

### 显示升级历史记录

**语法：**

upgrade show

### 立即升级

**语法：**

**upgrade** autoupNow ip <ip> port <port>

**示例：**

**upgrade** autoupNow ip 10.1.5.20 port 80

### 停止自动升级

**语法：**

**upgrade** autoup off

### 实时自动升级

**语法：**

**upgrade** autoup type real ip <ip> port <port>

**示例：**

**upgrade** autoup type real ip 10.1.5.20 port 80

### 定点自动升级

**语法：**

upgrade autoup type time ip <ip> port <port> hour <hour>  每隔<hour>小时自动升级一次

upgrade autoup type time ip <ip> port <port> day <day> 每天<day>点自动升级一次

upgrade autoup type time ip <ip> port <port>week <week> whour <whour> 每个星期<week>的<whour>点自动升级一次

**示例（与上命令对应）：**

upgrade autoup type time ip 10.1.5.20 port 80 hour 3

upgrade autoup type time ip 10.1.5.20 port 80 day 3

upgrade autoup type time ip 10.1.5.20 port 80 week 3 whour 3

## rz（上传文件）

**语法：**

rz

**参数说明：**

无

**注意事项：**

该命令只能通过终端登录执行，而且使用的终端必须支持 Zmodem 协议（如 SecureCRT，Windows 超级终端等）。

**示例：**

ac>rz

执行后终端程序会打开一个打开文件对话框，选择要上传的文件后确定，所选的文件就会传到安全网关上。

## sz（发送文件）

语法:

sz <filename>

说明：

这个程序可以从防火墙上把某个文件传送到 Web 管理主机的终端软件的默认接收路径下。

**注意事项：**

该命令只能通过终端登录执行，而且使用的终端必须支持 Zmodem 协议（如 SecureCRT，Windows 超级终端等）。

**示例：**

ac>sz /usr/local/cert/greenupdate/greenupdate.p12

执行后文件放在终端程序默认的接收文件路径下。这个命令的实际含义是把升级证书传送到管理主机的默认接收路径下。

# 4.24688.3 模块许可(license)

## 导入许可证

**语法：**

license upload <filename>

**参数说明：**

<filename> 许可证文件名称

## 查看许可证状态

**语法：**

license show [ module { AdvRoute | VMFW | PolicyAgent | ACSC | HA | VPN | SSLVPN | AV | AVUpdate | IPS | IPSUpdate | PC | APC | APCUpdate | URL | URLUpdate | URLTrojan | URLTrojanUpdate | Scanner | ScannerUpdate | UMA } ]

| 英文名称 | 中文名称 |
|---|---|
| AdvRoute | 动态路由 |
| VMFW | 虚拟网关 |
| PolicyAgent | 策略代理 |
| ACSC | 会话管理 |
| HA | 高可用性(HA) |
| VPN | 虚拟专用网(VPN) |
| SSLVPN | 安全套接层虚拟专用网(SSL VPN) |
| AV | 防病毒 |
| AVUpdate | 防病毒特征升级 |
| IPS | 入侵保护系统(IPS) |
| IPSUpdate | 入侵保护系统(IPS)特征升级 |
| PC | 协议控制 |
| APC | 应用协议识别 |
| APCUpdate | 应用协议识别特征升级 |
| URL | 统一资源定位符(URL) |
| URLUpdate | 统一资源定位符(URL)特征升级 |
| URLTrojan | 主动防御 |
| URLTrojanUpdate | 主动防御特征升级 |
| Scanner | 漏洞扫描 |
| ScannserUpdate | 漏洞扫描特征升级 |
| UMA | 统一认证 |

**参数说明：**

**注意事项：**

无

**示例：**

ac> license show

## 启用、试用模块

**语法：**

license set module { AdvRoute | VMFW | PolicyAgent | ACSC | HA | VPN | SSLVPN | AV | AVUpdate | IPS | IPSUpdate | PC | APC | APCUpdate | URL | URLUpdate | URLTrojan | URLTrojanUpdate | Scanner | ScannerUpdate | UMA } active { on | try }

# 4.24688.4 双系统(vsp)

## 设置默认系统

语法：

vsp set default_os <systemA | systemB>

举例：

vsp set default_os systemA

## 获取系统的版本号

语法：
vsp get {systemA | systemB | backup_os | default_os | current_os}
说明：systemA systemB 表示我们已经定义的双系统的版本号，backup_os 表示备份系统，default_os 表示缺省的系统，current_os 表示当前系统。
举例：
vsp get default_os

## 显示系统当前配置

语法：
vsp show
说明：
它把系统 A、系统 B、备份系统、缺省系统、当前系统的标签及版本号显示出来。
举例：
vsp show

## 备份当前系统

语法：
vsp backup system
说明：
它把当前系统进行备份，备份后原来的备份将消失。
举例：
vsp backup system

## 恢复系统

语法：

vsp recover <systemA | systemB>
说明：
它从备份系统中恢复系统，可以恢复到 systemA，也可以恢复到 systemB。
举例：
vsp recover systemA

# 4.24688.5 批处理

## export_pf(导出安全规则配置命令)

## 导出安全规则配置命令：

**语法：**

export_pf export <filename>

**参数说明：**

export 用户指定的导出安全规则文件的名字（文本文件）

**注意事项：**

无

**示例：**

ac> export_pf export rule.txt

## export_addr_service(导出资源定义配置命令)

## 导出安全规则配置命令：

**语法：**

export_addr_service export <filename>

**参数说明：**

export 用户指定的导出资源定义文件的名字（文本文件）

**注意事项：**

无

**示例：**

ac> export_addr_service export resource.txt

# 第5章 网络管理

## 5.1 网络接口（interface）

### 添加 VLAN 设备：

**语法：**

interface add vlan bind_if <name> vlan_id <number> [ ip { <single_ip> | none } ] [ netmask { <all_ip> | none } ] [ active { on | off } ] [ mac { <mac> | none } ] [ qos_enable { on | off } ] [ qos_device_bw <number> ] [ admin { on | off } ] [ ping { on | off } ] [ traceroute { on | off } ] [ workmode { route | trans } ] [ ipmac_check { on | off } ] [ ipmac_check_policy { on | off } ] [ antispoof { on | off } ] [ vlan_maxid <number> ]

**参数说明：**

| | |
|---|---|
| bind_if | VLAN 设备的绑定设备，它必须是已启用的，且工作模式是 trunk 模式的物理设备 |
| vlan_id | VLAN 设备的 VLAN ID，范围是 1-4094。 |
| ip | 合法的 IP 地址，路由模式下，IP 地址不能为空 |
| netmask | 合法的掩码，路由模式下，掩码不能为空 |
| active | on：启用设备，off：停用设备 |
| mac | 合法的 MAC 地址，none 将 MAC 清空 |
| qos_enable | on：启用设备带宽管理，off：停用设备的带宽管理 |
| qos_device_bw | 设备的带宽。VLAN 设备的设备带宽与它的绑定设备有关，如果绑定设备是十兆设备，带宽范围是 1-10000；如果绑定设备是百兆设备，带宽范围是 1-100000；如果绑定设备是千兆设备，带宽范围是 1-1000000；如果绑定设备是万兆设备，带宽范围是 1-10000000。 |
| admin | on：设备 IP 可用于管理，off：设备 IP 不可用于管理 |
| ping | on：设备 IP 允许 ping，off：设备 IP 不允许 ping |
| traceroute | on：设备 IP 允许 traceroute，off：设备 IP 不允许 traceroute |
| workmode | route：路由模式，trans：透明模式 |
| ipmac_check | on：启用 IPMAC 绑定检查，off：去掉 IPMAC 绑定检查 |
| ipmac_check_policy | on：允许未绑定的地址通过，off：禁止未绑定的地址通过 |
| antispoof | on：启用 IP 地址欺骗检查，off：关闭 IP 地址欺骗检查 |
| vlan_maxid | 如果 vlan_maxid>0,则表示为区间 vlan 设备，区间范围是[vlan_id,vlan_maxid],如果 vlan_maxid 为-1 。则表示为单号 vlan 设备，设备 id 为 vlan_id。 |

**注意事项：**

1.在命令行上，如果需要将 IP 地址或掩码置为空，可以在关键字 ip 或 netmask 后输入 none，它们在命令行或 Web 界面上列表时都显示为空。
2.设置透明模式，IP 地址和掩码会自动置为空。
3.启用的 vlan 设备要求绑定设备必须是启用的工作在 trunk 模式下的物理设备
4.未启用的 vlan 设备只要求绑定设备必须是物理设备

**示例：**

```
ac> interface add vlan bind_if eth0 vlan_id 1 ip 192.168.0.1 netmask 255.255.255.0 active on
```

## 添加桥接设备

**语法：**

interface add brg if <name> [ ip { <single_ip> | none } ] [ netmask { <all_ip> | none } ] [ active { on | off } ] [ interface_list { none | <string> } ] [ stp { on | off } ] [ admin { on | off } ] [ ping { on | off } ] [ traceroute { on | off } ] [ ipmac_check { on | off } ] [ ipmac_check_policy { on | off } ] [ antispoof { on | off } ]

**参数说明：**

| | |
|---|---|
| if | 桥接设备的名称可以填写名称有：brg1,brg2,brg3,brg4,brg5,brg6,brg7，其他名称都不允许出现 |
| ip | 合法的 IP 地址，如果设备的 IP 为空则不允许用于管理，不允许 PING，不允许 TRACEROUTE |
| netmask | 合法的掩码，如果掩码是空则不允许用于管理，不允许 PING，不允许 TRACEROUTE |
| active | on：启用设备，off：停用设备 |
| interface_list | 网桥设备绑定设备列表，它是一个以逗号分割的设备列表，none 用于清空绑定设备列表 |
| stp | on：启用 STP（生成树协议），off：关闭 STP |
| admin | on：允许设备 IP 用于管理，off：禁止设备 IP 用于管理 |
| ping | on：设备 IP 允许 ping，off：设备 IP 禁止 ping |
| traceroute | on：设备 IP 允许 traceroute，off：设备 IP 禁止 traceroute |
| ipmac_check | on：启用 IPMAC 绑定检查，off：去掉 IPMAC 绑定检查 |
| ipmac_check_policy | on：允许未绑定的地址通过，off：禁止未绑定的地址通过 |
| antispoof | on：启用 IP 地址欺骗检查，off：关闭 IP 地址欺骗检查 |

**注意事项：**

1.设备列表用逗号分隔，不允许有空格，下同。
2.在命令行上，如果需要将 IP 地址或掩码置为空，可以在关键字 ip 或 netmask 后输入 none
3.开启的桥接设备的绑定列表中的设备必须是开启的工作在透明模式下的物理、冗余或 vlan 设备
4 不开启的桥接设备只要求绑定列表中的设备必须是物理、冗余或 vlan 设备

**示例：**

**ac> interface add brg if brg1 ip 192.168.0.1 netmask 255.255.255.0 active on**

## 添加冗余设备

**语法：**

interface add rd if <name> [ ip { <single_ip> | none } ] [ netmask { <all_ip> | none } ] [ active { on | off } ] [ interface_list { none | <string> } ] [ workmode { route | trans } ] [ ipaddr_type { static | dhcp } ] [ dns_enable { on | off } ] [ domain_name { none | <string> } ] [ dhcp_relay { on | off } ] [ dhcpserver { none | <string> } ] [ admin { on | off } ] [ ping { on | off } ] [ traceroute { on | off } ] [ ipmac_check { on | off } ] [ ipmac_check_policy { on | off } ]

[ antispoof { on | off } ]

**参数说明：**

| | |
|---|---|
| if | 冗余设备的名称，可填写的设备名称有 bond1、bond2、bond3、bond4 |
| ip | 合法的 IP 地址，none 表示清空 ip 地址 |
| netmask | 合法的掩码，none 表示清空掩码 |
| active | on：启用设备，off：停用设备 |
| workmode | route：路由模式，trans：透明模式 |
| interface_list | 冗余设备的绑定设备列表，是以逗号分割的设备名称列表 |
| ipaddr_type | static：静态指定，dhcp：通过 DHCP 获取 |
| dns_enable | on：开启动态域名注册，off：停止动态域名注册 |
| domain_name | 动态域名注册的域名，只能是单个域名。 |
| dhcp_relay | on：允许设备做 DHCP 中继，off：禁止设备做 DHCP 中继 |
| dhcpserver | 这是一个 IP 地址的列表，none 表示清空 DHCP 中继服务器列表 |
| admin | on：允许设备 IP 用于管理，off：禁止设备 IP 用于管理 |
| ping | on：设备 IP 允许 PING，off：设备 IP 禁止 PING |
| traceroute | on：设备 IP 允许 TRACEROUTE，off：设备 IP 禁止 TRACEROUTE |
| ipmac_check | on：启用 IPMAC 绑定检查，off：去掉 IPMAC 绑定检查 |
| ipmac_check_policy | on：允许未绑定的地址通过，off：禁止未绑定的地址通过 |
| antispoof | on：启用 IP 地址欺骗检查，off：关闭 IP 地址欺骗检查 |

**注意事项：**

1 开启的冗余设备的绑定列表中的设备必须是开启的工作在冗余模式下的物理设备，且列表不能为空
2 不开启的桥接设备只要求绑定列表中的设备必须是物理设备

**示例：**

ac> interface add rd if bond1 interface_list eth0,eth1 ip 10.1.1.1 netmask 255.255.255.0 ping on admin on active on

## 添加别名设备

**语法：**

interface add alias bind_if <name> alias_id <number> ip <single_ip> netmask <all_ip> [ active { on | off } ] [ admin { on | off } ] [ ping { on | off } ] [ traceroute { on | off } ] [ vrid <id> ]

**参数说明：**

| | |
|---|---|
| bind_if | 别名设备绑定设备的名称。 |
| alias_id | 别名 ID，范围是 0－399 |
| ip | 合法的 IP 地址，不能为空、0 或 none |
| netmask | 合法的掩码，不能是空和 0 或 none |
| active | on：启用设备，off：停用设备 |
| admin | on：允许设备 IP 用于管理，off：禁止设备 IP 用于管理 |
| ping | on：设备 IP 允许 ping，off：设备 IP 禁止 ping |
| traceroute | on：设备 IP 允许 traceroute，off：设备 IP 禁止 traceroute |

vrid VRRP 的组 ID 号。1-255，请参见 5.8.3 节。

**注意事项：**

1 开启的别名设备的绑定列表中的设备必须是开启的工作在路由模式下的设备
2 不开启的桥接设备只要求绑定列表中的设备必须是物理、冗余、vlan 或桥接设备

**示例：**

**ac> interface add alias bind_if eth0 alias_id 0 ip 192.168.0.1 netmask 255.255.255.0 active on**

## 添加拨号设备

**语法：**

interface add dial if <name>

**参数说明：**

if 拨号设备的名称

**注意事项：**

添加拨号设备仅仅是添加一条记录，如果想启用或配置此路拨号，请使用拨号设备的配置命令。

**示例：**

**ac> interface add dial if dial1**

## 修改物理设备：

**语法：**

interface set phy if <name> [ ip { <single_ip> | none } ] [ netmask { <all_ip> | none } ] [ active { on | off } ] [ mac { <mac> | none } ] [ linkmode { auto | full | half } ] [ speed { 10 | 100 | 1000 |10000 } ] [ workmode { route | trans | rd } ] [ mtu <number> ] [ ipaddr_type { static | dhcp } ] [ dns_enable { on | off } ] [ domain_name { none | <string> } ] [ qos_enable { on | off } ] [ qos_device_bw <number> ] [ dhcp_relay { on | off } ] [ dhcpserver { none | <string> } ] [ admin { on | off } ] [ ping { on | off } ] [ traceroute { on | off } ] [ ipmac_check { on | off } ] [ ipmac_check_policy { on | off } ] [ antispoof { on | off } ] [ bind_vlanrange { <string> | none } ] [ native_vlanid { <number> | none } ] [ vlan_encap { nego | dot1q | iskl } ]

**参数说明：**

if 物理设备的名称，例如 eth0、eth1 等
ip 合法的 IP 地址，none 表示清空 ip 地址
netmask 合法的掩码，none 表示清空掩码
active on：启用设备，off：停用设备
mac 合法的 MAC 地址，none 用于清空 MAC 地址
linkmode auto：自适应，full：全双工，half：半双工
speed 链路速度，可填写的有 10,100,1000，10000
workmode route：路由模式，trans：透明模式，rd：冗余模式；trunk：trunk 模式。默认是路由
mtu 设备的 mtu。百兆设备的 MTU 范围是 60-1500，千兆设备的 MTU 范围是 68-9216。
ipaddr_type static：静态指定，dhcp：通过 DHCP 获取
dns_enable on：开启动态域名注册，off：停止动态域名注册

domain_name 动态域名注册的域名，只能是单个域名，none 表示清空动态域名。

qos_enable on：开启设备带宽管理，off：停止设备带宽管理

qos_device_bw 设备带宽，如果是十兆设备，带宽范围是 1-10000；如果是百兆设备，带宽范围是 1-100000；如果是千兆设备，带宽范围是 1-1000000；如果是万兆设备，带宽范围是 1-10000000。

dhcp_relay on：允许设备做 DHCP 中继，off：禁止设备做 DHCP 中继

dhcpserver 这是一个 IP 地址的列表，none 表示清空 dhcp 中继服务器列表

admin on：允许设备 IP 用于管理，off：禁止设备 IP 用于管理

ping on：设备 IP 允许 PING，off：设备 IP 禁止 PING

traceroute on：设备 IP 允许 TRACEROUTE，off：设备 IP 禁止 TRACEROUTE

ipmac_check on：启用 IPMAC 绑定检查，off：去掉 IPMAC 绑定检查

ipmac_check_policy on：允许未绑定的地址通过，off：禁止未绑定的地址通过

antispoof on：启用 IP 地址欺骗检查，off：关闭 IP 地址欺骗检查

bind_vlanrange string:VLAN 区间字符串，如“2-4094”；none 表示不绑定 VLAN 区间设备，此选项在 trunk 工作模式下有效。

native_vlanid Native VLAN ID，范围 1-4094。此选项在 trunk 工作模式下有效。

vlan_encap 表示 VLAN 的封装模式；nego 表示自动协商；dot1q 表示 802.1Q 封装；isl 表示 CISCO 的 ISL 封装。此选项在 trunk 工作模式下有效。

**注意事项：**

1.none 用来清空对应的关键字值

**示例：**

```
ac> interface set phy if eth0 ip 192.168.0.1 netmask 255.255.255.0 ping on active on
```

# 修改 VLAN 设备

**语法：**

interface set vlan if <name> [ ip { <single_ip> | none } ] [ netmask { <all_ip> | none } ] [ active { on | off } ] [ mac { <mac> | none } ] [ qos_enable { on | off } ] [ qos_device_bw <number> ] [ admin { on | off } ] [ ping { on | off } ] [ traceroute { on | off } ] [ workmode { route | trans } ] [ ipmac_check { on | off } ] [ ipmac_check_policy { on | off } ] [ antispoof { on | off } ]

**参数说明：**

if VLAN 设备的设备名称

ip 合法的 IP 地址，none 表示清空 ip 地址

netmask 合法的掩码，none 表示清空掩码

active on：启用设备，off：停用设备

mac 合法的 MAC 地址，none 将 MAC 地址清空

qos_enable on：启用设备的带宽管理，off：停用设备的带宽管理

qos_device_bw 设置设备带宽。VLAN 设备的设备带宽与它的绑定设备有关，如果绑定设备是十兆设备，带宽范围是 1-10000；如果绑定设备是百兆设备，带宽范围是 1-100000；如果绑定设备是千兆设备，带宽范围是 1-1000000；如果绑定设备是万兆设备，带宽范围是 1-10000000。

admin on：设备 IP 允许用于管理，off：设备 IP 不允许用于管理
ping on：设备 IP 允许 PING，off：设备 IP 不允许 PING
traceroute on：设备 IP 允许 TRACEROUTE，off：设备 IP 不允许 TRACEROUTE
workmode route：路由模式，trans：透明模式
ipmac_check on：启用 IPMAC 绑定检查，off：去掉 IPMAC 绑定检查
ipmac_check_policy on：允许未绑定的地址通过，off：禁止未绑定的地址通过
antispoof on：启用 IP 地址欺骗检查，off：关闭 IP 地址欺骗检查

**注意事项：**

1.vlan 区间设备不支持路由模式，只能配置为透明模式

**示例：**

**ac> interface set vlan if eth0.0 ip 192.168.0.1 netmask 255.225.255.0 active off**

# 修改桥接设备

**语法：**

interface set brg if <name> [ ip { <single_ip> | none } ] [ netmask { <all_ip> | none } ] [ active { on | off } ] [ interface_list { none | <string> } ] [ stp { on | off } ] [ admin { on | off } ] [ ping { on | off } ] [ traceroute { on | off } ] [ ipmac_check { on | off } ] [ ipmac_check_policy { on | off } ] [ antispoof { on | off } ]

**参数说明：**

if 桥接设备的设备名称
ip 合法的 IP 地址，none 表示清空 ip 地址
netmask 合法的掩码，none 表示清空掩码
active on：启用设备，off：停用设备
interface_list 桥接设备的绑定设备列表
stp on：开启 STP，off：停止 STP
admin on：设备 IP 允许用于管理，off：设备 IP 不允许用于管理
ping on：设备 IP 允许 PING，off：设备 IP 不允许 PING
traceroute on：设备 IP 允许 TRACEROUTE，off：设备 IP 不允许 TRACEROUTE
ipmac_check on：启用 IPMAC 绑定检查，off：去掉 IPMAC 绑定检查
ipmac_check_policy on：允许未绑定的地址通过，off：禁止未绑定的地址通过
antispoof on：启用 IP 地址欺骗检查，off：关闭 IP 地址欺骗检查

**注意事项：**

无

**示例：**

**ac> interface set brg if brg0 ip 192.168.0.1 netmask 255.255.255.0 active off**

# 修改别名设备

**语法：**

interface set alias if <name> [ ip <single_ip> ] [ netmask <all_ip> ] [ active { on | off } ] [ admin { on | off } ] [ ping { on | off } ] [ traceroute { on | off } ] [ vrid { <id> | none } ]

**参数说明：**

if 别名设备的设备名称
ip 合法的 IP 地址
netmask 合法的掩码
active on：启用设备，off：停用设备
admin on：设备 IP 允许用于管理，off：设备 IP 不允许用于管理
ping on：设备 IP 允许 PING，off：设备 IP 不允许 PING
traceroute on：设备 IP 允许 TRACEROUTE，off：设备 IP 不允许 TRACEROUTE
vrid ： 别名设备的 VRRP 的组 ID。请参加 5.8.3

**注意事项：**

无

**示例：**

**ac> interface set alias if eth0_0 ip 192.168.0.1 netmask 255.255.255.0 active on**

# 修改冗余设备

**语法：**

interface set rd if <name> [ ip { <single_ip> | none } ] [ netmask { <all_ip> | none } ] [ active { on | off } ] [ interface_list { none | <string> } ] [ workmode { route | trans } ] [ ipaddr_type { static | dhcp } ] [ dns_enable { on | off } ] [ domain_name { none | <string> } ] [ dhcp_relay { on | off } ] [ dhcpserver { none | <string> } ] [ admin { on | off } ] [ ping { on | off } ] [ traceroute { on | off } ] [ ipmac_check { on | off } ] [ ipmac_check_policy { on | off } ] [ antispoof { on | off } ]

**参数说明：**

if 冗余设备的名称，只能是 bond1、bond2、bond3、bond4
ip 合法的 IP 地址，none 表示清空 ip
netmask 合法的掩码，none 表示清空掩码
active on：启用设备，off：停用设备
interface_list 冗余设备的绑定列表，设备启用时不能为 none
workmode route：路由模式，trans：透明模式
ipaddr_type static：静态指定，dhcp：通过 DHCP 获取
dns_enable on：开启动态域名注册，off：停止动态域名注册
domain_name 动态域名注册的域名，只能是单个域名，none 表示清空动态域名。
dhcp_relay on：允许设备做 DHCP 中继，off：禁止设备做 DHCP 中继
dhcpserver 这是一个 IP 地址的列表，none 表示清空 dhcp 中继服务器列表
admin on：允许设备 IP 用于管理，off：禁止设备 IP 用于管理
ping on：设备 IP 允许 PING，off：设备 IP 禁止 PING
traceroute on：设备 IP 允许 TRACEROUTE，off：设备 IP 禁止 TRACEROUTE
ipmac_check on：启用 IPMAC 绑定检查，off：去掉 IPMAC 绑定检查
ipmac_check_policy on：允许未绑定的地址通过，off：禁止未绑定的地址通过
antispoof on：启用 IP 地址欺骗检查，off：关闭 IP 地址欺骗检查

**注意事项：**

无

**示例：**

**ac> interface set rd if bond1 interface_list eth0,eth1 ip 100.1.1.1 netmask 255.255.255.0 ping on admin on active on**

## 修改拨号设备

**语法：**

interface { set dial if <name> [ active {on|off} ] [ bind_if <name> ] [ username <string> ] [ password <string>] [ startup {on|off} ] [ time <name> ] [ qos_enable {on|off} ] [ qos_device_bw <number> ] [ dns_enable {on|off} ] [ domain_name {string|none} ] [ admin {on|off} ] [ ping {on|off} ] [ traceroute {on|off} ] }

**参数说明：**

| | |
|---|---|
| if | 设备名称 |
| active | on：启用设备，off：停止设备。启用设备时必须设置绑定设备，用户名和密码 |
| bind_if | 拨号设备的绑定设备 |
| username | 拨号用户名，1 至 15 个字符，包括除制表符和问号外的任意可打印字符 |
| password | 拨号密码，1 至 15 个字符，包括除制表符和问号外的任意可打印字符 |
| startup | on：系统启动时拨号；off：系统启动时不拨号 |
| time | time：自动拨号的时间资源，如果没有时间资源，则一直保持连接 |
| qos_enable | on：启用带宽管理；off：停止带宽管理 |
| qos_device_bw | 设备带宽 |
| dns_enable | on：启用动态域名注册；off：停止动态域名注册 |
| domain_name | 动态域名 |
| admin | on：设备 IP 用于管理；off：设备 IP 不能用于管理 |
| ping | on：设备 IP 允许 PING；off：设备 IP 不允许 PING |
| traceroute | on：设备 IP 允许 TRACEROUTE；off：设备 IP 不允许 TRACEROUTE |

**注意事项：**

无

**示例：**

ac>interface set dial if dial0 bind_if eth1 username aaa password bbb active on

## 修改无线设备

**语法：**

interface { set wireless if <name> [ ip <ip> ] [ netmask <netmask> ] [ active {on|off} ] [ admin {on|off} ] [ ping {on|off} ] [ traceroute {on|off} ] }

**参数说明：**

| | |
|---|---|
| if | 设备名称 |
| ip | 合法的 IP 地址 |
| netmask | 合法的掩码 |

active on：启用设备，off：停止设备。
admin on：设备 IP 用于管理；off：设备 IP 不能用于管理
ping on：设备 IP 允许 PING；off：设备 IP 不允许 PING
traceroute on：设备 IP 允许 TRACEROUTE；off：设备 IP 不允许 TRACEROUTE

**注意事项：**

无

**示例：**

ac>interface set wireless if wlan0 ip 192.168.1.1 netmask 255.255.255.0 active on

## 删除网络设备：

**语法：**

interface { del if <name> }

**参数说明：**

name 将要删除的设备名称

**注意事项：**

不能删除被其他设备绑定或被其他模块引用的设备，物理设备、拨号设备、默认桥接设备 brg0 不能被此命令删除

**示例：**

```
ac> interface del if eth0.0
```

## 显示所有设备：

**语法：**

interface show all

**参数说明：**

无

**注意事项：**

只显示当前有效的设备。

**示例：**

```
ac>interface show all
device              ip              netmask          active
eth0                 0.0.0.0         0.0.0.0          on
eth1                 0.0.0.0         0.0.0.0          on
eth2                 0.0.0.0         0.0.0.0          on
brg0                10.50.10.173     255.255.255.0    on
ipsec0                                                off
eth1_0               20.0.0.99       255.255.255.0    on
```

```
eth0.2                  10.50.10.173      255.255.255.0     off
eth1.2                  20.0.0.22         255.255.255.0     off
eth2.2                  30.0.0.22         255.255.255.0     off
rd1                     10.0.0.1          255.255.255.0     on
```

## 显示物理设备

**语法：**

interface show phy

**参数说明：**

无

**注意事项：**

无

**示例：**

**ac> interface show phy**

| device | ip | netmask | workmode | ipaddr_type | trunk | qos_enable | enable |
|---|---|---|---|---|---|---|---|
| eth0 | 0.0.0.0 | 0.0.0.0 | trans | static | off | off | on |
| eth1 | 0.0.0.0 | 0.0.0.0 | trans | static | off | off | on |
| eth2 | 0.0.0.0 | 0.0.0.0 | trans | static | off | off | on |

## 显示 VLAN 设备

**语法：**

interface show vlan

**参数说明：**

无

**注意事项：**

无

**示例：**

**ac> interface show vlan**

| device | ip | netmask | workmode | bind device | vlan id | qos_enable | active |
|---|---|---|---|---|---|---|---|
| eth0.2 | 10.50.10.173 | 255.255.255.0 | route | eth0 | 2 | off | off |
| eth1.2 | 20.0.0.22 | 255.255.255.0 | route | eth1 | 2 | off | off |
| eth2.2 | 30.0.0.22 | 255.255.255.0 | route | eth2 | 2 | off | off |

## 显示桥接设备

**语法：**

interface show brg

**参数说明：**
无

**注意事项：**
无

**示例：**
**ac> interface show brg**

| device | ip | netmask | stp | interface list | enable |
|---|---|---|---|---|---|
| brg0 | 10.50.10.173 | 255.255.255.0 | on | eth2,eth1,eth0 | on |

## 显示别名设备

**语法：**
interface show alias

**参数说明：**
无

**注意事项：**
无

**示例：**
**ac> interface show alias**

| device | ip | netmask | bind device | alias id | enable |
|---|---|---|---|---|---|
| eth1_0 | 20.0.0.99 | 255.255.255.0 | eth1 | 0 | on |

## 显示拨号设备

**语法：**
**interface show dial**

**参数说明：**
无

**注意事项：**
无

**示例：**
ac> interface show dial

| device | ip | netmask | bind device | qos_enable | enable |
|---|---|---|---|---|---|
| dial0 | | | eth2 | off | off |

## 显示无线设备

**语法：**

**interface show wireless**

**参数说明：**

无

**注意事项：**

无

**示例：**

ac> interface show wireless

| device | ip | netmask | admin | ping | traceroute | enable |
|---|---|---|---|---|---|---|
| wlan0 | 192.168.1.1 | 255.255.255.0 | on | on | on | on |

## 显示 trunk 模式下的物理设备

**语法：**

interface show trunk

**参数说明：**

**无**

**注意事项：**

**无**

**示例：**

**ac> interface show trunk**

| Dev name | TRUNK | Native VLAN ID | Encap Type | Nego |
|---|---|---|---|---|
| eth0 | Yes | 1 | ISL | No |

## 显示指定名称的设备：

**语法：**

interface show if <name>

**参数说明：**

name 将显示的设备名称

**注意事项：**

不同设备的显示内容不一样，根据设备类型来确定。

**示例：**

```
ac> interface show if eth0
device              eth0
device type         physical device
mac address         00:90:0B:1E:CF:78
linkmode            auto
speed               1000
mtu                 1500
workmode            trunk
bind vlan range     2-4
native vlan id      1
vlan encapsulation  isl
ipaddr type         static
qos_enable          off
qos_device_bw       0
dns_enable          off
domain name
dhcp_relay          off
dhcp server
ip
netmask
admin               off
ping                off
traceroute          off
ipmac_check         off
ipmac_check_policy  on
antispoof           off
active              on
```

通知：执行成功

# 3g 模块

## 启动 3g 模块：

**语法：**

3g_dail start

**参数说明：**

无

**注意事项：**

无

**示例：**

ac>3g_dail start

## 关闭 3g 模块：

**语法：**

3g_dail stop

**参数说明：**

无

**注意事项：**

无

**示例：**

ac>3g_dail stop

## 显示配置信息：

**语法：**

3g_dail show

**参数说明：**

无

**注意事项：**

无

**示例：**

```
ac>3g_dail show
3g pppd states:

user_name: ppp3g

in_name  : ppp00

ip       : 0.0.0.0
```

## 获取信号强度：

**语法：**

3g_at CSQ

**参数说明：**
无

**注意事项：**
Wu

**示例：**
ac>3g_at CSQ
+CSQ: 31, 99

## 添加配置信息：

**语法：**
**3g_manager add name phone username password**
**参数说明：**
Name 名字
**Phone 拨入号码**
**Username 拨入号码用户名**
**Password 拨入号码密码**
**注意事项：**
一般情况不需要修改

**示例：**
ac>3g_**manager add uninet #777 ctnet@mycdma.cn vnet.mobi**

## 修改配置信息：

**语法：**
**3g_manager edit name phone username password**
**参数说明：**
Name 名字（不能修改）
**Phone 修改拨入号码**
**Username 修改拨入号码用户名**
**Password 修改拨入号码密码**
**注意事项：**
一般情况不需要修改

**示例：**
ac>3g_**manager edit uninet1 #777 ctnet@mycdma.cn vnet.mobi**

## 修改配置信息：

**语法：**

**3g_manager del name**

**参数说明：**

**Name 要删除配置名字**

**注意事项：**

无

**示例：**

ac> 3g_**manager del uninet**

## 设置配置信息为主信息：

**语法：**

3g_manager def name

**参数说明：**

Name 要设置的配置名字

**注意事项：**

无

**示例：**

ac> 3g_manager def uninet

## 显示配置主信息：

## 语法：

3g_manager set

## 参数说明：

**无**

## 注意事项：

无

## 示例：

ac> 3g_manager set
name : china_telecom
phone : #777
username: ctnet@mycdma.cn
password: vnet.mobi

# 5.2 通告别名 IP (aliasip)

## 添加通告 ip 的别名设备

**语法：**

aliasip add aliasid <aliasid> if <name> ip <ip> state <on/off>

**参数说明：**

| | |
|---|---|
| aliasid | 别名设备的名称 |
| if | 真实设备名称 |
| ip | IP 地址 |
| state | 功能开启或关闭 |

**注意事项：**

**示例：**

```
ac>aliasip add aliasid eth0_1 if eth0 ip 2.2.2.2 state on
```

## 更新别名设备的通告 ip

**语法：**

aliasip update aliasid <aliasid> ip <ip> state <on/off>

**参数说明：**

| | |
|---|---|
| aliasid | 别名设备的名称 |
| ip | IP 地址 |
| state | 功能开启或关闭 |

**注意事项：**

**示例：**

```
ac>aliasip update aliasid eth0_1 ip 2.2.2.3 state on
```

## 删除通告 ip 的别名设备

**语法：**

aliasip del aliasid <aliasid>

**参数说明：**

| | |
|---|---|
| aliasid | 别名设备的名称 |

**注意事项：**

**示例：**

```
ac>aliasip del aliasid eth0_1
```

# 5.3 基本配置

## 5.3.1 网络审计(mirrorset)

命令行：
mirrorset { add <name> [ <name>+ ] | set <name> | del { all | <name> [ <name>+ ] } | show | stop | restart }

### 添加被审计的网口：

**语法：**
Mirrorset add <name> [ <name>+]
**参数说明：**
Name 网口名称
**注意事项：**
一次可以添加一个网口，也可以添加多个
**示例：**
**添加一个网口**
Themis> mirrorset add eth0
**添加多个网口**
Themis> mirrorset add eth2 eth3

### 添加审计网口：

**语法：**
Mirrorset set <name>
**参数说明：**
Name 网口名称
**注意事项：**
无
**示例：**
Themis> mirrorset set eth1

### 启动审计功能：

**语法：**
Mirrorset restart
**参数说明：**
无
**注意事项：**
无
**示例：**

```
Themis> mirrorset restart
```

## 显示当前审计设置：

**语法：**

Mirrorset show

**参数说明：**

无

**注意事项：**

无

**示例：**

```
Themis> mirrorset show
```

# 5.3.2 虚拟路由冗余协议(VRRP)

## 增加一个 VRID：

**语法：**

vrrp add vrid <id> prio<number> adv <number> prom {on|off} mcastip <ip> tif <name>

**参数说明：**

| | |
|---|---|
| vrid | 虚拟路由，有效值范围 ID： 1-254 |
| prio | 优先级，有效值范围：1-255 |
| adv | 通告时间 有效值范围：1-3 |
| prom | 强制抢占属性开关，on：开启，off：关闭 |
| mcastip | 通告 IP 地址 |
| tif | 监测的网络接口的外部接口名，多个网络接口之间用英文逗号隔开 |

**名词解释：**

vrid： 虚拟路由的标识号。

**注意事项：**

VRID 不能重复

通告 IP 为可选项，填写值与虚拟 IP 不能相同。

在多个墙之间，同一个 VRID 的墙的通告时间需相同，优先级不能相同。

必须在 vrrp 服务停止的状态下执行此命令。

**示例：**

```
ac>vrrp add 1 prio 100 adv 1 prom on mcastip 2.3.2.3 tif eth2,eth3
```

## 编辑一个 VRID：

**语法：**

vrrp set vrid <id> {prio<number> | adv <number> | mcastip <ip>| prom {on|off} | tif <name>}

**参数说明：**

| | |
|---|---|
| vrid | 虚拟路由 ID， 1-254 |
| prio | 优先级，1-255 |
| adv | 通告时间 1-3 |
| prom | 强制抢占属性开关，on：开启，off：关闭 |
| mcastip | 通告 IP 地址 |
| tif | 监测的网络接口的外部接口名，如 eth0,eth1 等多个网络接口之间用英文逗号隔开 |

**注意事项：**

VRID 不能重复，只能添加一次

通告 IP 为可选项，填写值与虚拟 IP 不能相同。

在多个墙之间，同一个 VRID 的墙的通告时间需相同，优先级不能相同。

必须在 vrrp 服务停止的状态下执行此命令

**示例：**

```
ac>vrrp set 1 prio 100 adv 1 prom on mcastip 2.3.2.3 tif eth2,eth3
```

## 删除一个 VRID：

**语法：**

vrrp del vrid <id>

**参数说明：**

| | |
|---|---|
| vrid | 虚拟路由 ID， 1-254 |

**注意事项：**

必须在 vrrp 服务停止的状态下执行此命令

**示例：**

```
ac>vrrp del vrid 1
```

## 显示 VRRP 运行状态：

**语法：**

vrrp show

**参数说明：**

无

**注意事项：**

无

**示例：**

```
ac>vrrp show
```

## 启动 VRRP 运行：

**语法：**

vrrp on

**参数说明：**

无

**注意事项：**

在启动 HA 集群状态同步的同时会启动 vrrp 的配置同步功能。请参见 5.8.1 节。

VRRP 功能与 HA 集群功能是互斥的，两者间只能选一种服务。

**示例：**

```
ac>vrrp on
```

## 停止 VRRP 运行：

**语法：**

vrrp off

**参数说明：**

无

**注意事项：**

无

**示例：**

```
ac>vrrp off
```

# 5.3.3 域名服务器（dns）

## 设置域名服务器：

**语法：**

dns set ip <ip> [ <ip> ]

**参数说明：**

| | |
|---|---|
| ip | 设置域名服务器的 IP 地址 |

**注意事项：**

无

**示例：**

```
ac>dns set ip 192.168.1.1 192.168.1.2
```

## 清除域名服务器：

**语法：**

dns unset

**参数说明：**

无

**注意事项：**

无

**示例：**

```
ac>dns unset
```

## 显示域名服务器：

**语法：**

dns show

**参数说明：**

无

**注意事项：**

无

**示例：**

```
ac>dns show
DNS 1: 192.168.1.1
DNS 2: 192.168.1.2
```

# 5.3.4 无线配置(wireless)

## 打开无线

**语法：**

wireless on

**参数说明：**
无

**注意事项：**
先配置并开启无线接口

**示例：**
```
ac>wireless on
```

## 关闭无线

**语法：**
wireless off

**参数说明：**
无

**注意事项：**
无线接口 wlan0 关闭时，无线也会关闭

**示例：**
```
ac>wireless off
```

## 扫描无线

**语法：**
wireless scan

**参数说明：**
无

**注意事项：**
无线必须处于关闭状态

**示例：**
```
ac>wireless scan
Wireless Scan Result.
ID        BSS          RSS(dBm)  Freq(Mhz)  Ch SSID
001 00:02:2d:4f:1a:54   -71.00      2437    6  LeadSec AP

002 00:0a:eb:e0:9e:8a   -60.00      2437    6  ccc

003 00:21:27:1f:4f:dc   -62.00      2437    6  TP-LINK_1F4FDC
```

```
004 5c:63:bf:ab:c8:5e   -78.00      2437    6  TP-LINK_ABC85E

005 40:16:9f:b7:3c:ac   -61.00      2437    6  TP-LINK_ZZZB73CAC
```

## 显示关联的客户端

**语法：**

wireless show station

**参数说明：**

无

**注意事项：**

无

**示例：**

```
ac>wireless show station
Wireless Station.
ID        MAC          RSSI(dbm) Tx(Mb/s) Still(ms) R(bytes) T(bytes)
001 00:24:8c:ad:48:db    -40       1.0    2520         7.9K   438B
```

## 显示无线配置

**语法：**

wireless show base | option | advanced

**参数说明：**

base 基本配置

option 可选配置

advanced 高级配置

**注意事项：**

无

**示例：**

```
ac>wireless show base
Wireless Base Setting.
     Active: On
Use_default: Yes
    Hw_mode: 802.11g
    Channel: CH6-2437MHZ
ac>wireless show option
Wireless Option Setting.
```

```
                Ssid: Themis_6000A1
Ignore_broadcast_ssid: No
       Security_mode: Disabled
ac>wireless show advanced
Wireless Advanced Setting.
       Beacon_int: 100 ms
      Dtim_period: 2 beacon
    Rts_threshold: 2347 bytes
  Fragm_threshold: 2346 bytes
         Preamble: Disabled
Ap_max_inactivity: 300 s
              Acl: Accept
        Deny_list:
```

## 恢复无线默认配置

**语法：**

wireless set default

**参数说明：**

无

**注意事项：**

无

**示例：**

```
ac>wireless set default
```

## 设置基本参数

**语法：**

wireless set base [ mode 11b | 11g ] { [ channel <number> ] | [ frequency <number> ] }

**参数说明：**

mode 工作模式，1-802.11b，2-802.11g，默认值：2

channel/frequency 工作频道，范围：1..14,14 代表自动选择，CH1-2412 MHz CH2-2417 MHz CH3-2422 MHz CH4-2427 MHz CH5-2432 MHz CH6-2437 MHz CH7-2442 MHz CH8-2447 MHz CH9-2452 MHz CH10-2457 MHz CH11-2462 MHz CH12-2467 MHz CH13-2472 MHz，默认为 CH6-2437 MHz

**注意事项：**

无

**示例：**

```
ac> wireless set base mode 11g channel 6
```

## 设置可选参数

**语法：**

wireless set option [ ssid <string> ] [ hidessid no | yes ] [ security_mode disabled | { wep [ auth open | share | mixed ] [ wep_default_key 0 | 1 | 2 | 3 ] [ key0type ascii | hex key0len 40 | 104 key0 <string> ] [ key1type ascii | hex key1len 40 | 104 key1 <string> ] [ key2type ascii | hex key2len 40 | 104 key2 <string> ] [ key3type ascii | hex key3len 40 | 104 key3 <string> ] } | { wpav1 | wpav2 [ wpa_key <string> ] [ wpa_key_mgmt psk ] [ wpa_key_algs TKIP | CCMP | mixed ] [ wpa_gtk_rekey <number> ] [ wpa_gmk_rekey <number> ] } ]

**参数说明：**

ssid 网络名称，范围：1..32 个非空字符，默认值：Themis_XXXXXX，无线网卡 MAC 地址的后三个字节

hidessid 隐藏 SSID

security_mode 加密方式，disabled，wep，wpav1，wpav2，默认值：disabled

auth 认证方式，open，share，mixed，默认值：open

wep_default_key 密钥索引，范围：0..3，默认值：0

key0type 密码 0 的类型为 16 进制或字符串

key0len 密码 0 的长度

key0 密码 0

key1type 密码 1 的类型为 16 进制或字符串

key1len 密码 1 的长度

key1 密码 1

key2type 密码 2 的类型为 16 进制或字符串

key2len 密码 2 的长度

key2 密码 2

key3type 密码 3 的类型为 16 进制或字符串

key3len 密码 3 的长度

key3 密码 3

wpav1 WPA 版本

wpav2 WPA 版本

wpa_key 密钥，长度 8 至 63 个字符

wpa_key_mgmt 密钥管理机制，固定值为 psk

wpa_key_algs 加密算法，TKIP，CCMP，mixed，默认值：TKIP

wpa_gtk_rekey 组密钥重协商周期，单位：s，范围：30..3600，默认值：60

wpa_gmk_rekey 组主密钥重协商周期，单位：s，范围：86400..864000，默认值：86400

**注意事项：**

无

**示例：**

```
ac> wireless set option ssid Themis_6000A1 hidessid no security_mode disabled
```

## 设置高级参数

**语法：**

wireless set advanced [ beacon_int <number> ] [ dtim_period <number> ] [ rts_threshold <number> ] [ fragm_threshold <number> ] [ shortpreamble enable | disable ] [ ap_max_inactivity <number> ] { [ accept_mac <mac>+ | none ] | [ deny_mac <mac>+ | none ] }

**参数说明：**

beacon_int 信标发送间隔，范围：15..65535，默认值：100，单位：ms
dtim_period 每间隔多少个信标携带 DTIM 消息，范围：1..255，默认值：2，单位：个
rts_threshold RTS 阀值，范围：0..2347，默认值：2347 代表不开启
fragm_threshold 分片阀值，范围：256..2346，默认值：2346 代表不开启
shortpreamble 是否使用 Short Preamble 来提高网络性能，默认值：否
ap_max_inactivity 允许客户端静止时间，范围：120..600，单位：s，默认值：300
accept_mac 允许接入的列表
deny_mac 拒绝接入的列表

**注意事项：**

无

**示例：**

```
ac> wireless set advanced beacon_int 100 dtim_period 2 rts_threshold 2347 fragm_threshold 2346 shortpreamble disable ap_max_inactivity 300 accept_mac
```

# 5.4 UPnP 服务器

## 设置 UPnP 接口

**语法：**

upnp set exif <exif> inif<inif>

**参数说明：**

exif 设置 UPnP 服务的外部接口
inif 设置 UPnP 服务的内部接口

**注意事项：**

外部接口和内部接口不能是同一个接口；
合法的接口为以下设备：
以太网物理设备或 VLAN 设备或网桥设备或别名设备

设备已经启用
设备具有非空 IP 地址且地址不为 0.0.0.0

**示例：**

```
ac>upnp set exif eth0 inif eth0
```

## 启动 upnp 服务

**语法：**

upnp start

**参数说明：**

无

**注意事项：**

已经利用 upnp set exif <exif> inif<inif> 设置了合法的接口。

**示例：**

```
ac>upnp start
```

## 显示 upnp 的接口设置和运行状态

**语法：**

upnp show status

**参数说明：**

无

**注意事项：**

无

**示例：**

```
ac> upnp show status
upnp interface para
external_name      internal_name      status
eth0               brg0               stopped
```

## 停止 upnp 服务

**语法：**

upnp stop

**参数说明：**

无

**注意事项：**

upnp 服务已经在运行

可通过 upnp show status 察看 upnp 服务的运行状态。

**示例：**

```
ac>upnp stop
```

## 添加可以使用 upnp 服务的地址

**语法：**

upnp rule add name <name> ip <ip > [comment <comment>]

**参数说明：**

| | |
|---|---|
| rule | 设置使用 upnp 服务的地址的规则 |
| name | 设置规则的名字 |
| ip | 设置使用 upnp 服务的地址，可以使用单个 IP 地址、IP 地址/子网掩码 |
| comment | 设置规则的注释，可选参数，默认为空 |

**注意事项：**

无

**示例：**

```
ac>upnp rule add name rule4 ip 175.10.0.0/255.255.0.0 comment “upnp rule”
```

## 删除可以使用 upnp 服务的地址

**语法：**

upnp rule del {id <id> | all}

**参数说明：**

| | |
|---|---|
| rule | 设置使用 upnp 服务的地址的规则 |
| id | 指定欲删除的地址项的 id |
| all | 删除所有地址 |

**注意事项：**

无

**示例：**

```
ac>upnp rule del id 3
```

## 修改可以使用 upnp 服务的地址

**语法：**

upnp rule set id <id > [name <name>] [ip <ip >] [comment <comment>]

**参数说明：**

rule 设置使用 upnp 服务的地址的规则

id 指定欲修改的地址项的 id

name 设置规则的名字

ip 设置使用 upnp 服务的地址，可以使用单个 IP 地址、IP 地址/子网掩码

comment 设置规则的注释，可选参数，默认为空

**注意事项：**

无

**示例：**

```
ac>upnp rule set id 2 ip 168.10.0.0/255.255.0.0
```

## 显示可以使用 upnp 服务的地址

**语法：**

upnp rule show

**参数说明：**

rule 设置使用 upnp 服务的地址的规则

**注意事项：**

无

**示例：**

```
ac>upnp rule show
total rules: 4
id   name              ip                              comment
1    name2             10.1.1.0/255.255.255.0          fjuy dfvd
2    r1                10.50.10.235/255.255.255.255    234 678
3    dsf               192.0.0.0/255.255.255.0         使用 upnp
4    rule              175.0.0.0/255.0.0.0             允许使用 UPnP
```

# 5.5 DHCP 服务器（dhcpserver）

## 显示 DHCP 服务器当前设置

**语法：**

dhcpserver show

**参数说明：**

无

**注意事项：**

无

**示例：**

ac>dhcpserver show

## 添加 DHCP 域

**语法：**

dhcpserver add domain network <network> netmask <netmask> range <range> [gateway <gateway>] [dns <dns>] [domainname <domainname>] [comment <comment>] [ is_vpnclient <yes/no> ] [ vpnclient_netmask <subnet mask> ] [ circuit_id <circuit id> ]

**参数说明：**

<network> 必填项，和“网络掩码”一起决定为哪个子网提供 DHCP 服务。

<netmask> 必填项，和网络地址一起决定子网地址；

<range> 必填项，DHCP 服务器可用于分配的 IP 地址段，只能选择在资源定义中定义好的地址段。参考 address 命令。

<gateway> 可选项，为 DHCP 客户端配置网关地址；

<dns> 可选项，为 DHCP 客户端配置 DNS 服务器地址；

<domainname> 可选项，为 DHCP 客户端配置域名；

<comment> 可选项，一些说明。

is_vpnclient 是否 vpn 客户端

vpnclient_netmask vpn 客户端掩码

circuit_id circuit id

**注意事项：**

这里定义的子网，必须是安全网关接口确实连接的子网，否则启动 DHCP 服务器会失败。

网络地址的主机部分一定为 0，如 10.1.1.0 是网络地址，而 10.1.1.1 是主机地址。

<range>必须在地址列表资源中定义地址段（注意，必须是地址段，而非掩码地址或反地址，参考：address 命令）。

**示例：**

ac> dhcpserver add domain network 10.1.1.0 netmask 255.255.255.0 range dhcp gateway 10.1.1.254 domainname “lenovo.com” dns 10.1.1.100 comment “lenovo dhcp domain”

## 设置 DHCP 域

**语法：**

dhcpserver set domain id <id> [network <network>] [netmask <netmask>] [range <range>] [gateway <gateway>] [domainname <domainname>] [dns <dns>] [comment <comment>] [ is_vpnclient <yes/no> ] [ vpnclient_netmask <subnet mask> ] [ circuit_id <circuit id> ]

**参数说明：**

<id> 必填项，指出要设置的域的 ID，可以用 dhcpserver show 查看；
<network> 可选项，修改子网地址。
<netmask> 可选项，修改网络掩码；
<range> 可选项，修改 IP 地址段。
<gateway> 可选项，修改网关地址；
<domainname> 可选项，修改域名；
<dns> 可选项，修改 DNS 服务器地址；
<comment> 可选项，一些说明。
is_vpnclient 是否 vpn 客户端
vpnclient_netmask vpn 客户端掩码
circuit_id circuit id

**注意事项：**

修改后的域，也必须满足添加域中的注意事项。

**示例：**

ac> dhcpserver set domain id 1 network 10.1.2.0
ac> dhcpserver set domain id 1 range dhcp2
ac> dhcpserver set domain id 1 gateway 10.1.2.254

## 删除 DHCP 域

**语法：**

dhcpserver del domain id <id>

**参数说明：**

<id> 要删除的域 ID，可以通过 dhcpserver show 查看

**注意事项：**

无

**示例：**

```
ac>dhcpserver del domain id 1
```

## 添加静态分配 IP 地址

**语法：**

dhcpserver add static hostname <hostname> mac <mac> ip <ip> [comment <comment>]

**参数说明：**

<hostname> 必填项，要分配固定 IP 地址的主机名称；
<mac> 必填项，主机的 MAC 地址；
<ip> 必填项，要分配给该主机的 IP 地址；
<comment> 可选项，一些说明。

**注意事项：**

无

**示例：**

```
ac>dhcpserver add static hostname themis mac 00:83:45:df:7a:9d ip 10.1.5.46 comment “host1”
```

## 设置静态分配 IP 地址

**语法：**

dhcpserver set static id <id> [hostname <hostname>] [mac <mac>] [ip <ip>] [comment <comment>]

**参数说明：**

<id> 必填项，指出要修改的主机 ID，可以通过 dhcpserver show 查看
<hostname> 可选项，修改要分配固定 IP 地址的主机名称；
<mac> 可选项，修改主机的 MAC 地址；
<ip> 可选项，修改要分配给该主机的 IP 地址；
<comment> 可选项，一些说明。

**注意事项：**

无

**示例：**

```
ac>dhcpserver set static id 1 hostname themis2
ac>dhcpserver set static id 1 mac 00:83:45:df:88:99
ac>dhcpserver set static id 1 ip 10.1.5.19
```

## 删除静态分配 IP 地址

**语法：**

dhcpserver del static id <id>

**参数说明：**

<id> 要删除的主机 ID，可以通过 dhcpserver show 查看

**注意事项：**

无

**示例：**

```
ac>dhcpserver del static id 1
```

## 设置 DHCP 服务器是否随安全网关同时启动（缺省关闭）

**语法：**

dhcpserver set startup {on | off}

**参数说明：**

on 打开 DHCP 服务器自动启动

off 关闭 DHCP 服务器自动启动

**注意事项：**

无

**示例：**

```
ac>dhcpserver set startup on
```

## 启动 DHCP 服务器

**语法：**

dhcpserver start

**参数说明：**

无

**注意事项：**

如果启动失败，请检查域和主机配置是否正确。

**示例：**

```
ac>dhcpserver start
```

## 停止 DHCP 服务器

**语法：**

dhcpserver stop

**参数说明：**
无

**注意事项：**
无

**示例：**
```
ac>dhcpserver stop
```

# 5.6 双机热备

## 5.6.1 集群（HA）

### 设置网络接口 HA 的 IP 地址：

**语法：**
ha set ip <ip> netmask <netmask> haif { on | off } syn { on | off }

**参数说明：**

| | |
|---|---|
| ip | 设置 IP 地址 |
| netmask | 设置子网掩码 |
| haif | HA 网口启动开关 on：开启，off：关闭 |
| syn | HA 状态同步开关 on：开启，off：关闭 |

**注意事项：**
欲设置的 IP 地址不能与其它网络接口上的 IP 地址或地址池在同一子网；
启用集群后不能修改网络接口 eth1 的 IP 地址。
若 HA 处于启动状态，不能将 HA 网口启动开关设置为关闭，只有先关闭 HA（用 ha off）才允许关闭 HA 网口
**示例：**
```
ac>ha set ip 192.168.1.1 netmask 255.255.255.0 haif on syn on
```

### 设置集群：

**语法：**
ha set mode { backup | cluster } node <number> id <number>

**参数说明：**

| | |
|---|---|
| mode | 设置集群工作模式，backup 为热备模式，cluster 为负载均衡模式 |

| | |
|---|---|
| node | 设置安全网关节点号，有效值为 1 至 4 |
| id | 设置集群 ID 号，有效值为 1 至 255 |

**注意事项：**
一个集群中的安全网关必须具有相同的 ID 号；
启用集群后不能修改集群设置。

**示例：**
```
ac>ha set mode backup node 1 id 100
```

## 启用集群：

**语法：**
ha on

**参数说明：**
无

**注意事项：**
无

**示例：**
```
ac>ha on
```

## 停止集群：

**语法：**
ha off

**参数说明：**
无

**注意事项：**
VRRP 功能与 HA 集群功能是互斥的，两者间只能选一种服务。

**示例：**
```
ac>ha off
```

## 同步集群：

**语法：**

ha sync

**参数说明：**
无

**注意事项：**
无

**示例：**
ac>ha sync

## 清除集群设置：

**语法：**
ha unset

**参数说明：**
无

**注意事项：**
启用集群后不能清除集群设置。

**示例：**
ac>ha unset

## 显示集群设置：

**语法：**
ha show config

**参数说明：**
无

**注意事项：**
无

**示例：**
ac>ha show config
Enable: on
IP Address: 192.168.1.1
Netmask: 255.255.255.0
Mode: cluster

Node: 1
ID: 1

### 显示集群状态：

**语法：**
ha show status

**参数说明：**
无

**注意事项：**
无

**示例：**
```
ac>ha show status
ID  Priority       IP_Address  Sync
 1         1      192.168.1.1  yes
 2         2      192.168.1.2  no
 3         0      192.168.1.3  no
```

## 5.6.2 集群探测（hadetect）

### 设置集群探测失效阈值：

**语法：**
hadetect set threshold <number>

**参数说明：**
threshold 设置集群探测失效阈值，有效值为 1 至 100

**注意事项：**
当集群中只有一台安全网关时，不会失效。

**示例：**
```
ac>hadetect set threshold 100
```

### 添加集群探测 IP 地址：

**语法：**

hadetect add ip <ip> weight <number> if <interface>

**参数说明：**

| | |
|---|---|
| ip | 设置欲探测的 IP 地址 |
| weight | 设置此 IP 地址的失效权重，有效值为 1 至 100 |
| if | 设置此 IP 地址对应的网络接口 |

**注意事项：**

无

**示例：**

```
ac>hadetect add ip 192.168.1.1 weight 10 if eth0
```

## 删除集群探测 IP 地址：

**语法：**

hadetect del ip <ip>

**参数说明：**

| | |
|---|---|
| ip | 指定欲删除的 IP 地址 |

**注意事项：**

无

**示例：**

```
ac>hadetect del ip 192.168.1.1
```

## 添加集群探测网络接口：

**语法：**

hadetect add if <interface>

**参数说明：**

| | |
|---|---|
| if | 设置欲探测的网络接口 |

**注意事项：**

无

**示例：**

```
ac>hadetect add if eth0
```

## 删除集群探测网络接口：

**语法：**
hadetect del if <interface>

**参数说明：**
if 指定欲删除的网络接口

**注意事项：**
无

**示例：**
```
ac>hadetect del if eth0
```

## 显示集群探测失效阈值：

**语法：**
hadetect show config

**参数说明：**
无

**注意事项：**
无

**示例：**
```
ac>hadetect show config
Failure Threshold: 100
```

## 显示 IP 地址探测状态：

**语法：**
hadetect show ip

**参数说明：**
无

**注意事项：**
无

**示例：**

```
ac>hadetect show ip
Failure Threshold:100
Failure Deteted now:0
--------------------------------------
IP_Address     Weight  Interface  Status
20.1.1.2           33  eth2        on
20.1.1.3           10  eth2        on
```

## 显示网络接口探测状态：

**语法：**

hadetect show if

**参数说明：**

无

**注意事项：**

无

**示例：**

```
ac>hadetect show if
Interface  Alert  Status
ge1        yes    on
ge2        yes    on
ge3        yes    off
eth0        yes    on
eth1        no     off
eth2        no     off
eth3        no     off
eth4        no     off
eth5        no     off
eth6        no     off
eth7        no     off
```

## 显示集群中其它安全网关上的 IP 地址探测状态：

**语法：**

hadetect show remote_ip <ip>

**参数说明：**

remote_ip 指定集群中其它安全网关的网络接口“ha”的 IP 地址

**注意事项：**

无

**示例：**

```
ac>hadetect show remote_ip 192.168.1.2
Failure Threshold: 100
Failure Deteted: 30
---------------------------------------
IP_Address     Weight  Interface  Status
192.168.100.1     10   ge1        on
192.168.100.2     20   ge1        on
192.168.100.3     30   ge1        off
```

## 显示集群中其它安全网关上的网络接口探测状态：

**语法：**

hadetect show remote_if <ip>

**参数说明：**

remote_if 指定集群中其它安全网关的网络接口“ha”的 IP 地址

**注意事项：**

无

**示例：**

```
ac>hadetect show remote_if 192.168.1.2
Interface  Alert  Status
ge1        yes    on
ge2        yes    on
ge3        yes    off
eth0        yes    on
eth1        no     off
eth2        no     off
eth3        no     off
eth4        no     off
eth5        no     off
eth6        no     off
eth7        no     off
```

## 启用探测

**语法：**

hadetect on

**参数说明：**

无

**注意事项：**
无

**示例：**
ac>hadetect on

## 停止探测

**语法：**
hadetect off

**参数说明：**
无

**注意事项：**
无

**示例：**
ac>hadetect off

# 第6章 路由

## 6.1.1 基本路由、高级路由表、高级路由表策略（route）

## 添加高级路由表：

**语法：**
route table add tablename <name> id <id> comment <string>

**参数说明：**

| | |
|---|---|
| tablename | 路由表名称 |
| id | 路由表 ID |
| comment | 注释信息 |

**注意事项：**
路由表 ID 的范围是 1-200

**示例：**

```
ac>route table add tablename table-1 id 1 comment table-frist
```

## 删除高级路由表：

**语法：**

route table del tablename <name>

**参数说明：**

| | |
|---|---|
| tablename | 路由表名称 |

**注意事项：**

无

**示例：**

```
ac>route table del tablename table-1
```

## 添加路由到路由表

**语法：**

route troute add destip <ip/mask> nexthop <ip> dev <if> metric <id> tablename <string>

**参数说明：**

| | |
|---|---|
| destip | 设置目的 IP 地址，可以使用单个 IP 地址、IP 地址/子网掩码 |
| nexthop | 设置下一跳网关的 IP 地址 |
| dev | 流出接口名称 |
| metric | 路由开销值 |
| tablename | 路由表名称 |

**注意事项：**

下一跳的 IP 地址必须与流出接口在同一网段

**示例：**

```
ac> route troute add destip 2.2.2.2/255.255.255.0 nexthop 10.1.5.218 dev eth0 metric 10
tablename table-1
```

## 编辑路由表中的路由：

**语法：**

route troute set destip <ip/mask> nexthop <ip> dev <if> metric <id> tablename <string> id <id>

**参数说明：**

| | |
|---|---|
| destip | 设置目的 IP 地址，可以使用单个 IP 地址、IP 地址/子网掩码 |

nexthop 设置下一跳网关的 IP 地址
dev 流出接口名称
metric 路由开销值
tablename 路由表名称
id 路由 ID

**注意事项：**

下一跳的 IP 地址必须与流出接口在同一网段

**示例：**

```
ac>route troute set destip 2.2.22.2/255.255.255.0 nexthop 10.1.5.168 dev eth0 metric 120
tablename table-1 id 2
```

## 删除路由表中的路由：

**语法：**

route troute del tablename <string> id <id>

**参数说明：**

tablename 路由表名称
id 路由 ID

**注意事项：**

无

**示例：**

```
ac>route troute del tablename table-1 id 2
```

## 添加高级路由规则：

**语法：**

route rule add sip <ip/mask> dip <ip/mask> iif <if> service <string> prio <id> tablename <string> isp <off/on>

**参数说明：**

sip 设置源 IP 地址，可以使用单个 IP 地址、IP 地址/子网掩码
dip 设置目的 IP 地址，可以使用单个 IP 地址、IP 地址/子网掩码
iif 流入网口
service 服务
prio 优先级
tablename 路由表名称
isp 是否设置 isp 路由表

**注意事项：**

优先级从 1 至 20000 依次递减

**示例：**

ac>route rule add sip 1.1.1.1/255.255.255.0 dip 2.2.2.2/255.255.255.0 iif eth0 service FTP prio 100 tablename table-1 isp off

## 修改高级路由规则：

**语法：**

route rule set sip <all_ip> dip <all_ip> iif <if> service <string> prio <id> tablename <string> id <id> isp <on/off>

**参数说明：**

sip 设置源 IP 地址，可以使用单个 IP 地址、IP 地址/子网掩码
dip 设置目的 IP 地址，可以使用单个 IP 地址、IP 地址/子网掩码
iif 流入网口
service 服务
prio 优先级
tablename 路由表名称
isp 是否设置 isp 路由表

**注意事项：**

优先级从 1 至 20000 依次递减。

**示例：**

ac> route rule set sip 100.1.1.1/255.255.255.0 dip 200.2.2.2/255.255.255.0 iif eth0 service FTP prio 200 tablename "table-1" id 2 isp off

## 删除高级路由规则：

**语法：**

route rule del prio <id>

**参数说明：**

prio 优先级

**示例：**

ac>route rule del prio 200

## 显示所有路由：

**语法：**

route show

**参数说明：**
无

**注意事项：**
无

**示例：**

```
ac> route show

Name                    Table Id    Comment
基本路由表              254         基本路由表
table-1                 1           table-frist

route list

Tablename    Destination IP         Gateway     Interface  Metric  Active
table-1      2.2.22.2/255.255.255.0 10.1.5.168  eth0        120     1
基本路由表   6.6.6.6/255.255.255.0  10.1.5.188  eth0        12      1

route rule

Priority   ID    Source IP   Destination IP   Dev      Service        Mark
32766      1     any         any              any       any          42766
```

## 6.1.2 多默认路由负载均衡（multiRoute）

## 添加默认路由：

**语法：**
multiroute add [ ip <ip> ] ifname <string> weight <number> active { on | off } [detectip1 <ip>] [detectip2 <ip>]
**参数说明：**

| | |
|---|---|
| ip | 默认路由网关 IP 地址 |
| ifname | 本地的网络设备接口名，该网络接口与上面指定的网关直接连接 |
| active | 是否在系统中启用该默认路由 |
| weight | 该默认路由被指定的权重 |
| detectip1 | 第二个探测 IP |
| detectip2 | 第三个探测 IP |

**注意事项：**

1、 默认路由网关的 IP 地址必须与指定的网络设备接口 IP 地址在同一网段
2、 有效权重值范围是：1-255
3、 如果待加入的默认路由出口设备是拨号设备，则不需要指定其网关 ip 地址
4、 目前支持的设备包括：物理设备、拨号设备、别名设备

**示例：**

```
ac>multiroute add ip 10.1.5.100 ifname eth0 active on weight 12
ac>multiroute add ifname dial0 active on weight 11
```

## 删除默认路由：

**语法：**

multiroute del ip <ip> ifname <interface>

**参数说明：**

| | |
|---|---|
| ip | 默认路由网关 IP 地址 |
| ifname | 本地的网络设备接口名，该网络接口与上面指定的网关直接连接 |

**注意事项：**

1、默认路由网关的 IP 地址必须与指定的网络设备接口 IP 地址在同一网段
2、如果待删除的默认路由出口设备是拨号设备，则不需要指定其网关 ip 地址

**示例：**

```
ac>multiroute del ip 10.1.5.100 ifname eth0
ac>multiroute del ifname dial0
```

## 修改默认路由：

**语法：**

multiroute set routeconfig ip <ip> ifname <interface> [ active { on | off } | weight <weight> ]

multiroute set { [ routeconfig [ ip <ip> ] ifname <string> [ weight <number> | active { on | off } ] [detectip1 <ip>] [detectip2 <ip>] ] }

**参数说明：**

| | |
|---|---|
| routeconfig | 指定对路由配置信息进行操作 |
| ip | 默认路由网关 IP 地址 |
| ifname | 本地的网络设备接口名，该网络接口与上面指定的网关直接连接 |
| active | 是否在系统中启用该默认路由 |
| weight | 该默认路由被指定的权重 |
| detectip1 | 第二个探测 IP |
| detectip2 | 第三个探测 IP |

**注意事项：**

1、有效权重值范围是：1-255

2、如果待修改的默认路由出口设备是拨号设备，则不需要指定其网关 ip 地址

**示例：**

```
ac>multiroute set routeconfig ip 10.1.5.100 ifname eth0 active on
ac>multiroute set routeconfig ip 10.1.5.100 ifname eth0 weight 34
ac>multiroute set routeconfig ip 10.1.5.100 ifname eth0 active off weight 23
ac>multiroute set routeconfig ifname dial0 active on
ac>multiroute set routeconfig ifname dial0 weight 54
ac>multiroute set routeconfig ifname dial0 active on weight 44
```

## 修改默认路由状态信息：

**语法：**

multiroute set routestatus [ active { on | off } | freq <freq> ]

**参数说明：**

| | |
|---|---|
| routestatus | 指定对默认路由的状态信息进行操作 |
| active | 是否启用网关检测（即是否监测网关的可连通性） |
| freq | 如果启用了网关监测，设置其监测频率 |

**注意事项：**

1、 启用网关监测功能时，系统会随时更新默认路由信息，以保证系统中的每一条默认路由网关都是可连通的，对于不可连通的默认路由网关，其相应的默认路由将不会出现在系统路由表中

2、 在不启用网关监测功能时，系统默认所有配置的默认路由网关都是可连通的

3、 拨号设备的默认路由实时监测功能不受 active 参数的影响，即其总是按照指定的监测频率 freq 对拨号设备进行监测

**示例：**

```
ac>multiroute set routestatus active on
ac>multiroute set routestatus freq 23
ac>multiroute set routestatus freq 23 active off
```

## 显示默认路由配置信息：

**语法：**

multiroute show routeconfig [ ip <ip> | ifname <interface> ]

**参数说明：**

| | |
|---|---|
| routeconfig | 指定对路由配置信息进行操作 |

| | |
|---|---|
| ip | 默认路由网关 IP 地址 |
| ifname | 本地的网络设备接口名，该网络接口与上面指定的网关直接连接 |

**示例：**

```
ac>multiroute show routeconfig
ac>multiroute show routeconfig ip 10.1.5.100
ac>multiroute show routeconfig ifname eth0
ac>multiroute show routeconfig ip 10.1.5.100 ifname eth0
ac>multiroute show routeconfig ifname dial0
```

## 显示默认路由状态信息：

**语法：**

multiroute show routestatus

**参数说明：**

| | |
|---|---|
| routestatus | 指定对默认路由状态信息进行操作 |

**示例：**

ac> multiroute show routestatus

## 显示系统默认路由信息：

**语法：**

multiroute show systemroute

**参数说明：**

| | |
|---|---|
| systemroute | 指定对系统中正在生效的默认信息进行操作 |

**示例：**

ac> multiroute show systemroute

## 停止系统中的多默认路由负载均衡：

**语法：**

multiroute off

**参数说明：**

| | |
|---|---|
| off | 关闭系统中的多默认路由负载均衡 |

**示例：**
ac> multiroute off

## 启用系统中的多默认路由负载均衡：

**语法：**
multiroute on

**参数说明：**
on 启用系统中的多默认路由负载均衡

**示例：**
ac> multiroute on

## 重启系统中的多默认路由负载均衡：

**语法：**
multiroute restart

**参数说明：**
restart 重启系统中的多默认路由负载均衡

**示例：**
ac> multiroute restart

# 6.1.3 ISP 路由(isp)

## 更新 ISP 地址文件：

**语法：**
isp update filename <file_name> id <id>
**参数说明：**
filename 导入文件名
id isp 的 id
**注意事项：**
联通的 id 为 1，电信的 id 为 2，教育网 id 为 3，移动 id 为 4，自定义 id 为 5

**示例：**
ac> isp update filename "unicom.txt" id 3

## 导出 ISP 地址文件：

**语法：**
isp export filename <file_name> id <id>
**参数说明：**
filename 导出的文件名
id isp 的 id
**注意事项：**
联通的 id 为 1，电信的 id 为 2，教育网 id 为 3，移动 id 为 4，自定义 id 为 5
**示例：**
```
ac> isp export filename "unicom.txt" id 1
```

## 清空 ISP 地址：

**语法：**
isp flush ispname <name>
**参数说明：**
Ispname isp 名称
**注意事项：**
无
**示例：**
```
ac> isp flush ispname "教育网"
```

## 添加 ISP 地址段：

**语法：**
isp insert ip <ip> netmask <netmask/id> ispaddr <name>

**参数说明：**
ip ip 地址
netmask 掩码
ispaddr ISP 名称

**注意事项：**

**示例：**
```
ac> isp insert ip 8.8.8.8 netmask 255.255.255.0 ispaddr "联通"
```

## 添加 ISP 路由表：

**语法：**

isp add ispaddr <name> nexthop <single_ip> dev <interface> metric <id>

**参数说明：**

ispaddr isp 名称
nexthop 下一跳 IP 地址
dev 流出网口
metric 路由开销值

**注意事项：**

下一跳的 IP 地址必须与流出接口在同一网段

**示例：**

```
ac> isp add ispaddr "电信" nexthop 10.1.5.5 dev eth0 metric 1
```

## 修改 ISP 路由表：

**语法：**

isp set ispaddr <name> nexthop <single_ip> dev <interface> metric <id>

**参数说明：**

ispaddr isp 名称
nexthop 下一跳 IP 地址
dev 流出网口
metric 路由开销值

**注意事项：**

下一跳的 IP 地址必须与流出接口在同一网段

**示例：**

```
ac> isp set ispaddr "电信" nexthop 10.1.5.50 dev eth0 metric 11
```

## 删除 ISP 路由表：

**语法：**

isp del ispaddr <name>

**参数说明：**

ispaddr isp 名称

**注意事项：**

无

**示例：**

ac> isp del ispaddr "电信"

## 6.1.4 动态路由管理(advroute)

### 配置 ospf 全局参数

用该命令可以配置 ospf 路由 id，ospf 进程启停，及使能重发布。

**语法：**

advroute set ospf routerid <ip> [connected { on | off } ] [static { on | off } ] [ rip { on | off } ] [ bgp {on | off } ] [ defgw { on | off } ] [ active { on | off } ]

参数说明：

routeid：是运行 ospf 路由器的 32 位标识号码，用 ip 地址表示

connected：指连接路由

static：指静态路由

rip：指 rip 路由

bgp：指 bgp 路由

defgw：指 ospf 缺省路由

active：ospf 进程启动开关

**示例：**

配置路由 id 为 0.0.0.1，启动 ospf 进程，并重发布连接路由。

ac> advroute set ospf routerid 0.0.0.1 connected on active on

### 添加 ospf 区域

**语法：**

advroute add ospf area <ip> [ type { regular | nssa | stub } ] [auth { none | text | md5 } ] [ virtual_link <ip> ]

**参数说明：**

area：指 ospf 区域 id

type：ospf 区域类型

nssa：指定该区域类型为端区

stub：指定该区域类型为非完全端区

auth：配置区域认证

text：明文认证

md5：md5 认证

virtual_link：该参数 ip 地址是虚连接远端路由器的 router-id.

**示例：**

**添加主干区域 0.0.0.0**

**ac> advroute add ospf area 0.0.0.0**

### 修改 ospf 区域配置

**语法：**

advroute set ospf area <ip> [ type { regular | nssa | stub } ] [ auth { none | text | md5 } ] [ virtual_link <ip> ]

**参数说明：**

<见添加 ospf 区域的相关说明>

**示例：**

修改区域 0.0.0.1 认证方式为 md5

ac> advroute set ospf area 0.0.0.1 auth md5

## 删除 ospf 区域

**语法：**

advroute del ospf area <ip>

**示例：**

删除区域 0.0.0.1

ac> advroute del ospf area 0.0.0.1

## 添加 ospf 网络

**语法：**

advroute add ospf net <ip> netmask <netmask> area <ip>

**参数说明：**

Net: 配置要参与 ospf 协议的网段 ip

Netmask: 子网掩吗

Area: 指区域 id

**示例：**

ac>advroute add ospf net 192.168.1.0 netmask 255.255.255.0 area 0.0.0.0

## 修改 ospf 网络配置

**语法：**

advroute set ospf net <ip> netmask <netmask> area <ip>

**注意事项：**

在此命令中，能修改的参数只能是区域 id，即 area。

**示例：**

ac>advroute set ospf net 192.168.1.0 netmask 255.255.255.0 area 0.0.0.1

## 删除 ospf 网络

**语法：**

advroute del ospf net <ip> netmask <netmask> area <ip>

**示例：**

ac>advroute del ospf net 192.168.1.0 netmask 255.255.255.0 area 0.0.0.1

## 添加 ospf 端口

**语法：**

advroute add ospf port <name> [ auth { none | text | md5 } ] [ passwd <string> ] [ hello <number> ] [ dead <number> ] [ comment <comment> ]

**参数说明：**

Port：端口名称如 eth0 等

Ip：该端口的 ip 地址 <= 请删除该行
Auth：使能端口的认证功能
Passwd:：配置明文密钥
Hello：hello 定时器，用于邻居发现
Dead：dead 定时器，在没有受到 hello 报文多长时间判定邻居已断连。
Comment：提示性说明
**注意事项：**
端口名称和其 ip 地址必须同系统配置一致，并该端口已启动。
**示例：**
ac> advroute add ospf port eth0

## 修改 ospf 端口配置

**语法：**
advroute set ospf port <name> [ auth { none | text | md5 } ] [ passwd <string> ] [ hello <number> ] [ dead <number> ] [ comment <comment> ]
**注意事项：**
可以通过此命令修改 auth，passwd, hello, dead comment 等参数。
**示例：**
ac> advroute set ospf port eth0 auth text passwd 123456

## 删除 ospf 端口

**语法：**
advroute del ospf port <name>
**示例：**
ac> advroute del ospf port eth0

## 添加 ospf 端口 md5 认证

**语法：**
advroute add ospf message-digest port <name> key <id> md5 <string>
**参数说明：**
key：指 key id。 取值范围<1-255>
md5：指 ospf 密钥。长度为 1 至 16 个字符。
**示例：**
ac> advroute add ospf message-digest port eth0 key 1 md5 123abc

## 修改 ospf 端口 md5 认证

**语法：**
advroute set ospf message-digest port <name> key <id> md5 <string>
**注意事项：**
该命令仅能修改 md5 密钥
**示例：**
ac> advroute set ospf message-digest port eth0 key 1 md5 456abc

## 删除 ospf 端口 md5 认证

**语法：**

advroute del ospf message-digest port <name> key <id>

**示例：**

ac> advroute del ospf message-digest port eth0 key 1

## 显示 ospf 路由

**语法：**

advroute show ospf route

## 启停 pim-sm

**语法：**

advroute set pim sparse-mode active {on|off}

**参数说明：**

active：pim-sm 启停开关

**示例：**

ac> advroute set pim sparse-mode active on

## 添加 pim rp

**语法：**

advroute add pim rp <ip>

**参数说明：**

rp: rp 的 ip 地址

**示例：**

ac> advroute add pim rp 192.168.1.100

## 删除 pim rp

**语法：**

advroute del pim rp <ip>

**示例：**

ac> advroute del pim rp 192.168.1.100

## 添加 pim-sm 端口

**语法：**

advroute add pim sparse-mode port <name> dr-priority <number> rp-candidate {on|off} rp-priority <number>

**参数说明：**

Port：多播端口，如：eth0

Dr-priority：dr 优先级，取值范围<0-4294967294>

Rp-candidate：rp-candidate 使能开关

Rp-priority：rp-candidate 优先级，取值范围<0-255>

**示例：**

ac> advroute add pim sparse-mode port eth0 dr-priority 1 rp-candidate on rp-priority 1

## 修改 pim-sm 端口配置

**语法：**

advroute set pim sparse-mode port <name> dr-priority <number> rp-candidate {on|off} rp-priority <number>

**注意事项：**

该命令可修改 dr-priority, rp-candidate, rp-priority 等参数

**示例：**

ac> advroute set pim sparse-mode port eth0 dr-priority 1 rp-candidate on rp-priority 10

## 删除 pim-sm 端口

**语法：**

advroute del pim sparse-mode port <name>

**示例：**

ac> advroute del pim sparse-mode port eth0

## 设置 RIP 全局参数

**语法：**

advroute set rip [ active { on | off } ] [ version { v1 | v2 } ] [ ospf { on [ ospf_metric <number> ] | off } ] [ connected { on [ connected_metric <number> ] | off } ] [ static { on [ static_metric <number> ] | off } ] [ kernel { on [ kernel_metric <number> ] | off } ] [ bgp { on [ bgp_metric <number> ] | off } ] [ isis { on [ isis_metric <number> ] | off } ] [ defgw { on | off } ] [ update <number> ] [ holddown <number> ] [ garbage <number> ]

## 添加 RIP 密码链

**语法：**

advroute add rip key_chain <name> keyid <number> keyword <string> start <string> { end <string> | infinite }

## 删除 RIP 密码链

**语法：**

advroute del rip key_chain <name> keyid <number>

## 设置 RIP 网络

**语法：**

advroute add rip net <all_ip> netmask <all_ip>

**示例：**

ac> advroute add rip net 5.5.5.5 netmask 255.255.255.0

## 设置 RIP 端口

**语法：**

advroute add rip port <name> [ auth { none | text [ { single_key <string> | key_chain <name> } ] | md5 [ { single_key <string> | key_chain <name> } ] } ] [ send { v1 | v2 | both } ] [ receive { v1 | v2 | both } ] [ passive ]

**示例：**

ac> advroute add rip port eth0 auth none send v2 receive v2

## 启停 RIP

**语法：**

advroute set rip [ active { on | off } ]

**示例：**

ac> advroute set rip active on

### 显示 RIP 路由表

**语法：**

advroute show rip route

# 第7章 防火墙

## 7.1 策略

### 7.1.1 安全策略(rule)

### 添加类型为代理的安全规则：

**语法：**

rule add type proxy name <name> [ id <id> ] [ sa { any | <name> | <ip> } ] [ sport <port> ] [ smac <mac> ] [ da { any | <name> | <ip> } ] [ iif { any | <interface> } ] service <name> proxy <name> [ time { <name> | none } ] [ authgroupname <name> ][ log { on | off } ] [ active { on | off } ] [ comment <comment> ]

**参数说明：**

| | |
|---|---|
| name | 设置安全规则的名字，必选参数 |
| id | 设置安全规则的序号，有效值为 1 至 65535，可选参数，默认为最后 |
| sa | 设置源地址，可以使用单个 IP 地址、IP 地址/子网掩码、地址定义、地址组定义、“any”，可选参数，默认为“any” |
| sport | 设置源端口，有效值为 1 至 65535，可以用,分割表示多个端口，或用:分割表示端口段，可选参数，默认为“any” |
| smac | 设置源 MAC 地址，可选参数，默认为“any” |
| da | 设置目的地址，可以使用单个 IP 地址、IP 地址/子网掩码、地址定义、地址组定义、“any”，可选参数，默认为“any” |
| iif | 设置流入网口，可选参数，默认为“any” |
| service | 设置服务，可以使用服务、服务组 |
| proxy | 设置代理服务类型，可以使用预定义代理服务、用户自定义代理服务 |
| time | 设置时间控制，可以使用时间定义、时间组定义、“none”，可选参数，默认为不使用 |

| | |
|---|---|
| | 时间控制 |
| authgroupname | 设置用户组名，对满足条件的数据包所在的连接进行用户认证检查，如果该连接的发起端还没有启动客户端到安全网关上进行认证，则丢弃该包，否则让该包通过 |
| log | 设置日志记录，可选参数，默认为不记录日志 |
| active | 设置是否生效，可选参数，默认为生效 |
| comment | 设置规则注释 |

**注意事项：**

当安全规则的类型为代理时，服务的目的端口必须是单个端口；

当代理服务类型为用户自定义代理服务时，目的地址必须为单个 IP 地址。

**示例：**

```
ac>rule add type proxy name rule3 id 3 sa any da a1 iif any service http proxy http time none log off active on
```

## 添加类型为端口映射的安全规则：

**语法：**

rule add type portmap name <name> [ id <id> ] [ sa { any | <name> | <ip> } ] [ sport <port> ] [ sat { <name> | <ip> | none } ] pa <ip> ia <name> [ iif { any | <interface> } ] [ oif { any | <interface> } ] ps <name> is <name> [ log { on | off } ] [ active { on | off } ] [hideinner { on | off }] [ comment <comment>]

**参数说明：**

| | |
|---|---|
| name | 设置安全规则的名字，必选参数 |
| id | 设置安全规则的序号，有效值为 1 至 65535，可选参数，默认为最后 |
| sa | 设置源地址，可以使用单个 IP 地址、IP 地址/子网掩码、地址定义、地址组定义、“any”，可选参数，默认为“any” |
| sport | 设置源端口，有效值为 1 至 65535，可以用,分割表示多个端口，或用:分割表示端口段，可选参数，默认为“any” |
| sat | 设置源地址转换，可以使用安全网关 IP 地址、地址池定义、“none”，可选参数，默认为不转换 |
| pa | 设置公开地址，仅能使用安全网关 IP 地址 |
| ia | 设置内部地址，仅能服务器地址定义 |
| iif | 设置流入网口，可选参数，默认为“any” |
| oif | 设置流出网口，可选参数，默认为“any”，注意：只有选择源地址转换才能设置流出网口 |
| ps | 设置对外服务，可以使用服务、服务组 |
| is | 设置内部服务，可以使用服务、服务组 |
| log | 设置日志记录，可选参数，默认为不记录日志 |
| active | 设置是否生效，可选参数，默认为生效 |
| hideinner | 是否隐藏内部地址和端口，默认隐藏 |
| comment | 设置规则注释 |

**注意事项：**

对外服务和内部服务必须仅包含类型相同的动态协议、TCP 协议、UDP 协议，且目的端口的数量相同。

**示例：**

```
ac>rule add type portmap name “rule5” id 5 sa any sat sat1 pa 192.168.1.1 ia http_server iif any oif any ps http is http log off active on
```

## 添加类型为允许的端口映射规则：

**语法：**

rule add type portaccept name <name> [ id <id> ] [ sa { any | <name> | <ip> } ] [ sport <port> ] pa <ip> [ iif { any | <interface> } ] ps <name> [ log { on | off } ] [ active { on | off } ] [ comment <comment>]

**参数说明：**

| | |
|---|---|
| name | 设置安全规则的名字，必选参数 |
| id | 设置安全规则的序号，有效值为 1 至 65535，可选参数，默认为最后 |
| sa | 设置源地址，可以使用单个 IP 地址、IP 地址/子网掩码、地址定义、地址组定义、“any”，可选参数，默认为“any” |
| sport | 设置源端口，有效值为 1 至 65535，可以用,分割表示多个端口，或用:分割表示端口段，可选参数，默认为“any” |
| pa | 设置公开地址，仅能使用安全网关 IP 地址 |
| iif | 设置流入网口，可选参数，默认为“any” |
| ps | 设置对外服务，可以使用服务、服务组 |
| is | 设置内部服务，可以使用服务、服务组 |
| log | 设置日志记录，可选参数，默认为不记录日志 |
| active | 设置是否生效，可选参数，默认为生效 |
| comment | 设置规则注释 |

**注意事项：**

**示例：**

```
ac>rule add type portaccept name “rule5” id 5 sa any pa 192.168.1.1 iif any ps http log off active on
```

## 添加类型为 IP 映射的安全规则：

**语法：**

rule add type ipmap name <name> [ id <id> ] [ sa { any | <name> | <ip> } ] [ sat { <name> | <ip> | none } ] pa <ip> ia <name> [ iif { any | <interface> } ] [ oif { any | <interface> } ] [ log { on | off } ] [ active { on | off } ] [hideinner { on | off }] [comment <comment>]

**参数说明：**

| | |
|---|---|
| name | 设置安全规则的名字，必选参数 |
| id | 设置安全规则的序号，有效值为 1 至 65535，可选参数，默认为最后 |

| | |
|---|---|
| sa | 设置源地址，可以使用单个 IP 地址、IP 地址/子网掩码、地址定义、地址组定义、“any”，可选参数，默认为“any” |
| sat | 设置源地址转换，可以使用安全网关 IP 地址、地址池、“none”，可选参数，默认为不转换 |
| pa | 设置公开地址，仅能使用安全网关 IP 地址 |
| ia | 设置内部地址，仅能使用服务器地址定义 |
| iif | 设置流入网口，可选参数，默认为“any” |
| oif | 设置流出网口，可选参数，默认为“any”，注意：只有选择源地址转换才能设置流出网口 |
| log | 设置日志记录，可选参数，默认为不记录日志 |
| active | 设置是否生效，可选参数，默认为生效 |
| hideinner | 是否隐藏内部地址，默认隐藏 |
| comment | 设置规则注释 |

**注意事项：**

无

**示例：**

```
ac>rule add type ipmap name “rule6” id 6 sa any sat sat1 pa 192.168.1.1 ia http_server iif any oif any log off active on
```

## 添加类型为允许的 IP 映射规则：

**语法：**

rule add type ipaccept name <name> [ id <id> ] [ sa { any | <name> | <ip> } ] pa <ip> [ iif { any | <interface> } ] [ log { on | off } ] [ active { on | off } ] [ comment <comment>]

**参数说明：**

| | |
|---|---|
| name | 设置安全规则的名字，必选参数 |
| id | 设置安全规则的序号，有效值为 1 至 65535，可选参数，默认为最后 |
| sa | 设置源地址，可以使用单个 IP 地址、IP 地址/子网掩码、地址定义、地址组定义、“any”，可选参数，默认为“any” |
| pa | 设置公开地址，仅能使用安全网关 IP 地址 |
| iif | 设置流入网口，可选参数，默认为“any” |
| log | 设置日志记录，可选参数，默认为不记录日志 |
| active | 设置是否生效，可选参数，默认为生效 |
| comment | 设置规则注释 |

**注意事项：**

无

**示例：**

```
ac>rule add type ipaccept name “rule6” id 6 sa any pa 192.168.1.1 iif any log off active on
```

## 添加类型为允许的包过滤规则：

**语法：**

rule add type permit name <name> [ id <id> ] [ sa { any | <name> | <ip> } ] [ sport <port> ] [ smac <mac> ] [ da { any | <name> | <ip> } ] [ iif { any | <interface> } ] [ oif { any | <interface> } ] [ service { any | <name> } ] [ time { <name> | none } ] [ dcf <id> ] [ long { <number> | off } ] [ log { on | off } ] [ synflood { <number> | off } ] [ udpflood { <number> | off } ] [ icmpflood { <number> | off } ] [ pingofdeath { on | off } ] [ apc <id> ] [ apc <id> ] [ active { on | off } ] [ comment <comment>]

**参数说明：**

| | |
|---|---|
| name | 设置安全规则的名字，必选参数 |
| id | 设置安全规则的序号，有效值为 1 至 65535，可选参数，默认为最后 |
| sa | 设置源地址，可以使用单个 IP 地址、IP 地址/子网掩码、地址定义、地址组定义、“any”，可选参数，默认为“any” |
| sport | 设置源端口，有效值为 1 至 65535，可以用,分割表示多个端口，或用:分割表示端口段，可选参数，默认为“any” |
| smac | 设置源 MAC 地址，可选参数，默认为“any” |
| da | 设置目的地址，可以使用单个 IP 地址、IP 地址/子网掩码、地址定义、地址组定义、“any”，可选参数，默认为“any” |
| iif | 设置流入网口，可选参数，默认为“any” |
| oif | 设置流出网口，可选参数，默认为“any” |
| service | 设置服务，可以使用服务、服务组、“any”，可选参数，默认为“any” |
| time | 设置时间控制，可以使用时间定义、时间组定义、“none”，可选参数，默认为不使用时间控制 |
| dcf | 修改深度过滤策略，可选参数，默认为“0”。可以选择定义好的深度过滤策略。“id”为“0”，表示不启用深度过滤 |
| long | 设置长连接分钟数，或关掉长连接，0 为不限时, 限时的有效范围是 30-288000 分钟。可选参数，默认为不使用长连接 |
| log | 设置日志记录，可选参数，默认为不记录日志 |
| synflood | 设置抗 Syn Flood 攻击每秒个数，或关掉抗攻击，可选参数，默认为不抗攻击，注意只有服务是 TCP 才能选择此参数 |
| udpflood | 设置抗 UDP Flood 攻击每秒个数，或关掉抗攻击，可选参数，默认为不抗攻击，注意只有服务是 UDP 才能选择此参数 |
| icmpflood | 设置抗 ICMP Flood 攻击每秒个数，或关掉抗攻击，可选参数，默认为不抗攻击，注意只有服务是 ICMP 才能选择此参数 |
| pingofdeath | 设置抗 Ping of Death 攻击开关，可选参数，默认为不抗攻击，注意只有服务是 ICMP 才能选择此参数 |
| apc | 设置应用识别策略 |
| urlblock | 设置 URL 过滤策略 |
| active | 设置是否生效，可选参数，默认为生效 |
| comment | 设置规则注释 |

**注意事项：**

无

**示例：**

```
ac>rule add type permit name “rule1” id 1 sa any da a1 iif any oif any service http time none apc 2 urlblock 2 dcf 0 log off active on
```

## 添加类型为禁止的包过滤规则：

**语法：**

rule add type deny name <name> [ id <id> ] [ sa { any | <name> | <ip> } ] [ sport <port> ] [ smac <mac> ] [ da { any | <name> | <ip> } ] [ iif { any | <interface> } ] [ oif { any | <interface> } ] [ service { any | <name> } ] [ time { <name> | none } ] [ log { on | off } ] [ active { on | off } ] [ comment <comment>]

**参数说明：**

| | |
|---|---|
| name | 设置安全规则的名字，必选参数 |
| id | 设置安全规则的序号，有效值为 1 至 65535，可选参数，默认为最后 |
| sa | 设置源地址，可以使用单个 IP 地址、IP 地址/子网掩码、地址定义、地址组定义、“any”，可选参数，默认为“any” |
| sport | 设置源端口，有效值为 1 至 65535，可以用,分割表示多个端口，或用:分割表示端口段，可选参数，默认为“any” |
| smac | 设置源 MAC 地址，可选参数，默认为“any” |
| da | 设置目的地址，可以使用单个 IP 地址、IP 地址/子网掩码、地址定义、地址组定义、“any”，可选参数，默认为“any” |
| iif | 设置流入网口，可选参数，默认为“any” |
| oif | 设置流出网口，可选参数，默认为“any” |
| service | 设置服务，可以使用服务、服务组、“any”，可选参数，默认为“any” |
| time | 设置时间控制，可以使用时间定义、时间组定义、“none”，可选参数，默认为不使用时间控制 |
| log | 设置日志记录，可选参数，默认为不记录日志 |
| active | 设置是否生效，可选参数，默认为生效 |
| comment | 设置规则注释 |

**注意事项：**

无

**示例：**

```
ac>rule add type deny name “rule2” id 2 sa any da a1 iif any oif any service http time none log off active on
```

## 添加类型为 VPN 的包过滤规则：

**语法：**

rule add type vpn name <name> [ id <id> ] [ sa { any | <name> | <ip> } ] [ sport <port> ] [ smac <mac> ] [ da { any | <name> | <ip> } ] [ iif { any | <interface> } ] [ oif { any | <interface> } ] [ service { any | <name> } ] [ time { <name> | none } ] [ log { on | off } ] [ synflood { <number> | off } ] [ udpflood { <number> | off } ] [ icmpflood { <number> | off } ] [ pingofdeath <on|off> ] [ active { on | off } ] [comment <comment>]

**参数说明：**

| | |
|---|---|
| name | 设置安全规则的名字，必选参数 |
| id | 设置安全规则的序号，有效值为 1 至 65535，可选参数，默认为最后 |
| sa | 设置源地址，可以使用单个 IP 地址、IP 地址/子网掩码、地址定义、地址组定义、“any”，可选参数，默认为“any” |
| sport | 设置源端口，有效值为 1 至 65535，可以用,分割表示多个端口，或用:分割表示端口段，可选参数，默认为“any” |
| smac | 设置源 MAC 地址，可选参数，默认为“any” |
| da | 设置目的地址，可以使用单个 IP 地址、IP 地址/子网掩码、地址定义、地址组定义、“any”，可选参数，默认为“any” |
| iif | 设置流入网口，可选参数，默认为“any” |
| oif | 设置流出网口，可选参数，默认为“any” |
| service | 设置服务，可以使用服务、服务组、“any”，可选参数，默认为“any” |
| time | 设置时间控制，可以使用时间定义、时间组定义、“none”，可选参数，默认为不使用时间控制 |
| log | 设置日志记录，可选参数，默认为不记录日志 |
| synflood | 设置抗 Syn Flood 攻击每秒个数，或关掉抗攻击，可选参数，默认为不抗攻击，注意只有服务是 TCP 才能选择此参数 |
| udpflood | 设置抗 UDP Flood 攻击每秒个数，或关掉抗攻击，可选参数，默认为不抗攻击，注意只有服务是 UDP 才能选择此参数 |
| icmpflood | 设置抗 ICMP Flood 攻击每秒个数，或关掉抗攻击，可选参数，默认为不抗攻击，注意只有服务是 ICMP 才能选择此参数 |
| pingofdeath | 设置抗 Ping of Death 攻击开关，可选参数，默认为不抗攻击，注意只有服务是 ICMP 才能选择此参数 |
| active | 设置是否生效，可选参数，默认为生效 |
| comment | 设置规则注释 |

**注意事项：**

无

**示例：**

```
ac>rule add type vpn name “rule1” id 1 sa any da a1 iif any oif any service http time none log off active on
```

## 添加类型为 NAT 的安全规则：

**语法：**

rule add type nat name <name> [ id <id> ] [ sa { any | <name> | <ip> } ] [ sport <port> ] sat { <name> | <ip> } [ satport <port> ] [ da { any | <name> | <ip> } ] [ oif { any | <interface> } ] [ service { any | <name> } ] [ log { on | off } ] [ active { on | off } ] [ comment <comment>]

**参数说明：**

| | |
|---|---|
| name | 设置安全规则的名字，必选参数 |
| id | 设置安全规则的序号，有效值为 1 至 65535，可选参数，默认为最后 |
| sa | 设置源地址，可以使用单个 IP 地址、IP 地址/子网掩码、地址定义、地址组定义、“any”，可选参数，默认为“any” |
| sport | 设置源端口，有效值为 1 至 65535，可以用,分割表示多个端口，或用:分割表示端口段，可选参数，默认为“any” |
| sat | 设置源地址转换，可以使用安全网关 IP 地址、地址池定义 |
| satport | 设置源端口转换，使用:或-分割 |
| da | 设置目的地址，可以使用单个 IP 地址、IP 地址/子网掩码、地址定义、地址组定义、“any”，可选参数，默认为“any” |
| oif | 设置流出网口，可选参数，默认为“any” |
| service | 设置服务，可以使用服务、服务组、“any”，可选参数，默认为“any” |
| log | 设置日志记录，可选参数，默认为不记录日志 |
| active | 设置是否生效，可选参数，默认为生效 |
| comment | 设置规则注释 |

**注意事项：**

无

**示例：**

```
ac>rule add type nat name “rule4” id 4 sa any sat 192.168.1.1 da a1 oif any service http log off active on
```

## 添加类型为伪装的安全规则：

**语法：**

rule add type masquerade name <name> [ id <id> ] [ sa { any | <name> | <ip> } ] [ sport <port> ] [ satport <port> ] [ da { any | <name> | <ip> } ] oif { any | <interface> } ] [ service { any | <name> } ] [ log { on | off } ] [ active { on | off } ] [ comment <comment>]

**参数说明：**

| | |
|---|---|
| name | 设置安全规则的名字，必选参数 |
| id | 设置安全规则的序号，有效值为 1 至 65535，可选参数，默认为最后 |
| sa | 设置源地址，可以使用单个 IP 地址、IP 地址/子网掩码、地址定义、地址组定义、“any”，可选参数，默认为“any” |
| sport | 设置源端口，有效值为 1 至 65535，可以用,分割表示多个端口，或用:分割表示端口段，可选参数，默认为“any” |

| | |
|---|---|
| sat | 设置源地址转换，可以使用安全网关 IP 地址、地址池定义 |
| satport | 设置源端口转换，使用:或-分割 |
| da | 设置目的地址，可以使用单个 IP 地址、IP 地址/子网掩码、地址定义、地址组定义、“any”，可选参数，默认为“any” |
| oif | 设置流出网口，可选参数，默认为“any” |
| service | 设置服务，可以使用服务、服务组、“any”，可选参数，默认为“any” |
| log | 设置日志记录，可选参数，默认为不记录日志 |
| active | 设置是否生效，可选参数，默认为生效 |
| comment | 设置规则注释 |

**注意事项：**

无

**示例：**

```
ac>rule add type masquerade name “rule4” id 4 sa any sat 192.168.1.1 da a1 oif any service http log off active on
```

## 添加类型为允许的 NAT 规则：

**语法：**

rule add type nataccept name <name> [ id <id> ] [ sa { any | <name> | <ip> } ] [ sport <port> ] [ da { any | <name> | <ip> } ] [ oif { any | <interface> } ] [ service { any | <name> } ] [ log { on | off } ] [ active { on | off } ] [ comment <comment>]

**参数说明：**

| | |
|---|---|
| name | 设置安全规则的名字，必选参数 |
| id | 设置安全规则的序号，有效值为 1 至 65535，可选参数，默认为最后 |
| sa | 设置源地址，可以使用单个 IP 地址、IP 地址/子网掩码、地址定义、地址组定义、“any”，可选参数，默认为“any” |
| sport | 设置源端口，有效值为 1 至 65535，可以用,分割表示多个端口，或用:分割表示端口段，可选参数，默认为“any” |
| da | 设置目的地址，可以使用单个 IP 地址、IP 地址/子网掩码、地址定义、地址组定义、“any”，可选参数，默认为“any” |
| oif | 设置流出网口，可选参数，默认为“any” |
| service | 设置服务，可以使用服务、服务组、“any”，可选参数，默认为“any” |
| log | 设置日志记录，可选参数，默认为不记录日志 |
| active | 设置是否生效，可选参数，默认为生效 |
| comment | 设置规则注释 |

**注意事项：**

无

**示例：**

```
ac>rule add type nataccept name “rule4” id 4 sa any da a1 oif any service http log off
```

active on

## 添加绿色上网规则：

**语法：**

rule add type greennet name <name> [ id <id> ] [ sa { any | <name> | <ip> } ] [ sport <port> ] [ da { any | <name> | <ip> } ] [ iif { any | <interface> } ] [apc <id>] [urlblock <id>] [time <none|name>] [log <on|off>] [ active { on | off } ] [ comment <comment>]

**参数说明：**

| | |
|---|---|
| name | 设置安全规则的名字，必选参数 |
| id | 设置安全规则的序号，有效值为 1 至 65535，可选参数，默认为最后 |
| sa | 设置源地址，可以使用单个 IP 地址、IP 地址/子网掩码、地址定义、地址组定义、“any”，可选参数，默认为“any” |
| sport | 设置源端口，有效值为 1 至 65535，可以用,分割表示多个端口，或用:分割表示端口段，可选参数，默认为“any” |
| da | 设置目的地址，可以使用单个 IP 地址、IP 地址/子网掩码、地址定义、地址组定义、“any”，可选参数，默认为“any” |
| iif | 设置流入网口，可选参数，默认为“any” |
| time | 设置时间控制，可以使用时间定义、时间组定义、“none”，可选参数，默认为不使用时间控制 |
| apc | 设置引用的 apc 策略，填写策略 id |
| urlblock | 设置引用的 url 策略，填写策略 id |
| log | 设置日志记录，可选参数，默认为不记录日志 |
| active | 设置是否生效，可选参数，默认为生效 |
| comment | 设置规则注释 |

**注意事项：**

无

**示例：**

ac> rule add type greennet id 6 name ″gn1″ sa any da any iif eth0 apc 1 urlblock 1 time none active on log on comment ″ss″ sport ″233″

## 添加主动防御规则：

**语法：**

rule add type ips_url_trojan name <name> [ id <id> ] [ sa { any | <name> | <ip> } ] [ sport <port> ] [ da { any | <name> | <ip> } ] [ iif { any | <interface> } ] [ oiif { any | <interface> } ] [ service <>] [ log { on | off } ] [ active { on | off } ] [ comment <comment> ]

**参数说明：**

| | |
|---|---|
| name | 设置安全规则的名字，必选参数 |
| id | 设置安全规则的序号，有效值为 1 至 65535，可选参数，默认为最后 |
| sa | 设置源地址，可以使用单个 IP 地址、IP 地址/子网掩码、地址定义、地址组定义、 |

“any”，可选参数，默认为“any”

sport 设置源端口，有效值为 1 至 65535，可以用,分割表示多个端口，或用:分割表示端口段，可选参数，默认为“any”

da 设置目的地址，可以使用单个 IP 地址、IP 地址/子网掩码、地址定义、地址组定义、“any”，可选参数，默认为“any”

iif 设置流入网口，可选参数，默认为“any”

oif 设置流出网口，可选参数，默认为“any”

service 设置服务，可以使用服务、服务组、“any”，可选参数，默认为“any”

time 设置时间控制，可以使用时间定义、时间组定义、“none”，可选参数，默认为不使用时间控制

log 设置日志记录，可选参数，默认为不记录日志

active 设置是否生效，可选参数，默认为生效

comment 设置规则注释

**注意事项：**

无

**示例：**

```
ac> rule add type ips_url_trojan id 7 name "ad7" sa any da any iif eth0 oif eth1 service http time none active on log off comment "nn" sport "80"
```

## 修改安全规则：

**语法：**

rule set id <id> [ type {proxy | portmap | portaccept | ipmap | ipaccept | permit | deny | auth| vpn | nat | masquerade | nataccept } ] [ name <name> ] [ newid <id> ] [ sa { any | <name> | <ip> } ] [ sat { <name> | <ip> | none } ] [ sport <port> ] [ satport <port> ] [ smac <mac> ] [ da { any | <name> | <ip> } ] [ pa <ip> ] [ ia <name> ] [ iif { any | <interface> } ] [ oif { any | <interface> } ] [ service { any | <name> } ] [ proxy <name> ] [ ps <name> ] [ is <name> ] [ time { <name> | none } ] [ dcf <id> ] [ long { <number> | off } ] [ log { on | off } ] [ synflood { <number> | off } ] [ udpflood { <number> | off } ] [ icmpflood { <number> | off } ] [ pingofdeath { on | off } ] [ apc < id> } ] [ edk <id> ] [ btlog { on | off } ] [ active { on | off } ] [ hideinner { on | off } ] [ comment <comment>]

**参数说明：**

id 指定欲修改的安全规则的序号

type 修改安全规则的类型

name 修改安全规则的名字

newid 修改安全规则的序号，有效值为 1 至 65535

sa 修改源地址，可以使用单个 IP 地址、IP 地址/子网掩码、地址定义、地址组定义、“any”

sat 修改源地址转换，可以使用安全网关 IP 地址、地址池、“none”

sport 设置源端口，有效值为 1 至 65535，可以用,分割表示多个端口，或用:分割表示端口段，可选参数，默认为“any”

satport 设置源端口转换，使用:或-分割

| | |
|---|---|
| smac | 设置源 MAC 地址，可选参数，默认为“any” |
| da | 修改目的地址，可以使用单个 IP 地址、IP 地址/子网掩码、地址定义、地址组定义、“any” |
| pa | 修改公开地址，仅能使用安全网关 IP 地址（不包括 “mng”上的 IP 地址） |
| ia | 修改内部地址，仅能使用服务器地址定义 |
| iif | 修改流入网口，不能使用网络接口 “mng” |
| oif | 修改流出网口，不能使用网络接口 “mng” |
| service | 修改服务，可以使用服务、服务组 |
| proxy | 修改代理服务类型，可以使用预定义代理服务、用户自定义代理服务 |
| ps | 修改对外服务，可以使用服务、服务组 |
| is | 修改内部服务，可以使用服务、服务组 |
| time | 修改时间控制，可以使用时间定义、时间组定义、“none” |
| dcf | 修改深度过滤策略，可选参数，默认为“0”。可以选择定义好的深度过滤策略。“id”为“0”，表示不启用深度过滤 |
| long | 设置长连接分钟数，或关掉长连接，可选参数，默认为不使用长连接 |
| log | 设置日志记录，可选参数，默认为不记录日志 |
| synflood | 设置抗 Syn Flood 攻击每秒个数，或关掉抗攻击，可选参数，默认为不抗攻击，注意只有服务是 TCP 才能选择此参数 |
| udpflood | 设置抗 UDP Flood 攻击每秒个数，或关掉抗攻击，可选参数，默认为不抗攻击，注意只有服务是 UDP 才能选择此参数 |
| icmpflood | 设置抗 ICMP Flood 攻击每秒个数，或关掉抗攻击，可选参数，默认为不抗攻击，注意只有服务是 ICMP 才能选择此参数 |
| pingofdeath | 设置抗 Ping of Death 攻击开关，可选参数，默认为不抗攻击，注意只有服务是 ICMP 才能选择此参数 |
| apc | 设置引用的 apc 策略，填写策略 id |
| urlblock | 设置引用的 urlblock 策略，填写策略 id |
| btlog | 设置是否记录 bt 和 edk 过滤的日志 |
| active | 修改是否生效 |
| hideinner | 设置是否隐藏内部地址和端口 |
| comment | 设置规则注释 |

**注意事项：**

修改安全规则的类型时，仅类型为允许和禁止的安全规则可以互相转换；

某些参数仅能使用在相应类型的安全规则中；

在不同类型的安全规则中，相同的参数可能会有不同的取值要求。

**示例：**

```
ac>rule set id 1 type deny sa any da any iif any oif any service any time none log off
active off
```

## 删除所有安全规则：

**语法：**

rule del all

**参数说明：**
无

**注意事项：**
无

**示例：**
```
ac>rule del all
```

## 删除指定序号的安全规则：

**语法：**
rule del id <id>

**参数说明：**
id 指定欲删除的安全规则的序号

**注意事项：**
无

**示例：**
```
ac>rule del id 1
```

## 显示所有安全规则：

**语法：**
rule show

**参数说明：**
id 指定欲显示的安全规则的序号

**注意事项：**
无

**示例：**
```
ac>rule show id 1
ID  Type     Active
 1  permit   on
 2  deny     off
 3  proxy    on
```

```
 4  nat       on
 5  portmap   on
 6  ipmap     on
```

## 显示指定序号的安全规则：

**语法：**
rule show id <id>

**参数说明：**
无

**注意事项：**
仅显示安全规则的部分内容。

**示例：**

```
ac>rule show id 1
ID: 1
Type: permit
Name: rule 1
Source Address: any
Destination Address: any
Input Interface: any
Output Interface: any
Service: any
Time: none
URL: off
Log: off
Active: on
```

## 更新安全规则：

**语法：**
rule refresh

**参数说明：**
无

**注意事项：**
修改资源定义后，使用此命令可以让安全规则使用修改后的资源定义。

**示例：**

```
ac>rule refresh
```

## 7.1.2 带宽管理（bw）

### 添加带宽管理规则：

**语法：**

```
bw add id <id> name <name> [ sa { any | name | <ip> } ] [ sport { port | none } ]  [ da { any | name | ip } ] [ dport { port | none } ] [ iif { any | interface } ] [ oif { any | <interface> } ] [ time { name | none } ] [ level { 0|1|2|3 } ] [ service { any | name } ] [ bandwidthname <name> ] [ apc { 0 | 512 } ] [ url { 0 | 512 } ] [ file { 0 | 256 } ] [ rate { maxrate | 0 } ] [ mode { dstip | srcip } ] [ autodelbw { 0 | 1 } ] [ active { on | off } ] [comment { comment | none } ]
```

**参数说明：**

| | |
|---|---|
| id | 安全规则的 ID 号，必选参数； |
| name | 设置安全规则的名字，必选参数 |
| sa | 设置源地址，可以使用单个 IP 地址、IP 地址/子网掩码、地址定义、地址组定义、“any”，可选参数，默认为“any” |
| sport | 设置源端口，有效值为 1 至 65535，可以用,分割表示多个端口，或用:分割表示端口段，可选参数，默认为“any” |
| da | 设置目的地址，可以使用单个 IP 地址、IP 地址/子网掩码、地址定义、地址组定义、“any”，可选参数，默认为“any” |
| dport | 设置目的端口，有效值为 1 至 65535，可以用,分割表示多个端口，或用:分割表示端口段，可选参数，默认为“any” |
| iif | 设置流入网口，可选参数，默认为“any” |
| oif | 设置流出网口，可选参数，默认为“any” |
| time | 设置时间控制，可以使用时间定义、时间组定义、“none”，可选参数，默认为不使用时间控制 |
| level | 快捷安全级别 |
| service | 设置服务，可以使用服务、服务组 |
| bandwidthname | 设置带宽定义的名字，该参数只能通过选择资源定义中的带宽管理列表中的定义来设置。 |
| apc | 设置选择的应用识别带宽策略的 id |
| url | 设置选择的 URL 识别带宽策略的 id |
| file | 设置选择的文件类型带宽策略的 id |
| rate | 主机带宽限制速率值 |
| mode | 主机带宽的控制模式 |
| autodelbw | 是否自动删除带宽资源,可选参数； |
| active | 设置是否生效，可选参数，默认为生效 |

comment 设置带宽管理规则的注释，可选参数，默认为空

**示例：**

ac> bw add id 1 name bw1 sa any sport none da any dport none iif any oif any time none service FTP bandwidthname eth0_1000_1000_5 apc 0 url 0 file 0 rate 0 mode srcip level 0 active on comment ''

## 修改带宽管理规则：

**语法：**

bw set id <id> name <name> [ sa { any | name | ip } ] [ sport { port | none } ] [ da { any | name | ip } ] [ dport { port | none } ] [ iif { any | interface } ] [ oif { any | interface } ] [ time { name | none } ] [ level { 0|1|2|3 } ] [ service { any | name } ] [ bandwidthname <name> ] [ apc { 0 | 512 } ] [ url { 0 | 512 } ] [ file { 0 | 256 } ] [ rate { maxrate | 0 } ] [ mode { dstip | srcip } ] [ autodelbw { 0 | 1 } ] [ active { on | off } ] [comment { comment | none } ]

**参数说明：**

| | |
|---|---|
| id | 安全规则的 ID 号，必选参数； |
| name | 设置安全规则的名字，必选参数 |
| sa | 设置源地址，可以使用单个 IP 地址、IP 地址/子网掩码、地址定义、地址组定义、“any”，可选参数，默认为“any” |
| sport | 设置源端口，有效值为 1 至 65535，可以用,分割表示多个端口，或用:分割表示端口段，可选参数，默认为“any” |
| da | 设置目的地址，可以使用单个 IP 地址、IP 地址/子网掩码、地址定义、地址组定义、“any”，可选参数，默认为“any” |
| dport | 设置目的端口，有效值为 1 至 65535，可以用,分割表示多个端口，或用:分割表示端口段，可选参数，默认为“any” |
| iif | 设置流入网口，可选参数，默认为“any” |
| oif | 设置流出网口，可选参数，默认为“any” |
| time | 设置时间控制，可以使用时间定义、时间组定义、“none”，可选参数，默认为不使用时间控制 |
| level | 快捷安全级别 |
| service | 设置服务，可以使用服务、服务组 |
| bandwidthname | 设置带宽定义的名字，该参数只能通过选择资源定义中的带宽管理列表中的定义来设置。 |
| apc | 设置选择的应用识别策略的 id |
| url | 设置选择的 URL 识别带宽策略的 id |
| file | 设置选择的文件类型带宽策略的 id |
| rate | 主机带宽限制速率值 |
| mode | 主机带宽的控制模式 |
| autodelbw | 是否自动删除带宽资源，可选参数； |
| active | 设置规则的状态，on 为启用，off 为禁用。 |

comment 设置带宽管理规则的注释，可选参数，默认为空

**示例：**

ac> bw set id 1 name bw1 sa any sport none da any dport none iif any oif any time none service https bandwidthname eth0_1000_1000_5 apc 0 url 0 file 0 rate 0 mode srcip level 0 active on comment ''

## 删除带宽管理规则：

**语法：**

bw del {id <id>|all}

**参数说明：**

id 安全规则的 ID 号，必选参数；

all 删除所有规则

**注意事项：**

无

**示例：**

ac> bw del id 4

## 显示带宽管理规则：

**语法：**

bw show id <id>

**参数说明：**

id 安全规则的 ID 号，必选参数；

**注意事项：**

无

**示例：**

ac> bw show id 5

## 快速添加带宽资源组：

**语法：**

bw quick_bw oif <interface> minbw <number> maxbw <number> prio <number>

**参数说明：**

oif 配置网口，必选参数；

minbw 配置最小带营帐

maxbw 配置最大带宽
prio 优先级别

**注意事项：**
无
**示例：**
ac> bw quick_bw oif eth0 maxbw 1000 minbw 1000 prio 5

### 一键快速安全级别带宽配置：

**语法：**
bw easyconfig id <1|2|3>

**参数说明：**
id 选择安全级别的 ID 号，必选参数；
**注意事项：**
无
**示例：**
ac> bw easyconfig id 2

# 7.2 代理

## 7.2.1 代理设置

### 是否开启 HTTP 代理：

**语法：**
proxy {on | off} http

**参数说明：**
无

**注意事项：**
无

**示例：**
ac>proxy on http
ac>proxy off http

## 修改 HTTP 代理配置：

**语法：**

proxy set http port <port> [java {permit | deny}] [javascript {permit | deny}] [activex {permit | deny}]

**参数说明：**

port： HTTP 代理端口号
java： 是否允许 java 网页通过
javascript： 是否允许 javascript 网页通过
activex： 是否允许 activex 网页通过

**注意事项：**

修改之前要关闭 HTTP 代理

**示例：**

ac> proxy set http port 80 java permit javascript deny activex permit

## 是否开启 FTP 代理：

**语法：**

proxy {on | off} ftp

**参数说明：**

无

**注意事项：**

无

**示例：**

ac>proxy on ftp
ac>proxy off ftp

## 修改 FTP 代理配置：

**语法：**

proxy set ftp port <port> [get {permit | deny}] [put {permit | deny}] [multi {permit | deny}]

**参数说明：**

port： FTP 代理端口
get： 命令控制，是否允许下载
put： 命令控制，是否允许上传
multi： 是否启用多线程控制

**注意事项：**

修改之前要关闭 FTP 代理

**示例：**
ac>proxy set ftp port 21 get permit put deny multi permit

## 是否开启 TELNET 代理：

**语法：**
proxy {on | off} telnet

**参数说明：**
无

**注意事项：**
无

**示例：**
ac>proxy on telnet
ac>proxy off telnet

## 修改 TELNET 代理配置：

**语法：**
proxy set telnet port <port>

**参数说明：**
port：TELNET 代理端口

**注意事项：**
修改之前要关闭 TELNET 代理

**示例：**
ac>proxy set telnet port 23

## 是否开启 POP3 代理：

**语法：**
proxy {on | off} pop3

**参数说明：**
无

**注意事项：**
无

**示例：**
ac>proxy on pop3
ac>proxy off pop3

## 修改 POP3 代理配置：

**语法：**
proxy set pop3 port <port> [ maxlength <number> ]

**参数说明：**
port： POP3 代理端口
maxlength： 每封邮件最大长度

**注意事项：**
修改之前要关闭 POP3 代理

**示例：**
ac>proxy set pop3 port 110 maxlength 20480

## 是否开启 SOCKS 代理：

**语法：**
proxy {on | off} socks

**参数说明：**
无

**注意事项：**
无

**示例：**
ac>proxy on socks
ac>proxy off socks

## 修改 SOCKS 代理配置：

**语法：**
proxy set socks port <port>

**参数说明：**
port：SOCKS 代理端口

**注意事项：**

修改之前要关闭 SOCKS 代理

**示例：**
ac>proxy set socks port 1080

## 是否开启 DNS 代理：

**语法：**
proxy {on | off} dns

**参数说明：**
无

**注意事项：**
无

**示例：**
ac>proxy on dns
ac>proxy off dns

## 修改 DNS 代理配置：

**语法：**
proxy set dns dnsserver <ip>

**参数说明：**
dnsserver：DNS 代理服务器 IP 地址，多个用英文逗号分隔

**注意事项：**
修改之前要关闭 DNS 代理

**示例：**
ac>proxy set dns dnsserver 1.2.3.4,1.2.3.5

## 显示默认代理配置：

**语法：**
proxy show default

**参数说明：**
无

**注意事项：**
无

**示例：**
ac>proxy show default

## 添加用户自定义代理：

**语法：**
proxy add custom <name> port <port>

**参数说明：**
custom：用户自定义代理名称
port： 用户自定义代理端口

**注意事项：**
只支持 TCP 一种类型

**示例：**
ac>proxy add custom “cusproxy” port 5080

## 删除用户自定义代理：

**语法：**
proxy del custom <name>

**参数说明：**
custom：用户自定义代理名称

**注意事项：**
无

**示例：**
ac> proxy del custom “cusproxy”

## 启用用户自定义代理：

**语法：**
proxy on custom <name>

**参数说明：**
custom：用户自定义代理名称

**注意事项：**
无

**示例：**
ac> proxy on custom “cusproxy”

## 关闭用户自定义代理：

**语法：**
proxy off custom <name>

**参数说明：**
custom：用户自定义代理名称

**注意事项：**
无

**示例：**
ac> proxy off custom “cusproxy”

## 显示用户自定义代理：

**语法：**
proxy show custom

**参数说明：**
无

**注意事项：**
无

**示例：**
ac>proxy show custom

# 7.2.2 代理规则

详见：流量管理∗策略∗rule(安全策略)→
添加类型为代理的安全规则：
修改安全规则：
删除指定序号的安全规则：
显示指定序号的安全规则：
更新安全规则：

# 7.3 地址

## 7.3.1 地址（address）

### 添加地址定义：

**语法：**
address add name <name> ip <ip> [ comment <comment> ]

**参数说明：**

| | |
|---|---|
| name | 设置地址定义的名字 |
| ip | 设置 IP 地址，可以使用单个 IP 地址、IP 地址/子网掩码、IP 地址段、或反 IP 地址/子网掩码 |
| comment | 设置地址定义的注释，可选参数，默认为空 |

**注意事项：**
ip 地址段的格式为：ip1:ip2 如：1.1.1.1:1.1.1.3
ip 地址/子网掩码格式为：ip1/mask 如：1.1.1.1/255.255.255.0
反 ip 地址/子网掩码格式为：ip1~mask 如：1.1.1.1~255.255.255.0
**示例：**
ac>address add name a1 ip 192.168.1.1 comment “address 1”

### 修改地址定义：

**语法：**
address set name <name> { [ ip <ip> ] [ comment <comment> ] }

**参数说明：**

| | |
|---|---|
| name | 设置地址定义的名字 |
| ip | 设置 IP 地址，可以使用单个 IP 地址、IP 地址/子网掩码、IP 地址段、或反 IP 地址/子网掩码 |
| comment | 设置地址定义的注释，可选参数，默认为空 |

**注意事项：**
无

**示例：**
ac>address set name a1 ip 192.168.1.0/255.255.255.0 comment “new address 1”

### 删除地址定义：

**语法：**
address del name <name>

**参数说明：**
name 指定欲删除的地址定义的名字

**注意事项：**
不能删除被安全规则或用户、用户组引用的地址定义，也不能删除作为地址组的成员的地址定义。

**示例：**
```
ac>address del name a1
```

## 显示所有地址定义：

**语法：**
address show

**参数说明：**
无

**注意事项：**
仅显示地址定义的部分内容。

**示例：**
```
ac>address show
名字                    ip 地址
a1                      192.168.1.1/255.255.255.255
```

## 显示指定名字的地址定义：

**语法：**
address show name <name>

**参数说明：**
name 指定欲显示的地址定义的名字

**注意事项：**
无

**示例：**
```
ac>address show name a1
```

名字：a1
IP 地址：192.168.1.1/255.255.255.255
备注：address 1

### 7.3.2 地址组（addrgrp）

## 添加地址组定义：

**语法：**
addrgrp add name <name> [ comment <comment> ]

**参数说明：**
name 设置地址组定义的名字
comment 设置地址组定义的注释，可选参数，默认为空

**注意事项：**
无

**示例：**
ac>addrgrp add name ag1 comment “address group 1”

## 修改地址组定义：

**语法：**
addrgrp set name <name> comment <comment>

**参数说明：**
name 指定欲修改的地址组定义的名字
comment 修改地址组定义的注释

**注意事项：**
无

**示例：**
ac>addrgrp set name ag1 comment “new address group 1”

## 向地址组添加成员：

**语法：**

addrgrp set name <name> addmbr <name>+

**参数说明：**

| | |
|---|---|
| name | 指定欲添加成员的地址组定义的名字 |
| addmbr | 指定一个或多个地址定义的名字，将它们添加到地址组中 |

**注意事项：**

地址组定义的成员只能是地址定义，不能是其它地址组定义。

**示例：**

```
ac>addrgrp set name ag1 addmbr a1 a2 a3
```

## 从地址组删除成员：

**语法：**

addrgrp set name <name> delmbr <name>+

**参数说明：**

| | |
|---|---|
| name | 指定欲删除成员的地址组定义的名字 |
| delmbr | 指定一个或多个地址定义的名字，将它们从地址组中删除 |

**注意事项：**

无

**示例：**

```
ac>addrgrp set name ag1 delmbr a1 a2 a3
```

## 删除地址组定义：

**语法：**

addrgrp del name <name>

**参数说明：**

| | |
|---|---|
| name | 指定欲删除的地址组定义的名字 |

**注意事项：**

不能删除被安全规则或用户、用户组引用的地址组定义。

**示例：**

```
ac>addrgrp del name ag1
```

## 显示所有地址组定义：

**语法：**
addrgrp show

**参数说明：**
无

**注意事项：**
仅显示地址组定义的部分内容。

**示例：**
```
ac>addrgrp show
Name                    Member
ag1                     a1
                        a2
                        a3
```

## 显示指定名字的地址组定义：

**语法：**
addrgrp show name <name>

**参数说明：**
name　　指定欲显示的地址组定义的名字

**注意事项：**
无

**示例：**
```
ac>addrgrp show name ag1
名字：ag1
成员：a1
        a2
        a3
描述：address group 1
```

### 7.3.3 地址池（sataddr）

## 添加地址池定义：

**语法：**

sataddr add name <name> ip <ip> [ comment <comment> ]

**参数说明：**

| | |
|---|---|
| name | 设置地址池定义的名字 |
| ip | 设置地址池定义的 IP 地址，仅能使用 IP 地址段 |
| comment | 设置地址池定义的注释，可选参数，默认为空 |

**注意事项：**

每个地址池定义中的 IP 地址数量不能超过 254 个。

**示例：**

```
ac>sataddr add name sat1 ip 192.168.1.10:192.168.1.20 comment “SAT address 1”
```

## 修改地址池定义：

**语法：**

sataddr set name <name> { [ ip <ip> ] [ comment <comment> ] }

**参数说明：**

| | |
|---|---|
| name | 指定欲修改的地址池定义的名字 |
| ip | 修改地址池定义的 IP 地址，仅能使用 IP 地址段 |
| comment | 修改地址池定义的注释 |

**注意事项：**

每个地址池定义中的 IP 地址数量不能超过 254 个。

**示例：**

```
ac>sataddr set name sat1 ip 192.168.1.30:192.168.1.40 comment “new SAT address 1”
```

## 删除地址池定义：

**语法：**

sataddr del name <name>

**参数说明：**

| | |
|---|---|
| name | 指定欲删除的地址池定义的名字 |

**注意事项：**

不能删除被安全规则引用的地址池定义。

**示例：**

```
ac>sataddr del name sat1
```

## 显示所有地址池定义：

**语法：**

sataddr show

**参数说明：**

无

**注意事项：**

仅显示地址池定义的部分内容。

**示例：**

```
ac>sataddr show
名称                    IP 地址
sat1                    192.168.1.10:192.168.1.20
```

## 显示指定名字的地址池定义：

**语法：**

sataddr show name <name>

**参数说明：**

| | |
|---|---|
| name | 指定欲显示的地址池定义的名字 |

**注意事项：**

无

**示例：**

```
ac>sataddr show name sat1
名称: sat1
IP 地址: 192.168.1.10:192.168.1.20
描述: SAT address 1
```

### 7.3.4 服务器地址（serveraddr）

## 添加服务器地址定义：

**语法：**

serveraddr add name <name> ip <ip> [ ip <ip> [ ip <ip> [ ip <ip> [ ip <ip> [ ip <ip> [ ip <ip> [ ip <ip> ] ] ] ] ] ] ] [ comment <comment> ]

**参数说明：**

| | |
|---|---|
| name | 设置服务器地址定义的名字 |
| ip | 设置服务器 1 的 IP 地址，仅能使用单个 IP 地址 |
| ip | 设置服务器 2 的 IP 地址，仅能使用单个 IP 地址，可选参数，默认为空 |
| ip | 设置服务器 3 的 IP 地址，仅能使用单个 IP 地址，可选参数，默认为空 |
| ip | 设置服务器 4 的 IP 地址，仅能使用单个 IP 地址，可选参数，默认为空 |
| ip | 设置服务器 5 的 IP 地址，仅能使用单个 IP 地址，可选参数，默认为空 |
| ip | 设置服务器 6 的 IP 地址，仅能使用单个 IP 地址，可选参数，默认为空 |
| ip | 设置服务器 7 的 IP 地址，仅能使用单个 IP 地址，可选参数，默认为空 |
| ip | 设置服务器 8 的 IP 地址，仅能使用单个 IP 地址，可选参数，默认为空 |
| comment | 设置服务器地址定义的注释，可选参数，默认为空 |

**注意事项：**

无

**示例：**

```
ac>serveraddr add name sa1 ip 192.168.100.1 ip 192.168.100.2 comment “server address 1”
```

## 修改服务器地址定义：

**语法：**

serveraddr set name <name> { [ ip <ip> [ ip <ip> [ ip <ip> [ ip <ip> [ ip <ip> [ ip <ip> [ ip <ip> [ ip <ip> ] ] ] ] ] ] ] ] [ comment <comment> ] }

**参数说明：**

| | |
|---|---|
| name | 指定欲修改的服务器地址定义的名字 |
| ip | 设置服务器 1 的 IP 地址，仅能使用单个 IP 地址 |
| ip | 设置服务器 2 的 IP 地址，仅能使用单个 IP 地址，可选参数，默认为空 |
| ip | 设置服务器 3 的 IP 地址，仅能使用单个 IP 地址，可选参数，默认为空 |
| ip | 设置服务器 4 的 IP 地址，仅能使用单个 IP 地址，可选参数，默认为空 |
| ip | 设置服务器 5 的 IP 地址，仅能使用单个 IP 地址，可选参数，默认为空 |
| ip | 设置服务器 6 的 IP 地址，仅能使用单个 IP 地址，可选参数，默认为空 |
| ip | 设置服务器 7 的 IP 地址，仅能使用单个 IP 地址，可选参数，默认为空 |
| ip | 设置服务器 8 的 IP 地址，仅能使用单个 IP 地址，可选参数，默认为空 |
| comment | 修改服务器地址定义的注释 |

**注意事项：**

无

**示例：**

```
ac>serveraddr set name sa1 ip 192.168.100.1 ip 192.168.100.2 comment “new server address 1”
```

## 删除服务器地址定义：

**语法：**

serveraddr del name <name>

**参数说明：**

| | |
|---|---|
| name | 指定欲删除的服务器地址定义的名字 |

**注意事项：**

不能删除被安全规则引用的服务器地址定义。

**示例：**

```
ac>serveraddr del name sa1
```

## 显示所有服务器地址定义：

**语法：**

serveraddr show

**参数说明：**

无

**注意事项：**

仅能显示服务器地址定义的部分内容。

**示例：**

```
ac>serveraddr show
名称                    IP 地址
sa1                     192.168.100.1
                        192.168.100.2
```

## 显示指定名字的服务器地址定义：

**语法：**

serveraddr show name <name>

**参数说明：**

name 指定欲显示的服务器地址定义的名字

**注意事项：**
无

**示例：**
```
ac>serveraddr show name sa1
名称：sa1
IP 1：192.168.100.1
IP2：192.168.100.2
描述：server address 1
```

### 7.3.5 域名地址（domain）

## 添加域名地址定义

**语法：**
domain add name <name> [ domain { <string> | none } ] [ auto_resolve {on|off} ] [ primary_dns { <ip> | none } ] [ slave_dns { <ip> | none } ] [ record_type {a|mx|all} ] [ max_record <number>] [ interval <number> ] [ expire <number> ] [ ip_type { static|dynamic } ] [ ip { <string>|none } ] [ comment { <comment> | none } ]

**参数说明：**
name 域名地址名称
domain 域名
auto_resolve 是否开启自动解析
primary_dns 主 DNS 服务器
slave_dns 次 DNS 服务器
record_type 解析类型，A：解析 DNS 的 A 记录（主机记录）；MX：解析 DNS 的 MX 记录（邮件交换记录）；ALL：解析所有的 DNS 记录
max_record 最大解析记录，一个域名可以对应的静态 IP 地址和动态 IP 地址的最大数目，如果超出这个值，动态解析的 IP 地址会自动删除最旧的地址，最大解析记录必须在 1-128 之间
interval 解析间隔，间隔必须在 1-525600 之间
expire 自动解析记录超时时间，是解析间隔的倍数，超时时间必须在 1-525600 之间
ip_type IP 地址的类型
ip IP 地址，是一个逗号分隔的 IP 地址列表
comment 注释

**注意事项：**
此命令可以添加域名地址，也可以向已存在的域名地址中添加 IP 地址。

**示例：**
ac>domain add name sohu domain www.sohu.com auto_resolve on

## 修改域名地址定义

**语法：**

domain set name <name> [ domain { <string> | none } ] [ auto_resolve {on|off} ] [ primary_dns { <ip> | none } ] [ slave_dns { <ip> | none } ] [ record_type {a|mx|all} ] [ max_record <number>] [ interval <number> ] [ expire <number> ] [ ip_type { static|dynamic } ] [ ip { <string>|none } ] [ comment { <comment> | none } ]

**参数说明：**

name 域名地址名称

domain 域名

auto_resolve 是否开启自动解析

primary_dns 主 DNS 服务器

slave_dns 次 DNS 服务器

record_type 解析类型，A：解析 DNS 的 A 记录（主机记录）；MX：解析 DNS 的 MX 记录（邮件交换记录）；ALL：解析所有的 DNS 记录

max_record 最大解析记录，一个域名可以对应的静态 IP 地址和动态 IP 地址的最大数目，如果超出这个值，动态解析的 IP 地址会自动删除最旧的地址，最大解析记录必须在 1-128 之间

interval 解析间隔，间隔必须在 1-525600 之间

expire 自动解析记录超时时间，是解析间隔的倍数，超时时间必须在 1-525600 之间

ip_type IP 地址的类型

ip IP 地址，是一个逗号分隔的 IP 地址列表

comment 注释

**注意事项：**

无

**示例：**

ac> domain set name sohu max_record 10

## 删除域名地址定义

**语法：**

domain del name <name> [ ip <string> ]

**参数说明：**

name 域名地址名次

ip IP 地址，是一个逗号分隔的 IP 地址列表

**注意事项：**

此命令可以删除域名地址也可以删除域名地址中的 IP 地址

**示例：**

ac> domain del name sohu

## 显示域名地址定义

**语法：**

domain show [ name <name> ]

**参数说明：**

name 域名地址名称

**注意事项：**
此命令可以显示所有域名地址，也可以显示单个域名地址

**示例：**
ac> domain show
ID 名称 域名 自动解析 首选 dns 备用 dns
1 sina www.sina.com.cn on
2 www.163.com www.163.com on
3 ebay www.ebay.com on
4 msn www.msn.com on
5 yahoo www.yahoo.com on
6 www.sohu.com www.sohu.com on
7 china www.china.com on
8 taobao www.taobao.com on
9 aol www.aol.com on
10 test www.test.com off
注意: 执行成功

### 刷新域名地址

**语法：**
domain refresh name <name>
**参数说明：**
name 域名地址名称
**注意事项：**
无

**示例：**
ac> domain refresh name sohu

## 7.4 服务

### 7.4.1 服务组（servgrp）

### 添加服务组定义：

**语法：**
servgrp add name <name> [ comment <comment> ]

**参数说明：**
name 设置服务组定义的名字

comment 设置服务组定义的注释，可选参数，默认为空

**注意事项：**
无

**示例：**
ac>servgrp add name sg1 comment “service group 1”

## 修改服务组定义：

**语法：**
servgrp set name <name> comment <comment>

**参数说明：**
name 指定欲修改的服务组定义的名字
comment 修改服务组定义的注释

**注意事项：**
无

**示例：**
ac>servgrp set name sg1 comment “new service group 1”

## 向服务组添加成员：

**语法：**
servgrp set name <name> addmbr <name>+

**参数说明：**
name 指定欲添加成员的服务组定义的名字
addmbr 指定一个或多个服务定义的名字，将它们添加到服务组中

**注意事项：**
服务组定义的成员只能是服务定义，不能是其它服务组定义。

**示例：**
ac>servgrp set name sg1 addmbr s1 s2 s3

## 从服务组删除成员：

**语法：**

servgrp set name <name> delmbr <name>+

**参数说明：**

| | |
|---|---|
| name | 指定欲删除成员的服务组定义的名字 |
| delmbr | 指定一个或多个服务定义的名字，将它们从服务组中删除 |

**注意事项：**

无

**示例：**

```
ac>servgrp set name sg1 delmbr s1 s2 s3
```

## 删除服务组定义：

**语法：**

servgrp del name <name>

**参数说明：**

| | |
|---|---|
| name | 指定欲删除的服务组定义的名字 |

**注意事项：**

不能删除被安全规则或用户、用户组引用的服务组定义。

**示例：**

```
ac>addrgrp del name ag1
```

## 显示所有服务组定义：

**语法：**

servgrp show

**参数说明：**

无

**注意事项：**

仅显示服务组定义的部分内容。

**示例：**

```
ac>servgrp show
名称                    成员
sg1                     s1
                        s2
```

s3

### 显示指定名字的服务组定义：

**语法：**
servgrp show name <name>

**参数说明：**
name 指定欲显示的服务组定义的名字

**注意事项：**
无

**示例：**
ac>servgrp show name sg1
名称: sg1
成员: s1
s2
s3
描述: service group 1

## 7.4.2 服务（service）

### 添加动态协议的服务定义：

**语法：**
service add name <name> protocol <dynamic_service> port <port> [ comment <comment> ]

**参数说明：**
name 设置服务定义的名字
protocol 动态协议类型，可以是 ftp，h323，tns, tftp，irc，rstp，mms， xdmcp,h323_gk,sip
port 设置动态协议的端口
comment 设置服务定义的注释，可选参数，默认为空

**注意事项：**
无

**示例：**
ac>service add name ftp_1 protocol ftp port 21 comment “FTP 1”

## 添加 ICMP 协议的服务定义：

**语法：**

service add name <name> protocol icmp [ type { 0 | 3 [ code { 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | any } ] | 4 | 5 [ code { 0 | 1 | 2 | 3 | any } ] | 8 | 9 | 10 | 11 [ code { 0 | 1 | any } ] | 12 [ code { 0 | 1 | any } ] | 13 | 14 | 17 | 18 | any } ] [ comment <comment> ]

**参数说明：**

| | |
|---|---|
| name | 设置服务定义的名字 |
| type | 设置 ICMP 协议的类型，可选参数，默认为“any” |
| code | 设置 ICMP 协议的 code，可选参数，默认为“any” |
| comment | 设置服务定义的注释，可选参数，默认为空 |

**注意事项：**

无

**示例：**

```
ac>service add name icmp1 protocol icmp type 3 code 10
```

## 添加基本服务：

**语法：**

service add name <name> protocol { { tcp | udp } sp <port> dp <port> | <number> } [ protocol { { tcp | udp } sp <port> dp <port> | <number> } [ protocol { { tcp | udp } sp <port> dp <port> | <number> } [ protocol { { tcp | udp } sp <port> dp <port> | <number> } [ protocol { { tcp | udp } sp <port> dp <port> | <number> } [ protocol { { tcp | udp } sp <port> dp <port> | <number> } [ protocol { { tcp | udp } sp <port> dp <port> | <number> } [ protocol { { tcp | udp } sp <port> dp <port> | <number> } ] ] ] ] ] ] ] [ comment <comment> ]

**参数说明：**

| | |
|---|---|
| name | 设置服务定义的名字 |
| protocol | 设置服务项的协议号，可以使用“TCP”、“UDP”、数字（不能为 1、6、17） |
| sp | 当服务项的协议号为“TCP”或“UDP”时，设置源端口，可以使用单个端口、端口段、“any”。端口的范围为 0~65535。 |
| dp | 当服务项的协议号为“TCP”或“UDP”时，设置目的端口，可以使用单个端口、端口段、“any”。端口的范围为 0~65535。 |
| comment | 设置服务定义的注释，可选参数，默认为空 |

**注意事项：**

在一个普通 IP 协议的服务定义中最多可以设置 8 个服务项。

**示例：**

```
ac>service add name base1 protocol tcp sp 1:3 dp 2:2 comment “base service”
```

## 修改动态协议的服务定义：

**语法：**

service set name <name> protocol <protocol> port <port>

**参数说明：**

| | |
|---|---|
| name | 指定欲修改的服务定义的名字 |
| protocol | 动态协议类型，可以是 ftp，h323，tns, tftp，irc，rstp，mms， xdmcp,h323_gk,sip |
| port | 修改动态协议的端口 |

**注意事项：**

无

**示例：**

```
ac>service set name sqlnet_1 protocol tns port 15210
```

## 修改 ICMP 协议的服务定义：

**语法：**

service set name <name> protocol icmp [ type { 0 | 3 [ code { 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 9 | 10 | 11 | 12 | 13 | 14 | 15 } ] | 4 | 5 [ code { 0 | 1 | 2 | 3 } ] | 8 | 9 | 10 | 11 [ code { 0 | 1 } ] | 12 [ code { 0 | 1 } ] | 13 | 14 | 17 | 18 } ]

**参数说明：**

| | |
|---|---|
| name | 指定欲修改的服务定义的名字 |
| type | 修改 ICMP 协议的类型 |
| code | 修改 ICMP 协议的 code |

**注意事项：**

无

**示例：**

```
ac>service set name icmp1 protocol icmp type 5 code 2
```

## 修改基本协议的服务定义：

**语法：**

service set name <name> protocol { { tcp | udp } sp <port> dp <port> | <number> } [ protocol { { tcp | udp } sp <port> dp <port> | <number> } [ protocol { { tcp | udp } sp <port> dp <port> | <number> } [ protocol { { tcp | udp } sp <port> dp <port> | <number> } [ protocol { { tcp | udp } sp <port> dp <port> | <number> } [ protocol { { tcp | udp } sp <port> dp <port> | <number> } [ protocol { { tcp | udp } sp <port> dp <port> | <number> } [ protocol { { tcp | udp } sp <port> dp <port> | <number> } ] ] ] ] ] ] ]

**参数说明：**

| | |
|---|---|
| name | 指定欲修改的服务定义的名字 |
| protocol | 设置服务项的协议号，可以使用“TCP”、“UDP”、数字（不能为 1、6、17） |

| | |
|---|---|
| sp | 当服务项的协议号为“TCP”或“UDP”时，设置源端口，可以使用单个端口、端口段、“any”。端口的范围为 0~65535。 |
| dp | 当服务项的协议号为“TCP”或“UDP”时，设置目的端口，可以使用单个端口、端口段、“any”。端口的范围为 0~65535。 |

**注意事项：**

在一个普通 IP 协议的服务定义中最多可以设置 8 个服务项。

**示例：**

```
ac>service set name common1 protocol 20 protocol udp sp 3000 dp any protocol tcp sp any dp 4000
```

## 修改服务定义的注释：

**语法：**

service set name <name> comment <comment>

**参数说明：**

| | |
|---|---|
| name | 指定欲修改的服务定义的名字 |
| comment | 修改服务定义的注释 |

**示例：**

```
ac>service set name icmp1 comment “new icmp 1”
```

## 删除服务定义：

**语法：**

service del name <name>

**参数说明：**

| | |
|---|---|
| name | 指定欲删除的服务定义的名字 |

**注意事项：**

不能删除被安全规则或用户、用户组引用的服务定义，也不能删除作为服务组的成员的服务定义。

**示例：**

```
ac>service del name common1
```

## 显示动态协议的服务定义：

**语法：**

service show dynamic

**注意事项：**

仅显示服务定义的部分内容。

**示例：**

```
ac>service show dynamic
```

## 显示 ICMP 协议的服务定义：

**语法：**

service show icmp

**注意事项：**

仅显示服务定义的部分内容。

**示例：**

```
ac>service show icmp
```

## 显示基本协议的服务定义：

**语法：**

service show common

**注意事项：**

仅显示服务定义的部分内容。

**示例：**

```
ac>service show common
```

## 显示指定名字的服务定义：

**语法：**

service show name <name>

**参数说明：**

| | |
|---|---|
| name | 指定欲显示的服务定义的名字 |

**注意事项：**

无

**示例：**

```
ac>service show name ftp_1
```

## 显示预定义服务定义：

**语法：**

service show default

**参数说明：**

无

**注意事项：**

无

**示例：**

```
ac>service show default
```

### 初始化动态协议模块：

**语法：**

service refresh

**参数说明：**

无

**注意事项：**

此功能目的是使当前的所有动态协议重新生效，以反应最新的改动。

**示例：**

```
ac> service refresh
```

## 7.5 时间

### 7.5.1 时间（time）

### 添加一次性时间定义：

**语法：**

time add name <name> type once start <date> <time> stop <date> <time> [ comment <comment> ]

**参数说明：**

| | |
|---|---|
| name | 指定时间定义的名字 |
| start | 指定开始时间，格式为 yyyy/mm/dd hh:mm:ss |
| stop | 指定结束时间，格式为 yyyy/mm/dd hh:mm:ss |
| comment | 指定时间定义的注释，可选参数，默认为空 |

**注意事项：**

开始时间必须早于结束时间。

**示例：**

```
ac>time add name t1 type once start 2004/01/01 09:00:00 stop 2004/01/01 12:00:00 comment
```

“time 1”

## 添加周循环时间定义：

**语法：**

time add name <name> type week { [ sun <time> ] [ mon <time> ] [ tue <time> ] [ wed <time> ] [ thu <time> ] [fri <time> ] [ sat <time> ] } [ comment <comment> ]

**参数说明：**

| | |
|---|---|
| name | 指定时间定义的名字 |
| sun | 指定周日的时间段，格式为 hh:mm:ss-hh:mm:ss 或 hh:mm-hh:mm |
| mon | 指定周一的时间段，格式为 hh:mm:ss-hh:mm:ss 或 hh:mm-hh:mm |
| tue | 指定周二的时间段，格式为 hh:mm:ss-hh:mm:ss 或 hh:mm-hh:mm |
| wed | 指定周三的时间段，格式为 hh:mm:ss-hh:mm:ss 或 hh:mm-hh:mm |
| thu | 指定周四的时间段，格式为 hh:mm:ss-hh:mm:ss 或 hh:mm-hh:mm |
| fri | 指定周五的时间段，格式为 hh:mm:ss-hh:mm:ss 或 hh:mm-hh:mm |
| sat | 指定周六的时间段，格式为 hh:mm:ss-hh:mm:ss 或 hh:mm-hh:mm |
| comment | 指定时间定义的注释，可选参数，默认为空 |

**注意事项：**

无

**示例：**

ac>time add name t2 type week mon 09:00-18:00 tue 09:00-18:00 wed 09:00-18:00 thu 09:00-18:00 fri 09:00-18:00 comment “work time”

## 修改一次性时间定义：

**语法：**

time set name <name> type once { [ start <date> <time> stop <date> <time> ] [ comment <comment>] }

**参数说明：**

| | |
|---|---|
| name | 指定欲修改的时间定义的名字 |
| start | 指定开始时间，格式为 yyyy/mm/dd hh:mm:ss |
| stop | 指定结束时间，格式为 yyyy/mm/dd hh:mm:ss |
| comment | 修改时间定义的注释 |

**注意事项：**

开始时间必须早于结束时间。

**示例：**

ac>time set name t1 type once start 2004/01/01 14:00:00 stop 2004/01/01 18:00:00 comment “new time 1”

## 修改周循环时间定义：

**语法：**

time set name <name> type week { [ sun <time> ] [ mon <time> ] [ tue <time> ] [ wed <time> ] [ thu <time> ] [fri <time> ] [ sat <time> ] [ comment <comment> ] }

**参数说明：**

| | |
|---|---|
| name | 指定欲修改的时间定义的名字 |
| sun | 指定周日的时间段，格式为 hh:mm:ss-hh:mm:ss 或 hh:mm-hh:mm |
| mon | 指定周一的时间段，格式为 hh:mm:ss-hh:mm:ss 或 hh:mm-hh:mm |
| tue | 指定周二的时间段，格式为 hh:mm:ss-hh:mm:ss 或 hh:mm-hh:mm |
| wed | 指定周三的时间段，格式为 hh:mm:ss-hh:mm:ss 或 hh:mm-hh:mm |
| thu | 指定周四的时间段，格式为 hh:mm:ss-hh:mm:ss 或 hh:mm-hh:mm |
| fri | 指定周五的时间段，格式为 hh:mm:ss-hh:mm:ss 或 hh:mm-hh:mm |
| sat | 指定周六的时间段，格式为 hh:mm:ss-hh:mm:ss 或 hh:mm-hh:mm |
| comment | 修改时间定义的注释 |

**注意事项：**

未指定时间段的日子将会被清空。

**示例：**

```
ac>time add name t2 type week mon 09:00-18:00 tue 09:00-18:00 wed 09:00-18:00 thu 09:00-18:00 fri 09:00-18:00 comment “work time”
```

## 删除时间定义：

**语法：**

time del name <name>

**参数说明：**

| | |
|---|---|
| name | 指定欲删除的时间定义的名字 |

**注意事项：**

不能删除被安全规则或用户、用户组引用的时间定义，也不能删除作为时间组的成员的时间定义。

**示例：**

```
ac>time del name t1
```

## 显示所有时间定义：

**语法：**

time show

**注意事项：**

仅显示时间定义的部分内容。

**示例：**

```
ac>time show
Name                    Type
t1                      once
t2                      week
```

## 显示指定名字的时间定义：

**语法：**

time show name <name>

**参数说明：**

name 指定欲显示的时间定义的名字

**注意事项：**

无

**示例：**

```
ac>time show name t1
Name: t1
Type: once
Start Time: 2004/01/01 09:00:00
Stop Time: 2004/01/01 12:00:00
Comment: time 1

ac>time show name t2
Name: t2
Type: week
Sunday:
Monday: 09:00:00-18:00:00
Tuesday: 09:00:00-18:00:00
Wednesday: 09:00:00-18:00:00
Thursday: 09:00:00-18:00:00
Friday: 09:00:00-18:00:00
Saturday:
Comment: work time
```

# 7.5.2 时间组（timegrp）

## 添加时间组定义：

**语法：**

timegrp add name <name> [ comment <comment> ]

**参数说明：**

| | |
|---|---|
| name | 设置时间组定义的名字 |
| comment | 设置时间组定义的注释，可选参数，默认为空 |

**注意事项：**

无

**示例：**

```
ac>timegrp add name tg1 comment “time group 1”
```

## 修改时间组定义：

**语法：**

timegrp set name <name> comment <comment>

**参数说明：**

| | |
|---|---|
| name | 指定欲修改的时间组定义的名字 |
| comment | 修改时间组定义的注释 |

**注意事项：**

无

**示例：**

```
ac>timegrp set name tg1 comment “new time group 1”
```

## 向时间组添加成员：

**语法：**

timegrp set name <name> addmbr <name>+

**参数说明：**

| | |
|---|---|
| name | 指定欲添加成员的时间组定义的名字 |
| addmbr | 指定一个或多个时间定义的名字，将它们添加到时间组中 |

**注意事项：**

无

**注意事项：**

时间组定义的成员只能是时间定义，不能是其它时间组定义。

**示例：**

```
ac>timegrp set name tg1 addmbr t1 t2 t3
```

## 从时间组删除成员：

**语法：**

timegrp set name <name> delmbr <name>+

**参数说明：**

| | |
|---|---|
| name | 指定欲删除成员的时间组定义的名字 |
| delmbr | 指定一个或多个时间定义的名字，将它们从时间组中删除 |

**注意事项：**

无

**示例：**

```
ac>timegrp set name tg1 delmbr t1 t2 t3
```

## 从时间组删除所有成员：

**语法：**

timegrp set name <name> delallmbr

**参数说明：**

| | |
|---|---|
| name | 指定欲删除成员的时间组定义的名字 |

**注意事项：**

无

**示例：**

```
ac>timegrp set name tg1 delallmbr
```

## 删除时间组定义：

**语法：**

timegrp del name <name>

**参数说明：**

| | |
|---|---|
| name | 指定欲删除的时间组定义的名字 |

**注意事项：**

不能删除被安全规则或用户、用户组引用的时间组定义。

**示例：**

```
ac>timegrp del name tg1
```

### 显示所有时间组定义：

**语法：**

timegrp show

**注意事项：**

仅显示时间组定义的部分内容。

**示例：**

```
ac>servgrp show
Name                    Member
tg1                     t1
                        t2
                        t3
```

### 显示指定名字的时间组定义：

**语法：**

timegrp show name <name>

**参数说明：**

| | |
|---|---|
| name | 指定欲显示的时间组定义的名字 |

**示例：**

```
ac>timegrp show name tg1
Name: tg1
Member: t1
        t2
        t3
Comment: time group 1
```

## 7.6 带宽（bandwidth）

### 添加非共享带宽定义：

**语法：**

bandwidth add type parent name <name> ifname <name> [ comment <comment> ]

**参数说明：**

| | |
|---|---|
| name | 设置带宽定义的名字 |

type 带宽资源类型
ifname 带宽限制的网络接口
comment 设置带宽定义的注释，可选参数，默认为空

**注意事项：**
每个网络接口上定义的非共享带宽不能超过 9 个。

**示例：**
ac>bandwidth add type parent name eth0_root ifname eth0 comment “eth0_root”

## 修改非共享带宽：

**语法：**
bandwidth set type parent name <name> [ comment <comment> ]

**参数说明：**
name 设置带宽定义的名字
type 带宽资源类型
ifname 带宽限制的网络接口
comment 设置带宽定义的注释，可选参数，默认为空

**注意事项：**
无

**示例：**
ac>bandwidth set type parent name eth0_root comment “eth0_root”

## 删除非共享带宽：

**语法：**
bandwidth del type parent { name <name> | all }

**参数说明：**
name 指定欲删除的带宽定义的名字
all 删除全部非共享带宽

**注意事项：**

**示例：**
ac>bandwidth del name “eth0_root”

## 显示非共享带宽定义：

**语法：**

bandwidth show type parent [name <name>]

**参数说明：**

name 指定欲显示的带宽定义的名字

**注意事项：**

**示例：**

ac>bandwidth show type parent name “eth0_root”

## 添加共享带宽定义：

**语法：**

bandwidth add type child name <name> minbw <number> maxbw <number> parentname <name> priority <number> [comment <comment>]

**参数说明：**

| | |
|---|---|
| name | 设置带宽定义的名字 |
| type | 带宽资源类型 |
| minbw | 设置带宽定义的保证带宽，有效值为0至1048576（千位/秒） |
| maxbw | 设置带宽定义的限制带宽，有效值为0至1048576（千位/秒） |
| parentname | 已定义过的非共享带宽的名字 |
| priority | 带宽的优先级，1-7，1最高 |
| comment | 设置带宽定义的注释，可选参数，默认为空 |

**注意事项：**

**示例：**

ac>bandwidth add type child name eth0_child minbw 1000 maxbw 2000 parentname eth0_root priority 5 comment “eth0_child”

## 修改共享带宽：

**语法：**

bandwidth set type child name <name> minbw <number> maxbw <number> parentname <name> priority <number> [comment <comment>]

**参数说明：**

| | |
|---|---|
| name | 设置带宽定义的名字 |
| type | 带宽资源类型 |
| minbw | 设置带宽定义的保证带宽，有效值为0至1048576（千位/秒） |
| maxbw | 设置带宽定义的限制带宽，有效值为0至1048576（千位/秒） |
| parentname | 已定义过的非共享带宽的名字 |
| priority | 带宽的优先级，1-7，1最高 |
| comment | 设置带宽定义的注释，可选参数，默认为空 |

**注意事项：**

无

**示例：**

ac>bandwidth set type child name eth0_child minbw 1000 maxbw 4000 parentname eth0_root priority 5 comment “eth0_child”

## 删除共享带宽：

**语法：**

bandwidth del type child { name <name> | all }

**参数说明：**

| | |
|---|---|
| name | 指定欲删除的带宽定义的名字 |
| all | 删除全部共享带宽 |

**注意事项：**

**示例：**

ac>bandwidth del type child name “eth0_child”

## 显示享带宽定义：

**语法：**

bandwidth show type child [name <name>]

**参数说明：**

| | |
|---|---|
| name | 指定欲显示的带宽定义的名字 |

**注意事项：**

**示例：**

ac>bandwidth show type child name “eth0_child”

## 添加带宽资源组定义：

**语法：**

bandwidth add type group name <name> [comment <comment>]

**参数说明：**

| | |
|---|---|
| name | 设置带宽定义的名字 |
| comment | 设置带宽定义的注释，可选参数，默认为空 |

**注意事项：**

**示例：**

ac>bandwidth add type group name bw_group

## 删除带宽资源组定义：

**语法：**

bandwidth del type group { name <name> | all }

**参数说明：**

| | |
|---|---|
| name | 指定欲删除的带宽定义的名字 |
| all | 删除全部共享带宽 |

**注意事项：**

**示例：**

ac>bandwidth del type group name “bw_group”

## 显示宽资源组定义：

**语法：**

bandwidth show type group [name <name>]

**参数说明：**

| | |
|---|---|
| name | 指定欲显示的带宽定义的名字 |

**注意事项：**

**示例：**

ac>bandwidth show type group name “bw_group”

## 修改宽资源组注释：

**语法：**

bandwidth set type group name <name> comment <comment>

**参数说明：**

name 要修改的带宽资源组的名字

comment 设置带宽资源组的注释，可选参数，默认为空

**注意事项：**

**示例：**

ac> bandwidth set type group name bw_group comment “ftp”

## 添加宽资源组成员：

**语法：**

bandwidth set type group name <name> addmbr <name>+

**参数说明：**

name 要修改的带宽资源组的名字

name 添加到带宽定义组的成员的名字

**注意事项：**

**示例：**

ac> bandwidth set type group name bw_group addmbr “eth0_child,eth1_child”

## 减少宽资源组成员：

**语法：**

bandwidth set type group name <name> delmbr <name>+

**参数说明：**

name 要修改的带宽资源组的名字

name 从带宽定义组中删除的成员的名字

**注意事项：**

**示例：**

ac> bandwidth set type group name bw_group delmbr “eth0_child”

## 删除宽资源组全部成员：

**语法：**

bandwidth set type group name <name> delallmbr

**参数说明：**

name 要修改的带宽资源组的名字

**注意事项：**

**示例：**

ac> bandwidth set type group name bw_group delallmbr

# 7.7 黑名单（blacklist）

**语法：**

blacklist add ip <ip> [ time <minute> ] [ comment <comment> ]
blacklist del ip <ip>
blacklist show

**参数说明：**

ip 单个 IP 地址
minute 阻断分钟，0 为永久阻断
comment 备注

**注意事项：**

无

**示例：**

ac> blacklist add ip 1.1.1.1 time 30
ac> blacklist del ip 1.1.1.1
ac> blacklist show

# 7.8 地址绑定（macbind）

## Ipmac 绑定全局开关

命令行：

全部语法格式：
ipmaccfg { { ipmac_log { on | off } } | { ipmac_check { on | off } } | show }

## 7.8.1 打开/关闭 ipmac 绑定日志记录

**语法：**
Ipmaccfg ipmac_log { on | off }
**参数说明：**
On 表示打开日志记录功能，这时能够看到被拒绝通过的日志记录。
off 表示关闭日志记录功能，这时拒绝通过的信息不做记录。
**注意事项：**
无
**示例：**
**打开 ipmac 绑定日志**
Themis> ipmaccfg ipmac_log on

## 7.8.2 打开/关闭 ipmac 绑定功能

**语法：**
Ipmaccfg ipmac_check { on | off }
**参数说明：**
On 表示打开绑定功能，这时相应网口再开启该功能后对应的功能才能生效。
off 表示关闭绑定功能，这时所有的 ipmac 数据全部失效。
**注意事项：**
无
**示例：**
**打开 ipmac 绑定功能**
Themis> ipmaccfg ipmac_check on

## 7.8.3 显示 ipmac 绑定的全局设置

**语法：**
Ipmaccfg show
**参数说明：**
**无**
**注意事项：**
无
**示例：**
Themis> ipmaccfg show

### 7.8.4 探测 IP/MAC 地址对（指定网络接口）：

**语法：**
macbind detect if <name>

**参数说明：**
if 指定欲探测的网络接口

**注意事项：**
无

**示例：**
```
ac>macbind detect if eth0
IP_Address       MAC_Address        Interface
192.168.1.1      00:00:00:00:00:01  eth0
192.168.1.2      00:00:00:00:00:02  eth0
```

### 7.8.5 探测 IP/MAC 地址对（指定 IP 地址）：

**语法：**
macbind detect ip <ip>

**参数说明：**
ip 指定欲探测的 IP 地址

**注意事项：**
无

**示例：**
```
ac>macbind detect ip 192.168.1.1
IP_Address       MAC_Address        Interface
192.168.1.1      00:00:00:00:00:01  eth0
```

### 7.8.6 添加 IP/MAC 地址对：

**语法：**

macbind add ip <ip> mac <mac> unique { on | off }

**参数说明：**

| | |
|---|---|
| ip | 指定 IP 地址 |
| mac | 指定 MAC 地址 |
| unique | 指定是否进行 MAC 地址的唯一性检查 |

**注意事项：**

无

**示例：**

```
ac>macbind add ip 192.168.1.1 mac 00:00:00:00:00:01 unique off
```

### 7.8.7 删除 IP/MAC 地址对：

**语法：**

macbind del ip <ip>

**参数说明：**

| | |
|---|---|
| ip | 指定欲删除的 IP/MAC 地址对中的 IP 地址 |

**注意事项：**

无

**示例：**

```
ac>macbind del ip 192.168.1.1
```

### 7.8.8 显示 IP/MAC 地址对：

**语法：**

macbind show

**参数说明：**

无

**注意事项：**

无

**示例：**

```
ac>macbind show
IP_Address        MAC_Address          Unique
192.168.1.1       00:00:00:00:00:01    off
```

# 7.9 安全选项

## 7.9.1 安全选项（filterconfig）

### 设置是否使能软件快转

**语法：**

filterconfig set fast_mode {on | off}

**参数说明：**

| | |
|---|---|
| fast_mode | 软件快转 |
| on | 启用软件快转 |
| off | 禁用软件快转 |

**注意事项：**

默认开始，用户不用关注此选项。

**示例：**

**filterconfig set fast_mode on**

### 设置是否使能硬件快转

**语法：**

filterconfig set hardfast_mode {on | off}

**参数说明：**

| | |
|---|---|
| hardfast_mode | 硬件快转 |
| on | 启用硬件快转 |
| off | 禁用硬件快转 |

**注意事项：**

默认开启，用户不用关注此选项。

**示例：**

**filterconfig set hardfast_mode on**

## 设置是否使能规则优先

**语法：**

filterconfig set rule_first {on | off}

**参数说明：**

| | |
|---|---|
| rule_first | 规则优先 |
| on | 启用规则优先 |
| off | 禁用规则优先 |

**注意事项：**

无

**示例：**

**filterconfig set rule_first on**

## 设置是否使能严格状态检查

**语法：**

filterconfig set state_check {on | off}

**参数说明：**

| | |
|---|---|
| state_check | 严格状态检查 |
| on | 启用严格状态检查 |
| off | 禁用严格状态检查 |

**注意事项：**

无

**示例：**

**filterconfig set state_check on**

## 设置是否使能基于状态路由的选择

**语法：**

filterconfig set route_state_backpacket {on | off}

**参数说明：**

| | |
|---|---|
| route_state_backpacket | 基于状态的路由选择 |
| on | 启用状态的路由选择 |

| | |
|---|---|
| off | 禁用状态的路由选择 |

**注意事项：**
无

**示例：**
**filterconfig set route_state_backpacket on**

## 设置是否使能基于状态路由的选择

**语法：**
filterconfig eth {add|del|set} <proto_name> [<proto_value>] [{on|off}]

**参数说明：**

| | |
|---|---|
| eth | 二层协议控制 |
| add | 添加一个二层协议控制 |
| del | 删除一个二层协议 |
| set | 修改一个二层协议的控制 |
| proto_name | 二层协议的协议名称，名字长度在 16 个字符以内 |
| proto_value | 二层协议协议号 |
| on | 允许该二层协议通过 |
| off | 禁止该二层协议通过 |

**注意事项：**
无

**示例：**
**filterconfig eth set 8021Q off**

## 设置运行模式（是否允许二层转发报文）

**语法：**
filterconfig set run_mode {on | off}

**参数说明：**

| | |
|---|---|
| run_mode | 运行模式 |
| on | 允许转发 |
| off | 禁止转发 |

**注意事项：**
这是系统开机启动过程中系统配置设置过程中需要设置，普通用户不用关注这个选项。

**示例：**

**filterconfig set run_mode on**

## 显示设置

**语法：**

filterconfig set show

filterconfig eth show

filterconfig show

**参数说明：**

| | |
|---|---|
| set | 设置选项：软/硬快转等 |
| eth | 二层协议控制设置项 |
| show | 显示设置的内容 |

**注意事项：**

无。

**示例：**

无

# 7.9.2 安全选项（option）

## 设置包过滤策略：

**语法：**

option set filter_policy [ accept | deny ]

**参数说明：**

| | |
|---|---|
| filter_policy | 包过滤的默认策略 |
| state_check | 严格的抗攻击开关 |

**注意事项：**

无

**示例：**

## 7.9.3 抗攻击（anti_config）

### 设置抗攻击选项：

anti_config [-t anti_name] [-h] [-l] [-A] [-D] [-U] [-i dev] [-s ip]
[-m mask] [-a anti_type] [-n num] [-c time] [-f action]
where anti_name := {config | attack | arp | ipconflict | ipcheat | cc | asic_syn}
For mere help type: anti_config -t anti_name -h

**语法：**

anti_config -t attack [-h] [-l] [-a type] [-j action]

**参数说明：**

-h 显示帮助信息
-l 显示抗攻击选项
type 抗攻击种类，可以是 ipspoofing, sroute, smurf, land, winnuke, queso, sf_scan, null_scan, full_xmas_scan, xmas_scan 中的一种,
通过-l 选项查看所有的类型和状态
action 设置为开启(on)或者关(off)状态

**注意事项：**

ipspoofing 开关和设备上的地址欺骗检查开关同时打开才能生效地址欺骗检查功能。

**示例：**

ac>anti_config -t attack -h
anti_config -t attack [-h] [-l] [-a type] [-j action]
l: display config infomation
type := {smurf | land | winnuke | queso | sf_scan | null_scan | full_xmas_scan | xmas_scan | ipspoofing | sroute}
action := {on | off | startup}

ac>anti_config -t attack -l
smurf off
land off
winnuke off
queso off
sf_scan off
null_scan off
full_xmas_scan off
xmas_scan off
ipspoofing off
sroute off

ac>anti_config -t attack –a land –j on

## arp 地址解析

**语法：**

anti_config -t arp [-h] [-i dev] [-s ip] [-m mask] [-j action]

**参数说明：**

| | |
|---|---|
| -h | 显示帮助信息 |
| dev | 显示设备名称，如 eth0,eth0,…。 |
| ip | IPv4 地址，如:1.1.1.1 |
| mask | 子网掩码，如:255.255.255.0 |
| action | 开启(on)或关闭(off) |

**注意事项：**

无

**示例：**

anti_config -t arp -i eth0 -s 10.1.5.254 -m 255.255.255.0 -j on

## ip 地址冲突

**语法：**

anti_config -t ipconflict [-h] [-i dev] [-s ip] [-m mask] [-j action]

**参数说明：**

| | |
|---|---|
| -h | 显示帮助信息 |
| dev | 显示设备名称，如 eth0,eth0,…。 |
| ip | IPv4 地址，如:1.1.1.1 |
| mask | 子网掩码，如:255.255.255.0 |
| action | 开启(on)或关闭(off) |

**注意事项：**

无

**示例：**

anti_config -t ipconflict -i eth0 -s 10.1.5.254 -m 255.255.255.0 -j on

## ip 地址欺骗

**语法：**

anti_config -t ipcheat [-h] [-i dev] [-j action]

**参数说明：**

-h 显示帮助信息
dev 显示设备名称，如 eth0,eth0,…。
ip IPv4 地址，如:1.1.1.1
action 开启(on)或关闭(off)

**注意事项：**

无

**示例：**

anti_config -t ipcheat -i eth0 -j on

# 7.10 负载均衡（ bl）

## 增加一个虚拟服务器：

**语法：**

bl add virtual <virtual name> pr <tcp|udp> ip <ip> port <port_num> pt <timeout> schd {rr|wrr|lc|wlc|dh|sh|lblc|lblcr}

**参数说明：**

virtual 虚拟服务器名
pr 协议类型，tcp 或者 udp
ip 虚拟服务的 ip 地址
port 虚拟服务提供的协议端口号
pt 持久时间
schd 真实服务器调度方法名

**名词解释：**

真实服务器：指实际组网中的运行服务的真实服务器，比如 HTTP、FTP 等服务。
虚拟服务： 指防火墙上提供的一个 ip 地址和端口号，提供真实服务器的真实服务。
持久时间：指每一个真实服务器提供服务时的连接超时时间。
调度方法：调度方法目前提供八中，列举如下：

1. rr: 轮叫调度（Round Robin）
2. wrr: 加权轮叫（Weighted Round Robin）
3. lc: 最少链接（Least Connections）
4. wlc: 加权最少链接（Weighted Least Connections）
5. dh: 目标地址散列（Destination Hashing）
6. sh: 源地址散列（Source Hashing）

7. lblc: 基于局部性的最少链接
8. lblcr: 带复制的基于局部性最少链接

**注意事项：**

虚拟服务器名不能重复。

虚拟服务所提供的 IP 指绑定在网络设备的一个 IP 地址，桥设备和拨号设备除外。

在多个墙之间，同一个 VRID 的墙的通告时间需相同，优先级不能相同。

必须在服务器负载均衡服务停止的状态下执行此命令。

**示例：**

```
ac>bl add virtual V1 pr tcp ip 1.1.1.1 port 80 pt 1~65535 schd rr
```

## 增加一个真实服务器器

**语法：**

bl add real <real name> to <virtual name> ip <ip> port <port_num> wt <weight value> gw <gw_ip>

**参数说明：**

| | |
|---|---|
| real | 真实服务器名 |
| to | 虚拟服务器名 |
| ip | 真实服务器的 ip 地址 |
| port | 真实服务器的服务端口号 |
| wt | 权重值 |
| gw | 真实服务器的网关 IP |

**注意事项：**

真实服务器名不能重复。

虚拟服务器名必须是之前已添加的虚拟服务器名

wt 取值范围是一个正整数

gw 直配置在真实服务器上的网关 IP，一般指防火墙上另一个端口的 IP。

必须在服务器负载均衡服务停止的状态下执行此命令。

**示例：**

```
ac>bl add real R1 to V1 ip 192.168.1.11 port 80 wt 1 gw 1.1.1.1
```

## 编辑虚拟服务器

**语法**

bl edit virtual < virtual name> pt <timeout> schd {rr|wrr|lc|wlc|dh|sh| lblc|lblcr}

**参数说明：**

| | |
|---|---|
| virtual | 虚拟服务器名 |
| pt | 持久时间 |
| schd | 真实服务器调度方法名 |

**注意事项：**
必须在服务器负载均衡服务停止的状态下执行此命令。

**实例：**
ac>bl edit virtual V1 pt 0 schd wrr

## 编辑真实服务器

**语法**
bl edit real <real name> wt <weight value>

**参数说明**

| | |
|---|---|
| real | 真实服务器名 |
| wt | 权重 |

**注意事项**
权重是一个正整数
必须在服务器负载均衡服务停止的状态下执行此命令。

**实例**
ac>bl edit real R1 wt 90

## 删除真实服务器

**语法**
bl del real <real name>

**参数说明**

| | |
|---|---|
| real | 真实服务器名 |

**注意事项**
无

**实例**
ac>bl del R1

## 删除虚拟服务器

**语法**
bl del virtual <virtual name>

**参数说明**

| | |
|---|---|
| virtual | 虚拟服务器名 |

**注意事项**
无

**实例**
bl del virtual V1

## 启动服务器负载均衡

**语法**
bl on

**参数说明**
无

**注意事项**
使用此功能必须先关闭防火墙中安全选项中的严格的状态检测.

**实例**
ac>bl on

## 停止服务器负载均衡

**语法**
bl off

**参数说明**
无

**注意事项**
无

**实例**
ac>bl off

## 显示服务器负载均衡状态

**语法**
bl show

**参数说明**
无

**注意事项**

无

**实例**

ac>show

## 设置服务探测状态

**语法**

bl detect {0|1|2} [dtimer <5-10>]

**参数说明**

| | |
|---|---|
| detect | 探测方式，3 个可选值。0 代表不探测，1 代表 ICMP 探测，2 代表服务端口探测 |
| dtimer | 持久时间，取值范围 5-10，单位为秒 |

**注意事项**

无

**实例**

ac>bl detect 1 dtimer 10

# 7.11 主动防御

## 7.11.1 服务

### 启动主动防御：

**语法：**

ips_url_trojan start

**参数说明：**

无

**注意事项：**

无

**示例：**

ac>ips_url_trojan start

### 关闭主动防御：

**语法：**

ips_url_trojan stop

**参数说明：**
无

**注意事项：**
无

**示例：**
ac>ips_url_trojan stop

### 7.11.2 规则

详见：流量管理＊策略＊rule(安全策略)→
添加类型为主动防御的安全规则：
修改安全规则：
删除指定序号的安全规则：
显示指定序号的安全规则：
更新安全规则：

# 第8章 应用防护

## 8.1 协议控制

### 8.1.1 协议控制总策略

#### 8.1.1.1 协议控制总表

### 添加协议控制总策略：

**语法：**
pc policy add name <name> httppolicyid <id> ftppolicyid <id> smtppolicyid <id> pop3policyid <id> comment <comment>

**参数说明：**

name： 协议控制总策略名称
httppolicyid： http 控制策略 ID
ftppolicyid： ftp 控制策略 ID
smtppolicyid： smtp 控制策略 ID
pop3policyid： pop3 控制策略 ID
comment： 协议控制总策略注释

**注意事项：**
无

**示例：**
ac>pc policy add name “pcpolicy1” httppolicyid 3 ftppolicyid 0 smtppolicyid 5 pop3policyid 0 comment “policy1Comment”

## 修改协议控制总策略：

**语法：**
pc policy set name <name> httppolicyid <id> ftppolicyid <id> smtppolicyid <id> pop3policyid <id> comment <comment>

**参数说明：**
name： 协议控制总策略名称
httppolicyid： http 控制策略 ID
ftppolicyid： ftp 控制策略 ID
smtppolicyid： smtp 控制策略 ID
pop3policyid： pop3 控制策略 ID
comment： 协议控制总策略注释

**注意事项：**
无

**示例：**
ac>pc policy add name “pcpolicy1” httppolicyid 3 ftppolicyid 0 smtppolicyid 5 pop3policyid 0 comment “policy1AnotherComment”

## 删除协议控制总策略

**语法：**
pc policy del name <name>

**参数说明：**
name：协议控制总策略名称

**注意事项：**

无

**示例：**
ac>pc policy del name “pcpolicy1”

## 显示协议控制总策略：

**语法：**
pc show policy

**参数说明：**
无

**注意事项：**
无

**示例：**
ac>pc show policy

#### 8.1.1.2 协议控制统计

## 启动协议统计：

**语法：**
pc count start

**参数说明：**
无

**注意事项：**
无

**示例：**
ac>pc count start

## 停止协议统计：

**语法：**
pc count stop

**参数说明：**
无

**注意事项：**
无

**示例：**
ac>pc count stop

## 清空协议统计：

**语法：**
pc count reset

**参数说明：**
无

**注意事项：**
无

**示例：**
ac>pc count reset

## 显示协议统计：

**语法：**
pc show count
**参数说明：**
无

**注意事项：**
无

**示例：**
ac>pc show count

# 8.1.2 协议控制策略

#### 8.1.2.1 HTTP 协议控制策略

## 添加 HTTP 协议策略：

**语法：**
pc httppolicy add name <name> method <str> action {forbidden | allow} urlgrpids <id,id,id…> action {forbidden | allow} urlcontentgrpid id action {forbidden | allow} extgrpids <id,id,id…> action {forbidden | allow}

mimegrpid <id> action {forbidden | allow} errcodegrpid <errcodegrpid> urlmax <num> webmail {on | off} advance {on | off} log {on | off} comment <comment>

**参数说明：**

| | |
|---|---|
| name： | HTTP 协议策略名称 |
| method： | HTTP 方法控制内容，GET,POST,PUT,HEAD,CONNECT |
| action： | 动作，阻止或允许 |
| urlgrpids： | URL 组 ID，可设置多个 |
| urlcontentgrpid： | URL 内容组 ID |
| extgrpids： | 文件扩展名组 ID，可设置多个 |
| mimegrpid： | MIME 组 ID |
| errcodegrpid: | 错误码组的 id 号 |
| urlmax： | URL 长度上限 |
| webmail： | 是否开启 webmail 发送控制 |
| advance： | 是否开启高级选项 |
| log： | 是否记录日志 |
| comment： | HTTP 协议策略备注 |

**注意事项：**

无

**示例：**

ac>pc httppolicy add name “httppolicy1” method “GET,PUT,” action forbidden urlgrpids 1,2,4, action allow urlcontentgrpid 3 action allow extgrpids 2,5,7, action forbidden mimegrpid 2 action allow errcodegrpid 1 urlmax 256 webmail on advance on log on comment “httppolicy1comment”

## 修改 HTTP 协议策略：

**语法：**

pc httppolicy set name <name> method <str> action {forbidden | allow} urlgrpids <id,id,id…> action {forbidden | allow} urlcontentgrpid id action {forbidden | allow} extgrpids <id,id,id…> action {forbidden | allow} mimegrpid <id> action {forbidden | allow} errcodegrpid <errcodegrpid> urlmax <num> webmail {on | off} advance {on | off} log {on | off} comment <comment>

**参数说明：**

| | |
|---|---|
| name： | HTTP 协议策略名称 |
| method： | HTTP 方法控制内容，GET,POST,PUT,HEAD,CONNECT |
| action： | 动作，阻止或允许 |
| urlgrpids： | URL 组 ID，可设置多个 |
| urlcontentgrpid： | URL 内容组 ID |
| extgrpids： | 文件扩展名组 ID，可设置多个 |
| mimegrpid： | MIME 组 ID |
| errcodegrpid: | 错误码组的 id 号 |
| urlmax： | URL 长度上限 |

webmail： 是否开启 webmail 发送控制
advance： 是否开启高级选项
log： 是否记录日志
comment： HTTP 协议策略备注

**注意事项：**
无

**示例：**
ac>pc httppolicy add name “httppolicy1” method “GET,PUT,” action forbidden urlgrpids 1,2, action allow urlcontentgrpid 3 action allow extgrpids 5,7, action forbidden mimegrpid 0 action allow errcodegrpid 1 urlmax 512 webmail on advance off log on comment “httppolicy1newcomment”

## 删除 HTTP 协议策略：

**语法：**
pc httppolicy del name <name>

**参数说明：**
name：HTTP 协议策略名称

**注意事项：**
无

**示例：**
ac>pc httppolicy del name “httppolicy1”

## 显示 HTTP 协议策略：

**语法：**
pc show httppolicy

**参数说明：**
无

**注意事项：**
无

**示例：**
ac>pc show httppolicy

#### 8.1.2.2 FTP 协议控制策略

## 添加 FTP 协议策略：

**语法：**

pc ftppolicy add name <name> method <str> action {forbidden | allow} userid <id> action {forbidden | allow} upids <id,id,id…> action {forbidden | allow} downids <id,id,id…> action {forbidden | allow} banner <string> advance {on | off} log {on | off} comment <comment>

**参数说明：**

name： FTP 策略名称
method： FTP 命令控制，LIST,DELE,NLST,CWD,RETR,STOR,XPWD
action： 动作，阻止或允许
userid： 用户名组 ID
upids： 上传控制，文件扩展名组 ID，可设置多个
downids： 下载控制，文件扩展名组 ID，可设置多个
banner： banner 替换内容
advance： 是否开启高级选项
log： 是否记录日志
comment： FTP 策略备注

**注意事项：**

无

**示例：**

ac>pc ftppolicy add name “ftppolicy1” method “LIST,CWD,” action allow userid 1 action forbidden upids 1,3, action allow downids 2,5, action forbidden banner “bannerstring” advance on log on comment “ftppolicy1comment”

## 修改 FTP 协议策略：

**语法：**

pc ftppolicy set name <name> method <str> action {forbidden | allow} userid <id> action {forbidden | allow} upids <id,id,id…> action {forbidden | allow} downids <id,id,id…> action {forbidden | allow} banner <string> advance {on | off} log {on | off} comment <comment>

**参数说明：**

name： FTP 策略名称
method： FTP 命令控制，LIST,DELE,NLST,CWD,RETR,STOR,XPWD
action： 动作，阻止或允许
userid： 用户名组 ID
upids： 上传控制，文件扩展名组 ID，可设置多个
downids： 下载控制，文件扩展名组 ID，可设置多个
banner： banner 替换内容

advance： 是否开启高级选项
log： 是否记录日志
comment： FTP 策略备注

**注意事项：**
无

**示例：**
ac>pc ftppolicy add name “ftppolicy1” method “LIST,CWD,” action allow userid 1 action forbidden upids 3, action allow downids 2, action forbidden banner “bannernewstring” advance on log on comment “ftppolicy1newcomment”

## 删除 FTP 协议策略：

**语法：**
pc ftppolicy del name <name>

**参数说明：**
name：FTP 协议策略名称

**注意事项：**
无

**示例：**
ac>pc ftppolicy del name “ftppolicy1”

## 显示 FTP 协议策略：

**语法：**
pc show ftppolicy

**参数说明：**
无

**注意事项：**
无

**示例：**
ac>pc show ftppolicy

#### 8.1.2.3 SMTP 协议控制策略

## 添加 SMTP 协议策略：

**语法：**

pc smtppolicy add name <name> toeid <id> action {forbidden | allow} fromeid <id> action {forbidden | allow} subjectid <id> action {forbidden | allow} blackaddrid <id> action {forbidden | allow} advance {on | off} ebomb slim <num> elim <num> time <sec> ebipid <id> log {on | off} comment <comment>

**参数说明：**

name： SMTP 协议策略名称
toeid： 收件人邮件地址组 ID
action： 动作，组织或允许
fromeid： 发件人邮件地址组 ID
subjectid： 邮件主题关键字组 ID
blackaddrid： 黑名单 IP 地址组 ID
advance： 是否开启高级选项
ebomb： 邮件炸弹防御 是关键字
slim： 邮件服务器阈值，范围 0~99999,0 为不限制
elim： 邮件阈值，范围 0~9999,0 为不限制
time： 统计时间，范围 10~60 秒
ebipid： 信任 IP 地址组 ID
log： 是否记录日志
comment： SMTP 协议策略备注

**注意事项：**

无

**示例：**

ac>pc smtppolicy add name “smtppolicy1” toeid 1 action allow fromeid 2 action allow subjectid 1 action forbidden blackaddrid 3 action forbidden advance on ebomb slim 1024 elim 512 time 30 ebipid 2 log on comment “smtppolicy1comment”

## 修改 SMTP 协议策略：

**语法：**

pc smtppolicy set name <name> toeid <id> action {forbidden | allow} fromeid <id> action {forbidden | allow} subjectid <id> action {forbidden | allow} blackaddrid <id> action {forbidden | allow} advance {on | off} ebomb slim <num> elim <num> time <sec> ebipid <id> log {on | off} comment <comment>

**参数说明：**

name： SMTP 协议策略名称
toeid： 收件人邮件地址组 ID
action： 动作，组织或允许

fromeid： 发件人邮件地址组 ID
subjectid： 邮件主题关键字组 ID
blackaddrid： 黑名单 IP 地址组 ID
advance： 是否开启高级选项
ebomb： 邮件炸弹防御 是关键字
slim： 邮件服务器阈值，范围 0~99999,0 为不限制
elim： 邮件阈值，范围 0~9999,0 为不限制
time： 统计时间，范围 10~60 秒
ebipid： 信任 IP 地址组 ID
log： 是否记录日志
comment： SMTP 协议策略备注

**注意事项：**
无

**示例：**
ac>pc smtppolicy set name “smtppolicy1” toeid 1 action allow fromeid 2 action allow subjectid 1 action forbidden blackaddrid 3 action forbidden advance on ebomb slim 2048 elim 256 time 30 ebipid 2 log on comment “smtppolicy1newcomment”

## 删除 SMTP 协议策略：

**语法：**
pc smtppolicy del name <name>

**参数说明：**
name：SMTP 协议策略名称

**注意事项：**
无

**示例：**
ac>pc smtppolicy del name “smtppolicy1”

## 显示 SMTP 协议策略：

**语法：**
pc show smtppolicy

**参数说明：**
无

**注意事项：**
无

**示例：**

ac>pc show smtppolicy

#### 8.1.2.4 POP3 协议控制策略

## 添加 POP3 协议策略：

**语法：**

pc pop3policy add name <name> toeid <id> action {forbidden | allow} fromeid <id> action {forbidden | allow} subjectid <id> action {forbidden | allow} log {on | off} comment <comment>

**参数说明：**

| | |
|---|---|
| name： | POP3 协议策略名称 |
| toeid： | 收件人邮件地址组 ID |
| action： | 动作，组织或允许 |
| fromeid： | 发件人邮件地址组 ID |
| subjectid： | 邮件主题关键字组 ID |
| log： | 是否记录日志 |
| comment： | POP3 协议策略备注 |

**注意事项：**

无

**示例：**

ac>pc pop3policy add name “pop3policy1” toeid 1 action forbidden fromeid 2 action forbidden subjectid 1 action allow log on comment “pop3policy1comment”

## 修改 POP3 协议策略：

**语法：**

pc pop3policy set name <name> toeid <id> action {forbidden | allow} fromeid <id> action {forbidden | allow} subjectid <id> action {forbidden | allow} log {on | off} comment <comment>

**参数说明：**

| | |
|---|---|
| name： | POP3 协议策略名称 |
| toeid： | 收件人邮件地址组 ID |
| action： | 动作，组织或允许 |
| fromeid： | 发件人邮件地址组 ID |
| subjectid： | 邮件主题关键字组 ID |
| log： | 是否记录日志 |
| comment： | POP3 协议策略备注 |

**注意事项：**

无

**示例：**

ac>pc pop3policy set name “pop3policy1” toeid 2 action forbidden fromeid 1 action forbidden subjectid 3 action allow log on comment “pop3policy1newcomment”

## 删除 POP3 协议策略：

**语法：**

pc pop3policy del name <name>

**参数说明：**

name：POP3 协议策略名称

**注意事项：**

无

**示例：**

ac>pc pop3policy del name “pop3policy1”

## 显示 POP3 协议策略：

**语法：**

pc show pop3policy

**参数说明：**

无

**注意事项：**

无

**示例：**

ac>pc show pop3policy

# 8.1.3 协议控制内容

#### 8.1.3.1 URL 组

## 添加 URL 组：

**语法：**

pc content urlgrp add name <name> comment <comment>

**参数说明：**

name： URL 组名称

comment： URL 组备注

**注意事项：**

无

**示例：**

ac>pc content urlgrp add name “urlgrp1” comment “urlgrp1comment”

## 修改 URL 组：

**语法：**

pc content urlgrp set name <name> comment <comment>

**参数说明：**

name： URL 组名称

comment： URL 组备注

**注意事项：**

无

**示例：**

ac>pc content urlgrp set name “urlgrp1” comment “urlgrp1newcomment”

## 删除 URL 组：

**语法：**

pc content urlgrp del name <name>

**参数说明：**

name：URL 组名称

**注意事项：**

无

**示例：**

ac> pc content urlgrp del name “urlgrp1”

## 显示 URL 组

**语法：**

pc show urlgrp

**参数说明：**
无

**注意事项：**
无

**示例：**
ac>pc show urlgrp

## 组内添加成员 URL：

**语法：**
pc content url add url <url> gid <id>

**参数说明：**
url：成员 URL
gid：URL 组 ID

**注意事项：**
无

**示例：**
ac>pc content url add url “yuufshjfh” gid 1

## 修改成员 URL

**语法：**
pc content url set id <id> url <url>

**参数说明：**
id：成员 URL 的 ID
url：成员 URL

**注意事项：**
无

**示例：**
ac>pc content url set id 1 url “jhjfgug”

## 删除成员 URL：

**语法：**
pc content url del id <id>

**参数说明：**
id：成员 URL 的 ID

**注意事项：**
无

**示例：**
ac>pc content url del id 1

## 显示组内成员 URL：

**语法：**
pc show urlgrp id <id>

**参数说明：**
id：URL 组 ID

**注意事项：**
无

**示例：**
ac>pc show urlgrp id 1

#### 8.1.3.2 文件扩展名组

## 添加文件扩展名组：

**语法：**
pc content extgrp add name <string> comment <comment>

**参数说明：**
name： 文件扩展名组名称
comment： 文件扩展名组备注

**注意事项：**
无

**示例：**
ac>pc content extgrp add name “extgrp1” comment “extgrp1comment”

## 修改文件扩展名组：

**语法：**

pc content extgrp set name <string> comment <comment>

**参数说明：**

name： 文件扩展名组名称

comment： 文件扩展名组备注

**注意事项：**

无

**示例：**

ac>pc content extgrp set name “extgrp1” comment “extgrp1newcomment”

## 删除文件扩展名组：

**语法：**

pc content extgrp del name <string>

**参数说明：**

name： 文件扩展名组名称

**注意事项：**

无

**示例：**

ac>pc content extgrp del name “extgrp1”

## 显示文件扩展名组：

**语法：**

pc show extgrp

**参数说明：**

无

**注意事项：**

无

**示例：**

ac>pc show extgrp

## 组内添加成员文件扩展名：

**语法：**

pc content ext add ext <ext> gid <id>

**参数说明：**
ext：成员文件扩展名内容
gid：文件扩展名组 ID

**注意事项：**
无

**示例：**
ac>pc content ext add ext “ghjkoi” gid 1

## 修改成员文件扩展名：

**语法：**
pc content ext set id <id> ext <ext>

**参数说明：**
id：成员文件扩展名 ID
ext：成员文件扩展名内容

**注意事项：**
无

**示例：**
ac>pc content ext set id 1 ext “yiuobf”

## 删除成员文件扩展名：

**语法：**
pc content ext del id <id>

**参数说明：**
id：成员文件扩展名 ID

**注意事项：**
无

**示例：**
ac>pc content ext del id 1

## 显示组内成员文件扩展名：

**语法：**

pc show extgrp id <id>

**参数说明：**
id：文件扩展名组 ID

**注意事项：**
无

**示例：**
ac>pc show extgrp 1

#### 8.1.3.3 MIME 组

## 添加 MIME 组：

**语法：**
pc content mimegrp add name <name> application {on | partial | off} video {on | partial | off} audio {on | partial | off} image {on | partial | off} text {on | partial | off} comment <comment>

**参数说明：**
name： MIME 组名称
application： 应用程序成员 mime 选择方式，on:全选，partial:部分选择，off:不选
video： 视频类成员 mime 选择方式，on:全选，partial:部分选择，off:不选
audio： 音频类成员 mime 选择方式，on:全选，partial:部分选择，off:不选
image： 图像类成员 mime 选择方式，on:全选，partial:部分选择，off:不选
text： 文本类成员 mime 选择方式，on:全选，partial:部分选择，off:不选
comment： MIME 组备注

**注意事项：**
无

**示例：**
ac>pc content mimegrp add name “mimegrp1” application on video partial audio off image on text partial comment “mimegrp1comment”

## 修改 MIME 组：

**语法：**
pc content mimegrp set name <name> application {on | partial | off} video {on | partial | off} audio {on | partial | off} image {on | partial | off} text {on | partial | off} comment <comment>

**参数说明：**
name： MIME 组名称

application： 应用程序成员 mime 选择方式，on:全选，partial:部分选择，off:不选
video： 视频类成员 mime 选择方式，on:全选，partial:部分选择，off:不选
audio： 音频类成员 mime 选择方式，on:全选，partial:部分选择，off:不选
image： 图像类成员 mime 选择方式，on:全选，partial:部分选择，off:不选
text： 文本类成员 mime 选择方式，on:全选，partial:部分选择，off:不选
comment： MIME 组备注

**注意事项：**
无

**示例：**
ac>pc content mimegrp set name “mimegrp1” application on video partial audio off image on text partial comment “mimegrp1newcomment”

## 删除 MIME 组：

**语法：**
pc content mimegrp del name <name>

**参数说明：**
name：MIME 组名称

**注意事项：**
无

**示例：**
ac>pc content mimegrp del name “mimegrp1”

## 显示 MIME 组：

**语法：**
pc show mimegrp

**参数说明：**
无

**注意事项：**
无

**示例：**
ac>pc show mimegrp

## 组内添加成员 mime 类型：

**语法：**

pc content mime add gid <id> name <name>

**参数说明：**

gid： MIME 组 ID

name： 成员 mime

**注意事项：**

无

**示例：**

ac>pc content mime add gid 1 name “dca-rft”

## 显示组内成员 mime 类型：

**语法：**

pc show mimegrp id <id>

**参数说明：**

id：MIME 组 ID

**注意事项：**

命令行中 id 字段是可选的，如无 id（即只执行 pc show mimegrp），则会将已有的 mime 类型都会显示出来。

**示例：**

ac>pc show mimegrp id 1

#### 8.1.3.4 用户名组

## 添加用户名组：

**语法：**

pc content usrnamegrp add name <name> comment <comment>

**参数说明：**

name： 用户名组名称

comment： 用户名组备注

**注意事项：**

无

**示例：**

ac>pc content usrnamegrp add name “usrnamegrp1” comment “usrnamegrp1comment”

## 修改用户名组：

**语法：**

pc content usrnamegrp set name <name> comment <comment>

**参数说明：**

name： 用户名组名称

comment： 用户名组备注

**注意事项：**

无

**示例：**

ac>pc content usrnamegrp set name “usrnamegrp1” comment “usrnamegrp1newcomment”

## 删除用户名组：

**语法：**

pc content usrnamegrp del name <name>

**参数说明：**

name： 用户名组名称

**注意事项：**

无

**示例：**

ac>pc content usrnamegrp del name “usrnamegrp1”

## 显示用户名组：

**语法：**

pc show usrnamegrp

**参数说明：**

无

**注意事项：**

无

**示例：**

ac>pc show usrnamegrp

## 组内添加成员用户名：

**语法：**

pc content usrname add name <name> gid <id>

**参数说明：**

name： 成员用户名名称

gid： 用户名组 ID

**注意事项：**

无

**示例：**

ac>pc content usrname add name “usrname1” gid 1

## 修改成员用户名：

**语法：**

pc content usrname set id <id> name <name>

**参数说明：**

id： 成员用户名 ID

name： 成员用户名名称

**注意事项：**

无

**示例：**

ac> pc content usrname set id 1 name “usrname2”

## 删除成员用户名：

**语法：**

pc content usrname del id <id>

**参数说明：**

id：成员用户名 ID

**注意事项：**

无

**示例：**

ac> pc content usrname del id 1

## 显示组内成员用户名：

**语法：**
pc show usrnamegrp id <id>

**参数说明：**
id：用户名组 ID

**注意事项：**
无

**示例：**
ac>pc show usrnamegrp id 1

#### 8.1.3.5 邮件地址组

## 添加邮件地址组：

**语法：**
pc content emailgrp add name <name> comment <comment>

**参数说明：**
name： 邮件地址组名称
comment： 邮件地址组备注

**注意事项：**
无

**示例：**
ac> pc content emailgrp add name “emailgrp1” comment “emailgrp1comment”

## 修改邮件地址组：

**语法：**
pc content emailgrp set name <name> comment <comment>

**参数说明：**
name： 邮件地址组名称
comment： 邮件地址组备注

**注意事项：**
无

**示例：**
ac> pc content emailgrp set name “emailgrp1” comment “emailgrp1newcomment”

## 删除邮件地址组：

**语法：**
pc content emailgrp del name <name>

**参数说明：**
name： 邮件地址组名称

**注意事项：**
无

**示例：**
ac> pc content emailgrp del name “emailgrp1”

## 显示邮件地址组：

**语法：**
pc show emailgrp

**参数说明：**
无

**注意事项：**
无

**示例：**
ac>pc show emailgrp

## 添加组内成员邮件地址：

**语法：**
pc content email add email <email> gid <id>

**参数说明：**
email： 成员邮件地址内容
gid： 邮件地址组 ID

**注意事项：**
无

**示例：**
ac>pc content email add email “xyz@mm.com” gid 1

## 修改成员邮件地址：

**语法：**
pc content email set id <id> email <email>

**参数说明：**
id： 成员邮件地址 ID
email： 成员邮件地址内容

**注意事项：**
无

**示例：**
ac>pc content email set id 1 email “abc@mm.com”

## 删除成员邮件地址：

**语法：**
pc content email del id <id>

**参数说明：**
id：成员邮件地址 ID

**注意事项：**
无

**示例：**
ac>pc content email del id 1

## 显示组内成员邮件地址：

**语法：**
pc show emailgrp id <id>

**参数说明：**
id：邮件地址组 ID

**注意事项：**
无

**示例：**

ac>pc show emailgrp id 1

#### 8.1.3.6 邮件主题关键字组

## 添加邮件主题关键字组：

**语法：**

pc content subjectgrp add name <name> comment <comment>

**参数说明：**

name： 邮件主题关键字组名称

comment： 邮件主题关键字组备注

**注意事项：**

无

**示例：**

ac>pc content subjectgrp add name “subjectgrp1” comment “subjectgrp1comment”

## 修改邮件主题关键字组：

**语法：**

pc content subjectgrp set name <name> comment <comment>

**参数说明：**

name： 邮件主题关键字组名称

comment： 邮件主题关键字组备注

**注意事项：**

无

**示例：**

ac>pc content subjectgrp set name “subjectgrp1” comment “subjectgrp1newcomment”

## 删除邮件主题关键字组：

**语法：**

pc content subjectgrp del name <name>

**参数说明：**

name：邮件主题关键字组名称

**注意事项：**

无

**示例：**
ac>pc content subjectgrp del name “subjectgrp1”

## 显示邮件主题关键字组：

**语法：**
pc show subjectgrp

**参数说明：**
无

**注意事项：**
无

**示例：**
ac>pc show subjectgrp

## 组内添加成员邮件主题关键字：

**语法;**
pc content subject add subject <subject> gid <id>

**参数说明：**
subject： 成员邮件主题关键字内容
gid： 邮件主题关键字组 ID

**注意事项：**
无

**示例：**
ac>pc content subject add subject “subject1” gid 1

## 修改成员邮件主题关键字：

**语法：**
pc content subject set id <id> subject <subject>

**参数说明：**
id： 成员邮件主题关键字 ID
subject： 成员邮件主题关键字内容

**注意事项：**

无

**示例：**
ac>pc content subject set id 1 subject “subject2”

## 删除成员邮件主题关键字：

**语法：**
pc content subject del id <id>

**参数说明：**
id：成员邮件主题关键字 ID

**注意事项：**
无

**示例：**
ac>pc content subject del id 1

## 显示组内成员邮件主题关键字：

**语法：**
pc show subjectgrp id <id>

**参数说明：**
id：邮件主题关键字组 ID

**注意事项：**
无

**示例：**
ac>pc show subjectgrp id 1

#### 8.1.3.7 IP 地址组

## 添加 IP 地址组：

**语法：**
pc content ipgrp add name <name> comment <comment>

**参数说明：**
name： IP 地址组名称
comment： IP 地址组备注

**注意事项：**
无

**示例：**
ac>pc content ipgrp add name “ipgrp1” comment “ipgrp1comment”

## 修改 IP 地址组：

**语法：**
pc content ipgrp set name <name> comment <comment>

**参数说明：**
name： IP 地址组名称
comment： IP 地址组备注

**注意事项：**
无

**示例：**
ac>pc content ipgrp set name “ipgrp1” comment “ipgrp1newcomment”

## 删除 IP 地址组：

**语法：**
pc content ipgrp del name <name>

**参数说明：**
name：IP 地址组名称

**注意事项：**
无

**示例：**
ac>pc content ipgrp del name “ipgrp1”

## 显示 IP 地址组：

**语法：**
pc show ipgrp

**参数说明：**
无

**注意事项：**

无

**示例：**

ac>pc show ipgrp

## 组内添加成员 IP 地址：

**语法：**

pc content ip add type <type>(1 v4 0 v6) addr <addr> gid <id>

**参数说明：**

type： 成员 IP 地址类型，1:IPV4，0:IPV6
addr： 成员 IP 地址内容
gid： IP 地址组 ID

**注意事项：**

无

**示例：**

ac>pc content ip add type 1 addr “1.2.3.4” gid 1
ac>pc content ip add type 0 addr “1:2::3” gid 1

## 修改成员 IP 地址：

**语法：**

pc content ip set id <id> type <type> addr <addr>

**参数说明：**

id： 成员 IP 地址 ID
type： 成员 IP 地址类型，1:IPV4，0:IPV6
addr： 成员 IP 地址内容

**注意事项：**

无

**示例：**

ac>pc content ip set id 1 type 1 addr “3.4.5.6”

## 删除成员 IP 地址：

**语法：**

pc content ip del id <id>

**参数说明：**

id：成员 IP 地址 ID

**注意事项：**
无

**示例：**
ac>pc content ip del id 1

## 显示组内成员 IP 地址：

**语法：**
pc show ipgrp id <id>

**参数说明：**
id：IP 地址组 ID

**注意事项：**
无

**示例：**
ac>pc show ipgrp id 1

#### 8.1.3.8 URL 内容组

## 添加 URL 内容组：

**语法：**
pc content urlcontentgrp add name <name> comment <comment>

**参数说明：**
name： URL 内容组名称
comment： URL 内容组备注

**注意事项：**
无

**示例：**
ac>pc content urlcontentgrp add name “urlcontentgrp1” comment “urlcontentgrp1comment”

## 修改 URL 内容组：

**语法：**
pc content urlcontentgrp set name <name> comment <comment>

**参数说明：**

name： URL 内容组名称

comment： URL 内容组备注

**注意事项：**

无

**示例：**

ac>pc content urlcontentgrp set name “urlcontentgrp1” comment “urlcontentgrp2comment”

## 删除 URL 内容组：

**语法：**

pc content urlcontentgrp del name <name>

**参数说明：**

name：URL 内容组名称

**注意事项：**

无

**示例：**

ac>pc content urlcontentgrp del name “urlcontentgrp1”

## 组内添加成员 URL 内容：

**语法：**

pc content urlcontent add urlcontent <urlcontent> gid <id>

**参数说明：**

urlcontent： 成员 URL 内容

gid： URL 内容组 ID

**注意事项：**

无

**示例：**

ac>pc content urlcontent add urlcontent “urlcontent1” gid 1

## 修改成员 URL 内容：

**语法：**

pc content urlcontent set id <id> urlcontent <urlcontent>

**参数说明：**

id： 成员 URL 内容的 ID

urlcontent： 成员 URL 内容

**注意事项：**

无

**示例：**

ac>pc content urlcontent set id 1 urlcontent “urlcontent2”

### 删除成员 URL 内容：

**语法：**

pc content urlcontent del id <id>

**参数说明：**

id：成员 URL 内容的 ID

**注意事项：**

无

**示例：**

ac>pc content urlcontent del id 1

### 显示组内成员 URL 内容：

**语法：**

pc show urlcontentgrp id <id>

**参数说明：**

id：URL 内容组 ID

**注意事项：**

无

**示例：**

ac>pc show urlcontentgrp id 1

## 8.1.4 规则应用

### 把规则下发到内核：

**语法：**
pc download

**参数说明：**
无

**注意事项：**
无

**示例：**
ac>pc download

### 把规则下发到应用程序代理进程：

**语法：**
pc appdownload

**参数说明：**
无

**注意事项：**
无

**示例：**
ac>pc appdownload

# 8.2 病毒防护

## 8.2.1 病毒防护策略

### 添加 AV 策略：

**语法：**
av add type policy name <name> comment <comment> policyid <id>

**参数说明：**
name： 病毒防护策略的名称
comment： 病毒防护策略的注释
policyid： 策略参考的已有病毒防护策略的 ID

**注意事项：**

无

**示例：**

ac> av add type policy name "AV1" comment "test" policyid 1

## 修改 AV 策略：

**语法：**

av set type policy name <name> protocol <protocol> { [ active { on | off }] | [ block { on | off }] | [ log { on | off }] | [ alertmail { on | off }] | [ sound { on | off }] | [resetsend {on | off}] | [resetrecv {on | off}]}

**参数说明：**

| | |
|---|---|
| name： | 病毒防护策略的名称 |
| protocol： | 应用层协议，支持 http,smtp,pop,ftp,imap,msn,webmail |
| active： | 病毒防护策略是否生效 |
| block： | 是否阻止病毒传播 |
| log： | 检测到病毒时是否记录日志 |
| alertmail： | 检测到病毒时是否发送告警邮件 |
| sound： | 检测到攻击时是否在最新事件列表中发出报警 |
| resetsend： | 检测到攻击时是否重置客户端连接 |
| resetrecv： | 检测到攻击时是否重置服务器端连接 |

**注意事项：**

无

**示例：**

ac> av set type policy name "AV1" protocol “http” block off

## 删除 AV 策略：

**语法：**

av del type policy policyid <id>

**参数说明：**

policyid：待删除的病毒防护策略的 ID

**注意事项：**

无

**示例：**

ac> av del type policy policyid 2

### 显示 AV 策略：

**语法：**
av show policy all

**参数说明：**
无

**注意事项：**
无

**示例：**
ac>av show policy all

### 显示 AV 策略配置：

**语法：**
av show policy id <id>

**参数说明：**
id：AV 策略 ID

**注意事项：**
无

**示例：**
ac>av show policy id 3

## 8.2.2 自定义病毒特征

### 添加自定义病毒特征：

**语法：**
av addsig name <name> sig <sig>

**参数说明：**
name： 自定义病毒特征名称
sig： 自定义病毒特征内容

**注意事项：**
无

**示例：**

ac>av addsig name “avsig1” sig “customsig”

### 修改自定义病毒特征：

**语法：**

av setsig name <name> sig <sig>

**参数说明：**

name： 自定义病毒特征名称

sig： 自定义病毒特征内容

**注意事项：**

无

**示例：**

ac>av setsig name “avsig1” sig “customsig1”

### 删除自定义病毒特征：

**语法：**

av delsig name <name>

**参数说明：**

name：自定义病毒特征名称

**注意事项：**

无

**示例：**

ac>av delsig name “avsig1”

## 8.2.3 服务端口

### 添加服务端口：

**语法：**

av addport name <protocol> port <port>

**参数说明：**

name： 服务名称，支持的服务名称有：HTTP,FTP,SMTP,POP,IMAP, WEBMAIL

port： 服务端口

**注意事项：**
无

**示例：**
ac>av addport name “http” port 8080

## 删除服务端口：

**语法：**
av delport name <protocol> {all | port <port>}

**参数说明：**
name： 服务名称，支持：HTTP,FTP,SMTP.POP,IMAP,WEBMAIL
all： 删除全部端口
port： 删除指定端口

**注意事项：**
无

**示例：**
ac>av delport name “http” all
ac>av delport name “http” port 8080

## 显示服务端口配置：

**语法：**
av show port all

**参数说明：**
无

**注意事项**
无

**示例：**
av show port all

### 8.2.4 病毒库

## 修改扫毒病毒库：

**语法：**

av setmode {quick | full}

**参数说明：**

quick： 常规病毒库(快速扫毒)

full： 扩展病毒库(全面扫毒)

**注意事项：**

无

**示例：**

ac>av setmode quick

ac>av setmode full

## 显示扫毒病毒库配置：

**语法：**

av show avmode

**参数说明：**

无

**注意事项：**

无

**示例：**

ac>av show avmode

### 8.2.5 文件过滤器

## 修改文件过滤器配置：

**语法：**

av engine {[filesize <size>] | [blockext <ext>] | [passext <ext>] | [compress { on | off }]}

**参数说明：**

filesize： 缓存文件大小上限，0~1024kb

blockext： 病毒文件黑名单后缀名，多个后缀名以“,”隔开
passext： 病毒文件白名单后缀名，多个后缀名以“,”隔开
compress： 是否启用压缩文件扫描

**注意事项：**
无

**示例：**
ac>av engine filesize 1024 blockext “.exe,.bat” passext “.txt,.c” compress on

## 显示文件过滤器配置：

**语法：**
av show engine option

**参数说明：**
无

**注意事项：**
无

**示例：**
ac>av show engine option

### 8.2.6 AV 云防护 agent

## 启用 AV 云防护：

**语法：**
uevent av active on

**参数说明：**
无

**注意事项：**
无

**示例：**
ac> uevent av active on

## 关闭 AV 云防护：

**语法：**
uevent av active off

**参数说明：**
无

**注意事项：**
无

**示例：**
ac> uevent av active off

## 修改云防护上传服务器信息：

**语法：**
uevent av server <string> port <port>

**参数说明：**
server： 云防护上传服务器域名
port： 云防护上传服务器端口

**注意事项：**
无

**示例：**
ac>uevent av server “Server.domain” port 8900

## 恢复云防护默认设置：

**语法：**
uevent av default

**参数说明：**
无

**注意事项：**
无

**示例：**
ac>uevent av default

## 显示 AV 云防护配置：

**语法：**

uevent show

**参数说明：**
无

**注意事项：**
无

**示例：**
ac>uevent show

## 8.2.7 隔离

### 修改病毒文件隔离配置：

**语法：**
vhq setvq on dir <string_mntpath> http {on | off} ftp {on | off} smtp {on | off} pop3 {on | off}
vhq setvq off

**参数说明：**
dir： usb 设备挂在路径
http： 是否隔离应用协议 http
ftp： 是否隔离应用协议 ftp
smtp： 是否隔离应用协议 smtp
pop3： 是否隔离应用协议 pop3

**注意事项：**
无

**示例：**
ac>vhq setvq on dir “/mount/path” http on ftp on smtp off pop3 off
ac>vhq setvq off

### 删除病毒文件记录：

**语法：**
vhq setvq del id <id>
vhq setvq del all

**参数说明：**
id： 删除指定编号的病毒文件
all：删除全部病毒文件，即清空

**注意事项：**

无

**示例：**

ac>vhq setvq del id 67

ac>vhq setvq del all

### 修改病毒主机隔离配置：

**语法：**

vhq sethq on time <seconds> http {on | off} ftp {on | off} smtp {on | off} pop3 {on | off}

vhq sethq off

**参数说明：**

time： 病毒主机隔离时间

http： 是否隔离应用协议 http

ftp： 是否隔离应用协议 ftp

smtp： 是否隔离应用协议 smtp

pop3： 是否隔离应用协议 pop3

**注意事项：**

无

**示例：**

ac>vhq sethq on time 1800 http off ftp off smtp on pop3 on

ac>vhq sethq off

# 8.3 入侵防护

## 8.3.1 入侵防护策略

### 添加入侵防护策略：

**语法：**

ipsconfig add type policy name <name> comment <comment> policyid <id>

**参数说明：**

name 入侵防护策略的名称

comment 入侵防护策略的注释

policyid 策略参考的已有入侵防护策略的 ID

**注意事项：**
无

**示例：**
ac> ipsconfig add type policy name “ipsrule01” comment “NewRule” policyid 1

## 修改入侵防护策略：

**语法：**
ipsconfig set type policy name <name> { signature | group } <signame> { active { on | off } drop { on | off } log { on | off } alertmail { on | off } resetsend { on | off } resetrecv {on | off} dropsession { on | off }}

**参数说明：**

| | |
|---|---|
| name | 入侵防护策略的名称 |
| signature | 入侵防护策略的签名名称 |
| group | 入侵防护策略的组名称，如 Access,Overflow 等 |
| active | 入侵防护策略是否生效 |
| drop | 检测到攻击时是否丢弃 |
| log | 检测到攻击时是否记录日志 |
| alertmail | 检测到攻击时是否发送告警邮件 |
| resetsend | 检测到攻击时是否重置客户端连接 |
| resetrecv | 检测到攻击时是否重置服务器端连接 |
| dropsession | 检测到攻击时是否在最新事件列表中发出报警 |

**注意事项：**
无

**示例：**
ac> ipsconfig set type policy name “ipsrule01” group “Access” active on drop off alertmail off log on resetsend off resetrecv off dropsession off

## 删除入侵防护策略：

**语法：**
ipsconfig del type policy policyid <id>

**参数说明：**
policyid 待删除的入侵防护策略的 ID

**注意事项：**
无

**示例：**

ac> ipsconfig del type policy policyid 3

### 显示入侵防护策略配置：

**语法：**

ipsconfig show policy

**参数说明：**

无

**注意事项：**

无

**示例：**

ac> ipsconfig show policy

## 8.3.2 自定义特征

### 添加自定义特征：

**语法：**

ipsconfig addlocal sip <all_ip> sport <all_port> dip <all_ip> dport <all_port> protocol {tcp|udp|icmp} name <name> signature <string> nocase {on |off} [offset <number>] [depth <number>]

参数说明：

| | |
|---|---|
| sip： | 源 IP 地址，默认为 any |
| sport： | 源端口 |
| dip： | 目的 IP 地址，默认为 any |
| dport： | 目的端口 |
| protocl： | 传输层协议，tcp、udp 二选一 |
| name： | 自定义特征名称 |
| signature： | 自定义特征内容 |
| nocase： | 入侵特征码是否区分大小写，off 时表示区分，on 表示不区分 |
| offset： | 可选项 |
| depth： | 可选项 |

**注意事项：**

无

**示例：**

ac>ipsconfig addlocal sip any sport 333 dip any dport 23 protocol “tcp” name “t1” signature “t1” nocase off

ac>ipsconfig addlocal sip any sport 555 dip any dport 32 protocol “tcp” name “t1” signature “t1” nocase off

offset 2 depth 3

## 修改自定义特征：

**语法：**

ipsconfig setlocal <id> sip <all_ip> sport <all_port> dip <all_ip> dport <all_port> protocol {tcp|udp|icmp} name <name> signature <string> nocase {on |off} [offset <number>][depth <number>]

参数说明：

<id>： 自定义特征 ID
sip： 源 IP 地址，默认为 any
sport： 源端口
dip： 目的 IP 地址，默认为 any
dport： 目的端口
protocol： 传输层协议，tcp/udp 二选一
name： 自定义特征名称
signature： 自定义特征内容
nocase： 入侵特征码是否区分大小写，off 时表示区分，on 表示不区分
offset： 可选项
depth： 可选项

**注意事项：**

无

**示例：**

ac>ipsconfig setlocal 1 sip any sport 333 dip any dport 24 protocol “tcp” name “t1” signature “t1” nocase off offset 11 depth 22

## 激活自定义特征：

**语法：**

ipsconfig activelocal <id>

**参数说明：**

<id>： 自定义特征 ID

**注意事项：**

无

**示例：**

ac>ipsconfig activelocal 1

## 阻断自定义特征：

**语法：**
ipsconfig blocklocal <id>

**参数说明：**
<id>： 自定义特征 ID

**注意事项：**
无

**示例：**
ac>ipsconfig blocklocal 1

## 删除自定义特征：

**语法;**
ipsconfig dellocal <id>

**参数说明：**
<id>：自定义特征 ID

**注意事项：**
无

**示例：**
ac>ipsconfig dellocal 1

## 显示自定义特征配置：

**语法：**
ipsconfig showlocal

**参数说明：**
无

**注意事项：**
无

**示例：**
ac>ipsconfig showlocal

## 8.3.3 IPS 云防护 agent

### 启用 IPS 云防护：

**语法：**
uevent ips active on

**参数说明：**
无

**注意事项：**
无

**示例：**
ac> uevent ips active on

### 关闭 IPS 云防护：

**语法：**
uevent ips active off

**参数说明：**
无

**注意事项：**
无

**示例：**
ac> uevent ips active off

### 修改云防护上传服务器信息：

**语法：**
uevent ips server <string> port <port>

**参数说明：**
server： 云防护上传服务器域名
port： 云防护上传服务器端口

**注意事项：**
无

**示例：**

ac>uevent ips server “Server.domain” port 8900

### 恢复云防护默认设置：

**语法：**

uevent ips default

**参数说明：**

无

**注意事项：**

无

**示例：**

ac>uevent ips default

### 显示 IPS 云防护配置：

**语法：**

uevent show

**参数说明：**

无

**注意事项：**

无

**示例：**

ac>uevent show

## 8.3.4 场景和模式设置

### 修改入侵场景保留设置：

**语法：**

ipsconfig setpkt usbstorage <string> maxsize <number> packet_max <number> active {on | off} upload { on server <string> port <number> | off }

**参数说明：**

usbstorage： usb 设备的挂在目录

maxsize： 存储上限，兆 M

packet_max：每个攻击存储报文上限
active：场景保留是否开启
upload：上传报文是否开启
server：FTP 服务器 IP 地址
port：FTP 服务器端口

**注意事项：**
无

**示例：**
ac>ipsconfig setpkt usbstorage “/mount/path” maxsize 2 packet_max 10 active on upload on server “1.2.3.4” port 24
ac>ipsconfig setpkt usbstorage “/mount/path” maxsize 2 packet_max 10 active on upload off

## 删除入侵场景保留记录：

**语法：**
ipsconfig delpkt id <number>

**参数说明：**
id：入侵场景保留记录 ID

**注意事项：**
无

**示例：**
ipsconfig delpkt id 5

## 显示入侵场景保留配置：

**语法：**
ipsconfig showpkt policy

**参数说明：**
无

**注意事项：**
无

**示例：**
ipsconfig showpkt policy

## 显示入侵场景保留记录：

**语法：**
ipsconfig showpkt filelist

**参数说明：**
无

**注意事项：**
无

**示例：**
ipsconfig showpkt filelist

### 8.3.5 规避乱序检测

#### 修改规避乱序检测设置：

**语法：**
ipsconfig setreasm active {on | off} max_session <number> max_mem <number>

**参数说明：**
active： 规避乱序检测是否开启
max_session： 并行连接上限，最大值为 50000
max_mem： 缓存上限，kbytes，最大值为 20480

**注意事项：**
无

**示例：**
ipsconfig setreasm active on max_session 50000 max_mem 20480

#### 显示规避乱序检测配置：

**语法：**
ipsconfig showreasm

**参数说明：**
无

**注意事项：**
无

**示例：**

ipsconfig showreasm

### 8.3.6 会话模式

#### 修改当前的会话模式：

**语法：**

ipsconfig setmode {stream | packet}

**参数说明：**

stream： 会话模式是基于流的

packet： 会话模式是基于单包的

**注意事项：**

无

**示例：**

ac>ipsconfig setmode stream

ac>ipsconfig setmode packet

#### 显示当前会话模式：

**语法：**

ipsconfig showmode

**参数说明：**

无

**注意事项：**

无

**示例：**

ac>ipsconfig showmode

# 8.4 反垃圾邮件

## 8.4.1 基本配置

### 垃圾邮件服务器 IP 地址黑名单功能：

**语法：**

antispam blackserver {on | off}

**参数说明：**

on： 开启垃圾邮件服务器 IP 地址黑名单功能

off： 关闭垃圾邮件服务器 IP 地址黑名单功能

**注意事项：**

无

**示例：**

ac> antispam blackserver on

ac> antispam blackserver off

### 启用垃圾邮件地址检查功能：

**语法：**

antispam checkspamaddress {on | off}

**参数说明：**

on： 开启垃圾邮件地址检查功能

off： 关闭垃圾邮件地址检查功能

**注意事项：**

无

**示例：**

ac> antispam checkspamaddress on

ac> antispam checkspamaddress off

### 启用主题关键字检查功能：

**语法：**

antispam checkkeywords {on | off}

**参数说明：**

on： 开启主题关键字检查功能

off： 关闭主题关键字检查功能

**注意事项：**

无

**示例：**

ac> antispam checkkeywords on

ac> antispam checkkeywords off

## 启用正文关键字检查功能：

**语法：**

antispam checkContent {on | off}

**参数说明：**

on： 开启正文关键字检查功能

off： 关闭正文关键字检查功能

**注意事项：**

无

**示例：**

ac> antispam checkContent on

ac> antispam checkContent off

## 启用附件名关键字检查功能：

**语法：**

antispam attachmentFilename {on | off}

**参数说明：**

on： 开启附件名关键字检查功能

off： 关闭附件名关键字检查功能

**注意事项：**

无

**示例：**

ac> antispam attachmentFilename on

ac> antispam attachmentFilename off

## 启用附件正文关键字检查功能：

**语法：**

antispam attachmentContent {on | off}

**参数说明：**

on： 开启附件正文关键字检查功能

off： 关闭附件正文关键字检查功能

**注意事项：**

无

**示例：**

ac> antispam attachmentContent on

ac> antispam attachmentContent off

## 启用附件大小检查功能：

**语法：**

antispam attachmentFilesize {on | off}

**参数说明：**

on： 开启附件大小检查功能

off： 关闭附件大小检查功能

**注意事项：**

无

**示例：**

ac> antispam attachmentFilesize on

ac> antispam attachmentFilesize off

单个附件大小上限：

语法：

antispam max_attachment_size edit <number>

参数说明：

<number>：单个附件大小(kb)，0 为不限制

注意事项：

无

示例：

ac> antispam max_attachment_size edit 100

全部附件大小上限：

语法：

antispam max_all_attachment_size edit <number>

参数说明：

<number>：全部附件大小(kb)，0 为不限制

注意事项：

无

示例：

ac> antispam max_all_attachment_size edit 10000

## 启用连接频率检查功能：

**语法：**

antispam checkClient {on | off}

**参数说明：**

on： 启用连接频率检查功能

off： 关闭连接频率检查功能

**注意事项：**

无

**示例：**

ac> antispam checkClient on

ac> antispam checkClient off

## 启用发送邮件收件人数量限制功能：

**语法：**

antispam rcpt {on | off}

**参数说明：**

on： 开启发送邮件收件人限制功能

off： 关闭关闭发送邮件人限制功能

**注意事项：**

无

**示例：**

ac> antispam rcpt on

ac> antispam rcpt off

## 限制发送邮件收件人数量：

**语法：**

antispam rcpt edit <number>

**参数说明：**

<number>：同一邮件中实际收件人(包括收件人、抄送人及暗送人)总数量，默认为 0 表示无限制。

**注意事项：**

无

**示例：**

ac> antispam rcpt edit 300

## 启用 SMTP 发送邮件地址白名单功能：

**语法：**

antispam whitemail {on | off}

**参数说明：**

on： 开启 smtp 发送邮件地址白名单功能

off： 关闭 smtp 发送邮件地址白名单功能

**注意事项：**

无

**示例：**

ac> antispam whitemail on

ac> antispam whitemail off

## 启用贝叶斯检查功能：

**语法：**

antispam bayes {on | off}

**参数说明：**

on： 开启贝叶斯检查功能

off： 关闭贝叶斯检查功能

**注意事项：**

无

**示例：**

ac> antispam bayes on

ac> antispam bayes off

## 禁止 OPEN RELAY 功能：

**语法：**

antispam openrelay {on | off}

**参数说明：**

on： 开启禁止虚假邮件路由功能

off： 关闭禁止虚假邮件路由功能，默认为关闭

**注意事项：**

无

**示例：**

ac>antispam openrelay on

ac>antispam openrelay off

## 阻断 TCP 连接功能：

**语法：**

antispam blocksmtpspam {on | off}

**参数说明：**

on： 开启阻断 TCP 连接功能(当检测到垃圾邮件时)，默认开启

off： 关闭阻断 TCP 连接功能

**注意事项：**

无

**示例：**

ac> antispam blocksmtpspam on

ac> antispam blocksmtpspam off

## 邮件主题中加入垃圾邮件标示功能：

**语法：**

antispam spamflag {on | off}

**参数说明：**

on： 开启在邮件主题中加入垃圾邮件标示功能(当检测到垃圾邮件时)

off： 关闭在邮件主题中加入垃圾邮件标示功能，默认关闭

**注意事项：**
无

**示例：**
ac> antispam spamflag on
ac> antispam spamflag off

## 垃圾邮件标示编辑：

**语法：**
antispam spamflag edit <string>

**参数说明：**
<string>：用户可自定义垃圾邮件标示文本，最大长度 1024 字节，默认为"SPAM MAIL FLAG"

**注意事项：**
无

**示例：**
ac> antispam spamflag edit “userdefine_spamflag”

## 发送垃圾邮件日志：

**语法：**
antispam spamlog {on | off}

**参数说明：**
on： 开启发送垃圾邮件日志
off： 关闭发送垃圾邮件日志，默认关闭

**注意事项：**
无

**示例：**
ac> antispam spamlog on
ac> antispam spamlog off

## 8.4.2 服务器黑名单

### 添加服务器黑名单：

**语法：**

antispam blackserver add ip <ip> comment <comment>

**参数说明：**

ip： 服务器黑名单 IP 地址

comment： 服务器黑名单备注

**注意事项：**

无

**示例：**

ac> antispam blackserver add ip “1.2.3.4” comment “blackservercomment”

### 删除服务器黑名单：

**语法：**

antispam blackserver del ip <ip>

**参数说明：**

ip：服务器黑名单 IP 地址

**注意事项：**

无

**示例：**

ac> antispam blackserver del ip “1.2.3.4”

### 导入服务器黑名单配置：

**语法：**

antispam blackserver import <fromfile>

**参数说明：**

import：导入服务器黑名单配置文件名

**注意事项：**

无

**示例：**
ac> antispam blackserver import “/import/filename”

### 导出服务器黑名单配置：

**语法：**
antispam blackserver export <tofile>

**参数说明：**
export：导出服务器黑名单配置文件名

**注意事项：**
无

**示例：**
ac> antispam blackserver export “/export/filename”

## 8.4.3 垃圾邮件地址

### 添加垃圾邮件地址：

**语法：**
antispam spammail add mailaddr <string> comment <comment>

**参数说明：**
mailaddr： 垃圾邮件地址内容
comment： 垃圾邮件地址备注

**注意事项：**
无

**示例：**
ac> antispam spammail add mailaddr “spammail1” comment “spammail1comment”

### 删除垃圾邮件地址：

**语法：**
antispam spammail del mailaddr <string>

**参数说明：**
mailaddr：垃圾邮件地址内容

**注意事项：**
无

**示例：**
ac> antispam spammail del mailaddr “spammail1”

### 导入垃圾邮件地址配置：

**语法：**
antispam spammail import <fromfile>

**参数说明：**
import：导入垃圾邮件地址配置文件名

**注意事项：**
无

**示例：**
ac> antispam spammail import “/import/filename”

### 导出垃圾邮件地址配置：

**语法：**
antispam spammail export <tofile>

**参数说明：**
export：导出垃圾邮件地址配置文件名

**注意事项：**
无

**示例：**
ac> antispam spammail export “/export/filename”

## 8.4.4 主题关键字

### 添加主题关键字：

**语法：**
antispam subjectkeywords add keyword <string> comment <comment>

**参数说明：**

keyword： 主题关键字内容
comment： 主题关键字备注

**注意事项：**
无

**示例：**
ac> antispam subjectkeywords add keyword “subkeywords1” comment “subkeywords1comment”

## 删除主题关键字：

**语法：**
antispam subjectkeywords del keyword <string>

**参数说明：**
keyword：主题关键字内容

**注意事项：**
无

**示例：**
ac> antispam subjectkeywords del keyword “subkeywords1”

## 导入主题关键字配置：

**语法：**
antispam subjectkeywords import <fromfile>

**参数说明：**
import：导入主题关键字配置文件名

**注意事项：**
无

**示例：**
ac> antispam subjectkeywords import “/import/filename”

## 导出主题关键字配置：

**语法：**
antispam subjectkeywords export <tofile>

**参数说明：**
export：导出主题关键字配置文件名

**注意事项：**
无

**示例：**
ac> antispam subjectkeywords export “/export/filename”

## 8.4.5 正文关键字

### 添加正文关键字：

**语法：**
antispam contentKeywords add keyword <string> comment <comment>

**参数说明：**
keyword： 正文关键字内容
comment： 正文关键字备注

**注意事项：**
无

**示例：**
ac> antispam contentKeywords add keyword “ctkeywords1” comment “ctkeywords1comment”

### 删除正文关键字：

**语法：**
antispam contentKeywords del keyword <string>

**参数说明：**
keyword：正文关键字内容

**注意事项：**
无

**示例：**
ac>antispam contentKeywords del keyword “ctkeywords1”

### 导入正文关键字配置：

**语法：**
antispam contentKeywords import <fromfile>

**参数说明：**
import：导入正文关键字配置文件名

**注意事项：**
无

**示例：**
ac>antispam contentKeywords import “/import/filename”

### 导出正文关键字配置：

**语法：**
antispam contentKeywords export <tofile>

**参数说明：**
export：导出正文关键字配置文件名

**注意事项：**
无

**示例：**
ac>antispam contentKeywords export “/export/filename”

## 8.4.6 附件名关键字

### 添加附件名关键字：

**语法：**
antispam attachmentFilename add keyword <string> comment <comment>

**参数说明：**
keyword： 附件名关键字内容
comment： 附件名关键字备注

**注意事项：**
无

**示例：**
ac>antispam attachmentFilename add keyword “attachkey1” comment “attachkey1comment”

### 删除附件名关键字：

**语法：**
antispam attachmentFilename del keyword <string>

**参数说明：**
keyword：附件名关键字内容

**注意事项：**
无

**示例：**
ac> antispam attachmentFilename del keyword “attachkey1”

## 导入附件名关键字配置：

**语法：**
antispam attachmentFilename import <fromfile>

**参数说明：**
import：导入附件名关键字配置文件名

**注意事项：**
无

**示例：**
ac> antispam attachmentFilename import “/import/filename”

## 导出附件名关键字配置：

**语法：**
antispam attachmentFilename export <tofile>

**参数说明：**
export：导出附件名关键字配置文件名

**注意事项：**
无

**示例：**
ac>antispam attachmentFilename export “/export/filename”

## 8.4.7 附件正文关键字

### 添加附件正文关键字：

**语法：**

antispam attachmentContent add keyword <string> comment <comment>

**参数说明：**

keyword： 附件正文关键字内容

comment： 附件正文关键字备注

**注意事项：**

无

**示例：**

ac>antispam attachmentContent add keyword “attachcontent1” comment “attachcontent1comment”

### 删除附件正文关键字：

**语法：**

antispam attachmentContent del keyword <string>

**参数说明：**

keyword：附件正文关键字内容

**注意事项：**

无

**示例：**

ac> antispam attachmentContent del keyword “attachcontent1”

### 导入附件正文关键字配置：

**语法：**

antispam attachmentContent import <fromfile>

**参数说明：**

import：导入附件正文关键字配置文件名

**注意事项：**

无

**示例：**

ac> antispam attachmentContent import “/import/filename”

### 导出附件正文关键字配置：

**语法：**

antispam attachmentContent export <tofile>

**参数说明：**

export：导出附件正文关键字配置文件名

**注意事项：**

无

**示例：**

ac>antispam attachmentContent export “/export/filename”

## 8.4.8 连接频率配置

### POP3 连接数：

**语法：**

antispam client_pop_client edit <number>

**参数说明：**

<number>：限制来自相同客户端网络地址对 pop 邮件服务端口的最大同时 TCP 连接数量，默认为 0 表示无限制。

**注意事项：**

无

**示例：**

ac> antispam client_pop_client edit 1000

### POP3 连接频率：

**语法：**

antispam client_pop_conn edit <number>

**参数说明：**

<number>：限制来自相同客户端网络地址对 pop 邮件服务端口的最大 TCP 连接频率，默认为 0 表示无限制。

**注意事项：**
无

**示例：**
ac> antispam client_pop_conn edit 100

### SMTP 连接频率：

**语法：**
antispam client_smtp_conn edit <number>

**参数说明：**
<number>：限制来自相同客户端网络地址对 smtp 邮件服务端口的最大 TCP 连接频率，默认为 0 表示无限制。

**注意事项：**
无

**示例：**
ac>antispam client_smtp_conn edit 100

### 发送 Email 频率：

**语法：**
antispam client_smtp_send edit <number>

**参数说明：**
<number>：限制来自相同客户端网络地址的单位时间内发送邮件的数量，默认为 0 表示无限制。

**注意事项：**
无

**示例：**
ac> antispam client_smtp_send edit 500

## 8.4.9 发送人白名单

### 添加发送人白名单：

**语法：**
antispam whitemail add mailaddr <string> comment <comment>

**参数说明：**
mailaddr： 发送人白名单邮箱地址
comment： 发送人白名单备注

**注意事项：**
无

**示例：**
ac> antispam whitemail add mailaddr “abc_leadsec@163.com” comment “whitemailcomment”

## 删除发送人白名单：

**语法：**
antispam whitemail del mailaddr <string>

**参数说明：**
mailaddr： 发送人白名单邮箱地址
comment： 发送人白名单备注

**注意事项：**
无

**示例：**
ac> antispam whitemail del mailaddr “abc_leadsec@163.com”

## 导入发送人白名单配置：

**语法：**
antispam whitemail import <fromfile>

**参数说明：**
import：导入发送人白名单配置文件名

**注意事项：**
无

**示例：**
ac> antispam whitemail import “/import/filename”

## 导出发送人白名单配置：

**语法：**
antispam whitemail export <tofile>

**参数说明：**
export：导出发送人白名单配置文件名

**注意事项：**
无

**示例：**
ac> antispam whitemail export “/export/filename”

# 8.5 上网行为管理

## 8.5.1 上网行为管理

### 添加上网行为管理策略：

**语法：**
eim add type policy name <name> comment <comment> apcpolicyid <id> urlpolicyid <id>

**参数说明：**
name： 上网行为管理策略名称
comment： 上网行为管理策略备注
apcpolicyid： 应用识别策略 ID
urlpolicyid： URL 过滤策略 ID

**注意事项：**
无

**示例：**
ac>eim add type policy name “eimpolicy1” comment “eimpolicy1comment” apcpolicyid 1 urlpolicyid 1

### 修改上网行为管理策略：

**语法：**
eim set type policy name <name> {comment <comment> | apcpolicyid <id> | urlpolicyid <id>}

**参数说明：**
name： 上网行为管理策略名称
comment： 上网行为管理策略备注
apcpolicyid： 应用识别策略 ID

urlpolicyid： URL 过滤策略 ID

**注意事项：**
无

**示例：**
ac>eim set type policy name “eimpolicy1” comment “eimnewcomment”
ac>eim set type policy name “eimpolicy1” comment “eimnewcomment” apcpolicyid 3
ac>eim set type policy name “eimpolicy1” comment “eimnewcomment” apcpolicyid 3 urlpolicyid 2

### 删除上网行为管理策略：

**语法：**
eim del type policy policyid <id>

**参数说明：**
policyid：上网行为管理策略 ID

**注意事项：**
无

**示例：**
ac>eim del type policy policyid 1

### 显示上网行为管理策略：

**语法：**
eim show policy

**参数说明：**
无

**注意事项：**
无

**示例：**
eim show policy

## 8.5.2 URL 过滤策略

### 添加 URL 过滤策略：

**语法：**

urlblock add type policy name <name> comment <comment> policyid <id>

**参数说明：**

name： URL 过滤策略名称
comment： URL 过滤策略备注
policyid： 策略参考的已有的 URL 过滤策略 ID

**注意事项：**

无

**示例：**

ac>urlblock add type policy name “urlblock1” comment “urlblock1comment” policyid 1

## 修改 URL 过滤策略：

**语法：**

urlblock set type policy name <name> signature <all | signame>
{
enabled {off | on} drop {off | on} log {off | on} alertmail {off | on}
resetsend {off | on} resetrecv {off | on} sound {off | on}
}

**参数说明：**

name： URL 过滤策略名称
signature： URL 类别，all:选择所有的 URL 类别，signame:具体的 URL 类别名称
enable： URL 检测是否启用
drop： 检测到此类别 URL 是否丢弃
log： 检测到此类别 URL 是否记录日志
alertmail： 检测到此类别 URL 是否是否发送告警邮件
resetsend： 检测到此类别 URL 是否重置客户端
resetrecv： 检测到此类别 URL 是否重置服务器
sound： 检测到此类别 URL 是否发出告警声音

**注意事项：**

当 signature 选择为 all 时，后面的动作只能指定一个

**示例：**

ac>urlblock set type policy name “urlblock1” signature all enable off
ac>urlblock set type policy name “urlblock1” signature “旅游出行” enable on drop off log on alertmail off resetsend on resetrecv on sound on

## 删除 URL 过滤策略：

**语法**

urlblock del type policy policyid <id>

**参数说明：**
policyid：URL 过滤策略 ID

**注意事项：**
无

**示例：**
ac>urlblock del type policy policyid 1

### 显示 URL 过滤策略：

**语法：**
urlblock show policy

**参数说明：**
无

**注意事项：**
无

**示例：**
ac>urlblock show policy

## 8.5.3 应用识别策略

### 添加应用识别策略：

**语法：**
apc add type policy name <name> comment <comment> policyid <id>

**参数说明：**
name： 应用识别策略名称
comment： 应用识别策略备注
policyid： 策略参考的已有的应用识别策略 ID

**注意事项：**
无

**示例：**
ac>apc add type policy name “apcpolicy1” comment “apcpolicy1comment” policyid 1

## 修改应用识别策略：

**语法：**

apc set type policy name <name> {group <name> | signature <name>}
{
{[active {on | off}] | [log {on | off} ] | [alertmail {on | off}]}
}

**参数说明：**

name： 应用识别策略名称
group： 特征组名称
signature： 特征名称
active： 应用识别是否生效
log： 是否记录日志
alertmail： 是否发送告警邮件

**注意事项：**

选择 group 时，后面的动作只能选择一个

**示例：**

ac>apc set type policy name “apcpolicy1” group “p2p_download” active on
ac>apc set type policy name “apcpolicy1” signature “BITTORRENT” active on log on alertmail off

## 删除应用识别策略：

**语法：**

apc del type policy policyid <id>

**参数说明：**

policyid：应用识别策略 ID

**注意事项：**

无

**示例：**

ac>apc del type policy policyid 3

## 显示应用识别策略：

**语法：**

apc show policy

**参数说明：**

无

**注意事项：**
无

**示例：**
ac>apc show policy

# 8.6 入侵检测模式

## 添加入侵检测模式规则：

**语法：**
IPv4 格式：
rule add type uids name <name> [id <id>] [sa {any | <name> | <ip>}] [da {any | <name> | <ip>}] [iif {any | <interface>}] [service {any | <name>}] [time {<name> | none}] [smac <mac>] [avpolicy <number>] [ipspolicy <number>] [active {on | off}] [comment <comment>]

IPv6 格式：
rule ipv6 add type uids name <name> [id <id>] [srcip {<ip6> | ipname <name> | any}] [dstip {<ip6> | ipname <name> | any}] [smac <mac>] [iif {any | <name>}] [service {any | <name>}] [avpolicy <number>] [ipspolicy <number>] [active {on | off}] [comment <comment>]

**参数说明：**
name： 安全规则的名称
id： 安全规则的序号
sa： IPv4 格式的源 IP 地址，可以使用单个 IP 地址、IP 地址/子网掩码、地址定义、地址组定义、“any”，默认为“any”
srcip： IPv6 格式的源 Ip 地址，可以使用单个 IP 地址、IP 地址/子网掩码、地址定义、地址组定义、“any”，默认为“any”
da： IPv4 格式的目的 IP 地址，可以使用单个 IP 地址、IP 地址/子网掩码、地址定义、地址组定义、“any”，默认为“any”
dstip： IPv6 格式的目的 IP 地址，可以使用单个 IP 地址、IP 地址/子网掩码、地址定义、地址组定义、“any”，默认为“any”
iif： 流入网口
service：服务，可以使用服务、服务组
time： 时间控制，可以使用时间定义、时间组定义、“none”，默认为不使用时间控制
smac： 源 MAC 地址，默认为“any”
avpolicy：
ipspolicy：
active： 是否生效，默认为生效

comment：规则注释

**注意事项：**

无

**示例：**

ac>rule add type uids name “uidsv4” id 1 sa any da any iif “eth0” service any time none avpolicy 4 ipspolicy 5 active on comment “uidsv4comment”

ac>rule ipv6 add type uids name “uidsv6” id 1 srcip any dstip any iif “eth1” service any time none avpolicy 5 ipspolicy 4 active on comment “uidsv6comment”

## 修改入侵检测模式规则：

**语法：**

IPv4 格式：

rule set id <id> [type uids] [newid <id>] [sa {any | <name> | <ip>}] [da {any | <name> | <ip>}] [iif {any | <interface>}] [service {any | <name>}] [time {<name> | none}] [smac <mac>] [avpolicy <number>] [ipspolicy <number>] [active {on | off}] [comment <comment>]

IPv6 格式;

rule ipv6 set id <id> [type uids] [newid <id>] [srcip {<ip6> | ipname <name> | any}] [dstip {<ip6> | ipname <name> | any}] [smac <mac>] [iif {any | <name>}] [service {any | <name>}] [avpolicy <number>] [ipspolicy <number>] [active {on | off}] [comment <comment>]

**参数说明：**

id： 指定欲修改的安全规则的序号

type： 修改安全规则的类型

newid： 修改安全规则的序号

sa： IPv4 格式的源 IP 地址，可以使用单个 IP 地址、IP 地址/子网掩码、地址定义、地址组定义、“any”，默认为“any”

srcip： IPv6 格式的源 Ip 地址，可以使用单个 IP 地址、IP 地址/子网掩码、地址定义、地址组定义、“any”，默认为“any”

da： IPv4 格式的目的 IP 地址，可以使用单个 IP 地址、IP 地址/子网掩码、地址定义、地址组定义、“any”，默认为“any”

dstip： IPv6 格式的目的 IP 地址，可以使用单个 IP 地址、IP 地址/子网掩码、地址定义、地址组定义、“any”，默认为“any”

iif： 流入网口

service：服务，可以使用服务、服务组

time： 时间控制，可以使用时间定义、时间组定义、“none”，默认为不使用时间控制

smac： 源 MAC 地址，默认为“any”

avpolicy：

ipspolicy：

active： 是否生效，默认为生效

comment：规则注释

**注意事项：**
无

**示例：**
ac>rule set type uids name “uidsv4” id 1 sa any da any iif “eth0” service any time none avpolicy 4 ipspolicy 5 active on comment “uidsv4comment”
ac>rule ipv6 set type uids name “uidsv6” id 1 srcip any dstip any iif “eth1” service any time none avpolicy 5 ipspolicy 4 active on comment “uidsv6comment”

### 删除入侵检测模式规则：

**语法：**
IPv4 格式：
rule del id <id>

IPv6 格式：
rule ipv6 del id <id>

**参数说明：**
id：指定欲删除的安全规则的序号

**注意事项：**
无

**示例：**
ac>rule del id 1
ac>rule ipv6 del id 2

# 8.7 抗扫描

## 8.7.1 抗扫描设置

### 修改端口扫描设置：

**语法：**
antiscan set portscan {option} {on | off} value <value> blocktime <blocktime>
option: active, log, mail, block, drop

**参数说明：**

portscan： 端口扫描
active： 抗扫描是否启用
log： 是否记录日志
mail： 是否发送告警邮件
block： 是否阻断
drop： 是否丢弃
value： 检测阈值
blocktime： 阻断时间

**注意事项：**
无

**示例：**
ac>antiscan set portscan active on log on mail off block on drop off value 12 blocktime 15

## 显示端口扫描配置：

**语法：**
antiscan show portscan

**参数说明：**
无

**注意事项：**
无

**示例：**
ac>antiscan show portscan

## 修改主机扫描配置：

**语法：**
antiscan set hostscan {option} {on | off} value <value> blocktime <blocktime>
option: active, log, mail, block, drop

**参数说明：**
hostscan： 主机扫描
active： 抗扫描是否启用
log： 是否记录日志
mail： 是否发送告警邮件
block： 是否阻断
drop： 是否丢弃
value： 检测阈值
blocktime： 阻断时间

**注意事项：**
无

**示例：**
ac>antiscan set hostscan active on log on mail off block on drop off value 12 blocktime 15

### 显示主机扫描配置：

**语法：**
antiscan show hostscan

**参数说明：**
无

**注意事项：**
无

**示例：**
ac>antiscan show hostscan

## 8.7.2 白名单

### 添加白名单：

**语法：**
antiscan add whitelist { ipv4 ip <single_ip> netmask <netmask> | ipv6 ip <single_ipv6> netmask <number> }

**参数说明：**
ip： ipv4 或者 ipv6 格式的 IP 地址
netmask： 对应 ip 格式的子网掩码,<netmask>:ipv4 的子网掩码，<number>:ipv6 子网掩码

**注意事项：**
IP 地址和子网掩码的对应

**示例：**
ac>antiscan add whitelist ipv4 ip 1.2.3.4 netmask 255.255.255.0
ac>antiscan add whitelist ipv6 ip 1::2 netmask 80

### 删除白名单：

**语法：**

antiscan del whitelist { ipv4 ip <single_ip> | ipv6 ip <single_ipv6> }

**参数说明：**

ip：ipv4 或者 ipv6 格式的 IP 地址

**注意事项：**

无

**示例：**

ac>antiscan del whitelist ipv4 ip 1.2.3.4

ac>antiscan del whitelist ipv6 ip 1::2

### 显示白名单：

**语法：**

antiscan show whitelist

**参数说明：**

无

**注意事项：**

无

**示例：**

ac>antiscan show whitelist

## 8.8 主机服务黑名单

### 添加主机服务黑名单

**语法**：

utm_blacklist add id<id> event_type <event_type> af <af> addr_type <addr_type> addr <addr> port_type <port_type> port<port> proto<proto> block_time <block_time>

**参数说明**：

(25536) event_type: 代表事件类型，只接收整型数，只能是这些数字之一：

2-AV（防病毒）,3-IPS（入侵检测）,4-URL（URL 过滤）,6-APC（应用识别）,7-PC（协议控制）,8-IUT（主动防御）,11-SCAN（漏洞扫描）

(25537) af:代表协议簇，只接收整型，只能是这些数字之一：0-IPv4，1-IPv6

(25538) addr_type：代表 ip 地址类型，只接收整型数，只能是这些数字之一：0-源地址，1-目的地址

(25539) address：代表 ip 地址，只接收合法的点分十进制形式的 ip 地址（以字符串的形式），例如:“10.1.5.200”

(25540) port_type: 代表端口类型，只接收整型数，只能是这些数字之一：0-源端口，1-目的端口

(25541) port：代表端口类型，只接受整型数，端口号必须合法，即在 0-65535 之间

(25542) proto：代表协议类型，只接收合法的、如“tcp”“udp”“icmp”等字符串

(25543) block_time:代表阻止时间，只接收 0-43200 之间的整数,0 表示永久阻断，这里的单位是分钟

**注意事项**：针对不同的事件，ip 地址类型和端口类型是不同的，如下表所示：

| 事件说明 | 地址类型 | 端口类型 | 事件名称 |
|---|---|---|---|
| 病毒防护事件 | 源地址 | 源端口 | 防病毒 |
| 入侵防护事件 | 源地址 | 目的端口 | 入侵检测 |
| url 过滤事件 | 目的地址 | 目的端口 | URL 过滤 |
| 绿色上网事件 | 目的地址 | 目的端口 | 绿色上网 |
| 协议控制事件 | 目的地址 | 目的端口 | 协议控制 |
| 主动防御事件 | 目的地址 | 目的端口 | 主动防御 |
| 漏洞扫描事件 | 目的地址 | 目的端口 | 漏洞扫描 |

如果不按上面的表进行该命令行操作，则不能成功添加相应的 iptables 规则。

**示例**：

ac>utm_blacklist add id 1 event_type 2 af 0 addr_type 0 addr “2.2.2.200” port_type 0 port 80 proto “tcp”block_time 30

## 显示主机服务黑名单

**语法**：

utm_blacklist show [ id < id > ]

**参数说明**：

如果命令行是两个参数（utm_blacklist show），则会将所有未过期的主机服务黑名单予以显示。如果命令行是四个参数（utm_blacklist show id ‘x’）,则只显示 id 为 x 的主机服务黑名单。

**示例**：

**ac> utm_blacklist show**

**ac> utm_blacklist show id 2**

## 更改主机服务黑名单的阻止时间

**语法**：

utm_blacklist set id < id > block_time < block_time >

**参数说明**：

无

**示例**：

ac>utm_blacklist set id 2 block_time 60

## 删除主机服务黑名单的记录

**语法**：utm_blacklist del id < id >

**参数说明**：
无

**示例**：
ac>utm_blacklist del id 2

# 第9章 用户认证

## 9.1 用户认证

### 9.1.1 接入规则(connect_rule)

**添加接入规则：**

**语法：**
connect-rule add rulename<name>
[ client-check { version-check <string> | proc-check <string> } ] *

**参数说明：**

| | |
|---|---|
| rulename | 设置接入规则名称，1-15 位中文、字母、数字、减号、下划线组合 |
| client-check | 开启客户端检查 |
| version-check | 版本检查，数字和小数点的组合，可输入多个，逗号分隔，单条最大长度 50 |
| proc-check | 进程检查，可输入多个，逗号分隔，单条最大长度 50，多个进程名之间不可重复 |

**注意事项：**
如果开启客户端检查，则版本检查和进程检查，至少要有一个。也可以两项都配置。
进程检查只支持 windows 进程名，大小写敏感，要写后缀名。
版本检查：版本列表中只要有一个正确的就可以通过检查。
进程检查：运行认证客户端的电脑上必须全部运行进程列表所列的进程，才可能认证通过。

**示例：**
ac>connect-rule add rulename rule1 client-check version-check 1.20 proc-check

auth_client.exe

## 修改接入规则

**语法：**

connect-rule set rulename<name>
[ client-check { version-check <string> | proc-check <string> } ] *

**参数说明：**

| | |
|---|---|
| rulename | 要修改的接入规则名称 |
| client-check | 开启客户端检查 |
| version-check | 版本检查，数字和小数点的组合，可输入多个，逗号分隔，单条最大长度 50 |
| proc-check | 进程检查，可输入多个，逗号分隔，单条最大长度 50，多个进程名之间不可重复 |

**注意事项：**

如果开启客户端检查，则版本检查和进程检查，至少要有一个。也可以两项都配置。
进程检查只支持 windows 进程名，大小写敏感，要写后缀名。

**示例：**

```
ac>connect-rule set rulename rule1 client-check version-check 2.1
```

## 删除接入规则

**语法：**

connect-rule del { rulename <name> | all }

**参数说明：**

| | |
|---|---|
| rulename | 要删除的接入规则名称 |
| all | 删除所有的接入规则 |

**注意事项：**

当接入规则被用户引用的时候，该规则不能被删除，除非先解除引用。

**示例：**

```
ac>connect-rule del rulename rule1
ac>connect-rule del all
```

## 显示接入规则

**语法：**

connect-rule show {rulename <name> | all }

**参数说明：**

| | |
|---|---|
| rulename | 要显示的接入规则名称 |
| all | 显示所有的接入规则 |

**示例：**

```
ac>connect-rule show rulename rule1
ac>connect-rule show all
```

### 9.1.2 用户管理(user)

## 添加用户

**语法：**

user add username <name> auth-type { local-pwd pwd <string> | local-cert | cert-pwd pwd <string> | dyn-pwd pwd <string> [ sn < string > ] | vip } [ role <string> ] [ true-name <string> ] [bind-ip4 <ip> ] [ bind-mac <string> ] [ active {on | off } ] [ modify-pwd-allow { on | of } ] [ first-change-pwd { on | of } ] [available-period <int> ] [pwd-available-period<int> ] [ connect-rule <string> ] [comment <string> ]

**参数说明：**

| | |
|---|---|
| username | 登录用户名称，1-15 位中文、字母、数字、减号、下划线组合 |
| auth-type | 认证类型 |
| local-pwd | 本地密码认证 |
| local-cert | 本地证书认证 |
| cert-pwd | 本地证书+口令认证 |
| dyn-pwd | 动态口令+口令认证 |
| vip | VIP 免认证 |
| pwd | 密码，满足全局认证参数配置的密码复杂度的要求，最长 20 |
| sn | 要导入的 sn 文件名称 |
| role | 所属角色名称，可输入多个，以逗号分开 |
| true-name | 真实用户名，命名规则同 username。可选 |
| bind-ip4 | 绑定 IP 地址，不能输入全 0,255，环回及多播地址 |
| bind-mac | 绑定 MAC 地址，xx:xx:xx:xx:xx:xx 或者 xx-xx-xx-xx-xx-xx,<br>不能输入多播 mac |
| active： | 该用户是否生效 on 或者 off，默认生效 |
| modify-pwd-allow | 是否允许修改密码 on 或者 off，默认允许 |
| first-change-pwd | 首次登录是否修改密码，on 或者 off，默认为认证参数的全局配置 |
| available-period | 用户有效期，单位天，0 为永久生效，默认永久生效 |
| pwd-available-period | 密码有效期，单位天，0 为永久生效，默认为认证参数的全局配置 |
| connect-rule | 接入规则对象。仅允许输入一个 |
| comment | 认证策略的注释，0-255 个字符，不含非法字符 “ '%*!\|>;&<()+?{}[]#^ ” |

**注意事项：**

用户有效期和密码有效期为创建日期开始计算，当天计算为 1 天，以夜里 0 点为划分。
经过夜里 0 点则为第 2 天计时。

**示例：**

```
ac>user add username user1 auth-type local-pwd pwd hello1234
```

## 修改用户

**语法：**

user set username <name> auth-type { local-pwd [ pwd <string> ] | local-cert | cert-pwd [ pwd <string> ] | dyn-pwd [ pwd <string> ] [ sn < string > ] | vip } [ role <string> ] [ true-name <string> ] [ < bind-ip4 > <ip> ] [ bind-mac <string> ] [ active {on | off } ] [ modify-pwd-allow { on | of } ] [ first-change-pwd { on | of } ] [available-period <int> ] [pwd-available-period<int> ] [ connect-rule <string> ] [comment <string> ]

**参数说明：**

| | |
|---|---|
| username | 登录用户名称，1-30 位中文、字母、数字、减号、下划线组合 |
| auth-type | 认证类型 |
| local-pwd | 本地密码认证 |
| local-cert | 本地证书认证 |
| cert-pwd | 本地证书+口令认证 |
| dyn-pwd | 动态口令+口令认证 |
| vip | VIP 免认证 |
| pwd | 密码，满足全局认证参数配置的密码复杂度的要求，最长 20 |
| sn | 要导入的 sn 文件名称 |
| role | 所属角色名称，可输入多个，以逗号分开 |
| true-name | 真实用户名，命名规则同 username。可选 |
| bind-ip4 | 绑定 IP 地址，不能输入全 0,255，环回及多播地址 |
| bind-mac | 绑定 MAC 地址, xx:xx:xx:xx:xx:xx 或者 xx-xx-xx-xx-xx-xx，不能输入多播 mac |
| active： | 该用户是否生效 on 或者 off，默认生效 |
| modify-pwd-allow | 是否允许修改密码 on 或者 off，默认允许 |
| first-change-pwd | 首次登录是否修改密码，on 或者 off，默认为认证参数的全局配置 |
| available-period | 用户有效期，单位天，0 为永久生效，默认永久生效 |
| pwd-available-period | 密码有效期，单位天，0 为永久生效，默认为认证参数的全局配置 |
| connect-rule | 接入规则对象。仅允许输入一个 |
| comment | 认证策略的注释，0-255 个字符，不含非法字符 “ '%*!\|>;&<()+?{}[]#^ ” |

**注意事项：**

用户有效期和密码有效期为创建日期开始计算，当天计算为 1 天，以夜里 0 点为划分。
经过夜里 0 点则为第 2 天计时。
如果原来用户有密码，则本地修改可以不修改密码。

**示例：**

```
ac>user set username user1 auth-type local-cert
```

## 删除用户

**语法：**

user del {username <name> | all }

**参数说明：**

| | |
|---|---|
| username | 要删除的用户名称 |
| all | 删除所有的用户 |

**注意事项：**

如果该用户在线，可以删除该用户，删除的同时该用户也被下线。

**示例：**

```
ac>user del username user1
ac>user del all
```

## 显示用户

**语法：**

user show {username <name> | all }

**参数说明：**

| | |
|---|---|
| username | 要显示的用户名称 |
| all | 显示所有的用户 |

**示例：**

```
ac>user show username user1
ac>user show all
user_name          create_date        valid_time(days)    role_name
user1              2012/01/11         FOREVER             role1
```

## 显示在线用户总数

**语法：**

user show online total

**示例：**

```
ac>user show online total
```

```
The online user total:1
```

## 显示所有用户总数

**语法：**

user show total

**示例：**

```
ac>user show total
The user total:1
```

## 显示在线用户

**语法：**

user show online [from <num1> to <num2> ]

**参数说明：**

| | |
|---|---|
| from | 从第几个在线用户开始显示 |
| to | 到第几个在线用户结束显示 |

**注意事项：**

如果没有配置 from /to ,则默认显示 1024 个

最多每次显示 1024 个，即 to – from <= 1024

**示例：**

```
ac>user show online
user_name auth_type logon_ip online_time(min) logon_time        role_name
user1     LOCAL-PWD 1.0.0.23  5               2012/01/11 23:49:13  role1
```

## 显示锁定用户

**语法：**

user show lock

**示例：**

```
ac>user show lock
user_name           unlock_time           role_name
user1               2012/01/12 01:07:54   role1
```

## 强制用户下线

**语法：**
user break username <name>

**参数说明：**
username 要强制下线的用户名称
**注意事项：**
当该用户被强制下线以后，其将会被永久禁止登录，除非管理员修改该用户的状态属性为启用

**示例：**
```
ac>user break username user1
```

## 强制所有用户下线

**语法：**
user break all

**参数说明：**
all 强制所有用户下线

**注意事项：**
当所有用户被强制下线以后，不会禁用全部用户，可以继续登录。

**示例：**
```
ac>user break all
```

## 重置用户时间

**语法：**
user reset username <name> time

**参数说明：**
username 要重置的用户名称
time 重置用户的在线时间

**注意事项：**
如果用户所属角色设置了时间限制，当用户使用完分配的时间，该用户就会处于资源已耗完状态，用此命令可以将用户状态恢复为初始状态，时间将重新开始计算；该功能仅适用于本地认证模式。

**示例：**

```
ac>user reset username user1 time
```

## 重置用户密码

**语法：**

user reset username <name> password < string>

**参数说明：**

| | |
|---|---|
| username | 要重置的用户名称 |
| password | 重置的密码，该密码满足全局认证参数配置的密码复杂度 |

**注意事项：**

**示例：**

```
ac>user reset username user1 password  hello12#$56
```

## 锁定用户

**语法：**

user lock username <name>  time < integer>

**参数说明：**

| | |
|---|---|
| username | 要锁定的用户名称 |
| time | 锁定的时间，单位分钟，0 为永久锁定 |

**注意事项：**

**示例：**

```
ac>user lock username user1 time 60
```

## 解锁用户

**语法：**

user unlock username <name>

**参数说明：**

| | |
|---|---|
| username | 要解锁的用户名称 |

**注意事项：**

**示例：**

```
ac>user unlock username user1
```

## 导入 SN 文件

**语法：**

user set username <string> import-sn <filename>

**参数说明：**

| | |
|---|---|
| username | 要导入 SN 的用户名称 |
| import-sn | 要导入的 SN 文件名称 |

**注意事项：**

只有动态口令+口令的认证方式的用户，才可以导入 SN 文件

在使用 cli 的时候，确保要导入的 SN 文件已经被上传

**示例：**

```
ac>user set username user1  import-sn SN9132368.txt
```

## 动态密码同步

**语法：**

user set username <string> syndynpass <string> dyntime <num> dynclock <string>

**参数说明：**

| | |
|---|---|
| username | 要动态同步的用户名称 |
| syndynpass | 用户的动态密码 |
| dyntime | 同步动态密码时间，暂时设置为 0 |
| dynclock | 同步动态密码时钟，暂时设置为 0 |

**注意事项：**

该命令会同步指定用户的动态密码，安全网关的时间与北京时间如果相差大于 5 分钟同步失败。

**示例：**

```
ac>user set username user1  syndynpass  12345678 dyntime 0 dynclock 0
```

### 9.1.3 角色管理(role)

## 添加角色

**语法：**

role add rolename <name> normal [time <num>] [always_online {on|off}]
[comment <string>]

**参数说明：**

| | |
|---|---|
| rolename | 设置角色名称，1-15 位中文、字母、数字、减号、下划线组合 |
| normal | 普通用户角色 |
| time | 角色分配时间，单位：分钟，无默认 |
| always_online | 永远在线标识，配置该参数后，该角色下的用户将不做空闲时间判断，不会自动注销，on 或者 off |
| comment | 认证策略的注释，0-255 个字符，不含非法字符 “ '%*!\|>;&<()+?{}[]#^ ” |

**示例：**

```
ac>role add rolename role1 normal time 60 always_online on comment ″one hour″
```

## 修改角色

**语法：**

role set rolename <name> normal [time <num>] [always_online {on|off}]
[comment <string>]

**参数说明：**

| | |
|---|---|
| rolename | 设置角色名称 |
| normal | 普通用户角色 |
| time | 角色分配时间，单位：分钟，无默认 |
| always_online | 永远在线标识，配置该参数后，该角色下的用户将不做空闲时间判断，不会自动注销，on 或者 off |
| comment | 认证策略的注释，0-255 个字符，不含非法字符 “ '%*!\|>;&<()+?{}[]#^ ” |

**示例：**

```
ac>role set rolename role1 normal time 30 always_online off
```

## 删除角色

**语法：**
role del {rolename <name>|all}

**参数说明：**
rolename 要删除的角色名称
all 删除所有的角色

**注意事项：**
当角色被用户或者安全策略，带宽策略引用的时候，不能被删除，除非先解除引用

**示例：**
```
ac>role del rolename role1
ac>role del all
```

## 重置角色时间

**语法：**
role reset rolename <name> time

**参数说明：**
rolename 要重置时间的角色名称

**注意事项：**
该命令将隶属于该角色的所有用户的时间重置为0，这些用户的时间将重新开始计算。

**示例：**
```
ac>role reset rolename role1 time
```

## 显示角色

**语法：**
role show {rolename <name>|all}

**参数说明：**
rolename 要显示的角色名称
all 显示所有角色的信息

**示例：**
```
ac>role show all
ac>role show rolename role2
role_name    creater      create_time      time(min)        user
role2        root         2012/01/10       525600           user1
```

### 9.1.4 认证策略(auth-policy)

## 添加认证策略

**语法：**

auth-policy add policyname <name> {ingress <string> | ipv4 {<name> |
<ip | ip/mask | ip:ip>} | port <string>}* [active {on | off} ] [comment <comment>]

**参数说明：**

| | |
|---|---|
| policyname | 设置认证策略名称，1-15 位中文、字母、数字、减号、下划线组合 |
| ingress | 流入网口，已经启用的网络接口设备 |
| ipv4 | 源地址限定，可以输入 ip:单个 ip，ip/mask: ip/掩码，ip:ip ip 地址段,或者一个地址对象（包括地址定义、地址组定义、服务器地址定义）<br>不能输入全 0,255，环回及多播地址 |
| port | 目的端口限定，1-65535，以逗号分割，最多可输入 10 个 |
| active | 是否启用该认证策略，on 或者 off, 默认启用 |
| comment | 认证策略的注释，0-255 个字符，不含非法字符 “ '%*!\|>;&<()+?{}[]#^ ” |

**注意事项：**

ingress，ipv4，port 三者至少要有一个。

建议在配置的时候，配置好 web server 的端口，否则会阻拦所有的服务，一般的 http 服务的端口默认为 80。

**示例：**

```
ac>auth-policy add policyname pcy4  ipv4 200.0.0.1:200.0.0.100  port 80
```

## 修改认证策略

**语法：**

auth-policy set policyname <name> {ingress <string> | ipv4 {<name> |
<ip | ip/mask | ip:ip>} | port <string>}*  [active {on | off} ] [comment <comment>]

**参数说明：**

| | |
|---|---|
| policyname | 要修改的认证策略名称 |
| ingress | 流入网口，已经启用的网络接口设备 |
| ipv4 | 源地址限定，可以输入 ip:单个 ip，ip/mask: ip/掩码，ip:ip ip 地址段,或者一个地址对象（包括地址定义、地址组定义、服务器地址定义）<br>不能输入全 0,255，环回及多播地址 |
| port | 目的端口限定，1-65535，以逗号分割，最多可输入 10 个 |

| | |
|---|---|
| active | 是否启用该认证策略，on 或者 off, 默认启用 |
| comment | 认证策略的注释，0-255 个字符，不含非法字符 “ '%*!\|>;&<()+?{}[]#^ ” |

**注意事项：**

ingress，ipv4，port 三者至少要有一个。

**示例：**

```
ac>auth-policy set policyname pcy4  ipv4 1.0.0.1:1.0.0.50 active on
```

## 删除认证策略

**语法：**

auth-policy del {policyname <name> | all }

**参数说明：**

| | |
|---|---|
| policyname | 要删除的认证策略名称 |
| all | 删除所有的认证策略 |

**示例：**

```
ac>auth-policy del policyname pcy4
ac>auth-policy del all
```

## 显示认证策略

**语法：**

auth-policy show {policyname <name> | all }

**参数说明：**

| | |
|---|---|
| policyname | 要显示的认证策略名称 |
| all | 显示所有的认证策略 |

**示例：**

```
ac>auth-policy show policyname pcy4
ac>auth-policy show all
policy_name   ingress         address                   active          port
pcy1          eth1                                    off
pcy4                        200.0.0.1:200.0.0.100     on
pcy6                                                  on          80,90
```

## 修改认证策略状态

**语法：**
auth-policy active policyname <name> { on | off }

**参数说明：**

| | |
|---|---|
| policyname | 要显示的认证策略名称 |
| on | 使认证策略生效 |
| off | 使认证策略不生效 |

**示例：**
```
ac>auth-policy active policyname pcy1 off
```

### 9.1.5 认证服务器(auth server)

## 本地端口配置

**语法：**
auth server localport <num>

**参数说明：**

| | |
|---|---|
| localport | 设置认证端口，只允许输入数字，输入范围为 1024-65535，默认值 9998 |

**注意事项：**
如果认证端口已经被占用，请输入其他的端口
当有用户已经登录的时候，不能修改认证端口。

**示例：**
```
ac>auth server localport 9998
```

## 日志配置

**语法：**
auth server log { on | off }

**参数说明：**

| | |
|---|---|
| log | 设置是否启用日志，取值范围 on 或者 off。 |

**示例：**
```
ac>auth server log off
```

# 本地认证配置

**语法：**

auth server workmode local

**参数说明：**

workmode 设置认证服务器的工作模式，local 为本地认证方式

**示例：**

ac>auth server workmode local

# LDAP 认证配置

**语法：**

auth server workmode ldap ip <ip> timeout <num> authport <num> basename <string> managername <sting> managersecret <string> type <string> dnmode <string>

**参数说明：**

| | |
|---|---|
| workmode | 设置认证服务器的工作模式，ldap 为 ldap 认证方式 |
| ip | 设置 ldap 服务器的 ip 地址，不允许输入全 0，255，环回及多播地址 |
| timeout | 设置超时重传时间，范围 3s-10s,默认 3 秒 |
| authport | 设置 ldap 认证服务器的认证监听端口，输入范围为 1-65534，默认 tcp 端口 389 |
| basename | 设置 ldap 的基准名，即 ldap 目录树的根条目，最大 200 个字符 |
| managername | 设置 ldap 服务器的管理员用户名，不用输入 dn，最大 50 个字符 |
| managersecret | 设置 ldap 服务器的管理员密码，最大 50 个字符 |
| type | 设置 ldap 服务器的认证方式，md5 或者匿名，默认 md5 |
| dnmode | 设置 ldap 的 dn 模式，即目录树从这儿开始搜索用户，最大 200 个字符 |

**注意事项：**

以上均为必选参数，请按序输入

**示例：**

ac>auth server workmode ldap ip 1.0.0.101 timeout 5 authport 389 basename dc=example,dc=com managername manager managersecret secret type md5 dnmode ou=Group,dc=example,dc=com

# RADIUS 认证配置

**语法：**

auth server workmode radius ip <ip> timeout <num> authport <num> auditport <num> secret <string> type

<string>

**参数说明：**

| | |
|---|---|
| workmode | 设置认证服务器的工作模式，radius 为 radius 认证方式 |
| ip | 设置 radius 服务器的 ip 地址，不允许输入全 0，255，环回及多播地址 |
| timeout | 设置超时重传时间，范围 3s-10s,默认 3 秒 |
| authpor | 设置 radius 认证服务器的认证监听端口，输入范围为 1-65534，默认 udp 端口 1812 |
| auditport | 设置 radius 认证服务器的审计监听端口，输入范围为 1-65534，默认 udp 端口 1813 |
| secret | 设置代理 freeradius 的共享密钥，1-16 个字母、数字、减号、以及下划线组成 |
| type | 设置 radius 服务器的认证方式，chap,pap,ms-chap，默认 chap |

**注意事项：**

以上均为必选参数，请按序输入

**示例：**

ac>auth server workmode radius ip 1.0.0.101 timeout 5 authport 1812 auditport 1813 secret testing123 type chap

## AD 认证配置

**语法：**

auth server workmode ad ip <ip> managername <sting> managersecret <string> realm <string> netbios <string>

**参数说明：**

| | |
|---|---|
| workmode | 设置认证服务器的工作模式，ad 为 ad 认证方式 |
| ip | 设置 ad 服务器的 ip 地址，不允许输入全 0，255，环回及多播地址 |
| managername | 设置 ad 服务器的管理员用户名，最大 50 个字符 |
| managersecret | 设置 ad 服务器的管理员密码，最大 50 个字符 |
| realm | 设置 ad 的域名 |
| netbios | 设置 ad 的 netbios 名，1-15 个字符，英文大小字母、数字、“-”，“_”、“.”组成 |

**注意事项：**

以上均为必选参数，请按序输入

**示例：**

ac>auth server workmode ad ip 1.0.0.31 managername administrator managersecret shangyp realm leadsecvpn.com netbios LEADSECVPN

## 重定向 url 配置

**语法：**

auth server redirecturl <string>

**参数说明：**

redirecturl 设置重定向 url

**参数说明：**

重定向 url，默认为 https://10.1.5.254:10008/cgi-bin/webui?op=pcm_auth_check_online，暂时只支持修改 ip 和端口

**注意事项：**

暂时不支持在 cli 下输入带有“？”的 URL, 可以在 WEB 界面上配置
当有用户已经登录的时候，不能修改重定向 URL。

**示例：**

```
ac>auth server redirecturl https://10.1.5.254:10008/cgi-bin/webui?op=pcm_auth_check_online
```

## 显示认证服务器配置

**语法：**

**auth server show**

**示例：**

```
ac> auth server show
AUTH SERVER INFO:
    workmode            :   local
    redirecturl         :   https://10.1.5.254:10008/cgi-bin/webui?op=pcm_auth_check_online
    localport           :   9998
    log                 :   off
```

### 9.1.6 认证参数(auth config)

## 认证参数配置

**语法：**

auth config forcemodify {yes|no} pwdcomplex {none|weak|normal|good|better|great} maxloadtimes <num> unlocktime <num> pwdperiod <num> pwdremind <num> idletime <num>

**参数说明：**

| | |
|---|---|
| forcemodify | 设置首次登录是否强制修改密码，yes 或者 no |
| pwdcomplex | 设置密码复杂度要求: 所有密码最长 20 个字符，缺省为 normal。 |
| none | 无，不要求密码复杂度 |
| weak | 较弱，4～8 个字符长度口令 |

| | |
|---|---|
| normal | 一般，8 个字符长度以上（不包含 8）的口令，但至少满足以下条件之一：<br>英文大写字母（从 A 到 Z）<br>英文小写字母（从 a 到 z）<br>10 个基本数字（从 0 到 9）<br>非字母字符（如：！,$,#,%）<br>口令达到 12 字符长度，最长 20 个字符 |
| good | 较好，8 个字符长度以上（不包含 8）的口令，但至少满足以下条件之二：<br>英文大写字母（从 A 到 Z）<br>英文小写字母（从 a 到 z）<br>10 个基本数字（从 0 到 9）<br>非字母字符（如：！,$,#,%）<br>口令达到 12 字符长度，最长 20 个字符 |
| better | 很好，8 个字符长度以上（不包含 8）的口令，但至少满足以下条件之三：<br>英文大写字母（从 A 到 Z）<br>英文小写字母（从 a 到 z）<br>10 个基本数字（从 0 到 9）<br>非字母字符（如：！,$,#,%）<br>口令达到 12 字符长度，最长 20 个字符 |
| great | 极佳，8 个字符长度以上（不包含 8）的口令，但至少满足以下条件之四：<br>英文大写字母（从 A 到 Z）<br>英文小写字母（从 a 到 z）<br>10 个基本数字（从 0 到 9）<br>非字母字符（如：！,$,#,%）<br>口令达到 12 字符长度，最长 20 个字符 |
| maxloadtimes | 设置重试次数,默认 5，输入范围要求 1-20 |
| unlocktime | 设置超时解锁时间，单位分钟，默认 10 分钟 |
| pwdperiod | 设置密码有效期，单位天，0 代表永久生效 |
| pwdremind | 设置密码到期提请，单位天，默认 7 天 |
| idletime | 设置用户空闲时间，单位分钟，0 代表永久在线 |

**注意事项：**

输入的密码复杂度级别可以高于所要求的密码复杂度级别。

**示例：**

```
ac>auth config forcemodify yes pwdcomplex normal maxloadtimes 10 unlocktime 20  pwdperiod 50 pwdremind 7 idletime 10
```

## 显示认证参数配置

**语法：**

auth config show

**示例：**

```
ac> auth config show
AUTH CONFIG INFO:
        Forcemodify          :   yes
        pwdcomplex           :   normal
        maxloadtimes         :   10
        unlocktime (minute)  :   20
        pwdperiod (day)      :   50
        pwdremind (day)      :   7
        idletime (minute)    :   10
```

# 第10章 会话管理

## 10.1 会话管理（conntrack）

### 10.1.1 启动命令接口：

**语法：**

conntrack -B

**参数说明：**

-B 系统启动，必选参数；

**示例：**

ac> conntrack -B

### 10.1.2 配置超时时间：

**语法：**

conntrack -Z -p <protocol> --state <state> -t <timeout>

**参数说明：**

protocol 协议类型，必选参数；

state 协议状态，必选参数；

timeout 超时时间值，必选参数；

**示例：**

```
ac>conntrack -Z -p tcp --state NONE -t 100 配置 TCP 协议各状态的超时时间
ac>conntrack -Z -p tcp --state SYN_SENT -t 200
ac>conntrack -Z -p tcp --state SYN_RECV -t 300
ac>conntrack -Z -p tcp --state ESTABLISED -t 400
ac>conntrack -Z -p tcp --state FIN_WAIT -t 500
ac>conntrack -Z -p tcp --state CLOSE_WAIT -t 600
ac>conntrack -Z -p tcp --state LAST_ACK -t 700
ac>conntrack -Z -p tcp --state TIME_WAIT -t 800
ac>conntrack -Z -p tcp --state CLOSE -t 900
ac>conntrack -Z -p tcp --state SYN_SENT2 -t 1000
ac>conntrack -Z -p udp  -t 100                配置 UDP 协议的超时时间
ac>conntrack -Z -p udp -k -t 1000          配置 UDP 协议流的超时时间
ac>conntrack -Z -p icmp -t 100                配置 ICMP 协议的超时时间
```

### 10.1.3 统计连接数：

**语法：**

```
conntrack -Y
```

**参数说明：**

-Y 统计连接数，必选参数；

**示例：**

```
ac> conntrack -Y
```

### 10.1.4 显示连接状态：

**语法：**

conntrack -X -f ipv4 -p <protocol> [-s <src>] [-d <dst>] [--orig-port-src <sport>] [--orig-port-dst <dport>]

**参数说明：**

protocol 协议类型，必选参数；
src 源 IP 地址
dst 目的 IP 地址

sport 源端口
dport 目的端口

**注意事项：**
无

**示例：**
ac> conntrack -X -f ipv4 -p tcp -s 10.1.5.10
ac> conntrack -X -f ipv4 -p tcp -d 19.19.19.19
ac> conntrack -X -f ipv4 -p tcp -s 10.1.5.10 --orig-port-src 22
ac> conntrack -X -f ipv4 -p tcp -s 10.1.5.10 -d 19.19.19.19 --orig-port-src 22 --orig-port-dst 1500
ac> conntrack -X -f ipv4 -p udp -s 10.1.5.10
ac> conntrack -X -f ipv4 -p udp -s 10.1.5.10 -d 19.19.19.19
ac> conntrack -X -f ipv4 -p udp -s 10.1.5.10 -d 19.19.19.19 --orig-port-src 22 --orig-port-dst 1500
ac>conntrack -X -f ipv4 -p icmp

## 10.1.5 删除某连接信息：

**语法：**
conntrack -D -p <protocol> [-s <src>] [-d <dst>] [--orig-port-src <sport>] [--orig-port-dst <dport>]

**参数说明：**
protocol 协议类型，必选参数；
src 源 IP 地址
dst 目的 IP 地址
sport 源端口
dport 目的端口

**注意事项：**
如果要删除具体的某一条连接，则必须指定五元组信息。

**示例：**
ac> conntrack -D -p tcp
ac> conntrack -D -p udp
ac> conntrack -D -p icmp
ac> conntrack -D -p tcp --orig-port-src 4795

```
ac> conntrack -D -p udp --orig-port-dst 445
ac> conntrack -D -p tcp -s 192.168.2.128 -d 192.168.2.45 --orig-port-src 4795 --orig-port-dst 4
45
ac> conntrack -D -p tcp -s 192.168.2.128 -d 192.168.2.45 --orig-port-src 4795 --orig-port-dst 4
45
```

# 第11章 VPN

## 11.1.IPSEC

### 11.1.1 与 ipsec 基本配置相关部分

vpn set default [ ipsec_active { on | off } ] [ ikelifetime <int> ] [ ipseclifetime <int >] [ prekey <string> ] [ dhcpactive { on | off } ] [ dhcpipaddr <ip >] [ dhcpdevice <name> ] }

**参数说明：**

| 参数 | 描述 |
|---|---|
| ipsec_active | 是否开启 Ipsec 开关，on 为开启，off 为关闭 |
| ikelifetime | Ike 生命周期，单位为秒，必须在［180,864000］之间,默认为 28800 |
| ipseclifetime | Ipsec 生命周期，单位为秒，必须在［180,86400］之间，默认为 3600 |
| prekey | 预共享密钥，长度是 6 到 20 |
| dhcpactive | 是否开启 dhcp over ipsec，on 表示开启，off 表示关闭 |
| dhcpipaddr | 中继地址。表示分配 ip 地址的 DHCP 服务器地址，如果 DHCP 服务器就在本地设备上，该地址应该为 127.0.0.1 |
| dhcpdevice | 中继设备。表示从哪一个设备上将 DHCP 请求中继出去。如果 DHCP 服务器就在本地设备上，中继设备应该为 lo |

### 11.1.2 Vpn 规则相关部分

添加，修改，删除,查看 vpn 规则

Vpn add rule name <name> subnettype { subnet leftsubnet <ip/netmask> ] rightsubnet <ip/netmask> | subnets leftsubnets <string > rightsubnets < string> } leftservicetype { defaultserver [ leftservice <name> ] | customserver leftprotoport <protocol/port> } rightservicetype { defaultserver [ rightservice <name> ] | customserver rightprotoport <protocol/port> }

Vpn set rule name <name> subnettype { subnet leftsubnet <ip/netmask> rightsubnet <ip/netmask> ]

| subnets [ leftsubnets <string > ] [ rightsubnets < string> ] } leftservicetype { defaultserver [ leftservice <name> ] | customserver leftprotoport <protocol/port>} rightservicetype { defaultserver [ rightservice <name> ] | customserver rightprotoport <protocol/port> }

vpn del rule name <name>

vpn del rule all

vpn show rule name <name>

vpn show rule all

**参数说明：**

| 参数 | 描述 |
|---|---|
| name | Vpn 规则名，最多 15 个字符,可以是 “- “,” _”,数字，字母，中文组合 |
| subnettype | 子网类型 |
| leftsubnet | 本端保护子网，格式为 subnet/netmask，最大 32 字符，子网掩码可以是 0-32，或者为 255.255.255.0 类似的掩码 |
| rightsubnet | 远端保护子网，同 leftsubnet |
| leftsubnets | 本端保护子网组的 id 号，此处的 id 号来源是引用地址组里面的 id |
| rightsubnets | 远端保护子网组的 id 号，此处的 id 号来源是引用地址组里面的 id |
| leftprotoport | 本端协议，格式为协议/端口号，协议号为 0-255，端口号范围为 1-65535 |
| rightprotoport | 对端协议，格式为协议/端口号，协议号为 0-255，端口号范围为 1-65535 |

### 11.1.3 ike 配置相关部分

**添加，修改，删除，查看 ike 配置**

按照隧道的类型（客户端类型、网关类型），隧道协商模式（主模式、野蛮模式），认证类型（预共享密钥、证书），共分为八种情况。

| 编号 | 类型 | 隧道协商模式 | 认证类型 |
|---|---|---|---|
| 1 | 客户端类型（client） | 主模式(main) | 预共享密钥(psk) |
| 2 | | | 证书(rsasig) |
| 3 | | 野蛮模式(aggr) | 预共享密钥(psk) |
| 4 | | | 证书(rsasig) |
| 5 | 网关类型(gateway) | 主模式(main) | 预共享密钥(psk) |
| 6 | | | 证书(rsasig) |
| 7 | | 野蛮模式(aggr) | 预共享密钥(psk) |
| 8 | | | 证书(rsasig) |

注意：其中第四种和第八种野蛮模式+证书，不支持。

按照分类情况，添加网关的命令分为七个：

vpn add ikeconfig client main psk …

vpn add ikeconfig client main rsasig …

vpn add ikeconfig client aggr psk …

vpn add ikeconfig gateway main psk …

vpn add ikeconfig gateway main rsasig …

vpn add ikeconfig gateway aggr psk …

**（1）添加，设置客户端类型、主模式、共享密钥的网关**

**语法：**

vpn add ikeconfig client main psk name <name> rightaddr <ip> [ prekey <string> ] [ ike { 3des-md5,3des-sha1,des-md5,des-sha1,aes128-md5,aes128-sha1,aes256-sha1,aes256-md5,SM1-md5,SM1-sha1 } ] [ dhgroup { g1 | g2 | g5 } ] [ ikelifetime <int> ] [ idtype <int> ] [ leftid <string> ] [ rightid <string>] [ xauth { on | off } ]

vpn set ikeconfig client main psk name <name> rightaddr <ip> [ prekey <string> ] [ ike { { 3des-md5,3des-sha1,des-md5,des-sha1,aes128-md5,aes128-sha1,aes256-sha1,aes256-md5,SM1-md5,SM1-sha1 } ] [dhgroup { g1 | g2 | g5 } ] [ ikelifetime <int> ] [ idtype <int> ] [ leftid <string> ] [ righted <string> ] [ xauth { on | off } ]

**参数说明：**

| 参数 | 描述 |
|---|---|
| <name> | 要添加网关的名称，要求唯一，由字母、数字和字符”-“、”_”组成和中文组合，长度不超过 15 个字符 |
| rightaddr | 要添加网关的 ip 地址，对于客户端类型网关，ip 地址应该为”0.0.0.0” |
| idtype | Id 类型 可以是 ip 地址，也可以是字符串，域名 |
| <int> | 1 表示 ip 地址，2 表示域名，3 表示字符串，4 表示 email 可以不输入，默认不输入 |
| leftid | 本地 id,id 类型为 ip 地址时，leftid 为 ip 地址格式。id 为字符串和域名时不能多于 20 个字符 |
| rightid | 对端 id，id 类型为 ip 地址时，rightid 为 ip 地址格式。id 为字符串和域名时不能多于 20 个字符 |
| prekey | 要添加网关的预共享密钥，长度范围为 6-20 个字符，可以有特殊字符 |
| Ike | Ike 算法组件，应该取 3des-md5, 3des-sha1，des-md5,des-sha1,aes128-md5,aes128-sha1,aes256-md5，aes256-sha1,SM1-md5,SM1-sha1, 最多四个，默认取 aes128-sha1，aes128-md5,3des-sha1,3des-md5 |
| dhgroup | g1，g2，g5，默认为 g2 |
| ikelifetime | 要添加网关的 ike 生命周期，单位为秒，必须在［180，86400］之间 |
| Xauth | 是否启用扩展认证。on 表示启用，off 表示不启用。<br>只有客户端类型，而且是主模式才能启用扩展认证。 |

**（2）添加，设置客户端类型、主模式、证书认证的网关**

**语法：**

vpn add ikeconfig client main rsasig name <name> rightaddr <ip> [ idtype <idtype> ] [ leftid <string > ] [ rightid <string> ] leftcert <name> rightcert <name> [ ike { 3des-md5,3des-sha1,des-md5 , des-sha1,aes128-md5,aes128-sha1,aes256-md5,aes256-sha1,SM1-md5,SM1-sha1 } ] [ dhgroup { g1 | g2 | g5 }] [ ikelifetime <int> ] [ xauth { on | off } ]

vpn set ikeconfig client main rsasig name <name> rightaddr <ip> [ idtype <idtype> ] [ leftid <string > ] [ rightid <string> ] leftcert <name> rightcert <name> [ ike { 3des-md5,3des-sha1,des-md5 , des-sha1,aes128-md5,aes128-sha1,aes256-md5,aes256-sha1,SM1-md5,SM1-sha1 } ] [ dhgroup { g1 | g2 | g5 }] [ ikelifetime <int> ] [ xauth { on | off } ]

**参数说明：**

| 参数 | 描述 |
|---|---|
| <name> | 要添加网关的名称，要求唯一，由字母、数字和字符”-“、”_”中文组合组成，长度不超过 15 个字符 |
| rightaddr | 要添加网关的 ip 地址，对于客户端类型网关，ip 地址应该为”0.0.0.0” |
| idtype | Id 类型 可以是 ip 地址，也可以是完成合格域名 |
| leftid | 本地 id,如（1） |
| rightid | 对端 id,如（1） |
| leftcert | 要添加网关的本地证书名称。输入的证书名称必须是已经存在的证书,有关添加证书请参照《证书管理》一章 |
| rightcert | 要添加网关的远端网关证书名称。输入的证书名称必须是已经存在的证书,有关添加证书请参照《证书管理》一章 |
| ike | Ike 算法组件，应该取 3des-md5, 3des-sha1，des-md5,des-sha1,aes128-md5,aes128-sha1,aes256-md5，aes256-sha1,SM1-md5,SM1-sha1,最多四个，默认取 aes128-sha1，aes128-md5,3des-sha1,3des-md5 |
| dhgroup | g1,g2,g5，如（1） |
| ikelifetime | 要添加网关的 ike 生命周期，单位为秒，必须在［180,86400］之间 |
| Xauth | 是否启用扩展认证。on 表示启用，off 表示不启用。<br>只有客户端类型，而且是主模式才能启用扩展认证。 |

**(3) 添加，设置客户端类型、野蛮模式、共享密钥的网关**

**语法：**

vpn add ikeconfig client aggr psk name <name> rightaddr <ip> [ prekey <string>] [ ike {3des-md5, 3des-sha1,des-md5,des-sha1,aes128-md5,aes128-sha1,aes256-md5,aes256-sha1,SM1-md5,SM1-sha1}] [ dhgroup {g1 | g2 | g5 } ] [ idtype <int>] [ leftid <string> ] [ rightid <string > ] [ ikelifetime <int> ]

vpn set ikeconfig client aggr psk name <name> rightaddr <ip> [ prekey <string>] [ ike {3des-md5, 3des-sha1,des-md5,des-sha1,aes128-md5,aes128-sha1,aes256-md5,aes256-sha1,SM1-md5 ,SM1-sha1}] [ dhgroup {g1 | g2 | g5 } ] [ idtype <int>] [ leftid <string> ] [ rightid <string > ] [ ikelifetime <int> ]

**参数说明：**

| 参数 | 描述 |
|---|---|
| <name> | 要添加网关的名称，要求唯一,由字母、数字和字符”-“、”_”中文组成，长度不超过 15 个字符 |
| rightaddr | 要添加网关的 ip 地址，对于客户端类型网关，ip 地址应该为”0.0.0.0” |
| prekey | 要添加网关的预共享密钥，长度范围为 6-20 个字符,如（1） |
| idtype | 如（1） |
| leftid | 如（1） |
| rightid | 如（1） |
| ike | 如（1） |
| dhgroup | 如（1） |
| ikelifetime | 要添加网关的 ike 生命周期，单位为秒，必须在［180,86400］之间 |

**(4) 添加，设置网关隧道类型、主模式、共享密钥的网关**

**语法：**

vpn add ikeconfig gateway main psk name <name> righttype <int> rightaddr <ip> [ idtype <int> ] [ leftid <string>] [ rightid <string>] [ prekey <string> ] [ ike { 3des-md5, 3des-sha1, des-md5 ,des-sha1, aes128-md5, aes128-sha1, aes256-md5, aes256-md5, SM1-md5, SM1-sha1 } ] [ dhgroup { g1 | g2 | g5 } ] [ ikelifetime <int > ]

vpn set ikeconfig gateway main psk name <name> righttype <int> rightaddr <ip> [ idtype <int> ] [ leftid <string> ] [ rightid <string> ] [ prekey <string>] [ ike { 3des-md5,3des-sha1, des-md5, des-sha1, aes128-md5, aes128-sha1 ,aes256-md5, aes256-md5, SM1-md5, SM1-sha1}] [ dhgroup { g1| g2 | g5 } ] [ ikelifetime <int >]

**参数说明：**

| | 描述 |
|---|---|
| <name> | 要添加网关的名称，要求唯一，由字母、数字和字符”-“、”_”中文组成，长度不超过 15 个字符 |
| righttype | 1 表示 ip 地址，2 表示域名 |
| ip | 要添加网关的 ip 地址，对于客户端类型网关，ip 地址应该为”0.0.0.0” |
| idtype | 如（1） |
| Leftid | 如（1） |
| rightid | 如（1） |
| prekey | 如（1） |
| Ike | 如（1） |
| dhgroup | 如（1） |
| ikelifetime | 要添加网关的 ike 生命周期，单位为秒，必须在［180,86400］之间 |

**(5) 添加，设置网关隧道类型、主模式、证书认证的网关**

**语法：**

vpn add ikeconfig gateway main rsasig name <name> righttype <int> rightaddr <ip> [ idtype < int> ] [ leftid <string> ] [ rightid <string> ] leftcert <name> rightcert <name> [ ike { 3des-md5, 3des-sha1,des-md5, des-sha1 , aes128-md5, aes128-sha1, aes256-md5, aes256-sha1, SM1-md5, SM1-sha1}] [ dhgroup { g1 | g2 | g5 } ] [ ikelifetime <int> ]

vpn set ikeconfig gateway main rsasig name <name> righttype <int> rightaddr <ip> [ idtype < int> ] [leftid <string> ] [ rightid <string> ] leftcert <name> rightcert <name> [ ike { 3des-md5, 3des-sha1 ,des-md5, des-sha1,aes128-md5, aes128-sha1, aes256-md5, aes256-sha1, SM1-md5, SM1-sha1 } ] [ dhgroup { g1 | g2 | g5 } ] [ ikelifetime <int> ]

**参数说明：**

| 参数 | 描述 |
|---|---|
| <name> | 要添加网关的名称，要求唯一，由字母、数字和字符”-“、”_”中文组成，长度不超过 15 个字符 |
| righttype | 1 表示 ip 地址，2 表示域名 |
| ip | 要添加网关的 ip 地址，对于客户端类型网关，ip 地址应该为”0.0.0.0” |
| idtype | 如（1） |
| leftid | 如（1） |
| rightid | 如（1） |
| leftcert | 要添加网关的本地证书名称。输入的证书名称必须是已经存在的证书,有关添加证书请参照《证书管理》一章 |

| | |
|---|---|
| rightcert | 要添加网关的远端网关证书名称。输入的证书名称必须是已经存在的证书,有关添加证书请参照《证书管理》一章 |
| ike | 如（1） |
| dhgroup | g1,g2,g5 |
| ikelifetime | 要添加网关的 ike 生命周期，单位为秒，必须在［180,86400］之间 |

**(6) 添加，设置网关隧道类型、野蛮模式、共享密钥的网关**

**语法：**

vpn add ikeconfig gateway aggr psk name <name> righttype <int> rightaddr <ip> [ prekey <string > ] [idtype <int > ] [ leftid <sting> ] [ righted <string> ] [ ike {3des-md5,3des-sha1, des-md5, des-sha1, aes128-md5, aes128-sha1, aes256-md5, aes256-sha1, SM1-md5, SM1-sha1 } ] [dhgroup { g1|g2|g5 } ] [ikelifetime <int>]

vpn set ikeconfig gateway aggr psk name <name> righttype <int> rightaddr <ip> [ prekey <string > ] [idtype <int > ] [ leftid <sting> ] [ righted <string> ] [ ike {3des-md5,3des-sha1, des-md5, des-sha1, aes128-md5, aes128-sha1, aes256-md5, aes256-sha1, SM1-md5, SM1-sha1 } ] [dhgroup { g1|g2|g5 } ] [ikelifetime <int>]

**参数说明：**

| 参数 | 描述 |
|---|---|
| <name> | 要添加网关的名称，要求唯一，由字母、数字和字符”-“、”_”中文组成，长度不超过 15 个字符 |
| ip | 要添加网关的 ip 地址，对于客户端类型网关，ip 地址应该为”0.0.0.0” |
| idtype | Id 类型 可以是 ip 地址，也可以是完成合格域名 |
| Leftid | 如（1） |
| rightid | 如（1） |
| leftcert | 要添加网关的本地证书名称。输入的证书名称必须是已经存在的证书,有关添加证书请参照《证书管理》一章 |
| rightcert | 要添加网关的远端网关证书名称。输入的证书名称必须是已经存在的证书,有关添加证书请参照《证书管理》一章 |
| ike | 如（1） |
| dhgroup | 如（1） |
| ikelifetime | 要添加网关的 ike 生命周期，单位为秒，必须在［180,86400］之间 |

显示网关的命令为 vpn show ikeconfig …，该命令用来显示指定网关的详细属性。

**语法：**

vpn show ikeconfig name <name>

vpn show ikeconfig all

**参数说明：**

| 参数 | 描述 |
|---|---|
| < name> | 要显示的网关的名称 |

删除网关的命令为 vpn del …，该命令用来删除指定的网关。在删除网关的同时，系统会自动删除所有引用该网关的隧道。

**语法：**

vpn del ikeconfig name <name>

vpn del ikeconfig all

**参数说明：**

| 参数 | 描述 |
|---|---|
| <name> | 要删除的网关的名称 |
| all | 当用 all 代替网关名称时，用来删除所有的网关。 |

### 11.1.4 网关隧道配置

添加网关隧道

**语法：**

vpn add gatewaytunnel name <tunnelname> interface <name> ikename < ikename> [rulename <name>] [ ipsec { 3des-md5, 3des-sha1,des-md5,des-sha1,aes128-md5,aes128-sha1,aes256-md5，aes256-sha1,SM1-md5,SM1-sha1 ,null-md5,null-sha1 ] [type { tunnel | transport } ] [ phase2 { esp |ah } ] [ pfs { yes | no } ] [ compress { yes | no } ] [ ipseclifetime <int> ] [ dpddelay <int>]

[ dpdtimeout <int >] [dpdaction < hold | restart>] [ initiator{ yes | no } ] [ active { on | off}]

**参数说明：**

| 参数 | 描述 |
|---|---|
| tunnelname | 要添加的隧道名称 |
| interface | 隧道使用的设备名称 |
| rulename | 规则名称，引用其中的规则 |
| ikename | 使用的 ike 配置名称 |
| ipsec | ipsec 算法组件 3des-md5,3des-sha1,des-md5,des-sha1, aes-md5,aes-sha1,SM1-md5,SM1-sha1,null-md5,null-sha1 默认取 aes128-sha1,aes128-md5,3des-sha1,3des-md5。 |
| Type | 传输模式 ，tunnel 或者 transport |
| phase2 | 数据包封装形式，esp 或者 ah，默认取 esp。Ah 不支持 NAT 穿越和 null 算法。 |
| pfs | 是否完美向前保密，on 或者 off，默认取 on。 |
| compress | 数据包是否压缩，yes 或者 no，默认取 no。 |
| ipseclifetime | Ipsec 生命周期，单位为秒，取值范围 180-86400。 |
| dpddelay | DPD 探测周期，单位为秒，取值范围 1-180。0 表示不启用 DPD。 |
| dpdtimeout | DPD 超时时间，单位为秒，取值范围 1-600。0 表示不启用 DPD。 |
| dpdaction | Dpd 超时后的操作 ，hold，restart |
| initiator | 是否主动连接， |
| active | 是否启动隧道 |

设置网关隧道

**语法：**

vpn set gatewaytunnel name <name> [ interface <name> ] [ ikename <name> ] [ rulename < name> ] [ ipsec { 3des-md5, 3des-sha1,des-md5,des-sha1,aes128-md5,aes128-sha1,aes256-md5, aes256-sha1,SM1-md5,SM1-sha1,null-md5 ,null-sha1 ] [ type { tunnel | transport } ]

[ phase2 { esp |ah}] [ pfs { yes | no } ] [ compress {yes | no } ] [ ipseclifetime <int>]

[ dpddelay <int >] [ dpdtimeout <int>] [ dpdaction { hold| restart } ] [ initiator { no | yes } ] [ active { on| off}]

| 参数 | 描述 |
|---|---|
| tunnelname | 要添加的隧道名称要求唯一，由字母、数字和字符”-“、”_” 中文组成，长度不超过 15 个字符 |

| | |
|---|---|
| interfame | 隧道使用的设备名称 |
| rulename | 规则名称，引用其中的规则 |
| ikename | 使用的 ike 配置名称 |
| ipsec | Ipsec 算法组建 3des-md5,3des-sha1,des-md5,des-sha1 ,aes128-md5,aes128-sha1,aes256-md5,aes256-sha1,SM1-md5,SM1-sha1,null-md5,null-sha1<br>默认取 aes128-sha1，aes128-md5,3des-sha1,3des-md5 |
| Type | 传输模式 ，tunnel 或者 transport |
| phase2 | 数据包封装形式，esp 或者 ah，默认取 esp。Ah 不支持 NAT 穿越和 null 算法 |
| pfs | 是否完美向前保密，on 或者 off，默认取 on |
| compress | 数据包是否压缩，yes 或者 no，默认取 no |
| ipseclifetime | Ipsec 生命周期，单位为秒，取值范围 180-86400 |
| dpddelay | DPD 探测周期，单位为秒，取值范围 1-180。0 表示不启用 DPD |
| dpdtimeout | DPD 超时时间，单位为秒，取值范围 1-600。0 表示不启用 DPD |
| dpdaction | DPD 超时后的操作 ，hold，restart |
| initiator | 是否主动连接 |
| active | 是否启动隧道 |

显示网关隧道

显示隧道的命令为 vpn show gatewaytunnel …，该命令用来显示指定隧道的详细属性。

**语法：**

vpn show gatewaytunnel all

vpn show gatewaytunnel name <name>

**参数说明：**

| 参数 | 描述 |
|---|---|
| <name> | 要显示的隧道的名称 |
| all | 当用 all 代替网隧道名称时，用来显示所有的隧道 |

删除网关隧道

删除隧道的命令为 vpn del gatewaytunnel …，该命令用来删除指定的隧道。

**语法：**

vpn del gatewaytunnel all

vpn del gatewaytunnel name <name>

**参数说明：**

| 参数 | 描述 |
|---|---|
| <name> | 要删除的隧道的名称 |
| all | 当用 all 代替隧道名称时，用来删除所有的隧道 |

### 11.1.5 客户端隧道配置

添加客户端隧道

**语法：**

vpn add clienttunnel name <name> interface < name> ikename < name> rulename <name> [ ipsec { 3des-md5, 3des-sha1,des-md5,des-sha1,aes128-md5,aes128-sha1,aes256-md5,aes256-sha1, SM1-md5,SM1-sha1,null-md5,null-sha1] [type{tunnel|transport}] [phase2 { esp|ah }] [ pfs { yes | no }] [ ipseclifetime <int> ] [dpddelay <int> ] [dpdtimeout <int> ] [ active { on | off } ]

**参数说明：**

| 参数 | 描述 |
| --- | --- |
| tunnelname | 要添加的隧道名称要求唯一，由字母、数字和字符”-“、”_”中文组成，长度不超过 15 个字符 |
| interface | 隧道使用的设备名称 |
| rulename | 规则名称，引用其中的规则 |
| ikename | 使用的 ike 配置名称 |
| ipsec | ipsec 算法组件 3des-md5, 3des-sha1,des-md5,des-sha1 ,aes128-md5,aes128-sha1,aes256-md5,aes256-sha1,SM1-md5,SM1-sha1,null-md5,null-sha1<br>默认取 aes128-sha1,aes128-md5,3des-sha1,3des-md5 |
| Type | 传输模式 ，tunnel 或者 transport |
| phase2 | 数据包封装形式，esp 或者 ah，默认取 esp。Ah 不支持 NAT 穿越和 null 算法 |
| ipseclifetime | Ipsec 生命周期，单位为秒，取值范围 180-86400 |
| dpddelay | DPD 探测周期，单位为秒，取值范围 1-180。0 表示不启用 DPD |
| dpdtimeout | DPD 超时时间，单位为秒，取值范围 1-600。0 表示不启用 DPD |
| active<br><br>initiator<br>dpdaction | 是否启动隧道<br><br>是否主动连接<br>DPD 超时后的操作 ，hold,restart |

**设置客户端隧道**

**语法：**

vpn set clienttunnel name <name> interface < name> ikename < name> rulename <name> [ ipsec { 3des-md5, 3des-sha1,des-md5,des-sha1,aes128-md5,aes128-sha1,aes256-md5,aes256-sha1, SM1-md5,SM1-sha1,null-md5,null-sha1] [type{tunnel|transport}] [phase2 { esp|ah }] [ pfs { yes | no }] [ ipseclifetime <int> ] [dpddelay <int> ] [dpdtimeout <int> ] [ active { on | off } ]

**参数说明：**

| 参数 | 描述 |
| --- | --- |
| tunnelname | 要添加的隧道名称要求唯一，由字母、数字和字符”-“、”_”中文组成，长度不超过 15 个字符 |
| interface | 隧道使用的设备名称 |
| rulename | 规则名称，引用其中的规则 |
| ikename | 使用的 ike 配置名称 |
| ipsec | ipsec 算法组件 3des-md5, 3des-sha1,des-md5,des-sha1, aes128-md5,aes128-sha1,aes256-md5,aes256-sha1,SM1-md5,SM1-sha1,null-md5,null-sha1<br>默认取 aes128-sha1,aes128-md5,3des-sha1,3des-md5 |
| Type | 传输模式 ，tunnel 或者 transport |
| phase2 | 数据包封装形式，esp 或者 ah，默认取 esp。Ah 不支持 NAT 穿越和 null 算法 |
| ipseclifetime | Ipsec 生命周期，单位为秒，取值范围 180-86400 |
| dpddelay | DPD 探测周期，单位为秒，取值范围 1-180。0 表示不启用 DPD |
| dpdtimeout | DPD 超时时间，单位为秒，取值范围 1-600。0 表示不启用 DPD |
| active | 是否启动隧道 |

**显示客户端隧道**

显示隧道的命令为 vpn show clienttunnel …，该命令用来显示指定隧道的详细属性。

**语法：**

vpn show clienttunnel all

vpn show clienttunnel name <name>

**参数说明：**

| 参数 | 描述 |
|---|---|
| <name> | 要显示的隧道的名称 |
| all | 当用 all 代替网隧道名称时，用来显示所有的隧道 |

删除客户端隧道

删除隧道的命令为 vpn del clienttunnel …，该命令用来删除指定的隧道。

**语法：**

vpn del clienttunnel all

vpn del clienttunnel name <name>

**参数说明：**

| 参数 | 描述 |
|---|---|
| <name> | 要删除的隧道的名称 |
| all | 当用 all 代替隧道名称时，用来删除所有的隧道 |

### 11.1.6 隧道组相关部分

添加隧道组

**语法：**

vpn add tunnelgroup name < name> rulename < name> tunnels <name1,name 2, ... ,> [comment <comment>]

**参数说明：**

| 参数 | 描述 |
|---|---|
| name | 要添加的隧道组的名称，要求唯一，由字母、数字和字符”-“、”_”中文组成，长度不超过 15 个字符 |
| rulename | 关联的 vpnrule 名称 |
| tunnels | 隧道名称 |
| <comment> | 备注,不能超过 255 个字符 |

设置隧道组（修改隧道优先级的时候，需要检查隧道组状态。如果隧道组已经启动了,修改以后，隧道组中的网关隧道重新协商）

**语法：**

vpn set tunnelgroup name < name> rulename <name> tunnels <name1,name2, ... ,> [comment <comment>]

**参数说明：**

| 参数 | 描述 |
|---|---|
| name | 要设置的隧道组的名称 |
| rulename | 关联的 vpnrule 名称 |
| tunnels | 隧道名称 |
| comment | 备注 |

显示隧道组

**语法：**

vpn show tunnelgroup all

vpn show tunnelgroup name <name>

**参数说明：**

| 参数 | 描述 |
| --- | --- |
| <name> | 隧道组的名称 |

**删除隧道组**

vpn del tunnelgroup all

vpn del tunnelgroup name <name>

**参数说明：**

| 参数 | 描述 |
| --- | --- |
| <name> | 要删除的隧道组的名称 |

### 11.1.7 隧道的启动与停止

用来启动或者停止启动的隧道。在启动一个隧道时，要求隧道存在而且已经启用。

**语法：**

**vpn up 用来启动一个已经启用的隧道**

vpn up all

vpn up gatewaytunnel <name>

vpn up clienttunnel <name>

**vpn down 用来停止一个启动的隧道**

vpn down all

vpn down gatewaytunnel < name>

vpn down clienttunnel < name>

**参数说明：**

| 参数 | 描述 |
| --- | --- |
| <name> | 要启动或者停止的隧道名称 |

### 11.1.8 隧道监控

用来显示隧道的建立情况。

vpn monitor show

## 11.2 gre 部分

GRE 命令行运行程序为 gre，用来对 GRE 隧道进行管理和配置。

按照命令行的组织格式，总共分为 7 类子命令，他们分别为：

gre add：该命令添加 gre 隧道。

gre del：该命令用来删除指定隧道。

gre show：该命令用来显示所有隧道。

gre set：该命令用来更改指定的隧道配置。

gre up/down：该命令用来启用/停用指定的隧道。

gre start/stop：该命令用来启用/停用所有隧道。

GRE 命令行具有智能提示，如果用户不熟悉命令，在输入部分命令后，直接按 TAB 或者?键，系统就会提示下一步可能的输入或者需要输入内容的格式。例如，如果用户在命令行输入 gre 后按 TAB 键，系统提示：

gre add…
gre del…
gre down…
gre set…
gre show…
gre start….
gre stop…
gre up…
gre restart…

也就是说用户下一步可以输入 add，也可以输入 del，等等。假如用户想添加一条隧道，但是不熟悉命令行，那么可以先输入 gre，按 TAB 键，参考提示，然后输入 add，按 TAB 键，就可以看到下面的提示：

gre add name…

表示在 add 后面的 name 是必须输入的，接下来就需要用户自己输入隧道名称了，再按 TAB 键，会得到本地网关的命令行格式提示。

### 11.2.1 添加 GRE 隧道

**语法：**

gre add name <name> local <localname> remote { <domainname> | <single_ip>} addr <single_ip> raddr <single_ip>

**GRE 隧道添加表**

| 参数 | 描述 |
|---|---|
| <name> | 要添加的 GRE 隧道名称，必须以 GRE_开头 |
| Local<name> | 本地网关接口名称 |
| <domainname> | 对端网关域名（对端网关可以为域名，也可以为 ip 地址） |
| <single_ip> | 对端网关 ip 地址（对端网关可以为域名，也可以为 ip 地址） |
| addr <single_ip> | 本地 GRE 设备 ip 地址 |
| raddr <single_ip> | 对端 GRE 设备 ip 地址 |

5.2.2 删除 GRE 隧道

**语法：**

gre del name <name>

**GRE 隧道删除表**

| 参数 | 描述 |
|---|---|
| <name> | 要删除的 GRE 隧道名称 |

### 11.2.3 GRE 隧道的参数修改

**语法：**

gre set name <name> { [ local <name> ] | [ remote {<domainname> | <single_ip>}] | [ addr <single_ip> ] | [ raddr <single_ip>]}

在这里，local | remote | addr | raddr 都是可选项，可以同时修改，也可以修改其中的一个或几个。

**修改 GRE 隧道表**

| 参数 | 描述 |
|---|---|
| <name> | 要修改的 GRE 隧道名称 |
| Local<name> | 本地网关接口名称 |
| <domainname> | 对端网关域名（对端网关可以为域名，也可以为 ip 地址） |
| <single_ip> | 对端网关 ip 地址（对端网关可以为域名，也可以为 ip 地址） |
| addr <single_ip> | 本地 GRE 设备 ip 地址 |
| raddr <single_ip> | 对端 GRE 设备 ip 地址 |

### 11.2.4 GRE 隧道的启用/停用

**语法：**

gre up name <name>

gre down name <name>

gre start

gre stop

gre restart

**启动、停止 GRE 隧道**

| 参数 | 描述 |
|---|---|
| <name> | 要启用/停用的 GRE 隧道名称。 |

## 11.3 pptp 和 l2tp

### 11.3.1 添加拨号用户

该命令用来添加一个 PPTP/L2TP 拨号用户。

**语法：**

pp_l2tp {pptp|l2tp} add dialuser name<username> password<password> [userip<single_ip>] [desc<comment>]

**参数说明：**

| 参数 | 描述 |
|---|---|
| <username> | 要添加的用户名。在添加新的拨号用户时，应该保证用户名有效并且唯一。 |
| <password> | 要添加的用户密码。 |
| <single_ip> | 给要添加用户指定一个虚拟 IP 地址 |
| <comment> | 备注信息，用来对要添加的用户进行说明。如果说明中有空格，用双引号将说明信息括起来。 |

**例子：**

添加一个 pptp 拨号用户，用户名为 tom，密码 tom123，ip 为 1.0.0.2，说明信息为 tom medic。

pp_l2tp pptp add dialuser name tom password tom123 userip 1.0.1.2 desc “Tom Medic”

### 11.3.2 设置拨号用户

该命令用来设置指定 PPTP/L2TP 拨号用户的信息。

**语法：**

pp_l2tp {pptp|l2tp} set dialuser name<username> [password<password>] [userip<single_ip>] [desc<comment>]

**参数说明：**

| 参数 | 描述 |
|---|---|
| <username> | 要修改的用户名。在添加新的拨号用户时，应该保证用户名有效并且唯一。 |
| <password> | 用户的有效密码（该项为可选）。 |
| <single_ip> | 给用户指定的虚拟 IP（该项为可选）。 |
| <comment> | 备注信息，用来对要添加的用户进行说明。 |

**例子：**

将 pptp 拨号用户 tom 的密码改为 super123，且 IP 地址和说明信息不变。

pp_l2tp pptp set dialuser name tom password super123

### 11.3.3 显示拨号用户

该命令用来显示 PPTP/L2TP 拨号用户的信息

**语法：**

pp_l2tp {pptp|l2tp} show dialuser {all | name <name>}

**参数说明：**

| 参数 | 描述 |
|---|---|
| <username> | 指定要显示的用户名。 |
| all | 用来显示所有的拨号用户信息 |

**举例：**

显示 PPTP 拨号用户 tom 的信息：

pp_l2tp pptp show dialuser name tom

显示所有 PPTP 拨号用户的信息：

pp_l2tp pptp show dialuser all

### 11.3.4 删除拨号用户

该命令用来删除指定的 PPTP/L2TP 拨号用户。

**语法：**

pp_l2tp {pptp|l2tp} del dialuser {all | name <name>}

**参数说明：**

| 参数 | 描述 |
|---|---|
| <username> | 要删除的用户名。 |
| all | 用来删除所有的拨号用户信息 |

**举例：**

删除 PPTP 拨号用户 tom：

pp_l2tp pptp del dialuser name tom

删除所有 PPTP 拨号用户：

pp_l2tp pptp del dialuser all

# 11.4 证书管理

证书的添加需要通过 Web 来完成，在命令行方式下，只能进行证书的显示和删除,OCSP,SCEP 操作。证书管理分为 6 部分：CA 证书，本地证书，对方证书，CRL，OCSP，SCEP 客户端。

### 11.4.1 显示证书

**语法：**

pki ca ipsec show cert { ca | remote | local }

**参数说明：**

| 参数 | 描述 |
|---|---|
| <ac> | 显示所有的 ca 证书。 |
| <remote> | 显示所有的远端证书。 |
| <local> | 删除所有的本地证书。 |

**举例：**

显示所有的本地证书：

pki ca ipsec show cert local

### 11.4.2 删除证书

用来删除指定的证书。

删除证书的命令按照证书的分类分为三个，分别用来删除 ca 证书，对端证书，本地证书。

如果某个证书被引用，则无法删除。而且，如果指定的证书类型与证书的实际类型不符，也无法删除该证书。

**语法：**

pki ca ipsec del cert { ca | local | remote } { all | <name>}

**参数说明：**

| 参数 | 描述 |
|---|---|
| ca | ca 证书 |
| local | 本地证书 |
| remote | 对端证书 |
| all | 所有证书 |
| name | 删除证书的名字 |

**举例：**

删除本地证书 cer1：

pki ca ipsec del cert local cer1

### 11.4.3 删除 CRL

用来删除所有和指定的 CRL

**语法：**

pki ca ipsec del crl { all | <name>}

**参数说明：**

| 参数 | 描述 |
| --- | --- |
| name | 要删除的撤销列表名称 |
| all | 删除所有的撤销列表 |

**举例：**

删除本地证书 crl1：

pki ca ipsec del crl crl1

### 11.4.4 OCSP

**1 添加 OCSP 服务器**

**语法：**

pki ca ocsp client add config name <name> ocspurl <string> strictpolicy { on | off }

**参数说明：**

| 参数 | 描述 |
| --- | --- |
| name | ca 名称 |
| string | ocspurl 地址 |
| on | 使能严格检查 |
| off | 去使能严格检查 |

**举例：**

添加 CA 的 ocsp 服务器

pki ca ocsp client add config name beijingCA ocspurl http://202.106.0.45 strictpolicy on

**2 设置 OCSP 服务器**

**语法：**

pki ca ocsp client set config name <name> ocspurl <string> strictpolicy { on | off }

**参数说明：**

| 参数 | 描述 |
| --- | --- |
| name | ca 名称 |
| string | ocspurl 地址 |
| on | 使能严格检查 |
| off | 去使能严格检查 |

**举例：**

设置 CA 的 OCSP 服务器

pki ca ocsp client add config name beijingCA ocspurl http://202.106.0.45 strictpolicy off

**3 删除 OCSP 服务器**

**语法：**

pki ca ocsp client del config name { all | <name>}

**参数说明：**

| 参数 | 描述 |
| --- | --- |
| name | ca 名称 |

**举例：**

**删除** CA 的 OCSP 配置

pki ca ocsp client del config name all

**4 显示 OCSP 服务器**

**语法：**

pki ca ocsp client show { all | <name>}

**参数说明：**

| 参数 | 描述 |
| --- | --- |
| name | CA 名称 |

**举例：**

显示 CA 的 ocsp 服务器

pki ca ocsp client show all

### 11.4.5 SCEP

**1 获取 CA 证书**

**语法：**

pki ca scep client getca caname <name> url <string>

**参数说明：**

| 参数 | 描述 |
| --- | --- |
| name | ca 名称 |
| string | scep 服务区 url 地址 |

**举例：**

获取 CA 证书

pki ca scep client getca caname bejingCA url http://202.106.0.10/certsrv/mscep/mscep.dll

**2 在线申请证书**

**语法：**

pki ca scep client enroll caname <caname> certname <certname> reqname <reqname> url <url> interval <interval> times <times> [challenge {ip|dns|email} <content> <changllenge>]

**参数说明：**

| 参数 | 描述 |
| --- | --- |

| | |
|---|---|
| caname | CA 证书名称 |
| certname | 申请证书名称 |
| reqname | 请求文件名称 |
| url | SCEP 服务器地址 |
| interval | 申请证书间隔 |
| times | 申请证书次数 |
| content | subjectAltName |
| changllenge | 挑战码 |

**举例：**

向 CA 中心申请证书

pki ca scep client enroll caname beijingCA certname mycert reqname myreq url http://www.beijingCA.com/certsrv/mscep/mscep.dll interval 60 times 5 challenge ip 1.0.0.101 F21ED3CC6C1E5B0E

# 11.5 拨号服务器管理

### 11.5.1 设置拨号服务器

用来设置 PPTP/L2TP 拨号服务器的信息

**语法：**

pp_l2tp {pptp|l2tp} set dialserver {[iprange<ipaddr-ipaddr>] [enctype{high|low}] [auth{chap+chapms+chapms-v2}] [active{on|off}] [ipserver<ipaddr>] [portserver<port>]}

**参数：**

| 参数 | 描述 |
|---|---|
| <ipaddr-ipaddr> | 拨号服务器提供的 ip 地址范围。格式为***.***.***.***-***.***.***.***<br>要求起始地址与结束地址在同一个 C 段内，并且 IP 个数不能超过 200，而且不能少于三个。<br>例如：<br>10.10.10.1-10.10.10.100 是有效的<br>10.10.10.1-10.1.10.100 是无效的 |
| enctype | 加密程度，high 表示比较高的加密等级(128 位)，low 表示比较低的加密等级(40 位)。 |
| auth | 支持的认证协议，从 chap、chapms、chapms-v2 三种协议中选出一个或者多个，然后用+相连。<br>例如：<br>chapms-v2、chap+chapms-v2、chap+chapms+chapms-v2<br>注意：选择 chap 或 chap+chapms 会认证失败。 |
| active | 表示启动或者停止拨号服务器，on 表示启动，off 表示停止。<br>在 active=on 时，如果拨号服务器原来已启动，则不会再重新启动。 |

| | |
|---|---|
| ipaddr | 指定拨号服务端的提供服务的 IP 地址。 |
| port | 提供服务的端口号。 |

**举例：**

设置 PPTP 拨号服务器的相关参数：

pp_l2tp pptp set dialserver iprange 1.0.10.2-1.0.10.10 enctype high auth chap+chapms+chapms-v2 active on ipserver 1.0.0.101 portserver 1723

### 11.5.2 显示拨号服务器

用来显示 PPTP/L2TP 拨号服务器的信息

**语法：**

pp_l2tp {pptp|l2tp} show dialserver

**参数：**

无。

**举例：**

pp_l2tp pptp show dialserver

### 11.5. 3 踢掉在线拨号用户

用来踢掉在线的 PPTP/L2TP 拨号用户

**语法：**

pp_l2tp kick {all | virtualIP <ipaddr>}

**参数：**

| 参数 | 描述 |
|---|---|
| all | 踢掉所有在线拨号用户。 |
| ipaddr | 踢掉某个已分配虚拟地址的拨号用户。 |

**举例：**

踢掉已分配的虚拟 IP 地址为 1.0.1.101 的拨号用户：

pp_l2tp kick 1.0.1.101

# 第12章 SSLVPN

## 12.1 基本配置相关命令及配置

### 12.1.1 开启 sag 服务：

**语法：**
sag config start

**参数说明：**
config sslvpn 命令行部分，宏观配置类相关命令
start 启动 sslvpn 服务

**注意事项：**
无

**示例：**
sag config start

### 12.1.2 关闭 sag 服务:

**语法：**
sag config stop

**参数说明：**
config sslvpn 命令行部分，宏观配置类相关命令
stop 停止 sslvpn 服务

**注意事项：**
无

**示例：**
sag config stopt

### 12.1.3 显示已配置的 ssl 端口:

**语法：**
sag config show sslport

**参数说明：**

| | |
|---|---|
| config | sslvpn 命令行部分，宏观配置类相关命令 |
| show | 显示类操作 |
| sslport | 单双向 https 端口 |

**注意事项：**
无

**示例：**
sag config show sslport

### 12.1.4 配置 https 端口：

**语法：**
sag config set sslport uni <port> bi <port>

**参数说明：**

| | |
|---|---|
| config | sslvpn 命令行部分，宏观配置类相关命令 |
| set | 设置修改类操作 |
| sslport | 单双向 https 端口标识 |
| uni | 单向 https 端口（1～65535） |
| bi | 双向 https 端口（1～65535） |

**注意事项：**
uni 和 bi 的<port>值不能重复

**示例：**
sag config set sslport uni 443 bi 444

### 12.1.5 显示 NC 相关配置：

**语法：**
sag config show nc

**参数说明：**
config sslvpn 命令行部分，宏观配置类相关命令
show 显示类操作
nc 内容实体标识，nc

**注意事项：**
无

**示例：**
sag config show nc

### 12.1.6 设置 NC 服务基本配置：

### 12.1.7 显示绑定用户:

**语法：**
sag config show binduser

**参数说明：**
config sslvpn 命令行部分，宏观配置类相关命令
show 显示类操作
binduser 内容实体标识，binduser

**注意事项：**
无

**示例：**
sag config show binduser

### 12.1.8 增加绑定用户:

**语法：**

sag config add binduser type { p | t | c sid <value> } name <name> vip <ip>

**参数说明：**

| | |
|---|---|
| config | sslvpn 命令行部分，宏观配置类相关命令 |
| add | 添加类基本操作 |
| binduser | 内容实体标识，binduser |
| type | 要添加的绑定用户的类型，p：口令用户，t：双因素用户，c：证书用户 |
| sid | 证书用户序列号，数字字符组合 |
| name | 要绑定用户的用户名，1-15 位中文、字母、数字、减号、下划线组合 |
| vip | 要绑定的虚拟 IP，格式如：192.168.0.1 |

**注意事项：**

无

**示例：**

sag config add binduser type c sid 132b4e10759 name nametext vip 1.0.2.1

### 12.1.9 修改绑定用户：

**语法：**

sag config set binduser type { p | t | c } vip <ip> id <value> tid <value>

**参数说明：**

| | |
|---|---|
| config | sslvpn 命令行部分，宏观配置类相关命令 |
| set | 设置修改类操作 |
| binduser | 内容实体标识，binduser |
| type | 要添加的绑定用户的类，p：口令用户，t：双因素用户，c：证书用户 |
| vip | 要绑定的虚拟 IP，格式如：192.168.0.1 |
| id | 口令或双因素用户的口令因素 id，6-15 位数字 |
| tid | 证书用户 id 或双因素用户的证书因素部分，6-15 位数字 |

**注意事项：**

无

**示例：**

sag config set binduser type c vip 1.0.0.2 id123456789 tid 132410759

### 12.1.10 删除已存在的绑定用户：

**语法：**
sag config del binduser type ｛ p | t | c ｝ id <value> tid <value>

**参数说明：**

| | |
|---|---|
| config | sslvpn 命令行部分，宏观配置类相关命令 |
| del | 删除类基本操作 |
| binduser | 内容实体标识，binduser |
| type | 要添加的绑定用户的类，p：口令用户，t：双因素用户，c：证书用户 |
| id | 口令或双因素用户的口令因素 id，6-15 位数字 |
| tid | 证书用户 id 或双因素用户的证书因素部分，6-15 位数字 |

**注意事项：**
无

**示例：**
sag config del binduser type t id 1234567890123 tid 13210732359

## 12.2 服务管理相关命令及配置：

### 12.2.1 显示 bs 服务：

**语法：**
sag service show bs

**参数说明：**

| | |
|---|---|
| service | sslvpn 命令行部分，宏观配置类相关命令 |
| show | 显示类操作 |
| bs | 内容实体标识，bs |

**注意事项：**
无

**示例：**
sag service show bs

### 12.2.2 删除 bs 服务:

**语法：**

sag service del bs id <value> wcs <boolean>

**参数说明：**

| | |
|---|---|
| service | sslvpn 命令行部分，宏观配置类相关命令 |
| del | 删除类基本操作 |
| bs | 内容实体标识，bs |
| id | 要删除服务的 id，6-15 位数字 |
| wcs | 服务中是否启用 cs，0：未启用，1：启用，默认不启用 |

**注意事项：**

无

**示例：**

sag service del bs id 1234567890123 wcs 0

### 12.2.3 修改 bs 服务:

**语法：**

sag service set bs id <value> server <string> name <name> allow_path <string\;string..> attribute { ls | lh | nh } authtype { a | p | c | t } [note <string>] withcs {yes [dns <dns>] compress { no | gzip } sso { no | basic | ntlm | form httpconmand {get|post} [ loginurl <string>] [submiturl <string>] [userkey <string>] [passwordkey <string>] [otherpara <string>] | client bindapp {on|off}}

[shortcut <string>] | no encrpy { l | m | h } htmlprocess { no | comman | all } sso { no | basic | ntlm | form httpconmand {get|post} [ loginurl <string>] [submiturl <string>] [ userkey <string>] [passwordkey <string>] [otherpara <string>] | client bindapp {on|off} }[shortcut <string>] indexmap <string> [note <string>] }

**参数说明：**

| | |
|---|---|
| service | sslvpn 命令行部分，宏观配置类相关命令 |
| set | 设置修改类操作 |
| bs | 内容实体标识，bs |
| id | 要删除服务的 id，6-15 位数字 |
| server | 服务器地址，如：\"http://1.0.0.1:8888\"或 \"https ://1.0.0.1:8889\"，必须以 http://或 https://开头，并且需要将服务器地址用'\"'将服务器地址括起来 |
| name | 客户端显示的 bs 名称，1-15 位中文、字母、数字、减号、下划线组合 |
| allow_path | bs 服务允许访问路径，多个允许路径的字符串,多个路径间以 '\;'分隔，每个路径需要以'\"'括起来，如：\"allow_path1\"\;\"allow_path2\" |
| attribute | 显示属性，ls：名称显示，链接显示，lh：名称显示，链接隐藏，nh 名称隐藏 |
| authtype | 认证类别，a：匿名访问，p：通过口令访问，c：通过证书访问，t：通过双 |

因素访问
note 注释或描述，可输入除制表符和分号外的任意可打印字符，以'\"'括起来
withcs 是否支持 c/s 服务，yes：支持 c/s 服务，no：不支持 c/s 服务
dns 虚拟域名
compress 数据压缩，no：不压缩，gzip：gzip 方式压缩
sso 单点登录，默认不启用， no：不启用，basic：basic 认证，ntlm： NTLM 认证，form： Form 认证，client：客户端 Form 代填
httpconmand http 命令，get：GET，post：POST，默认 POST
loginurl 登录页面地址，用'\"'将地址括起来
submiturl 提交路径，用'\"'将路径括起来
userkey 用户标识，用'\"'将用户名括起来
passwordkey 口令标识，用'\"'将口令括起来
otherpara 其他参数，用'\"'将参数括起来
bindapp 是否绑定应用，客户端 Form 代填专用，on：启用绑定，off：不启用绑定
shortcut 快捷方式，默认为空，至少 0 个。快捷方式需以'/'开头；多个快捷方式以‘\;’分隔,单条快捷方方式中不能包含'\;'字符，每个快捷方式需要以'\"'括起来，如：\"short_cut11\";\"short_cut2\"
encrpy 加密强度，默认为中，l：低，m：中，h：高
htmlprocess 处理 HTML，默认为一般处理。no：都不处理， comma：一般处理，all：完全处理
indexmap 映射目录

**注意事项：**
无

**示例：**
1）带 C/S 支持:
sag service set bs id 123456789 server \"http://1.0.0.1 \" name testname allow_path \"dir1/dir2\";\"dir3/dir4\" attribute ls authtype a withcs yes dns dnstext compress no sso form httpconmand get loginurl \"1.0.0.1\" submiturl \"1.0.0.2\" userkey \"user\" passwordkey \"123456789\" otherpara \"other\" shortcut \"/abc\"

2）不带 C/S 支持:
sag service set bs id 123456789 server \"http://1.0.0.1 \" name testname allow_path \"dir1/dir2\";\"dir3/dir4\" attribute ls authtype a withcs no encrpy l htmlprocess no sso no

## 12.2.4 添加 bs 服务:

**语法：**
sag service add bs server <string> name <name> allow_path <string\;string..> authtype { a | p | c | t } [note <string>] withcs {yes [dns <dns>] compress { no | gzip } | no encrpy { l | m | h } htmlprocess { no | comman | all } }

**参数说明：**
service sslvpn 命令行部分，宏观配置类相关命令
add 添加类基本操作
bs 内容实体标识，bs

server 服务器地址，如：\”http://1.0.0.1:8888\”或 \”https ://1.0.0.1:8889\”，必须以 http://或 https://开头,并且需要将服务器地址用'\”'将服务器地址括起来
name 客户端显示的 bs 名称，1-15 位中文、字母、数字、减号、下划线组合
allow_path bs 服务允许访问路径，多个允许路径的字符串,多个路径间以‘\;’分隔，每个路径需要以'\”'括起来，如：\”allow_path1\”\;\”allow_path2\”
attribute 显示属性，ls：名称显示，链接显示，lh：名称显示，链接隐藏，nh 名称隐藏
authtype 认证类别，a：匿名访问，p：通过口令访问，c：通过证书访问，t：通过双因素访问
note 注释或描述，可输入除制表符和分号外的任意可打印字符，以'\”'括起来
withcs 是否支持 c/s 服务，yes：支持 c/s 服务，no：不支持 c/s 服务
dns 虚拟域名
compress 数据压缩，no：不压缩，gzip：gzip 方式压缩
encrpy 加密强度，默认为中，l：低，m：中，h：高
htmlprocess 处理 HTML，默认为一般处理。no：都不处理， comma：一般处理，all：完全处理

**注意事项：**
无

**示例：**
1）带 C/S 支持:

```
sag service add bs server \”http://1.0.0.1 \” name testname
allow_path \”dir1/dir2\”\;\”dir3/dir4\” authtype a withcs yes compress no
```

2）不带 C/S 支持:

```
sag service add bs server \”http://1.0.0.1 \” name testname
allow_path \”dir1/dir2\”\;\”dir3/dir4\” authtype a withcs no compress no
encrpy l htmlprocess no
```

## 12.2.5 显示 CS 服务：

**语法：**

```
sag service show cs
```

**参数说明：**
service sslvpn 命令行部分，宏观配置类相关命令
show 显示类操作
cs 内容实体标识，cs

**注意事项：**
无

**示例：**

```
sag service show cs
```

### 12.2.6 删除 cs 服务:

**语法：**

sag service del cs id <value>

**参数说明：**

| | |
|---|---|
| service | sslvpn 命令行部分，宏观配置类相关命令 |
| del | 删除类基本操作 |
| cs | 内容实体标识，cs |
| id | 要删除服务的 id，6-15 位数字 |

**注意事项：**

无

**示例：**

sag service del cs id 1234567890123

### 12.2.7 修改现有 cs 服务:

**语法：**

sag service set cs id <value> server <string> port <type:port\;type:port...> name <name> [link <string>] attribute { nh | ns } [vname <name>] authtype { a | p | c | t } compress { no | gzip } [note <string>] [usernote <string>]

**参数说明：**

| | |
|---|---|
| service | sslvpn 命令行部分，宏观配置类相关命令 |
| set | 设置修改类操作 |
| cs | 内容实体标识，cs |
| id | 要删除服务的 id，6-15 位数字 |
| server | 服务器地址，如：\"http://1.0.0.1:8888\"，并且需要用'\"'将服务器地址括起来 |
| port | 服务器端口，格式为<类型：端口号>，类型有：TCP、UDP、DNS、FTP、IMAP、 LDAP、 MySQL、ORACLE、POP3、SMB、SMTP、SQLServer、TELNET 和 TFTP，端口号可以是 1～65535 之间的一个值 也可以是范围：如 254-888。可填为多个服务器端口，以'\;'分隔，如： TCP:443\;FTP:123-8888 |
| name | 客户端显示的 cs 名称，1-15 位中文、字母、数字、减号、下划线组合 |
| link | 页面链接 url，仅一个，以'\"'括起来 |
| attribute | 显示属性，ls：名称显示，链接显示，lh：名称显示，链接隐藏，nh 名称隐藏 |
| vname | 虚拟名字，1-15 位中文、字母、数字、减号、下划线组合 |
| authtype | 认证类别，a：匿名访问，p：通过口令访问，c：通过证书访问，t：通过双因素访问 |

compress 数据压缩，no：不压缩，gzip：gzip 方式压缩
note 注释或描述，可输入除制表符和分号外的任意可打印字符，以'\"'括起来
usernote 用户通知，以'\"'括起来

**注意事项：**
无

**示例：**
sag service set cs id 1702337717 server \"http://1.0.0.1:8888\" port TCP:443\;FTP:123-8888 name nametext attribute nh authtype a compress no
note \"notetext\" usernote \"usernotetext\"

## 12.2.8 添加 CS 服务：

**语法：**
sag service add cs server <string> port <type:port\;type:port...> name <name> [link <string>] attribute { nh | ns } [vname <name>] authtype { a | p | c | t } compress { no | gzip }[note <string>] [usernote <string>]

**参数说明：**
service sslvpn 命令行部分，宏观服务类相关命令
add 添加类基本操作
cs 内容实体标识，cs
server 服务器地址，如：\"http://1.0.0.1:8888\"，并且需要将服务器地址用'\"'将服务器地址括起来
port 服务器端口，格式为<类型：端口号>，类型有：TCP、UDP、DNS、FTP、IMAP、 LDAP、 MySQL、ORACLE、POP3、SMB、SMTP、SQLServer、TELNET 和 TFTP，端口号可以是 1～65535 之间的一个值 也可以是范围：如 254-888。可填为多个服务器端口，以'\;'分隔，如：TCP:443\;FTP:123-8888
name 显示名称,，1-15 位中文、字母、数字、减号、下划线组合
link 页面链接 url，仅一个，以'\"'括起来
attribute 显示属性，nh：名称显示，ns：名称隐藏
vname 虚拟名字，1-15 位中文、字母、数字、减号、下划线组合
authtype 认证类别，a：匿名访问，p：通过口令访问，c：通过证书访问 t：通过双因素访问
compress 数据压缩，no：不启用，gzip：压缩，默认为“不启用”
note 注释／描述，可输入除制表符和分号外的任意可打印字符，以'\"'括起来
usernote 用户通知，以'\"'括起来

**注意事项：**
无

**示例：**
sag service add cs server \"http://1.0.0.1\" port TCP:400-800 name nametext link \"http://www.baidu.com\" attribute ns vname virtual_name3 authtype c compress gzip note \"note_value\" usernote \"notice\"

## 12.2.9 显示网段服务:

**语法：**

sag service show net

**参数说明：**

| | |
|---|---|
| service | sslvpn 命令行部分，宏观服务类相关命令 |
| show | 显示类基本操作 |
| net | 显示对象，显示网段服务 |

**注意事项：**

无

**示例：**

sag service show net

## 12.2.10 删除现有网段服务:

**语法：**

sag service del net id <value>

**参数说明：**

| | |
|---|---|
| service | sslvpn 命令行部分，宏观服务类相关命令 |
| del | 删除类基本操作 |
| net | 标明对象，网段服务 |
| id | 要删除的服务 id，6-15 位数字 |

**注意事项：**

无

**示例：**

sag service del net id 1234567890123

## 12.2.11 修改现有网段服务:

**语法：**

sag service set net id <value> server <ip> port <type:port\;type:port...> name <name> attribute { nh | ns } authtype { a | p | c | t } [ note <string> ] [ usernote <string>]

**参数说明：**

service sslvpn 命令行部分，宏观服务类相关命令
set 修改类基本操作
net 标明对象，net 服务
id 要修改的服务 id，6-15 位数字
server 服务器地址，如：\”http://1.0.0.1:8888\”，并且需要将服务器地址用'\”'将服务器地址括起来
port 服务器端口，格式为<类型：端口号>，类型有：TCP、UDP，端口号可以是 1～65535 之间的一个值也可以是范围：如 254-888。可填为多个服务器端口，以'\;'分隔，如：TCP:443\;UDP:123-8888
name 显示名称，，1-15 位中文、字母、数字、减号、下划线组合
attribute 显示属性，nh：名称显示，ns：名称隐藏
authtype 认证类别，a：匿名访问，p：通过口令访问，c：通过证书访问
t：通过双因素访问
note 注释／描述，可输入除制表符和分号外的任意可打印字符，以'\”'括起来
usernote 用户通知，以'\”'括起来

**注意事项：**

无

**示例：**

sag service set net id 1702337717 \”http://1.0.0.1\” port TCP:400-800 name nametext attribute nh authtype a note \”note_value\” usernote \”notice\”

## 12.2.12 添加网段服务:

**语法：**

sag service add net server <ip> port <type:port\;type:port...> name <name> attribute { nh | ns } authtype { a | p | c | t } [note <string>] [usernote <string>]

**参数说明：**

service sslvpn 命令行部分，宏观服务类相关命令
add 添加类基本操作
net 标明对象，网段服务
server 服务器地址，如：\”http://1.0.0.1:8888\”，并且需要将服务器地址用'\”'将服务器地址括起来
port 服务器端口，格式为<类型：端口号>，类型有：TCP、UDP，端口号可以是 1～65535 之间的一个值也可以是范围：如 254-888。可填为多个服务器端口，以'\;'分隔，如：TCP:443\;UDP:123-8888
name 显示名称，1-15 位中文、字母、数字、减号、下划线组合
attribute 显示属性，nh：名称显示，ns：名称隐藏
authtype 认证类别，a：匿名访问，p：通过口令访问，c：通过证书访问
t：通过双因素访问
note 注释／描述，可输入除制表符和分号外的任意可打印字符，以'\”'括起来
usernote 用户通知，以'\”'括起来

**注意事项：**

无

**示例：**

sag service add net server \"http://1.0.0.1\" port TCP:400-800 name nametext attribute ns authtype c compress gzip note \"note_value\" usernote \"notice\"

## 12.2.13 显示 NC 服务:

**语法：**

sag service show nc

**参数说明：**

| | |
|---|---|
| service | sslvpn 命令行部分，宏观服务类相关命令 |
| show | 显示类基本操作 |
| nc | 显示对象，显示 NC 服务 |

**注意事项：**

无

**示例：**

sag service show nc。

## 12.2.14 删除 NC 服务:

**语法：**

sag service del nc id <string>

**参数说明：**

| | |
|---|---|
| service | sslvpn 命令行部分，宏观服务类相关命令 |
| del | 删除类基本操作 |
| nc | 标明对象，NC 服务 |
| id | 要删除的服务 id，6-15 位数字 |

**注意事项：**

无

**示例：**

sag service del nc id 1234567890123

## 12.2.15 修改 NC 服务:

**语法：**

sag service set nc id <value> server <string> port <type:port\;type:port...> name <name> [link <string>] attribute { nh | ns } [vname <name>] authtype { a | p | c | t } compress { no | gzip } [note <string>] [usernote <string>]

**参数说明：**

| | |
|---|---|
| service | sslvpn 命令行部分，宏观服务类相关命令 |
| set | 修改类基本操作 |
| nc | 标明对象，NC 服务 |
| id | 要修改的服务 id，6-15 位数字 |
| server | 服务器地址，如：\”http://1.0.0.1:8888\”，并且需要将服务器地址用\”"将服务器地址括起来 |
| port | 服服务器端口，格式为<类型：端口号>，类型有：TCP、UDP，端口号可以是 1～65535 之间的一个值也可以是范围：如 254-888。可填为多个服务器端口，以'\;'分隔，如：TCP:443\;UDP:123-8888 |
| name | 显示名称，1-15 位中文、字母、数字、减号、下划线组合 |
| link | 页面链接 url，仅一个，以\”"括起来 |
| attribute | 显示属性，nh：名称显示，ns：名称隐藏 |
| vname | 虚拟名字，1-15 位中文、字母、数字、减号、下划线组合 |
| authtype | 认证类别，a：匿名访问，p：通过口令访问，c：通过证书访问 t：通过双因素访问 |
| compress | 数据压缩，no：不启用，gzip：压缩，默认为“不启用” |
| note | 注释／描述，可输入除制表符和分号外的任意可打印字符，以\”"括起来 |
| usernote | 用户通知，以\”"括起来 |

**注意事项：**

无

**示例：**

sag service set nc id 1702337717 server \”http://1.0.0.1:8888\” port TCP:400-800 name nametext link \”link_value\” attribute ns vname vanemtext authtype c compress gzip note \”note_value\” usernote \”notice\”

## 12.2.16 添加 NC 服务:

**语法：**

sag service add nc server <string> port <type:port\;type:port...> name <name> [link <string>] attribute { nh | ns } [vname <name>] authtype { a | p | c | t } compress { no | gzip } [note <string>] [usernote <string>]

**参数说明：**

| | |
|---|---|
| service | sslvpn 命令行部分，宏观服务类相关命令 |
| add | 添加类基本操作 |

nc 标明对象，NC 服务
server 服务器地址，如：\”http://1.0.0.1:8888\”，并且需要将服务器地址用'\”'将服务器地址括起来
port 服务器端口，格式为<类型：端口号>，类型有：TCP、UDP，端口号可以是 1～65535 之间的一个值也可以是范围：如 254-888。可填为多个服务器端口，以'\;'分隔，如：TCP:443\;UDP:123-8888
name 显示名称，1-15 位中文、字母、数字、减号、下划线组合
link 页面链接 url，仅一个，以'\”'括起来
attribute 显示属性，nh：名称显示，ns：名称隐藏
vname 虚拟名字，1-15 位中文、字母、数字、减号、下划线组合
authtype 认证类别，a：匿名访问，p：通过口令访问，c：通过证书访问 t：通过双因素访问
compress 数据压缩，no：不启用，gzip：压缩，默认为“不启用”
note 注释／描述，可输入除制表符和分号外的任意可打印字符，以'\”'括起来
usernote 用户通知，以'\”'括起来

**注意事项：**
无

**示例：**
sag service add nc server \”http://1.0.0.1:8888\” port TCP:400-800 name nametext link \”link_value\” attribute ns vname vanemtext authtype c compress gzip note \”note_value\” usernote \”notice\”

## 12.2.17 显示授权界面：

**语法：**
sag service show auth id <value>

**参数说明：**
service sslvpn 命令行部分，宏观服务类相关命令
show 显示类基本操作
auth 显示对象，显示服务对应角色的授权信息
id 服务 id，6-15 位数字

**注意事项：**
无

**示例：**
sag service show auth id 1234567890123

## 12.2.18 添加角色给服务：

**语法：**

sag service add auth id <value> roleids <value;value...>

**参数说明：**

| | |
|---|---|
| service | sslvpn 命令行部分，宏观服务类相关命令 |
| add | 添加类基本操作 |
| auth | 标明对象，授权操作 |
| id | 服务 id，6-15 位数字 |
| roleids | 角色 id，6-15 位数字，可为多个，以'\;'分隔。不能为空 |

**注意事项：**

无

**示例：**

sag service add auth id 1234567890123 roleid 1234567890124\;1234567890125

## 12.2.19 显示用户访问规则：

**语法：**

sag service show rule id <value> roleid <value>

**参数说明：**

| | |
|---|---|
| service | sslvpn 命令行部分，宏观服务类相关命令 |
| show | 显示类基本操作 |
| rule | 显示对象，显示访问规则界面 |
| id | 服务 id，6-15 位数字 |
| roleid | 角色 id，6-15 位数字 |

**注意事项：**

无

**示例：**

sag service show rule id 1234567890123 roleid 1234567890124

## 12.2.20 配置用户访问规则：

**语法：**

sag service add rule id <value> roleid <value> display { on | off } direct { on | off } [saddr <ip;ip...>] [time <time;time..>] [day <day;day...>]

**参数说明：**

service　　sslvpn 命令行部分，宏观服务类相关命令
add　　添加类基本操作，该部分功能等同修改
rule　　标明对象，用户访问规则配置
id　　要修改的规则对应的服务 id，6-15 位数字
roleid　　要修改的规则对应的角色 id，6-15 位数字
display　　角色是否可见，on：可见，off：不可见，默认可见
direct　　角色是否跳转，on：跳转，off：不跳转，默认不跳转
saddr　　用户原地址范围，默认为空，格式：1.0.0.1/24，多个 ip 用'\;'分隔
time　　每天时间范围，格式：0:30-1:20，多个范围用'\;'分隔，时:（0～23）分：（00～59）
day　　每天天数范围，格式：0～6 或 0 到 6 单个值，不能存在前面数字比后面数字大的情况，如：6～4，多个范围用'\;'分隔

**注意事项：**

无

**示例：**

sag service add rule id <string> roleid <string> display on direct off saddr 1.0.0.1/24\;1.0.0.200/24 time 0:30-1:20\;2:30-4:10 day 0~3\;6

## 12.2.21 连通性测试：

**语法：**

sag service test connect target <string>

**参数说明：**

service　　sslvpn 命令行部分，宏观服务类相关命令
test　　测试类基本操作
connect　　测试对象，测试连通性
target　　参与测试的对象,格式：是否是 tcp（添 true 或 false）：服务器名：端口，支持多个，用'\;'相连，如： \"true:www.baidu.com:8889\"\;\"false:www.leadsec.com.cn:8000\"

**注意事项：**

无

**示例：**

sag service test connect target \"true:www.baidu.com:8889\"\;\"false:www.leadsec.com.cn:8000\"

## 12.2.22 自定义图标定制：

**语法：**

sag service set icon id <value> path <string> type { map | wcs | cs | csmap | NCMap }

**参数说明：**

service sslvpn 命令行部分，宏观服务类相关命令
set 设置类基本操作
icon 测试对象，图标
id 对应的服务 id，6-15 位数字
path 上传文件路径，包含文件名的完全路径，用'\"'括起来，如：\"/abc/ebd\"
type 服务类型，map , wcs ， cs， csmap， NCMap
服标识着几种不同的服务，map:bs 不带 cs，wcs：bs 带 cs 支持，cs：cs 服务，csmap：网段服务，NCMap：nc 服务

**注意事项：**

无

**示例：**

sag service set icon id 1234567890123 type map

## 12.2.23 缺省图标定制：

**语法：**

sag service set icon default id <value> type { map | wcs | cs | csmap | NCMap }

**参数说明：**

service sslvpn 命令行部分，宏观服务类相关命令
set 设置类基本操作
icon 测试对象，图标
default 缺省动作标识
id 对应的服务 id，6-15 位数字
type 服务类型，map , wcs ， cs， csmap， NCMap
服标识着几种不同的服务，map:bs 不带 cs，wcs：bs 带 cs 支持，cs：cs 服务，csmap：网段服务，NCMap：nc 服务

**注意事项：**

无

**示例：**

sag service set icon default id 1234567890123 type map

# 12.3 用户管理相关命令及配置：

## 12.3.1 显示部门基本信息：

**语法：**

sag user show department

**参数说明：**

| | |
|---|---|
| user | sslvpn 命令行部分，宏观用户类相关命令 |
| show | 显示类基本操作 |
| department | 显示对象，显示部门信息 |

**注意事项：**

无

**示例：**

sag user show department

## 12.3.2 增加部门：

**语法：**

sag user add department puid <value> name <name> role { on | off }

**参数说明：**

| | |
|---|---|
| user | sslvpn 命令行部分，宏观用户类相关命令 |
| add | 添加类基本操作 |
| department | 标明对象，部门相关操作 |
| puid | 上级部门 id，6-15 位数字或 0，无上级部门填 0 |
| name | 新创建部门名称，1-15 位中文、字母、数字、减号、下划线组合 |
| role | 是否创建与部门名称相同的角色，on：开启，off：不开启，默认为不开启 |

**注意事项：**

无

**示例：**

sag user add department puid 1234567890123 name leadsec role off

### 12.3.3 修改部门信息：

**语法：**

sag user set department puid <value> uid <value> name <name>

**参数说明：**

| | |
|---|---|
| user | sslvpn 命令行部分，宏观用户类相关命令 |
| set | 修改配置类基本操作 |
| department | 标明对象，部门相关操作 |
| puid | 上级部门 id，6-15 位数字或 0，无上级部门填 0 |
| uid | 该部门 id，6-15 位数字 |
| name | 新创建部门名称，1-15 位中文、字母、数字、减号、下划线组合 |

**注意事项：**

无

**示例：**

sag user set department puid 1234567890123 uid 1234567890126 name modname

### 12.3.4 删除某一个部门：

**语法：**

sag user del department puid <value> uid <value>

**参数说明：**

| | |
|---|---|
| user | sslvpn 命令行部分，宏观用户类相关命令 |
| del | 删除类基本操作 |
| department | 标明对象，部门相关操作 |
| puid | 上级部门 id，6-15 位数字或 0，无上级部门填 0 |
| uid | 该部门 id，6-15 位数字 |

**注意事项：**

无

**示例：**

sag user del department puid 1234567890123 uid 1234567890126

### 12.3.5 删除选中的多个部门：

**语法：**

sag user del department pid <value> uids <values;values...>

**参数说明：**

| | |
|---|---|
| user | sslvpn 命令行部分，宏观用户类相关命令 |
| del | 删除类基本操作 |
| department | 标明对象，部门相关操作 |
| pid | 上级部门 id，6-15 位数字或 0，无上级部门填 0 |
| uids | 部门 id,可为多个，中间使用‘\;’分隔 |

**注意事项：**

无

**示例：**

sag user del department pid 1234567890123 uids 1234567890126\;1234567890127

## 12.3.6 显示部门内用户：

**语法：**

sag user show user type { p | c | t } uid <value>

**参数说明：**

| | |
|---|---|
| user | sslvpn 命令行部分，宏观用户类相关命令 |
| show | 显示类基本操作 |
| user | 显示对象，显示用户信息 |
| type | 用户类型，p：口令用户，c：证书用户，t：双因素用户，默认口令用户 |
| uid | 该部门 id，6-15 位数字 |

**注意事项：**

无

**示例：**

sag user show user type p uid 1234567890123

## 12.3.7 增加口令用户：

**语法：**

sag user add passworduser uid <value> name <name> password <password> [username <name>] [email <email>] [phonenumber <number>] [bindip <ip>] [bindmac <mac>] [bindhost <hostname>] [note <string>] share { on | off } modifypsw { on | off} vip { on | off } sms { on | off }

**参数说明：**

| | |
|---|---|
| user | sslvpn 命令行部分，宏观用户类相关命令 |

| | |
|---|---|
| add | 添加类基本操作 |
| passworduser | 标明对象，口令用户相关操作 |
| uid | 该部门 id，6-15 位数字 |
| name | 新创建用户名称，1-15 位中文、字母、数字、减号、下划线组合 |
| password | 登录口令 |
| username | 用户名字，1-15 位中文、字母、数字、减号、下划线组合 |
| email | 电子邮件，标准邮件格式 |
| phonenumber | 手机号码 |
| bindip | 绑定 ip，格式如： 192.168.0.1 |
| bindmac | 绑定 MAC，可用字符：A—F 大小写英文字母，数字，减号，冒号；格式：XX-XX-XX-XX-XX-XX，或 XX:XX:XX:XX:XX:XX |
| bindhost | 绑定主机，可用字符：任意可打印字符，不包括斜线、反斜线、冒号、星号、问号、双引号、大于号、小于号、 管道符、制表符 |
| note | 描述，以'\"'括起来 |
| share | 帐号共享开关，on：开启，off：关闭，默认关闭 |
| modifypsw | 可修改口令开关，on：开启，off：关闭，默认开启 |
| vip | VIP 用户开关，on：开启，off：关闭，默认关闭 |
| sms | 短信用户，on：开启，off：关闭，默认关闭 |

**注意事项：**

无

**示例：**

sag user add passworduser uid 335168849 name PASSWORDUSER password 123456789 username leadsec email denglz3@leadsec.com.cn phonenumber 13811977477 bindip 192.168.0.1 bindmac ab:12:3a:34:b1:34 bindhost hostname share off modifypsw on vip off sms on

## 12.3.8 增加证书用户：

**语法：**

sag user add certuser uid <value> name <name> [company <string>] [department <string>] [country <country>] [email <email>] [phonenumber <number>] [bindip <ip>] [bindmac <mac>] [bindhost <hostname>] starttime

<y-m-d-h> endtime <y-m-d-h> share { on | off } [note <string>] csp <string> keylen {1024 | 2048} [certpsw <password>] keyexport { on | off } keyprotect { on | off }

**参数说明：**

| | |
|---|---|
| user | sslvpn 命令行部分，宏观用户类相关命令 |
| add | 添加类基本操作 |
| certuser | 标明对象，证书用户相关操作 |
| uid | 该部门 id，6-15 位数字 |
| name | 新创建用户名称，1-15 位中文、字母、数字、减号、下划线组合 |
| company | 单位，以'\"'括起来。默认为空 |
| department | 部门，以'\"'括起来。默认为空 |
| country | 国家，只能是字符或数字，为两个字节。默认 CN |
| email | 电子邮件，标准电子邮件格式，默认为空 |
| phonenumber | 手机号码，11 位数字 |
| bindip | 绑定 ip，格式如： 192.168.0.1 |
| bindmac | 绑定 MAC，可用字符：A—F 大小写英文字母，数字，减号，冒号；格 |

式：XX-XX-XX-XX-XX-XX，或 XX:XX:XX:XX:XX:XX
bindhost 绑定主机，可用字符：任意可打印字符，不包括斜线、反斜线、冒号、星号、问号、双引号、大于号、小于号、 管道符、制表符
starttime 启用时间，格式如：2011-5-17-8 或 2011/5/17/8
endtime 到期时间，格式如：2011-5-17-8 或 2011/5/17/8
share 帐号共享开关，on：开启，off：关闭；默认关闭
note 描述，以\"括起来
csp csp 值，以\"括起来，默认为：”Leadsec 网御安全网关”
keylen 密钥长度，密钥长度，1024 和 2048 位可选
certpsw 证书密码
keyexport 私钥可导开关，on：可导，off：不可导，默认不可导
keyprotect 密钥保护开关，on：开启，off：不开启，默认不开启

**注意事项：**
无

**示例：**
sag user add certuser uid 335168849 name CERTUSER company \"leadsec\" department \"soft\" country CN email denglizhi@163.com phonenumber 13811977477 bindip 192.168.0.1 bindmac ab:12:3a:34:b1:34 bindhost hostname starttime 2011-9-3-12 endtime 2011-10-11-2 share off csp cspvalue keylen 1024 certpsw 123456789 keyexport on keyprotect on

## 12.3.9 增加双因素用户：

**语法：**
sag user add twoauthuser uid <value> passworduser name <name> by {local {password <password> [username <name>] [email <email>] [phonenumber <number>] [bindip <ip>] [bindmac <mac>] [bindhost <hostname>] [note <string>] share { on | off } modifypsw { on | off} vip { on | off } sms { on | off }} | ldap | radius | ad} certuser by { local {name <name>[company <string>] [department <string>] [country <country>] [email <email>] [phonenumber <number>] [bindip <ip>] [bindmac <mac>] ［bindhost <hostname>］starttime <y-m-d-h> endtime <y-m-d-h> share { on | off } [note <string>] csp <string> keylen {1024 | 2048 } [certpsw <string>] keyexport { on | off } keyprotect { on | off}} | {ldap | ad | file } name <string> }

**参数说明：**
user sslvpn 命令行部分，宏观用户类相关命令
add 添加类基本操作
twoauthuser 标明对象，双因素用户相关操作
uid 该部门 id，6-15 位数字
passworduser 证书因素
name 新创建用户名称，1-15 位中文、字母、数字、减号、下划线组合
company 单位，以\"括起来
by 方法
local 方法类别
password 登录口令
username 用户名字
email 电子邮件，标准邮件格式
phonenumber 手机号码

bindip 绑定 ip，格式如 192.168.0.1
bindmac 绑定 MAC，可用字符：A—F 大小写英文字母，数字，减号，冒号；格式：XX-XX-XX-XX-XX-XX，或 XX:XX:XX:XX:XX:XX
bindhost 绑定主机，可用字符：任意可打印字符，不包括斜线、反斜线、冒号、星号、问号、双引号、大于号、小于号、 管道符、制表符
note 描述，以'\"'括起来
share 帐号共享开关，on：开启，off：关闭，默认关闭
modifypsw 可修改口令开关，on：开启，off：关闭，默认开启
vip VIP 用户开关，on：开启，off：关闭，默认关闭
sms 短信用户，on：开启，off：关闭，默认关闭
local|dap|radius|ad 添加口令因素方式，local 为本地口令用户，需要参数为该行以上部分；ldap，radius，ad 为三种第三方口令服务器添加用户方式。无其余参数
cert 证书因素
by 方法
local 方法类别
company 单位，以'\"'括起来
department 部门，以'\"'括起来
country 国家，只能是字符或数字，为两个字节。默认 CN
email 电子邮件，标准电子邮件格式，默认为空
phonenumber 手机号码，11 位数字
bindip 绑定 ip，格式如： 192.168.0.1
bindmac 绑定 MAC，可用字符：A—F 大小写英文字母，数字，减号，冒号；格式：XX-XX-XX-XX-XX-XX，或 XX:XX:XX:XX:XX:XX
bindhost 绑定主机，可用字符：任意可打印字符，不包括斜线、反斜线、冒号、星号、问号、双引号、大于号、小于号、 管道符、制表符
starttime 启用时间，格式如：2011-5-17-8 或 2011/5/17/8
endtime 到期时间，格式如：2011-5-17-8 或 2011/5/17/8
share 帐号共享开关，on-开启；off-关闭；默认关闭
note 描述，以'\"'括起来
csp csp 值，以'\"'括起来，默认为：”Leadsec 网御安全网关”
keylen 密钥长度，1024 和 2048 位可选
certpsw 证书密码，以'\"'括起来
keyexport 私钥可导开关，on：可导，off：不可导，默认不可导
keyprotect 密钥保护开关，on：开启，off：不开启，默认不开启
local|ldap|ad|file 添加口令因素方式，local 为本地口令用户，需要参数为该行以上部分；ldap，radius，ad 为三种第三方口令服 务器添加用户方式
name 第三方证书名，为从第三方服务器端获得值

**注意事项：**

无

**示例：**

sag user add twoauthuser uid 335168849 passworduser name localuser by local password 123456 username vname email denglizhi133@163.com phonenumber 13811977477 bindip 192.168.0.1 bindmac 123:456:789 bindhost denglizhi-host note new-note share on modifypsw off vip on sms on certuser by local name localuser company cnmp department software country china email denglizhi133@163.com phonenumber 13811977477 bindip 192.168.0.1 bindmac 123:456:789 bindhost denglizhi-host starttime 2010-01-02-08 endtime 2012-01-02-09 share on note

cert-note csp csp-value keylen 102 4 certpsw 147258369 keyexport off keyprotect on

## 12.3.10 修改口令用户信息：

**语法：**

sag user set passworduser uid <value> pid <value> name <name> password <password> [username <name>] [email <email>] [phonenumber <number>] [bindip <ip>] [bindmac <mac>] [bindhost <hostname>] [note <string>] accountpend { on | off } share { on | off } modifypsw { on | off} vip { on | off } sms { on | off }

**参数说明：**

| | |
|---|---|
| set | 修改配置类基本操作 |
| passworduser | 标明对象，口令用户相关操作 |
| uid | 该部门 id，6-15 位数字 |
| pid | 用户 id，6-15 位数字 |
| name | 新创建用户名称，1-15 位中文、字母、数字、减号、下划线组合 |
| password | 登录口令 |
| username | 用户名字，1-15 位中文、字母、数字、减号、下划线组合 |
| email | 电子邮件，标准邮件格式 |
| phonenumber | 手机号码 |
| bindip | 绑定 ip，格式如： 192.168.0.1 |
| bindmac | 绑定 MAC，可用字符：A—F 大小写英文字母，数字，减号，冒号；格式：XX-XX-XX-XX-XX-XX，或 XX:XX:XX:XX:XX:XX |
| bindhost | 绑定主机，可用字符：任意可打印字符，不包括斜线、反斜线、冒号、星号、问号、双引号、大于号、小于号、 管道符、制表符 |
| note | 描述，以\"括起来 |
| accountpend | 帐号挂起开关，on：挂起，off：不挂起，默认不挂起 |
| share | 帐号共享开关，on：开启，off：关闭，默认关闭 |
| modifypsw | 可修改口令开关，on：开启，off：关闭，默认开启 |
| vip | 用户开关，on：开启，off：关闭，默认关闭 |
| sms | 短信用户，on：开启，off：关闭，默认关闭 |

**注意事项：**

无

**示例：**

sag user add passworduser uid 335168849 pid 1234567890123 name PASSWORDUSER password 123456789 username leadsec email denglz3@leadsec.com.cn phonenumber 13811977477 bindip 192.168.0.1 bindmac ab:12:3a:34:b1:34 accountpend off share off modifypsw on vip off sms on

## 12.3.11 修改口令用户有效期：

**语法：**

sag user set passworduser uid <value> policy { a | n | s starttime <y-m-d-h> endtime <y-m-d-h>}

**参数说明：**

| | |
|---|---|
| user | sslvpn 命令行部分，宏观用户类相关命令 |
| set | 修改配置类基本操作 |
| passworduser | 标明对象，口令用户相关操作 |
| uid | 该用户 id，6-15 位数字 |
| policy | 期限控制策略，a：一直生效，n：一直失效，s：详细控制，默认一直生效 |
| starttime | 启用时间，格式如：2011-5-17-8 或 2011/5/17/8 |
| endtime | 到期时间，格式如：2011-5-17-8 或 2011/5/17/8 |

**注意事项：**
无

**示例：**
sag user set passworduser uid 1234567890123 policy s starttime 2011-10-10-12 endtime 2011-10-11-12

## 12.3.12 移动用户：

**语法：**
sag user mov user suid <value> duid <value> id <value> type { p | c | t }

**参数说明：**

| | |
|---|---|
| user | sslvpn 命令行部分，宏观用户类相关命令 |
| mov | 移动用户操作类基本操作 |
| user | 标明对象，用户相关操作 |
| suid | 原所属部门 id，6-15 位数字 |
| duid | 目的部门 id，6-15 位数字 |
| id | 该用户 id，6-15 位数字 |
| type | 用户类型，p：口令用户，c：证书用户，t：双因素用户 |

**注意事项：**
无

**示例：**
sag user mov user suid 1234567890123 duid 1234567890124 id 1234567890125 type p

## 12.3.13 删除口令用户：

**语法：**
sag user del passworduser uid <value> id <value>

**参数说明：**

| | |
|---|---|
| user | sslvpn 命令行部分，宏观用户类相关命令 |

| | |
|---|---|
| del | 删除类基本操作 |
| passworduser | 标明对象，口令用户 |
| uid | 所属部门 id，6-15 位数字 |
| id | 该用户 id，6-15 位数字 |

**注意事项：**
无

**示例：**
sag user del passworduser uid 335168849 id 3435036876

## 12.3.14 用户角色设置显示：

**语法：**
sag user show role type { p | c | t } uid <value> id <value>

**参数说明：**

| | |
|---|---|
| user | sslvpn 命令行部分，宏观用户类相关命令 |
| show | 显示类基本操作 |
| role | 显示对象，操作与用户角色相关 |
| type | 用户类型，p：口令用户，c：证书用户，t：双因素用户，默认口令用户 |
| uid | 该部门 id，6-15 位数字 |
| id | 用户 id，6-15 位数字 |

**注意事项：**
无

**示例：**
sag user show role type p uid 1234567890123 id 1234567890124

## 12.3.15 口令用户角色授权设置：

**语法：**
sag user add passworduser roletouser uid <value> rids <value;value..> id <value>

**参数说明：**

| | |
|---|---|
| user | sslvpn 命令行部分，宏观用户类相关命令 |
| add | 显示类基本操作 |
| passworduser | 显示对象，口令用户相关信息 |
| roletouser | 操作类型 |
| uid | 该部门 id，6-15 位数字 |

| | |
|---|---|
| rids | 角色 id，6-15 位数字，可为多个，中间使用‘\;’分隔 |
| id | 用户 id，6-15 位数字 |

**注意事项：**

无

**示例：**

sag user add passworduser roletouser uid 1234567890123 rids 1234567890125\; 1234567890128 id 1234567890126

## 12.3.16 口令用户升级为双因素用户:

**语法：**

sag user upgrade passworduser totwoauth uid <value> pid <value> name <name> [company <string>] [department <string>] [country <country>] [email <email>] [phonenumber <number>] [bindip <ip>] [bindmac <mac>] ［bindhost <hostname>］starttime <y-m-d-h> endtime <y-m-d-h> share { on | off } [note <string>] csp <string> keylen < 1024 | 2048 > [certpsw <password>] keyexport { on | off } keyprotect { on | off}

**参数说明：**

| | |
|---|---|
| user | sslvpn 命令行部分，宏观用户类相关命令 |
| upgrade | 升级类基本操作 |
| passworduser | 显示对象，口令用户相关操作 |
| totwoauth | 操作类型 |
| uid | 该部门 id，6-15 位数字 |
| pid | 口令用户 id，6-15 位数字 |
| name | 新创建用户名称，1-15 位中文、字母、数字、减号、下划线组合 |
| company | 单位，以\"”括起来 |
| department | 部门，以\"”括起来 |
| country | 国家，只能是字符或数字，为两个字节，默认 CN |
| email | 电子邮件，标准电子邮件格式，默认为空 |
| phonenumber | 手机号码，11 位数字 |
| bindip | 绑定 ip，格式如： 192.168.0.1 |
| bindmac | 绑定 MAC，可用字符：A—F 大小写英文字母，数字，减号，冒号；格式：XX-XX-XX-XX-XX-XX，或 XX:XX:XX:XX:XX:XX |
| bindhost | 绑定主机，可用字符：任意可打印字符，不包括斜线、反斜线、冒号、星号、问号、双引号、大于号、小于号、 管道符、制表符 |
| starttime | 启用时间，格式如：2011-5-17-8 或 2011/5/17/8 |
| endtime | 到期时间，格式如：2011-5-17-8 或 2011/5/17/8 |
| share | 帐号共享开关，on：开启，off：关闭，默认关闭 |
| note | 描述，以\"”括起来 |
| csp | csp，以\"”括起来，默认为“Leadsec 网御安全网关” |
| keylen | 密钥长度，1024 和 2048 位可选 |
| certpsw | 证书密码，以\"”括起来 |
| keyexport | 私钥可导开关，on：可导，off：不可导。默认不可导 |
| keyprotect | 密钥保护开关，on：开启，off：不开启。默认不开启 |

**注意事项：**

无

**示例：**

sag user upgrade passworduser totwoauth uid 1235678978 pid 1234564 name testname company \"leadsec\" department \"develop\" country CN email zhangsan@leadsec.com.cn phonenumber 123445678925 bindip 192.168.0.1 bindmac 123:456:789 bindhost hostname starttime 2010-1-2-8 endtime 2012-8-2-9 share on note \"notetext\" csp \"csp-value\" keylen 1024 certpsw \"147258369\" keyexport off keyprotect on

## 12.3.17 证书用户信息显示:

**语法：**

sag user show certuser uid <value> cid <value>

**参数说明：**

| | |
|---|---|
| user | sslvpn 命令行部分，宏观用户类相关命令 |
| show | 显示类基本操作 |
| certuser | 标明对象，证书用户相关操作 |
| uid | 该部门 id，6-15 位数字 |
| cid | 证书 id，数字字母组合 |

**注意事项：**

无

**示例：**

sag user show certuser uid 1234567890123 cid 12345adb7890125

## 12.3.18 修改证书用户信息:

**语法：**

sag user set certuser uid <value> cid <value> [email <email>] [phonenumber <number>] [bindip <ip>] [bindmac <mac>] [bindhost <hostname>] starttime <y-m- d-h> endtime <y-m-d-h> share { on | off } [note <string>]

**参数说明：**

| | |
|---|---|
| user | sslvpn 命令行部分，宏观用户类相关命令 |
| set | 修改配置类基本操作 |
| certuser | 标明对象，证书用户相关操作 |
| uid | 该部门 id，6-15 位数字 |
| cid | 证书用户 id，数字字母组合 |
| email | 电子邮件，标准邮件格式 |

phonenumber 手机号码
bindip 绑定 ip，格式如： 192.168.0.1
bindmac 绑定 MAC，可用字符：A—F 大小写英文字母，数字，减号，冒号；格式：XX-XX-XX-XX-XX-XX，或 XX:XX:XX:XX:XX:XX
bindhost 绑定主机，可用字符：任意可打印字符，不包括斜线、反斜线、冒号、星号、问号、双引号、大于号、小于号、 管道符、制表符
starttime 启用时间，格式如：2011-5-17-8 或 2011/5/17/8
endtime 到期时间，格式如：2011-5-17-8 或 2011/5/17/8
share 帐号共享开关，on：开启，off：关闭，默认关闭
note 描述，以'\"'括起来

**注意事项：**
无

**示例：**
sag user set certuser uid 1234567890123 cid 123233add2321 email shangyp@163.com phonenumber 13811075355 bindip 1.0.0.112 bindmac 32:ab:45:2d:63:1c starttime 2011-10-11-15 endtime 2011-11-10-15 share on note \"notetext\"

## 12.3.19 挂起证书用户:

**语法：**
sag user pend certuser uid <value> cid <value>

**参数说明：**
user sslvpn 命令行部分，宏观用户类相关命令
set 修改配置类基本操作
certuser 标明对象，证书用户相关操作
uid 该部门 id，6-15 位数字
cid 证书用户 id，数字字母组合

**注意事项：**
无

**示例：**
sag user pend certuser uid 1234567890123 cid 123321

## 12.3.20 证书用户升级为双因素用户：

**语法：**
sag user upgrade certuser totwoauth uid <value> cid <value> password <password> [email <email>] [phonenumber <number>] [bindip <ip>] [bindmac <mac>] [bindhost <hostname>] [note <string>]

**参数说明：**

| | |
|---|---|
| user | sslvpn 命令行部分，宏观用户类相关命令 |
| upgrade | 升级类基本操作 |
| certuser | 显示对象，口令用户相关操作 |
| totwoauth | 操作类型 |
| uid | 该部门 id，6-15 位数字 |
| cid | 证书用户 id，数字字母组合 |
| password | 登录口令 |
| email | 电子邮件，标准邮件格式 |
| phonenumber | 手机号码 |
| bindip | 绑定 ip，格式如： 192.168.0.1 |
| bindmac | 绑定 MAC，可用字符：A—F 大小写英文字母，数字，减号，冒号；格式：XX-XX-XX-XX-XX-XX，或 XX:XX:XX:XX:XX:XX |
| bindhost | 绑定主机，可用字符：任意可打印字符，不包括斜线、反斜线、冒号、星号、问号、双引号、大于号、小于号、 管道符、制表符 |
| note | 描述，以'\"'括起来 |

**注意事项：**

无

**示例：**

sag user upgrade certuser totwoauth uid 1234567890123 cid 12s345ad67890124 password 12345678 email wangjj11@leadsec.com.cn phonenumber 13811075355 bindip 1.0.0.112 bindmac 34:ab:3e:93:2f:92 bindhost hostname note \"notetext\"

## 12.3.21 证书用户授权:

**语法：**

sag user add certuser roletouser uid <value> rids <value;value...> cid <value>

**参数说明：**

| | |
|---|---|
| user | sslvpn 命令行部分，宏观用户类相关命令 |
| add | 添加类基本操作 |
| certuser | 显示对象，证书用户相关操作 |
| roletouser | 操作类型，用户授权 |
| uid | 该部门 id，6-15 位数字 |
| rids | 授予权限的角色 id，6-15 位数字，可为多个，以'\;'分隔 |
| cid | 证书用户 id，数字字母组合 |

**注意事项：**

无

**示例：**

sag user add certuser roletouser uid 1234567890123 rids 1234567890125\;23142351 cid 123456ab7890126

## 12.3.22 删除证书用户:

**语法：**

sag user del certuser uid <value> cid <value>

**参数说明：**

| | |
|---|---|
| user | sslvpn 命令行部分，宏观用户类相关命令 |
| del | 删除类基本操作 |
| certuser | 显示对象，证书用户相关操作 |
| uid | 该部门 id，6-15 位数字 |
| cid | 证书用户 id，数字字母组合 |

**注意事项：**

无

**示例：**

sag user del certuser uid 1234567890123 cid 1234567890126

## 12.3.23 双因素用户信息修改（带本地口令因素）:

**语法：**

sag user set twoauthuser password uid <value> pid <value> cid <value> password <password> modifypsw { on | off} [email <email>] [phonenumber <number>] [bindip <ip>] [bindmac <mac>] [bindhost <hostname>] starttime <y-m-d-h> endtime <y-m-d-h> share { on | off } [note <string>]

**参数说明：**

| | |
|---|---|
| user | sslvpn 命令行部分，宏观用户类相关命令 |
| set | 设置修改类基本操作 |
| twoauthuser | 显示对象，双因素用户相关操作 |
| password | 本地口令因素，该双因素用户的口令因素为本地添加 |
| uid | 该部门 id，6-15 位数字 |
| pid | 口令因素 id，6-15 位数字 |
| cid | 证书因素 id，数字字母组合 |
| password | 登录口令 |
| modifypsw | 可修改口令开关，on：开启，off：关闭，默认关闭 |
| email | 电子邮件，标准邮件格式 |
| phonenumber | 手机号码 |
| bindip | 绑定 ip，格式如： 192.168.0.1 |
| bindmac | 绑定 MAC，可用字符：A—F 大小写英文字母，数字，减号，冒号；格 |

式：XX-XX-XX-XX-XX-XX，或 XX:XX:XX:XX:XX:XX
bindhost 绑定主机，可用字符：任意可打印字符，不包括斜线、反斜线、冒号、星号、问号、双引号、大于号、小于号、 管道符、制表符
starttime 启用时间，格式如：2011-5-17-8 或 2011/5/17/8
endtime 到期时间，格式如：2011-5-17-8 或 2011/5/17/8
share 帐号共享开关，on：开启，off：关闭，默认关闭
note 描述，以\"括起来

**注意事项：**
无

**示例:**
sag user set twoauthuser password uid 1234567890123 pid 23423432423 cid 54545abc454 password 123456789 modifypsw off email shangyp@163.com phonenumber 15110268809 bindip 1.0.0.1 bindmac 34:ab:3e:93:2f:92 bindhost hostname starttime 2011-10-11-12 endtime 2011-10-11-14 share off note \"notetext\"

## 12.3.24 删除双因素用户:

**语法：**
sag user del twoauthuser uid <value> pid <value> cid <value>

**参数说明：**
user sslvpn 命令行部分，宏观用户类相关命令
del 删除类基本操作
twoauthuser 显示对象，双因素用户相关操作
uid 该部门 id，6-15 位数字
pid 口令因素 id，6-15 位数字
cid 证书因素 id，数字字母组合

**注意事项：**
无

**示例:**
sag user del twoauthuser uid 1234567890123 pid 1289843585 cid 123ab6789ef0

## 12.3.25 双因素用户降级:

**语法：**
sag user degrade twoauthuser uid <value> pid <value> cid <value> type { p | c }

**参数说明：**

| | |
|---|---|
| user | sslvpn 命令行部分，宏观用户类相关命令 |
| degrade | 降级类基本操作 |
| twoauthuser | 显示对象，双因素用户相关操作 |
| uid | 该部门 id，6-15 位数字 |
| pid | 口令因素 id，6-15 位数字 |
| cid | 证书因素 id，数字字母组合 |
| type | 要降级到的类型种类，p：口令用户，c：证书用户 |

**注意事项：**
无

**示例:**
sag user del twoauthuser uid 1234567890123 pid 1234567890125 cid 1234567890126 type c

## 12.3.26 挂起双因素用户:

**语法：**
sag user pend twoauthuser uid <value> pid <value> cid <value>

**参数说明：**

| | |
|---|---|
| user | sslvpn 命令行部分，宏观用户类相关命令 |
| pend | 挂起类基本操作 |
| twoauthuser | 显示对象，双因素用户相关操作 |
| uid | 该部门 id，6-15 位数字 |
| pid | 口令因素 id，6-15 位数字 |
| cid | 证书因素 id，数字字母组合 |

**注意事项：**
无

**示例:**
sag user pend twoauthuser uid 1234567890123 pid 1234567890125 cid
12367akl89de01

## 12.3.27 批量删除口令用户:

**语法：**
sag user del passworduser more uid <value> pids <value\;value..>

**参数说明：**

| | |
|---|---|
| user | sslvpn 命令行部分，宏观用户类相关命令 |

| | |
|---|---|
| del | 删除类基本操作 |
| passworduser | 显示对象，口令用户相关操作 |
| more | 批量删除 |
| uid | 该部门 id，6-15 位数字 |
| pids | 口令用户 id，可为多个，中间使用'\;'分隔 |

**注意事项：**
无

**示例:**
sag user del passworduser more uid 1234567890123 pids 1234567890125\ ;1234567890126

## 12.3.28 批量删除证书用户:

**语法：**
sag user del certuser more uid <value> cids <value;value..>

**参数说明：**

| | |
|---|---|
| user | sslvpn 命令行部分，宏观用户类相关命令 |
| del | 删除类基本操作 |
| certuser | 显示对象，证书用户相关操作 |
| more | 批量删除 |
| uid | 该部门 id，6-15 位数字 |
| cids | 证书用户 id，数字字母组合，可为多个，中间使用'\;'分隔 |

**注意事项：**
无

**示例:**
sag user del certuser more uid 1234567890123 cids 1234567890125\ ; 1234567890126

## 12.3.29 批量删除双因素用户:

**语法：**
sag user del twoauthuser more uid <value> { pids <value;value..> | cids <value;value..> }

**参数说明：**

| | |
|---|---|
| user | sslvpn 命令行部分，宏观用户类相关命令 |
| del | 删除类基本操作 |
| twoauthuser | 显示对象，证书用户相关操作 |
| more | 批量删除 |
| uid | 该部门 id，6-15 位数字 |

| | |
|---|---|
| pids | 口令因素 id，6-15 位数字，可为多个，中间使用'\;'分隔 |
| cids | 证书因素 id，数字字母组合，可为多个，中间使用'\;'分隔 |

**注意事项：**
无

**示例:**
sag user del twoauthuser more uid 1234567890123 cids 1234567890125\ ; 1234567890126

## 12.3.30 用户数据导出:

**语法：**
sag user export { csv | data }

**参数说明：**

| | |
|---|---|
| user | sslvpn 命令行部分，宏观用户类相关命令 |
| export | 导出文件格式，分为 csv 和 date 两种 |

**注意事项：**
无

**示例:**
sag user export csv

## 12.3.31 用户数据导入:

**语法：**
sag user inport { csv | data } path <string>

**参数说明：**

| | |
|---|---|
| user | sslvpn 命令行部分，宏观用户类相关命令 |
| inport | 导出文件格式，分为 csv 和 date 两种 |
| path | 上传用户备份文件路径，以'\"'括起来，实现将该文件按照固定文件名存储到指定路径下即可，若当前已经存在，则覆盖 |

**注意事项：**
无

**示例:**
sag user inport csv path \"e:/a/b/c/d.csv\"

## 12.3.32 升级口令用户，通过 ldap 添加证书因素:

**语法：**

sag user upgrade passworduser by ldap uid <value> pid <value> name <name>

**参数说明：**

| | |
|---|---|
| user | sslvpn 命令行部分，宏观用户类相关命令 |
| upgrade | 升级类基本操作 |
| passworduser | 口令用户 |
| by | 指明方式 |
| ldap | 第三方的方式种类 |
| uid | 部门 id，6-15 位数字 |
| pid | 口令用户 id，6-15 位数字 |
| name | 通过第三方添加的因素名称,对于 LDAP 和 AD 为 DN 全名，对于证书为其显示名字 |

**注意事项：**

无

**示例:**

sag user upgrade passworduser by ldap uid 1234567890123 pid 1234567890124 name uid=%user %,o=tcl,c=cn

## 12.3.33 升级口令用户，通过 ad 添加证书因素:

**语法：**

sag user upgrade passworduser by ad uid <value> pid <value> name <name>

**参数说明：**

| | |
|---|---|
| user | sslvpn 命令行部分，宏观用户类相关命令 |
| upgrade | 升级类基本操作 |
| by | 指明方式 |
| ad | 第三方的方式种类 |
| uid | 部门 id，6-15 位数字 |
| pid | 口令用户 id，6-15 位数字 |
| name | 通过第三方添加的因素名称,对于 LDAP 和 AD 为 DN 全名，对于证书为其显示名字 |

**注意事项：**

无

**示例:**

sag user upgrade passworduser by ad uid 1234567890123 pid 1234567890124 name %user %@leadsec.sag.com

## 12.3.34 升级口令用户，通过文件添加证书因素:

**语法：**

sag user upgrade passworduser by file uid <value> pid <value> name <name>

**参数说明：**

| | |
|---|---|
| user | sslvpn 命令行部分，宏观用户类相关命令 |
| upgrad | 升级类基本操作 |
| passworduser | 口令用户 |
| by | 指明方式 |
| file | 第三方的方式种类 |
| uid | 部门 id，6-15 位数字 |
| pid | 口令用户 id，6-15 位数字 |
| name | 通过第三方添加的因素名称，对于 LDAP 和 AD 为 DN 全名，对于证书为其显示名字 |

**注意事项：**

无

**示例:**

sag user upgrade passworduser by file uid 1234567890123 pid 1234567890124 name %user %@leadsec.sag.com

## 12.3.35 升级证书用户，通过 ldap 添加口令因素：

**语法：**

sag user upgrade certuser by ldap uid <value> cid <value> name <name>

**参数说明：**

| | |
|---|---|
| user | sslvpn 命令行部分，宏观用户类相关命令 |
| upgrade | 升级类基本操作 |
| certuser | 证书用户 |
| by | 指明方式 |
| ldap | 第三方的方式种类，第三方 ldap 用户 |
| uid | 部门 id，6-15 位数字 |
| cid | 证书用户 id，6-15 位数字 |

| | |
|---|---|
| name | 通过第三方添加的因素名称，对于 LDAP 和 AD 为 DN 全名，对于证书为其显示名字 |

**注意事项：**
无

**示例:**
sag user upgrade certuser by ldap uid 1234567890123 cid 12345678901234 name uid=%user%,o=tcl,c=cn

## 12.3.36 升级证书用户，通过 ad 添加口令因素：

**语法：**
sag user upgrade certuser by ad uid <value> cid <value> name <name>

**参数说明：**

| | |
|---|---|
| user | sslvpn 命令行部分，宏观用户类相关命令 |
| upgrade | 升级类基本操作 |
| certuser | 证书用户 |
| by | 指明方式 |
| ad | 第三方的方式种类，第三方 ad 用户 |
| uid | 部门 id，6-15 位数字 |
| cid | 证书用户 id，数字字母组合 |

**注意事项：**
无

**示例:**
sag user upgrade certuser by ad uid 1234567890123 cid 12345678901234 name %user %@leadsec.sag.com

## 12.3.37 升级证书用户，通过 radius 添加口令因素：

**语法：**
sag user upgrade certuser by radius uid <value> cid <value> name <name>

**参数说明：**

| | |
|---|---|
| user | sslvpn 命令行部分，宏观用户类相关命令 |
| upgrade | 升级类基本操作 |
| certuser | 证书用户 |

by 指明方式
radius 第三方的方式种类，第三方 radius 用户
uid 部门 id，6-15 位数字
cid 证书用户 id，6-15 位数字
name 通过第三方添加的因素名称，对于 LDAP 和 AD 为 DN 全名，对于证书为其显示名字

**注意事项：**
无

**示例:**
sag user upgrade certuser by radius uid 1234567890123 cid 12345678901234 name TEST

## 12.3.38 修改带有第三方因素的双因素用户信息：

**语法：**
sag user set twoauthuser thirdpart uid <value> pid <value> cid <value> [email <email>] [phonenumber <number>] [bindip <ip>] [bindmac <mac>] [bindhost <hostname>] starttime <y-m-d-h> endtime <y-m-d-h> share { on | off } [note <string>]

**参数说明：**
user sslvpn 命令行部分，宏观用户类相关命令
set 设置修改类基本操作
twoauthuser 双因素用户相关操作
thirdpart 显示对象，带有第三方口令因素的双因素用户相关操作
uid 该部门 id，6-15 位数字
pid 口令因素 id，6-15 位数字
cid 证书因素 id，数字字母组合
email 电子邮件，标准邮件格式
phonenumber 手机号码
bindip 绑定 ip，如 192.168.0.1
bindmac 绑定 MAC，可用字符：A—F 大小写英文字母，数字，减号，冒号；格式：XX-XX-XX-XX-XX-XX，或 XX:XX:XX:XX:XX:XX
bindhost 绑定主机，可用字符：任意可打印字符，不包括斜线、反斜线、冒号、星号、问号、双引号、大于号、小于号、 管道符、制表符
starttime 启用时间，格式如：2011-5-17-8 或 2011/5/17/8
endtime 到期时间，格式如：2011-5-17-8 或 2011/5/17/8
share 帐号共享开关，on：开启，off：关闭，默认关闭
note 描述，以\"括起来

**注意事项：**
无

**示例:**
sag user set thirdpassword uid 1234567890123 pid 1234567890124 cid 1234567890125 starttime 2011-10-11-12 endtime 2011-11-9-12 share on note \"notetext\"

# 12.4 角色管理类相关命令及配置:

## 12.4.1 显示现有角色信息:

**语法:**

sag role show role

**参数说明:**

| | |
|---|---|
| role | sslvpn 命令行部分，宏观角色类相关命令 |
| show | 显示类基本操作 |
| role | 操作对象，显示角色信息 |

**注意事项:**

无

**示例:**

sag role show role

## 12.4.2 批量删除选中项:

**语法:**

sag role del role more rids <value\;value...>

**参数说明:**

| | |
|---|---|
| role | sslvpn 命令行部分，宏观角色类相关命令 |
| del | 删除类基本操作 |
| role | 操作对象，角色相关操作 |
| more | 批量删除标志 |
| rids | 角色 id，6-15 位数字，多个角色 id 间使用'\;'分隔 |

**注意事项:**

角色里若包含有成员，则不可删除

**示例:**

sag role del role more rids 1234567890123\;1234567890124

### 12.4.3 删除单个角色:

**语法:**
sag role del role rid <value>

**参数说明:**

| | |
|---|---|
| role | sslvpn 命令行部分，宏观角色类相关命令 |
| del | 删除类基本操作 |
| role | 操作对象，删除角色 |
| rid | 角色 id，6-15 位数字 |

**注意事项:**
无

**示例:**
sag role del role rid 1234567890123

### 12.4.4 修改角色:

**语法:**
sag role set role rid <value> name <name> [note <string>]

**参数说明:**

| | |
|---|---|
| role | sslvpn 命令行部分，宏观角色类相关命令 |
| set | 设置类基本操作 |
| role | 操作对象，修改角色信息 |
| rid | 角色 id，6-15 位数字 |
| name | 角色名字，1-15 位中文、字母、数字、减号、下划线组合 |
| note | 角色补充注释，以\"括起来 |

**注意事项:**
无

**示例:**
sag role set role rid 1234567890123 name nametext note \"notetext\"

### 12.4.5 角色授权服务显示

**语法：**

sag role show service rid <value>

**参数说明：**

| | |
|---|---|
| role | sslvpn 命令行部分，宏观角色类相关命令 |
| show | 显示类基本操作 |
| service | 显示对象，服务授权操作 |
| rid | 角色 id，6-15 位数字 |

**注意事项：**

无

**示例:**

sag role show service rid 1234567890123

## 12.4.6 角色授权服务

**语法：**

sag role add service mids <value\;value...> rid <value>

**参数说明：**

| | |
|---|---|
| role | sslvpn 命令行部分，宏观角色类相关命令 |
| add | 添加类基本操作 |
| service | 操作对象，服务授权操作 |
| mids | 服务 id,可为多个服务 id 值，中间使用 '\;' 分隔 |
| rid | 角色 id，6-15 位数字 |

**注意事项：**

无

**示例:**

sag role add service mids 1234567890124\;123567890125 rid 1234567890123

## 12.4.7 角色策略显示:

**语法：**

sag role show policytorole rid <value>

**参数说明：**

role sslvpn 命令行部分，宏观角色类相关命令
show 显示类基本操作
policytorole 操作对象，策略管理相关操作
rid 角色 id，6-15 位数字

**注意事项：**
无

**示例：**
sag role show policytorole rid 1234567890123

## 12.4.8 角色策略添加：

**语法：**
sag role add policytorole rid <value> poids <value\;value...>

**参数说明：**
role sslvpn 命令行部分，宏观角色类相关命令
add 添加类基本操作
policytorole 操作对象，策略管理相关操作
rid 角色 id，6-15 位数字
poids 策略 id，6-15 位数字，可为多个，中间使用'\;'分隔

**注意事项：**
无

**示例：**
sag role add policytorole rid 1234567890123 poids 1234567890123\;1234567890124

## 12.4.9 增加角色：

**语法：**
sag role add role name <name> [note <string>]
**参数说明：**
role sslvpn 命令行部分，宏观角色类相关命令
add 添加类基本操作
role 操作对象，角色相关
name 角色名字，1-15 位中文、字母、数字、减号、下划线组合
note 角色补充注释，以'\"'括起来

**注意事项：**

无

**示例:**
sag role add role  name rolename  note  \”notettext\”

## 12.4.10 客户端安全策略显示:

**语法：**以'\”"括起来
sag role show policy

**参数说明：**

| | |
|---|---|
| role | sslvpn 命令行部分，宏观角色类相关命令 |
| show | 显示类基本操作 |
| policy | 操作对象，策略管理相关操作 |

**注意事项：**
无

**示例:**
sag role show policy

## 12.4.11 客户端安全策略具体策略内容显示:

**语法：**
sag role show policy id <value>

**参数说明：**

| | |
|---|---|
| role | sslvpn 命令行部分，宏观角色类相关命令 |
| show | 显示类基本操作 |
| policy | 操作对象，策略管理相关操作 |
| id | 客户端策略 id，6-15 位数字 |

**注意事项：**
无

**示例:**
sag role show policy id  1234567890123

## 12.4.12 修改客户端安全策略:

**语法:**

sag role set policy id <value> name <name> [note <string>] clear { on | off } limit { no | in | all } ［os <string\;string...>］ [broswer <string\ string...>] [desktop <string\;string...>] [ except <string\;string...>] access { on | off }

**参数说明:**

| | |
|---|---|
| role | sslvpn 命令行部分，宏观角色类相关命令 |
| set | 修改配置类基本操作 |
| policy | 操作对象，策略管理相关操作 |
| id | 客户端策略 id，6-15 位数字 |
| name | 安全策略名，1-15 位中文、字母、数字、减号、下划线组合 |
| note | 注释，以'\"'括起来 |
| clear | 清除网上记录，on：开启，off：关闭，默认为关闭 |
| limit | 访问受限，no：无限制，in：登录网关后禁止其他访问（内网不禁止），all：登录网关后禁止其他访问，默认为“无限制” |
| os | 操作系统检查，具体添加方式为预配置可选择，不需直接输入。可以为多个参数，之间用‘\;’分隔 |
| broswer | 浏览器检查，可以为多个参数，之间用‘\;’分隔 |
| desktop | 桌面安全检查，可以为多个参数，之间用‘\;’分隔 |
| except | 当“访问受限”选择为非“无受限”时，需配置例外，例外:<br>当 limit 选为 in 和 all 时，启用。可以为多个参数，之间用‘\;’分隔 |
| access | LeadSec 网御内网安全管理系统准入,是否准入开关，on：开启，off：关闭，默认为关闭 |

**注意事项:**

无

**示例:**

sag role set policy id 1234567890123 name plicyname clear off limit in os “windows xp,SP3”\;\”mac os\” broswer \”IE\”\;\”firefox\” desktop \”desktop1\”\;\”desktop\” except \”abc\”\;\”cba\” access off

## 12.4.13 增加客户端安全策略:

**语法:**

sag role add policy name <name> [note <string>] clear { on | off } limit { no | in | all } ［os <string \;string...>］ [broswer <string \;string...>] [desktop <string\;string...>]

[ except <string\;string...>] access { on | off }

**参数说明：**

| | |
|---|---|
| role | sslvpn 命令行部分，宏观角色类相关命令 |
| add | 添加类基本操作 |
| policy | 操作对象，策略管理相关操作 |
| name | 安全策略名，1-15 位中文、字母、数字、减号、下划线组合 |
| note | 注释，以'\"'括起来 |
| clear | 清除网上记录，on：开启，off：关闭，默认为关闭 |
| limit | 访问受限，no：无限制，in：登录网关后禁止其他访问（内网不禁止），all：登录网关后禁止其他访问，默认为“无限制” |
| os | 操作系统检查，具体添加方式为预配置可选择，不需直接输入。可以为多个参数，之间用‘\;’分隔 |
| broswer | 浏览器检查。可以为多个参数，之间用‘\;’分隔 |
| desktop | 桌面安全检查。可以为多个参数，之间用‘\;’分隔 |
| except | 当“访问受限”选择为非“无受限”时，需配置例外,例外:当 limit 选为，in 和 all 时，启用。可以为多个参数，之间用‘\;’分隔 |
| access | LeadSec 网御内网安全管理系统准入,是否准入开关，on：开启，off：关闭，默认为关闭 |

**注意事项：**

无

**示例:**

sag role add policy name plicyname clear off limit in os “windows xp,SP3”\;\”mac os\” broswer \”IE\”\;\”firefox\” desktop \”desktop1\”\;\”desktop\” except \”abc\”\;\”cba\” access off

## 12.4.14 删除客户端安全策略:

**语法：**

sag role del policy id <value>

**参数说明：**

| | |
|---|---|
| role | sslvpn 命令行部分，宏观角色类相关命令 |
| del | 删除类基本操作 |
| policy | 操作对象，客户端策略相关 |
| id | 策略 id，6-15 位数字 |

**注意事项：**

无

**示例:**

sag role del policy id 1234567890123

## 12.4.15 内网网段位置策略显示:

**语法：**

sag role show intranet

**参数说明：**

role sslvpn 命令行部分，宏观角色类相关命令
show 显示类基本操作
intranet 操作对象，内网位置策略相关操作

**注意事项：**

无

**示例:**

sag role show intranet

## 12.4.16 内网网段位置策略修改:

**语法：**

sag role add intranet innet <ip\;ip...> [outnet <ip\;ip...>]

**参数说明：**

role sslvpn 命令行部分，宏观角色类相关命令
add 显示类基本操作
intranet 操作对象，内网位置策略相关操作
innet 内网网段设置，该项为必填项，界面需加说明，带有默认值
可为多个，中间使用'\;'分隔，单个格式固定：1.0.0.1/24 即，
x.x.x.x/xx
outnet 例外地址设置，可为多个，中间使用'\;'分隔，单个格式固定：1.0.0.1/24 即，
x.x.x.x/xx

**注意事项：**

无

**示例:**

sag role add intranet innet 1.0.0.1/24\;1.0.1.1/24 outnet 1.0.2.1/24\;1.0.3.1/24

## 12.4.17 角色用户信息显示:

**语法:**

sag role show user rid <value>

**参数说明:**

| | |
|---|---|
| role | sslvpn 命令行部分，宏观角色类相关命令 |
| show | 显示类基本操作 |
| user | 操作对象，显示角色用户 |
| rid | 角色 id，6-15 位数字 |

**注意事项:**

无

**示例:**

sag role show user rid 1234567890123

## 12.4.18 批量删除角色内用户:

**语法:**

sag role del roleuser rid <value> ids <value\;value...>

**参数说明:**

| | |
|---|---|
| role | sslvpn 命令行部分，宏观角色类相关命令 |
| del | 删除类基本操作 |
| roleuser | 操作对象，操作角色用户 |
| rid | 角色 id，6-15 位数字 |
| ids | 选中的用户 id，可为多个，中间使用'\;'分隔 |

**注意事项:**

无

**示例:**

sag role del roleuser rid 1234567890123 ids 1234567890123\;1234567890123

## 12.4.19 移动用户更换角色界面显示:

**语法:**

sag role show usertorole

**参数说明:**

| | |
|---|---|
| role | sslvpn 命令行部分，宏观角色类相关命令 |
| show | 显示类基本操作 |
| usertorole | 操作对象，更改用户角色隶属相关 |

**注意事项:**

无

**示例:**

sag role show usertorole

## 12.4.20 移动用户更换角色:

**语法:**

sag role mov usertorole id <value> srid <value> drid <value>

**参数说明:**

| | |
|---|---|
| role | sslvpn 命令行部分，宏观角色类相关命令 |
| mov | 移动类基本操作 |
| usertorole | 操作对象，更改用户角色隶属相关 |
| id | 角色内用户 id，6-15 位数字 |
| srid | 源隶属的角色 id，6-15 位数字 |
| drid | 目的隶属的角色 id，6-15 位数字 |

**注意事项:**

无

**示例:**

sag role mov usertorole id 1234567890123 srid 1234567890124 drid 12345678901235

## 12.4.21 复制用户更换角色显示:

**语法:**

sag role show usertorole

**参数说明：**

| | |
|---|---|
| role | sslvpn 命令行部分，宏观角色类相关命令 |
| show | 显示类基本操作 |
| usertorole | 操作对象，更改用户角色隶属相关 |

**注意事项：**

无

**示例:**

sag role show usertorole

## 12.4.22 复制用户更换角色:

**语法：**

sag role copy usertorole id <value> srid <value> drid <value>

**参数说明：**

| | |
|---|---|
| **role** | sslvpn 命令行部分，宏观角色类相关命令 |
| copy | 复制类基本操作 |
| usertorole | 操作对象，更改用户角色隶属相关 |
| id | 角色内用户 id，6-15 位数字 |
| srid | 源隶属的角色 id，6-15 位数字 |
| drid | 目的隶属的角色 id，6-15 位数字 |

**注意事项：**

无

**示例:**

sag role copy usertorole id 1234567890123 srid 1234567890124 drid 12345678901235

## 12.4.23 位置策略显示:

**语法：**

sag role show userposition rid <value> id <value>

**参数说明：**

| | |
|---|---|
| role | sslvpn 命令行部分，宏观角色类相关命令 |
| show | 显示类基本操作 |
| userposition | 操作对象，用户位置策略相关 |
| rid | 隶属的角色 id，6-15 位数字 |

id 用户 id，6-15 位数字

**注意事项：**
无

**示例:**
sag role show userposition rid 123456789 id 987654321

## 12.4.24 修改位置策略:

**语法：**
sag role set userposition rid <value> id <value> pospolicy { no | in | out }

**参数说明：**

| | |
|---|---|
| role | sslvpn 命令行部分，宏观角色类相关命令 |
| set | 设置修改类基本操作 |
| userposition | 操作对象，用户位置策略相关 |
| rid | 隶属的角色 id，6-15 位数字 |
| id | 用户 id，6-15 位数字 |
| pospolicy | 位置策略，no：没有限制，in：内网，out-外网，默认为没有限制 |

**注意事项：**
无

**示例:**
sag role set userposition rid 1234567890123 id 1234567890124 pospolicy no

## 12.4.25 删除角色内用户:

**语法：**
sag role del user rid <value> id <value>

**参数说明：**

| | |
|---|---|
| role | sslvpn 命令行部分，宏观角色类相关命令 |
| del | 删除类基本操作 |
| user | 操作对象，用户相关操作 |
| rid | 用户所属角色 id，6-15 位数字 |
| id | 用户 id，6-15 位数字 |

**注意事项：**
无

**示例:**
sag role del user rid 1234567890123 id 1234567890124

## 12.4.26 添加名字过滤:

**语法:**
sag role add filter rid <value> type { cert | ldap | radius | ad } content <string>

**参数说明:**
role sslvpn 命令行部分，宏观角色类相关命令
add 添加类基本操作
filter 操作对象，过滤相关操作
rid 用户所属角色 id，6-15 位数字
type 名字过滤类型，cert：证书用户，ldap：LDAP 用户，radius：RADIUS 用户，ad：AD 用户
content 过滤内容，以\"括起来

**注意事项:**
无

**示例:**
sag role add filter rid <string> type ldap content \"OU=Unit1\"

## 12.4.27 添加名字修改:

**语法:**
sag role set filter rid <value> type { cert | ldap | radius | ad } content <string>

**参数说明:**
role sslvpn 命令行部分，宏观角色类相关命令
set 修改配置类基本操作
filter 操作对象，过滤相关操作
rid 用户所属角色 id
type 名字过滤类型，cert：证书用户，ldap：LDAP 用户，radius：RADIUS 用户，ad：AD 用户
content 过滤内容，以\"括起来

**注意事项:**
无

**示例:**

sag role set filter rid <string> type ldap content \"OU=Unit1\"

## 12.4.28 增加双因素用户显示:

**语法:**

sag role show departoftwoauth

**参数说明:**

| | |
|---|---|
| role | sslvpn 命令行部分，宏观角色类相关命令 |
| show | 显示类基本操作 |
| departoftwoauth | 操作对象，双因素用户相关 |

**注意事项:**

无

**示例:**

sag role show departoftwoauth

## 12.4.29 部门内双因素用户显示:

**语法:**

sag role show useroftwoauth uid <value>

**参数说明:**

| | |
|---|---|
| role | sslvpn 命令行部分，宏观角色类相关命令 |
| show | 显示类基本操作 |
| useroftwoauth | 操作对象，双因素用户相关 |
| uid | 要操作的部门 id，6-15 位数字 |

**注意事项:**

无

**示例:**

sag role show useroftwoauth uid 1234567890123

## 12.4.30 增加单个双因素用户到角色:

**语法:**

sag role add twoauthusertorole rid <value> uid <value> pid <value> cid <value>

**参数说明:**

| | |
|---|---|
| role | sslvpn 命令行部分，宏观角色类相关命令 |
| add | 添加类基本操作 |
| twoauthusertorole | 添加双因素用户到角色 |
| rid | 角色 id，6-15 位数字 |
| uid | 部门 id，6-15 位数字 |
| pid | 双因素用户口令因素 id，6-15 位数字 |
| cid | 双因素用户证书因素 id，数字字符组合 |

**注意事项:**

无

**示例:**

sag role add twoauthusertorole rid 1234567890124 uid 1234567890123 pid 1234567890125 cid 1234567890126

## 12.4.31 批量增加双因素用户:

**语法:**

sag role add twoauthusertoroles rid <value> uid <value> pids < value\;value ...> cids < value\;value ...>

**参数说明:**

| | |
|---|---|
| role | sslvpn 命令行部分，宏观角色类相关命令 |
| add | 添加类基本操作 |
| twoauthusertoroles | 添加多个双因素用户到角色 |
| rid | 角色 id，6-15 位数字 |
| uid | 部门 id，6-15 位数字 |
| pids | 双因素用户口令因素 id，6-15 位数字，可为多个，中间使用'\;'分隔 |
| cids | 双因素用户证书因素 id，6-15 位数字，可为多个，中间使用'\;'分隔 |

**注意事项:**

无

**示例:**

sag role add twoauthusertoroles rid 1234567890124 uid 1234567890123 pids 1234567890125 cids 1234567890126

## 12.4.32 增加证书用户显示:

**语法：**

sag role show departofcert

**参数说明：**

| | |
|---|---|
| role | sslvpn 命令行部分，宏观角色类相关命令 |
| show | 显示类基本操作 |
| departofcert | 操作对象，证书用户相关 |

**注意事项：**

无

**示例:**

sag role show departofcert

## 12.4.33 部门内证书用户显示:

**语法：**

sag role show userofcert uid <value>

**参数说明：**

| | |
|---|---|
| role | sslvpn 命令行部分，宏观角色类相关命令 |
| show | 显示类基本操作 |
| userofcert | 操作对象，双因素用户相关 |
| uid | 要操作的部门 id，6-15 位数字 |

**注意事项：**

无

**示例:**

sag role show userofcert uid 1234567890123

## 12.4.34 增加单个证书用户到角色:

**语法:**

sag role add certusertorole local rid <value> uid <value> cid <value>

**参数说明:**

| | |
|---|---|
| role | sslvpn 命令行部分，宏观角色类相关命令 |
| add | 添加类基本操作 |
| certusertorole | 添加证书用户到角色 |
| local | 本地证书用户 |
| rid | 角色 id，6-15 位数字 |
| uid | 部门 id，6-15 位数字 |
| cid | 证书用户 id，6-15 位数字 |

**注意事项:**

无

**示例:**

sag role add certusertorole local rid 1234567890124 uid 1234567890123 cid 1234567890126

## 12.4.35 批量增加证书用户到角色:

**语法:**

sag role add certusertoroles local rid <value> uid <value> cids < value;value ...>

**参数说明:**

| | |
|---|---|
| role | sslvpn 命令行部分，宏观角色类相关命令 |
| add | 添加类基本操作 |
| certusertoroles | 添加多个证书用户到角色 |
| local | 本地证书用户 |
| rid | 角色 id，6-15 位数字 |
| uid | 部门 id，6-15 位数字 |
| cids | 证书用户 id，6-15 位数字，可为多个，中间使用'\;'分隔 |

**注意事项:**

无

**示例:**

sag role add certusertoroles rid 1234567890124 uid 1234567890123 cids 1234567890126

## 12.4.36 角色内增加口令用户显示:

**语法:**

sag role show departofuser

**参数说明:**

| | |
|---|---|
| role | sslvpn 命令行部分，宏观角色类相关命令 |
| show | 显示类基本操作 |
| departofuser | 操作对象，口令用户相关 |

**注意事项:**

无

**示例:**

sag role show departofuser

## 12.4.37 部门内口令用户显示:

**语法:**

sag role show userofpassword uid <value>

**参数说明:**

| | |
|---|---|
| role | sslvpn 命令行部分，宏观角色类相关命令 |
| show | 显示类基本操作 |
| userofpassword | 操作对象，口令用户相关 |
| uid | 要操作的部门 id，6-15 位数字 |

**注意事项:**

无

**示例:**

sag role show userofpassword uid 1234567890123 '

## 12.4.38 增加单个口令用户到角色:

**语法:**

sag role add passwordusertorole local rid <value> uid <value> pid <value>

**参数说明：**

| | |
|---|---|
| role | sslvpn 命令行部分，宏观角色类相关命令 |
| add | 添加类基本操作 |
| passwordusertorole | 添加口令用户到角色 |
| local | 本地口令用户 |
| rid | 角色 id，6-15 位数字 |
| uid | 部门 id，6-15 位数字 |
| pid | 口令用户 id，6-15 位数字 |

**注意事项：**

无

**示例:**

sag role add certusertorole local rid 1234567890124 uid 1234567890123 pid 1234567890126

## 12.4.39 批量增加口令用户到角色:

**语法：**

sag role add passwordusertoroles local rid <value> uid <value> pids <value;value ..>

**参数说明：**

| | |
|---|---|
| role | sslvpn 命令行部分，宏观角色类相关命令 |
| add | 添加类基本操作 |
| passwordusertoroles | 添加多个口令用户到角色 |
| local | 本地口令用户 |
| rid | 角色 id，6-15 位数字 |
| uid | 部门 id，6-15 位数字 |
| pids | 口令用户 id，6-15 位数字，可为多个，中间使用'\;'分隔 |

**注意事项：**

无

**示例:**

sag role add passwordusertoroles rid 1234567890124 uid 1234567890123 pids 1234567890126

## 12.4.40 文件增加:

**语法：**

sag role add certusertorole by file rid <value> name <name>

**参数说明：**

| | |
|---|---|
| role | sslvpn 命令行部分，宏观角色类相关命令 |
| add | 添加类基本操作 |
| certusertorole | 操作对象，证书用户相关 |
| by | 增加方式 |
| file | 增加方式，通过文件增加 |
| rid | 角色 id，6-15 位数字 |
| name | 文件名，用于后台解析该文件使用，1-15 位中文、字母、数字、减号、下划线组合 |

**注意事项：**

无

**示例:**

sag role add certusertorole by file rid 1234567890123 name TESTCERT

## 12.4.41 通过 LDAP 增加证书

**语法：**

sag role add certusertorole by ldap rid <value> name <name>

**参数说明：**

| | |
|---|---|
| role | sslvpn 命令行部分，宏观角色类相关命令 |
| add | 添加类基本操作 |
| certusertorole | 操作对象，证书用户相关 |
| by | 增加方式 |
| ldap | 通过 LDAP 增加 |
| rid | 角色 id，6-15 位数字 |
| name | 文件名，用于后台解析该文件使用 |

**注意事项：**

无

**示例:**

sag role add certusertorole by ldap rid 1234567890123 name TESTCERT

## 12.4.42 通过 LDAP 批量增加证书:

**语法：**

sag role add certusertorole by ldap  more rid <value> names <name\;name..>

**参数说明：**

| | |
|---|---|
| role | sslvpn 命令行部分，宏观角色类相关命令 |
| add | 添加类基本操作 |
| certusertorole | 操作对象，证书用户相关 |
| by | 增加方式 |
| ldap | 通过 LDAP 增加 |
| more | 批量增加标志 |
| rid | 角色 id，6-15 位数字 |
| names | 文件名，显示的 DN 值等等，可为多个，使用'\;'分隔 |

**注意事项：**

首先，判断是否 LDAP 连接正常

**示例:**

sag role add certusertorole by ldap  more rid 1234567890123 names name1\;name2

## 12.4.43 通过 ad 增加证书:

**语法：**

sag role add certusertorole by ad rid <value> name <name>

**参数说明：**

| | |
|---|---|
| role | sslvpn 命令行部分，宏观角色类相关命令 |
| add | 添加类基本操作 |
| certusertorole | 操作对象，证书用户相关 |
| by | 增加方式 |
| ad | 增加方式，通过 AD 增加 |
| rid | 角色 id，6-15 位数字 |
| name | 文件名，用于后台解析该文件使用，1-15 位中文、字母、数字、减号、下划线组合 |

**注意事项：**

无

**示例:**

sag role add certusertorole by ad rid 1234567890123 name TESTCERT

## 12.4.44 通过 ad 批量增加证书

**语法：**

sag role add certusertorole by ad more rid <value> names <name\;name..>

**参数说明：**

| | |
|---|---|
| role | sslvpn 命令行部分，宏观角色类相关命令 |
| add | 添加类基本操作 |
| certusertorole | 操作对象，证书用户相关 |
| by | 增加方式 |
| ad | 增加方式，通过 AD 增加 |
| more | 批量增加标志 |
| rid | 角色 id，6-15 位数字 |
| names | 文件名，显示的 DN 值等等，可为多个，使用'\;'分隔 |

**注意事项：**

注意：首先，判断是否 AD 连接正常

**示例:**

sag role add certusertorole by ad more rid 1234567890123 names name1\;name2

## 12.4.45 通过 LDAP 增加口令用户

**语法：**

sag role add passwordusertorole by ldap rid <value> name <name>

**参数说明：**

| | |
|---|---|
| role | sslvpn 命令行部分，宏观角色类相关命令 |
| add | 添加类基本操作 |
| passwordusertorole | 操作对象，口令用户相关 |
| by | 增加方式 |
| ldap | 通过 LDAP 增加 |
| rid | 角色 id，6-15 位数字 |
| name | 文件名，用于后台解析该文件使用 |

**注意事项：**

无

**示例:**

sag role add passwordusertorole by ldap rid 1234567890123 name TESTCERT

## 12.4.46 通过 LDAP 批量增加口令用户

**语法：**

sag role add passwordusertorole by ldap more rid <value> names <name\;name..>

**参数说明：**

| | |
|---|---|
| role | sslvpn 命令行部分，宏观角色类相关命令 |
| add | 添加类基本操作 |
| passwordusertorole | 操作对象，口令用户相关 |
| by | 增加方式 |
| ldap | 通过 LDAP 增加 |
| more | 批量增加标志 |
| rid | 角色 id，6-15 位数字 |
| names | 文件名，显示的 DN 值等等，可为多个，使用'\;'分隔 |

**注意事项：**

注意：首先，判断是否 LDAP 连接正常

**示例:**

sag role add passwordusertorole by ldap more rid 1234567890123 names name1\;name2

## 12.4.47 增加 radius 口令用户:

**语法：**

sag role add passwordusertorole by radius rid <value> name <name> share { on | off } ［note <string>］

**参数说明：**

| | |
|---|---|
| role | sslvpn 命令行部分，宏观角色类相关命令 |
| add | 添加类基本操作 |
| passwordusertorole | 操作对象，口令用户相关 |
| by | 增加方式 |
| radius | 通过 radius 增加 |
| rid | 角色 id，6-15 位数字 |
| name | 文件名，radius 服务器存储的文件名（必须存在，否则添加失败） |
| share | 帐号共享，on：开启，off：关闭，默认关闭 |
| note | 用户描述，以'\"'括起来 |

**注意事项：**

无

**示例:**

sag role add passwordusertorole by radius rid 1234567890123 name TESTRADIUS share

off note \"notetext\"

## 12.4.48 增加 AD 增加口令用户:

**语法:**

sag role add passwordusertorole by ad rid <value> name <name>

**参数说明:**

| | |
|---|---|
| role | sslvpn 命令行部分，宏观角色类相关命令 |
| add | 添加类基本操作 |
| passwordusertorole | 操作对象，口令用户相关 |
| by | 增加方式 |
| ad | 通过 AD 增加 |
| rid | 角色 id，6-15 位数字 |
| name | 用户名，用于后台解析该文件使用，1-15 位中文、字母、数字、减号、下划线组合 |

**注意事项:**

无

**示例:**

sag role add passwordusertorole by ad rid 1234567890123 name TESTPASSWORD

## 12.4.49 增加 AD 批量增加口令用户:

**语法:**

sag role add passwordusertorole by ad more rid <value> names <name;name..>

**参数说明:**

| | |
|---|---|
| role | sslvpn 命令行部分，宏观角色类相关命令 |
| add | 添加类基本操作 |
| passwordusertorole | 操作对象，口令用户相关 |
| by | 增加方式 |
| ad | 通过 AD 增加 |
| more | 批量增加标志 |
| rid | 角色 id，6-15 位数字 |
| names | 用户名，显示的 DN 值等等，可为多个，使用'\;'分隔 |

**注意事项:**

首先，判断是否 AD 连接正常

**示例:**

sag role add passwordusertorole by ad more rid 1234567890123 names name1\;name2

## 12.4.50 修改角色内通过第三方方式添加的用户:

**语法：**

sag role set thirduser id <value> accountpend { on | off } share { on | off } vip { on | off } [bindip <ip>] [bindmac <mac>] [bindhost <hostname>] [bindvip <ip>]

**参数说明：**

| | |
|---|---|
| role | sslvpn 命令行部分，宏观角色类相关命令 |
| set | 设置修改类基本操作 |
| thirduser | 操作对象，第三方用户相关 |
| id | 用户 id，6-15 位数字 |
| accountpend | 帐号挂起开关，on：挂起，off：不挂起，默认不挂起 |
| share | 帐号共享开关，on：开启，off：关闭，默认关闭 |
| vip | VIP 用户开关，on：开启，off：关闭，默认关闭 |
| bindip | 绑定 ip，格式如 192.168.0.1 |
| bindmac | 绑定 MAC，可用字符：A—F 大小写英文字母，数字，减号，冒号；格式：XX-XX-XX-XX-XX-XX，或 XX:XX:XX:XX:XX:XX |
| bindhost | 绑定主机，可用字符：任意可打印字符，不包括斜线、反斜线、冒号、星号、问号、双引号、大于号、小于号、 管道符、制表符 |
| bindvip | 绑定主机 ip，格式如 192.168.0.1 |

**注意事项：**

无

**示例:**

sag role set thirduser id 12345467890123 accountpend off share off vip off

## 12.4.51 修改第三方方式添加用户的有效期:

**语法：**

sag role set thirduser id <value> policy { a | n | s starttime <y-m-d-h> endtime <y-m-d-h>}

**参数说明：**

| | |
|---|---|
| role | sslvpn 命令行部分，宏观角色类相关命令 |
| set | 设置修改类基本操作 |
| thirduser | 操作对象，第三方用户相关 |
| id | 用户 id，6-15 位数字 |

| | |
|---|---|
| policy | 有效期策略，a：一直生效，n：一直失效，s：详细控制，默认一直生效 |
| starttime | 启用时间，格式如：2011-5-17-8 或 2011/5/17/8 |
| endtime | 到期时间，格式如：2011-5-17-8 或 2011/5/17/8 |

**注意事项：**
无

**示例:**
sag role set thirduser 12345467890123 policy a

# 12.5 对等网关相关命令及配置:

## 12.5.1 对等网关显示:

**语法：**
sag peer show peer

**参数说明：**

| | |
|---|---|
| peer | sslvpn 命令行部分，宏观对等网关类相关命令 |
| show | 显示类基本操作 |
| peer | 操作对象，对等网关相关 |

**注意事项：**
无

**示例:**
sag peer show peer

## 12.5.2 修改对等网关显示:

**语法：**
sag peer show singlepeer id <value>

**参数说明：**

| | |
|---|---|
| peer | sslvpn 命令行部分，宏观对等网关类相关命令 |
| show | 显示类基本操作 |
| singlepeer | 操作对象，对等网关相关 |
| id | 对等网关 id，6-15 位数字 |

**注意事项：**

无

**示例:**

sag peer show singlepeer id 1318447028175

## 12.5.3 修改对等网关信息 :

**语法:**

sag peer set peer id <value> name <name> address <ip> port <port> subnet <ip> authtype { p {username <name> password <password>} | c } [note <string>]

**参数说明:**

| | |
|---|---|
| peer | sslvpn 命令行部分，宏观对等网关类相关命令 |
| set | 修改配置类基本操作 |
| peer | 操作对象，对等网关相关 |
| id | 对等网关 id，6-15 位数字 |
| name | 网关名字，1-15 位中文、字母、数字、减号、下划线组合 |
| address | 网关地址，格式：x.x.x.x |
| port | 网关端口，默认 443 |
| subnet | 对等网段，格式：x.x.x.x/xx |
| authtype | 认证方式，p：口令用户，c：证书用户，默认为口令用户 |
| username | 登录帐号，可用字符：大、小写英文字母，数字，减号，下划线，小数点,长度为 20。第一个字符必须是大、小写英文字母或数字 |
| password | 登录密钥，除制表符和问号、空格外的任意可打印字符，至少长度为 6，最大长度为 15 |
| note | 注释，以\"括起来 |

**注意事项:**

无

**示例:**

sag peer set peer id 1318447028175 name test address 1.0.0.1 port 443 subnet 1.0.1.1/24 authtype p username testname password 154348745 note \"notetext\"

## 12.5.4 删除单条网关信息:

**语法:**

sag peer del peer single id <value>

**参数说明：**

| | |
|---|---|
| peer | sslvpn 命令行部分，宏观对等网关类相关命令 |
| del | 删除类基本操作 |
| peer | 操作对象，对等网关相关 |
| single | 单条处理 |
| id | 对等网关 id，6-15 位数字 |

**注意事项：**

无

**示例:**

sag peer del peer single id 123467497967

## 12.5.5 连通性测试:

**语法：**

sag peer test peer id <value>

**参数说明：**

| | |
|---|---|
| peer | sslvpn 命令行部分，宏观对等网关类相关命令 |
| test | 测试类基本操作 |
| peer | 操作对象，对等网关相关 |
| id | 对等网关 id，6-15 位数字 |

**注意事项：**

无

**示例:**

sag peer test peer id 1318447028175

## 12.5.6 删除多条网关信息 ：

**语法：**

sag peer del peer more ids <value\;value...>

**参数说明：**

| | |
|---|---|
| peer | sslvpn 命令行部分，宏观对等网关类相关命令 |
| del | 删除类基本操作 |
| peer | 操作对象，对等网关相关 |
| more | 多条处理 |
| ids | 对等网关 id,可为多条，中间使用'\;'分隔 |

**注意事项：**
无

**示例:**
sag peer del peer more ids 1318447028175\;1318446938139

## 12.5.7 添加对等网关:

**语法：**
sag peer add peer name <name> address <ip> port <port> subnet <ip> authtype { p {username <name> password <password>} | c } [note <string>]

**参数说明：**

| | |
|---|---|
| peer | sslvpn 命令行部分，宏观对等网关类相关命令 |
| add | 添加类基本操作 |
| peer | 操作对象，对等网关相关 |
| name | 网关名字，可为中文 |
| address | 网关地址，格式：x.x.x.x |
| port | 网关端口，默认 443 |
| subnet | 对等网段，格式：x.x.x.x/xx |
| authtype | 认证方式，p：口令用户，c：证书用户，默认为口令用户 |
| username | 登录帐号，可用字符：大、小写英文字母，数字，减号，下划线，小数点,长度为 20。第一个字符必须是大、小写英文字母或数字 |
| password | 登录密钥，除制表符和问号、空格外的任意可打印字符，至少长度为 6，最大长度为 15 |
| note | 注释，以‘\”’括起来 |

**注意事项：**
无

**示例:**
sag peer set peer name test address 1.0.0.1 port 443 subnet 1.0.1.1/24 authtype p username test password test123 note \”TEST\”

## 12.5.8 对等网关状态测试:

**语法：**
sag peer show status

**参数说明：**

peer sslvpn 命令行部分，宏观对等网关类相关命令
show 显示类基本操作
status 操作对象，对等网关状态相关

**注意事项：**
无

**示例:**
sag peer show status

## 12.5.9 可信证书链显示:

**语法：**
sag peer show certchain

**参数说明：**
peer sslvpn 命令行部分，宏观对等网关类相关命令
show 显示类基本操作
certchain 操作对象，对等网关可信证书链相关

**注意事项：**
无

**示例:**
sag peer show certchain

## 12.5.10 删除可信证书链:

**语法：**
sag peer del certchain id <string>

**参数说明：**
peer sslvpn 命令行部分，宏观对等网关类相关命令
del 删除类基本操作
certchain 操作对象，对等网关可信证书链相关
id 证书 id，在此应为证书指纹或名称，以'\"'括起来

**注意事项：**
无

**示例:**
sag peer del certchain id

\”c5:05:40:0D:A3:D6:F1:93:1E:19:ED:2B:52:69:CC:73:82:6A\”

## 12.5.11 增加可信证书链:

**语法：**

sag peer add certchain path <string>

**参数说明：**

| | |
|---|---|
| peer | sslvpn 命令行部分，宏观对等网关类相关命令 |
| add | 添加类基本操作 |
| certchain | 操作对象，对等网关可信证书链相关 |
| path | 证书路径，主要包含名称，便于解析和存储，用'\”'括起来 |

**注意事项：**

无

**示例:**

sag peer add certchain path \”/a/b/c/BJCA.crt\”

## 12.5.12 第三方网关证书显示:

**语法：**

sag peer show thirdcert

**参数说明：**

| | |
|---|---|
| peer | sslvpn 命令行部分，宏观对等网关类相关命令 |
| show | 显示类基本操作 |
| thirdcert | 操作对象，对等网关第三方网关证书相关 |

**注意事项：**

无

**示例:**

sag peer show thirdcert

## 12.5.13 添加第三方网关证书:

**语法：**

sag peer add thirdcert path <string> password <password>

**参数说明：**

| | |
|---|---|
| peer | sslvpn 命令行部分，宏观对等网关类相关命令 |
| add | 添加类基本操作 |
| thirdcert | 操作对象，对等网关第三方网关证书相关 |
| path | 证书路径，主要包含名称，便于解析和存储，用'\"'括起来 |
| password | 文件保护口令，用'\"'括起来 |

**注意事项：**

无

**示例:**

sag peer add thirdcert path /a/b/c/BJCA.crt password 12345678

## 12.5.14 产生证书请求:

**语法：**

sag peer add certcsr country <country> org <string> department <string> ipordns <ip/dns> [province <string>] [town <string>]

**参数说明：**

| | |
|---|---|
| peer | sslvpn 命令行部分，宏观对等网关类相关命令 |
| add | 添加类基本操作 |
| certcsr | 操作对象，证书请求相关 |
| country | 国家，只能是字符或数字，为两个字节。默认 CN |
| org | 组织，默认“LeadSec 网御 SAG”，以'\"'括起来 |
| department | 部门，默认“SSLVPN”，以'\"'括起来 |
| ipordns | 网关地址或者域名，默认当前网关 ip，以'\"'括起来 |
| province | 省或直辖市，以'\"'括起来 |
| town | 县或区，以'\"'括起来 |

**注意事项：**

无

**示例:**

sag peer add certcsr country cn org \“LeadSec 网御 SAG\” department \“SSLVPN\” ipordns \”1.0.0.112\” province \”tianjin\” twon \”jixian\”

## 12.5.15 接收证书应答文件:

**语法：**

sag peer add certrespone path <string>

**参数说明：**

| | |
|---|---|
| peer | sslvpn 命令行部分，宏观对等网关类相关命令 |
| add | 添加类基本操作 |
| certrespone | 操作对象，证书应答文件相关 |
| path | 证书名称路径，以\"括起来 |

**注意事项：**

无

**示例:**

sag peer add certrespone path \"/a/b/c/CERTRESPONE\"

# 12.6 用户属性相关命令及配置:

## 12.6.1 HTTP 缺省登录显示:

**语法：**

sag attribute show defaulthttp

**参数说明：**

| | |
|---|---|
| attribute | sslvpn 命令行部分，宏观用户属性类相关命令 |
| show | 显示类基本操作 |
| defaulthttp | 操作对象，缺省 HTTP 相关 |

**注意事项：**

无

**示例:**

sag attribute show defaulthttp

## 12.6.2 设置 HTTP 缺省登录属性:

**语法：**

sag attribute set defaulthttp default { homepage | anonymous | sms| password | cert } disanonymous { on | off } dispassword { on | off } sms { on | off } cert { on | off } dischain { on | off }

**参数说明：**

| | |
|---|---|
| attribute | sslvpn 命令行部分，宏观用户属性类相关命令 |

set 设置修改类基本操作
defaulthttp 操作对象，缺省 HTTP 相关
default http 缺省登录,homepage：显示首页，anonymous： 跳转到匿名登录，sms：跳转到短信登录，password：跳转到口令登， cert：跳转到证书登录，默认为显示首页
disanonymous 显示匿名登录开关，on：开启；off-关闭，默认开启
dispassword 显示口令登录开关，on：开启；off-关闭，默认开启
sms 显示短信登录开关，on：开启；off-关闭，默认开启
cert 显示证书登录开关，on：开启；off-关闭，默认开启
dischain 显示可信证书链下载（PDA）登录开关，on：开启；off-关闭，默认关闭

**注意事项：**
无

**示例:**
sag attribute set defaulthttp default homepage disanonymous on dispassword on sms on cert on dischain off

## 12.6.3 HTTPS 缺省登录:

**语法：**
sag attribute show defaulthttps

**参数说明：**
attribute sslvpn 命令行部分，宏观用户属性类相关命令
show 显示类基本操作
defaulthttps 操作对象，缺省 HTTPS 相关

**注意事项：**
无

**示例:**
sag attribute show defaulthttps

## 12.6.4 设置 HTTPS 缺省登录属性:

**语法：**
sag attribute set defaulthttps default { password | anonymous | sms }

**参数说明：**
attribute sslvpn 命令行部分，宏观用户属性类相关命令
set 修改配置类基本操作

defaulthttps 操作对象，缺省 HTTPS 相关
default 单向 HTTPS 缺省登录, anonymous： 匿名登录，sms：短信登录，
password：口令登录

**注意事项：**
无

**示例:**
sag attribute set defaulthttps default password

## 12.6.5 文字定制显示:

**语法：**
sag attribute show text

**参数说明：**
attribute sslvpn 命令行部分，宏观用户属性类相关命令(标识)
show 显示类基本操作(标识)
text 操作对象，文字定制相关

**注意事项：**
无

**示例:**
sag attribute show text

## 12.6.6 文字定制设置:

**语法：**
sag attribute set text admintitle <string> usertitle <string> welcome <string> usernotice <string> passwordtitle <string> passwordnotice <string> passwordref <string> smstitle <string> smsnotice <string> smsref <string>

**参数说明：**
attribute sslvpn 命令行部分，宏观用户属性类相关命令
set 设置修改类基本操作
text 操作对象，文字定制相关
admintitle 管理员标题，用'\"'括起来，默认为“管理员登录”
usertitle 用户标题，用'\"'括起来，默认为“用户登录”
welcome 登录前提示，用'\"'括起来，默认为“欢迎登录安全网关!”
usernotice 登录后提示，用'\"'括起来，默认为“欢迎您：【%name%】！您与应用

服务器的通讯已受到 LeadSec 网御 SAG 的保护，请放心使用！”

passwordtitle 口令登录公告栏标题，用'\”'括起来，默认为“公告栏”

passwordnotice 口令登录公告栏内容，用'\”'括起来，默认为“欢迎使用 LeadSec 网御 SSL VPN！<a href='about:blank' target='_blank'>详细</a>”

passwordref 口令登录公告栏 ref，用'\”'括起来，目前不可配置，可传任意字符串，但不起作用，默认不可见

smstitle 短信登录公告栏标题，用'\”'括起来，默认为“公告栏”

smsnotice 短信登录公告栏内容，用'\”'括起来，默认为“欢迎使用 LeadSec 网御 SSL VPN！<a href='about:blank' target='_blank'>详细</a>”

smsref 短信登录公告栏 ref，用'\”'括起来，目前不可配置，可传任意字符串，但不起作用，默认不可见

**注意事项：**

无

**示例:**

sag attribute set text admintitle \”tilename\” usertitle \”usertitiename\” welcome \”hello \” usernotice \”noticetext\” passwordtitle \”titletext\” passwordnotice \”passwordnoticetext\” passwordref \”abc\” smstitle\” smstitletext \” smsnotice \”smstext\” smsref \”abc\”

## 12.6.7 文字定制缺省:

**语法：**

sag attribute show text default

**参数说明：**

attribute sslvpn 命令行部分，宏观用户属性类相关命令

show 显示类基本操作

text 操作对象，定制效果相关

default 显示内容格式

**注意事项：**

无

**示例:**

sag attribute show text default

## 12.6.8 IE 升级界面显示:

**语法：**

sag attribute show ieupdate

**参数说明：**

| | |
|---|---|
| attribute | sslvpn 命令行部分，宏观用户属性类相关命令 |
| show | 显示类基本操作 |
| ieupdate | 操作对象，IE 升级操作相关 |

**注意事项：**

无

**示例:**

sag attribute show ieupdate

## 12.6.9 IE 升级界面设置:

**语法：**

sag attribute set ieupdate link <string>

**参数说明：**

| | |
|---|---|
| attribute | sslvpn 命令行部分，宏观用户属性类相关命令 |
| set | 修改配置类基本操作 |
| ieupdate | 操作对象，IE 升级操作相关 |
| link | 升级链接地址，用'\"'括起来，默认：\"http://www.microsoft.com\" |

**注意事项：**

无

**示例:**

sag attribute set ieupdate link \"http://www.microsoft.com\"

## 12.6.10 图标定制显示:

**语法：**

sag attribute show icon

**参数说明：**

| | |
|---|---|
| attribute | sslvpn 命令行部分，宏观用户属性类相关命令 |
| show | 显示类基本操作 |
| icon | 操作对象，图标定制相关 |

**注意事项：**

无

**示例:**
sag attribute show icon

## 12.6.11 图标定制配置:

**语法:**
sag attribute set icon { on | off }

**参数说明:**
attribute sslvpn 命令行部分，宏观用户属性类相关命令
set 修改配置类基本操作
icon 操作对象，图标定制相关,是否使用图表定制，
on：启用，off：关闭，默认启用

**注意事项:**
无

**示例:**
sag attribute set icon on

## 12.6.12 文件定制显示:

**语法:**

sag attribute show file

**参数说明:**
attribute sslvpn 命令行部分，宏观用户属性类相关命令
show 显示类基本操作
file 操作对象，文件定制相关

**注意事项:**
无

**示例:**
sag attribute show file

## 12.6.13 修改连接显示名称显示:

**语法：**

sag attribute show filelink name <name>

**参数说明：**

| | |
|---|---|
| attribute | sslvpn 命令行部分，宏观用户属性类相关命令 |
| show | 显示类基本操作 |
| filelink | 操作对象，文件定制相关 |
| name | 文件存储名 |

**注意事项：**

无

**示例:**

sag attribute show filelink name index.html

## 12.6.14 修改链接显示名称:

**语法：**

sag attribute set filelink name <name> display <string>

**参数说明：**

| | |
|---|---|
| attribute | sslvpn 命令行部分，宏观用户属性类相关命令 |
| set | 设置类基本操作 |
| filelink | 操作对象，文件定制相关 |
| name | 文件存储名 |
| display | 链接显示名称，用'\"'括起来 |

**注意事项：**

无

**示例:**

sag attribute show filelink name index.html display \"filelink\"

## 12.6.15 页面定制配置删除:

**语法：**

sag attribute del file name <name>

**参数说明：**

| | |
|---|---|
| attribute | sslvpn 命令行部分，宏观用户属性类相关命令 |
| show | 显示类基本操作 |
| file | 操作对象，文件定制相关 |

name 文件存储名

**注意事项：**
无

**示例:**
sag attribute del file name index.html

## 12.6.16 设置为定制页面:

**语法：**
sag attribute set fileportal path <string> type { server | password | smslogin | smssubmit | passwordmodify | first | twoauth }

**参数说明：**
attribute sslvpn 命令行部分，宏观用户属性类相关命令
set 修改配置类基本操作
fileportal 操作对象，文件定制相关
path 文件存储路径，用'\"'括起来
type 目的页面类别，server：服务页面，password：口令登录页面 ，
smslogin： 短信登录页面，smssubmit： 短信提交页面，
passwordmodify：修改口令页面，first： 首次修改口令页面 ，
twoauth：双因素口令登录页面

**注意事项：**
无

**示例:**
sag attribute set fileportal path \"/ssl/bin/index.html\" type server

## 12.6.17 去掉定制页面定制属性:

**语法：**
sag attribute del fileportal index <num>

**参数说明：**
attribute sslvpn 命令行部分，宏观用户属性类相关命令
del 删除类基本操作
fileportal 操作对象，文件定制相关
index 文件存储路径，文件定制类型 0：服务页面，1：口令登录页面，
2：短信登录页面，3：短信提交页面，4：修改口令页面，5：首次修改口令页面，6：双因素口令登录页面

**注意事项：**
无

**示例:**
sag attribute del fileportal index 5

## 12.6.18 帐户安全策略显示:

**语法：**
sag attribute show accountlock

**参数说明：**

| | |
|---|---|
| attribute | sslvpn 命令行部分，宏观用户属性类相关命令 |
| show | 显示类基本操作 |
| accountlock | 操作对象，用户锁相关 |

**注意事项：**
无

**示例:**
sag attribute show accountlock

## 12.6.19 帐户安全策略设置:

**语法：**
sag attribute set accountlock active { off | on time <num> allow <boolean> date <d-h-M>}

**参数说明：**

| | |
|---|---|
| attribute | sslvpn 命令行部分，宏观用户属性类相关命令 |
| set | 修改配置类基本操作 |
| accountlock | 操作对象，用户锁开关，off：不启用，on：启用，默认不启用 |
| time | 最大出错次数，小于 9999，默认 5 |
| allow | 允许自动解锁，0：不允许，1：允许，默认不允许 |
| date | 自动解锁时限，<d-h-M>，例如：01-02-03，默认 00-00-00 |

**注意事项：**
无

**示例:**
sag attribute set accountlock active on time 5 allow 1 date 01-02-03

## 12.6.20 手动解锁帐号显示：

**语法：**

sag attribute show accountlock list

**参数说明：**

| | |
|---|---|
| attribute | sslvpn 命令行部分，宏观用户属性类相关命令 |
| show | 显示类基本操作 |
| accountlock | 操作对象，用户锁相关 |
| list | 操作对象，已被锁定帐号列表相关 |

**注意事项：**

无

**示例:**

sag attribute show accountlock list

## 12.6.21 手动解锁复位：

**语法：**

sag attribute unlock accountlock name <name> type { p | c }

**参数说明：**

| | |
|---|---|
| attribute | sslvpn 命令行部分，宏观用户属性类相关命令 |
| unlock | 解锁类基本操作 |
| accountlock | 操作对象，用户锁相关 |
| name | 用户名，已被锁定帐号列表相关，1-15 位中文、字母、数字、减号、下划线组合 |
| type | 用户类型,用户类型，p：口令用户，c：证书用户 |

**注意事项：**

无

**示例:**

sag attribute unlock accountlock name test type p

## 12.6.22 手动解锁批量复位:

**语法：**

sag attribute unlock accountlock names <name\;name...> types { p | c }

**参数说明：**

| | |
|---|---|
| attribute | sslvpn 命令行部分，宏观用户属性类相关命令 |
| unlock | 解锁类基本操作 |
| accountlock | 操作对象，用户锁相关 |
| names | 用户名，已被锁定帐号列表相关,可为多个，中间使用'\;'分隔 |
| type | 用户类型，p：口令用户，c：证书用户，多个以'-'连接 |

**注意事项：**

无

**示例:**

sag attribute unlock accountlock names test1\;test2 types p-c

## 12.6.23 首次登录强制修改页面显示:

**语法：**

sag attribute show passwordfirst

**参数说明：**

| | |
|---|---|
| attribute | sslvpn 命令行部分，宏观用户属性类相关命令 |
| show | 显示类基本操作 |
| passwordfirst | 操作对象，首次登录强制修改口令相关 |

**注意事项：**

无

**示例:**

sag attribute show passwordfirst

## 12.6.24 首次登录强制修改口令设置:

**语法：**

sag attribute set passwordfirst { true | false }

**参数说明：**

| | |
|---|---|
| attribute | sslvpn 命令行部分，宏观用户属性类相关命令 |
| set | 修改配置类基本操作 |
| passwordfirst | 操作对象，首次登录强制修改口令相关,配置项，true：启用， |

false：不启用；默认启用

**注意事项：**
无

**示例:**
sag attribute set passwordfirst true

## 12.6.25 口令复杂度要求显示:

**语法：**
sag attribute show passwordcheck

**参数说明：**
attribute sslvpn 命令行部分，宏观用户属性类相关命令
show 显示类基本操作
passwordcheck 操作对象，口令复杂度要求相关

**注意事项：**
无

**示例:**
sag attribute show passwordcheck

## 12.6.26 口令复杂度要求设置:

**语法：**
sag attribute set passwordcheck { no | weak | normal | good | better | perfect}

**参数说明：**
attribute sslvpn 命令行部分，宏观用户属性类相关命令
set 修改配置类基本操作
passwordcheck 操作对象，口令复杂度要求，no：无，weak：较弱，normal： 一般，good：较好， better：很好， perfect：极佳， 默认 weak

**注意事项：**
无

**示例:**
sag attribute set passwordcheck weak

## 12.6.27 登录超时控制显示:

**语法:**

sag attribute show timetoover

**参数说明:**

| | |
|---|---|
| attribute | sslvpn 命令行部分，宏观用户属性类相关命令 |
| show | 显示类基本操作 |
| timetoover | 操作对象，登录超时控制相关 |

**注意事项:**

无

**示例:**

sag attribute show timetoover

## 12.6.28 登录超时控制设置:

**语法:**

sag attribute set timtoover limit <num>

**参数说明:**

| | |
|---|---|
| attribute | sslvpn 命令行部分，宏观用户属性类相关命令 |
| set | 修改设置类基本操作 |
| timetover | 操作对象，登录超时控制相关 |
| limit | 超时限制，0~9999 分钟，默认 15 分钟 |

**注意事项:**

无

**示例:**

sag attribute set timtoover limit 15

## 12.6.29 动态附加码显示:

**语法:**

sag attribute show apc

**参数说明：**

| | |
|---|---|
| attribute | sslvpn 命令行部分，宏观用户属性类相关命令 |
| show | 显示类基本操作 |
| apc | 操作对象，动态附加码相关 |

**注意事项：**

无

**示例:**

sag attribute show apc

## 12.6.30 动态附加码设置:

**语法：**

sag attribute set apc {on | off} bitnum <num>

**参数说明：**

| | |
|---|---|
| attribute | sslvpn 命令行部分，宏观用户属性类相关命令 |
| set | 修改配置类基本操作 |
| apc | 操作对象，动态附加码开关，on：开启，off：关闭，默认关闭 |
| bitnum | 附加码位数（4~8），默认为 5 |

**注意事项：**

无

**示例:**

sag attribute set apc on  bitnum 5

## 12.6.31 用户口令修改策略显示:

**语法：**

sag attribute show passwordtestchange

**参数说明：**

| | |
|---|---|
| attribute | sslvpn 命令行部分，宏观用户属性类相关命令 |
| show | 显示类基本操作 |
| passwordtestchange | 操作对象，用户口令修改策略相关 |

**注意事项：**

无

**示例:**
sag attribute show passwordtestchange

## 12.6.32 用户口令修改策略设置:

**语法：**
sag attribute set passwordtestchange { true | false }

**参数说明：**
attribute sslvpn 命令行部分，宏观用户属性类相关命令
set 修改配置类基本操作
passwordtestchange 操作对象，用户口令修改策略相关，true：开启，false：关闭，默认不开启

**注意事项：**
无

**示例:**
sag attribute set passwordtestchange true

## 12.6.33 使用软键盘策略显示:

**语法：**
sag attribute show usesoftkey

**参数说明：**
attribute sslvpn 命令行部分，宏观用户属性类相关命令
show 显示类基本操作
usesoftkey 操作对象，用户软键盘策略相关

**注意事项：**
无

**示例:**
sag attribute show usesoftkey

## 12.6.34 使用软键盘策略设置:

**语法：**

sag attribute set usesoftkey { true | false }

**参数说明：**

attribute sslvpn 命令行部分，宏观用户属性类相关命令
set 设置修改类基本操作(标识)
usesoftkey 操作对象,用户软键盘开关，true：开启，false：关闭，默认开启

**注意事项：**

无

**示例:**

sag attribute set usesoftkey true

## 12.6.35 短信设备显示:

**语法：**

sag attribute show smsdevice

**参数说明：**

attribute sslvpn 命令行部分，宏观用户属性类相关命令
show 显示类基本操作
smsdevice 操作对象，短信相关

**注意事项：**

无

**示例:**

sag attribute show smsdevice

## 12.6.36 短信设备设置:

**语法：**

sag attribute set smsdevice {modem port { 1 | 2 | 3 | 4} baud {9600 | 19200 | 38400 | 57600 | 115200 } factory <string> model <string> | sp name <name> password <password> | raidus | ldap | cmpp ip <ip> port <port> name <name> password <password> factorycode <string>}

**参数说明：**

| | |
|---|---|
| attribute | sslvpn 命令行部分，宏观用户属性类相关命令 |
| set | 修改设置类基本操作 |
| smsdevice | 操作对象，短信相关 |
| modem | modem 方式 |
| port | 选择串口,串口可以选择：串口 1~串口 4，默 认 串口 1 |
| baud | 串口波特率,可以选择波特率为：9600 、9200 、38400 、 57600 、 115200 ，默认 57600 |
| factory | 厂商，用'\"'括起来，默认：”siemens” |
| model | 型号，用'\"'括起来，默认：“tc35” |
| sp | sp 方式 |
| name | 用户，默认：sslvpn |
| password | 口令 |
| radius | radius 方式 |
| ldap | ldap 方式 |
| cmpp, | cmpp 方式 |
| ip | 地址，默认 x.x.x.x |
| port | 端口 |
| name | 名字 |
| password | 口令 |
| factorycode | 企业代码，默认：123456 |

**注意事项：**

无

**示例:**

sag attribute set smsdevice modem port 1 baud 9600 factory \”siemens\” model \”TC35\”

## 12.6.37 短信属性显示 ：

**语法：**

sag attribute show smsattribute

**参数说明：**

| | |
|---|---|
| attribute | sslvpn 命令行部分，宏观用户属性类相关命令 |
| show | 显示类基本操作 |
| smsattribute | 操作对象，短信属性相关 |

**注意事项：**

无

**示例:**

sag attribute show smsdevice

## 12.6.38 短信属性设置:

**语法:**

sag attribute set smsattribute { { smsauth | authapc } passwordcheck { no | weak | normal | good | better | perfect} firstmodify { on | off} timeout <num> title <string> | { apc | no } timeout <num> title <string> }

**参数说明:**

| | |
|---|---|
| attribute | sslvpn 命令行部分，宏观用户属性类相关命令 |
| set | 修改配置类基本操作 |
| smsattribute | 操作对象，短信属性相关,smsauth：短信认证 ,authapc：认证码＋附加码 |
| passwordcheck | 口令复杂度要求，no：无，weak：较弱，normal： 一般，good：较好， better：很好， perfect：极佳， 默认 weak |
| firstmodify | 首次修改口令，on：开启，off：关闭，默认关闭 |
| timeout | 口令超时，默认 60 秒，999999 为上限 |
| title | 短信标题，用'\"'括起来，默认值：”Mobile PIN” |
| apc | no | 认证类型，动态附加码 | 无 |
| timeout | 口令超时，默认 60 秒，999999 为上限 |
| title | 短信标题，用'\"'括起来，默认值：”Mobile PIN” |

**注意事项:**

无

**示例:**

sag attribute set smsattribute smsauth passwordcheck weak firstmodify on timeout 60 title \“Mobile PIN\”

## 12.6.39 短信测试:

**语法:**

sag attribute test sms phonenumber <number> content <string>

**参数说明:**

| | |
|---|---|
| attribute | sslvpn 命令行部分，宏观用户属性类相关命令 |
| test | 显示类基本操作 |
| sms | 操作对象，短信属性相关 |
| phonenumber | 手机号码 |
| content | 短信内容，用'\"'括起来 |

**注意事项:**

无

**示例:**

sag attribute test sms phonenumber 15110268809 content \“for test!\”

# 12.7 认证配置相关命令及配置

## 12.7.1 CA 属性显示:

**语法:**

sag auth show caattribute

**参数说明:**

auth sslvpn 命令行部分，宏观认证类相关命令
show 显示类基本操作
caattribute 操作对象，CA 属性相关

**注意事项:**

无

**示例:**

sag auth show caattribute

## 12.7.2 CA 属性设置:

**语法:**

sag auth set caattribute model { no | { local | third } way { no | cert | sequence | name | email }}

**参数说明:**

auth sslvpn 命令行部分，宏观认证类相关命令
set 配置修改类基本操作
caattribute 操作对象，CA 属性相关
model Ca 模式，no：不使用 CA 标志，local：使用本地 CA，third：使用第三方 CA
way 应用交互方式，no： 没有交互，cert： 数字证书，sequence： 证书序列号 ，name： 一般名字，email：电子邮件 ，默认值为数字证书

**注意事项:**

无

**示例:**

sag auth set caattribute model local way cert

### 12.7.3 认证顺序显示:

**语法：**

sag auth show authorder

**参数说明：**

| | |
|---|---|
| auth | sslvpn 命令行部分，宏观认证类相关命令 |
| show | 显示类基本操作 |
| authorder | 操作对象，认证顺序相关 |

**注意事项：**

无

**示例:**

sag auth show authorder

### 12.7.4 认证顺序设置:

**语法：**

sag auth set authorder first { local | radius | ldap | no } second { local | radius | ldap | no } third { local | radius | ldap | no } fouth { local | radius | ldap | no } fifth { local | radius | ldap | no }

**参数说明：**

| | |
|---|---|
| auth | sslvpn 命令行部分，宏观认证类相关命令 |
| set | 配置修改类基本操作 |
| authorder | 操作对象(标识)，认证顺序相关 |
| first | 第一个认证方式，可为： local 、radius 、ldap 、no |
| second | 第二个认证方式，可为： local 、radius 、ldap 、no |
| third | 第三个认证方式，可为： local 、radius 、ldap 、no |
| fouth | 第四个认证方式，可为： local 、radius 、ldap 、no |
| fifth | 第五个认证方式，可为： local 、radius 、ldap 、no |

**注意事项：**

无

**示例:**

sag auth set authorder first local second no third no fouth no fifth no

## 12.7.5 显示第三方 RADIUS 服务器配置:

**语法:**

sag auth show radius

**参数说明:**

auth sslvpn 命令行部分，宏观认证类相关命令
show 显示类基本操作
radius 操作对象，radius 服务器相关

**注意事项:**

无

**示例:**

sag auth show radius

## 12.7.6 配置第三方 RADIUS 服务器信息:

**语法:**

sag auth set radius addr <url> port <port> key <password> authtype <chap|pap> cache {off | on [timeout <num>]}

**参数说明:**

auth sslvpn 命令行部分，宏观认证类相关命令
set 修改配置类基本操作
radius 操作对象，radius 服务器相关
addr 服务器地址，格式如：192.168.0.1
port 服务器端口，默认 1813
key 共享密钥
authtype 认证方式，chap、pap，默认为 chap
cache 启用缓存,off：不启用，on：启用，只有当选择开启时，timeout 选项可配置，默认为 off
timeout 缓存超时，默认 300

**注意事项:**

无

**示例:**

sag auth set radius addr 1.0.0.21 port 1813 key 12345678 authtype chap cache on timeout 300

## 12.7.7 测试第三方 RADIUS 服务器连接情况:

**语法:**

sag auth test radius addr <url> port <port> key <password> authtype <chap| pap> username <name> password <password>

**参数说明:**

| | |
|---|---|
| auth | sslvpn 命令行部分，宏观认证类相关命令 |
| test | 测试类基本操作 |
| radius | 操作对象，radius 服务器相关 |
| addr | 服务器地址，格式如 192.168.0.1 |
| port | 服务器端口，默认 1813 |
| key | 共享密钥 |
| authtype | 认证方式，chap、pap，默认为 chap |
| username | radius 服务器用户名 |
| password | radius 服务器密码 |

**注意事项:**

无

**示例:**

sag auth test radius addr 1.0.0.21 port 1813 key 12345678 authtype chap username radius-server password 123456789

## 12.7.8 显示第三方 LDAP 服务器配置:

**语法:**

sag auth show ldap

**参数说明:**

| | |
|---|---|
| auth | sslvpn 命令行部分，宏观认证类相关命令 |
| show | 显示类基本操作 |
| ldap | 操作对象，ldap 服务器相关 |

**注意事项:**

无

**示例:**

sag auth show ldap

## 12.7.9 配置第三方 LDAP 服务器信息:

**语法:**

sag auth set ldap addr <url> port <port> identify {password|DIGEST-MD5} userdn <string> cache {off | on timeout <num>} [adminname <name>] adminidentify {anonymous| password name <name> password <password>}

**参数说明:**

| | |
|---|---|
| auth | sslvpn 命令行部分，宏观认证类相关命令 |
| set | 修改配置类基本操作 |
| ldap | 操作对象，ldap 服务器相关 |
| addr | 服务器地址，格式如 192.168.0.1 |
| port | 服务器端口，默认 389 |
| identify | 鉴别方式，password：口令方 式，DIGEST-MD5：DIGEST－MD5 方式，默认口令方式 |
| userdn | 用户 DN 模式，用\"括起来，默认：”uid=%user%,o=tcl,c=cn” |
| cache | 启用缓存,off：不启用，on：启用，只有当选择开启时，timeout 选项可配置，默认为 off |
| timeout | 缓存超时，默认 300（秒） |
| adminname | 管理员基准名字，默认：o=tcl,c=cn |
| adminidentify | 管理鉴别方式,anonymous：匿名登录（默认无后续参数），password：口令登录，默认：口令登录 |
| name | 管理员名字，默认：cn=manager,o=tcl,c=cn |
| password | 管理员口令 |

**注意事项:**

无

**示例:**

sag auth set ldap addr 1.0.0.21 port 389 identify password userdn \”uid=%user %,o=tcl,c=cn\” cache on timeout 300 adminname adminnametext adminidentify password name cn=manager,o=tcl,c=cn password 12345678

## 12.7.10 测试第三方 LDAP 服务器连接情况:

**语法:**

sag auth test ldap addr <url> port <port> identify {password|DIGEST-MD5} userdn <string> cache {off | on timeout <num>} [adminname <name>] adminidentify {anonymous| password name <name> password <password>}

**参数说明:**

| | |
|---|---|
| auth | sslvpn 命令行部分，宏观认证类相关命令 |
| test | 测试类基本操作 |

ldap 操作对象，ldap 服务器相关
addr 服务器地址
port 服务器端口，默认 389
identify 鉴别方式，password：口令方 式，DIGEST-MD5：DIGEST－MD5 方式，默认口令方式
userdn 用户 DN 模式，用\"括起来，默认：”uid=%user%,o=tcl,c=cn”
cache 启用缓存,off：不启用，on：启用，只有当选择开启时，timeout 选项可配置，默认为 off
timeout 缓存超时，默认 300（秒）
adminname 管理员基准名字，默认：o=tcl,c=cn
adminidentify 管理鉴别方式,anonymous：匿名登录（默认无后续参数），password：口令登录，默认：口令登录
name 管理员名字，默认：cn=manager,o=tcl,c=cn
password 管理员口令

**注意事项：**
无

**示例:**
sag auth test ldap addr 1.0.0.21 port 389 identify password userdn \”uid=%user%,o=tcl,c=cn\” cache on timeout 300 adminname adminnametext adminidentify password name cn=manager,o=tcl,c=cn password 12345678

## 12.7.11 显示微软 AD 口令服务器配置:

**语法：**
sag auth show ad

**参数说明：**
auth sslvpn 命令行部分，宏观认证类相关命令
show 显示类基本操作
ad 操作对象，ad 服务器相关

**注意事项：**
无

**示例:**
sag auth show ad

## 12.7.12 配置微软 AD 口令服务器信息:

**语法：**
sag auth set ad addr <url> port <port> identify {password|DIGEST-MD5} userdn <string> cache {off | on

timeout <num>} [adminname <name>] adminidentify {anonymous| password name <name> password <password>}

**参数说明：**

auth sslvpn 命令行部分，宏观认证类相关命令
set 修改配置类基本操作
ad 操作对象，ad 服务器相关
addr 服务器地址
port 服务器端口，默认 389
identify 鉴别方式，password：口令方 式，DIGEST-MD5：DIGEST－MD5 方式，默认口令方式
userdn 用户 DN 模式，用\"括起来，默认：”uid=%user%,o=tcl,c=cn”
cache 启用缓存,off：不启用，on：启用，只有当选择开启时，timeout 选项可配置，默认为 off
timeout 缓存超时，默认 300（秒）
adminname 管理员基准名字，默认：o=tcl,c=cn
adminidentify 管理鉴别方式,anonymous：匿名登录（默认无后续参数），password：口令登录，默认：口令登录
name 管理员名字，默认：cn=manager,o=tcl,c=cn
password 管理员口令

**注意事项：**

无

**示例:**

sag auth set ad addr 1.0.0.21 port 389 identify password userdn uid=\”%user` %,o=tcl,c=cn\” cache on timeout 300 adminname o=tcl,c=cn adminidentify password name cn=manager,o=tcl,c=cn password 12345678

## 12.7.13 测试微软 AD 口令服务器连接情况:

**语法：**

sag auth test ad addr <url> port <port> identify {password|DIGEST- MD5} userdn <string> cache {off | on timeout <num>} [adminname <name>] adminidentify {anonymous| password name <name> password <password>}

**参数说明：**

auth sslvpn 命令行部分，宏观认证类相关命令
test 测试类基本操作
ad 操作对象，ad 服务器相关
addr 服务器地址
port 服务器端口，默认 389
identify 鉴别方式，password：口令方 式，DIGEST-MD5：DIGEST－MD5 方式，默认口令方式
userdn 用户 DN 模式，用\"括起来，默认：”uid=%user%,o=tcl,c=cn”
cache 启用缓存,off：不启用，on：启用，只有当选择开启时，timeout 选项可

配置，默认为 off
timeout 缓存超时，默认 300（秒）
adminname 管理员基准名字，默认：o=tcl,c=cn
adminidentify 管理鉴别方式,anonymous：匿名登录（默认无后续参数），password：口令登录，默认：口令登录
name 管理员名字，默认：cn=manager,o=tcl,c=cn
password 管理员口令

**注意事项：**
无

**示例:**
sag auth test ad addr 1.0.0.21 port 389 identify password userdn uid=%user %,o=tcl,c=cn on timeout 300 adminname o=tcl,c=cn adminidentify password name cn=manager,o=tcl,c=cn password 12345678

### 12.7.14 获取第三方服务器上用户信息

**语法：**
sag auth show thirdofuser by {ldap|ad} type { p|c} [dn<string>]

**参数说明：**
auth sslvpn 命令行部分，宏观认证类相关命令
show 显示类基本操作
thirdofuser 操作对象
by 服务器对象，可为：ldap，ad
type 用户类型 p：口令用户，c：或证书用户
dn 用户 dn 值

**示例:**
sag auth show thirdofuser by ldap type p dn cn=Manager,dc=example,dc=com

## 12.8 证书配置相关命令及配置：

**语法：**
sag cert show gatecert

**参数说明：**
cert sslvpn 命令行部分，宏观证书类相关命令
show 显示类基本操作
gatecert 操作对象，CA 网关证书相关

**注意事项：**
无

**示例:**
sag cert show gatecert

## 12.8.1 网关数字证书设置:

**语法：**
sag cert set gatecert org <string> department <string> name <string>

**参数说明：**

| | |
|---|---|
| cert | sslvpn 命令行部分，宏观证书类相关命令 |
| set | 修改配置类基本操作 |
| gatecert | 操作对象，CA 网关证书相关 |
| org | 组织，用'\"'括起来，默认值：”LeadSec 网御 SAG” |
| department | 部门，用'\"'括起来，默认值：”SSLVPN” |
| name | 名字，用'\"'括起来，默认值：”192.168.100.1”，默认输入网关 ip |

**注意事项：**
无

**示例:**
sag cert set gatecert org \”LeadSec 网御 SAG\” department \”SSLVPN\” name \”192.168.100.1\”

## 12.8.2 网关可信证书链显示:

**语法：**
sag cert show rootcert

**参数说明：**

| | |
|---|---|
| cert | sslvpn 命令行部分，宏观证书类相关命令 |
| show | 显示类基本操作 |
| rootcert | 操作对象，可信证书链相关 |

**注意事项：**
无

**示例:**
sag cert show rootcert

### 12.8.3 第三方可信证书链显示:

**语法：**

sag cert show thirdcert

**参数说明：**

| | |
|---|---|
| cert | sslvpn 命令行部分，宏观证书类相关命令 |
| show | 显示类基本操作 |
| thirdcert | 操作对象，可信证书链相关 |

**注意事项：**

无

**示例:**

sag cert show thirdcert

### 12.8.4 添加可信证书链:

**语法：**

sag cert add thirdcert peer <boolean> path <string>

**参数说明：**

| | |
|---|---|
| cert | sslvpn 命令行部分，宏观证书类相关命令 |
| add | 添加类基本操作 |
| thirdcert | 操作对象，可信证书链相关 |
| peer | peer，默认为 0，无法配置，直接发送 0 |
| path | 证书链文件路径，关键取和保存文件，包含文件名，用\"括起来 |

**注意事项：**

无

**示例:**

sag cert add thirdcert peer 0 path \"/xx/xx/xx.crt\"

### 12.8.5 删除可信证书链:

**语法：**

sag cert del thirdcert id <string>

**参数说明：**

| | |
|---|---|
| cert | sslvpn 命令行部分，宏观证书类相关命令 |
| del | 删除类基本操作 |
| thirdcert | 操作对象，可信证书链相关 |
| id | 证书标识，在此应为证书指纹或名称，用\"”括起来 |

**注意事项：**

无

**示例:**

sag cert del thirdcert id \”xxxxxxxxxxxxxxxxxx\”

## 12.8.6 第三方网关证书显示:

**语法：**

sag cert show thirdkeypair

**参数说明：**

| | |
|---|---|
| cert | sslvpn 命令行部分，宏观证书类相关命令 |
| show | 显示类基本操作 |
| thirdkeypair | 操作对象，第三方网关证书相关 |

**注意事项：**

无

**示例:**

sag cert show thirdkeypair

## 12.8.7 第三方网关证书设置:

**语法：**

sag cert set thirdkeypair peer <boobean> path <string> password <password>

**参数说明：**

| | |
|---|---|
| cert | sslvpn 命令行部分，宏观证书类相关命令 |
| set | 修改配置类基本操作 |
| thirdkeypair | 操作对象，第三方网关证书相关 |
| peer | peer，默认为 0，无法配置，直接发送 0 |
| path | 证书链文件路径，关键取和保存文件，包含文件名，用\"”括起来 |
| password | 文件保护口令 |

**注意事项：**
无

**示例:**
sag cert set thirdkeypair peer 0 path \"/a/b/xx.p12\" password 12345678

## 12.8.8 生成证书请求显示:

**语法：**
sag cert show localcert

**参数说明：**

| | |
|---|---|
| cert | sslvpn 命令行部分，宏观证书类相关命令 |
| show | 显示类基本操作 |
| localcert | 操作对象，证书请求相关 |

**注意事项：**
无

**示例:**
sag cert show localcert

## 12.8.9 生成证书请求:

**语法：**
sag cert add localcert country <country> org <string> department <string> ipdns <string> peer <boolean> [province <string>] [town string>]

**参数说明：**

| | |
|---|---|
| cert | sslvpn 命令行部分，宏观证书类相关命令 |
| add | 添加类基本操作 |
| localcert | 操作对象，证书请求相关 |
| country | 国家，只能是字符或数字，为两个字节。默认 CN。 |
| org | 组织，用'\"'括起来，默认值：”LeadSec 网御 SAG” |
| department | 部门，用'\"'括起来，默认值：”SSLVPN” |
| ipdns | 名字，用'\"'括起来，默认值：”192.168.100.1” |
| peer | peer，默认为 0，无法配置，直接发送 0 |
| province | 省或直辖市，用'\"'括起来，默认为空 |
| town | 县或区，用'\"'括起来，默认为空 |

**注意事项：**
无

**示例:**
sag cert add localcert country CN org \“LeadSec 网御 SAG\” department \”SSLVPN\” ipdns \“192.168.100.1\” peer 0 province \”Tianjin\” town \”jixian\”

## 12.8.10 上传证书应答文件:

**语法:**
sag cert upload responecert path <string>

**参数说明:**

| | |
|---|---|
| cert | sslvpn 命令行部分，宏观证书类相关命令 |
| upload | 上传类基本操作 |
| responecert | 操作对象，证书应答相关 |
| path | 证书链文件路径，关键取和保存文件，包含文件名，用'\”'括起来 |

**注意事项:**
无

**示例:**
sag cert upload responecert \”path /a/b/c.crt\”

## 12.8.11 证书验证显示:

**语法:**
sag cert show verifycert

**参数说明:**

| | |
|---|---|
| cert | sslvpn 命令行部分，宏观证书类相关命令 |
| show | 显示类基本操作 |
| verifycert | 操作对象，证书验证相关 |

**注意事项:**
无

**示例:**
sag cert show verifycert

## 12.8.12 证书验证设置:

**语法:**

sag cert set verifycert { no | self | crl | crlfile | ocsp | ldap } crl <url> ocsp <url> [ldapaddr <url>] [port <port>] [crlname <name>]

**参数说明:**

| | |
|---|---|
| cert | sslvpn 命令行部分，宏观证书类相关命令 |
| set | 修改配置类基本操作 |
| verifycert | 操作对象(标识)，证书验证相关，no \| self \| crl \| crlfile \| ocsp \| ldap，分别对应：不验证丨仅根据证书自带信息验证丨通过设置的 CRL 发布点验证丨通过设置的 CRL 文件验证丨通过设置的 OCSP 发布点验证丨通过设置的 LDAP 发布点验证 |
| crl | CRL 发布点，标准 url 地址 |
| ocsp | OCSP 发布点，标准 url 地址 |
| ldapaddr | LDAP 地址，标准 url 地址 |
| port | LDAP 端口 |
| crlname | CRL 名字 |

**注意事项:**

无

**示例:**

sag cert set verifycert crlfile crl http://192.168.1.1:8080/CA/open/CRL ocsp http://192.168.1.1:8080/CA/open/OCSPServlet ldapaddr http://172.168.1.1:80 port 256 crlname nametext

## 12.8.13 上传第三方 CRL 文件:

**语法:**

sag cert upload thirdcrl path <string>

**参数说明:**

| | |
|---|---|
| cert | sslvpn 命令行部分，宏观证书类相关命令 |
| unload | 上传类基本操作 |
| thirdcrl | 操作对象，证书验证相关 |
| path | 证书链文件路径，关键取和保存文件，包含文件名，用\"括起来 |

**注意事项:**

无

**示例:**

sag cert upload thirdcrl path \"/a/b/xx.cr\"

## 12.8.14 LDAP 证书发布服务器显示：

**语法：**

sag cert show ldap

**参数说明：**

| | |
|---|---|
| cert | sslvpn 命令行部分，宏观证书类相关命令 |
| show | 显示类基本操作 |
| ldap | 操作对象，ldap 服务器相关 |

**注意事项：**

无

**示例:**

sag cert show ldap

## 12.8.15 LDAP 证书发布服务器设置：

**语法：**

sag cert set ldap addr <string> port <port> [name <name>] type { anonymous | {password | digestmd5} admin <string> password <password> }

**参数说明：**

| | |
|---|---|
| cert | sslvpn 命令行部分，宏观证书类相关命令 |
| set | 配置修改类基本操作 |
| ldap | 操作对象，ldap 服务器相关 |
| addr | 服务器地址，url 或 ip，默认使用 http 协议 |
| port | 服务器端口，默认值：389 |
| name | 基准名字，格式：o=tcl,c=cn |
| type | 鉴别方式，anonymous：匿名登录，password：简单口令，digestmd5： DIGEST-MD5 方式，默认为：口令方式 |
| admin | 管理员名字，默认值：cn=manager,o=tcl,c=cn，用'\"'括起来 |
| password | 管理员口令 |

**注意事项：**

无

**示例:**

sag cert set ldap addr 1.0.0.21 port 389 name o=tcl,c=cn type password admin \"cn=manager,o=tcl,c=cn\" password 12345678

## 12.8.16 微软 AD 证书发布服务器显示：

**语法：**

sag cert show ad

**参数说明：**

| | |
|---|---|
| cert | sslvpn 命令行部分，宏观证书类相关命令 |
| show | 显示类基本操作 |
| ad | 操作对象，ad 服务器相关 |

**注意事项：**

无

**示例:**

sag cert show ad

## 12.8.17 微软 AD 证书发布服务器配置：

**语法：**

sag cert set ad addr <string> port <port> [name <name>] type { anonymous | {password | digestmd5} admin <string> password <password> }

**参数说明：**

| | |
|---|---|
| cert | sslvpn 命令行部分，宏观证书类相关命令 |
| set | 配置修改类基本操作 |
| ad | 操作对象，ldap 服务器相关 |
| addr | 服务器地址，url 或 ip，默认使用 http 协议。 |
| port | 服务器端口，默认值：389 |
| name | 基准名字，格式：CN= Users ,DC=leadsec, DC=sag, DC=com |
| type | 鉴别方式，anonymous：匿名登录，password：简单口令，digestmd5： DIGEST-MD5 方式，默认为：口令方式 |
| admin | 管理员名字，默认值 CN=administrator,CN=Users,DC=leadsec, DC=sag,DC=com，用\"括起来 |
| password | 管理员口令 |

**注意事项：**

无

**示例:**

sag cert set ad addr 1.0.0.21 port 389 name CN=Users,DC=leadsec,DC=sag,DC=com type password admin \"CN=administrator,CN=Users,DC=leadsec,DC=sag,DC=com \"password 12345678

# 12.9 高级配置相关命令及配置：

**语法：**
sag advance show rules

**参数说明：**
advance sslvpn 命令行部分，宏观高级属性类相关命令
show 显示类基本操作
rules 操作对象，相关替换规则相关

**注意事项：**
无

**示例:**
sag advance show rules

## 12.9.1 相对替换修改：

**语法：**
sag advance set rules content <string>

**参数说明：**
advance sslvpn 命令行部分，宏观高级属性类相关命令
set 修改配置类基本操作
rules 操作对象，相关替换规则相关
content 替换规则，用'\”'括起来，可为多个，之间用'\;'隔开

**注意事项：**
无

**示例:**
sag advance set rules content \”contenttext1\”\;\”contenttext2\”

## 12.9.2 绝对替换显示：

**语法：**
sag advance show replace

**参数说明：**

| | |
|---|---|
| advance | sslvpn 命令行部分，宏观高级属性类相关命令 |
| show | 显示类基本操作 |
| replace | 操作对象，绝对替换规则相关 |

**注意事项：**

无

**示例：**

sag advance show replace

## 12.9.3 绝对替换修改：

**语法：**

sag advance set replace content <string>

**参数说明：**

| | |
|---|---|
| advance | sslvpn 命令行部分，宏观高级属性类相关命令 |
| set | 设置修改类基本操作 |
| replace | 操作对象，绝对替换规则相关 |
| content | 替换规则，用'\”'括起来，可为多个，之间用'\;'隔开 |

**注意事项：**

无

**示例：**

sag advance set replace content \”contenttext1\”\;\”contenttext2\”

## 12.9.4 HTTP 压缩显示：

**语法：**

sag advance show httpcompress

**参数说明：**

| | |
|---|---|
| advance | sslvpn 命令行部分，宏观高级属性类相关命令 |
| show | 显示类基本操作 |
| httpcompress | 操作对象，HTTP 压缩相关 |

**注意事项：**

无

**示例：**

sag advance show httpcompress

### 12.9.5 HTTP 压缩设置：

**语法：**

sag advance set httpcompress { true | false }

**参数说明：**

| | |
|---|---|
| advance | sslvpn 命令行部分，宏观高级属性类相关命令 |
| set | 修改配置类基本操作 |
| httpcompress | HTTP 压缩启用与否开关，true：开启，false：关闭，默认关闭 |

**注意事项：**

无

**示例：**

sag advance set httpcompress false

### 12.9.6 用户 DNS 显示：

**语法：**

sag advance show dns

**参数说明：**

| | |
|---|---|
| advance | sslvpn 命令行部分，宏观高级属性类相关命令 |
| show | 显示类基本操作 |
| dns | 操作对象，用户 DNS 相关 |

**注意事项：**

无

**示例：**

sag advance show dns

### 12.9.7 用户 DNS 设置：

**语法：**

sag advance set dns foruser { on | off } dnss <dns\;dns...>

**参数说明：**

| | |
|---|---|
| advance | sslvpn 命令行部分，宏观高级属性类相关命令 |
| set | 修改配置类基本操作 |
| dns | 用户 DNS 相关 |
| foruser | 将网关 DNS 配置提供给用户，on：提供，off：不提供，默认“不提供” |
| dnss | DNS 后缀，可为多个，中间使用'\;'分隔 |

**注意事项：**

无

**示例：**

sag advance set dns foruser off dnss com\;cn

## 12.9.8 虚拟 DNS 管理显示：

**语法：**

sag advance show vdns

**参数说明：**

| | |
|---|---|
| advance | sslvpn 命令行部分，宏观高级属性类相关命令 |
| show | 显示类基本操作 |
| vdns | 操作对象，虚拟 DNS 相关 |

**注意事项：**

无

**示例：**

sag advance show vdns

## 12.9.9 虚拟 DNS 删除：

**语法：**

sag advance del vdns name <dns>

**数说明：**

| | |
|---|---|
| advance | sslvpn 命令行部分，宏观高级属性类相关命令 |
| del | 删除类基本操作 |
| vdns | 操作对象，虚拟 DNS 相关 |
| name | 虚拟 DNS 名字 |

**注意事项：**
无

**示例：**
sag advance del vdns name www.baidu.com

## 12.9.10 虚拟 DNS 批量删除：

**语法：**
sag advance del vdns names <dns\;dns...>

**参数说明：**

| | |
|---|---|
| advance | sslvpn 命令行部分，宏观高级属性类相关命令 |
| del | 删除类基本操作 |
| vdns | 操作对象，虚拟 DNS 相关 |
| names | 虚拟 DNS 名字，可为多条，中间使用'\;'分隔 |

**注意事项：**
无

**示例：**
sag advance del vdns names www.baidu.com\;www.163.com

## 12.9.11 虚拟 DNS 修改：

**语法：**
sag advande set vdns oldname <dns> name <dns> ip <ip> [note <string>]

**参数说明：**

| | |
|---|---|
| advance | sslvpn 命令行部分，宏观高级属性类相关命令 |
| set | 修改类基本操作 |
| vdns | 操作对象，虚拟 DNS 相关 |
| oldname | 未修改前的名字 |
| name | 虚拟 DNS 名字，可为多条，中间使用 ‘\;’分隔。 |
| ip | IP 地址，格式如：192.168.0.1 |
| note | 注释，用'\"'括起来 |

**注意事项：**
无

**示例：**
sag advande set vdns name www.baidu.com ip 1.0.0.1

## 12.9.12 虚拟 DNS 增加:

**语法：**

sag advande add vdns name <dns> ip <ip> [note <string>]

**参数说明：**

| | |
|---|---|
| advance | sslvpn 命令行部分，宏观高级属性类相关命令 |
| add | 添加类基本操作 |
| vdns | 操作对象，虚拟 DNS 相关 |
| name | 虚拟 DNS 名字，可为多条，中间使用“\;”分隔。 |
| ip | IP 地址，格式如：192.168.0.1 |
| note | 注释，用'\”'括起来 |

**注意事项：**

无

**示例：**

sag advande add vdns name www.baidu.com ip 1.0.0.1 note \”notetext\”

## 12.9.13 应用缓存显示：

**语法：**

sag advance show cache

**参数说明：**

| | |
|---|---|
| advance | sslvpn 命令行部分，宏观高级属性类相关命令 |
| show | 显示类基本操作 |
| cache | 操作对象，应用缓存相关 |

**注意事项：**

无

**示例：**

sag advance show cache

## 12.9.14 应用缓存设置：

**语法：**

sag advance set cache used { on | off } filelimit <num> memlimit <num> disklimit <num> lifetime <num>

**参数说明：**

| | |
|---|---|
| advance | sslvpn 命令行部分，宏观高级属性类相关命令 |
| set | 设置修改类基本操作 |
| cache | 操作对象，应用缓存相关 |
| used | 启用应用缓存，on：启用，off：不启用，默认关闭 |
| filelimit | 文件大小上限，默认 1024K |
| memlimit | 使用内存上限，默认 32M |
| disklimit | 使用磁盘上限，默认 1024M |
| lifetime | 缓存保存期限，默认 1 天 |

**注意事项：**

无

**示例：**

sag advance set cache used on filelimit 1024 memlimit 32 disklimit 1024 lifetime 1

## 12.9.15 重置应用缓存：

**语法：**

sag advance reset cache

**参数说明：**

| | |
|---|---|
| advance | sslvpn 命令行部分，宏观高级属性类相关命令 |
| reset | 复位类基本操作 |
| cache | 操作对象，应用缓存相关 |

**注意事项：**

无

**示例：**

sag advance reset cache

## 12.9.16 用户 ICMP 属性显示：

**语法：**

sag advance show icmp

**参数说明：**

| | |
|---|---|
| advance | sslvpn 命令行部分，宏观高级属性类相关命令 |
| show | 显示类基本操作 |
| icmp | 操作对象，ICMP 相关 |

**注意事项：**

无

**示例：**
sag advance show icmp

## 12.9.17 用户 ICMP 属性设置：

**语法：**
sag advance set icmp value { no | virtual | real}

**参数说明：**

| | |
|---|---|
| advance | sslvpn 命令行部分，宏观高级属性类相关命令 |
| set | 显示类基本操作 |
| icmp | 操作对象，ICMP 相关 |
| value | 属性， no ： 忽略，virtual ： 虚拟，real：实际，默认显示“忽略” |

**注意事项：**
无

**示例：**
sag advance set icmp value no

## 12.9.18 多线路优化显示:

**语法：**
sag advance show multiline

**参数说明：**

| | |
|---|---|
| advance | sslvpn 命令行部分，宏观高级属性类相关命令 |
| show | 显示类基本操作 |
| multiline | 操作对象，多线路优化相关 |

**注意事项：**
无

**示例：**
sag advance show multiline

## 12.9.19 多线路优化设置：

**语法：**

sag advance set multiline values <string\;string...>

**参数说明：**

| | |
|---|---|
| advance | sslvpn 命令行部分，宏观高级属性类相关命令 |
| set | 显示类基本操作 |
| multiline | 操作对象，多线路优化相关 |
| values | 多线路优化配置，用'\"'括起来，默认为空，可为多个，中间使用"\;"分隔 |

**注意事项：**

无

**示例：**

sag advance set multiline values \"中国网通＝1.0.0.1:443\"\;\"中国典型＝1.0.0.3:443\"

# 12.10 负载均衡相关命令及配置

## 12.10.1 负载均衡显示:

**语法：**

sag balance show balance

**参数说明：**

| | |
|---|---|
| balance | sslvpn 命令行部分，宏观负载均衡类相关命令 |
| show | 显示类基本操作 |
| balance | 操作对象，负载均衡相关 |

**注意事项：**

无

**示例：**

sag balance show balance

## 12.10.2 负载均衡设置:

**语法：**

sag balance set balance syn { on | off } config { master | slave } server <string> password <password> [infos <string\;string...>]

**参数说明：**

| | |
|---|---|
| balance | sslvpn 命令行部分，宏观负载均衡类相关命令 |
| set | 修改配置类基本操作 |
| balance | 操作对象，负载均衡相关 |
| syn | 是否启动自动同步，on：启动，off：不启动，默认不启动 |
| config | 主从配置,master \| slave，分别为：主模式丨从机模式，默认 slave |
| server | 服务器，用'\"'括起来，主设备 ip |
| password | 密码，主设备密码 |
| infos | 内外网信息，用'\"'括起来，默认：”外网信息＝1.0.0.1;443／444，内网信息＝2.0.0.2：443／444” |

**注意事项：**
无

**示例：**
sag balance set balance syn off config master server \”1.0.0.1\” password administrator infos "外网信息＝1.0.0.1：443／444，内网信息＝2.0.0.2：443／ 444”\;\”other info\”

# 12.11 在线用户相关命令及配置:

## 12.11.1 在线用户显示

**语法：**
sag online show user [page <num>] [order<num>]

**参数说明：**

| | |
|---|---|
| online | sslvpn 命令行部分，宏观在线用户类相关命令 |
| show | 显示类基本操作 |
| user | 操作对象，用户相关 |
| page | 显示页的对象 |
| order | 显示对象的顺序 |

**注意事项：**
无

**示例：**
sag online show user page 1 order 0

## 12.11.2 踢掉在线用户

**语法：**
sag online kick user key <value> name <name>

**参数说明：**
online sslvpn 命令行部分，宏观在线用户类相关命令
kick 强制下线类基本操作
user 操作对象，用户相关
key 用户 id，6-15 位数字
name 在线用户登录名，1-15 位中文、字母、数字、减号、下划线组合

**注意事项：**
无

**示例：**
sag online kick user key 1234567899 name test

### 12.11.3 统计当前并发用户数:

**语法：**
sag online show onlineuser

**参数说明：**
online sslvpn 命令行部分，宏观在线用户类相关命令
show 显示类基本操作
onlineuser 操作对象，在线用户相关

**注意事项：**
无

**示例：**
sag online show onlineuser

## 12.12 接入防护 和 应用防护相关命令及配置

### 12.12.1 Web 接入防护显示:

**语法：**
sag defend show access

**参数说明：**

| | |
|---|---|
| defend | sslvpn 命令行部分，宏观防护类相关命令 |
| show | 显示类基本操作 |
| access | 操作对象，接入防护操作相关 |

**注意事项：**

无

**示例：**

sag defend show access

## 12.12.2 接入防护增加策略:

**语法：**

sag defend add access name <name> protocal { get | post | all } rule { url | para | all } way { normal | regular} distinguish { yes | no } content <string> operate { log | prevent} [note <string>]

**参数说明：**

| | |
|---|---|
| defend | sslvpn 命令行部分，宏观防护类相关命令 |
| add | 添加类基本操作 |
| access | 操作对象，接入防护操作相关 |
| name | 策略名称，1-15 位中文、字母、数字、减号、下划线组合 |
| protocal | 匹配协议,get： HTTP GET，post： HTTP POST，all： HTTP GET&POST，默认 HTTP GET |
| rule | 匹配规则，url ：匹配 URL ，para： 匹配参数， all：匹配全部 ，默认： 匹配 URL |
| way | 匹配方式,normal ：一般匹配 ， regular： 正则表达式匹配，默认：一般匹配 |
| distinguish | 区分大小写，含义：yes：是， no：否，默认 yes |
| content | 配置内容，用'\"'括起来 |
| operate | 操作，log：记录日志， prevent： 阻止访问，默认：记录日志 |
| note | 注释，用'\"'括起来 |

**注意事项：**

无

**示例：**

sag defend add access name 网御 protocal get rule url way normal distinguish yes content \"content\" operate log note \"notetext\"

## 12.12.3 修改新增服务策略:

**语法：**

sag defend set access id <value> name <name> protocal { get | post | all } rule { url | para | all } way { normal | regular} distinguish { yes | no } content <string> operate { log | prevent} [note <string>]

**参数说明：**

| | |
|---|---|
| defend | sslvpn 命令行部分，宏观防护类相关命令 |
| set | 修改类基本操作 |
| access | 操作对象，接入防护操作相关 |
| id | 策略 id，6-15 位数字 |
| name | 策略名称，1-15 位中文、字母、数字、减号、下划线组合 |
| protocal | 匹配协议,get： HTTP GET，post： HTTP POST，all：HTTP GET&POST，默认 HTTP GET |
| rule | 匹配规则，url ：匹配 URL ，para： 匹配参数， all：匹配全部 ，默认： 匹配 URL |
| way | 匹配方式,normal ：一般匹配 ， regular： 正则表达式匹配，默认：一般匹配 |
| distinguish | 区分大小写，含义：yes：是， no：否，默认 yes |
| content | 配置内容，用'\"'括起来 |
| operate | 操作，log：记录日志， prevent： 阻止访问，默认：记录日志 |
| note | 注释，用'\"'括起来 |

**注意事项：**

无

**示例：**

sag defend add access id 1234667890123 name 网御 protocal get rule url way normal distinguish yes content content \"content\" operate log note \"notetext\"

## 12.12.4 删除新增策略:

**语法：**

sag defend del access id <value> name <name>

**参数说明：**

| | |
|---|---|
| defend | sslvpn 命令行部分，宏观防护类相关命令 |
| del | 删除类基本操作 |
| access | 操作对象，接入防护操作相关 |
| id | 策略 id，6-15 位数字 |
| name | 策略名称，1-15 位中文、字母、数字、减号、下划线组合 |

**注意事项：**

无

**示例：**

sag defend del access id 1234667890123 name 网御

### 12.12.5 修改原有策略:

**语法：**

sag defend set oldaccess id <value> name <name> operate { log | prevent}

**参数说明：**

| | |
|---|---|
| defend | sslvpn 命令行部分，宏观防护类相关命令 |
| set | 修改类基本操作 |
| oldaccess | 操作对象，接入防护操作相关 |
| id | 策略 id，6-15 位数字 |
| name | 策略名称，1-15 位中文、字母、数字、减号、下划线组合 |
| operate | 操作，log：记录日志， prevent： 阻止访问，默认：记录日志 |

**注意事项：**

无

**示例：**

sag defend set oldaccess id 1234667890123 name 网御 operate log

### 12.12.6 应用防护 DOS 防护用户显示:

**语法：**

sag defend show userdos

**参数说明：**

| | |
|---|---|
| defend | sslvpn 命令行部分，宏观防护类相关命令 |
| show | 显示类基本操作 |
| userdos | 操作对象，应用防护（用户 DOS）操作相关 |

**注意事项：**

无

**示例：**

sag defend show userdos

### 12.12.7 DOS 防护用户设置:

**语法：**

sag defend set userdos action { off | on maxconnect <string>}

**参数说明：**

| | |
|---|---|
| defend | sslvpn 命令行部分，宏观防护类相关命令 |
| set | 修改配置类基本操作 |
| userdos | 操作对象，应用防护（用户 DOS）操作相关 |
| action | 启用开关，off：不启用， on：启用，默认不启用 |
| maxconnect | 每用户最大连接数 |

**注意事项：**

无

**示例：**

sag defend set userdos action off

sag defend set userdos action on maxconnect 100

# 12.13 对外 RADIUS 服务相关命令及配置:

## 12.13.1 对外 RADIUS 服务显示

**语法：**

sag radius show service

**参数说明：**

| | |
|---|---|
| radius | sslvpn 命令行部分，宏观本地 RADIUS 类相关命令 |
| show | 显示类基本操作 |
| service | 操作对象，服务相关 |

**注意事项：**

无

**示例：**

sag radius show service

## 12.13.2 对外 RADIUS 服务设置:

**语法：**

sag radius set service action { on | off } sharesecret <password> port <port> nass <ip\;ip...>

**参数说明：**

| | |
|---|---|
| radius | sslvpn 命令行部分，宏观本地 RADIUS 类相关命令 |

| | |
|---|---|
| set | 修改配置类基本操作 |
| service | 操作对象，服务相关 |
| action | 是否启动服务，on：启动，off：不启动，默认不启动 |
| sharesecret | 共享口令 |
| port | 监听端口，默认 1812 |
| nass | NASS 地址，可为多个，以'\;'分隔，格式：x.x.x.x/xx\;x.x.x.x/xx |

**注意事项：**
无

**示例：**
sag radius set service action off sharesecret 12345678 port 1812 nass 1.0.0.1/24 \;1.0.1.1/24

# 第13章 IPv6

## 13.1 IPv6 配置

### 13.1.1 接口配置(Interface)

#### 编辑接口的 ipv6 地址及属性：

**语法：**
interface ipv6 set phy if <name> edit {ip <ip/mask> [ping {on|off}] [admin {on|off}] [traceroute {on|off}] [ ipra {on|off}] [valid_time <time>] [prefer_time <time> ]} +

**参数说明：**

| | |
|---|---|
| if | 物理设备的名称 |
| edit | 清除接口以前的 ipv6 地址及属性配置，按此次参数配置 |
| ip | ipv6 地址及掩码位数 |
| admin | on：设备 IP 可用于管理，off：设备 IP 不可用于管理 |
| ping | on：设备 IP 允许 ping，off：设备 IP 不允许 ping |
| traceroute | on：设备 IP 允许 traceroute，off：设备 IP 不允许 traceroute |
| ipra | on：此 ip 开启路由通告功能，off：此 ip 关闭路由通告功能 |
| valid_time | 路由通告信息中此 ip 的有效生存时间 |
| prefer_time | 路由通告信息中此 ip 的首选生存时间（优先生存时间） |

**注意事项：**

1.只有设备开启且处于路由模式时才可以为设备配置 ipv6
2.在命令行上，如果需要将所有 ip 清空，可以下发命令：

| Interface ipv6 set phy if <name> edit ip none |
|---|

**示例：**

```
ac>interface ipv6 set phy if eth0 edit ip 2011：：11:15/64 admin on ping on ipra on valid_time 1500 prefer_time 1200
```

## 添加接口的 ipv6 地址及属性：

**语法：**

interface ipv6 set phy if <name> add {ip <ip/mask> [ping {on|off}] [admin {on|off}] [traceroute {on|off}] [ ipra {on|off}] [valid_time <time>] [prefer_time <time> ]} +

**参数说明：**

| | |
|---|---|
| if | 物理设备的名称 |
| add | 保留接口以前的 ipv6 地址及属性配置，添加此次配置 |
| ip | ipv6 地址及掩码位数 |
| admin | on：设备 IP 可用于管理，off：设备 IP 不可用于管理 |
| ping | on：设备 IP 允许 ping，off：设备 IP 不允许 ping |
| traceroute | on：设备 IP 允许 traceroute，off：设备 IP 不允许 traceroute |
| ipra | on：此 ip 开启路由通告功能，off：此 ip 关闭路由通告功能 |
| valid_time | 路由通告信息中此 ip 的有效生存时间 |
| prefer_time | 路由通告信息中此 ip 的首选生存时间（优先生存时间） |

**注意事项：**

| 1.只有设备开启且处于路由模式时才可以为设备配置 ipv6 |
|---|

**示例：**

```
ac>interface ipv6 set phy if eth0 add ip 2012：：11:15/64 admin on ping off ipra on valid_time 1500 prefer_time 1200
```

## 修改接口的 ipv6 地址的属性：

**语法：**

interface ipv6 set phy if <name> set {ip <ip/mask> [ping {on|off}] [admin {on|off}] [traceroute {on|off}] [ ipra {on|off}] [valid_time <time>] [prefer_time <time> ]} +

**参数说明：**

| | |
|---|---|
| if | 物理设备的名称 |
| add | 修改接口已有的那些 ip 地址的属性 |
| ip | ipv6 地址及掩码位数 |
| admin | on：设备 IP 可用于管理，off：设备 IP 不可用于管理 |
| ping | on：设备 IP 允许 ping，off：设备 IP 不允许 ping |
| traceroute | on：设备 IP 允许 traceroute，off：设备 IP 不允许 traceroute |
| ipra | on：此 ip 开启路由通告功能，off：此 ip 关闭路由通告功能 |
| valid_time | 路由通告信息中此 ip 的有效生存时间 |
| prefer_time | 路由通告信息中此 ip 的首选生存时间（优先生存时间） |

**注意事项：**

| |
|---|
| 1.只有设备开启且处于路由模式时才可以为设备配置 ipv6<br>2.此处是修改已有的 ip 的管理、ping 等属性，不能改变 ip |

**示例：**

```
ac>interface ipv6 set phy if eth0 set ip 2012：：11:15/64 admin off ping off ipra off valid_time 1500 prefer_time 1200
```

## 删除接口的 ipv6 地址：

**语法：**

interface ipv6 set phy if <name> del {ip <ip/mask> } +

**参数说明：**

| | |
|---|---|
| if | 物理设备的名称 |
| add | 修改接口已有的那些 ip 地址的属性 |
| ip | ipv6 地址及掩码位数 |

**注意事项：**

| |
|---|
| 1.只有设备开启且处于路由模式时才可以为设备配置 ipv6<br>2.此所有删除的 ip 的属性会一并关闭和清空 |

**示例：**

```
ac>interface ipv6 set phy if eth0 del ip 2012：：11:15/64
```

## 修改接口的 natpt 的状态：

**语法：**

interface ipv6 set phy if <name> natpt {on|off}

**参数说明：**

| | |
|---|---|
| if | 物理设备的名称 |
| natpt | on：表示开启；off 表示关闭 |

**注意事项：**

| |
|---|
| 1.只有设备开启且处于路由模式时才可以为设备配置 ipv6 |

**示例：**

```
ac>interface ipv6 set phy if eth0 natpt on
```

## 修改接口的路由通告参数：

**语法：**

interface ipv6 set phy if <name> routeadv {on|off} [inter_time <time> ] [route_time <time>]

**参数说明：**

| | |
|---|---|
| if | 物理设备的名称 |
| routeadv | on：表示开启；off 表示关闭 |
| inter_time | 路由通告周期 |
| route_time | 路由器生命期 |

**注意事项：**

1.只有设备开启且处于路由模式时才可以为设备配置 ipv6

**示例：**

```
ac>interface ipv6 set phy if eth0 routeadv on inter_time 200 route_time 1800
```

## 查看接口的所有 ipv6 配置：

**语法：**

interface ipv6 show if <name>

**参数说明：**

| | |
|---|---|
| if | 物理设备的名称 |

**注意事项：**

1.此命令能查看某接口的所有 ipv6 配置，包括 ipv6 地址及属性、natot、路由通告的参数

**示例：**

```
ac>interface ipv6 show if eth0
```

# 13.1.2 安全规则(rule)

## 添加允许类型的安全策略：

**语法：**

rule ipv6 add type permit name <name> [ id <id> ] [ srcip { <ip6> | ipname <name> | any } ] [ dstip { <ip6> | ipname <name> | any } ] [ srcport <port> ] [ smac <mac> ] [ iif { any | <name> } ] [ oif { any | <name> } ] [ service { any | <name> } ] [ avpolicy <id> ] [ ipspolicy <id> ] [ pcpolicy <id> ] [ eimpolicy <id> ] [ exhah { on | off } [ spi <string> ] [ length <string> ] [ reschk { on | off } ] ] [ exhdst { on | off } [ length <string> ] [ opt <string> ] ] [ exhfrag { on | off } [ id <string> ] [ length <string> ] [ reschk { on | off } ] [ first { on | off } ] [ moreorlast { more | last } ] ] [ exhhbh { on | off } [ length <string> ] [ opt <string> ] ] [ exhmh { on | off } [ type <string> ] ] [ exhrt { on | off } [ type <string> ] [ segsleft <string> ] [ length <string> ] ] [ exhesp { on | off } [ spi <string> ] ] [ active { on | off } ] [ log { on | off } ] [ comment <comment> ] [time {none | <name>}]

**关键参数说明：**

| | |
|---|---|
| name | 设置安全规则的名字，必选参数 |
| id | 设置安全规则的序号，有效值为 1 至 65535，可选参数，默认为最后 |

| | |
|---|---|
| srcip | 设置源地址，可以使用单个 IP 地址、IP 地址/子网掩码、地址定义、地址组定义、“any”，可选参数，默认为“any” |
| dstip | 设置源地址，可以使用单个 IP 地址、IP 地址/子网掩码、地址定义、地址组定义、“any”，可选参数，默认为“any” |
| srcport | 设置源端口，有效值为 1 至 65535，可以用,分割表示多个端口，或用:分割表示端口段，可选参数，默认为“any” |
| smac | 设置源 MAC 地址，可选参数，默认为“any” |
| iif | 设置流入网口，可选参数，默认为“any” |
| service | 设置服务，可以使用服务、服务组 |
| avpolicy | 病毒防护策略 |
| ipspolicy | 入侵防护策略 |
| pcpolicy | 协议控制策略 |
| eimpolicy | 上网行为管理策略 |
| exhah | 身份验证头 |
| spi | 安全参数索引 |
| length | 身份验证头长度 |
| reschk | 预留字段检查 |
| exhdst | 目的地选项头 |
| length | 目的地选项头长度 |
| opt | 选项, 值范围{ 0 - 0xFF} |
| exhfrag | 分段头 |
| id | 分段 id |
| length | 分段头长度 |
| reschk | 预留字段检查 |
| first | 检查第一个分段 |
| moreorlast | 检查多个分段或最后一个分段 |
| exhhbh | 逐跳选项头 |
| length | 逐跳选项头长度 |
| opt | 选项, 值范围{ 0 - 0xFFFFFFFF} |
| exhmh | 移动扩展头 |
| type | 移动扩展头类型 |
| exhrt | 选路头 |
| type | 选路头类型 |
| segsleft | 匹配 Segments Left 域的值或范围 |
| length | 选路头长度 |
| exhesp | 封装安全性净荷头 |
| spi | 安全参数索引 |
| log | 设置日志记录，可选参数，默认为不记录日志 |
| active | 设置是否生效，可选参数，默认为生效 |
| comment | 设置规则注释 |

**注意事项：**

当安全规则的类型为代理时，服务的目的端口必须是单个端口；

当代理服务类型为用户自定义代理服务时，目的地址必须为单个 IP 地址。

## 添加禁止类型的安全策略：

**语法：**

rule ipv6 add type deny name <name> [ id <id> ] [ srcip { <ip6> | ipname <name> | any } ] [ dstip { <ip6> | ipname <name> | any } ] [ srcport <port> ] [ smac <mac> ] [ iif { any | <name> } ] [ oif { any | <name> } ] [ service { any | <name> } ] [ exhah { on | off } [ spi <string> ] [ length <string> ] [ reschk { on | off } ] ] [ exhdst { on | off } [ length <string> ] [ opt <string> ] ] [ exhfrag { on | off } [ id <string> ] [ length <string> ] [ reschk { on | off } ] [ first { on | off } ] [ moreorlast { more | last } ] ] [ exhhbh { on | off } [ length <string> ] [ opt <string> ] ] [ exhmh { on | off } [ type <string> ] ] [ exhrt { on | off } [ type <string> ] [ segsleft <string> ] [ length <string> ] ] [ exhesp { on | off } [ spi <string> ] ] [ active { on | off } ] [ log { on | off } ] [ comment <comment> [time {none | <name>}]

**关键参数说明：同上**

## 修改安全策略：

**语法：**

rule ipv6 set id <id> [ type { permit | deny } ] [ name <name> ] [ newid <id> ] [ srcip { <ip6> | ipname <name> | any } ] [ dstip { <ip6> | ipname <name> | any } ] [ srcport <port> ] [ smac <mac> ] [ iif { any | <name> } ] [ oif { any | <name> } ] [ service { any | <name> } ] [ avpolicy <id> ] [ ipspolicy <id> ] [ pcpolicy <id> ] [ eimpolicy <id> ] [ exhah { on | off } [ spi <string> ] [ length <string> ] [ reschk { on | off } ] ] [ exhdst { on | off } [ length <string> ] [ opt <string> ] ] [ exhfrag { on | off } [ id <string> ] [ length <string> ] [ reschk { on | off } ] [ first { on | off } ] [ moreorlast { more | last } ] ] [ exhhbh { on | off } [ length <string> ] [ opt <string> ] ] [ exhmh { on | off } [ type <string> ] ] [ exhrt { on | off } [ type <string> ] [ segsleft <string> ] [ length <string> ] ] [ exhesp { on | off } [ spi <string> ] ] [ active { on | off } ] [ log { on | off } ] [ comment <comment> [time {none | <name>}]

**关键参数说明：同上**

## 删除安全策略：

**语法：**

rule ipv6 del { id <id> | all }

## 显示安全策略：

**语法：**

rule ipv6 show [ id <id> ]

# 13.1.3 静态路由（ipv6）

## 添加 ipv6 路由到路由表

**语法：**

route ipv6 troute add destip <net_ip6> dev <name> metric <number> [nexthop <single_ip6>]

**参数说明：**

| | |
|---|---|
| destip | 设置目的 IP 地址，可以使用单个 IP 地址、IP 地址/子网掩码长度 |
| dev | 流出接口名称 |
| nexthop | 设置下一跳网关的 IP 地址 |
| metric | 路由开销值 |

**注意事项：**

下一跳的 IP 地址必须与流出接口在同一网段

**示例：**

```
ac> route ipv6 troute add destip 9e80::290:bff:fe19:6406/64 dev eth0 metric 10 nexthop
9e80::290:bff:fe19:6408
```

## 编辑 ipv6 路由表中的路由：

**语法：**

route ipv6 troute set id <number> destip <net_ip6> dev <name> metric <number> [nexthop <single_ip6>]

**参数说明：**

| | |
|---|---|
| id | 路由 ID |
| destip | 设置目的 IP 地址，可以使用单个 IP 地址、IP 地址/子网掩码长度 |
| dev | 流出接口名称 |
| metric | 路由开销值 |
| nexthop | 设置下一跳网关的 IP 地址 |

**注意事项：**

下一跳的 IP 地址必须与流出接口在同一网段

**示例：**

```
ac> route ipv6 troute set id 2 destip 9e80::290:bff:fe19:6406/64 dev eth0 metric 120
nexthop 9e80::290:bff:fe19:6408
```

## 删除 ipv6 路由表中的路由：

**语法：**

route ipv6 troute del id <number>

**参数说明：**

| | |
|---|---|
| id | 路由 ID |

**注意事项：**

无

**示例：**

```
ac>route ipv6 troute del id 2
```

## 显示 ipv6 所有路由：

**语法：**

route ipv6 show

**参数说明：**

无

**注意事项：**

无

**示例：**

```
ac> route ipv6 troute show

route6 list

     Destination IP             Gateway          Interface  Metric  Active  Effect  ID
9E80::0290:0BFF:FE19:6400/64    9E80::0290:0BFF:FE19:6402     eth0       1       1       1
1
```

# 13.1.4 动态路由管理(advroute)

## 添加 RIPng 端口：

**语法：**

advroute add ripng port <name> active { on | off } passive { on | off }

**关键参数说明：**

| 元素名 | 描述 | 类型与值范围 | 缺省值 |
|---|---|---|---|
| name | 已启用的端口名称，如 eth0 | CHAR(20) | |
| active | 在该端口是使能或禁止 ripng 协议<br>0：off<br>1：on | BOOL (0,1) | |
| passive | 阻止接口的 RIPng 广播<br>0：off<br>1：on | BOOL (0,1) | |

## 删除 RIPng 端口：

**语法：**

advroute del ripng port <name>

## 设置 RIPng 全局参数：

**语法：**

advroute set ripng [ active { on | off } ] [ ospfv3 { on [ ospfv3_metric <number> ] | off } ][ connected { on [ connected_metric <number> ] | off } ][ static { on [ static_metric <number> ] | off } ][ kernel { on [ kernel_metric <number> ] | off } ][ bgp { on [ bgp_metric <number> ] | off } ][ defgw { on | off } ] [ update <number> ][ holddown <number> ] [ garbage <number> ]

**关键参数说明：**

| 元素名 | 描述 | 类型与值范围 | 缺省值 |
|---|---|---|---|
| active | 启停 RIPng 协议<br>0：off<br>1：on | BOOL (0,1) | off |
| ospfv3 | RIPng 重发布 OSPFv3<br>0：off<br>1：on | BOOL (0,1) | off |
| ospfv3_metric | RIPng 重发布 OSPFv3 的 metric 值 | INT (0,16) | 0 |
| connected | RIPng 重发布 connected<br>0：off<br>1：on | BOOL (0,1) | off |
| connected_metric | RIPng 重发布 connected 的 metric 值 | INT (0,16) | 0 |
| static | RIPng 重发布 static<br>0：off<br>1：on | BOOL (0,1) | off |
| static_metric | RIPng 重发布 static 的 metric 值 | INT (0,16) | 0 |
| bgp | RIPng 重发布 bgp<br>0：off<br>1：on | BOOL (0,1) | off |
| bgp_metric | RIPng 重发布 bgp 的 metric 值 | INT (0,16) | 0 |
| kernel | RIPng 重发布 kernel<br>0：off<br>1：on | BOOL (0,1) | off |
| kernel_metric | RIPng 重发布 kernel 的 metric 值 | INT (0,16) | 0 |
| defgw | RIPng 重发布缺省路由<br>0：off<br>1：on | BOOL (0,1) | off |
| update_timer | 发送路由更新的时间间隔<br>单位：秒 | INT (5-65535) | 30 |
| holddown_timer | 路由老化时间。如果在老化时间内没有收到关于某条路由的更新报文，则该条路由在路由表中的度量值将会被设置为 16。单位：秒 | INT (5-65535) | 180 |
| garbage_timer | 一条路由从度量值变为 16 开始，直到它从路由表里被删除所经过的时间。在 garbage_timer 时间内 RIPng 以 16 作为度量值向外发送这条路由的更新，如果 garbage_timer 超时，该路由仍没有 | INT (5-65535) | 120 |

| | | | |
|---|---|---|---|
| | 得到更新，则该路由将从路由表中被彻底删除。<br>单位：秒 | | |

## 显示 RIPng 路由表：

**语法：**

advroute show ripng route

## 设置 OSPFv3 路由重发布：

**语法：**

advroute set ospfv3 [connected { on | off } ] [static { on | off } ] [ ripng { on | off } ][ bgp {on | off } ] [kernel { on | off } ]

**关键参数说明：**

| 元素名 | 描述 | 类型与值范围 | 缺省值 |
|---|---|---|---|
| router_id | 每一个 OSPFv3 进程必须存在自己的路由器 ID，可以在一个自治系统中唯一的标识一台路由器。 | CHAR(15)，一般以 32 位无符号整数或 IP 地址表示 | 0.0.0.1 |
| connected | OSPFv3 重发布 connected<br>0：off<br>1：on | BOOL (0,1) | off |
| static | OSPFv3 重发布 static<br>0：off<br>1：on | BOOL (0,1) | off |
| kernel | OSPFv3 重发布 kernel<br>0：off<br>1：on | BOOL (0,1) | off |
| ripng | OSPFv3 重发布 ripng<br>0：off<br>1：on | BOOL (0,1) | off |
| bgp | OSPFv3 重发布 bgp<br>0：off<br>1：on | BOOL (0,1) | off |

## 启停 OSPFv3 路由：

**语法：**

advroute set ospfv3 [ routerid <ipv4> ] [ active { on | off } ]

**关键参数说明：**

| 元素名 | 描述 | 类型与值范围 | 缺省值 |
|---|---|---|---|
| router_id | 每一个 OSPFv3 进程必须存在自己的路由器 ID，可以在一个自治系统中唯一的标识一台路由器。 | CHAR(15)，一般以 32 位无符号整数或 IP 地址表示 | 0.0.0.1 |
| active | 启停 OSPFv3 协议<br>0：off<br>1：on | BOOL (0,1) | off |

## 添加 OSPFv3 区域：

**语法：**

advroute add ospfv3 port <ifname> area <ipv4>

**关键参数说明：**

| 元素名 | 描述 | 类型与值范围 | 缺省值 |
|---|---|---|---|
| ifname | 已启用的接口名称 | CHAR(20) | |
| area | 区域是从逻辑上将路由器划分为不同的组，每个组用区域号（Area ID）来标识。Area id = 0,为骨干区域 | CHAR(15)，一般以 32 位无符号整数或 IP 地址表示 | |

## 删除 OSPFv3 区域：

**语法：**

advroute del ospfv3 port <ifname> area <ipv4>

## 显示 OSPFv3 路由：

**语法：**

advroute show ospfv3 route

# 13.1.5 tunnel ipv6-to-ipv4 隧道（Tunnel）

## 添加 tun6to4 隧道：

**语法：**

**tunnel ipv6 add tun6to4 ttl <number> local <ipv4-address> addr6 <ipv6-address>**

**参数说明：**

Ttl 1~255 跳

Local 物理网口地址

Addr6 虚拟接口 tun6to4 的 ipv6 地址

**注意事项：**

Addr6 参数配置的 ipv6 地址：前面 48 个字节组成为“2002”+“本地网口（local 参数地址）”地址组成。Local 参数为正在启用的物理网口地址，工作模式为路由模式，且没有工作在 HA 上。

**示例：**

无

## 设置 tun6to4 隧道：

**语法：**

**#tunnel ipv6 set tun6to4 ttl <number> local <ipv4-address> addr6 <ipv6-address>**

**参数说明：**

同“添加 tun6to4 隧道”

**注意事项：**
同“添加 tun6to4 隧道”

**示例：**
无

## 启动 tun6to4 隧道：

**语法：**
**tunnel ipv6 set tun6to4 active on**
**参数说明：**
无

**注意事项：**
无

**示例：**
无

## 停止 tun6to4 隧道：

**语法：**
**tunnel ipv6 set tun6to4 active off**
**参数说明：**
无

**注意事项：**
无

**示例：**
无

## 重启 tun6to4 隧道：

**语法：**
**tunnel ipv6 set  tun6to4 restart**
**参数说明：**
无

**注意事项：**
无

**示例：**
无

## 删除 tun6to4 隧道：

**语法：**
**tunnel ipv6 del tun6to4**
**参数说明：**
无

**注意事项：**
无

**示例：**
无

## 显示 tun6to4 隧道：

**语法：**
**Tunnel ipv6 show tun6to4**
**参数说明：**
无

**注意事项：**
无

**示例：**
Ac> tunnel ipv6 show tun6to4
命令：6to4 隧道版本号:1.0

端口 隧道名字 运行状态 生存时间 模式 ipv6 地址 目的地址 源 ip4 地址
eth0 tun6to4 1 64 sit 2002:ca6a:3201:2::1/64 any 202.106.50.1

# 13.1.6 NAT-PT 网络协议转换-地址转换（NATPT）

## 配置前缀：

**语法：**

interface ipv6 set nat prefix *prefix*::/96

**参数说明：**

Prefix ipv6 地址

**注意事项：**

Prefix 参数地址前缀必须为 96

**示例：**

无

## 删除前缀：

**语法：**

interface ipv6 del nat prefix *prefix*::/96

**参数说明：**

同“配置前缀”

**注意事项：**

同“配置前缀”

**示例：**

无

## 添加静态地址池：

**语法：**

interface ipv6 add nat static { 4to6 | 6to4 } <ip>

**参数说明：**

static 4to6 或者 6to4 方式

ip 参数依次为 Ipv4-address 和 Ipv6-address。

**注意事项：**

参数 ip 地址格式为 <ipv4-address ipv6-address>；

**示例：**

ac> interface ipv6 add nat static 6to4 1.1.1.1 2001:1::1

## 设置静态地址池：

**语法：**

**interface ipv6 set nat static id <id> {6to4 | 4to6} <ip>**

**参数说明：**

Id 修改静态地址池行号

**注意事项：**

无

**示例：**
无

## 删除静态地址池：

**语法：**
interface ipv6 del nat static {id <id> | all }
**参数说明：**
Id 删除静态地址池的行号或者清空静态地址池( “all”)

**注意事项：**
无

**示例：**
无

## 添加动态地址池：

**语法：**
interface ipv6 add nat dynamic <ip-ip:port-port> if <name>}
**参数说明：**
Dynamic 参数地址段：端口段
If 正在启用的物理网口且工作在路由模式下。
**注意事项：**
地址段和端口段之间使用“：”分割，段区间使用“-”分割。地址段前面地址小于后面的地址，端口段前面的端口号小于后面的端口号

**示例：**
无

## 设置动态地址池：

**语法：**
interface ipv6 set nat dynamic id <id> <ip-ip:port-port> if <name>
**参数说明：**
Id 修改动态地址池行号
<ip-ip:port-port> ip 地址区间，需要前 ip 地址小于后面的 ip 地址，端口行相等或者前面的端口小于后面的端口。或者是 port 端口都等于 0，表示随机端口号。
<name> 必须是启用的工作在路由模式下的物理网口。

**注意事项：**

**示例：**

无

## 删除动态地址池：

**语法：**

interface ipv6 del nat dynamic {id <id> | all }

**参数说明：**

Id 删除动态地址池的行号或者清空动态地址池( “all”)

**注意事项：**

无

**示例：**

无

## 显示 nat-pt：

**语法：**

interface ipv6 show nat {prefix | static | dynamic }

**参数说明：**

Nat 分别显示 prefix（前缀）、static（静态地址池）、dynamic（动态地址池）

**注意事项：**

无

**示例：**

```
Ac> interface ipv6 show nat prefix
 natpt 前缀 :  1::/96
```

# 13.26456 IPv6 资源

## 13.26456.1 IPv6 地址（address6）：

### 添加地址定义：

**语法：**

address6 add name <name> ip <ip> [ comment <comment> ]

**参数说明：**

| | |
|---|---|
| name | 设置地址定义的名字 |
| ip | 设置 IPv6 地址，可以使用单个 IP v6 地址、IP v6 地址/子网前缀长度、IP v6 地址段、或反 IP v6 地址/子网前缀长度 |
| comment | 设置地址定义的注释，可选参数，默认为空 |

**注意事项：**

ip 地址段的格式为：ip1:ip2 如：1:1:1::1~1:1:1::3

ip 地址/子网掩码格式为：ip1/prefix 如：1:1:1::1/64

反 ip 地址/子网掩码格式为：ip1@ prefix 如：1:1:1::1@64

**示例：**

```
ac>address6 add name a1 ip 1:1:1::1/128 comment “IPv6 address 1”
```

## 修改地址定义：

**语法：**

address6 set name <name> { [ ip <ip> ] [ comment <comment> ] }

**参数说明：**

| | |
|---|---|
| name | 指定欲修改的地址定义的名字 |
| ip | 修改 IPv6 地址，可以使用单个 IP v6 地址、IP v6 地址/子网前缀长度、IP v6 地址段、或反 IP v6 地址/子网前缀长度 |
| comment | 修改地址定义的注释 |

**注意事项：**

无

**示例：**

```
ac>address6 set name a1 ip 1:1:1::1@128 comment “new IPv6 address 1”
```

## 删除地址定义：

**语法：**

address6 del name <name>

**参数说明：**

| | |
|---|---|
| name | 指定欲删除的地址定义的名字 |

**注意事项：**
不能删除被安全规则或用户、用户组引用的地址定义，也不能删除作为地址组的成员的地址定义。

**示例：**
```
ac>address6 del name a1
```

## 显示所有地址定义：

**语法：**
address6 show

**参数说明：**
无

**注意事项：**
仅显示地址定义的部分内容。

**示例：**
```
ac>address6 show
Name                    IP6_Address
any                     ::/128
a1                    ! 1:1:1::1/128
```

## 显示指定名字的地址定义：

**语法：**
address6 show name <name>

**参数说明：**
name　　指定欲显示的地址定义的名字

**注意事项：**
无

**示例：**
```
ac>address6 show name a1
Name: a1
IP6 Address: ! 1:1:1::1/128
Comment: new IPv6 address 1
```

## 13.26456.2 IPv6 地址组（addrgrp6）

### 添加地址组定义：

**语法：**
addrgrp6 add name <name> [ comment <comment> ]

**参数说明：**
name 设置地址组定义的名字
comment 设置地址组定义的注释，可选参数，默认为空

**注意事项：**
无

**示例：**
ac> addrgrp6 add name ag1 comment “address group 1”

### 修改地址组定义：

**语法：**
addrgrp6 set name <name> comment <comment>

**参数说明：**
name 指定欲修改的地址组定义的名字
comment 修改地址组定义的注释

**注意事项：**
无

**示例：**
ac> addrgrp6 set name ag1 comment “new address group 1”

### 向地址组添加成员：

**语法：**
addrgrp6 set name <name> addmbr <name>+

**参数说明：**
name 指定欲添加成员的地址组定义的名字

addmbr 指定一个或多个地址定义的名字，将它们添加到地址组中

**注意事项：**
地址组定义的成员只能是地址定义，不能是其它地址组定义。

**示例：**
ac> addrgrp6 set name ag1 addmbr a1 a2 a3

## 从地址组删除成员：

**语法：**
addrgrp6 set name <name> delmbr <name>+

**参数说明：**
name 指定欲删除成员的地址组定义的名字
delmbr 指定一个或多个地址定义的名字，将它们从地址组中删除

**注意事项：**
无

**示例：**
ac> addrgrp6 set name ag1 delmbr a1 a2 a3

## 删除地址组定义：

**语法：**
addrgrp6 del name <name>

**参数说明：**
name 指定欲删除的地址组定义的名字

**注意事项：**
不能删除被安全规则或用户、用户组引用的地址组定义。

**示例：**
ac> addrgrp6 del name ag1

## 显示所有地址组定义：

**语法：**
addrgrp6 show [ name <name> ]

**参数说明：**

name 地址组的成员

**注意事项：**

仅显示地址组定义的部分内容。

**示例：**

```
ac>addrgrp6 show
Name                    Member
ag1                     a1
                        a2
                        a3
```

## 显示指定名字的地址组定义：

**语法：**

addrgrp6 show name <name>

**参数说明：**

name 指定欲显示的地址组定义的名字

**注意事项：**

无

**示例：**

```
ac>addrgrp6 show name ag1
Name: ag1
Member: a1
        a2
        a3
Comment: address group 1
```

### 13.26456.3 IPv6 服务器地址（serveraddr6）

## 添加服务器地址定义：

**语法：**

serveraddr6 add name <name> ip <ip> [ ip <ip> [ ip <ip> [ ip <ip> [ ip <ip> [ ip <ip> [ ip <ip> [ ip <ip> ] ] ] ] ] ] ] [ comment <comment> ]

**参数说明：**

| | |
|---|---|
| name | 设置服务器地址定义的名字 |
| ip | 设置服务器 1 的 IP 地址，仅能使用单个 IP 地址 |
| ip | 设置服务器 2 的 IP 地址，仅能使用单个 IP 地址，可选参数，默认为空 |
| ip | 设置服务器 3 的 IP 地址，仅能使用单个 IP 地址，可选参数，默认为空 |
| ip | 设置服务器 4 的 IP 地址，仅能使用单个 IP 地址，可选参数，默认为空 |
| ip | 设置服务器 5 的 IP 地址，仅能使用单个 IP 地址，可选参数，默认为空 |
| ip | 设置服务器 6 的 IP 地址，仅能使用单个 IP 地址，可选参数，默认为空 |
| ip | 设置服务器 7 的 IP 地址，仅能使用单个 IP 地址，可选参数，默认为空 |
| ip | 设置服务器 8 的 IP 地址，仅能使用单个 IP 地址，可选参数，默认为空 |
| comment | 设置服务器地址定义的注释，可选参数，默认为空 |

**注意事项：**

无

**示例：**

```
ac>serveraddr6 add name sa1 ip 1:1:1::1 ip 2:2:2::2 comment “server address 1”
```

## 修改服务器地址定义：

**语法：**

serveraddr6 set name <name> { [ ip <ip> [ ip <ip> [ ip <ip> [ ip <ip> [ ip <ip> [ ip <ip> [ ip <ip> [ ip <ip> ] ] ] ] ] ] ] ] [ comment <comment> ] }

**参数说明：**

| | |
|---|---|
| name | 指定欲修改的服务器地址定义的名字 |
| ip | 设置服务器 1 的 IP 地址，仅能使用单个 IP 地址 |
| ip | 设置服务器 2 的 IP 地址，仅能使用单个 IP 地址，可选参数，默认为空 |
| ip | 设置服务器 3 的 IP 地址，仅能使用单个 IP 地址，可选参数，默认为空 |
| ip | 设置服务器 4 的 IP 地址，仅能使用单个 IP 地址，可选参数，默认为空 |
| ip | 设置服务器 5 的 IP 地址，仅能使用单个 IP 地址，可选参数，默认为空 |
| ip | 设置服务器 6 的 IP 地址，仅能使用单个 IP 地址，可选参数，默认为空 |
| ip | 设置服务器 7 的 IP 地址，仅能使用单个 IP 地址，可选参数，默认为空 |
| ip | 设置服务器 8 的 IP 地址，仅能使用单个 IP 地址，可选参数，默认为空 |
| comment | 修改服务器地址定义的注释 |

**注意事项：**

无

**示例：**

```
ac>serveraddr6 set name sa1 ip 1:1:1::3 ip 3:3:3::3 comment “new server address 1”
```

## 删除服务器地址定义：

**语法：**
Serveraddr6 del name <name>

**参数说明：**
name 指定欲删除的服务器地址定义的名字

**注意事项：**
不能删除被安全规则引用的服务器地址定义。

**示例：**
```
ac>serveraddr6 del name sa1
```

## 显示所有服务器地址定义：

**语法：**
Serveraddr6 show

**参数说明：**
无

**注意事项：**
仅能显示服务器地址定义的部分内容。

**示例：**
```
ac>serveraddr6 show
Name                    IP_Address
sa1                     1:1:1::3
                        3:3:3::3
```

## 显示指定名字的服务器地址定义：

**语法：**
Serveraddr6 show name <name>

**参数说明：**
name 指定欲显示的服务器地址定义的名字

**注意事项：**
无

**示例：**

```
ac>serveraddr6 show name sa1
Name: sa1
IP Address 1: 1:1:1::3
IP Address 2: 3:3:3::3
Comment: server address 1
```

### 13.26456.4 IPv6 服务组（Servgrp6）

## 添加服务组定义：

**语法：**

servgrp6 add name <name> [ comment <comment> ]

**参数说明：**

| | |
|---|---|
| name | 设置服务组定义的名字 |
| comment | 设置服务组定义的注释，可选参数，默认为空 |

**注意事项：**

无

**示例：**

```
ac>servgrp6 add name sg1 comment “service group 1”
```

## 修改服务组定义：

**语法：**

servgrp6 set name <name> comment <comment>

**参数说明：**

| | |
|---|---|
| name | 指定欲修改的服务组定义的名字 |
| comment | 修改服务组定义的注释 |

**注意事项：**

无

**示例：**

```
ac>servgrp6 set name sg1 comment “new service group 1”
```

## 向服务组添加成员：

**语法：**
servgrp6 set name <name> addmbr <name>+

**参数说明：**
name 指定欲添加成员的服务组定义的名字
addmbr 指定一个或多个服务定义的名字，将它们添加到服务组中

**注意事项：**
服务组定义的成员只能是服务定义，不能是其它服务组定义。

**示例：**
```
ac>servgrp6 set name sg1 addmbr s1 s2 s3
```

## 从服务组删除成员：

**语法：**
servgrp6 set name <name> delmbr <name>+

**参数说明：**
name 指定欲删除成员的服务组定义的名字
delmbr 指定一个或多个服务定义的名字，将它们从服务组中删除

**注意事项：**
无

**示例：**
```
ac>servgrp6 set name sg1 delmbr s1 s2 s3
```

## 删除服务组定义：

**语法：**
servgrp6 del name <name>

**参数说明：**
name 指定欲删除的服务组定义的名字

**注意事项：**
不能删除被安全规则或用户、用户组引用的服务组定义。

**示例：**

```
ac>servgrp6 del name ag1
```

## 显示所有服务组定义：

**语法：**

servgrp6 show

**参数说明：**

无

**注意事项：**

仅显示服务组定义的部分内容。

**示例：**

```
ac>servgrp6 show
Name                    Member
sg1                     s1
                        s2
                        s3
```

## 显示指定名字的服务组定义：

**语法：**

servgrp6 show name <name>

**参数说明：**

| | |
|---|---|
| name | 指定欲显示的服务组定义的名字 |

**注意事项：**

无

**示例：**

```
ac>servgrp6 show name sg1
Name: sg1
Member: s1
        s2
        s3
Comment: service group 1
```

# 第14章 漏洞扫描

## 14.1 定时漏洞扫描

### 添加定时漏洞扫描任务：

**语法：**

nscanner add type <type> time <time> name <taskname> dip <ip_name> plugin_set <plugin_set> host_num <host_num> comment <comment> active {on | off}

**参数说明：**

type： 扫描类型，1:循环扫描，0:只扫描一次
time： 定时扫描时间
name： 定时扫描任务名称
dip： 定时扫描目的地址
plugin_set： 插件类型
host_num： 并发主机扫描数，数值在 1~15 之间
comment： 定时扫描任务备注
active： 定时扫描任务是否启用

**注意事项：**

无

**示例：**

ac>nscanner add type 1 time “00 10 * * 1” name scantask1 dip somedip1 plugin_set 3 host_num 10 comment “scantask1comment” active on

### 修改定时漏洞扫描任务：

**语法：**

nscanner edit type <type> time <time> name <taskname> dip <ip_name> plugin_set <plugin_set> host_num <host_num> comment <comment> active { on | off }

**参数说明：**

type： 扫描类型，1:循环扫描，0:只扫描一次
time： 定时扫描时间
name： 定时扫描任务名称
dip： 定时扫描目的地址

plugin_set： 插件类型
host_num： 并发主机扫描数，数值在 1~15 之间
comment： 定时扫描任务备注
active： 定时扫描任务是否启用

**注意事项：**
无

**示例：**
ac>nscanner edit type 1 time “00 10 * * 1” name scantask1 dip somedip1 plugin_set 324 host_num 5 comment “scantask1comment” active on

## 开启关闭定时漏洞扫描任务：

**语法：**
nscanner enable name <taskname>
nscanner disable name <taskname>

**参数说明：**
name：定时扫描任务名称

**注意事项：**
无

**示例：**
ac>nscanner enable name scantask1
ac>nscanner disable name scantask1

## 查看定时漏洞扫描任务：

**语法：**
nscanner show

**参数说明：**
无

**示例：**
ac>nscanner show

## 删除定时扫描任务：

**语法：**
nscanner del name <taskname>

**参数说明：**

name：定时扫描任务名称

**注意事项：**
无

**示例：**
ac>nscanner del name scantask1

# 14.2 手动漏洞扫描

## 配置并开始手动漏洞扫描：

**语法：**
nscanner dip <ip_name> resultfile <taskname> plugin_set <plugin_set> host_num <num>

**参数说明：**
dip： 手动扫描的目的地址
resultfile： 保存扫描结果的文件名
plugin_set： 插件类型
host_num： 并发主机扫描数

**注意事项：**
无

**示例：**
ac>nscanner dip somedip1 resultfile /path/filename plugin_set 3 host_num 10

## 停止手动漏洞扫描：

**语法：**
nscanner scan stoptask

**参数说明：**
无

**注意事项：**
无

**示例：**
ac>nscanner scan stoptask

# 第15章 状态监控

## 15.1 网络调试工具

### 15.1.1 ping

**检测一帧数据从当前主机传送到目的主机所需要的时间：**

**语法：**
ping { <single_ip> | <hostname> }

**参数说明：**

| | |
|---|---|
| <single_ip> | 单个 IP 地址 |
| hostname | 主机名称 |

**注意事项：**
无

**示例：**

```
ac>ping 10.50.10.130
PING 10.50.10.130 (10.50.10.130) from 10.50.10.122 : 56(84) bytes of data.
64 bytes from 10.50.10.130: icmp_seq=1 ttl=128 time=2.49 ms
64 bytes from 10.50.10.130: icmp_seq=2 ttl=128 time=1.26 ms
64 bytes from 10.50.10.130: icmp_seq=3 ttl=128 time=1.89 ms
64 bytes from 10.50.10.130: icmp_seq=4 ttl=128 time=1.77 ms
64 bytes from 10.50.10.130: icmp_seq=5 ttl=128 time=5.79 ms

--- 10.50.10.130 ping statistics ---
5 packets transmitted, 5 received, 0% loss, time 4046ms
rtt min/avg/max/mdev = 1.262/2.643/5.798/1.625 ms
```

## 15.1.2 traceroute

### 判定数据包到达目的主机所经过的路径

**语法：**

traceroute { <single_ip> | <hostname> }

**参数说明：**

| | |
|---|---|
| <single_ip> | 单个 IP 地址 |
| hostname | 主机名称 |

**注意事项：**

无

**示例：**

```
ac>traceroute 10.50.10.130
```

## 15.1.3 tcpdump

### 检测经过安全网关的数据包

**语法：**

tcpdump <ifname>

**参数说明：**

| | |
|---|---|
| <ifname> | 检测的网络接口。 |

**注意事项：**

无

**示例：**

```
ac>tcpdump eth0
```

## 15.1.4 arp

### 检查安全网关所能得到的硬件地址

**语法：**

arp

**参数说明：**

无

**注意事项：**

**无**

**示例：**

```
ac>arp
  Address       HWtype  HWaddress          Flags Mask    Iface
  10.50.10.175  ether   00:11:5B:13:4F:59  C             eth0
```

## 15.1.5 routeshow

### 检查各种路由信息

**语法：**

routeshow

**参数说明：**

无

**注意事项：**

无

**示例：**

```
ac>route show
static route
Destination     Gateway         Genmask         Iface
7.7.7.0         0.0.0.0         255.255.255.0   eth7
5.5.5.0         0.0.0.0         255.255.255.0   eth5
2.2.2.0         0.0.0.0         255.255.255.0   eth2
10.1.4.0        0.0.0.0         255.255.255.0   brg0
10.1.5.0        0.0.0.0         255.255.255.0   eth0
6.6.6.0         0.0.0.0         255.255.255.0   eth6
1.1.1.0         0.0.0.0         255.255.255.0   eth1
4.4.4.0         0.0.0.0         255.255.255.0   eth4
3.3.3.0         0.0.0.0         255.255.255.0   eth3
```

## 15.1.6 gwarp

### 让对端学到安全网关的 MAC 地址

**语法：**

gwarp interface <name> { ethdstmac <mac> ethsrcmac <mac> arpop { request | reply } arpdstaddr <single_ip> arpsrcaddr <single_ip> arpsrcmac <mac> [ repeat <number> ] [ change ] | [ arpop { request | reply } ] arpdstaddr <single_ip> }

**参数说明：**

| | |
|---|---|
| gwarp | 发送 arp 数据包 |
| interface | 设置输出网口 |
| ethdstmac | 以太包中目的 mac 地址 |
| ethsrcmac | 以太包中源 mac 地址 |
| arpop | arp 报文类型 |
| arpdstaddr | arp 报文中目的 ip 地址 |
| arpsrcaddr | arp 报文中源 ip 地址 |
| arpsrcmac | arp 报文中源 mac 地址 |
| repeat | 发送报文的次数 |
| change | arp 报文中源 ip 地址和 mac 地址随机变化 |

**注意事项：**

无

**示例：**

```
ac>gwarp interface eth0 arpop request arpdstaddr 172.168.1.1
```

# 第16章 日志与报警

## 16.1 日志信息（log）

### 显示所有日志：

**语法：**

log show

**参数说明：**

无

**注意事项：**

无

**示例：**

```
ac>log show
Date                    Type            Priority    Contents
2004/01/01  09:00:00       Management           notice          mod=fwip  act=add  if=ge1
ip=192.168.1.1 netmask=255.255.255.0 result=0
2004/01/01  09:01:00       Management           notice          mod=fwip  act=add  if=ge2
ip=192.168.2.1 netmask=255.255.255.0 result=0
```

## 显示指定类型的日志：

**语法：**

log show type { 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 }

**参数说明：**

| | |
|---|---|
| type | 指定欲显示的日志类型<br>1：包过滤日志<br>2：代理日志<br>3：IDS 日志<br>4：VPN 日志<br>5：用户认证日志<br>6：内容过滤日志<br>7：保留<br>8：设备状态日志<br>9：设备管理日志<br>10：集群日志<br>11：扩展日志 |

**注意事项：**

无

**示例：**

```
ac>log show type 9
Date                    Type            Priority    Contents
2004/01/01  09:00:00       Management           notice          mod=fwip  act=add  if=ge1
ip=192.168.1.1 netmask=255.255.255.0 result=0
2004/01/01  09:01:00       Management           notice          mod=fwip  act=add  if=ge2
ip=192.168.2.1 netmask=255.255.255.0 result=0
```

## 显示指定优先级的日志：

**语法：**

log show priority { 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 }

**参数说明：**

priority 指定欲显示的日志优先级
0：紧急事件
1：报警事件
2：危险事件
3：错误事件
4：警告事件
5：通知事件
6：消息事件
7：调试事件

**注意事项：**

无

**示例：**

```
ac>log show priority 5
Date                    Type             Priority     Contents
2004/01/01  09:00:00       Management            notice           mod=fwip  act=add  if=ge1
ip=192.168.1.1 netmask=255.255.255.0 result=0
2004/01/01  09:01:00       Management            notice           mod=fwip  act=add  if=ge2
ip=192.168.2.1 netmask=255.255.255.0 result=0
```

## 清除日志：

**语法：**

log clean

**参数说明：**

无

**注意事项：**

仅清除安全网关上的日志。

**示例：**

```
ac>log clean
```

# 16.2 日志服务器（logserver）

## 设置日志服务器：

**语法：**

**logserver set ip <ip> port <port> [ protocol udp ]**

**参数说明：**

| | |
|---|---|
| ip | 设置日志服务器的 IP 地址 |
| port | 设置日志服务器的端口 |
| protocol | 设置发送日志使用的协议，默认为 UDP |

**注意事项：**

无

**示例：**

ac> logserver set ip 192.168.100.1 port 514 protocol udp

## 清除日志服务器：

**语法：**

**logserver unset**

**参数说明：**

无

**注意事项：**

无

**示例：**

ac> logserver unset

## 显示日志服务器：

**语法：**

**logserver show**

**参数说明：**

无

**注意事项：**
无

**示例：**
ac> logserver show
Log Server IP: 1.1.1.1
Protocol: udp
Port: 514

# 16.3 网关邮箱（gwmail）

## 设置报警邮箱参数：

**语法：**
gwmail set sender <email> [receiver <email1,email2,email3> smtp <smtp name> port <port> password <password> log <on/off>]

**参数说明：**

| | |
|---|---|
| sender | 设置发件人邮箱地址 |
| receiver | 设置收件人邮箱地址 |
| smtp | 设置发送邮件的 SMTP 服务器，可选参数，默认为空 |
| port | 设置 SMTP 服务器的服务端口 |
| password | 设置发件人邮箱密码 |
| log | 设置日志开关 |

**注意事项：**
设置收件人 receiver 时，最多为三个邮件地址，中间以逗号隔开，不要用空格；smtp 服务器地址可以是 ip 也可以是域名地址；当邮箱参数没有被设置时，一定要输入发件人地址，收件人地址，smtp 服务器地址，以及发件人邮箱密码；当需要对某一项已经设置好的参数进行修改的时候，只需要逐个修改即可。

**示例：**
ac>gwmail set sender infosec@lenovo.com receiver admin@lenovo.com,liping@lenovo.com,wanglin@lenovo.com smtp smtp.lenovo.com port 25 password 111111 log on

## 清除报警邮箱参数：

**语法：**

gwmail unset

**参数说明：**
无

**注意事项：**
无

**示例：**
```
ac>gwmail unset
```

## 显示报警邮箱和 SMTP 服务器：

**语法：**
gwmail show

**参数说明：**
无

**注意事项：**
由于发件人邮箱密码涉及到个人隐私，因此，并不会在此显示出来。

**示例：**
```
ac>gwmail show
Mail Sender: infosec@lenovo.com
Mail Receiver1: admin@lenovo.com
Mail Receiver2: liping@lenovo.com
Mail Receiver3: wanglin@lenovo.com
SMTP Server: smtp.163.com
SMTP Port: 25
Gwmail state: on
Gwmail log: off
```

## 启用网关邮件：

**语法：**
gwmail set power on

**参数说明：**
无

**注意事项：**
无

**示例：**

ac>gwmail set power on

## 停止网关邮件：

**语法：**

gwmail set power off

**参数说明：**

无

**注意事项：**

无

**示例：**

ac> gwmail set power off

## 发送邮件：

**语法：**

gwmail send [subject <subject text> content <content text> signature <signature text> accessory <accessory name>]

**参数说明：**

| | |
|---|---|
| subject | 设置邮件主题，可选参数，默认为空 |
| content | 设置邮件内容，可选参数，默认为空 |
| signature | 设置邮件签名，可选参数，默认为空 |
| accessory | 设置邮件附件列表，可选参数，默认为空 |

**注意事项：**

各部分内容需要用引号括起来。当没有任何参数时，将发送一封空邮件到收件人邮箱中。

**示例：**

ac> gwmail send subject “error message”content “there are a error caused by NAT” signature “gateway ID 23”accessory config.log

# 16.4 设置日志存储（logset）

## 日志存储方式：

**语法：**

logset set overwrite <on/off> sendemail <on/off>

**参数说明：**

Overwrite on 日志存储空间满后采用覆盖的形式清空旧日志
Off 日志存储空间满后停止存储日志

Sendemail on 日志没有存储空间时邮件告警
Off 日志没有存储空间时不发送邮件告警

**注意事项：**

无

## 日志按级别存储：

**语法：**

logset set level [ <number> | help ]

**参数说明：**

Level 0 | 1 | 2 | 3 |...|7

**注意事项：**

无

**示例：**

```
Ac> logset set level help
请输入日志级别：0 | 1 | 2 | 3 |...|7

        ************************************************
        * 导致系统不可用的事件消息                   0  *
        * 应立即采取应对行动的事件消息               1  *
        * 达到临界条件的事件消息                     2  *
        * 一般出错事件消息                           3  *
        * 预警性提示事件消息                         4  *
        * 重要的正常事件消息                         5  *
        * 一般性的正常事件消息                       6  *
        * 调试消息                                   7  *
        ************************************************
```

## 日志按类别存储：

**语法：**

logset set type [ <module> …… | help ]

**参数说明：**

Module 类型 { [ all ] | [ packet | agent | ids | vpn | auth | virus | devstat | devmng | ha | tmvs | balanc | utm | iut | pc | apc | ips | hq | vq | url | antispam | exten] }

**注意事项：**

无

**示例：**

```
Ac> logset set type  help
    日志文件如需按类型分类存储，请输入
日志文件如需按类型分类存储，请输入
[ all ] or
[ packet | agent | vpn | auth | virus | devstat | devmng | ha | tmvs | balanc | utm | iut | pc
    | apc | ips | hq | vq | url | antispam | uids | uav | portsyn | sslvpn | exten ]
        ******************************************************
         *存储所有类型日志                              all     *
         *存储包过滤日志                                packet  *
         * 存储代理日志                                 agent   *
         * 存储 VPN 日志                                 vpn     *
         * 存储用户认证日志                             auth    *
         * 存储病毒过滤日志                             virus   *
         * 存储设备状态日志                             devstat *
         * 存储设备管理日志                             devmng  *
         * 存储 HA 日志                                  ha      *
         * 漏洞扫描日志                                 tmvs    *
         * 服务器负载均衡日志                           balanc  *
         * 统一威胁管理日志                             utm     *
         * 主动防御日志                                 iut     *
         * 协议控制日志                                 pc      *
         * 绿色上网日志                                 apc     *
         * 入侵防御日志                                 ips     *
         * 主机隔离功能日志                             hq      *
         * 病毒隔离功能日志                             vq      *
         * URL 过滤日志                                  url     *
         * 反垃圾邮件代理日志                           antispam*
         * UIDS 模式下的入侵检测日志                     uids    *
         * UIDS 模式下的病毒检测日志                     uav     *
         * 端口联动日志                                 portsyn *
         * 安全套接字层虚拟专用网日志                   sslvpn  *
         * 存储其他日志                                 exten   *
         ******************************************************
```

## 调整日志存储空间：

**语法：**

logset set space [ <number> | help ]

**参数说明：**

Space 1 | 2 | 3 |...|10 (M)

**注意事项：**

无

**示例：**

Ac> logset set space help

请输入： 1 | 2 | 3 |...|10 (M) 设置日志空间大小

## 日志 U 盘导出：

**语法：**

logset set export [ <path> | help ]

**参数说明：**

Export usb 设备挂载路径

**注意事项：**

本命令严重依赖 usbcli scan all 命令，请在使用本命令前，先执行 usbcli scan all 命令得到挂载路径。

具体请参考 usbcli 命令。

**示例：**

Ac> logset set export help

请确认防火墙正确插入 usb 设备，并执行：usbcli scan all 命令

Ac> logset set export /usbmnt/usbsdb1

# 16.5 外设存储配置

### 外设存储设置：

语法：

lcdb set [path <path>] [size <num>] [alert <num>]

参数说明：

path: 存储路径

size: 存储空间上限

alert: 当达实际存储量达到存储空间上限的（%alert）时，报警，并关闭服务

注意事项：

无

实例:

ac > lcdb set path /var/lib/mysql/ size 30 alert 90

### 启动|关闭|重启服务

语法：
lcdb {start | stop | restart}
参数说明：
start : 启动服务
stop: 关闭服务
restart: 重新启动服务
注意事项：
无

### 显示当前服务状态

语法：
lcdb show
参数说明：
show: 显示当前服务状态

注意事项：
无

### 修复数据

语法：
lcdb repair
参数说明：
repair: 修复存储过程中，出现损坏的数据
注意事项：
无

# 第17章 其他

## 17.1 显示总 cpu、各逻辑 cpu 利用率和内存利用率

**语法：**
Sysmon show
**参数说明：**

无

**注意事项：**

无

**示例：**

ac>sysmon show
cpuall : 1
cpu1 : 0
cpu2 : 22
memory : 83

# 17.2 网口联动模块

## 设置需要同步的网络端口，即相应的端口同时启用和禁用

**语法：**

端口同步配置
psyn set group <id> port <string> [action {on|off}] [decision {on|off}]
psyn set config [keepalive <number>] [recheck <number>]
启动/停止端口同步，需要指定运行同步组, 并可设置运行同步组构成.
psyn set rungroup <id> [ group <string> ] [ active {on|off} ] [startup {on|off}]
显示端口组连接状态
psyn show group <id>
显示版本和帮助信息
psyn

**参数说明：**

| | |
|---|---|
| port | string 表示可以引用的物理设备名称，如 fe1，fe2 |
| action | on 表示该组为主动组，off 表示被动组，缺省为 on |
| decision | on 表示该组为全端口决定，off 表示单端口决定，缺省为 on |
| keepalive | 检测时钟，单位秒， 指每间隔几秒检测一次连接状态 |
| recheck | 重复检测次数，以便增强检测结果准确性， 指当连接状态被检测为改变时, 进行几次验证, 验证间隔为一秒 |
| rungroup | 由两个已完成同步配置的端口组组成一个同步运行组，两组端口的状态同步的启停, 是通过配置该同步运行组的 active 选项实现的 |
| group | id 为端口组序号 |
| active | on 表示启用端口同步，off 表示停止端口同步 |
| startup | on 系统重新启动后将重新启动，off 系统重新启动后不启动，缺省为 off |

**限制说明：**

| | |
|---|---|
| rungroup id | 1≤rungroup id≤6，系统最多支持 6 个同步运行组 |
| group id | 1≤group id≤6.，1 代表端口 1 组， 2 代表端口 2 组， 系统最多支持 6 个同步组 |

port <string> string 格式是如“fe1,fe2,fe3”等设备的逻辑名，数量限制在 9 个以内
group <string> string 如“1,2”，数量限制在两个
number: 1≤keepalive≤60，0≤recheck≤10

**名词解释:**

主动组 两个组之间同步, 一个组的组状态发生改变, 另一组的组状态随之改变. 该组为主动组.

被动组 两个组之间同步, 一个组的连接状态发生改变, 不影响另一同步组的连接状态. 该组为被动组.

全端口决定 组内全部端口断开则组状态为*断开*; 组内有一个端口连接则组状态为*连接*.

单端口决定 组内任一个端口连接断开则组状态为*断开*; 当组内端口均连接则组状态为*连接*.

**示例:**

配置端口组:

psyn set group 1 port fe1 action on decision on

psyn set group 2 port fe2,fe3,fe4 action on decision off

改变端口组配置:

psyn set group 2 port fe2,fe4 action on decision off

注: 如果端口同步正在运行, 改变相关端口组配置, 需要重新启动端口同步才能生效.

配置同步属性:

psyn set config keepalive 1 recheck 0

配置同步运行组并启动:

psyn set rungroup 1 group 1,2 active on

同步状态查询:

psyn show group 1

停止同步运行组: (即停止端口组 1,2 的同步关系)

psyn set rungroup 1 active off

注: 即停止端口组 1,2 的同步关系

**注意事项:**

1 用户在启动端口同步之后, 要修改网路配置, 应停止端口同步. 否则, 可能导致用户配置失效.

2 用户在启动端口同步时, 应确信相关同步端口已处于连接状态. 否则, 端口同步不能正常启用.

# 17.3 登出

**语法:**

Exit

**参数说明:**

无

**注意事项:**

无

**示例:**

无