Hillstone
山 石 网 科

Hillstone山石网科

多核安全网关命令手册

软件版本号：StoneOS 4.5R3

www.hillstonenet.com

关于本手册

本手册为 Hillstone 山石网科多核安全网关命令手册。详细描述 StoneOS 中用到的所有命令，具体内容有命令的格式、使用方法、参数、默认值和使用实例等。

文档约定

在本手册中，StoneOS 命令语法描述使用以下约定：

- 大括弧（{ }）：指明该内容为必要元素。
- 方括弧（[ ]）：指明该内容为可选元素。
- 竖线（|）：分隔可选择的互相排斥的选项。
- **粗体**：粗体部分为命令的关键字，是命令行中不可变部分，用户必须逐字输入。
- *斜体*：斜体部分为需要用户提供值的参数。

命令实例约定：

- 命令实例中需要用户输入部分用粗体标出。
- 需要用户提供值的变量用斜体标出。
- 命令实例包括不同平台的输出，可能会有些许差别。

目录

怎样使用StoneOS CLI

CLI介绍

Hillstone 山石网科多核安全网关操作系统 StoneOS 提供一系列命令以及命令行接口（Command Line Interface），使用户能够对安全网关进行配置和管理。以下各节将介绍 StoneOS 命令行接口的使用方法及特点。

注意：使用 CLI 配置安全网关时，命令本身的关键字不区分大小写，但是，用户输入的内容区分大小写。

命令模式和提示符

StoneOS CLI 有不同级别的命令模式，一些命令只有在特定的命令模式下才可使用。例如，只有在相应的配置模式下，才可以输入并执行配置命令，这样也可以防止意外破坏已有的配置。不同的命令模式都有其相应的 CLI 提示符。

执行模式

用户进入到 CLI 时的模式是执行模式。执行模式允许用户使用其权限级别允许的所有的设置选项。该模式的提示符如下所示，包含了一个数字符号（#）：

```
hostname#
```

全局配置模式

全局配置模式允许用户修改安全网关的配置参数。用户在执行模式下，输入 `configure` 命令，可进入全局配置模式。该模式的提示符如下所示：

```
hostname(config)#
```

子模块配置模式

安全网关的不同模块功能需要在其对应的命令行子模块模式下进行配置。用户在全局配置模式输入特定的命令可以进入相应的子模块配置模式。例如，运行 `interface ethernet0/0` 命令进入 ethernet0/0 接口配置模式，此时的提示符变更为：

```
hostname(config-if-eth0/0)#
```

CLI命令模式切换

用户登录到安全网关就进入到 CLI 的执行模式。用户可以通过不同的命令在各种命令模式之间进行切换。表 1 列出 CLI 的模式切换命令：

模式	命令
执行模式到全局配置模式	configure
全局配置模式到子模块配置模式	不同功能使用不同的命令进入各自的命令配置模式。
退回到上一级命令模式	exit
从任何模式退回到执行模式	end

表 1：CLI 模式切换命令

命令行错误信息提示

StoneOS CLI 具有命令语法检查功能，只有通过了 CLI 语法的检查的命令能够正确执行。对于不能通过 CLI 语法检查的命令，StoneOS 会输出错误信息提示。常见的错误信息如表 2 所示：

提示信息	描述
Unrecognized command	StoneOS 找不到输入的命令或者关键字。
	输入的参数类型错误。
	输入的参数值越界。
Incomplete command	输入的命令不完整。
Ambiguous command	输入的参数不明确。

表 2：命令行常见错误信息

命令行的输入

为简化用户的输入操作，用户可以使用命令的缩写形式进行配置，除此之外，StoneOS CLI 还提供自动列出命令关键字和自动补齐命令功能。

命令行的缩写形式

命令的缩写形式一般是由命令中的几个独特字符组成。大部分 StoneOS 命令都有缩写形式。例如，用户可以仅输入 sho in 来查看设备的接口配置信息，而不用输入 show interface；仅输入 conf 就可进入全局配置模式。

自动列出命令关键字

StoneOS CLI 具有输入问号（？）列出命令关键字的功能。具体包括以下两种情况：

- 在一个或一组有效字符后输入问号，CLI 将自动列出以这个或该组字母开头的可用命令（包括命令功能的简短介绍）或者该有效字符后可以输入参数值。
- 如果直接输入问号，CLI 将列出所在模式下所有的可用命令和命令的简短介绍。

自动补齐命令关键字

StoneOS CLI 支持 TAB 键补齐命令关键字的功能。在部分字符后按 TAB 键，以该字符开头的命令会被自动补齐。但是，该自动补齐功能仅在只有唯一命令匹配时有效。例如，在执行模式下输入“conf”后点 TAB 键，系统会自动将命令补齐为“configure”。

命令行的编辑

StoneOS 命令行的编辑操作简单，主要包括以下几方面：

查看历史命令

StoneOS CLI 可记录最近输入的 64 条命令，用户可以通过上、下键或快捷键 Ctrl+P、Ctrl+N 来查看上一条或者下一条历史命令。用户可以编辑或是使用任何一条找到的历史命令。

快捷键

StoneOS CLI 支持快捷键的使用。表 3 列出 StoneOS 支持的快捷键及其功能：

快捷键	功能
Ctrl-A	将光标移至所在行的行首。
Ctrl-B	将光标向回移动一个字符。
Ctrl-D	删除光标所在的字符。
Ctrl-E	将光标移至所在行的行尾。
Ctrl-F	将光标向前移动一个字符。
Ctrl-K	删除光标后所有字符。
Ctrl-N	显示下一条历史命令。
Ctrl-P	显示上一条历史命令。
Ctrl-T	调换光标所在字母及其前一字母的顺序。
Ctrl-U	删除光标所在行。
Ctrl-W	删除光标前所有字符。
META-B	将光标移至所在词的词首。
META-D	删除光标前的词。
META-F	将光标移至所在词的词尾。
META-Backspace	删除光标后的词。
META-Ctrl-H	删除光标后的词。

表 3：快捷键及含义

说明：在没有 META 键的电脑上，请先按 ESC 键，再按字母键。例如，META-B 的操作过程为先按一下 ESC 键，然后再按字母 B。

过滤CLI输出信息

StoneOS CLI 用 show 命令显示设备的配置信息。用户可以根据需要对 show 命令的输出信息进行过滤。过滤方法为在 show 命令后添加一个过滤条件并用竖线（|）把命令和过滤条件隔开。过滤条件有三种：

- include <过滤条件>：输出符合过滤条件的信息。<过滤条件>中的字母区分字母大小写。
- exclude <过滤条件>：输出过滤条件以外的信息。<过滤条件>中的字母区分大小写。
- begin <过滤条件>：从第一条符合过滤条件的信息开始输出。<过滤条件>中的字母区分大小写。

CLI 输出信息过滤的语法格式为：

hostname# **show command | {include | exclude | begin}** {*filter-condition*}

在以上命令行中，第一个竖线（|）是命令的一部分，指明输出信息要按照过滤条件进行过滤。以后的竖线用来分隔命令的不同参数，并不是命令包含的部分。

过滤条件符合正则表达是规范。表 4 中列出正则表达式中常用的字符及其表示的含义：

字符	含义
句点（.）	匹配任意单字符。
星号（*）	一个单字符后紧跟*，匹配 0 个或多个此单字符。
加号（+）	一个单字符后紧跟+，匹配 1 个或多个此单字符。
脱字符号（^）	只匹配行首。
美元符号（$）	只匹配行尾。
下划线（_）	匹配逗号（,）、左大括号（{）、右大括号（}）、左圆括号（(）、右圆括号
方括号（[]）	指定单个字符的范围。
连字符（-）	分隔范围的终点。

表 4：字符及含义

分页显示CLI输出信息

一些命令的输出信息比较长，可能需要许多页显示，CLI 会用提示符“--More--”表示一页的结束。用户可以通过不同的操作指定继续显示信息或者终止显示信息。用户可执行的操作有：

- 显示下一行信息：按回车键。
- 返回到命令行：按“Q”键或者“q”键。
- 继续显示下一页信息：按除回车、“Q”和“q”以外的任意键。

设置终端属性

用户可以通过命令设置所使用终端的宽度和长度。默认情况下，终端宽为 80 个字符，长为 25 行。请使用以下命令设置终端的宽度和长度：

- 宽度：**terminal width** *character-number*
  character-number – 指定字符数。范围是 64 到 512 个字符。
- 长度：**terminal length** *line-number*
  line-number – 指定行数。范围是 0 到 256 行，0 的含义为不分屏显示。

终端的设置不会被记录，且不会影响其它终端属性。终端断开连接后再次登录时，终端的宽度和长度又会恢复到默认值。

设置连接超时时间

StoneOS CLI 可以设置控制台、SSH 或 Telnet 连接的超时时间。在全局配置模式下，输入以下命令设置超时时间：

- **console timeout** *timeout-value*
  timeout-value – 指定控制台超时时间。范围是 0 到 60 分钟，0 表示不会超时。默认值为 10 分钟。
- **ssh timeout** *timeout-value*
  timeout-value - 指定 SSH 超时时间。范围是 1 到 60 分钟。默认值是 10 分钟。
- **telnet timeout** *timeout-value*
  timeout-value - 指定 Telnet 超时时间。范围是 1 到 1440 分钟，默认是 5 分钟。

重定向输出

StoneOS 允许用户将 show 命令的输出信息重定向输出到其它的目的地址，包括安全设备的 Flash、FTP Server 和 TFTP Server。重定向输出命令的格式为：

show command | redirect *dst-address*

目的地址（*dst-address*）的格式为：

- Flash – `flash://filename`
- FTP – `ftp://[username:password@]x.x.x.x[:port]/filename`
- TFTP – `tftp://x.x.x.x/filename`

StoneOS系统管理命令

access

配置管理员的访问方式。

［命令］

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

［句法描述］

console	指定管理员通过配置口（CON）访问。
http	指定管理员通过 HTTP 访问。
https	指定管理员通过 HTTPS 访问。
ssh	指定管理员通过 SSH 访问。
telnet	指定管理员通过 Telnet 访问。
any	指定管理员可以通过以上任何一种方式访问。

［默认取值］

无默认值。

［命令模式］

管理员配置模式。

［使用指导］

无。

［命令实例］

hostname(config-admin)# **acess any**

active

开启统计集的统计功能。使用该命令 no 的形式关闭统计集的统计功能。

［命令］

active

no active

［句法描述］

无。

［默认取值］

关闭。

［命令模式］

统计集配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# statistics-set set1
hostname(config-statistic-set)# no active
```

admin

配置管理员密码策略。使用该命令 no 的形式恢复密码复杂度或密码最小长度的默认值。

［命令］

admin {complexity {0 | 1} | min-length *length-value*}

no admin complexity

no admin min-length

［句法描述］

complexity {0 | 1}	指定管理员密码的复杂度。
min-length *length-value*	指定管理员密码的最小长度。范围是 4 到 16 个字符。

［默认取值］

complexity - 0。

min-length - 4。

［命令模式］

管理员密码策略配置模式。

［使用指导］

管理员密码的复杂度为 0，表示不对密码字符进行复杂度限制；1 表示指定的密码中必须包含以下各项：两个大写字母、两个小写字母、两个数字和两个特殊字符（例如“@”等）。

［命令实例］

```
hostname(config-pwd-policy)# admin complexity 1
```

admin host

配置系统的可信主机。使用该命令 no 的形式取消可信主机的指定，或取消对可信主机特定登录类型的指定。

［命令］

admin host {*A.B.C.D A.B.C.D* | **any**} {**http** | **https** | **ssh** | **telnet** | **any**}

no admin host *A.B.C.D A.B.C.D*

no admin host {*A.B.C.D A.B.C.D* | **any**} {**http** | **https** | **ssh** | **telnet**}

［句法描述］

A.B.C.D A.B.C.D | **any**	指定可信主机的 IP 地址范围，**any** 表示任何 IP 地址。
http | **https** | **ssh** | **telnet** | **any**	指定可信主机的登录类型。**any** 表示可以使用 HTTP、HTTPS、SSH 和 Telnet 任意一种类型登录。

［默认取值］

无默认值。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **admin host 10.0.0.0 255.0.0.0 any**

admin user

创建本地管理员并且进入管理员配置模式，如果指定的管理员名称已经存在，则直接进入管理员配置模式。使用该命令 no 的形式删除指定的本地管理员。

［命令］

admin user *user-name*

no admin user *user-name*

［句法描述］

user-name	指定管理员的名称。

［默认取值］

无默认值。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# admin user abcd
hostname(config-admin)#
```

allow-pwd-change

开启允许本地用户修改登录密码功能。安全网关支持本地用户通过 Web 认证后，在认证登录成功页面修改自己的用户密码。使用该命令 no 的形式关闭该功能。

［命令］

allow-pwd-change

no allow-pwd-change

［句法描述］

无。

［默认取值］

关闭。

［命令模式］

本地 AAA 服务器配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# aaa-server local
hostname(config-aaa-server)# allow-pwd-change
```

{app | ips signature} stat-report

开启信息上报功能。为了更好的了解用户网络环境下设备的 APP 识别率或 IPS 统计信息的情况，系统支持信息上报功能，即当用户认为统计信息不理想时，开启该功能请求服务器帮助搜集用户的 APP 分类统计信息或 IPS 统计信息进行分析。

启用 APP 上报后，当在线升级 APP 特征库时，用户在前 24 小时内且排名前 20 的流量分类信息将被上报到服务器。APP 上报的信息内容包括用户设备的 IP 地址、序列号、软件版本、APP 特征库版本信息、上报的统计集名称、排名前 20 的流量分类信息（应用协议 ID、名称、流量信息）以及统计集记录的总流量。

启用 IPS 上报后，当在线升级 IPS 特征库时，用户在前 24 小时内且排名前 10 的 IPS 统计信息将被上报到服务器。IPS 上报的信息内容包括用户设备的 IP 地址、序列号、软件版本、IPS 特征库版本信息、命中次数排名前 10 的 IPS 统计集信息（命中的 IPS 规则 ID 和该 IPS 规则命中的次数）。

［命令］

{app | ips signature} stat-report

no {app | ips signature} stat-report

［句法描述］

无。

［默认取值］

关闭。

［命令模式］

全局配置模式。

［使用指导］

开启 APP 上报功能前，请先确保系统的流量统计功能为开启状态。

开启 IPS 上报功能前，请先确保系统的入侵防御统计功能为开启状态。

［命令实例］

hostname(config)# **app stat-report**

---

arp

配置 ARP 报文目标监测条目。使用该命令 no 的形式删除指定的监测条目。

［命令］

arp {*A.B.C.D*} **interface** *interface-name* [**interval** *value*] [**threshold** *value*] [**weight** *value*]

no arp *A.B.C.D*

［句法描述］

A.B.C.D	指定监测目标的 IP 地址。
interface *interface-*	指定发送 ARP 检测报文的出接口。

name	
interval *value*	指定发送 ARP 报文的时间间隔，单位为秒。范围是 1 到 255 秒。
threshold *value*	指定判断监测失败的警戒值。如果系统连续未收到该参数指定个数的响应报文，就判断为监测失败，即目标不可达。取值范围是 1 到 255。
weight *value*	指定该条监测失败对整个监测对象失败贡献的权重值。取值范围是 1 到 255。

［默认取值］

interval *value* — 3 秒。

threshold *value* — 1。

weight *value* — 255。

［命令模式］

监测对象配置模式。

［使用指导］

用户可以配置多条该命令为监测对象指定多个监测条目。

［命令实例］

```
hostname(config)# track trackobj1
hostname(config-trackip)# arp 1.1.1.1 interface ethernet0/0
```

external-bypass enable

开启旁路功能。使用外置 Bypass 模块时，用户需开启旁路功能才能使设备在特定情形下启动旁路模式。使用该命令 no 的形式关闭该功能。

［命令］

external-bypass enable

no external-bypass enable

［句法描述］

无。

［默认取值］

关闭。

［命令模式］

全局配置模式。

［使用指导］

仅部分型号安全网关提供旁路功能。

［命令实例］

hostname(config)# **external-bypass enable**

---

clear logging

清除系统日志信息。

［命令］

clear logging {alarm | configuration | debug | event | network | security | traffic}

［句法描述］

alarm	清除所有系统存储的告警日志信息。
configuration	清除所有系统存储的配置日志信息。
debug	清除所有系统存储的调试日志信息。
event	清除所有系统存储的事件日志信息。
network	清除所有系统存储的网络日志信息。
security	清除所有系统存储的安全日志信息。
traffic	清除所有系统存储的流量日志信息。

［默认取值］

无。

［命令模式］

执行模式。

［使用指导］

无。

［命令实例］

hostname# **clear logging debug**

---

clear nbt-cache

清除 NetBIOS 缓存数据。

［命令］

clear nbt-cache [*ip-address*][**vrouter** *vrouter-name*]

［句法描述］

ip-address	指定 IP 地址。配置该参数，系统将清除与指定 IP 地址相关的 NetBIOS 缓存数据。如果不配置该参数，系统将清除所有 NetBIOS 缓存数据。
vrouter *vrouter-name*	指定 VR 名称。配置该参数，系统将清除属于指定 VR 的 NetBIOS 缓存数据。如果没有指定 VR，系统将清除所有 VR 下的 NetBIOS 缓存数据。

［默认取值］

无默认值。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **clear nbt-cache 10.10.0.1**

clock time

配置安全网关系统的当前时间。

［命令］

clock time *HH:MM:SS Month Day Year*

［句法描述］

HH:MM:SS	指定当前的时间，格式为“小时：分钟：秒”。
Month	指定当前月份。月的取值范围是 1 到 12。
Day	指定当前日期。天的取值范围是 1 到 31。
Year	指定当前年。年的取值范围是 2000 到 2035 年。

［默认取值］

无默认值。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **clock time 14:26:00 6 22 2007**

---

clock zone

配置安全网关系统的时区。

［命令］

clock zone *timezone-name*

［句法描述］

timezone-name	指定时区的名称。

［默认取值］

无默认值。

［命令模式］

全局配置模式。

［使用指导］

输入 **clock zone ?** 可以查看所有支持的时区。

［命令实例］

hostname(config)# **clock zone china**

---

configure

使 CLI 从执行模式进入到全局配置模式。

［命令］

configure

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

执行模式。

［使用指导］

无。

［命令实例］

```
hostname# configure
hostname(config)#
```

console timeout

配置 Console 超时时间。使用该命令 no 的形式恢复 Console 超时默认值。

［命令］

console timeout *timeout-value*

no console timeout

［句法描述］

timeout-value	指定 Console 超时时间，范围是 0 到 60 分钟，0 表示永不超时。

［默认取值］

10 分钟。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# console timeout 20
```

cpu

设置监控规则，对系统资源对象进行监控。

［命令］

{cpu | memory utilization | interface-bandwidth *interface-name* **utilization | log-buffer {alarm | config | event | IPS | NBC | network | security | traffic} utilization | policy utilization | session utilization} interval** *interval-value* **absolute rising-threshold** *threshold-value* **sample-period** *period-value* **[count** *count-value*] **{log | snmp-trap}**

no {cpu | memory utilization | interface-bandwidth *interface-name* **utilization | log-buffer {alarm | config | event | IPS | NBC | network | security | traffic} utilization | policy utilization | session utilization}**

［句法描述］

cpu	指定监控对象为系统 CPU。
memory	指定监控对象为系统内存。
interface-bandwidth *interface-name*	指定监控对象为接口带宽。*interface-name* 为被监控接口的名称。
**log-buffer {alarm	config	event	IPS	NBC	network	security	traffic}**	指定监控对象为日志容量，并且指定日志类型（即 **alarm	config	event	IPS	NBC	network	security	traffic**）。
policy	指定监控对象为策略数。
session	指定监控对象为会话。
utilization	指定监控值为各监控对象的利用率。CPU（**cpu**）的监控值默认为利用率，不需要指定。
interval *interval-value*	指定监控间隔，即系统在报警计算时间段（**sample-period** *period-value*）内，每次取值后等待的时间间隔。取值范围为 3 到 10 秒。
absolute	指定监控值为绝对值。
rising-threshold *threshold-value*	指定上升阈值，即实际监控值超过该阈值满足报警条件的百分比。取值范围为 1 到 99。
sample-period *period-value*	指定报警计算时间段。取值范围为 30 到 3600 秒。
count *count-value*	指定在报警计算时间段（**sample-period**）内，监控对象的实际监控数值超过阈值（**rising-threshold**）的次数。取值范围为 1 到 1000。如果配置该参数，在监控时间段内，若监控对象值超过阈值的次数大于该 **count** 值，则发出警告；如果不配置该参数，在监控时间段内，若监控对象值的平均值大于阈值（**rising-threshold**），则发出警告。
**log	snmp-trap**	指定报警方式。可以使用告警日志（**log**）或者 SNMP Trap 报文（**snmp-trap**）。

［默认取值］

无默认值。

［命令模式］

监控配置模式。

［使用指导］

对于每种监控对象，只有最后配置的一条监控规则生效。

［命令实例］

CPU 峰值监控：

hostname(config)# **monitor**

hostname(config-monitor)# **cpu interval 5 absolute rising-threshold 65 sample-period 600 count 50 log**

完成该配置后，在 600 秒内，如果 CPU 利用率超过了阈值 65%，且发生过最少 50 次，则发出告警日志

会话均值监控：

hostname(config)# **monitor**

hostname(config-monitor)# **session utility interval 8 absolute rising-threshold 90 sample-period 600 log**

完成该配置后，在 600 秒内，如果会话平均利用率超过了阈值 90%，则发出告警日志

---

debug

开启系统调试功能。使用 undbug 命令关闭相应的调试功能。

［命令］

debug {**all** | *function-name*}

undebug {**all** | *function-name*}

［句法描述］

all	开启安全网关所有协议和功能的系统调试功能。
function-name	开启安全网关指定协议或功能的系统调试功能。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

可以通过双击“ESC”键关闭 debug 功能。由于部分信息被缓存，关闭过程可能会持续几分钟。

［命令实例］

hostname# **debug all**

---

delete configuration saved

删除设备的起始配置信息。

［命令］

delete configuration saved {**current** | *number*}

［句法描述］

current	删除当前起始配置信息。
number	删除指定的备份起始配置信息，*number* 为备份起始配置信息的数字标记。

［默认取值］

无默认值。

［命令模式］

全局配置模式。

［使用指导］

系统重启后生效。

［命令实例］

hostname(config)# **rollback configuration saved 2**

---

desc

为用户提供描述信息。

［命令］

desc *string*

［句法描述］

string	指定描述信息，范围是 1 到 31 个字符。

［默认取值］

无默认值。

［命令模式］

用户配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **aaa-server local**

```
hostname(config-aaa-server)# user user1
hostname(config-user)# desc test
```

dns

配置 DNS 报文目标监测条目。使用该命令 no 的形式删除指定的监测条目。

［命令］

dns *A.B.C.D* **interface** *interface-name* [**interval** *value*] [**threshold** *value*] [**weight** *value*] [**src-interface** *interface-name*]

no dns *A.B.C.D* **interface** *interface-name*

［句法描述］

A.B.C.D	指定监测目标的 IP 地址。
interface *interface-name*	指定发送 DNS 检测报文的出接口。
interval *value*	指定发送 DNS 报文的时间间隔，单位为秒。范围是 1 到 255 秒。
threshold *value*	指定判断监测失败的警戒值。如果系统连续未收到该参数指定个数的响应报文，就判断为监测失败，即目标不可达。取值范围是 1 到 255。
weight *value*	指定该条监测失败对整个监测对象失败贡献的权重值。取值范围是 1 到 255。
src-interface *interface-name*	指定 DNS 检测报文的源接口。

［默认取值］

interval *value* – 3 秒。

threshold *value* – 1。

weight *value* – 255。

［命令模式］

监测对象配置模式。

［使用指导］

用户可以配置多条该命令为监测对象指定多个监测条目。

［命令实例］

```
hostname(config)# track trackobj1
hostname(config-trackip)# dns 1.1.1.1 interface ethernet0/3
```

dst-addr-based-session-counter

开启安全域的目的 IP 地址统计功能（IP 地址会话统计和 IP 地址流量统计）。使用该命令 no 的形式关闭域的目的 IP 地址统计功能。

［命令］

dst-addr-based-session-counter

no dst-addr-based-session-counter

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

安全域统计模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# zone trust
hostname(config-zone-trust)# statistic session-counter
hostname(config-sess-stat)# dst-addr-based-session-counter
```

exec admin user password update

修改当前登录的 VSYS 管理员密码。

［命令］

exec admin user password update *password*

［句法描述］

password	指定本地管理员的新密码，为 4 到 31 个字符的字符串。

［默认取值］

无。

［命令模式］

执行模式。

［使用指导］

该命令主要为支持 VSYS RX 管理员修改密码。

［命令实例］

hostname# **exec admin user password update Hillstone12**

exec console baudrate

设置 Console 口的波特率。

［命令］

exec console baudrate {9600 | 19200 | 38400 | 57600 | 115200}

［句法描述］

9600	设置 Console 口的波特率为 9600bps。
19200	设置 Console 口的波特率为 19200bps。
38400	设置 Console 口的波特率为 38400bps。
57600	设置 Console 口的波特率为 57600bps。
115200	设置 Console 口的波特率为 115200bps。

［默认取值］

9600。

［命令模式］

任何模式。

［使用指导］

需要注意的是，完成波特率配置后，用户在通过 Console 口登录设备时需保证波特率与设备 Console 口所作配置一致。

［命令实例］

hostname# **exec console baudrate 38400**

exec format

格式化存储设备。

［命令］

exec format [sd0 | usb0 | usb1 | storage*X*]

［句法描述］

sd0	对 SD 卡槽内插入的 SD 存储卡进行格式化操作。

usb0 | usb1	对与指定 USB 口相连的存储设备进行格式化操作。
storage*X*	对指定的存储扩展模块进行格式化操作。*X* 为插入存储扩展模块的扩展槽号，不同平台 *X* 的取值范围不同。

［默认取值］

无。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **exec format sd0**

exec detach

安全删除存储设备。

［命令］

exec detach [sd0 | usb0 | usb1 | storage*X***]**

［句法描述］

sd0	安全删除 SD 卡槽内插入的 SD 存储卡。
usb0 | usb1	安全删除指定 USB 口相连的存储设备。
storage*X*	安全删除指定的存储扩展模块。*X* 为插入存储扩展模块的扩展槽号，不同平台 *X* 的取值范围不同。

［默认取值］

无。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **exec detach sd0**

exec customize

恢复 Web 认证、SCVPN 认证或 Web 重定向登录页面的默认图片。

［命令］

exec customize {scvpn | webauth | webredirect } [language {en | zh_cn}] default

［句法描述］

language {en | zh_cn}	指定将英文（**en**）或者中文（**zh_cn**）认证登录页面恢复为默认图片。

［默认取值］

无。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **exec customize scvpn**

exec license apply

进入许可证申请模式。

［命令］

exec license apply {advanced | platform | platform-trial | performance | session | other-wildcard}

［句法描述］

advanced	进入高级许可证申请模式。
platform	进入平台许可证申请模式。
platform-trial	进入试用平台许可证申请模式。
performance	进入性能许可证申请模式。
session	进入会话许可证申请模式。
other-wildcard	进入其它许可证申请模式。

［默认取值］

无。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **exec license apply performance**

---

exec license install

安装许可证。

［命令］

exec license install *license-string*

［句法描述］

license-string	要安装的许可证字符串。

［默认取值］

无。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **exec license install** *license-string*

---

exec license uninstall

卸载许可证。

［命令］

exec license uninstall *license-name*

［句法描述］

license-name	要卸载的许可证名称。

［默认取值］

无。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **exec license uninstall plat071220032206**

---

exec webauth kickout

强制断开某个用户与认证系统的连接。

［命令］

exec webauth kickout *user-name*

［句法描述］

user-name	指定 Web 认证的用户名称。

［默认取值］

无。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname(config)# **exec webauth kickout user1**

---

exit

使 CLI 从当前配置模式退回到上一级配置模式。

［命令］

exit

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# exit
hostname#
```

expire

指定用户的有效期。

［命令］

expire *Month/day/year HH:MM*

no expire

［句法描述］

Month/day/year HH:MM	指定用户有效期时间，格式为“月/日/年 小时:分钟”。例如命令 **expire 02/12/2010 12:00** 表示用户将在 2010 年 12 月 2 日的 12：00 过期。

［默认取值］

无。

［命令模式］

用户模式。

［使用指导］

默认情况下，用户没有有效期限制。

［命令实例］

```
hostname(config)# aaa-server local
hostname(config-aaa-server)# user user1
hostname(config-aaa-server)# user user1
hostname(config-user)# expire 02/12/2010 20:30
```

export configuration

导出系统的当前配置信息和备份配置信息到 FTP 服务器、TFTP 服务器或者 U 盘。

［命令］

export configuration {**current** | *number*} **to ftp server** *ip-address* [**user** *user-name* **password** *password*] [*file-name*]

export configuration {**current** | *number*} **to tftp server** *ip-address* [*file-name*]

export configuration {**current** | *number*} **to** {**usb0** | **usb1**} [*file-name*]

［句法描述］

current	指定导出当前配置信息。
number	指定导出以 *number* 为标识的备份配置信息。
ip-address	指定 FTP 或 TFTP 服务器的 IP 地址。
user-name	指定访问 FTP 服务器的用户名。
password	指定访问 FTP 服务器的密码。
usb0 | **usb1**	指定导出到 U 盘时使用的 USB 接口。
file-name	指定导出的配置信息文件的名称。

［默认取值］

无。

［命令模式］

执行模式。

［使用指导］

无。

［命令实例］

hostname# **export configuration 3 to tftp server 10.200.3.115 conf_3**

export log event

导出日志信息到 FTP 服务器、TFTP 服务器或 U 盘。

［命令］

export log {**event** | **alarm** | **security**} **to ftp server** *ip-address* **user** *user-name* **password** *password* [*file-name*]

export log {**event** | **alarm** | **security**} **to tftp server** *ip-address* [*file-name*]

export log {event | alarm | security} to {usb0 | usb1} [*file-name*]

［句法描述］

event	导出事件日志信息。
alarm	导出告警日志信息。
security	导出安全日志信息。
ip-address	指定 FTP 或 TFTP 服务器的 IP 地址。
user-name	指定访问 FTP 服务器的用户名。
password	指定访问 FTP 服务器的密码。
usb0 | usb1	指定导出到 U 盘时使用的 USB 接口。
file-name	指定导出的日志文件的名称。

［默认取值］

无。

［命令模式］

执行模式。

［使用指导］

无。

［命令实例］

hostname# **export log event to usb0 event1.log**

filter

为统计集配置过滤条件，以统计特定条件下的数据信息。使用该命令 no 的形式取消过滤条件配置。

［命令］

filter {ip {*A.B.C.D/M* | *address-entry*} [source | destination] | interface *name* [ingress | egress] | zone *name* [ingress | egress] | application *name* | attack-type *name*| service *name* | role *name* }

no filter {ip {*A.B.C.D/M* | *address-entry* } [source | destination] | interface *name* [ingress | egress] | zone *name* [ingress | egress] | application *name* | attack-type *name* | service *name* | role *name* | user *user-name aaa-server-name* | user-group *user-group-name aaa-server-name*}

no filter all（取消所有类型的过滤条件）

［句法描述］

ip {*A.B.C.D/M* | *address-entry*}	以指定 IP 为条件进行过滤。IP 可以是地址范围（比如 10.101.0.1 255.255.255.0 或者 10.101.0.1/24）或者系统地址簿中的地址条目。
source | **destination**	以源 IP 地址（**source**）或者目的 IP 地址（**destination**）为条件进行过滤。
interface *name*	以指定接口为条件进行过滤。
ingress | **egress**	以入接口（**ingress**）或出接口（**egress**）为条件进行过滤。
zone *name*	以指定安全域为条件进行过滤。
ingress | **egress**	以入接口（**ingress**）或出接口（**egress**）为条件进行过滤。
application *name*	以指定应用为条件进行过滤。
attack-type *name*	以指定攻击类型为条件进行过滤。
service *name*	以指定服务类型为条件进行过滤。
role *name*	以指定角色名称为条件进行过滤。
user *user-name aaa-server-name*	以指定用户名称为条件进行过滤。
user-group *user-group-name aaa-server-name*	以指定用户组名称为条件进行过滤。

［默认取值］

无。

［命令模式］

统计集配置模式。

［使用指导］

用户可以配置多条该命令，添加多个过滤条件。系统最多允许每个统计集配置 32 条过滤条件。如果为同一个统计集配置的多个过滤条件属于同一类型，那么这些过滤条件之间为逻辑“或”（or）的关系；如果分属不同类型，那么这些过滤条件之间为逻辑“与”（and）的关系。

［命令实例］

hostname(config-statistic-set)# **filter interface ethernet0/3**

generate-request

生成许可证请求。

［命令］

generate-request

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

许可证申请配置模式。

［使用指导］

无。

［命令实例］

hostname(apply-license)# **generate-require**

---

group

为用户指定用户组。使用该命令 no 的形式取消用户组的指定。

［命令］

group *user-group-name*

no group *user-group-name*

［句法描述］

user-group-name	指定系统中已配置的用户组的名称。

［默认取值］

无。

［命令模式］

用户配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **user user1 aaa-server local**

hostname(config-username)# **group group1**

---

group-by

配置统计集的数据组织方式（IP、接口、安全域、攻击类型、应用、病毒、用户、特征 ID、URL、URL 类别、关键字和关键字阻断类型）。数据组织方式会根据统计数据类型的不同而不同。使用该命令 no 的形式取消统计集数据组织方式的配置。

［命令］

group-by {[ip [directional] [initiator | responder | belong-to-zone *zone-name* **| not-belong-to-zone** *zone-name* **| belong-to-interface** *interface-name* **| not-belong-to-interface** *interface-name*]][**interface** [**directional**]][**zone**[**directional**]][**application**][**attack-type**][**virus**][**user**[**directional**]][**sig-id**][**url**][**url-category**][**keyword**][**block-type**]}

no group-by

［句法描述］

ip	指定统计集的数据组织方式为 IP 地址。用户可以通过 **initiator** | **responder** | **belong-to-zone** *zone-name* | **not-belong-to-zone** *zone-name* | **belong-to-interface** *interface-name* | **not-belong-to-interface** *interface-name* 参数指定被统计 IP 的范围，可以是发起会话的 IP（**initiator**），接收会话的 IP（**responder**），属于某特定安全域的 IP（**belong-to-zone** *zone-name*），不属于某特定安全域的 IP（**not-belong-to-zone** *zone-name*），属于某特定接口的 IP（**belong-to-interface** *interface-name*）或者不属于某特定接口的 IP（**not-belong-to-interface** *interface-name*）。
interface	指定统计集的数据组织方式为接口。
zone	指定统计集的数据组织方式为安全域。
application	指定统计集的数据组织方式为应用，此时的统计数据类型不可以为攻击速率、URL 命中次数和关键字阻断次数。
attack-type	指定统计集的数据组织方式为攻击类型，此时的统计数据类型只能为攻击速率。
virus	指定统计集的数据组织方式为病毒，此时的统计数据类型只能为病毒个数。
user	指定统计集的数据组织方式为用户。
sig-id	指定统计集的数据组织方式为特征 ID，此时的统计数据类型只能为入侵次数。
url	指定统计集的数据组织方式为 URL，此时的统计数据类型只能为 URL 命中次数。
url-category	指定统计集的数据组织方式为 URL 类别，此时的统计数据类型只能为 URL 命中次数。
keyword	指定统计集的数据组织方式为关键字，此时的统计数据类型只能为关键字阻断次数。

block-type	指定统计集的数据组织方式为关键字阻断类型，此时的统计数据类型只能为关键字阻断次数。
directional	指定统计结果为双向的，即统计以 IP、接口或者安全域为数据组织方式时的上行和下行带宽、接收和发送会话数、接收和发送新建会话速率；如不配置，系统默认统计结果为无方向的，即统计以 IP、接口或者安全域为数据组织方式的所有带宽、会话或者新建会话速率。

［默认取值］

无。

［命令模式］

用户配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **statistics-set set1**

hostname(config-statistic-set)# **group-by application**

hostname

指定安全网关名称。该名称也将会显示在命令提示符中。使用该命令 no 的形式恢复默认名称。

［命令］

hostname *host-name*

no hostname

［句法描述］

host-name	指定安全网关的名称。

［默认取值］

平台名称。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **hostname hillstone**

hillstone(config)#

http

配置 HTTP 方式目标监测条目。使用该命令 no 的形式删除指定的监测条目。

［命令］

http {*A.B.C.D* | **host** *host-name*} **interface** *interface-name* [**src-interface** *interface-name*] [**interval** *value*] [**threshold** *value*] [**weight** *value*]

no http {*A.B.C.D* | **host** *host-name*}

［句法描述］

A.B.C.D | **host** *host-name*	指定监测目标的 IP 地址或者主机名称。
interface *interface-name*	指定发送 HTTP 检测报文的出接口。
src-interface *interface-name*	指定 HTTP 检测报文的源接口。
interval *value*	指定发送 HTTP 报文的时间间隔，单位为秒。范围是 1 到 255 秒。
threshold *value*	指定判断监测失败的警戒值。如果系统连续未收到该参数指定个数的响应报文，就判断为监测失败，即目标不可达。取值范围是 1 到 255。
weight *value*	指定该条监测失败对整个监测对象失败贡献的权重值。取值范围是 1 到 255。

［默认取值］

interval *value* — 3 秒。

threshold *value* — 1。

weight *value* — 255。

［命令模式］

监测对象配置模式。

［使用指导］

用户可以配置多条该命令为监测对象指定多个监测条目。

［命令实例］

hostname(config)# **track trackobj1**

hostname(config-trackip)# **http host host1 interface ethernet0/0**

http port

指定 HTTP 端口号。使用该命令 no 的形式恢复 HTTP 默认端口号。

［命令］

http port *port-number*

no http port

［句法描述］

port-number	指定 HTTP 端口号。当使用 HTTP 方式访问设备时，浏览器的 HTTP 端口号必须与此处指定的端口号一致。范围是 1 到 65535。

［默认取值］

80。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **http port 8080**

https port

指定 HTTPS 端口号。使用该命令 no 的形式恢复 HTTPS 默认端口号。

［命令］

https port *port-number*

no https port

［句法描述］

port-number	指定 HTTPS 端口号。当使用 HTTPS 方式访问设备时，浏览器的 HTTPS 端口号必须与此处指定的端口号一致。范围是 1 到 65535。

［默认取值］

443。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **https port 4433**

https trust-domain

指定 HTTPS 方式访问时使用的 PKI 信任域。使用该命令 no 的形式恢复默认 PKI 信任域。

［命令］

https trust-domain *trust-domain-name*

no https trust-domain

［句法描述］

trust-domain-name	指定已配置的 PKI 信任域的名称。当 HTTPS 启动时，HTTPS 服务器将使用指定 PKI 信任域中的证书。

［默认取值］

系统缺省 PKI 信任域：trust_domain_default。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **https trust-domain td1**

ike-id

为拨号 VPN 用户指定 IKE ID。使用该命令 no 的形式取消用户的 IKE ID 配置。

［命令］

ike-id {**fqdn** *string* | **asn1dn** *string*}

no ike-id

［句法描述］

fqdn *string*	指定使用 FQDN 类型的 IKE ID。*string* 为 ID 的具体内容。
asn1dn *string*	指定使用 Asn1dn 类型的 ID，该类型只可应用于使用证书的情况。*string* 为 ID 的具体内容。

［默认取值］

无。

［命令模式］

用户配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# user user1 aaa-server local
hostname(config-username)# ike_id fqdn aaa
```

import configuration

从 FTP 服务器、TFTP 服务器或者 U 盘导入配置信息。

［命令］

import configuration from ftp server *ip-address* **user** *user-name* **password** *password file-name*

import configuration from tftp server *ip-address file-name*

import configuration from {usb0 | usb1} *file-name*

［句法描述］

ip-address	指定 FTP 或 TFTP 服务器的 IP 地址。
user-name	指定访问 FTP 服务器的用户名。
password	指定访问 FTP 服务器的密码。
usb0 | usb1	指定从 U 盘导入时使用的 USB 接口。
file-name	指定导入的配置信息文件的名称。

［默认取值］

无。

［命令模式］

执行模式。

［使用指导］

无。

［命令实例］

```
hostname# import configuration from usb1 conf_2
```

import customize

引入登录页面背景图片自行定制 Web 认证、SCVPN 认证或 Web 重定向登录页面。

［命令］

import customize {scvpn | webauth | webredirect } from {ftp server *ip-address* **[user** *user-name* **password** *password*] **| tftp server** *ip-address* **| usb0 | usb1}** *file-name*

［句法描述］

scvpn | webauth | webredirect	指定定制 Web 认证、SCVPN 认证或 Web 重定向登录页面。
ftp server *ip-address* **[user** *user-name* **password** *password*]	定从 FTP 服务器获取图片，并指定 FTP 服务器的 IP 地址以及访问服务器使用的用户名和密码。当不输入用户名和密码时表示采用匿名登录方式。
tftp server *ip-address*	指定从 TFTP 服务器获取图片，并指定 TFTP 服务器的 IP 地址。
usb0 | usb1	指定通过 USB 方式从 USB0 或者 USB1 插槽所对应的 U 盘根目录获取图片。
file-name	指定图片名称。对于 Web 认证登录页面图片，其文件名必须为“login_page_bg_en.gif”（用于英文登录页面）或“login_page_bg_cn.gif”（用于中文登录页面）；对于 SCVPN 认证登录页面图片，其文件名必须为“Login_box_bg_en.gif”（用于英文登录页面）或“Login_box_bg_cn.gif”（用于中文登录页面）。所有图片的分辨率必须为 624px * 376px，并且只有将它们压缩到 zip 包后才能上载。

［默认取值］

无。

［命令模式］

执行模式。

［使用指导］

无。

［命令实例］

hostname# **import customize scvpn from tftp server 10.101.0.113 test.zip**

import image

通过 FTP 服务器、TFTP 服务器或者 U 盘升级 StoneOS。

［命令］

import image from ftp server *ip-address* **user** *user-name* **password** *password file-name*

import image from tftp server *ip-address file-name*

import image from {usb0 | usb1} *file-name*

［句法描述］

ip-address	指定 FTP 或 TFTP 服务器的 IP 地址。
user-name	指定访问 FTP 服务器的用户名。
password	指定访问 FTP 服务器的密码。
usb0 | usb1	指定从 U 盘导入时使用的 USB 接口。
file-name	指定导入的 StoneOS 文件的名称。

［默认取值］

无。

［命令模式］

执行模式。

［使用指导］

无。

［命令实例］

hostname# **import image from ftp server 10.200.3.134 user user1 password user_password1 StoneOS-1.1R1**

interface

配置对接口链路状态进行监测的监测条目。使用该命令 no 的形式删除指定的监测条目。

［命令］

interface *interface-name* [**weight** *value*]

no interface *interface-name*

［句法描述］

interface-name	指定被监测接口的名称。
weight *value*	指定该条监测失败对整个监测对象失败贡献的权重值。

［默认取值］

weight *value* – 1 到 255。

［命令模式］

监测对象配置模式。

［使用指导］

配置多条该命令为监测对象指定多个监测条目。

［命令实例］

hostname(config)# **track trackobj**

hostname(config-trackip)# **interface ethernet0/2 weight 1**

---

ip

配置 Ping 报文目标监测条目。使用该命令 no 的形式删除指定的监测条目。

［命令］

ip {*A.B.C.D* | **host** *host-name*} **interface** *interface-name* [**src-interface** *interface-name*] [**interval** *value*] [**threshold** *value*] [**weight** *value*]

no ip {*A.B.C.D* | **host** *host-name*}

［句法描述］

A.B.C.D | **host** *host-name*	指定监测目标的 IP 地址或者主机名称。
interface *interface-name*	指定发送 Ping 检测报文的出接口。
src-interface *interface-name*	指定 Ping 检测报文的源接口。
interval *value*	指定发送 Ping 报文的时间间隔，单位为秒。范围是 1 到 255 秒。
threshold *value*	指定判断监测失败的警戒值。如果系统连续未收到该参数指定个数的响应报文，就判断为监测失败，即目标不可达。取值范围是 1 到 255。
weight *value*	指定该条监测失败对整个监测对象失败贡献的权重值。取值范围是 1 到 255。

［默认取值］

interval *value* – 3 秒。

threshold *value* – 1。

weight *value* – 255。

［命令模式］

监测对象配置模式。

［使用指导］

用户可以配置多条该命令为监测对象指定多个监测条目。

［命令实例］

```
hostname(config)# track trackobj1
hostname(config-trackip)# ip 1.1.1.1 interface ethernet0/0
```

language

设置系统信息（包括日志信息、错误信息和提示信息）显示语言。使用该命令 no 的形式恢复系统信息显示语言为默认情况。

［命令］

```
language {en | zh_CN}
no language
```

［句法描述］

en	指定系统信息的显示语言为英文。
zh_CN	指定系统信息的显示语言为简体中文。

［默认取值］

默认情况下，系统信息的显示语言为英文。

［命令模式］

全局配置模式。

［使用指导］

该命令的设置不会影响 Web 管理界面的语言。

［命令实例］

```
hostname(config)# language zh_CN
```

logging

开启系统指定类型的日志功能。使用该命令 no 的形式关闭系统指定类型的日志功能。

［命令］

logging {alarm | event | security | configuration | network | traffic | debug} on

no logging { alarm | event | security | configuration | network | traffic | debug} on

［句法描述］

无。

［默认取值］

默认情况下，配置和流量日志功能是关闭的（打开流量日志功能会影响系统性能），其它（事件、告警、安全、网络和调试）均为开启状态。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **logging event on**

hostname(config)# **no logging event on**

---

logging app-identification

开启应用安全日志功能。使用该命令 no 的形式关闭系统安全日志功能。

［命令］

logging app-identification

no logging app-identification

［句法描述］

无。

［默认取值］

关闭。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# logging app-identification
```

logging alarm to

指定流量日志信息的输出目的地。使用该命令 no 的形式关闭相关的输出功能。

［命令］

logging alarm to {console | remote | syslog| email | sms} [severity *severity-level*]

logging alarm to buffer [size *buffer-size*] **[severity** *severity-level*]

logging alarm to file [name {usb0 | usb1} *file-name*] **[size** *file-size*] **[severity** *severity-level*]

no logging alarm to {console | remote | syslog| email | sms}

no logging alarm to buffer

no logging alarm to file

［句法描述］

console	指定将流量日志信息输出到 console 口。
syslog	指定将流量日志信息输出到 Syslog Server。
buffer	指定将流量日志信息输出到内存缓存。
email	使用安全日志 email 提醒功能。
sms	指定将告警日志信息以短信的形式输出到某个手机。
usb0 | usb	指定保存日志信息的 U 盘。
file-name	指定存储到 U 盘的日志信息文件名称。
severity-level	指定输出的告警日志信息的级别从而对告警日志信息进行过滤。
file-size	指定日志信息文件大小。范围是 4096 到 4294967295 字节。
buffer-size	将流量日志信息输出到内存缓存时，该参数用来指定内存缓存的大小。范围是 4096 到 4294967295 字节。

［默认取值］

内存缓存默认值：1048576 字节；

日志信息文件大小默认值：1048576 字节。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# logging alarm to email severity alerts
```

logging configuration to

指定配置日志信息的输出目的地。使用该命令 no 的形式关闭相关的输出功能。

［命令］

logging configuration to {console | syslog}

logging configuration to buffer [size *buffer-size*]

no logging configuration to {console | syslog}

no logging configuration to buffer

［句法描述］

console	指定将配置日志信息输出到 console 口。
syslog	指定将配置日志信息输出到 Syslog Server。
buffer	指定将配置日志信息输出到内存缓存。
buffer-size	将配置日志信息输出到内存缓存时，该参数用来指定内存缓存的大小。范围是 4096 到 4294967295 字节。

［默认取值］

内存缓存默认值：1048576 字节。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# logging configuration to syslog
```

logging content [hostname | username]

设置流量日志是否显示主机名称或用户名称。使用该命令 no 的形式取消显示主机名称或用户名称。

［命令］

logging content [hostname | username]

no logging content [hostname | username]

［句法描述］

hostname	在流量日志中显示主机名称
username	在流量日志中显示用户名称

［默认取值］

默认情况下，流量日志中不显示主机名称和用户名称。

［命令模式］

全局配置模式。

［使用指导］

配置 NetBIOS 名字解析功能是流量日志中主机名称显示的前提条件。。

［命令实例］

hostname(config)# **logging content hostname**

hostname(config)# **logging content username**

logging debug to

指定调试日志信息的输出目的地。使用该命令 no 的形式关闭相关的输出功能。

［命令］

logging debug to {console | syslog}

logging debug to buffer [size *buffer-size*]

no logging debug to {console | syslog}

no logging debug to buffer

［句法描述］

console	指定将流量日志信息输出到 console 口。
syslog	指定将流量日志信息输出到 Syslog 服务器。
buffer	指定将调试日志信息输出到内存缓存。
buffer-size	将流量日志信息输出到内存缓存时，该参数用来指定内存缓存的大小。范围是 4096 到 4294967295 字节。

［默认取值］

内存缓存默认值：1048576 字节。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **logging debug to buffer size 4194304**

logging email to

配置事件日志信息邮件提醒功能使用的接收日志信息邮件的 email 地址。使用该命令 no 的形式取消对 email 地址的指定。

［命令］

logging email to *email-address* **smtp** *smtp-instance*

no logging email to *email-address*

［句法描述］

email-addres	指定接收日志信息邮件的 email 地址。
smtp-instance	指定 email 地址的 SMTP 实例（必须为系统中已经配置成功的 SMTP 实例）。

［默认取值］

无默认值。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **logging email to test@hillstonenet.com smtp test-smtp-name**

logging event to

指定流量日志信息的输出目的地。使用该命令 no 的形式关闭相关的输出功能。

［命令］

logging event to {**console** | **remote** | **syslog**| **email**} [**severity** *severity-level*]

logging event to buffer [**size** *buffer-size*] [**severity** *severity-level*]

logging event to file [**name** {**usb0** | **usb1**} *file-name*] [**size** *file-size*] [**severity** *severity-level*]

no logging event to {**console** | **remote** | **syslog**| **email**}

no logging event to buffer

no logging event to file

［句法描述］

console	指定将流量日志信息输出到 console 口。
syslog	指定将流量日志信息输出到 Syslog Server。
buffer	指定将流量日志信息输出到内存缓存。
email	使用安全日志 email 提醒功能。
usb0 | **usb**	指定保存日志信息的 U 盘。
file-name	指定存储到 U 盘的日志信息文件名称。
severity-level	指定输出的告警日志信息的级别从而对告警日志信息进行过滤。
file-size	指定日志信息文件大小。范围是 4096 到 4294967295 字节。
buffer-size	将流量日志信息输出到内存缓存时，该参数用来指定内存缓存的大小。范围是 4096 到 4294967295 字节。

［默认取值］

内存缓存默认值：1048576 字节；

日志信息文件大小默认值：1048576 字节。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **logging event to file**

logging network to

指定流量日志信息的输出目的地。使用该命令 no 的形式关闭相关的输出功能。

［命令］

logging network to {**console** | **syslog**}

logging network to buffer [**size** *buffer-size*]

no logging network to {**console** | **syslog**}

no logging network to buffer

［句法描述］

console	指定将流量日志信息输出到 console 口。
syslog	指定将流量日志信息输出到 Syslog Server。
buffer	指定将流量日志信息输出到内存缓存。
buffer-size	将流量日志信息输出到内存缓存时，该参数用来指定内存缓存的大小。范围是 4096 到 4294967295 字节。

［默认取值］

内存缓存默认值：1048576 字节。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **logging network to syslog**

logging facility

当把日志信息输出到 UNIX Syslog 服务器时，需要用该命令为 Syslog 服务器指定场所。使用该命令 no 的形式取消对场所的指定。

［命令］

logging facility local*x*

no logging facility

［句法描述］

local*x*	指定场所。*x* 的取值范围是 0 到 7。

［默认取值］

7。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **logging facility local5**

logging security to

指定流量日志信息的输出目的地。使用该命令 no 的形式关闭相关的输出功能。

［命令］

logging security to {console | remote | syslog| email}

logging security to buffer [size *buffer-size*]

logging security to file [name {usb0 | usb1} *file-name*] **[size** *file-size*]

no logging security to {console | remote | syslog| email}

no logging security to buffer

no logging security to file

［句法描述］

console	指定将流量日志信息输出到 console 口。
syslog	指定将流量日志信息输出到 Syslog Server。
buffer	指定将流量日志信息输出到内存缓存。
email	使用安全日志 email 提醒功能。
usb0 | usb	指定保存日志信息的 U 盘。
file-name	指定存储到 U 盘的日志信息文件名称。
file-size	指定日志信息文件大小。范围是 4096 到 4294967295 字节。
buffer-size	将流量日志信息输出到内存缓存时，该参数用来指定内存缓存的大小。范围是 4096 到 4294967295 字节。

［默认取值］

内存缓存默认值：1048576 字节；

日志信息文件大小默认值：1048576 字节。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **logging security to console**

logging sms

当配置告警日志信息以短信的形式输出到某个手机时，需要用该命令指定接收告警日志的手机号码。使用该命令 no 的形式取消指定手机号码。

［命令］

logging sms *phone-number*

no logging sms *phone-number*

［句法描述］

phone-number	指定告警日志信息输出的手机号码。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **logging sms 13810001100**

logging syslog

配置 Syslog Server 的 IP 地址或主机名称，也可以根据需要配置日志服务器的 VRouter 名称、UDP 或 TCP 的端口号。使用该命令 no 的形式取消对 Syslog 服务器的配置。

［命令］

logging syslog {*ip-address* | *hostname*} {**tcp** *port-number* | **udp** *port-number* | **vrouter** *vr-name* {**tcp** *port-number* | **udp** *port-number*}} [**type** *log-type*]

no logging syslog {*ip-address* | *hostname*} {**tcp** *port-number* | **udp** *port-number* | **vrouter** *vr-name* {**tcp** *port-number* | **udp** *port-number*}}[**type** *log-type*]

［句法描述］

ip-address | *hostname*	指定 Syslog 服务器的 IP 地址或主机名称。
tcp *port-number*	指定 TCP 端口号。
udp *port-number*	指定 UDP 端口号。
vrouter *vr-name*	指定 Syslog 服务器的 VRouter 的名称。

type *log-type*	指定日志信息类型。如果配置该参数，只有指定类型的日志信息会输出到该系统日志服务器。

［默认取值］

无默认值。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **logging syslog 192.168.1.1 tcp 32**

logging traffic to

指定流量日志信息的输出目的地。使用该命令 no 的形式关闭相关的输出功能。

［命令］

logging traffic to {console | syslog}

logging traffic to buffer [size *buffer-size***]**

no logging traffic to {console | syslog}

no logging traffic to buffer

［句法描述］

console	指定将流量日志信息输出到 console 口。
syslog	指定将流量日志信息输出到 Syslog Server。
buffer	指定将流量日志信息输出到内存缓存。
buffer-size	将流量日志信息输出到内存缓存时，该参数用来指定内存缓存的大小。范围是 4096 到 4294967295 字节。

［默认取值］

内存缓存默认值：1048576 字节。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# logging traffic to syslog
```

match

该命令用于配置角色映射条目。使用该命令 no 的形式删除指定的映射条目。

［命令］

match {**any** | **user** *user-name* | **user-group** *user-group-name*} **role** *role-name*

no match {**any** | **user** *user-name* | **user-group** *user-group-name*} **role** *role-name*

［句法描述］

any	指定映射条目中的用户或用户组为系统中的任何用户或者用户组。
user-name	指定映射条目中的用户名称。
user-group-name	指定映射条目中的用户组名称。
role-name	指定映射条目中的角色名称。

［默认取值］

无默认值。

［命令模式］

角色映射规则配置模式。

［使用指导］

配置多条该命令添加多个映射条目。系统最多支持 64 条角色映射规则，每个规则中最多可以包含 256 条映射条目。

［命令实例］

```
hostname(config)# role-mapping-rule rule1
hostname(config-role-mapping)# match user user1 role role1
```

member

为用户组添加成员，用户组成员可以是用户或者其它的用户组。

［命令］

member {**user** *user-name* | **group** *user-group-name*}

no member {**user** *user-name* | **group** *user-group-name*}

［句法描述］

user-name	指定用户名称。
user-group-name	指定用户组的名称。系统支持的用户组的嵌套层数最多为 5 层，并且不支持回环嵌套，用户组不可以再嵌套它所属的用户组。

［默认取值］

无默认值。

［命令模式］

用户组配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# aaa-server local
hostname(config-aaa-server)# user-group group1
hostname(config-user-group)# member user1
```

monitor

配置系统监控报警功能时，进入监控配置模式。

［命令］

monitor

［句法描述］

无

［默认取值］

无默认值。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# monitor
hostname(config-monitor)#
```

nbt-cache enable

开启安全域的 NetBIOS 主机名查询功能。使用该命令 no 的形式关闭该功能。

［命令］

nbt-cache enable

no nbt-cache enable

［句法描述］

无。

［默认取值］

禁用。

［命令模式］

安全域配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **zone trust**

hostname(config)# **nbt-cache enable**

---

nbtstat ip2name

指定主机的 IP 地址，实时查看该主机的 NetBIOS 主机名称和 MAC 地址。

［命令］

nbtstat ip2name *ip-address* [**vrouter** *vrouter-name*]

［句法描述］

ip-address	指定被查询的主机的 IP 地址。
vrouter *vrouter-name*	指定被查询的主机所属的 VR 名称。如果没有指定 VR，系统使用默认 VR，即 trust-vr。

［默认取值］

无默认值。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# nbtstat ip2name 10.101.25.3 vrouter trust-vr
```

ntp authentication

在安全网关上启用 NTP 身份验证功能。使用该命令 no 的形式关闭 NTP 身份验证功能。

［命令］

```
ntp authentication
no ntp authentication
```

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# ntp authentication
```

ntp authentication-key

配置 NTP 身份验证功能。使用 NTP 身份验证功能，用户需要配置 MD5 身份验证密钥，并指定可信密钥。启动该功能后，安全网关只会与能够提供相匹配的可信密钥的服务器进行同步。使用该命令 no 的形式取消验证密钥的配置。

［命令］

ntp authentication-key *number* **md5** *string*

no ntp authentication-key *number*

［句法描述］

number	指定验证密匙的 ID，范围是从 1 到 65535。
string	指定 MD5 验证密码，范围是 1 到 32 个字符。

［默认取值］

无默认值。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **ntp authentication-key 111 md5 abcd**

---

ntp enable

在安全网关上启用 NTP 功能。使用该命令 no 的形式关闭 NTP 功能。

［命令］

ntp enable

no ntp enable

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **ntp enable**

---

ntp max-adjustment

配置最大调整时间。如果安全网关和 NTP 时钟服务器的时间差在最大调整时间之内，就能成功进行时间同步，否则不做同步。使用该命令 no 的形式恢复最大调整时间的默认值。

［命令］

ntp max-adjustment *number*

no ntp max-adjustment

［句法描述］

number	最大调整时间值，范围是 0 到 3600 秒，0 表示没有时间限制。

［默认取值］

10 秒。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **ntp max-adjustment 30**

ntp query-interval

配置查询间隔。安全网关每隔一个查询间隔就与时钟服务器做一次同步，如果时钟服务器时间改变，安全网关能够及时更新时间确保与时钟服务器同步。

［命令］

ntp query-interval *time-interval*

［句法描述］

time-interval	查询间隔值，范围是 1 到 60 分钟。

［默认取值］

5 分钟。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **ntp query-interval 20**

ntp server

配置 NTP 时钟服务器。

［命令］

ntp server {*ip-address* | *host-name*} [**key** *number*] [**source** *interface-name*] [**prefer**]

［句法描述］

ip-address | *host-name*	指定时钟服务器的 IP 地址或主机名称。
key *number*	指定可以通过该服务器的验证密匙。如果要在配置的时钟服务器上使用 NTP 身份验证功能，用户必须指定 **key** 参数值。
interface-name	指定安全网关上发送和接收 NTP 包的接口。
prefer	如果指定了多个时钟服务器，该关键字用来指定该服务器为主时钟服务器。安全网关首先与主服务器进行时间同步，如果失败，再查找下一个时钟服务器。

［默认取值］

无默认值。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **ntp server 10.160.64.5 prefer**

password

指定本地管理员的密码。

［命令］

password *password*

［句法描述］

password	指定本地管理员的密码。

［默认取值］

无。

［命令模式］

管理员配置模式。

［使用指导］

该密码的设定需要遵循系统的密码策略。

［命令实例］

```
hostname(config-admin)# password Hillstone12
```

password（user）

指定用户的密码。

［命令］

password *password*

［句法描述］

password	指定用户的密码。

［默认取值］

无。

［命令模式］

用户配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-aaa-server)# user user1
hostname(config-user)# password 123456
```

password-policy

进入管理员密码策略配置模式。

［命令］

password-policy

［句法描述］

无。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config-admin)# **password-policy**

---

ping

检查网络连接及主机是否可达。

［命令］

ping {*ip-address* | *hostname*}[**count** *number*] [**size** *number*] [**source** *ip-address*] [**timeout** *time*] [**vrouter** *vrouter-name*]

［句法描述］

ip-address	指定需要检查的 IP 地址。
hostname	指定需要检查的主机名称。
Count *number*	指定发送 Ping 包的个数。范围是 1 到 65536。默认情况下，系统不限制发送 Ping 包的个数。
size *number*	指定发送 Ping 包的大小。范围是 28 到 65535 字节（byte）。
source *ip-address*	指定发送 Ping 包的源地址，可以是接口的 IP 地址也可以是接口名称。
timeout *time*	指定发送 Ping 包的超时时间。范围是 0 到 3600 秒。默认值是 0，即没有超时时间限制。
vrouter *vrouter-name*	指定发送 Ping 包的出接口所属的 VRouter。默认为缺省 VR，即 trust-vr。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname(config)# **ping 10.200.3.1**

```
Sending ICMP packets to 10.200.3.1
   Seq     ttl     time(ms)
   1       128     0.865
   2       128     0.584
   3       128     0.572
   4       128     0.574
   5       128     0.573
   6       128     0.546
   7       128     0.590
statistics:
7 packets sent, 7 received, 0% packet loss, time 5999ms
rtt min/avg/max/mdev = 0.546/0.614/0.865/0.107 ms
```

privilege

配置管理员的优先级。使用该命令 no 的形式恢复管理员的默认权限。

［命令］

privilege {RX | RXW | ip-mac RXW}

no privilege

［句法描述］

RX	管理员具有查看安全网关配置和执行已有配置的权限。
RXW	管理员具有查看安全网关配置、执行已有配置和对安全网关进行配置的权限。
ip-mac RXW	管理员具有读权限以及 IP-MAC 配置的写权限（不可进行其它功能的配置）。

［默认取值］

RX 为管理员的默认权限。

［命令模式］

管理员配置模式。

［使用指导］

无。

［命令实例］

hostname(config-admin)# **privilege RXW**

reboot

重启安全网关。

［命令］

reboot

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

执行模式。

［使用指导］

执行 reboot 命令时，系统首先会提示用户是否保存所做的配置。请谨慎使用该命令，因为 reboot 命令会导致网络工作在短时间内瘫痪。

［命令实例］

hostname# **reboot**

require

指定许可证的时限和使用的平台。

［命令］

require {duration-time [*number* **years | always] | support-platform** *platform-name* **| demo-time {default | 1-month | 3-month | 6-month | 1-year}}**

［句法描述］

duration-time [*number* **years	always]**	指定所申请许可证的使用期限。*number* **years** 指定可以使用多少年，取值范围是 1 到 10 年；**always** 为永久有效。
support-platform *platform-name*	当前使用的平台。
**demo-time {default	1-month	3-month	6-month	1-year}**	该参数为试用许可证专用。用来指定所申请的使用许可证的使用期限，分别是默认（**default**，即为三个月）、一个月（**1-month**）、三个月（**3-month**）、六个月（**6-**

	month）和一年（**1-year**）。

［默认取值］

无默认值。

［命令模式］

许可证申请配置模式。

［使用指导］

无。

［命令实例］

hostname(apply-license)# **require duration-time 2 years**

role

创建角色。使用该命令 no 的形式删除指定的角色。

［命令］

role *role-name*

no role *role-name*

［句法描述］

role-name	指定角色名称。

［默认取值］

无默认值。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **role role1**

role-expression

安全网关支持角色组合，即通过逻辑运算重新组合已有角色。该命令配置角色组合。使用该命令 no 的形式删除指定的角色表示式。

［命令］

role-expression [**not**] *r1* [{**and** | **or**} [**not**] *r2*] **role** *r3*

no role-expression [**not**] *r1* [{**and** | **or**} [**not**] *r2*] **role** *r3*

［句法描述］

[**not**] *r1*	指定表达式中的第一个角色。**not** 表示“非”； *r1* 为系统中已创建的角色名称。例如，**not testrole1** 表示的结果为非 testrole1 以外的所以角色。
and | **or**	指定运算符符号。**and** 表示“和”；**or** 表示“或”。
[**not**] *r2*	指定表达式中的第二个角色。**not** 表示“非”； *r2* 为系统中已创建的角色名称。
role *r3*	指定角色运算的结果角色。**role** 关键字为推导符，*r3* 为结果角色名称。

［默认取值］

无默认值。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **role-expression role1 and role2 role role3**

role-mapping-rule

角色映射规则表达指定角色与用户或者用户组的映射关系。该命令用于创建角色映射规则。执行该命令后，系统创建指定名称的角色映射规则，并且进入角色映射规则配置模式。如果指定的名称已存在，则直接进入角色映射规则配置模式。使用该命令 no 的形式删除指定的角色映射规则。

［命令］

role-mapping-rule *rule-name*

no role-mapping-rule *rule-name*

［句法描述］

rule-name	指定角色映射规则的名称。

［默认取值］

无默认值。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# role-mapping-rule rule1
hostname(config-role-mapping)#
```

rollback configuration saved

回退到已保存的指定的起始配置信息。系统重启后，系统将会使用该命令指定的配置信息。

［命令］

rollback configuration saved {*number*}

［句法描述］

number	备份起始配置信息的数字标记。

［默认取值］

无默认值。

［命令模式］

全局配置模式。

［使用指导］

系统重启后生效。

［命令实例］

```
hostname(config)# rollback configuration saved 2
```

save

保存安全网关的当前配置。

［命令］

save [*string*]

［句法描述］

string	对所保存信息的描述。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

如果不使用 *string* 对保存的配置文件进行描述，系统会直接覆盖原有配置文件。

［命令实例］

hostname# **save** *room1*

---

smtp

配置 SMTP 实例。使用该命令 no 的形式删除指定的 SMTP 实例。

［命令］

smtp name *smtp-name* **server** {*ip-address* | *hostname*} {**from** *email-addr* | **vrouter** *vr-name* **from** *email-addr*}[**username** *user-name* **password** *password*]

no smtp name *smtp-name*

［句法描述］

smtp-name	指定 SMTP 实例的名称。
ip-address	指定 SMTP 服务器的 IP 地址。
hostname	指定 SMTP 服务器的主机名称。
email-addr	指定发件人地址。
vr-name	指定 SMTP 服务器的 VRouter 的名称。
user-name	指定发件人帐号的用户名。
password	指定发件人帐号的密码。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# smtp name smtp1 server 192.168.1.2 from
kkang@hillstonenet.com
```

snmp-server contact

配置 SNMP 管理员的标识及联系方法。使用该命令 no 的形式删除该系统联系信息。

［命令］

snmp-server contact *string*

no snmp-server contact

［句法描述］

string	描述系统联络信息的字符串。

［默认取值］

无默认值。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# snmp-server contact abcd
```

snmp-server engineID

配置本地设备的 SNMP 引擎 ID。

［命令］

snmp-server engineID *string*

［句法描述］

string	指定引擎 ID 号。取值范围为 1 到 23 个字符。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

SNMP 引擎 ID 唯一标识一个引擎，SNMP 引擎是 SNMP 实体（网络管理平台或者被管理网络设备）的重要组成部分，完成 SNMP 消息的收发、验证、提取 PDU、组装消息与 SNMP 应用程序通信等功能。

［命令实例］

hostname(config)# **snmp-server engineID 10**

snmp-server group

配置 SNMPv3 用户组。使用该命令 no 的形式删除指定的用户组。

［命令］

snmp-server group *group-name* **v3 {noauth | auth | auth-enc} [read-view** *read-view*] [**write-view** *writeview*]

no snmp-server group *group-name*

［句法描述］

group-name	定用户组的名称。取值范围为 1 到 31 个字符。
noauth | auth | auth-enc	指定用户组的定安全级别。可以为 noAuth、Auth 或者 Auth-Enc。安全级别决定了在处理一个 SNMP 数据包时所采用的安全机制。noAuth 即无认证和加密；Auth 提供基于 MD5 或 SHA 算法的认证；Auth-Enc 提供基于 MD5 或 SHA 算法的认证和基于 AES 和 DES 的报文加密。
read-view *read-view*	指定该用户组的只读 MIB 视图名。如不指定该参数，系统默认为所有视图均为该用户组的只读 MIB 视图。
write-view *writeview*	指定该用户组的可写 MIB 视图名。如不指定该参数，系统默认为所有视图均为该用户组的可写 MIB 视图。

［默认取值］

无默认值。

［命令模式］

全局配置模式。

［使用指导］

系统最多允许配置 5 个用户组，且每个用户组最多可包含 5 个用户。

［命令实例］

hostname(config)# **snmp-server group group1 v3 auth**

snmp-server host

配置 SNMP 管理主机地址。使用该命令 no 的形式删除指定的管理主机。

［命令］

snmp-server host {*host-name* | *host-ip*} {**version** [*1* | *2c*] **community** *string* [**ro** | **rw**] | **version** *3*}

no snmp-server host {*host-name* | *host-ip*}

［句法描述］

host-name | *host-ip*	指定管理主机的名称或者 IP 地址。
1 | **2c**	指定 SNMP 的版本为 SNMPv1 或者 SNMPv2C。
string	团体字是管理进程和代理进程之间的口令，因此与安全网关认可的团体字不符的 SNMP 报文将被丢弃。该参数指定主机的团体字，取值范围为一个最多 31 位的字符串，且仅当 SNMP 为 v1 和 v2C 版本时有效。
ro | **rw**	定该团体字的读写权限。ro 为只读，此类团体字只可读取 MIB 中的信息；rw 为可读可写，此类团体字不仅可以读取 MIB 中的信息，还可以对信息进行修改。此项为可选，默认情况下，团体字的访问权限为只读。
version *3*	指定 SNMP 的版本为 SNMPv3。

［默认取值］

无默认值。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **snmp-server host 1.1.1.1 version 2c community public**

snmp-server location

指定安全网关的位置。使用该命令 no 的形式删除系统位置信息。

［命令］

snmp-server location *string*

no snmp-server location

［句法描述］

string	描述安全网关位置的字符串。

［默认取值］

无默认值。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **snmp-server location abcd**

snmp-server manager

开启安全网关的 SNMP 功能。使用该命令 no 的形式关闭 SNMP 功能。

［命令］

snmp-server manager

no snmp-server manager

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **snmp-server manager**

snmp-server port

配置 SNMP 代理设备端口号。

［命令］

snmp-server port *port-number*

［句法描述］

port-number	指定 SNMP 代理设备的端口号。范围为 1 到 65535。

［默认取值］

161。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **snmp-server port 11161**

snmp-server trap-host

为 SNMP 功能配置 trap 报文主机，配置内容包括主机 IP 地址和 SNMP 版本号。使用该命令 no 的形式删除指定的目标主机。

［命令］

snmp-server trap-host {*host-name* | *host-ip*} {**version** {*1* | *2c*} **community** *string* | **version** *3* **user** *user-name* **engineID** *string*} [**port** *port-number*]

no snmp-server trap-host {*host-name* | *ip-address*}

［句法描述］

host-name | *host-ip*	指定 trap 报文目标主机的主机名称或者 IP 地址。
version {*1* | *2c*}	指定使用 SNMPv1 或者 SNMPv2C 发送 trap 报文。
community *string*	指定 SNMPv1 或者 SNMPv2C 的团体字。
version *3*	指定使用 SNMPv3 发送 trap 报文。
user *user-name*	指定已配置的 SNMPv3 用户名。
engineID *string*	指定 trap 报文目标主机的引擎 ID 号。
port *port-number*	指定接收 trap 报文的目标主机端口号。取值范围为 1 到 65535。

［默认取值］

port-number - 162。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **snmp-server trap-host 1.1.1.1 version 2c community public**

---

snmp-server user

配置 SNMPv3 用户。使用该命令 no 的形式删除指定的用户。

［命令］

snmp-server user *user-name* **group** *group-name* **v3 remote** *remote-ip* [**auth-protocol** {**md5** | **sha**} *auth-pass* [**enc-protocol** {**des** | **aes**} *enc-pass*]]

no snmp-server user

［句法描述］

user-name	指定用户名称。取值范围为 1 到 31 个字符。
group-name	为所创建的用户指定已经配置好的用户组。
remote-ip	指定远程管理主机的 IP 地址。
auth-protocol {**md5** | **sha**}	指定用户安全级别为需要认证且认证协议可以为 MD5 或 SHA 算法。如不输入此参数，则默认是无认证，无加密模式。
auth-pass	指定认证密码。取值范围为 8 到 40 个字符。
enc-protocol {**des** | **aes**}	指定用户安全级别为加密且加密协议为 DES 或者 AES。
enc-pass	指定加密密码。取值范围为 8 到 40 个字符。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

系统最多允许配置 25 个用户。

［命令实例］

hostname(config)# **snmp-server user user1 group group1 v3 remote 1.1.1.1 auth md5 11111111 enc aes aaaaaaaa**

statistics-set

创建统计集并进入统计集配置模式。如果指定名称的统计集已存在，则直接进入统计集配置模式。使用该命令 no 的形式删除指定的统计集。

［命令］

statistics-set *name*

no statistics-set *name*

［句法描述］

name	指定统计集名称，范围为 1 到 31 个字符。

［默认取值］

关闭。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# statistics-set set1
hostname(config-statistic-set)#
```

ssh port

配置 SSH 端口号。使用该命令 no 的形式恢复 SSH 默认端口号。

［命令］

ssh port *port-number*

no ssh port

［句法描述］

port-number	指定 SSH 端口号。范围是 1 到 65535。

［默认取值］

22。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **ssh port 2222**

ssh timeout

配置 SSH 超时时间。使用该命令 no 的形式恢复 SSH 超时默认值。

［命令］

ssh timeout *timeout-value*

no ssh timeout

［句法描述］

timeout-value	指定 SSH 超时时间，范围是 1 到 60 分钟。

［默认取值］

10 分钟。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **ssh timeout 20**

tcp

配置 TCP 报文目标监测条目。使用该命令 no 的形式删除指定的监测条目。

［命令］

tcp {*A.B.C.D* | **host** *host-name*} **port** *port-number* **interface** *interface-name* [**interval** *value*] [**threshold** *value*] [**weight** *value*] [**src-interface** *interface-name*]

no tcp {*A.B.C.D* | **host** *host-name*} **port** *port-number* **interface** *interface-name*

［句法描述］

A.B.C.D | **host** *host-name*	指定监测目标的 IP 地址或者主机名称。
port *port-number*	指定监测目标的目的端口号。取值范围为 0 到 65535。
interface *interface-name*	指定发送 TCP 检测报文的出接口。
interval *value*	指定发送 TCP 报文的时间间隔，单位为秒。范围是 1 到 255 秒。
threshold *value*	指定判断监测失败的警戒值。如果系统连续未收到该参数指定个数的响应报文，就判断为监测失败，即目标不可达。取值范围是 1 到 255。
weight *value*	指定该条监测失败对整个监测对象失败贡献的权重值。取值范围是 1 到 255。
src-interface *interface-name*	指定 TCP 检测报文的源接口。

［默认取值］

interval *value* – 3 秒。

threshold *value* – 1。

weight *value* – 255。

［命令模式］

监测对象配置模式。

［使用指导］

用户可以配置多条该命令为监测对象指定多个监测条目。

对于同一个监测对象，不能同时配置对同一目标主机的 HTTP 监测和对端口 80（port 80）的 TCP 监测。

［命令实例］

hostname(config)# **track trackobj1**

hostname(config-trackip)# **tcp 1.1.1.1 port 118 interface ethernet0/3**

network-manager enable

开启设备的 HSM 代理功能以实现设备与服务器的正常连接。使用该命令 no 的形式关闭 HSM 代理功能。

［命令］

network-manager enble

no network-manager enble

［句法描述］

无。

［默认取值］

开启。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **no network-anager enable**

---

network-manager host

配置 HSM 服务器的 IP 地址、连接端口号和访问密码。使用该命令 no 的形式取消 HSM 服务器管理参数配置。

［命令］

network-manager host {*ip-address* | **port** *port-number* | **password** *password*}

no network-manager host

［句法描述］

ip-address	指定 HSM 服务器的 IP 地址。此 IP 地址不能为“0.0.0.0”、“255.255.255.255”以及组播地址。
port-number	指定 HSM 服务器的连接端口号。范围是 1 到 65535。
password	指定 HSM 服务器的访问密码。服务器通过该密码对设备进行认证。范围是 1 到 31 个字符。

［默认取值］

port-number — 9090。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# network-manager host 1.1.1.1
hostname(config)# network-manager host password aaaaaa
```

target-data

配置统计数据类型（带宽、会话、新建会话速率、攻击速率、病毒个数、入侵次数、URL 命中次数、关键字阻断次数和应用阻断次数）。使用该命令 no 的形式取消指定统计集统计数据类型的配置

［命令］

target-data {bandwidth | session | rampup-rate | attack-rate | virus-num | intrusion | url-hit | keyword-block | application-block} [record-history]

no target-data

［句法描述］

bandwidth | session | rampup-rate | attack-rate | virus-num | intrusion | url-hit | keyword-block | application-block	指定统计集的统计数据类型。可以为带宽（**bandwidth**）、会话（**session**）、新建会话速率（**rampup-rate**）、攻击速率（**attack-rate**）、病毒个数（**virus-num**）、入侵次数（**intrusion**）或者 URL 命中次数（**url-hit**）、关键字阻断次数（**keyword-block**）或者应用阻断次数（**application-block**）。
record-history	记录最近 5 分钟和最近 24 小时内的统计数据。

［默认取值］

无默认值。

［命令模式］

统计集配置模式。

［使用指导］

- 病毒个数统计数据类型仅对安装有病毒过滤许可证的用户可用。
- 入侵次数统计数据类型仅对安装有 IPS 许可证的用户可用。
- URL 命中次数统计数据类型仅对安装有 URL 许可证的用户可用。

［命令实例］

```
hostname(config)# statistics-set set1
hostname(config-statistic-set)# target-data bandwidth record-history
```

telnet authorization-try-count

该命令指定 Telnet 最大登录次数，即允许用户连续失败登录的最大次数。如果连续登录失败次数超出该指定数值，系统将断开此次 Telnet 连接。使用该命令 no 的形式恢复 Telnet 默认登录次数。

［命令］

telnet authorization-try-count *count-number*

no telnet authorization-try-count

［句法描述］

count-number	指定最大连接次数。范围是 1 到 10 次。

［默认取值］

3 次。

［命令模式］

全局配置模式。

［使用指导］

使用 Telnet、SSH、HTTP 或者 HTTPS 方式登录设备时，如果在一分钟内连续三次登录失败，系统会将登录失败的 IP 地址锁定两分钟。被锁定的 IP 地址在两分钟内不能建立与设备的连接。

［命令实例］

hostname(config)# **telnet authorization-try-count 2**

telnet connection-interval

指定设备处理 SSH 连接的时间间隔。建立一个 SSH 连接后，在时间间隔过后，设备才接受下一个 SSH 连接请求。使用该命令 no 的形式恢复 SSH 连接默认端时间间隔。

［命令］

ssh connection-interval *interval-time*

no ssh connection-interval

［句法描述］

interval-time	指定时间间隔，单位是秒。范围是 2 到 3600 秒。

［默认取值］

2 秒。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **ssh connection-interval 10**

---

telnet port

配置 Telnet 端口号。使用该命令 no 的形式恢复 Telnet 默认端口号。

［命令］

telnet port *port-number*

no telnet port

［句法描述］

port-number	指定 Telnet 端口号。范围是 1 到 65535。

［默认取值］

23。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **telnet port 2323**

---

telnet timeout

配置 Telnet 超时时间。使用该命令 no 的形式恢复 Telnet 超时默认值。

［命令］

telnet timeout *timeout-value*

no telnet timeout

［句法描述］

timeout-value	指定 Telnet 超时时间，范围是 1 到 1440 分钟。

［默认取值］

10 分钟。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **telnet timeout 20**

threshold

当监测对象中失败的监测条目的权重值的总和大于一定值，系统就判断整个监测对象失败。该命令为监测对象指定警戒值。使用该命令 no 的形式恢复警戒值的默认值。

［命令］

threshold *value*

no threshold

［句法描述］

value	指定监测对象警戒值的大小。范围是 1 到 255。

［默认取值］

255。

［命令模式］

监测对象配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **threshold 10**

traceroute

测试数据包从发送主机到目的地所经过的网关，检查网络连接是否可达，以及分析网络什么地方发生了故障。

［命令］

traceroute {*IP-address* | *hostname*} [**numberic**] [**port** *port-number*] [**probe** *probe-number*] [**timeout** *time*] [**ttl** [*min-ttl*] [*max-ttl*]] [**source** *interface*] [**use-icmp**] [**vrouter** *vrouter-name*]

［句法描述］

ip-address | *hostname*	指定 traceroute 命令的目的地址，可以是 IP 地址，也可以是主机名称。
numberic	指定用数字的方式显示地址。
port *port-number*	指定 UDP 端口号。范围是 1 到 65535。默认端口号为 33434。
timeout *time*	指定发送下一个探测包的超时时间。范围是 1 到 3600 秒。默认值是 5 秒。
ttl [*min-ttl*] [*max-ttl*]	*min-ttl* 用来指定最小 TTL 值，范围是 0 到 255，默认值是 1。*max-ttl* 用来指定最大 TTL 值，范围是 1 到 255，默认值是 30。
source *interface*	指定发送 traceroute 探测包的源地址，可以是接口的 IP 地址，也可以是接口名称。
use-icmp	指定使用 ICMP 包进行探测。如不配置该参数，系统将使用 UDP 包进行探测。
vrouter *vrouter-name*	指定发送 traceroute 探测包的出接口所属的 VRouter。默认为缺省 VRouter，即 trust-vr。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# traceroute 210.74.176.150
traceroute to 210.74.176.150 (210.74.176.150), 30 hops max, 52 byte
packets
 1  10.200.3.1 (10.200.3.1)  0.572 ms  0.541 ms  0.359 ms
 2  192.168.3.1 (192.168.3.1)  0.601 ms  0.754 ms  0.522 ms
```

```
 3  202.106.149.177 (202.106.149.177)  1.169 ms  1.723 ms  1.104 ms
 4  61.148.16.133 (61.148.16.133)  2.272 ms  1.940 ms  2.370 ms
 5  61.148.4.17 (61.148.4.17)  2.770 ms 61.148.4.101 (61.148.4.101)
6.030 ms 61.148.4.21 (61.148.4.21)  2.584 ms
```

track

安全网关的监测功能能够监测指定的目标（IP 地址或者主机）是否可达或者接口的链路是否连通。监测功能用于 HA 以及接口监控。该命令用于创建监测对象。执行该命令后，系统创建指定名称的监测对象，并且进入监测对象配置模式；如果指定的名称已存在，则直接进入监测对象的配置模式。使用该命令 no 的形式删除指定的监测对象。

［命令］

track *tack-object-name*

no track *tack-object-name*

［句法描述］

tack-object-name	指定监测对象名称。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **track trackobj1**

user

StoneOS 中的用户（User）是指使用安全网关设备提供的功能、服务、被设备管理、认证的用户。该命令用于创建本地用户。执行该命令后，系统创建指定名称的用户并且进入用户配置模式；如果指定的用户名称已存在，则直接进入用户配置模式。

［命令］

user *user-name*

no user *user-name*

［句法描述］

user-name	指定用户名称。

［默认取值］

无。

［命令模式］

本地 AAA 服务器配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# aaa-server local
hostname(config-aaa-server)# user user1
```

user-binding

将 IP 地址或 MAC 地址绑定到用户。使用该命令 no 的形式取消将 IP 地址或 MAC 地址绑定到用户。

［命令］

user-binding *aaa-server-name user-name* {**ip** *ip-address* [**auth-check-only**]| **mac** *mac-address*} [**vrouter** *vr-name*]

no user-binding *aaa-server-name user-name* {**ip** *ip-address* | **mac** *mac-address*} [**vrouter** *vr-name*]

［句法描述］

aaa-server-name	指定用户所属的 AAA 服务器名称。
user-name	指定用户名称。
ip *ip-address*	指定 IP 地址。
auth-check-only	配置了该参数后，系统在对用户进行认证之前将会先检查该用户 IP 地址的合法性，即检查是否与该用户绑定的 IP 地址一致。如果一致，则允许对用户进行认证。
mac *mac-address*	指定 MAC 地址。
vrouter *vr-name*	指定 IP 地址或 MAC 地址所属的 VRouter 的名称。默认为缺省 VR，即 trust-vr。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **user-binding local shanghai ip 10.10.0.1**

user-group

创建本地用户组。执行该命令后，系统创建指定名称的用户组并且进入用户组配置模式；如果指定的用户组名称已存在，则直接进入用户组配置模式。

［命令］

user-group *user-group-name*

no user-group *user-group-name*

［句法描述］

user-group-name	指定用户组名称。

［默认取值］

无。

［命令模式］

本地 AAA 服务器配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **aaa-server local**

hostname(config-aaa-server)# **user-group group1**

webauth force-timeout

配置强制用户重新登录时间。系统可以通过设置强制用户重新登录时间，使用户在指定的时间过后必须重新登录。使用该命令 no 的形式恢复默认配置。

［命令］

webauth force-timeout *timeout-value*

no webauth force-timeout

［句法描述］

timeout-value	指定用户重新登录的时间间隔，单位为分钟。范围为 10 到 60*24*100 分钟。

［默认取值］

默认情况下，系统不强制用户重新登录。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **webauth force-timeout 60**

webauth http

开启 HTTP 模式 Web 认证方式。使用该命令 no 的形式关闭系统的 Web 认证功能。

［命令］

webauth http

no webauth

［句法描述］

无关键数和参数。

［默认取值］

关闭。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **webauth http**

webauth http-port

指定认证服务器的 HTTP 的端口号。使用该命令 no 的形式恢复默认 HTTP 端口号。

［命令］

webauth http-port *port-number*

no webauth http-port

［句法描述］

port-number	指定认证服务器的 HTTP 端口号。取值范围是 1 到 65535。

［默认取值］

8181。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **webauth http-port 8081**

webauth https

开启 HTTPS 模式 Web 认证方式。使用该命令 no 的形式关闭系统的 Web 认证功能。

［命令］

webauth https

no webauth

［句法描述］

无关键数和参数。

［默认取值］

关闭。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# webauth https
```

webauth https-port

指定认证服务器的 HTTPS 的端口号。使用该命令 no 的形式恢复默认 HTTPS 端口号。

［命令］

webauth https-port *port-number*

no webauth https-port

［句法描述］

port-number	指定认证服务器的 HTTPS 端口号。取值范围是 1 到 65535。

［默认取值］

44433。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# webauth https-port 44400
```

webauth reauth

配置用户重认证的时间间隔。当用户认证成功并访问网络后，系统可以对用户进行重认证。使用该命令 no 的形式恢复默认值。

［命令］

webauth reauth *time*

no webauth reauth

［句法描述］

time	指定用户进行重认证的时间间隔，单位为分钟。范围为 10 到 60*24 分钟。

［默认取值］

默认情况下，系统不对用户进行重认证。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **webauth reauth 60**

webauth redirect

配置重定向 URL 功能。重定向 URL 是指用户在认证成功并返回认证页面后，弹出的新页面将会重定向到指定的 URL 页面。如果没有配置该功能，新弹出页面将返回用户输入的地址页面。使用该命令 no 的形式取消指定重定向 URL。

［命令］

webauth redirect *url*

no webauth redirect

［句法描述］

url	指定重定向的 URL 的地址。范围为 1 到 127 个字符。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

该功能的正确执行需要浏览器关闭弹出窗口阻止程序。如果浏览器阻止弹出窗口，新弹出的页面将被阻止，需要手工确认才能打开。

［命令实例］

hostname(config)# **webauth redirect www.baidu.com**

webauth timeout

认证成功后，系统会在超时时间结束前对认证成功页面进行自动刷新，确认登录信息。该命令指定 Web 认证超时时间。使用该命令 no 的形式恢复默认超时时间。

［命令］

webauth timeout *timeout-value*

no webauth timeout

［句法描述］

timeout-value	指定超时时间，单位为秒。取值范围是 10 到 3600*24 秒。

［默认取值］

120 秒。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **webauth timeout 100**

web timeout

配置 WebUI 超时时间。使用该命令 no 的形式恢复 Web 超时默认值。

［命令］

web timeout *timeout-value*

no ssh timeout

［句法描述］

timeout-value	指定 WebUI 超时时间，范围是 1 到 1440 分钟。

［默认取值］

10 分钟。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **web timeout 20**

系统结构命令

deny-session deny-type

指定建立 Deny Session 的情况。

［命令］

deny-session deny-type {all | ad | policy | route | self | session-limit}

no deny-session deny-type {all | ad | policy | route | self | session-limit}

［句法描述］

all	系统支持的五种情况下均建立 Deny Session。
ad	当数据包未通过 AD（二层和三层 IP 地址欺骗攻击防护）检查时建立 Deny Session。
policy	当数据包未找到相匹配的策略规则或者匹配“拒绝”策略规则时建立 Deny Session。
route	当数据包找不到转发或者逆向路由时建立 Deny Session。
self	当到设备自身的数据包被拒绝时建立 Deny Session。
session-limit	当数据包超出设备配置的会话限制时建立 Deny Session。

［默认取值］

无。

［命令模式］

Flow 配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# flow
hostname(config-flow)# deny-session deny-type policy
```

deny-session percentage

指定最大 Deny Session 数。

［命令］

deny-session percentage *number*

no deny-session percentage

［句法描述］

percentage *number*	指定 Deny Session 数占系统最大 Session 数的百分比。范围是 0 到 10。0 表示关闭 Deny Session 功能。

［默认取值］

2。

［命令模式］

Flow 配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# flow
hostname(config-flow)# deny-session percentage 5
```

deny-session timeout

指定 Deny Session 的超时时间。

［命令］

deny-session timeout *time*

no deny-session timeout

［句法描述］

timeout *time*	指定超时时间，单位为秒。取值范围为 1 到 3 秒。

［默认取值］

3 秒。

［命令模式］

Flow 配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# flow
hostname(config-flow)# deny-session timeout 2
```

fragment chain

指定系统允许的每个 IP 的最大分片数。使用该命令 no 的形式恢复系统默认的最大分片数。

［命令］

fragment chain *number*

no fragment chain

［句法描述］

number	指定系统允许的每个 IP 包的最大分片数。取值范围是 1 到 1024。

［默认取值］

48。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# fragment chain 20
```

fragment timeout

指定分片重组超时时间。使用该命令 no 的形式恢复系统默认超时时间。

［命令］

fragment timeout *time*

no fragment timeout

［句法描述］

time	指定分片重组超时时间。取值范围是 1 到 30 秒。

［默认取值］

2 秒。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **fragment timeout 5**

tcp-mss

为所有的的 TCP SYN/ACK 包或者 IPSec VPN 的 TCP SYN/ACK 包指定 MSS 值。使用该命令 no 的形式，恢复默认 MSS 值。

［命令］

tcp-mss {all | ipsec-vpn} *size*

no tcp-mss {all | ipsec-vpn}

［句法描述］

all	为所有 TCP SNY 包指定 MSS 值。
ipsec-vpn	为 IPSec VPN 的 TCP SYN 包指定 MSS 值。
size	指定 TCP SNY 包的 MSS 值。范围是 64 到 65535。

［默认取值］

所有 TCP SYN/ACK 包的默认 MSS 值 – 1448；

IPSec VPN 的 TCP SYN/ACK 包包的默认 MSS 值 – 1380。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **tcp-mss all 2000**

tcp-seq-check-disable

TCP 包序列号检查功能。如果 TCP 序列号超出 TCP 窗口，该 TCP 包将会被丢弃。

［命令］

tcp-seq-check-disable

no tcp-seq-check-disable

［句法描述］

无。

［默认取值］

默认情况下，该功能为开启状态。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **tcp-seq-check-disable**

---

tcp-syn-check

指定 TCP 三次握手超时时间。如果在超时时间内，未完成三次握手，则断掉该连接。

［命令］

tcp-syn-check [*timeout-value*]

no tcp-syn-check

［句法描述］

timeout-value	指定三次握手的超时时间，单位为秒。范围是 1 到 1800 秒。

［默认取值］

20 秒。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **tcp-syn-check 30**

---

tcp-syn-bit-check

配置 TCP SYN 包检查功能。只有检查收到的包为 TCP SYN 包后，才建立连接。

［命令］

tcp-syn-bit-check

no tcp-syn-bit-check

［句法描述］

无。

［默认取值］

关闭。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **no tcp-syn-bit-check**

安全网关应用模式命令

exec vrouter enable/disable

开启或者关闭系统的多 VR 功能。

［命令］

exec vrouter enable

exec vrouter disable

［句法描述］

无。

［默认取值］

默认情况下，系统的多 VR 功能是关闭的，即除缺省 VR 外，用户不可以创建和使用其它的 VR。

［命令模式］

任何模式。

［使用指导］

执行以上命令后，需要重启设备才能相应地开启或者关闭多 VR 功能。设备重启后，系统的最大并发连接数会根据多 VR 功能的开启或者关闭状态减少 15%或者恢复正常。如果在开启多 VR 功能的同时开启病毒过滤功能（开启病毒过滤功能后，最大并发连接数将会减半），最大并发连接数会在已经减少的基础上再减少 15%。计算公式为“实际最大并发连接数=原始最大并发连接数*(1-0.15)*(1-0.5)”。

［命令实例］

```
hostname(config)# exec vrouter enable
Warning: please reboot the device to make the change validation!
```

ip vrouter

该命令用于创建一个 VRouter 并且进入 VRouter 配置模式。使用该命令 no 的形式删除指定的 VRouter。

［命令］

ip vrouter *vrouter-name*

no ip vrouter *vrouter-name*

［句法描述］

vrouter-name	指定将要创建的 VRouter 的名称。如果指定的名称已存在，则直接进入 VRouter 配置模式。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# ip vrouter vrouter1
hostname(config-vrouter)#
```

forward-tagged-packet

配置 VSwitch 的 VLAN 透传功能。

［命令］

forward-tagged-packet

no forward-tagged-packet

［句法描述］

无。

［默认取值］

关闭。

［命令模式］

VSwitch 配置模式。

［使用指导］

配置和使用 VSwitch 的 VLAN 透传功能时，

- 包含有子接口的 VSwitch 不能开启 VLAN 透传功能；
- 已经开启 VLAN 透传的 VSwitch 中的二层安全域不能绑定子接口；
- 经过透传的带有 VLAN ID 的数据包不支持三层混合模式传输。

［命令实例］

```
hostname(config)# vswitch vswitch1
hostname(config-vswitch)# forward-tagged-packet
hostname(config-vswitch)# exit
hostname(config)#
```

l2-nonip-action

配置安全网关对于非 IP 包且非 ARP 包的处理方式。

［命令］

l2-nonip-action {drop | forward}

［句法描述］

drop	丢弃。
forward	转发。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# l2-nonip-action drop
```

virtual-wire enable

开启 VSwitch 的 Virtual Wire 功能。使用该命令 no 的形式关闭 VSwitch 的 Virtual Wire 功能。

［命令］

virtual-wire enable [strict | unstrict]

no virtual-wire enable

［句法描述］

strict | unstrict	指定 Virtual Wire 模式，可以是 Strict（**strict**）或者 Non-Strict（**unstrict**）。

［默认取值］

Strict。

［命令模式］

VSwtich 配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# vswitch vswitch2
hostname(config-vswitch)# virtual-wire enable
```

virtual-wire set

该命令用来配置 Virtual Wire 接口对。使用该命令 no 的形式删除 Virtual Wire 接口对。

［命令］

virtual-wire set *interface-name1 interface-name2*

no virtual-wire set *interface-name1 interface-name2*

［句法描述］

interface-name1 interface-name2	指定 Virtual Wire 接口对。

［默认取值］

无。

［命令模式］

VSwtich 配置模式。

［使用指导］

同一个 Virtual Wire 接口对中的两个接口不可以相同，同一个接口不可以同时属于两个 Virtual Wire 接口对。

［命令实例］

```
hostname(config)# vswitch vswitch2
hostname(config-vswitch)# virtual-wire set aggregate1 ethernet0/2.1
```

vswitch

创建 VSwitch。在新建一个 VSwitch 的同时，也新建了与 VSwitch 相对应的 VSwitch 接口。执行该命令后，系统创建指定名称的 VSwith 和 VSwitch 接口，并且进入 VSwitch 配置模式；如果指定的名称已经存在，则直接进入 VSwitch 配置模式。使用该命令 no 的形式删除指定的 VSwitch。

［命令］

vswitch vswitch*Number*

no vswitch vswitch*Number*

［句法描述］

Number	为 VSwitch 的数字标识。*Number* 的取值范围根据平台不同而不同。例如，命令 **vswitch vswitch2** 创建了名为 VSwitch2 的 VSwitch，同时也创建了 VSwitchif2 接口。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

系统缺省 VSwitch 为 VSwitch1。用户不可以删除 VSwitch1。

［命令实例］

```
hostname(config)# vswitch vswitch2
hostname(config-vswitch)#
```

安全网关网络部署模式命令

tap control-interface

配置旁路控制接口。

［命令］

tap control-interface *interface-name*

no tap control-interface

［句法描述］

interface-name	指定接口名称。

［默认取值］

默认情况下，旁路控制接口为旁路接口本身。

［命令模式］

旁路接口配置模式。

［使用指导］

无。

［命令实例］

hostname(config-if-eth0/4)# **zone tap2**

hostname(config-if-eth0/4)# **tap control-interface ethernet0/0**

tap lan-address

指定内网地址，即统计集的统计范围，对于源 IP 不在指定内网地址范围的数据包，系统将不做统计。使用该命令 no 的形式取消统计范围的指定。

［命令］

tap lan-address *address-entry*

no tap lan-address

［句法描述］

address-entry	指定地址条目名称。通常情况下，该地址条目中应包含被统计设备上所有的内网地址。

［默认取值］

无。

［命令模式］

旁路接口配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-if-eth0/4)# zone tap2
hostname(config-if-eth0/4)# tap lan-address addr1
```

zone （绑定接口到Tap域）

将接口绑定到已定义的 Tap 域。绑定到 Tap 域的接口即为旁路接口，工作在旁路模式。

［命令］

zone *zone-name*

no zone

［句法描述］

zone-name	需要绑定到的域的名称。

［默认取值］

无。

［命令模式］

接口配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-if-eth0/2)# zone tap1
```

zone （创建Tap域）

创建 Tap 域。

［命令］

zone *zone-name* **tap**

no zone *zone-name*

［句法描述］

zone-name	域的名称。
tap	指定所创建的域为 Tap 域。Tap 域为旁路模式功能域。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

创建 Tap 域后，系统将自动生成一条源安全域和目的安全域均为该 Tap 域的策略规则。

如果一条策略规则的源安全域（或者目的安全域）为某 Tap 域，则其对应的目的安全域（或者源安全域）必须也为该 Tap 域。

［命令实例］

```
hostname(config)# zone tap1 tap
hostname(config-zone-tap1)#
```

域（Zone）命令

bind

将一个二层域绑定到所指定的虚拟交换机上。使用该命令 no 的形式取消绑定。

［命令］

bind *vswitch-name*

no bind *vswitch-name*

［句法描述］

vswitch-name	将域绑定到的虚拟交换机的名称。

［默认取值］

默认情况下，新建的二层域会绑定到 vswitch1（默认虚拟交换机）。

［命令模式］

域配置模式。

［使用指导］

该命令只适用于二层域。

［命令实例］

```
hostname(config)# zone myzone l2
hostname(config-zone)# bind vswitch2
hostname(config-zone)# exit
```

vrouter

默认情况下，所有的三层域都绑定到 trust-vr 中。该命令用来改变三层域的 VRouter。使用该命令 no 的形式恢复域到 trust-vr 的绑定。

［命令］

vrouter *vrouter-name*

no vrouter

［句法描述］

vrouter-name	指定将三层域绑定到的 VRouter 的名称。

［默认取值］

无。

［命令模式］

域配置模式。

［使用指导］

该命令只适用于三层域。

［命令实例］

```
hostname(config)# zone zone1
hostname(config-zone-zone1)# vrouter vrouter1
```

zone

创建一个域并且进入域配置模式。如果域已存在，则直接进入域配置模式。使用该命令 no 的形式删除指定域。

［命令］

zone *zone-name* [**l2** | **tap**]

no zone *zone-name*

［句法描述］

zone-name	域的名称。
l2	表示创建一个二层域。
tap	指定所创建的域为 Tap 域。Tap 域为旁路模式功能域。

［默认取值］

无默认值。

［命令模式］

全局配置模式。

［使用指导］

预定义域不可以被删除。

［命令实例］

```
hostname(config)# zone zone1 l2
hostname(config-zone-zone1)# exit
```

接口（Interface）命令

aggregate aggregate*number*

把一个物理接口添加到集聚接口中。使用该命令 no 的形式把接口分离出集聚接口。

［命令］

aggregate aggregate*number*

no aggregate

［句法描述］

number	用来标识集聚接口。

［默认取值］

无默认值。

［命令模式］

接口配置模式。

［使用指导］

添加物理接口时，必须保证被添加的物理接口不属于任何其它接口也不属于任何安全域。

［命令实例］

```
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# aggregate aggregate1
```

arp timeout

设置接口的 ARP 超时时间值，单位为秒。使用该命令 no 的形式恢复接口的默认 ARP 超时时间。

［命令］

arp timeout *value*

no arp timeout

［句法描述］

value	要指定的 timeout 的时间值，范围是 5 到 65535 秒。

［默认取值］

默认值是 1200 秒。

［命令模式］

接口配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# arp timeout 1800
```

authenticated-arp

配置 ARP 认证功能，保护客户端免受 ARP 欺骗攻击。使用该命令 no 的形式关闭接口的 ARP 认证功能。

［命令］

```
authenticated-arp [force]
no authenticated-arp
```

［句法描述］

force	如果配置该参数，所有通过该接口访问 Internet 的 PC 都需要安装 ARP 认证客户端 Hillstone Secure Defender，否则设备将拒绝其访问 Internet。如不配置该参数，ARP 认证功能只对安装了客户端的 PC 起效。

［默认取值］

无。

［命令模式］

接口配置模式。

［使用指导］

由于 Loopback 接口和 PPPoE 子接口不具有 ARP 学习功能，所以这两种接口不支持 ARP 认证。

［命令实例］

```
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# authenticated-arp force
```

bgroup bgroup*number*

将物理接口添加到 BGroup 接口。使用该命令 no 的形式把接口分离出 BGroup 接口。

［命令］

bgroup bgroup*number*

no bgroup

［句法描述］

number	用来标识 BGroup 接口。

［默认取值］

无默认值。

［命令模式］

接口配置模式。

［使用指导］

添加物理接口时，必须保证被添加的物理接口不属于任何其它接口也不属于任何安全域。

［命令实例］

hostname(config)# **interface ethernet0/2**

hostname(config-if-eth0/2)# **bgroup bgroup1**

clear mac

清除所有 VSwitch 中的或者某个指定接口的 MAC 表项。

［命令］

clear mac [**interface** *interface-name*]

［句法描述］

interface-name	可选。特定的接口名称。

［默认取值］

如果不指定接口名称，该命令会清除系统中所有 VSwitch 的 MAC 表项。

［命令模式］

执行模式。

［使用指导］

无。

［命令实例］

```
hostname# clear mac
```

combo

部分型号的安全网关配有 SFP 口+电口的 Combo 口。当 Combo 口的 SFP 口与电口均有线缆连接时，用户可以通过命令控制使用 SFP 口还是电口。使用该命令 no 的形式恢复 Combo 口的默认工作状态。

［命令］

combo {copper-forced | copper-preferred | fiber-forced | fiber-preferred}

［句法描述］

copper-forced	强制使用电口。
copper-preferred	优先使用电口。
fiber-forced	强制使用 SFP 口。
fiber-preferred	优先使用 SFP 口。

［默认取值］

无默认值。

［命令模式］

接口配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# combo copper-preferred
```

duplex

指定电口的工作方式。使用该命令 no 的形式恢复到默认工作方式。

［命令］

duplex {auto | full | half}

no duplex

［句法描述］

auto	自动测定接口的工作状态。
full	将接口设置为全双功工作状态。
half	将接口设置为半双工工作状态。

［默认取值］

默认值为 auto。

［命令模式］

接口配置模式。

［使用指导］

如果接口的 duplex 被设置成 auto，那么它的 speed 值也会自动变成 auto。

［命令实例］

```
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# duplex full
```

ftp

用户可以通过接口的 FTP 服务功能获取设备的日志和配置等信息。开启接口的 FTP 服务功能后，用户可以创建 FTP 用户和修改 FTP 端口号。创建 FTP 用户。使用该命令 no 的形式取消 FTP 用户的配置。

［命令］

ftp user *user-name* **password** *password*

no ftp user *user-name*

［句法描述］

user *user-name*	指定 FTP 用户名。
password *password*	指定 FTP 用户密码。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

系统允许最多配置 3 个 FTP 用户。

［命令实例］

hostname(config)# **ftp user user1 password 123456**

ftp port

修改 FTP 端口号。使用该命令 no 的形式恢复缺省配置。

［命令］

ftp port *number*

no ftp port

［句法描述］

number	指定 FTP 端口号，取值范围为 1 到 65535。

［默认取值］

21。

［命令模式］

全局配置模式。

［使用指导］

修改 FTP 默认端口号后，如果客户端采用被动模式登录，需要在安全域配置模式下，使用 **application-identify** 命令开启接口所在安全域的应用识别功能。

［命令实例］

hostname(config)# **ftp port 121**

holddown

指定接口保持 down 状态的时间。使用该命令 no 的形式取消保持时间的配置。

［命令］

holddown *time*

no holddown

［句法描述］

time	指定接口保持 down 状态的时间。配置该命令后，如果处于 down 状态的接口突然 up，X 秒（X 通过 *time* 参数指定）后，如果接口仍为 up 状态，系统才认为接口已经 up。取值范围为 1 到 3600，单位为 500 毫秒。比如，若配置 **holddown 10**，则相应接口的保持 down 时间为 5 秒。

［默认取值］

无。

［命令模式］

接口配置模式。

［使用指导］

仅适用于物理接口。

［命令实例］

```
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# holddown 20
```

holdup

指定接口保持 up 状态的时间。使用该命令 no 的形式取消保持时间的配置。

［命令］

holdup *time*

no holdup

［句法描述］

time	指定接口保持 up 状态的时间。配置该命令后，如果处于 up 状态的接口突然 down，X 秒（X 通过 *time* 参数指定）后，如果接口仍为 down 状态，系统才认为接口已经 down。取值范围为 1 到 3600，单位为 500 毫秒。比如，若配置 **holdup 10**，则相应接口的保持 up 时间为 5 秒。

［默认取值］

无。

［命令模式］

接口配置模式。

［使用指导］

仅适用于物理接口。

［命令实例］

```
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# holdup 20
```

interface aggregate*number*

创建一个集聚接口并且进入接口配置模式。如果接口已存在，则直接进入接口配置模式。使用该命令 no 的形式删除指定的接口。

［命令］

interface aggregate*number*

no interface aggregate*number*

［句法描述］

number	用来标识所创建的集聚接口。

［默认取值］

无默认值。

［命令模式］

全局配置模式。

［使用指导］

删除接口之前，必须取消其它接口与集聚接口的绑定、集聚子接口的配置、接口的 IP 地址配置以及接口与安全域的绑定。

［命令实例］

hostname(config)# **interface aggregate1**

interface aggregate*number.tag*

创建一个集聚子接口并且进入子接口配置模式。如果子接口已存在，则直接进入子接口配置模式。使用该命令 no 的形式删除指定的子接口。

［命令］

interface aggregate*number.tag*

［句法描述］

number	用来标识集聚接口。
tag	用来标识子接口的数字。范围是从 1 到 4094。

［默认取值］

无默认值。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **interface aggregate1.1**

interface bgroup*number*

创建一个 BGroup 接口并且进入接口配置模式。如果接口已存在，则直接进入接口配置模式。使用该命令 no 的形式删除指定的接口。

［命令］

interface bgroup*number*

no interface bgroup*number*

［句法描述］

number	用来标识所创建的 BGroup 接口。

［默认取值］

无默认值。

［命令模式］

全局配置模式。

［使用指导］

删除接口之前，请先删除 BGroup 接口的子接口、取消接口的 IP 地址配置以及接口与安全域的绑定。

［命令实例］

hostname(config)# **interface bgroup1**

interface ethernet*m/n*

进入以太网接口配置模式。

［命令］

interface ethernet*m/n*

［句法描述］

m	接口的插槽号。
n	接口的端口号。

［默认取值］

无默认值。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# interface ethernet0/2
```

interface ethernetX/Y-pppoeZ

创建一个冗余 PPPoE 子接口并且进入子接口配置模式。使用该命令 no 的形式删除指定的 PPPoE 子接口。

［命令］

```
interface ethernetX/Y-pppoeZ
no interface ethernetX/Y-pppoeZ
```

［句法描述］

ethernetX/Y	指定以太网口的名称，例如 ethernet0/5。
pppoeZ	指定 PPPoE 子接口的名称，“Z”为 PPPoE 子接口的标识，取值范围是 1 到 8 的整数。

［默认取值］

无默认值。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# interface ethernet0/5-pppoe1
hostname(config-if-eth0/5-pppoe1)#
```

interface ethernet*m/n.tag*

创建以太网子接口并且进入以太网子接口配置模式。如果子接口已存在，则直接进入子接口配置模式。使用该命令 no 的形式删除指定的子接口。

［命令］

interface ethernet*m/n.tag*

［句法描述］

m	接口的插槽号。
n	接口的端口号。
tag	用来标识子接口的数字。范围是从 1 到 4094 的整数。

［默认取值］

无默认值。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **interface ethernet0/2.1**

interface loopback*number*

创建回环接口并且进入回环接口配置模式。如果接口已存在，则直接进入接口配置模式。使用该命令 no 的形式删除指定的接口。

［命令］

interface loopback*number*

［句法描述］

number	用来标识所创建的回环接口，范围是 1 到 256。

［默认取值］

无默认值。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# interface loopback1
```

interface redundant*number*

创建一个冗余接口并且进入接口配置模式。如果接口已存在，则直接进入接口配置模式。使用该命令 no 的形式删除指定的接口。

［命令］

interface redundant*number*

no interface redundant*number*

［句法描述］

number	用来标识所创建的冗余接口。

［默认取值］

无默认值。

［命令模式］

全局配置模式。

［使用指导］

删除接口之前，必须取消其它接口与冗余接口的绑定、冗余子接口的配置、接口的 IP 地址配置以及接口与安全域的绑定。

［命令实例］

```
hostname(config)# interface redundant1
```

interface redundant*number.tag*

创建一个冗余子接口并且进入子接口配置模式。如果子接口已存在，则直接进入子接口配置模式。使用该命令 no 的形式删除指定的子接口。

［命令］

interface redundant*number.tag*

［句法描述］

number	用来标识冗余接口。
tag	用来标识子接口的数字。范围是从 1 到 4094。

［默认取值］

无默认值。

［命令模式］

全局配置模式。

［使用指导］

删除接口之前，必须取消接口的 IP 地址配置以及接口与安全域的绑定。

［命令实例］

```
hostname(config)# interface redundant1.1
```

interface tunnel*number*

创建一个隧道接口并且进入接口配置模式。如果接口已存在，则直接进入接口配置模式。使用该命令 no 的形式删除指定的接口。

［命令］

interface tunnel*number*

no interface tunnel*number*

［句法描述］

number	用来标识所创建的隧道接口。

［默认取值］

无默认值。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# interface tunnel1
```

interface vlan*id*

创建 VLAN 接口并进入 VLAN 接口配置模式。如果接口已经存在，则直接进入接口配置模式。使用该命令 no 的形式删除指定的接口。

［命令］

interface vlan*id*

［句法描述］

id	用来标识所创建的 VLAN 接口，范围是 1 到 223 和 256 到 4094。

［默认取值］

无默认值。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **interface vlan10**

interface supervlan*X*

创建 super-VLAN 接口并进入 super-VLAN 接口配置模式。如果接口已经存在，则直接进入接口配置模式。使用该命令 no 的形式删除指定的接口。

［命令］

interface supervlan*X*

no interface supervlan*X*

［句法描述］

X	指定将要创建的 super-VLAN 接口的编号。不同平台 *X* 的取值范围不同。

［默认取值］

无默认值。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **interface supervlan1**

ip address

给接口指定 IP 地址或二级 IP 地址。为接口取消 IP 地址或者二级 IP 地址，使用相应的 no 格式命令。

［命令］

ip address {*ip-address/mask* | **dhcp** [**setroute**] | **pppoe** [**setroute**]}

ip address *ip-address/mask* **secondary**

［句法描述］

ip_address	接口的 IP 地址。
mask	可选。IP 地址的网络掩码。
dhcp [**setroute**]	指定接口通过 DHCP 协议获得 IP 地址。如果配置 **setroute** 参数，系统会将 DHCP 服务器提供的网关信息设置为默认网关路由。
pppoe [**setroute**]	指定接口通过 PPPoE 协议获得 IP 地址。如果配置 **setroute** 参数，系统会将 PPPoE 服务器提供的网关信息设置为默认网关路由。
secondary	指定 IP 地址为接口的二级 IP 地址。

［默认取值］

无默认值。

［命令模式］

接口配置模式。

［使用指导］

- StoneOS 支持两种子网掩码书写方法，所以 1.1.1.1/24 也可写成 1.1.1.1 255.255.255.0。
- 配置 IP 地址前，要先把接口绑定到三层域。绑定到二层域的接口或者在冗余、集聚模式下的接口不能绑定 IP 地址。
- 在配置二级 IP 地址前，请先配置主 IP 地址。删除 IP 地址前，如果存在二级 IP 地址，请先删除其二级 IP 地址。
- 配置了静态 IP 地址的接口可以有两个二级 IP 地址。

［命令实例］

```
hostname(config)# interface ethernet0/2
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no ip address
hostname(config-if)# ip address dhcp
hostname(config-if)# no ip address dhcp
```

ip mtu

指定接口的最大传输单元值。使用该命令 no 的形式将以太网接口的最大传输单元值重新设置成 1500。

［命令］

ip mtu *value*

no ip mtu

［句法描述］

value	MTU 的字节数。值的有效范围是 1280 到 1500 字节。

［默认取值］

以太网接口的默认 MTU 值为 1500 字节。

［命令模式］

接口配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# ip mtu 1500
```

mac-clone

将指定的 MAC 地址克隆到以太网子接口。使用该命令 no 的形式删除 MAC 地址的指定。

［命令］

mac-clone *H.H.H*

no mac-clone

［句法描述］

H.H.H	指定 MAC 地址。

［默认取值］

无。

［命令模式］

以太网子接口配置模式。

［使用指导］

若在 PPPoE 拨号成功后修改 MAC 地址，用户需要重新连接 PPPoE 客户端以使修改后的 MAC 地址生效。

［命令实例］

```
hostname(config)# interface ethernet0/2.1
hostname(config-if-eth0/2.1)# mac-clone 0000.0000.0000
```

manage

开启接口的 HTTP、HTTPS、Ping、SNMP、SSH、Telnet 功能。使用该命令 no 的形式关闭接口的相应功能。

［命令］

```
manage {ssh | telnet | ping | snmp | http | https }
no manage {ssh | telnet | ping | snmp | http | https}
```

［句法描述］

ssh	接口的 SSH 功能。
telnet	接口的 Telnet 功能。
ping	接口的 Ping 功能。
snmp	接口的 SNMP 功能。
http	接口的 HTTP 功能。
https	接口的 HTTPS 功能。

［默认取值］

无默认值。

［命令模式］

接口配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# manage http
```

mirror to

配置接口镜像功能。使用该命令 no 的形式取消接口的镜像配置。

［命令］

mirror to *interface-name* [**both** | **rx** | **tx**]

no mirror

［句法描述］

interface-name	指定分析接口的名称。分析接口上必须无任何配置，例如不能绑定到任何域。
both	指定镜像接口接收和发送的所有流量。
rx	指定仅镜像接口接收的流量。
tx	指定仅镜像接口发送的流量。

［默认取值］

无默认值。

［命令模式］

接口配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **interface ethernet0/2**

hostname(config-if-eth0/2)# **mirror to ethernet0/7**

primary

把一个接口指定为冗余接口的主接口。使用该命令 no 的形式取消主接口设置。

［命令］

primary *interface-name*

no primary *interface-name*

［句法描述］

interface-name	指定为主接口的接口名称。

［默认取值］

无默认值。

［命令模式］

接口配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# interface redundant1
hostname(config-if-red1)# primary ethernet0/2
```

proxy-arp

开启接口的代理 ARP 功能。使用该命令 no 的形式关闭接口的代理 ARP 功能。

［命令］

proxy-arp [dns]

no proxy-arp

［句法描述］

proxy-arp	开启接口的代理 ARP 功能。
dns	当需要实现 IP 即插即用时，使用该参数。

［默认取值］

关闭。

［命令模式］

接口配置模式。

［使用指导］

代理 ARP 功能仅适用于三层接口。配置了代理 ARP 功能（使用 **dns** 参数）和 DNS 代理的接口可以实现 IP 即插即用，即配有任意 IP 地址和 DNS 地址的内网 PC 客户端都可以通过接口访问外网。

［命令实例］

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# proxy-arp
```

redundant redundant*number*

把一个物理接口加到冗余接口中。使用该命令 no 的形式把接口分离出冗余接口。

［命令］

redundant redundant*number*

no redundant

［句法描述］

number	用来标志冗余接口。

［默认取值］

无默认值。

［命令模式］

接口配置模式。

［使用指导］

添加物理接口时，必须保证被添加的物理接口不属于任何其它接口也不属于任何安全域。如果被分离的接口是冗余接口的主接口，要先取消主接口的配置再将其从冗余接口中分离。

［命令实例］

hostname(config)# **interface ethernet0/2**

hostname(config-if-eth0/2)# **redundant aggregate1**

reverse-route

逆向路由功能配置。使用该命令 no 的形式关闭逆向路由功能。

［命令］

reverse-route {force | prefer}

no reverse-route

［句法描述］

无。

［默认取值］

所有的三层接口默认情况下都是强制逆向路由，即 force。

［命令模式］

接口配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **interface ethernet0/2**

```
hostname(config-if-eth0/2)# no reverse-route
```

shutdown

通过命令强制关闭特定接口，并且可以通过时间表控制接口的关闭时间，或者根据监测接口的链路状态控制接口的关闭。使用该命令 no 的形式取消强制关闭接口功能并清除此功能的所有相关配置。

［命令］

shutdown [**track** *track-object*] [**schedule** *schedule-name*]

no shutdown

［句法描述］

shutdown	立即关闭接口。
track *track-object*	指定监测对象名称。如果指定该参数，接口会在监测对象失败时处于关闭状态。
schedule *schedule-name*	指定时间表名称。如果指定该参数，接口会在时间表指定的时间范围内处于关闭状态。

［默认取值］

所有的物理接口默认情况下都是打开的。

［命令模式］

接口配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# shutdown track obj1
```

speed

指定接口的速率。使用该命令 no 的形式恢复到默认 speed 设置。

［命令］

speed {**auto** | **10** | **100** | **1000** }

no speed

［句法描述］

10	将速率设置成 10BASE-T。
100	将速率设置成 100BASE-T。
1000	将速率设置成 1000BASE-T。
auto	自动测定接口速率。

［默认取值］

默认值为 auto。

［命令模式］

接口配置模式。

［使用指导］

如果接口的 speed 被设置成 auto，那么它的 duplex 值也会自动设置成 auto。

［命令实例］

```
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# speed 1000
```

tunnel

绑定 VPN/GRE 隧道到隧道接口。使用该命令 no 的形式取消绑定。

［命令］

tunnel {{**ipsec** | **gre**} *tunnel-name* [**gw** *ip-address*] **scvpn** *vpn-name* | **l2tp** *tunnel-name* }

no tunnel {**ipsec** *vpn-name* | **gre** *tunnel-name* | **scvpn** *vpn-name* | **l2tp** *tunnel-name* }

［句法描述］

{**ipsec** | **gre**} *tunnel-name*	指定绑定到隧道接口的 IPSec VPN 隧道的名称或者 GRE 隧道的名称。
gw *ip-address*	指定 VPN/GRE 隧道的下一跳 IP 地址，可以为对端隧道接口的 IP 地址或者对端出接口的 IP 地址。当需要为隧道接口绑定多个 IPSec VPN/GRE 隧道时，此配置参数有效。系统默认值为 0.0.0.0。
scvpn *vpn-name*	指定绑定到隧道接口的 SCVPN 隧道的名称。一个隧道接口最多只能绑定一个 SCVPN 隧道。
l2tp *tunnel-name*	指定绑定到隧道接口的 L2TP 隧道的名称。一个隧道接口最多只能绑定一个 L2TP 隧道。

［默认取值］

无默认值。

［命令模式］

接口配置模式。

［使用指导］

一个隧道接口可以绑定多个 IPSec VPN 隧道或 GRE 隧道，也可以绑定一个 SCVPN 隧道或一个 L2TP 隧道。

多次配置该命令为隧道接口绑定多个 VPN/GRE 隧道。

［命令实例］

```
hostname(config)# interface tunnel1
hostname(config-if-tun1)# tunnel ipsec vpn1
```

webauth auth-arp-prompt

指定显示在客户端下载页面的 ARP 认证描述。使用该命令 no 的形式取消描述信息的指定。

［命令］

webauth auth-arp-prompt *description*

no webauth auth-arp-prompt

［句法描述］

description	指定描述信息。

［默认取值］

无默认值。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# webauth auth-arp-prompt ARP_auth
```

zone

将接口绑定到域。使用该命令 no 的形式取消接口与域的绑定。

［命令］

zone *zone-name*

no zone

［句法描述］

zone-name	域的名称。

［默认取值］

无默认值。

［命令模式］

接口配置模式。

［使用指导］

在使用 **no zone** 命令取消接口与三层域的绑定前，必须将此三层接口配置的 IP 地址取消。

［命令实例］

```
hostname(config-if-eth0/2)# zone trustzone1
hostname(config-if-eth0/2)# no zone
```

地址（Address）命令

address

向全局地址簿中添加一个地址条目并且进入地址配置模式。如果条目已存在，则直接进入地址配置模式。使用该命令 no 的形式删除该地址条目。

［命令］

address *address-entry*

no address *address-entry*

［句法描述］

address-entry	指定要添加的地址条目的名称。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

已经被其它模块引用的地址条目不能被删除。

［命令实例］

hostname(config)# **address internal**

hostname(config)# **no address internal**

host

为地址条目添加一个主机类型成员。使用该命令 no 的形式删除该成员。

［命令］

host *host-name*

no host *host-name*

［句法描述］

host-name	指定主机名称。

［默认取值］

无默认值。

［命令模式］

地址配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-address)# host host1.hilltonenet.com
hostname(config-address)# no host host1.hostnamenet.com
```

ip

为地址条目添加一个 IP 地址范围。使用该命令 no 的形式删除该地址范围。

［命令］

ip *ip-address* {*netmask* | *wildcardmask*}

no ip *ip-address* {*netmask* | *wildcardmask*}

［句法描述］

ip-address	指定 IP 成员的 IP 地址。
netmask | *wildcardmask*	指定子网掩码（*netmask*）或者通配符掩码（*wildcardmask*）。StoneOS 不支持掩码转换为二进制后，其位数里从右往左第一个“1”左边的“0”的个数超过 8 个的通配符掩码（“0”可以连续也可以不连续），比如 255.0.0.255 是无效的通配符掩码；255.0.255.0 和 255.32.255.0 等都为有效的通配符掩码。

［默认取值］

无默认值。

［命令模式］

地址配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-addr)# ip 192.168.1.0/24
hostname(config-addr)# no ip 192.168.1.0/24
```

member

为地址条目添加一个地址条目作为其条目成员。使用该命令 no 的形式删除该地址条目。

［命令］

member *address-entry*

no member *address-entry*

［句法描述］

address-entry	要添加或删除的地址条目的名称。

［默认取值］

无默认值。

［命令模式］

地址配置模式。

［使用指导］

无。

［命令实例］

hostname(config-addr)# **member my-laptop**

hostname(config-addr)# **no member my-laptop**

range

为地址条目添加一个 IP 地址段。使用该命令 no 的形式删除该 IP 地址段。

［命令］

range *min_ip* [*max-ip*]

no range *min_ip* [*max-ip*]

［句法描述］

min_ip [*max-ip*]	确定 IP 地址范围的两个 IP 地址。

［默认取值］

无默认值。

［命令模式］

地址配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-addr)# range 192.168.100.1 192.168.100.10
hostname(config-addr)# no range 192.168.100.1 192.168.100.10
```

服务（Service）命令

icmp

为用户自定义服务创建一条 ICMP 协议服务条目。使用该命令 no 的形式将指定条目从服务中删除。

［命令］

icmp type *type-value* [**code** *min-code* [*max-code*]][**timeout** *timeout-value*]

no icmp type *type-value* [**code** *min-code* [*max-code*]][**timeout** *timeout-value*]

［句法描述］

type *type-value*	指定 ICMP 协议服务条目的 type 值。
code	可选。指定 ICMP 协议服务条目的 code 值。
min-code	ICMP 协议服务条目 code 的最小值。
max-code	可选。ICMP 协议服务条目 code 的最大值。
timeout *timeout-value*	可选。指定服务条目超时时间值，单位为秒（s）。

［默认取值］

无默认值。

［命令模式］

服务配置模式。

［使用指导］

- 如果不指定 code 值，StoneOS 会使用默认值 0-5。
- 超时时间值范围是 1 到 65535 秒。如果不指定超时时间值，StoneOS 会使用 ICMP 协议的默认超时时间 6 秒。

［命令实例］

```
hostname(config)# service my-service
hostname(config-service)# icmp type 3 code 3 5 timeout 60
hostname(config-service)# exit
```

icmp type

以下命令用于修改 ICMP 类型预定义服务的超时时间。

［命令］

icmp type *type-value* **code** *code-value* **timeout** *timeout-value*

［句法描述］

type *type-value*	ICMP 类型预定义服务的 type 值。
code *code-value*	ICMP 类型预定义服务的 code 值。
timeout *timeout-value*	指定预定义服务的超时时间值，单位为秒。

［默认取值］

无默认值。

［命令模式］

服务配置模式。

［使用指导］

目前，StoneOS 预定义服务中只有 ICMP 和 PING 两个 ICMP 类型预定义服务。

［命令实例］

修改预定义服务 ICMP 的超时时间值：

```
hostname(config)# service icmp
hostname(config-service)# icmp type any code any timeout 30
```

修改预定义服务 PING 的超时时间值：

```
hostname(config)# service ping
hostname(config-service)# icmp type 8 code 0 timeout 30
```

longlife-sess-percent

指定长效会话占系统总会话数的百分比。使用该命令 no 的形式恢复默认百分比。

［命令］

longlife-sess-percent *percentage*

［句法描述］

percentage	指定长效会话的百分比。范围是 0 到 100。

［默认取值］

0，表示不可以建立长效会话。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **longlife-sess-percent 10**

---

protocol

以下命令用于为自定义服务添加其它类型服务条目。使用该命令 no 的形式将指定条目从服务中删除。

［命令］

protocol *protocol-number* [**timeout** *timeout-value*]

no protocol *protocol-number* [**timeout** *timeout-value*]

［句法描述］

protocol-number	指定自定义服务的协议号。范围是 1 到 255。
timeout-value	指定自定义服务的超时时间。范围是 1 到 65535 秒。

［默认取值］

无默认值。

［命令模式］

服务配置模式。

［使用指导］

无

［命令实例］

hostname(config-service)# **protocol 47 timeout 8**

---

servgroup

创建一个服务组并进入服务组配置模式。如果服务组已存在，则直接进入服务组的配置模式。使用该命令 no 的形式删除该服务组。

［命令］

servgroup *servicegroup-name*

no servgroup *servicegroup-name*

［句法描述］

servicegroup-name	服务组的名称。

［默认取值］

无默认值。

［命令模式］

全局配置模式。

［使用指导］

服务组的名称必须是唯一的。

［命令实例］

hostname(config)# **servgroup my-group**

service

将一个服务或者服务组添加到服务组中。

［命令］

service {*service-name* | *servicegroup-name*}

no service {*service-name* | *servicegroup-name*}

［句法描述］

service-name	服务名称。可以是预定义服务也可以是自定义服务。
servicegroup-name	服务组名称。

［默认取值］

无默认值。

［命令模式］

服务组配置模式。

［使用指导］

服务组的名称必须是唯一的。

［命令实例］

hostname(config)# **servgroup my-group**

hostname(config-svc-group)# **service my-service**

hostname(config-svc-group)# **service group1**

service *service-name*

进入预定义服务的服务配置模式，或创建一个用户自定义服务并且进入服务配置模式。如果自定义服务已存在，则直接进入服务配置模式。使用该命令 no 的形式删除指定的自定义服务。预定义服务不能被删除。

［命令］

service *service-name*

no service *service-name*

［句法描述］

service-name	预定义服务或用户自定义服务的名称。

［默认取值］

无默认值。

［命令模式］

全局配置模式。

［使用指导］

自定义服务名称的长度范围是 1 到 31 个字符。

［命令实例］

hostname(config)# **service my-service**

tcp | udp

以下命令用于修改 TCP 或者 UDP 类型预定义服务的超时时间。

［命令］

{**tcp** | **udp**} **dst-port** *min-port* [*max-port*] [**src-port** *min-port* [*max-port*]] **timeout** *timeout-value*

［句法描述］

dst-port	指定服务条目的目标端口号。
src-port	指定服务条目的源端口号。
min-port	目标或源端口号的最小值。
max-port	目标或源端口号的最大值。
timeout *timeout-value*	指定预定义服务的超时时间值，单位为秒。

［默认取值］

无默认值。

［命令模式］

服务配置模式。

［使用指导］

使用以上命令时，协议类型（TCP 或者 UDP）、目标端口号（dst-port）和源端口号（src-port）必须与欲修改超时时间的服务相一致；如果源端口号为 any，则 src-port 一项可以省略。

［命令实例］

```
hostname(config)# service ftp
hostname(config-service)# tcp dst-port 21 timeout 30
```

tcp | udp application

为用户自定义服务创建一条 TCP 或 UDP 协议服务条目。使用该命令 no 的形式，将指定条目从服务中删除。

［命令］

{tcp | udp} dst-port *min-port* [max-*port*] [**src-port** min-*port* [max-*port*]] [**application** *app-type* | **user-defined-application**] [**timeout** *timeout-value* | **timeout-day** *timeout-day-value*]

no {tcp | udp} dst-port *min-port* [max-*port*] [**src-port** min-*port* [max-*port*]] [**application** *app-type* | **user-defined-application**] [**timeout** *timeout-value* | **timeout-day** *timeout-day-value*]

［句法描述］

dst-port	指定服务条目的目标端口号。
src-port	指定服务条目的源端口号。
min-port	目标或源端口号的最小值。
max-port	可选。目标或源端口号的最大值。
application *app-type*	服务条目的应用程序类型。
user-defined-application	配置该关键字后，系统会为该自定义服务自动分配一个 Application ID 用于自定义服务的识别。
timeout *timeout-value* | **timeout-day** *timeout-day-value*	指定自定义服务的超时时间。timeout timeout-value 的时间范围是 1 到 65535 秒。timeout-day timeout-day-value 的时间范围是 1 到 100 天。如果不指定超时时间，系统会使用协议的默认值，TCP 是 1800 秒，UDP 是 60 秒。

［默认取值］

无默认值。

［命令模式］

服务配置模式。

［使用指导］

- 目标端口号和源端口号的范围是 0 到 65535，并且目标端口号不能为 0。

［命令实例］

```
hostname(config)# service my-service
hostname(config-service)# tcp dst-port 23 34 application ftp
timeout 60
hostname(config-service)# udp dst-port 24 src-port 25 26
hostname(config-service)# exit
```

策略（Policy）命令

absolute

配置时间表的绝对计划。使用该命令 no 的形式关闭绝对计划功能，使周期计划能够即时生效。

［命令］

absolute {[**start** *start-date start-time*] [**end** *end-date end-time*]}

［句法描述］

start *start-date start-time*	指定绝对计划的开始时间点，包括日期和具体时间。如果不指定该参数的值，开始时间为当前时间。
end *end-date end-time*	指定绝对计划的结束时间点，包括日期和具体时间。如果不指定该参数的值，则无结束时间，周期会从开始时间起，一直有效。

［默认取值］

无默认值。

［命令模式］

时间表配置模式。

［使用指导］

- 日期的书写格式为“月/日/年”，例如 10/23/2007。
- 时间的书写格式为“时:分”，例如 15:30。

［命令实例］

hostname(config-schedule)# **absolute start 10/23/2007 15:30 end 11/30/2007 10:00**

action

为匹配策略规则的流量指定行为。

［命令］

action {**permit** | **deny** | **tunnel** | **fromtunnel** | **webauth**}

［句法描述］

permit	为匹配的流量指定行为：permit 为允许通过安全网关。

deny	为匹配的流量指定行为：deny 为拒绝通过。
tunnel	当流量为从客户端访问服务器端时，使用该行为使流量通过 VPN 隧道。
fromtunnel	当流量为从服务器端访问客户端时，如果使用该行为，系统将会首先判断流量是否来自隧道，只有来自隧道的流量才会被允许通过。
webauth	对符合条件的流量进行 Web 认证。

［默认取值］

无默认值。

［命令模式］

策略规则配置模式。

［使用指导］

无。

［命令实例］

hostname(config-policy)# **rule id 3**

hostname(config-policy-rule)# **action deny**

clear policy hit-count

清除策略规则匹配次数统计信息。

［命令］

clear policy hit-count {**all** | **id** *id*}

［句法描述］

all	清除所有规则的匹配次数统计信息。
id *id*	清除指定 ID 规则的匹配次数统计信息。

［默认取值］

无默认值。

［命令模式］

任意模式。

［使用指导］

无。

［命令实例］

hostname(config)# **clear policy hit-count all**

clear policy hit-count default-action

清除策略规则的缺省行为匹配次数统计信息。

［命令］

clear policy hit-count default-action

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任意模式。

［使用指导］

无。

［命令实例］

hostname(config)# **clear policy hit-count default-acton**

---

default-action

为未匹配到任何已配置策略规则的流量指定缺省行为为允许，系统将按照指定的缺省行为对此类流量进行处理。使用该命令 no 的形式恢复系统缺省行为。

［命令］

default-action permit

no default-action permit

［句法描述］

无。

［默认取值］

默认情况下，系统会拒绝未匹配到任何已配置策略规则的流量通过。

［命令模式］

策略配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-policy)# default-action permit
```

description

为策略规则添加描述，使用该命令 no 的形式为规则删除描述。

［命令］

description *description*

no description *description*

［句法描述］

description	指定规则的描述信息，取值范围是 1 到 255 字节。

［默认取值］

无。

［命令模式］

策略规则配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-policy)# rule id 3
hostname(config-policy-rule)# description this policy is for user1
hostname(config-policy-rule)#
```

disable

禁用策略规则。

［命令］

disable

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

策略规则配置模式。

［使用指导］

默认情况下，配置好的策略规则会在系统中立即起效。用户可以通过命令禁用某条策略规则，使其不对流量进行控制。

［命令实例］

```
hostname(config-policy-rule)# disable
```

dst-addr

为策略规则添加地址簿条目类型目的地址。使用该命令 no 的形式为规则删除指定的目的地址。

［命令］

dst-addr *dst-addr*

no dst-addr *dst-addr*

［句法描述］

dst-addr	规则的目的地址。该地址来自域所在 VRouter 或 VSwitch 的地址簿。

［默认取值］

无默认值。

［命令模式］

策略规则配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-policy)# rule id 3
hostname(config-policy-rule)# dst-addr addr1
hostname(config-policy-rule)# no dst-addr addr1
```

dst-host

为策略规则添加主机成员类型目的地址。使用该命令 no 的形式为规则删除主机成员类型目的地址。

［命令］

dst-host *host-name*

no dst-addr *host-name*

［句法描述］

host-name	主机名称。

［默认取值］

无默认值。

［命令模式］

策略规则配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-policy)# rule id 3
hostname(config-policy-rule)# dst-host host1
hostname(config-policy-rule)# no dst-host host1
```

dst-ip

为策略规则添加 IP 成员类型目的地址。使用该命令 no 的形式为规则删除 IP 成员类型的目的地址。

［命令］

dst-ip *ip/netmask*

no dst-ip *ip/netmask*

［句法描述］

ip/netmask	IP 地址/子网掩码

［默认取值］

无默认值。

［命令模式］

策略规则配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-policy)# rule id 3
hostname(config-policy-rule)# dst-ip 10.3.4.5/24
hostname(config-policy-rule)# no dst-ip 10.3.4.5/24
```

dst-range

为策略规则添加 IP 地址范围类型目的地址。使用该命令 no 的形式为规则删除 IP 地址范围类型的目的地址。

［命令］

dst-range *min-ip* [*max-ip*]

no dst-range *min-ip* [*max-ip*]

［句法描述］

min-ip	IP 地址范围的最小值。
max-ip	IP 地址范围的最大值。

［默认取值］

无默认值。

［命令模式］

策略规则配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-policy)# rule id 3
hostname(config-policy-rule)# dst-range 10.3.4.5 10.3.4.36
hostname(config-policy-rule)# no dst-range 10.3.4.5 10.3.4.36
```

dst-zone

修改策略规则的目的安全域。使用该命令 no 的形式为规则删除目的安全域，并恢复系统默认目的安全域。

［命令］

dst-zone *dst-zone*

no dst-zone *dst-zone*

［句法描述］

dst-zone	指定流量的目的安全域。

［默认取值］

Any。

［命令模式］

策略规则配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-policy)# rule id 3
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)#
```

enable

启用策略规则。

［命令］

enable

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

策略规则配置模式。

［使用指导］

默认情况下，配置好的策略规则会在系统中立即起效。

［命令实例］

```
hostname(config-policy-rule)# enable
```

log

为策略规则配置日志管理功能。使用该命令 no 的形式取消策略规则日志管理功能的配置。

［命令］

log {policy-deny | session-start | session-end}

no log {policy-deny | session-start | session-end}

［句法描述］

policy-deny	适用于 deny 类型的策略规则。使系统生成规则拒绝流量的日志信息。
session-start	适用于 permit 类型的策略规则。使系统生成规则允许的流量建立会话的日志信息。
session-end	适用于 permit 类型的策略规则。使系统生成规则允许的流量结束会话的日志信息。

［默认取值］

无默认值。

［命令模式］

策略规则配置模式。

［使用指导］

使用该功能前，必须保证系统的流量日志功能是开启的，即在全局配置模式下使用 logging traffic on 命令。

［命令实例］

hostname(config-policy-rule)# **log policy-deny**

import customize webredirect

定制重定向提示页面。引入页面背景图片到系统，用户需首先将图片压缩到 zip 包。使用该命令 no 的形式取消策略规则日志管理功能的配置。

［命令］

import customize webredirect from {ftp server *ip-address* **[user** *user-name* **password** *password*] **| tftp server** *ip-address* **| usb0 | usb1}** *file-name*

no log {policy-deny | session-start | session-end}

［句法描述］

policy-deny	适用于 deny 类型的策略规则。使系统生成规则拒绝流量的日志信息。
session-start	适用于 permit 类型的策略规则。使系统生成规则允许的流量建立会话

	的日志信息。
session-end	适用于 permit 类型的策略规则。使系统生成规则允许的流量结束会话的日志信息。

［默认取值］

无默认值。

［命令模式］

执行模式。

［使用指导］

使用该功能前，必须保证系统的流量日志功能是开启的，即在全局配置模式下使用 logging traffic on 命令。

［命令实例］

hostname(config-policy-rule)# **log policy-deny**

move

移动指定策略规则从而改变规则的排列顺序。

［命令］

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

［句法描述］

id	指定要移动的规则的 ID 号。
top | **bottom**	为规则指定绝对排列顺序：top 为首位，bottom 为末位。
before *id*	为规则指定相对排列顺序：位于某规则之前。
after *id*	为规则指定相对排列顺序：位于某规则之后。

［默认取值］

无默认值。

［命令模式］

策略配置模式。

［使用指导］

无。

［命令实例］

hostname(config-policy)# **move 3 top**

periodic

配置时间表的周期计划，指定“每天”或者“每周的某几天”类型周期条目。使用该命令 no 的形式删除指定的周期条目。

［命令］

periodic {**daily** | **weekdays** | **weekend** | [**monday**] […] [**sunday**]} *start-time* **to** *end-time*

no periodic {**daily** | **weekdays** | **weekend** | [**monday**] […] [**sunday**]} *start-time* **to** *end-time*

［句法描述］

daily	每一天（周一到周日）。
weekdays	工作日（周一到周五）。
weekend	周末（周六到周日）。
[**monday**] […] [**sunday**]	选择需要的日期。例如选择周二、周三和周六，命令关键字为 **tuesday wednesday saturday**。
start-time	开始时间。书写格式为“时:分”。
end-time	结束时间。书写格式为“时:分”。

［默认取值］

无默认值。

［命令模式］

时间表配置模式。

［使用指导］

无。

［命令实例］

hostname(config-schedule)# **periodic daily 02:00 to 10:00**

---

periodic

配置时间表的周期计划，指定“每周一段时间”类型周期条目。使用该命令 no 的形式删除指定的周期条目。

［命令］

periodic {[**monday**] | […] | [**sunday**]} *start-time* **to** {[**monday**] | […] | [**sunday**]} *end-time*

no periodic {[**monday**] | […] | [**sunday**]} *start-time* **to** {[**monday**] | […] | [**sunday**]} *end-time*

［句法描述］

[monday] | […] | [sunday]	开始日期，可以是周一到周日的任意一天。
start-time	开始时间。书写格式为“时:分”。
[monday] | […] | [sunday]	结束日期，与开始日期相同或者晚于开始日期。
end-time	结束时间。书写格式为“时:分”。

［默认取值］

无默认值。

［命令模式］

时间表配置模式。

［使用指导］

无。

［命令实例］

hostname(config-schedule)# **periodic monday 02:00 to 10:00**

policy-global

进入策略配置模式。

［命令］

policy-global

［句法描述］

无。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **policy-global**

policy-qos-tag *tag*

修改策略规则的 Qos 标签。使用该命令 no 的形式删除规则的 Qos 标签。

［命令］

policy-qos-tag *tag*

no policy-qos-tag *tag*

［句法描述］

tag	Qos 标签，取值范围是 1-16。

［默认取值］

无默认值。

［命令模式］

策略规则配置模式。

［使用指导］

无。

［命令实例］

hostname(config-policy-rule)# **policy-qos-tag 1**

role

为策略规则指定角色。使用该命令 no 的形式取消策略规则的角色配置。

［命令］

role {**UNKNOWN** | *role-name*}

no role

［句法描述］

UNKNOWN	表示是系统预留的角色，是既没有经过系统认证也没有静态绑定的角色。
role-name	指定角色名称。

［默认取值］

无默认值。

［命令模式］

策略规则配置模式。

［使用指导］

当策略规则的行为是“Web 认证”时，使用 **role UNKNOWN** 触发系统的 Web 认证功能。

［命令实例］

```
hostname(config-policy)# rule id 4
 Rule id 4 is created
hostname(config-policy-rule)# role role1
```

user

为策略规则指定用户。使用该命令 no 的形式取消策略规则的用户配置。

［命令］

user *aaa-server-name user-name*

no user *aaa-server-name user-name*

［句法描述］

aaa-server-name	指定 AAA 服务器名称
user-name	指定用户名称。

［默认取值］

无。

［命令模式］

策略规则配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-policy)# rule id 4
 Rule id 4 is created
hostname(config-policy-rule)# user local user1
```

user-group

为策略规则指定用户组。使用该命令 no 的形式取消策略规则的用户组配置。

［命令］

user-group *aaa-server-name user-group-name*

no user-group *aaa-server-name user-group-name*

［句法描述］

aaa-server-name	指定 AAA 服务器名称
user-group-name	指定用户组名称。

［默认取值］

无。

［命令模式］

策略规则配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-policy)# rule id 4
 Rule id 4 is created
hostname(config-policy-rule)# user-group local usergroup1
```

rule

创建策略规则。

［命令］

rule [**id** *id*] [**top** | **before** *id* | **after** *id*] [**role** {**UNKNOWN** | *role-name*} | **user** *aaa-server-name user-name* | **user-group** *aaa-server-name user-group-name*] **from** *src-addr* **to** *dst-addr* **service** *service-name* {**permit** | **deny** | **tunnel** *tunnel-name* | **fromtunnel** *tunnel-name* | **webauth**}

［句法描述］

id *id*	为规则指定一个 ID 号。如果不指定，系统将会为策略规则自动分配一个 ID。
top	为规则指定绝对排列顺序：top 为首位
before *id*	为规则指定相对排列顺序：位于某规则之前。
after *id*	为规则指定相对排列顺序：位于某规则之后。
UNKNOWN	UNKNOWN 是系统预留的角色，既没有经过系统认证也没有静态绑定的。
role-name	指定角色名称
aaa-server-name	指定用户/用户组所属的 AAA 服务器名称。
user-name	指定用户名称。
user-group-name	指定用户组名称。

src-addr	指定策略规则的源地址。
dst-addr	指定策略规则的目的地址。
service-name	指定策略规则的服务名称。
permit | **deny**| **tunnel** *tunnel-name*| **fromtunnel** *tunnel-name* | **webauth**	指定 StoneOS 对匹配的流量所采取的行为。**permit**：允许流量通过。**deny**：拒绝流量通过。**tunnel**：当流量为从本地到对端时，使用该行为使流量通过 VPN 隧道。**fromtunnel**：当流量为从对端到本地时，如果使用该行为，系统将会首先判断流量是否来自隧道，只有来自隧道的流量才会被允许通过。**webauth** 对符合条件的流量进行 Web 认证。

［默认取值］

无默认值。

［命令模式］

策略配置模式。

［使用指导］

- 策略规则的默认源安全域及目的安全域都为 Any。
- 以下方法也可以创建一条规则：先用 **rule** [**id** *id*] [**top** | **bottom** | **before** *id* | **after** *id*]创建一个 ID，之后进入策略规则配置模式指定其它参数的值。
- 如让规则在某个特定的时期内生效，请先在全局配置模式用 schedule 命令指定时间段。

［命令实例］

```
hostname(config)# policy global
hostname(config-policy)# rule id 3 from addr1 to any service http permit
 Rule id 3 is created.
```

rule id

进入指定策略规则的规则配置模式，用户可以在该模式下修改该规则的各参数值。使用该命令 no 的形式可以删除该规则。

［命令］

rule [**id** *id*] [**top** | **before** *id* | **after** *id*] （该命令适用于规则 ID 不存在的情况）

rule id *id* （该命令适用于规则 ID 已存在的情况，并且用该命令 no 的形式，可以删除该条规则，即 **no rule id** *id*）

［句法描述］

id *id*	为规则指定一个 ID 号。
top	指定策略规则的位置为所有规则的首位。
before *id*	指定策略规则的位置为某个规则之前。
after *id*	指定策略规则的位置为某个规则之前。

［默认取值］

无默认值。

［命令模式］

策略配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-policy)# rule id 3
hostname(config-policy-rule)#
```

schedule

创建一个时间表并且进入时间表配置模式。如果指定的名称已存在，则直接进入时间表配置模式。使用该命令 no 的形式删除指定的时间表。

［命令］

schedule *schedule-name*

no schedule *schedule-name*

［句法描述］

schedule-name	指定时间表的名称。

［默认取值］

无默认值。

［命令模式］

全局配置模式。

［使用指导］

删除时间表之前，请从其它模块中取消对该时间表的引用。

［命令实例］

```
hostname(config)# schedule schedule1
```

schedule

为策略规则指定生效时间表。使用该命令 no 的形式取消规则生效时间限制。

［命令］

schedule *schedule-name*

no schedule *schedule-name*

［句法描述］

schedule-name	指定规则生效时间表的名称。

［默认取值］

无默认值。

［命令模式］

策略规则配置模式。

［使用指导］

时间段必须在全局配置模式配置好才可在该命令中使用。

［命令实例］

```
hostname(config-policy)# rule id 3
hostname(config-policy-rule)# schedule schedule1
hostname(config-policy-rule)# no schedule schedule1
```

service

为策略规则指定流量的服务类型。使用该命令 no 的形式为规则删除指定的服务。

［命令］

service *service-name*

no service *service-name*

［句法描述］

service-name	为流量指定服务或者服务组。该服务或者服务组来自服务簿。

［默认取值］

无默认值。

［命令模式］

策略规则配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-policy)# rule id 3
hostname(config-policy-rule)# service my-service
hostname(config-policy-rule)# no service my-service
```

src-addr

为策略规则添加地址簿条目类型源地址。使用该命令 no 的形式为规则删除地址簿条目类型源地址。

［命令］

src-addr *src-addr*

no src-addr *src-addr*

［句法描述］

src-addr	规则的源地址。该地址来自域所在 VRouter 或 VSwitch 的地址簿。

［默认取值］

无默认值。

［命令模式］

策略规则配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-policy)# rule id 3
hostname(config-policy-rule)# src-addr addr1
hostname(config-policy-rule)# no src-addr addr1
```

src-host

为策略规则添加主机成员类型源地址。使用该命令 no 的形式为规则删除主机成员类型源地址。

［命令］

src-host *host-name*

no src-addr *host-name*

［句法描述］

host-name	主机名称。

［默认取值］

无默认值。

［命令模式］

策略规则配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-policy)# rule id 3
hostname(config-policy-rule)# src-host host1
hostname(config-policy-rule)# no src-host host1
```

src-ip

为策略规则添加 IP 成员类型源地址。使用该命令 no 的形式为规则删除 IP 成员类型的源地址。

［命令］

src-ip *ip/netmask*

no src-ip *ip/netmask*

［句法描述］

ip/netmask	IP 地址/子网掩码

［默认取值］

无默认值。

［命令模式］

策略规则配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-policy)# rule id 3
```

```
hostname(config-policy-rule)# src-ip 10.3.4.5/24
hostname(config-policy-rule)# no src-ip 10.3.4.5/24
```

src-range

为策略规则添加 IP 地址范围类型源地址。使用该命令 no 的形式为规则删除 IP 地址范围类型的源地址。

［命令］

src-range *min-ip* [*max-ip*]

no src-range *min-ip* [*max-ip*]

［句法描述］

min-ip	IP 地址范围的最小值。
max-ip	IP 地址范围的最大值。

［默认取值］

无默认值。

［命令模式］

策略规则配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-policy)# rule id 3
hostname(config-policy-rule)# src-range 10.3.4.5 10.3.4.36
hostname(config-policy-rule)# no src-range 10.3.4.5 10.3.4.36
```

src-zone

修改策略规则的源安全域。使用该命令 no 的形式为规则删除源安全域，并恢复系统默认源安全域。

［命令］

src-zone *src-zone*

no src-zone *src-zone*

［句法描述］

src-zone	指定流量的源安全域。

［默认取值］

Any。

［命令模式］

策略规则配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-policy)# rule id 3
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)#
```

web-redirect

配置网页重定向 URL。网页重定向是指当客户端发送 HTTP 网页访问请求后，系统自动将该请求重新定向到指定的页面。StoneOS 提供基于策略的网页重定向功能。使用该命令 no 的形式取消指定重定向 URL。

［命令］

web-redirect [*url*]

no web-redirect

［句法描述］

url	指定重定向的 URL 地址，取值范围为 1 到 127 个字符。URL 地址格式为“http://www.abc.com”或“https://www.abc.com”。若不指定该项参数，网页将会定向到用户起始输入的 URL 地址的页面。

［默认取值］

无。

［命令模式］

策略规则配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-policy)# rule id 3
```

```
hostname(config-policy-rule)# web-redirect http://www.baidu.com
```

web-redirect idle-time

配置网页重定向的空闲时间。空闲时间是指网络在无流量状态下保持连接状态的最长时间。超出空闲时间后，网页将会重新定向到系统指定的页面。使用该命令 no 的形式恢复空闲时间的默认值。

［命令］

web-redirect idle-time *time-value*

no web-redirect idle-time

［句法描述］

time-value	指定空闲时间，单位为分钟。默认值是 30 分钟。取值范围是 3 到 1440 分钟。

［默认取值］

30 分钟。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# web-redirect idle-time 60
```

安全控制命令

arp

添加静态 IP-MAC 绑定条目。

［命令］

arp *ip-address mac-address* [**incompatible-auth-arp**] [**vrouter** *vrouter-name*]

no arp {**all** | *ip-address*} [**vrouter** *vrouter-name*]

［句法描述］

arp *ip-address mac-address* [**incompatible-auth-arp**] [**vrouter** *vrouter-name*]

ip-address	指定静态绑定的 IP 地址。
mac-address	指定静态绑定的 MAC 地址。
incompatible-auth-arp	如果配置该参数，则不对该 IP 地址做 ARP 认证。
vrouter *vrouter-name*	添加静态 IP-MAC 绑定条目到指定 VR。用 *vrouter-name* 参数指定 VR 名称。如不指定该参数，配置的静态 IP-MAC 绑定条目将属于缺省 VR——trust-vr。

no arp {**all** | *ip-address*} [**vrouter** *vrouter-name*]

all	指定删除系统中所有静态 IP-MAC 绑定条目。
ip-address	删除指定 IP 地址的 IP-MAC 绑定条目。
vrouter *vrouter-nam*	删除指定 VR 的静态 IP-MAC 绑定条目。用 *vrouter-name* 参数指定 VR 名称。如不指定该参数，系统将删除缺省 VR 中的全部或者指定 IP 地址的静态 IP-MAC 绑定条目。

［默认取值］

无。

［命令模式］

全局模式。

［使用指导］

无。

［命令实例］

hostname(config)# **arp 1.1.1.1 001c.2222.3333**

arp-disable-dynamic-entry

仅允许 IP-MAC 静态绑定的主机上网。使用该命令的 no 形式关闭该功能。

［命令］

arp-disable-dynamic-entry

no arp-disable-dynamic-entry

［句法描述］

无。

［默认取值］

默认情况下，系统允许 ARP 动态学习到的主机上网。

［命令模式］

接口配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# arp-disable-dynamic-entry
```

arp-inspection

配置接口的 ARP 检查功能。使用该命令 no 的形式关闭接口的 ARP 检查功能。

［命令］

arp-inspection {drop | forward}

no arp-inspection

［句法描述］

drop	丢弃 IP 地址不在 ARP 表中的 ARP 包。
forward	转发 IP 地址不在 ARP 表中的 ARP 包。

［默认取值］

无默认值。

［命令模式］

BGroup 或者 VSwitch 接口的接口配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# interface bgroup1
hostname(config-if-bgr1)# arp-inspection forward
```

arp-inspection rate-limit

配置接收 ARP 包的速率限制。使用该命令 no 的形式取消速率限制的配置。

［命令］

arp-inspection rate-limit *number*

no arp-inspection rate-limit

［句法描述］

number	指定接口每秒钟接收 ARP 包的个数。当每秒钟接收 ARP 包的个数超过该指定值时，系统将丢弃超出的 ARP 包。范围是 0 到 10000。

［默认取值］

0，即无速率限制。

［命令模式］

BGroup 或者 VSwitch 接口的接口配置模式。

［使用指导］

接口配置模式（仅适用于物理接口）。

［命令实例］

```
hostname(config)# interface ethernet0/4
hostname(config-if-eth0/4)# arp-inspection rate-limit 200
```

arp-inspection trust

配置设备的某个接口为可信接口。通过可信接口的数据包将不会受到 ARP 检查。使用该命令 no 的形式取消对可信接口的配置。

［命令］

arp-inspection trust

no arp-inspection trust

［句法描述］

无。

［默认取值］

默认情况下，所有的接口都为不可信接口。

［命令模式］

接口配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **interface ethernet0/4**

hostname(config-if-eth0/4)# **arp-inspection trust**

---

arp-inspection vlan

开启 VLAN 的 ARP 检查功能。使用该命令 no 的形式关闭 VLAN 的 ARP 检查功能。

［命令］

arp-inspection vlan *vlan-list* {**drop** | **forward**}

no arp-inspection vlan *vlan-list*

［句法描述］

vlan-list	指定开启 ARP 检查功能的 VLAN 编号。取值范围为 1 到 4094，可以为 1、2-4、1，2，5 等。StoneOS 为 BGroup 保留 32 个 VLAN 编号（从 VLAN224 到 VLAN255）。
drop	丢弃 IP 地址不在 ARP 表中的 ARP 包。
forward	转发 IP 地址不在 ARP 表中的 ARP 包。

［默认取值］

无默认值。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# arp-inspection vlan 2 drop
```

arp-learning

配置接口的 ARP 学习功能。使用该命令 no 的形式关闭接口的 ARP 学习功能。

［命令］

arp-learning

no arp-learning

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

接口配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-if-eth0/0)# arp-learning
```

clear arp

清除系统中的 ARP 绑定信息（静态与动态）。

［命令］

clear arp [**interface** *interface-name* | **vrouter** *vrouter-name*]

［句法描述］

interface-name	清除指定接口的 ARP 绑定信息，使用 *interface-name* 参数指定接口名称。
vrouter-name	删除指定 VRouter 的 ARP 绑定信息，使用 *vrouter-name* 参数知道 VRouter 的名称。如果不指定该参数，将清除缺省 VRouter——trust-vr 的 ARP 绑定信息。

［默认取值］

无。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# clear arp-spoofing-statistics
```

clear arp-spoofing-statistics

清除系统中的 ARP 欺骗攻击统计信息。

［命令］

clear arp-spoofing-statistics

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

执行模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# clear arp-spoofing-statistics
```

clear dhcp-snooping binding

删除所有的或者指定的 DHCP 监控列表条目。

［命令］

clear dhcp-snooping binding [**interface** *interface-name* [*A.B.C.D*] | **vlan** *vlan-id* [*A.B.C.D*]]

［句法描述］

clear dhcp-snooping binding	删除 DHCP 监控列表中所有的绑定条目。

interface *interface-name*	指定接口名称，删除指定接口的绑定条目。
interface *interface-name* [*A.B.C.D*]	指定某个接口下的 IP 地址，删除此接口下特定 IP 的绑定条目。
vlan *vlan-id*	指定 VLAN 编号，删除特定 VLAN 绑定条目。
vlan *vlan-id* [*A.B.C.D*]	指定某特定 VLAN 下的 IP 地址，删除此 VLAN 下特定 IP 的绑定条目。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname(config)# **clear dhcp-snooping binding**

dhcp-snooping（BGroup或者VSwitch接口）

开启 BGroup 或者 VSwitch 接口的 DHCP 监控功能。使用该命令 no 的形式关闭指定接口的 DHCP 监控功能。

［命令］

dhcp-snooping

no dhcp-snooping

［句法描述］

无。

［默认取值］

开启。

［命令模式］

在 BGroup 或者 VSwitch 接口的接口配置模式下。

［使用指导］

无。

［命令实例］

hostname(config)# **interface bgroup1**

```
hostname(config-if-bgr1)# dhcp-snooping
```

dhcp-snooping（物理接口）

配置设备的 DHCP 检查功能，包括配置对 DHCP 请求报文和响应报文的处理方式以及有效性检查。使用该命令 no 的形式关闭 DHCP 检查功能。

［命令］

dhcp-snooping {deny-request|deny-response|validity-check}

no dhcp-snooping {deny-request|deny-response|validity-check}

［句法描述］

deny-request	丢弃从客户端发送到服务器端的所有请求报文。
deny-response	丢弃从服务器端发送到客户端的所有响应报文。
validity-check	检查 DHCP 包的客户端 MAC 地址与以太网包的源 MAC 地址是否一致，如不一致，则丢弃。

［默认取值］

允许所有的 DHCP 请求和响应，无有效性检查。

［命令模式］

以太网接口（BGroup、VSwitch 或者 VLAN 接口中的物理接口）配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# interface ethernet0/3
hostname(config-if-eth0/3)# dhcp-snooping deny-request
```

dhcp-snooping rate-limit

配置接收 DHCP 包的速率限制。使用该命令 no 的形式取消速率限制的配置。

［命令］

dhcp-snooping rate-limit *number*

no dhcp-snooping rate-limit

［句法描述］

number	指定接口每秒钟接收 DHCP 包的个数。当每秒钟接收 DHCP 包的个数超

	过该指定值时，系统将丢弃超出的 DHCP 包。范围是 0 到 10000。

［默认取值］

0，表示无速率限制。

［命令模式］

以太网接口（BGroup、VSwitch 或者 VLAN 接口中的物理接口）配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# interface ethernet0/3
hostname(config-if-eth0/3)# dhcp-snooping rate-limit 2000
```

dhcp-snooping vlan

开启 VLAN 的 DHCP 监控功能。使用该命令 no 的形式关闭 VLAN 的 DHCP 监控功能。

［命令］

dhcp-snooping vlan *vlan-list*

no dhcp-snooping vlan *vlan-list*

［句法描述］

vlan-list	指定开启 DHCP 监控功能的 VLAN 编号。取值范围为 1 到 4094，可以为 1、2-4、1，2，5 等。StoneOS 为 BGroup 保留 32 个 VLAN 编号（从 VLAN224 到 VLAN255）。

［默认取值］

开启。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# dhcp-snooping vlan 2-4
```

exec mac-address dynamic-to-static

强制绑定系统通过 MAC 学习得到的动态 MAC-端口绑定信息。

［命令］

exec mac-address dynamic-to-static

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

执行模式。

［使用指导］

无。

［命令实例］

hostname(config)# **exec mac-address dynamic-to-static**

---

gratuitous-arp-send ip

配置主机防御功能，即安全网关代替不同主机发送免费 ARP 包，保护被代理主机免受 ARP 攻击。使用该命令 no 的形式取消代理指定主机发送免费 ARP 包。

［命令］

gratuitous-arp-send ip *ip-address* **mac** *mac-address* **switch-interface** *interface-name* **except-interface** *interface-name* **rate** *rate-value*

no gratuitous-arp-send ip *ip-address* **switch-interface** *interface-name*

［句法描述］

ip-address	指定被代理主机的 IP 地址。
mac-address	指定被代理主机的 MAC 地址。
switch-interface *interface-name*	指定发送 ARP 广播包的接口。可以是 VSwitch 接口或者 BGroup 接口。
except-interface *interface-name*	指定排除接口，即不发送免费 ARP 包的接口。通常为连接被代理主机的接口。
rate-value	指定安全网关发送免费 ARP 包的速率。单位为个/每秒。取值范围是 1 到 10 个。

［默认取值］

rate-value - 1 个。

［命令模式］

全局配置模式。

［使用指导］

配置多条该命令代理多台主机发送免费 ARP 包。安全网关最多可代理 16 台主机发送免费 ARP 包。

［命令实例］

```
hostname(config)# gratuitous-arp-send ip 1.1.1.1 mac 0000.0000.0001
switch-interface vswitchif1 except-interface ethernet0/5 rate 5
```

host-blacklist

添加主机黑名单条目。用户需要将主机的 MAC 或 IP 地址添加到黑名单中，通过绑定时间表来控制添加到黑名单中的主机在某一时间段不能上网。

［命令］

host-blacklist {**mac** *mac-address* | **ip from** *ip-address* **to** *ip-address* **vrouter** *vrouter-name*} [**schedule** *schedule-name*] [**enable** | **disable**]

［句法描述］

mac-address	指定添加到黑名单的主机的 MAC 地址。
ip-address	指定添加到黑名单的主机的 IP 地址。不允许输入重叠的 IP 地址范围。
vrouter-name	指定 IP 地址对应的 VRouter 的名称。
schedule-name	指定系统中已经配置的时间表名称。如果指定该参数，主机会在时间表指定的时间范围内禁止访问网络。如果不指定该参数，则认为主机永久禁止访问网络。
enable|disable	启用或禁用该主机黑名单条目。如果不指定此项参数，系统默认启用指定的黑名单条目。

［默认取值］

无默认值。

［命令模式］

全局配置模式。

［使用指导］

删除黑名单条目，使用以下命令：

no host-blacklist mac {*mac-address* | **id** *id-number*| **all**}

no host-blacklist ip {**from** *ip-address* **to** *ip-address* **vrouter** *vrouter-name*| **id** *id-number*| **vrouter** *vr-name*}

［命令实例］

hostname(config)# **host-blacklist ip from 1.1.1.1 to 1.1.1.10 vrouter trust-vr schedule night**

host-blacklist ip

用户可以通过指定主机的 IP 地址或指定已创建的 IP 地址主机黑名单条目的 id 编号，启用或禁用该主机黑名单条目。

［命令］

host-blacklist ip { **from** *ip-address* **to** *ip-address* **vrouter** *vrouter-name*|**id** *id-number*} {**enable**|**disable**}

［句法描述］

ip-address	指定添加到黑名单的主机的 IP 地址。不允许输入重叠的 IP 地址范围。
vrouter-name	指定 IP 地址对应的 VRouter 的名称。
id-number	指定主机黑名单条目的 id 编号。
enable|**disable**	启用或禁用该主机黑名单条目。

［默认取值］

无默认值。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **host-blacklist ip id 10 disable**

host-blacklist mac

用户可以通过指定主机的 MAC 地址或指定已创建的 MAC 地址主机黑名单条目的 id 编号，启用或禁用该条主机黑名单条目。

［命令］

host-blacklist mac {*mac-address* |**id** *id-number* }{**enable**|**disable**}

［句法描述］

mac-address	指定添加到黑名单的主机的 MAC 地址。
id-number	指定主机黑名单条目的 id 编号。
enable|**disable**	启用或禁用该主机黑名单条目。

［默认取值］

无默认值。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **host-blacklist mac 001c.f096.f1ea enable**

mac-address-static

添加静态 MAC-端口绑定条目。

［命令］

mac-address-static *mac-address* **interface** *interface-name*

删除系统中所有静态 MAC-端口绑定条目：**no mac-address-static all**

删除指定接口的所有静态 MAC-端口绑定条目：**no mac-address-static interface** *interface-name*

删除指定的 MAC-端口绑定条目：**no mac-address-static** *mac-address* **interface** *interface-name*

［句法描述］

mac-address	指定静态绑定的 MAC 地址。
interface-name	指定静态绑定的端口。

［默认取值］

无默认值。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# mac-address-static 0000.0000.0002 interface
ethernet0/5
```

mac-learning

配置安全网关的 MAC 学习功能。使用该命令 no 的形式关闭 MAC 学习功能。

［命令］

mac-learning

no mac-learning

［句法描述］

无。

［默认取值］

功能为开启状态。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# mac-learning
```

认证与授权命令

aaa-server

指定 AAA 服务器的名称并且进入 AAA 服务配置模式。如果指定的名称已存在，直接进入 AAA 服务配置模式。使用该命令 no 的形式删除指定的 AAA 服务器。

［命令］

aaa-server *aaa-server-name* **type {local | radius | active-directory | ldap}**

no aaa-server *aaa-server-name*

［句法描述］

aaa-server-name	指定 AAA 服务器的名称。
local	指定创建本地类型 AAA 服务器。
radius	指定创建 RADIUS 类型 AAA 服务器。
active-directory	指定创建 Active-Directory 类型服务器。
ldap	指定创建 LDAP 类型 AAA 服务器。

［默认取值］

服务器类型：**local**。

［命令模式］

全局配置模式。

［使用指导］

aaa-server-name 长度范围为 1～31 个字符，且区分大小写。

［命令实例］

```
hostname(config)# aaa-server rad type radius
hostname(config-aaa-server)#
```

accounting

配置 RADIUS 计费主/备份服务器的 IP 地址或域名。使用该命令 no 的形式取消计费主/备份服务器的 IP 地址或者域名配置。

［命令］

accounting {**host** {*ip-address* | *host-name*} | **backup1** {*ip-address* | *host-name*} | **backup2** {*ip-address* | *host-name*}}

no accounting {**host** | **backup1** | **backup2**}

［句法描述］

host {*ip-address* | *host-name*}	指定主服务器的 IP 地址或者域名。
backup1 {*ip-address* | *host-name*}	指定备份服务器 1 的 IP 地址或者域名。
backup2 {*ip-address* | *host-name*}	指定备份服务器 2 的 IP 地址或者域名。

［默认取值］

无。

［命令模式］

RADIUS 服务器配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# aaa-server rad type radius
hostname(config-aaa-server)# accounting host 10.10.10.1
```

accounting enable

开启 RADIUS 服务器的计费功能。使用该命令 no 的形式关闭 RADIUS 服务器的计费功能。

［命令］

accounting enable

no accounting enable

［句法描述］

无。

［默认取值］

关闭。

［命令模式］

RADIUS 服务器配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# aaa-server rad type radius
hostname(config-aaa-server)# accounting enable
```

accounting port

配置 RADIUS 计费服务器端口号。使用该命令 no 的形式恢复端口号的默认值。

［命令］

accounting port *port-number*

no accounting port

［句法描述］

port *port-number*	指定计费服务器的端口号。默认值是 1813。取值范围是 1 到 65535。

［默认取值］

1813。

［命令模式］

RADIUS 服务器配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# aaa-server rad type radius
hostname(config-aaa-server)# accounting port 1000
```

accounting secret

配置 RADIUS 计费服务器的秘密。使用该命令 no 的形式取消对计费服务器秘密的配置。

［命令］

accounting secret *secret*

no accounting secret

［句法描述］

secret *secret*	指定计费服务器的秘密字符串。字符串范围为 1 到 31 个字

	符。

［默认取值］

无。

［命令模式］

RADIUS 服务器配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# aaa-server rad type radius
hostname(config-aaa-server)# accounting secret radafcg
```

admin auth-server

指定系统管理员认证服务器。使用该命令 no 的形式恢复使用默认系统认证服务器“Local”。

［命令］

admin auth-server *server-name*

no admin auth-server

［句法描述］

server-name	指定认证服务器的名称。

［默认取值］

无默认值。

［命令模式］

全局配置模式。

［使用指导］

默认情况下，系统使用“Local”作为系统管理员认证服务器。如果所配置的外部服务器不可达或认证服务不可用，系统会使用“Local”进行系统管理员认证。

［命令实例］

```
hostname(config)# admin auth-server abc
```

agent

指定 Security Agent 监听端口及用户绑定信息删除超时时间。使用该命令 no 的形式取消已指定的监听端口和用户绑定信息删除超时时间。

［命令］

agent [**port** *port-number*] [**disconn-del-timeout** *time*]

no agent

［句法描述］

port *port-number*	指定监听端口号。取值范围为 1025 到 65535。
disconn-del-timeout *time*	指定用户绑定信息删除超时时间。取值范围为 0 到 1800，单位为秒。0 表示永不超时。

［默认取值］

监听端口号：6666；

用户绑定信息删除超时时间：300 秒。

［命令模式］

Active-Directory 服务器配置模式。

［使用指导］

无。

［命令实例］

hostname(config-aaa-server)# **agent port 2323 disconn-del-timeout 1800**

auth-method

指定 Active-Directory 或 LDAP 认证服务器的认证方法。使用该命令 no 的形式恢复 Active-Directory 或 LDAP 认证服务器的默认认证方法。

［命令］

auth-method {plain | digest-md5}

［句法描述］

plain	指定使用明文认证方法。
digest-md5	指定使用 MD5 摘要认证方法。

［默认取值］

digest-md5。

［命令模式］

Active-Directory 服务器配置模式或 LDAP 服务器配置模式。

［使用指导］

无。

［命令实例］

hostname(config-aaa-server)# **auth-method plain**

---

backup1

指定 RADIUS、Active-Directory 或者 LDAP 备份服务器 1 的 IP 地址。该命令可选。使用该命令 no 的形式取消备份服务器 1 的配置。

［命令］

backup1 {*host-name* | *ip-address*}

［句法描述］

host-name | *ip-address*	指定备份服务器 1 的主机名称或 IP 地址。

［默认取值］

无默认值。

［命令模式］

RADIUS 服务器配置模式、LDAP 服务器配置模式或者 Active-Directory 服务器配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **aaa-server rad type radius**
hostname(config-aaa-server)# **backup1 1.1.1.1**

---

backup2

指定 RADIUS、Active-Directory 或者 LDAP 备份服务器 2 的 IP 地址。该命令可选。使用该命令 no 的形式取消备份服务器 2 的配置。

［命令］

backup2 {*host-name* | *ip-address*}

［句法描述］

host-name | *ip-address*	指定备份服务器 2 的主机名称或 IP 地址。

［默认取值］

无默认值。

［命令模式］

RADIUS 服务器配置模式、Active-Directory 服务器配置模式或者 LDAP 服务器配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# aaa-server server1 type active-directory
hostname(config-aaa-server)# backup2 5.5.5.5
```

base-dn

指定 Active-Directory 或 LDAP 认证服务器的 Base-DN。使用该命令 no 的形式取消 Active-Directory 或 LDAP 认证服务器 Base-DN 的指定。

［命令］

base-dn *string*

no base-dn

［句法描述］

string	指定 Base-DN 的具体内容。

［默认取值］

无。

［命令模式］

Active-Directory 或 LDAP 服务器配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-aaa-server)# base-dn hillstone
```

debug aaa

显示 AAA 的调试信息。

［命令］

debug aaa [accounting | authentication | authorization | internal | radius | ldap | user]

［句法描述］

accounting	显示 AAA 计费的调试信息。
authentication	显示 AAA 认证的调试信息。
authorization	显示 AAA 授权的调试信息。
internal	显示 AAA 本地认证的调试信息。
radius	显示 AAA RADIUS 认证的调试信息。
ldap	显示 LDAP（包括 Active-Directory 和 LDAP 服务器）认证的调试信息
user	显示本地用户属性变化时的调试信息

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname(config)# **debug aaa radius**

group-class

指定 LDAP 认证服务器的组对象 objectClass 的值。使用该命令 no 的形式恢复默认值。

［命令］

group-class *string*

no group-class

［句法描述］

string	指定组对象 objectClass 的值。为 1 到 63 个字符的字符串。

［默认取值］

groupofuniquenames。

［命令模式］

LDAP 服务器配置模式。

［使用指导］

无。

［命令实例］

hostname(config-aaa-server)# **group-class uninames**

---

host

指定 RADIUS、Active-Directory 或者 LDAP 认证主服务器的主机名称或 IP 地址。

［命令］

host {*host-name* | *ip-address*}

［句法描述］

host-name | *ip-address*	指定认证主服务器的主机名称或 IP 地址。

［默认取值］

无默认值。

［命令模式］

RADIUS 服务器配置模式、Active-Directory 服务器配置模式或者 LDAP 服务器配置模式。

［使用指导］

无。

［命令实例］

hostname(config-aaa-server)# **host 202.100.10.1**

---

login-dn

指定 Active-Directory 或 LDAP 认证服务器的登录 DN。使用该命令 no 的形式取消 Active-Directory 或 LDAP 认证服务器登录 DN 的指定。

［命令］

login-dn *string*

no login-dn

［句法描述］

string	指定登录 DN 的具体内容。

［默认取值］

无。

［命令模式］

Active-Directory 服务器配置模式或 LDAP 服务器配置模式。

［使用指导］

无。

［命令实例］

hostname(config-aaa-server)# **login-dn aaa**

login-password

指定 Active-Directory 或 LDAP 认证服务器的登录密码。用该命令 no 的形式取消 Active-Directory 或 LDAP 认证服务器登录密码的指定。

［命令］

login-password *string*

no login-password

［句法描述］

string	指定登录密码的具体内容。

［默认取值］

无。

［命令模式］

Active-Directory 服务器配置模式。

［使用指导］

无。

［命令实例］

hostname(config-aaa-server)# **base-dn 123456**

member-attribute

指定 LDAP 认证服务器的成员属性名。使用该命令 no 的形式恢复 LDAP 认证服务器的成员属性名位默认值。

［命令］

member-attribute *string*

no member-attribute

［句法描述］

string	指定 LDAP 认证主服务器的成员属性名。为 1 到 63 个字符的字符串。

［默认取值］

uniqueMember。

［命令模式］

LDAP 服务器配置模式。

［使用指导］

无。

［命令实例］

hostname(config-aaa-server)# **member-attribute unimem**

naming-attribute

指定 LDAP 认证服务器的名称属性。使用该命令 no 的形式恢复 LDAP 认证服务器的名称属性为默认值。

［命令］

naming-attribute *string*

no naming-attribute

［句法描述］

string	指定 LDAP 认证主服务器的名称属性。为 1 到 63 个字符的字符串。

［默认取值］

uid。

［命令模式］

LDAP 服务器配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-aaa-server)# naming-attribute cn
```

port

指定 Active-Directory 或 LDAP 认证服务器的端口号。使用该命令 no 的形式恢复 Active-Directory 或 LDAP 认证服务器的默认端口号。

［命令］

port *port-number*

no port

［句法描述］

port-number	指定认证主服务器的端口号。范围是 1 到 65535。

［默认取值］

398。

［命令模式］

Active-Directory 或 LDAP 服务器配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-aaa-server)# port 3988
```

radius port

指定 RADIUS 服务器的端口号。该命令可选。

［命令］

radius port *port-unmber*

［句法描述］

port-unmber	指定 RADIUS 服务器的端口号。范围是 1 到 65535。

［默认取值］

1812。

［命令模式］

RADIUS 服务配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-aaa-server)# radius port 1810
```

radius secret

指定 RADIUS 服务器的秘密。

［命令］

radius secret *secret*

［句法描述］

secret	指定 RADIUS 服务器的秘密。

［默认取值］

无。

［命令模式］

RADIUS 服务配置模式。

［使用指导］

该命令指定的密钥必须与 RADIUS 服务器的秘密相同。

［命令实例］

```
hostname(config-aaa-server)# radius secret aaa
```

retries

该命令可选。指定安全网关在没有收到服务器回应时重新向 RADIUS 服务器发送认证报文的重传次数。使用该命令 no 的形式恢复重传次数的默认值。

［命令］

retries *times*

［句法描述］

times	指定 RADIUS 服务器的重传次数。取值范围是 1 到 10。

［默认取值］

默认为 3 次。

［命令模式］

RADIUS 服务配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-aaa-server)# retries 5
```

role-mapping-rule

为 AAA 认证服务器（local、RADIUS、Active-Directory 和 LDAP）指定角色映射规则。使用该命令 no 的形式取消角色映射规则的指定。

［命令］

role-mapping-rule *rule-name*

no role-mapping-rule

［句法描述］

rule-name	指定系统中已经配置的角色映射规则的名称。

［默认取值］

无。

［命令模式］

Local、RADIUS、Active-Directory 或者 LDAP 服务配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-aaa-server)# role-mapping-rule rule1
```

timeout

该命令可选。指定 RADIUS 服务器的应答超时时间。如果在超时时间结束时安全网关仍未收到服务器的应答，则会重新发送认证报文。使用该命令 no 的形式恢复超时时间的默认值。

［命令］

timeout *timeout-value*

［句法描述］

timeout-value	指定 RADIUS 服务器的重传次数。取值范围是 1 到 30 秒。

［默认取值］

3 秒。

［命令模式］

RADIUS 服务配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-aaa-server)# timeout 6
```

802.1X 认证协议命令

aaa-server

用户可以将已配置好的 AAA 服务器指定为 802.1X 的认证服务器。使用该命令 no 的形式删除指定的 802.1X 认证服务器。

［命令］

aaa-server *server-name*

no aaa-server *server-name*

［句法描述］

server-name	指定已配置好的 AAA 服务器名称。

［默认取值］

无。

［命令模式］

dot1x 配置模式。

［使用指导］

目前版本支持将 AAA 本地认证服务器或 RADIUS 服务器指定为 802.1X 认证服务器。

［命令实例］

hostname(config-dot1x)# **aaa-server local**

dot1x allow-multi-logon

配置 802.1X 用户同名登录功能。开启该功能后，系统允许同一用户在不同的客户端上登录。使用该命令 no 的形式关闭用户同名登录功能。

［命令］

dot1x allow-multi-logon

no dot1x allow-multi-logon

［句法描述］

无。

［默认取值］

关闭。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **dot1x allow-multi-logon**

---

dot1x allow-multi-logon *number*

开启用户同名登录功能后，使用该命令指定用户同名登录次数。

［命令］

dot1x allow-multi-logon *number*

［句法描述］

number	指定用户同名登录次数。范围是 2 到 1000。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **dot1x allow-multi-logon 3**

---

dot1x auto-kickout

开启拒绝同名用户登录功能。使用该命令的 no 形式关闭拒绝同名用户登录功能。

［命令］

dot1x auto-kickout

no dot1x auto-kickout

［句法描述］

无。

［默认取值］

开启。

［命令模式］

全局配置模式。

［使用指导］

802.1X 用户同名登录功能为关闭状态时，如果开启拒绝同名用户登录功能，同一用户再次登录的信息会替换掉已登录的信息，系统自动断开已登录的连接。如果关闭拒绝同名用户登录功能，则系统禁止同一用户再次登录。

［命令实例］

hostname(config)# **dot1x auto-kickout**

---

dot1x control-mode

配置 802.1X 端口接入控制的方式。使用该命令 no 的形式恢复默认设置。

［命令］

dot1x control-mode {mac | port}

no dot1x control-mode

［句法描述］

mac	基于 MAC 地址进行认证。对一个端口下连接的所有客户端都必须通过认证，才能访问网络资源。
port	基于端口进行认证。对一个端口下连接的所有客户端，只要有一个客户端通过认证，其他客户端不必通过认证，即可访问网络资源。

［默认取值］

port（基于端口进行认证）

［命令模式］

接口配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **interface ethernet0/0**

```
hostname(config-if-eth0/0)# dot1x enable
hostname(config-if-eth0/0)# dot1x profile profile1
hostname(config-if-eth0/0)# dot1x control-mode mac
```

dot1x enable

开启端口的 802.1X 认证。使用该命令 no 的形式关闭端口的 802.1X 认证。

［命令］

dot1x enable

no dot1x enable

［句法描述］

无。

［默认取值］

关闭。

［命令模式］

接口配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# dot1x enable
```

dot1x max-user

配置认证系统端口允许同时接入客户端数量最大值。使用该命令 no 的形式恢复端口允许接入的最大客户端数量的默认值。

［命令］

dot1x max-user *user-number*

no dot1x max-user

［句法描述］

user-number	指定允许同时接入的客户端数量最大值。范围是 1 至 1000。

［默认取值］

端口允许同时接入的客户端数量的默认值根据平台的不同而不同。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# dot1x max-user 15
```

dot1x port-control

配置 802.1X 在指定端口上进行接入控制的模式。使用该命令 no 的形式恢复默认设置。

［命令］

```
dot1x port-control {auto | force-unauthorized}
no dot1x port-control
```

［句法描述］

auto	自动模式。在此模式下，认证系统依据 802.1X 协议认证的结果决定客户端是否可以接入网络。
force-unauthorized	强制未授权模式。在此模式下，端口始终为未授权模式，任何客户端都无法与之建立连接。

［默认取值］

auto（自动模式）

［命令模式］

接口配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# dot1x enable
hostname(config-if-eth0/0)# dot1x profile profile1
hostname(config-if-eth0/0)# dot1x port-control auto
```

dot1x profile

将已创建的 802.1X Profile 绑定到端口上。使用该命令 no 的形式解除绑定。

［命令］

dot1x profile *profile-name*

no dot1x profile *profile-name*

［句法描述］

profile-name	指定已创建的 802.1X Profile 名称。

［默认取值］

无。

［命令模式］

接口配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# dot1x enable
hostname(config-if-eth0/0)# dot1x profile profile1
```

dot1x profile

创建 802.1X Profile。使用该命令 no 的形式删除指定的 802.1X Profile。

［命令］

dot1x profile *profile-name*

no dot1x profile *profile-name*

［句法描述］

profile-name	指定所创建的 802.1X Profile 的名称。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

执行该命令后，系统将创建指定名称的 802.1X Profile，并进入 dot1x 配置模式；如果指定的名称已存在，则直接进入 dot1x 配置模式。

［命令实例］

hostname(config)# **dot1x profile profile2**

dot1x timeout

指定已认证的客户端超时时间。对于已通过 802.1X 认证的客户端，用户可以配置它的认证超时时间。客户端在此时间内没有回应认证系统，则需要再次申请认证。使用该命令 no 的形式恢复默认值。

［命令］

dot1x timeout *timeout-value*

no dot1x timeout

［句法描述］

timeout-value	指定已认证的客户端超时时间，单位为秒。范围是 180 至 3600*24 秒。

［默认取值］

300 秒。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **dot1x timeout 500**

exec dot1x kickout

强制断开某个客户端与认证系统的连接。使用该命令 no 的形式恢复默认值。

［命令］

exec dot1x kickout *port-name authenticated-user-mac*

［句法描述］

port-name	指定客户端连接的端口名称。

authenticated-user-mac	指定被强制断开连接的已认证客户端的 MAC 地址。

［默认取值］

无。

［命令模式］

任何配置模式。

［使用指导］

无。

［命令实例］

hostname# **exec dot1x kickout ethernet0/1**

quiet-period

指定认证系统的静默时间。如果认证失败，认证系统需要静默一段时间后再重新处理同一客户端的请求。使用该命令 no 的形式恢复默认值。

［命令］

quiet-period *value*

no quiet-period

［句法描述］

value	指定认证系统在认证失败之后处于静默时间的秒数。范围为 0 至 65535 秒。

［默认取值］

60 秒。

［命令模式］

dot1x 配置模式。

［使用指导］

如果取值为 0，则表示认证系统一直处理同一客户端的请求。

［命令实例］

hostname(config-dot1x)# **quiet-period 360**

reauth-period

当客户端认证成功并接入网络后，指定认证系统对客户端进行重认证时间间隔。使用该命令 no 的形式恢复默认值。

［命令］

reauth-period *value*

no reauth-period

［句法描述］

value	指定认证系统对客户端的重认证时间间隔。范围为 0 至 65535 秒。

［默认取值］

3600 秒。

［命令模式］

dot1x 配置模式。

［使用指导］

如果取值为 0，则关闭重认证功能。

［命令实例］

hostname(config-dot1x)# **reauth-period 500**

retransmission-count

配置认证请求帧的最大可重复发送次数。如果认证系统初次向客户端发送认证请求帧后，在规定的时间内没有收到客户端的响应，则认证系统将再次向客户端发送请求。如果超过指定次数，放弃尝试。使用该命令 no 的形式恢复默认值。

［命令］

retransmission-count *value*

no retransmission-count

［句法描述］

value	指定认证请求帧的最大可重复发送次数。范围为 1 至 10 次。

［默认取值］

2 次。

［命令模式］

dot1x 配置模式。

［使用指导］

无。

［命令实例］

hostname(config-dot1x)# **retransmission-count 5**

server-timeout

指定认证服务器超时时间。认证系统将客户端响应后送上来的数据传送给认证服务器。如果在指定的认证服务器超时时间结束时，认证系统仍未收到认证服务器的应答，则会重新发送此数据包到认证服务器。使用该命令 no 的形式恢复默认值。

［命令］

server-timeout *value*

no server-timeout

［句法描述］

value	指定认证服务器应答超时时间。范围为 1 至 65535 秒。

［默认取值］

30 秒。

［命令模式］

dot1x 配置模式。

［使用指导］

无。

［命令实例］

hostname(config-dot1x)# **server-timeout 1000**

tx-period

指定客户端超时时间。当认证系统向客户端发送请求报文，请求客户端上传用户名后，客户端需要在指定时间内向认证系统发送应答报文。如果未在指定的客户端超时时间内完成发送，则认证系统将重发认证请求报文到客户端。使用该命令 no 的形式恢复默认值。

［命令］

tx-period *value*

no tx-period

［句法描述］

value	指定客户端传送应答报文的超时时间。范围为 1 至 65535 秒。

［默认取值］

30 秒。

［命令模式］

dot1x 配置模式。

［使用指导］

无。

［命令实例］

hostname(config-dot1x)# **tx-period 100**

网络地址转换（NAT）命令

dnatrule

配置或一条 DNAT 规则或者覆盖指定 ID 的 NAT 规则。

［命令］

做 NAT 转换：**dnatrule** [**id** *id*] [**before** *id* | **after** *id* | **top**] **from** *src-address* **to** *dst-address* [**service** *service-name*] **trans-to** *trans-to-address* [**port** *port*] [**load-balance**] [**track-tcp** *port*] [**track-ping**] [**log**] [**group** *group-id*]

不做 NAT 转换：**dnatrule** [**id** *id*] [**before** *id* | **after** *id* | **top**] **from** *src-address* **to** *dst-address* [**service** *service-name*] **no-trans** [**group** *group-id*]

［句法描述］

id *id*	指定 DNAT 规则 ID 号。每一条 DNAT 规则都有一个唯一的 ID。如果用户不指定，系统会为规则自动生成一个 ID。如果指定的 ID 为已有的 DNAT 规则的 ID，已有的规则会被覆盖。
before *id*	指定所创建的 DNAT 规则的位置是在某个 ID 之前。
after *id*	指定所创建的 DNAT 规则的位置是在某个 ID 之后。
top	指定所创建的 DNAT 规则的位置是在所有规则的首位。
from *src-address*	指定流量的源地址。该地址为 IP 地址或者系统地址簿中定义的地址条目。
to *dst-address*	指定流量的目的地址。该地址为 IP 地址或者系统地址簿中定义的地址条目。
service *service-name*	指定流量的服务类型。如果需要一并转换端口号（通过 **port** *port* 参数指定），这里指定的服务就只能拥有一个协议和一个端口，例如 TCP 端口号可以是 80，但不可以是 80 到 100。
no-trans	不做 NAT 转换。
trans-to *trans-to-address*	把相匹配的流量的目的 IP 地址转换成指定的 IP 地址。*trans-to-address* 是 IP 地址或者系统系统地址簿中定义的地址条目。流量目的 IP 地址 *dst-address* 的个数必须与 *trans-to-address* 的 IP 地址个数相同。
port	内网服务器的端口号。
load-balance	配置 **load-balance** 参数为该条 DNAT 规则开启负载均衡功能，即均衡流量到不同的内网服务器。
track-tcp *port*	配置 **track-tcp** 参数并指定内网服务器端口号，系统会向内网服务器发送 TCP 报文，监控服务器的特定 TCP 端口是否可达。

track-ping	配置 **track-ping** 参数，系统会向内网服务器发送 Ping 报文，监控服务器是否可达。
log	使用该参数开启该 DNAT 规则的日志功能（当有流量匹配该地址转换规则时产生日志信息）。
group *group-id*	指定 DNAT 规则所属的 HA 组。如不指定该参数，创建的 DNAT 规则属于 HA 组 0。

［默认取值］

无默认值。

［命令模式］

VRouter 配置模式/NAT 配置模式（仅用于为缺省 VR 即 trust-vr 配置 NAT）。

［使用指导］

如果不指定规则的排列位置，系统会把所创建的 DNAT 规则排在所有 DNAT 规则的末尾。

［命令实例］

```
hostname(config)# ip vrouter vrouter1
hostname(config-vrouter)# dnatrule from any to addr1 service any trans-to addr2
rule id=1
```

dnatrule move

移动已有 DNAT 规则以改变规则的排列顺序。

［命令］

dnatrule move *id* {**before** *id* | **after** *id*| **top** | **bottom**}

［句法描述］

id	指定要移动的规则的 ID 号。
before *id*	将规则移动到某个 ID 之前。
after *id*	将规则移动到某个 ID 之后。
top	将规则移动到所有 DNAT 规则之首。
bottom	将规则移动到所有 DNAT 规则的末尾。

［默认取值］

无默认值。

［命令模式］

VRouter 配置模式/NAT 配置模式（仅用于为缺省 VR 即 trust-vr 配置 NAT）。

［使用指导］

无。

［命令实例］

```
hostname(config-vrouter)# dnatrule move 1 bottom
```

expanded-port-pool

当 SNAT 的转换模式为 dynamicport 时，用户可以开启扩展 PAT 端口池功能，扩展 NAT 转换后的网络地址端口资源。

［命令］

开启扩展 PAT 端口池功能：**expanded-port-pool**

关闭扩展 PAT 端口池功能：**no expanded-port-pool**

［句法描述］

无。

［默认取值］

扩展 PAT 端口池功能默认关闭。

［命令模式］

全局配置模式。

［使用指导］

安全网关的部分平台支持扩展 PAT 端口池功能，并且不同平台支持的扩展端口资源倍数不同；

扩展 PAT 端口池功能在配置 SNAT 规则前开启有效；如果在开启该功能前，系统中已配置 SNAT 规则，请重启设备使其生效。

［命令实例］

```
hostname(config)# expanded-port-pool
```

nat

进入 NAT 配置模式（仅用于为缺省 VR 即 trust-vr 配置 NAT）。

［命令］

nat

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# nat
hostname(config-nat)#
```

no dnatrule id

删除指定 ID 号的 DNAT 规则。

［命令］

no dnatrule id *id*

［句法描述］

id	指定要删除的 DNAT 规则的 ID 号。

［默认取值］

无默认值。

［命令模式］

VRouter 配置模式/NAT 配置模式（仅用于为缺省 VR 即 trust-vr 配置 NAT）。

［使用指导］

无。

［命令实例］

```
hostname(config-vrouter)# no dnatrule id 5
```

no snatrule id

删除指定 ID 号的 SNAT 规则。

［命令］

no snatrule id *id*

［句法描述］

id	指定要删除的 SNAT 规则的 ID 号。

［默认取值］

无默认值。

［命令模式］

VRouter 配置模式/NAT 配置模式（仅用于为缺省 VR 即 trust-vr 配置 NAT）。

［使用指导］

无。

［命令实例］

hostname(config-vrouter)# **no snatrule id 5**

snatrule

配置或一条 SNAT 规则或者覆盖指定 ID 的 NAT 规则。

［命令］

做 NAT 转换：**snatrule** [**id** *id*] [**before** *id* | **after** *id* | **top**] **from** *src-address* **to** *dst-address* [**service** *service-name*] [**eif** *egress-interface* | **evr** *vrouter-name*] **trans-to** {**addressbook** *trans-to-address* | **eif-ip**} **mode** {**static** | **dynamicip** | **dynamicport** [**sticky**]} [**log**] [**group** *group-id*]

不做 NAT 转换：**snatrule** [**id** *id*] [**before** *id* | **after** *id* | **top**] **from** *src-address* **to** *dst-address* [**eif** *egress-interface* | **evr** *vrouter-name*] **no-trans** [**group** *group-id*]

［句法描述］

id *id*	指定 SNAT 规则 ID 号。每一条 SNAT 规则都有一个唯一的 ID。如果用户不指定，系统会为规则自动生成一个 ID。如果指定的 ID 为已有的 SNAT 规则的 ID，已有的规则会被覆盖。
before *id*	指定所创建的 SNAT 规则的位置是在某个 ID 之前。
after *id*	指定所创建的 SNAT 规则的位置是在某个 ID 之后。
top	指定所创建的 SNAT 规则的位置是在所有规则的首位。
from *src-*	指定流量的源地址。该地址为 IP 地址或者系统地址簿中定义的地址条

address	目。
to *dst-address*	指定流量的目的地址。该地址为 IP 地址或者系统地址簿中定义的地址条目。
service *service-name*	指定流量的服务类型。service-name 为服务簿中定义的服务，目前暂不支持指定带星号（“*”）的服务。
eif *egress-interface* | **evr** *vrouter-name*	指定流量的出接口（**eif** *egress-interface*）或者流量的下一跳 VRouter（**evr** *vrouter-name*）。
no-trans	不做 NAT 转换。
trans-to	把相匹配的流量的源 IP 地址转换成指定的 IP 地址。
addressbook *trans-to-address*	把相匹配的流量的源 IP 地址转换成 IP 地址或者系统地址簿中定义的地址条目。
eif-ip	把相匹配的流量的源 IP 地址转换成出接口的 IP 地址。
mode	指定转换模式。 • **static**：静态源 NAT 转换即一对一的转换。该模式要求被转换到的地址条目（*trans-to-address*）包涵的 IP 地址数与流量的源地址的地址条目（*src-address*）包含的 IP 地址数相同。 • **dynamicip**：动态源 NAT 转换即多对多的转换。该模式将源地址转换到指定的 IP 地址。每一个源地址会被映射到一个唯一的 IP 地址做转换，直到指定地址都被占用。 • **dynamicport [sticky]**：即 PAT。多个源地址将被转换成指定 IP 地址条目中的一个地址。如果不使用 sticky，地址条目中的第一个地址将会首先被使用，当地一个地址的端口资源被用尽，第二个地址将会被使用。如果使用了 sticky，每一个源 IP 会被映射到一个固定的 IP 地址。
log	使用该参数开启该 SNAT 规则的日志功能（当有流量匹配该地址转换规则时产生日志信息）。
group *group-id*	指定 SNAT 规则所属的 HA 组。如不指定该参数，创建的 SNAT 规则属于 HA 组 0。

［默认取值］

无默认值。

［命令模式］

VRouter 配置模式/NAT 配置模式（仅用于为缺省 VR 即 trust-vr 配置 NAT）。

［使用指导］

如果不指定规则的排列位置，系统会把所创建的 SNAT 规则排在所有 SNAT 规则的末尾位。

［命令实例］

```
hostname(config)# ip vrouter vrouter1
hostname(config-vrouter)# snatrule from any to any eif ethernet0/0
trans-to eif-ip mode dynamicport
```

```
rule id=1
```

snatrule move

移动已有 SNAT 规则以改变规则的排列顺序。

［命令］

snatrule move *id* {**before** *id* | **after** *id* | **top** | **bottom**}

［句法描述］

id	指定要移动的规则的 ID 号。
before *id*	将规则移动到某个 ID 之前。
after *id*	将规则移动到某个 ID 之后。
top	将规则移动到所有 SNAT 规则之首。
bottom	将规则移动到所有 SNAT 规则的末尾。

［默认取值］

无默认值。

［命令模式］

VRouter 配置模式/NAT 配置模式（仅用于为缺省 VR 即 trust-vr 配置 NAT）。

［使用指导］

无。

［命令实例］

```
hostname(config-nat)# snatrule move 1 bottom
```

应用层识别与控制命令

alg

开启应用的 ALG 功能。使用该命令 no 的形式关闭应用的 ALG 功能。

［命令］

alg {all | TFTP | FTP | RSH |…}

no alg {all | TFTP | FTP | RSH | …}

［句法描述］

all	开启或者关闭所有应用的 ALG 功能。
**TFTP	FTP	RSH	…**	开启或者关闭指定应用的 ALG 功能。

［默认取值］

无默认值。

［命令模式］

全局配置模式。

［使用指导］

如果关闭 HTTP 的 ALG 功能，安全网关的 HTTP 内容阻断功能将失效。

［命令实例］

hostname(config)# **alg all**

alg h323 session-time

指定 H323 的超时时间。使用 no 的形式取消对 H323 超时时间的指定。

［命令］

alg h323 session-time *time-value*

no alg h323 session-time

［句法描述］

time-value	指定 H323 的超时时间。范围是 60 到 1800 秒。

［默认取值］

默认为 60 秒。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# alg h323 session-time 1200
```

IPSec协议命令

accept-all-proxy-id

开启接受对端 ID 功能。开启该功能后，如果安全设备作为接收端，它将接受对端的 ID 为它的 IKE 协商第二阶段 ID，并返回该 ID 给对端。使用该命令 no 的形式关闭接受对端 ID 功能。

［命令］

accept-all-proxy-id

no accept-all-proxy-id

［句法描述］

无。

［默认取值］

禁用。

［命令模式］

IKE 隧道配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# tunnel ipsec 11 auto
hostname(config-tunnel-ipsec-auto)# accept-all-proxy-id
```

anti-replay

为 IKE 隧道配置防重放功能。使用该命令 no 的形式恢复系统的默认配置。

［命令］

anti-replay {32 | 64 | 128 | 256 | 512}

no anti-replay

［句法描述］

32	指定防重放的窗口为 32。

64	指定防重放的窗口为 64。
128	指定防重放的窗口为 128。
256	指定防重放的窗口为 256。
512	指定防重放的窗口为 512。

［默认取值］

32。

［命令模式］

IKE 隧道配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# tunnel t2 ipsec auto
hostname(config-tunnel-ipsec-auto)# anti-replay 256
```

authentication

为 P1 提议指定 IKE 身份认证方式。使用该命令 no 的形式恢复默认认证方式。

［命令］

```
authentication {pre-share | rsa-sig | dsa-sig}
no authentication
```

［句法描述］

pre-share	指定使用预共享密钥认证方式。
rsa-sig	指定使用 RSA 数字证书认证方式。
dsa-sig	指定使用 DSA 数字证书认证方式。

［默认取值］

预共享密钥认证方式。

［命令模式］

P1 提议配置模式。

［使用指导］

当使用 DSA 数字认证方式时，对应的验证算法只能为 SHA-1。

［命令实例］

```
hostname(config)# isakmp proposal proposal1
```

```
hostname(config-isakmp-proposal)# authentication pre-share
```

auto-connect

配置自动连接功能。使用该命令 no 的形式恢复默认方式。

［命令］

auto-connect

no auto-connect

［句法描述］

无。

［默认取值］

默认情况下，没有配置自动连接功能。

［命令模式］

IKE 隧道配置模式。

［使用指导］

安全网关提供了两种连接建立方式：自动方式和流量触发方式。默认情况下，使用流量触发方式。当需要配置为自动方式时可使用本命令。

［命令实例］

```
hostname(config)# tunnel ipsec 11 auto
hostname(config-tunnel-ipsec-auto)# auto-connect
```

compression deflate （manual）

为手工密钥 VPN 隧道指定压缩算法（DEFLATE 算法）。使用该命令 no 的形式取消对压缩算法的指定。

［命令］

compression deflate

no compression

［句法描述］

无。

［默认取值］

默认情况下，无任何压缩算法。

［命令模式］

手工密钥 VPN 配置模式。

［使用指导］

无

［命令实例］

```
hostname(config)# tunnel ipsec vpn1 manual
hostname(config-tunnel-ipsec-manual)# compression deflate
```

---

compression deflate （P2）

为 P2 提议指定压缩算法（DEFLATE 算法）。使用该命令 no 的形式取消对压缩算法的指定。

［命令］

```
compression deflate
no compression
```

［句法描述］

无。

［默认取值］

默认情况下，无任何压缩算法。

［命令模式］

P2 提议配置模式。

［使用指导］

无

［命令实例］

```
hostname(config)# ipsec proposal p2
hostname(config-ipsec-proposal)# compression deflate
```

---

connection-type

为 IKE 对等体指定连接类型。使用该命令 no 的形式恢复默认连接方式。

［命令］

connection-type {bidirectional | initiator-only | responder-only}

no connection-type

［句法描述］

bidirectional	指定该 IKE 对等体既是发起端也是响应端。
initiator-only	指定该 IKE 对等体仅是发起端。
responder-only	指定该 IKE 对等体仅是响应端。

［默认取值］

bidirectional。

［命令模式］

IKE 对等体配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **isakmp peer peer1**

hostname(config-isakmp-peer)# **connection-type initiator-only**

df-bit

为 IKE 隧道配置分片处理功能。使用该命令 no 的形式恢复系统的默认配置。

［命令］

df-bit {copy | clear | set}

no df-bit

［句法描述］

copy	直接从发包端拷贝 IP 包。
clear	允许转发设备对包做分片处理。
set	不允许转发设备对包做分片处理。

［默认取值］

copy。

［命令模式］

IKE 隧道配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# tunnel t2 ipsec auto
hostname(config-tunnel-ipsec-auto)# df-bit clear
```

dpd

为 IKE 对等体开启 DPD 功能。使用该命令 no 的形式关闭 DPD 功能。

［命令］

dpd [**interval** *seconds*] [**retry** *times*]

no dpd

［句法描述］

interval	指定向对端发送查询请求的时间间隔。范围是 0 到 10 秒。
retry	指定向对端发送查询请求的次数。范围是 1 到 10 次。

［默认取值］

interval – 0（不开启 DPD 功能）。

retry – 3 次。

［命令模式］

IKE 对等体配置模式。

［使用指导］

向对端发送查询请求后，如果本端在指定的时间间隔内收不到对端的报文，系统会在再次发送查询请求，如此反复，直到完成该参数指定的次数。在指定次数查询完成后如果仍然收不到对端的报文，则判断对端对等体已经死掉。

［命令实例］

```
hostname(config)# isakmp peer peer1
hostname(config-isakmp-peer)# dpd
```

encryption （P1）

为 P1 提议指定加密算法。使用该命令 no 的形式恢复默认加密算法。

［命令］

encryption {3des | des | aes | aes-192 | aes-256}

no encryption

［句法描述］

3des	指定使用 3DES 加密方法。密钥长度为 192 比特。
des	指定使用 DES 加密方法。密钥长度为 64 比特。
aes	指定使用 AES 加密方法。密钥长度为 128 比特。
aes-192	指定使用 192bit AES 加密方法。密钥长度为 192 比特。
aes-256	指定使用 256bit AES 加密方法。密钥长度为 256 比特。

［默认取值］

3DES 加密方法。

［命令模式］

P1 提议配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# isakmp proposal proposal1
hostname(config-isakmp-proposal)# encryption aes
```

encryption （manual）

为手动配置 IPSec 隧道指定加密算法。使用该命令 no 的形式恢复默认加密算法。

［命令］

encryption {3des | des | aes | aes-192 | aes-256 | null}

no encryption

［句法描述］

3des	指定使用 3DES 加密方法。密钥长度为 192 比特。
des	指定使用 DES 加密方法。密钥长度为 64 比特。
aes	指定使用 AES 加密方法。密钥长度为 128 比特。
aes-192	指定使用 192bit AES 加密方法。密钥长度为 192 比特。
aes-256	指定使用 256bit AES 加密方法。密钥长度为 256 比特。
null	不使用加密功能。

［默认取值］

3DES 加密方法。

［命令模式］

手工 IPSec 隧道配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# tunnel t1 ipsec manual
hostname(config-tunnel-ipsec-manual)# encryption aes
```

encryption （P2）

为 P2 提议指定加密算法。使用该命令 no 的形式恢复默认加密算法。

［命令］

encryption {3des | des | aes | aes-192 | aes-256 | null} [3des | des | aes | aes-192 | aes-256 | null] [3des | des | aes | aes-192 | aes-256 | null]…

no encryption

［句法描述］

3des	指定使用 3DES 加密方法。密钥长度为 192 比特。
des	指定使用 DES 加密方法。密钥长度为 64 比特。
aes	指定使用 AES 加密方法。密钥长度为 128 比特。
aes-192	指定使用 192bit AES 加密方法。密钥长度为 192 比特。
aes-256	指定使用 256bit AES 加密方法。密钥长度为 256 比特。
null	不使用加密功能。

［默认取值］

3des。

［命令模式］

P2 提议配置模式。

［使用指导］

最多可为一个 P2 提议指定四种不同的加密算法。

［命令实例］

```
hostname(config)# ipsec proposal proposal1
hostname(config-ipsec-proposal)# encryption 3des aes
```

encryption-key

为手动配置 IPSec 隧道指定协议的加密密钥。使用该命令 no 的形式取消对加密密钥的配置。

［命令］

encryption-key inbound *hex-number-string* **outbound** *hex-number-string*

no encryption-key

［句法描述］

inbound	配置本端进方向的加密密钥。
outbound	配置本端出方向的加密密钥。

［默认取值］

无默认值。

［命令模式］

手工 IPSec 隧道配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **tunnel t1 ipsec manual**

hostname(config-tunnel-ipsec-manual)# **encryption-key inbound 1111 outbound 2222**

group （P1）

为 P1 提议指定 DH 组。使用该命令 no 的形式恢复默验 DH 组的选择。

［命令］

group { **1** | **2** | **5** }

no group

［句法描述］

1	选择 DH 组 1。密钥的长度为 768 比特。
2	选择 DH 组 2。密钥的长度为 1024 比特。
5	选择 DH 组 5。密钥的长度为 1536 比特。

［默认取值］

2。

［命令模式］

P1 提议配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# isakmp proposal proposal1
hostname(config-isakmp-proposal)# group 5
```

group （P2）

为 P2 提议配置 PFS 功能。使用该命令 no 的形式恢复默认配置。

［命令］

group {nopfs | 1 | 2 | 5 }

no group

［句法描述］

nopfs	不使用 PFS 功能。
1	选择 DH 组 1。密钥的长度为 768 比特。
2	选择 DH 组 2。密钥的长度为 1024 比特。
5	选择 DH 组 5。密钥的长度为 1536 比特。

［默认取值］

nopfs。

［命令模式］

P2 提议配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# ipsec proposal proposal1
hostname(config-ipsec-proposal)# group 2
```

hash （P1）

为 P1 提议指定验证算法。使用该命令 no 的形式恢复默验证算法。

［命令］

hash {md5 | sha | sha256 | sha384 | sha512}

no hash

［句法描述］

md5	指定使用 MD5 验证算法。摘要为 128 比特。
sha	指定使用 SHA-1 验证算法。摘要为 160 比特。
sha256	指定使用 SHA-256 验证算法。摘要为 256 比特。
sha384	指定使用 SHA-384 验证算法。摘要为 384 比特。
sha512	指定使用 SHA-512 验证算法。摘要为 512 比特。

［默认取值］

SHA 验证算法。

［命令模式］

P1 提议配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# isakmp proposal proposal1
hostname(config-isakmp-proposal)# hash md5
```

hash （manual）

为手动配置 IPSec 隧道指定验证算法。使用该命令 no 的形式恢复默认验证算法。

［命令］

hash {md5 | sha | sha256 | sha384 | sha512 | null}

no hash

［句法描述］

md5	指定使用 MD5 验证算法。摘要为 128 比特。
sha	指定使用 SHA-1 验证算法。摘要为 160 比特。
sha256	指定使用 SHA-256 验证算法。摘要为 256 比特。
sha384	指定使用 SHA-384 验证算法。摘要为 384 比特。
sha512	指定使用 SHA-512 验证算法。摘要为 512 比特。
null	不使用验证功能。

［默认取值］

sha。

［命令模式］

手工 IPSec 隧道配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# tunnel t1 ipsec manual
hostname(config-tunnel-ipsec-manual)# hash sha
```

---

hash （P2）

为 P2 提议指定验证算法。使用该命令 no 的形式恢复默认验证算法。

［命令］

hash {md5 | sha | sha256 | sha384 | sha512 | null} [md5 | sha | sha256 | sha384 | sha512 | null] [md5 | sha | sha256 | sha384 | sha512 | null]

no hash

［句法描述］

md5	指定使用 MD5 验证算法。摘要为 128 比特。
sha	指定使用 SHA-1 验证算法。摘要为 160 比特。
sha256	指定使用 SHA-256 验证算法。摘要为 256 比特。
sha384	指定使用 SHA-384 验证算法。摘要为 384 比特。
sha512	指定使用 SHA-512 验证算法。摘要为 512 比特。
null	不使用验证功能。

［默认取值］

sha。

［命令模式］

P2 提议配置模式。

［使用指导］

最多可为一个 P2 提议指定三种不同的验证算法。

［命令实例］

```
hostname(config)# ipsec proposal proposal1
hostname(config-ipsec-proposal)# hash md5 sha
```

hash-key

为手动配置 IPSec 隧道指定协议的验证密钥。使用该命令 no 的形式取消对验证密钥的配置。

［命令］

hash-key inbound *hex-number-string* **outbound** *hex-number-string*

no hash-key

［句法描述］

inbound	配置本端进方向的验证密钥。
outbound	配置本端出方向的验证密钥。

［默认取值］

无默认值。

［命令模式］

手工 IPSec 隧道配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **tunnel t1 ipsec manual**

hostname(config-tunnel-ipsec-manual)# **hash-key inbound 1111 outbound 2222**

id

为 IKE IPSec 指定第二阶段 ID。使用该命令 no 的形式取消对 ID 的配置。

［命令］

id {**auto** | **local** *ip-address/mask* **remote** *ip-address/mask* **service** *name*}

no id

［句法描述］

auto	自动指定第二阶段 ID。
local	指定本端第二阶段的 local ID。
remote	指定本端第二阶段的 remote ID。

service	指定服务名称，包括服务的协议和端口号信息。

［默认取值］

无默认值。

［命令模式］

IKE 隧道配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **tunnel t2 ipsec auto**

hostname(config-tunnel-ipsec-auto)# **id local 1.1.1.0/24 remote 2.2.2.0/24 service any**

interface

绑定指定接口到 IKE 对等体或者为手工 IPSec 隧道指定出接口。使用该命令 no 的形式取消接口的指定。

［命令］

interface *interface-name*

no interface *interface-name*

［句法描述］

interface-name	指定接口的名称。

［默认取值］

无默认值。

［命令模式］

IKE 对等体配置模式或者手工 IPSec 隧道配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **isakmp peer peer1**

hostname(config-isakmp-peer)# **interface ethernet0/1**

ipsec proposal

创建 P2 提议，即 IPSec 安全提议，并且进入 P2 提议配置模式。使用该命令 no 的形式删除指定的 P2 提议。

［命令］

ipsec proposal *p2-name*

no ipsec proposal *p2-name*

［句法描述］

p2-name	指定 P2 提议的名称。

［默认取值］

无默认值。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# ipsec proposal proposal1
hostname(config-ipsec-proposal)#
```

ipsec-proposal

为 IKE 隧道指定 P2 提议。使用该命令 no 的形式取消对 P2 提议的指定。

［命令］

ipsec-proposal *p2-name*

no ipsec-proposal *p2-name*

［句法描述］

p2-name	指定 P2 提议的名称。

［默认取值］

无默认值。

［命令模式］

IKE 隧道配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# tunnel t2 ipsec auto
hostname(config-tunnel-ipsec-auto)# ipsec-proposal proposal1
```

isakmp peer

创建一个 IKE 对等体，并且进入 IKE 对等体配置模式。使用该命令 no 的形式删除指定的 IKE 对等体。

［命令］

isakmp peer *name*

no isakmp peer *name*

［句法描述］

name	指定 IKE 对等体的名称。

［默认取值］

无默认值。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# isakmp peer peer1
hostname(config-isakmp-peer)#
```

isakmp-peer

为 IKE IPSec 指定 IKE 对等体。使用该命令 no 的形式取消 IKE 对等体的指定。

［命令］

isakmp-peer *peer-name*

no isakmp-peer *peer-name*

［句法描述］

peer-name	指定 IKE 对等体的名称。

［默认取值］

无默认值。

［命令模式］

IKE 隧道配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# tunnel t2 ipsec auto
hostname(config-tunnel-ipsec-auto)# isakmp-peer peer1
```

isakmp proposal

创建一个 P1 提议，即 IKE 安全提议，并且进入 P1 提议配置模式。使用该命令 no 的形式删除指定的 P1 提议。

［命令］

isakmp proposal *p1-name*

no isakmp proposal *p1-name*

［句法描述］

p1-name	指定 P1 提议的名称。

［默认取值］

无默认值。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# isakmp proposal proposal1
hostname(config-isakmp-proposal)#
```

isakmp-proposal

为 IKE 对等体或者 IKE 隧道指定 IKE 安全提议。使用该命令 no 的形式取消 IKE 安全提议的指定。

［命令］

isakmp-proposal *name*

no isakmp-proposal

［句法描述］

name	指定 IKE 安全提议的名称。

［默认取值］

主模式。

［命令模式］

IKE 对等体配置模式或者 IKE 隧道配置模式。

［使用指导］

一个 IKE 对等体最多可被指定 4 个 IKE 安全提议。

［命令实例］

```
hostname(config)# isakmp peer peer1
hostname(config-isakmp-peer)# isakmp-proposal proposal1 proposal2
```

lifesize

为 P2 提议指定 SA 的周期流量。使用该命令 no 的形式恢复默认配置。

［命令］

lifesize *kilobytes*

no lifesize

［句法描述］

kilobytes	指定周期流量的值，单位为千字节。

［默认取值］

0，即没有周期流量限制。

［命令模式］

P2 提议配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# ipsec proposal proposal1
hostname(config-ipsec-proposal)# lifesize 2000
```

lifetime （P1）

为 P1 提议指定安全联盟的生命周期。使用该命令 no 的形式恢复默认生命周期长度。

［命令］

lifetime *time-value*

no lifetime

［句法描述］

time-value	指定 SA 第一阶段的生命周期长度，单位为秒。

［默认取值］

86400 秒。

［命令模式］

P1 提议配置模式。

［使用指导］

生命周期的范围是 300 到 86400 秒。

［命令实例］

```
hostname(config)# isakmp proposal proposal1
hostname(config-isakmp-proposal)# lifetime 14400
```

lifetime（P2）

为 P2 提议指定 SA 的生命周期。使用该命令 no 的形式恢复默认配置。

［命令］

lifetime *seconds*

no lifetime

［句法描述］

seconds	指定生命周期的时间长度，单位为秒。

［默认取值］

28800 秒。

［命令模式］

P2 提议配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# ipsec proposal proposal1
hostname(config-ipsec-proposal)# lifetime 28800
```

local-id

为 IKE 对等体指定本端 ID。使用该命令 no 的形式取消对本端 ID 的配置。

［命令］

local-id {**fqdn** *string* | **asn1dn** [*string*] | **u-fqdn** *string*}
no local-id

［句法描述］

fqdn *string*	指定使用 FQDN 类型的 ID。*string* 为 ID 的具体内容。
asn1dn [*string*]	指定使用 Asn1dn 类型的 ID。*string* 为 ID 的具体内容。用户可以不指定 ID 的具体内容，在此种情况下，系统将从证书中获取 ID。
u-fqdn *string*	指定使用 U-FQDN 类型的 ID，即电子邮件地址类型，例如 user1@hillstonenet.com。

［默认取值］

无默认值。

［命令模式］

IKE 对等体配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# isakmp peer peer1
hostname(config-isakmp-peer)# local-id fqdn center
hostname(config-isakmp-peer)# local-id asn1dn
```

```
hostname(config-isakmp-peer)# local-id asn1dn "OU=hostname, C=CN"
```

mode （协商模式）

为 IKE 对等体指定协商模式。使用该命令 no 的形式恢复默认协商模式。

［命令］

mode {main | aggressive}

no mode

［句法描述］

main	指定使用主模式，可提供 ID 保护功能。
aggressive	指定使用野蛮模式。

［默认取值］

主模式。

［命令模式］

IKE 对等体配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# isakmp peer peer1
hostname(config-isakmp-peer)# mode aggressive
```

mode （操作模式）

为手动配置 IPSec 隧道或者 IKE 隧道指定操作模式。使用该命令 no 的形式恢复默认模式。

［命令］

mode {transport | tunnel}

no mode

［句法描述］

transport	指定使用传输模式。
tunnel	指定使用隧道模式。

［默认取值］

tunnel。

［命令模式］

手工 IPSec 隧道配置模式或者 IKE 隧道配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# tunnel t1 ipsec manual
hostname(config-tunnel-ipsec-manual)# mode tunnel
```

---

nat-traversal

为 IKE 对等体开启 NAT 穿越功能。使用该命令 no 的形式关闭 NAT 穿越功能。

［命令］

nat-traversal

no nat-traversal

［句法描述］

无。

［默认取值］

关闭。

［命令模式］

IKE 对等体配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# isakmp peer peer1
hostname(config-isakmp-peer)# nat-traversal
```

---

peer

为 IKE 对等体或者手工 IPSec 隧道指定对端的 IP 地址。使用该命令 no 的形式取消对端 IP 地址的指定。

［命令］

peer *ip-address*

no peer

［句法描述］

ip-address	指定对端的 IP 地址。

［默认取值］

无默认值。

［命令模式］

IKE 对等体配置模式或者手工 IPSec 隧道配置模式。

［使用指导］

该指定的 IP 地址只有当对端的 IP 地址类型是静态的时候才有效。

［命令实例］

```
hostname(config)# isakmp peer peer1
hostname(config-isakmp-peer)# peer 1.1.1.1
```

peer-id

为 IKE 对等体指定对端 ID。使用该命令 no 的形式取消对对端 ID 的配置。

［命令］

peer-id {fqdn | asn1dn | u-fqdn} *string*

no peer-id

［句法描述］

fqdn	指定使用 FQDN 类型的 ID。*string* 为 ID 的具体内容。
asn1dn	指定使用 Asn1dn 类型的 ID。*string* 为 ID 的具体内容。当 ID 为 Asn1dn 类型时，StoneOS 支持星号“*”的模糊匹配，例如，用户可以将 ID 指定为“CN=XX, O=hostname, OU=*”。
u-fqdn	指定使用 U-FQDN 类型的 ID，即电子邮件地址类型，例如 user1@hillstonenet.com。

［默认取值］

无默认值。

［命令模式］

IKE 对等体配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# isakmp peer peer1
hostname(config-isakmp-peer)# peer-id fqdn center
hostname(config-isakmp-peer)# peer-id asn1dn “OU=hostname, C=CN”
```

pre-share

为 IKE 对等体指定预共享密钥认。使用该命令 no 的形式取消对预共享密钥的指定。

［命令］

pre-share *string*

no pre-share

［句法描述］

string	指定预共享密钥的内容。

［默认取值］

无默认值。

［命令模式］

IKE 对等体配置模式。

［使用指导］

适用于预共享密钥认证方式。

［命令实例］

```
hostname(config)# isakmp peer peer1
hostname(config-isakmp-peer)# pre-share abcd
```

protocol

为 P2 提议或者手动配置 IPSec 隧道指定协议类型。使用该命令 no 的形式恢复默认协议配置。

［命令］

protocol {esp | ah}

no protocol

［句法描述］

esp	指定使用 ESP 协议。

ah	指定使用 AH 协议。

［默认取值］

esp。

［命令模式］

P2 提议配置模式或者手工 IPSec 隧道配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# ipsec proposal proposal1
hostname(config-ipsec-proposal)# protocol ah
```

spi

为手动配置 IPSec 隧道指定 SPI。使用该命令 no 的形式取消 SPI 的配置。

［命令］

spi *spi-number out-spi-number*

no spi

［句法描述］

spi-number	指定本端的 SPI 参数。
out-spi-number	指定对端的 SPI 参数。

［默认取值］

无默认值。

［命令模式］

手工 IPSec 隧道配置模式。

［使用指导］

在为系统配置安全联盟时，必须分别设置 inbound 和 outbound 两个方向的安全联盟的参数。并且在安全隧道的两端设置的安全联盟参数必须是完全匹配的。本端的入方向安全联盟的 SPI 必须和对端的出方向安全联盟的 SPI 一样；本端的出方向安全联盟的 SPI 必须和对端的入方向安全联盟的 SPI 一样。

［命令实例］

```
hostname(config)# tunnel t1 ipsec manual
hostname(config-tunnel-ipsec-manual)# spi 6001 6002
```

track-event-notify

禁用或者启用 VPN 监控失败通知功能。

［命令］

track-event-notify {disable | enable}

［句法描述］

disable	禁用。
enable	启用。

［默认取值］

开启。

［命令模式］

IKE IPSec 隧道配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **tunnel ipsec vpn1-tunnel auto**
hostname(config-tunnel-ipsec-auto)# **track-event-notify disable**

trust-domain

为 IKE 对等体指定数字证书的 PKI 信任域。使用该命令 no 的形式取消对预共享密钥的指定。

［命令］

trust-domain *string*
no trust-domain

［句法描述］

string	指定 PKI 信任域。

［默认取值］

无默认值。

［命令模式］

IKE 对等体配置模式。

［使用指导］

适用于数字证书认证方式。

［命令实例］

```
hostname(config)# isakmp peer peer1
hostname(config-isakmp-peer)# trust-domain verisign
```

tunnel ipsec *name* auto

创建 IKE 隧道，并且进入 IKE 隧道配置模式。使用该命令 no 的形式删除指定的 IPSec 隧道。

［命令］

tunnel ipsec *name* **auto**

no tunnel ipsec *name* **auto**

［句法描述］

name	指定 IPSec 隧道的名称。

［默认取值］

无默认值。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# tunnel ipsec t1 auto
hostname(config-tunnel-ipsec-auto)#
```

tunnel ipsec *name* manual

创建手工配置 IPSec 隧道，并且进入手工密钥 VPN 配置模式。使用该命令 no 的形式删除指定的手工密钥 VPN 隧道。

［命令］

tunnel ipsec *name* **manual**

no tunnel ipsec *name* **manual**

［句法描述］

name	指定手工密钥 VPN 隧道的名称。

［默认取值］

无默认值。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# tunnel ipsec t1 manual
hostname(config-tunnel-ipsec-manual)#
```

type

为 IKE 对等体指定对端的 IP 地址类型。使用该命令 no 的形式恢复对端 IP 地址的默认类型。

［命令］

type {dynamic | static}

no type

［句法描述］

dynamic	指定对端的 IP 地址为动态 IP 地址。
static	指定对端的 IP 地址为静态 IP 地址。

［默认取值］

static。

［命令模式］

IKE 对等体配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# isakmp peer peer1
hostname(config-isakmp-peer)# type dynamic
```

vpn-track

配置 VPN 监控功能，用以监测指定的 VPN 隧道是否连通，并且能够实现两条或者多条 VPN 隧道的备份或者分流。使用该命令 no 的形式取消 VPN 监控功能的配置。

［命令］

vpn-track [*A.B.C.D*] [**src-ip** *A.B.C.D*] [**interval** *time-value*] [**threshold** *value*]

no vpn-track

［句法描述］

A.B.C.D	指定监测目标的 IP 地址。当对端设备为 Hillstone 安全网关时，如果不指定该参数，系统默认为对端 IP 地址。此 IP 地址不能为“0.0.0.0”和“255.255.255.255”。
src-ip *A.B.C.D*	指定发送 Ping 监测报文的源 IP 地址。当对端设备为 Hillstone 安全网关时，如果不指定该参数，系统默认为出接口 IP 地址。此 IP 地址不能为“0.0.0.0”和“255.255.255.255”。
interval *time-value*	指定发送 Ping 监测报文的时间间隔，单位为秒。范围是 1 到 255 秒。默认值是 10 秒。
threshold *value*	指定判断监测失败的警戒值。如果系统连续未收到该参数指定个数的响应报文，就判断为监测失败，即目标隧道中断。取值范围是 1 到 255。默认值是 10。

［默认取值］

无。

［命令模式］

IKE IPSec 隧道配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **tunnel ipsec vpn1-tunnel auto**

hostname(config-tunnel-ipsec-auto)# **vpn-track 172.16.10.1 src-ip 192.168.100.1 interval 3 threshold 9**

Secure Connect VPN命令

aaa-server

指定 AAA 服务器用于客户端用户身份认证。使用该命令 no 的形式取消对 AAA 服务器的指定。

［命令］

aaa-server *aaa-server-name* [**domain** *domain-name*]

no aaa-server *aaa-server-name* [**domain** *domain-name*]

［句法描述］

aaa-server-name	指定 AAA 服务器的名称。
domain-name	为 AAA 服务器指定域名以区分不同的 AAA 服务器。

［默认取值］

系统默认服务器：local。

［命令模式］

SCVPN 实例配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# tunnel scvpn scvpntunnel1
hostname(config-tunnel-scvpn)# aaa-server server1
```

anti-replay

配置防重放功能。使用该命令 no 的形式关闭防重放功能。

［命令］

anti-replay {**32** | **64** | **128** | **256** | **512**}

no anti-replay

［句法描述］

32	指定防重放的窗口为 32。

64	指定防重放的窗口为 64。
128	指定防重放的窗口为 128。
256	指定防重放的窗口为 256。
512	指定防重放的窗口为 512。

［默认取值］

32。

［命令模式］

SCVPN 实例配置模式。

［使用指导］

在网络状况较差时，例如存在严重乱序现象等，请选择较大的窗口。

［命令实例］

```
hostname(config)# tunnel scvpn scvpntunnel1
hostname(config-tunnel-scvpn)# anti-replay 64
```

address

为地址池配置地址范围和网络掩码。使用该命令 no 的形式删除配置的 IP 地址范围。

［命令］

address *start-ip end-ip* **netmask** *A.B.C.D*

no address

［句法描述］

start-ip	指定 IP 范围的起始 IP 地址。
end-ip	指定 IP 范围的结束 IP 地址。
A.B.C.D	指定网络掩码。

［默认取值］

无。

［命令模式］

SCVPN 地址池配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# scvpn pool pool1
```

```
hostname(config-pool-scvpn)# address 192.168.1.0 192.168.1.254
netmask 255.255.255.0
```

allow-multi-logon

配置用户同名登录功能。开启该功能后，系统允许同一个用户在多个地点同时登录使用 SCVPN。使用该命令 no 的形式关闭用户同名登录功能。

［命令］

allow-multi-logon

no allow-multi-logon

［句法描述］

无。

［默认取值］

开启。

［命令模式］

SCVPN 地址池配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# scvpn pool pool1
hostname(config-pool-scvpn)# no allow-multi-logon
```

allow-multi-logon number

开启用户同名登录功能后，使用该命令指定用户同名登录次数。使用该命令 no 的形式恢复系统的默认设置。

［命令］

allow-multi-logon number *number*

［句法描述］

number	指定用户同名登录次数。范围是 1 到 99999999。

［默认取值］

无。

［命令模式］

SCVPN 实例配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# tunnel scvpn scvpntunnel1
hostname(config-tunnel-scvpn)# allow-multi-logon number 2
```

allow-pwd-change

本地用户成功通过 SCVPN 认证后，使用该命令开启本地用户修改登录密码功能（默认修改密码功能关闭）。使用该命令 no 的形式关闭密码修改功能。

［命令］

```
allow-pwd-change
no allow-pwd-change
```

［句法描述］

无。

［默认取值］

关闭。

［命令模式］

SCVPN 实例配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# tunnel scvpn scvpntunnel1
hostname(config-tunnel-scvpn)# allow-pwd-change
```

client-auth-trust-domain

配置 USB Key 证书相应的 CA 证书的信任域。客户端所提交的证书匹配到其中任意一个信任域的 CA 证书，都会认证成功。使用该命令 no 的形式取消信任域的配置。

［命令］

client-auth-trust-domain *trust-domain*

no client-auth-trust-domain *trust-domain*

［句法描述］

trust-domain	指定用户证书相应 CA 证书的信任域。

［默认取值］

无。

［命令模式］

SCVPN 实例配置模式。

［使用指导］

- 指定的信任域需已经创建。
- 如果需要配置多个信任域，需重复使用本命令。
- 系统最多可以支持 10 个信任域。

［命令实例］

```
hostname(config)# tunnel scvpn scvpntunnel1
hostname(config-tunnel-scvpn)# client-auth-trust-domain stone
```

client-cert-authentication

开启 USB Key 证书认证功能。使用该命令 no 的形式关闭 USB Key 证书认证功能。

［命令］

client-cert-authentication [**usbkey-only**]

no client-cert-authentication [**usbkey-only**]

［句法描述］

usbkey-only	指定 USB Key 证书认证方式为“只用 USB Key”。如不指定该参数，认证方式为“用户名/密码 + USB Key”。

［默认取值］

关闭。

［命令模式］

SCVPN 实例配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# tunnel scvpn scvpntunnel1
hostname(config-tunnel-scvpn)# client-cert-authentication
```

df-bit

配置分片功能。使用该命令 no 的形式恢复系统的默认设置。

［命令］

df-bit {copy | clear | set}

no df-bit

［句法描述］

copy	直接从发包端拷贝 IP 包的 DF 选项。
clear	允许转发设备对包做分片处理。
set	不允许转发设备对包做分片处理。

［默认取值］

copy。

［命令模式］

SCVPN 实例配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# tunnel scvpn scvpntunnel1
hostname(config-tunnel-scvpn)# df-bit clear
```

dns

配置 DNS 服务器。使用该命令 no 的形式取消对 DNS 服务器的指定。

［命令］

dns *address1* [*address2*] [*address3*] [*address4*]

no dns

［句法描述］

address1	指定 DNS 服务器 IP 地址。

［默认取值］

无。

［命令模式］

SCVPN 地址池配置模式。

［使用指导］

用户最多可配置 4 个 DNS 服务器。

［命令实例］

```
hostname(config)# scvpn pool pool1
hostname(config-pool-scvpn)# dns 1.1.1.1
```

exclude address

配置保留地址池。保留地址池中的 IP 地址为地址池中的部分 IP 地址，不向客户端分配。使用该命令 no 的形式取消保留地址池的配置。

［命令］

exclude address *start-ip end-ip*

no exclude address

［句法描述］

start-ip	指定保留地址池的起始 IP 地址。
end-ip	指定保留地址池的结束 IP 地址。

［默认取值］

无。

［命令模式］

SCVPN 地址池配置模式。

［使用指导］

保留地址池中的 IP 地址为地址池中的部分 IP 地址。

［命令实例］

```
hostname(config)# scvpn pool pool1
hostname(config-pool-scvpn)# address 1.1.1.0 1.1.1.100 netmask
255.255.255.0
hostname(config-pool-scvpn)# exclude address 1.1.1.0 1.1.1.100
```

exec scvpn approve-binding

批准候选表项。

［命令］

exec scvpn *instance-name* **approve-binding user** *user-name* **host** *host-id*

［句法描述］

instance-name	指定 SCVPN 实例的名称。
user-name	指定候选表项对应的用户名称。
host-id	指定候选表项对应的主机 ID。

［默认取值］

无。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **exec scvpn scvpntunnel1 approve-binding user user host 6f1baedb111639784362bf74d34707eb**

exec scvpn clear-binding

清除绑定表或者指定的绑定表项。

［命令］

exec scvpn *instance-name* **clear-binding** [{**user** *user-name* [**host** *host-id*] | **host** *host-id* }]

［句法描述］

instance-name	指定 SCVPN 实例的名称。
user-name	指定用户名称。如果不指定 Host ID，则删除指定用户的所有绑定表项。
host-id	指定主机 ID。

［默认取值］

无。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **exec scvpn scvpntunnel1 clear-binding user user1**

---

exec scvpn increase-host-binding

增加预绑定主机数。

［命令］

exec scvpn *instance-name* **increase-host-binding user** *user-name number*

使用以下命令减少预绑定主机数：

exec scvpn *instance-name* **decrease-host-binding user** *user-name number*

［句法描述］

instance-name	指定 SCVPN 实例的名称。
user-name	指定用户名称。
number	指定增加或减少的预绑定主机数目。

［默认取值］

无。

［命令模式］

任何模式。

［使用指导］

当允许一个用户通过多台主机登录且设置了用户首次登录自动批准用户名和主机 ID 的绑定关系时，默认情况下，仅自动批准用户和首次登录主机 ID 的绑定关系表项（即：仅批准一个主机 ID，以后登录的主机 ID 进入候选表）。

［命令实例］

hostname# **exec scvpn scvpntunnel1 increase-host-binding user user1 3**

---

exec scvpn kickout

强制断开客户端 SCVPN 连接。

［命令］

exec scvpn *instance-name* **kickout** *user-name*

［句法描述］

instance-name	指定 SCVPN 实例的名称。
user-name	指定被强制断开连接的用户名称。

［默认取值］

无。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **exec scvpn scvpntunnel1 kickout user**

exec scvpn no-host-binding-check

配置超级用户。SCVPN 实例不对超级用户进行登录主机验证，即超级用户可以在任意主机登录。

［命令］

exec scvpn *instance-name* **no-host-binding-check user** *user-name*

使用以下命令取消超级用户的配置：

exec scvpn *instance-name* **host-binding-check user** *user-name*

［句法描述］

instance-name	指定 SCVPN 实例的名称。
user-name	指定超级用户的的名称。

［默认取值］

无。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **exec scvpn scvpntunnel1 no-host-binding-check user user1**

exec scvpn no-user-binding-check

配置共享主机。SCVPN 实例不对通过共享主机登录的用户进行认证。

［命令］

exec scvpn *instance-name* **no-user-binding-check host** *host-id*

使用以下命令取消共享主机的配置：

exec scvpn *instance-name* **user-binding-check host** *host-id*

［句法描述］

instance-name	指定 SCVPN 实例的名称。
host-id	指定共享主机的主机 ID。

［默认取值］

无。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **exec scvpn scvpntunnel1 no-user-binding-check host b45149ac3b8ce55f1a33ea7f02d167b4**

exec send test-message to

向指定手机号码发送测试短信。

［命令］

exec sms send test-message to *phone-number*

［句法描述］

phone-number	指定接收测试短信的手机号码。

［默认取值］

无。

［命令模式］

任意模式。

［使用指导］

如果测试短信发送成功，指定手机号码会收到系统发送的测试短信；如果测试短信发送失败，系统会记录日志并描述失败原因。

［命令实例］

hostname# **exec sms send test-message to phone-number 13*********

---

export aaa user-password

导出密码文件。

［命令］

export aaa user-password to {tftp server *ip-address* **| ftp server** *ip-address* [**user** *user-name* **password** *password*]} [*file-name*]

［句法描述］

ip-address	指定 FTP 或者 TFTP 服务器的 IP 地址。
user *user-name* **password** *password*	指定 FTP 服务器的用户名和密码。
file-name	指定导出的密码文件名称。

［默认取值］

无。

［命令模式］

执行模式。

［使用指导］

无。

［命令实例］

hostname# **export aaa user-password to tftp server 1.1.1.1 password123**

---

export scvpn user-host-binding

用户可以通过 FTP、TFTP 或 USB 方式导出绑定表。

［命令］

export scvpn user-host-binding to {ftp server *ip-address* **[user** *user-name* **password** *password*] **| tftp server** *ip-address* **| usb0 | usb1}** [*file-name*]

［句法描述］

ftp server *ip-address* [**user** *user-name* **password** *password*]	指定通过 FTP 方式导出绑定表。**user** *user-name* **password** *password* 指定 FTP 服务器的 IP 地址以及访问服务器使用的用户名和密码，当不指定用户名和密码时表示采用匿名登录方式。
tftp server *ip-address*	指定通过 TFTP 方式导出绑定表。*ip-address* 指定 TFTP 服务器的 IP 地址。
usb0 | usb1	指定将绑定表导出到 U 盘根目录。
file-name	指定导出的绑定表的文件名称。默认名称为 scvpn_bind_file。

［默认取值］

无。

［命令模式］

执行模式。

［使用指导］

无。

［命令实例］

hostname# **export scvpn user-host-binding to usb1**

host-check

配置主机安全检测策略规则。主机安全检测 Profile 配置完成后，只有把它引用到主机安全检测策略规则中，配置的安全检测功能才能对用户生效。使用该命令 no 的形式取消主机安全检测策略规则的配置。

［命令］

host-check [**role** *role-name*] **profile** *profile-name* [**guest-role** *guestrole-name*] [**periodic-check** *period-time*]

no host-check [**role** *role-name*] **profile** *profile-name* [**guest-role** *guestrole-name*] [**periodic-check** *period-time*]

［句法描述］

role *role-name*	指定用户的初级角色，该初级角色为 AAA 服务器中已配置的用户角色。如果配置该参数，该主机安全检测 Profile 对该指定角色有效；如果不配置此参数，该主机安全检测 Profile 对所有用户均有效。
profile *profile-name*	指定绑定的主机安全检测 Profile 名称。
guest-role *guestrole-name*	指定用户的次级角色。当客户端的主机安全检测失败时，如果配置该参数，用户将获得该次级角色拥有的访问权限；如果不配置该参数，系统将断开该客户端连接。
periodic-check *period-time*	指定该用户的自动检测周期。单位为分钟，取值范围为 5 到 1440 分钟，默认值为 30 分钟。

［默认取值］

无。

［命令模式］

SCVPN 实例配置模式。

［使用指导］

可以配置多条该命令添加多个安全检测策略规则。当一个用户可匹配多个安全检测策略规则时，设备端会按照查找到的第一条相匹配的规则进行处理。

一个用户可以绑定到一个或者多个角色，当一个用户绑定到多个角色且多个角色均配置安全检测策略规则时，设备端会按照查找到的第一条相匹配的规则进行处理。

［命令实例］

hostname(config)# **tunnel scvpn scvpntunnel1**

hostname(config-tunnel-scvpn)# **host-check role sw profile sw-security-check guest-role dl periodic-check 60**

https-port

指定 HTTPS 端口号。HTTPS 端口号用于客户端访问设备端时使用。使用该命令 no 的形式恢复默认 HTTPS 端口号。

［命令］

https-port *port-number*

no https-port

［句法描述］

port-number	指定 HTTPS 端口号。取值范围是 1 到 65535。

［默认取值］

4433。

［命令模式］

SCVPN 实例配置模式。

［使用指导］

为避免与 WebUI 使用的 HTTPS 端口号相冲突，建议用户不要把 HTTPS 端口号设置为 443。绑定到同一个接口的 SCVPN 实例需配置不同的 HTTPS 端口号。

［命令实例］

```
hostname(config)# tunnel scvpn scvpntunnel1
hostname(config-tunnel-scvpn)# https-port 44433
```

idle-time

配置空闲时间。空闲时间指客户端与设备端在无流量状态下能够保持连接状态的最长时间，超出空闲时间后，设备端将断开与客户端的连接。使用该命令 no 的形式恢复空闲时间的默认值。

［命令］

idle-time *time-value*

no idle-time

［句法描述］

time-value	指定空闲时间，单位为分钟。取值范围是 15 到 120 分钟。

［默认取值］

30 分钟。

［命令模式］

SCVPN 实例配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# tunnel scvpn scvpntunnel1
hostname(config-tunnel-scvpn)# idle-time 20
```

import pki cacert

用户可以通过多种方式（FTP、TFTP 和 USB）实现 CA 证书到信任域的导入。

［命令］

import pki *trust-domain-name* **cacert from** {**ftp server** *ip-address* [**user** *user-name* **password** *password*] | **tftp server** *ip-address* | **usb0** | **usb1**} *file-name*

［句法描述］

trust-domain-name	指定 PKI 信任域的名称。
ftp server *ip-address* [**user** *user-name* **password** *password*]	指定 FTP 服务器的 IP 地址以及访问服务器使用的用户名和密码。当不输入用户名和密码时表示采用匿名登录方式。
tftp server *ip-address*	指定 TFTP 服务器的 IP 地址。
usb0 | **usb1**	指定通过 USB 方式从 USB0 或者 USB1 插槽所对应的 U 盘根目录导入 CA 证书。
file-name	指定要导入的 CA 证书的文件名。

［默认取值］

无。

［命令模式］

执行模式。

［使用指导］

无。

［命令实例］

hostname# **import pki stone cacert from tftp server 10.101.10.1 certnew.cer**

import aaa user-password

导入密码文件。

［命令］

import aaa user-password from {**tftp server** *ip-address* | **ftp server** *ip-address* [**user** *user-name* **password** *password*]} *file-name*

［句法描述］

ip-address	指定 FTP 或者 TFTP 服务器的 IP 地址。
user *user-name* **password**	指定 FTP 服务器的用户名和密码。

password	
file-name	指定导入的密码文件名称。

［默认取值］

无。

［命令模式］

执行模式。

［使用指导］

无。

［命令实例］

hostname# **import aaa user-password from ftp server 10.10.1.1 password123**

import scvpn user-host-binding

用户可以通过 FTP、TFTP 或 USB 方式导入绑定表。

［命令］

import scvpn user-host-binding from {ftp server *ip-address* **[user** *user-name* **password** *password*] **| tftp server** *ip-address* **| usb0 | usb1}** *file-name*

［句法描述］

ftp server *ip-address* **[user** *user-name* **password** *password*]	指定通过 FTP 方式导入绑定表。**user** *user-name* **password** *password* 指定 FTP 服务器的 IP 地址以及访问服务器使用的用户名和密码，不指定用户名和密码时表示采用匿名登录方式。
tftp server *ip-address*	指定通过 TFTP 方式导入绑定表。*ip-address* 指定 TFTP 服务器的 IP 地址。
usb0 | usb1	指定从 U 盘根目录导入绑定表。
file-name	指定要导入的文件名。

［默认取值］

无。

［命令模式］

执行模式。

［使用指导］

无。

［命令实例］

```
hostname# import scvpn user-host-binding from usb1 scvpn_bind_file
```

interface

指定设备端 SCVPN 接口。使用该命令 no 的形式取消设备端接口的配置。

［命令］

interface *interface-name*

no interface

［句法描述］

interface-name	指定设备端接口的名称。

［默认取值］

无。

［命令模式］

SCVPN 实例配置模式。

［使用指导］

多次执行该命令启用多个 SCVPN 接口，系统允许最多开启两个接口。

［命令实例］

```
hostname(config)# tunnel scvpn scvpntunnel1
hostname(config-tunnel-scvpn)# interface ethernet0/1
```

ip-binding role

配置 IP 角色绑定规则。IP 角色绑定规则是将角色与已配置地址池中的某一 IP 地址范围绑定，当此客户端连接成功后，设备端会从绑定的地址范围中取出一个 IP 地址分配给客户端。

［命令］

ip-binding role *role-name* **ip-range** *start-ip end-ip*

no ip-binding role *role-name*

［句法描述］

role *role-name*	指定角色名称。
ip-range *start-ip end-ip*	指定绑定的 IP 范围的起始 IP 地址 start-ip 和结束 IP 地址 end-ip。此地址范围必须为地址池中可以分配的地址范围。

［默认取值］

无。

［命令模式］

SCVPN 地址池配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# scvpn pool pool1
hostname(config-pool-scvpn)# address 1.1.1.0 1.1.1.100 netmask
255.255.255.0
hostname(config-pool-scvpn)# ip-binding role role1 ip-range
 1.1.1.20 1.1.1.30
```

ip-binding user

配置 IP 用户绑定规则。IP 用户绑定规则将客户端用户与已配置地址池中的某个固定 IP 地址绑定，当客户端连接成功后，设备端会将绑定的 IP 地址分配给客户端。使用该命令 no 的形式取消对特定用户 IP 用户绑定规则的配置。

［命令］

ip-binding user *user-name* **ip** *ip-address*

no ip-binding user *user-name*

［句法描述］

user *user-name*	指定客户端用户名。
ip *ip-address*	指定绑定的 IP 地址。此地址必须为地址池中可以分配的地址。

［默认取值］

无。

［命令模式］

SCVPN 地址池配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# scvpn pool pool1
```

hostname(config-pool-scvpn)# **address 1.1.1.0 1.1.1.100 netmask 255.255.255.0**

hostname(config-pool-scvpn)# **ip-binding user user1 ip 1.1.1.10**

link-select

配置最优路径检测功能。使用该命令 no 的形式取消最优路径检测功能的配置。

［命令］

link-select [**server-detect**] [*A.B.C.D* [**https-port** *port-number*]] [*A.B.C.D* [**https-port** *port-number*]] [*A.B.C.D* [**https-port** *port-number*]] [*A.B.C.D* [**https-port** *port-number*]]

no link-select

［句法描述］

server-detect	开启设备端最优路径检测功能，默认情况下由客户端检测最优路径。
A.B.C.D	指定 DNAT 设备外网接口 IP。系统允许最多配置四个 IP 地址。
https-port *port-number*	指定 DNAT 设备外网接口 HTTPS 端口号。默认值是 4433。取值范围是 1 到 65535。为避免与 WebUI 使用的 HTTPS 端口号相冲突，建议用户不要把 HTTPS 端口号设置为 443。

［默认取值］

无。

［命令模式］

SCVPN 实例配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **tunnel scvpn scvpntunnel1**

hostname(config-tunnel-scvpn)# **link-select server-detect 202.2.3.1 https-port 2234 196.1.2.3 https-port 3367**

move

移动已有的 IP 角色绑定规则从而改变规则的排列顺序。

［命令］

move *role-name1* {**before** *role-name2* | **after** *role-name2* | **top** | **bottom**}

［句法描述］

role-name1	指定被移动的 IP 角色绑定规则的角色名称。
before *role-name2*	将 IP 角色绑定规则移动到某个 IP 角色绑定规则(角色名称为 role-name2 的规则)之前。
after *role-name2*	将 IP 角色绑定规则移动到某个 IP 角色绑定规则(角色名称为 role-name2 的规则)之后。
top	将 IP 角色绑定规则移动到所有 IP 角色绑定规则之首。
bottom	将 IP 角色绑定规则移动到所有 IP 角色绑定规则的末尾。

［默认取值］

默认情况下，系统会将新创建的规则放到所有规则的末尾。

［命令模式］

SCVPN 地址池配置模式。

［使用指导］

一个用户可以绑定到一个或者多个角色，不同角色可以配置不同的 IP 角色绑定规则。对于绑定到多个角色且多个角色有相应的 IP 角色绑定规则的用户，安全网关会对 IP 角色绑定规则进行顺序查找，然后按照查找到的相匹配的第一条规则为用户分配地址。

［命令实例］

```
hostname(config)# scvpn pool pool1
hostname(config-pool-scvpn)# move role1 before role2
```

phone

为本地用户设置短信认证手机号码。开启短信口令认证功能后，系统会向已指定的登录用户手机号码发送认证码短信。使用该命令 no 的形式取消用户手机号码的指定。

［命令］

phone *phone-number*

no phone

［句法描述］

phone-number	指定本地用户手机号码。

［默认取值］

无。

［命令模式］

用户配置模式。

［使用指导］

为 AD 用户设置手机号码，需要在 AD 服务器的“mobile”属性中配置手机号码。

［命令实例］

```
hostname(config)# aaa-server local1 type local
hostname(config)# user user1
hostname(config)# phone 13*********
```

pool

为 SCVPN 实例指定 SCVPN 地址池。

［命令］

pool *pool-name*

no pool

［句法描述］

pool-name	指定已配置的 SCVPN 地址池名称。

［默认取值］

无。

［命令模式］

SCVPN 实例配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# tunnel scvpn scvpntunnel1
hostname(config-tunnel-scvpn)# pool pool1
```

redirect-url

配置 URL 重定向功能。使用该命令 no 的形式取消 URL 重定向功能。

［命令］

redirect-url *url* **title-en** *name* **title-zh** *name*

no redirect-url *url* **title-en** *name* **title-zh** *name*

［句法描述］

url	指定 SCVPN 认证成功后，客户端自动跳转页面的 URL，取值范围为 1 到 255 字节。系统支持 HTTP 和 HTTPS 两种类型的 URL，输入 http://或者 https://分别指定相应类型的 URL。
title-en *name*	指定重定向 URL 的英文描述，范围为 1 到 31 字节。当客户端 PC 为英文操作系统时，该名称会在客户端菜单项中显示。
title-zh *name*	指定重定向 URL 的中文描述，范围为 1 到 63 字节。当客户端 PC 为中文操作系统时，该名称会在客户端菜单项中显示。建议选用支持中文输入的超级终端，当超级终端不支持中文输入时，请通过 WebUI 配置该参数。

［默认取值］

关闭。

［命令模式］

SCVPN 实例配置模式。

［使用指导］

根据重定向页面类型的不同，StoneOS 支持内容符合下列格式的 URL 输入，以 HTTP 类型 URL 为例：

- 要求用户名为 UTF-8 编码格式的页面：输入“URL”+“username=$USER&password=$PWD”。比如，http://www.abc.com/oa/login.do?username=$USER&password=$PWD
- 要求用户名为 GB2312 编码格式的页面：输入“URL”+“username=$GBUSER&password=$PWD”。比如，http://www.abc.com/oa/login.do?username=$GBUSER&password=$PWD
- 其它页面：直接输入 URL。比如，http://www.abc.com

［命令实例］

```
hostname(config)# tunnel scvpn ssl1
hostname(config-tunnel-scvpn)# redirect-url http://192.10.5.201/oa/login.do?username=$USER&password=$PWD title-en OA title-zh 中文 OA 系统
```

scvpn host-check-profile

指定主机安全检测 Profile。使用该命令 no 的形式删除指定的主机安全检测 Profile。

［命令］

scvpn host-check-profile *hostcheck-profile-name*

no scvpn host-check-profile *hostcheck-profile-name*

［句法描述］

hostcheck-profile-name	指定主机安全检测 Profile 的名称。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

该命令仅指定主机安全检测 Profile 名称，Profile 的内容需要通过 WebUI 进行配置。

［命令实例］

hostname(config)# **scvpn host-check-profile sw**

hostname(config-profile_scvpn)#

scvpn pool

创建 SCVPN 地址池。执行该命令后，系统创建指定名称的地址池，并且进入 SCVPN 地址池配置模式；如果指定的名称已存在，则直接进入 SCVPN 地址池配置模式。使用该命令 no 的形式删除指定的 SCVPN 地址池。

［命令］

scvpn pool *pool-name*

no scvpn pool *pool-name*

［句法描述］

pool-name	指定地址池的名称。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **scvpn pool pool1**

```
hostname(config-pool-scvpn)#
```

scvpn-udp-port

配置 SCVPN 连接采用的 UDP 端口号。使用该命令 no 的形式恢复默认 UDP 端口号。

［命令］

scvpn-udp-port *port-number*

no scvpn-udp-port

［句法描述］

port-number	指定 UDP 端口号。取值范围是 1 到 65535。

［默认取值］

4433。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **scvpn-udp-port 4411**

sms-auth enable

开启/关闭短信口令认证功能。

［命令］

开启：**sms-auth enable**

关闭：**sms-auth disable**

［句法描述］

无。

［默认取值］

关闭。

［命令模式］

SCVPN 实例配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# tunnel scvpn scvpntunnel1
hostname(config-tunnel-scvpn)# sms-auth enable
```

sms-auth expiration

配置短信认证码有效时间。每条短信认证码都有一个有效时间，如果用户在有效时间内没有输入短信认证码也没有重新申请认证码，SCVPN 设备端将自动断开连接。使用该命令 no 的形式取消短信认证码有效时间的指定。

［命令］

sms-auth expiration *expiration*

no sms-auth expiration

［句法描述］

expiration	指定短信认证码有效时间。范围为 1-10 分钟。

［默认取值］

10 分钟。

［命令模式］

SCVPN 实例配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# tunnel scvpn scvpntunnel1
hostname(config-tunnel-scvpn)# sms-auth expiration 8
```

sms modem

配置短信猫每小时或者每天最多发送的短信数量。对超出数量限制的短信，系统将自动丢弃并记录日志信息。使用该命令 no 的形式取消短信最大发送数量的指定。

［命令］

sms modem {num-per-hour | num-per-day} *number*

no sms modem {num-per-hour | num-per-day}

［句法描述］

{num-per-hour | num-per-day} *number*	指定短信猫每小时（**num-per-hour**）或者每天（**num-per-day**）最多发送的短信数量。范围为 1-1000 条。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **sms modem num-per-hour 100**

split-tunnel-route

配置 SCVPN 隧道路由。SCVPN 隧道路由是指通过 SCVPN 隧道到指定网段的路由。SCVPN 客户端通过设备下发的路由可以访问到指定的网段。使用该命令 no 的形式删除指定的路由。

［命令］

split-tunnel-route *ip-address/netmask* [**metric** *metric-number*]

no split-tunnel-route *ip-address/netmask* [**metric** *metric-number*]

［句法描述］

ip-address/netmask	指定目的地址和掩码。
metric-number	指定路由的度量值。取值范围是 1 到 9999。

［默认取值］

metric - 1。

［命令模式］

SCVPN 实例配置模式。

［使用指导］

用户可以配置多条该命令添加多条路由。

［命令实例］

hostname(config)# **tunnel scvpn scvpntunnel1**

```
hostname(config-tunnel-scvpn)# split-tunnel-route 192.168.3.0/24
```

ssl-protocol

为 SCVPN 指定 SSL 协议。使用该命令 no 的形式恢复 SSL 协议的默认值。

［命令］

ssl-protocol {sslv3 | tlsv1 | any}

no ssl-protocol

［句法描述］

sslv3	指定使用 SSLv3 协议。
tlsv1	指定使用 TLSv1 协议。
any	指定使用 SSLv2、SSLv3 或者 TLSv1 任何一种协议。

［默认取值］

sslv3。

［命令模式］

SCVPN 实例配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# tunnel scvpn scvpntunnel1
hostname(config-tunnel-scvpn)# ssl-protocol any
```

trust-domain

为 SCVPN 指定 PKI 信任域用于 HTTPS 访问认证。使用该命令 no 的形式恢复信任域的默认配置。

［命令］

trust-domain *trust-domain-name*

no trust-domain

［句法描述］

trust-domain-name	指定系统中已配置的 PKI 信任域的名称。

［默认取值］

系统默认 PKI 信任域：trust_domain_default。

［命令模式］

SCVPN 实例配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# tunnel scvpn scvpntunnel1
hostname(config-tunnel-scvpn)# trust-domain td1
```

tunnel-cipher encryption

为 SCVPN 指定隧道密码（包括加密算法、验证算法和压缩算法）。使用该命令 no 的形式恢复加密算法和验证算法的默认值，并取消压缩算法的配置。

［命令］

tunnel-cipher encryption {null | des | 3des | aes | aes192 | aes256} hash {null | md5 | sha | sha256 | sha384 | sha512} [compression defl]

no tunnel-cipher

［句法描述］

null | des | 3des | aes | aes192 | aes256	指定加密算法。**null** 表示不使用加密功能。
null | md5 | sha | sha256 | sha384 | sha512	指定验证算法。**null** 表示不使用验证功能。
compression defl	指定 DEFLATE 压缩算法。

［默认取值］

加密算法：**3des**。

验证算法：**sha**。

压缩算法：无。

［命令模式］

SCVPN 实例配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# tunnel scvpn scvpntunnel1
hostname(config-tunnel-scvpn)# tunnel-cipher encryption aes hash
md5 compression defl
```

tunnel scvpn

创建 SCVPN 实例。执行该命令后，系统创建指定名称的 SCVPN 实例，并且进入 SCVPN 实例配置模式；如果指定的名称已存在，则直接进入 SCVPN 实例配置模式。使用该命令 no 的形式删除指定的 SCVPN 实例。

［命令］

tunnel scvpn *instance-name*

no tunnel scvpn *instance-name*

［句法描述］

instance-name	指定 SCVPN 实例的名称。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# tunnel scvpn scvpntunnel1
hostname(config-tunnel-scvpn)#
```

tunnel scvpn

绑定 SCVPN 实例到隧道接口使其生效。使用该命令 no 的形式取消隧道接口与 SCVPN 实例的绑定。

［命令］

tunnel scvpn *instance-name*

no tunnel scvpn *instance-name*

［句法描述］

instance-name	指定 SCVPN 实例的名称。

［默认取值］

无。

［命令模式］

隧道接口配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# interface tunnel1
hostname(config-if-tun1)# tunnel scvpn scvpntunnel1
```

user-host-verify

开启主机验证功能。使用该命令 no 的形式关闭主机验证功能。

［命令］

user-host-verify [allow-multi-host] [allow-shared-host] [auto-approved-first-bind]

no user-host-verify

［句法描述］

user-host-verify	开启主机验证功能。默认情况下，仅允许一个用户通过一台主机登录，即用户名和主机一一对应。
allow-multi-host	允许一个用户通过多台主机登录。
allow-shared-host	允许多个用户通过一台主机登录。
auto-approved-first-bind	用户首次登录时自动把用户名和主机 ID 的对应关系加入绑定表。

［默认取值］

关闭。

［命令模式］

SCVPN 实例配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# tunnel scvpn scvpntunnel1
```

```
hostname(config-tunnel-scvpn)# user-host-verify auto-approved-
first-bind
```

wins

配置 WINS 服务器。使用该命令 no 的形式取消对 WINS 服务器的指定。

［命令］

wins *address1* [*address2*]

no wins

［句法描述］

address1	指定 WINS 服务器 IP 地址。

［默认取值］

无。

［命令模式］

SCVPN 地址池配置模式。

［使用指导］

用户最多可配置两个 WINS 服务器。

［命令实例］

```
hostname(config)# scvpn pool pool1
hostname(config-pool-scvpn)# wins 1.1.1.10
```

拨号VPN命令

关于P1 提议配置、ISAKMP网关配置、P2 提议配置以及隧道配置命令，请参考 IPSec协议命令一章。

exec generate-user-key rootkey

根据拨号端用户的用户名以及 IKE ID，中心设备使用该命令生成相应的预共享密钥。

［命令］

exec generate-user-key rootkey *pre-share-key* **userid** *string*

［句法描述］

pre-share-key	指定设备端的预共享密钥。
string	指定用户名称相对应的 IKE ID。

［默认取值］

无。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname(config)# **exec generate-user-key rootkey 123456 userid hillstone**

userkey: Wvan/cArRaWi+mLK+guk6AMx+qk=

generate-route

开启设备的自动生成路由功能。该功能允许设备自动添加从中心设备到分支机构的路由条目，从而避免了手工配置路由所带来的问题。使用该命令 no 的形式关闭自动生成路由功能。

［命令］

generate-route

no generate-route

［句法描述］

无。

［默认取值］

关闭。

［命令模式］

ISAKMP 配置模式。

［使用指导］

- 对于拨号 VPN，当拨号端的第二阶段 local ID 指定为 0.0.0.0/0 时，强烈建议用户不要开启自动生成路由功能。
- 当分支机构访问中心设备时，用户可以使用 **no reverse-route** 命令取消隧道接口的逆向路由功能，使所有反向数据原路返回。

［命令实例］

```
hostname(config)# isakmp peer peeer1
hostname(config-isakmp-peer)# generate-route
```

ike_id

指定用户的 IKE ID。使用该命令 no 的形式取消 IKE ID 的配置。

［命令］

ike_id {**fqdn** *string* | **asn1dn** *string*}

no ike_id

［句法描述］

fqdn *string*	指定使用 FQDN 类型的 IKE ID
asn1dn *string*	指定指定使用 Asn1dn 类型的 ID，该类型只可应用于使用证书的情况。

［默认取值］

无。

［命令模式］

用户配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# user user1 aaa-server local
hostname(config-username)# ike_id fqdn hillstone
```

user

在中心设备创建拨号端用户帐号。使用该命令 no 的形式删除指定的用户帐号。

［命令］

user *user-name* **aaa-server local**

no user *user-name*

［句法描述］

user-name	指定用户名称。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# user user1 aaa-server local
hostname(config-username)#
```

PnPVPN命令

关于P1 提议配置、ISAKMP网关配置、P2 提议配置以及隧道配置命令，请参考请参考 IPSec协议命令一章。本节仅介绍PnPVPN特有命令行。

dhcp-pool-address

为用户配置 DHCP 地址池。

［命令］

dhcp-pool-address *start-ipaddr end-ipaddr*

no dhcp-pool-address

［句法描述］

start-ipaddr	指定地址池的起始 IP 地址。
end-ipaddr	指定地址池的终止 IP 地址。

［默认取值］

无。

［命令模式］

本地用户配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# user user1 aaa-server local
hostname(config-username)# dhcp-pool-address 192.168.10.5
192.168.10.250
```

dhcp-pool-gateway

配置 DHCP 地址池的网关地址。该地址用来作为 PnPVPN 客户端内网接口的 IP 地址，并被设置为 PC 的网关地址，PC 的 IP 地址由以上设置的 DHCP 地址池的网段以及网络掩码确

定，所以网关地址应该和 DHCP 地址池在同一个网段。使用该命令 no 的形式取消网关地址的配置。

［命令］

dhcp-pool-gateway *A.B.C.D*

no dhcp-pool-gateway

［句法描述］

A.B.C.D	指定 DHCP 地址池的网关地址。

［默认取值］

无。

［命令模式］

本地用户配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# user user1 aaa-server local
hostname(config-username)# dhcp-pool-gateway 192.168.10.252
```

dhcp-pool-netmask

配置 DHCP 地址池的网络掩码。使用该命令 no 的形式取消网络掩码的配置。

［命令］

dhcp-pool-netmask *A.B.C.D*

no dhcp-pool-netmask

［句法描述］

A.B.C.D	指定 DHCP 地址池的网络掩码。

［默认取值］

无。

［命令模式］

本地用户配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# user user1 aaa-server local
hostname(config-username)# dhcp-pool-netmask 255.255.255.0
```

dns

配置 DNS 服务器。使用该命令 no 的形式取消对 DNS 服务器的指定。

［命令］

dns *A.B.C.D* [*A.B.C.D*] [*A.B.C.D*] [*A.B.C.D*]

no dns

［句法描述］

A.B.C.D	指定 DNS 服务器的 IP 地址。

［默认取值］

无。

［命令模式］

本地用户配置模式或隧道配置模式。

［使用指导］

用户最多可配置 4 个 DNS 服务器。

［命令实例］

```
hostname(config)# user user1 aaa-server local
hostname(config-username)# dns 10.10.100.5 10.10.100.15
```

peer_id fqdn

配置 ISAKMP 网关对端通配符。使用该命令 no 的形式配置。

［命令］

peer-id fqdn wildcard *string*

no peer-id

［句法描述］

fqdn	指定使用 FQDN 类型的通配符。
wildcard *string*	指定通配符 ID，通常为客户端的域名。如 abc.com。

［默认取值］

无。

［命令模式］

ISAKMP 网关配置模式。

［使用指导］

当 PnPVPN Server 通过 Radius 服务器进行认证时，需要配置 ISAKMP 网关对端的通配符。

［命令实例］

```
hostname(config)# isakmp peer test
hostname(config-isakmp-peer)# peer-id fqdn wildcard abc.com
```

split-tunnel-route

配置 PnPVPN 隧道路由。PnPVPN 隧道路由是指通过 PnPVPN 隧道到指定网段的路由。PnPVPN 客户端通过服务器端下发的隧道路由可以访问到指定的网段。使用该命令 no 的形式删除指定的路由。

［命令］

split-tunnel-route *A.B.C.D/Mask*

no split-tunnel-route *A.B.C.D/Mask*

［句法描述］

A.B.C.D/Mask	*A.B.C.D* 为 IP 地址前缀，*Mask* 为子网掩码的位数。

［默认取值］

无。

［命令模式］

本地用户配置模式或隧道配置模式。

［使用指导］

用户可以重复使用该命令添加多条隧道路由。

［命令实例］

```
hostname(config)# user user1 aaa-server local
hostname(config-username)# split-tunnel-route 192.168.3.0/24
```

tunnel-ip-address

指定客户端隧道接口的 IP 地址，并启用 SNAT 规则。使用该命令 no 的形式取消配置客户端的隧道接口。

［命令］

tunnel-ip-address *A.B.C.D* **[snat]**

no tunnel-ip-address

［句法描述］

A.B.C.D	指定客户端隧道接口的 IP 地址，该地址不能与客户端已存在的 IP 地址冲突。
snat	启用 SNAT 规则。默认情况下，系统不开启隧道接口的 SNAT 规则。

［默认取值］

无。

［命令模式］

本地用户配置模式。

［使用指导］

如果 PnPVPN 客户端是由 Hillstone SR 系列安全路由器充当，那么需要 SR 系列产品的版本支持该功能。

［命令实例］

```
hostname(config)# aaa-server local
hostname(config-aaa-server)# user shanghai
hostname(config-user)# tunnel-ip-address 172.1.1.16 snat
```

user

在 PnPVPN 服务端创建客户端拨号用户名。使用该命令 no 的形式删除指定的用户名。

［命令］

user *user-name* **aaa-server local**

no user *user-name*

［句法描述］

user-name	指定用户名称。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# user user1 aaa-server local
hostname(config-username)#
```

wins

配置 WINS 服务器。使用该命令 no 的形式取消对 WINS 服务器的指定。

［命令］

wins *A.B.C.D* [*A.B.C.D*]

no wins

［句法描述］

A.B.C.D	指定 WINS 服务器的 IP 地址。

［默认取值］

无。

［命令模式］

本地用户配置模式或隧道配置模式。

［使用指导］

用户最多可配置两个 WINS 服务器。

［命令实例］

```
hostname(config)# user user1 aaa-server local
hostname(config-username)# wins 10.10.100.6 10.10.100.16
```

GRE命令

destination

为 GRE 隧道指定目的地址。使用该命令 no 的形式取消目的地址的配置。

［命令］

destination *ip-address*

no destination

［句法描述］

ip-address	为 GRE 隧道指定目的地址。

［默认取值］

无。

［命令模式］

GRE 隧道配置模式。

［使用指导］

无。

［命令实例］

hostname(config-tunnel-gre)# **destination 1.1.1.1**

interface

为 GRE 隧道指定出接口。使用该命令 no 的形式取消出接口配置。

［命令］

interface *interface-name*

no interface

［句法描述］

interface-name	指定出接口的名称。

［默认取值］

无。

［命令模式］

GRE 隧道配置模式。

［使用指导］

无。

［命令实例］

hostname(config-tunnel-gre)# **interface ethernet0/3**

---

next-tunnel ipsec

指定 IPSec VPN 隧道对数据进行 IPSec 封装。使用该命令 no 的形式取消 IPSec VPN 隧道的指定。

［命令］

next-tunnel ipsec *tunnel-name*

no next-tunnel ipsec

［句法描述］

tunnel-name	指定 IPSec VPN 隧道的名称。

［默认取值］

无。

［命令模式］

GRE 隧道配置模式。

［使用指导］

无。

［命令实例］

hostname(config-tunnel-gre)# **next-tunnel ipsec vpn1**

---

source

为 GRE 隧道指定源地址。使用该命令 no 的形式取消源地址的配置。

［命令］

source {**interface** *interface-name* | *ip-address*}

no source

［句法描述］

interface *interface-name*	指定接口的 IP 地址为 GRE 隧道的源地址。通过 *interface-name* 参数指定接口名称。
ip-address	为 GRE 隧道指定源地址。

［默认取值］

无。

［命令模式］

GRE 隧道配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-tunnel-gre)# source 192.168.1.1
```

tunnel gre

绑定 GRE 隧道到隧道接口。使用该命令 no 的形式取消 GRE 隧道的绑定。

［命令］

tunnel gre *gre-tunnel-name* [**gw** *ip-address*]

no gre *gre-tunnel-name* [**gw** *ip-address*]

［句法描述］

gre-tunnel-name	指定将要绑定的 GRE 隧道的名称。该隧道为系统中已创建的 GRE 隧道。
gw *ip-address*	当配置多个隧道到隧道接口时，需要配置该参数。该参数指定 GRE 隧道的下一跳 IP 地址，为对端隧道接口的 IP 地址。系统默认值为 0.0.0.0。

［默认取值］

无。

［命令模式］

隧道接口配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# interface tunnel1
```

```
hostname(config-if-tun1)# tunnel gre test
```

L2TP命令

aaa-server

指定 AAA 服务器用于客户端用户身份认证。使用该命令 no 的形式取消对 AAA 服务器的指定。

［命令］

aaa-server *aaa-server-name* [**domain** *domain-name*]

no aaa-server *aaa-server-name* [**domain** *domain-name*]

［句法描述］

aaa-server-name	指定 AAA 服务器的名称。
domain-name	为 AAA 服务器指定域名以区分不同的 AAA 服务器。

［默认取值］

系统默认服务器：local。

［命令模式］

L2TP 实例配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# tunnel l2tp l2tptunnel1
hostname(config-tunnel-l2tp)# aaa-server server1
```

accept-client-ip

允许用户指定 IP 地址。默认情况下，客户端的 IP 地址由 LNS 从地址池中取出并自动分配。启用该功能后，用户可以指定 IP 地址。使用该命令 no 的形式禁止用户指定 IP 地址。

［命令］

accept-client-ip

no accept-client-ip

［句法描述］

无。

［默认取值］

开启。

［命令模式］

L2TP 实例配置模式。

［使用指导］

用户指定的 IP 地址必须属于已指定的地址池范围之内且与用户的用户名和角色一致。如果指定的 IP 地址已被占用，则系统禁止该用户登录。

［命令实例］

```
hostname(config)# tunnel l2tp l2tptunnel1
hostname(config-tunnel-l2tp)# accept-client-ip
```

address

为地址池配置地址范围。使用该命令 no 的形式删除配置的 IP 地址范围。

［命令］

address *start-ip end-ip*

no address

［句法描述］

start-ip	指定 IP 范围的起始 IP 地址。
end-ip	指定 IP 范围的结束 IP 地址。

［默认取值］

无。

［命令模式］

L2TP 地址池配置模式。

［使用指导］

用户可以为一个地址池最多指定 60000 个 IP 地址。

［命令实例］

```
hostname(config)# l2tp pool pool1
hostname(config-pool-l2tp)# address 192.168.1.0 192.168.1.254
```

allow-multi-logon

配置用户同名登录功能。开启该功能后，系统允许同一个用户在多个地点同时登录。使用该命令 no 的形式关闭用户同名登录功能。

［命令］

allow-multi-logon

no allow-multi-logon

［句法描述］

无。

［默认取值］

开启。

［命令模式］

L2TP 实例配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# tunnel l2tp l2tptunnel1
hostname(config-tunnel-l2tp)# no allow-multi-logon
```

---

avp-hidden

启用 AVP 数据隐含功能。在默认情况下，AVP 是采用明文形式传输的。为了保证数据安全，用户可以通过隧道密码加解密这些数据，将这些 AVP 隐藏起来传输。使用该命令 no 的形式关闭 AVP 数据隐含功能。

［命令］

avp-hidden

no avp-hidden

［句法描述］

无。

［默认取值］

关闭。

［命令模式］

L2TP 实例配置模式。

［使用指导］

启用 AVP 数据隐含功能需要配置隧道密码。

［命令实例］

```
hostname(config)# tunnel l2tp l2tptunnel1
hostname(config-tunnel-l2tp)# avp-hidden
```

clear l2tp

重启隧道。

［命令］

clear l2tp *tunnel-name*

［句法描述］

tunnel-name	指定 L2TP 实例的名称。

［默认取值］

无。

［命令模式］

任何模式。

［使用指导］

隧道重启后，所有与该隧道的连接将被清除。

［命令实例］

```
hostname(config)# clear l2tp l2tptunnel1
```

dns

配置 DNS 服务器。使用该命令 no 的形式取消对 DNS 服务器的指定。

［命令］

dns *address1* [*address2*]

no dns

［句法描述］

address1	指定 DNS 服务器 IP 地址。

［默认取值］

无。

［命令模式］

L2TP 实例配置模式。

［使用指导］

用户最多可配置 2 个 DNS 服务器。

［命令实例］

```
hostname(config)# tunnel l2tp l2tptunnel1
hostname(config-tunnel-l2tp)# dns 1.1.1.1
```

exclude address

配置保留地址池。保留地址池中的 IP 地址为地址池中的部分 IP 地址，不向客户端分配。使用该命令 no 的形式取消保留地址池的配置。

［命令］

exclude address *start-ip end-ip*

no exclude address

［句法描述］

start-ip	指定保留地址池的起始 IP 地址。
end-ip	指定保留地址池的结束 IP 地址。

［默认取值］

无。

［命令模式］

L2TP 地址池配置模式。

［使用指导］

保留地址池中的 IP 地址为地址池中的部分 IP 地址。

［命令实例］

```
hostname(config)# l2tp pool pool1
hostname(config-pool-l2tp)# address 1.1.1.0 1.1.1.100
hostname(config-pool-l2tp)# exclude address 1.1.1.0 1.1.1.10
```

exec l2tp kickout

强制断开某个用户与 LNS 的连接。

［命令］

exec l2tp *tunnel-name* **kickout user** *user-name*

［句法描述］

tunnel-name	指定 L2TP 实例的名称。
user-name	指定被强制断开连接的用户名称。

［默认取值］

无。

［命令模式］

执行模式。

［使用指导］

无。

［命令实例］

hostname# **exec l2tp l2tptunnel1 kickout user user1**

interface

指定隧道的出接口。使用该命令 no 的形式取消出接口的配置。

［命令］

interface *interface-name*

no interface

［句法描述］

interface-name	指定隧道出接口的名称。

［默认取值］

无。

［命令模式］

L2TP 实例配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# tunnel l2tp l2tptunnel1
hostname(config-tunnel-l2tp)# interface ethernet0/1
```

ip-binding role

配置角色-IP 地址绑定规则。角色-IP 地址绑定规则是将角色与已配置地址池中的某一 IP 地址范围绑定，当此客户端连接成功后，设备端会从绑定的地址范围中取出一个 IP 地址分配给客户端。

［命令］

ip-binding role *role-name* **ip-range** *start-ip end-ip*

no ip-binding role *role-name*

［句法描述］

role *role-name*	指定角色名称。
ip-range *start-ip end-ip*	指定绑定的 IP 范围的起始 IP 地址 start-ip 和结束 IP 地址 end-ip。此地址范围必须为地址池中可以分配的地址范围。

［默认取值］

无。

［命令模式］

L2TP 地址池配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# l2tp pool pool1
hostname(config-pool-l2tp)# address 1.1.1.0 1.1.1.100
hostname(config-pool-l2tp)# ip-binding role role1 ip-range 1.1.1.20
 1.1.1.30
```

ip-binding user

配置静态 IP 地址绑定规则。静态 IP 地址绑定规则将客户端用户与已配置地址池中的某个固定 IP 地址绑定，当客户端连接成功后，设备端会将绑定的 IP 地址分配给客户端。使用该命令 no 的形式取消对特定用户静态 IP 地址绑定规则的配置。

［命令］

ip-binding user *user-name* **ip** *ip-address*

no ip-binding user *user-name*

［句法描述］

user *user-name*	指定客户端用户名。
ip *ip-address*	指定绑定的 IP 地址。此地址必须为地址池中可以分配的地址。

［默认取值］

无。

［命令模式］

L2TP 地址池配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# l2tp pool pool1
hostname(config-pool-l2tp)# address 1.1.1.0 1.1.1.100
hostname(config-pool-l2tp)# ip-binding user user1 ip 1.1.1.10
```

keepalive

指定 Hello 报文发送的时间间隔。使用该命令 no 的形式取消指定 Hello 报文发送的时间间隔。

［命令］

keepalive *time*

no keepalive

［句法描述］

time	指定 Hello 报文发送的时间间隔。单位为秒。范围是 60 到 1800 秒。

［默认取值］

60 秒。

［命令模式］

L2TP 实例配置模式。

［使用指导］

L2TP 使用 Hello 报文来检测隧道是否连通。LNS 定时向 L2TP 客户端或 LAC 发送 Hello 报文，若在一段时间内未收到应答，该隧道连接将被断开。

［命令实例］

```
hostname(config)# tunnel l2tp l2tptunnel1
hostname(config-tunnel-l2tp)# keepalive 800
```

move

移动已有的角色-IP 地址绑定规则从而改变规则的排列顺序。

［命令］

move *role-name1* {**before** *role-name2* | **after** *role-name2* | **top** | **bottom**}

［句法描述］

role-name1	指定被移动的角色-IP 地址绑定规则的角色名称。
before *role-name2*	将角色-IP 地址绑定规则移动到某个角色-IP 地址绑定规则(角色名称为 role-name2 的规则)之前。
after *role-name2*	将角色-IP 地址绑定规则移动到某个角色-IP 地址绑定规则(角色名称为 role-name2 的规则)之后。
top	将角色-IP 地址绑定规则移动到所有角色-IP 地址绑定规则之首。
bottom	将角色-IP 地址绑定规则移动到所有角色-IP 地址绑定规则的末尾。

［默认取值］

默认情况下，系统会将新创建的规则放到所有规则的末尾。

［命令模式］

L2TP 地址池配置模式。

［使用指导］

一个用户可以绑定到一个或者多个角色，不同角色可以配置不同的角色-IP 地址绑定规则。对于绑定到多个角色且多个角色有相应的角色-IP 地址绑定规则的用户，安全网关会对角色-IP 地址绑定规则进行顺序查找，然后按照查找到的相匹配的第一条规则为用户分配地址。

［命令实例］

```
hostname(config)# l2tp pool pool1
hostname(config-pool-l2tp)# move role1 before role2
```

next-tunnel ipsec

在 L2TP 实例中引用 IPSec 隧道。使用该命令 no 的形式取消引用 IPSec 隧道。

［命令］

next-tunnel ipsec *tunnel-name*

［句法描述］

tunnel-name	指定已创建的 IPSec VPN 的隧道名称。

［默认取值］

无。

［命令模式］

L2TP 实例配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# tunnel l2tp l2tptunnel1
hostname(config-pool-l2tp)# next-tunnel ipsec vpn1
```

pool

为 L2TP 实例指定 L2TP 地址池。使用该命令 no 的形式取消指定地址池。

［命令］

pool *pool-name*

no pool

［句法描述］

pool-name	指定已配置的 L2TP 地址池名称。

［默认取值］

无。

［命令模式］

L2TP 实例配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# tunnel l2tp l2tptunnel1
hostname(config-tunnel-l2tp)# pool pool1
```

ppp-auth

指定 PPP 认证的协议。使用该命令 no 的形式恢复默认值。

［命令］

ppp-auth {pap | chap | any}

no ppp-auth

［句法描述］

pap	指定 PPP 认证方式为密码认证协议 PAP。
chap	指定 PPP 认证方式为质询握手认证协议 CHAP。
any	指定该参数后，系统首选认证方式为 CHAP，如果认证不支持 CHAP 协议，则使用 PAP 协议进行认证。

［默认取值］

CHAP。

［命令模式］

L2TP 实例配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **tunnel l2tp l2tptunnel1**

hostname(config-tunnel-l2tp)# **ppp-auth pap**

l2tp pool

创建 L2TP 地址池。执行该命令后，系统创建指定名称的地址池，并且进入 L2TP 地址池配置模式；如果指定的名称已存在，则直接进入 L2TP 地址池配置模式。使用该命令 no 的形式删除指定的 L2TP 地址池。

［命令］

l2tp pool *pool-name*

no l2tp pool *pool-name*

［句法描述］

pool-name	指定地址池的名称。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# l2tp pool pool1
hostname(config-pool-l2tp)#
```

local-name

指定 LNS 本端隧道的名称。使用该命令 no 的形式恢复 LNS 本端的默认名称。

［命令］

local-name *name*

no local-name

［句法描述］

name	指定 LNS 端隧道的名称。范围为 6 至 30 个字符。

［默认取值］

LNS。

［命令模式］

L2TP 实例配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# tunnel l2tp l2tptunnel1
hostname(config-tunnel-l2tp)# local-name LNS123456
```

secret

指定 LNS 端隧道认证的密码。使用该命令 no 的形式取消指定隧道密码。

［命令］

secret *secret-string* [**peer-name** *name*]

no secret *secret-string* [**peer-name** *name*]

［句法描述］

secret-string	指定隧道密码。范围为 30 至 60 字符。
peer-name *name*	指定 LAC 端设备的主机名称。如果多个 LAC 与 LNS 建立连接，用户可通过配置该项参数为不同的 LAC 端设备指定不同的隧道密码。如果没有指定该参数，系统对多个 LAC 端均使用相同的隧道密码。

［默认取值］

无。

［命令模式］

L2TP 实例配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **tunnel l2tp l2tptunnel1**

hostname(config-tunnel-l2tp)# **secret U8FdHNEEBz6sNn5Mvqx3yWuLRWce peer-name lac1**

hostname(config-tunnel-l2tp)# **secret NEEBz6sU8FdHNn5MvRWceqx3yWuL peer-name lac2**

transmit-retry

指定控制报文的重传次数。使用该命令 no 的形式恢复控制报文重传次数的默认值。

［命令］

transmit-retry *times*

no transmit-retry *times*

［句法描述］

times	指定控制报文重传次数。范围是 1 至 10 次。

［默认取值］

5 次。

［命令模式］

L2TP 实例配置模式。

［使用指导］

L2TP 协议使用两种类型的报文：控制报文和数据报文。控制报文负责创建、维护及清除 L2TP 隧道，数据报文负责传输数据。数据报文的传输是不可靠传输，若数据丢失，则不进行数据重传。控制报文的传输是可靠传输，如果在指定的重传次数内未收到对端的响应，则系统认为隧道连接已经断开。控制报文重传间隔从 1 秒开始，按照 2 的倍数增长，如 1 秒、2 秒、4 秒、8 秒、16 秒等。

［命令实例］

```
hostname(config)# tunnel l2tp l2tptunnel1
hostname(config-tunnel-l2tp)# transmit-retry 10
```

tunnel-authentication

启用隧道认证功能。使用该命令 no 的形式禁用隧道认证。

［命令］

```
tunnel-authentication
no tunnel-authentication
```

［句法描述］

无。

［默认取值］

关闭。

［命令模式］

L2TP 实例配置模式。

［使用指导］

在隧道建立连接前，用户可启用隧道认证功能以保证连接的安全。隧道认证可由 LNS 或 LAC 任何一端发起，只有两端均通过隧道认证，即隧道密码一致时，方可建立隧道。

［命令实例］

```
hostname(config)# tunnel l2tp l2tptunnel1
hostname(config-tunnel-l2tp)# tunnel-authentication
```

tunnel l2tp

创建 L2TP 实例。执行该命令后，系统创建指定名称的 L2TP 实例，并且进入 L2TP 实例配置模式；如果指定的名称已存在，则直接进入 L2TP 实例配置模式。使用该命令 no 的形式删除指定的 L2TP 实例。

［命令］

tunnel l2tp *tunnel-name*

no tunnel l2tp *tunnel-name*

［句法描述］

tunnel-name	指定 L2TP 实例的名称。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# tunnel l2tp l2tptunnel1
hostname(config-tunnel-l2tp)#
```

tunnel l2tp

绑定 L2TP 实例到隧道接口使其生效。使用该命令 no 的形式取消隧道接口与 L2TP 实例的绑定。

［命令］

tunnel l2tp *tunnel-name*

no tunnel l2tp *tunnel-name*

［句法描述］

tunnel-name	指定系统中已配置的 L2TP 实例的名称。

［默认取值］

无。

［命令模式］

隧道接口配置模式。

［使用指导］

每一个隧道接口只能绑定一个 L2TP 实例。

［命令实例］

```
hostname(config)# interface tunnel1
hostname(config-if-tun1)# tunnel l2tp l2tptunnel1
```

tunnel-receive-window

指定隧道传输数据的窗口大小。使用该命令 no 的形式恢复默认值。

［命令］

tunnel-receive-window *window-size*

no tunnel-receive-window *window-size*

［句法描述］

window-size	指定窗口大小。单位为包，取值范围为 4 至 800 包。

［默认取值］

8 包。

［命令模式］

L2TP 实例配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# tunnel l2tp l2tptunnel1
hostname(config-tunnel-l2tp)# tunnel-receive-window 20
```

wins

配置 WINS 服务器。使用该命令 no 的形式取消对 WINS 服务器的指定。

［命令］

wins *address1* [*address2*]

no wins

［句法描述］

address1	指定 WINS 服务器 IP 地址。

［默认取值］

无。

［命令模式］

L2TP 实例配置模式。

［使用指导］

用户最多可配置 2 个 WINS 服务器。

［命令实例］

```
hostname(config)# tunnel l2tp l2tptunnel1
hostname(config-tunnel-l2tp)# wins 1.1.1.10
```

攻击防护命令

ad all

开启域的所有攻击防范功能。使用该命令 no 的形式关闭域的所有攻击防范功能。

［命令］

ad all

no ad all

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

域配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **zone untrust**

hostname(config-zone-untrust)# **ad all**

ad arp-spoofing

开启并配置域的 ARP 欺骗攻击防范功能。使用该命令 no 的形式关闭域的 ARP 欺骗攻击防范功能或者恢复该功能参数的默认配置。

［命令］

ad arp-spoofing {**reverse-query** | **ip-number-per-mac** *number* [**action** [**drop** | **alarm**]] | **gratuitous-arp-send-rate** *number*}

no ad arp-spoofing reverse-query

no ad arp-spoofing ip-number-per-mac

no ad arp-spoofing gratuitous-arp-send-rate

［句法描述］

reverse-query	开启 ARP 反向查询功能。当设备收到 ARP 请求后，会纪录 IP 地址并且发送 ARP 请求检查是否会收到不同 MAC 地址的返回包或者返回包的 MAC 地址与 ARP 请求包的 MAC 地址是否相同。
ip-number-per-mac	指定是否检查 ARP 表中一个 MAC 地址对应的 IP 地址数。如果该参数值为 0，则不检查；如果非 0，则进行检查，并且如果每个 MAC 地址对应的 IP 地址数多于该参数的值，系统将按照 **action [drop | alarm]**参数的配置进行处理，处理行为可以是发出警报并且丢弃该 ARP 包（**drop**）或者发出警报但是允许包通过（**alarm**）。该参数的取值范围是 0 到 1024。
gratuitous-arp-send-rate	指定安全网关是否发出 Gratuitous ARP 包。如果该参数值是 0，则不发 Gratuitous ARP 包；如果非 0，则发出，并且每秒钟发出包的个数为该参数的值。该参数的取值范围是 0 到 10。

［默认取值］

reverse-query – 关闭。

ip-number-per-mac – 0（不检查）。

gratuitous-arp-send-rate – 0（不发出）。

［命令模式］

域配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# zone untrust
hostname(config-zone-untrust)# ad arp-spoofing ip-number-per-mac 256
```

ad dns-query-flood

开启并配置安全域的 DNS Query Flood 攻击防护功能。使用该命令 no 的形式关闭安全域的 DNS Query Flood 攻击防护功能或者恢复该功能参数的默认配置。

［命令］

ad dns-query-flood [recursion] [threshold *number* **| action {alarm | drop}]**

no ad dns-query-flood

no ad dns-query-flood threshold

no ad dns-query-flood action

［句法描述］

ad dns-query-flood	开启安全域的 DNS Query Flood 攻击防护功能。使用 **no ad dns-query-flood** 关闭该功能。
recursion	指定仅限制 DNS 递归查询报文。当不设置此选项时，表示限制所有 DNS 查询报文。
threshold *number*	指定安全网关收到的 DNS Query 包的个数的警戒值。如果同一个目的 IP 地址的同一个端口号在一秒钟内收到的 DNS Query 包的个数超过该警戒值，安全网关就判断为受到 DNS Query Flood 攻击，从而采取相应的处理。取值范围是 1 到 50000。对于 DNS 查询报文，*number* 的取值范围是 1 到 50000，默认值是 1500；对于 DNS 递归查询报文，*number* 的取值范围为 0 到 50000，默认值为 1000，当取值为 0 时禁止所有 DNS 递归查询报文通过。
action	指定设备对 DNS Query Flood 攻击采取的行为。 • **alarm**－发出警报但是允许 DNS 查询包通过； • **drop**－在发生攻击的当前秒和下一秒这段时间内，设备仅允许指定个数（**threshold** *number*）的 DNS 查询报文或 DNS 递归查询报文通过，并且发出警报，在这段时间内的其它同类包将会被丢弃。默认行为是 drop。

［默认取值］

threshold – 1500 个（DNS 查询报文）或 1000 个（DNS 递归查询报文）。

action – drop。

［命令模式］

域配置模式。

［使用指导］

DNS Query Flood 攻击防护功能仅对 UDP DNS 查询报文有效。

［命令实例］

```
hostname(config)# zone untrust
hostname(config-zone-untrust)# ad dns-query-flood threshold 100
```

ad huge-icmp-pak

开启并配置域的 Huge ICMP 攻击防范功能。使用该命令 no 的形式关闭域的 Huge ICMP 攻击防范功能或者恢复该功能参数的默认配置。

［命令］

ad huge-icmp-pak [threshold *number* **| action {alarm | drop}]**

no ad huge-icmp-pak

no ad huge-icmp-pak threshold

no ad huge-icmp-pak action

［句法描述］

threshold	指定 ICMP 包的大小的警戒值。如果收到的 ICMP 包的大小大于该指定值，安全网关就判断为受到 Huge ICMP 包攻击。范围是 1 到 50000 字节。
action	指定安全网关对于 Huge ICMP 包攻击的操作。 • **alarm**：发出警报但是允许包通过。 • **drop**：发出警报并且丢弃攻击包。

［默认取值］

threshold – 1024 字节。

action – drop。

［命令模式］

域配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **zone untrust**

hostname(config-zone-untrust)# **ad huge-icmp-pak threshold 500**

ad icmp-flood

开启并配置域的 ICMP Flood 攻击防范功能。使用该命令 no 的形式关闭域的 ICMP Flood 攻击防范功能或者恢复该功能参数的默认配置。

［命令］

ad icmp-flood [threshold *number* **| action {alarm | drop}]**

no ad icmp-flood

no ad icmp-flood threshold

no ad icmp-flood action

［句法描述］

threshold	指定安全网关收到的 ICMP 包的个数的警戒值。如果同一个目的 IP 地址

	在一秒钟内收到的 ICMP 包的个数超过该警戒值，安全网关就判断为受到 ICMP Flood 攻击。范围是 1 到 50000 个每秒。
action	指定安全网关对于 ICMP Flood 攻击的操作。 • **alarm**：发出警报但是允许包通过。 • **drop**：在发生攻击的当前秒和下一秒这段时间内，安全网关仅允许指定个数（**threshold** *number*）的 ICMP 包通过，并且发出警报，在这段时间内的其它同类包将会被丢弃。

［默认取值］

threshold – 1500 个每秒。

action – **drop**。

［命令模式］

域配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# zone untrust
hostname(config-zone-untrust)# ad icmp-flood threshold 1000
```

ad ip-directed-broadcast

开启并配置域的 Smurf 和 Fraggle 攻击防范功能。使用该命令 no 的形式关闭域的 Smurf 和 Fraggle 攻击防范功能或者恢复该功能参数的默认配置。

［命令］

ad ip-directed-broadcast [action {alarm | drop}]

no ad ip-directed-broadcast

no ad ip-directed-broadcast action

［句法描述］

action	指定安全网关对于 Smurf 和 Fraggle 攻击的操作。 • **alarm**：发出警报但是允许包通过。 • **drop**：发出警报并且丢弃攻击包。

［默认取值］

action – **drop**。

［命令模式］

域配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# zone untrust
hostname(config-zone-untrust)# ad ip-directed-broadcast
```

ad ip-fragment

开启并配置域的 IP 碎片攻击防范功能。使用该命令 no 的形式关闭域的 IP 碎片攻击防范功能或者恢复该功能参数的默认配置。

［命令］

```
ad ip-fragment [action {alarm | drop}]
no ad ip-fragment
no ad ip-fragment action
```

［句法描述］

action	指定安全网关对于 IP 碎片攻击的操作。 • **alarm**：发出警报但是允许包通过。 • **drop**：发出警报并且丢弃攻击包。

［默认取值］

action – drop。

［命令模式］

域配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# zone untrust
hostname(config-zone-untrust)# ad ip-fragment
```

ad ip-option

开启并配置域的 IP Option 攻击防范功能。使用该命令 no 的形式关闭域的 IP Option 攻击防范功能或者恢复该功能参数的默认配置。

［命令］

ad ip-option [action {alarm | drop}]

no ad ip-option

no ad ip-option action

［句法描述］

action	指定安全网关对于 IP Option 攻击的操作。 • **alarm**：发出警报但是允许包通过。 • **drop**：发出警报并且丢弃攻击包。

［默认取值］

action – drop。

［命令模式］

域配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **zone untrust**

hostname(config-zone-untrust)# **ad ip-option**

ad ip-spoofing

开启域的二层或者三层 IP 地址欺骗攻击防范功能。使用该命令 no 的形式关闭域的 IP 地址欺骗攻击防范功能。

［命令］

ad ip-spoofing

no ad ip-spoofing

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

二层安全域或者三层安全域配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# zone untrust
hostname(config-zone-untrust)# ad ip-spoofing
```

ad ip-sweep

开启并配置域的 IP 地址扫描攻击防范功能。使用该命令 no 的形式关闭域的 IP 地址扫描攻击防范功能或者恢复该功能参数的默认配置。

［命令］

ad ip-sweep [**threshold** *value*| **action** {**alarm** | **drop**}]

no ad ip-sweep

no ad ip-sweep threshold

no ad ip-sweep action

［句法描述］

threshold	指定地址扫描的警戒值。如果安全网关探测到在该指定时间内有 10 个以上来自同一个源 IP 地址的 ICMP 包发往不同的主机，安全网关就认为是受到 IP 地址扫描攻击。取值范围是 1 到 5000 毫秒。
action	指定安全网关对于 IP 地址扫描攻击的操作。 • **alarm**：发出警报但是允许包通过。 • **drop**：在指定时间内（**threshold** *value*），安全网关仅允许 10 个来自同一个源 IP 地址的发往不同主机的 ICMP 包通过，并且发出警报，指定时间内的其它同类包将会被丢弃。

［默认取值］

threshold – 1 毫秒。

action – **drop**。

［命令模式］

域配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# zone untrust
hostname(config-zone-untrust)# ad ip-sweep threshold 2000
```

ad land-attack

开启并配置域的 Land 攻击防范功能。使用该命令 no 的形式关闭域的 Land 攻击防范功能或者恢复该功能参数的默认配置。

［命令］

ad land-attack [action {alarm | drop}]

no ad land-attack

no ad land-attack action

［句法描述］

action	指定安全网关对于 Land 攻击的操作。 • **alarm**：发出警报但是允许包通过。 • **drop**：发出警报并且丢弃攻击包。

［默认取值］

action – drop。

［命令模式］

域配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# zone untrust
hostname(config-zone-untrust)# ad land-attack
```

ad ping-of-death

开启域的 Ping of Death 攻击防范功能。使用该命令 no 的形式关闭域的 Ping of Death 攻击防范功能。

［命令］

ad ping-of-death

no ad ping-of-death

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

域配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# zone untrust
hostname(config-zone-untrust)# ad ping-of-death
```

ad port-scan

开启并配置域的端口扫描攻击防范功能。使用该命令 no 的形式关闭域的端口扫描攻击防范功能或者恢复该功能参数的默认配置。

［命令］

ad port-scan [**threshold** *value*| **action** {**alarm** | **drop**}]

no ad port-scan

no ad port-scan threshold

no ad port-scan action

［句法描述］

threshold	指定端口扫描的时间警戒值。如果安全网关探测到在该指定时间内有 10 个以上 TCP SYN 包发往同一目标的不同端口，安全网关就认为是端口扫描攻击。取值范围是 1 到 5000 毫秒。
action	指定安全网关对于端口扫描攻击的操作。 • **alarm**：发出警报但是允许包通过。 • **drop**：在指定时间内（**threshold** *value*），安全网关仅允许 10 个发往同一目标的不同端口的 TCP SYN 包通过，并且发出警报，指定时间内的其它同类包将会被丢弃。

［默认取值］

threshold – 1 毫秒。

action – **drop**。

［命令模式］

域配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# zone untrust
hostname(config-zone-untrust)# ad port-scan threshold 1 action alarm
```

ad session-limit

限制基于域的 IP 地址的会话数。使用该命令 no 的形式删除安全域的会话限制规则。

［命令］

ad session-limit {[[**src-ip** *address-entry*] [**dst-ip** *address-entry*] | **ip** *address-entry*] [**service** *servicename*] [**role** *role-name* | **user** *aaa-server-name user-name* | **user-group** *aaa-server-name user-group-name*]} {**session** { **unlimit** | **max** *number* [**per-srcip** | **per-dstip** | **per-ip**] | **per-user**} | **ramp-rate max** *number*} [**schedule** *schedule-name*]

no ad session-limit

［句法描述］

src-ip *address-entry*	限制安全域的源 IP 地址会话数。*address-entry* 为 **src-ip** 的 IP 地址范围。该参数值为地址簿中定义的一条地址条目。
dst-ip *address-entry*	限制安全域的目的 IP 地址会话数。*address-entry* 为 **dst-ip** 的 IP 地址范围。该参数值为地址簿中定义的一条地址条目。
ip *address-entry*	限制安全域中某个 IP 地址段的会话数。*address-entry* 为 **ip** 的 IP 地址范围。该参数值为地址簿中定义的一条地址条目。
service *servicename*	限制安全域中特定服务的会话数。
role *role-name*	限制特定角色的会话数。
user *aaa-server-name user-name*	限制特定用户的会话数。
user-group *aaa-server-name user-group-name*	限制特定用户组的会话数。
session {**unlimit** | **max** *number* [**per-srcip** | **per-dstip** | **per-ip**] | **per-user** }	指定 IP 地址或角色的最大会话数。**unlimit** 为无会话数限制。**session max** *number* 指定地址条目中所有 IP 地址的最大会话数或者角色对应的所有用户的最大会话数；如果使用 **per-srcip**、**per-dstip**、**per-ip** 或者 **per-user** 关键字，则 **session max** *number* 指定的为每个 IP 地址的最大会话数或者角色对应的每个用户的最大会话数。**per-srcip**、**per-dstip**、**per-ip** 和 **per-user** 四个关键字需和前面的 **src-ip**、**dst-ip**、**ip** 和 **role** 关键字一一对应，如：只有在前面指定了 **src-ip** 才可以在后面选择 **per-srcip**。
ramp-rate max *number*	指定 IP 地址或者角色每秒钟可建立的最大会话数。

schedule *schedule-name*	指定会话限制规则的生效时间。

［默认取值］

无默认值。

［命令模式］

域配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **zone untrust**

hostname(config-zone-untrust)# **ad session-limit ip addr1 session max 2048**

ad syn-flood

开启并配置域的 SYN Flood 攻击防范功能。使用该命令 no 的形式关闭域的 SYN Flood 攻击防范功能或者恢复该功能参数的默认配置。

［命令］

ad syn-flood [**source-threshold** *number* | **destination-threshold** [**ip-based** | **port-based**] *number* | **destination** [**ip-based** | **port-based** [**address-book** *address-entry* | *A.B.C.D/M*] | **action** {**alarm** | **drop**}]

no ad syn-flood

no ad syn-flood source-threshold

no ad syn-flood destination-threshold [**ip-base** | **port-base**]

no ad syn-flood destination

no ad syn-flood action

［句法描述］

source-threshold	指定一秒钟内从一个源 IP 地址发出的 SYN 包的个数，无论目标 IP 地址和端口号是什么。如果安全网关探测到一秒钟内从同一个源 IP 地址发出的 SYN 包多余该指定数，就判断为受到了 SYN Flood 攻击。取值范围是 0 到 50000 个。0 表示不对源警戒值进行检测。
destination-threshold [**ip-based** | **port-based**] *number*	指定一秒钟内同一个目的 IP 地址（**ip-based**）或者同一目的 IP 的同一个目的端口（**port-based**）收到的 SYN 包个数，若不指定，则默认为 **ip-based**。如果安全网关探测到一秒钟同一个目的 IP 地址或者同一目的 IP 的同一个目的端口收到的

	SYN 包多于该指定数，就认为是受到了 SYN Flood 攻击。默认值是 1500 个。取值范围是 0 到 50000 个。0 表示不对目的警戒值进行检测。
destination [**ip-based** | **port-based** [**address-book** *address-entry* | *A.B.C.D/M*]	开启基于目的 IP 地址（**ip-based**）或者目的端口（**port-based**）的 SYN Flood 攻击防护功能，若不指定，则默认为 **ip-based**。使用 **address-book** *address-entry* | *A.B.C.D/M* 参数，指定开启特定网段的基于目的端口的 SYN Flood 攻击防护功能，其它网段做基于目的 IP 地址的 SYN Flood 攻击防护。目的 IP 地址掩码取值范围是 24 到 32。
action	指定安全网关对于 SYN Flood 攻击的操作。 • **alarm**：发出警报但是允许包通过。 • **drop**：在发生攻击的当前秒和下一秒这段时间内，安全网关仅允许指定个数（**source-threshold** *number* | **destination-threshold** *number*）的 SYN 包通过，并且发出警报，在这段时间内的其它同类包将会被丢弃；如果同时配置了源和目的警戒值，系统会先检查其是否为目的 SYN Flood 攻击，如果是，则丢弃并报警，如果不是，再检查其是否为源 SYN Flood 攻击，是则丢弃并报警。

［默认取值］

source-threshold – 1500 个。

destination-threshold – 1500 个。

action – **drop**。

［命令模式］

域配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# zone untrust
hostname(config-zone-untrust)# ad syn-flood source-threshold 1000
```

ad syn-proxy

开启并配置域的 SYN-Proxy 功能与 **ad syn-flood** 命令来共同防范 SYN Flood 攻击。使用该命令 no 的形式关闭域的 SYN-Proxy 功能或者恢复该功能参数的默认配置。

［命令］

ad syn-proxy [**min-proxy-rate** *number* \| **max-proxy-rate** *number* \| **proxy-timeout** *number* \| **cookie**]

no ad syn-proxy

no ad syn-proxy min-proxy-rate

no ad syn-proxy max-proxy-rate

no ad syn-proxy proxy-timeout

no ad syn-proxy cookie

［句法描述］

min-proxy-rate	指定激活 SYN-Proxy 机制的最小 SYN 包个数值。如果一个目的 IP 地址的同一个端口在一秒钟内收到的 SYN 包个数多余该参数的指定值，就会激活 SYN-Proxy 机制。因为 SYN-Proxy 功能需要配合 **ad syn-flood** 命令共同起效，该参数的值必须小余 **ad syn-flood** 命令的 **destination-threshold** 参数的值。范围是 1 到 50000 个每秒。
max-proxy-rate	如果一个目的 IP 地址的同一个端口在一秒钟内收到的 SYN 包个数多于该参数的指定值，安全网关会在当前秒和下一秒内仅允许该指定数值的 SYN 包通过，其它同类包将会被丢弃。范围是 1 到 1500000 个每秒。
proxy-timeout	指定半连接的超时时间值。半连接达到该超时值后会被丢弃。取值范围是 1 到 180 秒。
cookie	开启 SYN-Cookie 功能（如果需要开启该功能，请先开启 SYN-Proxy 功能）。该功能开启后，能够在功能上扩大安全网关处理多个 SYN 包的能力，因此用户可以适当的增大 **min-proxy-rate** 和 **max-proxy-rate** 两个参数之间的范围。

［默认取值］

min-proxy-rate – 1000 个每秒。

max-proxy-rate – 3000 个每秒。

proxy-timeout – 30 秒。

cookie – 关闭。

［命令模式］

安全域配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# zone untrust
hostname(config-zone-untrust)# ad syn-proxy
hostname(config-zone-untrust)# ad syn-proxy cookie
```

ad tcp-anomaly

开启并配置域的 TCP Anomaly 攻击防范功能。使用该命令 no 的形式关闭域的 TCP Anomaly 攻击防范功能或者恢复该功能参数的默认配置。

［命令］

ad tcp-anomaly [action {alarm | drop}]

no ad tcp-anomaly

no ad tcp-anomaly action

［句法描述］

action	指定安全网关对于 TCP Anomaly 攻击的操作。 • **alarm**：发出警报但是允许包通过。 • **drop**：发出警报并且丢弃攻击包。

［默认取值］

action – drop。

［命令模式］

域配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **zone untrust**

hostname(config-zone-untrust)# **ad tcp-anomaly**

ad tear-drop

开启域的 Teardrop 攻击防范功能。使用该命令 no 的形式关闭域的 Teardrop 攻击防范功能。

［命令］

ad tear-drop

no ad tear-drop

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

域配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# zone untrust
hostname(config-zone-untrust)# ad tear-drop
```

ad udp-flood

开启并配置域的 UDP Flood 攻击防护功能。使用该命令 no 的形式关闭域的 UDP Flood 攻击防护功能或者恢复该功能参数的默认配置。

［命令］

ad udp-flood [**source-threshold** *number* | **destination-threshold** *number* | **action** {**alarm** | **drop**}]

no ad udp-flood

no ad udp-flood source-threshold

no ad udp-flood destination-threshold

no ad udp-flood action

［句法描述］

ad udp-flood	开启安全域的 UDP Flood 攻击防护功能。
source-threshold *number*	指定同一个源 IP 地址在一秒钟内发出的 UDP 包个数的警戒值。如果安全网关在一秒钟内收到的 UDP 包超过该警戒值，则认为受到了 UDP Flood 攻击。number 的默认值是 1500 个，取值范围是 1 到 50000。
destination-threshold *number*	指定同一个目的 IP 地址的同一个端口号在一秒钟内收到的 UDP 包个数的警戒值。如果安全网关在一秒钟内收到的 UDP 包超过该警戒值，则认为受到了 UDP Flood 攻击。number 的默认值是 1500 个，取值范围是 1 到 50000。
action {**alarm** | **drop**}	指定安全网关对于 UDP Flood 攻击采取的行为。 • **alarm**：发出警报但是允许包通过。 • **drop**：在发生攻击的当前秒和下一秒这段时间内，安全网关仅允许指定个数（**source-threshold** *number* | **destination-threshold** *number*）的 UDP 包通过，并且发出警报，在这段时间内的其它同类包将会被丢弃。

［默认取值］

source-threshold *number* | **destination-threshold** *number* – 1500 个。

action – drop。

［命令模式］

域配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# zone untrust
hostname(config-zone-untrust)# ad udp-flood source-threshold 100
```

ad winnuke

开启域的 WinNuke 攻击防范功能。使用该命令 no 的形式关闭域的 WinNuke 攻击防范功能。

［命令］

ad winnuke

no ad winnuke

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

域配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# zone untrust
hostname(config-zone-untrust)# ad winnuke
```

ad tear-drop

开启并配置域的 Tear Drop 攻击防范功能。使用该命令 no 的形式关闭域的 Tear Drop 攻击防范功能或者恢复该功能参数的默认配置。

［命令］

ad tear-drop [action {alarm | drop}]

no ad tear-drop

no ad tear-drop action

［句法描述］

action	指定安全网关对于 Tear Drop 攻击的操作。 • **alarm**：发出警报但是允许包通过。 • **drop**：发出警报并且丢弃攻击包。

［默认取值］

action – drop。

［命令模式］

域配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **zone untrust**

hostname(config-zone-untrust)# **ad tear-drop**

clear ad zone

清除指定域的攻击防范统计信息。

［命令］

clear ad zone *zone-name* **statistics**

［句法描述］

zone-name	指定安全域的名称。

［默认取值］

无。

［命令模式］

执行模式。

［使用指导］

无。

［命令实例］

```
hostname# clear ad zone trust statistics
```

clear session-limit

清除会话限制规则中被丢弃会话数的统计信息。

［命令］

clear session-limit id *id* **statistics**

［句法描述］

id *id*	指定规则 ID 以删除特定会话限制规则中被丢弃的会话数统计信息。

［默认取值］

无。

［命令模式］

执行模式。

［使用指导］

无。

［命令实例］

```
hostname# clear session-limit id 1 statistics
```

交换命令

bridge priority

配置设备的桥优先级。使用该命令 no 的形式恢复设备的桥优先级为默认值。

［命令］

bridge priority *value*

no bridge priority

［句法描述］

value	指定桥优先级。*value* 的取值必须是 4096 的倍数，取值范围为 0 到 61400。

［默认取值］

32768。

［命令模式］

RSTP 配置模式。

［使用指导］

桥优先级数值越小，优先级就越高。

［命令实例］

hostname(config-stp)# **bridge priority 0**

enable

开启 RSTP 功能。使用该命令 no 的形式关闭 RSTP 功能。

［命令］

enable

no enable

［句法描述］

无。

［默认取值］

关闭。

［命令模式］

RSTP 配置模式。

［使用指导］

无。

［命令实例］

hostname(config-stp)# **enable**

---

forward-delay

配置设备的转发时延。使用该命令 no 的形式恢复设备的转发时延为默认值。

［命令］

forward-delay *value*

no forward-delay

［句法描述］

value	指定 Forward Delay 时间。*value* 的单位为秒，取值范围是 4 到 30。

［默认取值］

15 秒。

［命令模式］

RSTP 配置模式。

［使用指导］

无。

［命令实例］

hostname(config-stp)# **forward-delay 10**

---

hello

配置 hello 报文间隔。使用该命令 no 的形式恢复 hello 报文间隔为默认值。

［命令］

hello *seconds*

no hello

［句法描述］

seconds	指定 hello 报文间隔时间，单位为秒，取值范围为 1 到 10。

［默认取值］

2 秒。

［命令模式］

RSTP 配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-stp)# hello 3
```

interface vlan*id*

创建 VLAN 接口并进入 VLAN 接口配置模式。如果接口已经存在，则直接进入接口配置模式。使用该命令 no 的形式删除指定的接口。

［命令］

interface vlan*id*

［句法描述］

id	指定将要创建的 VLAN 接口的编号。范围是 1 到 223 和 256 到 4094。

［默认取值］

无默认值。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# interface vlan10
```

maximum-age

配置 BPDU 消息的生存时间。使用该命令 no 的形式恢复生存时间为默认值。

［命令］

maximum-age *value*

no maximum-age

［句法描述］

value	指定 BPDU 消息的生存时间。*value* 的单位为秒，取值范围是 6 到 40。

［默认取值］

20 秒。

［命令模式］

RSTP 配置模式。

［使用指导］

无。

［命令实例］

hostname(config-stp)# **maximum-age 10**

stp

创建 RSTP 并进入 RSTP 配置模式。如果 RSTP 已经创建则直接进入 RSTP 配置模式。使用该命令 no 的形式删除 RSTP。

［命令］

stp

no stp

［句法描述］

无。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **stp**

hostname(config-stp)#

stp cost

配置太网接口或集聚接口的 RSTP 开销。使用该命令 no 的形式恢复接口的 RSTP 开销为默认值。

［命令］

stp cost *value*

no stp cost

［句法描述］

value	指定接口的 RSTP 开销值。*value* 的取值范围为 1 到 200000000。

［默认取值］

auto，即由接口的类型（单接口或汇聚接口）、速率（10Mbps、100Mbps 或 1000Mbps）和双工状态（全双工或半双工）来决定。

［命令模式］

以太网接口或集聚接口配置模式。

［使用指导］

无。

［命令实例］

hostname(config-if-eth0/4)# **stp cost 15000**

stp enable

开启以太网接口或集聚接口的 RSTP 功能。使用该命令 no 的形式关闭接口的 RSTP 功能。

［命令］

stp enable

no stp enable

［句法描述］

无。

［默认取值］

关闭。

［命令模式］

以太网接口或集聚接口配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-if-eth0/4)# stp enable
```

stp priority

配置接口的 RSTP 优先级。使用该命令 no 的形式恢复接口的 RSTP 优先级为默认值。

［命令］

stp priority *value*

no stp priority

［句法描述］

value	指定当前接口的 RSTP 优先级，*value* 的取值必须是 16 的整数倍，取值范围为 0 到 240。

［默认取值］

128。

［命令模式］

以太网接口或集聚接口配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-if-eth0/4)# stp priority 144
```

sub-vlan

添加 sub-VLAN 到 super-VLAN。使用该命令 no 的形式将指定的 sub-VLAN 从 super-VLAN 中删除。

［命令］

subvlan *vlan-list*

no subvlan *vlan-list*

［句法描述］

vlan-list	指定将要添加的 sub-VLAN 的编号。取值范围为 1 到 4094。

［默认取值］

无。

［命令模式］

super-VLAN 配置模式。

［使用指导］

无。

［命令实例］

hostname(config-supervlan)# **subvlan 1**

---

supervlan

创建 super-VLAN，使用该命令 no 的形式删除指定的 super-VLAN。

［命令］

supervlan supervlan*X*

no supervlan supervlan*X*

［句法描述］

X	指定将要创建的 super-VLAN 的编号。不同平台 *X* 的取值范围不同。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **supervlan supervlan1**

---

switchmode

配置接口的类型和所属 VLAN。使用该命令 no 的形式取消配置。

［命令］

switchmode {**access vlan** *vlan-id* | **trunk** {**vlan** *vlan-list* [**native-vlan** *vlan-id*] | **native-vlan** *vlan-id*}}

no switchmode [**trunk** [**vlan** *vlan-list* | **native-vlan**]]

［句法描述］

access vlan *vlan-id*	配置接口类型为 Access 并指定接口所属的 VLAN 编号。
trunk vlan *vlan-list*	配置接口类型为 Trunk 并指定接口允许通过的 VLAN。
native-vlan *vlan-id*	配置接口的 Native VLAN 编号。

［默认取值］

无。

［命令模式］

以太网接口或集聚接口配置模式。

［使用指导］

所指定的 VLAN 需已经创建。

［命令实例］

hostname(config-if-eth0/2)# **switchmode trunk vlan 4 native-vlan 1**

vlan

创建 VLAN，使用该命令 no 的形式删除指定的 VLAN。

［命令］

vlan *vlan-list*

no vlan *vlan-list*

［句法描述］

vlan-list	指定将要创建的 VLAN 的编号。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **vlan 1**

```
hostname(config)# 3-5
```

路由命令

aggregate-address

创建 BGP 聚合路由。使用该命令 no 的形式取消聚合路由的指定。

［命令］

aggregate-address {*A.B.C.D/M* | *A.B.C.D A.B.C.D*} [**as-set**] [**summary-only**]

aggregate-address {*A.B.C.D/M* | *A.B.C.D A.B.C.D*}

［句法描述］

A.B.C.D/M | *A.B.C.D A.B.C.D*	指定聚合网络地址。安全网关支持两种方式，*A.B.C.D/M* 或者 *A.B.C.D A.B.C.D*，例如 1.1.1.0/24 或者 1.1.1.0 255.255.255.0。
as-set	如果指定该参数，系统会将被聚合路由的路径信息作为自己的路径信息发布给其它路由器。
summary-only	如果指定该参数，系统将只发布聚合路由。

［默认取值］

无。

［命令模式］

BGP 实例配置模式。

［使用指导］

无。

［命令实例］

hostname(config-router)# **aggregate-address 10.101.1.1 255.255.255.0 as-set**

area authentication

配置区域的认证方式。使用该命令 no 的形式取消对认证方式的指定。

［命令］

area {*id* | *A.B.C.D*} **authentication** [**message–digest**]

no area {*id* | *A.B.C.D*} **authentication**

［句法描述］

id | *A.B.C.D*	指定区域 ID。区域 ID 用 32 比特数来表示，可以是数字形式，也可以是 IP 地址形式。
message-digest	指定使用 MD5 认证方式。如果不使用该关键字，则为明文认证。

［默认取值］

无。

［命令模式］

OSPF 路由配置模式。

［使用指导］

无。

［命令实例］

hostname(config-router)# **area 1000 authentication**

area default-cost

指定区域的缺省花费。使用该命令 no 的形式恢复缺省花费的配置。

［命令］

area {*id* | *A.B.C.D*} **default-cost** *cost-value*

no area {*id* | *A.B.C.D*} **default-cost**

［句法描述］

id | *A.B.C.D*	指定区域 ID。区域 ID 用 32 比特数来表示，可以是数字形式，也可以是 IP 地址形式。
cost-value	指定花费值。范围是 0 到 16777214。

［默认取值］

cost-value - 1。

［命令模式］

OSPF 路由配置模式。

［使用指导］

无。

［命令实例］

hostname(config-router)# **area 1000 default-cost 1024**

area range

配置区域的路由聚合。使用该命令 no 的形式取消路由聚合的配置。

［命令］

area {*id* | *A.B.C.D*} **range** {*A.B.C.D/M*} [**advertise** | **not-advertise**]

no area {*id* | *A.B.C.D*} **range** {*A.B.C.D/M*} [**advertise** | **not-advertise**]

［句法描述］

id | *A.B.C.D*	指定区域 ID。区域 ID 用 32 比特数来表示，可以是数字形式，也可以是 IP 地址形式。
range {*A.B.C.D/M*}	指定被聚合的网段。
advertise	指定将这一网段的路由聚合并通告聚合后的路由。
not-advertise	指定将这一网段的路由聚合且不通告聚合后的路由。

［默认取值］

无。

［命令模式］

OSPF 路由配置模式。

［使用指导］

路由聚合功能仅对区域边界路由（连接骨干区域和非骨干区域的路由器，简称为 ABR）有效。

［命令实例］

hostname(config-router)# **area 1000 range 10.1.0.0/16 advertise**

area stub

配置 OSPF 的 stub 区域。使用该命令 no 的形式取消 stub 区域的配置。

［命令］

area {*id* | *A.B.C.D*} **stub** [**no-summary**]

no area {*id* | *A.B.C.D*} **stub** [**no-summary**]

［句法描述］

id | *A.B.C.D*	指定区域 ID。区域 ID 用 32 比特数来表示，可以是数字形式，也可以是 IP 地址形式。
no-summary	阻止 ABR 向 stub 区域发送 3 类或 4 类汇总 LSA。

［默认取值］

无。

［命令模式］

OSPF 路由配置模式。

［使用指导］

无。

［命令实例］

hostname(config-router)# **area 1000 stub**

area virtual-link

配置虚拟链路定时器参数。使用该命令 no 的形式恢复定时器的默认时间值。

［命令］

area {*id* | *A.B.C.D*} **virtual-link** *A.B.C.D* [**hello-interval** *interval-value*] [**retransmit-interval** *interval-value*] [**transmit-delay** *interval-value*] [**dead-interval** *interval-value*]

no area {*id* | *A.B.C.D*} **virtual-link** *A.B.C.D* [**hello-interval**] [**retransmit-interval**] [**transmit-delay**] [**dead-interval**]

［句法描述］

id | *A.B.C.D*	指定区域 ID。区域 ID 用 32 比特数来表示，可以是数字形式，也可以是 IP 地址形式。
virtual-link A.B.C.D	指定作为虚拟链路路由器的 Router ID。
hello-interval *interval-value*	指定接口发送 Hello 报文的时间间隔，范围是 1 到 65535 秒。
retransmit-interval *interval-value*	指定邻接路由器之间重传 LSA 的时间间隔，范围是 3 到 65535 秒。
transmit-delay *interval-value*	指定更新包的延迟时间，范围是 1 到 65536 秒。
dead-interval *interval-value*	指定失效时间值，范围是 1 到 655635 秒。

［默认取值］

hello-interval *interval-value* - 10。

retransmit-interval *interval-value* - 5。

transmit-delay *interval-value* - 1。

dead-interval *interval-value* - 40。

［命令模式］

OSPF 路由配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-router)# area 1000 virtual-link 1.1.1.1 hello-interval 60 retransmit-interval 120
```

area virtual-link authentication

配置虚拟链路的认证方式。使用该命令 no 的形式取消认证配置。

［命令］

area {*id* | *A.B.C.D*} **virtual-link** *A.B.C.D* **authentication** [**message-digest**] [**authentication-key** *string*] [**message-digest-key** *ID* **md5** *string*] [**null**]

no area {*id* | *A.B.C.D*} **virtual-link** *A.B.C.D* **authentication** [**message-digest**] [**authentication-key** *string*] [**message-digest-key** *ID*]

［句法描述］

id | *A.B.C.D*	指定区域 ID。区域 ID 用 32 比特数来表示，可以是数字形式，也可以是 IP 地址形式。
virtual-link A.B.C.D	指定作为虚拟链路路由器的 Router ID。
message-digest	指定使用 MD5 认证。
authentication-key *string*	指定明文认证的认证密码。
message-digest-key *ID* **md5** *string*	指定 MD5 认证的认证 ID 和密码。
null	不使用认证。

［默认取值］

无。

［命令模式］

OSPF 路由配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-router)# area 1000 virtual-link 1.1.1.1 authentication authentication-key yvhn5478
```

auto-cost reference-bandwidth

配置 OSPF 的引用带宽，使 OSPF 根据接口的带宽计算接口发送 OSPF 报文的花费。使用该命令 no 的形式使 OSFP 根据接口的类型计算接口发送 OSPF 报文的花费。

［命令］

auto-cost reference-bandwidth *bandwidth*

no auto-cost reference-bandwidth

［句法描述］

bandwidth	指定带宽值，单位为 Mbps，范围是 1 到 4294967。

［默认取值］

bandwidth - 100。

［命令模式］

OSPF 路由配置模式。

［使用指导］

无。

［命令实例］

hostname(config-router)# **auto-cost reference-bandwidth 1024**

bind pbr-policy

绑定 PBR 策略到接口、安全域和 Vrouter 来实现 PBR 策略的应用。使用该命令 no 的形式取消 PBR 策略在接口、安全域或 VRouter 的绑定。

［命令］

bind pbr-policy *name*

no bind pbr-policy

［句法描述］

name	PBR 策略名称。

［默认取值］

无默认值。

［命令模式］

接口配置模式、安全域配置模式或 VRouter 配置模式

［使用指导］

无。

［命令实例］

```
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# bind pbr-policy abc
```

clear ip bgp

重置 BGP 连接。

［命令］

clear ip bgp {***** | *A.B.C.D* | **external** | **peer-group** *peer-group-name* | *number*} [**vrouter** *vrouter-name*]

［句法描述］

*****	重置当前所有 BGP 会话连接。
A.B.C.D	重置指定对等体的 BGP 连接。
external	重置所有 EBGP 连接。
peer-group *peer-group-name*	重置指定 BGP 对等体组的连接。
number	重置指定自治系统中的 BGP 连接。
vrouter *vrouter-name*	指定需重置连接所在的 VRouter。

［默认取值］

无默认值。

［命令模式］

执行模式。

［使用指导］

无。

［命令实例］

```
hostname# clear ip bgp external
```

default-information originate

指定将默认路由发布到其它使用 RIP 协议的路由器。使用该命令 no 的形式不发送默认路由。

［命令］

default-information originate

no default-information originate

［句法描述］

无。

［默认取值］

无。

［命令模式］

RIP 路由配置模式。

［使用指导］

无。

［命令实例］

hostname(config-router)# **default-information originate**

---

default-information originate

指定将默认路由发布到其它使用 OSPF 协议的路由器。使用该命令 no 的形式不发送默认路由。

［命令］

default-information originate [**always**] [**type** { 1 | 2 }] [**metric** *value*]

no default-information originate

［句法描述］

always	OSPF 无条件产生并发送默认路由。
type { 1 | 2 }	指定与发送到 OSPF 路由域的默认路由相关联的外部路由的类型。**1** 指 type1 外部路由，**2** 指 type2 外部路由。
metric *value*	指定发送默认路由的度量。如果不使用该命令配置度量并且也没有使用 **default-metric** *value* 配置默认度量，其默认度量将会是 20。范围是 0 到 16777214。

［默认取值］

无。

［命令模式］

OSPF 路由配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-router)# default-information originate always type
1
```

default-metric

指定 RIP 或 OSPF 的缺省度量值。使用该命令 no 的形式恢复缺省度量的默认值。

［命令］

default-metric *value*

no default-metric

［句法描述］

value	指定缺省度量值。对于 RIP，取值范围是 1 到 15；对于 OSPF，取值范围是 0 到 16777214。

［默认取值］

1。

［命令模式］

RIP 路由配置模式或 OSPF 路由配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-router)# default-metric 15
```

default-metric（BGP）

指定 BGP 的缺省度量值。使用该命令 no 的形式恢复默认情况。

［命令］

default-metric *value*

no default-metric

［句法描述］

value	指定缺省度量值。范围是 1 到 4294967295。

［默认取值］

无。

［命令模式］

引入的直连路由的度量为 0。

［使用指导］

无。

［命令实例］

hostname(config-router)# **default-metric 15**

description

为 PBR 策略规则添加描述。

［命令］

description *string*

no description

［句法描述］

string	指定规则描述字符串，长度为 1 到 255 个字符的字符串。

［默认取值］

无。

［命令模式］

PBR 规则配置模式。

［使用指导］

无。

［命令实例］

hostname(config-pbr-match)# **description internal**

disable

禁用 PBR 策略规则。

［命令］

disable

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

PBR 规则配置模式。

［使用指导］

默认情况下，配置好的 PBR 策略规则会在系统中立即起效。用户可以通过命令禁用某条策略规则，使其不对流量进行控制。

［命令实例］

```
hostname(config-pbr-match)# disable
```

distance（BGP）

为从 BGP 对等体获得的 BGP 路由以及本地 BGP 路由指定管理距离。使用该命令 no 的形式恢复默认 BGP 路由管理距离。

［命令］

distance *ebgp-distance ibgp-distance local-distance*

no distance

［句法描述］

ebgp-distance	指定 EBGP 路由管理距离。取值范围是 1 到 255。
ibgp-distance	指定 IBGP 路由管理距离。取值范围是 1 到 255。
local-distance	指定本地路由管理距离。取值范围是 1 到 255。

［默认取值］

ebgp-distance - 20。

ibgp-distance - 200。

local-distance - 200。

［命令模式］

BGP 实例配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-router)# distance 30 100 150
```

distance

指定 RIP 路由或 OSPF 路由的缺省距离。使用该命令 no 的形式恢复缺省距离。

［命令］

distance *distance-value*

no distance

［句法描述］

distance-value	指定缺省距离。取值范围是 1 到 255。

［默认取值］

120（RIP）。

110（OSPF）。

［命令模式］

RIP 路由配置模式或 OSPF 路由配置模式。

［使用指导］

无。

［命令实例］

hostname(config-router)# **distance 255**

distance

为从一些指定网络得到的路由指定管理距离。使用该命令 no 的形式删除指定的距离。

［命令］

distance *distance-value ip-address/netmask*

no distance *ip-address/netmask*

［句法描述］

distance-value	指定管理距离。取值范围是 1 到 255。
ip-address/netmask	指定网络地址。安全网关支持两种方式，*A.B.C.D/M* 或者 *A.B.C.D A.B.C.D*。

［默认取值］

无。

［命令模式］

RIP 路由配置模式。

［使用指导］

用该命令指定的距离优先级高于通过 **distance** distance-*value* 指定的 RIP 路由缺省距离。

［命令实例］

hostname(config-router)# **distance 255 10.0.0.0/8**

---

distance ospf

根据路由类型指定管理距离。使用该命令 no 的形式恢复距离的默认值。

［命令］

distance ospf {**intra-area** *distance-value* | **inter-area** *distance-value* | **external** *distance-value*}

no distance ospf

［句法描述］

intra-area *distance-value*	指定区域内路由的管理距离。默认值是 110。范围是 1 到 255。
inter-area *distance-value*	指定区域间路由的管理距离。默认值是 110。范围是 1 到 255。
external *distance-value*	指定外部 type5 类型路由的管理距离。默认值是 110。范围是 1 到 255。

［默认取值］

intra-area *distance-value* - 110。

inter-area *distance-value* - 110。

external *distance-value* - 110。

［命令模式］

OSPF 路由配置模式。

［使用指导］

无。

［命令实例］

hostname(config-router)# **distance ospf external 8**

---

dst-addr

添加地址簿条目类型目的地址。使用该命令 no 的形式为规则删除指定的目的地址。

［命令］

dst-addr *dst-addr*

no dst-addr *dst-addr*

［句法描述］

dst-addr	规则的地址簿条目类型目的地址。

［默认取值］

无默认值。

［命令模式］

PBR 规则配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-pbr)# match id 3
hostname(config-pbr-match)# dst-addr addr1
```

dst-host

添加主机成员类型目的地址。使用该命令 no 的形式为规则删除主机成员类型目的地址。

［命令］

dst-host *host-name*

no dst-addr *host-name*

［句法描述］

host-name	主机名称。

［默认取值］

无默认值。

［命令模式］

PBR 规则配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-pbr)# match id 3
hostname(config-pbr-match)# dst-host host1
```

dst-ip

添加 IP 成员类型目的地址。使用该命令 no 的形式为规则删除 IP 成员类型的目的地址。

［命令］

dst-ip *ip/netmask*

no dst-ip *ip/netmask*

［句法描述］

ip/netmask	IP 地址/子网掩码

［默认取值］

无默认值。

［命令模式］

PBR 规则配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-pbr)# match id 3
hostname(config-pbr-match)# dst-ip 10.1.1.2/24
```

dst-range

添加 IP 地址范围类型目的地址。使用该命令 no 的形式为规则删除 IP 地址范围类型的目的地址。

［命令］

dst-range *min-ip* [*max-ip*]

no dst-range *min-ip* [*max-ip*]

［句法描述］

min-ip	IP 地址范围的最小值。
max-ip	IP 地址范围的最大值。

［默认取值］

无默认值。

［命令模式］

PBR 规则配置模式。

［使用指导］

添加了 IP 地址段作为目的地址后，只能全部删除该地址段，不能部分删除。如：添加了 1.1.1.1 到 1.1.1.6 地址段的 IP 地址范围时，不能使用 no 命令删除 1.1.1.2 到 1.1.1.4 地址段的 IP 地址范围，只能全部删除。

［命令实例］

```
hostname(config-pbr)# match id 3
hostname(config-pbr-match)# dst-range 10.3.4.5 10.3.4.36
hostname(config-pbr-match)# no dst-range 10.3.4.5 10.3.4.36
```

ecmp enable

配置 ECMP 功能。

［命令］

ecmp enable *ecmp-route-num*

［句法描述］

ecmp-route-num	系统允许的最大 ECMP 路由条目数。取值范围为 1 到 40。当取值为 1 时表示不使用 ECMP 功能。

［默认取值］

最多允许 40 条 ECMP 路由条目。

［命令模式］

VRouter 配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ecmp enable 4
```

ecmp-route-select

配置 ECMP 选路方式。

［命令］

ecmp-route-select {by-5-tuple | by-src | by-src-and-dst}

［句法描述］

by-5-tuple	基于五元组（源 IP 地址、目的 IP 地址、源端口、目的端口和服务类型）进行选路。
by-src	基于源 IP 地址进行选路。
by-src-and-dst	基于源 IP 地址和目的 IP 地址进行选路。该方式为系统默认选路方式。

［默认取值］

by-src-and-dst。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **ecmp-route-select by-5-tuple**

eif

指定组播数据的出接口。

［命令］

eif *interface-name*

［句法描述］

interface-name	指定出接口名称。

［默认取值］

无。

［命令模式］

静态组播路由配置模式。

［使用指导］

用户可以通过多次执行该命令，最多指定 32 个出接口。

［命令实例］

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip multicast-routing
hostname(config-vrouter)# ip mroute 1.1.1.2 224.91.91.2
hostname(config-mrt)# eif ethernet0/1
```

---

enable

启用 PBR 策略规则。

［命令］

enable

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

PBR 规则配置模式。

［使用指导］

默认情况下，配置好的策略规则会在系统中立即起效。

［命令实例］

```
hostname(config-pbr)# match id 1
hostname(config-pbr-match)# enable
```

---

exec isp-network clear-predefine

删除已上传的预定义 ISP 配置文件。

［命令］

exec isp-network clear-predefine

［句法描述］

无。

［默认取值］

无。

［命令模式］

执行模式。

［使用指导］

执行该命令后，重启系统，系统将恢复使用原有的预定义 ISP 配置文件（出厂时系统自带的预定义 ISP 配置文件）。

［命令实例］

```
hostname# exec isp-network clear-predefine
```

iif

指定组播数据的入接口。

［命令］

iif *interface-name*

［句法描述］

interface-name	指定入接口名称。

［默认取值］

无。

［命令模式］

静态组播路由配置模式。

［使用指导］

用户可以通过多次执行该命令，最多指定 2 个入接口。

［命令实例］

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip multicast-routing
hostname(config-vrouter)# ip mroute 1.1.1.2 224.91.91.2
hostname(config-mrt)# iif ethernet0/0
```

import vrouter

引入 VRouter 路由。

［命令］

import vrouter *vrouter-name* {**connected** | **static** | **rip** | **ospf** | **bgp**}

［句法描述］

vrouter-name	指定被引入路由所属的 VRouter。
connected | **static** | **rip** | **ospf** | **bgp**	指定被引入路由的类型。

［默认取值］

无。

［命令模式］

VRouter 配置模式。

［使用指导］

多次配置该命令引入多种类型路由。

［命令实例］

hostname(config)# **ip vrouter trust-vr**

hostname(config-vrouter)# **import vrouter trust-vr rip**

ip igmp-proxy enable

开启 IGMP Proxy 功能。使用该命令 no 的形式关闭 IGMP Proxy 功能。

［命令］

ip igmp-proxy enable

no ip igmp-proxy enable

［句法描述］

无。

［默认取值］

禁用。

［命令模式］

VRouter 配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip igmp-proxy enable
```

ip igmp-proxy {router-mode | host-mode}

配置接口的 IGMP 代理模式，使它处于主机模式或路由器模式。使用该命令 no 的形式取消指定接口的 IGMP 代理模式。

［命令］

ip igmp-proxy {**router-mode** | **host-mode**} [*A.B.C.D*]

no ip igmp-proxy {**router-mode** | **host-mode**} [*A.B.C.D*]

［句法描述］

router-mode	配置下行接口的 IGMP 代理模式为路由器模式。
host-mode	配置上行接口的 IGMP 代理模式为主机模式。
A.B.C.D	指定组播组地址。配置组播地址后，系统认为 IGMP 代理模式仅对此组播地址有效。

［默认取值］

无。

［命令模式］

接口配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# ip igmp-proxy host-mode
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# ip igmp-proxy router-mode
hostname(config-if-eth0/1)# exit
```

ip igmp-snooping enable

开启 IGMP Snooping 功能。使用该命令 no 的形式禁用 IGMP Snooping 功能。

［命令］

ip igmp-snooping enable

no ip igmp-snooping enable

［句法描述］

无。

［默认取值］

禁用。

［命令模式］

VSwitch 配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# vswitch vswitch1
hostname(config-vswitch)# ip igmp-snooping enable
```

---

ip igmp-snooping {router-mode | host-mode | auto | disable}

配置接口的 IGMP Snooping 功能。使用该命令 no 的形式取消配置该接口的 IGMP Snooping 功能。

［命令］

ip igmp-snooping {**router-mode** [*A.B.C.D*] | **host-mode** [*A.B.C.D*] | **disable** | **auto**}

no ip igmp-snooping {**router-mode** *A.B.C.D* | **host-mode** *A.B.C.D*}

［句法描述］

router-mode	配置下行接口的 IGMP Snooping 模式为路由器模式。
host-mode	配置上行接口的 IGMP Snooping 模式为主机模式。
A.B.C.D	指定组播组地址。
disable	禁用接口的 IGMP Snooping 功能。
auto	指定该参数，系统通过 IGMP 报文自动确定接口的模式。

［默认取值］

无。

［命令模式］

接口配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# ip igmp-snooping host-mode
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# ip igmp-snooping router-mode
hostname(config-if-eth0/1)# exit
```

ip multicast-routing

开启组播路由功能。使用该命令 no 的形式关闭组播路由功能。

［命令］

```
ip multicast-routing
no ip multicast-routing
```

［句法描述］

无。

［默认取值］

关闭。

［命令模式］

VRouter 配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip multicast-routing
```

ip mroute

创建静态组播路由条目。使用该命令 no 的形式删除指定的静态组播路由条目。

［命令］

ip mroute *A.B.C.D A.B.C.D* [**iif** *interface-name*] [**eif** *interface-name*]

no ip mroute *A.B.C.D A.B.C.D* [**iif** *interface-name*] [**eif** *interface-name*]

［句法描述］

A.B.C.D A.B.C.D	指定组播源和组播地址。第一个 A.B.C.D 为组播源 IP 地址；第二个 A.B.C.D 为组播地址，其地址范围是 224.0.0.0 至 239.255.255.255 之间。
iif *interface-name*	指定入接口名称。在此命令中，最多允许用户指定 2 个入接口名称。
eif *interface-name*	指定出接口名称。在此命令中，最多允许用户指定 4 个出接口名称。

［默认取值］

无。

［命令模式］

VRouter 配置模式。

［使用指导］

无。

［命令实例］

hostname(config-vrouter)# **ip mroute 1.1.1.2 224.91.91.2 iif ethernet0/0 eif ethernet0/1**

ip ospf authentication

开启接口的 OSPF 认证功能。使用该命令 no 的形式关闭接口的 OSPF 认证功能。

［命令］

ip ospf authentication

no ip ospf authentication

［句法描述］

无。

［默认取值］

默认情况下，接口的 OSFP 认证是关闭的。

［命令模式］

接口配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# ip ospf authentication
```

ip ospf authentication-key

配置接口 OSPF 认证采用明文的认证密码。使用该命令 no 的形式取消密码配置。

［命令］

ip ospf authentication-key *string*

no ip ospf authentication-key

［句法描述］

string	指定认证密码（最多为 8 个字符）。

［默认取值］

无。

［命令模式］

接口配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# ip ospf authentication-key fgeriq45
```

ip ospf cost

指定接口的链路花费。使用该命令 no 的形式取消对所需花费的指定。

［命令］

ip ospf cost *cost-value* [**local**]

no ip ospf cost

［句法描述］

cost-value	指定接口的链路花费。取值范围是 1 到 65535。
local	指定接口的链路花费为 local。当设备处于 HA AA 模式时，配置此参数，该接口的链路花费值将不会同步到备份设备，从而使两台设备具有不同的链路花费值，避免出现非对称 OSPF 路由。

［默认取值］

无。

［命令模式］

接口配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# ip ospf cost 10
```

ip ospf dead-interval

指定接口的相邻路由失效时间。使用该命令 no 的形式恢复默认失效时间。

［命令］

ip ospf dead-interval *interval*

no ip ospf dead-interval

［句法描述］

interval	指定接口的相邻路由失效时间。范围是 1 到 65535 秒。

［默认取值］

interval – 40 秒。

［命令模式］

接口配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# ip ospf dead-interval 60
```

ip ospf hello-interval

指定接口发送 Hello 包的时间间隔。使用该命令 no 的形式恢复默认时间间隔。

［命令］

ip ospf hello-interval *interval*

no ip ospf hello-interval

［句法描述］

interval	指定接口发送 Hello 包的时间间隔。范围是 1 到 65535 秒。

［默认取值］

interval – 10 秒。

［命令模式］

接口配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# ip ospf hello-interval 20
```

ip ospf message-digest-key

配置接口 OSPF 认证采用 MD5 的认证 ID 和密码。使用该命令 no 的形式取消密码配置。

［命令］

ip ospf message-digest-key *ID* **md5** *string*

no ip ospf message-digest-key *ID*

［句法描述］

ID	指定认证 ID。
string	指定认证密码。

［默认取值］

无。

［命令模式］

接口配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# ip ospf message-digest-key 10 md5
B5E9B60AE90C
```

ip ospf priority

指定接口路由器的优先级。使用该命令 no 的形式恢复默认优先级。

［命令］

ip ospf priority *level*

no ip ospf priority

［句法描述］

level	指定路由器的优先级。范围是 0 到 255。

［默认取值］

level – 1。

［命令模式］

接口配置模式。

［使用指导］

优先级为 0 的路由器不会被选中作为指定路由器。当同一个网络的两个路由器都可作为指定路由器时，优先级高的路由器会被选中；如果优先级也相同，Router ID 高的会被选中。

［命令实例］

```
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# ip ospf priority 3
```

ip ospf retransmit-interval

指定接口重传 LSA 的时间间隔。使用该命令 no 的形式恢复默认时间间隔。

［命令］

ip ospf retransmit-interval *interval*

no ip ospf retransmit-interval

［句法描述］

interval	指定接口重传 LSA 的时间间隔。范围是 1 到 65535 秒。

［默认取值］

interval — 5 秒。

［命令模式］

接口配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **interface ethernet0/2**

hostname(config-if-eth0/2)# **ip ospf retransmit-interval 10**

ip ospf transmit-delay

指定接口更新包的延迟时间。使用该命令 no 的形式恢复默认延迟时间。

［命令］

ip ospf transmit-delay *interval*

no ip ospf transmit-dealy

［句法描述］

interval	指定接口更新包的延迟时间。范围是 1 到 65535 秒。

［默认取值］

interval — 1 秒。

［命令模式］

接口配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **interface ethernet0/2**

hostname(config-if-eth0/2)# **ip ospf transmit-delay 10**

ip rip authentication mode

配置 RIP 报文的认证方式。使用该命令 no 的形式取消对认证方式的指定。

［命令］

ip rip authentication mode {md5 | text}

no ip rip authentication mode

［句法描述］

md5	指定为 MD5 密文认证方式。
text	指定为明文认证方式。

［默认取值］

text 明文认证方式。

［命令模式］

接口配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# ip rip authentication mode md5
```

ip rip authentication string

配置 RIP 报文的认证码。使用该命令 no 的形式取消对认证码的指定。

［命令］

ip rip authentication string *string*

no ip rip authentication string

［句法描述］

string	指定认证码。

［默认取值］

无。

［命令模式］

接口配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# ip rip authentication string
gfdhauk8547
```

ip rip receive version

指定接口接收 RIP 信息的版本号。使用该命令 no 的形式恢复默认版本号。

［命令］

ip rip receive version [1] [2]

no ip rip receive version

［句法描述］

1	指定只接收 RIP-1 的 RIP 信息。
2	指定只接收 RIP-2 的 RIP 信息。

［默认取值］

2。

［命令模式］

接口配置模式。

［使用指导］

使用 **ip rip receive version 1 2** 命令指定接口接受 RIP-1 和 RIP-2 的信息。

［命令实例］

```
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# ip rip receive version 1
```

ip rip send version

指定接口发送 RIP 信息的版本号。使用该命令 no 的形式恢复默认版本号。

［命令］

ip rip send version [1] [2]

no ip rip send version

［句法描述］

1	指定只发送 RIP-1 的 RIP 信息。
2	指定只发送 RIP-2 的 RIP 信息。

［默认取值］

2。

［命令模式］

接口配置模式。

［使用指导］

使用 **ip rip send version 1 2** 命令指定接口发送 RIP-1 和 RIP-2 的信息。

［命令实例］

```
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# ip rip send version 1
```

ip rip split-horizon

开启水平分割功能。使用该命令 no 的形式关闭水平分割功能。

［命令］

```
ip rip split-horizon
no ip rip split-horizon
```

［句法描述］

无。

［默认取值］

无。

［命令模式］

接口配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# ip rip split-horizon
```

ip route

添加目的路由条目。使用该命令 no 的形式删除指定的静态路由条目。

［命令］

ip route {*A.B.C.D/M* | *A.B.C.D A.B.C.D*} {*A.B.C.D* | *interface-name* [*A.B.C.D*] | **vrouter** *vrouter-name*} [*distance-value*] [**weight** *weight-value*]

no ip route {*A.B.C.D/M* | *A.B.C.D A.B.C.D*} {*A.B.C.D* | *interface-name*}

［句法描述］

A.B.C.D/M | *A.B.C.D A.B.C.D*	指定目的地址。
A.B.C.D | *interface-name* [*A.B.C.D*] | **vrouter** *vrouter-name*	指定下一跳。可以是网关地址（*A.B.C.D*）、接口（*interface-name*）或者 VRouter（**vrouter** *vrouter-name*）。当下一跳为接口时，用户可以选择隧道接口名称（当为多隧道接口时，用户必须使用 *A.B.C.D* 参数指定 IPSec VPN、GRE 或者 SCVPN 隧道的下一跳 IP 地址，并且此地址必须和该隧道接口绑定的相应隧道的下一跳 IP 地址相同）、Null0 接口或者 PPPoE 接口。
distance-value	指定路由的管理距离大小。
weight *weight-value*	指定路由权值的大小。路由权值决定负载均衡中流量转发的比重。范围是 1 到 255。

［默认取值］

distance-value – 1。

weight-value – 1。

［命令模式］

VRouter 配置模式。

［使用指导］

- 安全网关支持两种地址方式，*A.B.C.D/M* 或者 *A.B.C.D A.B.C.D*，例如 1.1.1.0/24 或者 1.1.1.0 255.255.255.0。
- *distance-value* 设定路由的优先级，取值越小，优先级越高，而在有多条路由选择的时候，优先级高的路由会被优先使用。取值范围是 1 到 255，当路由距离为 255 时，该路由无效。
- 使用多条该命令添加多条静态路由条目。

［命令实例］

hostname(config-vrouter)# **ip route 10.110.88.0/24 192.168.1.3**

ip route *isp-name*

添加 ISP 路由条目。使用该命令 no 的形式删除指定的 ISP 路由条目。

［命令］

ip route *isp-name* {*A.B.C.D* | *interface-name* | **vrouter** *vrouter-name*} [*distance-value*] [**weight** *weight-value*]

no ip route *isp-name* {*A.B.C.D* | *interface-name* | **vrouter** *vrouter-name* } [*distance-value*] [**weight** *weight-value*]

［句法描述］

isp-name	指定系统中已存在的 ISP 名称作为路由的目的地址。
A.B.C.D | *interface-name* | **vrouter** *vrouter-name*	指定下一跳。可以是网关地址（*A.B.C.D*）、接口（*interface-name*）或者 VRouter（**vrouter** *vrouter-name*）。
distance-value	指定路由的管理距离大小。该参数设定路由的优先级，取值越小，优先级越高，而在有多条路由选择的时候，优先级高的路由会被优先使用。取值范围是 1 到 255。当路由距离为 255 时，该路由无效。
weight-value	指定路由权值的大小。路由权值决定负载均衡中流量转发的比重。范围是 1 到 255。

［默认取值］

distance-value – 1。

weight-value – 1。

［命令模式］

VRouter 配置模式。

［使用指导］

使用多条该命令添加多条 ISP 路由条目。

［命令实例］

hostname(config)# **ip vrouter trust-vr**

hostname(config-vrouter)# **ip route isp1 10.101.0.1**

ip route source

添加源路由条目。使用该命令 no 的形式删除指定的源路由条目。

［命令］

ip route source {*A.B.C.D/M* | *A.B.C.D A.B.C.D*} {*A.B.C.D* | *interface-name* | **vrouter** *vrouter-name* } [*distance-value*] [**weight** *weight-value*]

no ip route source {*A.B.C.D/M* | *A.B.C.D A.B.C.D*} {*A.B.C.D* | *interface-name*}

［句法描述］

A.B.C.D/M | *A.B.C.D A.B.C.D*	指定源路由条目的网络地址。
A.B.C.D | *interface-name* | **vrouter** *vrouter-name*	指定下一跳。可以是网关地址（*A.B.C.D*）、接口（*interface-name*）或者 VRouter（**vrouter** *vrouter-name*）。当下一跳为接口时，用户可以选择隧道接口、Null0 接口或者 PPPoE 接口。
distance-value	指定路由的管理距离大小。
weight *weight-value*	指定路由权值的大小。路由权值决定负载均衡中流量转发的比重。范围是 1 到 255。

［默认取值］

distance-value – 1。

weight-value – 1。

［命令模式］

VRouter 配置模式。

［使用指导］

- 安全网关支持两种地址方式，*A.B.C.D/M* 或者 *A.B.C.D A.B.C.D*，例如 1.1.1.0/24 或者 1.1.1.0 255.255.255.0。
- *distance-value* 设定路由的优先级，取值越小，优先级越高，而在有多条路由选择的时候，优先级高的路由会被优先使用。取值范围是 1 到 255，当路由距离为 255 时，该路由无效。

［命令实例］

hostname(config-vrouter)# **ip route source 10.110.88.0/24 192.168.1.3**

ip route source in-interface

添加源接口路由条目。使用该命令 no 的形式删除指定的源接口路由条目。

［命令］

ip route source in-interface *interface-name* {*A.B.C.D/M* | *A.B.C.D A.B.C.D*} {*A.B.C.D* | *interface-name* | **vrouter** *vrouter-name* } [*distance-value*] [**weight** *weight-value*]

no ip route source in-interface *interface-name* {*A.B.C.D/M* | *A.B.C.D A.B.C.D*} {*A.B.C.D* | *interface-name* | **vrouter** *vrouter-name* }

［句法描述］

interface-name	指定路由条目的入接口。
A.B.C.D/M | *A.B.C.D A.B.C.D*	指定路由条目的网络地址。
A.B.C.D | *interface-name* | **vrouter** *vrouter-name*	指定下一跳。可以是网关地址（*A.B.C.D*）、接口（*interface-name*）或者 VRouter（**vrouter** *vrouter-name*）。当下一跳为接口时，用户可以选择隧道接口名称，也可以选择 Null0 接口（黑洞路由）。
distance-value	指定路由的管理距离大小。
weight *weight-value*	指定路由权值的大小。路由权值决定负载均衡中流量转发的比重。范围是 1 到 255。

［默认取值］

distance-value – 1。

weight-value – 1。

［命令模式］

VRouter 配置模式。

［使用指导］

- 安全网关支持两种地址方式，*A.B.C.D/M* 或者 *A.B.C.D A.B.C.D*，例如 1.1.1.0/24 或者 1.1.1.0 255.255.255.0。
- *distance-value* 设定路由的优先级，取值越小，优先级越高，而在有多条路由选择的时候，优先级高的路由会被优先使用。取值范围是 1 到 255，当路由距离为 255 时，该路由无效。

［命令实例］

hostname(config-vrouter)# **ip route source 10.110.88.0/24 192.168.1.3**

ip vrouter

进入 VRouter 配置模式。

［命令］

ip vrouter *vrouter-name*

［句法描述］

vrouter-name	指定 VRouter 的名称。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)#
```

isp-network

创建 ISP 名称。执行该命令后，系统创建指定的 ISP 名称，并且进入 ISP 信息配置模式；如果指定的名称已存在，则直接进入 ISP 信息配置模式。使用该命令 no 的形式删除指定名称的 ISP。

［命令］

isp-network *isp-name*

no isp-network *isp-name*

［句法描述］

isp-name	指定 ISP 名称。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# isp-network isp1
hostname(config-isp)#
```

match

创建一条 PBR 规则。使用该命令 no 的形式删除指定 ID 的规则。

［命令］

match [**id** *rule-id*] [**before** *rule-id* | **after** *rule-id* | **top**] *src-addr dst-addr service-name* **next-hop** {*interface-name* | *A.B.C.D* | **vrouter** *vrouter-name*}

no match id *rule-id*

［句法描述］

id *rule-id*	为规则指定一个 ID 号。如果不指定，系统将会为策略规则自动分配一个 ID。
before *rule-id*	为规则指定相对排列顺序：位于某规则之前。
after *rule-id*	为规则指定相对排列顺序：位于某规则之后。
top	为规则指定绝对排列顺序：top 为首位。
src-addr	指定源地址，该地址为地址簿条目。
dst-addr	指定目的地址，该地址为地址簿条目。
service-name	指定服务名称。*service-name* 为服务簿中定义的服务。
next-hop {*interface-name* | *A.B.C.D* | **vrouter** *vrouter-name* }	指定下一跳。*interface-name* 为出接口的名称，*A.B.C.D* 为下一跳的 IP 地址，**vrouter** *vrouter-name* 为 VRouter。

［默认取值］

无。

［命令模式］

PBR 策略配置模式。

［使用指导］

本命令一次性完成 PBR 规则参数配置。用户也可以通过 **match id** 命令先创建 PBR 规则并进入 PBR 规则配置进而完成源地址、目的地址、下一条等规则参数的添加操作。具体请参见 PBR 规则配置模式下的相关命令。

［命令实例］

```
hostname(config)# pbr-policy abc
hostname(config-pbr)# match id 1 sb db srv1 nexthop ethernet0/5
```

match id

进入指定 PBR 规则的 PBR 规则配置模式，用户可以在该模式下修改该规则的各参数值。使用该命令 no 的形式可以删除该规则。

［命令］

match [**id** rule-*id*] [**before** *rule-id* | **after** *rule-id* | **top**]（该命令适用于 PBR 规则 ID 不存在的情况）

match id *rule-id*（该命令适用于规则 ID 已存在的情况，并且用该命令 no 的形式，可以删除该条规则，即 **no match id** *rule-id*）

no match id *rule-id*

［句法描述］

id *rule-id*	为规则指定一个 ID 号。
before *rule-id*	指定规则的位置为当前 PBR 策略某个规则之前。
after *rule-id*	指定规则的位置为当前 PBR 策略某个规则之前。
top	指定规则的位置为当前 PBR 策略所有规则的首位。

［默认取值］

无。

［命令模式］

PBR 策略配置模式。

［使用指导］

规则 ID 在特定的 PBR 策略中应是唯一的。

［命令实例］

```
hostname(config)# pbr-policy abc
hostname(config-pbr)# match id 2 before 1
 Match id 2 is created.
hostname(config-pbr-match)#
```

max-route

指定 VRouter 允许的最大路由条目数（包含 VRouter 下的所有直连路由、静态路由和各种动态路由）。使用该命令 no 的形式取消最大路由条目数的指定。

［命令］

max-routes *number*

no max-routes

［句法描述］

number	指定最大路由条目数。范围是 1 到 100000。

［默认取值］

无。

［命令模式］

VRouter 配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# ip vrouter vrouter1
hostname(config-vrouter)# max-routes 50000
```

move

移动指定规则在 PBR 策略中的位置从而改变规则的排列顺序（即为规则匹配顺序）。

［命令］

move *rule-id* {**top** | **bottom** | **before** *rule-id* | **after** *rule-id*}

［句法描述］

rule-id	指定要移动的规则的 ID 号。
top | **bottom**	为规则指定绝对排列顺序：top 为首位，bottom 为末位。
before *id*	为规则指定相对排列顺序：位于某规则之前。
after *id*	为规则指定相对排列顺序：位于某规则之后。

［默认取值］

无。

［命令模式］

策略配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-pbr)# move 1 top
```

neighbor（BGP）

创建 BGP 对等体组。使用该命令 no 的形式删除指定的 BGP 对等组。

［命令］

neighbor *peer-group-name* **peer-group**

no neighbor *peer-group-name* **peer-group**

［句法描述］

peer-group-name	指定将要创建的对等体组的名称。

［默认取值］

无。

［命令模式］

BGP 实例配置模式。

［使用指导］

无。

［命令实例］

hostname(config-router)# **neighbor peer1 peer-group**

neighbor A.B.C.D peer-group

添加 BGP 对等体到对等体组。使用该命令 no 的形式将 BGP 对等体从对等体组中删除。

［命令］

neighbor *A.B.C.D* **peer-group** *peer-group-name*

no neighbor *A.B.C.D* **peer-group** *peer-group-name*

［句法描述］

A.B.C.D	指定将要添加的 BGP 对等体的 IP 地址。
peer-group-name	指定系统中已创建的对等体组的名称。

［默认取值］

无。

［命令模式］

BGP 实例配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-router)# neighbor 1.1.1.1 peer-group peer1
```

neighbor {A.B.C.D | peer-group} activate

激活 BGP 连接。使用该命令 no 的形式关闭指定对等体或者对等体组的 BGP 连接。

［命令］

neighbor {*A.B.C.D* | *peer-group*} **activate**

no neighbor {*A.B.C.D* | *peer-group*} **activate**

［句法描述］

A.B.C.D | *peer-group*	指定对等体 IP 地址或者对等体组的名称。

［默认取值］

无。

［命令模式］

BGP 实例配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-router)# neighbor 192.168.1.1 activate
```

neighbor {A.B.C.D | peer-group} default-originate

配置缺省信息发布，即指定当前设备是否将默认路由发布到其它 BGP 对等体或者对等体组。使用该命令 no 的形式关闭取消缺省信息发布。

［命令］

neighbor {*A.B.C.D* | *peer-group*} **default-originate**

no neighbor {*A.B.C.D* | *peer-group*} **default-originate**

［句法描述］

A.B.C.D | *peer-group*	指定对等体 IP 地址或者对等体组的名称。

［默认取值］

无。

［命令模式］

BGP 实例配置模式。

［使用指导］

无。

［命令实例］

hostname(config-router)# **neighbor 192.168.1.1 default-originate**

neighbor {A.B.C.D | peer-group} description

为对等体或者对等体组配置描述信息。使用该命令 no 的形式取消对等体或者对等体组的描述信息配置。

［命令］

neighbor {*A.B.C.D* | *peer-group*} **description** *description*

no neighbor {*A.B.C.D* | *peer-group*} **description**

［句法描述］

A.B.C.D | *peer-group*	指定对等体 IP 地址或者对等体组的名称。
description	指定描述信息。范围是 1 到 80 个字符。

［默认取值］

无。

［命令模式］

BGP 实例配置模式。

［使用指导］

无。

［命令实例］

hostname(config-router)# **neighbor 192.168.1.1 description test**

neighbor {A.B.C.D | peer-group} next-hop-self

配置下一跳路由为自身。配置该功能后，路由器将通告对等体或者对等体组 BGP 路由的下一跳为该路由器自身。使用该命令 no 的形式取消取消下一跳为自身的指定。

［命令］

neighbor {*A.B.C.D* | *peer-group*} **next-hop-self**

no neighbor {*A.B.C.D* | *peer-group*} **next-hop-self**

［句法描述］

A.B.C.D | *peer-group*	指定对等体 IP 地址或者对等体组的名称。

［默认取值］

无。

［命令模式］

BGP 实例配置模式。

［使用指导］

无。

［命令实例］

hostname(config-router)# **neighbor 192.168.1.1 next-hop-self**

neighbor {A.B.C.D | peer-group} remote-as

配置 BGP 对等体（对等体组）进行 BGP 路由信息交换。使用该命令 no 的形式取消 BGP 对等体或者对等体组的指定。

［命令］

neighbor {*A.B.C.D* | *peer-group*} **remote-as** *number*

no neighbor {*A.B.C.D* | *peer-group*} **remote-as**

［句法描述］

A.B.C.D | *peer-group*	指定对等体 IP 地址或者对等体组的名称。
number	指定所配置对等体或者对等体组所在的自治区域的编号。

［默认取值］

无。

［命令模式］

BGP 实例配置模式。

［使用指导］

无。

［命令实例］

hostname(config-router)# **neighbor 1.1.1.1 remote-as 20**

neighbor {A.B.C.D | peer-group} shutdown

关闭指定的对等体或者对等体组。使用该命令 no 的形式开启对等体或者对等体组。

［命令］

neighbor {*A.B.C.D* | *peer-group*} **shutdown**

no neighbor {*A.B.C.D* | *peer-group*} **shutdown**

［句法描述］

A.B.C.D | *peer-group*	指定对等体 IP 地址或者对等体组的名称。

［默认取值］

无。

［命令模式］

BGP 实例配置模式。

［使用指导］

无。

［命令实例］

hostname(config-router)# **neighbor 1.1.1.1 shutdown**

neighbor {A.B.C.D | peer-group} timers

为某个特定的 BGP 对等体或者对等体组指定不同的定时器数值。使用该命令 no 的形式取消对 BGP 对等体或对等体组定时器的指定。

［命令］

neighbor {*A.B.C.D* | *peer-group*} **timers** *keepalive holddown*

no neighbor {*A.B.C.D* | *peer-group*} **timers**

［句法描述］

A.B.C.D | *peer-group*	指定对等体 IP 地址或者对等体组的名称。
keepalive	指定发送保持激活信息的频率，单位为秒。取值范围是 0 到 65535，且小于或者等于 HOLDDOWN/3 的值，如果大于 HOLDDOWN/3，实际生效的时间将为 HOLDDOWN/3。参数值为 0 表示不发送 KEEPALIVE 信息。
holddown	指定保持时间，单位为秒。取值范围是 0 或者 3 到 65535。参数值为 0 表示不检查保持时间。

［默认取值］

keepalive - 60 秒。

holddown - 180 秒。

［命令模式］

BGP 实例配置模式。

［使用指导］

通过该命令配置的定时器优先级高于通过 **timer** *keepalive holddown* 设置的值。

［命令实例］

hostname(config-router)# **neighbor 1.1.1.1 timers 80 200**

---

neighbor（RIP）

指定邻居。使用该命令 no 的形式删除指定的邻居。

［命令］

neighbor *ip-address*

no neighbor *ip-address*

［句法描述］

ip-address	指定邻居的 IP 地址。

［默认取值］

无。

［命令模式］

RIP 路由配置模式。

［使用指导］

无。

［命令实例］

hostname(config-router)# **neighbor 10.0.0.1**

---

next-hop

配置 PBR 规则的下一跳。使用该命令 no 的形式取消下一跳的指定。

［命令］

nexthop {*interface-name* | *A.B.C.D* | **vrouter** *vrouter-name*}

no nexthop

［句法描述］

interface-name	出接口名称。
A.B.C.D	下一跳的 IP 地址。
vrouter-name	VRouter 名称。

［默认取值］

无。

［命令模式］

PBR 规则配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-pbr)# match id 1
hostname(config-pbr-match)# next-hop ethernet0/2
```

network（BGP）

向 BGP 路由表中添加静态 BGP 路由条目。使用该命令 no 的形式删除指定的静态路由条目。

［命令］

network {*A.B.C.D/M* | *A.B.C.D A.B.C.D*}

no network {*A.B.C.D/M* | *A.B.C.D A.B.C.D*}

［句法描述］

A.B.C.D/M | *A.B.C.D A.B.C.D*	指定 BGP 静态路由条目信息。安全网关支持两种方式，*A.B.C.D/M* 或者 *A.B.C.D A.B.C.D*，例如 1.1.1.0/24 或者 1.1.1.0 255.255.255.0。

［默认取值］

无。

［命令模式］

BGP 实例配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-router)# network 1.1.1.1/24
```

network（RIP）

配置网络，使得只有在指定网络中的接口才能接收和发送 RIP 更新。使用该命令 no 的形式删除指定的网络。

［命令］

network *ip-address/netmask*

no network *ip-address/netmask*

［句法描述］

ip-address/netmask	指定网络的 IP 地址。

［默认取值］

无。

［命令模式］

RIP 路由配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-router)# network 10.200.0.0/16
```

network area

指定运行 OSPF 协议的接口网络并且将网络配置到指定的区域中。使用该命令 no 的形式取消对网络的指定。

［命令］

network *A.B.C.D/M* **area** {*id* | *A.B.C.D*}

no network *A.B.C.D/M* **area** {*id* | *A.B.C.D*}

［句法描述］

A.B.C.D/M	指定运行 OSPF 协议的接口网络。
area {*id* | *A.B.C.D*}	指定将网络添加到的区域 ID。区域 ID 用 32 比特数来表示，可以是数字形式，也可以是 IP 地址形式。

［默认取值］

无。

［命令模式］

OSPF 路由配置模式。

［使用指导］

无。

［命令实例］

hostname(config-router)# **network 10.200.0.0/16 area 1000**

passive-interface

将接口配置为只接收更新但是不发送的接口，即被动接口。使用该命令 no 的形式消被动接口的配置。

［命令］

passive-interface *interface-name*

no passive-interface *interface-name*

［句法描述］

interface-name	指定接口的名称作为被动接口。

［默认取值］

无。

［命令模式］

RIP 路由配置模式或 OSPF 路由配置模式。

［使用指导］

无。

［命令实例］

hostname(config-router)# **passive-interface ethernet0/10**

pbr-policy

创建 PBR 策略，如果该 PBR 策略已创建则直接进入 PBR 策略配置模式。使用该命令 no 的形式删除指定名称的 PBR 策略。

［命令］

pbr-policy *name*

no pbr-policy *name*

［句法描述］

name	指定 PBR 策略名。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **pbr-policy abc**

redistribute（BGP）

配置引入到 BGP 中的其它路由协议的信息。使用该命令 no 的形式取消指定类型路由的引入。

［命令］

redistribute {connected |static | rip | ospf} [metric *value***]**

no redistribute {connected |static | rip | ospf}

［句法描述］

connected |static | rip | ospf	指定引入路由的类型，可以是直连路由（**connected**）、静态路由（**static**）、RIP（**rip**）或者 OSPF（**ospf**）。
metric *value*	指定引入路由的度量。范围是 0 到 4294967295。如果不指定该数值，系统会使用 BGP 的缺省度量（通过 **default-metric** *value* 配置）。

［默认取值］

无。

［命令模式］

RIP 路由配置模式。

［使用指导］

配置多条该命令引入不同类型的路由。

［命令实例］

```
hostname(config-router)# redistribute static
```

redistribute（RIP）

配置引入到 RIP 中的其它路由协议的信息。使用该命令 no 的形式取消指定类型路由的引入。

［命令］

redistribute {connected | static | ospf} [metric *value*]

no redistribute {connected | static | ospf}

［句法描述］

connected | static | ospf	指定引入路由的类型，可以是直连路由（**connected**）、静态路由（**static**）或者 OSPF（**ospf**）。
metric *value*	指定引入路由的度量。范围是 1 到 15。

［默认取值］

无。

［命令模式］

RIP 路由配置模式。

［使用指导］

如果不指定引入路由的度量，系统会使用 RIP 的缺省度量（通过 **default-metric *value*** 配置）。

［命令实例］

```
hostname(config-router)# redistribute static
```

redistribute（OSPF）

配置引入到 OSPF 中的其它路由协议的信息。使用该命令 no 的形式取消指定类型路由的引入。

［命令］

redistribute {connected | static | rip} [type {1 | 2}] [metric *value*]

no redistribute {connected | static | rip}

［句法描述］

connected | static | rip	指定引入路由的类型，可以是直连路由（**connected**）、静态路由（**static**）或者 RIP（**rip**）。
type {1 | 2}	指定外部路由的类型。**1** 指 type1 外部路由，**2** 指 type2 外部路由。
metric *value*	指定引入路由的度量。范围是 0 到 16777214。

［默认取值］

无。

［命令模式］

OSPF 路由配置模式。

［使用指导］

如果不指定该数值，系统会使用 OSPF 的缺省度量（通过 **default-metric** *value* 配置）。

［命令实例］

hostname(config-router)# **redistribute static**

role

添加角色类型源地址。使用该命令 no 的形式为规则删除角色类型的源地址。

［命令］

role *role-name*

no role *role-name*

［句法描述］

role-name	角色名称。

［默认取值］

无默认值。

［命令模式］

PBR 规则配置模式。

［使用指导］

无。

［命令实例］

hostname(config-pbr)# **match id 3**

hostname(config-pbr-match)# **role role1**

```
hostname(config-pbr-match)# no role role1
```

router bgp

开启/关闭策略路由、源接口路由和源路由查询。

［命令］

route enable {pbr | sibr | sbr}

route disable {pbr | sibr | sbr}

［句法描述］

pbr	开启/关闭策略路由查询。
sibr	开启/关闭源接口路由查询。
sbr	开启/关闭源路由查询。

［默认取值］

默认情况下，策略路由、源接口路由和源路由查询为开启状态。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# route enable pbr
```

router bgp

进入 BGP 路由配置模式，开启安全网关的 BGP 功能，并且为指定的 BGP 实例创建 BGP 实例。使用该命令 no 的形式删除 BGP 实例。

［命令］

router bgp *number*

no router bgp *number*

［句法描述］

number	指定自治系统的编号。范围是 1 到 65535。

［默认取值］

无。

［命令模式］

VRouter 配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# router bgp 20
```

---

router ospf

进入 OSPF 路由配置模式，同时开启安全网关的 OSPF 功能。使用该命令 no 的形式关闭 OSPF 功能。

［命令］

router ospf

no router ospf

［句法描述］

无。

［默认取值］

无。

［命令模式］

VRouter 配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-vrouter)# router ospf
hostname(config-router)#
```

---

router rip

进入 RIP 路由配置模式，同时开启安全网关的 RIP 功能。使用该命令 no 的形式关闭 RIP 功能。

［命令］

router rip

no router rip

［句法描述］

无。

［默认取值］

无。

［命令模式］

VRouter 配置模式。

［使用指导］

无。

［命令实例］

hostname(config-vrouter)# **router rip**

hostname(config-router)#

---

router-id （BGP）

为 BGP 协议配置路由器在整个 BGP 域中的唯一标识 Router ID。使用该命令 no 的形式取消 Router ID 的指定。

［命令］

router-id *A.B.C.D*

no router-id

［句法描述］

A.B.C.D	指定 BGP 协议使用的 Router ID，为 IP 地址形式。

［默认取值］

无。

［命令模式］

BGP 实例配置模式。

［使用指导］

无。

［命令实例］

hostname(config-router)# **router-id 1.1.1.1**

router-id （OSPF）

为 OSPF 协议配置路由器在整个 OSPF 域中的唯一标识 Router ID。

［命令］

router-id *A.B.C.D* [**local**]

［句法描述］

A.B.C.D	指定 OSPF 协议使用的 Router ID，为 IP 地址形式。
local	指定 OSPF 协议的 Router ID 为本地配置，该配置适用于 HA A/A 工作模式，并且不进行 HA 配置同步。

［默认取值］

默认情况下，Router ID 为非本地配置。

［命令模式］

OSPF 路由配置模式。

［使用指导］

无。

［命令实例］

hostname(config-router)# **router-id 1.1.1.1**

service

指定流量的服务类型。使用该命令 no 的形式为规则删除指定的服务。

［命令］

service *service-name*

no service *service-name*

［句法描述］

service-name	为流量指定服务或者服务组。该服务或者服务组来自服务簿。

［默认取值］

无默认值。

［命令模式］

PBR 规则配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# pbr-policy abc
hostname(config-pbr)# match id 3
hostname(config-policy-match)# service my-service
hostname(config-policy-match)# no service my-service
```

src-addr

添加地址簿条目类型源地址。使用该命令 no 的形式为规则删除地址簿条目类型源地址。

［命令］

src-addr *src-addr*

no src-addr *src-addr*

［句法描述］

src-addr	规则的源地址。

［默认取值］

无默认值。

［命令模式］

PBR 规则配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-pbr)# match id 3
hostname(config-pbr-match)# src-addr addr1
hostname(config-pbr-match)# no src-addr any
```

src-host

添加主机成员类型源地址。使用该命令 no 的形式为规则删除主机成员类型源地址。

［命令］

src-host *host-name*

no src-addr *host-name*

［句法描述］

host-name	主机名称。

［默认取值］

无默认值。

［命令模式］

PBR 规则配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-pbr)# match id 3
hostname(config-pbr-match)# src-host host1
hostname(config-pbr-match)# no src-host host1
```

src-ip

添加 IP 成员类型源地址。使用该命令 no 的形式为规则删除 IP 成员类型的源地址。

［命令］

src-ip *ip/netmask*

no src-ip *ip/netmask*

［句法描述］

ip/netmask	IP 地址/子网掩码

［默认取值］

无默认值。

［命令模式］

PBR 规则配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-pbr)# match id 3
hostname(config-pbr-match)# src-ip 10.3.4.5/24
hostname(config-pbr-match)# no src-ip 10.3.4.5/24
```

src-range

添加 IP 地址范围类型源地址。使用该命令 no 的形式为规则删除 IP 地址范围类型的源地址。

［命令］

src-range *min-ip* [*max-ip*]

no src-range *min-ip* [*max-ip*]

［句法描述］

min-ip	IP 地址范围的最小值。
max-ip	IP 地址范围的最大值。

［默认取值］

无默认值。

［命令模式］

PBR 规则配置模式。

［使用指导］

添加了 IP 地址段作为源地址后，只能全部删除该地址段，不能部分删除。如：添加了 1.1.1.1 到 1.1.1.6 地址段的 IP 地址范围时，不能使用 no 命令删除 1.1.1.2 到 1.1.1.4 地址段的 IP 地址范围，只能全部删除。

［命令实例］

```
hostname(config-pbr)# match id 3
hostname(config-pbr-match)# src-range 10.3.4.5 10.3.4.36
hostname(config-pbr-match)# no src-range 10.3.4.5 10.3.4.36
```

subnet

为 ISP 添加子网条目。使用该命令 no 的形式删除指定的子网。

［命令］

subnet *A.B.C.D/M*

no subnet *A.B.C.D/M*

［句法描述］

A.B.C.D/M	为 ISP 指定子网，格式为 IP 地址/掩码，例如 1.1.0/24。

［默认取值］

无。

［命令模式］

ISP 信息配置模式。

［使用指导］

在 ISP 信息配置模式下配置多条该命令，为 ISP 添加多个子网。

［命令实例］

```
hostname(config)# isp-network isp1
hostname(config-isp)# subnet 192.168.1.0/24
```

timers

配置 BGP 定时器。使用该命令 no 的形式恢复定时器的默认值。

［命令］

timer *keepalive holddown*

no timers

［句法描述］

keepalive	指定发送保持激活信息的频率，单位为秒。取值范围是 0 到 65535，且小于或者等于 HOLDDOWN/3 的值，如果大于 HOLDDOWN/3，实际生效的时间将为 HOLDDOWN/3。参数值为 0 表示不发送 KEEPALIVE 信息。
holddown	指定保持时间，单位为秒。取值范围是 0 或者 3 到 65535。参数值为 0 表示不检查保持时间。

［默认取值］

keepalive – 60。

holddown – 180。

［命令模式］

BGP 实例配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-router)# timer 30 200
```

timers basic

配置定时器。使用该命令 no 的形式恢复定时器的默认值。

［命令］

timers basic *interval-time invalid-time holddown-time flush-time*

no timers basic

［句法描述］

interval-time	指定发送更新的时间间隔，单位为秒。范围是 0 到 16777215 秒。
invalid-time	指定路由的失效时间，单位为秒。范围是 1 到 16777215 秒。
holddown-time	指定路由的保持时间，单位为秒。范围是 1 到 16777215 秒。
flush-time	指定路由的清除时间，单位为秒。范围是 1 到 16777215 秒。

［默认取值］

interval-time – 30。

invalid-time – 180。

holddown-time – 180。

flush-time – 240。

［命令模式］

RIP 路由配置模式。

［使用指导］

无。

［命令实例］

hostname(config-router)# **timers basic 40 200 200 260**

timers spf

配置 OSPF 定时器。使用该命令 no 的形式恢复定时器的默认值。

［命令］

timers spf *delay1 delay2*

no timers spf

［句法描述］

delay1	收到更新后，在该指定时间内进行重新计算，单位为秒。范围是 0 到 65535。
delay2	指定两次计算的时间间隔，单位为秒。范围是 0 到 65535。

［默认取值］

delay1 – 5。

delay – 10。

［命令模式］

OSPF 路由配置模式。

［使用指导］

无。

［命令实例］

hostname(config-router)# **timers spf 30 60**

---

unknown-multicast drop

开启未知组播报文功能后，安全设备将丢弃发往未知组播组的报文，从而节省带宽。使用该命令 no 的形式关闭该功能。

［命令］

unknown-multicast drop

no unknown-multicast drop

［句法描述］

无。

［默认取值］

禁用。

［命令模式］

VSwitch 配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **vswitch vswitch1**

hostname(config-vswitch)# **unknown-multicast drop**

---

user

添加用户类型源地址。使用该命令 no 的形式为规则删除用户类型的源地址。

［命令］

user *aaa-server-name user-name*

no user *aaa-server-name user-name*

［句法描述］

aaa-server-name	AAA 服务器名称。
user-name	用户名。

［默认取值］

无默认值。

［命令模式］

PBR 规则配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-pbr)# match id 3
hostname(config-pbr-match)# user local user1
hostname(config-pbr-match)# no user local user1
```

user-group

添加用户组类型源地址。使用该命令 no 的形式为规则删除用户组类型的源地址。

［命令］

user-group *aaa-server-name user-group-name*

no user-group *aaa-server-name user-group-name*

［句法描述］

aaa-server-name	AAA 服务器名称。
user-group-name	用户组名。

［默认取值］

无默认值。

［命令模式］

PBR 规则配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-pbr)# match id 3
hostname(config-pbr-match)# user-group local grp1
hostname(config-pbr-match)# no user-group local grp1
```

version

指定 RIP 协议版本号。使用该命令 no 的形式恢复默认版本配置。

［命令］

version *version-number*

no version

［句法描述］

version-number	RIP 协议版本号，取值为 1（RIP-1）或者 2（RIP-2）。

［默认取值］

2 (RIP-2)。

［命令模式］

RIP 路由配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-router)# version 1
```

网络参数命令

ac

为安全网关指定访问集中器。使用该命令 no 的形式取消对访问集中器的指定。

［命令］

ac *ac-name*

no ac

［句法描述］

ac-name	指定可使用的访问集中器的名称。

［默认取值］

无。

［命令模式］

PPPoE 实例配置模式。

［使用指导］

无。

［命令实例］

hostname(config-pppoe-group)# **ac ac1**

address

指定地址池的 IP 地址范围。使用该命令 no 的形式取消指定的 IP 地址范围。

［命令］

address *start-ip-address* [*end-ip-address*]

no address *start-ip-address* [*end-ip-address*]

［句法描述］

start-ip-address	指定地址范围的起始地址。
end-ip-address	指定地址范围的结束地址。

［默认取值］

无。

［命令模式］

DHCP 服务器配置模式。

［使用指导］

无。

［命令实例］

hostname(config-dhcp-server)# **address 192.168.1.100 192.168.1.200**

authentication

指定安全网关与 PPPoE 服务器建立连接时的验证方式。使用该命令 no 的形式恢复默认验证方式。

［命令］

authentication {chap | pap | any}

no authentication

［句法描述］

chap	指定验证方式为 CHAP。
pap	指定验证方式为 PAP。
any	指定验证方式为 CHAP 或者 PAP 任何一种。

［默认取值］

any。

［命令模式］

PPPoE 实例配置模式。

［使用指导］

无。

［命令实例］

hostname(config-pppoe-group)# **authentication chap**

auto-config interface

配置接口的 DHCP 自动配置功能。使用该命令 no 的形式取消自动配置功能。

［命令］

auto-config interface *interface-name*

no auto-config

［句法描述］

interface-name	同一台安全网关上开启了 DHCP 客户端功能的接口名称。

［默认取值］

无。

［命令模式］

DHCP 服务器配置模式。

［使用指导］

无。

［命令实例］

hostname(config-dhcp-server)# **auto-config interface ethernet0/2**

auto-connect

指定 PPPoE 连接断开后到系统自动重拨之间的时间间隔。使用该命令 no 的形式恢复默认自动连接值。

［命令］

auto-connect *time-value*

no auto-connect

［句法描述］

time-value	指定自动连接的时间，范围是 0 到 10000 秒。

［默认取值］

time-value – 0，表示关闭自动连接功能。

［命令模式］

PPPoE 实例配置模式。

［使用指导］

无。

［命令实例］

hostname(config-pppoe-group)# **auto-connect 10**

clear host

清除动态 DNS 映射条目。

［命令］

clear host [*host-name*]

［句法描述］

host-name	清除指定主机的 DNS 映射条目。

［默认取值］

无。

［命令模式］

执行模式。

［使用指导］

无。

［命令实例］

hostname# **clear host**

ddns enable

绑定接口到 DDNS 服务名称。使用该命令 no 的形式取消接口与 DDNS 服务名称的绑定。

［命令］

ddns enable *ddns-name* **interface** *interface-name* **hostname** *host-name*

no ddns enable *ddns-name* **interface** *interface-name*

［句法描述］

ddns-name	指定配置好的 DDNS 服务名称。
interface-name	指定要绑定的接口的名称。
host-name	指定在相应 DDNS 提供商处申请得到的域名。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **ddns enable 3322 interface ethernet0/2 hostname hillstonenet.3322.org**

ddns name

创建一个 DDNS 服务名称，指定其更新类型并且进入指定的 DDNS 服务配置模式。使用该命令 no 的形式删除指定的 DDNS 服务名称。

［命令］

ddns name *ddns-name* **type http**

no ddns name *ddns-name* **type http**

［句法描述］

ddns-name	指定 DDNS 服务名称。
type http	指定 DDNS 服务的更新方式，即发送 DDNS 更新请求的方式，为 HTTP。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **ddns name 3322 type http**

dhcp-client dns admin-preference

配置 DHCP 方式获得的 DNS 服务器的优先级。使用该命令 no 的形式恢复优先级的默认值。

［命令］

dhcp-client dns admin-preference *number*

［句法描述］

number	指定 DHCP 方式获得的 DNS 服务器的优先级。范围是 1 到 255。

［默认取值］

number - 20。

［命令模式］

接口配置模式。

［使用指导］

无。

［命令实例］

hostname(config-if-eth0/2)# **dhcp-client dns admin-preference 100**

---

dhcp-client ip

使接口释放或重新获取 IP 地址，或者查看接口获取的 DHCP IP 地址信息。

［命令］

dhcp-client ip {release | renew | show}

［句法描述］

release	释放 IP 地址。
type http	重新获取 IP 地址。
show	查看接口获取的 DHCP IP 地址信息。

［默认取值］

无。

［命令模式］

接口配置模式。

［使用指导］

无。

［命令实例］

hostname(config-if-eth0/2)# **dhcp-client ip release**

---

dhcp-client route

在 DHCP 接口设置了默认路由后，设置路由优先级（管理距离）和路由权值。使用该命令 no 的形式恢复路由优先级和路由权值的默认值。

［命令］

dhcp-client route {distance *value*| **weight** *value*}

［句法描述］

distance *value*	指定路由优先级。范围是 1 到 255。
weight *value*	指定路由权值。范围是 1 到 255。

［默认取值］

distance *value* - 1。

weight *value* – 1。

［命令模式］

接口配置模式。

［使用指导］

无。

［命令实例］

hostname(config-if-eth0/2)# **dhcp-client route distance 2**

dhcp-relay enable

开启接口的 DHCP 中继代理功能。使用该命令 no 的形式关闭接口的 DHCP 中继代理功能。

［命令］

dhcp-relay enable

no dhcp-relay enable

［句法描述］

无。

［默认取值］

无。

［命令模式］

接口配置模式。

［使用指导］

无。

［命令实例］

hostname(config-if-eth0/2)# **dhcp-relay enable**

dhcp-relay server

为 DHCP 中继代理功能指定 DHCP 服务器的 IP 地址。使用该命令 no 的形式取消对 DHCP 服务器 IP 地址的配置。

［命令］

dhcp-relay server *ip-address*

no dhcp-relay server *ip-address*

［句法描述］

ip-address	指定 DHCP 服务器的 IP 地址。

［默认取值］

无。

［命令模式］

接口配置模式。

［使用指导］

无。

［命令实例］

hostname(config-if-eth0/2)# **dhcp-relay server 192.168.0.1**

dhcp-server enable

绑定地址池到接口。使用该命令 no 的形式关闭接口的 DHCP 服务器功能。

［命令］

dhcp-server enable pool *pool-name*

no dhcp-server enable

［句法描述］

pool-name	指定已配置的地址池的名称。

［默认取值］

无。

［命令模式］

接口配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-if-eth0/2)# dhcp-server enable pool dhcp_pool1
```

dhcp-server pool

新建一个 DHCP 地址池，并且进入该地址池的 DHCP 服务器配置模式；如果指定的地址池名称已存在，则直接进入相应的 DHCP 服务器配置模式。使用该命令 no 的形式删除指定的 DHCP 地址池。

［命令］

dhcp-server pool *pool-name*

no dhcp-server pool *pool-name*

［句法描述］

pool-name	指定 DHCP 地址池名称。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# dhcp-server pool dhcp_pool1
```

dns

为 DHCP 客户端配置 DNS 服务器。使用该命令 no 的形式取消 DNS 服务器的配置。

［命令］

dns *ip-address1* [*ip-address2*]

no dns

［句法描述］

ip-address1	指定主 DNS 服务器的 IP 地址。
ip-address2	指定备用 DNS 服务器的 IP 地址。

［默认取值］

无。

［命令模式］

DHCP 服务器配置模式。

［使用指导］

无。

［命令实例］

hostname(config-dhcp-server)# **dns 202.98.101.28**

---

dns admin-preference

配置 PPPoE 方式获得的 DNS 服务器的优先级。使用该命令 no 的形式恢复优先级的默认值。

［命令］

dns admin-preference *number*

［句法描述］

number	指定 PPPoE 方式获得的 DNS 服务器的优先级。范围是 1 到 255。

［默认取值］

number - 20。

［命令模式］

PPPoE 实例配置模式。

［使用指导］

无。

［命令实例］

hostname(config-pppoe-group)# **dns admin-preference 100**

---

dns-proxy

开启接口的域名代理功能。使用该命令 no 的形式关闭接口的域名代理功能。

［命令］

dns-proxy [trans]

no dns-proxy [trans]

［句法描述］

dns-proxy	开启 DNS 普通代理功能。
dns-proxy trans	开启 DNS 透明代理功能。

［默认取值］

关闭。

［命令模式］

接口配置模式。

［使用指导］

安全网关的 DNS 代理功能分为 DNS 普通代理和 DNS 透明代理。二者的区别在于：配置 DNS 普通代理的同时，客户端仍需要配置 DNS 代理服务器的地址；而配置透明代理后，用户则不需要在客户端上进行任何代理配置。

［命令实例］

```
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# dns-proxy
```

domain

为 DHCP 客户端配置域名。使用该命令 no 的形式取消域名的配置。

［命令］

domain *domain-name*

no domain

［句法描述］

domain-name	指定域名。

［默认取值］

无。

［命令模式］

DHCP 服务器配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-dhcp-server)# domain hillstonenet.com
```

gateway

为客户端配置网关 IP 地址。使用该命令 no 的形式取消网关 IP 地址的配置。

［命令］

gateway *ip-address*

no gateway

［句法描述］

ip-address	指定网关的 IP 地址。

［默认取值］

无。

［命令模式］

DHCP 服务器配置模式。

［使用指导］

无。

［命令实例］

hostname(config-dhcp-server)# **gateway 192.168.1.1**

exclude address

配置保留地址池。使用该命令 no 的形式取消指定的保留地址池。

［命令］

exclude address *start-ip-address* [*end-ip-address*]

no exclude address *start-ip-address* [*end-ip-address*]

［句法描述］

start-ip-address	指定保留地址池的起始地址。
end-ip-address	指定保留地址池的结束地址。

［默认取值］

无。

［命令模式］

DHCP 服务器配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-dhcp-server)# exclude address 192.168.1.150
192.168.1.160
```

idle-interval

指定 PPPoE 接口的空闲时间。使用该命令 no 的形式恢复默认空闲时间值。

［命令］

idle-interval *time-value*

no idle-interval

［句法描述］

time-value	指定空闲时间，范围是 0 到 10000 分钟。

［默认取值］

time-value – 30 分钟。

［命令模式］

PPPoE 实例配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-pppoe-group)# idle-interval 20
```

ip address dhcp

使接口通过 DHCP 方式获取 IP 地址。使用该命令 no 的形式取消接口通过 DHCP 获取 IP 地址的方式。

［命令］

ip address dhcp [setroute]

no ip address dhcp

［句法描述］

setroute	将 DHCP 服务器提供的网关信息设置为默认网关路由。

［默认取值］

无。

［命令模式］

接口配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-if-eth0/2)# ip address dhcp setroute
```

---

ip dns-proxy black-list enable

开启 DNS 代理的黑名单功能。使用该命令 no 的形式关闭该功能。

［命令］

```
ip dns-proxy black-list enable
no ip dns-proxy black-list enable
```

［句法描述］

无。

［默认取值］

关闭。

［命令模式］

全局配置模式。

［使用指导］

开启并配置黑名单后，若客户端向属于黑名单中的域名发出查询请求，系统将不对该请求进行解析。黑白名单不可同时配置。

［命令实例］

```
hostname(config)# ip dns-proxy black-list enable
```

---

ip dns-proxy white-list enable

开启 DNS 代理的白名单功能。使用该命令 no 的形式关闭该功能。

［命令］

```
ip dns-proxy white-list enable
no ip dns-proxy white-list enable
```

［句法描述］

无。

［默认取值］

关闭。

［命令模式］

全局配置模式。

［使用指导］

开启并配置白名单后，系统仅对属于白名单中的域名进行解析。黑白名单不可同时配置。

［命令实例］

hostname(config)# **ip dns-proxy white-list enable**

---

ip dns-proxy black-list domain

添加域名到 DNS 代理黑名单中。使用该命令 no 的形式将指定的域名从黑名单中删除。

［命令］

ip dns-proxy black-list domain *suffix*

no ip dns-proxy black-list domain *suffix*

［句法描述］

suffix	指定添加到黑名单中的域名的后缀。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

使用多条该命令添加多个域名到黑名单。最多允许添加 100 个域名到黑名单。

［命令实例］

hostname(config)# **ip dns-proxy black-list domain com**

---

ip dns-proxy white-list domain

添加域名到 DNS 代理白名单中。使用该命令 no 的形式将指定的域名从白名单中删除。

［命令］

ip dns-proxy white-list domain *suffix*

no ip dns-proxy white-list domain *suffix*

［句法描述］

suffix	指定添加到白名单中的域名的后缀。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

使用多条该命令添加多个域名到白名单。最多允许添加 100 个域名到白名单。

［命令实例］

hostname(config)# **ip dns-proxy white-list domain cn**

ip address pppoe

使接口通过 PPPoe 方式获取 IP 地址。使用该命令 no 的形式取消接口通过 PPPoE 获取 IP 地址的方式。

［命令］

ip address pppoe [setroute]

no ip address pppoe

［句法描述］

setroute	将 PPPoE 服务器提供的网关信息设置为默认网关路由。

［默认取值］

无。

［命令模式］

接口配置模式。

［使用指导］

无。

［命令实例］

hostname(config-if-eth0/2)# **ip address pppoe setroute**

ip domain lookup

开启安全网关的 DNS 功能。使用该命令 no 的形式关闭 DNS 功能。

［命令］

ip domain lookup

no ip domain lookup

［句法描述］

无。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

默认情况下，安全网关的 DNS 功能是开启的。

［命令实例］

hostname(config)# **ip domain lookup**

ip domain name

为安全网关指定域名。使用该命令 no 的形式恢复默认域名。

［命令］

ip domain name *domain-name*

no ip domain name

［句法描述］

domain-name	指定域名。名称长度可以是 1 到 255 个字符，但是在两个句点（.）之间，最多可以有 63 个字符。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **ip domain name hillstonenet.com**

ip domain retry

设置发送 DNS 请求的重试次数。使用该命令 no 的形式恢复默认重试次数。

［命令］

ip domain retry *times*

no ip domain retry

［句法描述］

times	指定重试次数。取值范围为 1 到 3 次。

［默认取值］

times – 2 次。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **ip domain retry 3**

ip domain timeout

设置 DNS 请求的响应超时时间。使用该命令 no 的形式恢复默认超时时间。

［命令］

ip domain timeout *timeout-value*

no ip domain timeout

［句法描述］

timeout-value	指定超时时间。取值范围为 1 到 3 秒。

［默认取值］

timeout-value – 2 秒。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **ip domain timeout 3**

---

ip host

手动添加 DNS 映射条目到缓存。使用该命令 no 的形式删除指定的静态 DNS 映射条目。

［命令］

ip host *host-name* {*address1* [*address2*] ... [*address8*]}

no ip host *host-name*

［句法描述］

host-name	指定主机名称。名称范围是 1 到 255 个字符。
{*address1* [*address2*] ... [*address8*]}	指定主机的 IP 地址。最多可设置 8 个 IP 地址。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **ip host www 202.90.163.27**

---

ip name-server

设置 DNS 域名服务器。使用该命令 no 的形式取消对 DNS 域名服务器的配置。

［命令］

ip name-server *server-address1* [*server-address2*] ... [*server-address6*]

no ip name-server *server-address1* [*server-address2*] ... [*server-address6*]

［句法描述］

server-address1	指定域名服务器的 IP 地址。最多可配置 6 个域名服务器，可以使用一条命令配置 6 个域名服务器，也可分多条命令配置。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **ip name-server 202.106.0.20**

ip dns-proxy domain

为 DNS 代理服务选择列表添加条目。使用该命令 no 的形式删除选择条目。

［命令］

ip dns-proxy domain {*suffix* | **any**} {**name-server** {**use-system** | *server-ip1* [*server-ip2*] ... [*server-ip6*]}}

no ip dns-proxy domain {*suffix* | **any**}

［句法描述］

suffix | **any**	指定域名后缀，用来匹配 DNS 请求中的域名。**any** 为任意后缀。
name-server {**use-system** | *server-ip1* [*server-ip2*] ... [*server-ip6*]}	指定 DNS 服务器的 IP 地址，可以是安全网关系统的 DNS 域名服务器（**use-system**），也可以是指定的 IP 地址（*server-ip1* [*server-ip2*] ... [*server-ip6*]）。最多可以指定 6 个 DNS 服务器 IP 地址。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# ip dns-proxy domain com name-server 2.2.2.2
```

ipmac-bind

将 IP 与 MAC 地址绑定。使用该命令 no 的形式取消指定 IP 与 MAC 地址的绑定。

［命令］

ipmac-bind *ip-address mac*

no ipmac-bind *ip-address mac*

［句法描述］

ip-address	指定 IP 地址。IP 地址必须是 IP 地址池中的地址。
mac	指定与 IP 地址绑定 MAC 地址。

［默认取值］

无。

［命令模式］

DHCP 服务器配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-dhcp-server)# ipmac-bind 192.168.1.106
001c.5400.0c89
```

lease

配置 DHCP 服务器的租约。使用该命令 no 的形式恢复租约的默认值。

［命令］

lease *lease-time*

no lease

［句法描述］

lease-time	指定租约时间。范围是 300 到 1048575 秒。

［默认取值］

lease-time – 3600 秒。

［命令模式］

DHCP 服务器配置模式。

［使用指导］

无。

［命令实例］

hostname(config-dhcp-server)# **lease 7200**

maxupdate interval

配置 DDNS 最大更新间隔。使用该命令 no 的形式恢复默认最大更新间隔时间。

［命令］

maxupdate interval *time-value*

no maxupdate

［句法描述］

time-interval	指定最大更新间隔时间。取值范围为 24 到 8760 小时。

［默认取值］

24 小时。

［命令模式］

DDNS 服务名称配置模式。

［使用指导］

无。

［命令实例］

hostname(config-ddns)# **maxupdate interval 48**

minupdate interval

配置最小更新间隔时间。使用该命令 no 的形式恢复默认最小更新间隔时间。

［命令］

minupdate interval *time-value*

no minupdate

［句法描述］

time-interval	指定最小更新间隔时间。取值范围为 5 到 120 分钟。

［默认取值］

5 分钟。

［命令模式］

DDNS 服务名称配置模式。

［使用指导］

无。

［命令实例］

hostname(config-ddns)# **minupdate interval 10**

netmask（DHCP）

为客户端配置网络掩码。使用该命令 no 的形式取消网络掩码的配置。

［命令］

netmask *netmask*

no netmask

［句法描述］

netmask	指定网络掩码。

［默认取值］

无。

［命令模式］

DHCP 服务器配置模式。

［使用指导］

无。

［命令实例］

hostname(config-dhcp-server)# **netmask 255.255.255.0**

netmask（PPPoE）

为 PPPoE 方式获得的 IP 地址指定网络掩码。使用该命令 no 的形式取消网络掩码的配置。

［命令］

netmask *netmask*

no netmask

［句法描述］

netmask	指定网络掩码。

［默认取值］

无。

［命令模式］

PPPoE 实例配置模式。

［使用指导］

无。

［命令实例］

hostname(config-pppoe-group)# **netmask 255.255.255.0**

news

为 DHCP 客户端配置新闻服务器。使用该命令 no 的形式取消新闻服务器的配置。

［命令］

news *ip-address*

no news

［句法描述］

ip-address	指定新闻服务器的 IP 地址。

［默认取值］

无。

［命令模式］

DHCP 服务器配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-dhcp-server)# news 192.168.1.2
```

pop3

为 DHCP 客户端配置 POP3 服务器。使用该命令 no 的形式取消 POP3 服务器的配置。

［命令］

pop3 *ip-address*

no pop3

［句法描述］

ip-address	指定 POP3 服务器的 IP 地址。

［默认取值］

无。

［命令模式］

DHCP 服务器配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-dhcp-server)# pop3 192.168.1.2
```

pppoe enable group

绑定 PPPoE 实例到接口。使用该命令 no 的形式取消 PPPoE 实例与接口的绑定。

［命令］

pppoe enable group *group-name*

no pppoe enable group

［句法描述］

group-name	指定 PPPoE 实例的名称。

［默认取值］

无。

［命令模式］

接口配置模式。

［使用指导］

无。

［命令实例］

hostname(config-if-eth0/2)# **pppoe enable group pppoe_group1**

pppoe-client group

新建 PPPoE 实例，并且进入该实例配置模式；如果指定的实例名称存在，则直接进入 PPPoE 实例配置模式。使用该命令 no 的形式删除指定的 PPPoE 实例。

［命令］

pppoe-client group *group-name*

no pppoe-client group *group-name*

［句法描述］

group-name	指定 PPPoE 实例的名称。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **pppoe-client group pppoe_group1**

pppoe-client group

连接或者断开 PPPoE 连接。

［命令］

pppoe-client group *group-name* {**connect** | **disconnect**}

［句法描述］

group-name	指定 PPPoE 实例的名称。

connect	进行 PPPoE 连接。
disconnect	断开 PPPoE 连接。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **pppoe-client group pppoe_group1 disconnect**

relay-agent

配置中继代理 IP 地址和掩码。使用该命令 no 的形式取消中继代理 IP 地址的配置。

［命令］

relay-agent *ip-address netmask*

no relay-agent *ip-address netmask*

［句法描述］

ip-address netmask	指定中继代理的 IP 地址和掩码。

［默认取值］

无。

［命令模式］

DHCP 服务器配置模式。

［使用指导］

无。

［命令实例］

hostname(config-dhcp-server)# **relay-agent 192.168.1.5 255.255.255.0**

route

为 PPPoE 实例指定路由距离和权值。使用该命令 no 的形式恢复路由距离和权值的默认值。

［命令］

route {**distance** *value*| **weight** *value*}

no route {**distance** | **weight**}

［句法描述］

distance *value*	指定路由距离。范围是 1 到 255。
weight *value*	指定路由权值。范围是 1 到 255。

［默认取值］

distance *value* - 1。

weight *value* - 1。

［命令模式］

PPPoE 实例配置模式。

［使用指导］

无。

［命令实例］

hostname(config-pppoe-group)# **route distance 2**

---

server

指定 DDNS 服务器的名称和端口号。使用该命令 no 的形式取消 DDNS 服务器名称和服务器端口号的配置。

［命令］

server name *server-name* **port** *port-number*

no server

［句法描述］

server-name	指定所配置 DDNS 服务器相应的服务器名称。
port-number	指定所配置 DDNS 服务器相应的服务器端口号。范围是 1 到 65535。

［默认取值］

无。

［命令模式］

DDNS 服务名称配置模式。

［使用指导］

此处配置的名称和端口号必须为 DDNS 服务器相对应的名称和端口号。如果不知道确切信息，请勿配置该命令。与 DDNS 服务器连接成功后，服务器会自动将服务器名称和端口号信息一并返回。

［命令实例］

hostname(config-ddns)# **server name service1 22728**

---

schedule

为 PPPoE 实例配置时间表功能。使用该命令 no 的形式取消时间表配置。

［命令］

schedule *schedule-name* [**disconnect** | **sch-auto-connection** *time-value* | **sch-idle-timeout** *time-value*]

no schedule

［句法描述］

schedule-name	指定时间表条目的名称。
disconnect	配置系统在时间表条目指定的时间内断开 PPPoE 连接。
sch-auto-connection *time-value*	配置系统在时间表条目指定的时间内使用自动连接的方式连接因特网。*time-value* 指定自动连接的时间。范围是 0 到 10000 秒。
sch-idle-timeout *time-value*	配置系统在时间表条目指定的时间内使用按需拨号方式连接因特网。*time-value* 指定空闲时间。范围是 0 到 10000 分钟。

［默认取值］

sch-auto-connection *time-value* - 0，表示关闭自动连接功能。

sch-idle-timeout *time-value* – 30 分钟。

［命令模式］

PPPoE 实例配置模式。

［使用指导］

无。

［命令实例］

hostname(config-pppoe-group)# **schedule schedule1 sch-idle-timeout 20**

---

service

为 PPPoE 实例指定允许的服务。使用该命令 no 的形式取消对服务的指定。

［命令］

service *service-name*

no service

［句法描述］

service-name	指定服务。此处指定的服务必须与 PPPoE 服务器端提供的服务相同。如果不指定服务，安全网关自动接受服务器返回的任何服务。

［默认取值］

无。

［命令模式］

PPPoE 实例配置模式。

［使用指导］

无。

［命令实例］

hostname(config-pppoe-group)# **service http**

smtp

为 DHCP 客户端配置 SMTP 服务器。使用该命令 no 的形式取消 SMTP 服务器的配置。

［命令］

smtp *ip-address*

no smtp

［句法描述］

ip-address	指定 SMTP 服务器的 IP 地址。

［默认取值］

无。

［命令模式］

DHCP 服务器配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-dhcp-server)# smtp 192.168.1.2
```

static-ip

为 PPPoE 实例指定一个静态的 IP 地址。使用该命令 no 的形式取消对静态 IP 地址的指定。

［命令］

static-ip *ip-address*

no static-ip

［句法描述］

ip-address	指定静态 IP 地址。

［默认取值］

无。

［命令模式］

PPPoE 实例配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-pppoe-group)# static-ip 202.90.160.28
```

type

指定 DDNS 服务器。使用该命令 no 的形式取消对 DDNS 服务器的指定。

［命令］

type {huagai | qdns | zoneedit}

no type

［句法描述］

huagai	指定使用 Huagai.net 作为 DDNS 服务器。
qdns	指定使用 3322.org 作为 DDNS 服务器。
zoneedit	指定使用 ZoneEdit.com 作为 DDNS 服务器。

［默认取值］

无。

［命令模式］

DDNS 服务名称配置模式。

［使用指导］

无。

［命令实例］

hostname(config-ddns)# **type qdns**

---

user（DDNS）

指定在 DDNS 服务提供商处注册的用户信息。使用该命令 no 的形式取消用户信息的指定。

［命令］

user *user-name* **password** *user-password*

no user

［句法描述］

user-name	在 DDNS 服务提供商处注册的用户名称。
user-password	与用户名称相对应的密码。

［默认取值］

无。

［命令模式］

DDNS 服务名称配置模式。

［使用指导］

无。

［命令实例］

hostname(config-ddns)# **user gioly378 password grui2e6750**

---

user（PPPoE）

指定 PPPoE 用户信息。使用该命令 no 的形式取消用户信息的指定。

［命令］

user *user-name* **password** *password*

no user

［句法描述］

user-name	PPPoE 用户名称。
password	与用户名称相对应的密码。

［默认取值］

无。

［命令模式］

PPPoE 实例配置模式。

［使用指导］

无。

［命令实例］

hostname(config-pppoe-group)# **user gioly378 password grui2e6750**

wins

为 DHCP 客户端配置 WINS 服务器。使用该命令 no 的形式取消 WINS 服务器的配置。

［命令］

wins *ip-address1* [*ip-address2*]

no wins

［句法描述］

ip-address1	指定主 WINS 服务器的 IP 地址。
ip-address2	指定备用 WINS 服务器的 IP 地址。

［默认取值］

无。

［命令模式］

DHCP 服务器配置模式。

［使用指导］

无。

［命令实例］

hostname(config-dhcp-server)# **wins 202.98.101.29**

虚拟系统命令

enter-vsys

进入非根 VSYS。

［命令］

enter-vsys *vsys-name*

exit-vsys

［句法描述］

vsys-name	指定进入的 VSYS 名称。

［默认取值］

无。

［命令模式］

根 VSYS 执行模式或者全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# enter-vsys vsys-a
hostname(vsys-a)(config)# exit
hostname(vsys-a)# exit-vsys
hostname#
hostname# enter-vsys vsys-a
hostname(vsys-a)# configure
hostname(vsys-a)(config)# exit-vsys
hostname(config)#
```

export-to

所有物理接口都默认属于根 VSYS。根系统 RXW 管理员可以将根 VSYS 中的物理接口导入到非根 VSYS，也可以将非根 VSYS 中的物理接口导出到根 VSYS。

［命令］

将物理接口导入到非根 VSYS：**export-to** *vsys-name*

将非根 VSYS 中的物理接口导出到根 VSYS：**no export-to**

［句法描述］

vsys-name	指定物理接口导入到的 VSYS 名称。

［默认取值］

无。

［命令模式］

接口配置模式。

［使用指导］

导入或者导出的物理接口不能属于安全域，不能为 BGroup 接口、集聚接口、和冗余接口成员，且无子接口。导入到非根 VSYS 中的物理接口的相关接口（如子接口）只能在该非根 VSYS 中使用。

［命令实例］

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# export-to vsys-a
hostname(config-if-eth0/0)#
```

profile

将已经创建的 VSYS Profile 绑定到 VSYS。

［命令］

profile *vsys-profile-name*

no vsys-profile *vsys-profile-name*

［句法描述］

vsys-profile-name	指定绑定的 VSYS Profile 名称。

［默认取值］

无。

［命令模式］

VSYS 配置模式。

［使用指导］

当将一个 Profile 绑定到 VSYS 时，如果所有 VSYS 的保留配额之和超过当前系统 Capacity，则绑定失败。

［命令实例］

```
hostname(config)# vsys vsys-a
hostname(config-vsys)# profile profile1
```

session

设置 VSYS 中各项系统资源的预留配额和最大配额。预留配额即系统为每个 VSYS 预留的资源值；最大配额即每个 VSYS 可获得的最大资源值。

［命令］

{session | zone | policy | snat | dnat} max *max-num* **reserve** *reserve-num*

no {session | zone | policy | snat | dnat}

［句法描述］

max *max-num*	指定 VSYS 中会话数（**session**）、安全域个数（**zone**）、策略数（**policy**）、SNAT 规则数（**snat**）和 DNAT 规则数（**dnat**）的最大配额。
reserve *reserve-num*	指定 VSYS 中会话数（**session**）、安全域个数（**zone**）、策略数（**policy**）、SNAT 规则数（**snat**）和 DNAT 规则数（**dnat**）的保留配额。

［默认取值］

无。

［命令模式］

VSYS Profile 配置模式。

［使用指导］

最大配额根据不同平台取值范围不同。各资源最大配额的取值范围参见下表：

系统资源	最大配额（max *max-num*）取值范围
会话数	min (max-num1①/2, 256) - max-num1①
安全域数	1 - max-num2②
策略数	0 - max-num2②
SNAT 规则数	0 - max-num2②
DNAT 规则数	0 - max-num2②

max-num1①: max (capacity * 2/max-vsys-num, capacity/2)

max-num2②: max (capacity * 2/max-vsys-num, capacity/10)

例如：

某设备的系统会话数 Capacity 为 2000000，最多可以配置 100 个 VSYS。当为某 VSYS 设置资源配额时，最大会话数配额的取值范围计算如下： • 参数 max-num1： max (capacity*2/max-vsys-num, capacity/2) = max (2000000*2/100, 2000000/2) = 1000000 • 最大配额的最小值：min (max-num1/2, 256) = min (1000000/2, 256) = 256 所以，最大会话数配额取值范围“min (max-num1/2, 256) - max-num1”为 256 到 1000000。

［命令实例］

hostname(config-vsys-profile)# **session max 100000 reserve 1000**

---

vsys（创建）

创建非根 VSYS。

［命令］

vsys *vsys-name*

no vsys *vsys-name*

［句法描述］

vsys-name	指定 VSYS 名称。范围为 1 到 23 个字符，名称不能为 root（root 为保留名称），且不能包含“\”字符。

［默认取值］

无。

［命令模式］

根 VSYS 的全局配置模式。

［使用指导］

只有根系统 RXW 管理员能够创建非根 VSYS。

［命令实例］

hostname(config)# **vsys vsys-a**

---

vsys（接口）

根系统 RXW 管理员可以将根 VSYS 中的逻辑接口分配到非根 VSYS，也可以将已分配的逻辑接口恢复到根 VSYS。

［命令］

将逻辑接口分配到非根 VSYS：**vsys** *vsys-name*

将已分配的逻辑接口恢复到根 VSYS：**no vsys**

［句法描述］

vsys-name	指定将接口分配到的 VSYS 名称。

［默认取值］

无默认值。

［命令模式］

接口配置模式。

［使用指导］

无。

［命令实例］

hostname(config-if-aggregate1)# **vsys vsys1**

vsys-profile

创建 VSYS Profile。

［命令］

vsys-profile *vsys-profile-name*

no vsys-profile *vsys-profile-name*

［句法描述］

vsys-profile-name	指定 VSYS Profile 的名称。范围为 1 到 31 个字符。

［默认取值］

系统允许最多创建 128 个 VSYS Profile。

根 VSYS 的默认 Profile（root-vsys-profile）和非根 VSYS 的默认 Profile（default-vsys-profile）都不可以被删除和编辑。

删除 VSYS Profile 之前必须删除所有引用该 Profile 的 VSYS。

［命令模式］

根 VSYS 的全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# vsys-profile profile1
hostname(config-vsys-profile)#
```

---

vsys-shared

为根 VSYS 的 VRouter、VSwitch 或者安全域对象配置共享属性。

［命令］

```
vsys-shared
no vsys-shared
```

［句法描述］

无。

［默认取值］

无。

［命令模式］

根 VSYS 的 VRouter 配置模式、VSwitch 配置模式或者安全域配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# vsys-shared
hostname(config-vrouter)# exit
hostname(config)#
```

QoS管理命令

bandwidth

为 QoS Profile 的 class 指定最小带宽。使用该命令 no 的形式取消 class 的最小带宽配置。

［命令］

bandwidth {*bandwidth-value* | **percent** *percentage*} [**schedule** *schedule-name*]

no bandwidth

［句法描述］

bandwidth-name	指定 class 的最小带宽值，单位是 kbps。范围是 32 到 1000000。
percent *percentage*	指定 Class 的最小带宽占接口实际带宽的百分比。取值范围为 1 到 100。
schedule *schedule-name*	指定时间表名称。该条配置将会在时间表指定的时间范围内生效。可配置多次该命令指定多个时间表（最多 8 个）。为避免产生不可预知的问题，建议用户不要配置时间重叠的时间表。

［默认取值］

无。

［命令模式］

QoS Profile 的 Class 配置模式。

［使用指导］

无。

［命令实例］

hostname(config-qos-prof-cmap)# **bandwidth 1024**

class

为 QoS Profile 指定 class，并进入 QoS Profile 的 Class 配置模式。使用该命令 no 的形式从 QoS Profile 中删除指定的 class。

［命令］

class *class-name*

no class *class-name*

［句法描述］

class-name	指定 class 的名称。

［默认取值］

无。

［命令模式］

QoS Profile 配置模式。

［使用指导］

无。

［命令实例］

hostname(config-qos-profile)# **class class1**

class-map

创建指定的 class，并且进入 class 配置模式。如果指定的名称已存在，则直接进入 class 配置模式。使用该命令 no 的形式删除指定的 class。

［命令］

class-map *class-name*

no class-map *class-name*

［句法描述］

class-name	指定 class 的名称。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **class-map class1**

exception-list

配置排除策略。配置后，系统将不对指定流量做 QoS 控制。使用该命令 no 的形式删除排除策略。

［命令］

exception-list {**ip-range** *A.B.C.D A.B.C.D* | **address** *address-entry*}

no exception-list

［句法描述］

ip-range *A.B.C.D A.B.C.D*	指定 IP 地址范围。在该范围内的流量将不做带宽保障和限制。
address *address-entry*	指定地址簿名称。在该范围内的流量将不做带宽保障和限制。

［默认取值］

无。

［命令模式］

QoS Profile 配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **qos-profile ipqos**

hostname (config-qos-profile)# **exception-list ip-range 10.100.6.10 10.100.6.20**

disable

设置 QoS Profile 中的特定 Class 为无效状态。使用该命令 no 的形式恢复 Class 为有效状态。

［命令］

disable

no disable

［句法描述］

无。

［默认取值］

默认情况下，QoS Profile 中配置的所有 Class 都是有效的。

［命令模式］

QoS Profile 的 Class 配置模式。

［使用指导］

设置为无效状态的 Class 仍然存在于所属的 QoS Profile 中。如需从 QoS Profile 中删除特定 Class，请使用 **no class** *class-name* 命令。

［命令实例］

```
hostname(config-qos-prof-cmap)# disable
```

---

flex-qos

开启 Class 的弹性 QoS 功能。使用该命令 no 的形式关闭 Class 的弹性 QoS 功能。

［命令］

flex-qos

no flex-qos

［句法描述］

无。

［默认取值］

无。

［命令模式］

QoS Profile 的 Class 配置模式。

［使用指导］

默认情况下，系统的全局弹性 QoS 功能是关闭的，此时，无论 Class 的弹性 QoS 功能设置为开启还是关闭，它们的弹性 QoS 功能均无效。只有全局弹性 QoS 和 Class 弹性 QoS 均为开启状态时，Class 的弹性 QoS 功能才可生效。

［命令实例］

```
hostname(config-qos-prof-cmap)# flex-qos
```

---

flex-qos low-water-mark

配置全局弹性 QoS 功能。使用该命令 no 的形式关闭弹性 QoS 功能。

［命令］

flex-qos low-water-mark *value* **high-water-mark** *value*

no flex-qos

［句法描述］

low-water-mark *value*	指定最小门限值。范围是 50 到 80。
high-water-mark *value*	指定最大门限值。范围是 81 到 90。

［默认取值］

low-water-mark *value* - 75。

high-water-mark *value* - 85。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **flex-qos low-water-mark 80 high-water-mark 90**

flex-qos max-bandwidth

为 Class 的每个 IP 地址指定带宽上涨的最大限制。使用该命令 no 的形式恢复默认上涨最大限制。

［命令］

flex-qos max-bandwidth *bandwidth*

no flex-qos max-bandwidth

［句法描述］

bandwidth	指定带宽上涨的最大限制，单位为 kbps。取值范围是 64 到 1000000。

［默认取值］

是 IP 配置带宽的 100 倍。

［命令模式］

Class 配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# qos-profile pro1
hostname(config-qos-profile)# class classmap1
hostname(config-qos-prof-cmap)# flex-qos max-bandwidth 2000
```

flex-qos-up-rate

为弹性 QoS 功能指定带宽增加速率。使用该命令 no 的形式恢复默认增长速率。

［命令］

flex-qos-up-rate *rate*

no flex-qos-up-rate

［句法描述］

rate	指定带宽增长速率，单位是倍/分钟。用户使用带宽的增长计算方法为“增长速率*IP 配置带宽”。取值范围为 1 到 16。

［默认取值］

0.5。

［命令模式］

全局配置模式。

［使用指导］

配置的增长速率过大可能导致带宽上下剧烈变化。

［命令实例］

```
hostname(config)# flex-qos-up-rate 1
```

ip-qos

配置基于 IP 的 QoS。使用该命令 no 的形式取消基于 IP 的 QoS 的配置。

［命令］

ip-qos {**shared-bandwidth** | **per-ip**} {**max-bandwidth** *bandwidth* | **reserve-bandwidth** *bandwidth* [**max-bandwidth** *bandwidth*]} [**schedule** *schedule-name*]

no ip-qos {**shared-bandwidth** | **per-ip**} {**max-bandwidth** *bandwidth* | **reserve-bandwidth** *bandwidth* [**max-bandwidth** *bandwidth*]} [**schedule** *schedule-name*]

［句法描述］

shared-bandwidth	范围内的所有 IP 地址共享最大带宽（通过 **max-bandwidth** *bandwidth* 参数配置）或者预留带宽（通过 **reserve-bandwidth** *bandwidth* 参数配置）为指定带宽。
per-ip	指定范围内每一个 IP 地址能够得到的最大带宽（通过 **max-bandwidth** *bandwidth* 参数配置）或者预留带宽（通过 **reserve-bandwidth** *bandwidth* 参数配置）为指定带宽。
max-bandwidth *bandwidth*	指定最大带宽值，即 IP 地址范围内 IP 地址共享（**shared-bandwidth**）或者每个 IP 地址（**per-ip**）可获得的最大带宽值，单位是 kpbs。范围是 32 到 1000000。
reserve-bandwidth *bandwidth*	指定预留带宽值，即 IP 地址范围内 IP 地址共享（**shared-bandwidth**）或者每个 IP 地址（**per-ip**）可获得的预留带宽值，单位是 kpbs，该数值必须小于接口的实际带宽。范围是 32 到 1000000。
schedule *schedule-name*	指定时间表名称。该条配置将会在时间表指定的时间范围内生效。可配置多次该命令指定多个时间表（最多 8 个）。为避免产生不可预知的问题，建议用户不要配置时间重叠的时间表。

［默认取值］

当配置 **reserve-bandwidth** 时，**max-bandwidth** 默认值是 100000。

［命令模式］

QoS Profile 的 Class 配置模式。

［使用指导］

IP 地址范围由 class 的 ip-range 关键字指定。

［命令实例］

hostname(config-qos-prof-cmap)# **ip-qos per-ip max-bandwidth 100**

match address

定义地址条目 IP 地址范围。使用该命令 no 的形式删除定的地址条目匹配条件。

［命令］

match address *address-entry*

no match address *address-entry*

［句法描述］

address-entry	指定地址簿中已配置的地址条目的名称。

［默认取值］

无。

［命令模式］

Class 配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-class-map)# match address address1
```

match application

配置应用类型匹配条件。使用该命令 no 的形式删除指定的应用类型。

［命令］

match application *app-name*

no match application *app-name*

［句法描述］

app-name	指定应用类型的名称。改名称为系统预定义服务和用户自定义服务。

［默认取值］

无。

［命令模式］

Class 配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-class-map)# match application http
```

match cos

定义 CoS 值匹配条件。使用该命令 no 的形式删除指定的 CoS 值匹配条件。

［命令］

match cos *cos-value1* [*cos-value2*] [*cos-value3*] [*cos-value4*]

no match cos *dscp-value1* [*dscp-value2*] [*dscp-value3*] [*dscp-value4*]

［句法描述］

cos-value	指定 802.1Q 的 CoS 值。取值范围为 0 到 7 的整数。一条命令中最多可

	以指定 4 个 CoS 值，所有数值之间为“或”的关系。

［默认取值］

无。

［命令模式］

Class 配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-class-map)# match cos 4
```

match dscp

定义 DSCP 值匹配条件。使用该命令 no 的形式删除指定的 DSCP 值匹配条件。

［命令］

match dscp *dscp-value1* [*dscp-value2*] [*dscp-value3*] [*dscp-value4*]

no match dscp *dscp-value1* [*dscp-value2*] [*dscp-value3*] [*dscp-value4*]

［句法描述］

dscp-value	指定 DSCP 的值。安全网关支持两种 DSCP 值的表达方式，分别是 0 到 63 的数字和 RFC 中预定义的 DSCP 值。一条命令中最多可以指定 4 个 DSCP 值，所有数值之间为“或”的关系。

［默认取值］

无。

［命令模式］

Class 配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-class-map)# match dscp 20 32
```

match ip-range

定义 IP 地址范围匹配条件。使用该命令 no 的形式删除指定的 IP 地址范围匹配条件。

［命令］

match ip-range *start-ip end-ip*

no match ip-range *start-ip end-ip*

［句法描述］

start-ip	指定 IP 地址范围的起始 IP 地址。
end-ip	指定 IP 地址范围的结束 IP 地址。

［默认取值］

无。

［命令模式］

Class 配置模式。

［使用指导］

无。

［命令实例］

hostname(config-class-map)# **match ip-range 192.168.1.1 192.168.1.254**

match policy-qos-tag

定义 QoS 标签匹配条件。使用该命令 no 的形式删除指定的 QoS 标签匹配条件。

［命令］

match policy-qos-tag *tag-value*

no match policy-qos-tag *tag-value*

［句法描述］

tag-value	指定 QoS 标签的值。范围是 1 到 1024。

［默认取值］

无。

［命令模式］

Class 配置模式。

［使用指导］

无。

［命令实例］

hostname(config-class-map)# **match policy-qos-tag 8**

match precedence

定义 IP 优先权匹配条件。使用该命令 no 的形式删除指定的 IP 优先权匹配条件。

［命令］

match precedence *precedence-value1* [*precedence-value2*] [*precedence-value3*] [*precedence-value4*]

no match precedence *precedence-value1* [*precedence-value2*] [*precedence-value3*] [*precedence-value4*]

［句法描述］

precedence-value	指定 IP 优先权值。范围是 0 到 7。一条命令中最多可以指定 4 个 IP 优先权值，所有数值之间为“或”的关系。

［默认取值］

无。

［命令模式］

Class 配置模式。

［使用指导］

无。

［命令实例］

hostname(config-class-map)# **match precedence 2**

match-priority

配置 class 的匹配优先级。使用该命令 no 的形式取消 class 的匹配优先级配置。

［命令］

match-priority *priority-number*

no match-priority

［句法描述］

priority-number	指定 class 的匹配优先级，为 1 到 255 的整数。

［默认取值］

无。

［命令模式］

QoS Profile 的 Class 配置模式。

［使用指导］

1 为最高优先级，依次降低。除 class-default 以外的其它所有 class 的默认优先级是 255。未配置优先级的 class 按照添加到 QoS Profile 中的先后顺序进行匹配；class-default 的优先级是 256，即默认情况下，该 class 具有最低优先级。

［命令实例］

```
hostname(config-qos-prof-cmap)# match-priority 2
```

match role

定义角色/用户/用户组匹配条件。使用该命令 no 的形式删除指定的角色/用户/用户组匹配条件。

［命令］

match {**role** *role-name*| **user** *aaa-server-name user-name* | **user-group** *aaa-server-name user-group-name*}

no match {**role** *role-name*| **user** *aaa-server-name user-name* | **user-group** *aaa-server-name user-group-name*}

［句法描述］

role-name	指定角色名称。
user-name	指定用户名称。
user-group-name	指定用户组名称。
aaa-server-name	指定 AAA 服务器名称。

［默认取值］

无。

［命令模式］

Class 配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-class-map)# match role role1
```

police

配置流量管制功能。使用该命令 no 的形式取消 class 管制功能的配置。

［命令］

police *cir-value* [[*cbs-value*] [*ebs-value*]] **conform-action** {**drop** | **set-dscp-transmit** *dscp-value* | **set-prec-transmit** *precedence-value* | **transmit**} **exceed-action** {**drop** | **set-dscp-transmit** *dscp-value* | **set-prec-transmit** *precedence-value* | **transmit**} [**violate-action** {**drop** | **set-dscp-transmit** *dscp-value* | **set-prec-transmit** *precedence-value* | **transmit**}] [**schedule** *schedule-name*]

no police

［句法描述］

cir-value	指定 CIR，即向令牌桶中放置令牌的速率，单位是 kbps。该数值为 class 的最大带宽限制值，必须小于接口的实际带宽。范围是 32 到 1000000。
cbs-value	指定第一个令牌桶的容量，即 CBS 的大小，单位是字节。该数值必须小于接口的实际带宽。范围是 2048 到 51200000。
ebs-value	指定第二个令牌桶的容量，即 EBS 的大小，单位是字节。该数值必须小于接口的实际带宽。范围是 2048 到 51200000。
conform-action	指定对符合规格数据包所做的操作。
drop	丢弃数据包。
set-dscp-transmit *dscp-value*	为数据包设置 DSCP 值，然后传输数据包。
set-prec-transmit *precedence-value*	为数据包设置 IP 优先权值，然后传输数据包。
transmit	不改变并且传输数据包。
exceed-action	指定对超出数据包所做的操作。可选择操作与 **comform-action** 相同。
violate-action	指定对违约数据包所做的操作。可选择操作与 **comform-action** 相同。
schedule *schedule-name*	指定时间表名称。该条配置将会在时间表指定的时间范围内生效。可配置多次该命令指定多个时间表（最多 8 个）。为避免产生不可预知的问题，建议用户不要配置时间重叠的时间表。

［默认取值］

无。

［命令模式］

QoS Profile 的 Class 配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config -qos-prof-cmap)# police 10000 conform-action set-prec-transmit 2 exceed-action drop
```

priority

配置 class 的低延迟队列。使用该命令 no 的形式取消 class 的低延迟队列配置。

［命令］

priority {*bandwidth-value* | **percent** *percentage*} [*burst-size*] [**schedule** *schedule-name*]

no priority

［句法描述］

bandwidth-value	指定预留带宽，单位是 kbps。范围是 32 到 1000000。该带宽值既是 class 的最小带宽保证。
percent *percentage*	指定预留带宽占接口实际带宽的百分比。取值范围是 1 到 100。
burst-size	指定突发流量大小，单位为字节。范围是 2048 到 51200000。
schedule *schedule-name*	指定时间表名称。该条配置将会在时间表指定的时间范围内生效。可配置多次该命令指定多个时间表（最多 8 个）。为避免产生不可预知的问题，建议用户不要配置时间重叠的时间表。

［默认取值］

无。

［命令模式］

QoS Profile 的 Class 配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config -qos-prof-cmap)# priority 2048
```

qos-profile

创建指定名称的 QoS Profile，并且进入该 QoS Profile 配置模式；如果指定的名称已存在，则直接进入 QoS Profile 配置模式。使用该命令 no 的形式删除指定的 QoS Profile。

［命令］

qos-profile *qos-profile-name*

no qos-profile *qos-profile-name*

［句法描述］

qos-profile-name	指定 QoS Profile 的名称。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **qos-profile profile1**

qos-profile

绑定 QoS Profile 到接口。使用该命令 no 的形式取消 QoS Profile 在指定方向与接口的绑定。

［命令］

qos-profile [**1st-level** | **2nd-level**] {**input** | **output**} *qos-profile-name*

no qos-profile [**1st-level** | **2nd-level**] {**input** | **output**}

［句法描述］

1st-level | **2nd-level**	用于多层 QoS。**1st-level** 为第一层，**2nd-level** 为第二层。
input | **output**	指定 QoS Profile 在绑定到接口的方向，分别为通过该接口流入安全网关的流量上即入方向（**input**），和通过该接口流出安全网关的流量上即出方向（**output**）。
qos-profile-name	指定 QoS Profile 的名称。

［默认取值］

无。

［命令模式］

接口配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-if-eth0/2)# qos-profile input profile1
```

qos-profile（嵌套QoS Profile）

配置嵌套 QoS Profile。使用该命令 no 的形式取消嵌套 QoS Profile 的配置。

［命令］

qos-profile *qos-profile-name*

no qos-profile

［句法描述］

qos-profile-name	指定 QoS Profile 的名称。

［默认取值］

无。

［命令模式］

QoS Profile 的 Class 配置模式。

［使用指导］

- 应用 QoS 可以嵌套 IP QoS Profile 和角色 QoS Profile，不可以嵌套应用 QoS Profile；
- 被嵌套的 IP QoS Profile 和角色 QoS Profile 的带宽共享方式必须为共享方式，并且最多只可包含 7 个 Class（包括默认 Class）；
- IP QoS Profile 和角色 QoS Profile 不可以互相嵌套；
- 被嵌套的应用 QoS Profile 最多可包含 5 个 Class（包括默认 Class）；被嵌套的应用 QoS Profile 的最小带宽保证（bandwidth）和低延迟队列（priority）配置必须为百分比形式。

［命令实例］

```
hostname(config)# qos-profile profile2
hostname(config-qos-profile)# class class1
hostname(config-qos-prof-cmap)# qos-profile
hostname(config-qos-prof-cmap)# qos-profile profile1
```

random-detect

配置 WRED 机制避免拥塞。使用该命令 no 的形式取消 class 的用赛避免功能配置。

［命令］

random-detect [**dscp-based** | **prec-based**]

no random-detect

［句法描述］

dscp-based	指定 WRED 机制根据数据包的 DSCP 值计算其丢弃概率。
prec-based	指定 WRED 机制根据数据包的 IP 优先权值计算其丢弃概率。

［默认取值］

prec-based。

［命令模式］

QoS Profile 的 Class 配置模式。

［使用指导］

无。

［命令实例］

hostname(config-qos-prof-cmap)# **random-detect**

role-qos

配置角色 QoS。使用该命令 no 的形式取消角色 QoS 的配置。

［命令］

role-qos {**share** | **per-user**} {**max-bandwidth** *bandwidth* | **reserve-bandwidth** *bandwidth* [**max-bandwidth** *bandwidth*]} [**schedule** *schedule-name*]

no {**share** | **per-user**} {**max-bandwidth** *bandwidth* | **reserve-bandwidth** *bandwidth* [**max-bandwidth** *bandwidth*]} [**schedule** *schedule-name*]

［句法描述］

share	匹配角色对应的所有用户共享最大带宽（通过 **max-bandwidth** *bandwidth* 参数配置）或者预留带宽（通过 **reserve-bandwidth** *bandwidth* 参数配置）为指定带宽。
per-user	匹配角色对应的每一个用户能够得到的最大带宽（通过 **max-bandwidth** *bandwidth* 参数配置）或者预留带宽（通过 **reserve-bandwidth** *bandwidth* 参数配置）为指定带宽。

max-bandwidth *bandwidth*	指定最大带宽值，即匹配角色对应的所有用户共享（**share**）或者匹配角色对应的每个用户（**per-user**）可获得的最大带宽值，单位是 kpbs。范围是 32 到 1000000。
reserve-bandwidth *bandwidth*	指定预留带宽值，即匹配角色对应的所有用户共享（**shared-bandwidth**）或者匹配角色对应的每个用户（**per-ip**）可获得的预留带宽值，单位是 kpbs，该数值必须小于接口的实际带宽。范围是 32 到 1000000。
schedule *schedule-name*	指定时间表名称。该条配置将会在时间表指定的时间范围内生效。可配置多次该命令指定多个时间表（最多 8 个）。为避免产生不可预知的问题，建议用户不要配置时间重叠的时间表。

［默认取值］

当配置 **reserve-bandwidth** 时，**max-bandwidth** 默认值是 100000。

［命令模式］

QoS Profile 的 Class 配置模式。

［使用指导］

无。

［命令实例］

hostname(config-qos-prof-cmap)# **role-qos share max-bandwidth 12000**

set cos

为 Class 的流量设置 CoS 值。使用该命令 no 的形式取消 Class 的 CoS 值配置。

［命令］

set cos *cos-value*

no set cos

［句法描述］

cos-value	指定 CoS 值。取值范围是 0 到 7 的整数。

［默认取值］

无。

［命令模式］

QoS Profile 的 Class 配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-qos-prof-cmap)# set cos 4
```

set dscp

为 class 的流量设置 DSCP 值。使用该命令 no 的形式取消 class 的 DSCP 值配置。

［命令］

set dscp *dscp-value*

no set dscp

［句法描述］

dscp-value	指定 DSCP 值，可以数字形式（0 到 63）或者关键字形式（例如 af11、cs2 等）。

［默认取值］

无。

［命令模式］

QoS Profile 的 Class 配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-qos-prof-cmap)# set dscp 20
```

set ip-qos-priority

设置 IP QoS 优先级。使用该命令 no 的形式恢复默认 IP QoS 优先级。

［命令］

set ip-qos-priority *number*

no set ip-qos-priority

［句法描述］

number	指定 IP QoS 优先级。取值范围是 1 到 5 的整数。

［默认取值］

3。

［命令模式］

QoS Profile 的 Class 配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-qos-prof-cmap)# set ip-qos-priority 1
```

set precedence

为 class 的流量设置 IP 优先权值。使用该命令 no 的形式取消 class 的 IP 优先权值配置。

［命令］

set precedence *precedence-value*

no set precedence

［句法描述］

precedence-value	指定 IP 优先权值范围是 0 到 7。

［默认取值］

无。

［命令模式］

QoS Profile 的 Class 配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-qos-prof-cmap)# set precedence 1
```

shape

配置 class 的整形功能。使用该命令 no 的形式取消 class 整形功能的配置。

［命令］

shape *cir-value* [[*cbs-value*] [*ebs-value*]] [**schedule** *schedule-name*]

no shape

［句法描述］

cir-value	指定 CIR，即向令牌桶中放置令牌的速率，单位是 kbps。该数值为 class 的最大带宽限制值，必须小于接口的实际带宽。范围是 32 到 1000000。

cbs-value	指定第一个令牌桶的容量，即 CBS 的大小，单位是字节。该数值必须小于接口的实际带宽。范围是 2048 到 51200000。
ebs-value	指定第二个令牌桶的容量，即 EBS 的大小，单位是字节。该数值必须小于接口的实际带宽。范围是 2048 到 51200000。
schedule *schedule-name*	指定时间表名称。该条配置将会在时间表指定的时间范围内生效。可配置多次该命令指定多个时间表（最多 8 个）。为避免产生不可预知的问题，建议用户不要配置时间重叠的时间表。

［默认取值］

无。

［命令模式］

QoS Profile 的 Class 配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-qos-prof-cmap)# shape 2048
```

shaping-for-egress

指定对出接口流量进行整形。该功能适用于 IP QoS 和角色 QoS。使用该命令 no 的形式恢复默认管理操作，即对出接口流量进行管制。

［命令］

shaping-for-egress

no shaping-for-egress

［句法描述］

无。

［默认取值］

默认情况下，系统会对已配置 QoS 功能的出接口流量进行管制。

［命令模式］

QoS Profile 配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-qos-profile)# shaping-for-egress
```

PKI配置命令

crl

配置 CRL 的检查方式。

［命令］

crl {nocheck | optional | required}

［句法描述］

nocheck	安全设备不检查 CRL。该选项为默认选项。
optional	即使 CRL 不可用，安全网关仍然可以接受对端的认证。
required	只有 CRL 可用时，才可以接收对端认证。

［默认取值］

无。

［命令模式］

PKI 信任域配置模式。

［使用指导］

无。

［命令实例］

hostname(config-trust-domain)# **crl optional**

crl configure

进入 CRL 配置模式。

［命令］

crl configure

［句法描述］

无。

［默认取值］

无。

［命令模式］

PKI 信任域配置模式。

［使用指导］

无。

［命令实例］

hostname(config-trust-domain)# **crl configure**

enrollment

为 PKI 信任域指定证书获得方法。使用该命令 no 的形式取消证书获得方法的配置。

［命令］

enrollment {self | terminal}

no enrollment

［句法描述］

self	使用自签名的获得方法。
terminal	使用终端（剪切和粘贴）的获得方法。

［默认取值］

无。

［命令模式］

PKI 信任域配置模式。

［使用指导］

该命令没有默认值，因此，用户必须使用该命令指定一个证书获得方法。

［命令实例］

hostname(config-trust-domain)# **enrollment self**

export pki （PKI信任域信息）

导出 PKI 信任域信息到 FTP 服务器、TFTP 服务器或者 U 盘。

［命令］

export pki *trust-domain-name* **pkcs12** *password* **to ftp server** *ip-address* [**user** *user-name* **password** *password* [*file-name*] | *file-name*]

export pki *trust-domain-name* **pkcs12** *password* **to tftp server** *ip-address* [*file-name*]

export pki *trust-domain-name* **pkcs12** *password* **to** {**usb0** | **usb1**} [*file-name*]

［句法描述］

trust-domain-name	指定 PKI 信任域的名称。
pkcs12 *password*	指定私钥保护口令，用于解密私钥。
ip-address	指定 FTP 服务器或者 TFTP 服务器的 IP 地址。
user *user-name* **password** *password*	指定访问 FTP 服务器使用的用户名和密码。
file-name	指定导出的 PKI 信任域信息的文件名称。
usb0 | **usb1**	指定将文件通过 **usb0** 或者 **usb1** 导出到 U 盘根目录。

［默认取值］

无。

［命令模式］

执行模式。

［使用指导］

无。

［命令实例］

hostname# **export pki trust_domain_default pkcs12 hill2345 to ftp server 10.101.1.0 user user1 password 1111**

hostname# **export pki trust_domain_default pkcs12 hill2345 to tftp server 10.1.1.1**

hostname# **export pki trust_domain_default pkcs12 hill2345 to usb0**

export pki （本地证书）

导出本地证书到 FTP 服务器、TFTP 服务器或者 U 盘。

［命令］

export pki *trust-domain-name* **cert to ftp server** *ip-address* [**user** *user-name* **password** *password* [*file-name*] | *file-name*]

export pki *trust-domain-name* **cert to tftp server** *ip-address* [*file-name*]

export pki *trust-domain-name* **cert to** {**usb0** | **usb1**} [*file-name*]

［句法描述］

trust-domain-name	指定 PKI 信任域的名称。

ip-address	指定 FTP 服务器或者 TFTP 服务器的 IP 地址。
user *user-name* **password** *password*	指定访问 FTP 服务器使用的用户名和密码。
file-name	指定导出的本地证书文件名称。
usb0 | **usb1**	指定将文件通过 **usb0** 或者 **usb1** 导出到 U 盘根目录。

［默认取值］

无。

［命令模式］

执行模式。

［使用指导］

无。

［命令实例］

hostname# **export pki trust_domain_default cert to ftp server 10.101.1.0 user user1 password 1111**

hostname# **export pki trust_domain_default cert to tftp server 10.1.1.1**

hostname# **export pki trust_domain_default cert to usb0**

import pki （PKI信任域信息）

通过 FTP 服务器、TFTP 服务器或者 U 盘导入 PKI 信任域信息。

［命令］

import pki *trust-domain-name* **pkcs12** *password* **from ftp server** *ip-address* {**user** *user-name* **password** *password file-name* | *file-name*}

import pki *trust-domain-name* **pkcs12** *password* **from tftp server** *ip-address file-name*

import pki *trust-domain-name* **pkcs12** *password* **from** {**usb0** | **usb1**} *file-name*

［句法描述］

trust-domain-name	指定 PKI 信任域的名称。
pkcs12 *password*	指定私钥保护口令，用于解密私钥。
ip-address	指定 FTP 服务器或者 TFTP 服务器的 IP 地址。
user *user-name* **password** *password*	指定访问 FTP 服务器使用的用户名和密码。
file-name	指定导入的 PKI 信任域信息的文件名称。

usb0 | usb1	指定通过 USB 方式从 **usb0** 或者 **usb1** 插槽所对应的 U 盘根目录获取文件。

［默认取值］

无。

［命令模式］

执行模式。

［使用指导］

无。

［命令实例］

hostname# **import pki trust_domain_default pkcs12 hill2345 from ftp server 10.101.1.0 user user1 password 1111 pki_trust_domain_file**

hostname# **export pki trust_domain_default pkcs12 hill2345 from tftp server 10.1.1.1 pki_trust_domain_file**

hostname# **export pki trust_domain_default pkcs12 hill2345 from usb0 pki_trust_domain_file**

import pki （本地证书）

通过 FTP 服务器、TFTP 服务器或者 U 盘导入本地证书。

［命令］

import pki *trust-domain-name* **cert from ftp server** *ip-address* {**user** *user-name* **password** *password file-name* | *file-name*}

import pki *trust-domain-name* **cert from tftp server** *ip-address file-name*

import pki *trust-domain-name* **cert from** {**usb0** | **usb1**} *file-name*

［句法描述］

trust-domain-name	指定 PKI 信任域的名称。
ip-address	指定 FTP 服务器或者 TFTP 服务器的 IP 地址。
user *user-name* **password** *password*	指定访问 FTP 服务器使用的用户名和密码。
file-name	指定导入的本地证书文件名称。
usb0 | usb1	指定通过 USB 方式从 **usb0** 或者 **usb1** 插槽所对应的 U 盘根目录获取文件。

［默认取值］

无。

［命令模式］

执行模式。

［使用指导］

无。

［命令实例］

hostname# **import pki trust_domain_default cert from ftp server 10.101.1.0 user user1 password 1111 cert_file**

hostname# **export pki trust_domain_default cert from tftp server 10.1.1.1 pki_ cert_file**

hostname# **export pki trust_domain_default cert from usb0 cert_file**

---

keypair

为 PKI 信任域指定密钥对。使用该命令 no 的形式取消密钥对的指定。

［命令］

keypair *key-name*

no keypair

［句法描述］

key-name	指定密钥对的名称。

［默认取值］

无。

［命令模式］

PKI 信任域配置模式。

［使用指导］

无。

［命令实例］

hostname(config-trust-domain)# **keypair dsa-key1**

---

pki authenticate

为 PKI 信任域下载证书撤销列表（CRL）。

［命令］

pki crl request *trust-domain-name*

［句法描述］

trust-domain-name	指定 PKI 信任域的名称。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **pki crl request domain1**

pki crl request

生成证书服务请求。

［命令］

pki enroll *trust-domain-name*

［句法描述］

trust-domain-name	指定 PKI 信任域的名称。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **pki enroll domain1**

pki enroll

生成证书服务请求。

［命令］

pki enroll *trust-domain-name*

［句法描述］

trust-domain-name	指定 PKI 信任域的名称。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **pki enroll domain1**

pki export

导出 PKI 信任域的证书及密钥。

［命令］

pki export *trust-domain-name* **pkcs12** *pass-phrase*

［句法描述］

trust-domain-name	指定 PKI 信任域的名称。
pass-phrase	指定用于解密 PKCS12 数据的密码。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **pki export domain1 pkcs12 ghakjohn56**

pki import

安装本地证书。

［命令］

pki import *trust-domain-name* **certificate**

［句法描述］

trust-domain-name	指定 PKI 信任域的名称。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

执行该命令后，系统提示用户将证书内容拷贝到指定的位置，然后输入句点（.）并敲回车，系统将开始安装证书。

［命令实例］

hostname(config)# **pki import domain1 certificate**

pki import pkcs12

导入 PKI 信任域的证书及密钥。

［命令］

pki import *trust-domain-name* **pkcs12** *pass-phrase*

［句法描述］

trust-domain-name	指定 PKI 信任域的名称。
pass-phrase	指定用于解密 PKCS12 数据的密码。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# pki import domain1 pkcs12 ghakjohn56
```

pki key generate

创建 PKI 密钥对。

［命令］

pki key generate {rsa | dsa} {label *key-name*} [**modulus** *size*] [**noconfirm**]

［句法描述］

rsa | dsa	指定密钥对的类型，RSA 或者 DSA。
label *key-name*	指定密钥对的名称。该名称在系统中必须是唯一的。
modulus *size*	指定密钥对的模长，单位为比特。可选项有 1024（系统默认值）、2048、512 和 768。
noconfirm	禁止关于该密钥对的提示信息。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# pki key generate dsa label dsa-key1 noconfirm
```

pki key zeroize

删除已有的 PKI 密钥。

［命令］

pki key zeroize {default | label *key-name*} [**noconfirm**]

［句法描述］

default | label *key-name*	指定被删除密钥。**default** 为删除系统默认密钥（Default-Key），**label** *key-name* 为删除指定名称的密钥。
noconfirm	禁止该密钥对的提示信息。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **pki key zeroize label dsa-key1**

---

pki key zeroize noconfirm

禁止所有密钥对的提示信息。

［命令］

pki key zeroize noconfirm

［句法描述］

无。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **pki key zeroize noconfirm**

---

pki trust-domain

生成指定名称的 PKI 信任域并且进入 PKI 信任域配置模式；如果指定的名称已存在，则直接进入 PKI 信任域配置模式。使用该命令 no 的形式删除指定的 PKI 信任域。

［命令］

pki trust-domain *trust-domain-name*

no pki trust-domain *trust-domain-name*

［句法描述］

trust-domain-name	指定 PKI 信任域的名称。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **pki trust-domain domain1**

subject commonname

为 PKI 信任域配置普通名称。使用该命令 no 的形式取消普通名称的配置。

［命令］

subject commonname *string*

no subject commonname

［句法描述］

string	指定普通名称。

［默认取值］

无。

［命令模式］

PKI 信任域配置模式。

［使用指导］

无。

［命令实例］

hostname(config-trust-domain)# **subject commonname commonname1**

subject country

为 PKI 信任域配置国家名称（可选）。使用该命令 no 的形式取消国家名称的配置。

［命令］

subject country *string*

no subject country

［句法描述］

string	指定国家名称。只能包含两个字符。

［默认取值］

无。

［命令模式］

PKI 信任域配置模式。

［使用指导］

无。

［命令实例］

hostname(config-trust-domain)# **subject country cn**

subject localityname

为 PKI 信任域配置所在位置（可选）。使用该命令 no 的形式取消所在位置的配置。

［命令］

subject localityname *string*

no subject localityname

［句法描述］

string	指定所在位置。

［默认取值］

无。

［命令模式］

PKI 信任域配置模式。

［使用指导］

无。

［命令实例］

hostname(config-trust-domain)# **subject localityname beijing**

subject organization

为 PKI 信任域配置机构名称（可选）。使用该命令 no 的形式取消机构名称的配置。

［命令］

subject organization *string*

no subject organization

［句法描述］

string	指定机构名称。

［默认取值］

无。

［命令模式］

PKI 信任域配置模式。

［使用指导］

无。

［命令实例］

hostname(config-trust-domain)# **subject organization hillstone**

subject organizationunit

为 PKI 信任域配置机构单元（可选）。使用该命令 no 的形式取消机构单元的配置。

［命令］

subject organizationunit *string*

no subject organizationunit

［句法描述］

string	指定机构单元。

［默认取值］

无。

［命令模式］

PKI 信任域配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-trust-domain)# subject organizationunit unit1
```

subject stateorprovincename

为 PKI 信任域配置州或省名称（可选）。使用该命令 no 的形式取消州或省名称的配置。

［命令］

subject stateorprovincename *string*

no subject stateorprovincename

［句法描述］

string	指定州或省名称。

［默认取值］

无。

［命令模式］

PKI 信任域配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-trust-domain)# subject stateorprovincename state1
```

url

配置 CRL 的 URL 信息。

［命令］

url *index url*

［句法描述］

index	为 URL 指定排序指数。系统最多支持 3 个 URL，并且最先使用指数为 1 的 URL。
url	指定获得 CRL 信息的 URL。

［默认取值］

无。

［命令模式］

CRL 配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config-crl)# url 2 url1
```

高可靠性命令

arp

指定升级为主设备的设备向外发送 ARP 包的个数。使用该命令 no 的形式恢复发送 ARP 包个数的默认值。

［命令］

arp *number*

no arp

［句法描述］

number	指定发送 ARP 请求包的个数。范围是 1 到 8。

［默认取值］

5。

［命令模式］

HA 组配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# ha group 0
hostname(config-ha-group)# arp 4
```

description

为设备指定描述信息。使用该命令 no 的形式取消描述信息的指定。

［命令］

description *string*

no description

［句法描述］

string	指定描述信息内容。

［默认取值］

无。

［命令模式］

HA 组配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# ha group 0
hostname(config-ha-group)# description aaaaaa
```

---

exec ha sync

手动同步 HA 信息。

［命令］

exec ha sync { configuration | file *file-name* **| rdo {arp | dns | dhcp | mac | pki | session | vpn | webauth | ntp | scvpn | l2tp | route}}**

［句法描述］

无。

［默认取值］

无。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# exec ha sync rdo webauth
```

---

ha cluster

为设备配置 HA 簇，同时开启设备的 HA 功能。使用该命令 no 的形式关闭设备的 HA 功能。

［命令］

ha cluster *cluster-id*

no ha cluster

［句法描述］

cluster-id	指定 HA 簇 ID。范围是 1 到 7。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

如果网络中存在多对 HA 设备，用户需要为它们配置不同的 HA 簇 ID，否则可能出现 MAC 地址冲突现象。

［命令实例］

hostname(config)# **ha cluster 1**

ha group

进入 HA 组配置模式。使用该命令 no 的形式删除指定的 HA 组。

［命令］

ha group *group-id*

no ha group *group-id*

［句法描述］

group-id	指定 HA 组的 ID。范围是 0 到 7。当前版本用户只可以将 ID 指定为 0。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

ID 为 0 的 HA 组不可以被删除。

［命令实例］

hostname(config)# **ha group 0**

hostname(config-ha-group)#

ha link interface

配置 HA 连接接口用于主备设备之间 HA 同步信息以及 Hello 报文的传输。使用该命令 no 的形式删除对指定接口的 HA 连接接口的配置。

［命令］

ha link interface *interface-name*

no ha link interface *interface-name*

［句法描述］

interface-name	指定接口名称。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

当先配置的 HA 连接接口断开连接，后配置的 HA 连接接口会继续传输 HA 报文。

［命令实例］

hostname(config)# **ha link interface ethernet0/2**

ha link ip

为 HA 连接接口配置 IP 地址。使用该命令 no 的形式取消 HA 连接接口 IP 地址的配置。

［命令］

ha link ip *ip-address*

no ha link ip

［句法描述］

ip-address	指定 HA 连接接口的 IP 地址。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# ha link ip 1.1.1.1 255.255.255.0
```

hello interval

指定 Hello 报文间隔。Hello 报文间隔指 HA 设备向 HA 组中的其它设备发送心跳（Hello 报文）的时间间隔。使用该命令 no 的形式恢复时间间隔的默认值。

［命令］

hello interval *time-interval*

no hello interval

［句法描述］

time-interval	指定发送心跳的时间间隔，单位为毫秒。范围是 50 到 10000 毫秒。

［默认取值］

1000 毫秒。

［命令模式］

HA 组配置模式。

［使用指导］

同一个 HA 组的设备的 Hello 报文间隔时间必须相同。

［命令实例］

```
hostname(config)# ha group 0
hostname(config-ha-group)# hello interval 1500
```

hello threshold

指定失去心跳的警戒值，即如果设备没有收到对方设备的该命令指定个数的 Hello 报文，就判断对方无心跳。使用该命令 no 的形式恢复警戒值的默认值。

［命令］

hello threshold *value*

no hello threshold

［句法描述］

value	定失去心跳的警戒值。范围是 3 到 255。

［默认取值］

3。

［命令模式］

HA 组配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# ha group 0
hostname(config-ha-group)# hello threshold 10
```

interface

配置 HA 组 1 接口。使用该命令 no 的形式删除指定接口。

［命令］

interface {**ethernet***x/y*:*z* | **redundant***x:z* | **aggregate***x*:*z* | **tunnel***x*:*z* | **loopback***x*:*z* | **ethernet***x/y.u*:*z* | **redundant***x.y*:*z* | **aggregate***x.y*:*z*}

no interface {**ethernet***x/y*:*z* | **redundant***x:z* | **aggregate***x*:*z* | **tunnel***x*:*z* | **loopback***x*:*z* | **ethernet***x/y.u*:*z* | **redundant***x.y*:*z* | **aggregate***x.y*:*z*}

［句法描述］

ethernet*x/y*:*z*	指定以太网接口 ethernetx/y 作为组 z 接口，用于转发数据。
redundant*x:z*	指定冗余接口 redundantx 作为组 z 接口，用于转发数据。
aggregate*x*:*z*	指定集聚接口 aggregatex 作为组 z 接口，用于转发数据。
tunnel*x*:*z*	指定隧道接口 x 作为组 z 接口，用于转发数据。
loopback*x*:*z*	指定回环接口 loopbackx 作为组 z 接口，用于转发数据。
ethernet*x/y.u*:*z*	指定以太网子接口 ethernetx/y.u 作为组 z 接口，用于转发数据。
redundant*x.y*:*z*	指定冗余子接口 redundantx.y 作为组 z 接口，用于转发数据。
aggregate*x.y*:*z*	指定集聚子接口 aggregatex.y 作为组 z 接口，用于转发数据。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

当前版本用户只可以将组 z 的值指定为 1。

［命令实例］

```
hostname(config)# interface ethernet0/2:1
```

manage ip

为设备配置管理 IP。

［命令］

manage ip *ip-address*

［句法描述］

ip-address	指定管理 IP 地址。

［默认取值］

无。

［命令模式］

接口配置模式。

［使用指导］

管理 IP 能够实现对 HA 备份设备的管理。

［命令实例］

```
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# manage ip 192.168.3.1
```

monitor track

为设备指定监测对象，监控设备的工作状态。使用该命令 no 的形式取消监控配置。

［命令］

monitor track *track-object-name*

no monitor track

［句法描述］

track-object-name	指定系统中已配置的监测对象的名称。

［默认取值］

无。

［命令模式］

HA 组配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# ha group 0
hostname(config-ha-group)# hello interval 1500
```

preempt

指定设备的抢占模式。

［命令］

preempt [*delay-time*]

no preempt

［句法描述］

delay-time	指定延迟时间，单位为秒。范围是 1 到 600 秒。

［默认取值］

3 秒。

［命令模式］

HA 组配置模式。

［使用指导］

如果将设备配置为抢占模式，一旦设备发现自己的优先级高于主设备，就会将自己升级为主设备，而原先的主设备将变为备份设备；如果将设备设置为非抢占模式，即使设备的优先级高于主设备，它也只能在主设备故障时代替主设备工作。

［命令实例］

```
hostname(config)# ha group 0
hostname(config-ha-group)# hello preempt
```

priority

指定设备优先级用于 HA 选举。优先级高（数字小）的会被选举为主设备。使用该命令 no 的形式恢复优先级的默认值。

［命令］

priority *number*

no priority

［句法描述］

number	指定优先级。范围是 1 到 254 的整数。

［默认取值］

100。

［命令模式］

HA 组配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# ha group 0
hostname(config-ha-group)# priority 50
```

病毒过滤命令

anti-malicious-sites

开启防恶意网站功能。使用该命令 no 的形式关闭防恶意网站功能。

［命令］

anti-malicious-sites

no anti-malicious-sites

［句法描述］

无。

［默认取值］

开启。

［命令模式］

病毒过滤 Profile 配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **av-profile av-test**

hostname(config-av-profile)# **anti-malicious-sites**

av enable

绑定病毒过滤 Profile 到安全域。使用该命令 no 的形式取消病毒过滤 Profile 与安全域的绑定。

［命令］

av enable *av-profile-name*

no av enable

［句法描述］

av-profile-name	指定绑定到安全域的病毒过滤 Profile 的名称。一个安全域只能绑定一个病毒过滤 Profile。

［默认取值］

无。

［命令模式］

安全域配置模式。

［使用指导］

当策略规则已经绑定了病毒过滤 Profile，同时策略的目的安全域也绑定了病毒过滤 Profile，策略规则绑定的病毒过滤 Profile 将会生效，而目的安全域绑定的病毒过滤 Profile 无效。

［命令实例］

```
hostname(config)# zone trust
hostname(config-zone-trust)# av enable av-test
```

av max-decompression-recursion

配置压缩嵌套层数以及动作。

［命令］

av max-decompression-recursion *number* **exceed-action** {**log-only** | **reset-conn**}

no av max-decompression-recursion

［句法描述］

number	指定压缩嵌套层数。范围是 1 到 5。
log-only | **reset-conn**	指定对超出限制的压缩文件的处理动作，可以是产生日志信息（**log-only**）和断开连接（**reset-conn**）。默认动作为 **log-only**。

［默认取值］

number - 5

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# av max-decompression-recursion 3 exceed-action
reset-conn
```

av-profile

创建病毒过滤 Profile 并进入病毒过滤 Profile 配置模式。如果指定的病毒过滤 Profile 已存在，则直接进入病毒过滤 Profile 配置模式。使用该命令 no 的形式删除指定的病毒过滤 Profile。

［命令］

av-profile *av-profile-name*

no av-profile *av-profile-name*

［句法描述］

av-profile-name	指定所创建病毒过滤 Profile 的名称。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# av-profile av-test
hostname(config-av-profile)#
```

av signature update mode

配置病毒库更新方式。使用该命令 no 的形式恢复默认更新方式。

［命令］

av signature update mode {auto | manual}

no av signature update mode

［句法描述］

auto	指定自动更新病毒库。
manual	指定手动更新病毒库。

［默认取值］

auto

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **av signature update mode manual**

av signature update schedule

指定病毒库更新的频率和时间。

［命令］

av signature update schedule {daily | weekly {mon | tue | wed | thu | fri | sat | sun}} [*HH:MM*]

［句法描述］

daily	指定频率为每天更新。
**weekly {mon	tue	wed	thu	fri	sat	sun}**	指定频率为每周更新。**mon	tue	wed	thu	fri	sat	sun** 用来指定每周更新的日期。
HH:MM	指定更新的时间，例如 09：00。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

默认情况下，StoneOS 采用自动模式每日更新病毒库，并且为避免服务器流量过大，每日更新时间是随机的。

［命令实例］

hostname(config)# **av signature update schedule daily 13:30**

av signature update server

配置病毒库更新服务器下载最新病毒库特征。使用该命令 no 的形式取消更新服务器的指定。

［命令］

av signature update {server1 | server2 | server3} {*IP-address* | *domain-name*}

no av signature update {server1 | server2 | server3}

［句法描述］

server1 | server2 | server3	指定将要配置的服务器。
ip-address | *domain-name*	指定更新服务器的名称，可以是 IP 地址形式（*IP-address*）也可以是域名形式（*domain-name*，例如 update1.hillstonenet.com）。

［默认取值］

server1：update1.hillstonenet.com

server2：update2.hillstonenet.com

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **av signature update server2 update2.hillstonenet.com**

exec av

开启或者关闭系统的病毒过滤功能。

［命令］

exec av {enable | disable}

［句法描述］

enable	开启系统的病毒过滤功能。
disable	关闭系统的病毒过滤功能。

［默认取值］

开启。

［命令模式］

任何模式。

［使用指导］

用户可通过 show version 命令查看系统的病毒过滤功能是否开启。

［命令实例］

hostname# **exec av enable**

---

exec av signature update

立即更新病毒库。

［命令］

exec av signature update [full]

［句法描述］

exec av signature update	仅对当前病毒库与更新服务器最新发布病毒库的不同部分进行更新。
exec av signature update full	从更新服务器获取完整的最新发布病毒库信息进行更新。

［默认取值］

无。

［命令模式］

任何模式。

［使用指导］

无论更新模式为手动还是自动，用户都可以随时使用该命令更新病毒库。

［命令实例］

hostname# **exec av signature update**

---

file-type

指定病毒扫描文件类型。使用该命令 no 的形式取消文件类型的指定。

［命令］

file-type {bzip2 | cryptff | gzip | html | jpeg | mail | pe | rar | riff | tar | zip}

no file-type {bzip2 | cryptff | gzip | html | jpeg | mail | pe | rar | riff | tar | zip}

［句法描述］

bzip2	指定对 BZIP2 压缩文件进行病毒扫描。
cryptff	指定对 CryptFF 类型文件进行病毒扫描。
gzip	指定对 GZIP 压缩文件进行扫描。
html	指定对 HTML 类型文件进行病毒扫描。
jpeg	指定对 JPEG 类型文件进行扫描。
mail	指定对 mail 类型文件进行病毒扫描。
pe	指定对 PE 类型文件进行扫描。PE 即 Portable Executable（可移植的执行体）的缩写。它是 Win32 环境自身所带的执行体文件格式。可移植的执行体意味着此文件格式是跨 Win32 平台的：即使 Windows 运行在非 Intel 的 CPU 上，任何 Win32 平台的 PE 装载器都能识别和使用该文件格式。
rar	指定对 RAR 压缩文件进行病毒扫描。
riff	指定对 RIFF 类型文件进行扫描。RIFF 即 Resource Interchange File Format（资源交换文件格式）的缩写。是微软为 Windows 设计的一类多媒体文件格式，主要包括 WAV 和 AVI 两种。
tar	指定对 TAR 压缩文件进行病毒扫描。
zip	指定对 ZIP 压缩文件进行病毒扫描。

［默认取值］

无。

［命令模式］

病毒过滤配置模式。

［使用指导］

使用多条该命令可指定多个文件类型。

［命令实例］

```
hostname(config)# av-profile av-test
hostname(config-av-profile)# file-type http
```

import av signature

引入病毒特征文件。

［命令］

import av signature from {ftp server *IP-address* **[user** *user-name* **password** *password*] **| tftp server** *IP-address* **| usb0 | usb1}** *file-name*

［句法描述］

IP-address	指定 FTP 或者 TFTP 服务器的 IP 地址。
user *user-name*	指定 FTP 服务器的用户名和密码。

password *password*	
usb0 | usb1	指定 USB 接口。
file-name	指定导入的病毒特征文件的名称。

［默认取值］

无。

［命令模式］

执行模式。

［使用指导］

在某些情况下，用户设备可能无法连接到更新服务器对病毒库进行更新，针对这一问题，StoneOS 提供病毒特征文件引入功能，即通过 FTP、TFTP 服务器或者 U 盘将病毒特征文件引入到设备，从而更新设备的病毒库。

［命令实例］

hostname(config)# **import av signature from tftp server 192.168.1.1 signature-file**

label-mail

开启标签邮件功能。使用该命令 no 的形式关闭标签邮件功能。

［命令］

label-mail

no label-mail

［句法描述］

无。

［默认取值］

关闭。

［命令模式］

病毒过滤配置模式。

［使用指导］

对通过 SMTP 协议传输的邮件进行病毒扫描，用户可以对发出的电子邮件开启标签邮件功能，即系统对邮件及其附件进行扫描，扫描病毒的结果会包含在邮件的主体中，随邮件一起发送。

［命令实例］

hostname(config-av-profile)# **label-mail**

mail-sig

在开启标签邮件功能后，配置邮件的签名。使用该命令 no 的形式恢复默认值。

［命令］

mail-sig *signature-string*

no mail-sig

［句法描述］

无。

［默认取值］

Checked by Hillstone AntiVirus

［命令模式］

病毒过滤配置模式。

［使用指导］

邮件签名不支持中文签名。

［命令实例］

hostname(config-av-profile)# **mail-sig “Checked by Mail AntiVirus”**

protocol-type

指定病毒扫描协议类型。使用该命令 no 的形式取消协议类型的指定

［命令］

protocol-type {{ftp | imap4 | pop3 | smtp} [action {fill-magic | log-only | reset-conn}] | http [action {fill-magic | log-only | reset-conn | warning}]}

no protocol-type {{ftp | imap4 | pop3 | smtp} [action {fill-magic | log-only | reset-conn}] | http [action {fill-magic | log-only | reset-conn | warning}]}

［句法描述］

ftp	指定对通过 FTP 协议传输的信息进行病毒扫描。
http	指定对通过 HTTP 协议传输的信息进行病毒扫描。
imap4	指定对通过 IMAP4 协议传输的信息进行病毒扫描。
pop3	指定对通过 POP3 协议传输的邮件进行病毒扫描。

smtp	指定对通过 SMTP 协议传输的邮件进行病毒扫描。
action {fill-magic | log-only | reset-conn}	指定对发现病毒的协议采取的动作： • **fill-magic** – 使用文件填充的方式处理病毒文件，即从文件中被病毒感染部分的起始位置起使用魔术字（Virus is found, cleaned）进行填充，一直到被感染部分结束。 • **log-only** – 产生日志信息。该选项为系统的默认选项。 • **reset-conn** – 发现病毒后，重置病毒连接。

［默认取值］

无。

［命令模式］

病毒过滤配置模式。

［使用指导］

使用多条该命令可指定多个协议类型。

［命令实例］

```
hostname(config)# av-profile av-test
hostname(config-av-profile)# protocol-type ftp action fill-magic
```

IPS命令

attack-level

为特征集中不同安全级别的特征配置对应的操作。使用该命令 no 的形式恢复默认配置。

［命令］

attack-level {critical | warning | info} {[action {reset | log}] [block {ip | service} *timeout*]}

no attack-level {critical | warning | info}

［句法描述］

critical | warning | info	指定安全级别，可以是严重（**critical**）、警告（**warning**）或者信息（**info**）。
reset | log	为不同安全级别的特征指定相应的动作： • **reset**：发现入侵攻击后重置连接（TCP）或者发送目标不可达包（UDP）并且记录日志信息。 • **log**：发现入侵攻击后仅记录日志信息。
ip | service	指定阻断攻击者 IP（**ip**）或者服务（**service**）。
timeout	指定对攻击者 IP 或者服务进行阻断的时长，单位为秒，范围是 60 到 3600 秒。

［默认取值］

所有级别的特征对应的默认动作都是 **log**。

默认情况下不对攻击者的 IP 或者服务进行阻断。

［命令模式］

特征集配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# ips sigset http1 template http
hostname(config-http-sigset)# attack-level critical action reset
block ip 120
```

banner-protect enable

开启服务器（FTP、Web、POP3、SMTP）banner 信息保护功能并设置新信息替换原有服务器 banner 信息。使用该命令 no 的形式关闭服务器的 banner 保护功能。

［命令］

banner-protect enable replace-with *string*

no banner-protect enable

［句法描述］

string	指定 banner 信息。

［默认取值］

无。

［命令模式］

特征集配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# ips sigset test template ftp
hostname(config-ftp-sigset)# banner-protect enable replace-with
vsftp2.0
```

brute-force auth

为特征集开启暴力破解功能并对该功能进行配置。使用该命令 no 的形式关闭暴力破解功能。

［命令］

brute-force auth *times* **block {ip | service}** *timeout*

no brute-force auth

［句法描述］

times	指定允许的一分钟内认证/登录失败的次数。取值范围是 1 到 100000。
ip | service	指定对超出限定认证/登录失败频率的攻击者的 IP 地址（**ip**）或者服务（**service**）进行阻断。
timeout	指定对攻击者 IP 或者服务进行阻断的时长，单位为秒，范围是 60 到 3600 秒。

［默认取值］

无。

［命令模式］

特征集配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# ips sigset test1 template telnet
hostname(config-telnet-sigset)# brute-force auth 10 block service 120
```

brute-force lookup

为特征集开启暴力查找功能并对该功能进行配置。使用该命令 no 的形式关闭暴力查找功能。

［命令］

brute-force lookup *times* **block** {**ip** | **service**} *timeout*

no brute-force lookup

［句法描述］

times	指定允许的一分钟内查询的次数。取值范围是 1 到 100000。
ip | **service**	指定对超出限定查询频率的攻击者的 IP 地址（**ip**）或者服务（**service**）进行阻断。
timeout	指定对攻击者 IP 或者服务进行阻断的时长，单位为秒，范围是 60 到 3600 秒。

［默认取值］

无。

［命令模式］

特征集配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# ips sigset msrpc-cus template msrpc
hostname(config-msrpc-sigset)# brute-force lookup 20 block service 120
```

command-injection-check

为系统开启 HTTP 协议命令注入攻击检测功能。使用该命令 no 的形式关闭该功能。

［命令］

command-injection-check enable

no command-injection-check enable

［句法描述］

无。

［默认取值］

无。

［命令模式］

特征集配置模式。

［使用指导］

命令注入攻击事件为“严重”级别事件，检测出 SQL 注入攻击后，系统将按照攻击特征所在特征集中安全级别动作操作对流量进行处理。

［命令实例］

```
hostname(config)# ips sigset http1 template http
hostname(config-http-sigset)# command-injection-check enable
```

---

deny-method

指定系统拒绝的 HTTP 方法，并指定安全级别。使用该命令 no 的形式允许指定的 HTTP 方法。

［命令］

deny-method {connect | delete | get | head | options | post | put | trace | webdav}

no deny-method {connect | delete | get | head | options | post | put | trace | webdav}

［句法描述］

connect | delete | get | head | options | post | put | trace | webdav	指定拒绝/允许的 HTTP 方法。

［默认取值］

默认情况下，所有方法都是允许的。

［命令模式］

特征集配置模式。

［使用指导］

当系统发现请求方法不允许时，将直接断开连接。

［命令实例］

```
hostname(config)# ips sigset http1 template http
hostname(config-http-sigset)# deny-method post
```

exec block-ip remove

删除被阻断 IP 的记录信息。

［命令］

exec block-ip remove {all | ip *ip-address* [**vrouter** *vr-name*]**}**

［句法描述］

all	删除当前系统中存在的所有被阻断 IP 的信息。
ip *ip-address*	删除指定 IP 地址的阻断记录信息。
vr-name	指定 IP 地址所在的 VRouter 的名称。

［默认取值］

vr-name – trust-vr

［命令模式］

执行模式。

［使用指导］

无。

［命令实例］

```
hostname# exec block-ip remove ip 100.10.10.1
```

exec block-service remove

删除被阻断服务的记录信息。

［命令］

exec block-service remove {**all** | **src-ip** *src-ip-address* **dst-ip** *dst-ip-address* [**vrouter** *vr-name*] **dst-port** *port-number* **proto** *protocol*}

［句法描述］

all	删除当前系统中存在的所有被阻断服务的信息。
src-ip *src-ip-address* **dst-ip** *dst-ip-address* [**vrouter** *vr-name*] **dst-port** *port-number* **proto** *protocol*	删除指定服务的阻断记录信息： • **src-ip** *src-ip-address*：指定服务的源 IP 地址。 • **dst-ip** *dst-ip-address*：指定服务的目的 IP 地址。 • **vrouter** *vr-name*：指定 VRouter 名称。 • **dst-port** *port-number*：指定服务的目的端口号，范围是 1 到 65535。 • **proto** *protocol*:指定服务的协议，范围是 1 到 255。

［默认取值］

vr-name – trust-vr

［命令模式］

执行模式。

［使用指导］

无。

［命令实例］

hostname# **exec block-service remove all**

exec ips

开启/关闭系统的 IPS 功能。

［命令］

开启：**exec ips enable**

关闭：**exec ips disable**

［句法描述］

无。

［默认取值］

无。

［命令模式］

执行模式。

［使用指导］

- 该命令仅在安装有 IPS 许可证的平台有效。
- 执行 **exec ips enable** 命令后，需要重启设备才能开启 IPS 功能。
- 开启 IPS 功能后，系统支持的最大并发连接数会减少。执行 **exec ips disable** 命令后，IPS 功能立即被禁用，但是最大并发连接数仍保持减少后的数目，只有设备重启后，支持的最大并发连接数才可恢复。

［命令实例］

```
hostname# exec ips enable
```

external-link

配置外链URL。该URL为一个绝对路径（必须带协议“http://”或者“ftp://”），例如，http://www.abc.com/script，表示该路径下所有文件都可以被虚拟Web站点引用（被外链）。使用该命令no的形式删除指定外链URL。

［命令］

external-link *url*

no external-link *url*

［句法描述］

url	指定外链 URL。

［默认取值］

无。

［命令模式］

虚拟主机配置模式。

［使用指导］

每个虚拟主机最多配置 32 个外链 URL。

［命令实例］

```
hostname(config)# ips sigset http1 template http
hostname(config-http-sigset)# virtual-host www.abc.com enable
hostname(config-http-virtual-host)# external-link
http://www.abc.com/script
```

external-link-check

为系统开启站点外链检查功能，控制虚拟 Web 站点对其它站点资源的引用。使用该命令 no 的形式关闭该功能。

［命令］

external-link-check enable action {reset | log}

no external-link-check enable

［句法描述］

reset | log	为 Web 站点外链行为指定相应的控制动作： • **reset**：发现站点外链行为后重置连接（TCP）或者发送目标不可达包（UDP）并且记录日志信息。 • **log**：发现站点外链行为后仅记录日志信息。

［默认取值］

无。

［命令模式］

虚拟主机配置模式。

［使用指导］

Web 站点外链事件为“警告”级别事件。

［命令实例］

```
hostname(config)# ips sigset http1 template http
hostname(config-http-sigset)# virtual-host www.abc.com enable
hostname(config-http-virtual-host)# external-link-check enable
action reset
```

ips enable

在安全域上开启 IPS 功能，并指定使用的 IPS Profile。使用该命令 no 的形式关闭安全域的 IPS 功能。

［命令］

ips enable *profile-name* **{egress | ingress | bidirectional}**

no ips enable

［句法描述］

profile-name	指定在安全域上生效的 IPS Profile 的名称。
egress	指定对出该安全域的流量进行 IPS 检测。

ingress	指定对进入该安全域的流量进行 IPS 检测。
bidirectional	指定对出入该安全域的流量都进行 IPS 检测。

［默认取值］

无。

［命令模式］

安全域配置模式。

［使用指导］

- 如果策略规则绑定了 IPS Profile，同时源安全域和目的安全域也绑定了 IPS Profile，系统 IPS 检测的优先级由高到低依次为：策略规则的 IPS Profile >目的安全域的 IPS Profile>源安全域的 IPS Profile。
- 一个安全域只能绑定一个 IPS Profile。

［命令实例］

```
hostname(config)# zone trust
hostname(config-zone-trust)# ips enable test bidirectional
```

ips log disable

关闭 IPS 日志功能。使用该命令 no 的形式开启 IPS 日志功能。

［命令］

ips log disable

no ips log disable

［句法描述］

无。

［默认取值］

开启。

［命令模式］

全局配置模式。

［使用指导］

由于 IPS 功能耗费内存，某些特殊情况下，为保证系统的正常运行，可暂时关闭 IPS 日志功能，释放部分内存。

［命令实例］

```
hostname(config)# ips log disable
```

ips mode

指定 IPS 工作模式。当前支持 IPS 在线模拟模式和 IPS 模式。

［命令］

ips mode {ips | ips-logonly}

［句法描述］

ips	指定 IPS 工作模式为 IPS 模式，即在提供协议异常和网络攻击行为的告警、日志功能的同时，还对检出攻击做重置和阻断操作。
ips-logonly	指定 IPS 工作模式为 IPS 在线模拟模式，即提供协议异常和网络攻击行为的告警、日志功能，不对检出攻击做重置和阻断操作

［默认取值］

IPS 模式。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **ips mode ips-logonly**

ips profile

创建指定名称的 IPS Profile 并进入 IPS Profile 配置模式。如果指定的名称已存在，则直接进入 IPS Profile 配置模式。使用该命令 no 的形式删除指定名称的 IPS Profile。

［命令］

ips profile *profile-name*

no ips profile *profile-name*

［句法描述］

profile-name	指定 IPS Profile 的名称。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# ips profile test
hostname(config-ips-profile)#
```

ips signature

禁用某指定特征。使用该命令 no 的形式重新启用指定特征。

［命令］

ips signature *id* **disable**

no ips signature *id* **disable**

［句法描述］

id	指定被禁用/启用的特征 ID。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

当某特征在全局配置模式下配置为启用状态时，在某特征集下禁用该特征，该特征在该特征集下为禁用状态；当某特征在全局配置模式下配置为禁用状态，无论该特征在特征集下的配置为启用还是禁用，该特征在特征集下均为禁用状态。

［命令实例］

```
hostname(config)# ips signature 100120 disable
```

ips sigset

基于已有预定义特征集为模板创建用户自定义特征集并进入特征集配置模式。如果指定的名称已存在，则直接进入特征集配置模式。使用该命令 no 的形式删除指定的特征集。

［命令］

ips sigset *sigset-name* [**template** {**dhcp** | **dns** | **finger** | **ftp** | **http** | **imap** | **ldap** | **msrpc** | **mssql** | **mysql** | **netbios** | **nntp** | **oracle** |

other-tcp | other-udp | pop3 | smtp | snmp | sunrpc | telnet | tftp | voip}

no ips sigset *sigset-name*

［句法描述］

sigset-name	指定特征集的名称。
dhcp | dns … | voip	指定作为模板的预定义特征集。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

- 预定义特征集不可以被删除也不可以被编辑。
- 自定义特征集不可以与预定义特征集同名。
- 不可以基于自定义特征集创建新的特征集。
- 同种类型的特征集不可以添加到同一个 IPS Profile 中，例如两个以 HTTP 为模板的自定义特征集不可以添加到同一个 IPS Profile 中，同时它们也不可以与预定义特征集 HTTP 添加到同一个 IPS Profile 中。

［命令实例］

```
hostname(config)# ips sigset http1 template http
hostname(config-http-sigset)#
```

max-arg-length

指定 POP3 客户端命令参数的最大长度，并指定安全级别。使用该命令 no 的形式恢复默认值。

［命令］

max-arg-length *length* **[severity {info | warning | critical}]**

no max-arg-length（恢复默认长度和默认安全级别）

no max-arg-length severity（恢复默认安全级别）

［句法描述］

length	指定命令参数的最大长度，单位为字节。
info | warning | critical	指定超过限定命令参数行长度的事件的安全级别。系统将根据该安全级别确定相应的动作。

［默认取值］

length - 40 字节

安全级别 - **warning**

［命令模式］

特征集配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# ips sigset pop3-cus template pop3
hostname(config-pop3-sigset)# max-arg-length 30 severity info
```

max-bind-length

指定系统允许的 MSRPC 协议绑定报文的最大长度，并指定安全级别。使用该命令 no 的形式恢复默认值。

［命令］

max-bind-length *length* [**severity {info | warning | critical}**]

no max-bind-length（恢复默认长度和默认安全级别）

no max-bind-length severity（恢复默认安全级别）

［句法描述］

length	指定绑定报文的最大长度，单位为字节。取值范围是 16 到 65535 字节。
info | warning | critical	指定超过限定绑定报文长度的事件的安全级别。系统将根据该安全级别确定相应的动作。

［默认取值］

length - 2048 字节

安全级别 - **warning**

［命令模式］

特征集配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# ips sigset msrpc-cus template msrpc
hostname(config-msrpc-sigset)# max-bind-length 3000 severity info
```

max-black-list

指定虚拟主机黑名单中能够包含的最大 URL 数目。当用户访问某静态页面时，如果系统发现该页面中包含违反外链检查或者上传路径检查的内容，则将该页面的 URL 加入到黑名单，当用户再次访问该页面时会直接命中黑名单，从而提高系统处理速度。使用该命令 no 的形式取消指定。

［命令］

max-black-list *size*

no max-black-list

［句法描述］

size	指定黑名单能够包含的最大 URL 数目。取值范围是 0 到 4096。

［默认取值］

0。

［命令模式］

虚拟主机配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# ips sigset http1 template http
hostname(config-http-sigset)# virtual-host www.abc.com enable
hostname(config-http-virtual-host)# max-black-list 4096
```

max-cmd-line-length

指定 FTP 命令行/POP3 客户端命令行/SMTP 客户端命令行的最大长度（包含回车换行），并指定安全级别。使用该命令 no 的形式恢复默认值。

［命令］

max-cmd-line-length *length* [**severity {info | warning | critical}**]

no max-cmd-line-length（恢复默认长度和默认安全级别）

no max-cmd-line-length severity（恢复默认安全级别）

［句法描述］

length	指定命令行的最大长度，单位为字节。FTP 命令行最大长度的取值范围是 5 到 1024 字节；POP3 和 SMTP 客户端命令行最大长度的取值范围是 64 到 1024 字节。
info | warning | critical	指定超过限定命令行长度的事件的安全级别。系统将根据该安全级别确定相应的动作。

［默认取值］

length - 512 字节

安全级别 - **warning**

［命令模式］

特征集配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# ips sigset test1 template ftp
hostname(config-ftp-sigset)# max-cmd-line-length 80 severity info
```

max-content-type-length

指定系统允许的 SMTP 协议 Content-Type 值的最大长度，并指定安全级别。使用该命令 no 的形式恢复默认值。

［命令］

max-content-type-length *length* [**severity {info | warning | critical}**]

no max-content-type-length（恢复默认长度和默认安全级别）

no max-content-type-length severity（恢复默认安全级别）

［句法描述］

length	指定 SMTP 协议 Content-Type 值的最大长度，单位为字节。取值范围是 6 到 1024 字节。
info | warning | critical	指定超过限定 Content-Type 值长度的事件的安全级别。系统将根据该安全级别确定相应的动作。

［默认取值］

length - 128 字节

安全级别 - **warning**

［命令模式］

特征集配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# ips sigset smtp-cus template smtp
hostname(config-ftp-sigset)# max-content-type-length 256 severity info
```

max-content-filename-length

指定系统允许的 SMTP 协议邮件附件名称的最大长度，并指定安全级别。使用该命令 no 的形式恢复默认值。

［命令］

max-content-filename-length *length* [**severity {info | warning | critical}**]

no max-content-filename-length（恢复默认长度和默认安全级别）

no max-content-filename-length severity（恢复默认安全级别）

［句法描述］

length	指定 SMTP 协议邮件附件名称的最大长度，单位为字节。取值范围是 64 到 1024 字节。
info | warning | critical	指定超过限定 SMTP 协议邮件附件名称最大长度的事件的安全级别。系统将根据该安全级别确定相应的动作。

［默认取值］

length - 128 字节

安全级别 - **warning**

［命令模式］

特征集配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# ips sigset smtp-cus template smtp
hostname(config-ftp-sigset)# max-content-filename-length 512 severity info
```

max-content-type-length

指定系统允许的 SMTP 协议 Content-Type 值的最大长度，并指定安全级别。使用该命令 no 的形式恢复默认值。

［命令］

max-content-type-length *length* [**severity {info | warning | critical}**]

no max-content-type-length（恢复默认长度和默认安全级别）

no max-content-type-length severity（恢复默认安全级别）

［句法描述］

length	指定 SMTP 协议 Content-Type 值的最大长度，单位为字节。取值范围是 6 到 1024 字节。
info | warning | critical	指定超过限定 Content-Type 值长度的事件的安全级别。系统将根据该安全级别确定相应的动作。

［默认取值］

length - 128 字节

安全级别 - **warning**

［命令模式］

特征集配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# ips sigset smtp-cus template smtp
hostname(config-ftp-sigset)# max-content-type-length 256 severity info
```

max-failure

指定系统允许的 POP3 服务器/SMTP 服务器返回错误的最大次数（同一个 POP3 会话/SMTP 会话中），并指定安全级别。使用该命令 no 的形式恢复默认值。

［命令］

max-failure *times* [**severity {info | warning | critical}**]

no max-failure（恢复默认次数和默认安全级别）

no max-failure severity（恢复默认安全级别）

［句法描述］

times	指定系统允许的 POP3 服务器返回错误的最大次数（同一个 POP3 会话中）。范围为 0 到 512。
info | warning | critical	指定超过限定命令参数行长度的事件的安全级别。系统将根据该安全级别确定相应的动作。

［默认取值］

times – 0（不做次数限制）

安全级别 - **warning**

［命令模式］

特征集配置模式。

［使用指导］

对同一个 POP3 会话中的服务器返回错误的个数进行限制，可以有效防止用户的非法尝试。

［命令实例］

```
hostname(config)# ips sigset pop3-cus template pop3
hostname(config-pop3-sigset)# max-failure 8 severity info
```

max-input-length

指定系统允许的 Telnet 用户名和密码的最大长度，并指定安全级别。使用该命令 no 的形式恢复默认值。

［命令］

max-input-length *length* **[severity {info | warning | critical}]**

no max-input-length（恢复默认长度和默认安全级别）

no max-input-length severity（恢复默认安全级别）

［句法描述］

length	指定 Telnet 用户名和密码的最大长度，单位为字节，范围为 6 到 1024。
info | warning | critical	指定超过限定 Telnet 用户名和密码长度的事件的安全级别。系统将根据该安全级别确定相应的动作。

［默认取值］

length - 128 字节

安全级别 - **warning**

［命令模式］

特征集配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# ips sigset telnet-cus template http
hostname(config-telnet-sigset)# max-input-length 30 severity info
```

max-path-length

指定系统允许的 SMTP 客户端命令中 reverse-path 和 forward-path 的最大长度，并指定安全级别。使用该命令 no 的形式恢复默认值。

［命令］

max-path-length *length* [**severity {info | warning | critical}**]

no max-path-length（恢复默认长度和默认安全级别）

no max-paht-length severity（恢复默认安全级别）

［句法描述］

length	指定系统允许的 SMTP 客户端命令中 reverse-path 和 forward-path 的最大长度，单位为字节，范围为 16 到 512（含标点符号）。
info | warning | critical	指定超过限定客户端命令中 reverse-path 和 forward-path 的最大长度的事件的安全级别。系统将根据该安全级别确定相应的动作。

［默认取值］

length - 256 字节

安全级别 - **warning**

［命令模式］

特征集配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# ips sigset smtp-cus template http
hostname(config-smtp-sigset)# max-path-length 128 severity info
```

max-reply-line-length

指定系统允许的 SMTP 服务器端响应的最大长度，并指定安全级别。使用该命令 no 的形式恢复默认值。

［命令］

max-reply-line-length *length* **[severity {info | warning | critical}]**

no max-reply-line-length（恢复默认长度和默认安全级别）

no max-reply-line-length severity（恢复默认安全级别）

［句法描述］

length	指定系统允许的 SMTP 服务器端响应的最大长度，单位为字节，范围为 64 到 1024（含回车换行）。
info | warning | critical	指定超过限定 SMTP 服务器端响应的最大长度的事件的安全级别。系统将根据该安全级别确定相应的动作。

［默认取值］

length - 512 字节

安全级别 - **warning**

［命令模式］

特征集配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# ips sigset smtp-cus template http
hostname(config-smtp-sigset)# max-reply-line-length 1024 severity
info
```

max-request-length

指定系统允许的 MSRPC 协议请求报文的最大长度，并指定安全级别。使用该命令 no 的形式恢复默认值。

［命令］

max-request-length *length* **[severity {info | warning | critical}]**

no max-request-length（恢复默认长度和默认安全级别）

no max-request-length severity（恢复默认安全级别）

［句法描述］

length	指定请求报文的最大长度，单位为字节。取值范围是 16 到 65535 字节。
info | warning | critical	指定超过限定请求报文长度的事件的安全级别。系统将根据该安全级别确定相应的动作。

［默认取值］

length - 65535 字节

安全级别 - **warning**

［命令模式］

特征集配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# ips sigset msrpc-cus template msrpc
hostname(config-msrpc-sigset)# max-request-length 60000 severity info
```

max-rsp-line-length

指定 FTP 最大响应长度，并指定安全级别。使用该命令 no 的形式恢复默认值。

［命令］

max-rsp-line-length *length* [**severity {info | warning | critical}**]

no max-rsp-line-length（恢复默认长度和默认安全级别）

no max-rsp-line-length severity（恢复默认安全级别）

［句法描述］

length	指定最大响应长度，单位为字节。
info | warning | critical	指定超过限定响应长度的事件的安全级别。系统将根据该安全级别确定相应的动作。

［默认取值］

length - 512 字节

安全级别 - **warning**

［命令模式］

特征集配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# ips sigset test1 template ftp
hostname(config-ftp-sigset)# max-rsp-line-length 100 severity info
```

max-scan-bytes

指定最大扫描长度。使用该命令 no 的形式恢复默认值。

［命令］

max-scan-bytes *length*

no max-scan-bytes

［句法描述］

length	指定最大扫描长度，单位为字节。

［默认取值］

length – 0（无限制）

［命令模式］

特征集配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# ips sigset test1 template msrpc
hostname(config-ftp-sigset)# max-rsp-line-length 1000
```

max-text-line-length

指定系统允许的 SMTP 客户端邮件文本的最大长度，并指定安全级别。使用该命令 no 的形式恢复默认值。

［命令］

max-text-line-length *length* [**severity {info | warning | critical}**]

no max-text-line-length（恢复默认长度和默认安全级别）

no max-text-line-length severity（恢复默认安全级别）

［句法描述］

length	指定系统允许的 SMTP 客户端邮件文本的最大长度，单位为字节，范围为 64 到 2048（含回车换行）。
info | warning | critical	指定超过限定 SMTP 客户端邮件文本的最大长度的事件的安全级别。系统将根据该安全级别确定相应的动作。

［默认取值］

length – 1000 字节

安全级别 - **warning**

［命令模式］

特征集配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# ips sigset smtp-cus template http
hostname(config-smtp-sigset)# max-text-line-length 1024 severity
info
```

max-uri-length

指定系统允许的 HTTP 协议 URL 的最大长度，并指定安全级别。使用该命令 no 的形式恢复默认值。

［命令］

max-uri-length *length* [**severity {info | warning | critical}**]

no max-uri-length（恢复默认长度和默认安全级别）

no max-uri-length severity（恢复默认安全级别）

［句法描述］

length	指定 URL 最大长度，单位为字节，范围为 64 到 4096。
info | warning | critical	指定超过限定 URL 长度的事件的安全级别。系统将根据该安全级别确定相应的动作。

［默认取值］

length - 4096 字节

安全级别 - **warning**

［命令模式］

特征集配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# ips sigset http1 template http
hostname(config-http-sigset)# max-uri-length 1000 severity info
```

max-white-list

指定虚拟主机白名单中能够包含的最大 URL 数目。当用户访问某静态页面时，如果该页面没有发现任何违反外链检查或者上传路径检查的内容，则将该页面的 URL 加入到白名单，当用户再次访问该页面时则直接命中白名单，从而提高系统处理速度。使用该命令 no 的形式取消指定。

［命令］

max-white-list *size*

no max- white-list

［句法描述］

length	指定白名单能够包含的最大 URL 数目。取值范围是 0 到 4096。

［默认取值］

0。

［命令模式］

虚拟主机配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# ips sigset http1 template http
hostname(config-http-sigset)# virtual-host www.abc.com enable
hostname(config-http-virtual-host)# max-white-list 4096
```

protocol-check

为特征集配置协议合法性检查的严格性。

［命令］

protocol-check {loose | strict}

［句法描述］

loose	配置协议合法性检查为松散。配置为松散后，当系统在协议解析过程中发现协议解析错误时，系统将仅记录日志信息然后调用引擎进行特征匹配检查。
strict	配置协议合法性检查为严格。配置为严格后，当系统在协议解析过程中发现协议解析错误时，系统将根据错误的安全级别，按照特征集配置的相应级别对应的动作对攻击包进行操作。

［默认取值］

loose

［命令模式］

特征集配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# ips sigset http1 template http
hostname(config-http-sigset)# protocol-check strict
```

signature id

为特征集中的某一条特征指定动作。使用该命令 no 的形式恢复特征的默认配置。

［命令］

signature id *number* {[**action** {**reset** | **log**}] [{**block** {**ip** | **service**} *timeout*} | **noblock**]}

no signature id *number*

［句法描述］

number	指定特征 ID。
reset | **log**	为特征指定相应的动作： • **reset**：匹配该特征后重置连接（TCP）或者发送目标不可达包（UDP）并且记录日志信息。 • **log**：匹配该特征后仅记录日志信息。
ip | **service**	指定阻断攻击者 IP（**ip**）或者服务（**service**）。
timeout	指定对攻击者 IP 或者服务进行阻断的时长，单位为秒，范围是 60 到 3600 秒。
noblock	不对攻击者的 IP 或者服务进行阻断。

［默认取值］

不对特征进行动作配置时，默认使用其所在特征集指定的动作。

不对特征进行阻断配置时，默认使用其所在特征集指定的阻断配置。

［命令模式］

特征集配置模式。

［使用指导］

单个特征的动作和阻断配置优先级高于其所在特征集的动作和阻断配置。

［命令实例］

```
hostname(config)# ips sigset test
hostname(config-smtp-sigset)# signature id 200350 action reset
block ip 60
```

signature id *number* disable

禁用特征集中的某一条特征。使用该命令 no 的形式开启指定的特征。

［命令］

signature id *number* **disable**

no signature id *number* **disable**

［句法描述］

number	指定特征 ID。

［默认取值］

默认情况下，特征集下的所有特征都处于开启状态。

［命令模式］

特征集配置模式。

［使用指导］

特征的当某特征在全局配置模式下配置为启用状态时，在某特征集下禁用该特征，该特征在该特征集下为禁用状态；当某特征在全局配置模式下配置为禁用状态，无论该特征在特征集下的配置为启用还是禁用，该特征在特征集下均为禁用状态。

［命令实例］

```
hostname(config)# ips sigset test
hostname(config-smtp-sigset)# signature id 200350 disable
```

sigset

将特征集添加到 IPS Profile 中。使用该命令 no 的形式将特征集从 IPS Profile 中删除。

［命令］

sigset {*user-defined-profile* | *pre-defined-profile*}

no sigset {*user-defined-profile* | *pre-defined-profile*}

［句法描述］

user-defined-profile	指定添加已创建的用户自定义特征集到 IPS Profile。
pre-defined-profile	指定添加系统预定义的特征集到 IPS Profile。

［默认取值］

无。

［命令模式］

IPS Profile 配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# ips profile ips-profile1
hostname(config-profile)# sigset test
hostname(config-profile)# sigset dhcp
```

sql-injection-check

为系统开启 HTTP 协议 SQL 注入攻击检测功能并对该功能进行配置。使用该命令 no 的形式关闭该功能。

［命令］

sql-injection-check enable [**action** {**reset** | **log**}] [**block** {**ip** | **service**} *timeout*] [**noblock**]

no sql-injection-check enable

［句法描述］

reset | **log**	为 HTTP 协议 SQL 注入攻击指定相应的动作： • **reset**：发现 SQL 注入攻击后重置连接（TCP）或者发送目标不可达包（UDP）并且记录日志信息。 • **log**：发现 SQL 注入攻击后仅记录日志信息。
ip |	指定阻断 SQL 注入攻击者的 IP 地址（**ip**）或者服务（**service**）。

service	
timeout	指定对攻击者 IP 或者服务进行阻断的时长，单位为秒，范围是 60 到 3600 秒。
noblock	不对攻击者的 IP 或者服务进行阻断。

［默认取值］

无。

［命令模式］

特征集配置模式。

［使用指导］

SQL 注入攻击事件为“严重”级别事件。不进行动作配置时，检测出 SQL 注入攻击后，默认仅记录日志。

［命令实例］

```
hostname(config)# ips sigset http1 template http
hostname(config-http-sigset)# sql-injection-check enable
```

virtual-host

为系统添加虚拟 Web 站点。使用该命令 no 的形式删除虚拟 Web 站点。

［命令］

virtual-host *domain* {**enable** | **disable**}

no virtual-host *domain*

［句法描述］

domain	指定 Web 站点域名。
enable | **disable**	启用（**enable**）/关闭（**disable**）Web 站点。

［默认取值］

无。

［命令模式］

特征集配置模式。

［使用指导］

执行该命令后，系统进入虚拟主机配置模式。

每个特征集最多配置 32 个虚拟主机。

［命令实例］

```
hostname(config)# ips sigset http1 template http
hostname(config-http-sigset)# virtual-host www.abc.com enable
```

web-acl

配置 Web 站点路径并指定其属性，该路径为 Web 服务器的相对路径。使用该命令 no 的形式关闭该功能。

［命令］

web-acl *url* **{static | deny}**

no web-acl *url*

［句法描述］

url	指定 Web 站点路径。
static | deny	指定 Web 站点路径的属性： • **static**：该属性 Web 站点路径下的资源只能按照静态资源（图片和普通文本）进行访问；否则，将按照上传路径检查功能（**web-acl-check enable action {reset | log}**）中配置的控制动作进行处理。 • **deny**：该属性 Web 站点路径下的资源不允许访问。

［默认取值］

无。

［命令模式］

虚拟主机配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# ips sigset http1 template http
hostname(config-http-sigset)# virtual-host www.abc.com enable
hostname(config-http-virtual-host)# web-acl www.eee.com deny
```

web-acl-check

为系统开启上传路径检查功能，防止攻击者利用上传漏洞向虚拟 Web 站点上传恶意代码。使用该命令 no 的形式关闭该功能。

［命令］

web-acl-check enable action {reset | log}

no web-acl-check enable

［句法描述］

reset | log	为 Web 站点上传行为指定相应的控制动作： • **reset**：发现上传行为后重置连接（TCP）或者发送目标不可达包（UDP）并且记录日志信息。 • **log**：发现上传行为后仅记录日志信息。

［默认取值］

无。

［命令模式］

虚拟主机配置模式。

［使用指导］

Web 站点上传行为事件为“警告”级别事件。

［命令实例］

```
hostname(config)# ips sigset http1 template http
hostname(config-http-sigset)# virtual-host www.abc.com enable
hostname(config-http-virtual-host)# web-acl-check enable action reset
```

xss-check enable

为系统开启 HTTP 协议跨站攻击防御功能并对该功能进行配置。使用该命令 no 的形式关闭该功能。

［命令］

xss-check enable [action {log | reset}] [block {ip | service} *timeout*] **[noblock]**

no xss-check enable

［句法描述］

reset | log	为 HTTP 协议跨站攻击指定相应的动作： • **reset**：发现跨站攻击后重置连接（TCP）或者发送目标不可达包（UDP）并且记录日志信息。 • **log**：发现跨站攻击后仅记录日志信息。
ip | service	指定阻断跨站攻击者的 IP 地址（**ip**）或者服务（**service**）。
timeout	指定对攻击者 IP 或者服务进行阻断的时长，单位为秒，范围是 60 到 3600 秒。
noblock	不对攻击者的 IP 或者服务进行阻断。

［默认取值］

无。

［命令模式］

特征集配置模式。

［使用指导］

跨站攻击事件为“严重”级别事件。不进行动作配置时，检测出跨站攻击后，默认仅记录日志。

［命令实例］

```
hostname(config)# ips sigset http1 template http
hostname(config-http-sigset)# xss-check enable
```

网络行为控制命令

behavior

将行为 Profile 绑定到策略规则。使用该命令 no 的形式取消绑定。

［命令］

behavior *profile-name*

no behavior

［句法描述］

profile-name	指定所需要绑定的行为 Profile 名称。

［默认取值］

无。

［命令模式］

策略规则配置模式。

［使用指导］

进入策略规则配置模式需要进行两步配置。首先，在全局配置模式下，输入“**policy-global**”命令进入策略配置模式；然后，在策略配置模式下，输入“**rule** [**id** *id-number*]”命令进入策略规则配置模式。

［命令实例］

```
hostname(config)# policy-global
hostname(config-policy)# rule id 1
hostname(config-policy-rule)# behavior p1
```

behavior-profile

创建行为 Profile。使用该命令 no 的形式删除指定的行为 Profile。

［命令］

behavior-profile *profile-name*

no behavior-profile *profile-name*

［句法描述］

profile-name	指定所创建的行为 Profile 的名称，并且进入该行为 Profile 的配置模式。如果指定名称已存在，则直接进入行为 Profile 配置模式。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# behavior-profile p1
hostname(config-bhv-profile)#
```

bin-type

配置行为 Profile 对下载指定类型的二进制文件进行控制。使用该命令 no 的形式取消下载限制。

［命令］

```
bin-type {bat | com | exe | msi | pif | scr} {deny | permit}
no bin-type {bat | com | exe | msi | pif | scr}
```

［句法描述］

bat | com | exe | msi | pif | scr	指定二进制文件的类型。
deny | permit	阻止（deny）或者允许（permit）下载指定类型的二进制文件。

［默认取值］

不进行控制。

［命令模式］

行为 Profile 配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# behavior-profile p1
hostname(config-bhv-profile)# bin-type exe deny
```

block-notification

开启用户被阻断警告功能。使用该命令 no 的形式关闭用户被阻断警告功能。

［命令］

block-notification

no block-notification

［句法描述］

无。

［默认取值］

开启。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **block-notification**

category

新建关键字类别。使用该命令 no 的形式删除指定的关键字类别。

［命令］

category *category-name*

no category *category-name*

［句法描述］

category-name	指定关键字类别的名称，为 1 到 31 个字符长度的字符串。

［默认取值］

无。

［命令模式］

内容过滤配置模式。

［使用指导］

关键字类别的警界值为 100。

请在全局配置模式下，使用 **contentfilter** 命令进入内容过滤配置模式。

［命令实例］

```
hostname(config)# contentfilter
hostname(config-contentfilter)# category abc
```

---

clear logging nbc

清除系统 NBC 日志信息。

［命令］

clear logging nbc

［句法描述］

无。

［默认取值］

无。

［命令模式］

执行模式。

［使用指导］

无。

［命令实例］

```
hostname# clear logging nbc
```

---

clear sslproxy notification

清除 SSL 代理警告提示历史记录。

［命令］

clear sslproxy notification

［句法描述］

无。

［默认取值］

无。

［命令模式］

任意模式。

［使用指导］

无。

［命令实例］

hostname# **clear sslproxy notification**

---

contentfilter（进入内容过滤配置模式）

使用该命令进入内容过滤配置模式。

［命令］

contentfilter

［句法描述］

无。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **contentfilter**

hostname(config-contentfilter)#

---

contentfilter（绑定内容过滤Profile到策略规则）

将内容过滤 Profile 绑定到策略规则。使用该命令 no 的形式取消绑定。

［命令］

contentfilter *profile-name*

no contentfilter

［句法描述］

profile-name	指定所需要绑定的内容过滤 Profile 名称。

［默认取值］

无。

［命令模式］

策略规则配置模式。

［使用指导］

进入策略规则配置模式需要进行两步配置。首先，在全局配置模式下，输入“**policy-global**”命令进入策略配置模式；然后，在策略配置模式下，输入“**rule** [**id** *id-number*]”命令进入策略规则配置模式。

［命令实例］

```
hostname(config)# policy-global
hostname(config-policy)# rule id 1
hostname(config-policy-rule)# contentfilter contentfilter1
```

contentfilter-profile

创建内容过滤 Profile。使用该命令 no 的形式删除指定的内容过滤 Profile。

［命令］

contentfilter-profile *profile-name*

no contentfilter-profile *profile-name*

［句法描述］

profile-name	指定所创建的内容过滤 Profile 的名称，并且进入该内容过滤 Profile 的配置模式。如果指定名称已存在，则直接进入内容过滤 Profile 配置模式。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# contentfilter-profile profile1
```

exec contentfilter apply

当系统所定义的关键字增加、减少或者改变时，需使用该命令刷新关键字。

［命令］

exec contentfilter apply

［句法描述］

无。

［默认取值］

无。

［命令模式］

执行模式。

［使用指导］

无。

［命令实例］

hostname# **exec contentfilter apply**

exec url-db update

立即更新预定义 URL 数据库。

［命令］

exec url-db update [full]

［句法描述］

exec url-db update	仅对当前预定义 URL 数据库与更新服务器最新发布 URL 数据库的不同部分进行更新。
exec url-db update full	从更新服务器获取完整的最新发布 URL 数据库信息进行更新。

［默认取值］

无。

［命令模式］

执行模式。

［使用指导］

无论更新模式为手动还是自动，用户都可以随时使用该命令更新预定义 URL 数据库。

［命令实例］

hostname# **exec url-db update**

---

exclude-html-tag

配置内容过滤 Profile 对 HTML 网页进行关键字过滤时，只过滤 HTML 网页中显示的内容，不过滤 HTML 标签中的代码。使用该命令 no 的形式恢复默认值。

［命令］

exclude-html-tag

no exclude-html-tag

［句法描述］

无。

［默认取值］

禁用。

［命令模式］

内容过滤 Profile 配置模式。

［使用指导］

仅当 HTML 的 content 类型为“text/html”，即 content="text/html"时，该功能生效。

［命令实例］

hostname(config-contentfilter)# **exclude-html-tag**

---

export log nbc

导出系统 NBC 日志信息到 FTP 服务器、TFTP 服务器或 U 盘。

［命令］

export log nbc to ftp server *ip-address* **user** *user-name* **password** *password* [*file-name*]

export log nbc to tftp server *ip-address* [*file-name*]

export log nbc to {**usb0** | **usb1**} [*file-name*]

［句法描述］

ip-address	指定 FTP 或 TFTP 服务器的 IP 地址。
user-name	指定访问 FTP 服务器的用户名。
password	指定访问 FTP 服务器的密码。
usb0 | usb1	指定导出到 U 盘时使用的 USB 接口。
file-name	指定导出的日志文件的名称。

［默认取值］

无。

［命令模式］

执行模式。

［使用指导］

无。

［命令实例］

hostname# **export log nbc to usb0 nbc1.log**

export pki

从设备导出本地证书或者信任域信息。

［命令］

export pki *trust-domain-name* {**cacert** | **cert** | **pkcs12** *password* | **pkcs12-der** *password*} **to** {**ftp server** *ip-address* [**user** *user-name* **password** *password*] | **tftp server** *ip-address* | **usb0** | **usb1**} [*file-name*]

［句法描述］

trust-domain-name	指定 PKI 信任域的名称。
cacert | cert	导出 PKI 信任域的本地证书。
pkcs12 *password* | **pkcs12-der** *password*	以 PKCS12 或者 PKCS12-DER 格式导出信任域的证书（CA 证书和本地证书）以及本地证书对应的私钥信息，并指定私钥保护口令（*password*），用于解密私钥。
ftp server *ip-address* [**user** *user-name* **password** *password*]	指定 FTP 服务器的 IP 地址以及访问服务器使用的用户名和密码。当不输入用户名和密码时表示采用匿名登录方式。
tftp server *ip-address*	指定 TFTP 服务器的 IP 地址。
usb0 | usb1	指定导出本地证书或者信任域信息到 usb0 或者 usb1 插槽所对应的 U 盘根目录。
file-name	指定要导出的本地证书或者信任域信息的文件名。

［默认取值］

无。

［命令模式］

执行模式。

［使用指导］

无。

［命令实例］

```
hostname# export pki ssltest pkcs12-der xgfn321456 to tftp server
10.101.10.2
```

ftp

配置行为 Profile 对 FTP 应用程序行为进行控制。使用该命令 no 的形式取消控制。

［命令］

ftp {**login** [*user-name*] | **get** [*file-name*] | **put** [*file-name*]} {**block** | **permit**} [**log**]

no ftp {**login** [*user-name*] | **get** [*file-name*] | **put** [*file-name*]}

［句法描述］

login [*user-name*]	对 FTP 的登录行为进行控制。如果使用 *user-name* 参数指定用户名，可对指定用户的登录行为进行控制。
get [*file-name*]	对 FTP 的 Get 行为进行控制。如果使用 *file-name* 参数指定文件名，可对指定文件的 Get 行为进行控制。
put [*file-name*]	对 FTP 的 Put 行为进行控制。如果使用 *file-name* 参数指定文件名，可对指定文件的 Put 行为进行控制。
block | **permit**	指定控制动作，可以是阻止（**block**），或者允许通过（**permit**）。
log	指定对 FTP 应用程序行为进行日志记录。

［默认取值］

不进行控制。

［命令模式］

行为 Profile 配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# behavior-profile p1
```

```
hostname(config-bhv-profile)# ftp login user abc block
```

http

配置行为 Profile 对 HTTP 应用程序行为进行控制。使用该命令 no 的形式取消控制。

［命令］

http {**connect** | **delete** [*host*] | **get** [*host*] | **head** [*host*] | **options** [*host*] | **post** [*host*] | **put** [*host*] | **trace** [*host*]} {**block** | **permit**} [**log**]

no http {**connect** | **delete** [*host*] | **get** [*host*] | **head** [*host*] | **options** [*host*] | **post** [*host*] | **put** [*host*] | **trace** [*host*]}

［句法描述］

connect | **delete** [*host*] | **get** [*host*] | **head** [*host*] | **options** [*host*] | **post** [*host*] | **put** [*host*] | **trace** [*host*]	指定对 HTTP 应用程序的请求方法（**connect**、**delete**、**get**、**head**、**options**、**put** 或者 **trace**）进行控制。如果使用 *host* 参数指定主机名称，可对指定主机的行为进行控制。
block | **permit**	指定控制动作，可以是阻止（**block**），或者允许通过（**permit**）。
log	指定对 HTTP 应用程序行为进行日志记录。

［默认取值］

不进行控制。

［命令模式］

行为 Profile 配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# behavior-profile p1
hostname(config-bhv-profile)# http post category xyz block
```

im

将网络聊天 Profile 绑定到策略规则。使用该命令 no 的形式取消绑定。

［命令］

im *profile-name*

no im

［句法描述］

profile-name	指定所需要绑定的网络聊天 Profile 名称。

［默认取值］

无。

［命令模式］

策略规则配置模式。

［使用指导］

进入策略规则配置模式需要进行两步配置。首先，在全局配置模式下，输入“**policy-global**”命令进入策略配置模式；然后，在策略配置模式下，输入“**rule** [**id** *id-number*]”命令进入策略规则配置模式。

［命令实例］

```
hostname(config)# policy-global
hostname(config-policy)# rule id 1
hostname(config-policy-rule)# im im1
```

import pki

导入本地证书或者信任域信息到设备。

［命令］

import pki *trust-domain-name* {**cacert** | **cert** | **pkcs12** *password* | **pkcs12-der** *password*} **from** {**ftp server** *ip-address* [**user** *user-name* **password** *password*] | **tftp server** *ip-address* | **usb0** | **usb1**} *file-name*

［句法描述］

trust-domain-name	指定 PKI 信任域的名称。
cacert | **cert**	导入 PKI 信任域的本地证书。
pkcs12 *password* | **pkcs12-der** *password*	以 PKCS12 或者 PKCS12-DER 格式导入信任域的证书（CA 证书和本地证书）以及本地证书对应的私钥信息，并指定私钥保护口令（*password*），用于解密私钥。
ftp server *ip-address* [**user** *user-name* **password** *password*]	指定 FTP 服务器的 IP 地址以及访问服务器使用的用户名和密码。当不输入用户名和密码时表示采用匿名登录方式。
tftp server *ip-address*	指定 TFTP 服务器的 IP 地址。
usb0 | **usb1**	指定通过 USB 方式从 usb0 或者 usb1 插槽所对应的 U 盘

	根目录导入本地证书或者信任域信息。
file-name	指定要导入的本地证书或者信任域信息的文件名。

［默认取值］

无。

［命令模式］

执行模式。

［使用指导］

无。

［命令实例］

hostname# **import pki ssltest cert from ftp server 10.101.10.1 user user1 password 11111 ssltest.crt**

import sslproxy

可信 SSL 证书列表中包含业内广泛认可的 CA 证书，用于设备替换 SSL Web 站点证书前验证站点证书的合法性。如果合法，设备会将系统 SSL 代理证书下发给客户端 Web 浏览器；如果不合法，设备会下发系统内置证书，该内置证书会在 Subject 字段中表明该证书不可信，从而提醒用户对该站点的访问。导入单个或者多个可信 SSL 证书到设备。

［命令］

import sslproxy {trustca-single | trustca-package} from {ftp server *ip-address* **[user** *user-name* **password** *password*] **| tftp server** *ip-address* **| usb0 | usb1}** *file-name*

［句法描述］

trustca-single | trustca-package	指定导入单个（**trustca-single**）或者多个（**trustca-package**）可信 SSL 证书。
ftp server *ip-address* **[user** *user-name* **password** *password*]	指定 FTP 服务器的 IP 地址以及访问服务器使用的用户名和密码。当不输入用户名和密码时表示采用匿名登录方式。
tftp server *ip-address*	指定 TFTP 服务器的 IP 地址。
usb0 | usb1	指定通过 USB 方式从 usb0 或者 usb1 插槽所对应的 U 盘根目录导入可信 SSL 证书。
file-name	指定要导入的可信 SSL 证书文件名。

［默认取值］

无。

［命令模式］

执行模式。

［使用指导］

无。

［命令实例］

```
hostname# import sslproxy trustca-package from ftp server
10.101.10.1 user user1 password 35719 trustca.tgz
```

import url-db

从本地导入预定义 URL 数据库。

［命令］

import url-db from {ftp server *ip-address* **[user** *user-name* **password** *password*] **| tftp server** *ip-address* **| usb0 | usb1}** *file-name*

［句法描述］

ip-address	指定 FTP 或者 TFTP 服务器的 IP 地址。
user *user-name* **password** *password*	指定 FTP 服务器的用户名和密码，若不指定则为匿名登录。
usb0 | usb1	指定通过 USB 方式从 **usb0** 或者 **usb1** 插槽所对应的 U 盘根目录获取 URL 数据库特征文件
file-name	指定导入的 URL 数据库特征文件的名称。

［默认取值］

无。

［命令模式］

执行模式。

［使用指导］

在某些情况下，用户设备可能无法连接到更新服务器对预定义 URL 数据库进行更新，针对这一问题，StoneOS 提供 URL 数据库本地导入功能，即通过 FTP、TFTP 服务器或者 U 盘将 URL 数据库特征文件引入到设备，从而更新设备的 URL 数据库。

［命令实例］

```
hostname# import url-db from tftp server 192.168.1.1 signature-file
```

im-profile

创建网络聊天 Profile。使用该命令 no 的形式删除指定的网络聊天 Profile。

［命令］

im-profile *profile-name*

no im-profile *profile-name*

［句法描述］

profile-name	指定所创建的网络聊天 Profile 的名称，并且进入该网络聊天 Profile 的配置模式。如果指定名称已存在，则直接进入网络聊天 Profile 配置模式。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **im-profile im1**

keyword

配置关键字。使用该命令 no 的形式删除该指定的关键字。

［命令］

keyword *keyword* {**regexp** | **simple**} [**category** *category-name*] [**confidence** *value*]

no keyword *keyword*

［句法描述］

keyword	指定关键字。
regexp | **simple**	指定关键字的匹配方式。可以为完全匹配（**simple**）和正则匹配（**regexp**）。“完全匹配”按照字符进行逐字匹配，“正则匹配”按照正则表达式的计算结果进行匹配。StoneOS 支持 PCRE（Perl Compatible Regular Expressions）正则表达式语法。
category *category-name*	指定关键字所属的类别。
confidence *value*	指定关键字对应的信任值。*value* 的的取值范围为 1 到 100，默认值为 100。

［默认取值］

无。

［命令模式］

内容过滤配置模式。

［使用指导］

关键字支持 UTF-8 和 GB18030 两种编码方式。

一个关键字最多属于 16 个关键字类别。

［命令实例］

```
hostname(config-contentfilter)# keyword X simple category XYZ
confidence 10
```

keyword-category（URL过滤）

指定需要进行控制的 URL 关键字类别及控制动作。使用该命令 no 的形式取消 URL 关键字类别及控制动作的指定。

［命令］

keyword-category *keyword-category-name* [**block**] [**log**]

no keyword-category *keyword-category-name*

［句法描述］

keyword-category-name	指定需要进行控制的 URL 关键字类别名称。
block	指定阻止访问网址中含有相应关键字的网站。
log	指定对访问网址中含有相应关键字的网站的行为进行日志记录。

［默认取值］

无。

［命令模式］

URL 过滤 Profile 配置模式。

［使用指导］

使用多条该命令可指定多个 URL 关键字类别及相应的控制动作。

［命令实例］

```
hostname(config)# url-profile u1
hostname(config-url-profile)# keyword-category X block
```

keyword-category（网页关键字）

指定需要进行控制的网页内容关键字类别及控制动作。使用该命令 no 的形式取消关键字类别及控制动作的指定。

［命令］

keyword-category *keyword-category-name* [**block**] [**log**] [**content**]

no keyword-category *keyword-category-name*

［句法描述］

keyword-category-name	指定需要进行控制的网页内容关键字类别名称。
block	指定阻止访问内容中含有相应关键字的网站。
log	指定对访问含有相应关键字内容的网站的行为进行日志记录。
content	指定记录网站页面中与关键字相邻的上下文信息。只有当安全网关支持并已配置存储设备（存储设备指 SD 存储卡、U 盘和 Hillstone 山石网科提供的存储扩展模块），而且已安装网络行为控制许可证时，才能配置该参数。

［默认取值］

无。

［命令模式］

内容过滤 Profile 配置模式。

［使用指导］

使用多条该命令可指定多个关键字类别及相应的控制动作。

［命令实例］

hostname(config)# **contentfilter-profile c1**

hostname(config-contentfilter-profile)# **keyword-category web-keyword block log**

keyword-category（Web外发信息）

指定控制含有特定关键字的 Web 外发信息和相应的控制动作。使用该命令 no 的形式取消关键字类别及控制动作的指定。

［命令］

keyword-category *keyword-category-name* [**block**] [**log**] [**content**]

no keyword-category *keyword-category-name*

［句法描述］

keyword-category-name	指定需要进行控制的关键字类别名称。
block	指定阻止发布含有相应关键字的信息。
log	指定对访问含有相应关键字内容的网站的行为进行日志记录。
content	指定记录发布信息中与关键字相邻的上下文信息。只有当安全网关支持并已配置存储设备（存储设备指 SD 存储卡、U 盘和 Hillstone 山石网科提供的存储扩展模块），而且已安装网络行为控制许可证时，才能配置该参数。

［默认取值］

无。

［命令模式］

Web 外发信息 Profile 配置模式。

［使用指导］

使用多条该命令可指定多个关键字类别及相应的控制动作。

［命令实例］

```
hostname(config)# webpost-profile w1
hostname(config-webpost-profile)# keyword-category Y block log
```

keyword-category（邮件过滤）

指定控制含有特定关键字内容的外发邮件及相应的控制动作。使用该命令 no 的形式取消关关键字类别及控制动作的指定。

［命令］

keyword-category *keyword-category-name* [**block**] [**log**] [**content**]

no keyword-category *keyword-category-name*

［句法描述］

keyword-category-name	指定需要进行控制的关键字类别名称。
block	指定阻止发送含有相应关键字的邮件。
log	指定对发送含有相应关键字邮件的行为进行日志记录。
content	指定记录邮件内容。只有当安全网关支持并已配置存储设备（存储设备指 SD 存储卡、U 盘和 Hillstone 山石网科提供的存储扩展模块），而且已安装网络行为控制许可证时，才能配置该参数。

［默认取值］

无。

［命令模式］

Web 外发信息 Profile 配置模式。

［使用指导］

使用多条该命令可指定多个关键字类别及相应的控制动作。

［命令实例］

```
hostname(config)# mail-profile m1
hostname(config-mail-profile)# keyword-category Z block log
```

---

logging

开启系统 NBC 日志功能。使用该命令 no 的形式关闭 NBC 日志功能。

［命令］

```
logging nbc on
no logging nbc on
```

［句法描述］

无。

［默认取值］

开启。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# logging nbc on
```

---

logging nbc to

指定 NBC 日志信息的输出目的地。使用该命令 no 的形式关闭相关的输出功能。

［命令］

```
logging nbc to {console | remote | syslog| email}
```

logging nbc to buffer [**size** *buffer-size*]

logging nbc to file [**name** {**usb0** | **usb1** | **compactflash**} *file-name*] [**size** *file-size*]

logging nbc to localdb [**location sd0** | **usb0** | **usb1** | **storage***X*] [**size** *storage-percentage*]

no logging nbc to {**console** | **remote** | **syslog**| **email**}

no logging nbc to buffer

no logging nbc to file

no logging nbc to localdb

［句法描述］

console	指定将 NBC 日志信息输出到 console 口。
remote	指定将 NBC 日志信息输出到远程终端，包括 Telnet 和 SSH。
syslog	指定将 NBC 日志信息输出到 Syslog Server。
buffer	指定将 NBC 日志信息输出到内存缓存。
buffer-size	将 NBC 日志信息输出到内存缓存时，该参数用来指定内存缓存的大小。范围是 4096 到 4294967295 字节。
email	指定将 NBC 日志信息发送到某个邮件地址。
file	默认情况下，StoneOS 会生成一个文件记录日志信息，用户可以指定将信息输出到 U（**usb0	usb1**）盘或者 CF 卡（**compactflash**）的文件中。
**usb0	usb1	compactflash**	将 NBC 日志信息输出到文件时，该参数用来指定保存日志文件的 U（**usb0	usb1**）盘或者 CF 卡（**compactflash**）。
file-name	将 NBC 日志信息输出到文件时，该参数用来指定存储到 U 盘、硬盘卡或者 CF 卡的日志信息文件名称。
file-size	将 NBC 日志信息输出到文件时，该参数用来指定日志信息文件大小。范围是 4096 到 4294967295 字节。
localdb	指定将 NBC 日志信息发送到本地数据库。
**location sd0	usb0	usb1	storage***X*	将 NBC 日志信息输出到本地数据库时，该参数用来指定保存日志信息的本地数据库所在的存储设备。*X* 为插入存储扩展模块的扩展槽号。
size *storage-percentage*	将 NBC 日志信息输出到本地数据库时，该参数用来指定数据库存储空间占用硬盘卡的百分比。范围是 1 到 100。

［默认取值］

内存缓存默认值：1048576 字节；

日志信息文件大小默认值：1048576 字节；

数据库所在硬盘卡：storage 1；

数据库存储空间占用硬盘卡的百分比：1 到 100。

［命令模式］

全局配置模式。

［使用指导］

当日志信息存储到本地数据库（Localdb）时，系统将每天生成一个数据库文件，文件名称格式为“年_月_日-nbc.db”。例如，2009 年 8 月 1 日的 NBC 日志保存在 2009_8_1-nbc.db 中。当数据库所在的硬盘卡空间被用尽时，系统会自动删除日期最早的数据库文件。例如，硬盘卡中存储了从 2009 年 6 月 1 日到 2009 年 8 月 1 日之间的上网管理日志信息后，硬盘空间被用尽，若继续存储新的日志信息，系统将自动删除 2009_6_1-nbc.db 的日志信息。

当指定 NBC 日志输出的目的地为本地数据库时，请根据设备上插入硬盘卡的实际槽位选择本地数据库所在的硬盘卡。系统默认数据库所在硬盘卡为 storage 1，用户需要根据实际情况进行修改。

［命令实例］

hostname(config)# **logging nbc to localdb location storage 1**

mail

将邮件过滤 Profile 绑定到策略规则。使用该命令 no 的形式取消绑定。

［命令］

mail *profile-name*

no mail

［句法描述］

profile-name	指定所需要绑定的邮件过滤 Profile 名称。

［默认取值］

无。

［命令模式］

策略规则配置模式。

［使用指导］

进入策略规则配置模式需要进行两步配置。首先，在全局配置模式下，输入“**policy-global**”命令进入策略配置模式；然后，在策略配置模式下，输入“**rule** [**id** *id-number*]”命令进入策略规则配置模式。

［命令实例］

hostname(config)# **policy-global**

```
hostname(config-policy)# rule id 1
hostname(config-policy-rule)# mail mail1
```

mail any

指定控制所有外发邮件及相应的控制动作。使用该命令 no 的形式取消对所有邮件进行控制的指定。

［命令］

mail any [log] [content] [attachment]

no mail any

［句法描述］

log	指定对所有的外发邮件行为进行日志记录。
content	指定记录所有外发邮件的邮件内容。只有当安全网关支持并已配置存储设备（存储设备指 SD 存储卡、U 盘和 Hillstone 山石网科提供的存储扩展模块），而且已安装网络行为控制许可证时，才能配置该参数。
attachment	指定记录所有外发邮件的附件。只有当安全网关支持并已配置存储设备（存储设备指 SD 存储卡、U 盘和 Hillstone 山石网科提供的存储扩展模块），而且已安装网络行为控制许可证时，才能配置该参数。

［默认取值］

无。

［命令模式］

邮件过滤 Profile 配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# mail-profile mailfilter
hostname(config-mail-profile)# mail any log
```

mail attach

指定需要进行控制的附件名称及控制动作。使用该命令 no 的形式取消附件名称及控制动作的指定。

［命令］

mail attach [*attach-name*] [**block**] [**log**] [**content**] [**attachment**]

no mail attach [*attach-name*]

［句法描述］

attach-name	指定对特定附件名称进行控制。如不指定该参数，则对所有附件进行控制。
block	指定阻止发送特定名称的附件（指定 *attach-name* 参数时）；或者阻止发送所有附件（不指定 *attach-name* 参数时）。
log	指定对发送附件的行为进行日志记录。
content	指定记录邮件内容。只有当安全网关支持并已配置存储设备（存储设备指 SD 存储卡、U 盘和 Hillstone 山石网科提供的存储扩展模块），而且已安装网络行为控制许可证时，才能配置该参数。
attachment	指定记录邮件附件。只有当安全网关支持并已配置存储设备（存储设备指 SD 存储卡、U 盘和 Hillstone 山石网科提供的存储扩展模块），而且已安装网络行为控制许可证时，才能配置该参数。

［默认取值］

无。

［命令模式］

邮件过滤 Profile 配置模式。

［使用指导］

使用多条该命令可指定多个附件名称及相应的控制动作。

［命令实例］

hostname(config)# **mail-profile mailfilter**

hostname(config-mail-profile)# **mail attach block log**

mail control

指定受控邮箱类型。默认情况下，邮件过滤规则对系统支持的所有邮箱类型进行控制。使用该命令 no 的形式取消控制。

［命令］

mail control {all | webmail | smtp | 126 | 139 | 163 | 188 | 21cn | eyou | gmail | hotmail | qq | sina | sogou | sohu | tom | yahoo | yeah}

no mail control { all | 126 | 139 | 163 | 188 | 21cn | eyou | gmail | hotmail | qq | sina | smtp | sogou | sohu | tom | webmail | yahoo | yeah}

［句法描述］

all | 126 | 139 | 163 | 188 | 21cn | eyou | gmail | hotmail | qq | sina | smtp | sogou | sohu | tom | webmail | yahoo | yeah	指定需要进行控制的邮箱类型，可以为系统支持的所有邮箱（**all**）、所有 Web 邮箱（**webmail**）、SMTP 邮件（**smtp**）或者特定 Web 邮箱（**126 | 139 | 163 | 188 | 21cn | eyou | gmail | hotmail | qq | sina | sogou | sohu | tom | yahoo | yeah**）。

［默认取值］

对系统支持的所有邮箱类型进行控制。

［命令模式］

邮件过滤 Profile 配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# mail-profile mailfilter
hostname(config-mail-profile)# mail control smtp
```

mail enable

启用指定邮件控制内容。使用该命令 no 的形式关闭指定邮件控制内容。

［命令］

mail enable {sender | recipient | attach | keyword-category}

no mail enable {sender | recipient | attach | keyword-category}

［句法描述］

sender | recipient | attach | keyword-category	指定启用对邮件发件人（**sender**）、收件人（**recipient**）、附件（**attach**）和内容关键字（**keyword-category**）的控制。

［默认取值］

关闭。

［命令模式］

邮件过滤 Profile 配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# mail-profile mailfilter
hostname(config-mail-profile)# mail enable sender
```

mail max-attach-size

配置邮件过滤 Profile 对外发邮件的附件大小进行控制。使用该命令 no 的形式取消控制。

［命令］

mail max-attach-size *file-size* [**log**] [**content**] [**attachment**]

no max-attach-size

［句法描述］

file-size	指定附件大小，阻止发送超出指定大小范围的附件。
log	指定对发送超出指定大小范围附件的行为进行日志记录。
content	指定记录邮件内容。只有当安全网关支持并已配置存储设备（存储设备指 SD 存储卡、U 盘和 Hillstone 山石网科提供的存储扩展模块），而且已安装网络行为控制许可证时，才能配置该参数。
attachment	指定记录邮件附件。只有当安全网关支持并已配置存储设备（存储设备指 SD 存储卡、U 盘和 Hillstone 山石网科提供的存储扩展模块），而且已安装网络行为控制许可证时，才能配置该参数。

［默认取值］

不进行控制。

［命令模式］

邮件过滤 Profile 配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# mail-profile mailfilter
hostname(config-mail-profile)# mail max-attach-size 20 log content
attachment
```

mail others

指定其它邮件及控制动作，其它邮件为系统中已配置的指定邮件控制内容（包含特定发件人、收件人、内容关键字或附件的邮件）以外的邮件。使用该命令 no 的形式取消对其它邮件进行控制的指定。

［命令］

mail others [block] [log] [content] [attachment]

no mail others

［句法描述］

block	指定阻止发送特定邮件控制内容以外的邮件。
log	指定对发送特定邮件控制内容以外邮件的行为进行日志记录。
content	指定记录邮件内容。只有当安全网关支持并已配置存储设备（存储设备指 SD 存储卡、U 盘和 Hillstone 山石网科提供的存储扩展模块），而且已安装网络行为控制许可证时，才能配置该参数。
attachment	指定记录邮件附件。只有当安全网关支持并已配置存储设备（存储设备指 SD 存储卡、U 盘和 Hillstone 山石网科提供的存储扩展模块），而且已安装网络行为控制许可证时，才能配置该参数。

［默认取值］

不进行控制。

［命令模式］

邮件过滤 Profile 配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# mail-profile mailfilter
hostname(config-mail-profile)# mail others log content attachment
```

mail-profile

创建邮件过滤 Profile。使用该命令 no 的形式删除指定的邮件过滤 Profile。

［命令］

mail-profile *profile-name*

no mail-profile *profile-name*

［句法描述］

profile-name	指定所创建的邮件过滤 Profile 的名称，并且进入该邮件过滤 Profile 的配置模式。如果指定名称已存在，则直接进入邮件过滤 Profile 配置模式。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **mail-profile mail1**

mail {sender | recipient}

指定需要进行控制的发件人或者收件人及控制动作。使用该命令 no 的形式取消发件人或者收件人及控制动作的指定。

［命令］

mail {sender | recipient} *email-address* **[block] [log] [content] [attachment]**

no mail {sender | recipient} *email-address*

［句法描述］

email-address	指定发件人（**sender**）或者收件人（**recipient**）邮箱帐号。
block	指定阻止发送含特定发件人或者收件人的邮件。
log	指定对发送含有特定发件人或者收件人邮件的行为进行日志记录。
content	指定记录邮件内容。只有当安全网关支持并已配置存储设备（存储设备指 SD 存储卡、U 盘和 Hillstone 山石网科提供的存储扩展模块），而且已安装网络行为控制许可证时，才能配置该参数。
attachment	指定记录邮件附件。只有当安全网关支持并已配置存储设备（存储设备指 SD 存储卡、U 盘和 Hillstone 山石网科提供的存储扩展模块），而且已安装网络行为控制许可证时，才能配置该参数。

［默认取值］

无。

［命令模式］

邮件过滤 Profile 配置模式。

［使用指导］

使用多条该命令可指定多个发件人或者收件人及相应的控制动作。

［命令实例］

```
hostname(config)# mail-profile mailfilter
hostname(config-mail-profile)# mail sender user@126.com block log content attachment
```

mail whitelist

指定例外帐号，例外帐号为不受邮件过滤规则控制的邮箱帐号，可以为发件人帐号或者收件人帐号。使用该命令 no 的形式取消例外帐号的指定。

［命令］

mail whitelist *mail-address*

no mail whitelist

［句法描述］

mail-address	指定不受邮件过滤策略规则控制的邮箱帐号。

［默认取值］

无。

［命令模式］

邮件过滤 Profile 配置模式。

［使用指导］

使用多条该命令可指定多个例外帐号。

［命令实例］

```
hostname(config)# mail-profile mailfilter
hostname(config-mail-profile)# mail whitelist abc@126.com
```

msn | ymsg | qq

配置网络聊天 Profile 对 MSN、雅虎通和 QQ 聊天进行控制。使用该命令 no 的形式取消控制。

［命令］

{msn | ymsg | qq} {others | *im-account*} [block] [log]

no {msn | ymsg | qq} {others | *im-account*}

［句法描述］

**msn	ymsg	qq**	指定控制 MSN（**msn**）、雅虎通（**ymsg**）或者 QQ（**qq**）。
others	*im-account*	指定需要进行控制的 MSN、雅虎通或者 QQ 帐号（*im-account*）或者系统中已经指定帐号以外的帐号（**others**）。
block	指定阻止使用相应的 MSN、雅虎通或者 QQ 帐号。
log	指定记录相应 MSN、雅虎通或者 QQ 帐号的上下线日志。

［默认取值］

不进行控制。

［命令模式］

网络聊天 Profile 配置模式。

［使用指导］

使用多条上述命令可指定多个聊天工具帐号及相应的控制动作。

［命令实例］

```
hostname(config)# im-profile im1
hostname(config-im-profile)# msn others log
```

nbc-user-notification

开启用户被监控警告功能。使用该命令 no 的形式关闭用户被监控警告功能功能。

［命令］

nbc-user-notification

no nbc-user-notification

［句法描述］

无。

［默认取值］

关闭。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# nbc-user-notification
```

object

配置行为 Profile 控制 ActiveX 和 Java Applet 的使用。使用该命令 no 的形式取消对 ActiveX 或者 Java Applet 的使用限制。

［命令］

```
object {active-x | java-applet} {deny | permit}
no object {active-x | java-applet}
```

［句法描述］

active-x | java-applet	指定对 ActiveX 服务或者 Java Applet 服务进行操作控制。
deny | permit	阻止（deny）或者允许（permit）下载指定的 HTTP 对象。

［默认取值］

不进行控制。

［命令模式］

行为 Profile 配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# behavior-profile behaviorprf1
hostname(config-bhv-profile)# object java-applet deny
```

remove database

清除本地数据库 NBC 日志信息。

［命令］

remove database {active | all | *date*}

［句法描述］

active	指定清除当前本地数据库日志信息。
all	指定清除所有本地数据库日志信息。
date	指定清除指定日期的本地数据库日志信息。*date* 的书写格式为“年-月-日”，例如 2009-07-31。

［默认取值］

无。

［命令模式］

执行模式。

［使用指导］

无。

［命令实例］

hostname# **remove database all**

ssl-decode

启用 SSL 代理功能。使用该命令 no 的形式关闭 SSL 代理功能。

［命令］

ssl-decode

no ssl-decode

［句法描述］

无。

［默认取值］

未启用。

［命令模式］

SSL 代理 Profile 配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **sslproxy-profile ssl1**

hostname(config-sslproxy-profile)# **ssl-decode**

ssl-notification-disable

关闭 SSL 代理警告提示功能，使用该命令 no 的形式开启 SSL 代理警告提示功能。

［命令］

ssl-notification-disable

no ssl-notification-disable

［句法描述］

无。

［默认取值］

关闭。

［命令模式］

SSL 代理 Profile 配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# sslproxy-profile ssl1
hostname(config-sslproxy-profile)# ssl-notification-disable
```

sslproxy

将 SSL 代理 Profile 绑定到策略规则。使用该命令 no 的形式取消绑定。

［命令］

sslproxy *profile-name*

no sslproxy

［句法描述］

profile-name	指定所需要绑定的 SSL 代理 Profile 名称。

［默认取值］

无。

［命令模式］

策略规则配置模式。

［使用指导］

进入策略规则配置模式需要进行两步配置。首先，在全局配置模式下，输入“**policy-global**”命令进入策略配置模式；然后，在策略配置模式下，输入“**rule** [**id** *id-number*]”命令进入策略规则配置模式。

［命令实例］

```
hostname(config)# policy-global
hostname(config-policy)# rule id 1
hostname(config-policy-rule)# sslproxy sslproxy1
```

sslproxy exempt-match-subject

为“审计指定网站外的所有网站”方式指定网站。使用该命令 no 的形式取消网站证书的指定。

［命令］

sslproxy exempt-match-subject *subject-commom-name*

no sslproxy exempt-match-subject *subject-commom-name*

［句法描述］

subject-commom-name	指定网站证书 Subject 字段的 CommonName 字段。安全网关对采用此证书以外的证书加密的通信进行 SSL 代理。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# sslproxy exempt-match-subject www.google.com
```

sslproxy-profile

创建 SSL 代理 Profile。使用该命令 no 的形式删除指定的 SSL 代理 Profile。

［命令］

sslproxy-profile *profile-name*

no sslproxy-profile *profile-name*

［句法描述］

profile-name	指定所创建的 SSL 代理 Profile 的名称，并且进入该 SSL 代理 Profile 的配置模式。如果指定名称已存在，则直接进入 SSL 代理 Profile 配置模式。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **sslproxy-profile ssl1**

sslproxy require-match-subject

为“只审计指定网站”方式指定审计网站。使用该命令 no 的形式取消网站证书的指定。

［命令］

sslproxy require-match-subject *subject-commom-name*

no sslproxy require-match-subject *subject-commom-name*

［句法描述］

subject-commom-name	指定审计网站证书 Subject 字段的 CommonName 字段。安全网关对采用此证书加密的通信进行 SSL 代理。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **sslproxy require-match-subject www.google.com**

sslproxy {require-mode | exempt-mode}

指定 SSL 审计方式，包括“只审计指定网站”和“审计指定网站外的所有网站”两种。

［命令］

sslproxy {require-mode | exempt-mode}

［句法描述］

require-mode | exempt-mode	指定 SSL 代理方式，可以为“只审计指定网站”（**require-mode**）或者“审计指定网站外的所有网站”（**exempt-mode**）。

［默认取值］

只审计指定网站。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **sslproxy require-mode**

sslproxy trust-domain

指定设备证书的 PKI 信任域。安全网关会使用指定 PKI 信任域中的证书对 Web 服务器证书重新签发，生成 SSL 代理证书。使用该命令 no 的形式取消设备证书 PKI 信任域的指定。

［命令］

sslproxy trust-domain *trust-domain-name*

no sslproxy trust-domain *trust-domain-name*

［句法描述］

trust-domain-name	指定系统中已创建的 PKI 信任域名称。执行该命令后，设备会使用该信任域中的证书对 Web 服务器证书重新签发，生成 SSL 代理证书。

［默认取值］

使用缺省信任域 trust_domain_ssl_proxy 为设备证书的 PKI 信任域。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# sslproxy trust-domain ssltest
```

sslproxy trustca-delete

删除指定的可信 SSL 证书。

［命令］

sslproxy trustca-delete *file-name*

［句法描述］

file-name	指定要删除的可信 SSL 证书文件名。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# sslproxy trustca-delete abc.crt
```

url（添加URL条目）

添加 URL 条目。使用该命令 no 的形式删除该指定的 URL 条目。

［命令］

url *url* **url-category** *category-name*

no url *url*

［句法描述］

url	指定 URL。
category *category-name*	指定 URL 所属的类别。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# url www.abc.com url-category url1
```

url（绑定URL过滤Profile到策略规则）

将 URL 过滤 Profile 绑定到策略规则。使用该命令 no 的形式取消绑定。

［命令］

url *profile-name*

no url

［句法描述］

profile-name	指定所需要绑定的 URL 过滤 Profile 名称。

［默认取值］

无。

［命令模式］

策略规则配置模式。

［使用指导］

进入策略规则配置模式需要进行两步配置。首先，在全局配置模式下，输入“**policy-global**”命令进入策略配置模式；然后，在策略配置模式下，输入“**rule** [**id** *id-number*]”命令进入策略规则配置模式。

［命令实例］

```
hostname(config)# policy-global
hostname(config-policy)# rule id 1
hostname(config-policy-rule)# url url1
```

url-category（新建URL类别）

新建 URL 类别。使用该命令 no 的形式删除指定的 URL 类别。

［命令］

url-category *category-name*

no url-category *category-name*

［句法描述］

category-name	指定 URL 类别的名称，为 1 到 31 个字符长度的字符串。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

URL 类别名称不能只为连字符“-”。

系统最多支持 16 个自定义 URL 类别。

［命令实例］

hostname(config)# **url-category abc**

url-category（URL过滤）

指定需要进行控制的 URL 类别及控制动作。使用该命令 no 的形式取消 URL 类别及控制动作的指定。

［命令］

url-category {**all** | *url-category-name*} [**block**] [**log**]

no url-category {**all** | *url-category-name*}

［句法描述］

all | *url-category-name*	指定需要进行控制的 URL 类别名称，可以为所有的 URL 类别（**all**）或者特定 URL 类别（*url-category-name*）。
block	指定阻止访问相应的 URL 类别。
log	指定对用户的 URL 访问行为进行日志记录。

［默认取值］

无。

［命令模式］

URL 过滤 Profile 配置模式。

［使用指导］

使用多条该命令可指定多个 URL 类别及相应的控制动作。

［命令实例］

```
hostname(config)# url-profile u1
hostname(config-url-profile)# url-category News block log
```

url-category（网页关键字）

指定关键字控制范围，系统会对指定的网站做关键字控制。使用该命令 no 的形式取消 URL 类别的指定。

［命令］

url-category {**all** | *url-category-name*}

no url-category {**all** | *url-category-name*}

［句法描述］

all | *url-category-name*	指定需要进行关键字控制的 URL 类别名称，可以为所有的 URL 类别（**all**）或者特定 URL 类别（*url-category-name*）。

［默认取值］

无。

［命令模式］

内容过滤 Profile 配置模式。

［使用指导］

使用多条该命令可指定多个 URL 类别。

［命令实例］

```
hostname(config)# contentfilter-profile c1
hostname(config-contentfilter-profile)# url-category all
```

url-category（Web外发信息）

指定需要进行外发信息控制的网站，系统会对指定的网站做外发信息控制。使用该命令 no 的形式取消 URL 类别的指定。

［命令］

url-category {**all** | *url-category-name*}

no url-category {**all** | *url-category-name*}

［句法描述］

all | *url-category-name*	指定需要进行外发信息控制的 URL 类别名称，可以为所有的 URL 类别（**all**）或者特定 URL 类别（*url-category-name*）。

［默认取值］

无。

［命令模式］

Web 外发信息 Profile 配置模式。

［使用指导］

使用多条该命令可指定多个 URL 类别。

［命令实例］

hostname(config)# **webpost-profile w1**

hostname(config-webpost-profile)# **url-category abc**

url-db update mode

配置预定义 URL 数据库的更新模式。使用该命令 no 的形式恢复默认更新模式。

［命令］

url-db update mode {**auto** | **manual**}

no url-db update mode

［句法描述］

auto | **manual**	指定更新模式，可以是自动更新（**auto**）URL 数据库，或者手动更新（**manual**）URL 数据库。

［默认取值］

自动更新。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **url-db update mode auto**

url-db update schedule

指定预定义 URL 数据库更新的频率和时间。

［命令］

url-db update schedule {daily | weekly {mon | tue | wed | thu | fri | sat | sun}} [*HH:MM*]

［句法描述］

daily	指定频率为每天更新。
**weekly {mon	tue	wed	thu	fri	sat	sun}**	指定频率为每周更新。**mon	tue	wed	thu	fri	sat	sun** 用来指定每周更新的日期。
HH:MM	指定更新的时间，例如 09：00。

［默认取值］

每日自动更新。

［命令模式］

全局配置模式。

［使用指导］

默认情况下，StoneOS 采用自动模式每日更新预定义 URL 数据库库，并且为避免服务器流量过大，每日更新时间是随机的。

［命令实例］

hostname(config)# **url-db update schedule daily 13:30**

url-db update server

配置预定义 URL 数据库更新服务器下载最新 URL 特征库。使用该命令 no 的形式取消更新服务器的指定。

［命令］

url-db update {server1 | server2 | server3} {*ip-address* | *domain-name*} [vrouter *vrouter-name*]

no url-db update {server1 | server2 | server3}

［句法描述］

**server1	server2 |**	指定将要配置的服务器。

server3	
ip-address | *domain-name*	指定更新服务器的名称，可以是 IP 地址形式（*ip-address*）也可以是域名形式（*domain-name*，例如 update1.hillstonenet.com）。
vrouter *vrouter-name*	指定更新服务器的 VRouter。

［默认取值］

server1：update1.hillstonenet.com

server2：update2.hillstonenet.com

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **url-db update server2 update2.hillstonenet.com**

url-db-query

启用 URL 查询服务器。使用该命令 no 的形式取消查询服务器的指定。

［命令］

url-db-query {server1 | server2} enable

no url-db-query {server1 | server2} enable

［句法描述］

server1 | server2	指定将要启用的查询服务器。

［默认取值］

未开启。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **url-db-query server1 enable**

url-db-query server

配置 URL 查询服务器。使用该命令 no 的形式取消查询服务器的指定。

［命令］

url-db-query {**server1** | **server2**} {*ip-address* | *domain-name*} [**vrouter** *vrouter-name*] [**port** *port*] [**encrypt-type** *BCAP*]

no url-db-query {**server1** | **server2**} **enable**

［句法描述］

server1 | **server2**	指定将要配置的 URL 查询服务器。
ip-address | *domain-name*	指定查询服务器的名称，可以是 IP 地址形式（*ip-address*）也可以是域名形式（*domain-name*，例如 url1.hillstonenet.com）。
vrouter *vrouter-name*	指定查询服务器的 VRouter。
port *port*	指定查询服务器的服务端口号。
encrypt-type *BCAP*	指定查询服务器的数据加密类型，目前仅为 BCAP 类型。

［默认取值］

server1：url1.hillstonenet.com

server2：url2.hillstonenet.com

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **url-db-query server1 url1.hillstonenet.com**

url-profile

创建 URL 过滤 Profile。使用该命令 no 的形式删除指定的 URL 过滤 Profile。

［命令］

url-profile *profile-name*

no url-profile *profile-name*

［句法描述］

profile-name	指定所创建的 URL 过滤 Profile 的名称，并且进入该 URL 过滤 Profile 的配置模式。如果指定名称已存在，则直接进入 URL 过滤 Profile 配置模式。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# url-profile url1
```

webpost

将 URL 过滤 Profile 绑定到策略规则。使用该命令 no 的形式取消绑定。

［命令］

webpost *profile-name*

no webpost

［句法描述］

profile-name	指定所需要绑定的 Web 外发信息 Profile 名称。

［默认取值］

无。

［命令模式］

策略规则配置模式。

［使用指导］

进入策略规则配置模式需要进行两步配置。首先，在全局配置模式下，输入“**policy-global**”命令进入策略配置模式；然后，在策略配置模式下，输入“**rule** [**id** *id-number*]”命令进入策略规则配置模式。

［命令实例］

```
hostname(config)# policy-global
hostname(config-policy)# rule id 1
hostname(config-policy-rule)# webpost webpost1
```

webpost all

指定控制所有 Web 外发信息和相应的控制动作。使用该命令 no 的形式取消控制所有 Web 外发信息的指定。

［命令］

webpost all [block] [log] [content]

no webpost all

［句法描述］

block	指定阻止所有信息发布行为。
log	指定对所有信息发布行为进行日志记录。
content	指定记录发布的信息内容。只有当安全网关支持并已配置存储设备（存储设备指 SD 存储卡、U 盘和 Hillstone 山石网科提供的存储扩展模块），而且已安装网络行为控制许可证时，才能配置该参数。

［默认取值］

无。

［命令模式］

Web 外发信息 Profile 配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# webpost-profile w1
hostname(config-webpost-profile)# webpost all log content
```

webpost-profile

创建 Web 外发信息 Profile。使用该命令 no 的形式删除指定的 Web 外发信息 Profile。

［命令］

webpost-profile *profile-name*

no webpost-profile *profile-name*

［句法描述］

profile-name	指定所创建的 Web 外发信息 Profile 的名称，并且进入该 Web 外发信息 Profile 的配置模式。如果指定名称已存在，则直接进入 Web 外发信息 Profile 配置模式。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# webpost-profile profile1
```

GTP防护命令

apn

创建 APN 过滤规则。使用该命令 no 的形式取消 APN 过滤规则的指定。

［命令］

apn *apn-name* **select {net | ms | verified | all} id** *id*

no apn id *id*

［句法描述］

apn-name	指定接入点名称。长度范围为 1 到 255 个字符的字符串。支持通配符“*”和“？”。
select {net | ms | verified | all}	指定选择模式。选择模式表明 APN 的来源以及有没有进行用户签约验证。**net** 表示网络提供 APN，没有进行用户签约验证；**ms** 表示移动站提供 APN，没有进行用户签约验证；**verified** 表示网络或者移动站提供 APN，已进行用户签约验证；**all** 表示任意选择模式。
id *id*	过滤规则 ID。取值范围为 1 到 512。

［默认取值］

无。

［命令模式］

GTP Profile 配置模式。

［使用指导］

系统允许与 APN 规则相匹配的 GTP 流量通过。

系统允许最多创建 64 条 APN 过滤规则。

［命令实例］

```
hostname(config)# gtp-profile mail1
hostname(config-gprs)# apn mobiphone.com.mnc123.mcc456.gprs select all id 1
```

gtp-profile（创建GTP Profile）

创建 GTP Profile。使用该命令 no 的形式删除指定的 GTP Profile。

［命令］

gtp-profile *profile-name*

no gtp-profile *profile-name*

［句法描述］

profile-name	指定所创建的 GTP Profile 的名称，并且进入该 GTP Profile 的配置模式。如果指定名称已存在，则直接进入 GTP Profile 配置模式。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

系统允许最多创建 16 个 GTP Profile。

［命令实例］

```
hostname(config)# gtp-profile mail1
hostname(config-gprs)#
```

gtp-profile（绑定GTP Profile到策略规则）

将 GTP Profile 绑定到策略规则。使用该命令 no 的形式取消 GTP Profile 的绑定。

［命令］

gtp-profile *profile-name*

no gtp-profile *profile-name*

［句法描述］

profile-name	指定所绑定到策略规则的 GTP Profile 的名称。

［默认取值］

无。

［命令模式］

策略规则配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# policy-global
```

```
hostname(config-policy)# rule
hostname(config-policy-rule)# gtp-profile gprs-protect
```

imsi

创建 IMSI 过滤规则。使用该命令 no 的形式取消 IMSI 过滤规则的指定。

［命令］

imsi *mcc-mnc-value* **apn** *apn-name* **select** {**net** | **ms** | **verified** | **all**} **action** {**drop** | **pass**} **id** *id*

no imsi id *id*

［句法描述］

mcc-mnc-value	指定 IMSI 十六进制编码。长度范围为 1 到 15 个数字。支持通配符“*”和“？”。
apn-name	指定接入点名称。长度范围为 1 到 255 个字符的字符串。支持通配符“*”和“？”。
select {**net** | **ms** | **verified** | **all**}	指定选择模式。选择模式表明 APN 的来源以及有没有进行用户签约验证。**net** 表示网络提供 APN，没有进行用户签约验证；**ms** 表示移动站提供 APN，没有进行用户签约验证；**verified** 表示网络或者移动站提供 APN，已进行用户签约验证；**all** 表示任意选择模式。
action {**drop** | **pass**}	指定允许通过（**pass**）或者丢弃（**drop**）与该规则相匹配的 GTP 报文。
id *id*	过滤规则 ID。取值范围为 1 到 512。

［默认取值］

无。

［命令模式］

GTP Profile 配置模式。

［使用指导］

系统允许最多创建 64 条 IMSI 过滤规则。

［命令实例］

```
hostname(config)# gtp-profile mail1
hostname(config-gprs)# imsi ef12bcffn apn
mobiphone.com.mnc123.mcc456.gprs select all action pass id 1
```

imei

创建 IMEI 过滤规则。使用该命令 no 的形式取消 IMEI 过滤规则的指定。

［命令］

imei *uli-sv-value* **apn** *apn-name* **select {net | ms | verified | all} action {drop | pass} id** *id*

no imei id *id*

［句法描述］

uli-sv-value	指定 IMEI 十六进制编码。长度范围为 1 到 15 个数字。支持通配符“*”和“？”。
apn-name	指定接入点名称。长度范围为 1 到 255 个字符的字符串。支持通配符“*”和“？”。
select {net | ms | verified | all}	指定选择模式。选择模式表明 APN 的来源以及有没有进行用户签约验证。**net** 表示网络提供 APN，没有进行用户签约验证；**ms** 表示移动站提供 APN，没有进行用户签约验证；**verified** 表示网络或者移动站提供 APN，已进行用户签约验证；**all** 表示任意选择模式。
action {drop | pass}	指定允许通过（**pass**）或者丢弃（**drop**）与该规则相匹配的 GTP 报文。
id *id*	过滤规则 ID。取值范围为 1 到 512。

［默认取值］

无。

［命令模式］

GTP Profile 配置模式。

［使用指导］

系统允许最多创建 64 条 IMEI 过滤规则。

［命令实例］

```
hostname(config)# gtp-profile mail1
hostname(config-gprs)# imei acc12bcffn apn
mobiphone.com.mnc123.mcc456.gprs select all action pass id 4
```

message-type

配置 GTP 消息类型过滤功能。使用该命令 no 的形式取消对指定类型消息的过滤配置。

［命令］

message-type *message-type*

no message-type *message-type*

［句法描述］

message-type	指定过滤的消息类型。支持过滤的消息类型可以为 create-aapdp、create-pdp、delete-aapdp、delete-pdp、error-indication、failure-report、identification、note-ms、pdu-notify、send-route、sgsn-context 或者 update-pdp。

［默认取值］

无。

［命令模式］

GTP Profile 配置模式。

［使用指导］

系统拒绝指定消息类型的 GTP 流量通过。

［命令实例］

hostname(config)# **gtp-profile mail1**

hostname(config-gprs)# **message-type create-aapdp**

message gtp-in-gtp-deny

开启 GTP-in-GTP 过滤功能。使用该命令 no 的形式关闭 GTP-in-GTP 过滤功能。

［命令］

message gtp-in-gtp-deny

no message gtp-in-gtp-deny

［句法描述］

无。

［默认取值］

无。

［命令模式］

GTP Profile 配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **gtp-profile mail1**

```
hostname(config-gprs)# message gtp-in-gtp-deny
```

message length

配置 GTP 消息长度限制功能。使用该命令 no 的形式恢复默认消息长度限制范围。

［命令］

message length *min-length max-length*

no message length

［句法描述］

min-length max-length	指定 GTP 消息的最小长度（*min-length*）和最大长度（*max-length*）。单位为字节，取值范围为 8-8192。

［默认取值］

min-length：8 字节。

max-length：8192 字节。

［命令模式］

GTP Profile 配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# gtp-profile mail1
hostname(config-gprs)# message length 8 7900
```

message log

开启 GTP 日志功能。使用该命令 no 的形式关闭 GTP 日志功能。

［命令］

message log

no message log

［句法描述］

无。

［默认取值］

无。

［命令模式］

GTP Profile 配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# gtp-profile mail1
hostname(config-gprs)# message log
```

message rate

配置 GTP 消息速率限制功能。

［命令］

message rate *value*

［句法描述］

value	指定 GTP 消息速率。单位为个/秒。如果指定为 0 则表示不进行限制。

［默认取值］

无。

［命令模式］

GTP Profile 配置模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# gtp-profile mail1
hostname(config-gprs)# message rate 100000
```

message sanity-check

开启协议异常检查功能。使用该命令 no 的形式关闭协议异常检查功能。

［命令］

message sanity-check

no message sanity-check

［句法描述］

无。

［默认取值］

无。

［命令模式］

GTP Profile 配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **gtp-profile mail1**

hostname(config-gprs)# **message sanity-check**

---

rat

创建 RAT 过滤规则。使用该命令 no 的形式取消 RAT 过滤规则的指定。

［命令］

rat *rat-value* **apn** *apn-name* **select {net | ms | verified | all} action {drop | pass} id** *id*

no rat id *id*

［句法描述］

rat-value	指定 RAT 编码。取值范围为 1 到 5 个数字。支持通配符“*”和“？”。1 表示 UTRAN 技术，2 表示 GERAN 技术，3 表示 WLAN 技术，4 表示 GAN 技术，5 表示 HSPA Evolution 技术，*表示 1 至 5 中的任意一种技术。
apn-name	指定接入点名称。长度范围为 1 到 255 个字符的字符串。支持通配符“*”。
select {net | ms | verified | all}	指定选择模式。选择模式表明 APN 的来源以及有没有进行用户签约验证。**net** 表示网络提供 APN，没有进行用户签约验证；**ms** 表示移动站提供 APN，没有进行用户签约验证；**verified** 表示网络或者移动站提供 APN，已进行用户签约验证；**all** 表示任意选择模式。
action {drop | pass}	指定允许通过（**pass**）或者丢弃（**drop**）与该规则相匹配的 GTP 报文。
id *id*	过滤规则 ID。取值范围为 1 到 512。

［默认取值］

无。

［命令模式］

GTP Profile 配置模式。

［使用指导］

系统允许最多创建 64 条 RAT 过滤规则。

［命令实例］

```
hostname(config)# gtp-profile mail1
hostname(config-gprs)# rat * apn mobiphone.com.mnc123.mcc456.gprs
select all action pass id 2
```

rai

创建 RAI 过滤规则。使用该命令 no 的形式取消 RAI 过滤规则的指定。

［命令］

rai *rai-value* **apn** *apn-name* **select {net | ms | verified | all} action {drop | pass} id** *id*

no rai id *id*

［句法描述］

rai-value	指定 RAI 十六进制编码。长度范围为 1 到 12 个数字。支持通配符“*”和“？”。
apn-name	指定接入点名称。长度范围为 1 到 255 个字符的字符串。支持通配符“*”和“？”。
select {net | ms | verified | all}	指定选择模式。选择模式表明 APN 的来源以及有没有进行用户签约验证。**net** 表示网络提供 APN，没有进行用户签约验证；**ms** 表示移动站提供 APN，没有进行用户签约验证；**verified** 表示网络或者移动站提供 APN，已进行用户签约验证；**all** 表示任意选择模式。
action {drop | pass}	指定允许通过（**pass**）或者丢弃（**drop**）与该规则相匹配的 GTP 报文。
id *id*	过滤规则 ID。取值范围为 1 到 512。

［默认取值］

无。

［命令模式］

GTP Profile 配置模式。

［使用指导］

系统允许最多创建 64 条 RAI 过滤规则。

［命令实例］

```
hostname(config)# gtp-profile mail1
hostname(config-gprs)# rai ADCGB455FF apn
mobiphone.com.mnc123.mcc456.gprs select all action pass id 2
```

uli

创建 ULI 过滤规则。使用该命令 no 的形式取消 ULI 过滤规则的指定。

［命令］

uli *uli-value* **apn** *apn-name* **select** {**net** | **ms** | **verified** | **all**} **action** {**drop** | **pass**} **id** *id*

no uli id *id*

［句法描述］

uli-value	指定 ULI 十六进制编码。长度范围为 1 到 16 个数字。支持通配符“*”和“？”。
apn-name	指定接入点名称。长度范围为 1 到 255 个字符的字符串。支持通配符“*”和“？”。
select {**net** | **ms** | **verified** | **all**}	指定选择模式。选择模式表明 APN 的来源以及有没有进行用户签约验证。**net** 表示网络提供 APN，没有进行用户签约验证；**ms** 表示移动站提供 APN，没有进行用户签约验证；**verified** 表示网络或者移动站提供 APN，已进行用户签约验证；**all** 表示任意选择模式。
action {**drop** | **pass**}	指定允许通过（**pass**）或者丢弃（**drop**）与该规则相匹配的 GTP 报文。
id *id*	过滤规则 ID。取值范围为 1 到 512。

［默认取值］

无。

［命令模式］

GTP Profile 配置模式。

［使用指导］

系统允许最多创建 64 条 ULI 过滤规则。

［命令实例］

```
hostname(config)# gtp-profile mail1
```

```
hostname(config-gprs)# uli ccaGB455FF apn
mobiphone.com.mnc123.mcc456.gprs select all action pass id 2
```

Show命令

show aaa-server

查看 AAA 服务器的配置信息。

［命令］

show aaa-server [*server-name*]

［句法描述］

server-name	AAA 服务器的名称。

［默认取值］

无。

［命令模式］

任何模式。

［使用指导］

如果不指定服务器名称，则显示系统中所有 AAA 服务器的配置信息；如果指定 AAA 服务器名称，则显示指定 AAA 服务器的详细配置信息。

［命令实例］

```
hostname# show aaa-server
==============================================================
Name           Type    Address           Mapping-Rule
--------------------------------------------------------------
local          local
test1          radius  10.10.100.1       rule1
==============================================================
hostname# show aaa-server test1
==============================================================
aaa-server: test1
type: radius
role-mapping-rule : rule1
server address: 10.10.100.1
first  backup : 10.10.100.2

radius setting:
port: 1812      secret: U8FdHNEEBz6sNn5Mvqx3yWuLRWce
retries 3 time(s), timeout 3 second(s).
==============================================================
```

show ad zone

显示域的攻击防护配置信息和攻击防护统计信息。

［命令］

show ad zone *zone-name* {**configuration** | **statistics**}

［句法描述］

zone-name	指定域的名称。
configuration	显示指定域的攻击防护配置信息，例如各种攻击防护功能的开启状态以及警戒值等。
statistics	显示指定域的统计信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname# show ad zone trust configration
The configuration on zone trust:
=====================================================================
Attack defense type           threshold  action     status
---------------------------------------------------------------------
Tear Drop                     0          drop       off
IP Spoofing                   0          drop       on
Land Attack                   0          drop       off
IP Option                     0          drop       on
IP Fragment                   0          drop       on
Winnuke                       0          drop       off
Port Scan                     1          drop       on
TCP Anomaly                   0          drop       off
ICMP Flood                    1500       drop       on
Address Sweep                 1          drop       on
Ping of Death                 0          drop       on
Huge ICMP Packet              1024       drop       off
UDP Flood                     1500       drop       on
ip directed broadcast         0          drop       off
dns query flood               1500       drop       on
dns recursive query flood     1000       drop       on
---------------------------------------------------------------------
ARP spoofing
```

```
    reverse-query                                   on
    ip-number-per-mac                               off
    gratuitous arp rate       0                     off
-------------------------------------------------------------------
SYN Flood                 src_thres  dst_thres  action    status

                          1500       1500       drop      off
-------------------------------------------------------------------
                     min_rate   max_rate   timeout   action  status

SYN Proxy            1000       3000       30        drop    on
SYN Cookie           1000       3000       30        drop    on
===================================================================
```

hostname# **show ad zone untrust statistics**

```
Statistics counter on zone trust:
================================================================
Attack defense type                 Counter     State
----------------------------------------------------------------
Tear Drop                           0           off
IP Spoofing                         0           on
Land Attack                         0           off
IP Option                           0           on
IP Fragment                         0           on
Winnuke                             0           off
Port Scan                           0           on
Source SYN Flood                    0           off
Destination SYN Flood               0           off
SYN Proxy                           0           on
SYN Cookie                          0           on
TCP Anomaly                         0           off
ICMP Flood                          0           on
Address Sweep                       0           on
Ping of Death                       0           on
Huge ICMP Packet                    0           off
UDP Flood                           0           on
ip directed broadcast               0           off
dns query flood                     0           on
dns recursive query flood           0           on
ARP spoofing IP number per MAC      0           off
ARP spoofing reverse query          0           on
================================================================
```

show address

显示全局地址簿信息。信息包括地址条目信息、地址条目成员数以及成员的具体内容等。

［命令］

show address [*address-entry*] [**reference-zone** *zone-name*]

［句法描述］

address-entry	显示指定地址条目的信息。
zone-name	显示参考域对应的地址条目。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

如果不指定任何参数，将显示全局地址簿中的所有信息。

［命令实例］

```
hostname# show address
Total entry count: 2.
==========================================================
Address-name     Member-count  Members
----------------------------------------------------------
abc              2             2.2.2.2/24 2.2.3.1-2.2.3.4
Any              1             0.0.0.0/0
----------------------------------------------------------

Hostname# show address abc
Name:           abc
Total ip count: 260
Member count:   2
Members:
 2.2.2.2/24                     2.2.3.1-2.2.3.4
```

show admin host

显示系统的所有可信主机及登录类型信息，或显示指定主机的登录类型信息。

［命令］

show admin host [*A.B.C.D A.B.C.D* | **any**]

［句法描述］

A.B.C.D A.B.C.D	显示指定网段的登录类型信息。
any	显示 any（所有 ip 地址）的登录类型信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname# show admin host
```

show admin user

显示终端用户信息。

［命令］

show admin user

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname# show admin user
=========================================================
Username        Privilege  Console Telnet SSH HTTP HTTPS
---------------------------------------------------------
hillstone       RXW        Y       Y      Y   Y    Y
=========================================================
```

show app logging

显示系统应用安全日志配置状态。

［命令］

show app logging

［句法描述］

无

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show app logging**

---

show arp

显示 MAC 地址与 IP 地址对应信息。

［命令］

show arp [*A.B.C.D* | **generic** | **interface** *interface-name* | **vrouter** *vrouter-name*]

［句法描述］

A.B.C.D	显示指定 IP 地址的 ARP 信息。
generic	显示 ARP 概要信息。
interface-name	显示指定接口的 ARP 信息。
vrouter-name	显示指定 VRouter 的 ARP 信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname# show arp generic
```

show arp-spoofing-statistics

显示 ARP 欺骗攻击统计信息。

［命令］

show arp-spoofing-statistics [*number*]

［句法描述］

number	显示统计数最高的前 *number* 条记录。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname# show arp generic
```

show auth-user

显示通过认证的用户信息。

［命令］

show auth-user [*A.B.C.D* | **name** *user-name* | **web-auth** | **scvpn**]

［句法描述］

A.B.C.D	显示指定 IP 地址的在线用户信息。
name *user-name*	显示指定用户名的在线用户信息。
web-auth	显示所有在线 Web 认证用户信息。
scvpn	显示所有在线 SCVPN 用户信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show auth-user scvpn**

show auth-user agent

显示当前在线的 Active-Directory 服务器监控用户信息。

［命令］

show auth-user agent [**interface** *interface-name* | **vrouter** *vrouter-name*]

［句法描述］

interface *interface-name*	指定接口名称。
vrouter *vrouter-name*	指定 VRouter 名称。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show auth-user agent interface ethernet0/0**

show auth-user l2tp

显示所有 L2TP 实例当前在线的客户端信息。

［命令］

show auth-user l2tp [**interface** *interface-name* | **vrouter** *vrouter-name*]

［句法描述］

interface *interface-name*	指定接口名称。
vrouter *vrouter-name*	指定 VRouter 名称。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show auth-user l2tp interface ethernet0/1**

show auth-user webauth

查看在线的 Web 认证用户信息。

［命令］

show auth-user webauth

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show auth-user webauth**

show av-profile

查看设备的病毒过滤 profile 信息。

［命令］

show av-profile

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show av-profile**

---

show av signature info

查看设备的病毒库信息，包括病毒库版本、发布日期以及病毒特征个数等。

［命令］

show av signature info

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show arp generic**

show av zone-binding

查看安全域与病毒过滤 Profile 的绑定信息。

［命令］

show av zone-binding

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname(config-zone-trust)# show av zone-binding
=====================================================================
Name                            Type    AV-profile
---------------------------------------------------------------------
trust                             L3    av-test
=====================================================================
```

show behavior-object

查看行为 Profile 的对象信息。

［命令］

show behavior-object [**behavior-profile** *behavior-profile-name*]

［句法描述］

behavior-profile-name	显示指定行为 Profile 的对象信息。若不指定，显示系统中所有行为 Profile 的对象信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show behavior-object**

show behavior-profile

显示行为 Profile 的具体信息。

［命令］

show behavior-profile [*behavior-profile-name*]

［句法描述］

behavior-profile-name	显示指定行为 Profile 的信息。若不指定 Profile 名称，显示系统中所有行为 Profile 的信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show behavior-profile**

show block-ip

显示被阻断的 IPS 攻击 IP 地址的信息。

［命令］

show block-ip

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname# show block-ip
Total:  1
==============================
VROUTER    IP            AGE
------------------------------
trust-vr   100.100.0.2     20
==============================
```

show block-notification

显示用户被阻断警告功能的启用状态。

［命令］

show block-notification

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

功能开启时，显示 **block-notification enable**；功能关闭时，显示 **block-notification disable**。

［命令实例］

```
hostname# show block-notification
Block notification enable
```

show block-service

显示被阻断的 IPS 攻击服务的信息。

［命令］

show block-service

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname# show block-service
Total:  1
=========================================================
VROUTER    SRC-IP       DST-IP       D-PORT  PROT   AGE
---------------------------------------------------------
trust-vr   100.100.0.2  100.100.0.3  23      5      20
=========================================================
```

show class-map

显示 class 的信息。

［命令］

show class-map *class-name*

［句法描述］

class-name	指定 class 的名称。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname# show class-map class1
```

show clock

显示系统的时间信息。

［命令］

show clock

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname# show clock
Current time zone: UTC
Wed Jan  3 19:03:52 UTC 2007
```

show configuration

显示系统的当前配置信息。

［命令］

show configuration

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show configuration**

show configuration saved

显示系统的当前起始配置信息。

［命令］

show configuration saved [current]

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show configuration saved**

show configuration saved

显示系统的备份起始配置信息。

［命令］

show configuration saved *number*

［句法描述］

number	指定显示该标记号的备份起始配置信息。范围是 0 到 8。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname# show configuration saved 0
```

show configuration saved record

显示系统备份起始配置信息的记录。系统记录最近十次保存的配置信息，最近一次保存的配置信息会记录为系统的当前起始信息。前九次的配置信息按照保存时间的远近以数字 0 到 8 作为标记，当前系统配置信息以“current”作为标记。用户可以通过该命令查看备份起始配置信息的记录。

［命令］

```
show configuration saved record
```

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname# show configuration saved record
current 2007-01-03 19:01:46 by hostname via cli, size is 1286 bytes
0       2007-01-01 00:50:12 by hostname via cli, size is 1285 bytes
```

show console

显示 Console 信息。

［命令］

show console

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show console**

---

show contentfilter-profile

显示内容过滤 Profile 配置。

［命令］

show contentfilter-profile [*profile-name*]

［句法描述］

profile-name	显示指定内容过滤 Profile 的信息。不指定本选项时，将显示所有内容过滤 Profile 的信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show contentfilter-profile**

show contentfilter category

显示类别信息。

［命令］

show contentfilter category

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show contentfilter category**

show contentfilter count

显示类别和关键字的数目。

［命令］

show contentfilter count

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname# show contentfilter count
```

show contentfilter keyword

显示关键字信息。

［命令］

show contentfilter keyword

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname# show contentfilter keyword
```

show cpu

显示 CPU 利用情况。

［命令］

show cpu

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname# show cpu
```

show database

显示本地数据库信息。

［命令］

show database

［句法描述］

无。

［默认取值］

无。

［命令模式］

任何命令模式。

［使用指导］

无。

［命令实例］

```
hostname# show database
```

show debug

显示系统的调试开关状态信息。

［命令］

show debug

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何命令模式。

［使用指导］

无。

［命令实例］

```
hostname# show debug
```

show dhcp-server

显示 DHCP 地址池的绑定信息或统计信息。

［命令］

show dhcp-server {binding | statistics} *pool-name*

［句法描述］

pool-name	显示指定地址池的信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname# show dhcp-server binding dhcp_pool1
```

show dhcp-snooping binding

显示 DHCP 监控列表信息。

［命令］

show dhcp-snooping binding

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show dhcp-snooping binding**

show dhcp-snooping configuration

显示 DHCP 监控功能的配置信息。

［命令］

show dhcp-snooping configuration

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show dhcp-snooping configuration**

show dnat rule

显示 DNAT 配置信息。

［命令］

show dnat rule [*id*] [**vrouter** *vrouter-name*]

［句法描述］

id	显示指定 ID 号的 DNAT 规则。
vrouter-name	显示指定 VRouter 的 DNAT 规则信息。如果不指定该参数，系统将显示缺省 VRouter（trust-vr）的 DNAT 规则。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

如果不指定 ID，则显示所有 DNAT 配置信息。

［命令实例］

```
hostname# show dnat rule
id  from      to      service    translate to     port
2   test1     test2   HTTP       test3            8080
1   test1     test2   FTP        test3            2121
```

show dnat server

显示内网服务器状态信息。

［命令］

show dnat server [*ip-address*] [**vrouter** *vrouter-name*] [**tcp-port** *port*] [**ping**]

［句法描述］

ip-address	显示指定 IP 地址的内网服务器状态信息。
vrouter *vrouter-name*	显示指定 VRouter 的内网服务器状态信息。如果不指定该参数，系统将显示缺省 VR 即 trust-vr 的内网服务器状态信息。
tcp-port *port*	显示指定端口号的内网服务器状态信息
ping	显示内网服务器的 Ping 监控状态信息

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

如果不指定参数，则显示所有内网服务器状态信息。

［命令实例］

```
hostname# show dnat server 5.5.5.5
=====================================================================
vr name:trust-vr
Server/Port          HA-Group       Status       Fails    DnatRule
```

```
5.5.5.5/21            0                Active        0          2
=====================================================================
Total 1 entries
```

show dns

显示 DNS 配置信息。

［命令］

show dns

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show dns**

show dns-address

显示地址簿中的主机条目信息。

［命令］

show dns-address

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show dns-address**

show dot1x

显示 802.1X 配置信息。

［命令］

show dot1x [**profile** *profile-name*| **port** *port-name*| **statistics** [*port-name*]]

［句法描述］

profile *profile-name*	显示指定的 802.1X Profile 配置信息。
port *port-name*	显示指定的认证系统端口的配置信息，以及其绑定的 Profile 信息。
statistics [*port-name*]	显示指定的认证系统端口的统计信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

如果不指定参数，则显示 802.1X 全局参数。

［命令实例］

hostname# **show dot1x profile profile1**

show dp-filter ip

显示调试信息过滤条件。

［命令］

show dp-filter ip

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show dp-filter ip**

---

show environment

显示设备温度及风扇转速信息。

［命令］

show environment

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show environment**

---

show external-bypass

显示外置 Bypass 信息。

［命令］

show external-bypass

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname# show external-bypass
=================================================================
external-bypass:enable
device status:present
current mode:normal
device info:BSFT,version 28
=================================================================
```

show fib

显示 FIB 统计信息。

［命令］

show fib

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname# show fib
```

show file

显示存储设备顶级目录下的文件信息。

［命令］

show file {sd0 | usb0 | usb1 | stroage*X*}

［句法描述］

sd0	显示 SD 卡槽中 SD 存储卡内的文件信息。
usb0 | usb1	显示与指定 USB 接口相连的存储设备中的文件信息。
stroage*X*	显示与指定存储扩展模块中的文件信息。*X* 为存储扩展模块的扩展槽号。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

使用该命令时，指定的 SD 卡槽、USB 接口或存储扩展槽上应连接有存储设备。

［命令实例］

hostname# **show file usb0**

show flow deny-session

查看 Deny Session 的配置信息。

［命令］

show flow deny-session

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# show flow deny-session
Deny session:
 Percentage: 5
 Timeout: 3
 Deny-type: ad policy route self session-limit
```

show fragment

显示分片信息。

［命令］

show fragment

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname# show fragment
```

show ftp

显示系统中 FTP 服务配置信息。

［命令］

show ftp {port | user}

［句法描述］

port	查看 FTP 端口号。
user	查看 FTP 用户名、密码和在线状态。

stroage*X*	显示与指定存储扩展模块中的文件信息。*X* 为存储扩展模块的扩展槽号。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

使用该命令时，指定的 SD 卡槽、USB 接口或存储扩展槽上应连接有存储设备。

［命令实例］

```
hostname# show file usb0
```

show gtp-profile

显示系统中 GTP Profile 的配置信息。

［命令］

show gtp-profile *profile-name profile-subitem*

［句法描述］

profile-name	查看指定名称的 GTP Profile 的配置信息。
profile-subitem	查看 GTP Profile 的子项配置信息。包括 IE 过滤（APN、IMEI、IMSI、RAI、RAT、ULI）配置信息和消息类型过滤配置信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname# show gtp-profile gprs1
=====================================
GTP Profile:     gprs-protect
Sanity Check:    Disabled
GTP in GTP:      Enabled
```

```
Rate:           0 /Second
Length:         [8, 2400] Bytes
Log:            Enabled
Log Interval:   0 Second

------------------------------
Table     Rules   Capcitity
APN       1       64
IMSI      0       64
IMEI      0       64
RAI       0       64
RAT       0       64
ULI       0       64
--------------------------------------
```

show ha cluster

显示 HA 簇配置信息。

［命令］

show ha cluster

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# show ha cluster
HA is disabled
```

show ha flow statistics

显示 HA 统计信息。

［命令］

show ha flow statistics

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname(config)# **show ha flow statistics**

---

show ha group

显示 HA 组配置信息。

［命令］

show ha group {**config** | *group-id*}

［句法描述］

config	显示设备 HA 配置信息。
group-id	显示指定 HA 组的配置信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname(config)# **show ha group config**

```
Group Id:        0
Group Name:
Heart beat time:  1000(ms)
Heart beat num:  3
Priority:        100
Preempt:         0(s)
Gratuious arp:   5
Monitor
```

show ha link status

显示 HA 连接配置状态信息。

［命令］

show ha link status

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# show ha link status
Ha link status:
Ha link ip=0.0.0.0
```

show ha protocol statiscitc

显示接收和发送的 HA 协议统计信息。

［命令］

show ha protocol statiscitc

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# show ha protocol statiscitc
```

show ha sync state

显示 HA 同步状态。

［命令］

show ha sync state {pki | dns | dhcp | vpn | ntp | config | flow | scvpn | l2tp | route}

［句法描述］

pki	显示 PKI 信息的同步状态。
dns	显示 DNS 信息的同步状态。
dhcp	显示 DHCP 信息的同步状态。
vpn	显示 VPN 信息的同步状态。
ntp	显示 NTP 信息的同步状态。
config	显示配置信息的同步状态。
flow	显示 Flow 信息的同步状态。
scvpn	显示 SCVPN 信息的同步状态。
l2tp	显示 L2TP 信息的同步状态。
route	显示路由信息的同步状态。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# show ha sync state flow
Ha is syned
```

```
hostname(config)# show ha sync state pki
Ha is syned
```

show ha sync statistic

显示 HA 同步统计信息。

［命令］

show ha sync statistic {pki | dns | dhcp | vpn | ntp | config | scvpn | route}

［句法描述］

pki	显示 PKI 同步统计信息。
dns	显示 DNS 同步统计信息。
dhcp	显示 DHCP 同步统计信息。
vpn	显示 VPN 同步统计信息。
ntp	显示 NTP 同步统计信息。
config	显示配置同步统计信息。
scvpn	显示 SCVPN 同步统计信息。
route	显示路由同步统计信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# show ha sync statistic pki
Ha sync statistic
    Recevice ha sycn pki packets: 0
    Send ha sycn pki packets: 0
```

show host-blacklist

显示 MAC 地址或 IP 地址的主机黑名单条目。

［命令］

show host-blacklist {mac | ip}

［句法描述］

mac	显示所有 MAC 地址的主机黑名单条目。
ip	显示所有 IP 地址的主机黑名单条目。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# show host-blacklist mac
```

show http

显示 Web 信息。

［命令］

show http

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# show http
Http server options:
==========================================================
web(http/https) idle timeout is: 1440 minute(s)
http port is: 80
https port is: 443
https trust domain is: trust_domain_default
==========================================================
```

show im-object

查看受控制的即时通讯工具帐号信息。

［命令］

show im-object [**im-profile** *profile-name*]

［句法描述］

im-profile *profile-name*	显示指定网络聊天 Profile 中的受控即时通讯工具帐号信息。若不指定，显示系统中所有受控制的即时通讯工具帐号信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show im-object im-profile im1**

show im-profile

查看网络聊天 Profile 信息。

［命令］

show im-profile [*profile-name*]

［句法描述］

profile-name	显示指定名称的网络聊天 Profile 信息。如不指定该参数，显示所有网络聊天 Profile 信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show im-profile im1**

show image

显示系统固件信息。

［命令］

show image

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show image**

show interface

显示接口表或指定接口的信息。

［命令］

show interface [*interface-name*]

［句法描述］

interface-name	要查看信息的接口的名称。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

如果不指定接口名称，则显示接口表的信息。

［命令实例］

hostname# **show interface**

hostname# **show interface ethernet0/0**

show interface bind-tunnels

显示特定隧道接口的配置信息。

［命令］

show interface bind-tunnels *tunnel-name*

［句法描述］

tunnel-name	指定需要查看的隧道接口的名称。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show interface**

hostname# **show interface bind-tunnels tunnel1**

show interface supervlanX

显示特定 super-VLAN 接口的配置信息。

［命令］

show interface supervlan*X*

［句法描述］

X	指定需要查看的 super-VLAN 接口的编号。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show interface supervlan1**

---

show inventory

查看扩展卡的基本信息。

［命令］

show inventory

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

仅适用于 Hillstone 模块化安全网关。

［命令实例］

hostname# **show inventory**

---

show ip bgp

显示整个 BGP 路由表的路由信息。

［命令］

show ip bgp [*A.B.C.D* | *A.B.C.D/M*]

［句法描述］

A.B.C.D | *A.B.C.D/M*	显示到指定网络的 BGP 路由信息。

［默认取值］

无。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show ip bgp**

show ip bgp neighbor

显示 BGP 对等体状态。

［命令］

show ip bgp neighbor [*A.B.C.D*]

［句法描述］

A.B.C.D	显示指定对等体的状态。

［默认取值］

无。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show ip bgp neighbor 192.168.1.1**

show ip bgp paths

显示 BGP 数据库中存储的所有自治系统路径信息。

［命令］

show ip bgp paths

［句法描述］

无。

［默认取值］

无。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show ip bgp paths**

---

show ip bgp summary

显示所有 BGP 连接的状态参数，包括前缀、路径和属性信息等。

［命令］

show ip bgp summary

［句法描述］

无。

［默认取值］

无。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show ip bgp summary**

---

show ip hosts

查看 DNS 映射条目。

［命令］

show ip hosts [*host-name*]

［句法描述］

host-name	显示指定主机的 DNS 映射条目。

［默认取值］

无。

［命令模式］

任何模式。

［使用指导］

如果不指定主机名，则显示所有主机的 DNS 映射信息。

［命令实例］

hostname# **show ip hosts**

---

show ip igmp-proxy

查看 IGMP Proxy 信息。

［命令］

show ip igmp-proxy [*A.B.C.D*] [**vrouter** *name*]

［句法描述］

show ip igmp-proxy	显示系统中全部 IGMP Proxy 信息。
A.B.C.D	显示指定的组播组地址的 IGMP Proxy 信息。
vrouter *name*	显示指定的 VRouter 下的 IGMP Proxy 信息。

［默认取值］

无。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show ip igmp-proxy vrouter trust-vr**

---

show ip igmp-snooping

查看 IGMP Snooping 信息。

［命令］

show ip igmp-snooping [*A.B.C.D*] [**vswitch** *name*]

［句法描述］

show ip igmp-snooping	显示全部 IGMP Snooping 信息。
A.B.C.D	显示指定的组播组地址的 IGMP Snooping 信息。
vrouter *name*	显示指定的 VSwitch 下的 IGMP Snooping 信息。

［默认取值］

无。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show ip igmp-snooping vswitch vswitch1**

show ip mroute

查看组播路由信息。

［命令］

show ip mroute [*A.B.C.D A.B.C.D*| **static**| **summary**] [**vrouter** *vrouter-name*]

［句法描述］

A.B.C.D A.B.C.D	通过指定组播源地址和组播地址，显示其组播路由信息。第一个 A.B.C.D 为组播源地址，第二个 A.B.C.D 为组播地址。
static	显示静态组播路由信息。
summary	显示组播路由的摘要信息。
vrouter *vrouter-name*	显示指定 VRouter 下的组播路由信息。

［默认取值］

无。

［命令模式］

任何模式。

［使用指导］

如果不指定参数，则显示所有组播路由信息。

［命令实例］

hostname# **show ip mroute**

```
hostname# show ip mroute 1.1.1.2 224.91.91.2
hostname# show ip mroute static trust-vr
```

---

show ip ospf

查看 OSPF 信息。

［命令］

show ip ospf

［句法描述］

无。

［默认取值］

无。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname# show ip ospf
```

---

show ip ospf database

查看 OSPF 协议的数据库信息。

［命令］

show ip ospf database

［句法描述］

无。

［默认取值］

无。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show ip ospf database**

show ip ospf database

查看 OSPF 协议的数据库具体信息。

［命令］

show ip ospf database {asbr-summary | external | network | router | summary} [*A.B.C.D*] [{**adv-router** *A.B.C.D*} | **self-originate**] [**vrouter** *vrouter-name*]

show ip ospf database [**max-age** | **self-originate**] [**vrouter** *vrouter-name*]

［句法描述］

asbr-summary	显示自治系统边界路由器概要 LSA 的信息。
external	只显示外部 LSA 的有关信息。
network	只显示网络 LSA 的有关信息。
router	只显示路由器 LSA 的有关信息。
summary	只显示概要 LSA 的有关信息。
A.B.C.D	链路状态 ID，以 IP 地址形式表示。
adv-router *A.B.C.D*	显示指定路由器的所有 LSA。
self-originate	只显示自己产生的 LSA（从本地路由器）。
max-age	指定最大老化时间。
vrouter-name	指定 VRouter 名称。

［默认取值］

无。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show ip ospf database network self-originate**

show ip ospf interface

查看 OSPF 接口信息。

［命令］

show ip ospf interface [*interface-name*] [**vrouter** *vrouter-name*]

［句法描述］

interface-name	指定接口名称。
vrouter-name	指定 VRouter 名称。

［默认取值］

无。

［命令模式］

任何模式。

［使用指导］

如果不指定接口名称，则显示 OSPF 的所有接口信息。

［命令实例］

hostname# **show ip ospf interface ethernet0/2**

show ip ospf neighbor

查看 OSPF 相邻路由器信息。

［命令］

show ip ospf neighbor [*A.B.C.D* | **detail**] [**vrouter** *vrouter-name*]

［句法描述］

A.B.C.D	指定相邻路由器的 ID。
detail	显示所有相邻路由器的详细信息
vrouter-name	指定 VRouter 名称。

［默认取值］

无。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname# show ip ospf neighbor detail
```

show ip ospf route

查看 OSPF 路由信息。

［命令］

show ip ospf route [*ip-address/netmask*] [**vrouter** *vrouter-name*]

［句法描述］

ip-address/netmask	查看指定网段的 OSPF 路由信息。
vrouter-name	指定 VRouter 名称。

［默认取值］

无。

［命令模式］

任何模式。

［使用指导］

如果不指定网段，则显示所有 OSPF 路由信息。

［命令实例］

```
hostname# show ip ospf route
```

show ip ospf virtual-links

查看 OSPF 虚拟链路信息。

［命令］

show ip ospf virtual-links [**vrouter** *vrouter-name*]

［句法描述］

vrouter-name	指定 VRouter 名称。

［默认取值］

无。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show ip ospf virtual-links**

show ip rip

查看 RIP 信息。

［命令］

show ip rip

［句法描述］

无。

［默认取值］

无。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show ip rip**

show ip rip database

查看 RIP 数据库的信息。

［命令］

show ip rip database [*A.B.C.D/M*] [**vrouter** *vrouter-name*]

［句法描述］

A.B.C.D/M	显示指定目的 IP 地址的 RIP 信息。
vrouter *vrouter-name* **inactive**	显示指定 VRouter 的 RIP 信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

如果不指定 IP 地址，则显示 RIP 数据库的信息。

［命令实例］

hostname# **show ip rip database**

---

show ip route

显示路由信息。

［命令］

show ip route [**static** | **inactive**]

［句法描述］

static	显示目的路由信息。
inactive	显示未被使用的 SA 的配置信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show ip route static**

---

show ip route isp

查看 ISP 路由条目。

［命令］

show ip route isp [*isp-name* | **vrouter** *vrouter-name*]

［句法描述］

isp-name	显示指定 ISP 的路由信息。

vrouter-name	显示指定 VRouter 的 ISP 路由信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show ip route isp isp1**

show ip route source

显示源路由信息。

［命令］

show ip route source

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show ip route source**

show ip route source in-interface

显示源接口路由信息。

［命令］

show ip route source in-interface *interface-name*

［句法描述］

interface-name	指定路由条目的入接口。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname# show ip route source in-interface ethernet0/2
```

show ips sigset

显示 IPS 特征集的具体信息，包括特征集名称、级别对应动作、协议相关其它选项配置、被引用信息以及特征集包含的具体特征等。

［命令］

show ips sigset [*sigset-name*]

［句法描述］

sigset-name	显示指定名称的特征集。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# show ips sigset
Total count: 53
==============================================================
IPS signature set dhcp
  Default actions:
    Attack-level  Action     Block   Seconds
    INFO          log        noblock       0
    WARNING       log        noblock       0
```

```
    CRITICAL       log        noblock       0
  Max scan bytes per direction: 0(Unlimited)
  Used by 1 IPS profiles:
        test
-------------------------------------------------------------
……
```

show ipsec sa

显示 IPSec 安全联盟的配置信息。

［命令］

show ipsec sa [*id* | **active** | **inactive**]

［句法描述］

id	显示指定 ID 的 SA 的配置信息。
active	显示激活状态的 SA 的配置信息。
inactive	显示未被使用的 SA 的配置信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show ipsec sa**

show ipsec proposal

显示 IPSec 安全提议的配置信息。

［命令］

show ipsec proposal [*proposal-name*]

［句法描述］

proposal-name	显示指定名称的安全提议的配置信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname# show ipsec proposal
```

show ip vrouter

显示 VRouter 信息。

［命令］

show ip vrouter [*vrouter-name*]

［句法描述］

vrouter-name	显示指定名称 VRouter 的信息。如果不指定该参数，系统将显示所有 VRouter 的信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# show ip vrouter
Total vrouter count: 2
=====================================================================
 Name                                Zone-count       VR_ID
---------------------------------------------------------------------
 trust-vr                                 5              1
 vrouter1                                 0              2
=====================================================================
```

show ips status

显示系统的 IPS 相关信息，包括入侵检测结果、系统 IPS 启用状态以及 IPS 特征码。

［命令］

show ips status

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname# show ips status
All IPS event detected: 0

IPS feature: enabled
IPS magic: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

show isakmp peer

显示 IKE 对等体的配置信息。

［命令］

show isakmp peer [*peer-name*]

［句法描述］

peer-name	显示指定名称的 IKE 对等体的配置信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show isakmp peer**

show isakmp proposal

显示 IKE 安全提议的配置信息。

［命令］

show isakmp proposal [*proposal-name*]

［句法描述］

proposal-name	显示指定名称的 IKE 安全提议的配置信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show isakmp proposal**

show isakmp sa

显示 IKE 安全联盟的配置信息。

［命令］

show isakmp sa [*dsp_ip*]

［句法描述］

dsp_ip	显示对端 IKE 安全联盟的配置信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show isakmp sa**

show isp-network

查看通过设备配置的 ISP 信息。

［命令］

show isp-network {**all** | *isp-name*}

［句法描述］

all	显示全部 ISP 信息。
isp-name	显示指定名称的 ISP 信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show isp-network all**

show l2tp client

查看 L2TP 实例当前在线的客户端信息。

［命令］

show l2tp client {**tunnel-name** *l2tp-tunnel-name* [**user** *user-name*]| **tunnel-id** *ID*}

［句法描述］

tunnel-name *l2tp-tunnel-name*	指定 L2TP 实例的名称。
user *user-name*	指定用户名称。

tunnel-id *ID*	指定隧道 ID。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname# show l2tp client tunnel-name l2tptunnel1 user user1
hostname# show l2tp client tunnel-id 2
```

show l2tp pool

查看 L2TP 地址池的配置信息。

［命令］

show l2tp pool [*pool-name*]

［句法描述］

pool-name	指定地址池的名称。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname# show l2tp pool pool1
```

show l2tp pool statistics

查看 L2TP 地址池的统计信息。

［命令］

show l2tp pool *pool-name* **statistics**

［句法描述］

pool-name	指定地址池的名称。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show l2tp pool pool1 statistics**

show l2tp tunnel

查看已创建的 L2TP 隧道的状态信息。

［命令］

show l2tp tunnel *l2tp-tunnel-name*

［句法描述］

l2tp-tunnel-name	指定 L2TP 实例的名称。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show l2tp tunnel l2tptunnel1**

show license

查看系统许可证信息。

［命令］

show license *license-name*

［句法描述］

license-name	许可证名称。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show license plat071220032206**

show load-balance rule

显示配置有负载均衡功能的 DNAT 规则相关信息。

［命令］

show load-balance rule [*id*]

［句法描述］

id	显示指定 ID 号的配置有负载均衡功能的 DNAT 规则信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show load-balance rule id 3**

show load-balance server

显示负载均衡服务器状态。

［命令］

show load-balance server [*ip-address*] [**vrouter** *vrouter-name*]

［句法描述］

ip-address	显示指定 IP 地址的负载均衡服务器状态信息。
vrouter-name	显示指定 VRouter 的负载均衡服务器状态信息。如果不指定该参数，系统将显示缺省 VR 即 trust-vr 的负载均衡服务器状态信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show load-balance server 1.1.1.1**

show logging

显示日志配置信息或者指定类型（debug、network、security、configuration 或 IPS）的日志信息。

［命令］

show logging

show logging {debug | network | security | configuration | ips}

［句法描述］

debug	显示调试日志信息。
network	显示网络日志信息。
security	显示安全日志信息。
configuration	显示配置日志信息。
ips	显示 IPS 日志信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show logging debug**

show logging alarm

显示告警日志信息。

［命令］

show logging alarm [severity {alerts | critical | emergencies}]

［句法描述］

severity	显示指定级别的日志信息。不指定该参数时显示所有级别的告警日志信息。
alerts	显示 Alerts 级别的告警日志信息。
critical	显示 Critical 级别的告警日志信息。
emergencies	显示 Emergencies 级别的告警日志信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show logging alarm**

show logging configuration

显示配置日志的信息。

［命令］

show logging configuration [admin *admin-name***]**

［句法描述］

admin *admin-name*	指定用户名称。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show logging configuration admin hillstone**

show logging event

显示事件日志信息。

［命令］

show logging event [severity {debugging | errors | informational | notifications | warnings }]

［句法描述］

severity	显示指定级别的事件日志信息。不指定该参数时显示所有级别的事件日志信息。
debugging	显示 Debugging 级别的事件日志信息。
errors	显示 Errors 级别的事件日志信息。
informational	显示 Informational 级别的事件日志信息。
notifications	显示 Notifications 级别的事件日志信息。
warnings	显示 Warnings 级别的事件日志信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show logging event severity errors**

show logging traffic

显示所有流量日志信息。

［命令］

show logging traffic

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show logging traffic**

show logging traffic filter-session

显示会话流量日志信息。

［命令］

show logging traffic filter-session [**src-ip** *A.B.C.D* | **src-port** *port-num* | **dst-ip** *A.B.C.D* | **dst-port** *port-num* | **protocol** {**icmp** | **tcp** | **udp** | **others**} | **policy-id** *policy-id* | **action** {**policy-deny** | **session-start** | **session-end** | **policy-default**}]

［句法描述］

src-ip *A.B.C.D*	显示指定源 IP 地址的会话信息。
src-port *port-num*	显示指定源端口号的会话信息。
dst-ip *A.B.C.D*	显示指定目的 IP 地址的会话信息。
dst-port *port-num*	显示指定目的端口号的会话信息。
protocol {**icmp** | **tcp** | **udp** | **others**}	显示指定协议的会话信息。 • **icmp** – 显示所有 ICMP 协议的会话日志信息； • **tcp** – 显示所有 TCP 协议的会话日志信息； • **udp** – 显示所有 UDP 协议的会话日志信息；

	• **others** – 显示除 ICMP、TCP 和 UDP 协议外的其他协议的会话日志信息。
policy-id *policy-id*	显示匹配指定策略规则的会话信息。
action {policy-deny | session-start | session-end | policy-default}	显示指定动作的会话信息。 • **policy-deny** – 显示被策略规则拒绝的会话信息； • **session-start** – 显示所有会话开始信息； • **session-end** – 显示所有会话结束信息； • **policy-default** – 显示所有与策略规则动作一致的会话信息。假如有两个策略规则，ID 分别为 1 和 2，1 对所有流量都是允许，2 对所有流量都是拒绝。当使用此参数查看会话信息时，将显示规则 1 允许的会话信息和规则 2 拒绝的会话信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show logging traffic filter-session protocol tcp**

show logging traffic filter-nat

显示所有 NAT 流量日志信息。

［命令］

show logging traffic filter-nat [**src-ip** *A.B.C.D* | **src-port** *port-num* | **dst-ip** *A.B.C.D* | **dst-port** *port-num* | **protocol** {**icmp** | **tcp** | **udp** | **others**} | **trans-src-ip** *A.B.C.D* | **trans-src-port** *port-num* | **trans-dst-ip** *A.B.C.D* | **trans-dst-port** *port-num* | **snat-rule-id** *rule-id* | **dnat-rule-id** *rule-id*]

［句法描述］

src-ip *A.B.C.D*	显示指定源 IP 地址的 NAT 日志信息。
src-port *port-num*	显示指定源端口号的 NAT 日志信息。
dst-ip *A.B.C.D*	显示指定目的 IP 地址的 NAT 日志信息。
dst-port *port-num*	显示指定目的端口号的 NAT 日志信息。
protocol {icmp | tcp | udp | others}	显示指定协议的 NAT 日志信息。 • **icmp** – 显示所有 ICMP 协议的 NAT 日志信息；

	• **tcp** – 显示所有 TCP 协议的 NAT 日志信息； • **udp** – 显示所有 UDP 协议的 NAT 日志信息； • **others** – 显示除 ICMP、TCP 和 UDP 协议外的其他协议的 NAT 日志信息。
trans-src-ip *A.B.C.D*	显示经过 NAT 转换后的指定源 IP 地址的 NAT 日志信息。
trans-src-port *port-num*	显示经过 NAT 转换后的指定源端口号的 NAT 日志信息。
trans-dst-ip *A.B.C.D*	显示经过 NAT 转换后的指定目的 IP 地址的 NAT 日志信息。
trans-dst-port *port-num*	显示经过 NAT 转换后的指定目的端口号的 NAT 日志信息。
snat-rule-id *rule-id*	显示指定源 NAT 规则 ID 的 NAT 日志信息。
dnat-rule-id *rule-id*	显示指定目的 NAT 规则 ID 的 NAT 日志信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show logging traffic filter-nat dst-ip 202.102.228.68**

show mac

显示所有 VSwitch 中的或者某个指定接口的 MAC 表项。

［命令］

show mac [**generic**] [**interface** *interface-name*]

［句法描述］

generic	显示 MAC 表的统计信息，包括共有多少 MAC 表项以及多少 MAC 表项正在使用中。
interface-name	特定的接口名称。

［默认取值］

如果不指定接口名称，该命令将会显示系统中所有 VSwitch 的 MAC 表项。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname# show mac
=========================================================
MAC Address      VSWITCH  IF               TYPE  AGE(sec)
---------------------------------------------------------
001c.5400.0c81   5        ethernet0/1      L     -
001c.5400.0c80   4        ethernet0/0      L     -
=========================================================
Total 2 MAC entries showed.
```

show mac-black-list

显示阻止了哪些 MAC 的流量。

［命令］

show mac-black-list

［句法描述］

无。

［默认取值］

无。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname# show mac-black-list
```

show mail-object

查看指定邮件控制内容信息。

［命令］

show mail-object [**mail-profile** *profile-name*]

［句法描述］

mail-profile *profile-name*	显示指定邮件过滤 Profile 中的指定邮件控制内容信息。若不指定，显示系统中所有指定邮件控制内容信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show mail-object**

show mail-profile

查看邮件过滤 Profile 信息。

［命令］

show mail-profile [*profile-name*]

［句法描述］

profile-name	显示指定邮件过滤 Profile 的信息。若不指定 Profile 名称，显示系统中所有邮件过滤 Profile 的信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show mail-profile mail1**

show memory

显示安全网关内存使用状况。

［命令］

show memory

［句法描述］

无。

［默认取值］

无。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show memory**

---

show mfib

查看组播 FIB 信息。

［命令］

show mfib [*A.B.C.D A.B.C.D*|**summary**] [**vrouter** *vrouter-name*]

［句法描述］

A.B.C.D A.B.C.D	通过指定组播源地址和组播地址，显示其组播 FIB 信息。第一个 A.B.C.D 为组播源地址，第二个 A.B.C.D 为组播地址。
summary	显示组播 FIB 的摘要信息。
vrouter *vrouter-name*	显示指定 VRouter 下的组播 FIB 信息。

［默认取值］

无。

［命令模式］

任何模式。

［使用指导］

如果不指定参数，则显示所有组播 FIB 信息。

［命令实例］

hostname# **show mfib summary**

show mirror

查看接口的镜像功能配置信息。

［命令］

show mirror

［句法描述］

无。

［默认取值］

无。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show mirror**

show module

显示扩展卡的状态信息、名称和序列号等。

［命令］

show module [*slot-number*]

［句法描述］

slot-number	指定该扩展卡插入的插槽名称。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

仅适用于 Hillstone 模块化安全网关。

［命令实例］

```
hostname# show module slot 1
```

show monitor

显示系统监控报警配置。

［命令］

show monitor

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname# show monitor
```

show nbt-cache

显示 NetBIOS 缓存数据，包括 IP 地址、主机名称、MAC 地址以及 VR 信息。

［命令］

show nbt-cache [*ip-address*][**vrouter** *vrouter-name*]

［句法描述］

ip-address	指定 IP 地址。配置该参数，系统将显示与指定 IP 地址相关的 NetBIOS 缓存数据。如果不配置该参数，系统将显示所有 NetBIOS 缓存数据。
vrouter *vrouter-name*	显示属于指定 VR 的 NetBIOS 缓存数据。如果没有指定 VR，系统将显示所有 VR 下的 NetBIOS 缓存数据。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname# show nbt-cache 58.62.3.1
```

show network-manager

查看设备上 HSM 代理的配置信息。

［命令］

show network-manager

［句法描述］

无。

［默认取值］

无。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# show network-manager
```

show ntp status

显示当前的 NTP 配置信息和 NTP 状态。

［命令］

show ntp status

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname# show ntp status
ntp client is disable, authentication is disable
ntp query-interval is 1, max adjust time is 10
```

show online

显示终端用户信息。

［命令］

show online

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname# show online
=========================================================
USER           VIA      IDLE   TIME         HOST
hillstone      telnet   .      Jan  8 18:11 10.200.3.109
hillstone      console  00:10  Jan  8 18:13 localhost
---------------------------------------------------------
```

show password-policy

显示管理员密码策略的具体信息。

［命令］

show password-policy

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show password-policy**

---

show pbr-policy

显示 PBR 策略的具体信息。

［命令］

show pbr-policy [*name*]

［句法描述］

name	显示指定名称的 PBR 策略的具体信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

当不指定 PBR 策略名称时，则显示所有 PBR 策略的具体信息。

［命令实例］

hostname# **show pbr-policy abc**

show pki

显示 PKI 配置的具体信息。

［命令］

show pki {**key** [**label** *key-name*] | **trust-domain** [*trust-domain-name*]}

［句法描述］

key	显示 PKI 密钥的配置信息。
label *key-name*	显示指定名称的密钥对配置信息。如果不指定该参数值，则显示系统中所以密钥对的配置信息。
trust-domain	指定显示 PKI 信任域的配置信息。
trust_domain_name	显示指定的 PKI 信任域的配置信息。如果不指定该参数，则显示系统中所有 PKI 信任域的配置信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show pki trust-domain trust_domain_default**

show policy

显示策略规则的具体信息。

［命令］

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

［句法描述］

id *id*	显示指定 ID 规则的详细信息。
from *src-zone*	显示源安全域为指定域的规则的详细信息。
to *dst-zone*	显示目标安全域为指定域的规则的详细信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname# show policy
Total rules count: 2.
Policies for trust => untrust:
============================================================
Id   Src          Dst         Service         Action
------------------------------------------------------------
 1   Any          Any         FTP             PERMIT
 3   Any          addr1       HTTP            DENY
============================================================
```

show policy hit-count

显示策略规则匹配次数统计信息。

［命令］

show policy hit-count {id *id* **| [from** *src-zone*] **[to** *dst-zone*] **top {10 | 20 | 50}}**

［句法描述］

id *id*	显示指定 ID 规则的匹配次数统计信息。
from *src-zone*	显示源安全域为指定域的规则的匹配次数统计信息。
to *dst-zone*	显示目标安全域为指定域的规则的匹配次数统计信息。
top {10 | 20 | 50}	显示匹配次数位于前 10、20 或者 50 位的规则的匹配次数统计信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname# show policy hit-count id 1
Policy id 1 is hit 342424 times
```

show pppoe-client

查看 PPPoE 实例的参数信息以及连接状态。

［命令］

show pppoe-client {all | group *group-name*}

［句法描述］

all	显示所有 PPPoE 实例的信息。
group *group-name*	显示指定 PPPoE 实例的信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname# show pppoe-client all
```

show predefine-servgroup

显示预定义服务组信息。

［命令］

show predefine-servgroup

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show predefine-servgroup**

---

show process

显示系统进程的信息。

［命令］

show process *process-name*

［句法描述］

process-name	显示指定进程的详细信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show process cli**

---

show qos interface

查看接口的 QoS 配置情况以及 QoS 统计信息。

［命令］

show qos interface *interface-name* **[1st-level-input | 1st-level-output | 2nd-level-input | 2nd-level-output] [detail]**

［句法描述］

interface-name	指定接口名称。
1st-level-input	指定仅查看接口第一层入方向的 QoS 统计信息。
1st-level-output	指定仅查看接口第一层出方向的 QoS 统计信息。

2nd-level-input	指定仅查看接口第二层入方向的 QoS 统计信息。
2nd-level-output	指定仅查看接口第二层出方向的 QoS 统计信息。
detail	指定除显示相应的统计信息外，还需要显示相应的 QoS 配置信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show qos interface ethernet0/2 1st-level-input detail**

show qos-profile

查看 QoS Profile 的配置信息。

［命令］

show qos-profile [*qos-profile-name*]

［句法描述］

qos-profile-name	显示指定名称的 QoS Profile 的信息。

［默认取值］

无默认值。

［命令模式］

如果不指定 *qos-profile-name*，则显示系统中所有 QoS Profile 的信息。

［使用指导］

无。

［命令实例］

hostname# **show qos-profile**

show reference

显示地址条目/服务/服务组被系统其它功能模块引用的情况，即地址条目/服务/服务组的关联项。

［命令］

show reference [**address** | **service**] *name*

［句法描述］

address *name*	显示指定地址条目的关联项。
service *name*	显示指定服务/服务组的关联项。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname# show address address1
=================================================
Name:           | address1
-------------------------------------------------
Address:        | -
-------------------------------------------------
Policy rule:    | policy 20 src-addr
-------------------------------------------------
SNAT rule:      | -
-------------------------------------------------
DNAT rule:      | -
-------------------------------------------------
Statistics:     | -
-------------------------------------------------
Session limit: | rule 1
-------------------------------------------------
Policy route:   | -
```

```
-----------------------------------------------------
QoS:            | -
=====================================================
```

show role

显示角色信息。

［命令］

show role

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# show role
=========================================================
Name                ID   Description
---------------------------------------------------------
role1               001
role2               002
role3               003
=========================================================
```

show role-expression

显示角色组合信息。

［命令］

show role-expression

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# show role-expression
==========================================================
 role1 and role2 role role3
==========================================================
```

show role-mapping-rule

显示角色映射信息。

［命令］

show role-mapping-rule [*rule-name*]

［句法描述］

rule-name	显示指定名称的映射规则信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# show role-mapping-rule
==========================================================
Name                        Description
----------------------------------------------------------
rule1                       Configured role-mapping-rule
==========================================================
hostname(config)# show role-mapping-rule rule1
==========================================================
Name rule1
----------------------------------------------------------
```

```
Match user user1 Role role1
==========================================================
```

show schedule

显示时间表信息。

［命令］

show schedule [**name** *schedule-name*]

［句法描述］

name *schedule-name*	显示指定时间表的详细信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

如果不指定时间表，则显示系统中所有时间表的信息。

［命令实例］

hostname# **show schedule name schedule1**

show scvpn client

显示当前在线的客户端信息。

［命令］

show scvpn client *scvpn-instance-name* [**user** *user-name*]

［句法描述］

scvpn-instance-name	显示指定 SCVPN 实例的信息。
user-name	显示指定用户的会话信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# show scvpn client scvpntunnel1
```

show scvpn pool

显示 SCVPN 地址池具体信息。

［命令］

show scvpn pool [*pool-name*]

［句法描述］

pool-name	指定 SCVPN 地址池名称以显示指定的地址池具体信息。如果不指定该参数值，系统将显示所有已配置的 SCVPN 地址池具体信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname# show scvpn pool
```

show scvpn pool （statistics）

显示 SCVPN 地址池统计信息。

［命令］

show scvpn pool *pool-name* **statistics**

［句法描述］

pool-name	指定 SCVPN 地址池名称以显示指定的地址池统计信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname# show scvpn pool pool1 statistics
```

show scvpn session

显示通过浏览器访问 SCVPN 的 HTTP 会话信息。

［命令］

show scvpn session *scvpn-instance-name* [**user** *user-name*]

［句法描述］

scvpn-instance-name	显示指定 SCVPN 实例的信息。
user-name	显示指定用户的会话信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# show scvpn session scvpntunnel1
```

show scvpn user-host-binding

显示 SCVPN 实例的绑定表。

［命令］

show scvpn user-host-binding *scvpn-instance-name* {**host** [*host-id*] | **user** [*user-name*]}

［句法描述］

instance-name	指定 SCVPN 实例的名称。
host-id	指定主机 ID。不指定主机 ID 时将显示所有主机 ID 的绑定表项信息。

user-name	指定用户名称。如果不指定用户名将显示所有用户的绑定表项信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show scvpn user-host-binding ssl2 user**

show servgroup

显示所有服务组或者某个指定服务组的信息。

［命令］

show servgroup [*servicegroup-name*]

［句法描述］

servicegroup-name	服务组的名称。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

如果不指定服务组，则显示系统中所有服务组的信息。

［命令实例］

hostname# **show servgroup group1**

show service

显示预定义服务、自定义服务、某特定服务或者所有服务的信息。

［命令］

show service {**predefined** | **userdefined** | **all** | **name** *service-name*}

［句法描述］

predefined	显示所有预定义服务的信息。
userdefined	显示所有自定义服务的信息。
all	显示所有服务的信息。
name *service-name*	显示某个指定服务的信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show service predefined**

show session

显示会话信息。

［命令］

show session [**generic** | **h323**]

show session [**id** *number* [*end-id*]] [**src-ip** *A.B.C.D* [*netmask*|*wildcard*]] [**dst-ip** *A.B.C.D* [*netmask*|*wildcard*]] [**protocol** *protocol-number*][**src-port** *port-number* [*port-number*]] [**dst-port** *port-number* [*port-number*]]

［句法描述］

generic	显示会话概要信息。
h323	显示 H323 会话信息。
id *number* [*end-id*]	显示指定 ID 或一段 ID 的会话信息。
src-ip *A.B.C.D*	显示指定源 IP 地址或地址段的会话信息。
dst-ip *A.B.C.D*	显示指定目的 IP 地址或地址段的会话信息。
netmask|*wildcard*	指定子网掩码或者通配符掩码。
protocol-number	显示指定协议号的会话信息。
src-port *port-number* [*port-number*]	显示指定源端口的会话信息。
dst-port *port-number* [*port-number*]	显示指定目的端口的会话信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show session protocol 6**

---

show session deny

查看系统中存在的 Deny Session 的具体信息。

［命令］

show session deny

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show session deny**

---

show session-limit

显示对域的 IP 地址会话数限制的信息。

［命令］

show session-limit

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname# show session-limit
```

show sms modem

显示短信猫的配置信息，包括存在状态和短信最大发送数量。

［命令］

show sms modem

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname# show sms modem
Modem state:    Non-exist
Number per Day:  Unlimit
Number per Hour: 100
```

show smtp

显示 SMTP 信息。

［命令］

show smtp

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show smtp**

---

show snat

显示 SNAT 配置信息。

［命令］

show snat [*id*] [*resource*]

［句法描述］

id	显示指定 ID 号的 SNAT 规则。
resource	当 SNAT 的转换模式为 dynamicport 时，该参数用来指定显示源端口地址池中资源的利用情况。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname# show snat
id from   to    egress interface translate to   mode
1  addr1  addr2                  addr3          Dyn-Pt
```

show snmp-group

显示安全网关的 SNMPv3 用户组信息。

［命令］

show snmp-group

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show snmp-group**

show snmp-user

显示安全网关的 SNMPv3 用户信息。

［命令］

show snmp-user

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show snmp-user**

---

show snmp-server

显示 SNMP 配置信息。

［命令］

show snmp-server

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show snmp-server**

---

show ssh

显示 SSH 配置信息。

［命令］

show ssh

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# show ssh
Ssh server options:
============================================================
ssh idle timeout is: 10 minute(s)
ssh server listen port is: 22
ssh server accept connection interval: 2
============================================================
```

show sslproxy exempt-match-subject

查看“审计所有网站，但排除下表指定网站”审计方式下列表证书的相关信息。

［命令］

show sslproxy exempt-match-subject

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show sslproxy exempt-match-subject**

show sslproxy-profile

查看 SSL Profile 信息。

［命令］

show sslproxy-profile [*profile-name*]

［句法描述］

profile-name	显示指定名称的 SSL Profile 信息。如不指定该参数，显示所有 SSL Profile 信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show sslproxy-profile ssl1**

show sslproxy require-match-subject

查看“只审计下表指定网站”审计方式下列表证书的相关信息。

［命令］

show sslproxy require-match-subject

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show sslproxy require-match-subject**

show sslproxy state

显示 SSL 代理信息，包括 SSL 证书审计方式和 SSL 代理证书的 PKI 信任域信息。

［命令］

show sslproxy state

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show sslproxy state**

---

show sslproxy trustca

显示可信 SSL 证书信息。

［命令］

show sslproxy trustca [*file-name*]

［句法描述］

file-name	显示指定名称的可信 SSL 证书信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show sslproxy trustca**

---

show statistics app-session

显示某种应用的当前或者历史统计信息，并且输出指定应用的原始统计数据。

［命令］

show statistics app-session *app-type* {**raw-data** | **summary**}

［句法描述］

app-type	指定应用的类型。
raw-data	指定输出特定应用统计信息的原始数据。
summary	指定输出特定应用的当前统计信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show statistics app-session icmp raw-data**

show statistics app-session summary

查看所有应用的统计信息。

［命令］

show statistics app-session summary {number | ramp-rate | packets-count | bytes-count}

［句法描述］

number	指定输出所有应用的当前连接数统计信息。
ramp-rate	指定输出所有应用的当前连接速率统计信息。
packets-count	指定输出所有应用的当前包数的统计信息。
bytes-count	指定输出所有应用的当前字节数的统计信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show statistics app-session summary number**

show statistics interface-counter interface

查看基于接口的统计信息。

［命令］

show statistics interface-counter interface *interface-name* {**second** | **minute** | **hour**}

［句法描述］

interface-name	指定接口名称。
second	指定显示接口前 60 秒钟每秒的流量统计信息。
minute	指定显示接口前 60 分钟每分钟的流量统计信息。
hour	指定显示接口前 24 小时每小时的流量统计信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show statistics interface-counter interface ethernet0/2 second**

show statistics ip-counter zone

查看某个安全域 IP 地址会话数的统计信息。

［命令］

show statistic ip-counter zone *zone-name* [{**from** | **to**} {**name** *address-entry* [**interface** *interface-name*] | **top10** | **top50** | **top100**}]

［句法描述］

zone-name	指定安全域的名称。
from | **to**	指定显示源 IP 地址的统计信息（**from**）或者目的 IP 地址的统计

	信息（**to**）。
address-entry	地址簿中定义的地址，来指定被统计 IP 地址范围。
interface-name	指定被统计 IP 地址的接口名称。
top10	指定显示流量最大的前 10 个 IP 地址的统计信息。
top50	指定显示流量最大的前 50 个 IP 地址的统计信息。
top100	指定显示流量最大的前 100 个 IP 地址的统计信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show statistics ip-counter zone trust**

show statistics session-counter zone

查看某个安全域 IP 地址会话数的统计信息。

［命令］

show statistic session-counter zone *zone-name* [{**from** | **to**} {**name** *address-entry* [**interface** *interface-name*] | top10 | top50 | top100}]

［句法描述］

zone-name	指定包进入的安全域的名称。
from | **to**	指定显示源 IP 地址的统计信息（**from**）或者目的 IP 地址的统计信息（**to**）。
address-entry	地址簿中定义的地址，来指定被统计 IP 地址范围。
interface-name	指定被统计 IP 地址的接口名称。
top10	指定显示连接数最多的前 10 个 IP 地址的统计信息。
top50	指定显示连接数最多的前 50 个 IP 地址的统计信息。
top100	指定显示连接数最多的前 100 个 IP 地址的统计信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show statistics session-counter zone trust**

show statistics-set

查看系统预定义和用户自定义统计集的配置信息。

［命令］

show statistics-set *name* [{**current** | **history**} [**sort-by** {**up** | **down** | **item**}]]

［句法描述］

show statistics-set	显示系统中所有统计集的配置信息。
name	指定统计集名称，显示特定统计集的配置信息。
current | **history**	显示特定统计集的当前（**current**）数据统计信息或历史（**history**）数据统计记录。
sort-by {**up** | **down** | **item**}	指定特定统计集统计数据的排列顺序（从大到小排列） • **up** - 按上行数据进行排序。 • **down** – 当配置 group-by 时指定了 directional 参数，使用该参数按下行数据进行排序。 • **item** - 按照 group-by 的对象进行排序。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show statistics-set set1**

show stp

查看 RSTP 配置信息。

［命令］

show stp [**port** *interface-name*]

[句法描述]

interface-name	指定以太网接口或者集聚接口的名称。

[默认取值]

无。

[命令模式]

任何模式。

[使用指导]

无。

[命令实例]

hostname(config)# **show stp port ethernet0/2**

show supervlan

显示 super-VLAN 配置信息。

[命令]

show supervlan[*X*]

[句法描述]

X	显示指定编号的 super-VLAN 配置信息。如不指定该参数显示所有 super-VLAN 配置信息。

[默认取值]

无默认值。

[命令模式]

任何模式。

[使用指导]

无。

[命令实例]

hostname# **show show supervlan1**

show tcp-mss

显示 TCP 包的 MSS 设置信息。

［命令］

show tcp-mss

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show tcp-mss**

---

show tech-support

显示技术支持信息。

［命令］

show tech-support

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show tech-support**

---

show telnet

显示 Telnet 配置信息。

［命令］

show telnet

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname# show telnet
Telnet server paramters:
============================================================
telnet idle timeout is: 60 minute(s)
telnet server port is: 23
telnet authorization-try-count is: 3
============================================================
```

show terminal

显示终端配置参数信息。

［命令］

show terminal

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show terminal**

show track

显示 Track 对象的信息。

［命令］

show track *object-name*

［句法描述］

object-name	显示指定 Track 对象的信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show track trackobj1**

show tunnel gre

显示 GRE 隧道配置信息。

［命令］

show tunnel gre [*gre-tunnel-name*]

［句法描述］

gre-tunnel-name	显示指定名称的 GRE 隧道配置信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show tunnel gre**

show tunnel ipsec auto

显示 IKE 隧道的配置信息。

［命令］

show tunnel ipsec auto [*tunnel-name*]

show tunnel ipsec auto {*tunnel-name*}

［句法描述］

tunnel-name	显示指定名称的 IKE 隧道的配置信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

如果不指定 IKE 隧道，则显示所有 IKE 隧道的配置信息。

查看 VPN 监控功能的配置信息时，必须指定 IKE 隧道。

［命令实例］

hostname# **show tunnel ipsec auto tunnel1**

show tunnel ipsec manual

显示手工 IPSec 隧道的配置信息。

［命令］

show tunnel ipsec manual [*tunnel-name*]

show tunnel ipsec manual {*tunnel-name*}

［句法描述］

tunnel-name	显示指定名称的 IPSec 隧道的配置信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

如果不指定 IPSec 隧道，则显示所有手工 IPSec 隧道的配置信息。

查看 VPN 监控功能的配置信息时，必须指定 IKE 隧道。

［命令实例］

hostname# **show tunnel ipsec manual tunnel1**

---

show tunnel l2tp

查看 L2TP 实例信息。

［命令］

show tunnel l2tp [*l2tp-tunnel-name*]

［句法描述］

l2tp-tunnel-name	指定 L2TP 实例的名称。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show tunnel l2tp l2tptunnel2**

---

show tunnel scvpn

显示 SCVPN 实例信息。

［命令］

show tunnel scvpn [*scvpn-instance-name*]

［句法描述］

scvpn-instance-name	显示指定 SCVPN 实例的信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# show tunnel scvpn
============================================================
Name     Port  Protocol  Interface  Pool     Trust-Domain
------------------------------------------------------------
scvpntunnel14433  any             pool1 trust_domain_def
============================================================
```

show url

显示 URL 信息。

［命令］

show url [*url-string*]

［句法描述］

url-string	显示指定 URL（包括自定义 URL 和预定义 URL）的信息。若不指定该参数，则显示所有自定义 URL 信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname# show url
```

show url-category

显示 URL 类别。

［命令］

show url-category

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show url-category**

---

show url-db info

显示 URL 数据库信息。

［命令］

show url-db info

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show url-db info**

show url-db update

显示 URL 数据库更新配置信息。

［命令］

show url-db update

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show url-db update**

show url-db query

显示 URL 查询服务器信息。

［命令］

show url-db-query [server1 | server2]

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname# show url-db url-db-query server1
```

show url-profile

查看 URL 过滤 Profile 信息。

［命令］

show url-profile [*profile-name*]

［句法描述］

profile-name	显示指定名称的 URL 过滤 Profile 信息。如不指定该参数，显示所有 URL 过滤 Profile 信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname# show url-profile url1
```

show user

显示系统中已配置的用户信息。

［命令］

show user [**name** *user-name* | **aaa-server** *server-name*]

［句法描述］

user-name	显示指定名称的用户信息。
server-name	显示指定 AAA 服务器的用户信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname# show user
=============================================================
Username                        Password
-------------------------------------------------------------
user1                           U8FdHNEEBz6sNn5Mvqx3yWuLRWce
=============================================================
hostname(config)# show user name user1
=========================================================
username: user1
password: U8FdHNEEBz6sNn5Mvqx3yWuLRWce
IKE type: FQDN
IKE ID:   aaa
groups:   number:   1
          group1
=========================================================
```

show user-binding

显示静态绑定用户的信息。

［命令］

show user-binding aaa-server *server-name*

［句法描述］

server-name	显示指定 AAA 服务器的用户信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname# show user-binding aaa-server local
```

show version

显示固件版本信息。

［命令］

show version

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show version**

show virtual-wire

查看 Virtual Wire 接口对的配置信息。

［命令］

show virtual-wire [**vswitch** *vswitch-name*]

［句法描述］

vswitch-name	显示指定 VSwitch 的 Virtual Wrie 接口对信息。如果不指定该参数，则显示系统中所有已配置的 Virtual Wire 接口对。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname(config)# show virtual-wire vswitch vswitch1
=====================================================================
aggregate1                        ethernet0/2.1
=====================================================================
```

```
Total 1 entries
```

show vlan

显示所有 VLAN 或指定 VLAN 的信息。

［命令］

show vlan [*vlanid*]

［句法描述］

vlanid	显示指定 VLAN 的信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show vlan 1**

show vlan port

显示指定接口的类型以及所属 VLAN 信息。

［命令］

show vlan port *interface-name*

［句法描述］

interface-name	显示指定接口的信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show vlan port ethernet0/2**

show vswitch

显示所有虚拟交换机中包含的接口信息。

［命令］

show vswitch [*vswitch-name*]

［句法描述］

vswitch-name	显示指定 VSwitch 的信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show vswitch**

show vsys

查看系统中 VSYS 信息。

［命令］

show vsys [*vsys-name*]

［句法描述］

vsys-name	指定需要查看的 VSYS 的名称。

［默认取值］

无默认值。

［命令模式］

根 VSYS 的任意模式。

［使用指导］

无。

［命令实例］

hostname# **show vsys**

show vsys-profile

查看系统中 VSYS Profile 信息。

［命令］

show vsys-profile [*vsys-profile-name*]

［句法描述］

vsys-profile-name	指定需要查看的 VSYS Profile 的名称。

［默认取值］

无。

［命令模式］

根 VSYS 的任意模式。

［使用指导］

无。

［命令实例］

hostname# **show vsys-profile profile1**

show webpost-profile

查看 Web 外发信息 Profile 信息。

［命令］

show webpost-profile [*profile-name*]

［句法描述］

profile-name	显示指定 Web 外发信息 Profile 的信息。若不指定 Profile 名称，显示系统中所有 Web 外发信息 Profile 的信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show webpost-profile ssl1**

show web-redirect-user

查看网页重定向用户的详细信息。

［命令］

show web-redirect-user

［句法描述］

无。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show web-redirect-user**

show zone

查看系统中的域信息。

［命令］

show zone [*zone-name*]

［句法描述］

zone-name	指定域的名称显示指定域的信息。

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

```
hostname# show zone
```

Hillstone®
山 石 网 科

www.hillstonenet.com

北京总部
地 址: 北京市海淀区上地七街1号汇众大厦3层
邮 编: 100085
电 话: +86(10) 8289 7229
传 真: +86(10) 8289 9814

销售与服务热线: 400-650-0259

文档编号: SG-CLI0811-4.5R3C-01