Hillstone Networks

StoneOS 命令行用户手册

威胁防护 分册

Version 5.5R7

TechDocs | docs.hillstonenet.com

Hillstone Networks

联系信息

公司总部（北京总部）：

地址：北京市海淀区宝盛南路1号院20号楼5层

邮编： 100192

联系我们：http://www.hillstonenet.com.cn/about/contact_Hillstone.html

关于本手册

本手册介绍Hillstone Networks 公司的产品系统的使用方法。

获得更多的文档资料，请访问：https://docs.hillstonenet.com.cn

针对本文档的反馈，请发送邮件到：hs-doc@hillstonenet.com

Hillstone Networks

https://www.hillstonenet.com.cn

TWNO: TW-CUG-UNI-TRT-5.5R7-CN-V1.0-2019/6/5

目 录

关于本手册

手册约定

为方便用户阅读与理解，本手册遵循以下约定：

内容约定

本手册内容约定如下：

- 提示：为用户提供相关参考信息。
- 说明：为用户提供有助于理解内容的说明信息。
- 注意：如果该操作不正确，会导致系统出错。
- 『 』：用该方式表示Hillstone设备WebUI界面上的链接、标签或者按钮。例如，“点击『登录』按钮进入Hillstone设备的主页”。
- < >：用该方式表示WebUI界面上提供的文本信息，包括单选按钮名称、复选框名称、文本框名称、选项名称以及文字描述。例如，“改变MTU值，选中<手动>单选按钮，然后在文本框中输入合适的值”。

CLI约定

本手册在描述CLI时，遵循以下约定：

- 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。

- 命令实例中，命令提示符中的主机名称均使用“hostname”。

命令行接口（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，包含了一个井号（#）：

```
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CLI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。下表列出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

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。常见的错误信息如下表所示：

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。

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 int`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`”后敲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。下表列出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-H	删除光标前一个字符。
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	删除光标前的词。
META-B	将光标移至所在词的词首。
META-D	删除光标后的词。
META-F	将光标移至所在词的词尾。
META-Backspace	删除光标前的词。
META-Ctrl-H	删除光标前的词。

提示: 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式规范。下表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（））、行首、行尾或者空格。
方括号（[]）	指定单个字符的范围。
连字符（-）	分隔范围的终点。

分页显示CLI输出信息

一些命令回显输出信息比较长，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，终端显示的行数为指定行数减1（但是如果配置行数为1，则显示1行）。范围是0到256行，0的含义为不分屏显示。

终端的设置只对当前连接有效，不会被记录到配置文件。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Console、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Console超时时间。范围是0到60分钟，0表示永不超时。默认值为10分钟。

  在全局配置模式使用**no console timeout**命令恢复Console超时时间的默认值。

- **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。

  在全局配置模式使用**no ssh timeout**命令恢复SSH超时时间的默认值。

- **telnet timeout** *timeout-value*

  timeout-value - 指定Telnet超时时间。范围是1到60分钟，默认是10分钟。

  在全局配置模式使用**no telnet timeout**命令恢复Telnet超时时间的默认值。

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：

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

诊断命令

StoneOS CLI支持`ping`和`traceroute`两个诊断命令。用户可以通过这两个命令查看网络和路由是否连通。

威胁防护

本章节包含以下内容：

- "主机防御" 在第11页：介绍了如何配置主机防御功能来保护被代理主机免受ARP攻击。
- "攻击防护" 在第24页: 介绍了常见的网络攻击、如何配置攻击防护功能以及攻击防护配置举例。
- "沙箱防护" 在第62页：介绍了沙箱防护功能、如何配置沙箱防护规则以及如何更新沙箱所使用的域名白名单。
- "入侵防御系统" 在第72页 ：介绍了如何检测并防护针对主流应用层协议（DNS、FTP、HTTP、POP3、SMTP、TELNET、MYSQL、MSSQL、ORACLE、NETBIOS等）的入侵攻击、基于Web的攻击行为以及常见的木马攻击。
- "异常行为检测" 在第141页 :介绍了如何配置基于安全域的异常行为检测功能从而判断检测对象的异常行为，以及如何更新异常行为模型库。
- "高级威胁检测" 在第145页 : 介绍了如何通过对基于主机的可疑流量进行智能分析，判断是否为恶意软件，以及如何更新恶意软件行为模型库。
- "边界流量过滤" 在第148页：介绍了如何通过对基于已知的IP地址黑白名单对流量进行过滤，并对命中黑名单的恶意流量采取阻断措施进行处理，以及如何更新IP信誉特征库。
- "风险减缓措施" 在第157页：介绍了如何配置风险减缓措施规则来动态识别网络中潜在的风险并作出相应的行为控制，以及如何更新风险减缓措施规则特征库。
- "关联分析" 在第161页：介绍了如何使用系统提供关联分析引擎，对威胁防护各个模块产生的威胁事件进行关联分析。
- "核心资产" 在第162页：介绍了如何配置核心资产对象。
- "威胁地理信息库" 在第165页：介绍了如何更新威胁地理信息库。
- "僵尸网络C&C防御" 在第169页：介绍了如何配置基于安全域和基于策略的僵尸网络C&C防御功能从而进行僵尸网络C&C检查。

- "垃圾邮件过滤" 在第177页：介绍了如何配置基于安全域和基于策略的垃圾邮件过滤功能从而及时发现、处理邮件携带的威胁。
- "终端防护" 在第181页：介绍了如何通过与终端安全控制中心进行联动交互，获取终端安全控制中心监测的终端数据信息，实现终端防护的目的。
- "IoT监控" 在第188页：通过分析流经设备的流量，识别视频监控专网中的IPC（网络摄像机）和NVR（网络硬盘录像机）等网络视频监控设备，并对识别出的设备进行实时监控，然后根据配置对出现非法行为的网络视频监控设备进行阻断等操作。

主机防御

设备的主机防御功能即设备代替不同主机发送免费ARP包，保护被代理主机免受ARP攻击。配置主机防御功能，在全局配置模式下，使用以下命令：

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

- **ip** *ip-address* – 指定被代理主机的IP地址。
- **mac** *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***rate-value* - 指定设备发送免费ARP包的速率。单位为个/每秒。默认值为1个。取值范围是1到10个。

配置多条该命令代理多台主机发送免费ARP包。设备最多可代理16台主机发送免费ARP包。

在全局配置模式下，使用以下命令取消代理指定主机发送免费ARP包功能：

no gratuitous-arp-send ip *ip-address* **switch-interface** *interface-name*

主机黑名单

通过使用设备的主机黑名单功能，设备可以控制用户在指定时间内不能访问网络。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。

如果将主机IP地址添加到黑名单的同时，又配置其为不受限IP并且开启了不受限IP功能，系统仍会阻断该主机上网。

添加黑名单条目

在全局配置模式下，输入以下命令将主机加入黑名单：

host-blacklist {**mac** *mac-address* | **ip from** *ip-address* **to** *ip-address* **vrouter** *vrouter-name*} [**schedule** *schedule-name*] [**enable** | **disable**]

- *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，系统将在时间表指定的时间范围内禁止主机访问网络；如果不指定该参数，系统将永久禁止主机访问网络。关于如何创建时间表，请参阅《系统管理》的“配置时间表功能”部分。
- **enable** | **disable** – 启用或禁用该主机黑名单条目。默认情况下，所有的主机黑名单条目都为启用状态。

例如，添加MAC地址为001c.f096.f1ea的主机到黑名单，并为其绑定已创建的时间表night，使该主机在“night”指定时间范围内不能上网，命令行如下：

```
hostname(config)# schedule night
hostname(config-schedule)# periodic daily 22:00 to 06:00
hostname(config-schedule)# exit
hostname(config)# host-blacklist mac 001c.f096.f1ea schedule night
```

修改时间表

在全局配置模式下，使用以下命令修改指定的主机黑名单条目的时间表：

host-blacklist {**mac** *mac-address* | **ip from** *ip-address* **to** *ip-address* **vrouter** *vrouter-name*} **schedule** *new-schedule-name*

- **schedule** *new-schedule-name* – 新的时间表名称。

例如，修改MAC地址为001c.f096.f1ea的主机黑名单条目的时间表，更改其已有的时间表schedule1为新的时间表schedule2。命令行如下：

```
hostname(config)# schedule schedule1
hostname(config-schedule)# periodic monday 9:00 to 18:00
hostname(config-schedule)# exit
hostname(config)# schedule schedule2
hostname(config-schedule)# absolute start 01/01/2009 9:00 end
05/01/2009 9:00
hostname(config-schedule)# exit
hostname(config)# host-blacklist mac 001c.f096.f1ea schedule sched-
ule1
hostname(config)# host-blacklist mac 001c.f096.f1ea schedule
schedule2
```

启用或禁用主机黑名单条目

已创建的主机黑名单条目可以通过MAC地址或者ID进行标识。在全局配置模式下，使用以下命令启用或者禁用指定的主机黑名单条目：

host-blacklist mac {*mac-address* | **id** *id-number* }{**enable** | **disable**}

已创建的主机黑名单条目可以通过IP地址或者ID进行标识。在全局配置模式下，使用以下命令启用或者禁用指定的主机黑名单条目：

host-blacklist ip {**from** *ip-address* **to** *ip-address* **vrouter** *vrouter-name* | **id** *id-number*} {**enable** | **disable**}

例如，禁用ID编号为1的MAC地址主机黑名单条目。命令行如下：

```
hostname(config)# host-blacklist mac id 1 disable
```

禁用该条目后，条目未被删除，仍存在黑名单中。如使其再次生效，输入以下命令启用ID编号为1的MAC地址主机黑名单条目：

```
hostname(config)# host-blacklist mac id 1 enable
```

查看主机黑名单内容

在任何模式下，输入以下命令显示主机黑名单内容：

- 显示所有MAC地址的主机黑名单条目：**show host-blacklist mac**
- 显示所有IP地址的主机黑名单条目：**show host-blacklist ip**

删除主机黑名单条目

在全局配置模式下，使用以下命令从黑名单中删除MAC地址的主机：

no host-blacklist mac {*mac-address* | **id** *id-number*| **all**}

- *mac-address* – 通过输入主机MAC地址，删除该主机黑名单条目。
- **id** *id-number* – 通过输入已创建的主机黑名单条目ID编号，删除该主机黑名单条目。
- **all** – 删除所有已创建的MAC地址的主机黑名单条目。

在全局配置模式下，使用以下命令从黑名单中删除IP地址的主机：

no host-blacklist ip {**from** *ip-address* **to** *ip-address* **vrouter** *vrouter-name* | **id** *id-number*| **vrouter** *vr-name*}

- **from** *ip-address* **to** *ip-address* **vrouter** *vr-name* – 在黑名单中删除指定VRouter下的IP地址范围对应的主机黑名单条目。
- **id** *id-number* - 通过输入已创建的主机黑名单ID编号，删除该主机黑名单条目。
- **vrouter** *vrouter-name* – 从黑名单中删除属于该VRouter的全部IP地址主机黑名单条目。

注意: 当用户使用**no ip vrouter** *vrouter-name* 命令删除VRouter时，会将IP黑名单中关联此VRouter的全部记录一同删除。

IP-MAC绑定

为加强网络安全控制，设备支持IP-MAC地址绑定、MAC-端口绑定以及IP-MAC-端口绑定。这些绑定信息分为静态和动态两种。通过ARP学习功能、ARP扫描功能以及MAC学习功能获得绑定信息为动态绑定信息；而手工配置的绑定信息为静态信息。同时，设备还具有ARP检查功能。

静态绑定

用户可以添加静态IP-MAC绑定条目和MAC-端口绑定条目；还可以限制IP-MAC地址动态学习到的主机不能上网，仅IP-MAC静态绑定的主机可以上网。

添加静态IP-MAC绑定条目

添加静态IP-MAC绑定条目，在全局模式下，使用以下命令：

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。

在全局配置模式下，使用以下命令删除静态IP-MAC绑定条目：

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-name* – 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。

添加静态MAC-端口绑定条目

添加静态MAC-端口绑定条目，在全局配置模式下，使用以下命令：

mac-address-static *mac-address* **interface** *interface-name*

- *mac-address* – 指定静态绑定的MAC地址。
- **interface** *interface-name* – 指定静态绑定的端口。

在全局配置模式下，使用以下命令删除MAC-端口绑定条目：

- 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 |
vid vlan-id}
```

仅允许IP-MAC静态绑定主机上网

默认情况下，系统允许ARP动态学习到的主机上网。如果仅允许IP-MAC静态绑定的主机上网，在接口配置模式下，输入以下命令：

```
arp-disable-dynamic-entry
```

使用该命令的no形式关闭该功能：

```
no arp-disable-dynamic-entry
```

动态IP-MAC-端口绑定

设备可以通过以下两种方式获得动态IP-MAC-端口绑定信息：

- ARP学习功能
- MAC学习功能

ARP学习功能

设备通过ARP学习过程获得内网中的IP-MAC的绑定信息，并将绑定信息添加到系统ARP表中。默认情况下，设备的ARP学习功能是开启的，设备会一直进行ARP学习，并将学到的IP-MAC绑定信息添加到系统ARP表中。在ARP学习过程中，如果IP或者MAC地址发生变化，设备会将更新的IP-MAC

绑定信息添加到系统ARP表中。关闭ARP学习功能，只有已经在系统ARP表中的IP地址可以访问Internet。

配置ARP学习功能，在VSwitch或者BGroup接口配置模式下，使用以下命令：

- 开启ARP学习功能：**arp-learning**
- 关闭ARP学习功能：**no arp-learning**

MAC学习功能

设备通过MAC学习过程获得内网中的MAC-端口绑定信息，并将其添加到系统MAC表中。默认情况下，设备的MAC学习功能是开启的，设备会一直进行MAC学习，并将学到的MAC-端口绑定信息添加到系统MAC表中。在MAC学习过程中，如果MAC地址或者端口发生变化，设备会将更新的MAC-端口绑定信息添加到MAC表中。

配置MAC学习功能，在VSwitch接口的接口配置模式下，使用以下命令：

- 开启MAC学习功能：**mac-learning**
- 关闭MAC学习功能：**no mac-learning**

显示IP-MAC-端口绑定信息

用户可以通过以下命令查看系统的IP-MAC绑定信息（静态与动态）和MAC-端口绑定信息（静态与动态）。

- IP-MAC绑定信息：**show arp** [**vrouter** *vrouter-name*]
- MAC-端口绑定信息：**show mac**

清除ARP绑定信息

用户可以通过以下命令清除系统中的ARP绑定信息（静态与动态）：

clear arp [**interface** *interface-name* [*A.B.C.D*] | **vrouter** *vrouter-name*]

- **interface** *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。

- *A.B.C.D* - 清除接口上指定IP地址的ARP绑定信息。

- **vrouter** *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。

强制绑定动态MAC-端口绑定信息

用户可以将系统通过MAC学习得到的动态MAC-端口绑定信息进行强制绑定。配置强制绑定功能，在任何模式下，使用以下命令：

exec mac-address dynamic-to-static

DHCP监控

DHCP为动态主机配置协议（Dynamic Host Configuration Protocol），它能够自动为子网分配适当的IP地址以及其它网络参数。DHCP监控通过分析DHCP客户端与DHCP服务器之间的DHCP报文建立DHCP客户端的MAC地址和被分配的IP地址的对应关系。在启动ARP检查功能后，将检查经过设备的ARP包是否与该表的内容匹配，如果不匹配则丢弃该ARP包。在用DHCP获取地址的网络中，可以通过启用ARP检查和DHCP监控功能来防止ARP欺骗。

由于DHCP服务的客户端是以广播的方式寻找服务器，并且只接收第一个到达的服务器提供的网络配置参数，因此，如果网络中存在非授权的DHCP服务器，就有可能引发DHCP服务器欺骗。设备可以通过在相应端口上设置丢弃DHCP响应报文来防止DHCP服务器欺骗。

另外，一些恶意攻击者通过伪造不同的MAC地址不断地向DHCP服务器发送DHCP请求，从而耗尽服务器的IP地址资源，最终导致合法用户不能获得IP地址。这种攻击也即网络上常见的DHCP Starvation Attack。设备可以通过在相应端口上设置丢弃请求报文、设置DHCP包速率限制或者打开合法性检查功能来防止该类攻击。

开启/关闭DHCP监控功能

系统的BGroup接口、VSwitch接口以及VLAN均支持DHCP监控功能。默认情况下，该功能是关闭的。开启BGroup或者VSwitch接口的DHCP监控功能，在BGroup或者VSwitch接口的接口配置模式下，使用以下命令：

dhcp-snooping

在BGroup或者VSwitch接口的接口配置模式下，使用该命令no的形式关闭接口的DHCP监控功能：

no dhcp-snooping

开启VLAN的DHCP监控功能，在全局配置模式下，使用以下命令：

dhcp-snooping vlan *vlan-list*

- *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。系统为BGroup保留32个VLAN编号（从VLAN224到VLAN255）。

在全局配置模式下，使用该命令no的形式关闭VLAN的DHCP监控功能：

no dhcp-snooping vlan *vlan-list*

配置DHCP检查功能

用户可以配置设备的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。默认情况下，所有的DHCP请求和响应报文都是允许的，并且无有效性检查。配置DHCP检查功能，在以太网接口（BGroup、VSwitch或者VLAN接口中的物理接口）配置模式下，使用以下命令：

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

- **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。

在接口配置模式下，使用该命令no的形式关闭DHCP检查功能：

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

配置DHCP包速率限制

配置接收DHCP包的速率限制，在以太网接口（BGroup、VSwitch或者VLAN接口中的物理接口）配置模式下，使用以下命令：

dhcp-snooping rate-limit *number*

- *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。默认值是0，即无速率限制。

在接口配置模式下，使用该命令no的形式取消速率限制的配置：

no dhcp-snooping rate-limit

显示DHCP监控配置信息

用户可以在任何模式下通过以下命令查看DHCP监控功能的配置信息：

show dhcp-snooping configuration

DHCP监控列表

启用DHCP监控功能后，系统会对通过接口的所有DHCP包进行检查，并在此过程中建立并维护一个包含IP-MAC绑定信息的DHCP监控列表。另外，当系统的BGroup接口、VSwitch接口、VLAN接口以及其它三层物理接口配置为DHCP服务器时，不用开启DHCP监控功能，系统也会自动建立IP-MAC绑定信息并将它们添加到DHCP监控列表中。列表中的绑定条目包含合法用户的MAC 地址、所获IP地址、设备接口、VLAN编号、租约期限等信息。用户可以在任何模式下通过以下命令查看DHCP监控列表信息：

show dhcp-snooping binding

在任何模式下，用户可以使用以下命令删除所有的或者指定的DHCP监控列表条目：

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

- **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。

ARP检查功能

设备支持接口的ARP检查功能。开启该功能后，系统会对通过接口的所有ARP包进行检查，将ARP包的IP地址与系统ARP表中的静态表项以及DHCP监控列表中的IP-MAC绑定表项进行对比：

- 如果IP地址在ARP表中，并且与表中记录的MAC地址相同，则继续转发该ARP包；
- 如果IP地址在ARP表中，但是与表中记录的MAC地址不一致，系统将丢弃该ARP包；
- 如果IP地址不在ARP表中，则继续检查该IP地址是否在DHCP监控列表中；
- 如果IP地址在DHCP监控列表中，并且与表中记录的MAC地址相同，则继续转发该ARP包；
- 如果IP地址在DHCP监控列表中，但是与表中记录的MAC地址不一致，系统将丢弃该ARP包；
- 如果IP地址不在DHCP监控列表中，则根据配置进行丢弃或者转发。

开启/关闭ARP检查功能

系统的BGroup接口、VSwitch接口以及VLAN均支持ARP检查功能。默认情况下，该功能是关闭的。开启BGroup或者VSwitch接口的ARP检查功能，在BGroup或者VSwitch接口的接口配置模式下，使用以下命令：

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

- **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。

在BGroup或者VSwitch接口的接口配置模式下，使用该命令no的形式关闭接口的ARP检查功能：

no arp-inspection

开启VLAN的ARP检查功能，在全局配置模式下，使用以下命令：

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

- *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。系统为BGroup保留32个VLAN编号（从VLAN224到VLAN255）。

在全局配置模式下，使用该命令no的形式关闭VLAN的ARP检查功能：

```
no arp-inspection vlan vlan-list
```

配置可信接口

用户可以设置设备的接口(BGroup、VSwitch或者VLAN接口中的物理接口)为可信接口，通过可信接口的数据包将不会受到ARP检查。默认情况下，设备所有的接口都是不可信的。配置设备的某个接口为可信接口，在接口配置模式下，使用以下命令：

```
arp-inspection trust
```

在接口配置模式下，使用该命令no的形式取消可信接口的配置：

```
no arp-inspection trust
```

配置ARP包速率限制

配置接收ARP包的速率限制，在接口配置模式下，使用以下命令：

```
arp-inspection rate-limit number
```

- *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。默认值是0，即无速率限制。

在接口配置模式下，使用该命令no的形式取消速率限制的配置：

```
no arp-inspection rate-limit
```

注意: 只能在绑定到二层域的物理接口上配置ARP包速率检查。

ARP防御

通过使用ARP学习、MAC学习、ARP认证以及ARP检查功能，系统能够很好的防御ARP欺骗攻击。并且，系统能够对ARP欺骗攻击进行统计。显示ARP欺骗攻击统计信息，任何模式下，使用以下命令：

```
show arp-spoofing-statistics [number]
```

- *number* – 显示统计数最高的前*number*条记录。

清除系统中的ARP欺骗攻击统计信息，在执行模式下，使用以下命令：

```
clear arp-spoofing-statistics
```

攻击防护

网络中存在多种防不胜防的攻击，如侵入或破坏网络上的服务器、盗取服务器的敏感数据、破坏服务器对外提供的服务，或者直接破坏网络设备导致网络服务异常甚至中断。作为网络安全设备的设备，必须具备攻击防护功能来检测各种类型的网络攻击，从而采取相应的措施保护内部网络免受恶意攻击，以保证内部网络及系统正常运行。设备提供基于域的攻击防护功能。

常见网络攻击概述

本节介绍一些常见的网络攻击。设备能够对这些网络攻击进行合理处理从而保证用户网络系统的安全。

ICMP Flood和UDP Flood攻击

这种攻击在短时间内向被攻击目标发送大量的ICMP消息（如ping）和UDP报文，请求回应，致使被攻击目标负担过重而不能完成正常的传输任务。

ARP欺骗攻击

局域网的网络流通根据MAC地址进行传输。ARP欺骗攻击是通过填写错误的发送端MAC地址和IP地址，使目标主机的ARP缓存表中IP地址和MAC地址对应关系错误。导致目标主机后续将IP数据报文时发给错误主机，目标网络不通且报文资源被窃取。

SYN Flood攻击

由于资源的限制，服务器只能允许有限个TCP连接。而SYN Flood攻击正是利用这一点，它伪造一个SYN报文，将其源地址设置成伪造的或者不存在的地址，然后向服务器发起连接。服务器在收到报文后用SYN-ACK应答，而此应答发出去后，不会收到ACK报文，从而造成半连接。如果攻击者发送大量这样的报文，会在被攻击主机上出现大量的半连接，直到半连接超时，从而消耗尽其资源，使正常的用户无法访问。在连接不受限制的环境里，SYN Flood会消耗掉系统的内存等资源。

WinNuke攻击

WinNuke攻击通常向装有Windows系统的特定目标的NetBIOS端口（139）发送OOB（out-of-band）数据包，引起一个NetBIOS片断重叠，致使被攻击主机崩溃。还有一种是IGMP分片报文。一般情况下，IGMP报文是不会分片的，所以，不少系统对IGMP分片报文的处理有问题。如果收到IGMP分片报文，则基本可判定受到了攻击。

IP地址欺骗（IP Spoofing）攻击

IP地址欺骗攻击是一种获取对计算机未经许可的访问的技术，即攻击者通过伪 IP地址向计算机发送报文，并显示该报文来自于真实主机。对于基于IP地址进行验证的应用，此攻击方法能够使未被授权的用户访问被攻击系统。即使响应报文不能到达攻击者，被攻击系统也会遭到破坏。

地址扫描与端口扫描攻击

这种攻击运用扫描工具探测目标地址和端口，对此作出响应的表示其存在，从而确定哪些目标系统确实存活着并且连接在目标网络上，这些主机使用哪些端口提供服务。

Ping of Death攻击

Ping of Death就是利用一些尺寸超大的ICMP报文对系统进行的一种攻击。IP报文的字段长度为16位，这表明一个IP报文的最大长度为65535字节。对于ICMP 回应请求报文，如果数据长度大于65507字节，就会使ICMP数据、IP头长度（20字节）和ICMP头长度（8字节）的总合大于65535字节。一些路由器或系统在接收到这样一个报文后会由于处理不当，造成系统崩溃、死机或重启。

Teardrop攻击防护

Teardrop攻击是一种拒绝服务攻击。是基于UDP的病态分片数据包的攻击方法，其工作原理是向被攻击者发送多个分片的IP包（IP分片数据包中包括该分片数据包属于哪个数据包以及在数据包中的位置等信息），某些操作系统收到含有重叠偏移的伪造分片数据包时将会出现系统崩溃、重启等现象。

Land攻击

在Land攻击中，攻击者将一个特别打造的数据包的源地址和目标地址都设置成被攻击服务器地址。这样被攻击服务器向它自己的地址发送消息，结果这个地址又发回消息并创建一个空连接，每一个这样的连接都将保留直到超时。在这种Land攻击下，许多服务器将崩溃。

Smurf攻击

Smurf攻击分简单和高级两种。简单Smurf攻击用来攻击一个网络。方法是将ICMP应答请求包的目标地址设置为被攻击网络的广播地址，这样该网络的所有主机都会对此ICMP应答请求作出答复，从而导致网络阻塞。高级Smurf攻击主要用来攻击目标主机。方法是将ICMP应答请求包的源地址更改为被攻击主机的地址，最终导致被攻击主机崩溃。理论上讲，网络的主机越多，攻击的效果越明显。

Fraggle攻击

Fraggle攻击与Smurf攻击为同种类型攻击。不同之处在于Fraggle攻击使用UDP包形成攻击。

IP Fragment攻击

攻击者通过向目标主机发送分片偏移小于5的分片报文，导致主机对分片报文进行重组时发生错误而造成系统崩溃。

IP Option攻击

攻击者利用IP报文中的异常选项的设置，达到探测网络结构的目的，也可由于系统缺乏对错误报文的处理而造成系统崩溃。

Huge ICMP包攻击

某些主机或设备收到超大的报文，会引起内存分配错误而导致协议栈崩溃。攻击者通过发送超大ICMP报文，让目标主机崩溃，达到攻击目的。

TCP Flag异常攻击

不同操作系统对于非常规的TCP标志位有不同的处理。攻击者通过发送带有非常规TCP标志的报文探测目标主机的操作系统类型，若操作系统对这类报文处理不当，攻击者便可达到使目标主机系统崩溃的目的。

DNS Query Flood攻击

DNS服务器收到任何DNS Query报文时都会试图进行域名解析并且回复该DNS报文。攻击者通过构造并向DNS服务器发送大量虚假DNS Query报文，占用DNS服务器的带宽或计算资源，使得正常的DNS Query得不到处理。

TCP Split Handshake攻击

客户端与恶意TCP服务器建立TCP连接时，恶意服务器伪造SYN包及其内容，向客户端发起TCP连接。建立TCP连接后，恶意TCP服务器反转角色变成了发起TCP连接的“客户端”，使得恶意流量进入内网。

配置攻击防护功能

设备的攻击防护功能在默认情况下，只有部分功能在Untrust安全域是开启的，包括IP地址欺骗攻击防护、IP扫描攻击防护、端口扫描攻击防护、ICMP Flood攻击防护、SYN Flood攻击防护、UDP Flood攻击防护、WinNuke攻击防护、Ping of Death攻击防护、Teardrop攻击防护、IP Option攻击防护、IP Fragment攻击防护、IP Directed Broadcast攻击防护和Land攻击防护。开启安全域的所有攻击防护功能，在安全域配置模式下，使用以下命令：

```
ad all
```

在安全域配置模式下使用**no ad all**命令关闭安全域的所有攻击防护功能。

用户可以对各种攻击防护功能的具体参数根据需求进行配置。设备的攻击防护配置包括：

- 配置IP地址扫描攻击防护功能
- 配置端口扫描攻击防护功能
- 配置IP地址欺骗攻击防护功能

- 配置SYN Flood攻击防护功能
- 配置SYN-Proxy功能
- 配置ICMP Flood攻击防护功能
- 配置UDP Flood攻击防护功能
- 配置Huge ICMP包攻击防护功能
- 配置WinNuke攻击防护功能
- 配置Ping of Death攻击防护功能
- 配置Teardrop攻击防护功能
- 配置IP Option攻击防护功能
- 配置TCP异常攻击防护功能
- 配置Land攻击防护功能
- 配置IP 碎片攻击防护功能
- 配置Smurf和Fraggle攻击防护功能
- 配置ARP欺骗防护功能
- 配置DNS Query Flood攻击防护功能
- 限制IP地址连接数
- 显示安全域的攻击防护配置和统计信息

配置IP地址扫描攻击防护功能

用户可以单独开启或者关闭安全域的IP地址扫描攻击防护功能，也可以配置地址扫描的警戒时间值和设备采取的行为。配置指定域的IP地址扫描攻击防护功能，在安全域配置模式使用以下命令：

ad ip-sweep [**threshold** *value*| **action** {**alarm** | **drop**}]

- **ad ip-sweep** – 开启安全域的IP地址扫描攻击防护功能。使用**no ad ip-sweep**关闭该功能。

- **threshold** *value* – 指定地址扫描的时间警戒值。如果设备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，设备就认为是受到IP地址扫描攻击。默认值是1，单位是毫秒，取值范围是1到5000毫秒。使用**no ad ip-sweep threshold**命令恢复警戒默认值。

- **action** {**alarm** | **drop**} – 指定设备对于IP地址扫描攻击的所采取的行为。**alarm**–发出警报但是允许包通过；**drop** – 在指定时间内（**threshold** *value*），设备仅允许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。默认行为是drop。使用**no ad ip-sweep action**恢复默认操作。

配置端口扫描攻击防护功能

用户可以单独开启或者关闭安全域的端口扫描攻击防护功能，也可以配置端口扫描的警戒时间值和设备采取的行为。配置安全域的端口扫描攻击防护功能，在安全域配置模式使用以下命令：

ad port-scan [**threshold** *value* | **action** {**alarm** | **drop**}]

- **ad port-scan** – 开启安全域的端口扫描攻击防护功能。使用**no ad port-scan**关闭该功能。

- **threshold** *value* – 指定端口扫描的时间警戒值。如果设备探测到同一个源IP地址在该指定时间内有10个以上TCP SYN包发往同一目标的不同端口，设备就认为是受到了端口扫描攻击。默认值是1，单位是毫秒，取值范围是1到5000毫秒。使用no ad port-scan threshold命令恢复警戒默认值。

- **action** {**alarm** | **drop**} – 指定设备对于端口扫描攻击所采取的行为。**alarm**– 发出警报但是允许包通过；**drop**–在指定时间内（**threshold** *value*），设备仅允许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。默认行为是drop。使用**no ad port-scan action**恢复默认操作。

配置IP地址欺骗攻击防护功能

系统可防护三层IP地址欺骗攻击。

开启设备的三层IP地址欺骗攻击防护功能后，数据包进入设备后，系统会对其源IP地址进行反向路由查询，并根据反向路由查询结果采取不同的行为，包括：

- 如果以该IP为源地址的数据包进入设备的安全域和以该IP为目的地址的数据包离开设备的安全域是一致的（根据反向路由查询结果可以知道以该IP为目的地址的数据包离开设备的安全域），则该数据包正常通过。
- 反之，系统判断该数据包为非正常数据包，将发出警报并丢弃该数据包。

开启安全域的三层IP地址欺骗攻击防护功能，在三层安全域配置模式下使用以下命令：

ad ip-spoofing

在安全域配置模式下使用**no ad ip-spoofing**关闭安全域的IP地址欺骗攻击防护功能。

配置SYN Flood攻击防护功能

用户可以单独开启或者关闭域的SYN Flood攻击防护功能，也可以配置SYN Flood攻击的源IP、目的IP和目的端口的警戒值以及设备的采取的行为。配置设备的SYN Flood攻击防护功能，在域配置模式下使用以下命令：

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**}]

- **ad syn-flood** – 开启安全域的SYN Flood攻击防护功能。使用**no ad syn-flood**关闭该功能。
- **source-threshold** *number* – 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。如果设备探测到一秒钟内从同一个源IP地址发出的SYN包多于该指定数，就判断为受到了SYN Flood攻击。默认值是1500个。取值范围是0到50000个。0表示不对源警戒值进行检测。使用**no ad syn-flood source-threshold**命令恢复默认值。
- **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**。如果设备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。使用**no**

ad syn-flood destination-threshold [**ip-base** | **port-base**]命令恢复默认值。

- **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。使用**no ad syn-flood destination**命令取消相应配置。

- **action** {**alarm** | **drop**} – 指定设备对于SYN Flood攻击采取的行为。**alarm**– 发出警报但是允许包通过； **drop** – 设备仅允许指定个数（**source-threshold** *number* | **destination-threshold** *number*）的SYN包通过，并且发出警报；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。默认行为是drop。使用**no ad syn-flood action**恢复默认操作。

配置SYN-Proxy功能

设备还提供SYN-Proxy功能配合ad syn-flood命令来共同防护SYN Flood攻击。当ad syn-flood和SYN-Proxy功能都开启时，SYN-Proxy功能对已经通过ad syn-flood检测的数据包起效。

设备支持SYN-Cookie功能。SYN-Cookie是一种无状态的SYN-Proxy机制。

配置安全域的SYN-Proxy以及SYN-Cookie功能，在安全域配置模式下使用以下命令：

ad syn-proxy [**min-proxy-rate** *number* | **max-proxy-rate** *number* | **proxy-timeout** number | cookie]

- **ad syn-proxy** – 开启安全域的SYN-Proxy功能用以防护SYN Flood攻击。使用**no ad syn-proxy**关闭该功能。

- **min-proxy-rate** *number* –指定激活SYN-Proxy机制或者SYN-Cookie机制（通过cookie参数开启SYN-Cookie功能后）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包个数多于该参数的指定值，就会激活SYN-Proxy或者SYN-Cookie

机制。*number*默认值是1000个每秒，取值范围是0到50000。使用**no ad syn-proxy min-proxy-rate**恢复默认值。

- **max-proxy-rate** *number* – 指定SYN-Proxy机制或者SYN-Cookie机制（通过cookie参数开启SYN-Cookie功能后）在指定时间内允许通过的最大SYN包个数。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，设备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。*number*默认值是3000个每秒，取值范围是1到1500000。使用**no ad syn-proxy max-proxy-rate**命令恢复默认值。

- **proxy-timeout** *number* – 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。默认值是30，单位为秒，取值范围是1到180秒。使用**no ad syn-proxy proxy-timeout**命令恢复默认值。

- **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，能够在功能上扩大设备处理多个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。使用**no ad syn-proxy cookie**命令关闭SYN-Cookie功能。

配置ICMP Flood攻击防护功能

用户可以单独开启或者关闭安全域的ICMP Flood攻击防护功能，也可以配置ICMP包个数的警戒值以及设备采取的操作。配置设备的ICMP Flood攻击防护功能，在安全域配置模式下使用以下命令：

ad icmp-flood [**threshold** *number* | **action** {**alarm** | **drop**}]

- **ad icmp-flood** – 开启安全域的ICMP Flood攻击防护功能。使用**no ad icmp-flood**关闭该功能。

- **threshold** *number* – 指定设备收到的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，设备就判断为受到ICMP Flood攻击，从而采取相应的处理。*number*的默认值是1500个，取值范围是1到50000。使用**no ad icmp-flood threshold**恢复默认值。

- **action** {**alarm** | **drop**} – 指定设备对于ICMP 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，设备仅允许指定个数（**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。默认行为是drop。使用**no ad icmp-flood action**恢复默认操作。

配置UDP Flood攻击防护功能

用户可以单独开启或者关闭安全域的UDP Flood攻击防护功能，也可以配置UDP包个数的警戒值以及设备采取的操作。配置设备的UDP Flood攻击防护功能，在安全域配置模式下使用以下命令：

ad udp-flood [**session-state-check**] [**source-threshold** *number* | **destination-threshold** *number* | **action** {**alarm** | **drop**}]

- **ad udp-flood** – 开启安全域的UDP Flood攻击防护功能。使用**no ad udp-flood**关闭该功能。
- **session-state-check** – 开启会话状态检查功能。开启后，系统将对识别到会话的UDP报文的回包流量不做UDP Flood攻击的检查。使用**no ad udp-flood session-state-check**关闭该功能，即默认对所有UDP报文都做UDP Flood攻击的检查。
- **source-threshold** *number* – 指定设备发送的UDP包的个数的警戒值。如果同一个源IP地址在一秒钟内发送的UDP包的个数超过该警戒值，设备就判断为受到UDP Flood攻击，从而采取相应的处理。*number*的默认值是1500个，取值范围是0到300000。使用**no ad udp-flood source-threshold**恢复默认值。
- **destination-threshold** *number* –指定设备收到的UDP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UDP包的个数超过该警戒值，设备就判断为受到UDP Flood攻击，从而采取相应的处理。*number*的默认值是1500个，取值范围是0到300000。使用**no ad udp-flood destination-threshold**恢复默认值。
- **action** {**alarm** | **drop**} – 指定设备对于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，设备仅允许指定个数（**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。默认行为是drop。使用**no ad udp-flood action**恢复默认操作。

配置Huge ICMP包攻击防护功能

用户可以单独开启或者关闭安全域的Huge ICMP攻击防护功能，也可以配置ICMP包的大小的警戒值以及设备采取的行为。配置设备的Huge ICMP报攻击防护功能，在安全域配置模式下使用一下命令：

ad huge-icmp-pak [**threshold** *number* | **action** {**alarm** | **drop**}]

- **ad huge-icmp-pak** – 开启安全域的Huge ICMP包攻击防护功能。使用**no ad huge-icmp-pak**关闭该功能。
- **threshold** *number* – 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，设备就判断为受到Huge ICMP包攻击，从而采取相应的处理措施。*number*默认值是1024字节，取值范围是1到50000字节。使用**no ad huge-icmp-pak threshold**恢复默认值。
- **action** {**alarm** | **drop**} – 指定设备对于Huge ICMP包攻击采取的行为。**alarm**– 发出警报但是允许包通过；**drop**– 发出警报并且丢弃攻击包。默认行为是drop。使用**no ad udp-flood action**恢复默认操作。

配置WinNuke攻击防护功能

WinNuke攻击防护功能开启后，当设备发现受到WinNuke攻击后，会丢弃攻击包并且发出警报通知。开启安全域的WinNuke攻击防护功能，在安全域配置模式使用以下命令：

ad winnuke

在安全域配置模式下，使用**no ad winnuke**关闭安全域的WinNuke攻击防护功能。

配置Ping of Death攻击防护功能

Ping of Death攻击防护功能开启后，当设备发现受到Ping of Death攻击后，会丢弃攻击包并且发出警报通知。开启安全域的Ping of Death攻击防护功能，在安全域配置模式使用以下命令：

ad ping-of-death

在安全域配置模式下，使用**no ad ping-of-death**关闭安全域的Ping of Death攻击防护功能。

配置Teardrop攻击防护功能

Teardrop攻击防护功能开启后，当设备发现受到Teardrop攻击后，会丢弃攻击包并且发出警报通知。开启安全域的Teardrop攻击防护功能，在安全域配置模式使用以下命令：

```
ad tear-drop
```

在安全域配置模式下，使用**no ad tear-drop**关闭安全域的Teardrop攻击防护功能。

配置IP Option攻击防护功能

IP Option攻击防护功能开启后，默认情况下当设备发现受到IP Option攻击后，会丢弃攻击包并且发出警报通知。用户可以根据需要改变设备的行为。设备会对以下IP Option类型进行防护：Security、Loose Source Route、Record Route、Stream ID、Strict Source Route和Timestamp。配置IP Option攻击防护功能，在安全域配置模式使用以下命令：

```
ad ip-option [action {alarm | drop}]
```

- **ad ip-option** – 开启安全域的IP Option攻击防护功能。使用**no ad ip-option**命令关闭该功能。
- **action** {**alarm** | **drop**} – 指定设备对于IP Option攻击采取的行为。**alarm**– 发出警报但是允许包通过；**drop**– 发出警报并且丢弃攻击包。默认行为是drop。使用**no ad ip-option action**恢复默认行为。

配置TCP异常攻击防护功能

TCP异常攻击防护功能开启后，默认情况下当设备发现受到TCP异常攻击后，会丢弃攻击包并且发出警报通知。用户可以根据需要改变设备的行为。当设备检测到以下各种情况，就会判断为受到TCP异常攻击：

- SYN包被分片；
- TCP包仅设置了FIN flag；
- TCP包仅没有设置flag；
- TCP包的FIN和RST flag同时被设置；

- TCP包的SYN和URG flag同时被设置；
- TCP包的SYN和RST flag同时被设置；
- TCP包的SYN和FIN flag同时被设置。

配置TCP异常攻击防护功能，在安全域配置模式使用以下命令：

```
ad tcp-anomaly [action {alarm | drop}]
```

- **ad tcp-anomaly** – 开启安全域的TCP异常攻击防护功能。使用**no ad tcp-anomaly**命令关闭该功能。
- **action {alarm | drop}** – 指定设备对于TCP异常攻击采取的行为。**alarm**– 发出警报但是允许包通过；**drop**– 发出警报并且丢弃攻击包。默认行为是drop。使用**no ad tcp-anomaly action**恢复默认操作。

配置Land攻击防护功能

Land攻击防护功能开启后，默认情况下当设备发现受到Land攻击后，会丢弃数据包并且发出警报通知。用户可以根据需要改变设备的行为。配置Land攻击防护功能，在安全域配置模式使用以下命令：

```
ad land-attack [action {alarm | drop}]
```

- **ad land-attack** – 开启安全域的Land攻击防护功能。使用**no ad land-attack**命令关闭该功能。
- **action {alarm | drop}** – 指定设备对于Land攻击采取的行为。**alarm**– 发出警报但是允许包通过；**drop**– 发出警报并且丢弃攻击包。默认行为是drop。使用**no ad land-attack action**恢复默认操作。

配置IP 碎片攻击防护功能

数据包在不同网络间进行传输时，有时需要根据网络的MTU值将数据包分片。攻击者可以通过修改IP碎片在重组过程中发现漏洞进行攻击。当被攻击方收到被修改过的IP碎片后，轻则不能正确重组碎片，重则导致整个系统崩溃。

默认情况下当设备发现受到IP碎片攻击后，会丢弃攻击包并且发出警报通知。用户可以根据需要改变设备的行为。配置IP 碎片攻击防护功能，在安全域配置模式使用以下命令：

ad ip-fragment [**action** {**alarm** | **drop**}]

- **ad ip-fragment** – 开启安全域的IP碎片攻击防护功能。使用**no ad ip-fragment**命令关闭该功能。
- **action** {**alarm** | **drop**} – 指定设备对于IP碎片攻击采取的行为。**alarm**– 发出警报但是允许包通过；**drop**– 发出警报并且丢弃攻击包。默认行为是drop。使用**no ad ip-fragment action**恢复默认操作。

配置Smurf和Fraggle攻击防护功能

Smurf和Fraggle攻击防护功能开启后，默认情况下当设备发现受到Smurf或者Fraggle攻击后，会丢弃数据包并且发出警报通知。用户可以根据需要改变设备的行为。配置Smurf和Fraggle攻击防护功能，在安全域配置模式下使用以下命令：

ad ip-directed-broadcast [**action** {**alarm** | **drop**}]

- **ad ip-directed-broadcast** – 开启安全域的Smurf和Fraggle攻击防护功能。使用**no ad ip-directed-broadcast**命令关闭该功能。
- **action** {**alarm** | **drop**} – 指定设备对于Smurf和Fraggle攻击采取的行为。**alarm**– 发出警报但是允许包通过；**drop**– 发出警报并且丢弃所有包。默认行为是drop。使用**no ad ip-directed-broadcast action**恢复默认操作。

配置ARP欺骗防护功能

设备的ARP欺骗防护功能能够保护内网不受ARP欺骗攻击。配置ARP欺骗防护功能，在安全域配置模式使用以下命令：

ad arp-spoofing {**reverse-query** | **ip-number-per-mac** *number* [**action** [**drop** | **alarm**]] | **gratuitous-arp-send-rate** *number*}

- **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。使用**no ad arp-spoofing reverse-query** 命令关闭ARP反向查询功能。

- **ip-number-per-mac** *number* – 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（参数的默认值），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**）。该参数值的范围是0到1024。使用**no ad arp-spoofing ip-number-per-mac**命令恢复参数默认值。

- **gratuitous-arp-send-rate***number*– 指定设备是否发出Gratuitous ARP包。如果该参数值是0，则不发Gratuitous ARP包（参数的默认值）；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。使用**no ad arp-spoofing gratuitous-arp-send-rate**命令恢复参数的默认值。

配置DNS Query Flood攻击防护功能

DNS是域名系统（Domain Name System）的简称，用来实现域名转换为IP地址和IP地址解析为域名。DNS是应用层协议，既可以基于TCP连接也可以基于UDP连接，DNS Query Flood攻击主要是指基于UDP的DNS查询报文洪水攻击。

DNS Query Flood攻击采用的方法是向被攻击的DNS服务器发送大量的域名解析请求，通常请求解析的域名是随机生成或者是网络上根本不存在的域名。被攻击的DNS服务器在接收到域名解析请求时，首先会在服务器上查找是否有对应的缓存，如果查找不到并且该域名无法直接由服务器解析时，DNS服务器会向其上层DNS服务器递归查询域名信息。域名解析的过程给服务器带来了很大的负载，每秒钟域名解析请求超过一定的数量就会造成DNS服务器解析域名超时。

设备支持DNS Query Flood攻击防护功能，用户可以单独开启或者关闭安全域的DNS Query Flood攻击防护功能，也可以配置DNS查询报文个数的警戒值以及设备采取的操作。配置设备的DNS Query Flood攻击防护功能，在安全域配置模式下使用以下命令：

ad dns-query-flood [**recursion**] [**source-threshold** *number*] [**destination-threshold** *number* | **action** {**alarm** | **drop**}]

- **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。

- **source-threshold** *number* – 指定设备发送的DNS查询报文或DNS递归查询报文的个数的警戒值。如果一秒钟内同一个源IP地址发送的DNS查询报文个数超过该警戒值，设备就判断为受到DNS Query Flood攻击，从而采取相应的处理措施。*number*的默认值是1500个，取值范围是0到300000。使用**no ad dns-query-flood source-threshold**恢复默认值。

- **destination-threshold** *number* – 指定设备收到的DNS查询报文或DNS递归查询报文的个数的警戒值。如果一秒钟内设备收到的到达同一个目的IP地址的DNS查询报文个数超过该警戒值，设备就判断为受到DNS Query Flood攻击，从而采取相应的处理措施。*number*的默认值是1500个，取值范围是0到300000。使用**no ad dns-query-flood destination-threshold**恢复默认值。

- **action** {**alarm** | **drop**} – 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查询报文通过；**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。使用**no ad dns-flood action**恢复默认操作。

注意: DNS Query Flood攻击防护功能仅对UDP DNS查询报文有效。

配置TCP Split Handshake攻击防护功能

TCP Split Handshake攻击防护功能开启后，默认情况下当设备发现受到此类型攻击后，会丢弃数据包并且发出警报通知。用户可以根据需要改变设备的行为。配置TCP Split Handshake攻击防护功能，在安全域配置模式使用以下命令：

ad tcp-split-handshake [**action** {**alarm** | **drop**}]

- **ad tcp-split-handshake** – 开启安全域的TCP Split Handshake攻击防护功能。使用no ad tcp-split-handshake命令关闭该功能。

- **action** {**alarm** | **drop**} – 指定设备对于TCP Split Handshake攻击采取的行为。**alarm**发出警报但是允许包通过； **drop**发出警报并且丢弃攻击包。默认行为是**drop**。使用**no ad land-attack action**恢复默认操作。

配置攻击防护白名单

开启攻击防护功能后，安全域中的所有流量都会受到攻击防护功能的检查。在实际应用中，用户可能出于测试等目的不希望对某些主机所发送的流量进行检查。针对这种情况，用户可以将特定的地址或地址范围添加到攻击防护白名单。白名单中的地址或地址范围不受攻击防护功能的检查。

配置攻击防护白名单，在安全域配置模式下，使用以下命令：

ad whitelist [**id** *id*] **ip** {*A.B.C.D/M* | *address-entry*}

- **id** – 指定白名单规则的ID。各设备型号ID取值范围不同。如果不指定，系统将自动为该条规则分配一个ID。

- A.B.C.D/M–指定添加到白名单规则中的IP地址和网络掩码。

- *address-entry*–指定添加到白名单规则中的地址条目。

使用该命令no的形式删除指定的白名单规则：

no ad whitelist {**id** *id* | **ip** {*A.B.C.D/M* | *addr-book*}}

显示安全域的攻击防护配置和统计信息

系统能够显示安全域的攻击防护配置和统计信息。显示安全域的攻击防护配置和统计信息，在任何模式下使用以下命令：

show ad zone *zone-name* {**statistics** | **configuration** | **whitelist**}

- *zone-name* – 指定安全域的名称。

- **statistics** – 显示指定安全域的统计信息。

- **configuration** – 显示指定安全域的攻击防护配置信息。
- **whitelist** – 显示指定安全域的攻击防护白名单配置信息。

攻击防护配置举例

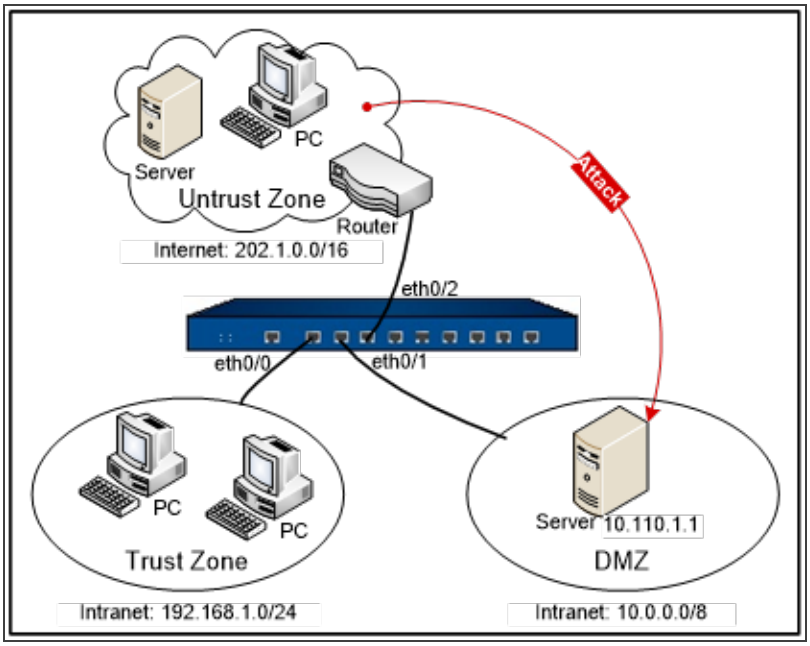
本节介绍攻击防护的配置实例以帮助用户更好的理解与配置设备的攻击防护功能。

Land攻击防护功能配置举例

本小节介绍Land攻击防护功能的配置实例。

组网需求

将设备的以太网口ethernet 0/0配置为Trust域，以太网口ethernet 0/2配置为Untrust域，以太网口ethernet 0/1配置为DMZ域。需要对DMZ域内的服务器进行Land攻击防护。下图为该需求的组网图：



配置步骤

第一步：配置设备接口ethernet0/0。

```
hostname(config)# interface ethernet0/0

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

```
hostname(config-if-eth0/0)# ip address 192.168.1.1/24
hostname(config-if-eth0/0)# exit
hostname(config)#
```

第二步：配置设备接口ethernet0/2。

```
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# zone untrust
hostname(config-if-eth0/2)# ip address 202.1.0.1/24
hostname(config-if-eth0/2)# exit
hostname(config)#
```

第三步：配置设备接口ethernet0/1。

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone dmz
hostname(config-if-eth0/1)# ip address 10.0.0.1/8
hostname(config-if-eth0/1)# exit
hostname(config)#
```

第四步：配置策略规则。

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zone dmz
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config)#
```

第五步：开启untrust域的Land攻击防护功能。

```
hostname(config)# zone untrust
hostname(config-zone)# ad land-attack
hostname(config-if)# exit
hostname(config)#
```

第六步：检测对服务器10.110.1.1配置的Land攻击防护功能。给报文设置相同的源IP和目的IP地址，向10.110.1.1发送。设备检测到Land攻击，并报警。

SYN Flood攻击防护功能配置举例

本小节介绍SYN Flood攻击防护功能的配置实例。

组网需求

将设备的以太网口ethernet0/0配置为Trust域，以太网口ethernet0/2配置为Untrust域，以太网口ethernet0/1配置为DMZ域。需要对DMZ域内的服务器进行SYN Flood攻击防护。

配置步骤

第一步：配置设备接口ethernet0/0。

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 192.168.1.1/24
hostname(config-if-eth0/0)# exit
hostname(config)#
```

第二步：配置设备接口ethernet0/2。

```
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# zone untrust
hostname(config-if-eth0/2)# ip address 202.1.0.1/24
hostname(config-if-eth0/2)# exit
hostname(config)#
```

第三步：配置设备接口ethernet0/1。

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone dmz
hostname(config-if-eth0/1)# ip address 10.0.0.1/8
hostname(config-if-eth0/1)# exit
hostname(config)#
```

第四步：配置策略规则。

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zone dmz
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config)#
```

第五步：开启untrust域的SYN Flood攻击防护功能。

```
hostname(config)# zone untrust
hostname(config-zone)# ad syn-flood
hostname(config-if)# exit
hostname(config)#
```

第六步：检测对服务器10.110.1.1配置的SYN Flood攻击防护功能。以大于1500包/秒的速度向服务器10.110.1.1发送报文。设备检测到SYN Flood攻击，并报警。

IP地址扫描攻击防护功能配置举例

本小节介绍IP地址扫描攻击防护功能的配置实例。

组网需求

将设备的以太网口ethernet0/0配置为Trust域，以太网口ethernet0/2配置为Untrust域，以太网口ehernet0/1配置为DMZ域。需要对DMZ域内的服务器进行IP地址扫描攻击防护。

配置步骤

第一步：配置设备接口ethernet0/0。

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 192.168.1.1/24
hostname(config-if-eth0/0)# exit
hostname(config)#
```

第二步：配置设备接口ethernet0/2。

```
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# zone untrust
hostname(config-if-eth0/2)# ip address 202.1.0.1/24
hostname(config-if-eth0/2)# exit
hostname(config)#
```

第三步：配置设备接口ethernet0/1。

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone dmz
hostname(config-if-eth0/1)# ip address 10.0.0.1/8
hostname(config-if-eth0/1)# exit
hostname(config)#
```

第四步：配置策略规则。

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zone dmz
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config)#
```

第五步：开启untrust域的IP地址扫描攻击防护功能。

```
hostname(config)# zone untrust
hostname(config-zone)# ad ip-sweep
hostname(config-if)# exit
hostname(config)#
```

第六步：检测配置的IP扫描攻击防护功能。用smartbits构造报文，对ethernet0/2进行IP扫描攻击，以大于10包/毫秒的速度向202.1.0.1发送。设备检测到扫描攻击，并报警。

病毒过滤

系统具有许可证控制的病毒过滤功能，能够为用户提供高速、高性能以及低延迟的病毒过滤解决方案。配置系统的病毒过滤功能后，设备能够探测各种病毒威胁，例如蠕虫、木马、恶意软件、恶意网站等，并且根据配置对发现的病毒进行处理。

系统支持基于安全域和基于策略的病毒过滤配置方式。为安全域配置病毒过滤规则后，系统将会对以绑定安全域为目的安全域的流量根据病毒过滤规则配置进行病毒过滤检查。将病毒过滤规则绑定到策略规则后，系统将会对与策略规则相匹配的流量根据规则配置进行病毒过滤检查。

系统病毒特征库包含百万余种病毒特征，支持病毒特征库的每日自动升级，也可以手动实时升级。

系统病毒过滤功能可扫描协议类型包括POP3、HTTP、SMTP、IMAP4以及FTP；可扫描文件类型包括存档文件（包含压缩存档文件，支持压缩类型有GZIP、BZIP2、TAR、ZIP和RAR）、PE、HTML、Mail、RIFF和JPEG。

如设备开启了IPv6，病毒过滤功能支持基于IPv6传输的病毒过滤。

病毒过滤配置

实现系统的病毒过滤功能，用户需要按照以下步骤进行操作：

1. 定义病毒过滤Profile，在Profile中指定扫描文件类型、扫描协议、系统发现病毒后采取的动作以及标签邮件功能。
2. 绑定病毒过滤Profile到适当的策略规则或者将病毒过滤Profile绑定到安全域。如需对HTTPS流量进行病毒过滤检查，请参照下文绑定病毒过滤Profile到策略规则。

注意: 初次使用病毒过滤功能，需要首先更新病毒特征库。关于病毒特征库更新配置，请参阅“病毒特征库更新配置”。为保证能够正常连接到默认更新服务器，请在更新前为设备配置DNS服务器。

安装病毒过滤功能许可证并重启设备后，系统的病毒过滤功能为开启状态，并且此时系统的最大并发连接数将会减半。用户可以通过show version命令查看系统的病毒过滤功能是否开启。开启或者关闭病毒过滤功能，在任何模式下使用以下命令：

```
exec av {enable | disable}
```

- **enable** – 开启系统的病毒过滤功能。
- **disable** – 关闭系统的病毒过滤功能。

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

创建病毒过滤Profile

病毒过滤Profile中主要指定需要病毒扫描的文件类型、协议类型，以及系统发现病毒后的动作。创建病毒过滤Profile，在全局配置模式下使用以下命令：

av-profile *av-profile-name*

- *av-profile-name* - 指定所创建的病毒过滤Profile的名称，并且进入该病毒过滤Profile的配置模式。如果指定名称已存在，则直接进入病毒过滤Profile配置模式。使用**no av-profile** *av-profile-name*删除指定的病毒过滤 Profile。

为实现精确扫描控制，在病毒过滤Profile配置模式下，用户可以分别指定需扫描协议类型以及动作和文件类型。其中，协议类型为必配，而文件类型可以根据需要进行选择性配置。如果只配置协议类型，而未配置文件类型，系统仅对通过指定协议传输的文本文件进行扫描。如果需要扫描的对象为通过指定类型传输的指定类型文件，例如通过HTTP协议传输的HTML文件，用户需要在病毒过滤Profile中同时配置对HTTP协议和HTML文件进行扫描。

防恶意网站功能

为保护用户，防止用户点击恶意链接并访问恶意网站，系统提供防恶意网站功能。开启防恶意网站功能后，系统会对用户试图访问的网站链接进行木马以及钓鱼等恶意网站检测，并根据系统发现病毒后的动作配置，对恶意链接进行相应处理。关于系统发现病毒后的动作配置，请参阅“指定协议类型”。默认情况下，防恶意网站功能是开启的。开启防恶意网站功能，在病毒过滤Profile配置模式下使用以下命令：

anti-malicious-sites

使用该命令no的形式关闭防恶意网站功能：

```
no anti-malicious-sites
```

指定防恶意网站访问控制动作

指定防恶意网站访问控制动作，在病毒过滤Profile配置模式下使用以下命令：

```
anti-malicious-sites [action{ log-only | reset-conn | warning}| pacp]
```

- **action** {**log-only** | **reset-conn** | **warning**} – 指定对发现恶意网站采取的动作。
  - **log-only** – 产生日志信息。该选项为FTP、IMAP4、POP3或者SMTP协议发现病毒时系统采取的默认动作。
  - **reset-conn** – 发现病毒后，重置病毒连接。
  - **warning** – 弹出警告提示页面，提示用户发现恶意网站。扫描发现恶意网站时，给出警告提示页面，如下图所示。

    用户可以点击“为何要阻止此网站”按钮，跳转到Google诊断页面，查看阻止访问原因。
    或者，点击“忽略此警告”链接，跳过警告提示页面，继续访问。跳过警告提示页面后，若用户一小时之内再次访问该网站，将不会收到警告提示。

- **pcap** – 指定对防恶意网站访问控制进行抓包。

使用该命令no的形式取消对防恶意网站访问控制动作的指定。

```
no anti-malicious-sites [action{ log-only | reset-conn | warning}| pacp]
```

指定协议类型

指定病毒扫描协议类型，在病毒过滤配置模式下使用以下命令：

protocol-type {{**ftp** | **imap4** | **pop3** | **smtp**} [**pcap** | **action** {**fill-magic** | **log-only** | **reset-conn**}] | **http** [**pcap** |**action** {**fill-magic** | **log-only** | **reset-conn** | **warning**}]}

- **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。
- **pcap** – 指定对协议传输信息病毒扫描进行抓包。
- **action** {**fill-magic** | **log-only** | **reset-conn** | **warning**} – 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FTP、IMAP4、POP3或者SMTP协议发现病毒时系统采取的默认动作。
  - **reset-conn** – 发现病毒后，重置病毒连接。
  - **warning** – 弹出警告提示页面，提示用户发现病毒或者恶意下载链接。该选项只对通过HTTP协议传输的信息进行病毒扫描时有效，且为发现病毒或者恶意下载链接时系统采取的默认动作。
    扫描发现病毒时，给出警告提示页面，如下图所示：

扫描发现恶意下载链接时，给出警告提示页面，如下图所示：

用户可以点击“忽略此警告”链接，跳过警告提示页面，继续访问。跳过警告提示页面后，若用户一小时之内再次访问该网站，将不会收到警告提示。

使用多条该命令可指定多个协议类型。

使用以上命令no的形式取消协议类型的指定：

no protocol-type {**ftp** | **imap4** | **pop3** | **smtp** | **http**}

SMTP、POP3和IMAP4都是邮件传输协议，用来传送mail类型的文件。当配置对邮件进行扫描时，必须在配置对SMTP、POP3或IMAP4协议进行扫描的同时配置对mail类型文件进行扫描；并且，由于邮件的正文和附件都是嵌套在mail文件中的，因此还需要配置对邮件中可能包含的附件类型进行扫描。

指定文件类型

指定病毒扫描文件类型，在病毒过滤Profile配置模式下使用以下命令：

file-type {**bzip2** | **gzip** | **html** | **jpeg** | **mail** | **pe** | **rar** | **riff** | **tar** | **zip** | **elf** | **pdf** | **office** | **raw-data** | **others** }

- **bzip2** – 指定对BZIP2压缩文件进行病毒扫描。
- **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。另外，系统还支持对已经加壳（支持的加壳类型有ASPack 2.12、UPack 0.399、UPX的所有版本以及FSG的1.3、1.31、1.33和2.0版本）的PE文件进行扫描。
- **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。
- **elf** – 指定对ELF类型文件进行病毒扫描。
- **pdf** – 指定对PDF类型文件进行病毒扫描。
- **office** – 指定对office文件进行病毒扫描。
- **raw-data** – 指定对txt文件和无法识别的文件进行病毒扫描。
- **others**– 指定对除上述可配置文件类型以外的其他类型文件进行病毒扫描。

使用多条该命令可指定多个文件类型。

使用以上命令no的形式取消文件类型的指定：

no file-type { **bzip2** | **gzip** | **html** | **jpeg** | **mail** | **pe** | **rar** | **riff** | **tar** | **zip** | **elf** | **pdf** | **office** | **raw-data** | **others** }

标签邮件功能

如果对通过SMTP协议传输的邮件进行病毒扫描，则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。如果没有发现病毒，则提示“No virus found”，如下表所示：

邮件正文
No virus found. Checked by Hillstone AntiVirus

如发现病毒，则显示邮件中病毒相关信息，包括系统扫描文件的名称、文件的路径、扫描结果以及对该病毒的执行动作，如下表所示：

邮件正文
Here are the AntiVirus scanning results: Body: Found virus: virusname1, action: log; Attachment1.zip/virustest1.exe: Found virus: virusname2, action: log; Attachment2.tar/subfolder/file1.doc: Found virus: virusname3, action: log; Checked by Hillstone AntiVirus

注意: 邮件中最多显示三个病毒文件（包含邮件主体和附件）的扫描信息。全部文件的扫描信息请在日志中查看。

开启或关闭标签邮件功能

默认情况下，标签邮件功能是关闭的。用户需要在病毒过滤Profile配置模式下，输入以下命令开启标签邮件功能：

```
label-mail
```

使用该命令no的形式关闭标签邮件功能：

no label-mail

配置邮件签名

在开启标签邮件功能后，用户可以指定标签邮件的签名。默认情况下，标签邮件签名为“Checked by Hillstone AntiVirus”。邮件签名不支持中文签名。在病毒过滤配置模式下，输入以下命令配置签名：

mail-sig *signature-string*

- *signature-string* – 配置标签邮件的签名。

在病毒过滤配置模式下，使用该命令no形式恢复默认值：

no mail-sig

绑定病毒过滤Profile到安全域

将病毒过滤Profile绑定到安全域后，系统将会对以该安全域为目的安全域的流量按照Profile配置进行病毒过滤检查。当策略规则已经绑定了病毒过滤Profile，同时策略规则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。

绑定病毒过滤Profile到安全域，在安全域配置模式下，使用以下命令：

av enable *av-profile-name*

- *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。

在安全域配置模式下，使用该命令no的形式取消病毒过滤Profile的绑定：

no av enable

查看安全域与病毒过滤Profile的绑定信息，使用**show av zone-binding**命令。

绑定病毒过滤Profile到策略规则

将病毒过滤Profile绑定到策略规则后，系统将会对与策略规则相匹配的流量根据Profile配置进行病毒过滤检查。绑定病毒过滤Profile到策略规则，在策略规则配置模式下使用以下命令：

av {*av-profile-name* | **no-av**}

- *av-profile-name* – 指定绑定到策略规则的病毒过滤Profile的名称。

- **no-av** – 绑定名为“no-av”的预定义病毒过滤Profile到策略规则，含义为不做病毒过滤。当为策略规则绑定该Profile后，即使系统中有相匹配的其他病毒过滤Profile，系统仍不会对流量进行病毒过滤检测。

在策略规则配置模式下使用该命令no的形式取消病毒过滤Profile的绑定：**no av**

如果需要病毒过滤对HTTPS流量进行扫描，需要为此条策略规则（病毒过滤Profile绑定到的策略规则）启用SSL代理功能。系统将根据SSL代理Profile解密HTTPS流量，对解密后的数据根据病毒过滤Profile进行检测。根据安全策略规则的配置不同，系统将进行如下操作：

安全策略规则配置	操作
启用SSL代理 不启用病毒过滤	根据SSL代理Profile解密HTTPS流量，对解密后的数据不进行病毒过滤。
启用SSL代理 启用病毒过滤	根据SSL代理Profile解密HTTPS流量，对解密后的数据根据病毒过滤Profile进行病毒过滤。
不启用SSL代理 启用病毒过滤	对HTTP流量根据病毒过滤Profile进行病毒过滤。对HTTPS流量不进行解密，不进行病毒过滤，只进行转发。

当安全策略规则所关联的安全域也启用病毒过滤时，系统也将进行如下操作：

安全策略规则配置	安全域配置	操作
启用SSL代理 不启用病毒过滤	启用病毒过滤	根据SSL代理Profile解密HTTPS流量，对解密后的数据根据安全域配置的病毒过滤Profile进行病毒过滤。
启用SSL代理 启用病毒过滤	启用病毒过滤	根据SSL代理Profile解密HTTPS流量，对解密后的数据根据安全策略规则中配置的病毒过滤Profile进行病毒过滤。
不启用SSL代	启用病毒过滤	对HTTP流量根据安全策略规则中配置的病毒过滤Pro-

安全策略规则配置	安全域配置	操作
理 启用病毒过滤		file进行病毒过滤。对HTTPS流量不进行解密，不进行病毒过滤，只进行转发。

提示: 更多关于SSL代理Profile的配置，请参阅“SSL代理”章节。

显示病毒过滤profile信息

在任何模式下，输入以下命令显示病毒过滤profile信息：

```
show av-profile
```

指定可压缩嵌套层数

默认情况下，系统可以对最多5层压缩嵌套的文件进行扫描（含5层），用户可以对该层数进行配置，并且指定对超出该层数限制的压缩嵌套文件的处理动作。配置压缩嵌套层数以及动作，在全局配置模式下，使用以下命令：

```
av max-decompression-recursion number exceed-action {log-only | reset-conn}
```

- *number* – 指定压缩嵌套层数。范围是1到5。默认值是1。
- **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**。

使用以上命令no的形式恢复默认值：

```
no av max-decompression-recursion
```

注意: 对于包含docx、pptx，xlsx、jar、apk格式的压缩文件，当处理动作被指定为断开连接（**reset-conn**）时，用户需要将压缩嵌套层数增加1层，以避免无法下载该压缩文件的问题。

病毒特征库更新配置

默认情况下，系统会每日自动更新病毒特征库，用户可以根据需要更改病毒特征库更新配置。病毒特征库更新配置包括：

- 配置病毒特征库更新模式
- 配置更新服务器
- 指定HTTP代理服务器
- 指定更新时间
- 立即更新
- 导入病毒特征文件
- 显示病毒特征信息
- 显示病毒特征库更新配置信息

配置病毒特征库更新模式

系统支持手动和自动两种更新方式。配置病毒特征库更新方式，在全局配置模式下，使用以下命令：

```
av signature update mode {auto | manual}
```

- **auto** – 指定自动更新病毒特征库。该方式为系统的默认更新方式。
- **manual** – 指定手动更新病毒特征库。

在全局配置模式下使用该命令no的形式恢复默认更新模式：

```
no av signature update mode
```

配置更新服务器

系统提供默认的病毒特征库更新服务器，即update1.hillstonenet.com和update2.hillstonenet.com，同时用户也可以根据需要配置其它更新服务器下载最新病毒特征。最多可配置3个。配置更新服务器，在全局配置模式下，使用以下命令：

av signature update {**server1** | **server2** | **server3**} {*ip-address* | *domain-name*}

- **server1** | **server2** | **server3** – 指定将要配置的服务器。**server1**的默认值为update1.hillstonenet.com，**server2**的默认值为update2.hillstonenet.com。
- *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）。

在全局配置模式下，使用该命令no的形式取消更新服务器的指定：

no av signature update {**server1** | **server2** | **server3**}

指定HTTP代理服务器

当设备需要通过HTTP代理服务器访问互联网时，为确保特征库能够正常升级，需要在设备上指定代理服务器的IP地址和端口号。

为病毒过滤特征库升级指定代理服务器，在全局配置模式下，使用如下命令：

av signature update proxy-server {**main** | **backup**} *ip-address port-number*

- **main** | **backup** – 使用main参数指定主代理服务器，使用backup指定备份代理服务器。
- *ip-address port-number* – 指定代理服务器的IP地址和端口号。

取消指定的代理服务器，使用**no av signature update proxy-server** {**main** | **backup**}命令。

指定更新时间

默认情况下，系统采用自动模式每日更新病毒特征库，并且为避免服务器流量过大，每日更新时间是随机的。用户可以根据需要指定病毒特征库更新的频率和时间，在全局配置模式下，使用以下命令：

av signature update schedule {**daily** | **weekly** {**mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun**}} [*HH:MM*]

- **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。

立即更新

无论更新模式为手动还是自动，用户都可以随时使用以下命令更新病毒特征库。立即更新病毒特征库，在任何模式下，使用以下命令：

exec av signature update

- **exec av signature update** – 仅对当前病毒特征库与更新服务器最新发布病毒特征库的不同部分进行更新。

导入病毒特征文件

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特征库进行更新，针对这一问题，系统提供病毒特征文件导入功能，即通过FTP、TFTP服务器或者U盘将病毒特征文件导入到设备，从而更新设备的病毒特征库。导入病毒特征文件，在执行模式下，使用以下命令：

import av signature from {**ftp server** *ip-address* [**user** *user-name* **password** *password*] | **tftp server** *ip-address* } [**vrouter** *vr-name*] *file-name*

- *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。
- **vrouter** *vr-name* – 指定FTP或者TFTP服务器所属的VRouter。
- *file-name* – 指定导入的病毒特征文件的名称。

显示病毒特征库信息

用户可以随时使用相应的show命令查看设备的病毒特征库信息，包括病毒特征库版本、发布日期以及病毒特征个数等。查看病毒特征库信息，在任何模式下使用以下命令：

show av signature info

显示病毒特征库更新配置信息

用户可以随时使用相应的show命令查看设备上的病毒特征库更新信息，包括更新服务器信息、更新模式、更新频率及时间以及病毒特征库更新状况等。查看病毒特征库更新配置信息，在任何模式下使用以下命令：

```
show av signature update
```

病毒过滤配置举例

使用病毒过滤功能前，确认已经为设备安装了相应的病毒过滤许可证。

本节介绍病毒过滤配置实例，通过病毒过滤配置，使设备能够：

- 对Email及其附件进行病毒过滤扫描，并将发出的邮件病毒扫描结果显示在邮件中。Email通过SMTP和POP3协议传输，附件中可能包含.exe和.jpeg文件。
- 对压缩文件进行扫描。RAR压缩文件中包含.jpeg文件，压缩文件通过FTP协议进行传输。

配置步骤

第一步：配置病毒过滤Profile，指定需要进行扫描的协议以及文件类型：

```
hostname(config)# av-profile email-scan
hostname(config-av-profile)# protocol-type smtp action fill-magic
hostname(config-av-profile)# protocol-type pop3 action fill-magic
hostname(config-av-profile)# protocol-type ftp action fill-magic
hostname(config-av-profile)# file-type pe
hostname(config-av-profile)# file-type jpeg
hostname(config-av-profile)# file-type mail
hostname(config-av-profile)# label-mail
hostname(config-av-profile)# mail-sig “Checked by Mail AntiVirus”
hostname(config-av-profile)# exit
hostname(config)#
```

第二步：创建策略规则，并在规则中引用病毒过滤Profile：

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# av email-scan
hostname(config-policy-rule)# exit
hostname(config)#
```

第三步：通过show version命令查看系统病毒过滤功能的开启状态。如果为关闭，则运行以下命令开启系统的病毒过滤功能并重启系统使其生效：

```
hostname(config)# exec av enable
```

沙箱防护

沙箱在虚拟环境中执行可疑文件，收集可疑文件的动态行为，对这些动态行为进行分析，并根据分析结果判断文件合法性。

系统的沙箱防护功能使用云沙箱技术，将可疑文件上传到云端。云沙箱对可疑文件分析，搜集可疑文件的动态行为，判断文件合法性，将分析结果反馈给系统。

沙箱防护功能包括如下内容：

- 收集及上传可疑文件：沙箱防护功能对设备流量进行解析，提取出流量里的可疑文件。
    - 如果此可疑文件在本地数据库中暂无分析结果，则将其上传到云平台，并由云平台将可疑文件上传到云沙箱进行检测。
    - 如果此文件已经在本地沙箱防护数据库中标记为恶意文件，则将产生威胁日志和云沙箱日志。

此外，用户需要配置沙箱防护规则，指定可疑文件标准。

- 检查云沙箱分析结果并采取响应措施：沙箱防护功能从云沙箱接收到可疑文件的分析结果后，检查分析结果，判断文件合法性，保存分析结果到本地数据库。若分析结果判定可疑文件为恶意文件，则产生威胁日志和云沙箱日志。此部分工作由沙箱防护功能自动完成，无需相关配置。
- 维护本地沙箱防护数据库：标识上传的文件，记录文件上传时间，保存其分析结果。此部分工作由沙箱防护功能自动完成，无需相关配置。

沙箱防护配置准备工作

使用的沙箱防护功能，必须完成以下准备工作：

- 确认系统版本支持沙箱防护御功能；
- 当前设备已经连接到云平台。如何连接，参阅启用云·景。
- 安装沙箱防护许可证，然后重启设备。设备成功重启后，沙箱防护功能即处于开启状态。

除部分设备（M8860/M8260/M7860/M7360/M7260）以外，开启沙箱防护后，系统的最大并发连接数将会减半。

用户可以通过show version命令查看沙箱防护功能是否开启。开启或者关闭沙箱防护功能，在任何模式下使用以下命令：

```
exec sandbox {enable | disable}
```

- **enable** – 开启系统的沙箱防护功能。
- **disable** – 关闭系统的沙箱防护功能。

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

配置沙箱防护功能

系统支持基于策略的沙箱防护配置方式。用户需要按照以下步骤进行操作：

1. 开启沙箱防护功能。
2. 定义沙箱防护Profile，在Profile中指定域名白名单，配置可疑文件识别标准。
3. 绑定沙箱防护Profile到策略规则。

其中，沙箱防护Profile用于指定是否启用域名白名单，配置可疑文件识别标准。域名白名单中包含安全域名，当文件的来源是域名白名单中的域名时，此文件被认为是合法文件，不会被上传到云沙箱进行检测。可疑文件识别标准是指将符合标准的文件判断为可疑文件，并上传到云沙箱进行检测。可疑文件的检查结果决定文件是合法文件或是恶意文件。

用户可使用系统默认的沙箱防护规则，也可自行创建规则。系统提供3个默认的沙箱防护规则predef_low、predef_middle和predef_high：

- **predef_low** -- 宽松的沙箱检测策略。此规则开启域名白名单、可信证书验证，扫描HTTP/FTP/POP3/SMTP/IMAP4协议流量，将PE类型文件作为检测对象。
- **predef_middle** -- 中等的沙箱检测策略。此规则开启域名白名单、可信证书验证，扫描HTTP/FTP/POP3/SMTP/IMAP4协议流量，将PE、APK、JAR、MS-Office、PDF文件作为检测对象。

- **predef_high** -- 严格的沙箱检测策略。此规则扫描HTTP/FTP/POP3/SMTP/IMAP4协议流量，将所有文件类型（PE、APK、JAR、MS-Office、PDF、SWF、RAR以及ZIP）作为检测对象。

创建沙箱防护Profile

沙箱防护Profile用于指定域名白名单，配置可疑文件识别标准。创建沙箱防护Profile，在全局配置模式下使用以下命令：

sandbox-profile *sandbox-profile-name*

- *sandbox-profile-name* - 指定所创建的沙箱防护Profile的名称，并且进入该沙箱防护Profile的配置模式。如果指定名称已存在，则直接进入沙箱防护Profile配置模式。

使用**no sandbox-profile** *sandbox-profile-name*删除指定的沙箱防护Profile。

开启域名白名单

域名白名单中预定义安全域名，当文件的来源是域名白名单中的域名时，此文件被认为是合法文件，不会被上传到云沙箱进行检测。

开启域名白名单，在沙箱防护Profile配置模式下，使用如下命令：

whitelist enable

使用**no whitelist enable**命令关闭域名白名单功能。

可信证书验证

系统支持对PE文件进行可信证书验证，即如文件的签名证书是可信的，系统将不对其进行检测。

开启可信证书验证，在沙箱防护Profile配置模式下，使用如下命令：

certificate-validation enable

使用**no certificate-validation enable**命令关闭可信证书验证功能。

指定可疑文件识别标准

将符合标准的文件判断为可疑文件，并上传到云沙箱进行检测。可疑文件的检查结果决定文件是合法文件或是非法文件。

用户可设置如下识别标准：

将指定类型的文件识别为可疑文件。支持识别PE（.exe）、APK、JAR、MS-Office、PDF、SWF、RAR以及ZIP文件为可疑文件。在沙箱防护Profile配置模式下，使用如下命令指定类型：

file-type {**pe** | **apk** | **jar** | **swf** | **ms-office** | **pdf** | **rar** | **zip**} **max-file-size** *size*

- **pe** - 将PE（.exe）文件作为检测对象。
- **apk** - 将Android安装文件作为检测对象
- **jar** - 将Java文件作为检测对象。
- **swf** - 将Flash文件作为检测对象。
- **ms-office** - 将Windows Office文件识别为可疑文件。
- **pdf** - 将PDF文件作为检测对象。
- **rar** | **zip** - 将压缩文件作为检测对象。
- **max-file-size** *size* - 指定文件大小。系统将小于指定大小的文件作为检测对象。

取消指定类型，使用**no file-type** {**pe** | **apk** | **jar** | **swf** | **ms-office** | **pdf** | **rar** | **zip**}命令。不指定类型表示沙箱防护功能不将任何文件识别为可疑文件。

扫描指定类型的协议报文并指定该协议可疑流方向。支持扫描HTTP、FTP、POP3、SMTP及IMAP4协议报文。在沙箱防护Profile配置模式下，使用如下命令指定协议类型：

protocol {**http** | **ftp** | **imap4** | **pop3** | **smtp**} **direction** {**download** | **upload** | **both**}

- **http** | **ftp** | **imap4** | **pop3** | **smtp** - 指定协议类型。
- **download** | **upload** | **both** - 指定该协议可疑流方向，包含上传**upload**、下载**download**、双向**both**。

不指定协议类型，使用**no protocol** {**http** | **ftp** | **imap4** | **pop3** | **smtp**}命令。不指定协议类型表示沙箱防护功能不扫描任何协议的报文。

上述各个标准的逻辑关系为或。

指定对恶意文件的处理动作

当系统判断可疑文件为恶意后，将按指定的动作处理恶意文件。指定系统处理动作，在沙箱防护Profile配置模式下，使用以下命令：

action {**reset** | **log-only**}

- **reset** - 指定该参数后，系统发现恶意文件后，重置恶意链接连接，并记录威胁日志和云沙箱日志。
- **log-only** – 指定该参数后，系统发现恶意文件后，对流量放行，仅记录日志信息（威胁日志和云沙箱日志）。

禁用可疑文件上传

系统在认定文件为可疑文件后，会默认上传该文件到云沙箱进行检测。由于部分可疑文件包含用户敏感信息，用户可以禁用可疑文件上传，即该可疑文件将不会被上传到云沙箱。在沙箱防护Profile配置模式下，使用以下命令：

file-upload-disable

使用**no file-upload-disable**命令取消禁用可疑文件上传，即恢复默认上传可疑文件功能。

绑定沙箱防护Profile到策略规则

将沙箱防护Profile绑定到策略规则后，系统将会对与策略规则相匹配的流量根据沙箱防护Profile配置进行沙箱防护检查。绑定沙箱防护Profile到策略规则，在策略规则配置模式下使用以下命令：

sandbox {*sandbox-profile-name* | **predef_low** | **predef_middle** | **predef_high**}

- *sandbox-profile-name* – 指定绑定到策略规则的沙箱防护Profile的名称。
- **predef_low** – 绑定名为**predef_low**的预定义沙箱防护Profile到策略规则。
- **predef_middle** – 绑定名为**predef_middle**的预定义沙箱防护Profile到策略规则。
- **predef_high** – 绑定名为**predef_high**的预定义沙箱防护Profile到策略规则。

在策略规则配置模式下使用该命令no的形式取消沙箱防护Profile的绑定：**no sandbox**

开启良性文件上报

开启良性文件上报，系统在认定文件为良性文件时，即上报该文件相关的沙箱日志。默认情况下，系统不对良性文件结果记录日志。开启良性文件上报，在全局配置模式下，使用以下命令：

```
sandbox benign-file report enable
```

使用**no sandbox benign-file report enable**关闭良性文件上报。

开启灰文件上报

灰文件指无法断定其是良性文件或恶意文件的所有其他文件。开启灰文件上报，系统在认定文件为灰文件时，将上报该文件相关的沙箱日志。默认情况下，系统不对灰文件结果记录日志。开启灰文件上报，在全局配置模式下，使用以下命令：

```
sandbox greyware report enable
```

使用**no sandbox greyware report enable**关闭灰文件上报。

添加威胁条目到信任列表

设备收集可疑流量上传至云端。当云端确认其为恶意文件后，可向设备列表中的其他设备同步推送沙箱威胁列表。当有新设备开启沙箱防护功能并注册到云端时，云端即会向其推送该威胁列表。当设备获取到威胁列表后，可按已配置的动作对威胁列表中的威胁进行阻断。

用户可将威胁条目，加入到信任列表中。信任列表中的条目一旦被匹配，对应的流量将被无条件放行，不受沙箱防护规则中动作的控制。

在任何模式下，使用以下命令在信任列表中添加或移除威胁条目：

```
exec sandbox-threat value {trust | untrust}
```

- *value* – 指定威胁条目的MD5的值。
- **trust** – 将指定的威胁条目加入到信任列表。
- **untrust** – 将指定的威胁条目从信任列表中移除。

显示沙箱防护信息

在任何模式下，输入以下命令显示沙箱防护profile信息：

show sandbox-profile [*sandbox-profile-name*]

在任何模式下，输入以下命令显示沙箱防护状态信息和上传统计信息：

show sandbox status

在任何模式下，输入以下命令显示沙箱威胁列表的威胁条目信息：

show sandbox threat-entry info

配置域名白名单更新

默认情况下，系统会每日自动更新域名白名单，用户可以根据需要更改更新配置。域名白名单更新配置包括：

- 配置域名白名单更新模式
- 配置更新服务器
- 指定HTTP代理服务器
- 指定更新时间
- 立即更新
- 导入域名白名单文件
- 显示域名白名单信息
- 显示域名白名单更新配置信息

配置域名白名单更新模式

系统支持手动和自动两种更新方式。配置域名白名单更新方式，在全局配置模式下，使用以下命令：

sandbox whitelist update mode {**auto** | **manual**}

- **auto** – 指定自动更新域名白名单。该方式为系统的默认更新方式。
- **manual** – 指定手动更新域名白名单。

在全局配置模式下使用该命令no的形式恢复默认更新模式：

no sandbox whitelist update mode

配置更新服务器

系统提供默认的域名白名单更新服务器，即update1.hillstonenet.com和update2.hillstonenet.com，同时用户也可以根据需要配置其它更新服务器下载最新域名白名单。最多可配置3个。配置更新服务器，在全局配置模式下，使用以下命令：

sandbox whitelist update {**server1** | **server2** | **server3**} {*ip-address* | *domain-name*}

- **server1** | **server2** | **server3** – 指定将要配置的服务器。**server1**的默认值为update1.hillstonenet.com，**server2**的默认值为update2.hillstonenet.com。
- *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）。

在全局配置模式下，使用该命令no的形式取消更新服务器的指定：

no sandbox whitelist update {**server1** | **server2** | **server3**}

指定HTTP代理服务器

当设备需要通过HTTP代理服务器访问互联网时，为确保特征库能够正常升级，需要在设备上指定代理服务器的IP地址和端口号。

为域名白名单升级指定代理服务器，在全局配置模式下，使用如下命令：

sandbox whitelist update proxy-server {**main** | **backup**} *ip-address port-number*

- **main** | **backup** – 使用main参数指定主代理服务器，使用backup指定备份代理服务器。
- *ip-address port-number* – 指定代理服务器的IP地址和端口号。

取消指定的代理服务器，使用**no sandbox whitelist update proxy-server** {**main** | **backup**}命令。

指定更新时间

默认情况下，系统采用自动模式每日更新域名白名单，并且为避免服务器流量过大，每日更新时间是随机的。用户可以根据需要指定域名白名单更新的频率和时间，在全局配置模式下，使用以下命令：

sandbox whitelist update schedule {**daily** | **weekly** {**mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun**}} [*HH:MM*]

- **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。

立即更新

无论更新模式为手动还是自动，用户都可以随时使用以下命令更新域名白名单。立即更新域名白名单，在任何模式下，使用以下命令：

exec sandbox whitelist update

- **exec sandbox whitelist update** – 仅对当前域名白名单与更新服务器最新发布域名白名单的不同部分进行更新。

导入域名白名单文件

在某些情况下，用户设备可能无法连接到更新服务器对域名白名单进行更新，针对这一问题，系统提供域名白名单文件导入功能，即通过FTP、TFTP服务器或者U盘将域名白名单文件导入到设备，从而更新设备的域名白名单。导入域名白名单文件，在执行模式下，使用以下命令：

import sandbox whitelist from {**ftp server** *ip-address* [**user** *user-name* **password** *password*] | **tftp server** *ip-address* } [**vrouter** *vr-name*] *file-name*

- *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。
- **vrouter** *vr-name* – 指定FTP或者TFTP服务器所属的VRouter。
- *file-name* – 指定导入的域名白名单文件的名称。

显示域名白名单信息

用户可以随时使用相应的show命令查看设备的域名白名单信息，包括域名白名单版本以及发布日期。查看域名白名单信息，在任何模式下使用以下命令：

```
show sandbox whitelist info
```

显示域名白名单更新配置信息

用户可以随时使用相应的show命令查看设备上的域名白名单更新信息，包括更新服务器信息、更新模式、更新频率及时间以及域名白名单更新状况等。查看域名白名单更新配置信息，在任何模式下使用以下命令：

```
show sandbox whitelist update
```

入侵防御系统

入侵防御系统（Intrusion Prevention System）简称IPS，能够实时监控多种网络攻击并根据配置对网络攻击进行阻断等操作。系统支持许可证控制的IPS功能，即为支持IPS功能的系统安装入侵防御（IPS）许可证或威胁防护（TP）许可证后，IPS功能才可使用。

系统的IPS功能能够实现完整的基于状态的检查，从而极大降低误报率。当设备开启多项应用层数据检测功能时，启用IPS功能不会导致设备性能的明显下降。另外，系统每天通过特征服务器自动更新特征库，保证特征的完整性和正确性。

IPS检测及报告流程

系统的IPS功能对协议的检测流程包括两部分，分别是协议解析和特征匹配。

- 协议解析：对流量所在协议进行分析，发现流量不符合协议的规定后，系统会根据配置处理流量（记录日志、重置、阻断），并产生日志信息报告给管理员，系统生成的威胁日志信息详情中包含"威胁ID“，即为协议异常的特征ID，用户可以通过查看威胁日志查看详细信息；

- 特征匹配：提取流量的元素，对其进行特征匹配，发现其与特征库中特征相匹配后，系统会根据配置处理流量（记录日志、重置、阻断），并产生日志信息报告给管理员。系统生成的威胁日志信息详情中包含"威胁ID“，即为特征库中的特征ID，用户可以根据该ID查看错误的具体信息。

特征介绍

特征ID作为特征的唯一标识， 根据协议进行分类。特征ID由两部分构成，分别为协议ID（第1位或者第1和第2位）和攻击特征ID（后5位），例如ID“605001”中，“6”表示Telnet协议，“05001”表示攻击特征ID。攻击特征ID的第1位是“6”的为协议异常特征，其余为攻击特征。协议ID与协议的对应关系下表所示：

协议ID	协议	协议ID	协议	协议ID	协议	协议ID	协议
1	DNS	7	Other-TCP	13	TFTP	19	NetBIOS
2	FTP	8	Other-UDP	14	SNMP	20	DHCP
3	HTTP	9	IMAP	15	MySQL	21	LDAP

协议ID	协议	协议ID	协议	协议ID	协议	协议ID	协议
4	POP3	10	Finger	16	MSSQL	22	VoIP
5	SMTP	11	SUNRPC	17	Oracle	-	-
6	Telnet	12	NNTP	18	MSRPC	-	-

上表中，“Other-TCP”表示除表中已列出的标准TCP协议以外的其他TCP协议；“Other-UDP”表示除表中已列出的标准UDP协议以外的其他UDP协议。

特征库更新

默认情况下，系统会每日自动更新IPS特征库，用户可以根据需要更改IPS特征库更新配置。Hillstone山石网科提供两个默认特征库更新服务器，分别是update1.hillstonenet.com和update2.hillstonenet.com。系统支持在线更新和本地更新两种方式供用户进行选择。需要注意的是，非根VSYS不支持特征库更新。特征库更新配置，请参阅下表：

配置	CLI
配置更新模式，默认为自动	全局配置模式下使用以上命令： • 指定方式：**ips signature update mode {auto | manual}** • 恢复默认：**no ips signature update mode**
配置更新服务器	全局配置模式下使用以下命令： • 指定服务器：**ips signature update** {**server1** | **server2** | **server3**} {*ip-address* | *domain-name*} • 取消服务器的指定：**no ips signature update** {**server1** | **server2** | **server3**}
指定更新时间	全局配置模式下使用以下命令，启用每日或每周更新，并指定更新的时间： **ips signature update schedule** {**daily** | **weekly** {**mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun**}}

配置	CLI
	[*HH:MM*] 全局配置模式下使用以下命令，启用每小时更新，并指定更新的时间： **ips signature update schedule hourly** *minute* • *minute* – 指定更新的时间，即，在每小时的第多少分钟进行更新。
立即更新	执行模式下使用以下命令： **exec ips signature update**
本地更新	执行模式下使用以下命令： **import ips signature from** {**ftp server** *ip-address* [**user** *user-name* **password** *password* | **vrouter** *vr-name*] | **tftp server** *ip-address* [**vrouter** *vr-name*]} *file-name*
显示特征库统计信息	**show ips signature info**
显示特征库配置信息	**show ips signature update**

指定HTTP代理服务器

当设备需要通过HTTP代理服务器访问互联网时，为确保特征库能够正常升级，需要在设备上指定代理服务器的IP地址和端口号。

为入侵防御特征库升级指定代理服务器，在全局配置模式下，使用如下命令：

ips signature update proxy-server {**main** | **backup**} *ip-address port-number*

- **main** | **backup** – 使用main参数指定主代理服务器，使用**backup**指定备份代理服务器。
- *ip-address port-number* – 指定代理服务器的IP地址和端口号。

取消指定的代理服务器，使用**no ips signature update proxy-server {main | backup}**命令。

IPS工作模式

系统支持两种IPS工作模式，分别是只记录日志模式和IPS模式。只记录日志模式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；IPS模式在提供协议异常和网络攻击行为的日志功能的同时，还对检出攻击做重置和阻断操作。系统默认情况下工作在IPS模式下。

切换IPS工作模式，在全局配置模式下，**ips mode {ips-logonly | ips}**命令。

配置入侵防御

IPS配置准备工作

使用IPS功能前，必须完成以下准备工作：

1. 确认StoneOS版本支持IPS功能。
2. 安装入侵防御（IPS）许可证或威胁防护（TP）许可证，然后重启设备。设备成功重启后，IPS功能即处于开启状态。

IPS功能配置包含以下配置内容：

- 特征集配置：提取流量的元素，对其进行特征匹配，发现其与特征集中指定的特征相匹配后，系统会根据配置处理流量（记录日志、重置、阻断）。
- 协议配置：对流量所在协议进行分析，发现流量不符合协议的规定后，系统会根据配置处理流量（记录日志、重置、阻断）。
- IPS Profile：包含特征集配置、协议配置、以及抓包三部分的配置。将IPS Profile绑定到安全域的不同方向（出方向、入方向、双向），可将IPS功能应用到安全域不同方向的流量。将IPS Profile绑定到策略规则上，可将IPS功能应用到与策略规则相匹配的流量。

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。

为系统配置IPS功能后，当系统发现入侵攻击，会生成相应的威胁日志信息。威胁日志信息中包含检测出的攻击特征ID。查看威胁日志信息，可以通过运行show logging threat命令。

配置指导说明

在IPS配置中，多处配置都会对最终的攻击处理行为产生影响，因此，系统在决定处理行为时遵循以下原则：

- IPS工作模式具有最高优先级。当系统的IPS工作模式指定为只记录日志模式时，无论其他相关配置是否指定动作，最终的结果均为仅记录日志。
- 用户创建多个特征集规则且这些特征集规则中包含同一个特征时，如果不同特征集规则指定的行为不一致，那么，当发现某个攻击的特征符合多个特征集规则中的同一个特征时：
  - 总是采取更严格的行为对攻击进行处理。哪个特征集规则设置的行为更严格，则使用哪个特征集规则设置的行为对攻击进行处理。严格程度：阻断IP > 阻断服务 > 只记录日志。对于阻断IP和阻断服务，如果在一个特征集规则中的配置为阻断IP15s，另外一个特征集规则中的配置为阻断服务30s，则，采取的行为时阻断IP30s。
  - 只要一个特征集规则中配置了抓包，就会对异常数据包进行抓包。
  - 通过检索条件创建的特征集规则所配置的行为，优先级高于通过特征条件创建的特征集规则所配置的行为。
- 对于已绑定到安全域或者已绑定到策略规则的IPS Profile，用户可以修改IPS Profile的配置。在对IPS Profile进行修改时，系统对相关会话的处理遵循以下原则：
  - 当IPS Profile的引用关系发生变化时，该变化对于已经建立的会话不能立即生效，即当将绑定到安全域trust的IPS Profile由IPS-pro1变为IPS-pro2后，已经建立的会话仍使用IPS-pro1，只有新建立的会话使用IPS-pro2。更改IPS Profile引用关系后，执行clear session命令可使配置对已有会话立即生效。
  - 修改已被引用的IPS Profile中的特征集，变化将对已有会话立即生效。

对HTTPS流量进行IPS检测

如果需要IPS对HTTPS流量进行扫描，需要为HTTPS流量所匹配的策略规则配置SSL代理功能。系统将为匹配此条策略的HTTPS流量根据SSL代理Profile解密HTTPS流量，对解密后的数据根据IPS Profile进行IPS检测。根据安全策略规则的配置不同，系统将进行如下操作：

安全策略规则配置	操作
启用SSL代理 不启用IPS	根据SSL代理Profile解密HTTPS流量，对解密后的数据不进行IPS检测。
启用SSL代理 启用IPS	根据SSL代理Profile解密HTTPS流量，对解密后的数据根据IPS Profile进行IPS检测。
不启用SSL代理 启用IPS	对HTTP流量根据IPS Profile进行IPS检测。对HTTPS流量不进行解密，不进行IPS检测，只进行转发。

当安全策略规则所关联的安全域也启用IPS时，系统也将进行如下操作：

安全策略规则配置	安全域配置	操作
启用SSL代理 不启用IPS	启用IPS	根据SSL代理Profile解密HTTPS流量，对解密后的数据根据安全域配置的IPS Profile进行IPS检测。
启用SSL代理 启用IPS	启用IPS	根据SSL代理Profile解密HTTPS流量，对解密后的数据根据安全策略规则中配置的IPS Profile进行IPS检测。
不启用SSL代理 启用IPS	启用IPS	对HTTP流量根据安全策略规则中配置的IPS Profile进行IPS检测。对HTTPS流量不进行解密，不进行IPS检测，只进行转发。

提示: 更多关于SSL代理Profile的配置，请参阅SSL代理章节。

IPS命令

action

对于过滤规则和搜索规则筛选出的特征，当流量命中特征时，指定相应的处理动作。

[命令]

action {block-service *timeout*| **block-ip** *timeout* | **log-only** | **reset**}

[句法描述]

action {**block-service** *timeout*| **block-ip** *timeout* | **log-only** | **reset**}
- **block-service**指定阻断攻击者服务,**block-ip**指定阻断攻击者服务IP，*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。**log-only**匹配该特征后仅记录日志信息。**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。

[默认取值]

log-only。

[命令模式]

过滤规则配置模式;

搜索规则配置模式。

[使用指导]

无。

[命令实例]

```
hostname(config)# ips profile test
hostname(config-ips-profile)# filter-class 1
hostname(config-ips-filter-class)# action log-only
```

affected-software

通过过滤规则筛选特征时，可配置affected-software参数，筛选出指定软件相关的特征。

[命令]

affected-software {**Apache** | **IE** | **Firefox** | …}

no affected-software {**Apache** | **IE** | **Firefox** | …}

[句法描述]

Apache | **IE** | **Firefox** | … – 指定软件名称。用户可通过在**affected-software**参数后使用Tab键，查看完整的软件列表。

[默认取值]

无。

[命令模式]

过滤规则配置模式。

[使用指导]

无。

[命令实例]

```
hostname(config)# ips profile test
hostname(config-ips-profile)# filter-class 1
hostname(config-ips-filter-class)# affected-software Apache
```

attack-type

通过过滤规则筛选特征时，可配置attack-type参数，筛选出指定攻击类型的特征。

[命令]

attack-type {**Access-Control** | **SPAM** | **Mail** | …}

no attack-type {**Access-Control** | **SPAM** | **Mail** | …}

[句法描述]

Access-Control | SPAM | Mail | … - 指定攻击类型。用户可通过在**attack-type**参数后使用Tab键，查看完整的攻击类型列表。

[默认取值]

无。

[命令模式]

过滤规则配置模式。

[使用指导]

无。

[命令实例]

```
hostname(config)# ips profile test
```

```
hostname(config-ips-profile)# filter-class 1
hostname(config-ips-filter-class)# attack-type WEB-PHP
```

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]

协议配置模式。

[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 vsft-p2.0
```

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]

协议配置模式。

[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]

协议配置模式。

[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
```

bulletin-board

通过过滤规则筛选特征时，可配置bulletin-board参数，筛选出指定组织发布的特征。

[命令]

bulletin-board {**CVE** | **BID** | **OSVDB** | …}

no bulletin-board {**CVE** | **BID** | **OSVDB** | …}

[句法描述]

CVE | **BID** | **OSVDB** | … 指定发布漏洞的组织名称。用户可通过在**bulletin-board**参数后使用Tab键，查看完整的组织列表。

[默认取值]

无。

[命令模式]

过滤规则配置模式。

[使用指导]

无。

[命令实例]

```
hostname(config)# ips profile test
hostname(config-ips-profile)# filter-class 1
hostname(config-ips-filter-class)# bulletin-board CVE
```

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]

协议配置模式。

[使用指导]

无。

[命令实例]

```
hostname(config)# ips sigset http1 template http
hostname(config-http-sigset)# command-injection-check enable
```

cc-url

为CC URL限制功能配置URL路径。配置后，系统将对访问该路径的HTTP请求进行访问频率进行统计。若访问频率超过阈值，系统将阻断该请求的源IP,该IP将无法访问Web服务器。用该命令no的形式删除该高频URL路径设置。

[命令]

cc-url *url_string*

no cc-url *url_string*

[句法描述]

url_string - 指定CC URL限制功能的URL路径。指定后，包含该路径名称的所有路径也将被统计。系统会对访问这些路径的HTTP请求进行访问频率检查。若HTTP请求的访问频率超过阈值，会阻断该请求的源IP，该IP将无法访问Web服务器。例如：配置/home/ab，系统将对访问/home/-ab/login与/home/abc/login的HTTP请求进行频率检查。URL路径不支持带主机名或域名的路径格式，例如：不能配置www.baidu.com/home/login.html，应该配置/home/login.html，而www.baidu.com应该配置在对应的Web服务器的域名设置里。系统最多允许配置32条URL路径，每条路径长度取值范围为1-255字符。

[默认取值]

无。

[命令模式]

Web服务器配置模式。

[使用指导]

无。

[命令实例]

```
hostname(config)# ips sigset test_http template http
hostname(config-http-sigset)# web-server web_server1
hostname(config-web-server)# domain www.abc.com
hostname(config-web-server)# cc-url /home/login.php
```

cc-url-limit

为CC URL限制功能配置URL路径的被访问次数的阈值及阻断IP的时间。配置后，系统将统计URL路径被访问的频率，若访问频率超过阈值，系统将阻断该请求的源IP，该IP将无法访问Web服务器。超过阻断时间后，系统将释放阻断的IP，该IP可以重新访问Web服务器。使用该命令no的形式恢复默认值。

[命令]

cc-url-limit threshold *value* **action block-ip** *block-ip_time*

no cc-url-limit

[句法描述]

value 指定单个源IP每分钟访问URL路径的最大次数。当某源IP的访问的频率超过此阈值，系统将会对此IP进行阻断。其取值范围为1-65535次/分钟。

block-ip_time 指定阻断IP的时间，默认是60秒，取值范围为60-3600秒。超过此时间，系统将释放阻断的IP，此IP可以重新访问Web服务器。

[默认取值]

value – 1次/分钟；

block-ip_time – 60秒；

[命令模式]

Web服务器配置模式。

[使用指导]

无。

[命令实例]

```
hostname(config)# ips sigset test_http template http
hostname(config-http-sigset)# web-server web_server1
hostname(config-web-server)# domain www.abc.com
hostname(config-web-server)# cc-url /home/login.php
hostname(config-web-server)# cc-url-limit threshold 1500 action block-ip 100
```

deny-method

指定系统拒绝的HTTP方法。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]

协议配置模式。

[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
```

domain

为Web服务器配置域名。使用该命令no的形式删除Web服务器域名设置。

[命令]

domain *domain_name*

no domain *domain_name*

[句法描述]

domain_name 指定Web服务器域名，为1到255个字符长度的字符串。

[默认取值]

无。

[命令模式]

Web服务器配置模式。

[使用指导]

无法为默认Web服务器指定域名。

每个Web服务器最多允许配置5个域名。

Web服务器域名遵循从后往前的最长匹配原则。例如，进行以下配置：

```
hostname(config-http-sigset)# web-server web_server1
hostname(config-web-server)# domain abc.com
hostname(config-web-server)# exit
hostname(config-http-sigset)# web-server web_server2
hostname(config-web-server)# domain email.abc.com
```

完成上述配置后，访问news.abc.com的流量将匹配web_server1；访问www.email.abc.com的流量将匹配web_server2；访问www.abc.com.cn的流量将匹配默认Web服务器。

[命令实例]

```
hostname(config)# ips sigset test_http template http
hostname(config-http-sigset)# web-server web_server1
hostname(config-web-server)# domain www.abc.com
```

dst-ip

配置IPS白名单的目的IP地址。使用该命令no的形式删除目的IP地址的配置。

[命令]

dst-ip *A.B.C.D*|*A.B.C.D/M*

no dst-ip

[句法描述]

A.B.C.D|*A.B.C.D/M* 指定IPS白名单需匹配的目的地址IP地址。

[默认取值]

无。

[命令模式]

IPS白名单配置模式。

[使用指导]

无。

[命令实例]

```
hostname(config)# ips whitelist white1
hostname(config-ips-whitelist)# dst-ip 10.1.1.2
```

enable

启用Web服务器。使用该命令no的形式禁用Web服务器。

[命令]

enable

no enable

[句法描述]

无。

[默认取值]

开启。

[命令模式]

Web服务器配置模式。

[使用指导]

默认Web服务器缺省为开启状态，且不能被禁用。

[命令实例]

```
hostname(config)# ips sigset test_http template http
hostname(config-http-sigset)# web-server web_server1
hostname(config-web-server)# enable
```

exec block-ip add

增加一个被阻断的IP地址。

[命令]

exec block-ip add {**ip** *ipv4-address* |**ipv6** *ipv6-address*} [**vrouter** *vr-name*] **timeout** *timeout*

[句法描述]

ip *ipv4-address* | **ipv6** *ipv6-address* - 指定被阻断的IP地址。

timeout *timeout* - 指定对攻击者IP进行阻断的时长，单位为秒，范围是60到3600秒。超过时长后，系统会自动从被阻断IP列表中删除此IP。

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]

非根VSYS不支持此命令。

[命令实例]

```
hostname# exec block-ip add ipv4 100.10.10.1 timeout 60
```

exec block-ip remove

从阻断IP地址表中删除被阻断的IP，即不对该IP进行阻断。

[命令]

exec block-ip remove {**all** | **ipv4** *ipv4-address* |**ipv6** *ipv6-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。

ipv4 *ipv4-address*|**ipv6** *ipv6-address* - 删除指定IP地址。

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]

非根VSYS不支持此命令。

[命令实例]

```
hostname# exec block-ip remove ipv4 100.10.10.1
```

exec block-service add

增加一个被阻断的服务条目。

[命令]

exec block-service add {**src-ipv4** *src-ipv4-address* **dst-ipv4** *dst-ipv4-address*|**src-ipv6** *src-ipv6-address* **dst-ipv6** *dst-ipv6-address*} [**vrouter** *vr-name*] **dst-port** *port-number* **proto** *protocol*

[句法描述]

src-ipv4 *src-ipv4-address* **dst- ipv4** *dst- ipv4-address*- 指定服务的源IPv4地址和目的地址。

src-ipv6 *src-ipv6-address* **dst-ipv6** *dst-ipv6-address* - 指定服务的源IPv6地址和目的地址。

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]

非根VSYS不支持此命令。

[命令实例]

```
hostname# exec block-service add src-ipv4 100.10.10.1 dst-ipv4
100.20.10.4 dst-port 1025 proto 23
```

exec block-service remove

删除被阻断的服务条目，即不对满足该条件的服务进行阻断。

[命令]

exec block-service remove {**all** | {**src-ipv4** *src-ipv4-address* **dst-ipv4** *dst-ipv4-address*|**src-ipv6** *src-ipv6-address* **dst-ipv6** *dst-ipv6-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的服务条目。

src-ipv4 *src-ipv4-address* **dst- ipv4** *dst- ipv4-address* - 指定服务的源IPv4地址和目的地址。

src-ipv6 *src-ipv6-address* **dst-ipv6** *dst-ipv6-address* - 指定服务的源IPv6地址和目的地址。

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]

非根VSYS不支持此命令。

[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。
- 非根VSYS不支持此命令。

[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://”、“https://”或者“ftp://”），例如，http://www.abc.com/script，表示该路径下所有文件都可以被Web服务器引用（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]

Web服务器配置模式。

[使用指导]

每个Web服务器最多配置32个外链URL。

[命令实例]

```
hostname(config)# ips sigset http1 template http
hostname(config-http-sigset)# web-server www.abc.com
```

```
hostname(config-web-server)# 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Web服务器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]

Web服务器配置模式。

[使用指导]

无。

[命令实例]

```
hostname(config)# ips sigset http1 template http
hostname(config-http-sigset)# web-server www.abc.com
hostname(config-http-web-server)# external-link-check enable action
reset
```

filter-class

进行特征集配置时，可通过过滤条件筛选出特定的特征。使用如下命令创建过滤规则并进入过滤规则配置模式。使用该命令no的形式删除过滤规则。

[命令]

filter-class id [**name** *name*]

no filter-class id

[句法描述]

id - 指定过滤规则的ID。

name *name* - 指定过滤规则的名称。

[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 test
hostname(config-http-sigset)# filter-class 1 name test2
```

http-request-flood auth

为CC防护功能配置认证方法。系统通过认证判断HTTP请求的源IP是否合法，从而识别攻击流量并进行防护。如果某个源IP认证失败，系统将阻断该源IP发起的本次HTTP请求。使用该命令no的形式取消认证方法配置。

[命令]

http-request-flood auth {**auto-js-cookie** | **auto-redirect** | **manual-CAPTCHA** | **manual-confirm**} [**crawlers-friendly**]

no http-request-flood auth

[句法描述]

auto-js-cookie | **auto-redirect** | **manual-CAPTCHA** | **manual-confirm**

指定认证方法：

- **auto-js-cookie**：自动（JS Cookie）。该认证方法由浏览器自动完成认证交互。
- **auto-redirect**：自动（重定向）。该认证方法由浏览器自动完成认证交互。
- **manual-CAPTCHA**：手动（访问确认）。该认证方法需要HTTP请求发起者点击返回提示框上的“确认”按钮进行认证。
- **manual-confirm**：手动（验证码）。该认证方法需要请求发起者输入验证码进行认证。

crawlers-friendly -指定不对爬虫进行认证。

[默认取值]

无。

[命令模式]

Web服务器配置模式。

[使用指导]

无。

[命令实例]

```
hostname(config)# ips sigset http1 template http
hostname(config-http-sigset)# web-server web_server1
hostname(config-web-server)# http-request-flood auth auto-js-cookie
```

http-request-flood enable

为系统开启HTTP协议CC防护功能并设置开启该功能的请求阈值。当HTTP连接请求速率达到设定阈值时，即判断为发生CC攻击，并启动CC防护功能。使用该命令no的形式关闭HTTP协议CC防护功能。

[命令]

http-request-flood enable [**threshold request** *value*]

no http-request-flood enable

[句法描述]

threshold request value 指定开启HTTP协议CC防护功能的请求阈值。取值范围为0到1000000次/秒。

[默认取值]

请求阈值：1500次/秒。

[命令模式]

Web服务器配置模式。

[使用指导]

无。

[命令实例]

```
hostname(config)# ips sigset http1 template http
hostname(config-http-sigset)# web-server web_server1
hostname(config-web-server)# http-request-flood enable
```

http-request-flood proxy-limit

为CC防护功能配置代理限速。配置代理限速后，系统会检查每个源IP是否属于代理服务器，若属于，则根据配置进行请求速率限制。使用该命令no的形式取消代理限速配置。

[命令]

http-request-flood proxy-limit threshold *value* {**blockip timeout** *value* | **reset**} [**nolog**]

no http-request-flood proxy-limit

[句法描述]

threshold *value* - 指定请求速率阈值。如果收到的请求速率超过该指定值且CC防护功能已开启，系统会对超出的请求数做相应的限制操作。取值范围为0到1000000次/秒。

blockip timeout *value* | **reset** - 指定系统对超出请求速率阈值的请求数的限制操作：

- **blockip timeout** *value*：对超出的请求数的源IP进行阻断，并指定阻断时长，单位为秒，范围是60到3600秒。
- **reset**：重置超出的请求数的请求连接。

nolog - 指定不记录日志信息。

[默认取值]

无。

[命令模式]

Web服务器配置模式。

[使用指导]

无。

[命令实例]

```
hostname(config)# ips sigset http1 template http
hostname(config-http-sigset)# web-server web_server1
hostname(config-web-server)# http-request-flood proxy-limit threshold 10000 reset nolog
```

http-request-flood request-limit

为CC防护功能配置访问限速。配置访问限速后，系统会根据配置对每个源IP进行请求速率限制。使用该命令no的形式取消访问限速配置。

[命令]

http-request-flood request-limit threshold *value* {**blockip timeout** *value* | **reset**} [**nolog**]

no http-request-flood request-limit

[句法描述]

threshold *value* - 指定访问速率阈值。如果收到的请求速率超过该指定值且CC防护功能已开启，系统会对超出的请求数做相应的限制操作。取值范围为0到1000000次/秒。

blockip timeout *value* | **reset** - 指定系统对超出请求速率阈值的请求数的限制操作：

- **blockip timeout** *value*：对攻超出的请求数的源IP进行阻断，并指定阻断时长，单位为秒，范围是60到3600秒。
- **reset**：重置超出的请求数的请求连接。

nolog - 指定不记录日志信息。

[默认取值]

无。

[命令模式]

Web服务器配置模式。

[使用指导]

无。

[命令实例]

```
hostname(config)# ips sigset http1 template http
hostname(config-http-sigset)# web-server web_server1
hostname(config-web-server)# http-request-flood request-limit threshold
10000 blockip timeout 60
```

http-request-flood statistics

开启URL请求统计功能。使用该命令no的形式关闭URL请求统计功能。

[命令]

http-request-flood statistics enable

no http-request-flood statistics enable

[句法描述]

无。

[默认取值]

关闭。

[命令模式]

Web服务器配置模式。

[使用指导]

执行**http-request-flood statistics enable**命令后，**show ips sigset** *sigset-name* **web-server** *server-name* **http-request-flood req-stat top**命令才会生效。

[命令实例]

```
hostname(config)# ips sigset http1 template http
```

```
hostname(config-http-sigset)# web-server web_server1
hostname(config-web-server)# http-request-flood statistics enable
```

http-request-flood white-list

为CC防护功能配置白名单。添加到白名单中的源IP地址不做CC防护检查。使用该命令no的形式取消CC防护白名单配置。

[命令]

http-request-flood white-list *address_entry*

no http-request-flood white-list

[句法描述]

address_entry 指定不做CC防护检查的地址条目。

[默认取值]

无。

[命令模式]

Web服务器配置模式。

[使用指导]

地址条目不能为域名和IPv6地址；

如果白名单中源IP地址的流量超出CC防护请求阈值（**http-request-flood enable** [**threshold request** *value*]），则会触发CC防护功能的开启。

[命令实例]

```
hostname(config)# ips sigset http1 template http
hostname(config-http-sigset)# web-server web_server1
hostname(config-web-server)# http-request-flood white-list addr1
```

http-request-flood x-forward-for

为CC防护功能配置HTTP请求的x-forward-for字段的取值。配置后，系统会按照该字段统计其访问频率，当某设定的完整URL的被访问频率超过阈值且持续20s时，系统判定CC攻击发生。使用该命令no的形式取消x-forward-for字段的取值配置。

[命令]

http-request-flood x-forward-for {**first** | **last** | **all**}

no http-request-flood x-forward-for

[句法描述]

first | last | all - 指定x-forwarded-for字段的取值，**first** 为x-forwarded-for字段第一个值，**last**为x-forwarded-for字段的最后一个值， **all**为x-forwarded-for字段的全部的值。

[默认取值]

无。

[命令模式]

Web服务器配置模式。

[使用指导]

无。

[命令实例]

```
hostname(config)# ips sigset http1 template http
hostname(config-http-sigset)# web-server web_server1
hostname(config-web-server)# http-request-flood x-forward-for first
```

http-request-flood x-real-ip

为系统开启CC防护功能中HTTP请求的x-real-for字段统计。启用后，系统会对x-real-for字段的值进行统计。使用该命令no的形式取消配置。

[命令]

http-request-flood x-real-ip enable

no http-request-flood x-real-ip

[句法描述]

无。

[默认取值]

无。

[命令模式]

Web服务器配置模式。

[使用指导]

无。

[命令实例]

```
hostname(config)# ips sigset http1 template http
hostname(config-http-sigset)# web-server web_server1
hostname(config-web-server)# http-request-flood x-real-ip enable
```

iframe-check

为系统开启HTTP协议iframe检查功能并对该功能进行配置。通过iframe检查，系统会识别出是否有隐藏的iframe的HTML页面，从而进行记录日志或重置连接。用该命令no的形式删除iframe设置。

[命令]

iframe-check enable action {**log** | **reset**}

no iframe-check enable

[句法描述]

reset | **log** 为隐藏iframe行为的HTTP请求指定相应的动作：

- **reset**：发现隐藏iframe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**：发现隐藏iframe行为后仅记录日志信息。

[默认取值]

无。

[命令模式]

Web服务器配置模式。

[使用指导]

[命令实例]

```
hostname(config)# ips sigset test_http template http
hostname(config-http-sigset)# web-server web_server1
```

```
hostname(config-web-server)# iframe-check enable action log
```

iframe width

为iframe检查功能配置高度和宽度的限制。系统会根据设定的iframe高度和宽度来检查HTML页面中的iframe，当高度和宽度中任意一项小于或等于设定值，系统将会识别为隐藏的iframe攻击发生，从而进行记录日志或重置连接。用该命令no的形式删除iframe设置。

[命令]

iframe width *width_value* **height** *height_value*

no iframe

[句法描述]

width *width_value* - 指定iframe的限定的宽度值，取值范围为0-4096px。

height *height_value* - 指定iframe的限定的高度值，取值范围为0-4096px。

[默认取值]

无。

[命令模式]

Web服务器配置模式。

[使用指导]

[命令实例]

```
hostname(config)# ips sigset test_http template http
hostname(config-http-sigset)# web-server web_server1
hostname(config-web-server)# iframe width 0 height 1
```

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 {**no-ips** | **predef_default** | **predef_loose** | *profile-name*} {**egress** | **ingress** | **bidirectional**}

no ips enable

[句法描述]

no-ips- 指定使用名为“no-ips”的预定义IPS Profile，含义为不做IPS检测。

predef_default - 指定使用名为“predef_default”的预定义IPS Profile，包含所有IPS 特征，对检测效果要求严格，且处理行为默认为重置。

predef_loose - 指定使用名为“predef_loose”的预定义IPS Profile，仅包含大部分严重程度比较高或流行度比较高的IPS特征，检测效率较高，且处理行为默认为只记录日志。

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 aggregation

系统可将符合聚合规则（协议ID相同、VSYS ID相同、特征规则ID相同、日志信息ID相同、聚合类型相同）的日志信息进行聚合，从而减少日志数量，避免日志服务器接受冗余的日志信息。

[命令]

ips log aggregation {**by-src** | **by-dst** | **by-src-dst**}

[句法描述]

by-src -将相同源IP并符合其他聚合规则的日志进行聚合。

by-dst -将相同目的IP并符合其他聚合规则的日志进行聚合。

by-src-dst -将相同源IP、相同目的IP并符合其他聚合规则的日志进行聚合。

[默认取值]

该功能为关闭状态，即不聚合日志。

[命令模式]

全局配置模式。

[使用指导]

- 系统仅支持聚合由IPS功能所产生的日志信息。
- 非根VSYS不支持此命令。

[命令实例]

```
hostname(config)# ips log aggregation by-src
```

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工作模式为只记录日志模式，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]

非根VSYS不支持此命令。

[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 {**no-ips** | **predef_default** | **predef_loose**| **predef_critical** | *profile-name*}

no ips profile *profile-name*

[句法描述]

no-ips - 指定使用名为“no-ips”的预定义IPS Profile，含义为不做IPS检测。

predef_default -指定使用名为“predef_default”的预定义IPS Profile，包含所有IPS 特征，对检测效果要求严格，且处理行为默认为重置。

predef_loose -指定使用名为“predef_loose”的预定义IPS Profile，仅包含大部分严重程度比较高或流行度比较高的IPS特征，检测效率较高，且处理行为默认为只记录日志。

predef_critical - 指定使用名为“predef_critical”的预定义IPS Profile，包含所有严重程度为高的IPS特征，且处理行为默认为只记录日志。

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]

非根VSYS中同样支持预定义IPS Profile。

[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]

- 当某特征在被配置为禁用状态，该特征在特征集下亦为禁用状态。
- 非根VSYS不支持此命令。

[命令实例]

```
hostname(config)# ips signature 160009 disable
```

ips sigset

基于已有预定义协议为模板创建用户自定义协议并进入协议配置模式。如果指定的名称已存在，则直接进入协议配置模式。使用该命令no的形式删除指定的协议。

[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 - 指定协议的名称。

dhcp | dns … | voip - 指定作为模板的预定义协议。

[默认取值]

无。

[命令模式]

全局配置模式。

[使用指导]

- 预定义协议不可以被删除也不可以被编辑。
- 自定义协议不可以与预定义特征集同名。
- 不可以基于自定义协议创建新的特征集。
- 同种类型的协议不可以添加到同一个IPS Profile中，例如两个以HTTP为模板的自定义协议不可以添加到同一个IPS Profile中。

[命令实例]

```
hostname(config)# ips sigset http1 template http
hostname(config-http-sigset)#
```

ips whitelist

创建IPS白名单并进入IPS白名单配置模式。如果IPS白名单名称已存在，则直接进入IPS白名单配置模式。配置后，系统将对匹配到IPS白名单中的报文放行，即不再做检测和防御，从而降低威胁的误报率。IPS白名单匹配条件包括：源地址、目的地址、特征ID、VRouter。用户至少需要配置一项匹配条件;当用户配置多条匹配条件时，流经设备的报文需满足所有条件，系统才会放行。使用该命令no的形式删除指定的白名单。

[命令]

ips whitelist *list-name*

no ips whitelist *list-name*

[句法描述]

list-name - 指定白名单的名称，取值范围为1-255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)# ips whitelist white1
hostname(config-ips-whitelist)#
```

issue-date

通过过滤规则筛选特征时，可配置issue-date数，筛选出指定发布时间内的特征。

[命令]

issue-date *year*

no issue-date *year*

[句法描述]

year - 指定特征的发布年度。取值范围2004到2020。

[默认取值]

无。

[命令模式]

过滤规则配置模式。

[使用指导]

无。

[命令实例]

```
hostname(config)# ips profile test
hostname(config-ips-profile)# filter-class 1
hostname(config-ips-filter-class)# issue-date 2006
```

max-arg-length

指定POP3客户端命令参数的最大长度，并指定发现异常后的处理动作。使用该命令no的形式恢复默认值。

[命令]

max-arg-length *length* **action** {**block-service** *timeout*| **block-ip** *timeout* | **log-only** | **reset**}

no max-arg-length（恢复默认长度）

[句法描述]

length - 指定命令参数的最大长度，单位为字节。

action {**block-service** *timeout*| **block-ip** *timeout* | **log-only** | **reset**} - **block-service**指定阻断攻击者服务,**block-ip**指定阻断攻击者服务IP，*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。**log-only**匹配该特征后仅记录日志信息。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。

[默认取值]

length - 40字节

[命令模式]

协议配置模式。

[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 action log-only
```

max-bind-length

指定系统允许的MSRPC协议绑定报文的最大长度，并并指定发现异常后的处理动作。使用该命令no的形式恢复默认值。

[命令]

max-bind-length *length* **action** {**block-service** *timeout*| **block-ip** *timeout* | **log-only** | **reset**}

no max-bind-length（恢复默认长度）

[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。

action {**block-service** *timeout*| **block-ip** *timeout* | **log-only** | **reset**} - **block-service** 指定阻断攻击者服务, **block-ip**指定阻断攻击者服务IP，*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。**log-only**匹配该特征后仅记录日志信息。**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。

[默认取值]

length - 2048字节

[命令模式]

协议配置模式。

[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 action log-only
```

max-black-list

指定Web服务器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]

Web服务器配置模式。

[使用指导]

无。

[命令实例]

```
hostname(config)# ips sigset http1 template http
hostname(config-http-sigset)# web-server www.abc.com
hostname(config-http-web-server)# 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），并指定发现异常后的处理动作。使用该命令no的形式恢复默认值。

[命令]

max-cmd-line-length *length* **action** {**block-service** *timeout*| **block-ip** *timeout* | **log-only** | **reset**}

no max-cmd-line-length（恢复默认长度）

[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。

action {**block-service** *timeout*| **block-ip** *timeout* | **log-only** | **reset**} - **block-service** 指定阻断攻击者服务, **block-ip**指定阻断攻击者服务IP，*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。**log-only**匹配该特征后仅记录日志信息。**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。

[默认取值]

length - 512字节

[命令模式]

协议配置模式。

[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 action log-only
```

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，并指定发现异常后的处理动作。使用该命令no的形式恢复默认值。

[命令]

max-content-filename-length *length* **action** {**block-service** *timeout*| **block-ip** *timeout* | **log-only** | **reset**}

no max-content-filename-length（恢复默认长度）

[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。

action {**block-service** *timeout*| **block-ip** *timeout* | **log-only** | **reset**} - **block-service** 指定阻断攻击者服务, **block-ip**指定阻断攻击者服务IP，*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。**log-only**匹配该特征后仅记录日志信息。**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。

[默认取值]

length - 128字节

[命令模式]

协议配置模式。

[使用指导]

无。

[命令实例]

```
hostname(config)# ips sigset smtp-cus template smtp
hostname(config-smtp-sigset)# max-content-filename-length 512 action
log-only
```

max-content-type-length

指定系统允许的SMTP协议Content-Type值的最大长度，并指定发现异常后的处理动作。使用该命令no的形式恢复默认值。

[命令]

max-content-type-length *length* **action** {**block-service** *timeout*| **block-ip** *timeout* | **log-only** | **reset**}

no max-content-type-length（恢复默认长度）

[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64到1024字节。

action {**block-service** *timeout*| **block-ip** *timeout* | **log-only** | **reset**}

- **block-service** 指定阻断攻击者服务, **block-ip**指定阻断攻击者服务IP，*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。**log-only**匹配该特征后仅记录日志信息。**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。

[默认取值]

length - 128字节

[命令模式]

协议配置模式。

[使用指导]

无。

[命令实例]

```
hostname(config)# ips sigset smtp-cus template smtp
hostname(config-smtp-sigset)# max-content-type-length 256 action log-
only
```

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），并指定发现异常后的处理动作。使用该命令no的形式恢复默认值。

[命令]

max-failure *times* **action** {**block-service** *timeout*| **block-ip** *timeout* | **log-only** | **reset**}

no max-failure（恢复默认次数）

[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。

action {**block-service** *timeout*| **block-ip** *timeout* | **log-only** | **reset**} - **block-service**指定阻断攻击者服务,**block-ip**指定阻断攻击者服务IP，*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。**log-only**匹配该特征后仅记录日志信息。**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。

[默认取值]

times – 0（不做次数限制）

[命令模式]

协议配置模式。

[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 action log-only
```

max-input-length

指定系统允许的Telnet用户名和密码的最大长度，并指定发现异常后的处理动作。使用该命令no的形式恢复默认值。

[命令]

max-input-length *length* **action** {**block-service** *timeout*| **block-ip** *timeout* | **log-only** | **reset**}

no max-input-length（恢复默认长度）

[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。

action {**block-service** *timeout*| **block-ip** *timeout* | **log-only** | **reset**} - **block-service** 指定阻断攻击者服务，**block-ip**指定阻断攻击者服务IP，*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。**log-only**匹配该特征后仅记录日志信息。**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。

[默认取值]

length - 128字节

[命令模式]

协议配置模式。

[使用指导]

无。

[命令实例]

```
hostname(config)# ips sigset telnet-cus template telnet
hostname(config-telnet-sigset)# max-input-length 30 action log-only
```

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，并指定发现异常后的处理动作。使用该命令no的形式恢复默认值。

[命令]

max-path-length *length* **action** {**block-service** *timeout*| **block-ip** *timeout* | **log-only** | reset}

no max-path-length（恢复默认长度）

[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）。

action {**block-service** *timeout*| **block-ip** *timeout* | **log-only** | **reset**}

- **block-service** 指定阻断攻击者服务, **block-ip**指定阻断攻击者服务IP，*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。**log-only**匹配该特征后仅记录日志信息。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。

[默认取值]

length - 256字节

[命令模式]

协议配置模式。

[使用指导]

无。

[命令实例]

```
hostname(config)# ips sigset smtp-cus template smtp
hostname(config-smtp-sigset)# max-path-length 128 action log-only
```

max-reply-line-length

指定系统允许的SMTP服务器端响应的最大长度，并指定发现异常后的处理动作。使用该命令no的形式恢复默认值。

[命令]

max-reply-line-length *length* **action** {**block-service** *timeout*| **block-ip** *timeout* | **log-only** | **reset**}

no max-reply-line-length（恢复默认长度）

[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）。

action {**block-service** *timeout*| **block-ip** *timeout* | **log-only** | **reset**} - **block-service**指定阻断攻击者服务, **block-ip**指定阻断攻击者服务IP，*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。**log-only**匹配该特征后仅记录日志信息。**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。

[默认取值]

length - 512字节

[命令模式]

协议配置模式。

[使用指导]

无。

[命令实例]

```
hostname(config)# ips sigset smtp-cus template smtp
hostname(config-smtp-sigset)# max-reply-line-length 1024 action log-only
```

max-request-length

指定系统允许的MSRPC协议请求报文的最大长度，并指定发现异常后的处理动作。使用该命令no的形式恢复默认值。

[命令]

max-request-length *length* **action** {**block-service** *timeout*| **block-ip** *timeout* | **log-only** | **reset**}

no max-request-length（恢复默认长度）

[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。

action {**block-service** *timeout*| **block-ip** *timeout* | **log-only** | **reset**}- **block-service**指定阻断攻击者服务, **block-ip**指定阻断攻击者服务IP，*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。**log-only**匹配该特征后仅记录日志信息。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。

[默认取值]

length - 65535字节

[命令模式]

协议配置模式。

[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 action log-only
```

max-rsp-line-length

指定系统允许的FTP最大响应长度，并指定发现异常后的处理动作。使用该命令no的形式恢复默认值。

[命令]

max-rsp-line-length *length* **action** {**block-service** *timeout*| **block-ip** *timeout* | **log-only** | **reset**}

no max-rsp-line-length（恢复默认长度）

[句法描述]

length - 指定最大响应长度，单位为字节。取值范围是5到1024字节。

action {**block-service** *timeout*| **block-ip** *timeout* | **log-only** | **reset**} - **block-service**指定阻断攻击者服务, **block-ip**指定阻断攻击者服务IP，*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。**log-only**匹配该特征后仅记录日志信息。**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。

[默认取值]

length - 512字节

[命令模式]

协议配置模式。

[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 action log-only
```

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 – 4096

[命令模式]

协议配置模式。

[使用指导]

无。

[命令实例]

```
hostname(config)# ips sigset test1 template other-tcp
hostname(config-other-tcp-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，并指定发现异常后的处理动作。使用该命令no的形式恢复默认值。

[命令]

max-text-line-length *length* **action** {**block-service** *timeout*| **block-ip** *timeout* | **log-only** | **reset**}

no max-text-line-length（恢复默认长度）

[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）。

action {**block-service** *timeout*| **block-ip** *timeout* | **log-only** | **reset**} - **block-service**指定阻断攻击者服务, **block-ip**指定阻断攻击者服务IP，*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。**log-only**匹配该特征后仅记录日志信息。**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。

[默认取值]

length – 1000字节

[命令模式]

协议配置模式。

[使用指导]

无。

[命令实例]

```
hostname(config)# ips sigset smtp-cus template smtp
hostname(config-smtp-sigset)# max-text-line-length 1024 action log-only
```

max-uri-length

指定系统允许的HTTP协议URL的最大长度，并指定发现异常后的处理动作。使用该命令no的形式恢复默认值。

[命令]

max-uri-length *length* **action** {**block-service** *timeout*| **block-ip** *timeout* | **log-only** | **reset**}

no max-uri-length（恢复默认长度）

[句法描述]

length - 指定URL最大长度，单位为字节，范围为64到4096。

action {**block-service** *timeout*| **block-ip** *timeout* | **log-only** | **reset**} - **block-service**指定阻断攻击者服务, **block-ip**指定阻断攻击者服务IP，*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。**log-only**匹配该特征后仅记录日志信息。**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。

[默认取值]

length - 4096字节

[命令模式]

协议配置模式。

[使用指导]

无。

[命令实例]

```
hostname(config)# ips sigset http1 template http
hostname(config-http-sigset)# max-uri-length 1000 action log-only
```

max-white-list

指定Web服务器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]

Web服务器配置模式。

[使用指导]

无。

[命令实例]

```
hostname(config)# ips sigset http1 template http
hostname(config-http-sigset)# web-server www.abc.com
hostname(config-http-web-server)# max-white-list 4096
```

pcap

对于过滤规则和搜索规则筛选出的特征，当流量命中特征时，指定是否抓包。

[命令]

pcap enable

pcap disable

[句法描述]

enable -对异常数据包进行抓包。对异常的数据包抓取后，可在威胁日志中查看。

disable -对异常数据包不抓包。

[默认取值]

disable。

[命令模式]

过滤规则配置模式；

搜索规则配置模式。

[使用指导]

无。

[命令实例]

```
hostname(config)# ips profile test
hostname(config-ips-profile)# pcap enable
```

protocol-check

特征集配置协议合法性检查的启用与关闭，以及检测到异常后采取的行为。严格性并启用协议合法性检查。

[命令]

protocol-check disable

protocol-check enable action {**block-service** *timeout*| **block-ip** *timeout* | **log-only** | **reset**} **pcap** {**disable** | **enable**}

[句法描述]

enable -启用协议合法性检查。

block-service - 指定阻断攻击者服务,并指定对攻击者服务进行阻断的时长，单位为秒，范围是60到3600秒。

block-ip -指定阻断攻击者服务IP，并指定对攻击者IP或者服务进行阻断的时长，单位为秒，范围是60到3600秒。

log-only- 匹配该特征后仅记录日志信息。

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。

pcap {disable | enable} enable对异常数据包进行抓包；**disable**不对异常数据包进行抓包。

[默认取值]

协议合法性检查：关闭；

[命令模式]

协议配置模式。

[使用指导]

无。

[命令实例]

```
hostname(config)# ips sigset http1 template http
hostname(config-http-sigset)# protocol-check strict
hostname(config-http-sigset)# protocol-check enable action log-only
```

protocol

通过过滤规则筛选特征时，可配置protocol参数，筛选出指定协议对应的特征。

[命令]

protocol {**DNS** | **FTP** | **HTTP** | …}

no protocol { **DNS** | **FTP** | **HTTP** | …}

[句法描述]

DNS | FTP | HTTP | … -指定协议。用户可通过在**protocol**参数后使用Tab键，查看完整的协议列表。

[默认取值]

无。

[命令模式]

过滤规则配置模式。

[使用指导]

无。

[命令实例]

```
hostname(config)# ips profile test
hostname(config-ips-profile)# filter-class 1
hostname(config-ips-filter-class)# protocol Telnet
```

referer-white-list

为Web服务器配置首部特例URL。配置后，该URL可引用Web站点，其他未添加的URL则不可以引用Web站点。用该命令no的形式删除首部特例URL的设置。

[命令]

referrer-white-list *url_string*

no referrer-white-list *url_string*

[句法描述]

url_string - 指定可以引用Web站点的特例URL。

[默认取值]

无。

[命令模式]

Web服务器配置模式。

[使用指导]

每个Web服务器最多允许配置32条URL路径。

[命令实例]

```
hostname(config)# ips sigset test_http template http
hostname(config-http-sigset)# web-server web_server1
hostname(config-web-server)# referrer-white-list www.abc.com
```

referer-white-list-check

为系统开启HTTP首部检查功能并对该功能进行配置。配置后，系统可对盗链和CSRF(Cross Site Request Forgery跨网站请求欺骗)攻击行为的HTTP请求重置连接或记录日志。使用该命令no的形式关闭该功能。

[命令]

```
referrer-white-list-check enable action {log | reset}
no referrer-white-list-check enable
```

[句法描述]

reset | log 为发生盗链行为的HTTP请求指定相应的动作：

- **reset**：发现盗链或攻击后重置连接（TCP）或者发送目标不可达包（UDP）并且记录日志信息。
- **log**：发现盗链或攻击后仅记录日志信息。

[默认取值]

无。

[命令模式]

Web服务器配置模式。

[使用指导]

无。

[命令实例]

```
hostname(config)# ips sigset test_http template http
hostname(config-http-sigset)# web-server web_server1
```

```
hostname(config-web-server)# referrer-white-list-check enable action
log
```

response-bypass

指定不对服务器返回的HTTP数据包进行扫描。

[命令]

response-bypass

no response-bypass

[句法描述]

无。

[默认取值]

无。

[命令模式]

协议配置模式。

[使用指导]

仅对HTTP协议适用。

[命令实例]

```
hostname(config)# ips sigset http1 template http
hostname(config-http-sigset)# response-bypass
```

search-class

进行特征集配置时，可通过搜搜条件筛选出特定的特征。使用如下命令创建搜索规则并进入搜索规则配置模式。使用该命令no的形式删除搜索规则。

[命令]

search-class *id* **name** *name*

no search-class *id*

[句法描述]

id -指定搜索规则的ID。

name *name* -指定搜索规则的名称。

[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 test
hostname(config-ips-profile)# search-class 1 name test1
```

search-condition

通过搜索规则筛选特征时，可指定特征的信息进行检索。系统将在如下字段中进行模糊检索：特征ID，特征名称，描述信息，CVE-ID。

[命令]

search-condition *description*

no search-condition *description*

[句法描述]

description - 指定特征的信息。

[默认取值]

无。

[命令模式]

搜索规则配置模式。

[使用指导]

无。

[命令实例]

```
hostname(config)# ips profile test
```

```
hostname(config-ips-profile)# search-class 1
hostname(config-ips-filter-class)# search-condition DNS
```

severity

通过过滤规则筛选特征时，可配置severity参数，筛选出指定严重程度的特征。

[命令]

severity {**Low** | **Medium** | **High**}

no severity {**Low** | **Medium** | **High**}

[句法描述]

Low | Medium | High - 指定严重程度。

[默认取值]

无。

[命令模式]

过滤规则配置模式。

[使用指导]

无。

[命令实例]

```
hostname(config)# ips profile test
hostname(config-ips-profile)# filter-class 1
hostname(config-ips-filter-class)# severity Low
```

signature id

通过搜索规则筛选特征时，可配置signature id，筛选出指定ID的特征。

[命令]

signature id *id*

no signature id *id*

[句法描述]

id 指定特征ID。

[默认取值]

无。

[命令模式]

搜索规则配置模式。

[使用指导]

无。

[命令实例]

```
hostname(config)# ips profile test
hostname(config-ips-profile)# search-class 1
hostname(config-ips-filter-class)# signature id 105001
```

signature-id

配置IPS白名单的特征ID。使用该命令no的形式删除源IP地址的配置。

[命令]

signature-id *id*

no signature-id *id*

[句法描述]

id - 指定IPS白名单需匹配的特征ID。

[默认取值]

无。

[命令模式]

IPS白名单配置模式。

[使用指导]

一个白名单只允许配置一个威胁ID；

[命令实例]

```
hostname(config)# ips whitelist white1
hostname(config-ips-whitelist)# signature-id 105002
```

sigset

将协议配置添加到IPS Profile中。使用该命令no的形式将协议配置从IPS Profile中删除。

[命令]

sigset *user-defined-profile*

no sigset *user-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。

[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
```

src-ip

配置IPS白名单的源IP地址。使用该命令no的形式删除源IP地址的配置。

[命令]

src-ip *A.B.C.D*|*A.B.C.D/M*

no src-ip

[句法描述]

A.B.C.D|*A.B.C.D/M* - 指定IPS白名单需匹配的源IP地址。

[默认取值]

无。

[命令模式]

IPS白名单配置模式。

[使用指导]

无。

[命令实例]

```
hostname(config)# ips whitelist white1
hostname(config-ips-whitelist)# src-ip 10.1.1.1
```

system

通过过滤规则筛选特征时，可配置system参数，筛选出指定操作系统对应的特征。

[命令]

```
system {Windows | Linux | FreeBSD | …}
no system { Windows | Linux | FreeBSD | …}
```

[句法描述]

Windows | Linux | FreeBSD | … -指定操作系统。用户可通过在**system**参数后使用Tab键，查看完整的操作系统列表。

[默认取值]

无。

[命令模式]

过滤规则配置模式。

[使用指导]

无。

[命令实例]

```
hostname(config)# ips profile test
hostname(config-ips-profile)# filter-class 1
hostname(config-ips-filter-class)# system Linux
```

sql-injection

关闭SQL注入检查点。使用该命令no的形式开启检查点。

[命令]

sql-injection {**cookie** | **cookie2** | **post** | **referer** | **uri**} **disable**

no sql-injection {**cookie** | **cookie2** | **post** | **referer** | **uri**} **disable**

[句法描述]

{cookie | cookie2 | post | referer | uri} disable - 关闭指定的SQL注入检查点，可以为HTTP Cookie、HTTP Cookie2、HTTP Post、HTTP Referer或者HTTP URI。

[默认取值]

无。

[命令模式]

Web服务器配置模式。

[使用指导]

无。

[命令实例]

```
hostname(config)# ips sigset http1 template http
hostname(config-http-sigset)# web-server web_server1
hostname(config-web-server)# sql-injection cookie disable
```

sql-injection-check

为系统开启HTTP协议SQL注入检查功能并对该功能进行配置。

[命令]

sql-injection-check enable [**sensitive** {**low** | **medium** | **high**}] [**action** {**reset** | **log**}] [**block** {**ip** | **service**} **timeout**] [**noblock**]

sql-injection-check disable

[句法描述]

sensitive {low | medium | high} -为HTTP协议SQL注入检查指定检测敏感度，可以为“高（**high**）”、“中（**medium**）”或者“低（**low**）”。敏感度越高，漏报率越低。

reset | log -为HTTP协议SQL注入检查指定相应的动作：

- **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 | **service** - 指定阻断SQL注入攻击者的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]

敏感度：低。

[命令模式]

Web服务器配置模式。

[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)# web-server www.abc.com
hostname(config-web-server)# sql-injection-check enable
```

vr

配置IPS白名单的VRouter。使用该命令no的形式删除VRouter的配置。

[命令]

vr *vr-name*

no vr

[句法描述]

vr-name -指定IPS白名单需匹配的VRouter的名称。

[默认取值]

无。

[命令模式]

IPS白名单配置模式。

[使用指导]

无。

[命令实例]

```
hostname(config)# ips whitelist white1
hostname(config-ips-whitelist)# src-ip 10.1.1.1
hostname(config-ips-whitelist)# vr trust-vr
```

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]

Web服务器配置模式。

[使用指导]

无。

[命令实例]

```
hostname(config)# ips sigset http1 template http
hostname(config-http-sigset)# web-server www.abc.com
hostname(config-http-web-server)# 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Web服务器上传恶意代码。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]

Web服务器配置模式。

[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)# web-server www.abc.com
hostname(config-http-web-server)# web-acl-check enable action reset
```

web-server

新建Web服务器，并且进入Web服务器配置模式。如果指定名称已存在，则直接进入Web服务器配置模式。使用该命令no的形式删除已存在的Web服务器。

[命令]

web-server {**default** | *server_name*}

no web-server *server_name*

[句法描述]

default - 配置默认Web服务器。新建HTTP特征集时，系统会自动创建一个默认Web服务器。

server_name -指定所创建的Web服务器名称，为1到31个字符长度的字符串。

[默认取值]

无。

[命令模式]

协议配置模式。

[使用指导]

默认Web服务器不可以添加，且不能被删除。

每个特征集最多配置32个Web服务器，不包括默认服务器。

[命令实例]

```
hostname(config)# ips sigset test_http template http
hostname(config-http-sigset)# web-server web_server1
hostname(config-web-server)#
```

xss-injection

关闭XSS注入检查点。使用该命令no的形式开启检查点。

[命令]

xss-check {**cookie** | **cookie2** | **post** | **referer** | **uri**} **disable**

no xss-injection {**cookie** | **cookie2** | **post** | **referer** | **uri**} **disable**

[句法描述]

{cookie | cookie2 | post | referer | uri} disable 关闭指定的XSS注入检查点，可以为HTTP Cookie、HTTP Cookie2、HTTP Post、HTTP Referer或者HTTP URI。

[默认取值]

无。

[命令模式]

Web服务器配置模式。

[使用指导]

无。

[命令实例]

```
hostname(config)# ips sigset http1 template http
hostname(config-http-sigset)# web-server web_server1
hostname(config-web-server)# xss-injection uri disable
```

xss-check enable

为系统开启HTTP协议XSS注入检查功能并对该功能进行配置。

[命令]

xss-check enable [**sensitive** {**low** | **medium** | **high**}] [**action** {**log** | **reset**}] [**block** {**ip** | **service**} *timeout*] [**noblock**]

xss-check disable

[句法描述]

sensitive {**low** | **medium** | **high**} -为HTTP协议XSS注入检查指定检测敏感度，可以为“高（**high**）”、“中（**medium**）”或者“低（**low**）”。敏感度越高，漏报率越低。

reset | **log** -为HTTP协议XSS注入检查指定相应的动作：

- **reset**：发现XSS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XSS注入攻击后仅记录日志信息。

ip | **service** -指定阻断XSS注入攻击者的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]

敏感度：低。

[命令模式]

Web服务器配置模式。

[使用指导]

XSS注入攻击事件为“严重”级别事件。不进行动作配置时，检测出XSS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)# web-server www.abc.com
hostname(config-web-server)# xss-check enable
```

show ips

显示IPS相关配置的相关信息。

[命令]

显示IPS配置的全部信息：**show ips configuration**（非根VSYS不支持）

显示IPS Profile配置的全部信息：**show ips profile** [*profile-name*] [**signature-class** *signature-class-id*]

显示IPS协议配置的全部信息：**show ips sigset** [*sigset-name*]

显示CC防护认证相关信息：**show ips sigset** *sigset-name* **web-server** *server-name* **http-request-flood auth-ck**

显示CC防护源IP的最大速率排名和总数排名：**show ips sigset** *sigset-name* **web-server** *server-name* **http-request-flood ip-top** {**max-rate** | **total**}

显示CC防护的总体信息、防护信息以及请求的URL排名：**show ips sigset** *sigset-name* **web-server** *server-name* **http-request-flood req-stat** {**overview** {**by-day** |

by-hour | **by-minute** | **by-second**} | **protect** {**by-day** | **by-hour** | **by-minute** | **by-second**} | **top**}

显示IPS状态信息：**show ips status**

显示安全域与IPS Profile的绑定信息：**show ips zone-binding**

[句法描述]

sigset-name -指定需要显示的协议配置名称。

profile-name 指定需要显示的IPS Profile的名称。

signature-class-id - 指定需要显示的过滤规则或搜索规则的ID。

web-server *server-name* - 指定需要显示的Web服务器的名称。

ip-top {**max-rate** | **total**} - 指定显示源IP的最大速率排名（**max-rate**）或者总数排名（**total**）。

req-stat {**overview** {**by-day** | **by-hour** | **by-minute** | **by-second**} - 指定显示报文的总体信息，包括请求数、不同请求方法（GET、POST）对应的请求数、应答数、不同状态码（4XX、5XX）对应的应答数。可以按照天、小时、分钟和秒进行显示。

protect {**by-day** | **by-hour** | **by-minute** | **by-second**} - 指定显示报文的防护信息，包括请求数、应答数、代理请求数限制丢弃数、非代理请求数限制丢弃数、认证应答数、认证丢弃数。可以按照天、小时、分钟和秒进行显示。

top - 指定显示请求的URL排名。

[默认取值]

无默认值。

[命令模式]

任何模式。

[使用指导]

执行**http-request-flood statistics enable**命令后，**show ips sigset** *sigset-name* **web-server** *server-name* **http-request-flood req-stat top**命令才会生效。

[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
--------------------------------------------------------------
```

异常行为检测

异常行为检测（ABD）介绍

网络中存在着多种的攻击，例如Web攻击、DDoS攻击、应用层攻击、端口/服务扫描攻击、对主机的攻击等，这些攻击都表现出多种多样的异常行为。因此系统提供了基于安全域的异常行为检测（Abnormal Behavior Detection）功能。该功能对检测对象的会话特征进行多维度监控统计，根据特征库中的异常行为检测规则检测，并根据正常的网络行为建立模型，当检测对象的多个参量发生异常时，系统将分析其参量异常的关联关系，判断检测对象是否产生了异常行为。若判定存在异常行为，系统会发出行为异常告警，产生相关的威胁日志。

异常行为检测功能相关概念解释如下：

- 检测对象：主机防护中的保护对象，以及核心资产中的保护对象。
- 参量：会话的基本统计指标，例如每秒内的连入流量。参量统计值是判断特定检测对象是否有异常行为的基本条件。
- 参量异常：当参量值高于上限值或者低于下限值时，参考值即被判断为异常。此时系统发出异常告警，产生威胁日志。上下限值根据历史数据的学习生成。
- 异常行为模型库：异常行为模型库包含异常相关信息，包括异常行为检测规则、异常描述、异常原因以及异常建议等。异常行为模型库帮助用户分析以及解决异常。默认情况下，系统会每日自动更新异常行为模型库，用户可以根据需要更改异常行为模型库更新配置。关于异常行为模型库更新配置，请参阅“异常行为模型库更新配置”。为保证能够正常连接到默认更新服务器，请在更新前为设备配置DNS服务器。

异常行为检测配置

使用异常行为检测功能前，必须完成以下准备工作：

1. 确认系统版本支持异常行为检测功能。
2. 安装StoneShield许可证，然后重启设备。设备成功重启后，异常行为检测功能才可使用。

开启/关闭异常行为检测功能

开启基于指定安全域的异常行为检测功能。默认对此安全域下整体的网络进行检测。在安全域配置模式下，使用以下命令：

anomaly-detection [**host-enable** [**advanced-protection**] [**ddos-protection**]] | [**forensic**]

- **host-enable** – 启用主机防护功能，即对此安全域下的每一台识别到的主机建立学习模型，对主机的网络行为进行分析，并且为不同的网络行为定义相应的特征维度，再根据特征维度来检测主机是否出现异常行为，发现更为隐藏的威胁攻击。启用主机防护功能时，默认不开启HTTP维度的异常行为检测和DDoS防护。如需开启HTTP维度的异常行为检测，使用advanced-protection参数。如需开启主机的DDoS防护，使用ddos-protectoin参数，目前可对如下几种类型的DDos攻击进行防护：Zip of Death、SSL DDoS、DDoS Flood、DDoS Sockstress、DDoS Reflect、Application DDoS、DNS Query Flood。
- **forensic** – 指定抓取证据报文，如果指定该参数，系统将在产生异常行为告警时保存相关证据报文。

在安全域配置模式下，使用该命令no的形式关闭基于指定安全域的异常行为检测功能、主机防护功能或抓取证据报文功能：

no anomaly-detection [**host-enable** [**advanced-protection** | **ddos-protection**]][**forensic**]

DNS 映射

DNS作为域名解析协议，用于地址和域名的双向解析，由于域名使用方便，被广泛应用，因此攻击者会采取不同手段利用域名产生攻击。例如： 一个IP地址可对应多个域名，服务器根据HTTP报文的Host字段来确定目标网站，一些恶意软件会利用这一特性通过修改Host字段来伪装域名，产生恶意攻击行为；DGA（Domain Generation Algorithm）即域名生成算法，该算法会生成大量的伪随机域名，并且会被恶意软件所采用；运营商DNS劫持，将一些长期被恶意软件所采用的恶意域名加入其黑名单。

针对上述这些问题，DNS域名的分析可以作为重要依据来判断恶意行为。设备启用异常行为检测功能后，系统将会DNS响应报文进行检测，建立DNS 映射列表，DNS 映射列表用来存储域名和IP地

址对应关系、DGA算法生成的伪随机域名以及从云端同步的黑白域名，设备能够及时根据DNS 映射列表检测出恶意软件和恶意行为攻击，产生相关的威胁日志。

查看DNS 映射列表条目

用户通过show命令查看DNS映射列表存储的域名与IP地址对应关系条目数以及域名条目数。在任何模式下使用以下命令：

```
show dns-mapping
```

显示DoS攻击检测状态

在任何模式下，输入以下命令显示针对DoS攻击的异常行为检测状态：

```
show anomaly-detection ddos status
```

异常行为模型库更新配置

默认情况下，系统会每日自动更新异常行为模型库，用户可以根据需要更改异常行为模型库更新配置。异常行为模型库更新配置包括：

- 配置异常行为模型库更新模式
- 指定异常行为模型库自动更新周期
- 立即更新
- 导入异常行为模型文件
- 显示异常行为模型库更新配置信息

配置异常行为模型库更新模式

异常行为模型库支持手动和自动（周期性）两种更新方式。配置异常行为模型库更新方式，在全局配置模式下，使用以下命令：

```
cloud abnormal-behavior-detection mode {1 | 2}
```

- 1 – **manual**，指定手动更新异常行为模型库。
- 2 – **period**，指定自动（周期性）更新异常行为模型库。

指定异常行为模型库自动更新周期

指定异常行为模型库自动更新周期，在全局配置模式下，使用以下命令：

cloud abnormal-behavior-detection period *period*

- *period* - 指定自动更新周期。范围为600到86400，单位为秒。

立即更新

无论更新模式为手动还是自动（周期性），用户都可以随时使用以下命令立即更新异常行为模型库。立即更新异常行为模型库，在任何模式下，使用以下命令：

exec cloud abnormal-behavior-detection update

- **exec cloud abnormal-behavior-detection update** – 仅对当前异常行为模型库与更新服务器最新发布异常行为模型库的不同部分进行更新。

导入异常行为模型文件

在某些情况下，用户设备可能无法连接到更新服务器对异常行为模型库进行更新，针对这一问题，系统提供异常行为模型文件导入功能，即通过FTP、TFTP服务器或者U盘将异常行为模型文件导入到设备，从而更新设备的异常行为模型库。导入异常行为模型文件，在执行模式下，使用以下命令：

import cloud abnormal-behavior-detection from {**ftp server** *ip-address* [**user** *user-name* **password** *password*] | **tftp server** *ip-address* } [**vrouter** *vr-name*] *file-name*

- *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。
- **vrouter** *vr-name* – 指定FTP或者TFTP服务器所属的VRouter。
- *file-name* – 指定导入的异常行为模型文件的名称。

显示异常行为模型库更新配置信息

用户可以随时使用相应的show命令查看设备上的异常行为模型库更新信息，在任何模式下使用以下命令：

show cloud abnormal-behavior-detection update

高级威胁检测

高级威胁检测（ATD）介绍

高级威胁检测（Advanced Threat Detection）功能在学习恶意软件行为模型库的基础上，对基于主机的可疑流量进行智能分析，来检测恶意行为进而识别APT（Advanced Persistent Threat）攻击，并产生相关威胁日志。

使用该功能前，用户需要首先更新恶意软件行为模型库。默认情况下，系统会每日自动更新恶意软件行为模型库，用户可以根据需要更改恶意软件行为模型库更新配置。关于恶意软件行为模型库更新配置，请参阅“恶意软件行为模型库更新配置”。

高级威胁检测配置

使用高级威胁检测功能前，必须完成以下准备工作：

1. 确认系统版本支持高级威胁检测功能。
2. 安装StoneShield许可证，然后重启设备。设备成功重启后，高级威胁检测功能才可使用。

配置基于指定安全域的高级威胁检测功能。在安全域配置模式下，使用以下命令：

malware-detection [**forensic**]

- **malware-detection** – 开启指定安全域的高级威胁检测功能。
- **forensic** – 指定抓取证据报文，如果指定该参数，系统将保存相关证据报文并支持用户下载报文。

在安全域配置模式下，使用该命令no的形式关闭基于指定安全域的高级威胁检测功能或抓取证据报文功能：

no malware-detection [**forensic**]

恶意软件行为模型库更新配置

默认情况下，StoneOS会每日自动更新恶意软件行为模型库，用户可以根据需要更改恶意软件行为模型库更新配置。恶意软件行为模型库更新配置包括：

- 配置恶意软件行为模型库更新模式
- 指定恶意软件行为模型库自动更新周期
- 立即更新
- 导入恶意软件行为模型文件
- 显示恶意软件行为模型库更新配置信息

配置恶意软件行为模型库更新模式

恶意软件行为模型库支持手动和自动（周期性）两种更新方式。配置恶意软件行为模型库更新方式，在全局配置模式下，使用以下命令：

```
cloud advanced-threat-detection mode {1 | 2}
```

- 1 – **manual**，指定手动更新恶意软件行为模型库。
- 2 – **period**，指定自动（周期性）更新恶意软件行为模型库。

指定恶意软件行为模型库自动更新周期

指定异高级威胁检测征库自动更新周期，在全局配置模式下，使用以下命令：

```
cloud advanced-threat -detection period period
```

- **period** - 指定自动更新周期。范围为600到86400，单位为秒。

立即更新

无论更新模式为手动还是自动（周期性），用户都可以随时使用以下命令立即更新恶意软件行为模型库。立即更新恶意软件行为模型库，在任何模式下，使用以下命令：

```
exec cloud advanced-threat -detection update
```

- **exec cloud advanced-threat-detection update** – 仅对当前恶意软件行为模型库与更新服务器最新发布恶意软件行为模型库的不同部分进行更新。

导入恶意软件行为模型文件

在某些情况下，用户设备可能无法连接到更新服务器对高级威胁检测检测特征库进行更新，针对这一问题，系统提供恶意软件行为模型文件导入功能，即通过FTP、TFTP服务器或者U盘将恶意软件行为模型文件导入到设备，从而更新设备的恶意软件行为模型库。导入恶意软件行为模型文件，在执行模式下，使用以下命令：

import cloud advanced-threat -detection from {**ftp server** *ip-address* [**user** *user-name* **password** *password*] | **tftp server** *ip-address* } [**vrouter** *vr-name*] *file-name*

- *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。
- **vrouter** *vr-name* – 指定FTP或者TFTP服务器所属的VRouter。
- *file-name* – 指定导入的恶意软件行为模型文件的名称。

显示恶意软件行为模型库更新配置信息

用户可以随时使用相应的show命令查看设备上的恶意软件行为模型库更新信息，在任何模式下使用以下命令：

show cloud advanced-threat -detection update

边界流量过滤

边界流量过滤介绍

边界流量过滤（Perimeter Traffic Filtering）功能是基于已知的风险IP对流量进行过滤，并对命中风险IP的恶意流量采取阻断、记录日等措施进行处理。

风险IP包括以下三种类型：

- IP信誉：通过更新系统的IP信誉特征库，从云端同步符合僵尸主机、垃圾邮件、Tor节点、失陷主机、暴力破解等特征的信誉风险IP。
- 自定义黑白名单：用户根据实际需求，把指定的IP地址添加到自定义黑白名单。
- 第三方风险IP：与趋势TDA进行联动，定期从趋势TDA设备上获取风险IP地址。

使用IP信誉功能前，用户需要首先更新IP信誉特征库。默认情况下，系统会每日自动更新IP信誉特征库，用户可以根据需要更改IP信誉特征库更新配置。关于IP信誉特征库更新配置，请参阅“异常行为模型库更新配置”。

边界流量过滤配置

使用边界流量过滤功能前，必须完成以下准备工作：

1. 确认系统版本支持边界流量过滤功能。
2. 安装威胁防护（TP）许可证，然后重启设备。设备成功重启后，边界流量过滤功能才可使用。

开启/关闭边界流量过滤功能

开启基于指定安全域的边界流量过滤功能并且进入边界流量过滤配置模式。在安全域配置模式下，使用以下命令：

```
perimeter-traffic-filtering
```

在安全域配置模式下，使用该命令no的形式关闭基于指定安全域的边界流量过滤功能：

```
no perimeter-traffic-filtering
```

开启/关闭各类风险IP的边界流量过滤功能

针对三种类型的风险IP（IP信誉、自定义黑名单以及第三方风险IP），用户可以分别开启边界流量过滤功能以及指定命中后的处理动作，在边界流量过滤配置模式下，使用以下命令：

- IP信誉：**ip-reputation category** {**bot** | **brute-forcer** | **compromised** | **ddos-attacker** | **proxy** | **scanner** | **spam** | **tornode**} {**drop** | **log-only** | **block-ip** *timeout*}
  - **bot | brute-forcer | compromised |ddos-attacker | proxy | scanner | spam | tornode** – 指定IP信誉的类别，包括僵尸主机（bot）、暴力破解（brute-forcer）、失陷主机（compromised）、DDos攻击者（ddos-attacker）、代理（proxy）、扫描（scanner）、垃圾邮件（spam）、Tor节点（tornode）。
  - **drop** – 系统命中IP信誉分类的恶意流量后丢弃数据包。
  - **log-only** – 系统命中IP信誉分类的恶意流量后仅记录日志信息。该选项为系统默认处理行为。
  - **block-ip** *timeout* - 系统命中IP信誉分类的恶意流量后阻断IP一定的时间，timeout为阻断的时长，单位为秒，范围是60到3600秒。
- 自定义黑白名单：**user-define [drop | log-only]**
  - **drop** –系统命中自定义黑白名单的恶意流量后丢弃数据包。
  - **log-only** – 系统命中自定义黑白名单的恶意流量后仅记录日志信息。该选项为系统默认处理行为。
- 第三方风险IP：**trend-micro** [**drop** | **log-only**]
  - **drop** –系统命中第三方的恶意流量后丢弃数据包。
  - **log-only** – 系统命中第三方风险IP的恶意流量后仅记录日志信息。该选项为系统默认处理行为。

在边界流量过滤配置模式下，使用以上命令no的形式关闭基于不同黑白名单的边界流量过滤功能：

- IP信誉黑名单：**no ip-reputation category** {**bot** | **brute-forcer** | **compromised** | **ddos-attacker** | **proxy** | **scanner** | **spam** | **tornode**}
- 自定义黑白名单：**no user-define**
- 第三方风险IP：**no trend-micro**

配置自定义黑白名单

进入边界流量过滤配置模式下，在全局配置模式下，使用以下命令：

perimeter-traffic-filtering

添加指定IP地址条目到自定义黑白名单，在边界流量过滤配置模式下，使用以下命令：

userdefined-iplist [**id** *id*] **ip** *ip-address*

- **id** *id* – 指定黑白名单地址条目ID。如果不指定该参数，系统会自动为添加的地址条目分配一个ID。
- **ip** *ip-address* – 指定需要添加到黑白名单的条目IP地址。

在边界流量过滤配置模式下，使用该命令no的形式删除指定ID的黑白名单地址条目：

no userdefined-iplist id *id*

配置第三方风险IP

系统支持设备与第三方“趋势TDA”进行联动，从而获取黑名单。第三方风险IP的配置包括：

- 进入第三方风险IP配置模式
- 开启/关闭与趋势TDA设备互动
- 配置趋势TDA设备地址
- 配置与趋势TDA设备的互动请求周期
- 开启/关闭沙箱互动

进入第三方风险IP配置模式

进入第三方黑白名单配置模式，在全局配置模式下，使用以下命令：

third-party trendmicro

开启/关闭与趋势TDA设备互动

开启/关闭与趋势TDA设备进行互动，在第三方风险IP配置模式下，使用以下命令：

global-blacklist {**enable** | **disable**}

- **enable** – 开启与趋势TDA设备进行互动。
- **disable** – 关闭与趋势TDA设备的互动。

配置趋势TDA设备地址

配置设备与TDA设备联动的交互地址和端口号，在第三方风险IP配置模式下，使用以下命令：

query-server ip *ip-address* [**port** *port-number*]

- *ip-address* – 指定设备与TDA设备联动的交互地址。
- **port** *port-number* – 指定设备与TDA设备联动的交互端口号。范围是1到65535。

在第三方风险IP配置模式下，使用该命令no的形式恢复默认值， 默认值为**ip**： 0.0.0.0， **port**：443。

no query-server

配置与趋势TDA设备的互动请求周期

配置设备与TDA设备联动的互动请求周期，即获取黑名单的周期，在第三方风险IP配置模式下，使用以下命令：

query-cycle *cycle*

- *cycle* – 指定设备与TDA设备联动的互动请求周期， 范围是1到60，单位是分钟，默认值是30分钟。

在第三方风险IP配置模式下，使用该命令no的形式恢复默认值：

no query-cycle

开启/关闭沙箱互动

开启/关闭沙箱互动，即获取TDA设备沙箱分析的黑名单。在第三方风险IP配置模式下，使用以下命令：

sandbox-blacklist {**enable** | **disable**}

- **enable** – 开启沙箱互动。
- **disable** – 关闭沙箱互动。

查询用户自定义黑白名单

在任何模式下，输入以下命令查询用户自定义黑白名单信息：

show perimeter-traffic-filtering userdefined

查询黑白名单命中次数

在任何模式下，输入以下命令查询黑白名单命中次数：

show perimeter-traffic-filtering hit-count

查询黑白名单中指定IP的命中次数

在任何模式下，输入以下命令查询黑白名单中指定IP的命中次数：

show perimeter-traffic-filtering ip *ip-address*

显示趋势TDA相关配置信息

在任何模式下，输入以下命令显示趋势TDA相关配置信息：

show third-party trendmicro configuration

显示从趋势TDA获取的相关数据信息

在任何模式下，输入以下命令显示从趋势TDA获取的相关数据信息：

show third-party trendmicro statistics

IP信誉特征库更新配置

默认情况下，StoneOS会每日自动更新IP信誉特征库，用户可以根据需要更改IP信誉特征库更新配置。IP信誉特征库更新配置包括：

- 配置IP信誉特征库更新模式
- 配置更新服务器
- 指定更新时间
- 立即更新
- 导入IP信誉特征文件
- 显示IP信誉特征信息
- 显示IP信誉特征库更新配置信息

配置IP信誉特征库更新模式

系统支持手动和自动两种更新方式。配置IP信誉特征库更新方式，在全局配置模式下，使用以下命令：

ip-reputation update mode {**auto** | **manual**}

- **auto** – 指定自动更新IP信誉特征库。该方式为系统的默认更新方式。
- **manual** – 指定手动更新IP信誉特征库。

在全局配置模式下使用该命令no的形式恢复默认更新模式：

no ip-reputation update mode

配置更新服务器

系统提供默认的IP信誉特征库更新服务器，即update1.hillstonenet.com和update2.hillstonenet.com，同时用户也可以根据需要配置其它更新服务器下载最新IP信誉特征。最多可配置3个。配置更新服务器，在全局配置模式下，使用以下命令：

ip-reputation update {**server1** | **server2** | **server3**} {*ip-address* | *domain-name*}

- **server1** | **server2** | **server3** – 指定将要配置的服务器。**server1**的默认值为update1.hillstonenet.com，**server2**的默认值为update2.hillstonenet.com。
- **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）。

在全局配置模式下，使用该命令no的形式取消更新服务器的指定：

no ip-reputation signature update {**server1** | **server2** | **server3**}

指定HTTP代理服务器

当设备需要通过HTTP代理服务器访问互联网时，为确保特征库能够正常升级，需要在设备上指定代理服务器的IP地址和端口号。

为IP信誉特征库升级指定代理服务器，在全局配置模式下，使用如下命令：

ip-reputation update proxy-server {**main** | **backup**} *ip-address port-number*

- **main** | **backup** – 使用main参数指定主代理服务器，使用backup指定备份代理服务器。
- **ip-address** *port-number* – 指定代理服务器的IP地址和端口号。

取消指定的代理服务器，使用**no perimeter-traffic-filter update proxy-server** {**main** | **backup**}命令。

指定更新时间

默认情况下，系统采用自动模式每日更新IP信誉特征库，并且为避免服务器流量过大，每日更新时间是随机的。用户可以根据需要指定IP信誉特征库更新的频率和时间，在全局配置模式下，使用以下命令：

ip-reputation update schedule {**daily** [*HH:MM*] | **weekly** {**mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun**} | **hourly** *minute* }

- **daily** [*HH:MM*] – 指定频率为每天更新，*HH:MM* 用来指定更新的时间，例如09：00。不指定更新时间将按照系统默认的更新时间进行更新。

- **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。
- **hourly** *minute* – 指定频率为每小时更新，*minute*用来指定每小时更新的具体分钟时刻。

立即更新

无论更新模式为手动还是自动，用户都可以随时使用以下命令更新IP信誉特征库。立即更新IP信誉特征库，在任何模式下，使用以下命令：

exec ip-reputation update

- **exec av signature update** – 仅对当前IP信誉特征库与更新服务器最新发布IP信誉特征库的不同部分进行更新。

导入IP信誉特征文件

在某些情况下，用户设备可能无法连接到更新服务器对IP信誉特征库进行更新，针对这一问题，StoneOS提供IP信誉特征文件导入功能，即通过FTP、TFTP服务器或者U盘将IP信誉特征文件导入到设备，从而更新设备的IP信誉特征库。导入IP信誉特征文件，在执行模式下，使用以下命令：

import ip-reputation from {**ftp server** *ip-address* [**user** *user-name* **password** *password*] | **tftp server** *ip-address* } [**vrouter** *vr-name*] *file-name*

- *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。
- **vrouter** *vr-name* – 指定FTP或者TFTP服务器所属的VRouter。
- *file-name* – 指定导入的IP信誉特征文件的名称。

显示IP信誉特征库信息

用户可以随时使用相应的show命令查看设备的IP信誉特征库信息，包括IP信誉特征库版本、发布日期以及IP信誉特征个数等。查看IP信誉特征库信息，在任何模式下使用以下命令：

show ip-reputation info

显示IP信誉特征库更新配置信息

用户可以随时使用相应的show命令查看设备上的IP信誉特征库更新信息，包括更新服务器信息、更新模式、更新频率及时间以及IP信誉特征库更新状况等。查看IP信誉特征库更新配置信息，在任何模式下使用以下命令：

```
show ip-reputation update
```

风险减缓措施

风险减缓措施介绍

风险减缓措施，即系统能够动态识别网络中潜在的风险和攻击，针对符合规则触发条件的风险作出相应的行为限制。

风险减缓措施规则

风险减缓措施规则包括以下两类：

- 预定义规则：该规则是根据系统的风险减缓规则特征库，从云端同步的风险减缓规则。随着风险减缓规则特征库版本的不同，预定义规则不同。关于风险减缓规则特征库更新配置，请参阅“风险减缓规则特征库更新配置”。
- 自定义规则：用户根据需求，配置风险减缓措施规则，指定符合的触发条件以及限制行为。

注意:

- 风险减缓措施规则仅对Scan、DoS以及Spam类型的威胁适用。
- 不允许用户编辑或删除风险减缓措施规则的预定义规则。

自动风险减缓措施配置包括：

- 开启/关闭自动风险减缓
- 配置风险减缓措施规则
- 查看自动风险减缓启用状态

开启/关闭自动风险减缓

自动风险减缓，即针对符合触发条件的风险，系统自动下发限制行为动作，从而减缓风险和阻止威胁攻击。在开启自动风险减缓功能后，风险减缓措施规则（包括预定义规则和自定义规则）才能够生效。

开启/关闭自动风险减缓，在全局配置模式下，使用以下命令：

mitigation-status {**enable** | **disable**}

- **enable** – 开启自动风险减缓。
- **disable** – 关闭自动风险减缓。

配置风险减缓措施规则

风险减缓措施规则的配置，仅支持通过WebUI方式配置，具体配置方式请参阅《StoneOS WebUI用户手册》。

查看自动风险减缓启用状态

在任何模式下，输入以下命令查看自动风险减缓启用状态：

show mitigation-status

风险减缓规则特征库更新配置

默认情况下，系统会每日自动更新风险减缓规则特征库，用户可以根据需要更改风险减缓规则特征库更新配置。风险减缓规则特征库更新配置包括：

- 配置风险减缓规则特征库更新模式
- 指定风险减缓规则特征库自动更新周期
- 立即更新
- 导入风险减缓规则特征文件
- 显示风险减缓规则特征库更新配置信息

配置风险减缓规则特征库更新模式

风险减缓规则特征库支持手动和自动（周期性）两种更新方式。配置风险减缓规则特征库更新方式，在全局配置模式下，使用以下命令：

cloud mitigation mode {**1** | **2**}

- 1 – **manual**，指定手动更新风险减缓规则特征库。
- 2 – **period**，指定自动（周期性）更新风险减缓规则特征库。

指定风险减缓规则特征库自动更新周期

指定风险减缓规则特征库自动更新周期，在全局配置模式下，使用以下命令：

cloud mitigation period *period*

- **period** - 指定自动更新周期。范围为600到86400，单位为秒。

立即更新

无论更新模式为手动还是自动（周期性），用户都可以随时使用以下命令立即更新风险减缓规则特征库。立即更新风险减缓规则特征库，在任何模式下，使用以下命令：

exec cloud mitigation update

- **exec cloud mitigation update** – 仅对当前风险减缓规则特征库与更新服务器最新发布风险减缓规则特征库的不同部分进行更新。

导入风险减缓规则特征文件

在某些情况下，用户设备可能无法连接到更新服务器对风险减缓规则特征库进行更新，针对这一问题，StoneOS提供风险减缓规则特征文件导入功能，即通过FTP、TFTP服务器或者U盘将风险减缓规则特征文件导入到设备，从而更新设备的风险减缓规则特征库。导入风险减缓规则特征文件，在执行模式下，使用以下命令：

import cloud mitigation from {**ftp server** *ip-address* [**user** *user-name* **password** password] | **tftp server** *ip-address* } [**vrouter** *vr-name*] *file-name*

- *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。

- **vrouter** *vr-name* – 指定FTP或者TFTP服务器所属的VRouter。
- *file-name* – 指定导入的风险减缓规则特征文件的名称。

显示风险减缓规则特征库更新配置信息

用户可以随时使用相应的show命令查看设备上的风险减缓规则特征库更新信息，在任何模式下使用以下命令：

```
show cloud mitigation update
```

关联分析

系统提供关联分析引擎，对威胁防护各个模块产生的威胁事件进行关联分析。关联分析引擎针对已经生成的威胁事件，通过定义的一些规则，找出威胁事件的内在关联关系以及跨主机的威胁，从已有的威胁事件中找出潜在的高危害威胁。关联分析的结果，在系统WebUI的iCenter页面中的威胁标签页查看。

关联分析引擎/规则升级

关联分析引擎和规则的升级，随同异常行为模型库的更新而同步更新。对异常行为模型库的更新，请参阅 “"异常行为检测" 在第141页”章节。

核心资产

核心资产(Critical Assets)是指保障公司运行和获取收益的关键IT资产，包括各种服务器、网络设备以及数据存储设备等。由于核心资产在一个公司运营中占据的重要性，最有可能称为攻击者的首选目标。因此，核心资产相比于普通主机需要更高的关注的和防御优先级。

配置核心资产对象后，系统会自动在选择的安全域上开启高级威胁检测和异常行为检测功能，保证核心资产监控的优先级和资源，在iCenter的核心资产页面展现核心资产对象以及相关联的威胁和流量。

核心资产配置包括：

- 指定核心资产名称
- 指定核心资产IP地址
- 指定核心资产所在的安全域
- 查看核心资产对象配置

指定核心资产名称

指定核心资产名称，在全局配置模式下，使用如下命令：

critical-asset name *name*

- *name* – 指定核心资产的名称，并且进入该核心资产对象的配置模式。如果指定名称已存在，则直接进入该核心资产对象的配置模式。

使用**no critical-asset name** *name*删除指定的核心资产对象。

指定核心资产IP地址

指定核心资产的IP地址，在核心资产对象配置模式下，使用如下命令：

ip *ip-address*

- *ip-address* – 指定核心资产的IP地址。

使用**no ip**命令取消指定的IP地址。

指定核心资产所在的安全域

指定核心资产所在的安全域，在核心资产对象配置模式下，使用如下命令：

zone *zone-name*

- *zone-name* – 指定核心资产所在的安全域。此安全域的高级威胁检测和异常行为检测功能将自动开启。

使用**no zone**命令取消指定的安全域。

开启/关闭Web Server高级防护功能

Web Server高级防护功能用来检测HTTP协议类型的服务器的Web攻击，能够及时准确的发现异常行为。开启该功能，能够检测以下类型的攻击和行为：

- Web Vulnerability Scan：通过尝试各种访问方式和输入，探测web应用系统是否存在某些已知的安全漏洞。
- Http-based DoS Attack：基于HTTP协议的DoS攻击，利用HTTP协议本身的漏洞，使目标Server不能提供正常的服务，典型的如http request flood攻击。
- Web Spider ： Web爬虫是指定期收集网站内容的自动机，可用于搜索引擎或其它目的，一些不友好的Spider不遵守相关标准，会造成网站敏感信息泄露或较大的性能消耗。

开启Web Server高级防护功能，在核心资产对象配置模式下，使用以下命令：

mark-webserver

在核心资产对象配置模式下，使用该命令no的形式关闭Web Server高级防护功能：

no mark-webserver

核心资产重命名

在核心资产对象配置模式下，用户可以通过使用以下命令为核心资产重命名：

rename *new-name*

- *new-name* – 指定核心资产的新名称。

查看核心资产对象配置

使用**show critical-asset object**命令查看各个核心资产的配置信息。

威胁地理信息库

威胁地理信息库介绍

系统可以通过WebUI页面展示外部威胁地图，用户可以根据所选择的威胁或风险主机，查看该威胁的攻击主机或该风险主机来源区域。使用该功能前，需要先更新威胁地理信息库。

注意: 目前仅支持通过CLI方式更新威胁地理信息库。

威胁地理信息库更新配置

默认情况下，系统会每日自动更新威胁地理信息库，用户可以根据需要更改威胁地理信息库更新配置。威胁地理信息库更新配置包括：

- 配置威胁地理信息库更新模式
- 配置更新服务器
- 指定自动更新时间
- 立即更新
- 导入威胁地理信息库文件
- 显示威胁地理信息库信息
- 显示威胁地理信息库更新配置信息

配置威胁地理信息库更新模式

系统支持手动和自动两种更新方式。配置威胁地理信息库更新方式，在全局配置模式下，使用以下命令：

```
geolocation-IP-signature update mode {auto | manual}
```

- **auto** – 指定自动更新威胁地理信息库。该方式为系统的默认更新方式。
- **manual** – 指定手动更新威胁地理信息库。

在全局配置模式下使用该命令no的形式恢复默认更新模式：

no geolocation-IP-signature update mode

配置更新服务器

系统提供默认的威胁地理信息库更新服务器，即update1.hillstonenet.com和update2.hillstonenet.com，同时用户也可以根据需要配置其它更新服务器下载最新威胁地理信息。最多可配置3个。配置更新服务器，在全局配置模式下，使用以下命令：

geolocation-IP-signature update {**server1** | **server2** | **server3**} {*ip-address* | *domain-name*}

- **server1 | server2 | server3** – 指定将要配置的服务器。**server1**的默认值为update1.hillstonenet.com，**server2**的默认值为update2.hillstonenet.com。
- *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）。

在全局配置模式下，使用该命令no的形式取消更新服务器的指定：

no geolocation-IP-signature update {**server1** | **server2** | **server3**}

指定HTTP代理服务器

当设备需要通过HTTP代理服务器访问互联网时，为确保特征库能够正常升级，需要在设备上指定代理服务器的IP地址和端口号。

为威胁地理信息库升级指定代理服务器，在全局配置模式下，使用如下命令：

geolocation-ip-signature update proxy-server {**main** | **backup**} *ip-address port-number*

- **main | backup** – 使用main参数指定主代理服务器，使用backup指定备份代理服务器。
- *ip-address port-number* – 指定代理服务器的IP地址和端口号。

取消指定的代理服务器，使用**no geolocation-ip-signature update proxy-server** {**main** | **backup**}命令。

指定更新时间

默认情况下，系统采用自动模式每日更新威胁地理信息库，并且为避免服务器流量过大，每日更新时间是随机的。用户可以根据需要指定威胁地理信息库更新的频率和时间，在全局配置模式下，使用以下命令：

geolocation-IP-signature update schedule {**daily** | **weekly** {**mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun**}} [*HH:MM*]

- **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。

立即更新

无论更新模式为手动还是自动，用户都可以随时使用以下命令更新威胁地理信息库。立即更新威胁地理信息库，在任何模式下，使用以下命令：

exec geolocation-IP-signature update [full]

- **exec geolocation-IP-signature update** – 仅对当前威胁地理信息库与更新服务器最新发布威胁地理信息库的不同部分进行更新。
- **full** – 强制升级当前威胁地理信息库。

导入威胁地理信息库文件

在某些情况下，用户设备可能无法连接到更新服务器对威胁地理信息库进行更新，针对这一问题，系统提供威胁地理信息库文件导入功能，即通过FTP、TFTP服务器或者U盘将威胁地理信息库文件导入到设备，从而更新设备的威胁地理信息库。导入威胁地理信息库文件，在执行模式下，使用以下命令：

import geolocation-IP-signature from {**ftp server** *ip-address* [**user** *user-name* **password** *password*] | **tftp server** *ip-address* } [**vrouter** *vr-name*] *file-name*

- *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。
- **vrouter** *vr-name* – 指定FTP或者TFTP服务器所属的VRouter。
- *file-name* – 指定导入的威胁地理信息库文件的名称。

显示威胁地理信息库信息

用户可以随时使用相应的show命令查看设备的威胁地理信息库信息，包括威胁地理信息库版本、发布日期等。查看威胁地理信息库信息，在任何模式下使用以下命令：

```
show geolocation-IP-signature info
```

显示威胁地理信息库更新配置信息

用户可以随时使用相应的show命令查看设备上的威胁地理信息库更新信息，包括更新服务器信息、更新模式、更新频率及时间以及威胁地理信息库更新状况等。查看威胁地理信息库更新配置信息，在任何模式下使用以下命令：

```
show geolocation-IP-signature update
```

僵尸网络C&C防御

僵尸网络，是指采用一种或多种传播手段，使大量主机感染僵尸程序，从而在控制者和被感染主机之间所形成的一个可一对多控制的网络，对用户的网络安全以及数据安全造成很大的威胁隐患。

系统的僵尸网络C&C防御功能能够根据特征库中的地址及时发现用户内网的僵尸主机，并且根据配置对发现的僵尸主机进行处理，从而避免发生进一步的威胁攻击。

系统支持基于安全域和基于策略的僵尸网络C&C防御配置方式。为安全域配置僵尸网络C&C防御规则后，系统将会对以绑定安全域为目的安全域的流量根据僵尸网络C&C防御规则配置进行僵尸网络C&C检查。将僵尸网络C&C防御规则绑定到策略规则后，系统将会对与策略规则相匹配的流量根据规则配置进行僵尸网络C&C检查。

注意: 僵尸网络C&C防御功能受许可证控制，即为支持僵尸网络C&C防御功能的设备安装僵尸网络C&C防御许可证后，功能才可使用。

僵尸网络C&C防御配置准备工作

使用僵尸网络C&C防御功能前，必须完成以下准备工作：

1. 确认系统版本支持僵尸网络C&C防御功能。
2. 安装僵尸网络C&C防御许可证，然后重启设备。设备成功重启后，僵尸网络C&C防御功能即处于开启状态。

用户可以通过**show version**命令查看僵尸网络C&C防御功能是否开启。开启或者关闭僵尸网络C&C防御功能，在任何模式下使用以下命令：

exec botnet-c2-prevention {**enable** | **disable**}

- **enable** – 开启系统的僵尸网络C&C防御功能。
- **disable** – 关闭系统的僵尸网络C&C防御功能。

配置僵尸网络C&C防御功能

实现系统的僵尸网络C&C防御功能，用户需要按照以下步骤进行操作：

1. 开启僵尸网络C&C防御功能。

2. 定义僵尸网络C&C防御Profile，在Profile中指定扫描协议、系统发现僵尸网络后采取的动作。

3. 绑定僵尸网络C&C防御Profile到适当的策略规则或者将僵尸网络C&C防御Profile绑定到安全域。

注意: 初次使用僵尸网络C&C防御功能，需要首先更新僵尸网络C&C防御特征库。关于僵尸网络C&C防御特征库更新配置，请参阅“僵尸网络C&C防御特征库更新配置”。为保证能够正常连接到默认更新服务器，请在更新前为设备配置DNS服务器。

创建僵尸网络C&C防御Profile

僵尸网络C&C防御Profile中主要指定需要C&C检查的协议类型，以及系统发现僵尸主机后的动作。创建僵尸网络C&C防御Profile，在全局配置模式下使用以下命令：

botnet-c2-prevention profile *profile-name*

- *profile-name* - 指定所创建的僵尸网络C&C防御Profile的名称，并且进入该僵尸网络C&C防御Profile的配置模式。如果指定名称已存在，则直接进入僵尸网络C&C防御Profile配置模式。

使用**no botnet-c2-prevention** *profile-name*删除指定的僵尸网络C&C防御 Profile。

指定协议类型及控制动作

指定协议类型及控制动作，在僵尸网络C&C防御Profile配置模式下，使用以下命令：

botnet-c2-prevention protocol {**tcp** | **http** | **dns** }**action** {**reset**| **log-only** }

- **tcp** – 指定对通过TCP协议传输的信息进行僵尸网络C&C防御检查。
- **http** – 指定对通过HTTP协议传输的信息进行僵尸网络C&C防御检查。
- **dns** – 指定对通过DNS协议传输的信息进行僵尸网络C&C防御检查。

- **action** { **reset** | **log-only** } – 指定采取的动作。
- **reset** – 指定该参数后，系统发现僵尸主机后，重置恶意链接连接，并记录威胁日志。
- **log-only** – 指定该参数后，系统发现僵尸主机后，对流量放行，仅记录日志信息（威胁日志），该选项采取的默认动作。

使用以上命令no的形式取消协议类型的指定：

no botnet-c2-prevention protocol {**tcp** | **http** | **dns** }

启用/禁用指定IP/域名的特征

用户可以在全局配置模式下，用户可以通过使用以下命令禁用特征库中指定IP/域名的地址特征条目：

botnet-c2-prevention signature *signature-string* **disable**

- *signature-string* – 指定需要禁用的地址特征条目。

使用以上命令no的形式启用特征库中指定IP/域名的地址特征条目：

no botnet-c2-prevention signature *signature-string* **disable**

绑定僵尸网络C&C防御Profile到安全域

将僵尸网络C&C防御Profile绑定到安全域后，系统将会对以该安全域为目的安全域的流量按照Profile配置进行僵尸网络C&C防御检查。当策略规则已经绑定了僵尸网络C&C防御Profile，同时策略规则的目的安全域也绑定了僵尸网络C&C防御Profile，策略规则绑定的僵尸网络C&C防御Profile将会生效，而目的安全域绑定的僵尸网络C&C防御Profile无效。

绑定僵尸网络C&C防御Profile到安全域，在安全域配置模式下，使用以下命令：

botnet-c2-prevention enable *profile-name*

- *profile-name* – 指定绑定到安全域的僵尸网络C&C防御Profile的名称。一个安全域只能绑定一个僵尸网络C&C防御Profile。

在安全域配置模式下，使用该命令no的形式取消僵尸网络C&C防御Profile的绑定：

no botnet-c2-prevention enable

绑定僵尸网络C&C防御Profile到策略规则

将僵尸网络C&C防御Profile绑定到策略规则后，系统将会对与策略规则相匹配的流量根据Profile配置进行僵尸网络C&C防御检查。绑定僵尸网络C&C防御Profile到策略规则，在策略规则配置模式下使用以下命令：

botnet-c2-prevention *profile-name*

- *profile-name* – 指定绑定到策略规则的僵尸网络C&C防御Profile的名称。

在策略规则配置模式下使用该命令no的形式取消僵尸网络C&C防御Profile的绑定：**no botnet-c2-prevention**

显示僵尸网络C&C防御profile信息

在任何模式下，输入以下命令显示僵尸网络C&C防御profile信息：

show botnet-c2-prevention-profile *profile-name*

显示僵尸网络C&C防御状态

在任何模式下，输入以下命令显示僵尸网络C&C防御状态信息：

show botnet-c2-prevention status

僵尸网络C&C防御特征库更新配置

默认情况下，系统会每日自动更新僵尸网络C&C防御特征库，用户可以根据需要更改僵尸网络C&C防御特征库更新配置。僵尸网络C&C防御特征库更新配置包括：

- 配置僵尸网络C&C防御特征库更新模式
- 配置更新服务器
- 指定HTTP代理服务器
- 指定更新时间
- 立即更新

- 导入僵尸网络C&C防御特征文件
- 显示僵尸网络C&C防御特征信息
- 显示僵尸网络C&C防御特征库更新配置信息

配置僵尸网络C&C防御特征库更新模式

系统支持手动和自动两种更新方式。配置僵尸网络C&C防御特征库更新方式，在全局配置模式下，使用以下命令：

botnet-c2-prevention signature update mode {**auto** | **manual**}

- **auto** – 指定自动更新僵尸网络C&C防御特征库。该方式为系统的默认更新方式。
- **manual** – 指定手动更新僵尸网络C&C防御特征库。

在全局配置模式下使用该命令no的形式恢复默认更新模式：

no botnet-c2-prevention signature update mode

配置更新服务器

系统提供默认的僵尸网络C&C防御特征库更新服务器，即update1.hillstonenet.com和update2.hillstonenet.com，同时用户也可以根据需要配置其它更新服务器下载最新C&C防御特征。最多可配置3个。配置更新服务器，在全局配置模式下，使用以下命令：

botnet-c2-prevention signature update {**server1** | **server2** | **server3**} {*ip-address* | *domain-name*}

- **server1** | **server2** | **server3** – 指定将要配置的服务器。**server1**的默认值为update1.hillstonenet.com，**server2**的默认值为update2.hillstonenet.com。
- *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）。

在全局配置模式下，使用该命令no的形式取消更新服务器的指定：

no botnet-c2-prevention signature update {**server1** | **server2** | **server3**}

指定HTTP代理服务器

当设备需要通过HTTP代理服务器访问互联网时，为确保特征库能够正常升级，需要在设备上指定代理服务器的IP地址和端口号。

为僵尸网络C&C防御特征库升级指定代理服务器，在全局配置模式下，使用如下命令：

botnet-c2-prevention signature update proxy-server {**main** | **backup**} *ip-address port-number*

- **main** | **backup** – 使用main参数指定主代理服务器，使用**backup**指定备份代理服务器。
- *ip-address port-number* – 指定代理服务器的IP地址和端口号。

取消指定的代理服务器，使用**no botnet-c2-prevention signature update proxy-server** {**main** | **backup**}命令。

指定更新时间

默认情况下，系统采用自动模式每日更新僵尸网络C&C防御特征库，并且为避免服务器流量过大，每日更新时间是随机的。用户可以根据需要指定僵尸网络C&C防御特征库更新的频率和时间，在全局配置模式下，使用以下命令：

botnet-c2-prevention signature update schedule {{**daily** | **weekly** {**mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun**}} [*HH:MM*] | **hourly** *MM* }

- **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。
- **hourly** *MM*– 指定频率为每小时更新。MM为分钟数。

立即更新

无论更新模式为手动还是自动，用户都可以随时使用以下命令更新僵尸网络C&C防御特征库。立即更新僵尸网络C&C防御特征库，在任何模式下，使用以下命令：

exec botnet-c2-prevention signature update

- **exec botnet-c2-prevention signature update** – 仅对当前僵尸网络C&C防御特征库与更新服务器最新发布僵尸网络C&C防御特征库的不同部分进行更新。

导入僵尸网络C&C防御特征文件

在某些情况下，用户设备可能无法连接到更新服务器对僵尸网络C&C防御特征库进行更新，针对这一问题，系统提供僵尸网络C&C防御特征文件导入功能，即通过FTP、TFTP服务器或者U盘将僵尸网络C&C防御特征文件导入到设备，从而更新设备的僵尸网络C&C防御特征库。导入僵尸网络C&C防御特征文件，在执行模式下，使用以下命令：

import botnet-c2-prevention signature from {**ftp server** *ip-address* [**user** *user-name* **password** *password*] | **tftp server** *ip-address* | **usb0** | **usb1** } [**vrouter** *vr-name*] *file-name*

- *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。
- **vrouter** *vr-name* – 指定FTP或者TFTP服务器所属的VRouter。
- *file-name* – 指定导入的僵尸网络C&C防御特征文件的名称。

显示僵尸网络C&C防御特征库信息

用户可以随时使用相应的show命令查看设备的僵尸网络C&C防御特征库信息。在任何模式下使用以下命令：

show botnet-c2-prevention signature info

显示僵尸网络C&C防御特征库更新配置信息

用户可以随时使用相应的show命令查看设备上的僵尸网络C&C防御特征库更新信息，包括更新服务器信息、更新模式、更新频率及时间以及僵尸网络C&C防御特征库更新状况等。查看僵尸网络C&C防御特征库更新配置信息，在任何模式下使用以下命令：

```
show botnet-c2-prevention signature update
```

垃圾邮件过滤

垃圾邮件过滤功能介绍

系统的垃圾邮件过滤功能能够通过垃圾邮件过滤云端服务器对SMTP、POP3协议传输的邮件进行识别过滤，及时发现邮件携带的威胁，例如垃圾邮件、钓鱼邮件、蠕虫病毒邮件等，并且根据配置对发现的垃圾邮件进行处理，从而保护用户的邮件客户端或邮件服务器。

垃圾邮件过滤功能受许可证控制，即为支持垃圾邮件过滤功能的设备安装反垃圾邮件过滤许可证后，功能才可使用。

注意: 为保证能够正常连接到垃圾邮件过滤云端服务器，请在配置垃圾邮件过滤功能前为设备配置DNS服务器。

配置垃圾邮件过滤功能

系统支持基于安全域和基于策略的垃圾邮件过滤配置方式。

通过CLI配置垃圾邮件过滤功能，请按照以下步骤进行操作：

1. 定义垃圾邮件过滤Profile，在Profile中指定需要进行过滤的邮件协议类型、垃圾邮件类别、采取的控制动作以及发件人免监控域。
2. 将垃圾邮件过滤Profile绑定到安全域/策略规则。

创建垃圾邮件过滤Profile

垃圾邮件过滤Profile中主要指定需要进行过滤的邮件协议类型、垃圾邮件类别、采取的控制动作以及发件人免监控域。创建垃圾邮件过滤Profile，在全局配置模式下使用以下命令：

antispam-profile *antispam-profile-name*

- *antispam-profile-name* - 指定所创建的垃圾邮件过滤Profile的名称，并且进入该垃圾邮件过滤Profile的配置模式。如果指定名称已存在，则直接进入垃圾邮件过滤Profile配置模式。最多可以新建32个垃圾邮件过滤Profile。

使用**no antispam-profile** *antispam-profile-name*删除指定的垃圾邮件过滤Profile。

指定邮件协议类型

指定邮件协议类型并进入邮件协议配置模式，在垃圾邮件过滤Profile配置模式下使用以下命令：

protocol {**pop3** | **smtp**}

- **pop3** – 指定对通过POP3协议传输的邮件进行垃圾邮件过滤。
- **smtp** – 指定对通过SMTP协议传输的邮件进行垃圾邮件过滤 。

使用以上命令no的形式取消协议类型的指定：

no protocol{ **pop3** | **smtp** }

指定垃圾邮件类别

指定所指定协议下的垃圾邮件类别以及采取的控制动作，在邮件协议配置模式下使用以下命令：

spam-class {**bulk** | **confirmed** | **suspected** | **validbulk**} **action** { **log-only** | **reset** }

- **bulk** – 指定对恶意群发类型的邮件采取控制动作。
- **confirmed** – 指定对确定为垃圾邮件的邮件采取控制动作。
- **suspected** – 指定对可疑垃圾邮件类型的邮件采取控制动作。
- **validbulk** – 指定对正常群发邮件类型的邮件采取控制动作。
- **action** { **log-only** | **reset** } – 指定对发现的垃圾邮件采取的动作。
- **log-only** – 记录日志信息。该选项为发现垃圾邮件时系统采取的默认动作。对使用POP3协议传输的垃圾邮件仅支持记录日志动作（log-only）。
- **reset** – 发现垃圾邮件后，重置连接。

使用以上命令no的形式取消垃圾邮件类别的指定：

no spam-class {**bulk** | **confirmed** | **suspected** | **validbulk**}

配置发件人免监控域

对于指定的发件人免监控域，系统将不对其进行垃圾邮件的过滤。每一个垃圾邮件过滤Profile最多可指定16个发件人免监控域。

配置发件人免监控域，在垃圾邮件过滤Profile配置模式下使用以下命令：

sender-exempt-domain *domain-name*

- *domain-name* – 指定免监控域的名称。域名名称长度可以是1到255个字符。如果是多级邮件域名，每一级域名长度最多不能超过63个字符。

使用以上命令no的形式删除指定的发件人免监控域：

no sender-exempt-domain *domain-name*

绑定垃圾邮件过滤Profile到安全域

将垃圾邮件过滤Profile绑定到安全域后，系统将会对以该安全域为目的安全域的流量按照Profile配置进行垃圾邮件过滤检查。当策略规则已经绑定了垃圾邮件过滤Profile，同时策略规则的目的安全域也绑定了垃圾邮件过滤Profile，策略规则绑定的垃圾邮件过滤Profile将会生效，而目的安全域绑定的垃圾邮件过滤Profile无效。

绑定垃圾邮件过滤Profile到安全域，在安全域配置模式下，使用以下命令：

antispam *antispam-profile-name*

- *antispam-profile-name* – 指定绑定到安全域的垃圾邮件过滤Profile的名称。一个安全域只能绑定一个垃圾邮件过滤Profile。

在安全域配置模式下，使用该命令no的形式取消垃圾邮件过滤Profile的绑定：

no antispam

绑定垃圾邮件过滤Profile到策略规则

将垃圾邮件过滤Profile绑定到策略规则后，系统将会对与策略规则相匹配的流量根据Profile配置进行垃圾邮件过滤检查。绑定垃圾邮件过滤Profile到策略规则，在策略规则配置模式下使用以下命令：

antispam *antispam-profile-name*

- *antispam-profile-name* – 指定绑定到策略规则的垃圾邮件过滤Profile的名称。

在策略规则配置模式下使用该命令no的形式取消垃圾邮件过滤Profile的绑定：*no antispam*

配置邮件扫描最大限制

指定邮件扫描最大限制值，在全局配置模式下，使用以下命令：

antispam max-mail-size *max-mail-size-value*

- *max-mail-size-value* – 指定邮件扫描最大限制值。范围是512到2048Kb，默认值是1024Kb。

在全局配置模式下使用该命令no的形式恢复邮件扫描最大限制默认值：**no antispam** *max-mail-size*

显示垃圾邮件过滤Profile信息

在任何模式下，输入以下命令显示垃圾邮件过滤Profile信息：

show antispam-profile [*antispam-profile-name*]

- *antispam-profile-name* – 显示指定垃圾邮件过滤Profile的信息。若不指定Profile名称，显示系统中所有垃圾邮件过滤Profile的信息。

显示垃圾邮件过滤状态信息

在任何模式下，输入以下命令显示垃圾邮件过滤状态信息：

show antispam status

显示垃圾邮件过滤全局配置信息

在任何模式下，输入以下命令显示垃圾邮件过滤全局配置信息：

show antispam configuration

终端防护

终端安全控制中心用来监测各接入终端的安全状态以及终端的系统信息。

系统的终端防护功能是通过与终端安全控制中心进行联动交互，获取终端安全控制中心监测的终端数据信息，并且能够根据终端的安全状态指定相应的处理动作，从而达到控制终端网络行为的目的。

注意:

- 目前终端防护功能仅支持与“江民科技”终端安全控制中心进行联动。
- 终端防护功能受许可证控制，即为支持终端防护功能的设备安装终端防护许可证后，功能才可使用。

配置终端防护

准备工作

使用终端防护功能前，必须完成以下准备工作：

1. 确认系统版本支持终端防护功能。
2. 安装终端防护许可证，然后重启设备。

配置终端防护功能

实现系统的终端防护功能，用户需要按照以下步骤进行操作：

1. 配置终端安全控制中心服务器参数。
2. 定义终端防护Profile，在Profile中指定终端状态对应的防护动作。
3. 绑定终端防护Profile到适当的策略规则或者将终端防护Profile绑定到安全域。

配置终端安全控制中心参数

终端安全控制中心服务器参数配置包括：

- 指定终端安全控制中心服务器名称
- 指定终端安全控制中心服务器地址
- 指定终端安全控制中心服务器端口号
- 指定同步周期

指定终端安全控制中心服务器类型

指定终端安全控制中心服务器类型为江民，并且进入终端安全控制中心服务器配置模式，在全局配置模式下，使用以下命令：

```
epp server jiangmin
```

使用**no epp server**删除指定的终端安全控制中心服务器。

注意: 系统仅支持配置一个相同类型的终端安全控制中心服务器。

指定终端安全控制中心服务器地址

指定终端安全控制中心服务器地址，在终端安全控制中心服务器配置模式下，使用以下命令：

host *hostname*

- *hostname* - 指定终端安全控制中心服务器IP地址或域名，范围是1到255字符。

使用**no host**删除指定的终端安全控制中心服务器地址。

指定终端安全控制中心服务器端口号

指定终端安全控制中心服务器端口号，在终端安全控制中心服务器配置模式下，使用以下命令：

port *port-number*

- *port-number* - 指定端口号。范围是1到65535，默认端口号为80。

使用**no port**删除指定的终端安全控制中心服务器端口号。

指定同步周期

指定设备与终端安全控制中心同步终端数据信息的周期，在终端安全控制中心服务器配置模式下，使用以下命令：

sync *sync-cycle*

- *sync-cycle* - 指定同步周期。范围是1到60分钟，默认周期为10分钟。

使用**no sync**恢复默认同步周期。

启用/禁用同步信息

默认情况下，系统已同步的终端数据信息处于禁用状态。当设备与终端安全控制中心断开连接后，并且在经过两个同步周期后仍未恢复连接，系统已同步到的信息无效并将会被清空。用户可以根据需要启用同步信息，继续使用系统最后一次已同步到的终端数据信息。

启用或禁用同步信息，在终端安全控制中心服务器配置模式下，使用以下命令：

- 启用：**timeout-used**
- 禁用：**no timeout-used**

创建终端防护Profile

终端防护Profile中主要指定终端状态对应的防护动作。创建终端防护Profile，在全局配置模式下使用以下命令：

epp-profile *profile-name*

- *profile-name* - 指定所创建的终端防护Profile的名称，并且进入该终端防护Profile的配置模式。如果指定名称已存在，则直接进入终端防护Profile配置模式。

使用**no epp-profile** *profile-name*删除指定的终端防护Profile。

指定终端状态对应的防护动作

指定对状态为未安装杀毒客户端的终端执行的防护动作，在终端防护Profile配置模式下，使用以下命令：

status uninstall { **log-only** | **redirect** *url* | **block** [*block-interval*]}

- **log-only** – 指定对未安装客户端的终端流量放行，仅记录日志信息
- **redirect** *url* – 对未安装客户端的终端连接重定向到指定的*url*。
- **block** [*block-interval*] – 指定对未安装客户端的终端进行阻断连接，并指定阻断时长*block-interval*。

使用以上命令no的形式取消对状态为未安装杀毒客户端的终端执行的防护动作的指定：

no status uninstall

指定对状态为健康指数低、已中毒、行为异常的终端执行的防护动作，在终端防护Profile配置模式下，使用以下命令：

status { **unhealthy** | **infected** | **abnormal** } { **log-only** | **block** [*block-interval*]}

- **unhealthy** – 指定对状态为健康指数低的终端执行防护动作。
- **infected** – 指定对状态为已中毒的终端执行防护动作。
- **abnormal** – 指定对状态为行为异常的终端执行防护动作。
- **log-only** – 指定防护动作为仅记录日志信息。
- **block** [*block-interval*] –对指定状态的终端进行阻断连接，并指定阻断时长 *block-interval*。

使用以上命令no的形式取消对状态为健康指数低、已中毒、行为异常的终端执行的防护动作的指定：

no status { **unhealthy** | **infected** | **abnormal** }

指定例外地址

例外地址为不受终端防护Profile控制的终端地址。指定例外地址，在终端防护Profile配置模式下，使用以下命令：

address *address-name*

- *address-name* - 指定引用的地址簿名称。

使用以上命令no的形式取消对例外地址的指定：

no address

注意: 在指定例外地址前，需要提前将例外的终端地址添加到地址簿中。具体配置方式，请参阅配置地址簿。

绑定终端防护Profile到安全域

将终端防护Profile绑定到安全域后，系统将会对以该安全域为源安全域的流量按照Profile配置进行终端防护检查。

绑定终端防护Profile到安全域，在安全域配置模式下，使用以下命令：

epp enable *profile-name*

- *profile-name* – 指定绑定到安全域的终端防护Profile的名称。一个安全域只能绑定一个终端防护Profile。

在安全域配置模式下，使用该命令no的形式取消终端防护Profile的绑定：

```
no epp enable
```

绑定终端防护Profile到策略规则

将终端防护Profile绑定到策略规则后，系统将会对与策略规则相匹配的流量根据Profile配置进行终端防护。绑定终端防护Profile到策略规则，在策略规则配置模式下使用以下命令：

```
epp profile-name
```

- *profile-name* – 指定绑定到策略规则的终端防护Profile的名称。

在策略规则配置模式下使用该命令no的形式取消终端防护Profile的绑定：**no epp**

手动同步终端数据信息

用户可以在任何模式下使用以下命令进行手动同步终端数据信息：

```
exec epp jiangmin server-flush
```

显示终端防护profile信息

在任何模式下，输入以下命令显示终端防护profile信息：

```
show epp-profile [profile-name]
```

显示终端状态信息

在任何模式下，输入以下命令显示终端状态信息：

```
show epp ep-status {jiangmin | dp}
```

- **jiangmin** – 显示从江民终端安全控制中心获取的终端状态信息。
- **dp** – 系统将相同信息处理为一条信息后，显示从所有第三方终端安全控制中心获取的终端状态信息，供终端防护Profile使用。

显示终端信息同步状态

在任何模式下，输入以下命令显示终端信息同步状态信息：

```
show epp sync-status
```

显示终端安全控制中心信息

在任何模式下，输入以下命令显示终端安全控制中心信息：

```
show epp server
```

IoT监控

物联网（Internet of Things）简称为IoT，是指将大量物理设备（如网络视频监控设备）实现互联互通的网络。

系统的IoT监控功能是通过分析流经设备的流量，识别视频监控专网中的IPC（网络摄像机）和NVR（网络硬盘录像机）等网络视频监控设备，并对识别出的设备进行实时监控，然后根据配置对出现非法行为的网络视频监控设备进行阻断等操作。

注意:

- 目前IoT监控功能仅支持识别海康威视、大华和宇视的IPC和NVR设备。
- IoT监控功能受许可证控制，即为支持IoT监控功能的设备安装IoT管控许可证后，功能才可使用。
- IoT监控功能不支持识别处于NAT场景下的网络视频监控设备。

配置IoT监控

准备工作

使用IoT监控功能前，必须完成以下准备工作：

1. 确认系统版本支持IoT监控功能。
2. 安装IoT管控许可证，然后重新登录设备。

配置IoT监控功能

实现系统的IoT监控功能，用户需要按照以下步骤进行操作：

1. 配置准入名单。
2. 定义IoT监控Profile，在Profile中指定准入名单、终端行为监控对应的动作等。
3. 将IoT监控Profile绑定到安全域。

配置准入名单

对于经过绑定IoT监控Profile安全域的流量，系统支持配置IP、MAC或IP/MAC类型准入名单对其进行限制。配置之后，系统仅允许命中准入名单的流量通过。默认情况下，系统允许经过绑定IoT监控Profile安全域的所有流量通过。

当同时配置IP/MAC、IP和MAC类型的准入名单时，流量匹配的顺序为：IP/MAC > IP > MAC。当符合以下情况时，系统允许流量通过：

- 当流量匹配IP/MAC类型的准入名单时，IP地址和MAC地址均匹配成功。
- 当流量匹配IP/MAC类型的准入名单时，仅IP地址匹配成功。之后流量依次匹配IP类型的准入名单和MAC类型的准入名单，且均匹配成功。

创建准入名单

创建准入名单，并且进入IoT准入名单配置模式，在全局配置模式下，使用以下命令：

```
iot-monitor admittance-list list-name
```

- *list-name* - 指定准入名单的名称，并且进入IoT准入名单配置模式。如果指定名称已存在，则直接进入IoT准入名单配置模式。

在全局配置模式下，使用**no iot-monitor admittance-list** *list-name*删除指定的准入名单。

注意: 被绑定到IoT监控Profile的准入名单只有在解除绑定后，才可以进行删除。

配置IP/MAC类型的准入名单

将允许通过的网络视频监控设备的IP地址、MAC地址、用户名和密码添加到准入名单中，在IoT准入名单配置模式下，使用以下命令：

ip-mac *ip-address mac-address* [**onvifusername** *username* **onvifpassword** *password*]

- *ip-address* - 指定网络视频监控设备的IP地址。
- *mac-address* - 指定与配置的IP地址对应的MAC地址。
- *username* - 指定管理网络视频监控设备的用户名。
- *password* - 指定与用户名对应的密码。

在IoT准入名单配置模式下，使用**no ip-mac** *ip-address mac-address*从准入名单中删除指定网络视频监控设备的IP地址和MAC地址。

配置IP类型的准入名单

指定IP网段

将允许通过的网络视频监控设备所在IP网段、用户名和密码添加到准入名单中，在IoT准入名单配置模式下，使用以下命令：

ip network {*ip-prefix/mask* | *ip-address mask*} [**onvifusername** *username* **onvifpassword** *password*]

- *ip-prefix/mask* - 指定网络视频监控设备所在网段的IP地址和子网掩码，如1.1.1.1/24。
- *ip-address* - 指定网络视频监控设备所在网段的IP地址，如1.1.1.1。
- *mask* - 指定网络视频监控设备所在网段的网络掩码，如255.255.255.0。
- *username* - 指定管理网络视频监控设备的用户名。
- *password* - 指定与用户名对应的密码。

在IoT准入名单配置模式下，使用**no ip network** {*ip-prefix/mask* | *ip-address mask*}从准入名单中删除指定网络视频监控设备所在的IP网段。

注意: 当配置的IP网段与已配置IP地址存在冲突时，系统会出现错误提示。

指定IP地址范围

将允许通过的网络视频监控设备所在IP地址范围、用户名和密码添加到准入名单中，在IoT准入名单配置模式下，使用以下命令：

ip range *start-ip end-ip* [**onvifusername** *username* **onvifpassword** *password*]

- *start-ip* - 指定网络视频监控设备所在IP地址范围的起始IP地址。
- *end-ip* - 指定网络视频监控设备所在IP地址范围的结束IP地址。
- *username* - 指定管理网络视频监控设备的用户名。
- *password* - 指定与用户名对应的密码。

在IoT准入名单配置模式下，使用**no ip network** *start-ip end-ip*从准入名单中删除指定网络视频监控设备所在的IP地址范围。

注意: 当配置的IP范围与已配置IP地址存在冲突时，系统会出现错误提示。

配置MAC类型的准入名单

将允许通过的网络视频监控设备的MAC地址添加到准入名单中，在IoT准入名单配置模式下，使用以下命令：

mac *mac-address*

- *mac-address*- 指定网络视频监控设备的MAC地址。

在IoT准入名单配置模式下，使用**no mac** *mac-address*从准入名单中删除指定网络视频监控设备的MAC地址。

导入准入名单

用户可以通过FTP或TFTP服务器导入准入名单。从FTP或TFTP服务器导入准入名单，在执行模式下使用以下命令：

import iot-monitor admittance-list *list-name* **from** {**ftp server** *ip-address* **user** *user-name* **password** *password* [**vrouter** *vrouter-name*] | **tftp server** *ip-address* [**vrouter** *vrouter-name*] | {**usb0** | **usb1**} *file-name*

- *list-name*- 指定导入的目标准入名单的名称。
- *ip-address*- 指定FTP或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。
- *vrouter-name* - 为指定的VRouter导入准入名单。如果不指定该参数，VRouter为trust-vr。
- *file-name* - 指定FTP服务器或TFTP服务器上准入名单文件的名称。

配置IoT监控Profile

创建IoT监控Profile

创建IoT监控Profile，并且进入IoT监控Profile配置模式，在全局配置模式下，使用以下命令：

iot-monitor profile *profile-name*

- *Profile-name* - 指定IoT监控Profile的名称，并且进入IoT监控Profile配置模式。如果指定名称已存在，则直接进入IoT监控Profile配置模式。

在全局配置模式下，使用**no iot-monitor profile** *profile-name*删除指定的IoT监控Profile。

注意: 被绑定到安全域的IoT监控Profile只有在解除绑定后，才可以进行删除。

绑定准入名单到IoT监控Profile

绑定已创建的准入名单到IoT监控Profile，在IoT监控Profile配置模式下，使用以下命令：

iot-admittance-list *list-name*

- *list-name* - 指定绑定到IoT监控Profile的准入名单的名称。一个IoT监控Profile仅允许绑定一个准入名单。

在IoT监控Profile配置模式下，使用**no iot-admittance-list** *list-name*删除绑定到IoT监控Profile的准入名单。

开启/关闭终端识别功能

默认情况下，终端识别功能是开启的。系统将主动探测IoT监控列表中的终端IP，根据反馈的探测报文信息识别网络视频监控设备的厂商、型号等信息，并显示在IoT监控列表中。

开启终端识别功能后，以下三种情况会触发终端识别：

- 当新的终端IP加入到IoT监控列表时；
- 当网络视频监控设备重新上线时；
- 当网络视频监控设备在线时，每隔5分钟触发一次终端识别。

关闭终端识别功能，在IoT监控Profile配置模式下，使用以下功能：

ipc-monitor iot-identify disable

在IoT监控Profile配置模式下，使用该命令no的形式恢复开启终端识别功能：

no ipc-monitor iot-identify disable

开启/关闭终端行为监控功能

开启终端行为监控功能后，系统会监控已识别的网络视频监控设备的行为特征是否异常，并对异常流量记录日志或进行阻断。默认情况下，终端行为监控功能是开启的，且系统对异常流量进行阻断。

关闭终端行为监控功能，在IoT监控Profile配置模式下，使用以下命令：

```
ipc-monitor abnormal-behavior-monitor disable
```

开启终端行为监控功能，并指定对异常流量记录日志或进行阻断，在IoT监控Profile配置模式下，使用以下命令：

```
ipc-monitor abnormal-behavior-monitor enable action [log-only | block-ip]
```

- **log-only** - 系统对异常流量放行，仅记录日志信息。
- **block-ip** - 系统对异常流量进行阻断。

在IoT监控Profile配置模式下，使用以下命令no的形式恢复默认情况：

```
no ipc-monitor abnormal-behavior-monitor disable
```

绑定IoT监控Profile到安全域

将IoT监控Profile绑定到安全域后，系统将会对经过安全域的流量根据Profile配置进行处理。绑定IoT监控Profile到安全域，需要在域配置模式下进行。

在全局配置模式下，输入以下命令进入域配置模式：

```
zone zone-name
```

进入域配置模式后，使用以下命令将IoT监控Profile绑定到安全域：

```
iot-monitor enable profile-name
```

- *profile-name* - 指定需要绑定到安全域的IoT监控Profile名称。一个安全域仅允许绑定一个IoT监控Profile。

在域配置模式下，使用该命令no的形式解除绑定IoT监控Profile到安全域：

```
no iot-monitor enable
```

删除IoT监控列表条目

删除全部或指定IoT监控列表条目，在任何模式下，使用以下命令：

exec iot-monitor delete iot-monitor-list [**ip** *ip-address*] [**vrouter** *vr-name* | **vswitch** *vs-name*] [**manufacturer** {**hikivison** | **dahua** | **uniview** | **other**}] [**type** {**nvr** | **ipc** | **other**}] [**status** {**online** | **offline**}] [**trust** {**y** | **n**}]

- *ip-address* - 删除指定IP地址的IoT监控列表条目。
- *vr-name* - 删除指定VRouter的IoT监控列表条目。
- *vs-name* - 删除指定VSwitch的IoT监控列表条目。
- **manufacturer** {**hikivison** | **dahua** | **uniview** | **other**} - 删除指定厂商的IoT监控列表条目。其中，**hikivison**为海康威视，**dahua**为大华，**uniview**为宇视，**other**为其他。
- **type** {**nvr** | **ipc** | **other**} - 删除指定设备类型的IoT监控列表条目。其中，**nvr**为网络硬盘录像机，**ipc**为网络摄像机，**other**为其他。
- **status** {**online** | **offline**} - 删除指定状态的IoT监控列表条目。其中，**online**为在线，**offline**为离线。
- **trust** {**y** | **n**} - 删除指定可信状态的IoT监控列表条目。其中，**y**为可信，**n**为不可信。

修改IoT监控列表条目

修改指定的IoT监控列表条目，在任何模式下，使用以下命令：

exec iot-monitor modify iot-monitor-list ip *ip-address* {**vrouter** *vr-name* | **vswitch** *vs-name*} [**manufacturer** {**hikivison** | **dahua** | **uniview** | **other**}] [**type** {**nvr** | **ipc** | **other**}] [**model** *model-name*] [**trust** {**y** | **n**}]

- *ip-address* - 修改指定IP地址的IoT监控列表条目。
- *vr-name* - 指定IP地址所在的VRouter名称。
- *vs-name* - 指定IP地址所在的VSwitch名称。
- **manufacturer** {**hikivison** | **dahua** | **uniview** | **other**} - 修改指定IP地址的IoT监控列表条目的厂商。其中，**hikivison**为海康威视，**dahua**为大华，**uniview**为宇视，**other**为其他。
- **type** {**nvr** | **ipc** | **other**} - 修改指定IP地址的IoT监控列表条目的设备类型。其中，**nvr**为网络硬盘录像机，**ipc**为网络摄像机，**other**为其他。
- *model-name* - 修改指定IP地址的IoT监控列表条目的设备型号。
- **trust** {**y** | **n**} - 修改指定IP地址的IoT监控列表条目的可信状态。其中，**y**为可信，**n**为不可信。

显示准入名单信息

显示准入名单信息，在任何模式下，使用以下命令：

show iot-monitor admittance-list *list-name* [**ip-entry** | **ip-mac-entrty** | **mac-entry**]

- *list-name* - 显示指定名称的所有准入名单信息。
- **ip-entry** - 显示IP类型的准入名单信息。
- **ip-mac-entrty** - 显示IP/MAC类型的准入名单信息。
- **mac-entrty** - 显示MAC类型的准入名单信息

显示IoT监控Profile信息

显示IoT监控Profile信息，在任何模式下，使用以下命令：

show iot-monitor profile *profile-name*

- *profile-name* - 显示指定IoT监控Profile的信息。若不指定Profile名称，显示系统中所有IoT监控Profile的信息。

显示IoT监控列表信息

显示全部或指定IoT监控列表信息，在任何模式下，使用以下命令：

show iot-monitor-list [**ip** *ip-address*] [**vrouter** *vr-name* | **vswitch** *vs-name*] [**manufacturer** {**hikivison** | **dahua** | **uniview** | **other**}] [**type** {**nvr** | **ipc** | **other**}] [**status** {**online** | **offline**}] [**trust** {**y** | **n**}]

- *ip-address* - 显示指定IP地址的所有IoT监控信息。
- *vr-name* - 显示指定VRouter的IoT监控列表条目信息。
- *vs-name* - 显示指定VSwitch的IoT监控列表条目信息。
- **manufacturer** {**hikivison** | **dahua** | **uniview** | **other**} - 显示指定厂商的IoT监控列表条目信息。其中，**hikivison**为海康威视，**dahua**为大华，**uniview**为宇视，**other**为其他。
- **type** {**nvr** | **ipc** | **other**} - 显示指定设备类型的IoT监控列表条目信息。其中，**nvr**为网络硬盘录像机，**ipc**为网络摄像机，**other**为其他。
- **status** {**online** | **offline**} - 显示指定状态的IoT监控列表条目信息。其中，**online**为在线，**offline**为离线。
- **trust** {**y** | **n**} - 显示指定可信状态的IoT监控列表条目信息。其中，**y**为可信，**n**为不可信。

显示IoT监控列表统计信息

显示所有在线网络视频监控设备数/不同设备类型的分布、在线IPC数/不同厂商的分布以及在线NVR数/不同厂商的分布。在任何模式下，使用以下命令：

show iot-monitor-list statistic