天翼云·云下一代防火墙

用户命令行使用手册

天翼云科技有限公司

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

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。

{b}提示: {/b}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。
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 200 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。

第 1 章 防火墙

本章节包含以下内容:

- "StoneOS 系统结构": 介绍 StoneOS 系统中的基本组成部分，包括接口、安全域、VSwitch、VRouter、策略以及 VPN 等。
- "安全域": 介绍系统的安全域。安全域将网络划分为不同部分，例如trust、untrust 等。将配置的策略规则应用到安全域上后，系统就能够对出入安全域的流量进行管理和控制。
- "接口": 介绍系统的接口。接口用于设备间的互联，完成数据交换。
- "地址": 介绍系统的地址簿功能。地址簿包含地址信息，可被多个功能模块引用，例如策略规则、NAT 规则、QoS、会话限制等。
- "服务和应用": 介绍系统的服务簿和应用簿功能。服务簿储存和管理服务和服务组，应用簿储存和管理应用和应用组。
- "DNS": 介绍系统的域名系统功能。DNS 主要用于寻找 Internet 域名（如 www.xxxx.com）并转化为 IP 地址（如“10.1.1.1”）以定位相应的计算机和相应服务。
- "DDNS": 介绍系统的动态域名服务功能。DDNS 主要用于实现固定域名到动态 IP 地址之间的解析。
- "网络地址转换（NAT）": 介绍系统的网络地址转换功能。NAT 将 IP 数据包包头中的源 IP 地址或者目的 IP 地址转换为另一个 IP 地址。
- "应用层识别与控制": 介绍系统的应用层识别与控制功能。ALG 技术能够保证采用多通道数据传送的应用程序进行正常的数据通信，且保证 NAT 地址转换后，VoIP 应用能够正常通信。

StoneOS 系统结构

StoneOS 系统介绍

StoneOS 是设备运行的系统固件。StoneOS 系统中的基本组成部分包括：接口、安全域、VSwitch、VRouter、策略以及 VPN。

接口

接口允许流量进出安全域。因此，为使流量能够流入和流出某个安全域，必须将接口绑定到该安全域，并且，如果是三层安全域，还需要为接口配置 IP 地址。然后，必须配置相应的策略规则，允许流量在不同安全域中的接口之间传输。多个接口可以被绑定到一个安全域，但是一个接口不能被绑定到多个安全域。

StoneOS 支持多种类型接口，实现不同功能。

安全域

安全域将网络划分为不同部分，例如 trust（通常为内网等可信任部分）、untrust（通常为因特网等存在安全威胁的不可信任部分）等。将配置的策略规则应用到安全域上后， 设备就能够对出入安全域的流量进行管理和控制。StoneOS 提供 8 个预定义安全域，分别是：trust、untrust、dmz、L2-trust、L2-untrust、L2-dmz、VPNHub 和 HA。

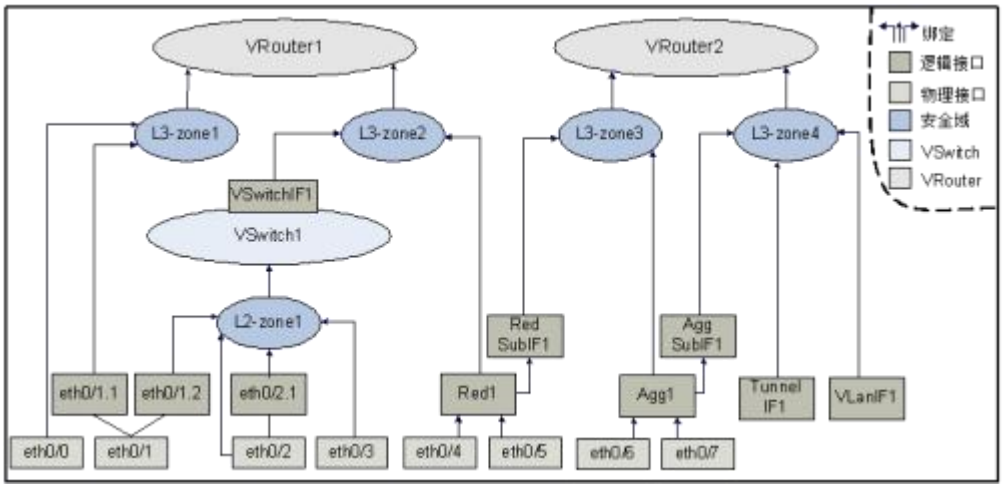
VSwitch

VSwitch（Virtual Switch）即虚拟交换机，具有交换机功能。VSwitch 工作在二层，将二层安全域绑定到 VSwitch 上后，绑定到安全域的接口也被绑定到该VSwitch 上。StoneOS 有一个默认的VSwitch，名为 VSwitch1，默认情况下，二层安全域都会被绑定到 VSwtich1 中。用户可以根据需要创建其它 VSwitch，绑定二层安全域到不同 VSwitch 中。

一个VSwitch 就是一个二层转发域，每个 VSwitch 都有自己独立的 MAC 地址表，因此设备的二层转发在 VSwitch 中实现。并且，流量可以通过 VSwitch 接口，实现二层与三层之间的转发。

VRouter

VRouter（Virtual Router）即虚拟路由器，在 StoneOS 系统中简称为VR。VRouter 具有路由器功能，不同 VR 拥有各自独立的路由表。系统中有一个默认 VR，名为 trust-vr，默认情况下，所有三层安全域都将会自动绑定到 trust-vr 上。系统支持多VR 功能且不同硬件平台支持的最大 VR 数不同。多 VR 将设备划分成多个虚拟路由器，每个虚拟路由器使用和维护各自完全独立的路由表，此时一台设备可以充当多台路由器使用。多VR 使设备能够实现不同路由域的地址隔离与不同VR 间的地址重叠，同时能够在一定程度上避免路由泄露，增加网络的路由安全。下图描述了接口、安全域、VSwitch 和VRouter 之间的关系：



如上图所示，接口、安全域、VSwitch 和VRouter 之间的绑定关系如下：

- 接口绑定到安全域。绑定到二层安全域的接口为二层接口，绑定到三层安全域的接口为三层接口。一个接口只能绑定到一个安全域。主接口与子接口可以分别属于不同的安全域。
- 安全域绑定到VSwitch 或者 VRouter。二层安全域绑定到 VSwitch（预定义二层安全域默认绑定到系统缺省 VSwitch——VSwitch1），三层安全域绑定到 VRouter（预定义三层安全域默认绑定到系统缺省 VRouter——trust-vr）。由此，也实现了接口与 VSwitch 或者VRouter 的绑定。一个安全域只能绑定到一个VSwtich 或者 VRouter

策略

策略实现设备保证网络安全的功能。策略通过策略规则决定从一个安全域到另一个安全域的哪些流量该 被允许，哪些流量该被拒绝。默认情况下，所有通过 设备的流量都是被拒绝的，用户可以根据需要，创建策略规则，允许特定的流量在不同安全域之间或者安全域内通过，例如，允许从 trust 域发起到 untrust 域的所有类型流量通过，或者只允许从 untrust 域发起到 DMZ 域的某种特定应用类型的流量在指定的时间内（时间表功能）通过。

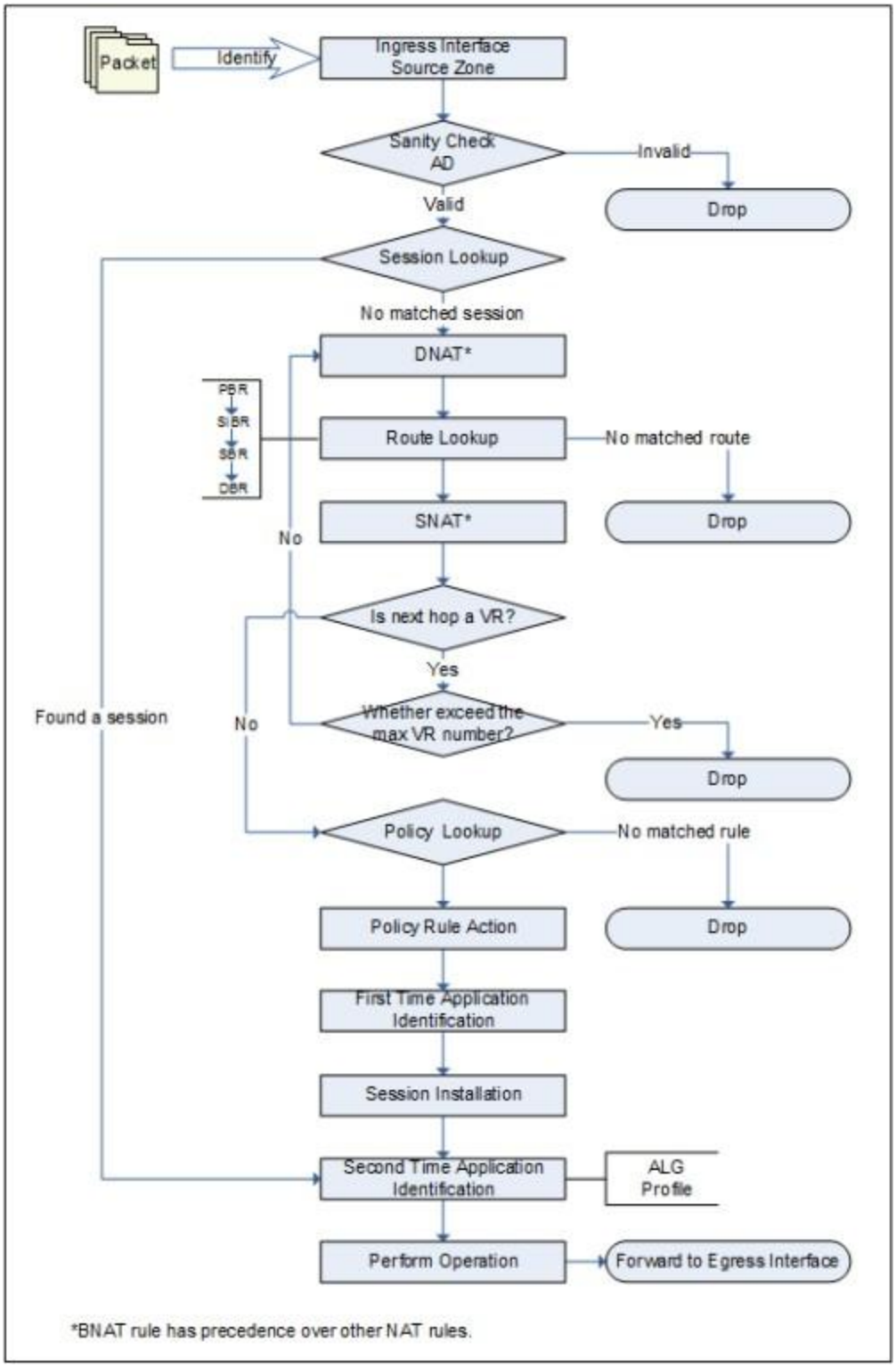
VPN

StoneOS 支持 VPN 功能，包括 IPSec VPN、基于 SSL 的远程登录解决方案——Secure Connect VPN（简称为 SCVPN）、拨号 VPN、PnPVPN 和 L2TP VPN。用户可以配置 VPN 隧道，并且根据不同需求选择以下两种VPN 隧道的应用方式：

- 基于策略的 VPN：将配置成功的 VPN 隧道名称引用到策略规则中，使符合条件的流量通过指定的 VPN 隧道进行传输。
- 基于路由的 VPN：将配置成功的 VPN 隧道与隧道接口绑定；配置静态路由时，将隧道接口指定为下一跳路由。符合条件的流量将会经过VPN 隧道进行传输

数据包处理流程

StoneOS 的三层处理流程如下图所示。



1.识别数据包的逻辑入接口，可能是一般无标签接口，也可能是子接口。从而确定数据包的源安全域。

2.StoneOS 对数据包进行合法性检查。如果源安全域配置了攻击防护功能，系统会在这一步同时进行攻击防护功能检查。

3.会话查询。如果该数据包属于某个已建立会话，则跳过 4 到 10，直接进行第 11 步。

4.目的 NAT（DNAT）操作。如果能够查找到相匹配的 DNAT 规则，则为包做 DNAT 标记。因为路由查询需要DNAT 转换的 IP 地址，所以先进行DNAT 操作。
如果系统配置静态一对一 BNAT 规则，那么先查找匹配的 BNAT 规则。数据包匹配了 BNAT 规则之后，按照 BNAT 的设定进行处理，不再查找普通的 DNAT 规则。

5.路由查询。StoneOS 的路由查询顺序从前到后依次为：策略路由（PBR） 源接口路由（SIBR） 源路由（SBR） 目的路由（DBR） ISP 路由。
此时，系统得到了数据包的逻辑出接口和目的安全域

6.源 NAT（SNAT）操作。如果能够查找到相匹配的 SNAT 规则，则为包做SNAT 标记。
如果系统配置静态一对一 BNAT 规则，那么先查找匹配的 BNAT 规则。数据包匹配了 BNAT 规则之后，按照 BNAT 的设定进行处理，不再查找普通的 DNAT 规则。

7.下一跳 VR 查询。如果下一跳为 VR，则继续查看指定的下一跳 VR 是否超出最大VR 数限制（当前版本系统仅允许数据包最多通过 3 个 VR），如果超过则丢弃数据包，如果未超过，返回 4；如果下一跳不是 VR，则继续进行下一步策略查询。

8.策略查询。系统根据数据包的源安全域、目的安全域、源 IP 地址和端口号、目的 IP 地址和端口号以及协议，查找策略规则。如果找不到匹配的策略规则，则丢弃数据包；如果找到匹配的策略规 则，则根据规则指定的行为进行处理，分别是：

- 允许（Permit）：允许数据包通过。
- 拒绝（Deny）：拒绝数据包通过。
- 隧道（Tunnel）：将数据包转发到指定的隧道。
- 是否来自隧道（Fromtunnel）：检查数据包是否来自指定的隧道，如果是，则允许通过，如果不是，则丢弃。
- Web 认证（WebAuth）：对符合条件的流量进行 Web 认证。

9.第一次应用类型识别。系统根据策略规则中配置的端口号和服务，尝试识别应用类型。

10.会话建立。

11.如果需要，进行第二次应用类型识别。根据数据包的内容和流量行为再次对应用类型进行精确识别。

12.应用层行为控制。根据确定的应用类型，系统将在此执行配置的 Profile 和 ALG 功能。

13.根据会话中记录的信息，例如 NAT 标记等，执行相应的处理操作。

14.将数据包转发到出接口。

TCP RST 包检查

系统支持 TCP RST 包检查。开启该功能后，如果第一个包为 TCP RST 包，系统将不创建会话，否则将创建会话。开启 TCP RST 包检查，在Flow 配置模式下，输入以下命令：

tcp-rst-bit-check

使用 **no tcp-rst-bit-check** 关闭 TCP RST 包检查。

会话信息

用户可以对会话信息进行以下操作：

- 显示会话信息
- 清除会话信息

显示会话信息

用户可以在任何模式下通过使用 show 命令随时查看系统中的会话信息。具体命令如下：

show session [**generic** | **h323**]

- **generic** – 显示会话概要信息。
- **h323** – 显示 H323 会话信息。

show session [**id** *number* [*end-id*]] [**src-ip** *A.B.C.D* [*netmask* | *wildcard*]] [**dst-ip** *A.B.C.D* [*netmask* | *wildcard*]] [**protocol** *protocol-number*] [**src-port** *port-number* [*port-number*]] [**dst-port** *port-number* [*port-number*]] [**application** *name*] [**policy** *policy-id*] [**vrouter** *vrouter-name*] [**vsys** *vsys-name*] [**slot** *slot-number*] [**cpu** *cpu-number*] [{**flow0-interface** | **flow1-interface**} *interface-name*]

- **id** *number* [*end-id*] – 显示指定 ID 或一段 ID 的会话信息。
- **src-ip** *A.B.C.D* – 显示指定源 IP 地址或地址段的会话信息。
- **dst-ip** *A.B.C.D* – 显示指定目的 IP 地址或地址段的会话信息。
- *netmask* | *wildcard* – 指定子网掩码或者通配符掩码。
- *protocol-number* – 显示指定协议号的会话信息。
- **src-port** *port-number* [*port-number*] – 显示指定源端口的会话信息。
- **dst-port** *port-number* [*port-number*] – 显示指定目的端口的会话信息。
- **application** *name* – 显示指定应用的会话信息。

- **policy** *policy-id* – 显示指定策略的会话信息。
- **vrouter** *vrouter-name* – 显示指定 VRouter 的会话信息。
- **vsys** *vsys-name* – 显示指定 VSYS 的会话信息。
- **slot** *slot-number* – 显示指定插槽的会话信息。
- **cpu** *cpu-number* – 显示指定 CPU 的会话信息。
- {**flow0-interface** | **flow1-interface**} *interface-name* - 显示指定 flow0 或者 flow1 的入接口的会话信息。

清除会话信息

用户可以在任何模式下通过使用 clear 命令随时清除系统中的会话信息。具体命令如下:

clear session [**h323**] [**id** *number* [*end-id*]] [**src-ip A.B.C.D** [*netmask* | *wildcard*]] [**dst-ip** *A.B.C.D* [*netmask* | *wildcard*]] [**protocol** *protocol-number*] [**src-port** *port-number* [*port-number*]] [**dst-port** *port-number* [*port-number*]] [**vrouter** *vrouter-name*] [**vsys** *vsys-name*] [**slot** *slot-number*] [**cpu** *cpu-number*]

- **h323** – 清除 H323 会话信息。
- **id** *number* [*end-id*] – 清除指定 ID 或一段 ID 的会话信息。
- **src-ip** *A.B.C.D* – 清除指定源 IP 地址或地址段的会话信息。
- **dst-ip** *A.B.C.D* – 清除指定目的 IP 地址或地址段的会话信息。
- *netmask* | *wildcard* – 清除指定子网掩码或者通配符掩码。
- *protocol-number* – 清除指定协议号的会话信息。
- **src-port** *port-number* [*port-number*] – 清除指定源端口的会话信息。
- **dst-port** *port-number* [*port-number*] – 清除指定目的端口的会话信息。
- **vrouter** *vrouter-name* – 清除指定 VRouter 的会话信息。
- **vsys** *vsys-name* – 清除指定VSYS 的会话信息。
- **slot** *slot-number* – 清除指定插槽的会话信息。
- **cpu** *cpu-number* – 清除指定 CPU 的会话信息。

安全域

域介绍

在系统中，域是一个逻辑的实体，一个或多个接口可以绑定到域。被应用了策略规则的域即为安全域，为实现某个特定功能而存在的域即为功能域。域具有以下特点：

- 接口绑定到域，二层域绑定到VSwitch，三层域绑定到 VRouter。因此，二层域所在的 VSwitch 决定了该域中接口的VSwitch，三层域所在的 VRouter 决定了该域中接口的VRouter。
- 二层和三层域决定其接口工作在二层模式或是三层模式。
- 系统支持域内部策略规则，比如“从 trust 到 trust”的策略规则。

预定义安全域

系统中为用户预定义了 9 个安全域，分别是：trust、untrust、dmz、L2-trust、L2-untrust、L2-dmz、mgt、vpnhub（VPN 功能域）以及ha（HA 功能域）。用户也可以自定义域。事实上，预定义域与用户自定义域在功能上没有任何差别，用户可以自由选择。

配置安全域

用户可以对域进行以下操作：

- 显示域信息
- 创建域
- 指定描述信息
- 绑定二层域到VSwitch
- 绑定三层域到VRouter

显示域信息

用户可以在任何模式下通过使用 **show** 命令随时查看系统中的域信息。具体命令如下：

show zone [*zone-name*]

- *zone-name* – 指定域的名称显示指定域的信息。

创建域

用户创建安全域时,如果不指定二层域参数，则默认为三层域。创建一个域并且进入域配置模式，在全局配置模式下，输入以下命令：

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

- *zone-name* - 创建域的名称。
- **l2** – 指定所创建域为二层域。
- **tap** -指定所创建的域为 Tap 域。Tap 域为旁路模式功能域。

如果所指定的域的名称存在，则直接进入域配置模式。

在全局配置模式下，使用 **no zone** *zone-name* [l2]命令删除指定域。

注意:预定义域不可以被删除。

指定描述信息

为所配置的域指定描述信息，请在域配置模式下，使用以下命令:

description *description*

- *description* – 安全域的描述信息。

使用 **no description** 命令删除安全域的描述信息。

绑定三层域到 VRouter

用户通过把三层域绑定到VRouter 来实现接口与VRouter 的绑定。默认情况下，所有的三层域都绑定到 trust-vr 中。改变三层域的VRouter，在域配置模式下，使用以下命令:

vrouter *vrouter-name*

- *vrouter-name* – 指定将三层域绑定到的VRouter 的名称。

恢复域到trust-vr 的绑定，在域配置模式下，使用 **no vrouter** 命令。

注意:改变域所属的VRouter 时，必须保证域中没有绑定的接口。

绑定二层域到 VSwitch

用户通过把二层域绑定到VSwitch 来实现接口与VSwtich 的绑定。默认情况下，每一个二层域都被绑定到 VSwitch1 中。改变二层域的VSwitch，在域配置模式下，使用以下命令:

bind *vswitch-name*

- *vswitch-name* - 指定将二层域绑定到的 VSwitch 的名称。

恢复域到VSwitch1 的绑定，在域配置模式下，使用 **no bind** 命令。

注意:改变域所属的VSwitch 时，必须保证域中没有绑定的接口。

安全域配置示例

例如，创建 VSwitch2，创建二层安全域 zone1，将 zone1 绑定到VSwitch2，再将 ethernet0/2 绑定到 zone1，请参考以下命令：

```
hostname(config)# vswitch vswitch2
hostname(config-vswitch)# exit
hostname(config)# zone zone1 l2
hostname(config-zone-zone1)# bind vswitch2
hostname(config-zone-zone1)# exit
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# zone zone1
hostname(config-if-eth0/2)# exit
hostname(config)#
```

接口

查看接口信息

查看所有接口信息

通过 CLI 查看所有接口信息，请使用 **show interface** 命令。接口表中显示每个接口的下列信息：

项目	描述
Interface name	显示接口的名称。
IP address/mask	显示接口的 IP 地址。
Zone name	显示接口的绑定域的名称。
Vsys	显示接口所属虚拟系统的名称。
H (Physical state)	显示接口的物理状态是否为可用（UP/DOWN）。
A (Admin state)	显示接口的管理状态是否为可用（UP/DOWN）。
L (Link state)	显示接口的链路状态是否为可用（UP/DOWN）。
P (Protocol state)	显示接口的协议状态是否为可用（UP/DOWN）。
MAC address	显示接口的 MAC 地址。
Description	显示接口的描述信息。

H、A、L 和 P 是接口的四种状态。状态的值为可用（UP）或不可用（DOWN）。

- H（Physical state）：接口的物理状态。如果接口的物理连接是完好的，该接口 PHY 值就是 UP，反之则为 DOWN。
- A（Admin state）：接口的管理状态。用户可以通过 **no shutdown** 和 **shutdown** 命令来打开和关闭接口。如果接口被打开，该接口的 A 值就是 UP，反之则为 DOWN。
- L（Link state）：接口的链路状态。链路状态的值由 H 和 A 的值来决定。只有H 和 A 均为 UP 时，L 的值才为 UP。
- P（Protocol state）：接口的协议状态。只有当接口的链路状态为 UP 并且 IP 地址已经被分配到该接口，P 的值才会为 UP。

请参考下图接口表示例图：

```
hillstone# show interface

H:physical state;A:admin state;L:link state;P:protocol state;U:up;D:down
================================================================================
Interface name    IP address/mask     Zone name       H A L P MAC address
--------------------------------------------------------------------------------
ethernet0/0       192.168.1.1/24      trust           D U D D 001c.5400.02ec
ethernet0/1       10.200.3.251/24     trust           U U U U 001c.5400.02ed
ethernet0/10      0.0.0.0/0           NULL            D U D D 001c.5400.02f6
ethernet0/11      0.0.0.0/0           NULL            D U D D 001c.5400.02f7
ethernet0/2       0.0.0.0/0           NULL            D U D D 001c.5400.02ee
ethernet0/3       0.0.0.0/0           NULL            D U D D 001c.5400.02ef
ethernet0/4       0.0.0.0/0           NULL            D U D D 001c.5400.02f0
ethernet0/5       0.0.0.0/0           NULL            D U D D 001c.5400.02f1
ethernet0/6       0.0.0.0/0           NULL            D U D D 001c.5400.02f2
ethernet0/7       0.0.0.0/0           NULL            D U D D 001c.5400.02f3
ethernet0/8       0.0.0.0/0           NULL            D U D D 001c.5400.02f4
ethernet0/9       0.0.0.0/0           NULL            D U D D 001c.5400.02f5
vswitchif1        0.0.0.0/0           NULL            D U D D 001c.5400.0308
================================================================================
```

查看指定接口信息

查看某个指定接口的信息，请在 **show interface** 命令后添加要查看接口名称，即 **show interface** *interface-name*。下图为接口 ethernet0/0 的信息：

```
hillstone# show interface ethernet0/0
------------------------------------------------------------
Interface ethernet0/0
description:
                Physical down                   Admin up
                Link down                       Protocol down
                Interface ID:4
                IP address:192.168.1.1
                IP address mask:255.255.255.0
                MAC address:001c.5400.02ec
                Ip mtu:1500
                ARP learn:enable
                ARP timeout:1200
                Speed mode:10
                Duplex mode:half
                downstream bandwidth is 1000000000
                upstream   bandwidth is 1000000000
                Bind to zone trust
                Belong to vsys root
                manage service:SSH;TELNET;PING;SNMP;HTTP;HTTPS;
                Secondary ip address0: 0.0.0.0 mask:0.0.0.0
                Secondary ip address1: 0.0.0.0 mask:0.0.0.0
============================================================
```

配置接口

本节将介绍接口的基本配置操作，具体内容有：

- 绑定接口到域
- 配置接口 IP 地址
- 强制关闭接口
- 配置接口功能管理
- 配置接口逆向路由功能

- 配置接口 Local 属性

绑定接口到域

用户可以将任何物理接口绑定到已定义的二层或三层域。将接口绑定到域，在接口配置模式下输入以下命令：

zone *zone-name*

在接口配置模式下使用 **no zone** 命令取消接口与域的绑定。在取消三层接口与域的绑定前，必须将三层接口配置的 IP 地址取消。

注意:将接口绑定到域时：

- 如果想让接口在二层工作，就必须把该接口绑定到二层域。
- 把接口从三层接口转换成二层接口前，必须将三层接口配置的 IP 地址取消。

配置接口 IP 地址

设备上所有接口配置的 IP 地址都必须在不同网段。用户可以为接口配置静态 IP 地址，也可以让接口通过 DHCP 或者PPPoE 协议动态获得 IP 地址。配置接口的 IP 地址，在接口配置模式下，输入以下命令：

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

- *ip-address/mask* – 为接口指定静态 IP 地址。
- **dhcp** [**setroute**] – 指定接口通过 DHCP 协议获得 IP 地址。如果配置 setroute 参数，系统会将 DHCP 服务器提供的网关信息设置为默认网关路由。
- **pppoe** [**setroute**] – 指定接口通过 PPPoE 协议获得 IP 地址。如果配置setroute 参数，系统会将 PPPoE 服务器提供的网关信息设置为默认网关路由。

例如把 IP 地址 1.1.1.1 分配给以太网接口ethernet0/0，请输入以下命令：

```
进入接口 ethernet0/0 配置模式：
hostname(config)# interface ethernet0/0
配置接口 ethernet0/0 的主 IP 地址：
hostname (config-if-eth0/0)# ip address 1.1.1.1/24
退出接口配置模式：
hostname(config-if)# exit
```

在为接口指定 IP 地址时，请注意以下两点：

- 系统支持两种子网掩码书写方法，所以 1.1.1.1/24 也可写成 1.1.1.1 255.255.255.0。
- 只有已经绑定到域的接口才可以配置 IP 地址。

在接口配置模式下，使用 **no ip address** [*ip-address/mask* | **dhcp** | **pppoe**]命令取消接口的 IP 地址配置。

强制关闭接口

设备支持接口的强制关闭功能。用户不仅可以根据需要用命令强制关闭特定接口，还可以通过时间表控制接口的关闭时间，或者根据监测接口的链路状态控制接口的关闭。在 CLI 中强制关闭接口，请在接口配置模式下输入以下命令：

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

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

在接口配置模式下，使用 **no shutdown** 命令，取消强制关闭接口功能并清除此功能的所有相关配置。

配置接口管理功能

接口的以下功能需要通过命令开启后才可以使用，包括 SSH、Telnet、Ping、SNMP、HTTP、HTTPS 和 FTP。开启这些功能后，用户可以使用接口上的 IP 地址通过相应的功能管理和配置设备。开启以上所述功能，在接口配置模式下，使用以下命令：

manage {**ssh** | **telnet** | **ping** | **snmp** | **http** | **https** | **ftp**}

- **ssh** - 开启接口的 SSH 功能。
- **telnet** - 开启接口的 Telnet 功能。
- **ping** - 开启接口的Ping 功能。
- **snmp** - 开启接口的 SNMP 功能。
- **http** - 开启接口的 HTTP 功能。
- **https** - 开启接口的 HTTPS 功能。
- **ftp** - 开启接口的FTP 服务功能

使用 **no manage** {**ssh** | **telnet** | **ping** | **snmp** | **http** | **https** | **ftp**}命令关闭相应的功能。

配置接口逆向路由功能

逆向路由功能是指用于转发反向数据的路由。反向是相对于初始化数据流方向。逆向路由功能仅适用于三层接口。在接口配置模式下，使用以下命令完成逆向路由功能的配置：

reverse-route [force | prefer]

- force – 强制逆向路由。如果能找到逆向路由则使用逆向路由转发反向数据；如果找不到逆向路由则丢弃数据包。默认情况下，三层接口强制逆向路由。
- prefer – 优先逆向路由。如果能找到逆向路由则使用逆向路由转发反向数据；如果找不到逆向路由则按原路径返回（即从当前接口转发出去）。

在接口配置模式下，使用 no reverse-route 命令取消逆向路由的使用。不使用逆向路由时，所有反向数据原路返回，不进行逆向路由检查。

注意:如果找到的逆向路由出接口和原入接口不在同一个安全域，设备仍会丢弃数据包。

配置接口 Local 属性

为了解决在同一个二层网络管理大量 HA 设备时 MAC 地址冲突的问题，系统支持为所有接口（除 VSwitch 口）配置一个可编辑的 HA Local 属性。子接口和Virtual Forward 接口不需要配置，可直接继承主接口的 HA Local 属性。配置后，系统将不向备份设备同步该接口下的配置信息。在接口配置模式下，使用以下命令：

local

在接口配置模式下，使用 no local 删除 HA Local 属性。

地址

地址（Address）介绍

在系统中，IP 地址是系统多个功能模块配置的重要组成元素，例如策略规则、网络地址转换规则以及会话数限制等。因此，为方便引用 IP 地址，实现灵活配置，系统支持地址簿功能。用户可以给一个 IP 地址范围指定一个名称，在配置时，只需引用该名称。而地址簿就是系统中用来储存 IP 地址范围与其名称的对应关系的数据库。地址簿中的 IP 地址与名称的对应关系条目被称作地址条目（Address Entry）。

地址条目

系统拥有一个全局地址簿。用户需要为全局地址簿定义地址条目。在定义地址条目时，DNS 名称可以直接用来代替 IP 地址范围。地址条目还具有以下特点：

- 地址簿中有一条默认条目“Any”。“Any”对应的 IP 地址是 0.0.0.0/0，也就是代表所有 IP 地址。“Any”不可以编辑也不可以被删除。

- 一条地址条目中可以包含地址簿中另外的地址条目。
- 如果地址条目的 IP 地址范围发生了变化，系统会自动更新其它引用了该地址条目的模块。

配置地址簿

用户可以通过 CLI 对地址簿进行以下配置：

- 添加或者删除地址条目
- 指定地址条目的 IP 地址范围
- 指定排除地址条目成员
- 重新命名地址条目
- 查看地址条目关联项
- 查看地址簿信息

添加或者删除地址条目

在全局配置模式，使用address 命令向地址簿中添加一个地址条目，同时进入地址配置模式：

address *address-entry* [**ipv6**]

- *address-entry* - 指定要添加的地址条目的名称。
- **ipv6** - 指定添加的地址条目为 IPv6 类型。若不指定，则为 IPv4 类型。

使用该命令 no 的形式将地址条目从地址簿中删除：

no address *address-entry*

注意:已经被其它模块或者其它地址条目引用的地址条目不能被删除。

指定地址条目的 IP 地址范围

在系统中，地址条目的 IP 地址范围是其成员 IP 地址范围的总和。地址条目成员有以下几种：

- IP 地址：包括两种类型，一种为“IP 地址/子网掩码”，如 10.100.2.0/24；另一种为“IP 地址通配符掩码”，如 192.168.0.1 255.255.0.255
- 主机名称，如host1. net.com；支持含有通配符的主机名称，如*.baidu.com
- IP 地址段，如 10.100.2.3 – 10.100.2.100
- 国家/地区：某一国家或地区的 IP 地址的集合。
- 其它地址条目

在地址配置模式下，使用 **ip** 命令来为地址条目添加指定 IP 地址范围成员。用该命令 no 的形式删除指定成员。

- **ip** {*ip-address* {*netmask* | *wildcardmask*} | *ip/netmask*}
  - *ip-address* – 指定 IP 成员的 IP 地址。
  - *netmask* / *wildcardmask* – 指定子网掩码（netmask）或者通配符掩码（wildcardmask）。StoneOS 不支持掩码转换为二进制后，其位数里从右往左第一个“1”左边的“0”的个数超过 8 个的通配符掩码（“0”可以连续也可以不连续），比如 255.0.0.255 是无效的通配符掩码；255.0.255.0 和 255.32.255.0 等都为有效的通配符掩码。
  - *ip/netmask* – 指定 IP 成员的 IP 地址和网络掩码。
- **no ip** {*ip-address* {*netmask* | *wildcardmask*} | *ip/netmask*}

在地址配置模式下，用 **host** 命令来为地址条目添加主机类型成员。用该命令no 的形式删除指定成员。

- **host** *host-name* [**vrouter** *vrouter-name*]
  - *host-name* – 指定主机类型成员名称；支持含有通配符的主机名称。名称范围是 1 到 255 个字符。
  - *vrouter-name* -为地址条目添加指定VRouter 下的主机类型成员。
- **no host** *host-name* [**vrouter** *vrouter-name*]

在地址配置模式下，用 **range** 命令来为地址条目添加 IP 地址段成员。用该命令no 的形式删除指定成员。

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

在地址配置模式下，用 **country** 命令为地址条目添加某一国家或地区的 IP 地址的集合。用该命令 no 的形式删除指定成员。

- **country** *country-name*
  - *country-name* - 可选值，可通过在 **country** 关键字后使用 TAB 键进行查看。
- **no country** *country-name*

在地址配置模式下，用 **member** 命令为地址条目添加另一地址条目。用该命令no 的形式删除指定条目。

- **member** *address-entry*
- **no member** *address-entry*

注意:在配置地址簿时:

- “国家/地区”成员仅在 IPv4 地址簿中支持。
- 添加了“国家/地区”成员的地址簿，仅可以被策略规则和策略路由规则引用。
- 添加了“国家/地区”成员的地址簿，不支持排除地址成员配置。
- 设备最多支持 128 条含有通配符的主机条目。

指定排除地址条目成员

系统的地址簿中同时支持 IPv4 和 IPv6 的地址条目，用户可以通过配置排除地址功能，将个别 IPv4 或 IPv6 地址条目成员从地址簿中排除。可以排除的 IPv4 或 IPv6 地址条目成员有以下 2 种:

- IP 地址：IPv4 地址包括两种类型，一种为“IP 地址/子网掩码”，如 10.100.2.0/24；另一种为“IP 地址通配符掩码”，如 192.168.0.1 255.255.0.255；IPv6 地址为“IPv6 前缀/前缀长度”，如 2001::1/64
- IP 地址段，如 10.100.2.3 - 10.100.2.100 或 2002::0-2002::10

注意:每个地址簿能够配置的排除地址条目成员有限，最多占地址条目成员最大值的 10%。

指定排除 IPv4 地址条目成员

为 IPv4 地址条目排除 IP 地址范围成员，在地址配置模式下，使用以下命令:

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

- *ip-address* - 指定排除 IPv4 地址条目成员的 IP 地址。
- *netmask* / *wildcardmask* - 指定子网掩码（*netmask*）或者通配符掩码（*wildcardmask*）。StoneOS 不支持掩码转换为二进制后，其位数里从右往左第一个“1”左边的“0”的个数超过 8 个的通配符掩码（“0”可以连续也可以不连续），比如 255.0.0.255 是无效的通配符掩码；255.0.255.0 和 255.32.255.0 等都为有效的通配符掩码。

使用 **no exclude ip** *ip-address* {*netmask* | *wildcardmask*}恢复排除的 IP 地址范围成员。

为 IPv4 地址条目排除 IP 地址段成员，在地址配置模式下，使用以下命令:

exclude range *min-ip max-ip*

- *min-ip max-ip* - 指定 IP 地址范围的两个 IP 地址。

使用 **no exclude range** *min-ip max-ip* 恢复排除的 IP 地址段成员。

指定排除 IPv6 地址条目成员

为 IPv6 地址条目排除 IP 地址范围成员，在地址配置模式下，使用以下命令：

exclude ip *ipv6-prefix / prefix-length*

- *ipv6-prefix / prefix-length* – 指定 IPv6 前缀以及前缀长度。取值范围为 65 到 128。

使用 **no exclude ip** *ipv6-prefix / prefix-length* 恢复排除的 IP 地址范围成员。

为 IPv6 地址条目排除 IP 地址段成员，在地址配置模式下，使用以下命令：

exclude range *min-ipv6-address max-ipv6-address*

- *min-ipv6-address* – 指定 IPv6 地址范围的最小地址。
- *max-ipv6-address* – 指定 IPv6 地址范围的最大地址。

使用 **no exclude range** *min-ipv6-address max-ipv6-address* 恢复排除的 IP 地址段成员。

重新命名地址条目

在地址配置模式下，使用 rename 命令来重新命名已创建的地址条目：

rename *name*

- *name* - 指定新的地址条目名称。如果出现重名，该命令会失效。

查看地址条目关联项

在系统中，地址条目可以被其他功能模块引用，比如策略规则、网络地址转换规则以及会话数限制等。用户可以在任何模式下查看地址条目被系统其它功能模块引用的情况，即地址条目的关联项。命令如下：

show reference address *address-entry*

- *address-entry*- 显示指定地址条目的关联项。

例如：

```
hostname(config)# show reference address 10.101.0.194
============================================================
Name: | 10.101.0.194 （地址条目名称）
------------------------------------------------------
Address: | - （被其它地址条目引用的信息）
```

```
-------------------------------------------------
Policy rule: | policy 20 src-addr （被策略规则引用的信息）
-------------------------------------------------
SNAT rule: | - （被 SNAT 规则引用的信息）
-------------------------------------------------
DNAT rule: | - （被 DNAT 规则引用的信息）
-------------------------------------------------
Statistics: | - （被统计集引用的信息）
-------------------------------------------------
Session limit: | rule 1 （被会话限制规则引用的信息）
-------------------------------------------------
PBR: | - （被策略路由规则引用的信息）
-------------------------------------------------
QoS: | - （被 QoS 规则引用的信息）
-------------------------------------------------
ExStats: | - （被所选地址簿或应用组的统计集引用的信息）
=================================================
```

查看地址簿信息

用户可以在任何模式下使用以下命令查看全局地址簿的具体信息，包括地址簿内地址条目的名称、地址条目的成员数以及成员的具体内容。命令如下：

show address [**filter-ip** *A.B.C.D*] | [*address-entry*]

- **show address** - 显示地址簿内所有地址条目的具体信息。
- **filter-ip** *A.B.C.D* - 显示包含有指定 IP 地址的地址条目信息。
- *address-entry* - 显示指定地址条目的具体信息。

用户可以在任何模式下使用以下命令查看指定 IP 地址所在的国家或地区。命令如下：

show country ip *A.B.C.D*

- *A.B.C.D* – 输入待查询 IP 地址。

地址簿配置示例

配置示例 1

例如，为地址簿创建名为 address1 和 address2 的地址条目；将以下成员添加到 address1 中：10.200.1.0/16、192.168.1.0/24、192.168.0.1/255.255.0.255 以及 net.com；将以下成员添加到 address2 中：10.100.3.1 到 10.100.3.10 以及 address1。请参考以下命令：

```
hostname(config)# address address1
hostname(config-addr)# ip 10.200.1.0/16
hostname(config-addr)# ip 192.168.1.0 255.255.255.0
hostname(config-addr)# ip 192.168.0.1 255.255.0.255
hostname(config-addr)# host net.com
hostname(config-addr)# exit
hostname(config)# address address2
hostname(config-addr)# range 10.100.3.1 10.100.3.10
hostname(config-addr)# member address1
hostname(config-addr)# exit
hostname(config)#
```

配置示例 2

配置包含通配符的主机名称，以下是设置主机名称为*.baidu.com 的命令配置示例：

```
hostname(config)# addr baidu
hostname(config-addr)# host *.baidu.com
```

服务和应用

本章节包含以下内容:

- "服务（Service）": 介绍系统的服务簿。服务簿用于存储和管理服务和服务组。
- "应用（Application）": 介绍系统的应用簿。应用簿用于存储和管理应用和应用组。

服务（Service）

服务（Service）是具有协议标准的信息流。服务具有一定的特征，例如相应的协议、端口号等，举例来 讲，FTP 服务使用 TCP 传输协议，其目的端口号是 21。服务是系统多个功能模块配置的重要组成元素， 例如策略规则、网络地址转换规则等。系统提供了百余种预定义服务以及 10 余种预定义服务组（Service Group），同时用户也可以根据自己的需要创建自定义服务或服务组。系统用服务簿来储存和管理这些服务和服务组。服务簿中的每一条服务包含具体的服务条目。

通过 CLI 查看服务信息

用户可以在任何模式下通过使用 **show service** 命令查看到所有服务的信息。该命令的使用方法为:

show service {**predefined** | **userdefined** | **name** *service-name*}

- **predefined** – 指定显示预定义服务信息。
- **userdefined** – 指定显示用户自定义服务信息。
- **name** *service-name* - 指定显示某个服务信息。

查看服务关联项

在系统中，服务可以被其他功能模块引用，比如策略规则、网络地址转换规则以及应用 QoS 管理等。用户可以在任何模式下查看服务或者服务组被系统其它功能模块引用的情况，即服务或者服务组的关联项。命令如下:

show reference service *service-name*

- *service-name* – 显示指定服务或者服务组的关联项。

例如:

```
hostname(config)# show reference service ftp
=======================================================
```

```
Name: | ftp  （服务或者服务组名称）
----------------------------------------------------
Service group: | SRV_INTERNET_PROTOCOL （被其它服务组引用的信息）
----------------------------------------------------
Policy rule: | policy 105 , policy 100 （被策略规则引用的信息）
----------------------------------------------------
DNAT rule: | - （被 DNAT 规则引用的信息）
----------------------------------------------------
SNAT rule: | - （被 SNAT 规则引用的信息）
----------------------------------------------------
Statistics: | - （被统计集引用的信息）
----------------------------------------------------
Policy route: | - （被策略路由规则引用的信息）
====================================================
```

预定义服务（Predefined Services）

系统提供百余种预定义服务。使用以上 **show** 命令或者通过 WebUI 页面可以查看当前版本支持的所有预定义服务。

以下介绍几个常见的预定义服务。

远程 Shell（RSH）

RSH ALG（Remote Shell）允许被认证的用户在远程主机上运行 **shell** 命令。设备支持透明模式、路由模式和 NAT 模式的 RSH 服务。

Sun 远程程序调用（Sun RPC）

Sun RPC（Sun Remote Procedure Call）提供了一种方法能够使一台主机上运行的程序调用另一台主机正在运行的程序的过程。因为 RPC 服务数量众多，并且有广播的需要，RPC 服务的传输地址是基于服务程序的数量和版本而动态协商的。人们会定义一些绑定的协议将 RPC 程序数量和版本映射到传输地址。

设备支持 Sun RPC 预定义服务，使用户能够根据所配置的策略允许或者拒绝流量。用户可以定义一条设备策略来允许或者拒绝所有 RPC 请求。例如，需要使用网络文件系统（NFS），请通过策略规则允许 SunRPC 服务。

微软远程过程调用（MS RPC）

微软远程过程调用应用层网关是微软对分布式计算环境 RPC 的实现。MS RPC 提供一种方法，使一台主机上运行的程序能够调用另一台主机上正在运行的程序过程。因为 RPC 服务数量众多，并且有广播的需求，RPC 的传输地址将基于服务程序的 UUID（Universal Unique Identifier）进行动态协商。

设备支持 MS RPC 预定义服务，使用户能够根据所配置的策略允许或者拒绝流量。用户可以定义一条设备策略来允许或者拒绝所有的 RPC 请求。例如，需要使用Outlook/Exchange 交互或者 MSqueue 服务，请通过策略规则允许 MSRPC 服务。

预定义服务组

预定义服务组中包含相关的预定义服务，可方便用户配置。系统提供 10 余种预定义服务组。其中，包含动态识别预定义服务的预定义服务组为动态识别预定义服务组，需要与其它服务组区分开单独配置。通过特征库更新动态识别预定义服务时，也将同时更新动态识别预定义服务组。用户可以查看和使用预定义服务组，但是不能编辑和删除预定义服务组。

查看预定义服务组，在任何模式下，使用以下命令：

show predefined-servgroup

用户自定义服务

除了使用系统提供的预定义服务以外，用户还可以很容易地创建自己的自定义服务。用户自定义服务可包含最多 8 条服务条目。用户需指定的自定义服务条目的参数包括：

- 名称
- 传输协议
- TCP 或 UDP 类型服务的源和目标端口号或者 ICMP 类型服务的 type 和 code 值
- 超时时间
- 应用类型

创建和删除自定义服务

在 CLI 中创建一个服务并将其添加到服务簿，请在全局配置模式下使用以下命令，并且用该命令 no 的形式删除一个服务：

service *service-name*

no service *service-name*

- *service-name* – 指定自定义服务的名称。长度范围是 1 至 31 个字符。该名称在整个系统中必须是唯一的。运行命令后，CLI 进入所创建服务的配置模式。

如需创建长连接服务，在全局模式下，使用 *longlife-sess-percent* 命令配置长连接会话的占比。默认占比为 0。

为自定义服务添加和删除自定义服务条目

每一个自定义服务可最多包含八个服务条目。根据服务条目的协议类型的不同，添加服务条目所使用的命令也不同。

添加 TCP 或者 UDP 类型服务条目，在服务配置模式下输入以下命令：

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

- **dst-port** *min-port* [*max-port*] – 指定自定义服务的目的端口号。如果目的端口号为一个范围，*min-port* 为最小目的端口号，*max-port* 为最大目的端口号。目的端口号的范围是 0 到 65535，并且目的端口号不能为单一的 0，例如，目的端口号可以是 0 到 20，但是不能仅为 0。
- **src-port** *min-port* [*max-port*] – 指定自定义服务的源端口号。如果源端口号为一个范围，*min-port* 为最小源端口号，*max-port* 为最大源端口号。源端口号的范围是 0 到 65535。
- **timeout** *time-out-value* – 指定超时时间。单位为秒，取值范围 1-65535。超出超时时间后，连接将断开。
- **timeout-day** *time-out-value* – 指定长连接的超时时间。单位为天，取值范围 1-1000。超出超时时间后，连接将断开。配置长连接的超时时间，需先在全局配置模式下配置长连接的会话占比。

添加 ICMP 类型服务条目，在服务配置模式下输入以下命令：

icmp type *type-value* [**code** *min-code* [*max-code*]] [**timeout** *time-out-value* | **timeout-day** *time-out-value*]

- *type-value* – 指定自定义服务的 ICMP type 值。范围是 3（Destination-Unreachable）、4（Source Quench）、5（Redirect）、8（Echo）、11（Time Exceeded）、12（Parameter Problem）、13（Timestamp）和 15（Information）以及 any（表示以上所有 type 值）。
- **code** *min-code* [*max-code*] – 指定自定义服务的 ICMP code 值。范围是 0 到 5。默认值是“0-5”。
- **timeout** *time-out-value* – 指定超时时间。单位为秒，取值范围 1-65535。超出超时时间后，连接将断开。
- **timeout-day** *time-out-value* – 指定长连接的超时时间。单位为天，取值范围 1-1000。超出超时时间后，连接将断开。配置长连接的超时时间，需先在全局配置模式下配置长连接的会话占比。

添加其它类型服务条目，在服务配置模式下输入以下命令：

protocol *protocol-number* [**timeout** *time-out-value* | **timeout-day** *time-out-value*]

- *protocol-number* – 指定自定义服务的协议号。范围是 1 到 255。
- **timeout** *time-out-value* – 指定超时时间。单位为秒，取值范围 1-65535。超出超时时间后，连接将断开。
- **timeout-day** *time-out-value* – 指定长连接的超时时间。单位为天，取值范围 1-1000。超出超时时间后，连接将断开。配置长连接的超时时间，需先在全局配置模式下配置长连接的会话占比。

使用以上三条命令 no 的形式可以删除服务条目。并且已经创建的服务条目不能修改只能删除。

- **no** {**tcp** | **udp**} **dst-port** *min-port* [*max-port*] [**src-port** *min-port*[*max-port*]]
- **no icmp type** *type-value* [**code** *min-code* [*max-code*]]
- **no protocol** *protocol-number*

自定义服务重命名

为已创建的自定义服务重命名，在服务配置模式下，使用以下命令：

rename *new-name*

- *new-name* – 指定自定义服务的新名称。

用户还可以在全局配置模式下，使用以下命令为指定的自定义服务重命名。

rename service *old-name new-name*

- *old-name* – 指定自定义服务的旧名称。
- *new-name* – 指定自定义服务的新名称。

自定义服务配置示例

例如，创建名为 my-service 的自定义服务，为my-service 添加以下 3 条服务条目：

- TCP 类型服务，目的端口号为 2121，源端口号为 80；
- ICMP 类型服务，type 为 8，code 为 0；
- 其它类型服务，协议号为 47。

请参考以下命令：

```
hostname(config)# service my-service
hostname(config-service)# tcp dst-port 2121 src-port 80
```

```
hostname(config-service)# icmp type 8 code 0
hostname(config-service)# protocol 47
hostname(config-service)# exit
hostname(config)#
```

自定义服务组

用户将一些服务组织到一起便组成了服务组。用户可以直接将服务组应用到设备策略中，这样便简化了管理。服务组有以下特征：

- 服务簿中的每一条服务都可以被一个或多个服务组引用。
- 每个服务组中既可以包含预定义服务，也可以包含用户自定义服务。
- 服务组可以包含服务组。系统的服务组支持 8 层嵌套。

服务组还有以下限制：

- 服务组名称与服务名称不能相同。
- 被策略引用的服务组不能被删除。如果要删除一个服务组，必须首先从其它模块中删除对该服务组的引用。
- 如果用户从服务簿中删除了一条用户自定义服务，该条服务也将会从所有引用它的服务组中被删除。

创建和删除服务组

在 CLI 中创建一个服务组并将该组添加到服务簿中，请在全局配置模式下，输入以下命令：

servgroup *servicegroup-name*

注意:服务组的名称必须是唯一的。

运行该命令后，系统进入服务组配置模式。

删除一个服务组，请在全局配置模式下，输入以下命令：

no servgroup *servicegroup-name*

为服务组添加和删除服务或者服务组

服务组的成员可以是一条服务，也可以是一个服务组。在 CLI 中为服务组添加或者删除服务，请在服务组配置模式输入以下命令：

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

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

为服务组添加服务或者服务组时，请注意以下两点：

- 服务组中的服务必须是唯一的。
- 每个服务组最多可以包含 64 条服务；服务组与服务组之间最多可以嵌套 8 层。

为服务或者服务组添加/删除描述信息

在 CLI 的服务或服务组配置模式下，用户可以通过使用以下命令为服务或服务组添加描述信息。

description *description*

- *description* – 指定服务或服务组的描述信息。范围是 1 到 255 字节。

在 CLI 的服务或服务组配置模式下，使用以下命令删除服务或服务组的描述信息。

no description

服务组重命名

为已创建的服务组重命名，在服务组配置模式下，使用以下命令：

rename *new-name*

- *new-name* – 指定服务组的新名称。

用户还可以在全局配置模式下，使用以下命令为指定的服务组重命名。

rename servgroup *old-name new-name*

- *old-name* – 指定服务组的旧名称。
- *new-name* – 指定服务组的新名称。

应用（Application）

应用（Application）具有一定的特征，例如相应的协议、端口号、应用类型等。应用是系统多个功能模块配置的重要组成元素，例如策略规则、网络地址转换规则和应用QoS 管理等。系统提供了百余种预定义应用以及 20 余种预定义应用组。同时用户也可以根据自己的需要创建自定义应用或应用组。系统用应用簿来储存和管理这些应用和应用组。 如接口开启了 IPv6 功能，系统支持识别 IPv6 地址。

预定义应用（Predefined Application）

系统提供百余种预定义应用。使用 **show application predefined** 命令可以查看当前版本支持的所有预定义应用。

预定义应用组

预定义应用组中包含相关的预定义应用，可方便用户配置。通过特征库更新来动态识别出预定义应用。目前，系统提供 20 余种预定义应用组。用户可以查看和使用预定义应用组，但是不能编辑和删除预定义应用组。

用户自定义应用（Userdefined Application）

除了使用系统提供的预定义应用以外，用户还可以根据需要创建自定义应用，并可以通过配置自定义应用特征规则，对进入设备的流量进行识别控制，从而识别出应用类型。

自定义应用配置包括：

- 创建/删除自定义应用
- 创建/删除应用特征规则
- 配置自定义应用特征规则的条目
- 配置应用超时时间
- 修改自定义应用特征排列顺序

创建和删除自定义应用

创建一个自定义应用并将其添加到应用簿，请在全局配置模式下使用以下命令，并且用该命令 no 的形式删除一个自定义应用：

application *application-name*

运行该命令后，系统进入应用配置模式。

no application *application-name*

- *application-name* – 指定自定义应用的名称。长度范围是 1 至 31 个字符。该名称在整个系统中必须是唯一的。

进入自定义应用特征配置模式

进入自定义应用特征配置模式，在全局配置模式下使用以下命令：

app-signature

创建和删除自定义应用特征规则

系统支持用户在两种配置模式下创建自定义应用特征规则，分别是：

- 自定义应用特征配置模式：配置自定义应用的所有特征。
- 应用特征规则配置模式：分别配置自定义应用的任意一个特征。

在自定义应用特征配置模式配置自定义应用特征规则

在自定义应用特征配置模式下使用以下命令，配置自定义应用的所有特征，并且用该命令 no 的形式删除一个自定义应用特征规则：

signature from { *src-addr* | *src-ip* } **to** { *dst-addr* | *dst-ip* } **protocol** {**tcp** | **udp**} **dst-port** *min-port* [*max-port*] [**src-port** *min-port* [*max-port*]] **application** *application-name*

- *src-addr* – 指定自定义应用特征的地址簿条目类型源地址。
- *src-ip* – 指定自定义应用特征的 IP 成员类型源地址。
- *dst-addr* – 指定自定义应用特征的地址簿条目类型目的地址。
- *dst-ip* – 指定自定义应用特征的 IP 成员类型目的地址。
- **dst-port** *min-port* [*max-port*] – 指定自定义应用特征的目的端口号。如果目的端口号为一个范围，*min-port* 为最小目的端口号，*max-port* 为最大目的端口号。目的端口号的范围是 0 到 65535，并且目的端口号不能为单一的 0，例如，目的端口号可以是 0 到 20，但是不能仅为 0。
- **src-port** *min-port* [*max-port*] – 指定自定义应用特征的源端口号。如果源端口号为一个范围，*min-port* 为最小源端口号，*max-port* 为最大源端口号。源端口号的范围是 0 到 65535。
- *application-name* – 指定特征规则所属于的应用名称。

在应用特征规则配置模式配置自定义应用特征规则

在应用特征规则配置模式下，可以分别配置自定义应用的任意一个特征。

创建一个自定义应用特征规则并进入应用特征规则配置模式，如果指定的应用特征规则 ID 已存在，则直接进入应用特征规则配置模式。请在自定义应用特征配置模式下使用以下命令，并且用该命令 no 的形式删除一个自定义应用特征规则：

signature id *id*

no signature id *id*

- *id* – 指定自定义应用特征规则 ID。

配置自定义应用特征规则条目

一个自定义应用特征规则中可以包含多个特征规则条目，这些条目之间是与（AND）关系，即流量必须满足自定义应用特征规则中的所有条目才会认定为命中了该条应用特征规则，从而识别出对应的应用类型。

用户需配置的自定义应用特征规则的条目主要包括：

- 源安全域
- 源/目的 IP 地址
- TCP 或 UDP 类型应用的源和目标端口号或者 ICMP 类型应用的 type 和 code 值
- 应用名称

指定特征规则的源安全域，在应用特征规则配置模式下输入以下命令：

src-zone *zone-name*

- *zone-name* – 指定特征规则的源安全域名称。

指定特征规则的地址簿条目类型源地址，在应用特征规则配置模式下输入以下命令：

src-addr *src-addr*

- *src-addr* – 自定义应用特征的地址簿条目类型源地址。

指定特征规则的 IP 成员类型源地址，在应用特征规则配置模式下输入以下命令：

src-ip *src-ip*

- *src-ip* – 自定义应用特征的 IP 成员类型源地址。

指定特征规则的地址簿条目类型目的地址，在应用特征规则配置模式下输入以下命令：

dst-addr *dst-addr*

- *dst-addr* – 自定义应用特征的地址簿条目类型目的地址。

指定特征规则的 IP 成员类型目的地址，在应用特征规则配置模式下输入以下命令：

dst-ip *dst-ip*

- *dst-ip* – 自定义应用特征的 IP 成员类型目的地址。

指定特征规则的 TCP 或 UDP 类型条目，在应用特征规则配置模式下输入以下命令：

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

- **dst-port** *min-port* [*max-port*] – 指定自定义应用特征的目的端口号。如果目的端口号为一个范围，*min-port* 为最小目的端口号，*max-port* 为最大目的端口号。目的端口号的范围是 0 到 65535，并且目的端口号不能为单一的 0，例如，目的端口号可以是 0 到 20，但是不能仅为 0。
- **src-port** *min-port* [*max-port*] – 指定自定义应用特征的源端口号。如果源端口号为一个范围，*min-port* 为最小源端口号，*max-port* 为最大源端口号。源端口号的范围是 0 到 65535。

指定特征规则的 ICMP 类型条目，在应用特征规则配置模式下输入以下命令：

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

- *type-value* – 指定自定义应用特征的 ICMP type 值。范围是 3（Destination-Unreachable）、4（Source Quench）、5（Redirect）、8（Echo）、11（Time Exceeded）、12（Parameter Problem）、13（Timestamp）和 15（Information）以及 any（表示以上所有 type 值）。
- **code** *min-code* [*max-code*] – 指定自定义应用特征的 ICMP code 值。范围是 0 到 5。默认值是 0。

指定特征规则的其它类型条目，在应用特征规则配置模式下输入以下命令：

protocol other-protocol *protocol-number*

- *protocol-number* – 指定自定义应用特征的协议号。范围是 1 到 255。

指定特征规则的应用名称，在应用特征规则配置模式下输入以下命令：

application *application-name*

- *application-name* – 指定特征规则的应用名称。

使用以上命令 no 的形式可以删除特征规则条目。并且已经创建的特征规则条目不能修改只能删除。

配置应用超时时间

用户可以配置应用的超时时间，如果不指定超时时间，系统会使用协议的默认值，在应用配置模式下，使用以下命令：

timeout {**tcp** | **udp** | **icmp** | **other-protocol**} *timeout-value*

- **tcp** | **udp** | **icmp** | **other-protocol** – 指定协议类型。
- *tiemout-value* – 指定应用的超时时间，取值范围为 1 到 864000 秒。

修改自定义应用特征规则排列顺序

每一条自定义应用特征规则都有唯一一个 ID 号。流量进入安全网关时，安全网关对自定义应用特征规则进行顺序查找，然后按照查找到的相匹配的第一条规则对流量进行处理。但是，自定义应用特征规则 ID 的大小顺序并不是规则查找时的匹配顺序。使用 **show app-signature static** 命令列出的特征规则顺序才是应用特征规则匹配顺序（系统将由上到下进行查找）。用户在创建自定义应用特征规则时可以指定该特征规则的排列位置，也可以在自定义应用特征配置模式下修改其位置。自定义应用特征的排列位置可以是绝对位置，即处在首位（Top）或者处在末位（Bottom），也可以是相对位置，即位于某个 ID 之前或之后。修改自定义应用特征规则排列顺序，在自定义应用特征配置模式下使用以下命令：

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

自定义应用组（Application Group）

用户将一些应用组织到一起便组成了应用组。用户可以直接将应用组应用到安全网关策略中，这样便简化了管理。应用组有以下特征：

- 应用簿中的每一条应用都可以被一个或多个应用组引用。
- 每个应用组中既可以包含预定义应用，也可以包含用户自定义应用。
- 应用组可以包含应用组。系统的应用组支持 8 层嵌套。

应用组还有以下限制：

- 应用组名称与应用名称不能相同。
- 被策略引用的应用组不能被删除。如果要删除一个应用组，必须首先从其它模块中删除对该应用组的引用。
- 如果用户从应用簿中删除了一条用户自定义应用，该条应用也将会从所有引用它的应用组中被删除。

创建和删除应用组

创建一个应用组并将该组添加到应用簿中，请在全局配置模式下，输入以下命令：

application-group *application-group-name*

注意:应用组的名称必须是唯一的。

运行该命令后，系统进入应用组配置模式。

删除一个应用组，请在全局配置模式下，输入以下命令：

no application-group *application-group-name*

为应用组添加和删除应用或者应用组

应用组的成员可以是一条应用，也可以是一个应用组。为应用组添加或者删除应用，请在应用组配置模式输入以下命令：

application {*application-name* | *application-group-name*}

no application { *application-name* | *application-group-name*}

为应用组添加应用或者应用组时，请注意以下两点：

- 应用组中的应用必须是唯一的。
- 每个应用组最多可以包含 64 个应用；应用组与应用组之间最多可以嵌套 8 层。

为应用或者应用组添加/删除描述信息

在应用或应用组配置模式下，用户可以通过使用以下命令为应用或应用组添加描述信息。

description *description*

- *description* – 指定应用或应用组的描述信息。范围是 1 到 255 字节。

在 CLI 的应用或应用组配置模式下，使用以下命令删除应用或应用组的描述信息。

no description

应用识别

系统中的多个功能模块需要根据数据流的应用类型（使用 **show application list** 命令可以查看Application ID 和 Application 名称的对应关系）对数据流进行相应的处理，例如统计集和 QoS 管理。所以系统需要首先对数据流进行识别，然后才能根据识别结果（Application ID）以及配置进行统计和管理。

动态识别

动态识别即系统可以根据应用的特征（signature）自动进行识别。系统对应用的自动识别是基于安全域实现的，默认情况下，所有安全域的自动识别功能为关闭状态。开启安全域的动态识别功能，在安全域配置模式下，使用以下命令：

application-identify

开启动态识别功能后，系统会对所有支持的动态识别应用进行识别。通过 show session 命令，可以查看到被识别的会话信息。在安全域配置模式下，使用该命令 no 的形式关闭安全域的动态识别功能：

no application-identify

不开启安全域的自动识别功能情况下，系统仍可以通过配置适当的策略规则对某种特定的应用进行识别。例如对 QQ 进行识别，需要配置以下两条策略规则（以从 untrust 域到trust 域的策略规则为例）：

```
hostname(config)# policy-global
hostname(config-policy)# rule from any to any application QQ permit
Rule id 5 is created
hostname(config-policy)# rule from any to any application any permit
Rule id 6 is created
hostname(config-policy)# exit
hostname(config)#
```

应用识别缓存表

应用识别缓存表存储应用信息，用以为应用识别以及策略路由功能提供支持。系统支持动态应用识别缓存表以及静态应用识别缓存表。

- 动态应用识别缓存表：存储系统通过动态学习获得的应用信息（动态识别结果信息）。
- 静态应用识别缓存表：存储静态应用信息。该缓存表包含在应用特征库中。

在不同的使用场景下，用户可根据需要，对应用缓存表进行相关配置。

启用/禁用应用识别缓存表

动态和静态应用识别缓存表默认都处于启用状态。禁用动态应用识别缓存表后，系统会继续向缓存表中写入缓存条目，但不会基于缓存表中的条目执行应用识别。静态应用识别缓存表只有在动态应用缓存表为启用状态时才生效。禁用动态应用识别缓存表的同时也会禁用静态应用识别缓存表。

禁用/启用动态应用识别缓存表，在全局配置模式下，使用以下命令：

- 禁用：app cache disable
- 启用：no app cache disable

禁用/启用静态应用识别缓存表，在全局配置模式下，使用以下命令：

- 禁用：app cache static disable
- 启用：no app cache static disable

指定动态应用识别缓存表应用方式

用户可以指定动态应用识别缓存表的应用方式。在全局配置模式下，使用以下命令：

app cache {**cache-strict** | **response-check** | **pbr-check-strict**}

- **cache-strict** – 适用于源 NAT 场景（内网客户端通过 NAT 设备访问外网服务器）。在源 NAT 环境下，配置该参数可有效避免应用误识别。该选项默认为禁用状态。
- **response-check** – 当系统有可能遭受到单方向数据包攻击时，为保证应用识别的准确性，建议开启该选项。该选项默认为禁用状态。
- **pbr-check-strict** – 指定策略路由的应用识别方式。默认情况下，即使系统已经通过动态应用识别缓存表识别出策略路由中的应用，仍要继续执行动态识别，并根据最终识别结果按照策略路由选路。配置该参数后，系统通过动态应用识别缓存表识别出应用后不再执行动态识别，直接根据识别结果按照策略路由选路。

取消动态应用识别缓存表的上述应用方式，使用该命令 no 的形式：

no app cache {**cache-strict** | **response-check** | **pbr-check-strict**}

清除应用识别缓存表信息

清除动态应用识别缓存表中的所有条目，在任意模式下，使用以下命令：

clear app cache table

清除静态应用识别缓存表中的所有条目，在任意模式下，使用以下命令：

clear app cache table static

查看应用识别缓存表信息

查看系统是否启用动态和静态应用识别缓存表及缓存表的配置信息，在任意模式下，使用 **show app cache status** 命令。

特征库更新

由于各种应用软件的升级更新快，为保证设备能够及时响应各种应用软件的变化，做出识别，系统提供特征库更新功能，用户可以下载最新的特征库文件并将其加载到设备。系统定期将新的特征库文件放在网 站，用户需要首先下载该文件，然后将下载的文件装载到设备。

通过 CLI 装载特征库文件，在执行模式下，使用以下命令：

import application-signature from {**ftp server** *ip-address* [**user** *user-name* **password** *password*] | **tftp server** *ip-address*} *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。
- *file-name* – 指定需要装载的特征库文件的名称。

特征库文件装载成功后，如果特征库文件仅对已有应用进行更新升级，则不需要重启设备，如果有新动态识别应用添加到系统，则必须重启设备使新添加应用可用。

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，为确保特征库能够自动正常升级，需要在设备上指定代理服务器的 IP 地址和端口号。

为应用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：

app 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 app update proxy-server** {**main** | **backup**}命令

应用过滤组

为了细分应用种类以及简化用户重复的搜索，系统支持定义应用过滤组。用户可依次根据应用的主类别、子类别、所用技术、风险等级、特征等条件定义应用过滤组。

应用过滤组的配置步骤如下：

1. 创建应用过滤组的名称
2. 根据主类别过滤应用
3. 根据子类别过滤应用
4. 根据所用技术过滤应用
5. 根据风险等级过滤应用
6. 根据特性过滤应用。应用的特性包括易逃逸、大量消耗带宽、能够传输文件、存在已知漏洞、易被滥用、被其他应用使用、被恶意软件利用、已被大规模使用。

创建应用过滤组的名称

创建应用过滤组的名称，在全局配置模式下使用以下命令：

application-filter *filter-name*

- *filter-name* – 指定应用过滤组的名称。

使用 no application-filter *filter-name* 删除应用过滤组名称。

根据主类别过滤应用

根据主类别过滤应用，在应用过滤组配置模式下，使用以下命令：

category *category-type*

- *category-type* – 为该应用过滤组指定应用的主类别名称。

使用 no category *category-type* 删除应用过滤组的主类别。

根据子类别过滤应用

根据子类别过滤应用，在应用过滤组配置模式下，使用以下命令：

subcategory *subcategory-type*

- *subcategory-type* – 为该应用过滤组指定应用的子类别名称。

使用 no subcategory *subcategory-type* 删除应用过滤组的子类别。

根据所用技术过滤应用

根据该应用的所用技术过滤应用，在应用过滤组配置模式下，使用以下命令：

technology *technology-type*

- *technology-type* – 为该应用过滤组指定应用的所用技术名称。

使用 no technology *technology-type* 删除应用过滤组的技术名称。

根据风险等级过滤应用

根据风险等级过滤应用，在应用过滤组配置模式下，使用以下命令：

risk *risk-value*

- *risk-value* – 为该应用过滤组指定应用的风险等级。取值范围为 1 至 5，数字越大，表示风险等级越高。

使用 no risk *risk-value* 删除应用过滤组的风险等级。

根据特性过滤应用

根据应用特性过滤应用，在应用过滤组配置模式下，使用以下命令：

- 根据特性易逃逸过滤应用：**evasive** [yes | no]
- 根据特性大量消耗带宽过滤应用：**excessive-bandwidth** [yes | no]
- 根据特性能够传输文件过滤应用：**file-transfer** [yes | no]
- 根据特性存在已知漏洞过滤应用：**known-vunerabilities** [yes | no]
- 根据特性易被滥用过滤应用：**prone-to-misuse** [yes | no]
- 根据特性被其它应用使用过滤应用：**tunnels-other-apps** [yes | no]
- 根据特性被恶意软件利用过滤应用：**used-by-malware** [yes | no]
- 根据特性已被大量使用过滤应用：**widely-used** [yes | no]

自定义应用配置示例

例如，创建名为 my-application 的自定义应用，并为my-application 添加以下配置：

- 为 my-application 添加一个自定义应用特征规则，特征规则 ID 为 1；
- 指定应用特征规则条目：
  源安全域：untrust
  源 地 址 ： any
  目的地址： any
  TCP 类型应用，目的端口号为 2121；

请参考以下命令：

```
hostname(config)# app-signature
hostname(config-appsig)# signature id 1
hostname(config-appsig-rule)# application my-application
hostname(config-appsig-rule)# src-zone untrust
hostname(config-appsig-rule)# src-addr any
hostname(config-appsig-rule)# dst-addr any
hostname(config-appsig-rule)# protocol tcp dst-port 2121
hostname(config-appsig-rule)# exit
```

```
hostname(config-appsig)# exit
hostname(config)#
```

完成配置后，符合特征规则 1 的流量被识别为名称为 my-application 的应用。

DNS

DNS 为域名系统（Domain Name System）的缩写。DNS 是一种组织成域层次结构的计算机和网络服务命名系统，用于 TCP/IP 网络，主要用来寻找 Internet 域名（如 www.xxxx.com）并转化为 IP 地址（如“10.1.1.1”）以定位相应的计算机和相应服务。

StoneOS 的 DNS 功能

DNS 功能如下：

- 名字服务：为设备配置DNS 服务器和默认域名。
- DNS 代理功能： 设备作为 DNS 代理服务器，为与其连接的PC 等（客户端）提供 DNS 代理功能。同时， 设备可以根据域名选择不同的域名服务器。
- 解析：为设备的 DNS 功能设置重试次数和响应超时时间。
- 缓存：将DNS 映射项储存在缓存中，用以提高查找速度。

配置 DNS 名字服务

DNS 名字服务的配置包含：

- 为 设备配置域名
- 为 设备设置 DNS 服务器

设置域名

用户可以为设备指定一个域名。 设备会将域名作为后缀添加到用户输入的名称后。例如，如果设置域名为“sina.com”，在 设备上 Ping“www”，系统会把域名加上去查找“www.sina.com”。并且，把域名设置为“sina.com”和“com”后的解析顺序不同：设置为“sina.com”后，Ping“www”，系统会先查找 www.sina.com；而设置为“com”后，Ping“www.sina”，系统会先查找 www.sina 然后再查找 www.sina.com。

设置系统域名，在全局配置模式下使用以下命令：

ip domain name *domain-name*

- *domain-name* – 指定域名。名称长度可以是 1 到 255 个字符，但是在两个句点（.）之间，最多可以有 63 个字符。

使用 **no ip domain name** 命令恢复默认域名。

以下是设置默认域名名称为 test.com 的命令配置示例：

```
hostname(config)# ip domain name test.com
```

设置 DNS 域名服务器

该命令指定的DNS 域名服务器为设备进行 DNS 解析时使用的服务器。设置DNS 域名服务器，在全局配置模式下使用以下命令：

ip name-server *server-address1* [*server-address2*] ... [*server-address6*] [**vrouter** *vrouter-name*]

- *server-address1* – 指定域名服务器的 IP 地址。用户最多可配置 6 个域名服务器。用户可以使用一条命令配置 6 个域名服务器，也可分多条命令配置，即运行命令 **ip name-server 1.1.1.1 2.2.2.2** 与运行命令 **ip name-server 1.1.1.1** 和 **ip name-server 2.2.2.2** 等效，最多可以配置 64 个域名服务器。
- *vrouter-name* – 为指定的VRouter 指定 DNS 代理服务器。

使用 **no ip name-server** *server-address1* [*server-address2*] ... [*server-address6*]取消对 DNS 域名服务器的配置。

配置 DNS 代理功能

DNS 代理功能通过 DNS 代理规则来实现。DNS 代理规则分为过滤条件和行为两部分。入接口、源地址、目的地址及 DNS 域名构成 DNS 代理规则的过滤条件。DNS 代理规则的行为包括代理、放行及阻断共三种。当代理规则的行为被指定为代理时，用户需同时配置 DNS 代理服务器，这样满足条件的 DNS 请求将通过指定的 DNS 代理服务器进行地址解析。

每条DNS 代理规则都有其独有的 ID 号。规则 ID 会在定义规则时自动生成，同时用户也可以按自己的需求为规则指定 ID 号。整个系统的所有策略规则有特定的排列顺序。在流量进入系统时，系统会对流量按照找到的第一条与过滤条件相匹配的规则进行处理。

DNS 代理功能的配置包括：

- 配置DNS 代理规则
- 修改DNS 代理规则的排列顺序
- 配置DNS 代理服务器探测功能
- 开启/关闭 DNS 代理的 UDP 报文校验和功能
- 指定DNS 代理响应报文的 TTL

配置 DNS 代理规则

用户可以通过配置DNS 代理规则，对进入设备的DNS 流量进行控制。DNS 代理规则配置包括：

- 创建DNS 代理规则
- 配置DNS 代理匹配条件
- 指定DNS 代理规则行为
- 配置DNS 代理服务器
- 配置描述信息
- 启用/禁用 DNS 代理规则

创建 DNS 代理规则

创建DNS 代理规则或进入DNS 代理规则配置模式，在全局配置模式下使用以下命令：

dns-proxy rule [**id** *id*]

- **id** *id* – 指定 DNS 代理规则的 ID。如果不指定，系统将会为 DNS 代理规则自动分配一个 ID。规则 ID 在整个系统中必须是唯一的。

在全局配置模式下，使用命令 **no dns-proxy rule id** *id* 删除 DNS 代理规则。

配置 DNS 代理过滤条件

DNS 代理过滤条件包括DNS 请求的入接口、源地址、目的地址及DNS 域名共四种。用户需同时配置四种过滤条件，配置完成后，系统将对 DNS 请求进行过滤。只有 DNS 请求同时满足以上四种条件时，系统才认为匹配成功。

指定 DNS 入接口

用户可指定 DNS 请求的入接口，对DNS 请求报文进行过滤，可指定多个入接口。指定后，系统将按照规则设定的行为，对该入接口流量进行处理。在 DNS 代理规则配置模式下，使用以下命令：

- 添加DNS 流量的入接口：**ingress-interface** *interface-name*
- 删除DNS 流量的入接口：**no ingress-interface** *interface-name*

指定 DNS 源地址

用户可指定 DNS 请求的源地址，对DNS 请求报文进行过滤。用户可指定多条源地址类目。指定后，系统将按照规则设定的行为，对匹配成功的流量进行处理。在 DNS 代理规则配置模式下，使用以下命令：

- 添加地址簿条目类型源地址：**src-addr** { *addr-name* | **any**}
- 删除地址簿条目类型源地址：**no src-addr** { *addr-name*| **any**}
- 添加 IP 成员类型源地址：**src-ip** {*ip/netmask* | *ip-address netmask*}
- 删除 IP 成员类型源地址：**no src-ip** {*ip/netmask* | *ip-address netmask*}
- 添加 IP 地址范围类型源地址：**src-range** *min-ip max-ip*
- 删除 IP 地址范围类型源地址：**no src-range** *min-ip max-ip*

指定 DNS 目的地址

用户可指定 DNS 请求的目的地址，对 DNS 请求报文进行过滤。用户可指定多条目的地址类目。指定后，系统将按照规则设定的行为，对匹配成功的流量进行处理。在 DNS 代理规则配置模式下，使用以下命令：

- 添加地址簿条目类型目的地址：**dst-addr** { *addr-name* | **any**}
- 删除地址簿条目类型目的地址：**no dst-addr** { *addr-name* | **any**}
- 添加 IP 成员类型目的地址：**dst-ip** {*ip/netmask* | *ip-address netmask*}
- 删除 IP 成员类型目的地址：**no dst-ip** {*ip/netmask* | *ip-address netmask*}
- 添加 IP 地址范围类型目的地址：**dst-range** *min-ip max-ip*
- 删除 IP 地址范围类型目的地址：**no dst-range** *min-ip max-ip*

指定 DNS 域名

用户可指定 DNS 域名，用来匹配 DNS 请求中的域名，对DNS 请求报文进行过滤。用户可指定多条域名过滤条件。指定后，系统将按照规则设定的行为，对相应的DNS 请求流量进行处理。在 DNS 代理规则配置模式下，使用以下命令：

domain { **any** | *domain-name* | **host-book** *host-book-entry* }

- *domain-name* - 指定需匹配的具体域名。

- **any** – 指定为可匹配任意域名。
- **host-book** *host-book-entry* – 指定需匹配的域名条目的名称。

使用 **no domain any** | *domain-name* | **host-book** *host-book-entry* 删除DNS 域名。

配置 DNS 代理规则行为

对符合过滤条件的DNS 请求，系统可对其进行代理、放行和阻断流量共 3 种处理行为，用户可按需进行设定，在DNS 代理规则配置模式下，使用以下命令：

action {**proxy** [**rollback**] | **bypass** | **block**}

- **proxy** [**rollback**] – 将 DNS 代理规则的行为指定为代理，即 DNS 请求将通过代理服务器进行DNS 解析。用户可按需配置 **rollback** 属性，配置 **rollback** 后，当 DNS 请求找不到DNS 服务器或服务器无法解析DNS 地址时，系统将对 DNS 请求报文进行放行,然后转发给原始报文的 DNS 服务器。
- **bypass** – 将 DNS 代理规则的行为指定为放行，即DNS 请求将被转发给原始报文的 DNS 服务器。
- **block** – 将 DNS 代理规则的动作指定为阻断，即DNS 请求将被丢弃。

配置 DNS 代理服务器

当用户将DNS 代理规则的行为指定为代理时，需继续指定 DNS 代理服务器。每条DNS 规则最多可指定 6 个 DNS 代理服务器。用户可按需为 DNS 服务器指定出接口和首选属性。当用户配置多个DNS 服务器时，将首先选择首选 DNS 服务器进行域名解析。若没有指定首选服务器，系统将查询是否有指定出接口的 DNS 服务器；若有，则轮询选择出接口 DNS 服务器；若无出接口 DNS 服务器，即只有普通的DNS 服务器，则轮询选择此类普通的 DNS 服务器。

在 DNS 代理规则配置模式下，用户可以通过使用以下命令添加一条条目到DNS 代理服务选择列表中：

name-server *server-ip* [**vrouter** *vrouter-name*| **egress-interface** *interface-name*| **preferred**]

- *server-ip* – 指定DNS 代理服务器的 IP 地址。
- *vrouter-name* – 指定 DNS 代理服务器所属的虚拟路由器。
- *interface-name* – 表示 DNS 代理服务器将对该出接口转发出的 DNS 请求进行 DNS 解析。
- *preferred* – 指定 DNS 代理服务器为首选服务器，一条DNS 代理规则仅可指定一台服务器为首选服务器。

使用 **no name-server** *server-ip* [**vrouter** *vrouter-name*]删除 DNS 代理服务器。

配置描述信息

对 DNS 代理规则添加描述信息，在DNS 代理规则配置模式下，使用以下命令：

description *description*

- *description* – 指定描述信息，如规则的作用。取值范围是 0 到 127 个字符。

使用 **no description** 删除描述信息。

启用/禁用 DNS 代理规则

默认情况下，配置完成的DNS 代理规则会在系统中立即生效。用户可以通过命令禁用某条规则，使其不对流量进行控制。禁用或者启用某条规则，在 DNS 代理规则配置模式下，使用以下命令：

- 禁用：**disable**
- 启用：**enable**

修改 DNS 代理规则的排列顺序

DNS 代理规则通过 ID 进行唯一标识。DNS 请求到达设备后，设备对DNS 代理规则进行顺序查找，然后按照查找到的相匹配的第一条规则对 DNS 请求进行处理。但是，DNS 代理规则 ID 的大小顺序并不是规则查找时的匹配顺序。使用 **show dns-proxy** 命令列出的规则顺序才是规则匹配顺序（系统将由上到下进行查找匹配）。默认情况下，系统会将新创建的 DNS 代理规则放到所有规则的末尾，用户可以修改 DNS 代理规则的排列位置。DNS 代理规则的排列位置可以是绝对位置，即处在首位（Top）或者处在末位（Bottom），也可以是相对位置，即位于某个 ID 之前或之后。修改规则排列顺序， 在全局配置模式下，使用以下命令：

dns-proxy move *rule-id* {**top** | **bottom** | **before** *rule-id* | **after** *rule-id* }

- **move** *rule-id* – 指定需排列顺序的 DNS 代理规则的 ID。
- **top** | **bottom** | **before** *rule-id* | **after** *rule-id* – 指定 DNS 代理规则的位置。默认情况下，系统会将新创建的 DNS 代理规则放到所有规则的末尾。
- **top** – 指定DNS 代理规则的位置为所有规则的首位。
- **bottom** – 指定 DNS 代理规则的位置为所有规则的末尾。
- **before** *rule-id* – 指定DNS 代理规则的位置为某个规则 ID 之前。
- **after** *rule-id* – 指定 DNS 代理规则的位置为某个规则 ID 之后。

配置 DNS 代理服务器探测功能

DNS 代理服务器探测功能即对DNS 代理服务器的可达性进行检测。配置该功能后，系统将按照指定的探测间隔周期性地对DNS 代理服务器进行探测，并且及时将不可达的服务器 IP 地址从 DNS 解析列表中删

除，待链路恢复后再重新加入到轮询解析列表。默认情况下，DNS 解析探测功能是开启的。配置 DNS 代理服务器探测的探测间隔，在全局配置模式下使用以下命令：

dns-proxy server-track [**interval** *interval-time*]

- *interval-time* – 指定 DNS 代理解析探测的探测间隔。取值范围为 3 至 60s，默认值为 10s。

在全局配置模式下，使用 **no dns-proxy server-track** 关闭 DNS 代理解析探测功能。

开启/关闭 DNS 代理的 UDP 报文校验和功能

设备开启DNS 代理功能后，DNS 代理的 UDP 报文校验和功能默认情况下是开启的，即 UDP 报文头部经过更改后设备会重新计算UDP 校验和。用户如果希望提高设备的性能，可以关闭DNS 代理UDP 报文校验和功能，设备将不再进行 UDP 校验和的计算。开启/关闭 DNS 代理的 UDP 报文校验和功能，请在全局配置模式下使用以下命令：

- 开启DNS 代理的 UDP 报文校验和功能：**dns-proxy udp-checksum enable**
- 关闭DNS 代理的 UDP 报文校验和功能：**dns-proxy udp-checksum disable**

指定 DNS 代理响应报文的 TTL

DNS 代理响应报文的 TTL(Time-to-Live)是指域名解析记录在 DNS 客户端上的保存时间。设置DNS 代理响应报文的 TTL，在全局配置模式下使用以下命令：

dns-proxy ttl *ttl-time*

- *ttl-time* – 指定 DNS 代理响应报文的 TTL。如果超过设定的 TTL 值， DNS 客户端上缓存的域名解析记录将被清除。取值范围是 30 到 600 秒，默认值是 60。

使用 **dns-proxy ttl disable** 关闭修改报文 TTL 值的功能。

查看 DNS 代理规则信息

用户可以在任何模式下，通过 **show** 命令查看 DNS 代理规则的具体信息。具体命令以下：

show dns-proxy [**rule id** *rule-id*]

- *rule-id* – 显示指定 DNS 代理规则的详细信息。如果不指定名称则显示所有DNS 代理规则。

解析

用户可以为设备的DNS 功能设置DNS 请求重试次数、DNS 请求响应超时时间、DNS 响应报文的 TTL 和负载均衡分发 DNS 请求。

设置 DNS 请求的响应超时时间

设 备向 DNS 服务器发送DNS 请求后，会等待 DNS 服务器的 DNS 响应，如果一定时间内，仍没有响应， 设备会再次发送请求。该命令指定设备再次发送请求前，等待响应的时间。设置DNS 请求的响应超时时间，在全局配置模式下，使用以下命令：

ip domain timeout *timeout-value*

- *timeout-value* – 指定超时时间。取值范围为 1 到 3 秒。默认超时时间为 2 秒。

使用 **no ip domain timeout** 恢复默认超时时间。

设置 DNS 请求重试次数

当 设备发送DNS 请求时，如果在超时时间内得不到对方的DNS 响应，设备会再次发出 DNS 请求。该命令设置的是发送 DNS 请求的重试次数。如果在指定的重试次数内仍得不到响应， 设备会向下一个 DNS 服务器发送 DNS 请求。设置重试次数，在全局配置模式下，使用以下命令：

ip domain retry *times*

- *times* – 指定重试次数。取值范围为 1 到 3 次。默认重试次数为 2 次。

使用 **no ip domain retry** 恢复默认重试次数。

指定 DNS 解析动态缓存的 TTL

TTL(Time-to-Live)是域名解析动态缓存在设备上的保存时间。设置 DNS 解析动态缓存的 TTL，在全局配置模式下使用以下命令：

ip domain ttl *ttl-time*

- *ttl-time* – 指定 DNS 解析动态缓存的 TTL。如果超过设定的 TTL 值，系统将清除设备上缓存的域名解析记录。取值范围是 60 到 600 秒。默认值是 60。

开启 DNS 解析日志功能

用户可以通过开启记录DNS 解析日志功能，将 DNS 解析结果进行记录，并且生成日志信息，日志内容包括域名、解析后的 IP 地址以及生成时间。默认情况下，该功能是关闭的。开启记录 DNS 解析日志功能，在全局配置模式下，使用以下命令：

ip domain response-log

使用 **no ip domain response-log** 关闭记录 DNS 解析日志功能。

缓存

在使用 DNS 功能过程中，系统可以将 DNS 映射条目储存到缓存中以提高查找速度。系统有以下三种获得 DNS 映射条目的方法：

- 动态获得：来自DNS 响应。
- 静态获得：手动添加DNS 映射条目到缓存。
- 注册获得：设备的一些功能模块，例如 NTP、AAA 和地址簿等，定义的 DNS 主机。

用户可以通过命令添加静态 DNS 映射条目到缓存、查看系统的 DNS 映射条目以及清除DNS 动态映射条目。

添加静态 DNS 映射条目

手动添加DNS 映射条目到缓存，在全局配置模式使用以下命令：

ip host *host-name* {*address1* [*address2*] ... [*address8*]} [**vrouter** *vrouter-name*]

- *host-name* – 指定主机名称。名称范围是 1 到 255 个字符。
- {*address1* [*address2*] ... [*address8*]} – 指定主机的 IP 地址。最多可设置 8 个 IP 地址。
- *vrouter-name* – 添加指定VRouter 下的 DNS 映射条目。

使用 **no ip host** *host-name* 删除指定的静态 DNS 映射条目。

查看 DNS 映射条目

使用 **show** 命令可以查看系统中所有的 DNS 映射条目。查看 DNS 映射条目，在任何模式下使用以下命令：

show ip hosts [*host-name*] [**vrouter** *vrouter-name*]

- *host-name* – 显示指定主机的DNS 映射条目。
- *vrouter-name* - 显示指定 VRouter 下的 DNS 映射条目。

清除动态 DNS 映射条目

手动清除动态DNS 映射条目，在执行模式下使用以下命令。

clear host [*host-name* [**vrouter** *vrouter-name*]]

- *host-name* – 清除指定主机的DNS 映射条目。
- *vrouter-name* – 清除指定VRouter 下主机的 DNS 映射条目。

该命令用来清除指定的或者所有动态 DNS 映射条目。手工配置的静态DNS 映射项使用 **no ip host** 命令清除。

DNS Snooping

设备启用DNS 代理功能后，系统会对 DNS 响应报文进行监测。当系统发现与其匹配的通配符主机报文时，将自动建立监测列表（包括带通配符的主机名称、域名名称、老化时间、IP 地址和VRouter 名称等信息）。系统同时将列表中的 IP 地址下发到地址薄。成功下发后，用户可以通过PBR 引用地址薄的信息， 实现设备按指定链路访问主机的功能。

注意:使用 DNS Snooping 功能前，请先确保开启 DNS 代理功能，并配置了包含通配符的主机名称和 DNS 代理响应报文的 TTL。

指定 DNS Snooping 列表的老化时间

用户可以指定 DNS Snooping 表项的老化时间，如果超过设定的老化时间，系统将清空 DNS Snooping 表项中的信息，在全局配置模式下使用以下命令:

ip dns-resp-snooping ttl *ttl-time*

- *ttl-time* – 指定 DNS Snooping 表项的老化时间。范围是 60 到 86400 秒。默认值是 86400。建议此参数设置为较大值，使地址薄中 IP 地址的变更相对缓慢。

开启精确域名探测功能

当 DNS 流量经过设备时，系统支持开启精确域名探测功能，通过对 DNS 响应报文探测并且与系统地址簿中的域名进行匹配，当系统发现与其匹配的域名时，将记录域名对应的 IP 地址并下发到地址薄。默认情况下，精确域名探测功能是关闭的，系统会主动发起 DNS 请求，经过解析后获取域名对应 IP 地址。

开启精确域名探测功能，在全局配置模式下，使用以下命令:

ip dns-resp-snooping enable-specific

在全局配置模式下，使用 **no ip dns-resp-snooping enable-specific** 关闭精确域名探测功能。

指定 DNS 响应报文的处理速率

配置接收 DNS 响应报文的处理速率，当每秒钟接收DNS 响应报文的个数超过该指定值时，系统将丢弃超出的DNS 响应报文。在全局配置模式下使用以下命令:

ip dns-resp-snooping pak-limit *packet-limit*

- *packet-limit* – 指定接收DNS 响应报文的处理速率。范围是 0 到 4294967295。默认值是 0，即无速率限制。

查看 DNS Snooping 列表条目

用户通过 **show** 命令查看 DNS Snooping 列表条目。在任何模式下使用以下命令:

show ip dns-resp-snooping [**host**] [**vrouter** *vrouter-name*]

- *host* – 指定主机名称。
- *vrouter-name* – 指定 VRouter 名称。

同时用户可以通过以下命令查看通配符域名/精确域名 DNS Snooping 列表条目:

show dp-dns-resp-snooping {**specific** | **wildcard**} [*host*] [**vrouter** *vrouter-name*][**cpu** *cpu-number*] [**slot** *slot-number*]

- **specific** – 查看精确域名的 DNS Snooping 列表条目。
- **wildcard** - 查看通配符域名的 DNS Snooping 列表条目。
- *host* – 指定主机名称。
- **vrouter** *vrouter-name* – 指定 VRouter 名称。
- **cpu** *cpu-number* – 指定 cpu 名称，仅 SX 系列设备支持此参数。
- **slot** *slot-number* - 指定 slot 名称，仅 SX 系列设备支持此参数。

用户可以通过以下命令查看所有的精确域名和通配符域名的 DNS Snooping 列表条目。:

show dp-dns-resp-snooping all [**vrouter** *vrouter-name*][**cpu** *cpu-number*] [**slot** *slot-number*]

- **vrouter** *vrouter-name* – 指定 VRouter 名称。
- **cpu** *cpu-number* – 指定 cpu 号码，仅 SX 系列设备支持此参数。
- **slot** *slot-number* - 指定 slot 号码，仅 SX 系列设备支持此参数。

在任何模式下，用户可以使用以下命令清除所有的或者指定的 DNS Snooping 列表条目:

clear dns-resp-snooping [*host*] [**vrouter** *vrouter-name*]

- *host* – 指定主机名称。
- *vrouter-name* – 指定 VRouter 名称。

开启/关闭 DNS 功能

默认情况下，DNS 功能是开启的。开启/关闭 DNS 功能，在全局配置模式下使用以下命令:

- 开启：ip domain lookup
- 关闭：no ip domain lookup

显示 DNS 配置信息

用户可以在任何模式下使用以下命令查看系统中DNS 的配置信息：

show dns

DNS 配置举例

本节介绍一个DNS 的典型配置实例。

组网需求

公司通过设备将 trust 安全域中的 PC1 通过 DNS 代理上网。公网的DNS 域名服务器的 IP 地址为 202.106.0.20； 设备的ethernet0/0 接口的 IP 地址为 192.168.10.1/24，连接 trust 安全域中的PC1，IP 地址为 192.168.10.3 /24；ethernet0/1 接口的 IP 地址为 10.160.65.31/24，连接公网，公网为 untrust 安全域。

配置步骤

第一步：将设备各接口分配安全域并配置 IP 地址：

```
hostname# configure
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 192.168.10.1/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 10.160.65.31/24
hostname(config-if-eth0/1)# exit
```

第二步：在设备上配置DNS 代理规则：

```
hostname(config)# dns-proxy rule
hostname(config-dns-proxy-rule)# ingress-interface ethernet0/0
```

```
hostname(config-dns-proxy-rule)# src-addr any
hostname(config-dns-proxy-rule)# dst-addr any
hostname(config-dns-proxy-rule)# domain any
hostname(config-dns-proxy-rule)# action proxy
hostname(config-dns-proxy-rule)# name-server 202.106.0.20
hostname(config-dns-proxy-rule)# exit
```

第三步：在 PC1 上 ping www.sina.com.cn 可以正常解析到。

DDNS

DDNS 是动态域名服务（Dynamic Domain Name Server）的缩写，可以实现固定域名到动态 IP 地址之间的解析。通常情况下，用户每次连接因特网时都会从 ISP 得到一个动态 IP 地址，即用户每次连接因特网得到的 IP 地址都不同。动态域名解析功能可以将域名绑定到用户的动态 IP 地址，每次当用户连接到因特网时，它都会自动更新自己的动态 IP 与域名的绑定。

在使用 DDNS 功能之前，用户需要在 DDNS 服务的提供商那里进行注册，以获取动态域名。设备支持以下五个动态域名服务提供商：

- 3322.org：http://www.3322.org
- Huagai.net：http://www.ddns.com.cn
- ZoneEdit.com：http://www.zoneedit.com
- no-ip.com： http://www. no-ip.com
- dyndns.org：http://www.dyndns.org

请访问相应的主页进行注册。

配置 DDNS 功能

当设备的外网接口 IP 地址发生变化后，设备会向DDNS 服务器发送更新请求（HTTP 方式），来更新 IP 地址与域名的绑定。用户可以在设备上配置不同的 DDNS 服务名称，然后为 DDNS 服务名称配置 DDNS 参数，例如更新方式、DDNS 服务器和更新间隔时间等，最后将配置的 DDNS 服务名称绑定到接口上，从而启用 DDNS 功能。

- 配置 DDNS 服务名称
- 绑定 DDNS 服务名称到接口

配置 DDNS 服务名称

DDNS 服务参数配置需要在DDNS 服务名称配置模式下完成。在全局配置模式下，使用以下命令，用户可以创建一个 DDNS 服务名称、指定其更新类型并且进入指定的 DDNS 服务配置模式：

ddns name *ddns-name* **type http**

- *ddns-name* – 指定 DDNS 服务名称。
- **type http** – 指定 DDNS 服务的更新方式，即发送DDNS 更新请求的方式，为 HTTP。

运行该命令后，CLI 进入该 DDNS 服务名称的配置模式，用户可以为该DDNS 服务名称配置各种 DDNS 参数，包括 DDNS 服务器类型、DDNS 服务器名称和端口号、最小更新间隔、最大更新间隔以及 DDNS 用户名称密码。

使用 **no ddns name** *ddns-name* **type http** 命令删除指定的DDNS 服务名称。

指定 DDNS 服务器类型

设备支持通过五个 DDNS 服务商实现动态域名服务，分别是 3322.org、Huagai.net、ZoneEdit.com、no-ip.com 和 dyndns.org。指定 DDNS 服务商，在 DDNS 服务名称配置模式下使用以下命令：

type {**dyndns** | **huagai** | **no-ip** | **qdns** | **zoneedit**}

- **dyndns** - 指定 dyndns.org 作为 DDNS 服务商。
- **huagai** - 指定 Huagai.net 作为 DDNS 服务商。
- **no-ip** - 指定 no-ip.com 作为 DDNS 服务商。
- **qdns** - 指定 3322.org 作为DDNS 服务商。
- **zoneedit** - 指定 ZoneEdit.com 作为 DDNS 服务商。

使用 **no type** 命令取消对 DDNS 服务商的指定。

指定 DDNS 服务器名称和端口号

不同的 DDNS 服务器具有不同的服务器名称和端口号。指定 DDNS 服务器的名称和端口号，在 DDNS 服务名称配置模式下使用以下命令：

server name *server-name* **port** *port-number*

- *server-name* – 指定所配置 DDNS 服务器相应的服务器名称。
- *port-number* – 指定所配置 DDNS 服务器相应的服务器端口号。范围是 1 到 65535。

使用 **no server** 命令取消DDNS 服务器名称和服务器端口号的配置。

注意:此处配置的名称和端口号必须为 DDNS 服务器相对应的名称和端口号。如果不知道确切信息，请勿配置该命令。与 DDNS 服务器连接成功后，服务器会自动将服务器名称和端口号信息一并返回。

指定最小更新间隔

启用 DDNS 功能的接口的 IP 地址发生变化后， 设备需要向 DDNS 服务器发送更新请求。如果发送的请求没有响应， 设备会根据此处配置的最小更新间隔再次发送请求。例如，设置最小更新间隔为 5 分钟，当第一次失败后，设备会在 5 分钟后发出第二次请求，如果再次失败，设备会在 10（5x2）分钟后再次发出请求，再次失败，则在 20（10x2）分钟后发出请求，以此类推，直到时间为 120 分钟后，不再增加时间，即以固定的每隔 120 分钟发出一次请求。配置最小更新间隔时间，在DDNS 服务名称配置模式下使用以下命令:

minupdate interval *time-value*

- *time-value* – 指定最小更新间隔时间，单位为分钟。取值范围为 5 到 120 分钟。默认值为 5 分钟。

使用 **no minupdate** 恢复默认最小更新间隔时间。

指定最大更新间隔

最大更新间隔为在无 IP 地址变化的情况下，设备在多长时间后向 DDNS 服务器发出一次更新请求。配置 DDNS 最大更新间隔，在 DDNS 服务名称配置模式下使用以下命令:

maxupdate interval *time-value*

- *time-value* – 指定最大更新间隔时间，单位为小时。取值范围为 24 到 8760 小时。默认值为 24 小时。

使用 **no maxupdate** 恢复默认最大更新间隔时间。

指定 DDNS 用户

该命令指定的是在 DDNS 服务提供商处注册的用户信息。配置用户信息，在 DDNS 服务名称配置模式下使用以下命令:

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

- *user-name* - 在 DDNS 服务提供商处注册的用户名称。
- *user-password*- 与用户名称相对应的密码。

使用 **no user** 命令取消用户信息的指定。

绑定 DDNS 服务名称到接口

只有把配置的 DDNS 服务名称绑定到接口上，当接口 IP 地址发生变化时，域名才能够按照配置的 DDNS 参数进行更新。绑定接口到 DDNS 服务名称，在全局配置模式下，使用以下命令：

ddns enable *ddns-name* **interface** *interface-name* **hostname** *host-name*

- *ddns-name* – 指定配置好的 DDNS 服务名称。
- *interface-name* – 指定要绑定的接口的名称。
- *host-name* – 指定在相应 DDNS 提供商处申请得到的域名。

使用 **no ddns enable** *ddns-name* **interface** *interface-name* 取消接口与DDNS 服务名称的绑定。

显示 DDNS 信息

用户可以在任何模式下，通过 **show** 命令查看 DDNS 信息：

- 显示 DDNS 服务配置信息：**show ddns config** *ddns-name*
- 显示 DDNS 服务状态信息：**show ddns state** *ddns-name*

DDNS 配置举例

本节介绍一个 DDNS 的典型配置实例。

组网需求

设备的 ethernet0/1 在 untrust 域，接口通过 PPPoE 方式获得 IP 地址。当接口进行PPPoE 连接 IP 地址发生变化时，向 DDNS 服务器发送更新请求。

配置步骤

第一步：创建名为 pppoe1 的 PPPoE 实例，指定各项参数：

```
hostname(config)# pppoe-client group pppoe1
hostname(config-pppoe-group)# auto-connect 10
hostname(config-pppoe-group)# idle-interval 5
hostname(config-pppoe-group)# route distance 2
hostname(config-pppoe-group)# route weight 10
hostname(config-pppoe-group)# authentication any
```

```
hostname(config-pppoe-group)# user user1 password 123456
hostname(config-pppoe-group)# exit
hostname(config)#
```

第二步：配置 ethernet0/1：

```
hostname# configure
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address pppoe setroute
hostname(config-if-eth0/1)# pppoe enable group pppoe1
hostname(config-if-eth0/1)# exit
```

第三步：在设备上配置DDNS 服务：

```
hostname(config)# ddns name 3322 type http
hostname(config-ddns)# type qdns
hostname(config-ddns)# user test password 123456
hostname(config-ddns)# exit
```

第四步：将接口ethernet0/1 绑定到配置的 DDNS 服务名称 3322 上（从 3322.org 申请的域名为 net.3322.org）：

```
hostname(config)# ddns enable 3322 interface ethernet0/1 hostname net.3322.org
```

第五步：在设备上配置域名服务器以便能解析域名：

```
hostname(config)# ip name-server 202.106.0.20
```

第六步：触发 PPPoE 连接，以便接口的 IP 地址改变时触发 DDNS 服务：

```
hostname(config)# pppoe-client group pppoe1 connect
```

网络地址转换（NAT）

网络地址转换（NAT）简介

网络地址转换（Network Address Translation）简称为 NAT，是将 IP 数据包包头中的 IP 地址转换为另一个 IP 地址的协议。当 IP 数据包通过路由器或者设备时，路由器或者设备会把 IP 数据包的源 IP 地址和/或者目的 IP 地址进行转换。在实际应用中，NAT 主要用于私有网络访问外部网络或外部网络访问私有网络的情况。NAT 有以下优点：

- 通过使用少量的公有 IP 地址代表多数的私有 IP 地址，缓解了可用 IP 地址空间枯竭的速度。
- NAT 可以隐藏私有网络，达到保护私有网络的目的。

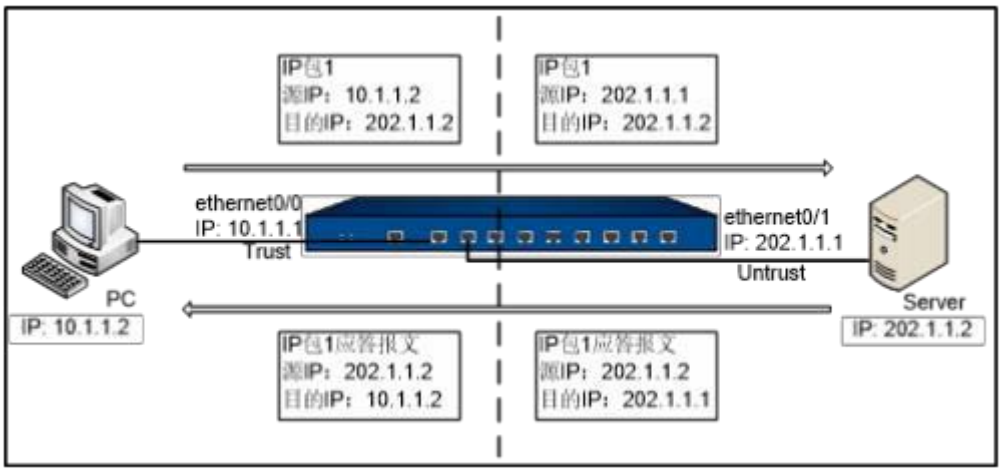
私有网络一般使用私有地址，RFC1918 规定的三类私有地址如下：

- A 类：10.0.0.0 - 10.255.255.255（10.0.0.0/8）
- B 类：172.16.0.0 - 172.31.255.255（172.16.0.0/12）
- C 类：192.168.0.0 - 192.168.255.255（192.168.0.0/16）

上述三个范围的 IP 地址不会在因特网上被分配，因而可以不必向 ISP（Internet Service Provider）或注册中心申请，而在公司或企业内部自由使用。

NAT 的基本转换过程

设备执行NAT 功能时，处于公有网络和私有网络的连接处。下图描述了NAT 的基本转换过程。



如上图所示， 设备处于私有网络和公有网络的连接处。当内部 PC（10.1.1.2）向外部服务器（202.1.1.2）发送一个 IP 包 1 时，IP 包将通过设备。 设备查看包头内容，发现该 IP 包是发向公有网络的，然后它将 IP 包 1 的源地址 10.1.1.2 换成一个可以在 Internet 上选路的公有地址 202.1.1.1，并将该 IP 包发送到外部服

务器，与此同时， 设备还在网络地址转换表中记录这一映射。外部服务器给内部PC 发送 IP 包 1 的应答报文 2（其初始目的地址为 202.1.1.1），到达设备后， 设备再次查看包头内容，然后查找当前网络地址转换表的记录，用内部 PC 的私有地址 10.1.1.2 替换目的地址。这个过程中，设备对PC 和 Server 来说是透明的。对外部服务器来说，它认为内部 PC 的地址就是 202.1.1.1，并不知道 10.1.1.2 这个地址。因此，

NAT“隐藏”了企业的私有网络。

StoneOS 的 NAT 功能

设备的 NAT 功能将内部网络主机的 IP 地址和端口替换为设备外部网络的地址和端口，以及将设备的外部网络地址和端口转换为内部网络主机的 IP 地址和端口。也就是“私有地址+端口”与“公有地址+端口”之间的转换。

设备通过创建并执行 NAT 规则来实现 NAT 功能。NAT 规则一般有两类，分别为源 NAT 规则（SNAT Rule）和目的 NAT 规则（DNAT Rule）。SNAT 转换源 IP 地址，从而隐藏内部 IP 地址或者分享有限的 IP 地址；DNAT 转换目的 IP 地址，通常是将受设备保护的内部服务器（如 WWW 服务器或者 SMTP 服务器）的 IP 地址转换成公网 IP 地址。

除此之外，系统也支持将内网地址和外网地址进行一对一的静态 NAT 转换。BNAT（Bidirectional NAT）规则可以看作是目的 NAT 和源 NAT 的结合，用一条 BNAT 规则实现源和目的的互换。

在数据处理流程上，BNAT 的匹配顺序先于 DNAT，当数据包匹配到 BNAT 规则时，将按照 BNAT 规则分别作 DNAT 和 SNAT 转换，接下来数据包开始匹配策略规则。

配置 NAT 规则

NAT 规则基于VRouter 创建并生效。用户可以在VRouter 配置模式下，创建 SNAT/DNAT 规则、修改 SNAT/DNAT 规则排列以及删除 SNAT/DNAT 规则等。为缺省 VR 即trust-vr 配置 NAT，也可以使用 NAT 模式（在全局配置模式下，使用 nat 命令进入 NAT 配置模式）。

进入VRouter 配置模式，在全局配置模式下使用以下命令：

ip vrouter *vrouter-name*

- *vrouter-name* – 指定 VRouter 的名称。

创建静态 NAT 一对一功能（BNAT）

BNAT（Bidirectional NAT）规则可以看作是目的 NAT 和源 NAT 的结合，用一条BNAT 规则实现源和目的的互换。

在数据处理流程上，BNAT 的匹配顺序先于 DNAT，当数据包匹配到 BNAT 规则时，将按照 BNAT 规则分别作 DNAT 和 SNAT 转换，接下来数据包开始匹配策略规则。

该功能操作方法如下：

在 VRouter 配置模式下，使用以下命令配置一对一 BNAT 功能。

bnatrule [**id** *id*] **interface** *interface-name* **virtual** {**ip** {*A.B.C.D/M* | *X:X:X:X:X::X/M*} | **address-book** *address-name* } **real** {**ip** {*A.B.C.D* | *A.B.C.D/M* | *X:X:X:X:X::X/M*} | **address-book** *address-name* }

- **id** *id* – 为 BNAT 规则指定 ID 号。每一条 BNAT 规则都有一个唯一的 ID。如果不指定，系统会自动分配。如果指定的 ID 为已有的 BNAT 规则的 ID，已有的规则会被覆盖。
- **virtual** {**ip** { *A.B.C.D/M* | *X:X:X:X:X::X/M*} | **address-book** *address-name* } – 指定供外网用户访问的外网地址。支持单个 IP 地址的一对一转换。如果是地址簿或地址段的转换，要求地址簿或地址段中的地址个数相同，映射关系按照从上向下的顺序对应。

  注意：输入 IP 地址时，必须同时指定子网掩码。不支持无子网掩码的 IP 地址。
- **real** {**ip** {*A.B.C.D/M* | *X:X:X:X:X::X/M*} | **address-book** *address-name* } -指定内网中的真实内网地址。改地址对外不可见，是服务器的真实内网地址。

  注意：输入 IP 地址时，必须同时指定子网掩码。不支持无子网掩码的 IP 地址。

使用该命令的 no 形式，删除 BNAT 规则。

no bnatrule id *id*

创建 SNAT 规则

SNAT 规则指定是否对符合条件的流量的源 IP 地址做 NAT 转换，如果需要转换，则同时指定转换的地址和方式。配置做 NAT 转换的 SNAT 规则，在VRouter 配置模式下使用以下命令：

snatrule [**id** *id*] [**ingress-interface** *interface-name*] [**before** *id* | **after** *id* | **top**] **from** *src-address* **to** *dst-address* [**service** *service-name*] [**eif** *egress-interface* | **evr** *vrouter-name*] **trans-to** {**addressbook** *trans-to-address* | **eif-ip**} **mode** {**static** | **dynamicip** | **dynamicport** [**sticky** | **round-robin**]} [**log**] [**group** *group-id*] [**disable**] [**track** *track-name*] [**description** *description*]

- **id** *id* – 为 SNAT 规则指定 ID 号。每一条 SNAT 规则都有一个唯一的 ID。如果不指定，系统会自动分配。如果指定的 ID 为已有的 SNAT 规则的 ID，已有的规则会被覆盖。
- **ingress-interface** *interface-name* – 指定匹配该 SNAT 规则的入接口。配置了入接口之后，只有从该接口进入的流量才会继续匹配这条 SNAT 规则，其他接口进入的流量不匹配。
- **before** *id* | **after** *id* | **top** – 指定规则所在的位置，可以是位于某个 ID 之前（before id）或者之后（after id），也可以是位于所有规则的首位（top）。如果不指定，该规则会处于所有 SNAT 规则的末尾。默认情况下，系统会将新创建的 SNAT 规则放到所有 SNAT 规则的末尾。
- **from** *src-address* **to** *dst-address* [**eif** *egress-interface* | **evr** *vrouter-name*] – 指定该规则中流量应符合的条件。条件包括：
  - **from** *src-address* - 指定流量的源 IP 地址，*src-address* 为 IP 地址（IPv4 或 IPv6）或者系统地址簿中指定的地址条目（IPv4 或 IPv6）。

- **to** *dst-address* - 指定流量的目的 IP 地址，*dst-address* 为 IP 地址（IPv4 或 IPv6）或者系统地址簿中指定的地址条目（IPv4 或 IPv6）。
- **service** *service-name* – 指定流量的服务类型。service-name 为服务簿中定义的服务。
- **eif** *egress-interface* | **evr** *vrouter-name* - 指定流量的出接口（**eif** *egress-interface*）或者流量的下一跳 VRouter（**evr** *vrouter-name*）。

- **addressbook** *trans-to-address* | **eif-ip** – 指定 NAT 转换地址。可以是 IP 地址或者系统地址簿中的地址，也可以是出接口的 IP 地址（eif-ip）。
- **mode** {**static** | **dynamicip** | **dynamicport** [**sticky** | **round-robin**]} – 指定转换模式。系统支持三种转换模式：static、dynamicip 和 dynamicport。具体描述请参阅下表：

模式	描述
static	静态源 NAT 转换即一对一的转换。该模式要求被转换到的地址条目（*trans-to-address*）包含的 IP 地址数与流量的源地址的地址条目（*src-address*）包含的 IP 地址数相同。
dynamicip	动态源 NAT 转换即多对多的转换。该模式将源地址转换到指定的 IP 地址。每一个源地址会被映射到一个唯一的 IP 地址做转换，直到指定地址全部被占用。
dynamicport	即 PAT。多个源地址将被转换成指定 IP 地址条目中的一个地址。 如果使用了 sticky，每一个源 IP 产生的所有会话将被映射到同一个固定的 IP 地址。 如果使用了 Round-robin，每一个源 IP 产生的会话将以轮询的方式进行 IP 地址映射。 如果不使用 sticky 和 Round-robin，地址条目中的第一个地址将会首先被使用，当第一个地址的端口资源被用尽，第二个地址将会被使用。 注意：Sticky 功能和 Round-robin 功能是互斥的，二者不能同时配置。

- **log** – 使用该参数开启该 SNAT 规则的日志功能（当有流量匹配该地址转换规则时产生日志信息）。
- **group** *group-id* - 指定 SNAT 规则所属的 HA 组。如不指定该参数，创建的 SNAT 规则属于 HA 组 0。
- **disable** – 如选择该选项，系统将禁用此 SNAT 规则。
- **track** *track-name* – 指定已创建的监测对象名称。配置该参数后，系统将对NAT 转换后的公网地址是否有效进行监测，即以其作为源地址来监测到目标网站或主机的访问是否正常。可配置的监测对象包括 Ping 报文监测对象、HTTP 报文监测对象、TCP 报文监测对象。。该功能仅支持动态端口模式（dynamicport），且 NAT 转换后的地址必须为 IP 地址或者地址簿中的地址（即 trans-to addressbook trans-to-address）。系统优先使用监测成功的转换地址，当某个转换地址对目标网站或主机监测失败时，该地址被临时禁用，直至再次监测成功。当监测对象失败时，系统将在下个监测周期内禁用此地址并生成日志信息，不再转换私网地址为该公网地址，直到该地址被判定为可达。若 SNAT 规则的公网地址簿中地址全部被判定为不可达，系统将不禁用任何转换地址并发出日志信息。

- **description** *description* – 指定 SNAT 规则的描述信息。范围是 1 到 63 个字符。

例如，以下命令示例实现了 untrust 域中以太接口ethernet0/0 的基于接口的NAT 转换：

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# snatrule from any to any eif ethernet0/0 trans-to eif-ip mode dynamicport
rule id=1
```

配置不做 NAT 转换的 SNAT 规则，在 NAT 配置模式下使用以下命令：

snatrule [**id** *id*] [**before** *id* | **after** *id* | **top**] **from** *src-address* **to** *dst-address* [**eif** *egress-interface* | **evr** *vrouter-name*] **no-trans** [**group** *group-id*] [**description** *description*]

启用/禁用 SNAT 规则

在 CLI 的 NAT 配置模式下，用户可以通过使用以下命令启用或者禁用 SNAT 规则：

snatrule id *id* [**enable** | **disable**]

- **enable** – 启用指定 ID 的 SNAT 规则。
- **disable** – 禁用指定 ID 的 SNAT 规则。

修改 SNAT 规则排列顺序

每一条 SNAT 都有唯一一个 ID 号。流量进入设备时， 设备对 SNAT 规则进行顺序查找，然后按照查找到的相匹配的第一条规则对流量的源 IP 做 NAT 转换。但是，ID 的大小顺序并不是规则匹配顺序。使用 **show snat** 命令列出的规则顺序才是规则匹配顺序。用户可以移动已有的 SNAT 规则从而改变规则的排列顺序。改变规则的排列顺序，在 VRouter 配置模式下使用以下命令：

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

- *id* – 指定被移动的SNAT 规则的 ID 号。
- **before** *id* – 将 SNAT 规则移动到某个 ID 之前。
- **after** *id* – 将 SNAT 规则移动到某个 ID 之后。
- **top** – 将 SNAT 规则移动到所有 SNAT 规则之首。
- **bottom** – 将 SNAT 规则移动到所有 SNAT 规则的末尾。

开启/关闭扩展 PAT 端口池功能

当 SNAT 的转换模式为 dynamicport 时，用户可以开启扩展PAT 端口池功能，扩展 NAT 转换后的网络地址端口资源。默认情况下，该功能是关闭的。开启扩展PAT 端口池功能，在全局模式下使用以下命令：

expanded-port-pool

在全局模式下，使用该命令 no 的形式关闭扩展 PAT 端口池功能：

no expanded-port-pool

注意:

- 设备的部分平台支持扩展PAT 端口池功能，并且不同平台支持的扩展端口资源倍数不同。
- 该功能在配置SNAT 规则前开启有效；如果在开启该功能前，系统中已配置 SNAT 规则，请重启设备使其生效。

删除 SNAT 规则

在 CLI 的 NAT 配置模式下，用户可以通过使用以下命令删除指定 ID 号的 SNAT 规则：

no snatrule id *id*

修改/删除 SNAT 描述信息

在 CLI 的 NAT 配置模式下，用户可以通过使用以下命令修改指定 ID 号的 SNAT 描述信息。

snatrule id *id* description *description*

- *id* – 指定要修改描述信息的 SNAT 规则 ID 号。
- description *description* – 指定 SNAT 规则的描述信息。范围是 1 到 63 个字符。

在 CLI 的 NAT 配置模式下，使用以下命令删除修改指定 ID 号的 SNAT 描述信息。

no snatrule id *id* description

显示 SNAT 配置信息

SNAT 配置完毕，用户可以在任何 CLI 模式下通过使用以下命令查看系统中 SNAT 的配置信息：

show snat [id *id* | vrouter *vrouter-name*]

- id *id* – 显示指定 ID 号的 SNAT 规则信息。
- vrouter *vrouter-name* – 显示指定 VRouter 的 SNAT 配置信息。如果不指定该参数，系统将显示缺省 VRouter（trust-vr）的 SNAT 规则。

显示 SNAT 的资源利用情况

当 SNAT 的转换模式为 dynamicport 时，显示转换地址池端口资源的利用情况，在任何 CLI 模式下，使用以下命令：。

show snat id *id* resource [ip *A.B.C.D*] [detail]

show snatresource [**vrouter** *vrouter-name*][**ip** *A.B.C.D*] [**detail**]

- **resource** – 当 SNAT 的转换模式为 dynamicport 时，该参数用来指定显示转换地址池端口资源的利用情况。
  - **ip** – 显示转换地址池中指定 IP 端口资源的利用情况。
  - **detail** -显示转换地址池中端口资源利用情况的详细信息，如分配状态、转换模式和端口范围等。
- **vrouter** *vrouter-name* – 显示指定 VRouter 的 SNAT 配置信息。如果不指定该参数，系统将显示缺省 VRouter（trust-vr）的 SNAT 规则。

查看监测失败的 SNAT 转换地址

查看监测失败的 SNAT 转换地址，在任何 CLI 模式下，使用以下命令：

show snat track-failed {**slot** *slot-number* | **cpu** *cpu-numb*} [**vrouter** *vrouter-name*][**ip** *A.B.C.D*] [**detail**]

show snat track-failed [**vrouter** *vrouter-name*]

- **track-failed** – 显示监测失败的 SNAT 转换地址。
- **slot** *slot-number* – 显示指定插槽的监测失败的 SNAT 转换地址。
  - **ip** – 显示指定插槽的指定 IP 的监测失败的SNAT 转换地址。
  - **detail** - 显示指定插槽的监测失败的的详细信息，如分配状态、转换模式和端口范围等。
- **vrouter** *vrouter-name* – 显示指定 VRouter 的监测失败的 SNAT 转换地址。如果不指定该参数，系统将显示缺省VRouter（trust-vr）的监测失败的 SNAT 转换地址。
- **cpu** *cpu-number* – 显示指定 CPU 的监测失败的SNAT 转换地址。

创建 DNAT 规则

DNAT 规则指定是否对符合条件的流量的目的 IP 地址做 NAT 转换。配置做NAT 转换的 DNAT 规则，在 VRouter 配置模式下使用以下命令：

dnatrule [**id** *id*] [**before** *id* | **after** *id* | **top**] [**ingress-interface** *interface*] **from** *src-address* **to** *dst-address* [**service** *service-name*] **trans-to** *trans-to-address* [**redirect**] [**port** *port*] [**load-balance**] [**track-tcp** *port*] [**track-ping**] [**log**] [**group** *group-id*] [**disable**] [**description** *description*]

- **id** *id* – 为 DNAT 规则指定 ID 号。每一条 DNAT 规则都有一个唯一的 ID。如果用户不指定，系统会为规则自动生成一个 ID。如果指定的 ID 为已有的 DNAT 规则的 ID，已有的规则会被覆盖。
- **before** *id* | **after** *id* | **top** – 指定规则所在的位置，可以是位于某个 ID 之前（**before** *id*）或者之后（**after** *id*），也可以是位于所有规则的首位（top）。如果不指定，该规则会处于所有 DNAT 规则

的末尾。默认情况下，系统会将新创建的DNAT 规则放到所有 DNAT 规则的末尾。流量进入 设备时， 设备对 DNAT 规则进行查找，然后按照查找到的相匹配的第一条规则对流量的目的 IP 做 NAT 转换。

- **ingress-interface** *interface* – 指定匹配该 dnat 规则的入接口。配置了入接口之后，只有从该接口进入的流量才会继续匹配这条 DNAT 规则，其他接口进入的流量不匹配。

- **from** *src-address* **to** *dst-address* [**service** *service-name*] – 指定该规则中流量应符合的条件。条件包括:

    - **from** *src-address* – 指定流量的源 IP 地址/掩码。*src-address* 为 IP 地址/掩码或者系统地址簿中指定的地址条目。可以为 IPv6 地址或 IPv6 地址条目。

    - **to** *dst-address* – 指定流量的目的 IP 地址/掩码。*dst-address* 为 IP 地址/掩码或者系统地址簿中指定的地址条目。可以为 IPv6 地址或 IPv6 地址条目。

    - **service** *service-name* – 指定流量的服务类型。如果需要一并转换端口号（通过 port port 参数指定），这里指定的服务就只能拥有一个协议和一个端口，例如 TCP 端口号可以是 80，但不可以是 80 到 100。

- **trans-to** *trans-to-address* – 指定 NAT 转换地址。*trans-to-address* 为 IP 地址/掩码或者系统地址簿中定义的地址条目。此处指定的 NAT 转换地址个数如果与流量目的 IP 地址（由命令的 **to** *dst-address* 参数指定）的个数不相同或者流量目的 IP 地址指定为 any 时，则需要为该条 DNAT 规则开启重定向功能（**redirect**）。如果为该条 DNAT 规则开启负载均衡功能（**load-balance**），也可以允许 NAT 转换地址个数与流量目的 IP 地址的个数不同，但是不允许流量目的 IP 地址为 **any**。如果此处指定的 NAT 转换地址为包含 DNS 域名的地址簿条目，则需要为该条DNAT 规则开启负载均衡功能（load-balance）。

- **redirect** - 配置 **redirect** 参数为该条 DNAT 规则开启重定向功能，允许指定流量目的 IP 地址为 **any**。

- **port** *port* – 内网服务器的端口号。

- **load-balance** – 配置 **load-balance** 参数为该条DNAT 规则开启负载均衡功能，采用持续性算法分发流量，基于用户 IP 地址的散列值来选择服务器，均衡流量到不同的内网服务器。

- **track-tcp** *port* – 配置 **track-tcp** 参数并指定内网服务器端口号，系统会每隔 3 秒向内网服务器发送 TCP 报文，监控服务器的特定 TCP 端口是否可达。若连续三次发送报文均未收到响应，系统认为内网服务器出现故障。

- **track-ping** –配置 **track-ping** 参数，系统会每隔 3 秒向内网服务器发送Ping 报文，监控服务器是否可达。若连续三次发送报文均未收到响应，系统认为内网服务器出现故障。

- **log** – 使用该参数开启该 DNAT 规则的日志功能（当有流量匹配该地址转换规则时产生日志信息）。

- [**group** *group-id*] - 指定 DNAT 规则所属的 HA 组。如不指定该参数，创建的DNAT 规则属于 HA 组 0。

- **disable** – 如选择该选项，系统将禁用此 DNAT 规则。
- **description** *description* – 指定 DNAT 规则的描述信息。范围是 1 到 63 个字符。

例如，以下命令将任何到 addr1 的请求的 IP 转换成 addr2 的 IP 地址，并且不转换服务的端口号：

```
hostname(config-vrouter)# dnatrule from any to addr1 service any trans-to addr2
rule id=1
```

配置不做 NAT 转换的 DNAT 规则，在 NAT 配置模式下使用以下命令：

dnatrule [**id** *id*] [**before** *id* | **after** *id* | **top**] **from** *src-address* **to** *dst-address* [**service** *service-name*] **no-trans** [**group** *group-id*] [**description** *description*]

启用/禁用 DNAT 规则

在 CLI 的 NAT 配置模式下，用户可以通过使用以下命令启用或者禁用 DNAT 规则：

dnatrule id *id* [**enable** | **disable**]

- **enable** – 启用指定 ID 的 DNAT 规则。
- **disable** – 禁用指定 ID 的 DNAT 规则。

修改 DNAT 规则排列顺序

每一条 DNAT 都有唯一一个 ID 号。每一条 DNAT 都有唯一一个 ID 号。流量进入设备时， 设备对 DNAT 规则进行顺序查找，然后按照查找到的相匹配的第一条规则对流量的目的 IP 做 NAT 转换。但是，ID 的大小顺序并不是规则匹配顺序。使用 show dnat 命令列出的规则顺序才是规则匹配顺序。用户可以移动已有的 DNAT 规则从而改变规则的排列顺序。修改 DNAT 规则排列顺序，请在 NAT 配置模式下使用以下命令：

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

- *id* – 指定被移动的DNAT 规则的 ID 号。
- **before** *id* – 将 DNAT 规则移动到某个 ID 之前。
- **after** *id* – 将 DNAT 规则移动到某个 ID 之后。
- **top** – 将 DNAT 规则移动到所有 SNAT 规则之首。
- **bottom** – 将 DNAT 规则移动到所有 SNAT 规则的末尾。

修改/删除 DNAT 描述信息

在 CLI 的 NAT 配置模式下，用户可以通过使用以下命令修改指定 ID 号的 DNAT 描述信息。

dnatrule id *id* **description** *description*

- *id* – 指定需修改描述信息的 DNAT 规则 ID 号。
- **description** *description* – 指定 DNAT 规则的描述信息。范围是 1 到 63 个字符。

在 CLI 的 NAT 配置模式下，使用以下命令删除修改指定 ID 号的 DNAT 描述信息。

no dnatrule id *id* **description**

删除 DNAT 规则

在 CLI 的 NAT 配置模式下，用户可以通过使用以下命令删除指定 ID 号的 DNAT 规则：

no dnatrule id *id*

显示 DNAT 配置信息

DNAT 配置完毕，用户可以在任何 CLI 模式下通过使用以下命令查看系统中 DNAT 的配置信息：

show dnat [**id** *id* | **vrouter** *vrouter-name*]

- **id** *id* – 显示指定 ID 号的 DNAT 规则信息。
- **vrouter** *vrouter-name* – 显示指定 VRouter 的 DNAT 规则信息。如果不指定该参数，系统将显示缺省 VRouter（trust-vr）的 DNAT 规则。

显示配置有负载均衡功能的 DNAT 规则相关信息，在任何模式下，使用以下命令：

show load-balance rule [*id*]

- *id* – 显示指定 ID 号的配置有负载均衡功能的 DNAT 规则信息。

显示负载均衡服务器状态，请在任何模式下，使用以下命令：

show load-balance server [*ip-address*] [**vrouter** *vrouter-name*]

- *ip-address* – 显示指定 IP 地址的负载均衡服务器状态信息。
- **vrouter** *vrouter-name* – 显示指定 Vter 的负载均衡服务器状态信息。如果不指定该参数，系统将显示缺省 VR 即 trust-vr 的负载均衡服务器状态信息。

显示内网服务器状态，请在任何模式下，使用以下命令：

show dnat server [*ip-address*] [**vrouter** *vrouter-name*] [**tcp-port** *port*] [**ping**]

- *ip-address* – 显示指定 IP 地址的内网服务器状态信息。

- **vrouter** *vrouter-name* – 显示指定 VRouter 的内网服务器状态信息。如果不指定该参数，系统将显示缺省 VR 即 trust-vr 的内网服务器状态信息。
- **tcp-port** *port* – 显示指定端口号的内网服务器状态信息。
- **ping** – 显示内网服务器的Ping 监控状态信息。

配置排除端口规则

用户可以通过配置排除端口规则，将个别端口或者端口范围排除，在进行源地址转换的时候，将不会对指定的端口转换。

实现系统的 SNAT 排除端口功能，用户需要按照以下步骤进行操作:

1. 创建 SNAT 端口组。
2. 配置 SNAT 端口组，在端口组中指定描述信息、排除的端口号。
3. 绑定 SNAT 端口组到指定的 VRouter，使其生效。

创建 SNAT 端口组

创建 SNAT 端口组，在全局配置模式下，使用以下命令:

snat-port-group *snat-port-group-name*

- *snat-port-group-name* - 指定 SNAT 端口组名称。范围为 1 到 95 个字符。并且进入 SNAT 端口组配置模式。如果指定名称已存在，则直接进入 SNAT 端口组模式。

注意:系统支持创建最多 8 个 SNAT 端口组。

删除一个 SNAT 端口组，请在全局配置模式下，输入以下命令:

no snat-port-group *snat-port-group-name*

指定 SNAT 端口组描述信息

指定 SNAT 端口组描述信息，在 SNAT 端口组配置模式下，使用以下命令:

description *description*

- *description* – 指定 SNAT 端口组的描述信息。范围是 0 到 256 字节。

在 SNAT 端口组配置模式下，使用以下命令删除 SNAT 端口组描述信息。

no description

指定排除端口号

指定需要排除的端口范围，在 SNAT 端口组配置模式下，使用以下命令：

port {**TCP** | **UDP**} **min-port** *min-port* [**max-port** *max-port*]

- **TCP** | **UDP** – 指定排除端口的协议类型。
- **min-port** *min-port* [**max-port** *max-port*]- 指定排除的端口号。如果端口号为一个范围，*min-port* 为最小目的端口号，*max-port* 为最大目的端口号。

在 SNAT 端口组配置模式下，使用以下命令取消对排除端口号的指定。

no port {**TCP** | **UDP**} **min-port** *min-port* [**max-port** *max-port*]

绑定 SNAT 端口组到 VRouter

绑定 SNAT 端口组到指定的VRouter 后，该 VRouter 下所有动态端口的 SNAT 规则都会排除 SNAT 端口组中指定的端口号。在指定VRouter 配置模式下，使用以下命令：

snat-exclude-port *snat-port-group-name*

在 VRouter 配置模式下，使用该命令 no 的形式取消 SNAT 端口组的绑定：

no snat-exclude-port

显示 SNAT 端口组配置信息

用户可以在任何 CLI 模式下通过使用以下命令查看 SNAT 端口组的配置信息：

show snat-port-group [*snat-port-group-name*]

- *snat-port-group-name* – 显示指定名称的SNAT 端口组配置信息。

查看 SNAT 端口组关联项

用户可以在任何 CLI 模式下通过使用以下命令查看 SNAT 端口组的关联项：

show reference snat-port-group [*snat-port-group-name*]

- *snat-port-group-name* – 显示指定名称的SNAT 端口组关联项。

DNS Rewrite

当客户端发起DNS 请求，位于公网的 DNS 服务器返回DNS response 报文时，安全设备将对报文中的 IP 地址进行重写，将其改为私网 IP 地址以保护和隐藏组网环境中的网络配置。配置该功能，在 NAT 配置模式下，输入以下命令：

dns-rewrite-rule [**id** *id*] **dns-response** {**ip** *ip-address* | **address-book** *address-name*} **rewrite-to** {**ip** *ip-address* | **address-book** *address-name*} [**group** *group-id*] **dynamic-mapping**

- **id** *id* – 指定该规则的 ID。每一条规则都有一个唯一的 ID。如果不指定，系统会自动分配。如果指定的 ID 为已有的规则的 ID，已有的规则会被覆盖。
- **dns-response** {**ip** *ip-address* | **address-book** *address-name*} - 指定 DNS response 报文中的公网 IP 地址或地址簿名称。
- **rewrite-to** {**ip** *ip-address*| **address-book** *address-name*} – 指定设备重写后的私网 IP 地址或地址簿名称。
- **group** *group-id* – 指定该规则所属的 HA 组的组 ID。

在任何模式下，使用 **show dns-rewrite-rule** [**id** *id* | **vrouter** *vr-name*] **dynamic-mapping** 查看 DNS rewrite 规则：

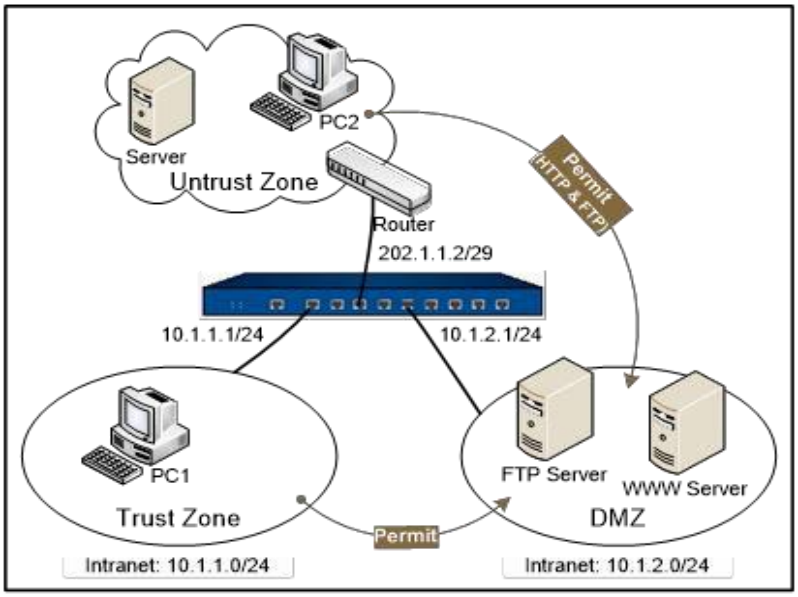
- **id** *id* | **vrouter** *vr-name* – 查看指定 ID 或 VRouter 下的 DNS rewrite 规则。

NAT 配置举例

本节列举一个 NAT 的典型配置示例。

组网需求

公司通过设备将网络划分为三个域：Trust 域、DMZ 域和 Untrust 域。员工工作网段处于 Trust 域，分配私网地址 10.1.1.0/24，并且具有最高安全级别；WWW 服务器和FTP 服务器处于 DMZ 域，分配私网地址 10.1.2.0 /24，并且能够被内部员工和外部用户访问；外部网络处于 Untrust 域。该示例的组网图如下：



现有以下三个需求：

- 需求 1：要求公司 Trust 域的 10.1.1.0/24 网段用户可以访问 Internet，而该域其它网段的 PC 机不能访问 Internet。提供的访问外部网络的合法 IP 地址范围从 202.1.1.3 到 202.1.1.5。由于公网地址不多，需要使用 NAT 功能进行地址复用。
- 需求 2：提供两个内部服务器供外部网络用户访问，其中，FTP 服务器的内部 IP 地址为 10.1.2.2，端口为 21，WWW 服务器的内部 IP 地址为 10.1.2.3，端口为 80；对外映射的 IP 地址为 202.1.1.6。
- 需求 3：Trust 域的任意 PC 访问 Untrust 域中设备后，Untrust 域中的所有用户可以利用Full-cone NAT 功能反向连接到 Trust 域中的该台PC。

配置步骤

第一步：将设备各接口分配安全域并配置 IP 地址。

```
hostname# configure
hostname(config)# address addr1
hostname(config-addr)# ip 10.1.1.1/24
hostname(config-addr)# exit
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# zone untrust
hostname(config-if-eth0/2)# ip address 202.1.1.2/29
hostname(config-if-eth0/2)# exit
hostname(config)# interface ethernet0/3
hostname(config-if-eth0/3)# zone dmz
hostname(config-if-eth0/3)# ip address 10.1.2.1/24
hostname(config-if-eth0/3)# exit
hostname(config)#
```

第二步：配置地址条目。

```
hostname(config)# address addr2
hostname(config-addr)# range 202.1.1.3 202.1.1.5
hostname(config-addr)# exit
hostname(config)# address test1
hostname(config-addr)# ip 202.1.1.6/32
hostname(config-addr)# exit
hostname(config)# address test2
hostname(config-addr)# ip 10.1.2.2/32
hostname(config-addr)# exit
hostname(config)# address test3
hostname(config-addr)# ip 10.1.2.3/32
hostname(config-addr)# exit
```

第三步：配置安全策略规则。

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# src-addr addr1
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-policy)# rule
hostname(config-policy-rule)# src-zone trust
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-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 http
hostname(config-policy-rule)# service ftp
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config)#
```

第四步：配置 NAT 规则。

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# snatrule id 1 from addr1 to any eif ehternet0/2 trans-to address-book addr2 mode dynamicport sticky
rule id=1
hostname(config-vrouter)# dnatrule id 2 from any to test1 service ftp trans-to test2 port 21
rule id=2
hostname(config-vrouter)# dnatrule id 3 from any to test1 service http trans-to test3 port 80
rule id=3
hostname(config-vrouter)# exit
hostname(config)# nat type full-cone
hostname(config)# nat protocol tcp
```

应用层识别与控制

应用层识别与控制介绍

设备提供广泛的应用层监控、统计和控制过滤功能。该功能能够对 FTP、HTTP、P2P 应用、实时通信工具以及 VoIP 语音数据等应用进行识别，并根据安全策略配置规则，保证应用的正常通信或对其进行指定的操作，如监控、流量统计、流量控制和阻断等。系统利用分片重组及传输层代理技术，使设备能够适应复杂的网络环境，即使在完整的应用层数据被分片且传送分片出现乱序的情况下，也能够有效地重组报文识别应用，从而保证安全策略的有效实施。

分片重组

通常的网络中间设备，如路由器或者交换机，并不重组它们收到的分片报文。目的主机在收到所有分片报文后进行重组。由于网络环境的复杂性，分片报文可能出现丢失、乱序的情况，而对分片的重组需要接收所有的分片，并进行排序方能完成，这会耗费一定的系统资源。网络设备从职能及转发效率角度考虑，一般不做重组，只负责转发。但作为设备，安全策略的应用要求对应用层信息进行分析，以过滤存在安全 隐患的恶意信息或阻断任何入侵及攻击企图。但是设备只有在接收到应用层完整信息的情况下才能作出 裁决。系统具备传输层代理功能，能够先对分片报文进行缓存、排序和重组，并且在完成分析并作出裁决的情况下，对正常数据进行重新封装和转发。

应用层网关（ALG）

一些应用程序采用多通道数据传送，常见的如 FTP，其控制通道和数据通道是分开的。在严格安全策略控制条件下的设备，对每种数据通道进行严格限制，例如只允许从内网到外网的 FTP 数据在知名的 TCP 21 号端口上进行传输，一旦FTP 主动模式下，在公网上的FTP 服务器试图主动连接内网主机的随机端口，设备就会进行拦截，此时FTP 无法正常工作。这就要求设备足够智能以正确处理严格安全策略下合法应用的随机性。在 FTP 的实例中， 设备通过分析FTP 控制通道上传送的信息，得知服务器与客户端达成一致，服务器将主动连接客户端的某端口， 设备就能临时的打开一条通道，使FTP 正常工作。

系统采用最严格的 NAT 模式。一些VoIP 应用在进行 NAT 穿越时，由于 IP 地址和端口号的改变可能导致 VoIP 无法正常工作，ALG 技术在此时将保证 NAT 地址转换后，VoIP 应用能够正常通信。因此，应用层网关提供以下功能：

- 在严格的安全策略规则下，利用应用层网关ALG 技术，保证多通道应用程序正常的通信，如 FTP、TFTP、PPTP、RTSP、RSH、MSRPC、SUNRPC 和 SQLNET。
- 保证VoIP 应用，如 SIP 和 H.323 等，在 NAT 模式下的正常工作，并能够根据安全策略要求，进行监控和过滤。

HTTP、P2P 和 IM

在传输层代理及分片重组的支持下，系统支持三大类应用的识别与控制，分别是 HTTP 应用、P2P 应用和 IM 应用。通过Profile 定义，可以针对每种应用实施各种操作，如流量监控、流量限制和阻断等，例如：

- 对 HTTP Java Applet 程序的过滤。保证受保护的用户不受有害 Java Applet 程序的侵害。
- 对 HTTP ActiveX 程序的过滤。防止恶意ActiveX 程序破坏用户系统。
- P2P 应用的识别、监控和流量控制乃至阻断。支持 BT、eMule、以及 Thunder（迅雷）等。
- 针对实时通信工具的各种操作，如聊天和文件传输等进行识别与控制，如 MSN Messenger、QQ 和 Yahoo Messenger 等。

配置 ALG 功能

系统可根据每种应用分别开启或关闭 ALG 控制功能。用户可在设备上配置以下应用的ALG 控制功能：FTP、HTTP、MSRPC、PPTP、Q.931、RAS、RSH、RTSP、SIP、SQLNetV2、SUNRPC、TFTP、DNS、H323 和 XDMCP。用户可以开启或者关闭应用的 ALG 功能，也可以指定 H323 协议的超时时间。

开启或者关闭应用的 ALG 控制功能，在全局配置模式下使用以下命令：

开启：**alg {all | auto | TFTP | FTP | RSH |…}**

关闭：**no alg {all | auto | TFTP | FTP | RSH | …}**

- **all** – 开启或者关闭所有应用的ALG 控制功能。
- **auto** – 根据应用识别的结果自动开启或关闭应用的ALG 控制功能。
- **TFTP | FTP | RSH | …** - 开启或者关闭指定应用的ALG 控制功能。

注意:如果关闭HTTP 的 ALG 功能，设备的 HTTP 内容阻断功能将失效。

ALG 支持严格模式和非严格模式。严格模式创建的PINHOLE 中所分配的 SNAT 端口和控制连接分配的 SNAT 端口一致。系统默认开启严格模式。开启ALG 严格模式，在全局配置模式下，使用以下命令：

alg strict-mode

使用 **no alg strict-mode** 命令开启非严格模式。在如下场景中，建议用户开启非严格模式，避免影响数据流量：

- 存在第三方PINHOLE
- 配置了 SNAT 并开启了端口扩展
- 协商数据连接的PAYLOAD 中的 IP 地址和端口号与控制连接的 IP 地址和端口号一致

指定 H323 协议的超时时间，在全局配置模式下使用以下命令：

alg h323 session-time *time-value*

- *time-value* - 指定 H323 的超时时间。默认为 60 秒。范围是 60 到 1800 秒。

使用以上命令 no 的形式取消对 H323 超时时间的指定：

no alg h323 sesstion-time

开启或者关闭对每秒处理 SIP 消息数目的限制功能，在全局配置模式下使用以下命令：

开启：**alg sip-message-rate** *number*

- *number* - 指定每秒处理 SIP 消息数目的最大值。取值范围是 1 到 65535。

关闭：**no alg sip-message-rate**

用户可以在任意模式下使用 **show** 命令查看ALG 控制功能的状态和配置：

- 查看是否对应用启用了ALG 控制功能：**show alg**
- 查看 SIP 网关的 ALG 配置和状态：**show alg sip-capacity**

指定 SIP 代理模式

SIP 是一个应用层的控制协议，它通常用于多媒体会话，例如 Internet 电话。SIP 协议可以承载多种多媒体会话数据，比如声音、影像、或者文本。

SIP 服务器可以作为代理转发 SIP 客户端之间的通信。SIP 客户端之间通信有两种模式，一种是媒体数据经过 SIP 服务器进行代理，另一种是媒体数据是不经过 SIP 服务器，SIP 客户端之间直接通信。防火墙应该配合 SIP 客户端的通信模式，选择与实际情况相同的模式，如果不一致可能会导致通信问题。

在全局配置模式下，使用以下命令使防火墙工作在客户端不经过 SIP 代理服务器而直接通信的模式下。防火墙默认使用这种模式，它能保证不通过代理服务器的 SIP 客户端的通信正常。

no alg sip media-proxied-by-server

在全局配置模式下，使用以下命令使防火墙工作在 SIP 服务器做代理的通信模式下。

alg sip media-proxied-by-server

查看 ALG SIP 信息

查看防火墙是否开启了 SIP 代理模式、每秒处理 SIP 消息数目的最大值、注册话机数量和正在进行通话的话机数量，SIP 的在任意模式下，使用以下命令：

show alg sip

ALG 配置举例

本节介绍两个应用层识别与控制的具体实例。分别是

- 实例 1：严格限制内网客户只能在知名端口上访问外部网上的 TFTP、FTP 和 RTSP 服务，同时保证这些应用在多通道上的正常通信。
- 实例 2：阻断来自外部的ActiveX 控件及 Java-applet 程序。

实例 1 配置步骤

第一步：在安全策略中严格限制服务类型。

```
地址条目 “internal” 包含内网客户的所有 IP 地址
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# src-addr internal
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service tftp
hostname(config-policy-rule)# service ftp
hostname(config-policy-rule)# service rtsp
hostname(config-policy-rule)# application tftp
hostname(config-policy-rule)# application ftp
hostname(config-policy-rule)# application rtsp
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

第二步：确保打开这些应用的ALG 开关。

```
hostname(config)# alg tftp
```

```
hostname(config)# alg ftp
hostname(config)# alg rtsp
```

实例 2 配置步骤

第一步：确保打开 HTTP 应用的 ALG 开关。

```
hostname(config)# alg http
```

第二步：配置 Profile 来定义对 Java-applet 和ActiveX 的控制。

```
hostname(config)# behavior-profile test
hostname(config-bhv-profile)# object active-x deny
hostname(config-bhv-profile)# object java-applet deny
hostname(config-bhv-profile)# exit
hostname(config)#
```

第三步：将 Profile 绑定到安全策略中。

```
地址条目 “internal” 包含内网客户的所有 IP 地址
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# src-addr internal
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service http
hostname(config-policy-rule)# application http
hostname(config-policy-rule)# behavior test
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
```

```
hostname(config)#
```

第 2 章 安全策略

安全策略

安全策略介绍

策略是网络安全设备的基本功能，控制安全域间/不同地址段间的流量转发。默认情况下，安全设备会拒绝设备上所有安全域/地址段@之间的信息传输。而策略则通过策略规则（Policy Rule）决定从一个（多个）安全域到另一个（多个）安全域/从一个地址段到另一个地址段的哪些流量该被允许，哪些流量该被拒绝。

策略规则的基本元素

策略规则允许或者拒绝从一个（多个）安全域到另一个（多个）安全域/从一个地址段到另一个地址段的流量。流量的类型、流量的源安全域/源地址与目的安全域/目的地址以及行为构成策略规则的基本元素。

- Source Zone/Address - 流量的源安全域/源地址。
- Destination Zone/Address – 流量的目的安全域/目的地址。
- Service – 流量的服务类型。
- Action – 安全设备在遇到指定类型流量时所做的行为，包括允许（Permit）、拒绝（Deny）、隧道（Tunnel）、是否来自隧道（Fromtunnel）以及 Web 认证五个行为。

以下的 CLI 通过配置策略规则，允许从任意域的任意地址到任意域的任意地址 ICMP 服务流量通过设备。

```
hostname(config)# policy-global
hostname(config-policy)# rule from any to any service icmp permit
```

- Source Address – Any，即任意地址。它是地址簿中的一个默认地址条目。
- Destination Address – Any，即任意地址。它是地址簿中的默认地址条目。
- Service – ICMP。
- Action – 允许（Permit），即安全设备允许这种流量穿过 设备。

定义策略规则

一般来讲，策略规则分为两部分：过滤条件和行为。安全域间流量的源安全域/源地址、目的安全域/目的地址、服务类型以及角色构成策略规则的过滤条件。策略规则都有其独有的 ID 号。策略规则 ID 会在定义规则时自动生成，同时用户也可以按自己的需求为策略规则指定 ID。整个系统的所有策略规则有特定的排列顺序。在流量进入系统时，系统会对流量按照找到的第一条与过滤条件相匹配的策略规则进行处 理。

不同设备平台支持的全局最大策略规则数不同。

Profile 介绍

通过安全策略与 Profile 相结合，能够使设备完成细粒度的应用层安全策略控制。Profile 针对不同的应用定义不同的操作，将复杂控制信息简单化，从而简化 设备配置。StoneOS 支持 9 类 Profile，分别是 URL 过 滤 Profile、内容过滤 Profile、Web 外发信息 Profile、邮件过滤 Profile、IM Profile、行为 Profile、病毒过滤 Profile、IPS Profile 和 GTP Profile。每一类 Profile 可以针对具体应用分别配置不同的控制动作。

QoS 标签

设备的策略规则支持 QoS 标签功能。用户可以为策略中允许通过的流量添加QoS 标签。

> {b}提示: {/b}关于 QoS 配置，请参阅《流量管理》。

配置策略规则

用户可以通过配置策略规则，对进入设备的流量进行控制。策略规则配置包括:

- 创建策略规则
- 编辑策略规则
- 指定缺省行为
- 修改规则排列顺序

进入策略配置模式

进入策略配置模式，在全局配置模式下使用以下命令:

policy-global

创建策略规则

在全局配置模式或者策略配置模式下，执行以下命令创建策略规则:

rule [id *id*] [name *name*] [top | before {name *rule-name*| *id*} | after {name *rule-name*| *id*}] [role {UNKNOWN | *role-name*} | user *aaa-server-name user-name* | user-group *aaa-server-name user-group-name*] [from {host *host-name* | range *min-ip max-ip* | *src-addr*}] [to {host *host-name* | range *min-ip max-ip* | *dst-addr*}] [from-zone *zone-name* to-zone *zone-name*] [service *service-name*] [application *app-name*] [permit | deny | tunnel *tunnel-name* | fromtunnel *tunnel-name* | webauth | portal-server *server-name*]

- id *id* – 指定策略规则的 ID。如果不指定，系统将会为策略规则自动分配一个 ID。规则 ID 在整个系统中必须是唯一的。
- name *name* – 指定策略规则的名称。
- top | before {name *rule-name*| *id*} | after {name *rule-name*| *id* – 指定策略规则的位置。默认情况下，系统会将新创建的策略规则放到所有规则的末尾。
  - top - 指定策略规则的位置为所有规则的首位。
  - before {name *rule-name*| *id*} – 指定策略规则的位置为某个规则 ID 或者名称之前。
  - after {name *rule-name*| *id* – 指定策略规则的位置为某个规则 ID 或者名称之后。
- role {UNKNOWN | *role-name*} | user *aaa-server-name user-name* | user-group *aaa-server-name user-group-name* – 指定策略规则的角色/用户/用户组。
  - role {UNKNOWN | *role-name*} – 指定角色名称，其中 UNKNOWN 是系统预留的角色，是既没有经过系统认证也没有静态绑定的角色。
  - user *aaa-server-name user-name* – 指定用户。*aaa-server-name* 为用户所属的AAA 服务器名称，*user-name* 为用户名称。
  - user-group *aaa-server-name user-group-name* – 指定用户组。*aaa-server-name* 为用户组所属的 AAA 服务器名称，*user-group-name* 为用户组名称。
- from {host *host-name* | range *min-ip max-ip* | *src-addr*} – 指定策略规则的源地址。
  - host *host-name* - 为地址簿中定义的主机类型的源地址条目。
  - range *min-ip max-ip* – 为地址簿中定义的 IP 地址段类型的源地址条目。
  - *src-addr* – 为地址簿中定义的地址条目。
- to {host *host-name* | range *min-ip max-ip* | *dst-addr*} – 指定策略规则的目的地址。
  - host *host-name* – 为地址簿中定义的主机类型的目的地址条目。
  - range *min-ip max-ip* – 为地址簿中定义的 IP 地址段类型的目的地址条目。
  - *dst-addr* - 为地址簿中定义的地址条目。
- from-zone *zone-name* – 指定策略规则的源安全域。

- **to-zone** *zone-name* – 指定策略规则的目的安全域。
- **service** *service-name* – 指定策略规则的服务名称。*service-name* 为服务簿中定义的服务。
- **application** *app-name* – 指定策略规则的应用名称。*app-name* 为应用簿中定义的应用。
- **permit** | **deny** | **tunnel** *tunnel-name* | **fromtunnel** *tunnel-name*| **webauth** } – 指定策略规则的处理行为。
  - **permit** - 允许流量通过。
  - **deny** - 拒绝流量通过。
  - **tunnel** - 当流量为从本地到对端时，使用该行为使流量通过 VPN 隧道。
  - **fromtunnel** - 当流量为从对端到本地时，如果使用该行为，系统将会首先判断流量是否来自隧道，只有来自隧道的流量才会被允许通过。
  - **webauth** - 对符合条件的流量进行 Web 认证。

例如，创建允许从任意地址到任意地址的 ICMP 服务的策略规则，请输入以下命令：

```
hostname(config)# policy-global
hostname(config-policy)# rule from any to any service icmp permit
Rule id 5 is created.
```

删除策略规则，在全局配置模式或者策略配置模式下，使用以下命令：

no rule {**id** *id* | **name** *name*}

- **id** *id* – 删除指定 ID 的策略规则。
- **name** *name* – 删除指定名称的策略规则。

{b}提示: {/b}关于如何配置其它策略相关参数，请参考下一节“编辑策略规则”。

编辑策略规则

创建好的策略规则可以进行编辑来修改不合适的参数值，但是修改工作必须在规则配置模式下进行。在 CLI 中进入策略规则配置模式，请在全局配置模式或策略配置模式下输入以下命令：

rule [**id** *id*] [**top** | **before** {**name** *name* | *id*} | **after** {**name** *name* | *id*]

进入策略规则配置模式后，可使用的编辑策略规则的命令如下：

- 命名/重新命名策略规则：**name** *policy-name*
- 指定/修改源安全域：**src-zone** *src-zone*
- 删除源安全域：**no src-zone**（执行该命令后，策略规则无源安全域限制）
- 指定/修改目的安全域：**dst-zone** *dst-zone*
- 删除目的安全域：**no dst-zone**（执行该命令后，策略规则无目的安全域限制）
- 添加地址簿条目类型源地址：**src-addr** *src-addr*
- 删除地址簿条目类型源地址：**no src-addr** *src-addr*
- 添加 IP 成员类型源地址：**src-ip** *ip/netmask*
- 删除 IP 成员类型源地址：**no src-ip** *ip/netmask*
- 添加主机成员类型源地址：**src-host***host-name*
- 删除主机成员类型源地址：**no src-host** *host-name*
- 添加 IP 地址范围类型源地址：**src-range** *min-ip* [*max-ip*]
- 删除 IP 地址范围类型源地址：**no src-range** *min-ip* [*max-ip*]
- 添加地址簿条目类型目的地址：**dst-addr** *dst-addr*
- 删除地址簿条目类型目的地址：**no dst-addr** *dst-addr*
- 添加 IP 成员类型目的地址：**dst-ip** {*ip/netmask* | *ip-address netmask*}
- 删除 IP 成员类型目的地址：**no dst-ip** {*ip/netmask* | *ip-address netmask*}
- 添加主机成员类型目的地址：**dst-host** *host-name*
- 删除主机成员类型目的地址：**no dst-host** *host-name*
- 添加 IP 地址范围类型目的地址：**dst-range** *min-ip* [*max-ip*]
- 删除 IP 地址范围类型目的地址：**no dst-range** *min-ip* [*max-ip*]
- 添加服务类型：**service** *service-name*
- 删除服务类型：**no service** *service-name*
- 添加/删除服务规则：服务规则包括服务的协议类型和端口号，可以根据需要的协议和端口号，配置服务规则并在策略中添加该服务规则。关于如何添加/删除服务规则，请参阅配置服务规则。
- 添加应用类型：**application** *application-name*
- 删除应用类型：**no application** *application-name*

- 指定角色：**role** {**UNKNOWN** | *role-name*}
- 删除角色：**no role** {**UNKNOWN** | *role-name*}
- 指定用户：**user** *aaa-server-name user-name*
- 删除用户：**no user** *aaa-server-name user-name*
- 指定用户组：**user-group** *aaa-server-name user-group-name*
- 删除用户组：**no user-group** *aaa-server-name user-group-name*
- 修改处理行为：**action** {**permit** | **deny** | **tunnel** | **fromtunnel** | **webauth**}
- 配置时间表：**schedule** *schedule-name*
- 删除时间表：**no schedule** *schedule-name*

{b}提示: {/b}默认情况下，配置的策略规则会即时生效，而当为策略规则配置时间表功能后，策略规则就只在时间表所指定的时间内生效。用户最多可以为一条策略规则配置 8 个时间表，策略规则的生效时间为所有被配置到该策略规则的时间表的时间的总和。关于如何配置时间表，请参阅“系统管理”的“配置时间表”部分。

- 添加描述：**description** *description*（*description* 的取值范围是 1 到 255 字节
- 删除描述：**no description** *description*
- 修改规则的QoS 标签：**policy-qos-tag** *tag*（*tag* 的取值范围是 1 到 1024）
- 删除规则的QoS 标签：**no policy-qos-tag** *tag*
- 绑定病毒过滤Profile：**av** {*av-profile-name* | **no-av**}（**no-av** 参数表示绑定系统预定义的名为“no-av”的病毒过滤Profile，含义为不做病毒过滤检测）
- 取消病毒过滤Profile 的绑定：**no av**
- 绑定 IPS Profile：**ips** {*ips-profile-name* | **no-ips**}（**no-ips** 参数表示绑定系统预定义的名为“no-ips”的 IPS Profile，含义为不做 IPS 检测）
- 取消 IPS Profile 的绑定：**no ips**
- 绑定行为Profile：**behavior** {*behavior-profile-name* | **no-behavior**}（**no-behavior** 参数表示绑定系统预定义的名为“no-behavior”的行为Profile，含义为不做行为控制）
- 取消行为Profile 的绑定：**no behavior**
- 绑定内容过滤Profile：**contentfilter** {*contentfilter-profile-name* | **no-contentfilter**}（**no-contentfilter** 参数表示绑定系统预定义的名为“no-contentfilter”的内容过滤Profile，含义为不做内容过滤）

- 取消内容过滤Profile 的绑定：**no contentfilter**
- 绑定邮件过滤Profile：**mail** {*mail-profile-name* | **no-mail**}（**no-mail** 参数表示绑定系统预定义的名为“no-mail”的邮件过滤Profile，含义为不做邮件过滤）
- 取消邮件过滤Profile 的绑定：**no mail**
- 绑定网络聊天Profile：**im** {*im-profile-name* | **no-im**}（**no-im** 参数表示绑定系统预定义的名为“no-im”的网络聊天Profile，含义为不做网络聊天监控）
- 取消网络聊天Profile 的绑定：**no im**
- 绑定 Web 外发信息Profile: **webpost** {*webpost-profile-name* | **no-webpost**}（**no-webpost** 参数表示绑定系统预定义的名为“no-webpost”的 Profile，含义为不做 Web 外发信息检测）
- 取消 Webpost Profile 的绑定：**no webpost**
- 绑定 URL 过滤 Profile: **url** {*url-profile-name* | **no-url**}（**no-url** 参数表示绑定系统预定义的名为“no-url”的Profile，含义为不做 URL 过滤检测）
- 取消 URL 过滤 Profile 的绑定：**no url**
- 绑定 GTP Profile：**gtp-profile** *profile-name*
- 取消 GTP Profile 的绑定：**no gtp-profile**

启用/禁用策略规则

默认情况下，配置好的策略规则会在系统中立即起效。用户可以通过命令禁用某条策略规则，使其不对流量进行控制。禁用或者启用某条策略规则，在策略规则配置模式下，使用以下命令：

- 禁用：**disable**
- 启用：**enable**

策略规则的日志管理

- 对于 permit 类型的策略规则，可以记录两种情况，分别是符合策略规则的流量建立会话时生成日志信息和结束会话时生成日志信息。
- 对于 deny 类型的策略规则，可以记录的情况为：符合策略规则的流量被 deny 时生成日志信息。

使用该功能前，必须保证系统的流量日志功能是开启的，即在全局配置模式下，执行 **logging traffic on** 命令。配置规则的日志管理，在策略规则配置模式下，使用以下命令：

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

- **policy-deny** – 适用于 deny 类型的策略规则。使系统生成规则拒绝流量的日志信息。

- **session-start** – 适用于 permit 类型的策略规则。使系统生成会话建立的日志信息。
- **session-end** – 适用于 permit 类型的策略规则。使系统生成会话结束的日志信息。

使用 **no log** {**policy-deny** | **session-start** | **session-end**}命令取消策略规则日志管理功能的配置。

另外，对于从指定源安全域到目的安全域的未匹配到策略规则的流量，用户可以指定是否为其生成日志信息。默认情况下，系统不为此类流量生成日志信息。生成日志信息，在策略配置模式下，使用以下命令：

log policy-default

在策略配置模式下，使用该命令 no 的形式恢复默认值：

no log policy-default

配置服务规则

在配置策略规则的服务时，可以添加服务簿中已配置好的预定义服务或者自定义服务。当所需要的服务在服务簿中不存在时，管理员可以通过配置服务规则，直接指定服务的协议类型以及端口号等信息，从而简化策略的配置步骤。

配置TCP 或者 UDP 类型服务规则，在策略规则配置模式下，使用以下命令：

service-rule {**tcp** | **udp**} **dst-port***min-port* [*max-port*] [**src-port***min-port* [*max-port*]]

- **tcp** | **udp** - 指定服务规则的协议类型：TCP 或者 UDP。
- **dst-port***min-port* [*max-port*] – 指定服务规则的目的端口号。如果目的端口号为一个范围，*min-port* 为最小目的端口号，*max-port* 为最大目的端口号；如果不配置 *max-port*，系统将使用 *min-port* 作为单一目的端口号。目的端口号的范围是 0 到 65535。
- **src-port***min-port* [*max-port*] – 指定服务规则的源端口号。如果源端口号为一个范围，*min-port* 为最小源端口号，*max-port* 为最大源端口号；如果不配置 *max-port*，系统将使用 *min-port* 作为单一源端口号。源端口号的范围是 0 到 65535。

配置ICMP 类型服务规则，在策略规则配置模式下，使用以下命令：

service-ruleicmp type*type-value* [**code***min-code* [*max-code*]]

- *type-value* – 指定服务规则的 ICMP type 值。范围是 0（Echp-Reply）、3（Destination-Unreachable）、4（Source Quench）、5（Redirect）、8（Echo）、11（Time Exceeded）、12（Parameter Problem）、13（Timestamp）、14（Timestamp Reply）、15（Information Request）、16（Information Reply）、17（Address Mask Request）、18（Address Mask Reply）、30（Traceroute）、31（Datagram Conversion Error）、32（Mobile Host Redirect）、33（IPv6 Where-Are-You）、34（IPv6 I-Am-Here）、35（Mobile Registration Request）、36（Mobile Registration Reply）。

- **code** *min-code* [*max-code*] – 指定服务规则的ICMP code 值。如果 ICMP code 值为一个范围，*min-code* 为最小 code 值，*max-code* 为最大 code 值；如果不配置 *max-code*，系统将使用 *min-code* 作为单一code 值。范围是 0 到 15。默认值是 *min-code* 为 0、*max-code* 为 15。

配置ICMPv6 类型服务规则，在策略规则配置模式下，使用以下命令：

service-rule icmpv6 type *type-value* [**code** *min-code* [*max-code*]]

- *type-value* – 指定服务规则的 ICMPv6 type 值。取值范围请参考附表：ICMPv6 Type 以及 Code 值对照表。
- **code** *min-code* [*max-code*] – 指定服务规则的ICMPv6 code 值。如果 ICMPv6 code 值为一个范围，*min-code* 为最小 code 值，*max-code* 为最大code 值；如果不配置 *max-code*，系统将使用 *min-code* 作为单一code 值。范围是 0 到 255。默认值是 *min-code* 为 0、*max-code* 为 255。

配置其它类型服务规则，在策略规则配置模式下输入以下命令：

service-rule protocol *protocol-number*

- *protocol-number* – 指定服务规则的协议号。范围是 1 到 255。

使用以上四条命令 no 的形式可以删除对应服务规则。

- **no service-rule** {**tcp** | **udp**} **dst-port** *min-port* [*max-port*] [**src-port** *min-port* [*max-port*]]
- **no service-rule icmp type** *type-value* [**code** *min-code* [*max-code*]]
- **no service-rule icmpv6 type** *type-value* [**code** *min-code* [*max-code*]]
- **no service-rule protocol** *protocol-number*

指定缺省行为

用户可以为未匹配到任何已配置策略规则的流量指定缺省行为，系统将按照指定的缺省行为对此类流量进行处理。默认情况下，系统会拒绝未匹配到任何已配置策略规则的流量通过。指定缺省行为为允许，在策略配置模式下，使用以下命令：

default-action permit

在策略配置模式下，使用该命令 no 的形式，恢复缺省行为为“拒绝”：

no default-action permit

修改规则排列顺序

每一条策略规则都有唯一一个 ID 号和名称。流量进入设备时， 设备对策略规则进行顺序查找，然后按照查找到的相匹配的第一条规则对流量进行处理。但是，策略规则 ID 的大小顺序并不是规则查找时的匹

配顺序。使用 **show policy** 命令列出的规则顺序才是规则匹配顺序（系统将由上到下进行查找）。用户在创建策略规则时可以指定该规则的排列位置，也可以在策略配置模式下修改其位置。策略规则的排列位置可以是绝对位置，即处在首位（Top）或者处在末位（Bottom），也可以是相对位置，即位于某个 ID 或者名称的前后。修改规则排列顺序，在策略配置模式下使用以下命令：

move {**name** *name* | *id*} {**top** | **bottom** | **before** {**name** *rule-name* | *id*} | **after** {**name** *rule-name* | *id*} }

- **name** *name* | *id* – 指定需要修改排列顺序的策略规则 ID 或者名称。
- **top** – 指定策略规则修改后的位置为所有规则的首位。
- **before** {**name** *rule-name* | *id*} – 指定策略规则修改后的位置为某个规则 ID 或者名称之前。
- **after** {**name** *rule-name* | *id*} – 指定策略规则修改后的位置为某个规则 ID 或者名称之后。

规则冗余检测

为保证策略中规则的有效性，系统可对规则进行冗余检测，即检查规则的覆盖情况，帮助用户排除由于规则覆盖导致的匹配问题。

在任何模式下，使用以下命令开始规则的冗余检测：

exec policy redundancy-check start

检测开始后，将持续一段时间，请耐心等待。检测完成后，用户可使用 **show policy redundancy-check** 命令查看策略规则 ID 和被覆盖的规则 ID。

用户也可使用 **exec policy redundancy-check stop** 命令停止冗余检测，或使用 **exec policy redundancy-check clear** 命令清除上一次的规则冗余检测结果缓存。

策略组

用户可以将一些策略规则组织到一起便组成了策略组。用户可以直接将对策略组进行配置，这样便简化了管理。

配置策略组

用户可以通过 CLI 对策略组进行以下配置：

- 新建/删除策略组
- 启用/禁用策略组
- 添加/删除策略组描述信息
- 添加/删除策略规则成员
- 策略组重命名

- 配置 VSYS Profile 策略组

新建/删除策略组

新建策略组，请在全局配置模式下，输入以下命令：

policy-group *group-name*

- *group-name* – 指定策略组名称。范围是 1 到 95 个字符。

运行该命令后，系统进入策略组配置模式。

删除策略组，请在全局配置模式下，输入以下命令：

no policy-group *group-name*

启用/禁用策略组

默认情况下，策略组为启用状态。启用/禁用策略组，在策略组配置模式下，使用以下命令：

- 启用：**enable**
- 禁用：**disable**

注意：

- 启用/禁用策略组后，策略组中的策略规则成员启用状态同时被修改。
- 不允许直接启用或者禁用策略组中的某个策略规则成员。

添加/删除策略组描述信息

在策略组配置模式下，用户可以通过使用以下命令为策略组添加描述信息。

description *description*

- *description* – 指定策略组名称。范围是 1 到 95 个字符。

在策略组配置模式下，使用以下命令删除策略组的描述信息。

no description

添加/删除策略规则成员

在策略组配置模式下，用户可以通过使用以下命令为策略组添加策略规则成员。

rule *id*

- *id* – 指定策略规则 ID。

在策略组配置模式下，使用以下命令删除策略组的策略规则成员。

no rule *id*

注意:一条策略规则只能添加到一个策略组中。

策略组重命名

在全局配置模式下，用户可以通过使用以下命令为策略组重命名。

rename policy-group *old-name new-name*

- *old-name* – 指定策略组的旧名称。
- *new-name* – 指定策略组的新名称。

配置 VSYS Profile 策略组

在 VSYS Profile 配置模式下，用户可以通过使用以下命令为 VSYS Profile 配置策略组。

policy-group max *max-num* **reserve** *reserve-num*

- **max** *max-num* **reserve** *reserve-num* – 指定 VSYS 中策略组的最大配额（**max** *max-num*）和预留配额（**reserve** *reserve-num*）。最大配额和预留配额根据不同平台取值范围不同。预留配额不能超过最大配额。

查看策略组配置信息

查看策略组配置信息，在任何模式下，使用以下命令:

show policy-group [*name*]

- *name* – 查看指定策略组名称的配置信息。

查看策略规则信息

用户可以在任何模式下，通过 show 命令查看策略规则的具体信息。具体命令以下:

show policy [**id** *id*] [**from** *src-zone*] [**to** *dst-zone*] [**src-addr** *src-addr*] [**dst-addr** *dst-addr*] [**service** *service-name*] [**application** *application-name*] [**description** *description*] [**name** *name*] [**name-filter** *filter-name*]

- **id** *id* – 显示指定 ID 规则的详细信息。
- **from** *src-zone* – 显示源安全域为指定域的规则的详细信息。
- **to** *dst-zone* – 显示目标安全域为指定域的规则的详细信息。
- **src-addr** *src-addr* – 显示指定地址簿条目类型源地址的规则的详细信息。
- **dst-addr** *dst-addr* – 显示指定地址簿条目类型目的地址的规则的详细信息。
- **service** *service-name* – 显示指定服务类型的规则详细信息。
- **application** *application-name* – 显示指定应用类型的规则详细信息。
- **description** *description* – 显示指定描述信息的规则详细信息。
- **name** *name* – 显示指定名称的规则详细信息。
- **name-filter** *filter-name* – 显示名称包含指定关键字的所有规则详细信息。

查看设备的当前策略配置信息

查看设备的当前策略配置信息，在任何命令模式下输入以下命令：

show configuration policy [**name** *name* | **id** *id* | **by-line**]

- **name** *name* – 单行显示指定名称的策略规则配置信息。
- **id** *id* – 单行显示指定 ID 的策略规则配置信息。
- **by-line** – 单行显示所有策略规则配置信息。

查看策略规则匹配次数

为方便用户对策略规则的管理和维护， 设备支持策略规则匹配次数统计功能。该功能能够对系统流量与策略规则的匹配次数进行统计，即每当进入系统的流量与某条策略规则相匹配时，该策略规则的匹配次数会自动加 1。用户可以在任何模式下通过以下命令查看策略规则匹配次数统计信息：

show policy hit-count [**id** *id* | **name** *name* | [**from** *src-zone*] [**to** *dst-zone*] **top** {10 | 20 | 50 | **all** }]

- **id** *id* – 显示指定 ID 规则的匹配次数统计信息。
- **name** *name* – 显示指定名称规则的匹配次数统计信息。
- **from** *src-zone* – 显示源安全域为指定域的规则的匹配次数统计信息。

- top {10 | 20 | 50 | all } – 显示匹配次数位于前 10、20、50 位的规则的匹配次数统计信息或者按降序方式显示所有规则的匹配次数统计信息。

例如:

查看所有规则的匹配次数统计信息

hostname(config)# **show policy hit-count**

Most hit policy rules:

==========

No. Id Src-zone Dst-zone Src-addr Dst-addr Service Applica~ Action Hit-count

---

1 14 trust trust Any Any Any PERMIT 0

2 4 untrust trust Any Any Any PERMIT 1

3 3 trust untrust Any Any Any PERMIT 761697

4 1 Any Any Any Any Any PERMIT 64203455

==========

查看指定ID 规则的匹配次数统计信息

hostname(config)# **show policy hit-count id 1**

Policy id 1 is hit 342424 times

查看指定名称规则的匹配次数统计信息

SG-6000(config)# **show policy hit-count name a**

Policy "a" is hit 0 times

查看匹配次数位于前 10 位的规则的匹配次数统计信息

hostname(config)# **show policy hit-count top 10**

Most hit policy rules:

==========

No. Id Src-zone Dst-zone Src-addr Dst-addr Service Action Hit-count

```
---------------------------------------------------------------
1 4 trust trust any any http permit 40029
2 6 zone2 untrust addr1 any any deny 7487
3 3 zone2 untrust s1 d1 ftp permit 3834
4 29 trust untrust any any any permit 2899
5 14 zone1 zone2 s2 any pop3 permit 2046
按降序方式查看所有规则的匹配次数统计信息
hostname(config)# show policy hit-count top all
Most hit policy rules:
==========================================================================
==========
No. Id Src-zone Dst-zone Src-addr Dst-addr Service Applica~ Action Hit-count
---------------------------------------------------------------------------
1 1 Any Any Any Any Any PERMIT 64212319
2 3 trust untrust Any Any Any PERMIT 762070
3 4 untrust trust Any Any Any PERMIT 1
4 14 trust trust Any Any Any PERMIT 0
==========================================================================
==========
```

清除策略规则匹配次数统计信息，请在任意模式下使用以下命令：

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

- **all** – 清除所有规则的匹配次数统计信息。
- **id** *id* – 清除指定 ID 规则的匹配次数统计信息。
- **name** *name* – 清除指定名称规则的匹配次数统计信息。

清除策略规则的缺省行为匹配次数统计信息，请在任意模式下使用以下命令：

clear policy hit-count default-action

配置策略助手

为了提高用户配置安全策略的完整性、准确性和快速性，系统提供策略助手功能。策略助手能够提取命中指定策略 ID 的流量作为流量数据分析源，并根据用户设置的聚合规则聚合数据流量列表，最后自动生成符合用户期望的安全策略规则。

开启/关闭策略助手

启用策略助手功能，在策略规则配置模式下，使用以下命令：

assistant enable

注意:根VSYS 最多支持开启 4 个策略规则 ID 的策略助手功能；非根 VSYS 最多支持开启 1 个策略规则 ID 的策略助手功能。

关闭策略助手功能，在策略规则配置模式下，使用以下命令：

assistant disable

示例：

```
hostname(config)# policy-global
hostname(config-policy)# rule id 2
hostname(config-policy-rule)# assistant enable
```

查看开启策略助手的策略

查看已开启策略助手功能的策略的详细信息，在任意模式下，使用以下命令：

show policy assistant-enable

第 3 章 路由

路由是将数据包从一个网络转发到另一个网络中的目的地址的过程。路由器是处在两个网络之间转发数据包的设备。路由器根据路由表中储存的各种传输路径传输数据包，每一个传输路径即为一个路由条目。

StoneOS 具有三层路由功能，通过VRouter，进行路由配置，对不同的数据包进行转发。StoneOS 支持静态路由（Static Routing）、ISP 路由、源路由（Source-Based Routing，简称 SBR）、源接口路由（Source-Interface-Based Routing，简称 SIBR）、目的接口路由（Destination-Interface-Based Routing，简称 DIBR）、策略路由（Policy-Based Routing，简称 PBR）、就近探测路由（Proximity Routing）、动态路由（包括 RIP、OSPF、IS-IS 和 BGP）和等价多径路由（Equal Cost MultiPath Routing，简称 ECMP）和静态组播路由（Static Multicast-routing）。

本章节包含以下内容:

- "静态路由"：手工配置的、根据目的 IP 地址确定下一跳的路由。
- "目的接口路由"：根据数据包的目的 IP 地址和入接口，选择路由，进行转发。
- "ISP 路由"：根据不同的 ISP 确定下一跳。
- "配置源路由"：根据数据包的源 IP 地址，选择路由，进行转发。
- "配置源接口路由 "：根据数据包的源 IP 地址和入接口，选择路由，进行转发。
- "配置策略路由"：根据数据包的源地址、源用户、目的地址以及服务类型，选择路由，进行转发。
- 就近探测路由：根据出站就近探测的结果选择路由，进行转发。
- "动态路由"：设备按照动态路由协议（RIP、OSPF 或者 BGP）自动生成的动态路由表项对数据包进行路由选择并转发。
- "等价多径路由（ECMP）"：到达相同目的 IP 地址或网段的数据流量在多条相同管理距离的路径上进行负载均衡。
- "静态组播路由"：手工配置的、将数据从一个组播源传送至组播组内各成员的路由。

当设备对进入的数据包进行转发时，按照这样的顺序选路：策略路由->源接口路由->源路由->目的接口路由->目的路由/ISP 路由/就近探测路由/动态路由。

开启/关闭静态路由查询

对于策略路由、源接口路由和源路由，用户可以单独控制是否需要对它们进行查询（系统要求必须进行目的路由查询）。默认情况下，策略路由、源接口路由和源路由查询为开启状态。开启/关闭策略路由、源接口路由和源路由查询，在全局配置模式下，使用以下命令（适用于所有VRouter）：

- 开启：**route enable {pbr | sibr | sbr}**
- 关闭：**route disable {pbr | sibr | sbr}**

开启/关闭会话重匹配路由

默认情况下，会话重匹配路由的功能是开启的。当用户添加、修改或者删除路由时，会话会重新匹配最优路由。在会话重新匹配路由的过程中，符合以下情况的会话会被删除：

- 当会话之前匹配的路由或者路由的出接口被删除时，该会话会被删除。
- 当会话之前匹配的路由不是最优路由，且重新匹配的路由的出接口发生变化时，该会话会被删除。

在某些情况下（如添加或删除策略路由的应用类型），会话可能会被大量删除，导致流量异常。此时，需要关闭会话重新匹配功能。

在 Flow 配置模式下，使用以下命令关闭或开启此功能：

- **session rematch route disable**
- **session rematch route enable**

VRouter

VRouter 的功能与路由器相同，并且拥有自己的路由表。系统有一个默认 VRouter，即 trust-vr，同时系统支持多 VRouter（多 VR）功能。 设备的所有路由配置都需要在相应的VRouter 配置模式下进行。进入 VRouter 配置模式，在全局配置模式下使用以下命令：

ip vrouter *vrouter-name*

- *vrouter-name* – 指定 VRouter 的名称。

在 VRouter 配置模式下，用户可以配置静态路由条目、动态路由协议，也可以指定 VRouter 支持的最大路由条目数以及从其它 VRouter 引入路由。

使用多 VR 功能，需要先执行 **exec vrouter enable** 命令后再重启系统使多 VR 功能生效。

指定最大路由条目数

指定VRouter 允许的最大路由条目数（包含VRouter 下的所有直连路由、静态路由和各种动态路由），在VRouter 配置模式下，使用以下命令：

max-routes *number*

- *number* – 指定最大路由条目数。范围是 1 到 100000。

在 VRouter 配置模式下，使用该命令 no 的形式取消最大路由条目数的指定：

no max-routes

当路由条目数达到最大路由条目数，系统将会发出警告。

引入 VRouter 路由

用户可以把其它 VRouter 中的路由条目引入到当前VRouter 进行使用。引入VRouter 路由，在VRouter 配置模式下使用以下命令：

import vrouter *vrouter-name* {**connected** | **static** | **rip** | **ospf** | **bgp**}

- *vrouter-name* – 指定被引入路由所属的VRouter。
- **connected** | **static** | **rip** | **ospf** | **bgp** – 指定被引入路由的类型。

多次配置该命令引入多种类型路由。

注意:从其它VRouter 引入的路由的优先级低于 VRouter 自身的路由。

取消直连路由优先

直连路由拥有最高路由优先级，在同时配置其他路由时，直连路由会被优先使用，使得其他路由不生效，因此，用户可以根据需要，取消直连路由优先，使其他路由优先使用。在VRouter 配置模式下使用以下命令：

fib-lookup connect-first-disable

在 VRouter 配置模式下，使用该命令 no 的形式恢复直连路由优先：

no fib-lookup connect-first-disable

静态路由

静态路由是手工定义的路由条目，根据目的地址指定下一跳，因此也称作目的路由。对外连接较少或者内网连接相对比较稳定的网络通常使用静态路由。用户可以根据需要确定是否添加默认路由条目。

配置静态路由

用户可以添加目的路由条目并且显示目的路由信息。

添加目的路由条目

用户可以为 VRouter 添加目的路由条目。但是，添加目的路由条目之前，需要进入 VRouter 配置模式。请在全局配置模式下使用以下命令：

ip vrouter *vrouter-name*

- *vrouter-name* – 指定 VRouter 的名称。

进入到 VRouter 配置模式下后，用户可以添加目的路由条目。在VRouter 配置模式下使用以下命令：

ip route {*A.B.C.D/M* | *A.B.C.D A.B.C.D*} {*A.B.C.D* | *interface-name*[*A.B.C.D*] | **vrouter** *vrouter-name*} [*distance-value*] [**weight** *weight-value*] [**tag** *tag-value*] [**description** *description*] [**schedule** *schedule-name*]

- *A.B.C.D/M* | *A.B.C.D A.B.C.D* – 指定目的地址。设备支持两种方式，A.B.C.D/M 或者 A.B.C.D A.B.C.D，例如 1.1.1.0/24 或者 1.1.1.0 255.255.255.0。
- *A.B.C.D* | *interface-name* [*A.B.C.D*] | **vrouter** *vrouter-name* – 指定下一跳。可以是网关地址（*A.B.C.D*）、接口（*interface-name*）或者 VRouter（**vrouter** *vrouter-name*）。当下一跳为接口时，用户可以选择隧道接口名称（当为多隧道接口时，用户必须使用A.B.C.D 参数指定 IPSec VPN、GRE 或者 SCVPN 隧道的下一跳 IP 地址，并且此地址必须和该隧道接口绑定的相应隧道的下一跳 IP 地址相同）、Null0 接口或者PPPoE 接口。
- *distance-value* – 指定路由的管理距离大小。该参数设定路由的优先级，取值越小，优先级越高，而在有多条路由选择的时候，优先级高的路由会被优先使用。取值范围是 1 到 255，默认值为 1。当路由距离为 255 时，该路由无效。
- **weight** *weight-value* – 指定路由权值的大小。路由权值决定负载均衡中流量转发的比重。范围是 1 到 255，默认值是 1。
- **tag** *tag-value* – 指定目的路由的标记值。在 OSPF 引入路由时，如果此处配置的路由标记值匹配到路由映射表中的规则，那么将会引入该路由，从而实现对引入路由信息的过滤。取值范围是 1 到 4294967295。
- **description** *description* – 指定路由的描述信息。范围是 1 到 63 个字符。
- **schedule** *schedule-name* – 指定时间表名称。该条配置将会在时间表指定的时间范围内生效。可配置多次该命令指定多个时间表（最多 8 个）。为避免产生不可预知的问题，建议用户不要配置时间重叠的时间表。

使用多条该命令添加多条静态路由条目。

使用以上命令 no 的形式删除指定的静态路由条目：

no ip route {*A.B.C.D/M* | *A.B.C.D A.B.C.D*} {*A.B.C.D* | *interface-name A.B.C.D* | *interface-name* [*A.B.C.D*] | **vrouter** *vrouter-name*} [**description** *description*] [**schedule** *schedule-name*]

显示目的路由信息

用户可以在任何模式下使用以下命令查看目的路由信息：

show ip route static [**vrouter** *vrouter-name*]

- *vrouter-name* - 显示指定的VRouter 的目的路由信息。

目的接口路由

目的接口路由（DIBR）根据数据包的目的 IP 地址和入接口，选择路由，进行转发。

添加目的接口路由条目

目的接口路由的配置也需要在VRouter 配置模式下完成。进入 VRouter 配置模式，在全局配置模式下，使用以下命令：

ip vrouter *vrouter-name*

进入到 VRouter 配置模式下后，用户可以添加目的接口路由条目。在VRouter 配置模式下使用以下命令：

ip route in-interface *interface-name* {*A.B.C.D/M* | *A.B.C.D A.B.C.D*} {*A.B.C.D* | *interface-name* [*A.B.C.D*] | **vrouter** *vrouter-name*} [*distance-value*] [**weight** *weight-value*] [**description** *description*] [**schedule** *schedule-name*]

- **in-interface** *interface-name* - 指定路由条目的入接口。
- *A.B.C.D/M* | *A.B.C.D A.B.C.D* – 指定目的地址。 设备支持两种方式，*A.B.C.D/M* 或者 *A.B.C.D A.B.C.D*，例如 1.1.1.0/24 或者 1.1.1.0 255.255.255.0。
- *A.B.C.D* | *interface-name* [*A.B.C.D*] | **vrouter** *vrouter-name* – 指定下一跳。可以是网关地址（*A.B.C.D*）、接口（*interface-name*）或者 VRouter（**vrouter** *vrouter-name*）。当下一跳为接口时，用户可以选择隧道接口名称（当为多隧道接口时，用户必须使用A.B.C.D 参数指定 IPSec VPN、GRE 或者 SCVPN 隧道的下一跳 IP 地址，并且此地址必须和该隧道接口绑定的相应隧道的下一跳 IP 地址相同）、Null0 接口或者PPPoE 接口。
- *distance-value* – 指定路由的管理距离大小。该参数设定路由的优先级，取值越小，优先级越高，而在有多条路由选择的时候，优先级高的路由会被优先使用。取值范围是 1 到 255，默认值为 1。当路由距离为 255 时，该路由无效。
- **weight** *weight-value* – 指定路由权值的大小。路由权值决定负载均衡中流量转发的比重。范围是 1 到 255，默认值是 1。
- **description** *description* – 指定路由的描述信息。范围是 1 到 63 个字符。

- **schedule** *schedule-name* – 指定时间表名称。该条配置将会在时间表指定的时间范围内生效。可配置多次该命令指定多个时间表（最多 8 个）。为避免产生不可预知的问题，建议用户不要配置时间重叠的时间表。

使用多条该命令添加多条目的接口路由条目。

使用以上命令 no 的形式删除指定的目的接口路由条目：

no ip route in-interface *interface-name* {*A.B.C.D/M* | *A.B.C.D A.B.C.D*} {*A.B.C.D* | *interface-name* [*A.B.C.D*] | **vrouter** *vrouter-name*} [**description** *description*] [**schedule** *schedule-name*]

查看目的接口路由信息

用户可以在任何模式下使用以下命令查看目的接口路由信息：

show ip route in-interface *interface-name*

- **in-interface** *interface-name* - 显示指定入接口的目的接口路由信息。

查看目的接口路由的 FIB 信息

用户可以在任何模式下使用以下命令查看目的接口路由的 FIB 信息：

show ip fib in-interface *interface-name*

- **in-interface** *interface-name* - 显示指定入接口的目的接口路由的FIB 信息。

ISP 路由

很多用户通常会申请多条线路进行流量负载均衡。然而，一般的均衡是不会根据流量的流向做均衡的，如果网通的服务器通过电信访问，网速就会很慢。 设备针对该问题，提供 ISP 路由功能，使不同 ISP 流量走专有路由，从而提高网络速度。

配置 ISP 路由，用户首先需要将子网条目添加到一个 ISP，然后才可以配置以 ISP 名称为目的地的 ISP 路由。用户可以自定义 ISP 信息，也可以上传 ISP 包含不同 ISP 信息的配置文件。同时StoneOS 提供一个预定义 ISP 配置文件，包含两个 ISP，分别是中国电信（China-telecom）和中国网通（China-netcom）。

配置 ISP 路由，用户需要进行的操作如下：

- 配置 ISP 信息
- 配置 ISP 路由
- 上传 ISP 配置文件
- 查看 ISP 路由配置信息

- 删除已上传的预定义 ISP 配置文件

配置 ISP 信息

在设备上配置 ISP 信息，首先需要进入 ISP 信息配置模式。在全局配置模式下，使用以下命令，创建 ISP 名称并且进入 ISP 信息配置模式：

isp-network *isp-name*

- *isp-name* – 指定 ISP 名称。

在全局配置模式下，使用该命令 no 的形式删除指定名称的 ISP：

no isp-network *isp-name*

为 ISP 添加子网条目，在ISP 信息配置模式下，使用以下命令：

subnet *A.B.C.D/M*

- *A.B.C.D/M* – 为 ISP 指定子网，格式为 IP 地址/掩码，例如 1.1.1.0/24。

在 ISP 信息配置模式下配置多条该命令，为 ISP 添加多个子网。

在 ISP 信息配置模式下使用该命令 no 的形式删除指定的子网：

no subnet *A.B.C.D/M*

配置 ISP 路由

ISP 路由需要在VRouter 配置模式下进行配置。进入VRouter 配置模式，在全局配置模式下使用以下命令：

ip vrouter *vrouter-name*

- *vrouter-name* – 指定 VRouter 的名称。

在 VRouter 配置模式，使用以下命令配置 ISP 路由条目：

ip route *isp-name* {*A.B.C.D* | *interface-name* | **vrouter** *vrouter-name*} [*distance-value*] [**weight** *weight-value*] [**description** *description*] [**schedule** *schedule-name*]

- *isp-name* – 指定系统中已存在的 ISP 名称作为路由的目的地址。
- *A.B.C.D* | *interface-name* | **vrouter** *vrouter-name* – 指定下一跳。可以是网关地址（*A.B.C.D*）、接口（*interface-name*）或者 VRouter（**vrouter** *vrouter-name*）。当下一跳为接口时，用户可以选择隧道接口名称、Null0 接口或者 PPPoE 接口。

- *distance-value* – 指定路由的管理距离大小。该参数设定路由的优先级，取值越小，优先级越高，而在有多条路由选择的时候，优先级高的路由会被优先使用。取值范围是 1 到 255，默认值为 1。当路由距离为 255 时，该路由无效。
- **weight** *weight-value* – 指定路由权值的大小。路由权值决定负载均衡中流量转发的比重。范围是 1 到 255，默认值是 1。
- **description** *description* – 指定路由的描述信息。范围是 1 到 63 个字符。
- **schedule** *schedule-name* – 指定时间表名称。该条配置将会在时间表指定的时间范围内生效。可配置多次该命令指定多个时间表（最多 8 个）。为避免产生不可预知的问题，建议用户不要配置时间重叠的时间表。

使用多条该命令添加多条 ISP 路由条目。

使用以上命令 no 的形式删除指定的 ISP 路由条目：

no ip route *isp-name* {*A.B.C.D* | *interface-name* | **vrouter** *vrouter-name*} [*distance-value*] [**weight** *weight-value*] [**description** *description*] [**schedule** *schedule-name*]

查看 ISP 路由配置信息

用户可以通过 show 命令查看 ISP 路由配置信息。

- 查看通过设备配置的 ISP 信息：
  show isp-network {**all** | *isp-name*}
- 查看 ISP 路由条目：
  show ip route isp [*isp-name* | **vrouter** *vrouter-name*]

上传 ISP 配置文件

ISP 配置文件的上传只能通过WebUI 来完成。 设备支持两种 ISP 配置文件，分别是用户自定义 ISP 配置文件和系统预定义配置文件。

请按照下所示实例格式书写用户自定义配置文件，否则，即使文件上传成功，也不可以在系统中生效。预定义/用户自定义配置文件中包含的 ISP 的个数最多为 26 个，也就是作为索引值的 26 个英文字母的个数。

```
# NOTICE: Keep the following comment lines intact!!!
E --- China-55
R --- China-66
# China-55
```

```
E:55.10.2.0/24
E:55.10.3.0/24
# China-66
R:66.20.2.0/24
R:66.20.3.0/24
```

上传预定义 ISP 配置文件

StoneOS 的预定义 ISP 配置文件为加密形式。 更新预定义 ISP 配置文件后，用户需要重新上传新的预定义 ISP 配置文件。步骤如下：

1. 从页面左侧导航树选择并点击“配置　网络　路由”，进入路由页面。
2. 点击『ISP 信息』标签，进入 ISP 页面。
3. 点击 ISP 列表左上角的『上传』按钮，弹出<从 PC 上载 ISP 配置文件>对话框。
4. 选中<从电脑上传预定义的 ISP 配置文件>或<从电脑上传用户定义的 ISP 配置文件>的单选按钮。
5. 点击『浏览』按钮在电脑上选择需要的 ISP 配置文件，然后点击『上传』按钮上传所选择的 ISP 配置文件至设备。版本行显示了当前预定义 ISP 配置文件的版本号。

保存自定义 ISP 配置文件

用户还可以将在设备上配置的 ISP 信息保存到电脑。保存步骤如下：

1. 从页面左侧导航树选择并点击“配置>网络>路由”，进入路由页面。
2. 点击『ISP 信息』标签，进入 ISP 页面。
3. 点击 ISP 列表左上角的『保存』按钮，弹出<保存用户自定义 ISP 配置到 PC>对话框。
4. 在<ISP 名称>下拉菜单中选择需要保存的 ISP 的名称。
5. 点击『保存』按钮，保存相应的 ISP 配置文件到电脑的指定位置。

删除已上传的预定义 ISP 配置文件

如果已经上传过预定义 ISP 配置文件，用户可以在执行模式下，通过使用以下命令将上传的预定义 ISP 配置文件从系统中删除：

exec isp-network clear-predefine

执行该命令后，重启系统，系统将恢复使用原有的预定义 ISP 配置文件（出厂时系统自带的预定义 ISP 配置文件）。

配置源路由

源路由的配置需要在 VRouter 配置模式下完成。进入VRouter 配置模式，在全局配置模式下，使用以下命令：

ip vrouter *vrouter-name*

添加源路由条目

在 VRouter 配置模式下，使用以下命令添加一条源路由条目：

ip route source {*A.B.C.D/M* | *A.B.C.D A.B.C.D*} {*A.B.C.D* | *interface-name* | **vrouter** *vrouter-name*} [*distance-value*] [**weight** *weight-value*] [**schedule** *schedule-name*]

- *A.B.C.D/M* | *A.B.C.D A.B.C.D* – 指定源路由条目的网络地址。设备支持两种方式，*A.B.C.D/M*或者 *A.B.C.D A.B.C.D*，例如 1.1.1.0/24 或者 1.1.1.0 255.255.255.0。
- *A.B.C.D* | *interface-name* – 指定下一跳。可以是网关地址（*A.B.C.D*）、接口（*interface-name*）或者 VRouter（**vrouter** *vrouter-name*）。当下一跳为接口时，用户可以选择隧道接口、Null0 接口或者 PPPoE 接口。
- *distance-value* – 指定路由的管理距离大小。该参数设定路由的优先级，取值越小，优先级越高，而在有多条路由选择的时候，优先级高的路由会被优先使用。取值范围是 1 到 255，默认值为 1。当路由距离为 255 时，该路由无效。
- **weight***weight-value* – 指定路由权值的大小。路由权值决定负载均衡中流量转发的权重。范围是 1 到 255，默认值是 1。
- **schedule** *schedule-name* – 指定时间表名称。该条配置将会在时间表指定的时间范围内生效。可配置多次该命令指定多个时间表（最多 8 个）。为避免产生不可预知的问题，建议用户不要配置时间重叠的时间表。

使用以上命令 no 的形式删除指定的源路由条目：

no ip route source { *A.B.C.D/M* | *A.B.C.D A.B.C.D*} {*A.B.C.D* | *interface-name*}

查看源路由条目信息

用户可以在任何模式下通过 show 命令查看源路由条目信息。在任何模式下，使用以下命令：

源路由：**show ip route source** [**vrouter** *vrouter-name*]

- *vrouter-name* – 显示指定的 VRouter 的源路由信息。

配置源接口路由

源接口路由的配置也需要在 VRouter 配置模式下完成。进入VRouter 配置模式，在全局配置模式下，使用以下命令：

ip vrouter *vrouter-name*

添加源接口路由条目

在 VRouter 配置模式下，使用以下命令添加一条源接口路由条目：

ip route source in-interface *interface-name* { *A.B.C.D/M* | *A.B.C.D A.B.C.D*} {*A.B.C.D* | *interface-name* | **vrouter** *vrouter-name*} [*distance-value*] [**weight** *weight-value*] [**schedule** *schedule-name*]

- *interface-name* – 指定路由条目的入接口。
- *A.B.C.D/M* | *A.B.C.D A.B.C.D* – 指定路由条目的源网络地址。设备支持两种方式，*A.B.C.D/M* 或者 *A.B.C.D A.B.C.D*，例如 1.1.1.0/24 或者 1.1.1.0 255.255.255.0。
- *A.B.C.D* | *interface-name* | **vrouter** *vrouter-name* – 指定下一跳。可以是网关地址（*A.B.C.D*）、接口（*interface-name*）或者 VRouter（**vrouter** *vrouter-name*）。当下一跳为接口时，用户可以选择隧道接口名称，也可以选择 Null0 接口（黑洞路由）。
- *distance-value* – 指定路由的管理距离大小。该参数设定路由的优先级，取值越小，优先级越高，而在有多条路由选择的时候，优先级高的路由会被优先使用。取值范围是 1 到 255，默认值为 1。当路由距离为 255 时，该路由无效。
- **weight** *weight-value* – 指定路由权值的大小。路由权值决定负载均衡中流量转发的权重。范围是 1 到 255，默认值是 1。
- **schedule** *schedule-name* – 指定时间表名称。该条配置将会在时间表指定的时间范围内生效。可配置多次该命令指定多个时间表（最多 8 个）。为避免产生不可预知的问题，建议用户不要配置时间重叠的时间表。

使用以上命令 no 的形式删除指定的源接口路由条目：

no ip route source in-interface *interface-name* { *A.B.C.D/M* | *A.B.C.D A.B.C.D*} {*A.B.C.D* | *interface-name* | **vrouter** *vrouter-name* }

查看源接口路由条目信息

用户可以在任何模式下通过 show 命令查看源接口路由条目信息。在任何模式下，使用以下命令：

源接口路由：**show ip route source in-interface** *interface-name*

配置策略路由

策略路由功能检查数据包的源 IP、目的 IP 和服务类型，对匹配策略的数据包的下一跳进行指定。

创建 PBR 策略

创建PBR 策略，在全局配置模式下使用以下命令：

pbr-policy *name*

- *name* – 指定 PBR 策略名，名称范围是 1 到 31 个字符。如果该策略已经创建，则直接进入PBR 策略配置模式。

使用 **no pbr-policy** *name* 删除指定的PBR 策略。

创建 PBR 规则

进入PBR 策略配置模式下，用户便可定义自己的PBR 规则。在 CLI 中创建 PBR 规则的命令如下：

{**match** | **match-v6** } [**id** *rule-id*] [**before***rule-id* | **after** rule-id | **top**] *src-addr dst-addr service-name* [*application-name*] **nexthop** {*interface-name* | *A.B.C.D* | **vrouter** *vrouter-name* | **vsys** *vsys-name*} [**weight** *value*] [**track** *track-object-name*]

- **id** *rule-id* – 指定新建策略规则的 ID，取值范围为 1 到 255。如果不指定，系统将会为 PBR 规则自动分配一个 ID。规则 ID 在该PBR 策略中必须是唯一的。
- **before** *rule-id* | **after** *rule-id* | **top** – 指定 PBR 规则的位置，可以是某个规则之前（**before** *rule-id*）、某个规则之后（**after** *rule-id*）或者所有规则的首位（**top**）。默认情况下，系统会将新创建的策略规则放到所有规则的末尾。
- *src-addr* – 指定源地址，该地址为地址簿条目。
- *dst-addr* – 指定目的地址，该地址为地址簿条目。
- *service-name* – 指定服务名称。*service-name* 为服务簿中定义的服务。
- *application-name* – 指定应用名称。*application-name* 为应用簿中定义的应用。
- **nexthop** {*interface-name* | *A.B.C.D* | **vrouter** *vrouter-name* | **vsys** *vsys-name*} – 指定下一跳。interface-name 为出接口的名称，A.B.C.D 为下一跳的 IP 地址，vrouter vrouter-name 为 VRouter，**vsys** *vsys-name* 为虚拟系统。
- **weight** *value* – 指定下一跳的权重，取值范围是 1 到 255，默认值是 1。如果一条策略路由匹配多个下一跳，系统会按照权重值比例分配流量。
- **track** *track-object-name* – 指定下一跳的监测对象。如果监控对象失败，本条策略路由也会失败。关于如何配置监测对象，请参阅“系统管理“的“配置监测对象”部分。

使用该命令 no 的形式删除指定 ID 的规则。在PBR 策略配置模式下，执行以下命令：

no match id *rule-id*

另外，用户还可以在 PBR 策略配置模式下使用以下命令，创建一个策略规则 ID，并且进入 PBR 策略规则配置模式，再进一步配置其它策略规则相关参数：

match [**id** *rule-id*] [**before** *rule-id* | **after** *rule-id* | **top**]

- **id** *id* – 指定 PBR 策略规则的 ID。如果不指定，系统将会为策略规则自动分配一个 ID。规则 ID 在整个系统中必须是唯一的。策略规则的 ID 大小并不表示策略规则的匹配先后顺序。
- **top** | **before** *rule-id* | **after** *rule-id* – 指定策略规则的位置，可以是某个规则 ID 之前（**before** *id*）、某个规则 ID 之后（**after** *id*）或者所有规则的首位（**top**）。默认情况下，系统会将新创建的策略规则放到所有规则的末尾。

注意:关于如何配置其它策略相关参数，请参考下一节“编辑 PBR 策略规则”。

编辑 PBR 策略规则

创建好的PBR 策略规则可以通过编辑来修改不合适的参数值，但是修改工作必须在 PBR 策略规则配置模式下才可以进行。在 CLI 中进入 PBR 策略规则配置模式，请输入以下命令：

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

进入PBR 策略规则配置模式后，可使用的编辑策略规则的命令如下：

- 添加地址簿条目类型源地址：**src-addr** *src-addr*
- 删除地址簿条目类型源地址：**no src-addr** *src-addr*
- 添加 IP 成员类型源地址：**src-ip** {*ip/netmask* | *ip-address netmask*}
- 删除 IP 成员类型源地址：**no src-ip** {*ip/netmask* | *ip-address netmask*}
- 添加主机成员类型源地址：**src-host** *host-name*
- 删除主机成员类型源地址：**no src-host** *host-name*
- 添加 IP 地址范围类型源地址：**src-range** *min-ip max-ip*
- 删除 IP 地址范围类型源地址：**no src-range** *min-ip max-ip*
- 添加地址簿条目类型目的地址：**dst-addr** *dst-addr*

- 删除地址簿条目类型目的地址：**no dst-addr** *dst-addr*
- 添加 IP 成员类型目的地址：**dst-ip** *ip/netmask*
- 删除 IP 成员类型目的地址：**no dst-ip** *ip/netmask*
- 添加主机成员类型目的地址：**dst-host***host-name*
- 删除主机成员类型目的地址：**no dst-host** *host-name*
- 添加 IP 地址范围类型目的地址：**dst-range** *min-ip* [*max-ip*]
- 删除 IP 地址范围类型目的地址：**no dst-range** *min-ip* [*max-ip*]
- 添加角色类型源用户：**role** *role-name*
- 删除角色类型源用户：**no role** *role-name*
- 添加用户类型源用户：**user** *aaa-server-nameuser-name*
- 删除用户类型源用户：**no user** *aaa-server-nameuser-name*
- 添加用户组类型源用户：**user-group** *aaa-server-nameuser-group-name*
- 删除用户组类型源用户：**no user-group** *aaa-server-name user-group-name*
- 添加服务类型：**service** *service-name*
- 删除服务类型：**no service** *service-name*
- 添加应用类型：**application** *application-name*
- 删除应用类型：**no application** *application-name*
- 指定下一跳：**nexthop** {*interface-name* | *A.B.C.D* | *vrouter-name* | **vsys** *vsys-name*}
- 取消下一跳配置：**no nexthop**
- 配置时间表：**schedule** *schedule-name*
- 删除时间表：**no schedule**
- 添加规则描述：**description** *string*
- 删除规则描述：**no description**
- 开启日志记录功能：**log enable**
- 关闭日志记录功能：**no log enable**

启用/禁用 PBR 策略规则

默认情况下，配置好的PBR 策略规则会在系统中立即生效。用户可以通过命令禁用某条策略规则，使其不对流量进行控制。禁用或者启用某条策略规则，在 PBR 策略规则配置模式下，使用以下命令：

- 禁用：**disable**
- 启用：**enable**

修改规则排列顺序

PBR 策略中的规则通过 ID 进行唯一标识。流量进入设备时，设备对 PBR 策略规则进行顺序查找，然后按照查找到的相匹配的第一条规则对流量进行处理。但是，PBR 策略规则 ID 的大小顺序并不是规则查找时的匹配顺序。使用 **show pbr-policy** 命令列出的规则顺序才是规则匹配顺序（系统将由上到下进行查找匹配）。用户在创建PBR 策略规则时可以指定该规则的排列位置，也可以在PBR 策略配置模式下修改其位置。PBR 策略规则的排列位置可以是绝对位置，即处在首位（Top）或者处在末位（Bottom），也可以是相对位置，即位于某个 ID 之前或之后。修改规则排列顺序，在 PBR 策略配置模式下使用以下命令：

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

配置目的路由优先查找

默认情况下，设备对进入的数据包进行转发时，按照这样的顺序选路：策略路由>源接口路由>源路由>目的路由，在某些情况下，用户需要使匹配 PBR 策略规则的数据包，转发时优先查找目的路由，即选路的顺序为：目的路由　策略路由。配置 PBR 策略规则的目的路由（DBR）优先查找，在 PBR 策略规则配置模式下，使用以下命令：

fib-lookup dbr-first

使用以上命令 no 的形式取消PBR 策略规则的目的路由（DBR）优先查找：**no fib-lookup dbr-first**

应用 PBR 策略

可以通过绑定PBR 策略到接口、安全域或者VRouter 来实现 PBR 策略的应用。在接口配置模式、安全域配置模式或 VRouter 配置模式下，使用以下命令：

bind pbr-policy *name*

- *name* – 绑定指定的PBR 策略到接口、安全域或者VRouter。

使用以上命令 no 的形式取消PBR 策略在接口、安全域或者 VRouter 的绑定：

no bind pbr-policy

配置 PBR 策略全局匹配顺序

默认情况下，如果接口和其所在安全域或者VRouter 绑定了 PBR 策略，流量匹配顺序为：接口->安全域->VRouter。用户可以根据需要自行配置 PBR 策略的全局匹配顺序，在全局配置模式下，使用以下命令：

pbr-match order *index*

- *index* – 为 PBR 策略指定全局匹配顺序的排序指数。包括 1-6，顺序分别表示如下：
  - 1 - 接口->安全域->Vrouter。该排序指数为默认值。
  - 2 - 安全域->接口 ->Vrouter。
  - 3 - Vrouter ->安全域->接口。
  - 4 - 接口-> Vrouter ->安全域。
  - 5 - Vrouter ->接口->安全域。
  - 6 - 安全域-> Vrouter->接口。

使用 **no pbr-match** 恢复默认匹配顺序配置。

显示 PBR 策略全局匹配顺序

用户可以在任何模式下，通过 show 命令查看PBR 策略规则的全局匹配顺序信息。具体命令以下：

show pbr-match order

策略路由规则支持配置 TTL

用户可以在 PBR 规则中配置报文的 TTL，符合条件的报文将被设备转发到特定的出口链路。配置 TTL，请先执行以下命令进入PBR 策略规则配置模式：

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

在 PBR 策略规则配置模式下，输入以下命令：

ttl-range *min-ttl max-ttl*

- *min-ttl max-ttl* – 指定策略路由规则中报文的生存时间范围。*min-ttl* 指定生存时间的最小值，取值范围为 1 到 255；*max-ttl* 指定生存时间的最大值，取值范围为 1 到 255。

在 PBR 策略规则配置模式下，执行 **no ttl-range** 命令取消 TTL 范围的配置。

查看 PBR 策略规则信息

用户可以在任何模式下，通过 show 命令查看PBR 策略规则的具体信息。具体命令以下：

show pbr-policy [*name*]

- *name* – 显示指定PBR 策略的详细信息。如果不指定名称则显示所有PBR 策略的详细信息。

动态路由

动态路由是根据网络系统的运行情况而自动调整的路由。 设备根据路由协议自动调整动态路由表。StoneOS 支持 RIP、OSPF、IS-IS 和 BGP 四种动态路由协议。

配置 RIP

RIP（Routing Information Protocol）是路由信息协议。它是一种在路由器之间交换路由信息的内部网关路由协议。目前，RIP 有 RIP-1 和 RIP-2 两个版本，设备均支持。

对 RIP 协议的配置包括基本配置、引入路由、被动接口、邻居、网络和距离。另外，RIP 参数配置完成后，用户还需要在不同的接口上配置 RIP 参数，包括指定接口接收和发送更新的 RIP 版本号、水平分割以及接口的 RIP 认证。

基本配置

RIP 协议的基本配置包括指定 RIP 版本号、指定缺省度量、指定缺省距离、配置缺省信息发布以及配置定时器（时间间隔、失效时间、保持时间和清除时间）。用户可以为不同的VRouter 分别配置 RIP 协议。对 RIP 协议的基本配置需要在 RIP 路由模式下进行。进入 RIP 路由模式，请在全局配置模式下，使用以下命令：

ip vrouter *vrouter-name* （进入VRouter 配置模式）

router rip（进入 RIP 路由模式，同时开启设备的 RIP 功能）

在 VRouter 配置模式下，使用 **no router rip** 关闭 RIP 功能。

指定版本号

设备支持 RIP-1 和 RIP-2 两个版本。RIP-1 以广播方式传输报文；而 RIP-2 使用组播方式。指定 RIP 协议版本号，在 RIP 路由模式使用以下命令：

version *version-number*

- *version-number* – 指定版本号，1（RIP-1）或者 2（RIP-2）。默认为 2。

使用 **no version** 命令恢复默认版本配置。

指定缺省度量

RIP 协议使用跳数来衡量到达目的网络的距离，称为度量。路由器到与它直接相连网络的度量为 1，通过一个路由器可达的网络的度量为 2，依此类推，度量的最大值可以到 15，度量大于 15 的网络为不可达网络。缺省度量在引入路由时生效。指定 RIP 的缺省度量，在 RIP 路由配置模式下使用以下命令：

default-metric *value*

- *value* – 指定缺省度量值。范围是 1 到 15，默认值是 1。

使用 **no default-metric** 命令恢复缺省度量值。

指定缺省距离

指定 RIP 路由的缺省距离，在 RIP 路由配置模式下使用以下命令：

distance *distance-value*

使用 **no distance** 命令恢复缺省距离值。

配置缺省信息发布

用户可以指定是否默认路由发布到其它使用 RIP 协议的路由器。默认情况下，RIP 协议不发送默认路由。配置缺省信息发布，在 RIP 路由配置模式下使用以下命令：

发送：**default-information originate**

不发送：**no default-information originate**

配置定时器

RIP 可配置的定时器分别是时间间隔（Interval）、失效时间（Invalid）、保持时间（Holddown）和清除时间（Flush）。具体描述如下：

- 时间间隔：每次向所有邻居发送全部 RIP 路由所间隔的时间。默认是 30 秒。
- 失效时间：如果一条路由在失效时间内一直没有被更新，该路由的度量就会被标记为 16，表示为不可达路由。默认的失效时间是 180 秒。
- 保持时间：如果一条更新后的路由的度量变大，例如，从 2 更新到 4，该路由会被赋予一个保持时间，路由在保持时间内，不接受任何更新。默认的保持时间是 180 秒。
- 清除时间：度量被标记为 16 的不可达路由会一直被发布到其它 RIP 协议路由，直到清除时间结束；如果该路由仍没有被更新，清除时间结束后，将会被从 RIP 路由信息数据库中删除。默认的清除时间是 240 秒。

用户可以修改以上四个定时器的时间值。配置定时器，在 RIP 路由配置模式下使用以下命令：

timers basic *interval-time invalid-time holddown-time flush-time*

- *interval-time* – 指定发送更新的时间间隔，单位为秒。范围是 0 到 16777215 秒。默认值是 30 秒。
- *invalid-time* – 指定路由的失效时间，单位为秒。范围是 1 到 16777215 秒。默认值是 180 秒。
- *holddown-time* – 指定路由的保持时间，单位为秒。范围是 1 到 16777215 秒。默认值是 180 秒。
- *flush-time* – 指定路由的清除时间，单位为秒。范围是 1 到 16777215 秒。默认值是 240 秒。

使用 **no timers basic** 命令恢复定时器的默认值。

引入路由

RIP 协议允许用户将设备上其它路由协议（BGP、直连、静态和 OSPF）的路由信息引入到 RIP 中，并向外发布。同时，用户可以设置被引入路由的度量。配置引入路由，在 RIP 路由配置模式下使用以下命令：

redistribute {**bgp** | **connected** | **static** | **ospf**} [**metric** *value*]

- **bgp** | **connected** | **static** | **ospf** – 指定引入路由的类型，可以是 BGP（**bgp**）、直连路由（**connected**）、静态路由（**static**）或者 OSPF（**ospf**）。
- **metric** *value* – 指定引入路由的度量。范围是 1 到 15。如果不指定该数值，系统会使用 RIP 的缺省度量（通过 **default-metric** *value* 配置）。

用户可以配置多条该命令引入不同类型的路由。

使用 **no redistribute** {**bgp** | **connected** | **static** | **ospf**}命令取消指定类型路由的引入。

配置被动接口

用户可以将一些接口配置为只接收更新但是不发送，这种只接收更新的接口就是被动接口。配置被动接口，在 RIP 路由配置模式下使用以下命令：

passive-interface *interface-name*

- *interface-name* – 指定接口的名称作为被动接口。

用户可以配置多条该命令添加多个被动接口。

使用 **no passive-interface** *interface-name* 命令取消被动接口的配置。

配置邻居

用户可以指定一些邻居，使邻居和设备之间能够允许点到点（非广播）的 RIP 信息交换。指定邻居，在 RIP 路由配置模式下使用以下命令：

neighbor *ip-address*

- *ip-address* – 指定邻居的 IP 地址。

用户可以配置多条该命令添加多个邻居。

使用 **no neighbor** *ip-address* 命令删除指定的邻居。

配置网络

用户需要配置一些网络，只有在指定网络中的接口才能接收和发送 RIP 更新。配置网络，在 RIP 路由配置模式下使用以下命令：

network *ip-address/netmask*

- *ip-address/netmask* – 指定网络的 IP 地址，例如 10.200.0.0/16。

用户可以配置多条该命令添加多个网络。

使用 **no network** *ip-address/netmask* 命令删除指定的网络。

配置距离

用户可以为从一些指定网络得到的路由指定管理距离。配置距离，在 RIP 路由配置模式下使用以下命令：

distance *distance-value ip-address/netmask*

- *distance-value* – 指定管理距离。范围是 1 到 255。用该命令指定的距离优先级高于 RIP 基本配置中的缺省距离（通过 distance distance-value 指定）。
- *ip-address/netmask* – 指定网络的 IP 地址，例如 10.200.0.0/16。

用户可以配置多条该命令为从不同的网络更新的路由指定距离。

使用 **no distance** *ip-address/netmask* 命令删除指定的管理距离。

RIP 数据库

设备运行 RIP 协议，就拥有一个 RIP 路由数据库，该数据库中储存了所有可达目的网络的路由条目。路由条目包含的信息有目的地址、下一跳、度量、来源以及定时器信息。用户可以在任何模式下，通过以下命令，随时查看 RIP 数据库的信息：

show ip rip database [*A.B.C.D/M*] [**vrouter** *vrouter-name*]

- *A.B.C.D/M* – 显示指定目的 IP 地址的 RIP 信息。
- **vrouter** *vrouter-name* – 显示指定 VRouter 的 RIP 信息。StoneOS 目前只支持trust-vr 一个 VRouter。

配置接口的 RIP 功能

RIP 功能在设备接口上的配置包括：认证方式、发送和接收的 RIP 版本号以及水分割功能。接口的 RIP 功能配置需要在接口配置模式下完成。

配置 RIP 报文认证

只有 RIP-2 支持 RIP 报文认证。认证方式有两种，分别是明文认证和 MD5 密文认证。明文认证不能提供安全保障。未加密的认证字随 RIP 报文一同传送，所以明文认证不能用于安全性要求较高的情况。默认为明文认证。用户需要配置 RIP 报文的认证方式和认证码。在接口配置模式下，使用以下命令：

- 方式：**ip rip authentication mode {md5 | text}**
- 认证码：**ip rip authentication string** *string*

使用以上两个命令 no 的形式可以取消对认证方式和认证码的指定：

- **no ip rip authentication mode**
- **no ip rip authentication string**

配置发送和接收的 RIP 版本号

默认情况下，接口发送 RIP-2 信息。指定接口发送 RIP 信息的版本号，在接口配置模式下，使用以下命令：

ip rip send version [1][2]

- **1** – 指定只发送 RIP-1 的 RIP 信息。
- **2** – 指定只发送 RIP-2 的 RIP 信息。

使用 **no ip rip send version** 命令恢复默认版本号。

默认情况下，接口接收 RIP-2 信息。指定接口接收 RIP 信息的版本号，在接口配置模式下，使用以下命令：

ip rip receive version [1][2]

- **1** – 指定只发送 RIP-1 的 RIP 信息。
- **2** – 指定只发送 RIP-2 的 RIP 信息。

使用 **no ip rip receive version** 命令恢复默认版本号。

配置水平分割

水平分割是指不从本接口发送从该接口学到的路由。它可以在一定程度上避免产生路由环，保证路由的正确传播。配置水平分割功能，在接口配置模式下，使用以下命令：

开启水平分割：**ip rip split-horizon**

关闭水平分割：**no ip rip split-horizon**

显示系统 RIP 信息

用户可以通过 show 命令随时查看系统的 RIP 信息。查看 RIP 信息，在任何模式下使用以下命令：

show ip rip

配置 OSPF

OSPF 是开放式最短路径优先协议（Open Shortest Path First）的缩写。它是 IETF 组织开发的一个基于链路状态的内部网关协议。当前的OSPF 版本为版本 2（RFC2328）。OSPF 适应各种规模的网络，快速收敛特性能够在网络拓扑结构发生变化后立即发送更新报文，并且其算法本身决定了不会生成路由环路。OSPF 还具有以下特性：

- 区域划分：将自治系统的网络划分成区域来管理，从而减少了协议对 CPU 和内存的占用，提高性能。
- 无类路由：无类路由特性允许可变长子网掩码的使用。
- 等价路由：支持等价路由，提高多条路由的利用率。
- 组播发送：支持组播地址发送，减少对非 OSPF 设备的影响。
- 支持验证：支持基于接口的报文验证以保证路由计算的安全性。

{b}提示: {/b}“自治系统”是处于一个管理机构控制之下的路由器和网络群组。一个自治系统中的所有路由器必须运行相同的路由协议。

OSPF 协议配置

用户可以为不同的VRouter 分别配置OSPF 协议。OSPF 协议配置包括以下各项：

- 配置 Router ID
- 配置区域认证
- 配置接口的网络类型
- 配置区域的路由聚合

- 配置区域的缺省花费
- 配置区域的虚拟链路
- 配置 stub 区域
- 配置 NSSA 区域
- 配置接口发送OSPF 报文的缺省花费
- 配置缺省度量
- 配置缺省信息发布
- 配置缺省距离
- 配 置 OSPF 定时器
- 指定运行OSPF 协议的接口网络
- 引入路由
- 配置路由映射表
- 匹配多条路由匹配规则
- 修改引入路由属性
- 配置路由访问控制列表
- 配置距离
- 配置被动接口

OSPF 协议的基本配置需要在OSPF 路由模式下进行。进入OSPF 路由模式，请在VRouter 配置模式下，使用以下命令：

ip vrouter *vrouter-name*（进入 VRouter 配置模式）

router ospf [*process-id*]（进入 OSPF 路由模式，同时开启设备的 OSPF 功能）

- *process-id* – 指定 OSPF 的进程 ID。默认值是 1，取值范围是 1 到 65535。每个 OSPF 进程相互独立，有各自的链路状态数据库和对应的OSPF 路由表信息。每一个 VRouter 支持最多 4 个 OSPF 进程，多个进程共同维护一个 VRouter 的路由表。

在指定 OSPF 进程 ID 时，注意如下事项：

- 每个OSPF 进程中运行OSPF 协议的接口网络不能重叠。

- 当多个 OSPF 进程中存在相同前缀的路由条目时，首先比较比较各个路由条目的管理距离，管理距离低的将被优先加入到VRouter 的路由表中；管理距离相同时，，优先发现的的路由条目将被加入到 VRouter 的路由表中。
- 当其他路由协议引入OSPF 路由时，将默认引入进程 ID 为 1 的 OSPF 路由信息。如果此进程不存在，将无法引入OSPF 路由。

在 VRouter 配置模式下，使用 **no router ospf** [*process-id*]关闭 OSPF 功能。

配置 Router ID

每一台运行 OSPF 协议的路由器都必须拥有一个 Router ID。Router ID 是每个路由器在整个OSPF 域中唯一标识，使用 IP 地址的形式表示。为设备的OSPF 协议配置 Router ID，在 OSPF 路由模式下，使用以下命令：

router-id *A.B.C.D* [**local**]

- *A.B.C.D* – 指定OSPF 协议使用的 Router ID，为 IP 地址形式。
- **local** - 指定OSPF 协议的Router ID 为本地配置，该配置适用于 HA A/A 工作模式，并且不进行 HA 配置同步。默认情况下，Router ID 为非本地配置。

配置区域认证

用户可以配置区域的认证方式。默认情况下，区域是没有认证方式的。配置区域的认证方式，在 OSPF 路由模式下，使用以下命令：

area {*id* | *A.B.C.D*} **authentication** [**message-digest**]

- *id* | *A.B.C.D* – 指定区域 ID。区域 ID 用 32 比特数来表示，可以是数字形式，也可以是 IP 地址形式。
- [**message-digest**] – 指定使用 MD5 认证方式。如果不使用该关键字，则为明文认证。

用该命令指定的认证类型必须与区域内其它的路由相同。同一网络中通过OSPF 协议通信的路由器的认证密码必须相同。

使用 **no area** {*id* | *A.B.C.D*} **authentication** 命令取消对认证方式的指定。

配置接口的网络类型

OSPF 协议的接口的网路类型有以下三种：广播、点到点（Point-to-point）以及点到多点（Point-to-multipoint）网络类型。默认情况下，接口的网络类型为广播类型。配置接口的网络类型，在接口配置模式下，使用以下命令：

ip ospf network {**point-to-point** | **point-to-multipoint**}

- point-to-point – 指定接口网络类型为点到点网络类型。
- point-to-multipoint -指定接口网络类型为点到多点网络类型。

在隧道接口配置模式下，使用该命令 no 的形式恢复接口网络类型为广播类型:

no ip ospf network

配置区域的路由聚合

路由聚合是指将具有相同前缀的路由信息通过 ABR 聚合在一起，只发布一条路由到其它区域。一个区域可以配置多条聚合网段，这样OSPF 可以对多个网段进行聚合。默认情况下，区域的路由聚合功能是关闭的。配置区域的路由聚合，在OSPF 路由模式下，使用以下命令:

area {*id* | *A.B.C.D*} range {*A.B.C.D/M*} [advertise | not-advertise]

- *id* | *A.B.C.D* – 指定需要进行路由聚合的区域 ID。区域 ID 用 32 比特数来表示，可以是数字形式，也可以是 IP 地址形式。
- range {*A.B.C.D/M*} – 指定被聚合的网段。
- advertise – 指定将这一网段的路由聚合并通告聚合后的路由。
- not-advertise – 指定将这一网段的路由聚合且不通告聚合后的路由。

路由聚合功能仅对区域边界路由（连接骨干区域和非骨干区域的路由器，简称为ABR）有效。

使用 no area {*id* | *A.B.C.D*} range {*A.B.C.D/M*} [advertise | not-advertise]命令取消路由聚合的配置。

配置区域的缺省花费

区域的缺省花费是指将报文发送到 stub 区域的缺省路由花费。指定区域的缺省花费，在OSPF 路由模式下，使用以下命令:

area {*id* | *A.B.C.D*} default-cost *cost-value*

- *id* | *A.B.C.D* – 指定需要指定缺省花费的区域 ID。区域 ID 用 32 比特数来表示，可以是数字形式，也可以是 IP 地址形式。
- *cost-value* – 指定花费值。默认值是 1。范围是 0 到 16777214。

使用 no area {*id* | *A.B.C.D*} default-cost 命令恢复缺省花费的配置。

注意:该命令仅对 NSSA 区域有效。

配置区域的虚拟链路

虚拟链路（Virtual Links）用来连接不连续的骨干区域，使他们能够保持逻辑上的连续性。配置虚拟链路以及定时器参数，在OSPF 路由模式下，使用以下命令：

area {*id* | *A.B.C.D*} **virtual-link** *A.B.C.D* [**hello-interval** *interval-value*] [**retransmit-interval** *interval-value*] [**transmit-delay** *interval-value*] [**dead-interval** *interval-value*]

- *id* | *A.B.C.D* – 需要做虚拟链路进行连接的区域 ID。区域 ID 用 32 比特数来表示，可以是数字形式，也可以是 IP 地址形式。
- **virtual-link** *A.B.C.D* – 指定作为虚拟链路路由器的 Router ID。
- **hello-interval** *interval-value* – 指定接口发送Hello 报文的时间间隔，单位为秒，默认值是 10 秒。范围是 1 到 65535 秒。
- **retransmit-interval** *interval-value* – 一台路由器向它的邻居发送一条 LSA 后需要获得对方的确认报文。若在指定的时间内没有收到对方的确认报文，就会向邻居重传这条 LSA。该参数用来指定邻接路由器之间重传LSA 的时间间隔，单位为秒，默认值是 5 秒。范围是 3 到 65535 秒。
- **transmit-delay** *interval-value* – 指定更新包的延迟时间，单位为秒，默认值是 1 秒。范围是 1 到 65536 秒。
- **dead-interval** *interval-value* – 如果路由器在一定的时间内都没有收到对方的 Hello 报文，则认为对端路由器失效，这个一定的时间就是相邻路由器间的失效时间。该参数指定失效时间值，单位为秒，默认值是 40 秒。范围是 1 到 655635 秒。

使用 **no area** {*id* | *A.B.C.D*} **virtual-link** *A.B.C.D* [**hello-interval**] [**retransmit-interval**] [**transmit-delay**] [**dead-interval**]命令恢复定时器的默认时间值。

用户可以配置虚拟链路的认证方式。在OSPF 路由模式下，使用以下命令：

area {*id* | *A.B.C.D*} **virtual-link** *A.B.C.D* **authentication** [**message-digest**] [**authentication-key** *string*] [**message-digest-key** *ID* **md5** *string*] [**null**]

- *id* | *A.B.C.D* – 需要做虚拟链路进行连接的区域 ID。区域 ID 用 32 比特数来表示，可以是数字形式，也可以是 IP 地址形式。
- **virtual-link** *A.B.C.D* – 指定作为虚拟链路路由器的 Router ID。
- **message-digest** – 指定使用 MD5 认证。
- **authentication-key** *string* – 指定明文认证的认证密码。
- **message-digest-key** *ID* **md5** *string* – 指定 MD5 认证的认证 ID 和密码。
- **null** – 不使用认证。

使用 **no area** {*id* | *A.B.C.D*} **virtual-link** *A.B.C.D* **authentication** [**message-digest**] [**authentication-key** *string*] [**message-digest-key** *ID*]命令取消认证配置。

配置 stub 区域

stub 区域是不收发Type-5 的 LSA（AS-external-LSAs）区域。对于产生大量 Type-5 LSA 的网络，这种处理方式能够有效减小 stub 区域内路由器的 LSDB 规模，并缓解 SPF 计算对路由器资源的占用。stub 区域通常位于自治系统边界。配置 OSPF 的 stub 区域，在OSPF 路由模式下，使用以下命令：

area {*id* | *A.B.C.D*} **stub** [**no-summary**]

- *id* | *A.B.C.D* – 指定 stub 区域的区域 ID。区域 ID 用 32 比特数来表示，可以是数字形式，也可以是 IP 地址形式。
- **no-summary** – 阻止 ABR 向 stub 区域发送 3 类或 4 类汇总 LSA。使

用 **no area** {*id* | *A.B.C.D*} **stub** [**no-summary**]命令取消 stub 区域的配置。

配置 NSSA 区域

Stub 区域不能引入外部路由，为了在允许将自治系统外部路由通告到OSPF 路由域内部的同时，保持其余部分的 Stub 区域的特征，网络管理员可以将区域配置为 NSSA 区域。配置OSPF 的 NSSA 区域，在OSPF 路由模式下，使用以下命令：

area {*id* | *A.B.C.D*} **nssa** [**no-summary** | **no-redistribution** | **default-information-originate**]

- *id* / *A.B.C.D* – 指定 NSSA 区域的区域 ID。区域 ID 用 32 比特数来表示，可以是数字形式，也可以是 IP 地址形式。
- **no-summary** | **no-redistribution** | **default-information-originate** – **no-summary** 参数只用于 NSSA 区域的 ABR，配置后，NSSA ABR 只通过 Type-3 的 Summary-LSA 向区域内发布一条缺省路由，不再向区域内发布任何其它 Summary-LSAs（这种区域又称为 Totally NSSA 区域）。**no-redistribution** 参数用于禁止将 AS 外部路由以 Type-7 LSA 的形式引入到 NSSA 区域中，这个参数通常只用在既是 NSSA 区域的ABR，也是 OSPF 自治系统的ASBR 的路由器上，以保证所有外部路由信息能正确地进入OSPF 路由域。**default-information-originate** 参数只用于 NSSA 区域的ABR 或 ASBR，配置后，对于ABR，不论本地是否存在缺省路由，都将生成一条 Type-7 LSA 向区域内发布缺省路由；对于 ASBR，只有当本地存在缺省路由时，才产生 Type-7 LSA 向区域内发布缺省路由。

使用 **no area** {*id* | *A.B.C.D*} **nssa** [**no-summary** | **no-redistribution** | **default-information-originate**]命令取消 NSSA 区域的配置。

配置 OSPF 的引用带宽

OSPF 可以根据接口的带宽计算接口发送OSPF 报文的花费。配置OSPF 的引用带宽，在 OSPF 路由模式下，使用以下命令：

auto-cost reference-bandwidth *bandwidth*

- *bandwidth* – 指定带宽值，单位为 Mbps，默认值是 100。范围是 1 到 4294967。

使用 no auto-cost reference-bandwidth 命令使OSFP 根据接口的类型计算接口发送OSPF 报文的花费。

指定缺省度量

此处配置的 OSPF 协议的缺省度量在引入路由时生效。指定OSPF 的缺省度量，在OSPF 路由配置模式下使用以下命令：

default-metric *value*

- *value* – 指定缺省度量值。范围是 1 到 16777214。

使用 no default-metric 命令恢复缺省度量的默认值。

配置缺省信息发布

用户可以指定是否将默认路由发布到其它使用 OSPF 协议的路由器。默认情况下，是不发送默认路由的。配置缺省信息发布，在OSPF 路由配置模式下使用以下命令：

default-information originate [always] [type {1 | 2}] [metric *value*]

- always – OSPF 无条件产生并发送默认路由。
- type {1 | 2} – 指定与发送到 OSPF 路由域的默认路由相关联的外部路由的类型。1 指 type1 外部路由，2 指 type2 外部路由。
- metric *value* – 指定发送默认路由的度量。如果不使用该命令配置度量并且也没有使用 default-metric *value* 配置默认度量，其默认度量将会是 20。范围是 0 到 16777214。

使用 no default-information originate 命令恢复默认值。

指定缺省距离

指定OSPF 路由的缺省距离，在 OSPF 路由配置模式下使用以下命令：

distance *distance-value*

- *distance-value* – 指定缺省管理距离。范围是 1 到 255，默认值是 110。

使用 no distance 命令恢复缺省距离的默认值。

配置 OSPF 定时器

用户可以指定以下两个OSPF 协议的定时器：OSPF 收到更新后在多长时间内进行重新计算以及OSPF 两次计算的时间间隔。配置OSPF 定时器，在OSPF 路由配置模式下使用以下命令：

timers spf *delay1 delay2*

- *delay1* – 收到更新后，在该指定时间内进行重新计算，单位为秒。范围是 0 到 65535，默认值是 5 秒。
- *delay2* – 指定两次计算的时间间隔，单位为秒。范围是 0 到 65535，默认值是 10 秒。

使用 **no timers spf** 命令恢复默认值。

指定运行 OSPF 协议的接口网络

指定运行OSPF 协议的接口网络并且将网络配置到指定的区域中，在OSPF 路由配置模式下使用以下命令：

network *A.B.C.D/M* **area** {*id* | *A.B.C.D*}

- *A.B.C.D/M* – 指定运行OSPF 协议的接口网络。
- **area** {*id* | *A.B.C.D*} – 指定将网络添加到的区域 ID。区域 ID 用 32 比特数来表示，可以是数字形式，也可以是 IP 地址形式。

使用 **no network** *A.B.C.D/M* **area** {*id* | *A.B.C.D*}命令取消对网络的指定。

引入路由

OSPF 协议允许用户引入其他OSPF 进程路由信息以及其它路由协议（BGP、IS-IS、直连、静态、RIP 和 VPN）的路由信息，并向外发布。用户可以设置被引入路由的度量以及外部路由的类型，还可以引用路由映射表对路由信息进行过滤，仅允许引入或拒绝引入特定的路由信息。配置引入路由，在OSPF 路由配置模式下使用以下命令：

redistribute {**bgp** | **connected** | **isis** | **ospf** *process-id* | **static** | **rip** | **vpn**} [**type** {**1** | **2**}] [**metric** *value*] [**route-map** *name*] [**tag** *tag-value*]

- **bgp** | **connected** | **isis** | **ospf** *process-id* | **static** | **rip** | **vpn** – 指定引入路由的类型，可以是 BGP（**bgp**）、ISIS(**isis**)、指定的 OSPF 进程（**ospf** *process-id*）、直连路由（**connected**）、静态路由（**static**）、RIP（**rip**）或者 VPN 路由（**vpn**）。
- **type** {**1** | **2**} – 指定外部路由的类型。1 指 type1 外部路由，2 指 type2 外部路由。
- **metric** *value* – 指定引入路由的度量。范围是 0 到 16777214。如果不指定该数值，系统会使用OSPF 的缺省度量（通过 **default-metric** *value* 配置）。

- **route-map** *name* – 指定用于过滤引入路由信息的路由映射表。有关路由映射表的更多信息，请参考“配置路由映射表”。
- **tag** *tag-value* – 指定引入的路由的标记值。取值范围是 1 到 4294967295。

用户可以配置多条该命令引入不同类型的路由。

使用 **no redistribute** {**bgp** | **connected** | **static** | **rip**}命令取消指定类型路由的引入。

配置路由映射表

默认情况下系统会引入所有的路由信息。用户可以引用路由映射表对引入的路由信息进行过滤。路由映射表主要由路由匹配规则和匹配成功后所执行操作（允许或拒绝）两部分组成。如果引入的路由信息命中了任何路由匹配规则，系统就会执行对应的操作，允许或拒绝引入这些路由信息。

注意:

- 如果用户设置的操作是允许，匹配成功后系统仅允许引入匹配的路由信息，拒绝引入所有未匹配的路由信息。
- 如果用户设置的操作是拒绝，匹配成功后系统会拒绝引入匹配的路由信息，但仍允许引入未匹配的路由信息。

用户可通过以下步骤配置路由映射表，实现对引入路由信息的过滤:

1. 创建路由映射表并在表中创建路由匹配规则。不同的匹配规则通过序列号区分。序列号越小，匹配优先级越高。默认情况下，引入的路由信息命中任何路由匹配规则，系统将不再继续匹配后续的规则；如果引入的路由信息没有命中任何匹配规则，系统将执行拒绝操作。
2. 在路由匹配规则中配置匹配条件。匹配条件可以是引入路由的度量值、目的地址、下一跳地址或下一跳接口。一条路由匹配规则中可以包含多个匹配条件，这些匹配条件之间是与（AND）关系，即引入的路由信息必须满足匹配规则中的所有匹配条件才会认定为命中了该条规则。
3. 如果匹配条件为路由的目的地址或下一条地址，配置匹配时所引用的路由访问控制列表。有关路由访问控制列表的更多信息，请参考“配置路由访问控制列表”。
4. 如有需要，设置系统在命中一条路由匹配规则后继续匹配其他规则。
5. 如有需要，修改引入路由的部分属性后再对外发布。

创建路由映射表并在表中配置路由匹配规则，在全局配置模式下，使用以下命令:

route-map *name* {**deny** | **permit**} *sequence*

- **route-map** *name* – 指定路由映射表名称，并进入路由映射表配置模式。取值范围是 1 到 31 个字符。如果该名称已经存在，则直接进入路由映射表配置模式。
- **deny** | **permit** – 指定对匹配的路由信息所执行的操作。deny 为拒绝，permit 为允许。

- *sequence* – 指定该路由映射表下路由匹配规则的序列号。取值范围是 1 到 65535。

使用该命令 no 的形式删除路由映射表:

no route-map *name* [*sequence*]

- *sequence* – 仅删除路由映射表中指定的匹配规则。

配置路由匹配规则中的匹配条件，在路由映射表配置模式下，使用以下命令:

match {**as-path** *access-list-number* | **community** {*community-list-name* | *community-list-number*} [*exact-match*] | **metric** *metric-value* | **interface** *interface-name* | **ip address** *access-list* | **ip next-hop** *access-list* | **tag** *tag-value* }

- **as-path** *access-list-number* – 匹配路由的AS 路径。access-list-number 为用户配置的AS 路径访问控制列表号。如果路由的 AS 路径匹配该访问控制列表中允许的 AS 路径，则认为匹配成功。有关AS 路径访问控制列表配置的更多信息，请参考“配置 AS 路径访问控制列表”。
- **community** {*community-list-name* | *community-list-number*} [*exact-match*] – 匹配路由的团体属性。*community-list-name* 为团体属性列表名称；*community-list-number* 为团体属性列表号；*exact-match* 指定对团体属性进行精确匹配。有关团体属性列表列表配置的更多信息，请参考“配置团体属性列表”。
- **metric** *metric-value* – 匹配路由的度量值。取值范围是 0 到 4294967295。
- **interface** *interface-name* – 匹配路由的下一跳接口。
- **ip address** *access-list* – 匹配路由的目的地址。access-list 为用户配置的路由访问控制列表。如果路由的目的地址属于该访问控制列表中允许的地址，则认为匹配成功。有关访问控制列表配置的更多信息，请参考“配置路由访问控制列表”。
- **ip next-hop** *access-list* – 匹配路由的下一跳地址。*access-list* 为用户配置的路由访问控制列表。如果路由的下一跳地址属于该访问控制列表中允许的地址，则认为匹配成功。有关访问控制列表配置的更多信息，请参考“配置路由访问控制列表”。
- **tag** *tag-value* – 匹配 OSPF 协议的路由的标记值。如果此处配置的路由的标记值匹配静态路由中的标记值，则认为匹配成功。取值范围是 1 到 4294967295。

重复以上命令向路由匹配规则中添加多个匹配条件。使用该命令 no 的形式删除匹配条件:

no match {**metric** | **interface** | **ip address** | **ip next-hop**}

注意:如果用户仅创建了路由映射表但没有在映射表中配置任何路由匹配规则，系统默认会认为引入的路由信息匹配成功。

例如，设置 OSPF 协议仅引入 BGP 协议中下一跳接口为eth0/1 且度量值为 50 的路由信息，命令行如下:

```
hostname(config)# route-map test permit 10
```

```
hostname(config-route-map)# match interface ethernet0/1
hostname(config-route-map)# match metric 50
hostname(config-route-map)# exit
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# router ospf
hostname(config-router)# redistribute bgp route-map test
hostname(config-router)# end
```

匹配多条路由匹配规则

默认情况下，如果引入的路由信息命中任何路由匹配规则，系统将不再继续匹配后续的规则。用户可以要求系统在命中一条规则后仍继续匹配其他规则，以实现更精细的控制。设置系统在匹配成功后继续匹配其他规则，在路由映射表配置模式下，使用以下命令：

continue [*sequence*]

- *sequence* – 指定继续匹配的规则序列号。取值范围是 1 到 65535。该序列号必须大于当前规则的序列号。如果没有指定此参数，系统在当前规则匹配成功后会继续匹配下一条规则。

使用该命令 no 的形式取消继续匹配其他规则：

no continue

例如，也可以通过以下命令行设置OSPF 协议仅引入 BGP 协议中下一跳接口为 eth0/1 且度量值为 50 的路由信息：

```
hostname(config)# route-map test permit 10
hostname(config-route-map)# match interface ethernet0/1
hostname(config-route-map)# continue 20
hostname(config-route-map)# exit
hostname(config)# route-map test permit 20
hostname(config-route-map)# match metric 50
hostname(config-route-map)# exit
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# router ospf
```

```
hostname(config-router)# redistribute bgp route-map test
hostname(config-router)# end
```

修改引入路由属性

对于满足匹配条件的引入路由，用户可以在修改路由的部分属性后再对外发布。修改引入路由的属性，在路由映射表配置模式下，使用以下命令：

set {**metric** *metric-value* | **metric-type** {**type-1** | **type-2**} | **tag** *tag-value*}

- **metric** *metric-value* – 修改引入路由的度量值。取值范围是取值范围是 0 到 4294967295。
- **metric-type** {**type-1** | **type-2**} – 修改外部路由的度量类型。**type-1** 指 type1 类型外部路由度量，**type-2** 指 type2 类型外部路由度量。
- **tag** *tag-value* – 指定 OSPF 协议的引入路由的标记值。取值范围是 1 到 4294967295。

使用该命令 no 的形式取消对路由属性的修改并还原到引入路由时的设置：

no set {**metric** | **metric-type** | **tag** }

配置路由访问控制列表

路由匹配规则中的目的地址和下一跳地址匹配是通过引用路由访问控制列表实现的。路由访问控制列表主要由 IP 地址匹配规则和匹配成功后所执行操作（允许或拒绝）两部分组成。如果目的地址或下一跳地址匹配指定的 IP 地址，系统会继续执行指定的操作。一个路由访问控制列表中可以包含多条 IP 地址匹配规则，系统按照添加时间顺序依次匹配，命中任何一条规则会立即结束匹配；如果匹配失败，系统会执行拒绝操作。

配置路由访问控制列表，在全局配置模式下，执行以下命令：

access-list route *name* {**deny** | **permit**} {*A.B.C.D/M* [**exact-match**] | **any**}

- *name* – 指定路由访问控制列表的名称并进入路由访问控制列表配置模式。取值范围是 1 到 31 个字符。如果该名称已经存在，则直接进入路由访问控制列表配置模式。
- **deny** | **permit** – 指定对匹配的 IP 地址所执行的操作。deny 为拒绝，permit 为允许。
- *A.B.C.D/M* – 指定需要匹配的 IP 地址或 IP 地址前缀（不包括掩码）。
- **exact-match** – 对 IP 地址前缀进行精确匹配（包括掩码）。
- **any** – 匹配任意 IP 地址。

使用该命令 no 的形式删除路由访问控制列表：

no access-list route *name* [{**deny** | **permit**} {*A.B.C.D/M* [**exact-match**] | **any**}]

如果指定了具体的 IP 地址匹配规则，该命令只从路由访问控制列表中删除对应的规则而不会删除整个访问控制列表。

对路由访问控制列表添加描述信息，在全局配置模式下，使用以下命令：

access-list route *name* **description** *description*

- *name* – 指定路由访问控制列表的名称。取值范围是 1 到 31 个字符。
- *description* – 指定描述信息。取值范围是 1 到 31 个字符。

使用该命令 no 的形式删除描述信息：

no access-list route *name* **description**

例如，设置 OSPF 协议拒绝引入 BGP 协议中下一跳地址为 192.168.1.1 和 192.168.2.0 网段中 IP 地址和的路由信息，命令行如下：

```
hostname(config)# route-map test deny 10
hostname(config-route-map)# match ip next-hop access_list
hostname(config-route-map)# exit
hostname(config)# access-list route access_list permit 192.168.1.1/32
hostname(config)# access-list route access_list permit 192.168.2.0/24
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# router ospf
hostname(config-router)# redistribute bgp route-map test
hostname(config-router)# end
```

配置距离

用户可以根据路由类型指定管理距离。配置距离，在 OSPF 路由配置模式下使用以下命令：

distance ospf {**intra-area** *distance-value* | **inter-area** *distance-value* | **external** *distance-value*}

- **intra-area** *distance-value* – 指定区域内路由的管理距离。默认值是 110。范围是 1 到 255。
- **inter-area** *distance-value* – 指定区域间路由的管理距离。默认值是 110。范围是 1 到 255。
- **external** *distance-value* – 指定外部type5 类型路由的管理距离。默认值是 110。范围是 1 到 255。

使用 no distance ospf 命令恢复距离的默认值。

配置被动接口

用户可以将一些接口配置为只接收更新但是不发送，这种只接收更新的接口就是被动接口。配置被动接口，在 OSPF 路由配置模式下使用以下命令：

passive-interface *interface-name*

- *interface-name* – 指定接口的名称作为被动接口。

用户可以配置多条该命令添加多个被动接口。

使用 **no passive-interface** *interface-name* 命令取消被动接口的配置。

配置基于路由访问控制列表的路由过滤

OSFP 协议支持通过路由访问控制列表对引入的路由进行过滤。配置基于路由访问控制列表的路由过滤，在 OSPF 路由配置模式下，使用以下命令：

distribute-list *access-list-name* **in** [*interface-name*]

- *access-list-name* – 指定路由访问控制列表的名称。关于路由访问控制列表的更多信息，请参考“配置路由访问控制列表”。
- **in** – 指定对引入的路由（**in**）进行过滤。
- *interface-name* – 指定接口名称。指定后，将过滤从指定接口学习到的OSPF 路由。如果不指定接口名称，系统将过滤所有OSPF 路由。

如果不指定接口名称，系统将过滤所有OSPF 路由。

使用该命令 no 的形式取消基于路由访问控制列表的路由过滤的配置：

no distribute-list *access-list-name* **in** [*interface-name*]

配置接口 OSPF 功能

接口的 OSPF 功能配置需要在接口配置模式下完成。OSPF 协议在设备接口上的配置包括：

- 配置接口的OSPF 认证
- 指定接口的链路花费
- 配置接口定时器
- 指定接口路由器优先级
- 配置接口的网络类型

配置接口的 OSPF 认证

接口的 OSPF 认证优先于区域OSPF 认证。 设备支持明文认证和 MD5 认证。默认情况下，接口的 OSFP 认证是关闭的。开启或者关闭接口的 OSPF 认证功能，在接口配置模式下使用以下命令:

ip ospf authentication

no ip ospf authentication

配置明文认证的认证密码，在接口配置模式下，使用以下命令:

ip ospf authentication-key *string*

- *string* – 指定认证密码（最多为 8 个字符）。

使用 **no ip ospf authentication-key** 命令取消密码配置。

配置 MD5 认证 ID 和密码，在接口配置模式下，使用以下命令:

ip ospf message-digest-key *ID* **md5** *string*

- *ID* – 指定认证 ID。
- *string* – 指定认证密码。

使用 **no ip ospf message-digest-key** *ID* 命令取消密码配置。

指定接口的链路花费

指定接口的链路花费，在接口配置模式下，使用以下命令:

ip ospf cost *cost-value* [**local**]

- *cost-value* – 指定接口的链路花费。取值范围是 1 到 65535。
- **local** – 指定接口的链路花费为 **local**。当设备处于 HA AA 模式时，配置此参数，该接口的链路花费值将不会同步到备份设备，从而使两台设备具有不同的链路花费值，避免出现非对称OSPF 路由。

使用 **no ip ospf cost** [**local**]命令取消对所需花费的指定。

配置接口定时器

接口的定时器有以下四个：接口发送 Hello 包的时间间隔、接口相邻路由器的失效时间、接口重传 LSA 的时间间隔以及接口更新包的延迟时间。

指定接口发送 Hello 包的时间间隔，在接口配置模式下，使用以下命令:

ip ospf hello-interval *interval*

- *interval* – 指定接口发送Hello 包的时间间隔，单位为秒。默认值是 10 秒。范围是 1 到 65535 秒。

使用 **no ip ospf hello-interval** 恢复默认时间间隔。

如果接口在一定的时间内都没有收到对方的 Hello 报文，则认为对端路由器失效，这个一定的时间就是相邻路由器间的失效时间。指定接口的相邻路由失效时间，在接口配置模式下，使用以下命令：

ip ospf dead-interval *interval*

- *interval* – 指定接口的相邻路由失效时间，单位为秒。默认值是 40 秒（发送 Hello 包时间间隔的 4 倍）。范围是 1 到 65535 秒。

使用 **no ip ospf dead-interval** 恢复默认失效时间。

指定接口重传 LSA 的时间间隔，在接口配置模式下，使用以下命令：

ip ospf retransmit-interval *interval*

- *interval* – 指定接口重传 LSA 的时间间隔，单位为秒。默认值是 5 秒。范围是 3 到 65535 秒。

使用 **no ip ospf retransmit-interval** 恢复默认时间间隔。

指定接口更新包的延迟时间，在接口配置模式下，使用以下命令：

ip ospf transmit-delay *interval*

- *interval* – 指定接口更新包的延迟时间，单位为秒。默认值是 1 秒。范围是 1 到 65535 秒。

使用 **no ip ospf transmit-delay** 恢复默认延迟时间。

指定接口路由器优先级

路由器的优先级用来决定使用哪个路由器作为指定路由器。指定路由器用来接收网络中所有其它路由器的链路信息，并将收到的链路信息广播出去。指定接口路由器的优先级，在接口配置模式下，使用以下命 令：

ip ospf priority *level*

- *level* – 指定路由器的优先级。默认值是 1。范围是 0 到 255。优先级为 0 的路由器不会被选中作为指定路由器。当同一个网络的两个路由器都可作为指定路由器时，优先级高的路由器会被选中；如果优先级也相同，Router ID 高的会被选中。

使用 **no ip ospf priority** 命令恢复默认优先级。

配置接口的网络类型

OSPF 协议的接口的网路类型有以下三种：广播、点到点（Point-to-point）以及点到多点（Point-to-multipoint）网络类型。默认情况下，接口的网络类型为广播类型。配置接口的网络类型，在接口配置模式下，使用以下命令：

ip ospf network {**point-to-point** | **point-to-multipoint**}

- **point-to-point** – 指定接口网络类型为点到点网络类型。
- **point-to-multipoint** -指定接口网络类型为点到多点网络类型。

在隧道接口配置模式下，使用该命令 no 的形式恢复接口网络类型为广播类型：

no ip ospf network

显示 OSPF 信息

显示OSPF 路由信息，在任何模式下使用以下命令：

show ip route ospf [**vrouter** *vrouter-name*]

- *vrouter-name* - 显示指定的VRouter 的 OSPF 路由信息。

显示防火墙的OSPF 信息，在任何模式下使用以下命令：

show ip ospf [**vrouter** *vrouter-name*] [**process** *process-id*]

- *vrouter-name* - 指定 VRouter 名称。
- **process** *process-id* – 指定 OSPF 进程 ID。

显示防火墙 OSPF 协议的数据库信息，在任何模式下使用以下命令：

show ip ospf database {**asbr-summary** | **external** | **nssa-external** | **network** | **router** | **summary**} [*A.B.C.D*] [{**adv-router** *A.B.C.D*} | **self-originate**] [**vrouter** *vrouter-name*] [**process** *process-id*]

- **asbr-summary** – 显示自制系统边界路由 LSAs。
- **external** – 显示外部路由 LSAs。
- **nssa-external** - 显示 NSSA 的外部 LSA 的有关信息。
- **network** – 显示网络 LSAs。
- **router** – 显示路由 LSAs。
- **summary** – 显示汇总 LSAs。

- *A.B.C.D* - 链路状态 ID，以 IP 地址形式表示。
- **adv-router** *A.B.C.D* – 显示指定路由器的 LSAs。
- **self-originate** - 只显示自己产生的 LSA（从本地路由器）。
- *vrouter-name* - 指定 VRouter 名称。
- **process** *process-id* – 指定 OSPF 进程 ID。

show ip ospf database [**max-age** | **self-originate**] [**vrouter** *vrouter-name*] [**process** *process-id*]

- **max-age** - 指定最大老化时间。
- **self-originate** - 只显示自己产生的 LSA（从本地路由器）。
- *vrouter-name* - 指定 VRouter 名称。
- **process** *process-id* – 指定 OSPF 进程 ID。

显示OSPF 接口信息，在任何模式下使用以下命令：

show ip ospf interface [*interface-name*] [**vrouter** *vrouter-name*] [**process** *process-id*]

显示OSPF 虚拟链路信息，在任何模式下使用以下命令：

show ip ospf virtual-links [**vrouter** *vrouter-name*] [**process** *process-id*]

显示OSPF 邻居信息，在任何模式下使用以下命令：

show ip ospf neighbor [*A.B.C.D* | **detail**] [**vrouter** *vrouter-name*] [**process** *process-id*]

显示OSPF 路由信息，在任何模式下使用以下命令：

show ip ospf route [*A.B.C.D*] [**vrouter** *vrouter-name*] [**process** *process-id*]

显示路由映射表信息，在任何模式使用以下命令：

show route-map [*name*]

显示路由访问控制列表信息，在任何模式使用以下命令：

show access-list route [*name*]

显示OSPF 路由过滤信息，在任何模式下使用以下命令：

show ip ospf distribute-list [**vrouter** *vrouter-name*] [**process** *process-id*]

等价多径路由（ECMP）

等价多径路由（ECMP）是对经过安全设备的数据流量在多条等价路径（同协议）上进行负载均衡转发的方法。

配置 ECMP 功能

默认情况下，系统的 ECMP 功能为开启状态，并允许最多 40 条等价路由条目进行负载均衡。在VRouter 配置模式下，使用以下命令开启或关闭ECMP 功能：

ecmp enable *ecmp-route-num*

- *ecmp-route-num* – 系统允许的最大ECMP 路由条目数。取值范围为 1 到 1000。当取值为 1 时表示不使用 ECMP 功能。

配置 ECMP 选路方式

在全局配置模式下，使用以下命令配置ECMP 选路方式：

ecmp-route-select {**by-5-tuple** | **by-src** | **by-src-and-dst**}

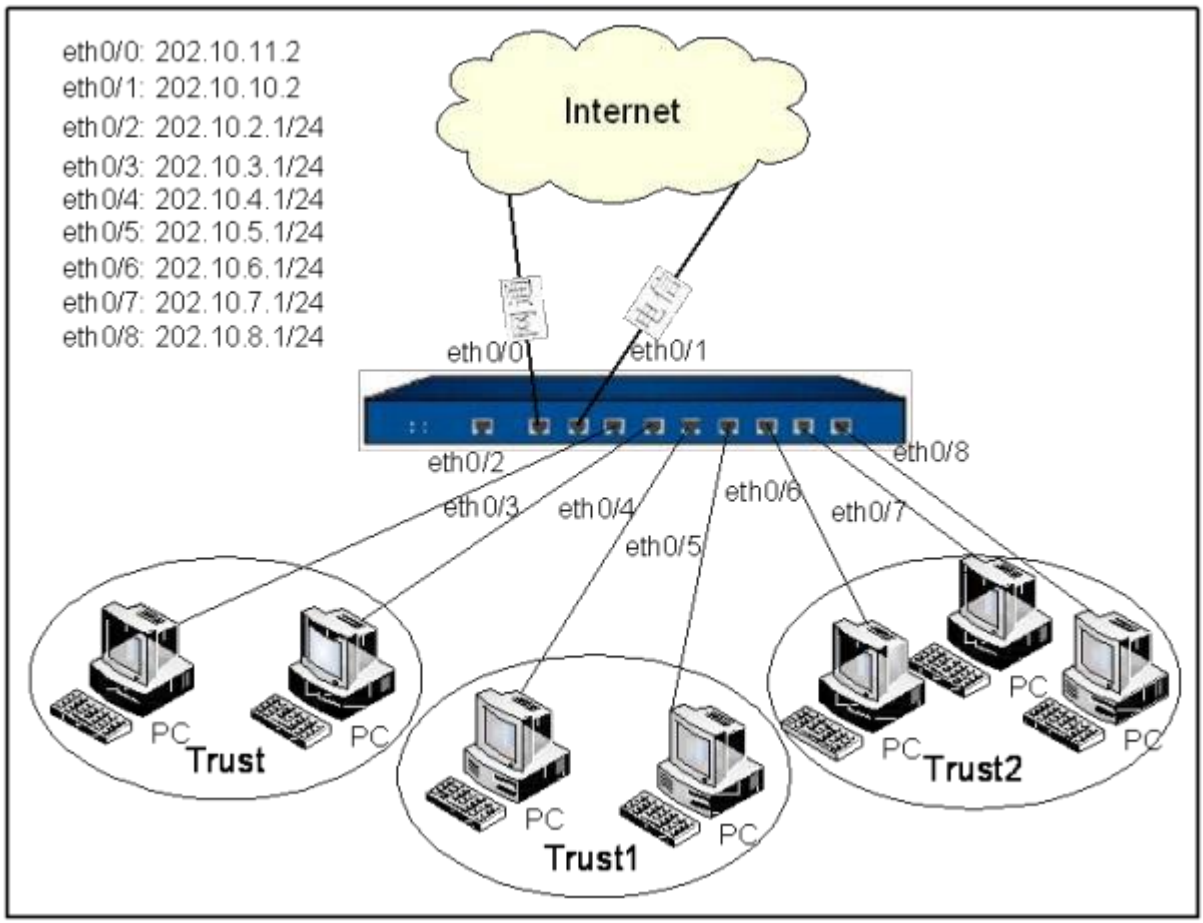
- **by-5-tuple** – 基于五元组（源 IP 地址、目的 IP 地址、源端口、目的端口和服务类型）进行选路。
- **by-src** – 基于源 IP 地址进行选路。
- **by-src-and-dst** - 基于源 IP 地址和目的 IP 地址进行选路。该方式为系统默认选路方式。

路由配置举例

本节介绍路由相关配置实例，包括开启/关闭静态路由查询功能配置举例、多VR 配置举例、静态组播路由配置举例、IGMP Proxy 配置举例和链路负载均衡配置举例。

开启/关闭静态路由查询功能配置举例

设备的 ethernet0/0 和 ethernet0/1 两个接口分别连接网通和电信的两条线路，内网中 Trust 域和 Trust1 域的流量走网通线路，其它的流量走电信线路。组网图如下图所示：



如上图所示，接口etherent0/0 和 ethernet0/1 属于 untrust 域，IP 地址分别是 202.10.11.2 和 202.10.10.2，接口 etherent0/2 和 ethernet0/3 属于 Ttrust 域，IP 地址分别是 202.10.2.1/24 和 202.10.3.1/24，接口 etherent0/4 和 ethernet0/5 属于 Ttrust1 域，IP 地址分别是 202.10.4.1/24 和 202.10.5.1/24，接口 etherent0/6、ethernet0/7 和 etherent0/8 属于 Ttrust2 域，IP 地址分别是 202.10.6.1/24、202.10.7.1/24 和 202.10.8.1/24。

配置步骤

以下配置步骤略去安全域以及接口配置，重点描述路由配置。路由配置:

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip route 0.0.0.0/0 202.10.10.2（默认流量走电信）
hostname(config-vrouter)# ip route source 202.10.2.1/24 202.10.11.2（该网段流量走网通）
hostname(config-vrouter)# ip route source 202.10.3.1/24 202.10.11.2（该网段流量走网通）
hostname(config-vrouter)# ip route source 202.10.4.1/24 202.10.11.2（该网段流量走网通）
hostname(config-vrouter)# ip route source 202.10.5.1/24 202.10.11.2（该网段流量走网通）
```

根据以上源路由配置，Trust 和 Trust1 域的流量都走网通线路，而其它的流量走电信线路。如果由于某些原因，网通线路故障，Trust 和 Trust1 域的用户将无法上网，此时需要将以上的四条源路由删除，流量才会全部汇总到电信线路进行传输。如果相关的源路由很多，删除工作和线路故障排除后的路由添加工作的工作量将十分庞大，同时也容易出错。现在的解决方案是：线路故障时，关闭源路由的查询，Trust 和 Trust1 域的用户就都可以走默认路由通过电信线路上网。配置命令如下：

```
hostname(config)# route disable sbr
```

```
hostname(config)# hostname(config)# route enable sbr
```

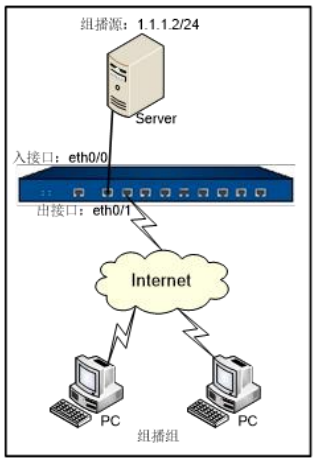
故障排除后，重新开启源路由的查询功能：

静态组播路由配置举例

本节介绍一个静态组播路由的配置举例。

组网需求

组播源发送数据至组播组，组播地址为 224.91.91.2。接口 ethernet0/0 属于 trust 安全域，为组播数据入接口；接口ethernet0/1 属于 untrust 安全域，为组播数据出接口。配置静态组播路由使组播数据可以正常转发给属于组播组的客户端PC。组网图如下图所示：



配置步骤

第一步：配置接口和安全域：

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 1.1.1.1/24
hostname(config-if-eth0/0)# exit
```

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 2.1.1.1/24
hostname(config-if-eth0/1)# exit
hostname(config)#
```

第二步：配置并开启静态组播功能：

```
hostname(config)# ip vrouter trust-vr
hostname(config)# address src
hostname(config-addr)# ip 1.1.1.2/32
hostname(config-addr)# exit
hostname(config)# address dst
hostname(config-addr)# ip 224.91.91.2/32
hostname(config-addr)# exit
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# src-addr src
hostname(config-policy-rule)# dst-addr dst
hostname(config-policy-rule)# service any
```

第三步：配置策略：

```
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

第 4 章 系统管理

命名规则

为不同的对象命名时，请遵循以下规则：

- 系统不建议使用以下特殊符号：逗号（，）、单引号（‘’）、双引号（“”）、制表符、空格、分号（；）、反斜杠（\）、斜杠（/）、尖括号（<>）、特殊字符（&、#）。为避免产生错误，建议用户尽量使用数字（0-9）和字母（a-z，A-Z）组成对象名称。
- 使用 CLI 创建对象时，如果对象名称中包含空格，请用双引号引住对象名称。在 WebUI 上创建带空格名称的对象时则无此限制，可直接输入对象名称。

配置主机名称

有些情况下，用户的网络环境中会配有一台以上设备，为区分这些设备，就需要为每一台设备指定不同的名称。设备的默认名称是其平台名称。通过 CLI 配置设备名称，在全局配置模式输入以下命令：

hostname *host-name*

- *host-name* - 指定设备名称。长度范围是 1 到 63 个字符。执行该命令后，命令行提示符也会变为新的设备的名称。在全局配置模式下使用 **no hostname** 命令恢复设备的默认名称。

以下是配置设备名称的命令示例：

```
hostname# configure（进入全局配置模式）hostname(config)# hostname
(config)#
```

配置系统信息显示语言

系统信息包括日志信息、错误信息和提示信息。设备支持简体中文和英文两种系统信息显示语言，在全局配置模式下，使用以下命令设置显示语言：

language {**en** | **zh_CN**}

- **en** – 设置系统信息显示语言为英文。默认情况下，系统信息显示语言为英文。
- **zh_CN** – 设置系统信息显示语言为简体中文。

在全局配置模式下使用 **no language** 命令恢复显示语言为默认情况。

需要注意的是，该命令的设置不会影响 Web 管理界面的语言。

配置管理员

设备的管理员根据角色的不同，对系统可执行的管理和配置权限不同。系统支持预定义管理员角色和自定义管理员角色。

系统默认预定义如下四类管理员角色，这四类管理员角色不可被删除和编辑:

- 系统管理员（admin）：拥有读、执行和写权限，可以通过 show 命令查看当前或者历史配置信息、在执行模式下运行import、export 和 save 等命令以及在任何模式下对设备所有功能模块进行配置。
- 系统管理员（只读）（admin-read-only）：拥有读和部分执行权限，可以通过 show 命令查看当前或者历史配置信息，可以在执行模式下运行 export 命令。
- 系统操作员（operator）：拥有读、执行和部分写权限，可以修改除管理员配置、重启设备、恢复出厂设置以及升级版本以外的其他功能模块配置，通过 show 命令查看当前或者历史配置信息、但是不能查看日志信息，以及在执行模式下运行部分执行命令。
- 系统审计员（auditor）：只可以对日志信息进行操作，包括查看、导出和清除。

下表为管理员的详细权限列表。

功能	权限			
	系统管理员	系统管理员（只读）	系统操作员	系统审计员
配置（包括保存配置）	√	χ	√	χ
管理员配置	√	χ	χ	χ
恢复出场配置	√	χ	χ	χ
删除配置文件	√	χ	√	χ
回退起始配置信息	√	χ	√	χ
重启设备	√	χ	χ	χ
查看配置信息	√	√	√	χ
查看日志信息	√	√	χ	√
修改当前管理员密码	√	√	√	√
import 命令	√	χ	√（除系统升级外）	χ
export 命令	√	√	χ	√
clear 命令	√	√	√	√
ping/traceroute 命令	√	√	√	χ
debug 命令	√	√	√	χ
exec 命令	√	√	√	√

功能	权限			
	系统管理员	系统管理员（只读）	系统操作员	系统审计员
terminal width 命令	√	√	√	√

- 设备拥有一个默认系统管理员“ ”，用户可以对系统管理员“ ”进行编辑（只可编辑密码和访问方式），但是不能删除该管理员。
- 除了系统管理员，其他角色的管理员不能编辑管理员的任何属性，只能修改自身密码。
- 系统审计员可以管理一种或多种日志信息，管理日志类型需要系统管理员配置。

用户可自定义管理员角色，指定管理员角色对 CLI 的权限和 WebUI 的权限。

- 新建管理员角色
- 指定管理员角色的权限
- 指定管理员角色的描述信息
- 创建管理员
- 配置管理员角色
- 配置管理员密码
- 配置管理员访问方式
- 配置系统审计员可管理日志类型
- 配置管理员登录限制
- 显示管理员角色的配置
- 显示管理员配置
- VSYS 管理员

新建管理员角色

新建管理员角色， 在全局配置模式下，使用如下命令：

admin role *role-name*

- *role-name* – 指定管理员角色的名称。长度范围是 4 到 95 个字符。执行该命令后，系统创建指定名称的管理员角色，并且进入管理员角色配置模式；如果指定的管理员角色名称已经存在，则直接进入管理员配置模式。

使用 **no admin role** *role-name* 命令删除指定的管理员角色。

指定管理员角色的权限

指定管理员角色的 CLI 权限，在管理员角色配置模式下，使用如下命令：

cli-privilege all {**rw** | **none**}

- **rw** | **none** – **rw** 表示管理员角色对全部 CLI 具有读写权限；**none** 表示管理员角色不具有 CLI 权限，不可使用 CLI 命令。

指定管理员角色的描述信息

指定管理员角色的描述信息，在管理员角色配置模式下，使用如下命令：

description *description*

- *description* – 指定描述信息标示此管理员角色。长度范围是 0 到 255 个字符。

使用 **no description** 命令删除描述信息。

创建管理员

创建管理员并进入管理员配置模式，请在全局配置模式下输入以下命令：

admin user *user-name*

- *user-name* - 指定管理员名称。长度范围是 4 到 31 个字符。执行该命令后，系统创建指定名称的管理员，并且进入管理员配置模式；如果指定的管理员名称已经存在，则直接进入管理员配置模式。

在全局配置模式下使用 **no admin user** *user-name* 命令删除指定的管理员。

在管理员配置模式下，用户可以配置管理员角色、管理员密码、访问方式和系统审计员可管理日志类型。

配置管理员角色

配置管理员角色，在管理员配置模式下输入以下命令：

role {**admin** | **operator** | **auditor** | **admin-read-only**}

- **admin** - 指定管理员角色为系统管理员（Administrator）。
- **operator** - 指定管理员角色为系统操作员（Operator）。
- **auditor** - 指定管理员角色为系统审计员（Auditor）。
- **admin-read-only** - 指定管理员角色为系统管理员（只读）（Administrator-read-only）。

配置管理员密码

设备具有密码策略。请为管理员指定符合密码策略的密码。指定管理员密码，在管理员配置模式下，输入以下命令配置管理员的密码：

password *password*

- *password* – 指定管理员的密码。范围是 4 到 31 个字符。

在管理员配置模式下使用 **no password** 命令取消管理员密码的配置。

系统允许当前登录的系统操作员、系统审计员或系统管理员（只读）修改自身密码，在任意模式下使用以下命令：

exec admin user password update *password*

- *password* – 指定管理员的新密码，为 4 到 31 个字符的字符串。

注意:系统管理员可以修改所有管理员的密码。

配置管理员密码策略

管理员密码策略中可以配置管理员密码的复杂度。密码复杂度包括密码的总长度、密码中组成元素的长度以及密码的有效期。其中组成元素包括以下 4 种类型：

- 大写字母（从 A 到 Z）。
- 小写字母（从 a 到 z）。
- 数字（从 0 到 9）。
- 其他可见字符。例如：分号（；）、斜杠（/）等字符（仅支持半角字符）。

管理员密码策略的配置需要在管理员密码策略配置模式下进行。进入管理员密码策略配置模式，在全局配置模式下，使用以下命令：

password-policy

如果系统默认的管理员密码复杂度设置无法满足安全性的需求，用户可以自定义密码复杂度。自定义密码复杂度前，用户必须先开启复杂度检测功能。

开启或关闭管理员密码的复杂度检测功能，在管理员密码策略配置模式下，使用以下命令：

admin complexity {**enable** | **disable**}

- **enable** | **disable** – 开启或关闭管理员密码的复杂度检测功能。默认情况下，管理员密码的复杂度检测功能为关闭状态。开启后，该功能默认要求密码中必须包含以下各项：两个大写字母、两个小写字母、两个数字和两个特殊字符（例如“@”等）。

用户自定义密码组成元素长度，在管理员密码策略配置模式下，使用以下命令：

admin {**capital-letters** | **non-alphanumeric-letters** | **numeric-characters** | **small-letters**} *value*

- **capital-letters** *value* – 指定管理员密码中大写字母的长度。默认值是 2 个字符，范围是 0 到 16。
- **non-alphanumeric-letters** *value* – 指定管理员密码中其他可见字符的长度。默认值是 2 个字符，范围是 0 到 16。
- **numeric-characters** *value* – 指定管理员密码中数字的长度。默认值是 2 个字符，范围是 0 到 16。
- **small-letters** *value* – 指定管理员密码中小写字母的长度。默认值是 2 个字符，范围是 0 到 16。

用户自定义管理员密码的最小长度，在管理员密码策略配置模式下，使用以下命令：

admin min-length *length-value*

- **min-length** *length-value* – 指定管理员密码的最小长度。默认值是 4 个字符，范围是 4 到 16 个字符。当开启管理员密码的复杂度检测功能时，最小长度的默认值为 8 个字符（两个大写字母、两个小写字母、两个数字和两个特殊字符），范围是 8 到 16 个字符。

注意:无论管理员密码的复杂度检测功能是否开启，用户都可以配置管理员密码的最小长度，以提高密码的安全性。

密码的有效期用来限制管理员密码的使用时间。当用户登录时，如果用户输入已经过期的密码，系统将提示重新设置密码，回车后再次输入新密码。如果输入的新密码不符合密码复杂度要求，或连续两次输入的新密码不一致，系统将要求用户重新输入。连续输入三次不符合要求的密码系统将会断开连接，用户重新登录时系统仍要求用户设置新密码。用户设置的新密码可以和旧密码相同。用户自定义管理员密码的有效期，在管理员密码策略配置模式下，使用以下命令：

admin password-expiration *value*

- **password-expiration** *value* – 指定管理员密码的有效期。单位为天，范围是 0 到 365 天，默认值是 0，表示不对有效期进行限制。在管理员密码策略配置模式下，使用 **no admin complexity** 命令恢复管理员密码的复杂度检测功能的默认情况。

显示管理员密码策略信息

用户可以在任何模式下，随时使用 show 命令查看管理员密码策略信息：

show password-policy

配置管理员访问方式

默认情况下，新建的管理员不可以访问设备进行配置。用户需指定管理员的访问方式。系统只允许系统 管理员指定其他角色的管理员的访问方式。在管理员配置模式下，输入以下命令配置管理员的访问方式：

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

- console – 指定管理员通过 Console 访问。
- http – 指定管理员通过 HTTP 访问。
- https – 指定管理员通过HTTPS 访问。
- ssh – 指定管理员通过 SSH 访问。
- telnet – 指定管理员通过 Telnet 访问。
- any – 指定管理员可以通过以上任何一种方式访问。

使用多条该命令为管理员指定多种访问方式。

使用 no access {console | http | https | ssh | telnet | any}命令取消指定的访问方式。

配置系统审计员可管理日志类型

系统审计员只允许对日志信息进行查看、导出和清除，可管理的日志类型需要系统管理员来指定。在管理员配置模式下，输入以下命令配置系统审计员可管理日志类型:

log {config | event | nbc | ips | traffic | network | security | iot-monitor}

- config – 指定系统审计员可管理配置日志信息。
- event – 指定系统审计员可管理事件日志信息。
- nbc – 指定系统审计员可管理 NBC 日志信息。
- ips – 指定系统审计员可管理 IPS 日志信息。
- traffic – 指定系统审计员可管理流量日志信息。
- network – 指定系统审计员可管理网络日志信息。
- security – 指定系统审计员可管理安全日志信息。
- iot-monitor – 指定系统审计员可管理 IoT 监控日志信息。

使用多条该命令为管理员指定多种可管理的日志类型。

使用 no log {config | event | nbc | ips | traffic | network | security| iot-monitor}命令取消指定的系统审计员可管理日志类型。

配置管理员登录限制

管理员使用某一账户登录设备时，密码输入错误次数超过设定次数时，系统会在指定时间内禁止使用该账户登录设备。指定禁止访问时长，在全局配置模式下，使用以下命令：

admin lockout-duration *time*

- lockout-duration *time* – 指定禁止访问时长。单位为分钟。范围是 1 到 65535。默认值是 2 分钟。

使用 no admin lockout-duration 命令恢复管理员登录时长默认配置。

指定密码输入错误最大次数，在全局配置模式下，使用以下命令：

admin max-login-failure *times*

- max-login-failure *times* – 指定管理员密码输入错误最大次数。默认值是 3，范围是 1 到 256。

使用 no admin max-login-failure 命令恢复管理员密码输入错误次数默认配置。

注意:只允许系统管理员配置管理员登录限制。

配置管理员的最大数量

系统支持配置管理员的最大数量。配置后，系统支持创建的管理员的最大数量将为指定数值，用户可根据需要进行调整。调整后，需将设备重启，指定值才能生效。配置管理员的最大数量，在全局配置模式下，使用以下命令：

capacity management max-administrative-users *capacity-num*

- *capacity-num* - 指定管理员最大数量的数值，取值范围为 1-128。

使用 no capacity management max-administrative-users 命令恢复默认的管理员最大数量的数值。不同平台的默认值不同，请以实际为准。

注意:该命令为本地配置命令，不支持 HA 同步。在HA 环境下，若主设备与备设备上设置的管理员最大数量不同，HA 状态显示正常，但系统会定时发出告警信息。

显示管理员角色的配置

显示管理员角色的配置：show admin role [*role-name*]

显示管理员配置

用户可以在任何模式下，随时使用 show 命令查看管理员配置：

- 显示管理员信息：show admin user
- 显示管理员具体配置信息：show admin user *user-name*

- 显示管理员禁止访问时长配置信息：**show admin lockout-duration**
- 显示管理员密码输入错误最大次数配置信息：**show admin max-login-failure**

配置可信主机

设备使用可信主机来进一步保证系统安全。管理员可以指定一个 IP 地址范围，在该指定范围内的主机为可信主机。只有可信主机才可以对设备进行管理。

默认情况下，设备的可信主机范围是 0.0.0.0/0，即所有主机都是可信主机。所有可信主机列表中可信主机范围都是有效的。因此，建议用户在创建好合适的可信主机后，将系统原有的“0.0.0.0/0”可信主机范围删除。

注意:如果远程主机不能访问设备，请检查设备的可信主机配置。

配置系统的可信主机，在全局配置模式下，使用以下命令:

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

- *A.B.C.D A.B.C.D* | **range** *A.B.C.D A.B.C.D* | *A.B.C.D/M* | **any** – 指定可信主机的 IP 地址范围，例如，1.1.1.1 255.255.0.0。**any** 表示任何 IP 地址。
- **http** | **https** | **ssh** | **telnet** | **any** – 指定可信主机的登录类型。**any** 表示可以使用 HTTP、HTTPS、SSH 和 Telnet 任意一种类型登录。

用户可以配置多条该命令添加多个可信主机范围。系统最多允许配置 128 条可信主机范围。

使用 **no admin host** *A.B.C.D A.B.C.D* 命令取消可信主机的指定。

使用 **no admin host** {*A.B.C.D A.B.C.D* | **range** *A.B.C.D A.B.C.D* | *A.B.C.D/M* | **any**} {**http** | **https** | **ssh** | **telnet**| **any** }取消对可信主机特定登录类型的指定。

配置 IPv6 可信主机

管理员可以指定一个 IPv6 地址范围，在该指定范围内的主机为可信主机。

配置 IPv6 地址的可信主机，在全局配置模式下，使用以下命令:

admin ipv6-host {*X:X:X:X::X/M* | **range***X:X:X:X::X X:X:X:X::X* | **any**} {**http** | **https** | **ssh** | **telnet**| **any** }

- *X:X:X:X::X/M* | **range***X:X:X:X::X X:X:X:X::X* | **any** – 指定可信主机的 IPv6 地址范围。any 表示任何 IP 地址。
- **http** | **https** | **ssh** | **telnet** | **any** – 指定可信主机的登录类型。**any** 表示可以使用 HTTP、HTTPS、SSH 和 Telnet 任意一种类型登录。

用户可以配置多条该命令添加多个可信主机范围。系统最多允许配置 128 条可信主机范围。

使用 **no admin ipv6-host***X:X:X:X::X/M* 命令取消可信主机的指定。

使用 **no admin ipv6-host** {*X:X:X:X::X/M* | **range***X:X:X:X::X X:X:X:X::X* | **any**} {**http** | **https** | **ssh** | **telnet**| **any** }取消对可信主机特定登录类型的指定。

显示可信主机配置

用户可以在任何模式下，随时使用 show 命令查看可信主机配置：

show admin host

配置管理接口

系统支持 Console、Telnet、SSH 以及 WebUI 方式的访问。用户可以配置各种访问方式的超时时间、端口号以及 HTTPS 的 PKI 信任域。

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

配置 Telnet 管理接口

用户可以配置 Telnet 的超时时间以及 Telnet 端口号。使用 Telnet 方式连接设备时，使用的端口号必须与此处配置的端口号一致。同时，用户还可以配置 Telnet 最大登录次数。

如果已经建立的 Telnet 连接在超时时间内未发送 Telnet 请求，系统将断开此次 Telnet 连接。配置 Telnet 超时时间，在全局配置模式下，使用以下命令：

telnet timeout *timeout-value*

- *timeout-value* – 指定 Telnet 超时时间，单位为分钟。范围是 1 到 60 分钟。默认值是 10 分钟。

在全局配置模式下，使用该命令 no 的形式恢复 Telnet 超时默认值：

no telnet timeout

配置 Telnet 最大会话数，在全局配置模式下，使用以下命令：

telnet max-session *max-session*

- *max-session* – 指定 Telnet 最大会话数。范围是 1 到 X，不同平台 X 的取值不同。默认值为 X。

在全局配置模式下，使用该命令 no 的形式恢复 Telnet 默认会话数：

no telnet max-session

配置 Telnet 端口号，在全局配置模式下，使用以下命令：

telnet port *port-number*

- *port-number* – 指定 Telnet 端口号。范围是 1 到 65535。默认值是 23。

在全局配置模式下，使用该命令 no 的形式恢复 Telnet 默认端口号：

no telnet port

Telnet 最大登录次数，是指允许用户连续失败登录的最大次数。如果连续登录失败次数超出该指定数值，系统将断开此次 Telnet 连接。配置 Telnet 最大登录次数，在全局配置模式下，使用以下命令：

telnet authorization-try-count *count-number*

- *count-number* – 指定最大连接次数。范围是 1 到 10 次。默认为 3 次。

在全局配置模式下，使用该命令 no 的形式恢复 Telnet 默认登录次数：

no telnet authorization-try-count

配置 SSH 管理接口

用户可以配置 SSH 超时时间以及端口号。并且可以指定 SSH 连接的间隔时间。

如果已经建立的 SSH 连接在超时时间内未发送 SSH 请求，系统将断开此次 SSH 连接。配置 SSH 超时时间，在全局配置模式下，使用以下命令：

ssh timeout *timeout-value*

- *timeout-value* – 指定 SSH 超时时间，单位为分钟。范围是 1 到 60 分钟。默认值是 10 分钟。

在全局配置模式下，使用该命令 no 的形式恢复 SSH 默认超时时间：

no ssh timeout

配置 SSH 最大会话数，在全局配置模式下，使用以下命令：

ssh max-session *max-session*

- *max-session* – 指定 SSH 最大会话数。范围是 1 到 X，不同平台 X 的取值不同。默认值为 X。

在全局配置模式下，使用该命令 no 的形式恢复 SSH 默认会话数：

no ssh max-session *max-session*

配置 SSH 端口号，在全局配置模式下，使用以下命令：

ssh port *port-number*

- *port-number* – 指定 SSH 端口号。范围是 1 到 65535。默认值是 22。

在全局配置模式下，使用该命令 no 的形式恢复 SSH 默认端口号：

no ssh port

用户可以指定设备处理 SSH 连接的时间间隔。建立一个 SSH 连接后，在时间间隔过后，设备才接受下一个 SSH 连接请求。配置 SSH 连接时间间隔，在全局配置模式下，使用以下命令：

ssh connection-interval *interval-time*

- *interval-time* – 指定时间间隔，单位是秒。范围是 2 到 3600 秒。默认值是 2 秒。

在全局配置模式下，使用该命令 no 的形式恢复 SSH 连接默认端时间间隔：

no ssh connection-interval

配置 WebUI 管理接口

用户可以通过 HTTP 和 HTTPS 方式访问设备，进行配置。配置 WebUI 超时时间，在全局配置模式下，使用以下命令：

web timeout *timeout-value*

- *timeout-value* – 指定 WebUI 超时时间，单位为分钟。范围是 1 到 1440 分钟。默认值是 10 分钟。

在全局配置模式下，使用该命令 no 的形式恢复 WebUI 超时默认值：

no web timeout

指定 HTTP 端口号，在全局配置模式下，使用以下命令：

http port *port-number*

- *port-number* – 指定 HTTP 端口号。当使用 HTTP 方式访问设备时，浏览器的 HTTP 端口号必须与此处指定的端口号一致。范围是 1 到 65535。默认值是 80。

在全局配置模式下，使用该命令 no 的形式，恢复默认 HTTP 端口号：

no http port

配置防跨站脚本攻击（anti-xss）服务，在全局配置模式下，使用以下命令：

http anti-xss { **disable** | **enable** | **mode** {**normal**| **strict**}}

- **disable** | **enable** – 启用和禁用防跨站脚本攻击服务。默认情况下，防跨站脚本攻击服务为启用状态。
- **mode** {**normal**| **strict**} – 指定防跨站脚本攻击服务模式。包括字符匹配模式（**normal**）和正则表达式匹配模式（**strict**）。

在全局配置模式下，使用该命令 no 的形式，恢复防跨站脚本攻击（anti-xss）服务默认值：

no http anti-xss { **disable** | **enable** | **mode** {**normal**| **strict**}}

指定 HTTPS 端口号，在全局配置模式下，使用以下命令：

https port *port-number*

- *port-number* – 指定 HTTPS 端口号。当使用 HTTPS 方式访问设备时，浏览器的 HTTPS 端口号必须与此处指定的端口号一致。范围是 1 到 65535。默认值是 443。

在全局配置模式下，使用该命令 no 形式恢复默认HTTPS 端口号：

no https port

指定 HTTPS 方式访问时使用的PKI 信任域，在全局配置模式下，使用以下命令：

https trust-domain *trust-domain-name*

- *trust-domain-name* – 指定已配置的PKI 信任域的名称。当 HTTPS 启动时，HTTPS 服务器将使用指定PKI 信任域中的证书。默认情况下，系统将使用缺省 PKI 信任域trust_domain_default。

在全局配置模式下，使用该命令 no 的形式恢复默认PKI 信任域：

no https trust-domain

显示管理接口配置

用户可以在任何模式下，随时使用 show 命令查看管理接口配置信息。命令如下：

- 显示 Console 配置：**show console**
- 显示 Telnet 配置：**show telnet**
- 显示 SSH 配置：**show ssh**
- 显示 Web 配置：**show http**

配置文件管理

系统的配置信息都被保存在系统的配置文件中。用户通过运行相应的命令或者访问相应的 WebUI 页面查看系统的各种配置信息，例如系统的初始配置信息和当前配置信息等。配置文件以命令行的格式保存配置信息，并且也以这种格式显示配置信息。

配置 设备配置信息

用户可以查看和保存系统的配置信息，也可以导出和导入配置信息。

查看配置信息

配置文件中保存的用来初始化系统的配置信息称作起始配置信息，系统通过读取起始配置信息进行启动时的初始化工作；如果找不到起始配置信息，系统则使用系统的缺省参数初始化。与起始配置信息相对应，系统运行过程中正在生效的配置称为当前配置信息。

系统起始配置信息包括系统的当前起始配置信息（系统启动时使用的配置信息），和系统的备份起始信 息。系统纪录最近十次保存的配置信息，最近一次保存的配置信息会纪录为系统的当前起始配置信息，当前系统配置信息以“startup”作为标记。前九次的配置信息按照保存时间的先后以数字 0 到 8 作为标记。

查看系统的当前起始配置信息，在任何命令模式下输入以下命令：**show configuration** [**startup**]

查看设备的备份起始信息，在任何命令模式下使用以下命令：

show configuration backup *number*

- *number* - 备份起始信息的数字标记。

查看设备的当前配置信息，在任何命令模式下输入以下命令：

show configuration

查看设备的当前接口配置信息，在任何命令模式下输入以下命令：

show configuration interface [*interface-name* | **last** *number*]

- *interface-name* – 指定显示配置信息的接口名称。
- **last** *number* – 指定显示配置信息的接口条目数。显示从倒数指定数值的条目开始到最后条目的接口配置信息。如果指定数值大于所有接口条目数，则显示所有接口配置信息。

查看设备的备份起始信息记录，在任何命令模式下输入以下命令：

show configuration record

查看设备的当前运行的配置信息记录，在任何命令模式下输入以下命令：

show configuration running

查看设备的当前地址簿配置信息，在任何命令模式下输入以下命令：

show configuration address [**last** *number*]

- **last** *number* – 指定显示配置信息的地址簿条目数。显示从倒数指定数值的条目开始到最后条目的地址簿配置信息。如果指定数值大于所有地址簿条目数，则显示所有地址簿配置信息。

查看设备的当前策略配置信息，在任何命令模式下输入以下命令：

show configuration policy [**last** *number*]

- *last number* – 指定显示配置信息的策略条目数。显示从倒数指定数值的条目开始到最后条目的策略配置信息。如果指定数值大于所有策略条目数，则显示所有策略配置信息。

查看设备的当前路由配置信息，在任何命令模式下输入以下命令：

show configuration vrouter [**last** *number*]

- **last** *number* – 指定显示配置信息的路由条目数。显示从倒数指定数值的条目开始到最后条目的路由配置信息。如果指定数值大于所有路由条目数，则显示所有路由配置信息。

以 xml 方式输出当前配置信息，在任何命令模式下输入以下命令：

show configuration xml

回退配置信息

回退配置信息，系统支持以下两种方式：

在执行模式下，使用以下命令回退起始配置信息。系统能够纪录最近十次保存的起始配置信息，用户可以根据需要回退到已保存的指定的起始配置信息。系统将在重启后使用指定的起始配置信息。

rollback configuration backup *number*

- *number* – 备份起始配置信息的数字标记。

在配置回滚模式下，使用以下命令回退配置信息并退出配置回滚模式。用户不需要重启设备，该配置直接生效。

exec configuration rollback

注意:在执行模式下，使用 **exec configuration start** 进入配置回滚模式。

示例:

```
hostname# exec configuration start（进入配置回滚模式）
hostname[TRN]# configure （进入全局配置模式）
..... （进行任意配置，且所做配置即时生效）
hostname[TRN](config)# exec configuration rollback （回退配置并退出配置回滚模式）
hostname#
```

退出配置回滚模式

直接退出配置回滚模式，系统支持以下两种方式：

在配置回滚模式下，使用以下命令直接退出配置回滚模式：

exec configuration commit

示例:

```
hostname# exec configuration start （进入配置回滚模式）hostname[TRN]# configure （进入全局配置模式）
..... （进行任意配置，且所做配置即时生效）
hostname[TRN](config)# exec configuration commit （直接退出配置回滚模式）
hostname#
```

在配置回滚模式下，使用 **exit** 命令直接退出登录终端，从而退出配置回滚模式。

- 当不同用户同时登录设备时，先进入配置回滚模式的用户可以继续配置操作，其他用户无法进行配置操作。
- 当相同用户通过不同访问方式登录设备时，先进入配置回滚模式的某访问方式的用户可以继续配置操作，其他访问方式的用户无法进行配置操作，但其可以使用 **exec configuration commit** 或者 **exec configuration rollback** 命令强制进入配置回滚模式的某访问方式的用户退出配置回滚模式。

配置退出配置回滚模式的动作

当使用 **exit** 命令退出配置回滚模式时，默认情况下，系统会直接退出配置回滚模式。回退配置后退出配置回滚模式，在全局配置模式下，使用以下命令：

cli-exit-action rollback

恢复直接退出配置回滚模式，在全局配置模式下，使用以下命令：

cli-exit-action commit

删除配置文件

用户可以删除设备的起始配置信息。删除起始配置信息，在执行模式下，使用以下命令：

delete configuration {**startup** | **backup** *number*}

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

保存配置信息

用户可以保存系统的当前配置信息使其成为系统下次启动时的起始配置。保存系统的当前配置信息，在任何命令模式下输入以下命令：

save [*string*]

- *string* - 对所保存配置信息的描述。如果不使用 *string* 对保存的配置文件进行描述，系统会直接覆盖原有配置文件。

自动备份配置文件

用户可以通过配置自动备份配置文件功能，能够实现设备定期检查配置文件，在当前配置文件发生变化时，系统会自动将当前的配置文件上传到 FTP 或 TFTP 服务器上。

指定自动备份配置文件到FTP 服务器，在全局配置模式下，使用以下命令：

configuration auto-backup ftp *ip-address* [**user** *user-name* **password** *password*] [**vrouter** *vrouter-name*] **path** *path* [**interval** *time-value*]

- *ip-address* - 指定 FTP 服务器的 IP 地址。
- **user** *user-name* **password** *password* – 指定访问 FTP 服务器的用户名和密码。
- **vrouter** *vrouter-name* – 指定 VRouter 的名称。
- **path** *path* – 指定配置文件的上传路径。
- **interval** *time-value* – 指定自动备份配置文件的时间间隔。单位为小时，默认值是 1 小时。范围是 1 到 7*24 小时。如果不指定该参数，系统将每 1 小时检查配置文件，在发生变化时，自动备份到 FTP 服务器上。

在全局配置模式下，使用 **no configuration auto-backup ftp** 取消自动备份配置文件到FTP 服务器。

指定自动备份配置文件到 TFTP 服务器，在全局配置模式下，使用以下命令：

configuration auto-backup tftp *ip-address* [**vrouter** *vrouter-name*] **path** *path* [**interval** *time-value*]

在全局配置模式下，使用 **no configuration auto-backup tftp** 取消自动备份配置文件到 TFTP 服务器。

查看自动备份配置文件信息

查看自动备份配置文件功能的信息，在任何命令模式下输入以下命令：

show configuration auto-backup

导出配置信息

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

导出系统配置信息到 FTP 服务器，在执行模式下使用以下命令：

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

- **startup** | **backup** *number* – 指定导出的配置信息。**startup** 为导出当前配置信息；*number* 为导出以 *number* 为标识的备份配置信息。
- *ip-address* – 指定 FTP 服务器的 IP 地址。
- *vrouter-name* - 导出指定 VRouter 的配置信息。
- **user** *user-name* **password** *password* – 指定访问 FTP 服务器的用户名和密码。
- *file-name* – 指定导出的配置信息文件的名称。

导出系统配置信息到 TFTP 服务器，在执行模式下使用以下命令：

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

导出系统配置信息到 U 盘，在执行模式下使用以下命令：

export configuration {**startup** | **backup** *number*} **to** {**usb0** | **usb1**} [**vrouter** *vrouter-name*] [*file-name*]

导入配置信息

用户可以通过FTP 和 TFTP 服务器导入配置信息，也可以将配置信息放入 U 盘中，通过设备的 USB 口导入配置信息。

从 FTP 服务器导入配置信息，在执行模式下使用以下命令：

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

- *ip-address* – 指定 FTP 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 导入配置信息。
- *file-name* – 指定导入的配置信息文件的名称。

从 TFTP 服务器导入配置信息，在执行模式下使用以下命令：

import configuration from tftp server *ip-address* [**vrouter** *vrouter-name*] *file-name*

从 U 盘导入配置信息，在执行模式下使用以下命令：

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

恢复出厂配置

用户除使用设备上的 CLR 按键使系统恢复到出厂配置外，也可以使用命令恢复。恢复出厂配置，在任何模式下，使用以下命令：

unset all

注意:小心使用该命令。执行该命令后，设备的所有配置将被清除。

查看当前对象的配置信息

当用户在某一配置模式下完成指定对象的配置之后，用户可以当前配置模式下，使用 **show this** 命令查看当前对象的配置信息。

下表列出了目前系统支持查看当前配置信息的对象名称和配置模式:

对象名称	配置模式	配置模式提示符
管理员	管理员配置模式	hostname(config-admin)#
AAA 服务器	AAA 服务配置模式	hostname(config-aaa-server)#
接口	接口配置模式	hostname(config-if-eth0/0)#
安全域	安全域配置模式	hostname(config-zone-trust)#
地址簿	地址配置模式	hostname(config-addr)#
服务	服务配置模式	hostname(config-service)#
服务组	服务组配置模式	hostname(config-svc-group)#
策略路由	PBR 策略配置模式	hostname(config-pbr)#
VRouter	VRouter 配置模式	hostname(config-vrouter)#
为 trust-vr 配置 NAT	NAT 配置模式	hostname(config-nat)#

系统维护与调试

系统支持网络连接测试工具 Ping 和 Traceroute，当网络出现问题时，用户可以用这些工具对网络进行测试，查找故障原因。系统同时具有调试功能，供用户查阅与分析。

Ping 命令

Ping 命令主要用于检查网络连接状态以及主机是否可达。用户可以随时在任何 CLI 命令模式下使用 Ping 命令，检查网络连接状态及主机是否可达。其使用方法为:

ping [**ipv6**] {*ip-address* | *hostname*} [**count** *number*] [**size** *number*] [**source** *ip-address*] [**timeout** *time*] [**vrouter** *vrouter-name*]

- *ip-address* | *hostname* – 指定接受 Ping 报文的目的地址，可以是 IP 地址，也可以是主机名称。在双栈系统固件下，可以是 IPv6 地址。
- **count** *number* – 指定发送Ping 包的个数。范围是 1 到 65535。默认情况下，系统不限制发送 Ping 包的个数。
- **size** *number* – 指定发送Ping 包的大小。范围是 28 到 65500 字节（byte）。
- **source** *ip-address* – 指定发送 Ping 包的源地址，只能是接口名称。
- **timeout** *time* – 指定发送 Ping 包的超时时间。范围是 0 到 3600 秒。默认值是 0，即为没有超时时间限制。
- **vrouter** *vrouter-name* – 指定发送 Ping 包的出接口所属的VRouter。默认为缺省 VR，即 trust-vr。

命令输出结果包括以下两部分：

- 对每个 ping 报文的响应情况。如果在超时时间到后仍没有收到响应报文，则输出 Destination Host Not Responding 等，否则显示响应报文中报文序号、TTL 和响应时间；如果 ping 包没有到达目的路由或发送 ping 包的接口发生变化，则输出 Network is unreachable；如果接受 Ping 报文的目的地址无法解析时，则输出unknown host *hostname*。
- 最后的统计信息，包括发送报文数、接收报文数、未响应报文百分比、命令执行时间和响应时间的最小、平均、最大和平均偏差值。

以下是 Ping 命令使用示例：

```
hostname(config)# ping 10.200.3.1
Sending ICMP packets to 10.200.3.1
Seq ttl time(ms)
1 128 2.53
2 128 1.48
3 128 1.48
4 128 1.47
5 128 1.46
statistics:
5 packets sent, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 1.464/1.689/2.536/0.423 ms
```

Traceroute 命令

Traceroute 用于测试数据包从发送主机到目的地所经过的网关。它主要用于检查网络连接是否可达，以及分析网络什么地方发生了故障。Traceroute 通常的执行过程是：首先发送一个 TTL 为 1 的数据包，因此第一跳发送回一个 ICMP 错误消息以指明此数据包不能被发送（因为 TTL 超时），之后此数据包被重新发送，TTL 为 2，同样第二跳返回 TTL 超时，这个过程不断进行，直到到达目的地。执行这些过程的目的是记录每一个 ICMP TTL 超时消息的源地址，以提供一个 IP 数据包到达目的地所经历的路径。

用户可以随时在任何 CLI 命令模式下使用 Traceroute 命令测试数据包经过的网关。其使用方法为：

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

- *ip-address* | *hostname* – 指定 traceroute 命令的目的地址，可以是 IP 地址，也可以是主机名称。
- **numberic** - 指定用数字的方式显示地址，而不对地址进行解析。
- **port** *port-number* – 指定 UDP 端口号。范围是 1 到 65535。默认端口号为 33434。
- **probe** *probe-number* – 指定 traceroute 命令在每一跳发出的探测包的数目。范围是 1 到 65535。默认值是 3。
- **timeout** *time* – 指定发送下一个探测包的超时时间。范围是 1 到 3600 秒。默认值是 5 秒。
- **ttl** [*min-ttl*] [*max-ttl*] – *min-ttl* 用来指定最小 TTL 值，范围是 1 到 255，默认值是 1。*max-ttl* 用来指定最大 TTL 值，范围是 1 到 255，默认值是 30。指定 TTL 值，用来显示 *min-ttl* 跳到 *max-ttl* 跳的回显。
- **source** *interface* – 指定发送 traceroute 探测包的源地址，只可以是源接口名称。
- **use-icmp** – 指定使用 ICMP 包进行探测。如不配置该参数，系统将使用UDP 包进行探测。
- **vrouter** *vrouter-name* – 指定发送 traceroute 探测包的出接口所属的VRouter。默认为缺省 VRouter，即 trust-vr。

以下是使用 traceroute 命令分析网络情况的示例：

```
hostname(config)# traceroute 210.74.176.150
traceroute to 210.74.176.150 (210.74.176.150), 30 hops max, 52 byte packets
1 10.200.3.1 (10.200.3.1) 0.572 ms 0.541 ms 0.359 ms
2 192.168.3.1 (192.168.3.1) 0.601 ms 0.754 ms 0.522 ms
3 202.106.149.177 (202.106.149.177) 1.169 ms 1.723 ms 1.104 ms
```

```
4 61.148.16.133 (61.148.16.133) 2.272 ms 1.940 ms 2.370 ms

5 61.148.4.17 (61.148.4.17) 2.770 ms 61.148.4.101 (61.148.4.101) 6.030 ms 61.148.4.21 (61.148.4.21) 2.584 ms

6 202.106.227.45 (202.106.227.45) 4.893 ms 5.010 ms 3.917 ms

7 202.106.193.70 (202.106.193.70) 5.407 ms 202.106.193.126 (202.106.193.126) 4.247 ms 202.106.193.70
(202.106.193.70) 6.954 ms

8 61.148.143.30 (61.148.143.30) 3.459 ms 3.758 ms 2.853 ms

9 * * *

10 * * *
```

从以上示例结果中可以看出，从源主机到目的主机经过了哪些网关，以及哪些网关出现了故障。

系统调试功能

系统调试功能可以帮助用户对错误进行诊断和定位。设备的各种协议和功能基本上都具有相应的调试功 能。默认情况下，所有协议和功能的系统调试功能都是关闭的。用户只可以通过 CLI 对系统调试功能进行配置。开启设备的系统调试功能，请在任何模式下输入以下命令：

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

- **all** – 开启设备所有协议和功能的系统调试功能。
- *function-name* – 开启设备指定协议或功能的系统调试功能。

在任何配置模式输入以下命令关闭所有或指定功能的系统调试功：

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

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

查看调试功能开启或者关闭状态，请在任何模式下输入以下命令：

show debug

注意:调试功能开启后，如果需要在终端输出 debug 信息，请开启系统的 debug 日志功能（执行 **logging debug on** 命令）。

收集并保存技术支持信息到文件

为了便于定位系统故障，系统支持收集 show 相关命令的显示信息，并保存成tech-support 文件。收集并保存技术支持信息到文件，在任意模式下，使用以下命令：

show tech-support [**cpu** cpu-number | **all**]

- *cpu-number* – 收集并保存指定 CPU 的技术支持信息到文件。该参数仅在多CPU 系统中显示。
- **all** – 收集并保存所有技术支持信息到文件。该参数仅在多 CPU 系统中显示。

注意:单CPU 系统直接通过 **show tech-support** 命令收集并保存所有技术支持信息到文件。

显示技术支持信息

显示技术支持信息到 Console 口，在任意模式下，使用以下命令:

show tech-support [**cpu** *cpu-number* | **all**] **toconsole**

- *cpu-number* – 显示指定CPU 的技术支持信息到Console 口。该选项仅在多 CPU 系统中显示。
- **all** – 显示所有技术支持信息到 Console 口。该选项仅在多 CPU 系统中显示。

注意:单CPU 系统直接通过 **show tech-support toconsole** 命令显示技术支持信息到 Console 口。

自动收集技术支持信息

配置系统自动收集技术支持信息，在任意模式下，使用以下命令:

show tech-support-auto interval *interval-time* **count** *count-time*

- *interval-time* - 指定自动收集技术支持信息的间隔时间。取值范围为 10 到 1440。单位为分钟。
- *count-time* – 指定自动收集信息技术支持信息的次数。取值范围为 1 到 10 次。

注意:

- 系统最多可以保存 10 个 tech-support 文件，当生成的文件个数超过 10 个时，新生成的文件会从头开始覆盖老的文件。
- 当配置完成并执行该命令时，如果再次配置自动收集技术支持信息，新的配置会覆盖之前的配置。

配置系统重启

在设备运行过程中，由于各种原因，如系统文件升级等，用户需要重启设备。用户可以通过下电再重新上电重启设备，也可以通过 CLI 或者 WebUI 重启设备。

重启设备，请在执行模式下使用 **reboot** 命令重启。请参阅以下示例:

```
hostname# reboot
System configuration has been modified. Save? [y]/n （键入字母"y"或者敲回车键，系统将保存配置；键入字母"n"，系统将不保存配置）
```

```
Building configuration..

Saving configuration is finished

System reboot, are you sure? y/[n] （键入字母"y"，系统将重启；键入字母"n"或者敲回车键，系统将返回到执行模式）
```

执行 **reboot** 命令时，系统首先会提示用户是否保存先前所做的配置。请谨慎使用 reboot 命令，因为执行该命令会导致网络工作在短时间内中断。

StoneOS 版本升级

用户在使用设备的过程中，有时需要升级设备的系统固件 StoneOS 的版本。本节介绍设备的启动系统以及 StoneOS 的升级方法。

通过 CLI 升级 StoneOS

除了可以在 Sysloader 中升级 StoneOS 以外，用户还可以在 CLI 中通过 FTP 服务器、TFTP 服务器或者 U 盘升级 StoneOS。

登录进入 CLI 后，在执行模式下，使用以下命令通过 FTP 服务器升级 StoneOS：

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

- *ip-address* – 指定 FTP 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* - 通过指定的VRouter 升级 StoneOS。
- *file-name* – 指定 StoneOS 名称。

登录进入 CLI 后，在执行模式下，使用以下命令通过 TFTP 服务器升级 StoneOS：

import image from tftp server *ip-address* [**vrouter** *vrouter-name*] *file-name*

登录进入 CLI 后，在执行模式下，使用以下命令通过 U 盘升级 StoneOS：

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

升级 StoneOS 成功后，重启系统使新的 StoneOS 生效。

许可证管理

许可证（license）用来授权用户使用一些功能、服务，或者用来扩展性能。对于基于许可证的功能、服务和性能来说，如果没有购买和安装相应的许可证，该功能和服务就无法使用，或不能达到更高的性能。

系统的许可证的分类和规则如下表：

平台许可证	说明	许可证过期
平台试用许可证（Platform Trial）	平台许可证是其他许可证运行的基础，如果平台许可证无效，其他许可证均不生效。	到期后， 已有的配置不能修改，若设备重启，系统恢复出厂配置。
平台正式许可证（Platform Base）	设备正式销售后，可以安装平台正式许可证。该许可证提供基础防火墙功能和 VPN 功能。	到期后，设备仍可正常使用，但不能升级到期后的 OS 版本。
功能许可证	**说明**	**许可证过期**
SSL VPN 许可证	授权 SSL VPN 的最大接入数量。多个 SSL VPN 许可证可以叠加允许接入用户的最大数量。	无过期。
QoS/iQoS 许可证	开启流量管理功能。	到期后，无法使用 QoS/iQoS 的功能升级和维护服务。
沙箱防护许可证	提供沙箱防护功能，授权每天允许上传到云沙箱的可疑文件样本数目，并且提供域名白名单的升级。 分为以下 3 种许可证： •Sandbox-300 许可证：每天允许上传 300 个文件。 •Sandbox-500 许可证：每天允许上传 500 个文件。 •Sandbox-1000 许可证：每天允许上传 1000 个文件。	有效期包括 1 年、2 年、3 年。过期后，云端分析功能无法使用，不能升级域名白名单。 仅可根据本地数据库缓存结果使用沙箱防护功能，重启设备之后，功能不可用。
服务许可证	**说明**	**许可证过期**
病毒过滤（AV）许可证	提供病毒过滤功能和病毒特征库的升级。	过期后，不能升级病毒特征库，病毒过滤功能正常使用。
入侵防御（IPS）许可证	提供入侵防御功能和 IPS 特征库升级。	过期后，不能升级 IPS 特征库，入侵防御功能正常使用。
URL DB 许可证	提供 URL 分类库和 URL 分类库的在线查询功能。	过期后，不能提供 URL 分类库的在线查询功能，自定

		义 URL 和 URL 过滤功能仍正常使用。
APP DB 许可证	提供 APP 库升级功能。APP DB 许可证不需要单独申请，随平台许可证一同发放，有效期也同平台许可证。	过期后不能升级 APP 特征库。
IP 信誉许可证	提供 IP 信誉的边界流量过滤（PTF）功能和 IP 信誉特征库升级。从 StoneOS 5.5R6 及以后版本，预定义黑名单边界流量过滤功能（由 PTF 许可证提供）升级为 IP 信誉边界流量过滤，用户可购买 IP 信誉许可证进行升级使用。	到期后，系统会自动删除 IP 信誉特征库，且 IP 信誉边界流量过滤功能将不能使用。
僵尸网络 C&C 防御许可证	提供僵尸网络 C&C 防御功能和僵尸网络 C&C 防御特征库的升级。	过期后，不能提供其包含的特征库的升级，功能仍可使用。

安装许可证

许可证为一串字符串。获得许可证后，用户需要将许可证安装到相应的设备。

在 CLI 中安装许可证，在任何模式下使用 **exec license install** *license-string* 命令。具体命令描述，请参考“许可证命令”。许可证正确安装完后，用户需重启设备以使许可证生效。

许可证校验

虚拟化防火墙产品安装许可证后，需连接到 LMS（许可证管理系统），进行合法性校验，以防止许可证被克隆。目前系统支持两种校验方式，分别是通过互联网连接到公网 LMS 进行校验和通过局域网连接到内网 LMS 进行校验，用户可根据需要选择其中的一种方式。

- 通过公网 LMS 校验适用于小型私有云或公有云场景。连接到公网 LMS 后，公网 LMS 将提供许可证的合法性校验（目前公网 LMS 暂不提供许可证的分发和管理）。若发现克隆许可证的行为，克隆设备（安装许可证较晚的设备）将会立即被重启。
- 通过局域网LMS 校验适用于大型私有云或行业云场景。连接到内网 LMS 后，内网 LMS 不仅能提 供许可证的校验，还可提供许可证的自动分发和管理。若发现克隆许可证的行为，克隆设备（安装许可证较晚的设备）上的许可证将会被卸载，同时设备也将立即被重启。

若未连接到 LMS 进行校验，设备将会每隔 30 天进行重启。

连接 LMS，在任何模式下使用以下命令：

exec lms enable { **public** | **private ip** *A.B.C.D* **port** *port-number*}

断开与 LMS 的连接，在任何模式下使用以下命令：

exec lms disable

具体命令描述，请参考“许可证命令”。 安装许可证并连接到 LMS 后，用户需重启系统以使许可证生效。

配置 HA 备设备通过主设备与 LMS 进行通信

以 HA 的方式进行部署时，若没有足够公网 IP 提供给备设备来连接公网 LMS 时，可以配置通过主设备连接公网 LMS 进行通信，进而完成许可证的校验。此时，主设备将作为备设备的代理，备设备与公网 LMS 的认证请求，将通过主备之间的 HA 链路转发给主设备，最终由主设备发送到公网LMS 服务器上。该功能默认情况下为关闭状态。开启通过主设备连接 LMS，在主设备的全局配置模式下，使用以下命令：

lms master-auth-proxy { **enable** | **disable** }

- **enable** - 开启通过主设备连接 LMS。开启后，主设备将作为备设备的代理，备设备与公网 LMS 的认证请求，将通过 HA 链路转发给主设备，最终通过主设备发送到公网 LMS 服务器上。
- **disable** - 关闭通过主设备连接 LMS 的功能。当备设备本身能够与 LMS 连接时，可关闭该功能。

许可证命令

本节具体描述申请、安装和卸载许可证所需的命令。

安装/卸载许可证

获得许可证后，用户可在任何模式下通过使用以下命令安装许可证：

exec license install *license-string*

- *license-string* – 要安装的许可证字符串。

卸载许可证，在任何模式下使用以下命令：

exec license uninstall *license-name*

- *license-name* – 要卸载的许可证名称。

安装部分许可证后，需要输入命令 **reboot** 使系统重启。以下许可证将在重启后生效，其他许可证直接生效。

- 首次安装以下许可证后，需要重启系统：Platform 订阅许可证、Platform 正式许可证、AV 许可证、IPS 许可证、僵尸网络 C&C 防御正式许可证、反垃圾邮件许可证、Stoneshield 许可证、URL DB 许可证、沙箱防护许可证、vCPU 正式许可证、链路负载均衡许可证（LLB）、IP 信誉许可证 。
- 每次安装以下许可证后，需要重启系统：AEL 许可证、VSYS 许可证。

许可证校验

云•界安装许可证后，需要用户连接到 LMS 进行合法性验证，以防止许可证被克隆。在任何模式下使用以下命令：

exec lms enable { **public** | **private ip** *A.B.C.D* **port** *port-number*}

- **public** – 指定通过公网 LMS 进行许可证校验。
- **private ip** *A.B.C.D* – 指定通过内网 LMS 进行许可证校验，并指定内网 LMS 的 IP 地址。
- **port** *port-number* – 指定连接内网 LMS 的端口号，取值范围为 1 到 65535，默认为 8001。

许可证将在设备重启后生效，若此前未重启过，连接 LMS 成功后，可输入命令 **reboot** 重启设备。

断开与 LMS 的连接，在任何模式下使用以下命令：

exec lms disable

注意:通过公网LMS 进行许可证验证时，请保证连接公网 LMS 的接口在trust-vr 安全域内并且通过 trust-vr 安全域可以访问互联网。

显示与 LMS 的连接信息

在任意模式下，使用以下命令查看与 LMS 的连接信息：

show lms

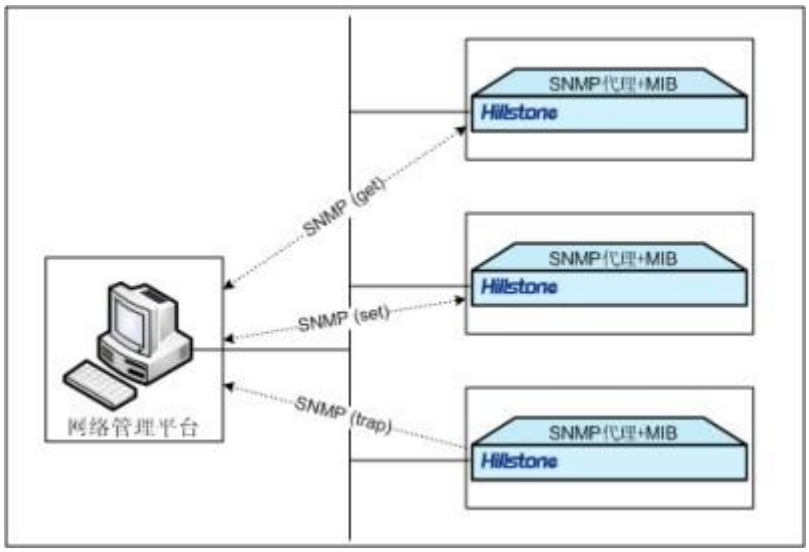
简单网络管理协议（SNMP）

简单网络管理协议（SNMP， Simple Network Management Protocol）是应用层协议，它通过标准框架、公共语言和相对应的安全机制来监控和管理网络设备。SNMP 的体系结构包括网络管理平台、SNMP 代理、网络管理协议和管理信息库（MIB， Management Information Base）四部分。

- 网络管理平台：是一个通过网络管理软件（如 adventnet、solarwinds 等）向 SNMP 代理发出 Get 和 Set 报文并接收代理的应答，以达到管理和监控网络设备目的的系统。
- SNMP 代理：是运行在被管理网络设备上的一个软件模块，用来维护被管理设备的信息数据并在需要时把管理数据发送给网络管理平台。
- 网络管理协议：网络管理平台和 SNMP 代理之间是通过网络管理协议连接的，通过 SNMP 报文的形式来交换信息。协议主要支持 Get、Set 和 Trap 三种功能，Get 用于管理平台获取代理的 MIB 对象值，Set 用于管理平台去设置代理的 MIB 对象值，Trap 用于代理向管理平台通告重要事件。
- 管理信息库（MIB）：是由 SNMP 代理维护的有关网络设备的信息数据库，信息库里的内容可供网络管理平台查询或设置其中变量的值。

设备的 SNMP 功能

设备拥有 SNMP 代理功能，该 SNMP 代理功能能够接受网络管理平台的操作请求并反馈网络和设备的相应信息。下图为 SNMP 管理框架在设备中实现的示意图：



SNMP 版本

设备支持以下版本的 SNMP：

- SNMPv1 协议，具体描述请参阅 RFC-1157，A Simple Network Management Protocol。
- SNMPv2 协议，具体描述请参阅 RFC-1901，Introduction to Community-based SNMPv2；RFC-1905，Protocol Operations for Version 2 of the Simple Network Management Protocol；RFC-1906，Transport Mappings for Version 2 of the Simple Network Management Protocol。
- SNMPv3 协议，具体描述请参阅 RFC2263，SNMPv3 Applications；RFC2264，User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)；RFC2265，View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)。

SNMPv1 和 SNMPv2c 都使用了团体字的认证方式，可以限制网络管理平台获取设备信息。SNMPv3 引入了基于用户的安全模型用于保证消息安全及基于视图的访问控制模型用于访问控制。

MIB 信息库

设备支持 RFC-1213 中定义的所有相关的管理信息库组（Management Information Base for Network Management of TCP/IP-based Internets: MIB-II）和 RFC-2233 中定义的使用 SMIv2 的接口组 MIB（The Interfaces Group MIB using SMIv2：IF-MIB）。此外，StoneOS 提供一个私有MIB 库，MIB 库中包含 设备的系统信息、IPSec VPN 信息以及系统统计信息，用户可以将其导入到管理主机的 MIB 浏览器，进行使用。

Trap 报文信息

设备的 SNMP 代理功能在设备发生异常情况时，会主动向网络管理平台发送 Trap 报文报告所发生的事件。 设备的 SNMP 代理可以生成以下各种 trap 信息：

- 热启动 trap
- SNMP 验证失败 trap
- 端口状态改变trap
- VPN SA 协商状态改变trap
- HA 状态改变trap
- 系统状态改变trap， 如CPU 使用率超过 80%的 trap、风扇状态改变 trap、内存过低 trap 等
- 网络攻击trap， 如 ARP 欺骗攻击 trap、IP 地址欺骗攻击trap、SYN Flood 攻击 trap 等
- 配置改变trap

配置 SNMP

设备的 SNMP 的配置包括以下各项：

- 开启或者关闭SNMP 代理功能
- 配置 SNMP 代理设备端口号
- 配置 SNMP 引擎 ID
- 创建 SNMPv3 用户组
- 创建 SNMPv3 用户
- 配置管理主机地址
- 配 置 trap 报文目标主机地址
- 配置管理员的标识及联系方法
- 配置设备位置
- 指定启用 SNMP 功能的虚拟路由器

开启或者关闭 SNMP 代理功能

默认情况下，系统的 SNMP 代理功能是关闭的。开启 设备的 SNMP 代理功能，请在全局配置模式下使用以下命令。用该命令 no 的形式关闭 SNMP 代理功能。

- snmp-server manager

- **no snmp-server manager**

配置 SNMP 代理设备端口号

配置 SNMP 代理设备端口号，在全局配置模式下，使用以下命令：

snmp-server port *port-number*

- *port-number* – 指定 SNMP 代理设备的端口号。范围为 1 到 65535。默认值为 161。

配置 SNMP 引擎 ID

SNMP 引擎 ID 唯一标识一个引擎，SNMP 引擎是 SNMP 实体（网络管理平台或者被管理网络设备）的重要组成部分，完成 SNMP 消息的收发、验证、提取PDU、组装消息与 SNMP 应用程序通信等功能。配置本地设备的 SNMP 引擎 ID，在全局配置模式下使用以下命令：

snmp-server engineID *string*

- *string* – 指定引擎 ID 号。取值范围为 1 到 23 个字符。

创建 SNMPv3 用户组

配置 SNMPv3 用户组，请在全局配置模式下使用以下命令：

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

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

系统最多允许配置 5 个用户组，且每个用户组最多可包含 5 个用户。在全局配置模式下使用 **no snmp-server group** *group-name* 命令删除指定的用户组。

创建 SNMPv3 用户

配置 SNMPv3 用户，请在全局配置模式下使用以下命令：

snmp-server user *user-name* **group** *group-name* **v3 remote** *A.B.C.D/M* [**auth-protocol** {**md5** | **sha**} *auth-pass* [**enc-protocol** {**des** | **aes**} *enc-pass*]]

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

系统最多允许配置 25 个用户。在全局配置模式下使用 **no snmp-server user** *user-name* 命令删除指定的用户。

配置管理主机地址

配置管理主机地址，请在全局配置模式下使用以下命令：

snmp-server host { *ip-address* | *ip-address/mask* | **range** *start-ip end-ip*} {**version** [*1* | *2c*] **community** *string* [**ro** | **rw**] | **version** *3*}

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

全局配置模式下使用 **no snmp-server host** {*host-name* | *ip-address* | *ip-address/mask* | **range** *start-ip end-ip*} 命令删除指定的管理主机。

配置 trap 报文目标主机地址

用户可以配置接收 SNMP trap 报文的主机。配置 SNMP trap 报文目标主机地址，请在全局配置模式下使用以下命令：

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

- *host-ip* – 指定 trap 报文目标主机的 IP 地址。
- **port** *port-number* – 指定接收 trap 报文的目标主机端口号。取值范围为 1 到 65535，默认值为 162。
- **version** {*1* | *2c*} – 指定使用 SNMPv1 或者 SNMPv2C 发送 trap 报文。
- **community** *string* – 指定 SNMPv1 或者 SNMPv2C 的团体字。
- **version** *3* – 指定使用 SNMPv3 发送 trap 报文。
- **user** *string* – 指定已配置的 SNMPv3 用户名。
- **engineID** *string* – 指定 trap 报文目标主机的引擎 ID 号。
- **port** *port-number* – 指定接收 trap 报文的目标主机端口号。取值范围为 1 到 65535，默认值为 162。

在全局配置模式下使用 **no snmp-server trap-host** {*host-name* | *ip-address*}命令删除指定的 trap 报文目标主机。

配置管理员的标识及联系方法

sysContact 即系统联络，是MIB II 中系统组的一个管理变量，内容为被管理设备（此处为设备）相关人员的标识及联系方法。用户可以通过配置此参数，将重要信息存储在设备中，以便出现紧急问题时查询使 用。配置管理员的标识及联系方法，请在全局配置模式下使用以下命令：

snmp-server contact *string*

- *string* – 描述系统联络信息的字符串。取值范围为 1 到 255 个字符。

在全局配置模式下使用 **no snmp-server contact** 命令该系统联系信息。

配置 设备位置

sysLocation 是 MIB 中系统组的一个管理变量，用于表示被管理设备（此处为设备）的位置。指定 设备的位置，请在全局配置模式下使用以下命令：

snmp-server location *string*

- *string* – 描述设备位置的字符串。取值范围为 1 到 255 个字符。在

全局配置模式下使用 **no snmp-server location** 命令删除系统位置信息。

指定启用 SNMP 功能的 VRouter

用户可以指定启用 SNMP 功能的 VRouter。指定启用 SNMP 功能的VRouter，请在全局配置模式下使用以下命令：

snmp-server vrouter *vrouter-name*

- *vrouter-name* – 指定VRouter 的名称。

在全局配置模式下使用 **no snmp-server vrouter** 命令关闭指定 VRouter 的 SNMP 功能。

配置 SNMP 服务器

用户可以配置 SNMP 服务器，从而通过 SNMP 协议来获取相关的ARP 信息。配置 SNMP 服务器，在全局配置模式下，使用以下命令：

arp-mib-query server *ip-address* **community** *string* [**vrouter** *vrouter-name*] [**source** *interface-name*] [**port** *port-number*] [**interval** *value*]

- *ip-address* – 指定 SNMP 服务器的 IP 地址。
- **community** *string* – 指定 SNMPv1 或者 SNMPv2C 的团体字，取值范围为一个最多 31 位的字符串。
- **vrouter** *vrouter-name* – 指定 VRouter 的名称。
- **source** *interface-name* – 指定 SNMP 服务器上用来接收 ARP 信息的源接口名称。
- **port** *port-number* – 指定SNMP 服务器的端口号。范围为 1 到 65535。默认值为 161。
- **interval** *value* – 指定 SNMP 服务器上接收ARP 信息的时间间隔，单位为秒，范围是 5 到 1800 秒，默认值是 60 秒。

在全局配置模式下使用 **no arp-mib-query server** *ip-address* 命令删除指定的 SNMP 服务器。

清除 SNMP 服务器的 ARP 表项信息

用户可以在任何模式下通过以下命令清除 SNMP 服务器的 ARP 表项信息：

clear arp-mib-query

显示 SNMP 信息

用户可以在任何模式下通过以下命令查看 SNMP 的相关配置信息：

- 显示设备的 SNMP 配置信息：**show snmp-server**
- 显示设备的 SNMPv3 用户组信息：**show snmp-group**

- 显示设备的 SNMPv3 用户信息：**show snmp-user**

显示 SNMP 服务器信息

用户可以在任何模式下通过以下命令查看 SNMP 服务器的相关信息：

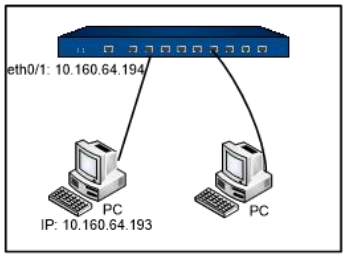
- 显示 SNMP 服务器状态信息：**show arp-mib-query status**
- 显示 SNMP 服务器的ARP 表项信息：**show arp-mib-query table** [*ip-address*]
- 显示 SNMP 服务器配置信息：**show configuration arp-mib-query**

SNMP 配置示例

为方便用户更好的理解和使用设备的 SNMP 功能，本节介绍两个典型的 SNMP 配置示例。

组网要求

网络管理平台与设备通过以太网相连，网络管理平台的 IP 地址为 10.160.64.193， 设备以太网口 IP 地址为 10.160.64.194。请看以下示意图：



- 示例一：通过SNMPv2C 实现 IP 地址为 10.160.64.193 的 PC 对设备的管理，使用团体字 public。另外，允许向网络管理平台 10.160.64.193 发送 trap 报文，使用团体字 private。
- 示例二：通过SNMPv3 实现 IP 地址为 10.160.64.193 的 PC 对设备的管理。安全级别为需要认证和加密，指定认证协议为 MD5、认证密码为 password1，指定加密协议为 DES、加密密码为 password2。同时，PC 只能读取 MIB-II 信息库的内容并且只能对 usm 信息库的内容进行设置。另外，允许向设备发送 trap 报文。

示例一配置步骤

第一步：配置设备：

```
进入全局配置模式
hostname# configure
启动 设备接口的 SNMP 功能
hostname(config)# interface ethernet0/1
```

```
hostname(config-if-eth0/1)# manage snmp
启动 SNMP 功能
hostname(config)# snmp-server manager
配置团体字和访问权限
hostname(config)# snmp-server host 10.160.64.193 version 2c community public ro
配置管理员标识、联系方法以及 设备物理位置
hostname(config)# snmp-server contact cindy-Tel:218
hostname(config)# snmp-server location Hostname-Network
允许向网络管理平台 10.160.64.193 发送 trap 报文，使用的团体字为 private
hostname(config)# snmp-server trap-host 10.160.64.193 version 2c community private
```

第二步：配置网络管理平台。

示例二配置步骤

第一步：配置设备：

```
进入全局配置模式
hostname# configure
启动 设备接口的 SNMP 功能
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# manage snmp
启动 SNMP 功能
hostname(config)# snmp-server manager
配置本地引擎ID
hostname(config)# snmp-server engineID
配置用户组，网络管理平台只能读取 MIB-II 信息库的内容并且可以对 usm 信息库的内容进行设置
hostname(config)# snmp-server group group1 v3 auth-enc read-view mib2 write-view usm
配置用户，认证协议为 MD5，密码为 password1；加密协议为 DES，密码为 password2
```

hostname(config)# **snmp-server user user1 group group1 v3 remote 10.160.64.193 auth md5 password1 enc des password2**

配置管理主机地址

hostname(config)# **snmp-server host** 10.160.64.193 version 3

配置 trap 报文目标主机地址，允许向网络管理平台 10.160.64.193 发送 trap 报文

hostname(config)# snmp-server trap-host 10.160.64.193 version 3 user user1 engineID remote-engineid

配置管理员标识、联系方法以及 设备物理位置

hostname(config)# snmp-server contact cindy-Tel:218

hostname(config)# **snmp-server location Hostname-Network**

第二步：配置网络管理平台。

网络时间协议（NTP）

网络时间协议（Network Time Protocol），简称为 NTP。NTP 为整个网络传递统一、标准的时间。实现方法是在网络上指定若干时钟源，为用户提供授时服务，并且这些时钟服务器间能够相互对比以提高准确 度。NTP 协议采用 UDP 传输协议格式，使用专用端口 123。

设备的时间影响到设备的许多功能模块，例如 VPN 隧道的建立、时间表功能的实现以及自签名证书的使用等，因此系统时间的精确性十分重要。为保证设备系统能够一直保持精确时间， 设备允许用户通过 NTP 来使系统时间与网络上的 NTP 服务器同步。 设备支持两种设置时间的方式，分别是手动设置和通过 NTP 与服务器同步。

> 注意:为保证自签名证书时间的正确性，避免证书使用错误，初次使用设备时，请务必将设备时间与 PC 时间同步。

配置 NTP

手动配置时间

手动配置系统的时间，在全局配置模式下，使用以下命令:

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

- *HH:MM:SS Month Day Year* - 指定系统时间。HH、MM 和 SS 分别表示小时、分钟和秒，Month、Day 和Year 分别表示月、日和年。

手动配置时区

系统提供多个预定义时区，同时，为实现更精确的时区配置，系统支持自定义时区配置，并且，用户可以为自定义时区指定夏令时。

系统的默认时区是东 8 区。为系统指定时区，在全局配置模式下，使用以下命令：

clock zone {*timezone-name* | *cus-timezone-name hours minutes*}

- *timezone-name* - 指定预定义时区名称。
- *cus-timezone-name* - 指定自定义时区名称，范围是 1 到 6 个字符。
- *hours minutes* – 为自定义时区指定相对 UTC（Universal Time Coordinated，协调世界时）时间的偏移量。hours 的取值范围是-13 到 12；minutes 的取值范围是 0 到 59。

配置夏令时

夏令时（summer-time）是为节约能源而人为规定的地方时间制度。按国家法令，在夏季及其前后实施。一般在天亮早的夏季人为将时间提前一小时，夏季结束再将时间调回一小时。用户可以为系统自定义时区指定夏令时的绝对时间段和循环时间段。

为系统指定夏令时的绝对时间段，在全局配置模式下，使用以下命令：

clock summer-time *cus-timezone-name* **date** *start-date start-time end-date end-time* [*compensation-time*]

- *cus-timezone-name* – 指定自定义时区名称，范围是 1 到 6 个字符。
- **date** – 指定夏令时的绝对时间段。
- *start-date* – 指定夏令时起始日期。书写格式为“月/日/年”，例如 7/20/2011。
- *start-time* – 指定夏令时起始时间。书写格式为“小时：分钟”，例如 10:30。
- *end-date* – 指定夏令时终止日期。书写格式为“月/日/年”，例如 7/20/2011。
- *end-time* - 指定夏令时终止时间。书写格式为“小时：分钟”，例如 10:30。
- *compensation-time* – 指定夏令时生效时的时间补偿，默认值为 0。例如夏令时开始时，某些地区时间须调快 1 小时 30 分；夏令时结束时，时间须调慢 1 小时 30 分。“1 小时 30 分”即为夏令时生效时的时间补偿。书写格式为“小时：分钟”，例如 1:30。

例如：

自定义时区`test`的夏令时从`6/22/2011`的`10:30`开始，到`9/23/2011`的`10:00`结束。夏令时期间的时间将比非夏令时期间的时间快`2`小时`30`：

hostname（config）# **clock summer-time test date 6/22/2011 10:30 9/23/2011 10:00 2:30**

为系统指定夏令时的循环时间段，即在每年的指定时间段内，执行夏令时。在全局配置模式下，使用以下命令：

clock summer-time *cus-timezone-name* **recurring** { [**Mon**] | [···] | [**Sun**] } {**after** | **before**} *start-day start-month start-time* { [**Mon**] | [···] | [**Sun**]} {**after** | **before**} *end-day end-month end-time* [**compensation-time**]

- *cus-timezone-name* – 指定自定义时区名称，范围是 1 到 6 个字符。
- **recurring** – 指定夏令时的循环时间段。
- { [**Mon**] | [···] | [**Sun**] } {**after** | **before**} *start-day start-month start-time* – 指定夏令时循环时间段的起始时间。例如命令关键字为 **Mon before 22 6 10:30**，即夏令时起始时间为每年 6 月 22 日前的第一个周一的 10:30。
- { [**Mon**] | [···] | [**Sun**]} {**after** | **before**} *end-day end-month end-time* – 指定夏令时循环时间段的终止时间。例如命令关键字为 **Fri after 23 9 10:00**，即夏令时终止时间为每年 9 月 23 日后的第一个周五的 10:00。
- *compensation-time* – 指定夏令时生效时的时间补偿，默认值为 0。例如夏令时开始时，某些地区时间须调快 1 小时 30 分；夏令时结束时，时间须调慢 1 小时 30 分。“1 小时 30 分”即为夏令时生效时的时间补偿。书写格式为“小时：分钟”，例如 1:30。

例如：

自定义时区`test`的夏令时在从每年的 6 月 22 日前的第一个周一的`10:30`开始，到 9 月 23 日后的第一个周五的`10:00`结束。夏令时期间的时间将比非夏令时期间的时间快 2 小时`30`：

hostname（config）# **clock summer-time test recurring Mon before 22 6 10:30 Fri after 23 9 10:00 2:30**

注意:夏令时的配置会对日志和基于时间的功能模块产生影响。例如，当 9/23/2011 的 10:00 夏令时结束时，系统时间将自动调慢 2 小时 30 分，恢复为非夏令时期间的 7:30。这样，9/23/2011 的 7:30 到 10:00 在这一天会出现两次。

使用 **no clock summer-time** *cus-timezone-name* **date** 命令取消夏令时的配置。

查看系统时间配置信息

在 CLI 任何命令模式下使用 **show clock** 命令，查看当前的时区配置信息。

在 CLI 任何命令模式下使用 **show config** 命令，查看当前的夏令时配置信息。

配置 NTP 功能

通过 NTP 配置，可以使设备的系统时间与时钟服务器同步。在设备上可以做的 NTP 配置有以下各项：

- 开启/关闭 NTP 功能

- 配置 NTP 服务器
- 配置最大调整时间
- 配置查询间隔
- 开启/关闭身份验证功能
- 配置 NTP 身份验证功能

开启/关闭 NTP 功能

默认情况下，系统的 NTP 功能是关闭的。在设备上开启或者关闭 NTP 功能，在全局配置模式下使用以下命令：

- 启用：**ntp enable**
- 禁用：**no ntp enable**

配置 NTP 时钟服务器

用户最多可以指定 3 个时钟服务器，同时可以使用 **prefer** 关键字指定主时钟服务器（设备首先与主服务器进行时间同步）；如果没有为服务器指定 **prefer** 关键字，设备会使用户最先配置的服务器做时间同步。配置 NTP 时钟服务器，请在全局配置模式下输入以下命令：

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

- *ip-address* | *host-name* – 指定时钟服务器的 IP 地址或主机名称。主机名称取值范围为 1 到 127 个字符。
- **key** *number* – 指定可以通过该服务器的验证密钥。如果要在配置的时钟服务器上使用 NTP 身份验证功能，用户必须指定 **key** 参数值。
- **source** *interface-name* – 指定设备上发送和接收 NTP 包的接口。
- **prefer** – 如果指定了多个时钟服务器，该关键字用来指定该服务器为主时钟服务器。设备首先与主服务器进行时间同步，如果失败，再查找下一个时钟服务器。
- *vrouter-name* - 为指定的 VRouter 指定时钟服务器。

使用 **no ntp server** {*ip-address* | *host-name*}命令取消指定时钟服务器的配置。

以下是时钟服务器配置示例：

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

配置最大调整时间

如果设备和 NTP 时钟服务器的时间差在最大调整时间之内，就能成功进行时间同步，否则同步不成功。配置最大调整时间，在全局配置模式下，输入以下命令：

ntp max-adjustment *time-value*

- *time-value* – 最大调整时间值。范围是 0 到 3600 秒，0 表示没有时间限制。默认值是 10 秒。

使用 **no ntp max-adjustment** 命令恢复最大调整时间的默认值。

配置查询间隔

设备每隔一个查询间隔就与时钟服务器做一次同步，保证设备系统时间的准确。配置查询间隔，在全局配置模式下，输入以下命令：

ntp query-interval *time-interval*

- *time-interval* – 查询间隔值。范围是 1 到 60 分钟。默认值是 5 分钟。

使用 **no ntp query-interval** 命令恢复查询间隔的默认值。

开启/关闭身份验证功能

默认情况下，系统的 NTP 身份验证功能是关闭的。在 设备上开启或者关闭NTP 身份验证功能，在全局配置模式下使用以下命令：

- 启用：**ntp authentication**
- 禁用：**no ntp authentication**

配置 NTP 身份验证功能

使用 NTP 身份验证功能，用户需要配置 MD5 身份验证密钥 ID 和密钥。启动该功能后，设备只会与通过验证的服务器进行同步。配置 NTP 验证密钥 ID 和密钥，请在全局配置模式下，输入以下命令：

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

- *number* - 验证密钥 ID，范围是从 1 到 65535;
- *string* - MD5 验证密钥，范围是 1 到 31 个字符。

在全局配置模式下，使用 **no ntp authentication-key** *number* 命令取消验证密钥的配置。

查看 NTP 状态

NTP 配置完成后，在任何模式下运行 **show ntp status** 命令可以查看当前的 NTP 配置信息和 NTP 状态。

NTP 配置示例

NTP 服务器的 IP 地址是 10.10.10.10；身份验证密钥 ID 和 MD5 验证密钥分别是 1 和 aaaa；查询间隔为 3 分钟；最大调整时间为 5 秒。配置完成后开启设备的 NTP 身份验证功能和 NTP 功能。最后查看 NTP 配置信息和状态。请参考以下配置命令:

```
hostname(config)# ntp authentication-key 1 md5 aaaa
hostname(config)# ntp server 10.10.10.10 key 1 prefer
hostname(config)# ntp query-interval 3
hostname(config)# ntp max-adjustment 5
hostname(config)# ntp authentication
hostname(config)# ntp enable
hostname(config)# show ntp status
ntp client is enabled, authentication is enabled
ntp query-interval is 3, max-adjustment time is 5
ntp server 10.10.10.10, key 1, prefer
```

配置时间表功能

设备支持时间表（Schedule）功能。时间表功能可以使策略规则在指定的时间生效，也可以控制 PPPoE 接口与因特网的连接时间。时间表包含绝对计划和周期计划。周期计划通过周期条目指定时间表的时间点或者时间段；而绝对计划决定周期计划的生效时间。每个周期计划最多可以拥有 16 条周期条目。

创建时间表

创建一个时间表，在全局配置模式下，使用以下命令:

schedule *schedule-name*

- *schedule-name* – 指定时间表的名称。范围是 1 到 31 个字符。

执行该命令后，系统创建指定名称的时间表并且进入时间表配置模式；如果指定的名称已存在，则直接进入时间表配置模式。在时间表配置模式下，用户可以配置时间表的周期和绝对时间。

使用 **no schedule** *schedule-name* 命令删除指定的时间表。删除时间表之前，请从其它模块中取消对该时间表的引用。

指定绝对计划

绝对计划是一个时间范围，指定的周期计划会在绝对计划的时间范围内生效。同时，用户也可以不启用绝对计划功能，此时周期计划会在被应用到系统中某项功能上时，立即生效。指定绝对计划，在时间表配置模式下，使用以下命令：

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

- **start** *start-date start-time* – 指定绝对计划的开始时间点，包括日期和具体时间。start-date 为开始的日期，书写格式为“月/日/年”，例如 10/23/2007；start-time 为开始的具体时间，书写格式为“小时：分钟”，例如 15：30。如果不指定该参数的值，开始时间为当前时间。
- **end** *end-date end-time* – 指定绝对计划的结束时间点，包括日期和具体时间。end-date 为结束的日期，书写格式为“月/日/年”，例如 11/05/2007；end-time 为结束的具体时间，书写格式为“小时：分钟”，例如 09：00。如果不指定该参数的值，则无结束时间，周期会从开始时间起，一直有效。

使用 **no absolute** 命令关闭绝对计划功能，使周期计划能够即时生效。

指定周期计划

周期计划的时间是该周期计划中周期条目的总和。一个周期计划中最多可以添加 16 个条周期条目。用户可以配置三种类型的周期条目：

- 每天：每天的指定时间。例如每天的 9：00 到 18：00。
- 每周的某几天：一周中指定天的指定时间。例如每周一、周二和周六的 9：00 到 13：30。
- 每周一段时间：一周中的一个连续时间段。例如从周一早上 9：30 到周三下午 15：00。

指定“每天”或者“每周的某几天”类型周期条目，在时间表配置模式下，使用以下命令：

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

- **daily** – 每一天（周一到周日）。
- **weekdays** – 工作日（周一到周五）。
- **weekend** – 周末（周六到周日）。
- [**monday**] [···] [**sunday**] – 选择需要的日期。例如选择周二、周三和周六，命令关键字为 **tuesday wednesday saturday**。
- *start-time* – 开始时间。书写格式为“小时：分钟”，例如 09：00。
- *end-time* – 结束时间。书写格式为“小时：分钟”，例如 16：30。

使用多条该命令添加多个“每天”或者“每周的某几天”类型周期条目。

使用 **no periodic** {**daily** | **weekdays** | **weekend** | [**monday**] [···] [**sunday**]} *start-time* **to** *end-time* 命令删除指定的周期条目。

指定“每周一段时间”类型周期条目，在时间表配置模式下，使用以下命令：

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

- [**monday**] | [···] | [**sunday**] – 开始日期，可以是周一到周日的任意一天。
- *start-time* – 开始时间。书写格式为“小时：分钟”，例如 09：00。
- [**monday**] | [···] | [**sunday**] – 结束日期，与开始日期相同或者晚于开始日期。
- *end-time* – 结束时间。书写格式为“小时：分钟”，例如 16：30。

使用多条该命令添加多条“每周一段时间”类型周期条目。

使用 **no periodic** {[**monday**] | [···] | [**sunday**]} *start-time* **to** {[**monday**] | [···] | [**sunday**]} *end-time* 命令删除指定的周期条目。

配置监测对象

系统的监测功能能够监测指定的目标（IP 地址或者主机）是否可达或者接口的链路是否连通，以及监测目标或接口链路是否出现拥塞。如果监测目标不可达或接口链路没有连通，系统会直接判断监测失败；如果监测目标可达或接口链路连通，系统可以继续根据报文延时和接口流量判断监测目标或链路是否出现拥塞。监测功能主要用在HA、策略路由、链路负载均衡等场景，用户可以通过配置监控功能确保系统始终选择相对健康的链路。

注意：

- 监测失败后，系统会断开到监测对象的所有会话。
- 出现拥塞后，系统仍会保留到监测对象的所有会话，但不允许新建会话。

配置监测功能，首先需配置监测对象，在全局配置模式下，使用以下命令：

track *track-object-name* [**local**]

- *track-object-name* – 指定监测对象名称。范围是 1 到 31 个字符。
- **local** – 若指定该参数，系统将不向备份设备同步该监测对象的相关配置信息。默认情况下，不指定该参数。

执行该命令后，系统创建指定名称的监测对象，并且进入监测对象配置模式；如果指定的名称已存在，则直接进入监测对象的配置模式。使用该命令 no 的形式删除指定的监测对象：

no track *track-object-name*

系统支持通过 ICMP 报文、HTTP 报文、ARP 报文、DNS 报文和 TCP 报文五种方式对目标进行主动监测，还支持通过统计指定接口的流量信息对目标进行被动监测。

ICMP 报文监测

通过 ICMP 报文对目标进行监测，在监测对象配置模式下使用以下命令：

icmp {*A.B.C.D* | **host** *host-name*} **interface** *interface-name* [**interval** *value*] [**threshold** *value*] [**src-interface** *interface-name* [**prior-used-srcip**]] [**weight** *value*] [**delay high-watermark** *value* **low-watermark** *value*] [**delay-weight** *value*]

- *A.B.C.D* | **host** *host-name* – 指定监测目标的 IP 地址或者主机名称。主机名称范围是 1 到 63 个字符。
- **interface** *interface-name* – 指定发送Ping 检测报文的出接口。
- **interval** *value* – 指定发送Ping 报文的时间间隔，单位为秒。范围是 1 到 255 秒。默认值是 3 秒。
- **threshold** *value* – 指定判断监测失败的警戒值。如果系统连续未收到该参数指定个数的响应报文，就判断为监测失败，即目标不可达。取值范围是 1 到 255。默认值是 3。
- **src-interface** *interface-name* – 指定 Ping 检测报文的源接口。
- **prior-used-srcip** – 若源接口上已配置多个 IP，将其中一个 IP 指定为 **prior-used-srcip** 后，系统将使用此 IP 发送 track 报文；若没有指定该参数，则使用默认的源接口主 IP 发送 track 报文。
- **weight** *value* – 指定该条监测失败对整个监测对象失败贡献的权重值。取值范围是 1 到 255。默认值是 255。
- **delay high-watermark** *value* **low-watermark** *value* – 指定监测目标响应 Ping 报文延时的高水位线和低水位线，单位为毫秒。取值范围是 1 到 65535 毫秒。延时小于指定的高水位线，系统会判断链路为正常状态；延时大于或等于指定的高水位下，系统会判断出现链路拥塞；出现链路拥塞后，只有在延时小于或等于指定的低水位线后系统才会判断链路恢复正常状态。这种高低水位线的设计可以有效的防范链路在正常与拥塞状态之间频繁切换。
- **delay-weight** *value* – 指定该条监测出现链路拥塞对整个监测对象出现链路拥塞所贡献的权重值。取值范围是 1 到 255。默认值是 255。

用户可以配置多条该命令为监测对象指定多个监测条目。使用该命令 no 的形式删除指定的监测条目：

no icmp {*A.B.C.D* | **host** *host-name*} **interface** *interface-name* [**delay**]

HTTP 报文监测

通过 HTTP 报文对目标进行监测，在监测对象配置模式下使用以下命令：

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

- *A.B.C.D* | **host** *host-name* – 指定监测目标的 IP 地址或者主机名称。主机名称范围是 1 到 63 个字符。
- **interface** *interface-name* – 指定发送 HTTP 检测报文的出接口。
- **interval** *value* – 指定发送 HTTP 报文的时间间隔，单位为秒。范围是 1 到 255 秒。默认值是 3 秒。
- **threshold** *value* – 指定判断监测失败的警戒值。如果系统连续未收到该参数指定个数的响应报文，就判断为监测失败，即目标不可达。取值范围是 1 到 255。默认值是 3。
- **src-interface** *interface-name* – 指定 HTTP 检测报文的源接口。
- **weight** *value* – 指定该条监测失败对整个监测对象失败贡献的权重值。取值范围是 1 到 255。默认值是 255。
- **delay high-watermark** *value* **low-watermark** *value* – 指定监测目标响应 HTTP 报文延时高水位线和低水位线，单位为毫秒。取值范围是 1 到 65535 毫秒。延时小于指定的高水位线，系统会判断链路为正常状态；延时大于或等于指定的高水位下，系统会判断出现链路拥塞；出现链路拥塞后，只有在延时小于或等于指定的低水位线后系统才会判断链路恢复正常状态。这种高低水位线的设计可以有效的防范链路在正常与拥塞状态之间频繁切换。
- **delay-weight** *value* – 指定该条监测出现链路拥塞对整个监测对象出现链路拥塞所贡献的权重值。取值范围是 1 到 255。默认值是 255。

用户可以配置多条该命令为监测对象指定多个监测条目。使用该命令 no 的形式删除指定的监测条目：

no http {*A.B.C.D* | **host** *host-name*} **interface** *interface-name* [**delay**]

ARP 报文监测

通过ARP 报文对目标进行监测，在监测对象配置模式下使用以下命令：

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

- *A.B.C.D* – 指定监测目标的 IP 地址。
- **interface** *interface-name* – 指定发送ARP 检测报文的出接口。
- **interval** *value* – 指定发送ARP 报文的时间间隔，单位为秒。范围是 1 到 255 秒。默认值是 3 秒。
- **threshold** *value* – 指定判断监测失败的警戒值。如果系统连续未收到该参数指定个数的响应报文，就判断为监测失败，即目标不可达。取值范围是 1 到 255。默认值是 3。

- **weight** *value* – 指定该条监测失败对整个监测对象失败贡献的权重值。取值范围是 1 到 255。默认值是 255。

用户可以配置多条该命令为监测对象指定多个监测条目。使用该命令 no 的形式删除指定的监测条目：

no arp {*A.B.C.D*} **interface** *interface-name*

DNS 报文监测

通过DNS 报文对目标进行监测，在监测对象配置模式下使用以下命令：

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

- *A.B.C.D* – 指定监测目标的 IP 地址。
- **interface** *interface-name* – 指定发送DNS 检测报文的出接口。
- **interval** *value* – 指定发送DNS 报文的时间间隔，单位为秒。范围是 1 到 255 秒。默认值是 3 秒。
- **threshold** *value* – 指定判断监测失败的警戒值。如果系统连续未收到该参数指定个数的响应报文，就判断为监测失败，即目标不可达。取值范围是 1 到 255。默认值是 3。
- **weight** *value* – 指定该条监测失败对整个监测对象失败贡献的权重值。取值范围是 1 到 255。默认值是 255。
- **src-interface** *interface-name* – 指定 DNS 检测报文的源接口。
- **delay high-watermark** *value* **low-watermark** *value* – 指定监测目标响应 DNS 报文延时高水位线和低水位线，单位为毫秒。取值范围是 1 到 65535 毫秒。延时小于指定的高水位线，系统会判断链路为正常状态；延时大于或等于指定的高水位下，系统会判断出现链路拥塞；出现链路拥塞后，只有在延时小于或等于指定的低水位线后系统才会判断链路恢复正常状态。这种高低水位线的设计可以有效的防范链路在正常与拥塞状态之间频繁切换。
- **delay-weight** *value* – 指定该条监测出现链路拥塞对整个监测对象出现链路拥塞所贡献的权重值。取值范围是 1 到 255。默认值是 255。

用户可以配置多条该命令为监测对象指定多个监测条目。使用该命令 no 的形式删除指定的监测条目：

no dns *A.B.C.D* **interface** *interface-name* [**delay**]

TCP 报文监测

通过 TCP 报文对目标端口进行监测，在监测对象配置模式下使用以下命令：

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

- *A.B.C.D* | **host** *host-name* – 指定监测目标的 IP 地址或者主机名称。主机名称范围是 1 到 63 个字符。
- **port** *port-number* – 指定监测目标的目的端口号。取值范围为 0 到 65535。
- **interface** *interface-name* – 指定发送 TCP 检测报文的出接口。
- **interval** *value* – 指定发送 TCP 报文的时间间隔，单位为秒。范围是 1 到 255 秒。默认值是 3 秒。
- **threshold** *value* – 指定判断监测失败的警戒值。如果系统连续未收到该参数指定个数的响应报文，就判断为监测失败，即目标不可达。取值范围是 1 到 255。默认值是 3。
- **src-interface** *interface-name* – 指定 TCP 检测报文的源接口。
- **weight** *value* – 指定该条监测失败对整个监测对象失败贡献的权重值。取值范围是 1 到 255。默认值是 255。
- **delay high-watermark** *value* **low-watermark** *value* – 指定监测目标响应 TCP 报文延时的高水位线和低水位线，单位为毫秒。取值范围是 1 到 65535 毫秒。延时小于指定的高水位线，系统会判断链路为正常状态；延时大于或等于指定的高水位下，系统会判断出现链路拥塞；出现链路拥塞后，只有在延时小于或等于指定的低水位线后系统才会判断链路恢复正常状态。这种高低水位线的设计可以有效的防范链路在正常与拥塞状态之间频繁切换。
- **delay-weight** *value* – 指定该条监测出现链路拥塞对整个监测对象出现链路拥塞所贡献的权重值。取值范围是 1 到 255。默认值是 255。

用户可以配置多条该命令为监测对象指定多个监测条目。对于同一个监测对象，不能同时配置对同一目标主机的 HTTP 监测和对端口 80（**port** 80）的 TCP 监测。使用该命令 no 的形式删除指定的监测条目：

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

接口链路状态监测

配置监测接口的链路状态，在监测对象配置模式下使用以下命令：

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

- *interface-name* – 指定被监测接口的名称。
- **weight** *value* – 指定该条监测失败对整个监测对象失败贡献的权重值。取值范围是 1 到 255。默认值是 255。

用户可以配置多条该命令为监测对象指定多个监测条目。使用该命令 no 的形式删除指定的监测条目：

no interface *interface-name*

接口带宽监测

配置监测接口带宽，在监测对象配置模式下使用以下命令：

bandwidth interface *interface-name* **direction** {**in** | **out** | **both**} **high-watermark** *value* **low-watermark** *value* [**interval** *value*] [**threshold** *value*] [**weight** *value*]

- *interface-name* – 指定被监测接口的名称。
- **direction** {**in** | **out** | **both**} – 指定监测的流量方向。**in** 指流入方向，**out** 指流出方向，**both** 指双方向。默认为流出方向（**out**）。
- **high-watermark** *value* **low-watermark** *value* – 指定接口流量的高水位线和低水位线，单位为 kbps。取值范围是 1 到 100000000kbps。接口流量小于指定的高水位线，系统会判断链路为正常状态；接口流量大于或等于指定的高水位下，系统会判断出现链路拥塞；出现链路拥塞后，只有在接口流量小于或等于指定的低水位线后系统才会判断链路恢复正常状态。这种高低水位线的设计可以有效的防范链路在正常与拥塞状态之间频繁切换。
- **interval** *value* – 指定监控接口流量的间隔时间，单位为秒。取值范围是 1 到 255 秒。默认值是 1 秒。
- **threshold** *value* – 指定判断该条监测出现拥塞的警戒值。如果系统连续检测到参数指定次数的链路过载情况，就判断该条监测出现拥塞。取值范围是 1 到 255。默认值是 3。
- **weight** *value* – 指定该条监测出现拥塞对整个监测对象出现拥塞贡献的权重值。取值范围是 1 到 255。默认值是 255。

用户可以配置多条该命令为监测对象指定多个监测条目。使用该命令 no 的形式删除指定的监测条目：

no bandwidth interface *interface-name*

接口链路质量监测

通过统计指定接口的采样流量信息，系统可以监测该接口的链路状态。配置接口链路对象监测，在监测对象配置模式下使用以下命令：

traffic-condition interface *interface-name* [**condition-threshold** *low-watermark high-watermark*] [**interval** *value*] [**threshold** *value*] [**weight** *value*]

- *interface-name* – 指定被监测接口的名称。
- **condition-threshold** *low-watermark high-watermark* – 指定每个监测周期的新建会话成功率阈值。默认情况下，失败界定阈值为 30，成功界定阈值为 50。取值范围是 0 到 100。在某个监测周期内，当新建会话成功率小于指定的失败界定阈值时，判断为监测失败；当新建会话成功率大于指定的成功界定阈值时，判断为监测成功；当新建会话成功率大于等于失败界定阈值且小于等于成功界定阈值时，系统保持原来的监测状态。

- **interval** *value* – 指定每个监测周期的持续时间，单位为秒。取值范围是 1 到 255 秒。默认值是 3 秒。每个监测周期结束后，系统会重置探测到的新建会话相关数值。
- **threshold** *value* – 指定判断监测失败的警戒值。如果系统连续检测到参数指定次数的监测失败情况，就判断该条监测失败。取值范围是 1 到 255。默认值是 3。
- **weight** *value* – 指定该条监测失败对整个监测对象失败贡献的权重值。取值范围是 1 到 255。默认值是 255。

用户可以配置多条该命令为监测对象指定多个监测条目。使用该命令 no 的形式删除指定的监测条目：

no traffic-condition interface *interface-name*

系统监控报警

StoneOS 的系统监控报警功能能够监控系统资源的使用状况，并根据配置发出报警信息。当前版本支持的报警方式为日志信息和 SNMP Trap 信息。

配置系统监控报警功能，首先要进入监控配置模式。进入监控配置模式，在全局配置模式下，使用以下命令：

monitor

进入监控配置模式后，用户可以根据需要监控的系统资源对象，设置相应的监控规则：

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

- **cpu** | **memory utilization** | **interface-bandwidth** *interface-name* **utilization** | **log-buffer** { **config** | **event** | **ips** | **nbc** | **network** | **security** | **traffic** {**session** | **nat** | **urlfilter**}} **utilization** | **policy utilization** | **session utilization** | **snat-resource utilization** – 指定监控对象，可以为系统 CPU（**cpu**）、内存（**memory**）、接口带宽（**interface-bandwidth**）、日志容量（**log-buffer**）、策略数（**policy**）、会话（**session**）和 SNAT 转换后的 IP 地址端口资源（**snat-resource**）。当用户设备为 X 平台时，选择 CPU 监控对象后，需要继续选择对应的板卡。
  - *interface-name* – 指定监控的接口名称。
  - **config** | **event** | **ips** | **network** | **security** | **traffic** {**session** | **nat** | **urlfilter**} – 指定具体的日志类型。
  - **utilization** – 指定监控值为各对象的利用率。CPU（cpu）的监控值默认为利用率，不需要指定。

- **interval** *interval-value* – 指定监控间隔，即系统在报警计算时间段（**sample-period** *period-value*）内，每次取值后等待的时间间隔。取值范围为 3 到 10 秒。
- **absolute** – 指定监控值为绝对值。
- **rising-threshold** *threshold-value* – 指定上升阈值，即实际监控值超过该阈值满足报警条件的百分比。取值范围为 1 到 99。
- **sample-period** *period-value* – 指定报警计算时间段。取值范围为 30 到 3600 秒。
- **count** *count-value* – 指定在报警计算时间段（**sample-period**）内，监控对象的实际监控数值超过阈值（**rising-threshold**）的次数。取值范围为 1 到 1000。如果配置该参数，在监控时间段内，若监控对象值超过阈值的次数大于该count 值，则发出警告；如果不配置该参数，在监控时间段内，若监控对象值的平均值大于阈值（**rising-threshold**），则发出警告。
- **log** [**snmp-trap**] | **snmp-trap** – 指定报警方式。可以使用日志（**log**）或者 SNMP Trap 报文（**snmp-trap**），也可以同时使用这两种报警方式。

例如：

配置 CPU 峰值监控：

hostname(config)# **monitor**

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

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

配置会话均值监控：

hostname(config)# **monitor**

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

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

在监控配置模式下使用该命令 no 的形式删除指定的监控规则：

no {**cpu** | **memory utilization** | **interface-bandwidth** interface-name **utilization** | **log-buffer** { **config** | **event** | **ips** | **network** | **security** | **traffic** {**session** | **nat** | **urlfilter**}} **utilization** | **policy utilization** | **session utilization** | **snat-resource utilization**}

注意：

- 不支持对 SNAT 转换后地址为出接口 IP 地址（eif-ip）的端口资源的监控报警；
- 对于每种监控对象，只有最后配置的一条监控规则生效。

查看系统监控报警配置，在任意模式下，使用以下命令：

show monitor

系统监控报警功能的日志信息类别为事件（Event），严重等级为严重（Critical）。用户可以查看系统事件日志信息，或者配置事件日志 email 提醒功能将日志信息发送到管理员邮件。关于如何配置系统日志的详细信息，请参阅《监控》的“日志”。

查看系统监控严重等级为严重（Critical）以上的事件日志，在任意模式下，使用以下命令：

show logging alarm [**severity** *severity-level*]

系统最大并发连接数变化

在 设备部分平台上开启多VR、病毒过滤、入侵防御、URL 特征库、沙箱防护、反垃圾邮件、僵尸网络防御、NetFlow 等功能后，或者使用 IPv6 版本系统软件，系统的最大并发连接数会发生变化。下表列出设备平台型号、系统文件版本以及相应的系统最大并发连接数的变化情况。

第 5 章 高可靠性

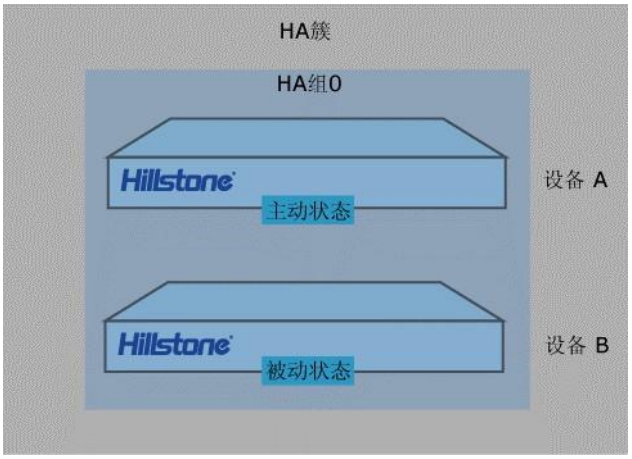
介绍

高可靠性（High Availability），简称为 HA，能够在通信线路或设备产生故障时提供备用方案，从而保证数据通信的畅通，有效增强网络的可靠性。实现 HA 功能，用户需要配置两台采用完全相同的硬件平台、固件版本，均安装相同的许可证、且所有接口对应关系一致的设备组成 HA 簇。当一台设备不可用或者不能处理来自客户端的请求时，该请求会及时转到另外的可用设备来处理，这样就保证了网络通信的不间断进行，极大地提高了通信的可靠性。

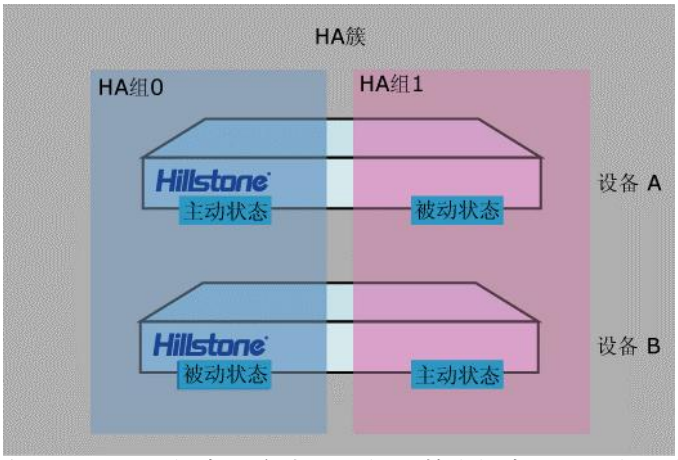
设备支持 HA 的 2 种工作模式：Active-Passive（A/P）模式、Active-Active（A/A）模式：

- Active-Passive（A/P）模式：在 HA 簇中配置两台设备组成一个 HA 组，组内只有一台主设备。主设备处于活动状态，转发报文，同时将其所有网络和配置信息以及当前会话信息传递给备份设备。当主设备出现故障时，备份设备接替主设备工作，转发报文。这种 A/P 模式具有较强冗余性，而

且其网络结构简单，便于维护管理。A/P 模式设备关系图如下图所示：



- Active-Active（A/A）模式：当安全设备处于 NAT 模式、路由模式或两者的组合时，可以将HA 簇中的两台设备都配置成主动，使两台设备同时运行各自的工作，且相互监测对方的情况。当其中一台设备发生故障时，另外一台设备运行其自身的工作并且接管故障设备的工作，以保证工作不间 断，该模式称为Active-Active 模式。这种A/A 模式具有高性能以及负载均衡的优点。A/A 模式设备关系图如下图所示：



如上图所示，设备A 充当 HA 组 0 的主设备和 HA 组 1 的备份设备。设备B 充当HA 组 1 的主设备和 HA 组 0 的备份设备。充当HA 组 0 的主设备被称为Admin Master，充当 HA 组 1 的主设备被称为 Master。

配置 HA Active-Active 模式时，为了避免出现主备设备配置不同步现象，建议：

- 在 Admin Master 上配置各项参数；
- 首先开启Admin Master 的 HA 功能，然后再开启Master 的 HA 功能。

注意:对启用 HA 功能的设备进行配置时，请尽量在HA 状态稳定的情况下进行各种配置操作，从而避免出现配置不同步或者配置命令执行缓慢的情况。

HA 簇

HA 簇是实现 HA 功能的设备的组合。对于外部网络设备而言，一个 HA 簇是一个单一的设备，处理网络流量和提供安全服务。HA 簇通过簇 ID 进行标识。为设备指定HA 簇 ID 后，设备进入 HA 状态，执行 HA 功能。

HA 组

系统会对HA 簇中相同 HA 组 ID 的设备，按照 HCMP 协议，根据设备的HA 配置，进行主备选举。主设备处于活动状态处理网络流量，而当主设备出现故障时，其它设备代替主设备继续工作。当为安全设备设置簇 ID 时，组 ID 为 0 的HA 组会自动创建。在Active-Passive（A/P）模式中，设备仅具有 HA 组 0。在 Active-Active（A/A）模式中，目前的版本支持用户创建 2 个 HA 组，组 0 和组 1。

HA Node

为区分 HA 簇中的 HA 设备，用户可使用HA Node 值来标识设备。目前的版本仅支持 Node 值为 0 和 1。

在 HA Peer 模式下，系统可通过标识 HA Node 值来决定哪个设备处于主动状态，哪个处于禁用状态。在 HA 组 0 中，HA Node 值为 0 的设备处于主动状态， Node 值为 1 的设备处于禁用状态。在HA 组 1 中，Node 值为 1 的设备处于主动状态， Node 值为 0 的设备处于禁用状态。

HA 组接口和虚拟 MAC

在 HA 环境中，每个HA 组都具有接口，流量通过接口进行传输。每个 HA 组的主设备维护对应接口的虚拟 MAC（VMAC）地址，流量通过这些具有VMAC 地址的接口进行转发。HA 簇中不同HA 组之间不互相转发数据。VMAC 地址由 HA 虚拟基 MAC、簇 ID、HA 组 ID 以及物理接口索引确定。

HA 选举

HA 簇中，拥有同样 HA 组 ID 的具有高优先级（数值越小，优先级越高）的设备会被选举为 HA 组的主设备。

HA 同步

为保证备份设备能够在主设备失效时代替主设备工作，主设备需要与备用设备进行同步。同步的信息类型有三种：配置信息、文件以及 RDO（Runtime Dynamic Object）。RDO 的具体内容主要包括：

- 会话信息（以下类型会话信息不会同步：到设备本身的会话、隧道会话、Deny Session、ICMP 会话以及 tentative 会话）
- IPSec VPN 信息
- SCVPN 信息
- L2TP 信息
- DNS 缓存映射条目
- ARP 表
- PKI 信息
- DHCP 信息
- MAC 表
- Web 认证信息

系统使用两种方法进行同步，分别是实时同步和批量同步。当主设备刚刚选举成功时，系统会使用批量同步方法，将主设备信息全部同步到备份设备；当配置发生变化时，系统将使用实时同步的方法将变化的信息同步到备份设备。除 HA 相关配置和本地配置（例如，主机名称配置），其它的配置都会被同步。

注意:

- 指定接口的Local 属性后，该接口模式下的所有配置信息将不再进行主备同步。请避免配置业务接口的 Local 属性。
- 对于部分设备（SG-6000-X6150、SG-6000-X6180、SG-6000-X7180、SG-6000-X10800），在 Active-Passive（A/P）模式下，备份设备不支持热插 IOM 模块卡，否则会影响到同步的配置信息。

HA 配置

使用高可靠性功能，用户需要按照以下步骤进行配置:

1. 配置 HA 组。HA 组的配置包括指定设备优先级（选举使用）以及设备HA 报文相关参数等。
2. 配置 HA 组的接口。
3. 配置 HA 连接。包括HA 连接接口和连接接口 IP 的配置。用于设备同步以及传输HA 报文。
4. 配置 HA 簇。为设备指定HA 簇 ID，并且开启设备的 HA 功能。

HA 组配置

HA 组配置需要在 HA 组配置模式下进行。进入 HA 组配置模式，在全局配置模式下，输入以下命令：

ha group *group-id*

- *group-id* – 指定 HA 组的 ID。范围是 0 到 1。

执行该命令后，系统进入HA 组配置模式。使用该命令 no 的形式删除指定的 HA 组。

no ha group *group-id*

在 HA 组配置模式下，用户可以做如下配置：

- 指定优先级
- 指定 Hello 报文间隔
- 指定 Hello 报文警戒值
- 配置抢占模式
- 指定发送ARP 包个数
- 指定描述信息
- 指定监测对象

指定优先级

该命令指定的优先级用于HA 选举。优先级高（数字小）的会被选举为主设备。为设备指定优先级，在 HA 组配置模式下使用以下命令：

priority *number*

- *number* – 指定优先级。范围是 1 到 254 的整数。默认值是 100。

在 HA 组配置模式下使用该命令 no 的形式恢复优先级的默认值：

no priority

> {b}提示: {/b}相同优先级下，设备序列号的第 10 至 14 位数值越小，优先级越高。

配置抢占模式

如果将设备配置为抢占模式，一旦设备发现自己的优先级高于主设备，就会将自己升级为主设备，而原先的主设备将变为备份设备；如果将设备设置为非抢占模式，即使设备的优先级高于主设备，它也只能在主

设备故障时代替主设备工作。在配置抢占模式时，用户还可以设置延迟时间，使备份设备在延迟时间过后升级为主设备。配置抢占模式，在HA 组配置模式下使用以下命令：

preempt [*delay-time*]

- *delay-time* – 指定延迟时间，单位为秒。范围是 1 到 600 秒。默认值为 30 秒。

在 HA 组配置模式下使用 **no preempt** 恢复为非抢占模式。

指定描述信息

为设备指定描述信息，在HA 组配置模式下使用以下命令：

description *string*

- *string* – 指定描述信息内容。

在 HA 组配置模式下使用 **no description** 取消描述信息的指定。

指定监测对象

用户可以为设备指定监测对象，监控设备的工作状态。一旦发现设备不能正常工作，即采取相应措施。指定监测对象，在 HA 组配置模式下使用以下命令：

monitor track *track-object-name*

- *track-object-name* – 指定系统中已配置的监测对象的名称。

在 HA 组配置模式下使用 **no monitor track** 取消监控配置。注意: 建议将 HA 组所引用的监测对象配置成 Local 属性。

配置 HA 组的接口

配置HA 组 0 接口，在全局配置模式下，使用创建接口命令，并进入接口配置模式对接口进行配置。命令如下：

interface {**ethernet***m/n* | **redundant***number* | **aggregate***number* | **tunnel***number* | **loopback***number* | **bgroup***number* | **ethernet***m/n.tag* | **redundant***number.tag* | **aggregate***number.tag*}

配置HA 组 1 接口，在全局配置模式下，输入以下命令：

interface {**ethernet***x/y:z* | **redundant***x:z* | **aggregate***x:z* | **tunnel***x:z* | **loopback***x:z* | **ethernet***x/y.u:z* | **redundant***x.y:z* | **aggregate***x.y:z*}

- **ethernet***x/y:z*：指定以太网接口 ethernetx/y 作为组 z 接口，用于转发数据。
- **redundant***x:z*：指定冗余接口 redundantx 作为组z 接口，用于转发数据。

- **aggregate***x:z*：指定集聚接口 aggregatex 作为组z 接口，用于转发数据。
- **tunnel***x:z*：指定隧道接口 x 作为组 z 接口，用于转发数据。
- **loopback***x:z*：指定回环接口 loopbackx 作为组 z 接口，用于转发数据。
- **ethernet***x/y.u:z*：指定以太网子接口 ethernetx/y.u 作为组z 接口，用于转发数据。
- **redundant***x.y:z*：指定冗余子接口 redundantx.y 作为组 z 接口，用于转发数据。
- **aggregate***x.y:z*：指定集聚子接口 aggregatex.y 作为组z 接口，用于转发数据。

在全局配置模式下，使用该命令的 no 形式删除指定接口：

no interface {**ethernet***x/y:z* | **redundant***x:z* | **aggregate***x:z* | **tunnel***x:z* | **loopback***x:z* | **ethernet***x/y.u:z* | **redundant***x.y:z* | **aggregate***x.y:z*}

配置接口下一跳

在 HA Peer 组网模式中，为了避免在对端设备间同步数据时查找路由失败，用户可直接配置接口的下一跳地址，以确保会话创建成功。指定接口的下一跳 IP 地址，在接口配置模式下，使用以下命令：

direct-send default-nexthop *A.B.C.D* [**local**]

- *A.B.C.D* – 指定接口的下一跳 IP 地址。
- **local** – 若指定该参数，系统将不向备份设备同步此配置。默认情况下，不指定该参数。

在接口配置模式下，使用 **no direct-send default-nexthop** [*A.B.C.D*] [**local**]取消指定接口下一跳 IP。

配置 SNAT 端口分割

系统支持 SNAT 端口分割功能，即两台HA 设备均配置了相同的 SNAT 地址池，系统会按照 HA Node 值在两台设备上平均分配 SNAT 端口资源。若关闭该功能，两台HA 设备需配置不同的 SNAT 地址池，每台设备将独占所有的端口资源。该功能仅在 HA Peer 模式下生效。

开启 SNAT 端口分割功能，在全局配置模式下，使用以下命令：

split-port-pool by ha-node

在全局配置模式下，使用 **no split-port-pool by ha-node** 关闭该功能。

HA 连接配置

指定 HA 连接接口

用户最多可以指定两个 HA 控制连接接口，后配置的 HA 连接接口可以作为先配置的HA 连接接口的备份接口工作。当先配置的 HA 连接接口断开连接，后配置的 HA 连接接口会继续传输 HA 报文。

指定HA 控制连接接口，在全局配置模式下，使用以下命令：

ha link interface *interface-name*

- *interface-name* – 指定接口名称。

指定HA 数据连接接口，在全局配置模式下，使用以下命令：

ha link data interface *interface-name*

- *interface-name* – 指定接口名称。
- **data** – 指定 HA 连接为数据连接。指定后，会话信息将通过HA 连接接口同步完成。目前仅支持将物理接口和集聚接口配置为 Data Link 的接口。用户最多可以指定 1 个 HA 数据连接接口。

在全局配置模式使用该命令 no 的形式删除对指定接口的HA 连接接口的配置：

no ha link interface *interface-name*

no ha link data interface *interface-name*

注意:对于 X 系列设备，仅支持将 X7180 设备的 IOM-2Q8SFP+ -200 模块卡的接口指定为HA 连接接口，其他模块卡接口不支持该功能。

指定 HA 连接接口 IP 地址

HA 连接接口指定完毕，用户需要为HA 连接接口配置 IP 地址。在全局配置模式下，使用以下命令：

ha link ip *ip-address netmask*

- *ip-address netmask* – 指定 HA 连接接口的 IP 地址和网络掩码。

在全局配置模式使用该命令 no 的形式取消HA 连接接口 IP 地址的配置：

no ha link ip *ip-address netmask*

指定 HA 心跳口 MAC 地址

HA 心跳口 MAC 地址指 HA 设备向 HA 组中的其它设备发送心跳（Hello 报文）时所使用的源 MAC 地址。默认情况下，系统使用默认的 MAC 地址发送心跳报文，用户也可指定控制连接接口的 MAC 或者自定义 MAC 作为 HA 心跳口的 MAC 地址。指定 HA 心跳口 MAC 地址，在全局配置模式下，使用以下命令：

ha link mac { **1st-interface-mac** | *mac-address*}

- **1st-interface-mac** – 指定使用控制连接接口的 MAC 地址作为HA 心跳口的 MAC 地址。当用户配置多个控制连接接口时，系统将使用第一个控制连接接口的 MAC 作为 HA 心跳口的 MAC 地址。

- *mac-address* – 指定使用自定义的 MAC 地址作为HA 心跳口的 MAC 地址。

在全局配置模式使用 **no ha link mac** 恢复默认的 HA 心跳口的 MAC 地址:

配置使用接口的真实 MAC

该功能仅对于的接口（除 HA 连接接口和配置了 Local 属性的接口）生效。默认情况下，设备接口使用系统分配的虚拟 MAC 进行正常的数据流量转发。配置该功能后，将使用云平台分配给接口的真实 MAC 进行业务通信。配置使用接口的真实的 MAC，在全局配置模式下，使用以下命令:

no ha virtual-mac enable

使用 **ha virtual-mac enable** 命令恢复默认配置。

注意:当设备被添加到 HA 簇后，将无法修改接口所使用的 MAC。如需修改，请先执行命令 no ha cluster 关闭设备 HA 功能。

配置通过二层单播方式进行 HA 协商通信

默认情况下，HA 环境中的两台设备使用组播方式进行协商通信，但在虚拟化环境中，部分云平台要求设备使用其分配的 MAC 地址进行通信，否则报文将被丢弃。系统支持通过二层单播的方式进行 HA 协商通信。在 HA 部署环境中，用户可以在两台设备上，分别配置对端HA 连接接口的 IP 地址或同时配置对端 HA 连接接口的 IP 和MAC 地址（即心跳口 MAC 地址），这样两台设备将采用二层单播的方式进行HA 协商通信。配置 HA 对端的 IP 和 MAC 地址，在全局配置模式下，使用以下命令:

ha peer ip *ip-address* [**mac** *mac-address*]

- **ip** *ip-address* – 指定对端设备的HA 连接接口的 IP 地址。
- **mac** *mac-address* - 指定对端设备的HA 连接接口的MAC 地址，即心跳口的MAC 地址。。

在全局配置模式下，使用命令 **no ha peer ip** 恢复默认配置。

注意:当设备被添加 HA 簇后，将无法修改 HA 对端 IP 和MAC 地址。如需修改，请先执行命令 **no ha cluster** 关闭设备 HA 功能。

HA 簇配置

为设备配置了HA 组、HA 组接口和HA 连接接口后，用户需要将设备添加到HA 簇中，才能够使设备的 HA 功能生效。如果网络中存在多对HA 设备，用户需要为它们配置不同的 HA 簇 ID，否则可能出现 MAC 地址冲突现象。配置HA 簇，在全局配置模式下使用以下命令:

ha cluster *cluster-id* [[**peer-mode node** *ID* [**symmetric-routing**]] | **node** *ID*]

- *cluster-id* – 指定 HA 簇 ID。范围依据 HA 的虚 MAC 前缀而变化。

- **peer-mode node** *ID* – 配置 HA Peer 模式，并标识该设备在HA 簇中的角色。范围是 0 到 1。 默认情况下，HA Node ID 为 0 的设备上的组 0 为主动状态，HA Node ID 为 1 的设备上的组 0 为禁用状态。
- **symmetric-routing** - 若指定该参数，设备将工作在对称路由模式下。
- **node** *ID* - 为设备指定HA Node 值，两台设备需指定不同的 Node 值。范围是 0 到 1。SG-6000-X10800 设备需要指定该参数，否则系统会出现错误提示。其他 设备如不指定该参数，设备将通过自动协商获取 Node ID。

在全局配置模式下使用 **no ha cluster** 关闭设备的 HA 功能。

接口管理 IP 配置

为实现对HA 备份设备的管理，用户需要为备份设备配置管理 IP。配置管理 IP 地址，在接口配置模式下，使用以下命令：

manage ip *ip-address*

- *ip-address* - 指定管理 IP 地址。

手动同步 HA 信息

在某些特殊情况下，可能出现主备配置信息不同步现象。此时，需要用户手动同步主备设备的配置信息。用户可以通过以下方法判断是否需要进行手动同步：

1. 分别在主备设备上执行相应的 show 命令查看相关配置信息。
2. 根据显示的配置信息，判断是否需要手动同步：

- 如果显示的配置信息一致，则无需进行手动同步；
- 如果显示的配置信息不一致，需要手动执行相应的命令完成配置信息同步（相关 show 命令和执行命令，参阅下表）。

注意：

- 本地配置信息不一致时，例如配置口超时时间等，不需要进行手动同步。
- 对于动态信息，例如会话等，只有当正常动态信息没有同步时，才需要进行手动同步，否则无需手动同步。

手动同步配置命令列表如下所示：

HA 同步信息	show 命令	手动同步命令
所有静态配置及动态数据	show ha sync state all	exec ha sync all

HA 同步信息	show 命令	手动同步命令
配置信息	show configuration	exec ha sync configuration
文件信息	show file	exec ha sync file *file-name*
ARP 表项	show arp	exec ha sync rdo arp
DNS 配置信息	show ip hosts	exec ha sync rdo dns
DNS rewrite 规则信息	show dns-rewrite-rule	exec ha sync rdo dns-rewrite
DHCP 配置信息	show dhcp	exec ha sync rdo dhcp
MAC 地址表	show mac	exec ha sync rdo mac
PKI 配置信息	show pki key	exec ha sync rdo pki
	show pki trust-domain	
会话信息	show session	exec ha sync rdo session
IPSec VPN 信 息	show ipsec sa	exec ha sync rdo vpn
	show isakmp sa	
SCVPN 信息	show scvpn client test	exec ha sync rdo scvpn
	show scvpn host-check-profile	
	show scvpn pool	
	show scvpn user-host-binding	
	show scvpn session	
	show auth-user scvpn	
L2TP 信息	show l2tp tunnel	exec ha sync rdo l2tp
	show l2tp pool	
	show l2tp client {tunnel-name *name* [user *user-name*] | tunnel-id *ID*}	
	show auth-user l2tp [interface *interface-name* | vrouter *vrouter-name* | slot *slot-no*]	
Web 认证信息	show auth-user webauth	exec ha sync rdo webauth
NTP 信息	show ntp	exec ha sync rdo ntp
SCVPN 信息	show scvpn	exec ha sync rdo scvpn
路由信息	show ip route	exec ha sync rdo route
IGMP 信息	show ha sync statistic igmp	exec ha sync rdo igmp

HA 同步信息	show 命令	手动同步命令
	show ha sync state igmp	

启用/禁用 HA 会话自动同步

默认情况下，HA 设备之间会自动同步会话信息。同步会话会产生一定流量，在高负载情况下可能会对设备性能造成影响。用户可以根据设备负载情况启用或禁用 HA 会话自动同步功能，以确保设备的稳定性。

启用或禁用 HA 会话自动同步功能，在全局配置模式下，使用以下命令：

- 启用：**ha sync rdo session enable**
- 禁用：**ha sync rdo session disable**

手动切换 HA 设备的主备状态

用户可以在任何模式下使用以下命令进行主备设备的手动切换：

exec ha master switch-over

注意：

- 仅支持在HA 的主设备上执行此命令。
- 如果在执行切换操作时，该设备正在进行批量同步或者部分设备（SG-6000-X6150、SG-6000-X6180、SG-6000-X7180、SG-6000-X10800）正在进行主控卡的批量同步，那么无法成功切换 HA 设备的主备状态。

显示 HA 配置

系统提供相应的 show 命令，查看 HA 配置信息。

- 查看HA 簇配置信息：**show ha cluster**
- 查看HA 组配置信息：**show ha group** {**config** | *group-id*}
- 查看HA 连接配置状态：**show ha link status**
- 查看各个模块的 HA 同步状态：**show ha sync state** {**pki** | **dns** | **dhcp** | **vpn** | **ntp** | **config** | **flow** | **scvpn** | **l2tp** | **route** | **igmp** }
- 查看HA 同步的总体状态及各模块的同步状态：**show ha sync state all**
- 查看 HA traffic 状态：**show ha traffic**
- 查看HA 同步统计信息：**show ha sync statistic** {**pki** | **dns** | **dhcp** | **vpn** | **ntp** | **config** | **scvpn** | **route** | **igmp** }

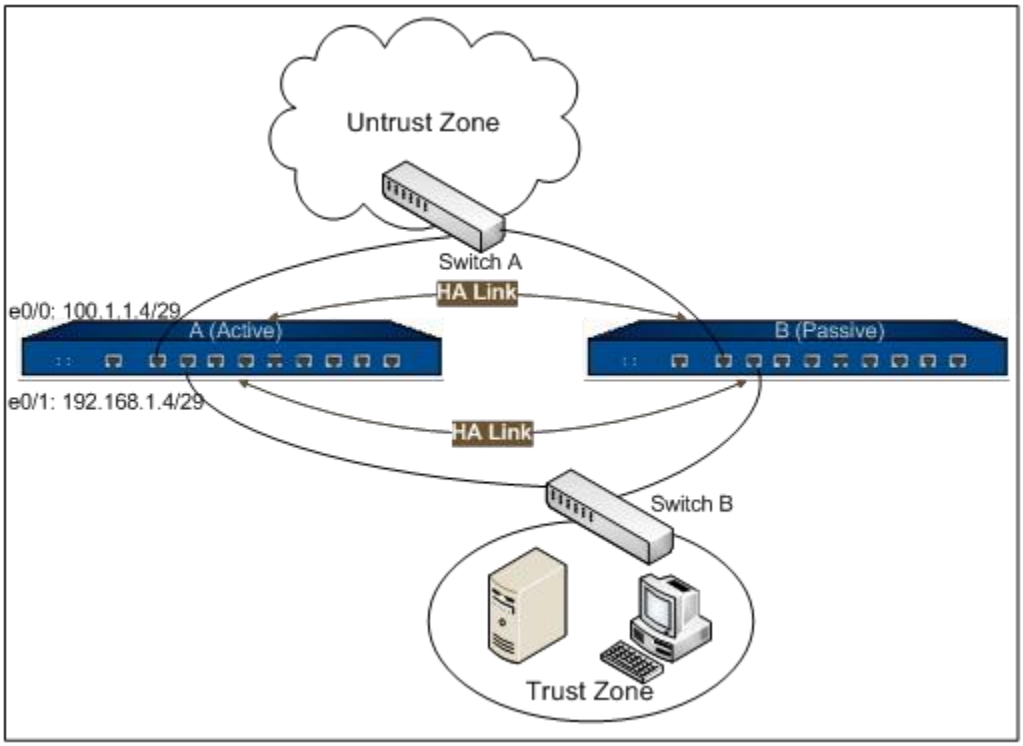
- 查看 HA 会话自动同步功能是否开启：**show ha sync rdo session config**
- 显示接收和发送的 HA 协议统计信息：**show ha protocol statiscitc**
- 显示已同步或未同步的 HA 会话信息：**show session** {**sync** | **unsync**}
- 显示 HA 统计信息：**show ha flow** [[**slot** *slot-number*] | [**cpu** *cpu-number*]]**statistics**

HA 配置举例

例 1: HA Active-Passive 工作模式

组网需求

两台设备采用完全相同的硬件平台、固件版本和许可证，组成 Active-Passive 工作模式，并且两台设备使用同样的接口连接到网络。组网图请参见下图：



配置步骤

第一步：配置设备A 的接口及策略。

设备 A

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

hostname(config-if-eth0/0)# **zone untrust**

```
hostname(config-if-eth0/0)# ip address 100.1.1.4/29
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# ip address 192.168.1.4/29
hostname(config-if-eth0/1)# exit
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
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-policy)# exit
hostname(config)#
```

第二步：配置设备A 的监测对象。监控设备A ethernet0/0 的工作状态，一旦发现接口故障，则进行切换。

```
hostname(config)# track trackobj1
hostname(config-trackip)# interface ethernet0/0 weight 255
hostname(config-trackip)# exit
hostname(config)#
```

第三步：配置HA 组。

设备 A

```
hostname(config)# ha group 0
```

```
hostname(config-ha-group)# priority 50
hostname(config-ha-group)# monitor track trackobj1
hostname(config-ha-group)# exit
hostname(config)#
```

设备 B

```
hostname(config)# ha group 0
hostname(config-ha-group)# priority 100
hostname(config-ha-group)# exit
hostname(config)#
```

第四步：配置HA 连接接口。

设备 A

```
hostname(config)# ha link interface ethernet0/2
hostname(config)# ha link interface ethernet0/3
hostname(config)# ha link ip 1.1.1.1/24
hostname(config)#
```

设备 B

```
hostname(config)# ha link interface ethernet0/2
hostname(config)# ha link interface ethernet0/3
hostname(config)# ha link ip 1.1.1.2/24
hostname(config)#
```

第五步：配置HA 簇开启HA 功能。

设备 A

```
hostname(config)# ha cluster 1
```

设备 B

```
hostname(config)# ha cluster 1
```

第六步：主备同步完成后，配置主设备与备份设备的管理 IP。

```
设备 A
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# manage ip 192.168.1.253
```

```
设备 B
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# manage ip 192.168.1.254
```

第七步：配置设备B 的监测对象。监控设备 B ethernet0/0 的工作状态，一旦发现接口故障，则进行切换。

```
设备 B
hostname(config)# ha group 0
hostname(config-ha-group)# monitor track trackobj1
hostname(config-ha-group)# exit
hostname(config)#
```

以上配置完成后，系统会将设备 A 选举为主设备，进行流量转发。设备B 为备份设备。设备 A 会将其配置信息以及状态数据同步到设备 B。当设备A 出现故障不能正常转发流量或设备A 的 ethernet0/0 接口断开时，设备 B 会在不影响用户通信的状态下切换为主设备，继续转发流量。

第 6 章 IPv6

系统支持互联网协议版本 6，即 IPv6（Internet Protocol Version 6）。与 IPv4 相比，IPv6 具有一些明显优势，包括大大增加的地址空间、更加简化的报文头、灵活的扩展头部以及选项、具有良好的层次性的地址分配、无状态地址自动配置、通过 IPSec 头部实现数据安全以及更强的 QoS 管理支持等。

StoneOS 为 IPv4 和 IPv6 同时支持的双栈系统固件，同时支持隧道技术（当前版本支持手工 IPv6 隧道）实现 IPv6 的通信。

注意:当前版本的IPv6 相关功能支持多 VR；系统提供默认 VR——trust-vr。

IPv6 地址配置

由于设备为 IPv4 与 IPv6 同时支持的双栈设备，设备的接口可同时支持 IPv4 和 IPv6 两个版本的 IP 地址。默认情况下，接口支持 IPv4 协议，使接口支持 IPv6，需要首先开启接口的 IPv6 功能。开启接口的 IPv6 功能，在接口配置模式下使用以下命令：

ipv6 enable

使用以上命令开启接口的 IPv6 功能的同时，系统会自动为该接口生成一个IPv6 链路本地（link-local）单播地址。

使用 **no ipv6 enable** 命令关闭接口的 IPv6 功能，同时删除为接口自动分配的链路本地地址。但是，对于已经配置了 IPv6 相关配置的接口，该命令不可执行。

例如，开启接口 ethernet0/1 的 IPv6 功能，执行以下命令：

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# ipv6 enable
```

开启接口的 IPv6 功能后，用户可以为接口进行以下 IPv6 配置：

- 指定全局 IPv6 地址
- 指定无状态地址自动配置
- 指定 EUI-64 地址
- 指定链路本地地址
- 指定接口 IPv6 最大传输单元（MTU）
- 显示接口的 IPv6 配置

指定全局 IPv6 地址

通常情况下，为接口指定的全局 IPv6 地址为“IPv6 地址前缀/前缀长度”形式，除该形式外，系统还支持 IPv6“通用前缀”形式的地址，即指定的地址由“通用前缀”以及“子前缀”组成。其中的“通用前缀”需要在全局模式下进行配置，为接口指定地址时，直接引用已配置的“通用前缀”名称。为接口手动指定 IPv6 全球单播地址，在接口配置模式下，使用以下命令：

ipv6 address {*ipv6-address/Mask* | *general-prefix-name sub-prefix/Mask*}

- *ipv6-address* – 指定 IPv6 地址前缀。
- *Mask* – 指定前缀长度。取值范围为 1 到 128。
- *general-prefix-name* – 指定通用前缀的名称。
- *sub-prefix/Mask* – 指定子前缀。

例如，通用前缀名称为test-prefix，其 IPv6 网络前缀为 2002:ae3:1111::/48，指定的子前缀为 0:0:0:2222::1/64，则通过命令 ipv6 address test-prefix 0:0:0:2222::1/64 为接口指定的 IPv6 地址为 2002:ae3:1111:2222::1/64。

使用该命令 no 的形式取消接口的 IPv6 全局单播地址的指定：

no ipv6 address（取消接口所有的 IPv6 地址的指定）

no ipv6 address {*ipv6-address/Mask* | *general-prefix-name sub-prefix/Mask*}（取消接口指定的 IPv6 地址）

配置 IPv6 通用前缀

系统支持普通的 IPv6 通用前缀和 6to4 通用前缀。当指定的通用前缀为 6to4 前缀时，其格式为“2002:a.b.c.d::/48”，其中的“a.b.c.d”为被引用的接口的IPv4 地址（通过 interface-name 参数指定）。配置 IPv6 通用前缀，在全局配置模式下使用以下命令：

ipv6 general-prefix *prefix-name* {*X:X:X:X::X/M* | **6to4** *interface-name*}

- *prefix-name* – 指定通用前缀的名称。
- *X:X:X:X::X/M* – 为通用前缀指定具体 IPv6 网络前缀。
- **6to4** – 指定 IPv6 通用前缀为 6to4 前缀。
- *interface-name* – 指定 6to4 前缀引用的接口（引用接口的 IPv4 地址）。

在全局配置模式下使用该命令 no 的形式删除指定的 IPv6 通用前缀：

no ipv6 general-prefix *prefix-name* {*X:X:X:X::X/M* | **6to4** *interface-name*}

显示系统中已配置的 IPv6 通用前缀信息，在任何模式下使用以下命令：

show ipv6 general-prefix

指定无状态地址自动配置

在无状态地址自动配置方式下，接口先接收 RA 报文中的地址前缀，然后结合接口标识得到一个全球地址。指定无状态地址自动配置，在接口配置模式下使用以下命令：

ipv6 address autoconfig [**default**]

- **default** – 如果为该接口指定了缺省路由器，指定该参数将产生一条缺省路由器的缺省路由。

在接口配置模式下使用该命令 no 的形式取消接口的无状态地址自动配置：

no ipv6 address autoconfig

指定 EUI-64 地址

为接口指定使用 EUI-64 接口 ID 的 IPv6 地址，在接口配置模式下使用以下命令：

ipv6 address *ipv6-address/Mask* **eui-64**

- *ipv6-address* – 指定 IPv6 地址前缀。
- *Mask* – 指定前缀长度。取值范围为 1 到 128。如果指定的前缀长度小于或者等于 64，地址的后 64 位均使用生成的接口 ID；如果指定的前缀长度大于 64，地址的后（128-前缀长度）位均使用生成的接口 ID。

使用命令 **no ipv6 address** *ipv6-address/Mask* **eui-64** 命令取消接口的EUI-64 地址的指定。

指定链路本地地址

链路本地地址（link-local 地址）用于同一链路的相邻节点间通信，例如单条链路上没有路由器时主机间的通信。默认情况下，开启接口的 IPv6 功能后（在接口配置模式下执行 ipv6 enable），系统会自动为接口生成一个链路本地地址，用户也可以根据需要为接口指定，通过命令指定的链路本地地址将取代系统自动生成的链路本地地址。为接口指定链路本地地址，在接口配置模式下，使用以下命令：

ipv6 address *ipv6-address* **link-local**

- *ipv6-address* – 指定 IPv6 地址。

使用命令 **no ipv6 address** *ipv6-address* **link-local** 命令取消接口的链路本地地址的指定（恢复使用系统生成的链路本地地址）。

指定接口 IPv6 最大传输单元

为接口指定允许发送的 IPv6 数据包的最大传输单元值，在接口配置模式下使用以下命令：

ipv6 mtu *value*

- *value* – 指定最大传输单元的值，单位为字节，默认值为 1500。取值范围是 1280 到 1500。

使用命令 **no ipv6 mtu** 命令恢复接口的默认 MTU 值。

显示接口的 IPv6 配置

显示接口的 IPv6 配置，在任何模式下使用以下命令：

show ipv6 interface [*interface-name*] [**prefix**]

- *interface-name* – 显示指定接口的 IPv6 配置信息。如果不指定该参数，系统将显示所有开启了 IPv6 功能的接口信息。
- **prefix** – 显示指定接口的 IPv6 前缀。

IPv6 邻居发现协议配置

邻居发现协议（Neighbor Discovery Protocol）是 IPv6 协议的基本组成部分，该协议工作在链路层，负责发现链路上其他节点、决定其他节点的链路层地址、寻找可用路由器并且维护到其他节点的可达信息。它在实现了 IPv4 的地址解析协议（ARP）、控制报文协议（ICMP）中的路由器发现部分和重定向协议的所有功能同时，还提供更高级功能，例如邻居不可达检测机制。

当前版本的 StoneOS 支持以下协议相关配置：

- 配置 DAD 功能
- 指定可达时间
- 配置 RA 报文参数
- 指定 RA 报文发送间隔
- 指定 RA 报文生存时间
- 指定 DRP
- 配置 LAN 口 RA 报文发送状态
- 添加/删除静态 IPv6 邻居缓存表项

DAD 功能配置

DAD 功能即地址重复检测（Duplicate Address Detection）功能，其作用为验证 IPv6 地址的唯一性。该功能是通过发送NS（邻居请求，Neighbor Solicitation）报文实现的。NS 报文发出后，如果链路上有其他主

机发现发送 NS 请求方的地址与自己的重复，它就会发送 NA（邻居通告，Neighbor Advertisment）报文告知对方这个地址已经有人在用，然后发送 NS 请求方会把这个地址标记为“Duplicate”状态，这个地址就是一个无效的 IPv6 地址。

StoneOS 的DAD 功能配置包括指定接口发送NS 报文的次数以及指定发送 NS 报文的时间间隔。

指定接口发送NS 报文的次数，在接口配置模式下使用以下命令：

ipv6 nd dad attempts *times*

- *times* – 指定接口发送NS 报文的次数，默认值为 1。取值范围为 0 到 20。取值为 0 表示接口不启用 DAD 检测功能。如果系统在指定次数内均未收到 NA 回复报文，则证明该 IPv6 地址为可用的唯一地址。

使用 **no ipv6 nd dad attempts** 命令恢复默认次数。

指定接口发送NS 报文时间间隔，在接口配置模式下使用以下命令：

ipv6 nd ns-interval *interval*

- *interval* – 指定接口发送 NS 报文的时间间隔，单位为毫秒，默认值为 1000 毫秒。取值范围是 1000 到 3600000 毫秒。

使用 **no ipv6 nd ns-interval** 命令恢复默认时间间隔。

指定可达时间

可达时间指接口在发送 NS 报文后，在得到邻居可达性确认后，认为邻居可达的时间。指定可达时间，在接口配置模式下使用以下命令：

ipv6 nd reachable-time *time*

- *time* – 指定可达时间，单位为毫秒，默认值为 30000 毫秒。取值范围是 0 到 3600000 毫秒。

使用 **no ipv6 nd reachable-time** 命令恢复默认值。

配置 RA 报文参数

路由器通告（Router Advertisement）报文简称为 RA 报文，路由器通告周期性地发布 RA 报文，通告其可用性以及用于配置的链路和 Internet 参数，包括所使用的网络地址前缀、建议的 Hop Limit 值、本地 MTU 值、以及节点应使用的自动配置类型的标签等。

指定 Hop Limit

Hop Limit 是指接口发出的 IPv6 报文的最大跳数或者RA 报文中的最大跳数。指定 Hop Limit，在接口配置模式下使用以下命令：

ipv6 nd hoplimit *number*

- *number* - 指定最大跳数，默认值为 64。取值范围为 0 到 255。

在接口配置模式下使用该命令 no 的形式恢复最大跳数的默认值：

no ipv6 nd hoplimit

指定是否通告 MTU 值

当设备通过接口发送 RA 报文时，用户可以指定是否在 RA 报文中包含 MTU 值告知其他路由器。默认情况下将通告 MTU 值。指定是否通告 MTU 值，在接口配置模式下使用以下命令：

ipv6 nd adv-linkmtu

在接口配置模式下使用该命令 no 的形式指定不通告MTU 值：

no ipv6 nd adv-linkmtu

指定自动配置类型标签

用户可以通过指定 RA 报文的自动配置类型标签通告相连主机是否使用状态自动配置方式（例如 DHCP）获取 IP 地址以及其他自动配置参数信息。指定使用状态自动配置方式获得 IP 地址，在接口配置模式下使用以下命令：

ipv6 nd managed-config-flag

在接口配置模式下使用命令 **no ipv6 nd managed-config-flag** 取消相关配置

指定使用状态自动配置方式获得 IP 地址以外的其他自动配置参数信息，在接口配置模式下使用以下命令：

ipv6 nd other-config-flag

在接口配置模式下使用命令 **no ipv6 nd other-config-flag** 取消相关配置。

指定 IPv6 前缀及参数

RA 报文会将接口的IPv6 前缀通告出去，用户还可以指定其他 IPv6 前缀进行通告，并且配置 IPv6 前缀通告相关参数。指定 RA 报文的 IPv6 前缀以及相关参数，在接口配置模式下使用以下命令：

ipv6 nd prefix {*ipv6-prefix/M* | **default**} [**no-advertise** | [*valid-lifetime preferred-lifetime* [**off-link** | **no-autoconfig**]] | [**at** *valid-date* [*preferred-date* [**off-link** | **no-autoconfig**]]]

- *ipv6-prefix/M* – 指定 RA 报文需要发送的 IPv6 前缀以及前缀长度。
- **default** – 为所有前缀指定默认参数值。
- **no-advertise** – 指定 RA 报文中不通告 IPv6 前缀信息。

- *valid-lifetime* – 指定 IPv6 前缀的有效生存时间（valid lifetime），单位为秒，默认值为 2592000 秒（30 天）。取值范围是 0 到 4294967295。
- *preferred-lifetime* – 指定 IPv6 前缀的优选生存时间（preferred lifetime），单位为秒，默认值为 604800 秒（7 天）。优选生存时间必须小于或者等于有效生存时间。
- **off-link** – 指定前缀为“off-link”状态，即收到该 RA 报文的节点不会将该前缀写入到自己的路由表中，即使该前缀的信息已经在路由表中，节点会将其从路由表中删除。
- **no-autoconfig** – 通告接收主机该前缀不能作为 IPv6 自动配置地址使用。
- *valid-date* – 指定前缀的有效日期，即前缀在该日期之前有效。格式为“MM/DD/YYYY HH:MM”，例如“09/20/2010 09:30”。
- *preferred-date* – 指定前缀的优选有效日期。格式为“MM/DD/YYYY HH:MM”。该日期必须早于有效日期。

在接口配置模式下使用该命令 no 的形式取消 IPv6 前缀参数配置：

no ipv6 nd prefix {*ipv6-prefix/M* | **default**}

指定 RA 报文发送间隔

RA 报文发送间隔指接口发送 RA 报文的间隔时间，该时间间隔应该小于或者等于 RA 报文的生存时间（通过命令配置）。为减少与同一链路上的其他路由器同时发送 RA 的可能性，系统通常从最大间隔和最小间隔之间选择一个随机数作为实际间隔时间。配置 RA 报文发送时间间隔，在接口配置模式下使用以下命令：

ipv6 nd ra interval *max-interval* [*min-interval*]

- *max-interval* – 指定最大时间间隔，单位为秒，默认值为 600。取值范围为 4 到 1800。
- *min-interval* – 指定最小时间间隔，单位为秒。取值范围为 3 到 1350。最小间隔必须小于等于最大间隔的 75%且大于 3 秒。如果不指定最小间隔，系统将使用最大间隔的 1/3 作为最小间隔。

在接口配置模式下，使用该命令 no 的形式回复发送间隔默认值：

no ipv6 nd ra interval

指定 RA 报文的生存时间

RA 报文生存时间指路由器作为接口的缺省路由器的有效时间。指定 RA 报文生存时间，在接口配置模式下使用以下命令：

ipv6 nd ra lifetime *time*

- *time* – 指定 RA 报文的生存时间，单位为秒，默认值为 1800 秒。取值范围是 0 到 9000。“0”表示该路由器不是接口的缺省路由器。当取非零值时，该时间必须等于或者大于RA 报文的发送间隔时间。

在接口配置模式下使用该命令 no 的形式恢复默认生存时间：

no ipv6 nd ra lifetime

指定 DRP

DRP 即 Default Router Preference。当节点接收到来自不同路由器的等价路由时，会根据 DRP 的值选择优选路由器。指定 DRP，在接口配置模式下使用以下命令：

ipv6 nd router-preference {**high** | **medium** | **low**}

- **high** – 指定 DRP 为高。
- **medium** – 指定 DRP 为中。该值为默认值。
- **low** – 指定 DRP 为低。

在接口配置模式下，使用该命令 no 的形式恢复默认值：

no ipv6 nd router-preference

配置 LAN 口 RA 报文传输状态

默认情况下，配置了 IPv6 单播路由的 FDDI 接口会自动发送 RA 报文，其他类型的接口不发送 RA 报文。配置 LAN 口 RA 报文传输状态，在接口配置模式下，使用以下命令：

ipv6 nd ra suppress

执行以上命令后，指定的接口不再传输 RA 报文。在接口配置模式下使用该命令 no 的形式使接口能够传输 RA 报文：

no ipv6 nd ra suppress

添加/删除 IPv6 邻居缓存表项

IPv6 邻居缓存表项是一组有关单个邻居的表项，这些表项是连接单播地址的关键。查看系统的 IPv6 邻居缓存表项，在任何模式下使用以下命令：

show ipv6 neighbor [**interface** *interface-name* | **slot** *slot-num* | **static** | **vrouter** *vr-name* | *ipv6-address* | **generic**]

- *interface-name* – 显示指定接口的 IPv6 邻居缓存表项。

- *ipv6-address* – 显示指定地址的 IPv6 邻居缓存表项。
- **slot** *slot-num* – 显示指定槽位号的 IPv6 邻居缓存表项。部分设备（X6150、X6180、X7180、X10800）支持。
- **vrouter** *vr-name* – 显示指定 VRouter 的 IPv6 邻居缓存表项。
- **static** – 显示静态 IPv6 邻居缓存表项。
- **generic** – 显示邻居缓存表项的统计信息。

添加静态 IPv6 缓存表项，在全局配置模式下使用以下命令：

ipv6 neighbor *ipv6-address interface-name mac-address*

- *ipv6-address* – 指定 IPv6 地址。
- *interface-name* – 指定接口名称。
- *mac-address* – 指定 IPv6 地址对应的 MAC 地址。

删除 IPv6 缓存表项，在全局配置模式下使用以下命令：

clear ipv6 neighbor [*ipv6-address*] [**vrouter** *vr-name*]

- *ipv6-address* – 删除指定地址的 IPv6 邻居缓存表项。
- **vrouter** *vr-name* – 删除指定 VRouter 的 IPv6 邻居缓存表项。

IPv6 系统管理配置

StoneOS 支持 IPv6 的FTP、TFTP、HTTP 以及 HTTPS 协议，即 StoneOS 支持通过 IPv6 地址访问FTP 和 TFTP 服务器，用户可以通过 IPv6 地址访问 StoneOS 的 WebUI。IPv4 和 IPv6 的 HTTP 以及 HTTPS 服务使用相同的协议端口号。

通过 IPv6 地址的 FTP 和 TFTP 服务器，用户可以导出以下对象：配置信息文件、系统固件、许可证、部分日志信息（告警、事件、安全）、PKI 证书、SCVPN 主机验证绑定表、以及 URL 数据库信息。在执行模式下使用以下命令：

- 导出配置文件：**export configuration** {{**startup** | **backup**} *number*} **to** {**ftp server** *ipv6-address* [**vrouter** *vrouter-name*] [**user** *username* **password** *string*] | **tftp server** *ipv6-address* [**vrouter** *vrouter-name*]} [*file-name*]
- 导出系统固件：**export image** *name* **to** {**ftp server** *ipv6-address* [**vrouter** *vrouter-name*] [**user** *username* **password** *string*] | **tftp server** *ipv6-address*} [*file-name*]

- 导出许可证：**export license** *name* **to** {**ftp server** *ipv6-address* [**user** *username* **password** *string*] | **tftp server** *ipv6-address*} [*file-name*]
- 导出日志信息：**export log** { **event** | **security**} **to** {**ftp server** *ipv6-address* [**user** *username* **password** *string*] | **tftp server** *ipv6-address*} [*file-name*]
- 导出 PKI 证书：**export pki** *trust-domain-name* {**cacert** | **cert** | **pkcs12** *password*} **to** {**ftp server** *ipv6-address* [**user** *username* **password** *string*] | **tftp server** *ipv6-address*} [*file-name*]
- 导出 SCVPN 主机验证绑定列表：**export scvpn user-host-binding to** {**ftp server** *ipv6-address* [**user** *username* **password** *string*] | **tftp server** *ipv6-address*} [*file-name*]
- 导出 URL 数据库信息：**export urlfilter-database to** {**ftp server** *ipv6-address* [**user** *username* **password** *string*] | **tftp server** *ipv6-address*} [*file-name*]

通过 IPv6 地址的 FTP 和 TFTP 服务器，用户可以导入以下对象：特征库信息、配置文件、SCVPN 以及 Web 认证页面自定义图片、系统固件、ISP 文件、许可证、PKI 证书、SCVPN 主机验证绑定表以及 URL 数据库信息。在执行模式下使用以下命令：

- 导入特征库信息：**import application-signature from** {**ftp server** *ipv6-address* [**user** *username* **password** *string*] | **tftp server** *ipv6-address*} *file-name*
- 导入配置文件：**import configuration from** {**ftp server** *ipv6-address* [**user** *username* **password** *string*] | **tftp server** *ipv6-address*} *file-name*
- 导入 SCVPN 或者 Web 认证页面自定义图片：**import customize** {**scvpn** | **webauth**} **from** {**ftp server** *ipv6-address* [**user** *username* **password** *string*] | **tftp server** *ipv6-address*} *file-name*
- 导入系统固件：**import image from** {**ftp server** *ipv6-address* [**user** *username* **password** *string*] | **tftp server** *ipv6-address*} *file-name*
- 导入 ISP 文件：**import ispfile from** {**ftp server** *ipv6-address* [**user** *username* **password** *string*] | **tftp server** *ipv6-address*} *file-name*
- 导入许可证：**import license from** {**ftp server** *ipv6-address* [**user** *username* **password** *string*] | **tftp server** *ipv6-address*} *file-name*
- 导入 PKI 证书：**import pki** *trust-domain-name* {**cacert** | **cert** | **pkcs12** *password*} **from**{**ftp server** *ipv6-address* [**user** *username* **password** *string*] | **tftp server** *ipv6-address*} *file-name*
- 导入 SCVPN 主机验证绑定表：**import scvpn user-host-binding from** {**ftp server** *ipv6-address* [**user** *username* **password** *string*] | **tftp server** *ipv6-address*} *file-name*
- 导入 URL 数据库信息：**import urlfilter-database from** {**ftp server** *ipv6-address* [**user** *username* **password** *string*] | **tftp server** *ipv6-address*} *file-name*

{b}提示: {/b}关于命令参数的详细说明，请参考<防火墙>相关章节。

IPv6 SNMP 管理配置

StoneOS 支持通过 SNMP 网络管理协议查看设备上通用的 IPv6 相关 MIB 信息。设备的SNMP IPv6 相关配置包括:

- 配置 IPv6 管理主机
- 配置 IPv6 Trap 报文目标主机
- 创建 SNMPv3 用户（IPv6 远程管理主机）

配置 IPv6 管理主机

配置 IPv6 管理主机，在全局配置模式下，使用以下命令:

snmp-server ipv6-host {*host-name* | *ipv6-address*} {**version** [*1* | *2c*] **community** *string* [**ro** | **rw**] | **version** *3*}

- *host-name* | *ipv6-address* – 指定管理主机的主机名称或者 IPv6 地址。
- **version** [*1* | *2c*] – 指定 SNMP 的版本为 SNMPv1 或者 SNMPv2C。
- **community** *string* – 团体字是管理进程和代理进程之间的口令，因此与设备认可的团体字不符的 SNMP 报文将被丢弃。该参数指定主机的团体字，取值范围为一个最多 31 位的字符串，且仅当 SNMP 为 v1 和 v2C 版本时有效。
- **ro** | **rw** – 指定该团体字的读写权限。ro 为只读，此类团体字只可读取 MIB 中的信息；rw 为可读可写，此类团体字不仅可以读取 MIB 中的信息，还可以对信息进行修改。此项为可选，默认情况下，团体字的访问权限为只读。
- **version** *3* – 指定 SNMP 的版本为 SNMPv3。

全局配置模式下使用 **no snmp-server ipv6-host** {*host-name* | *ipv6-address*}命令删除指定的 IPv6 管理主机。

配置 IPv6 Trap 报文目标主机

用户可以配置接收 SNMP trap 报文的 IPv6 目标主机。配置 IPv6 trap 报文目标主机地址，在全局配置模式下使用以下命令:

snmp-server ipv6-trap-host {*host-name* | *ipv6-address*} {**version** {*1* | *2c*} **community** *string* | **version** *3* **user** *user-name* **engineID** *string* } [**port** *port-number*]

- *host-name* / *ipv6-address* – 指定 trap 报文目标主机的主机名称或者 IPv6 地址。

- **version** {*1* | *2c*} – 指定使用 SNMPv1 或者 SNMPv2C 发送 trap 报文。
- **community** *string* – 指定 SNMPv1 或者 SNMPv2C 的团体字。
- **version** *3* – 指定使用 SNMPv3 发送 trap 报文。
- **user** *user-name* – 指定已配置的 SNMPv3 用户名。
- **engineID** *string* – 指定 trap 报文目标主机的引擎 ID 号。
- **port** *port-number* – 指定接收trap 报文的目标主机端口号。取值范围为 1 到 65535，默认值为 162。

在全局配置模式下使用 **no snmp-server ipv6-trap-host** {*host-name* | *ip-address*}命令删除指定的 trap 报文目标主机。

创建 SNMPv3 用户（IPv6 远程管理主机）

配置 SNMPv3 用户，请在全局配置模式下使用以下命令：

snmp-server user *user-name* **group** *group-name* **v3** {**remote** *remote-ip* | **ipv6-remote** *ipv6-address*} [**auth-protocol** {**md5** | **sha**} *auth-pass* [**enc-protocol** {**des** | **aes**} *enc-pass*]]

- **user** *user-name* – 指定用户名称。取值范围为 1 到 31 个字符。
- **group** *group-name* – 为所创建的用户指定已经配置好的用户组。
- **remote** *remote-ip* – 指定远程管理主机的 IP 地址。
- **ipv6-remote** *ipv6-address* – 指定远程 IPv6 管理主机的地址。
- **auth-protocol** {**md5** | **sha**} – 指定用户安全级别为需要认证且认证协议可以为MD5 或 SHA 算法。如不输入此参数，则默认是无认证，无加密模式。
- *auth-pass* – 指定认证密码。取值范围为 8 到 40 个字符。
- **enc-protocol** {**des** | **aes**} – 指定用户安全级别为加密且加密协议为 DES 或者 AES。
- *enc-pass* – 指定加密密码。取值范围为 8 到 40 个字符。

系统最多允许配置 25 个用户。在全局配置模式下使用 **no snmp-server user** *user-name* 命令删除指定的用户。

IPv6 系统调试配置

StoneOS 支持 IPv6 地址的Ping 功能。执行 IPv6 地址的 Ping 功能，在任何模式下，使用以下命令：

ping ipv6 *ipv6-address* [**count** *number*] [**size** *number*] [**source** {*ipv6-address* | *interface-name*}] [**timeout** *time*] [**vrouter** *vr-name*]

- *ipv6-address* – 指定接受Ping 报文的目的地址。
- **count** *number* – 指定发送Ping 包的个数。范围是 1 到 65535。默认个数为 5。
- **size** *number* – 指定发送Ping 包的大小。范围是 28 到 65535 字节（byte）。
- **source** {*ipv6-address* | *interface-name*} – 指定发送Ping包的源地址，可以是接口的 IP 地址也可以是接口名称。
- **timeout** *time* – 指定发送Ping 包的超时时间。范围是 0 到 3600 秒。默认值是 0，即为没有超时时间限制。
- **vrouter** *vr-name* – 指定发送 Ping 包的 VRouter。

IPv6 路由配置

StoneOS 支持 IPv6 的目的路由（DBR）、源路由（SBR）以及源接口路由（SIBR）。IPv6 的路由配置需要在 VRouter 配置模式下进行。进入VRouter 配置模式，在全局配置模式下使用以下命令：

ip vrouter *vrouter-name*

- *vrouter-name* – 指定 VRouter 的名称。执行该命令后，系统进入指定名称的VRouter 配置模式。

配置 IPv6 目的路由条目

在 VRouter 配置模式下使用以下命令添加一条目的路由条目：

ipv6 route *ipv6-address/M* {**null0** | *ipv6-address* | **vrouter** *vrouter-name* | *interface-name* [*ipv6-address*]} [*distance-value*] [**name** *name*] [**weight** *weight-value*]

- *ipv6-address/M* – 指定目的地址网段。
- **null0**- 指定为 Null0 接口（黑洞路由）。
- *ipv6-address* | **vrouter** *vrouter-name* | *interface-name* [*ipv6-address*] – 指定下一跳。可以是网关地址（ipv6-address）、VRouter（vrouter vrouter-name）或者接口（interface-name）。
- *distance-value* – 指定路由的管理距离大小。该参数设定路由的优先级，取值越小，优先级越高，而在有多条路由选择的时候，优先级高的路由会被优先使用。取值范围是 1 到 255，默认值为 1。当路由距离为 255 时，该路由无效。
- *name* – 指定路由名称。

- *weight-value* – 指定路由权值的大小。路由权值决定负载均衡中流量转发的比重。范围是 1 到 255，默认值是 1。

使用多条该命令添加多条目的路由条目。

使用以上命令 no 的形式删除指定的目的路由条目：

no ipv6 route *ipv6-address/M* { **null0** | *ipv6-address* | **vrouter** *vrouter-name* | *interface-name* [*ipv6-address*]}

配置 IPv6 源路由条目

在 VRouter 配置模式下，使用以下命令添加一条源路由条目：

ipv6 route source *ipv6-address/M* { **null0** | *ipv6-address* / *interface-name* | **vrouter** *vrouter-name* } [*distance-value*] [**name** *name*] [**weight** *weight-value*]

- *ipv6-address/M* – 指定源地址网段。
- **null0**- 指定为 Null0 接口（黑洞路由）。
- *A.B.C.D* / *interface-name* | **vrouter** *vrouter-name* – 指定下一跳。可以是网关地址（ipv6-address）、VRouter（vrouter vrouter-name）或者接口（interface-name）。
- *distance-value* – 指定路由的管理距离大小。该参数设定路由的优先级，取值越小，优先级越高，而在有多条路由选择的时候，优先级高的路由会被优先使用。取值范围是 1 到 255，默认值为 1。当路由距离为 255 时，该路由无效。
- *name* – 指定路由名称。
- *weight-value* – 指定路由权值的大小。路由权值决定负载均衡中流量转发的权重。范围是 1 到 255，默认值是 1。

使用多条该命令添加多条源路由条目。

使用以上命令 no 的形式删除指定的源路由条目：

no ipv6 route source *ipv6-address/M* { **null0** | *ipv6-address* / *interface-name* | **vrouter** *vrouter-name*}

配置源接口路由

在 VRouter 配置模式下，使用以下命令添加一条源接口路由条目：

ipv6 route source in-interface *interface-name ipv6-address/M* { **null0** | *ipv6-address* / *interface-name*| **vrouter** *vrouter-name* } [*distance-value*] [**name** *name*] [**weight** *weight-value*]

- *interface-name* – 指定路由条目的入接口。
- **null0**- 指定为 Null0 接口（黑洞路由）。

- *ipv6-address/M* – 指定源地址网段。
- *ipv6-address* | *interface-name* | **vrouter** *vrouter-name* – 指定下一跳。可以是网关地址（ipv6-address）、VRouter（vrouter vrouter-name）或者接口（interface-name）。
- *distance-value* – 指定路由的管理距离大小。该参数设定路由的优先级，取值越小，优先级越高，而在有多条路由选择的时候，优先级高的路由会被优先使用。取值范围是 1 到 255，默认值为 1。当路由距离为 255 时，该路由无效。
- *name* – 指定路由名称。
- *weight-value* – 指定路由权值的大小。路由权值决定负载均衡中流量转发的权重。范围是 1 到 255，默认值是 1。

使用多条该命令添加多条源接口路由条目。

使用以上命令 no 的形式删除指定的源接口路由条目：

no ipv6 route source in-interface *interface-name ipv6-address/M* { **null0** | *ipv6-address* | *interface-name* | **vrouter** *vrouter-name* }

查看 IPv6 路由信息

查看 IPv6 路由信息，在任何模式下使用以下命令：

- 查看目的路由信息：**show ipv6 route static** [**vrouter** *vr-name*]
- 查看源接口路由信息：**show ipv6 route source in-interface** *interface-name*
- 查看直连路由信息：**show ipv6 route connected** [**vrouter** *vr-name*]
- 查看指定目的地址的路由信息：**show ipv6 route** *ipv6-address/[M]* [**vrouter** *vr-name*]
- 查看系统 IPv6 路由的统计信息：**show ipv6 route summary** [**vrouter** *vr-name*]
- 查看 IPv6 FIB 表信息：**show ipv6 fib** [**source** | **source in-interface** *interface-name* | *ipv6-address/[M]* | **summary**] [**vrouter** *vr-name*]

配置 RIPng 动态路由

RIPng (RIP next generation，下一代 RIP 协议）是对原来的 IPv4 网络中 RIP-2 协议的扩展。大多数 RIP 的概念都可以用于 RIPng。

为了在 IPv6 网络中应用，RIPng 对原有的 RIP 协议进行了如下修改：

- UDP 端口号：使用UDP 的 521 端口发送和接收路由信息。
- 组播地址：使用FF02::9 作为链路本地范围内的 RIPng 路由器组播地址。

- 前缀长度：目的地址使用 128 比特的前缀长度。
- 下一跳地址：使用 128 比特的 IPv6 地址。
- 源地址：使用链路本地地址 FE80::/10 作为源地址发送 RIPng 路由信息更新报文。

对 RIPng 协议的配置包括基本配置、引入路由、被动接口、网络和距离。另外，RIPng 参数配置完成后，用户还需要在不同的接口上配置 RIPng 参数，包括指定接口水平分割以及接口的中毒反转。

基本配置

RIPng 协议的基本配置包括指定缺省度量、指定缺省距离、配置缺省信息发布以及配置定时器（时间间隔、失效时间和清除时间）。用户可以为不同的VRouter 分别配置 RIPng 协议。对 RIPng 协议的基本配置需要在 RIPng 路由模式下进行。进入 RIPng 路由模式，请在全局配置模式下，使用以下命令：

ip vrouter *vrouter-name* （进入VRouter 配置模式）

ipv6 router rip（进入 RIPng 路由模式，同时开启设备的 RIPng 功能。每个 RIPng 进程之间相互独立，每个虚拟路由器可以创建一个 RIPng 进程。）

在 VRouter 配置模式下，使用 **no ipv6 router rip** 关闭 RIPng 功能。

指定缺省度量

RIPng 协议使用跳数来衡量到达目的网络的距离，称为度量。路由器到与它直接相连网络的度量为 1，通过一个路由器可达的网络的度量为 2，依此类推，度量的最大值可以到 15，度量大于 15 的网络为不可达网络。缺省度量在引入路由时生效。指定 RIPng 的缺省度量，在 RIPng 路由配置模式下使用以下命令：

default-metric *value*

- *value* – 指定缺省度量值。范围是 1 到 15，默认值是 1。

使用 **no default-metric** 命令恢复缺省度量值。

指定缺省距离

指定 RIPng 路由的缺省距离，在 RIPng 路由配置模式下使用以下命令：

distance *distance-value*

- *distance-value* – 指定缺省管理距离。范围是 1 到 255，默认值是 120。

使用 **no distance** 命令恢复缺省距离值。

配置定时器

RIPng 可配置的定时器分别是时间间隔（Interval）、失效时间（Invalid）、和清除时间（Flush）。具体描述如下：

- 时间间隔：每次向所有邻居发送全部 RIPng 路由所间隔的时间。默认是 30 秒。
- 失效时间：如果一条路由在失效时间内一直没有被更新，该路由的度量就会被标记为 16，表示为不可达路由。默认的失效时间是 180 秒。
- 清除时间：度量被标记为 16 的不可达路由会一直被发布到其它 RIPng 协议路由，直到清除时间结束；如果该路由仍没有被更新，清除时间结束后，将会被从 RIPng 路由信息数据库中删除。默认的清除时间是 120 秒。

用户可以修改以上三个定时器的时间值。配置定时器，在 RIPng 路由配置模式下使用以下命令：

timers basic *interval-time invalid-time flush-time*

- *interval-time* – 指定发送更新的时间间隔，单位为秒。范围是 0 到 16777215 秒。默认值是 30 秒。
- *invalid-time* – 指定路由的失效时间，单位为秒。范围是 1 到 16777215 秒。默认值是 180 秒。
- *flush-time* – 指定路由的清除时间，单位为秒。范围是 1 到 16777215 秒。默认值是 120 秒。

使用 **no timers basic** 命令恢复定时器的默认值。

配置缺省信息发布

用户可以指定是否将默认路由发布到其它使用 RIPng 协议的路由器。默认情况下，RIPng 协议不发送默认路由。配置缺省信息发布，在 RIPng 路由配置模式下使用以下命令：

发送：**default-information originate**

不发送：**no default-information originate**

引入路由

RIPng 协议允许用户将设备上其它路由协议（IPv6 BGP、直连、静态和 OSPFv3）的路由信息引入到 RIPng 中，并向外发布。同时，用户可以设置被引入路由的度量。配置引入路由，在 RIPng 路由配置模式下使用以下命令：

redistribute {**bgp** | **connected** | **static** | **ospf**} [**metric** *value*]

- **bgp** | **connected** | **static** | **ospf** – 指定引入路由的类型，可以是 IPv6 BGP（bgp）、直连路由（connected）、静态路由（static）或者 OSPFv3（ospfv3）。
- **metric** *value* – 指定引入路由的度量。范围是 1 到 15。如果不指定该数值，系统会使用 RIPng 的缺省度量（通过 default-metric value 配置）。

用户可以配置多条该命令引入不同类型的路由。

使用 **no redistribute** {**bgp** | **connected** | **static** | **ospfv3**}命令取消指定类型路由的引入。

配置网络

用户需要配置一些网络，只有在指定网络中的接口才能接收和发送 RIPng 更新。配置网络，在 RIPng 路由配置模式下使用以下命令：

network {*interface-name* | *X:X:X:X::X/M*}

- *interface-name* – 指定接口所在的网络。
- *X:X:X:X::X/M* – 指定网络的 IPv6 地址。

用户可以配置多条该命令添加多个网络。

使用 **no network** {*interface-name* | *X:X:X:X::X/M*}命令删除指定的网络。

配置被动接口

用户可以将一些接口配置为只接收更新但是不发送，这种只接收更新的接口就是被动接口。配置被动接口，在 RIPng 路由配置模式下使用以下命令：

passive-interface *interface-name*

- *interface-name* – 指定接口的名称作为被动接口。

用户可以配置多条该命令添加多个被动接口。

使用 **no passive-interface** *interface-name* 命令取消被动接口的配置。

配置接口的水平分割

水平分割是指不从本接口发送从该接口学到的路由。它可以在一定程度上避免产生路由环，保证路由的正确传播。配置水平分割功能，在接口配置模式下，使用以下命令：

开启水平分割：**ipv6 rip split-horizon**

关闭水平分割：**no ipv6 rip split-horizon**

配置接口的中毒反转

中毒反转是指：收到路由中毒消息的路由器，不遵守水平分割原则将中毒消息转发给所有的相邻路由器，也包括发送中毒信息的源路由器，从而通告相邻路由器这条路由信息已失效。配置中毒反转功能，在接口配置模式下，使用一下命令：

开启中毒反转：**ipv6 rip poison-reverse**

关闭中毒反转：**no ipv6 rip poison-reverse**

显示系统 RIPng 信息

用户可以通过 show 命令随时查看系统的 RIPng 信息。查看 RIPng 信息，在任何模式下使用以下命令：

show ipv6 rip

运行 RIPng 协议的VR 拥有一个 RIPng 路由数据库，该数据库中储存了所有可达目的网络的路由条目。路由条目包含的信息有目的地址、下一跳、度量、来源以及定时器信息。用户可以在任何模式下，通过以下命令，随时查看 RIPng 数据库的信息：

show ipv6 rip database [**vrouter** *vrouter-name*]

- **vrouter** *vrouter-name* – 显示指定 VRouter 的 RIPng 信息。

配置 OSPFv3 动态路由

OSPFv3 是OSPF（Open Shortest Path First，开放式最短路径优先）的第 3 个版本，主要提供对 IPv6 的支持。

OSPFv3 和 OSPFv2 在很多方面是相同的：

- Router ID，Area ID 仍然是 32 位的。
- 相同类型的报文：Hello 报文，DD（Database Description，数据库描述）报文，LSR（Link State Request，链路状态请求）报文，LSU（Link State Update，链路状态更新）报文和 LSAck（Link State Acknowledgment，链路状态确认）报文。
- 相同的邻居发现机制和邻接形成机制。
- 相同的 LSA 扩散机制和老化机制。

OSPFv3 和 OSPFv2 的不同主要有：

- OSPFv3 是基于链路（Link）运行，OSPFv2 是基于网段（Network）运行。
- OSPFv3 在同一条链路上可以运行多个实例。
- OSPFv3 是通过 Router ID 来标识邻接的邻居。OSPFv2 则是通过 IP 地址来标识邻接的邻居。

用户可以为不同的VRouter 分别配置OSPFv3 协议。OSPFv3 协议配置包括以下各项：

- 配置 Router ID
- 配置区域的虚拟链路
- 配置缺省度量

- 配置缺省管理距离
- 配置缺省路由发布
- 指定接口区域及实例
- 配置引入路由
- 配置被动接口
- 配置 OSPFv3 接口定时器
- 指定接口路由器优先级
- 指定接口的链路花费
- 关闭/开启 OSPFv3 协议
- 配置接口 MTU 匹配检查

OSPFv3 协议的基本配置需要在OSPFv3 路由模式下进行。进入 OSPFv3 路由模式，请在配置模式下，使用以下命令：

ip vrouter *vrouter-name* （进入VRouter 配置模式）

ipv6 router ospf（进入 OSPFv3 路由模式，并创建OSPFv3 进程。每个OSPFv3 进程之间相互独立，每个虚拟路由器可以创建一个OSPFv3 进程。）

在 VRouter 配置模式下，使用 **no ipv6 router ospf** 关闭 OSPFv3 进程。

配置 Router ID

每一台运行 OSPFv3 协议的路由器都必须拥有一个 Router ID。Router ID 是每个路由器在整个 OSPFv3 自治系统中唯一标识，使用 IP 地址的形式表示。为设备的OSPFv3 协议配置 Router ID，在 OSPFv3 路由模式下，使用以下命令：

router-id *A.B.C.D*

- *A.B.C.D* – 指定OSPFv3 协议使用的 Router ID，为 IP 地址形式。

配置区域的虚拟链路

非骨干区域之间的路由信息必须通过骨干区域来转发。对此，OSPFv3 有两个规定：

- 所有非骨干区域必须与骨干区域保持连通；
- 骨干区域自身也必须保持连通。

但在实际应用中，可能会因为各方面条件的限制，无法满足这个要求。这时可以通过配置OSPF 虚连接（Virtual Link）予以解决。虚拟链路用来保持非骨干区域与骨干区域的连通，以及保持骨干区域自身的连

通。虚链路总是建立在两台区域边界路由器(ABR)之间，且必须在两端同时配置才能生效。其中至少一台ABR 属于骨干区域。配置虚拟链路，在OSPFv3 路由模式下，使用以下命令：

area { *id* | *A.B.C.D* } **virtual-link** *A.B.C.D*

- *id* | *A.B.C.D* – 指定虚拟链路穿过的区域 ID。区域 ID 用 32 比特数来表示，可以是数字形式，也可以是 IP 地址形式。
- *A.B.C.D* – 指定虚拟链路对端ABR 的 Router ID。

指定缺省度量

指定OSPFv3 协议的缺省度量。如果引入路由时没有配置度量值，则指定的缺省度量在引入路由时生效。指定OSPFv3 的缺省度量，在OSPFv3 路由配置模式下使用以下命令：

default-metric *value*

- *value* – 指定缺省度量值。范围是 1 到 16777214。

使用 **no default-metric** 命令恢复缺省度量的默认值。

配置缺省管理距离

用户可以根据路由类型指定管理距离。配置距离，在 OSPFv3 路由配置模式下使用以下命令：

distance {*distance-value* | **ospf** [**intra-area** *distance-value* | **inter-area** *distance-value* | **external** *distance-value*}

- *distance-value* – 指定所有路由的管理距离。默认值是 110。范围是 1 到 255。
- **intra-area** *distance-value* – 指定区域内路由的管理距离。默认值是 110。范围是 1 到 255。
- **inter-area** *distance-value* – 指定区域间路由的管理距离。默认值是 110。范围是 1 到 255。
- **external** *distance-value* – 指定外部类型路由的管理距离。默认值是 110。范围是 1 到 255。

使用 **no distance ospf** 命令恢复距离的默认值。

配置缺省路由发布

用户可以指定是否将缺省路由通告到本区域内其他的路由器。配置缺省路由发布，在OSPF 路由配置模式下使用以下命令：

default-information originate [**always**] [**type** {1 | 2}] [**metric** value]

- **always** – 指定 always 参数时，当前路由器产生并通告默认路由。如果当前路由器不存在缺省路由，会引入一条缺省路由并通告出去。这条缺省路由的下一跳指向当前路由器。当不指定always 参数时，如果当前路由器不存在缺省路由，将不会通告缺省路由。

- **type** {1 | 2} – 指定与发送到 OSPF 路由域的缺省路由相关联的外部路由的类型。1 指 type1 外部路由，这类路由的可信程度较高，并且和OSPFv3 自身路由的开销具有可比性，所以到第一类外部路由的开销等于当前路由器到相应的ASBR 的开销与ASBR 到该路由目的地址的开销之和。2 指 type2 外部路由，这类路由的可信度比较低，所以OSPF 协议认为从 ASBR 到自治系统之外的开销远远大于在自治系统之内到达ASBR 的开销。所以计算路由开销时将主要考虑前者，即到第二类外部路由的开销等于ASBR 到该路由目的地址的开销。如果计算出开销值相等的两条路由，再考虑本路由器到相应的ASBR 的开销。

- **metric** *value* – 指定缺省路由的度量。范围是 0 到 16777214。如果不使用该命令配置度量并且也没有使用 **default-metric** *value* 配置默认度量，其默认度量将会是 20。

使用 **no default-information originate** 命令恢复默认值。

指定接口区域及实例

在接口配置模式下，指定接口所属的 OSPFv3 区域及实例。

ipv6 ospf area { *A.B.C.D* | *id*} {**instance** *id*}

- **area** { *A.B.C.D* | *id*} – 指定接口所属区域的 ID。区域 ID 用 32 比特数来表示，可以是数字形式，也可以是 IP 地址形式。

- **instance** *id* – 指定接口所属的实例 ID。建立邻居关系的接口必须属于相同的实例。取值范围是 0 到 255。默认值是 0。

使用 **no ipv6 ospf area** { *A.B.C.D* | *id*}取消接口上的区域及实例配置。

配置引入路由

OSPFv3 协议允许用户引入其它路由协议（BGP、直连、静态和 RIPng）的路由信息，并向外发布。同时，用户可以设置被引入路由的度量以及外部路由的类型。配置引入路由，在 OSPF 路由配置模式下使用以下命令：

redistribute {**bgp** | **connected** | **static** | **ripng**} [**type** {**1** | **2**}] [**metric** *value*]

- **bgp** | **connected** | **static** | **ripng** – 指定引入路由的类型，可以是 BGP（bgp）、直连路由（connected）、静态路由（static）或者 RIPng（ripng）。

- **type** {1 | 2} – 指定外部路由的类型。1 指 type1 外部路由，2 指 type2 外部路由。

- **metric** *value* – 指定引入路由的度量。范围是 0 到 16777214。如果不指定该数值，系统会使用OSPF 的缺省度量（通过 **default-metric** *value* 配置）。

用户可以配置多条该命令引入不同类型的路由。

使用 **no redistribute** {**bgp** | **connected** | **static** | **rip**}命令取消指定类型路由的引入。

配置被动接口

用户可以将一些接口配置为只接收更新但是不发送，这种只接收更新的接口就是被动接口。配置被动接口，在接口配置模式下使用以下命令：

ipv6 ospf passive

用户可以配置多条该命令添加多个被动接口。

使用 **no ipv6 ospf passive** 命令取消被动接口的配置。

配置 OSPFv3 接口定时器

接口的定时器有以下四个：接口发送 Hello 包的时间间隔、接口相邻路由器的失效时间、接口重传 LSA 的时间间隔以及接口更新包的延迟时间。

指定接口发送 Hello 包的时间间隔，在接口配置模式下，使用以下命令：

ipv6 ospf hello-interval *interval*

- *interval* – 指定接口发送Hello 包的时间间隔，单位为秒。默认值是 10 秒。范围是 1 到 65535 秒。

使用 **no ipv6 ospf hello-interval** 恢复默认时间间隔。

如果接口在一定的时间内都没有收到邻居的 Hello 报文，则认为邻居路由器失效，这个一定的时间就是相邻路由器间的失效时间。指定接口的相邻路由失效时间，在接口配置模式下，使用以下命令：

ipv6 ospf dead-interval *interval*

- *interval* – 指定接口的相邻路由器失效时间，单位为秒。默认值是 40 秒（发送 Hello 包时间间隔的 4 倍）。范围是 1 到 65535 秒。

使用 **no ipv6 ospf dead-interval** 恢复默认失效时间。

ipv6 ospf retransmit-interval *interval*

- *interval* – 指定接口重传 LSA 的时间间隔，单位为秒。默认值是 5 秒。范围是 3 到 65535 秒。

使用 **no ipv6 ospf retransmit-interval** 恢复默认时间间隔。

ipv6 ospf transmit-delay *interval*

- *interval* – 指定接口更新包的延迟时间，单位为秒。默认值是 1 秒。范围是 1 到 65535 秒。

使用 **no ipv6 ospf transmit-delay** 恢复默认延迟时间。

指定接口路由器优先级

路由器的优先级用来决定使用哪个路由器作为指定路由器。指定路由器用来接收网络中所有其它路由器的链路信息，并将收到的链路信息广播出去。指定接口路由器的优先级，在接口配置模式下，使用以下命 令:

ipv6 ospf priority *level*

- *level* – 指定路由器的优先级。默认值是 1。范围是 0 到 255。优先级为 0 的路由器不会被选中作为指定路由器。当同一个网络的两个路由器都可作为指定路由器时，优先级高的路由器会被选中；如果优先级也相同，Router ID 高的会被选中。

使用 **no ipv6 ospf priority** 命令恢复默认优先级。

配置接口的链路花费

OSPF 有两种方式来配置接口的花费:

- 在接口配置模式下直接配置花费;
- 配置接口的带宽参考值，OSPFv3 根据带宽参考值自动计算接口的花费。

指定接口的花费，在接口配置模式下，使用以下命令:

ipv6 ospf cost *cost-value*

- *cost-value* – 指定接口的花费。取值范围是 1 到 65535。

使用 **no ipv6 ospf cost** 命令取消对所需花费的指定。

OSPFv3 可以根据接口的带宽计算接口发送 OSPFv3 报文的花费。指定接口带宽值，在OSPFv3 路由模式下，使用以下命令:

auto-cost reference-bandwidth *bandwidth*

- *bandwidth* – 指定接口带宽值，单位为 Mbps，默认值是 100。范围是 1 到 4294967。

使用 **no auto-cost reference-bandwidth** 命令恢复默认的带宽值。

配置接口 MTU 匹配检查

OSPFv3 通过 DBD 报文检查邻居间的接口 MTU 设置是否匹配。如果相邻的OSPFv3 路由器接口之间的 MTU 不匹配，则他们之间不能建立邻接关系。为了用户可通过修改接口的 MTU 来解决此问题。但是，有些接口无法修改 MTU。用户可对 OSPFv3 进行配置，使OSPFv3 忽略对 MTU 匹配的检查。

使 OSPFv3 忽略对MTU 匹配的检查，在接口配置模式下，使用如下命令:

ipv6 ospf mtu-ignore

使用 **no ipv6 ospf mtu-ignore** 命令恢复对邻居间接口MTU 匹配的检查。

关闭/开启 OSPFv3 协议

在接口上正常关闭OSPFv3 协议，在接口配置模式下，使用 **ipv6 ospf shutdown** 命令。

在接口上重新开启OSPFv3 协议，在接口配置模式下，使用 **no ipv6 ospf shutdown** 命令。

查看 OSPFv3 信息

显示OSPFv3 路由信息，在任何模式下使用以下命令:

show ipv6 ospf [**vrouter** *vrouter-name*]

- *vrouter-name* - 显示指定的VRouter 的 OSPF 路由信息。

显示OSPFv3 协议的数据库信息，在任何模式下使用以下命令:

show ipv6 ospf database

show ipv6 ospf database {**inter-router** | **external** | **network** | **router** | **inter-prefix** | **link** | **intra-prefix**} [*A.B.C.D*] [{**adv-router** *A.B.C.D*} | **self-originate**] [**vrouter** *vrouter-name*]

- **inter-router** – 此类型 LSA 显示到本自治系统内的ASBR 的路由。该 LSA 由 ABR 生成，在与该 LSA 相关的区域内传播。每一条 inter-router 类型的 LSA 描述了一条到达本自治系统内的 ASBR（Autonomous System Border Router，自治系统边界路由器）的路由。
- **external** – 此类型 LSA 显示到自治系统系统外部的路由。由ASBR 生成，描述到达其它 AS（Autonomous System，自治系统）的路由，传播到整个 AS（Stub 区域除外）。
- **network** – 此类型 LSA 的链路状态显示本网段接口的链路状态。由广播网络和 NBMA（Non-Broadcast Multi-Access）网络的 DR（Designated Router，指定路由器）生成，描述本网段接口的链路状态，只在 DR 所处区域内传播。
- **router** – 此类型 LSA 由每个路由器生成，描述本路由器的链路状态和开销，只在路由器所处区域内传播。
- **inter-prefix** – 该类型 LSA 显示到本自治系统内其他区域的 IPv6 地址前缀的路由。该 LSA 由 ABR（Area Border Router，区域边界路由器）生成，在与该 LSA 相关的区域内传播。每一条 inter-prefix LSA 描述了一条到达本自治系统内其他区域的 IPv6 地址前缀（IPv6 Address Prefix）的路由。
- **link** – 路由器为每一条链路生成一个 link 类型的 LSA，在本地链路范围内传播。每一个 Link 类型的 LSA 描述了该链路上所连接的 IPv6 地址前缀及路由器的 Link-local 地址。

- **intra-prefix** - 每个该类型 LSA 包含路由器上的IPv6 前缀信息，Stub 区域信息或穿越区域（Transit Area）的网段信息，该LSA 在区域内传播。由router 类型 LSA 和 network 类型 LSA 不再包含地址信息，导致了 intra-prefix 类型 LSA 的引入。
- *A.B.C.D* - 链路状态 ID，以 IP 地址形式表示。
- **adv-router** *A.B.C.D* – 显示指定路由器的 LSAs。
- **self-originate** - 只显示自己产生的 LSA（从本地路由器）。
- *vrouter-name* - 指定 VRouter 名称。

显示OSPF 接口信息，在任何模式下使用以下命令：

show ipv6 ospf interface [*interface-name*] [**vrouter** *vrouter-name*]

显 示OSPF 邻居信息，在任何模式下使用以下命令：

show ip ospf neighbor [*A.B.C.D* | **detail**][**vrouter** *vrouter-name*]

显 示OSPF 边界路由器信息，在任何模式下使用以下命令：

show ipv6 ospf border-routers [*A.B.C.D*][**vrouter** *vrouter-name*]

显 示OSPF 路由信息，在任何模式下使用以下命令：

show ip ospf route [*X:X:X:X::X/M* [**vrouter** *vrouter-name*]

配置 IPv6 BGP 动态路由

BGP-4 只能管理 IPv4 的路由信息，对于使用其它网络层协议（如 IPv6 等）的应用，在跨自治系统传播时就受到一定限制。

为了提供对多种网络层协议的支持，IETF 对 BGP-4 进行了扩展，形成 MP-BGP（Multiprotocol Border Gateway Protocol，多协议边界网关协议）。其中，针对 IPv6 地址族的 BGP 扩展，称为 IPv6 BGP。IPv6 BGP 是利用 BGP 的多协议扩展属性，来达到在 IPv6 网络中应用的目的，BGP-4 原有的消息机制和路由机制并没有改变。

用户在对 IPv6 BGP 如下内容进行配置时，请参考《StoneOS 命令行用户手册_路由》中“BGP 配置”部分的相应章节。

- 配置对等体(对等体组)
- 等价负载均衡
- 配置定时器
- 配置 MD5 认证
- 关闭对等体或者对等体组

- 配置 EBGP 多跳
- 配置描述信息
- 配置 BGP 对等体定时器

本节介绍如下针对 IPv6 BGP 的配置：

- 引入 IPv6 单播路由
- 激活 BGP 连接
- 配置向对等体或者对等体组发送团体属性
- 配置前缀的最大接收长度

进入 IPv6 单播路由配置模式

对 IPv6 单播路由进行相关配置，需进入 IPv6 单播路由配置模式。进入 IPv6 单播路由配置模式，在 BGP 实例配置模式下，使用如下命令：

address-family ipv6 unicast

引入 IPv6 单播路由

IPv6 BGP 支持引入 IPv6 单播路由。允许用户引入其它路由协议（OSPFv3、直连、静态和 RIPng）的路由信息，并向外发布。同时，用户可以设置被引入路由的度量。配置引入路由，在 IPv6 单播路由配置模式下使用以下命令：

redistribute {**ospf** | **connected** | **static** | **rip**} [**metric** *value*]

- **ospf** | **connected** | **static** | **rip** – 指定引入路由的类型，可以是OSPFv3（ospf）、直连路由（connected）、静态路由（static）或者 RIPng（rip）。
- **metric** *value* – 指定引入路由的度量。范围是 0 到 4294967295。

用户可以配置多条该命令引入不同类型的路由。

使用 **no redistribute** {**ospf** | **connected** | **static** | **rip**}命令取消指定类型路由的引入。

激活 BGP 连接

默认情况下，已配置的对等体或者对等体组与当前设备的 IPv6 BGP 连接是激活的。用户可以关闭连接也可以重新激活 IPv6 BGP 连接。激活 IPv6 BGP 连接，在 IPv6 单播路由配置模式下，使用以下命令：

neighbor {*X:X:X:X::X* | *A.B.C.D* | *peer-group*} **activate**

- *X:X:X:X::X* | *A.B.C.D* | *peer-group* – 指定对等体 IPv6/IPv4 地址或者对等体组的名称。

在 IPv6 单播路由配置模式下使用该命令 no 的形式关闭指定对等体或者对等体组的 IPv6 BGP 连接：

no neighbor {*X:X:X:X::X* | *A.B.C.D* | *peer-group*} **activate**

配置向对等体或者对等体组发送团体属性

配置向对等体（对等体组）发送团体属性，在 IPv6 单播路由配置模式下，使用以下命令：

neighbor {*X:X:X:X::X* | *A.B.C.D* | *peer-group*} **send-community** {**standard** | **extended** | **both**}

- {*X:X:X:X::X* | *A.B.C.D* | *peer-group*} – 指定 BGP 对等体的 IPv6/IPv4 地址或者对等体组的名称。
- **standard** | **extended** | **both** – 指定发送团体属性的类别，可以是标准团体属性（standard），扩展团体属性（extended），或者标准团体属性和扩展团体属性（both）。

使用该命令 no 的形式取消发送团体属性配置：

no neighbor {*X:X:X:X::X* | *A.B.C.D* | *peer-group*} **send-community**

配置接收的最大前缀数

配置允许从 IPv6 对等体/IPv6 对等体组接收的最大 IPv6 地址前缀数，在 IPv6 单播路由配置模式下，使用如下命令：

neighbor {*X:X:X:X::X* | *A.B.C.D* | *peer-group*} **maximum-prefix** *maximum* [*threshold*] [**restart** *restart-interval*] [**warning-only**]

- {*X:X:X:X::X* | *A.B.C.D* | *peer-group*} – 指定 BGP 对等体的 IPv6/IPv4 地址或者对等体组的名称。
- *maximum* - 指定从 IPv6 对等体/IPv6 对等体组接收的最大 IPv6 地址前缀数。
- *threshold* – 指定产生日志信息的警戒值。当接收到的前缀达到此警戒值时，系统产生日志信息。取值范围为 1 到 100。默认值是 75。
- **restart** *restart-interval* – 当接收的前缀达到警戒值后，断开与对等体会话并在指定的时间间隔后与对等体重建会话，单位为分钟。取值范围为 1 到 65525。
- **warning-only** – 当接收的前缀达到警戒值后，产生相应的日志信息。

使用该命令 no 的形式取消最大前缀数的配置：

no neighbor {*X:X:X:X::X* | *A.B.C.D* | *peer-group*} **maximum-prefix**

查看 BGP 信息

显示 IPv6 BGP 路由信息，在任何模式下使用以下命令：

show ip bgp ipv6 unicast {*X:X:X:X::X/Mask* | **vrouter** *vrouter-name*}

- *X:X:X:X::X/Mask* – 显示到指定网络的 IPv6 BGP 路由信息。
- *vrouter-name* - 显示指定VRouter 的 IPv6 BGP 路由信息。

显示所有 IPv6 BGP 连接的状态参数，包括前缀、路径和属性信息等，在任何模式下使用以下命令：

show ip bgp ipv6 unicast summary [**vrouter** *vrouter-name*]

- *vrouter-name* - 显示指定 VRouter 的 IPv6 BGP 连接状态参数。

显示 BGP 对等体状态，在任何模式下使用以下命令：

show ip bgp ipv6 unicast neighbor [*X:X:X:X::X* | *A.B.C.D*] [**vrouter** *vrouter-name*]

- *X:X:X:X::X* | *A.B.C.D* – 显示指定对等体的状态。指定 BGP 对等体的 IPv6/IPv4 地址。
- *vrouter-name* - 显示指定 VRouter 的 IPv6 BGP 对等体状态。

配置 IPv6 策略路由

策略路由功能检查数据包的源 IP、目的 IP 和服务类型，对匹配策略的数据包的下一跳进行指定。系统支持对 IPv6 格式的地址进行检测。

用户对 IPv6 PBR 如下内容进行配置时，请参考《StoneOS 命令行用户手册_路由》中“配置策略路由”一节。

- 编辑 PBR 策略规则
- 启用/禁用 PBR 策略规则
- 修改规则排列顺序
- 应用 PBR 策略

创建 PBR 策略

创建PBR 策略，在全局配置模式下使用以下命令：

pbr-policy *name*

- *name* – 指定 PBR 策略名，名称范围是 1 到 31 个字符。如果该策略已经创建，则直接进入PBR 策略配置模式。

使用 **no pbr-policy** *name* 删除指定的PBR 策略。

创建 IPv6 PBR 规则

进入PBR 策略配置模式下，用户便可定义自己的 IPv6 PBR 规则。在 CLI 中创建 IPv6 PBR 规则的命令如下：

match-v6 [**id** *rule-id*] [**before** *rule-id* | **after** *rule-id* | **top**] *src-addr dst-addr service-name* [*application-name*]
nexthop {*interface-name* / *A.B.C.D* | **vrouter** *vrouter-name* | **vsys** *vsys-name*} [**weight** *value*] [**track** *track-object-name*]

- **id** *rule-id* – 指定新建策略规则的 ID，取值范围为 1 到 255。如果不指定，系统将会为 PBR 规则自动分配一个 ID。规则 ID 在该PBR 策略中必须是唯一的。
- **before** *rule-id* | **after** *rule-id* | **top** – 指定 PBR 规则的位置，可以是某个规则之前（before rule-id）、某个规则之后（after rule-id）或者所有规则的首位（top）。默认情况下，系统会将新创建的策略规则放到所有规则的末尾。
- *src-addr* – 指定 IPv6 格式的源地址，该地址为地址簿条目。
- *dst-addr* – 指定 IPv6 格式的目的地址，该地址为地址簿条目。
- *service-name* – 指定服务名称。service-name 为服务簿中定义的服务。
- *application-name* – 指定应用名称。application-name 为应用簿中定义的应用。
- **nexthop** {*interface-name* / *A.B.C.D* | **vrouter** *vrouter-name* | **vsys** *vsys-name*} – 指定下一跳。interface-name 为出接口的名称，也可以是 link-local 地址；A.B.C.D 为下一跳的 IP 地址，vrouter vrouter-name 为 VRouter，vsys vsys-name 为虚拟系统。
- **weight** *value* – 指定下一跳的权重，取值范围是 1 到 255，默认值是 1。如果一条策略路由匹配多个下一跳，系统会按照权重值比例分配流量。
- **track** *track-object-name* – 指定下一跳的监测对象。如果监控对象失败，本条策略路由也会失败。关于如何配置监测对象，请参阅“系统管理“的“配置监测对象”部分。

使用该命令 no 的形式删除指定 ID 的规则。在PBR 策略配置模式下，执行以下命令：

no match-v6 id *rule-id*

另外，用户还可以在 PBR 策略配置模式下使用以下命令，创建一个策略规则 ID，并且进入 PBR 策略规则配置模式，再进一步配置其它策略规则相关参数：

match-v6 [**id** *rule-id*] [**before** *rule-id* | **after** *rule-id* | **top**]

- **id** *id* – 指定 PBR 策略规则的 ID。如果不指定，系统将会为策略规则自动分配一个 ID。规则 ID 在整个系统中必须是唯一的。策略规则的 ID 大小并不表示策略规则的匹配先后顺序。

- top | before *rule-id* | after *rule-id* – 指定策略规则的位置，可以是某个规则 ID 之前（before id）、某个规则 ID 之后（after id）或者所有规则的首位（top）。默认情况下，系统会将新创建的策略规则放到所有规则的末尾。

配置 IPv6 IS-IS 动态路由

IS-IS（Intermediate System-to-Intermediate System，中间系统到中间系统）支持多种网络层协议，其中包括 IPv6 协议，支持IPv6 协议的 IS-IS 路由协议又称为IPv6 IS-IS 动态路由协议。在 IPv6 网络环境中，可以通过配置 IPv6 IS-IS 路由协议来实现 IPv6 网络的互连。

用户在对 IPv6 IS-IS 如下内容进行配置时，请参考《StoneOS 命令行用户手册_路由》中“配置 IS-IS”部分的相应章节。

- 指定路由器类型
- 配置接口 IS-IS 类型
- 配置网络类型为点对点类型
- 配置 NET 地址
- 配置度量类型
- 配置 Hello 报文相关参数
- 配置 DIS 选举优先级
- 配置被动接口
- 配置 LSP 报文相关参数
- 配置主机名映射
- 配置认证
- 配置接口认证模式

本节介绍如下针对 IPv6 IS-IS 的配置:

- 使能接口 IPv6 IS-IS
- 配置接口度量值
- 进入 IPv6 单播路由配置模式
- 发布缺省路由
- 配置管理距离
- 引入路由

- 配置过载标志位
- 配置 SPF 计算时间间隔
- 查看 IPv6 IS-IS 路由信息

使能接口 IPv6 IS-IS

默认情况下，IPv6 IS-IS 功能在接口上处于关闭状态。在当前路由器上创建 IS-IS 进程后，需要在接口上使能 IPv6 IS-IS。在接口配置模式下，使用如下命令：

isis ipv6 enable

使用 **no isis ipv6 enable** 命令在接口上关闭 IPv6 IS-IS 功能。

配置接口度量值

度量值用来计算经过此链路到达网络目的地址的链路开销。在 IPv6 IS-IS 路由中，为接口配置所在链路的度量值，在接口配置模式下，使用如下命令：

isis ipv6 metric *value* [**level-1** | **level-2**]

- *value* – 指定接口所在链路的度量值。取值范围为 1 到 16777214。默认值为 10.
- **level-1** | **level-2** – 使用 level-1 参数指定 Level-1 路由信息的度量值。使用 level-2 参数指定 Level-2 路由信息的度量值。不指定 level-1 和 level-2 参数时，设定的度量值将会同时对 Level-1 和 Level-2 路由信息生效。

使用 **no isis ipv6 metric** 命令恢复接口度量值的默认值。

进入 IPv6 单播路由配置模式

对 IPv6 IS-IS 单播路由进行相关配置，需进入 IS-IS 的 IPv6 单播路由配置模式。依次使用如下命令进入此模式：

ip vrouter *vrouter-name* – 在全局配置模式下使用此命令，进入 VRouter 配置模式。

router isis – 进入 IS-IS 路由配置模式，同时在此VRouter 创建一个 IS-IS 进程。每个 VRouter 的 IS-IS 进程之间相互独立。

address-family ipv6 unicast - 进入 IPv6 单播路由配置模式。

发布缺省路由

对于引入其他协议的路由信息时所存在的缺省 IPv6 路由，不会被路由器引入并使用。如果需要在路由域中发布缺省 IPv6 路由，在 IS-IS 的 IPv6 单播路由配置模式下使用以下命令：

default-information originate

当配置了此命令的路由器的路由表中存在一条缺省 IPv6 路由，IS-IS 将只通过Level-2 LSP 通告此路由。

使用 **no default-information originate** 命令取消发布缺省 IPv6 路由。

配置管理距离

指定 IS-IS IPv6 路由的管理距离，在 IS-IS 的 IPv6 单播路由配置模式下，使用以下命令：

distance *distance-value*

- *distance-value* – 为 IS-IS IPv6 路由指定管理距离。范围是 1 到 255，默认值是 115。

使用 **no distance** 命令恢复缺省管理距离。

引入路由

IPv6 IS-IS 协议允许用户将设备上其它路由协议（直连、静态、OSPFv3、IPv6 BGP 和 RIPng）的 IPv6 路由信息引入到 IPv6 IS-IS 中，并向外发布。同时，用户可以设置被引入路由的度量。配置引入路由，在 IS-IS 的 IPv6 单播路由配置模式下使用以下命令：

redistribute {**connected** | **static** | **ospf** | **bgp** | **rip**} [**level-1** | **level-1-2** | **level-2**] [**metric** *value*] [**metric-type** {**external** | **internal**}]

- **connected** | **static** | **ospf** | **bgp** | **rip** – 指定引入路由的类型，可以是直连路由（connected）、静态路由（static）、OSPFv3（ospf），IPv6 BGP（bgp）或者 RIP ng(rip)。
- **level-1** | **level-1-2** | **level-2** – 指定引入路由的级别，可以作为 Level-1 路由（level-1）、Level-2 路由（level-2）或者同时作为 Level-1 和 Level-2 路由（level-1-2）。默认值为 level-2。
- **metric** *value* – 指定引入路由的度量。范围是 0 到 4294967295。默认值为 0。
- **metric-type** {**external** | **internal**} – 当指定 metric 类型为 external 时，metric 值为使用命令 **metric** *value* 中配置的值加 64；当指定 metric 类型为 **internal** 时，metric 值为命令 **metric** *value* 中配置的数值。默认类型为 **internal**。

使用 **no redistribute** {**connected** | **static** | **ospf** | **bgp** | **rip**} [**level-1** | **level-1-2** | **level-2**]命令取消指定类型路由的引入。

配置过载标志位

当路由器因资源不足而导致 LSDB 不完整或不准确时，可在通告的 LSPs 中设置过载标志位，抑制引入路由的发布，使得从其他协议引入的路由不会被通告，从而减少经由自己转发的报文。但到此路由器直连地址的报文或经过此路由器到达区域内其他路由器的报文仍然可以被转发给此路由器。为路由器手工配制过载标志位，抑制引入路由的发布，在 IS-IS IPv6 单播路由配置模式下，使用如下命令：

set-overload-bit suppress external

使用 **no set-overload-bit** 命令取消配置过载标志位。

配置 SPF 计算时间间隔

当 LSDB 发生变化时需要进行路由计算。计算 SPF 的时间间隔可以由用户根据需要进行配置。为 IPv6 IS-IS 配置 SPF 计算时间间隔，在 IS-IS IPv6 单播路由配置模式下，使用如下命令：

spf-interval *value* [**level-1** | **level-2**]

- *value* – 指定计算 SPF 的时间间隔。取值范围为 1 到 120。默认值为 10。单位为秒。
- **level-1** | **level-2** – 选择 **level-1** 仅为 Level-1 SPF 指定计算时间间隔；选择 **level-2** 仅为 level-2 SPF 指定计算时间间隔。不指定参数时，配置的计算时间间隔适用于 Level-1 SPF 和 Level-2 SPF 的计算。

使用 **no spf-interval** 命令恢复默认值。

配置多拓扑路由

在使用 IPv6 IS-IS 时，设备支持单拓扑路由和多拓扑路由。使用单拓扑路由时，设备为 IPv4 和 IPv6 的混合拓扑计算路由。

使用多拓扑路由（Multi-Topology Routing），设备将为 IPv4 拓扑和 IPv6 拓扑单独进行SPF 计算，分别生成独立的路由。

系统默认使用单拓扑路由。在开启多拓扑路由前，需要在 IS-IS 路由配置模式下，使用 **metric-style wide** 命令，修改度量类型为 wide 类型。开启多拓扑路由，在 IS-IS IPv6 单播路由配置模式下，使用如下命令：

multi-topology

关闭多拓扑路由功能，使用 **no multi-topology** 命令。

查看 IS-IS IPv6 路由信息

显示 IS-IS IPv6 路由信息，在任何模式下使用以下命令：

show isis ipv6 route

显示 IS-IS 进程信息及相关配置，在任何模式下使用以下命令：

show isis [**vrouter** *vrouter-name*]

- *vrouter-name* - 显示指定的VRouter 的 IS-IS 进程信息及相关配置。

显示 IS-IS 链路状态数据库，任何模式下使用以下命令：

show isis database [**detail**] [**vrouter** *vrouter-name*]

- **detail** – 显示链路状态数据库的详细信息。

- *vrouter-name* - 显示指定的VRouter 的链路状态数据库信息。

显示 IS-IS 接口信息，在任何模式下使用以下命令：

show isis interface [*interface-name*]

IPv6 DHCP 配置

系统支持通过 IPv6 DHCP 实现动态分配 IPv6 地址，确保不会出现地址冲突，且可以重新分配闲置的 IPv6 地址资源。

设备支持 IPv6 DHCP 客户端功能、DHCP 服务器功能和 DHCP 中继代理功能。

- DHCP 客户端： 设备的接口可以设置成 DHCP 客户端，从 DHCP 服务器动态获得 IPv6 地址。
- DHCP 服务器： 设备的接口可以设置成 DHCP 服务器，通过配置的地址池，向与该接口相连的主机分配 IPv6 地址。
- DHCP 中继代理： 设备的接口可以设置成 DHCP 中继代理，中继代理从 DHCP 服务器获得 DHCP 信息，然后将获得信息传递到与接口相连的主机。

虽然设备同时具有以上三种DHCP 功能，但是在为设备配置 DHCP 功能时， 设备的一个接口只能配置一种功能。

配置 DHCP 客户端功能

用户可以将设备的接口配置成 DHCP 客户端，从DHCP 服务器获得 IPv6 地址。接口的 DHCP 客户端配置需要在接口配置模式下进行。DHCP 客户端配置包括：

- 配置 DHCP 方式获取 IPv6 地址
- 释放和重新获取 IP 地址

配置 DHCP 方式获取 IPv6 地址

使接口通过 DHCP 方式获取客户端的 IPv6 地址，在接口配置模式下使用以下命令：

ipv6 address dhcp [**rapid-commit**]

- **ipv6 address dhcp** – 开启接口的 DHCP 获取 IPv6 地址方式。
- **rapid-commit** – 若选择该参数，可与服务器进行快速交互以获取 IPv6 地址。仅当客户端的 rapid-commit 与服务器的 rapid-commit 功能都启用时，该功能生效。

使用 **no ipv6 address dhcp** 取消接口的 DHCP 获取 IPv6 地址方式。

释放和重新获取 IPv6 地址

通过 DHCP 动态获取 IPv6 地址的接口可以释放已经获得的 IPv6 地址，然后重新获取 IPv6 地址。释放和重新获取 IPv6 地址，在接口配置模式下使用以下命令：

- 释放：**dhcpv6-client ip release**
- 重新获取：**dhcpv6-client ip renew**

设备提供命令查看接口获取的 DHCP IPv6 地址信息。在接口配置模式下，使用以下命令：

show dhcpv6-client interface *interface-name*

配置 DHCP 服务器功能

设备可以作为 DHCP 服务器为子网中 DHCP 客户端设备分配 IPv6 地址。DHCP 服务器功能需要在 DHCP 服务器配置模式下进行。

进入 DHCP 服务器配置模式，在全局配置模式下使用以下命令：

dhcpv6-server pool *pool-name*

- *pool-name* – 指定 DHCP 地址池名称。

执行该命令后，系统新建一个 DHCP 地址池，并且进入该地址池的 DHCP 服务器配置模式；如果指定的地址池名称已存在，则直接进入相应的 DHCP 服务器配置模式。

使用 **no dhcpv6-server pool** *pool-name* 命令删除指定的DHCP 地址池。

DHCP 服务器功能配置包括：

- 配置 DHCP 服务器地址池
- 绑定地址池到接口

配置 DHCP 服务器地址池

DHCP 服务器地址池的基本配置有：地址范围、地址池域名、地址池DNS 服务器名称。

配置地址范围

用户需要指定地址池的地址范围用来对外分配。指定地址池的 IPv6 地址范围，在 DHCP 服务器配置模式下，使用以下命令：

address prefix *ipv6-address/prefix-length* [**lifetime** {*valid-lifetime* | **infinite**} | {*preferred-lifetime* | **infinite**}]

- *ipv6-address/prefix-length* – 指定地址池的 IPv6 地址的通用前缀和前缀长度。

- *valid-lifetime* – 指定 IPv6 地址的有效生存时间，即地址在该时间之前生效；单位为秒。
- **infinite** – 若指定该参数，表示地址永久有效。
- *preferred-lifetime* – 指定 IPv6 地址的优选生存时间（preferred lifetime），单位为秒。优选生存时间必须小于或者等于有效生存时间。

在 DHCP 服务器配置模式下，使用 **no address prefix** 命令取消指定的 IP 地址范围。

配置地址池域名

为 DHCP 客户端配置域名，在 DHCP 服务器配置模式下，使用以下命令：

domain *domain-name*

- *domain-name* – 指定服务器给客户端分配的域名。

在 DHCP 服务器配置模式下，使用 **no domain** 命令删除指定的域名。

配置地址池 DNS 服务器

为 DHCP 客户端配置 DNS 服务器，在 DHCP 服务器配置模式下，使用以下命令：

dns-server ipv6-address [*ipv6-address1*] [*ipv6-address2*]

- *ipv6-address1* – 指定主DNS 服务器的 IPv6 地址。
- *ipv6-address2* – 指定备用DNS 服务器的 IPv6 地址。

在 DHCP 服务器配置模式下，使用 **no dns-server** 命令删除指定的DNS 服务器。

绑定地址池到接口

DHCP 服务器地址池配置完毕，用户需要将配置的 DHCP 地址池绑定到接口，才能在接口开启 DHCP 服务器功能。使接口通过DHCP 方式获取服务器的IPv6 地址，在接口配置模式下使用以下命令：

dhcpv6-server enable pool *pool-name* [**rapid-commit**] [**preference** *preference*]

- *pool-name* – 指定从 DHCP 服务器获取的IPv6 地址池的名称。
- **rapid-commit** – 若选择该参数，可与服务器进行快速交互以获取 IPv6 地址。仅当客户端的 rapid-commit 与服务器的 rapid-commit 功能都启用时，该功能生效。
- **preference** *preference* – 指定绑定到接口上的 DHCP 服务器的优先级。取值范围为 0 至 255。数值越大，表示优先级越高。

在接口配置模式下，使用 **no dhcpv6-server enable** 取消通过 DHCP 获取服务器的 IPv6 地址。

配置 DHCP 中继代理功能

设备可以作为 DHCP 中继代理，接受 DHCP 客户端请求，并且将请求发送到 DHCP 服务器，然后将从 DHCP 服务器获得DHCP 信息再返回给 DHCP 客户端。DHCP 中继代理功能需要在接口配置模式下完成，包括：

- 指定 DHCP 服务器的 IP 地址
- 开启接口的DHCP 中继代理功能

开启接口的 DHCP 中继代理功能

开启接口的 DHCP 中继代理功能，在接口配置模式下，使用以下命令：

dhcpv6-relay enable

在接口配置模式下，使用 **no dhcpv6-relay enable** 命令关闭接口的 DHCP 中继代理功能。

指定中继服务器的 IPv6 地址

指定中继服务器的转发地址，在接口配置模式下，使用以下命令：

dhcpv6-relay server *ipv6-address* [**interface** *interface-name*]

- *ip-address* – 指定 DHCP 服务器的 IPv6 地址。
- **interface** *interface-name* – 若配置的 DHCP 服务器为本地链路地址，指定对应的出接口名称。

在接口配置模式下，使用 **no dhcpv6-relay server** *ipv6-address* [**interface** *interface-name*]命令删除中继服务器的转发地址。

查看设备的 DHCP IPv6 信息

在任何模式下，使用以下命令查看相关信息：

- **show dhcpv6 duid**：查看设备的 IPv6 UID 信息。
- **show dhcpv6 interface**：查看设备所有开启 DHCP IPv6 模式的接口信息。
- **show dhcpv6-client interface** *interface-name*：查看设备开启 DHCP 客户端 IPv6 模式的接口信息。
- **show dhcpv6-server binding** *pool-name*：查看 DHCP 服务器的 IP 地址和客户端的绑定关系。
- **show dhcpv6-server pool** *pool-name*：查看 DHCP 服务器的地址池信息。

IPv6 DNS 配置

StoneOS 支持通过IPv6 DNS 实现域名与 IPv6 地址的转换。IPv6 引入了新的 DNS 记录类型用于 IPv6 地址解析，能够将域名转换为 IPv6 地址。

IPv6 DNS 代理规则配置

设备的 IPv6 DNS 代理规则配置包括：

- 创建DNS 代理规则
- 配置DNS 代理匹配条件
- 指定DNS 代理规则行为
- 配置DNS 代理服务器
- 配置描述信息
- 启用/禁用 DNS 代理规则

{b}提示: {/b}该章节仅介绍 DNS 代理匹配条件IPv6 相关配置（IPv6 DNS 源地址、IPv6 DNS 目的地址）和 IPv6 DNS 代理服务器配置，其他配置与 IPv4 DNS 代理配置相同，请参考《防火墙》的“配置DNS 代理功能”部分。

指定 IPv6 DNS 源地址

用户可指定 DNS 请求的 IPv6 源地址，对 DNS 请求报文进行过滤。用户可指定多条源地址类目。指定后，系统将按照规则设定的行为，对匹配成功的流量进行处理。在 DNS 代理规则配置模式下，使用以下命令：

- 添加地址簿条目类型 IPv6 源地址：**src-addr** { *ipv6-addr-name* | *ipv6-any*}
- 删除地址簿条目类型 IPv6 源地址：**no src-addr** { *ipv6-addr-name* | *ipv6-any*}
- 添加 IP 成员类型 IPv6 源地址：**src-ip** *ipv6-address/netmask*
- 删除 IP 成员类型 IPv6 源地址：**no src-ip** *ipv6-address/netmask*
- 添加 IP 地址范围类型IPv6 源地址：**src-range** *min-ipv6-address max-ipv6-address*
- 删除 IP 地址范围类型IPv6 源地址：**no src-range** *min-ipv6-address max-ipv6-address*

指定 IPv6 DNS 目的地址

用户可指定 DNS 请求的 IPv6 目的地址，对DNS 请求报文进行过滤。用户可指定多条目的地址类目。指定后，系统将按照规则设定的行为，对匹配成功的流量进行处理。在DNS 代理规则配置模式下，使用以下命令：

- 添加地址簿条目类型 IPv6 目的地址：**dst-addr** { *ipv6-addr-name* | **ipv6-any** }
- 删除地址簿条目类型 IPv6 目的地址：**no dst-addr** { *ipv6-addr-name* | *ipv6-any* }
- 添加 IP 成员类型 IPv6 目的地址：**dst-ip** *ipv6-address/netmask*
- 删除 IP 成员类型 IPv6 目的地址：**no dst-ip** *ipv6-address/netmask*
- 添加 IP 地址范围类型IPv6 目的地址：**dst-range** *min-ipv6-address max-ipv6-address*
- 删除 IP 地址范围类型IPv6 目的地址：**no dst-range** *min-ipv6-address max-ipv6-address*

配置 IPv6 DNS 代理服务器

当用户将 IPv6 DNS 代理规则的行为指定为代理时，需继续指定 IPv6 DNS 代理服务器。每条 IPv6 DNS 规则最多可指定 6 个 IPv6 DNS 代理服务器。用户可按需为 IPv6 DNS 服务器指定出接口和首选属性。当用户配置多个 IPv6 DNS 服务器时，将首先选择首选 IPv6 DNS 服务器进行域名解析。若没有指定首选服务器，系统将查询是否有指定出接口的 IPv6 DNS 服务器；若有，则轮询选择出接口 IPv6 DNS 服务器；若无出接口 IPv6 DNS 服务器，即只有普通的 IPv6 DNS 服务器，则轮询选择此类普通的 IPv6 DNS 服务器。

在 DNS 代理规则配置模式下，用户可以通过使用以下命令添加一条条目到 IPv6 DNS 代理服务选择列表中：

name-server *server-ipv6-address* [**vrouter** *vrouter-name*] [**egress-interface** *interface-name*|[**preferred**]

- *server-ipv6-address* – 指定 DNS 代理服务器的 IPv6 地址。
- *vrouter-name* – 指定 DNS 代理服务器所属的虚拟路由器。
- *interface-name* – 指定发送 DNS 代理请求的出接口。
- **preferred** – 指定 DNS 代理服务器为首选服务器，一条DNS 代理规则仅可指定一台服务器为首选服务器。

使用 **no name-server** *server-ipv6-address* [**vrouter** *vrouter-name*]删除 DNS 代理服务器。

配置 IPv6 DNS 域名服务器

该命令指定的 IPv6 DNS 域名服务器为设备进行 DNS 解析时使用的服务器。配置 IPv6 DNS 域名服务器，在全局配置模式下使用以下命令：

ipv6 name-server *ipv6-address1* [*ipv6-address2*] ... [*ipv6-address6*] [**vrouter** *vr-name*]

- *ipv6-address1* – 指定域名服务器的 IPv6 地址。用户最多可配置 6 个域名服务器。用户可以使用一条命令配置 6 个域名服务器，也可分多条命令配置，即运行命令 **ipv6 name-server 2002:ae3:1111:2222::1 2001:0db8::3** 与运行命令 **ipv6 name-server 2002:ae3:1111:2222::1** 和 **ipv6 name-server 2001:0db8::3** 等效。
- **vrouter** *vr-name* – 指定 IPv6 DNS 域名服务器的VRouter。

使用 **no ipv6 name-server** *ipv6-address1* [*ipv6-address2*] ... [*ipv6-address6*] [**vrouter** *vr-name*]命令取消对 IPv6 DNS 域名服务器的配置。

配置 IPv6 DNS 代理服务选择列表

IPv6 DNS 代理服务选择列表包含域名和对应 IPv6 DNS 服务器的选择条目，选择列表中最多可以包含 6 条选择条目。在全局配置模式下，用户可以通过使用以下命令添加一条条目到 IPv6 DNS 代理服务选择列表中：

ipv6 dns-proxy domain {*domain-suffix* | **any**} **name-server** {**use-system** | *ipv6-address1* [*ipv6-address2*] ... [*ipv6-address6*]} [**vrouter** *vr-name*]

- *domain-suffix* | **any** – 指定域名后缀，用来匹配 IPv6 DNS 请求中的域名。any 为任意后缀。
- **name-server** {**use-system** | *server-ip1* [*server-ip2*] ... [*server-ip6*]} – 指定 DNS 服务器的 IPv6 地址，可以是设备系统的 IPv6 DNS 域名服务器（**use-system**），也可以是指定的 IPv6 地址（*ipv6-address1* [*ipv6-address2*] ... [*ipv6-address6*]）。最多可以指定 6 个 IPv6 DNS 服务器 IP 地址。
- **vrouter** *vr-name* – 指定 IPv6 DNS 服务器的VRouter。

使用 **no ipv6 dns-proxy domain** {*domain-suffix* | **any**} [**vrouter** *vr-name*]删除选择条目。

例如，添加一条后缀为“com”且 IPv6 DNS 服务器的 IP 地址是 2010::1 的选择条目，命令行如下：

```
hostname(config)# ipv6 dns-proxy domain com name-server 2010::1
```

开启/关闭接口的 IPv6 DNS 代理功能

默认情况下，接口的 IPv6 域名代理功能是关闭的。开启接口的 IPv6 域名代理功能，在接口配置模式下使用以下命令：

dns-proxy

使用 **no dns-proxy** 关闭接口的 IPv6 域名代理功能。

添加静态 IPv6 DNS 映射条目

手动添加 IPv6 DNS 映射条目到缓存，在全局配置模式下使用以下命令：

ipv6 host *host-name* {*ipv6-address1* [*ipv6-address2*] ... [*ipv6-address8*]} [**vrouter** *vr-name*]

- *host-name* – 指定主机名称。名称范围是 1 到 255 个字符。
- {*ipv6-address1* [*ipv6-address2*] ... [*ipv6-address8*]} – 指定主机的 IPv6 地址。最多可设置 8 个 IPv6 地址。
- **vrouter** *vr-name* – 指定主机的VRouter。

使用 **no ipv6 host** *host-name* [**vrouter** *vr-name*]删除指定的静态 IPv6 DNS 映射条目。

清除动态 IPv6 DNS 映射条目

手动清除动态 IPv6 DNS 映射条目，在执行模式下使用以下命令：

clear ipv6 host [*host-name* [**vrouter** *vr-name*]]

- *host-name* – 清除指定主机的 IPv6 DNS 映射条目。
- **vrouter** *vr-name* – 指定主机的VRouter。

该命令用来清除指定的或者所有动态 IPv6 DNS 映射条目。手工配置的静态 IPv6 DNS 映射项，在全局配置模式下使用 **no ipv6 host** *host-name* [**vrouter** *vr-name*]删除。

查看 IPv6 DNS 映射条目

使用 show 命令可以查看系统中所有的 IPv6 DNS 映射条目。查看 IPv6 DNS 映射条目，在任何模式下使用以下命令：

show ipv6 host [*host-name*] [**vrouter** *vr-name*]

- *host-name* – 显示指定主机的 IPv6 DNS 映射条目。
- **vrouter** *vr-name* – 指定主机的VRouter。

查看 IPv6 DNS 配置信息

查看 IPv6 DNS 配置信息，在任何模式下使用以下命令：

show ipv6 dns

PMTU 配置

当一个 IPv6 节点有大量的数据要发送给另一节点时，数据是作为一系列的 IPv6 数据报文进行传输的。这些被传输的报文最好具有在从源节点到目的节点的路径上不需要分片的最大尺寸。这一尺寸称作为路径 MTU，即 PMTU，它等于路径上每一跳的 MTU 之中的最小值。IPv6 定义了一个标准机制来用于发现任意路径上的PMTU 值。StoneOS 支持该PMTU 发现机制。

默认情况下，StoneOS 的PMTU 发现机制为开启状态。更改系统的PMTU 发现机制状态，在Flow 配置模式下使用以下命令：

- 启用：**ipv6 pmtu enable**
- 禁用：**no ipv6 pmtu enable**

说明：进入 Flow 配置模式，在全局配置模式下使用 flow 命令。

开启PMTU 功能后，系统会在收到 ICMPv6“Packet Too Big”错误信息后生成PMTU 条目，记录目的地 址、接口信息、PMTU 值以及老化时间。PMTU 条目生成后，在条目的老化时间内，如果有到达条目指定的目的地址的会话生成，该条目的老化时间将会被刷新，即重新开始计数。如果在老化时间内没有会话匹配该条目，该条目将老化并且从系统中删除。用户可根据实际情况指定 PMTU 条目的老化时间。

指定PMTU 老化时间，在Flow 配置模式下使用以下命令：

ipv6 pmtu ageout-time *time*

- *time* – 指定老化时间，单位为秒，默认值是 300 秒。取值范围是 10 到 600。

在 Flow 配置模式下使用该命令 no 的形式回复默认老化时间：

no ipv6 pmtu ageout-time

除条目自身老化以外，用户还可以根据需要立即清除 PMTU 条目。清除PMTU 条目，在任何模式下使用以下命令（如果不指定参数，则清除系统中当前存在的所有PMTU 条目）：

clear ipv6 pmtu [**dst-ip** *ipv6-address* **interface** *interface-name*]

- *ipv6-address* – 指定需要清除的条目的 IPv6 地址。
- *interface-name* – 指定需要清除的条目的接口。

显示PMTU 条目信息，在任何模式下使用以下命令（如果不指定参数，则显示系统中当前存在的所有PMTU 条目）：

show ipv6 pmtu [**dst-ip** *ipv6-address* **interface** *interface-name*]

- *ipv6-address* – 指定需要显示的条目的 IPv6 地址。

- *interface-name* – 指定需要显示的条目的接口。

显示系统当前PMTU 功能状态信息，例如开启状态、老化时间等，在任何模式下使用以下命令：

show ipv6 pmtu status

自定义应用配置

除了使用 StoneOS 提供的预定义应用以外，用户还可以根据需要创建自定义应用，并可以通过配置自定义应用特征规则，对进入设备的流量进行识别控制，从而识别出应用类型。如设备开启 IPv6，系统支持对 IPv6 地址的流量进行识别。

设备的自定义应用 IPv6 相关配置包括：

- 配置 IPv6 源地址
- 配置 IPv6 目的地址
- 配置 ICMPv6 类型应用特征条目

{b}提示: {/b}自定义应用的具体配置信息请参考《防火墙》的“服务和应用”部分。

创建和删除自定义应用

创建一个自定义应用并将其添加到应用簿，请在全局配置模式下使用以下命令：

application *application-name*

- *application-name* – 指定自定义应用的名称。长度范围是 1 至 31 个字符。该名称在整个系统中必须是唯一的。

运行该命令后，系统进入应用配置模式。

使用该命令 no 的形式删除一个自定义应用：

no application *application-name*

进入自定义应用特征配置模式

进入自定义应用特征配置模式，在全局配置模式下使用以下命令：

app-signature

进入应用特征规则配置模式

在应用特征规则配置模式下，可以分别配置自定义应用的任意一个特征。

创建一个自定义应用特征规则并进入应用特征规则配置模式，如果指定的应用特征规则 ID 已存在，则直接进入应用特征规则配置模式。请在自定义应用特征配置模式下使用以下命令，并且用该命令 no 的形式删除一个自定义应用特征规则：

signature [**id** *id*]

- *id* – 指定自定义应用特征规则 ID。如果不指定 ID 值，系统自动创建一个自定义应用特征规则并分配 ID。

no signature id *id*

指定 IPv6 源地址

指定自定义应用特征的 IP 成员类型源地址，在应用特征配置模式下使用以下命令：

src-ipv6 *ipv6-address*

- *ipv6-address* – 指定自定义应用特征的 IPv6 源地址。

指定 IPv6 目的地址

指定自定义应用特征的 IP 成员类型目的地址，在应用特征配置模式下使用以下命令：

dst-ipv6 *ipv6-address*

- *ipv6-address* – 指定自定义应用特征的 IPv6 目的地址。

指定 ICMPv6 类型应用特征条目

在应用特征配置模式下，使用以下命令添加 ICMPv6 类型特征条目：

protocol icmpv6 type *type-value* [**code** *min-code* [*max-code*]]

- *type-value* – 指定自定义应用特征的 ICMPv6 type 值。取值范围请参考附表：ICMPv6 Type 以及 Code 值对照表。默认值为 Any，表示所有 ICMPv6 type 值。
- **code** *min-code* [*max-code*] – 指定自定义应用特征的 ICMPv6 的最小 code 值（min-code）和最大 code 值（max-code）。范围是 0 到 255。如果不指定 code 值，系统默认将使用指定 Type 值对应的 code 值（已在 RFC 中定义的）；如果不指定最大code 值，系统默认将使用与最小 code 值相同的最大code 值。

在应用特征配置模式下，使用以上命令 no 的形式删除指定的 ICMPv6 应用特征条目：

no protocol

IPv6 策略配置

策略是网络安全设备的基本功能，通过策略规则控制网络流量的传输。StoneOS 在支持 IPv4 流量策略规则控制的同时，还支持 IPv6 流量策略规则控制。组成策略规则的基本元素包括地址（源、目的地址）、服务、以及动作，以下分别介绍这些基本元素的 IPv6 配置。

IPv6 地址簿配置

系统的地址簿中同时支持 IPv4 和 IPv6 的地址条目。IPv4 地址条目中只能包含 IPv4 地址成员、IPv4 地址段成员、地址为 IPv4 类型的主机成员以及其他 IPv4 地址条目；IPv6 地址条目只能包含IPv6 地址成员、IPv6 地址段成员以及其他 IPv6 地址条目。地址簿中默认包含一条表示所有IPv6 地址的地址条目，即“ipv6-any”；地址条目“Any”表示所有 IPv4 地址。

{b}提示: {/b}配置 IPv4 地址条目，请参阅《防火墙》的“配置 IPv4 地址条目”。

在全局配置模式下，使用以下命令新建地址条目并进入地址条目配置模式；如果指定名称的地址条目已存在，则直接进入地址条目配置模式：

address *address-entry* **ipv6**

为地址条目添加或者删除 IPv6 地址成员，在地址条目配置模式下使用以下命令：

ip *ipv6-address/M*

no ip *ipv6-address/M*

为地址条目添加或者删除 IPv6 地址范围成员，在地址条目配置模式下使用以下命令：

range *min-ipv6-address max-ipv6-address*

no range *min-ipv6-address max-ipv6-address*

创建 IPv6 地址条目，需要注意以下几点：

- IPv6 和 IPv4 的地址条目不能混合嵌套；
- 配置 IPv6 地址范围成员时，范围的前 64 位必须相同，例如 2005::1 到 2006::1 是系统不支持的配置范围，而 2005::1 到 2005::1000 则是允许的范围；
- 当前版本暂时不支持 IPv6 地址的主机成员。

IPv6 服务簿配置

为支持 IPv6 服务，系统服务簿添加新预定义服务支持 IPv6 服务，同时支持部分网络应用的 IPv6 端口。使用 show service predefined 以及 show predefined-servgroup 命令可以查看系统支持的所有预定义服务以及预定义服务组。一个服务组中可同时包含 IPv4 和 IPv6 服务。用户也可以根据需要创建 IPv6 自定义服务（ICMPv6）。

{b}提示: {/b}关于 IPv4 服务簿配置，请参考《防火墙》的“服务”。

关于创建 ICMPv6 类型自定义服务条目，请参考以下命令：

在全局配置模式下，使用以下命令创建自定义服务并进入自定义服务配置模式；如果指定名称的自定义服务已存在，则直接进入自定义服务配置模式：

service *service-name*

在自定义服务配置模式下，使用以下命令添加 ICMPv6 类型服务条目：

icmpv6 type *type-value* [**code** *min-code* [*max-code*]]

- *type-value* – 指定自定义服务的 ICMPv6 type 值。取值范围请参考附表：ICMPv6 Type 以及 Code 值对照表。默认值为Any，表示所有 ICMPv6 type 值。
- **code** *min-code* [*max-code*] – 指定自定义服务的 ICMPv6 的最小code 值（min-code）和最大 code 值（max-code）。范围是 0 到 6 和Any（任何 ICMPv6 code 值）。如果不指定code 值，系统默认将使用指定 Type 值对应的code 值（已在 RFC 中定义的）；如果不指定最大 code 值，系统默认将使用与最小 code 值相同的最大code 值。

在服务配置模式下，使用以上命令 no 的形式删除指定的ICMPv6 服务条目：

no icmpv6 type *type-value* [**code** *min-code* [*max-code*]][**timeout** *timeout-value*]

IPv6 策略规则行为配置

IPv4 策略规则支持以下 5 种行为：拒绝（deny）、允许（permit）、来自隧道（fromtunnel）、隧道（tunnel）以及 Web 认证（webauth）。IPv6 策略规则在当前版本中仅支持基本的拒绝（deny）和允许（permit）两种行为。

IPv6 策略规则配置

配置策略规则时，规则中指定的源地址和目的地址必须为同种类型地址，即如果源地址为 IPv6 地址，则目的地址也必须为 IPv6 地址。

配置 IPv6 策略规则，在策略配置模式下（全局配置模式下使用 policy-global 命令进入策略配置模式），使用以下命令：

rule [id *id*] [top | before *id* | after *id*] from {*src-addr* / *ipv6-address*} to {*dst-addr* / *ipv6-address*} service *service-name* [application *app-name*] {permit | deny}

- id *id* – 指定策略规则的 ID。如果不指定，系统将会为策略规则自动分配一个 ID。规则 ID 在整个系统中必须是唯一的。
- top | before *id* | after *id* – 指定策略规则的位置，可以是所有规则的首位（top）、某个规则之前（before *id*）或者某个 ID（after *id*）之后。默认情况下，系统会将新创建的策略规则放到所有规则的末尾。
- from *src-addr* – 指定 IPv6 策略规则的源地址，可以是 IPv6 地址、系统中已定义的地址簿中的 IPv6 地址条目，也可以是“ipv6-any”。
- to *dst-addr* – 指定 IPv6 策略规则的目的地址，可以是 IPv6 地址、系统中已定义的地址簿中的 IPv6 地址条目，也可以是“ipv6-any”。
- service *service-name* – 指定策略规则的服务名称。service-name 为服务簿中定义的服务。
- permit | deny – 指定策略规则的行为。 permit 表示允许流量通过。deny 表示拒绝流量通过。

另外，用户还可以在策略配置模式下使用以下命令，创建一个策略规则 ID，并且进入策略规则配置模式，再进一步配置其它策略规则相关参数：

rule {id *id* | {top | before *id* | after *id*}}

- id *id* – 指定策略规则的 ID。如指定的规则已存在，系统将直接进入策略规则编辑模式。如果不指定，系统将会为策略规则自动分配一个 ID。规则 ID 在整个系统中必须是唯一的。策略规则的 ID 大小并不表示策略规则的匹配先后顺序。
- top | before *id* | after *id* – 指定策略规则的位置，可以是所有规则的首位（top）、某个规则之前（before *id*）或者某个 ID（after *id*）之后。默认情况下，系统会将新创建的策略规则放到所有规则的末尾。

编辑 IPv6 策略规则

创建好的策略规则可以进行编辑来修改不合适的参数值，但是修改工作必须在规则配置模式下才可以进行。在 CLI 中进入规则配置模式，请输入以下命令：

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

进入规则配置模式后，可使用的编辑策略规则的命令如下：

- 添加 IP 成员类型源地址：**src-ip** *ipv6-address/M*
- 删除 IP 成员类型源地址：**no src-ip** *ip-address/M*
- 添加 IP 地址范围类型源地址：**src-range** *min-ipv6-address* [*max-ipv6-address*]
- 删除 IP 地址范围类型源地址：**no src-range** *min-ipv6-address* [*max-ipv6-address*]
- 添加 IP 成员类型目的地址：**dst-ip** *ipv6-address/M*
- 删除 IP 成员类型目的地址：**no dst-ip** *ipv6-address/M*
- 添加 IP 地址范围类型目的地址：**dst-range** *min-ipv6-address* [*max-ipv6-address*]
- 删除 IP 地址范围类型目的地址：**no dst-range** *min-ipv6-address* [*max-ipv6-address*]

IPv6 策略访问控制

IPv6 策略访问控制功能，即通过将策略规则与 ACL Profile 相结合，在策略规则控制的基础上，进一步对 IPv6 报文进行细粒度的访问控制，如 IPv6 扩展报文、源/目的 MAC 地址等。

通常情况下，配置策略访问控制功能，需要以下几个步骤：

1. 创建 ACL Profile。ACL Profile 包含访问控制规则。
2. 配置策略访问控制规则。该规则用来指定需要进行控制的 IPv6 扩展报文、规则类型以及控制动作。
3. 绑定 ACL Profile 到策略规则。

只有将 ACL Profile 绑定到策略规则上，该功能才能在设备上起作用。

创建 ACL Profile

ACL Profile 的配置需要在ACL Profile 配置模式下进行。进入ACL Profile 配置模式，在全局配置模式下，使用以下命令：

acl-profile *acl-profile-name*

- *acl-profile-name* – 指定ACL Profile 的名称。执行该命令后，系统创建指定名称的ACL Profile，并且进入该ACL Profile 配置模式；如果指定的名称已存在，则直接进入ACL Profile 配置模式。最多只能创建 64 个 ACL Profile。

在全局配置模式下，使用 **no acl-profile** *acl-profile-name* 命令删除指定的ACL Profile。

配置策略访问控制规则

配置策略访问控制规则以及控制动作，在 ACL Profile 配置模式下，使用以下命令：

sequence *id* {**drop** | **pass**} [**both** | **forward** | **backward**] [**src-mac** *src-mac-address*] [**dst-mac** *dst-mac-address*][**dscp** *dscp-value*] [**flow-label** *flow-label-value* [*end-flow-label-value*]] [**ext-header** [**ah**][**fragment**][**esp**][**hop**][**none**][**dest** [*dest-value1* [*dest-value2* | **home-address**]]][**mobility** [*mobility-value1 [mobility-value2*] | **bind-refresh** | **bind-ack** | **bink-err** | **bind-update** | **cot** | **coti**| **hot** | **hoti**]][**routing** [*routing-value1* [*routing-value2*]]]

- *id* – 指定策略访问控制规则的 ID。范围是 1-32。
- **drop** | **pass** – 指定采取的控制动作，丢弃或允许通过。
- **both** | **forward** | **backward** – 指定策略规则访问控制的流量方向， forward 指上行方向， backward 指下行方向，both 指双方向。默认为双方向。
- **src-mac** *src-mac-address* – 指定访问控制规则的源MAC 地址。
- **dst-mac** *dst-mac-address* – 指定访问控制规则的目的MAC 地址。
- **dscp** *dscp-value* – 指定 DSCP 的值。范围是 0-63。
- **flow-label** *flow-label-value* [*end-flow-label-value*] – 指定访问控制规则的 IPv6 流标签或流标签范围，取值范围是 0 到 1048575。
- [**ext-header** [**ah**][**fragment**][**esp**][**hop**][**none**][**dest** [*dest-value1* [*dest-value2* | **home-address**]]][**mobility** [*mobility-value1 [mobility-value2*] | **bind-refresh** | **bind-ack** | **bink-err** | **bind-update** | **cot** | **coti**| **hot** | **hoti**]][**routing** [*routing-value1* [*routing-value2*]]] – 指定访问控制规则包含的 IPv6 报文扩展头以及参数取值。
- **ah** - 包含 IPv6 报文身份验证扩展头。
- **fragment** - 包含 IPv6 报文分段扩展头。
- **esp** - 包含 IPv6 报文 ESP 扩展头。
- **hop** - 包含 IPv6 报文逐跳扩展头。
- **none** - 不包含扩展头。
- **dest** [*dest-value1* [*dest-value2* | **home-address**]] - 包含 IPv6 报文目的地选项扩展头。dest-value1 为起始值，dest-value2 为结束值。范围是 0 到 255。home-address 表示目的地选项取值为 201。
- **mobility** [*mobility-value1* [*mobility-value2*] | **bind-refresh** | **bind-ack** | **bink-err** | **bind-update** | **cot** | **coti**| **hot** | **hoti**] - 包含 IPv6 报文移动性扩展头。mobility-value1 为起始值，mobility-value2 为结束值。范围是 0 到 255。
- **routing** [*routing-value1* [*routing-value2*]] - 包含 IPv6 报文路由扩展头。范围是 0 到 255。

在 ACL Profile 配置模式下，使用 **no sequence** *id* 命令删除指定的策略访问控制规则。

配置默认控制动作

当未命中任何访问控制规则时，系统将采取指定的默认访问控制动作。配置默认控制动作，在ACL Profile 配置模式下，使用以下命令：

default-action {**drop** | **pass**}

- **drop** | **pass** – 指定采取的默认控制动作，丢弃或允许通过。

在 ACL Profile 配置模式下，使用 **no default-action** 命令删除指定的默认访问控制动作。

绑定策略规则

ACL Profile 以及访问控制规则配置完成后，只有把它们绑定到策略规则上，访问控制功能才会生效。绑定 ACL Profile 到策略规则，在策略配置模式下，使用以下命令：

acl *acl-profile-name*

- *acl-profile-name* – 指定绑定的ACL Profile 名称。

在策略配置模式下使用 **no acl** 命令取消ACL Profile 在指定策略规则的绑定。

查看 ACL Profile 信息

用户可以在任何模式下随时使用 show 命令查看ACL Profile 的配置信息。

show acl-profile [*acl-profile-name*]

- *acl-profile-name* – 显示指定名称的ACL Profile 的信息。如果不指定该参数，则显示系统中所有 ACL Profile 的信息。

IPv6 ALG 配置

与 IPv4 的 ALG 功能相比，系统当前支持以下应用的 ALG 功能：FTP、TFTP、HTTP、RSH。同时，对于 URL 过滤功能的不受限 IP，用户可以指定 IPv6 地址。在配置ALG 功能相关策略规则时，请确保策略规则中引用的是 IPv6 地址，例如“rule from ipv6-any to ipv6-any service ftp permit”。

NDP 安全防护

NDP 协议是 IPv6 协议中的一个关键协议，但是，由于 NDP 协议并未提供认证机制，导致网络中的节点不可信，也使攻击者有机可乘，可针对 NDP 协议发起一系列攻击。主要攻击类型有以下几类：

- 地址欺骗攻击：攻击者利用 RS（Router Solicitation）/NS（Neighbor Solicitation）/NA（Neighbor Advertisement）/RA（Router Advertisement）/Redirect 报文来修改受害主机的MAC 地址，或者利用 RS/NS/NA/RA 报文来修改网关的 MAC 地址，致使受害主机与网络无法正常通信。
- DAD 攻击：当受害主机进行 DAD 查询时，攻击者通过NS 或 NA 报文进行干扰，致使受害主机的 DAD 过程失败，无法获取到 IP 地址。
- 路由通告欺骗：攻击者通过伪造 RA 报文，造成受害主机网络配置错误，从而引发欺骗攻击。
- 泛洪攻击：攻击者通过发送大量的 NS/RS/NA/RA 报文，造成网关的ND 表项溢出。
- 重定向欺骗攻击：攻击者以网关的链路层地址作为源地址发送重定向报文给受害主机，受害主机接受该错误重定向消息，导致受害主机路由表修改。

针对以上攻击类型，系统提供一系列 NDP 安全防护功能，保证用户 IPv6 网络环境的安全。防护功能包括：

- IP-MAC 绑定
- NDP 学习功能
- NDP 检查
- NDP 欺骗防护（NDP 反向查询、MAC 对应 IP 地址数检查、非请求NA 报文发送速率）
- NDP 防御

根据防护功能的不同，用户可以针对不同的网络情况应用不同的防护功能。例如，实现二层 NDP 防护，用户可启用 NDP 检查功能（限制接收 DNP 报文速率、配置可信接口、禁止接收 RA 报文）；实现三层 NDP 防护，可以启用禁止ND 学习功能或者禁用动态学习表项、启用ND 主动反向查询功能或者执行“一键绑定”功能将动态 IP-MAC 表项转换为静态表项。

以下将具体介绍各种防护功能的配置与使用。

IP-MAC 绑定

为加强网络安全控制， 设备支持 IP-MAC 地址绑定功能。IP-MAC 绑定信息可通过静态绑定和动态获取两种方式获得。通过 NDP 学习功能获得的 IP-MAC 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。为进一步控制网络安全，简化手工静态 IP-MAC 绑定配置，用户可以通过“一键绑定”功能，将动态获得的 IP-MAC 绑定信息转换为静态信息。静态和动态绑定信息都储存在 IPv6 ND 缓存列表中。

添加静态 IP-MAC 绑定表项

添加静态 IP-MAC 绑定表项到缓存列表，在全局配置模式下使用以下命令：

ipv6 neighbor *ipv6-address interface-name mac-address*

- *ipv6-address* – 指定静态绑定条目的 IPv6 地址。
- *interface-name* – 指定静态绑定条目的接口。
- *mac-address* – 指定静态绑定条目的 MAC 地址。

使用该命令 no 的形式删除指定的 IP-MAC 绑定表项：

no ipv6 neighbor {**all** | *ipv6-address interface-name*}

一键绑定

“一键绑定”功能即在内网主机都能上网时，通过执行相关操作将当前通过ND 学习学到的动态 IP-MAC 表项转化为静态表项。配置“一键绑定”功能，在执行模式下使用以下命令：

exec ipv6 nd-dynamic-to-static [**vrouter** *vr-name*]

- *vr-name* – 指定需要执行该功能的VRouter 的名称。默认为系统缺省VR 即 trust-vr。

执行以上命令后，当前系统中所有的动态 IP-MAC 绑定表项全部转换为静态表项。

仅允许 IP-MAC 静态绑定主机上网

默认情况下，系统允许NDP 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：

ipv6 nd-disable-dynamic-entry

使用该命令的 no 形式关闭该功能：

no ipv6 nd-disable-dynamic-entry

查看 IP-MAC 绑定信息

在任何模式下，通过以下命令查看系统中的 IP-MAC 绑定信息（如果不指定任何参数，则显示系统中当前存在的所有静态和动态 IP-MAC 绑定表项）：

show ipv6 neighbor [**generic** | **interface** *interface-name* | **slot** *slot-num* | **static** | **vrouter** *vr-name* | *ipv6-address*]

- **generic** – 显示 IP-MAC 绑定表项的统计信息。
- **interface** *interface-name* – 显示指定接口的 IP-MAC 绑定表项。
- **slot** *slot-num* – 显示指定槽位号的 IP-MAC 绑定表项。部分设备（X6150、X6180、X7180、X10800）支持。
- **vrouter** *vr-name* – 显示指定 VRouter 的 IP-MAC 绑定表项。
- **static** – 显示静态 IP-MAC 绑定表项。

- *ipv6-address* – 显示指定 IPv6 地址的 IP-MAC 绑定表项。

清除动态 IP-MAC 绑定信息

清除 IP-MAC 绑定信息，在任何模型下使用以下命令（如果不指定参数，则清除系统中当前存在的所有动态 IP-MAC 绑定信息）：

clear ipv6 neighbor [*ipv6-address*]

- *ipv6-address* – 清除指定 IP 地址的 IP-MAC 绑定信息。

NDP 学习功能

设备通过 NDP 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ND 表中。默认情况下，设备的 NDP 学习功能是开启的，设备会一直进行 NDP 学习，并将学到的 IP-MAC 绑定信息添加到系统 ND 表中。在 NDP 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 ND 表中。关闭 NDP 学习功能后，只有已经在系统 ND 表中的 IP 地址才可以通过设备转发报文。

配置 NDP 学习功能，在接口配置模式下，使用以下命令：

- 开启 NDP 学习功能：**ipv6 nd-learning**
- 关闭 NDP 学习功能：**no ipv6 nd-learning**

NDP 检查

设备支持接口的 NDP 检查功能。开启该功能后，系统会对通过接口的所有NDP 报文进行检查，将 NDP 报文的 IP 地址与系统ND 缓存列表中的静态表项进行对比：

- 如果 IP 地址在 ND 缓存列表中，并且与表中记录的MAC 地址以及接口相同，则继续转发该 NDP 报文；
- 如果 IP 地址在 ND 缓存列表中，但是与表中记录的 MAC 地址或者接口不一致，系统将丢弃该 DNP 报文；
- 如果 IP 地址不在ND 缓存列表中，则根据配置（**ipv6 nd-inspection** {**drop** | **forward**}）进行丢弃或者转发。

开启/关闭 NDP 检查功能

系统的 BGroup 接口和VSwitch 接口支持 NDP 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 NDP 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：

ipv6 nd-inspection {**drop** | **forward**}

- **drop** – 丢弃 IP 地址不在ND 缓存列表中的 NDP 报文。
- **forward** – 转发 IP 地址不在 ND 缓存列表中的 NDP 报文。

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 NDP 检查功能：

no ipv6 nd-inspection

配置可信接口

用户可以设置设备的接口(BGroup 或者 VSwitch 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 NDP 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：

ipv6 nd-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 ipv6 nd-inspection trust

禁止接收 RA 报文

为避免网络中 RA 报文的任意发送，用户可以禁止某些特定接口（仅适用于物理接口）接收 RA 报文，使 RA 报文只能从允许的接口接收。此方法可以有效防护 RA 攻击，提升局域网的安全性。禁止接口接收RA 报文，在接口配置模式下使用以下命令：

ipv6 nd-inspection deny-ra

在接口配置模式下使用该命令 no 的形式取消 RA 报文的接收限制：

no ipv6 nd-inspection deny-ra

配置 NDP 报文速率限制

配置接收 NDP 报文的速率限制，在接口配置模式下（仅适用于物理接口），使用以下命令：

ipv6 nd-inspection rate-limit *number*

- *number* – 指定接口每秒钟接收 NDP 报文的个数。当每秒钟接收 NDP 报文的个数超过该指定值时，系统将丢弃超出的NDP 报文。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 ipv6 nd-inspection rate-limit

查看 NDP 检查功能配置

查看 NDP 检查功能配置，在任何模式下使用以下命令：

show ipv6 nd-inspection configuration

配置 NDP 欺骗防护功能

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

ad ipv6 nd-spoofing {**reverse-query** | **ip-number-per-mac** *number* [**action** [**drop** | **alarm**]] | **unsolicited-na-send-rate** *number*}

- **reverse-query** – 开启 NDP 反向查询功能。当设备收到 NDP 请求后，会纪录 IP 地址并且发送 NDP 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 NDP 请求包的 MAC 地址是否相同。使用 **no ad ipv6 nd-spoofing reverse-query** 命令关闭 NDP 反向查询功能。
- **ip-number-per-mac** *number* – 指定是否检查 ND 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NDP 报文（**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 ipv6 nd-spoofing ip-number-per-mac** 命令恢复参数默认值。
- **unsolicited-na-send-rate** *number* – 指定设备是否发出非请求 NA 报文。如果该参数值是 0，则不发非请求 NA 报文（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 ipv6 nd-spoofing unsolicited-na-send-rate** 命令恢复参数的默认值。

查看 NDP 欺骗防护功能统计信息

配置 NDP 欺骗攻击防护功能后，用户可以通过以下命令查看该功能执行的后的统计信息：

show ipv6 nd-spoofing-statistics

NDP 防御

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

show ipv6 nd-spoofing-statistics [*number*]

- *number* – 显示统计数最高的前 number 条记录。

清除系统中的 NDP 欺骗攻击统计信息，在执行模式下，使用以下命令：

clear ipv6 nd-spoofing-statistics

攻击防护

系统支持下表所列的 IPv6 攻击防护功能，各功能的具体描述和配置，请参考《威胁防护》中的“攻击防护”部分。

攻击防护功能	配置（安全域配置模式）
Huge ICMP 包攻击防护	ad huge-icmp-pak [threshold *number* | action {alarm | drop}]
IP 地址扫描攻击防护	ad ip-sweep [threshold *value*| action {alarm | drop}]
L3 IP 地址欺骗攻击防护	ad ip-spoofing
ICMP Flood 攻击防护	ad icmp-flood [threshold *number* | action {alarm | drop}]
UDP Flood 攻击防护	ad udp-flood [threshold *number* | action {alarm | drop}]
SYN Flood 攻击防护	ad syn-flood [source-threshold *number* | destination-threshold *number* | action {alarm | drop} | destination [ip-based | port-based [address-book *address-book-name* | *ip-address/netmask*]]]
SYN-Proxy SYN-Cookie	ad syn-proxy [min-proxy-rate *number* | max-proxy-rate *number* | proxy-timeout *number* | cookie]
Teardrop 攻击防护	ad tear-drop
IP 碎片攻击防护	ad ip-fragment [action {alarm | drop}]
Ping of Death 攻击防护	ad ping-of-death
端口扫描攻击防护	ad port-scan [threshold *value* | action {alarm | drop}]
TCP 异常攻击防护	ad tcp-anomaly [action {alarm | drop}]
Land 攻击防护	ad land-attack [action {alarm | drop}]

IPv6 6to4 隧道配置

当前网络中，IPv4 网络仍是主流网络，IPv6 网络往往作为网络孤岛存在。而隧道技术则实现了 IPv6 孤岛之间通过 IPv4 网络的通信。系统支持对 IPv6 数据包的处理，并通过隧道技术实现 IPv4 与 IPv6 的互通。当前版本支持 6to4 手工隧道和 6to4 自动隧道。

- 6to4 手工隧道：提供点到点的连接，其通道的终止点是手工静态配置的。

- 6to4 自动隧道：点到多点的自动隧道，主要用于将多个 IPv6 孤岛通过 IPv4 网络连接到 IPv6 网络。根据不同网络环境，设备既可做 6to4 路由器，也可做 6to4 中继路由器。

6to4 隧道配置如下：

- 创建隧道
- 指定隧道的出接口
- 指定手工隧道的目的地址
- 绑定隧道到隧道接口

创建隧道

创建 IPv6 6to4 隧道，在全局配置模式下使用以下命令。执行以下命令后，系统创建指定名称的 IPv6 6to4 隧道，并进入隧道配置模式；如果指定的名称已存在，则直接进入隧道配置模式。

tunnel ip6in4 *tunnel-name* {**manual** | **6to4**}

- *tunnel-name* – 指定 IPv6 6to4 隧道的名称。
- **manual** | **6to4** – 指定隧道类型，可以是 6to4 手工隧道（**manual**）或者 6to4 自动隧道（**6to4**）。

在全局配置模式下，使用以上命令 no 的形式删除指定的IPv6 6to4 隧道：

no tunnel ip6in4 *tunnel-name* {**manual** | **6to4**}

指定 6to4 子隧道最大数

系统内最多可创建 10 个 6to4 隧道，且每个接口最多可配置一个 6to4 隧道。每个隧道下最多可配置 1200 个子隧道。指定 6to4 子隧道数，在隧道配置模式下，使用以下命令：

subtunnel-limit *maximum*

- *maximum* – 指定 6to4 子隧道数，取值范围为 1 至 1200，默认值为 200。

在隧道配置模式下，使用该命令 no 的形式恢复子隧道数的默认值。

no subtunnel-limit

指定隧道的出接口

指定隧道的出接口，在隧道配置模式下，使用以下命令：

interface *interface-name*

- *interface-name* – 指定隧道出接口的名称。可以是物理接口或者逻辑接口（隧道接口除外）。

在隧道配置模式下，使用以上命令 no 的形式取消隧道出接口的指定。

no interface

指定手工隧道的目的地址

6to4 自动隧道的目的地址可以通过 IPv4 兼容 IPv6 地址中嵌入的 IPv4 地址自动获得，因此用户无需指定 6to4 自动隧道的目的地址。指定 IPv6 6to4 手工隧道的目的地址，在隧道配置模式下，使用以下命令：

destination *ipv4-address*

- *ipv4-address* – 指定手工隧道的目的地址。该地址是一个 IPv4 地址。

在隧道配置模式下，使用以上命令 no 的形式取消手工隧道目的地址的指定：

no destination

绑定 IPv6 6to4 隧道到隧道接口

绑定 IPv6 6to4 隧道到隧道接口，在隧道接口配置模式下（全局配置模式下使用 **interface tunnel***X* 命令进入隧道接口配置模式），使用以下命令：

tunnel ip6in4 *ipv6-tunnel-name*

- *ipv6-tunnel-name* – 指定 IPv6 6to4 隧道的名称。

隧道接口配置模式下，使用以上命令 no 的形式取消 IPv6 6to4 隧道与隧道接口的绑定：

no tunnel ip6in4 *ipv6-tunnel-name*

显示 IPv6 6to4 隧道配置信息

显示 IPv6 6to4 隧道配置信息，在任何模式下使用以下命令：

show ip6in4 {**manual-tunnel** | **6to4-tunnel**}

IPv6 4to6 隧道配置

当前网络中，IPv4 网络仍是主流网络，但 IPv6 网络的应用越来越广泛。随着 IPv6 网络的大规模部署，为了让 IPv4 孤岛之间进行通信，StoneOS 支持 IPv6 4to6 隧道技术，即通过 IPv6 网络实现 IPv4 孤岛之间的通信。

当前版本仅支持手工方式配置。手工隧道提供点到点的连接，其通道的终止点是手工静态配置的。

手工隧道配置方式如下：

- 创建隧道
- 指定隧道的源地址/出接口
- 指定隧道的目的地址
- 绑定隧道到隧道接口

创建隧道

创建 IPv6 4to6 手工隧道，在全局配置模式下使用以下命令。执行以下命令后，系统创建指定名称的 IPv6 4to6 隧道，并进入隧道配置模式；如果指定的名称已存在，则直接进入隧道配置模式。

tunnel ip4in6 *tunnel-name* **manual**

- *tunnel-name* – 指定 IPv6 4to6 隧道的名称。

在全局配置模式下，使用以上命令 no 的形式删除指定的IPv6 手工隧道：

no tunnel ip4in6 *tunnel-name* **manual**

指定隧道的源地址/出接口

指定 IPv6 4to6 手工隧道的出接口和源地址，在隧道配置模式下，使用以下命令：

interface *interface-name* **source** *ipv6-address*

- *interface-name* – 指定隧道的出接口。
- *ipv6-address* – 指定 IPv6 4to6 隧道的源地址。该地址是一个 IPv6 地址。

在隧道配置模式下，使用该命令 no 的形式删除隧道出接口和源地址：

no interface

指定隧道的目的地址

指定 IPv6 4to6 手工隧道的目的地址，在隧道配置模式下，使用以下命令：

destination *ipv6-address*

- *ipv6-address* – 指定 IPv6 4to6 隧道的目的地址。该地址是一个 IPv6 地址。

在隧道配置模式下，使用以上命令 no 的形式取消隧道目的地址的指定：

no destination

绑定 IPv6 4to6 隧道到隧道接口

绑定 IPv6 4to6 手工隧道到隧道接口，在隧道接口配置模式下（全局配置模式下使用 **interface tunnel***X* 命令进入隧道接口配置模式），使用以下命令：

tunnel ip4in6 *tunnel-name*

- *tunnel-name* – 指定 IPv6 4to6 手工隧道的名称。

在隧道接口配置模式下，使用以上命令 no 的形式取消 IPv6 4to6 隧道与隧道接口的绑定：

no tunnel ip4in6 *tunnel-name*

显示 IPv6 4to6 隧道配置信息

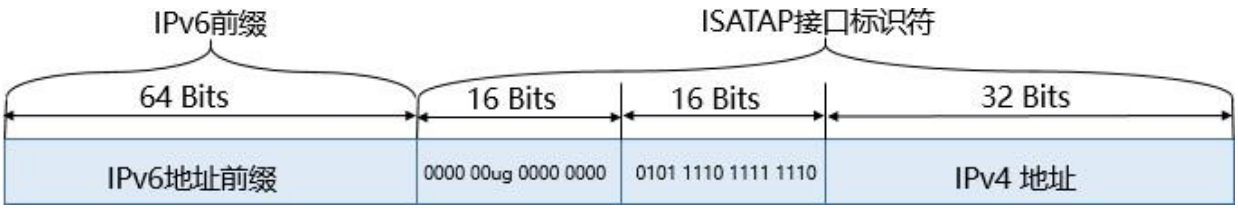
显示 IPv6 4to6 隧道配置信息，在任何模式下使用以下命令：

show ip4in6 manual-tunnel

ISATAP 隧道配置

ISATAP（Intra-Site Automatic Tunnel Addressing Protocol）是一种 IPv6 点到多点的自动隧道技术，主要用于 IPv4 网络中的双栈主机通过 ISATAP 隧道访问 IPv6 网络，通过在 IPv6 报文的目的地址中嵌入的 IPv4 地址，可以自动获取隧道的终点。

使用 ISATAP 隧道时，IPv6 报文的目的地址和隧道接口的 IPv6 地址都要采用特殊的 ISATAP 地址。ISATAP 地址包含一个IPv6 前缀和 ISATAP 接口标识符。ISATAP 地址格式如下：



- 如果 IPv4 地址是全局唯一的，则 u 位为 1，否则 u 位为 0。
- g 位是 IEEE 群体/个体标志，固定为 0。

例如，IPv6 地址前缀为：2001:DB8:1234:5678::/64；需要嵌入的 IPv4 地址为：10.173.129.8，该 IPv4 地址在 ISATAP 格式中表示为 16 进制：0AAD:8108; 最终的 ISATAP 地址即为：2001:DB8:1234:5678:0000:5EFE:0AAD:8108。

ISATAP 隧道配置如下：

- 创建 ISATAP 隧道
- 指定 ISATAP 子隧道最大数
- 指定 ISATAP 隧道的出接口
- 绑定 ISATAP 隧道到隧道接口

创建 ISATAP 隧道

创建 ISATAP 隧道，在全局配置模式下使用以下命令。执行以下命令后，系统创建指定名称的 ISATAP 隧道，并进入 ISATAP 隧道配置模式；如果指定的名称已存在，则直接进入 ISATAP 隧道配置模式。

tunnel ip6in4 *tunnel-name* **isatap**

- *tunnel-name* – 指定 ISATAP 隧道的名称。
- **isatap** – 指定隧道类型为 ISATAP 隧道。

在全局配置模式下，使用以上命令 no 的形式删除指定的 ISATAP 隧道：

no tunnel ip6in4 *tunnel-nam***isatap**

指定 ISATAP 子隧道最大数

系统内最多可创建 10 个 ISATAP 隧道，且每个接口最多可配置一个 ISATAP 隧道。每个隧道下最多可配置 1200 个子隧道。指定 ISATAP 子隧道数，在 ISATAP 隧道配置模式下，使用以下命令：

subtunnel-limit*maximum*

- *maximum* – 指定 ISATAP 子隧道数，取值范围为 1 至 1200，默认值为 200。

在 ISATAP 隧道配置模式下，使用该命令 no 的形式恢复子隧道数的默认值。

no subtunnel-limit

指定 ISATAP 隧道的出接口

指定 ISATAP 隧道的出接口，在 ISATAP 隧道配置模式下，使用以下命令：

interface *interface-name*

- *interface-name* – 指定 ISATAP 隧道出接口的名称。可以是物理接口或者逻辑接口（隧道接口除外）。

在 ISATAP 隧道配置模式下，使用以上命令 no 的形式取消隧道出接口的指定。

no interface

绑定 ISATAP 隧道到隧道接口

绑定 ISATAP 隧道到隧道接口，在隧道接口配置模式下（全局配置模式下使用 **interface tunnel***X* 命令进入隧道接口配置模式），使用以下命令：

tunnel ip6in4*ipv6-tunnel-name*

- *ipv6-tunnel-name* – 指定 ISATAP 隧道的名称。

隧道接口配置模式下，使用以上命令 no 的形式取消 ISATAP 隧道与隧道接口的绑定：

no tunnel ip6in4*ipv6-tunnel-name*

显示 ISATAP 隧道配置信息

显示 ISATAP 隧道配置信息，在任何模式下使用以下命令：

show ip6in4isatap-tunnel

配置 DS-lite

系统支持DS-lite 技术。DS-lite 技术结合 IPv4-in-IPv6 隧道技术和 NAT 技术。IPv4 终端用户使用 B4（Base Bridge Broadband）设备与 AFTR(Adress Family Transition Router)设备在 IPv6 网络中创建隧道，从而与 IPv4 网络进行通信。在 IPv6 4to6 隧道的终点，AFTR 设备使用 NAT 技术，将用户的 IPv4 私网地址进行转换。

设备可以作为AFTP 设备，提供 DS-lite 功能和NAT 功能。DS-lite 功能配置包含如下内容：

- 创建DS-lite 隧道
- 为 DS-lite 隧道指定接口及地址
- 指定最大子隧道数

在实际使用 DS-lite 技术的时候，除了配置 DS-lite 相关配置，也需要配置 NAT 相关配置。

创建 DS-lite 隧道

每台设备支持创建最多 10 条 DS-lite 隧道。创建DS-lite 隧道，在全局配置模式下使用以下命令。执行以下命令后，系统创建指定名称的DS-lite 隧道，并进入DS-lite 隧道配置模式；如果指定的名称已存在，则直接进入 DS-lite 隧道配置模式。

tunnel ip4in6 *tunne-name* **ds-lite**

- *tunnel-name* – 指定 DS-lite 隧道的名称。

在全局配置模式下，使用以上命令 no 的形式删除隧道：

no tunnel ip4in6 *tunnel-name* **ds-lite**

为 DS-lite 隧道指定接口及地址

指定DS-lite 隧道的接口及接口地址，在DS-lite 隧道配置模式下，使用以下命令：

interface *interface-name* **src-ip** *X:X:X:X::X*

- *interface-name* - 为 DS-lite 隧道指定出接口。
- *X:X:X:X::X* – 为 DS-lite 隧道出接口指定IPv6 地址。此 IPv6 地址需要为出接口的某一个 IPv6 地址。

在 DS-lite 隧道配置模式下，使用 **no interface** 取消接口和地址的指定。

指定最大子隧道数

当一个新的 B4 设备隧道接入时，AFTR 为其动态生成一条子隧道。指定可以创建的最大子隧道数，在 DS-lite 隧道配置模式下，使用以下命令：

subtunnel-limit *value*

- *value* – 指定 AFTR 可以创建的最大子隧道数。默认值是 200。取值范围是 1 到 1200。

使用该命令 no 的形式恢复默认值。

显示 DS-lite 隧道配置信息

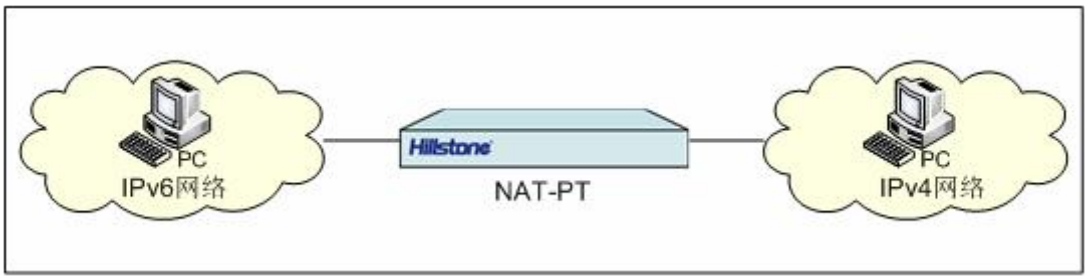
显示DS-lite 隧道配置信息，在任何模式下使用以下命令：

show ip4in6 ds-lite-tunnel

NAT-PT 配置

IPv6 能够很好地解决 IP 地址日益短缺的问题，并将取代 IPv4 成为下一代互联网的核心。但是，互联网不可能在短时间内从现有的 IPv4 网络升级到 IPv6 网络，而且在相当长的一段时间内，IPv6 网络将和 IPv4 网络共存并且需要相互通信。

NAT-PT（Network Address Translation – Protocol Translation）即网络地址转换及协议转换，是一种可以解决纯 IPv6 网络和纯 IPv4 网络相互通信的过渡机制。NAT-PT 主要是利用NAT 进行 IPv4 地址和 IPv6 地址的相互转换，同时通过PT 按照语义等价的原则对协议进行转换，包括网络层协议、传输层协议以及应用层协议。通过使用 NAT-PT，用户无需对现有的 IPv4 网络做任何改变就能实现 IPv6 网络和 IPv4 网络的相互通信。下图为纯 IPv6 网络和纯 IPv4 网络通过开启 NAT-PT 功能的 设备实现相互通信的示意图。



注意:当前版本的NAT-PT 功能支持 IP、TCP、UDP 和 ICMP 协议转换，并且支持FTP-ALG、TFTP-ALG 和 HTTP-ALG。

配置 NAT-PT 规则

NAT-PT 规则基于VRouter 创建并生效。用户可以在VRouter 配置模式下，创建 SNAT/DNAT 规则、修改 SNAT/DNAT 规则排列以及删除 SNAT/DNAT 规则等。

进入VRouter 配置模式，在全局配置模式下使用以下命令：

ip vrouter *vrouter-name*

- *vrouter-name* – 指定 VRouter 的名称。

创建 SNAT 规则

SNAT 规则指定是否对符合条件的流量的源 IPv6/IPv4 地址做 NAT-PT 转换，如果需要转换，则同时指定转换的地址和方式。配置做 NAT-PT 转换的 SNAT 规则，在VRouter 配置模式下使用以下命令：

snatrule [**id** *id*] [**before** *id* | **after** *id* | **top**] **from** *src-address* **to** *dst-address* [**eif** *egress-interface* | **evr** *vrouter-name*] **trans-to** {**addressbook** *trans-to-address* | **eif-ip**} **mode** {**static** | **dynamicip** | **dynamicport** [**sticky**]} [**log**] [**group** *group-id*] [**description** *description*]

- **id** *id* – 为 SNAT 规则指定 ID 号。每一条 SNAT 规则都有一个唯一的 ID。如果不指定，系统会自动分配。如果指定的 ID 为已有的 SNAT 规则的 ID，已有的规则会被覆盖。
- **before** *id* | **after** *id* | **top** – 指定规则所在的位置，可以是位于某个 ID 之前（**before** *id*）或者之后（**after** *id*），也可以是位于所有规则的首位（**top**）。如果不指定，该规则会处于所有 SNAT 规则的末尾。默认情况下，系统会将新创建的 SNAT 规则放到所有 SNAT 规则的末尾。
- **from** *src-address* **to** *dst-address* [**eif** *egress-interface* | **evr** *vrouter-name*] – 指定该规则中流量应符合的条件。条件包括：
  - **from** *src-address* - 指定流量的源 IP 地址，*src-address* 可以是 IPv4 地址、IPv6 地址或者系统地址簿中指定的地址条目。
  - **to** *dst-address* - 指定流量的目的 IP 地址，*dst-address* 可以是 IPv4 地址、IPv6 地址或者系统地址簿中指定的地址条目。
  - **eif** *egress-interface* | **evr** *vrouter-name*- 指定流量的出接口（**eif** *egress-interface*）或者流量的下一跳 VRouter（**evr** *vrouter-name*）。
- **addressbook** *trans-to-address* | **eif-ip** – 指定 NAT-PT 转换地址。可以是 IPv4 地址、IPv6 地址或者系统地址簿中的地址，也可以是出接口的 IP 地址（**eif-ip**）。当配置为 NAT46 时，不支持指定为 **eif-ip**。
- **mode** {**static** | **dynamicip** | **dynamicport** [**sticky**]} – 指定转换模式。系统支持三种模式实现 IPv4 地址和 IPv6 地址之间的相互转换：static、dynamicip 和 dynamicport。
  - **static** - 静态源NAT-PT 转换即一对一的转换。该模式要求被转换到的地址条目（trans-to-address）包含的 IP 地址数与流量的源地址的地址条目（src-address）包含的 IP 地址数相同。
  - **dynamicip** - 动态源 NAT-PT 转换即多对多的转换。该模式将源地址转换到指定的 IP 地址。每一个源地址会被映射到一个唯一的 IP 地址做转换，直到指定地址全部被占用。

- **dynamicport** - 即 NAPT-PT（Network Address Port Translation – Protocol Translation）。多个源地址将被转换成指定 IP 地址条目中的一个地址。如果不使用 sticky，系统会根据 hash 算法选择地址条目中的一个地址，当这个地址的端口资源被用尽，下一个地址将会被使用。如果使用了 sticky，每一个源 IP 产生的所有会话将被映射到同一个固定的 IP 地址。

- **log** – 使用该参数开启该 SNAT 规则的日志功能（当有流量匹配该地址转换规则时产生日志信息）。

- **group** *group-id* - 指定 SNAT 规则所属的 HA 组。如不指定该参数，创建的 SNAT 规则属于 HA 组 0。

例如，以下命令示例实现了 untrust 域中以太网接口ethernet0/0 的基于接口的 NAT-PT 转换：

```
hostname(config-vrouter)# snatrule from ipv6-any to ipv6-any eif ethernet0/0 trans-to eif-ip mode dynamicport
rule id=1
```

配置不做 NAT-PT 转换的 SNAT 规则，在VRouter 配置模式下使用以下命令：

snatrule [**id** *id*] [**before** *id* | **after** *id* | **top**] **from** *src-address* **to** *dst-address* [**eif** *egress-interface* | **evr** *vrouter-name*] **no-trans** [**group** *group-id*]

修改 SNAT 规则排列顺序

每一条 SNAT 都有唯一一个 ID 号。流量进入设备时，设备对 SNAT 规则进行顺序查找，然后按照查找到的相匹配的第一条规则对流量的源 IP 做 NAT-PT 转换。但是，ID 的大小顺序并不是规则匹配顺序。使用 show snat 命令列出的规则顺序才是规则匹配顺序。用户可以移动已有的 SNAT 规则从而改变规则的排列顺序。改变规则的排列顺序，在 VRouter 配置模式下使用以下命令：

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

- *id* – 指定被移动的 SNAT 规则的 ID 号。

- **before** *id* – 将 SNAT 规则移动到某个 ID 之前。

- **after** *id* – 将 SNAT 规则移动到某个 ID 之后。

- **top** – 将 SNAT 规则移动到所有 SNAT 规则之首。

- **bottom** – 将 SNAT 规则移动到所有 SNAT 规则的末尾。

删除 SNAT 规则

在 VRouter 配置模式下，用户可以通过使用以下命令删除指定 ID 号的 SNAT 规则：

no snatrule id *id*

显示 SNAT 配置信息

SNAT 配置完毕，用户可以在任何 CLI 模式下通过使用以下命令查看系统中 SNAT 的配置信息：

show snat [**id** *id*] [**vrouter** *vrouter-name*]

- **id** *id* – 显示指定 ID 号的 SNAT 规则信息。
- **vrouter** *vrouter-name* – 显示指定 VRouter 的 SNAT 配置信息。

当 SNAT 的转换模式为 dynamicport 时，用户可以在任何 CLI 模式下通过使用以下命令查看源端口地址池中资源的利用情况：

show snat resource [**vrouter** *vrouter-name*]

- **vrouter** *vrouter-name* – 显示指定 VRouter 的 SNAT 源端口地址池中资源的利用情况。

创建 DNAT 规则

DNAT 规则指定是否对符合条件的流量的目的 IPv6/IPv4 地址做NAT-PT 转换。配置做 NAT-PT 转换的 DNAT 规则，在VRouter 配置模式下使用以下命令：

dnatrule [**id** *id*] [**before** *id* | **after** *id* | **top**] **from** *src-address* **to** *dst-address* [**service** *service-name*] **trans-to** *trans-to-address* [**port** *port*] [**load-balance**] [**track-tcp** *port*] [**track-ping**] [**log**] [**group** *group-id*] [**description** *description*]

- id id – 为 DNAT 规则指定 ID 号。每一条 DNAT 规则都有一个唯一的 ID。如果用户不指定，系统会为规则自动生成一个 ID。如果指定的 ID 为已有的 DNAT 规则的 ID，已有的规则会被覆盖。
- **before** *id* | **after** *id* | **top** – 指定规则所在的位置，可以是位于某个 ID 之前（**before** *id*）或者之后（**after** *id*），也可以是位于所有规则的首位（**top**）。如果不指定，该规则会处于所有 DNAT 规则的末尾。默认情况下，系统会将新创建的 DNAT 规则放到所有 DNAT 规则的末尾。流量进入设备时，设备对DNAT 规则进行查找，然后按照查找到的相匹配的第一条规则对流量的目的 IP 做 NAT 转换。
- **from** *src-address* **to** *dst-address* [**service** *service-name*] – 指定该规则中流量应符合的条件。条件包括：
  - **from** *src-address* – 指定流量的源 IP 地址。*src-address* 可以是 IPv4 地址、IPv6 地址或者系统地址簿中指定的地址条目。
  - **to** *dst-address* – 指定流量的目的 IP 地址。*dst-address* 可以是 IPv4 地址、IPv6 地址或者系统地址簿中指定的地址条目。
  - **service** *service-name* – 指定流量的服务类型。如果需要一并转换端口号（通过 **port** *port* 参数指定），这里指定的服务就只能拥有一个协议，并且该协议只能对应一个端口，例如 TCP 端口号可以是 80，但不可以是 80 到 100。

- **trans-to** *trans-to-address* – 指定 NAT-PT 转换地址。*trans-to-address* 可以是 IPv4 地址、IPv6 地址或者系统地址簿中定义的地址条目。此处指定的 NAT-PT 转换地址个数必须与流量目的 IP 地址（由命令的 **to** *dst-address* 参数指定）的个数相同。
- **port** *port* – 内网服务器的端口号。
- **load-balance** – 配置 load-balance 参数为该条 DNAT 规则开启负载均衡功能，即均衡流量到不同的内网服务器。
- **track-tcp** *port* – 配置 track-tcp 参数并指定内网服务器端口号，系统会向内网服务器发送 TCP 报文，监控服务器的特定 TCP 端口是否可达。
- **track-ping** – 配置 track-ping 参数，系统会向内网服务器发送Ping 报文，监控服务器是否可达。
- **log** – 使用该参数开启该 DNAT 规则的日志功能（当有流量匹配该地址转换规则时产生日志信息）。
- [**group** *group-id*] - 指定 DNAT 规则所属的 HA 组。如不指定该参数，创建的DNAT 规则属于 HA 组 0。

例如，以下命令将任何到 addr1 的请求的 IP 转换成 addr2 的 IP 地址，并且不转换服务的端口号：

```
hostname(config-vrouter)# dnatrule from ipv6-any to addr1 service any trans-to addr2
rule id=1
```

配置不做 NAT-PT 转换的 DNAT 规则，在VRouter 配置模式下使用以下命令：

dnatrule [**id** *id*] [**before** *id* | **after** *id* | **top**] **from** *src-address* **to** *dst-address* [**service** *service-name*] **no-trans** [**group** *group-id*]

修改 DNAT 规则排列顺序

每一条 DNAT 都有唯一一个 ID 号。每一条 DNAT 都有唯一一个 ID 号。流量进入设备时，设备对 DNAT 规则进行顺序查找，然后按照查找到的相匹配的第一条规则对流量的目的 IP 做 NAT 转换。但是，ID 的大小顺序并不是规则匹配顺序。使用 show dnat 命令列出的规则顺序才是规则匹配顺序。用户可以移动已有的 DNAT 规则从而改变规则的排列顺序。修改DNAT 规则排列顺序，在 VRouter 配置模式下使用以下命令：

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

- *id* – 指定被移动的DNAT 规则的 ID 号。
- **before** *id* – 将 DNAT 规则移动到某个 ID 之前。
- **after** *id* – 将 DNAT 规则移动到某个 ID 之后。

- top – 将 DNAT 规则移动到所有 SNAT 规则之首。
- bottom – 将 DNAT 规则移动到所有 SNAT 规则的末尾。

删除 DNAT 规则

在 VRouter 配置模式下，用户可以通过使用以下命令删除指定 ID 号的 DNAT 规则：

no dnatrule id *id*

显示 DNAT 配置信息

DNAT 配置完毕，用户可以在任何 CLI 模式下通过使用以下命令查看系统中 DNAT 的配置信息：

show dnat [**id** *id*] [**vrouter** *vrouter-name*]

- **id** *id* – 显示指定 ID 号的 DNAT 规则信息。
- **vrouter** *vrouter-name* – 显示指定 VRouter 的 DNAT 规则信息。

显示配置有负载均衡功能的 DNAT 规则相关信息，在任何模式下，使用以下命令：

show dnat server [*ip-address*] [**vrouter** *vrouter-name*] [**tcp-port** *port*] [**ping**]

- *ip-address* – 显示指定 IP 地址的内网服务器状态信息。
- **vrouter** *vrouter-name* – 显示指定 VRouter 的内网服务器状态信息。
- **tcp-port** *port* – 显示指定端口号的内网服务器状态信息。
- **ping** – 显示内网服务器的Ping 监控状态信息。

DNS64 和 NAT64 配置

DNS64 和 NAT64 作为纯 IPv6 网络和纯 IPv4 网络相互通信的过渡机制，主要支持 IPv6 客户端主动发起通信请求，访问 IPv4 服务端网络资源。该机制解决了 NAT-PT 技术在 IPv6 网络和 IPv4 网络相互通信时的大部分缺陷。

DNS64 用于当 IPv6 客户端主机收到DNS 查询时，先解析DNS 查询信息中的AAAA 记录（IPv6 地址），如果解析成功，则直接将 IPv6 地址返回给客户端；如果解析失败，那么DNS64 将会解析DNS 查询信息中的A 记录（IPv4 地址），并将 A 记录（IPv4 地址）合成 AAAA 记录（IPv6 地址）返回给客户端。

NAT64 与 DNS64 配合使用，NAT64 主要实现 IPv6 地址到 IPv4 地址的转换。在做源地址转换时，NAT64 通过 IPv4 地址池将源 IPv6 地址转换为源 IPv4 地址；而在做目的地址转换时，NAT64 直接从 DNS64 返回的 IPv6 地址中抽取对应的目的 IPv4 地址。

设备通过结合 IPv6 DNS 代理规则并且配置 DNS64 功能和 NAT64 规则来实现 DNS64 和 NAT64 功能。NAT64 规则包括 SNAT 规则和 DNAT 规则。其中，创建SNAT 规则和NAT-PT 中的 SNAT 规则配置方法相同。关于如何创建 SNAT 规则的详细情况，

请参阅 NAT-PT 配置一节中的“创建 SNAT 规则”。

创建 DNS64 规则

仅部分版本支持 DNS64 规则。创建 DNS64 规则，在全局配置模式下使用以下命令：

ipv6 dns64-proxy id *id* **prefix** *ipv6-address/Mask* [**source** {*ipv6-address/Mask* | *address-entry-v6*} | **trans-mapped-ip** {*ipv4-address/Mask* | *address-entry-v4*}]

- **id** *id* – 为 DNS64 规则指定 ID 号，取值范围为 1 到 16。每一条 DNS64 规则都有一个唯一的 ID。如果指定的 ID 为已有的DNS64 规则的 ID，已有的规则会被覆盖。
- **prefix** *ipv6-address/Mask* – 指定 IPv6 前缀以及前缀长度。DNS64 使用此前缀进行 IPv4 地址到 IPv6 地址的合成。前缀长度取值范围为 0 到 96。
- **source** {*ipv6-address/Mask* | *address-entry-v6*} – 指定流量的源 IP 地址，可以是 IPv6 地址或者系统地址簿中指定的 IPv6 地址条目。
- **trans-mapped-ip** {*ipv4-address/Mask* | *address-entry-v4*} – 指定 IPv4 DNS 服务器的响应地址，可以是 IPv4 地址或者系统地址簿中指定的 IPv4 地址条目。

在全局配置模式下，使用以下命令删除指定 ID 号的 DNS64 规则：

no ipv6 dns64-proxy id *id*

开启/关闭 DNS64 功能

当用户配置了 IPv6 DNS 代理规则后，可以指定开启或关闭 DNS64 功能。默认情况下DNS64 功能是关闭的，在 DNS 代理规则配置模式下，使用以下命令：

- 开启：**dns64 enable**（执行该命令后，系统进入 DNS64 配置模式）
- 关闭：**no dns64 enable**

注意:仅支持在IPv6 DNS 代理规则中开启 DNS64 功能，IPv4 DNS 代理规则中不支持。

配置 DNS64 服务器

DNS64 服务器用于解析DNS 查询信息中的A 记录（IPv4 地址），每条 IPv6 DNS 代理规则最多可以指定 6 个 DNS64 服务器。配置 DNS64 服务器，在 DNS64 配置模式下，使用以下命令：

server *server-ip* [**vrouter** *vrouter-name*]

- *server-ip* – 指定 DNS64 服务器的 IP 地址，该 IP 地址只能为 IPv4 地址。
- *vrouter-name* – 指定 DNS64 服务器所属的虚拟路由器。

使用 **no server** *server-ip* [**vrouter** *vrouter-name*] 删除 DNS64 服务器。

配置 DNS64 前缀

用户需要指定 DNS64 前缀来用于将A 记录（IPv4 地址）合成AAAA 记录（IPv6 地址），合成的 IPv6 地址为“DNS64 前缀+IPv4 地址”形式。默认情况下，DNS64 前缀为“64:ff9b:: /96”。指定 DNS64 前缀以及前缀长度，在 DNS64 配置模式下，使用以下命令：

prefix *ipv6-address/Mask*

- *ipv6-address* – 指定 DNS64 前缀地址。
- *Mask* – 指定前缀长度。取值范围为 1 到 96。

使用 **no prefix** *ipv6-address/Mask* 取消 DNS64 前缀的配置。

创建 DNAT 规则

创建 DNAT 规则，在VRouter 配置模式下使用以下命令：

dnatrule [**id** *id*] [**before** *id* | **after** *id* | **top**] **from** *src-address* **to** *dst-address* [**service** *service-name*] **v4-mapped** [**log**] [**group** *group-id*]

- **id** *id* – 为 DNAT 规则指定 ID 号。每一条 DNAT 规则都有一个唯一的 ID。如果用户不指定，系统会为规则自动生成一个 ID。如果指定的 ID 为已有的 DNAT 规则的 ID，已有的规则会被覆盖。
- **before** *id* | **after** *id* | **top** – 指定规则所在的位置，可以是位于某个 ID 之前（**before** *id*）或者之后（**after** *id*），也可以是位于所有规则的首位（**top**）。如果不指定，该规则会处于所有 DNAT 规则的末尾。默认情况下，系统会将新创建的 DNAT 规则放到所有 DNAT 规则的末尾。流量进入设备时，设备对DNAT 规则进行查找，然后按照查找到的相匹配的第一条规则对流量的目的 IP 做 NAT 转换。
- **from** *src-address* **to** *dst-address* [**service** *service-name*] – 指定该规则中流量应符合的条件。条件包括：
  - **from** *src-address* – 指定流量的源 IP 地址。src-address 可以是 IPv6 地址或者系统地址簿中指定的 IPv6 地址条目。
  - **to** *dst-address* – 指定流量的目的 IP 地址。dst-address 可以是 IPv6 地址或者系统地址簿中指定的 IPv6 地址条目。
  - *service-name* – 指定流量的服务类型。这里指定的服务就只能拥有一个协议，并且该协议只能对应一个端口，例如 TCP 端口号可以是 80，但不可以是 80 到 100。

- **v4-mapped** – 指定直接从报文的目的 IPv6 地址中抽取目的 IPv4 地址。
- **log** – 使用该参数开启该 DNAT 规则的日志功能（当有流量匹配该地址转换规则时产生日志信息）。
- **group** *group-id* - 指定 DNAT 规则所属的 HA 组。如不指定该参数，创建的DNAT 规则属于 HA 组 0。

在 VRouter 配置模式下，使用以下命令删除指定 ID 号的 DNAT 规则：

no dnatrule id *id*

IPv6 监测对象配置

配置 IPv6 监测功能，首先需配置监测对象，在全局配置模式下，使用以下命令：

track *track-object-name* [**local**]

- **track-object-name** – 指定监测对象名称。范围是 1 到 31 个字符。
- **local** – 若指定该参数，系统将不向备份设备同步该监测对象的相关配置信息。默认情况下，不指定该参数。

执行该命令后，系统创建指定名称的监测对象，并且进入监测对象配置模式；如果指定的名称已存在，则直接进入监测对象的配置模式。使用该命令 no 的形式删除指定的监测对象：

no track *track-object-name*

系统支持通过 ICMP 报文、HTTP 报文、DNS 报文、NDP 报文和 TCP 报文五种方式对目标进行基于 IPv6 的主动监测。

IPv6 ICMP 报文监测

通过 ICMP 报文对目标进行监测，在监测对象配置模式下使用以下命令：

icmp6 {*ipv6-address* | **host***host-name*} **interface***interface-name* [**interval***value*] [**threshold***value*] [**src-interface***interface-name* [**prior-used-srcip**]] [**weight***value*]

- *ipv6-address* | **host** *host-name* – 指定监测目标的IPv6 地址或者主机名称。主机名称范围是 1 到 63 个字符。
- **interface** *interface-name* – 指定发送Ping 检测报文的出接口。
- **interval** *value* – 指定发送Ping 报文的时间间隔，单位为秒。范围是 1 到 255 秒。默认值是 3 秒。
- **threshold** *value* – 指定判断监测失败的警戒值。如果系统连续未收到该参数指定个数的响应报文，就判断为监测失败，即目标不可达。取值范围是 1 到 255。默认值是 3。

- **src-interface** *interface-name* – 指定 Ping 检测报文的源接口。
- **prior-used-srcip** *ipv6-address* – 若源接口上已配置多个 IPv6 地址，将其中一个 IP 指定为 prior-used-srcip 后，系统将使用此 IP 发送track 报文；若没有指定该参数，则使用默认的源接口主 IP 发送 track 报文。
- **weight** *value* – 指定该条监测失败对整个监测对象失败贡献的权重值。取值范围是 1 到 255。默认值是 255。

用户可以配置多条该命令为监测对象指定多个监测条目。使用该命令 no 的形式删除指定的监测条目：

no icmp6 {*ipv6-address* | **host***host-name*} **interface***interface-name* [**delay**]

IPv6 HTTP 报文监测

通过 HTTP 报文对目标进行监测，在监测对象配置模式下使用以下命令：

http ipv6 {*ipv6-address* | **host***host-name*} **interface***interface-name* [**interval***value*] [**threshold***value*] [**src-interface***interface-name*] [**weight***value*]

- *ipv6-address* | **host** *host-name* – 指定监测目标的IPv6 地址或者主机名称。主机名称范围是 1 到 63 个字符。
- **interface** *interface-name* – 指定发送 HTTP 检测报文的出接口。
- **interval** *value* – 指定发送 HTTP 报文的时间间隔，单位为秒。范围是 1 到 255 秒。默认值是 3 秒。
- **threshold** *value* – 指定判断监测失败的警戒值。如果系统连续未收到该参数指定个数的响应报文，就判断为监测失败，即目标不可达。取值范围是 1 到 255。默认值是 3。
- **src-interface** *interface-name* – 指定 HTTP 检测报文的源接口。
- **weight** *value* – 指定该条监测失败对整个监测对象失败贡献的权重值。取值范围是 1 到 255。默认值是 255。

用户可以配置多条该命令为监测对象指定多个监测条目。使用该命令 **no** 的形式删除指定的监测条目：

no http ipv6 { *ipv6-address* | **host***host-name*} **interface***interface-name*

IPv6 DNS 报文监测

通过DNS 报文对目标进行监测，在监测对象配置模式下使用以下命令：

dns ipv6 *ipv6-address* **interface***interface-name* [**interval***value*] [**threshold***value*] [**weight***value*] [**src-interface***interface-name*]

- *ipv6-address* – 指定监测目标的IPv6 地址。**interface***interface-name* – 指定发送 DNS 检测报文的出接口。

- **interval***value* – 指定发送DNS 报文的时间间隔，单位为秒。范围是 1 到 255 秒。默认值是 3 秒。
- **threshold***value* – 指定判断监测失败的警戒值。如果系统连续未收到该参数指定个数的响应报文，就判断为监测失败，即目标不可达。取值范围是 1 到 255。默认值是 3。
- **weight***value* – 指定该条监测失败对整个监测对象失败贡献的权重值。取值范围是 1 到 255。默认值是 255。
- **src-interface***interface-name* – 指定 DNS 检测报文的源接口。

用户可以配置多条该命令为监测对象指定多个监测条目。使用该命令 no 的形式删除指定的监测条目：

no dns ipv6*ipv6-address***interface***interface-name*

NDP 报文监测

通过 NDP 报文对目标进行监测，在监测对象配置模式下使用以下命令：

ndp ipv6-address interface interface-name [interval value] [threshold value] [weight value]

ndp *ipv6-address***interface***interface-name* [**interval***value*] [**threshold***value*] [**weight***value*]

- *ipv6-address* – 指定监测目标的 IPv6 地址。
- **interface** *interface-name* – 指定发送 NDP 检测报文的出接口。
- **interval** *value* – 指定发送 NDP 报文的时间间隔，单位为秒。范围是 1 到 255 秒。默认值是 3 秒。
- **threshold** *value* – 指定判断监测失败的警戒值。如果系统连续未收到该参数指定个数的响应报文，就判断为监测失败，即目标不可达。取值范围是 1 到 255。默认值是 3。
- **weight** *value* – 指定该条监测失败对整个监测对象失败贡献的权重值。取值范围是 1 到 255。默认值是 255。

用户可以配置多条该命令为监测对象指定多个监测条目。使用该命令 no 的形式删除指定的监测条目：

no ndp *ipv6-address* **interface** *interface-name*

IPv6 TCP 报文监测

通过 TCP 报文对目标端口进行监测，在监测对象配置模式下使用以下命令：

tcp ipv6 {{ipv6-addres | **host***host-name*} **port***port-number***interface***interface-name* [**interval***value*] [**threshold***value*] [**src-interface***interface-name*] [**weight***value*]

- *ipv6-address* | **host** *host-name* – 指定监测目标的IPv6 地址或者主机名称。主机名称范围是 1 到 63 个字符。
- **port***port-number* – 指定监测目标的目的端口号。取值范围为 0 到 65535。

- **interface***interface-name* – 指定发送 TCP 检测报文的出接口。
- **interval***value* – 指定发送 TCP 报文的时间间隔，单位为秒。范围是 1 到 255 秒。默认值是 3 秒。
- **threshold***value* – 指定判断监测失败的警戒值。如果系统连续未收到该参数指定个数的响应报文，就判断为监测失败，即目标不可达。取值范围是 1 到 255。默认值是 3。
- **src-interface***interface-name* – 指定 TCP 检测报文的源接口。
- **weight***value* – 指定该条监测失败对整个监测对象失败贡献的权重值。取值范围是 1 到 255。默认值是 255。

用户可以配置多条该命令为监测对象指定多个监测条目。对于同一个监测对象，不能同时配置对同一目标主机的 HTTP 监测和对端口 80（port 80）的 TCP 监测。使用该命令 no 的形式删除指定的监测条目：

no tcp ipv6 {*ipv6-address* | **host***host-name*} **port***port-number***interface***interface-name*

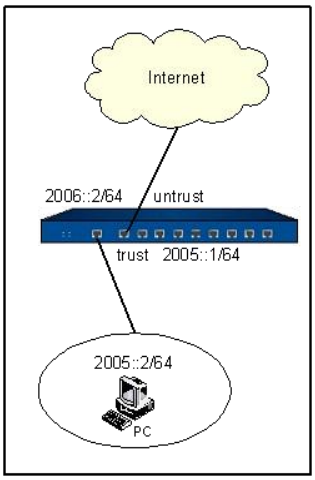
IPv6 配置举例

本节介绍 IPv6 相关的具体配置实例，包括：

- 例 1：IPv6 路由模式转发
- 例 2：IPv6 NAT-PT 配置举例
- 例 3：IPv6 DNS64 和 NAT64 配置举例

例 1：IPv6 路由模式转发

将设备以路由模式部署到网络中。接口ethernet0/0 属于trust 安全域，连接内网；接口ethernet0/1 属于untrust，连接 Internet。ISP 提供的公网地址为 2006::1/64。通过配置，保证内网 PC 可以访问 Internet。组网图如下图所示：



请按照以下步骤进行配置：

第一步：配置接口。

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ipv6 enable
hostname(config-if-eth0/0)# ipv6 address 2005::1/64
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ipv6 enable
hostname(config-if-eth0/1)# ipv6 address 2006::2/64
hostname(config-if-eth0/1)# exit
```

第二步：配置默认路由。

```
hostname(config)# ip vrouter trust-vr
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# src-addr 2005::2/64
hostname(config-policy-rule)# dst-addr ipv6-any
```

第三步：配置策略规则。

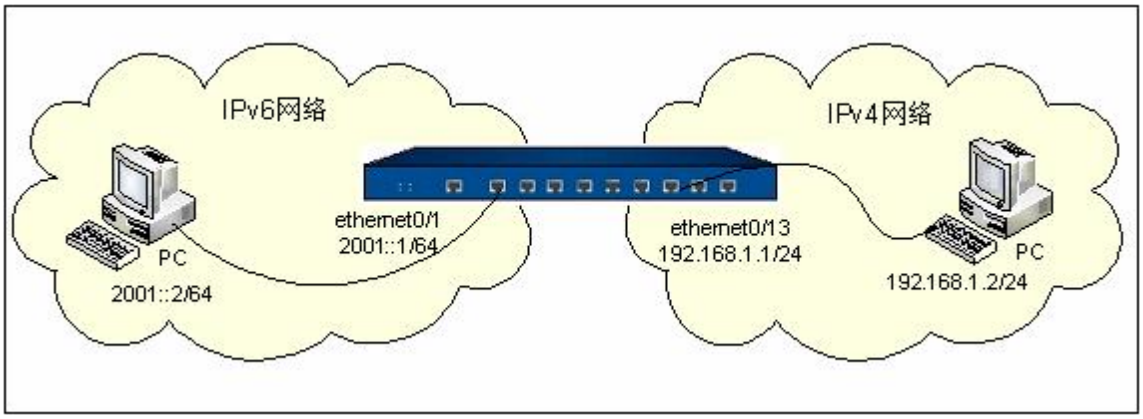
```
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config)#
```

例 2：IPv6 NAT-PT 配置举例

IPv6 网络和 IPv4 网络通过设备相连。要求通过在设备上进行 NAT-PT 配置，实现以下两个需求：

- 需求一：IPv6 网络中的主机可以主动访问 IPv4 网络中的主机，而 IPv4 网络中的主机不能主动访问 IPv6 网络中的主机；
- 需求二：IPv4 网络中的主机可以主动访问 IPv6 网络中的主机，而 IPv6 网络中的主机不能主动访问 IPv4 网络中的主机。

组网图如下图所示：



需求一

实现 IPv6 网络中的主机可以主动访问 IPv4 网络中的主机，而 IPv4 网络中的主机不能主动访问 IPv6 网络中的主机。假设对于 IPv6 网络中的主机来说，IPv4 中 PC 主机映射的 IPv6 地址为“2003::2”。请按照以下步骤进行配置：

第一步：配置接口。

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# ipv6 enable
```

```
hostname(config-if-eth0/1)# ipv6 address 2001::1/64
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/13
hostname(config-if-eth0/13)# zone trust
hostname(config-if-eth0/13)# ip address 192.168.1.1/24
hostname(config-if-eth0/13)# exit
hostname(config)#
```

第二步：配置 NAT-PT 规则。

```
hostname(config)# ip vrouter trust-vr
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr 2001::2/64
hostname(config-policy-rule)# dst-addr 2003::2/128
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
```

第三步：配置策略规则。

```
hostname(config)#
```

需求二

实现 IPv4 网络中的主机可以主动访问 IPv6 网络中的主机，而 IPv6 网络中的主机不能主动访问 IPv4 网络中的主机。假设对于 IPv4 网络中的主机来说，IPv6 中 PC 主机映射的 IPv4 地址为 192.168.2.2。请按照以下步骤进行配置：

第一步：配置接口。

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# ipv6 enable
hostname(config-if-eth0/1)# ipv6 address 2001::1/64
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/13
hostname(config-if-eth0/13)# zone trust
hostname(config-if-eth0/13)# ip address 192.168.1.1/24
hostname(config-if-eth0/13)# exit
hostname(config)#
```

第二步：配置 NAT-PT 规则。

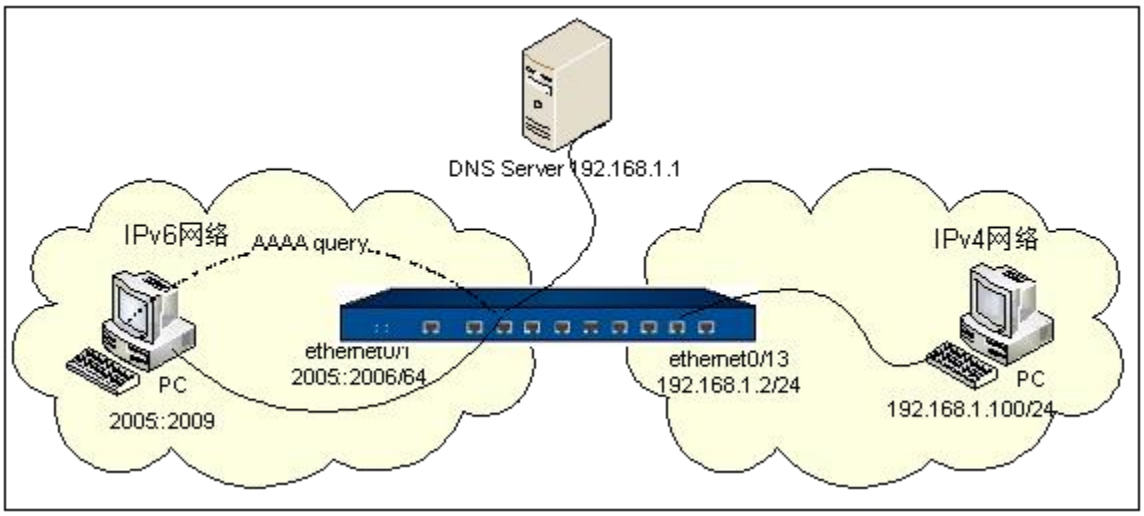
```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# snatrule from any to 192.168.2.2 service any trans-to 2001::2 mode dynamicport
rule ID=2
hostname(config-vrouter)# dnatrule from any to 192.168.2.2 service any trans-to 2001::2
rule ID=2
hostname(config-vrouter)# exit
hostname(config)#
```

第三步：配置策略规则。

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr 192.168.1.2/24
hostname(config-policy-rule)# dst-addr 192.168.2.2/32
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config)#
```

例 3：IPv6 DNS64 和 NAT64 配置举例

IPv6 网络和 IPv4 网络通过设备相连。要求通过在设备上进行 DNS64 和 NAT64 配置，实现 IPv6 网络中的主机可以主动访问 IPv4 网络中的主机。组网图如下图所示：



请按照以下步骤进行配置：

第一步：配置DNS 代理规则并开启 DNS64 功能。

```
hostname(config)# dns-proxy rule
hostname(config-dns-proxy-rule)# ingress-interface ethernet0/1
hostname(config-dns-proxy-rule)# src-addr 2005::2006/64
```

```
hostname(config-dns-proxy-rule)# dst-addr IPv6-any
hostname(config-dns-proxy-rule)# domain any
hostname(config-dns-proxy-rule)# action proxy
hostname(config-dns-proxy-rule)# name-server 192.168.1.1
hostname(config-dns-proxy-rule)# dns64 enable
hostname(config-dns-proxy-dns64)# prefix 64:ff9b:: /96
hostname(config-dns-proxy-dns64)# server 192.168.1.1
hostname(config-dns-proxy-dns64)# exit
hostname(config-dns-proxy-rule)# exit
hostname(config)#
```

第二步：配置 NAT64。

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# snatrule from 2005::2009 to 64:ff9b:: /96 trans-to eif-ip mode dynamicport
rule ID=1
hostname(config-vrouter)# dnatrule from 2005::2009 to 64:ff9b:: /96 v4-mapped
rule ID=1
hostname(config-vrouter)# exit
hostname(config)#
```

附表：ICMPv6 Type 以及 Code 值对照表

ICMPv6 Type	ICMPv6 Code	Reference
1 Destination Unreachable	0 - no route to destination	[RFC4443]
	1 - communication with destination administratively prohibited	[RFC4443]
	2 - beyond scope of source address	[RFC4443]
	3 - address unreachable	[RFC4443]
	4 - port unreachable	[RFC4443]

ICMPv6 Type	ICMPv6 Code	Reference
	5 - source address failed ingress/egress policy	[RFC4443]
	6 - reject route to destination	[RFC4443]
2 Packet Too Big	0	[RFC4443]
3 Time Exceeded	0 - hop limit exceeded in transit	[RFC4443]
	1 - fragment reassembly time exceeded	[RFC4443]
4 Parameter Problem	0 - erroneous header field encountered	[RFC4443]
	1 - unrecognized Next Header type encountered	[RFC4443]
	2 - unrecognized IPv6 option encountered	[RFC4443]
100 Private experimentation	-	[RFC4443]
101 Private experimentation	-	[RFC4443]
102-126 Unassigned	-	[RFC4443]
127 Reserved for expansion of ICMPv6 error messages	-	[RFC4443]
128 Echo Request	0	[RFC4443]
129 Echo Reply	0	[RFC4443]
130 Multicast Listener Query	0	[RFC2710]
131 Multicast Listener Report	0	[RFC2710]
132 Multicast Listener Done	0	[RFC2710]
133 Router Solicitation	0	[RFC4861]
134 Router Advertisement	0	[RFC4861]
135 Neighbor Solicitation	0	[RFC4861]
136 Neighbor Advertisement	0	[RFC4861]
137 Redirect Message	0	[RFC4861]
138 Router Renumbering	0 - Router Renumbering Command	[Crawford] [RFC2894]
	1 - Router Renumbering Result	[Crawford] [RFC2894]
	255 - Sequence Number Reset	[Crawford] [RFC2894]
139 ICMP Node Information Query	0 - The Data field contains an IPv6 address which is the Subject of this Query	[RFC4620]
	1 - The Data field contains a name which is the Subject of this Query, or is empty, as in the case of a NOOP.	[RFC4620]

ICMPv6 Type	ICMPv6 Code	Reference
	2 - The Data field contains an IPv4 address which is the Subject of this Query.	[RFC4620]
140 ICMP Node Information Response	0 - A successful reply. The Reply Data field may or may not be empty.	[RFC4620]
	1 - The Responder refuses to supply the answer. The Reply Data field will be empty.	[RFC4620]
	2 - The Qtype of the Query is unknown to the Responder. The Reply Data field will be empty.	[RFC4620]
141 Inverse Neighbor Discovery Solicitation Message	0	[RFC3122]
142 Inverse Neighbor Discovery Advertisement Message	0	[RFC3122]
143 Version 2 Multicast Listener Report	-	[RFC3810]
144 Home Agent Address Discovery Request Message	0	[RFC3775]
145 Home Agent Address Discovery Reply Message	0	[RFC3775]
146 Mobile Prefix Solicitation	0	[RFC3775]
147 Mobile Prefix Advertisement	0	[RFC3775]
148 Certification Path Solicitation Message	-	[RFC3971]
149 Certification Path Advertisement Message	-	[RFC3971]
150 ICMP messages utilized by experimental mobility protocols such as Seamoby	-	[RFC4065]
151 Multicast Router Advertisement	-	[RFC4286]
152 Multicast Router Solicitation	-	[RFC4286]
153 Multicast Router Termination	-	[RFC4286]
154 FMIPv6 Messages	-	[RFC5268]
200 Private experimentation	-	[RFC4443]

ICMPv6 Type	ICMPv6 Code	Reference
201 Private experimentation	-	[RFC4443]
255 Reserved for expansion of ICMPv6 informational messages	-	[RFC4443]

第 7 章 VPN

本章节包含以下内容:

IPSec 协议：主要介绍 IPSec 协议、IPSec VPN 的应用、配置 IPSecVPN 以及相关的配置举例。

SSL VPN：主要介绍了 SSL VPN 的概念、设备端的配置以及各种客户端的配置和配置举例。

IPSec 协议

IPSec 协议介绍

IPSec 是为实现VPN 功能而最普遍使用的协议。IPSec 不是一个单独的协议，它给出了应用于 IP 层上网络数据安全的一整套体系结构。该体系结构包括认证头协议（Authentication Header，简称为 AH）、封装安全负载协议（Encapsulating Security Payload，简称为 ESP）、密钥管理协议（Internet Key Exchange，简称为 IKE）和用于网络认证及加密的一些算法等。IPSec 规定了如何在对等体之间选择安全协议、确定安全算法和密钥交换，向上提供了访问控制、数据源认证、数据加密等网络安全服务。

- 认证头协议（AH）：IPsec 体系结构中的一种主要协议，它为 IP 数据包提供无连接完整性的保护与数据源认证，并提供保护以避免重播情况。AH 尽可能为 IP 头和上层协议数据提供足够多的认证。
- IPsec 封装安全负载（ESP）：IPsec 体系结构中的一种主要协议。ESP 加密需要保护的数据并且在 IPsec ESP 的数据部分进行数据的完整性校验，以此来保证机密性和完整性。ESP 提供了与AH 相同的安全服务并提供了一种保密性（加密）服务，ESP 与 AH 各自提供的认证根本区别在于它们的覆盖范围。
- 密钥管理协议（IKE）：用于协商 AH 和 ESP 所使用的密码算法，并将算法所需的必备密钥放到恰当位置。

注意:IPSec VPN 支持使用国家商用密码算法配置。详细的国密算法标准，请参阅国家密码管理局颁发的《IPSec VPN 技术规范》。

安全联盟（Security Association）

IPSec 在两个端点之间提供安全通信，两个端点被称为 IPSec ISAKMP 网关。安全联盟（简称为 SA）是 IPSec 的基础，也是IPSec 的本质。SA 是通信对等体间对某些要素的约定，例如使用哪种协议、协议的操作模式、加密算法（DES、3DES、AES-128、AES-192 和 AES-256）、特定流中保护数据的共享密钥以及 SA 的生存周期等。

安全联盟是单向的，在两个对等体之间的双向通信，最少需要两个安全联盟来分别对两个方向的数据流进行安全保护。

SA 建立方式

建立安全联盟的方式有两种，一种是手工方式（Manual），一种是 IKE 自动协商（ISAKMP）方式。

手工方式配置比较复杂，创建安全联盟所需的全部信息都必须手工配置，而且 IPSec 的一些高级特性（例如定时更新密钥）不能被支持，但优点是可以不依赖 IKE 而单独实现 IPSec 功能。该方式适用于当与之进行通信的对等体设备数量较少的情况，或是 IP 地址相对固定的环境中。

IKE 自动协商方式相对比较简单，只需要配置好 IKE 协商安全策略的信息，由 IKE 自动协商来创建和维护安全联盟。该方式适用于中、大型的动态网络环境中。该方式建立 SA 的过程分两个阶段。第一阶段，协商创建一个通信信道（ISAKMP SA），并对该信道进行认证，为双方进一步的 IKE 通信提供机密性、数据完整性以及数据源认证服务；第二阶段，使用已建立的 ISAKMP SA 建立 IPsec SA。分两个阶段来完成这些服务有助于提高密钥交换的速度。

第一阶段 SA

第一阶段 SA 为建立信道而进行的安全联盟。第一阶段协商的步骤是：

1. 参数配置。包括：
    - 认证方法：选择预共享密钥或数字证书认证
    - Diffie-Hellman 组的选择
2. 策略协商。包括：
    - 加密算法：选择 DES、3DES、AES-128、AES-192 或 AES-256
    - hash 算法：选择 MD5、SHA-1 或 SHA-2
3. DH 交换。虽然名为“密钥交换”，但事实上在任何时候，两台通信主机之间都不会交换真正的密钥，它们之间交换的只是一些DH 算法生成共享密钥所需要的基本材料信息。DH 交换，可以是公开的，也可以受保护。在彼此交换过密钥生成“材料”后，两端主机可以各自生成出完全一样的共享“主密钥”，保护紧接其后的认证过程。
4. 认证 。DH 交换需要得到进一步认证，如果认证不成功，通信将无法继续下去。“主密钥”结合在第一步中确定的协商算法，对通信实体和通信信道进行认证。在这一步中，整个待认证的实体载 荷，包括实体类型、端口号和协议，均由前一步生成的“主密钥”提供机密性和完整性保证。

第二阶段 SA

第二阶段 SA 为快速 SA，为数据传输而建立的安全联盟。这一阶段协商建立 IPsec SA，为数据交换提供 IPSec 服务。第二阶段协商消息受第一阶段 SA 保护，任何没有第一阶段 SA 保护的消息将被拒收。第二阶段协商（快速模式协商）步骤是：

1. 策略协商，双方交换保护需求：
    - 使用哪种 IPSec 协议：AH 或 ESP
    - 是否使用 hash 算法：MD5、SHA-1、SHA-2 或 NULL
    - 是否要求加密，若是，选择加密算法：DES 或 3DES、AES-128、NULL、AES-192 或 AES-256
    - 是否使用压缩算法：DEFLATE

- 在上述四方面达成一致后，将建立起两个 SA，分别用于入站和出站通信。

2. 会话密钥“材料”刷新或交换。
   在这一步中，将通过 DH 交换生成加密 IP 数据包的“会话密钥”。

3. 将 SA 递交给 IPSec 驱动程序。
   在第二阶段协商过程中，如果响应超时，则自动尝试重新进行第二阶段 SA 协商。

验证算法

AH 和ESP 都能够对 IP 报文的完整性进行验证，以判别报文在传输过程中是否被篡改。验证算法的实现主要是通过杂凑函数。杂凑函数是一种能够接受任意长的消息输入，并产生固定长度输出的算法，该输出称为消息摘要。IPSec 对等体计算摘要，如果两个摘要是相同的，则表示报文是完整未经篡改的。一般来说 IPSec 使用下列验证算法：

- MD5：MD5 输入任意长度的消息，产生 128bit 的消息摘要。
- SHA-1：SHA-1 输入长度小于 2 的 64 次方比特的消息，产生 160bit 的消息摘要。SHA-1 的摘要长于 MD5，因而是更安全的。
- SHA-2：SHA-2 一般包含 SHA-256、SHA-384 和 SHA-512 三种杂凑函数，能将输入消息对应到更长的消息摘要。SHA-256 输入长度小于 2 的 64 次方比特的消息，产生 256bit 的消息摘要；SHA-384 输入长度小于 2 的 128 次方比特的消息，产生 384bit 的消息摘要；SHA-512 输入长度小于 2 的 128 次方比特的消息，产生 512bit 的消息摘要。
- SM3：SM3 输入长度小于 2 的 64 次方比特的消息，产生 256bit 的消息摘要。

加密算法

ESP 能够对 IP 报文内容进行加密保护，防止报文内容在传输过程中被窥探。加密算法实现主要通过对称密钥系统，它使用相同的密钥对数据进行加密和解密。StoneOS 实现了三种加密算法：

- DES（Data Encryption Standard）：使用 56bit 的密钥对每个 64bit 的明文块进行加密。
- 3DES（Triple DES）：使用三个 56bit 的 DES 密钥（共 168bit 密钥）对明文进行加密。
- AES（Advanced Encryption Standard）：StoneOS 实现了 128bit、192bit 和 256bit 密钥长度的 AES 算法。
- SM1: 国家密码管理局编制的一种商用密码分组标准对称算法。分组长度和密钥长度都为 128bit。仅国密设备支持该算法。
- SM4: 国家密码管理局编制的一种商用密码分组标准对称算法。分组长度和密钥长度都为 128bit。

压缩算法

IPComp（IP Payload Compression，IP 有效载荷压缩）是一个减少 IP 数据报长度的协议，该协议通过支持不同的压缩算法对 IP 数据报的有效负载进行压缩处理，从而实现通信数据在低带宽条件下的高负载传输。

应用 IPComp 的关键在于通信的两个端点之间必须首先建立一个 IPComp 关联（IPCA），此关联中包含了 IPComp 操作要求的所有信息，例如所使用的压缩算法以及所选择的压缩算法要求的参数等。使用 IPComp 对 IPSec 处理的网络数据流进行压缩时，用户可以手工配置创建 IPCA，也可以通过动态协商创建 IPCA。当使用动态协商方式时，ISAKMP 网关提供建立IPCA 必须的机制。 设备的 IPSec 功能提供以下 IPComp 压缩算法：

- DEFLATE：使用 LZ77 算法和 Huffman 译码，是一种可以在 IPComp 中实现的自由可用的无损耗压缩算法。

相关资料

StoneOS 的 IPSec 功能遵循 RFC 中 IPSec 协议的规定。关于IPSec 协议的更多详细信息，请参阅以下 RFC 文档的相关章节：

- Security Architecture for the Internet Protocol: RFC2401/RFC4301
- ESP：RFC2406/RFC4303
- AH：RFC2402/RFC4302
- 加密算法参考：RFC2410（Null Encryption），RFC2405（DES-CBC），RFC2451（3DES-CBC）以及 RFC3602（AES-CBC）
- 验证算法参考：：FIPS180-2（SHA），RFC2404（SHA-1），RFC4868（SHA-2）以及 RFC2403（MD5）
- 压缩算法参考：RFC2393（IPComp）以及 RFC2394（DEFLATE）

IPSec VPN 的应用

StoneOS 通过“基于策略的 VPN”和“基于路由的VPN”两种方式把配置好的 VPN 隧道应用到设备上，实现流量的加密解密安全传输。

- 基于策略的 VPN：将配置成功的 VPN 隧道名称引用到策略规则中，使符合条件的流量通过指定的 VPN 隧道进行传输。
- 基于路由的 VPN：将配置成功的 VPN 隧道与隧道接口绑定；配置静态路由时，将隧道接口指定为下一跳路由。

配置 IPSec VPN 功能

StoneOS 支持两种配置 IPSec VPN 的方法，分别是：

- 手工密钥VPN
- IKE VPN，支持 IKEv1 和 IKEv2 两个版本。

提升 IPSec VPN 解密性能

当使用的 CPU 数大于 2 个 vCPU 以上时，用户可以根据需要开启 IPSec VPN 解密性能提升功能。开启后，系统将采用多核解密技术对数据包进行解密，IPSec VPN 解密性能将提升，同时设备的吞吐量也将增大。开启 IPSec VPN 解密性能提升功能，在全局配置模式下使用以下命令：

tunnel-core-unbind

在全局配置模式下，使用 **no tunnel-core-unbind** 恢复默认配置。

手工密钥 VPN

手工密钥VPN 的配置包括指定 IPSec 协议的操作模式、安全参数索引、协议类型、加密算法/验证算法和压缩算法等。

创建手工密钥 VPN

创建手工密钥VPN，在全局配置模式下，使用以下命令：

tunnel ipsec *name* **manual**

- *name* – 指定所创建的手工密钥 VPN 隧道的名称。

执行该命令后，CLI 进入到手工密钥 VPN 配置模式。对手工密钥VPN 的所有参数配置都需要在该模式下进行。在全局配置模式下使用以下命令删除指定的手工密钥VPN 隧道：

no tunnel ipsec *name* **manual**

指定 IPSec 协议的操作模式

指定 IPSec 协议的操作模式，可以是隧道模式或者传输模式，在手工密钥 VPN 配置模式下使用以下命令：

mode {**transport** | **tunnel**}

- **transport** – 指定 IPSec 协议的操作模式为传输模式。
- **tunnel** – 指定 IPSec 协议的操作模式为隧道模式。该模式为系统默认模式。

使用 no mode 命令恢复默认模式。

指定安全参数索引

安全参数索引（Security Parameter Index，简称为 SPI）是为唯一标识 SA 而生成的一个 32 比特的数值，它在 AH 和 ESP 头中传输。SPI 的作用是查找对应的 VPN 隧道进行解密。指定手工密钥 VPN 隧道的 SPI，在手工密钥 VPN 配置模式下使用以下命令：

spi *spi-number out-spi-number*

- *spi-number* – 指定本端的 SPI 参数。
- *out-spi-number* – 指定对端的 SPI 参数。

使用 no spi 命令取消对 SPI 参数的配置。

在为系统配置安全联盟时，必须分别设置进方向（inbound）和出方向（outbound）两个方向的安全联盟的参数。并且在隧道的两端设置的安全联盟参数必须是完全匹配的。本端的入方向安全联盟的 SPI 必须和对端的出方向安全联盟的 SPI 一样；本端的出方向安全联盟的 SPI 必须和对端的入方向安全联盟的 SPI 一样。

指定协议类型

IPSec 协议的类型为ESP 和 AH 两种。为手工密钥VPN 隧道指定协议类型，在手工密钥 VPN 配置模式下使用以下命令：

protocol {esp | ah}

- esp – 指定使用ESP 协议。该协议为系统默认协议。
- ah – 指定使用 AH 协议。

使用 no protocol 恢复默认协议配置。

指定加密算法

为手工密钥 VPN 隧道指定加密算法，请在手工密钥VPN 配置模式下使用以下命令：

encryption {3des | des | aes | aes-192 | aes-256 | null}

- 3des – 指定使用 3DES 加密方法。密钥长度为 192 比特。该方法为系统默认方法。
- des – 指定使用 DES 加密方法。密钥长度为 64 比特。
- aes – 指定使用 AES 加密方法。密钥长度为 128 比特。
- aes-192 – 指定使用 192bit AES 加密方法。密钥长度为 192 比特。

- **aes-256** – 指定使用 256bit AES 加密方法。密钥长度为 256 比特。
- **null** – 不使用加密功能。

使用 **no encryption** 命令恢复默认加密算法。

指定验证算法

为手工密钥 VPN 隧道指定验证算法，请在手工密钥VPN 配置模式下使用以下命令：

hash {**md5** | **sha** | **sha256** | **sha384** | **sha512** | **null**}

- **md5** – 指定使用 MD5 验证算法。摘要为 128 比特。
- **sha** – 指定使用 SHA-1 验证算法。摘要为 160 比特。该算法为 StoneOS 的默认算法。
- **sha256** – 指定使用 SHA-256 验证算法。摘要为 256 比特。
- **sha384** – 指定使用 SHA-384 验证算法。摘要为 384 比特。
- **sha512** – 指定使用 SHA-512 验证算法。摘要为 512 比特。
- **null** – 不使用验证功能。

使用 **no hash** 命令恢复默认验证算法。

指定压缩算法

默认情况下，手工密钥 VPN 不使用任何压缩算法。为手工密钥 VPN 隧道指定压缩算法（DEFLATE 算法），请在手工密钥 VPN 配置模式下使用以下命令：

compression deflate

使用 **no compression** 命令取消对压缩算法的指定。

指定对端 IP 地址

配置对端的 IP 地址，请在手工密钥VPN 配置模式下使用以下命令：

peer *ip-address*

- *ip-address* – 指定对端的 IP 地址。使

用 **no peer** 命令取消对端 IP 地址的配置。

配置协议的验证密钥

用户需要为安全隧道两端均配置协议的验证密钥，且本端入方向验证密钥必须与对端出方向的验证密钥相同，而本端出方向的验证密钥必须与对端入方向的验证密钥相同。配置协议验证密钥，请在手工密钥 VPN 配置模式下使用以下命令：

hash-key inbound *hex-number-string* **outbound** *hex-number-string*

- **inbound** *hex-number-string* – 配置本端进方向的验证密钥。
- **outbound** *hex-number-string* – 配置本端出方向的验证密钥。

使用 **no hash-key** 命令取消对验证密钥的配置。

配置协议的加密密钥

用户需要为安全隧道两端均配置协议的加密密钥，且本端入方向加密密钥必须与对端出方向的加密密钥相同，而本端出方向的加密密钥必须与对端入方向的加密密钥相同。配置协议加密密钥，请在手工密钥 VPN 配置模式下使用以下命令：

encryption-key inbound *hex-number-string* **outbound** *hex-number-string*

- **inbound** *hex-number-string* – 配置本端进方向的加密密钥。
- **outbound** *hex-number-string* – 配置本端出方向的加密密钥。

使用 **no encryption-key** 命令取消对加密密钥的配置。

指定出接口

为手工密钥 VPN 隧道指定出接口，请在手工密钥 VPN 配置模式下使用以下命令：

- **interface** *interface-name*
- **interface-name** – 指定出接口名称。

使用 **no interface** 命令取消对出接口的指定。

注意:非根 VSYS 中的出接口不可以为 VSYS 共享接口。

IKEv1 VPN

IKEv1 VPN 的配置包括：

- 配置 P1 提议
- 配置 ISAKMP 网关

- 配置P2提议
- 配置隧道

配置 P1 提议

P1 提议是 IKE 安全提议，可应用到 ISAKMP 网关上，在 SA 第一阶段使用。对 IKE 安全提议的配置包括指定认证方式、加密算法、验证算法、DH 组和安全联盟的生命周期。

创建 P1 提议

创建一个P1 提议，即 IKE 安全提议，请在全局配置模式下使用以下命令：

isakmp proposal *p1-name*

- *p1-name* – 指定所创建的P1 提议的名称。执行该命令后，CLI 进入到 P1 提议配置模式。用户可以在该模式下对P1 提议进行参数配置。

使用 **no isakmp proposal** *p1-name* 命令删除指定的P1 提议。

指定认证方式

此处指定的是 IKE 身份认证的方式。身份认证用来确认通信双方的身份。方式有预共享密钥认证、数字证书认证和国密数据信封认证。对于预共享密钥认证方式，认证字用来作为一个输入产生密钥，认证字不同是不可能在双方产生相同的密钥的。指定 IKE 安全提议的身份认证方式，在 P1 提议配置模式下使用以下命令：

authentication {**pre-share** | **rsa-sig** | **dsa-sig** | **gm-de** }

- **pre-share** – 指定使用预共享密钥认证方式。该方式为默认认证方式。
- **rsa-sig** – 指定使用 RSA 数字证书认证方式。
- **dsa-sig** – 指定使用 DSA 数字证书认证方式。此方式对应的验证算法只能为SHA-1。
- **gm-de** – 指定使用国密数据信封认证方式。当认证方式为此选项时，加密算法仅支持使用 SM1 和 SM4，验证算法仅支持使用 SHA 或 SM3。

使用 **no authentication** 命令恢复默认认证方式。

指定加密算法

指定 IKE 安全提议的加密算法，在P1 提议配置模式下使用以下命令：

encryption {3des | des | aes | aes-192 | aes-256 | sm1 | sm4}

- **3des** – 指定使用 3DES 加密方法。密钥长度为 192 比特。该方法为 StoneOS 系统默认方法。
- **des** – 指定使用 DES 加密方法。密钥长度为 64 比特。
- **aes** – 指定使用 AES 加密方法。密钥长度为 128 比特。
- **aes-192** – 指定使用 192bit AES 加密方法。密钥长度为 192 比特。
- **aes-256** – 指定使用 256bit AES 加密方法。密钥长度为 256 比特。
- **sm1** – 指定使用国家商用密码 SM1 分组密码算法。密钥长度为 128 比特。
- **sm4** – 指定使用国家商用密码 SM4 分组密码算法。密钥长度为 128 比特。

使用 **no encryption** 命令恢复默认加密算法。

指定验证算法

指定 IKE 安全提议的验证算法，在P1 提议模式下使用以下命令:

hash {**md5** | **sha** | **sha256** | **sha384** | **sha512** | **sm3**}

- **md5** – 指定使用 MD5 验证算法。摘要为 128 比特。
- **sha** – 指定使用 SHA-1 验证算法。摘要为 160 比特。该算法为 StoneOS 的默认算法。
- **sha256** – 指定使用 SHA-256 验证算法。摘要为 256 比特。
- **sha384** – 指定使用 SHA-384 验证算法。摘要为 384 比特。
- **sha512** – 指定使用 SHA-512 验证算法。摘要为 512 比特。
- **sm3** – 指定使用国密 SM3 验证算法。摘要为 256 比特。该算法用于密码应用中的数字签名和验证、消息认证码的生成与验证，可满足多种密码应用的安全需求。

使用 **no hash** 命令恢复默认认证方式。

选择 DH 组

Diffie-Hellman（DH）是一种建立密钥的方法。DH 组决定 DH 交换中密钥生成“材料”的长度。密钥的牢固性部分决定于DH 组的强度。密钥“材料”长度越长，所生成的密钥安全度也就越高，越难被破译。

DH 组的选择很重要，因为 DH 组只在第一阶段的 SA 协商中确定，第二阶段的协商不再重新选择 DH 组，两个阶段使用的是同一个DH 组，因此该 DH 组的选择将影响所有会话密钥的生成。在协商过程中，

两个 ISAKMP 网关间应选择同一个DH 组，即密钥“材料”长度应该相等。若 DH 组不匹配，将协商失败。

在 P1 提议选择 DH 组，在 P1 提议配置模式下使用以下命令：

group {1 | 2 | 5 | 14 | 15 |16 | 19 | 20 | 21 | 24}

- **1** – 选择 DH 组 1。密钥的长度为 768 比特（MODP Group）。
- **2** – 选择 DH 组 2。密钥的长度为 1024 比特（MODP Group）。2 为系统默认值。
- **5** – 选择 DH 组 5。密钥的长度为 1536 比特（MODP Group）。
- **14** – 选择 DH 组 14。密钥的长度为 2048 比特（MODP Group）。
- **15** – 选择 DH 组 15。密钥的长度为 3072 比特（MODP Group）。
- **16** – 选择 DH 组 16。密钥的长度为 4096 比特（MODP Group）。
- **19** – 选择 DH 组 19。密钥的长度为 256 比特（ECP Group）。
- **20** – 选择 DH 组 20。密钥的长度为 384 比特（ECP Group）。
- **21** – 选择 DH 组 21。密钥的长度为 521 比特（ECP Group）。
- **24** – 选择 DH 组 24。密钥的长度为 2048 比特（MODP Group with 256-bit Prime Order Subgroup）。

使用 **no group** 命令取消恢复默认 DH 组。

在 P2 提议中配置PFS 时，也可选用如上DH 组。

指定安全联盟的生命周期

第一阶段 SA 有一个默认的生命周期，如果 ISAKMP SA 生命期时间到，要向对方发送第一阶段 SA 删除消息，通知对方第一阶段 SA 已经过期。之后需要重新进行 SA 协商。指定安全联盟的生命周期，在P1 提议配置模式下使用以下命令：

lifetime *time-value*

- *time-value* – 指定 SA 第一阶段的生命周期长度，单位为秒。默认 86400 秒。范围是 300 到 86400 秒。

使用 **no lifetime** 命令恢复默认生命周期长度。

配置 ISAKMP 网关

创建一个 ISAKMP 网关后，用户可以配置 ISAKMP 网关的 IKE 协商模式、ISAKMP 网关 IP 地址及类型、IKE 安全提议、预共享密钥、PKI 信任域、本地 ID、ISAKMP 网关 ID 、ISAKMP 网关连接方式以及是否开启 ISAKMP 网关的 NAT 穿越功能等。

创建 ISAKMP 网关

创建 ISAKMP 网关，在全局配置模式下，使用以下命令:

isakmp peer *peer-name*

- *peer-name* – 指定 ISAKMP 网关的名称。

执行该命令后，CLI 进入到 ISAKMP 网关配置模式。用户可以在该模式下对ISAKMP 网关进行参数配置。

在全局配置模式下使用 **no isakmp peer** *peer-name* 命令删除指定的 ISAKMP 网关。

绑定接口到 ISAKMP 网关

用户可以绑定某个接口到 ISAKMP 网关。将接口绑定到 ISAKMP 网关，在 ISAKMP 网关配置模式下使用以下命令:

interface *interface-name*

- *interface-name* – 指定被绑定接口的名称。使

用 **no interface** *interface-name* 命令取消接口绑定。

配置 IKE 协商模式

IKE 的协商模式有两种：主模式（main mode）和野蛮模式（aggressive mode）。IKE 野蛮模式不提供身份保护，以下情况只能用野蛮模式：中心设备的 IP 地址为固定分配的地址，而客户端设备的 IP 地址为动态获取的地址。配置 IKE 协商模式，在 ISAKMP 网关配置模式下使用以下命令:

mode {**main** | **aggressive**}

- **main** – 指定使用主模式，可提供 ID 保护功能。该模式为系统的默认模式。
- **aggressive** – 指定使用野蛮模式。

使用 **no mode** 命令恢复默认协商模式。

配置自定义 IKE 协商端口

用户可以自定义 UDP 端口进行 IKE 协商，并且建立 IPSec 连接。配置自定义 IKE 协商端口，在 ISAKMP 网关配置模式下使用以下命令：

ipsec-over-udp port *port-number*

- *port-number* – 指定UDP 端口号。取值范围是 1 到 65535。

使用 **no ipsec-over-udp** 命令取消自定义的 UDP 端口配置。

指定对端的 IP 地址及类型

用户可以为所创建的 ISAKMP 网关指定对端的 IP 地址和 IP 地址的类型（静态或者动态）。指定对端的 IP 地址，请在ISAKMP 网关配置模式下使用以下命令：

type {**dynamic** | **static**}

- **dynamic** – 指定对端的 IP 地址为动态 IP 地址。
- **static** – 指定对端的 IP 地址为静态 IP 地址。该选项为系统的默认选项。

使用 **no type** 命令恢复对端 IP 地址的默认类型。

peer *ip-address*

- *ip-address* - 指定对端的 IP 地址或主机名称。该 IP 地址只有当对端的 IP 地址类型是静态的时候才有效。

使用 **no peer** 命令取消对端 IP 地址或主机名称的指定。

接受对端 ID

使所创建的 ISAKMP 网关接受任意的对端 ID，不对对端进行 ID 检查，在 ISAKMP 网关配置模式下使用以下命令：

accept-all-peer-id

使用 **no accept-all-peer-id** 关闭该功能。

指定 P1 提议

为 ISAKMP 网关指定P1 提议，在 ISAKMP 网关配置模式下使用以下命令：

isakmp-proposal p1-proposal1 [p1-proposal2] [p1-proposal3] [p1-proposal4]

- p1-proposal1 – 指定 P1 提议的名称。用户最多可以为 ISAKMP 网关指定 4 个 P1 提议供对端选择使用。

使用 no isakmp-proposal 取消对P1 提议的指定。

配置预共享密钥

如果使用预共享密钥认证方式，用户就需要指定预共享密钥。为 ISAKMP 网关指定预共享密钥，在 ISAKMP 网关配置模式下使用以下命令：

pre-share *string*

- *string* – 指定预共享密钥的内容。

使用 no pre-share 取消对预共享密钥的指定。

配置 PKI 信任域

如果使用数字证书认证方式，用户就需要指定数字证书的 PKI 信任域。为 ISAKMP 网关指定PKI 信任域，在 ISAKMP 网关配置模式下使用以下命令：

trust-domain *string*

- *string* – 指定PKI 信任域。

使用 no trust-domain 取消对 PKI 信任域的指定。

> {b}提示: {/b}关于如何配置 PKI 信任域，请参阅《用户认证》的“PKI 配置”部分。

配置对端证书的信任域

对端证书一般用于协商中数据加密以及认证，需由发起VPN 连接的一端先导入对端证书。该命令仅适用于国密 1.0 版本。配置对端证书所在的信任域，请在 ISAKMP 网关配置模式下使用以下命令：

remote-trust-domain *string*

- *string* – 指定对端证书所在的信任域。

使用 no remote-trust-domain 命令删除对端证书的信任域配置。

配置加密证书的信任域

加密证书一般用于协商中数据加密。该命令仅适用于国密 1.1 版本，需为系统指定双证书。配置加密证书所在的信任域，请在 ISAKMP 网关配置模式下使用以下命令：

trust-domain-enc *string*

- string – 指定加密证书所在的信任域。

使用 **no trust-domain-enc** 命令删除加密证书的信任域配置。

配置协商协议标准

协商协议标准分为国际标准 IKEv1 和国密标准。默认情况下，系统使用国际标准 IKEv1 为协商协议标准。指定协商协议的标准，请在 ISAKMP 网关配置模式下使用以下命令：

protocol-standard {**ikev1** | **guomi**[**v1.0** | **v1.1**]}

- **ikev1** – 指定使用国际标准 IKEv1 为协商协议标准。
- **guomi**[**v1.0** | **v1.1**] – 指定使用国密标准为协商协议标准。v1.0 为国密 1.0 版本；v1.1 为国密 1.1 版本。如指定版本号 v1.0 或 v1.1，进行协商的两端设备必须是相同的版本号才能协商成功，否则协商失败。如不指定版本号，那么发起端国密协议版本号为国密 v1.0 或 v1.1 都可协商。

使用 **no protocol-standard** 命令取消协商协议标准的配置。

配置本端 ID

配置本端的 ID，请在 ISAKMP 网关配置模式下使用以下命令：

local-id {**fqdn** *string* | **asn1dn** [*string*] | **u-fqdn** *string* | **key-id** *string* |**ip** *ip-address* }

- **fqdn** *string* – 指定使用FQDN 类型的 ID。string 为 ID 的具体内容。
- **asn1dn** [*string*] – 指定使用 Asn1dn 类型的 ID，该类型只可应用于使用证书的情况。string 为 ID 的具体内容。用户可以不指定 ID 的具体内容，在此种情况下，系统将从证书中获取 ID。
- **u-fqdn** *string* – 指定使用U-FQDN 类型的 ID，即电子邮件地址类型，例如 user1@ net.com。
- **key-id** *string*- 指定使用 Key ID 类型的 ID。该类型仅应用于 XAUTH 功能。
- **ip** *ip-address* - 指定使用 IP 地址类型的 ID。ip-address 为 ID 的具体内容。

使用 no local-id 命令取消对本端 ID 的配置。

配置对端 ID

配置对端的 ID，请在 ISAKMP 网关配置模式下使用以下命令：

peer-id {**fqdn** | **asn1dn** | **u-fqdn** | **key-id** | **ip** } *string*

- **fqdn** – 指定使用FQDN 类型的 ID。string 为 ID 的具体内容。
- **asn1dn** – 指定使用Asn1dn 类型的 ID，该类型只可应用于使用证书的情况。string 为 ID 的具体内容。
- **u-fqdn string** – 指定使用U-FQDN 类型的 ID，即电子邮件地址类型，例如 user1@ net.com。
- **key-id** - 指定使用 Key ID 类型的 ID。该类型仅应用于 XAUTH 功能。
- **ip** - 指定使用 IP 地址类型的 ID。

使用 **no peer-id** 命令取消对对端 ID 的配置。

指定连接类型

创建的 ISAKMP 网关可以是发起端、响应端或者既是发起端也是响应端。指定 ISAKMP 网关的连接类型，在 ISAKMP 网关配置模式下使用以下命令：

connection-type {**bidirectional** | **initiator-only** | **responder-only**}

- **bidirectional** – 指定该 ISAKMP 网关既是发起端也是响应端。该选项为系统的默认选项。
- **initiator-only** – 指定该 ISAKMP 网关仅是发起端。
- **responder-only** – 指定该 ISAKMP 网关仅是响应端。

使用 **no connection-type** 命令恢复默认连接方式。

开启 NAT 穿越功能

在 IPSec 或者 IKE 组建的VPN 隧道中，若存在NAT 网关设备，且NAT 网关设备对 VPN 数据进行了 NAT 转换，则必须开启 IPSec 或者 IKE 的 NAT 穿越功能。默认情况下，NAT 穿越功能是关闭的。开启 NAT 穿越功能，在 ISAKMP 网关配置模式下，使用以下命令：

nat-traversal

使用 **no nat-traversal** 命令关闭 NAT 穿越功能。

配置自动生成路由功能

对于 IKEv1 VPN，当指定对端的 IP 地址类型为 static 或 dynamic 时，配置自动生成路由功能后，每创建一个 IPSec SA，设备会将目的地址为对端的 local ID、下一跳为隧道接口的路由条目添加到自己的路由表。删除一个 IPSec SA 后，相应的路由条目也会被删除。

默认情况下，设备的自动生成路由功能是关闭的。开启此功能，请在 ISAKMP 配置模式下，使用以下命令：

generate-route

使用 **no generate-route** 命令关闭自动生成路由功能。

配置 DPD 功能

DPD（Dead Peer Detection）为安全隧道对端状态探测功能。该功能开启后，如果接收端长时间收不到对端的报文，便触发 DPD 查询，主动向对端发送请求报文，对 ISAKMP 网关是否存在进行检测。默认情况下，DPD 功能是关闭的。配置 DPD 功能，在 ISAKMP 网关配置模式下使用以下命令：

dpd [**interval** *seconds*] [**retry** *times*]

- **interval seconds** – 指定向对端发送查询请求的时间间隔。间隔范围是 0 到 10 秒。默认值是 0，表示不开启 DPD 功能。
- **retry times** – 指定向对端发送查询请求的次数。向对端发送查询请求后，如果本端在指定的时间间隔内收不到对端的报文，系统会在再次发送查询请求，如此反复，直到完成该参数指定的次数。在指定次数查询完成后如果仍然收不到对端的报文，则判断对端 ISAKMP 网关已经死掉。查询请求的次数范围是 1 到 20 次，默认是 3 次。

使用 **no dpd** 命令恢复默认的DPD 配置。

指定描述信息

为所配置的 ISAKMP 网关指定描述信息，请在 ISAKMP 网关配置模式下使用以下命令：

description *string*

- *string* – ISAKMP 网关的描述信息。

使用 **no description** 命令删除 ISAKMP 网关的描述信息。

配置 P2 提议

P2 提议使用在 SA 第二阶段。对 P2 提议的配置包括指定协议类型、加密算法、验证算法、压缩算法和生命周期。

创建 P2 提议

创建P2 提议，即IPSec 安全提议，请在全局配置模式下使用以下命令：

ipsec proposal *p2-name*

- *p2-name* – 指定所创建的P2 提议的名称。执行该命令后，CLI 进入到 P2 提议配置模式。对P2 提议各项参数的配置都要在该模式下进行。

使用 **no ipsec proposal** *p2-name* 命令删除指定的 IPSec proposal。

指定协议类型

P2 提议可使用的协议类型有 AH 以及 ESP。为 P2 提议指定协议类型，在 P2 提议配置模式下使用以下命令：

protocol {**esp** | **ah**}

- **esp** – 指定使用ESP 协议。该协议为系统默认协议。
- **ah** – 指定使用 AH 协议。

使用 **no protocol** 命令恢复默认协议配置。

指定加密算法

用户可以为 P2 提议指定至少一种最多四种加密算法。为P2 提议指定加密算法，在P2 提议配置模式下使用以下命令：

encryption {**3des** | **des** | **aes** | **aes-192** | **aes-256** | **sm1** | **sm4** | **null**} [**3des** | **des** | **aes** | **aes-192** | **aes-256** | **sm1** | **sm4** | **null**] [**3des** | **des** | **aes** | **aes-192** | **aes-256** | **sm1** | **sm4** | **null**]……

- **3des** – 指定使用 3DES 加密方法。密钥长度为 192 比特。该方法为 StoneOS 系统默认方法。
- **des** – 指定使用 DES 加密方法。密钥长度为 64 比特。
- **aes** – 指定使用 AES 加密方法。密钥长度为 128 比特。
- **aes-192** – 指定使用 192bit AES 加密方法。密钥长度为 192 比特。

- **aes-256** – 指定使用 256bit AES 加密方法。密钥长度为 256 比特。
- **sm1** – 指定使用国家商用密码 SM1 分组密码算法。密钥长度为 128 比特。
- **sm4** – 指定使用国家商用密码 SM4 分组密码算法。密钥长度为 128 比特。
- **null** – 不使用加密功能。

使用 **no encryption** 命令恢复默认加密算法。

指定验证算法

用户可以为 P2 提议指定至少一种最多三种验证算法。为P2 提议指定验证算法，在P2 提议配置模式下使用以下命令：

hash {**md5** | **sha** | **sha256** | **sha384** | **sha512** | **sm3** | **null**} [**md5** | **sha** | **sha256** | **sha384** | **sha512** | **sm3** | **null**] [**md5** | **sha** | **sha256** | **sha384** | **sha512** | **sm3** | **null**]

- **md5** – 指定使用 MD5 验证算法。摘要为 128 比特。
- **sha** – 指定使用 SHA-1 验证算法。摘要为 160 比特。该算法为 StoneOS 的默认算法。
- **sha256** – 指定使用 SHA-256 验证算法。摘要为 256 比特。
- **sha384** – 指定使用 SHA-384 验证算法。摘要为 384 比特。
- **sha512** – 指定使用 SHA-512 验证算法。摘要为 512 比特。
- **sm3** – 指定使用国密 SM3 验证算法。摘要为 256 比特。
- **null** – 不使用验证功能。

使用 **no hash** 命令恢复默认验证算法。

指定压缩算法

默认情况下，P2 提议不使用任何压缩算法。为 P2 提议指定压缩算法（DEFLATE 算法），请在P2 提议配置模式下使用以下命令：

compression deflate

使用 **no compression** 命令取消对压缩算法的指定。

配置 PFS 功能

PFS（Perfect Forward Security）功能决定新密钥的生成方式，而不是新密钥的生成时间。PFS 保证无论在哪一阶段，一个密钥只能使用一次，而且，生成密钥的“材料”也只能使用一次。某个“材料”在生成了一个密钥后就被弃，绝不用来再生成任何其它密钥。这样可以确保一旦单个密钥泄密，最多只可能影响用该密钥加密的数据，而不会危及整个通信。PFS 功能是由 DH 算法做保障的。配置P2 提议的PFS 功能，在 P2 提议配置模式下使用以下命令：

group {**nopfs** | **1** | **2** | **5** | **14** | **15** |**16**| **19** | **20** | **21** | **24**}

- **nopfs** – 不使用PFS 功能。该选项为系统的默认选项。
- **1** – 选择 DH 组 1。密钥的长度为 768 比特（MODP Group）。
- **2** – 选择 DH 组 2。密钥的长度为 1024 比特（MODP Group）。
- **5** – 选择 DH 组 5。密钥的长度为 1536 比特（MODP Group）。
- **14** – 选择 DH 组 14。密钥的长度为 2048 比特（MODP Group）。
- **15** – 选择 DH 组 15。密钥的长度为 3072 比特（MODP Group）。
- **16** – 选择 DH 组 16。密钥的长度为 4096 比特（MODP Group）。
- **19** – 选择 DH 组 19。密钥的长度为 256 比特（ECP Group）。
- **20** – 选择 DH 组 20。密钥的长度为 384 比特（ECP Group）。
- **21** – 选择 DH 组 21。密钥的长度为 521 比特（ECP Group）。
- **24** – 选择 DH 组 24。密钥的长度为 2048 比特（MODP Group with 256-bit Prime Order Subgroup）。

使用 **no group** 命令恢复默配置。

指定生命周期

设备有两种衡量生命周期的方法，分别是按时间和按流量。当 SA 的流量或者时间达到特定值时，SA 就会过期，需要重新进行协商。指定P2 提议的生命周期，在P2 提议配置模式，使用以下命令：

lifetime *seconds*

- *seconds* – 指定时间类型生命周期的时间长度，单位为秒。默认值是 28800 秒。

lifesize *kilobytes*

- *kilobytes* – 指定流量类型周期的流量值，单位为字节。默认值是 0，意义为没有周期流量限制。

使用以上两个命令 no 的形式恢复默认配置。即

no lifetime

no lifesize

配置隧道

通过 IKE 配置 IPSec 隧道，用户需要配置的选项有指定协议类型、ISAKMP 网关、IKE 安全提议、ID 号、是否分片以及防重放等。

创建 IKE 隧道

创建 IKE 隧道，在全局配置模式下，使用以下命令：

tunnel ipsec *tunnel-name* **auto**

- *tunnel-name* - 指定所创建的 IKE 隧道的名称。

执行该命令后，CLI 进入到 IKE 隧道配置模式。对 IKE 隧道的所有参数配置都需要在该模式下进行。

在全局配置模式下使用 **no tunnel ipsec** *tunnel-name* **auto** 删除指定的 IKE 隧道。

指定 IPSec 协议的操作模式

为 IKE 隧道指定操作模式，可以是隧道模式或者传输模式，在 IKE 隧道配置模式下使用以下命令：

mode {**transport** | **tunnel**}

- **transport** – 指定 IPSec 协议的操作模式为传输模式。
- **tunnel** – 指定 IPSec 协议的操作模式为隧道模式。该模式为系统默认模式。

使用 **no mode** 命令恢复默认模式。

指定 ISAKMP 网关

为 IKE 隧道指定 ISAKMP 网关，请在 IKE 隧道配置模式下使用以下命令：

isakmp-peer *peer-name*

- *peer-name* – 指定 ISAKMP 网关的名称。使

用 **no isakmp-peer** 取消对 ISAKMP 网关的指定。

指定 P2 提议

为 IKE 隧道指定 P2 提议，请在 IKE 隧道配置模式下使用以下命令：

ipsec-proposal *p2-name*

- *p2-name* – 指定 P2 提议的名称。

使用 **no ipsec-proposal** 取消对P2 提议的指定。

指定第二阶段 ID

为 IKE IPSec 隧道指定第二阶段 ID，请在 IKE 隧道配置模式下使用以下命令：

id {**auto** | **local** *ip-address/mask* **remote** *ip-address/mask* **service** *service-name*}

- **auto** – 自动指定第二阶段 ID。此参数为系统默认配置。
- **local** *ip-address/mask* – 指定本端第二阶段 local ID。
- **remote** *ip-address/mask* – 指定本端第二阶段 remote ID。
- **service** *service-name* – 指定服务名称。

用户可配置最多 64 个第二阶段 ID 用于协商建立多个 IKE 隧道。

使用 **no id** {**auto** | **local** *ip-address/mask* **remote** *ip-address/mask* **service** *service-name*} 命令恢复系统默认配置。

配置 IPsec VPN 流量分流与限流

流量分流功能根据第二阶段 ID 的配置，在 IKE 隧道入口对进入 IKE 隧道的流量进行分流。如果流量的源 IP 地址、目的 IP 地址、以及流量的类型(service)匹配某一个第二阶段 ID 的配置，则该流量进入相应的 IKE 隧道进行封装发送。如果没有匹配的第二阶段 ID，则该流量被丢弃。

流量限流功能根据第二阶段 ID 的配置，在 IKE 隧道出口对解封装后的流量进行限流。如果解封装后流量的源 IP 地址、目的 IP 地址、以及流量的类型(service)匹配某一个第二阶段 ID 的配置，则该流量被接收设备继续处理；如果流量无法匹配任何一个第二阶段 ID 的配置，则该流量被丢弃。

开启流量分流与限流功能，在 IKE 隧道配置模式，使用如下命令：

check-id

在 IKE 隧道配置模式下，使用该命令 no 的形式关闭流量分流与限流功能。

启用接受对端 ID 功能

默认情况下，该功能为禁用状态。开启该功能后，如果安全设备作为接收端，它将接受对端的 ID 为它的 IKE 协商第二阶段 ID，并返回该 ID 给对端。如果用户配置了多个第二阶段 ID，需要关闭此功能。在 IKE 隧道配置模式下，使用以下命令开启接受对端 ID 的功能：

accept-all-proxy-id

在 IKE 隧道配置模式下，使用该命令 no 的形式关闭接受对端 ID 功能：

no accept-all-proxy-id

配置自动连接功能

设备提供了两种触发建立 SA 的方式：自动方式和流量触发方式。

- 自动方式是指设备每 60 秒检查一次 SA 的状态，如果 SA 未建立则自动发起协商请求；
- 流量触发方式是指当有数据流量需要通过隧道进行传输时，该隧道才发起协商请求。

默认情况下，使用流量触发方式。欲使用自动方式，请在 IKE 隧道配置模式下使用以下命令：

auto-connect

使用 no auto-connect 命令恢复系统的默认设置。

注意:自动连接功能仅在对端 IP 地址为静态类型且本端可以作为发起端时有效。

配置分片功能

用户可以指定是否允许转发设备将包进行分片处理。为 IKE 隧道配置分片功能，请在 IKE 隧道配置模式下使用以下命令：

df-bit {copy | clear | set}

- copy – 直接从发包端拷贝 IP 包的 DF 选项。该选项为系统默认选项。
- clear – 允许转发设备对包做分片处理。
- set – 不允许转发设备对包做分片处理。

使用 no df-bit 恢复系统的默认设置。

配置防重放功能

防重放（anti-replay）指防止恶意用户通过重复发送捕获到的数据包所进行的攻击，即接收方会拒绝旧的或重复的数据包。默认情况下，防重放功能是关闭的。为 IKE IPSec 隧道配置防重放功能，请在 IKE IPSec 隧道配置模式下使用以下命令：

anti-replay {**32** | **64** | **128** | **256** | **512**}

- **32** – 指定防重放的窗口为 32。
- **64** – 指定防重放的窗口为 64。
- **128** – 指定防重放的窗口为 128。
- **256** – 指定防重放的窗口为 256。
- **512** – 指定防重放的窗口为 512。

在网络状况较差时，例如存在严重乱序现象等，请选择较大的窗口。

使用 **no anti-replay** 命令关闭防重放功能。

配置 VPN 监控及冗余备份功能

设备能够监测指定的 VPN 隧道是否连通，并且能够实现两条或者多条 VPN 隧道的备份或者分流。该功能仅对基于路由的VPN 以及基于策略的VPN 均有效。具体实现包括以下两种环境：

- 为同一个远程对端配置备份 VPN 隧道，并且在任意时刻只有一个隧道处于活动状态。最初，主 VPN 隧道处于活动状态，如果监测到该主隧道中断， 设备会通过备份隧道重新传输信息流；
- 为同一个远程对端配置了两个或者多个VPN 隧道，所有隧道都同时处于活动状态，并且通过等价多径路由（ECMP）实现负载均衡。如果监测到隧道中断， 设备会通过其它隧道重新传输信息流。

VPN 监控功能支持通过Ping 报文对目标隧道进行监测。默认情况下，该功能是关闭的。配置 VPN 监控功能，请在 IKE IPSec 隧道配置模式下使用以下命令：

vpn-track [*A.B.C.D*] [**src-ip** *A.B.C.D*] [**interval** *time-value*] [**threshold** *value*]

- *A.B.C.D* – 指定监测目标的 IP 地址。当对端设备为设备时，如果不指定该参数，系统默认为对端 IP 地址。此 IP 地址不能为“0.0.0.0”和“255.255.255.255”。
- **src-ip** *A.B.C.D* – 指定发送 Ping 监测报文的源 IP 地址。当对端设备为设备时，如果不指定该参数，系统默认为出接口 IP 地址。此 IP 地址不能为“0.0.0.0”和“255.255.255.255”。
- **interval** *time-value* – 指定发送Ping 监测报文的时间间隔，单位为秒。范围是 1 到 255 秒。默认值是 10 秒。

- **threshold** *value* – 指定判断监测失败的警戒值。如果系统连续未收到该参数指定个数的响应报文，就判断为监测失败，即目标隧道中断。取值范围是 1 到 255。默认值是 10。

使用 **no vpn-track** 命令取消 VPN 监控功能的配置。

VPN 监控功能包括active 和 dead 两种状态。用户可以使用相应的 show 命令在 CLI 的任何模式下查看 VPN 监控功能的状态以及配置信息：

- 查看VPN 监控功能的状态：**show ipsec sa** {*id*}
- 查看VPN 监控功能的配置情况：**show tunnel ipsec** {**manual** | **auto**} {*tunnel-name*}

例如：

查看VPN 监控功能状态

hostname(config)# **show ipsec sa 5**

VPN Name: vpn1

Outbound

Gateway: 1.1.1.2

.....

VPN track status: alive

Inbound

Gateway: 1.1.1.2

.....

VPN track status: alive

查看VPN 监控功能配置

hostname(config)# **show tunnel ipsec auto vpn1**

Name: vpn1

mode: tunnel

.....

vpn-track: enable

tracknotify: enable

vpntrack destination 1.1.1.1

vpntrack source ip: 2.2.2.2

vpntrack interval: 3

vpntrack threshold: 3

{b}提示: {/b}关于 VPN 监控及冗余备份的具体实例，请参阅 VPN 监控及冗余备份的具体实例一节。

开启/关闭 VPN 隧道状态通知功能

默认情况下，VPN 隧道状态通知功能为关闭状态。在开启 VPN 隧道状态通知功能后，如果是基于路由的 VPN，系统一旦监测到中断的VPN 隧道，会立即通知路由模块中断的VPN 隧道信息并进行隧道路由的更新处理；如果是基于策略的 VPN，系统一旦监测到中断的 VPN 隧道，会立即通知策略模块中断的 VPN 隧道信息并进行隧道策略的更新处理。用户可以通过命令开启/关闭 VPN 隧道状态通知功能，对中断状态下的VPN 隧道信息进行通知。开启/关闭VPN 隧道状态通知功能，在 IKE IPSec 隧道配置模式下，使用以下命令：

- 开启：**tunnel-state-notify**
- 关闭：**no tunnel-state-notify**

设置 Commit 位

用户可以配置使响应方设置 Commit 位，从而防止出现丢包和时间差现象。但是，设置 Commit 位可能导致响应速度变慢。设置 Commit 位，请在 IKE IPSec 隧道配置模式下使用以下命令：

响应方设置 Commit 位：**responder-set-commit**

响应方不设置 Commit 位：**no responder-set-commit**

指定描述信息

为所配置的 IKE 隧道指定描述信息，请在 IKE IPSec 隧道配置模式下使用以下命令：

description *string*

- *string* – IKE 隧道的描述信息。

使用 **no description** 命令删除 IKE 隧道的描述信息。

IKEv2 VPN

IKEv2 VPN 的配置包括:

- 配置 P1 提议
- 配置 IKEv2 对等体
- 配置 P2 提议
- 配置隧道

配置 P1 提议

P1 提议是 IKEv2 安全提议，用于保存 IKE_SA_INIT 交换中所使用的安全参数，包括加密算法、完整性验证算法、PRF（pseudo-random function）算法和 DH 组。一个完整的 IKEv2 安全提议中至少应该包含一组安全参数，即一个加密算法、一个完整性验证算法、一个 PRF 算法和一个 DH 组。

创建 P1 提议

创建一个P1 提议，即 IKEv2 安全提议，请在全局配置模式下使用以下命令:

ikev2 proposoal *p1-name*

- *p1-name* – 指定所创建的P1 提议的名称。执行该命令后，CLI 进入到 P1 提议配置模式。用户可以在该模式下对P1 提议进行参数配置。

使用 **no ikev2 proposoal** *p1-name* 命令删除指定的P1 提议。

指定验证算法

StoneOS 支持以下验证算法：MD5、SHA-1 以及 SHA-2（包括 SHA-256、SHA-384 和 SHA-512）。用户可指定至少一种最多四种验证算法。指定 IKEv2 安全提议的验证算法，在 P1 提议模式下使用以下命令:

hash {**md5** | **sha** | **sha256** | **sha384** | **sha512**}

- **md5** – 指定使用 MD5 验证算法。摘要为 128 比特。
- **sha** – 指定使用 SHA-1 验证算法。摘要为 160 比特。该算法为 StoneOS 的默认算法。
- **sha256** – 指定使用 SHA-256 验证算法。摘要为 256 比特。
- **sha384** – 指定使用 SHA-384 验证算法。摘要为 384 比特。

- **sha512** – 指定使用 SHA-512 验证算法。摘要为 512 比特。

使用 **no hash** 命令恢复默认认证方式。

指定 PRF 算法

StoneOS 支持以下PRF 算法：MD5、SHA-1 以及 SHA-2（包括 SHA-256、SHA-384 和 SHA-512）。用户可指定至少一种最多四种PRF 算法。指定 IKEv2 安全提议的 PRF 算法，在 P1 提议模式下使用以下命令：

prf {**md5** | **sha** | **sha256** | **sha384** | **sha512**}

- **md5** – 指定使用 MD5 算法。摘要为 128 比特。
- **sha** – 指定使用 SHA-1 算法。摘要为 160 比特。该算法为 StoneOS 的默认算法。
- **sha256** – 指定使用 SHA-256 算法。摘要为 256 比特。
- **sha384** – 指定使用 SHA-384 算法。摘要为 384 比特。
- **sha512** – 指定使用 SHA-512 算法。摘要为 512 比特。

使用 **no prf** 命令恢复默认认证方式。

指定加密算法

StoneOS 提供以下四种加密算法：3DES、128bit AES、192bit AES 以及 256bit AES。用户可指定至少一种最多四种加密算法。指定 IKEv2 安全提议的加密算法，在P1 提议配置模式下使用以下命令：

encryption {**3des** | **aes** | **aes-192** | **aes-256**}

- **3des** – 指定使用 3DES 加密方法。密钥长度为 192 比特。该方法为 StoneOS 系统默认方法。
- **aes** – 指定使用 AES 加密方法。密钥长度为 128 比特。
- **aes-192** – 指定使用 192bit AES 加密方法。密钥长度为 192 比特。
- **aes-256** – 指定使用 256bit AES 加密方法。密钥长度为 256 比特。

使用 **no encryption** 命令恢复默认加密算法。

选择 DH 组

Diffie-Hellman（DH）是一种建立密钥的方法。DH 组决定 DH 交换中密钥生成“材料”的长度。密钥的牢固性部分决定于DH 组的强度。指定 IKEv2 安全提议的 DH 组，在P1 提议配置模式下使用以下命令：

group {1 | 2 | 5 | 14 | 15 |16 | 19 | 20 | 21 | 24}

- 1 – 选择 DH 组 1。密钥的长度为 768 比特（MODP Group）。
- 2 – 选择 DH 组 2。密钥的长度为 1024 比特（MODP Group）。DH 组 2 为 StoneOS 系统默认选择。
- 5 – 选择 DH 组 5。密钥的长度为 1536 比特（MODP Group）。
- 14 – 选择 DH 组 14。密钥的长度为 2048 比特（MODP Group）。
- 15 – 选择 DH 组 15。密钥的长度为 3072 比特（MODP Group）。
- 16 – 选择 DH 组 16。密钥的长度为 4096 比特（MODP Group）。
- 19 – 选择 DH 组 19。密钥的长度为 256 比特（ECP Group）。
- 20 – 选择 DH 组 20。密钥的长度为 384 比特（ECP Group）。
- 21 – 选择 DH 组 21。密钥的长度为 521 比特（ECP Group）。
- 24 – 选择 DH 组 24。密钥的长度为 2048 比特（MODP Group with 256-bit Prime Order Subgroup）。

使用 **no group** 命令取消恢复默认 DH 组。

指定的生命周期

IKEv2 SA 的生命周期不需要协商，由各自的配置决定，重协商总是由生命周期较小的一方发起，可尽量避免两端同时发起重协商造成冗余 SA 的生成，导致两端 SA 状态不一致。指定本端 IKEv2 SA 的生命周期，在 P1 提议配置模式下使用以下命令：

lifetime *time-value*

- *time-value* – 指定 IKEv2 SA 的生命周期长度，单位为秒。默认 28800 秒。范围是 180 到 86400 秒。

使用 **no lifetime** 命令恢复默认生命周期长度。

配置 IKEv2 对等体

创建一个 IKEv2 对等体后，用户可以配置对等体的 IKE 协商模式、对等体的 IP 地址、IKE 安全提议、本地 ID 等。

创建 IKEv2 对等体

创建 IKEv2 对等体，在全局配置模式下，使用以下命令：

ikev2 peer *peer-name*

- *peer-name* – 指定对等体的名称。

执行该命令后，CLI 进入到 IKEv2 对等体配置模式。用户可以在该模式下对IKEv2 对等体进行参数配置。

在全局配置模式下使用 **no ikev2 peer** *peer-name* 命令删除指定的 IKEv2 对等体。

绑定接口到对等体

用户可以绑定某个接口到 IKEv2 对等体。将接口绑定到 IKEv2 对等体，在 IKEv2 对等体配置模式下使用以下命令：

interface *interface-name*

- *interface-name* – 指定被绑定接口的名称。

使用 **no interface** 命令取消接口绑定。

指定对端的 IP 地址

用户可以为所创建的 IKEv2 指定对端的 IP 地址。指定对端的 IP 地址，在 IKEv2 对等体配置模式下使用以下命令：

match-peer *ip-address*

- *ip-address* - 指定对端的 IP 地址。

使用 **no match-peer** 命令取消对端 IP 地址。

配置认证方式

StoneOS 支持预共享密钥认证方式，且该认证方式为默认认证方式。为 IKEv2 对等体指定预共享密钥认证方式，在 IKEv2 对等体配置模式下使用以下命令：

auth psk

指定 P1 提议

为 IKEv2 对等体指定P1 提议，在 IKEv2 对等体配置模式下使用以下命令：

ikev2-proposal *p1-name*

- *p1-name* – 指定 P1 提议的名称。

使用 **no ikev2-proposal** *p1-name* 取消对P1 提议的指定。

配置本端 ID

配置本端的 ID，请在 IKEv2 对等体配置模式下使用以下命令：

local-id {**fqdn** *string* | **key-id** *string* |**ip** *ip-address* }

- **fqdn***string* – 指定使用 FQDN 类型的 ID。string 为 ID 的具体内容。
- **key-id***string* - 指定使用 Key ID 类型的 ID。string 为 ID 的具体内容。
- **ip***ip-address* - 指定使用 IP 地址类型的 ID。ip-address 为 ID 的具体内容。

使用 **no local-id** 命令取消对本端 ID 的配置。

指定连接类型

创建的 IKEv2 对等体可以是发起端、响应端或者既是发起端也是响应端。指定 IKEv2 对等体的连接类型，在 IKEv2 对等体配置模式下使用以下命令：

connection-type {**bidirectional** | **initiator-only** | **responder-only**}

- **bidirectional** – 指定该 ISAKMP 网关既是发起端也是响应端。该选项为系统的默认选项。
- **initiator-only** – 指定该 ISAKMP 网关仅是发起端。
- **responder-only** – 指定该 ISAKMP 网关仅是响应端。

使用 **no connection-type** 命令恢复默认连接方式。

创建 IKEv2 Profile

IKEv2 profile 用来保存非协商的 IKEv2 SA 的参数，例如对端的身份信息、预共享密钥、被保护数据流量的信息。IKEv2 profile 在发起端和响应端都需要配置。创建 IKEv2 Profile，在 IKEv2 对等体配置模式下使用以下命令：

ikev2-profile *profile-name*

- *profile-name* – 指定该 IKEv2 profile 的名称。

执行该命令后，CLI 进入到 IKEv2 profile 配置模式。用户可以在该模式下对非协商的 IKEv2 SA 的参数进行配置。

在全局配置模式下使用 **no ikev2-profile** *profile-name* 命令删除指定的 IKEv2 profile。

配置对端 ID

配置对端的 ID，请在 IKEv2 profile 配置模式下使用以下命令：

remote id {**fqdn** *string* | **key-id** *string* | **ip** *ip-address* }

- **fqdn** *string* – 指定使用FQDN 类型的 ID。string 为 ID 的具体内容。
- **key-id** *string* - 指定使用 Key ID 类型的 ID。string 为 ID 的具体内容。
- **ip** *ip-address* - 指定使用 IP 地址类型的 ID。ip-address 为 ID 的具体内容。

使用 **no remote id** 命令取消对对端 ID 的配置。

配置预共享密钥

两端的预共享密钥的值相同时，IKEv2 隧道才能建立。配置预共享密钥，在IKEv2 profile 配置模式下使用以下命令：

remote key *key-value*

- *key-value* – 指定预共享密钥的值。

使用 **no remote key** 命令删除所指定的预共享密钥。。

配置被保护的数据流量信息

IKEv2 VPN 能够对一个或者多个数据流进行安全保护，也就是对需要进入 IPSec 隧道的流量进行保护。在某些情况下，通过 IPSec 隧道加密的数据流量，其源地址和目的地址可能为多个不同网段，因此，用户可以通过以下命令，在 IKEv2 Profile 下配置一个或者多个被保护的数据流量的信息。目前，同一个 IKEv2 Profile 下最多可以允许配置 16 个被保护的数据流。

创建被保护的数据流，在 IKEv2 profile 配置模式下使用以下命令：

traffic-selector*traffic-selector-name*

- *traffic-selector-name* – 指定被保护的数据流名称。

执行该命令后，CLI 进入到被保护的数据流配置模式。用户可以在该模式下对被保护的数据流的参数（本端地址、对端地址）进行配置。

使用 **no traffic-selector***traffic-selector-name* 命令删除所配置的被保护的数据流信息。

配置本端地址

配置被保护的数据流的本端地址，在被保护的数据流配置模式下，使用以下命令：

local*A.B.C.D/Mask*

- *A.B.C.D/Mask* – 被保护的数据流的本端地址和掩码。

使用 **no local***A.B.C.D/Mask* 命令取消对被保护的数据流的本端地址的配置。

配置对端地址

配置被保护的数据流的对端地址，在被保护的数据流配置模式下，使用以下命令：

remote*A.B.C.D/Mask*

- *A.B.C.D/Mask* – 被保护的数据流的对端地址和掩码。

使用 **no remote***A.B.C.D/Mask* 命令取消对被保护的数据流的对端地址的配置。

配置自动生成路由功能

对于 IKEv2 VPN，配置自动生成路由功能后，每创建一个 IPSec SA，设备会将目的地址为被保护的数据流的目的网段、下一跳为隧道接口的路由条目添加到自己的路由表。删除一个 IPSec SA 后，相应的路由条目也会被删除。

默认情况下，设备的自动生成路由功能是关闭的。开启此功能，请在 IKEv2 对等体配置模式下，使用以下命令：

generate-route

使用 **no generate-route** 命令关闭自动生成路由功能。

配置 P2 提议

P2 提议是 IPSec 安全提议，用于保存 IPsec 需要使用的安全协议、加密/认证算法等，为协商 IPSec SA 提供各种安全参数。对 P2 提议的配置包括指定协议类型、加密算法、验证算法、压缩算法和生命周期。

创建P2 提议，即IPSec 安全提议，请在全局配置模式下使用以下命令：

ikev2 ipsec proposal *p2-name*

- *p2-name* – 指定所创建的P2 提议的名称。执行该命令后，CLI 进入到 P2 提议配置模式。对P2 提议各项参数的配置都要在该模式下进行。

使用 **no ikev2 ipsec proposal** *p2-name* 命令删除指定的 IPSec 安全提议。

指定协议类型

P2 提议可使用的协议类型有ESP。为P2 提议指定协议类型，在 P2 提议配置模式下使用以下命令：

protocol esp

- esp – 指定使用ESP 协议。该协议为系统默认协议。

指定验证算法

用户可以为 P2 提议指定至少一种最多四种验证算法。为P2 提议指定验证算法，在P2 提议配置模式下使用以下命令：

hash {md5 | sha | sha256 | sha384 | sha512 | null}

- md5 – 指定使用 MD5 验证算法。摘要为 128 比特。
- sha – 指定使用 SHA-1 验证算法。摘要为 160 比特。该算法为 StoneOS 的默认算法。
- sha256 – 指定使用 SHA-256 验证算法。摘要为 256 比特。
- sha384 – 指定使用 SHA-384 验证算法。摘要为 384 比特。
- sha512 – 指定使用 SHA-512 验证算法。摘要为 512 比特。
- null – 不使用验证功能。

使用 no hash 命令恢复默认验证算法。

指定加密算法

用户可以为 P2 提议指定至少一种最多四种加密算法。为P2 提议指定加密算法，在P2 提议配置模式下使用以下命令：

encryption {3des| des | aes-192 | aes-256 | null }

- 3des – 指定使用 3DES 加密方法。密钥长度为 192 比特。该方法为 StoneOS 系统默认方法。
- des – 指定使用 DES 加密方法。密钥长度为 64 比特。
- aes-192 – 指定使用 192bit AES 加密方法。密钥长度为 192 比特。
- aes-256 – 指定使用 256bit AES 加密方法。密钥长度为 256 比特。
- null – 不使用加密功能。

使用 no encryption 命令恢复默认加密算法。

配置 PFS 功能

PFS（Perfect Forward Security）功能决定新密钥的生成方式，而不是新密钥的生成时间。PFS 保证无论在哪一阶段，一个密钥只能使用一次，而且，生成密钥的“材料”也只能使用一次。某个“材料”在生成了一个密钥后就被弃，绝不用来再生成任何其它密钥。这样可以确保一旦单个密钥泄密，最多只可能影响用该密钥加密的数据，而不会危及整个通信。PFS 功能是由 DH 算法做保障的。配置 P2 提议的PFS 功能，在 P2 提议配置模式下使用以下命令：

group {**nopfs** | **1** | **2** | **5** | **14** | **15** |**16**| **19** | **20** | **21** | **24**}

- **nopfs** – 不使用PFS 功能。该选项为系统的默认选项。
- **1** – 选择 DH 组 1。密钥的长度为 768 比特（MODP Group）。
- **2** – 选择 DH 组 2。密钥的长度为 1024 比特（MODP Group）。
- **5** – 选择 DH 组 5。密钥的长度为 1536 比特（MODP Group）。
- **14** – 选择 DH 组 14。密钥的长度为 2048 比特（MODP Group）。
- **15** – 选择 DH 组 15。密钥的长度为 3072 比特（MODP Group）。
- **16** – 选择 DH 组 16。密钥的长度为 4096 比特（MODP Group）。
- **19** – 选择 DH 组 19。密钥的长度为 256 比特（ECP Group）。
- **20** – 选择 DH 组 20。密钥的长度为 384 比特（ECP Group）。
- **21** – 选择 DH 组 21。密钥的长度为 521 比特（ECP Group）。
- **24** – 选择 DH 组 24。密钥的长度为 2048 比特（MODP Group with 256-bit Prime Order Subgroup）。

使用 **no group** 命令恢复默配置。

指定生命周期

设备按时间衡量生命周期。当 IPSec SA 的时间达到特定值时，SA 就会过期，需要重新进行协商。指定 P2 提议的生命周期，在P 配置模式，使用以下命令：

lifetime *seconds*

- *seconds* – 指定时间类型生命周期的时间长度，单位为秒。默认值是 28800 秒。范围是 180 到 86400 秒。

使用以 no lifetime 命令恢复默认配置。

配置隧道

通过 IKEv2 配置 IPSec 隧道，用户需要配置的选项有指定操作模式、IKEv2 对等体、IKEv2 安全提议、以及自动连接。

创建 IKEv2 隧道

创建 IKEv2 隧道，在全局配置模式下，使用以下命令：

tunnel ipsec *tunnel-name* **ikev2**

- **tunnel-name** - 指定所创建的 IKEv2 隧道的名称。

执行该命令后，CLI 进入到 IKEv2 隧道配置模式。对 IKEv2 隧道的所有参数配置都需要在该模式下进行。

在全局配置模式下使用 **no tunnel ipsec** *tunnel-name* **ikev2** 删除指定的 IKEv2 隧道。

指定 IKEv2 隧道的操作模式

StoneOS 支持 IKEv2 隧道的操作模式为隧道模式。该模式为系统默认模式。

指定 IKEv2 对等体

为 IKEv2 隧道指定 IKEv2 对等体，请在 IKEv2 隧道配置模式下使用以下命令：

ikev2-peer *peer-name*

- *peer-name* – 指定 IKEv2 对等体的名称。

使用 **no ikev2-peer** 取消对 IKEv2 对等体的指定。

指定 P2 提议

为 IKEv2 隧道指定 P2 提议，请在 IKEv2 隧道配置模式下使用以下命令：

ipsec-proposal p2-name1 [p2-name2] [p2-name3]

- **p2-name** – 指定 P2 提议的名称。用户最多可以为 IKEv2 隧道指定 3 个 P2 提议供对端选择使用。

使用 **no ipsec-proposal** 取消对P2 提议的指定。

配置自动连接功能

设备支持自动方式触发建立 SA。自动方式是指设备每 60 秒检查一次 SA 的状态，如果 SA 未建立则自动发起协商请求。自动连接功能默认不开启。使用自动方式，请在 IKE 隧道配置模式下使用以下命令:

auto-connect

注意:自动连接功能仅在本端可以作为发起端时有效。

XAUTH

XAUTH 是对 IKE 协议的扩展和增强，允许设备结合已配置的认证服务器（RADIUS 和本地 AAA 服务器）对试图访问 IPSec VPN 网络的用户进行身份认证，目前大量应用在移动终端上。远程用户发起 VPN 连接请求后，设备上的 XAUTH 服务器会中断VPN 协商过程并要求用户输入有效的用户名和密码进行认证，认证成功后会继续 VPN 协商过程并为合法的客户端分配 IP 地址，否则会中断VPN 连接。

{b}提示: {/b}有关认证服务器配置的更多信息，请参考《用户认证》的“认证、授权与计费”部分。

XAUTH 的配置包括:

- 启用 XAUTH 服务器
- 配置 XAUTH 地址池
- 绑定地址池到XAUTH 服务器
- 配置 IP 用户绑定和 IP 角色绑定规则
- 配置推送到客户端的 WINS 服务器或 DNS 服务器

启用 XAUTH 服务器

XAUTH 服务器在设备上默认是禁用的。启用 XAUTH 服务器，在 ISAKMP 网关配置模式下，使用以下命令:

xauth server

在 ISAKMP 网关配置模式下，使用该命令 no 的形式禁用 XAUTH 服务器:

no xauth server

配置 XAUTH 地址池

XAUTH 通过地址池为客户端分配 IP 地址。当客户端连接XAUTH 服务端成功后，设备端会从地址池里取出一个 IP 地址与其它相关参数（如 DNS 服务器地址、WINS 服务器地址等）一起分配给客户端。创建 XAUTH 地址池，在全局配置模式下，使用以下命令：

xauth pool *pool-name*

- *pool-name* - 指定 XAUTH 地址池名称并进入XAUTH 地址池配置模式。如果指定的名称已存在，系统会直接进入XAUTH 地址池配置模式。

在 XAUTH 地址池配置模式下，使用该命令 no 的形式删除指定的 XAUTH 地址池：

no xauth pool p*ool-name*

指定 XAUTH 地址池中允许分配的 IP 地址范围，在XAUTH 地址池配置模式下，使用以下命令：

address *start-ip end-ip* **netmask** *mask*

- *start-ip* - 指定 XAUTH 地址池的起始 IP 地址。
- *end-ip* - 指定 XAUTH 地址池的结束 IP 地址。
- *mask* - 指定网络掩码

在 XAUTH 地址池配置模式下，使用该命令 no 的形式删除指定的 IP 地址范围：

no address

保留地址池中的 IP 地址为XAUTH 地址池中的部分 IP 地址，当 XAUTH 服务器从地址池里取出 IP 地址分配给客户端时，可以保留已经被占用的部分 IP 地址，不进行分配。

指定 XAUTH 保留地址池，在 XAUTH 地址池配置模式下，使用以下命令：

exclude-address *start-ip end-ip*

- *start-ip* - 指定 XAUTH 保留地址池的起始 IP 地址。
- *end-ip* - 指定 XAUTH 保留地址池的结束 IP 地址。

在 XAUTH 地址池配置模式下，使用该命令 no 的形式删除指定的保留地址池 IP 范围：

no exclude-address

绑定地址池到 XAUTH 服务器

XAUTH 地址池只有在绑定到XAUTH 服务器后才会生效。将指定的 XAUTH 地址池绑定到 XAUTH 服务器，在 ISAKMP 网关配置模式下，使用以下命令：

xauth pool-name *pool-name*

- *pool-name* - 指定绑定的地址池名称。

在 ISAKMP 网关配置模式下，使用该命令 no 的形式取消地址池绑定：

no xauth pool-name

配置 IP 用户绑定和 IP 角色绑定规则

XAUTH 服务器通过创建和执行 IP 地址绑定规则来满足客户端的固定 IP 地址需求。IP 地址绑定规则包括 IP 用户绑定规则和 IP 角色绑定规则。IP 用户绑定规则将客户端用户与已配置地址池中的某个固定 IP 地址绑定，当客户端连接成功后，设备端会将绑定的 IP 地址分配给客户端；IP 角色绑定规则是将角色与已配置地址池中的某一 IP 地址范围绑定，当此客户端连接成功后，设备端会从绑定的地址范围中取出一个 IP 地址分配给客户端。

当 XAUTH 通过地址池给客户端分配 IP 地址时，系统会按照一定的顺序对客户端的 IP 地址绑定规则进行检查，决定如何为客户端分配 IP 地址：

1. 检查是否已为客户端用户配置 IP 用户绑定规则，如果是，则将绑定的 IP 地址分配给客户端；否则，需要进一步检查。注意，如果此 IP 用户绑定规则中的 IP 地址已被占用，则该用户无法登录。
2. 检查是否已为客户端用户配置 IP 角色绑定规则，如果是，则从绑定的地址范围中取出一个 IP 地址分配给客户端；否则，在未绑定的 IP 地址范围中取出一个 IP 地址分配给客户端。注意，如果绑定的地址范围中的地址都已经被分配，则该用户无法登录。

注意:IP 用户绑定规则中的 IP 地址和 IP 角色绑定规则中的 IP 地址不能重叠。

配置 IP 用户绑定规则，在XAUTH 地址池配置模式下使用以下命令：

ip-binding user *user-name* **ip** *ip-address*

- **user** *user-name* - 指定客户端用户名。
- **ip** *ip-address* - 指定绑定的 IP 地址。此地址必须为地址池中可以分配的地址。

在 XAUTH 地址池配置模式下，使用该命令 no 的形式取消对特定用户 IP 用户绑定规则的配置：

no ip-binding user *user-name*

配置 IP 角色绑定规则，在XAUTH 地址池配置模式下使用以下命令：

ip-binding role *role-name* **ip-range** *start-ip end-ip*

- **role** *role-name* - 指定角色名称。

- **ip-range** *start-ip end-ip* - 指定绑定的 IP 范围的起始 IP 地址 start-ip 和结束 IP 地址 end-ip。此地址范围必须为地址池中可以分配的地址范围。

在 XAUTH 地址池配置模式下使用该命令 no 的形式取消对特定角色的 IP 角色绑定规则的配置：

no ip-binding role *role-name*

修改 IP 角色绑定规则排列顺序

一个用户可以绑定到一个或者多个角色，不同角色可以配置不同的 IP 角色绑定规则。对于绑定到多个角色且多个角色有相应的 IP 角色绑定规则的用户，设备会对 IP 角色绑定规则进行顺序查找，然后按照查找到的相匹配的第一条规则为用户分配地址。默认情况下，系统会将新创建的规则放到所有规则的末尾，管理员可以移动已有的 IP 角色绑定规则从而改变规则的排列顺序。改变规则的排列顺序，在 XAUTH 地址池配置模式下使用以下命令：

move *role-name1* {**before** *role-name2* | **after***role-name2*| **top** | **bottom**}

- *role – name1* – 指定被移动的 IP 角色绑定规则的角色名称。
- **before** *role-name2* – 将 IP 角色绑定规则移动到某个 IP 角色绑定规则(角色名称为 role-name2 的规则)之前。
- **after** *role-name2* – 将 IP 角色绑定规则移动到某个 IP 角色绑定规则(角色名称为role-name2 的规则)之后。
- **top** – 将 IP 角色绑定规则移动到所有 IP 角色绑定规则之首。
- **bottom** – 将 IP 角色绑定规则移动到所有 IP 角色绑定规则的末尾。

配置推送到客户端的 WINS/DNS 服务器

配置DNS 服务器，在 XAUTH 地址池配置模式下使用以下命令：

dns *address1* [*address2*]

- *address1* - 指定 DNS 服务器 IP 地址。用户最多可配置 2 个 DNS 服务器。

在 XAUTH 地址池配置模式下，使用该命令 no 的形式取消对DNS 服务器的指定：

no dns

配置 WINS 服务器，在 XAUTH 地址池配置模式下使用以下命令：

wins *address1* [*address2*]

- *address1* - 指定 WINS 服务器 IP 地址。用户最多可配置 2 个 WINS 服务器。在

XAUTH 地址池配置模式下，使用该命令 no 的形式取消对 WINS 服务器的指定：

强制断开客户端 XAUTH 连接

XAUTH 服务端可以通过命令强制断开某个客户端与设备端的连接。强制断开客户端XAUTH 连接，在执行模式使用以下命令：

exec xauth *isakmp-peer-name* **kickout** *user-name*

- *isakmp-peer-name* - 指定 ISAKMP 对端的名称。
- *user-name* - 指定被强制断开连接的用户名称。

配置非根 VSYS 隧道配额

配置非根VSYS 的 IPSec 隧道资源配额，在 VSYS Profile 配置模式下使用以下命令：

tunnel-ipsec max *max-num* **reserve** *reserve-num*

- **max** *max-num* **reserve** *reserve-num* – 指定非根VSYS 中 IPSec 隧道数的最大配额（*max-num* **reserve**）和预留配额（**reserve** *reserve-num*）。最大配额和预留配额根据不同平台取值范围不同。预留配额不能超过最大配额。最大配额取值范围为 0 至 max (capacity*2/max-vsys-num, capacity/10)，默认值为(capacity*2/max-vsys-num, capacity/10)；预留配额的最小值为 0。

在 VSYS Profile 配置模式下使用该命令 no 的形式删除配额：

notunnel-ipsec max *max-num* **reserve** *reserve-num*

显示 IPSec 配置信息

用户可以使用相应的 show 命令在 CLI 的任何模式下查看IPSec 功能的配置信息。

- 查看 IKEv1 P1 提议的配置信息：**show isakmp proposal** [**p1-name**]
- 查看 IKEv2 P1 提议的配置信息：**show ikev2 proposal** [*p1-name*]
- 查看 IKEv1 ISAKMP 网关的配置信息：**show isakmp peer** [*peer-name*]
- 查看 IKEv2 对等体的配置信息：**show ikev2 peer** [*peer-name*]
- 查看 IKEv2 对等体中 IKEv2 profile 的配置信息：**show ikev2 peer** [*peer-name*] **profile** [*profile-name*]
- 查看 IKEv1 P2 提议的配置信息：**show ipsec proposal** [*proposal-name*]
- 查看手工密钥VPN 隧道的配置信息：**show tunnel ipsec manual** [*tunnel-name*]
- 查看 IKEv1 隧道的配置信息：**show tunnel ipsec auto** [*tunnel-name*]
- 查看 IKEv2 隧道的配置信息：**show tunnel ipsec ikev2** [*tunnel-name*]

- 查看 IKEv1 安全联盟的配置信息：**show isakmp sa** [*dsp_ip*]
- 查看 IKEv2 安全联盟的配置信息：**show ikev2 ike-sa**
- 查看基于 IKEv1 的 IPSec 安全联盟的配置信息：**show ipsec sa** [*id* | **active** | **inactive**]
- 查看基于 IKEv2 的 IPSec 安全联盟的配置信息：**show ikev2 ipsec-sa** [*sa-id*]
- 查看 XAUTH 地址池信息：**show xauth pool** [*pool-name*]
- 查看接入的XAUTH 用户信息：**show xauth client** *isakmp-peer-name* [**user** *user-name*]

配置举例

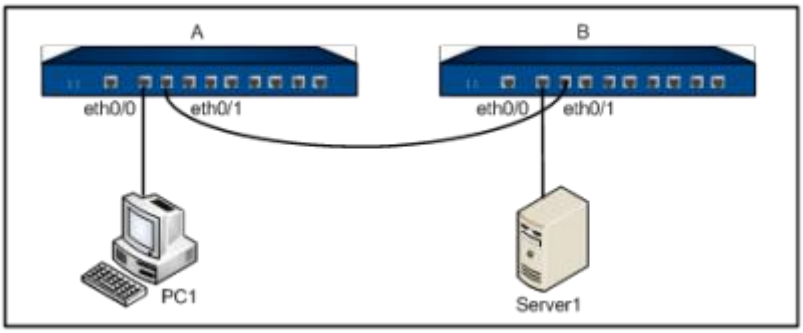
本节介绍通过手工密钥 VPN 和 IKE VPN 两种方式建立安全联盟的具体实例、VPN 监控及冗余备份的具体实例以及 XAUTH 的配置实例。

手工密钥 VPN

手工密钥VPN 隧道要求安全联盟的所有相关配置都由用户手动一一指定。请看以下实例。

组网需求

在 设备 A 和 设备 B 之间建立一个安全隧道，PC1 作 设备 A 端的主机，IP 地址为 188.1.1.2，网关为 188.1.1.1；server1 作为 设备 B 端的服务器，IP 地址为 10.110.88.210，网关是 10.110.88.220。要求对PC1 代表的子网（188.1.1.0/24）与 Server1 代表的子网（10.110.88.0/24）之间的数据流进行安全保护（通过基于策略的 VPN 方式实现VPN 的应用）。安全协议采用 ESP 协议，加密算法采用 3DES，验证算法采用 SHA1，压缩算法采用 DEFLATE。下图为该需求的组网图。



配置步骤

第一步：配置设备接口。

```
设备 Ahostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
```

```
hostname(config-if-eth0/0)# ip address 188.1.1.1/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 192.168.1.2/24
hostname(config-if-eth0/1)# exitip address 10.1.1.1/24
设备 B
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 10.110.88.220/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/0
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 192.168.1.3/24
hostname(config-if-eth0/1)# exitip route 172.16.10.0/24 tunnel1 10
```

第二步：配置路由。

```
设 备 Ahostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip route 10.110.88.0/24 192.168.1.3
hostname(config-vrouter)# exit
设备 B
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip route 188.1.1.0/24 192.168.1.2
hostname(config-vrouter)# exit
```

第三步：手动配置名为VPN1 的隧道。

```
设备 Ahostname(config)# tunnel ipsec vpn1 manual
```

```
hostname(config-tunnel-ipsec-manual)# interface ethernet0/1
hostname(config-tunnel-ipsec-manual)# protocol esp
hostname(config-tunnel-ipsec-manual)# peer 192.168.1.3
hostname(config-tunnel-ipsec-manual)# hash sha
hostname(config-tunnel-ipsec-manual)# hash-key inbound 1234 outbound 5678
hostname(config-tunnel-ipsec-manual)# encryption 3des
hostname(config-tunnel-ipsec-manual)# encryption-key inbound 00ff outbound 123a
hostname(config-tunnel-ipsec-manual)# compression deflate
hostname(config-tunnel-ipsec-manual)# spi 6001 6002
hostname(config-tunnel-ipsec-manual)# exit
```

设备 B

```
hostname(config)# tunnel ipsec vpn1 manual
hostname(config-tunnel-ipsec-manual)# interface ethernet0/1
hostname(config-tunnel-ipsec-manual)# protocol esp
hostname(config-tunnel-ipsec-manual)# peer 192.168.1.2
hostname(config-tunnel-ipsec-manual)# hash sha
hostname(config-tunnel-ipsec-manual)# hash-key inbound 5678 outbound 1234
hostname(config-tunnel-ipsec-manual)# encryption 3des
hostname(config-tunnel-ipsec-manual)# encryption-key inbound 123a outbound 00ff
hostname(config-tunnel-ipsec-manual)# compression deflate
hostname(config-tunnel-ipsec-manual)# spi 6002 6001
hostname(config-tunnel-ipsec-manual)# exit
```

第四步：配置设备策略规则。

设备 A

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

hostname(config-policy-rule)# src-zone trust

hostname(config-policy-rule)# dst-zone untrust

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 fromtunnel vpn1

hostname(config-policy-rule)# exit

hostname(config-policy)# exit

hostname(config)#

设备 B

hostname(config)# policy-global

hostname(config-policy)# rule

hostname(config-policy-rule)# src-zone trust

hostname(config-policy-rule)# dst-zone untrust

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 tunnel vpn1

hostname(config-policy-rule)# exit

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 fromtunnel vpn1

hostname(config-policy-rule)# exit

```
hostname(config-policy)# exit

hostname(config)#
```

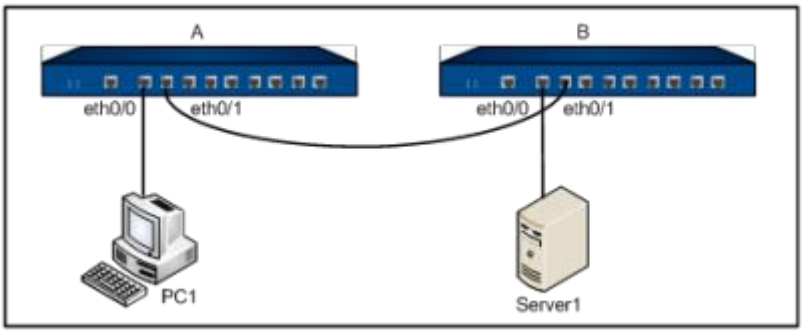
完成以上配置后， 设备A 和 设备 B 之间的安全隧道便建立成功了。子网（188.1.1.0/24）与 server1 代表的子网（10.110.88.0/24）之间的数据流将会被加密传输。

IKE VPN

本节介绍通过 IKE 方式创建安全联盟的实例。

组网需求

在 设备 A 和 设备 B 之间建立一个安全隧道，PC1 作为 设备A 端的主机，IP 地址为 10.1.1.1，网关为 10.1.1.2； Server1 作为 设备 B 端的服务器，IP 地址为 192.168.1.1，网关是 192.168.1.2。要求对 PC1 代表的子网（10.1.1.0/24）与 server1 代表的子网（192.168.1.0/24）之间的数据流进行安全保护（通过基于路由的 VPN 方式实现VPN 的应用）。安全协议采用 ESP 协议，加密算法采用 3DES，验证算法采用 SHA1，压缩算法采用 DEFLATE。组网图请参考下图：



配置步骤

第一步：配置设备接口。

```
设备 A
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 10.1.1.2/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if)# zone untrust
```

```
hostname(config-if-eth0/1)# ip address 1.1.1.1/24
hostname(config-if-eth0/1)# exit
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone trust
hostname(config-if-tun1)# exit
```

设备 B

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 192.168.1.2/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 1.1.1.2/24
hostname(config-if-eth0/1)# exit
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone trust
hostname(config-if-tun1)# exit
```

第二步：配置设备策略规则。

设备 A

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
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-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)# exit

hostname(config-policy)# rule

hostname(config-policy-rule)# src-zone trust

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)# exit

hostname(config-policy)# exit

hostname(config)#

设备 B

hostname(config)# policy-global

hostname(config-policy)# rule

hostname(config-policy-rule)# src-zone trust

hostname(config-policy-rule)# dst-zone untrust

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

第三步：配置路由。

设备 A

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip route 192.168.1.0/24 tunnel1
hostname(config-vrouter)# exit
```

设备 B

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip route 10.1.1.0/24 tunnel1
hostname(config-vrouter)# exit
```

第四步：配置P1 提议。

设备 A

```
hostname(config)# isakmp proposal p1
hostname(config-isakmp-proposal)# authentication pre-share
hostname(config-isakmp-proposal)# group 2
hostname(config-isakmp-proposal)# hash sha
hostname(config-isakmp-proposal)# encryption 3des
hostname(config-isakmp-proposal)# exit
```

设备 B

```
hostname(config)# isakmp proposal p1
hostname(config-isakmp-proposal)# authentication pre-share
hostname(config-isakmp-proposal)# group 2
hostname(config-isakmp-proposal)# hash sha
hostname(config-isakmp-proposal)# encryption 3des
hostname(config-isakmp-proposal)# exit
```

第五步：配置 ISAKMP 网关。

设备 A

```
hostname(config)# isakmp peer east
hostname(config-isakmp-peer)# interface ethernet0/1
hostname(config-isakmp-peer)# isakmp-proposal p1
hostname(config-isakmp-peer)# peer 1.1.1.2
```

```
hostname(config-isakmp-peer)# pre-share hello1
hostname(config-isakmp-peer)# exit
```

设备 B

```
hostname(config)# isakmp peer west
hostname(config-isakmp-peer)# interface ethernet0/1
hostname(config-isakmp-peer)# isakmp-proposal p1
hostname(config-isakmp-peer)# peer 1.1.1.1
hostname(config-isakmp-peer)# pre-share hello1
hostname(config-isakmp-peer)# exit
```

第六步：配置 P2 提议。

设备 A

```
hostname(config)# ipsec proposal p2
hostname(config-ipsec-proposal)# protocol esp
hostname(config-ipsec-proposal)# hash sha
hostname(config-ipsec-proposal)# encryption 3des
hostname(config-ipsec-proposal)# compression deflate
hostname(config-ipsec-proposal)# exit
```

设备 B

```
hostname(config)# ipsec proposal p2
hostname(config-ipsec-proposal)# protocol esp
hostname(config-ipsec-proposal)# hash sha
hostname(config-ipsec-proposal)# encryption 3des
hostname(config-ipsec-proposal)# compression deflate
hostname(config-ipsec-proposal)# exit
```

第七步：配置名为 VPN 的隧道。

设备 A

```
hostname(config)# tunnel ipsec vpn auto
hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2
hostname(config-tunnel-ipsec-auto)# isakmp-peer east
hostname(config-tunnel-ipsec-auto)# id local 10.1.1.0/24 remote 192.168.1.0/24 service any
hostname(config-tunnel-ipsec-auto)# exit
hostname(config)# interface tunnel1
hostname(config-if-tun1)# tunnel ipsec vpn
hostname(config-if-tun1)# exit
```

设备 B

```
hostname(config)# tunnel ipsec vpn auto
hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2
hostname(config-tunnel-ipsec-auto)# isakmp-peer east
hostname(config-tunnel-ipsec-auto)# id local 192.168.1.0/24 remote 10.1.1.0/24 service any
hostname(config-tunnel-ipsec-auto)# exit
hostname(config)# interface tunnel1
hostname(config-if-tun1)# tunnel ipsec vpn
hostname(config-if-tun1)# exit
```

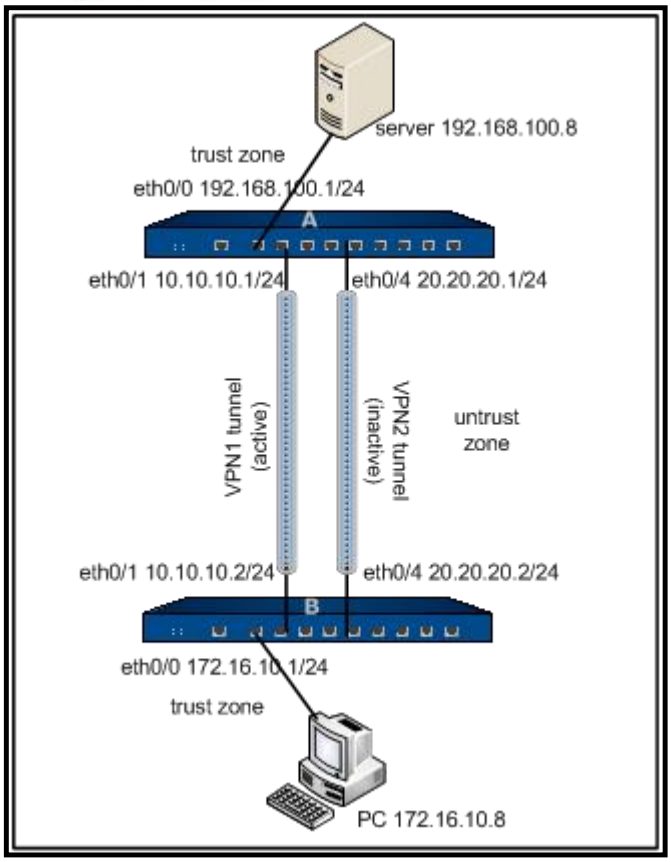
完成以上配置后， 设备A 和 设备 B 之间的安全隧道便建立成功了。子网（10.1.1.0/24）与 Server1 代表的子网（192.168.1.0/24）之间的数据流将会被加密传输。

基于路由的 VPN 监控及冗余备份功能配置举例

该节介绍基于路由的 VPN 监控及冗余备份功能配置实例。

组网需求

在 设备 A 和设备B 之间配置 IKE VPN 隧道VPN1 tunnel 和 VPN2 tunnel，server 作为 设备 A 端的服务器，IP 地址为 192.168.100.8，网关是 192.168.100.1；PC 作为 设备 B 端的主机，IP 地址为 172.16.10.8，网关为 172.16.10.1。要求实现 VPN1 tunnel 和 VPN2 tunnel 的 VPN 监控，并当主隧道（VPN1 tunnel）链路发生故障时，流量转向备份隧道（VPN2 tunnel）；主隧道恢复正常时，流量切换回主隧道。组网图参见下图：



配置步骤

第一步：配置 设备 A：

配置接口：

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 192.168.100.1/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 10.10.10.1/24
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/4
hostname(config-if-eth0/4)# zone untrust
```

hostname(config-if-eth0/4)# ip address 20.20.20.1/24

hostname(config-if-eth0/4)# exit

配置P1 提议

hostname(config)# isakmp proposal p1

hostname(config-isakmp-proposal)# authentication pre-share

hostname(config-isakmp-proposal)# group 2

hostname(config-isakmp-proposal)# hash md5

hostname(config-isakmp-proposal)# encryption des

hostname(config-isakmp-proposal)# exit

配置 ISAKMP 网关:

hostname(config)# isakmp peer gwa-peer-1

hostname(config-isakmp-peer)# interface ethernet0/1

hostname(config-isakmp-peer)# isakmp-proposal p1

hostname(config-isakmp-peer)# peer 10.10.10.2

hostname(config-isakmp-peer)# pre-share U8FdHNEEBz6sNn5Mvqx3yWuLRWce

hostname(config-isakmp-peer)# exit

hostname(config)# isakmp peer gwa-peer-2

hostname(config-isakmp-peer)# interface ethernet0/4

hostname(config-isakmp-peer)# isakmp-proposal p1

hostname(config-isakmp-peer)# peer 20.20.20.2

hostname(config-isakmp-peer)# pre-share i39jnnNiCSh9rXb77oGA7Fg7BNQy

hostname(config-isakmp-peer)# exit

配置P2 提议：

hostname(config)# ipsec proposal p2

hostname(config-ipsec-proposal)# protocol esp

hostname(config-ipsec-proposal)# hash md5

hostname(config-ipsec-proposal)# encryption des

hostname(config-ipsec-proposal)# exit

配置VPN 隧道：

hostname(config)# tunnel ipsec vpn1-tunnel auto

hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2

hostname(config-tunnel-ipsec-auto)# isakmp-peer gwa-peer-1

hostname(config-tunnel-ipsec-auto)# vpn-track interval 3 threshold 9

hostname(config-tunnel-ipsec-auto)# track-event-notify enable

hostname(config-tunnel-ipsec-auto)# exit

hostname(config)# tunnel ipsec vpn2-tunnel auto

hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2

hostname(config-tunnel-ipsec-auto)# isakmp-peer gwa-peer-2

hostname(config-tunnel-ipsec-auto)# vpn-track interval 3 threshold 9

hostname(config-tunnel-ipsec-auto)# track-event-notify enable

hostname(config-tunnel-ipsec-auto)# auto-connect

hostname(config-tunnel-ipsec-auto)# exit

创建隧道接口并绑定VPN 隧道：

hostname(config)# interface tunnel1

hostname(config-if-tun1)# zone untrust

hostname(config-if-tun1)#

hostname(config-if-tun1)# tunnel ipsec vpn1-tunnel

hostname(config-if-tun1)# exit

hostname(config)# interface tunnel2

hostname(config-if-tun2)# zone untrust

hostname(config-if-tun2)# ip address 10.2.2.1/24

hostname(config-if-tun2)# tunnel ipsec vpn2-tunnel

hostname(config-if-tun2)# exit

配置路由：

hostname(config)# ip vrouter trust-vr

hostname(config-vrouter)#

hostname(config-vrouter)# ip route 172.16.10.0/24 tunnel2 20

hostname(config-vrouter)# exit

配 置 策 略 :

hostname(config)# policy-global

hostname(config-policy)# rule

hostname(config-policy-rule)# src-zone trust

hostname(config-policy-rule)# dst-zone untrust

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-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)# exit

hostname(config-policy)# exit

hostname(config)#

第二步: 配置 设备 B:

配置接口:

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 172.16.10.1/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 10.10.10.2/24
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/4
hostname(config-if-eth0/4)# zone untrust
hostname(config-if-eth0/4)# ip address 20.20.20.2/24
hostname(config-if-eth0/4)# exit
```

配置 P1 提议

```
hostname(config)# isakmp proposal p1
hostname(config-isakmp-proposal)# authentication pre-share
hostname(config-isakmp-proposal)# group 2
hostname(config-isakmp-proposal)# hash md5
hostname(config-isakmp-proposal)# encryption des
hostname(config-isakmp-proposal)# exit
```

配置 ISAKMP 网关：

```
hostname(config)# isakmp peer gwb-peer-1
hostname(config-isakmp-peer)# interface ethernet0/1
hostname(config-isakmp-peer)# isakmp-proposal p1
hostname(config-isakmp-peer)# peer 10.10.10.1
hostname(config-isakmp-peer)# pre-share U8FdHNEEBz6sNn5Mvqx3yWuLRWce
hostname(config-isakmp-peer)# exit
hostname(config)# isakmp peer gwb-peer-2
```

hostname(config-isakmp-peer)# interface ethernet0/4

hostname(config-isakmp-peer)# isakmp-proposal p1

hostname(config-isakmp-peer)# peer 20.20.20.1

hostname(config-isakmp-peer)# pre-share i39jnnNiCSh9rXb77oGA7Fg7BNQy

hostname(config-isakmp-peer)# exit

配置 P2 提议：

hostname(config)# ipsec proposal p2

hostname(config-ipsec-proposal)# protocol esp

hostname(config-ipsec-proposal)# hash md5

hostname(config-ipsec-proposal)# encryption des

hostname(config-ipsec-proposal)# exit

配置 VPN 隧道：

hostname(config)# tunnel ipsec vpn1-tunnel auto

hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2

hostname(config-tunnel-ipsec-auto)# isakmp-peer gwb-peer-1

hostname(config-tunnel-ipsec-auto)# vpn-track interval 3 threshold 9

hostname(config-tunnel-ipsec-auto)# track-event-notify enable

hostname(config-tunnel-ipsec-auto)# auto-connect

hostname(config-tunnel-ipsec-auto)# exit

hostname(config)# tunnel ipsec vpn2-tunnel auto

hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2

hostname(config-tunnel-ipsec-auto)# isakmp-peer gwb-peer-2

hostname(config-tunnel-ipsec-auto)# vpn-track interval 3 threshold 9

hostname(config-tunnel-ipsec-auto)# track-event-notify enable

hostname(config-tunnel-ipsec-auto)# auto-connect

hostname(config-tunnel-ipsec-auto)# exit

创建隧道接口并绑定 VPN 隧道：

hostname(config)# interface tunnel1

hostname(config-if-tun1)# zone untrust

hostname(config-if-tun1)# ip address 10.1.1.2/24

hostname(config-if-tun1)# tunnel ipsec vpn1-tunnel

hostname(config-if-tun1)# exit

hostname(config)# interface tunnel2

hostname(config-if-tun2)# zone untrust

hostname(config-if-tun2)# ip address 10.2.2.2/24

hostname(config-if-tun2)# tunnel ipsec vpn2-tunnel

hostname(config-if-tun2)# exit

配置路由：

hostname(config)# ip vrouter trust-vr

hostname(config-vrouter)# ip route 192.168.100.0/24 tunnel1 1

hostname(config-vrouter)# ip route 192.168.100.0/24 tunnel2 2

hostname(config-vrouter)# exit

配 置 策 略 :

hostname(config)# policy-global

hostname(config-policy)# rule

hostname(config-policy-rule)# src-zone trust

hostname(config-policy-rule)# dst-zone untrust

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-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)# exit
hostname(config-policy)# exit
hostname(config)#
```

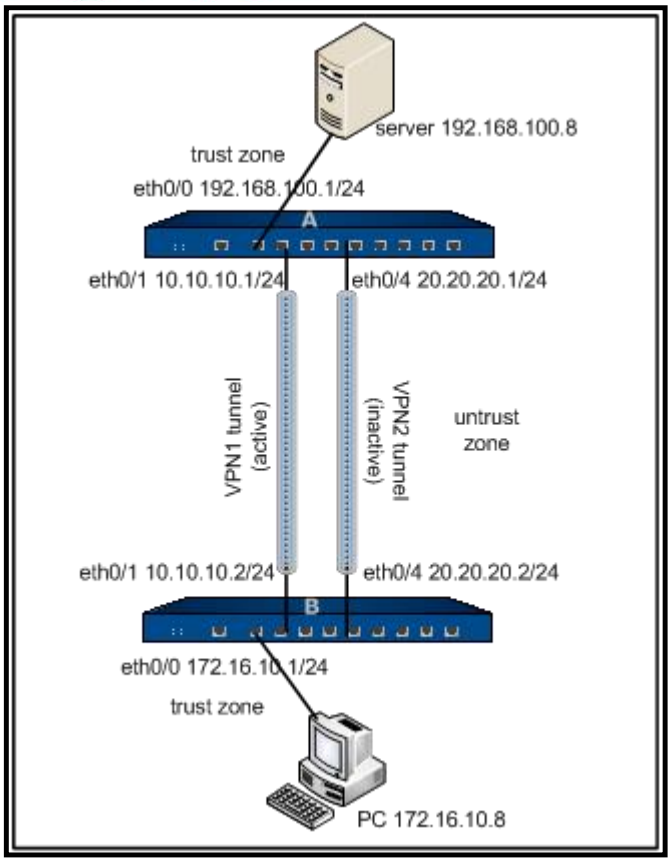
由于本例中 VPN 终端设备都是设备，因此可使用缺省源和目标地址进行 VPN 监控。

基于策略的 VPN 监控及冗余备份功能配置举例

该节介绍基于策略的 VPN 监控及冗余备份功能配置实例。

组网需求

在 设备 A 和设备B 之间配置 IKE VPN 隧道VPN1 tunnel 和 VPN2 tunnel，server 作为 设备 A 端的服务器，IP 地址为 192.168.100.8，网关是 192.168.100.1；PC 作为 设备 B 端的主机，IP 地址为 172.16.10.8，网关为 172.16.10.1。要求实现 VPN1 tunnel 和 VPN2 tunnel 的 VPN 监控，并当主隧道（VPN1 tunnel）链路发生故障时，流量转向备份隧道（VPN2 tunnel）；主隧道恢复正常时，流量切换回主隧道。组网图参见下图:



配置步骤

第一步:配置 设备 A:

配置接口：

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 192.168.100.1/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 10.10.10.1/24
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/4
hostname(config-if-eth0/4)# zone untrust
```

hostname(config-if-eth0/4)# ip address 20.20.20.1/24

hostname(config-if-eth0/4)# exit

配置路由：

hostname(config)# ip vrouter trust-vr

hostname(config-vrouter)# ip route 172.16.10.0/24 20.20.20.2

hostname(config-vrouter)# exit

配置P1 提议

hostname(config)# isakmp proposal p1

hostname(config-isakmp-proposal)# authentication pre-share

hostname(config-isakmp-proposal)# group 2

hostname(config-isakmp-proposal)# hash md5

hostname(config-isakmp-proposal)# encryption des

hostname(config-isakmp-proposal)# exit

配置ISAKMP 网关：

hostname(config)# isakmp peer gwa-peer-1

hostname(config-isakmp-peer)# interface ethernet0/1

hostname(config-isakmp-peer)# isakmp-proposal p1

hostname(config-isakmp-peer)# peer 10.10.10.2

hostname(config-isakmp-peer)# pre-shareU8FdHNEEBz6sNn5Mvqx3yWuLRWce

hostname(config-isakmp-peer)# exit

hostname(config)# isakmp peer gwa-peer-2

hostname(config-isakmp-peer)# interface ethernet0/4

hostname(config-isakmp-peer)# isakmp-proposal p1

hostname(config-isakmp-peer)# peer 20.20.20.2

hostname(config-isakmp-peer)# pre-share i39jnnNiCSh9rXb77oGA7Fg7BNQy

hostname(config-isakmp-peer)# exit

配置P2 提议：

hostname(config)# ipsec proposal p2

hostname(config-ipsec-proposal)# protocol esp

hostname(config-ipsec-proposal)# hash md5

hostname(config-ipsec-proposal)# encryption des

hostname(config-ipsec-proposal)# exit

配置VPN 隧道：

hostname(config)# tunnel ipsec vpn1-tunnel auto

hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2

hostname(config-tunnel-ipsec-auto)# isakmp-peer gwa-peer-1

hostname(config-tunnel-ipsec-auto)# vpn-track interval 1 threshold 5

hostname(config-tunnel-ipsec-auto)# track-event-notify enable

hostname(config-tunnel-ipsec-auto)# exit

hostname(config)# tunnel ipsec vpn2-tunnel auto

hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2

hostname(config-tunnel-ipsec-auto)# isakmp-peer gwa-peer-2

hostname(config-tunnel-ipsec-auto)# vpn-track interval 1 threshold 5

hostname(config-tunnel-ipsec-auto)# track-event-notify enable

hostname(config-tunnel-ipsec-auto)#auto-connect

hostname(config-tunnel-ipsec-auto)# exit

配置策略：

hostname(config)# policy-global

hostname(config-policy)# rule id 1

hostname(config-policy-rule)# src-ip 192.168.100.8/24

hostname(config-policy-rule)# dst-ip 172.16.10.8/24

hostname(config-policy-rule)# service any

hostname(config-policy-rule)# action tunnel vpn1-tunnel

hostname(config-policy-rule)# exit

```
hostname(config-policy)# rule id 2
hostname(config-policy-rule)# src-ip 172.16.10.8/24
hostname(config-policy-rule)# dst-ip 192.168.100.8/24
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action fromtunnel vpn1-tunnel
hostname(config-policy-rule)# exit
hostname(config-policy)# rule id 3
hostname(config-policy-rule)# src-ip 192.168.100.8/24
hostname(config-policy-rule)# dst-ip 172.16.10.8/24
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action tunnel vpn2-tunnel
hostname(config-policy-rule)# exit
hostname(config-policy)# rule id 4
hostname(config-policy-rule)# src-ip 172.16.10.8/24
hostname(config-policy-rule)# dst-ip 192.168.100.8/24
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action fromtunnel vpn2-tunnel
hostname(config-policy-rule)# exit
hostname(config-policy)# rule id 5
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-policy)# exit
hostname(config)#
```

第二步：配置 设备 B:

配置接口：

hostname(config)# interface ethernet0/0

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

hostname(config-if-eth0/0)# ip address 172.16.10.1/24

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

hostname(config)# interface ethernet0/1

hostname(config-if-eth0/1)# zone untrust

hostname(config-if-eth0/1)# ip address 10.10.10.2/24

hostname(config-if-eth0/1)# exit

hostname(config)# interface ethernet0/4

hostname(config-if-eth0/4)# zone untrust

hostname(config-if-eth0/4)# ip address 20.20.20.2/24

hostname(config-if-eth0/4)# exit

配置路由：

hostname(config)# ip vrouter trust-vr

hostname(config-vrouter)# ip route 192.168.100.0/24 20.20.20.1

hostname(config-vrouter)# exit

配置P1 提议

hostname(config)# isakmp proposal p1

hostname(config-isakmp-proposal)# authentication pre-share

hostname(config-isakmp-proposal)# group 2

hostname(config-isakmp-proposal)# hash md5

hostname(config-isakmp-proposal)# encryption des

hostname(config-isakmp-proposal)# exit

配置ISAKMP 网关：

hostname(config)# isakmp peer gwb-peer-1

hostname(config-isakmp-peer)# interface ethernet0/1

hostname(config-isakmp-peer)# isakmp-proposal p1

hostname(config-isakmp-peer)# peer 10.10.10.1

hostname(config-isakmp-peer)# pre-shareU8FdHNEEBz6sNn5Mvqx3yWuLRWce

hostname(config-isakmp-peer)# exit

hostname(config)# isakmp peer gwb-peer-2

hostname(config-isakmp-peer)# interface ethernet0/4

hostname(config-isakmp-peer)# isakmp-proposal p1

hostname(config-isakmp-peer)# peer 20.20.20.1

hostname(config-isakmp-peer)# pre-sharei39jnnNiCSh9rXb77oGA7Fg7BNQy

hostname(config-isakmp-peer)# exit

配置P2 提议：

hostname(config)# ipsec proposal p2

hostname(config-ipsec-proposal)# protocol esp

hostname(config-ipsec-proposal)# hash md5

hostname(config-ipsec-proposal)# encryption des

hostname(config-ipsec-proposal)# exit

配置VPN 隧道：

hostname(config)# tunnel ipsec vpn1-tunnel auto

hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2

hostname(config-tunnel-ipsec-auto)# isakmp-peer gwb-peer-1

hostname(config-tunnel-ipsec-auto)# vpn-track interval 1threshold 5

hostname(config-tunnel-ipsec-auto)# auto-connect

hostname(config-tunnel-ipsec-auto)# exit

hostname(config)# tunnel ipsec vpn2-tunnel auto

hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2

hostname(config-tunnel-ipsec-auto)# isakmp-peer gwa-peer-2

hostname(config-tunnel-ipsec-auto)# vpn-track interval 1 threshold 5

hostname(config-tunnel-ipsec-auto)# track-event-notify enable

hostname(config-tunnel-ipsec-auto)#auto-connect

hostname(config-tunnel-ipsec-auto)# exit

配置策略：

hostname(config)# policy-global

hostname(config-policy)# rule id 1

hostname(config-policy-rule)# src-ip 172.16.10.8/24

hostname(config-policy-rule)# dst-ip 192.168.100.8/24

hostname(config-policy-rule)# service any

hostname(config-policy-rule)# action fromtunnel vpn1-tunnel

hostname(config-policy-rule)# exit

hostname(config-policy)# rule id 2

hostname(config-policy-rule)# src-ip 192.168.100.8/24

hostname(config-policy-rule)# dst-ip 172.16.10.8/24

hostname(config-policy-rule)# service any

hostname(config-policy-rule)# action tunnel vpn1-tunnel

hostname(config-policy-rule)# exit

hostname(config-policy)# rule id 3

hostname(config-policy-rule)# src-ip 172.16.10.8/24

hostname(config-policy-rule)# dst-ip 192.168.100.8/24

hostname(config-policy-rule)# service any

hostname(config-policy-rule)# action fromtunnel vpn2-tunnel

hostname(config-policy-rule)# exit

hostname(config-policy)# rule id 4

hostname(config-policy-rule)# src-ip 192.168.100.8/24

hostname(config-policy-rule)# dst-ip 172.16.10.8/24

hostname(config-policy-rule)# service any

```
hostname(config-policy-rule)# action tunnel vpn2-tunnel
hostname(config-policy-rule)# exit
hostname(config-policy)# rule id 5
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-policy)# exit
hostname(config)#
```

由于本例中 VPN 终端设备都是设备，因此可使用缺省源和目标地址进行 VPN 监控。SSL VPN

SSL VPN 介绍

为解决远程用户安全访问私网数据的问题， 设备提供基于 SSL 的远程登录解决方案 SSL VPN。SSL VPN 功能可以通过简单易用的方法实现信息的远程连通。

StoneOS 的 SSL VPN 功能包含设备端和客户端两部分。配置了 SSL VPN 功能的 设备作为设备端，具有以下功能：

- 接受客户端连接；
- 为客户端分配 IP 地址、DNS 服务器地址和 WINS 服务器地址；
- 进行客户端用户的认证与授权；
- 进行客户端主机的安全检测；
- 对 IPSec 数据进行加密与转发。

设备 SSL VPN 的客户端工具为 Secure Connect。用户可以通过浏览器下载该客户端，然后将其安装到 PC，连接设备端成功后，用户就可以通过 SSL VPN 功能安全的传输数据信息。

不同型号的设备默认情况下支持的同时在线最大 VPN 客户端数不同，如果想增加支持的客户端数，请向代理商购买相应的许可证。

SSL VPN 设备端配置

设备的 SSL VPN 功能配置包括以下各部分：

- 地址池配置
- 资源列表配置
- UDP 端口号配置
- SSL VPN 实例配置
- 绑定 SSL VPN 实例到隧道接口
- 配置客户端USB Key 证书认证
- 配置短信口令认证功能
- 配置主机验证功能
- 配置主机安全检测功能
- 配置最优路径检测功能
- 强制断开客户端 SSL VPN 连接
- 允许本地用户修改密码

地址池配置

SSL VPN 设备端通过地址池给客户端分配 IP 地址。当客户端连接 SSL VPN 设备端成功后，设备端会从地址池里取出一个 IP 地址与其它相关参数（如 DNS 服务器地址与 WINS 服务器地址等）一起分配给客户 端。在全局配置模式，使用以下命令创建 SSL VPN 地址池：

scvpn pool *pool-name*

- *pool-name* – 指定地址池的名称。

执行该命令后，系统创建指定名称的地址池，并且进入 SSL VPN 地址池配置模式；如果指定的名称已存在，则直接进入 SSL VPN 地址池配置模式。在全局配置模式下，使用该命令no 的形式删除指定的 SSL VPN 地址池：

no scvpn pool *pool-name*

在 SSL VPN 地址池配置模式下可进行如下配置：

- 配置地址池地址范围和网络掩码
- 配置保留地址池
- 配置 IP 地址绑定规则
- 配 置 DNS 服务器
- 配置 WINS 服务器

配置地址池地址范围

为地址池配置地址范围和网络掩码，在 SSL VPN 地址池配置模式下使用以下命令：

address *start-ip end-ip* **netmask** *A.B.C.D*

- *start-ip* – 指定 IP 范围的起始 IP 地址。
- *end-ip* – 指定 IP 范围的结束 IP 地址。
- **netmask** *A.B.C.D* – 指定地址池 IP 范围的网络掩码。

在 SSL VPN 地址池配置模式下使用该命令 no 的形式删除配置的 IP 地址范围：

no address

配置保留地址池

保留地址池中的 IP 地址为地址池中的部分 IP 地址，当 SSL VPN 设备端从地址池里取出 IP 地址分配给客户端时，需要保留已经被占用的部分 IP 地址（如网关、FTP 服务器等），不进行分配。配置保留地址池，在 SSL VPN 地址池配置模式下使用以下命令：

exclude address *start-ip end-ip*

- *start-ip* – 指定保留地址池的起始 IP 地址。
- *end-ip* – 指定保留地址池的结束 IP 地址。

在 SSL VPN 地址池配置模式下使用该命令 no 的形式取消保留地址池的配置：

no exclude

配置 IP 地址绑定规则

设备 SSL VPN 通过创建和执行 IP 地址绑定规则来满足客户端的固定 IP 地址需求。IP 地址绑定规则包括 IP 用户绑定规则和 IP 角色绑定规则。IP 用户绑定规则将客户端用户与已配置地址池中的某个固定 IP 地址绑定，当客户端连接成功后，设备端会将绑定的 IP 地址分配给客户端；IP 角色绑定规则是将角色与已配置地址池中的某一 IP 地址范围绑定，当此客户端连接成功后，设备端会从绑定的地址范围中取出一个 IP 地址分配给客户端。

当 SSL VPN 设备端通过地址池给客户端分配 IP 地址时，系统会按照一定的顺序对客户端的 IP 地址绑定规则进行检查，决定如何为客户端分配 IP 地址：

1. 检查是否已为客户端用户配置 IP 用户绑定规则，如果是，则将绑定的 IP 地址分配给客户端；否则，需要进一步检查。注意，如果此 IP 用户绑定规则中的 IP 地址已被占用，则该用户无法登录。

2.检查是否已为客户端用户配置 IP 角色绑定规则，如果是，则从绑定的地址范围中取出一个 IP 地址分配给客户端；否则，在未绑定的 IP 地址范围中取出一个 IP 地址分配给客户端。注意，如果绑定的地址范围中的地址都已经被分配，则该用户无法登录。

注意:IP 用户绑定规则中的 IP 地址和 IP 角色绑定规则中的 IP 地址不能重叠。

配置 IP 用户绑定规则

配置 IP 用户绑定规则，在 SSL VPN 地址池配置模式下使用以下命令:

ip-binding user *user-name* **ip** *ip-address*

- **user** *user-name* – 指定客户端用户名。
- **ip** *ip-address* – 指定绑定的 IP 地址。此地址必须为地址池中可以分配的地址。

在 SSL VPN 地址池配置模式下使用该命令 no 的形式取消对特定用户 IP 用户绑定规则的配置:

no ip-binding user *user-name*

配置 IP 角色绑定规则

配置 IP 角色绑定规则，在 SSL VPN 地址池配置模式下使用以下命令:

ip-binding role *role-name* **ip-range** *start-ip end-ip*

- **role** *role -name* – 指定角色名称。
- **ip-range** *start-ip end-ip* – 指定绑定的 IP 范围的起始 IP 地址 **start-ip** 和结束 IP 地址 **end-ip**。此地址范围必须为地址池中可以分配的地址范围。

在 SSL VPN 地址池配置模式下使用该命令 no 的形式取消对特定角色的 IP 角色绑定规则的配置:

no ip-binding role *role-name*

修改 IP 角色绑定规则排列顺序

一个用户可以绑定到一个或者多个角色，不同角色可以配置不同的 IP 角色绑定规则。对于绑定到多个角色且多个角色有相应的 IP 角色绑定规则的用户， 设备会对 IP 角色绑定规则进行顺序查找，然后按照查找到的相匹配的第一条规则为用户分配地址。默认情况下，系统会将新创建的规则放到所有规则的末尾， 管理员可以移动已有的 IP 角色绑定规则从而改变规则的排列顺序。改变规则的排列顺序，在 SSL VPN 地址池配置模式下使用以下命令:

move *role-name1* {**before** *role-name2* | **after** *role-name2*| **top** | **bottom**}

- *role –name1* – 指定被移动的 IP 角色绑定规则的角色名称。
- **before** *role-name2* – 将 IP 角色绑定规则移动到某个 IP 角色绑定规则(角色名称为 role-name2 的规则)之前。
- **after** *role-name2* – 将 IP 角色绑定规则移动到某个 IP 角色绑定规则(角色名称为role-name2 的规则)之后。
- **top** – 将 IP 角色绑定规则移动到所有 IP 角色绑定规则之首。
- **bottom** – 将 IP 角色绑定规则移动到所有 IP 角色绑定规则的末尾。

配置 DNS 服务器

配置DNS 服务器，在 SSL VPN 地址池配置模式下使用以下命令：

dns *address1* [*address2*] [*address3*] [*address4*]

- *address1* – 指定 DNS 服务器 IP 地址。用户最多可配置 4 个 DNS 服务器。

在 SSL VPN 地址池配置模式下使用该命令 no 的形式取消对 DNS 服务器的指定：

no dns

配置 WINS 服务器

配置 WINS 服务器，在 SSL VPN 地址池配置模式下使用以下命令：

wins *address1* [*address2*]

- *address1* – 指定 WINS 服务器 IP 地址。用户最多可配置两个 WINS 服务器。

在 SSL VPN 地址池配置模式下使用该命令 no 的形式取消对 WINS 服务器的指定：

no wins

显示 SSL VPN 地址池信息

显示 SSL VPN 地址池信息，在任何模式下使用以下命令：

show scvpn pool [*pool-name*]

- *pool-name* – 指定 SSL VPN 地址池名称以显示指定的地址池信息。如果不指定该参数值，系统将显示所有已配置的 SSL VPN 地址池信息。

以下是显示 SSL VPN 地址池具体信息的命令示例：

```
hostname(config)# show scvpn pool pool_test1
```

```
Name: pool_test1
Address range: 3.3.3.1 - 3.3.3.10 （地址池IP 地址范围）
Exclude range: 3.3.3.1 - 3.3.3.2 （保留地址池地址范围）
Netmask: 255.255.255.0 （地址池网络掩码）
Wins server: （WINS 服务器信息）
wins1: 10.1.1.1
Dns server: （DNS 服务器信息）
dns1: 10.10.209.1
IP Binding User: （IP 用户绑定信息）
test 3.3.3.8
IP Binding Role: （IP 角色绑定信息）
role1 3.3.3.3 3.3.3.7
```

显示 SSL VPN 地址池统计信息，在任何模式下使用以下命令：

show scvpn pool *pool-name* **statistics**

- *pool-name* – 指定 SSL VPN 地址池名称以显示指定的地址池统计信息。

以下是显示 SSL VPN 地址池统计信息的命令示例：

```
hostname(config)# show scvpn pool pool_test1 statistics
Total Ip Num 10 （地址池中IP 地址总数）
Exclude Ip Num 2 （保留IP 地址个数）
Fixed Ip Num 6 （绑定IP 地址个数）
Used Ip Num 2 （已分配IP 地址个数）
Fixed Used Ip Num 0 （已分配绑定IP 地址个数）
Free Ip Num 6 （可用地址个数）
```

资源列表配置

资源列表是指系统中配置的用户可便捷访问的资源，其中每个资源又包含多个资源条目。资源条目的展现形式为“资源条目名称+对应的 URL“。SSL VPN 用户登录认证通过后，认证服务器将该用户所属的用户

组信息发送给 SSL VPN 服务器，然后服务器会根据配置的 SSL VPN 实例中用户组和资源的绑定关系，把该用户可访问的内网资源列表发送给 SSL VPN 客户端，客户端对接收到的资源列表信息进行分析并展示在用户系统自带的 IE 浏览器弹出的页面中，用户可以通过点击 URL 链接直接访问内网资源。需要注意的是，该资源列表页面只在认证通过后显示一次。如果登录的用户不属于任何用户组，认证成功后浏览器不会弹出资源列表页面。

配置 SSL VPN 资源，在全局配置模式下，使用以下命令：

scvpn resource-list *list-name*

- *list-name* – 指定资源的名称。取值范围是 1 到 31 个字符。

执行该命令后，系统进入 SSL VPN 资源列表配置模式，用户可以继续为该新建资源配置资源条目。在全局配置模式下，使用该命令 no 的形式删除指定的资源：

no resource-list *list-name*

- 配置的资源数目不能超过 48。
- SSL VPN 的资源列表功能仅适用于 Windows 的 SSL VPN 客户端。

添加资源条目

每个资源中可以添加的资源条目数量为 0~48。所有资源中包含的资源条目的总数不能超过 48 条。在 SSL VPN 资源列表配置模式下，为新建资源添加资源条目：

name *name* **url** *url-string*

- *name* – 指定资源条目的名称。取值范围是 1 到 63 个字符。
- *url-string* – 指定资源条目所对应的 URL。取值范围是 1 到 255 个字符。

在 SSL VPN 资源列表配置模式下，使用以下命令删除指定的资源条目：

no name *name*

查看资源列表

用户可以在任何模式下，使用以下命令查看资源列表的配置信息：

show scvpn resource-list [*list-name*]

- *list-name* – 指定要查看的资源的名称。取值范围是 1 到 31 个字符。如果不指定该参数，则显示所有资源的配置信息。

UDP 端口号配置

配置 SSL VPN 连接采用的UDP 端口号，在全局配置模式下，使用以下命令：

scvpn-udp-port *port-number*

- *port-number* – 指定 UDP 端口号。默认值是 4433。取值范围是 1 到 65535。

执行该命令后，所有配置的 SSL VPN 实例均采用此UDP 端口号进行数据连接。

在全局配置模式下使用该命令 no 的形式恢复默认UDP 端口号：

no scvpn-udp-port

配置空闲时间

空闲时间指客户端与设备端在无流量状态下能够保持连接状态的最长时间，超出空闲时间后，设备端将断开与客户端的连接。

默认情况下，空闲时间为 30 分钟。配置设备的空闲时间，请在 SCVPN 隧道配置模式下，使用以下命令：

idle-time *time*

- *time* – 指定设备的空闲时间，单位为分钟，取值范围是 1 到 1500 分钟。

使用 **no idle-time** 命令删除设备的空闲时间。

SSL VPN 实例配置

创建 SSL VPN 实例，在全局配置模式下，使用以下命令：

tunnel scvpn *instance-name*

- *instance-name* – 指定 SSL VPN 实例的名称。

执行该命令后，系统创建指定名称的 SSL VPN 实例，并且进入 SSL VPN 实例配置模式；如果指定的名称已存在，则直接进入 SSL VPN 实例配置模式。在全局配置模式下，使用该命令no 的形式删除指定的 SSL VPN 实例：

no tunnel scvpn *instance-name*

在 SSL VPN 实例配置模式下，用户可以进行如下配置：

- 指定地址池
- 指定设备端接口
- 指定 SSL 协议

- 指定 PKI 信任域
- 指定隧道密码
- 指定 AAA 服务器
- 指定 HTTPS 端口号
- 配置防重放功能
- 配置分片功能
- 配置空闲时间
- 配置用户同名登录功能
- 配置 URL 重定向功能
- 配置 SSL VPN 隧道路由
- 启用/禁用清除 SSL VPN 桌面版客户端缓存数据功能
- 在 HA Peer 模式中使用 SSL VPN
- 绑定 L2TP VPN 实例
- 绑定资源
- 开启/关闭浏览器登录功能

指定地址池

为 SSL VPN 实例指定 SSL VPN 地址池，在 SSL VPN 实例配置模式下，使用以下命令：

pool *pool-name*

- *pool-name* – 指定已配置的 SSL VPN 地址池名称。

在 SSL VPN 实例配置模式下使用该命令 no 的形式取消地址池的指定：

no pool

指定设备端接口

客户端通过 HTTPS 协议访问设备端接口。指定设备端 SSL VPN 接口，在 SSL VPN 实例配置模式下，使用以下命令：

interface *interface-name*

- *interface-name* – 指定设备端接口的名称。

在 SSL VPN 实例配置模式下使用该命令 no 的形式取消设备端接口的配置：

no interface *interface-name*

指定 SSL 协议

为 SSL VPN 指定 SSL 协议，在 SSL VPN 实例配置模式下，使用以下命令：

ssl-protocol {**sslv3** | **tlsv1** | **tlsv1.2** | **gmsslv1.0** | **any**}

- **sslv3** – 指定使用 SSLv3 协议。
- **tlsv1** – 指定使用 TLSv1 协议。
- **tlsv1.2** – 指定使用 TLSv1.2 协议。
- **gmsslv1.0** – 指定使用国密 GMSSLv1.0 协议。当协议为此选项时，PKI 信任域和加密信任域必须选择配置含有 SM2 类型密钥的信任域，加密算法建议优先选择 SM4，Hash 算法建议优先选择 SM3.
- **any** – 指定使用 SSLv2、SSLv3、TLSv1、TLSv1.1 或者 TLSv1.2 任何一种协议。此为系统默认设置。

在 SSL VPN 实例配置模式下使用该命令 no 的形式恢复 SSL 协议的默认值：

no ssl-protocol

如果设备端指定的 SSL 协议类型为tlsv1.2 或者 any，在 SSL VPN 客户端进行数字证书认证前，需要用户将要导入到浏览器中的软证书或者 USB Key 中的.pfx 格式证书进行处理，使得证书能够支持tlsv1.2 协议，以便用户在使用“用户名/密码+数字证书”或者“数字证书”认证方式进行认证时，能够连接成功。处理 证书前，请先准备一台安装了OpenSSL1.0.1 版本及以上的 PC（Windows 或 Linux 系统均可）。以文件名称为 oldcert.pfx 的证书为例，处理步骤如下：

1. 在 OpenSSL 软件界面中，输入以下命令将.pfx 格式的证书转换为.pem 格式的证书。openssl pkcs12 – in oldcert.pfx – out cert.pem
2. 继续输入下面的命令将.pem 格式的证书转换为支持tlsv1.2 的.pfx 格式证书。openssl pkcs12 – export – in cert.pem – out newcert.pfx – CSP “Microsoft Enhanced RSA and AES Cryptographic Provider”
3. 将新生成的.pfx 格式证书导入到浏览器或者 USB Key。

上述操作完成后，请使用 1.4.6.1239 及以上版本的 SSL VPN 客户端进行登录。当配置使用国密标准的 SSL VPN 功能时，PC 端需安装支持国密标准的 SSL VPN 客户端（当前支持国密标准的 Windows 客户端版本为 1.4.7.1252），并且使用“国密 SSL”相关登录模式进行登录。

指定 PKI 信任域

此处指定的 PKI 信任域用于 HTTPS 访问认证。为SSL VPN 指定PKI 信任域，在 SSL VPN 实例配置模式下，使用以下命令：

trust-domain *trust-domain-name*

- *trust-domain-name* – 指定系统中已配置的 PKI 信任域的名称。默认信任域为 trust_domain_default。

在 SSL VPN 实例配置模式下使用该命令 no 的形式恢复信任域的默认配置：

no trust-domain

{b}提示: {/b}关于如何创建 PKI 信任域，请参阅《用户认证》的“PKI 配置”部分。

指定加密信任域

此处为 SSL VPN 指定加密信任域，加密信任域用于国密 SSL 协商。在 SSL VPN 实例配置模式下，使用以下命令：

trust-domain-enc *enc-cert*

- *enc-cert* – 指定系统预定义的用于国密 SSL 协商的加密信任域的名称。

在 SSL VPN 实例配置模式下使用该命令 no 的形式删除加密信任域的配置：

no trust-domain-enc

指定隧道密码

隧道密码包括加密算法和验证算法。为 SSL VPN 指定隧道密码，在 SSL VPN 实例配置模式下，使用以下命令：

tunnel-cipher encryption {**null** | **des** | **3des** | **aes** | **aes192** | **aes256** | **sm4**} **hash** {**null** | **md5** | **sha** | **sha256** | **sha384** | **sha512** | **sm3**} [**compression defl**]

- **null** | **des** | **3des** | **aes** | **aes192** | **aes256** | **sm4** – 指定加密算法。默认加密算法为 3des。null 表示不使用加密功能。关于加密算法的详细描述，请参阅“加密算法”。
- **null** | **md5** | **sha** | **sha256** | **sha384** | **sha512**| **sm3** – 指定验证算法。默认验证算法为 sha。null 表示不使用验证功能。关于验证算法的详细描述，请参阅“验证算法”。
- **compression defl** – 指定 DEFLATE 压缩算法。默认无压缩算法。关于压缩算法的详细描述，请参阅“压缩算法”。

在 SSL VPN 实例配置模式下使用该命令 no 的形式恢复加密算法和验证算法的默认值并取消压缩算法的配置：

no tunnel-cipher

指定 AAA 服务器

此处指定的 AAA 服务器为进行客户端用户身份认证的 AAA 服务器。指定 AAA 服务器，在 SSL VPN 实例配置模式下，使用以下命令：

aaa-server *aaa-server-name* [**domain** *domain-name*] [**keep-domain-name**]

- aaa-server-name – 指定 AAA 服务器的名称。
- **domain** *domain-name* – 为 AAA 服务器指定域名以区分不同的AAA 服务器。
- **keep-domain-name** – 指定该参数后， 用于身份认证的用户名将验证域名。

在 SSL VPN 实例配置模式下使用该命令 no 的形式取消对 AAA 服务器的指定：

no aaa-server *aaa-server-name* [**domain** *domain-name*]

指定 HTTPS 端口号

HTTPS 端口号用于客户端访问设备端时使用。指定 HTTPS 端口号，在 SSL VPN 实例配置模式下，使用以下命令：

https-port *port-number*

- *port-number* – 指定 HTTPS 端口号。默认值是 4433。取值范围是 1 到 65535。为避免与 WebUI 使用的 HTTPS 端口号相冲突，建议用户不要把 HTTPS 端口号设置为 443。绑定到同一个接口的 SSL VPN 实例需配置不同的HTTPS 端口号。

在 SSL VPN 实例配置模式下使用该命令 no 的形式恢复默认 HTTPS 端口号：

no https-port

配置 SSL VPN 隧道路由

SSL VPN 隧道路由是指通过 SSL VPN 隧道到指定网段/域名的路由。SSL VPN 客户端接收到指定网段后，生成到达指定网段的路由条目；接收到指定域名后，根据域名解析结果，生成到达域名所在地址的路由条目。

指定网段

使用网段方式配置 SSL VPN 隧道路由，在 SSL VPN 实例配置模式下，使用以下命令：

split-tunnel-route *ip-address/netmask* [**metric** *metric-number*]

- *ip-address/netmask* – 指定目的地址和掩码。
- **metric** *metric-number* – 指定路由的度量值。默认值是 35。取值范围是 1 到 9999。

用户可以配置多条该命令添加多条路由。

在 SSL VPN 实例配置模式下使用该命令 no 的形式删除指定的路由：

no split-tunnel-route *ip-address/netmask* [**metric** *metric-number*]

指定域名

使用域名方式配置 SSL VPN 隧道路由后，系统将域名下发给客户端。客户端根据域名解析结果，生成到达域名所在地址的路由条目。指定域名，在 SSL VPN 实例配置模式下，使用以下命令：

domain-route {**disable** | **enable** | **max-entries** *value* | *url*}

- **disable** – 不下发域名到客户端。此为系统默认设置。
- **enable** – 下发域名到客户端。
- **max-entries** *value* – 指定客户端可以根据域名解析后地址所生成的最大路由条目数。默认值是 1000，取值范围是 1 到 10000。
- *url* – 指定域名。每次可添加一个，支持最多 64 个域名。每个域名的字符串长度不得超过 63 个字符。域名末尾不能为“.”，不支持通配符，且不支持过于宽泛的 URL，比如：“.com”、“com”。

在 SSL VPN 实例配置模式下使用该命令 no 的形式删除指定的路由：

no domain-route *url*

配置防重放功能

防重放（anti-replay）指防止恶意用户通过重复发送捕获到的数据包所进行的攻击，即接收方会拒绝旧的或重复的数据包。配置防重放功能，在 SSL VPN 实例配置模式下，使用以下命令：

anti-replay {**32** | **64** | **128** | **256** | **512**}

- **32** – 指定防重放的窗口为 32。该数值为系统的默认数值。
- **64** – 指定防重放的窗口为 64。
- **128** – 指定防重放的窗口为 128。
- **256** – 指定防重放的窗口为 256。
- **512** – 指定防重放的窗口为 512。

在网络状况较差时，例如存在严重乱序现象等，请选择较大的窗口。

在 SSL VPN 实例配置模式下使用该命令 no 的形式恢复默认防重放窗口：

no anti-replay

配置分片功能

用户可以指定是否允许转发设备将包进行分片处理。配置分片功能，在 SSL VPN 实例配置模式下，使用以下命令：

df-bit {copy | clear | set}

- copy – 直接从发包端拷贝 IP 包的 DF 选项。该选项为系统默认选项。
- clear – 允许转发设备对包做分片处理。
- set – 不允许转发设备对包做分片处理。

在 SSL VPN 实例配置模式下使用该命令 no 的形式恢复系统的默认设置：

no df-bit

配置空闲时间

空闲时间指客户端与设备端在无流量状态下能够保持连接状态的最长时间，超出空闲时间后，设备端将断开与客户端的连接。配置空闲时间，在 SSL VPN 实例配置模式下，使用以下命令：

idle-time *time-value*

- *time-value* – 指定空闲时间，单位为分钟。默认值是 30 分钟。取值范围是 15 到 1500 分钟。

在 SSL VPN 实例配置模式下使用该命令 no 的形式恢复空闲时间的默认值：

no idle-time

配置用户同名登录功能

用户同名登录功能指允许同一个用户在多个地点同时登录认证。开启用户同名登录功能，在 SSL VPN 实例配置模式下，使用以下命令：

allow-multi-logon

执行该命令后，开启用户同名登录功能，并且不对同一用户名的登录次数做限制。用户可以在 SSL VPN 实例配置模式下通过使用以下命令指定用户同名登录次数：

allow-multi-logon number *number*

- *number* – 指定用户同名登录次数。范围是 1 到 99999999。

在 SSL VPN 实例配置模式下使用以下命令 no 的形式关闭用户同名登录功能：

no allow-multi-logon

配置 URL 重定向功能

URL 重定向功能是指在SSL VPN 设备端配置重定向的URL，客户端认证成功后将自动跳转到指定 URL 的页面。默认情况下，URL 重定向功能是关闭的。配置 URL 重定向功能，在 SSL VPN 实例配置模式下，使用以下命令：

redirect-url *url* **title-en** *name* **title-zh** *name*

- *url* – 指定认证成功后，客户端自动跳转页面的 URL，取值范围为 1 到 255 字节。系统支持 HTTP（http://）和 HTTPS（https://）两种类型的 URL。
- **title-en** *name* – 指定重定向 URL 的英文描述，范围为 1 到 31 字节。当客户端PC 为英文操作系统时，该名称会在客户端菜单项中显示。
- **title-zh** *name* – 指定重定向 URL 的中文描述，范围为 1 到 63 字节。当客户端PC 为中文操作系统时，该名称会在客户端菜单项中显示。建议选用支持中文输入的超级终端，当超级终端不支持中文输入时，请通过WebUI 配置该参数。

在 SSL VPN 实例配置模式下使用该命令 no 的形式取消URL 重定向功能：

no redirect-url

URL 内容格式

根据重定向页面类型的不同，StoneOS 支持内容符合下列格式的 URL 输入，以 HTTP 类型 URL 为例：

- UTF-8 编码格式的页面：输入“URL”+“username=$USER&password=$PWD”。比如，“http://www.abc.com/oa/login.do?username=$USER&password=$PWD”
- GB2312 编码格式的页面：输入“URL”+“username=$GBUSER&password=$PWD”。比如，“http://www.abc.com/oa/login.do?username=$GBUSER&password=$PWD”
- 其它页面：直接输入 URL。比如，http://www.abc.com

注意:关于 URL 重定向功能的具体实例，请参阅“URL 重定向配置举例”。

启用/禁用清除 SSL VPN 桌面版客户端主机缓存数据功能

为了保证用户 SSL VPN 桌面版客户端主机的隐私数据安全性，用户可以在 SSL VPN 桌面版客户端断开后，启用清除桌面版客户端主机缓存数据功能，清除浏览器缓存、临时文件等隐私数据。启用/禁用清除桌面版客户端主机缓存数据功能，在 SSL VPN 实例配置模式下，使用以下命令：

- 启用：**host-cache-clear enable**

- 禁用：**host-cache-clear disable**

在 HA Peer 模式中使用 SSL VPN

在 HA Peer 模式的网络环境中，分别在两台设备上配置正确有效的 SSL VPN。当一台主设备或者其上下链路出现故障时，SSL VPN 客户端可以重新连接到另外一台主设备。用户需要指定重连地址列表。SSL VPN 客户端将根据重连地址列表中地址的优先级进行重连。若重连失败，将会循环尝试列表中的地址，直到连接成功。用户可最多指定四个重连地址。四个重连地址按配置先后顺序进行优先级排列。先配置的重连地址具有较高优先级。配置重连地址列表，在 SSL VPN 实例配置模式下，使用如下命令：

cluster { **ip** *A.B.C.D* | **domain** *url* } [**port** *port-number*] [{ **ip** *A.B.C.D* | **domain** *url* } [**port** *port-number*]] [{ **ip** *A.B.C.D* | **domain** *url* } [**port** *port-number*]] [{ **ip** *A.B.C.D* | **domain** *url* } [**port** *port-number*]]

- **ip** *A.B.C.D* | **domain** *url* – 指定用于 SSL VPN 连接的服务器 IP 地址或者域名。
- **port** *port-number* – 指定用于 SSL VPN 连接的端口号。默认值是 4433。

使用 **no cluster** 命令清除以上配置。

在使用此功能时，需要注意以下事项：

- 当 SSL VPN 客户端选择<自动重连>选项且用户通过 client-auto-connect count 命令在服务器端设置自动重连次数为 unlimited 时，SSL VPN 客户端将连接之前指定的连接地址，不会连接重连地址列表中的地址；当用户通过命令设置自动重连次数为X 次时，SSL VPN 客户端将在 X 次连续重连失败后，使用重连地址列表中的地址进行重连。
- 当 SSL VPN 客户端不选择<自动重连>选项时，无论服务器端的配置如何，SSL VPN 客户端将直接使用地址重连列表中的地址进行重连。
- 当使用支持此功能的系统固件时，如果服务器端没有配置重连地址列表，低于 1.4.4.1207 版本的SSL VPN 客户端可正常连接 SSL VPN 服务器端。StoneOS 会提示用户存在新版本的 SSL VPN 客户端。如果服务器端配置重连地址列表，当低于 1.4.4.1207 版本的 SSL VPN 客户端连接 SSL VPN 服务器端时，StoneOS 会提示用户进行升级。用户需要手动卸载旧版本的 SSL VPN 客户端，然后登陆SSL VPN 的 Web 登陆界面进行 SSL VPN 客户端的下载与安装。新版本的 SSL VPN 客户端可与不支持此功能的系统固件兼容。

绑定 L2TP VPN 实例

在使用 iOS 的 SSL VPN 客户端与 SSL VPN 服务器进行连接时，需要为 SSL VPN 实例绑定 L2TP VPN 实例且此实例需引用 IPSec 隧道。进行绑定配置，在 SSL VPN 实例配置模式下，使用以下命令：

client-bind-lns *tunnel-name*

- *tunnel-name* – 指定系统中已配置的 L2TP VPN 实例。此实例需要引用 IPSec 隧道。使用该命令 no 的形式取消绑定配置：**no client-bind-lns**

- 对于绑定的L2TP VPN 实例和引用的 IPSec 隧道，需要满足如下条件：
  - IPSec 隧道的认证方式需要使用预共享密钥认证。
  - L2TP 实例的隧道密码（通过 secret secret-string 指定）需要与IPSec 隧道的预共享密钥一致。
  - L2TP 实例与 SSL VPN 实例指定的AAA 服务器需要一致。
  - L2TP 实例的地址池需要正确配置，设备根据 L2TP 实例的地址池为 iOS 的 SSL VPN 客户端下发相关地址。

绑定资源

配置资源和用户组的绑定关系后，SSL VPN 客户端才能在用户认证成功后将其可访问的资源列表显示在 IE 浏览器的页面中。一个用户组可以绑定多个资源，一个资源也可以绑定多个用户组。一个 SSL VPN 实例中最多可以配置 32 个绑定条目。

配置资源和用户组的绑定条目，在 SSL VPN 实例配置模式下，使用以下命令：

bind resource-list *list-name* **user-group** *aaa-server-name group-name*

- *list-name* – 指定资源的名称。取值范围是 1 到 31 个字符。
- *aaa-server-name* – 指定用户组所属的认证服务器的名称。目前仅支持本地认证服务器和 RADIUS 认证服务器。
- *group-name* – 指定用户组的名称。

在 SSL VPN 实例配置模式下，使用以下命令可以取消指定的资源和用户组的绑定关系：

no bind resource-list *list-name* **user-group** *aaa-server-name group-name*

开启/关闭浏览器登录功能

浏览器登录功能指通过浏览器 Web 页面的方式登录 SSL VPN。默认情况下，该功能为开启状态。当关闭该功能后，用户只能通过客户端方式登录 SSL VPN。

开启浏览器登录功能，在 SSL VPN 实例配置模式下，使用以下命令：

web-login enable

关闭浏览器登录功能，在 SSL VPN 实例配置模式下，使用以下命令：

web-login disable

绑定 SSL VPN 实例到隧道接口

配置好的 SSL VPN 实例需要绑定到隧道接口，才能够生效。绑定 SSL VPN 实例到隧道接口，在隧道接口配置模式下，使用以下命令：

tunnel scvpn *instance-name*

- *instance-name* – 指定系统中已配置的 SSL VPN 实例的名称。

在隧道接口配置模式下使用该命令 no 的形式取消隧道接口与 SSL VPN 实例的绑定：

no tunnel scvpn *instance-name*

配置客户端 USB Key 证书认证

设备支持客户端 USB Key 证书认证。只要用户持有的 USB Key 支持标准的 Windows SDK （Certificate Store Functions），并且存储合法的证书，就能通过认证进而实现网络连通的目的。

USB Key 证书认证功能支持以下两种认证方式：

- 用户名/密码 + USB Key：SSL VPN 用户需要持有存储正确数字证书的 USB Key，并且在登录时输入正确的用户名、密码和USB Key 用户口令，才能通过认证；
- 只用 USB Key：SSL VPN 用户需要持有存储正确数字证书的 USB Key，并且在登录时输入正确的 USB Key 用户口令，即可通过认证，无需输入用户名和密码。

实现 USB Key 证书认证功能，用户需在设备端配置以下功能：

- 开启 USB Key 证书认证功能
- 导入 USB Key 证书相应 CA 证书到信任域
- 配置 USB Key 证书相应 CA 证书的信任域

开启 USB Key 证书认证功能

默认情况下，设备端的 USB Key 证书认证功能为关闭状态，用户可以在 SSL VPN 实例配置模式下使用以下命令开启 USB Key 证书认证功能：

client-cert-authentication [**usbkey-only**]

- **usbkey-only** – 指定 USB Key 证书认证方式为“只用USB Key”。如不指定该参数，认证方式为“用户名/密码+ USB Key”。

在 SSL VPN 实例配置模式下使用该命令 no 的形式关闭USB Key 证书认证功能：

no client-cert-authentication [**usbkey-only**]

导入 USB Key 证书相应 CA 证书到信任域

用户可以通过多种方式（FTP、TFTP 和 USB）实现 CA 证书到信任域的导入。在执行模式下使用以下命令：

import pki *trust-domain-name* **cacert from** {**ftp server** *ip-address* [**user** *user-name* **password** *password*] | **tftp server** *ip-address* | **usb0** | **usb1**} *file-name*

- *trust-domain-name* – 指定 PKI 信任域的名称。
- **ftp server ip-address** [**user** *user-name* **password** *password*] – 指定FTP 服务器的 IP 地址以及访问服务器使用的用户名和密码。当不输入用户名和密码时表示采用匿名登录方式。
- **tftp server** *ip-address* – 指定 TFTP 服务器的 IP 地址。
- **usb0 | usb1** – 指定通过 USB 方式从 usb0 或者 usb1 插槽所对应的 U 盘根目录导入CA 证书。
- *file-name* – 指定要导入的CA 证书的文件名。

配置 USB Key 证书相应 CA 证书的信任域

设备端开启客户端 USB Key 证书认证功能后，还需要指定用户证书相应的 CA（Certification Authority）的信任域。客户端所提交的证书匹配到其中任意一个信任域的CA 证书，都会认证成功。在 SSL VPN 实例配置模式下，使用以下命令：

client-auth-trust-domain *trust-domain*

- *trust-domain* – 指定 CA 证书所在的PKI 信任域，该信任域需已经创建。

如果需要配置多个信任域，需重复使用本命令。系统最多可以支持 10 个信任域。

在 SSL VPN 实例配置模式下使用该命令 no 的形式取消对PKI 信任域的指定：

no client-auth-trust-domain *trust-domain*

配置主机验证功能

主机验证功能是指 SSL VPN 实例对运行 SSL VPN 客户端的主机进行验证。用户在PC 上通过 SSL VPN 客户端登录时，客户端先收集主机的主板序列号、硬盘序列号、CPU ID 和 BIOS 序列号，然后客户端对这些信息进行 MD5 运算，生成一个 32 位的字符串，即主机 ID。之后，客户端将主机 ID 以及用户名密码信息发送到 SSL VPN 设备端进行验证。SSL VPN 设备端根据候选表和绑定表中记录表项以及主机验证配置进行验证。候选表和绑定表描述如下：

- 候选表：客户端首次登录时，SSL VPN 设备端会记录用户名与主机 ID 的对应关系，并加入候选表中。
- 绑定表：绑定表中包含允许验证通过的主机 ID 与用户名对应关系的表项。用户可以通过手工操作或首次登录自动批准方式把候选表中的表项移入绑定表中。客户端登录时，SSL VPN 设备端会先检查绑定表中是否有该主机 ID 与用户名的对应关系表项，如果有，则通过主机验证，继续进行用户名密码验证；如果没有，则直接中断 SSL 通讯过程。

开启主机验证功能

默认情况下，设备端的主机验证功能处于关闭状态。在 SSL VPN 实例配置模式下，使用以下命令开启主机验证功能：

user-host-verify [**allow-multi-host**] [**allow-shared-host**] [**auto-approved-first-bind**]

- **user-host-verify** – 开启主机验证功能。默认情况下，仅允许一个用户通过一台主机登录，即用户名和主机一一对应。
- **allow-multi-host** – 允许一个用户通过多台主机登录。
- **allow-shared-host** – 允许多个用户通过一台主机登录。
- **auto-approved-first-bind** – 用户首次登录时自动把用户名和主机 ID 的对应关系加入绑定表。

在 SSL VPN 实例配置模式下使用该命令 no 的形式关闭主机验证功能：

no user-host-verify

批准候选表项

批准候选表项是把候选表中的主机 ID 与用户名的对应关系表项移到绑定表中。在任意模式下，使用以下命令批准指定的候选表项：

exec scvpn *instance-name* **approve-binding user** *user-name* **host** *host-id*

- **scvpn** *instance-name* – 指定 SSL VPN 实例的名称。
- **user** *user-name* – 指定候选表项对应的用户名称。
- **host** *host-id* – 指定候选表项对应的主机 ID。

配置超级用户

超级用户不受主机验证功能限制，可以通过任意主机登录。在任意模式下使用以下命令配置候选表或者绑定表中的用户为超级用户：

exec scvpn *instance-name* **no-host-binding-check user** *user-name*

- **scvpn** *instance-name* – 指定 SSL VPN 实例的名称。
- **user** *user-name* – 指定超级用户的用户名称。

使用以下命令取消超级用户配置：

exec scvpn *instance-name***host-binding-checkuser** *user-name*

配置共享主机

通过共享主机登录的用户不受主机验证功能限制。在任意模式下使用以下命令配置候选表或者绑定表中的主机为共享主机：

exec scvpn *instance-name* **no-user-binding-check host** *host-id*

- **scvpn** *instance-name* – 指定 SSL VPN 实例的名称。
- **host** *host-id* – 指定共享主机的主机 ID。该主机 ID 需要为候选表或者绑定表中的主机 ID。

使用以下命令取消共享主机配置：

no exec scvpn *instance-name* **no-user-binding-check host** *host-id*

增加/减少预批准主机数

当允许一个用户通过多台主机登录且设置了用户首次登录自动批准用户名和主机 ID 的绑定关系时，默认情况下，仅自动批准用户和首次登录主机 ID 的绑定关系表项，即仅批准一个主机 ID，以后登录的主机 ID 进入候选表。在任意模式下，使用以下命令增加/减少预批准主机数：

exec scvpn *instance-name* **increase-host-binding user** *user-name number*

- **scvpn** *instance-name* – 指定 SSL VPN 实例的名称。
- **user** *user-name* – 指定用户名称。
- *number* – 指定增加的预批准主机数。取值范围为 1 到 32。系统将在原预批准主机数的基础上进行增加。单个用户的预批准主机数的总数范围为 0 到 100。

exec scvpn *instance-name* **decrease-host-binding user** *user-name number*

- **scvpn** *instance-name* – 指定 SSL VPN 实例的名称。
- **user** *user-name* – 指定用户名称。
- *number* – 指定减少的预批准主机数。取值范围为 1 到 32。系统将在原预批准主机数的基础上进行减少。单个用户的预批准主机数的总数范围为 0 到 100。

清除绑定表

在任意模式下，使用以下命令清除绑定表或指定的绑定表项：

exec scvpn *instance-name* **clear-binding** [{**user** *user-name* [**host** *host-id*] | **host** *host-id* }]

- **scvpn** *instance-name* – 指定 SSL VPN 实例的名称。
- **user** *user-name* – 指定用户名称。如果不指定 Host ID，则删除指定用户的所有绑定表项。

- **host** *host-id* – 指定主机 ID。

导出/导入绑定表

用户可以通过FTP、TFTP 或 USB 方式实现绑定表的导出或导入。在执行模式下使用以下命令导出绑定表：

export scvpn user-host-binding to {**ftp server** ip-address [**user** user-name **password** password] | **tftp server** ip-address | **usb0** | **usb1**} [**file-name**]

- **ftp server** *ip-address* [**user** *user-name* **password** *password*] – 指定通过FTP 方式导出绑定表。**user** *user-name* **password** *password* 指定 FTP 服务器的 IP 地址以及访问服务器使用的用户名和密码，当不指定用户名和密码时表示采用匿名登录方式。
- **tftp server** *ip-address* – 指定通过 TFTP 方式导出绑定表。*ip-address* 指定 TFTP 服务器的 IP 地址。
- **usb0 | usb1** – 指定将绑定表导出到 U 盘根目录。
- *file-name* – 指定导出的绑定表的文件名称。默认名称为 scvpn_bind_file。

在执行模式下，使用以下命令导入绑定表：

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

- **ftp server** *ip-address* [**user** *user-name* **password** *password*] – 指定通过FTP 方式导入绑定表。**user** *user-name* **password** *password* 指定 FTP 服务器的 IP 地址以及访问服务器使用的用户名和密码，不指定用户名和密码时表示采用匿名登录方式。
- **tftp server** *ip-address* – 指定通过 TFTP 方式导入绑定表。*ip-address* 指定 TFTP 服务器的 IP 地址。
- **usb0 | usb1** – 指定从U 盘根目录导入绑定表。
- *file-name* – 指定要导入的文件名。

配置主机安全检测功能

主机安全检测功能是指 SSL VPN 实例对运行 SSL VPN 客户端主机的安全状况进行检测，通过检查客户端主机的操作系统、IE 版本以及特定软件的安装情况等因素来评估客户端主机的安全级别，并根据不同安全级别为客户端分配不同的资源访问权限，保证 SSL VPN 接入的安全性。

主机安全检测内容

设备主机安全检测功能对客户端主机的详细检查内容，请参见下表：

检查项目	详细描述
操作系统配置	•操作系统版本（如 Windows 2000、Windows 2003、Windows XP、Windows Vista 等） •操作系统补丁包版本（如 Service Pack 1 等） •Windows 特定补丁包是否安装（如 KB958215 等）
	•Windows 安全中心和自动升级是否打开 • 防病毒软件是否必须安装，实时监控和病毒特征库在线升级是否打开 •防间谍软件是否必须安装，实时监控和特征库在线升级是否打开 • 个人防火墙是否必须安装和实时保护是否打开
其他配置	IE 版本和安全级别是否达到指定标准 指定进程是否正在运行 指定服务是否已经安装 指定服务是否正在运行 指定注册表条目是否存在 指定文件是否存在于操作系统中

基于角色的访问控制和主机安全检测流程

基于角色的访问控制是指用户的权限不是由用户名而是由用户在系统中的角色决定的，一个登录于某系统的用户，可以通过它所对应角色的权限来决定其可以访问的系统资源。在权限管理中，角色作为中间桥梁把用户和权限联系起来。

设备 SSL VPN 在主机安全检测流程中实现了基于角色的访问控制，在安全检测策略规则中引入初级角色和次级角色的概念。初级角色主要用于用户从设备端获取对应的安全检测Profile（包含主机安全检测的内容以及安全级别，可通过 WebUI 进行配置）以及决定检测成功用户的实际访问权限；次级角色决定检测失败用户的实际访问权限。关于角色配置与安全检测结果之间的关系，请参见本章配置主机安全检测策略规则中的表 7：主机安全检测策略规则配置和检测结果以及权限授予对应列表。

主机安全检测流程如下：

1.客户端发起连接请求并成功认证。

2.设备端下发安全检测 Profile 到客户端。

3.客户端根据安全检测 Profile 对主机系统进行相应的安全检测。

4.客户端将最终检测结果返回给设备端。

5. 如果安全检测成功，设备端根据配置的安全检测策略规则中的初级角色授予用户实际访问权限；如果安全检测失败，设备端断开检测失败客户端的连接并给出提示或者根据配置的安全检测策略规则中的次级角色授予用户实际访问权限。

另外， 设备主机安全检测功能还支持动态的访问权限控制。一方面，当设备端的安全状况发生变化时， 设备端会主动下发Profile 给客户端，并要求客户端重新进行安全检测；另一方面，客户端可以周期性地进行安全检查，比如可以定时地检查客户端主机的防病毒软件是否开启，如果用户在使用过程中关闭了防病毒软件，系统可能会因此在用户的访问过程中改变该用户所属的角色，重新为该用户分配相应的权限。

配置主机安全检测 Profile

主机安全检测Profile 指定主机安全检查的内容以及安全级别。用户可以通过 WebUI 和 CLI 指定安全检测 Profile 名称，但是Profile 的内容需要通过 WebUI 进行配置。指定主机安全检测 Profile，在全局配置模式下使用以下命令：

scvpn host-check-profile *hostcheck-profile-name*

- *hostcheck-profile-name* – 指定主机安全检测Profile 的名称。执行该命令后，系统创建指定名称的主机安全检测Profile。

在全局配置模式下，使用 **no scvpn host-check-profile** *hostcheck-profile-name* 删除指定的主机安全检测 Profile。

通过 WebUI 配置主机安全检测 Profile

用户可以通过 WebUI 配置主机安全检测Profile，指定主机安全检测内容。通过 WebUI 配置主机安全检测 Profile，按照以下步骤进行配置：

1. 访问页面“配置 > 网络> SSL VPN”，在页面右侧辅助栏的<任务>区选择『主机检测』链接进入主机检测配置页面。
2. 在该页面点击『新建』按钮，弹出<主机检测配置>对话框。
3. 依次填写或者选择各项。配置选项具体描述如下：

基本配置

- **名称：** 指定主机检测Profile 名称。
- **OS 版本：** 指定是否检测客户端主机的操作系统版本。从下拉菜单中选择合适的检测类型，包括：
  - 不检测- 不对客户端主机操作系统版本进行检测。
  - 必须匹配- 客户端主机操作系统版本必须和指定操作系统版本一致。分别在后面的下拉菜单中选择操作系统版本和操作系统补丁包版本。

- 至少 - 客户端主机操作系统版本必须高于指定操作系统版本或者和指定操作系统版本一致。分别在后面的下拉菜单中选择操作系统版本和操作系统补丁包版本。

- **补丁包x：** 指定客户端主机必须安装的特定 Windows 补丁包，在文本框中输入补丁包名称。用户最多可以为每条主机检测Profile 指定 5 个补丁包。

- **最低IE 版本：** 指定检测客户端主机 Internet zone 的 IE 版本必须高于指定版本或者和指定版本一致。选中所需选项的单选按钮。

- 最低 IE 安全级别：指定检测客户端主机的 IE 安全级别必须高于指定级别或者和指定级别一致。选中所需选项的单选按钮

高级配置

- **安全中心：** 指定检测客户端主机的 Windows 安全中心是否开启。选中<必须启用>复选框指定客户端主机必须开启 Windows 安全中心。

- **自动更新：** 指定检测客户端主机的 Windows 自动升级功能是否开启。选中<必须启用>复选框指定客户端主机必须开启 Windows 自动升级功能。

- **防病毒软件：** 指定检测客户端主机的反病毒软件是否安装，实时监控和病毒特征库更新是否打开。选项包括:

  - 安装软件- 选中该复选框指定客户端主机必须安装防病毒软件。

  - 实时监控- 选中该复选框指定客户端主机必须开启防病毒软件实时监控功能。

  - 病毒特更新- 选中该复选框指定客户端主机必须开启防病毒软件病毒特征库在线升级功能。

- **防间谍软件：** 指定检测客户端主机的防间谍软件是否安装，实时监控和特征库更新是否打开。选项包括:

  - 安装软件- 选中该复选框指定客户端主机必须安装防间谍软件。

  - 实时监控- 选中该复选框指定客户端主机必须开启防间谍软件实时监控功能。

  - 特征库更新- 选中该复选框指定客户端主机必须开启防间谍软件特征库在线升级功能。

- **防火墙：** 指定检测客户端主机的个人防火墙是否安装，实时监控是否打开。选项包括:

  - 安装软件- 选中该复选框指定客户端主机必须安装个人防火墙。

  - 实时监控- 选中该复选框指定客户端主机必须开启个人防火墙实时监控功能。

- **注册表键值x：** 指定检测客户端主机的特定注册表条目是否存在。用户最多可以为每条主机检测 Profile 指定 5 个注册表条目名称。从下拉菜单中选择合适的检测类型，包括:

  - 不检测 - 不检测特定注册表条目是否存在。

- 存在 - 客户端主机中包含指定注册表条目。在文本框中输入注册表条目名称。
- 不存在 - 指定注册表条目在客户端主机中不存在。在文本框中输入注册表条目名称。

- **文件路径名称x：** 指定检测客户端主机的特定文件是否存在。用户最多可以为每条主机检测 Profile 指定 5 个文件路径名称。从下拉菜单中选择合适的检测类型，包括：
  - 不检测 - 不检测特定文件是否存在。
  - 存在 - 客户端主机操作系统中包含指定文件。在文本框中输入文件路径名称。
  - 不存在 - 指定文件在客户端主机操作系统中不存在。在文本框中输入文件路径名称。
- **运行进程名称x：** 指定检测客户端主机的特定进程是否正在运行。用户最多可以为每条主机检测 Profile 指定 5 个进程名称。从下拉菜单中选择合适的检测类型，包括：
  - 不检测 - 不对特定进程的运行情况进行检测。
  - 存在 - 指定进程在客户端主机中正在运行。在文本框中输入进程名称。
  - 不存在 - 指定进程在客户端主机中没有运行。在文本框中输入进程名称。
- **安装服务名称x：** 指定检测客户端主机的特定服务是否已经安装。用户最多可以为每条主机检测 Profile 指定 5 个服务名称。从下拉菜单中选择合适的检测类型，包括：
  - 不检测 - 不对特定服务的安装情况进行检测。
  - 存在 - 指定服务在客户端主机中已经安装。在文本框中输入服务名称。
  - 不存在 - 指定服务在客户端主机中没有安装。在文本框中输入服务名称。
- **运行服务名称x：** 指定检测客户端主机的特定服务是否正在运行。用户最多可以为每条主机检测 Profile 指定 5 个服务名称。从下拉菜单中选择合适的检测类型，包括：
  - 不检测 - 不对特定服务的运行情况进行检测。
  - 存在 - 指定服务在客户端主机中正在运行。在文本框中输入服务名称。
  - 不存在 - 指定服务在客户端主机中没有运行。在文本框中输入服务名称。

4.配置完成，点击『确定』或者『应用』按钮保存所做配置。

配置主机安全检测策略规则

主机安全检测Profile 配置完成后，只有把它引用到主机安全检测策略规则中，配置的安全检测功能才能对用户生效。配置主机安全检测策略规则，请在 SSL VPN 实例配置模式下使用以下命令：

host-check [**role** *role-name*] **profile** *profile-name* [**guest-role** *guestrole-name*] [**periodic-check** *period-time*]

- **role** *role-name* – 指定用户的初级角色，该初级角色为 AAA 服务器中已配置的用户角色。如果配置该参数，该主机安全检测Profile 对该指定角色有效；如果不配置此参数，该主机安全检测Profile 将作为缺省Profile 并对所有未指定Profile 的用户生效。
- **profile** *profile-name* – 指定绑定的主机安全检测 Profile 名称。
- **guest-role** *guestrole-name* – 指定用户的次级角色。当客户端的主机安全检测失败时，如果配置该参数，用户将获得该次级角色拥有的访问权限；如果不配置该参数，系统将断开该客户端连接。
- **periodic-check** *period-time* – 指定该用户的自动检测周期。单位为分钟，取值范围为 5 到 1440 分钟，默认值为 30 分钟。

可以配置多条该命令添加多个安全检测策略规则。当一个用户可匹配多个安全检测策略规则时，设备端会按照查找到的第一条相匹配的规则进行处理；另外，一个用户可以绑定到一个或者多个角色，当一个用户绑定到多个角色且多个角色均配置安全检测策略规则时，设备端会按照查找到的第一条相匹配的规则进行处理。

在 SSL VPN 实例配置模式下，使用 **no host-check** [**role** *role-name*] **profile** *profile-name* [**guest-role** *guestrole-name*] [**periodic-check** *period-time*]取消主机安全检测策略规则的配置。

- **role** *role-name* – 删除指定初级角色相关的安全检测Profile。若未指定初级角色和次级角色，将删除缺省主机安全检测Profile。
- **guest-role** *guestrole-name* – 在指定初级角色的前提下，删除所指定的次级角色。
- **periodic-check** *period-time* – 在指初级定角色的前提下，将指定角色所对应的自动检测周期恢复为默认值 30 分钟。

根据上述主机安全检测策略规则 CLI 描述，表 20-3 列出主机安全检测策略规则配置情况、检测结果和权限授予之间的详细对应关系：

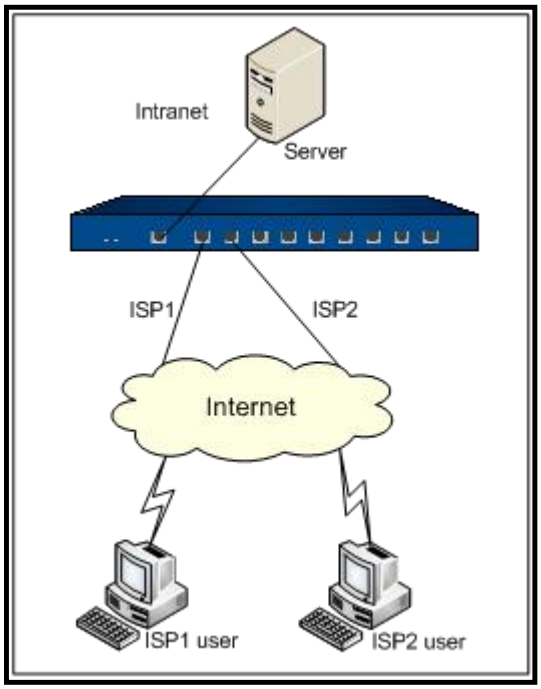
策略规则配置	检测结果	
	通过检测	未通过检测
初级角色：配置 profile：配置 次级角色：配置	获得初级角色对应访问权限	获得次级角色对应访问权限
初级角色：配置 profile：配置 次级角色：未配置	获得初级角色对应访问权限	断开连接并给出提示
初级角色：未配置 profile：配置 次级角色：配置	正常连接	获得次级角色对应访问权限

策略规则配置	检测结果	
	通过检测	未通过检测
初级角色：未配置 profile：配置 次级角色：未配置	正常连接	断开连接并给出提示

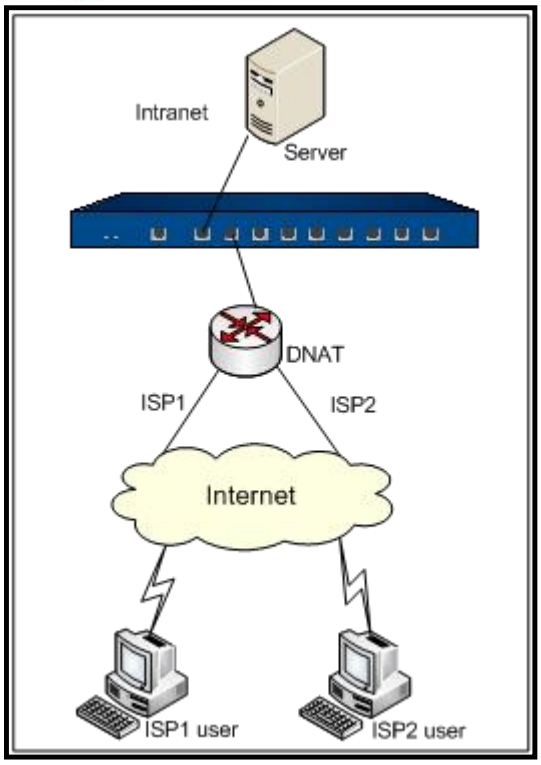
配置最优路径检测功能

目前，大规模VPN 网络往往都是跨 ISP（Internet Service Provider，互联网服务提供商）的，但是不同 ISP 间通信时带宽小、延迟大，严重影响了VPN 的应用效果。针对此问题， 设备 SSL VPN 支持最优路径检测功能，该功能能够使不同 ISP 线路接入的客户端自动选择最快线路连接到 SSL VPN 设备端，从而提高访问总部资源时的速度。

设备 SSL VPN 最优路径检测功能的网络环境实现包括以下两种:



如上图所示，SSL VPN 客户端直接访问设备端出接口地址。SSL VPN 设备端首先需要申请多条不同的 ISP 上网线路连接到 Internet，并启用相应数目的设备端接口作为 SSL VPN 通道出接口。当客户端使用不同的 ISP 上网线路访问总部资源时，如果开启了设备端检测最优通道功能，设备端设备会通过客户端的源接入地址判断其 ISP 类型，根据判断，将所有的 SSL VPN 出接口 IP 地址按照优先级重新排序并下发给客户端，由客户端选择连接的最优通道；否则，客户端通过发送 UDP 探测包自动判断最优链路，并选择连接的最优通道。



如上图所示，SSL VPN 客户端通过 DNAT 设备访问 SSL VPN 设备端，该 DNAT 设备会将客户端的访问地址映射到 SSL VPN 设备端的出接口地址。这种方式下，DNAT 设备外网端口通过多条不同的 ISP 上网线路连接到 Internet，用户需要将 DNAT 设备的外网接口地址配置为设备端地址簿中的地址条目，当客户端使用不同的 ISP 上网线路访问 DNAT 设备外网接口地址时，如果开启了设备端检测最优通道功能，设备端 设备会通过客户端的源接入地址判断其 ISP 类型，根据判断，将所有的DNAT 外网接口 IP 地址按照优先级重新排序并下发给客户端，由客户端选择连接的最优通道；否则，客户端通过发送 UDP 探测包自动判断最优链路，并选择连接的最优通道。

启用设备端接口作为 SSL VPN 通道出接口，在 SSL VPN 实例配置模式下，使用以下命令：

interface *interface-name*

- *interface-name* – 指定设备端接口的名称。

多次执行该命令启用多个接口，系统允许最多开启两个接口。在 SSL VPN 实例配置模式下使用该命令no 的形式取消指定设备端接口的配置：

no interface *interface-name*

配置自动检测最优通道功能，在 SSL VPN 实例配置模式下，使用以下命令：

link-select [**server-detect**] [*A.B.C.D* [**https-port** *port-number*]] [**A.B.C.D** [**https-port** *port-number*]] [*A.B.C.D* [**https-port** *port-number*]] [*A.B.C.D* [**https-port** *port-number*]]

- **server-detect** – 开启设备端检测最优通道功能，默认情况下由客户端检测最优通道。

- *A.B.C.D* – 指定 DNAT 设备外网接口 IP。系统允许最多配置四个 IP 地址。
- **https-port** *port-number* – 指定 DNAT 设备外网接口HTTPS 端口号。默认值是 4433。取值范围是 1 到 65535。为避免与 WebUI 使用的 HTTPS 端口号相冲突，建议用户不要把 HTTPS 端口号设置为 443。

在 SSL VPN 实例配置模式下使用 **no link-select** 命令取消自动检测最优通道功能的配置。

另外，SSL VPN 最优路径检测的应用还提供多链路冗余的功能，当任意一条链路不通时，数据均会自动切换到另外的链路，从而保证客户端连接的稳定性（切换过程中流量可能会中断）。

强制断开客户端 SSL VPN 连接

设备端可以通过命令强制断开某个客户端与设备端的连接。强制断开客户端 SSL VPN 连接，在执行模式使用以下命令：

exec scvpn *instance-name* **kickout** *user-name*

- *instance-name* – 指定 SSL VPN 实例的名称。
- *user-name* – 指定被强制断开连接的用户名称。

允许本地用户修改密码

设备支持本地用户成功通过 SSL VPN 认证后，在客户端修改自己的用户密码。默认情况下，该功能为关闭状态。在本地 AAA 服务器配置模式下，使用以下命令开启或关闭允许本地用户修改登录密码功能：

- 开启：**allow-pwd-change**
- 关闭：**no allow-pwd-change**

{b}提示: {/b}SSL VPN 客户端 1.2.0.1106（Secure Connect 1.2.0.1106）及后续版本支持允许本地用户修改密码功能。为避免出错，建议用户使用最新版本的 SSL VPN 客户端。

开启该功能并成功通过 SSL VPN 认证后，本地用户可通过以下步骤修改登录密码：

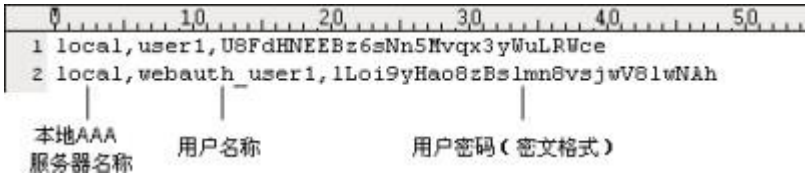
1. 右键单击系统任务栏通知区域的 Secure Connect 绿色图标，系统弹出客户端菜单，如下图所示：

2. 点击<修改密码>，系统弹出<修改密码>对话框。在<当前密码>文本框中输入正确的旧密码，在<新密码>文本框中输入新密码并在<确认新密码>处再次输入相同的新密码。如下图所示：

3. 点击『确定』按钮，系统显示提示信息“修改密码成功”。

导出和导入密码文件

为防止恢复配置时误将密码信息重置，用户可以将密码信息以文件格式从设备端导出或者导入。导出或者导入的密码文件为 CSV 格式，下图为密码文件及参数描述示例：



导入密码信息的原则是：

- 如果密码文件中的用户信息和系统中的用户信息一致，按照密码文件的信息恢复所有本地用户的密码；
- 如果密码文件中的用户信息比系统中的用户信息少，只恢复密码文件中已有用户的信息，系统中其它用户的信息不变；

- 如果密码文件中的用户信息比系统中的用户信息多，只恢复系统中已有用户的信息，密码文件中其它用户的信息删除。

注意:

- 若需直接用 Excel 打开密码文件，请将密码文件的扩展名改成“.csv”。
- 导入密码文件后，配置立即生效。
- 导入密码文件后，系统会在 CLI 中提示导入成功的用户数目。

导出密码文件

导出密码文件，在执行模式下使用以下命令:

export aaa user-password to {**tftp server** *ip-address* | **ftp server** *ip-address* [**user** *user-name* **password** *password*]} [*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。
- *file-name* – 指定导出的密码文件名称。

导入密码文件

导入密码文件，在执行模式下使用以下命令:

import aaa user-password from {**tftp server** *ip-address* | **ftp server ip-address** [**user** *user-name* **password** *password*]} *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。
- *file-name* – 指定导入的密码文件名称。

定制登录页面

设备支持用户自行定制 SSL VPN 认证登录页面。

定制登录页面

用户可以通过改变登录页面上的背景图片自行定制登录页面。引入登录页面背景图片到系统，请在执行模式下使用以下命令：

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

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

恢复默认图片，在任何配置模式下，使用以下命令：

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

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

通过 Radius 认证服务器限定用户的访问范围

当用户使用 Radius 认证方式时，系统可限定已认证用户的访问范围。对于已认证的用户，系统从 Radius 服务器上获取此用户的授权区域信息（即可访问的目的地址范围）。根据该授权区域，系统为此用户动态创建从其源地址到授权区域的安全策略；对于未通过认证的用户，系统拒绝将其接入网络。当用户注销登录、登陆超时、或被系统管理员强制登出后，对应的安全策略将被自动删除。

在任何模式下，使用以下命令查看用户的授权区域信息：

show auth-user username *user-name*

- *user-name* – 指定要查看的用户的用户名。

配置 Radius 服务器

用户需要在 Radius 服务器的字典文件中增如下自定义属性：

属性名称	属性类型	描述
-user-policy-dst-ip-begin	ipaddr	授权区域的起始 IP 地址。请输入 IPv4 地址。

属性名称	属性类型	描述
-user-policy-dst-ip-end	ipaddr	授权区域的终止 IP 地址。请输入 IPv4 地址。

添加自定义属性后，为 Radius 服务器中的用户赋予相应的属性值。完成赋值后，重启 Radius 服务。当用户使用 SSL VPN 客户端成功认证后，系统将根据此用户在 Radius 服务器中配置的属性值限定其可访问的网络资源。如果没有为此用户设定授权区域，用户将不受访问限制。

配置客户端升级 URL

客户端通过配置的 URL 进行新版本检查及下载升级。系统默认已经存在指向官方升级服务器的 URL，且此 URL 不可删除。客户端会通过此官方升级服务器的URL 进行新版本检查以及下载升级。当用户需要使用内网服务器进行客户端新版本的检查以及下载升级时，可配置新的升级 URL 后，且新配置 URL 生效。配置升级 URL，在全局配置模式下执行以下命令：

scvpn-update-url *ip-address*

- *ip-address* – 如果需要使用内网服务器进行客户端新版本的检查以及下载升级，则输入内网服务器 URL。用户需要自行在此服务器部署客户端新版本。

在全局配置模式下，使用该命令 no 的形式恢复默认的官方升级服务器的URL：

no scvpn-update-url

注意:当客户端版本为 1.4.4.1199 或更低版本且 StoneOS 版本为 5.5R1 或更高版本，推荐卸载旧版客户端并重新登陆 Web 下载安装。

显示 SSL VPN 信息

用户可以通过 show 命令查看系统 SSL VPN 信息。

- 显示 SSL VPN 实例信息：
  show tunnel scvpn [*scvpn-instance-name]*
- 显示通过浏览器访问 SSL VPN 的 HTTP 会话信息：
  show scvpn session *scvpn-instance-name* [**user** *user-name*]
- 显示指定 SSL VPN 实例当前在线的客户端信息：
  show scvpn client *scvpn-instance-name* [**user** *user-name*]
- 显示所有 SSL VPN 实例当前在线的客户端信息：
  show auth-user scvpn [**interface** *interface-name* | **vrouter** *vrouter-name* | **slot** *slot-no*]
- 显示主机验证绑定表：
  show scvpn user-host-binding *scvpn-instance-name* {**host** [*host-id*] | **user** [*user-name*]}

SSL VPN 客户端 for Windows

针对 Windows 操作系统的 SSL VPN 客户端程序为 Secure Connect。 Secure Connect 可在以下操作系统中运行：Windows 2000/2003/2008/XP/Vista/Windows 7/Windows 8/Windows 8.1/Windows10/Windows2012。通过客户端与设备端的连接，即可实现数据的加密通信。该客户端的主要作用包括：

- 从所在 PC 获得接口和路由信息；
- 显示与连接状态、数据流统计数据以及接口和路由信息；
- 显示应用程序日志信息；
- 调用客户端更新程序进行客户端更新；
- 解析从服务器端接收到的资源列表信息。

本节主要介绍 SSL VPN 客户端的下载、安装和启动。根据设备端配置的认证方式的不同，客户端的下载、安装和启动方法将不同。SSL VPN 设备端支持以下三种认证方式：

- 用户名/密码
- 用户名/密码 + 数字证书（包括 USB Key 证书和软证书）
- 只用数字证书（包括USB Key 证书和软证书）

客户端的下载与安装

初次使用 SSL VPN 客户端时，用户需要下载和安装客户端程序 Secure Connect。本节将根据设备端的三种认证方式，分别介绍对应的客户端下载和安装方法。对于“用户名/密码 + 数字证书”认证方式，数字证书可以是厂商提供的 USB Key 证书或管理员所提供的软证书。

下载与安装（用户名/密码）

当设备端配置“用户名/密码”认证方式时，请按照以下步骤下载和安装客户端程序 Secure Connect：

1. 在浏览器的地址栏输入以下 URL 访问设备端：https://IP-Address:Port-Number。其中“IP-Address”和“Port-Number”分别为设备端 SSL VPN 实例中指定的接口的 IP 地址（interface interface-name 命令）和 HTTPS（https-port port-number 命令）端口号。
2. 浏览器转到登录页面，输入用户名和密码，并点击『登录』按钮。
   - 如果设备端采用本地认证服务器进行用户认证，此处的用户名和密码为设备中配置的用户及其相应的密码；
   - 如果设备端采用“RADIUS 认证+通过 RSA Server 进行 RSA SecurID Token 认证”相结合的方式，并且是首次登录，此处输入的用户名应为 RADIUS 服务器中的用户名称，密码为该用户绑定的实时 Token 动态口令。输入完成并点击『登录』按钮后，浏览器将转到 PIN 码设置页面，用户需要在该页面设置PIN 码，为 4 至 8 位数字。PIN 码设置成功后，系统会提

示使用新密码重新登录，点击<重新登录>，浏览器返回登录页面，输入正确的用户名和新密码，并点击『登录』按钮。此处的新密码为“PIN 码+实时 Token 动态口令”，例如，如果 PIN 码设置为 54321，实时 Token 动态口令为 808771，则新密码为 54321808771；

- 如果设备端采用“RADIUS 认证+通过 RSA Server 进行 RSA SecurID Token 认证”相结合的方式，但不是首次登录，此处输入的用户名为 RADIUS 服务器中的用户名称，密码为首次重新登录时输入的新密码“PIN 码+实时 Token 动态口令”。

3. 如果设备端开启短信口令认证功能，浏览器将转到短信口令认证对话框，如下图所示。输入短信认证码，并点击『认证』按钮。如果用户在 1 分钟内没收到认证码短信，可以重新申请认证码。

- 通过用户名和密码验证后，用户最多可以输入 3 次认证码。如果连续 3 次输入错误，设备端将自动断开连接。
- 用户最多能重新申请 3 次认证码，新认证码短信发送的时间间隔为 1 分钟。重新申请认证码后，旧认证码信息失效，用户必须输入最新认证码才能认证成功。

4. 成功登录后，如果使用 IE 浏览器，系统将自动完成下载任务，用户只需按照提示安装即可；如果使用Firefox 等浏览器，请点击『下载』按钮下载客户端程序 scvpn.exe，下载完成，双击 scvpn.exe，按照安装向导提示进行安装。

成功安装 Secure Connect 后，将有一个虚拟网卡安装到PC 上。该虚拟网卡用来实现客户端与设备端信息的安全加密传输。

下载与安装（用户名/密码 + USB Key 证书）

当设备端配置“用户名/密码 + 数字证书”认证方式时，对于 USB Key 证书，请按照以下步骤下载和安装客户端程序 Secure Connect：

1. 将 USB Key 插入 PC 的 USB 接口。
2. 在浏览器的地址栏输入以下 URL 访问设备端：https://IP-Address:Port-Number。其中“IP-Address”和“Port-Number”分别为设备端 SSL VPN 实例中指定的接口的 IP 地址（**interface** *interface-name* 命令）和 HTTPS（**https-port** *port-number* 命令）端口号。
3. 浏览器弹出<选择数字证书>对话框，如图所示。选中需要的数字证书，点击『确定』按钮。继续在弹出的<请输入PIN 码>对话框（如图所示）中输入 UKey 的 PIN 码，并点击『确定』按钮。

{b}提示: {/b} UKey 的正常使用需要有配套的驱动程序和管理员软件，具体信息请参阅《 UKey 使用指南》。

4. 浏览器转到登录页面。输入用户名和密码，并点击『登录』按钮。此处的用户名和密码为 设备中配置的用户及其相应的密码。

5. 如果设备端开启短信口令认证功能，浏览器将转到短信口令认证对话框。输入短信认证码，并点击『认证』按钮。如果用户在 1 分钟内没收到认证码短信，可以重新申请认证码。

6. 成功登录后，如果使用 IE 浏览器，系统将自动完成下载任务，用户只需按照提示安装即可；如果使用Firefox 等浏览器，请点击『下载』按钮下载客户端程序 scvpn.exe，下载完成，双击 scvpn.exe，按照安装向导提示进行安装。

成功安装 Secure Connect 后，将有一个虚拟网卡安装到PC 上。该虚拟网卡用来实现客户端与设备端信息的安全加密传输。

下载与安装（用户名/密码 + 软证书）

当设备端配置“用户名/密码 + 数字证书”认证方式时，对于软证书，请按照以下步骤下载和安装客户端程 序 Secure Connect：

1. 手动导入管理员所提供的软证书。
2. 在浏览器的地址栏输入以下 URL 访问设备端：https://IP-Address:Port-Number。其中“IP-Address”和“Port-Number”分别为设备端 SSL VPN 实例中指定的接口的 IP 地址（**interface** *interface-name* 命令）和 HTTPS（**https-port** *port-number* 命令）端口号。
3. 浏览器弹出<选择数字证书>对话框。选中需要的数字证书，点击『确定』按钮。
4. 浏览器转到登录页面。输入用户名和密码，并点击『登录』按钮。此处的用户名和密码为 设备中配置的用户及其相应的密码。
5. 如果设备端开启短信口令认证功能，浏览器将转到短信口令认证对话框。输入短信认证码，并点击『认证』按钮。如果用户在 1 分钟内没收到认证码短信，可以重新申请认证码。
6. 成功登录后，如果使用 IE 浏览器，系统将自动完成下载任务，用户只需按照提示安装即可；如果使 用Firefox 等浏览器，请点击『下载』按钮下载客户端程序 scvpn.exe，下载完成，双击 scvpn.exe，按照安装向导提示进行安装。

成功安装 Secure Connect 后，将有一个虚拟网卡安装到PC 上。该虚拟网卡用来实现客户端与设备端信息的安全加密传输。

下载与安装（只用 USB Key 证书）

当设备端配置“只用数字证书”认证方式时，对于USB Key 证书，请按照以下步骤下载和安装客户端程序 Secure Connect：

1. 将 USB Key 插入 PC 的 USB 接口。
2. 在浏览器的地址栏输入以下 URL 访问设备端：https://IP-Address:Port-Number。其中“IP-Address”和“Port-Number”分别为设备端 SSL VPN 实例中指定的接口的 IP 地址（**interface** *interface-name* 命令）和 HTTPS（**https-port** *port-number* 命令）端口号。
3. 浏览器弹出<选择数字证书>对话框。选中需要的数字证书，点击『确定』按钮。继续在弹出的<请输入用户口令>对话框中输入 UKey 的用户口令（默认为“1111”），并点击『确定』按钮。
4. 成功登录后，如果使用 IE 浏览器，系统将自动完成下载任务，用户只需按照提示安装即可；如果使 用Firefox 等浏览器，请点击『下载』按钮下载客户端程序 scvpn.exe，下载完成，双击 scvpn.exe，按照安装向导提示进行安装。

成功安装 Secure Connect 后，将有一个虚拟网卡安装到PC 上。该虚拟网卡用来实现客户端与设备端信息的安全加密传输。

下载与安装（只用软证书）

当设备端配置“只用数字证书”认证方式时，对于软证书，请按照以下步骤下载和安装客户端程序 Secure Connect：

1. 手动导入管理员所提供的软证书。
2. 在浏览器的地址栏输入以下 URL 访问设备端：https://IP-Address:Port-Number。其中“IP-Address”和“Port-Number”分别为设备端 SSL VPN 实例中指定的接口的 IP 地址（**interface** *interface-name* 命令）和 HTTPS（**https-port** *port-number* 命令）端口号。
3. 浏览器弹出<选择数字证书>对话框。选中需要的数字证书，点击『确定』按钮。
4. 成功登录后，如果使用 IE 浏览器，系统将自动完成下载任务，用户只需按照提示安装即可；如果使用Firefox 等浏览器，请点击『下载』按钮下载客户端程序 scvpn.exe，下载完成，双击 scvpn.exe，按照安装向导提示进行安装。

成功安装 Secure Connect 后，将有一个虚拟网卡安装到PC 上。该虚拟网卡用来实现客户端与设备端信息的安全加密传输。

客户端的启动

PC 上安装 SSL VPN 客户端程序 Secure Connect 后，用户有两种方法可以启动客户端：

- Web 方式启动
- 直接启动

Web 方式启动

本节将根据设备端的三种认证方式，分别介绍对应的客户端 Web 启动方法。对于“用户名/密码+ 数字证书”认证方式，数字证书可以是厂商提供的 USB Key 证书或管理员所提供的软证书。

Web 方式启动（用户名/密码）

当设备端配置“用户名/密码”认证方式时，请按照以下步骤通过 Web 启动客户端，完成客户端与设备端的连接：

1. 在 IE 浏览器的地址栏输入以下 URL 访问设备端：https://IP-Address:Port-Number。
2. 浏览器转到登录页面（如图所示）。输入用户名和密码，并点击『登录』按钮。
   如果设备端采用本地认证服务器进行用户认证，此处的用户名和密码为设备中配置的用户及其相应的密码；
   如果设备端采用“RADIUS 认证+通过 RSA Server 进行 RSA SecurID Token 认证”相结合的方式，并且是首次登录，此处输入的用户名应为 RADIUS 服务器中的用户名称，密码为该用户绑定的实时 Token 动态口令。输入完成并点击『登录』按钮后，浏览器将转到PIN 码设置页面，用户需要

在该页面设置PIN 码，为 4 至 8 位数字。PIN 码设置成功后，系统会提示使用新密码重新登录，点击<重新登录>，浏览器返回登录页面，输入正确的用户名和新密码，并点击『登录』按钮。此处 的新密码为“PIN 码+实时 Token 动态口令”，例如，如果PIN 码设置为 54321，实时 Token 动态口令为 808771，则新密码为 54321808771；
如果设备端采用“RADIUS 认证+通过 RSA Server 进行 RSA SecurID Token 认证”相结合的方式，但不是首次登录，此处输入的用户名为 RADIUS 服务器中的用户名称，密码为首次重新登录时输入的新密码“PIN 码+实时 Token 动态口令”。

3. 如果设备端开启短信口令认证功能，浏览器将转到短信认证对话框。输入短信认证码，并点击『认证』按钮。如果用户在 1 分钟内没收到认证码短信，可以重新申请认证码。

完成以上各步骤后，客户端将发起自动连接以接入VPN。连接成功后，在系统任务栏的通知区域将会显示绿色的图标。此时就可以通过 SSL VPN 实现加密通信。

Web 方式启动（用户名/密码 + USB Key 证书）

当设备端配置“用户名/密码 + 数字证书”认证方式时，对于 USB Key 证书，请按照以下步骤通过 Web 启动客户端，完成客户端与设备端的连接：

1. 将 USB Key 插入 PC 的 USB 接口。
2. 在 IE 浏览器的地址栏输入以下 URL 访问设备端：https://IP-Address:Port-Number。
3. 浏览器弹出<选择数字证书>对话框。选中需要的数字证书，点击『确定』按钮。继续在弹出的<请输入用户口令>对话框中输入 UKey 的用户口令（默认为“1111”），并点击『确定』按钮。
4. 浏览器转到登录页面。输入用户名和密码，并点击『登录』按钮。此处的用户名和密码为 设备中配置的用户及其相应的密码。
5. 如果设备端开启短信口令认证功能，浏览器将转到短信认证对话框。输入短信认证码，并点击『认证』按钮。如果用户在 1 分钟内没收到认证码短信，可以重新申请认证码。
6. 浏览器弹出<USB Key 口令>对话框，如下图所示。输入 UKey 的用户口令（默认为“1111”），并点击『确定』按钮。

完成以上各步骤后，客户端将发起自动连接以接入VPN。连接成功后，在系统任务栏的通知区域将会显示绿色的图标。此时就可以通过 SSL VPN 实现加密通信。

Web 方式启动（用户名/密码 + 软证书）

当设备端配置“用户名/密码 + 数字证书”认证方式时，对于软证书，请按照以下步骤通过 Web 启动客户端，完成客户端与设备端的连接：

1. 手动导入管理员所提供的软证书。
2. 在 IE 浏览器的地址栏输入以下 URL 访问设备端：https://IP-Address:Port-Number。
3. 浏览器弹出<选择数字证书>对话框。选中需要的数字证书，点击『确定』按钮。
4. 浏览器转到登录页面。输入用户名和密码，并点击『登录』按钮。此处的用户名和密码为 设备中配置的用户及其相应的密码。
5. 如果设备端开启短信口令认证功能，浏览器将转到短信认证对话框。输入短信认证码，并点击『认证』按钮。如果用户在 1 分钟内没收到认证码短信，可以重新申请认证码。

完成以上各步骤后，客户端将发起自动连接以接入VPN。连接成功后，在系统任务栏的通知区域将会显示绿色的图标。此时就可以通过 SSL VPN 实现加密通信。

Web 方式启动（只用 USB Key 证书）

当设备端配置“只用数字证书”认证方式时，对于USB Key 证书，请按照以下步骤通过Web 启动客户端，完成客户端与设备端的连接：

1. 将 USB Key 插入 PC 的 USB 接口。
2. 在 IE 浏览器的地址栏输入以下 URL 访问设备端：https://IP-Address:Port-Number。
3. 浏览器弹出<选择数字证书>对话框。选中需要的数字证书，点击『确定』按钮。继续在弹出的<请输入用户口令>对话框中输入 UKey 的用户口令（默认为“1111”），并点击『确定』按钮。
4. 浏览器会弹出<USB Key 口令>对话框。输入 UKey 的用户口令（默认为“1111”），并点击『确定』按钮。

完成以上各步骤后，客户端将发起自动连接以接入VPN。连接成功后，在系统任务栏的通知区域将会显示绿色的图标。此时就可以通过 SSL VPN 实现加密通信。

Web 方式启动（只用软证书）

当设备端配置“只用数字证书”认证方式时，对于软证书，请按照以下步骤通过 Web 启动客户端，完成客户端与设备端的连接：

1. 手动导入管理员所提供的软证书。

2.在 IE 浏览器的地址栏输入以下 URL 访问设备端：https://IP-Address:Port-Number。

3.浏览器弹出<选择数字证书>对话框。选中需要的数字证书，点击『确定』按钮。

完成以上各步骤后，客户端将发起自动连接以接入VPN。连接成功后，在系统任务栏的通知区域将会显示绿色的图标。此时就可以通过 SSL VPN 实现加密通信。

直接启动

本节将根据设备端的三种认证方式以及 SSL 协议类型，分别介绍对应的通过启动文件直接启动客户端的方法。

基于 TLS/SSL 协议的启动方式

对于“用户名/密码+ 数字证书”（TLS/SSL）认证方式，数字证书可以是厂商提供的 USB Key 证书或管理员所提供的软证书。

基于 TLS/SSL 协议的启动方式如下：

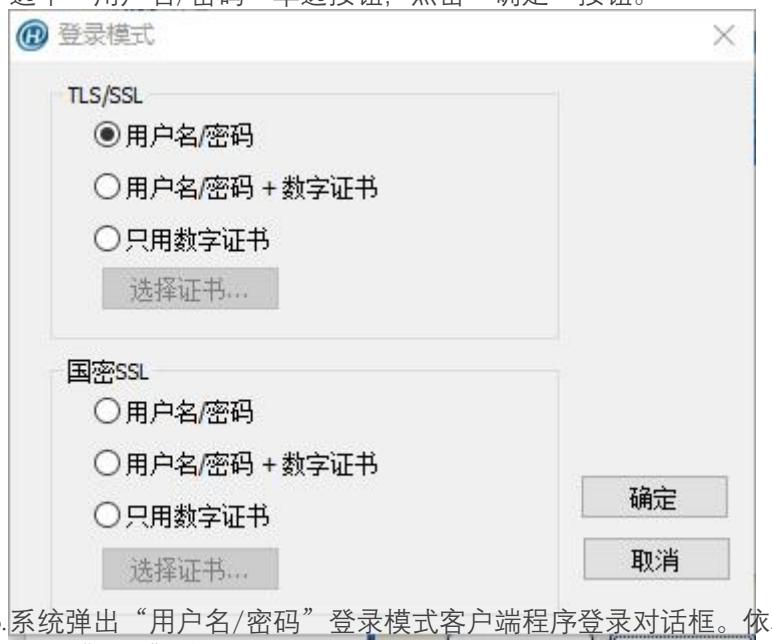
- 用户名/密码
- 用户名/密码 + USB Key 证书
- 用户名/密码 + 软证书
- 只用 USB Key 证书
- 只用软证书

使用“用户名/密码”方式

当设备端配置“用户名/密码”认证方式时，请按照以下步骤通过启动文件直接启动客户端，完成客户端与设备端的连接：

1.双击桌面的 Secure Connect 快捷方式，或者点击“开始菜单”中的“所有程序 Secure Connect Secure Connect”，系统弹出登录对话框。

2. 点击对话框中的“模式”按钮，系统弹出<登录模式>对话框，如下图所示。在“TLS/SSL”部分，选中“用户名/密码”单选按钮，点击“确定”按钮。



3. 系统弹出“用户名/密码”登录模式客户端程序登录对话框。依次填写登录对话框中的各项，然后点击“登录”按钮。

如果设备端采用本地认证服务器进行用户认证，此处的用户名和密码为设备中配置的用户及其相应的密码；

如果设备端采用“RADIUS 认证+通过 RSA Server 进行 RSA SecurID Token 认证”相结合的方式，并且是首次登录，此处输入的用户名应为 RADIUS 服务器中的用户名称，密码为该用户绑定的实时 Token 动态口令。输入完成并点击『登录』按钮后，浏览器将转到PIN 码设置对话框（如下图所示）。

用户需要在该对话框设置PIN 码，为 4 至 8 位数字。PIN 码设置成功后，系统会提示使用新密码重新登录（如下图所示）。

点击“确定”按钮返回登录对话框，输入新密码，并点击『登录』按钮。此处的新密码为“PIN 码

+实时 Token 动态口令”，例如，如果PIN 码设置为 54321，实时 Token 动态口令为 808771，则新密码为 54321808771；
如果设备端采用“RADIUS 认证+通过 RSA Server 进行 RSA SecurID Token 认证”相结合的方式，但不是首次登录，此处输入的用户名为 RADIUS 服务器中的用户名称，密码为首次重新登录时输入的新密码“PIN 码+实时 Token 动态口令”。

最近访问：在下拉菜单中选择登录信息条目标识（关于登录信息条目的详细描述请参见 Secure Connect 设置部分）。如不选择，请依次填写以下各项。

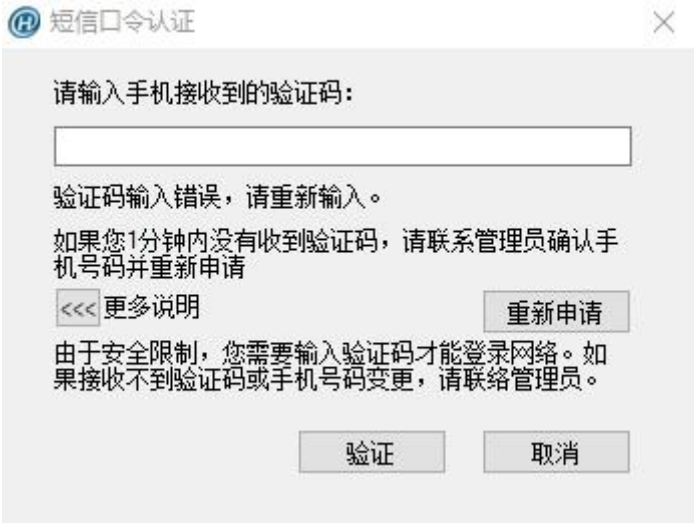
服务器：填写设备端的 IP 地址。

端口：填写设备端的 HTTPS 端口号。

用户名：填写客户端用户名。

密码：填写与用户名相对应的密码。如果用户在 1 分钟内连续 3 次输入错误密码登录 SCVPN 客户端，在接下来的 2 分钟内系统将禁止该用户再次登录。

如果设备端开启短信口令认证功能，系统将弹出<短信口令认证>对话框，如下图所示。在该对话框中输入认证码，并点击“验证”按钮。如果用户在 1 分钟内没收到认证码短信，可以重新申请认证码。



连接成功后，在系统任务栏的通知区域将会显示绿色的图标。此时就可以通过 SSL VPN 实现加密通信。

使用“用户名/密码 + USB Key 证书” 方式

当设备端配置“用户名/密码 + 数字证书”认证方式时，对于 USB Key 证书，请按照以下步骤通过启动文件直接启动客户端，完成客户端与设备端的连接：

1. 将 USB Key 插入 PC 的 USB 接口。
2. 双击桌面的 Secure Connect 快捷方式，或者点击“开始菜单”中的“所有程序 Secure Connect Secure Connect”，系统弹出登录对话框。
3. 点击“模式”按钮，系统弹出<登录模式>对话框。首先，在“TLS/SSL”部分，选中<用户名/密码 + 数字证书>单选按钮；如需要，点击“选择证书”按钮，在弹出的<选择证书>对话框中选择“使用 USB Key 证书”（如下图所示）。如果当前证书列表中没有显示 USB Key 证书，请点击

“刷新”按钮。客户端会将选中的 USB Key 证书传送至设备端，设备端对收到的 USB Key 证书进行认证；最后，点击“确定”按钮。

使用默认系统证书：选中该复选框，客户端自动选择默认系统证书传送至设备端进行认证。 设备采用 UKey 证书作为默认系统证书。该选项为系统默认选项。
使用 USB Key 证书：选中该单选按钮，客户端自动选择厂商所提供的 USB Key 证书传送至设备端进行认证。
使用软证书：选中该单选按钮，客户端自动选择管理员所提供的软证书传送至设备端进行认证。
当前证书列表：显示系统中已有的证书，用户可以通过该列表选择所需证书进行认证。

{b}提示: {/b}用户可以通过 USB Key 批量部署工具将第三方 USB Key 证书设置为默认系统证书。关于 USB Key 批量部署工具的详细信息，请参阅“USB Key 批量部署”。

4.系统弹出“用户名/密码 + USB Key 证书”登录模式客户端程序登录对话框。依次填写登录对话框中的各项，然后点击“登录”按钮。
最近访问：在下拉菜单中选择登录信息条目标识（关于登录信息条目的详细描述请参见 Secure Connect 设置部分）。如不选择，请依次填写以下各项。
端口：填写设备端的 HTTPS 端口号。
用户名：填写客户端用户名。
密码：填写与用户名相对应的密码。
PIN 码：填写 USB Key 对应的用户口令（默认为“1111”）。一个USB Key 对应一个用户口令。

5.如果设备端开启短信口令认证功能，系统将弹出<短信口令认证>对话框。在该对话框中输入认证码，并点击“验证”按钮。如果用户在 1 分钟内没收到认证码短信，可以重新申请认证码。

连接成功后，在系统任务栏的通知区域将会显示绿色的图标。此时就可以通过 SSL VPN 实现加密通信。

使用“用户名/密码 + 软证书”方式

当设备端配置“用户名/密码 + 数字证书”认证方式时，对于软证书，请按照以下步骤通过启动文件直接启动客户端，完成客户端与设备端的连接。

1. 手动导入管理员所提供的软证书。
2. 双击桌面的 Secure Connect 快捷方式，或者点击“开始菜单”中的“所有程序 Secure Connect Secure Connect”，系统弹出登录对话框。
3. 点击“模式”按钮，系统弹出<登录模式>对话框。首先，在“TLS/SSL”部分，选中<用户名/密码 + 数字证书>单选按钮；如需要，点击“选择证书”按钮，在弹出的<选择证书>对话框中选择软证书（如下图所示）。如果当前证书列表中没有显示软证书，请点击“刷新”按钮。客户端会将选中的软证书传送至设备端，设备端对收到的软证书进行认证；最后，点击“确定”按钮。

4. 系统弹出“用户名/密码 + 软证书”登录模式客户端程序登录对话框。依次填写登录对话框中的各项，然后点击“登录”按钮。
   最近访问：在下拉菜单中选择登录信息条目标识（关于登录信息条目的详细描述请参见 Secure Connect 设置部分）。如不选择，请依次填写以下各项。
   服务器：填写设备端的 IP 地址。
   端口：填写设备端的 HTTPS 端口号。
   用户名：填写客户端用户名
   密码：填写与用户名相对应的密码。
5. 如果设备端开启短信口令认证功能，系统将弹出<短信口令认证>对话框。在该对话框中输入认证码，并点击“验证”按钮。如果用户在 1 分钟内没收到认证码短信，可以重新申请认证码。

连接成功后，在系统任务栏的通知区域将会显示绿色的图标。此时就可以通过 SSL VPN 实现加密通信。

使用“只用 USB Key 证书”方式

当设备端配置“只用数字证书”认证方式时，对于USB Key 证书，请按照以下步骤通过启动文件直接启动客户端，完成客户端与设备端的连接：

1. 将 USB Key 插入 PC 的 USB 接口。
2. 双击桌面的 Secure Connect 快捷方式，或者点击“开始菜单”中的“所有程序 Secure Connect Secure Connect”，系统弹出登录对话框。
3. 点击“模式”按钮，系统弹出<登录模式>对话框。首先，选中<只用数字证书>单选按钮；如需要，点击“选择证书”按钮，在弹出的<选择证书>对话框中选择 USB Key 证书。如果当前证书列表中没有显示USB Key 证书，请点击“刷新”按钮。客户端会将选中的 USB Key 证书传送至设备端，设备端对收到的USB Key 证书进行认证；最后，点击“确定”按钮。
4. 系统弹出“只用数字证书”登录模式客户端程序登录对话框（如下图所示）依次填写登录对话框中的各项，然后点击“登录”按钮。
   最近访问：在下拉菜单中选择登录信息条目标识（关于登录信息条目的详细描述请参见 Secure Connect 设置部分）。如不选择，请依次填写以下各项。
   服务器：填写设备端的 IP 地址。
   端口：填写设备端的 HTTPS 端口号。
   PIN 码：填写 USB Key 对应的用户口令（默认为“1111”）。一个USB Key 对应一个用户口令。

连接成功后，在系统任务栏的通知区域将会显示绿色的图标。此时就可以通过 SSL VPN 实现加密通信。

使用“只用软证书”方式

当设备端配置“只用数字证书”认证方式时，对于软证书，请按照以下步骤通过启动文件直接启动客户端，完成客户端与设备端的连接：

1. 手动导入管理员所提供的软证书。
2. 双击桌面的 Secure Connect 快捷方式，或者点击“开始菜单”中的“所有程序 Secure Connect Secure Connect”，系统弹出登录对话框。
3. 点击“模式”按钮，系统弹出<登录模式>对话框。首先，选中<只用数字证书>单选按钮；如需要，点击“选择证书”按钮，在弹出的<选择证书>对话框中选择软证书。如果当前证书列表中没有显示软证书，请点击“刷新”按钮。客户端会将选中的软证书传送至设备端，设备端对收到的软证书进行认证；最后，点击“确定”按钮。
4. 系统弹出“只用数字证书”登录模式客户端。依次填写登录对话框中的各项。
   最近访问：在下拉菜单中选择登录信息条目标识（关于登录信息条目的详细描述请参见 Secure Connect 设置部分）。如不选择，请依次填写以下各项，然后点击『登录』按钮。
   服务器：填写设备端的 IP 地址。
   端口：填写设备端的 HTTPS 端口号。

连接成功后，在系统任务栏的通知区域将会显示绿色的图标。此时就可以通过 SSL VPN 实现加密通信。

基于国密 SSL 协议的启动方式

基于国密 SSL 协议的启动方式如下：

- 用户名/密码
- 用户名/密码 + 数字证书
- 只用数字证书

使用“用户名/密码”方式

请按照以下步骤通过启动文件直接启动客户端，完成客户端与设备端的连接：

1. 双击桌面的 Secure Connect 快捷方式，或者点击“开始菜单”中的“所有程序 Secure Connect Secure Connect”，系统弹出登录对话框。
2. 点击对话框中的“模式”按钮，系统弹出<登录模式>对话框，如下图所示。在“国密 SSL”部分，选中“用户名/密码”单选按钮，点击“确定”按钮。

3. 系统弹出“用户名/密码”登录模式客户端程序登录对话框。依次填写登录对话框中的各项，然后点击“登录”按钮。
   最近访问：在下拉菜单中选择登录信息条目标识（关于登录信息条目的详细描述请参见 Secure Connect 设置部分）。如不选择，请依次填写以下各项。
   服务器：填写设备端的 IP 地址。
   端口：填写设备端的 HTTPS 端口号。
   用户名：填写客户端用户名。

密码：填写与用户名相对应的密码。如果用户在 1 分钟内连续 3 次输入错误密码登录 SCVPN 客户端，在接下来的 2 分钟内系统将禁止该用户再次登录。

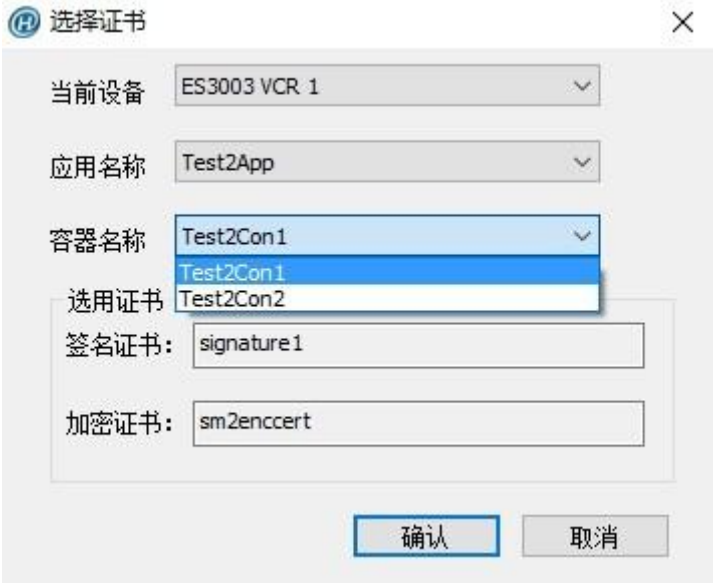
连接成功后，在系统任务栏的通知区域将会显示绿色的图标。此时就可以通过 SSL VPN 实现加密通信。

使用“用户名/密码+数字证书”方式

当设备端配置“用户名/密码 + 数字证书”认证方式时，请按照以下步骤通过启动文件直接启动客户端，完成客户端与设备端的连接：

1. 将 USB Token 插入 PC 的 USB 接口。

2. 双击桌面的 Secure Connect 快捷方式，或者点击“开始菜单”中的“所有程序 Secure Connect Secure Connect”，系统弹出登录对话框。
点击“模式”按钮，系统弹出<登录模式>对话框。首先，在“国密 SSL”部分，选中<用户名/密码 + 数字证书>单选按钮；如需要，点击“选择国密证书”按钮，在弹出的<选择证书>对话框中选择证书相关信息（如下图所示），最后，点击“确定”按钮。



当前设备：在下拉菜单中选择当前 USB Token 设备名称。
应用名称：应用是包含容器、设备认证密钥以及文件的一种结构。在下拉菜单选择指定的应用名称。
容器名称： 容器是 USB Token 设备中用于保存密钥所划分的唯一性存储空间。用来存储加密密钥对、与加密密钥对所对应的加密证书、签名密钥对、与签名密钥对所对应的签名证书。在下拉菜单选择指定的容器名称。
签名证书：显示指定容器内的 SM2 签名证书名称。
加密证书：显示指定容器内的 SM2 加密证书名称。

3. 系统弹出“用户名/密码 + 数字证书”登录模式客户端程序登录对话框。依次填写登录对话框中的各项，然后点击“登录”按钮。
最近访问：在下拉菜单中选择登录信息条目标识（关于登录信息条目的详细描述请参见 Secure Connect 设置部分）。如不选择，请依次填写以下各项。

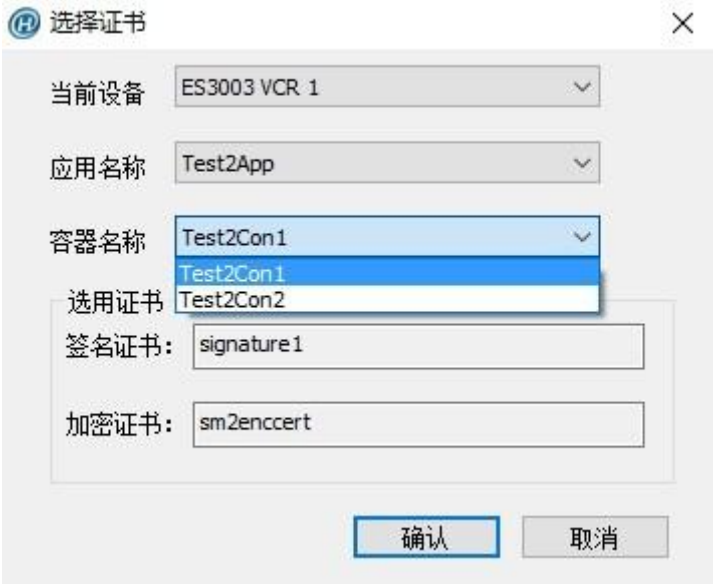
服务器：填写设备端的 IP 地址。
端口：填写设备端的 HTTPS 端口号。
用户名：填写客户端用户名。
密码：填写与用户名相对应的密码。
PIN 码：填写 USB Token 对应的用户口令。

连接成功后，在系统任务栏的通知区域将会显示绿色的图标。此时就可以通过 SSL VPN 实现加密通信。

使用“只用数字证书”方式

当设备端配置“只用数字证书”认证方式时，请按照以下步骤通过启动文件直接启动客户端，完成客户端与设备端的连接：

1. 将 USB Token 插入 PC 的 USB 接口。
2. 双击桌面的 Secure Connect 快捷方式，或者点击“开始菜单”中的“所有程序 Secure Connect Secure Connect”，系统弹出登录对话框。
   点击“模式”按钮，系统弹出<登录模式>对话框。首先，在“国密 SSL”部分，选中<只用数字证书>单选按钮；如需要，点击“选择国密证书”按钮，在弹出的<选择证书>对话框中选择证书相关信息（如下图所示），最后，点击“确定”按钮。



当前设备：在下拉菜单中选择当前 USB Token 设备名称。
应用名称：应用是包含容器、设备认证密钥以及文件的一种结构。在下拉菜单选择指定的应用名称。
容器名称：容器是 USB Token 设备中用于保存密钥所划分的唯一性存储空间。用来存储加密密钥对、与加密密钥对所对应的加密证书、签名密钥对、与签名密钥对所对应的签名证书。在下拉菜单选择指定的容器名称。
签名证书：显示指定容器内的 SM2 签名证书名称。
加密证书：显示指定容器内的 SM2 加密证书名称。

3. 系统弹出“只用数字证书”登录模式客户端程序登录对话框。依次填写登录对话框中的各项，然后点击“登录”按钮。
   最近访问：在下拉菜单中选择登录信息条目标识（关于登录信息条目的详细描述请参见 Secure Connect 设置部分）。如不选择，请依次填写以下各项。
   服务器：填写设备端的 IP 地址。
   端口：填写设备端的 HTTPS 端口号。
   PIN 码：填写 USB Token 对应的用户口令。

连接成功后，在系统任务栏的通知区域将会显示绿色的图标。此时就可以通过 SSL VPN 实现加密通信。

通过计划任务启动并自动连接

SSL VPN 客户端支持在用户登录系统前完成启动及连接。用户需要对 SSL VPN 客户端进行配置并创建计划任务。当通过计划任务启动并自动连接时，登录模式只支持“用户名/密码”认证方式。

通过 SSL VPN 客户端对自动连接进行相关的配置。

1. 双击桌面的 Secure Connect 快捷方式，或者点击“开始菜单”中的“所有程序 Secure Connect Secure Connect”，系统弹出登录对话框。
2. 右键单击系统通知栏区域的 Secure Connect 图标。
3. 在左侧选项列表中选择登录信息。
   - **最近访问**：输入信息作为登录信息条目标识。用户可选择不填写。如果不填写，则在点击『应用』后，客户端根据服务器信息，端口信息，以及用户名称自动生成。生成后，用户可对其进行修改。
   - **服务器：**填写设备端 的域名或 IP 地址。
   - **端口：**填写设备端 SCVPN 实例的 HTTPS 端口号。
   - **用户名：**填写需要连接的用户的用户名。
   - **密码：**填写与用户名相对应的密码。
   - **登录模式：**选择"密码"登录模式。当通过计划任务启动并自动连接时，登录模式只支持此种模式。
   - **记住密码：**选中<记住密码>复选框使用记住密码功能。
   - **最优通道：**选中该复选框开启最优路径检测功能。
4. 点击『应用』，客户端保存此登录信息条目。
5. 在左侧选项列表中选择设置。在右侧配置区域选择<自动登录>。在登录用户下拉菜单中，选择登录信息条目。

6. 点击『应用』，保存配置。

通过创建计划，SCVPN 客户端可以在指定的时间内完成启动。以 Windows 7 为例，介绍创建计划任务过程。

1. 点击开始菜单中的<控制面板>。在控制面板中依次进入”系统和安全　管理工具　计划任务”，系统弹出<任务计划程序>对话框。
2. 在<任务计划程序>对话框中，点击<创建基本任务>。系统弹出<创建基本任务向导>对话框。
3. 在<创建基本任务>页面，输入任务名称和描述。完成后点击『下一步』。
4. 在<触发器>，选择<计算机启动时>。
5. 在<操作>页面，选择<启动程序>。完成后点击『下一步』。
6. 在<启动程序>页面，点击『浏览』并选择 SCVPN 客户端执行程序 SecureConnect.exe。默认路径为 C:\Program Files (x86)\ \ Secure Connect\bin 。
7. 在<添加参数>文本框中输入如下参数。
    - -l “C:\Users\Administrator\AppData\Roaming\ \ Secure Connect\ SecurecConfig.xml”
    - 参数中的C:\Users\Administrator\AppData\Roaming\ \ Secure Connect\ SecurecConfig.xml 为用户 Administrator 的 SCVPN 客户端配置文件的默认路径。若当前为其他登录用户，请输入与当前用户匹配的路径。
8. 完成上述操作后后点击『下一步』。
9. 在<完成>页面，选择<当点击”完成”时，打开此任务属性的对话框>复选框。选择后点击『完成』。
10. 在弹出对话框中，选择<不管用户是否登录都要运行>单选框。选择后点击『完成』。系统弹出对话框要求指定运行此程序的用户及其密码。输入具有管理员权限的用户名及密码。
11. 点击『确认』完成配置。

完成上述配置后，SCVPN 客户端即可在用户登录系统前完成启动及连接。

USB Key 批量部署

设备采用 UKey 证书作为默认系统证书。使用默认系统证书进行认证时，客户端会自动选择默认系统证书传送至设备端，设备端对收到的数字证书进行认证，整个认证过程对用户来说是透明的，不需要用户手动进行证书选择。针对用户使用第三方 USB Key 进行 SSL VPN 客户端认证的情况， 提供 USB Key 批量部署工具 SelectUSBKey。通过 SelectUSBKey，用户能够将第三方 USB Key 证书设置为默认系统证书，从而简化认证时的操作过程。

通过 SelectUSBKey 将第三方 USB Key 证书设置为默认系统证书，用户首先要将USB Key 的 CSP Name 信息以注册表文件的格式导出，然后将文件中的信息添加进客户端PC 注册表。

请按照以下步骤导出 USB Key 的 CSP Name 信息：

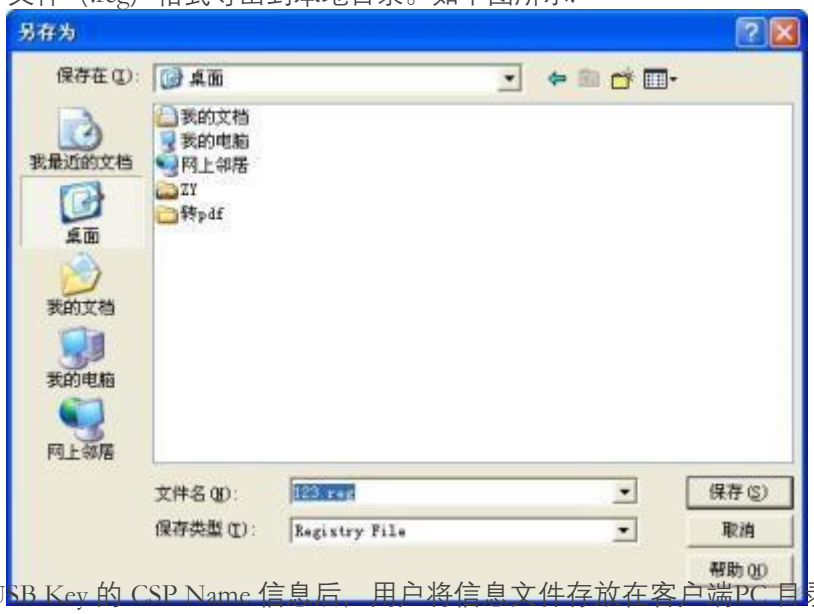
1. 在 PC 中安装第三方USB Key 驱动程序。
2. 插入第三方 USB Key。
3. 双击 SelectUSBKey.exe，系统弹出<Select Default Certificate>对话框。如下图所示：

格式导出到本地目录。

Update：刷新证书列表。

Close：关闭对话框。

4.在<Certificate List>中选中所需证书，点击『Export』按钮，将 USB Key 的 CSP Name 信息以注册表文件（.reg）格式导出到本地目录。如下图所示:



导出 USB Key 的 CSP Name 信息后，用户将信息文件存放在客户端PC 目录中并双击该文件，将文件中的信息添加进客户端PC 注册表。添加完成后，当用户通过该 USB Key 进行 SSL VPN 客户端认证时，客户端会自动选择 USB Key 中的数字证书传送至设备端，不需要用户手动选择证书。

客户端的卸载

从 PC 上卸载 Secure Connect，从“开始菜单”点击“所有程序 Secure Connect Uninstall”。

SSL VPN 客户端 for Android

支持Android 系统的 SSL VPN 客户端工具为 Secure Connect，可在 Android 4.0 以上系统环境中运行。Secure Connect 主要作用包括:

- 从所在 Android 系统中获得接口信息;
- 显示与设备端连接状态、数据流统计以及接口和路由信息;
- 显示应用程序日志信息。

下载与安装

下载和安装 Secue Connect，参照如下步骤:

1.访问客户端下载页面：http://www. net.com.cn/product/technology/VPN.html。

2.在右侧边栏，用手机扫描 Android 客户端二维码。

3.通过二维码扫描结果打开下载链接并下载安装文件 -Secure-Connect-Versione_Number.apk 到手机。

4. 下载完成后，在手机存储器中找到该安装文件。

5. 点击该安装文件。弹出程序安装界面。

6. 阅读权限需求。

7. 点击“安装”按钮。

安装成功后会在 Android 系统中出现程序图标，如下图所示：

启动与登录

启动与登录客户端，按照以下步骤进行操作：

1. 点击 Android 系统桌面上的 Secure Connect 图标，进入登录界面。

2. 依次填写对话框中的各项，然后点击“登入”按钮：

   - **请选择：** 在下拉菜单中选择登录信息条目标识（关于登录信息条目的详细描述请参见VPN连接配置管理部分）。如不选择，请依次填写以下各项。
   - **服务器：** 填写设备端的 IP 地址或域名。
   - **端口：** 填写设备端的 HTTPS 端口号。
   - **用户名：** 填写登录用户名。
   - **密码：** 填写与用户名相对应的密码。

3. 如果设备端开启短信口令认证功能，系统将弹出短信验证界面，如下图所示。在该对话框中输入认证码，并点击“提交“按钮。如果用户在 1 分钟内没收到认证码短信，可以重新申请认证码。

4.连接成功后，Android 系统通知栏显示钥匙形图标（  ），此时就可以实现客户端与设备端之间的加密通信。

SSL VPN 客户端 for iOS

支持 iOS 系统的 SSL VPN 客户端工具为 Access Connect，可在 iOS 10.0 以上系统环境中运行。 Access Connect 的主要作用包括：

- 简化与设备端建立VPN 的过程；
- 显示与设备端连接状态；
- 显示日志信息。

安装与建立连接

为使用客户端，用户需要从 App Store 搜索应用 Access Connect 并完成应用的安装。

应用安装完成后，需要使用 Access Connect 与设备端建立连接。

注意:卸载此应用后，再次安装后的登录也为首次登录；如果这 5 个登录参数中任何一个变化后进行登录，也为首次登录。

按照以下步骤与设备端建立连接：

1.点击 iOS 系统桌面上的 HSAccess 图标，系统进入 HSAccess 的登录界面。

2.依次填写对话框中的各项创建 VPN 连接实例，然后点击“登录”按钮。

- 请选择
- **名称：**输入连接名称标示此 VPN 连接实例。
- **服务器地址**：填写设备端的 IP 地址或域名。
- **端口号**：填写设备端的 HTTPS 端口号。
- **用户名**：填写登录用户名。
- **密码**：填写与用户名相对应的密码。

3.如果设备端开启短信口令认证功能，系统将弹出短信验证界面。在该对话框中输入认证码，并点击“验证“按钮。如果用户在 1 分钟内没收到认证码短信，可以重新申请认证码。

4.登录成功后，客户端与设备端成功建立连接。

5.在<允许安装 VPN 配置文件>对话框中，点击“允许”按钮。

6.在<输入密码>页面中，输入 iOS 锁屏密码。密码输入正确后，iOS 开始执行安装。

建立 VPN 连接

完成客户端与设备端的连接以及安装 VPN 配置文件后，用户可按照如下步骤建立客户端与设备端之间的 VPN 连接：

1. 打开 iOS 设置功能，点击“通用>VPN”。在<选择配置>列表中，选中需要连接的 VPN 名称，即在 VPN 配置中设置的连接名。
2. 打开 VPN 开关。iOS 进行 VPN 连接。
3. 当 iOS 显示 VPN 连接成功且客户端在<连接状态>界面显示“当前已经连接”，表明客户端与设备端成功建立 VPN 连接。

注意:如果不是首次登录，将不会进行 VPN 配置文件的安装。只需要登录客户端与设备端进行连接，并在 iOS 系统中完成VPN 的连接，即可对客户端与设备端之间传输的数据进行加密。

SSL VPN 客户端 for Mac OS

支持 Mac OS 系统的 SSL VPN 客户端工具为 Secure Connect，可在 Mac OS X 10.6.8 及以上系统环境中运行。通过客户端与设备端的连接，即可实现数据的加密通信。客户端的主要作用包括：

- 与设备端建立 SSL VPN 连接；
- 显示与设备端的连接状态、数据流统计数据以及路由信息；
- 显示应用程序日志信息；

下载与安装

访问官方地址 http://swupdate. net.com:1337/sslvpn/download?os=osx 下载客户端。

下载完成后，双击安装程序，在弹出窗口中将 SCVPN 拖拽到Applications 中即可完成安装。

注意:需要符合如下条件才可打开客户端安装程序：

- 需要管理员权限才可以打开客户端安装程序。
- 在系统偏好设置的“安全性与隐私”中，将“允许从以下位置下载的应用”设置为“任何来源”，才可以打开客户端安装程序。

启动与连接

启动客户端并建立与设备端的连接，按照以下步骤进行操作：

1. 在 Mac OS Launchpad 中单击 SCVPN，启动客户端。
2. 点击“新建”，弹出<新建连接>对话框。

3. 依次填写对话框中的各项，然后点击“确定”按钮。

- **连接名称**：为此VPN 连接指定名称。
- **描述**：为此VPN 连接指定描述信息。
- **主机**：填写设备端的 IP 地址或域名。
- **端口**：填写设备端的 HTTPS 端口号。
- **用户名**：填写登录用户名。
- **密码**：填写与用户名相对应的密码。
- **记住密码**：选择是否记住密码。
- **国密 SSL**：勾选复选框，使用国密 SSL 协议方式建立连接。

4. 在连接列表中选择连接名称，在工具栏中点击“连接”。如果没有选择记住密码，则在弹出窗口中输入用户名对应的密码并点击“确认”。客户端开始连接设备端。

连接成功后，客户端状态栏显示“连接成功”，同时，系统通知栏显示已连接图标（ ），此时就可以实现客户端与设备端之间的加密通信。

客户端菜单

客户端“SCVPN”菜单包括如下选项：

- 关于 SCVPN：显示此客户端相关信息。

- 退出 SCVPN：退出客户端。

客户端“日志”菜单包括如下选项：

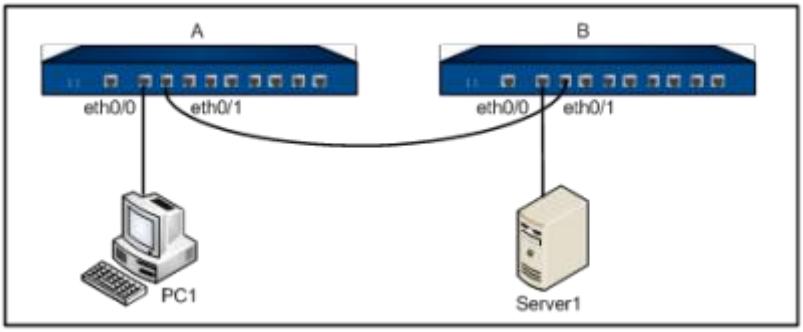
- 查看：查看日志信息。
- 日志级别：选择需要查看的日志的日志级别。选择菜单栏中位于下部的级别时，显示的日志包含上方级别的日志。选择菜单栏中位于上部的级别时，显示的日志不包含下方级别的日志。

SSL VPN 配置举例

该节介绍 SSL VPN 配置实例。分别针对用户名密码方式认证和 USB Key 认证方式进行进行举例。

组网需求

外网PC1（IP：6.6.6.5/24）通过 设备设备访问内网服务器 Server1（IP：10.160.65.52/21），要求使用 SSL VPN 对数据进行加密。组网图参见下图：



- 需求一：使用用户名密码方式对用户进行认证。
- 需求二：使用USB Key 方式对用户进行认证。

需求一配置步骤

第一步：创建本地用户：

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

第二步：配置 SSL VPN 地址池：

```
hostname(config)# scvpn pool pool1
hostname(config-pool-scvpn)# address 20.1.1.1 20.1.1.100 netmask 255.255.255.0
hostname(config-pool-scvpn)# dns 20.1.1.1
hostname(config-pool-scvpn)# wins 20.1.1.2
hostname(config-pool-scvpn)# exit
hostname(config)#
```

第三步：配置 SSL VPN 实例。系统默认添加 split-tunnel-route 0.0.0.0/0 的路由条目，如需限定远程用户访问范围，请使用 no split-tunnel-route 0.0.0.0/0 命令。

```
hostname(config)# tunnel scvpn ssl1
hostname(config-tunnel-scvpn)# pool pool1
hostname(config-tunnel-scvpn)# aaa-server local
hostname(config-tunnel-scvpn)# interface ethernet0/5
hostname(config-tunnel-scvpn)# https-port 4433
hostname(config-tunnel-scvpn)# split-tunnel-route 10.160.64.0/21
hostname(config-tunnel-scvpn)# exit
hostname(config)#
```

第四步：创建隧道接口并把 SSL VPN 实例绑定到此接口（隧道接口的 IP 地址必须与 SSL VPN 地址池的 IP 地址在同一网段）：

```
hostname(config)# zone VPN
hostname(config-zone-VPN)#
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone VPN
hostname(config-if-tun1)# ip address 20.1.1.101/24
hostname(config-if-tun1)# tunnel scvpn ssl1
hostname(config-if-tun1)# exit
hostname(config)#
```

第五步：配置从VPN 安全域到trust 安全域的策略：

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone VPN
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)# exit
hostname(config-policy)# exit
hostname(config)#
```

第六步:在PC1 的浏览器中输入 https://6.6.6.1:4433，在弹出的登录页面输入用户名密码，分别是“user1”和“123456”。认证通过后下载并安装 Secure Connect。

第七步:通过 Web 方式或客户端方式登录 SSL VPN 设备端成功后，PC1 便可通过 SSL VPN 安全地访问 trust 安全域中的资源。

需求二配置步骤

为了增加安全性，在需求一的基础上开启 USB Key 证书认证功能：只有当用户的 USB Key 支持标准的 Windows SDK （Certificate Store Functions），并且存储的证书合法时，用户才可以登录设备。本例以用户持有 UKey 为例。

准备工作

使用 USB Key 认证，用户需要做以下准备工作：

- 准备数字证书和相应的 CA 证书。
- 准备 UKey 和配套光盘。
- 使用 UKey 管理员软件导入数字证书到 USB Key。

配置步骤

第一步：配置设备端：

```
#创建 PKI 信任域 stone，并指定该信任域的证书获得方式为 terminal
hostname(config)# pki trust-domain stone
hostname(config-trust-domain)# enrollment terminal
hostname(config-trust-domain)# exit
hostname(config)#
#开启 SSL VPN 实例 SSL1 的 USB Key 证书认证功能，并指定 CA 证书的信任域
hostname(config)# tunnel scvpn ssl1
hostname(config-tunnel-scvpn)# client-cert-auth
hostname(config-tunnel-scvpn)# client-auth-trust-domain stone
hostname(config-tunnel-scvpn)# exit
hostname(config)#
#导入 CA 证书文件到 CA 证书的信任域
hostname(config)# exit
hostname# import pki stone cacert from tftp server 192.168.1.2 certnew.cer
```

第二步：客户端操作，步骤如下：

1. 在客户端 PC 安装 UKey 驱动程序。
2. 插入 USB Key。
3. 打开 SSL VPN 客户端，按下图所示依次填写登录信息（密码为“123456”；PIN 码为 USB Key 的用户口令，默认为 1111）。填写完毕，点击『登录』按钮，进行连接。

第 8 章 流量管理

本章包含以下内容：

iQoS：介绍了 iQoS 的实现机制、智能流量管理的处理流程、管道的概念及如何配置 iQoS 等。

负载均衡：介绍了服务器负载均衡和链路负载均衡的概念及配置方法。

会话限制：介绍了会话限制的相关概念及配置方法。

iQoS

注意:如果用户在升级到 5.5 版本前已经配置了旧版QoS 功能，则旧版QoS 在升级后生效，无对应的WebUI，需要在 CLI 中进行配置； iQoS 功能将在WebUI 上隐藏且不生效。如果用户在升级到 5.5 版本前，没有配置旧版 QoS 功能，在升级后，将默认启动 iQoS 功能，可在WebUI 进行配置。此时，旧版QoS 功能不生效。

本章内容包含智能流量管理（iQoS）和 QoS 管理，与产品版本的具体关系如下表所示，请根据购买的产品版本参见对应的手册说明。iQoS/QoS 与产品版本对应关系如下:

产品版本	说明
5.5 前的版本，没有配置QoS 管理功能	升级后，系统默认使用 iQoS 管理功能。
5.5 前的版本，已配置QoS 管理功能	升级后，QoS 管理功能仍然生效。建议用户使用 iQoS 管理功能，iQoS 支持原 QoS 的所有功能，切换到 iQoS 管理功能的方法，请参见 iQoS。
5.5 版本和 5.5 后的版本	系统默认使用 iQoS 管理功能。

iQoS 管理

随着网络应用的快速发展以及网民数量的增加，网络带宽的压力也与日俱增，这导致企事业单位包括运营商都面临着网络拥堵和带宽资源有效利用的问题。设备提供的智能流量管理功能，能够保障和管理优化重要带宽，提高用户的网络体验和带宽资源利用率。

流量管理，即网络为特定流量提供更高优先服务的同时控制抖动和延迟的能力，并且能够降低数据传输丢包率。当网络过载或拥塞时，系统能够确保重要业务流量的正常传输。

设备支持许可证控制的流量管理功能。如需使用流量管理功能，请先申请并正确安装流量管理许可证。

实现机制

数据包进入系统后，首先会被分类和标记。对于分类标记后的流量，系统会通过整形机制使流量平滑的转发或管制机制丢弃。若选择整形机制转发流量，系统则会通过拥塞管理机制和拥塞避免机制对数据包进行管理，为数据包排列优先次序并且在发生拥塞时保证高优先级数据包优先调度。

通常来讲，实现流量管理的工具包括:

- 分类和标记工具：分类和标记的过程就是识别出需进行不同处理（优先或者区分）的流量的过程。分类和标记是执行流量管理的第一步。
- 管制和整形工具：识别流量违约并做出响应。管制工具对流量违约进行即时检查，发现违约后立即采取设定的动作进行处理。整形工具是一个与排队机制一起工作的流量平滑工具，整形的目的是控制流量永远不超出指定的速率，使流量平滑地转发。

- 拥塞管理工具：即排队工具，应用在产生拥塞处。由于网络之间的速率不匹配，在广域网或者局域网中都有可能出现拥塞。只有当发生拥塞时，排队工具才会被启用。
- 拥塞避免工具：拥塞避免工具是排队算法的补充，它的目的是为了处理基于 TCP 的数据流。

智能流量管理功能

设备通过配置管道来实现流量管理。管道，即带宽通道，是一个虚拟概念。系统以管道为单位对流量进 行划分，并根据管道配置的流控动作对管道内的流量进行管控。所有流经设备的流量，都将按照设置的匹配条件进入虚拟管道。未匹配到的流量将进入系统预定义的默认管道。

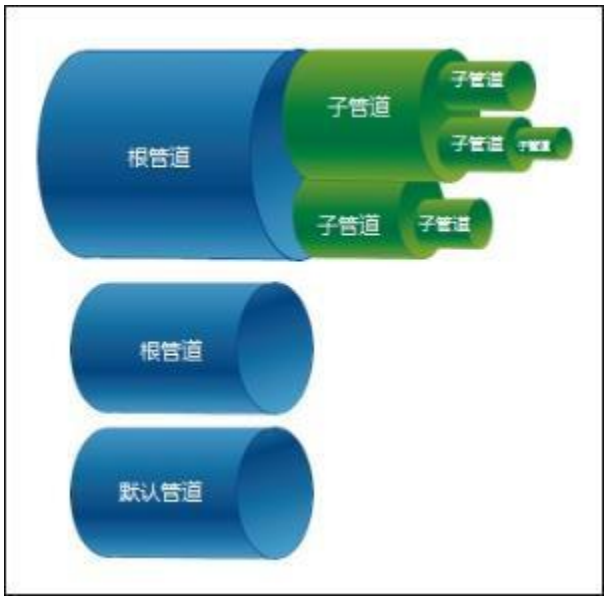
管道（除默认管道）必须包含两部分，分别是流量匹配条件和流量管理动作:

- 流量匹配条件：定义设备需要匹配的流量，从而设备可以将流量进行区分。流经设备的流量会根据用户设置的条件分类，划入对应的管道。系统为匹配到匹配条件的流量提供带宽控制。
- 流量管理动作：对已被划分到管道中的流量所做的动作。流控分为正向控制和反向控制。正向控制即对从源到目的方向的流量进行控制；反向控制即对从目的到源方向的流量进行控制。

注意:一个管道可以有多个流量匹配条件，各个匹配条件之间为“或”的关系。流量只要匹配到其中一个匹配条件，就会进入该管道。

多级管道

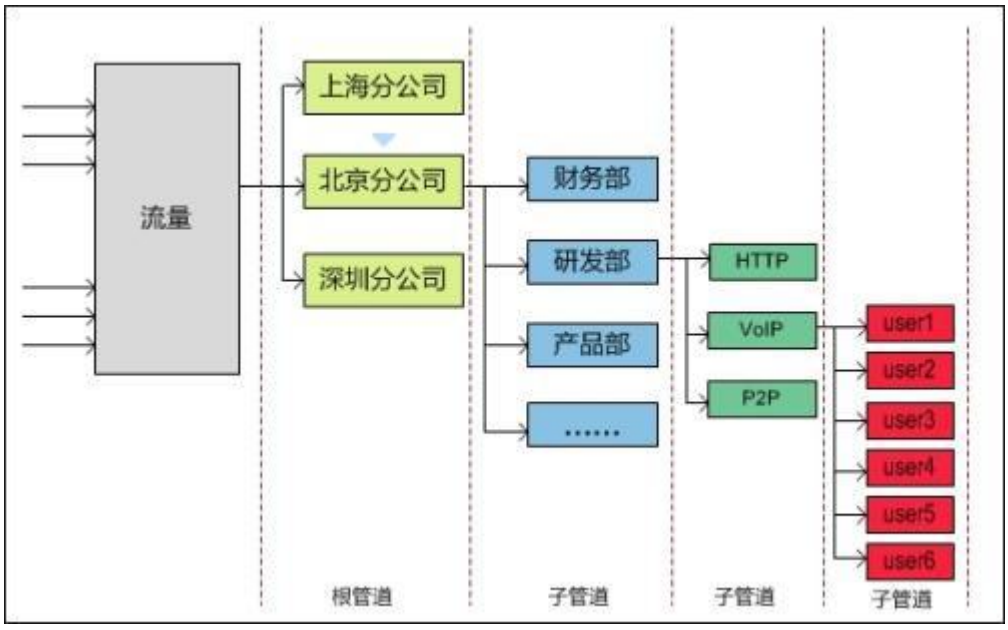
为了给用户提供灵活和方便的配置，系统支持多级管道。配置多级管道，可将不同用户的不同应用分别限制在一定带宽之内，从而能优先保障重要用户或重要应用的带宽。管道最多支持四级嵌套，默认管道不可嵌套子管道。管道逻辑关系如下图所示:



- 用户可创建多个根管道，各个根管道之间是彼此独立的。每个根管道下均可嵌套三级子管道。

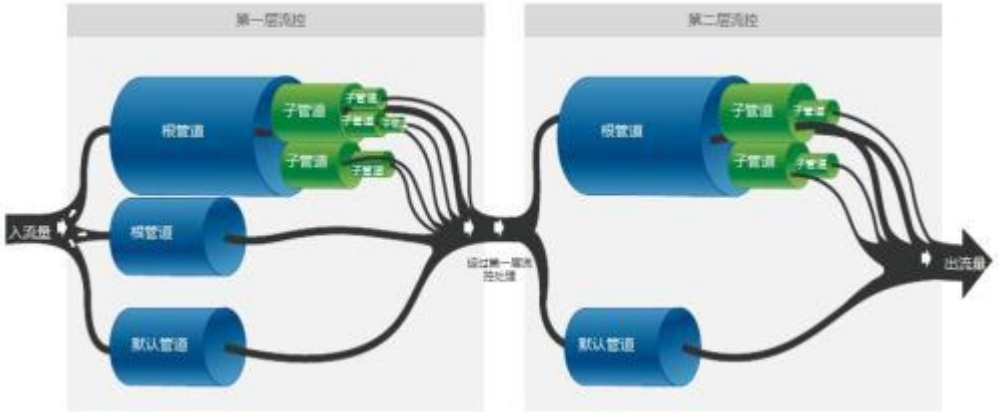
- 子管道的最小带宽之和不能大于其上一级管道的最小带宽，最大带宽也不能大于其上一级管道的最大带宽
- 用户若在根管道上配置了正向或反向的流量管理动作后，该根管道下的所有子管道都必须继承根管道设定的流量方向。
- 仅配置了反向流量管理动作的管道不可用。

以某企业的应用场景为例说明如何嵌套多级管道。如下图所示，管理员可创建一个根管道，限制该企业北京分公司的流量。创建一个子管道，限制其研发部门的流量。再创建子管道对研发部应用进行划分，限制不同应用拥有不同的带宽。最后为某种应用的每用户设置子管道，限制该应用的每位用户的流量。



流量管理处理流程

系统支持两层流控，即第一层流控和第二层流控。在每层流控中，流量的具体控制通过管道来实现。经过第一层流控处理过的流量进入第二层流控，系统再根据第二层流控的管道设置对流量进行进一步管控。流量进入设备后，流量管理处理流程如下图所示：



根据上图所示，系统的流控处理流程描述如下：

1. 流量首先进入第一层流控，系统根据第一层流控中管道的匹配条件设置划分流量到不同的管道中。不匹配任何管道的流量进入默认管道。如果存在相同匹配条件的根管道，流量优先匹配位置靠前的根管道。流量进入根管道后，再根据子管道的匹配条件逐层匹配。
2. 系统根据管道配置的流控动作对匹配到的流量进行管控。
3. 经过第一层流控处理的流量进入第二层流控进行再次管控。系统在第二层流控中的管道匹配以及流量管控原理与第一层流控相同。
4. 流控处理结束。

注意：

- 对于部分设备（SG-6000-X6150、SG-6000-X6180、SG-6000-X7180）,使用 iQoS 功能前须确保设备已安装 QSM 模块。
- 对于 SG-6000-X7180，当设备没有 QSM 模块时，用户还可以安装 IOM 模块来获取 iQoS 功能（需确保设备已经安装 iQoS 许可证）。这种情况下，iQoS 功能仅支持管制模式，不支持其他的流控模式。
- 对于 SG-6000-X7180，当设备同时装有 QSM 和 IOM 模块时，QSM 模块优先生效，来提供 iQoS 功能。
- 对于 SG-6000-X7180，当设备装有多个 IOM 模块时，各个 IOM 模块独立工作，仅处理本模块的流量，不对其他 IOM 模块的流量进行限制。

配置 iQoS

系统通过创建管道来实现流量管理，进而保障和优化管理网络带宽。创建管道，包括：

1. 创建流量匹配条件，系统对匹配到匹配条件的流量进行控制。若为管道配置多个匹配条件，各匹配条件之间为“或”的关系。
2. 根据需求创建流量白名单。目前仅根管道和默认管道支持配置白名单。配置后，系统将不对白名单中指定的流量做流量管理。
3. 指定流量管理动作，即对已被划分到管道中的流量指定动作。

指定流控层级

指定进入第一层流控或第二层流控，并进入流控模式，用户可创建管道实现流量管理。在全局配置模式下，使用以下命令：

qos-engine {first | second}

- first – 指定进入第一层流控。

- second – 指定进入第二层流控。

启用/禁用流控层级/根管道/子管道

启用/禁用流控层级，在指定层级的流控模式下，使用以下命令：

- 禁用：disable
- 启用：no disable

启用/禁用根管道，在指定根管道配置模式下，使用以下命令：

- 禁用：disable
- 启用：no disable

启用/禁用子管道，在指定子管道配置模式下，使用以下命令：

- 禁用：disable
- 启用：no disable

注意:被禁用的流控层级或者管道不参与流控处理。不可用的管道也不参与流控处理。

启用/禁用 NAT IP 匹配

在指定层级的流控模式下，用户可按需启用 NAT IP 匹配功能。启用后，对于该流控层级，系统将使用流量的源 NAT 后和目的NAT 前的 IP 地址作为匹配项。如果匹配成功，系统将会对这些 IP 地址进行流控管理。启用 NAT IP 匹配功能，在指定层级的流控模式下，使用以下命令：

match-nat-ip enable

在指定层级的流控模式下，使用 no match-nat-ip enable 禁用 NAT IP 匹配。

注意:在启用NAT IP 匹配功能之前，必须配置 NAT 规则。否则，该配置不生效。

创建根管道

创建根管道，并进入该根管道配置模式。如果指定的根管道名称已经存在，则直接进入根管道配置模式。在流控模式下，使用以下命令：

root-pipe {pipe-name | default}

- pipe-name – 指定将要创建的根管道名称。
- default – 进入默认管道。

在流控模式下，使用该命令 no 的形式删除创建的根管道：

no root-pipe pipe-name

注意:

- 管道名字不能超过 63 个字符。
- 根管道下可嵌套 3 级子管道。
- 默认管道不能删除。

进入根管道配置模式后，可进行如下配置:

- 启用/禁用根管道
- 配置根管道流量匹配条件
- 配置根管道流量白名单
- 配置根管道流量管理动作
- 配置根管道流控模式
- 为根管道指定时间表
- 创建子管道

创建子管道

创建子管道，并进入子管道配置模式。如果指定的子管道名称已经存在，则直接进入子管道配置模式。在管道配置模式下，使用以下命令:

pipe *pipe-name*

- *pipe-name* – *指定将要创建的子管道名称。*

在管道配置模式下，使用该命令 no 的形式删除创建的子管道:

no pipe *pipe-name*

注意:

- 管道名字不能超过 63 个字符。
- 删除子管道，需在其父管道配置模式下，使用 no pipe*pipe-name* 命令。

进入子管道配置模式后，可进行如下配置:

- 启用/禁用子管道

- 配置子管道流量匹配条件
- 创建子管道

配置流量匹配条件

配置匹配条件前，用户需先创建匹配条件并进入其匹配条件配置模式。如果指定的 ID 已存在，直接进入其匹配条件配置模式。若不指定 ID，系统将直接创建一个匹配条件并进去其配置模式。创建匹配条件并且进入匹配条件配置模式。在管道配置模式下，使用以下命令：

pipe-map *[id]*

- *id* – 指定匹配条件的 ID。

使用 **no pipe-map** *[id]*命令删除指定的匹配条件。

进入匹配条件配置模式后，可使用的配置流量匹配条件的命令如下：

- 指定流量源安全域的名称：**src-zone** *src-zone*
- 删除流量源安全域的名称：**no src-zone**
- 指定流量目的安全域的名称：**dst-zone** *dst-zone*
- 删除流量目的安全域的名称：**no dst-zone**
- 指定流量的源主机名称：**src-host** *host-name*
- 删除流量的源主机名称：**no src-host** *host-name*
- 指定流量的目的主机名称：**dst-host** *host-name*
- 删除流量的目的主机名称：**no dst-host** *host-name*
- 指定流量的源地址（IPv4 或 IPv6）：**src-ip** {*ip/netmask* | *ip-address netmask* | *ipv6-address/prefix* }
- 删除指定流量的源地址（IPv4 或 IPv6）：**no src-ip** {*ip/netmask* | *ip-address netmask* | *ipv6-address/prefix* }
- 指定流量的目的地址（IPv4 或 IPv6）：**dst-ip** {*ip/netmask* | *ip-address netmask* | *ipv6-address/prefix* }
- 删除流量的目的地址（IPv4 或 IPv6）：**no dst-ip** {*ip/netmask* | *ip-address netmask* | *ipv6-address/prefix* }
- 指定流量的源地址范围（IPv4 或 IPv6）：**src-range***min-ip*[*max-ip*]
- 删除流量的源地址范围（IPv4 或 IPv6）：**no src-range***min-ip* [*max-ip*]
- 指定流量的目的地址范围（IPv4 或 IPv6）：**dst-range***min-ip* [*max-ip*]

- 删除流量的目的地址范围（IPv4 或 IPv6）：**no dst-range***min-ip* [*max-ip*]
- 指定流量的入接口名称：**ingress-if** *interface-name*
- 删除流量的入接口名称：**no ingress-if** *interface-name*
- 指定流量的出接口名称：**egress-if** *interface-name*
- 删除流量的出接口名称：**no egress-if** *interface-name*
- 指定流量的源地址条目（IPv4 或 IPv6）：**src-addr***address-book*
- 删除流量的源地址条目（IPv4 或 IPv6）：**no src-addr***address-book*
- 指定流量的目的地址条目（IPv4 或 IPv6）：**dst-addr***address-book*
- 删除流量的目的地址条目（IPv4 或 IPv6）：**no dst-addr***address-book*
- 指定用户及其所属的 AAA 服务器：**user** *AAA-server user-name*
- 删除用户及其所属的 AAA 服务器：**no user** *AAA-server user-name*
- 指定用户组及其所属的 AAA 服务器：**user-group** *AAA-server usergroup-name*
- 删除用户组及其所属的 AAA 服务器：**no user-group** *AAA-server usergroup-name*
- 指定应用或应用组，包括预定义应用和自定义应用：**application** *app-name*
- 删除应用或应用组，包括预定义应用和自定义应用：**no application** *app-name*
- 指定服务组或者服务的名称：**service** *service-name*
- 删除服务组或者服务的名称：**no service** *service-name*
- 指定 ToS 字段：**tos** *tos-value*
- 删除 ToS 字段：**no tos** *tos-value*
- 指定 Vlan 信息：**vlan** *vlan-id*
- 删除 Vlan 信息：**no vlan** *vlan-id*
- 指定 URL 类别：**url-category** *category-name*
- 删除 URL 类别：**no url-category** *category-name*
- 指定 TrafficClass 字段：**traffic-class***traffic-class-value*
- 删除 TrafficClass 字段：**no traffic-class***traffic-class-value*

注意:对于部分设备（SG-6000-X6150、SG-6000-X6180、SG-6000-X7180 、SG-6000-X10800）配置流量匹配条件时，不支持指定服务组或服务名称。

配置流量白名单

配置流量白名单。配置后，系统将不对白名单中指定的流量做流量管理。用户可为根管道或默认管道指定流量白名单。

配置白名单前，用户需先创建白名单并进入其白名单配置模式。如果指定的 ID 已存在，直接进入其白名单配置模式。若不指定 ID，系统将直接创建一个白名单并进去其配置模式。创建白名单并且进入白名单配置模式，在管道配置模式下，使用以下命令：

exception-map [*id*]

- *id* – 指定白名单的 ID。

使用 **no exception-map** [*id*]命令删除指定的白名单。

进入白名单配置模式后，可使用的配置白名单匹配条件的命令如下：

- 指定流量源安全域的名称：**src-zone***src-zone*
- 删除流量源安全域的名称：**no src-zone**
- 指定流量目的安全域的名称：**dst-zone***dst-zone*
- 删除流量目的安全域的名称：**no dst-zone**
- 指定流量的入接口名称：**ingress-if** *interface-name*
- 删除流量的入接口名称：**no ingress-if** *interface-name*
- 指定流量的出接口名称：**egress-if** *interface-name*
- 删除流量的出接口名称：**no egress-if** *interface-name*
- 指定流量的源地址：**src-ip** {*ip/netmask* | *ip-address netmask*}
- 删除指定流量的源地址：**no src-ip** {*ip/netmask* | *ip-address netmask*}
- 指定流量的目的地址：**dst-ip** {*ip/netmask* | *ip-address netmask*}
- 删除流量的目的地址：**no dst-ip** {*ip/netmask* | *ip-address netmask*}
- 指定用户及其所属的 AAA 服务器：**user** *AAA-server user-name*
- 删除用户及其所属的 AAA 服务器：**no user** *AAA-server user-name*
- 指定用户组及其所属的 AAA 服务器：**user-group** *AAA-server usergroup-name*
- 删除用户组及其所属的 AAA 服务器：**no user-group** *AAA-server usergroup-name*
- 指定应用或应用组，包括预定义应用和自定义应用：**application** *app-name*

- 删除应用或应用组，包括预定义应用和自定义应用：**no application** *app-name*
- 指定服务组或者服务的名称：**service** *service-name*
- 删除服务组或者服务的名称：**no service** *service-name*
- 指定 ToS 字段：**tos** *tos-value*
- 删除 ToS 字段：**no tos** *tos-value*
- 指定 Vlan 信息：**vlan** *vlan-id*
- 删除 Vlan 信息：**no vlan** *vlan-id*
- 指定 URL 类别：**url-category** *category-name*
- 删除 URL 类别：**no url-category** *category-name*

注意:对于部分设备（SG-6000-X6150、SG-6000-X6180、SG-6000-X7180、SG-6000-X10800）配置流量白名单匹配条件时，不支持指定服务组或服务名称。

配置根管道流量管理动作

配置根管道流量管理动作，在根管道配置模式下，使用以下命令：

pipe-rule {**forward** | **backward**} **bandwidth** {**Kbps** | **Mbps** | **Gbps** *bandwidth-value* [**per-ip-min** *min-value*] [**per-ip-max** *max-value* [**delay** *delay-time*]] [**per-ip-using** {**src-ip** | **dst-ip**}] [**tos-marking** *tos-value*] [**mode aggressive** [**strength-level** *level-value*]] [**priority** *value*]

pipe-rule {**forward** | **backward**} **bandwidth** {**Kbps** | **Mbps** | **Gbps**} [**per-user-min** *min-value*] [**per-user-max** *max-value* [**delay** *delay-time*]] [**tos-marking** *tos-value*] [**mode aggressive** [**strength-level** *level-value*]] [**priority** *value*]

pipe-rule {**forward** | **backward**} **bandwidth** {**Kbps** | **Mbps** | **Gbps**} *bandwidth-value* **average-using** {**src-ip** | **dst-ip** | **user**} [**tos-marking** *tos-value*] [**mode aggressive** [**strength-level** *level-value*]] [**priority** *value*]

- **forward** – 对匹配到匹配条件中从源到目的方向的流量指定流控动作。
- **backward** -对匹配到匹配条件中从目的到源方向的流量指定流控动作。
- **bandwidth** {**Kbps** | **Mbps** | **Gbps**} - 指定管道的最小带宽值。选择 **Kbps** 时，取值范围为 32Kbps 到 100000000Kbps；选择 **Mbps** 时，取值范围为 1Mbps 到 100000Mbps；选择 **Gbps** 时，取值范围为 1Gbps 到 100Gbps。percent，**Mbps，Gbps** 只在配置子管道的时候生效。
- **per-ip-min** *min-value* -指定每个 IP 的最小带宽值。取值范围为 32Kbps 到 1000000Kbps。
- **per-ip-max** *max-value* -指定每个 IP 的最大带宽值。取值范围为 32Kbps 到 1000000Kbps。
- **per-ip-using** {**src-ip**|**dst-ip**} - 选择为管道内每个源 IP（src-ip）或者目的 IP（dst-ip）限制带宽。该选项仅当用户配置了每 IP 最小/最大带宽值时生效。

- **per-user-min** *min-value* - 指定每个用户的最小带宽值。选择 **Kbps** 时，取值范围为 32Kbps 到 10000000KBPS；选择 **Mbps** 时，取值范围为 1Mbps 到 10000Mbps。
- **per-user-max** *max-value* - 指定每个用户的最大带宽值。选择 **Kbps** 时，取值范围为 32Kbps 到 10000000Kbps；选择 **Mbps** 时，取值范围为 1Mbps 到 10000Mbps。
- **delay** *delay-time* – 指定延时时间。取值范围为 1 秒到 3600 秒。在延时时间范围内，对每 IP/用户的最大带宽限制不生效。
- **tos-marking** *tos-value* - 指定 TOS 字段。
- **mode aggressive** [**strength-level** *level-value*] - 开启对端抑制功能。默认情况下，该功能为关闭状态。对端抑制功能可根据用户分配的带宽， 使到达设备的流量尽可能与分配带宽相符，以减少设备上的丢包。开启对端抑制功能后，默认抑制强度（**strength-level**）为 1，抑制强度取值范围为 1-8。数值越大，抑制强度越大，丢包越少。
- **priority** *value* - 指定管道优先级。取值范围为 0 到 7，默认值为 7。数值越小，表示该管道的优先级越高。优先级较高的管道，系统将优先调度，并优先借用其他管道的空闲带宽。
- **average-using** {**src-ip** | **dst-ip** | **user**} - 对管道内每个源 IP（src-ip）或者目的 IP（dst-ip）或者用户（user）平均分配带宽。

使用该命令 no 的形式删除指定方向的流量管理动作。

注意:

- 不可同时指定每用户和每 IP 的带宽限制。
- 对端抑制功能只能在正反流控的一个方向开启。只有最末端管道支持配置对端抑制功能。

配置子管道流量管理动作

配置子管道流量管理动作，在根管道配置模式下，使用以下命令:

pipe-rule {**forward** | **backward**} {**min** | **reserve-bandwidth**} {**percent** | **Kbps** | **Mbps** | **Gbps**} *value* **max** {**percent** | **Kbps** | **Mbps** | **Gbps**} *max-value* [**per-ip-min** *min-value*] [**per-ip-max** *max-value* [**delay** *delay-time*]] [**per-ip-using** {**src-ip** | **dst-ip**}] [**tos-marking** *tos-value*] [**mode aggressive** [**strength-level** *level-value*]] [**priority** *value*]

pipe-rule {**forward** | **backward**} {**min** | **reserve-bandwidth**} {**percent** | **Kbps** | **Mbps** | **Gbps**} *min-value* **max** {**percent** | **Kbps** | **Mbps** | **Gbps**} *max-value* [**per-user-min** *min-value*] [**per-user-max** *max-value* [**delay** *delay-time*]] [**tos-marking** *tos-value*] [**mode aggressive** [**strength-level** *level-value*]] [**priority** *value*]

- **forward** – 对匹配到匹配条件中从源到目的方向的流量指定流控动作。
- **backward** -对匹配到匹配条件中从目的到源方向的流量指定流控动作。

- {**min** | **reserve-bandwidth**} {**percent** | **Kbps** | **Mbps** | **Gbps**} *value* -指定管道的最小带宽值，或为管道设定保留带宽。min 代表指定最小带宽。**reserve-bandwidth** 代表指定保留带宽。设定最小带宽/保留带宽时，**percent** 表示此管道的最小带宽/保留带宽占父管道带宽的百分比，取值范围为 1 到 100；选择 **Kbps** 时，取值范围为 32Kbps 到 100000000Kbps；选择 **Mbps** 时，取值范围为 1Mbps 到 100000Mbps；选择 **Gbps** 时，取值范围为 1Gbps 到 100Gbps。
- **max** {**percent** | **Kbps** | **Mbps** | **Gbps**} *max-value* - 指定管道的最大带宽值或最大带宽占比。**percent** 表示此管道的最大带宽占父管道带宽的百分比，取值范围为 1 到 100；选择 **Kbps** 时，取值范围为 32Kbps 到 100000000Kbps；选择 **Mbps** 时，取值范围为 1Mbps 到 100000Mbps；选择 **Gbps** 时，取值范围为 1Gbps 到 100Gbps。
- **per-ip-min** *min-value* -指定每个 IP 的最小带宽值。取值范围为 32Kbps 到 1000000Kbps。
- **per-ip-max** *max-value* -指定每个 IP 的最大带宽值。取值范围为 32Kbps 到 1000000Kbps。
- **per-ip-using** {**src-ip**|**dst-ip**} - 选择为管道内每个源 IP（src-ip）或者目的 IP（dst-ip）限制带宽。该选项仅当用户配置了每 IP 最小/最大带宽值时生效。
- **per-user-min** *min-value* - 指定每个用户的最小带宽值。选择 **Kbps** 时，取值范围为 32Kbps 到 10000000KBPS；选择 **Mbps** 时，取值范围为 1Mbps 到 10000Mbps。
- **per-user-max** *max-value* - 指定每个用户的最大带宽值。选择 **Kbps** 时，取值范围为 32Kbps 到 10000000Kbps；选择 **Mbps** 时，取值范围为 1Mbps 到 10000Mbps。
- **delay** *delay-time* – 指定延时时间。取值范围为 1 秒到 3600 秒。在延时时间范围内，对每 IP/用户的最大带宽限制不生效。
- **tos-marking** *tos-value* - 指定 TOS 字段。
- **mode aggressive** [**strength-level** *level-value*] - 开启对端抑制功能。默认情况下，该功能为关闭状态。对端抑制功能可根据用户分配的带宽， 使到达设备的流量尽可能与分配带宽相符，以减少设备上的丢包。开启对端抑制功能后，默认抑制强度（**strength-level**）为 1，抑制强度取值范围为 1-8。数值越大，抑制强度越大，丢包越少。
- **priority** *value* - 指定管道优先级。取值范围为 0 到 7，默认值为 7。数值越小，表示该管道的优先级越高。优先级较高的管道，系统将优先调度，并优先借用其他管道的空闲带宽。

注意:

- 不可同时指定每用户和每 IP 的带宽限制。
- 对端抑制功能只能在正反流控的一个方向开启。只有最末端管道支持配置对端抑制功能。

配置根管道的流控模式

根管道的流控模式可以为以下三种模式:

- 整形模式：配置该模式后，系统能够限制数据传输速率，使流量平滑地转发。根管道范围内流量将支持带宽借用和优先级调度
- 管制模式：配置该模式后，系统将对超出带宽限制的流量进行丢弃。该模式不支持带宽借用和优先级调度，且不做最小带宽保障。
- 监控模式：配置该模式后，系统仅对匹配到的流量进行监控和统计，不对流量进行任何控制。

带宽借用：即同一根管道内的所有子管道，在确保自身管道流量正常转发的情况下，可将空闲流量分配给带宽不足的管道。

优先级调度：即在流量拥塞时，超出带宽限制的流量将进入等待队列，用户可设置优先级以确保某些应用优先调度。

默认情况下。流控模式为整形模式。指定根管道的流控模式，在根管道配置模式下，使用以下命令：

qos-mode {police | shape | stat}

- police – 指定流控模式为管制模式。
- shape – 指定流控模式为整形模式。
- stat – 指定流控模式为监控模式。

配置根管道时间表

设备支持时间表功能，用户可以为根管道指定一个时间表条目，令根管道在指定的时间内生效。配置根管道时间表功能，在根管道配置模式下，使用以下命令：

schedule *schedule-name*

- schedule-name – 指定时间表的名称。

使用 no schedule *schedule-name* 取消时间表配置。

{b}提示: {/b}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。

配置子管道时间表

用户可以为子管道指定一个时间表条目，令子管道在指定的时间内生效。配置子管道时间表功能，在子管道配置模式下，使用以下命令：

schedule *schedule-name*

- *schedule-name* – 指定时间表的名称。

使用 **no schedule** *schedule-name* 取消时间表配置。

{b}提示: {/b}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。

配置根管道绑定到 QSM 模块

对于部分设备（SG-6000-X6150、SG-6000-X6180、SG-6000-X7180、SG-6000-X10800）配置 iQoS 功能时，可以将根管道绑定到指定 QSM 模块，提高流量限制的准确性。配置根管道绑定到 QSM 模块，在根管道配置模式下，使用以下命令：

bind slot {*number*}

- *number* – 指定 QSM 模块所在的槽位号。

查看流控层级及管道的配置信息

查看流控层级及管道的配置信息，在任何模式下，使用以下命令：

show qos-engine {**first** | **second**} [**root-pipe** *pipe-name*]

- **first** – 查看第一层流控及其管道的配置信息。
- **second** -查看第二层流控及其管道的配置信息。
- **root-pipe** *pipe-name* -查看指定根管道的配置信息。

负载均衡

本章节包含以下内容：

- 服务器负载均衡:包含 SLB 服务器池、均衡算法、监测规则等的配置方法。
- 链路负载均衡:包含入站链路负载均衡和出站负载均衡及相关的配置举例。

服务器负载均衡

服务器负载均衡功能（SLB），可以通过负载均衡算法均衡流量到不同的内网服务器，从而达到充分利用各内网服务器，提高业务处理能力。可通过如下方式进行服务器负载均衡：

- 均衡流量到不同的内网服务器的指定端口，适用于不同内网服务器在各自指定端口分别且同时提供同一个应用服务的场景。
- 均衡流量到同一内网服务器的不同端口，适用于同一服务器在多个端口运行多个进程来提供同一个应用服务的场景。

- 结合以上两种方式进行流量均衡。

通过 CLI 配置服务器负载均衡功能，包含以下配置：

- 添加/删除 SLB 服务器池条目
- 配置 SLB 服务器池条目
- 配置服务器负载均衡的算法
- 添加/删除服务器负载均衡的监测规则
- 配置监测警戒值
- 配置 DNAT 规则引用 SLB 服务器池条目

添加/删除 SLB 服务器池条目

StoneOS 系统拥有一个全局 SLB 服务器池，是一个用来储存内网服务器的 IP 地址范围与其名称的对应关系的数据库。SLB 服务器池中的 IP 地址与名称的对应关系条目被称作 SLB 服务器池条目。

用户需要为全局 SLB 服务器池定义 SLB 服务器池条目。在全局配置模式下，使用 **slb-server-pool** 命令向 SLB 服务器池中添加一个SLB 服务器池条目，同时进入 SLB 服务器池配置模式：

slb-server-pool *pool-name*

- *pool-name* - 指定要添加的 SLB 服务器池条目的名称。

使用该命令 no 的形式将 SLB 服务器池条目从 SLB 服务器池中删除：

no slb-server-pool *pool-name*

注意:已经被引用的 SLB 服务器池条目不能被删除。

配置 SLB 服务器池条目

SLB 服务器池条目参数包括 IP 地址范围、端口数、权重、最大连接数等。SLB 服务器池条目的 IP 地址范围以下 2 种：

- IP 地址/子网掩码，如 10.100.2.0/24、10.100.20.1/32 等。
- IP 地址段，如 10.100.2.3 – 10.100.2.100

在 SLB 服务器池配置模式下，使用以下命令来为 SLB 服务器池条目添加成员并配置相关参数。最多可添加 256 个成员。

server {**ip** *ip/netmask* | **ip-range** *min-ip* [*max-ip*]} [**port** *port-num*] {**weight-per-server** *weight-num*} [**max-connection-per-server** *max-num*]

- **ip** *ip-address* – 指定服务器的 IP 地址和网络掩码。
- **ip-range** *start-ip* [*max-ip*] – 指定服务器 IP 地址范围段。*start-ip* 为起始 IP 地址，*end-ip* 为结束 IP 地址。
- **port** *port-num* – 指定服务器端口号。
- **weight-per-server** *weight-num* – 指定负载均衡中流量转发的权重。范围是 1 到 255，默认值是 1。
- **max-connection-per-server** *max-num* – 指定服务器最大连接数。范围是 1 到 1000000000，默认值是 0，表示无最大连接数限制。

使用以上命令 no 的形式删除指定 SLB 服务器池条目成员：

no server {**ip** *ip/netmask* | **ip-range** *min-ip* [*max-ip*]} [**port** *port-num*] {**weight-per-server** *weight-num*} [**max-connection-per-server** *max-num*]

配置服务器负载均衡的算法

系统支持的服务器负载均衡算法包括： 加权散列算法、加权最小连接数算法和加权轮询算法。默认情况下，使用加权散列算法。配置服务器负载均衡的算法，在 SLB 服务器池配置模式下，使用以下命令：

load-balance-algorithm {**weighted-hash** | **weighted-round-robin** [**sticky**] | **weighted-least-connection** [**sticky**]}

- **weighted-hash** - 指定负载均衡的算法为加权散列算法。
- **weighted-round-robin** - 指定负载均衡的算法为加权轮询算法。
- **weighted-least-connection** - 指定负载均衡的算法为加权最小连接数算法。
- **sticky** – 指定使用 sticky，使每一个源 IP 产生的所有会话将被映射到同一个服务器上。**timeout** *value* 指定会话保持时间，即在该时间范围内 sticky 功能生效。

添加/删除服务器负载均衡的监测规则

添加服务器负载均衡的监测规则，在 SLB 服务器池配置模式下，使用以下命令：

monitor {**track-ping** | {**track-tcp** | **track-udp** } [**port** *port-num*]} **interval** *interval-value* **threshold** *number* **weight** *weight-num*

- **track-ping** - 指定监测规则协议类型为 PING。
- **track-tcp** - 指定监测规则协议类型为 TCP。
- **track-udp** - 指定监测规则协议类型为 UDP
- **port** *port-num* - 指定监测规则端口号，范围是 0 到 65535。

- 当 SLB 服务器池中的成员具有同一 IP 地址和不同端口号时，配置监测规则不需要指定端口号。系统将对地址池中的 IP 地址及其端口号进行监测。
- 当 SLB 服务器池中的成员只配置了 IP 地址，没有配置端口号时，配置监测规则必须指定端口号。系统将对地址池中的 IP 地址的指定端口号进行监测。
- 当 SLB 服务器池中的成员都配置了 IP 地址和端口号且这些 IP 地址没有重复的时候，配置监测规则可选择是否指定端口号。如果指定端口号，系统将对地址池中的 IP 地址的指定端口号进行监测。如果不指定端口号，系统将对地址池中成员的 IP 地址及其端口号进行监测。

- **interval** *interval-value* - 指定发送报文间隔，范围是 1 到 255。
- **threshold** *number* - 指定判断监测失败的警戒值。如果系统连续未收到该参数指定个数的响应报文，就判断为监测失败，即目标不可达。取值范围是 1 到 255。默认值是 3。
- **weight** *weight-num* - 指定该条监测失败对整个监测对象失败贡献的权重值，范围是 1 到 255。

使用该命令 no 的形式删除服务器负载均衡的监测规则：

no monitor {**track-ping** | {**track-tcp** | **track-udp** } [**port** *port-num*]}

配置监测警戒值

当失败监测规则的权重之和高于设置的监测警戒值后，则认为该服务器不可用。指定监测警戒值，在 SLB 服务器池配置模式下，使用以下命令：

monitor threshold *number*

- *number* - 指定监测警戒值。范围是 1 到 255。

配置 DNAT 规则引用 SLB 服务器池条目

DNAT 规则可以引用 SLB 服务器池条目，来实现服务器负载均衡功能。在VRouter 配置模式下使用以下命令：

dnatrule [**id** *id*] [**before** *id* | **after** *id* | **top**] **from** *src-address* **to** *dst-address* [**service** *service-name*] **trans-to** *trans-to-address* [**slb-server-pool** *pool-name*] [**port** *port*] [**load-balance**] [**track-tcp** *port*] [**track-ping**] [**log**] [**group** *group-id*] [**description** *description*]

- **slb-server-pool** *pool-name* – 指定引用的 SLB 服务器池条目名称。

{b}提示: {/b}关于如何 DNAT 规则其他参数介绍，请参考《防火墙》的“网络地址转换”部分中“创建 DNAT 规则”一节。

查看服务器负载均衡信息

查看 SLB 服务器池条目以及监测规则信息，在任意模式下，使用以下命令：

show slb-server-pool *pool-name*

- *pool-name* – 指定 SLB 服务器池条目的名称。

查看负载均衡服务器的 SLB 地址池，在任意模式下，使用以下命令：

show load-balance server

查看负载均衡服务器信息，在任意模式下，使用以下命令：

show load-balance slb-server-pool *pool-name*

查看引用负载均衡的 DNAT 规则信息，在任意模式下，使用以下命令：

show load-balance rule

链路负载均衡

对于多 ISP 链路，系统利用实时链路监控技术和动态链路探测技术将流量合理分发到不同链路，缩小了各链路上的网络时延、抖动、丢包率，从而获得较为平衡的带宽利用率。 用户可以在出站方向和入站方向分别启用链路负载均衡功能。出站和入站方向使用两种不同的动态链路探测技术，分别是出站的实时链路监控技术技术和入站的 SmartDNS 技术。最终根据探测的结果，实现流量的自动负载均衡。

出站负载均衡

系统通过实时监控各链路的时延、抖动、丢包率和带宽利用率，实现智能选路、动态调整各链路的流量负载。用户可以配置灵活的LLB Profile，并通过配置 LLB 规则将 LLB Profile 绑定到路由上（目前系统仅支持目的路由和策略路由），以实现对出站链路流量的控制及负载均衡。

配置 LLB Profile

LLB Profile 包含负载均衡算法中的各项参数供用户灵活配置，如带宽利用率阈值、探测模式、均衡方向等。

用户新建或配置 LLB Profile,在全局配置模式下，使用以下命令：

llb profile *llb-profile-name*

- *llb-profile-name* – 指定 LLB Profile 的名称。执行该命令后，系统创建指定名称的LLB Profile，并且进入该 LLB Profile 配置模式；如果指定的名称已存在，则直接进入 LLB Profile 配置模式。

在全局配置模式下，使用 **no llb profile** *llb-profile-name* 命令删除指定的 LLB Profile。

在 LLB Profile 配置模式下，默认情况下，网络探测功能为开启状态。关闭和开启探测，使用以下命令：

detect {**disable** | **enable**}

- **disable** – 禁用探测功能。禁用探测功能后，系统仅根据各出口链路的带宽占用率来选路，优先选用带宽占用率低的链路。
- **enable** – 启用探测功能。当探测功能开启后，系统会根据用户配置的参数对网络链路状态进行探测，然后选出最优路由。选择的优先级如下：

1. 当链路带宽占用率低于用户设定的带宽阈值时，系统将只根据延时、丢包、抖动计算链路质量，优先选择质量高的链路；
2. 当链路带宽占用率高于用户设定的带宽阈值时，系统将综合延时、丢包、抖动和带宽占用率来计算链路质量，优先选择质量高的链路。

在 LLB Profile 配置模式下，用户可以按需配置相关的参数，使用以下命令：

detect { **netmask** {*A.B.C.D* | *num*} | **threshold** *value* | **max-entry-number** *num* | **weight-update-interval** *interval* | **weight-factors** *delay-factor jitter-factor loss-rate-factor bw-rate-factor*}

- **netmask** {*A.B.C.D* | *num*} - 指定探测子网，系统将以该子网为单位对流量进行实时监控，相同子网的流量将会选择相同的链路。系统支持两种格式，A.B.C.D 和 num。A.B.C.D 的取值范围 255.255.240.0 到 255.255.255.255，默认值为 255.255.255.240；num 的取值范围是 20 到 32，默认值为 28。
- **threshold** *value* – 指定接口带宽利用率阈值。当接口的带宽利用率没有超过阈值时,系统将只分析链路的时延、抖动、丢包状况来动态调整选路的方法；当接口的带宽利用率超过阈值时，系统将同时分析各链路上“带宽利用率”这一参数来调整选路方法。Value 的取值范围为 0-100（0%-100%），默认为 60%。
- **max-entry-number** *num* - 指定 subnet entry 的最大值。范围是 200 到 2000000。subnet entry 是指包含每个目的子网多有链路的探测结果以及权重值的条目。当超过指定的最大值后，系统将会删除保存的 subnet entry。
- **weight-update-interval** *interval* - 指定 subnet entry 权重的更新周期，范围是 1 到 300 秒，默认值是 10 秒。
- **weight-factors** *delay-factor jitter-factor loss-rate-factor bw-rate-factor*- 指定链路的特征值时延、抖动、丢包率和带宽利用率的占比，范围是 0 到 15，默认值分别是：*delay-factor*：1；*jitter-factor*：2；*loss-rate-factor*：4；*bw-rate-factor*：1。

使用 **detect** { **netmask** | **threshold**| **max-entry-number** | **weight-update-interval** | **weight-factors** }恢复参数默认值。

当链路的带宽利用率超过指定的限制值时，系统将会记录日志信息。指定记录日志信息，使用以下命令：

log enable [**utilization-limit** *utilization-limit*]

- **utilization-limit** *utilization-limit* - 指定链路带宽利用率的限制值，范围是 1 到 100，默认值为 90。

用户取消记录日志信息，使用命令：**no log enable**。

计算负载均衡的带宽利用率时，需配置数据流量的方向，使用以下命令：

bandwidth-balance-direction {**bidirection** | **downstream** | **upstream**}

- **bidirection** – 系统将取数据流的入和出两个方向上带宽利用率较大的值与带宽利用率阈值进行比较，进而调整选路方法。
- **downstream** – 系统将取数据流的入方向上的带宽利用率的值与带宽利用率阈值进行比较，进而调整选路方法。该参数为默认方向。
- **upstream** - 系统将取数据流出方向上带宽利用率的值与带宽利用率阈值进行比较，进而调整选路方法。

使用 **no bandwidth-balance-direction** 恢复默认模式。

用户配置负载均衡的模式，使用以下命令：

mode {**compatibility** | **performance**}

- **compatibility** – 配置负载均衡模式为高兼容模式。当链路负载变动时，系统不会频繁地切换链路，而是优先保证业务尽量在先前链路上。此模式多适用于对链路切换比较敏感的业务，如银行业务。
- **performance** – 配置负载均衡为高性能模式，此模式下系统会跟据链路实时的时延、抖动、丢包情况，迅速调整以最大限度的保持链路负载均衡。该模式为默认模式。

使用 **no mode** 恢复默认模式。

用户配置负载均衡的描述信息，使用以下命令：

description *description*

- *description* – 配置 LLB Profile 的描述信息。

用户取消配置描述信息，使用命令：**no description**。

配置 LLB 规则

LLB Profile 与路由绑定形成 LLB 规则，才能够真正生效，目前支持绑定有目的路由（DBR）和策略路由(PBR)。配置 LLB 规则，在全局模式下，使用以下命令：

llb rule*rule-name* {**pbr***pbr-name***id***match-id* | **dbr** [**vrouter***vr-name*] {*A.B.C.D/M* | *A.B.C.D A.B.C.D* }}
{**profile***profile-name*}

- *rule-name* – 指定 LLB 规则名称。

- **pbr** *pbr-name* – 指定策略路由名称。
- **id***match-id* – 配置策略路由 id。
- **dbrvrouter***vr-name* – 指定目的路由的 Vrouter。
- *A.B.C.D/M* | *A.B.C.D A.B.C.D* - 指定 Vrouter 目的地址。设备支持两种方式，*A.B.C.D/M* 或者 *A.B.C.D A.B.C.D*，例如 1.1.1.0/24 或者 1.1.1.0 255.255.255.0。
- **profile***profile-name* – 绑定指定的 LLB Profile。

在全局配置模式下，使用 **no llb rule***llb-rule-name* 命令删除指定的 LLB 规则。

查看指定域名的链路探测结果

查看指定域名进行链路探测的结果，在任意模式下，使用以下命令：

show llb rule [*rule-name*] **spec-host task** { **all** | *host-name*} [**slot***slot-number*]

- **rule** [*rule-name*] – 指定 LLB 规则名称。
- **spec-host task** { **all** | *host-name*} - 查看根据指定域名进行链路探测的结果。
  - **all**- 查看 LLB 规则中所有域名的链路探测结果。
  - *host-name*- 指定域名，查看该域名的链路探测结果。
- **slot***slot-number* - 指定模块卡所在的槽位号，查看该模块卡上根据所有域名（*all*）或者指定域名（*host-name*）的链路探测结果。仅 X 系列设备支持此参数。

入站负载均衡

对入站流量启用负载均衡功能后，系统可以根据DNS 请求的来源将域名解析成不同的 IP 地址，并将不同的 ISP 所对应的 IP 地址返回给相应的请求用户，从而达到减少跨 ISP 访问的目的。这种解析方式被称为智能域名解析（SmartDNS）。

用户可通过以下步骤启用入站负载均衡功能：

1. 启用 SmartDNS 功能。启用该功能是实现入站负载均衡的前提条件。
2. 配置 SmartDNS 规则表。系统基于规则表中配置的规则实现智能域名解析。

启用 SmartDNS 功能

默认情况下，SmartDNS 功能为启用状态。禁用或启用该功能，在全局配置模式下，使用以下命令：

llb inbound smartdns {**disable** | **enable**}

- **disable** – 禁用 SmartDNS 功能。

- **enable** – 启用 SmartDNS 功能。

配置 SmartDNS 规则表

SmartDNS 规则表的配置包括创建规则表以及在规则表中指定域名、返回 IP 地址和匹配规则。系统根据匹配规则将域名解析为不同 ISP 链路对应的 IP 地址。

创建 SmartDNS 规则表

创建 SmartDNS 规则表，在全局配置模式下，使用以下命令：

llb inbound smartdns *name*

- *name* – 新建一个 SmartDNS 规则表，并进入SmartDNS 规则表配置模式。如果指定的名称已存在，则直接进入到该 SmartDNS 规则表的配置模式。系统最多支持 2500 个 SmartDNS 规则表。

在全局配置模式下，使用该命令的 no 形式删除指定的 SmartDNS 规则表：

no llb inbound smartdns *name*

指定域名

指定需要被智能解析的域名，在 SmartDNS 规则表配置模式下，使用以下命令：

domain *domain-name*

- *domain-name* – 指定需要被智能解析的域名。取值范围是 1 到 255 个字符。

重复使用以上命令向 SmartDNS 规则表中添加多个域名。每个规则表最多支持 64 个不同的域名（不区分大小写）。

在 SmartDNS 规则表配置模式下，使用该命令的 no 形式从规则表中删除指定的域名：

no domain *domain-name*

指定返回 IP 地址

用户可以对不同 ISP 链路上的请求指定不同的返回 IP 地址。系统判断请求来源的依据是 ISP 路由中的地 址簿（ISP 静态地址簿）。如果请求源地址匹配上述地址簿中的地址条目，则系统返回指定的 IP 地址。在 SmartDNS 规则表配置模式下，使用以下命令：

ip *ip-address* **isp** *isp-name* [**interface** *interface-name*] [**weight** *value*]

- *ip-address* – 指定返回的 IP 地址。用户可以为一个域名最多配置 64 个 IP 地址。

- **isp** *isp-name* – 指定请求源地址需要匹配的 ISP 名称。当请求源地址匹配该 ISP 中的地址条目，系统返回指定的 IP 地址（**ip** *ip-address*）。*isp-name* 为系统中预定义或用户自定义的 ISP 名称。每个 ISP 名称最多可以对应 16 个 IP 地址。
- **interface** *interface-name* – 为返回 IP 地址指定入站接口。系统将根据入站接口的监测结果或入站接口协议状态来判断返回 IP 地址是否有效，系统只返回有效的 IP 地址给请求源。当入站接口上配置了监测对象，若监测成功，则返回 IP 地址有效；否则 IP 地址无效。当入站接口没有配置监测对象，若该接口的协议状态为 UP，则返回 IP 地址有效；否则 IP 地址无效。若用户不配置入站接口，返回 IP 地址始终有效。
- **weight** *value* – 指定返回 IP 地址的权重。取值范围是 1 到 100，默认值为 1。SmartDNS 规则表中一个域名可能对应多个 IP 地址，系统会根据权重值对 IP 地址进行排序后返回给用户。

在 SmartDNS 规则表配置模式下，使用该命令的 no 形式从规则表中删除指定的 IP 地址：

no ip *ip-address*

注意：

- 用户无法删除正在被 SmartDNS 规则表引用的 ISP 路由。有关 ISP 路由的更多信息，请参考《路由》的“ISP 路由”部分。
- 在完成域名、返回 IP 地址等配置之前，新建的 SmartDNS 规则表处于禁用状态。

查看链路负载均衡信息

查看出站方向链路负载均衡的配置信息，在任意模式下，使用以下命令：

show llb {**profile** [*profile-name*] | **rule** [*rule-name*]}

- **profile** [*profile-name*] – 查看出站方向链路负载均衡模板。*profile-name* 为模板名称。
- **rule** [*rule-name*] – 查看出站方向链路负载均衡的规则。*rule-name* 为规则名称。

查看入站方向的负载均衡及 SmartDNS 规则表的配置信息，在任意模式下，使用以下命令：

show llb inbound [**smartdns** *name*]

- **inbound** – 查看入站方向链路负载均衡的配置信息。
- **smartdns***name* – 指定 SmartDNS 规则表的名称。

例如，使用 **show llb inbound smartdns***test* 命令查看系统中名为 test 的 SmartDNS 规则表的配置信息。以下是一个返回结果示例：

```
hostname# show llb inbound smartdns test
```

```
domain:domain name; IP: ip address; ISP: isp name; IF: interface;
PROXY: proximity address book status; E: enable; D:disable
TRACK: track object name; W: ip weight; S:ip status;A:active; I: inactive
================================================================================
-----
table name: test（SmartDNS 规则表名称）
table status: enable（SmartDNS 规则表状态）
domain count: 1（域名数量）
rule count: 1（域名解析规则数量）
domains: www.test.com;（需要被智能解析的域名）
ip addresses:
-----
IP ISP IF PROX TRACK W S
1.1.1.1 China-telecom ethernet0/1 E 1 I
================================================================================
```

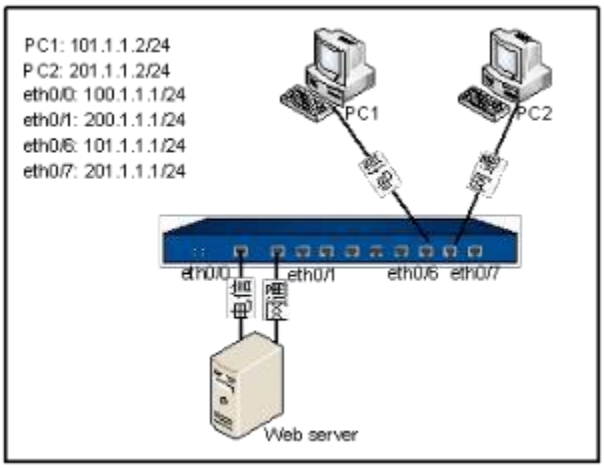
- 有关 TRACK 列下监测对象的更多信息，请参考《系统管理》的“配置监测对象”部分。
- S 列下所显示规则状态可能为活跃（active）或非活跃（inactive），由接口及接口上的监测对象决定：
  - 如果只配置了引用的 ISP 路由（**isp** *isp-name*）但没有配置接口（**interface** *interface-name*），规则状态始终为活跃；
  - 如果配置了接口（**interface***interface-name*）但接口上没有配置监测对象，接口的协议状态为 可用（UP）时规则状态为活跃，协议状态为不可用（DOWN）时规则状态为非活跃；
  - 如果配置了接口（**interface***interface-name*）且接口上配置了监测对象，监测成功时规则状态 为活跃，监测失败时规则状态为非活跃。

链路负载均衡功能配置举例

本节介绍一个入站链路负载均衡功能的配置举例。

组网需求

设备的 ethernet0/6 和 ethernet0/7 两个接口分别连接电信和网通的两条线路。配置入站链路负载均衡功能后，设备对电信用户发送的 DNS 请求返回电信 ISP 静态地址簿中所对应的 IP 地址，对网通用户所发送的 DNS 请求返回网通静态 ISP 地址簿中所对应的 IP 地址。组网图如下图所示：



配置步骤

以下配置步骤略去接口配置，重点描述 ISP 信息和入站链路负载均衡功能的相关配置。

第一步：配置 ISP 信息：

```
hostname(config)# isp-network telecom
hostname(config-isp)# 101.1.1.0/24
hostname(config-isp)# exit
hostname(config)# isp-network netcom
hostname(config-isp)# 201.1.1.0/24
hostname(config-isp)# exit
```

第二步：启用 SmartDNS 功能并配置 SmartDNS 规则表：

```
hostname(config)# llb inbound smartdns enable
hostname(config)# llb inbound smartdns test
hostname(config-llb-smartdns)# domain www.test.com
hostname(config-llb-smartdns)# ip 100.1.1.2 isp telecom interface ethernet0/0 weight 10
hostname(config-llb-smartdns)# ip 200.1.1.2 isp netcom interface ethernet0/1 weight 10
```

```
hostname(config-llb-smartdns)# exit
```

第三步：使用 show 命令确认上述配置已经生效：

```
hostname(config)# show isp-network all
ISP telecom status: Active
Binding to nexthop: 0
Subnet(IP/Netmask): 1
101.1.1.0/24
ISP netcom status: Active
Binding to nexthop: 0
Subnet(IP/Netmask): 1
201.1.1.0/24
hostname(config)# show llb inbound smart test
domain:domain name; IP: ip address; ISP: isp name; IF: interface;
PROXY: proximity address book status; E: enable; D:disable
TRACK: track object name; W: ip weight; S:ip status;A:active;
I: inactive
==========================================================================
--------------------------------------------------------------------------
name: test
domain count: 1
rule count: 2
status: enable
domains: www.test.com;
ip addresses:
--------------------------------------------------------------------------
ID IP ISP IF PROX TRACK W S
```

```
1 100.1.1.2 telecom ethernet0/0 D 10 A

3 200.1.1.2 netcom ethernet0/1 D 10 A

==============================================================================
```

此时PC1 请求域名www.test.com，设备会返回电信的 IP 地址 100.1.1.2；PC2 请求域名www.test.com，设备会返回网通的 IP 地址 200.1.1.2。

会话限制

会话限制功能介绍

设备支持基于安全域的会话限制功能。用户可以对安全域内的源 IP 地址、目的 IP 地址、指定的 IP 地址、特定协议类型、应用、角色或用户进行会话数量或者建立会话速率控制，从而保护连接表不被 DoS 攻击填满，并且能够在一定程度上限制一些应用的带宽，如 IM 或者P2P 等。

会话限制配置

配置会话限制功能，在安全域配置模式下，使用以下命令：

ad session-limit [**id** *id*] {{**src-ip** *address-entry* **dst-ip** *address-entry* | **ip** *address-entry* } [**application** *application-name*] [**protocol** *protocol-id*] [**role** *role-name* | **user** *aaa-server-name user-name* | **user-group** *aaa-server-name user-group-name*] } {**session** {**unlimit** | **max** *number* [**per-srcip** | **per-dstip** | **per-ip**] | **per-user**} | **ramp-rate max** *number*} [**schedule** *schedule-name*]

- **id** *id* – 指定安全域的会话限制规则 ID。
- **src-ip** *address-entry* – 限制安全域的源 IP 地址会话数。*address-entry* 为 **src-ip** 的 IP 地址范围。该参数值为地址簿中定义的一条地址条目。
- **dst-ip** *address-entry* – 限制安全域的目的 IP 地址会话数。*address-entry* 为 *dst-ip* 的 IP 地址范围。该参数值为地址簿中定义的一条地址条目。
- **ip** *address-entry* – 限制安全域中某个 IP 地址段的会话数。*address-entry* 为 **ip** 的 IP 地址范围。该参数值为地址簿中定义的一条地址条目。
- **protocol** *protocol-id* – 限制安全域中特定 IP 协议类型的会话数。*protocol-id* 为 **ip** 的协议号，取值范围为 1 到 255。
- **application** *application-name* – 限制安全域中特定应用的会话数。
- **role** *role-name* – 限制特定角色的会话数。

- **user** *aaa-server-name user-name* – 限制特定用户的会话数。*aaa-server-name* 为用户所属的 AAA 服务器名称，*user-name* 为用户名称。
- **user-group** *aaa-server-name user-group-name* – 限制特定用户组的会话数。*aaa-server-name* 为用户组所属的 AAA 服务器名称，*user-name* 为用户组名称。
- **session** {**unlimit** | **max** *number* [**per-srcip** | **per-dstip** | **per-ip**] | **per-user**} – 指定 IP 地址或角色的最大会话数。**unlimit** 为无会话数限制。**session max** *number* 指定地址条目中所有 IP 地址的最大会话数或者角色对应的所有用户的最大会话数；如果使用 **per-srcip**、**per-dstip**、**per-ip** 或者 **per-user** 关键字，则 **session max** *number* 指定的为每个IP 地址的最大会话数或者角色对应的每个用户的最大会话数。**per-srcip**、**per-dstip**、**per-ip** 和 **per-user** 四个关键字需和前面的 **src-ip**、**dst-ip**、**ip** 和 **role** 关键字一一对应，如：只有在前面指定了 **src-ip** 才可以在后面选择 **per-srcip**。
- **ramp-rate max** *number* – 指定 IP 地址或者角色每 5 秒钟可建立的最大会话数。
- **schedule** *schedule-name* – 指定会话限制规则的生效时间。
- - 指定记录会话限制日志。

注意:会话限制功能支持IPv4 地址和 IPv6 地址。如开启接口的 IPv6 功能，用户可配置 IPv6 类型的地址条目。源地址条目与目的地址条目的地址类型需一致。

在安全域配置模式下，使用以下命令删除安全域的会话限制规则：

no ad session-limit id *id*

- **id** *id* – 安全域的会话限制规则 ID。可通过 show session-limit 命令获取相应规则的 ID。

配置会话限制功能后，超出最大会话数限制的会话将被丢弃，用户可以通过 show session-limit 命令查看被丢弃的会话数统计信息。删除特定会话限制规则中被丢弃会话数的统计信息，请在任何置模式下使用以下命令：

clear session-limit id *id* **statistics**

- **id** *id* – 指定规则 ID 以删除特定会话限制规则中被丢弃的会话数统计信息。

注意:在设备上启用了Full-cone NAT 功能后，会话限制中的目的 IP 地址指的是 DNAT 转换之前的 IP 地址。有关Full-cone NAT 功能的更多信息，请参考《防火墙》的“Full-cone NAT”部分。

会话限制显示

配置会话限制功能后，在任何模式下使用以下命令查看会话限制配置信息：

show session-limit

第 9 章 威胁防护

本章节包含以下内容:

"主机防御"：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" 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"：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"：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。

"边界流量过滤"：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。

"僵尸网络 C&C 防御"：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。

.....

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 schedule1
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（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。如果设备探测到在该指定时间内有 10 个以上 TCP SYN 包发往不同的目的端口，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*），仅允许 10 个发往不同的目的端口的 TCP SYN 包通过，其它同类包将会被丢弃，并且发出警报。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*] {*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*] {*A.B.C.D/M* | *address-entry*}

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

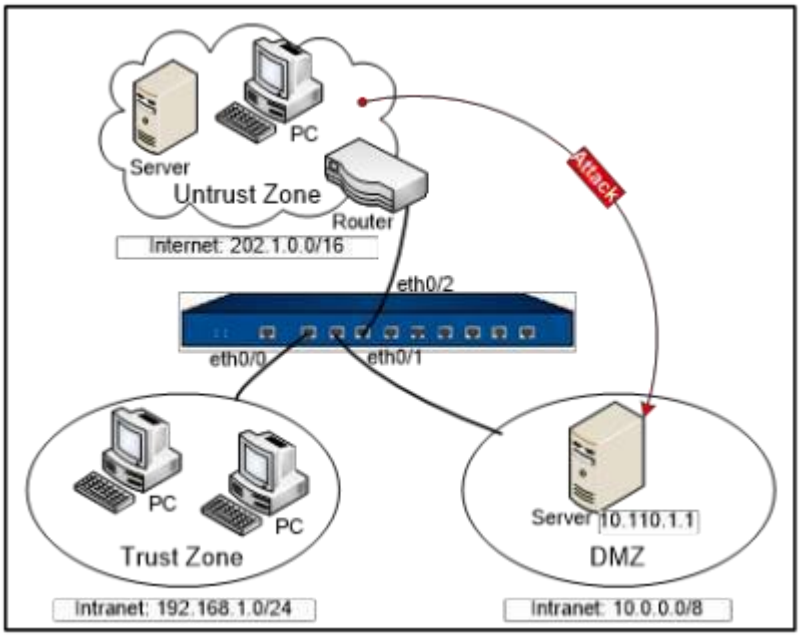
本节介绍攻击防护的配置实例以帮助用户更好的理解与配置设备的攻击防护功能。

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:

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。

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 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 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 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。

安全策略规则配置	操作
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 代理 启用病毒过滤	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 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。

{b}提示: {/b}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. net.com 和 update2. net.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. net.com，**server2** 的默认值为 update2. net.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. net.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。

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:

开启沙箱防护功能。

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。

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 4 个默认的沙箱防护规则 predef_low、predef_middle、predef_high 和 predef_pe:

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。

predef_pe – 仅支持 PE 文件检测的沙箱检测策略。此规则扫描 HTTP/FTP/POP3/SMTP/IMAP4 协议流量，将 PE 文件作为检测对象。

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恶意文件。

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，默认情况下，会上传该可疑文件文件到云沙箱进行检测。用户可以根据需求禁用可疑文件上传，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

绑定沙箱防护 Profile 到安全域

将沙箱防护 Profile 绑定到安全域后，系统将会对安全域中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 到安全域，在安全域配置模式下使用以下命令：

sandbox enable*sandbox-profile-name*

sandbox-profile-name – 指定绑定到安全域的沙箱防护 Profile 的名称。

在安全域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 enable

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. net.com 和 update2. net.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. net.com，**server2** 的默认值为 update2. net.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. net.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
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。 提供两个默认特征库更新服务器，分别是 update1. net.com 和 update2. net.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}}** [*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：

配置	CLI
	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：

确认 StoneOS 版本支持 IPS 功能。

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	对 HTTP 流量根据安全策略规则中配置的 IPS Profile 进行 IPS 检测。对

安全策略规则配置	安全域配置	操作
启用 IPS		HTTPS 流量不进行解密，不进行 IPS 检测，只进行转发。

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 vsftp2.0**

brute-force auth

为特征集开启暴力破解功能并对该功能进行配置。使用该命令 no 的形式关闭暴力破解功能。

［命令］

brute-force auth *times* **block** {**ip** | **service**} *timeout*

no brute-force auth

［句法描述］

times - 指定允许的一分钟内认证/登录失败的次数。取值范围是 1 到 100000。

ip | service - 指定对超出限定认证/登录失败频率的攻击者的 IP 地址（**ip**）或者服务（**service**）进行阻断。

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

［默认取值］

无。

［命令模式］

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**| **others**}

no deny-method {**connect** | **delete** | **get** | **head** | **options** | **post** | **put** | **trace** | **webdav**| **others**}

［句法描述］

connect | **delete** | **get** | **head** | **options** | **post** | **put** | **trace** | **webdav** | **others** 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

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：

确认系统版本支持边界流量过滤功能。

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. net.com 和 update2. net.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. net.com，**server2** 的默认值为 update2. net.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. net.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

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:

确认系统版本支持僵尸网络 C&C 防御功能。

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:

开启僵尸网络 C&C 防御功能。

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。

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。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. net.com 和 update2. net.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. net.com，**server2** 的默认值为 update2. net.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. net.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

URL 过滤

URL 过滤功能可以控制用户对某些网站的访问。通过配置URL 过滤功能，可以实现：

控制用户对某类网站的访问。比如，阻止用户访问赌博、色情类网站。

分时段控制用户对某类网站的访问。比如，阻止用户在上班时间访问在线聊天类网站，下班后则允许访问。

控制用户对网址中含有特定关键字的网站的访问。比如，阻止用户访问网址中含有关键字“游戏”的网站。

配置 URL 过滤功能

系统支持基于安全域和基于策略的 URL 过滤配置方式。URL 过滤支持配置 IPv4 和 IPv6 地址的 URL 和关键字（keyword）。

通过 CLI 配置 URL 过滤功能，请按照以下步骤进行操作：

定义 URL 过滤 Profile，在 Profile 中指定需要进行控制的 URL 类别、URL 关键字类别以及采取的控制动作。

将 URL 过滤Profile 绑定到安全域/策略规则。

创建 URL 过滤 Profile

URL 过滤Profile 中主要指定URL 过滤功能的控制类型，包括 URL 类别，URL 关键字，以及上网日志记录。URL 类别指定需要进行控制的 URL 类别以及相应的控制动作；URL 关键字指定需要进行控制的 URL 关键字类别以及相应的控制动作；上网日志记录记录用户的 GET，POST 请求，以及POST 请求的内容。每一个 URL 过滤 Profile 只可以配置一种控制类型。系统有一个缺省的 URL 过滤 Profile，名称为 no-url， 不可编辑和删除，该 Profile 不对任何 URL 进行过滤。创建URL 过滤 Profile，在全局配置模式下使用以下命令：

url-profile *profile-name*

> *profile-name* - 指定所创建的 URL 过滤 Profile 的名称，并且进入该 URL 过滤 Profile 的配置模式。如果指定名称已存在，则直接进入 URL 过滤 Profile 配置模式。不同的 VSYS 中可以配置相同名称的 URL 过滤Profile。使用 **no url-profile** *profile-name* 删除指定的 URL 过滤 Profile。

指定 URL 类别及控制动作

指定需要进行控制的 URL 类别及控制动作，在 URL 过滤Profile 配置模式下使用以下命令：

url-category {**all** | *url-category-name*} [**block**] [**log**]

> **all** | *url-category-name* – 指定需要进行控制的URL 类别名称，可以为所有的URL 类别（**all**）或者特定 URL 类别（*url-category-name*）。系统不支持指定非本 VSYS 中自定义的URL 类别名称。关于新建 URL 类别的详细信息，请参阅“指定 HTTP 代理服务器”。
>
> **block** – 指定阻止访问相应的 URL 类别。
>
> **log** – 指定对用户的URL 访问行为进行日志记录。

使用多条该命令可指定多个 URL 类别及相应的控制动作。

在 URL 过滤 Profile 配置模式下，使用 **no url-category** {**all** | *url-category-name*}命令取消 URL 类别及控制动作的指定。

SSL 协商报文检测

对于 HTTPS 流量，通过开启 SSL 协商报文检测功能，系统可以从 SSL 协商报文中获取用户要访问的站点的域名，从而进行 URL 过滤。此功能仅适用于控制类型为 URL 类别的 URL 过滤功能。如果同时配置了 SSL 代理功能，系统会优先使用 SSL 协商报文检测方式进行 URL 过滤。开启 SSL 协商报文检测功能，在 URL 过滤Profile 配置模式下使用以下命令：

url-category ssl-inspection

在 URL 过滤 Profile 配置模式下，使用 **no url-category ssl-inspection** 命令关闭 SSL 协商报文检测功能。

指定 URL 关键字类别及控制动作

指定需要进行控制的 URL 关键字类别及控制动作，在URL 过滤 Profile 配置模式下使用以下命令：

keyword-category {*keyword-category-name* | **other**} [**block**] [**log**]

> *keyword-category-name* | **other** – 指定需要进行控制的 URL 关键字类别名称，可以为特定 URL 关键字类别（*keyword-category-name*）或除此之外的所有 URL 关键字类别（**other**）。
>
> **block** – 指定阻止访问网址中含有相应关键字的网站。
>
> **log** – 指定对访问网址中含有相应关键字的网站的行为进行日志记录。

使用多条该命令可指定多个 URL 关键字类别及相应的控制动作。

在 URL 过滤 Profile 配置模式下，使用 **no keyword-category** {*keyword-category-name* | **other**}命令取消 URL 关键字类别及控制动作的指定。

开启安全搜索功能

许多搜索引擎，如 Google、Bing、Yahoo!、Yandex、Youtube，都包含“安全搜索”设置项，该设置用来过滤搜索结果中的成人内容，搜索引擎会根据该设置项的设置返回不同级别的搜索结果。系统支持通过在 URL 过滤Profile 中开启安全搜索功能，来检测搜索引擎“安全搜索”的设置以及执行相应的控制动作。

开启安全搜索功能并指定控制动作，在 URL 过滤 Profile 配置模式下，使用以下命令：

safe-search {**block** | **enforce**}

> **block** – 指定动作为阻断，即当检测出搜索引擎“安全搜索”未设置时，阻止用户访问搜索页面并显示警告提示页面，提供“安全搜索”设置链接提示用户前往设置。
>
> **enforce** – 指定动作为执行，即当检测出搜索引擎“安全搜索”未设置时，系统强制将搜索引擎的“安全搜索”设置为最严格级别。

在 URL 过滤 Profile 配置模式下，使用 **no safe-search** 关闭安全搜索功能。

注意:

> 安全搜索功能目前仅支持以下搜索引擎：Google、Bing、Yahoo!、Yandex、Youtube。
>
> 由于搜索引擎使用 HTTPS 协议，因此安全搜索功能与 SSL 代理功能结合才可使用，需要为 URL 过滤Profile（已开启安全搜索功能）绑定的策略规则启用 SSL 代理功能。
>
> 为了保证 Google 搜索引擎安全搜索功能的有效性，需要配置策略规则阻断UDP 80 和 UDP 443 端口号。

绑定 URL 过滤 Profile 到安全域

将 URL 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 URL 过滤检查。当策略规则已经绑定了 URL 过滤 Profile，同时策略规则的目的安全域也绑定了 URL 过滤 Profile，策略规则绑定的 URL 过滤Profile 将会生效，而目的安全域绑定的 URL 过滤Profile 无效。

绑定 URL 过滤 Profile 到安全域，在安全域配置模式下，使用以下命令：

url enable *url-profile-name*

> *url-profile-name* – 指定绑定到安全域的 URL 过滤 Profile 的名称。一个安全域只能绑定一个 URL 过滤 Profile。

在安全域配置模式下，使用该命令 no 的形式取消URL 过滤Profile 的绑定：

no url enable

绑定 URL 过滤 Profile 到策略规则

将 URL 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 配置进行处理。绑定 URL 过滤 Profile 到策略规则，需要在策略规则配置模式下进行。

进入策略规则配置模式需要进行两步配置。首先，在全局配置模式下，输入以下命令进入策略配置模式：

policy-global

然后，在策略配置模式下，输入以下命令进入策略规则配置模式：

rule [**id** *id-number*]

进入策略规则配置模式后，输入以下命令将 URL 过滤 Profile 绑定到策略规则

url *profile-name*

> *profile-name* - 指定所需要绑定的 URL 过滤 Profile 名称。

注意:被绑定的URL 过滤Profile 只有在解除绑定后，才可以进行删除。

绑定配置完成后，需要修改策略规则的优先级，确保流量优先匹配此策略规则，然后可以继续指定策略规则的用户、目的安全域和时间表参数，并能禁用或者启用该条策略规则。

如果需要对 HTTPS 流量执行 URL 过滤功能，需要为上述策略规则启用 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 URL 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 URL 过滤	根据 SSL 代理Profile 解密 HTTPS 流量，对解密后的数据不进行 URL 过滤。
启用 SSL 代理 启用 URL 过滤	根据 SSL 代理Profile 解密 HTTPS 流量，对解密后的数据根据 URL 过滤Profile 进行 URL 过滤。
不启用 SSL 代理 启用 URL 过滤	对 HTTP 流量根据 URL 过滤 Profile 进行 URL 过滤。对 HTTPS 流量不进行解密，不进行URL 过滤，只进行转发。

如果此条策略启用了 SSL 代理，但是 URL 过滤 Profile 对应的 URL 过滤规则中的控制类型为“上网日志记录”，系统将不会对 HTTPS 流量中的 GET 和 POST 方法及内容进行记录。

当安全策略规则所关联的安全域也启用 URL 过滤时，系统将进行如下操作:

安全策略规则配置	安全域配置	操作
启用 SSL 代理 不启用 URL 过滤	启用 URL 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 URL 过滤 Profile 进行 URL 过滤。
启用 SSL 代理 启用 URL 过滤	启用 URL 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 URL 过滤Profile 进行URL 过滤。
不启用 SSL 代理 启用 URL 过滤	启用 URL 过滤	对 HTTP 流量根据安全策略规则中配置的 URL 过滤 Profile 进行URL 过滤。对 HTTPS 流量不进行解密，不进行 URL 过滤，只进行转发。

显示 URL 过滤 Profile 信息

在任何模式下，输入以下命令显示 URL 过滤 Profile 信息:

show url-profile [*profile-name*]

> *profile-name* – 显示指定 URL 过滤Profile 的信息。若不指定 Profile 名称，显示系统中所有 URL 过滤 Profile 的信息。

第 10 章 监控

本章节包含以下内容:

"监控": 介绍了如何配置系统的所有监控统计功能。

"告警": 介绍了如何配置告警规则命令对告警信息进行分析统计。

"日志": 介绍了系统的所有日志功能，以及如何输出设备的各种日志信息。

"故障排查": 介绍了所有故障排查的命令。

监控

监控介绍

系统的监控统计功能包括以下功能：

用户监控：基于用户的监控统计功能，统计属于特定用户、用户组、地址簿的数据量、数据包。

应用监控：基于应用的监控统计功能，统计属于特定应用、应用组的数据量、数据包。

终端接入监控：基于应用特征的监控统计功能，统计属于特定 IP、接入数量或 VRouter 的终端接入监控信息。

威胁监控：基于威胁的监控统计功能，统计属于特定威胁的信息。

管道监控：基于管道的监控统计功能，统计属于特定管道的流量信息。

服务网络监控：基于服务网络的监控统计功能，统计服务网络节点丢包率和延迟时间等信息。

设备监控：基于设备的监控统计功能，统计整机、接口、安全域、在线 IP 数、流量以及硬件状态的信息。

URL 访问：基于 URL 的监控统计信息，统计 URL 访问次数和 URL 类别的信息。

链路状态监控：链路状态监控是通过统计链路中特定接口的采样流量信息，包括延迟、丢包率、抖动、带宽利用率，从而实现链路整体状态的监控和展示。

应用阻断：统计被阻断应用以及用户的信息。

关键字阻断：统计网页关键字、邮件内容关键字、 Web 外发信息关键字阻断次数信息。

认证用户：统计所有认证登录的用户信息。

自定义监控：配置自定义监控统计集为用户提供更加灵活的统计信息查看方法。

如设备开启 IPv6 功能，系统支持同时统计 IPv4 地址和 IPv6 地址的带宽、会话数、AD、URL 和应用。支持 IPv6 统计的监控包含：用户监控、应用监控、设备监控、URL 访问、应用阻断、自定义监控。

{b}提示: {/b}Web 界面可以更加直观的显示所有监控的数据信息，因此建议用户通过 WebUI 配置监控功能和查看监控结果，不建议使用 CLI。

用户监控

用户监控用于统计属于特定用户、用户组、地址簿的数据量、数据包。如设备开启 IPv6 功能，系统支持 IPv4 和 IPv6 地址的统计。

配置监控地址簿

监控地址簿用来储存需要统计地址簿流量的用户地址条目，即在全局地址簿中选择需要统计的地址条目。在全局配置模式下，使用以下命令：

statistics address *address-entry-name*

address-entry-name – 指定地址条目名称。

使用该命令 no 的形式关闭基于指定地址的统计功能：

no statistics address *address-entry-name*

查看地址簿的监控统计信息

在任何模式下，使用以下命令查看地址簿的监控统计信息：

show statistics address [*address-entry-name*] [**current** | **lasthour** | **lastday** | **lastmonth**]

address-entry-name – 指定地址条目名称。如果不指定该参数，该命令将显示系统中所有被统计功能所引用地址条目的流量统计信息。

current – 指定显示地址条目的即时流量统计信息。

lasthour – 指定显示地址条目前 60 分钟每 30 秒的流量统计信息。

lastday – 指定显示地址条目前 24 小时每 10 分钟的流量统计信息。

查看监控地址簿成员信息

在任何模式下，使用以下命令查看监控地址簿成员信息：

show monitor-address

查看用户监控相关统计集统计信息

用户监控相关预定义统计集如下：

类别	名称	描述
用户监控	predef_user_bw	统计所有用户的流量。
	predef_user_sess	统计所有用户的会话数。
	predef_user_app_bw	统计所有用户下应用的流量。
	predef_exstat_exstat_ip_bw	统计所选地址簿下用户的流量
	predef_exstat_exstat_ip_sess	统计所选地址簿下用户的会话数
	predef_exstat_exstat_app_bw	统计所选地址簿下应用的流量
	predef_exstat_exstat_app_sess	统计所选地址簿下应用的会话数

查看用户监控相关统计集信息，具体命令请参阅“查看统计集信息”。

{b}提示: {/b}非根 VSYS 同样支持用户监控，但是不支持地址簿监控。

应用监控

基于应用的监控统计功能，可以统计指定应用的即时流量统计信息、前 60 分钟每 30 秒的流量统计信息、前 24 小时每 10 分钟的流量统计信息和前 30 天每天的流量统计信息。如设备开启 IPv6 功能，系统支持 IPv4 和 IPv6 地址的统计。

配置监控应用组

配置监控应用组，在全局配置模式下，使用以下命令：

statistics application-group *application-group-name*

application-group-name – 指定应用组名称。

使用该命令 no 的形式删除监控应用组指定应用组：

no statistics application-group *application-group-name*

查看基于应用的统计信息

在任何模式下，使用以下命令查看基于应用的流量统计信息：

show statistics application-group [*application-group-name*] [**current** | **lasthour** | **lastday** | **lastmonth**]

application-group-name – 指定应用组名称。如果不指定该参数，该命令将显示系统中所有被流量统计功能所引用应用组的流量统计信息。

current – 指定显示应用组的即时流量统计信息。

lasthour – 指定显示应用组前 60 分钟每 30 秒的流量统计信息。

lastday – 指定显示应用组前 24 小时每 10 分钟的流量统计信息。

lastmonth – 指定显示应用组前 30 天每天的流量统计信息。

查看应用监控相关统计集统计信息

应用监控相关预定义统计集如下：

类别	名称	描述
应用监控	predef_app_bw	统计所有应用的流量。
	predef_app_sess	统计所有应用的会话数。

类别	名称	描述
	predef_exstat_exstat_ip_bw	统计所选地址簿下用户的流量。
	predef_exstat_exstat_ip_sess	统计所选地址簿下用户的会话数。
	predef_exstat_exstat_app_bw	统计所选地址簿下应用的流量。
	predef_exstat_exstat_app_sess	统计所选地址簿下应用的会话数。

查看应用监控相关统计集信息，具体命令请参阅“查看统计集信息”。

{b}提示: {/b}非根 VSYS 同样支持应用监控，但是不支持应用组监控。

终端接入监控

查看指定过滤条件下的终端接入监控信息，在任何模式下，使用以下命令：

show host share-access [**ip** *ip-address* | **device-num** *number*] [**vrouter** *vrouter-name*]

ip *ip-address* – 以源 IP 地址为条件进行过滤。系统显示指定 IP 地址的终端接入监控信息。

device-num *number* – 以共享接入数量为条件进行过滤。系统显示指定接入数量的终端接入监控信息。

vrouter *vrouter-name* – 以 VRouter 为条件进行过滤。系统显示指定VRouter 的终端接入监控信息。

威胁监控

查看威胁监控相关统计集统计信息

非根VSYS 同样支持威胁监控（仅 T 系列支持）。威胁监控相关预定义统计集如下：

类别	名称	描述
威胁监控	predef_ip_dip_threat	统计所有受到威胁攻击

仅支持通过 CLI 查看威胁相关统计集信息，具体命令请参阅“查看统计集信息”。

管道监控

仅支持通过 WebUI 方式查看管道监控统计信息，具体配置方式请参阅《StoneOS WebUI 用户手册》。

设备监控

查看接口的统计信息

在任何模式下，使用以下命令查看指定接口的流量统计信息：

show statistics interface-counter interface *interface-name* {**second** | **minute** | **hour**}

interface-name – 指定接口名称。

second – 指定显示接口前 60 秒钟每 5 秒的流量统计信息。

minute – 指定显示接口前 60 分钟每分钟的流量统计信息。

hour – 指定显示接口前 24 小时每小时的流量统计信息。

查看设备监控相关统计集统计信息

设备监控相关预定义统计集如下：

类别	名称	描述
设备监控	predef_zone_ bw	统计所有安全域的流量
	predef_if_bw	统计所有接口的流量
	predef_zone_sess	统计所有安全域的会话数
	predef_if_sess	统计所有接口的会话数

查看设备监控相关统计集信息，具体命令请参阅“查看统计集信息“。

URL 访问

查看 URL 访问相关统计集统计信息

URL 访问相关预定义统计集如下：

类别	名称	描述
URL 访问	predef_url_hit	统计 URL 命中次数。
	predef_user_url	统计用户访问 URL 的次数。
	predef_url_cat_hit	统计 URL 类别的命中次数。
	predef_user_url_cat_hit	统计用户访问 URL 类别的次数。

如设备开启 IPv6 功能，系统支持 IPv4 和 IPv6 地址的统计。

仅支持通过 CLI 查看 URL 访问相关统计集信息。

链路状态监控

通过统计链路中特定接口的采样流量信息，包括延迟、丢包率、抖动、带宽利用率，从而实现链路整体状态的监控和展示。

开启/关闭接口的链路状态监控功能

开启接口的链路状态监控功能，在全局配置模式下，使用以下命令：

link-perf-monitor interface *interface-name*

interface-name – 指定接口名称。执行该命令后，开启指定接口的链路状态监控功能，并且进入链路状态监控配置模式；如果指定接口的链路状态监控功能已经开启，则直接进入链路状态监控配置模式。

使用 **no link-perf-monitor interface** *interface-name* 命令关闭指定接口的链路状态监控功能。

开启/关闭接口的应用维度

开启接口的应用维度后，系统可以统计链路中特定接口下具体应用的信息，包括延迟、丢包率、抖动、带宽利用率。接口的应用维度默认情况下是关闭的。开启应用维度，在链路状态监控配置模式下，使用以下命令：

application on

使用 **no application on** 命令关闭指定接口的应用维度。

配置 NAT 地址池

当用户创建 NAT 地址池后，系统会按照 NAT 地址池的 IP 地址进一步为链路接口的流量进行分类统计。创建 NAT 地址池，在链路状态监控配置模式下，使用以下命令：

snat-pool *pool-name*

pool-name - 指定 NAT 地址池名称并进入 NAT 地址池配置模式。如果指定的名称已存在，系统会直接进入 NAT 地址池配置模式。

在 NAT 地址池配置模式下，使用该命令 no 的形式删除指定的 NAT 地址池：

no snat-pool *pool-name*

指定 NAT 地址池的 IP 地址，在 NAT 地址池配置模式下，使用以下命令：

address-book *address-name* | **ip** *A.B.C.D* | *A.B.C.D/M* | **ip-range** *start-ip end-ip*

address-book *address-name* - 指定 NAT 地址池的引用的地址簿名称。

ip *A.B.C.D* | *A.B.C.D/M* - 指定 NAT 地址池的 IP 地址。

start-ip - 指定 NAT 地址池的起始 IP 地址。

end-ip - 指定 NAT 地址池的结束 IP 地址。

在 NAT 地址池配置模式下，使用该命令 no 的形式删除指定的 IP 地址范围：

no address-book *address-name* | **ip** *A.B.C.D* | *A.B.C.D/M* | **ip-range** *start-ip end-ip*

查看链路状态监控配置信息

查看链路状态监控的所有配置信息，在任何模式下使用以下命令：

show link-perf-monitor information

查看链路状态监控统计信息

查看链路状态监控统计信息，在任何模式下使用以下命令：

show link-perf-monitor statistics [**interface** *interface-name* [**snat-pool** *pool-name*] [**application** *application-name*][**history** {**minute** | **hour** | **day** | **month**}]]

interface *interface-name* – 按照指定接口显示链路状态监控统计信息。

snat-pool *pool-name* – 按照指定 NAT 地址池显示链路状态监控统计信息。如果不指定该参数，则显示指定接口的所有统计信息。

application *application-name* – 按照指定应用显示链路状态监控统计信息。如果不指定该参数，则显示指定接口或指定NAT 地址池的所有统计信息。

history {**minute** | **hour** | **day** | **month**} – 显示历史链路状态监控统计信息。

例如：

```
查看所有接口的链路状态监控信息
hostname(config)# show link-perf-monitor statistics
link performance monitor statistics:
Latency, Jitter is in milliseconds.
Loss-Rate, Bandwidth Utilization has already removed %.
LTC: Latency; JIT: Jitter;
UPLR: Up Loss Rate; DWLR: Down Loss Rate; TLLR: Total Loss Rate;
UPBU: Up Bandwidth Utilization; DWBU: Down Bandwidth Utilization;
IF LTC JIT UPLR DWLR TLLR UPBU DWBU
============================================================
ethernet1/7 0 0 N/A 0 0 1 78
ethernet1/9 0 0 N/A 0 0 1 67
============================================================
```

查看指定接口的链路状态监控信息

hostname(config)# **show link-perf-monitor statistics interface ethernet1/7**

link performance monitor statistics:

Latency, Jitter is in milliseconds.

Loss-Rate, Bandwidth Utilization has already removed %.

LTC: Latency; JIT: Jitter;

UPLR: Up Loss Rate; DWLR: Down Loss Rate; TLLR: Total Loss Rate;

UPBU: Up Bandwidth Utilization; DWBU: Down Bandwidth Utilization;

==========

ethernet1/7|ALL|ALL LTC JIT UPLR DWLR TLLR UPBU DWBU

---

0 0 0 N/A 0 0 3 100

==========

查看指定接口的历史（最近一天）链路状态监控信息

hostname(config)# show link-perf-monitor statistics interface ethernet1/9 history day

link performance monitor statistics:

Latency, Jitter is in milliseconds.

Loss-Rate, Bandwidth Utilization has already removed %.

LTC: Latency; JIT: Jitter;

UPLR: Up Loss Rate; DWLR: Down Loss Rate; TLLR: Total Loss Rate;

UPBU: Up Bandwidth Utilization; DWBU: Down Bandwidth Utilization;

==========

ethernet1/9|ALL|ALL LTC JIT UPLR DWLR TLLR UPBU DWBU

---

0 0 0 N/A 0 0 0 33

```
1 0 0 N/A 0 0 1 56
2 0 0 N/A 0 0 0 33
3 0 0 N/A 0 0 2 89
4 0 0 N/A 0 0 0 0
5 0 0 N/A 0 0 0 0
6 0 0 N/A 0 0 0 0
7 0 0 N/A 0 0 0 0
8 0 0 N/A 0 0 0 0
9 0 0 N/A 0 0 0 0
10 0 0 N/A 0 0 0 0
```

应用阻断

应用阻断相关预定义统计集如下：

类别	名称	描述
应用阻断	predef_app_block	统计所有应用的阻断次数。
	predef_user_app_block	统计用户的应用阻断次数。
	predef_user_app_app_block	统计用户下各应用的阻断次数。

如设备开启 IPv6 功能，系统支持 IPv4 和 IPv6 地址的统计。

关键字阻断

关键字阻断相关预定义统计集如下：

类别	名称	描述
关键字阻断	predef_kw_block	统计所有网页关键字/邮件过滤关键字/Web 外发信息关键字的阻断次数。
	predef_user_kw_block	统计用户的关键字阻断次数。
	predef_user_kw_kw_block	统计用户下各关键字的阻断次数。

仅支持通过 CLI 查看关键字阻断相关统计集信息。

自定义监控

系统的统计集功能可以对所有流经安全网关的数据进行统计。配置自定义监控统计集功能后，用户可以查看实时的或者一定统计周期内，基于不同的统计数据类型以及数据组织方式的系统统计信息，并且可以根据不同需求过滤统计信息，从而帮助用户更加详细和精确地了解系统的资源分配及网络安全状态。如设备开启 IPv6 功能，系统支持 IPv4 和 IPv6 地址的统计。

自定义统计集配置包括：

创建统计集

配置统计数据类型

配置数据组织方式

配置过滤条件

创建统计集

创建统计集，在全局模式下使用以下命令：

statistics-set *name*

name – 指定统计集名称，范围为 1 到 31 个字符。

执行该命令后，系统创建指定名称的统计集并且进入统计集配置模式；如果指定的统计集名称已存在，则直接进入统计集配置模式。

在全局配置模式下，使用该命令 no 的形式删除指定统计集：

no statistics-set *name*

配置统计数据类型

统计集的统计数据类型包括流量、会话、新建会话速率、URL 命中次数、关键字阻断次数和应用阻断次数。配置统计数据类型，在统计集配置模式下使用以下命令：

target-data {bandwidth | session | rampup-rate | url-hit | keyword-block | application-block| attack-rate } [record-history] [root-vsys-only]

bandwidth | session | rampup-rate | url-hit | keyword-block | application-block | attack-rate – 指定统计集的统计数据类型。可以为带宽（bandwidth）、会话（session）、新建会话速率（rampup-rate）、URL 命中次数（url-hit）、关键字阻断次数（keyword-block）或者应用阻断次数（application-block），或 AD 攻击防护次数（attack-rate）。

record-history – 记录最近 24 小时内的统计数据。

root-vsys-only – 指定仅统计 Root VSYS 中的数据。如果不配置此参数，则统计所有 VSYS 中的数据。

在统计集配置模式下，使用该命令 no 的形式取消指定统计集统计数据类型的配置：

no target-data

注意:配置统计集时，

URL 命中次数统计数据类型仅对安装有 URL 许可证的用户可用。

非根VSYS 仅支持带宽、会话、新建会话速率和 URL 命中次数数据类型。

指定 root-vsys-only 参数后，数据组织方式不能指定为 VSYS。

配置数据组织方式

统计集的数据组织方式包括 IP、接口、安全域、应用、用户、URL、URL 类别和VSYS。可配置的数据组织方式会根据统计数据类型的不同而不同。非根VSYS 同样支持 IP、接口、安全域、应用、用户、URL 和 URL 类别数据组织方式。

配置数据组织方式，在统计集配置模式下使用以下命令：

group-by {[**ip** [**directional**] [**initiator** | **responder** | **belong-to-zone** *zone-name* | **not-belong-to-zone** *zone-name* | **belong-to-interface** *interface-name* | **not-belong-to-interface** *interface-name*]] | **interface** [**directional**] | **zone** [**directional**] | **application** | **user** [**directional**] | **url** | **url-category** | **vsys**}

ip – 指定统计集的数据组织方式为 IP 地址。用户可以通过 **initiator** | **responder** | **belong-to-zone** *zone-name* | **not-belong-to-zone** *zone-name* | **belong-to-interface** *interface-name* | **not-belong-to-interface** *interface-name* 参数指定被统计 IP 的范围，可以是发起会话的 IP（**initiator**），接收会话的 IP（**responder**），属于某特定安全域的 IP（**belong-to-zone** *zone-name*），不属于某特定安全域的 IP（**not-belong-to-zone** *zone-name*），属于某特定接口的 IP（**belong-to-interface** *interface-name*）或者不属于某特定接口的 IP（**not-belong-to-interface** *interface-name*）。

directional – 指定统计结果为双向的，即统计以 IP、接口或者安全域为数据组织方式时的上行和下行带宽、接收和发送会话数、接收和发送新建会话速率；如不配置，系统默认统计结果为无方向 的，即统计以 IP、接口或者安全域为数据组织方式的所有带宽、会话或者新建会话速率。

interface – 指定统计集的数据组织方式为接口。

zone – 指定统计集的数据组织方式为安全域。

application – 指定统计集的数据组织方式为应用，此时的统计数据类型不可以为攻击速率、URL 命中次数和关键字阻断次数。

user – 指定统计集的数据组织方式为用户。

url – 指定统计集的数据组织方式为 URL。

url-category – 指定统计集的数据组织方式为 URL 类别。

vsys – 指定统计集的数据组织方式为 VSYS。

在统计集配置模式下，使用该命令 no 的形式取消指定统计集数据组织方式的配置：

no group-by

下表列出了以 IP 为数据组织方式时的数据统计信息：

方式	条件	统计数据类型					
		流量	会话	新建会话速率	URL 访问次数	关键字阻断次数	应用阻断次数
无方向	发起者 (initiator)	统计发起会话 IP 的流量	统计发起会话 IP 的会话个数	统计发起会话 IP 的新建会话速率	统计 IP 的 URL 命中次数	统计 IP 的关键字阻断次数	统计 IP 的应用阻断次数
	回应者 (responder)	统计接收会话 IP 的流量	统计接收会话 IP 的会话个数	统计接收会话 IP 的新建会话速率			
	属于安全域 (belong to zone)	统计属于某安全域的 IP 的流量	统计属于某安全域的 IP 的会话数	统计属于某安全域的 IP 的新建会话速率			
	不属于安全域(not belong to zone)	统计不属于某安全域的 IP 的流量	统计不属于某安全域的 IP 的会话数	统计不属于某安全域的 IP 的新建会话速率			
	属于接口 (belong to interface)	统计属于某接口的 IP 的流量	统计属于某接口的 IP 的会话数	统计属于某接口的 IP 的新建会话速率			
	不属于接口 (not belong to interface)	统计不属于某接口的 IP 的流量	统计不属于某接口的 IP 的会话数	统计不属于某接口的 IP 的新建会话速率			
双向	发起者 (initiator)	统计发起会话 IP 的上行和下行流量	统计发起会话 IP 的接收和发送会话个数	统计发起会话 IP 的接收和发送新建会话速率			

方式	条件	统计数据类型					
		流量	会话	新建会话速率	URL 访问次数	关键字阻断次数	应用阻断次数
	回应者 (responder)	统计接收会话 IP 的上行和下行流量	统计接收会话 IP 的接收和发送会话个数	统计接收会话 IP 的接收和发送新建会话速率			
	属于安全域 (belong to zone)	统计属于某安全域的 IP 的上行和下行流量	统计属于某安全域的 IP 的接收和发送会话个数	统计属于某安全域的 IP 的接收和发送新建会话速率			
	不属于安全域(not belong to zone)	统计不属于某安全域的 IP 的上行和下行流量	统计不属于某安全域的 IP 的接收和发送会话个数	统计不属于某安全域的 IP 的接收和发送新建会话速率			
	属于接口 (belong to interface)	统计属于某接口的 IP 的上行和下行流量	统计属于某接口的 IP 的接收和发送会话个数	统计属于某接口的 IP 的接收和发送新建会话速率			
	不属于接口 (not belong to interface)	统计不属于某接口的 IP 的上行和下行流量	统计不属于某接口的 IP 的接收和发送会话个数	统计不属于某接口的 IP 的接收和发送新建会话速率			

下表列出了以接口、安全域、应用为数据组织方式时的数据统计信息：

组织方式	方式	统计数据类型					
		流量	会话	新建会话速率	URL 命中次数	关键字阻断	应用阻断次数
安全域	无方向	统计安全域的流量	统计安全域的会话个数	统计安全域的新建会话速率	统计安全域的 URL 命中次数	N/A	N/A
	双向	统计安全域的上行和下行流量	统计安全域的接收和发送会话个数	统计安全域的接收和发送新			

组织方式	方式	统计数据类型					
		流量	会话	新建会话速率	URL 命中次数	关键字阻断	应用阻断次数
接口	无方向	统计接口的流量	统计接口的会话个数	统计接口的新建会话速率	统计接口的 URL 命中次数	N/A	N/A
	双向	统计接口的上行和下行流量	统计接口的接收和发送会话个数	统计接口的接收和发送新建会话速率			
应用	N/A	统计应用的流量	统计应用的会话个数	统计应用的新建会话速率	N/A	N/A	统计应用的应用阻断次数
用户	无方向	统计用户的流量	统计用户的会话个数	统计用户的新建会话速率	统计用户的 URL 命中次数	统计用户的关键字阻断次数	统计用户的应用阻断次数
	双向	统计用户的上行和下行流量					
URL	N/A	N/A	N/A	N/A	统计 URL 命中次数	N/A	N/A
URL 类别	N/A	N/A	N/A	N/A	统计 URL 类别命中次数	N/A	N/A
VSYS	N/A	统计VSYS 的带宽	统计VSYS 的会话个数	统计 VSYS 的新建会话速率	统计 VSYS 的 URL 命中次数	N/A	N/A

配置过滤条件

用户可以为统计集配置过滤条件，以统计特定条件下的数据信息，比如统计某个特定安全域的会话数、统计某个特定目的 IP 的带宽等等。下表列出了 StoneOS 统计集功能的所有过滤条件类型。

类型	描述
安全域（filter zone）	以安全域为条件进行过滤

类型	描述
安全域-流入（filter zone zone-name ingress）	以入安全域为条件进行过滤
安全域-流出（filter zone zone-name egress）	以出安全域为条件进行过滤
接口（filter interface）	以接口为条件进行过滤
接口-流入（filter interface if-name ingress）	以入接口为条件进行过滤
接口-流出（filter interface if-name egress）	以出接口为条件进行过滤
应用（filter application）	以应用为条件进行过滤
地址条目（filter ip）	以地址条目为条件进行过滤
地址条目-源（filter ip add-entry source）	以源地址（地址条目）为条件进行过滤
地址条目-目的（filter ip add-entry destination）	以目的地址（地址条目）为条件进行过滤
IP/掩码（filter ip A.B.C.D/M）	以 IP 为条件进行过滤
IP/掩码-源（filter ip A.B.C.D/M source）	以源 IP 为条件进行过滤
IP/掩码-目的（filter ip A.B.C.D/M destination）	以目的 IP 为条件进行过滤
用户（filter user）	以用户名称为条件进行过滤
用户组（filter user-group）	以用户组名称为条件进行过滤
严重级别（filter severity）	以攻击特征的严重级别为条件进行过滤

配置过滤条件，在统计集配置模式下，使用以下命令：

filter {**ip** {*A.B.C.D/M* | *address-entry*} [**source** | **destination**] | **interface** *name* [**ingress** | **egress**] | **zone** *name* [**ingress** | **egress**] | **application** *name* | **user** *user-name aaa-server-name* | **user-group** *user-group-name aaa-server-name*}

ip {*A.B.C.D/M* | *address-entry*} – 以指定 IP 为条件进行过滤。IP 可以是地址范围（比如 10.101.0.1 255.255.255.0 或者 10.101.0.1/24）或者系统地址簿中的地址条目。如设备开启 IPv6 功能，系统支持只查看 IPv6 地址的统计项。

source|**destination** – 以源 IP 地址（source）或者目的 IP 地址（destination）为条件进行过滤。

interface *name* – 以指定接口为条件进行过滤。

ingress | **egress** – 以入接口（ingress）或出接口（egress）为条件进行过滤。

zone *name* – 以指定安全域为条件进行过滤。

ingress | **egress** – 以入安全域（**ingress**）或出安全域（**egress**）为条件进行过滤。

application *name* – 以指定应用为条件进行过滤。

user *user-name aaa-server-name* – 以指定用户名称为条件进行过滤。

user-group *user-group-name aaa-server-name* – 以指定用户组名称为条件进行过滤。

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

在统计集配置模式下，使用该命令 no 的形式删除指定类型的过滤条件：

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

取消所有类型的过滤条件，在统计集配置模式下使用以下命令：

no filter all

开启/关闭统计集统计功能

默认情况下，仅用户监控、应用监控、设备监控预定义统计集为开启状态，其他所有预定义统计集的统计功能均为关闭状态。

在统计集配置模式下，使用以下命令开启或关闭统计集的统计功能：

开启：**active**

关闭：**no active**

{b}提示: {/b}在根 VSYS 中执行上述命令后，会开启或关闭所有 VSYS 相应的预定义统计集功能(除 non-root VSYS 不支持外)。非根VSYS 中不能开启或关闭自身的预定义统计集功能。

查看统计集信息

用户可以在任何模式下通过以下命令查看系统预定义和用户自定义统计集的配置信息：

show statistics-set *name* [{**current** | **history** | **history-max**} [**sort-by** {**up** | **down** | **item**}]]

show statistics-set – 显示系统中所有统计集的配置信息。

name – 指定统计集名称，显示特定统计集的配置信息。

current | **history** | **history-max** – 指定显示特定统计集的数据统计信息，包括：

current – 显示特定统计集的当前数据统计信息。

history – 显示特定统计集的历史数据统计信息。系统以每 5 分钟为单位进行数据采样。

history-max – 显示特定统计集的历史数据峰值统计信息。该参数仅用于统计数据类型为会话（session）的统计集。

sort-by {up | down | item} – 指定特定统计集统计数据的排列顺序（从大到小排列）：

up - 按上行数据进行排序。

down – 当配置 group-by 时指定了 directional 参数，使用该参数按下行数据进行排序。

item - 按照 group-by 的对象进行排序。

告警

告警介绍

告警功能按照告警规则的设定，对用户网络进行主动检测，探测网络问题和设备故障，并发出事故告警。

告警功能可以对告警信息进行分析统计，并且以分布图和时间轴相结合的方式展示分析结果。同时，系统还可以通过电子邮件或手机短信的方式将告警信息实时发送给管理员，帮助管理员在第一时间得知监测对象的动态信息，并根据告警内容对监测对象进行处理。

告警相关命令

action

指定告警信息发送方式。

［命令］

action {mail | sms } {on | off}

no action {mail | sms}

［句法描述］

mail -发送告警电子邮件给收件人。

sms -发送手机短信给收件人。

on | off -启用/禁用该发送方式。

［默认取值］

无。

［命令模式］

告警规则配置模式。

［使用指导］

无。

［命令实例］

hostname<config-alarm-app># **action mail on**

alarm

进入告警配置模式。

[命令]

alarm

[句法描述]

无。

[默认取值]

无。

[命令模式]

全局配置模式。

[使用指导]

无

[命 令 实 例]

hostname# **config**

hostname<config># **alarm**

hostname<config-alarm>#

alarm-expiration-time

配置告警信息的过期时间。

［命令］

alarm-expiration-time *time*

no alarm-expiration-time

［句法描述］

time -指定告警信息的过期时间。单位为天，默认值为 7。

［默认取值］

无。

［命令模式］

告警规则配置模式。

［使用指导］

无。

［命令实例］

hostname<config-alarm># **alarm-expiration-time 10**

alarm-receiver

配置接收告警信息的收件人信息。

［命令］

alarm-receiver name *name* **desc** *description* **mail** *mail* **sms** *sms*

no alarm-receiver name *name*

［句法描述］

name *name* -指定收件人的名字。

desc *description* -指定收件人的描述信息。

mail *mail* -指定收件人的邮箱地址。

sms *sms* -指定收件人的手机号码。

［默认取值］

无。

［命令模式］

告警规则配置模式。

［使用指导］

无。

［命令实例］

hostname<config-alarm># **alarm-receiver name admin1 mail admin1@mail.com sms 1391234567**

alarm-rule (application)

创建应用类告警规则，同时进入该告警规则的配置模式。如果该规则已经存在，则直接进入该规则的配置模式。

[命令]

alarm-rule [**id** *id*] **name** *name* [**desc** *description*] **type application bandwidth** | **concurrent-sessions** | **packet-forward-rate** | **rampup**

no alarm-rule {**id** *id* | **name** *name*}

[句法描述]

id *id* -指定告警规则的 ID。该 ID 是告警规则的唯一标识。

name *name* -指定告警规则的名称。

desc *description* -为告警规则添加描述信息。

bandwidth -针对每个应用的带宽发出告警。

concurrent-sessions -针对每个应用的并发连接发出告警。

packet-forward-rate -针对每个应用的包转发率发出告警。

rampup -针对每个应用的新建连接发出告警。

[默认取值]

无。

[命令模式]

告警配置模式。

[使用指导]

该命令所创建的告警规则使用的是系统默认参数。若要修改该规则的参数，参考本节其他命令。

[命 令 实 例]

hostname# **config**

hostname<config># **alarm**

hostname<config-alarm># **alarm-rule id 25 name rule-app type application bandwidth**

hostname<config-alarm-app>#

alarm-rule (network)

创建网络类告警规则，同时进入该告警规则的配置模式。如果该规则已经存在，则直接进入该规则的配置模式。

[命令]

alarm-rule [**id** *id*] **name** *name* [**desc** *description*] **type network host id** *id*

no alarm-rule id *id* | **name** *name*

[句法描述]

id *id* -指定告警规则的 ID。该 ID 是告警规则的唯一不变的标识。

name *name* -指定告警规则的名称。

desc *description* -为告警规则添加描述信息。

host id *id*- 指定网络节点的 ID。

[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**

hostname<config># **alarm**

hostname<config-alarm># **alarm-rule id 12 desc rule-network type network host id 14**

hostname<config-alarm-network>#

alarm-rule (resource)

创建设备类告警规则，同时进入该告警规则的配置模式。如果该规则已经存在，则直接进入该规则的配置模式。

[命令]

alarm-rule [**id** *id*] **name** *name* [**desc** *description*] **type resource** {**chassis-temperature** | **concurrent-sessions** | **cpu-temperature** | **cpu-usage** | **interface-bandwidth** *interface* | **memory** | **rampup** | **storage**}

no alarm-rule id *id* | **name** *name*

[句法描述]

id *id* -指定告警规则的 ID。该 ID 是告警规则的唯一不变的标识。

name *name* -指定告警规则的名称。

desc *description* -为告警规则添加描述信息。

chassis-temperature -针对设备的机箱温度发出告警。

concurrent-sessions- 针对设备的并发连接数发出告警。

cpu-temperature -针对设备的CPU 温度发出告警。

cpu-usage -针对设备的 CPU 利用率发出告警。

interface-bandwidth *interface* -针对指定接口的接口带宽发出告警。

memory -针对设备的内存利用率发出告警。

rampup -针对设备的新建连接发出告警**storage**

-针对设备的磁盘空间利用率发出告警

[默认取值]

无。

[命令模式]

告警配置模式。

[使用指导]

该命令所创建的告警规则使用的是系统默认参数。若要修改该规则的参数，参考本节其他命令。

[命 令 实 例]

hostname# **config**

hostname<config># **alarm**

hostname<config-alarm># **alarm-rule id 12 name rule-resource desc rule-chas-temp type resource chassis-temperature**

hostname<config-alarm-resource>#

alarm-rule (service)

创建服务类告警规则，同时进入该告警规则的配置模式。如果该规则已经存在，则直接进入该规则的配置模式。

[命令]

alarm-rule [**id** *id*] **name** *name* [**desc** *description*] **type service host id** *id*

no alarm-rule id *id* | **name** *name*

[句法描述]

id *id* -指定告警规则的 ID。该 ID 是告警规则的唯一不变的标识。

name *name* -指定告警规则的名称。

desc *description* -为告警规则添加描述信息。

host id *id* -指定服务节点的 ID。

[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**

hostname<config># **alarm**

hostname<config-alarm># **alarm-rule id 12 name rule-scv desc rule-service type service host id id**

hostname<config-alarm-service>#

app-name

为应用类告警规则添加应用或应用组。

[命令]

app-name *name*

no app-name *name*

[句法描述]

name -添加到告警规则的应用或应用组的名称。

[默认取值]

无。

［命令模式］

应用类告警规则配置模式。

［使用指导］

无。

［命令实例］

hostname# **config**

hostname<config># **alarm**

hostname<config-alarm># **alarm-rule id 25 name rule-app type application bandwidth**

hostname<config-alarm-app># **app-name msn**

disable

禁用告警规则。

［命令］

disable

［句法描述］

无。

［默认取值］

无。

［命令模式］

告警规则配置模式。

［使用指导］

无。

［命令实例］

hostname<config-alarm-app># **disable**

enable

启用告警规则。

［命令］

enable

［句法描述］

无。

［默认取值］

无。

［命令模式］

告警规则配置模式。

［使用指导］

无。

［命令实例］

hostname<config-alarm-app># **enable**

level

指定告警事件的严重程度。

［命令］

level {**critical** | **warning** | **info**}

［句法描述］

critical -指定事件严重程度为“严重”。

warning -指定事件严重程度为“警告”。

info -指定时间严重程度为“信息”。

［默认取值］

无。

［命令模式］

告警规则配置模式。

［使用指导］

无。

［命令实例］

hostname<config-alarm-app># **level critical**

receiver

为告警规则添加收件人。

［命令］

receiver {**mail** | **sms** } *sendobject-name*

no receiver {**mail** | **sms** } *sendobject-name*

［句法描述］

mail -指定发送告警电子邮件。

sms -指定发送手机短信。

sendobject-name -收件人的名字。该收件人必须已经存在。

［默认取值］

无。

［命令模式］

告警规则配置模式。

［使用指导］

无。

［命令实例］

hostname<config-alarm-app># **receiver sms admin-1**

schedule

为告警规则指定时间表。

［命令］

schedule *schedule-name*

no schedule *schedule-name*

［句法描述］

schedule-name -时间表的名称。

［默认取值］

无。

［命令模式］

告警规则配置模式。

［使用指导］

无。

［命令实例］

hostname<config-alarm-app># **schedule time-1**

warning

设置告警规则的过滤条件。

[命令]

warning sustain [**delay** | **loss-rate**] **time** *time* {**higher-than** |**lower-than** *threshhold1*} {**on** | **off**}

warning threshhold [**delay** | **loss-rate**] {**higher-than** | **lower-than** *threshhold2* } {**on** | **off**}

no warning {**sustain** | **trend** | **threshhold**} [**delay** | **loss-rate**]

［句法描述］

sustain -表示对某一持续的时间段进行告警条件设置。

threshhold- 表示对峰值进行告警条件设置。

delay -指定延迟时间。该参数只在网络类告警规则配置模式下出现。

loss-rate -指定丢包率。该参数只在网络类告警规则配置模式下出现。

time *time* -指定持续的时间段。在该时间段内，某事件持续发生即可触发告警。

higher-than |**lower-than** *threshhold1* 在 **time** *time*-规定的时间段内，指定某事件的上限和下限。

higher-than | **lower-than** *threshhold2* -指定某事件的峰值。

on | **off** -启用或禁用该告警规则。

［默认取值］

持续时间段的取值范围和默认值：

应用的带宽取值范围为 1 至 231，单位是 kbps。

应用的新建连接数最大值为该设备的性能参数，单位为个/秒。

应用的并发连接数最大值为该设备的性能参数，位为个。

应用的包转发率的取值范围为 1 至 231，单位是 pps。

设备的磁盘利用率的取值范围为 10 至 100，单位是%。

设备的新建连接数的取值范围为 1 至 100，单位是%。

设备的并发连接数的取值范围为 1 至 100，单位是%。

设备指定接口的流量取值范围为 1 至 100，单位是%。

设备的 CPU 占用率取值范围为 1 至 100，单位是%。

设备的内存占用率取值范围为 1 至 100，单位是%。

设备的指定 SNAT 的资源利用率的取值范围为 1 至 100，单位是%。

设备的 CPU 温度取值范围 1 至 90，单位是摄氏度。

设备的机箱温度取值范围 1 至 90，单位是摄氏度。

网络类节点的延迟时间取值范围 1 至 3,000，单位是 ms。

服务类节点的延迟时间取值范围 1 至 5,000，单位是 ms。

峰值的取值范围和单位：

应用的带宽取值范围为 1 至 231，单位是 kbps。

应用的新建连接数最大值为该设备本身的新建连接最大个数，单位为个/秒。

应用的并发连接数最大值为该设备本身的并发连接最大个数，单位为个。

应用的包转发率的取值范围为 1 至 231，单位是 pps。

设备的磁盘利用率的取值范围为 10 至 100，单位是%。

设备的新建连接数的取值范围为 1 至 100，单位是%。

设备的并发连接数的取值范围为 1 至 100，单位是%。

设备指定接口的流量取值范围为 1 至 100，单位是%。

设备的 CPU 占用率取值范围为 1 至 100，单位是%。设

备的内存占用率取值范围为 1 至 100，单位是%。

设备的指定 SNAT 的资源利用率的取值范围为 1 至 100，单位是%。

设备的 CPU 温度取值范围 1 至 90，单位是摄氏度。

设备的机箱温度取值范围 1 至 90，单位是摄氏度。

网络类节点的延迟时间取值范围 1 至 3,000，单位是 ms。

服务类节点的延迟时间取值范围 1 至 5,000，单位是 ms。

[命令模式]

告警规则配置模式。

［使用指导］

无。

［命令实例］

hostname<config-alarm-app># **warning sustain time 10 higher-than 80 on**

resource bandwidth

配置对设备接口流量的监控探测功能。

［命令］

resource bandwidth interface *interface-name* **ingress** *bandwidth* **egress** *bandwidth* [**probe-interval** *interval*] {**enable** | **disable**}

删除对指定接口的流量监控探测：**no resource bandwidth interface** *interface-name*

恢复探测间隔默认值：**no resource bandwidth interface** *interface-name* **probe-interval**

［句法描述］

interface *interface-name* -指定需要配置监控探测功能的接口的名称。

ingress *bandwidth* -指定接口的最大下行带宽值，范围为 1 至 10000000Kbps。

egress *bandwidth* -指定接口的最大上行带宽值，范围为 1 至 10000000Kbps。

probe-interval *interval* -指定探测间隔值，系统按照探测间隔对监控值进行采样。取值范围为 5 至 30 秒。

enable | **disable** -开启（**enable**）或者关闭（**disable**）接口流量监控探测功能。

［默认取值］

ingress *bandwidth*：1000000Kbps；

egress *bandwidth*：1000000Kbps；

probe-interval *interval*：10 秒。

［命令模式］

监控配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **monitor**

hostname(config-monitor)# **resource bandwidth interface ethernet0/0 ingress 100000 egress 100000 enable**

resource concurrent-sessions

配置对设备并发流量的监控探测功能。默认情况下，设备的并发流量监控探测功能是永久开启的。使用该命令 no 的形式恢复探测间隔默认值。

［命令］

resource concurrent-sessions probe-interval *interval*

no concurrent-sessions probe-interval

［句法描述］

probe-interval *interval* -指定探测间隔值，系统按照探测间隔对监控值进行采样。取值范围为 5 至 30 秒。

［默认取值］

probe-interval *interval*：10 秒。

［命令模式］

监控配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **monitor**

hostname(config-monitor)# **resource concurrent-sessions probe-interval 8**

resource cpu

配置对设备 CPU 利用率的监控探测功能。默认情况下，设备的 CPU 利用率监控探测功能是永久开启的。使用该命令 no 的形式恢复探测间隔默认值。

［命令］

resource cpu probe-interval *interval*

no resource cpu probe-interval

［句法描述］

probe-interval *interval* -指定探测间隔值，系统按照探测间隔对监控值进行采样。取值范围为 5 至 30 秒。

［默认取值］

probe-interval *interval*：10 秒。

［命令模式］

监控配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **monitor**

hostname(config-monitor)# **resource cpu probe-interval 20**

resource memory

配置对设备内存利用率的监控探测功能。默认情况下，设备的内存利用率监控探测功能是永久开启的。使用该命令 no 的形式恢复探测间隔默认值。

［命令］

resource memory probe-interval *interval*

no resource memory probe-interval

［句法描述］

probe-interval *interval* -指定探测间隔值，系统按照探测间隔对监控值进行采样。取值范围为 30 至 300 秒。

［默认取值］

probe-interval *interval*：60 秒。

［命令模式］

监控配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **monitor**

hostname(config-monitor)# **resource memory probe-interval 120**

resource rampup

配置对设备新建连接的监控探测功能。默认情况下，设备的新建连接监控探测功能是永久开启的。使用该命令 no 的形式恢复探测间隔默认值。

［命令］

resource rampup probe-interval *interval*

no resource rampup probe-interval

［句法描述］

probe-interval *interval* -指定探测间隔值，系统按照探测间隔对监控值进行采样。取值范围为 1 至 10 秒。

［默认取值］

probe-interval *interval*：5 秒。

［命令模式］

监控配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **monitor**

hostname(config-monitor)# **resource rampup probe-interval 10**

resource storage

配置对磁盘空间利用率的监控探测功能。默认情况下，设备的磁盘空间利用率监控探测功能是永久开启的。使用该命令 no 的形式恢复探测间隔默认值。

［命令］

resource storage probe-interval *interval*

no resource storage probe-interval

［句法描述］

probe-interval *interval* -指定探测间隔值，系统按照探测间隔对监控值进行采样。取值范围为 1 至 15 分钟。

［默认取值］

probe-interval *interval*：5 分钟。

［命令模式］

监控配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **monitor**

hostname(config-monitor)# **resource storage probe-interval 10**

resource temperature

配置对设备机箱及 CPU 温度的监控探测功能。默认情况下，设备机箱及 CPU 温度的监控探测功能是永久开启的。使用该命令 no 的形式恢复探测间隔默认值。

［命令］

resource temperature probe-interval *interval*

no resource temperature probe-interval

［句法描述］

probe-interval *interval* -指定探测间隔值，系统按照探测间隔对监控值进行采样。取值范围为 30 至 300 秒。

［默认取值］

probe-interval *interval*：60 秒。

［命令模式］

监控配置模式。

［使用指导］

无。

［命令实例］

hostname(config)# **monitor**

hostname(config-monitor)# **resource temperature probe-interval 100**

show alarm-rule

查看各类型的告警规则。

［命令］

show alarm-rule [all | app | resource | health | serviceandnetwork | threat]

［句法描述］

无

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show alarm all**

show alarm-receiver

显示所有的告警信息收件人。

［命令］

show alarm-receiver

［句法描述］

无

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **show alarm-receiver**

show alarm-expiration-time

显示告警信息的过期时间。

［命令］

show alarm-expiration-time

［句法描述］

无

［默认取值］

无默认值。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# show alarm-expiration-time

日志

日志介绍

设备拥有日志管理功能。系统的日志功能记录并输出安全网关的各种日志信息，分别是事件（Event）、配置（Configuration）、操作（Operation）、网络（Network）、威胁（Threat）、文件过滤日志、内容过滤日志、上网行为审计日志、流量（Traffic）、云沙箱日志和调试（Debug）信息。

事件 – 事件日志信息，包括错误、警告、通告、信息、紧急、警报、严重和调试 8 个级别的系统事件信息。。

配置 – 配置日志信息，与 CLI 配置相关的日志信息，例如接口配置等。

操作 – 操作日志信息，包括与clear、exec 命令以及对应 WebUI 操作相关的日志信息。例如 NBT 缓存中的删除操作等。

网络 – 网络日志信息，与网络服务操作相关的日志信息，例如 PPPoE 以及 DDNS 等。

威胁 – 威胁日志信息，与系统威胁相关的日志信息，例如攻击防护和应用安全等。

流量 – 流量日志信息分为会话、NAT 和上网日志信息三部分。

会话 – 会话日志信息，与会话相关的日志信息，例如会话的协议、源/目的 IP 地址、源/目的端口等。

NAT – NAT 日志信息，与 NAT 行为相关的日志信息，例如 NAT 类型、源/目的 IP 地址、源/目的端口等。

URL - URL 日志信息，与上网行为相关的日志信息，例如用户的上网时间和网页访问情况等。

文件过滤日志 – 与文件过滤相关的日志信息，例如对用户通过网络协议传输的文件检测过滤记录。

内容过滤日志 – 与内容过滤相关的日志信息，例如网页关键字过滤、Web 外发信息控制、外发邮件行为以及应用行为控制记录等。

上网行为审计日志-与上网行为相关的日志信息，例如用户上网情况、IM 行为等。

云沙箱日志- 与沙箱检测相关的日志信息。

调试 – 系统调试信息。

系统的多种日志信息能够有效的记录设备的运行情况，从而为用户分析网络情况和防护网络攻击提供依据。

日志的严重等级

系统的事件日志信息根据日志信息的严重程度区分的。系统日志的严重等级可分为 8 级，关于各级的具体信息，请参阅下表：

级别	级别号	描述	日志定义
紧急（Emergencies）	0	系统不可用信息。	LOG_EMERG
警报（Alerts）	1	需要立即处理的信息，如设备受到攻击等。	LOG_ALERT
严重（Critical）	2	危急信息，如硬件出错。	LOG_CRIT
错误（Errors）	3	错误信息。	LOG_ERR
警告（Warnings）	4	报警信息。	LOG_WARNING
通告（Notifications）	5	非错误信息，但需要特殊处理。	LOG_NOTICE
信息（Informational）	6	通知信息。	LOG_INFO
调试（Debugging）	7	调试信息，包括正常的使用信息。	LOG_DEBUG

日志信息输出目的地

日志信息可以输出到不同的目的地，设备支持以下几种日志信息输出目的地，用户可以根据自己的需要指定：

Console - Console 端口终端。

终端（Remote） – 包括 Telnet 和 SSH 两种终端。

内存缓存（Buffer）- 内存缓存。

文件（File） – 默认情况下，StoneOS 会生成一个文件记录日志信息，用户可以指定将信息输出到 USB 口的文件中。

系统（Syslog Server）- 系统可以将日志信息发往 UNIX 或 Windows Syslog Server。

Email 地址 – 将日志信息发送到某个邮件地址。

本地数据库（Localdb）- 将日志信息发送到本地数据库。本地数据库存在于存储设备中，包括 SD 存储卡、U 盘提供的存储扩展模块。

手机- 将日志信息以短信的形式发送到某个手机上。

事件日志信息可以输出到除本地数据库以外的其它目的地，威胁日志信息可以输出到除手机和本地数据库以外的其它目的地，流量日志可以输出到 Console、内存缓存、系统日志服务器和文件，而网络和调试日志信息只能输出到 Console、内存缓存和系统日志服务器。

日志信息格式

为方便用户查阅和分析系统日志信息，系统按照固定的格式输出日志信息。该格式为：**时间，级别@模块：日志描述**。请参阅以下示例：

2018-02-05 01:51:21, WARNING@LOGIN: Admin user " " logged in through console from localhost.

配置系统日志功能

通过 CLI，用户可以对系统日志功能做以下配置：

开启和关闭日志功能

事件日志信息的输出及过滤

威胁日志信息的输出

配置、调试和网络日志信息的输出

流量日志信息的输出

数据安全日志（文件过滤日志、内容过滤日志、上网行为审计日志）信息的输出

云沙箱日志信息的输出

终端防护日志信息的输出

IoT 监控日志信息的输出

配置 Syslog Server

配置 GBK 编码

指定场所

设置流量日志的主机名称/用户名称的显示状态

配置日志信息输出到Email 地址

显示日志配置相关信息

显示日志信息

导出日志信息

清除日志信息

开启和关闭日志功能

默认情况下，流量日志功能是关闭的（打开流量日志功能会影响系统性能）。开启或者关闭系统的各种日志功能，请在全局配置模式下输入以下命令：

开启：**logging** {**event** | **configuration** | **operation** | **network** | **traffic** {**session** | **nat** | **urlfilter** | **iot-monitor**} | **debug** | **threat**} **on**

关闭：**no logging** {**event** | **configuration** | **operation** | **network** | **traffic** {**session** | **nat** | **urlfilter** | **iot-monitor**} | **debug** | **threat**} **on**

事件日志信息的输出及过滤

用户可以根据需要指定事件日志信息的输出目的地，并且按照日志信息的严重级别对输出信息进行过滤。

将事件日志信息输出到console、远程终端、系统日志服务器、手机、设备硬盘卡或者使用事件日志 email 提醒功能，并且对日志信息进行过滤，在全局配置模式下使用以下命令：

logging event to {**console** | **remote** | **syslog**| **sms** | **email** | **localdb** [**size** *size*][**location** *storage-name*][**storage** {**automatically-overwrite** | **stop-overwrite**}} [**severity** *severity-level*]

console – 指定将事件日志信息输出到 console 口。

remote – 指定将事件日志信息输出到远程终端。

syslog – 指定将事件日志信息输出到 Syslog Server。关于如何配置 Syslog Server，请参阅“配置 Syslog_Server”。

sms – 指定将严重等级在严重（Critical）以上的事件日志信息以短信的形式输出到某个手机。关于如何设置手机号码，请参阅配置接收事件日志信息的手机号码一节。

email – 指定将日志信息输出到Email 地址。关于如何配置 Email 地址，请参阅“配置 Email 地址”。

localdb – 指定将事件日志信息输出到设备硬盘卡。（该功能仅部分型号设备支持。）

location – 指定存储事件日志信息的存储设备名称。

size – 指定事件日志信息占存储设备空间的百分比，取值范围为 1 到 90，默认值为 10，即事件日志信息占存储设备空间的百分比为 10%。

storage {**automatically-overwrite** | **stop-overwrite**} – 若选择 **automatically-overwrite**，表示超过存储空间的日志信息将自动覆盖旧的日志信息。若选择 **stop-overwrite**，当日志信息超过存储空间时，系统将停止存储新的日志。

severity *severity-level* – 指定输出的事件日志信息的级别从而对事件日志信息进行过滤。输出信息的级别将会是指定级别或者高于指定级别，即数字等于或者小于指定级别。例如指定级别是通告， 系统将会输出通告、警告和错误级别的日志信息。

在全局配置模式下，用以上命令 no 的形式可以关闭相关的输出功能。命令如下：

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

将事件日志信息输出到内存缓存，并且对日志信息进行过滤，在全局配置模式下使用以下命令：

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

severity *severity-level* – 指定输出的事件日志信息的级别从而对事件日志信息进行过滤。输出信息的级别将会是指定级别或者高于指定级别，即数字等于或者小于指定级别。例如指定级别是通告， 系统将会输出通告、警告和错误级别的日志信息。

size *buffer-size* – 指定内存缓存的大小。范围是 4096 到 1048576 字节。默认值为 1048576。

在全局配置模式下，用以上命令 **no logging event to buffer** 命令关闭相关的输出功能。

将事件日志信息输出到文件，并且对日志信息进行过滤，在全局配置模式下使用以下命令：

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

severity *severity-level* – 指定输出的事件日志信息的级别从而对事件日志信息进行过滤。输出信息的级别将会是指定级别或者高于指定级别，即数字等于或者小于指定级别。例如指定级别是通告，StoneOS 将会输出通告、警告和错误级别的日志信息。

name [**usb0** | **usb1**] *file-name* – 该参数用来指定保存日志信息的 U 盘和日志信息文件的名称。

size *file-size* – 将事件日志信息输出到文件（U 盘或者 Flash）时，该参数用来指定日志信息文件的大小。范围是 4096 到 1048576 字节。默认是 1048576 字节。

在全局配置模式下，用以上命令 **no logging event to file** 命令关闭相关的输出功能。

配置接收事件日志信息的手机号码

用户可将严重等级在严重（Critical）以上的事件日志信息以短信的形式输出到某个手机。指定接收事件日志的手机号码，在全局配置模式下，使用以下命令：

logging sms *phone-number*

phone-number – 指定接收事件日志的手机号码。

在全局配置模式下使用 **no logging sms** *phone-number* 命令取消手机号码的指定。

威胁日志信息的输出

用户可以根据需要指定威胁日志信息的输出目的地。将威胁日志信息输出到 console、远程终端、系统日志服务器、设备硬盘卡或者 Email 地址，在全局配置模式下使用以下命令：

logging threat to {**console** | **remote** | **syslog** [**custom-format** [**distributed** [**round-robin** | **src-ip-hash**]]] | **email** | **localdb** [**size** *size*][**location** *storage-name*][**storage** {**automatically-overwrite** | **stop-overwrite**}]

console – 指定将威胁日志信息输出到 console 口。

remote – 指定将威胁日志信息输出到远程终端。

syslog – 指定将威胁日志信息输出到 Syslog Server。关于如何配置 Syslog Server，请参阅“配置 Syslog Server”。

custom-format – 发送明文日志信息。默认情况下，系统发送明文日志信息。

distributed – 分布发送日志信息到多台日志服务器。

src-ip-hash | **round-robin** – 指定服务器选择算法。**src-ip-hash** 为源地址哈希算法。**round-robin** 为轮询调度算法，该算法为系统默认算法。

email – 指定将日志信息输出到Email 地址。关于如何配置 Email 地址，请参阅“配置 Email 地址”。

localdb – 指定日志信息的输出目的地为设备硬盘卡。（仅部分型号设备支持）。

size – 指定日志信息占存储设备空间的百分比，取值范围为 1 到 90，默认值为 10，即日志信息占存储设备空间的百分比为 10%。

location – 指定存储事件日志信息的存储设备。

storage {**automatically-overwrite** | **stop-overwrite**} – 若选择 **automatically-overwrite**，表示超过存储空间的日志信息将自动覆盖旧的日志信息。若选择 **stop-overwrite**，当日志信息超过存储空间时，系统将停止存储新的日志。

在全局配置模式下，用以上命令 no 的形式可以关闭相关的输出功能。命令如下：

no logging threat to {**console** | **remote** | **syslog** [**custom-format** [**distributed** [**round-robin** | **src-ip-hash**]]] | **email**| **localdb** }

将威胁日志信息输出到内存缓存，在全局配置模式下使用以下命令：

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

> **severity** *severity-level* – 指定输出的威胁日志信息的级别从而对威胁日志信息进行过滤。输出信息的级别将会是指定级别或者高于指定级别，即数字等于或者小于指定级别。例如指定级别是通告，StoneOS 将会输出通告、警告和错误级别的日志信息。
>
> **size** *buffer-size* – 指定内存缓存的大小。范围是 4096 到 1048576 字节。默认值为 1048576。

在全局配置模式下，用该命令 **no logging threat to buffer** 命令关闭相关的输出功能。

将威胁日志信息输出到文件，在全局配置模式下使用以下命令：

logging threat to file [**severity** *severity-level*] [**name** [**usb0** | **usb1**] file-name] [size file-size]

> **severity** *severity-level* – 指定输出的威胁日志信息的级别从而对威胁日志信息进行过滤。输出信息的级别将会是指定级别或者高于指定级别，即数字等于或者小于指定级别。例如指定级别是通告， 系统将会输出通告、警告和错误级别的日志信息。
>
> **name** [**usb0** | **usb1**] *file-name* – 该参数用来指定保存日志信息的 U 盘和日志信息文件的名称。
>
> **size** *file-size* – 将威胁日志信息输出到文件（U 盘或者 Flash）时，该参数用来指定日志信息文件的大小。范围是 4096 到 1048576 字节。默认是 1048576 字节。

在全局配置模式下，用以上命令 **no logging threat to file** 命令关闭相关的输出功能。

配置、操作、调试和网络日志信息的输出

用户可以根据需要指定日志信息的输出目的地，可以是缓存、Console 口、Syslog 服务器、文件和设备硬盘卡。操作日志和调试日志不可输出到设备硬盘卡。

将日志信息输出到 Console 口、Syslog 服务器或者设备硬盘卡，在全局配置模式下使用以下命令：

logging {**configuration** | **network**} **to** {**console** | **syslog** | **localdb** [**size** *size*]|[**location** *storage-name*]|[**storage** {**automatically-overwrite** | **stop-overwrite**}}

> **configuration** | **network** – 指定将要输出的日志信息的类型，可以是配置（configuration）或者网络（network）。
>
> **console** – 指定日志信息的输出目的地为 Console 口。
>
> **syslog** - 指定日志信息的输出目的地为 Syslog Server。关于如何配置 Syslog Server，请参阅“配置 Syslog Server”。

localdb – 指定日志信息的输出目的地为设备硬盘卡。（仅部分型号设备支持）。

size – 指定日志信息占存储设备空间的百分比，取值范围为 1 到 90，默认值为 10，即日志信息占存储设备空间的百分比为 10%。

location – 指定存储事件日志信息的存储设备。

storage {**automatically-overwrite** | **stop-overwrite**} – 若选择 **automatically-overwrite**，表示超过存储空间的日志信息将自动覆盖旧的日志信息。若选择 **stop-overwrite**，当日志信息超过存储空间时，系统将停止存储新的日志。

logging [**debug** | **operation**]**to** {**console** | **syslog**}

console – 指定调试（debug）和操作（operation）日志信息的输出目的地为 Console 口。

syslog - 指定调试（debug）和操作（operation）日志信息的输出目的地为 Syslog Server。关于如何配置 Syslog Server，请参阅“配置 Syslog Server”。

在全局配置模式下，用 **no logging** {**configuration**| **operation** | **debug** | **network**} **to** {**console** | **syslog** | **localdb**}命令关闭相关的输出功能。

将配置、操作和网络日志信息输出到文件，在全局配置模式下使用以下命令：

logging {**configuration** | **operation** | **network**} **to file** [**name** [**usb0** | **usb1**] *file-name*] [**size** *file-size*]

configuration | operation | network – 指定将要输出的日志信息的类型，可以是配置（configuration）、操作（Operation）或者网络（network）。

name [**usb0** | **usb1**] *file-name* – 该参数用来指定保存日志信息的 U 盘和日志信息文件的名称。

size *file-size* – 将配置、操作和网络日志信息输出到文件（U 盘或者Flash）时，该参数用来指定日志信息文件的大小。范围是 4096 到 1048576 字节。默认是 1048576 字节。

在全局配置模式下，用以上命令 **no logging** {**configuration** | **operation** | **network**} **to file** 命令关闭相关的输出功能。

将配置、操作、调试和网络日志信息输出到内存缓存，在全局配置模式下使用以下命令：

logging {**configuration** | **operation** | **debug** | **network**} **to buffer** [**size** *buffer-size*]

configuration | **operation** | **debug** | **network** – 指定将要输出的日志信息的类型，可以是配置（configuration）、操作（Operation）、调试（debug）或者网络（network）。

size *buffer-size* - 内存缓存的大小。范围是 4096 到 524288 字节。默认值为 1048576。

在全局配置模式下，用 **no logging** {**configuration** | **operation** | **traffic** | **debug** | **network**} **to buffer** 命令关闭相关的输出功能。

流量日志信息的输出

流量日志信息分为会话、NAT 和上网日志信息三部分，可以输出到缓存、Console 口、Syslog 服务器和文件。用户可以根据需要指定不同类别日志信息的输出目的地。

将流量日志信息输出到 Console 口、Syslog 服务器或者内存缓存，在全局配置模式下使用以下命令：

logging traffic {**session** | **nat** | **urlfilter**} **to** {**console** | **syslog** | **buffer** [**size** *buffer-size*]}

> **session** | **nat** | **urlfilter** – 指定将要输出的日志信息的类型，可以是会话（session）、NAT（nat）或者 URL（urlfilter）。
>
> **console** | **syslog** | **buffer** – 指定日志信息的输出目的地，可以是 Console 口（console）、输出到 Syslog Server（syslog）或者内存缓存。关于如何配置 Syslog Server，请参阅“配置 Syslog Server”。
>
> **size** *buffer-size* - 内存缓存的大小。范围是 4096 到 2097152 字节。默认值为 1048576。

在全局配置模式下，用 **no logging traffic** {**session** | **nat** | **urlfilter**} **to** {**console** | **syslog** | **buffer** }命令关闭相关的输出功能。

配置流量日志信息输出到文件

安全网关支持流量日志信息输出到文件功能。结合安全网关的监测对象功能，将 Syslog 服务器作为监测对象，当监测失败时，流量日志信息将会输出到 USB 口的文件中；当监测对象恢复正常后，流量日志将继续输出到 Syslog 服务器。

使用该功能前，必须保证系统的以下功能是开启的：

> 流量日志功能。在全局配置模式下，执行 **logging traffic** {**session** | **nat** | **urlfilter**}**on** 命令。
>
> 流量日志信息发送到 Syslog 服务器功能。在全局配置模式下，执行 **logging traffic to syslog** 命令。

指定流量日志信息输出到文件，在全局配置模式下使用以下命令：

logging traffic {**session** | **nat** | **urlfilter**} **to file** [**name usb0** *file-name*]

> **session** | **nat** | **urlfilter** – 指定将要输出的日志信息的类型，可以是会话（session）、NAT（nat）或者 URL（urlfilter）。
>
> **name usb0** *file-name* – 该参数用来指定保存流量日志信息的 U 盘和日志信息文件夹的名称。取值范围是 1 到 64 个字符。

在全局配置模式下，使用 **no logging traffic** {**session** | **nat** | **urlfilter**} **to file** 命令关闭相关的输出功能。

另外，还需要指定已创建的 Syslog 服务器监测对象和设置日志信息输出到文件的最大发送速率。在全局配置模式下，使用以下命令：

logging traffic {**session** | **nat** | **urlfilter**} **to syslog** [**track** {*track-object-name*}[**local-backup rate-limit** *value*]

track *track-object-name* – 指定已创建的监测对象名称。当监测失败时，流量日志信息将输出到文件；当监测对象恢复正常后，流量日志将继续输出到 Syslog 服务器。。

local-backup rate-limit *value* – 流量日志信息输出到本地文件的最大发送速率。单位为条/秒。默认值 500，范围是 1 到 800。

在全局配置模式下，使用 **no logging traffic to syslog** 命令关闭相关的输出功能。

注意:

支持该功能的平台有 M2105。具体应用请以实际产品为准。

不支持 WebUI 管理方式。

不支持 HA Active-Active（A/A）模式。

建议用户使用Ping 报文进行监测。

数据安全日志信息的输出

数据安全日志（文件过滤日志、内容过滤日志、上网行为审计日志）信息可以输出到缓存、Console 口、Syslog 服务器。用户可以根据需要指定数据安全日志（文件过滤日志、内容过滤日志、上网行为审计日志）信息的输出目的地。

输出数据安全日志（文件过滤日志、内容过滤日志、上网行为审计日志）信息到 Console、系统日志服务器，在全局配置模式下使用以下命令:

logging data-security [**dlp** | **cf** | **nbr**] **to** {**console** | **syslog**[**binary-format** [**distributed** [**src-ip-hash** | **round-robin**]] | **custom-format**]] }

console – 指定将数据安全日志（文件过滤日志、内容过滤日志、上网行为审计日志）信息输出到 console 口。

syslog – 指定将数据安全日志（文件过滤日志、内容过滤日志、上网行为审计日志）信息输出到 Syslog Server。关于如何配置 Syslog Server，请参阅“配置 Syslog Server”。

binary-format – 发送二进制类型日志信息。

distributed – 分布发送二进制日志信息到多台日志服务器。

src-ip-hash | round-robin – 指定服务器选择算法。**src-ip-hash** 为源地址哈希算法。**round-robin** 为轮询调度算法，该算法为系统默认算法。

custom-format – 发送明文日志信息。默认情况下，系统发送明文日志信息。

在全局配置模式下，用以上命令 no 的形式可以关闭相关的输出功能。命令如下：

no logging data-security [**dlp** | **cf** | **nbr**] **to** {**console** | **syslog** }

将数据安全日志（文件过滤日志、内容过滤日志、上网行为审计日志）信息输出到内存缓存，在全局配置模式下使用以下命令：

logging data-security [**dlp** | **cf** | **nbr**] **to buffer** [**size** *buffer-size*]

size *buffer-size* – 指定内存缓存的大小。范围是 4096 到 524288 字节。默认值为 524288。

在全局配置模式下，用该命令 **no logging data-security** [**dlp** | **cf** | **nbr**] **to buffer** 命令关闭相关的输出功能。

云沙箱日志信息的输出

云沙箱日志可以输出到缓存、Console 口、文件、Syslog 服务器。用户可以根据需要指定云沙箱日志的输出目的地。指定前，用户需在全局配置模式下，使用以下命令开启云沙箱日志功能：

logging sandbox on

在全局配置模式下，使用 **no logging sandbox on** 命令关闭云沙箱日志功能。

指定云沙箱日志输出地，在全局配置模式下，使用以下命令：

logging sandbox to {**console** | **syslog** | **buffer** [**size** *buffer-size*] | **file** *file-name* [**size** *file-size*]}

console – 指定将云沙箱日志信息输出到console 口。

syslog – 指定将云沙箱日志信息输出到 Syslog 服务器。

buffer [**size** *buffer-size*] - 将云沙箱日志信息输出到内存缓存，并指定缓存的大小。范围是 4096 到 524288 字节。默认值为 524288。

file *file-name* [**size** *file-size*] - 指定将云沙箱日志信息输出到文件，并指定日志信息文件的大小。范围是 4096 到 1048576 字节。默认是 1048576 字节。

在全局配置模式下，用以上命令 **no logging sandbox to** {**console** | **syslog** | **buffer** | **file**}命令关闭相关的输出功能。

终端防护日志信息的输出

终端防护日志可以输出到缓存、Console 口、文件、Syslog 服务器、终端、Email。用户可以根据需要指定终端防护日志的输出目的地。指定前，用户需在全局配置模式下，使用以下命令开启终端防护日志功能：

logging epp on

在全局配置模式下，使用 **no logging epp on** 命令关闭终端防护日志功能。

指定终端防护日志输出地，在全局配置模式下，使用以下命令：

logging epp to {**console** | **syslog** | **buffer** [**size***buffer-size*] | **file** *file-name* [**size***file-size*] | **remote** | **email**}

console – 指定将终端防护日志信息输出到 console 口。

syslog – 指定将终端防护日志信息输出到 Syslog 服务器。

buffer [**size***buffer-size*] - 将终端防护日志信息输出到内存缓存，并指定缓存的大小。范围是 4096 到 524288 字节。默认值为 524288。

file *file-name* [**size***file-size*] - 指定将终端防护日志信息输出到文件，并指定日志信息文件的大小。范围是 4096 到 1048576 字节。默认是 1048576 字节。

remote – 指定将终端防护信息输出到远程终端。

email – 指定将终端防护日志信息输出到Email 地址。

在全局配置模式下，用以上命令 **no logging epp to** {**console** | **syslog** | **buffer** | **file**| **remote** | **email** }命令关闭相关的输出功能。

IoT 监控日志信息的输出

IoT 监控日志信息可以输出到缓存、Console 口、Syslog 服务器。用户可以根据需要指定 IoT 监控日志信息的输出目的地。指定前，用户需在全局配置模式下，使用以下命令开启 IoT 监控日志功能：

logging iot-monitor on

在全局配置模式下，使用 **no logging iot-monitor on** 命令关闭 IoT 监控日志日志功能。

输出 IoT 监控日志信息到缓存、Console、系统日志服务器，在全局配置模式下使用以下命令：

logging iot-monitor to {**console** | **buffer** [**size** *buffer-size*] | **syslog** [**custom-format** [**distributed** [**src-ip-hash** | **round-robin**]]]}

console – 指定将 IoT 监控日志信息输出到 Console 口。

syslog – 指定将 IoT 监控日志信息输出到 Syslog Server。关于如何配置 Syslog Server，请参阅“配置 Syslog Server”。

custom-format – 发送明文日志信息。默认情况下，系统发送明文日志信息。

distributed – 分布发送明文日志信息到多台日志服务器。

src-ip-hash | round-robin – 指定服务器选择算法。**src-ip-hash** 为源地址哈希算法。**round-robin** 为轮询调度算法，该算法为系统默认算法。

custom-format – 发送明文日志信息。默认情况下，系统发送明文日志信息。

在全局配置模式下，使用以上命令 no 的形式可以关闭相关的输出功能。命令如下：

no logging iot-monitor to {console | buffer | syslog}

配置日志信息的输出格式

系统按照固定的格式输出日志信息，默认情况下，输出到 Syslog Server 的日志信息不显示年份、主机名称和日志级别，用户可以根据需要配置日志信息的输出格式。在全局配置模式下，使用以下命令使用以下命令：

指定输出的日志信息显示四位数年份：**logging syslog 4digit-year-timestamp**

指定输出的日志信息显示主机名称和日志级别：**logging syslog additional-information**

在全局配置模式下，使用以上命令 no 的形式取消输出的日志信息显示年份、主机名称和日志级别：

取消显示四位数年份：**no logging syslog 4digit-year-timestamp**

取消显示主机名称和日志级别：**no logging syslog additional-information**

配置 Syslog Server

将日志信息输出到 Syslog Server， 用户需要配置 Syslog Server 的 IP 地址或主机名称，也可以根据需要配置 Syslog Server 的 VRouter 名称、UDP 或者 TCP 的端口号。进行 Syslog Server 的配置，在全局配置模式下，使用以下命令：

logging syslog {*ip-address* | *hostname*} {**tcp** *port-number* | **udp** *port-number* | **secure-tcp** *port-number* [**server-cert-check-disable**] | **vrouter** *vr-name* {**tcp** *port-number* | **udp** *port-number* | **secure-tcp** *port-number* [**server-cert-check-disable**]} | **source-interface** *interface-name* {**tcp** *port-number* | **udp** *port-number* | **secure-tcp** *port-number* [**server-cert-check-disable**]}} [**type** *log-type*]

ip-address | *hostname* – 指定 Syslog Server 的 IP 地址或者主机名称。

tcp *port-number* | **udp** *port-number* | **secure-tcp** *port-number* [**server-cert-check-disable**] – 指定协议类型及协议端口号。若选择“Secure-TCP”协议，用户可根据需要指定 **server-cert-check-disable**，系统将与日志服务器不需验证证书即可正常传输日志。

vrouter *vr-name* – 指定 VRouter 的名称。

source-interface *interface-name* - 指定发送日志信息的源接口，设备会以指定接口的 IP 地址为源 IP，向日志服务器发送日志信息。如果该接口配有管理 IP 地址，优先使用管理 IP 地址。

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

在全局配置模式下使用以上命令 no 的形式取消对 Syslog Server 的配置。

no logging syslog {*ip-address* | *hostname*} {**tcp** *port-number* | **udp** *port-number* | **secure-tcp** *port-number* [**server-cert-check-disable**] | **vrouter** *vr-name* {**tcp** *port-number* | **udp** *port-number* | **secure-tcp** *port-number* [**server-cert-check-disable**]} | **source-interface** *interface-name* {**tcp** *port-number* | **udp** *port-number* | **secure-tcp** *port-number* [**server-cert-check-disable**]}} [**type** *log-type*]

配置 GBK 编码

输出到 Syslog Server 的日志信息默认的编码格式为 UTF-8,用户可根据需要开启 GBK 编码。开启 GBK 编码格式后，输出到 Syslog Server 的日志编码格式将变为 GBK 编码。在全局配置模式下，使用以下命令：

logging syslog GBK

在全局配置模式下使用 **no logging syslog GBK** 命令关闭 GBK 编码，日志编码格式将恢复为 UTF-8 编码。

指定场所

当把日志信息输出到 UNIX Syslog 服务器时，用户需要为Syslog 服务器指定场所（Facility）。指定场所，在全局配置模式下，使用以下命令：

logging facility local*x*

local*x* – 指定场所。x 的范围是 0 到 7 的整数。默认值是 7。

在全局配置模式下使用 **no logging facility** 命令恢复场所的默认值。

设置流量日志的主机名称/用户名称的显示状态

流量日志信息分为会话、NAT 和上网日志信息三类，默认情况下，流量日志中不显示主机名称和用户名称。在全局配置模式下，输入以下命令使流量日志中显示主机名称或用户名称：

在会话、NAT 和上网日志日志中显示主机名称：**logging content hostname**

在会话日志中显示用户名称：**logging session content username**

执行以上命令后，系统显示的流量日志信息中将包含主机名称/用户名称。 注意:配置 NetBIOS 名字解析功能是流量日志中主机名称显示的前提条件。

在全局配置模式下，使用以上命令 no 的形式取消主机名称/用户名称的显示：

no logging {**session** | **nat** | **urlfilter**} **content hostname**

no logging session content username

配置日志信息输出到 Email 地址

系统支持日志信息输出到指定的 Email 地址，用户需要配置接收日志信息邮件的Email 地址以及 SMTP 服务器实例。

配置 Email 地址

配置接收日志信息邮件的Email 地址。配置Email 地址，在全局配置模式下，使用以下命令：

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

email-address – 指定接收日志信息邮件的 Email 地址。

smtp *smtp-instance* – 指定用于发送邮件的 SMTP 服务器实例的名称（必须为系统中已经配置成功的 SMTP 服务器实例）。

在全局配置模式下使用以上命令 no 的形式取消对Email 地址的配置。

no logging email to *email-address*

配置 SMTP 服务器实例

配置 SMTP 服务器实例，在全局配置模式下，使用以下命令：

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

smtp-name – 指定 SMTP 服务器实例的名称。

ip-address / *hostname* – 指定 SMTP 服务器的 IP 地址或者主机名称。

email-addr – 指定发件人地址。

vrouter *vr-name* – 指定 SMTP 服务器的VRouter 的名称。

username *user-name* **password** *password* – 指定发件人帐号的用户名和密码。

mode { **plain** | **starttls** | **ssl**}- 指定系统发送的日志信息邮件的传输方式。

plain- 指定为 plain 方式，日志信息邮件将使用明文且非加密的方式传输。该方式为默认传输方式。

starttls- STARTTLS 是对纯文本通信协议的扩展，它将纯文本连接升级为加密连接。指定为 starttls 方式，日志信息邮件将使用加密方式传输。

ssl - SSL 协议是为网络通信提供安全及数据完整性的一种安全协议。指定为 ssl 方式，日志信息邮件将使用加密方式传输。

port *server-port* - 指定 SMTP 服务器的端口号。范围是 1 到 65535。不同传输方式下的默认端口号不同，PLAIN：25，STARTTLS：25，SSL：465 。

在全局配置模式下，使用 **no smtp name** *smtp-name* 命令删除指定的 SMTP 服务器实例。

配置策略路由日志功能

开启策略路由日志功能后，当策略路由规则被流量匹配到后，系统会产生策略路由日志。

开启策略路由日志功能

设备支持基于策略路由规则来开启日志功能。默认情况下，策略路由日志功能是关闭的。开启或者关闭策略路由日志功能，请在PBR 策略规则配置模式下输入以下命令：

开启：**log enable**

关闭：**no log enable**

如果需要显示策略路由日志，请在全局配置模式下，输入以下命令来开启策略路由日志显示功能：

logging traffic pbr on

在全局配置模式下，使用 **no logging traffic pbr on** 命令来关闭策略路由日志显示功能。

{b}提示: {/b}当配置了目的路由优先查找后，即使流量匹配到了策略路由规则，系统也不会产生策略路由日志。

策略路由日志信息的输出

策略路由的流量日志可以输出到 Console 终端、Syslog 服务器和内存缓存。用户可以根据需要指定输出目的地。

将策略路由的流量日志信息输出到 Console 终端、Syslog 服务器或者内存缓存，在全局配置模式下使用以下命令：

logging traffic pbr to {**console** | **syslog** | **buffer** [**size** *buffer-size*]}

console | **syslog** | **buffer** – 指定日志信息的输出目的地，可以是 Console 终端（console）、输出到 Syslog Server（syslog）或者内存缓存。关于如何配置 Syslog Server，请参阅“配置 Syslog Server”。

size *buffer-size* - 内存缓存的大小。范围是 4096 到 2097152 字节。默认值为 1048576。

在全局配置模式下，用 **no logging traffic pbr to** {**console** | **syslog** | **buffer**}命令关闭相应的输出功能。

{b}提示: {/b}设备不支持输出：

二进制格式的策略路由日志。

IPv6 的策略路由日志。

配置 PBR 日志主机名/用户名的显示状态

默认情况下，策略路由日志中不显示主机名和用户名信息。在策略路由日志中显示主机名或用户名信息，请在全局配置模式下，使用以下命令：

logging pbr content {hostname | username}

在全局配置模式下，用 no logging pbr content {hostname | username}命令取消在策略路由日志中显示主机名或用户名信息。

显示策略路由日志信息

用户可以在任何模式下通过以下命令查看所有的策略路由日志信息：

show logging traffic pbr

显示日志配置信息

用户可以在任何模式下通过以下命令查看日志配置信息：

查看系统日志信息配置状态：show logging

查看系统日志服务器的配置信息：show logging syslog

查看Email 地址的配置信息：show logging email

查看系统日志信息的统计信息：show logging statistics

查看 SMTP 服务器配置信息：show smtp

查看流量日志中主机名称和用户名称的显示状态：show logging content

查看接受事件日志的手机配置信息：show logging sms

显示日志信息

用户可以在任何模式下通过以下命令查看日志信息：

显示事件日志信息：
show logging event [severity *severity-level*]

显示调试、网络或者威胁日志信息：

show logging {**debug** [**slot** *slot-number*] [**cpu** *cpu-number*] | **network** | **threat** }

显示配置日志信息：

show logging configuration

显示操作日志信息：

show logging [**operation**]

显示数据安全日志（文件过滤日志、内容过滤日志、上网行为审计日志）：

show logging data-security [**dlp** | **cf** | **nbr**]

显示所有流量日志信息：

show logging traffic

显示流量日志信息（会话日志部分）：

show logging traffic *session* **filter-session** [**src-ip** *A.B.C.D* | **src-port** *port-num* | **dst-ip** *A.B.C.D* | **dst-port** *port-num* | **protocol** {**icmp** | **tcp** | **udp** | **others**} | **policy-id** *policy-id* | **action** {**policy-deny** | **session-start** | **session-end** | **policy-default**}]

显示流量日志信息（NAT 日志部分）：

show logging traffic *nat* **filter-nat** [**src-ip** *A.B.C.D* | **src-port** *port-num* | **dst-ip** *A.B.C.D* | **dst-port** *port-num* | **protocol** {**icmp** | **tcp** | **udp** | **others**} | **trans-src-ip** *A.B.C.D* | **trans-src-port** *port-num* | **trans-dst-ip** *A.B.C.D* | **trans-dst-port** *port-num* | **snat-rule-id** *rule-id* | **dnat-rule-id** *rule-id*]

显示流量日志信息（URL 日志部分）：

show logging traffic urlfilter

显示 IoT 监控日志信息：

show logging iot-monitor

导出日志信息

用户可以导出事件和威胁日志信息，导出的目的地包括FTP 服务器、TFTP 服务器和 U 盘。

导出事件或安全日志信息到 FTP 服务器，在执行模式使用以下命令：

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

event | **threat** - 指定导出的系统日志的类型。

ip-address - 指定 FTP 服务器的 IP 地址。

user *user-name* **password** *password* - 指定访问FTP 服务器的用户名和密码。

file-name - 指定导出的事件日志信息文件的名称。

导出事件事件或威胁日志信息到 TFTP 服务器，在执行模式下使用以下命令：

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

导出事件或威胁日志信息到 U 盘，在执行模式下使用以下命令：

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

清除日志信息

用户可以通过命令将日志信息从系统中清除。清除系统日志信息，在执行模式下，使用以下命令：

clear logging { **configuration** | **operation** | **debug** | **event** | **network** | **threat** | **traffic** {**session** | **nat** | **urlfilter**} | **data-security** [**dlp** | **cf** | **nbr**] | **iot-monitor**}

configuration -清除所有系统存储的配置日志信息。

operation -清除所有系统存储的操作日志信息。

debug – 清除所有系统存储的调试日志信息。**event**

– 清除所有系统存储的事件日志信息。**network** –

清除所有系统存储的网络日志信息。**threat** – 清除

所有系统存储的威胁日志信息。

traffic {**session** | **nat** | **urlfilter**} – 清除所有系统存储的流量日志信息，可以是会话（session）、NAT（nat）或者 URL（urlfilter）日志信息。

data-security [**dlp** | **cf** | **nbr**] – 清除所有系统存储的数据安全日志信息，可以是文件过滤日志（**dlp**）、内容过滤日志（**cf**）、上网行为审计日志（**nbr**）。

iot-monitor – 清除所有系统存储的 IoT 监控日志信息。

注意:该命令不能清除以下重要的事件日志信息：

重启：系统重启、模块卡重启；

硬件发生异常：风扇、电源等；

配置信息删除或回滚；

主备设备切换；

双主控 HA。

日志分布式外发

设备产生大量的日志信息时，单台日志服务器可能无法满足日志信息的接收需求。针对这一问题， 设备提供日志分布式外发功能，即设备能够按照一定的算法把日志信息分布发送到多个日志服务器，进而缓解单台日志服务器的压力，保证日志信息的完整、快速发送和接收。

当前版本仅支持流量和数据安全日志信息的分布式发送以及威胁日志的明文日志分布式发送。配置流量和数据安全日志信息的分布式发送功能，在全局配置模式下使用以下命令：

logging {traffic {session | nat | urlfilter} | data-security [dlp | cf | nbr]} to syslog [binary-format [distributed [src-ip-hash | round-robin]] | custom-format]

traffic {session | nat | urlfilter} | data-security [dlp | cf | nbr] – 指定分布发送式发送的日志信息类型。

syslog – 发送日志信息到日志服务器。

binary-format – 发送二进制类型日志信息。

distributed – 分布发送二进制日志信息到多台日志服务器。

src-ip-hash | round-robin – 指定服务器选择算法。src-ip-hash 为源地址哈希算法。round-robin 为轮询调度算法，该算法为系统默认算法。

custom-format – 发送明文日志信息。默认情况下，系统发送明文日志信息。

在全局配置模式下，使用以下命令取消日志信息到日志服务器的输出：

no logging {traffic {session | nat | urlfilter} | data-security [dlp | cf | nbr]} to syslog

配置威胁日志信息的明文日志分布式发送功能，在全局配置模式下使用以下命令：

logging threat to syslog [custom-format [distributed [src-ip-hash | round-robin]]]

custom-format – 发送明文日志信息。默认情况下，系统发送明文日志信息。

syslog – 发送日志信息到日志服务器。

distributed – 分布发送日志信息到多台日志服务器。

src-ip-hash | round-robin – 指定服务器选择算法。src-ip-hash 为源地址哈希算法。round-robin 为轮询调度算法，该算法为系统默认算法。

在全局配置模式下，使用以下命令取消日志信息到日志服务器的输出：

no logging threat to syslog

日志功能配置示例

本节介绍两个典型的日志功能 CLI 配置示例，分别为向 Console 口输出日志信息配置示例和向 Syslog Server 输出日志信息配置示例。

示例 1：向 Console 口输出事件日志信息

第一步：开启事件日志功能。

```
hostname# configure
hostname(config)# logging event on
```

第二步：配置 Console 口日志输出，信息级别为 Debugging。

```
hostname(config)# logging event to console severity debugging
```

示例 2：向 Syslog Server 输出事件日志信息

第一步：开启安全网关的日志功能，将 IP 地址为 202.38.1.10 的工作站用作 Syslog Server，类型为 UDP，设置信息级别为 Informational。

```
hostname(config)# logging event on
hostname(config)# logging syslog 202.38.1.10 udp 514 type event
hostname(config)# logging event to syslog severity informational
```

第二步：开启 Syslog Server。

示例 3：向本地文件输出流量日志信息

第一步：配置监测对象。将 IP 地址为 202.38.1.10 的工作站用作 Syslog Server，作为监测对象。

```
hostname(config)# track abc
hostname(config-trackip)# threshold 3
hostname(config-trackip)# ip 202.38.1.10 interface ethernet0/1 interval 2
```

第二步：开启安全网关的流量日志输出到 Syslog Server 功能，将 IP 地址为 202.38.1.10 的工作站用作 Syslog Server，VRouter 的名称为 trust-vr，类型为 UDP，端口号为 514，日志信息类型为 traffic 流量日志信息（NAT 日志部分）。

```
hostname(config)# logging traffic nat on
hostname(config)# logging syslog 202.38.1.10 vrouter "trust-vr" udp 514 type traffic nat
hostname(config)# logging traffic nat to syslog
```

第三步：开启 Syslog Server。

第四步：配置流量日志输出到本地文件，文件夹名称为”aa”。

```
hostname(config)# logging traffic nat to file name usb0 aa
```

第五步：开启 Syslog Server 监测功能以及指定最大发送速率为 600。

```
hostname(config)# logging traffic nat to syslog track abc local-backup rate-limit 600
```

故障排查

故障排查命令

exec packet-capture

开始/停止在线抓包。

［命令］

开始在线抓包：**exec packet-capture filter** *name* **start**

停止在线抓包：**exec packet-capture stop**

［句法描述］

filter *name* 指定开始在线抓包的条目名称。

［默认取值］

无。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **exec packet-capture filter filter1 start**

hostname# **exec packet-capture stop**

exec trouble-shooting packet-trace（在线）

开始/停止在线数据包路径检测。

［命令］

开始在线数据包路径检测：**exec trouble-shooting packet-trace filter** *name* [**packet-capture**] **start** [**time-out** *value*]

停止在线数据包路径检测：**exec trouble-shooting packet-trace stop**

［句法描述］

filter *name* -指定在线检测源名称。

packet-capture -开启在线抓包功能。

time-out *value* -指定检测的时间长度。达到指定时间时，系统会自动停止检测。范围为 1 到 1440 分钟。

［默认取值］

time-out *value* - 30 分钟。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **exec trouble-shooting packet-trace filter 123 start time-out 60**

hostname# **exec trouble-shooting packet-trace stop**

exec trouble-shooting packet-trace（导入）

开始/停止导入数据包路径检测。

［命令］

开始导入数据包路径检测：**exec trouble-shooting packet-trace filter** *name* **start**

停止导入数据包路径检测：**exec trouble-shooting packet-trace stop**

［句法描述］

filter *name* 指定导入检测源名称。

［默认取值］

无。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **exec trouble-shooting packet-trace filter test1 start**

hostname# **exec trouble-shooting packet-trace stop**

exec trouble-shooting packet-trace template

开始模拟数据包路径检测。

［命令］

exec trouble-shooting packet-trace template *name* **start**

［句法描述］

template *name* 指定模拟检测源名称。

［默认取值］

无。

［命令模式］

任何模式。

［使用指导］

无。

［命令实例］

hostname# **exec trouble-shooting packet-trace template test start**

export packet-capture-file

导出已抓取的数据包文件。

［命令］

export packet-capture-file to {**ftp server** *ip-address* [**user** *user-name* **password** *password*] | **tftp server** *ip-address*} [**vrouter** *vr-name*] [*file-name*]

［句法描述］

ftp server *ip-address* [**user** *user-name***password** *password*] -指定将数据包文件导出到 FTP 服务器。需要配置的参数为：

ip-address - 指定 FTP 服务器的 IP 地址

user *user-name* **password***password* – 指定访问 FTP 服务器使用的用户名和密码。当不输入用户名和密码时表示采用匿名登录方式。

tftp server *ip-address* -指定将数据包文件导出到 TFTP 服务器。指定 TFTP 服务器的 IP 地址。

vrouter *vr-name* -指定服务器所属的VR。

file-name -指定导出的数据包文件的名称。

［默认取值］

vrouter *vr-name* - trust-vr;

file-name – pktdump.pcap。

［命令模式］

执行模式。

［使用指导］

无。

［命令实例］

hostname# **export packet-capture-file to tftp server 10.1.1.1**

export trouble-shooting packet-trace packet-capture-file

导出在线数据包路径检测时抓取的数据包文件。

［命令］

export trouble-shooting packet-trace packet-capture-file to {**ftp server** *ip-address* [**user** *user-name* **password** *password*] | **tftp server** *ip-address*} [**vrouter** *vr-name*] [*file-name*]

［句法描述］

ftp server *ip-address* [**user** *user-name* **password** *password*] -指定将数据包文件导出到 FTP 服务器。需要配置的参数为：

ip-address - 指定 FTP 服务器的 IP 地址

user *user-name***password***password* – 指定访问FTP 服务器使用的用户名和密码。当不输入用户名和密码时表示采用匿名登录方式。

tftp server *ip-address* -指定将数据包文件导出到 TFTP 服务器。指定 TFTP 服务器的 IP 地址。

vrouter *vr-name* -指定服务器所属的VR。

file-name- 指定导出的数据包文件的名称。

［默认取值］

vrouter *vr-name* - trust-vr;

file-name – ts_pktdump.pcap。

［命令模式］

执行模式。

［使用指导］

无。

［命令实例］

hostname# **export trouble-shooting packet-trace packet-capture-file to tftp server 10.1.1.1**

export trouble-shooting packet-trace template

导出模拟检测报文。

［命令］

export trouble-shooting packet-trace template *name* **to** {**ftp server** *ip-address* [**user** *user-name* **password** *password*] | **tftp server** *ip-address*} [**vrouter** *vr-name*] [*file-name*]

［句法描述］

ftp server *ip-address* [**user** *user-name* **password** *password*] -指定将模拟检测报文导出到FTP 服务器。需要配置的参数为:

ip-address - 指定 FTP 服务器的 IP 地址

user *user-name* **password** *password* – 指定访问 FTP 服务器使用的用户名和密码。当不输入用户名和密码时表示采用匿名登录方式。

tftp server *ip-address* -指定将模拟检测报文导出到 TFTP 服务器。指定 TFTP 服务器的 IP 地址。

vrouter *vr-name* -指定服务器所属的VR。

file-name -指定导出的模拟检测报文文件的名称。

［默认取值］

vrouter *vr-name* - trust-vr。

［命令模式］

执行模式。

［使用指导］

无。

［命令实例］

hostname# **export trouble-shooting packet-trace template temp1 to tftp server 10.1.1.1**

import trouble-shooting packet-trace

为导入数据包路径检测导入数据包。

［命令］

import trouble-shooting packet-trace replay-file from {**ftp server** *ip-address* [**user** *user-name* **password** *password*] | **tftp server** *ip-address*} [**vrouter** *vr-name*] *file-name*

［句法描述］

ftp server *ip-address* [**user** *user-name* **password** *password*] -指定从FTP 服务器导入数据包文件。需要配置的参数为:

ip-address - 指定 FTP 服务器的 IP 地址

user *user-name* **password** *password* – 指定访问 FTP 服务器使用的用户名和密码。当不输入用户名和密码时表示采用匿名登录方式。

tftp server *ip-address* -指定从 TFTP 服务器导入数据包文件。指定 TFTP 服务器的 IP 地址。

vrouter *vr-name* -指定服务器所属的VR。

file-name -指定要导入的数据包文件的名称。

［默认取值］

vrouter *vr-name* - trust-vr。

［命令模式］

执行模式。

［使用指导］

无。

［命令实例］

hostname# **import trouble-shooting packet-trace replay-file from ftp server 10.1.1.1 user user1 password password1 test.pcap**

packet-capture filter

配置在线抓包条目。使用该命令 no 的形式删除指定的在线抓包条目。

［命令］

packet-capture filter *name* {[[**src-ip** *ip-address*] | [**user** *aaa-server user-name*] | [**user-group** *aaa-server user-name*]] [**src-port** *port-num*] [[**dst-ip** *ip-address*] | [**url** *url*]] [**dst-port** *port-num*] [**proto** {**tcp** | **udp** | **icmp** | *proto-num*}] [**application** *app-name*]} [**max-size** *file-size*] [**description** *description*]

no packet-capture filter *name*

［句法描述］

filter *name* -指定在线抓包条目的名称。

src-ip *ip-address* -指定需要抓取数据包的源 IP 地址。

user *aaa-server user-name* -指定需要抓取数据包的源用户，并指定用户所属的AAA 服务器。

user-group *aaa-server user-name* -指定需要抓取数据包的源用户组，并指定用户组所属的AAA 服务器。

dst-ip *ip-address* -指定需要抓取数据包的目的 IP 地址。

url *url*-指定需要抓取数据包的目的 URL 地址。**application**

app-name -指定需要抓取数据包的应用类型。

proto {**tcp** | **udp** | **icmp** | *proto-num*} -指定需要抓取数据包的协议类型或者协议号。

src-port *port-num* -指定需要抓取数据包的源端口号。

dst-port *port-num* -指定需要抓取数据包的目的端口号。

max-size *file-size* -指定需要抓取数据包文件的大小。抓取的数据包文件大小达到该设定值时，系统会自动停止抓包。取值范围为 2M 至 20M，默认为 10M。

description *description* -该抓包条目的描述信息。

［默认取值］

max-size *file-size* – 10 M。

［命令模式］

全局配置模式。

［使用指导］

系统最多允许创建 5 条在线抓包条目。

［命令实例］

hostname(config)# **packet-capture filter filter1 src-ip 192.168.0.1 application http max-size 20 description test**

trouble-shooting packet-trace filter（在线）

配置在线检测源。使用该命令 no 的形式删除指定的在线检测源。

［命令］

trouble-shooting packet-trace filter *name* **type live-traffic** {[[**src-ip** *ip-address*] | [**user** *aaa-server user-name*] | [**user-group** *aaa-server user-name*]] [**src-port** *port-num*] [[**dst-ip** *ip-address*] | [**url** *url*]] [**dst-port** *port-num*] [**proto** {**tcp** | **udp** | **icmp** | *proto-num*}] [**application** *app-name*] [**ingress-interface** *interface-name*]} [**description** *description*]

no trouble-shooting packet-trace filter *name*

［句法描述］

filter *name* -指定在线检测源名称。

src-ip *ip-address* -指定在线检测源的源 IP 地址。

user *aaa-server user-name* -指定在线检测源的源用户，并指定用户所属的 AAA 服务器。

user-group *aaa-server user-name* -指定在线检测源的源用户组，并指定用户组所属的 AAA 服务器。

src-port *port-num* -指定在线检测源的源端口号。

dst-ip *ip-address* -指定在线检测源的目的 IP 地址。

url *url* -指定在线检测源的目的 URL 地址。

dst-port *port-num* -指定在线检测源的目的端口号。

proto {**tcp** | **udp** | **icmp** | *proto-num*} -指定在线检测源的协议类型或者协议号。

application *app-name* 指定在线检测源的应用类型。

ingress-interface *interface-name* -指定在线检测源的入接口。

description *description*- 该在线检测源的描述信息。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

系统最多允许创建 5 个在线检测源。

［命令实例］

hostname(config)# **trouble-shooting packet-trace filter test type live-traffic dst-ip 10.1.1.1 application http ingress-interface ethernet0/0**

trouble-shooting packet-trace filter（导入）

配置导入检测源。使用该命令 no 的形式删除指定的导入检测源。

［命令］

trouble-shooting packet-trace filter *name* **type replay-file** {[**src-ip** *ip-address*] [**src-port** *port-num*] [**dst-ip** *ip-address*] [**dst-port** *port-num*] [**proto** {**tcp** | **udp** | **icmp** | *proto-num*}] [**application** *app-name*] **ingress-interface** *interface-name*} [**description** *description*]

no trouble-shooting packet-trace filter *name*

［句法描述］

filter *name* -指定导入检测源名称。

src-ip *ip-address* -指定导入检测源的源 IP 地址。

src-port *port-num* -指定导入检测源的源端口号。

dst-ip *ip-address* -指定导入检测源的目的 IP 地址。

dst-port *port-num* -指定导入检测源的目的端口号。

proto {**tcp** | **udp** | **icmp** | *proto-num*} -指定导入检测源的协议类型或者协议号。

application *app-name* -指定导入检测源的应用类型。

ingress-interface *interface-name* -指定导入检测源的入接口。

description *description* -该导入检测源的描述信息。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

系统最多允许创建 5 个导入检测源。

［命令实例］

hostname(config)# **trouble-shooting packet-trace filter test1 type replay-file src-ip 10.0.0.1 ingress-interface ethernet0/0**

trouble-shooting packet-trace template

配置模拟检测源。使用该命令 no 的形式删除指定的模拟检测源。

［命令］

trouble-shooting packet-trace template *name* **type** {**tcp** | **udp**} **src-ip** *ip-address* **src-port** *port-num* **dst-ip** *ip-address* **dst-port** *port-num* **ingress-interface** *interface-name* [**description** *description*]

trouble-shooting packet-trace template *name* **type icmp src-ip** *ip-address* **dst-ip** *ip-address* **type** *type-value* **code** *code-value* **ingress-interface** *interface-name* [**description** *description*]

no trouble-shooting packet-trace template *name*

［句法描述］

template *name* -指定模拟检测源名称。

type {**tcp** | **udp**} /**type icmp** -指定模拟检测源的协议类型，可以为 TCP、UDP 或者 ICMP。

src-ip *ip-address* -指定模拟检测源的源 IP 地址。

dst-ip *ip-address*- 指定模拟检测源的目的 IP 地址。

src-port *port-num* -当模拟检测源的协议类型为 TCP 或者 UDP 时，指定源端口号。

dst-port *port-num* -当模拟检测源的协议类型为 TCP 或者 UDP 时，指定目的端口号。

type *type-value* **code** *code-value* -当模拟检测源的协议类型为 ICMP 时，指定 ICMP Type 值和 Code 值。

ingress-interface *interface-name* -指定模拟检测源的入接口。

description *description* -该模拟检测源的描述信息。

［默认取值］

无。

［命令模式］

全局配置模式。

［使用指导］

系统最多允许创建 20 个模拟检测源。

［命令实例］

hostname(config)# trouble-shooting packet-trace template temp1 type udp src-ip 10.0.0.1 src-port 10 dst-ip 192.168.0.1 dst-port 100 ingress-interface ethernet0/0