Cisco Cisco Secure Firewall Threat Defense 命令参考

首次发布日期: 2017 年 9 月 25 日

上次修改日期: 2023 年 4 月 5 日

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

使用命令行界面 (CLI)

以下主题介绍如何使用 Cisco Secure Firewall Threat Defense 设备的命令行界面 (CLI) 以及如何解释命令参考主题。使用 CLI 进行基本系统设置和故障排除。

注释 使用 Cisco Secure Firewall Management Center 或 Secure Firewall 设备管理器部署配置更改时，请勿将 threat defense CLI 用于长时间运行的命令（例如具有大量重复计数或大小的 ping）；这些命令可能会导致部署失败。

登录命令行界面 (CLI)

要登录 CLI，使用 SSH 客户端连接到管理 IP 地址。使用 **admin** 用户名（默认密码为 Admin123）或其他 CLI 用户账号登录。

如果您为SSH连接打开某个数据接口，您也可以连接到该接口上的地址。默认情况下，禁用SSH数据接口访问。要启用 SSH 访问，请使用设备管理器（管理中心 或 设备管理器）允许与特定数据接口的 SSH 连接。您无法通过 SSH 连接到诊断接口。

您可以使用 **configure user add** 命令创建可登录 CLI 的用户账号。但这些用户只能登录 CLI，他们无法登录 设备管理器 Web 接口。CLI 仅支持本地身份验证。您无法使用外部身份验证访问 CLI。

Console Port Access

除 SSH，您还可以直接连接到设备上的控制台端口。使用设备随附的控制台电缆将您的 PC 连接到使用终端仿真器的控制台，终端仿真器的设置为 9600 波特率、8 个数据位、无奇偶校验、1 个停止位、无流量控制。有关控制台电缆的详细信息，请参阅设备的硬件指南。

在控制台端口上访问的初始 CLI 因设备类型而异。

- ASA 硬件平台 - 控制台端口上的 CLI 是常规 threat defense CLI。
- 其他硬件平台 - 控制台端口上的 CLI 是常规 Secure Firewall eXtensible 操作系统 (FXOS)。您可以使用 **connect** 命令进入 threat defense CLI。仅将 FXOS CLI 用于机箱级配置和故障排除。 对于 Firepower 2100，您无法在 FXOS CLI 上执行任何配置。使用 threat defense CLI 进行基本配置、监控和正常的系统故障排除。有关 Firepower 4100 和 9300 的 FXOS 命令的信息，请参阅 FXOS 文档。请参阅 FXOS 故障排除指南，了解其他型号的 FXOS 命令的信息。

命令模式

threat defense 设备上的 CLI 具有不同的模式，这些模式实际上是单独的 CLI，而不是单个 CLI 的子模式。您可以通过查看命令提示符来判断您所处的模式。

常规 威胁防御 CLI

使用此 CLI 进行 threat defense 管理配置和故障排除。

```
>
```

诊断 CLI

使用此 CLI 可进行高级故障排除。此 CLI 包括附加的显示和其他命令，包括通过 ASA 5506 上的无线接入点进入 CLI 所需的 **session wlan console** 命令。此 CLI 有两种子模式；特权 EXEC 模式下有更多命令可用。

要进入此模式下，请在 threat defense CLI 中使用 **system support diagnostic-cli** 命令。

- 用户 EXEC 模式。提示符反映了运行配置中定义的系统主机名。

  ```
  firepower>
  ```

- 特权 EXEC 模式。输入 **enable** 命令以进入此模式（当系统提示输入密码时，请按 Enter 键输入密码。）请注意，您无法为此模式设置密码。访问权限仅受登录 threat defense CLI 的账户保护。但是，用户无法在特权 EXEC 模式下进入配置模式，因此不需要额外的密码保护。

  ```
  firepower#
  ```

专家模式

仅当书面程序指出必须使用或思科技术支持中心要求使用专家模式时，才使用专家模式。要进入此模式下，请在 threat defense CLI 中使用 **expert** 命令。

如果您使用 admin 用户登录，则提示符为 username@hostname。如果使用其他用户，则仅显示主机名。主机名是为管理接口配置的主机名。例如，

```
admin@firepower:~$
```

FXOS CLI

除 ASA 硬件型号外，FXOS 是控制整个机箱的操作系统。根据型号，您可以使用 FXOS 进行配置和故障排除。在 FXOS 中，您可以使用 **connect** 命令进入 threat defense CLI。

对于所有设备模式型号（Firepower 4100/9300 以外的型号），您可以使用 **connect fxos** 命令从 threat defense CLI 转到 FXOS CLI。

FXOS 命令提示符如下所示，但提示符会根据模式而变化。有关 FXOS CLI 使用的详细信息，请参阅 FXOS 文档。

```
Firepower-module2>
Firepower-module2#
```

语法格式

命令语法说明使用以下约定：

约定	Description
command	**Command** 文本指示按字面显示输入的命令和关键字。
变量	变量 文本指示由您提供值的参数。
[x]	方括号中包含可选元素（关键字或参数）。
[x | y]	将以竖线分隔的关键字或参数括起来的方括号指示可选选项。
{x | y}	将以竖线分隔的关键字或参数括起来的大括号指示必需选项。
[x {y | z}]	方括号或大括号的嵌套集合指示可选或必需元素中的可选或必需选项。方括号中的大括号和竖线指示可选元素中的必需选项。

输入命令

当您通过控制台端口或 SSH 会话登录 CLI 时，系统会显示以下命令提示符：

```
>
```

在提示符后键入命令，然后按 Enter 键执行命令。其他功能包括：

- 滚动命令历史记录 - 可以使用向上和向下箭头键滚动浏览已输入的命令。您可以重新输入或编辑并重新输入历史记录中的命令。
- 完成命令-要在输入部分字符串后补全命令或关键字，请按空格或Tab键。部分字符串必须与单个命令或关键字匹配才能完成。
- 缩写命令 - 在常规 CLI 中，不能缩写命令。您必须输入完整的命令字符串。但是，在诊断 CLI 中，您可以将大多数命令缩写为最少的唯一字符；例如，您可以输入 **show ver** instead of **show version**。
- 停止命令输出 - 如果命令产生大量输出，可以按 q 键退出。
- 停止长时间运行的命令 - 如果某个命令没有足够快地返回输出，而您想要尝试其他命令，请按 Ctrl+C。

过滤 show 命令输出

您可以通过将输出传送给过滤命令来过滤 **show** 命令的输出。管道输出可搭配所有 **show** 命令使用，但搭配产生大量文本的命令使用时最为有用。

要使用过滤功能，请使用以下格式。在这种情况下，显示命令后的竖线 | 是管道字符，属于命令，而不属于语法说明。过滤选项在 | 字符后输入。

show 命令 | {**grep** | **include** | **exclude** | **begin**} 正则表达式

过滤命令

您可以使用以下过滤命令：

- **grep**- 仅显示匹配该模式的那些行。
- **include**- 仅显示匹配该模式的那些行。
- **exclude**- 排除匹配该模式的所有行并显示所有其他行。
- **begin**- 查找包含模式的第一行，并显示该行和所有后续行。

regular_expression

正则表达式，通常是简单的文本字符串。不要将表达式括在单引号或双引号中，这些引号将被视为表达式的一部分。此外，尾随空格也会包含在表达式中。

以下示例显示如何将 **show access-list** 命令的输出更改为仅显示适用于 inside1_2 接口的规则。

```
> show access-list | include inside1_2
access-list NGFW_ONBOX_ACL line 3 advanced trust ip ifc inside1_2 any ifc inside1_3 any
rule-id 268435458
event-log both (hitcnt=0) 0x2c7f5801
access-list NGFW_ONBOX_ACL line 4 advanced trust ip ifc inside1_2 any ifc inside1_4 any
rule-id 268435458
event-log both (hitcnt=0) 0xf170c15b
access-list NGFW_ONBOX_ACL line 5 advanced trust ip ifc inside1_2 any ifc inside1_5 any
rule-id 268435458
event-log both (hitcnt=0) 0xce627c77
access-list NGFW_ONBOX_ACL line 6 advanced trust ip ifc inside1_2 any ifc inside1_6 any
rule-id 268435458
event-log both (hitcnt=0) 0xe37dcdd2
access-list NGFW_ONBOX_ACL line 7 advanced trust ip ifc inside1_2 any ifc inside1_7 any
rule-id 268435458
event-log both (hitcnt=0) 0x65347856
access-list NGFW_ONBOX_ACL line 8 advanced trust ip ifc inside1_2 any ifc inside1_8 any
rule-id 268435458
event-log both (hitcnt=0) 0x6d622775
access-list NGFW_ONBOX_ACL line 9 advanced trust ip ifc inside1_3 any ifc inside1_2 any
rule-id 268435458
event-log both (hitcnt=0) 0xc1579ed7
access-list NGFW_ONBOX_ACL line 15 advanced trust ip ifc inside1_4 any ifc inside1_2 any
rule-id 268435458
event-log both (hitcnt=0) 0x1d1a8032
access-list NGFW_ONBOX_ACL line 21 advanced trust ip ifc inside1_5 any ifc inside1_2 any
rule-id 268435458
event-log both (hitcnt=0) 0xf508bbd8
```

```
access-list NGFW_ONBOX_ACL line 27 advanced trust ip ifc inside1_6 any ifc inside1_2 any
rule-id 268435458
event-log both (hitcnt=0) 0xa6be4e58
access-list NGFW_ONBOX_ACL line 33 advanced trust ip ifc inside1_7 any ifc inside1_2 any
rule-id 268435458
event-log both (hitcnt=0) 0x699725ea
access-list NGFW_ONBOX_ACL line 39 advanced trust ip ifc inside1_8 any ifc inside1_2 any
rule-id 268435458
event-log both (hitcnt=0) 0xd2014e58
access-list NGFW_ONBOX_ACL line 47 advanced trust ip ifc inside1_2 any ifc outside any
rule-id 268435457
event-log both (hitcnt=0) 0xea5bdd6e
```

命令帮助

通过输入以下命令，可从命令行获取帮助信息：

- **?** 查看所有命令的列表。
- *command_name* **?** 查看命令的选项。例如，**show ?**。
- *string***?** 以显示与该字符串匹配的命令或关键字。例如， **n?** 显示以字母 n 开头的所有命令。
- **help** *command_name* 以查看命令的语法和限制使用信息。输入 **help ?** 以查看哪些命令具有帮助页面。

第 I 部分

A - R 命令

a - clear e

aaa-server active, fail

要重新激活标记为故障的 AAA 服务器，请使用 **aaa-server active** 命令。要使主用 AAA 服务器发生故障，请使用 **aaa-server fail** 命令。

aaa-server *groupname* {**active** | **fail**} **host** *hostname*

Syntax Description

active	将服务器设置为活动状态。
fail	将服务器设置为故障状态。
groupname	AAA 服务器组或领域名称。
host *hostname*	对其执行操作的服务器的 FQDN 或 IP 地址。

Command History

版本	修改
6.2.1	引入了此命令。

使用指南

若没有此命令，则发生故障的组中的服务器仍处于故障状态，直到该组中的所有服务器发生故障为止，届时重新激活所有服务器。您可以在 **show aaa-server** 命令的输出中找到服务器组或领域名称，以及所有 AAA 服务器信息。

示例

以下示例展示在组1中的服务器 192.168.125.60 的状态并手动将其重新激活：

```
> show aaa-server group1 host 192.68.125.60
Server Group: group1
Server Protocol: RADIUS
Server Address: 192.68.125.60
Server port: 1645
Server status: FAILED. Server disabled at 11:10:08 UTC Fri Aug...
>
> aaa-server group1 active host 192.168.125.60
>
> show aaa-server group1 host 192.68.125.60
Server Group: group1
Server Protocol: RADIUS
Server Address: 192.68.125.60
Server port: 1645
Server status: ACTIVE (admin initiated). Last Transaction at 11:40:09 UTC Fri Aug...
```

Related Commands

命令	Description
clear aaa-server statistics	清除 AAA 服务器统计信息。
show aaa-server	显示 AAA 服务器统计信息

命令	Description
test aaa-server	验证 AAA 服务器的配置。

app-agent heartbeat

要为 threat defense 设备上运行的 app-agent（应用代理）配置心跳消息间隔，请使用 **app-agent heartbeat** 命令。

app-agent heartbeat ［**interval** *milliseconds*］［**retry-count** *integer*］

Syntax Description

interval *milliseconds*	指定心跳消息之间的时间间隔（以毫秒为单位）。您可以以 100 毫秒为增量调整间隔。默认值为 1000。对于版本 6.2.2 及更高版本，允许的范围为 100 到 6000，但对于较早的版本，允许的范围为 300 到 6000。 达到重试计数的连续心跳消息丢失会触发向系统其余部分发出的故障通知。默认值 1000 毫秒提供积极的故障检测设置，但存在误报故障的风险。
retry-count 整数	指定在没有响应或应用代理收到心跳消息的错误响应时，应用代理应重试心跳消息的次数，范围为 3 到 10。默认值为 3。

Command Default

默认间隔值为 1000 毫秒。

Retry-count 默认值为 3。

Command History

版本	修改
6.1	引入了此命令。
6.2.2	允许的间隔范围已更改为 100 到 6000。

使用指南

在 threat defense 设备上运行的应用代理的主要职责是在 threat defense 模块与 Firepower 2100、4100 和 9300 FXOS 机箱之间建立接口和通信。

心跳通信通道用于监控 FXOS 机箱和 threat defense应用代理之间的链路的运行状况。 threat defense 应用按特定间隔向 FXOS 机箱管理引擎发送请求消息，并按设定的次数重试，直到收到来自 FXOS 机箱管理引擎的正确响应。

threat defense 应用代理和 FXOS 机箱管理引擎之间的心跳机制还会监控硬件旁路功能是否发生故障。对于 Firepower 2100、4100 和 9300 系列上的某些接口模块，您可以启用硬件绕行功能。硬件绕行确保流量在断电期间继续在接口对之间流动。在软件或硬件发生故障时，此功能可用于维持网络连接性。

示例

以下示例将 app-agent 心跳间隔设置为 600 毫秒，将重试计数设置为 6 次：

```
> app-agent heartbeat interval 600 retry-count 6
```

Related Commands

命令	Description
show app-agent	显示应用代理状态。
show inline-set	显示内联集信息。
show interface	显示接口状态信息。

asp inspect-dp egress-optimization

要启用出口优化，请使用 **asp inspect-dp egress-optimization** 命令。要禁用出口优化，请使用此命令的 **no** 形式。

出口优化是针对所选 IPS 流量的性能特征。此功能默认在所有 威胁防御 平台上启用。

注释 我们强烈建议您启用此功能。仅在思科 TAC 建议的情况下禁用它。

asp inspect-dp egress-optimization
no asp inspect-dp egress-optimization

Command Default

默认情况下启用出口优化。

Command History

版本	修改
6.4	引入了此命令。

使用指南

出口优化应始终启用，以提高性能。出于故障排除目的，仅根据思科 TAC 的建议禁用出口优化。

示例

以下示例显示如何启用出口优化：

```
> asp inspect-dp egress-optimization
```

Related Commands

命令	Description
show conn state egress_optimization	显示符合出口优化条件的流的相关信息。根据思科TAC的建议使用此命令。
show asp inspect-dp egress-optimization	显示与出口优化相关的统计信息。
clear asp inspect-dp egress-optimization	清除与出口优化相关的统计信息。

asp load-balance per-packet

要将多个核心上的负载均衡行为更改为每个数据包，请使用 **asp load-balance per-packet** 命令。要恢复默认负载平衡机制，请使用此命令的 **no** 形式。

asp load-balance per-packet
no asp load-balance per-packet

Command Default

默认状态下，每数据包负载均衡处于禁用状态。

Command History

版本	修改
6.1	引入了此命令。

使用指南

负载均衡器的工作是将数据包分发到CPU核心并维护数据包顺序。默认情况下，一个连接一次只能由一个核心处理。由于此行为，如果与核心数量相比，使用的接口/RX 环数量较少，则核心将未得到充分利用。例如，如果threat defense设备上仅使用两个千兆以太网接口，则仅使用两个核心。（10 个千兆以太网接口有 4 个 RX 环，一个千兆以太网接口作为 1 个 RX 环。）您可能希望通过启用按数据包负载均衡来优化负载均衡器，以便使用更多核心。

当您有许多接口正在使用时，默认负载均衡行为会优化整体系统性能，而当您有较少数量的活动接口时，按数据包负载均衡器会优化整体系统性能。

如果启用按数据包负载均衡，则当一个核心处理来自某个接口的数据包时，另一个核心可以接收并处理来自同一接口的下一个数据包。因此，所有核心都可以同时处理来自同一接口的数据包。

在以下情况下，按数据包进行负载均衡可提高性能：

- 系统将丢弃数据包
- **show cpu** 命令显示 CPU 使用率远低于 100% - CPU 使用率是正在使用的核心数量的良好指标。例如，在 8 核系统上，如果使用两个核心，则 **show cpu** 显示 25%；四核：50%；六个核心：75%。
- 有少量接口正在使用

注释 通常，如果 threat defense上的并发流少于 64 个，则启用按数据包负载均衡将产生更多的开销。

示例

以下示例展示如何更改默认负载平衡行为：

```
> asp load-balance per-packet
```

Related Commands

命令	Description
clear asp load-balance history	清除和重置每数据包 ASP 负载平衡历史统计信息。正常
show asp load-balance	显示负载平衡器队列大小的柱状图。正常

asp packet-profile

要获取有关 threat defense 设备如何处理网络流量的统计信息，请使用 **asp packet-profile** 命令。要禁用数据包分析，请使用此命令的 **no** 形式。

加速安全路径或 ASP 过程决定了预过滤器策略快速路径的数据包数量、作为大型流进行了卸载、完全通过访问控制（Snort）进行评估等。

asp packet-profile
no asp packet-profile

Command Default

默认情况下启用数据包分析。

Command History

版本	修改
6.5	引入了此命令。

使用指南

数据包分析旨在始终启用。如果由于统计信息收集和进一步计算导致CPU使用率较高，则可以禁用该功能。

示例

以下示例显示如何启用数据包分析：

```
> asp packet-profile
```

Related Commands

命令	Description
show asp packet-profile	显示仅通过数据平面、数据平面和Snort并分流到硬件的数据包的统计信息。
clear asp packet-profile	清除与数据包分析相关的统计信息。

asp rule-engine transactional-commit

使用 **asp rule-engine transactional-commit** 命令为规则引擎启用或禁用交易提交模式。

asp rule-engine transactional-commit *option*
asp rule-engine transactional-commit *option*

Syntax Description

选项	对选定策略启用规则引擎的交易执行模式。选项包括： • **access-group**- 全局应用或应用于接口的访问规则。 • **nat**- 网络地址转换规则

Command Default

默认情况下，禁用交易执行模式。

Command History

版本	修改
6.6	引入了此命令。

使用指南

默认情况下，当更改基于规则的策略（例如访问规则）时，更改会立即生效。但是这种即时性会在一定程度上降低性能。对于每秒高连接环境的大量规则列表而言，例如当您更改具有 25,000 条规则的策略而设备每秒处理 18,000 个连接时，性能降低更加明显。

由于规则引擎要编译规则以实现更快的规则查找，所以性能会受到影响。默认情况下，系统在评估连接尝试以便可应用新的规则时，也搜索未编译的规则；因为规则没有编译，所以搜索需要更长时间。

您可以更改此行为，以便规则引擎在实施规则更改时使用交易模式，并在新规则编译并可用之前继续使用旧规则。使用交易模式时，性能不应在规则编译期间降低。下表解释了行为差异。

Model	编译前	编译中	编译后
默认	匹配原规则。	匹配新规则。 （每秒连接率将降低。）	匹配新规则。
事务性	匹配原规则。	匹配原规则。 （每秒连接率将不受影响。）	匹配新规则。

交易模式的另一个优势是，当替换访问组中使用的ACL时，在删除旧的 ACL 和应用新的 ACL 之间没有间隙。这将减少在操作期间丢失可接受连接的可能性。

提示 如果启用规则类型的交易模式，则会出现标记编译开始和结束的系统日志消息。这些消息从 780001 开始并往后编号。

示例

以下示例为访问组启用交易执行模式：

```
> asp rule-engine transactional-commit access-group
```

blocks

要分配额外的内存来阻止诊断（由 **show blocks** 命令显示），请使用 **blocks** 命令。要将此值恢复为默认值，请使用此命令的 **no** 形式。

blocks queue history enable ［*memory_size*］
no blocks queue history enable ［*memory_size*］

Syntax Description

memory_size	（可选）设置块诊断程序的内存大小（以字节为单位），而不是应用动态值。如果该值大于可用内存，将显示错误消息且不接受该值。如果该值大于 50% 的可用内存，将显示警告消息，但接受该值。

Command Default

分配给跟踪块诊断程序的默认内存为 2136 字节。

Command History

版本	修改
6.1	引入了此命令。

使用指南

要查看当前分配的内存，请输入 **show blocks queue history** 命令。

如果重新加载 threat defense 设备，内存分配将恢复为默认值。

分配的内存量最多将为 150 KB，但从不超过可用内存的 50%。（可选）您可以手动指定内存大小。

示例

以下示例增加块诊断程序的内存大小：

```
> blocks queue history enable
```

以下示例将内存大小增加到 3000 字节：

```
> blocks queue history enable 3000
```

以下示例尝试将内存大小增加到 3000 字节，但该值已超出可用内存：

```
> blocks queue history enable 3000
ERROR: memory size exceeds current free memory
```

以下示例将内存大小增加到 3000 字节，但该值已超出 50% 的可用内存：

```
> blocks queue history enable 3000
WARNING: memory size exceeds 50% of current free memory
```

Related Commands

命令	Description
clear blocks	清除系统缓冲区统计信息。
show blocks	显示系统缓冲区使用情况。

capture

要启用数据包捕获功能以进行数据包嗅探和网络故障隔离，请使用 **capture** 命令。要禁用数据包捕获功能，请使用此命令的 no 形式。

捕获网络流量：

capture *capture_name* [**type** { **asp-drop** [**all** | *drop-code*] | **raw-data** | **isakmp** [**ikev1** | **ikev2**] | **inline-tag** [*tag*] }] { **interface** { *interface_name* | **data-plane | management-plane | cplane** } } [**buffer** *buf_size*] [**file-size** *file_size*] [**ethernet-type** *type*] [**headers-only**] [**packet-length** *bytes*] [**circular-buffer**] [**trace** [**trace-count** *number*] [**match** *protocol* { **host** *source_ip* | *source_ip mask* | **any4** | **any6** } [*operator src_port*] { **host** *dest_ip* | *dest_ip mask* | **any4** | **any6** } [*operator dest_port*]]

捕获群集控制链路流量：

capture *capture_name* **type lacp interface** *interface_id* [**buffer** *buf_size*] [**packet-length** *bytes*] [**circular-buffer**] [**real-time** [**dump**] [**detail**]]
capture *capture_name* **interface cluster** [**buffer** *buf_size*] [**ethernet-type** *type*] [**packet-length** *bytes*] [**circular-buffer**] [**trace** [**trace-count** *number*]] [**real-time** [**dump**] [**detail**]] [**trace**] [**match** *protocol* { **host** *source_ip* | *source_ip mask* | **any4** | **any6** } [*operator src_port*] { **host** *dest_ip* | *dest_ip mask* | **any4** | **any6** } [*operator dest_port*]]

捕获整个群集范围内的数据包：

cluster exec capture *capture_name* [**persist**] [**include-decrypted**]

从捕获中删除数据包捕获或参数。如果要完全删除捕获，请忽略参数。

no capture *capture_name* [*arguments*]

停止数据包捕获而不将其删除：

capture *capture_name* **stop**

Syntax Description

any4	指定任意 IPv4 地址而不是单个 IP 地址和掩码。
any6	指定任意 IPv6 地址而不是单个 IP 地址和掩码。
all	捕获加速安全路径丢弃的数据包。
asp-drop *drop-code*	（可选）捕获通过加速安全路径丢弃的数据包。drop-code 指定通过加速安全路径丢弃的流量的类型。有关丢弃代码列表，请参阅 CLI 帮助。您可以使用 **packet-length** 、 **circular-buffer** 和 **buffer** 关键字输入此关键字，但不能使用 **interface** 或 **ethernet-type** 关键字。在集群中，还将捕获从一台设备转发到另一台设备时丢失的转发数据包。

buffer *buf_size*	（可选）定义用于存储数据包的缓存大小（以字节为单位）。一旦字节缓冲区已满，数据包捕获将停止。用于集群中时，此值是指每台设备的大小，而不是所有设备的总和。支持的最大缓冲区大小为 32 MB。 缓冲区大小和文件大小选项相互排斥。
capture_name	指定数据包捕获的名称。在多个 **capture** 语句中使用同一个 名称可捕获多种类型的流量。当使用 **show capture** 命令查看捕获配置时，所有选项均合并到一行。
data-plane	指定在数据平面接口上捕获的数据包。
management-plane	指定管理接口上捕获的数据包。
circular-buffer	（可选）当缓冲区已满时，从开头开始覆盖缓冲区。
ethernet-type *type*	（可选）选择要捕获的以太网类型。支持的以太网类型包括 8021Q、ARP、IP、IP6、LACP、PPPOED、PPPOES、RARP 和 VLAN。802.1Q 或 VLAN 类型会出现异常。802.1Q 标记会被自动跳过，内部以太网类型用于匹配。
file-size *file-size*	（可选） **file-size** 指定将数据包捕获到磁盘上的文件。 文件大小 指定捕获文件的大小，范围为 32 MB 到 10 GB。 捕获文件将在闪存 **(disk0:/)** 中创建，名称为 **capture_name.pcap** 。 配置 **文件大小** 时，硬盘内存（文件）用于将捕获的数据写入捕获缓冲区。捕获的数据根据文件名存储在磁盘中。 缓冲区大小和文件大小选项相互排斥。
headers-only	（可选）选择要在没有数据的情况下捕获的数据包的第 2 层和第 3/4 层报头。
host *source_ip*, *dest_ip*	指定数据包发送到或来自的主机的单个 IP 地址。
include-decrypted	（可选）在包含正常流量和已解密流量的已解密 IPsec 数据包进入防火墙设备后对其进行捕获。它还捕获 SSL 解密流量的数据包。但是，此选项不适用于 VTI 隧道，因为只能在 VTI 接口上看到解密格式的数据包；而不是在外部，例如加密映射 VPN。
inline-tag *tag*	为特定 SGT 值指定标记或将其保持未指定状态以捕获标记了任何 SGT 值的数据包。
interface *interface_name*	设置将用于数据包捕获的接口的名称。您必须为除了 **type asp-drop**之外的任何要捕获的数据包配置接口。可以使用多个具有相同名称的 **capture** 命令配置多个接口。要捕获管理平面上的数据包，可以使用 **interface** 关键字和 **asa_mgmt_plane** 作为接口名称。可以指定 **cluster** 为接口名称，以捕获集群控制链路接口上的流量。 要在数据接口上启用访问 管理中心 时捕获内部背板接口上的数据包，请指定 **nlp_int_tap**。如果配置了 **lacp** 类型的捕获，则接口名称为物理名称。

ikev1，**ikev2**	仅捕获 IKEv1 或 IKEv2 协议信息。
isakmp	（可选）捕获 VPN 连接的 ISAKMP 流量。ISAKMP 子系统无权访问上层协议。捕获是伪捕获，并将物理层、IP 层和 UDP 层结合在一起来满足 PCAP 解析器。对等设备地址通过 SA 交换获得，存储在 IP 层中。
lacp	（可选）捕获 LACP 流量。如果已配置，则接口名称为物理接口名称。
mask	IP 地址的子网掩码，例如，C 类掩码为 255.255.255.0。
match *protocol*	指定与五元组匹配的数据包以允许过滤要捕获的数据包。在一行中最多可以使用三次此关键字。
operator src_port, *dest_port*	（可选）匹配源或目标使用的端口号。允许的运算符如下： • **lt**- 小于 • **gt**-大于 • **eq**-等于 • **neq**-不等于 • **range**-范围
packet-length *bytes*	（可选）设置每个要存储在捕获缓冲区中的数据包的最大字节数。
persit	（可选）捕获集群设备上的持久性数据包。
raw-data	（可选）捕获一个或多个接口上的入站和出站数据包。
stop	停止数据包捕获而不将其删除。使用命令的**no**形式和此选项重新启动捕获。
trace *trace_count*	（可选）捕获数据包跟踪信息和要捕获的数据包数量。将此选项与访问列表一起使用来向数据路径插入跟踪数据包，以确定是否已按预期处理数据包。
type	（可选）指定所捕获数据的类型。

Command Default

默认值如下：

- 默认 **type** 为 **raw-data**。
- 默认 **buffer** 大小 为512 KB。
- 默认以太网类型为 IP 数据包。
- 默认的 **packet-length** 为 1518 个字节。

Command History

版本	修改
6.1	引入了此命令。

版本	修改
6.2.1	此命令已更新，以在设备崩溃时将所有活动捕获的内容存储到闪存或磁盘上的文件中。
6.2.3	选项 asa_mgmt_plane 和 asa_dataplane 分别重命名为 **management-plane** 和 **data-plane** 。
6.2.3.x	引入 **any4** 和 **any6** 选项是为了分别捕获 IPv4 和 IPv6 网络流量。
6.3	选项［**file-size** *file-size*］允许您以 MB (32-10000) 为单位捕获文件大小。
6.7	添加 **interface nlp_int_tap**管理中心 接口名称是为了在数据接口上启用访问时捕获内部背板接口上的数据包。

使用指南

当对连接问题进行故障排除或监视可疑活动时，捕获数据包可能非常有用。可以创建多个捕获。**capture** 命令不会保存到运行配置，也不会在高可用性期间复制到备用设备。

threat defense 设备能跟踪所有流经它的 IP 流量，并能捕获所有以它为目标的 IP 流量，包括所有管理流量（如 SSH 和 Telnet 流量）。

threat defense 架构包括三组不同的处理器进行数据包处理；这种架构对捕获功能具有某些限制。通常 threat defense 设备中的大部分数据包转发功能由两个前端网络处理器处理，数据包仅在需要应用检查时才发送到控制平面通用处理器。仅当加速路径处理器中缺少会话时，数据包才发送到会话管理路径网络处理器。

由于 threat defense 设备转发或丢弃的所有数据包都会到达两个前端网络处理器，因此在这两个网络处理器中实施数据包捕获功能。所以如果为流量接口配置合适的捕获，到达 threat defense 设备的所有数据包都会被这两个前端处理器捕获。在入口端，在数据包到达接口时捕获数据包，而在出口端，先捕获数据包，再在线发出。

要保存捕获的数据，数据包捕获会自动将捕获的数据即时写入物理存储，而无需使用**copy**命令。捕获大小最高支持 10 GB。大于 100 MB 的捕获将自动压缩。

保存捕获

当 threat defense 设备崩溃时，系统会保存设备上任何活动捕获的内容。在故障排除流程中激活捕获时，必须注意以下几点：

- 要使用的捕获缓冲区的大小，以及闪存/磁盘上是否有足够的空间。
- 对于所有使用案例，捕获缓冲区应标记为循环，以便捕获的数据包是崩溃前的最新数据包。

用于保存活动捕获内容的文件的名称为：

[<context_name> .]<capture_name> .pcap

context_name 表示在多情景模式下激活捕获的用户情景的名称。对于单情景模式，context_name 不适用。

capture_name 表示已激活的捕获的名称。

捕获保存发生在控制台或故障转储之前。对于 33 MB 的捕获缓冲区，这会增加大约 5 秒的崩溃停机时间。嵌套崩溃的风险很小，因为将捕获的内容复制到文件是一个简单的流程。

查看捕获

要查看数据包捕获，请使用 **show capture** *name* 命令。要将捕获保存到文件，请使用 **copy capture** 命令。使用 **https://***FTP-ip-address***/***admin***/capture/***capture_name*[**/pcap**] 命令在网络浏览器中查看数据包捕获信息。如果指定 **pcap** 可选关键字，则一个 libpcap 格式文件会下载到网络浏览器，并可以使用网络浏览器保存。（可以使用 TCPDUMP 或 Ethereal 查看 libcap 文件。）

如果将缓冲区内容以 ASCII 格式复制到 TFTP 服务器，将只能看到数据包的信头，而看不到详细信息和十六进制转储。要查看详细信息和十六进制转储，您需要传送 PCAP 格式的缓冲区并使用 TCPDUMP 或 Ethereal 读取。

删除捕获

输入不带任何关键字的 **no capture** 将删除捕获。要保留捕获，请指定 **interface** 关键字；捕获从指定接口分离，并保留捕获。

群集技术

您可以在 **capture** 命令前面加上 **cluster exec**，在一个单元上发出 **capture** 命令，同时在所有其他单元上运行该命令。当执行集群范围的捕获后，要同时将相同捕获文件从集群中的所有设备复制到 TFTP 服务器，请在主设备上输入 **cluster exec copy** 命令：

cluster exec capture *capture_name arguments*

cluster exec copy /pcap capture: *cap_name* **tftp://***location***/***path***/***filename***.pcap**

多个 PCAP 文件（一个文件来自一个设备）将复制到 TFTP 服务器。目标捕获文件名会自动附加设备名称，例如 filename_A.pcap、filename_B.pcap 等。在此示例中，A 和 B 是集群设备名称。

注释 如果在文件名末尾添加设备名称，将生成不同的目标名称。

限制

以下是一些捕获功能限制。大多数限制由 threat defense 架构的分布式性质以及 threat defense 设备中使用的硬件加速器导致。

- 对于内联 SGT 标记数据包，捕获的数据包包含您的 PCAP 查看器可能无法识别的其他 CMD 信头。
- 如果数据包中的 802.1Q 标记与配置的子接口不同，则不会捕获此类数据包。数据包将被忽略，因为它们未与任何命名接口关联。
- 如果没有入口接口并因而没有全局接口，则在背板上发送的数据包将被视为系统情景 。这些数据包将绕过访问列表检查并始终被捕获。

- show capture 命令显示捕获特定 asp-drop 时的正确原因。但是，在捕获所有 asp-drop 时，show capture 命令不会显示正确的原因。

具有 file-size 选项的数据包捕获功能具有以下限制：

- 仅适用于Firepower 4100/9300 系列。
- 对于现有捕获，您无法添加文件大小选项。
- 不支持 **copy** 命令。
- 不支持实时、跟踪、线性和循环缓冲区。
- 如果使用文件大小选项增加捕获数量，系统的性能将会降低。
- 如果系统负载较高，则会导致数据包捕获数据丢失。

示例

要捕获数据包，请输入以下命令：

```
> capture captest interface inside
> capture captest interface outside
```

在网络浏览器中，可以在以下名为“captest”的位置查看发出的 **capture** 命令的内容：

```
https://171.69.38.95/admin/capture/captest
```

要将 libpcap 文件（网络浏览器使用的文件）下载到本地机器，请输入以下命令：

```
https://171.69.38.95/capture/http/pcap
```

以下示例显示如何在 threat defense 设备崩溃时在单模式下捕获数据包：

```
> capture 789 interface inside
```

捕获 '789' 的内容另存为 *789.pcap* 文件。

以下示例显示如何在 threat defense 崩溃时在多模式下捕获数据包：

```
>capture 624 interface inside
```

管理情景中的捕获“624”的内容另存为 *admin.624.pcap* 文件。

以下示例展示如何捕获 ARP 数据包：

```
> capture arp ethernet-type arp interface outside
```

群集技术的捕获

要在集群中的所有设备上启用捕获，可以在每个命令的前面添加 cluster exec 关键字。

以下示例展示如何为群集技术环境创建 LACP 捕获：

```
> capture lacp type lacp interface gigabitEthernet0/0
```

以下示例 显示如何为集群链路中的控制路径数据包 创建捕获：

```
> capture cp interface cluster match udp any eq 49495 any
> capture cp interface cluster match udp any any eq 49495
```

以下示例显示如何通过集群捕获数据路径流量：

```
> capture abc interface inside match tcp host 1.1.1.1 host 2.2.2.2 eq www
> capture abc interface inside match dup host 1.1.1.1 any
```

Related Commands

命令	Description
clear capture	清除捕获缓冲区。
copy capture	将捕获文件复制到服务器。
show capture	在未指定选项时显示捕获配置。

capture-traffic

要拦截和捕获通过 threat defense 接口的数据包，请使用 **capture-traffic** 命令。您可以捕获与显示的选项列表中的整数表达式匹配的指定 threat defense 域（管理接口 (br1) 或流量接口）上的流量。

capture-traffic

系统将提示您输入域和 TCP 转储选项。

Syntax Description

domain	指定捕获流量的域： • 0 - br1，捕获来自管理接口的流量 • 1 - 路由器，捕获来自已配置数据接口的流量
-A	以 ASCII 格式打印每个数据包（减去其链路级信头）。便于捕获网页。
-B	将操作系统捕获缓冲区大小设置为 buffer_size。
-c	收到 count 个数据包后退出。
-C	在将原始数据包写入保存文件之前，检查文件当前是否大于 file_size，如果是，则关闭当前保存文件并打开一个新的保存文件。在第一个保存文件之后的保存文件将具有使用 -w 标志指定的名称，其后有一个数字，从 1 开始一直向上。file_size 的单位是数百万字节（1,000,000 字节，而不是 1,048,576 字节）。
-d	以人类可读的形式将已编译的数据包匹配代码转储到标准输出并停止。
-dd	将数据包匹配代码转储为 C 程序片段。
-ddd	将数据包匹配代码转储为十进制数字（前面带有计数）。
-D	打印系统上可用以及 tcpdump 可以捕获数据包的网络接口的列表。对于每个网络接口，打印一个编号和接口名称，可能后跟接口的文本说明。可以向 -i 标志提供接口名称或编号，以指定要捕获的接口。 这在没有用于列出它们的命令的系统上非常有用（Windows 系统或缺少 ifconfig -a 的 UNIX 系统）；编号在 Windows 2000 和更高版本的系统上很有用，其中接口名称是一个比较复杂的字符串。 如果 tcpdump 是使用缺少 pcap_findaclldevs() 函数的旧版本 libpcap 构建的，则不支持 -D 标志。
-e	在每个转储行上打印链路级信头。
-E	使用 spi@ipaddr algo:secret 解密发往 addr 并包含安全参数索引值 spi 的 IPsec ESP 数据包。可以使用逗号或换行符来重复此组合。

-f	以数字方式而不是符号方式打印“外部”IPv4 地址（此选项旨在绕过 Sun 的 NIS 服务器中的严重脑损伤，通常它会在转换非本地互联网号码时永远挂起）。 使用进行捕获的接口的 IPv4 地址和网络掩码来完成对“外部”IPv4 地址的测试。 如果该地址或网络掩码不可用，则可能是因为执行捕获的接口没有地址或网络掩码，或者因为捕获是在 Linux 的“任意”接口上完成的，而该接口可以在多个接口上捕获，此选项将无法正常工作。
-F	使用文件作为过滤器表达式的输入。命令行上给出的其他表达式将被忽略。
-G	如果已指定，则每隔rotate_seconds 秒轮换使用 -w 选项指定的转储文件。 保存文件将具有 -w 指定的名称，其中应包含 strftime(3) 定义的时间格式。如果未指定时间格式，则每个新文件都将覆盖以前的文件。 如果与 -C 选项结合使用，文件名将采用“file”的形式<count>'。
-I	将接口置于“监控模式”；此功能仅在 IEEE 802.11 Wi-Fi 接口上受支持，并且仅在某些操作系统上受支持。
-K	不尝试验证 TCP 校验和。 这对于在硬件中执行 TCP 校验和计算的接口很有用；否则，所有传出 TCP 校验和都将被标记为错误。
-l	缓冲标准输出行。如果要在捕获数据时查看数据，则非常有用。示例，"tcpdump -l | tee dat”或“tcpdump -l > dat & tail -f dat”。
-L	列出接口和出口的已知数据链路类型。
-m	从文件模块加载 SMI MIB 模块定义。 可以多次使用此选项将多个 MIB 模块加载到 tcpdump 中。
-M	使用密钥作为共享密钥，以验证在 TCP-MD5 选项 (RFC 2385)（如果有）的 TCP 分段中找到的摘要。
-n	不将地址（即主机地址、端口号等）转换为名称。
-N	不打印主机名的域名限定条件。 例如，如果您提供此标志，则 tcpdump 将打印“nic”而不是“nic.ddn.mil”。
-O	不运行数据包匹配代码优化器。仅当您怀疑优化器中存在漏洞时，这才有用。
-p	不会将接口置于混杂模式。请注意，接口可能由于其他原因而处于混杂模式；因此，“-p”不能用作“ether host {local-hw-addr}”或“ether broadcast”的缩写。
-q	快速输出。打印较少的协议信息，因此输出行更短。

-R	假定 ESP/AH 数据包基于旧规范（RFC1825 至 RFC1829）。如果指定，tcpdump 将不会打印重放预防字段。 由于 ESP/AH 规范中没有协议版本字段，因此 tcpdump 无法推断 ESP/AH 协议的版本。
-r	从文件（使用 -w 选项创建）中读取数据包。如果文件为“-”，则使用标准输入。
-S	输出 TCP 序列号的绝对值，而不是相对值。
-s	从每个数据包中捕获数据的 snaplen 字节，而不是默认值 68（对于 SunOS 的 NIT，最小值实际上是 96）。对于 IP、ICMP、TCP 和 UDP 而言，68 字节已足够，但可能会截断名称服务器和 NFS 数据包中的协议信息（请参阅下文）。由于快照有限而被截断的数据包在输出中用“[|proto]”表示，其中 proto 是发生截断的协议级别的名称。 请注意，拍摄较大的快照会增加处理数据包所需的时间，并有效地减少数据包缓冲量。这可能会导致数据包丢失。您应将 snaplen 限制为将捕获您感兴趣的协议信息的最小数字。将 snaplen 设置为 0 意味着使用所需的长度来捕获整个数据包。
-T	强制按指定类型解释由“表达式”选择的数据包。目前已知的类型包括 aodv（临时按需距离矢量协议）、cnfp（思科 NetFlow 协议）、rpc（远程过程调用）、rtp（实时应用协议）、rtcp（实时应用控制协议）， snmp（简单网络管理协议）、tftp（简单文件传输协议）、vat（可视音频工具）和 wb（分布式白板）。
-t	不在每个转储行上打印时间戳。
-tt	在每个转储行上打印未格式化的时间戳。
-ttt	在每个转储行上打印当前行和上一行之间的增量（微秒分辨率）。
-tttt	在每个转储行上按日期打印默认格式的时间戳。
-ttttt	在每个转储行上打印当前行和第一行之间的增量（微秒分辨率）。
-u	打印未解码的 NFS 句柄。
-U	通过 -w 选项“packet-buffered”保存输出；即，当每个数据包被保存时，它将被写入输出文件，而不是仅在输出缓冲区填满时写入。 如果 tcpdump 是使用缺少 pcap_dump_flush() 函数的旧版本 libpcap 构建的，则不支持 -U 标志。
-v	在解析和打印时，生成（略多）冗长输出。例如，系统会打印 IP 数据包中的持续时间、标识、总长度和选项。还可以启用其他数据包完整性检查，例如验证 IP 和 ICMP 信头校验和。 使用 -w 选项写入文件时，每 10 秒报告捕获的数据包数。

-vv	更冗长的输出。例如，系统会从 NFS 应答数据包打印更多字段，并对 SMB 数据包进行完全解码。
-vvv	更冗长的输出。例如，telnet SB ... SE 选项。使用 -X 时，Telnet 选项也以十六进制显示。
-w	将原始数据包写入文件，而不是解析并打印出来。稍后可以使用 -r 选项打印它们。如果文件为“-”，则使用标准输出。
-W	与 -C 选项结合使用，这会将创建的文件数限制为指定的数量，并从头开始写入文件，从而创建“循环”缓冲区。此外，它将使用足够的前导 0 来命名文件，以支持最大数量的文件，从而使它们能够正确排序。
-x	在解析和打印时，除了打印每个数据包的信头外，还以十六进制格式打印每个数据包的数据（除去其链路级报头）。将打印整个数据包或 snaplen 字节中较小的一个。请注意，这是整个链路层数据包，因此对于填充的链路层（例如以太网），当较高层数据包短于所需填充时，也会打印填充字节。
-xx	在解析和打印时，除了打印每个数据包的信头外，还以十六进制格式打印每个数据包的数据。
-X	在解析和打印时，除了打印每个数据包的报头外，还以十六进制和 ASCII 格式打印每个数据包的数据（除去其链路级信头）。 这对于分析新协议非常方便。
-XX	在解析和打印时，除了打印每个数据包的信头外，还以十六进制和 ASCII 格式打印每个数据包的数据。
-y	将捕获数据包时使用的数据链路类型设置为 datalinktype。
-Z	删除权限（如果是 root）并将用户 ID 更改为 user，将组 ID 更改为用户的主要组。

Command History

版本	修改
6.1	引入了此命令。

使用指南

默认情况下， **capture-traffic** 命令会为拦截的每个数据包生成一行文本。每行包括：时间戳；协议名称；源地址和目的地址（对于 IP 数据包，这些是 IP 地址；对于其他协议，除非明确要求，否则 **capture-traffic** 不会打印任何标识符（请参阅 **-e** 命令行描述））；信息包括 TCP 序列号、标志、ARP/ICMP 命令等。

注释 **pcap** 文件（ **capture-traffic** 或 **debug daq**命令的输出）显示已接收数据包的未转换详细信息；**Connection Events** 列表 (管理中心) 显示策略实际应用的已转换数据包详细信息。

要停止捕获，请键入 Control + C。如果使用 **-w** *outputfile* 选项，数据包捕获将使用该文件名保存在 /var/common/ 中。否则，它将写入显示屏。

示例

以下示例显示如何从管理接口捕获流量：

```
> capture-traffic
Please choose domain to capture traffic from:
  0 - br1
  1 - Router
Selection? 0
Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
-v
```

Related Commands

命令	Description
show traffic	显示流量统计信息。
show interface	显示接口状态信息。

clear aaa-server statistics

要重置 AAA 服务器的统计信息，请使用 **clear aaa-server statistics** 命令。

clear aaa-server statistics ［**LOCAL** | *groupname* ［**host** *hostname*］ | **protocol** *protocol*］

Syntax Description

groupname	（可选）清除组中服务器的统计信息。
host *hostname*	（可选）清除组中特定服务器的统计信息。
LOCAL	（可选）清除 LOCAL 用户数据库的统计信息。
protocol *protocol*	（可选）清除指定协议的服务器的统计信息。输入 ? 查看可用的协议。

Command Default

删除所有组内的所有 AAA 服务器统计信息。

Command History

版本	修改
6.2.1	引入了此命令。

示例

以下示例展示如何重置所有服务器组的 AAA 统计信息：

```
> clear aaa-server statistics
```

以下示例展示如何重置整个服务器组的 AAA 统计信息：

```
> clear aaa-server statistics svrgrp1
```

以下示例展示如何重置组中特定服务器的 AAA 统计信息：

```
> clear aaa-server statistics svrgrp1 host 10.2.3.4
```

Related Commands

命令	Description
show aaa-server	显示 AAA 服务器统计信息

clear access-list

要清除访问列表计数器，请使用 clear access-list 命令。

clear access-list *ID*

Syntax Description

ID	访问列表的名称。

Command History

版本	修改
6.1	引入了此命令。

使用指南

当输入 **clear access-list** 命令时，必须指定访问列表的 *id* 才能清除计数器。使用 **show access-list** 命令获取 ACL 列表。

示例

以下示例展示如何清除特定访问列表计数器：

```
> clear access-list inbound
```

Related Commands

命令	Description
show access-list	按编号显示访问列表条目。
show running-config access-list	显示在自适应安全设备上运行的访问列表配置。

clear arp

要清除动态 ARP 条目或 ARP 统计信息，请使用 **clear arp** 命令。

clear arp ［**statistics** | *interface_name*］

Syntax Description

statistics	清除 ARP 统计信息。
interface_name	清除指定接口的统计信息。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例清除所有 ARP 统计信息：

```
> clear arp statistics
```

Related Commands

命令	Description
show arp statistics	显示 ARP 统计信息。
show running-config arp	显示 ARP 超时的当前配置。

clear asp

要清除加速安全路径 (ASP) 统计信息，请使用 **clear asp** 命令。

clear asp { **cluster counter** | **dispatch** | **drop** [**flow** | **frame**] | **event dp-cp** | **inspect-dp ack-passthrough** | **inspect-dp egress-optimization** | **inspect-dp snort** { **counters** [**instance** *number* [**queue** *number*]] | **queue-exhaustion** [**snapshot** *number*] } | **load-balance history** | **overhead** | **packet-profile** | **table** [**arp** | **classify** | **filter** [**access-list** *acl_name*]] }

Syntax Description

access-list *acl_name*	仅清除指定访问列表的命中计数器。
arp	仅清除 ASP ARP 表中的命中计数器。
classify	仅清除 ASP 分类表中的命中计数器。
cluster counter	清除集群计数器。
counters	清除数据路径检测 Snort 计数器。
dispatch	清除调度统计数据。
event	清除控制平面事件统计信息的数据路径。
filter	仅清除 ASP 过滤器表中的命中计数器
flow	清除丢弃的流统计信息。
frame	清除丢弃的帧/数据包统计信息。
inspect-dp ack-passthrough	清除绕过 Snort 检查的空 TCP ACK 数据包的计数器。
inspect-dp egress-optimization	清除出口优化统计信息。
inspect-dp snort	清除数据路径检测 Snort 统计信息。
instance *number*	按实例 ID 清除计数器。
load-balance history	清除每个数据包的 ASP 负载平衡历史并重置自动切换发生的次数
overhead	清除所有 ASP 多处理器开销统计信息。
packet-profile	清除数据包配置文件统计信息。
queue *number*	按实例 ID 和队列 ID 清除计数器。
queue-exhaustion	清除数据路径检测 Snort 队列快照。
snapshot *number*	按快照 ID 清除队列耗尽。

table	清除 ASP ARP 表和 ASP 分类表中的命中计数器。

Command History

版本	修改
6.1	引入了此命令。
6.4	引入了 **clear asp inspect-dp egress-optimization** 命令。
6.5	添加了 **packet-profile** 关键字。
7.0	添加了 **inspect-dp ack-passthrough** 关键字。

示例

以下示例清除所有调度统计信息：

```
> clear asp dispatch
```

Related Commands

命令	Description
show asp	显示 ASP 统计信息。

clear bfd

要清除所有双向转发检测 (BFD) 计数器，请使用 **clear bfd counters** 命令。

clear bfd counters [**ld** *local_discr* | *interface_name* | **ipv4** *ip_address* | **ipv6** *ip_address*]

Syntax Description

ld *local_discr*	（可选）清除指定本地鉴别器 1 - 4294967295 的 BFD 计数器。
interface_name	（可选）清除指定接口的 BFD 计数器。
ipv4 *ip_address*	（可选）清除指定邻居 IPv4 地址的 BFD 计数器。
ipv6 *ip_address*	（可选）清除指定邻居 IPv6 地址的 BFD 计数器。

Command History

版本	修改
6.3	引入了此命令。

示例

以下示例清除所有 BFD 计数器：

```
> clear bfd counters
```

Related Commands

命令	Description
show bfd	显示 BFD 协议信息，包括丢弃的数据包、邻居和映射条目。

clear bgp

要使用硬重新配置或软重新配置重置边界网关协议 (BGP) 连接，请使用 **clear bgp** 命令。

clear bgp {[***** | **external**] [**ipv4 unicast** [*as_number* | *neighbor_address* | **table-map**] | **ipv6 unicast** [*as_number* | *neighbor_address*]] [**soft**] [**in** | **out**] | *as_number* [**soft**] [**in** | **out**] | *neighbor_address* [**soft**] [**in** | **out**] | **table-map**}

Syntax Description

*****	指定将重置所有当前 BGP 会话。
as_number	（可选）将重置所有 BGP 对等会话的自主系统的编号。
external	指定将重置所有外部 BGP 会话。
in	（可选）启动入站重新配置。如果未指定 **in** 和 **out** 关键字，入站和出站会话都会重置。
ipv4 unicast	使用硬/软重新配置来重置 IPv4 地址系列会话的 BGP 连接。
ipv6 unicast	使用硬/软重新配置来重置 IPv6 地址系列会话的 BGP 连接。
neighbor_address	（可选）指定仅重置已标识的 BGP 邻居。此参数的值可以是 IPv4 或 IPv6 地址。
out	（可选）启动入站或出站重新配置。如果未指定 **in** 和 **out** 关键字，入站和出站会话都会重置。
soft	（可选）以强制方式清除慢速对等设备状态，并将其移至原始更新组。
table-map	清除 BGP 路由表中的表映射配置信息。此命令可用于清除配置了 BGP 策略记账功能的流量索引信息。

Command History

版本	修改
6.1	引入了此命令。

使用指南

clear bgp 命令可用于启动硬重置或软重新配置。硬重置会断开并重建指定的对等会话并重建 BGP 路由表。软重新配置使用存储的前缀信息来重新配置并激活 BGP 路由表，无需断开现有对等会话。软重新配置使用存储的更新信息（以使用额外内存存储更新为代价），允许您应用新 BGP 策略而无需中断网络。软重新配置可针对入站或出站会话进行配置。

示例

在以下示例中，所有 BGP 会话都重置：

```
> clear bgp *
```

在以下示例中，针对邻居为 10.100.0.1 的入站会话启动软重新配置，出站会话不受影响：

```
> clear bgp 10.100.0.1 soft in
```

在以下示例中，在 BGP 邻居路由器上启用路由刷新功能，并针对邻居为 172.16.10.2 的入站会话启动软重新配置，出站会话不受影响：

```
> clear bgp 172.16.10.2 in
```

在以下示例中，针对编号 35700 的自主系统中的所有路由器的会话启动硬重置：

```
> clear bgp 35700
```

在以下示例中，针对所有入站 eBGP 对等会话配置软重新配置：

```
> clear bgp external soft in
```

在以下示例中，清除所有出站地址系列 IPv4 组播 eBGP 对等会话：

```
> clear bgp external ipv4 multicast out
```

在以下示例中，针对自主系统 65400 的 IPv4 单播地址系列会话中的 BGP 邻居入站会话启动软重新配置，出站会话不受影响：

```
> clear bgp ipv4 unicast 65400 soft in
```

在以下示例中，针对符号为 65538（asplain 记数法）的 4 字节自主系统的 IPv4 单播地址系列会话中的 BGP 邻居启动硬重置。

```
> clear bgp ipv4 unicast 65538
```

在以下示例中，针对符号为 1.2（asdot 记数法）的 4 字节自主系统的 IPv4 单播地址系列会话中的 BGP 邻居启动硬重置：

```
> clear bgp ipv4 unicast 1.2
```

以下示例清除 IPv4 单播对等会话的表映射：

```
> clear bgp ipv4 unicast table-map
```

clear blocks

要重置数据包缓冲区计数器（例如耗尽条件和历史记录信息），请使用 **clear blocks** 命令。

clear blocks ［**exhaustion** ｛**history** | **snapshot**｝ | **export-failed** | **queue** ［**history** ［**core-local** ［数字］］］］

Syntax Description

core-local [编号]	（可选）清除按应用排队的所有核心的系统缓冲区，或者，如果指定核心编号，则清除特定核心。
exhaustion	（可选）清除耗尽条件。
export-failed	（可选）清除导出失败的计数器。
history	（可选）清除历史记录。
queue	（可选）清除排队的块。
snapshot	（可选）清除快照信息。

Command History

版本	修改
6.1	引入了此命令。

使用指南

将低水印计数器重置为每个池中当前可用的块数。此外，此命令会清除上次缓冲区分配失败时存储的历史记录信息。

示例

以下示例清除块数：

```
> clear blocks
```

Related Commands

命令	Description
blocks	增加为块诊断分配的内存。
show blocks	显示系统缓冲区利用率。

clear capture

要清除捕获缓冲区，请使用 **clear capture** 命令。

clear capture {**/all** | *capture_name*}

Syntax Description

/all	清除所有接口上的数据包。
capture_name	指定数据包捕获的名称。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例展示如何清除捕获缓冲区“example”：

```
> clear capture example
```

Related Commands

命令	Description
capture	启用数据包捕获功能以进行数据包嗅探和网络故障隔离。
show capture	在未指定选项时显示捕获配置。

clear clns

要清除无连接模式网络协议 (CLNP) 信息，请使用 **clear clns** 命令。

clear clns {**is-neighbors** | **neighbors** | **traffic**}

Syntax Description

is-neighbors	清除中间系统邻居路由。
neighbors	清除所有 CLNS 邻居路由。
traffic	清除 CLNS 协议统计信息。

Command History

版本	修改
6.3	引入了此命令。

示例

此示例显示如何清除所有 CLNS 邻居路由：

```
> clear clns neighbors
```

Related Commands

命令	Description
show clns	显示无连接模式网络协议 (CLNP) 网络信息。

clear cluster info

要清除集群统计信息，请使用 **clear cluster info** 命令。

clear cluster info {**flow-mobility counters** | **health details** | **trace** | **transport**}

Syntax Description

flow-mobility counters	清除集群流移动性计数器。
health details	清除集群运行状况信息。
trace	清除集群事件跟踪信息。
transport	清除集群传输统计信息。

Command History

版本	修改
6.1	引入了此命令。

使用指南

要查看集群统计信息，请使用 show cluster info 命令。

示例

以下示例清除集群事件跟踪信息：

```
> clear cluster info trace
```

Related Commands

命令	Description
show cluster info	显示集群统计信息。

clear configure key chain

要删除已配置的密钥链，请使用 **clear configure key chain** 命令。

clear configure key chain*key-chain-name*

Command History

版本	修改
6.4	引入了此命令。

使用指南

使用 **clear configure key chain** 命令删除已配置的密钥链。

示例

以下示例显示如何删除已配置的密钥链。

```
> clear configure key chain CHAIN1
>
```

Related Commands

命令	Description
key chain	为 ospfv2 身份验证配置密钥链。
show key chain	显示已配置的密钥链。
show running key chain	显示当前处于活动状态的密钥链详细信息。

clear conn

要清除特定连接或多个连接，请使用 **clear conn** 命令。

clear conn [**vrf** { *name* | **global** }] { **all** | **protocol** { **tcp** | **udp** | **sctp** } | **address** *ip* [*- ip*] [*netmask mask*] | **port** *port* [*- port*] | **inline-set** *name* | **security-group** { **name** | **tag** } *attribute* } | **user** [*domain_nickname* \ ] *user_name* | **user-group** [*domain_nickname* \\ ] *user_group_name*] | **zone** [*zone_name*] [**data-rate**] }

Syntax Description

address *ip*[*-ip*]	清除具有指定源或目标 IP 地址（IPv4 或 IPv6）的连接。要指定范围，请使用破折号 (-) 分隔各个 IP 地址。例如：10.1.1.1-10.1.1.5
all	清除所有连接（包括到设备的连接）。如果没有 all 关键字，则仅清除通过设备的连接。
inline-set *name*	清除与指定的内联集匹配的连接。
netmask *mask*	（可选）指定要与给定 IP 地址配合使用的子网掩码。
port *port*[*-port*]	清除具有指定源或目标端口的连接。要指定范围，请使用破折号 (-) 分隔各个端口号。例如：1000-2000
protocol {**tcp** | **udp** | **sctp**}	清除指定协议的连接。
security-group {**name** | **tag**} *attribute*	清除具有指定安全组属性的连接。
user [*domain_nickname*\] *user_name*	清除属于指定用户的连接。如果不包含 *domain_nickname* 参数， 系统将清除默认域中用户的连接。
user-group [*domain_nickname*\\] *user_group_name*]	清除属于指定用户组的连接。如果不包含 *domain_nickname* 参数，系统将清除默认域中用户组的连接。
zone [*zone_name*]	清除属于安全区域的连接。
[**vrf** {*name* | **global**}]	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将该命令限制为特定虚拟路由器。指定 **vrf global** 以将命令限制为全局虚拟路由器。如果省略此关键字，则命令适用于所有虚拟路由器。
data-rate	（可选）清除当前存储的最大数据速率。

Command History

版本	修改
6.1	引入了此命令。
6.6	添加了 **vrf** 和 **data-rate** 关键字。

使用指南

更改配置的安全策略后，所有新连接将使用新安全策略。现有连接将继续使用在连接建立时配置的策略。要确保所有连接都使用新策略，需要断开当前连接，以便使用新策略使用 **clear conn** 命令重新连接。可以使用 **clear local-host** 命令清除每台主机的连接，或者使用 **clear xlate** 命令清除使用动态 NAT 的连接。

当设备创建用于允许辅助连接的针孔时，将在 **show conn** 命令输出中显示为不完整的连接。要清除此不完整的连接，请使用 **clear conn** 命令。

注释 此命令不会清除与管理接口的连接；它只能清除与数据接口或诊断接口的管理连接。

示例

以下示例显示如何查看所有连接，然后从 10.10.10.108 清除管理连接：

```
> show conn all
TCP mgmt 10.10.10.108:4168 NP Identity Ifc 10.0.8.112:22, idle 0:00:00,
bytes 3084, flags UOB
> clear conn address 10.10.10.108
```

以下示例显示如何清除存储在扩展内存中的连接最大数据速率：

```
> clear conn data-rate
Released conn extension memory for 10 connection(s)
```

Related Commands

命令	Description
clear local-host	按特定本地主机或所有本地主机清除所有连接。
clear xlate	清除动态 NAT 会话以及使用 NAT 的任何连接。
show conn	显示连接信息。
show local-host	显示本地主机的网络状态。
show xlate	显示 NAT 会话。

clear console-output

要删除当前捕获的控制台输出，请使用 **clear console-output** 命令。

clear console-output

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例展示如何删除当前捕获的控制台输出：

```
> clear console-output
```

Related Commands

命令	Description
show console-output	显示捕获的控制台输出。
show running-config console timeout	显示与设备之间的控制台连接的空闲超时。

clear counters

要清除协议栈计数器，请使用 **clear counters** 命令。

clear counters ［**all** | **summary** | **top** *n*］［**detail**］［**protocol** *protocol_name* ［*counter_name*］］［**threshold** *n*］

Syntax Description

all	（可选）清除所有过滤器详细信息。
counter_name	（可选）按名称指定计数器。使用 **show counters protocol** 命令查看可用的计数器名称。
detail	（可选）清除计数器详细信息。
protocol *protocol_name*	（可选）清除指定协议的计数器。
summary	（可选）清除计数器摘要。
threshold *n*	（可选）清除达到或超过指定阈值的计数器。范围为 1 到 4294967295。
top *n*	（可选）清除达到或超过指定阈值的计数器。范围为 1 到 4294967295。

Command Default

默认为 **clear counters summary detail** 命令。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例展示如何清除协议栈计数器：

```
> clear counters
```

Related Commands

命令	Description
show counters	显示协议栈计数器。

clear cpu profile

要清除 CPU 分析统计信息，请使用 **clear cpu** 命令。

clear cpu profile

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例展示如何删除故障文件：

```
> clear cpu profile
```

Related Commands

命令	Description
show cpu	显示有关 CPU 的信息。
show cpu profile	显示 CPU 分析数据。

clear crashinfo

要删除闪存中崩溃文件的内容，请使用 **clear crashinfo** 命令。

clear crashinfo ［**module** {**0** | **1**}］

Syntax Description

module {**0** |**1**}	（可选）清除插槽 0 或 1 中的模块的崩溃文件。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例展示如何删除故障文件：

```
> clear crashinfo
```

Related Commands

命令	Description
crashinfo force	强制系统崩溃。
crashinfo test	测试系统将故障信息保存到闪存中文件的能力。
show crashinfo	显示存储在闪存中的故障文件的内容。

clear crypto accelerator statistics

要从加密加速器MIB中清除全局和特定于加速器的统计信息，请使用 **clear crypto accelerator statistics** 命令。

clear crypto accelerator statistics

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例在全局配置模式下显示加密加速器统计信息：

```
> clear crypto accelerator statistics
>
```

Related Commands

命令	Description
clear crypto protocol statistics	清除加密加速器 MIB 中的协议特定统计信息。
show crypto accelerator statistics	显示加密加速器 MIB 中的全局统计信息和加速器特定统计信息。
show crypto protocol statistics	显示来自加密加速器 MIB 的协议特定统计信息。

clear crypto ca crls

要清空与指定信任点关联的所有 CRL 的 CRL 缓存要从缓存中清空与信任池关联的所有 CRL，或者要清空所有 CRL 的 CRL 缓存，请在特权 EXEC 模式下使用 **clear crypto ca crls** 命令。

clear crypto ca crls ［**trustpool** | **trustpoint** *trust_point_name*］

Syntax Description

trustpoint *trust_point_name*	信任点的名称。如果不指定名称，此命令将清除系统上所有缓存CRL。如果提供没有信任点名称的信任点关键字，此命令将失败。
trustpool	表示操作应仅应用于与信任池中证书关联的 CRL。

Command History

版本	修改
6.1	引入了此命令。

示例

以下独立示例清除所有 trustpool CRL，清除与 trustpoint123 关联的所有 CRL，并从设备中删除所有缓存的 CRL：

```
> clear crypto ca crl trustpool
> clear crypto ca crl trustpoint trustpoint123
> clear crypto ca crl
```

Related Commands

命令	Description
show crypto ca crl	显示所有缓存 CRL 或指定信任点的缓存 CRL。

clear crypto ca trustpool

要从信任池中删除所有证书，请使用 **clear crypto ca trustpool** 命令。

clear crypto ca trustpool noconfirm

Syntax Description

noconfirm	禁止用户确认提示，此命令将根据请求进行处理。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例清除所有证书：

```
> clear crypto ca trustpool
>
```

Related Commands

命令	Description
crypto ca trustpool export	导出构成 PKI 信任池的证书。
crypto ca trustpool import	导入构成 PKI 信任池的证书。
crypto ca trustpool remove	从信任池中删除一个指定的证书。

clear crypto ikev1

要删除 IPsec IKEv1 SA 或统计信息，请使用 **clear crypto ikev1** 命令。

clear crypto ikev1 {**sa** [*ip_address*] | **stats**}

Syntax Description

sa*ip_address*	清除 SA。要清除所有 IKEv1 SA，请使用此选项而不指定 IP 地址。否则，请指定要清除的 SA 的 IPv4 或 IPv6 地址。
stats	清除 IKEv1 统计信息。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例从 threat defense 设备中删除所有 IPsec IKEv1 统计信息：

```
> clear crypto ikev1 stats
>
```

以下示例删除对等体 IP 地址为 10.86.1.1 的 SA：

```
> clear crypto ikev1 sa 10.86.1.1
>
```

Related Commands

命令	Description
show ipsec sa	显示有关 IPsec SA 的信息，包括计数器、条目、映射名称、对等 IP 地址和主机名。
show running-config crypto	显示整个加密配置，包括 IPsec、加密映射、动态加密映射和 ISAKMP。

clear crypto ikev2

要删除 IPsec IKEv2 SA 或统计信息，请使用 **clear crypto ikev2** 命令。

clear crypto ikev2 {**sa** [*ip_address*] | **stats**}

Syntax Description

sa*ip_address*	清除 SA。要清除所有 IKEv2 SA，请使用此选项而不指定 IP 地址。否则，请指定要清除的 SA 的 IPv4 或 IPv6 地址。
stats	清除 IKEv2 统计信息。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例从 threat defense 设备中删除所有 IPsec IKEv2 统计信息：

```
> clear crypto ikev2 stats
>
```

以下示例删除对等体 IP 地址为 10.86.1.1 的 SA：

```
> clear crypto ikev2 sa 10.86.1.1
>
```

Related Commands

命令	Description
show ipsec sa	显示有关 IPsec SA 的信息，包括计数器、条目、映射名称、对等 IP 地址和主机名。
show running-config crypto	显示整个加密配置，包括 IPsec、加密映射、动态加密映射和 ISAKMP。

clear crypto ipsec sa

要删除 IPsec SA 计数器、条目、加密映射或对等连接，请使用 **clear crypto ipsec sa** 命令。

clear crypto ipsec sa [**counters** | **entry** *ip_address* {**esp** | **ah**} *spi* | **inactive** | **map** *map_name* | **peer** *ip_address*]

Syntax Description

ah	身份验证信头。
counters	清除每个 SA 的所有 IPsec 统计信息。
entry *ip_address*	删除与指定 IP 地址/主机名、协议和 SPI 值匹配的隧道。
esp	加密安全协议。
inactive	清除所有非活动 IPsec SA。
map *map_name*	删除与指定加密映射（通过映射名称识别）关联的所有隧道。
peer *ip_address*	删除通过指定主机名或 IP 地址识别的对等设备的所有 IPsec SA。
spi	确定安全参数索引（十六进制数）。必须是入站 SPI。此命令不支持出站 SPI。

Command History

版本	修改
6.1	引入了此命令。

使用指南

要清除所有 IPsec SA，请使用此命令的不带参数形式。

示例

以下示例从 threat defense中删除所有 IPsec SA：

```
> clear crypto ipsec sa
>
```

以下示例删除对等体 IP 地址为 10.86.1.1 的 SA：

```
> clear crypto ipsec sa peer 10.86.1.1
```

Related Commands

命令	Description
show ipsec sa	显示有关IPsec SA 的信息，包括计数器、条目、映射名称、对等 IP 地址和主机名。

命令	Description
show running-config crypto	显示整个加密配置，包括 IPsec、加密映射、动态加密映射和 ISAKMP。

clear crypto isakmp

要清除 ISAKMP SA 或统计信息，请使用 **clear crypto isakmp** 命令。

clear crypto isakmp ［**sa** | **stats**］

Syntax Description

sa	清除 IKEv1 和 IKEv2 SA。
stats	清除 IKEv1 和 IKEv2 统计信息。

Command History

版本	修改
6.1	引入了此命令。

使用指南

要清除所有 ISAKMP 操作数据，请使用此命令（不带参数）。

示例

以下示例删除所有 ISAKMP SA：

```
> clear crypto isakmp sa
>
```

Related Commands

命令	Description
show isakmp	显示有关 ISAKMP 运行数据的信息。
show running-config crypto	显示整个加密配置，包括 IPsec、加密映射、动态加密映射和 ISAKMP。

clear crypto protocol statistics

要清除加密加速器 MIB 中的协议特定统计信息，请使用 **clear crypto protocol statistics** 命令。

clear crypto protocol statistics 协议

Syntax Description

protocol	指定要清除统计信息的协议的名称。协议选项如下所示： • **all**- 当前支持的所有协议。 • **ikev1**-互联网密钥交换 (IKE) 第 1 版。 • **ikev2**-互联网密钥交换 (IKE) 第 2 版。 • **ipsec**- IP 安全 (IPsec) 阶段 2 协议。 • **other**- 保留以用于新协议。 • **srtp**- 安全 RTP (SRTP) 协议 • **ssh**-安全外壳 (SSH) 协议 • **ssl**-安全套接字层 (SSL) 协议

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例清除所有加密加速器统计信息：

```
> clear crypto protocol statistics all
>
```

Related Commands

命令	Description
clear crypto accelerator statistics	清除加密加速器 MIB 中的全局统计信息和加速器特定统计信息。
show crypto accelerator statistics	显示来自加密加速器MIB的全局统计信息和加速器特定统计信息。
show crypto protocol statistics	显示加密加速器 MIB 中的协议特定统计信息。

clear crypto ssl

要清除 SSL 信息，请使用 **clear crypto ssl** 命令。

clear crypto ssl {**cache** [**all**] | **errors** | **mib** | **objects**}

Syntax Description

cache	清除 SSL 会话缓存中已过期的会话。
all	（可选）清除 SSL 会话缓存中的所有会话和统计信息。
errors	清除 SSL 错误。
mib	清除 SSL MIB 统计信息。
objects	清除 SSL 对象统计信息。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例清除所有 SSL 缓存会话和统计信息：

```
> clear crypto ssl cache all
```

Related Commands

命令	Description
show crypto ssl	显示 SSL 信息。

clear dhcpd

要清除 DHCP 服务器绑定和统计信息，请使用 **clear dhcpd** 命令。

clear dhcpd {**binding** [**all** | *ip_address*] | **statistics**}

Syntax Description

all	（可选）清除所有 dhcpd 绑定。
binding	清除所有客户端地址绑定。
ip_address	（可选）清除指定 IP 地址的绑定。
statistics	清除统计信息计数器。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例展示如何清除 dhcpd 统计信息：

```
> clear dhcpd statistics
```

Related Commands

命令	Description
show dhcpd	显示 DHCP 绑定、统计信息或状态信息。

clear dhcprelay statistics

要清除 DHCP 中继统计信息计数器，请使用 **clear dhcprelay statistics** 命令。

clear dhcprelay statistics

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例展示如何清除 DHCP 中继统计信息：

```
> clear dhcprelay statistics
```

Related Commands

命令	Description
show dhcprelay statistics	显示 DHCP 中继代理统计信息。
show running-config dhcprelay	显示当前 DHCP 中继代理配置。

clear dns

要清除与通过 DNS 请求解析的完全限定域名 (FQDN) 主机关联的 IP 地址，请使用 **clear dns** 命令。

clear dns ［ **host** *fqdn_name* ］ ［ **ipcache** ［ **counters** ］］

Syntax Description

host *fqdn_name*	（可选）指定要清除其 IP 地址的完全限定域名。如果不指定主机，则会清除所有 DNS 解析。
ipcache ［**counters**］	清除通过 DNS 监听获取的 IP 缓存中的所有条目，用于基于策略的直接互联网访问。 指定 **counters** 仅重置缓存中条目的所有命中计数，而不将其删除。

Command History

版本	修改
6.1	引入了此命令。
7.1	添加了 **ipcache** ［**counters**］关键字。

示例

以下示例清除与指定 FQDN 主机关联的 IP 地址：

```
> clear dns host www.example.com
```

以下示例清除 IP 缓存。删除 IP 缓存后，系统使用网络服务对象和对象组中的域名的新 DNS 查询重新填充缓存。在 DNS 查询完成之前，将不再为包含已清除 IP 缓存条目的域名的网络服务组对发往域名的流量进行分类。

```
> clear dns ip-cache
```

Related Commands

命令	Description
show dns hosts	显示特定主机的 DNS 解析。

clear dns-hosts cache

要清除 DNS 缓存，请使用 **clear dns-hosts cache** 命令。

clear dns-hosts cache

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例清除 DNS 缓存：

```
> clear dns-hosts cache
```

Related Commands

命令	Description
show dns-hosts	显示 DNS 缓存。

clear efd-throttle

要从已限制的大流中清除限制并绕过 Snort 检查，请使用 **clear efd-throttle** 命令。

clear efd-throttle { *IPv4_address* | *IPv6_address/prefix* | **all bypass** | **any** { *source_port* { *destination_IPv4_address* | *destination_IPv6_address/prefix* | **any** } | **any** { *destination_IPv4_address* | *destination_IPv6_address/prefix* | **any** { *destination_port* { **tcp bypass** | **udp bypass** } | **any** { **tcp bypass** | **udp bypass** } } } } }

Syntax Description

IPv4_address	清除指定 IPv4 地址（5 元组）的已限制大流。
IPv6_address/prefix	清除指定 IPv6 地址的已限制大流。
all	清除限制并检查所有大流。
bypass	（可选）清除限制并绕过所有大型流的 Snort 检查。
any	• 用作源地址和掩码 0.0.0.0 0.0.0.0 和 ::/0 的缩写 • 用于任何源端口或目的端口。
source_port	清除与指定源端口的连接的限制。
destination_port	清除具有指定目标端口的连接的限制。
tcp	仅清除 TCP 连接的限制。
udp	仅清除 UDP 连接的限制。

Command History

版本	修改
7.2	引入了此命令。

示例

以下示例显示如何清除受限制的大流的限制，并继续对该流进行 Snort 检查：

```
> clear efd-throttle 172.16.77.0 255.255.255.0 1234 172.16.4.0 255.255.255.0 80 tcp
```

以下示例显示如何清除受限制的大流的限制并绕过该流的 Snort 检查：

```
> clear efd-throttle 172.16.77.0 255.255.255.0 1234 172.16.4.0 255.255.255.0 80 tcp bypass
```

以下示例显示如何清除所有受限制的大流的限制，并继续对所有流进行 Snort 检查：

```
> clear efd-throttle all
```

以下示例显示如何清除受限制的大流的限制并绕过该流的 Snort 检查：

```
> clear efd-throttle all bypass
```

clear eigrp events

要清除 EIGRP 事件日志，请使用 **clear eigrp events** 命令。

clear eigrp ［*as_number*］ **events**

Syntax Description

as_number	（可选）指定要清除事件日志的 EIGRP 进程的自主系统编号。由于设备仅支持一个EIGRP路由进程，因此，无需指定自主系统编号（进程ID）。

Command History

版本	修改
6.1	引入了此命令。

使用指南

您可以使用 **show eigrp events** 命令查看 EIGRP 事件日志。

示例

以下示例清除 EIGRP 事件日志：

```
> clear eigrp events
```

Related Commands

命令	Description
show eigrp events	显示 EIGRP 事件日志。

clear eigrp neighbors

要从 EIGRP 邻居表中删除条目，请使用 **clear eigrp neighbors** 命令。

clear eigrp ［*as_number*］ **neighbors** ［*ip_addr* | *if_name*］［**soft**］

Syntax Description

as_number	（可选）指定要删除邻居条目的 EIGRP 流程的自主系统编号。由于设备仅支持一个 EIGRP 路由进程，因此，无需指定自主系统编号 (AS)，即进程 ID。
if_name	（可选）接口的名称。指定接口名称将删除通过该接口获悉的所有邻居表条目。
ip_addr	（可选）要从邻居表删除的邻居的 IP 地址。
soft	导致设备与邻居重新同步但不重置邻接。

Command Default

如果不指定邻居 IP 地址或接口名称，将从邻居表删除所有动态条目。

Command History

版本	修改
6.1	引入了此命令。

使用指南

clear eigrp neighbors 命令不会从邻居表中删除手动定义的邻居。此命令仅删除动态发现的邻居。

您可以使用 **show eigrp neighbors** 命令查看 EIGRP 邻居表。

示例

以下命令从 EIGRP 邻居表删除所有条目：

```
> clear eigrp neighbors
```

以下示例从 EIGRP 邻居表删除通过名为“outside”的接口获悉的所有条目：

```
> clear eigrp neighbors outside
```

Related Commands

命令	Description
show eigrp neighbors	显示 EIGRP 邻居表。

clear eigrp topology

要从 EIGRP 拓扑表中删除条目，请使用 **clear eigrp topology** 命令。

clear eigrp ［*as_number*］ **topology** *ip_addr* ［*mask*］

Syntax Description

as_number	（可选）指定 EIGRP 流程的自主系统编号。由于设备仅支持一个 EIGRP 路由进程，因此，无需指定自主系统编号 (AS)，即进程 ID。
ip_addr	要从拓扑表清除的 IP 地址。
mask	（可选）要应用于 *ip-addr* 参数的网络掩码。

Command History

版本	修改
6.1	引入了此命令。

使用指南

此命令从 EIGRP 拓扑表清除现有 EIGRP 条目。您可以使用 **show eigrp topology** 命令查看拓扑表条目。

示例

以下示例从 EIGRP 拓扑表删除 192.168.1.0 网络中的条目：

```
> clear eigrp topology 192.168.1.0 255.255.255.0
```

Related Commands

命令	Description
show eigrp topology	显示 EIGRP 拓扑表。

clear f - clear z

clear facility-alarm output

要断开输出继电器并清除 ISA 3000 中 LED 的警报状态，请使用 **clear facility-alarm output** 命令

clear facility-alarm output

Command History

版本	修改
6.3	引入了此命令。

使用指南

此命令会断开输出继电器并清除输出LED的警报状态。这会关闭外部报警。但是，此命令不会修复触发外部警报的警报条件：您仍必须解决问题。使用 **show facility-alarm status** 命令确定当前警报条件。

示例

以下示例断开输出继电器并清除输出 LED 的警报状态：

```
> clear facility-alarm output
```

Related Commands

命令	Description
show alarm settings	显示所有全局报警设置。
show environment alarm-contact	显示输入警报触点的状态。
show facility-alarm	显示已触发警报的状态信息。

clear failover statistics

要清除高可用性统计信息计数器，请使用 **clear failover statistics** 命令。

clear failover statistics

Command History

版本	修改
6.1	引入了此命令。

使用指南

此命令清除用 **show failover statistics** 命令显示的统计信息以及 **show failover** 命令输出的“状态故障转移逻辑更新统计信息”部分中的计数器。

示例

以下示例显示如何清除高可用性统计信息计数器：

```
> clear failover statistics
```

Related Commands

命令	Description
show failover	显示有关高可用性配置和操作统计信息的信息。

clear flow-export counters

要将 NetFlow 统计和错误数据的运行时间计数器重置为零，请使用 **clear flow-export counters** 命令。

clear flow-export counters

Command History

版本	修改
6.3	引入了此命令。

示例

以下示例显示如何重置 NetFlow 运行时间计数器：

```
> clear flow-export counters
```

Related Commands

命令	Description
show flow-export counters	显示所有 NetFlow 运行时间计数器。

clear flow-offload

要清除已分流的流的计数器和统计信息，请使用 **clear flow-offload** 命令。

此命令在 Firepower 4100/9300 机箱的 threat defense 上可用。

clear flow-offload statistics

Syntax Description

statistics	将所有分流的数据流的统计信息重置为零。

Command History

版本	修改
6.3	引入了此命令。

示例

以下是清除所有流计数器的示例：

```
> clear flow-offload statistics
```

Related Commands

命令	Description
show flow-offload	显示动态数据流分流计数器、统计信息和信息。
configure flow-offload	启用或禁用动态数据流分流。

clear flow-offload-ipsec

要清除与 IPsec 数据流分流相关的信息，请使用 **clear flow-offload-ipsec** 命令。

clear flow-offload-ipsec statistics

Syntax Description

statistics	清除与IPsec流量分流相关的统计信息。

Command History

版本	修改
7.2	引入了此命令。

示例

以下示例清除所有 IPsec 流分流统计信息。

```
> clear flow-offload-ipsec statistics
```

Related Commands

命令	Description
show flow-offload-ipsec	显示IPsec流分流统计信息和信息。

clear fragment

要清除 IP 分段重组模块的操作数据，请输入 **clear fragment** 命令。

clear fragment {**queue** | **statistics** [*interface_name*]}

Syntax Description

queue	清除 IP 分段重组队列。
statistics *interface_name*	清除 IP 分段重组统计信息。您可以选择指定接口名称，以仅清除该接口的统计信息。否则，将清除所有接口的统计信息。

Command History

版本	修改
6.1	引入了此命令。

使用指南

此命令清除当前在队列中等待重组的分段（如果输入了 **queue** 关键字），或者清除所有 IP 分段重组统计信息（如果输入了 **statistics** 关键字）。统计信息即为计数器，可显示成功重组了多少个分段链，有多少分段链重组失败，以及由于缓冲区溢出而造成超过最大分段大小的次数。

示例

以下示例展示如何清除 IP 分段重组模块的运行数据：

```
> clear fragment queue
```

Related Commands

命令	Description
show fragment	显示 IP 分段重组模块的运行数据。
show running-config fragment	显示 IP 分段重组配置。

clear gc

要删除垃圾收集 (GC) 流程统计信息，请使用 **clear gc** 命令。

clear gc

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例展示如何删除 GC 流程统计信息：

```
> clear gc
```

Related Commands

命令	Description
show gc	显示 GC 流程统计信息。

clear igmp

要清除所有 IGMP 计数器、组缓存和流量，请使用 **clear igmp** 命令。

clear igmp {**counters** [*if_name*] | **group** [**interface** *name*] | **traffic**}

Syntax Description

counters [*if_name*]	清除IGMP统计计数器。您可以选择指定接口名称，以仅清除该接口的计数器。
group [**interface** 名称]	删除IGMP组缓存条目。您可以选择指定接口名称，以仅删除与该接口关联的组。 此命令不会清除静态配置的组。
traffic	清除流量计数器。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例清除 IGMP 统计信息计数器：

```
> clear igmp counters
```

以下示例展示如何从 IGMP 组缓存清除所有发现的 IGMP 组：

```
> clear igmp group
```

以下示例清除 IGMP 统计信息流量计数器：

```
> clear igmp traffic
```

Related Commands

命令	Description
show igmp	显示 IGMP 信息。

clear ikev1

要删除 IPsec IKEv1 SA 或统计信息，请使用 **clear ikev1** 命令。

clear ikev1 {**sa** [*ip_address*] | **stats**}

Syntax Description

sa*ip_address*	清除 SA。要清除所有 IKEv1 SA，请使用此选项而不指定 IP 地址。否则，请指定要清除的 SA 的 IPv4 或 IPv6 地址。
stats	清除 IKEv1 统计信息。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例从 threat defense 设备中删除所有 IPsec IKEv1 统计信息：

```
> clear ikev1 stats
>
```

以下示例删除对等体 IP 地址为 10.86.1.1 的 SA：

```
> clear ikev1 sa 10.86.1.1
>
```

Related Commands

命令	Description
show ipsec sa	显示有关 IPsec SA 的信息，包括计数器、条目、映射名称、对等 IP 地址和主机名。
show running-config crypto	显示整个加密配置，包括 IPsec、加密映射、动态加密映射和 ISAKMP。

clear ikev2

要删除 IPsec IKEv2 SA 或统计信息，请使用 **clear ikev2** 命令。

clear ikev2 {**sa** [*ip_address*] | **stats**}

Syntax Description

sa*ip_address*	清除 SA。要清除所有 IKEv2 SA，请使用此选项而不指定 IP 地址。否则，请指定要清除的 SA 的 IPv4 或 IPv6 地址。
stats	清除 IKEv2 统计信息。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例从 threat defense 设备中删除所有 IPsec IKEv2 统计信息：

```
> clear ikev2 stats
>
```

以下示例删除对等体 IP 地址为 10.86.1.1 的 SA：

```
> clear ikev2 sa 10.86.1.1
>
```

Related Commands

命令	Description
show ipsec sa	显示有关 IPsec SA 的信息，包括计数器、条目、映射名称、对等 IP 地址和主机名。
show running-config crypto	显示整个加密配置，包括 IPsec、加密映射、动态加密映射和 ISAKMP。

clear interface

要清除接口统计信息，请使用 **clear interface** 命令。

clear interface ［*physical_interface*［**.***subinterface*］ ｜ *interface_name*］

Syntax Description

interface_name	（可选）标识接口 ID。
physical_interface	（可选）标识接口 ID，例如 **gigabit**ethernet0/1。
subinterface	（可选）识别一个介于 1 到 4294967293 之间整数，用以指定逻辑子接口。

Command Default

默认情况下，此命令清除所有接口统计信息。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例清除所有接口统计信息：

```
> clear interface
```

Related Commands

命令	Description
show interface	显示接口的运行时间状态和统计信息。
show running-config interface	显示接口配置。

clear ip

要清除某些传统功能的统计信息，请使用 **clear ip** 命令。

clear ip ｛**audit count** ［**global**］ | **verify statistics**｝［**interface** *interface_name*］

Syntax Description

audit count［**global**］	清除审核策略的签名匹配计数。如果不指定 **interface** 关键字，则会全局清除所有签名的计数。您可以选择包含 **global** 关键字来明确指定此项（不能同时指定全局和接口）。
interface *interface_name*	（可选）仅清除指定接口的统计信息。
verify statistics	清除单播逆向转发 (RPF) 丢弃的数据包数。

Command History

版本	修改
6.1	引入了此命令。

使用指南

这些功能通常不会启用，因此通常没有要清除的统计信息。

示例

以下示例清除所有接口的 IP 审核数：

```
> clear ip audit count
```

Related Commands

命令	Description
show ip audit count	显示单播 RPF 统计信息。
show ip verify statistics	显示单播 RPF 统计信息。
show running-config ip audit name	显示 **ip audit name** 命令的配置。除 **name**外，您可以检查 **interface** 和 **signature** 配置。
show running-config ip verify reverse-path	显示 **ip verify reverse-path** 配置。

clear ipsec sa

要删除 IPsec SA 计数器、条目、加密映射或对等连接，请使用 **clear ipsec sa** 命令。

clear ipsec sa [**counters** | **entry** *ip_address* {**esp** | **ah**} *spi* | **inactive** | **map** *map_name* | **peer** *ip_address*]

Syntax Description

ah	身份验证信头。
counters	清除每个 SA 的所有 IPsec 统计信息。
entry *ip_address*	删除与指定 IP 地址/主机名、协议和 SPI 值匹配的隧道。
esp	加密安全协议。
inactive	清除所有非活动 IPsec SA。
map *map_name*	删除与指定加密映射（通过映射名称识别）关联的所有隧道。
peer *ip_address*	删除通过指定主机名或 IP 地址识别的对等设备的所有 IPsec SA。
spi	确定安全参数索引（十六进制数）。必须是入站 SPI。此命令不支持出站 SPI。

Command History

版本	修改
6.1	引入了此命令。

使用指南

要清除所有 IPsec SA，请使用此命令的不带参数形式。

示例

以下示例在全局配置模式下从 threat defense删除所有 IPsec SA：

```
> clear ipsec sa
>
```

以下示例在全局配置模式下删除具有与 10.86.1.1 对等的 IP 地址的 SA：

```
> clear ipsec sa peer 10.86.1.1
```

Related Commands

命令	Description
show ipsec sa	显示有关IPsec SA 的信息，包括计数器、条目、映射名称、对等 IP 地址和主机名。

命令	Description
show running-config crypto	显示整个加密配置，包括 IPsec、加密映射、动态加密映射和 ISAKMP。

clear ipv6 dhcp

要清除 DHCPv6 统计信息，请使用 **clear ipv6 dhcp** 命令。

clear ipv6 dhcp {**client** [**pd**] | **interface** *interface_name* | **server**} **statistics**

Syntax Description

client [**pd**]	清除 DHCPv6 客户端统计信息。添加 **pd** 关键字以清除前缀委派客户端统计信息。
interface *interface_name*	清除指定接口的 DHCPv6 统计信息。
server	清除 DHCPv6 服务器统计信息。

Command History

版本	修改
6.2.1	引入了此命令。

示例

以下示例清除 DHCPv6 客户端统计信息：

```
> clear ipv6 dhcp client statistics
```

Related Commands

命令	Description
show ipv6 dhcp	显示 DHCPv6 统计信息。

clear ipv6 dhcprelay

要清除 IPv6 DHCP 中继绑定条目和统计信息，请使用 **clear ipv6 dhcprelay** 命令。

clear ipv6 dhcprelay {**binding** [*ip_address*] | **statistics**}

Syntax Description

binding	清除 IPv6 DHCP 中继绑定条目。
ip_address	（可选）指定 DHCP 中继绑定的 IPv6 地址。如果指定 IP 地址，将仅清除与指定 IP 地址关联的中继绑定条目。
statistics	清除 IPv6 DHCP 中继代理统计信息。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例展示如何清除 IPv6 DHCP 中继绑定的统计信息：

```
> clear ipv6 dhcprelay binding
>
```

以下示例展示如何清除 IPv6 DHCP 中继代理的统计信息：

```
> clear ipv6 dhcprelay statistics
```

Related Commands

命令	Description
show ipv6 dhcprelay binding	显示中继代理创建的中继绑定条目。
show ipv6 dhcprelay statistics	显示 IPv6 DHCP 中继代理信息。

clear ipv6 mld traffic

要清除并重置 IPv6 组播侦听程序发现 (MLD) 流量计数器，请使用 **clear ipv6 mld traffic** 命令。

clear ipv6 mld traffic

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例展示如何清除 IPv6 MLD 的流量计数器：

```
> clear ipv6 mld traffic
>
```

Related Commands

命令	Description
show ipv6 mld traffic	显示 IPv6 MLD 流量计数器。

clear ipv6 neighbors

要清除 IPv6 邻居发现缓存，请使用 **clear ipv6 neighbors** 命令。

clear ipv6 neighbors

Command History

版本	修改
6.1	引入了此命令。

使用指南

此命令从缓存中删除所有发现的 IPv6 邻居，但不会删除静态条目。

示例

以下示例删除 IPv6 邻居发现缓存中除静态条目以外的所有条目：

```
> clear ipv6 neighbors
>
```

Related Commands

命令	Description
show ipv6 neighbor	显示 IPv6 邻居缓存信息。

clear ipv6 ospf

要清除 OSPFv3 路由参数，请使用 **clear ipv6 ospf** 命令。

clear ipv6 ［*process_id*］［**counters**］［**events**］［**force-spf**］［**process**］［**redistribution**］［**traffic**］

Syntax Description

counters	重置 OSPF 进程计数器。
events	清除 OSPF 事件日志。
force-ospf	清除 OSPF 进程的 SPF。
process	重置 OSPFv3 进程。
process_id	清除流程 ID 号。有效值范围为 1 到 65535。
redistribution	清除 OSPFv3 路由重分布。
traffic	清除与流量相关的统计信息。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例展示如何清除所有 OSPFv3 路由重分布：

```
> clear ipv6 ospf redistribution
>
```

Related Commands

命令	Description
show running-config ipv6 router	显示 OSPFv3 进程的运行配置。

clear ipv6 prefix-list

要清除路由 IPv6 前缀列表，请使用 **clear ipv6 prefix-list** 命令。

clear ipv6 prefix-list ［*name*］

Syntax Description

name	清除已命名的 IPv6 前缀列表。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例显示如何清除 list1 IPv6 前缀列表：

```
> clear ipv6 prefix-list list1
>
```

Related Commands

命令	Description
show running-config ipv6 prefix-list	显示 IPv6 前缀列表的运行配置。

clear ipv6 route

要从 IPv6 路由表中删除路由，请使用 clear ipv6 route 命令。

clear ipv6 route ［**management-only**］｛**all** | *ipv6-prefix/prefix-length*｝

Syntax Description

management-only	仅清除 IPv6 管理路由表。
ipv6-prefix/prefix-length	清除 IPv6 前缀的路由。
all	清除所有 IPv6 路由。

Command History

版本	修改
6.1	引入了此命令。

使用指南

clear ipv6 route 命令与 **clear ip route** 命令类似，不同之处在于它是 IPv6 特定的命令。

此外，还会清除每个目标的最大传输单位 (MTU) 缓存。

示例

以下示例删除 2001:0DB8::/35 的 IPv6 路由：

```
> clear ipv6 route 2001:0DB8::/35
```

Related Commands

命令	Description
show ipv6 route	显示 IPv6 路由。

clear ipv6 traffic

要重置 IPv6 流量计数器，请使用 **clear ipv6 traffic** 命令。

clear ipv6 traffic

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用此命令将重置 **show ipv6 traffic** 命令输出中的计数器。

示例

以下示例重置 IPv6 流量计数器。

```
> clear ipv6 traffic
>
```

Related Commands

命令	Description
show ipv6 traffic	显示 IPv6 流量统计信息。

clear isakmp

要清除 ISAKMP SA 或统计信息，请使用 **clear isakmp** 命令。

clear isakmp ［**sa** | **stats**］

Syntax Description

sa	（可选）清除 IKEv1 和 IKEv2 SA。
stats	（可选）清除 IKEv1 和 IKEv2 统计信息。

Command History

版本	修改
6.1	引入了此命令。

使用指南

要清除所有 ISAKMP 操作数据，请使用此命令（不带参数）。

示例

以下示例删除所有 ISAKMP SA：

```
> clear isakmp sa
>
```

Related Commands

命令	Description
show isakmp	显示有关 ISAKMP 运行数据的信息。
show running-config crypto	显示整个加密配置，包括 IPsec、加密映射、动态加密映射和 ISAKMP。

clear isis

要清除 IS-IS 数据结构，请使用 **clear isis** 命令。

clear isis {***** | **lspfull** | **rib redistribution** [**level-1** | **level-2**] [*network_prefix*] [*network_mask*]}

Syntax Description

*****	清除所有 IS-IS 数据结构。
level-1	（可选）从重新分发缓存中清除 1 级 IS-IS 重新分发的前缀。
level-2	（可选）从重新分发缓存中清除第 2 级 IS-IS 重新分发的前缀。
lspfull	清除 IS-IS LSPFULL 状态。
network_mask	（可选）要从 RIB 中清除的特定网络前缀的网络掩码的 ABCD 格式的网络ID。如果不为前缀提供网络掩码，则将使用前缀的主网作为网络掩码。
network_prefix	（可选）要从重新分发路由信息库 (RIB) 中清除的特定网络前缀的 ABCD 格式的网络 ID。如果不为前缀提供网络掩码，则将使用前缀的主网作为网络掩码。
rib redistribution	清除 IS-IS 重新分发缓存中的前缀。

Command History

版本	修改
6.3	引入了此命令。

使用指南

如果链路状态 PDU (LSP) 由于重新分发的路由过多而变满，请在解决问题后使用 **clear isis lspfull** 命令清除状态。

我们建议您仅在出现软件错误后，思科技术支持中心代表要求您执行故障排除时才使用 **clear isis rib** 命令。

示例

以下示例清除 LSPFULL 状态：

```
> clear isis lspfull
```

以下示例从 IP 本地重新分发缓存中清除网络前缀 10.1.0.0：

```
> clear isis rib redistribution 10.1.0.0 255.255.0.0
```

Related Commands

命令	Description
show clns	显示 CLNS 特定信息。
show isis	显示 IS-IS 信息。
show route isis	显示 IS-IS 路由。

clear kernel cgroup-controller

要清除内核的 cgroup 控制器统计信息，请使用 **clear kernel cgroup-controller** 命令。

clear kernel cgroup-controller ［**cpu** | **memory**］

Syntax Description

cpu	（可选）清除 cpu/cpuacct 控制器统计信息。
memory	（可选）清除内存控制器统计信息。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例显示如何清除 cgroup-controller 统计信息：

```
> clear kernel cgroup-controller
```

Related Commands

命令	Description
show kernel cgroup-controller	显示 cgroup 控制器统计信息。

clear lacp

要清除 EtherChannel LACP 端口通道统计信息，请使用 **clear lacp** 命令。

clear lacp ［*channel_group_number*］

Syntax Description

channel_group_number	（可选。）按编号（1 到 48）清除信道组信息。

Command Default

如果不指定编号，则将清除所有端口通道的统计信息。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例显示如何清除端口通道统计信息：

```
> clear lacp 12
```

Related Commands

命令	Description
show lacp	显示端口通道信息。

clear lisp eid

要清除 Lisp EID 表，请使用 **clear list eid** 命令。

clear lisp eid ［*ip_address*］

Syntax Description

ip_address	从 EID 表中删除指定的 IP 地址。

Command History

版本	修改
6.2	引入了此命令。

使用指南

设备维护着一个将 EID 和站点 ID 相关联的 EID 表。 **clear lisp eid** 命令会清除表中的 EID 条目。

Related Commands

命令	Description
clear cluster info flow-mobility counters	清除流移动性计数器。
show cluster info flow-mobility counters	显示流移动性计数器。
show conn	显示受 LISP 流移动性影响的流量。
show lisp eid	显示 EID 表。

clear local-host (Deprecated)

要重新初始化每客户端运行时状态，例如连接限制和初始化限制，请使用 **clear local-host** 命令。

clear local-host ［*hostname* ｜ *ip_address*］［**all**］［**zone**］

Syntax Description

all	（可选）清除所有连接，包括流向设备的流量。如果没有 **all** 关键字，则只会清除通过设备的流量。
hostname or *ip_address*	（可选）指定本地主机名或 IPv4 或 IPv6 地址。
zone	（可选）清除流量区域中的所有连接。

Command Default

清除所有通过设备的流量的运行时状态。

Command History

版本	修改
6.1	引入了此命令。
7.0	此命令已弃用。使用 **clear conn address** 命令清除与本地地址的连接。

使用指南

更改配置的安全策略后，所有新连接将使用新安全策略。现有连接将继续使用在连接建立时配置的策略。要确保所有连接都使用新策略，需要断开当前连接，以便使用新策略使用 **clear local-host** 命令重新连接。可以使用 **clear conn** 命令实现更精细的连接清理，或者使用 **clear xlate** 命令清除使用动态 NAT 的连接。

clear local-host 命令根据主机许可证上限释放主机。输入 **show local-host** 命令可以查看计入许可证上限的主机数量。

示例

以下示例清除主机 10.1.1.15 的运行时状态及关联连接：

```
> clear local-host 10.1.1.15
```

Related Commands

命令	Description
clear conn	终止处于任何状态的连接。
clear xlate	清除动态 NAT 会话以及使用 NAT 的任何连接。
show local-host	显示本地主机的网络状态。

clear logging

要清除日志记录缓冲区，请使用 **clear logging** 命令。

clear logging {**buffer** | **counter** 选项 | **queue bufferwrap** | **unified-client**}

Syntax Description

buffer	清除内部日志记录缓冲区。
counter *destination*	清除指定日志记录目标的计数器和统计信息。指定 **all** 以清除所有日志记录目标的统计信息。或者，您可以指定以下选项之一，将操作限制为该目标：**buffer**、 **console**、 **mail**、 **monitor**、 **trap**。
queue bufferwrap	清除已保存的 FTP 和闪存日志记录缓冲区队列。
unified-client	从统一日志记录客户端 loggerD 清除日志记录统计信息。

Command History

版本	修改
6.1	引入了此命令。
6.3	添加了 **unified-client** 关键字。
6.6	添加了 **counter** 关键字。

示例

以下示例展示如何清除日志缓冲区的内容：

```
> clear logging buffer
```

以下示例展示如何清除保存的日志缓冲区的内容：

```
> clear logging queue bufferwrap
```

以下示例显示如何清除 loggerD 服务的统计信息：

```
> clear logging unified-client
```

Related Commands

命令	Description
logging savelog	指定可选的闪存文件名。
show logging	显示日志记录信息。

clear mac-address-table

要清除动态 MAC 地址表条目，请使用 **clear mac-address-table** 命令。

clear mac-address-table ［*interface_name*］

Syntax Description

interface_name	（可选）清除选定接口的 MAC 地址表条目。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例清除动态 MAC 地址表条目：

```
> clear mac-address-table
```

Related Commands

命令	Description
show mac-address-table	显示 MAC 地址表条目。

clear memory

要清除内存工具的队列和统计信息，请使用 **clear memory** 命令。

clear memory {**delayed-free-poisoner** | **profile** [**peak**] | **tracking**}

Syntax Description

delayed-free-poisoner	将延迟的可用内存毒化工具队列中保留的所有内存返回到系统，而不进行验证，并清除相关的统计计数器。使用 **memory delayed-free-poisoner enable** 命令启用此功能。
profile [**peak**]	清除内存分析功能保留的缓冲区。包括可选 **peak** 关键字，以清除峰值内存缓冲区的内容。 在清除配置文件缓冲区之前，使用 **no memory profile enable** 命令停止内存分析。
tracking	清除 **memory tracking enable** 命令收集的内存跟踪信息。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例清除 delayed free-memory poisoner 工具队列和统计信息：

```
> clear memory delayed-free-poisoner
```

Related Commands

命令	Description
memory	启用各种内存工具。
show memory delayed-free-poisoner	显示 delayed free-memory poisoner 工具队列使用摘要。
show memory profile	显示内存分析结果。
show memory tracking	显示内存分析结果。

clear mfib counters

要清除组播转发信息库 (MFIB) 路由器数据包计数器，请使用 **clear mfib counters** 命令。

clear mfib {**cluster-stats** | **counters** [*source_or_group* [*source*]]}

Syntax Description

cluster-stats	清除 MFIB 集群同步统计信息。
count	清除 MFIB 路由和数据包计数数据。使用不带参数的 **count** 时，将清除所有路由的路由计数器。
source_or_group [*group*]	（可选）源或组 IPv4、IPv6 或名称。如果同时指定两者，请先指定源。源地址为单播地址。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例清除所有 MFIB 路由器数据包计数器：

```
> clear mfib counters
```

Related Commands

命令	Description
show mfib	显示 MFIB 路由和数据包计数数据。

clear nat counters

要清除 NAT 计数器，请使用 clear nat counters 命令。

clear nat counters [**interface** *name*] [*ip_addr mask* | {**object** | **object-group**} *name*] [**translated** [**interface** *name*] [*ip_addr mask* | {**object** | **object-group**} *name*]]

Syntax Description

interface *name*	（可选）指定源或目的（转换）接口。
ip_addr mask	（可选）指定 IP 地址和子网掩码。
object *name*	（可选）指定网络对象或服务对象。
object-group *name*	（可选）指定网络对象组
translated	（可选）指定转换参数。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例展示如何清除 NAT 策略计数器：

```
> clear nat counters
```

Related Commands

命令	Description
show nat	显示协议栈计数器。

clear object

要清除网络服务对象的命中计数，请使用 **clear object** 命令。

clear object [**id** *object_name* | **network-service**]

Syntax Description

id *name*	（可选）清除指定网络服务对象的计数器。大小写很重要。例如，“object-name”与“Object-Name”不匹配。
network-service	（可选。）清除所有网络服务对象的计数器。此操作与在 命令中不指定参数所获得的操作相同。

Command Default

如果没有参数，系统将清除所有对象命中计数。

Command History

版本	修改
7.1	引入了此命令。

示例

以下示例清除所有对象的命中计数。

```
> clear object
```

Related Commands

命令	Description
show object	显示网络服务对象和其命中计数。

clear object-group

要清除网络 或网络服务 对象组中对象的命中计数，请使用 **show object-group** 命令。

clear object-group ［ *object_group_name* ］

Syntax Description

object_group_name	应清除其计数器的对象组的名称。如果不指定名称，则所有对象组的计数器都将被清除。

Command History

版本	修改
6.1	引入了此命令。
7.1	此命令已扩展为使用网络服务对象。

示例

以下示例显示如何清除名为 “Anet” 的对象组的命中数：

```
> clear object-group Anet
```

Related Commands

命令	Description
show object-group	显示对象组信息。

clear ospf

要清除 OSPF 流程信息，请使用 **clear ospf** 命令。

clear ospf ［**vrf** *name* | **all**］ {**counters** ［**neighbor** *interface*］ | **events** | **force-spf** | **process /noconfirm** | **redistribution** | **traffic**}

Syntax Description

counters	清除 OSPF 计数器。
neighbor *interface*	（可选）仅清除该邻居的统计信息。
events	清除 OSPF 事件日志。
force-spf	清除增量 SPF 统计信息。
process /noconfirm	重新启动 OSPF 路由流程。
redistribution	清除 OSPF 路由重新分发统计信息。
traffic	清除与 OSPF 流量相关的统计信息。
［**vrf** *name*	**all**］	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将该命令限制为特定虚拟路由器。如果您希望 命令影响所有虚拟路由器，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则 命令适用于全局 VRF 虚拟路由器。

Command History

版本	修改
6.1	引入了此命令。
6.6	添加了 ［**vrf** *name*	**all**］ 关键字。

使用指南

此命令不会删除配置的任何部分，只会清除统计信息。

示例

以下示例展示如何清除所有 OSPF 邻居计数器：

```
> clear ospf counters
```

Related Commands

命令	Description
show ospf	显示运行配置中的所有 OSPF 信息。

clear packet-debugs

要从数据库中删除调试日志，请使用 **clear packet-debugs** 命令。

clear packet-debugs

Command History

版本	修改
6.4	引入了此命令。
6.5	**clear packet debugs** 命令已更改为 **clear packet-debugs**。

使用指南

使用 **clear packet-debugs** 命令从数据库中删除所有调试日志。

示例

以下示例显示如何删除调试日志数据库中存储的所有调试日志。

```
> clear packet-debugs
```

Related Commands

命令	Description
debug packet-start	开始将调试日志写入数据库。

clear packet-tracer

要删除持久性数据包跟踪器，请使用 **clear packet-tracer** 命令。

clear packet-tracer

Command History

版本	修改
6.3	引入了此命令。

使用指南

持久性数据包跟踪器是在 **packet-tracer** 命令中使用 **persist** 关键字配置的那些。

示例

以下示例显示如何删除所有持久性数据包跟踪器。

```
> clear packet-tracer
>
```

Related Commands

命令	Description
packet-tracer	配置数据包跟踪器。

clear path-monitoring

要清除接口上的路径监控设置，请使用 **clear path-monitoring** 命令。

clear path-monitoring ［ **interface** *name* ］

Syntax Description

Interface *name*	删除在指定接口上配置的路径监控设置。

Command History

版本	修改
7.2	引入了此命令。

示例

以下示例清除 *outside1* 接口上的路径监控设置：

```
> clear path-montoring outside1
```

Related Commands

命令	Description
show path-monitoring	显示路径监控指标信息。

clear pclu

要清除 PC 逻辑更新统计信息，请使用 **clear pclu** 命令。

clear pclu

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例清除 PC 信息：

```
> clear pclu
```

Related Commands

命令	Description
show pclu	显示 PCLU 信息。

clear pim

要清除 PIM 流量计数器和映射，请使用 **clear pim** 命令。

clear pim {**counters** | **group-map** [*rp-address*] | **reset** | **topology** [*group*]}

Syntax Description

counters	清除 PIM 流量计数器。
group-map [*rp-address*]	从 RP 映射缓存中删除组到交汇点 (RP) 映射条目。您可以选择指定汇聚点的名称，以仅清除该 RP 的条目。名称可以是： • RP 的名称，如域名系统 (DNS) 主机表中所定义。 • RP 的 IP 地址。这是采用四点分十进制符号的组播 IP 地址。
reset	通过重置强制 MRIB 同步。此命令会从拓扑表中清除所有信息并重置 MRIB 连接。您可以使用此选项在 PIM 拓扑表和 MRIB 数据库之间同步状态。
topology [*group*]	从 PIM 拓扑表中清除现有 PIM 路由。会保留从 MRIB 表获得的信息（例如，IGMP 本地成员身份）。可选择性地指定要从拓扑表中删除的组播组地址或名称。名称可以是以下其中一项： • 组播组的名称，如 DNS 主机表中所定义。 • 组播组的 IPv4 或 IPV6 地址。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例清除 PIM 流量计数器：

```
> clear pim counters
```

以下示例删除位于 23.23.23.2 RP 地址的组 RP 映射条目：

```
> show pim group-map

Group Range         Proto Client Groups RP address      Info
224.0.1.39/32*      DM    static 0      0.0.0.0
224.0.1.40/32*      DM    static 0      0.0.0.0
224.0.0.0/24*       L-Localstatic 1      0.0.0.0
232.0.0.0/8*        SSM   config 0      0.0.0.0
224.0.0.0/4*        SM    config 0      9.9.9.9         RPF: ,0.0.0.0
224.0.0.0/4         SM    BSR    0      23.23.23.2      RPF: Gi0/3,23.23.23.2
> clear pim group-map 23.23.23.2
```

```
> show pim group-map
Group Range          Proto Client Groups RP address      Info
224.0.1.39/32*       DM    static 0      0.0.0.0
224.0.1.40/32*       DM    static 0      0.0.0.0
224.0.0.0/24*        L-Localstatic 1      0.0.0.0
232.0.0.0/8*         SSM   config 0      0.0.0.0
224.0.0.0/4*         SM    config 0      9.9.9.9         RPF: ,0.0.0.0
224.0.0.0/4          SM    static 0      0.0.0.0         RPF: ,0.0.0.0
```

Related Commands

命令	Description
show pim	显示 PIM 流量信息。

clear prefix-list

要重置前缀列表条目的命中计数，请使用 **clear prefix-list** 命令。

clear prefix-list ［*prefix_list_name*］

Syntax Description

prefix_list_name	（可选）要从中清除命中计数的前缀列表的名称。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例显示如何从名为 first_list 的列表中清除前缀列表信息：

```
> clear prefix-list first_list
>
```

Related Commands

命令	Description
show prefix-list	显示有关前缀列表或前缀列表条目的信息。

clear priority-queue statistics

要清除接口或所有已配置接口的优先级队列统计信息计数器，请使用 **clear priority-queue statistics** 命令

clear priority-queue statistics *interface_name*

Syntax Description

interface_name	（可选）清除指定接口的优先级队列统计信息。

Command History

版本	修改
6.3	引入了此命令。

示例

以下示例清除所有接口的优先级队列统计信息。

```
> clear priority-queue statistics
```

Related Commands

命令	Description
show priority-queue statistics	显示指定接口或所有接口的优先级队列统计信息。

clear process

要清除 threat defense 设备上运行的指定流程的统计信息，请使用 clear process 命令。

clear process {**cpu-hog** | **internals**}

Syntax Description

cpu-hog	清除 CPU 占用统计信息。
internals	清除流程内部统计信息。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例展示如何清除 CPU 占用统计信息：

```
> clear process cpu-hog
```

Related Commands

命令	Description
cpu hog granular-detection	触发实时 CPU 占用检测信息。
show processes	显示正在 threat defense 上运行的流程的列表。

clear resource usage

要清除资源使用情况统计信息，请使用 **clear resource usage** 命令。

clear resource usage [**detail** | **resource** {[**rate**] *resource_name* | **all**}]

Syntax Description

detail	清除所有资源使用情况详细信息。
resource [**rate**] *resource_name*	清除特定资源的使用统计信息。为所有资源指定 **all**（默认值）。指定 **rate** 将清除资源的使用率。按使用率衡量的资源包括 **conns**、**inspects**和 **syslogs**。对于这些资源类型，必须指定 **rate** 关键字。conns 资源也可以按并发连接数来测量；要查看每秒连接数，必须使用 **rate** 关键字。 资源包括以下类型： • **Conns**—任意两台主机之间的 TCP 或 UDP 连接数，包括一台主机和多台其他主机之间的连接。 • **Hosts**- 可以通过设备连接的主机。 • **IPSec**- 通过设备连接的 IPSec 管理隧道。 • **Mac-addresses**- MAC 地址表中允许的 MAC 地址数量。 • **Routes**-路由表条目。 • **SSH**-SSH 会话。 • **Storage**-情景目录的存储限制 (以 MB 为单位)。 • **Telnet**-Telnet 会话。 • **VPN**- VPN 资源。 • **Xlates**—NAT 转换。

Command Default

默认资源名称为 **all**（清除所有资源类型）。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例清除系统范围的使用统计信息：

```
> clear resource usage resource all
```

Related Commands

命令	Description
show resource types	显示资源类型列表。
show resource usage	显示设备的资源使用情况。

clear route

要从路由表中删除动态获知的路由，请使用 **clear route** 命令。

clear route ［**vrf** *name* | **all**］ ［**management-only**］ ［**all** | *ip_address*［*ip_mask_or_prefix*］］

Syntax Description

all	指定要删除的所有已获知的路由。
ip_address mask_or_prefix	要删除的路由的 IPv4 或 IPv6 目的地址和掩码或前缀。如果不指定路由，则会删除所有动态获知的路由。
management-only	（可选）清除管理路由表。您可以指定目的地址以清除特定管理路由。
［**vrf** *name*	**all**］	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将该命令限制为特定虚拟路由器。如果您希望 命令影响所有虚拟路由器，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则 命令适用于全局 VRF 虚拟路由器。

Command History

版本	修改
6.1	引入了此命令。
6.6	添加了 ［**vrf** *name*	**all**］ 关键字。
7.1	从版本 7.1 开始，对于属于高可用性组或集群的设备，此命令仅在主用或控制设备上可用。命令会清除 HA 组或集群中所有设备的路由。在以前的版本中， 命令仅清除运行设备上的路由。

示例

以下示例展示如何删除所有动态获知的路由。

```
> clear route
```

Related Commands

命令	Description
show route	显示路由信息。

clear rule hits

要清除访问控制策略和预过滤器策略的所有评估规则的命中信息并将其重置为零，请使用 **clear rule hits** 命令。

clear rule hits ［*ID*］

Syntax Description

ID	（可选）规则的 ID。包含此参数将仅清除指定规则的规则命中信息。 使用 **show access-list** 命令标识规则 ID。

Command Default

如果不指定规则 ID，则所有规则的规则命中信息都将被清除并重置为零。

注释 使用此命令时请谨慎操作，因为此操作不可逆。

Command History

版本	修改
6.4	引入了此命令。

使用指南

规则命中信息仅涵盖访问控制规则和预过滤器规则。

示例

以下是清除所有规则命中信息的示例：

```
> clear rule hits
```

Related Commands

命令	Description
show rule hits	显示访问控制策略和预过滤器策略的所有评估规则的规则命中信息。
show cluster rule hits	以汇总格式显示来自集群所有节点的访问控制策略和预过滤器策略的所有评估规则命中信息。
cluster exec show rule hits	以隔离的格式显示集群中每个节点的访问控制策略和预过滤器策略的所有评估规则命中信息。
cluster exec clear rule hits	从集群中的所有节点清除访问控制策略和预过滤器策略的所有评估规则的规则命中信息，并将其重置为零。

clear service-policy

要清除已启用策略的运行数据或统计信息，请使用 **clear service-policy** 命令。

clear service-policy [**global** | **interface** *intf* | **shape** | **user-statistics**]

Syntax Description

global	（可选）清除全局服务策略的统计信息。
interface *intf*	（可选）清除特定接口的服务策略统计信息。
shape	（可选）清除整形策略的统计信息。
user-statistics	（可选）清除用户统计信息的全局计数器，但不清除每个用户的统计信息。 threat defense上不支持此功能。

Command Default

默认情况下，此命令清除所有已启用的服务策略的所有统计信息。

Command History

版本	修改
6.1	引入了此命令。

使用指南

某些检测引擎允许您选择性地清除统计信息。请参阅 **clear service-policy inspect** 命令。

示例

以下示例显示如何清除外部接口的服务策略统计信息。

```
> clear service-policy interface outside
```

Related Commands

命令	Description
clear service-policy inspect	清除 GTP、M3UA 和 RADIUS 检测引擎的服务策略统计信息。
show service-policy	显示服务策略。
show running-config service-policy	显示在运行配置中配置的服务策略。

clear service-policy inspect gtp

要清除 GTP 检测统计信息，请使用 **clear service-policy inspect gtp** 命令。

clear service-policy inspect gtp {**pdp-context** {**all** | **apn** *ap_name* | **imsi** *IMSI_value* | **ms-addr** *IP_address* | **tid** *tunnel_ID* | **version** *version_num*} | **requests** [**map** *name* | **version** *version_num*] | **statistics** [*IP_address*]}

Syntax Description

pdp-context {**all** | **apn** *ap_name* | **imsi** *IMSI_value* | **ms-addr** *IP_address* | **tid** *tunnel_ID* | **version** *version_num*}	清除数据包数据协议(PDP)或承载情景信息。您可以使用以下关键字指定要清除的情景： • **all**- 清除所有情景。 • **apn** *ap_name*- 清除指定无线接入点名称的情景。 • **imsi** *IMSI_value*- 清除指定 IMSI 十六进制数字的情景。 • **ms-addr** *IP_address*- 清除指定移动用户 (MS) IP 地址的情景。 • **tid** *tunnel_ID*- 清除指定 GTP 隧道 ID（一个十六进制数字）的情景。 • **version** *version_num*- 清除指定 GTP 版本 (0-255) 的情景。
requests [**map** *name* | **version** *version_num*]	清除 GTP 请求。您可以选择使用以下参数限制要清除的请求： • **map** *name*- 清除与指定 GTP 检测策略映射关联的请求。 • **version** *version_num*- 清除指定 GTP 版本 (0-255) 的请求。
statistics [*IP_address*]	清除 **inspect gtp** 命令的 GTP 统计信息。您可以通过指定终端的地址来清除特定终端的统计信息。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例清除 GTP 统计信息：

```
> clear service-policy inspect gtp statistics
```

Related Commands

命令	Description
show service-policy inspect gtp	显示 GTP 统计信息。

clear service-policy inspect m3ua

要清除 M3UA 检测统计信息，请使用 **clear service-policy inspect m3ua** 命令。

clear service-policy inspect m3ua {**drops** | **endpoint** [*ip_address*]}

Syntax Description

drops	清除 M3UA 丢弃统计信息。
endpoint [*ip_address*]	清除 M3UA 终端统计信息。您可以选择包含终端的 IP 地址，以仅清除该终端的统计信息。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用此命令可清除 M3UA 检测的统计信息。使用此命令的 **show** 版本可查看统计信息。

示例

以下示例清除 M3UA 终端统计信息：

```
> clear service-policy inspect m3ua endpoint
```

Related Commands

命令	Description
show service-policy inspect m3ua	显示 M3UA 统计信息。

clear service-policy inspect radius-accounting

要清除 RADIUS 记账用户，请使用 **clear service-policy inspect radius-accounting** 命令。

clear service-policy inspect radius-accounting users {**all** | *ip_address* | *policy_map*}

Syntax Description

all	清除所有用户。
ip_address	清除使用此 IP 地址的用户。
policy_map	清除与指定策略映射关联的用户。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例清除所有 RADIUS 计费用户：

```
> clear service-policy inspect radius-accounting users all
```

clear shun

要禁用当前启用的所有规避并清除规避统计信息，请使用 **clear shun** 命令。

clear shun ［**statistics**］

Syntax Description

statistics	（可选）仅清除接口计数器。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例展示如何禁用当前已启用的所有规避功能并清除规避统计信息：

```
> clear shun
```

Related Commands

命令	Description
shun	阻止新连接并禁止通过任何现有连接传输数据包，从而允许对攻击主机作出动态响应。
show shun	显示 shun 信息。

clear snmp-server statistics

要清除 SNMP 服务器统计信息（SNMP 数据包输入和输出计数器），请使用 **clear snmp-server statistics** 命令。

clear snmp-server statistics

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例展示如何清除 SNMP 服务器统计信息：

```
> clear snmp-server statistics
```

Related Commands

命令	Description
show snmp-server statistics	显示 SNMP 服务器配置信息。

clear snort statistics

要清除 Snort 统计信息（数据包计数器、流计数器和事件计数器），请使用 **clear snort statistics** 命令。

clear snort statistics

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例展示如何清除 Snort 统计信息：

```
> clear snort statistics
```

Related Commands

命令	Description
show snort statistics	显示有关 Snort 服务配置的信息。

clear snort tls-offload

要清除与 SSL 硬件加速（连接、加密、解密）相关的 Snort 统计信息，请使用 **clear snort tls-offload** 命令。请咨询思科 TAC 以帮助您使用此命令调试您的系统。此命令仅在以下支持 SSL 硬件加速的受管设备上可用：

- 采用 威胁防御 的 Firepower 2100
- 采用 威胁防御的 Firepower 4100/9300

  有关 TLS 加密加速Firepower 4100/9300 支持威胁防御 容器实例的信息，请参阅 *FXOS* 配置指南。

所有虚拟设备或除前面所述设备之外的任何硬件上都不支持 TLS 加密加速。

clear snort tls-offload [proxy | tracker]

Syntax Description

proxy	（可选。）仅清除代理的统计信息。
tracker	（可选。）仅清除跟踪器的统计信息。

Command History

版本	修改
6.2.3	引入了此命令。

以下示例显示如何清除代理的静态数据：

```
> clear snort tls-offload proxy
```

Related Commands

命令	Description
show snort tls-offload	显示所有 Snort 流程的统计信息。
debug snort tls-offload	显示所有 Snort 流程的所有类型的错误调试消息。

clear ssl

要清除 SSL 信息以进行调试，请使用 **clear ssl** 命令。

clear ssl {**cache** [**all**] | **errors** | **mib** | **objects**}

Syntax Description

cache [**all**]	清除 SSL 会话缓存中已过期的会话。添加可选 **all** 关键字以清除 SSL 会话缓存中的所有会话和统计信息。
errors	清除 SSL 错误。
mib	清除 SSL MIB 统计信息。
objects	清除 SSL 对象统计信息。

Command History

版本	修改
6.1	引入了此命令。

使用指南

不会清除 DTLS 缓存，因为这样做会影响 AnyConnect 功能。

示例

以下示例清除 SSL 缓存并清除 SSL 会话缓存中的所有会话和统计信息：

```
> clear ssl cache
SSL session cache cleared: 2
No SSL VPNLB session cache
No SSLDEV session cache
DLTS caches are not cleared
> clear ssl cache all
Clearing all sessions and statistics
SSL session cache cleared: 5
No SSL VPNLB session cache
No SSLDEV session cache
DLTS caches are not cleared
```

clear sunrpc-server active

要清除 Sun RPC 应用检测打开的针孔，请使用 **clear sunrpc-server active** 命令。

clear sunrpc-server active

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用 **clear sunrpc-server active** 命令可清除通过 Sun RPC 应用检查打开的针孔，这些针孔允许服务流量（例如 NFS 或 NIS）通过设备。

示例

以下示例展示如何清除 SunRPC 服务表：

```
> clear sunrpc-server active
```

Related Commands

命令	Description
show sunrpc-server active	显示有关活动的 Sun RPC 服务的信息。

clear threat-detection rate

要将威胁检测率统计信息重置为零，请使用 **clear threat-detection rate** 命令。

clear threat-detection rate

Command History

版本	修改
6.3	引入了此命令。

示例

```
> clear threat-detection rate
>
```

Related Commands

命令	Description
show threat-detection rate	显示威胁检测率统计信息。

clear threat-detection scanning-threat

要删除有关通过扫描威胁检测识别的攻击者和目标的信息，请使用 **clear threat-detection scanning-threat** 命令。

clear threat-detection scanning-threat [**attacker** [*ip_address* [*mask*]] | **target** [*ip_address* [*mask*]]]

Syntax Description

attacker [*ip_address* [*mask*]]	（可选。）仅清除攻击者。您可以提供 IP 地址和可选掩码来清除单个攻击者。
target [*ip_address* [*mask*]]	（可选。）仅清除目标。您可以提供IP地址和可选掩码来清除单个目标。

Command Default

清除所有攻击者和目标。

Command History

版本	修改
6.3	引入了此命令。

示例

以下示例显示当前扫描威胁，然后清除它们。

```
> show threat-detection scanning-threat
Latest Target Host & Subnet List:
    192.168.1.0
    192.168.1.249
   Latest Attacker Host & Subnet List:
    192.168.10.234
    192.168.10.0
    192.168.10.2
    192.168.10.3
    192.168.10.4
    192.168.10.5
    192.168.10.6
    192.168.10.7
    192.168.10.8
    192.168.10.9
> clear threat-detection scanning-threat
```

Related Commands

命令	Description
show threat-detection scanning-threat	显示扫描威胁攻击者和目标。

clear threat-detection shun

如果将扫描威胁检测配置为自动避开攻击者，则可以使用 **clear threat-detection shun** 命令从自动避开列表中删除主机。使用 **clear shun** 命令停止避开手动避开的主机。

clear threat-detection shun ［*ip_address* ［*mask*］］

Syntax Description

ip_address [*mask*]	（可选）解除对特定 IP 地址的规避。子网掩码是可选的。

Command Default

释放所有避开的攻击者。

Command History

版本	修改
6.3	引入了此命令。

示例

以下示例显示避开列表，然后释放主机 10.1.1.6。

```
> show threat-detection shun
Shunned Host List:
10.1.1.6
198.1.6.7
> clear threat-detection shun 10.1.1.6
```

Related Commands

命令	Description
show threat-detection shun	显示自动避开的主机。

clear threat-detection statistics

要将威胁检测统计信息重置为零，请使用 **clear threat-detection statistics** 命令。

clear threat-detection statistics ［**tcp-intercept**］

Syntax Description

tcp-intercept	（可选）清除 TCP 拦截统计信息。

Command History

版本	修改
6.3	引入了此命令。

示例

以下示例清除所有威胁检测统计信息。

```
> clear threat-detection statistics
```

Related Commands

命令	Description
show threat-detection statistics	显示威胁检测统计信息。

clear traffic

要重置传输和接收活动的计数器，请使用 **clear traffic** 命令。

clear traffic

Command History

版本	修改
6.1	引入了此命令。

使用指南

clear traffic 命令重置使用 **show traffic** 命令显示的传输和接收活动的计数器。这些计数器指明自上一次输入 clear traffic 命令或自设备进入在线状态以来通过每个接口的数据包和字节的数量。秒数表示自设备上一次重新启动后处于在线状态的持续时间。

示例

以下示例显示了 **clear traffic** 命令：

```
> clear traffic
```

Related Commands

命令	Description
show traffic	显示传输和接收活动的计数器。

clear vpn-sessiondb statistics

要清除 VPN 会话的统计信息，请使用 **clear vpn-sessiondb statistics** 命令。

clear vpn-sessiondb statistics {**all** | **anyconnect** | **failover** | **global** | **index** *number* | **ipaddress** *IP_address* | **l2l** | **name** *username* | **ospfv3** | **protocol** *protocol* | **ra-ikev1-ipsec** | **ra-ikev2-ipsec** | **tunnel-group** *name* | **vpn-lb** | **webvpn**}

Syntax Description

all	清除所有会话的统计信息。
anyconnect	清除 AnyConnect VPN 客户端会话的统计信息。
failover	清除故障转移 IPsec 会话的统计信息。
global	清除所有全局会话数据的统计信息。
index *index_number*	按索引号清除单个会话的统计信息。 **show vpn-sessiondb detail** 命令的输出显示每个会话的索引号。
ipaddress *IP_address*	清除指定 IP 地址的会话的统计信息。
l2l	清除 VPN LAN-to-LAN 会话的统计信息。
protocol *protocol*	清除特定协议的统计信息。输入“？”查看协议列表。
ra-ikev1-ipsec	清除 IPsec IKEv1 会话的统计信息。
ra-ikev2-ipsec	清除 IPsec IKEv2 会话的统计信息。
tunnel-group *groupname*	清除指定的隧道组（连接配置文件）的会话的统计信息。
vpn-lb	清除 VPN 负载平衡管理会话的统计信息。
webvpn	清除无客户端 SSL VPN 会话的统计信息。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例清除所有 VPN 会话的统计信息：

```
> clear vpn-sessiondb statistics all
INFO: Number of sessions cleared : 20
```

Related Commands

命令	Description
show vpn-sessiondb	显示有关 VPN 会话的信息。

clear wccp

要重置 Web 缓存通信协议 (WCCP) 信息，请使用 **clear wccp** 命令。

clear wccp ［**web-cache** | *service_number*］

Syntax Description

web-cache	指定网络缓存服务。
service-number	动态服务标识符，表示缓存所指定的服务定义。动态服务编号为0到254。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例展示如何重置网络缓存服务的 WCCP 信息：

```
> clear wccp web-cache
```

Related Commands

命令	Description
show wccp	显示 WCCP 配置。

clear webvpn statistics

要清除远程访问 VPN 的统计信息，请使用 **clear webvpn statistics** 命令。

clear webvpn statistics

Command History

版本	修改
6.2.1	引入了此命令。

示例

以下示例清除远程访问 VPN 统计信息：

```
> clear webvpn statistics
```

Related Commands

命令	Description
show webvpn	显示有关远程访问 VPN 的信息。

clear xlate

要清除当前的动态 NAT 转换和连接信息，请使用 **clear xlate** 命令。

clear xlate ［**global** *ip1*［*-ip2*］［**netmask** *mask*］］［**local** *ip1*［*-ip2*］［**netmask** *mask*］］［**gport** *port1*［*-port2*］］［**lport** *port1*［*-port2*］］［**interface** *if_name*］［**type** *type*］

Syntax Description

global *ip1*[*-ip2*]	（可选）按全局 IP 地址或地址范围清除活动转换。
gport *port1*[*-port2*]	（可选）按全局端口或端口范围清除活动转换。
interface *if_name*	（可选）按接口显示活动转换。
local *ip1*[*-ip2*]	（可选）按本地 IP 地址或地址范围清除活动转换。
lport *port1*[*-port2*]	（可选）按本地端口或端口范围清除活动转换。
netmask *mask*	（可选）指定用于限定全局或本地 IP 地址的网络掩码或 PIv6 前缀。
type *type*	（可选）按类型清除活动转换。您可以输入以下一个类型： • **dynamic**- 指定动态转换。 • **portmap**- 指定 PAT 全局转换。 • **static**- 指定静态转换。 • **twice-nat**- 指定手动 NAT 转换。

Command History

版本	修改
6.1	引入了此命令。

使用指南

clear xlate 命令清除转换槽的内容（“xlate”是指转换槽）。转换槽在密钥更改后仍可继续存在。添加、更改或删除 NAT 规则后，请始终使用 **clear xlate** 命令。

转换描述 NAT 或 PAT 会话。可以使用 **show xlate detail** 命令查看这些会话。

有两种类型的转换：静态和动态。静态转换是使用静态 NAT 规则创建的持久转换。 **clear xlate** 命令不会清除静态条目。只能通过从配置中删除静态 NAT 规则来删除静态转换。如果从配置中删除某个静态规则，使用该静态规则的先前存在的连接仍可转发流量。使用 **clear local-host** 或 **clear conn** 命令停用这些连接。

动态转换是根据需要创建的流量处理转换。 **clear xlate** 命令删除动态转换以及与这些转换关联的连接。您还可以使用 **clear local-host** 或 **clear conn** 命令清除转换和关联连接。如果从配置中删除动态 NAT 规则，则动态转换和关联连接可能保持活动状态。使用 **clear xlate** 命令可删除这些连接。

示例

以下示例展示如何清除当前的转换和连接槽信息：

```
> clear xlate global
```

Related Commands

命令	Description
clear local-host	清除本地主机网络信息。
show conn	显示所有活动连接。
show local-host	显示本地主机网络信息。
show xlate	显示当前转换信息。

clf - cz

cluster disable

要在设备上禁用集群，请使用 **cluster disable** 命令。

cluster disable

Command History

版本	修改
6.5	引入了此命令。

使用指南

此命令允许您从集群中手动删除集群设备。此命令会保持集群配置不变，以便您稍后可以使用 **cluster enable** 命令将其重新添加到集群。

示例

以下示例在设备上禁用集群：

```
> cluster disable
```

Related Commands

命令	Description
cluster enable	启用集群。
cluster master unit	将新的设备设置为集群的主设备。
cluster remove unit	从集群中删除设备。
show cluster info	显示集群信息。
cluster exec	将命令发送到所有集群成员。

cluster enable

要在设备上启用群集技术，请使用 **cluster enable** 命令。

cluster enable

Command History

版本	修改
6.1	引入了此命令。

使用指南

启用第一台设备后，将进行主设备选举。由于第一台设备应是截至目前为止唯一的集群成员，因此它将成为主设备。请勿在此期间执行任何配置更改。

示例

以下示例在设备上启用群集技术：

```
> cluster enable
```

Related Commands

命令	Description
cluster disable	禁用群集技术。
cluster master unit	将新的设备设置为集群的主设备。
cluster remove unit	从集群中删除设备。
show cluster info	显示集群信息。
cluster exec	将命令发送到所有集群成员。

cluster exec

要在集群中的所有设备或特定成员上执行命令，请使用 **cluster exec** 命令。

cluster exec ［**unit** *unit_name*］ *command*

Syntax Description

unit *unit_name*	（可选）对特定设备执行此命令。要查看成员名称，请输入 **cluster exec unit ?**（查看除当前设备以外的所有名称），或输入 **show cluster info** 命令。
command	指定要执行的命令。

Command History

版本	修改
6.1	引入了此命令。

使用指南

向所有成员发送 **show** 命令以收集所有输出并将其显示在当前设备的控制台上。也可在整个群集范围内执行其他命令（如 **capture** 和 **copy**）。

示例

要同时将同一捕获文件从群集中的所有设备复制到 TFTP 服务器，请在主设备上输入以下命令：

```
> cluster exec copy /pcap capture: tftp://10.1.1.56/capture1.pcap
```

多个 PCAP 文件（一个文件来自一个设备）将复制到 TFTP 服务器。目标捕获文件名会自动附加设备名称，例如 capture1_device1.pcap, capture1_device2.pcap 等。在本示例中，device1 和 device2 是群集设备名称。

以下是 **cluster exec show port-channel** 汇总命令的输出示例，显示了集群内每个成员的 EtherChannel 信息：

```
> cluster exec show port-channel summary
primary(LOCAL):*************************************************************
 Number of channel-groups in use: 2
Group  Port-channel  Protocol  Span-cluster  Ports
------+-------------+-----------+-----------------------------------------------
1         Po1             LACP       Yes  Gi0/0(P)
2         Po2             LACP       Yes  Gi0/1(P)
 secondary:*********************************************************************
 Number of channel-groups in use: 2
Group  Port-channel  Protocol  Span-cluster   Ports
------+-------------+-----------+-----------------------------------------------
1         Po1             LACP       Yes   Gi0/0(P)
2         Po2             LACP       Yes   Gi0/1(P)
```

Related Commands

命令	Description
cluster enable	在设备上启用群集技术。
cluster master unit	将新的设备设置为集群的主设备。
cluster remove unit	从集群中删除设备。
show cluster info	显示集群信息。
cluster exec	将命令发送到所有集群成员。

cluster exec clear rule hits

要从集群中的所有节点清除访问控制策略和预过滤器策略的所有评估规则的规则命中信息并将其重置为零，请使用 **cluster exec clear rule hits** 命令。

cluster exec clear rule hits ［*ID*］

Syntax Description

ID	（可选）规则的 ID。包含此参数将仅清除指定规则的规则命中信息。 使用 **show access-list** 命令标识规则 ID。但是，此命令的输出中并未列出所有规则。您可以在以下 URL 上触发 REST API GET 操作，以查看所有规则及其 ID： • `/api/fmc_config/v1/domain/{domainUUID}/policy/accesspolicies/{containerUUID}/operational/hitcounts?filter="deviceId:{deviceId}"&expanded=true` • `/api/fmc_config/v1/domain/{domainUUID}/policy/prefilterpolicies/{containerUUID}/operational/hitcounts?filter="deviceId:{deviceId}"&expanded=true`

Command Default

如果不指定规则 ID，则所有规则的规则命中信息都将被清除并重置为零。

注释 使用此命令时请谨慎操作，因为此操作不可逆。

Command History

版本	修改
6.4	引入了此命令。

使用指南

规则命中信息仅涵盖访问控制规则和预过滤器规则。

示例

以下是清除所有规则命中信息的示例：

```
> cluster exec clear rule hits
```

Related Commands

命令	Description
show cluster rule hits	以汇总格式显示来自集群所有节点的访问控制策略和预过滤器策略的所有评估规则命中信息。
cluster exec show rule hits	以隔离的格式显示集群中每个节点的访问控制策略和预过滤器策略的所有评估规则命中信息。

命令	Description
show rule hits	显示访问控制策略和预过滤器策略的所有评估规则的规则命中信息。
clear rule hits	清除访问控制策略和预过滤器策略的所有评估规则的规则命中信息，并将其重置为零。

cluster exec show rule hits

要从集群的每个节点以隔离格式显示访问控制策略和预过滤器策略的所有评估规则的命中信息，请使用 **cluster exec show rule hits** 命令。

cluster exec show rule hits [*id* | **raw** | **gt** *#hit-count* | **lt** *#hit-count* | **range** *#hit-count1 #hit-count2*]

Syntax Description

ID	（可选）规则的 ID。包含此参数会限制向指定规则显示的信息。 使用 **show access-list** 命令标识规则 ID。但是，此命令的输出中并未列出所有规则。您可以在以下 URL 上触发 REST API GET 操作，以查看所有规则及其 ID： • `/api/fmc_config/v1/domain/{domainUUID}/policy/accesspolicies/{containerUUID}/operational/hitcounts?filter="deviceId:{deviceId}"&expanded=true` • `/api/fmc_config/v1/domain/{domainUUID}/policy/prefilterpolicies/{containerUUID}/operational/hitcounts?filter="deviceId:{deviceId}"&expanded=true`
raw	（可选）以 .csv 格式显示规则命中信息。
gt *#hit-count*	（可选）显示命中计数大于 #hit-count 的所有规则。
lt *#hit-count*	（可选）显示命中计数小于 #hit-count 的所有规则。
range *#hit-count1 #hit-count2*	（可选）显示命中计数介于 #hit-count1 和 #hit-count2 之间的所有规则。

Command Default

如果不指定规则 ID，则会显示所有规则的规则命中信息。

Command History

版本	修改
6.4	引入了此命令。

使用指南

规则命中信息仅涵盖访问控制规则和预过滤器规则。

示例

以下示例以隔离格式显示来自集群的每个节点的规则命中信息：

```
> cluster exec show rule hits
unit-1-1(LOCAL):**************************************************

RuleID               Hit Count           First Hit Time(UTC)     Last Hit Time(UTC)
-------------------------------------------------------------------------------------
268435260            1                   06:55:17 Mar 8 2019     06:55:17 Mar 8 2019
268435261            1                   06:55:19 Mar 8 2019     06:55:19 Mar 8 2019
```

```
unit-1-3:************************************************************

RuleID               Hit Count           First Hit Time(UTC)     Last Hit Time(UTC)
-------------------------------------------------------------------------------------
268435264            1                   06:54:43 Mar 8 2019     06:54:43 Mar 8 2019
268435265            1                   06:54:57 Mar 8 2019     06:54:57 Mar 8 2019


unit-1-2:************************************************************

RuleID               Hit Count           First Hit Time(UTC)     Last Hit Time(UTC)
-------------------------------------------------------------------------------------
268435270            1                   06:54:53 Mar 8 2019     06:54:53 Mar 8 2019
268435271            1                   06:55:01 Mar 8 2019     06:55:01 Mar 8 2019
```

Related Commands

命令	Description
cluster exec clear rule hits	从集群中的所有节点清除访问控制策略和预过滤器策略的所有评估规则的规则命中信息，并将其重置为零。
show cluster rule hits	以汇总格式显示来自集群所有节点的访问控制策略和预过滤器策略的所有评估规则命中信息。
show rule hits	显示访问控制策略和预过滤器策略的所有评估规则的规则命中信息。
clear rule hits	清除访问控制策略和预过滤器策略的所有评估规则的规则命中信息，并将其重置为零。

cluster master unit

要将新设备设置为设备集群的主设备，请使用 **cluster master unit** 命令。

cluster master unit *unit_name*

Syntax Description

unit_name	指定要成为新的主设备的本地设备的名称。要查看成员名称，请输入**cluster master unit ?**（查看除当前设备以外的所有名称），或输入 **show cluster info** 命令。

Command History

版本	修改
6.1	引入了此命令。

使用指南

您需要重新连接到主集群 IP 地址。

示例

以下示例将 **device2** 设置为主设备：

```
> cluster master unit device2
```

Related Commands

命令	Description
cluster enable	在设备上启用群集技术。
cluster exec	将命令发送到所有集群成员。
cluster remove unit	从集群中删除设备。
show cluster info	显示集群信息。

cluster remove unit

要从集群中删除设备，请使用 **cluster remove unit** 命令。

cluster remove unit *unit_name*

Syntax Description

unit_name	指定要从集群中删除的本地设备的名称。要查看成员名称，请输入 **cluster remove unit ?**，或输入 **show cluster info** 命令。

Command History

版本	修改
6.1	引入了此命令。

使用指南

引导程序配置保持不变，从主设备同步的最新配置也保持不变，因此您可于稍后重新添加该设备而不会丢失配置。如果在从属设备上输入此命令来删除主设备，将会选举新的主设备。

示例

以下示例检查设备的名称，然后从集群中删除 device2：

```
> cluster remove unit ?
Current active units in the cluster:
device2
> cluster remove unit device2
WARNING: Clustering will be disabled on unit device2. To bring it back
to the cluster please logon to that unit and re-enable clustering
```

Related Commands

命令	Description
cluster enable	在设备上启用群集技术。
cluster exec	将命令发送到所有集群成员。
cluster master unit	将新的设备设置为集群的主设备。
show cluster info	显示集群信息。

cluster reset-interface-mode

要在禁用集群后将集群设备转换为独立模式，请使用 **cluster reset-interface-mode** 命令。

cluster reset-interface-mode

Command History

版本	修改
7.0	引入了此命令。

使用指南

必须先使用 **cluster disable** 命令禁用集群。 **cluster reset-interface-mode** 命令会清除 threat defense 配置并重新启动逻辑设备。在 4100 系列的 FXOS 中，逻辑设备也会转换为独立类型的设备。维护引导程序配置和接口分配。

示例

以下示例禁用集群，然后删除集群配置：

```
> cluster disable
> cluster reset-interface-mode

Broadcast message from root@firepower (Tue Apr 27 18:36:12 2021):

The system is going down for reboot NOW!
```

Related Commands

命令	Description
cluster enable	在设备上启用群集技术。
cluster exec	将命令发送到所有集群成员。
cluster master unit	将新的设备设置为集群的主设备。
show cluster info	显示集群信息。

configure cert-update auto-update

要在 threat defense 设备上启用或禁用 CA 证书的自动更新，请使用 **configure cert-update auto-update** 命令。

configure cert-update auto-update { **enable** | **disable** }

Syntax Description

enable	启用 CA 证书的自动更新。
disable	禁用 CA 证书的自动更新。

Command History

版本	修改
7.0.5	引入了此命令。

使用指南

默认情况下，当您安装或升级 threat defense 到版本 7.0.5 时，CA 证书会自动更新。如果要禁用此功能，请使用 **disable** 关键字。要重新启用 CA 捆绑包的自动更新，请使用 **enable** 关键字。当您对 CA 证书启用自动更新时，系统将每天在系统定义的时间执行更新流程。

示例

以下是 **configure cert-update auto-update** 命令的输出示例：

```
> configure cert-update auto-update disable
Autoupdate is disabled
> configure cert-update auto-update enable
Autoupdate is enabled and set for every day at 12:18 UTC
```

Related Commands

命令	Description
show cert-update	显示 CA 证书的自动更新状态。
configure cert-update run-now	立即尝试更新 CA 认证。
configure cert-update test	使用来自思科服务器的最新 CA 证书执行连接检查。

configure cert-update run-now

要立即执行 CA 证书的自动更新，请使用 **configure cert-update run-now** 命令。

configure cert-update run-now [**force**]

Syntax Description

force	即使连接检查失败，也会执行 CA 证书更新。

Command History

版本	修改
7.0.5	引入了此命令。

使用指南

如果要立即更新 CA 证书，请使用 **configure cert-update run-now**。但是，即使其中一台思科服务器的 SSL 连接检查失败，该流程也会终止。要在连接失败的情况下继续更新，请使用 **force** 关键字。例如，本地 CA 捆绑包具有访问多种思科服务（例如智能许可、AMP 注册和 ThreatGrid 服务）的证书，如果与思科智能许可服务的连接失败，则在使用 **configure cert-update run-now force** 命令时仍会执行证书更新过程。

注释 在仅 IPv6 部署中，CA 证书的自动更新可能会失败，因为某些思科服务器不支持 IPv6。在这种情况下，请使用 **configure cert-update run-now force** 命令强制更新 CA 证书。

示例

以下是连接检查失败时 **configure cert-update run-now** 命令的输出示例：

```
> configure cert-update run-now
Certs failed some connection checks.
```

以下是连接检查成功且本地 CA 捆绑包已更新时 **configure cert-update run-now** 命令的输出示例：

```
>configure cert-update run-now
Certs have been replaced or was already up to date.
```

以下是 **configure cert-update run-now force** 命令的输出示例：

```
> configure cert-update run-now force
Certs failed some connection checks, but replace has been forced.
```

Related Commands

命令	Description
configure cert-update auto-update	启用或禁用每天自动更新 CA 证书。

命令	Description
show cert-update	显示 CA 证书的自动更新状态。
configure cert-update test	使用来自思科服务器的最新 CA 证书执行连接检查。

configure cert-update test

要验证本地系统中的 CA 证书是否是最新的（如果它们已过期），要使用新的 CA 捆绑包测试与服务器的 SSL 连接，请使用 **configure cert-update test** 命令。

configure cert-update test

Command History

版本	修改
7.0.5	引入了此命令。

使用指南

configure cert-update test 命令将本地系统上的 CA 捆绑包与最新的 CA 捆绑包（来自思科服务器）进行比较。如果 CA 捆绑包是最新的，则不会执行检查，并且会显示测试结果，如下面的“示例”部分所示。如果 CA 捆绑包已过期，则对下载的 CA 捆绑包执行连接检查，结果如下面的“示例”部分所示。

示例

以下是本地 CA 捆绑包为最新时 **configure cert-update test** 命令的输出示例：

```
> configure cert-update test
Test succeeded, certs can safely be updated or are already up to date.
```

以下是本地CA 捆绑包过期且对下载的捆绑包进行连接检查失败时 **configure cert-update test** 命令的输出示例：

```
> configure cert-update test
Test failed, not able to fully connect.
```

以下是当本地 CA 捆绑包过期且对已下载捆绑包的连接检查成功或 CA 捆绑包已为最新版本时 **configure cert-update test** 命令的输出示例：

```
> configure cert-update test
Test succeeded, certs can safely be updated or are already up to date.
```

Related Commands

命令	Description
configure cert-update auto-update	启用或禁用每天自动更新 CA 证书。
show cert-update	显示 CA 证书的自动更新状态。
configure cert-update run-now	立即尝试更新 CA 认证。

configure coredump packet-engine

要启用或禁用数据包引擎核心转储生成，请使用 **configure coredump packet-engine** 命令。

configure coredump packet-engine {**enable** | **disable**}

Syntax Description

disable	禁用数据包引擎核心转储生成。
enable	启用数据包引擎核心转储生成。

Command History

版本	修改
6.2.1	引入了此命令。

使用指南

默认情况下，启用数据包引擎核心转储生成。

此命令仅在Firepower 2100 系列上可用。在不受支持的平台上运行此命令时，系统会返回以下消息：

```
This command is not available on this platform.
```

示例

以下示例禁用数据包引擎核心转储生成。

```
> configure coredump packet-engine disable
```

Related Commands

命令	Description
show coredump	显示数据包引擎核心转储生成设置。

configure disable-https-access

要清除 HTTPS 访问列表，将设备配置为拒绝来自所有 IP 地址的 HTTPS 连接尝试，请使用 **configure disable-https-access** 命令。

configure disable-https-access

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用此命令可禁用对设备的 HTTPS 访问。使用本地管理器 设备管理器时，需要 HTTPS 访问。

如果设备是本地管理的高可用性组中的设备，则下次主用设备部署配置更新时，您的更改将被覆盖。如果这是主用设备，您的更改将在部署期间传播到对等设备。

示例

以下示例将设备配置为拒绝来自任何地址的 HTTPS 连接：

```
> configure disable-https-access
```

Related Commands

命令	Description
configure https-access-list	将设备配置为接受来自指定 IP 地址的 HTTPS 连接。
show https-access-list	显示当前的 HTTPS 访问列表。

configure disable-ssh-access

要清除 SSH 访问列表，将设备配置为拒绝来自所有 IP 地址的 SSH 连接尝试，请使用 **configure disable-ssh-access** 命令。

configure disable-ssh-access

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用此命令可禁用对设备的 SSH 访问。这可以防止 CLI 访问（通过控制台端口除外）。

如果设备是本地管理的高可用性组中的设备，则下次主用设备部署配置更新时，您的更改将被覆盖。如果这是主用设备，您的更改将在部署期间传播到对等设备。

示例

以下示例将设备配置为拒绝来自任何地址的 SSH 连接：

```
> configure disable-ssh-access
```

Related Commands

命令	Description
configure ssh-access-list	将设备配置为接受来自指定 IP 地址的 SSH 连接。
show ssh-access-list	显示当前的 SSH 访问列表。

configure firewall

要将防火墙模式设置为透明或路由模式，请使用 **configure firewall** 命令。

configure firewall {**routed** | **transparent**}

Syntax Description

routed	将防火墙模式设置为路由防火墙模式。
transparent	将防火墙设置为透明模式。

Command Default

默认情况下，设备处于路由模式。

Command History

版本	修改
6.1	引入了此命令。

使用指南

透明防火墙是 2 层防火墙，充当“嵌入式防火墙”或“隐藏防火墙”，并且不会被视为所连接设备的路由器跃点。

更改模式时， 设备会清除配置，因为许多命令不会在这两种模式下同时受到支持。如果您已经具有填充的配置，请务必在更改模式之前备份配置；在创建新配置时，可以使用此备份作为参考。

注释 如果使用的是 设备管理器，则无法切换到透明防火墙模式。如果您使用的是本地管理器，并且要转换为透明模式，则必须先使用 **configure manager delete** 删除管理器，然后使用 转换为透明模式，然后使用 **configure manager add** 指向 管理中心。

示例

以下示例将防火墙模式更改为透明：

```
> configure firewall transparent
```

Related Commands

命令	Description
show running-config	显示运行配置。
show firewall	显示防火墙模式。

configure flow-offload

此命令通过在硬件中处理某些流（即流量）来启用或禁用加速。将流处理分流到硬件可提高性能，默认情况下已启用。

Firepower 4100/9300 机箱上 threat defense 支持动态数据流分流。动态流分流使您能够选择要分流到硬件的流量，这意味着它不由 threat defense 设备的软件或 CPU 处理。

configure flow-offload dynamic whitelist {enable | disable}

Syntax Description

dynamic whitelist enable	启用动态分流。
dynamic whitelist disable	禁用动态分流。

Command Default

默认启用。

Command History

版本	修改
6.3	引入了此命令。

使用指南

有关动态数据流分流支持和限制的信息，请参阅 管理中心配置指南 中有关通用规则特征的章节。

示例

以下是禁用动态分流的示例：

```
> configure flow-offload dynamic whitelist disable
```

以下是启用动态分流的示例：

```
> configure flow-offload dynamic whitelist enable
```

Related Commands

命令	Description
show flow-offload	显示动态数据流分流计数器、统计信息和信息。
clear flow-offload	清除动态数据流分流数据流、计数器或统计信息。

configure high-availability

要禁用、暂停或恢复设备之间的高可用性配置（故障转移），请使用 **configure high-availability** 命令。

configure high-availability {**disable** [**clear-interfaces**] | **resume** | **suspend** [**clear-interfaces**]}

Syntax Description

clear-interfaces	（可选）在禁用或暂停高可用性时清除接口配置。
disable	中断此设备与其对等体之间的高可用性关系。 您不能在本地管理的设备上使用此选项；请改为使用 设备管理器 。如果您错误地使用了禁用命令，则必须使用 BreakHAStatus 资源调用 threat defense API 来完成操作。
resume	恢复此设备与其对等体之间的临时暂停的高可用性配置。该设备将与对等设备协商主用/备用状态。您无法恢复已禁用的配置。
suspend	临时暂停此设备与其对等体之间的高可用性配置。您可以稍后恢复配置。 如果您从主用设备暂停高可用性，配置将在主用和备用设备上暂停。如果从备用设备暂停，配置仅在备用设备上暂停，但主用设备不会尝试故障切换至暂停的设备。

Command History

版本	修改
6.1	引入了此命令。

使用指南

可以将两个设备配置成一个高可用性对。这也称为故障转移配置，如果对中的另一台设备发生故障，则一台设备可以接管。

如果由于某种原因无法更新设备管理器中的配置，可以使用 **configure high-availability** 命令来管理高可用性对。例如，如果无法访问高可用性对，可以使用 **configure high-availability disable** 删除两个高可用性对等体的故障转移配置。

您还可以暂时挂起故障转移配置，稍后再将其恢复。在以下情况下，暂停设备上的 HA 非常有用：

- 两台设备都在主用 - 主用情况下，且修复故障转移链路上的通信不能更正问题。
- 希望对主用或备用设备进行故障排除，并且不希望设备在此期间发生故障切换。
- 您想要在备用设备上安装软件升级期间阻止故障转移。

暂停高可用性时，停止将设备对用作故障转移设备。当前主用设备保持活动状态，并处理所有用户连接。但是，不会再监控故障转移条件，并且系统永远不会故障切换到现在的伪备用设备。备用设备将保留其配置，但将保持非活动状态。

暂停 HA 和中断 HA 之间的主要区别是，在暂停的 HA 设备上将保留高可用性配置。如果中断 HA，则会清除配置。因此，您可以选择在暂停系统上恢复高可用性，这样可启用现有配置并再次将两台设备设置为故障转移对。

注释 暂停高可用性是一种临时状态。如果您重新加载一台设备，它会自动恢复高可用性配置，并与对等体协商主用/备用状态。

示例

以下示例显示如何临时暂停然后恢复高可用性配置。

```
> show failover
Failover On
Failover unit Primary
Failover LAN Interface: failover GigabitEthernet0/2 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 61 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.7(0)74, Mate 9.7(0)74
Serial Number: Ours 9A41CKDXQJU, Mate 9A3MFP0H1CP
Last Failover at: 19:23:17 UTC Oct 26 2016
        This host: Primary - Active
                Active time: 776671 (sec)
                slot 0: empty
                  Interface outside (192.168.77.1): Normal (Waiting)
                  Interface inside (192.168.87.1): Normal (Waiting)
                  Interface diagnostic (0.0.0.0): Normal (Waiting)
                slot 1: snort rev (1.0)  status (up)
                slot 2: diskstatus rev (1.0)  status (up)
        Other host: Secondary - Standby Ready
                Active time: 53 (sec)
                  Interface outside (0.0.0.0): Normal (Waiting)
                  Interface inside (0.0.0.0): Normal (Waiting)
                  Interface diagnostic (0.0.0.0): Normal (Waiting)
                slot 1: snort rev (1.0)  status (up)
                slot 2: diskstatus rev (1.0)  status (up)
(...Output truncated...)
> configure high-availability suspend
Please ensure that no deployment operation is in progress before suspending
high-availability.
Please enter 'YES' to continue if there is no deployment operation in progress and
'NO' if you wish to abort: Yes
Successfully suspended high-availability.
> show failover
Failover Off
Failover unit Primary
Failover LAN Interface: failover GigabitEthernet0/2 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 61 maximum
MAC Address Move Notification Interval not set
```

```
failover replication http
> configure high-availability resume
Successfully resumed high-availablity.
> show failover
Failover On
Failover unit Primary
Failover LAN Interface: failover GigabitEthernet0/2 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 61 maximum
MAC Address Move Notification Interval not set
failover replication http
Unit Enrollment Hold action is active, timeout in 1792 seconds
Version: Ours 9.7(0)74, Mate 9.7(0)74
Serial Number: Ours 9A41CKDXQJU, Mate Unknown
Last Failover at: 20:26:06 UTC Nov 4 2016
        This host: Primary - Active
                Active time: 778071 (sec)
                slot 0: empty
                  Interface outside (192.168.77.1): Normal (Waiting)
                  Interface inside (192.168.87.1): Normal (Waiting)
                  Interface diagnostic (0.0.0.0): Normal (Waiting)
                slot 1: snort rev (1.0)  status (up)
                slot 2: diskstatus rev (1.0)  status (up)
        Other host: Secondary - App Sync
                Active time: 53 (sec)
                  Interface outside (0.0.0.0): Unknown (Waiting)
                  Interface inside (0.0.0.0): Unknown (Waiting)
                  Interface diagnostic (0.0.0.0): Unknown (Waiting)
                slot 1: snort rev (1.0)  status (up)
                slot 2: diskstatus rev (1.0)  status (up)
(...Output truncated...)
```

Related Commands

命令	Description
show failover	显示故障转移（高可用性）配置。
show high-availability config	显示故障转移（高可用性）配置。提供 **show failover**相同的输出。

configure https-access-list

要将设备配置为接受来自指定 IP 地址的 HTTPS 连接，请使用 **configure https-access-list** 命令。

configure https-access-list *address_list*

Syntax Description

address_list	主机或网络的 IP 地址的逗号分隔列表，采用 IPv4 无类域间路由 (CIDR) 符号或 IPv6 前缀长度符号。例如，10.100.10.0/24 or 2001:DB8::/96。 要指定所有 IPv4 主机，请输入 0.0.0.0/0。要指定所有 IPv6 主机，请指定 ::/0。

Command History

版本	修改
6.1	引入了此命令。

使用指南

您必须在一个命令中包含所有受支持的主机或网络。此命令中指定的地址将覆盖 HTTPS 访问列表的当前内容。

仅允许 HTTPS 访问不允许用户登录本地管理器。对配置软件的访问由用户名和密码控制。

如果设备是本地管理的高可用性组中的设备，则下次主用设备部署配置更新时，您的更改将被覆盖。如果这是主用设备，您的更改将在部署期间传播到对等设备。

示例

以下示例将设备配置为接受来自任何 IPv4 或 IPv6 地址的 HTTPS 连接：

```
> configure https-access-list 0.0.0.0/0,::/0
The https access list was changed successfully.
> show https-access-list
ACCEPT     tcp  --  anywhere             anywhere             state NEW tcp dpt:https
ACCEPT     tcp      anywhere             anywhere             state NEW tcp dpt:https
```

Related Commands

命令	Description
configure disable-https-access	清除 HTTPS 访问列表。
show https-access-list	显示 HTTPS 访问列表。

configure identity-subnet-filter

要从接收 ISE 的用户到 IP 和安全组标记 (SGT) 到 IP 的映射中排除子网，请使用 **configure identity-subnet-filter** 命令。您通常应对内存较低的受管设备执行此操作，以防止 Snort 身份运行状况监控器内存错误。

configure identity-subnet-filter { **add** | **remove** } *subnet*

Syntax Description

add	将指定的子网添加到排除的子网列表。
remove	从排除的子网列表中删除指定的子网。
子网	指定要添加或排除的子网。

Command History

版本	修改
6.7	引入了此命令。

示例

以下示例为管理接口配置静态 IPv6 地址。

```
> configure identity-subnet-filter 192.0.2.0/24
```

Related Commands

命令	Description
show identity-subnet-filter	显示当前从用户到 IP 和 SGT 到 IP 映射中排除的子网。

configure inspection

要启用或禁用默认应用协议检测引擎，请使用 **configure inspection** 命令。

configure inspection 协议 {**enable** | **disable**}

Syntax Description

disable	禁用检测引擎。
enable	启用检测引擎。
protocol	要启用或禁用的检测协议。有关选项列表，请参阅使用指南部分。

Command History

版本	修改
6.2	引入了此命令。

使用指南

注释 虽然您可以在使用 设备管理器时禁用检测，但每次从 设备管理器部署配置时，都会重新启用默认检测。如果要保持禁用检测，则必须在每次部署后重新输入 命令。从版本 6.2.3 开始，您可以使用 FlexConfig 启用和禁用这些检查，以使更改保持不变。

仅在思科技术支持人员的指示下，或者在确定网络上不会出现关联类型的流量时，才禁用默认检测引擎。例如，如果阻止受检查端口上的所有流量，则可以安全地禁用该端口上的检查。这些检测适用于所有数据接口。

这些检测引擎独立于 Snort 检测。这些引擎提供以下服务：

- 创建小孔 - 一些应用协议在标准端口或协商的端口上打开辅助 TCP 或 UDP 连接。检测会为这些辅助端口打开小孔，使您无需创建访问控制规则予以允许。
- NAT 重写 - 诸如 FTP 等协议会在数据包数据中嵌入用于辅助连接的 IP 地址和端口，作为协议的一部分。如果 NAT 转换涉及到任一终端，则检测引擎会重写数据包数据以反映嵌入式地址和端口的 NAT 转换。在没有 NAT 重写的情况下，辅助连接不起作用。有关 NAT 限制，请参阅您用于配置设备的管理器（管理中心 或 设备管理器）的配置指南中的 NAT 一章。
- 协议实施 - 一些检测会为检测到的协议实施某种程度的 RFC 一致性。

您可以禁用并随后启用以下检测引擎。要查看当前已启用的功能，请使用 **show running-config policy-map** 命令并查找 **inspect** 命令。要查看每个检测的默认参数的详细信息，请使用 **show running-config all policy-map** 命令。

- **dcerpc**-（TCP 端口 135。）分布式计算环境/远程过程调用系统。DCERPC 检测引擎在已知 TCP 端口 135 上检测终端映射程序 (EPM) 与客户端之间的本地 TCP 通信。Microsoft 远程过程调用

(MSRPC) 基于 DCERPC，是 Microsoft 分布式客户端和服务器应用广泛使用的协议，允许软件客户端在服务器上远程执行程序。检测提供针孔创建和 NAT 服务。

- **dns**-（UDP 端口 53。）域名系统。在 UDP 端口 53 上检查 DNS。检测提供 NAT 服务和协议实施。您必须启用此检测引擎，才能在 NAT 规则上使用 NAT 重写选项。在 IPv4 和 IPv6 网络 (NAT64/46) 之间执行 NAT 时，通常需要重写 NAT。
- **esmtp**-（TCP 端口 25。）扩展的简单邮件传输协议。ESMTP 检测可检测垃圾邮件、网络钓鱼、变形邮件等攻击和缓冲流量上溢/下溢攻击。另外，它还支持应用安全和协议符合性（实施 ESMTP 消息合理性检查及冻结发件人/收件人）并可冻结邮件中继。有关检查期间应用的控制的详细信息，请使用 **show running-config all policy-map** 命令并查找“policy-map type inspect esmtp _default_esmtp_map”行和后续参数。

  ESMTP 应用检测可控制和减少用户可使用的命令数以及服务器返回的消息数。它提供 NAT 服务和协议一致性。ESMTP 检测主要执行三种任务：

  - 将 SMTP 请求限制为七个基本 SMTP 命令和八个扩展命令。支持的命令如下：

    扩展 SMTP - AUTH、EHLO、ETRN、HELP、SAML、SEND、SOML、STARTTLS 和 VRFY。

    SMTP (RFC 821) - DATA、HELO、MAIL、NOOP、QUIT、RCPT、RSET。
  - 监控 SMTP 命令-响应序列。
  - 生成审计追踪。邮件地址中嵌入的无效字符被替换时，会生成系统日志审计记录 108002。有关详细信息，请参阅 RFC 821。
- **ftp**-（TCP 端口 21。）文件传输协议。检测提供针孔和 NAT 服务。
- **h323_h225**-（TCP 端口 1720，UDP 端口 1718。）H.323 检测支持 RAS、H.225 和 H.245，这项检测功能会转换所有嵌入式 IP 地址和端口。它执行状态跟踪和过滤。H.323 检测支持符合 H.323 规范的应用，例如思科 CallManager。H.323 是国际电信联盟制定的一套协议，用于通过 LAN 进行多媒体会议。设备最高支持 H.323 v6，其中包括 H.323 v3“支持在一个呼叫信令信道上进行多个呼叫”的功能。

  H.323 检测具有如下两个主要功能：

  - 对 H.225 和 H.245 消息中必要的嵌入式 IPv4 地址进行 NAT 转换。由于 H.323 消息以 PER 编码格式编码，所以 ASA 使用 ASN.1 解码器来解码 H.323 消息。
  - 动态分配协商的 H.245 和 RTP/RTCP 连接。使用 RAS 时，也可以动态分配 H.225 连接。
- **h323_ras**-（UDP 端口 1718-1719。）请参阅 **h323_h225**的说明。此检查适用于 RAS 信令。
- **icmp**-（仅限 ICMP 流量。）ICMP 检测引擎允许 ICMP 流量具有“会话”，这样可以像对 TCP 和 UDP 流量那样对这种流量进行检测。如果没有 ICMP 检测引擎，我们建议您不要允许 ICMP 通过设备（使用访问控制规则屏蔽）。如果不进行状态检测，ICMP 可能被用于攻击网络。ICMP 检测引擎确保每个请求只有一个响应，并确保序列号是正确的。检测还提供 NAT 服务。

- **icmp_error**-（仅限 ICMP 流量。）如果启用了 ICMP 错误检测，设备会根据 NAT 配置为发送 ICMP 错误消息的中间跃点创建转换会话。设备用转换后的 IP 地址覆盖数据包。这对于在通过设备的跟踪路由中提供有意义的信息是必要的。
- **ip-options**-（仅限 RSVP 流量。）IP 选项检查根据数据包信头中 IP 选项字段的内容控制允许哪些 IP 数据包。允许具有 Router Alert 选项的数据包。丢弃包含任何其他选项的数据包。
- **netbios**—(UDP 源端口137, 138.) NetBIOS Name Server over IP。NetBIOS 应用检测对 NetBIOS 名称服务 (NBNS) 数据包和 NetBIOS 数据报服务数据包中嵌入的 IP 地址执行 NAT。这项检测还会检查各个数量字段和长度字段的一致性，从而强制执行协议符合性。
- **rsh**-（TCP 端口 514。）RSH 协议在 TCP 端口 514 上使用从 RSH 客户端到 TCP RSH 服务器的连接。客户端和服务器协商出 TCP 端口号，客户端会在该端口上侦听 STDERR 输出流。如有必要，RSH 检测打开针孔并支持协商端口号的 NAT。
- **rtsp**-（TCP 端口 554。）实时流传输协议。RTSP 检测引擎使设备可以传递 RTSP 数据包。RealAudio、RealNetworks、Apple QuickTime、RealPlayer 和思科 IP/TV 连接都使用 RTSP。RTSP 应用使用已知 TCP（很少用 UDP）端口 554 作为控制信道。设备仅支持 TCP（这符合 RFC 2326 的要求）。该 TCP 控制信道用于根据客户端配置的传输模式协商用于传输音频/视频流量的数据信道。支持如下 RDT 传输：rtp/avp、rtp/avp/udp、x-real-rdt、x-real-rdt/udp 和 x-pn-tng/udp。
- **sqlnet**-（TCP 端口 1521。）检测引擎支持 SQL*Net 版本 1 和 2，但仅支持透明网络底层 (TNS) 格式。检测不支持表格数据流 (TDS) 格式。系统会扫描嵌入式地址和端口的 SQL*Net 消息，并在需要时应用 NAT 重写。

  当与 SQL 控制 TCP 端口 1521 相同的端口上发生 SQL 数据传输时，请禁用 SQL*Net 检测。安全设备在启用 SQL*Net 检测之后充当代理，且将客户端窗口大小从 65000 缩小至大约 16000，从而导致数据传输问题。
- **sip**-（TCP/UDP 端口 5060。）会话发起协议。SIP 是一种广泛用于网络会议、电话、展示、事件通知和即时消息的协议。部分原因是 SIP 本质上是文本协议，部分原因是其具有灵活性，因此，SIP 网络面临大量安全威胁。SIP 应用检测会在消息信头和正文中提供地址转换，会动态打开端口，还会执行基本健全性检查。
- **skinny**-（TCP 端口 2000。）瘦客户端控制协议 (SCCP)。SCCP（瘦客户端）应用检测对数据包数据中的嵌入式 IP 地址和端口号执行转换，并会动态打开针孔。它还执行其他协议符合性检查和基本状态跟踪。
- **sunrpc**-（TCP/UDP 端口 111。）Sun RPC 可供 NFS 和 NIS 使用。Sun RPC 服务可在任何端口上运行。当客户端尝试访问服务器上的 Sun RPC 服务时，必须获悉服务运行所在的端口。它通过查询端口映射程序流程执行此操作，通常为 rpcbind，位于公认端口 111。

  客户端将发送服务的 Sun RPC 程序号，而端口映射程序流程将用服务的端口号进行响应。客户端发送其 Sun RPC 查询至服务器，指定端口映射程序流程识别的端口。服务器回复后，设备会截取此数据包，并打开该端口上的初始化 TCP 和 UDP 连接。不支持 Sun RPC 负载信息的 NAT 或 PAT。
- **tftp**-（UDP 端口 69。）简单文件传输协议。检测引擎检测 TFTP 读取请求 (RRQ)、写入请求 (WRQ) 和错误通知 (ERROR)，并且如有必要，还会动态创建连接和转换，从而允许在 TFTP 客户端和服务器之间传输文件。

如有必要，在接收有效的读取 (RRQ) 或写入 (WRQ) 请求时会分配动态辅助信道和 PAT 转换。随后，TFTP 会使用该辅助信道进行文件传输或错误通知。只有 TFTP 服务器可以通过辅助信道发起流量；此外，TFTP 客户端与服务器之间最多只能有一个不完整的辅助信道。服务器发出的错误通知会致使辅助信道关闭。如果使用静态 PAT 重定向 TFTP 流量，则必须启用 TFTP 检测。

- **xdmcp**-（UDP 端口 177。）X 显示管理器控制协议。XDMCP 是使用 UDP 端口 177 来协商 X 会话（建立后使用 TCP）的协议。为了成功协商和启动 XWindows 会话，设备必须允许来自 Xhosted 计算机的 TCP 向后连接。要允许该向后连接，可以使用访问控制来允许 TCP 端口。

  在 XWindows 会话期间，管理器将与已知端口 6000 | n 上的显示器 Xserver 通信。使用以下终端设置，每个显示器都会独立连接到 Xserver：当 *n* 是展示序号时， **setenv DISPLAY Xserver:***n*。

  使用 XDMCP 时，系统将使用 IP 地址协商显示，以便设备可在需要时应用 NAT。XDCMP 检测不支持 PAT。

示例

以下示例显示当前检测配置并禁用XDMCP检测。您可以启用或禁用检测引擎，但不能更改其默认行为。例如，此输出显示 DNS/TCP 检测已禁用。不能使用 **configure inspection** 命令将 DNS 检测配置为应用于 TCP 流量。

```
> show running-config policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect icmp
  inspect icmp error
  inspect dcerpc
!
> configure inspection xdmcp disable
Building configuration...
Cryptochecksum: 46dbea1d 51c2089a fcc3e42f 3dafd2d5
12386 bytes copied in 0.160 secs
[OK]
> show running-config policy-map
!
policy-map type inspect dns preset_dns_map
```

```
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect icmp
  inspect icmp error
  inspect dcerpc
  inspect ftp
!
```

Related Commands

命令	Description
show running-config policy-map	显示服务策略的策略映射，包括检测配置。
show service-policy	显示服务策略统计信息，包括用于检测的统计信息。

configure log-events-to-ramdisk

要启用或禁用将连接事件日志记录到 RAM 磁盘以提高系统性能并减少与将连接事件写入固态驱动器 (SSD) 相关的磁盘磨损，请使用 **configure log-events-to-ramdisk** 命令。

configure log-events-to-ramdisk {**enable** | **disable**}

Syntax Description

enable	启用 RAM 磁盘的连接事件日志记录。
disable	禁用连接事件日志记录到 RAM 磁盘。然后将连接事件记录到 SSD。

Command Default

在支持此功能的平台上会默认启用此功能。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用此命令可在使用 RAM 磁盘或物理 SSD 到日志连接事件之间切换。如果启用，连接事件将记录到 RAM 磁盘中。如果禁用，连接事件将记录到 SSD。在断电的情况下，记录到 RAM 磁盘的连接事件将丢失。

此命令并非在所有设备类型上都可用。在不受支持的平台上运行此命令时，系统会返回以下消息：

```
This command is not available on this platform.
```

示例

以下示例禁用 RAM 磁盘日志记录。

```
> configure log-events-to-ramdisk disable
```

Related Commands

命令	Description
show log-events-to-disk	显示日志记录的当前状态。
show disk-manager	显示系统每个部分（包括孤岛、低水位线和高水位线）的磁盘使用情况详细信息。

configure manager add

要将设备配置为接受来自或启动到 管理中心 和/或 CDO 的连接，请使用 **configure manager add** 命令。

⚠

注意 添加远程管理器会将配置重置为出厂默认设置。

configure manager add { *hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE** } *regkey* [*nat_id*] [*display_name*]

Syntax Description

hostname	指定 管理中心的主机名。
IPv4_address	指定 管理中心的 IPv4 地址。
IPv6_address	指定 管理中心的 IPv6 地址。
display_name	使用 **show managers** 命令提供用于显示此管理器的显示名称。如果您将 CDO 标识为仅用于分析的主用管理器和本地部署 管理中心，则此选项非常有用。如果不指定此参数，防火墙将使用以下方法之一自动生成显示名称： • *hostname* | *IP_address*（如果不使用 **DONTRESOLVE** 关键字） • **manager-***timestamp*
DONTRESOLVE	如果 管理中心无法直接寻址，请使用 **DONTRESOLVE**。如果使用 **DONTRESOLVE**，则需要使用 *nat_id*。当您将此设备添加到 管理中心时，请确保同时指定设备 IP 地址和 *nat_id*；连接的一端需要指定 IP 地址，两端需要指定相同的唯一 NAT ID。
regkey	指定向 管理中心 注册设备所需的唯一字母数字注册密钥。允许使用字母数字和连字符 (-)。
nat_id	当一方未指定 IP 地址时，指定在 管理中心 与设备之间的注册流程中使用的可选字母数字字符串。在 管理中心上指定相同的 NAT ID。如果使用数据接口进行管理，则必须在 threat defense 和 管理中心 上指定注册用的 NAT ID。

Command History

版本	修改
6.1	引入了此命令。
7.2	增加了对多个管理器的支持：主要的云交付 管理中心 (CDO) 和仅用于分析的本地管理器 管理中心 。

使用指南

向 管理中心注册设备始终需要一个唯一的字母数字注册密钥。

通常，需要两个 IP 地址（连同一个注册密钥）： 管理中心 指定设备 IP 地址，设备指定 管理中心 IP 地址。但是，如果您只知道其中一个 IP 地址，您还必须在连接的两端指定唯一的 NAT ID，以建立对初始通信的信任，并查找正确的注册密钥。如果您不知道 管理中心 IP 地址，请使用 **DONTRESOLVE** 关键字而不是 IP 地址或主机名。

注释 如果使用数据接口进行管理，则必须在 threat defense 和d 管理中心 上指定注册用的 NAT ID。

如果注册了 管理中心 和一个使用 IPv4 的设备并要将其转换为 IPv6，则必须在 管理中心删除并重新注册该设备

要从 管理中心 更改为本地 设备管理器，请使用 **configure manager delete** 命令，然后使用 **configure manager local** 命令。

注释 在将设备从一个 管理中心 移动到另一个或更改为本地管理器之前，请将其从当前 管理中心管理器中删除。

示例

```
> configure manager add DONTRESOLVE abc123 efg456
```

Related Commands

命令	Description
configure manager delete	删除管理 管理中心。
configure manager edit	编辑管理 管理中心。
configure manager local	配置本地管理器。
show managers	显示当前的管理器。

configure manager delete

要禁用当前管理器并进入无管理器模式，请使用 **configure manager delete** 命令。

⚠

注意 删除管理器会将 threat defense 配置重置为出厂默认设置。但是，管理引导程序配置会保留。

configure manager delete *identifier*

Syntax Description

identifier	如果定义了多个管理器，则需要指定标识符（也称为 UUID；请参阅 **show managers** 命令）。单独删除每个管理器条目。

Command History

版本	修改
6.1	引入了此命令。
6.3	已添加检查高可用性模式。
7.2	为配置多个管理器时添加了 标识符 变量。

使用指南

使用此命令可删除当前设备管理器(s)。设备处于无管理器模式，然后您可以添加远程管理器(管理中心)或使用本地管理器(设备管理器)。在本地和远程管理之间切换时，或者当远程管理器不再处于活动状态时，可以使用此命令。

如果设备已配置为高可用性，您必须首先使用设备管理器（如果可能）或 **configure high-availability disable** 命令中断高可用性配置。理想情况下，应从主用设备中断高可用性。

命令行为因当前管理器而异。

- 远程 - 无法访问 管理中心 。如果 管理中心 仍与 threat defense 通信，请先从 管理中心的库存中删除设备。然后，您可以使用此命令。
- 本地 - 无限制。您会立即进入无管理器模式。

示例

以下示例删除当前管理器并进入无管理器模式。

```
> configure manager delete

If you enabled any feature licenses, you must disable them in
Firepower Device Manager before deleting the local manager.
Otherwise, those licenses remain assigned to the device in
Cisco Smart Software Manager.
Do you want to continue[yes/no]:yes

DHCP Server Disabled
>
```

Related Commands

命令	Description
configure manager add	为设备配置管理 管理中心 。
configure manager local	配置本地管理器。
show managers	显示当前的管理器。

configure manager edit

要编辑 threat defense 配置中的 管理中心 IP 地址，请使用 **configure manager edit** 命令。

configure manager edit *identifier* { **hostname** { *ip_address* | *hostname* } | **displayname** *display_name* }

Syntax Description

identifier	指定 管理中心的标识符 (UUID)。使用 **show managers** 命令查看标识符（7.2 或更高版本）或从 管理中心 CLI **show version** 命令获取 UUID。
hostname {*ip_address* | *hostname*}	更改主机名/IP 地址。
displayname *display_name*	更改显示名称。

Command History

版本	修改
6.7	引入了此命令。
7.2	添加了 **hostname** 和 **displayname** 关键字。

使用指南

如果更改 管理中心 IP 地址或主机名，还应在设备 CLI 中更改值，以便配置匹配。虽然在大多数情况下，无需更改设备上的管理中心IP地址或主机名即可重新建立管理连接，但在至少一种情况下，必须执行此任务才能重新建立连接：将设备添加到管理中心 并指定仅NAT ID。即使在其他情况下，我们也建议保持 管理中心 IP 地址或主机名为最新状态，以实现额外的网络恢复能力。

如果 管理中心 最初由 **DONTRESOLVE** 和 NAT ID 标识，则可以使用此命令将该值更改为主机名或 IP 地址。不能将 IP 地址或主机名更改为 **DONTRESOLVE**。

管理连接将关闭，然后重新建立。您可以使用 **sftunnel-status** 命令监控连接状态。

示例

管理中心UUID明确标识管理中心；例如，在 管理中心 高可用性的情况下，您需要在threat defense 设备上指定主用 管理中心 。

输入 **show managers** 命令以查看标识符：

```
> show managers
Type                      : Manager
Host                      : 10.10.1.4
Display name              : 10.10.1.4
Identifier                : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration              : Completed
Management type           : Configuration
```

获取 UUID 后，即可编辑 threat defense 设备上的 IP 地址。例如：

```
> configure manager edit f7ffad78-bf16-11ec-a737-baa2f76ef602 10.10.5.1
```

Related Commands

命令	Description
configure manager delete	删除管理 管理中心。
configure manager add	配置 管理中心。
show managers	显示当前的管理器。

configure manager local

要将设备配置为使用本地管理器 设备管理器，请使用 **configure manager local** 命令。

configure manager local

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用此命令可启用本地管理器 设备管理器。当您不想使用单独的管理器时，请使用本地管理器管理中心。通过启用本地管理器，您可以使用位于 **http://***management_ip_address* 的浏览器打开 设备管理器 。

注释 完成此命令最多可能需要 4-6 分钟，因为系统必须重新初始化其数据库。Please be patient.

本地管理器适用于从 6.5 开始的大多数平台。如果它不适用于您的平台，请使用 **configure manager add** 命令配置远程管理器。

其他限制

- 设备必须处于无管理器模式，才能切换到本地管理器。使用 **configure manager delete** 命令进入无管理器模式。使用 **show managers** 命令可确定您当前的管理器。
- 设备不能在透明防火墙模式下运行（请参阅 **configure firewall** 命令）。本地管理器仅支持路由模式。

示例

以下示例显示如何配置本地管理器。

```
> configure manager local
```

Related Commands

命令	Description
configure manager add	为设备配置管理 管理中心 。
configure manager delete	删除管理 管理中心。
show managers	显示当前的管理器。

configure mini-coredump

要启用或禁用迷你核心转储生成，请使用 **configure mini-coredump** 命令。

configure mini-coredump { **enable** | **disable** }

Syntax Description

enable	启用迷你核心转储生成。
disable	禁用迷你核心转储生成。

Command History

版本	修改
7.0	引入了此命令。

使用指南

默认情况下，迷你核心转储生成处于启用状态。

由于其多线程性质，Snort 3 流程会转储巨大的核心文件。这些转储需要一段时间才能写入硬盘。在写入核心并启动新流程之前，Snort的流量检查会中断。创建迷你核心转储可避免时间延迟。迷你核心转储具有有助于调试的堆栈和内存值的基本详细信息。

示例

以下示例禁用迷你核心转储生成。

```
> configure mini-coredump disable
```

Related Commands

命令	Description
show mini-coredump status	显示迷你核心转储生成设置。

configure network dns searchdomains

要配置 DNS 搜索域列表，请使用 **configure network dns searchdomains** 命令。

configure network dns searchdomains ［*dnslist*］

Syntax Description

dnslist	指定 DNS 搜索域列表（用逗号隔开）。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用此命令可将当前的DNS搜索域列表替换为新列表。如果没有在命令中指定完全限定域名，例如 **ping system**，则这些域将添加到主机名中。这些域仅用于管理接口，或通过管理接口的命令。

如果设备是本地管理的高可用性组中的设备，则下次主用设备部署配置更新时，您的更改将被覆盖。如果这是主用设备，您的更改将在部署期间传播到对等设备。

示例

以下示例配置新的搜索域列表，然后 ping 不完全限定的主机名。

```
> configure network dns searchdomains example.com
> show dns system
search example.com
nameserver 10.163.47.11
> ping system www
PING www.example.com (10.163.4.161) 56(84) bytes of data.
64 bytes from www.example.com (10.163.4.161): icmp_seq=1 ttl=242 time=8.01 ms
64 bytes from www.example.com (10.163.4.161): icmp_seq=2 ttl=242 time=16.7 ms
^C
--- origin-www.cisco.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 7.961/10.216/16.718/3.755 ms
```

Related Commands

命令	Description
configure network dns servers	配置 DNS 服务器。
show dns system	显示管理接口的当前 DNS 配置。

configure network dns servers

要为管理接口配置 DNS 服务器，请使用 **configure network dns servers** 命令。

configure nework dns servers ［*dnslist*］

Syntax Description

dnslist	指定 DNS 服务器列表（用逗号隔开）。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用此命令可将当前的DNS服务器列表替换为新列表。这些服务器仅通过管理接口使用。它们无法解析通过数据接口的命令的完全限定域名。

从版本 6.3 开始，仅对于本地管理的设备，如果数据和管理接口使用相同的 DNS 组，则在下次部署时从管理器更新该组，这意味着更改也应用于数据接口上使用的DNS组。管理接口的更改会立即生效。我们建议您从本地管理器进行所有 DNS 更改，而不是使用此命令。

如果设备是本地管理的高可用性组中的设备，则下次主用设备部署配置更新时，您的更改将被覆盖。如果这是主用设备，您的更改将在部署期间传播到对等设备。

示例

以下示例为管理接口配置 DNS 服务器。

```
> configure network dns servers 10.163.47.11,10.124.1.10
> show dns system
search example.com
nameserver 10.163.47.11
nameserver 10.124.1.10
```

Related Commands

命令	Description
configure network dns searchdomains	配置 DNS 搜索域。
show dns system	显示管理接口的当前 DNS 配置。

configure network hostname

要为设备的管理接口配置主机名，请使用 **configure network hostname** 命令。

configure network hostname *name*

Syntax Description

name	指定主机名。

Command History

版本	修改
6.1	引入了此命令。

使用指南

系统主机名在多个位置定义。如果从管理器更新主机名，则系统会在所有进程之间同步主机名。如果在使用 设备管理器 （本地管理器）时使用此命令，则需要从 设备管理器 部署更改以完成更新，以便所有系统进程使用相同的名称。

示例

以下示例将主机名设置为 sfrocks。

```
> configure network hostname sfrocks
```

Related Commands

命令	Description
show network	显示管理接口配置。

configure network http-proxy

要为管理接口配置 HTTP 代理，请使用 **configure network http-proxy** 命令。

configure network http-proxy

Command History

版本	修改
6.1	引入了此命令。
6.6	此命令现在适用于本地管理的系统。

使用指南

使用此命令为设备设置 HTTP 代理地址。发出命令后，系统将提示您 HTTP 代理地址和端口，是否需要进行代理身份验证，如果需要，还会提示代理用户名、代理密码和代理密码确认。

示例

以下示例为管理接口配置 HTTP 代理。在本示例中，配置了身份验证。CLI 不显示您键入的密码。

```
> configure network http-proxy
Manual proxy configuration
Enter HTTP Proxy address: 10.100.10.10
Enter HTTP Proxy Port: 80
Use Proxy Authentication? (y/n) [n]: Y
Enter Proxy Username: proxyuser
Enter Proxy Password: proxypassword
Confirm Proxy Password: proxypassword
```

Related Commands

命令	Description
configure network http-proxy-disable	禁用 HTTP 代理设置。
show network	显示管理接口配置。

configure network http-proxy-disable

要删除管理接口的 HTTP 代理，请使用 **configure network http-proxy-disable** 命令。

configure network http-proxy-disable

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例删除管理接口的 HTTP 代理。

```
> show network
(...Output Truncated...)
===============[ Proxy Information ]================
State                        : Enabled
HTTP Proxy                   : 10.100.10.10
Port                         : 80
Authentication               : Enabled
Username                     : proxyuser
> configure network http-proxy-disable
Are you sure that you wish to delete the current http-proxy configuration? (y/n): y
Configuration successfully deleted.
> show network
(...Output Truncated...)
===============[ Proxy Information ]================
State                        : Disabled
Authentication               : Disabled
```

Related Commands

命令	Description
configure network http-proxy	配置 HTTP 代理设置。
show network	显示管理接口配置。

configure network ipv4 delete

要禁用设备管理接口的 IPv4 配置，请使用 **configure network ipv4 delete** 命令。

configure network ipv4 delete ［*management_interface*］

Syntax Description

management_ interface	指定管理接口。如果不指定接口，则此命令将配置默认管理接口。仅当使用 **configure management-interface** 命令启用多个管理接口时，才需要此参数。仅在 Firepower 4100 和 9300 系列设备上支持多个管理接口。请勿为其他平台指定此参数。在 Firepower 4100 和 9300 上的管理接口 ID 为 **management0**（对于默认管理接口）和 **management1**（对于可选事件接口）。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用此命令以禁用设备管理接口的 IPv4 配置。如果您连接到已删除的 IP 地址，您将失去与该设备的连接。在删除 IPv4 地址之前，请确保已配置 IPv6 地址。

您无需删除配置即可更改 IPv4 地址。如果要保留 IPv4 地址，但只想更改地址，请使用 **configure network ipv4 manual** 或 **configure network ipv4 dhcp** 命令。

示例

以下示例删除 IPv4 地址配置。

```
> configure network ipv4 delete
```

Related Commands

命令	Description
configure network ipv4 dhcp	将 IPv4 配置为从 DHCP 服务器获取地址。
configure network ipv4 manual	使用静态 IP 地址手动配置 IPv4。
show network	显示管理接口配置。

configure network ipv4 dhcp

要将管理接口配置为从 DHCP 服务器获取 IPv4 地址，请使用 **configure network ipv4 dhcp** 命令。

configure network ipv4 dhcp ［*management_interface*］

Syntax Description

management_ interface	指定管理接口。仅在默认管理接口上支持 DHCP，因此您不需要使用此参数。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用此命令可指定设备的管理接口从 DHCP 服务器接收其 IPv4 配置。管理接口与 DHCP 服务器通信以获取其配置信息。

注释 如果使用 **configure network management-data-interface** 命令配置数据接口进行 管理中心 访问，则无法将 DHCP 用于管理接口；您必须设置手动 IP 地址，因为默认路由（必须是**数据接口**）可能会被从 DHCP 服务器接收的路由覆盖。虽然您不打算使用管理接口，但必须设置 IP 地址，例如专用地址。当流量转发到数据接口时，此 IP 地址将进行 NAT 转换。

示例

以下示例将管理接口配置为使用 DHCP 获取其 IPv4 地址。

```
> configure network ipv4 dhcp
```

Related Commands

命令	Description
configure network ipv4 delete	禁用 IPv4 网络。
configure network ipv4 manual	手动配置 IPv4。
show network	显示管理接口配置。

configure network ipv4 dhcp-dp-route

要恢复管理接口默认 IP 地址、网络掩码和网关，请使用 **configure network ipv4 dhcp-dp-route** 命令。此命令不会更改其他网络设置，例如 DNS 服务器。

注释 Cisco Secure Firewall Threat Defense Virtual (threat defense virtual)、 Firepower 4100/9300或 ISA 3000 不支持此命令。

configure network ipv4 dhcp-dp-route

Command History

版本	修改
6.6	引入了此命令。

使用指南

您必须同时输入此命令的 IPv4 和 IPv6 版本，才能将配置恢复为出厂默认设置，即使您没有识别其中一个版本的 IP 地址。

示例

以下示例恢复管理接口的默认配置。

```
> configure network ipv4 dhcp-dp-route
Creating /etc/sf/sftunnel.conf with header line
Set up management0 as DHCP ipv4 client with the default route through data interfaces.
>
```

Related Commands

命令	Description
configure network ipv4 delete	禁用 IPv4 网络。
configure network ipv4 dhcp	通过 DHCP 配置 IPv4。
configure network ipv4 manual	手动配置 IPv4。
show network	显示管理接口配置。

configure network ipv4 dhcp-server-disable

要在管理接口上禁用 DHCP 服务器，请使用 **configure network ipv4 dhcp-server-disable** 命令。

configure network ipv4 dhcp-server-disable

Command History

版本	修改
6.2	引入了此命令。

使用指南

如果管理接口上有活动的 DHCP 服务器，则可以将其禁用。禁用时，管理网络上的客户端必须配置静态地址，或者您需要在网络上配置其他设备来提供 DHCP 服务器服务。

如果将管理 IP 地址更改为使用 DHCP 获取地址，则会自动禁用 DHCP 服务器（如果已启用）。

示例

以下示例显示如何检查 DHCP 服务器是否已启用，以及如何禁用它。

```
> show network-dhcp-server
DHCP Server Enabled
192.168.45.46-192.168.45.254
> configure network ipv4 dhcp-server-disable
DCHP Server Disabled
> show network-dhcp-server
DHCP Server Disabled
```

Related Commands

命令	Description
configure network ipv4 dhcp-server-enable	启用管理接口上的 DHCP 服务器。
show dhcp-server	显示管理接口上的 DHCP 服务器的状态。

configure network ipv4 dhcp-server-enable

要在管理接口上启用可选的 DHCP 服务器，请使用 **configure network ipv4 dhcp-server-enable** 命令。

configure network ipv4 dhcp-server-enable *start_ip_address end_ip_address*

Syntax Description

start_ip_address *end_ip_address*	指定 DHCP 地址池的起始和结束 IPv4 地址。当管理接口收到 DHCP 客户端请求时，它会提供此池中的地址。该池必须与管理 IPv4 地址位于同一子网上。 请勿在 DHCP 地址池中包含网络地址、管理地址或广播地址。

Command History

版本	修改
6.2	引入了此命令。

使用指南

如果为管理接口配置手动（静态）IPv4 地址，则可以配置 DHCP 服务器为管理网络上的终端提供地址。

在启用服务器之前，请确保管理网络上没有其他 DHCP 服务器。每个网络最多只能有一个 DHCP 服务器，否则结果可能无法预测。

注释 threat defense virtual 设备上不支持此命令。

示例

以下示例显示如何配置 DHCP 服务器并显示其状态。

```
> configure network ipv4 dhcp-server-enable 192.168.45.46 192.168.45.254
DHCP Server Enabled
> show network-dhcp-server
DHCP Server Enabled
192.168.45.46-192.168.45.254
```

Related Commands

命令	Description
configure network ipv4 dhcp-server-disable	禁用管理接口上的 DHCP 服务器。
show dhcp-server	显示管理接口上的 DHCP 服务器的状态。

configure network ipv4 manual

要在管理接口上配置静态 IPv4 地址，请使用 **configure network ipv4 manual** 命令。

configure network ipv4 manual *ipaddr netmask gw* [*management_interface*]

Syntax Description

ipaddr	指定 IP 地址。
netmask	指定子网掩码。
gw	指定默认网关的 IPv4 地址。 您可以选择指定 **data-interfaces**，它将设备上的数据接口用作网关，而不是管理网络上的显式网关。如果不想将管理物理接口连接到单独的管理网络，请使用数据接口。 有关 管理中心 数据接口管理，请参阅 **configure network management-data-interface** 命令。 请注意，此命令中的*gw*用于为设备创建默认路由。如果配置仅事件接口，则必须输入 *gw* 作为命令的一部分；但是，此条目只是将默认路由配置为您指定的值，并且不会为事件接口创建单独的静态路由。如果您在与管理接口不同的网络上使用仅事件接口，我们建议您将 *gw* 设置为与管理接口配合使用，然后使用 **configure network static-routes** 命令单独为仅事件接口创建静态路由。
management_ interface	指定管理接口。如果不指定接口，则此命令将配置默认管理接口。仅当使用 **configure management-interface** 命令启用多个管理接口时，才需要此参数。仅在 Firepower 4100 和 9300 系列设备上支持多个管理接口。请勿为其他平台指定此参数。在 Firepower 4100 和 9300 上的管理接口 ID 为 **management0**（对于默认管理接口）和 **management1**（对于可选事件接口）。

Command History

版本	修改
6.1	引入了此命令。
6.2	为网关添加了 **data-interfaces** 关键字。
6.7	**data-interfaces** 关键字现在可用于数据接口上的 管理中心 管理。

使用指南

如果使用 **configure network management-data-interface** 命令为访问 管理中心 配置数据接口，则必须手动设置 IP 地址（IPv4 或 IPv6）。虽然您不打算使用管理接口，但必须设置 IP 地址，例如专用地址。当流量转发到数据接口时，此 IP 地址将进行 NAT 转换。您无法使用 DHCP（默认），因为默认路由（必须是 **数据接口**）可能会被从 DHCP 服务器收到的路由覆盖。

示例

以下示例在管理接口上配置静态 IPv4 地址。

```
> configure network ipv4 manual 10.123.1.10 255.255.0.0 10.123.1.1
```

Related Commands

命令	Description
configure network ipv4 delete	禁用 IPv4 网络。
configure network ipv4 dhcp	通过 DHCP 配置 IPv4。
show network	显示管理接口配置。

configure network ipv6 delete

要禁用设备管理接口的 IPv6 配置，请使用 **configure network ipv4 delete** 命令。

configure network ipv6 delete ［*management_interface*］

Syntax Description

management_ interface	指定管理接口。如果不指定接口，则此命令将配置默认管理接口。仅当使用 **configure management-interface** 命令启用多个管理接口时，才需要此参数。仅在 Firepower 4100 和 9300 系列设备上支持多个管理接口。请勿为其他平台指定此参数。在 Firepower 4100 和 9300 上的管理接口 ID 为 **management0**（对于默认管理接口）和 **management1**（对于可选事件接口）。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用此命令以禁用设备管理接口的 IPv6 配置。如果您连接到已删除的 IP 地址，您将失去与该设备的连接。在删除 IPv6 地址之前，请确保已配置 IPv4 地址。

您无需删除配置即可更改 IPv6 地址。如果要保留 IPv6 寻址，但只想更改地址，请使用 **configure network ipv6** {**manual** | **dhcp** | **router**} 命令。

示例

以下示例删除 IPv6 地址配置。

```
> configure network ipv6 delete
```

Related Commands

命令	Description
configure network ipv6 dhcp	通过 DHCP 配置 IPv6。
configure network ipv6 manual	手动配置 IPv6。
configure network ipv6 router	通过路由器配置 IPv6。
show network	显示管理接口配置。

configure network ipv6 destination-unreachable

要在管理接口上使用 IPv6 时启用或禁用 ICMPv6 目标不可达数据包，请使用 **configure network ipv6 destination-unreachable** 命令。

configure network ipv6 destination-unreachable {**enable** | **disable**}

Syntax Description

enable	启用目标不可达数据包。该设置为默认设置。
disable	禁用目标不可达数据包。

Command Default

默认启用。

Command History

版本	修改
6.4.0	命令已添加。

使用指南

您可能希望禁用这些数据包以防止潜在的拒绝服务攻击。

示例

以下示例禁用“目的地不可达”消息。

```
> configure network ipv6 destination-unreachable disable
```

Related Commands

命令	Description
configure network ipv6 delete	禁用 IPv6 网络。
configure network ipv6 echo-reply	启用或禁用回应应答数据包。
configure network ipv6 manual	手动配置 IPv6 地址。
configure network ipv6 router	通过路由器配置 IPv6。
show network	显示管理接口配置。

configure network ipv6 dhcp

要将管理接口配置为从 DHCP 服务器获取 IPv6 地址，请使用 **configure network ipv6 dhcp** 命令。

configure network ipv6 dhcp ［*management_interface*］

Syntax Description

management_ interface	指定管理接口。仅在默认管理接口上支持DHCP，因此您不需要使用此参数。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用此命令可指定设备的管理接口从 DHCP 服务器接收其 IPv6 配置。管理接口与 DHCP 服务器通信以获取其配置信息。

注释 如果使用 **configure network management-data-interface** 命令配置数据接口进行 管理中心 访问，则无法将 DHCP 用于管理接口；您必须设置手动 IP 地址，因为默认路由（必须是**数据接口**）可能会被从 DHCP 服务器接收的路由覆盖。虽然您不打算使用管理接口，但必须设置 IP 地址，例如专用地址。当流量转发到数据接口时，此 IP 地址将进行 NAT 转换。

示例

以下示例将管理接口配置为使用 DHCP 获取其 IPv6 地址。

```
> configure network ipv6 dhcp
```

Related Commands

命令	Description
configure network ipv6 delete	禁用 IPv6 网络。
configure network ipv6 manual	手动配置 IPv6。
configure network ipv6 router	通过路由器配置 IPv6。
show network	显示管理接口配置。

configure network ipv6 dhcp-dp-route

要恢复管理接口默认 IP 地址、网络掩码和网关，请使用 **configure network ipv6 dhcp-dp-route** 命令。此命令不会更改其他网络设置，例如 DNS 服务器。

注释 threat defense virtual、Firepower 4100/9300或 ISA 3000 不支持此命令。

configure network ipv6 dhcp-dp-route

Command History

版本	修改
6.6	引入了此命令。

使用指南

您必须同时输入此命令的 IPv4 和 IPv6 版本，才能将配置恢复为出厂默认设置，即使您没有识别其中一个版本的 IP 地址。

示例

以下示例恢复管理接口的默认配置。

```
> configure network ipv6 dhcp-dp-route
Set up management0 as DHCP ipv6 client with the default route through data interfaces.
>
```

Related Commands

命令	Description
configure network ipv6 delete	禁用 IPv6 网络。
configure network ipv6 dhcp	通过 DHCP 配置 IPv6。
configure network ipv6 manual	手动配置 IPv6 地址。
show network	显示管理接口配置。

configure network ipv6 echo-reply

要在管理接口上使用 IPv6 时启用或禁用 ICMPv6 回应应答数据包，请使用 **configure network ipv6 echo-reply** 命令。

configure network ipv6 echo-reply {**enable** | **disable**}

Syntax Description

enable	启用回应应答数据包。该设置为默认设置。
disable	禁用回应应答数据包。

Command Default

默认启用。

Command History

版本	修改
6.4.0	命令已添加。

使用指南

您可能希望禁用这些数据包以防止潜在的拒绝服务攻击。禁用回应应答数据包意味着无法使用 IPv6 ping 到设备管理接口，以进行测试。

示例

以下示例禁用回应应答消息。

```
> configure network ipv6 echo-reply disable
```

Related Commands

命令	Description
configure network ipv6 delete	禁用 IPv6 网络。
configure network ipv6 destination-unreachable	启用或禁用目标不可达数据包。
configure network ipv6 manual	手动配置 IPv6 地址。
configure network ipv6 router	通过路由器配置 IPv6。
show network	显示管理接口配置。

configure network ipv6 manual

要在管理接口上配置静态 IPv6 地址，请使用 **configure network ipv6 manual** 命令。

configure network ipv6 manual *ip6addr ip6prefix* ［*ip6gw*］［*management_interface*］

Syntax Description

ip6addr	指定 IP 地址。
ip6prefix	指定前缀长度。
ip6gw	指定默认网关的 IPv6 地址。 您可以选择指定 **data-interfaces**，它将设备上的数据接口用作网关，而不是管理网络上的显式网关。如果不想将管理物理接口连接到单独的管理网络，请使用数据接口。 有关 管理中心 数据接口管理，请参阅 **configure network management-data-interface** 命令。 请注意，此命令中的 *ip6gw* 用于为设备创建默认路由。如果配置仅事件接口，则必须输入 *ip6gw* 作为命令的一部分；但是，此条目只是将默认路由配置为您指定的值，并且不会为事件接口创建单独的静态路由。如果您在与管理接口不同的网络上使用仅事件接口，我们建议您将 *ip6gw* 设置为与管理接口配合使用，然后使用 **configure network static-routes** 命令单独为仅事件接口创建静态路由。
management_ interface	指定管理接口。如果不指定接口，则此命令将配置默认管理接口。仅当使用 **configure management-interface** 命令启用多个管理接口时，才需要此参数。仅在 Firepower 4100 和 9300 系列设备上支持多个管理接口。请勿为其他平台指定此参数。在 Firepower 4100 和 9300 上的管理接口 ID 为 **management0**（对于默认管理接口）和 **management1**（对于可选事件接口）。

Command History

版本	修改
6.1	引入了此命令。
6.2	为网关添加了 **data-interfaces** 关键字。
6.7	**data-interfaces** 关键字现在可用于在数据接口上进行 管理中心 管理。

使用指南

如果使用 **configure network management-data-interface** 命令配置数据接口以访问 管理中心，则必须手动设置 IP 地址（IPv4 或 IPv6）。虽然您不打算使用管理接口，但必须设置 IP 地址，例如专用地址。当流量转发到数据接口时，此 IP 地址将进行 NAT 转换。您无法使用 DHCP（默认），因为默认路由（必须是 **数据接口**）可能会被从 DHCP 服务器收到的路由覆盖。

示例

以下示例为管理接口配置静态 IPv6 地址。

```
> configure network ipv6 manual 2001:DB8:3ffe:1900:4545:3:200:f8ff:fe21:67cf 64
```

Related Commands

命令	Description
configure network ipv6 delete	禁用 IPv6 网络。
configure network ipv6 dhcp	通过 DHCP 配置 IPv6。
configure network ipv6 router	通过路由器配置 IPv6。
show network	显示管理接口配置。

configure network ipv6 router

要将管理接口配置为使用无状态自动配置从路由器获取 IPv6 地址，请使用 **configure network ipv6 router** 命令。

configure network ipv6 router ［*management_interface*］

Syntax Description

management_ interface	指定管理接口。如果不指定接口，则此命令将配置默认管理接口。仅当使用 **configure management-interface** 命令启用多个管理接口时，才需要此参数。仅在 Firepower 4100 和 9300 系列设备上支持多个管理接口。请勿为其他平台指定此参数。在 Firepower 4100 和 9300 上的管理接口 ID 为 **management0**（对于默认管理接口）和 **management1**（对于可选事件接口）。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用此命令可指定设备的管理接口从路由器接收其 IPv6 配置。管理接口与 IPv6 路由器通信以获取其配置信息。

示例

以下示例使用无状态自动配置将管理接口配置为从路由器接收其 IPv6 地址。

```
> configure network ipv6 router
```

Related Commands

命令	Description
configure network ipv6 delete	禁用 IPv6 网络。
configure network ipv6 dhcp	通过 DHCP 配置 IPv6。
configure network ipv6 manual	手动配置 IPv6。
show network	显示管理接口配置。

configure network management-data-interface

要配置用于 管理中心 管理的数据接口而不是管理接口，请使用 **configure network management-data-interface** 命令。

configure network managament-data-interface [{ **ipv4** { **dhcp** | [**manual** *ip_address netmask*] [**default-gw** *gateway_ip*] } | **ipv6** { **manual** *ip_address prefix*] [**default-gw** *gateway_ip*] } | **ddns update-url** **https://** *username* **:** *password* **@** *provider-domain* **/** *path* **?hostname=<h>&myip=<a>** | **nameif** *name* | **client** *ip_address mask-or-prefix* | } **interface** *id* | **disable**]

Syntax Description

ipv4	为 IP 地址指定 IPv4。
ipv6	为 IP 地址指定 IPv6。
dhcp	为 IPv4 地址指定 DHCP。
manual *ip_address netmask-or-prefix*	指定手动 IP 地址和网络掩码或前缀。
default-gw *gateway_ip*	指定默认网关的 IP 地址。 如果在 CLI 中编辑辅助接口，您将无法配置网关或以其他方式更改默认路由，因为只能在 管理中心 中编辑此接口的静态路由。
ddns update-url **https://** *username* **:** *password* **@** *provider-domain* **/** *path* **?hostname=<h>&myip=<a>**	指定 DDNS Web 类型更新 URL。在 DDNS 提供商处指定用户名和密码。请向您的 DDNS 提供商咨询正确的路径。 在输入问号 (？) 字符之前，请同时按 Ctrl + V 键。这样，你就可以输入“?”，软件也不会将“?”解释为帮助查询。 虽然这些关键字看起来像参数，但您需要在 URL 末尾逐字输入此文本。这种 threat defense 将自动替换<h>发送 DDNS 更新时包含主机名和 IP 地址的 <a> 字段。
nameif 名称	设置接口的名称。
client *ip_address*	限制在特定网络上通过数据接口访问 管理中心 。请注意，当您输入不带参数的 **configure network managament-data-interface** 命令时，此关键字不是向导的一部分。
interface *ID*	指定要用于 管理中心 管理访问的数据接口 ID。您只能指定一个数据接口进行 管理中心 访问。
disable	禁用数据接口上的 管理中心 管理访问。

Command History

版本	修改
6.7	引入了此命令。

版本	修改
7.3	在 管理中心中添加辅助管理接口后，可以使用此命令在 CLI 中编辑其某些设置。

使用指南

如果首次配置此命令时未指定任何参数，系统将提示您配置数据接口的基本网络设置。

注释 使用此命令时，应使用控制台端口。如果使用 SSH 访问管理接口，连接可能会断开，您必须重新连接到控制台端口。有关 SSH 用法的详细信息，请参阅下文。

如果在管理中心 中配置了辅助管理接口，则可以使用此命令对其进行编辑。您无法在 CLI 中手动添加辅助接口；您必须使用 管理中心。

请参阅以下有关使用此命令的详细信息：

- 如果您要使用数据接口进行管理，则原始管理接口无法使用 DHCP。如果在初始设置期间没有手动设置 IP 地址，则可以使用 **configure network** {**ipv4** | **ipv6**} **manual** 命令立即设置它。如果您尚未将管理接口网关设置为 **data-interfaces**，此命令将立即设置它。
- 从数据接口进行管理中心 访问具有以下限制：
  - 只能在 物理数据接口上启用管理器访问。不能使用子接口或 EtherChannel。 您还可以使用管理中心 在单个辅助接口上启用管理器访问，以实现冗余。
  - 此接口不能是仅管理接口。
  - 仅路由防火墙模式，使用路由接口。
  - 不支持 PPPoE。如果您的 ISP 需要 PPPoE，则必须在 威胁防御 与 WAN 调制解调器之间放入支持 PPPoE 的路由器。
  - 接口只能位于全局 VRF 中。
  - 默认不对数据接口启用 SSH，因此必须稍后使用 管理中心 来启用 SSH。由于管理接口网关将更改为数据接口，因此您也无法启动从远程网络到管理接口的 SSH 会话，除非您使用 **configure network static-routes** 命令为管理接口添加静态路由。对于 Amazon Web 服务上的 threat defense virtual ，控制台端口不可用，因此您应保持对管理接口的 SSH 访问：在继续配置之前为管理添加静态路由。或者，请确保在配置用于管理器访问的数据接口并断开连接之前完成所有 CLI 配置（包括 **configure manager add** 命令）。
  - 您不能使用单独的管理接口和仅事件接口。
  - 不支持高可用性。在这种情况下，必须使用管理接口。
  - 不支持集群技术。在这种情况下，必须使用管理接口。
- 当您将 threat defense 添加到 管理中心时， 管理中心 会发现并维护接口配置，包括以下设置：接口名称和 IP 地址、网关静态路由、DNS 服务器和 DDNS 服务器。有关 DNS 服务器配置的详

细信息，请参阅下文。在 管理中心 中，您可以稍后对 管理中心 访问接口配置进行更改，但要确保更改不会阻止 threat defense 或 管理中心 重新建立管理连接。如果管理连接中断， threat defense 将包含 **configure policy rollback** 命令以恢复以前的部署。

- 如果配置 DDNS 服务器更新 URL，则 threat defense 会自动添加来自 Cisco 受信任根 CA 捆绑包的所有主要 CA 证书，以便 threat defense 可以验证用于 HTTPS 连接的 DDNS 服务器证书。 threat defense 支持使用 DynDNS 远程 API 规范 (https://help.dyn.com/remote-access-api/) 的任何 DDNS 服务器。
- 此命令设置数据接口 DNS 服务器。使用设置脚本（或使用 **configure network dns servers** 命令）设置的管理 DNS 服务器用于管理流量。数据 DNS 服务器用于 DDNS（如果已配置）或适用于此接口的安全策略。

  在 管理中心 上，数据接口 DNS 服务器在您分配给此 threat defense 的平台设置策略中配置。当您将 threat defense 添加到 管理中心 时，本地设置将保留，并且 DNS 服务器不会添加到平台设置策略。但是，如果稍后将平台设置策略分配给包含 DNS 配置的 threat defense，则该配置将覆盖本地设置。我们建议您主动配置与此设置匹配的 DNS 平台设置，以使 管理中心 和 threat defense 同步。

  此外，仅当在初始注册时发现 DNS 服务器，管理中心 才会保留本地 DNS 服务器。例如，如果您使用管理接口注册了设备，但随后使用 **configure network management-data-interface** 命令配置数据接口，则必须在 管理中心中手动配置所有这些设置（包括 DNS 服务器），以便与 threat defense 配置匹配。
- 将 threat defense 注册到 管理中心 后，您可以将该管理接口更改为管理接口或另一数据接口。
- 您在安装向导中设置的 FQDN 将用于此接口。
- 您可以通过命令清除整个设备配置；在恢复场景中可使用此选项，但我们不建议您在初始设置或正常操作中使用它。
- 要禁用数据管理，请输入 **configure network management-data-interface disable** 命令。

示例

以下示例使用 DHCP 将以太网接口 1/1 设置为 管理中心 管理接口。

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]:
IP address (manual / dhcp) [dhcp]:
DDNS server update URL [none]:
https://jcrichton:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow FMC access from any network, if you wish to change
 the FMC access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

以下示例使用手动 IP 地址将以太网接口 1/1 设置为 管理中心 管理接口。

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow FMC access from any network, if you wish to change
 the FMC access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

Related Commands

命令	Description
configure network ipv4 manual	使用手动 IPv4 IP 地址配置管理接口。
configure network ipv6 manual	使用手动 IPv6 IP 地址配置管理接口。
configure policy rollback	如果管理连接中断， 将恢复以前的部署。
show network	显示管理接口配置。

configure network management-interface

要在 Firepower 4100 或 9300 系列设备上配置多个管理接口以分隔事件和管理流量，请使用 **configure network management-interface** 命令。对于 threat defense，多个管理接口仅适用于 Firepower 4100 和 9300 系列设备。您还可以使用此命令设置用于 管理中心 通信的 MTU 和 TCP 端口。

configure network management-interface { [**disable** | **disable-event-channel** | **disable-management-channel** | **enable** | **enable-event-channel** | **enable-management-channel**] *interface_id*] | **tcpport** *number* | **mtu-event-channel** [*bytes*] | **mtu-management-channel** [*bytes*] }

Syntax Description

disable	禁用指定的管理接口。
disable-event-channel	在指定的接口上禁用事件信道。
disable-management-channel	在指定的接口上禁用管理信道。
enable	启用指定的管理接口。
enable-event-channel	在指定的接口上启用事件信道。
enable-management-channel	在指定的接口上启用管理信道。
interface_id	指定要启用或禁用的管理接口， **management0** 或 **management1**。management0 和 management1 是这些接口的内部名称，而不考虑物理接口 ID。
tcpport *number*	配置用于与 管理中心通信的 TCP 端口。默认值为 8305。如果更改默认值，请勿指定 SSH (22) 或 HTTPS (443) 端口。保持数字在 1024 以上的高范围内，最高可达 65535。此命令与 **configure network management-port** 命令等效：
mtu-event-channel [*bytes*]	设置事件接口的 MTU，以字节为单位，如果启用 IPv4，该值可以介于 64 和 9000 之间；如果启用 IPv6，该值可以介于 1280 和 9000 之间。如果同时启用 IPv4 和 IPv6，则最小值为 1280。如果不输入字节，系统会提示您输入值。此命令与 **configure network mtu** 命令等效：
mtu-management-channel [*bytes*]	设置管理接口的 MTU，以字节为单位，如果启用 IPv4，该值可以介于 64 和 1500 之间；如果启用 IPv6，该值可以介于 1280 和 1500 之间。如果同时启用 IPv4 和 IPv6，则最小值为 1280。如果不输入字节，系统会提示您输入值。此命令与 **configure network mtu** 命令等效： **注释** 如果设置了 非常 低的 MTU，设备管理器 性能可能会受到影响。

Command Default

management0 接口已启用，并用于事件和管理流量。 management1 已禁用。

默认 UDP 端口为 8305。

管理和事件的默认 MTU 为 1500。

Command History

版本	修改
6.1	引入了此命令。
6.6	我们添加了 **mtu-event-channel** 和 **mtu-management-channel** 关键字。

使用指南

对于设备管理，管理中心管理接口承载两个单独的流量信道：管理流量信道承载所有内部流量（如特定于设备管理的设备间流量），而事件流量通道承载所有事件流量（如 Web 事件）。您可以选择在 管理中心 中配置单独的仅事件接口来处理事件流量（请参阅 管理中心 Web 界面以执行此配置）。只能配置一个仅事件接口。事件流量这能会占用大量带宽，因此将事件流量从管理流量中分离出来可以提高 管理中心的性能。

在 Firepower 4100 和 9300 系列设备上，分配给逻辑设备的管理类型接口被指定为 threat defense 应用中的默认 management0 接口。默认情况下，此接口包括管理信道和事件通道。如果在 管理中心上配置了单独的事件接口，则在 Firepower 4100 或 9300 设备上，可以选择将事件类型接口分配给 threat defense 逻辑设备，以利用这种分离。此接口被指定为 management1 接口。如果可能，在设备事件接口和 管理中心事件接口之间发送事件流量。如果事件网络关闭，则事件流量将恢复到默认管理接口。尽可能使用单独的事件接口，但管理接口始终为备用接口。

管理中心仅事件接口不能接受管理通道流量，因此您应在设备事件接口上禁用管理通道。您可以选择为管理接口禁用事件。不管是哪种情况，设备都会尝试通过事件专属接口发送事件，如果该接口关闭，那么即使您禁用了事件信道，设备也会通过管理接口发送事件。

将事件接口分配给逻辑设备后，此接口不会启用或配置网络设置。您必须访问 threat defense CLI 并使用 **configure network management-interface** 命令启用它。然后使用 **configure network** {**ipv4** | **ipv6**} **manual** 命令来配置接口的地址。

示例

以下示例启用 management1，并禁用管理信道。默认情况下，两个信道均已启用。

```
> configure network management-interface enable management1
> configure network management-interface disable-management-channel management1
>
```

以下示例更改用于与 管理中心通信的端口。

```
> configure network management-interface tcpport 8306
Management port changed to 8306.
```

以下示例将事件接口上的 MTU 设置为 9000。

```
> configure network management-interface mtu-event-channel 9000
```

```
MTU set successfully to 9000 from 1500 for management1
Refreshing Network Config...
Interface management1 speed is set to '10000baseT/Full'
>
```

以下示例使用 CLI 提示符将管理接口上的 MTU 设置为 1400。

```
> configure network management-interface mtu-management-channel
Do you want to change the MTU [1500] for management0 interface?(Yes/No): Yes
Enter the new value for MTU [1500]> 1400
MTU set successfully to 1400 from 1500 for management0
Refreshing Network Config...
Interface management0 speed is set to '10000baseT/Full'
>
```

Related Commands

命令	Description
configure network mtu	设置管理或事件接口 MTU。
configure network static-routes ipv4/ipv6	为管理接口配置静态路由。
show network	显示管理接口配置。

configure network management-port

要配置用于与 管理中心通信的 TCP 端口，请使用 **configure network management-port** 命令。

configure network management-port 编号

Syntax Description

number	配置用于与 管理中心通信的 TCP 端口。默认值为 8305。如果更改默认值，请勿指定 SSH (22) 或 HTTPS (443) 端口。保持数字在 1024 以上的高范围内，最高可达 65535。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用此命令可将用于管理连接的端口更改为管理中心。此命令不会更改用于本地管理器设备管理器的端口。此命令等同于**configure network management-interface tcpport** 命令；您不需要同时使用这两个命令。

示例

以下示例更改用于与 管理中心通信的端口。

```
> configure network management-port 8306
Management port changed to 8306.
```

Related Commands

命令	Description
configure network ipv4	为管理接口配置 IPv4 寻址。
configure network ipv6	为管理接口配置 IPv6 寻址。
show network	显示管理接口配置。

configure network mtu

要为管理或事件接口配置 MTU，请使用 **configure network mtu** 命令。

configure network mtu ［ *interface_id* ］ ［ *bytes* ］

Syntax Description

bytes	（可选）以字节为单位设置 MTU。对于管理接口，如果启用 IPv4，则值可以介于 64 和 1500 之间；如果启用 IPv6，则值可以介于 1280 和 1500 之间。 对于事件接口，如果启用 IPv4，该值可以介于 64 和 9000 之间；如果启用 IPv6，该值可以介于 1280 和 9000 之间。 如果同时启用 IPv4 和 IPv6，则最小值为 1280。如果不输入 字节，系统会提示您输入值。 **注释** 如果设置了 非常 低的 MTU，设备管理器 性能可能会受到影响。
interface_id	（可选）- 指定要设置 MTU 的接口 ID。使用 **show network** 命令查看可用的接口 ID，例如 management0、management1、br1 和 eth0，具体取决于平台。如果未指定接口，则使用管理接口。

Command Default

管理和事件的默认 MTU 为 1500。

Command History

版本	修改
6.6	引入了此命令。

使用指南

此命令等同于 和 命令；您不需要同时使用 **configure network management-interface mtu-event-channel** 和 **configure network management-interface mtu-management-channel** 命令。

示例

以下示例将事件接口 management1 上的 MTU 设置为 8192。

```
> configure network mtu 8192 management1
MTU set successfully to 8192 from 1500 for management1
Refreshing Network Config...
NetworkSettings::refreshNetworkConfig MTU value at start 8192

Interface management1 speed is set to '10000baseT/Full'
NetworkSettings::refreshNetworkConfig MTU value at end 8192
>
```

以下示例使用 CLI 提示符将管理接口上的 MTU 设置为 1400。

```
> configure network mtu
Do you want to change the MTU [1500] for management0 interface?(Yes/No): Yes
Enter the new value for MTU [1500]> 1400
MTU set successfully to 1400 from 1500 for management0
Refreshing Network Config...
Interface management0 speed is set to '10000baseT/Full'
>
```

Related Commands

命令	Description
configure network ipv4	为管理接口配置 IPv4 寻址。
configure network ipv6	为管理接口配置 IPv6 寻址。
configure network management-interface	设置管理或事件接口 MTU。
show network	显示管理接口配置。

configure network speed

要设置管理接口或数据接口的速度，请使用 **configure network speed** 命令。

注释 仅在 Secure Firewall 3100 上支持此命令。

configure network speed { *speed* | **sfp-detect** [*interface_id*]

Syntax Description

interface_id	（可选）指定要设置速度的接口 ID。默认值为 management0。
sfp-detect	检测已安装的SFP模块的速度并使用适当的速度。该设置为默认设置。复用始终为全复用，并且始终启用自动协商。如果您稍后将网络模块更改为其他型号，并希望速度自动更新，则此选项非常有用。
速度	将速度设置为特定速度。可用速度因接口而异。

Command Default

默认速度为 **sfp-detect**。

Command History

版本	修改
7.1	此命令是为安全防火墙 3100 引入的。

使用指南

我们建议使用默认 **sfp-detect**，除非您想将速度设置为特定速度，而不考虑 SFP 功能。

示例

以下示例将管理接口 management0 上的速度设置为 1gbps。

```
> configure network speed 1gbps
```

Related Commands

命令	Description
configure network ipv4	为管理接口配置 IPv4 寻址。
configure network ipv6	为管理接口配置 IPv6 寻址。
configure network management-interface	设置管理或事件接口 MTU。
show network	显示管理接口配置。

configure network static-routes

要添加或删除静态路由，请使用此命令的 **configure network static-routes** 形式。

configure network static-routes {**ipv4** | **ipv6**} {**add** *interface destination netmask_or_prefix gateway* | **delete**}

Syntax Description

add	为管理接口添加静态路由。
delete	为管理接口删除静态路由。系统会提示您选择要删除的路由。
interface	管理接口的 ID。使用 **show network** 命令查看您的型号的管理接口 ID。
ipv4	添加或删除 IPv4 管理地址的静态路由。
ipv6	添加或删除 IPv6 管理地址的静态路由。
destination	要添加或删除的目标 IP 地址，采用 IPv4 或 IPv6 格式（视情况而定）。例如，10.100.10.10 或 2001:db8::201。
netmask_or_prefix	IPv4 的网络地址掩码或 IPv6 的前缀。IPv4 网络掩码必须采用点分十进制格式，例如 255.255.255.0。IPv6 前缀是标准前缀编号，例如 96。
gateway	要添加或删除的网关地址，采用 IPv4 或 IPv6 格式（视情况而定）。

Command History

版本	修改
6.0.1	引入了此命令。

使用指南

如果使用 **configure network management-interface** 命令配置仅事件接口，并且此接口与管理接口位于不同的网络，则需要配置静态路由。静态路由不会影响通过设备的流量，即数据接口上的流量。如果没有静态路由，所有管理流量都使用指定为默认管理接口网关的默认路由。使用单个管理接口或事件专用接口位于同一网络时，通常不需要静态路由。

注释 对于默认路由，请勿使用此命令；当您将 **configure network ipv4** 或 **ipv6** 命令用于默认管理接口时，只能更改默认路由网关 IP 地址。

示例

以下示例使用目的地址、网络地址掩码和网关地址为管理接口添加 IPv4 静态路由：
management110.115.24.0255.255.255.010.115.9.2

```
> configure network static-routes ipv4 add management1 10.115.24.0 255.255.255.0 10.115.9.2
```

以下示例使用 的目的地址、IPv6 前缀长度和网关地址为管理接口添加 IPv6 静态路由。
management12001:db8::201642001:db8::3657

```
> configure network static-routes ipv6 add management1 2001:db8::201 64 2001:db8::3657
```

以下示例显示如何删除静态路由。

```
> show network-static-routes
---------------[ IPv4 Static Routes ]---------------
Interface                 : management1
Destination               : 10.1.1.0
Gateway                   : 192.168.0.254
Netmask                   : 255.255.255.0
> configure network static-routes ipv4 delete
Please select which IPv4 Static Route to delete:
1) management1:   dest 10.1.1.0          nmask 255.255.255.0     gw 192.168.0.254
Please enter number of route to delete: 1
Interface:    management1
Destination:  10.1.1.0
Netmask:      255.255.255.0
Gateway:      192.168.0.254
Are you sure that you want to delete this route?  (y/n) [n]: y
Configuration updated successfully
> show network-static-routes
No static routes currently configured.
```

Related Commands

命令	Description
configure network management-interface	配置多个管理接口。
configure network static-routes ipv4	为管理接口添加或删除 IPv4 静态路由。
show network-static-routes	显示为管理接口配置的静态路由。

configure password

要更改当前登录的用户账号的密码，请使用 **configure password** 命令。

configure password

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用此命令，当前用户可以在 CLI 中更改其密码。发出命令后，CLI 会提示用户其当前（或旧）密码，然后提示用户输入新密码两次。

示例

以下示例更改当前用户账号的密码。

```
> configure password
Enter current password: oldpassword
Enter new password: newpassword
Confirm new password: newpassword
```

Related Commands

命令	Description
configure user add	添加用于 CLI 访问的用户账号。

configure policy rollback

要将 threat defense 上的配置回滚到上次部署的配置，请使用 **configure policy rollback** 命令。

configure policy rollback

Command History

版本	修改
6.7	引入了此命令。
7.2	支持回滚以实现高可用性。

使用指南

如果将 threat defense 上的数据接口用于 管理中心 管理（请参见 **configure network management-data-interface** 命令），并从 管理中心 部署影响网络连接的配置更改，则可以将 threat defense 上的配置回滚到上次部署的配置，以便恢复管理连接。然后，您可以调整 管理中心 中的配置设置，以便保持网络连接并重新部署。即使没有丢失连接，也可以使用回滚功能；它不仅限于此故障排除情况。

请参阅以下准则：

- 只有以前的部署可以在 threat defense 上本地提供；您无法回滚到任何较早的部署。
- 从 管理中心 7.2 开始，支持回滚以实现高可用性。
- 群集技术部署不支持回滚。
- 回滚只会影响您可以在 管理中心中设置的配置。例如，回滚不会影响与专用管理接口相关的任何本地配置，您只能在 threat defense CLI 中进行配置。请注意，如果您在上次 管理中心 部署后使用 **configure network management-data-interface** 命令更改了数据接口设置，然后使用了回滚命令，则这些设置将不会保留；它们将回滚到上次部署的 管理中心 设置。
- UCAPL/CC 模式无法回滚。
- 无法回滚上一次部署期间更新的带外 SCEP 证书数据。
- 在回滚期间，连接将被丢弃，因为当前配置将被清除。

回滚后，threat defense 会通知 管理中心 已成功完成回滚。在 管理中心中，部署屏幕将显示一条横幅，说明配置已回滚。

如果回滚失败，请参阅 https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw-virtual/215258-troubleshooting-firepower-threat-defense.html 以了解常见的部署问题。在某些情况下，恢复 管理中心 管理访问权限后回滚可能会失败；在这种情况下，您可以解决 管理中心 配置问题，并从 管理中心重新部署。

示例

以下示例回滚上次部署的配置。

```
> configure policy rollback

The last deployment to this FTD was on June 1, 2020 and its status was Successful.
Do you want to continue [Y/N]?

Y

Rolling back complete configuration on the FTD. This will take time.
.....................
Policy rollback was successful on the FTD.
Configuration has been reverted back to transaction id:
Following is the rollback summary:
...................
.....................
>
```

Related Commands

命令	Description
configure network management-data-interface	为 管理中心 管理配置数据接口。

configure raid

要管理 RAID 中的 SSD，请使用 **configure raid** 命令。

注释 仅在 Secure Firewall 3100 上支持此命令。

configure raid { **add** | **remove** | **remove-secure** } **local-disk** { **1** | **2** } [*psid*]

Syntax Description

add	将 SSD 添加到 RAID。将新 SSD 同步到 RAID 可能需要几个小时，在此期间防火墙完全正常运行。您甚至可以重新启动，同步将在启动后继续。
psid	如果您添加的 SSD 以前在另一个系统上使用过，并且仍处于锁定状态，请输入 *psid*。*Psid* 印在 SSD 背面的标签上。或者，您可以重新启动系统，SSD 将被重新格式化并添加到 RAID。
remove	从 RAID 中删除 SSD 并保持数据不变。
remove-secure	从 RAID 中删除 SSD，禁用自加密磁盘功能，并对 SSD 执行安全清除。
local-disk {**1** | **2**}	指定 SSD、disk1 或 disk2。

Command Default

如果您有两个 SSD，它们会在您启动时形成 RAID。

Command History

版本	修改
7.1	此命令是为安全防火墙 3100 引入的。

使用指南

防火墙启动时，您可以在 CLI 上执行以下任务： 威胁防御

- 热插拔其中一个 SSD - 如果 SSD 出现故障，您可以更换它。请注意，如果您只有一个 SSD，则无法在防火墙开启时将其删除。
- 删除一个 SSD - 如果您有两个 SSD，可以删除一个。
- 添加第二个 SSD - 如果您有一个 SSD，可以添加第二个 SSD 并形成 RAID。

注意 请勿在未使用此程序从 RAID 中移除 SSD 的情况下将其移除。可能会导致数据丢失。

示例

以下示例从 RAID 中删除 disk2 并执行安全清除。

```
> configure raid remove-secure local-disk 2
```

Related Commands

命令	Description
show raid	显示 RAID 状态。
show ssd	显示 SSD 状态。

configure snort

要配置 Snort 检测引擎的高级行为，请使用 **configure snort** 命令。

configure snort preserve-connection {**enable** | **disable**}

Syntax Description

preserve-connection {**enable** | **disable**}	是否在Snort流程关闭时保留路由和透明接口上的现有TCP/UDP连接。默认情况下该选项处于启用状态，但可以禁用它。启用后，已被允许的连接仍保持建立状态，但在Snort再次可用之前，无法建立新连接。当禁用时，所有新的或现有连接会在 Snort 关闭时被丢弃。 非 TCP/UDP 连接（例如 ICMP ping）不会保留。 要查看当前设置，请使用 **show running-config snort** 命令。查看整个运行配置时， **snort preserve-connection** 命令的 **no** 形式表示该功能已禁用。

Command History

版本	修改
6.2.0.2、 6.2.3	引入了此命令。但是， **preserve-connection disable** 不支持 设备管理器 与 （本地管理）一起使用，每次部署配置时都会重新启用保留连接。 此命令在 threat defense 或 管理中心 运行版本 6.2.1、6.2.2、6.2.2.x 或早于 6.2.0.2 的版本时不可用，这种情况下，设备行为就像已禁用该命令一样，因此，当Snort关闭时，所有新的或现有的连接都会被丢弃。

使用指南

启用 **preserve-connection** 后，如果 Snort 关闭，任何现有连接仍会保持建立。当 Snort 可用时，这些已建立的连接会继续绕过 Snort 检查。任何需要 Snort 检查的新连接都将被丢弃，直到 Snort 再次可用。

示例

以下示例禁用 **preserve-connection**。

```
> configure snort preserve-connection disable
```

Related Commands

命令	Description
show conn	显示连接。
show conn detail	在连接详细信息中包括 snort 检测信息。
show conn detail long	在长格式连接详细信息中包括 snort 检测信息。

configure ssh-access-list

要将设备配置为接受来自指定 IP 地址的 SSH 连接，请使用 **configure ssh-access-list** 命令。

configure ssh-access-list *address_list*

Syntax Description

address_list	主机或网络的 IP 地址的逗号分隔列表，采用 IPv4 无类域间路由 (CIDR) 符号或 IPv6 前缀长度符号。例如，10.100.10.0/24 or 2001:DB8::/96。 要指定所有 IPv4 主机，请输入 0.0.0.0/0。要指定所有 IPv6 主机，请指定 ::/0。

Command History

版本	修改
6.1	引入了此命令。

使用指南

您必须在一个命令中包含所有受支持的主机或网络。此命令中指定的地址将覆盖 SSH 访问列表的当前内容。

仅允许 SSH 访问不允许用户登录本地管理器。对配置软件的访问由用户名和密码控制。

如果排除当前登录 CLI 的 IP 地址，连接将中断。您需要更改 IP 地址才能重新进入 CLI。

如果设备是本地管理的高可用性组中的设备，则下次主用设备部署配置更新时，您的更改将被覆盖。如果这是主用设备，您的更改将在部署期间传播到对等设备。

示例

以下示例将设备配置为接受来自任何 IPv4 或 IPv6 地址的 SSH 连接：

```
> configure ssh-access-list 0.0.0.0/0,::/0
The ssh access list was changed successfully.
> show ssh-access-list
ACCEPT     tcp  --  anywhere             anywhere             state NEW tcp dpt:ssh
ACCEPT     tcp      anywhere             anywhere             state NEW tcp dpt:ssh
```

Related Commands

命令	Description
configure disable-ssh-access	清除 SSH 访问列表。
show ssh-access-list	显示 SSH 访问列表。

configure ssl-protocol

要配置客户端可在与设备的 HTTPS 连接中使用的 SSL 协议，请在使用本地管理器时使用 **configure ssl-protocol** 命令。

configure ssl-protocol {*protocol_list* | **default**}

Syntax Description

default	启用默认 SSL 协议列表： **TLSv1.1**、 **TLSv1.2**。
protocol_list	指定以下任何协议的逗号分隔列表： **TLSv1**、 **TLSv1.1**、 **TLSv1.2**、 **SSLv3**。

Command Default

默认设置为 **TLSv1.1**、 **TLSv1.2**。

Command History

版本	修改
6.1	引入了此命令。

使用指南

此命令设置客户端可用于对设备进行 HTTPS Web 访问的协议。这与本地管理器 设备管理器配合使用。它不与远程管理器一起使用。

注释 如果使用此命令禁用当前用于与设备通信的协议，则会断开连接。

示例

以下示例将设备配置为接受 HTTPS 连接的所有 SSL 协议。

```
> show ssl-protocol
The supported ssl protocols are TLSv1.1 TLSv1.2
> configure ssl-protocol TLSv1,TLSv1.1,TLSv1.2,SSLv3
The following ssl protocols are now enabled:  TLSv1 TLSv1.1 TLSv1.2 SSLv3
> show ssl-protocol
The supported ssl protocols are  TLSv1 TLSv1.1 TLSv1.2 SSLv3
```

Related Commands

命令	Description
show ssl-protocol	显示当前配置的 SSL 协议。

configure tcp-randomization

要禁用 TCP 序列号随机化，请使用 **configure tcp-randomization** 命令。

configure tcp-randomization {**enable** | **disable**}

Syntax Description

enable	随机更改传入和传出数据包中的 TCP 序列号，以防止攻击者预测下一个数据包的序列号。
disable	请勿更改传入和传出数据包中的 TCP 序列号。

Command Default

默认启用 TCP 序列号随机化。

Command History

版本	修改
6.2	引入了此命令。

使用指南

每个 TCP 连接都有两个初始序列号 (ISN)：一个由客户端生成，一个由服务器生成。threat defense设备会为通过入站和出站两个方向的 TCP SYN 随机生成 ISN。

随机化受保护主机的 ISN 可防止攻击者预测新连接的下一个 ISN 而潜在劫持新会话。

可以根据需要禁用 TCP 初始序列号随机化，例如，由于数据混乱。例如，您可能正在使用依赖于具有顺序编号的TCP数据包的软件测试工具、软件产品或硬件设备。更改TCP随机化设置会影响设备上的所有接口和所有流量；不能更改特定接口或流量类。

仅当因随机化而遇到特定问题时，才应禁用 TCP 序列号随机化。

注释 虽然您可以在使用 设备管理器 时禁用 TCP 序列号随机化，但每次从 设备管理器 部署配置时，此功能都会重新启用。如果要保持禁用 TCP 序列号随机化，则必须在每次部署后重新输入命令。

示例

以下示例禁用 TCP 序列号随机化。

```
> configure tcp-randomization disable
```

要确定 TCP 序列号随机化当前是启用还是禁用，请查看 **set connection random-sequence-number disable** 命令的运行配置。此命令将位于 global_policy 策略映射中，因此您可以使用 **show running-config policy-map** 命令限制配置视图。如果 **set connection random-sequence-number** 命令未出现在配置中，则 TCP 序列号随机化已启用。

例如，以下内容显示 TCP 序列号随机化已禁用（相关命令已突出显示）。

```
> show running-config policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect icmp
  inspect icmp error
 class tcp
  set connection random-sequence-number disable
!
```

以下示例显示已启用 TCP 序列号随机化，因为 **set connection random-sequence-number** 命令不在 global_policy 策略映射中。

```
> show running-config policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect icmp
  inspect icmp error
```

configure unlock_time

要设置用户账户在超过最大失败登录次数后自动解锁的时间长度，请使用 **configure unlock_time** 命令。此命令仅在 CC/UCAPL 合规性模式下有效。

configure unlock_time 编号

Syntax Description

number	指定解锁时间（以分钟为单位），范围为 1 到 9999。

Command Default

在 CC/UCAPL 模式下运行时，默认解锁时间为 30 分钟。

当不在 CC/UCAPL 模式下运行时，用户账户将保持锁定状态，直到您使用 **configure user unlock** 命令将其解锁。您无法设置自动解锁时间。

Command History

版本	修改
6.2.1	引入了此命令。

使用指南

如果您在CC/UCAPL合规性模式下运行，则可以为锁定的用户设置全局解锁时间。在超过用户账户最大失败登录尝试次数的给定用户的时间到期后，账户将被解锁，用户可以重试。使用 **configure user maxfailedlogins** 命令设置允许的最大失败登录尝试次数。

即使设置了解锁时间，您也可以随时使用 **configure user unlock** 命令解锁用户账户。用户无需等待解锁时间到期。

示例

以下示例将解锁时间配置为 60 分钟。

```
> configure unlock_time 60
```

Related Commands

命令	Description
configure user add	添加新用户。
configure user maxfailedlogins	为用户设置最多允许的登录失败次数。
configure user unlock	解锁指定用户的账户。
show user	显示用户账号。

configure user access

要更改现有用户的访问授权级别，请使用 **configure user access** 命令。

configure user access *username* {**basic** | **config**}

Syntax Description

username	指定现有用户的名称。
basic	提供用户基本访问权限。此级别不允许用户输入配置命令。
config	提供用户配置访问权限。此级别将赋予用户完整管理员权限，让其可以输入所有配置命令。

Command History

版本	修改
6.1	引入了此命令。

使用指南

创建用户账号时，需要指定用户的访问权限。使用 **configure user access** 命令以修改指定用户的访问级别。命令在指定用户下次登录时生效。

示例

以下示例将用户 jdoe 的访问权限更改为 Basic。

```
> configure user access jdoe basic
```

Related Commands

命令	Description
configure user add	添加新用户。
show user	显示用户账号和访问权限。

configure user add

要创建用于 CLI 访问的新用户账号，请使用 **configure user add** 命令。

configure user add 用户名 {**basic** | **config**}

Syntax Description

username	指定现有用户的名称。
basic	提供用户基本访问权限。此级别不允许用户输入配置命令。
config	提供用户配置访问权限。此级别将赋予用户完整管理员权限，让其可以输入所有配置命令。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用此命令可创建具有指定名称、访问级别和密码的新用户。此命令提示输入密码。所有其他账户属性均使用默认属性进行配置。

示例

以下示例将添加一个名为 joecool 且具有配置访问权限的用户账号。在您键入密码时，密码不会显示。

```
> configure user add joecool config
Enter new password for user joecool: newpassword
Confirm new password for user joecool: newpassword
> show user
Login              UID   Auth Access  Enabled Reset    Exp Warn  Str Lock Max
admin             1000  Local Config  Enabled    No  Never  N/A  Dis   No N/A
joecool           1001  Local Config  Enabled    No  Never  N/A  Dis   No   5
```

Related Commands

命令	Description
configure user access	设置用户访问级别。
configure user aging	设置用户密码时效。
configure user delete	删除指定用户。
configure user disable	禁用指定用户。
configure user enable	启用指定用户。
configure user forcereset	强制重置指定用户的密码。

命令	Description
configure user maxfailedlogins	为指定用户设置最多登录失败次数。
configure user password	为指定用户设置密码。
configure user strengthcheck	为指定用户设置密码强度检查要求。
configure user unlock	为指定用户解锁账户。
show user	显示用户账号。

configure user aging

要设置用户密码的到期日期，请使用 **configure user aging** 命令。

configure user aging *username max_days warn_days* [*grace_period*]

Syntax Description

username	指定用户的名称。您无法更改 **管理员** 用户老化设置。
max_days	指定密码的最大有效天数。值范围为 1 到 9999。
warning_days	指定在密码到期前允许用户更改密码的天数。值范围为 1 到 9999，但必须小于最大天数。
grace_period	（可选，仅限 FXOS 平台。）指定在密码到期后用户仍可更改密码的天数。在非 FXOS 平台上，该参数被接受，但 **show user** 输出显示宽限期已禁用。

Command History

版本	修改
6.1	引入了此命令。
7.0	添加了 *grace_period* 参数。

示例

以下示例将用户的密码设置为在 100 天后到期，并在密码到期前 30 天开始警告用户。在 show user 输出中，请注意 Exp 和 Warn 列中的数字。

```
> configure user aging jdoe 100 30
> show user
Login              UID   Auth Access  Enabled Reset    Exp Warn  Str Lock Max
admin             1000  Local Config  Enabled    No  Never  N/A  Dis   No N/A
jdoe              1001  Local Config  Enabled    No    100   30  Dis   No   5
```

以下示例将密码设置为在 180 天后到期，在到期前 7 天开始警告用户，并包括 7 天的宽限期。

```
> configure user aging joeuser 180 7 7
> show user
Login          UID   Auth Access  Enabled Reset   Exp   Warn    Grace  MinL Str Lock Max
admin          100  Local Config  Enabled    No  10000     7  Disabled    8 Ena   No N/A
extuser        501 Remote Config Disabled   N/A  99999     7  Disabled    1 Dis   No N/A
joeuser       1000  Local Config  Enabled   Yes    180     7         7    8 Dis   No   5
```

Related Commands

命令	Description
configure user add	添加新用户。

命令	Description
configure user forcereset	强制重置指定用户的密码。
configure user password	为指定用户设置密码。
show user	显示用户账号。

configure user delete

要删除用户账号，请使用 **configure user delete** 命令。

configure user delete 用户名

Syntax Description

username	指定用户的名称。您无法删除 管理员 用户。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例删除用户账号。

```
> configure user delete jdoe
```

Related Commands

命令	Description
configure user add	添加新用户。
configure user disable	禁用用户账号，而不将其删除。
show user	显示用户账号。

configure user disable

要禁用用户账号而不将其删除，请使用 **configure user disable** 命令。

configure user disable 用户名

Syntax Description

username	指定用户的名称。您无法禁用 管理员 用户。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用此命令可禁用用户账号而不将其删除。被禁用的用户将无法登录。使用 **configure user enable** 命令重新启用已禁用的用户账号。

示例

以下示例禁用用户账号。

```
> configure user disable jdoe
> show user
Login              UID   Auth Access  Enabled Reset    Exp Warn  Str Lock Max
admin             1000  Local Config  Enabled    No  Never  N/A  Dis   No N/A
jdoe              1001  Local Config Disabled    No    100   30  Dis   No   5
```

Related Commands

命令	Description
configure user add	添加新用户。
configure user delete	删除指定用户。
configure user enable	启用指定用户。
configure user unlock	为指定用户解锁账户。
show user	显示用户账号。

configure user enable

要启用以前禁用的用户，请使用 **configure user enable** 命令。

configure user enable 用户名

Syntax Description

username	指定用户的名称。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用此命令可启用用户并允许登录。

示例

以下示例启用已禁用的用户账户。请注意 **show user** “已启用”列中的更改。

```
> show user
Login              UID   Auth Access  Enabled Reset    Exp Warn  Str Lock Max
admin             1000  Local Config  Enabled    No  Never  N/A  Dis   No N/A
jdoe              1001  Local Config Disabled    No    100   30  Dis   No   5
> configure user enable jdoe
> show user
Login              UID   Auth Access  Enabled Reset    Exp Warn  Str Lock Max
admin             1000  Local Config  Enabled    No  Never  N/A  Dis   No N/A
jdoe              1001  Local Config  Enabled    No    100   30  Dis   No   5
```

Related Commands

命令	Description
configure user add	添加新用户。
configure user disable	禁用指定用户。
configure user forcereset	强制重置指定用户的密码。
configure user unlock	为指定用户解锁账户。
show user	显示用户账号。

configure user forcereset

要强制用户在下次登录时更改密码，请使用 **configure user forcereset** 命令。

configure user forcereset 用户名

Syntax Description

username	指定用户的名称。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用此命令以强制用户在下次登录时更改密码。当用户登录并更改密码时，会自动启用强度检查。

示例

以下示例强制用户在下次登录时重置密码。

```
> configure user forcereset jdoe
```

Related Commands

命令	Description
configure user password	为指定用户设置密码。
configure user strengthcheck	为指定用户设置密码强度检查要求。
show user	显示用户账号。

configure user maxfailedlogins

要设置用户的最大连续登录失败次数，请使用 **configure user maxfailedlogins** 命令。

configure user maxfailedlogins *username number*

Syntax Description

username	指定用户的名称。
number	指定最大连续失败登录次数，范围为 1 到 9999。

Command Default

没有默认行为或值。但是，当您创建新账户时，默认的最大连续登录失败次数为 5。

Command History

版本	修改
6.1	引入了此命令。
6.2.2	在 CC/UCAPL 合规性模式下运行时，还可以配置 **admin** 用户的最大失败登录尝试次数。

使用指南

使用此命令可设置指定用户在其账户被锁定之前的最大连续登录失败次数。如果用户账号被锁定，请使用 **configure user unlock** 命令将其解锁。

示例

以下示例将最大连续失败登录次数设置为 3。

```
> configure user maxfailedlogins jdoe 3
```

Related Commands

命令	Description
configure user add	添加新用户。
configure user password	为指定用户设置密码。
configure user unlock	解锁指定用户的账户。
show user	显示用户账号。

configure user minpasswdlen

要设置用户密码的最小长度，请使用 **configure user minpasswdlen** 命令。

configure user minpasswdlen *username number*

Syntax Description

username	指定用户的名称。
number	指定密码的最小长度，从 1 到 127。

Command Default

无最小密码长度。

Command History

版本	修改
6.1	引入了此命令。
6.2.2	您现在可以为 **admin** 用户配置最小密码长度。

使用指南

使用此命令可设置指定用户的最小密码长度。系统将提示您输入用户账号的当前密码。如果最小长度大于当前密码长度，系统还会提示您设置新密码。

示例

以下示例将最小密码长度设置为 8 个字符。在本示例中，当前密码小于新的最小值，因此您需要设置新密码。

```
> configure user minpasswdlen jdoe 8
Setting minimum password length to 8
Enter current password: <enter old password>
Enter new password for user jdoe: <enter new password>
Confirm new password for user jdoe: <enter new password>

Setting Minimum password length succeeded
```

Related Commands

命令	Description
configure user add	添加新用户。
show user	显示用户账号。

configure user password

要设置其他用户账户的密码，请使用 **configure user password** 命令。

configure user password 用户名

Syntax Description

username	指定用户的名称。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用此命令可设置指定用户的密码。此命令提示输入用户密码。要更改您自己的密码，请使用 **configure password** 命令而不是此命令。

示例

以下示例设置另一个用户账户的密码。在您键入密码时，密码不会显示。

```
> configure user password jdoe
Enter new password for user jdoe: newpassword
Confirm new password for user jdoe: newpassword
```

Related Commands

命令	Description
configure password	更改当前登录用户的密码。
configure user add	添加新用户。
configure user aging	设置用户密码时效。
configure user forcereset	强制重置指定用户的密码。
configure user maxfailedlogins	为指定用户设置最多登录失败次数。
configure user strengthcheck	为指定用户设置密码强度检查要求。
show user	显示用户账号。

configure user strengthcheck

要启用或禁用针对用户密码的强度要求，请使用 **configure user strengthcheck** 命令。

configure user strengthcheck 用户名 {**enable** | **disable**}

Syntax Description

username	指定用户的名称。
enable	设置指定用户密码的要求。
disable	删除对指定用户密码的要求。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用此命令启用或禁用强度检查，用户修改密码时需要满足特定的密码条件。如果用户密码到期或使用了 **configure user forcereset** 命令，则此要求会在用户下次登录时自动启用。

示例

以下示例对用户账号启用强度检查。

```
> configure user strengthcheck jdoe enable
```

Related Commands

命令	Description
configure user add	添加新用户。
configure user forcereset	强制重置指定用户的密码。
configure user maxfailedlogins	为指定用户设置最多登录失败次数。
configure user password	为指定用户设置密码。
configure user unlock	为指定用户解锁账户。
show user	显示用户账号。

configure user unlock

要解锁登录失败次数超过最大数量的用户账号，请使用 **configure user unlock** 命令。

configure user unlock 用户名

Syntax Description

username	指定用户的名称。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例解锁用户账号。

```
> configure user unlock jdoe
```

Related Commands

命令	Description
configure user add	添加新用户。
configure user maxfailedlogins	为指定用户设置最多登录失败次数。
show user	显示用户账号。

conn data-rate

要查看传输大量数据的设备上的连接，请使用 **conn data-rate** 命令。此命令展示每个流的数据速率与现有的连接信息。要禁用按数据速率收集连接，请使用命令的 **no** 形式。

conn data-rate

no conn data-rate

Command History

版本	修改
6.6	引入了此命令。

使用指南

conn data-rate 命令对于确定哪些连接和用户可能对设备的整体负载贡献最大。

启用后， **conn data-rate** 功能会跟踪所有连接的两项统计信息：

- 连接的正向和反向的当前（1 秒）数据速率。
- 连接的前向和反向最大 1 秒数据速率。

示例

以下示例显示如何启用连接数据速率收集，验证该功能是否已启用，以及如何查看数据速率：

```
> conn data-rate
> show conn data-rate
Connection data rate tracking is currently enabled.
Use 'show conn detail' to see the data rates of active connections.

> show conn detail

TCP outside: 198.51.100.1/46994 NP Identity Ifc: 203.0.113.1/22,
flags UOB , idle 0s, uptime 9m24s, timeout 1h0m, bytes 68627
Initiator: 198.51.100.1, Responder: 203.0.113.1
data-rate forward/reverse
current rate: 1194/0 bytes/sec <----------------current data rate for forward/reverse flows
max rate: 2520/0 bytes/sec <----------------max data rate for forward/reverse flows
time since last max 0:08:54/NA <----------------time since last max data rate for
forward/reverse flows
```

Related Commands

命令	Description
show conn data-rate	显示连接数据速率跟踪的当前状态。
show conn detail	按数据速率值显示已过滤的连接。
clear conn data-rate	清除当前最大数据速率值。

connect fxos

要进入 FXOS 服务管理器 CLI 模式，请使用 **connect fxos** 命令。

connect fxos

Command History

版本	修改
6.2.1	引入了此命令。

使用指南

FXOS 是 Firepower 2100、4100 和 9300 系列设备上的基础软件。

示例

以下示例显示在 threat defense CLI 中启动时如何进入 FXOS CLI。输入 ? 查看 FXOS 中的可用命令。

```
> connect fxos
Cisco Firepower Extensible Operating System (FX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2009-2015, Cisco Systems, Inc. All rights reserved.

The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license.

(...remaining copyrights omitted...)

kp-fpr2100-2#
```

以下示例显示如果您最初从 FXOS CLI 进入 threat defense CLI（使用 **connect ftd** FXOS 命令），会发生什么情况。

```
> connect fxos
You came from FXOS Service Manager. Please enter 'exit' to go back.
```

copy

要将文件复制到闪存或从闪存中复制，请使用 **copy** 命令。

copy [**/noconfirm** | **/noverify**] [*interface_name*] { **/pcap capture:/** [*buffer_name*] | *src_url* | **running-config** | **startup-config** } *dest_url*

Syntax Description

/noverify	（可选）复制开发密钥签名映像时跳过签名验证。
/noconfirm	（可选）复制文件而不提示确认。
interface_name	（可选）指定将通过其复制文件的接口名称。如果不指定接口，threat defense 将检查 数据路由表。要使用不属于数据路由表的 **管理** 接口或任何其他管理专用接口，必须使用此选项进行指定。
/pcap capture:/ [*buffer_name*]	从指定缓冲区复制 **capture** 命令的原始数据包捕获转储。
running-config	指定存储在系统内存中的运行配置。
startup-config	指定存储在闪存中的启动配置。闪存中启动配置是隐藏文件。

src-url *dest-url*	指定源文件（您要复制的文件）和目标文件（您通过复制创建的文件）。您无法在两个远程位置之间复制，因此如果源文件是本地文件，则目标文件可以是本地文件或远程文件。如果源文件是远程文件，则目标文件必须是本地文件。对文件位置使用以下URL 语法： • **disk0:/**[[*path/*]*filename*] 或 **flash:/**[[*path/*]*filename*] - **flash** 和 **disk0** 均指示内部闪存。可以使用任一选项。 • **disk***n***:/**[[*path/*]*filename*]- 表示可选的外部闪存驱动器，其中 *n* 指定驱动器编号。 • **smb:/**[[*path/*]*filename*] - 指示服务器消息阻止（一种 UNIX 服务器本地文件系统）。 • **ftp://**[[*user*[**:***password*]@] *server*[:*port*]/[*path/*] *filename*[**;type=***xx*]]—The **type** can be one of these keywords: **ap** (ASCII passive mode), **an** (ASCII normal mode), **ip** (Default—Binary passive mode), **in** (Binary normal mode). • **http**[**s**]**://**[[*user*[**:***password*] **@**]*server*[:*port*]/[*path/*]*filename*] • **scp://**[[*user*[:*password*]@] *server*[/*path*]/*filename*[**;int=***interface_name*]]—Indicates an SCP server. **;int=***interface* 选项会绕过路由查找，并始终使用指定接口来访问安全复制 (SCP) 服务器。 • **system:/**[[*path/*]*filename*]- 表示系统内存。 • **tftp://**[[*user*[**:***password*]@] *server*[:*port*] /[*path/*]*filename*[**;int=***interface_name*]] - 指示 TFTP 服务器。路径名不能包含空格。**;int=***interface* 选项会绕过路由查找并始终使用指定接口来访问 TFTP 服务器。 • **cluster_trace:** - 表示 cluster_trace 文件系统。

Command History

版本	修改
7.1	如果不指定接口， threat defense将检查数据路由表。没有回退到管理路由表。以前，默认查找是回退到数据路由表的管理路由表。由于管理和诊断接口合并，管理路由表不再自动使用；如果要使用管理接口，则必须指定该接口。
6.1	引入了此命令。

使用指南

执行一个整个集群范围内的捕获后，您可以通过在主设备上输入以下命令，将同一个捕获文件同时从集群中的所有设备复制到 TFTP 服务器：

cluster exec copy /noconfirm /pcap capture:*cap_name* **tftp://***location*/*path*/*filename***.pcap**

多个 PCAP 文件（一个文件来自一个设备）将复制到 TFTP 服务器。目标捕获文件名自动附有设备名称，如 filename_A.pcap、filename_B.pcap，其中 A 和 B 是集群设备名称。

注释 如果在文件名末尾添加设备名称，将生成不同的目标名称。

示例

以下示例复制安装日志。

```
> copy /noconfirm flash:/install.log flash:/install.save.log
Copy in progress...CC
INFO: No digital signature found
150498 bytes copied in 0.20 secs
```

以下示例展示如何将文件从磁盘复制到系统执行空间中的 TFTP 服务器：

```
> copy /noconfirm disk0:/install.log
tftp://10.7.0.80/install.log
```

以下示例展示如何将运行配置复制到 TFTP 服务器：

```
> copy /noconfirm running-config tftp://10.7.0.80/firepower/device1.cfg
```

以下示例展示如在不对开发密钥签名的映像不进行验证的情况下对其进行复制：

```
> copy /noverify /noconfirm lfbff.SSA exa_lfbff.SSA
Source filename [lfbff.SSA]?
Destination filename [exa_lfbff.SSA]?
Copy in progress...CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
Writing file disk0:/exa_lfbff.SSA...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Digital Signature was not verified
124125968 bytes copied in 61.740 secs (2034851 bytes/sec)
```

Related Commands

命令	Description
write net	将运行配置复制到 TFTP 服务器。

cpu hog granular-detection

要在短时间内提供实时占用检测并设置 CPU 占用阈值，请使用 **cpu hog granular-detection** 命令。

cpu hog granular-detection ［**count** *number*］［**threshold** *value*］

Syntax Description

count *number*	指定已执行的代码执行中断的数量。值为 1 到 10000000。默认值和建议值均为 1000。
threshold *value*	范围为 1 至 100。如果未设置，则使用默认值，平台之间有所不同。

Command Default

count 默认值为 1000。 **threshold** 默认设置因平台而异。

Command History

版本	修改
6.1	引入了此命令。

使用指南

cpu hog granular-detection 命令每隔 10 毫秒中断当前代码执行并总计中断数。CPU 占用的中断检查。如果存在，则登录。此命令可缩短数据路径中 CPU 占用检测的时间间隔。

每个基于安排的占用最多与 5 个基于中断的占用条目关联；每个条目可最多有 3 个回溯。无法覆盖基于中断的占用；如果没有空间，将丢弃新的。根据LRU策略仍可重用基于安排的占用，且当时会清除其关联的基于中断的占用。

示例

以下示例展示如何触发 CPU 占用检测：

```
> cpu hog granular-detection count 1000 threshold 10
Average time spent on 1000 detections is 10 seconds, and it may take longer
under heavy traffic.
Please leave time for it to finish and use show process cpu-hog to check results.
```

Related Commands

命令	Description
show processes cpu-hog	显示占用 CPU 的进程。
clear process cpu-hog	清除占用 CPU 的进程。

cpu profile activate

要启动 CPU 分析，请使用 **cpu profile activate** 命令。

cpu profile activate ［*n_samples* ［**sample-process** *process_name*］［**trigger cpu-usage** *cpu%* ［*process_name*］］］

Syntax Description

n_samples	分配用于存储 *n* 采样号的内存。有效值为从 1 到 100,000。
sample-process *process_name*	仅对特定流程采样。
trigger cpu-usage *cpu%* [*process_name*]	在全局 CPU 百分比大于 5 秒之前防止分析器启动，并且在 CPU 百分比低于此值时，停止分析器。 如果指定流程名称，它将使用该流程的 5 秒 CPU 百分比作为触发器。

Command Default

n_samples 默认值为 1000。

cpu% 默认值为 0。

Command History

版本	修改
6.1	引入了此命令。

使用指南

CPU 分析器可帮助您确定哪个流程正在使用 CPU。在计时器中断时，分析 CPU 可捕获已在 CPU 上运行的流程地址。无论 CPU 负载如何，每隔 10 毫秒进行此分析。例如，如果需要 5000 份采样，分析确切的需要 50 秒完成。如果 CPU 分析器使用的 CPU 时间数量相对较低，则收集采样的时间会更长。CPU 配置文件记录在单独的缓冲区进行采样。

将 **show cpu profile** 命令与 **cpu profile activate** 命令配合使用可显示可收集的信息，以及 TAC 可用于排除 CPU 问题的故障的信息。 **show cpu profile dump** 命令输出为十六进制格式。

如果 CPU 分析器等待启动条件发生， **show cpu profile** 命令会显示以下输出：

```
CPU profiling started: 12:45:57.209 UTC Wed Nov 14 2012
CPU Profiling waiting on starting condition.
Core 0: 0 out of 10 samples collected.
Core 1: 0 out of 10 samples collected.
Core 2: 0 out of 10 samples collected.
Core 3: 0 out of 10 samples collected.
CP
0 out of 10 samples collected.
```

示例

默认情况下，以下示例激活分析器并指示其存储 1000 份采样。接下来， **show cpu profile** 命令显示正在进行分析。等待一段时间后，下一个 **show cpu profile** 命令显示分析已完成。最

后，我们使用 **show cpu profile dump** 命令获取结果。复制输出并将其提供给思科技术支持。您可能需要记录 SSH 会话以获取完整输出。

```
> cpu profile activate
Activated CPU profiling for 1000 samples.
Use "show cpu profile" to display the progress or "show cpu profile dump" to interrupt
profiling and display the incomplete results.
> show cpu profile
CPU profiling started: 16:13:48.279 UTC Thu Oct 20 2016
CPU profiling currently in progress:
    Core 0: 501 out of 1000 samples collected.
    CP: 586 out of 1000 samples collected.
Use "show cpu profile dump" to see the results after it is complete or to interrupt
profiling and display the incomplete results.
> show cpu profile
CPU profiling started: 16:13:48.279 UTC Thu Oct 20 2016
CPU Profiling has stopped.
    Core 0 done with 1000 samples
    CP done with 1000 samples
Use "show cpu profile dump" to see the results.
> show cpu profile dump
(...output omitted...)
```

Related Commands

命令	Description
show cpu profile	显示 CPU 分析进程。
show cpu profile dump	显示不完整的或已完成的分析结果。

cpu profile dump

要将 CPU 分析的结果保存到文本文件，请使用 **cpu profile dump** 命令。

cpu profile dump *dest_url*

Syntax Description

dest_url	• **disk0:**/[[*path/*]*filename*] 或 **flash:**/[[*path/*]*filename*] - **flash** 和 **disk0** 均指示内部闪存。可使用任一选项。 • **disk***n***:**/[[*path/*]*filename*]- 表示可选的外部闪存驱动器，其中 *n* 指定驱动器编号。 • **smb:**/[[*path/*]*filename*] - 指示 UNIX 服务器本地文件系统。使用 LAN 管理器及类似的网络系统中的 Server Message Block（服务器消息块）文件系统协议包装数据并与其他系统交换信息。 • **ftp://**[[*user*[**:***password*]@] *server*[:*port*]/[*path/*] *filename*[**;type=***xx*]]—The **type** can be one of these keywords: **ap** (ASCII passive mode), **an** (ASCII normal mode), **ip** (Default—Binary passive mode), **in** (Binary normal mode). • **http**[**s**]**://**[[*user*[**:***password*] **@**]*server*[:*port*]/[*path/*]*filename*] • **scp://**[[*password*]@] *server*[/*path*]/*filename*[*;int=***;int=***interface_name*]] **-;int=***interface* 选项会绕过路由查找并始终使用指定接口来访问安全复制 (SCP) 服务器。 • **tftp://**[[*user*[**:***password*]@] *server*[:*port*] /[*path/*]*filename*[**;int=***interface_name*]]—路径名不能包含空格。**;int=***interface* 选项会绕过路由查找并始终使用指定接口来访问 TFTP 服务器。 • **cluster:**- 表示集群文件系统。

Command History

版本	修改
6.1	引入了此命令。

使用指南

CPU profile dump 命令以十六进制格式将 CPU 分析器输出写入指定的文本文件。

示例

以下示例将最新的 CPU 配置文件转储存储到名为 cpudump.txt 的文件：

```
> cpu profile dump disk0:/cpudump.txt
```

Related Commands

命令	Description
show cpu profile dump	显示不完整的或已完成的分析结果。

crashinfo force

要强制设备崩溃，请使用 **crashinfo force** 命令。

crashinfo force /noconfirm {**page-fault** | **watchdog** | **process** *process_ID*}

Syntax Description

page-fault	由于页面错误而强制崩溃。
watchdog	由于监视而强制崩溃。
process *process_ID*	强制 process_ID 指定的流程崩溃。使用 **show kernel process** 命令查看流程 ID。

Command Default

默认情况下，设备将崩溃信息文件保存到闪存。

Command History

版本	修改
6.1	引入了此命令。

使用指南

您可以使用 **crashinfo force** 命令测试崩溃输出生成。在崩溃输出中，没有什么可以区分实际崩溃与由 **crashinfo force page-fault** 或 **crashinfo force watchdog** 命令导致的崩溃（因为这些都是真正的崩溃）。设备将在故障转储完成后重新加载。

注意事项 请勿在生产环境中使用 **crashinfo force** 命令。 **crashinfo force** 命令会使设备崩溃并强制其重新加载。

示例

以下示例因页面错误而强制崩溃。

```
> crashinfo force /noconfirm page-fault
```

Related Commands

命令	Description
clear crashinfo	清除崩溃信息文件的内容。
crashinfo test	测试设备将故障信息保存到闪存中文件的能力。
show crashinfo	显示崩溃信息文件的内容。

crashinfo test

要测试设备将崩溃信息保存到闪存中的文件的能力，请使用 **crashinfo test** 命令。

crashinfo test

Command History

版本	修改
6.1	引入了此命令。

使用指南

输入 **crashinfo test** 命令不会使设备崩溃。如果以前的崩溃信息文件已存在于闪存中，则覆盖该文件。

示例

以下示例展示崩溃信息文件测试的输出。

```
> crashinfo test
```

Related Commands

命令	Description
clear crashinfo	清除崩溃信息文件的内容。
crashinfo force	强制设备崩溃。
show crashinfo	显示崩溃信息文件的内容。

crypto ca trustpool export

要导出构成 PKI 信任池的证书，请使用 **crypto ca trustpool export** 命令。

crypto ca trustpool export *filename*

Syntax Description

filename	要在其中存储已导出信任池证书的文件。

Command History

版本	修改
6.1	引入了此命令。

使用指南

此命令将活动信任池的全部内容复制到 PEM 编码格式的指定文件路径。

示例

```
> crypto ca trustpool export disk0:/exportfile.pem
Trustpool certificates exported to disk0:/exportfile.pem
>
> more exportfile.pem
-----BEGIN CERTIFICATE-----
MIIEMjCCAxqgAwIBAgIBATANBgkqhkiG9w0BAQUFADB7MQswCQYDVQQGEwJHQjEb
MBkGA1UECAwSR3JlYXRlciBNYW5jaGVzdGVyMRAwDgYDVQQHDAdTYWxmb3JkMRow
GAYDVQQKDBFDb21vZG8gQ0EgTGltaXRlZDEhMB8GA1UEAwwYQUFBIENlcnRpZmlj
YXRlIFNlcnZpY2VzMB4XDTA0MDEwMTAwMDAwMFoXDTI4MTIzMTIzNTk1OVowezEL
MAkGA1UEBhMCR0IxGzAZBgNVBAgMEkdyZWF0ZXIgTWFuY2hlc3RlcjEQMA4GA1UE
<More>
```

Related Commands

命令	Description
crypto ca trustpool import	导入构成 PKI 信任池的证书。
crypto ca trustpool remove	从 PKI 信任池中删除单个证书。
show crypto ca trustpool	显示 PKI 信任池。

crypto ca trustpool import

要导入构成 PKI 信任池的证书，请使用 **crypto ca trustpool import** 命令。

crypto ca trustpool import ［**clean**］ **url** *URL* **noconfirm** ［**signature-required**］
crypto ca trustpool import ［**clean**］ **default noconfirm**

Syntax Description

clean	在导入之前删除所有下载的信任池证书。
default	恢复设备的默认受信任 CA 列表。
noconfirm	抑制所有交互式提示。
signature-required	指示仅接受经过签署的文件。如果包括 **signature-required** 关键字，但签名不存在或无法验证，则导入失败。
url *url*	指定要导入的信任池文件的位置。 • [[*path/*]disk0:/filename] - 指示内部闪存。 • **disk***n***:/**[[*path/*]*filename*]- 表示可选的外部闪存驱动器，其中 *n* 指定驱动器编号。 • **smb:/**[[*path/*]*filename*] - 指示 UNIX 服务器本地文件系统。使用 LAN 管理器及类似的网络系统中的 Server Message Block（服务器消息块）文件系统协议包装数据并与其他系统交换信息。 • **ftp://**[[*user*[**:***password*]@] *server*[:*port*]/[*path/*] *filename*[**;type=***xx*]]—The **type** can be one of these keywords: **ap** (ASCII passive mode), **an** (ASCII normal mode), **ip** (Default—Binary passive mode), **in** (Binary normal mode). • **http**[**s**]**://**[[*user*[**:***password*] **@**]*server*[:*port*]/[*path/*]*filename*] • **scp://**[[*password*]@] *server*[/*path*]/*filename*[*;int=***;int=***interface_name*]] **-;int=***interface* 选项会绕过路由查找并始终使用指定接口来访问安全复制 (SCP) 服务器。 • **tftp://**[[*user*[**:***password*]@] *server*[:*port*] /[*path/*]*filename*[**;int=***interface_name*]]—路径名不能包含空格。**;int=***interface* 选项会绕过路由查找并始终使用指定接口来访问 TFTP 服务器。

Command History

版本	修改
6.1	引入了此命令。

使用指南

此命令可在从 cisco.com 下载信任池捆绑包时验证文件上的签名。当从其他源下载捆绑包或其格式不支持签名时，有效签名不是必填项。用户获悉签名状态并且可以选择是否接受捆绑包。

可能出现的交互警告如下：

- 具有无效签名的思科捆绑包格式
- 非思科捆绑包格式
- 具有有效签名的思科捆绑包格式

注释 除非您通过其他方法验证了文件的合法性，否则在文件签名无法验证时请勿安装证书。

示例

以下示例恢复默认信任池。

```
> crypto ca trustpool import clean default noconfirm
```

Related Commands

命令	Description
crypto ca trustpool export	导出构成 PKI 信任池的证书。
crypto ca trustpool remove	从 PKI 信任池中删除单个证书。
show crypto ca trustpool	显示 PKI 信任池。

crypto ca trustpool remove

要从 PKI 信任池中删除单个指定证书，请使用 **crypto ca trustpool remove** 命令。

crypto ca trustpool remove *cert_fingerprint* ［**noconfirm**］

Syntax Description

cert_fingerprint	十六进制的证书指纹。
noconfirm	指定此关键字以抑制所有交互式提示。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例删除证书。

```
> crypto ca trustpool remove 497904b0eb8719ac47b0bc11519b74d0
```

Related Commands

命令	Description
clear crypto ca trustpool	从信任池删除所有证书。
crypto ca trustpool export	导出构成 PKI 信任池的证书。
crypto ca trustpool import	导入构成 PKI 信任池的证书。
show crypto ca trustpool	显示 PKI 信任池。

d - r

debug

要显示给定功能的调试消息，请使用 **debug** 命令。要禁用调试消息的显示，请使用此命令的 **no** 形式。使用 **no debug all** 关闭所有调试命令。

debug *feature* [*subfeature*] [*level*]
no debug *feature* [*subfeature*]

Syntax Description

feature	指定要为其启用调试的功能。若要查看可用功能，请使用 **debug ?** 命令获取 CLI 帮助。
subfeature	（可选）根据功能，您可以为一项或多项子功能启用调试消息。使用 ? 查看可用的子功能。
level	（可选）指定调试级别。级别可能并非对所有功能都适用。使用 ? 可查看可用的级别。

Command Default

默认调试级别为 1。

Command History

版本	修改
6.1	引入了此命令。
7.2	此命令已修改为包括用于路径监控的调试。

使用指南

由于调试输出在CPU进程中享有高优先级，因此可导致系统不可用。为此，应仅在对特定问题进行故障排除或与思科 Technical Assistance Center (TAC) 进行故障排除会话时使用 **debug** 命令。此外，最好在网络流量较低和用户较少时使用 **debug** 命令。在这些时段进行调试会减少因 **debug** 命令处理开销增加而影响系统使用的可能性。

您只能在 CLI 会话中查看调试输出。在连接到控制台端口的情况下，或者在诊断 CLI 中，您可以直接查看输出结果（输入 **system support diagnostic-cli**）。此外，您也可以使用 **show console-output** 命令在常规 threat defense CLI 中查看输出。

示例

以下示例启用 DNS 调试并执行在诊断 CLI 中生成消息的操作。调试消息在“ERROR: % Invalid Hostname”消息之后开始。Press enter to get to the prompt. 然后，该示例将显示这些调试消息在 **show console-output** 显示屏中的外观。

```
> debug dns
debug dns enabled at level 1.

> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
```

```
firepower# ping www.example.com
                ^
ERROR: % Invalid Hostname
firepower# DNS: get global group DefaultDNS handle 1fa0b047
DNS: Resolve request for 'www.example.com' group DefaultDNS
DNS: No interfaces enabled
DNS: get global group DefaultDNS handle 1fa0b047
DNS: Resolve request for 'www.example.com' group DefaultDNS
DNS: No interfaces enabled

firepower# (press Ctrl+a, then d, to return to the regular CLI.)

Console connection detached.
> show console-output
... (output redacted)...
Message #75 : DNS: get global group DefaultDNS handle 1fa0b047
Message #76 : DNS: Resolve request for 'www.cisco.com' group DefaultDNS
Message #77 : DNS: No interfaces enabled
Message #78 : DNS: get global group DefaultDNS handle 1fa0b047
Message #79 : DNS: Resolve request for 'www.cisco.com' group DefaultDNS
Message #80 : DNS: No interfaces enabled
```

Related Commands

命令	Description
show debug	显示当前活动的调试设置。
undebug	禁用功能调试。此命令与 **no debug** 的效果相同。

debug packet-condition

要对必须调试的流应用过滤器，请使用 **debug packet-condition** 命令。要删除流上的过滤器，可使用此命令的 **no** 形式。使用 **no debug packet-condition** 以关闭流上的所有过滤器。

debug packet-condition [**position** *<line>*] **match** *<proto> {any|any4|any6|host <ip>|<ipv4>|<ipv4_mask>|<ipv6>/<prefixlen>}* [*<src_operator> <ports> {any|any4|any6|host <ip>|<ipv4>|<ipv4_mask>|<ipv6>/<prefixlen>}*] [*<dest_operator> <ports>*] [*<icmp_type>* | *<icmp6_type>*] [*connection <connection-id>*] [*unidirectional*]

Syntax Description

position *<line>*	指定过滤器应放置在现有过滤器列表中的位置。 *<line>* 表示数字。
match*<proto> {any|any4|any6|host <ip>|<ipv4>|<ipv4_mask>| <ipv6>/<prefixlen>}*	指定过滤器的匹配条件。 *<proto>* 表示协议。 *{any|any4|any6|host<ip> |<ipv4> |<ipv4_mask> |<ipv6> /<prefixlen> }* 表示 IP 地址选项。
<src_operator><port> {any|any4|any6|host <ip>|<ipv4>|<ipv4_mask>| <ipv6>/<prefixlen>}	（可选）指定源的端口或 IP 地址详细信息。
<dest_operator><port> {any|any4|any6|host <ip>|<ipv4>|<ipv4_mask>| <ipv6>/<prefixlen>}	（可选）指定目标的端口或 IP 地址详细信息。
<icmp_type>|<icmp6_type>	（可选）指定连接的 ICMP 类型。
connection <connection-id>	（可选）指定正在进行的连接的连接 ID。
unidirectional	（可选）指定应仅对指定方向的数据包执行调试。如果未提供该变量，则默认行为是双向的，其中流量将与连接的正向和反向流量匹配。

Command Default

Command History

版本	修改
6.4	引入了此命令。
6.5	**debug packet condition** 命令已更改为 **debug packet-condition**。
6.6	**debug packet-condition** 命令已得到增强，以提供对持续连接的支持。

使用指南

由于调试输出在CPU进程中享有高优先级，因此可导致系统不可用。为此，应仅在对特定问题进行故障排除或与思科 Technical Assistance Center (TAC) 进行故障排除会话时使用 **debug** 命令。此外，最好在网络流量较低和用户较少时使用 **debug** 命令。在这些时段进行调试会减少因 **debug** 命令处理开销增加而影响系统使用的可能性。

您只能在 CLI 会话中查看调试输出。在连接到控制台端口的情况下，或者在诊断 CLI 中，您可以直接查看输出结果（输入 **system support diagnostic-cli**）。此外，您也可以使用 **show console-output** 命令在常规 threat defense CLI 中查看输出。

示例

以下示例显示如何为必须调试的流设置过滤器。

```
> debug packet-condition position 7 match tcp 1.2.3.0 255.255.255.0 any4
> debug packet-condition match tcp 1.2.3.0 255.255.255.0 eq www any4 unidirectional
> debug packet-condition match connection 70856531
> no debug packet-condition match tcp 1.2.3.0 255.255.255 eq www unidirectional
```

Related Commands

命令	Description
debug packet-start	打开与调试日志数据库的连接，并开始将调试日志写入数据库。
debug packet-stop	关闭与调试日志数据库的连接，并停止将调试日志写入数据库。

debug packet-module

要为每个模块设置发送调试消息的级别，请使用 **debug packet-module** 命令。级别可以设置为介于 0（应急）到 7（调试）之间。设置级别后，系统将记录具有相同或更高严重性的所有消息。目前，仅支持 DAQ、PDTS、ACL 和 Snort 模块。

debug packet-module [**acl** | **all** | **daq** | **pdts** | **snort-engine** | **snort-fileprocessor** | **snort-firewall**] < *0-7* >

Syntax Description

acl	选择数据包处理路径中的访问控制策略。
all	选择数据包处理路径中的所有模块。
daq	选择数据包处理路径中的 DAQ 信息。
pdts	选择数据包处理路径中的 PDTS（数据平面传输/接收队列到 snort）通信。
snort-engine	选择数据包处理路径中的 Snort 信息。
snort-fileprocessor	选择数据包处理路径中的 Snort 文件处理器信息。
snort-firewall	选择数据包处理路径中的 Snort 防火墙信息。

Command History

版本	修改
6.4	引入了此命令。
6.5	**debug packet** 命令已更改为 **debug packet-module**。

使用指南

由于调试输出在 CPU 进程中享有高优先级，因此可导致系统不可用。为此，应仅在对特定问题进行故障排除或与思科 Technical Assistance Center (TAC) 进行故障排除会话时使用 **debug** 命令。此外，最好在网络流量较低和用户较少时使用 **debug** 命令。在这些时段进行调试会减少因 **debug** 命令处理开销增加而影响系统使用的可能性。

您只能在 CLI 会话中查看调试输出。在连接到控制台端口的情况下，或者在诊断 CLI 中，您可以直接查看输出结果（输入 **system support diagnostic-cli**）。此外，您也可以使用 **show console-output** 命令在常规 threat defense CLI 中查看输出。

示例

以下示例显示如何在数据包处理路径中设置 DAQ 信息的级别。

```
> debug packet daq 6
```

Related Commands

命令	Description
debug packet-start	打开与调试日志数据库的连接，并开始将调试日志写入数据库。

命令	Description
debug packet-stop	关闭与调试日志数据库的连接，并停止将调试日志写入数据库。

debug packet-module trace

要启用模块级数据包跟踪，请使用 **debug packet-module trace** 命令。

debug packet-module trace

Command History

版本	修改
6.6	引入了此命令。

使用指南

由于调试输出在CPU进程中享有高优先级，因此可导致系统不可用。为此，应仅在对特定问题进行故障排除或与思科 Technical Assistance Center (TAC) 进行故障排除会话时使用 **debug** 命令。此外，最好在网络流量较低和用户较少时使用 **debug** 命令。在这些时段进行调试会减少因 **debug** 命令处理开销增加而影响系统使用的可能性。

您只能在 CLI 会话中查看调试输出。在连接到控制台端口的情况下，或者在诊断 CLI 中，您可以直接查看输出结果（输入 **system support diagnostic-cli**）。此外，您也可以使用 **show console-output** 命令在常规 threat defense CLI 中查看输出。

示例

以下示例显示如何启用模块级数据包跟踪。

```
> debug packet-module trace
```

以下是 **debug packet-module trace** 命令的输出示例：

```
ID          | Details                                                                 | Time (ns)

----------- -------------------------------------------------------------------------
------------------------------
6525759     | TCP        74.125.24.156      : 443   -> 192.168.0.31      : 58280 | 19-02-2020
 06:48:43.050675868
```

此外，可以使用以下命令获取数据包的详细信息。

```
> show packet debugs module trace packet-id 6525759

Module: tcp-normalizer
Entry Time: 19-02-2020 06:48:43.050675868(ns)
****************************************
Module: translate
Entry Time: 19-02-2020 06:48:43.050684452(ns)
****************************************
Module: inspect_snort
Entry Time: 19-02-2020 06:48:43.050688028(ns)
****************************************
Module: pdts
Entry Time: 19-02-2020 06:48:43.050691843(ns)
****************************************
Module: pdts
Entry Time: 19-02-2020 06:48:43.051417112(ns)
****************************************
Module: pdts
Entry Time: 19-02-2020 06:48:43.051421642(ns)
```

```
****************************************
Module: tcp-normalizer
Entry Time: 19-02-2020 06:48:43.051424980(ns)
****************************************
Module: adjacency
Entry Time: 19-02-2020 06:48:43.051438331(ns)
****************************************
Module: fragment
Entry Time: 19-02-2020 06:48:43.051442861(ns)
****************************************
Module: daq
Entry Time: 19-02-2020 06:48:43.750763893(ns)
****************************************
Module: daq
Entry Time: 19-02-2020 06:48:43.750815391(ns)
****************************************
Module: daq
Entry Time: 19-02-2020 06:48:43.750831365(ns)
****************************************
Module: daq
Entry Time: 19-02-2020 06:48:43.750843286(ns)
****************************************
Module: daq
Entry Time: 19-02-2020 06:48:43.750889778(ns)
****************************************
Module: daq
Entry Time: 19-02-2020 06:48:43.750911474(ns)
****************************************
Module: daq
Entry Time: 19-02-2020 06:48:43.750942230(ns)
****************************************
Module: snort_engine
Entry Time: 19-02-2020 06:48:43.750986576(ns)
****************************************
Module: snort_engine
Entry Time: 19-02-2020 06:48:43.750999689(ns)
****************************************
Module: snort_engine
Entry Time: 19-02-2020 06:48:43.751020193(ns)
****************************************
Module: snort_engine
Entry Time: 19-02-2020 06:48:43.751051425(ns)
****************************************
Module: snort_firewall
Entry Time: 19-02-2020 06:48:43.751075029(ns)
****************************************
Module: snort_firewall
Entry Time: 19-02-2020 06:48:43.751084804(ns)
****************************************
Module: snort_engine
Entry Time: 19-02-2020 06:48:43.751099348(ns)
****************************************
Module: snort_engine
Entry Time: 19-02-2020 06:48:43.751118421(ns)
****************************************
Module: snort_engine
Entry Time: 19-02-2020 06:48:43.751137018(ns)
****************************************
Module: daq
Entry Time: 19-02-2020 06:48:43.751152753(ns)
****************************************
Module: daq
Entry Time: 19-02-2020 06:48:43.751164197(ns)
****************************************
```

```
Module: daq
Entry Time: 19-02-2020 06:48:43.751177072(ns)
****************************************
Module: daq
Entry Time: 19-02-2020 06:48:43.751186609(ns)
****************************************
Module: daq
Entry Time: 19-02-2020 06:48:43.751203775(ns)
****************************************
Module: daq
Entry Time: 19-02-2020 06:48:43.751224517(ns)
****************************************
Module: daq
Entry Time: 19-02-2020 06:48:43.751236677(ns)
****************************************
```

Related Commands

命令	Description
show packet debugs module trace	显示从每个模块收集的所有调试跟踪的列表。
debug packet-start	打开与调试日志数据库的连接，并开始将调试日志写入数据库。
debug packet-stop	关闭与调试日志数据库的连接，并停止将调试日志写入数据库。

debug packet-start

要开始调试数据包并将调试日志写入调试日志数据库，请使用 **debug packet-start** 命令。

debug packet-start

Command History

版本	修改
6.4	引入了此命令。
6.5	**debug packet start** 命令已更改为 **debug packet-start**。

使用指南

debug packet-start 打开与调试日志数据库的连接。除非调用此命令，否则不会将调试日志写入数据库。

示例

以下示例显示如何开始调试数据包：

```
> debug packet-start
```

Related Commands

命令	Description
debug packet-stop	关闭与调试日志数据库的连接，并停止将调试日志写入数据库。

debug packet-stop

要停止数据包调试并停止将调试日志写入调试日志数据库，请使用 **debug packet-stop** 命令。

debug packet-stop

Command History

版本	修改
6.4	引入了此命令。
6.5	**debug packet stop** 命令已更改为 **debug packet-stop**。

使用指南

debug packet-stop 关闭与调试日志数据库的连接。

示例

以下示例显示如何停止调试数据包：

```
> debug packet-stop
```

Related Commands

命令	Description
debug packet-start	打开与调试日志数据库的连接，并开始将调试日志写入数据库。

delete

要从闪存中删除文件，请使用 **delete** 命令。

delete /noconfirm ［**/recursive**］［**/replicate**］［**disk0:** | **disk***n***:** | **flash:**］［*path/*］*filename*

Syntax Description

/noconfirm	不提示确认。
/recursive	（可选）循环删除所有子目录中指定的文件。
/replicate	（可选）删除备用设备上指定的文件。
disk0:	（可选）指定内部闪存。
disk*n***:**	（可选）表示可选的外部闪存驱动器，其中 n 指定驱动器编号。这通常是 disk1：
filename	指定要删除的文件的名称。
flash:	（可选）指定内部闪存。此关键字与 **disk0** 相同。
path/	（可选）指定文件的路径。

Command Default

如果不指定目录，则默认为当前工作目录。

Command History

版本	修改
6.1	引入了此命令。

使用指南

如果未指定路径，将从当前工作目录删除文件。删除文件时支持通配符。

示例

以下示例展示如何从当前工作目录中删除名为 test.cfg 的文件：

```
> delete /noconfirm test.cfg
```

Related Commands

命令	Description
cd	将当前工作目录更改为指定的目录。
dir	列出当前目录中的文件。
rmdir	删除文件或目录。

dig

要查找完全限定域名 (FQDN) 的 IP 地址，请使用 **dig** 命令。

dig *hostname*

Syntax Description

hostname	要查找其 IP 地址的主机的完全限定域名。例如，www.example.com。

Command History

版本	修改
7.1	引入了此命令。它取代了 **nslookup** 命令。

使用指南

某些允许完全限定域名的命令无法使用为管理接口配置的 DNS 服务器来查找名称的 IP 地址。如果没有为通过数据接口的命令配置 DNS 服务器，请使用 命令确定 IP 地址，然后在 **dig** 命令中使用 IP 地址。

dig 命令仅通过管理接口工作，并从为管理接口配置的 DNS 服务器返回信息。如果为数据接口配置不同的服务器，则在通过数据接口的命令上使用 FQDN 可能会返回不同的 IP 地址，或者如果这些 DNS 服务器无法解析名称，则根本不会返回 IP 地址。

示例

以下示例查找 FQDN www.example.com 的 IP 地址。地址在输出的 ANSWER 部分突出显示。输出末尾附近的 SERVER 指示显示返回解析的 DNS 服务器的 IP 地址（本示例中的 IP 地址已清理）。

信头中的 NOERROR 状态表示请求成功；任何其他值均表示错误。例如，NXDOMAIN 表示响应的 DNS 服务器中不存在域名。您可以在互联网上搜索有关读取 Linux dig 命令输出的更多详细信息。

```
> dig www.example.com
; <<>> DiG 9.11.4 <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14008
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
; COOKIE: 88335c9f3dc2ca124e36b5eb60db9067b6cae4de2ea5bffb (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        0       IN      A       93.184.216.34
;; AUTHORITY SECTION:
example.com.            58911   IN      NS      a.iana-servers.net.
example.com.            58911   IN      NS      b.iana-servers.net.

;; ADDITIONAL SECTION:
```

```
a.iana-servers.net.     0       IN      A       199.43.135.53

;; Query time: 12 msec
;; SERVER: 10.163.47.11#53(10.163.47.11)
;; WHEN: Tue Jun 29 21:28:07 UTC 2021
;; MSG SIZE  rcvd: 152
```

dir

使用 dir 命令显示目录中的内容。

dir ［**/all**］［**all-filesystems**］［**/recursive**］［ **disk0:** | **disk***n***:** | **flash:** | **system:**］［*path*］［*filename*］

Syntax Description

/all	（可选）显示所有文件。
/recursive	（可选）递归显示目录内容。
all-filesystems	（可选）显示所有文件系统的文件。
disk0:	（可选）指定内部闪存，后跟冒号。
disk*n***:**	（可选）表示可选的外部闪存驱动器，其中 *n* 指定驱动器编号。这通常是 disk1：
flash:	（可选）显示默认闪存分区的目录内容。
path	（可选）指定特定路径。
filename	（可选）指定文件的名称。
system:	（可选）显示文件系统的目录内容。

Command Default

如果不指定目录，则默认为当前工作目录。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例展示如何显示目录内容：

```
> dir
Directory of disk0:/
1      -rw-  1519        10:03:50 Jul 14 2003    my_context.cfg
2      -rw-  1516        10:04:02 Jul 14 2003    my_context.cfg
3      -rw-  1516        10:01:34 Jul 14 2003    admin.cfg
60985344 bytes total (60973056 bytes free)
```

Related Commands

命令	Description
cd	将当前工作目录更改为指定的目录。

命令	Description
pwd	系统随即会显示当前工作目录。
mkdir	Creates a directory.
rmdir	删除目录。

dns update

要不等待 DNS 轮询计时器到期即启动 DNS 查找以解析指定的主机名，请在特权 EXEC 模式下使用 **dns update** 命令。

dns update ［**host** *fqdn_name*］［**timeout seconds** *number*］

Syntax Description

host *fqdn_name*	指定要运行 DNS 更新的主机的完全限定域名。
timeout seconds *number*	指定查找操作的超时时间（以秒为单位），范围为 3-30。默认值为 30。

Command History

版本	修改
6.3	引入了此命令。

使用指南

此命令立即启动 DNS 查找以解析指定的主机名，而不等待 DNS 轮询计时器到期。在不指定主机名的情况下运行DNS更新时，访问控制规则中使用的所有名称（称为“已激活”）都将被解析。该命令完成运行后，系统将在命令提示符下显示[已完成]，然后生成系统日志消息。

示例

以下示例对访问控制规则中使用的所有 FQDN 执行 DNS 更新。

```
> dns update
INFO: update dns process started
> [Done]
```

Related Commands

命令	Description
clear dns	删除 FQDN 网络对象 DNS 解析。
show dns	显示 FQDN 网络对象 DNS 解析。

eotool commands

只能在思科技术支持中心的指导下使用 **eotool** 命令。

exit

要退出 CLI，请使用 **exit** 命令。

exit

Command History

版本	修改
6.1	引入了此命令。

使用指南

在常规 CLI 中， **exit** 和 **logout** 命令执行相同的操作，即关闭与设备的 SSH 会话。

当您处于专家模式时， **exit** 会离开专家模式并返回到常规 CLI。

当您处于诊断 CLI (**system support diagnostic-cli**) 中时， **exit** 命令还会将您从特权 EXEC 模式移回用户 EXEC 模式。

示例

以下示例显示如何使用 **exit** 命令关闭与 CLI 的 SSH 连接。

```
> exit
```

以下示例显示如何使用 **exit** 命令 go 从诊断 CLI 中的特权 EXEC 模式（在提示符中以 # 符号表示）返回到用户 EXEC 模式。您可以忽略注销消息，您的 CLI 会话保持活动状态。

```
firepower# exit
Logoff
Type help or '?' for a list of available commands.
firepower>
```

Related Commands

命令	Description
logout	从 CLI 会话注销。

expert

要进入某些程序所需的专家模式，请使用 **expert** 命令。

expert

Command History

版本	修改
6.1	引入了此命令。

使用指南

仅当书面程序指出必须使用或思科技术支持中心告知使用专家模式时，才使用专家模式。

⚠

注意 您可能能够在专家模式下执行其结果未反映在 设备管理器中的命令。仅在专家模式下使用记录的命令，或按照思科技术支持的指示使用命令，以避免出现意外结果。

示例

以下示例显示如何进入和退出专家模式。专家模式提示符显示 username@hostname 信息。

```
> expert
admin@firepower:~$
admin@firepower:~$ exit
logout
>
```

Related Commands

命令	Description
exit	从专家模式退出。

failover active

要将备用设备 切换到主用状态，请使用 **failover active** 命令。要将主用设备 切换到备用状态，请使用此命令的 **no** 形式。

failover active
no failover active

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用 **failover active** 命令从备用设备发起故障转移，或使用 **no failover active** 命令从主用设备发起故障转移。您可以使用此功能使故障设备恢复服务，或强制主用设备离线以进行维护。如果不使用“状态故障转移”，所有活动连接都将被丢弃，并且在进行故障切换之后必须由客户端重新建立。

示例

以下示例将备用设备切换为主用设备：

```
> failover active
```

Related Commands

命令	Description
failover reset	使设备从故障状态变为备用状态。

failover exec

要在故障转移对中的特定设备上执行命令，请使用 **failover exec** 命令。

failover exec {**active** | **standby** | **mate**} *cmd_string*

Syntax Description

active	指定在故障转移对中的主用设备 上执行命令。
cmd_string	要执行的命令。有关支持的命令，请参阅 CLI 帮助。
mate	指定在故障转移对等设备上执行命令。
standby	指定在故障转移对中的备用设备 上执行命令。

Command History

版本	修改
6.1	引入了此命令。

使用指南

您可以使用 **failover exec** 命令向故障转移对中的特定设备发送命令。

命令的输出显示在当前终端会话中，所以您可以使用 **failover exec** 命令在对等设备上发出 **show** 命令并在当前终端中查看结果。

您必须拥有足够在本地设备上执行命令的权限才能在对等设备上执行命令。

限制

- 命令完成和情景帮助对于 *cmd_string* 参数中的命令不可用。
- 不能将 **debug** (**undebug**) 命令与 **failover exec** 命令配合使用。
- 备用设备处于故障状态时，如果这种故障是因服务卡故障引起，则该设备仍可以从 **failover exec** 命令接收命令；否则远程命令执行失败。
- 不能输入递归 **failover exec** 命令，例如 **failover exec mate failover exec mate** 命令。
- 需要用户输入或确认的命令必须使用 **/nonconfirm** 选项。

示例

以下示例使用 **failover exec** 命令显示故障转移对等设备的故障转移配置。命令在主要设备（主用设备）上执行，因此所显示的信息来自辅助设备（备用设备）。

```
> failover exec mate show running-config failover
failover
failover lan interface failover GigabitEthernet0/3
failover polltime unit 1 holdtime 3
failover polltime interface 3 holdtime 15
failover link failover GigabitEthernet0/3
```

```
failover interface ip failover 10.0.5.1 255.255.255.0 standby 10.0.5.2
```

以下示例使用 **failover exec** 命令将 **show interface** 命令发送到备用设备：

```
> failover exec standby show interface
Interface GigabitEthernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps
      Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
      MAC address 000b.fcf8.c290, MTU 1500
      IP address 192.168.5.111, subnet mask 255.255.255.0
      216 packets input, 27030 bytes, 0 no buffer
      Received 2 broadcasts, 0 runts, 0 giants
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
      0 L2 decode drops
      284 packets output, 32124 bytes, 0 underruns
      0 output errors, 0 collisions
      0 late collisions, 0 deferred
      input queue (curr/max blocks): hardware (0/0) software (0/0)
      output queue (curr/max blocks): hardware (0/1) software (0/0)
  Traffic Statistics for "outside":
      215 packets input, 23096 bytes
      284 packets output, 26976 bytes
      0 packets dropped
      1 minute input rate 0 pkts/sec,  21 bytes/sec
      1 minute output rate 0 pkts/sec,  23 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  21 bytes/sec
      5 minute output rate 0 pkts/sec,  24 bytes/sec
      5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet0/1 "inside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps
      Auto-Duplex(Half-duplex), Auto-Speed(10 Mbps)
      MAC address 000b.fcf8.c291, MTU 1500
      IP address 192.168.0.11, subnet mask 255.255.255.0
      214 packets input, 26902 bytes, 0 no buffer
      Received 1 broadcasts, 0 runts, 0 giants
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
      0 L2 decode drops
      215 packets output, 27028 bytes, 0 underruns
      0 output errors, 0 collisions
      0 late collisions, 0 deferred
      input queue (curr/max blocks): hardware (0/0) software (0/0)
      output queue (curr/max blocks): hardware (0/1) software (0/0)
  Traffic Statistics for "inside":
      214 packets input, 23050 bytes
      215 packets output, 23140 bytes
      0 packets dropped
      1 minute input rate 0 pkts/sec,  21 bytes/sec
      1 minute output rate 0 pkts/sec,  21 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  21 bytes/sec
      5 minute output rate 0 pkts/sec,  21 bytes/sec
      5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet0/2 "failover", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps
      Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
      Description: LAN/STATE Failover Interface
      MAC address 000b.fcf8.c293, MTU 1500
      IP address 10.0.5.2, subnet mask 255.255.255.0
      1991 packets input, 408734 bytes, 0 no buffer
      Received 1 broadcasts, 0 runts, 0 giants
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
```

```
      0 L2 decode drops
      1835 packets output, 254114 bytes, 0 underruns
      0 output errors, 0 collisions
      0 late collisions, 0 deferred
      input queue (curr/max blocks): hardware (0/0) software (0/0)
      output queue (curr/max blocks): hardware (0/2) software (0/0)
  Traffic Statistics for "failover":
      1913 packets input, 345310 bytes
      1755 packets output, 212452 bytes
      0 packets dropped
      1 minute input rate 1 pkts/sec,  319 bytes/sec
      1 minute output rate 1 pkts/sec,  194 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 1 pkts/sec,  318 bytes/sec
      5 minute output rate 1 pkts/sec,  192 bytes/sec
      5 minute drop rate, 0 pkts/sec
...
```

以下示例展示当向对等设备发出非法命令时返回的错误消息：

```
> failover exec mate bad command
bad command
  ^
ERROR: % Invalid input detected at '^' marker.
```

以下示例展示在禁用故障转移的情况下使用 **failover exec** 命令时返回的错误消息：

```
> failover exec mate show failover
ERROR: Cannot execute command on mate because failover is disabled
```

Related Commands

命令	Description
debug fover	显示故障转移相关的调试消息。
debug xml	显示 **failover exec** 命令使用的 XML 解析器的调试消息。
show failover exec	显示 **failover exec** 命令模式。

failover reload-standby

要强制备用设备重新启动，请使用 **failover reload-standby** 命令。

failover reload-standby

Command History

版本	修改
6.1	引入了此命令。

使用指南

当故障切换设备不同步时，请使用此命令。备用设备会重新启动并在完成启动后与主用设备重新同步。

示例

以下示例展示如何在主用设备上使用 **failover reload-standby** 命令强制备用设备重新启动：

```
> failover reload-standby
```

failover reset

要将故障设备恢复为正常状态，请使用 **failover reset** 命令。

failover reset

Command History

版本	修改
6.1	引入了此命令。

使用指南

failover reset 命令允许您将故障设备 切换为无故障状态。 **failover reset** 命令可在任一设备上输入，但我们建议您始终在主用设备上输入该命令。在主用设备输入 **failover reset** 命令将使备用设备“无故障”。

可以使用 **show failover** 命令显示设备的故障转移状态。

示例

以下示例展示将故障设备切换为无故障状态：

```
> failover reset
```

Related Commands

命令	Description
show failover	显示有关设备的故障转移状态的信息。

file copy

要通过 FTP 将文件从公共目录传输到远程主机，请使用 **file copy** 命令。

file copy *host_name user_id path filename_1* [*filename_2 . . . filename_n*]

Syntax Description

host_name	指定目标远程主机的名称或 IP 地址。
user_id	指定远程主机上的用户。
path	指定远程主机上的目的路径。
filename_1 through *filename_n*	指定要从公共目录传输的文件的名称。如果指定了多个文件名，则必须以空格分隔它们。此参数支持通配符。

Command Default

此命令仅从系统写入故障排除文件的通用目录传输文件。

Command History

版本	修改
6.0.1	引入了此命令。

示例

此示例将公共目录中的所有文件传输到 **/pub** 通过用户 **jdoe**访问的远程主机 **sentinel** 上的目录：

```
> file copy sentinel jdoe /pub *
```

Related Commands

命令	Description
file list	列出公共目录中的文件。
file delete	从公共目录中删除文件。
file secure-copy	通过 SCP 传输公共目录中的文件。

file delete

要清除公共目录中的文件，请使用 **file delete** 命令。

file delete *filename_1* [*filename_2 . . . filename_n*]

Syntax Description

filename_1 through *filename_n*	指定要从公用目录中删除的文件的名称。如果指定了多个文件名，则必须以空格分隔它们。此参数支持通配符。

Command Default

此命令仅对系统写入故障排除文件的通用目录中的文件起作用。

Command History

版本	修改
6.0.1	引入了此命令。

示例

此示例删除单个文件：

```
> file delete 10.83.170.31-43235986-2363-11e6-b278-aff0a43948fe-troubleshoot.tar.gz
```

Related Commands

命令	Description
file list	列出公共目录中的文件。
file copy	通过 FTP 传输公共目录中的文件。
file secure-copy	通过 SCP 传输公共目录中的文件。

file list

要列出公共目录中的文件，请使用 **file list** 命令。

file list ［*filename_1 . . . filename_n*］

Syntax Description

filename_1 through *filename_n*	指定要从公共目录列出的文件的名称。如果指定了多个文件名，则必须以空格分隔它们。此参数支持通配符。

Command History

版本	修改
6.0.1	引入了此命令。

使用指南

此命令仅列出系统写入故障排除文件的通用目录中的文件。如果未指定文件名，则列出公共目录中的所有文件。

示例

此示例列出了通用目录的内容：

```
> file list
May 26 17:46        137474048 /core_1464284811_rackham-sfr.cisco.com_diskmanager_11.21145
Jun 27 20:36       1464696832 /core_1467059810_rackham-sfr.cisco.com_lina_6.21293
```

Related Commands

命令	Description
file copy	通过 FTP 传输公共目录中的文件。
file delete	从公共目录中删除文件。
file secure-copy	通过 SCP 传输公共目录中的文件。

file secure-copy

要通过 SCP 将文件从通用目录传输到远程主机，请使用 **file secure-copy** 命令。

file secure-copy *host_name user_id path filename_1* [*filename_2 . . . filename_n*]

Syntax Description

host_name	指定目标远程主机的名称或 IP 地址。
user_id	指定远程主机上的用户。
path	指定远程主机上的目的路径。
filename_1 through *filename_n*	指定要从公共目录传输的文件的名称。如果指定了多个文件名，则必须以空格分隔它们。此参数支持通配符。

Command Default

此命令仅从系统写入故障排除文件的通用目录传输文件。

Command History

版本	修改
6.0.1	引入了此命令。

示例

此示例将公共目录中的所有文件传输到 **/tmp** 通过用户 **jdoe**访问的远程主机 **101.123.31.1** 上的目录：

```
> file secure-copy 101.123.31.1 jdoe /tmp *
```

Related Commands

命令	Description
file copy	通过 FTP 传输公共目录中的文件。
file delete	从公共目录中删除文件。
file list	列出公共目录中的文件。

fsck

要执行文件系统检查并修复损坏，请使用 **fsck** 命令。

fsck /noconfirm disk*n*:

Syntax Description

disk*n*:	指定闪存驱动器，其中 *n* 是驱动器编号。
/noconfirm	指定命令在不提示的情况下运行。此关键字是必需的。

Command History

版本	修改
6.1	引入了此命令。

使用指南

fsck 命令检查并尝试修复损坏的文件系统。请在尝试更永久性的修复过程之前使用此命令。

如果 FSCK 实用程序修复磁盘损坏实例（例如由于电源故障或异常关闭导致的损坏），则会创建名为 FSCKxxx.REC 的恢复文件。这些文件可以包含 FSCK 在运行时恢复的文件的一小部分或整个文件。在极少数情况下，您可能需要检查这些文件以恢复数据；通常不需要这些文件，可以将其安全删除。

注释 FSCK 实用程序在启动时自动运行，因此，即使没有手动输入 **fsck** 命令，您也可能看到这些恢复文件。

示例

以下示例展示如何检查闪存的文件系统：

```
> fsck /noconfirm disk0:
```

Related Commands

命令	Description
delete	删除用户可见的所有文件。
erase	删除所有文件并格式化闪存。
format	格式化文件系统。

help

要显示指定命令的帮助信息，请使用 **help** 命令。

help { 命令 | **?**}

Syntax Description

?	显示所有可获得帮助的命令。
command	指定为其显示 CLI 帮助的命令。

Command History

版本	修改
6.1	引入了此命令。

使用指南

help 命令显示有关某些命令的帮助信息。您可以输入 **help** 命令后跟命令名，以获取某个命令的帮助。如果不指定命令名称并输入 **?**，则列出所有具有帮助的命令。

您还可以通过输入？输入部分命令后。这将显示命令字符串中该位置的有效参数。

示例

以下示例展示如何显示 **traceroute** 命令的帮助：

```
> help traceroute
USAGE:
        traceroute <destination> [source <src_address|src_intf>]
                   [numeric] [timeout <time>] [ttl <min-ttl> <max-ttl>]
                   [probe <probes>] [port <port-value>] [use-icmp]
DESCRIPTION:
traceroute      Print the route packets take to a network host
SYNTAX:
destination     Address or hostname of destination
src_address     Source address used in the outgoing probe packets
src_intf        Interface through which the destination is accessible
numeric         Do not resolve addresses to hostnames
time            The time in seconds to wait for a response to a probe
min-ttl         Minimum time-to-live value used in probe packets
max-ttl         Maximum time-to-live value used in probe packets
probes          The number of probes to send for each TTL value
port-value      Base UDP destination port used in probes
use-icmp        Use ICMP probes instead of UDP probes
```

history

要显示当前会话的命令行历史记录，请使用 **history** 命令。

history *limit*

Syntax Description

limit	历史记录列表的大小（以条目数表示）。要将大小设置为无限制，即查看完整历史记录，请输入 0。

Command History

版本	修改
6.1	引入了此命令。

使用指南

您还可以使用向上箭头滚动浏览过去的命令。

历史记录视图包括命令输入顺序的序列号。

示例

以下示例显示命令历史记录。

```
> history 0
   48  show environment
   49  show network-static-routes
   50  show network
   51  show running-config
   52  show service-policy
   53  show ntp
   54  show cpu
   55  show memory
   56  history 0
>
```

logging savelog

要将日志缓冲区保存到闪存，请使用 **logging savelog** 命令。

logging savelog ［*savefile*］

Syntax Description

savefile	（可选）已保存日志的文件名。如果您未指定文件名，则系统将使用如下所示的默认时间戳格式保存日志文件： `LOG-YYYY-MM-DD-HHMMSS.TXT` 其中 *YYYY* 是年，*MM* 是月，*DD* 是月日期，*HHMMSS* 是时间（以小时、分钟和秒为单位）。

Command History

版本	修改
6.1	引入了此命令。

使用指南

在您将日志缓冲区保存到闪存之前，您必须启用日志记录到缓冲区；否则日志缓冲区始终不会将数据保存到闪存。但是，如果配置的日志记录缓冲区大小超过 2 MB，则内部日志缓冲区不会写入闪存。使用 管理中心 （远程）或 设备管理器 （本地）配置缓冲区日志记录。

注释 **logging savelog** 命令不会清除缓冲区。要清除缓冲区，请使用 **clear logging buffer** 命令。

示例

以下示例使用文件名 latest-logfile.txt 将日志缓冲区保存到闪存：

```
> logging savelog latest-logfile.txt
>
```

Related Commands

命令	Description
clear logging buffer	清除包含的所有系统日志消息的日志缓冲区。
copy	将文件从一个位置复制到另一个位置，包括复制到 TFTP 或 FTP 服务器。
delete	从磁盘分区删除文件（如已保存的日志文件）。

logout

要退出 CLI，请使用 **logout** 命令。

logout

Command History

版本	修改
6.1	引入了此命令。

使用指南

logout 命令允许您注销设备并结束 CLI 会话。您也可以使用 **exit** 命令。

示例

以下示例显示如何注销设备：

```
> logout
```

memory caller-address

要为呼叫跟踪或主叫方 PC 配置特定范围的程序内存，以帮助隔离内存问题，请使用 **memory caller-address** 命令。调用方 PC 是调用内存分配基元的程序的地址。要删除地址范围，请使用此命令的 no 形式。

memory caller-address *startPC endPC*
no memory caller-address

Syntax Description

endPC	指定内存块的结束地址范围。
startPC	指定内存块的开始地址范围。

Command Default

实际调用方 PC 会被记录以用于内存跟踪。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用 **memory caller-address** 命令将内存问题隔离到特定的内存块。

在某些情况下，内存分配基元的实际调用方 PC 是程序中许多位置使用的已知库功能。要隔离程序中的个别位置，请配置库功能的开始和结束程序地址，从而记录库功能调用方的程序地址。

注释 启用调用方地址跟踪时，设备的性能可能会临时下降。

示例

以下示例显示了使用 **memory caller-address** 命令配置的地址范围，以及 **show memory caller-address** 命令的结果显示：

```
> memory caller-address 0x00109d5c 0x00109e08
> memory caller-address 0x009b0ef0 0x009b0f14
> memory caller-address 0x00cf211c 0x00cf4464
> show memory caller-address
Move down stack frame for the addresses:
pc = 0x00109d5c-0x00109e08
pc = 0x009b0ef0-0x009b0f14
pc = 0x00cf211c-0x00cf4464
```

Related Commands

命令	Description
memory profile enable	启用对内存使用（内存分析）的监控。

命令	Description
memory profile text	配置要分析的内存的文本范围。
show memory	显示可供操作系统使用的最大物理内存量和当前可用内存量的摘要。
show memory binsize	显示为特定存储空间分配的数据块的摘要信息。
show memory profile	显示设备内存使用情况（分析）的信息。
show memory caller-address	显示设备上配置的地址范围。

memory delayed-free-poisoner

使用 **memory delayed-free-poisoner** 命令设置延迟可用内存毒化工具的参数。要启用延迟的可用内存毒化工具，请使用 **memory delayed-free-poisoner enable** 命令。要禁用 delayed free-memory poisoner 工具，请使用此命令的 **no** 形式。delayed free-memory poisoner 工具可用于监视可用的内存在被应用释放后有何变化。

memory delayed-free-poisoner {**enable** | **desired-fragment-count** *frag_count* | **desired-fragment-size** *frag-size* | **threshold** *heap_use_percent* | **validate** | **watchdog-percent** *watchdog_limit*}
no memory delayed-free-poisoner enable

Syntax Description

enable	启动延迟的可用内存毒化工具。
desired-fragment-count *frag_count*	设置要在毒化器队列中保留的内存分段数。合法值范围为 0 到 8192；默认值为 16
desired-fragment-size *Frag-size*	设置要保留在毒化器队列中的连续可用内存分段的大小（以字节为单位）。合法值范围为 0 到 268435456；默认值为 102400。
threshold *heap_use_percent*	设置系统将从毒化器队列中释放内存的系统内存使用百分比阈值，范围为 0 到 100。默认值为 100。
validate	强制验证 delay-free-poisoner 队列中的所有元素。
watchdog-percent *watchdog_limit*	将监视器限制设置为监视器阈值的百分比，即 15 秒。值范围为 10 到 100。默认值为 50。

Command Default

memory delayed-free-poisoner enable 命令默认禁用。

desired-fragment-count 默认值为 16。

desire-fragment-size 默认值为 102400。

watchdog-percent 默认值为 50。

Command History

版本	修改
6.1	引入了此命令。

使用指南

启用 delayed free-memory poisoner 工具对内存使用和系统性能有重大影响。此命令只能在思科技术支持中心的监督下使用。在大量使用系统的生产环境下不应该运行此工具。

启用此工具时，要求释放设备上运行的应用可用内存的请求将写入 FIFO 队列。当每个请求写入毒化器队列时，低层内存管理不需要的每个关联内存字节会写入值 0xcc 而“中毒”。

释放的内存请求会一直保留在队列中，直到应用要求的内存超过系统可用内存。当需要更多内存时，毒化器至少会在其队列中查找 **desired-fragment-count** 内存缓冲区，从 **desired-fragment-size** 队列字

节中提取该内存，并对其进行验证。您可以通过更改 **desired-fragment-size** 和 **desired-fragment-count** 的值来调整毒化器满足大内存请求所需的时间。

如果内存未经修改，将返回到系统可用内存池，然后该毒化器从发出初始请求的应用重新发出内存请求。此流程会重复到为请求的应用释放足够的内存为止。

如果中毒的内存已修改，则系统发生故障并产生诊断输出来确定故障的原因。

延迟释放毒化器包括一种监视机制，可防止流程过度使用资源。监视器阈值是15秒，当流程在这段时间内持续执行而不放弃 CPU 时，中毒者会强制系统崩溃。

您可以通过设置监视器限制（表示15秒看门狗阈值的百分比）来调整监视器行为；默认值为50%。因此，当延迟释放毒化器处于活动状态时，如果流程在不放弃 CPU 的情况下连续执行 7.5 秒，则该流程的进一步内存分配请求将失败，直到重新安排该进程。您可以通过更改监视程序限制的值来调整此行为。

为防止内存碎片过多并减少系统 CPU 负载，可以设置毒化器自动将内存从其队列释放到 **threshold** 系统内存池的可用内存使用率百分比。（默认情况下，在系统内存耗尽之前，投毒器不会从其队列中释放内存。）

delayed free-memory poisoner 工具自动定期验证队列的所有元素。您还可以使用 **memory delayed-free-poisoner validate** 命令手动启动验证。如果有元素包含非预期的值，则系统发生故障并产生诊断输出来确定故障的原因。如果没有出现非预期的值，这些元素将保留在队列中被工具正常处理； **memory delayed-free-poisoner validate** 命令不会使队列中的内存返回到系统内存池。

若使用此命令的 **no** 形式，则队列中请求引用的所有内存不经过验证即返回到可用内存池，同时清除所有统计数据计数器。

示例

以下示例启用 delayed free-memory poisoner 工具：

```
> memory delayed-free-poisoner enable
```

下面是 delayed free-memory poisoner 工具检测到非法内存重用时的示例输出：

```
delayed-free-poisoner validate failed because a
        data signature is invalid at delayfree.c:328.
    heap region:    0x025b1cac-0x025b1d63 (184 bytes)
    memory address: 0x025b1cb4
    byte offset:    8
    allocated by:   0x0060b812
    freed by:       0x0060ae15
Dumping 80 bytes of memory from 0x025b1c88 to 0x025b1cd7
025b1c80:                         ef cd 1c a1 e1 00 00 00  |           ........
025b1c90: 23 01 1c a1 b8 00 00 00 15 ae 60 00 68 ba 5e 02  |  #.........`.h.^.
025b1ca0: 88 1f 5b 02 12 b8 60 00 00 00 00 00 6c 26 5b 02  |  ..[...`.....l&[.
025b1cb0: 8e a5 ea 10 ff ff ff ff cc cc cc cc cc cc cc cc  |  ................
025b1cc0: cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc  |  ................
025b1cd0: cc cc cc cc cc cc cc cc                         |  ........
An internal error occurred.  Specifically, a programming assertion was
violated.  Copy the error message exactly as it appears, and get the
output of the show version command and the contents of the configuration
file.  Then call your technical support representative.
```

```
assertion "0" failed: file "delayfree.c", line 191
```

下表描述了输出的主要部分。

表 *1:* 非法内存使用输出说明

字段	Description
heap region	可供请求的应用使用的地址区域以及内存区域大小。这与请求的大小不同，根据发出内存请求时系统分配内存的方式，它可能小于请求的大小。
memory address	内存中检测到故障的位置。
byte offset	字节偏移与堆区域的开头有关，可在结果用于保存以此地址开头的数据结构时用于查找修改的字段。0 或大于堆区域字节计数的值可能表示问题是低层堆数据包中的值异常。
allocated by/freed by	指示最近发出的、涉及此特定内存区域的 malloc/calloc/realloc 和释放调用的地址。
Dumping...	一个或两个内存区域的转储，具体取决于检测到的故障相距堆内存区域开头的距离。任何系统堆信头后的八个字节是此工具用来保存各系统报头散列值以及队列链路的内存。区域中在遇到任何系统堆尾部之前的所有其他字节应设置为 0xcc。

Related Commands

命令	Description
clear memory delayed-free-poisoner	清除 delayed free-memory poisoner 工具队列和统计信息。
show memory delayed-free-poisoner	显示 delayed free-memory poisoner 工具队列使用摘要。

memory logging

要启用内存日志记录，请使用**memory logging**命令。要禁用内存日志记录功能，请使用此命令的**no**形式。

memory logging 1024-4194304 ［**wrap** ［**size** ［**1-2147483647**］ | **process** *process-name*］
no memory logging

Syntax Description

1024-4194304	指定内存日志记录缓冲区中的日志记录条目数。这是唯一需要指定的参数。
process *process-name*	指定要监控的进程。 注释 Checkheaps 进程被当作一个进程完全忽略，因为它以非标准方式使用内存分配器。
size 1-2147483647	指定要监控的条目的大小和数量。
wrap	回绕时保存缓冲区。缓冲区只能保存一次。如果它wrap多次，会被覆写。当缓冲区wrap时，系统会将触发器发送到事件管理器，以启用数据保存。

Command History

版本	修改
6.1	引入了此命令。

使用指南

要更改内存日志记录参数，必须将其禁用，然后重新启用。使用 **show memory logging** 命令查看日志。

示例

以下示例启用内存日志记录：

```
> memory logging 202980
```

Related Commands

命令	Description
show memory logging	显示内存日志记录结果。

memory profile enable

要启用内存使用情况监控（内存分析），请使用 **memory profile enable** 命令。要禁用内存分析功能，请使用此命令的 **no** 形式。

memory profile enable ［**peak** *peak_value*］
no memory profile enable ［**peak** *peak_value*］

Syntax Description

peak *peak_value*	指定内存使用阈值，达到此阈值就会在峰值使用缓冲区中保存内存使用率快照。此缓冲区的内容以后可用来分析以确定系统的峰值内存需求。

Command Default

内存分析默认禁用。

Command History

版本	修改
6.1	引入了此命令。

使用指南

在启用内存分析之前，必须先使用 **memory profile text** 命令配置要分析的内存文本范围。

部分内存由分析系统保留，直到您输入 **clear memory profile** 命令。请参阅 **show memory profile status** 命令的输出。

注释 启用内存分析时，设备的性能可能会临时下降。

示例

以下示例启用内存分析：

```
> memory profile enable
```

Related Commands

命令	Description
memory profile text	配置要分析的内存的文本范围。
show memory profile	显示设备内存使用情况（分析）的信息。

memory profile text

要配置内存的程序文本范围，请使用 **memory profile text** 命令。要禁用，请使用此命令的 no 形式。

memory profile text {*startPC endPC* | **all**} *resolution*
no memory profile text {*startPC endPC* | **all**} *resolution*

Syntax Description

all	指定内存块的整个文本范围。
endPC	指定内存块的整个文本范围。
resolution	您必须为源文本区域设置跟踪分辨率，范围为 1-44582263。
startPC	指定内存块的开始文本范围。

Command History

版本	修改
6.1	引入了此命令。

使用指南

如果文本范围小，分辨率“4”通常便可跟踪对指令的调用。如果文本范围较大，低分辨率对第一遍可能够了，但在下一遍时范围可能需要缩小到一组更小的区域。

使用 **memory profile text** 命令输入文本范围后，必须输入 **memory profile enable** 命令以开始内存分析。内存分析默认禁用。

注释 启用内存分析时，设备的性能可能会临时下降。

示例

以下示例显示如何在分辨率为 100 的条件下配置要分析的内存文本范围。

```
> memory profile text all 100
```

以下示例显示文本范围的配置和内存分析的状态 (OFF)：

```
> show memory profile status
InUse profiling: OFF
Peak profiling: OFF
Memory used by profile buffers: 0 bytes
Profile:
0x00007efc3e0227a8-0x00007efc40aa1f8e(00000100)
```

注释 要开始内存分析，必须输入 **memory profile enable** 命令。内存分析默认禁用。

Related Commands

命令	Description
clear memory profile	清除内存分析功能保留的缓冲区。
memory profile enable	启用对内存使用（内存分析）的监控。
show memory profile	显示设备内存使用情况（分析）的信息。

memory tracking

要启用堆内存请求跟踪，请使用 **memory tracking** 命令。要禁用内存日志跟踪功能，请使用此命令的 **no** 形式。

memory tracking {**enable** | **allocates-by-threshold** *min_allocates* | **bytes-threshold** *min_bytes* | **filter-from-address-pool** *address*}
no memory tracking enable

Syntax Description

enable	启用内存跟踪。
allocates-by-threshold *min_allocates*	调用方的地址池条目必须至少进行此数量的分配调用，范围为 0-4294967295。
bytes-threshold *min_bytes*	调用方的地址池条目必须至少消耗这么多字节的内存才能包含在内，范围为 0-4294967295。
filter-from-address-pool *address*	排除此地址的地址池条目。要确定地址，请先启用跟踪，然后使用 show memory tracking address。在“内存跟踪地址池”列表中查找“分配者”地址。例如，如果您看到以下内容： ...allocated by 0x00007efc3f80e508 您可以使用以下命令将其排除： **filter-from-address-pool 0x00007efc3f80e508**

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例启用跟踪堆内存请求：

```
> memory tracking enable
```

Related Commands

命令	Description
clear memory tracking	清除所有当前收集的信息。
show memory tracking	显示内存跟踪结果。

more

要显示文件的内容，请使用 **more** 命令。

more [**/ascii** | **/binary** | **/ebcdic** | **disk0:** | **disk1:** | **flash:** | **ftp:** | **http:** | **https:** | **tftp:**] *filename*

Syntax Description

/ascii	（可选）在二进制模式下显示二进制文件和 ASCII 文件。
/binary	（可选）在二进制模式下显示任何文件。
/ebcdic	（可选）以 EBCDIC 显示二进制文件。
disk0:	（可选）显示内部闪存上的文件。
disk1:	（可选）显示外部闪存卡上的文件。
filename	指定要显示的文件的名称。
flash:	（可选）指定内部闪存，后跟冒号。在ASA 5500 系列自适应安全设备中，**flash** 关键字是 **disk0**的别名。
ftp:	（可选）显示 FTP 服务器上的文件。
http:	（可选）显示网站上的文件。
https:	（可选）显示安全网站上的文件。
tftp:	（可选）显示 FTP 服务器上的文件。

Command Default

ASCII 模式。

Command History

版本	修改
6.1	引入了此命令。

使用指南

system support view-files 命令是查找和查看日志文件的更好选择。

示例

以下示例显示如何显示名为“test.cfg”的本地文件的内容：

```
> more test.cfg
: Saved
: Written by enable_15 at 10:04:01 Apr 14 2005
XXX Version X.X(X)
nameif vlan300 outside security10
enable password 8Ry2YjIyt7RRXU24 encrypted
```

```
passwd 2KFQnbNIdI.2KYOU encrypted
ciscoasa test
fixup protocol ftp 21
fixup protocol h323 H225 1720
fixup protocol h323 ras 1718-1719
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
access-list deny-flow-max 4096
access-list alert-interval 300
access-list 100 extended permit icmp any any
access-list 100 extended permit ip any any
pager lines 24
icmp permit any outside
mtu outside 1500
ip address outside 172.29.145.35 255.255.0.0
no asdm history enable
arp timeout 14400
access-group 100 in interface outside
!
interface outside
!
route outside 0.0.0.0 0.0.0.0 172.29.145.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 rpc 0:10:00 h3
23 0:05:00 h225 1:00:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
snmp-server host outside 128.107.128.179
snmp-server location my_context, USA
snmp-server contact admin@example.com
snmp-server community public
no snmp-server enable traps
floodguard enable
fragment size 200 outside
no sysopt route dnat
telnet timeout 5
ssh timeout 5
terminal width 511
gdb enable
mgcp command-queue 0
Cryptochecksum:00000000000000000000000000000000
: end
```

Related Commands

命令	Description
cd	更改为指定的目录。
pwd	系统随即会显示当前工作目录。
system support view-files	查找并查看日志文件的内容。

nslookup (deprecated)

要查找完全限定域名 (FQDN) 的 IP 地址或 reverse，请使用 **nslookup** 命令。

nslookup {*hostname* | *ip_address*}

Syntax Description

hostname	要查找其 IP 地址的主机的完全限定域名。例如，www.example.com。
ip_address	要查找其完全限定域名的主机的 IP 地址。

Command History

版本	修改
6.1	引入了此命令。
6.6	此命令不再有效，已弃用。
7.1	此命令已被删除并替换为 **dig**。

使用指南

某些允许完全限定域名的命令无法使用为管理接口配置的 DNS 服务器来查找名称的 IP 地址。如果没有为通过数据接口的命令配置 DNS 服务器，请使用 命令确定 IP 地址，然后在 **nslookup** 命令中使用 IP 地址。

nslookup 命令还可用于确定给定 IP 地址的完全限定域名。

示例

以下示例查找 www.cisco.com 的 IP 地址。初始服务器和地址信息显示 DNS 服务器（可以是完全限定域名）、IP 地址和端口。（此示例中的地址是伪造的。）以下信息显示您输入的名称的规范（实际）主机名和 IP 地址。

```
> nslookup www.cisco.com
Server:         10.102.6.247
Address:        10.102.6.247#53

www.cisco.com   canonical name = origin-www.cisco.com.
Name:   origin-www.cisco.com
Address: 173.37.145.84
```

以下示例显示如何执行反向查找并确定 IP 地址的主机名。初始信息适用于所使用的 DNS 服务器。映射的主机名由 **name =** 字段指示。

```
> nslookup 173.37.145.84
Server:         10.102.6.247
Address:        10.102.6.247#53

84.145.37.173.in-addr.arpa      name = www2.cisco.com.
```

packet-tracer

要通过指定 5 元组测试防火墙规则来启用数据包跟踪功能以进行故障排除，请使用 **packet-tracer** 命令。为清楚起见，下面分开展示了 ICMP、TCP/UDP 和 IP 数据包建模的语法。您可以使用 **pcap** 关键字重放多个数据包并跟踪完整的工作流程。

packet-tracer input *ifc_name* **icmp** {*sip* | **user** *username*} *type code* [*ident*] {*dip* | **fqdn** *fqdn-string*} [**detailed**] [**xml**]
packet-tracer input *ifc_name* {**tcp** | **udp**} {*sip* | **user** *username*} *sport* {*dip* | **fqdn** *fqdn-string*} *dport* [**detailed**] [**xml**]
packet-tracer input *ifc_name* **rawip** {*sip* | **user** *username*} *protocol* {*dip* | **fqdn** *fqdn-string*} [**detailed**] [**xml**]
packet-tracer input *ifc_name* **pcap** *pcap_filename* [**bypass-checks** | **decrypted** | **detailed** | **persist** | **transmit** | **xml** | **json** | **force**]

Syntax Description

bypass-checks	（可选）绕过针对模拟数据包的安全检查。
decrypted	（可选）将模拟数据包视为 IPsec/SSL VPN 解密。
code	指定 ICMP 数据包跟踪的 ICMP 代码。
detailed	（可选）提供详细的跟踪结果信息。
dip	指定数据包跟踪的目标 IPv4 或 IPv6 地址。
dport	指定 TCP/UDP/SCTP 数据包跟踪的目标端口。
fqdn *fqdn-string*	指定主机的完全限定域名。仅支持 IPv4 的 FQDN。
force	删除现有的 pcap 跟踪并执行新的 pcap 文件。
icmp	指定要使用的协议为 ICMP。
ident	（可选。）指定 ICMP 数据包跟踪的 ICMP 标识符。
inline-tag *tag*	指定要嵌入第 2 层 CMD 信头中的安全组标记值。有效值范围为 0 到 65533。
input *ifc_name*	指定在其上跟踪数据包的源接口的名称。
json	（可选）以 JSON 格式显示跟踪结果。
pcap	指定 pcap 作为输入。
pcap_filename	包含要跟踪的数据包的 pcap 文件名。
protocol	指定原始 IP 数据包跟踪的协议编号，从 0 到 255。
persist	（可选）启用长期跟踪，并在集群中进行跟踪。

rawip	指定要使用的协议为原始 IP。
sip	指定数据包跟踪的源 IPv4 或 IPv6 地址。
sport	指定 TCP/UDP/SCTP 数据包跟踪的源端口。
tcp	指定要使用的协议为 TCP。
transmit	（可选）允许从设备传输模拟数据包
type	指定 ICMP 数据包跟踪的 ICMP 代码。
udp	指定要使用的协议为 UDP。
user *username*	如果您要指定用户为源 IP 地址，请以域\用户格式指定用户身份。跟踪中使用最近为用户映射的地址（如有）。
xml	（可选）以 XML 格式显示跟踪结果。

Command History

版本	修改
6.1	引入了此命令。
6.6	增强了输出，以提供在路由数据包时允许/丢弃数据包的具体原因。
7.1	增强了 packet-tracer 命令，以允许 pcap 文件作为跟踪的输入。

使用指南

除捕获数据包外，还可以通过 threat defense 设备跟踪数据包的寿命，查看它的行为是否与预期一致。**packet-tracer** 命令使您能够执行以下操作：

- 调试生产网络中的所有数据包丢弃。
- 验证配置是否达到预期。
- 显示适用于数据包和导致规则添加的 CLI 行的所有规则。
- 显示数据路径中数据包更改的时间线。
- 向数据路径中注入跟踪数据包。

packet-tracer 命令可提供有关数据包的详细信息，以及 threat defense 设备对数据包的处理方式。如果配置的命令没有导致数据包丢弃，则 **packet-tracer** 命令以易读格式提供有关原因的信息。例如，如果因无效信头验证丢弃了数据包，将显示以下消息：“数据包因错误的 IP 报头 [原因] 而丢弃。”

packet-tracer 注入和跟踪单个数据包时，使用 **pcap** 关键字可使数据包跟踪器重放多个数据包（最多 100 个数据包）并跟踪整个数据流。您可以提供 pcap 文件作为输入，并以 XML 或 JSON 格式获取结果以进行进一步分析。要清除跟踪输出，请使用 **clear packet-tracer** 的 **pcap trace** 子命令。在跟踪过程中，您无法使用跟踪输出。

示例

以下示例显示如何使用 pcap 文件作为输入运行 packet-tracer：

```
> packet-tracer input inside pcap http_get.pcap detailed xml
```

以下示例显示如何通过清除现有的 pcap 跟踪缓冲区并提供 pcap 文件作为输入来运行 packet-tracer：

```
> packet-tracer input inside pcap http_get.pcap force
```

以下示例跟踪从 10.100.10.10 到 10.100.11.11 的 HTTP 端口的 TCP 数据包。结果表明隐式拒绝访问规则将丢弃该数据包。

```
> packet-tracer input outside tcp 10.100.10.10 80 10.100.11.11 80
Phase: 1
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 10.86.116.1 using egress ifc  outside
Phase: 2
Type: ACCESS-LIST
Subtype:
Result: DROP
Config:
Implicit Rule
Additional Information:
Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
output-status: up
output-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule
```

以下示例跟踪具有下一跳 ARP 条目的直连主机中的 TCP 数据包。

```
firepower(config)# packet-tracer input inside tcp 192.168.100.100 12345 192.168.102.102 80
 detailed
Phase: 1
Type: ROUTE-LOOKUP
Subtype: No ECMP load balancing
Result: ALLOW
Config:
Additional Information:
Destination is locally connected. No ECMP load balancing.
Found next-hop 192.168.102.102 using egress ifc  outside(vrfid:0)

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group TEST global
```

```
access-list TEST advanced trust ip any any
Additional Information:
Forward Flow based lookup yields rule:
in  id=0x2ae2a8aa5e90, priority=12, domain=permit, trust
hits=17, user_data=0x2ae29aabc100, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any, vlan=0, dscp=0x0
input_ifc=any, output_ifc=any

Phase: 3
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in  id=0x2ae2a69a7240, priority=0, domain=nat-per-session, deny=false
hits=34, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=6
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=any, output_ifc=any

Phase: 4
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in  id=0x2ae2a8488800, priority=0, domain=inspect-ip-options, deny=true
hits=22, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=inside(vrfid:0), output_ifc=any

Phase: 5
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Reverse Flow based lookup yields rule:
in  id=0x2ae2a69a7240, priority=0, domain=nat-per-session, deny=false
hits=36, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=6
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=any, output_ifc=any

Phase: 6
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Reverse Flow based lookup yields rule:
in  id=0x2ae2a893e230, priority=0, domain=inspect-ip-options, deny=true
hits=10, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=outside(vrfid:0), output_ifc=any

Phase: 7
Type: FLOW-CREATION
Subtype:
```

```
Result: ALLOW
Config:
Additional Information:
New flow created with id 21, packet dispatched to next module
Module information for forward flow ...
snp_fp_inspect_ip_options
snp_fp_tcp_normalizer
snp_fp_translate
snp_fp_adjacency
snp_fp_fragment
snp_fp_tracer_drop
snp_ifc_stat

Module information for reverse flow ...
snp_fp_inspect_ip_options
snp_fp_translate
snp_fp_tcp_normalizer
snp_fp_adjacency
snp_fp_fragment
snp_fp_tracer_drop
snp_ifc_stat

Phase: 8
Type: INPUT-ROUTE-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP
Subtype: Resolve Preferred Egress interface
Result: ALLOW
Config:
Additional Information:
Found next-hop 192.168.102.102 using egress ifc  outside(vrfid:0)

Phase: 9
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop IP address to MAC
Result: ALLOW
Config:
Additional Information:
found adjacency entry for next-hop 192.168.102.102 on interface  outside
Adjacency :Active
mac address 0aaa.0bbb.00cc hits 5 reference 1

Result:
input-interface: inside(vrfid:0)
input-status: up
input-line-status: up
output-interface: outside(vrfid:0)
output-status: up
output-line-status: up
Action: allow
```

以下示例跟踪由于缺少有效的下一跳 ARP 条目而被丢弃的 TCP 数据包。请注意，丢弃原因提供了检查 ARP 表的提示。

```
<Displays same phases as in the previous example till Phase 8>

Result:
input-interface: inside(vrfid:0)
input-status: up
input-line-status: up
output-interface: outside(vrfid:0)
output-status: up
output-line-status: up
Action: drop
Drop-reason: (no-v4-adjacency) No valid V4 adjacency. Check ARP table (show arp) has entry
 for nexthop., Drop-location: frame snp_fp_adj_process_cb:200 flow (NA)/NA
```

以下示例描述了使用 NAT 和可访问的下一跳进行次优路由的数据包跟踪器。

```
firepower(config)# sh run route
route inside 0.0.0.0 0.0.0.0 192.168.100.100 1
route outside 0.0.0.0 0.0.0.0 192.168.102.102 10

firepower(config)# sh nat detail
Manual NAT Policies (Section 1)
1 (outside) to (dmz) source static src_real src_mapped  destination static dest_real
dest_mapped
translate_hits = 3, untranslate_hits = 3
Source - Origin: 9.9.9.0/24, Translated: 10.10.10.0/24
Destination - Origin: 192.168.104.0/24, Translated: 192.168.104.0/24
firepower(config)# packet-tracer input dmz tcp 192.168.104.104 12345 10.10.10.10 80 detailed


Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (outside,dmz) source static src_real src_mapped destination static dest_real dest_mapped
Additional Information:
NAT divert to egress interface outside(vrfid:0)
Untranslate 10.10.10.10/80 to 9.9.9.10/80

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group TEST global
access-list TEST advanced trust ip any any
Additional Information:
Forward Flow based lookup yields rule:
in  id=0x2ae2a8aa5e90, priority=12, domain=permit, trust
hits=20, user_data=0x2ae29aabc100, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any, vlan=0, dscp=0x0
input_ifc=any, output_ifc=any

Phase: 3
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (outside,dmz) source static src_real src_mapped destination static dest_real dest_mapped
Additional Information:
Static translate 192.168.104.104/12345 to 192.168.104.104/12345
Forward Flow based lookup yields rule:
in  id=0x2ae2a8aa4ff0, priority=6, domain=nat, deny=false
hits=4, user_data=0x2ae2a8a9d690, cs_id=0x0, flags=0x0, protocol=0
src ip/id=192.168.104.0, mask=255.255.255.0, port=0, tag=any
dst ip/id=10.10.10.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
input_ifc=dmz(vrfid:0), output_ifc=outside(vrfid:0)

Phase: 4
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in  id=0x2ae2a69a7240, priority=0, domain=nat-per-session, deny=false
```

```
hits=40, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=6
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=any, output_ifc=any

Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in  id=0x2ae2a89de1b0, priority=0, domain=inspect-ip-options, deny=true
hits=4, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=dmz(vrfid:0), output_ifc=any

Phase: 6
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
nat (outside,dmz) source static src_real src_mapped destination static dest_real dest_mapped
Additional Information:
Forward Flow based lookup yields rule:
out id=0x2ae2a8aa53d0, priority=6, domain=nat-reverse, deny=false
hits=5, user_data=0x2ae2a8a9d580, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
src ip/id=192.168.104.0, mask=255.255.255.0, port=0, tag=any
dst ip/id=9.9.9.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
input_ifc=dmz(vrfid:0), output_ifc=outside(vrfid:0)

Phase: 7
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Reverse Flow based lookup yields rule:
in  id=0x2ae2a69a7240, priority=0, domain=nat-per-session, deny=false
hits=42, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=6
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=any, output_ifc=any

Phase: 8
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Reverse Flow based lookup yields rule:
in  id=0x2ae2a893e230, priority=0, domain=inspect-ip-options, deny=true
hits=13, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=outside(vrfid:0), output_ifc=any

Phase: 9
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
```

```
New flow created with id 24, packet dispatched to next module
Module information for forward flow ...
snp_fp_inspect_ip_options
snp_fp_tcp_normalizer
snp_fp_translate
snp_fp_adjacency
snp_fp_fragment
snp_fp_tracer_drop
snp_ifc_stat

Module information for reverse flow ...
snp_fp_inspect_ip_options
snp_fp_translate
snp_fp_tcp_normalizer
snp_fp_adjacency
snp_fp_fragment
snp_fp_tracer_drop
snp_ifc_stat

Phase: 10
Type: INPUT-ROUTE-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP
Subtype: Resolve Preferred Egress interface
Result: ALLOW
Config:
Additional Information:
Found next-hop 192.168.100.100 using egress ifc  inside(vrfid:0)

Phase: 11
Type: SUBOPTIMAL-LOOKUP
Subtype: suboptimal next-hop
Result: ALLOW
Config:
Additional Information:
Input route lookup returned ifc  inside is not same as existing ifc  outside
Doing adjacency lookup lookup on existing ifc outside

Phase: 12
Type: NEXTHOP-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP
Subtype: Lookup Nexthop on interface
Result: ALLOW
Config:
Additional Information:
Found next-hop 192.168.102.102 using egress ifc  outside(vrfid:0)

Phase: 13
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop IP address to MAC
Result: ALLOW
Config:
Additional Information:
found adjacency entry for Next-hop 192.168.102.102 on interface  outside
Adjacency :Active
mac address 0aaa.0bbb.00cc hits 5 reference 1

Result:
input-interface: dmz(vrfid:0)
input-status: up
input-line-status: up
output-interface: outside(vrfid:0)
output-status: up
output-line-status: up
Action: allow
```

以下示例描述了使用 NAT 进行次优路由的数据包跟踪器，其中，由于下一跳不可达而丢弃数据包。

```
firepower(config)# sh run route
route inside 0.0.0.0 0.0.0.0 192.168.100.100 1

firepower(config)# sh nat detail
Manual NAT Policies (Section 1)
1 (outside) to (dmz) source static src_real src_mapped  destination static dest_real
dest_mapped
translate_hits = 3, untranslate_hits = 3
Source - Origin: 9.9.9.0/24, Translated: 10.10.10.0/24
Destination - Origin: 192.168.104.0/24, Translated: 192.168.104.0/24


<Displays same phases as in the previous example till Phase 11>

Result:
input-interface: dmz(vrfid:0)
input-status: up
input-line-status: up
output-interface: outside(vrfid:0)
output-status: up
output-line-status: up
Action: drop
Drop-reason: (no-adjacency) No valid adjacency, Drop-location: frame
snp_fp_adjacency_internal:5890 flow (NA)/NA
```

Related Commands

命令	Description
capture	捕获数据包信息，包括跟踪数据包。
show capture	在未指定选项时显示捕获配置。
show packet-tracer	显示最近在 PCAP 文件上运行的数据包跟踪器的跟踪缓冲区输出。

perfmon

要在控制台显示性能信息，请使用 **perfmon** 命令。

perfmon {**verbose** | **interval**几秒 | **settings**}

Syntax Description

verbose	在控制台上显示性能监控信息。默认为不显示信息，在 perfmon 设置中显示为“quiet”。 您必须在诊断 CLI 中才能关闭 **perfmon verbose**。
interval *seconds*	指定控制台上刷新性能显示前的秒数。
settings	显示间隔，以及 perfmon 是安静模式还是详细模式。

Command Default

间隔默认值为 120 秒。

Command History

版本	修改
6.1	引入了此命令。

使用指南

perfmon 命令允许您监控设备的性能。使用 **show perfmon** 命令以立即显示这些信息。

使用 **perfmon verbose** 命令在每个时间间隔的控制台上显示信息。

仅当您在控制台端口上实际连接到 CLI 或在诊断 CLI 中（**system support diagnostic-cli**）时，才会自动显示该信息。如果您位于不同端口（包括管理接口）的 CLI 中，请使用 **show console-output** 命令查看自动生成的信息。或者，不要使用此命令，而直接使用 **show perfmon** 命令。

我们建议您仅在诊断 CLI 中使用此命令。

注释 您无法从常规 CLI 关闭 **verbose** 。相反，您必须在诊断 CLI 中从特权 EXEC 模式下将其关闭。请参阅示例部分。

示例

以下示例显示如何在控制台上每隔 120 秒显示性能监控统计信息：在输出中，“Fixup”统计信息是指相关的协议检测引擎。

```
> perfmon verbose
> perfmon settings
interval: 120 (seconds)
verbose
> show console-output
...
Message #109 :
```

```
Message #110 : PERFMON STATS:                      Current      Average
Message #111 : Xlates                                 0/s          0/s
Message #112 : Connections                            0/s          0/s
Message #113 : TCP Conns                              0/s          0/s
Message #114 : UDP Conns                              0/s          0/s
Message #115 : URL Access                             0/s          0/s
Message #116 : URL Server Req                         0/s          0/s
Message #117 : TCP Fixup                              0/s          0/s
Message #118 : TCP Intercept Established Conns        0/s          0/s
Message #119 : TCP Intercept Attempts                 0/s          0/s
Message #120 : TCP Embryonic Conns Timeout            0/s          0/s
Message #121 : FTP Fixup                              0/s          0/s
Message #122 : AAA Authen                             0/s          0/s
Message #123 : AAA Author                             0/s          0/s
Message #124 : AAA Account                            0/s          0/s
Message #125 : HTTP Fixup                             0/s          0/s
Message #126 :
...
```

以下示例显示如何关闭详细模式。您必须从诊断 CLI 执行此操作。

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

firepower> enable
Password: <Press return, do not enter a password>

firepower# perfmon quiet
firepower# perfmon settings
interval: 120 (seconds)
quiet
firepower# <Press Ctrl+a, d>

Console connection detached.
> perfmon settings
interval: 120 (seconds)
quiet
```

Related Commands

命令	Description
show perfmon	显示性能信息。

pigtail commands

只能在思科技术支持中心的指导下使用 **pigtail** 命令。

如果要查看写入的日志，请使用 **tail-logs** 命令而不是 **pigtail**。

⚠

注意 请勿让尾纤进程继续运行，因为它可能会导致磁盘使用率过高。如果此过程在部署期间运行，也可能会干扰策略部署。有关如何停止尾纤流程的信息，请联系思科技术支持中心。

ping

要测试从指定接口到 IP 地址的连接，请使用 **ping** 命令。常规基于 ICMP 的 ping、TCP ping 和“系统”ping 的可用参数有所不同。此外，系统 ping 操作来自管理接口，而其他类型的 ping 操作则通过数据接口。请务必使用正确的 ping 类型进行测试。

ping [**interface** *if_name* | **vrf** *name*] *host* [**repeat** *count*] [**timeout** *seconds*] [**data** *pattern*] [**size** *bytes*] [**validate**]
ping tcp [**interface** *if_name* | **vrf** *name*] *host port* [**repeat** *count*] [**timeout** *seconds*] [**source** *host port*]
ping system *host*

Syntax Description

data *pattern*	（可选，仅限 ICMP。）指定十六进制格式的 16 位数据模式，范围为 0 到 FFFF。默认值为 0xabcd。
host	指定要 ping 的主机的 IPv4 地址或名称。对于 ICMP ping，您还可以指定 IPv6 地址。TCP 或系统 ping 不支持 IPv6。 ping 操作是否可以使用完全限定域名（例如 www.example.com）取决于 DNS 服务器是否可以解析名称。系统 ping 使用管理接口的 DNS 服务器，但其他类型的 ping 不使用管理 DNS 服务器。必须为数据接口配置 DNS，才能使非系统主机名 ping 正常工作。 如果 **ping** 无法解析主机名，请使用 **nslookup** 确定与该名称关联的 IP 地址，然后 ping 通该 IP 地址。
interface *if_name*	（可选）对于ICMP，这是可通过其访问主机的接口的名称。如果不提供，则主机将解析为 IP 地址，并会参考路由表来确定目标接口。对于 TCP，这是来源用来发送 SYN 数据包的输入接口。 如果在启用虚拟路由和转发 (VRF) 时指定 **interface** 关键字，则 ping 将使用指定接口的虚拟路由表。
port	（仅限 TCP。）为您正在 ping 的主机指定 TCP 端口号 (1-65535)。
repeat *count*	（可选）指定重复 ping 请求的次数。默认值为 5。
size *bytes*	（可选，仅限 ICMP。）指定数据报大小（以字节为单位）。默认值为 100。
source *host port*	（可选，仅限 TCP。）指定从其发送 ping 的某个 IP 地址和端口（对于随机端口，使用端口 = 0）。
system	通过管理接口 ping 通主机。不同于通过数据接口进行 ping 操作，系统 ping 没有默认计数。ping 操作会持续执行，直到您使用 Ctrl+c 将其停止。

tcp	（可选）测试基于 TCP 的连接（默认为 ICMP）。TCP ping 发送 SYN 数据包，如果目标发送了 SYN-ACK 数据包，则认为 ping 取得了成功。您还可以同时运行最多 2 个 TCP ping 操作。
timeout *seconds*	（可选）指定超时间隔的秒数。默认值为 2 秒。
validate	（可选，仅限 ICMP。）验证回复数据。
vrf 名称	（可选。）如果启用虚拟路由和转发 (VRF)，也称为虚拟路由器，则可以通过指定虚拟路由器的名称来选择使用哪个虚拟路由表。此关键字与 **interface** 关键字互斥。 如果在启用虚拟路由和转发 (VRF) 时指定 **interface** 关键字，则 ping 将使用指定接口的虚拟路由表。

Command History

版本	修改
6.1	引入了此命令。
6.6	添加了 **vrf** 关键字。

使用指南

ping 命令使您能够确定设备是否已连接或某主机在网络上是否可用。

使用基于 ICMP 的常规 ping 时，请确保您没有禁止这些数据包的 ICMP 规则（如果不使用 ICMP 规则，则允许所有 ICMP 流量）。

使用 TCP ping 时，您必须确保访问策略允许在您指定的端口上的 TCP 流量。

需要此配置，以允许设备响应和接受通过 **ping** 命令生成的消息。 **ping** 命令输出显示是否接收了响应。如果输入 **ping** 命令后主机未响应，将出现如下所示的类似消息：

```
> ping 10.1.1.1
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
?????
Success rate is 0 percent (0/5)
```

使用 **show interface** 命令可确保设备连接到网络并正在传递流量。指定的指定接口的地址用作 ping 的源地址。

示例

以下示例显示如何确定是否可通过数据接口访问 IP 地址。由于未指定接口，因此使用路由表来确定如何到达该地址。

```
> ping 171.69.38.1
Sending 5, 100-byte ICMP Echos to 171.69.38.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

以下示例使用 TCP ping 来确定是否可通过数据接口访问主机。

```
> ping tcp 10.0.0.1 21
Type escape sequence to abort.
No source specified. Pinging from identity interface.
Sending 5 TCP SYN requests to 10.0.0.1 port 21
from 10.0.0.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

> ping tcp 10.0.0.1 21 source 192.168.1.1 2002 repeat 10
Type escape sequence to abort.
Sending 10 TCP SYN requests to 10.0.0.1 port 21
from 192.168.1.1 starting port 2002, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 1/2/2 ms
```

以下示例执行系统 ping 操作，以确定是否可通过管理接口访问 www.cisco.com。必须使用 Ctrl+c 停止 ping（在输出中用 ^C 表示）。

```
> ping system www.cisco.com
PING origin-www.cisco.COM (72.163.4.161) 56(84) bytes of data.
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=1 ttl=242 time=10.6 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=2 ttl=242 time=8.13 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=3 ttl=242 time=8.51 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=4 ttl=242 time=8.40 ms
^C
--- origin-www.cisco.COM ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 8.139/8.927/10.650/1.003 ms
>
```

以下示例使用名为 red 的虚拟路由器的路由表对地址执行 ping 操作。

```
> ping vrf red 2002::2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2002::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/20 ms
```

Related Commands

命令	Description
nslookup	对主机名或 IP 地址执行 DNS 查找。
show interface	显示有关接口配置的信息。

pmtool commands

只能在思科技术支持中心的指导下使用 **pmtool** 命令。

reboot

要重新启动设备，请使用 **reboot** 命令。

reboot

Command History

版本	修改
6.1	引入了此命令。

示例

```
> reboot
This command will reboot the system. Continue?
Please enter 'YES' or 'NO': yes

Broadcast message from root@firepower

The system is going down for reboot NOW!
...
```

redundant-interface

要设置冗余接口的哪个成员接口处于活动状态，请使用 **redundant-interface** 命令。

redundant-interface redundant *number* **active-member** *physical_interface*

Syntax Description

active-member *physical_interface*	设置活动成员。使用 show interface 命令查看可用的物理接口名称，例如 GigabitEthernet0/0。两个成员接口均必须为相同的物理类型。
redundant *number*	指定标识冗余接口 ID，例如 **redundant 1**。数字为 1-8。

Command Default

默认情况下，主用接口是在配置中列出的第一个成员接口（如果可用）。

Command History

版本	修改
6.1	引入了此命令。

使用指南

在 设备管理器中创建冗余接口。创建冗余接口时，需要指定主接口。使用此命令可更改运行时处于活动状态的接口。

要查看哪个接口处于活动状态，请输入以下命令：

show interface redundant*number* **detail** | **grep Member**

例如：

```
> show interface redundant1 detail | grep Member
      Members GigabitEthernet0/3(Active), GigabitEthernet0/2
```

示例

以下示例更改了冗余接口 1 的活动接口。

```
> show interface redundant1 detail | grep Member
      Members GigabitEthernet0/3(Active), GigabitEthernet0/2

> redundant-interface redundant 1 active-member gigabitethernet0/2
```

Related Commands

命令	Description
clear interface	清除 **show interface** 命令的计数器。
show interface	显示接口的运行时间状态和统计信息。

restore

要从 Cisco Secure Firewall Management Center管理的 Cisco Secure Firewall Threat Defense 设备恢复本地备份的配置，请使用**restore**命令。要恢复保存到远程位置的备份，请为备份文件的位置和用户名指定其他参数。

restore remote-manager-backup[*backup tar-file*|**location** [*scp-hostname username filepath backup tar-file*]]

Syntax Description

remote-manager-backup *backup tar-file*	恢复 Cisco Secure Firewall Management Center 创建的本地备份。本地备份文件保存在 Cisco Secure Firewall Threat Defense 设备上。
remote-manager-backup location *scp-hostname username filepath backup tar-file*	恢复 Cisco Secure Firewall Management Center 创建的远程备份。远程备份保存在用户配置的位置，可由 SCP 服务器访问，并由主机名、用户名和文件路径标识。

Command History

版本	修改
6.3	引入了此命令。

使用指南

restore 命令用于恢复新/替换设备上的 Cisco Secure Firewall Threat Defense 系统文件、Snort 数据库表和 LINA 运行配置 Cisco Secure Firewall Threat Defense。 **restore** 命令还可以确保在实际恢复操作继续之前删除 Cisco Secure Firewall Threat Defense 设备上的现有 LINA 运行配置。这可确保 Cisco Secure Firewall Threat Defense 设备仅传输进行备份时存在的配置。恢复操作成功后，除替换设备的序列号外，所有设备配置都将被替换。

恢复操作可确保使用分配给原始设备的通用唯一标识符 (UUID) 重新建立替换设备/新 Cisco Secure Firewall Threat Defense 设备与原始 Cisco Secure Firewall Management Center 设备之间的连接。成功恢复后， Cisco Secure Firewall Management Center 会将设备的所有策略标记为过期，以便在设备更换程序完成后， Cisco Secure Firewall Management Center 将可能影响替换的任何配置 Cisco Secure Firewall Threat Defense 更改部署到该设备。这可确保新的 Cisco Secure Firewall Threat Defense 和 Cisco Secure Firewall Management Center配置同步。

示例

以下示例显示从本地备份文件执行的恢复操作：

```
> restore remote-manager-backup 10.10.1.168_PRIMARY_20180614055906.tar
```

以下示例显示从远程备份文件执行的恢复操作：

```
>restore remote-manager-backup location 10.106.140.100 admin /Volume/home/admin
10.10.1.168_PRIMARY_20180614055906.tar
```

第 II 部分

S 命令

sa - show a

sftunnel-status

要查看设备和管理 管理中心之间的连接（隧道）状态，请使用 **sftunnel-status** 命令。

sftunnel-status

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用 **sftunnel-status** 命令查看设备和管理 管理中心之间的连接状态。如果使用的是本地管理器 设备管理器，则此命令不提供任何信息。

状态信息包括以下会话：

- SFTUNNEL 状态 - 建立连接的时间以及连接中使用的管理接口的相关信息。
- RUN STATUS - IP 地址、加密和注册状态信息。
- 对等体信息 - 有关 管理中心 及其与此设备的连接的信息。本节还包括可能在系统之间传输的各种服务的几种消息类型的统计信息块，包括身份、运行状况事件、RPC、NTP、IDS、恶意软件查找、CSM_CCM（用于配置设备）、EStreamer、UE 通道和 FSTREAM。
- RPC 状态:

示例

以下是 **sftunnel-status** 命令的输出示例。

```
> sftunnel-status

SFTUNNEL Start Time: Tue Oct 11 21:44:44 2016
        Both IPv4 and IPv6 connectivity is supported
        Broadcast count = 2
        Reserved SSL connections: 0
        Management Interfaces: 1
        br1 (control events) 10.83.57.37,2001:420:2710:2556:1:0:0:37

**********************

**RUN STATUS****10.83.57.41*************
        Cipher used = AES256-GCM-SHA384 (strength:256 bits)
        ChannelA Connected: Yes, Interface br1
        Cipher used = AES256-GCM-SHA384 (strength:256 bits)
        ChannelB Connected: Yes, Interface br1
        Registration: Completed.
        IPv4 Connection to peer '10.83.57.41' Start Time: Tue Oct 11 21:46:00 2016

PEER INFO:
        sw_version 6.2.0
        sw_build 2007
        Management Interfaces: 1
        eth0 (control events) 10.83.57.41,2001:420:2710:2556:1:0:0:41
```

```
        Peer channel Channel-A is valid  type (CONTROL), using 'br1',
connected to '10.83.57.41' via '10.83.57.37'
        Peer channel Channel-B is valid  type (EVENT), using 'br1',
connected to '10.83.57.41' via '10.83.57.37'

        TOTAL TRANSMITTED MESSAGES <3> for Identity service
        RECEIVED MESSAGES <2> for Identity service
        SEND MESSAGES <1> for Identity service
        HALT REQUEST SEND COUNTER <0> for Identity service
        STORED MESSAGES for Identity service (service 0/peer 0)
        STATE <Process messages> for Identity service
        REQUESTED FOR REMOTE <Process messages> for Identity service
        REQUESTED FROM REMOTE <Process messages> for Identity service

        TOTAL TRANSMITTED MESSAGES <2760> for Health Events service
        RECEIVED MESSAGES <1380> for Health Events service
        SEND MESSAGES <1380> for Health Events service
        HALT REQUEST SEND COUNTER <0> for Health Events service
        STORED MESSAGES for Health service (service 0/peer 0)
        STATE <Process messages> for Health Events service
        REQUESTED FOR REMOTE <Process messages> for Health Events service
        REQUESTED FROM REMOTE <Process messages> for Health Events service

        TOTAL TRANSMITTED MESSAGES <656> for RPC service
        RECEIVED MESSAGES <328> for RPC service
        SEND MESSAGES <328> for RPC service
        HALT REQUEST SEND COUNTER <0> for RPC service
        STORED MESSAGES for RPC service (service 0/peer 0)
        STATE <Process messages> for RPC service
        REQUESTED FOR REMOTE <Process messages> for RPC service
        REQUESTED FROM REMOTE <Process messages> for RPC service

        TOTAL TRANSMITTED MESSAGES <25131> for IP(NTP) service
        RECEIVED MESSAGES <13532> for IP(NTP) service
        SEND MESSAGES <11599> for IP(NTP) service
        HALT REQUEST SEND COUNTER <0> for IP(NTP) service
        STORED MESSAGES for IP(NTP) service (service 0/peer 0)
        STATE <Process messages> for IP(NTP) service
        REQUESTED FOR REMOTE <Process messages> for IP(NTP) service
        REQUESTED FROM REMOTE <Process messages> for IP(NTP) service

        TOTAL TRANSMITTED MESSAGES <2890> for IDS Events service
        RECEIVED MESSAGES <1445> for service IDS Events service
        SEND MESSAGES <1445> for IDS Events service
        HALT REQUEST SEND COUNTER <0> for IDS Events service
        STORED MESSAGES for IDS Events service (service 0/peer 0)
        STATE <Process messages> for IDS Events service
        REQUESTED FOR REMOTE <Process messages> for IDS Events service
        REQUESTED FROM REMOTE <Process messages> for IDS Events service

        TOTAL TRANSMITTED MESSAGES <4> for Malware Lookup Service service
        RECEIVED MESSAGES <1> for Malware Lookup Service) service
        SEND MESSAGES <3> for Malware Lookup Service service
        HALT REQUEST SEND COUNTER <0> for Malware Lookup Service service
        STORED MESSAGES for Malware Lookup Service service (service 0/peer 0)
        STATE <Process messages> for Malware Lookup Service service
        REQUESTED FOR REMOTE <Process messages> for Malware Lookup Service) service
        REQUESTED FROM REMOTE <Process messages> for Malware Lookup Service service

        TOTAL TRANSMITTED MESSAGES <372> for CSM_CCM service
        RECEIVED MESSAGES <186> for CSM_CCM service
        SEND MESSAGES <186> for CSM_CCM service
        HALT REQUEST SEND COUNTER <0> for CSM_CCM service
        STORED MESSAGES for CSM_CCM (service 0/peer 0)
```

```
        STATE <Process messages> for CSM_CCM service
        REQUESTED FOR REMOTE <Process messages> for CSM_CCM service
        REQUESTED FROM REMOTE <Process messages> for CSM_CCM service

        TOTAL TRANSMITTED MESSAGES <2907> for EStreamer Events service
        RECEIVED MESSAGES <1453> for service EStreamer Events service
        SEND MESSAGES <1454> for EStreamer Events service
        HALT REQUEST SEND COUNTER <0> for EStreamer Events service
        STORED MESSAGES for EStreamer Events service (service 0/peer 0)
        STATE <Process messages> for EStreamer Events service
        REQUESTED FOR REMOTE <Process messages> for EStreamer Events service
        REQUESTED FROM REMOTE <Process messages> for EStreamer Events service

        Priority UE Channel 1 service

        TOTAL TRANSMITTED MESSAGES <2930> for UE Channel service
        RECEIVED MESSAGES <11> for UE Channel service
        SEND MESSAGES <2919> for UE Channel service
        HALT REQUEST SEND COUNTER <0> for UE Channel service
        STORED MESSAGES for UE Channel service (service 0/peer 0)
        STATE <Process messages> for UE Channel service
        REQUESTED FOR REMOTE <Process messages> for UE Channel service
        REQUESTED FROM REMOTE <Process messages> for UE Channel service

        Priority UE Channel 0 service

        TOTAL TRANSMITTED MESSAGES <2942> for UE Channel service
        RECEIVED MESSAGES <11> for UE Channel service
        SEND MESSAGES <2931> for UE Channel service
        HALT REQUEST SEND COUNTER <0> for UE Channel service
        STORED MESSAGES for UE Channel service (service 0/peer 0)
        STATE <Process messages> for UE Channel service
        REQUESTED FOR REMOTE <Process messages> for UE Channel service
        REQUESTED FROM REMOTE <Process messages> for UE Channel service

        TOTAL TRANSMITTED MESSAGES <29286> for FSTREAM service
        RECEIVED MESSAGES <14648> for FSTREAM service
        SEND MESSAGES <14638> for FSTREAM service

        Heartbeat Send Time:     Wed Oct 12 21:58:31 2016
        Heartbeat Received Time: Wed Oct 12 21:59:48 2016

**********************

**RPC STATUS****10.83.57.41*************
  'ip' => '10.83.57.41',
  'uuid' => 'c03cb3c2-8fe2-11e6-bce8-8c278d49b0dd',
  'ipv6' => '2001:420:2710:2556:1:0:0:41',
  'name' => '10.83.57.41',
  'active' => '1',
  'uuid_gw' => '',
  'last_changed' => 'Tue Oct 11 19:32:20 2016'

Check routes:
```

Related Commands

命令	Description
configure manager add	添加远程管理器 管理中心。

sftunnel-status-brief

要查看设备和管理 管理中心之间的连接（隧道）的简要状态，请使用 **sftunnel-status-brief** 命令。

sftunnel-status-brief

Command History

版本	修改
6.7	引入了此命令。

使用指南

输入 **sftunnel-status-brief** 命令以查看管理连接状态。您还可以使用 **sftunnel-status** 查看更完整的信息。

示例

请参阅以下有关关闭连接的输出示例；没有显示“连接至“信息，也没有显示心跳信息：

```
> sftunnel-status-brief
PEER:10.10.17.202
Registration: Completed.
Connection to peer '10.10.17.202' Attempted at Mon Jun 15 09:21:57 2020 UTC
Last disconnect time : Mon Jun 15 09:19:09 2020 UTC
Last disconnect reason : Both control and event channel connections with peer went down
```

请参阅以下关于已建立连接的输出示例，其中显示了对等信道和心跳信息：

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '10.10.17.202'
via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '10.10.17.202' via
 '10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

Related Commands

命令	Description
sftunnel-status	显示管理隧道状态的详细信息。

show aaa-server

要显示 AAA 服务器的统计信息，请使用 **show aaa-server** 命令。

show aaa-server [**LOCAL** | *groupname* [**host** *hostname*] | **protocol** *protocol*]

Syntax Description

groupname	（可选）显示组中服务器的统计信息。
host *hostname*	（可选）显示组中特定服务器的统计信息。
LOCAL	（可选）显示 LOCAL 用户数据库的统计信息。
protocol *protocol*	（可选）显示指定协议的服务器的统计信息： **ldap** 或 **radius**。

Command Default

默认显示所有 AAA 服务器统计信息。

Command History

版本	修改
6.2.1	引入了此命令。

使用指南

下表显示了 **show aaa-server** 命令的输出的字段描述：

字段	Description
Server Group	服务器组名称。
Server Protocol	服务器组的服务器协议。
Server Address	AAA 服务器的 IP 地址。
Server port	系统和 AAA 服务器使用的通信端口。
Server status	服务器的状态。如果状态后接“(admin initiated)”，则表示服务器是使用 **aaa-server active** 或 **aaa-server fail** 命令手动重新激活或设置成失败的。其值如下： • ACTIVE - 系统将与此 AAA 服务器通信。 • FAILED - 系统无法与 AAA 服务器通信。根据配置的策略，处于此状态的服务器将保持该状态一段时间，然后重新激活。 最后一个事务的日期和时间使用以下形式之一显示： • `Last Transaction success at time timezone date` • `Last Transaction failure at time timezone date` • 如果设备尚未与服务器通信，则`Last Transaction at Unknown`。

字段	Description
Number of pending requests	仍在进行中的请求数。
Average round trip time	完成与服务器的事务所需的平均时间。
Number of authentication requests	系统发送的身份验证请求数。此值不包括在超时之后的重新传输。
Number of authorization requests	授权请求数。此值是指源于以下项的授权请求：命令授权、通过机箱流量的授权、为隧道组启用的 WebVPN 和 IPsec 授权功能。此值不包括在超时之后的重新传输。
Number of accounting requests	记账请求数。此值不包括在超时之后的重新传输。
Number of retransmissions	在内部超时后重新传输消息的次数。此值仅适用于RADIUS服务器(UDP)。
Number of accepts	成功的身份验证请求数。
Number of rejects	拒绝的请求数。此值包括错误情况以及来自AAA服务器的真实凭证拒绝。
Number of challenges	AAA 服务器在收到初始用户名和密码信息后要求提供其他信息的次数。
Number of malformed responses	此值没有意义。
Number of bad authenticators	此值仅适用于 RADIUS。 RADIUS 数据包中的“authenticator”字符串损坏（罕见）或系统上的共享密钥与RADIUS服务器上的密钥不匹配的次数。要解决此问题，请输入正确的服务器密钥。
Number of timeouts	系统检测到 AAA 服务器未响应或行为错误并已宣布其离线的次数。
Number of unrecognized responses	系统从 AAA 服务器收到它无法标识或支持的响应的次数。例如，来自服务器的 RADIUS 数据包代码是“access-accept”、“access-reject”、“access-challenge”或“accounting-response”以外的未知类型。通常情况下，这意味着来自服务器的RADIUS响应数据包已损坏，但这种情况很少出现。

示例

以下示例展示如何显示组中特定服务器的 AAA 统计信息：

```
> show aaa-server group1 host 192.68.125.60
Server Group: group1
Server Protocol: RADIUS
Server Address: 192.68.125.60
Server port: 1645
```

```
Server status: ACTIVE. Last transaction (success) at 11:10:08 UTC Fri Aug 22
Number of pending requests 20
Average round trip time 4ms
Number of authentication requests 20
Number of authorization requests 0
Number of accounting requests 0
Number of retransmissions 1
Number of accepts 16
Number of rejects 4
Number of challenges 5
Number of malformed responses 0
Number of bad authenticators 0
Number of timeouts 0
Number of unrecognized responses 0
```

Related Commands

命令	Description
clear aaa-server statistics	清除 AAA 服务器统计信息。

show access-control-config

要显示有关访问控制策略的摘要信息，请使用 **show access-control-config** 命令。

show access-control-config

Command History

版本	修改
6.1	引入了此命令。

使用指南

此命令提供访问控制策略的摘要说明，包括每个访问控制规则的特征。输出显示访问控制策略的名称和说明、其默认操作、安全情报策略以及有关访问控制规则集和每个访问控制规则的信息。也显示引用的 SSL 的名称、网络分析、入侵和文件策略名称；入侵变量集数据；日志记录设置；以及其他高级设置，包括政策级别性能、预处理和常规设置。

信息包括策略相关的连接信息，例如源端口和目标端口数据（包括 ICMP 条目的类型和代码）以及与每条访问控制规则匹配的连接数（命中次数）。

该信息还显示用于 URL 过滤的阻止和交互式阻止操作的 HTML。

如果您使用 设备管理器（本地管理器），则不受支持的功能将显示其默认设置或为空。如果您使用的是 管理中心，则可以使用管理器调整任何这些设置。您无法使用 CLI 配置此输出中显示的任何规则或选项；您必须使用管理器。

示例

以下示例显示使用本地管理器 设备管理器管理的设备的访问控制配置。

```
> show access-control-config

===============[ NGFW-Access-Policy ]===============
Description               :
=================[ Default Action ]=================
Default Action            : Block
Logging Configuration
    DC                    : Enabled
    Beginning             : Disabled
    End                   : Disabled
Rule Hits                 : 0
Variable Set              : Default-Set

===[ Security Intelligence - Network Whitelist ]====
===[ Security Intelligence - Network Blacklist ]====
Logging Configuration     : Disabled
    DC                    : Disabled

=====[ Security Intelligence - URL Whitelist ]======
=====[ Security Intelligence - URL Blacklist ]======
Logging Configuration     : Disabled
    DC                    : Disabled

=======[ Security Intelligence - DNS Policy ]=======
    Name                  : Default DNS Policy
```

```
======[ Rule Set: admin_category (Built-in) ]=======

=====[ Rule Set: standard_category (Built-in) ]=====

------------[ Rule: Inside_Inside_Rule ]------------
    Action                : Fast-path

    Source Zones          : inside_zone
    Destination Zones     : inside_zone
    Users
    URLs
    Logging Configuration
      DC                  : Enabled
      Beginning           : Enabled
      End                 : Enabled
      Files               : Disabled
    Safe Search           : No
    Rule Hits             : 0
    Variable Set          : Default-Set

-----------[ Rule: Inside_Outside_Rule ]------------
    Action                : Fast-path

    Source Zones          : inside_zone
    Destination Zones     : outside_zone
    Users
    URLs
    Logging Configuration
      DC                  : Enabled
      Beginning           : Enabled
      End                 : Enabled
      Files               : Disabled
    Safe Search           : No
    Rule Hits             : 0
    Variable Set          : Default-Set

=======[ Rule Set: root_category (Built-in) ]=======

===============[ Advanced Settings ]================
General Settings
  Maximum URL Length                  : 1024
  Interactive Block Bypass Timeout    : 600
  Do not retry URL cache miss lookup  : No
  Inspect Traffic During Apply        : Yes
Network Analysis and Intrusion Policies
  Initial Intrusion Policy            : Balanced Security and Connectivity
  Initial Variable Set                : Default-Set
  Default Network Analysis Policy     : Balanced Security and Connectivity
Files and Malware Settings
  File Type Inspect Limit             : 1460
  Cloud Lookup Timeout                : 2
  Minimum File Capture Size           : 6144
  Maximum File Capture Size           : 1048576
  Min Dynamic Analysis Size           : 15360
  Max Dynamic Analysis Size           : 2097152
  Malware Detection Limit             : 10485760
Transport/Network Layer Preprocessor Settings
  Detection Settings
    Ignore VLAN Tracking Connections  : No
  Maximum Active Responses            : No Maximum
  Minimum Response Seconds            : No Minimum
  Session Termination Log Threshold   : 1048576
Detection Enhancement Settings
```

```
  Adaptive Profile                    : Disabled
Performance Settings
  Event Queue
    Maximum Queued Events             : 5
    Disable Reassembled Content Checks: False
  Performance Statistics
    Sample time (seconds)             : 300
    Minimum number of packets         : 10000
    Summary                           : False
    Log Session/Protocol Distribution : False
  Regular Expression Limits
    Match Recursion Limit             : Default
    Match Limit                       : Default
  Rule Processing Configuration
    Logged Events                     : 5
    Maximum Queued Events             : 8
    Events Ordered By                 : Content Length
Intelligent Application Bypass Settings
    State                                        : Off
Latency-Based Performance Settings
  Packet Handling                     : Disabled

============[ HTTP Block Response HTML ]============
HTTP/1.1 403 Forbidden
Connection: close
Content-Length: 506
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html>
<head>
<meta http-equiv="content-type" content="text/html; charset=UTF-8" />
<title>Access Denied</title>
<style type="text/css">body {margin:0;font-family:verdana,sans-serif;} h1 {margin:0;pa
dding:12px 25px;background-color:#343434;color:#ddd} p {margin:12px 25px;} strong {col
or:#E0042D;}</style>
</head>
<body>
<h1>Access Denied</h1>
<p>
<strong>You are attempting to access a forbidden site.</strong><br/><br/>
Consult your system administrator for details.
</p>
</body>
</html>
```

Related Commands

命令	Description
show access-list	显示访问控制列表 (ACL) 的内容。

show access-list

要显示访问列表的规则和命中计数器，请使用 **show access-list** 命令。

show access-list [*id* [*ip_address* | **brief** | **numeric**] | **element-count**]

Syntax Description

ID	（可选）现有访问列表的名称，以将视图限制为此访问列表。
ip_address	（可选）源 IPv4 或 IPv6 地址，以将视图限制为具有此地址的规则。
brief	（可选）显示访问列表标识符、命中计数以及最后规则命中的时间戳，全部采用十六进制格式。
numeric	（可选。）如果指定ACL名称，则将端口显示为编号而不是名称。例如，80 而不是 www。
element-count	（可选。）显示系统上定义的所有访问列表中的访问控制条目总数。

Command History

版本	修改
6.1	引入了此命令。
6.6	添加了 **numeric** 和 **element-count** 关键字。
7.1	如果启用了对象组搜索，则 **element-count** 输出包括对象组的细分。

使用指南

系统将访问控制策略的某些元素构建为高级访问控制列表 (ACL) 条目。如果可能，根据第 3 层条件阻止流量的访问控制规则将成为ACL中的拒绝规则。您可能还会看到与信任访问控制规则一致的信任 ACL 规则。

但是，如果访问控制规则需要检查，即使规则操作是阻止，ACL 条目实际上也允许流量。然后，这些允许的流量将传递到检测引擎（例如 snort），最终会阻止不需要的流量。

因此， **show access-list** 显示的低级 ACL 规则与设备的访问控制策略规则之间没有一对一的关系。高级 ACL 允许系统及早对流量做出丢弃或信任决策，因此可以尽快通过或丢弃不需要检查的连接。

注释 如果您的目标是查看访问控制和预过滤器规则的命中计数信息，请使用 **show rule hits** 命令而不是此命令。

ACL 还可用于其他用途，例如路由地图和服务策略的匹配条件。标准和扩展 ACL 用于这些目的。

您可以在一个命令中输入访问列表标识符，一次显示多个访问列表。

您可以指定**brief**关键字，以十六进制格式显示访问列表命中数、标识符和时间戳信息。以十六进制格式显示配置标识符分三列显示，与系统日志 106023 和 106100 中使用的标识符相同。

如果访问列表最近已更改，则该列表将从输出中排除。系统将显示一条消息，指示何时发生这种情况。

注释 输出显示 ACL 中有多少个元素。此数量不一定与 ACL 中的访问控制条目 (ACE) 数量相同。例如，当您使用具有地址范围的网络对象时，系统可能会创建额外的元素，而这些额外的元素不包含在输出中。

集群准则

使用集群时，由于集群管理逻辑的作用，如果其中一台设备收到流量，其他设备仍可能显示ACL的命中计数。这是预期行为。由于未直接从客户端收到任何数据包的设备可能会收到通过所有者请求的集群控制链路转发的数据包，因此，该设备在将数据包发回接收设备之前，可能会检查 ACL。因此，即使设备未传递流量，ACL 命中计数也会增加。

示例

以下是 **show access-list** 命令的输出示例，显示了使用 设备管理器 （本地或“on box”管理器时）为访问控制策略生成的高级访问列表。这些备注是系统生成的，可帮助您了解访问控制条目 (ACE)。请注意，备注为您提供相关规则的名称；根据规则生成的 ACE 如下。这些备注在下面的示例中突出显示。

```
> show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list NGFW_ONBOX_ACL; 50 elements; name hash: 0xf5cc3f88
access-list NGFW_ONBOX_ACL line 1 remark rule-id 268435458: ACCESS POLICY:
NGFW_Access_Policy
access-list NGFW_ONBOX_ACL line 2 remark rule-id 268435458: L5 RULE: Inside_Inside_Rule
access-list NGFW_ONBOX_ACL line 3 advanced trust ip ifc inside1_2 any ifc inside1_3 any
rule-id 268435458 event-log both (hitcnt=0) 0x2c7f5801
access-list NGFW_ONBOX_ACL line 4 advanced trust ip ifc inside1_2 any ifc inside1_4 any
rule-id 268435458 event-log both (hitcnt=0) 0xf170c15b
access-list NGFW_ONBOX_ACL line 5 advanced trust ip ifc inside1_2 any ifc inside1_5 any
rule-id 268435458 event-log both (hitcnt=0) 0xce627c77
access-list NGFW_ONBOX_ACL line 6 advanced trust ip ifc inside1_2 any ifc inside1_6 any
rule-id 268435458 event-log both (hitcnt=0) 0xe37dcdd2
access-list NGFW_ONBOX_ACL line 7 advanced trust ip ifc inside1_2 any ifc inside1_7 any
rule-id 268435458 event-log both (hitcnt=0) 0x65347856
access-list NGFW_ONBOX_ACL line 8 advanced trust ip ifc inside1_2 any ifc inside1_8 any
rule-id 268435458 event-log both (hitcnt=0) 0x6d622775
access-list NGFW_ONBOX_ACL line 9 advanced trust ip ifc inside1_3 any ifc inside1_2 any
rule-id 268435458 event-log both (hitcnt=0) 0xc1579ed7
access-list NGFW_ONBOX_ACL line 10 advanced trust ip ifc inside1_3 any ifc inside1_4 any
rule-id 268435458 event-log both (hitcnt=0) 0x40968b8f
access-list NGFW_ONBOX_ACL line 11 advanced trust ip ifc inside1_3 any ifc inside1_5 any
rule-id 268435458 event-log both (hitcnt=0) 0xc5a178c1
access-list NGFW_ONBOX_ACL line 12 advanced trust ip ifc inside1_3 any ifc inside1_6 any
rule-id 268435458 event-log both (hitcnt=0) 0xdbc1560f
access-list NGFW_ONBOX_ACL line 13 advanced trust ip ifc inside1_3 any ifc inside1_7 any
rule-id 268435458 event-log both (hitcnt=0) 0x3571535c
access-list NGFW_ONBOX_ACL line 14 advanced trust ip ifc inside1_3 any ifc inside1_8 any
rule-id 268435458 event-log both (hitcnt=0) 0xc4a66c0a
access-list NGFW_ONBOX_ACL line 15 advanced trust ip ifc inside1_4 any ifc inside1_2 any
```

```
rule-id 268435458 event-log both (hitcnt=0) 0x1d1a8032
access-list NGFW_ONBOX_ACL line 16 advanced trust ip ifc inside1_4 any ifc inside1_3 any
rule-id 268435458 event-log both (hitcnt=0) 0x8f7bbcdf
access-list NGFW_ONBOX_ACL line 17 advanced trust ip ifc inside1_4 any ifc inside1_5 any
rule-id 268435458 event-log both (hitcnt=0) 0xe616991f
access-list NGFW_ONBOX_ACL line 18 advanced trust ip ifc inside1_4 any ifc inside1_6 any
rule-id 268435458 event-log both (hitcnt=0) 0x4db9d2aa
access-list NGFW_ONBOX_ACL line 19 advanced trust ip ifc inside1_4 any ifc inside1_7 any
rule-id 268435458 event-log both (hitcnt=0) 0xf8a88db4
access-list NGFW_ONBOX_ACL line 20 advanced trust ip ifc inside1_4 any ifc inside1_8 any
rule-id 268435458 event-log both (hitcnt=0) 0x1d3b5b80
access-list NGFW_ONBOX_ACL line 21 advanced trust ip ifc inside1_5 any ifc inside1_2 any
rule-id 268435458 event-log both (hitcnt=0) 0xf508bbd8
access-list NGFW_ONBOX_ACL line 22 advanced trust ip ifc inside1_5 any ifc inside1_3 any
rule-id 268435458 event-log both (hitcnt=0) 0x7084f3fc
access-list NGFW_ONBOX_ACL line 23 advanced trust ip ifc inside1_5 any ifc inside1_4 any
rule-id 268435458 event-log both (hitcnt=0) 0xd989f9aa
access-list NGFW_ONBOX_ACL line 24 advanced trust ip ifc inside1_5 any ifc inside1_6 any
rule-id 268435458 event-log both (hitcnt=0) 0xd5aa77f5
access-list NGFW_ONBOX_ACL line 25 advanced trust ip ifc inside1_5 any ifc inside1_7 any
rule-id 268435458 event-log both (hitcnt=0) 0x4a7648b2
access-list NGFW_ONBOX_ACL line 26 advanced trust ip ifc inside1_5 any ifc inside1_8 any
rule-id 268435458 event-log both (hitcnt=0) 0x118ef4b4
access-list NGFW_ONBOX_ACL line 27 advanced trust ip ifc inside1_6 any ifc inside1_2 any
rule-id 268435458 event-log both (hitcnt=0) 0xa6be4e58
access-list NGFW_ONBOX_ACL line 28 advanced trust ip ifc inside1_6 any ifc inside1_3 any
rule-id 268435458 event-log both (hitcnt=0) 0xda17cb9e
access-list NGFW_ONBOX_ACL line 29 advanced trust ip ifc inside1_6 any ifc inside1_4 any
rule-id 268435458 event-log both (hitcnt=0) 0xc6bfe6b7
access-list NGFW_ONBOX_ACL line 30 advanced trust ip ifc inside1_6 any ifc inside1_5 any
rule-id 268435458 event-log both (hitcnt=0) 0x5fe085c3
access-list NGFW_ONBOX_ACL line 31 advanced trust ip ifc inside1_6 any ifc inside1_7 any
rule-id 268435458 event-log both (hitcnt=0) 0x4574192b
access-list NGFW_ONBOX_ACL line 32 advanced trust ip ifc inside1_6 any ifc inside1_8 any
rule-id 268435458 event-log both (hitcnt=0) 0x36203c1e
access-list NGFW_ONBOX_ACL line 33 advanced trust ip ifc inside1_7 any ifc inside1_2 any
rule-id 268435458 event-log both (hitcnt=0) 0x699725ea
access-list NGFW_ONBOX_ACL line 34 advanced trust ip ifc inside1_7 any ifc inside1_3 any
rule-id 268435458 event-log both (hitcnt=0) 0x36a1e6a1
access-list NGFW_ONBOX_ACL line 35 advanced trust ip ifc inside1_7 any ifc inside1_4 any
rule-id 268435458 event-log both (hitcnt=0) 0xe415bb76
access-list NGFW_ONBOX_ACL line 36 advanced trust ip ifc inside1_7 any ifc inside1_5 any
rule-id 268435458 event-log both (hitcnt=0) 0x18ebff70
access-list NGFW_ONBOX_ACL line 37 advanced trust ip ifc inside1_7 any ifc inside1_6 any
rule-id 268435458 event-log both (hitcnt=0) 0xf9bfd690
access-list NGFW_ONBOX_ACL line 38 advanced trust ip ifc inside1_7 any ifc inside1_8 any
rule-id 268435458 event-log both (hitcnt=0) 0xf08a88b4
access-list NGFW_ONBOX_ACL line 39 advanced trust ip ifc inside1_8 any ifc inside1_2 any
rule-id 268435458 event-log both (hitcnt=0) 0xd2014e58
access-list NGFW_ONBOX_ACL line 40 advanced trust ip ifc inside1_8 any ifc inside1_3 any
rule-id 268435458 event-log both (hitcnt=0) 0x952c7254
access-list NGFW_ONBOX_ACL line 41 advanced trust ip ifc inside1_8 any ifc inside1_4 any
rule-id 268435458 event-log both (hitcnt=0) 0xfc38a46f
access-list NGFW_ONBOX_ACL line 42 advanced trust ip ifc inside1_8 any ifc inside1_5 any
rule-id 268435458 event-log both (hitcnt=0) 0x3f878e23
access-list NGFW_ONBOX_ACL line 43 advanced trust ip ifc inside1_8 any ifc inside1_6 any
rule-id 268435458 event-log both (hitcnt=0) 0x48e852ce
access-list NGFW_ONBOX_ACL line 44 advanced trust ip ifc inside1_8 any ifc inside1_7 any
rule-id 268435458 event-log both (hitcnt=0) 0x83c65e52
access-list NGFW_ONBOX_ACL line 45 remark rule-id 268435457: ACCESS POLICY:
NGFW_Access_Policy
access-list NGFW_ONBOX_ACL line 46 remark rule-id 268435457: L5 RULE: Inside_Outside_Rule
access-list NGFW_ONBOX_ACL line 47 advanced trust ip ifc inside1_2 any ifc outside any
rule-id 268435457 event-log both (hitcnt=0) 0xea5bdd6e
```

```
access-list NGFW_ONBOX_ACL line 48 advanced trust ip ifc inside1_3 any ifc outside any
rule-id 268435457 event-log both (hitcnt=0) 0xd7461ffc
access-list NGFW_ONBOX_ACL line 49 advanced trust ip ifc inside1_4 any ifc outside any
rule-id 268435457 event-log both (hitcnt=0) 0x6e13508e
access-list NGFW_ONBOX_ACL line 50 advanced trust ip ifc inside1_5 any ifc outside any
rule-id 268435457 event-log both (hitcnt=0) 0xfe1fcdd6
access-list NGFW_ONBOX_ACL line 51 advanced trust ip ifc inside1_6 any ifc outside any
rule-id 268435457 event-log both (hitcnt=0) 0xa4dba9a8
access-list NGFW_ONBOX_ACL line 52 advanced trust ip ifc inside1_7 any ifc outside any
rule-id 268435457 event-log both (hitcnt=0) 0x2cfd43cd
access-list NGFW_ONBOX_ACL line 53 advanced trust ip ifc inside1_8 any ifc outside any
rule-id 268435457 event-log both (hitcnt=0) 0xc3c3fafb
access-list NGFW_ONBOX_ACL line 54 remark rule-id 1: ACCESS POLICY: NGFW_Access_Policy
access-list NGFW_ONBOX_ACL line 55 remark rule-id 1: L5 RULE: DefaultActionRule
access-list NGFW_ONBOX_ACL line 56 advanced deny ip any any rule-id 1 (hitcnt=0)
0x84953cae
>
```

以下示例以十六进制格式显示指定访问策略的简短信息（命中计数不是零的 ACE）。前两列以十六进制格式显示标识符，第三列显示命中计数，第四列显示时间戳值（也是十六进制格式）。命中计数值代表流量命中规则的次数。时间戳值报告最后一次命中的时间。如果命中计数为零，则不会显示任何信息。

以下是当 Telnet 流量通过时 **show access-list brief** 命令的输出示例：。

```
> show access-list test brief
access-list test; 3 elements; name hash: 0xcb4257a3
7b1c1660 44ae5901 00000001 4a68ab51
```

以下是当 SSH 流量通过时 **show access-list brief** 命令的输出示例：。

```
> show access-list test brief
access-list test; 3 elements; name hash: 0xcb4257a3
7b1c1660 44ae5901 00000001 4a68ab51
3666f922 44ae5901 00000001 4a68ab66
```

以下示例显示元素计数，即系统上定义的所有访问列表的访问控制条目总数。对于分配为访问组的访问列表，要全局控制访问或在接口上控制访问，可以通过启用对象组搜索来减少元素计数，这在运行配置中由 **object-group-search access-control** 命令表示。启用对象组搜索时，将在访问控制条目中使用网络对象；否则，对象将扩展为对象中包含的单个 IP 地址，并为每个源/目标地址对写入单独的条目。因此，使用具有 5 个 IP 地址的源网络对象和具有 6 个地址的目标对象的单个规则将扩展为 5 * 6 个条目，而不是一个元素。元素计数越高，访问列表越大，这可能会影响性能。

```
> show access-list element-count
Total number of access-list elements: 33934
```

从 7.1 开始，如果启用对象组搜索，则会显示有关规则 (OBJGRP) 中对象组数量的其他信息，包括源 (SRC OBJ) 和目标 (DST OBJ) 对象之间的拆分，以及添加的和已删除的组。

```
> show access-list element-count
Total number of access-list elements: 892
```

```
OBJGRP      SRC OG      DST OG      ADD OG      DEL OG
842         842         842         842         0
```

Related Commands

命令	Description
clear access-list	清除访问列表计数器。
show running-config access-list	显示当前正在运行的访问列表配置。

show alarm settings

要显示 ISA 3000 中每种警报的配置，请使用 **show alarm settings** 命令。

show alarm settings

Command History

版本	修改
6.3	引入了此命令。

示例

以下是 **show alarm settings** 命令的输出示例：

```
> show alarm settings

Power Supply
         Alarm                   Disabled
         Relay                   Disabled
         Notifies                Disabled
         Syslog                  Disabled
Temperature-Primary
         Alarm                   Enabled
         Thresholds              MAX: 92C                MIN: -40C
         Relay                   Enabled
         Notifies                Enabled
         Syslog                  Enabled
Temperature-Secondary
         Alarm                   Disabled
         Threshold
         Relay                   Disabled
         Notifies                Disabled
         Syslog                  Disabled
Input-Alarm 1
         Alarm                   Enabled
         Relay                   Disabled
         Notifies                Disabled
         Syslog                  Enabled
Input-Alarm 2
         Alarm                   Enabled
         Relay                   Disabled
         Notifies                Disabled
         Syslog                  Enabled
```

Related Commands

命令	Description
clear facility-alarm output	断开输出继电器并清除 LED 的警报状态。
show environment alarm-contact	显示输入警报触点的状态。
show facility-alarm	显示已触发警报的状态信息。

show allocate-core

要显示有关如何分配 CPU 核心的信息，请使用 **show allocate-core** 命令。

show allocate-core { **lina-cpu-percentage** | **lina-mem-percentage** | **profile state** }

Syntax Description

lina-cpu-percentage	显示分配给 Lina 流程的 CPU 核心百分比。其余核心分配给 Snort 流程。
lina-mem-percentage	显示分配给 Lina 流程的系统内存百分比。剩余的内存分配给 Snort 流程。
profile	显示设备上当前运行的核心分配配置文件。
state	显示核心分配流程是已启用还是已禁用。

Command History

版本	修改
7.3	添加了此命令。

使用指南

您可以从管理软件分配CPU核心分配配置文件。使用此命令可查看和验证设备上运行的配置文件。可能的配置文件包括：

- default - Lina 和 Snort 流程的默认核心分配方案。确切的分配因硬件平台而异。使用其他选项确定百分比。
- ips-heavy - 为 IPS 为主的使用案例向 Snort 分配更多 CPU。分配比例为 Lina 30%，Snort 70%。
- vpn-heavy-prefilter-fastpath - 将预过滤器策略配置为快速路径 VPN 流量时，会为大量使用 VPN 的使用案例向 Lina 分配更多 CPU。分配比例为 Lina 90%，Snort 10%。
- vpn-heavy-with-inspection - 未将预过滤器策略配置为快速路径 VPN 流量，而是在访问控制策略中检查流量时，为 VPN 大量使用案例向 Lina 分配更多 CPU。分配比例为 Lina 60%，Snort 40%。

示例

以下示例显示 Lina CPU 和内存百分比、配置文件和核心分配状态。

```
> show allocate-core lina-cpu-percentage

Lina CPU percentage is set to : 48
> show allocate-core lina-mem-percentage

Lina memory percentage is set to : 50
> show allocate-core profile

Core allocation profile is set to : default
> show allocate-core state
Core allocation is disabled
```

show app-agent heartbeat

要显示应用代理的状态，请使用 **show app-agent heartbeat** 命令。

show app-agent heartbeat

Command History

版本	修改
6.1	引入了此命令。

使用指南

应用代理心跳通信信道用于监控 FXOS 机箱管理引擎和 threat defense 应用代理之间的链路的运行状况。如果在 Firepower 4100 或 9300 系列设备上配置硬件绕行，则使用此选项。它不适用于运行 threat defense 软件的其他设备型号。

使用 **show app-agent heartbeat** 命令查看 app-agent 心跳通信信道上的状态。

示例

以下示例显示了 app-agent 心跳状态。

```
> show app-agent heartbeat
appagent heartbeat timer 1 retry-count 3
```

Related Commands

命令	Description
app-agent	为硬件旁路配置应用代理。

show arp

要查看 ARP 表，请使用 **show arp** 命令。

show arp

Command History

版本	修改
6.1	引入了此命令。

使用指南

显示输出会显示动态、静态和代理 ARP 条目。动态 ARP 条目包括 ARP 条目时限（秒）。静态 ARP 条目以短划线 (-) 取代时限，代理 ARP 条目则显示“别名”。

ARP 表可以包括用于系统通信的内部接口条目，例如 nlp_int_tap。

示例

以下是 **show arp** 命令的输出示例。第一个条目是时限为 2 秒的动态条目。第二个条目是静态条目，第三个条目来自代理 ARP。

```
> show arp
        outside 10.86.194.61 0011.2094.1d2b 2
        outside 10.86.194.1 001a.300c.8000 -
        outside 10.86.195.2 00d0.02a8.440a alias
```

Related Commands

命令	Description
clear arp statistics	清除 ARP 统计信息。
show arp statistics	显示 ARP 统计信息。
show running-config all arp	显示 ARP 超时的当前配置。

show arp-inspection

要查看每个接口的 ARP 检测设置，请使用 **show arp-inspection** 命令。

show arp-inspection

Command History

版本	修改
6.1	添加了此命令。
6.2	添加了对路由模式的支持。

示例

以下是 **show arp-inspection** 命令的输出示例：

```
> show arp-inspection
interface                arp-inspection         miss
-----------------------------------------------------
inside1                  enabled                flood
outside                  disabled                -
```

Miss 列显示在 ARP 检查启用后要对非匹配数据包采取的默认操作（“泛洪”或“无泛洪”）。

Related Commands

命令	Description
clear arp statistics	清除 ARP 统计信息。
show arp statistics	显示 ARP 统计信息。
show running-config all arp	显示 ARP 超时的当前配置。

show arp statistics

要查看 ARP 统计信息，请使用 **show arp statistics** 命令。

show arp statistics

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show arp statistics** 命令的输出示例：

```
> show arp statistics
        Number of ARP entries:
        ASA : 6
        Dropped blocks in ARP: 6
        Maximum Queued blocks: 3
        Queued blocks: 1
        Interface collision ARPs Received: 5
        ARP-defense Gratuitous ARPS sent: 4
        Total ARP retries: 15
        Unresolved hosts: 1
        Maximum Unresolved hosts: 2
```

下表对每个字段进行了说明。

表 *2: show arp statistics* 字段（续）

字段	Description
Number of ARP entries	ARP 表条目的总数。
Dropped blocks in ARP	当 IP 地址解析为其相应的硬件地址时丢弃的块数。
Maximum queued blocks	在等待 IP 地址被解析时曾排入 ARP 模块队列的最大块数。
Queued blocks	当前排入 ARP 模块队列的块数。
Interface collision ARPs received	所有接口上收到的 IP 地址与接口 IP 地址相同的 ARP 数据包数量。
ARP-defense gratuitous ARPs sent	由设备作为 ARP 防御机制一部分发送的自然 ARP 数。
Total ARP retries	当地址在对第一个 ARP 请求的响应中未解析时由 ARP 模块发送的 ARP 请求总数。
Unresolved hosts	其 ARP 请求仍由 ARP 模块发出的未解析主机数。

字段	Description
Maximum unresolved hosts	自上次清除或设备启动后曾在 ARP 模块中的未解析主机最大数。

Related Commands

命令	Description
clear arp statistics	清除 ARP 统计信息。
show arp	显示 ARP 表。
show running-config all arp	显示 ARP 超时的当前配置。

show as-path-access-list

要显示所有当前自治系统 (AS) 路径访问列表的内容，请使用 **show as-path-access-list** 命令。

show as-path-access-list ［编号］

Syntax Description

number	（可选）指定 AS 路径访问列表序号。有效值介于 1 与 500 之间。

Command Default

如果没有指定 序号 参数，命令输出将显示所有 AS 路径访问列表。

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show as-path-access-list** 命令的输出示例：

```
> show as-path-access-list
 AS path access list 1

 AS path access list 2
```

show asp cluster counter

要调试群集技术环境中的全局或情景特定信息，请使用 **show asp cluster counter** 命令。

show asp cluster counter

Command History

版本	修改
6.1	引入了此命令。

使用指南

show asp cluster counter 命令显示全局和情景特定的 DP 计数器，可帮助您对问题进行故障排除。此信息仅用于调试目的，信息输出可能会随时更改。请咨询思科 TAC 以帮助您使用此命令调试您的系统。

示例

以下是 **show asp cluster counter** 命令的输出示例：

```
> show asp cluster counter
Global dp-counters:
Context specific dp-counters:
MCAST_FP_TO_SP                  361136
MCAST_SP_TOTAL                  361136
MCAST_SP_PKTS                   143327
MCAST_SP_PKTS_TO_CP             143327
MCAST_FP_CHK_FAIL_NO_HANDLE     217809
MCAST_FP_CHK_FAIL_NO_ACCEPT_IFC 81192
MCAST_FP_CHK_FAIL_NO_FP_FWD     62135
```

Related Commands

命令	Description
show asp drop	显示已丢弃数据包的加速安全路径计数器。

show asp dispatch

要显示设备负载均衡 ASP 调度程序的统计信息（这对诊断性能问题非常有用），请使用 **show asp dispatch** 命令。它仅适用于混合轮询/中断模式的 threat defense virtual 设备。

show asp dispatch

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show asp dispatch** 命令的输出示例。

```
> show asp dispatch
==== Lina DP thread dispatch stats - CORE 0 ====
Dispatch loop count        :         92260212
Dispatch C2C poll count    :                2
CP scheduler busy          :         14936242
CP scheduler idle          :         77323971
RX ring busy               :          1513632
Async lock global q busy   :           809481
Global timer q busy        :          1958684
SNP flow bulk sync busy    :              174
Purg process busy          :             2838
Block attempts             :         44594355
Maximum timeout specified  :         10000000
Minimum timeout specified  :          1572864
Average timeout specified  :          9999994
Waken up with OK status    :          2476791
Waken up with timeout      :         42117564
Sleep interrupted          :            85753
Number of interrupts       :          2492566
Number of RX interrupts    :          1454442
Number of TX interrupts    :          2492566
Enable interrupt ok        :        174566236
Disable interrupt ok       :        174231423
Maximum elapsed time       :         54082257
Minimum elapsed time       :             6165
Average elapsed time       :          9658532
Message pipe stats         :

Last clearing of asp dispatch: Never

==== Lina DP thread home-ring/interface list - CORE 0 ====
Interface Internal-Data0/0: port-id 0 irq 10 fd 37
Interface GigabitEthernet0/0: port-id 256 irq 5 fd 38
Interface GigabitEthernet0/1: port-id 512 irq 9 fd 39
Interface GigabitEthernet0/2: port-id 768 irq 11 fd 40
>
```

show asp drop

要调试加速安全路径丢弃的数据包或连接，请使用 **show asp drop** 命令。

show asp drop [**flow** [*flow_drop_reason*] | **frame** [*frame_drop_reason*]]

Syntax Description

flow [*flow_drop_reason*]	（可选）显示丢弃的流量（连接）。您可以选择指定特定原因。使用 ?查看可能的流丢弃原因列表。
frame [*frame_drop_reason*]	（可选）显示丢弃的数据包。您可以选择指定特定原因。使用 ?查看可能的丢帧原因列表。

Command History

版本	修改
6.1	引入了此命令。

使用指南

show asp drop 命令显示加速安全路径丢弃的数据包或连接，可帮助您对问题进行故障排除。此信息仅用于调试目的，信息输出可能会随时更改。请咨询思科 TAC 以帮助您使用此命令调试您的系统。

有关可能的丢弃原因的信息，请参阅“显示 ASP 丢弃命令用法”文档，网址为 http://www.cisco.com/c/en/us/td/docs/security/asa/asa-command-reference/show_asp_drop/show_asp_drop.html。

示例

以下是 **show asp drop** 命令的输出示例，带有指示计数器上次清除时间的时间戳：

```
> show asp drop

Frame drop:
  Flow is denied by configured rule (acl-drop)                          3
  Dst MAC L2 Lookup Failed (dst-l2_lookup-fail)                      4110
  L2 Src/Dst same LAN port (l2_same-lan-port)                         760
  Expired flow (flow-expired)                                           1

Last clearing: Never

Flow drop:
  Flow is denied by access rule (acl-drop)                             24
  NAT failed (nat-failed)                                           28739
  NAT reverse path failed (nat-rpf-failed)                          22266
  Inspection failure (inspect-fail)                                 19433

Last clearing: 17:02:12 UTC Jan 17 2012 by enable_15
```

show asp event

要调试数据路径或控制路径事件队列，请使用 **show asp event** 命令。

show asp event {dp-cp | cp-dp}

Syntax Description

dp-cp	显示从 ASP 数据路径发送到控制平面的事件。
cp-dp	显示从控制平面发送到 ASP 数据路径的事件。

Command History

版本	修改
6.1	引入了此命令。

使用指南

show asp event 命令显示数据路径和控制路径的内容，可帮助您对问题进行故障排除。这些表格仅用于调试目的，信息输出可能会随时更改。请咨询思科 TAC 以帮助您使用此命令调试您的系统。

示例

以下是 **show asp event dp-cp** 命令的输出示例：

```
> show asp event dp-cp
DP-CP EVENT QUEUE                    QUEUE-LEN  HIGH-WATER
Punt Event Queue                             0           0
Routing Event Queue                          0           0
Identity-Traffic Event Queue                 0           1
PTP-Traffic Event Queue                      0           0
General Event Queue                          0           0
Syslog Event Queue                           0           0
Non-Blocking Event Queue                     0           8
Midpath High Event Queue                     0           0
Midpath Norm Event Queue                     0           0
Crypto Event Queue                           0         146
HA Event Queue                               0           0
Threat-Detection Event Queue                 0           0
SCP Event Queue                              0           0
ARP Event Queue                              0           1
IDFW Event Queue                             0           0
CXSC Event Queue                             0           0
BFD Event Queue                              0           0

EVENT-TYPE          ALLOC ALLOC-FAIL ENQUEUED ENQ-FAIL  RETIRED 15SEC-RATE
crypto-msg            810          0      810        0      810          0
arp-in              17288          0    17288        0    17288          0
identity-traffic        2          0        2        0        2          0
scheduler             239          0      239        0      239          0
```

show asp inspect-dp ack-passthrough

要显示与绕过 Snort 检查的空 ACK 数据包相关的统计信息，请使用 **show asp inspect-dp ack-passthrough** 命令。

show asp inspect-dp ack-passthrough

Command History

版本	修改
7.0	引入了此命令。

使用指南

使用 **clear asp inspect-dp ack-passthrough** 命令重置这些统计信息。

示例

以下是输出示例。信息包括是否启用 ACK 传递，以及以下统计信息：

- 绕过的 ACK 数据包数 - 未转发到 Snort 进行检查的空 ACK 数据包的数量。
- 已发送的元 ACK - 发送到 Snort 的后续数据包上附带的空 ACK 的数量。此数字可能小于绕过的数据包数量，因为如果同一方向的后续数据包具有更高序列号的 ACK，则不需要且不包括先前保存的空 ACK 信息。

```
> show asp inspect-dp ack-passthrough

Current running state: Enabled

Packet Statistics:
 ACK packets bypassed                    506
 Meta ACK sent                           506
>
```

show asp inspect-dp egress-optimization

显示有关出口优化的统计信息，这是一项提高性能的功能。根据思科 TAC 的建议使用此命令。

show asp inspect-dp egress optimization

Command History

版本	修改
6.4	引入了此命令。

使用指南

show asp inspect-dp egress-optimization 命令显示有关符合出口优化条件的流的信息，出口优化是一种增强性能的功能。输出结果将显示以下信息：

- 当前运行状态：出口优化是启用还是禁用。
- 流（ 流 包含一个或多个 数据包）：
  - 当前：当前符合出口优化处理条件的流数量。
  - 最大值：自上次重新启动检测引擎或清除出口优化统计信息以来，符合出口优化条件的流量总数。
- 数据包：
  - 已处理：已处理的数据包总数。
  - 例外：最初被确定为符合出口优化条件，但后来被确定为不符合出口优化条件的数据包数量。

示例

以下是 **show asp inspect-dp egress-optimization** 命令的输出示例。

```
> show asp inspect-dp egress-optimization
Current running state: Enabled
Flow:
  current: 1, maximum: 3
  snort-unreachable: 0, snort-unsupported-header: 1, snort-unsupported-verdict: 2
Packet:
  processed: 5
  excepted: 0
```

Related Commands

命令	Description
clear asp inspect-dp egress-optimization	清除出口优化统计信息。

命令	Description
show conn state egress_optimization	显示符合出口优化条件的流的相关信息。根据思科 TAC 的建议使用此命令。

show asp inspect-dp snort

要查看 PDTS（数据平面传输/接收队列到 Snort）环的快照，请使用 **show asp inspect-dp snapshot** 命令。

show asp inspect-dp snapshot {**config** | **instance** *instance_id* **queue** *queue_id*}

Syntax Description

config	显示 PDTS 快照的全局配置。
instance *instance_id*	显示指定 PDTS 使用者实例 ID 的快照。值范围为 0-2147483647。
queue *queue_id*	显示 PDTS 环的指定数据路径传输队列 ID 的快照。值范围为 0-2147483647。

Command History

版本	修改
6.1	引入了此命令。

使用指南

show asp inspect-dp snapshot 命令显示 PDTS 环快照功能的全局配置。输出结果将显示以下信息：

- 最大快照数：允许的最大自动快照数。
- 当前正在使用：到目前为止已存储的快照数量。
- 间隔：时间间隔值指定允许在同一 PDTS 环上创建两个快照的时长
- 自动快照：显示是否启用或禁用自动 PDTS 快照功能

示例

以下是 **show asp inspect-dp snapshot config** 命令的输出示例。

```
> show asp inspect-dp snapshot config
Max snapshots  Current in use  Interval (min)  Auto Snapshot
-------------  --------------  --------------  -------------
2              0               5               OFF
```

以下是 **show asp inspect-dp snapshot instance** 命令的输出示例。

```
> show asp inspect-dp snapshot instance 2 queue 1
0 packet captured
0 packet shown
```

show asp inspect-dp snort

要显示所有 snort 实例的状态，请使用 **show asp inspect-dp snort** 命令。

show asp inspect-dp snort [instance *instance_id***]**

Syntax Description

instance *instance_id*	显示特定 snort 实例的状态。的值范围为 0-2147483647。

Command History

版本	修改
6.1	引入了此命令。

使用指南

此命令显示所有 snort 实例的状态。输出结果将显示以下信息：

- Id: Snort 实例 ID。
- PID：Snort 实例流程 ID。
- CPU 使用率：Snort 实例 ID 的 CPU 使用率。打印总数和用户/系统。**注意：** Firepower 2100 系列不显示此字段。
- 连接数：Snort 实例当前持有的连接数。
- 分段/数据包：Snort 实例当前处理的分段或数据包的数量。
- 状态：Snort 实例的状态。

示例

以下是 **show asp inspect-dp snort** 命令的输出示例。

```
> show asp inspect-dp snort

SNORT Inspect Instance Status Info

Id Pid       Cpu-Usage    Conns      Segs/Pkts  Status
          tot (usr | sys)
-- ----- ---------------- ---------- ---------- ----------
0  9188    0% (  0%|  0%)   0          0        READY
1  9187    0% (  0%|  0%)   0          0        READY
2  9186    0% (  0%|  0%)   0          0        READY
```

以下是 Firepower 2100 上 **show asp inspect-dp snort** 命令的输出示例。

```
> show asp inspect-dp snort

SNORT Inspect Instance Status Info

Id Pid   Conns      Segs/Pkts  Status
-- ----- ---------- ---------- ----------
```

```
0  30080  40          0        READY
1  30081  14          0        READY
2  30079  20          0        READY
```

show asp inspect-dp snort counters

要显示 snort 实例的 PDTS 相关原始计数器，请使用 **show asp inspect-dp snort counters** 命令。

show asp inspect-dp snort counters [instance *instance_id***] [queues] [rate] [debug] [zeros]**

Syntax Description

instance *instance_id*	显示特定 snort 实例的计数器。值范围为 0-2147483647。
queues	详细显示队列信息。单独显示实例的每个生产者队列。系统不会汇聚实例的队列信息。
rate	它需要 5 秒的计数器快照，平均为 1 秒，并显示计数器更改的速率。
debug	它会显示某些未以其他方式显示的调试计数器。
zeros	系统将显示所有计数器，包括零计数器。

Command Default

如果未指定实例，则显示所有实例。

Command History

版本	修改
6.1	引入了此命令。

使用指南

此命令显示 snort 实例的 PDTS 相关原始计数器。输出结果将显示以下信息：

- Id: Snort 实例 ID。“全部”表示汇聚的所有 snort 实例。
- QId：Lina 传输队列 ID。它对应于 Lina 线程的数量。“全部”表示汇聚所有队列。
- 类型：计数器的类型。数据计数器、错误计数器、调试计数器等。
- 名称：计数器的名称。
- 值：人类可读的计数器值。
- 原始值：计数器的原始值。

计数器名称：

- 发送字节数：Lina 发送到 snort 实例的字节数。
- 发送分段：Lina 发送到 snort 实例的帧/分段数。
- 接收字节数：Lina 从 snort 实例接收的字节数。
- 接收分段：Lina 从 snort 实例接收的帧/分段数。
- NewConns：发送到 snort 实例的连接数。
- RxQ-唤醒

- TxQ-唤醒
- TxQ-LB-Dynamic：启动 PDTS 动态负载均衡的次数。
- TxQ-Data-Hi-Thresh：达到 Lina 传输队列的高阈值限制的次数。
- RxQ-Full：Lina 的接收队列已满的次数。
- TxQ-Full：Lina 的传输队列已满的次数。
- TxQ-Data-Limit：达到 Lina 传输队列数据限制的次数。
- TxQ-LB-Failed：PDTS 动态负载均衡失败的次数。
- TxQ-Unavail：Lina 的传输队列不可用的次数。
- TxQ-Not-Ready：Lina 的传输队列未就绪的次数。
- TxQ-Suspended：Lina 的传输队列暂停的次数。
- RxQ-Unavail：Lina 的接收队列不可用的次数。
- RxQ-Not-Ready：Lina 的接收队列未就绪的次数。
- RxQ-Suspended：Lina 的接收队列暂停的次数。

示例

以下是 **show asp inspect-dp snort counters** 命令的输出示例。

```
> show asp inspect-dp snort counters summary instance 5 debug zeros
SNORT Inspect Instance Counters
Id   QId    Type    Name                            Value      Raw-Value
--   ----   ----    ----                            ---------  ----------
5    All    data    Tx Bytes                         3.3 GB   (3549197468)
5    All    data    Tx Segs                          4.7 M    (4671722)
5    All    data    Rx Bytes                         3.3 GB   (3495936190)
5    All    data    Rx Segs                          4.7 M    (4677344)
5    All    data    NewConns                         11.1 K   (11103)
5    All    debug   RxQ-Wakeup                       0        (0)
5    All    debug   TxQ-Wakeup                       4.7 M    (4655982)
5    All    warn    TxQ-LB-Dynamic                   0        (0)
5    All    warn    TxQ-Data-Hi-Thresh               0        (0)
5    All    drop    RxQ-Full                         0        (0)
5    All    drop    TxQ-Full                         0        (0)
5    All    drop    TxQ-Data-Limit                   0        (0)
5    All    drop    TxQ-LB-Failed                    0        (0)
5    All    err     TxQ-Unavail                      0        (0)
5    All    err     TxQ-Not-Ready                    0        (0)
5    All    err     TxQ-Suspended                    0        (0)
5    All    err     RxQ-Unavail                      0        (0)
5    All    err     RxQ-Not-Ready                    0        (0)
5    All    err     RxQ-Suspended                    0        (0)
```

show asp inspect-dp snort counters summary

要显示 snort 实例的 PDTS 相关计数器，请使用 **show asp inspect-dp snort counters summary** 命令。计数器汇总到每个实例。

show asp inspect-dp snort counters summary [instance *instance_id***] [queues] [rate]**

Syntax Description

instance *instance_id*	显示特定 snort 实例的计数器。值范围为 0-2147483647。
queues	详细显示队列信息。单独显示实例的每个生产者队列。系统不会汇聚实例的队列信息。
rate	显示计数器中的一秒平均增量。目前，一秒平均值基于命令的上次调用和当前调用之间的增量增量。这将更改，以便增量增加基于 5 秒滚动平均值，每秒采样一次。

Command Default

如果未指定实例，则显示所有实例。

Command History

版本	修改
6.1	引入了此命令。

使用指南

此命令显示 snort 实例的 PDTS 相关计数器。输出结果将显示以下信息：

- Id: Snort 实例 ID。“全部”表示汇聚的所有 snort 实例。
- QId：Lina 传输队列 ID。它对应于 Lina 线程的数量。“全部”表示汇聚所有队列。
- TxBytes：Lina 发送到 snort 实例的总字节数。
- TxFrames：Lina 发送到 snort 实例的帧/分段总数。
- RxBytes：Lina 从 snort 实例接收的总字节数。
- RxFrames：Lina 从 snort 实例接收的帧/网段总数。
- 连接：Snort 实例处理的连接总数。

示例

以下是 **show asp inspect-dp snort counters summary** 命令的输出示例。

```
> show asp inspect-dp snort counters summary instance 2
SNORT Inspect Instance Counter Summary
Id   QId  TxBytes    TxFrames   RxBytes    RxFrames   Conns
--   ---- ---------- ---------- ---------- ---------- -----
2    All    0          0          0          0          0
```

show asp inspect-dp snort queues

要显示将所有队列汇聚到同一实例的所有 snort 实例（进程）的队列信息，请使用 **show asp inspect-dp snort queues** 命令。

show asp inspect-dp snort queues [instance *instance_id***] [detail] [debug]**

Syntax Description

instance *instance_id*	显示特定 snort 实例的队列。值范围为 0-2147483647。
detail	详细显示队列信息。单独显示实例的每个生产者队列。系统不会汇聚实例的队列信息。
debug	系统还会显示额外的调试信息。

Command Default

如果未指定实例，则显示所有实例。

Command History

版本	修改
6.1	引入了此命令。

使用指南

此命令显示将所有队列汇聚到同一实例的所有 snort 实例（进程）的队列信息，输出显示以下信息：

- Id: Snort 实例 ID。“全部”表示汇聚的所有 snort 实例。
- QId：Lina 传输队列 ID。它对应于 Lina 线程的数量。“全部”表示汇聚所有队列。
- Rx 队列：Lina 的接收队列。“Used”表示数据量，“util”表示队列利用率，“state”表示共享内存状态。
- TxQ：Lina 的传输队列。“Used”表示数据量，“util”表示队列利用率，“state”表示共享内存状态。

Counters:

- RxQ-Size：Lina 的接收队列大小。
- TxQ-Size：Lina 的传输队列大小。
- TxQ-Data-Limit：传输队列的数据限制。一旦超过此阈值，数据包将被丢弃。百分比显示传输队列的阈值。
- TxQ-Data-Hi-Thresh：传输队列的高阈值。一旦超过此阈值，PDTS 动态负载均衡将开始尝试均衡流向其他 snort 实例的流量。

示例

以下是 **show asp inspect-dp snort queues** 命令的输出示例。

```
> show asp inspect-dp snort counters summary instance 2
SNORT Inspect Instance Queue Configuration

RxQ-Size:              1   MB
TxQ-Size:            128   KB
TxQ-Data-Limit:      102.4 KB   (80%)
TxQ-Data-Hi-Thresh:   35.8 KB   (28%)

Id QId  RxQ        RxQ    TxQ        TxQ
        (used)     (util) (used)     (util)
-- ---- ---------- ------ ---------- ------
0  All    0        0%       0        0%
1  All    0        0%       0        0%
2  All    0        0%       0        0%
```

show asp inspect-dp snort queue-exhaustion

要显示 snort 队列耗尽时的自动快照，请使用 **show asp inspect-dp snort queue-exhaustion** 命令。

show asp inspect-dp snort queue-exhaustion ［**snapshot** *snapshot_id*］［**export** *location*］

Syntax Description

snapshot *snapshot_id*	此选项指定用于打印队列耗尽信息的特定快照。值介于 1 和 24 之间。
export *location*	快照的内容将导出到指定位置的 pcap 文件中，以便进行机下分析。

Command History

版本	修改
6.1	引入了此命令。

使用指南

show asp inspect-dp snort queue-exhaustion 命令显示 snort 队列耗尽时拍摄的快照的内容。它显示所选快照的内容。输出类似于 **show capture** 命令的输出。

示例

以下是 **show asp inspect-dp snort queue-exhaustion** 命令的输出示例。

```
> show asp inspect-dp snort queue-exhaustion snapshot 1
102 packets captured
   1: 13:52:36.266343       10.100.26.6.80 > 192.168.26.6.45858: .
693143043:693144411(1368) ack 1996534769 win 235 <nop,nop,timestamp 25172833 64977907>
   2: 13:52:36.266343       10.100.26.6.80 > 192.168.26.6.45858: .
693144411:693145779(1368) ack 1996534769 win 235 <nop,nop,timestamp 25172833 64977907>
   3: 13:52:36.266343       10.100.26.6.80 > 192.168.26.6.45858: .
693145779:693147147(1368) ack 1996534769 win 235 <nop,nop,timestamp 25172838 64977912>
   4: 13:52:36.266343       10.100.26.6.80 > 192.168.26.6.45858: .
693147147:693148515(1368) ack 1996534769 win 235 <nop,nop,timestamp 25172838 64977912>
   5: 13:52:36.266343       10.100.26.6.80 > 192.168.26.6.45858: .
693153987:693155355(1368) ack 1996534769 win 235 <nop,nop,timestamp 25172858 64977932>
   6: 13:52:36.266343       10.100.26.6.80 > 192.168.26.6.45858: .
(...output truncated...)
```

show asp load-balance

要显示负载均衡器队列大小的直方图，请使用 **show asp load-balance** 命令。

show asp load-balance ［**detail**］

Syntax Description

detail	（可选）显示有关示例中使用的散列存储桶的详细信息。

Command History

版本	修改
6.1	引入了此命令。

使用指南

show asp load-balance 命令可能会帮助您排除故障。通常，数据包将由从接口接收环拉入的同一核心进行处理。但是，如果另一个核心已经处理与刚接收的数据包相同的连接，则该数据包将排队至该核心。这种排队可能会导致负载均衡器队列增长，而其他核心处于空闲状态。有关详细信息，请参阅 **asp load-balance per-packet** 命令。

示例

以下是 **show asp load-balance** 命令的输出示例。X 轴表示在不同队列中排队的数据包数量。Y 轴表示有数据包排队的负载均衡器散列桶数量，请不要与直方图标题中的桶（指直方图桶）混淆。要了解拥有队列的散列桶的确切数量，请使用 **detail** 关键字。

```
> show asp load-balance
Histogram of 'ASP load balancer queue sizes'
  64 buckets sampling from 1 to 65 (1 per bucket)
  6 samples within range (average=23)
                    ASP load balancer queue sizes
  100 +
      |
      |
      |
S     |
a     |
m     |
p     |
l  10 +
e     |
s     |
      |
      |
      |                          #
      |   # #                    # #           #
      |   # #                    # #           #
      +---------+---------+---------+---------+---------+---------+----
                10        20        30        40        50        60
                          # of queued jobs per queue
```

Related Commands

命令	Description
asp load-balance per-packet	更改多核心 ASA 型号的核心负载平衡方法。

show asp multiprocessor accelerated- features

要调试加速安全路径多处理器加速，请使用 **show asp multiprocessor accelerated-features** 命令。

show asp multiprocessor accelerated-features

Command History

版本	修改
6.1	引入了此命令。

使用指南

show asp multiprocessor accelerated-features 命令显示为多处理器加速的功能列表，这可能有助于您解决性能问题。

示例

以下是 **show asp multiprocessor accelerated-features** 命令的输出示例：

```
> show asp multiprocessor accelerated-features
MultiProcessor accelerated feature list:
        Access Lists
        DNS Guard
        Failover Stateful Updates
        Flow Operations(create, update, and tear-down)
        Inspect HTTP URL Logging
        Inspect HTTP (AIC)
        Inspect IPSec Pass through
        Inspect ICMP and ICMP error
        Inspect RTP/RTCP
        IP Audit
        IP Fragmentation & Re-assembly
        IPSec data-path
        MPF L2-L4 Classify
        Multicast forwarding
        NAT/PAT
        Netflow using UDP transport
        Non-AIC Inspect DNS
        Packet Capture
        QOS
        Resource Management
        Routing Lookup
        Shun
        SSL data-path
        Syslogging using UDP transport
        TCP Intercept
        TCP Security Engine
        TCP Transport
        Threat Detection
        Unicast RPF
        WCCP Re-direct
Above list applies to routed, transparent, single and multi mode.
```

show asp overhead

要跟踪和显示自旋锁和异步丢失统计信息，请使用 **show asp overhead** 命令。

show asp overhead ［**sort-by-average**］［**sort-by-file**］

Syntax Description

sort-by-average	按每次调用的平均周期对结果进行排序
sort-by-file	按文件名对结果进行排序

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show asp overhead** 命令的输出示例：

```
> show asp overhead
0.0% of available CPU cycles were lost to Multiprocessor overhead
        since last the MP overhead statistics were last cleared
              File Name Line Function Call             Avg         Cycles      %
---------------------- ---- ----------------------  -----  -------------  -----
```

show asp packet-profile

要显示预过滤器策略快速路径的数据包数量、作为大型流进行了卸载、完全通过访问控制（Snort）进行评估，请使用 **show asp packet-profile** 命令。

show asp packet-profile [data-path offload snort]

Syntax Description

data-path	显示数据平面数据包配置文件的计数器。
offload	显示硬件负载分流数据包配置文件的计数器。
snort	显示 snort 数据包配置文件的计数器。

Command Default

如果未指定实例，则显示所有实例。

Command History

版本	修改
6.5	引入了此命令。

使用指南

根据配置的访问策略、Snort 判定和数据流分流支持等硬件功能，通过 threat defense 设备的每个数据包都会经历不同的处理阶段。

全局计数器用于跟踪这些统计信息，并在每个会话结束时进行更新。这些全局计数器以直方图的形式收集和表示。在任何给定点，直方图都会显示自设备启动或上次重启以来系统处理的累积数据包计数器。

示例

以下是 **show asp packet-profile** 命令的输出示例。

```
> show asp packet-profile
Current config state: Enabled

Packets Processed
=================

        hw-dynamic-offload                :                   0
        hw-static-offload                 :                   0
        data-path-trust                   :             1419636
        data-path-snort                   :             3522634
        data-path-snort-bypass-allowedlist :              144496
        data-path-snort-bypass-blockedlist :                   0
        data-path-snort-busy-failopen     :                   0
        data-path-snort-down-failopen     :                  10

        data-path-snort-pre-allowedlist-distribution
        --------------------------------------------

                Packets         :    Connections
                [0-3]           :                0
                [4-7]           :             6202
```

```
        [8-15]          :                10950
        [16-31]         :                 2487
        [32-63]         :                   85
        [64-127]        :                    0
        [128-255]       :                    0
        [256-511]       :                    0
        [512-1023]      :                    0
        [1024 and above]:                    0

data-path-snort-pre-blockedlist-distribution
-------------------------------------------

        Packets         :    Connections
        [0-3]           :                    0
        [4-7]           :                    0
        [8-15]          :                    0
        [16-31]         :                    0
        [32-63]         :                    0
        [64-127]        :                    0
        [128-255]       :                    0
        [256-511]       :                    0
        [512-1023]      :                    0
        [1024 and above]:                    0

data-path-snort-post-allowedlist-distribution
---------------------------------------------

        Packets         :    Connections
        [0-3]           :                    0
        [4-7]           :                    0
        [8-15]          :                    0
        [16-31]         :                    0
        [32-63]         :                    0
        [64-127]        :                    0
        [128-255]       :                    0
        [256-511]       :                    0
        [512-1023]      :                    0
        [1024 and above]:                    0

offload-post-allowedlist-distribution
-------------------------------------

        Packets         :    Connections
        [0-3]           :                    0
        [4-7]           :                    0
        [8-15]          :                    0
        [16-31]         :                    0
        [32-63]         :                    0
        [64-127]        :                    0
        [128-255]       :                    0
        [256-511]       :                    0
        [512-1023]      :                    0
        [1024 and above]:                    0
>
>
```

show asp rule-engine

要查看 tmatch 编译过程的状态，请使用 **show asp rule-engine** 命令。

show asp rule-engine

Command History

版本	修改
7.1	引入了此命令。

示例

以下示例显示用作访问组的访问列表的编译正在进行还是已完成。编译时间取决于访问列表的大小。“开始”和“已完成”的时间状态对于所有规则都是通用的，因为它是一个批处理过程，而不是特定于模块。大多数模块元素计数将显示在表中。状态还显示 NAT 规则、路由、对象和接口编译。

```
> show asp rule-engine

Rule compilation Status:   Completed
Duration(ms):              421
Start Time:                18:58:34 UTC Apr 7 2021
Last Completed Time:       18:58:44 UTC Apr 7 2021
ACL Commit Mode:           MANUAL
Object Group Search:       DISABLED
Transitional Commit Model: DISABLED

Module    |  Insert   |  Remove   |  Current   |

 NAT      |       90  |       60  |        30  |
 ROUTE    |      107  |       40  |        67  |
 IFC      |       30  |       22  |         8  |
 ACL      |     1446  |      970  |       476  |
```

show asp table arp

要调试加速安全路径 ARP 表，请使用 **show asp table arp** 命令。

show asp table arp ［**interface** *interface_name*］［**address** *ip_address* ［**netmask** *mask*］］

Syntax Description

address *ip_address*	（可选）标识您要查看 ARP 表条目的 IP 地址。
interface *interface_name*	（可选）标识您要查看 ARP 表的特定接口。
netmask *mask*	（可选）设置 IP 地址的子网掩码。

Command History

版本	修改
6.1	引入了此命令。

使用指南

show arp 命令显示控制层面的内容，而 **show asp table arp** 命令显示加速安全路径的内容，可帮助您对问题进行故障排除。这些表格仅用于调试目的，信息输出可能会随时更改。请咨询思科 TAC 以帮助您使用此命令调试您的系统。

示例

以下是 **show asp table arp** 命令的输出示例：

```
> show asp table arp
Context: single_vf, Interface: inside
  10.86.194.50                            Active   000f.66ce.5d46 hits 0
  10.86.194.1                             Active   00b0.64ea.91a2 hits 638
  10.86.194.172                           Active   0001.03cf.9e79 hits 0
  10.86.194.204                           Active   000f.66ce.5d3c hits 0
  10.86.194.188                           Active   000f.904b.80d7 hits 0
Context: single_vf, Interface: identity
  ::                                      Active   0000.0000.0000 hits 0
  0.0.0.0                                 Active   0000.0000.0000 hits 50208
```

Related Commands

命令	Description
show arp	显示 ARP 表。
show arp statistics	显示 ARP 统计信息。

show asp table classify

要调试加速安全路径分类器表，请使用 **show asp table classify** 命令。

show asp table classify ［**interface** *interface_name*］［**crypto** | **domain** *domain_name*］［**hits**］［**match** *regexp*］

Syntax Description

crypto	（可选）仅显示加密、解密和 ipsec 隧道流域。
domain *domain_name*	（可选）显示特定分类器域的条目。有关可用域的列表，请参阅 CLI 帮助。
hits	（可选）显示具有非零命中值的分类器条目。
interface *interface_name*	（可选）标识您要查看分类器表的特定接口。
match *regexp*	（可选）显示匹配正则表达式的分类器条目。正则表达式包含空格时请使用引号。

Command History

版本	修改
6.1	引入了此命令。

使用指南

show asp table classify 命令显示加速安全路径的分类器内容，可帮助您对问题进行故障排除。分类器检查传入数据包的属性（例如协议）以及源和目的地址，从而将每个数据包匹配适当的分类规则。每个规则均使用确定执行何种类型操作（例如丢弃数据包还是允许其通过）的分类域进行标记。所示信息仅用于调试目的，输出可能会随时更改。请咨询思科 TAC 以帮助您使用此命令调试您的系统。

示例

以下是 **show asp table classify** 命令的输出示例：

```
> show asp table classify
Interface test:
No. of aborted compiles for input action table 0x33b3d70: 29
in  id=0x36f3800, priority=10, domain=punt, deny=false
        hits=0, user_data=0x0, flags=0x0
        src ip=0.0.0.0, mask=0.0.0.0, port=0, tag=any
        dst ip=10.86.194.60, mask=255.255.255.255, port=0, tag=any
in  id=0x33d3508, priority=99, domain=inspect, deny=false
        hits=0, user_data=0x0, use_real_addr, flags=0x0
        src ip=0.0.0.0, mask=0.0.0.0, port=0, tag=any
        dst ip=0.0.0.0, mask=0.0.0.0, port=0, tag=any
in  id=0x33d3978, priority=99, domain=inspect, deny=false
        hits=0, user_data=0x0, use_real_addr, flags=0x0
        src ip=0.0.0.0, mask=0.0.0.0, port=53, tag=any
        dst ip=0.0.0.0, mask=0.0.0.0, port=0, tag=any
```

```
...
```

以下是 **show asp table classify hits** 命令的输出示例，带有上次清除命中计数器的记录：

```
Interface mgmt:
in id=0x494cd88, priority=210, domain=permit, deny=true
       hits=54, user_data=0x1, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip=0.0.0.0,
       mask=0.0.0.0, port=0 dst ip=255.255.255.255, mask=255.255.255.255, port=0,
       dscp=0x0
in id=0x494d1b8, priority=112, domain=permit, deny=false
       hits=1, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=1 src ip=0.0.0.0,
       mask=0.0.0.0, port=0 dst ip=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0

Interface inside:
in id=0x48f1580, priority=210, domain=permit, deny=true
       hits=54, user_data=0x1, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip=0.0.0.0,
       mask=0.0.0.0, port=0 dst ip=255.255.255.255, mask=255.255.255.255, port=0,
       dscp=0x0
in id=0x48f09e0, priority=1, domain=permit, deny=false
       hits=101, user_data=0x0, cs_id=0x0, l3_type=0x608 src mac=0000.0000.0000,
       mask=0000.0000.0000 dst mac=0000.0000.0000, mask=0000.0000.0000
Interface outside:
in id=0x48c0970, priority=210, domain=permit, deny=true
       hits=54, user_data=0x1, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip=0.0.0.0,
       mask=0.0.0.0, port=0 dst ip=255.255.255.255, mask=255.255.255.255, port=0, dscp=0x0
```

以下是来自包含 Layer 2 信息地 **show asp table classify hits** 命令的输出示例：

```
Input Table
in  id=0x7fff2de10ae0, priority=120, domain=permit, deny=false
    hits=4, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=1
    src ip/id=0.0.0.0, mask=0.0.0.0, icmp-type=0
    dst ip/id=0.0.0.0, mask=0.0.0.0, icmp-code=0, dscp=0x0
    input_ifc=LAN-SEGMENT, output_ifc=identity in  id=0x7fff2de135c0, priority=0,
domain=inspect-ip-options, deny=true
    hits=41, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
    src ip/id=0.0.0.0, mask=0.0.0.0, port=0
    dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
    input_ifc=LAN-SEGMENT, output_ifc=any
...

Output Table:

L2 - Output Table:

L2 - Input Table:
in  id=0x7fff2de0e080, priority=1, domain=permit, deny=false
    hits=30, user_data=0x0, cs_id=0x0, l3_type=0x608
    src mac=0000.0000.0000, mask=0000.0000.0000
    dst mac=0000.0000.0000, mask=0000.0000.0000
    input_ifc=LAN-SEGMENT, output_ifc=any
in  id=0x7fff2de0e580, priority=1, domain=permit, deny=false
    hits=382, user_data=0x0, cs_id=0x0, l3_type=0x8
    src mac=0000.0000.0000, mask=0000.0000.0000
    dst mac=0000.0000.0000, mask=0100.0000.0000
    input_ifc=LAN-SEGMENT, output_ifc=any
in  id=0x7fff2de0e800, priority=1, domain=permit, deny=false
    hits=312, user_data=0x0, cs_id=0x0, l3_type=0x8
    src mac=0000.0000.0000, mask=0000.0000.0000
    dst mac=ffff.ffff.ffff, mask=ffff.ffff.ffff
```

```
input_ifc=LAN-SEGMENT, output_ifc=any
```

show asp table cluster chash-table

要调试用于群集技术的加速安全路径 cHash 表，请使用 **show asp table cluster chash-table** 命令。

show asp table cluster chash-table

Command History

版本	修改
6.1	引入了此命令。

使用指南

show asp table cluster chash-table 命令显示加速安全路径的内容，可帮助您对问题进行故障排除。这些表格仅用于调试目的，信息输出可能会随时更改。请咨询思科 TAC 以帮助您使用此命令调试您的系统。

示例

以下是 **show asp table cluster chash-table** 命令的输出示例：

```
> show asp table cluster chash-table
Cluster current chash table:

00003333
21001200
22000033
02222223
33331111
21110000
00133103
22222223
30000102
11222222
23222331
00002223
(...output truncated...)
```

Related Commands

命令	Description
show asp cluster counter	显示集群数据路径计数器信息。

show asp table interfaces

要调试加速安全路径接口表，请使用 **show asp table interfaces** 命令。

show asp table interfaces

Command History

版本	修改
6.1	引入了此命令。

使用指南

show asp table interfaces 命令显示加速安全路径的接口表内容，可帮助您对问题进行故障排除。这些表格仅用于调试目的，信息输出可能会随时更改。请咨询思科 TAC 以帮助您使用此命令调试您的系统。

示例

以下是 **show asp table interfaces** 命令的输出示例：

```
> show asp table interfaces
** Flags: 0x0001-DHCP, 0x0002-VMAC, 0x0010-Ident Ifc, 0x0020-HDB Initd,
   0x0040-RPF Enabled
Soft-np interface 'dmz' is up
    context single_vf, nicnum 0, mtu 1500
        vlan 300, Not shared, seclvl 50
        0 packets input, 1 packets output
        flags 0x20
Soft-np interface 'foo' is down
    context single_vf, nicnum 2, mtu 1500
        vlan <None>, Not shared, seclvl 0
        0 packets input, 0 packets output
        flags 0x20
Soft-np interface 'outside' is down
    context single_vf, nicnum 1, mtu 1500
        vlan <None>, Not shared, seclvl 50
        0 packets input, 0 packets output
        flags 0x20
Soft-np interface 'inside' is up
    context single_vf, nicnum 0, mtu 1500
        vlan <None>, Not shared, seclvl 100
        680277 packets input, 92501 packets output
        flags 0x20
...
```

show asp table network-service

要调试加速安全路径网络服务对象表，请使用 **show asp table network-service** 命令。

show asp table network-service

Command History

版本	修改
7.1	引入了此命令。

示例

以下示例显示如何显示网络服务对象表：

```
> show asp table network-service
Per-Context Category NSG:
        subnet=0.0.0.0/0, branch_id=214491, branch_name=connect.facebook.net.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=214491, branch_name=connect.facebook.net.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=370809, branch_name=facebook.com.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=370809, branch_name=facebook.com.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=490321, branch_name=fbcdn.net.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=490321, branch_name=fbcdn.net.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=548791, branch_name=fbcdn-photos-a.akamaihd.net.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=548791, branch_name=fbcdn-photos-a.akamaihd.net.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=681143, branch_name=fbcdn-photos-e-a.akamaihd.net.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=681143, branch_name=fbcdn-photos-e-a.akamaihd.net.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=840741, branch_name=fbcdn-photos-b-a.akamaihd.net.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=840741, branch_name=fbcdn-photos-b-a.akamaihd.net.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=1014669, branch_name=fbstatic-a.akamaihd.net.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=1014669, branch_name=fbstatic-a.akamaihd.net.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=1098051, branch_name=fbexternal-a.akamaihd.net.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=1098051, branch_name=fbexternal-a.akamaihd.net.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=1217875, branch_name=fbcdn-profile-a.akamaihd.net.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=1217875, branch_name=fbcdn-profile-a.akamaihd.net.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=1379985, branch_name=fbcdn-creative-a.akamaihd.net.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=1379985, branch_name=fbcdn-creative-a.akamaihd.net.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
```

```
        subnet=0.0.0.0/0, branch_id=1524617, branch_name=channel.facebook.com.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=1524617, branch_name=channel.facebook.com.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=1683343, branch_name=fbcdn-dragon-a.akamaihd.net.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=1683343, branch_name=fbcdn-dragon-a.akamaihd.net.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=1782703, branch_name=contentcache-a.akamaihd.net.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=1782703, branch_name=contentcache-a.akamaihd.net.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=1868733, branch_name=facebook.net.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=1868733, branch_name=facebook.net.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=2068293, branch_name=plus.google.com.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=2068293, branch_name=plus.google.com.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=2176667, branch_name=instagram.com.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=2176667, branch_name=instagram.com.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=2317259, branch_name=linkedin.com.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=2317259, branch_name=linkedin.com.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
```

show asp table routing

要调试加速安全路径路由表，请使用 **show asp table routing** 命令。此命令支持 IPv4 和 IPv6 地址。

show asp table routing ［**vrf** *name* | **all**］ ［**management-only**］［**input** | **output**］［**address** *ip_address* ［**netmask** *mask*］ | **interface** *interface_name*］

Syntax Description

address *ip_address*	设置您要查看路由条目的IP地址。对于IPv6地址，您可以包含子网掩码，形式为斜线 (/) 后跟前缀（0 至 128）。例如，输入 fe80::2e0:b6ff:fe01:3b7a/128。
input	显示输入路由表的条目。
interface *interface_name*	（可选）标识您要查看路由表的特定接口。
netmask *mask*	对于 IPv4 地址，指定子网掩码。
output	显示输出路由表的条目。
management-only	显示管理路由表中的号码携带路由。
［**vrf** *name*	**all**］	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将视图限制为特定虚拟路由器。如果要查看所有虚拟路由器的路由表，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则命令会显示全局 VRF 虚拟路由器的路由表。

Command History

版本	修改
6.1	引入了此命令。
6.6	添加了 ［**vrf** *name*	**all**］ 关键字。

使用指南

show asp table routing 命令显示加速安全路径的路由表内容，可帮助您对问题进行故障排除。这些表格仅用于调试目的，信息输出可能会随时更改。请咨询思科TAC以帮助您使用此命令调试您的系统。management-only 关键字显示管理路由表中的号码可携带性路由。

示例

以下是 **show asp table routing** 命令的输出示例：

```
> show asp table routing

in   255.255.255.255 255.255.255.255 identity
in   224.0.0.9       255.255.255.255 identity
in   10.86.194.60    255.255.255.255 identity
in   10.86.195.255   255.255.255.255 identity
in   10.86.194.0     255.255.255.255 identity
in   209.165.202.159 255.255.255.255 identity
```

```
in   209.165.202.255 255.255.255.255 identity
in   209.165.201.30  255.255.255.255 identity
in   209.165.201.0   255.255.255.255 identity
in   10.86.194.0     255.255.254.0   inside
in   224.0.0.0       240.0.0.0       identity
in   0.0.0.0         0.0.0.0         inside
out  255.255.255.255 255.255.255.255 foo
out  224.0.0.0       240.0.0.0       foo
out  255.255.255.255 255.255.255.255 test
out  224.0.0.0       240.0.0.0       test
out  255.255.255.255 255.255.255.255 inside
out  10.86.194.0     255.255.254.0   inside
out  224.0.0.0       240.0.0.0       inside
out  0.0.0.0         0.0.0.0         via 10.86.194.1, inside
out  0.0.0.0         0.0.0.0         via 0.0.0.0, identity
out  ::              ::              via 0.0.0.0, identity
```

以下示例显示名为 alpha 的虚拟路由器的路由表。

```
> show asp table routing vrf alpha
Routing table for vrf alpha
route table timestamp: 3916283895
in   1.1.1.1         255.255.255.255 identity
in   1.1.1.0         255.255.255.0   i1
out  255.255.255.255 255.255.255.255 i1
out  1.1.1.1         255.255.255.255 i1
out  1.1.1.0         255.255.255.0   i1
out  224.0.0.0       240.0.0.0       i1
```

Related Commands

命令	Description
show route	在控制层面中显示路由表。

show asp table socket

要帮助调试加速安全路径套接字信息，请使用 **show asp table socket** 命令。

show asp table socket ［处理］［**stats**］

Syntax Description

处理	指定套接字的长度。
stats	显示加速安全路径套接字表的统计信息。

Command History

版本	修改
6.1	引入了此命令。

使用指南

show asp table socket 命令显示加速安全路径套接字信息，可在对加速安全路径套接字问题进行故障排除时提供帮助。这些表格仅用于调试目的，信息输出可能会随时更改。请咨询思科 TAC 以帮助您使用此命令调试您的系统。

示例

以下是 **show asp table socket** 命令的输出示例。

```
Protocol  Socket    Local Address               Foreign Address         State
TCP       00012bac  10.86.194.224:23            0.0.0.0:*               LISTEN
TCP       0001c124  10.86.194.224:22            0.0.0.0:*               LISTEN
SSL       00023b84  10.86.194.224:443           0.0.0.0:*               LISTEN
SSL       0002d01c  192.168.1.1:443             0.0.0.0:*               LISTEN
DTLS      00032b1c  10.86.194.224:443           0.0.0.0:*               LISTEN
SSL       0003a3d4  0.0.0.0:443                 0.0.0.0:*               LISTEN
DTLS      00046074  0.0.0.0:443                 0.0.0.0:*               LISTEN
TCP       02c08aec  10.86.194.224:22            171.69.137.139:4190     ESTAB
```

以下是 **show asp table socket stats** 命令的输出示例。

```
TCP Statistics:
  Rcvd:
     total 14794
     checksum errors 0
     no port 0
  Sent:
     total 0
UDP Statistics:
  Rcvd:
     total 0
     checksum errors 0
  Sent:
     total 0
     copied 0
NP SSL System Stats:
  Handshake Started: 33
  Handshake Complete: 33
```

```
SSL Open: 4
SSL Close: 117
SSL Server: 58
SSL Server Verify: 0
SSL Client: 0
```

TCP/UDP 统计信息是数据包计数器，表示指向设备上运行或侦听的服务（例如 Telnet、SSH 或 HTTPS）的发送或接收数据包数量。校验和错误是由于计算的数据包校验和不匹配数据包中存储的校验和值（也就是说，数据包已损坏）而丢弃的数据包数量。NP SSL 统计信息指示收到的每种类型的消息数量。大多数消息均指示开始和结束到 SSL 服务器或 SSL 客户端实例的新 SSL 连接。

Related Commands

命令	Description
show asp table vpn-context	显示加速安全路径 VPN 情景表。

show asp table vpn-context

要调试加速安全路径 VPN 情景表，请使用 **show asp table vpn-context** 命令。

show asp table vpn-context ［**detail**］

Syntax Description

detail	（可选）显示 VPN 情景表的更多详细信息。

Command History

版本	修改
6.1	引入了此命令。

使用指南

show asp table vpn-context 命令显示加速安全路径的 VPN 情景内容，可帮助您对问题进行故障排除。这些表格仅用于调试目的，信息输出可能会随时更改。请咨询思科 TAC 以帮助您使用此命令调试您的系统。

示例

以下是 **show asp table vpn-context** 命令的输出示例：

```
> show asp table vpn-context
VPN ID=0058070576, DECR+ESP, UP, pk=0000000000, rk=0000000000, gc=0
VPN ID=0058193920, ENCR+ESP, UP, pk=0000000000, rk=0000000000, gc=0
VPN ID=0058168568, DECR+ESP, UP, pk=0000299627, rk=0000000061, gc=2
VPN ID=0058161168, ENCR+ESP, UP, pk=0000305043, rk=0000000061, gc=1
VPN ID=0058153728, DECR+ESP, UP, pk=0000271432, rk=0000000061, gc=2
VPN ID=0058150440, ENCR+ESP, UP, pk=0000285328, rk=0000000061, gc=1
VPN ID=0058102088, DECR+ESP, UP, pk=0000268550, rk=0000000061, gc=2
VPN ID=0058134088, ENCR+ESP, UP, pk=0000274673, rk=0000000061, gc=1
VPN ID=0058103216, DECR+ESP, UP, pk=0000252854, rk=0000000061, gc=2
...
```

以下是启用永久 IPsec 隧道流功能后（如 PRESERVE 标记所示） **show asp table vpn-context** 命令的输出示例：

```
> show asp table vpn-context
VPN CTX=0x0005FF54, Ptr=0x6DE62DA0, DECR+ESP+PRESERVE, UP, pk=0000000000,
rk=0000000000, gc=0
VPN CTX=0x0005B234, Ptr=0x6DE635E0, ENCR+ESP+PRESERVE, UP, pk=0000000000,
rk=0000000000, gc=0
```

以下是 **show asp table vpn-context detail** 命令的输出示例。启用持久 IPsec 隧道流量功能后，这些标志将包括 PRESERVE 标志。

```
> show asp table vpn-context detail

VPN Ctx  = 0058070576 [0x03761630]
State    = UP
Flags    = DECR+ESP
```

```
SA       = 0x037928F0
SPI      = 0xEA0F21F0
Group    = 0
Pkts     = 0
Bad Pkts = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0

VPN Ctx  = 0058193920 [0x0377F800]
State    = UP
Flags    = ENCR+ESP
SA       = 0x037B4B70
SPI      = 0x900FDC32
Group    = 0
Pkts     = 0
Bad Pkts = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0
...
```

Related Commands

命令	Description
show asp drop	显示已丢弃数据包的加速安全路径计数器。

show asp table zone

要调试加速安全路径区域表，请使用 **show asp table zone** 命令。

show asp table zone

Command History

版本	修改
6.1	引入了此命令。

使用指南

show asp table zone 命令显示加速安全路径的内容，可帮助您对问题进行故障排除。这些表格仅用于调试目的，信息输出可能会随时更改。请咨询思科 TAC 以帮助您使用此命令调试您的系统。

示例

以下是 **show asp table zone** 命令的输出示例。在本示例中，名为 is-154 的区域实际上是一个内联集，而不是流量区域。

```
> show asp table zone
Zone: krjones-passive-security-zone id: 48947
    Security-level: 0
    Context       : single_vf
    Zone member(s):
      passive                       GigabitEthernet0/0

Zone: passive_default_context_0 id: 1
    Security-level: 0
    Context       : single_vf
    Zone member(s):

Zone: is-154 id: 34309
    Security-level: 0
    Context       : single_vf
    Zone member(s):
      out                           GigabitEthernet0/2
      in                            GigabitEthernet0/1
```

Related Commands

命令	Description
show inline-set	显示内联集。
show zone	显示流量区域。

show audit-log

要显示系统审核日志，请使用 **show audit-log** 命令。

show audit-log

Command History

版本	修改
6.1	引入了此命令。

使用指南

此命令按时间倒序显示审核日志；首先列出最近的审核日志事件。

事件可能包括系统更新、权限问题、配置更改和策略应用。此信息仅适用于管理中心远程管理的设备。本地托管系统的审核日志为空。

示例

以下示例显示了审核日志。

```
> show audit-log
Audit Log Output:
 time                   :  1476223151 (Tue Oct 11 21:59:11 2016)
 event_type             :  notify
 subsystem              :  Task Queue
 actor                  :  System
 message                :  Successful task completion : Clam update synchronization
from firepower
 result                 :  Success
 action_source_ip       :  localhost
 action_destination_ip  :  localhost
-------------------------------------------------------------
 time                   :  1476222646 (Tue Oct 11 21:50:46 2016)
 event_type             :  notify
 subsystem              :  Task Queue
 actor                  :  System
 message                :  Successful task completion : Apply AMP Dynamic Analysis C
onfiguration from firepower
 result                 :  Success
 action_source_ip       :  localhost
 action_destination_ip  :  localhost
-------------------------------------------------------------
 time                   :  1476222564 (Tue Oct 11 21:49:24 2016)
 event_type             :  notify
 subsystem              :  Task Queue
 actor                  :  System
 message                :  Successful task completion : Apply Initial_Health_Policy
2016-10-11 18:54:59 from firepower
 result                 :  Success
 action_source_ip       :  localhost
 action_destination_ip  :  localhost
-------------------------------------------------------------
 time                   :  1476222563 (Tue Oct 11 21:49:23 2016)
 event_type             :  notify
 subsystem              :  Health > Health Policy > Apply > Initial_Health_Policy 20
16-10-11 18:54:59 > firepower
```

```
 actor                  :  admin
 message                :  Apply
 result                 :  Success
 action_source_ip       :  127.0.0.1
 action_destination_ip  :  localhost
-----------------------------------------------------------
 time                   :  1476222508 (Tue Oct 11 21:48:28 2016)
 event_type             :  notify
 subsystem              :  Task Queue
 actor                  :  System
 message                :  Successful task completion : Registration '10.83.57.41'
 result                 :  Success
 action_source_ip       :  localhost
 action_destination_ip  :  localhost
-----------------------------------------------------------
 time                   :  1476222473 (Tue Oct 11 21:47:53 2016)
 event_type             :  Restart
 subsystem              :  NTP Configuration changed
 actor                  :  Default User
 message                :  Restart
 result                 :  Success
 action_source_ip       :  Default User IP
 action_destination_ip  :  Default Target IP
-----------------------------------------------------------
```

show b

- show bridge-group，第 471 页

show banner

要显示已配置的横幅消息，请输入 **show banner** 命令。

show banner ［**login**］

Syntax Description

login	显示为密码登录提示设置的横幅。

Command History

版本	修改
6.1	引入了此命令。

示例

```
> show banner
```

show bfd drops

要显示 BFD 中丢弃的数据包的编号，请使用 **show bfd drops** 命令。

show bfd drops

Command History

版本	修改
6.3	引入了此命令。

示例

以下示例显示 BFD 丢弃的数据包。

```
> show bfd drops
BFD Drop Statistics
                         IPV4 IPV6 IPV4-M IPV6-M
Invalid TTL              0    0    0      0
BFD Not Configured       0    0    0      0
No BFD Adjacency         0    0    0      0
Invalid Header Bits      0    0    0      0
Invalid Discriminator    0    0    0      0
Session AdminDown        0    0    0      0
Authen invalid BFD ver   0    0    0      0
Authen invalid len       0    0    0      0
Authen invalid seq       0    0    0      0
Authen failed            0    0    0      0
```

Related Commands

命令	Description
clear bfd counters	清除 BFD 计数器。
show bfd map	显示配置的 BFD 映射。
show bfd neighbors	显示现有 BFD 邻接关系逐行列表。
show bfd summary	显示 BFD 的概要信息。

show bfd map

要显示已配置的 BFD 映射，请使用 **show bfd map** 命令。

show bfd map

Command History

版本	修改
6.3	引入了此命令。

示例

以下示例显示 BFD 映射。

```
> show bfd map
Destination: 40.40.40.2/24
 Source: 50.50.50.2/24
 Template: mh
 Authentication(Type): sha-1
```

Related Commands

命令	Description
clear bfd counters	清除 BFD 计数器。
show bfd drops	显示 BFD 中已丢弃的数据包数。
show bfd neighbors	显示现有 BFD 邻接关系逐行列表。
show bfd summary	显示 BFD 的概要信息。

show bfd neighbors

要显示现有 BFD 邻接关系逐行列表，请使用 **show bfd neighbors** 命令。

show bfd neighbors ［**client bgp**］［**ipv4** ［*ip_address*］ | **ipv6** ［*ipv6_address*］ | **multihop-ipv4** ［*ip_address*］ | **multihop-ipv6** ［*ipv6_address*］］［**inactive**］［**detail**］

Syntax Description

client bgp	（可选）显示 BGP 客户端的邻居。
ipv4 [ip_address]	（可选）显示单跳 IPv4 邻居。您可以选择指定特定的邻居地址。
ipv6 [*ipv6_address*]	（可选）显示单跳 IPv6 邻居。您可以选择指定特定的邻居地址。
multihop-ipv4 [*ip_address*]	（可选）显示多跳 IPv4 邻居。您可以选择指定特定的邻居地址。
multihop-ipv6 [*ipv6_address*]	（可选）显示多跳 IPv6 邻居。您可以选择指定特定的邻居地址。
inactive	（可选）显示非活动邻接关系。
detail	（可选）显示每个邻居的所有 BFD 协议参数和计时器。

Command History

版本	修改
6.3	引入了此命令。

示例

以下示例显示 BFD 邻居。

```
> show bfd neighbors
OurAddr     NeighAddr    LD/RD  RH     Holdown(mult)     State Int
172.16.10.1 172.16.10.2  1/6    1      260 (3 )          Up    Fa0/1
```

Related Commands

命令	Description
clear bfd counters	清除 BFD 计数器。
show bfd drops	显示 BFD 中已丢弃的数据包数。
show bfd map	显示配置的 BFD 映射。
show bfd summary	显示 BFD 的概要信息。

show bfd summary

要显示 BFD 的摘要信息，请使用 **show bfd summary** 命令。

show bfd summary ［**client** | **session**］

Syntax Description

client	（可选）显示客户端的 BFD 摘要。
session	（可选）显示会话的 BFD 摘要。

Command History

版本	修改
6.3	引入了此命令。

使用指南

使用此命令以显示 BFD、BFD 客户端或 BFD 会话的摘要信息。当 BFD 客户端启动与对等体的会话时，BFD会定期向对等体发送BFD控制数据包。此命令的输出中包含有关会话的以下状态的信息：

- Up - 当另一个 BFD 接口确认 BFD 控制数据包时，会话进入 Up 状态。
- 关闭 - 如果发生数据路径故障，并且 BFD 在配置的时间内未收到控制数据包，则声明会话和数据路径关闭。当会话关闭时，BFD会通知BFD客户端，以便客户端可以执行必要的操作来重新路由流量。

示例

以下示例显示 BFD 摘要。

```
> show bfd summary
         Session         Up      Down
Total    1               1       0

> show bfd summary session
Protocol Session     Up  Down
IPV4     1           1     0
Total    1           1     0

> show bfd summary client
Client   Session      Up     Down
BGP      1            1      0
EIGRP    1            1      0
Total    2            2      0
```

Related Commands

命令	Description
clear bfd counters	清除 BFD 计数器。
show bfd drops	显示 BFD 中已丢弃的数据包数。

命令	Description
show bfd map	显示配置的 BFD 映射。
show bfd neighbors	显示现有 BFD 邻接关系逐行列表。

show bgp

要显示边界网关协议 (BGP) 路由表中的条目，请使用 **show bgp** 命令。

show bgp ［**vrf** *name* | **all**］ ［*ip-address* ［*mask* ［**longer-prefixes** ［**injected**］ | **shorter-prefixes** ［*length*］ | **bestpath** | **multipaths** | **subnets**］ | **bestpath** | **multipaths**］ | **all** | **prefix-list** *name* | **pending-prefixes** | **route-map** *name*］］

Syntax Description

ip-address	（可选）指定 BGP 路由表中要显示的网络。
mask	（可选）用于过滤作为指定网络的一部分的主机或与它们匹配的掩码。
longer-prefixes	（可选）显示指定的路由和所有更具体的路由。
injected	（可选）显示向 BGP 路由表中注入的更具体的前缀。
shorter-prefixes	（可选）显示指定的路由和所有不太具体的路由。
length	（可选）前缀长度。此参数的值是一个介于 0 到 32 之间的数字。
bestpath	（可选）显示此前缀的最佳路径。
multipaths	（可选）显示此前缀的多个路径。
subnets	（可选）显示指定前缀的子网路由。
all	（可选）显示 BGP 路由表中的所有地址系列信息。
prefix-list *name*	（可选）过滤基于指定的前缀列表的输出。
pending-prefixes	（可选）显示 BGP 路由表的待定删除的前缀。
route-map *name*	（可选）过滤基于指定的路由地图的输出。
［**vrf** *name*	**all**］	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将该命令限制为特定虚拟路由器。如果您希望 命令影响所有虚拟路由器，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则 命令适用于全局 VRF 虚拟路由器。

Command History

版本	修改
6.1	引入了此命令。
6.6	添加了 ［**vrf** *name*	**all**］ 关键字。

使用指南

使用 **show bgp** 命令可显示路由表内容：可以过滤输出以显示特定前缀、前缀长度和通过前缀列表、路由地图或条件通告注入的前缀的条目。

示例

以下输出示例展示 BGP 路由表：

```
> show bgp
BGP table version is 22, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete
Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.1/32      0.0.0.0                  0         32768 i
*>i10.2.2.2/32      172.16.1.2               0    100      0 i
*bi10.9.9.9/32      192.168.3.2              0    100      0 10 10 i
*>                  192.168.1.2                            0 10 10 i
* i172.16.1.0/24    172.16.1.2               0    100      0 i
*>                  0.0.0.0                  0         32768 i
*> 192.168.1.0      0.0.0.0                  0         32768 i
*>i192.168.3.0      172.16.1.2               0    100      0 i
*bi192.168.9.0      192.168.3.2              0    100      0 10 10 i
*>                  192.168.1.2                            0 10 10 i
*bi192.168.13.0     192.168.3.2              0    100      0 10 10 i
*>                  192.168.1.2                            0 10 10 i
```

下表对每个字段进行了说明。

表 *3: show bgp* 字段

字段	Description
BGP table version	表的内部版本号。每当表更改时，此数字就会增加。
local router ID	路由器的 IP 地址。

字段	Description
Status codes	表条目的状态。该状态显示在表中每行的开头。它可以是下列值之一： • s - 表条目被抑制。 • d - 表条目被阻尼。 • h - 表条目历史记录。 • * - 表条目有效。 • > - 表条目是用于该网络的最佳条目。 • i - 通过内部 BGP (iBGP) 会话获知表条目。 • r - 表条目为 RIB 故障。 • S - 表条目过时。 • m - 表条目具有用于该网络的多个路径。 • b - 表条目具有用于该网络的备用路径。 • x - 表条目具有用于该网络的最佳外部路由。
Origin codes	条目的来源。源代码已置于表中每行的末尾。它可以是下列值之一： • i - 条目源自内部网关协议 (IGP) 并已通告。 • e - 从外部网关协议 (EGP) 发起的条目。 • ? - 路径的来源不明确。通常，这是一个从 IGP 向 BGP 重新分发的路由器。
Network	网络实体的 IP 地址。
Next Hop	在将数据包转发到目标网络时使用的下一个系统的 IP 地址。0.0.0.0 的条目表示路由器具有一些到此网络的非 BGP 路由。
Metric	自主系统间指标的值（如果显示）。
LocPrf	本地优先级值。默认值为 100。
Weight	通过自主系统过滤器设置的路由的权重。
Path	目标网络的自主系统路径。该路径中的每个自主系统都可在此字段中具有一个条目。
(stale)	表示在平滑重启过程中将指定的自主系统的以下路径标记为“stale”。

以下输出示例展示 BGP 路由表中的 192.168.1.0 条目的有关信息：

```
> show bgp 192.168.1.0
BGP routing table entry for 192.168.1.0/24, version 22
Paths: (2 available, best #2, table default)
```

```
  Additional-path
  Advertised to update-groups:
     3
  10 10
    192.168.3.2 from 172.16.1.2 (10.2.2.2)
      Origin IGP, metric 0, localpref 100, valid, internal, backup/repair
  10 10
    192.168.1.2 from 192.168.1.2 (10.3.3.3)
      Origin IGP, localpref 100, valid, external, best , recursive-via-connected
```

以下输出示例展示 BGP 路由表中的 10.3.3.3 255.255.255.255 条目的有关信息：

```
> show bgp 10.3.3.3 255.255.255.255

BGP routing table entry for 10.3.3.3/32, version 35
Paths: (3 available, best #2, table default)
Multipath: eBGP
Flag: 0x860
  Advertised to update-groups:
     1
  200
    10.71.8.165 from 10.71.8.165 (192.168.0.102)
      Origin incomplete, localpref 100, valid, external, backup/repair
      Only allowed to recurse through connected route
  200
    10.71.11.165 from 10.71.11.165 (192.168.0.102)
      Origin incomplete, localpref 100, weight 100, valid, external, best
      Only allowed to recurse through connected route
  200
    10.71.10.165 from 10.71.10.165 (192.168.0.104)
      Origin incomplete, localpref 100, valid, external,
      Only allowed to recurse through connected route
```

下表对每个字段进行了说明。

表 *4: show bgp (4 byte autonomous system numbers)* 字段

字段	Description
BGP routing table entry for	路由表条目的 IP 地址或网络号。
version	表的内部版本号。每当表更改时，此数字就会增加。
Paths	可用路径的数量和安装的最佳路径的数量。当最佳路径安装在 IP 路由表中时，此行显示“Default-IP-Routing-Table”。
Multipath	启用多路径负载共享时，显示此字段。此字段表示多个路径是 iBGP，还是 eBGP。
Advertised to update-groups	为每个更新组处理通告的数量。
Origin	条目的来源。来源可以是 IGP、EGP 或不完整的协议。此行显示配置的指标（0，如果未配置任何指标）、本地首选项值（100 为默认值）和路由（内部、外部、多路径、最佳）的状态和类型。

字段	Description
Extended Community	如果路由具有扩展的社区属性，则显示此字段。属性代码显示在此行上。在后面的一行上显示有关扩展的社区的信息。

以下是使用 **all** 关键字输入的 **show bgp** 命令的输出示例：显示有关所有配置的地址系列的信息。

```
> show bgp all

For address family: IPv4 Unicast   *****
BGP table version is 27, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.0/24      0.0.0.0                  0         32768 ?
*> 10.13.13.0/24    0.0.0.0                  0         32768 ?
*> 10.15.15.0/24    0.0.0.0                  0         32768 ?
*>i10.18.18.0/24    172.16.14.105         1388  91351      0 100 e
*>i10.100.0.0/16    172.16.14.107          262    272      0 1 2 3 i
*>i10.100.0.0/16    172.16.14.105         1388  91351      0 100 e
*>i10.101.0.0/16    172.16.14.105         1388  91351      0 100 e
*>i10.103.0.0/16    172.16.14.101         1388    173    173 100 e
*>i10.104.0.0/16    172.16.14.101         1388    173    173 100 e
*>i10.100.0.0/16    172.16.14.106         2219  20889      0 53285 33299 51178 47751 e
*>i10.101.0.0/16    172.16.14.106         2219  20889      0 53285 33299 51178 47751 e
*  10.100.0.0/16    172.16.14.109         2309             0 200 300 e
*>                  172.16.14.108         1388             0 100 e
*  10.101.0.0/16    172.16.14.109         2309             0 200 300 e
*>                  172.16.14.108         1388             0 100 e
*> 10.102.0.0/16    172.16.14.108         1388             0 100 e
*> 172.16.14.0/24   0.0.0.0                  0         32768 ?
*> 192.168.5.0      0.0.0.0                  0         32768 ?
*> 10.80.0.0/16     172.16.14.108         1388             0 50 e
*> 10.80.0.0/16     172.16.14.108         1388             0 50 e
```

以下是使用 **longer-prefixes** 关键字输入的 **show bgp** 命令的输出示例：

```
> show bgp 10.92.0.0 255.255.0.0 longer-prefixes

BGP table version is 1738, local router ID is 192.168.72.24
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop          Metric LocPrf Weight Path
*> 10.92.0.0        10.92.72.30         8896         32768 ?
*                   10.92.72.30                          0 109 108 ?
*> 10.92.1.0        10.92.72.30         8796         32768 ?
*                   10.92.72.30                          0 109 108 ?
*> 10.92.11.0       10.92.72.30        42482         32768 ?
*                   10.92.72.30                          0 109 108 ?
*> 10.92.14.0       10.92.72.30         8796         32768 ?
*                   10.92.72.30                          0 109 108 ?
*> 10.92.15.0       10.92.72.30         8696         32768 ?
*                   10.92.72.30                          0 109 108 ?
*> 10.92.16.0       10.92.72.30         1400         32768 ?
*                   10.92.72.30                          0 109 108 ?
```

```
*> 10.92.17.0        10.92.72.30        1400         32768 ?
*                    10.92.72.30                         0 109 108 ?
*> 10.92.18.0        10.92.72.30        8876         32768 ?
*                    10.92.72.30                         0 109 108 ?
*> 10.92.19.0        10.92.72.30        8876         32768 ?
*                    10.92.72.30                         0 109 108 ?
```

以下是使用 **shorter-prefixes** 关键字输入的 **show bgp** 命令的输出示例：指定 8 位前缀长度。

```
> show bgp 172.16.0.0/16 shorter-prefixes 8
*> 172.16.0.0         10.0.0.2                              0 ?
*                     10.0.0.2                0             0 200 ?
```

以下是使用 **prefix-list** 关键字输入的 **show bgp** 命令的输出示例：

```
> show bgp prefix-list ROUTE

BGP table version is 39, local router ID is 10.0.0.1
Status codes:s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes:i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 192.168.1.0      10.0.0.2                              0 ?
*                   10.0.0.2                 0            0 200 ?
```

以下是使用 **route-map** 关键字输入的 **show bgp** 命令的输出示例：

```
> show bgp route-map LEARNED_PATH

BGP table version is 40, local router ID is 10.0.0.1
Status codes:s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes:i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 192.168.1.0      10.0.0.2                              0 ?
*                   10.0.0.2                 0            0 200 ?
```

show bgp cidr-only

要显示具有无类域间路由 (CIDR) 的路由，请使用 **show bgp cidr-only** 命令。

show bgp cidr-only ［**vrf** *name* | **all**］

Syntax Description

［**vrf** *name*	**all**］	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将该命令限制为特定虚拟路由器。如果您希望 命令影响所有虚拟路由器，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则 命令适用于全局 VRF 虚拟路由器。

Command History

版本	修改
6.1	引入了此命令。
6.6	添加了 ［**vrf** *name*	**all**］ 关键字。

示例

以下是 **show bgp cidr-only** 命令的输出示例。有关输出的说明，请参阅 **show bgp** 命令。

```
> show bgp cidr-only

BGP table version is 220, local router ID is 172.16.73.131
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf Weight Path
*> 192.168.0.0/8    172.16.72.24                         0 1878 ?
*> 172.16.0.0/16    172.16.72.30                         0 108 ?
```

show bgp community

要显示属于指定 BGP 社区的路由，请使用 **show bgp community** 命令。

show bgp community ［**vrf** *name* | **all**］ ［*community-number*］［**exact-match**］［**no-advertise**］［**no-export**］

Syntax Description

community-number	（可选）有效值为一个从 1 到 4294967295 或 AA:NN 的范围内的社区编号（自主系统：社区编号，即一个 2 字节数字）。
exact-match	（可选）仅显示具有完全匹配项的路由。
no-advertise	（可选）仅显示不向任何对等设备（已知社区）通告的路由。
no-export	（可选）仅显示未在本地自主系统（已知社区）的外部导出的路由。
［**vrf** *name*	**all**］	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将该命令限制为特定虚拟路由器。如果您希望 命令影响所有虚拟路由器，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则 命令适用于全局 VRF 虚拟路由器。

Command History

版本	修改
6.1	引入了此命令。
6.6	添加了 ［**vrf** *name*	**all**］ 关键字。

示例

以下是 **show bgp community** 命令的输出示例。有关输出的说明，请参阅 **show bgp** 命令。

```
> show bgp community 111:12345
BGP table version is 10, local router ID is 224.0.0.10
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf Weight Path
*> 172.16.2.2/32    10.43.222.2           0             0 222 ?
*> 10.0.0.0         10.43.222.2           0             0 222 ?
*> 10.43.0.0        10.43.222.2           0             0 222 ?
*> 10.43.44.44/32   10.43.222.2           0             0 222 ?
*  10.43.222.0/24   10.43.222.2           0             0 222 i
*> 172.17.240.0/21  10.43.222.2           0             0 222 ?
*> 192.168.212.0    10.43.222.2           0             0 222 i
*> 172.31.1.0       10.43.222.2           0             0 222 ?
```

show bgp community-list

要显示边界网关协议 (BGP) 社区列表允许的路由，请使用 **show bgp community-list** 命令。

show bgp community-list [**vrf** *name* | **all**] {*community-list-number* | *community-list-name* [**exact-match**]}

Syntax Description

community-list-number	标准或扩展的社区列表编号，范围为从 1 到 500。
community-list-name	社区列表名称。社区列表名称可以是标准名称或扩展的名称。
exact-match	（可选）仅显示具有完全匹配项的路由。
[**vrf** *name* | **all**]	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将该命令限制为特定虚拟路由器。如果您希望 命令影响所有虚拟路由器，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则 命令适用于全局 VRF 虚拟路由器。

Command History

版本	修改
6.1	引入了此命令。
6.6	添加了 [**vrf** *name* | **all**] 关键字。

示例

以下是 **show bgp community-list**的输出示例：有关输出的说明，请参阅 **show bgp** 命令。

```
> show bgp community-list 20
BGP table version is 716977, local router ID is 192.168.32.1
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

  Network          Next Hop          Metric LocPrf Weight Path
* i10.3.0.0         10.0.22.1              0    100      0 1800 1239 ?
*>i                 10.0.16.1              0    100      0 1800 1239 ?
* i10.6.0.0         10.0.22.1              0    100      0 1800 690 568 ?
*>i                 10.0.16.1              0    100      0 1800 690 568 ?
* i10.7.0.0         10.0.22.1              0    100      0 1800 701 35 ?
*>i                 10.0.16.1              0    100      0 1800 701 35 ?
*                   10.92.72.24                         0 1878 704 701 35 ?
* i10.8.0.0         10.0.22.1              0    100      0 1800 690 560 ?
*>i                 10.0.16.1              0    100      0 1800 690 560 ?
*                   10.92.72.24                         0 1878 704 701 560 ?
* i10.13.0.0        10.0.22.1              0    100      0 1800 690 200 ?
*>i                 10.0.16.1              0    100      0 1800 690 200 ?
*                   10.92.72.24                         0 1878 704 701 200 ?
* i10.15.0.0        10.0.22.1              0    100      0 1800 174 ?
*>i                 10.0.16.1              0    100      0 1800 174 ?
* i10.16.0.0        10.0.22.1              0    100      0 1800 701 i
*>i                 10.0.16.1              0    100      0 1800 701 i
```

```
*                  10.92.72.24                        0 1878 704 701 i
```

show bgp filter-list

要显示与指定的过滤器列表相符的路由，请使用 **show bgp filter-list** 命令。

show bgp filter-list ［**vrf** *name* | **all**］ *access-list-name*

Syntax Description

access-list-name	自主系统路径访问列表的名称。有效值范围为 1 至 500。
［**vrf** *name*	**all**］	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将该命令限制为特定虚拟路由器。如果您希望 命令影响所有虚拟路由器，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则 命令适用于全局 VRF 虚拟路由器。

Command History

版本	修改
6.1	引入了此命令。
6.6	添加了 ［**vrf** *name*	**all**］ 关键字。

示例

以下是 **show bgp filter-list** 命令的输出示例。有关输出的说明，请参阅 **show bgp** 命令。

```
> show bgp filter-list filter-list-acl
BGP table version is 1738, local router ID is 172.16.72.24
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf Weight Path
*  172.16.0.0       172.16.72.30                           0 109 108 ?
*  172.16.1.0       172.16.72.30                           0 109 108 ?
*  172.16.11.0      172.16.72.30                           0 109 108 ?
*  172.16.14.0      172.16.72.30                           0 109 108 ?
*  172.16.15.0      172.16.72.30                           0 109 108 ?
*  172.16.16.0      172.16.72.30                           0 109 108 ?
*  172.16.17.0      172.16.72.30                           0 109 108 ?
*  172.16.18.0      172.16.72.30                           0 109 108 ?
*  172.16.19.0      172.16.72.30                           0 109 108 ?
*  172.16.24.0      172.16.72.30                           0 109 108 ?
*  172.16.29.0      172.16.72.30                           0 109 108 ?
*  172.16.30.0      172.16.72.30                           0 109 108 ?
*  172.16.33.0      172.16.72.30                           0 109 108 ?
*  172.16.35.0      172.16.72.30                           0 109 108 ?
*  172.16.36.0      172.16.72.30                           0 109 108 ?
*  172.16.37.0      172.16.72.30                           0 109 108 ?
*  172.16.38.0      172.16.72.30                           0 109 108 ?
*  172.16.39.0      172.16.72.30                           0 109 108 ?
```

show bgp injected-paths

要显示边界网关协议 (BGP) 路由表中的所有注入路径，请使用 **show bgp injected-paths** 命令。

show bgp injected-paths ［**vrf** *name* | **all**］

Syntax Description

［**vrf** *name*	**all**］	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将该命令限制为特定虚拟路由器。如果您希望 命令影响所有虚拟路由器，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则 命令适用于全局 VRF 虚拟路由器。

Command History

版本	修改
6.1	引入了此命令。
6.6	添加了 ［**vrf** *name*	**all**］ 关键字。

示例

以下是 **show bgp injected-paths** 命令的输出示例。有关输出的说明，请参阅 **show bgp** 命令。

```
> show bgp injected-paths
BGP table version is 11, local router ID is 10.0.0.1
Status codes:s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes:i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 172.16.0.0       10.0.0.2                             0 ?
*> 172.17.0.0/16    10.0.0.2                             0 ?
```

show bgp ipv4 unicast

要显示 IP 版本 4 (IPv4) 边界网关协议 (BGP) 路由表中的条目，请使用 **show bgp ipv4 unicast** 命令。

show bgp ipv4 unicast ［**vrf** *name* | **all**］ ［**cidr-only**］

Syntax Description

unicast	指定 IPv4 单播地址前缀。
cidr-only	（可选）显示具有非自然网络掩码的路由。
［**vrf** *name*	**all**］	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将该命令限制为特定虚拟路由器。如果您希望 命令影响所有虚拟路由器，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则 命令适用于全局 VRF 虚拟路由器。

Command History

版本	修改
6.1	引入了此命令。
6.6	添加了 ［**vrf** *name*	**all**］ 关键字。

示例

以下是 **show bgp ipv4 unicast** 命令的输出示例：。有关输出的说明，请参阅 **show bgp** 命令。

```
> show bgp ipv4 unicast
 BGP table version is 4, local router ID is 10.0.40.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.10.10.0/24   172.16.10.1              0             0  300 i
*> 10.10.20.0/24   172.16.10.1              0             0  300 i
*  10.20.10.0/24   172.16.10.1              0             0  300 i
```

show bgp ipv6 unicast

要显示 IPv6 边界网关协议 (BGP) 路由表中的条目，请使用 **show bgp ipv6** 命令。

show bgp ipv6 unicast ［**vrf** *name* | **all**］ ［*ipv6-prefix/prefix-length*］［**longer-prefixes**］［**labels**］

Syntax Description

unicast	指定 IPv6 单播地址前缀。
ipv6-prefix	（可选）IPv6 网络号，输入该网络号以显示 IPv6 BGP 路由表中的特定网络。 此参数必须采用 RFC 2373 中记录的形式，其中地址是用冒号分隔的十六进制 16 位值。
/prefix-length	（可选）IPv6 前缀的长度。是一个十进制值，表示构成前缀（地址的网络部分）的地址高位的连续位数。十进制值前面必须有斜线标记。
longer-prefixes	（可选）显示路由和更具体的路由。
labels	（可选）显示每个地址系列应用于此邻居的策略。
［**vrf** *name*	**all**］	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将该命令限制为特定虚拟路由器。如果您希望 命令影响所有虚拟路由器，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则 命令适用于全局 VRF 虚拟路由器。

Command History

版本	修改
6.1	引入了此命令。
6.6	添加了 ［**vrf** *name*	**all**］ 关键字。

示例

以下是 **show bgp ipv6 unicast** 命令的输出示例，其中显示前缀 3FFE:500::/24 的信息：有关输出的说明，请参阅 **show bgp** 命令。

```
> show bgp ipv6 unicast 3FFE:500::/24
BGP routing table entry for 3FFE:500::/24, version 19421
Paths: (6 available, best #1)
  293 3425 2500
    3FFE:700:20:1::11 from 3FFE:700:20:1::11 (192.168.2.27)
      Origin IGP, localpref 100, valid, external, best
  4554 293 3425 2500
    3FFE:C00:E:4::2 from 3FFE:C00:E:4::2 (192.168.1.1)
      Origin IGP, metric 1, localpref 100, valid, external
  33 293 3425 2500
    3FFE:C00:E:5::2 from 3FFE:C00:E:5::2 (209.165.18.254)
      Origin IGP, localpref 100, valid, external
```

```
  6175 7580 2500
    3FFE:C00:E:1::2 from 3FFE:C00:E:1::2 (209.165.223.204)
      Origin IGP, localpref 100, valid, external
1849 4697 2500, (suppressed due to dampening)
    3FFE:1100:0:CC00::1 from 3FFE:1100:0:CC00::1 (172.31.38.102)
      Origin IGP, localpref 100, valid, external
237 10566 4697 2500
    3FFE:C00:E:B::2 from 3FFE:C00:E:B::2 (172.31.0.3)
      Origin IGP, localpref 100, valid, external
> show bgp ipv6 unicast
BGP table version is 28, local router ID is 172.10.10.1
Status codes:s suppressed, h history, * valid, > best, i -
internal,
              r RIB-failure, S Stale
Origin codes:i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*>i4004::/64        ::FFFF:172.11.11.1
                                             0    100      0 ?
* i                 ::FFFF:172.30.30.1
                                             0    100      0 ?
```

show bgp ipv4/ipv6 unicast community

要显示 IPv4 或 IPv6 边界网关协议 (BGP) 路由表中的条目，请分别使用 **show bgp ipv4 unicast community** 或 **show bgp ipv6 unicast community** 命令。

show bgp ［**vrf** *name* ｜ **all**］ ｛**ipv4** ｜ **ipv6**｝ **unicast community** ［*community-number*］ ［**exact-match**］ ［**local-as** ｜ **no-advertise** ｜ **no-export**］

Syntax Description

unicast	指定 IPv4 或 IPv6 单播地址前缀。
community-number	（可选）有效值为一个从 1 到 4294967295 或 AA:NN 的范围内的社区编号（自主系统：社区编号，即一个 2 字节数字）。
exact-match	（可选）仅显示具有完全匹配项的路由。
local-as	（可选）仅显示未在本地自主系统（已知社区）的外部发送的路由。
no-advertise	（可选）仅显示不向任何对等设备（已知社区）通告的路由。
no-export	（可选）仅显示未在本地自主系统（已知社区）的外部导出的路由。
［**vrf** *name* ｜ **all**］	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将该命令限制为特定虚拟路由器。如果您希望 命令影响所有虚拟路由器，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则 命令适用于全局 VRF 虚拟路由器。

Command History

版本	修改
6.1	引入了此命令。
6.6	添加了 ［**vrf** *name* ｜ **all**］ 关键字。

示例

以下是 **show bgp ipv6 unicast community** 命令的输出示例。有关输出的说明，请参阅 **show bgp** 命令。

```
BGP table version is 69, local router ID is 10.2.64.5
Status codes:s suppressed, h history, * valid, > best, i - internal
Origin codes:i - IGP, e - EGP, ? - incomplete
      Network              Next Hop              Metric LocPrf Weight Path
*> 2001:0DB8:0:1::1/64      ::                                   0 32768 i
*> 2001:0DB8:0:1:1::/80     ::                                   0 32768 ?
*> 2001:0DB8:0:2::/64       2001:0DB8:0:3::2                        0 2 i
*> 2001:0DB8:0:2:1::/80     2001:0DB8:0:3::2                        0 2 ?
* 2001:0DB8:0:3::1/64       2001:0DB8:0:3::2                        0 2 ?
*>                      ::                                  0 32768 ?
*> 2001:0DB8:0:4::/64       2001:0DB8:0:3::2                        0 2 ?
*> 2001:0DB8:0:5::1/64      ::                                   0 32768 ?
```

```
*> 2001:0DB8:0:6::/64       2000:0:0:3::2                  0 2 3 i
*> 2010::/64                ::                             0 32768 ?
*> 2020::/64                ::                             0 32768 ?
*> 2030::/64                ::                             0 32768 ?
*> 2040::/64                ::                             0 32768 ?
*> 2050::/64                ::                             0 32768 ?
```

show bgp ipv4/ipv6 unicast community-list

要显示 IPv4 或 IPv6 边界网关协议 (BGP) 社区列表允许的路由，请分别使用 **show bgp ipv4 unicast community-list** 或 **show bgp ipv6 unicast community-list** 命令。

show bgp ［**vrf** *name* | **all**］ ｛**ipv4** | **ipv6**｝ **unicast community-list** ｛*number* | *name*｝ ［**exact-match**］

Syntax Description

unicast	指定 IPv4 或 IPv6 单播地址前缀。
number	社区列表编号，范围为从 1 到 199。
name	社区列表名称。
exact-match	（可选）仅显示具有完全匹配项的路由。
［**vrf** *name*	**all**］	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将该命令限制为特定虚拟路由器。如果您希望 命令影响所有虚拟路由器，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则 命令适用于全局 VRF 虚拟路由器。

Command History

版本	修改
6.1	引入了此命令。
6.6	添加了 ［**vrf** *name*	**all**］ 关键字。

示例

以下是社区列表编号 3 的 **show bgp ipv6 unicast community-list** 命令输出示例。有关输出的说明，请参阅 **show bgp** 命令。

```
> show bgp ipv6 unicast community-list 3
BGP table version is 14, local router ID is 10.2.64.6
Status codes:s suppressed, h history, * valid, > best, i - internal
Origin codes:i - IGP, e - EGP, ? - incomplete

    Network                Next Hop            Metric LocPrf Weight Path
*> 2001:0DB8:0:1::/64     2001:0DB8:0:3::1                         0 1 i
*> 2001:0DB8:0:1:1::/80   2001:0DB8:0:3::1                         0 1 i
*> 2001:0DB8:0:2::1/64    ::                                     0 32768 i
*> 2001:0DB8:0:2:1::/80   ::                                     0 32768 ?
* 2001:0DB8:0:3::2/64     2001:0DB8:0:3::1                         0 1 ?
*>                       ::                                   0 32768 ?
*> 2001:0DB8:0:4::2/64    ::                                     0 32768 ?
*> 2001:0DB8:0:5::/64     2001:0DB8:0:3::1                         0 1 ?
*> 2010::/64              2001:0DB8:0:3::1                         0 1 ?
*> 2020::/64              2001:0DB8:0:3::1                         0 1 ?
*> 2030::/64              2001:0DB8:0:3::1                         0 1 ?
```

```
*> 2040::/64                2001:0DB8:0:3::1                        0 1 ?
*> 2050::/64                2001:0DB8:0:3::1                        0 1 ?
```

show bgp ipv4/ ipv6 unicast neighbors

要显示到邻居的 IPv4 或 IPv6 边界网关协议 (BGP) 连接的相关信息，请使用 **show bgp ipv4 unicast neighbors** 或 **show bgp ipv6 neighbors** 命令。

show bgp ［**vrf** *name* | **all**］ ｛**ipv4** | **ipv6**｝ **unicast neighbors** ［*ip-address*］［**received-routes** | **routes** | **advertised-routes** | **paths** *regular-expression*］

Syntax Description

unicast	指定 IPv4 或 IPv6 单播地址前缀。
ip-address	（可选）IPv4 或 IPv6 BGP 发言邻居的地址。如果省略此参数，则显示所有 IPv4 或 IPv6 邻居。 IPv6 前缀必须采用 RFC 2373 规定的格式，其中地址以十六进制的 16 位值指定，各个值之间用冒号分隔。
received-routes	（可选）显示从指定邻居收到的所有路由（接受和拒绝的路由）。
routes	（可选）显示收到并接受的所有路由。这是 received-routes 关键字的输出的子集。
advertised-routes	（可选）显示向邻居通告的网络设备的所有路由。
paths *regular-expression*	（可选）用于与收到的路径匹配的正则表达式。
［**vrf** *name*	**all**］	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将该命令限制为特定虚拟路由器。如果您希望 命令影响所有虚拟路由器，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则 命令适用于全局 VRF 虚拟路由器。

Command History

版本	修改
6.1	引入了此命令。
6.6	添加了 ［**vrf** *name*	**all**］ 关键字。

示例

以下是 **show bgp ipv6 unicast neighbors** 命令的输出示例。

```
> show bgp ipv6 unicast neighbors
BGP neighbor is 3FFE:700:20:1::11,  remote AS 65003, external link
  BGP version 4, remote router ID 192.168.2.27
  BGP state = Established, up for 13:40:17
  Last read 00:00:09, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received
    Address family IPv6 Unicast: advertised and received
```

```
  Received 31306 messages, 20 notifications, 0 in queue
  Sent 14298 messages, 1 notifications, 0 in queue
  Default minimum time between advertisement runs is 30 seconds
 For address family: IPv6 Unicast
  BGP table version 21880, neighbor version 21880
  Index 1, Offset 0, Mask 0x2
  Route refresh request: received 0, sent 0
  Community attribute sent to this neighbor
  Outbound path policy configured
  Incoming update prefix filter list is bgp-in
  Outgoing update prefix filter list is aggregate
  Route map for outgoing advertisements is uni-out
  77 accepted prefixes consume 4928 bytes
  Prefix advertised 4303, suppressed 0, withdrawn 1328
  Number of NLRIs in the update sent: max 1, min 0
  1 history paths consume 64 bytes
  Connections established 22; dropped 21
  Last reset 13:47:05, due to BGP Notification sent, hold time expired
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Local host: 3FFE:700:20:1::12, Local port: 55345
Foreign host: 3FFE:700:20:1::11, Foreign port: 179
Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)
Event Timers (current time is 0x1A0D543C):
Timer          Starts    Wakeups            Next
Retrans          1218          5             0x0
TimeWait            0          0             0x0
AckHold          3327       3051             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0
iss: 1805423033  snduna: 1805489354  sndnxt: 1805489354     sndwnd:  15531
irs:  821333727  rcvnxt:  821591465  rcvwnd:      15547  delrcvwnd:    837
SRTT: 300 ms, RTTO: 303 ms, RTV: 3 ms, KRTT: 0 ms
minRTT: 8 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: higher precedence, nagle
Datagrams (max data segment is 1420 bytes):
Rcvd: 4252 (out of order: 0), with data: 3328, total data bytes: 257737
Sent: 4445 (retransmit: 5), with data: 4445, total data bytes: 244128
```

下表描述屏幕上展示的重要字段。

表 *5: show bgp ipv4/ipv6 unicast neighbor* 字段

字段	Description
BGP neighbor	BGP邻居IP地址及其自主系统编号。如果邻居位于与路由器相同的自主系统中，则它们之间的链路是内部链路；否则，将该链路视为外部链路。
remote AS	邻居的自主系统。
internal link	表示此对等设备为内部边界网关协议 (iBGP) 对等设备。
BGP version	正在用于与远程路由器通信的BGP版本；还指定邻居的路由器ID（IP地址）。
remote router ID	一个 32 位数字，写为以句点分隔的 4 八位组（点分十进制格式）。

字段	Description
BGP state	此 BGP 连接的内部状态。
up for	基本 TCP 连接已存在的时间量。
Last read	BGP 最后从此邻居读取消息的时间。
hold time	对等设备的消息之间可消耗的最大时间量。
keepalive interval	发送保持连接数据包之间的时间段，这有助于确保 TCP 连接正常运行。
Neighbor capabilities	从此邻居通告并收到的 BGP 功能。
Route refresh	表示邻居使用路由刷新功能支持动态软重置。
Address family IPv6 Unicast	表示 BGP 对等设备正在交换 IPv6 连通性信息。
Received	从此对等设备收到的 BGP 消息（包括保持连接消息）的总数。
notifications	从对等设备收到的错误消息的数量。
Sent	已发送给此对等设备的 BGP 消息（包括保持连接消息）的总数。
notifications	路由器已发送给此对等设备的错误消息的数量。
advertisement runs	最小通告间隔的值。
For address family	以下字段引用的地址系列。
BGP table version	表的内部版本号。每当表更改时，此数字就会增加。
neighbor version	编号，软件使用它跟踪已发送和必须发送给此邻居的前缀。
Route refresh request	从此邻居发送和收到的路由刷新请求的数量。
Community attribute (not shown in sample output)	如果为此邻居配置邻居 send-community 命令，则出现该字段。
Inbound path policy (not shown in sample output)	表示是配置入站过滤器列表，还是配置路由地图。
Outbound path policy (not shown in sample output)	表示是配置出站过滤器列表、路由地图，还是配置未抑制映射。
bgp-in (not shown in sample output)	用于 IPv6 单播地址系列的入站更新前缀过滤器列表的名称。
aggregate (not shown in sample output)	用于 IPv6 单播地址系列的出站更新前缀过滤器列表的名称。

字段	Description
uni-out (not shown in sample output)	用于 IPv6 单播地址系列的出站路由地图的名称。
accepted prefixes	接受的前缀的数量。
Prefix advertised	通告的前缀的数量。
suppressed	抑制的前缀的数量
withdrawn	撤消的前缀的数量。
history paths (not shown in sample output)	保存以记录历史的路径条目的数量。
Connections established	路由器已建立TCP连接的次数，且两个对等设备已同意彼此使用BGP发言。
dropped	正常的连接失败或被关闭的次数。
Last reset	最后重置此对等会话后的已用时间（采用小时：分钟：秒钟格式）。
Connection state	BGP 对等设备的状态
unread input bytes	仍然要处理的数据包的字节数。
Local host, Local port	本地路由器的对等地址和端口。
Foreign host, Foreign port	邻居的对等地址。
Event Timers	显示每个计时器的启动和唤醒数量的表。
snduna	最后发送本地主机发送但未收到确认的序列号。
sndnxt	本地主机接下来将发送的序列号。
sndwnd	远程主机的 TCP 窗口大小。
irs	最初接收序列号。
rcvnxt	最后接收本地主机已确认的序列号。
rcvwnd	本地主机的 TCP 窗口大小。
delrecvwnd	延迟的接收窗口 - 本地主机从连接中读取，但未从主机向远程主机通告的接收窗口中减去的数据。此字段中的值逐渐增加，直到它大于全尺寸数据包为止，届时将该值应用于 rcvwnd 字段。
SRTT	计算的平滑的往返超时（以毫秒为单位）。
RTTO	往返超时（以毫秒为单位）。

字段	Description
RTV	往返时间的差量（以毫秒为单位）。
KRTT	新的往返超时（以毫秒为单位），使用Karn算法。此字段分别跟踪重新发送的数据包的往返时间。
minRTT	记录的最小往返超时（以毫秒为单位），具有用于计算的硬接线值。
maxRTT	记录的最大往返超时（以毫秒为单位）。
ACK hold	本地主机将延迟确认以在其上“背载”数据的时间（以毫秒为单位）。
Flags	BGP 数据包的 IP 优先级。
Datagrams: Rcvd	从邻居收到的更新数据包的数量。
with data	与数据一起收到的更新数据包的数量。
total data bytes	数据的总字节数。
Sent	发送的更新数据包的数量。
with data	具有发送的数据的更新数据包的数量。
total data bytes	数据的总字节数。

以下是使用 **advertised-routes** 关键字的 **show bgp ipv6 unicast neighbors** 命令的输出示例：
有关输出的说明，请参阅 **show bgp** 命令。

```
> show bgp ipv6 unicast neighbors 3FFE:700:20:1::11 advertised-routes
BGP table version is 21880, local router ID is 192.168.7.225
Status codes: s suppressed, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 2001:200::/35    3FFE:700:20:1::11                       0 293 3425 2500 i
*> 2001:208::/35    3FFE:C00:E:B::2                         0 237 7610 i
*> 2001:218::/35    3FFE:C00:E:C::2                         0 3748 4697 i
```

以下是使用 **routes** 关键字的 **show bgp ipv6 unicast neighbors** 命令的输出示例：

```
> show bgp ipv6 unicast neighbors 3FFE:700:20:1::11 routes
BGP table version is 21885, local router ID is 192.168.7.225
Status codes: s suppressed, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 2001:200::/35    3FFE:700:20:1::11                       0 293 3425 2500 i
*  2001:208::/35    3FFE:700:20:1::11                       0 293 7610 i
*  2001:218::/35    3FFE:700:20:1::11                       0 293 3425 4697 i
*  2001:230::/35    3FFE:700:20:1::11                       0 293 1275 3748 i
```

以下是使用 **paths** 关键字的 **show bgp ipv6 neighbors** 命令的输出示例：

```
> show bgp ipv6 unicast neighbors 3FFE:700:20:1::11 paths ^293
Address    Refcount Metric Path
0x6131D7DC        2      0 293 3425 2500 i
0x6132861C        2      0 293 7610 i
0x6131AD18        2      0 293 3425 4697 i
0x61324084        2      0 293 1275 3748 i
0x61320E0C        1      0 293 3425 2500 2497 i
0x61326928        1      0 293 3425 2513 i
0x61327BC0        2      0 293 i
0x61321758        1      0 293 145 i
0x61320BEC        1      0 293 3425 6509 i
0x6131AAF8        2      0 293 1849 2914 ?
0x61320FE8        1      0 293 1849 1273 209 i
0x613260A8        2      0 293 1849 i
0x6132586C        1      0 293 1849 5539 i
0x6131BBF8        2      0 293 1849 1103 i
0x6132344C        1      0 293 4554 1103 1849 1752 i
0x61324150        2      0 293 1275 559 i
0x6131E5AC        2      0 293 1849 786 i
0x613235E4        1      0 293 1849 1273 i
0x6131D028        1      0 293 4554 5539 8627 i
0x613279E4        1      0 293 1275 3748 4697 3257 i
0x61320328        1      0 293 1849 1273 790 i
0x6131EC0C        2      0 293 1275 5409 i
```

下表描述屏幕上展示的重要字段。

表 *6: show bgp ipv6 neighbors paths* 字段

字段	Description
Address	存储路径的内部地址。
Refcount	使用该路径的路由的数量。
Metric	路径的多出口标识符 (MED) 指标。（用于 BGP 版本 2 和 3 的此指标名称是 INTER_AS。）
Path	该路由的自主系统路径，其后是该路由的源代码。

show bgp ipv6 neighbors 命令的以下输出示例显示了 IPv6 地址 2000:0:0:4::2 的 **received routes** **：**

```
> show bgp ipv6 unicast neighbors 2000:0:0:4::2 received-routes
BGP table version is 2443, local router ID is 192.168.0.2
Status codes:s suppressed, h history, * valid, > best, i - internal
Origin codes:i - IGP, e - EGP, ? - incomplete

   Network               Next Hop           Metric LocPrf Weight Path
*> 2000:0:0:1::/64      2000:0:0:4::2                          0 2 1 i
*> 2000:0:0:2::/64      2000:0:0:4::2                          0 2 i
*> 2000:0:0:2:1::/80    2000:0:0:4::2                          0 2 ?
*> 2000:0:0:3::/64      2000:0:0:4::2                          0 2 ?
*  2000:0:0:4::1/64     2000:0:0:4::2                          0 2 ?
```

show bgp ipv4/ ipv6 unicast paths

要显示数据库中的所有 IPv4 或 IPv6 边界网关协议 (BGP) 路径，请分别使用 **show bgp ipv4 unicast paths** 或 **show bgp ipv6 unicast paths** 命令。

show bgp ［**vrf** *name* | **all**］ ｛**ipv4** | **ipv6**｝ **unicast paths** ［*regular-expression*］

Syntax Description

regular-expression	（可选）用于与收到的路径匹配的正则表达式。
［**vrf** *name*	**all**］	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将该命令限制为特定虚拟路由器。如果您希望 命令影响所有虚拟路由器，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则 命令适用于全局 VRF 虚拟路由器。

Command History

版本	修改
6.1	引入了此命令。
6.6	添加了 ［**vrf** *name*	**all**］ 关键字。

示例

以下是 **show bgp ipv6 unicast paths** 命令的输出示例：

```
> show bgp ipv6 unicast paths
Address    Hash Refcount Metric Path
0x61322A78    0        2      0 i
0x6131C214    3        2      0 6346 8664 786 i
0x6131D600   13        1      0 3748 1275 8319 1273 209 i
0x613229F0   17        1      0 3748 1275 8319 12853 i
0x61324AE0   18        1      1 4554 3748 4697 5408 i
0x61326818   32        1      1 4554 5609 i
0x61324728   34        1      0 6346 8664 9009 ?
0x61323804   35        1      0 3748 1275 8319 i
0x61327918   35        1      0 237 2839 8664 ?
0x61320504   38        2      0 3748 4697 1752 i
0x61320988   41        2      0 1849 786 i
0x6132245C   46        1      0 6346 8664 4927 i
```

下表描述屏幕上展示的重要字段。

表 *7:* 显示 ***bgp ipv4/ipv6*** 单播路径字段

字段	Description
Address	存储路径的内部地址。
Refcount	使用该路径的路由的数量。

字段	Description
Metric	路径的多出口标识符 (MED) 指标。（用于 BGP 版本 2 和 3 的此指标名称是 INTER_AS。）
Path	该路由的自主系统路径，其后是该路由的源代码。

show bgp ipv4/ ipv6 unicast prefix-list

要显示与前缀列表匹配的路由，请使用 **show bgp ipv4 prefix-list** 或 **show bgp ipv6 prefix-list** 命令。

show bgp ［**vrf** *name* | **all**］ {**ipv4** | **ipv6**} **unicast prefix-list** *name*

Syntax Description

prefix-list *name*	指定的前缀列表。
［**vrf** *name*	**all**］	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将该命令限制为特定虚拟路由器。如果您希望 命令影响所有虚拟路由器，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则 命令适用于全局 VRF 虚拟路由器。

Command History

版本	修改
6.1	引入了此命令。
6.6	添加了 ［**vrf** *name*	**all**］ 关键字。

示例

以下是 **show bgp ipv6 prefix-list** 命令的输出示例：

```
> show bgp ipv6 unicast prefix-list pin
ipv6 prefix-list pin:
   count:4, range entries:3, sequences:5 - 20, refcount:2
   seq 5 permit 747::/16 (hit count:1, refcount:2)
   seq 10 permit 747:1::/32 ge 64 le 64 (hit count:2, refcount:2)
   seq 15 permit 747::/32 ge 33 (hit count:1, refcount:1)
   seq 20 permit 777::/16 le 124 (hit count:2, refcount:1)
The ipv6 prefix-list match the following prefixes:
   seq 5: matches the exact match 747::/16
   seq 10:first 32 bits in prefix must match with a prefixlen of /64
   seq 15:first 32 bits in prefix must match with any prefixlen up to /128
   seq 20:first 16 bits in prefix must match with any prefixlen up to /124
```

show bgp ipv4/ ipv6 unicast regexp

要显示与自治系统路径正则表达式相匹配的 IPv4 或 IPv6 边界网关协议 (BGP) 路由，请使用 **show bgp ipv4 regexp** 或 **show bgp ipv6 regexp** 命令。

show bgp ［**vrf** *name* | **all**］ ｛**ipv4** | **ipv6**｝ **unicast regexp** *regular-expression*

Syntax Description

regexp *regular-expression*	用于与 BGP 自主系统路径匹配的正则表达式。
［**vrf** *name*	**all**］	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将该命令限制为特定虚拟路由器。如果您希望 命令影响所有虚拟路由器，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则 命令适用于全局 VRF 虚拟路由器。

Command History

版本	修改
6.1	引入了此命令。
6.6	添加了 ［**vrf** *name*	**all**］ 关键字。

示例

以下是展示从 33 开始或包含 293 的路径的 **show bgp ipv6 unicast regexp** 命令的输出示例：有关输出的说明，请参阅 **show bgp** 命令。

```
> show bgp ipv6 unicast regexp ^33|293
BGP table version is 69964, local router ID is 192.168.7.225
Status codes: s suppressed, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*  2001:200::/35    3FFE:C00:E:4::2          1             0 4554 293 3425 2500 i
*                   2001:0DB8:0:F004::1                    0 3320 293 3425 2500 i
*  2001:208::/35    3FFE:C00:E:4::2          1             0 4554 293 7610 i
*  2001:228::/35    3FFE:C00:E:F::2                        0 6389 1849 293 2713 i
*  3FFE::/24        3FFE:C00:E:5::2                        0 33 1849 4554 i
*  3FFE:100::/24    3FFE:C00:E:5::2                        0 33 1849 3263 i
*  3FFE:300::/24    3FFE:C00:E:5::2                        0 33 293 1275 1717 i
*                   3FFE:C00:E:F::2                        0 6389 1849 293 1275
```

show bgp ipv4/ ipv6 unicast route-map

要显示无法安装在路由表中的 IPv4 或 IPv6 边界网关协议 (BGP) 路由，请使用 **show bgp ipv4 unicast route-map** 或 **show bgp ipv6 unicast route-map** 命令。

show bgp ［**vrf** *name* | **all**］ ｛**ipv4** | **ipv6**｝ **unicast route-map** *name*

Syntax Description

route-map *name*	要匹配的指定路由地图。
［**vrf** *name*	**all**］	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将该命令限制为特定虚拟路由器。如果您希望 命令影响所有虚拟路由器，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则 命令适用于全局 VRF 虚拟路由器。

Command History

版本	修改
6.1	引入了此命令。
6.6	添加了 ［**vrf** *name*	**all**］ 关键字。

示例

以下是名为 rmap 的路由地图的 **show bgp ipv6 unicast route-map** 命令的输出示例：。有关输出的说明，请参阅 **show bgp** 命令。

```
> show bgp ipv6 unicast route-map rmap
BGP table version is 16, local router ID is 172.30.242.1
Status codes:s suppressed, h history, * valid, > best, i - internal,
             r RIB-failure, S Stale
Origin codes:i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*>i12:12::/64       2001:0DB8:101::1             0    100     50 ?
*>i12:13::/64       2001:0DB8:101::1             0    100     50 ?
*>i12:14::/64       2001:0DB8:101::1             0    100     50 ?
*>i543::/64         2001:0DB8:101::1             0    100     50 ?
```

show bgp ipv4/ ipv6 unicast summary

要显示所有 IPv4 或 IPv6 边界网关协议 (BGP) 连接的状态，请分别使用 s **how bgp ipv4 unicast summary** 或 **show bgp ipv6 unicast summary** 命令。

show bgp ［**vrf** *name* | **all**］ ｛**ipv4** | **ipv6**｝ **unicast summary**

Syntax Description

［**vrf** *name*	**all**］	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将该命令限制为特定虚拟路由器。如果您希望 命令影响所有虚拟路由器，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则 命令适用于全局 VRF 虚拟路由器。

Command History

版本	修改
6.1	引入了此命令。
6.6	添加了 ［**vrf** *name*	**all**］ 关键字。

示例

以下是 **show bgp ipv6 unicast summary** 命令的输出示例：

```
> show bgp ipv6 unicast summary
BGP device identifier 172.30.4.4, local AS number 200
BGP table version is 1, main routing table version 1
Neighbor           V    AS  MsgRcvd  MsgSent   TblVer  InQ  OutQ  Up/Down   State/PfxRcd
2001:0DB8:101::2   4    200    6869     6882        0    0     0  06:25:24  Active
```

下表描述屏幕上展示的重要字段。

表 8: show bgp ipv4/ipv6 unicast summary fields

字段	Description
BGP device identifier	网络设备的 IP 地址。
BGP table version	表的内部版本号。每当表更改时，此数字就会增加。
main routing table version	注入主路由表中的 BGP 数据库的上一版本。
Neighbor	邻居的 IPv6 地址。
V	向该邻居传达的 BGP 版本号。
AS	自治系统
MsgRcvd	从该邻居收到的 BGP 消息。

字段	Description
MsgSent	发送给该邻居的 BGP 消息。
TblVer	发送给邻居的 BGP 数据库的上一版本。
InQ	来自该等待处理的邻居的消息的数量。
OutQ	等待发送给该邻居的消息的数量。
Up/Down	BGP 会话处于“已建立”状态或当前状态（如果它不处于“已建立”状态）的时间长度。
State/PfxRcd	BGP 会话的当前状态/设备已从邻居收到的前缀的数量。达到（如 neighbor maximum-prefix 命令所设置）最大数量时，条目中显示字符串“PfxRcd”，邻居会关闭，且连接处于“空闲”状态。 具有空闲状态的 (Admin) 条目表示使用 neighbor shutdown 命令已关闭连接。

show bgp neighbors

要显示边界网关协议 (BGP) 和到邻居的 TCP 连接的有关信息，可在用户或特权 EXEC 模式下使用 show bgp neighbors 命令。

show bgp neighbors ［**vrf** *name* | **all**］ ［**slow** | *ip-address* ［**advertised-routes** | **paths** ［*reg-exp*］ | **policy** ［**detail**］ | **received prefix-filter** | **received-routes** | **routes**］］

Syntax Description

slow	（可选）显示动态配置的缓慢对等设备的有关信息。
ip-address	（可选）显示有关 IPv4 邻居的信息。如果省略此参数，则显示有关所有邻居的信息。
advertised-routes	（可选）显示已向邻居通告的所有路由。
paths [*reg-exp*]	（可选）显示从指定的邻居获知的自主系统路径。可选正则表达式用于过滤输出。
policy	（可选）显示每个地址系列应用于此邻居的策略。
detail	（可选）显示详细的策略信息，例如路由映射、前缀列表、社区列表、访问控制列表 (ACL) 和自主系统路径过滤器列表。
received prefix-filter	（可选）显示从指定邻居（出站路由过滤器 [ORF]）发送的前缀列表。
received-routes	（可选）显示从指定邻居收到的所有路由（接受和拒绝的路由）。
routes	（可选）显示收到并接受的所有路由。输入此关键字时显示的输出是 **received-routes** 关键字显示的输出的子集。
［**vrf** *name*	**all**］	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将该命令限制为特定虚拟路由器。如果您希望 命令影响所有虚拟路由器，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则 命令适用于全局 VRF 虚拟路由器。

Command Default

此命令的输出展示所有邻居的信息。

Command History

版本	修改
6.1	引入了此命令。
6.6	添加了 ［**vrf** *name*	**all**］ 关键字。

使用指南

使用 **show bgp neighbors** 命令显示邻居会话的 BGP 和 TCP 连接信息。对于 BGP，这包括详细的邻居属性、功能、路径和前缀信息。对于 TCP，这包括与 BGP 邻居会话建立和维护相关的统计信息。

根据通告和撤消的前缀的数量显示前缀活动。策略拒绝显示已通告但随后基于输出中显示的功能或属性忽略的路由的数量。

示例

以下示例展示位于 10.108.50.2 的 BGP 邻居的输出。此邻居是内部 BGP (iBGP) 对等设备。此邻居支持路由刷新和平滑重启功能。

```
> show bgp neighbors 10.108.50.2
BGP neighbor is 10.108.50.2,  remote AS 1, internal link
  BGP version 4, remote router ID 192.168.252.252
  BGP state = Established, up for 00:24:25
  Last read 00:00:24, last write 00:00:24, hold time is 180, keepalive interval is
   60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received(old & new)
    MPLS Label capability: advertised and received
    Graceful Restart Capability: advertised
    Address family IPv4 Unicast: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0
                         Sent       Rcvd
    Opens:                  3          3
    Notifications:          0          0
    Updates:                0          0
    Keepalives:           113        112
    Route Refresh:          0          0
    Total:                116        115
  Default minimum time between advertisement runs is 5 seconds

 For address family: IPv4 Unicast
  BGP additional-paths computation is enabled
  BGP advertise-best-external is enabled
  BGP table version 1, neighbor version 1/0
 Output queue size : 0
  Index 1, Offset 0, Mask 0x2
  1 update-group member
                               Sent       Rcvd
  Prefix activity:             ----       ----
    Prefixes Current:             0          0
    Prefixes Total:               0          0
    Implicit Withdraw:            0          0
    Explicit Withdraw:            0          0
    Used as bestpath:           n/a          0
    Used as multipath:          n/a          0

                                  Outbound    Inbound
  Local Policy Denied Prefixes:   --------    -------
    Total:                               0          0

  Number of NLRIs in the update sent: max 0, min 0

  Connections established 3; dropped 2
  Last reset 00:24:26, due to Peer closed the session
External BGP neighbor may be up to 2 hops away.
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection is ECN Disabled
Local host: 10.108.50.1, Local port: 179
Foreign host: 10.108.50.2, Foreign port: 42698
```

```
Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)

Event Timers (current time is 0x68B944):
Timer          Starts    Wakeups            Next
Retrans            27          0             0x0
TimeWait            0          0             0x0
AckHold            27         18             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0

iss: 3915509457  snduna: 3915510016  sndnxt: 3915510016     sndwnd:  15826
irs:  233567076  rcvnxt:  233567616  rcvwnd:      15845  delrcvwnd:    539

SRTT: 292 ms, RTTO: 359 ms, RTV: 67 ms, KRTT: 0 ms
minRTT: 12 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: passive open, nagle, gen tcbs
IP Precedence value : 6

Datagrams (max data segment is 1460 bytes):
Rcvd: 38 (out of order: 0), with data: 27, total data bytes: 539
Sent: 45 (retransmit: 0, fastretransmit: 0, partialack: 0, Second Congestion: 08
```

下表描述屏幕上展示的重要字段。仅当计数器具有非零值时，才显示星号字符 (*) 后的字段。

表 *9:* 显示 *bgp* 邻居字段

字段	Description
BGP neighbor	BGP 邻居 IP 地址及其自主系统编号。
remote AS	邻居的自主系统编号。
local AS 300 no-prepend (not shown in display)	验证未将本地自主系统编号预置到收到的外部路由。迁移自主系统时，此输出支持隐藏本地自主系统。
internal link	系统会为 iBGP 邻居显示“内部链路”。为外部 BGP (eBGP) 邻居显示“外部链路”。
BGP version	正在用于与远程路由器通信的 BGP 版本。
remote router ID	邻居的 IP 地址。
BGP state	会话协商的有限状态机 (FSM) 阶段。
up for	基本 TCP 连接已存在的时间（采用 hh:mm:ss 格式）。
Last read	BGP 最后收到此邻居的消息后的时间（采用 hh:mm:ss 格式）。
last write	BGP 最后向此邻居发送消息后的时间（采用 hh:mm:ss 格式）。
hold time	BGP 将保持与此邻居的会话（没有收到消息）的时间（以秒为单位）。

字段	Description
keepalive interval	向此邻居传输保持连接消息的时间间隔（以秒为单位）。
Neighbor capabilities	从此邻居通告并收到的 BGP 功能。在两个路由器之间成功交换功能时显示“advertised and received”。
Route Refresh	路由刷新功能的状态。
Graceful Restart Capability	平滑重启功能的状态。
Address family IPv4 Unicast	此邻居的特定于 IP 版本 4 单播的属性。
Message statistics	按消息类型组织的统计信息。
InQ depth	输入队列中的消息的数量。
OutQ depth	输出队列中的消息的数量。
Sent	传输的消息的总数。
Received	收到的消息的总数。
Opens	发送和收到的 OPEN 消息的数量。
notifications	发送和收到的通知（错误）消息的数量。
Updates	发送和收到的更新消息的数量。
Keepalive	发送和收到的保持连接消息的数量。
Route Refresh	发送和收到的路由刷新请求消息的数量。
Total	发送和收到的消息的总数。
Default minimum time between...	通告传输之间的时间（以秒为单位）。
For address family:	以下字段引用的地址系列。
BGP table version	表的内部版本号。每当表更改时，此数字就会增加。
neighbor version	编号，软件使用它跟踪已发送和需要发送的前缀。
update-group	此地址系列的更新组成员的编号。
Prefix activity	此地址系列的前缀统计信息。
Prefixes current	为此地址系列接受的前缀的数量。
Prefixes total	收到的前缀的总数。

字段	Description
Implicit Withdraw	已撤消和重新通告前缀的次数。
Explicit Withdraw	因不再可行而撤消前缀的次数。
Used as bestpath	收到的作为最佳路径安装的前缀的数量。
Used as multipath	收到的作为多个路径安装的前缀的数量。
* Saved (soft-reconfig)	通过支持软重新配置的邻居执行的软重置的数量。仅当计数器具有非零值时，才显示此字段。
* History paths	仅当计数器具有非零值时，才显示此字段。
* Invalid paths	无效路径的数量。仅当计数器具有非零值时，才显示此字段。
Local Policy Denied Prefixes	因本地策略配置而拒绝的前缀。为入站和出站策略拒绝更新计数器。仅当计数器具有非零值时，才显示此标题下的字段。
* route-map	显示入站和出站路由映射策略拒绝。
* filter-list	显示入站和出站过滤器列表策略拒绝。
* prefix-list	显示入站和出站前缀列表策略拒绝。
* AS_PATH too long	显示出站 AS 路径长度策略拒绝。
* AS_PATH loop	显示出站 AS 路径环路策略拒绝。
* AS_PATH confed info	显示出站联盟策略拒绝。
* AS_PATH contains AS 0	显示自主系统 (AS) 0 的出站拒绝。
* NEXT_HOP Martian	显示出站 martian 拒绝。
* NEXT_HOP non-local	显示出站非本地下一跃点拒绝。
* NEXT_HOP is us	显示出站下一跃点自拒绝。
* CLUSTER_LIST loop	显示出站集群列表环路拒绝。
* ORIGINATOR loop	显示本地发起的路由的出站拒绝。
* unsuppress-map	显示因未抑制映射而引起的入站拒绝。
* advertise-map	显示因通告映射而引起的入站拒绝。

字段	Description
* Well-known Community	显示已知社区的入站拒绝。
* SOO loop	显示因源站点而引起的入站拒绝。
* Bestpath from this peer	显示因最佳路径来自本地路由器而引起的入站拒绝。
* Suppressed due to dampening	显示因邻居或链路处于阻尼状态而引起的入站拒绝。
* Bestpath from iBGP peer	部署因最佳路径来自 iBGP 邻居而引起的入站拒绝。
* Incorrect RIB for CE	部署因 CE 路由器的 RIB 错误而引起的入站拒绝。
* BGP distribute-list	显示因分发列表而引起的入站拒绝。
Number of NLRIs...	更新中的网络层可达性属性的数量。
Connections established	已成功建立 TCP 和 BGP 连接的次数。
dropped	有效会话失败或被关闭的次数。
Last reset	最后重置此对等会话后的时间。重置的原因显示在此行上。
External BGP neighbor may be... (not shown in the display)	表示启用 BGP TTL 安全检查。可分离本地和远程对等设备的跃点的最大数量显示在此行上。
Connection state	BGP 对等设备的连接状态。
Connection is ECN Disabled	显式堵塞通知状态（启用或禁用）。
Local host: 10.108.50.1, Local port: 179	本地 BGP 扬声器的 IP 地址。BGP 端口号 179。
Foreign host: 10.108.50.2, Foreign port: 42698	邻居地址和 BGP 目标端口号。
Enqueued packets for retransmit:	排队进行 TCP 重新传输的数据包。
Event Timers	TCP 事件计时器。用于启动和唤醒的计数器（到期的计时器）。
Retrans	已重新传输数据包的次数。
TimeWait	等待重新传输计时器到期的时间。

字段	Description
AckHold	确认保持计时器。
SendWnd	传输（发送）窗口。
keepalive	保持连接数据包的数量。
GiveUp	因不确认而丢弃数据包的次数。
PmtuAger	路径 MTU 发现计时器。
DeadWait	失效段的到期计时器。
iss:	初始数据包传输序列号。
snduna	未确认的最后一个传输序列号。
sndnxt:	要传输的下一个数据包序列号。
sndwnd:	远程邻居的 TCP 窗口大小。
irs:	初始数据包接收序列号。
rcvnxt:	本地确认的最后一个接收序列号。
rcvwnd:	本地主机的 TCP 窗口大小。
delrcvwnd:	延迟的接收窗口 - 本地主机从连接中读取，但未从主机向远程主机通告的接收窗口中减去的数据。此字段中的值逐渐增加，直到它大于全尺寸数据包为止，届时将该值应用于 rcvwnd 字段。
SRTT:	计算的平滑的往返超时。
RTTO:	往返超时。
RTV:	往返时间的差异。
KRTT:	新的往返超时（使用Karn算法）。此字段分别跟踪重新发送的数据包的往返时间。
minRTT:	记录的最小往返超时（用于计算的硬接线值）。
maxRTT:	记录的最大往返超时。
ACK hold:	本地主机将延迟确认以携带（背载）附加数据的时间长度。
IP Precedence value:	BGP 数据包的 IP 优先级。
Datagrams	从邻居收到的更新数据包的数量。
Rcvd:	已接收的数据包数

字段	Description
with data	与数据一起发送的更新数据包的数量。
total data bytes	收到的数据的总量（以字节为单位）。
Sent	发送的更新数据包的数量。
Second Congestion	因堵塞而发送的第二次重新传输的数量。
Datagrams: Rcvd	从邻居收到的更新数据包的数量。
out of order:	在序列外收到的数据包的数量。
with data	与数据一起收到的更新数据包的数量。
Last reset	最后重置此对等会话后消耗的时间。
unread input bytes	仍然要处理的数据包的字节数。
retransmit	重新传输的数据包的数量。
fastretransmit	在重新传输计时器到期前为无序段重新传输的重复确认的数量。
partialack	部分确认的重新传输的数量（在后续确认前或无后续确认时传输）。

以下示例展示仅为 172.16.232.178 邻居通告的路由：有关输出的说明，请参阅 **show bgp** 命令。

```
> show bgp neighbors 172.16.232.178 advertised-routes
BGP table version is 27, local router ID is 172.16.232.181
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
Network          Next Hop          Metric LocPrf Weight Path
*>i10.0.0.0      172.16.232.179         0    100      0 ?
*> 10.20.2.0     10.0.0.0               0         32768 i
```

以下是使用 **paths** 关键字输入的 **show bgp neighbors** 命令的输出示例：

```
> show bgp neighbors 172.29.232.178 paths ^10
Address    Refcount Metric Path
0x60E577B0        2     40 10 ?
```

下表对每个字段进行了说明。

***表 10: show bgp neighbors paths* 字段**

字段	Description
Address	存储路径的内部地址。
Refcount	使用该路径的路由的数量。

字段	Description
Metric	路径的多出口标识符 (MED) 指标。（用于 BGP 版本 2 和 3 的此指标名称是 INTER_AS。）
Path	该路由的自主系统路径，其后是该路由的源代码。

以下示例展示已从 192.168.20.72 邻居收到过滤 10.0.0.0 网络中的所有路由的前缀列表：

```
> show bgp neighbors 192.168.20.72 received prefix-filter
Address family:IPv4 Unicast
ip prefix-list 192.168.20.72:1 entries
   seq 5 deny 10.0.0.0/8 le 32
```

以下输出示例展示应用于位于192.168.1.2的邻居的策略。输出展示邻居设备上配置的策略。

```
> show bgp neighbors 192.168.1.2 policy
Neighbor: 192.168.1.2, Address-Family: IPv4 Unicast
Locally configured policies:
 route-map ROUTE in
Inherited polices:
 prefix-list NO-MARKETING in
 route-map ROUTE in
 weight 300
 maximum-prefix 10000
```

以下是 **show bgp neighbors** 命令的输出示例，该命令验证是否为位于 172.16.1.2 的 BGP 邻居启用 BGP TCP 路径最大传输单元 (MTU) 发现：

```
> show bgp neighbors 172.16.1.2
BGP neighbor is 172.16.1.2,  remote AS 45000, internal link
  BGP version 4, remote router ID 172.16.1.99
....
 For address family: IPv4 Unicast
  BGP table version 5, neighbor version 5/0
...
  Address tracking is enabled, the RIB does have a route to 172.16.1.2
  Address tracking requires at least a /24 route to the peer
  Connections established 3; dropped 2
  Last reset 00:00:35, due to Router ID changed
  Transport(tcp) path-mtu-discovery is enabled
....
SRTT: 146 ms, RTTO: 1283 ms, RTV: 1137 ms, KRTT: 0 ms
minRTT: 8 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: higher precedence, retransmission timeout, nagle, path mtu capable
```

show bgp paths

要显示数据库中的所有 BGP 路径，请使用 **show bgp paths** 命令。

show bgp paths ［**vrf** *name* | **all**］ ［*regexp*］

Syntax Description

regexp	与 BGP 自主系统路径匹配的正则表达式。
［**vrf** *name*	**all**］	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将该命令限制为特定虚拟路由器。如果您希望 命令影响所有虚拟路由器，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则 命令适用于全局 VRF 虚拟路由器。

Command History

版本	修改
6.1	引入了此命令。
6.6	添加了 ［**vrf** *name*	**all**］ 关键字。

示例

以下是 **show bgp paths** 命令的输出示例。

```
> show bgp paths
Address    Hash Refcount Metric Path
0x60E5742C    0        1      0 i
0x60E3D7AC    2        1      0 ?
0x60E5C6C0   11        3      0 10 ?
0x60E577B0   35        2     40 10 ?
```

下表对每个字段进行了说明。

表 *11: show bgp paths* 字段

字段	Description
Address	存储路径的内部地址。
Hash	存储路径的散列储存桶。
Refcount	使用该路径的路由的数量。
Metric	路径的多出口标识符 (MED) 指标。（用于 BGP 版本 2 和 3 的此指标名称是 INTER_AS。）
Path	该路由的自主系统路径，其后是该路由的源代码。

show bgp prefix-list

要显示有关前缀列表或前缀列表条目的信息，请使用 **show bgp prefix-list** 命令。

show bgp prefix-list ［**vrf** *name* | **all**］ ［**detail** | **summary**］［*prefix-list-name* ［**seq** *sequence-number* | *network/length* ［**longer** | **first-match**］］］

Syntax Description

detail	**summary**	（可选）显示有关所有前缀列表的详细信息或摘要信息。
first-match	（可选） 显示与给定 网络/长度匹配的指定前缀列表的第一个条目。
longer	（可选）显示与给定 网络/长度匹配或比其更具体的指定前缀列表的所有条目。
network/length	（可选）显示使用此网络地址和网络掩码长度（以位为单位）的指定前缀列表中的所有条目。
prefix-list-name	（可选）显示特定前缀列表中的条目。
seq *sequence-number*	（可选）仅显示指定前缀列表中具有指定序列号的前缀列表条目。
［**vrf** *name*	**all**］	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将该命令限制为特定虚拟路由器。如果您希望 命令影响所有虚拟路由器，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则 命令适用于全局 VRF 虚拟路由器。

Command History

版本	修改
6.1	引入了此命令。
6.6	添加了 ［**vrf** *name*	**all**］ 关键字。

示例

以下示例展示 **show bgp prefix-list** 命令的输出，其中具有有关名为 test 的前缀列表的详细信息：

```
> show bgp prefix-list detail test
ip prefix-list test:
Description: test-list
 count: 1, range entries: 0, sequences: 10 - 10, refcount: 3
 seq 10 permit 10.0.0.0/8 (hit count: 0, refcount: 1)
```

show bgp regexp

要显示与自治系统路径正则表达式相匹配的路由，请使用 **show bgp regexp** 命令。

show bgp regexp ［**vrf** *name* | **all**］ *regexp*

Syntax Description

regexp	与 BGP 自主系统路径匹配的正则表达式。
［**vrf** *name*	**all**］	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将该命令限制为特定虚拟路由器。如果您希望 命令影响所有虚拟路由器，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则 命令适用于全局 VRF 虚拟路由器。

Command History

版本	修改
6.1	引入了此命令。
6.6	添加了 ［**vrf** *name*	**all**］ 关键字。

示例

以下是 **show bgp regexp** 命令的输出示例。

```
> show bgp regexp 108$
BGP table version is 1738, local router ID is 172.16.72.24
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop          Metric LocPrf Weight Path
*  172.16.0.0       172.16.72.30                           0 109 108 ?
*  172.16.1.0       172.16.72.30                           0 109 108 ?
*  172.16.11.0      172.16.72.30                           0 109 108 ?
*  172.16.14.0      172.16.72.30                           0 109 108 ?
*  172.16.15.0      172.16.72.30                           0 109 108 ?
*  172.16.16.0      172.16.72.30                           0 109 108 ?
*  172.16.17.0      172.16.72.30                           0 109 108 ?
*  172.16.18.0      172.16.72.30                           0 109 108 ?
*  172.16.19.0      172.16.72.30                           0 109 108 ?
*  172.16.24.0      172.16.72.30                           0 109 108 ?
*  172.16.29.0      172.16.72.30                           0 109 108 ?
*  172.16.30.0      172.16.72.30                           0 109 108 ?
*  172.16.33.0      172.16.72.30                           0 109 108 ?
*  172.16.35.0      172.16.72.30                           0 109 108 ?
*  172.16.36.0      172.16.72.30                           0 109 108 ?
*  172.16.37.0      172.16.72.30                           0 109 108 ?
*  172.16.38.0      172.16.72.30                           0 109 108 ?
*  172.16.39.0      172.16.72.30                           0 109 108 ?
```

show bgp rib-failure

要显示无法安装在路由信息库 (RIB) 表中的边界网关协议 (BGP) 路由，请使用 **show bgp rib-failure** 命令。

show bgp rib-failure ［**vrf** *name* | **all**］

Syntax Description

［**vrf** *name*	**all**］	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将该命令限制为特定虚拟路由器。如果您希望 命令影响所有虚拟路由器，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则 命令适用于全局 VRF 虚拟路由器。

Command History

版本	修改
6.1	引入了此命令。
6.6	添加了 ［**vrf** *name*	**all**］ 关键字。

示例

以下是 **show bgp rib-failure** 命令的输出示例：

```
> show bgp rib-failure
Network           Next Hop                 RIB-failure   RIB-NH Matches
10.1.15.0/24      10.1.35.5          Higher admin distance             n/a
10.1.16.0/24      10.1.15.1          Higher admin distance             n/a
```

下表对每个字段进行了说明。

表 *12: show bgp rib-failure* 字段

字段	Description
Network	网络实体的 IP 地址
Next Hop	在将数据包转发到目标网络时使用的下一个系统的 IP 地址。0.0.0.0 的条目表示路由器具有一些到此网络的非 BGP 路由。
RIB-failure	RIB 故障的原因。更高的管理距离意味着具有更好（较低）管理距离的路由（例如静态路由）已存在于 IP 路由表中。

字段	Description
RIB-NH Matches	仅当更高管理距离出现在 RIB 故障列中，且为正在使用的地址系列配置 **bgp suppress-inactive** 时才应用的路由状态。有三种选择： • 是 - 意味着 RIB 中的路由具有与 BGP 路由相同的下一跃点，或下一跃点下行递归到与 BGP 下一跃点相同的邻接。 • 否 - 意味着 RIB 中的下一跃点下行递归到与 BGP 路由不同的下一跃点。 • n/a - 表示 **bgp suppress-inactive** 未为正在使用的地址系列配置。

show bgp summary

要显示所有边界网关协议 (BGP) 连接的状态，请使用 **show bgp summary** 命令。

show bgp summary ［**vrf** *name* | **all**］

Syntax Description

［**vrf** *name*	**all**］	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将该命令限制为特定虚拟路由器。如果您希望 命令影响所有虚拟路由器，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则 命令适用于全局 VRF 虚拟路由器。

Command History

版本	修改
6.1	引入了此命令。
6.6	添加了 ［**vrf** *name*	**all**］ 关键字。

使用指南

show bgp summary 命令用于显示到 BGP 邻居的所有连接的 BGP 路径、前缀和属性信息。

前缀是IP地址和网络掩码。它可表示整个网络、网络的子集或单个主机路由。路径是到给定目标的路由。默认情况下，BGP仅会为每个目标安装一个路径。如果配置多路径路由，则BGP会为每个多路径路由安装一个路径条目，且仅会将一个多路径路由标记为最佳路径。

分别显示 BGP 属性和缓存条目，以组合形式显示会影响最佳路径选择过程。当配置相关 BGP 功能或收到属性时，显示此输出的字段。以字节为单位显示内存使用率。

示例

以下是 **show bgp summary** 命令在特权 EXEC 模式下的输出示例：

```
> show bgp summary
BGP router identifier 172.16.1.1, local AS number 100
BGP table version is 199, main routing table version 199
37 network entries using 2850 bytes of memory
59 path entries using 5713 bytes of memory
18 BGP path attribute entries using 936 bytes of memory
2 multipath network entries and 4 multipath paths
10 BGP AS-PATH entries using 240 bytes of memory
7 BGP community entries using 168 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
90 BGP advertise-bit cache entries using 1784 bytes of memory
36 received paths for inbound soft reconfiguration
BGP using 34249 total bytes of memory
Dampening enabled. 4 history paths, 0 dampened paths
BGP activity 37/2849 prefixes, 60/1 paths, scan interval 15 secs
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down State/PfxRcd
10.100.1.1      4   200      26      22      199    0    0 00:14:23 23
10.200.1.1      4   300      21      51      199    0    0 00:13:40 0
```

下表对每个字段进行了说明。

表 *13: show bgp summary* 字段

字段	Description
BGP router identifier	按优先级和可用性顺序排列，依次为路由器标识符、环回地址或最高IP地址。
BGP table version	BGP 数据库的内部版本号。
main routing table version	注入主路由表中的 BGP 数据库的上一版本。
...network entries	BGP 数据库中的单一前缀条目的数量。
...using ... bytes of memory	为同一行上显示的路径、前缀或属性条目所消耗的内存量（以字节为单位）。
...path entries using	BGP数据库中的路径条目的数量。仅会为给定目标安装一个路径条目。如果配置多路径路由，则会为每个多路径路由安装一个路径条目。
...multipath network entries using	为给定目标安装的多路径条目的数量。
* ...BGP path/bestpath attribute entries using	单一 BGP 属性组合的数量，其中选择这些组合的路径为最佳路径。
* ...BGP rrinfo entries using	单一 ORIGINATOR 和 CLUSTER_LIST 属性组合的数量。
...BGP AS-PATH entries using	单一 AS_PATH 条目的数量。
...BGP community entries using	单一 BGP 社区属性组合的数量。
*...BGP extended community entries using	单一扩展的社区属性组合的数量。
BGP route-map cache entries using	BGP 路由映射 match 和 set 子句组合的数量。0 值表示路由缓存为空。
...BGP filter-list cache entries using	与 AS 路径访问列表 permit 或 deny 语句匹配的过滤器列表条目的数量。0 值表示过滤器列表缓存为空。
BGP advertise-bit cache entries using	通告的位字段条目数和关联的内存使用量。位域条目表示向对等设备通告前缀时生成的一部分信息（一个位）。在需要时动态构建通告的位缓存。

字段	Description
1 received paths for inbound soft reconfiguration	为入站软重新配置收到和存储的路径的数量。
BGP using...	BGP 流程使用的内存总量（以字节为单位）。
Dampening enabled...	表示启用BGP阻尼。携带累积处罚规则的路径的数量和阻尼的路径的数量显示在此行上。
BGP activity...	显示已为路径或前缀分配或释放内存的次数。
Neighbor	邻居的 IP 地址。
V	向该邻居传达的 BGP 版本号。
AS	自主系统编号。
MsgRcvd	从邻居收到的消息的数量。
MsgSent	发送给邻居的消息的数量。
TblVer	发送给邻居的 BGP 数据库的上一版本。
InQ	要从邻居排队处理的消息的数量。
OutQ	要排队发送给邻居的消息的数量。
Up/Down	BGP会话处于“已建立”状态或当前状态（如果它不处于“已建立”状态）的时间长度。
State/PfxRcd	BGP会话的当前状态和已从邻居或对等设备组收到的前缀的数量。当达到最大数量时，条目中会显示字符串“PfxRcd”，邻居将关闭，连接设置为空闲。 状态为“空闲”的 (Admin) 条目表示连接已关闭。

show bgp summary 命令的以下输出展示动态创建 BGP 邻居 192.168.3.2，且它是侦听范围组 group192 的成员。输出还展示为名为 group192 的侦听范围组定义 192.168.0.0/16 的 IP 前缀范围。

```
> show bgp summary
BGP router identifier 192.168.3.1, local AS number 45000
BGP table version is 1, main routing table version 1

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
*192.168.3.2    4 50000       2       2        0    0    0 00:00:37        0
* Dynamically created based on a listen range command
Dynamically created neighbors: 1/(200 max), Subnet ranges: 1

BGP peergroup group192 listen range group members:
  192.168.0.0/16
```

show bgp summary 命令的以下输出展示两个采用不同4字节自主系统编号（65536和65550）的 BGP 邻居（192.168.1.2 和 192.168.3.2）。本地自主系统 65538 也是一个 4 字节自主系统编号，且编号以默认 asplain 格式显示。

```
> show bgp summary
BGP router identifier 172.17.1.99, local AS number 65538
BGP table version is 1, main routing table version 1
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  Statd
192.168.1.2     4        65536       7       7        1    0    0 00:03:04      0
192.168.3.2     4        65550       4       4        1    0    0 00:00:15      0
```

show bgp summary 命令的以下输出展示相同的两个 BGP 邻居，但以 asdot 记数法格式显示 4 字节自主系统编号。

```
> show bgp summary
BGP router identifier 172.17.1.99, local AS number 1.2
BGP table version is 1, main routing table version 1
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  Statd
192.168.1.2     4          1.0       9       9        1    0    0 00:04:13      0
192.168.3.2     4         1.14       6       6        1    0    0 00:01:24      0
```

show bgp update-group

显示有关 BGP 更新组的信息，请使用 **show bgp update-group** 命令。

show bgp update-group ［**vrf** *name* | **all**］ ［*index-group* | *ip-address*］［**summary**］

Syntax Description

index-group	（可选）使用相应的索引号更新组类型。更新组索引编号的范围为从 1 到 4294967295。
ip-address	（可选）作为更新组成员的单个邻居的 IP 地址。
summary	（可选）显示更新组成员信息的摘要。可以使用 index-group 或 ip-address 参数过滤输出，以显示单个索引组或对等体的信息。
［**vrf** *name*	**all**］	如果启用虚拟路由和转发(VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将该命令限制为特定虚拟路由器。如果您希望 命令影响所有虚拟路由器，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则 命令适用于全局 VRF 虚拟路由器。

Command History

版本	修改
6.1	引入了此命令。
6.6	添加了 ［**vrf** *name*	**all**］ 关键字。

使用指南

使用此命令以显示有关 BGP 更新组的信息。发生出站策略更改时，路由器自动重新计算更新组成员，并在 1 分钟计时器到期后通过触发出站软重置应用更改。如果产生错误，则此行为设计为为网络操作员提供更改配置的时间。

示例

show bgp update-group 命令的以下输出示例显示所有邻居的更新组信息：

```
> show bgp update-group
BGP version 4 update-group 1, internal, Address Family: IPv4 Unicast
  BGP Update version : 0, messages 0/0
  Route map for outgoing advertisements is COST1
  Update messages formatted 0, replicated 0
  Number of NLRIs in the update sent: max 0, min 0
  Minimum time between advertisement runs is 5 seconds
  Has 1 member:
  10.4.9.21
BGP version 4 update-group 2, internal, Address Family: IPv4 Unicast
  BGP Update version : 0, messages 0/0
  Update messages formatted 0, replicated 0
  Number of NLRIs in the update sent: max 0, min 0
  Minimum time between advertisement runs is 5 seconds
  Has 2 members:
```

```
10.4.9.5 10.4.9.8
```

下表对每个字段进行了说明。

表 *14: show bgp update-group* 字段

字段	Description
BGP version	BGP 版本。
update-group	更新组编号和类型（内部或外部）。
update messages formatted..., replicated...	已格式化和复制的更新消息数。
Number of NLRIs...	更新中发送的 NLRI 信息。
Default minimum time between...	为同一行上显示的路径、前缀或属性条目所消耗的内存量（以字节为单位）。
...path entries using	BGP 数据库中的路径条目的数量。仅会为给定目标安装一个路径条目。如果配置多路径路由，则会为每个多路径路由安装一个路径条目。
...multipath network entries using	为给定目标安装的多路径条目的数量。
* ...BGP path/bestpath attribute entries using	单一 BGP 属性组合的数量，其中选择这些组合的路径为最佳路径。
* ...BGP rrinfo entries using	单一 ORIGINATOR 和 CLUSTER_LIST 属性组合的数量。
...BGP AS-PATH entries using	单一 AS_PATH 条目的数量。
...BGP community entries using	单一 BGP 社区属性组合的数量。
*...BGP extended community entries using	单一扩展的社区属性组合的数量。
BGP route-map cache entries using	BGP 路由映射 match 和 set 子句组合的数量。0 值表示路由缓存为空。
...BGP filter-list cache entries using	与 AS 路径访问列表 permit 或 deny 语句匹配的过滤器列表条目的数量。0 值表示过滤器列表缓存为空。
BGP advertise-bit cache entries using	通告的位字段条目数和关联的内存使用量。位域条目表示向对等设备通告前缀时生成的一部分信息（一个位）。在需要时动态构建通告的位缓存。

字段	Description
1 received paths for inbound soft reconfiguration	为入站软重新配置收到和存储的路径的数量。
BGP using...	BGP 流程使用的内存总量（以字节为单位）。
Dampening enabled...	表示启用BGP阻尼。携带累积处罚规则的路径的数量和阻尼的路径的数量显示在此行上。
BGP activity...	显示已为路径或前缀分配或释放内存的次数。
Neighbor	邻居的 IP 地址。
V	向该邻居传达的 BGP 版本号。
AS	自主系统编号。
MsgRcvd	从邻居收到的消息的数量。
MsgSent	发送给邻居的消息的数量。
TblVer	发送给邻居的 BGP 数据库的上一版本。
InQ	要从邻居排队处理的消息的数量。
OutQ	要排队发送给邻居的消息的数量。
Up/Down	BGP会话处于“已建立”状态或当前状态（如果它不处于“已建立”状态）的时间长度。
State/PfxRcd	BGP会话的当前状态和已从邻居或对等设备组收到的前缀的数量。当达到最大数量时，条目中会显示字符串“PfxRcd”，邻居将关闭，连接设置为空闲。 状态为“空闲”的 (Admin) 条目表示连接已关闭。

show blocks

要显示系统缓冲区利用率，请使用 **show blocks** 命令。

show blocks [**core** | **export-failed** | **interface**]
show blocks address *hex* [**diagnostics** | **dump** | **header** | **packet**]
show blocks {**all** | **assigned** | **free** | **old**} [**core-local** [*core-num*] [**diagnostics** | **dump** | **header** | **packet**]]
show blocks exhaustion {**history** [**list** | *snapshot_num*] | **snapshot**}
show blocks pool *block-size*
show blocks queue history [**core-local** [*core-num*]] [**detail**]

Syntax Description

address *hex*	（可选）显示与此地址对应的块（以十六进制形式）。
all	（可选）显示所有块。
assigned	（可选）显示分配的且应用正在使用的块。
core	（可选）显示特定于核心的缓冲区。
core-local [*core-num*]	（可选）显示所有核心的系统缓冲区。您还可以指定核心编号（例如 1），以查看特定核心的缓冲区。
detail	（可选）显示每个单一队列类型的第一个块的一部分（128 个字节）。
dump	（可选）显示整个块内容，包括信头和数据包信息。转储与数据包之间的差异在于转储包括信头和数据包之间的附加信息。
diagnostics	（可选）显示块诊断。
exhaustion snapshot	（可选）打印拍取的最后 x 个（x 当前为 10）快照和最后一个快照的时间戳。拍取快照后，如果已过不到 5 分钟，则不拍取另一个快照。
exhaustion history [**list** | *snapshot_num*]	（可选）显示耗尽快照历史记录。您可以指定快照编号以将信息限制为单个快照，或指定列表以查看 **list** 快照。
export-failed	（可选）显示系统缓冲区导出失败计数器。
free	（可选）显示可用的块。
header	（可选）显示块的信头。
interface	（可选）显示连接到接口的缓冲区。
old	（可选）显示超过一分钟前分配的块。
packet	（可选）显示块的信头和数据包内容。
pool *block-size*	（可选）显示特定大小的块。

queue history	（可选）显示当 threat defense 设备耗尽块时分配块的位置。有时，从池中分配块，但从不将块分配给队列。在这种情况下，位置是分配块的代码地址。

Command History

版本	修改
6.1	引入了此命令。
7.0(1)	此命令的输出已增强，包括失败计数。

使用指南

show blocks 命令可帮助您确定 threat defense 设备是否过载。此命令列出预分配的系统缓冲区利用率。只要流量通过 threat defense 设备移动，内存已满就不是问题。您可以使用 **show conn** 命令查看流量是否移动。如果流量不移动且内存已满，则可能存在问题。您也可以使用 SNMP 查看此信息。

示例

以下是 **show blocks** 命令的输出示例。

```
> show blocks
  SIZE    MAX    LOW    CNT    FAILED
     0   1450   1450   1450       0
     4    100     99     99       0
    80   1996   1992   1992       0
   256   4148   4135   4142       0
  1550   6274   6270   6272       0
  2048    100    100    100       0
  2560    164    164    164       0
  4096    100    100    100       0
  8192    100    100    100       0
  9344    100    100    100       0
 16384    100    100    100       0
 65536     16     16     16       0
```

下表对每个字段进行了说明。

表 *15: show blocks Fields*

字段	Description
大小	块池的大小（以字节为单位）。每个大小表示一个特定类型。
0	为 dupb 块使用。
4	复制应用（例如 DNS、ISAKMP、URL 过滤、uauth、TFTP 和 TCP 模块）中的现有块。此外，代码通常可使用这种大小的块将数据包发送给驱动程序等。
80	用于在 TCP 拦截中为故障转移问候消息生成确认数据包。

字段	Description
256	用于状态化故障转移更新、系统日志记录和其他 TCP 功能。 这些块主要用于状态化故障转移消息。主用 threat defense 设备生成并发送数据包到备用 threat defense 设备以更新转换和连接表。在突发流量中，创建或断开高速率连接时，可用块的数量可能降至 0。此情况表示未将一个或多个连接更新到备用 threat defense 设备。状态化故障转移协议会在下次捕获缺少的转换或连接。如果 256 字节块的 CNT 列在扩展的时间段内保持为或接近于 0，则 threat defense 设备会因 threat defense 设备每秒处理的连接的数量而难以保持转换和连接表同步。 从 threat defense 设备发出的系统日志消息也使用 256 字节块，但通常不会如此大量地释放它们，以免导致 256 字节块池耗尽。如果 CNT 列显示 256 字节块的数量接近于 0，请确保您不会在调试级别（第 7 级）登录到系统日志服务器。这通过 threat defense 配置中的日志记录陷阱行表示。我们建议您在通知级别（第 5 级）或更低级别设置日志记录，除非您需要附加信息来进行调试。
1550	用于存储通过 threat defense 设备处理的以太网数据包。 当数据包进入接口时，它被置于输入接口队列中，传递到操作系统上，然后置于块中。设备确定是应根据安全策略允许数据包，还是予以拒绝，然后在出站接口上处理到达输出队列的数据包。如果设备难以承载流量负载，则可用块的数量会在 0（正如命令输出的 CNT 列中所示）附近浮动。当 CNT 列是零时，设备尝试分配更多块。如果发出此命令，则 1550 字节块的最大数量可大于 8192。如果无更多可用块，则设备丢弃数据包。
2048	用于控制更新的控制或引导的帧。
16384	仅用于 64 位 66 MHz 千兆位以太网卡 (i82543)。 请参阅 1550 的说明，了解有关以太网数据包的更多信息。
MAX	指定字节块池的可用块的最大数量。在启动时从内存中划分块的最大数量。通常，块的最大数量不会更改。但 256 字节和 1550 字节块的最大数量是例外，其中设备可在需要时动态创建更多块。如果发出此命令，则 1550 字节块的最大数量可大于 8192。
LOW	下限。此数字表示自设备通电或最后清除块（使用 **clear blocks** 命令）后这种大小的可用块的最小数量。LOW 列中的零表示上一个事件，其中内存已满。
CNT	该特定大小块池的可用块的当前数量。CNT 列中的零意味着内存现在已满。

以下是 **show blocks all** 命令的输出示例：

```
> show blocks all
Class 0, size 4
     Block   allocd_by    freed_by data size  alloccnt  dup_cnt  oper location
0x01799940  0x00000000  0x00101603         0         0        0 alloc not_specified
0x01798e80  0x00000000  0x00101603         0         0        0 alloc not_specified
0x017983c0  0x00000000  0x00101603         0         0        0 alloc not_specified
...
    Found 1000 of 1000 blocks
```

```
    Displaying 1000 of 1000 blocks
```

下表对每个字段进行了说明。

表 *16: show blocks all* 字段

字段	Description
Block	块地址。
allocd_by	最后使用块的应用的程序地址（如果未使用，则为 0）。
freed_by	最后释放块的应用的程序地址。
data size	块内的应用缓冲区/数据包数据的大小。
alloccnt	自块存在后已使用此块的次数。
dup_cnt	对此块（如果使用）的引用的当前数量：0 表示 1 个引用，1 表示 2 个引用。
oper	最后在块上执行的四个操作之一：分配、获得、放置或释放。
location	使用块的应用，或最后分配块的应用的程序地址（与 allocd_by 字段相同）。

以下是 **show blocks exhaustion history list** 命令的输出示例：

```
> show blocks exhaustion history list
1 Snapshot created at 18:01:03 UTC Feb 19 2014:
   Snapshot created due to 16384 blocks running out

2 Snapshot created at 18:02:03 UTC Feb 19 2014:
   Snapshot created due to 16384 blocks running out

3 Snapshot created at 18:03:03 UTC Feb 19 2014:
   Snapshot created due to 16384 blocks running out

4 Snapshot created at 18:04:03 UTC Feb 19 2014:
   Snapshot created due to 16384 blocks running out
```

Related Commands

命令	Description
blocks	增加分配给块诊断的内存。
clear blocks	清除系统缓冲区统计信息。
show conn	显示活动连接。

show bootvar

要显示引导文件和配置属性，请使用 **show bootvar** 命令。

show bootvar

Command History

版本	修改
6.1	引入了此命令。

使用指南

BOOT 变量指定各种设备上的可引导映像的列表。CONFIG_FILE 变量指定在系统初始化期间使用的配置文件。

此命令的输出可能对 threat defense没有意义。

示例

以下是显示threat defense引导变量的示例。虽然变量为空，但此示例来自正常运行的系统。

```
> show bootvar
BOOT variable =
Current BOOT variable =
CONFIG_FILE variable =
Current CONFIG_FILE variable =
```

show bridge-group

要显示网桥组信息，如分配的接口、MAC 地址和 IP 地址，请使用 **show bridge-group** 命令。

show bridge-group ［*bridge_group_number*］

Syntax Description

bridge_group_number	将网桥组编号指定为一个介于 1 和 250 之间的整数。如果不指定编号，则会显示所有网桥组。

Command History

版本	修改
6.1	添加了此命令。
6.2	使用集成路由和桥接时，我们在路由防火墙模式下添加了支持。

示例

以下是 **show bridge-group** 命令的输出示例。

```
> show bridge-group
Static mac-address entries:  0 (in use), 16384 (max)
Dynamic mac-address entries: 0 (in use), 16384 (max)
 Bridge Group: 1
 Interfaces:
 GigabitEthernet1/2
 GigabitEthernet1/3
 GigabitEthernet1/4
 GigabitEthernet1/5
 GigabitEthernet1/6
 GigabitEthernet1/7
 GigabitEthernet1/8
 Management System IP Address:  192.168.1.1 255.255.255.0
 Management Current IP Address: 192.168.1.1 255.255.255.0
 Management IPv6 Global Unicast Address(es):
    2000:100::1, subnet is 2000:100::/64
 Static mac-address entries:  0
 Dynamic mac-address entries: 0
```

Related Commands

命令	Description
show running-config interface bvi	显示该桥组接口配置。

show c

show capture

在未指定选项时显示捕获配置，请使用 **show capture** 命令。

show capture ［*capture_name*］［**access-list** *access_list_name*］［**count** *number*］［**decode**］［**detail**］［**dump**］［**packet-number** *number*］［**trace**］

Syntax Description

access-list *access_list_name*	（可选）显示基于用于标识特定访问列表的 IP 或较高字段的数据包的信息。
capture_name	（可选）指定数据包捕获的名称。
count *number*	（可选）显示数据包指定的数据的数量。有效值为 0 到 4294967295。
decode	当类型 ISAKMP 的捕获应用于接口时，此选项非常有用。在解密后会捕获流过该接口的所有 ISAKMP 数据，并在解码字段后展示更多信息。
detail	（可选）显示每个数据包的附加协议信息。
dump	（可选）显示通过数据链路传输的数据包的十六进制转储。
packet-number *number*	（可选）以指定的数据包编号开始显示。有效值为 0 到 4294967295。
trace	（可选）显示每个数据包的扩展跟踪信息 - 如果使用上述 trace 关键字设置了捕获，则会显示入站方向上每个数据包的数据包跟踪器的输出。

Command History

版本	修改
6.1	引入了此命令。

使用指南

如果指定捕获名称，则显示该捕获的捕获缓冲区内容。

dump 关键字不显示十六进制转储中的 MAC 信息。

数据包的解码输出取决于数据包的协议。在下表中，当您指定 **detail** 关键字时，会显示括号内的输出。

表 *17:* 数据包捕获输出格式

数据包类型	捕获输出格式
802.1Q	*HH:MM:SS.ms* [ether-hdr] *VLAN-info encap-ether-packet*
ARP	*HH:MM:SS.ms* [ether-hdr] *arp-type arp-info*
IP/ICMP	*HH:MM:SS.ms* [ether-hdr] *ip-source* > *ip-destination:* icmp: *icmp-type icmp-code* [checksum-failure]

数据包类型	捕获输出格式
IP/UDP	*HH:MM:SS.ms* [ether-hdr] *src-addr.src-port dest-addr.dst-port:* [checksum-info] udp *payload-len*
IP/TCP	*HH:MM:SS.ms* [ether-hdr] *src-addr.src-port dest-addr.dst-port: tcp-flags* [header-check] [checksum-info] *sequence-number ack-number tcp-window urgent-info tcp-options*
IP/Other	*HH:MM:SS.ms* [ether-hdr] *src-addr dest-addr: ip-protocol ip-length*
其他	*HH:MM:SS.ms ether-hdr: hex-dump*

如果 threat defense 设备收到的数据包带有格式不正确的 TCP 信头，并因 ASP 丢弃原因 invalid-tcp-hdr-length 而丢弃这些数据包，则接收这些数据包的接口上的 **show capture** 命令输出不会显示这些数据包。

注释 使用文件大小选项时：

- **show capture** ［*capture_name*］命令显示捕获和跳过的数据包数。
- **show capture** 命令以 KB 和 MB 为单位显示捕获的数据。

示例

此示例展示如何显示捕获配置：

```
> show capture
capture arp ethernet-type arp interface outside
capture http access-list http packet-length 74 interface inside
```

此示例展示如何显示 ARP 捕获捕获的数据包：

```
> show capture arp
2 packets captured
19:12:23.478429 arp who-has 171.69.38.89 tell 171.69.38.10
19:12:26.784294 arp who-has 171.69.38.89 tell 171.69.38.10
2 packets shown
```

以下示例展示如何显示在一个集群技术环境中的单个设备上捕获的数据包：

```
> show capture
capture 1 cluster type raw-data interface primary interface cluster [Buffer Full - 524187
bytes]
capture 2 type raw-data interface cluster [Capturing - 232354 bytes]
```

以下示例展示如何显示在一个集群技术环境中的所有设备上捕获的数据包：

```
> cluster exec show capture
mycapture (LOCAL):--------------------------------------------------------------
capture 1 type raw-data interface primary [Buffer Full - 524187 bytes]
capture 2 type raw-data interface cluster [Capturing - 232354 bytes]

yourcapture:--------------------------------------------------------------------
capture 1 type raw-data interface primary [Capturing - 191484 bytes]
capture 2 type raw-data interface cluster [Capturing - 532354 bytes]
```

以下示例展示已在接口上启用 SGT 和以太网标记时捕获的数据包：

```
> show capture my-inside-capture
1: 11:34:42.931012 INLINE-TAG 36 10.0.101.22 > 11.0.101.100: icmp: echo request
2: 11:34:42.931470 INLINE-TAG 48 11.0.101.100 > 10.0.101.22: icmp: echo reply
3: 11:34:43.932553 INLINE-TAG 36 10.0.101.22 > 11.0.101.100: icmp: echo request
4: 11.34.43.933164 INLINE-TAG 48 11.0.101.100 > 10.0.101.22: icmp: echo reply
```

已在接口上启用 SGT 和以太网标记时，该接口仍可收到标记或取消标记的数据包。展示的示例用于标记的数据包，该数据包在输出中具有 INLINE-TAG 36。当同一接口收到取消标记的数据包时，输出保持不变（即输出中不包括任何“INLINE-TAG 36”条目）。

Related Commands

命令	Description
capture	启用数据包捕获功能以进行数据包嗅探和网络故障隔离。
clear capture	清除捕获缓冲区。
copy capture	将捕获文件复制到服务器。

show cert-update

要显示 threat defense 设备上 CA 证书的自动更新状态，请使用 **show cert-update** 命令。

show cert-update

Command History

版本	修改
7.0.5	引入了此命令。

示例

以下是 **show cert-update** 命令的输出示例：

```
> show cert-update
Autoupdate is enabled and set for every day at 09:34 UTC
CA bundle was last modified 'Thu Sep 15 16:12:35 2022'
```

Related Commands

命令	Description
configure cert-update auto-update	启用或禁用每天自动更新 CA 证书。
configure cert-update run-now	立即尝试更新 CA 认证。
configure cert-update test	使用来自思科服务器的最新 CA 证书执行连接检查。

show checkheaps

要显示检查堆统计信息，请使用 **show checkheaps** 命令。Checkheaps 是验证堆内存缓冲区健全性（动态内存分配自系统堆内存区域）和代码区域完整性的定期流程。

show checkheaps

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show checkheaps** 命令的输出示例：

```
> show checkheaps
Checkheaps stats from buffer validation runs
--------------------------------------------
Time elapsed since last run     : 42 secs
Duration of last run            : 0 millisecs
Number of buffers created       : 8082
Number of buffers allocated     : 7808
Number of buffers free          : 274
Total memory in use             : 43570344 bytes
Total memory in free buffers    : 87000 bytes
Total number of runs            : 310
```

show checksum

要显示配置校验和，请使用 **show checksum** 命令。

show checksum

Command History

版本	修改
6.1	引入了此命令。

使用指南

show checksum 命令允许您显示充当配置内容的数字摘要的四组十六进制数字。仅当您在闪存中存储配置时，才计算此校验和。

如果点（“.”）出现在 **show running-config** 或 **show checksum** 命令输出中的校验和之前，则输出表示常规配置负载或写入模式指示器（当从 threat defense 闪存分区加载或写入该分区时）。“.”显示 threat defense 设备正忙于操作，但未“挂断”。此消息类似于“系统正在处理，请稍候”消息。

示例

此示例展示如何显示配置或校验和：

```
> show checksum
Cryptochecksum: 1a2833c0 129ac70b 1a88df85 650dbb81
```

show chunkstat

要显示数据块统计信息，请使用 **show chunkstat** 命令。

show chunkstat

Command History

版本	修改
6.1	引入了此命令。

示例

此示例展示如何显示数据块统计信息：

```
> show chunkstat
Global chunk statistics: created 181, destroyed 34, siblings created 94, siblings destroyed
 34

Per-chunk statistics: siblings created 0, siblings trimmed 0
Dump of chunk at 01edb4cc, name "Managed Chunk Queue Elements", data start @ 01edbd24, end
 @ 01eddc54
next: 01eddc8c, next_sibling: 00000000, prev_sibling: 00000000
flags 00000001
maximum chunk elt's: 499, elt size: 16, index first free 498
# chunks in use: 1, HWM of total used: 1, alignment: 0
Per-chunk statistics: siblings created 0, siblings trimmed 0
Dump of chunk at 01eddc8c, name "Registry Function List", data start @ 01eddea4, end @
01ede348
next: 01ede37c, next_sibling: 00000000, prev_sibling: 00000000
flags 00000001
maximum chunk elt's: 99, elt size: 12, index first free 42
# chunks in use: 57, HWM of total used: 57, alignment: 0
```

Related Commands

命令	Description
show counters	显示协议栈计数器。
show cpu	显示 CPU 利用率信息。

show clns

要显示 IS-IS 的无连接模式网络服务 (CLNS) 信息，请使用 **show clns** 命令。

show clns {**filter-set** [*name*] | **interface** [*interface_name*] | **is-neighbors** [*interface_name* [**detail**] | **neighbors** [**areas**] [*interface_name*] [**detail**] | **protocol** [*domain*] | **traffic**}

Syntax Description

filter-set [*name*]	显示 CLNS 过滤器集。您可以选择指定过滤器集的名称。
interface [*interface_name*]	显示 CLNS 接口状态和配置。您可以选择指定接口的名称以聚焦输出。
is-neighbors [*interface_name*] [**detail**]	显示 IS 邻居邻接关系。邻居条目根据它们所在的区域进行排序。您可以选择指定接口的名称以聚焦输出。 指定 **detail** 以包括与中间系统关联的区域。否则，将提供摘要显示。
neighbors [**areas**] [*interface_name*] [**detail**]	显示终端系统 (ES)、中间系统 (IS) 和多拓扑集成中间系统到中间系统 (M-ISIS) 邻居。您可以选择指定接口的名称以聚焦输出。 包括 **areas** 关键字以显示 CLNS 多区域邻接关系。 指定 **detail** 以包括与中间系统关联的区域。否则，将提供摘要显示。
protocol [*domain*]	显示 CLNS 路由协议流程信息。始终至少有两个路由流程（第 1 级和第 2 级），并且可以更多。您可以选择指定CLNS域的名称以突出显示输出。
traffic	列出此路由器已发现的 CLNS 数据包。

Command History

版本	修改
6.3	引入了此命令。

示例

以下示例显示在运行配置中定义的 CLNS 过滤器集，并使用 **show clns filter-set** 命令显示它们。

```
> show running-config clns
clns filter-set US-OR-NORDUNET permit 47.0005...
clns filter-set US-OR-NORDUNET permit 47.0023...
clns filter-set LOCAL permit 49.0003
> show clns filter-set

CLNS filter set US-OR-NORDUNET
      permit 47.0005...
      permit 47.0023...
CLNS filter set LOCAL
      permit 49.0003...
```

以下是 **show clns interface** 命令的输出示例。“路由协议：IS-IS”下的信息显示与中间系统到中间系统 (IS-IS) 相关的信息，包括级别 1 和级别 2 指标、优先级、电路 ID 以及活动级别 1 和级别的数量2 邻接关系。

```
> show clns interface
GigabitEthernet0/1 is up, line protocol is up
  Checksums enabled, MTU 1500
  ERPDUs enabled, min. interval 10 msec.
  DEC compatibility mode OFF for this interface
  Next ESH/ISH in 0 seconds
  Routing Protocol: IS-IS
    Circuit Type: level-1-2
    Interface number 0x0, local circuit ID 0x1
    Level-1 Metric: 10, Priority: 64, Circuit ID: c2.01
    DR ID: c2.01
    Level-1 IPv6 Metric: 10
    Number of active level-1 adjacencies: 3
    Level-2 Metric: 10, Priority: 64, Circuit ID: c2.01
    DR ID: c2.01
    Level-2 IPv6 Metric: 10
    Number of active level-2 adjacencies: 3
    Next IS-IS LAN Level-1 Hello in 1 seconds
    Next IS-IS LAN Level-2 Hello in 1 seconds
```

以下是 **show clns neighbors** 命令的输出示例。

```
> show clns neighbors

System Id      Interface   SNPA            State  Holdtime  Type Protocol
CSR7001        inside      000c.2921.ff44  Up          29   L1L2
CSR7002        inside      000c.2906.491c  Up          27   L1L2
```

下表对邻居输出字段进行了解释。

表 *18:* 邻居输出中的字段

字段	Description
System Id	标识区域中的系统的六字节值。
Interface	从中获知系统的接口的名称。
SNPA	子网连接点。这是数据链路地址。
State	ES、IS 或 M-ISIS 的状态。 • Init - 系统是 IS，正在等待 IS-IS hello 消息。IS-IS 将邻居视为不相邻。 • Up - 系统认为 ES 或 IS 可访问。
Holdtime	此邻接关系条目超时之前的秒数。

字段	Description
Type	邻接类型。 • ES - 通过 ES-IS 协议发现或静态配置的终端系统邻接关系。 • IS - 通过 ES-IS 协议发现或静态配置的路由器邻接关系。 • M-ISIS - 通过多拓扑 IS-IS 协议发现的路由器邻接关系。 • L1 - 仅用于 1 级路由的路由器邻接关系。 • L1L2 - 用于第 1 级和第 2 级路由的路由器邻接关系。 • L2 - 仅适用于第 2 级的路由器邻接关系。
Protocol	获知邻接关系的协议。有效的协议源包括ES-IS、IS-IS、ISO IGRP、Static、DECnet 和 M-ISIS。

以下是 **show clns neighbors detail** 命令的输出示例。

```
> show clns neighbors detail

System Id      Interface   SNPA            State  Holdtime  Type Protocol
CSR7001        inside      000c.2921.ff44      Up          26   L1L2
  Area Address(es): 49.0001
  IP Address(es):  1.3.3.3*
  Uptime: 01:16:33
  NSF capable
  Interface name: inside
CSR7002        inside      000c.2906.491c      Up          27   L1L2
  Area Address(es): 49.0001
  IP Address(es):  20.3.3.3*
  Uptime: 01:16:33
  NSF capable
  Interface name: inside
```

以下是 **show clns is-neighbors** 命令的输出示例。

```
> show clns is-neighbors

System Id      Interface   State  Type Priority  Circuit Id         Format
CSR7001        inside      Up     L1L2 64/64    ciscoasa.01        Phase V
CSR7002        inside      Up     L1L2 64/64    ciscoasa.01        Phase V
```

下表对 is-邻居输出栏进行了解释。

表 *19: IS* 邻居输出中的字段

字段	Description
System Id	系统的标识值。
Interface	发现路由器的接口。

字段	Description
State	邻接状态。Up 和 Init 是状态。有关详细信息，请参阅 **show clns neighbors** 说明。
Type	邻接关系类型：L1、L2 或 L1L2。有关详细信息，请参阅 **show clns neighbors** 说明。
Priority	相应邻居通告的 IS-IS 优先级。最高优先级邻居被选为接口的指定 IS-IS 路由器。
Circuit Id	邻居对接口的指定 IS-IS 路由器的想法。
Format	指示邻居是阶段 V (OSI) 邻接关系还是阶段 IV (DECnet) 邻接关系的格式。

以下是 **show clns is-neighbors detail** 命令的输出示例。

```
> show clns is-neighbors detail

System Id      Interface   State  Type Priority  Circuit Id         Format
CSR7001        inside      Up     L1L2 64/64    ciscoasa.01        Phase V
  Area Address(es): 49.0001
  IP Address(es):  1.3.3.3*
  Uptime: 00:12:49
  NSF capable
  Interface name: inside
CSR7002        inside      Up     L1L2 64/64    ciscoasa.01        Phase V
  Area Address(es): 49.0001
  IP Address(es):  20.3.3.3*
  Uptime: 00:12:50
  NSF capable
  Interface name: inside
```

以下是 **show clns protocol** 命令的输出示例。

```
> show clns protocol
IS-IS Router
  System Id: 0050.0500.5008.00  IS-Type: level-1-2
  Manual area address(es):
        49.0001
  Routing for area address(es):
        49.0001
  Interfaces supported by IS-IS:
        outside - IP
  Redistribute:
    static (on by default)
  Distance for L2 CLNS routes: 110
  RRR level: none
  Generate narrow metrics: level-1-2
  Accept narrow metrics:   level-1-2
  Generate wide metrics:   none
  Accept wide metrics:     none
```

以下是 **show clns traffic** 命令的输出示例。

```
> show clns traffic
```

```
CLNS:  Time since last clear: never
CLNS & ESIS Output: 0, Input: 8829
CLNS Local: 0, Forward: 0
CLNS Discards:
  Hdr Syntax: 0, Checksum: 0, Lifetime: 0, Output cngstn: 0
  No Route: 0, Discard Route: 0, Dst Unreachable 0, Encaps. Failed: 0
  NLP Unknown: 0, Not an IS: 0
CLNS Options: Packets 0, total 0 , bad 0, GQOS 0, cngstn exprncd 0
CLNS Segments:  Segmented: 0, Failed: 0
CLNS Broadcasts: sent: 0, rcvd: 0
Echos: Rcvd 0 requests, 0 replies
      Sent 0 requests, 0 replies
ESIS(sent/rcvd): ESHs: 0/0, ISHs: 0/0, RDs: 0/0, QCF: 0/0
Tunneling (sent/rcvd): IP: 0/0, IPv6: 0/0
Tunneling dropped (rcvd) IP/IPV6:  0
ISO-IGRP: Querys (sent/rcvd): 0/0 Updates (sent/rcvd): 0/0
ISO-IGRP: Router Hellos: (sent/rcvd): 0/0
ISO-IGRP Syntax Errors: 0

IS-IS: Time since last clear: never
IS-IS: Level-1 Hellos (sent/rcvd): 1928/1287
IS-IS: Level-2 Hellos (sent/rcvd): 1918/1283
IS-IS: PTP Hellos     (sent/rcvd): 0/0
IS-IS: Level-1 LSPs sourced (new/refresh): 7/13
IS-IS: Level-2 LSPs sourced (new/refresh): 7/14
IS-IS: Level-1 LSPs flooded (sent/rcvd): 97/2675
IS-IS: Level-2 LSPs flooded (sent/rcvd): 73/2628
IS-IS: LSP Retransmissions: 0
IS-IS: Level-1 CSNPs (sent/rcvd): 642/0
IS-IS: Level-2 CSNPs (sent/rcvd): 639/0
IS-IS: Level-1 PSNPs (sent/rcvd): 0/554
IS-IS: Level-2 PSNPs (sent/rcvd): 0/390
IS-IS: Level-1 DR Elections: 1
IS-IS: Level-2 DR Elections: 1
IS-IS: Level-1 SPF Calculations: 9
IS-IS: Level-2 SPF Calculations: 8
IS-IS: Level-1 Partial Route Calculations: 0
IS-IS: Level-2 Partial Route Calculations: 0
IS-IS: LSP checksum errors received: 0
IS-IS: Update process queue depth: 0/200
IS-IS: Update process packets dropped: 0
```

下表对流量输出中的字段进行了解释。

表 *20:* 流量输出中的字段

字段	**Description**
CLNS & ESIS Output	通过此路由器发送的数据包总数。
Input	通过此路由器接收的数据包总数。
CLNS Local	此路由器生成的数据包的数量。
Forward	此路由器已转发的数据包数。
CLNS Discards	CLNS 已丢弃的数据包数，按丢弃原因分类。
CLNS Options	CLNS 数据包中显示的选项。

字段	Description
CLNS Segments	已分段的数据包数以及由于无法对数据包进行分段而发生的失败次数。
CLNS Broadcasts	发送和接收的 CLNS 广播数量。
Echos	收到的回应请求数据包和回应应答数据包的数量。此字段后面的行列出发送的回应请求数据包和回应应答数据包的数量。
ESIS (sent/rcvd)	发送和接收的终端系统 Hello (ESH)、中间系统 Hello (ISH) 和重定向的数量。
ISO IGRP	发送和接收的 ISO 内部网关路由协议 (IGRP) 查询和更新的数量。
Router Hellos	发送和接收的 ISO IGRP 路由器问候信头数。
IS-IS: Level-1 hellos (sent/rcvd)	发送和接收的第 1 级 IS-IS hello 数据包的数量。
IS-IS: Level-2 hellos (sent/rcvd)	发送和接收的第 2 级 IS-IS hello 数据包的数量。
IS-IS: PTP hello (sent/rcvd)	通过串行链路发送和接收的点对点 IS-IS hello 数据包的数量。
IS-IS：1 级 LSP (sent/rcvd)	发送和接收的第 1 级链路状态协议数据单元 (PDU) 的数量。
IS-IS: Level-2 LSPs (sent/rcvd)	发送和接收的第 2 级链路状态 PDU 的数量。
IS-IS: Level-1 CSNPs (sent/rcvd)	发送和接收的第 1 级完整序列号数据包 (CSNP) 的数量。
IS-IS: Level-2 CSNPs (sent/rcvd)	发送和接收的第 2 级 CSNP 的数量。
IS-IS: Level-1 PSNPs (sent/rcvd)	发送和接收的第 1 级部分序列号数据包 (PSNP) 的数量。
IS-IS: Level-2 PSNPs (sent/rcvd)	发送和接收的第 2 级 PSNP 的数量。
IS-IS: Level-1 DR Elections	发生 1 级指定路由器选举的次数。
IS-IS: Level-2 DR Elections	发生第 2 级指定路由器选举的次数。
IS-IS: Level-1 SPF Calculations	计算 1 级最短路径优先 (SPF) 树的次数。
IS-IS: Level-2 SPF Calculations	计算 2 级 SPF 树的次数。

Related Commands

命令	Description
clear clns	清除 CLNS 特定信息。

show cluster

要查看整个集群的聚合数据或其他信息，请使用 **show cluster** 命令。

show cluster { access-list [*acl_name*] | **conn** [**count**] | **cpu** [**usage**] | **interface-mode** | **memory** | **resource usage** | **rule hits** [**raw**] | **service-policy** | **traffic** | **xlate count** }

Syntax Description

access-list [*acl_name*]	显示访问策略的命中计数器。要查看用于特定 ACL 的计数器，请输入 acl_name。
conn [**count**]	显示所有设备上正在使用的连接的聚合计数。如果输入 **count** 关键字，则仅显示连接计数。
cpu [**usage**]	显示 CPU 使用率信息。
interface-mode	显示集群接口模式，即跨区模式或单个模式。
memory	显示系统内存利用率和其他信息。
resource usage	显示系统资源和使用率。
rule hits ［**raw**］	显示访问控制策略和预过滤器策略的所有评估规则的规则命中信息。**raw** 关键字以 .csv 格式显示数据。
service-policy	显示 MPF 服务策略统计信息。
traffic	显示流量统计信息。
xlate count	显示当前转换信息。

Command History

版本	修改
6.4	添加了 **rule hits** ［**raw**］关键字。
6.1	引入了此命令。

示例

以下是 **show cluster access-list** 命令的输出示例：

```
> show cluster access-list
hitcnt display order: cluster-wide aggregated result, unit-A, unit-B,  unit-C, unit-D
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval 300
access-list 101; 122 elements; name hash: 0xe7d586b5
access-list 101 line 1 extended permit tcp 192.168.143.0 255.255.255.0 any eq www
  (hitcnt=0, 0, 0, 0, 0) 0x207a2b7d
access-list 101 line 2 extended permit tcp any 192.168.143.0 255.255.255.0
  (hitcnt=0, 0, 0, 0, 0) 0xfe4f4947
```

```
access-list  101 line 3 extended permit tcp host 192.168.1.183 host 192.168.43.238
  (hitcnt=1, 0, 0, 0, 1) 0x7b521307
access-list 101 line 4 extended permit tcp host 192.168.1.116 host 192.168.43.238
  (hitcnt=0, 0, 0, 0, 0) 0x5795c069
access-list 101 line 5 extended permit tcp host 192.168.1.177 host 192.168.43.238
  (hitcnt=1, 0, 0, 1, 0) 0x51bde7ee
access list 101 line 6 extended permit tcp host 192.168.1.177 host 192.168.43.13
  (hitcnt=0, 0, 0, 0, 0) 0x1e68697c
access-list 101 line 7 extended permit tcp host 192.168.1.177 host 192.168.43.132
  (hitcnt=2, 0, 0, 1, 1) 0xc1ce5c49
access-list 101 line 8 extended permit tcp host 192.168.1.177 host 192.168.43.192
  (hitcnt=3, 0, 1, 1, 1) 0xb6f59512
access-list 101 line 9 extended permit tcp host 192.168.1.177 host 192.168.43.44
  (hitcnt=0, 0, 0, 0, 0) 0xdc104200
access-list 101 line 10 extended permit tcp host 192.168.1.112 host 192.168.43.44
  (hitcnt=429, 109, 107, 109, 104)0xce4f281d
access-list 101 line 11 extended permit tcp host 192.168.1.170 host 192.168.43.238
  (hitcnt=3, 1, 0, 0, 2) 0x4143a818
access-list 101 line 12 extended permit tcp host 192.168.1.170 host 192.168.43.169
  (hitcnt=2, 0, 1, 0, 1) 0xb18dfea4
access-list 101 line 13 extended permit tcp host 192.168.1.170 host 192.168.43.229
  (hitcnt=1, 1, 0, 0, 0) 0x21557d71
access-list 101 line 14 extended permit tcp host 192.168.1.170 host 192.168.43.106
  (hitcnt=0, 0, 0, 0, 0) 0x7316e016
access-list 101 line 15 extended permit tcp host 192.168.1.170 host 192.168.43.196
  (hitcnt=0, 0, 0, 0, 0) 0x013fd5b8
access-list 101 line 16 extended permit tcp host 192.168.1.170 host 192.168.43.75
  (hitcnt=0, 0, 0, 0, 0) 0x2c7dba0d
```

要显示所有设备在用连接的 汇聚计数，请输入：

```
> show cluster conn count
Usage Summary In Cluster:*********************************************
  200 in use (cluster-wide aggregated)
     cl2(LOCAL):************************************************************
  100 in use, 100 most used
  cl1:************************************************************
  100 in use, 100 most used
```

Related Commands

命令	Description
show cluster info	显示集群信息。

show cluster history

要查看集群的事件历史记录，请在特权 EXEC 模式下使用 **show cluster history** 命令。

show cluster history [**brief**] [**latest** [*number*]] [**reverse**] [**time** [*year month day*] *hh* **:** *mm* **:** *ss*]

Syntax Description

brief	显示没有通用事件的集群历史记录。
latest [*number*]	显示最新的事件。默认情况下，设备会显示最近的 512 个事件。您可以将事件 数 限制在 1 到 512 之间。
reverse	以相反的顺序显示事件。
time [*year month day*] *hh*:*mm*:*ss*	显示指定日期和时间之前的事件。

Command Default

无默认行为或值。

Command History

版本	修改
7.0	添加了 **brief**、 **latest**、 **reverse**、 **time** 关键词。
6.6	**show cluster history** 命令增强了有关集群设备未能加入或离开集群的原因的消息。
6.1	添加了此命令。

Usage Guidelines

以下是 **show cluster history time** 命令的输出示例：

```
> show cluster history time august 26 10:10:05
================================================================================
From State            To State              Reason
================================================================================

10:08:49 UTC Aug 26 2020
DISABLED              DISABLED              Disabled at startup


10:09:43 UTC Aug 26 2020
DISABLED              ELECTION              Enabled from CLI


10:10:01 UTC Aug 26 2020
ELECTION              ONCALL                Event: Cluster unit A state is MASTER


10:10:02 UTC Aug 26 2020
ONCALL                SLAVE_COLD            Slave proceeds with configuration sync


10:10:02 UTC Aug 26 2020
```

```
SLAVE_COLD            SLAVE_CONFIG          Client progression done


10:10:04 UTC Aug 26 2020
SLAVE_CONFIG          SLAVE_FILESYS         Configuration replication finished


10:10:05 UTC Aug 26 2020
SLAVE_FILESYS         SLAVE_BULK_SYNC       Client progression done
```

以下是 **show cluster history brief** 命令的输出示例：

```
> show cluster history brief
================================================================================
From State            To State              Reason
================================================================================

10:08:49 UTC Aug 26 2020
DISABLED              DISABLED              Disabled at startup


10:09:43 UTC Aug 26 2020
DISABLED              ELECTION              Enabled from CLI



10:10:02 UTC Aug 26 2020
ONCALL                SLAVE_COLD            Slave proceeds with configuration sync


10:10:02 UTC Aug 26 2020
SLAVE_COLD            SLAVE_CONFIG          Client progression done


10:10:04 UTC Aug 26 2020
SLAVE_CONFIG          SLAVE_FILESYS         Configuration replication finished


10:10:05 UTC Aug 26 2020
SLAVE_FILESYS         SLAVE_BULK_SYNC       Client progression done
```

以下是 **show cluster history latest** 命令的输出示例：

```
> show cluster history latest 3
================================================================================
From State            To State              Reason
================================================================================

10:10:05 UTC Aug 26 2020
SLAVE_FILESYS         SLAVE_BULK_SYNC       Client progression done


10:10:04 UTC Aug 26 2020
SLAVE_CONFIG          SLAVE_FILESYS         Configuration replication finished


10:10:02 UTC Aug 26 2020
SLAVE_COLD            SLAVE_CONFIG          Client progression done
```

Related Commands

命令	Description
show cluster	显示整个集群的汇总数据和其他信息。
show cluster info	显示集群信息。

show cluster info

要查看集群信息，请使用 **show cluster info** 命令。

show cluster info [**auto-join** | **clients** | **conn-distribution** | **flow-mobility counters** | **goid** [*options*] | **health** | **incompatible-config** | **instance-type** | **loadbalance** | **old-members** | **packet-distribution** | **trace** [*options*] | **transport** { **asp** | **cp** }]

Syntax Description

auto-join	显示集群设备是否将在一段延迟后自动重新加入集群，以及是否已清除故障条件（例如等待许可证、机箱运行状况检查失败，等等）。如果设备已永久禁用，或设备已在群集中，则此命令将不会显示任何输出。
clients	（可选）显示注册客户端的版本。
conn-distribution	（可选）显示集群中的连接分布。
flow-mobility counters	（可选）显示 EID 移动和流所有者移动信息。
goid [*options*]	（可选）显示全局对象 ID 数据库。选项包括： classmap conn-set hwidb idfw-domain idfw-group interface policymap virtual-context
health	（可选）显示运行健康监控信息。
incompatible-config	（可选）显示与当前运行配置中的集群技术不兼容的命令。此命令在启用集群技术前有用。
instance-type	（可选）使用多实例集群技术时，显示每个集群成员的模块类型和资源大小。
loadbalance	（可选）显示负载平衡信息。
old-members	（可选）显示集群的前成员。
packet-distribution	（可选）显示集群中的数据包分布。

trace [*options*]	（可选）显示集群技术控制模块事件跟踪。选项包括： • **latest** [*number*]-显示最新 number 事件，其中该数字介于 1 和 2147483647 之间。默认值为全部显示。 • **level** *level*- 按级别过滤事件，其中级别为以下项之一： **all**、 **critical**、 **debug**、 **informational**或 **warning**。 • **module** *module*- 按模块过滤事件，其中模块为以下其中一项： **ccp**、 **datapath**、 **fsm**、 **general**、 **hc**、 **license**、 **rpc**或 **transport**。 • **time** {[*month day*] [*hh:mm:ss*]}- 在指定时间或日期前显示事件。
transport {**asp** | **cp**}	（可选）显示与以下项的统计信息相关的传输： • **asp**— 数据平面传输统计信息。 • **cp**— 控制平面传输统计信息。

Command History

版本	修改
6.1	引入了此命令。
6.2.3	添加了 **auto-join** 关键字。
6.6	输出已增强，以显示多实例集群技术特征。还添加了 **instance-type** 关键字，以显示每个集群成员的模块类型和资源大小。

使用指南

如果您不指定任何选项，则 **show cluster info** 命令显示通用集群信息，其中包括集群名称和状态、集群成员、成员状态等。

使用 **clear cluster info** 命令清除统计信息。

示例

以下是 **show cluster info** 命令的输出示例：

```
> show cluster info
Cluster stbu: On
  This is "C" in state SLAVE
      ID        : 0
      Site ID : 1
      Version   : 6.2
      Serial No.: P3000000025
      CCL IP    : 10.0.0.3
      CCL MAC   : 000b.fcf8.c192
      Last join : 17:08:59 UTC Sep 26 2011
      Last leave: N/A
Other members in the cluster:
  Unit "D" in state SLAVE
      ID        : 1
      Site ID : 1
```

```
      Version   : 6.2
      Serial No.: P3000000001
      CCL IP    : 10.0.0.4
      CCL MAC   : 000b.fcf8.c162
      Last join : 19:13:11 UTC Sep 23 2011
      Last leave: N/A
  Unit "A" in state MASTER
      ID        : 2
      Site ID : 2
      Version   : 6.2
      Serial No.: JAB0815R0JY
      CCL IP    : 10.0.0.1
      CCL MAC   : 000f.f775.541e
      Last join : 19:13:20 UTC Sep 23 2011
      Last leave: N/A
  Unit "B" in state SLAVE
      ID        : 3
      Site ID : 2
      Version   : 6.2
      Serial No.: P3000000191
      CCL IP    : 10.0.0.2
      CCL MAC   : 000b.fcf8.c61e
      Last join : 19:13:50 UTC Sep 23 2011
      Last leave: 19:13:36 UTC Sep 23 2011
```

以下是使用多实例集群技术时 **show cluster info** 命令的输出示例：

```
> show cluster info
Cluster MI: On
    Interface mode: spanned
    This is "unit-3-1" in state MASTER
        ID             : 0
        Site ID         : 1
        Version           : 6.6
        Serial No.        : FLM2123050F12T
        CCL IP             : 127.2.3.1
        CCL MAC   : a28e.6000.0012
        Module.
: FPR4K-SM-12
        Resource.
: 10 cores / 23876 MB RAM
        Last join          : 19:48:33 UTC Nov 13 2018
        Last leave: N/A
Other members in the cluster:
    Unit "unit-4-1" in state SLAVE
        ID                : 1
        Site ID            : 1
        Version            : 6.6
        Serial No.         : FLM212305ELPXW
        CCL IP             : 127.2.4.1
        CCL MAC     : a2f7.2000.0009
        Module
: FPR4K-SM-12
        Resource
: 6 cores / 14426 MB RAM
        Last join           : 20:29:55 UTC Nov 14 2018
        Last leave        : 19:07:53 UTC Nov 14 2018


Warning: Mixed module and / or mismatched resource profile size in cluster. System may not
 run in an optimized state.
```

以下是使用多实例集群技术时 **show cluster info instance-type** 命令的输出示例：

```
> show cluster info instance-type

     Cluster Member     Module Type                CPU Cores        RAM (MB)
         unit-3-1       FPR4K-SM-12                  10              23876
         unit-4-1       FPR4K-SM-12                  6               14446

Warning: Mixed module type and / or mismatched resource profile in cluster. System may not
 run in an optimized state.
```

以下是 **show cluster info incompatible-config** 命令的输出示例：

```
> show cluster info incompatible-config
INFO: Clustering is not compatible with following commands which given a
user's confirmation upon enabling clustering, can be removed automatically
from running-config.
policy-map global_policy
 class scansafe-http
  inspect scansafe http-map fail-close
policy-map global_policy
 class scansafe-https
  inspect scansafe https-map fail-close
INFO: No manually-correctable incompatible configuration is found.
```

以下是 **show cluster info trace** 命令的输出示例：

```
> show cluster info trace
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Send CCP message to all: CCP_MSG_KEEPALIVE from 80-1 at MASTER
```

以下是 **show cluster info flow-mobility counters** 命令的输出示例：

```
> show cluster info flow-mobility counters
EID movement notification received  : 0
EID movement notification processed : 0
Flow owner moving requested         : 0
```

有关 **show cluster info auto-join** 命令，请参阅以下输出：

```
> show cluster info auto-join
Unit will try to join cluster in 253 seconds.
Quit reason: Received control message DISABLE

> show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Master has application down that slave has up.

> show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Chassis-blade health check failed.

> show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Service chain application became down.

> show cluster info auto-join
```

```
Unit will try to join cluster when quit reason is cleared.
Quit reason: Unit is kicked out from cluster because of Application health check failure.

> show cluster info auto-join
Unit join is pending (waiting for the smart license entitlement: ent1)

> show cluster info auto-join
Unit join is pending (waiting for the smart license export control flag)
```

Related Commands

命令	Description
show cluster	显示整个集群的聚合数据。

cluster exec show rule hits

要从集群的所有节点以聚合格式显示访问控制策略和预过滤器策略的所有评估规则的命中信息，请使用 **show cluster rule hits** 命令。

show cluster rule hits ［**raw**］

Syntax Description

raw	（可选）以 .csv 格式显示规则命中信息。

Command Default

显示来自集群所有节点的所有规则的规则命中信息。

Command History

版本	修改
6.4	引入了此命令。

使用指南

规则命中信息仅涵盖访问控制规则和预过滤器规则。

示例

以下示例以隔离格式显示来自集群的每个节点的规则命中信息：

```
> show cluster rule hits
RuleID               Hit Count           First Hit Time(UTC)     Last Hit Time(UTC)
-------------------------------------------------------------------------------------
268435264            1                   06:54:44 Mar 8 2019     06:54:44 Mar 8 2019
268435265            1                   06:54:58 Mar 8 2019     06:54:58 Mar 8 2019
268435270            1                   06:54:53 Mar 8 2019     06:54:53 Mar 8 2019
268435271            1                   06:55:01 Mar 8 2019     06:55:01 Mar 8 2019
268435260            1                   06:55:17 Mar 8 2019     06:55:17 Mar 8 2019
268435261            1                   06:55:19 Mar 8 2019     06:55:19 Mar 8 2019
```

Related Commands

命令	Description
cluster exec show rule hits	以隔离的格式显示集群中每个节点的访问控制策略和预过滤器策略的所有评估规则命中信息。
cluster exec clear rule hits	从集群中的所有节点清除访问控制策略和预过滤器策略的所有评估规则的规则命中信息，并将其重置为零。
show rule hits	显示访问控制策略和预过滤器策略的所有评估规则的规则命中信息。
clear rule hits	清除访问控制策略和预过滤器策略的所有评估规则的规则命中信息，并将其重置为零。

show community-list

要显示特定社区列表允许的路由，请使用 **show community-list** 命令。

show community-list ［*community_list_name*］

Syntax Description

community_list_name	（可选）社区列表名称。

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show community-list** 命令的输出示例：

```
> show community-list

Named Community expanded list comm2
    permit 10
Named Community standard list excomm1
    permit internet 100 no-export no-advertise
```

show conn

要显示指定连接类型的连接状态，请使用 **show conn** 命令。此命令支持 IPv4 和 IPv6 地址。

show conn [**vrf** { *name* | **global** }] [**count** | [**all**] [**detail**] [**data-rate-filter** { **lt** | **eq** | **gt** } **value** }]] [**long**] [**state** *state_type*] [**flow-rule**] [**inline-set**] [**protocol** { **tcp** | **udp** | **sctp** }] [**address** *src_ip* [− *src_ip*] [**netmask** *mask*]] [**port** *src_port* [− *src_port*]] [**address** *dest_ip* [− *dest_ip*] [**netmask** *mask*]] [**port** *dest_port* [− *dest_port*]] [**state** *state_type*] [**zone** [*zone_name*]]
[**data-rate**]

Syntax Description

address {*src_ip* | *dest_ip*}	（可选）显示具有指定源或目标 IPv4 或 IPv6 地址的连接。要指定范围，请使用破折号 (-) 分隔各个 IP 地址。例如，10.1.1.1-10.1.1.5。
all	（可选）除通过流量连接外还显示到达设备或从设备发起的连接。
count	（可选）显示活动连接的数量。
detail	（可选）显示连接的详细信息，包括转换类型和接口信息。
data-rate-filter {lt | eq | gt}*value*	（可选）显示根据数据速率值（每秒字节数）过滤的连接。例如： *data-rate-filter gt 123*
flow-rule	（可选）显示流规则的连接。
inline-set	（可选）显示内联集的连接。
long	（可选）以长格式显示连接。
netmask *mask*	（可选）指定要与给定 IP 地址配合使用的子网掩码。
port {*src_port* | *dest_port*}	（可选）显示具有指定源或目标端口的连接。要指定范围，请使用破折号 (-) 分隔各个端口号。例如，1000-2000。
protocol {**tcp | udp |sctp**}	（可选）指定连接协议。
state *state_type*	（可选）指定连接状态类型。有关可用于连接状态类型的关键字列表，请参阅“用法”部分中的表。
zone [*zone_name*]	（可选）显示区域的连接。**long** 和 **detail** 关键字可显示用于构建连接的主接口和用于转发流量的当前接口。
[**vrf** {*name* | **global**}]	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将该命令限制为特定虚拟路由器。指定 **vrf global** 以将命令限制为全局虚拟路由器。如果省略此关键字，则命令适用于所有虚拟路由器。
data-rate	（可选）显示数据速率跟踪状态是已启用还是已禁用。

Command Default 默认情况下显示所有通过连接。您还需要使用 **all** 关键字查看到设备的管理连接。

Command History

版本	修改
6.1	引入了此命令。
6.4	已添加 **egress_optimization** 连接状态类型。
6.5	失效连接检测 (DCD) 发起方/响应方探测计数已添加到启用 DCD 的连接的 **show conn detail** 输出中。
6.6	引入了以下更改： • 添加了 **vrf** 关键字。 连接数据速率跟踪状态已添加。 `show conn detail` 命令中添加了 **data-rate-filter** 关键字，以按用户指定的数据速率值过滤连接。 • **show conn detail** 命令输出中的 **packet id** 参数已更改为 **Connection lookup keyid**。
6.7	命令输出中添加了 B 标志，以指示 tcp 流用于获取 TLS 服务器证书。
7.2	命令输出的 N 标志已增强，包括 3、4 和 5，以指示大流连接以及对它们采取的操作。
7.3	添加了 QUIC 协议的 Q 标志。

使用指南 **show conn** 命令显示活动 TCP 和 UDP 连接的数量，并提供各种类型的连接的有关信息。使用 **show conn all** 命令查看整个连接表。您可以使用此命令查找受特定 QoS 规则 ID 限制的实时连接。

注释 当 threat defense 设备创建用于允许辅助连接的针孔时，将在 **show conn** 命令输出中显示为不完整的连接。要清除此不完整的连接，请使用 **clear conn** 命令。

下表定义了可以使用 **show conn state** 命令指定的连接类型。指定多个连接类型时，请使用逗号，不用空格分隔关键字。以下示例展示处于“打开”状态的 RPC、H.323 和 SIP 连接的有关信息：

```
> show conn state up,rpc,h323,sip
```

表 *21:* 连接状态类型

关键字	显示的连接类型
up	处于打开状态的连接。

关键字	显示的连接类型
conn_inbound	请勿使用此关键字。它无法正确显示入站连接。
ctiqbe	CTIQBE 连接
data_in	入站数据连接。
data_out	出站数据连接。
egress_optimization	显示有关符合出口优化条件的连接的信息，这是一项可提高性能的功能。根据思科 TAC 的建议使用此命令。此命令使用标志 **F**（仅前向流符合出口优化条件）、**R**（仅反向流符合条件）或 **FR**（前向和反向流均符合条件）。
finin	FIN 入站连接。
finout	FIN 出站连接。
h225	H.225 连接
h323	H.323 连接
http_get	HTTP 获得连接。
mgcp	MGCP 连接。
nojava	拒绝访问 Java 小应用的连接。
rpc	RPC 连接。
service_module	SSM 扫描的连接。
sip	SIP 连接。
skinny	SCCP 连接。
smtp_data	SMTP 邮件数据连接。
sqlnet_fixup_data	SQL*Net 数据检查引擎连接。
tcp_embryonic	TCP 初期连接。
vpn_orphan	孤立的 VPN 隧道流。

使用 **detail** 选项时，系统使用下表中定义的连接标志显示有关转换类型的信息和接口信息。

表 *22:* 连接标志

标志	**Description**
a	等待发起方 ACK 到 SYN

标志	Description
A	等待响应方 ACK 到 SYN
b	TCP 状态绕行或钉牢
B	服务器证书的 TCP 探测
C	计算机电话接口快速缓冲编码 (CTIQBE) 媒体连接
c	集群集中式
d	转储
D	DNS
E	外部回连接。这是必须从内部主机发起的辅助数据连接。例如，使用 FTP 时，内部客户端发出 PASV 命令且外部服务器接受该命令后， threat defense 预分配具有此标志集的外部回连接。如果内部客户端尝试回连接到服务器，则 threat defense 拒绝此连接尝试。仅外部服务器可以使用预分配的辅助连接。
e	半分布式
f	发起方 FIN
F	响应方 FIN
g	媒体网关控制协议 (MGCP) 连接
G	group G 标志表示连接是组的一部分。它由 GRE 和 FTP Strict 检查修复设置，用以指定控制连接及其所有关联的辅助连接。如果控制连接终止，则也会终止所有关联的辅助连接。
h	H.225
H	H.323
i	不完整的 TCP 或 UDP 连接
I	发起方数据
j	GTP 数据
J	GTP
k	瘦客户端控制协议 (SCCP) 媒体连接
K	GTP t3-response
L	要解封的外部流
m	SIP 媒体连接

标志	Description
M	SMTP 数据
n	GUP （网守更新协议）
N	由 Snort 检查。 如果系统配置为在 Snort 关闭时保留连接（默认情况下启用），则 N 标志包含一个数字。有关详细信息，请参阅 **configure snort** 命令。 • 1 - 如果 Snort 关闭，将保留此连接。 • 2 - Snort 已关闭，此连接已保留。Snort 将不再检查该连接。 • 3 - 表示与大流相关的连接。 • 4 - 对大型流绕过了 Snort 检测。 • 5 - 动态速率限制策略（降低 10%）被应用于象流。
o	分流流量。
O	响应方数据
p	客流量
P	内部回连接。这是必须从内部主机发起的辅助数据连接。例如，使用 FTP 时，内部客户端发出 PASV 命令且外部服务器接受该命令后， threat defense 预分配具有此标志集的外部回连接。如果外部服务器尝试回连接到服务器，则设备拒绝此连接尝试。仅内部客户端可以使用预分配的辅助连接。
q	SQL*Net 数据
Q	QUIC 协议。
r	发起方已确认 FIN。当发起方的 FIN 被响应方确认时，会出现此标志。
R	响应方已确认 TCP 连接的 FIN。当发起方确认响应方的 FIN 时，会显示此标志。
R	UDP RPC。 由于 **show conn** 命令输出的每行表示一个连接（TCP 或 UDP），因此每行将只有一个 R 标志。
t	SIP 临时连接。 对于 UDP 连接，值 t 表示该连接将在一分钟后超时。
T	SIP 连接。 对于 UDP 连接，值 T 表示该连接将根据使用 **timeout sip** 命令指定的值超时。
U	up

标志	Description
v	M3UA 连接
V	VPN 孤立
W	WAAS
w	对于 Firepower 9300 上的机箱间集群，标识单独机箱上的备份所有者上的流。
X	由服务模块检查。
x	每个会话
y	对于集群，标识备用末节流。
Y	对于集群，标识控制器末节流。
z	对于集群，标识转发器末节流。
Z	Scansafe 重定向

注释 对于使用 DNS 服务器的连接，可以用 **show conn** 命令输出中的 DNS 服务器的 IP 地址替换连接的源端口。

只要多个 DNS 会话在相同的两个主机之间，且会话具有相同的 5 元组（源/目标 IP 地址、源/目标端口和协议），就为这些会话创建一个连接。可通过 *app_id*跟踪 DNS 标识，且每个 app_id 的空闲计时器独立运行。

由于 app_id 的期限是独立，因此，合法的 DNS 应答只能在有限的时间段内通过 threat defense 设备，而且不会累积资源。但是，输入 **show conn** 命令时，将会看到新的 DNS 会话正在重置 DNS 连接的空闲计时器。这由共享 DNS 连接的性质和设计用意决定。

注释 当在连接非活动超时期间（默认情况下为 1:00:00）没有 TCP 流量时，连接将关闭，相应的连接标志条目将不再显示。

如果局域网至局域网/网络扩展模式隧道丢弃且不会复原，则可能会存在许多孤立的隧道流。这些流量不会因为隧道发生故障而被拆解，但是试图从中流过的所有数据都会被丢弃。 **show conn** 命令输出展示这些具有 V 标志的孤立的流。

在版本 6.2.0.2 和 6.2.3 或更高版本中使用 **count** 选项时，系统使用下表中定义的状态显示有关连接数的信息。

表 *23:* 连接状态

Status	Description
enabled	当前启用了保留连接的连接。
in effect	保留连接的连接当前已生效。
most enabled	保留的最大连接数。
most in effect	保留的最大同步保留连接数。

使用 **data-rate** 关键字查看连接数据速率跟踪功能的当前状态 - 已启用或已禁用。使用 **data-rate filter** 关键字根据数据速率值（以字节/秒为单位）过滤连接。使用关系运算符（小于、等于或大于）过滤连接数据。输出显示活动连接以及两个数据速率值 - 瞬时一秒和最大数据速率，适用于正向和反向流。

示例

以下是 **show conn** 命令的输出示例。此示例展示一个从内部主机 10.1.1.15 到位于 10.10.49.10 的外部 Telnet 服务器的 TCP 会话连接。由于不存在 B 标志，连接从内部发起。“U”、“I”和“O”标志表示连接处于活动状态并已收到入站和出站数据。

```
> show conn
54 in use, 123 most used
TCP out 10.10.49.10:23 in 10.1.1.15:1026 idle 0:00:22, bytes 1774, flags UIO
UDP out 10.10.49.10:31649 in 10.1.1.15:1028 idle 0:00:14, bytes 0, flags D-
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:5060, idle 0:00:24, bytes 1940435, flags UTIOB
TCP dmz 10.10.10.50:49764 inside 192.168.1.21:5060, idle 0:00:42, bytes 2328346, flags UTIOB
TCP dmz 10.10.10.51:50196 inside 192.168.1.22:2000, idle 0:00:04, bytes 31464, flags UIB
TCP dmz 10.10.10.51:52738 inside 192.168.1.21:2000, idle 0:00:09, bytes 129156, flags UIOB
TCP dmz 10.10.10.50:49764 inside 192.168.1.21:0, idle 0:00:42, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):49736 inside 192.168.1.21:0, idle 0:01:32, bytes 0,
flags Ti
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:0, idle 0:00:24, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:01:34, bytes 0,
flags Ti
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:0, idle 0:02:24, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:03:34, bytes 0,
flags Ti
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:0, idle 0:04:24, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:05:34, bytes 0,
flags Ti
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:0, idle 0:06:24, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:07:34, bytes 0,
flags Ti
```

以下是 **show conn count** 命令的输出示例：

```
> show conn count
30 in use, 3194964 most used
Cluster:
        fwd connections: 1 in use, 52 most used
        dir connections: 7 in use, 43826206 most used
        centralized connections: 0 in use, 15 most used
```

```
Inspect Snort:
       preserve-connection: 100 enabled, 80 in effect, 400 most enabled, 300 most in effect
```

以下是 **show conn detail** 命令的输出示例。此示例展示一个从外部主机 10.10.49.10 到内部主机 10.1.1.15 的 UDP 连接。D 标志表示这是 DNS 连接。数字 1028 是通过连接的 DNS ID。

```
> show conn detail
2 in use, 39 most used
Inspect Snort:
        preserve-connection: 2 enabled, 0 in effect, 39 most enabled, 0 most in effect
Flags: A - awaiting responder ACK to SYN, a - awaiting initiator ACK to SYN,
       b - TCP state-bypass or nailed,
       C - CTIQBE media, c - cluster centralized,
       D - DNS, d - dump, E - outside back connection, e - semi-distributed,
       F - initiator FIN, f - responder FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - initiator data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, L - decap tunnel, M - SMTP data, m - SIP media
       N - inspected by Snort (1 - preserve-connection enabled, 2 - preserve-connection in
 effect)
       n - GUP, O - responder data, o - offloaded,
       P - inside back connection, p - passenger flow
       q - SQL*Net data, R - initiator acknowledged FIN,
       R - UDP SUNRPC, r - responder acknowledged FIN,
       T - SIP, t - SIP transient, U - up,
       V - VPN orphan, v - M3UA W - WAAS,
       w - secondary domain backup,
       X - inspected by service module,
       x - per session, Y - director stub flow, y - backup stub flow,
       Z - Scansafe redirection, z - forwarding stub flow

TCP out: 151.101.128.134/443 in: 192.168.1.9/51570,
    flags UfrxIO N1, idle 39s, uptime 10m39s, timeout 10m0s, bytes 4698, xlate id
0x2b8a6ec9b140
  Initiator: 192.168.1.9, Responder: 151.101.128.134
  Connection lookup keyid: 23610071

TCP out: 151.101.120.134/443 in: 192.168.1.9/51568,
    flags UfrxIO N1, idle 39s, uptime 10m40s, timeout 10m0s, bytes 5564, xlate id
0x2b8a6ec9ad40
  Initiator: 192.168.1.9, Responder: 151.101.120.134
 Connection lookup keyid: 23388003
```

以下为存在孤立流量时 **show conn** 命令的示例输出，孤立流量以 V 标志表示：

```
> show conn
16 in use, 19 most used
TCP out 192.168.110.251:7393 in 192.168.150.252:21 idle 0:00:00, bytes 1048, flags UOVB
TCP out 192.168.110.251:21137 in 192.168.150.252:21 idle 0:00:00, bytes 1048, flags UIOB
```

要将报告内容限定为具有孤立流量的连接，请将 **vpn_orphan** 选项添加至 **show conn state** 命令，如以下示例所示：

```
> show conn state vpn_orphan
14 in use, 19 most used
TCP out 192.168.110.251:7393 in 192.168.150.252:5013, idle 0:00:00, bytes 2841019, flags
UOVB
```

对于群集，要对连接流进行故障排除，请先在主设备上输入 **cluster exec show conn** 命令查看所有设备上的连接。寻找具有以下标志的流：导向者 (Y)、备用 (y) 和转发者 (z)。下例显示了三台设备上的一条从 172.18.124.187:22 到 192.168.103.131:44727 的 SSH 连接； threat defense1 带有 z 标志，表示其是该连接的转发者； threat defense3 带有 Y 标志，表示其是该连接的导向者；而 threat defense2 则没有特殊的标志，表示其是所有者。在出站方向，此连接的数据包进入 threat defense2 上的内部接口并从外部接口流出。在入站方向，此连接的数据包进入 threat defense1 和 threat defense3 上的外部接口，通过集群控制链路被转发到 threat defense2，然后流出 threat defense2 上的内部接口。

```
> cluster exec show conn
FTD1(LOCAL):**************************************************
18 in use, 22 most used
Cluster stub connections: 0 in use, 5 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727,
idle 0:00:00, bytes 37240828, flags z
FTD2:**************************************************
12 in use, 13 most used
Cluster stub connections: 0 in use, 46 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727,
idle 0:00:00, bytes 37240828, flags UIO
FTD3:**************************************************
10 in use, 12 most used
Cluster stub connections: 2 in use, 29 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727,
idle 0:00:03, bytes 0, flags  Y
```

threat defense2 上的 show conn detail 命令的输出展示最近的转发器为 threat defense1：

```
> show conn detail
12 in use, 13 most used
Cluster stub connections: 0 in use, 46 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       b - TCP state-bypass or nailed,
       C - CTIQBE media, c - cluster centralized,
       D - DNS, d - dump, E - outside back connection, e - semi-distributed,
       F - outside FIN, f - inside FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, L - LISP triggered flow owner mobility,
       M - SMTP data, m - SIP media, n - GUP
       O - outbound data, o - offloaded,
       P - inside back connection,
       Q - Diameter, q - SQL*Net data,
       R - outside acknowledged FIN,
       R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
       V - VPN orphan, W - WAAS,
       w - secondary domain backup,
       X - inspected by service module,
       x - per session, Y - director stub flow, y - backup stub flow,
       Z - Scansafe redirection, z - forwarding stub flow
TCP outside: 172.18.124.187/22 inside: 192.168.103.131/44727,
    flags UIO , idle 0s, uptime 25s, timeout 1h0m, bytes 1036044,
cluster sent/rcvd bytes 0/1032983, cluster sent/rcvd total bytes 0/1080779, owners (1,255)
Traffic received at interface outside
        Locally received: 0 (0 byte/s)
        From most recent forwarder FTD1: 1032983 (41319 byte/s)
Traffic received at interface inside
```

```
        Locally received: 3061 (122 byte/s)
```

使用 **detail** 关键字时，您可以查看有关失效连接检测 (DCD) 探测的信息，这会显示发起方和响应方探测连接的频率。例如，对于启用 DCD 的连接，其连接详细信息如下所示：

```
TCP dmz: 10.5.4.11/5555 inside: 10.5.4.10/40299,
    flags UO , idle 1s, uptime 32m10s, timeout 1m0s, bytes 11828,
cluster sent/rcvd bytes 0/0, owners (0,255)
  Traffic received at interface dmz
        Locally received: 0 (0 byte/s)
  Traffic received at interface inside
        Locally received: 11828 (6 byte/s)
  Initiator: 10.5.4.10, Responder: 10.5.4.11
  DCD probes sent: Initiator 5, Responder 5
```

以下示例显示如何查看连接数据速率跟踪功能的状态：

```
ciscoasa# show conn data-rate
Connection data rate tracking is currently enabled.
```

以下示例显示如何根据指定的数据速率过滤连接：

```
firepower# show conn detail data-rate-filter ?
eq  Enter this keyword to show conns with data-rate equal to specified value
gt  Enter this keyword to show conns with data-rate greater than specified value
lt Enter this keyword to show conns with data-rate less than specified value
firepower# show conn detail data-rate-filter gt ?
<0-4294967295> Specify the data rate value in bytes per second
firepower# show conn detail data-rate-filter gt 123 | grep max rate
max rate: 3223223/399628 bytes/sec
max rate: 3500123/403260 bytes/sec
```

以下示例是带有 B 标志的 **show conn** 和 **show conn detail** 的输出。B 标志表示 TCP 流用于获取 TLS1.3 服务器证书。当从客户端和 threat defense 的连接获取对 TLS 1.3 证书的请求时，会在 TLS 1.3 服务器和 threat defense之间建立另一个连接。因此，在 threat defense 和客户端之间建立了一个连接；在 TLS 1.3 服务器和 threat defense之间建立了另一个连接。

```
>show conn
1 in use, 3 most used
Inspect Snort:
       preserve-connection: 1 enabled, 0 in effect, 1 most enabled, 0 most in effect
 TCP outside  33.33.33.2:80 inside  1.1.1.2:35226, idle 0:00:00, bytes 246324931, flags
UIOBN1

> show conn detail
1 in use, 3 most used
Inspect Snort:
       preserve-connection: 1 enabled, 0 in effect, 1 most enabled, 0 most in effect
Flags: A - awaiting responder ACK to SYN, a - awaiting initiator ACK to SYN,
       b - TCP state-bypass or nailed,
       B - TCP probe for server certificate
       C - CTIQBE media, c - cluster centralized,
       D - DNS, d - dump, E - outside back connection, e - semi-distributed,
       F - initiator FIN, f - responder FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - initiator data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, L - decap tunnel, M - SMTP data, m - SIP media
       N - inspected by Snort (1 - preserve-connection enabled, 2 - preserve-connection in
 effect)
       n - GUP, O - responder data, o - offloaded,
       P - inside back connection, p - passenger flow
```

```
       q - SQL*Net data, R - initiator acknowledged FIN,
       R - UDP SUNRPC, r - responder acknowledged FIN,
       T - SIP, t - SIP transient, U - up,
       V - VPN orphan, v - M3UA W - WAAS,
       w - secondary domain backup,
       X - inspected by service module,
       x - per session, Y - director stub flow, y - backup stub flow,
       Z - Scansafe redirection, z - forwarding stub flow

TCP outside: 33.33.33.2/80 inside: 1.1.1.2/35226,
    flags UIOBN1, idle 0s, uptime 12s, timeout 1h0m, bytes 698500915
  Initiator: 1.1.1.2, Responder: 33.33.33.2
  Connection lookup keyid: 865399
```

以下是 **show conn detail** 命令的输出示例。此示例显示的是 N4，表示已绕过 Elephant 流的 snort 检查。

```
> show conn detail
0 in use, 19 most used
Inspect Snort:
preserve-connection: 0 enabled, 0 in effect, 1 most enabled, 0 most in effect
Flags: A - awaiting responder ACK to SYN, a - awaiting initiator ACK to SYN,
       B - TCP probe for server certificate,
       b - TCP state-bypass or nailed,
       C - CTIQBE media, c - cluster centralized,
       D - DNS, d - dump, E - outside back connection, e - semi-distributed,
       F - initiator FIN, f - responder FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - initiator data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, L - decap tunnel, M - SMTP data, m - SIP media
       N - inspected by Snort (1 - preserve-connection enabled, 2 - preserve-connection in
 effect,
           3 - elephant-flow, 4 - elephant-flow bypassed, 5 - elephant-flow throttled)
       n - GUP, O - responder data, o - offloaded,
       P - inside back connection, p - passenger flow
       q - SQL*Net data, R - initiator acknowledged FIN,
       R - UDP SUNRPC, r - responder acknowledged FIN,
       T - SIP, t - SIP transient, U - up,
       V - VPN orphan, v - M3UA W - WAAS,
       w - secondary domain backup,
       X - inspected by service module,
       x - per session, Y - director stub flow, y - backup stub flow,
       Z - Scansafe redirection, z - forwarding stub flow

TCP outside_https: 172.16.4.1/80 inside_https: 172.16.77.1/38992,
    flags UIO N1N4, idle 0s, uptime 2m24s, timeout 1h0m, bytes 1891172595
  Initiator: 172.16.77.1, Responder: 172.16.4.1
  Connection lookup keyid: 1556755610
```

此示例显示输出中的 N5，表示对 Elephant 流应用了动态速率限制策略（降低 10%）。

```
> show conn detail
0 in use, 19 most used
Inspect Snort:
preserve-connection: 0 enabled, 0 in effect, 1 most enabled, 0 most in effect
Flags: A - awaiting responder ACK to SYN, a - awaiting initiator ACK to SYN,
       B - TCP probe for server certificate,
       b - TCP state-bypass or nailed,
       C - CTIQBE media, c - cluster centralized,
       D - DNS, d - dump, E - outside back connection, e - semi-distributed,
       F - initiator FIN, f - responder FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - initiator data,
```

```
      i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
      k - Skinny media, L - decap tunnel, M - SMTP data, m - SIP media
      N - inspected by Snort (1 - preserve-connection enabled, 2 - preserve-connection in
 effect,
          3 - elephant-flow, 4 - elephant-flow bypassed, 5 - elephant-flow throttled)
      n - GUP, O - responder data, o - offloaded,
      P - inside back connection, p - passenger flow
      q - SQL*Net data, R - initiator acknowledged FIN,
      R - UDP SUNRPC, r - responder acknowledged FIN,
      T - SIP, t - SIP transient, U - up,
      V - VPN orphan, v - M3UA W - WAAS,
      w - secondary domain backup,
      X - inspected by service module,
      x - per session, Y - director stub flow, y - backup stub flow,
      Z - Scansafe redirection, z - forwarding stub flow

TCP outside_https: 172.16.4.1/80 inside_https: 172.16.77.1/38822,
    flags UIO N1N5, qos-rule-id 20000, idle 0s, uptime 4m8s, timeout 1h0m, bytes 585732628
  Initiator: 172.16.77.1, Responder: 172.16.4.1
  Connection lookup keyid: 1933458538
```

Related Commands

命令	Description
clear conn	清除连接。
clear conn data-rate	清除当前存储的最大数据速率。

show console-output

要显示当前捕获的控制台输出，请使用 **show console-output** 命令。

show console-output

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show console-output** 命令的输出示例。

```
> show console-output
Message #1 : Message #2 : Setting the offload CPU count to 0
Message #3 :
Compiled on Fri 20-May-16 13:36 PDT by builders
Message #4 :
Total NICs found: 14
Message #5 : i354 rev03 Gigabit Ethernet @ irq255 dev 20 index 08 MAC: e865.49b8.97f1
Message #6 : ivshmem rev03 Backplane Data Interface     @ index 09 MAC: 0000.0001.0002
Message #7 : en_vtun rev00 Backplane Control Interface  @ index 10 MAC: 0000.0001.0001
Message #8 : en_vtun rev00 Backplane Int-Mgmt Interface     @ index 11 MAC: 0000.0001.0003
Message #9 : en_vtun rev00 Backplane Ext-Mgmt Interface     @ index 12 MAC: 0000.0000.0000
Message #10 : en_vtun rev00 Backplane Tap Interface     @ index 13 MAC: 0000.0100.0001
Message #11 : Running Permanent Message
#12 : Activation Key: Message
#13 : 0x00000000 Message
#14 : 0x00000000 Message
#15 : 0x00000000 Message
#16 : 0x00000000 Message
#17 : 0x00000000 Message #18 :
Message #19 : The Running Activation Key is not valid, using default settings:
Message #20 :
(...output truncated...)
```

show coredump

要显示数据包引擎核心转储生成的设置，请输入 **show coredump** 命令。

show coredump

Command History

版本	修改
6.2.1	引入了此命令。

使用指南

默认情况下，启用数据包引擎核心转储生成。

此命令仅在Firepower 2100 系列上可用。在不受支持的平台上运行此命令时，系统会返回以下消息：

```
This command is not available on this platform.
```

示例

以下示例显示启用了数据包引擎核心转储生成。

```
> show coredump

Process Type: Coredump State:
packet-engine enabled
```

Related Commands

命令	Description
configure coredump packet-engine	启用或禁用数据包引擎核心转储生成。

show counters

要显示协议栈计数器，请使用 **show counters** 命令。

show counters ［**all** | **summary** | **top** *N*］［**description**］［**detail**］［**protocol** *protocol_name* ［**:***counter_name*］］［ **threshold** *N*］

Syntax Description

all	显示过滤器详细信息。
:counter_name	按名称指定计数器。
description	显示各种计数器和说明。
detail	显示附加计数器信息。
protocol *protocol_name*	显示指定协议的计数器。输入 ? 获取选项列表。
summary	显示计数器摘要。
threshold *N*	仅显示那些等于或高于指定阈值的计数器。范围为 1 到 4294967295。
top *N*	显示等于或高于指定阈值的计数器。范围为 1 到 4294967295。

Command Default

默认值为 **show counters summary detail threshold 1**。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例显示如何显示默认信息。

```
> show counters
Protocol     Counter                                   Value   Context
IP           IN_PKTS                                  785064   Summary
IP           OUT_PKTS                                  19196   Summary
IP           OUT_DROP_DWN                             177099   Summary
IP           TO_ARP                                   785064   Summary
TCP          OUT_PKTS                                  38378   Summary
TCP          SESS_CTOD                                 19189   Summary
TCP          OUT_CLSD                                  19189   Summary
TCP          HASH_ADD                                  19189   Summary
TCP          SND_SYN                                   19189   Summary
SSLERR       BAD_SIGNATURE                                 3   Summary
SSLDEV       NEW_CTX                                       3   Summary
VPIF         BAD_VALUE                                   673   Summary
VPIF         NOT_FOUND                             106843325   Summary
```

命令	Description
clear counters	清除协议堆栈计数器。

show cpu

要显示 CPU 利用率信息，请使用 **show cpu** 命令。

show cpu ［**detailed** | **external** | **profile** ［**dump**］ | **system** ［*processor_num*］］
show cpu core ［**all** | *core_id*］
show cpu usage ［**detailed** | **core** ［**all** | *core_id*］ ］

Syntax Description

core [**all** | *core_id*]	显示 每个核心的 CPU 统计信息。您可以查看所有核心（默认）或按编号指定核心。使用不带参数的关键字可查看设备上可用的核心编号。核心编号从 0 开始。 **show cpu core** 和 **show cpu usage core** 命令提供相同的信息。
detailed	（可选）显示 CPU 使用内部详细信息。
external	（可选）显示外部进程的 CPU 使用情况。
profile [**dump**]	（可选）显示CPU分析数据。包含 **dump** 关键字可查看分析数据的转储。
system [*processor_num*]	（可选）显示与整个系统相关的信息。您可以选择包含处理器编号，以查看特定处理器的信息。使用不带 关键字的 命令可查看可用处理器（称为 CPU）的数量。处理器编号从 0 开始。因此，如果输出显示有 8 个 CPU，则系统的有效编号为 0-7。
usage	（可选）显示 CPU 使用率。这是默认选项。

Command History

版本	修改
6.1	引入了此命令。

使用指南

每五秒使用负载近似值和通过进一步将此近似值输入以下两个移动平均数来计算 CPU 使用率。

您可以将 **show cpu profile dump** 命令与 **cpu profile activate** 命令结合使用，以收集信息以供 TAC 用于排除 CPU 问题。 **show cpu profile dump** 命令输出为十六进制格式。

对于 **detailed** 和 **core** 视图，当整体 CPU 使用率较低时，核心的使用率通常为零。

对于 threat defense virtual， **show cpu** 命令还会根据 vCPU 平台许可证限制显示分配给 VM 的 CPU 数量是否在允许的限制范围内。状态可以是“合规”、“不合规：过度调配”或“不合规：调配不足”。此信息可能不准确。

示例

以下示例展示如何显示 CPU 利用率：

```
> show cpu
```

```
CPU utilization for 5 seconds = 18%; 1 minute: 18%; 5 minutes: 18%
```

以下示例展示如何显示详细的 CPU 利用率信息：

```
> show cpu detailed
Break down of per-core data path versus control point cpu usage:
Core         5 sec           1 min           5 min
Core 0       0.0 (0.0 + 0.0)  3.3 (0.0 + 3.3)  2.4 (0.0 + 2.4)
Current control point elapsed versus the maximum control point elapsed for:
      5 seconds = 99.0%; 1 minute: 99.8%; 5 minutes: 95.9%
CPU utilization of external processes for:
      5 seconds = 0.2%; 1 minute: 0.0%; 5 minutes: 0.0%
Total CPU utilization for:
      5 seconds = 0.2%; 1 minute: 3.3%; 5 minutes: 2.5%
```

注释 “Current control point elapsed versus the maximum control point elapsed for”语句意味着在定义的时间段内将当前控制点负载与看到的最大负载进行比较。这是一个比率而非绝对数。数字 99% 与 5 秒间隔对应意味着当前控制点负载为在此 5 秒间隔内可见的最大负载的 99%。如果负载一直继续增加，则它会始终保持在 100%。但是，由于尚未定义最大绝对值，实际 CPU 可能仍然具有许多可用容量。

以下示例显示如何显示系统级 CPU 使用情况。请注意第一行中的“(2 CPU)”指示。这是此设备上的处理器数量。

```
> show cpu system
Linux 3.10.62-ltsi-WR6.0.0.27_standard (ftd1.example.com)        10/20/16        _x86_64_   (2 CPU)

Time         CPU    %usr   %nice    %sys %iowait    %irq   %soft  %steal  %guest  %gnice   %idle
15:48:26     all   50.36    0.00   10.04    0.78    0.00    0.03    0.00    0.00    0.00   38.79
```

下表对 **show cpu system** 输出字段进行了解释。

表 *24:* 显示 *CPU* 系统字段

字段	Description
Time	确定这些数字的时间。
CPU	处理器编号。
%user	在用户级别（应用）执行时发生的 CPU 利用率。
%nice	在具有 nice 优先级的用户级别执行时发生的 CPU 利用率。
%sys	在系统级别（内核）执行时发生的 CPU 利用率百分比。其中不包括中断或软中断的修复时间。软中断（软件中断）是可以同时在多个CPU上运行的32个枚举软件中断之一。
%iowait	当系统有未处理的磁盘 I/O 请求时 CPU 空闲时间的百分比。

字段	Description
%irq	CPU 修复中断所用时间的百分比。
%soft	CPU 修复软件中断所用时间的百分比。
%steal	当虚拟机监控程序为其他虚拟处理器提供服务时，虚拟 CPU 被强制等待时间的百分比。
%guest	CPU 运行虚拟处理器所用时间的百分比。
%gnice	在具有 nice 优先级的访客级别执行时发生的 CPU 利用率。
%idle	当系统没有未处理的磁盘 I/O 请求时 CPU 空闲时间的百分比。

默认情况下，以下示例激活分析器并指示其存储 1000 份采样。接下来， **show cpu profile** 命令显示正在进行分析。等待一段时间后，下一个 **show cpu profile** 命令显示分析已完成。最后，我们使用 **show cpu profile dump** 命令获取结果。复制输出并将其提供给思科技术支持。您可能需要记录 SSH 会话以获取完整输出。

```
> cpu profile activate
Activated CPU profiling for 1000 samples.
Use "show cpu profile" to display the progress or "show cpu profile dump" to interrupt
profiling and display the incomplete results.
> show cpu profile
CPU profiling started: 16:13:48.279 UTC Thu Oct 20 2016
CPU profiling currently in progress:
    Core 0: 501 out of 1000 samples collected.
    CP: 586 out of 1000 samples collected.
Use "show cpu profile dump" to see the results after it is complete or to interrupt
profiling and display the incomplete results.
> show cpu profile
CPU profiling started: 16:13:48.279 UTC Thu Oct 20 2016
CPU Profiling has stopped.
    Core 0 done with 1000 samples
    CP done with 1000 samples
Use "show cpu profile dump" to see the results.
> show cpu profile dump
(...output omitted...)
```

Related Commands

命令	Description
clear cpu profile	清除 CPU 分析数据。
cpu profile activate	激活 CPU 分析。
show counters	显示协议栈计数器。

show crashinfo

要显示闪存中存储的崩溃文件的内容，请输入 **show crashinfo** 命令。

show crashinfo ［**console** | **module** 数字 | **save** | **webvpn** ［**detailed**］］

Syntax Description

console	（可选）显示 crashinfo 控制台输出的状态。
module *number*	（可选）显示从指定模块检索的崩溃信息。按编号指示模块，例如 1。
save	（可选）显示设备是否已配置为将崩溃信息保存到闪存。
webvpn [**detailed**]	（可选）显示 threat defense 崩溃恢复转储。

Command History

版本	修改
6.1	引入了此命令。

使用指南

如果崩溃文件来自测试崩溃（从 **crashinfo test** 命令生成），则崩溃文件的第一个字符串为“: Saved_Test_Crash”而最后一个字符串为“: End_Test_Crash”。如果崩溃文件来自真实崩溃，则崩溃文件的第一个字符串为“: Saved_Crash”而最后一个字符串为“: End_Crash”。（这包括因使用 **crashinfo force page-fault** 或 **crashinfo force watchdog** 命令而导致的崩溃）。

FIPS 140-2 的合规性禁止在加密边界（机箱）以外分布关键安全参数（密钥、密码等）。设备由于维护或检查堆故障崩溃时，堆栈或内存区域可能会转储到包含敏感数据的控制台。此输出在FIPS模式下必须抑制。

示例

以下示例显示没有 crashinfo 信息。

```
> show crashinfo
------------------ show crashinfo module 1 ------------------
INFO: This module has no crashinfo available.
```

以下示例展示如何显示当前崩溃信息配置：

```
> show crashinfo save
crashinfo save enable
```

以下示例显示 crashinfo 控制台输出的状态。

```
> show crashinfo console
crashinfo console enable
```

以下示例展示崩溃文件测试的输出。此测试实际上不会使threat defense设备崩溃。它提供一个模拟的示例文件。

```
> crashinfo test
> show crashinfo
: Saved_Test_Crash
Thread Name: ci/console (Old pc 0x001a6ff5 ebp 0x00e88920)
Traceback:
0: 00323143
1: 0032321b
2: 0010885c
(...Remaining output truncated...)
```

Related Commands

命令	Description
clear crashinfo	删除崩溃文件的内容。
crashinfo force	强制 threat defense 设备崩溃。
crashinfo test	测试 threat defense 设备将故障信息保存到闪存中文件的能力。

show crypto accelerator load-balance

要显示硬件加密加速器 MIB 中特定于加速器的负载均衡信息，请使用 **show crypto accelerator load-balance** 命令。

show crypto accelerator load-balance ［**ipsec** | **ssl** | **detail** ［**ipsec | ssl**］］

Syntax Description

detail	（可选）显示详细信息。您可以在此选项后添加 **ipsec** 或 **ssl** 关键字。
ipsec	（可选）显示加密加速器 IPSec 负载均衡详细信息。
ssl	（可选）显示加密加速器 SSL 负载均衡详细信息。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例显示全局加密加速器负载均衡统计信息：

```
> show crypto accelerator load-balance

                  Crypto IPSEC Load Balancing Stats:
                  ==================================

Engine      Crypto Cores             IPSEC Sessions          Active Session
                                                             Distribution (%)
======     ==============      ============================   ================
  0        IPSEC 1, SSL 1      Total:     0  Active:     0          0.0%

Commands Completed       1 second         5 second         60 second
==================       ========         ========         =========
 Engine 0 (load)            0.0%             0.0%             0.0%

Encrypted Data           1 second         5 second         60 second
==================       ========         ========         =========
 Engine 0 (load)            0.0%             0.0%             0.0%

Decrypted Data           1 second         5 second         60 second
==================       ========         ========         =========
 Engine 0 (load)            0.0%             0.0%             0.0%

Engine 0 Per Core Load Balancing Stats:
=======================================

Commands Completed       1 second         5 second        60 second
==================       ========         ========         =========
 IPSec ring 0   (load)      0.0%             0.0%             0.0%

Encrypted Data           1 second         5 second         60 second
==================       ========         ========         =========
 IPSec ring 0   (load)      0.0%             0.0%             0.0%
```

```
Decrypted Data           1 second         5 second        60 second
==================       ========         ========         =========
 IPSec ring 0   (load)      0.0%             0.0%             0.0%

                  Crypto SSL Load Balancing Stats:
                  ================================

Engine      Crypto Cores             SSL Sessions            Active Session
                                                             Distribution (%)
======     ==============      ============================   ================
  0        IPSEC 1, SSL 1      Total:     0  Active:     0          0.0%

Commands Completed       1 second         5 second         60 second
==================       ========         ========         =========
 Engine 0 (load)            0.0%             0.0%             0.0%

Encrypted Data           1 second         5 second         60 second
==================       ========         ========         =========
 Engine 0 (load)            0.0%             0.0%             0.0%

Decrypted Data           1 second         5 second         60 second
==================       ========         ========         =========
 Engine 0 (load)            0.0%             0.0%             0.0%

Engine 0 Per Core Load Balancing Stats:
=======================================

Commands Completed       1 second         5 second        60 second
==================       ========         ========         =========
 Admin ring 0   (load)      0.0%             0.0%             0.0%

Encrypted Data           1 second         5 second         60 second
==================       ========         ========         =========
 Admin ring 0   (load)      0.0%             0.0%             0.0%

Decrypted Data           1 second         5 second        60 second
==================       ========         ========         =========
 Admin ring 0   (load)      0.0%             0.0%             0.0%
```

Related Commands

命令	Description
clear crypto accelerator statistics	清除加密加速器 MIB 中的全局统计信息和加速器特定统计信息。
clear crypto protocol statistics	清除加密加速器 MIB 中的协议特定统计信息。
show crypto protocol statistics	显示来自加密加速器 MIB 的协议特定统计信息。

show crypto accelerator statistics

要显示硬件加密加速器 MIB 中的全局和特定于加速器的统计信息，请使用 **show crypto accelerator statistics** 命令。

show crypto accelerator statistics

Command History

版本	修改
6.1	引入了此命令。

使用指南

输出统计信息定义如下：

加速器 0 显示基于软件的加密引擎的统计信息。

加速器 1 显示基于硬件的加密引擎的统计信息。

RSA 统计信息显示 2048 位密钥的 RSA 操作，该操作默认情况下在软件中执行。这意味着当您拥有 2048 位密钥时，IKE/SSL VPN 在 IPsec/SSL 协商阶段在软件中执行 RSA 操作。实际的 IPsec/SSL 流量仍使用硬件处理。如果有许多同时开始的并发会话，这可能会导致高 CPU，从而可能导致多个 RSA 密钥操作和高 CPU。如果由于此原因进入高 CPU 情况，则应使用 1024 位密钥在硬件中处理 RSA 密钥操作。为此，您必须重新注册身份证书。在版本 8.3(2) 或更高版本中，您还可以在 5510-5550 平台上使用 crypto engine large-mod-accel 命令，以在硬件中执行这些操作。

如果使用 2048 位 RSA 密钥并在软件中执行 RSA 处理，您可以使用 CPU 评测来确定哪些功能导致高 CPU 使用率。通常，bn_* 和 BN_* 函数是用于 RSA 的大型数据集的数学运算，对在软件中执行 RSA 操作期间检查 CPU 使用率最有用。例如：

```
@@@@@@@@@@@@@@@@@@@@..............................  36.50% : _bn_mul_add_words
@@@@@@@@@@.....................................  19.75% : _bn_sqr_comba8
```

Diffie-Hellman 统计信息显示在软件中执行模数大小大于 1024 的任何加密操作（例如，DH5 (Diffie-Hellman 组 5) 使用 1536）。如果是这样，则 2048 位密钥证书将在软件中进行处理，因此在运行许多会话时可导致高 CPU 使用率。

DSA 统计信息在两个阶段显示密钥生成。第一个阶段是选择算法参数，该参数可在系统的不同用户之间共享。第二个阶段计算单一用户的专用密钥和公共密钥。

SSL 统计信息显示到硬件加密加速器的 SSL 事务中涉及的处理器密集公共密钥加密算法记录。

RNG 统计数据显示发送方和接收方的记录，可以自动生成相同的随机号码用作密钥。

示例

以下示例显示全局加密加速器统计信息：

```
> show crypto accelerator statistics

Crypto Accelerator Status
```

```
-------------------------
[Capacity]
   Supports hardware crypto: True
   Supports modular hardware crypto: False
   Max accelerators: 1
   Max crypto throughput: 100 Mbps
   Max crypto connections: 750
[Global Statistics]
   Number of active accelerators: 1
   Number of non-operational accelerators: 0
   Input packets: 700
   Input bytes: 753488
   Output packets: 700
   Output error packets: 0
   Output bytes: 767496
[Accelerator 0]
   Status: Active
   Software crypto engine
   Slot: 0
   Active time: 167 seconds
   Total crypto transforms: 7
   Total dropped packets: 0
   [Input statistics]
      Input packets: 0
      Input bytes: 0
      Input hashed packets: 0
      Input hashed bytes: 0
      Decrypted packets: 0
      Decrypted bytes: 0
   [Output statistics]
      Output packets: 0
      Output bad packets: 0
      Output bytes: 0
      Output hashed packets: 0
      Output hashed bytes: 0
      Encrypted packets: 0
      Encrypted bytes: 0
   [Diffie-Hellman statistics]
      Keys generated: 0
      Secret keys derived: 0
   [RSA statistics]
      Keys generated: 0
      Signatures: 0
      Verifications: 0
      Encrypted packets: 0
      Encrypted bytes: 0
      Decrypted packets: 0
      Decrypted bytes: 0
   [DSA statistics]
      Keys generated: 0
      Signatures: 0
      Verifications: 0
   [SSL statistics]
      Outbound records: 0
      Inbound records: 0
   [RNG statistics]
      Random number requests: 98
      Random number request failures: 0
[Accelerator 1]
   Status: Active
   Encryption hardware device : Cisco ASA-55x0 on-board accelerator
(revision 0x0)
                            Boot microcode   : CNlite-MC-Boot-Cisco-1.2
                            SSL/IKE microcode: CNlite-MC-IPSEC-Admin-3.03
```

```
                          IPsec microcode  : CNlite-MC-IPSECm-MAIN-2.03
Slot: 1
Active time: 170 seconds
Total crypto transforms: 1534
Total dropped packets: 0
[Input statistics]
   Input packets: 700
   Input bytes: 753544
   Input hashed packets: 700
   Input hashed bytes: 736400
   Decrypted packets: 700
   Decrypted bytes: 719944
[Output statistics]
   Output packets: 700
   Output bad packets: 0
   Output bytes: 767552
   Output hashed packets: 700
   Output hashed bytes: 744800
   Encrypted packets: 700
   Encrypted bytes: 728352
[Diffie-Hellman statistics]
   Keys generated: 97
   Secret keys derived: 1
[RSA statistics]
   Keys generated: 0
   Signatures: 0
   Verifications: 0
   Encrypted packets: 0
   Encrypted bytes: 0
   Decrypted packets: 0
   Decrypted bytes: 0
[DSA statistics]
   Keys generated: 0
   Signatures: 0
   Verifications: 0
[SSL statistics]
   Outbound records: 0
   Inbound records: 0
[RNG statistics]
   Random number requests: 1
   Random number request failures: 0
```

下表对输出进行了解释。

输出	Description
Capacity	此部分涉及 threat defense 设备能够支持的加密加速。
Supports hardware crypto	(True/False) threat defense 设备可以支持硬件加密加速。
Supports modular hardware crypto	(True/False) 任何支持的硬件加密加速器均可作为单独的插件卡或模块插入。
Max accelerators	threat defense 设备支持的最大硬件加密加速器数。
Mac crypto throughput	设备的最大额定 VPN 吞吐量。
Max crypto connections	设备的最大支持 VPN 隧道数。

输出	Description
Global Statistics	此部分涉及设备中的组合硬件加密加速器。
Number of active accelerators	活动硬件加速器数。活动硬件加速器已初始化并可用于处理加密命令。
Number of non-operational accelerators	非活动硬件加速器数。已检测到非活动硬件加速器，但尚未完成初始化，或已失效且不再可用。
Input packets	所有硬件加密加速器处理的入站数据包数。
Input bytes	已处理入站数据包中数据的字节数。
Output packets	所有硬件加密加速器处理的出站数据包数。
Output error packets	其中检测到错误的所有硬件加密加速器处理的出站数据包数。
Output bytes	已处理出站数据包中数据的字节数。
Accelerator 0	每个部分均涉及加密加速器。第一个（加速器 0）始终为软件加密引擎。尽管并非硬件加速器，但 threat defense 使用它来执行特定加密任务，并且其统计信息在此处显示。加速器 1 及更高编号始终均为硬件加密加速器。
Status	加速器的状态，指示加速器是已初始化、活动还是已失效。
Software crypto engine	加速器类型和固件版本（如果适用）。
Slot	加速器的插槽编号（如果适用）。
Active time	加速器处于活动状态的时长。
Total crypto transforms	加速器执行的加密命令总数。
Total dropped packets	加速器由于错误而丢弃的数据包总数。
Input statistics	本部分涉及加速器处理的输入流量。输入流量被视为必须进行解密和/或验证的密文。
Input packets	加速器已处理的输入数据包数。
Input bytes	加速器已处理的输入字节数。
Input hashed packets	加速器已执行散列操作的数据包数。
Input hashed bytes	加速器已执行散列操作的字节数。
Decrypted packets	加速器已执行对称解密操作的数据包数。
Decrypted bytes	加速器已执行对称解密操作的字节数。

输出	Description
Output statistics	本部分涉及加速器已处理的输出流量。输出流量被视为必须进行加密和/或散列的明文。
Output packets	加速器已处理的输入数据包数。
Output bad packets	其中检测到错误的加速器已处理的输出数据包数。
Output bytes	加速器已处理的输出字节数。
Output hashed packets	加速器已执行出站散列操作的数据包数。
Output hashed bytes	加速器已执行出站散列操作的字节数。
Encyrpted packets	加速器已执行对称加密操作的数据包数。
Encyrpted bytes	加速器已执行对称加密操作的字节数。
Diffie-Hellman statistics	本部分涉及 Diffie-Hellman 密钥交换操作。
Keys generated	加速器已生成的 Diffie-Hellman 密钥集数。
Secret keys derived	加速器已衍生的 Diffie-Hellman 共享密钥数。
RSA statistics	本部分涉及 RSA 加密操作。
Keys generated	加速器已生成的 RSA 密钥集数。
Signatures	加速器已执行的 RSA 签名操作数。
Verifications	加速器已执行的 RSA 签名验证数。
Encrypted packets	加速器已执行 RSA 加密操作的数据包数。
Decrypted packets	加速器已执行 RSA 解密操作的数据包数。
Decrypted bytes	加速器已执行 RSA 解密操作的数据字节数。
DSA statistics	本部分涉及 DSA 操作。请注意，自版本 8.2 起不再支持 DSA，因此不再显示这些统计信息。
Keys generated	加速器生成的 DSA 密钥集的数量。
Signatures	加速器已执行的 DSA 签名操作的数量。
Verifications	加速器已执行的 DSA 签名验证的数量。
SSL statistics	本部分涉及 SSL 记录处理操作。
Outbound records	加速器已加密和已验证的 SSL 记录数。

输出	Description
Inbound records	加速器已解密和已验证的 SSL 记录数。
RNG statistics	本部分涉及随机号码生成。
Random number requests	加速器的随机号码请求数。
Random number request failures	对未成功的加速器的随机号码请求数。

在支持 IPsec 流分流的平台上，输出显示已分流的流的统计信息，而全局计数器显示设备上所有加速器引擎的所有分流和非分流流量的总和。

```
> show crypto accelerator statistics

Crypto Accelerator Status
-------------------------
[Capability]
   Supports hardware crypto: True
   Supported TLS Offload Mode: HARDWARE
   Supports modular hardware crypto: False
   Max accelerators: 3
   Max crypto throughput: 3000 Mbps
   Max crypto connections: 3000
[Global Statistics]
   Number of active accelerators: 2
   Number of non-operational accelerators: 0
   Input packets: 108
   Input bytes: 138912
   Output packets: 118
   Output error packets: 0
   Output bytes: 142329

[Accelerator 0]
   Status: OK
   Software crypto engine
   Slot: 0
   Active time: 489 seconds
   Total crypto transforms: 2770
   Total dropped packets: 0
   [Input statistics]
      Input packets: 0
      Input bytes: 19232
      Input hashed packets: 0
      Input hashed bytes: 0
      Decrypted packets: 0
      Decrypted bytes: 19232
   [Output statistics]
      Output packets: 0
      Output bad packets: 0
      Output bytes: 18784
      Output hashed packets: 0
      Output hashed bytes: 0
      Encrypted packets: 0
      Encrypted bytes: 18784
   [Diffie-Hellman statistics]
      Keys generated: 0
      Secret keys derived: 0
   [RSA statistics]
      Keys generated: 1
```

```
      Signatures: 1
      Verifications: 1
      Encrypted packets: 1
      Encrypted bytes: 28
      Decrypted packets: 1
      Decrypted bytes: 256
   [ECDSA statistics]
      Keys generated: 13
      Signatures: 12
      Verifications: 15
   [EDDSA statistics]
      Keys generated: 0
      Signatures: 0
      Verifications: 0
   [SSL statistics]
      Outbound records: 0
      Inbound records: 0
   [RNG statistics]
      Random number requests: 0
      Random number request failures: 0
   [HMAC statistics]
      HMAC requests: 54

[Accelerator 1]
   Status: OK
   Encryption hardware device : Cisco ASA Crypto on-board accelerator (revision 0x1)
                            AE microcode        : CNN5x-MC-AE-MAIN-0007
                            SE SSL microcode    : CNN5x-MC-SE-SSL-0018
   Slot: 1
   Active time: 497 seconds
   Total crypto transforms: 2910
   Total dropped packets: 0
   [Input statistics]
      Input packets: 4
      Input bytes: 13056
      Input hashed packets: 0
      Input hashed bytes: 0
      Decrypted packets: 4
      Decrypted bytes: 6528
   [Output statistics]
      Output packets: 14
      Output bad packets: 0
      Output bytes: 20786
      Output hashed packets: 0
      Output hashed bytes: 0
      Encrypted packets: 14
      Encrypted bytes: 10393
   [Offloaded Input statistics]
      Input packets: 106
      Input bytes: 115328
      Input hashed packets: 0
      Input hashed bytes: 0
      Decrypted packets: 107
      Decrypted bytes: 112992
   [Offloaded Output statistics]
      Output packets: 107
      Output bytes: 116416
      Output hashed packets: 0
      Output hashed bytes: 0
      Encrypted packets: 107
      Encrypted bytes: 112992
   Total dropped packets: 0
   [Diffie-Hellman statistics]
      Keys generated: 194
```

```
   Secret keys derived: 1
[RSA statistics]
   Keys generated: 0
   Signatures: 2
   Verifications: 1
   Encrypted packets: 3
   Encrypted bytes: 162
   Decrypted packets: 2
   Decrypted bytes: 512
[ECDSA statistics]
   Keys generated: 0
   Signatures: 0
   Verifications: 0
[EDDSA statistics]
   Keys generated: 0
   Signatures: 0
   Verifications: 0
[SSL statistics]
   Outbound records: 14
   Inbound records: 4
[RNG statistics]
   Random number requests: 34
   Random number request failures: 0
[HMAC statistics]
   HMAC requests: 26
```

Related Commands

命令	Description
clear crypto accelerator statistics	清除加密加速器 MIB 中的全局统计信息和加速器特定统计信息。
clear crypto protocol statistics	清除加密加速器 MIB 中的协议特定统计信息。
show crypto protocol statistics	显示来自加密加速器 MIB 的协议特定统计信息。

show crypto accelerator usage

此命令允许您查看 TLS 加密加速 所有核心的核心使用率和平均使用率。此命令并非在所有硬件平台上都可用。

有关 TLS 加密加速的准则和限制，请参阅 管理中心 配置指南。

show crypto accelerator usage [**detail**]

Syntax Description

detail	（可选。）显示更多详细信息，这在受管设备具有 威胁防御 容器实例时非常有用。

Command History

版本	修改
6.6	引入了此命令。

使用指南

显示每个核心的核心使用率和每个核心的平均使用率。根据您的硬件型号， 命令可能不可用，并且可能显示不同的统计信息。

示例

以下是查看 TLS 加密加速核心使用情况的示例：

```
> show crypto accelerator usage
Crypto engine 0: 64 ADMIN SE cores, utilization 18.8%
Crypto engine 1: 64 ADMIN SE cores, utilization 17.2%
Total 128 ADMIN SE cores, utilization18%
Crypto engine 0: 64 ADMIN AE cores, utilization 0%
Crypto engine 1: 64 ADMIN AE cores, utilization 0%
Total 128 ADMIN AE cores, utilization0%
```

以下是查看详细使用信息的示例：

```
 show crypto accelerator usage detail
Crypto engine 0: 64 IPSec/SSL crypto cores, utilization 18.8%
Crypto engine 1: 64 IPSec/SSL crypto cores, utilization 17.2%
Total 128 IPSec/SSL cryto cores, utilization 18%
Crypto engine 0: 64 Asymmetric crypto cores, utilization 0%
Crypto engine 1: 64 Asymmetric crypto cores, utilization 0%
Total 128 Asymmetric crypto cores, utilization 0%
```

show crypto ca certificates

要显示与特定信任点关联的证书或显示系统上安装的所有证书，请使用 **show crypto ca certificates** 命令。

show crypto ca certificates ［*trustpointname*］

Syntax Description

trustpointname	（可选）信任点的名称。如果您没有指定名称，此命令将显示threat defense设备上安装的所有证书。

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show crypto ca certificates** 命令的输出示例：

```
>show crypto ca certificates tp1
CA Certificate
    Status: Available
    Certificate Serial Number 2957A3FF296EF854FD0D6732FE25B45
    Certificate Usage: Signature
    Issuer:
        CN = ms-root-sha-06-2004
        OU = rootou
        O = cisco
        L = franklin
        ST - massachusetts
        C = US
        EA = a@b.con
   Subject:
        CN = ms-root-sha-06-2004
        OU = rootou
        O = cisco
        L = franklin
        ST = massachusetts
        C = US
        EA = example.com
   CRL Distribution Point
        ldap://w2kadvancedsrv/CertEnroll/ms-root-sha-06-2004.crl
   Validity Date:
        start date: 14:11:40 UTC Jun 26 2004
        end date: 14:01:30 UTC Jun 4 2022
   Associated Trustpoints: tp2 tp1
```

show crypto ca crls

要显示所有缓存的证书撤销列表 (CRL) 或显示为指定信任点缓存的所有 CRL，请使用 **show crypto ca crl** 命令。

show crypto ca crls [**trustpool** | **trustpoint** *trustpointname*]

Syntax Description

trustpoint *trustpointname*	（可选）信任点的名称。如果您没有指定名称，此命令将显示 threat defense 设备上缓存的所有 CRL。
trustpool	显示所有与信任池相关的 CRL。

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show crypto ca crl** 命令的输出示例：

```
> show crypto ca crl trustpoint tp1
CRL Issuer Name:
    cn=ms-sub1-ca-5-2004,ou=Franklin DevTest,o=Cisco
Systems,l=Franklin,st=MA,c=US,ea=user@example.com
    LastUpdate: 19:45:53 UTC Dec 24 2004
    NextUpdate: 08:05:53 UTC Jan 1 2005
    Retrieved from CRL Distribution Point:
      http://win2k-ad2.frk-ms-pki.cisco.com/CertEnroll/ms-sub1-ca-5-2004.crl
    Associated Trustpoints: tp1
```

show crypto ca trustpoints

要显示 CA 信任点，请使用 **show crypto ca trustpoints** 命令。

show crypto ca trustpoints ［*trustpoint_name*］

Syntax Description

trustpoint_name	（可选）要显示的信任点的名称。

Command Default

如果不指定信任点，则显示所有信任点。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例显示如何显示 CA 信任点。

```
> show crypto ca trustpoints
Trustpoint ftd-self:
    Configured for self-signed certificate generation.
```

show crypto ca trustpool

要显示构成信任池的证书，请使用 **show crypto ca trustpool** 命令。

show crypto ca trustpool ［**detail** | **policy**］

Syntax Description

detail	（可选）显示证书详细信息。
policy	（可选）显示已配置的信任池策略。

Command Default

此命令显示所有信任池证书的缩略显示。指定 **detail** 选项后，将包含详细信息。

Command History

版本	修改
6.1	引入了此命令。

使用指南

show crypto ca trustpool 命令的输出包括每个证书的指纹值。删除操作需要这些值。

示例

以下示例显示如何显示信任池中的证书。

```
> show crypto ca trustpool
CA Certificate
Status: Available
Certificate Serial Number: 6c386c409f4ff4944154635da520ed4c
Certificate Usage: Signature
Public Key Type: RSA (2048 bits)
Signature Algorithm: SHA1 with RSA Encryption
Issuer Name: cn=bxb2008-root
dc=bdb2008
dc=mycompany
dc=com
Subject Name:
cn=bxb2008-root
dc=bxb2008
dc=cisco
dc=com
Validity Date:
start date:17:21:06 EST Jan 14 2009
end date:17:31:06 EST Jan 14 2024
CA Certificate
Status: Available
Certificate Serial Number: 58d1c756000000000059
Certificate Usage: Signature
Public Key Type: RSA (2048 bits)
Signature Algorithm: SHA1 with RSA Encryption
Issuer Name:
cn=bxb2008-root
dc=bxb2008
dc=mycompany
dc=com
Subject Name:
```

```
cn=BXB2008SUB1-CA
dc=bxb2008
dc=cisco
dc=com
OCSP AIA:
URL: http://bxb2008-1.bxb2008.mycompany.com/ocsp
CRL Distribution Points:
(1) http://bxb2008-1.bxb2008.mycompany.com/CertEnroll/bxb2008-root.crl
Validity Date:
start date:11:54:34 EST May 18 2009
end date:12:04:34 EST May 18 2011
```

以下示例显示如何显示信任池策略。

```
> show crypto ca trustpool policy
800 trustpool certificates installed
Trustpool auto import statistics:
 Last import result: SUCCESS
 Next scheduled import at 22:00:00 Tues Jul 21 2015
Trustpool Policy
Trustpool revocation checking is disabled
CRL cache time: 123 seconds
CRL next update field: required and forced
Automatic import of trustpool certificates is enabled
Automatic import URL: http://www.thawte.com
Download time: 22:00:00
Policy overrides:
map: map1
match:issuer-name eq cn=Mycompany Manufacturing CA
match:issuer-name eq cn=Mycompany CA
action:skip revocation-check
map: map2
match: issuer-name eq cn=mycompany Manufacturing CA
match: issuer-name eq cn=mycompany CA2
action: allowed expired certificates
```

Related Commands

命令	Description
clear crypto ca trustpool	从信任池删除所有证书。

show crypto debug-condition

要显示当前配置的过滤器、不匹配状态以及 IPsec 和 ISAKMP 调试消息的错误状态，请使用 **show crypto debug-condition** 命令。

show crypto debug-condition

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例展示过滤条件：

```
> show crypto debug-condition
Crypto conditional debug is turned ON
IKE debug context unmatched flag:  OFF
IPsec debug context unmatched flag:  ON
IKE peer IP address filters:
1.1.1.0/24   2.2.2.2
IKE user name filters:
my_user
```

Related Commands

命令	Description
debug crypto condition	设置 IPsec 和 ISAKMP 调试消息的过滤条件。
debug crypto condition error	显示调试消息是否已经指定过滤条件。
debug crypto condition unmatched	显示 IPsec 和 ISAKMP 的调试消息（未包含足够的情景信息用于过滤）。

show crypto ikev1

要显示有关互联网密钥交换版本 1 (IKEv1) 的信息，请使用 **show crypto ikev1** 命令。

show crypto ikev1 {**ipsec-over-tcp** | **sa** [**detail**] | **stats**}

Syntax Description

ipsec-over-tcp	显示 IPsec over TCP 数据。
sa [**detail**]	显示有关 IKEv1 运行时安全关联 (SA) 数据库的信息。包括 **detail** 关键字以显示有关 SA 数据库的详细输出。
stats	显示 IKEv1 统计信息。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例显示有关 SA 数据库的详细信息。如果不包括 detail 关键字，则仅显示 IKE Peer、Type、Dir、Rky 和 State 列。

```
> show crypto ikev1 sa detail
IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
1 209.165.200.225 User  Resp  No   AM_Active  3des    SHA   preshrd 86400

IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
2 209.165.200.226 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
3 209.165.200.227 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
4 209.165.200.228 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400
```

以下示例显示 IPsec over TCP 数据：

```
> show crypto ikev1 ipsec-over-tcp
Global IKEv1 IPSec over TCP Statistics
--------------------------------
Embryonic connections: 0
Active connections: 0
Previous connections: 0
Inbound packets: 0
Inbound dropped packets: 0
Outbound packets: 0
Outbound dropped packets: 0
RST packets: 0
Recevied ACK heart-beat packets: 0
Bad headers: 0
Bad trailers: 0
```

```
Timer failures: 0
Checksum errors: 0
Internal errors: 0
```

以下示例显示全局 IKEv1 统计信息：

```
> show crypto ikev1 stats
Global IKEv1 Statistics
  Active Tunnels:              0
  Previous Tunnels:            0
  In Octets:                   0
  In Packets:                  0
  In Drop Packets:             0
  In Notifys:                  0
  In P2 Exchanges:             0
  In P2 Exchange Invalids:     0
  In P2 Exchange Rejects:      0
  In P2 Sa Delete Requests:    0
  Out Octets:                  0
  Out Packets:                 0
  Out Drop Packets:            0
  Out Notifys:                 0
  Out P2 Exchanges:            0
  Out P2 Exchange Invalids:    0
  Out P2 Exchange Rejects:     0
  Out P2 Sa Delete Requests:   0
  Initiator Tunnels:           0
  Initiator Fails:             0
  Responder Fails:             0
  System Capacity Fails:       0
  Auth Fails:                  0
  Decrypt Fails:               0
  Hash Valid Fails:            0
  No Sa Fails:                 0

IKEV1 Call Admission Statistics
  Max In-Negotiation SAs:               50
  In-Negotiation SAs:                    0
  In-Negotiation SAs Highwater:          0
  In-Negotiation SAs Rejected:           0
```

Related Commands

命令	Description
show crypto ikev2 sa	显示 IKEv2 运行时 SA 数据库。
show running-config crypto isakmp	显示所有活动的 ISAKMP 配置。

show crypto ikev2

要显示有关互联网密钥交换版本 2 (IKEv2) 的信息，请使用 **show crypto ikev2** 命令。

show crypto ikev2 {**sa** [**detail**] | **stats**}

Syntax Description

sa [**detail**]	显示有关 IKEv2 运行时安全关联 (SA) 数据库的信息。包括 **detail** 关键字以显示有关 SA 数据库的详细输出。
stats	显示 IKEv2 统计信息。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例显示有关 SA 数据库的详细信息：

```
> show crypto ikev2 sa detail
IKEv2 SAs:
Session-id:1, Status:UP-ACTIVE, IKE count:1, CHILD count:1
Tunnel-id            Local              Remote              Status   Role
671069399            10.0.0.0/500       10.255.255.255/500  READY    INITIATOR
      Encr: AES-GCM, keysize: 256, Hash: N/A, DH Grp:20, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/188 sec
      Session-id: 1
      Status Description: Negotiation done
      Local spi: 80173A0373C2D403       Remote spi: AE8AEFA1B97DBB22
      Local id: asa
      Remote id: asa1
      Local req mess id: 8              Remote req mess id: 7
      Local next mess id: 8             Remote next mess id: 7
      Local req queued: 8               Remote req queued: 7
      Local window: 1                   Remote window: 1
      DPD configured for 10 seconds, retry 2
      NAT-T is not detected
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 0.0.0.0/0 - 255.255.255.255/65535
          ESP spi in/out: 0x242a3da5/0xe6262034
          AH spi in/out: 0x0/0x0
          CPI in/out: 0x0/0x0
          Encr: AES-GCM, keysize: 128, esp_hmac: N/A
          ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
```

以下示例显示 IKEv2 统计信息：

```
> show crypto ikev2 stats
Global IKEv2 Statistics
  Active Tunnels:                         0
  Previous Tunnels:                       0
  In Octets:                              0
```

```
  In Packets:                             0
  In Drop Packets:                        0
  In Drop Fragments:                      0
  In Notifys:                             0
  In P2 Exchange:                         0
  In P2 Exchange Invalids:                0
  In P2 Exchange Rejects:                 0
  In IPSEC Delete:                        0
  In IKE Delete:                          0
  Out Octets:                             0
  Out Packets:                            0
  Out Drop Packets:                       0
  Out Drop Fragments:                     0
  Out Notifys:                            0
  Out P2 Exchange:                        0
  Out P2 Exchange Invalids:               0
  Out P2 Exchange Rejects:                0
  Out IPSEC Delete:                       0
  Out IKE Delete:                         0
  SAs Locally Initiated:                  0
  SAs Locally Initiated Failed:           0
  SAs Remotely Initiated:                 0
  SAs Remotely Initiated Failed:          0
  System Capacity Failures:               0
  Authentication Failures:                0
  Decrypt Failures:                       0
  Hash Failures:                          0
  Invalid SPI:                            0
  In Configs:                             0
  Out Configs:                            0
  In Configs Rejects:                     0
  Out Configs Rejects:                    0
  Previous Tunnels:                       0
  Previous Tunnels Wraps:                 0
  In DPD Messages:                        0
  Out DPD Messages:                       0
  Out NAT Keepalives:                     0
  IKE Rekey Locally Initiated:            0
  IKE Rekey Remotely Initiated:           0
  CHILD Rekey Locally Initiated:          0
  CHILD Rekey Remotely Initiated:         0

IKEV2 Call Admission Statistics
  Max Active SAs:                    No Limit
  Max In-Negotiation SAs:                 250
  Cookie Challenge Threshold:           Never
  Active SAs:                             0
  In-Negotiation SAs:                     0
  Incoming Requests:                      0
  Incoming Requests Accepted:             0
  Incoming Requests Rejected:             0
  Outgoing Requests:                      0
  Outgoing Requests Accepted:             0
  Outgoing Requests Rejected:             0
  Rejected Requests:                      0
  Rejected Over Max SA limit:             0
  Rejected Low Resources:                 0
  Rejected Reboot In Progress:            0
  Cookie Challenges:                      0
  Cookie Challenges Passed:               0
  Cookie Challenges Failed:               0
```

Related Commands

命令	Description
show crypto ikev1 sa	显示 IKEv1 运行时间 SA 数据库。
show running-config crypto isakmp	显示所有活动的 ISAKMP 配置。

show crypto ipsec df-bit

要显示指定接口的 IPsec 数据包的 IPsec 不分片（DF 位）策略，请使用 **show crypto ipsec df-bit** 命令。您还可以使用 **show ipsec df-bit** 命令同义词。

show crypto ipsec df-bit *interface*

Syntax Description

interface	指定接口名称。

Command History

版本	修改
6.1	引入了此命令。

使用指南

df-bit 设置确定系统如何处理封装信头中的不分片 (DF) 位。IP 信头中的 DF 位确定是否允许设备对数据包分段。根据此设置，系统在应用加密时会清除、设置或复制明文数据包的 DF 位设置，也可以将其复制到外 IPsec 信头。

示例

以下示例展示名为 inside 的接口的 IPsec DF 位策略：

```
> show crypto ipsec df-bit inside
df-bit inside copy
```

Related Commands

命令	Description
show crypto ipsec fragmentation	显示 IPsec 数据包的分段策略。

show crypto ipsec fragmentation

要显示 IPsec 数据包的分段策略，请使用 **show crypto ipsec fragmentation** 命令。您还可以使用 **show ipsec fragmentation** 命令同义词。

show crypto ipsec fragmentation *interface*

Syntax Description

interface	指定接口名称。

Command History

版本	修改
6.1	引入了此命令。

使用指南

为 VPN 加密数据包时，系统会将数据包长度与出站接口的 MTU 进行比较。如果加密数据包将超过 MTU，则必须对数据包进行分段。此命令显示系统是在数据包加密后（加密后）还是加密前（加密前）对数据包进行分片。在加密之前对数据包进行分片也称为预分片，这是默认的系统行为，因为它可以提高整体加密性能。

示例

以下示例显示名为 inside 的接口的 IPsec 分段策略：

```
> show crypto ipsec fragmentation inside
fragmentation inside before-encryption
```

Related Commands

命令	Description
show crypto ipsec df-bit	显示指定接口的 DF 位策略。

show crypto ipsec policy

要显示为 OSPFv3 配置的 IPsec 安全套接字 API (SS API) 安全策略，请使用 **show crypto ipsec policy** 命令。您还可以使用此命令的替代形式： **show ipsec policy**。

show crypto ipsec policy

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例显示 OSPFv3 身份验证和加密策略。

```
> show crypto ipsec policy
Crypto IPsec client security policy data

Policy name:      OSPFv3-1-256
Policy refcount:  1
Policy flags:     0x00000000
SA handles:       sess 268382208 (0xfff3000) / in 55017 (0xd6e9) / out 90369 (0x16101)
Inbound  ESP SPI:        256 (0x100)
Outbound ESP SPI:        256 (0x100)
Inbound  ESP Auth Key:   12345678901234567890123456789012345678901234567890
Outbound ESP Auth Key:   12345678901234567890123456789012345678901234567890
Inbound  ESP Cipher Key: 123456789012345678901234567890123456789012
Outbound ESP Cipher Key: 123456789012345678901234567890123456789012
Transform set:    esp-aes esp-sha-hmac
```

Related Commands

命令	Description
show ipv6 ospf interface	显示有关 OSPFv3 接口的信息。
show crypto sockets	显示安全套接字信息。

show crypto ipsec sa

要显示 IPsec SA 列表，请使用 **show crypto ipsec sa** 命令。您还可以使用此命令的替代形式： **show ipsec sa**。

show crypto ipsec sa ［**assigned-address** | **entry** | **identity** | **inactive** | **map** *map-name* | **peer** *peer-addr* | **spi** | **summary** | **user**］［**detail**］

Syntax Description

assigned-address	（可选）显示已分配地址的 IPsec SA。
detail	（可选）显示有关所显示内容的详细错误信息。
entry	（可选）显示按对等设备地址排序的 IPsec SA
identity	（可选）显示按身份排序的 IPsec SA，不包括 ESP。这是简洁形式。
inactive	（可选）显示非活动 IPsec SA。
map *map-name*	（可选）显示指定加密映射的 IPsec SA。
peer *peer-addr*	（可选）显示指定对等设备 IP 地址的 IPsec SA。
spi	（可选）显示 SPI 的 IPsec SA
summary	（可选）按类型显示 IPsec SA 摘要
user	（可选）显示用户的 IPsec SA。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例显示包含标识为 OSPFv3 的隧道的 IPsec SA。

```
> show crypto ipsec sa
interface: outside2
    Crypto map tag: def, local addr: 10.132.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (172.20.0.21/255.255.255.255/0/0)
      current_peer: 172.20.0.21
      dynamic allocated peer ip: 10.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1145, #pkts decrypt: 1145, #pkts verify: 1145
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 2, #pre-frag failures: 1, #fragments created: 10
```

```
      #PMTUs sent: 5, #PMTUs rcvd: 2, #decapstulated frags needing reassembly: 1
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 10.132.0.17, remote crypto endpt.: 172.20.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={L2L, Transport, Manual key, (OSPFv3), }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 548
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={L2L, Transport, Manual key, (OSPFv3), }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 548
         IV size: 8 bytes
         replay detection support: Y

    Crypto map tag: def, local addr: 10.132.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
```

注释 如果 IPsec SA 策略表明在 IPsec 处理前进行碎片整理，则碎片整理统计信息为碎片整理前统计信息。如果 SA 策略表明在 IPsec 处理后进行碎片整理，则显示碎片整理后统计信息。

以下示例显示名为 def 的加密映射的 IPsec SA。

```
> show crypto ipsec sa map def
cryptomap: def
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1146, #pkts decrypt: 1146, #pkts verify: 1146
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
```

```
      slot: 0, conn_id: 3, crypto-map: def
      sa timing: remaining key lifetime (sec): 480
      IV size: 8 bytes
      replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
      transform: esp-3des esp-md5-hmac
      in use settings ={RA, Tunnel, }
      slot: 0, conn_id: 3, crypto-map: def
      sa timing: remaining key lifetime (sec): 480
      IV size: 8 bytes
      replay detection support: Y

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73672, #pkts encrypt: 73672, #pkts digest: 73672
      #pkts decaps: 78824, #pkts decrypt: 78824, #pkts verify: 78824
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73672, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
      transform: esp-3des esp-md5-hmac
      in use settings ={RA, Tunnel, }
      slot: 0, conn_id: 4, crypto-map: def
      sa timing: remaining key lifetime (sec): 263
      IV size: 8 bytes
      replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
      transform: esp-3des esp-md5-hmac
      in use settings ={RA, Tunnel, }
      slot: 0, conn_id: 4, crypto-map: def
      sa timing: remaining key lifetime (sec): 263
      IV size: 8 bytes
      replay detection support: Y
```

以下示例显示 **entry** 关键字的 IPsec SA。

```
> show crypto ipsec sa entry
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
```

```
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 429
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 429
         IV size: 8 bytes
         replay detection support: Y

peer address: 10.135.1.8
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73723, #pkts encrypt: 73723, #pkts digest: 73723
      #pkts decaps: 78878, #pkts decrypt: 78878, #pkts verify: 78878
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73723, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 212
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 212
         IV size: 8 bytes
         replay detection support: Y
```

以下示例显示带有 **entry detail** 关键字的 IPsec SA。

```
> show crypto ipsec sa entry detail
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1148, #pkts decrypt: 1148, #pkts verify: 1148
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 322
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 322
         IV size: 8 bytes
         replay detection support: Y

peer address: 10.135.1.8
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73831, #pkts encrypt: 73831, #pkts digest: 73831
      #pkts decaps: 78989, #pkts decrypt: 78989, #pkts verify: 78989
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73831, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0
```

```
      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 104
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 104
         IV size: 8 bytes
         replay detection support: Y
```

以下示例显示带有 **identity** 关键字的 IPsec SA。

```
> show crypto ipsec sa identity
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73756, #pkts encrypt: 73756, #pkts digest: 73756
      #pkts decaps: 78911, #pkts decrypt: 78911, #pkts verify: 78911
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73756, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
```

以下示例显示具有关键字 **identity** 和 **detail** 的 IPsec SA。

```
> show crypto ipsec sa identity detail
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73771, #pkts encrypt: 73771, #pkts digest: 73771
      #pkts decaps: 78926, #pkts decrypt: 78926, #pkts verify: 78926
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73771, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
```

Related Commands

命令	Description
clear isakmp sa	清除 IKE 运行时间 SA 数据库。
show running-config isakmp	显示所有活动的 ISAKMP 配置。

show crypto ipsec stats

要显示 IPsec 统计信息列表，请使用 **show crypto ipsec stats** 命令。

show crypto ipsec stats

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例显示 IPsec 统计信息：

```
> show crypto ipsec stats

IPsec Global Statistics
-----------------------
Active tunnels: 2
Previous tunnels: 9
Inbound
    Bytes: 4933013
    Decompressed bytes: 4933013
    Packets: 80348
    Dropped packets: 0
    Replay failures: 0
    Authentications: 80348
    Authentication failures: 0
    Decryptions: 80348
    Decryption failures: 0
    Decapsulated fragments needing reassembly: 0
Outbound
    Bytes: 4441740
    Uncompressed bytes: 4441740
    Packets: 74029
    Dropped packets: 0
    Authentications: 74029
    Authentication failures: 0
    Encryptions: 74029
    Encryption failures: 0
 Fragmentation successes: 3
  Pre-fragmentation successes:2
  Post-fragmentation successes: 1
 Fragmentation failures: 2
  Pre-fragmentation failures:1
  Post-fragmentation failures: 1
 Fragments created: 10
 PMTUs sent: 1
 PMTUs recvd: 2
Protocol failures: 0
Missing SA failures: 0
System capacity failures: 0
```

Related Commands

命令	Description
clear ipsec sa	基于指定的参数清除 IPsec SA 或计数器。
show ipsec sa	根据指定参数显示 IPsec SA。
show ipsec sa summary	显示 IPsec SA 摘要。

show crypto isakmp

要显示 IKEv1 和 IKEv2 的 ISAKMP 信息，请使用 **show crypto isakmp** 命令。

show crypto isakmp {**sa** [**detail**] | **stats**}

Syntax Description

sa [**detail**]	显示有关运行时间安全关联 (SA) 数据库的信息。包括 **detail** 关键字以显示有关 SA 数据库的详细输出。
stats	显示 IKEv1 和 IKEv2 统计信息。

Command History

版本	修改
6.1	引入了此命令。

使用指南

show crypto isakmp 命令结合了等效命令 **show crypto ikev1** 和 **show crypto ikev2** 命令的输出。

以下是阅读 SA 信息的一些提示。

- Rky 可以是 No 或 Yes。如果是，则密钥更新正在进行，第二个匹配的 SA 将处于不同的状态，直到密钥更新完成。
- 角色是发起方或响应方状态。这是 SA 状态机的当前状态。
- 状态 - 正常且正在传递数据的隧道的值为 MM_ACTIVE 或 AM_ACTIVE。

示例

以下示例显示有关 SA 数据库的详细信息。

```
> show crypto isakmp sa detail

IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
1 209.165.200.225 User  Resp  No   AM_Active  3des    SHA   preshrd 86400

IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
2 209.165.200.226 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
3 209.165.200.227 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
4 209.165.200.228 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400
```

以下示例显示 ISAKMP 统计信息。IKEv1 和 IKEv2 分别显示。

```
> show crypto isakmp stats

Global IKEv1 Statistics
  Active Tunnels:             136
```

```
  Previous Tunnels:            0
  In Octets:                   0
  In Packets:                  0
  In Drop Packets:             0
  In Notifys:                  0
  In P2 Exchanges:             0
  In P2 Exchange Invalids:     0
  In P2 Exchange Rejects:      0
  In P2 Sa Delete Requests:    0
  Out Octets:               1344
  Out Packets:                 8
  Out Drop Packets:            0
  Out Notifys:                 0
  Out P2 Exchanges:            0
  Out P2 Exchange Invalids:    0
  Out P2 Exchange Rejects:     0
  Out P2 Sa Delete Requests:   0
  Initiator Tunnels:           2
  Initiator Fails:             2
  Responder Fails:             0
  System Capacity Fails:       0
  Auth Fails:                  0
  Decrypt Fails:               0
  Hash Valid Fails:            0
  No Sa Fails:                 0

IKEV1 Call Admission Statistics
  Max In-Negotiation SAs:                50
  In-Negotiation SAs:                     0
  In-Negotiation SAs Highwater:           0
  In-Negotiation SAs Rejected:            0
In Drop Packets: 925

Global IKEv2 Statistics
  Active Tunnels:                        132
  Previous Tunnels:                      132
  In Octets:                             195471
  In Packets:                            1854
  In Drop Packets:                       925
  In Drop Fragments:                     0
  In Notifys:                            0
  In P2 Exchange:                        132
  In P2 Exchange Invalids:               0
  In P2 Exchange Rejects:                0
  In IPSEC Delete:                       0
  In IKE Delete:                         0
  Out Octets:                            119029
  Out Packets:                           796
  Out Drop Packets:                      0
  Out Drop Fragments:                    0
  Out Notifys:                           264
  Out P2 Exchange:                       0
Out P2 Exchange Invalids:               0
  Out P2 Exchange Rejects:               0
  Out IPSEC Delete:                      0
  Out IKE Delete:                        0
  SAs Locally Initiated:                 0
  SAs Locally Initiated Failed:          0
  SAs Remotely Initiated:                0
  SAs Remotely Initiated Failed:         0
  System Capacity Failures:              0
  Authentication Failures:               0
  Decrypt Failures:                      0
  Hash Failures:                         0
```

```
  Invalid SPI:                            0
  In Configs:                             0
  Out Configs:                            0
  In Configs Rejects:                     0
  Out Configs Rejects:                    0
  Previous Tunnels:                       0
  Previous Tunnels Wraps:                 0
  In DPD Messages:                        0
  Out DPD Messages:                       0
  Out NAT Keepalives:                     0
  IKE Rekey Locally Initiated:            0
  IKE Rekey Remotely Initiated:           0
  CHILD Rekey Locally Initiated:          0
  CHILD Rekey Remotely Initiated:         0

IKEV2 Call Admission Statistics
  Max Active SAs:                   No Limit
  Max In-Negotiation SAs:                300
  Cookie Challenge Threshold:            150
  Active SAs:                              0
  In-Negotiation SAs:                      0
  Incoming Requests:                       0
  Incoming Requests Accepted:              0
  Incoming Requests Rejected:              0
  Outgoing Requests:                       0
  Outgoing Requests Accepted:              0
  Outgoing Requests Rejected:              0
  Rejected Requests:                       0
  Rejected Over Max SA limit:              0
  Rejected Low Resources:                  0
  Rejected Reboot In Progress:             0
  Cookie Challenges:                       0
  Cookie Challenges Passed:                0
  Cookie Challenges Failed:                0
```

Related Commands

命令	Description
clear crypto isakmp sa	清除 IKE 运行时间 SA 数据库。
show running-config crypto isakmp	显示所有活动的 ISAKMP 配置。

show crypto key mypubkey

要显示 ECDSA 或 RSA 密钥的密钥名称、用途和椭圆曲线大小，请使用 **show crypto key mypubkey** 命令。

show crypto key mypubkey {**ecdsa** | **rsa**}

Syntax Description

ecdsa	显示 RSA 公共密钥。
rsa	显示 RSA 公共密钥。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例显示 RSA 公共密钥：

```
> show crypto key mypubkey rsa
Key pair was generated at: 18:19:26 UTC May 26 2016
Key name: <Default-RSA-Key>
 Usage: General Purpose Key
 Modulus Size (bits): 1024
 Key Data:

  30819f30 0d06092a 864886f7 0d010101 05000381 8d003081 89028181 00c0bf77
  d651ead6 fca31c72 12064272 36f699b9 e971e198 1503ba6b f0112b63 97252a26
  38827d83 cd71863e b8962da5 bb905a47 666452a1 9eb1a36e dd8aab00 0e4493f1
  4422bf09 4bcfcb95 a83d38a9 7b9caba6 83c9b5b2 cff251f8 a0422a68 3690c9e5
  0cbbe83b 1a8b2460 1f83b43b a9b06912 7cc9f7f9 f596b81e e2a7bde7 8f020301
  0001
>
```

show crypto protocol statistics

要在加密加速器 MIB 中显示协议特定的统计信息，请使用 **show crypto protocol statistics** 命令。

show crypto protocol statistics 协议

Syntax Description

protocol	指定要显示统计信息的协议名称。协议选项如下所示： **ikev1**-互联网密钥交换第 1 版。 **ikev2**-互联网密钥交换第 2 版。 **ipsec**- IP 安全阶段 2 协议。 **ssl**-安全套接字层。 **ssh**-安全外壳协议 **srtp**-安全实时传输协议 **other**- 保留以用于新协议。 **all**- 当前支持的所有协议。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例展示所有协议的加密加速器统计信息：

```
> show crypto protocol statistics all
[IKEv1 statistics]
   Encrypt packet requests: 46
   Encapsulate packet requests: 46
   Decrypt packet requests: 40
   Decapsulate packet requests: 40
   HMAC calculation requests: 91
   SA creation requests: 1
   SA rekey requests: 3
   SA deletion requests: 3
   Next phase key allocation requests: 2
   Random number generation requests: 0
   Failed requests: 0
[IKEv2 statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
   Decrypt packet requests: 0
   Decapsulate packet requests: 0
   HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
```

```
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0
[IPsec statistics]
   Encrypt packet requests: 700
   Encapsulate packet requests: 700
   Decrypt packet requests: 700
   Decapsulate packet requests: 700
   HMAC calculation requests: 1400
   SA creation requests: 2
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0
[SSL statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
   Decrypt packet requests: 0
   Decapsulate packet requests: 0
   HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0
[SSH statistics are not supported]
[SRTP statistics are not supported]
[Other statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
   Decrypt packet requests: 0
   Decapsulate packet requests: 0
   HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 99
   Failed requests: 0
>
```

Related Commands

命令	Description
clear crypto accelerator statistics	清除加密加速器 MIB 中的全局统计信息和加速器特定统计信息。
clear crypto protocol statistics	清除加密加速器 MIB 中的协议特定统计信息。
show crypto accelerator statistics	显示来自加密加速器MIB的全局统计信息和加速器特定统计信息。

show crypto sockets

要显示加密安全套接字信息，请使用 **show crypto sockets** 命令。

show crypto sockets

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例显示加密安全套接字信息：

```
> show crypto sockets
Number of Crypto Socket connections 1

       Gi0/1  Peers: (local): 2001:1::1
                     (remote): ::
              Local Ident (addr/plen/port/prot): (2001:1::1/64/0/89)
              Remote Ident (addr/plen/port/prot): (::/0/0/89)
              IPsec Profile: "CSSU-UTF"
              Socket State: Open
              Client: "CSSU_App(UTF)" (Client State: Active)

       Crypto Sockets in Listen state:
```

下表显示 **show crypto sockets** 命令的输出的字段。

字段	Description
Number of Crypto Socket connections	系统中的加密套接字数量。
Socket State	此状态可以是 Open（开放），这意味着存在活动的 IPsec 安全关联 (SA)；也可以是 Closed（关闭），这意味着不存在活动的 IPsec SA。
Client	应用名称及其状态。
Flags	如果该字段表明“共享”，则套接字与多个隧道接口共享。
Crypto Sockets in Listen state	加密 IPsec 配置文件的名称。

Related Commands

命令	Description
show crypto ipsec policy	显示加密安全套接字 API 安装策略信息。

show crypto ssl

要显示 threat defense 设备上的活动 SSL 会话的信息，请使用 **show crypto ssl** 命令

show crypto ssl ［**cache** | **ciphers** | **errors** ［**trace**］ | **mib** ［**64**］ | **objects**］

Syntax Description

cache	（可选）显示 SSL 会话缓存统计信息。
ciphers	（可选）显示可用的 SSL 密码。
errors	（可选）显示 SSL 错误。
trace	（可选）显示 SSL 错误跟踪信息。
mib	（可选）显示 SSL MIB 统计信息。
64	（可选）显示 SSL MIB 64 位计数器统计信息。
objects	（可选）显示 SSL 对象统计信息。

Command History

版本	修改
6.1	引入了此命令。

使用指南

此命令显示有关当前 SSLv3 或更高会话的信息，包括启用的密码顺序、禁用了哪些密码、正在使用的 SSL 信任点，以及是否启用证书身份验证。

示例

以下是 **show ssl** 命令的输出示例：

```
> show crypto ssl

Accept connections using SSLv3 or greater and negotiate to TLSv1 or greater
Start connections using TLSv1 and negotiate to TLSv1 or greater
SSL DH Group: group2 (1024-bit modulus)
SSL ECDH Group: group19 (256-bit EC)

SSL trust-points:
  Self-signed (RSA 2048 bits RSA-SHA256) certificate available
  Self-signed (EC 256 bits ecdsa-with-SHA256) certificate available
Certificate authentication is not enabled
```

要显示 SSL 会话缓存统计信息，请使用 **show crypto ssl cache** 命令

```
> show crypto ssl cache

SSL session cache statistics:
  Maximum cache size:          100    Current cache size:           0
```

```
  Cache hits:                    0    Cache misses:                  0
  Cache timeouts:                0    Cache full:                    0
  Accept attempts:               0    Accepts successful:            0
  Accept renegotiates:           0
  Connect attempts:              0    Connects successful:           0
  Connect renegotiates:          0
SSL VPNLB session cache statistics:
  Maximum cache size:           10    Current cache size:            0
  Cache hits:                    0    Cache misses:                  0
  Cache timeouts:                0    Cache full:                    0
  Accept attempts:               0    Accepts successful:            0
  Accept renegotiates:           0
  Connect attempts:              0    Connects successful:           0
  Connect renegotiates:          0
SSLDEV session cache statistics:
  Maximum cache size:           20    Current cache size:            0
  Cache hits:                    0    Cache misses:                  0
  Cache timeouts:                0    Cache full:                    0
  Accept attempts:               0    Accepts successful:            0
  Accept renegotiates:           0
  Connect attempts:              0    Connects successful:           0
  Connect renegotiates:          0
DTLS session cache statistics:
  Maximum cache size:          100    Current cache size:            0
  Cache hits:                    0    Cache misses:                  0
  Cache timeouts:                0    Cache full:                    0
  Accept attempts:               0    Accepts successful:            0
  Accept renegotiates:           0
  Connect attempts:              0    Connects successful:           0
  Connect renegotiates:          0
```

要显示 SSL 密码列表，请使用 **show crypto ssl cipher** 命令

```
> show crypto ssl cipher

Current cipher configuration:
default (medium):
  ECDHE-ECDSA-AES256-GCM-SHA384
  ECDHE-RSA-AES256-GCM-SHA384
  DHE-RSA-AES256-GCM-SHA384
  AES256-GCM-SHA384
  ECDHE-ECDSA-AES256-SHA384
  ECDHE-RSA-AES256-SHA384
  DHE-RSA-AES256-SHA256
  AES256-SHA256
  ECDHE-ECDSA-AES128-GCM-SHA256
  ECDHE-RSA-AES128-GCM-SHA256
  DHE-RSA-AES128-GCM-SHA256
  AES128-GCM-SHA256
  ECDHE-ECDSA-AES128-SHA256
  ECDHE-RSA-AES128-SHA256
  DHE-RSA-AES128-SHA256
  AES128-SHA256
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
  DES-CBC3-SHA
tlsv1 (medium):
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
```

```
  AES128-SHA
  DES-CBC3-SHA
tlsv1.1 (medium):
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
  DES-CBC3-SHA
tlsv1.2 (medium):
  ECDHE-ECDSA-AES256-GCM-SHA384
  ECDHE-RSA-AES256-GCM-SHA384
  DHE-RSA-AES256-GCM-SHA384
  AES256-GCM-SHA384
  ECDHE-ECDSA-AES256-SHA384
  ECDHE-RSA-AES256-SHA384
  DHE-RSA-AES256-SHA256
  AES256-SHA256
  ECDHE-ECDSA-AES128-GCM-SHA256
  ECDHE-RSA-AES128-GCM-SHA256
  DHE-RSA-AES128-GCM-SHA256
  AES128-GCM-SHA256
  ECDHE-ECDSA-AES128-SHA256
  ECDHE-RSA-AES128-SHA256
  DHE-RSA-AES128-SHA256
  AES128-SHA256
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
  DES-CBC3-SHA
dtlsv1 (medium):
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
  DES-CBC3-SHA
```

show ctiqbe

要显示有关跨 threat defense 设备建立的 CTIQBE 会话的信息，请使用 **show ctiqbe** 命令。

show ctiqbe

Command History

版本	修改
6.2	引入了此命令。

示例

以下是 **show ctiqbe** 命令在以下情况时的输出示例。在设备中仅建立了一个活动 CTIQBE 会话。该会话建立在本地地址 10.0.0.99 上的内部 CTI 设备（例如 Cisco IP SoftPhone）与地址 172.29.1.77 上的外部 Cisco Call Manager 之间，其中 TCP 端口 2748 是 Cisco CallManager。该会话的心跳间隔为 120 秒。

```
> show ctiqbe

Total: 1
        LOCAL           FOREIGN         STATE   HEARTBEAT
-----------------------------------------------------------------
1       10.0.0.99/1117  172.29.1.77/2748        1       120
        ---------------------------------------------
        RTP/RTCP: PAT xlates: mapped to 172.29.1.99(1028 - 1029)
        ---------------------------------------------
        MEDIA: Device ID 27     Call ID 0
               Foreign 172.29.1.99      (1028 - 1029)
               Local   172.29.1.88      (26822 - 26823)
        ---------------------------------------------
```

CTI 设备已向 CallManager 注册。该设备的内部地址和 RTP 侦听端口通过 PAT 方式转换到 172.29.1.99 UDP 端口 1028。该设备的 RTCP 侦听端口通过 PAT 方式转换到 UDP 1029。

以 “RTP/RTCP: PAT xlates:” 开头的行仅在满足如下条件时显示：内部 CTI 设备已向外部 CallManager 注册，且 CTI 设备地址和端口已通过 PAT 方式转换到该外部接口。如果 CallManager 位于内部接口上，或者，如果内部 CTI 设备地址和端口 NAT 到 CallManager 使用的外部接口上，此行将不会显示。

该输出表示已在此 CTI 设备与位于 172.29.1.88 的另一个电话之间建立呼叫。另一个电话的 RTP 和 RTCP 侦听端口分别是 UDP 26822 和 26823。由于 threat defense 设备不保留与第二个电话和 CallManager 相关的 CTIQBE 会话记录，因此，另一个电话和 CallManager 位于同一接口上。CTI 设备端的活动呼叫分支可通过设备 ID 27 和呼叫 ID 0 进行标识。

Related Commands

命令	Description
inspect ctiqbe	启用 CTIQBE 应用检查。

命令	Description
show service-policy	显示服务策略信息和统计信息。
show conn	显示不同连接类型的连接状态。

show ctl-provider

要显示统一通信中使用的 CTL 提供程序的配置，请使用 **show ctl-provider** 命令。

show ctl-provider [*name*]

Syntax Description

name	（可选）仅显示此 CTL 提供程序的信息。

Command History

版本	修改
6.3	引入了此命令。

示例

此示例显示如何显示 CTL 提供程序的配置。

```
> show ctl-provider
!
ctl-provider my-ctl
 client interface inside address 192.168.1.55
 client interface inside address 192.168.1.56
 client username admin password gWe.oMSKmeGtelxS encrypted
 export certificate ccm-proxy
!
```

show curpriv

要显示诊断 CLI 会话的当前用户权限，请使用 **show curpriv** 命令：

show curpriv

Command History

版本	修改
6.1	引入了此命令。

使用指南

show curpriv 命令显示当前特权级别。较低特权级别编号表示较低特权级别。

此信息不适用于 **configure user** 命令定义的用户。相反，这些是 **system support diagnostistic-cli** 会话中用户的权限。您无法更改这些权限。

示例

以下示例显示如何查看已登录用户的权限。这些权限适用于诊断 CLI；它们不适用于使用 configure 命令的功能。您无法为 enable_1 用户配置权限。这些权限对于 **Basic** 和 **Config** 权限是相同的。

```
> show curpriv
Username : enable_1
Current privilege level : 15
Current Mode/s : P_PRIV P_CONF
```

show d - show h

show database

要显示有关系统数据库的信息，请使用 **show database** 命令。

show database {**processes** | **slow-query-log**}

Syntax Description

processes	显示有关当前正在运行的数据库查询的信息。
slow-query-log	显示数据库的慢查询日志。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例显示如何显示数据库进程信息。

```
> show database processes
Database Processes:
        Id :  3
      User :  barnyard
      Host :  localhost
  Database :  sfsnort
   Command :  Sleep
      Time :  6
     State :  Null
      Info :  Null
--------------------------------------------------------------
(...Remaining output truncated...)
```

show ddns update

要显示有关 DDNS 更新方法的信息，请使用 **show ddns update interface** 命令。

show ddns update {**interface** [*interface-name*] | **method** [*method-name*]}

Syntax Description

interface [*interface-name*]	显示分配给 threat defense 接口的方法。您可以选择指定接口名称，以仅查看有关该接口的信息。
method [*method-name*]	显示有关 DDNS 更新方法的信息。您可以选择输入方法的名称，以仅查看有关该方法的信息。

Command History

版本	修改
6.1	引入了此命令。
6.7	对于 Web 更新方法， **interface** 关键字的输出包括上次成功更新的 FQDN/IP 地址映射。对于 **method** 关键字，添加了 Web 更新方法的输出。

示例

以下示例展示分配给内部接口的 DDNS 方法：

```
> show ddns update interface inside
Dynamic DNS Update on inside:
  Update Method Name            Update Destination
  ddns-2                        not available
>
```

以下示例显示 Web 类型更新成功：

```
> show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name            Update Destination
  test                          not available

Last Update attempted on 09:01:52.729 UTC Mon Mar 23 2020
Status : Success
FQDN : ftd1.example.com
IP addresses(s): 10.10.32.45,2001:DB8::1
```

以下示例显示 Web 类型故障：

```
> show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name            Update Destination
  test                          not available
```

```
Last Update attempted on 09:01:52.729 UTC Mon Mar 23 2020
Status : Failed
Reason : Could not establish a connection to the server
```

以下示例显示 DNS 服务器返回 Web 类型更新错误：

```
> show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name            Update Destination
  test                          not available

Last Update attempted on 09:01:52.729 UTC Mon Mar 23 2020
Status : Failed
Reason : Server error (Error response from server)
```

以下示例显示，由于 IP 地址未配置或 DHCP 请求失败，尚未尝试 Web 更新，例如：

```
> show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name            Update Destination
  test                          not available

Last Update Not attempted
```

以下示例展示名为 ddns-2 的 DDNS 方法：

```
> show ddns update method ddns-2
Dynamic DNS Update Method: ddns-2
  IETF standardized Dynamic DNS 'A' and 'PTR' records update
  Maximum update interval: 0 days 0 hours 10 minutes 0 seconds
>
```

以下示例显示有关 Web 更新方法的详细信息：

```
> show ddns update method web1

Dynamic DNS Update Method: web1
 Dynamic DNS updated via HTTP(s) protocols
  URL used to update record: https://cdarwin:*****@ddns.cisco.com/update?hostname=<h>&myip=<a>
```

Related Commands

命令	Description
show running-config ddns	显示运行的配置中所有配置 DDNS 方法的类型和间隔。

show debug

要显示当前调试配置，请使用 **show debug** 命令。

show debug ［命令 ［关键词］］

Syntax Description

command	（可选）指定要查看其当前配置的 **debug** 命令。
关键词	（可选）对于每个命令，命令后跟的关键词与关联 **debug** 命令支持的关键词完全相同。

Command History

版本	修改
6.1	引入了此命令。

使用指南

对于每个命令，命令后跟的关键词与关联 **debug** 命令支持的关键词完全相同。有关支持的语法的信息，请输入 ?在关键字位置。

例如：

- **show debug ?** 列出可用的命令。
- **show debug tcp ?** 列出可用于 TCP 调试的关键字。

示例

以下示例启用 TCP 调试，然后显示调试状态。

```
> debug tcp
debug tcp  enabled at level 1
> show debug tcp
debug tcp  enabled at level 1
debug tcp  enabled at level 1 (persistent)
```

Related Commands

命令	Description
debug	启用调试。

show debug

要显示当前调试配置，请使用 **show debug** 命令。

show debug ［命令 ［关键词］］

Syntax Description

command	（可选）指定要查看其当前配置的 **debug** 命令。
关键词	（可选）对于每个命令，命令后跟的关键词与关联 **debug** 命令支持的关键词完全相同。

Command History

版本	修改
6.1	引入了此命令。

使用指南

对于每个命令，命令后跟的关键词与关联 **debug** 命令支持的关键词完全相同。有关支持的语法的信息，请输入 ?在关键字位置。

例如：

- **show debug ?** 列出可用的命令。
- **show debug tcp ?** 列出可用于 TCP 调试的关键字。

示例

以下示例启用 TCP 调试，然后显示调试状态。

```
> debug tcp
debug tcp  enabled at level 1
> show debug tcp
debug tcp  enabled at level 1
debug tcp  enabled at level 1 (persistent)
```

Related Commands

命令	Description
debug	启用调试。

show dhcpd

要查看 DHCP 绑定、状态和统计信息，请使用 **show dhcpd** 命令。

show dhcpd {**binding** [*IP_address*] | **state** | **statistics**}

Syntax Description

binding	显示指定服务器IP地址的绑定信息及其关联客户端硬件地址和租用时长。
IP_address	显示指定 IP 地址的绑定信息。
state	显示DHCP服务器的状态，例如在当前情景下是否已启用以及在每个接口上是否已启用。
statistics	显示统计信息，例如地址池、绑定、过期绑定、格式不正确的消息、已发送消息和已接收消息的数量。

Command History

版本	修改
6.1	引入了此命令。

使用指南

如果您在 **show dhcpd binding** 命令中包含了可选的 IP 地址，则仅显示该 IP 地址的绑定。

示例

以下是 **show dhcpd binding** 命令的输出示例：

```
> show dhcpd binding
IP Address Client-id         Lease Expiration  Type
10.0.1.100 0100.a0c9.868e.43 84985 seconds     automatic
```

以下是 **show dhcpd state** 命令的输出示例。在本例中，外部接口是 DHCP 客户端，而许多其他接口充当 DHCP 服务器。

```
> show dhcpd state
Context  Configured as DHCP Server
Interface outside, Configured for DHCP CLIENT
Interface inside1_2, Configured for DHCP SERVER
Interface inside1_3, Configured for DHCP SERVER
Interface inside1_4, Configured for DHCP SERVER
Interface inside1_5, Configured for DHCP SERVER
Interface inside1_6, Configured for DHCP SERVER
Interface inside1_7, Configured for DHCP SERVER
Interface inside1_8, Not Configured for DHCP
Interface diagnostic, Not Configured for DHCP
Interface inside, Configured for DHCP SERVER
```

以下是 **show dhcpd statistics** 命令的输出示例：

```
> show dhcpd statistics

DHCP UDP Unreachable Errors: 0
DHCP Other UDP Errors: 0

Address pools         1
Automatic bindings    1
Expired bindings      1
Malformed messages    0

Message               Received
BOOTREQUEST           0
DHCPDISCOVER          1
DHCPREQUEST           2
DHCPDECLINE           0
DHCPRELEASE           0
DHCPINFORM            0

Message               Sent
BOOTREPLY             0
DHCPOFFER             1
DHCPACK               1
DHCPNAK               1
```

Related Commands

命令	Description
clear dhcpd	清除 DHCP 服务器绑定和统计计数器。
show running-config dhcpd	显示当前 DHCP 服务器配置。

show dhcprelay

要查看 DHCP 中继代理状态和统计信息，请使用 **show dhcprelay state** 命令。

show dhcprelay {**state** | **statistics**}

Syntax Description

state	显示每个接口的 DHCP 中继代理的状态。
statistics	显示 DHCP 中继统计信息。

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show dhcprelay state** 命令的输出示例：

```
> show dhcprelay state

Context  Configured as DHCP Relay
Interface outside, Not Configured for DHCP
Interface infrastructure, Configured for DHCP RELAY SERVER
Interface inside, Configured for DHCP RELAY
```

以下显示 **show dhcprelay statistics** 命令的输出示例。

```
> show dhcprelay statistics

DHCP UDP Unreachable Errors: 0
DHCP Other UDP Errors: 0

Packets Relayed
BOOTREQUEST          0
DHCPDISCOVER         7
DHCPREQUEST          3
DHCPDECLINE          0
DHCPRELEASE          0
DHCPINFORM           0

BOOTREPLY            0
DHCPOFFER            7
DHCPACK              3
DHCPNAK              0
```

Related Commands

命令	Description
clear dhcprelay statistics	清除 DHCP 中继代理统计计数器。
show dhcpd	显示 DHCP 服务器统计信息和状态信息。

show diameter

要显示每个 Diameter 连接的状态信息，请使用 **show diameter** 命令。

show diameter

Command History

版本	修改
6.2	引入了此命令。

使用指南

要显示 Diameter 连接状态信息，必须检查 Diameter 流量。要检查 Diameter 流量，您需要在 管理中心中配置 FlexConfig。

示例

以下显示 **show diameter** 命令的输出示例。

```
> show diameter
Total active diameter sessions: 5
Session 3638
       ==========
       ref_count: 1 val = .; 1096298391; 2461;
           Protocol : diameter Context id : 0
           From inside:211.1.1.10/45169 to outside:212.1.1.10/3868
...
```

Related Commands

命令	Description
clear service-policy	清除服务策略统计信息。

show disk

要仅显示 threat defense 设备的闪存内容，请使用 **show disk** 命令。

show disk
show {**disk0:** | **disk1:**} [**filesys** | **all** | **controller**]

Syntax Description

{**disk0:** |**disk1:**}	指定内部闪存 (disk0:) 或外部闪存 (disk1:)。如果输入不带数字的 **show disk** 命令，则会看到有关文件系统的信息。
all	显示闪存内容以及文件系统和控制器信息。
controller	显示闪存控制器型号。
filesys	显示关于紧凑型闪存卡的信息。

Command Default

默认情况下，此命令显示文件系统信息。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例显示有关文件系统的信息。

```
> show disk
Filesystem        Size  Used Avail Use% Mounted on
tmpfs             3.9G  440K  3.9G   1% /run
tmpfs             3.9G  168K  3.9G   1% /var/volatile
none              3.8G  9.4M  3.8G   1% /dev
/dev/sdb1         7.4G  104M  7.3G   2% /mnt/disk0
/dev/mapper/root  3.7G  943M  2.6G  27% /ngfw
/dev/mapper/var    81G  4.0G   73G   6% /home
tmpfs             3.9G     0  3.9G   0% /dev/cgroups
```

以下是 **show disk0:** 命令的输出示例：

```
> show disk0:
--#--  --length--  -----date/time------  path
   48  107030784   Oct 05 2016 02:10:26  os.img
   49  33          Oct 11 2016 21:32:16  .boot_string
   50  150484      Oct 06 2016 15:36:02  install.log
   11  4096        Oct 06 2016 15:58:16  log
   13  1544        Oct 13 2016 18:59:06  log/asa-appagent.log
   16  4096        Oct 06 2016 15:59:07  crypto_archive
   51  4096        Oct 06 2016 15:59:12  coredumpinfo
   52  59          Oct 06 2016 15:59:12  coredumpinfo/coredump.cfg
   53  36          Oct 06 2016 16:04:47  enable_configure
   56  507281      Oct 20 2016 18:10:20  crashinfo-test_20161020_181021_UTC
```

```
7935832064 bytes total (7827599360 bytes free)
```

以下是 **show disk0: filesys** 命令的输出示例：

```
> show disk0: filesys

******** Flash Card Geometry/Format Info ********

COMPACT FLASH CARD GEOMETRY
   Number of Heads:          245
   Number of Cylinders      1022
   Sectors per Cylinder       62
   Sector Size               512
   Total Sectors          15524180
```

以下是 **show disk0: controller** 命令的输出示例：

```
> show disk0: controller

Flash Model: ATA Micron_M500DC_MT
```

Related Commands

命令	Description
dir	系统随即会显示目录的内容。

show disk-manager

要显示系统每个部分（包括孤岛、低水位线和高水位线）的磁盘使用情况详细信息，请使用 **show disk-manager** 命令。

show disk-manager

Command History

版本	修改
6.1	引入了此命令。

示例

以下是磁盘管理器信息的示例。

```
> show disk-manager
Silo                                Used        Minimum     Maximum
Temporary Files                     0 KB        499.197 MB  1.950 GB
Action Queue Results                0 KB        499.197 MB  1.950 GB
User Identity Events                0 KB        499.197 MB  1.950 GB
UI Caches                           4 KB        1.462 GB    2.925 GB
Backups                             0 KB        3.900 GB    9.750 GB
Updates                             0 KB        5.850 GB    14.625 GB
Other Detection Engine              0 KB        2.925 GB    5.850 GB
Performance Statistics              33 KB       998.395 MB  11.700 GB
Other Events                        0 KB        1.950 GB    3.900 GB
IP Reputation & URL Filtering       0 KB        2.437 GB    4.875 GB
Archives & Cores & File Logs        0 KB        3.900 GB    19.500 GB
Unified Low Priority Events         1.329 MB    4.875 GB    24.375 GB
RNA Events                          0 KB        3.900 GB    15.600 GB
File Capture                        0 KB        9.750 GB    19.500 GB
Unified High Priority Events        0 KB        14.625 GB   34.125 GB
IPS Events                          0 KB        11.700 GB   29.250 GB
```

show dns

要显示完全限定域名 (FQDN) 网络对象的当前已解析 DNS 地址或管理接口上的 DNS 服务器配置，请使用 **show dns** 命令。

show dns ［**host** *fqdn* | **system**］

Syntax Description

host *fqdn*	仅显示有关指定的完全限定域名 (FQDN) 的信息。
system	显示为管理接口配置的 DNS 服务器和搜索域。

Command Default

如果不包括 **system** 关键字，该命令将显示访问控制规则中使用的所有 FQDN 网络对象的 DNS 解析。

Command History

版本	修改
6.1	引入了此命令。
6.3	添加了对基于 FQDN 的访问控制规则的支持。

示例

以下示例显示管理地址的 DNS 配置。

```
> show dns system
search example.com
nameserver 72.163.47.11
```

以下示例显示访问控制规则中使用的 FQDN 网络对象的 DNS 解析。仅当在规则中使用 FQDN 对象时才会对其进行解析：仅定义对象不会启动名称的 DNS 查找。

```
> show dns
Name:   www.example1.com
  Address: 10.1.3.1                          TTL 00:03:01
  Address: 10.1.3.3                          TTL 00:00:36
  Address: 10.4.1.2                          TTL 00:01:01
Name: www.example2.com
  Address: 10.2.4.1                          TTL 00:25:13
  Address: 10.5.2.1                          TTL 00:25:01
Name: server.ddns-exampleuser.com
  Address: fe80::21e:8cff:feb5:4faa          TTL 00:00:41
  Address: 10.10.10.2                        TTL 00:25:01
```

以下是 **show dns host** 命令的输出示例：

```
> show dns host www.example1.com
Name:   www.example1.com
  Address: 10.1.3.1                          TTL 00:03:01
  Address: 10.1.3.3                          TTL 00:00:36
  Address: 10.4.1.2                          TTL 00:01:01
```

Related Commands

命令	Description
clear dns	删除 FQDN 网络对象 DNS 解析。
show network	显示管理接口的配置。

show dns-hosts

要显示 DNS 缓存，请使用 **show dns-hosts** 命令。DNS 缓存包括从 DNS 服务器动态获知的条目以及手动输入的名称和 IP 地址。

show dns-hosts

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show dns-hosts** 命令的输出示例：

```
> show dns-hosts
Host                        Flags      Age Type   Address(es)
ns2.example.com             (temp, OK) 0    IP    10.102.255.44
ns1.example.com             (temp, OK) 0    IP    192.168.241.185
snowmass.example.com        (temp, OK) 0    IP    10.94.146.101
server.example.com          (temp, OK) 0    IP    10.94.146.80
```

下表对每个字段进行了说明。

表 *25: show dns-hosts* 字段

字段	Description
Host	显示主机名。
Flags	显示条目状态为以下各项的组合： • temp - 由于来自 DNS 服务器，此条目是临时的。设备会在 72 小时不活动后删除此条目。 • perm - 由于使用 name 命令添加，此条目是永久的。 • OK - 此条目有效。 • ?? - 此条目可疑并需要重新验证。 • EX - 此条目已过期。
Age	显示自此条目上次引用后经过的小时数。
Type	显示 DNS 记录的类型；该值始终为 IP。
Address(es)	IP 地址。

Related Commands

命令	Description
clear dns-hosts	清除 DNS 缓存。

show eigrp events

要显示 EIGRP 事件日志，请使用 **show eigrp events** 命令。

show eigrp [*as-number*] **events** [{*start end*} | **type**]

Syntax Description

as_number	（可选）指定您查看事件日志的 EIGRP 流程的自主系统编号。由于 threat defense 设备仅支持一个 EIGRP 路由流程，因此，无需指定自主系统编号。
end	（可选）限制以 *start* 索引号开头并以 *end* 索引号结尾的条目的输出。
start	（可选）指定日志条目索引号的数字。指定起始编号将导致输出以指定的事件开头并以通过 *end* 参数指定的事件结尾。有效值范围为 1 至 500。
type	（可选）显示所记录的事件。

Command Default

如果没有指定 start 和 end，则显示所有日志条目。

Command History

版本	修改
6.1	引入了此命令。

使用指南

show eigrp events 输出最多显示 500 个事件。达到最大事件数后，新事件将添加到输出底部，并且旧事件将从输出顶部删除。

您可以使用 **clear eigrp events** 命令清除 EIGRP 事件日志。

show eigrp events type 命令显示 EIGRP 事件的日志记录状态。默认情况下，将记录邻居变更、邻居警告和 DUAL FSM 消息。您无法禁用 DUAL FSM 事件的日志记录。

示例

以下是 **show eigrp events** 命令的输出示例：

```
> show eigrp events

Event information for AS 100:
1    12:11:23.500 Change queue emptied, entries: 4
2    12:11:23.500 Metric set: 10.1.0.0/16 53760
3    12:11:23.500 Update reason, delay: new if 4294967295
4    12:11:23.500 Update sent, RD: 10.1.0.0/16 4294967295
5    12:11:23.500 Update reason, delay: metric chg 4294967295
6    12:11:23.500 Update sent, RD: 10.1.0.0/16 4294967295
7    12:11:23.500 Route install: 10.1.0.0/16 10.130.60.248
8    12:11:23.500 Find FS: 10.1.0.0/16 4294967295
9    12:11:23.500 Rcv update met/succmet: 53760 28160
10   12:11:23.500 Rcv update dest/nh: 10.1.0.0/16 10.130.60.248
11   12:11:23.500 Metric set: 10.1.0.0/16 4294967295
```

以下是定义了起始和停止编号的 **show eigrp events** 命令的输出示例：

```
> show eigrp events 3 8

Event information for AS 100:
3    12:11:23.500 Update reason, delay: new if 4294967295
4    12:11:23.500 Update sent, RD: 10.1.0.0/16 4294967295
5    12:11:23.500 Update reason, delay: metric chg 4294967295
6    12:11:23.500 Update sent, RD: 10.1.0.0/16 4294967295
7    12:11:23.500 Route install: 10.1.0.0/16 10.130.60.248
8    12:11:23.500 Find FS: 10.1.0.0/16 4294967295
```

以下是 EIGRP 事件日志中没有条目时 **show eigrp events** 命令的输出示例：

```
> show eigrp events

Event information for AS 100:  Event log is empty.
```

以下是 **show eigrp events type** 命令的输出示例：

```
> show eigrp events type

EIGRP-IPv4 Event Logging for AS 100:
      Log Size          500
      Neighbor Changes  Enable
      Neighbor Warnings Enable
      Dual FSM          Enable
```

Related Commands

命令	Description
clear eigrp events	清除 EIGRP 事件日志记录缓冲区。

show eigrp interfaces

要显示参与 EIGRP 路由的接口，请使用 **show eigrp interfaces** 命令。

show eigrp ［*as-number*］ **interfaces** ［*if-name*］［**detail**］

Syntax Description

as_number	（可选）指定您显示活动接口的 EIGRP 流程的自主系统编号。由于 threat defense 设备仅支持一个 EIGRP 路由流程，因此，无需指定自主系统编号。
detail	（可选）显示详细信息。
if-name	（可选）接口的名称。指定限制指定接口显示的接口名称。

Command Default

如果没有指定接口名称，则显示所有 EIGRP 接口的信息。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用 **show eigrp interfaces** 命令确定哪些接口上的 EIGRP 处于活动状态，并了解与这些接口相关的 EIGRP 的信息。

如果指定了接口，则仅显示该接口。否则将显示正在运行 EIGRP 的所有接口。

如果指定了自主系统，则仅显示该指定自主系统的路由流程。否则将显示所有 EIGRP 流程。

示例

以下是 **show eigrp interfaces** 命令的输出示例：

```
> show eigrp interfaces

EIGRP-IPv4 interfaces for process 100

                    Xmit Queue    Mean   Pacing Time   Multicast   Pending
Interface   Peers   Un/Reliable   SRTT   Un/Reliable   Flow Timer  Routes
mgmt          0         0/0          0      11/434          0          0
outside       1         0/0        337       0/10           0          0
inside        1         0/0         10       1/63         103          0
```

下表描述屏幕上展示的重要字段。

表 *26: show eigrp interfaces* 字段说明

字段	Description
process	EIGRP 路由流程的自主系统编号。
Peers	直连对等设备的数量。

字段	Description
Xmit Queue Un/Reliable	不可靠队列和可靠传输队列中包含的数据包数量。
Mean SRTT	平均顺利往返时间间隔（以秒为单位）。
Pacing Time Un/Reliable	用于确定 EIGRP 数据包应何时发出接口（不可靠和可靠数据包）的定步计时（以秒为单位）。
Multicast Flow Timer	threat defense 设备将发送组播 EIGRP 数据包的最大秒数。
Pending Routes	等待发送的传输队列中的数据包内的路由数。

show eigrp neighbors

要显示 EIGRP 邻居表，请使用 **show eigrp neighbors** 命令。

show eigrp ［*as-number*］ **neighbors** ［**detail** | **static**］［*if-name*］

Syntax Description

as_number	（可选）指定要删除邻居条目的 EIGRP 流程的自主系统编号。由于 threat defense 设备仅支持一个 EIGRP 路由流程，因此，无需指定自主系统编号。
detail	（可选）显示详细邻居信息。
if-name	（可选）接口的名称。指定接口名称将显示通过该接口获知的所有邻居表条目。
static	（可选）显示静态定义的 EIGRP 邻居。

Command Default

如果没有指定接口名称，则显示通过所有接口获知的邻居。

Command History

版本	修改
6.1	引入了此命令。

使用指南

您可以使用 **clear eigrp neighbors** 命令清除从 EIGRP 邻居表动态获知的邻居。除非您使用 **static** 关键字，否则静态邻居不包含在输出中。

示例

以下是 **show eigrp neighbors** 命令的输出示例：

```
> show eigrp neighbors

EIGRP-IPv4 Neighbors for process 100

Address                 Interface     Holdtime Uptime   Q      Seq  SRTT  RTO
                                      (secs)   (h:m:s)  Count  Num  (ms)  (ms)
172.16.81.28            Ethernet1     13       0:00:41  0      11   4     20
172.16.80.28            Ethernet0     14       0:02:01  0      10   12    24
172.16.80.31            Ethernet0     12       0:02:02  0      4    5     20
```

下表描述屏幕上展示的重要字段。

表 *27: show eigrp neighbors* 字段说明

字段	Description
process	EIGRP 路由流程的自主系统编号。
Address	EIGRP 邻居的 IP 地址。

字段	Description
Interface	threat defense 设备在其上接收来自邻居的问候数据包的接口。
Holdtime	threat defense 设备在宣告关闭之前等待从邻居收到消息的时长（以秒为单位）。此保持时间从问候数据包中的邻居接收，然后开始减少，直到从邻居接收另一个问候数据包。 如果邻居使用默认保持时间，此数值将小于 15。如果对等设备配置了非默认的保持时间，则会显示非默认的保持时间。 如果该值达到 0，则 threat defense 设备认为邻居不可访问。
Uptime	自 threat defense 设备初次从邻居收到消息后的已用时间（小时:分钟:秒钟格式）。
Q Count	等待 threat defense 设备发送的 EIGRP 数据包（更新、查询和应答）数。
Seq Num	从邻居接收到的最后一个更新数据包、查询数据包或应答数据包的顺序号。
SRTT	顺利往返时间。EIGRP 数据包发送到此邻居和 threat defense 设备接收该数据包确认所需的毫秒数。
RTO	重新传输超时（以毫秒为单位）。这是 threat defense 设备将数据包从重新传输队列重新发送到邻居之前等待的时间量。

以下是 **show eigrp neighbors static** 命令的输出示例：

```
> show eigrp neighbors static

EIGRP-IPv4 neighbors for process 100
Static Address                Interface
192.168.1.5                   management
```

下表描述屏幕上展示的重要字段。

表 *28: show ip eigrp neighbors static* 字段说明

字段	Description
process	EIGRP 路由流程的自主系统编号。
Static Address	EIGRP 邻居的 IP 地址。
Interface	threat defense 设备在其上接收来自邻居的问候数据包的接口。

以下是 **show eigrp neighbors detail** 命令的输出示例：

```
> show eigrp neighbors detail

EIGRP-IPv4 neighbors for process 100
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q Seq Tye
```

```
                                          (sec)          (ms)       Cnt Num
3   1.1.1.3                 Et0/0           12 00:04:48 1832  5000  0  14
   Version 12.2/1.2, Retrans: 0, Retries: 0
   Restart time 00:01:05
0   10.4.9.5                Fa0/0           11 00:04:07  768  4608  0  4   S
   Version 12.2/1.2, Retrans: 0, Retries: 0
2   10.4.9.10               Fa0/0           13 1w0d        1  3000  0  6   S
   Version 12.2/1.2, Retrans: 1, Retries: 0
1   10.4.9.6                Fa0/0           12 1w0d        1  3000  0  4   S
   Version 12.2/1.2, Retrans: 1, Retries: 0
```

下表描述屏幕上展示的重要字段。

表 *29: show ip eigrp neighbors details* 字段说明

字段	Description
process	EIGRP 路由流程的自主系统编号。
H	该列列出了与指定邻居建立对等会话的顺序。该顺序由从0开始的有序编号指定。
Address	EIGRP 邻居的 IP 地址。
Interface	threat defense 设备在其上接收来自邻居的问候数据包的接口。
Holdtime	threat defense 设备在宣告关闭之前等待从邻居收到消息的时长（以秒为单位）。此保持时间从问候数据包中的邻居接收，然后开始减少，直到从邻居接收另一个问候数据包。 如果邻居使用默认保持时间，此数值将小于 15。如果对等设备配置了非默认的保持时间，则会显示非默认的保持时间。 如果该值达到 0，则 threat defense 设备认为邻居不可访问。
Uptime	自 threat defense 设备初次从邻居收到消息后的已用时间（小时:分钟:秒钟格式）。
SRTT	顺利往返时间。EIGRP 数据包发送到此邻居和 threat defense 设备接收该数据包确认所需的毫秒数。
RTO	重新传输超时（以毫秒为单位）。这是 threat defense 设备将数据包从重新传输队列重新发送到邻居之前等待的时间量。
Q Count	等待 threat defense 设备发送的 EIGRP 数据包（更新、查询和应答）数。
Seq Num	从邻居接收到的最后一个更新数据包、查询数据包或应答数据包的顺序号。
Version	指定的对等设备运行的软件版本。
Retrans	数据包已重传的次数。
Retries	重传数据包的尝试次数。

字段	Description
Restart time	指定从邻居重启之后的已用时间（格式：小时:分钟:秒）。

show eigrp topology

要显示 EIGRP 拓扑表，请使用 **show eigrp topology** 命令。

show eigrp [*as-number*] **topology** [*ip-addr* [*mask*] | **active** | **all-links** | **pending** | **summary** | **zero-successors**]

Syntax Description

active	（可选）仅显示 EIGRP 拓扑表中的活动条目。
all-links	（可选）显示 EIGRP 拓扑表中的所有路由，即使并非可行后续路由。
as_number	（可选）指定 EIGRP 流程的自主系统编号。由于 threat defense 设备仅支持一个 EIGRP 路由流程，因此，无需指定自主系统编号。
ip-addr	（可选）定义要显示的拓扑表 IP 地址。使用掩码指定时，将提供条目的详细说明。
mask	（可选）定义要应用于 *ip-addr* 参数的网络掩码。
pending	（可选）显示等待来自邻居的更新或等待回复邻居的 EIGRP 拓扑表中的所有条目。
summary	（可选）显示 EIGRP 拓扑表的摘要。
zero-successors	（可选）显示 EIGRP 拓扑表中可用的路由。

Command Default

仅显示可行后续路由。使用 **all-links** 关键字以显示所有路由，包括并非可行后续的路由。

Command History

版本	修改
6.1	引入了此命令。

使用指南

您可以使用 **clear eigrp topology** 命令删除拓扑表的动态条目。

示例

以下是 **show eigrp topology** 命令的输出示例：

```
EIGRP-IPv4 Topology Table for AS(100)/ID(192.168.1.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 10.2.1.0 255.255.255.0, 2 successors, FD is 0
          via 10.16.80.28 (46251776/46226176), Ethernet0
          via 10.16.81.28 (46251776/46226176), Ethernet1
P 10.2.1.0 255.255.255.0, 1 successors, FD is 307200
          via Connected, Ethernet1
          via 10.16.81.28 (307200/281600), Ethernet1
```

```
        via 10.16.80.28 (307200/281600), Ethernet0
```

下表描述屏幕上展示的重要字段。

表 *30: show eigrp topology* 字段说明

字段	Description
Codes	此拓扑表条目的状态。passive（被动）和 active（主动）指与该目标相关的 EIGRP 状态；update（更新）、query（查询）和 reply（应答）指所发送的数据包的类型。
P - Passive	路由已知良好并且没有对此目标执行任何 EIGRP 计算。
A - Active	对此目标执行 EIGRP 计算。
U - Update	表示向此目标发送了一个更新数据包。
Q - Query	表示向此目标发送了一个查询数据包。
R - Reply	表示向此目标发送了一个应答数据包。
r - Reply status	在软件发送查询之后等待应答期间所设置的标志。
address mask	目标 IP 地址和掩码。
successors	后继路由数量。该数字对应 IP 路由表中的下一跳数量。如果“successors”为大写，则路由或下一跳处于过渡状态。
FD	可行距离。可行距离是到达目的地的最佳度量，或是路由进入活动状态后所获知的最佳度量。该值用于检查可行性条件。如果路由器的报告距离（斜杠后的度量）小于可行距离，则符合可行性条件，该路径为可行后继路由。软件确定其有可行后续路由后，无需发送该目标的查询。
via	将关于此目标的信息告知软件的对等设备 IP 地址。前 n 个条目（其中 n 为后继路由数）为当前后继路由。列表上其余的条目是可行后继路由。
(cost/adv_cost)	第一个数字为 EIGRP 度量，表示到达目标的成本。第二个数字是此对等设备所通告的 EIGRP 度量。
interface	获知该信息所使用的接口。

以下是 **show eigrp topology** 使用的 IP 地址的输出示例。所示输出适用于内部路由。

```
> show eigrp topology 10.2.1.0 255.255.255.0
EIGRP-IPv4 (AS 100): Topology Default-IP-Routing-Table(0) entry for entry for 10.2.1.0
255.255.255.0

    State is Passive, Query origin flag is 1, 1 Successor(s), FD is 281600
    Routing Descriptor Blocks:
        0.0.0.0 (Ethernet0/0), from Connected, Send flag is 0x0
            Composite metric is (281600/0), Route is Internal
```

```
        Vector metric:
            Minimum bandwidth is 10000 Kbit
            Total delay is 1000 microseconds
            Reliability is 255/255
            Load is 1/255
            Minimum MTU is 1500
            Hop count is 0
```

以下是 **show eigrp topology** 使用的 IP 地址的输出示例。所示输出适用于外部路由。

```
> show eigrp topology 10.4.80.0 255.255.255.0
EIGRP-IPv4 (AS 100): Topology Default-IP-Routing-Table(0) entry for entry for 10.4.80.0
255.255.255.0

    State is Passive, Query origin flag is 1, 1 Successor(s), FD is 409600
    Routing Descriptor Blocks:
        10.2.1.1 (Ethernet0/0), from 10.2.1.1, Send flag is 0x0
            Composite metric is (409600/128256), Route is External
            Vector metric:
                Minimum bandwidth is 10000 Kbit
                Total delay is 6000 microseconds
                Reliability is 255/255
                Load is 1/255
                Minimum MTU is 1500
                Hop count is 1
            External data:
                Originating router is 10.89.245.1
                AS number of route is 0
                External protocol is Connected, external metric is 0
                Administrator tag is 0 (0x00000000)
```

Related Commands

命令	Description
clear eigrp topology	清除从 EIGRP 拓扑表动态查找的条目。

show eigrp traffic

要显示发送和接收的 EIGRP 数据包的数量，请使用 **show eigrp traffic** 命令。

show eigrp ［*as-number*］ **traffic**

Syntax Description

as_number	（可选）指定您查看事件日志的 EIGRP 流程的自主系统编号。由于 threat defense 设备仅支持一个 EIGRP 路由流程，因此，无需指定自主系统编号。

Command History

版本	修改
6.1	引入了此命令。

使用指南

您可以使用 **clear eigrp traffic** 命令清除 EIGRP 流量统计信息。

示例

以下是 **show eigrp traffic** 命令的输出示例：

```
> show eigrp traffic
EIGRP-IPv4 Traffic Statistics for AS 100
  Hellos sent/received: 218/205
  Updates sent/received: 7/23
  Queries sent/received: 2/0
  Replies sent/received: 0/2
  Acks sent/received: 21/14
  Input queue high water mark 0, 0 drops
  SIA-Queries sent/received: 0/0
  SIA-Replies sent/received: 0/0
  Hello Process ID: 1719439416
  PDM Process ID: 1719439824
```

下表描述屏幕上展示的重要字段。

表 *31: show eigrp traffic* 字段说明

字段	Description
process	EIGRP 路由流程的自主系统编号。
Hellos sent/received	发送和接收的问候数据包数。
Updates sent/received	发送和接收的更新数据包数。
Queries sent/received	发送和接收的查询数据包数。
Replies sent/received	发送和接收的回复数据包数。
Acks sent/received	发送和接收的确认数据包数。

字段	Description
Input queue high water mark/drops	接近最大接收阈值的发送数据包数和丢弃数据包数。
SIA-Queries sent/received	发送和接收的 Stuck-in-active 查询。
SIA-Replies sent/received	发送和接收的 Stuck-in-active 回复。

show environment

要显示系统组件的系统环境信息，请使用 **show environment** 命令。

注释 Firepower 2100、 4100 和 9300 系列设备不支持此命令。连接到 FXOS CLI 并使用 **show env** 命令而不是此命令。

show environment [**alarm-contact** | **driver** | **fans** | **power-supplies** | **power_consumption** | **voltage** | **temperature** [**accelerator** | **chassis** | **cpu** | **io-hub** | **mother-board** | **power-supply**]]

Syntax Description

alarm-contact	（可选）显示 ISA 3000 设备上输入警报触点的运行状态。
driver	（可选）显示环境监控 (IPMI) 驱动程序状态。驱动程序状态可为以下各项之一： • 运行 - 驱动程序正常运行。 • 已停止 - 错误导致驱动程序停止。
fans	（可选）显示冷却风扇的运行状态。状态为以下之一： • 正常 - 风扇正常运行。 • 故障 - 风扇出现故障并应进行更换。
power-supplies	（可选）显示电源设备的运行状态。每个电源设备的状态均为以下各项之一： • 正常 - 电源设备正常运行。 • 故障 - 电源设备出现故障并应进行更换。 • 不存在 - 指定的电源设备未安装。 电源设备冗余状态也将显示。冗余状态为以下各项之一： • 正常 - 设备以完整资源正常运行。 • 丢失 - 设备已丢失冗余但以最低资源正常运行。任何进一步的故障都将导致系统关闭。 • 不适用 - 设备未配置电源设备冗余。
power_consumption	（可选）显示功耗值
voltage	（可选）显示 CPU 电压通道 1-24 的值。不包括运行状态。

temperature	（可选）显示处理器和机箱的温度和状态。温度单位为摄氏度。您可以包含关键字以将输出限制为特定区域：**accelerator**、**chassis**、**cpu**、**io-hub**、**motherboard**、**power-supply**。 状态为以下之一： • 正常 - 温度在正常工作范围内，低于 70 摄氏度。 • 严重 - 温度超出正常操作范围。70-80 被认为是温暖的； 80-90 为严重，大于 90 被视为不可恢复。

Command Default

如果没有指定关键字，则显示所有运行信息（驱动程序除外）。

Command History

版本	修改
6.1	引入了此命令。
6.3	我们为 ISA 3000 添加了 **alarm-contact** 关键字。

使用指南

您可以显示设备中物理组件的运行环境信息。此信息包括风扇和电源设备的运行状态，以及CPU和机箱的温度和状态。对于 ISA 3000 设备，它包括有关输入警报触点的信息。

示例

以下是 **show environment** 命令的常规输出示例：

```
> show environment
Cooling Fans:
-------------------------------------
   Power Supplies:
   --------------------------------
   Left Slot (PS0): 6900 RPM - OK  (Power Supply Fan)
   Right Slot (PS1): 7000 RPM - OK  (Power Supply Fan) Power Supplies:
-------------------------------------
   Power Supply Unit Redundancy: OK
   Temperature:
   --------------------------------
   Left Slot (PS0): 26 C - OK  (Power Supply Temperature)
   Right Slot (PS1): 27 C - OK  (Power Supply Temperature)
   Cooling Fans:
   --------------------------------
   Left Slot (PS0): 6900 RPM - OK  (Power Supply Fan)
   Right Slot (PS1): 7000 RPM - OK  (Power Supply Fan)
Temperature:
-------------------------------------
   Processors:
   --------------------------------
   Processor 1: 44.0 C - OK  (CPU1 Core Temperature)
   Processor 2: 45.0 C - OK  (CPU2 Core Temperature)
   Chassis:
   --------------------------------
   Ambient 1: 28.0 C - OK  (Chassis Front Temperature)
   Ambient 2: 40.5 C - OK  (Chassis Back Temperature)
   Ambient 3: 28.0 C - OK  (CPU1 Front Temperature)
```

```
   Ambient 4: 36.50 C - OK  (CPU1 Back Temperature)
   Ambient 5: 34.50 C - OK  (CPU2 Front Temperature)
   Ambient 6: 43.25 C - OK  (CPU2 Back Temperature)
   Power Supplies:
   --------------------------------
   Left Slot (PS0): 26 C - OK  (Power Supply Temperature)
   Right Slot (PS1): 27 C - OK  (Power Supply Temperature)
```

以下是 **show environment driver** 命令的输出示例：

```
> show environment driver
Cooling Fans:
-----------------------------------
   Chassis Fans:
   --------------------------------
   Cooling Fan 1: 5888 RPM - OK
   Cooling Fan 2: 5632 RPM - OK
   Cooling Fan 3: 5888 RPM - OK
   Power Supplies:
   --------------------------------
   Left Slot (PS0): N/A
   Right Slot (PS1): 8448 RPM - OK
Power Supplies:
-----------------------------------
   Left Slot (PS0): Not Present
   Right Slot (PS1): Present
   Left Slot (PS0): N/A
   Right Slot (PS1): 33 C - OK
   Left Slot (PS0): N/A
   Right Slot (PS1): 8448 RPM - OK
Temperature:
-----------------------------------
   Processors:
   --------------------------------
   Processor 1: 70.0 C - OK
   Chassis:
   --------------------------------
   Ambient 1: 36.0 C - OK  (Chassis Back Temperature)
   Ambient 2: 31.0 C - OK  (Chassis Front Temperature)
   Ambient 3: 39.0 C - OK  (Chassis Back Left Temperature)
   Power Supplies:
   --------------------------------
   Left Slot (PS0): N/A
   Right Slot (PS1): 33 C - OK
Voltage:
-----------------------------------
   Channel 1:  1.168 V -  (CPU Core 0.46V-1.4V)
   Channel 2: 11.954 V -  (12V)
   Channel 3:  4.998 V -  (5V)
   Channel 4:  3.296 V -  (3.3V)
   Channel 5:  1.496 V -  (DDR3 1.5V)
   Channel 6:  1.048 V -  (PCH 1.5V)
```

以下是 show environment alarm-contact 命令的输出示例。

```
> show environment alarm-contact
ALARM CONTACT 1
   Status:      not asserted
   Description: external alarm contact 1
   Severity:    minor
   Trigger:     closed
ALARM CONTACT 2
```

```
Status:      not asserted
Description: external alarm contact 2
Severity:    minor
Trigger:     closed
```

Related Commands

命令	Description
clear facility-alarm output	断开输出继电器并清除 LED 的警报状态。
show facility-alarm	显示已触发警报的状态信息。
show version	显示硬件和软件版本。

show facility-alarm

要显示 ISA 3000 设备中触发的警报，请使用 **show facility-alarm** 命令。

show facility-alarm {**relay** | **status** [**major** | **minor** | **info**]}

Syntax Description

relay	显示已激活报警输出继电器的报警。
status [**major** | **minor** | **info**]	显示已触发的所有警报。您可以添加以下关键字来限制列表： • **major**- 显示所有主要严重性警报。 • **minor**- 显示所有次要严重性警报。 • **info**- 显示所有警报。此关键字提供与不使用关键字时相同的视图。

Command History

版本	修改
6.3	引入了此命令。

使用指南

使用 **relay** 关键字可仅查看已激活警报输出继电器的警报。输出警报继电器根据您是否配置触发警报来激活它。启动报警输出中继，激活连接的设备，比如蜂鸣器或闪烁灯的外部警报。

使用 **status** 关键字查看已触发的所有警报，无论警报操作是否触发了外部警报输出继电器。

下表对输出列进行了解释。

列	Description
Source	从中触发报警的设备。这通常是在该设备上配置的主机名。
Severity	严重或轻微。
Description	触发的报警的类型。例如，温度、外部警报接触或冗余电源。
Relay	外部报警输出继电器是通电还是断电。根据您的警报配置触发外部输出警报。
Time	触发的报警的时间戳。

示例

以下是 **show facility-alarm relay** 命令的输出示例：

```
> show facility-alarm relay
Source    Severity   Description                          Relay      Time
firepower minor      external alarm contact 1 triggered  Energized  06:56:50 UTC Mon Sep
22 2014
```

以下是 **show facility-alarm status** 命令的输出示例：

```
> show facility-alarm status info
Source    Severity  Description                          Relay         Time
firepower minor external alarm contact 1 triggered  Energized     06:56:50 UTC Mon Sep 22
2014
firepower minor Temp below Secondary Threshold      De-energized  06:56:49 UTC Mon Sep 22
2014
firepower major Redundant pwr missing or failed     De-energized  07:00:19 UTC Mon Sep 22
2014
firepower major Redundant pwr missing or failed     De-energized  07:00:19 UTC Mon Sep 22
2014

> show facility-alarm status major
Source    Severity  Description                        Relay         Time
firepower major     Redundant pwr missing or failed   De-energized  07:00:19 UTC Mon Sep
22 2014
firepower major     Redundant pwr missing or failed   De-energized  07:00:19 UTC Mon Sep
22 2014


> show facility-alarm status minor
Source    Severity  Description                          Relay         Time
firepower minor     external alarm contact 1 triggered  Energized     06:56:50 UTC Mon Sep
 22 2014
firepower minor     Temp below Secondary Threshold      De-energized  06:56:49 UTC Mon Sep
 22 2014
```

Related Commands

命令	Description
clear facility-alarm output	断开输出继电器并清除 LED 的警报状态。
show alarm settings	显示所有全局报警设置。
show environment alarm-contact	显示输入警报触点的状态。

show failover

要显示有关设备的故障转移状态的信息，请使用 **show failover** 命令。

show failover [**group** *num* | **history** [**details**] | **interface** | **state** | **trace** [*options*] | **statistics** | **details**]

Syntax Description

group *num*	显示指定的故障转移组的运行状态。
history [**details**]	显示故障转移历史记录。故障转移历史记录显示已结束的故障转移状态更改和状态更改的原因。此信息可帮助进行故障排除。 添加 **details** 关键字可显示对等体的故障转移历史记录。这包括故障转移状态更改和对等设备发生状态更改的原因。 历史记录信息会随设备重启而被清除。
interface	显示故障转移和有状态链路信息。
state	显示两个故障切换设备的故障转移状态。显示的信息包括设备的主要或辅助状态、设备的主用/备用状态以及最新报告的故障转移原因。即使清除了故障的原因，故障原因信息也会保留在输出中。
trace [*options*]	（可选）显示故障转移事件跟踪。选项包括按级别 (1-5) 显示故障转移事件跟踪： • **critical** - 过滤故障转移关键事件跟踪（级别 = 1） • **debugging**- 过滤故障转移调试跟踪（调试级别 = 5） • **error**- 过滤故障转移内部异常（级别 = 2） • **informational**- 过滤故障转移信息跟踪（级别 = 4） • **warning**- 过滤故障转移警告（级别 = 3）
statistics	显示故障转移命令接口的传输和接收数据包计数。
details	显示高可用性对中的故障转移详细信息。

Command History

版本	修改
6.1	引入了此命令。
6.2.3	添加了 **history details** 关键字。

版本	修改
6.4	添加了以下对象静态计数。 • 规则数据库 B 同步 • 规则数据库 P-Sync • 规则数据库删除
7.0	添加了 **details** 关键字。

使用指南

show failover 命令显示动态故障转移信息、接口状态和有状态故障转移统计信息。

如果接口上配置了 IPv4 和 IPv6 地址，则两个地址都会出现在输出中。由于一个接口上可配置多个 IPv6 地址，因此只显示本地链路的地址。如果接口上未配置 IPv4 地址，则输出中的 IPv4 地址会显示为 0.0.0.0。如果接口上未配置 IPv6 地址，则输出中会直接省略地址。

只有在启用有状态故障转移时，才会出现有状态故障切换逻辑更新统计信息输出。“xerr”和“rerr”值并不指示故障转移中的错误数，而是指示数据包传输或接收错误数。

在 **show failover** 命令输出中，有状态故障转移字段包含以下值：

- 有状态对象具有以下值：
  - xmit - 指示传输的数据包数。
  - xerr - 指示传输错误数。
  - rcv - 指示接收的数据包数。
  - rerr - 指示接收错误数。
- 每行是针对特定对象的静态计数，如下所示：
  - General - 指示所有有状态对象的总和。
  - sys cmd - 指逻辑更新系统命令，例如 **login** 或 **stay alive**。
  - up time - 指示 threat defense 设备正常工作时间的值，即主用 threat defense 设备传递到备用 threat defense 设备的时间。
  - RPC services - 远程过程调用连接信息。
  - TCP conn - 动态 TCP 连接信息。
  - UDP conn - 动态 UDP 连接信息。
  - ARP tbl - 动态 ARP 表信息。
  - Xlate_Timeout - 指示连接转换超时信息。
  - IPv6 ND tbl - IPv6 邻居发现表信息。
  - VPN IKE upd - IKE 连接信息。

- VPN IPSEC upd - IPsec 连接信息。
- VPN CTCP upd - cTCP 隧道连接信息。
- VPN SDI upd - SDI AAA 连接信息。
- VPN DHCP upd - 隧道化 DHCP 连接信息。
- SIP Session - SIP 信令会话信息。
- Route Session - 路由同步更新的 LU 统计信息
- Rule DB B-Sync - 指示执行规则数据库批量同步的次数以及相应的错误（如有）
- Rule DB P-Sync - 指示规则数据库定期同步的次数以及此操作的错误（如有）
- Rule DB Delete - 指示发送规则数据库删除消息的次数以及此操作的错误（如有）

如果不输入故障转移 IP 地址，则 **show failover** 命令显示 IP 地址为 0.0.0.0，且接口的监控仍处于“等待”状态。您必须设置一个故障转移 IP 地址，故障转移才能工作。

下表介绍了故障转移的接口状态。

表 *32*: 故障转移接口状态

State	Description
Normal	接口正在运行并正在接收来自对等设备上相应接口的问候数据包。
Normal (Waiting)	接口已打开，但尚未从对等体设备上的对应接口接收欢迎数据包。验证已为接口配置备用 IP 地址，并且两个接口之间存在连接。 当故障转移接口关闭时，您也可以看到此状态。
Normal (Not-Monitored)	接口正在运行，但故障转移进程并未监控它。未受监控的接口发生故障时不会触发故障转移。
No Link	物理链路断开。
No Link (Waiting)	物理链路断开，且接口尚未收到来自对等设备上相应接口的问候数据包。在恢复链路后，验证已为接口配置备用IP地址，并且两个接口之间存在连接。
No Link (Not-Monitored)	物理链路断开，但故障转移进程并未监控它。未受监控的接口发生故障时不会触发故障转移。
Link Down	物理链路处于工作状态，但是接口处于管理性关闭状态。
Link Down (Waiting)	物理链路处于工作状态，但是接口处于管理性关闭状态，且接口尚未收到来自对等设备上相应接口的问候数据包。将接口启动后，请检查该接口是否配置了备用 IP 地址，并且两个接口之间是否连接。

State	Description
Link Down (Not-Monitored)	物理链路处于工作状态，但是接口处于管理性关闭状态，且故障转移流程并未监控它。未受监控的接口发生故障时不会触发故障转移。
Testing	接口由于丢失来自对等设备上相应接口的问候数据包而处于测试模式。
Failed	接口测试失败，并且接口标记为发生故障。如果接口故障符合故障转移条件，则接口故障会导致故障转移到备用设备或故障转移组。

示例

以下是主用/备用故障转移的 **show failover** 命令的输出示例。

```
Failover unit Primary
Failover LAN Interface: failover GigabitEthernet0/2 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Failover On
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 61 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.7(0)74, Mate 9.7(0)74
Serial Number: Ours 9A41CKDXQJU, Mate 9A3MFP0H1CP
Last Failover at: 19:23:17 UTC Oct 26 2016
    This host: Primary - Active
        Active time: 589 (sec)
        slot 0: empty
          Interface diagnostic (0.0.0.0): Normal (Waiting)
          Interface outside (192.168.77.1): Normal (Waiting)
          Interface inside (192.168.87.1): Normal (Waiting)
        slot 1: snort rev (1.0)  status (up)
        slot 2: diskstatus rev (1.0)  status (up)
    Other host: Secondary - Standby Ready
        Active time: 0 (sec)
          Interface diagnostic (0.0.0.0): Normal (Waiting)
          Interface outside (0.0.0.0): Normal (Waiting)
          Interface inside (0.0.0.0): Normal (Waiting)
        slot 1: snort rev (1.0)  status (up)
        slot 2: diskstatus rev (1.0)  status (up)
Stateful Failover Logical Update Statistics
    Link : failover GigabitEthernet0/2 (up)
    Stateful Obj       xmit       xerr       rcv        rerr
    General            45         0          44         0
    sys cmd            44         0          44         0
    up time            0          0          0          0
    RPC services       0          0          0          0
    TCP conn           0          0          0          0
    UDP conn           0          0          0          0
    ARP tbl            0          0          0          0
    Xlate_Timeout      0          0          0          0
    IPv6 ND tbl        0          0          0          0
    VPN IKEv1 SA       0          0          0          0
    VPN IKEv1 P2       0          0          0          0
    VPN IKEv2 SA       0          0          0          0
```

```
VPN IKEv2 P2        0           0           0           0
VPN CTCP upd        0           0           0           0
VPN SDI upd         0           0           0           0
VPN DHCP upd        0           0           0           0
SIP Session         0           0           0           0
SIP Tx              0           0           0           0
SIP Pinhole         0           0           0           0
Route Session       0           0           0           0
Router ID           0           0           0           0
User-Identity       1           0           0           0
CTS SGTNAME         0           0           0           0
CTS PAC             0           0           0           0
TrustSec-SXP        0           0           0           0
IPv6 Route          0           0           0           0
STS Table           0           0           0           0
Rule DB B-Sync      0           0           1           0
Rule DB P-Sync      5           0           1           0
Rule DB Delete      12          0           5           0

Logical Update Queue Information
           Cur   Max  Total
Recv Q:    0     10    44
Xmit Q:    0     11    238
```

以下是主用-备用设置的 **show failover state** 命令的输出示例。

```
> show failover state

               State          Last Failure Reason      Date/Time
This host  -   Primary
               Negotiation    Backplane Failure        15:44:56 UTC Jun 20 2016
Other host -   Secondary
               Not Detected   Comm Failure             15:36:30 UTC Jun 20 2016

====Configuration State===
        Sync Done
====Communication State===
        Mac set
```

下表介绍了 **show failover state** 命令的输出。

表 *33: show failover state* 输出说明

字段	Description
Configuration State	显示配置同步状态。 以下是备用设备的可能配置状态： • **Config Syncing - STANDBY**- 在执行同步配置时设置。 • **Interface Config Syncing - STANDBY** • **Sync Done - STANDBY**- 当备用设备完成从主用设备的配置同步时设置。 以下是主用设备的可能配置状态： • **Config Syncing**- 在主用设备执行与备用设备的配置同步时在主用设备上设置。 • **Interface Config Syncing** • **Sync Done**- 在主用设备已成功完成到备用设备的配置同步时设置。 • **Ready for Config Sync**- 在备用设备发出准备好接收配置同步的信号时在主用设备上设置。
Communication State	显示 MAC 地址同步状态。 • **Mac set**- MAC 地址已完成从对等设备至此设备的同步。 • **Updated Mac**- 在 MAC 地址已更新并需要同步到另一设备时使用。在设备正在更新从对等设备同步的本地 MAC 地址的过渡期间也使用此状态。
Date/Time	显示故障的日期和时间戳。
Last Failure Reason	显示最后报告故障的原因。此信息不会清除，即使故障情况已清除。只有发生故障转移时，此信息才会变更。 以下是可能的故障原因： • **Interface Failure**- 发生故障的接口数量符合故障切换条件并导致故障转移。 • **Comm Failure**- 故障转移链路发生故障或对等体关闭。 • **Backplane Failure**
State	显示设备的主要/辅助和主用/备用状态。
This host/Other host	此主机指示被执行命令的设备的信息。其他主机指示故障转移配对中的另一个设备的信息。

以下是主设备上 **show failover history** 命令的输出示例：

```
> show failover history
==========================================================================
From State                To State                  Reason
==========================================================================
14:29:59 UTC Nov 11 2017
Not Detected              Negotiation               No Error

14:30:36 UTC Nov 11 2017
Negotiation               Cold Standby              Detected an Active mate

14:30:38 UTC Nov 11 2017
Cold Standby              Sync Config               Detected an Active mate

14:30:47 UTC Nov 11 2017
Sync Config               Sync File System          Detected an Active mate

14:30:47 UTC Nov 11 2017
Sync File System          Bulk Sync                 Detected an Active mate

14:31:00 UTC Nov 11 2017
Bulk Sync                 Standby Ready             Detected an Active mate

14:31:39 UTC Nov 11 2017
Standby Ready             Failed                    Interface check
                                                    This host:1
                                                    single_vf: OUTSIDE
                                                    Other host:0

14:31:46 UTC Nov 11 2017
Failed                    Standby Ready             Interface check
                                                    This host:0
                                                    Other host:0

14:33:36 UTC Nov 11 2017
Standby Ready             Just Active               HELLO not heard from mate

14:33:36 UTC Nov 11 2017
Just Active               Active Drain              HELLO not heard from mate

14:33:36 UTC Nov 11 2017
Active Drain              Active Applying Config    HELLO not heard from mate

14:33:36 UTC Nov 11 2017
Active Applying Config    Active Config Applied     HELLO not heard from mate

14:33:36 UTC Nov 11 2017
Active Config Applied     Active                    HELLO not heard from mate

==========================================================================
```

以下是辅助设备上 **show failover history** 命令的输出示例：

```
> show failover history
==========================================================================
From State                To State                  Reason
==========================================================================
17:17:29 UTC Nov 10 2017
Not Detected              Negotiation               No Error
```

```
17:18:06 UTC Nov 10 2017
Negotiation               Cold Standby              Detected an Active mate

17:18:08 UTC Nov 10 2017
Cold Standby              Sync Config               Detected an Active mate

17:18:17 UTC Nov 10 2017
Sync Config               Sync File System          Detected an Active mate

17:18:17 UTC Nov 10 2017
Sync File System          Bulk Sync                 Detected an Active mate

17:18:30 UTC Nov 10 2017
Bulk Sync                 Standby Ready             Detected an Active mate

17:19:09 UTC Nov 10 2017
Standby Ready             Failed                    Interface check
                                                    This host:1
                                                    single_vf: OUTSIDE
                                                    Other host:0

17:19:21 UTC Nov 10 2017
Failed                    Standby Ready             Interface check
                                                    This host:0
                                                    Other host:0

================================================================================
```

每个条目提供状态更改的时间和日期、初始状态、结果状态和状态更改的原因。最新的条目位于显示画面的底部。较旧的条目显示在顶部。最多可以显示 60 个条目。一旦到达条目数上限，随着新条目添加至底部，最旧的条目就会从输出的顶部移除。

失败原因包括有助于进行故障排除的详细信息。其中包括接口检查、故障转移状态检查、状态进程故障和服务模块故障。

以下是 **show failover history details** 命令的输出示例：

```
>show failover history details
================================================================================
From State                To State                  Reason
================================================================================
09:58:07 UTC Jan 18 2017
Not Detected              Negotiation               No Error

09:58:10 UTC Jan 18 2017
Negotiation               Just Active               No Active unit found

09:58:10 UTC Jan 18 2017
Just Active               Active Drain              No Active unit found

09:58:10 UTC Jan 18 2017
Active Drain              Active Applying Config    No Active unit found

09:58:10 UTC Jan 18 2017
Active Applying Config    Active Config Applied     No Active unit found

09:58:10 UTC Jan 18 2017
Active Config Applied     Active                    No Active unit found

================================================================================
```

```
PEER History Collected at 09:58:54 UTC Jan 18 2017
=======================PEER-HISTORY=========================================
From State                To State                    Reason
=========================PEER-HISTORY=========================================
09:57:46 UTC Jan 18 2017
Not Detected              Negotiation                 No Error

09:58:19 UTC Jan 18 2017
Negotiation               Cold Standby                Detected an Active mate

09:58:21 UTC Jan 18 2017
Cold Standby             Sync Config                  Detected an Active mate

09:58:29 UTC Jan 18 2017
Sync Config              Sync File System             Detected an Active mate

09:58:29 UTC Jan 18 2017
Sync File System         Bulk Sync                    Detected an Active mate

09:58:42 UTC Jan 18 2017
Bulk Sync                Standby Ready                Detected an Active mate

=========================PEER-HISTORY=========================================
```

show failover history details 命令会请求对等体的故障转移历史记录，并打印设备故障转移历史记录以及对等体的最新故障转移历史记录。如果对等体在一秒内未响应，则会显示上次收集的故障转移历史记录信息。

下表显示了故障转移状态。有稳定和临时两种状态类型。稳定状态是发生如故障之类的情况而导致状态更改之前设备可保持的状态。临时状态是设备达到稳定状态时所经过的状态。

表 *34:* 故障转移状态

状态	Description
Disabled	禁用故障转移。这是稳定状态。
Failed	设备处于故障状态。这是稳定状态。
Negotiation	设备建立与对等设备的连接，并与其协商确定软件版本兼容性和主用/备用角色。根据协商的角色，设备将经历备用设备状态或主用设备状态，或进入故障状态。这是临时状态。
Not Detected	ASA 无法检测到对等设备的存在。若 ASA 启动并启用故障转移而对等设备不存在或关闭，会发生这种情况。
备用设备状态	
Cold Standby	设备等待对等设备进入主用状态。当对等设备进入主用状态时，此设备进入备用配置状态。这是临时状态。
Sync Config	设备请求来自对等设备的运行配置。如果配置同步时发生错误，设备会回到初始化状态。这是临时状态。
Sync File System	设备与对等设备同步文件系统。这是临时状态。

状态	Description
Bulk Sync	设备接收对等设备的状态信息。只有启用有状态故障转移时，才会出现此状态。这是临时状态。
Standby Ready	设备已准备好在主用设备发生故障时接管。这是稳定状态。
主用设备状态	
Just Active	设备成为主用设备时进入的第一个状态。在此状态时会向对等设备发送消息，向对等设备警报该设备成为主用设备并为接口设置IP地址和MAC地址。这是临时状态。
Active Drain	丢弃来自对等设备的消息队列。这是临时状态。
Active Applying Config	设备正在应用系统配置。这是临时状态。
Active Config Applied	设备已完成应用系统配置。这是临时状态。
Active	设备处于主用状态并在处理流量。这是稳定状态。

每个状态更改后面都附带状态更改原因。在设备从临时状态过渡到稳定状态时，原因通常保持相同。以下是可能的状态更改原因：

- 未出现错误
- 通过 CI config 命令设置
- 故障转移状态检查
- 故障转移接口恢复正常
- 未收到对方的问候消息
- 另一设备具有不同的软件版本
- 另一设备操作模式不同
- 另一设备许可证不同
- 另一设备机箱配置不同
- 另一设备卡配置不同
- 另一设备要本设备成为主用设备
- 另一设备要本设备成为备用设备
- 另一设备报告本设备已发生故障
- 另一设备报告该设备已发生故障
- 配置不匹配
- 检测到主用对等设备

- 未找到主用设备
- 已完成配置同步
- 已从通信故障恢复
- 另一设备具有不同的 VLAN 组配置
- 无法验证 VLAN 配置
- 配置同步未完成
- 配置同步失败
- 接口检查
- 我的通信失败
- 针对故障转移消息没有收到 ACK
- 另一设备在同步后进入卡机状态
- 从对等设备中检测不到电源
- 没有故障转移电缆
- 高可用性状态进度失败
- 检测服务卡故障
- 另一设备中的服务卡发生故障
- 本设备与对等设备的服务卡都正常
- LAN 接口变成未配置
- 对等设备刚刚重新加载
- 从串行电缆切换到基于 LAN 的故障切换
- 无法验证配置同步的状态
- 自动更新请求
- 未知原因

以下是 **show failover interface** 命令的输出示例。设备已对故障转移接口配置 IPv6 地址。

```
> show failover interface
        interface folink GigabitEthernet0/2
                System IP Address: 2001:a0a:b00::a0a:b70/64
                My IP Address    : 2001:a0a:b00::a0a:b70
                Other IP Address : 2001:a0a:b00::a0a:b71
```

以下是来自高可用性对上的对等设备的 **show failover details** 命令的输出示例。

```
> show failover details
        Failover On
Failover unit Secondary
Failover LAN Interface: HA-LINK GigabitEthernet0/3 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
1 Hold Interval Success: 12 Failure: 0
2 Hold Interval Success: 15 Failure: 0
3 Hold Interval Success: 15 Failure: 0
4 Hold Interval Success: 15 Failure: 0
5 Hold Interval Success: 15 Failure: 0
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 1 of 311 maximum
Interface: management
        1 Hold Success: 0 Failure: 0
        2 Hold Success: 0 Failure: 0
        3 Hold Success: 0 Failure: 0
        4 Hold Success: 0 Failure: 0
        5 Hold Success: 0 Failure: 0
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 99.16(2)10, Mate 99.16(2)10
Serial Number: Ours 9A7WJNE35T5, Mate 9A3497TXPU6
Last Failover at: 06:56:25 UTC Jan 25 2021
        This host: Secondary - Standby Ready
                Active time: 0 (sec)
                slot 0: ASAv hw/sw rev (/99.16(2)10) status (Up Sys)
                  Interface management (203.0.113.130/fe80::250:56ff:feb7:4927): Unknown
(Waiting)
                slot 1: snort rev (1.0)  status (up)
                snort poll success:2877 miss:0
                slot 2: diskstatus rev (1.0)  status (up)

                disk poll success:2877 miss:0
        Other host: Primary - Active
                Active time: 2910 (sec)
                  Interface management (203.0.113.130): Unknown (Waiting)
                slot 1: snort rev (1.0)  status (up)
                peer snort poll success:2877 miss:0
                slot 2: diskstatus rev (1.0)  status (up)

                peer disk poll success:2877 miss:0

Stateful Failover Logical Update Statistics
        Link : HA-LINK GigabitEthernet0/3 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         379        0          380        0
        sys cmd         379        0          379        0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        0          0          0          0
        UDP conn        0          0          0          0
        ARP tbl         0          0          0          0
        Xlate_Timeout   0          0          0          0
        IPv6 ND tbl     0          0          0          0
        VPN IKEv1 SA    0          0          0          0
        VPN IKEv1 P2    0          0          0          0
        VPN IKEv2 SA    0          0          0          0
        VPN IKEv2 P2    0          0          0          0
        VPN CTCP upd    0          0          0          0
        VPN SDI upd     0          0          0          0
        VPN DHCP upd    0          0          0          0
```

```
SIP Session     0          0          0          0
SIP Tx  0       0          0          0
SIP Pinhole     0          0          0          0
Route Session   0          0          0          0
Router ID       0          0          0          0
User-Identity   0          0          1          0
CTS SGTNAME     0          0          0          0
CTS PAC         0          0          0          0
TrustSec-SXP    0          0          0          0
IPv6 Route      0          0          0          0
```

以下是 **show failover trace** 命令的故障转移警告示例：

```
> show failover trace warning
        Warning:Output can be huge. Displaying in pager mode
        Oct 14 UTC 20:56:56.345 [CABLE]    [ERROR]fover: peer rcvd down ifcs info
        Oct 14 UTC 20:56:56.345 [CABLE]    [ERROR]fover: peer has  1  down ifcs
        Oct 14 UTC 20:56:56.345 [CABLE]    [ERROR]fover: peer rcvd down ifcs info
        Oct 14 UTC 20:56:56.345 [CABLE]    [ERROR]fover: peer has  1  down ifcs
        Oct 14 UTC 20:56:56.345 [CABLE]    [ERROR]fover: peer rcvd down ifcs info
```

Related Commands

命令	Description
show running-config failover	在当前配置中显示 **failover** 命令。

show failover exec

要显示指定设备的 **failover exec** 命令模式，请使用 **show failover exec** 命令。

show failover exec {**active** | **standby** | **mate**}

Syntax Description

active	显示主用设备的 **failover exec** 命令模式。
mate	显示对等设备的 **failover exec** 命令模式。
standby	显示备用设备的 **failover exec** 命令模式。

Command History

版本	修改
6.1	引入了此命令。

使用指南

failover exec 命令会创建与指定设备的会话。默认情况下，该会话处于全局配置模式，即使 threat defense 不支持 CLI 配置。模式信息与 threat defense无关。

show failover exec 命令显示指定设备上的命令模式，通过 **failover exec** 命令发送的命令在该设备中执行。

示例

以下是 **show failover exec** 命令的输出示例。

```
> show failover exec mate
Standby unit Failover EXEC is at config mode
```

Related Commands

命令	Description
failover exec	在故障切换对中的指定设备上执行提供的命令。

show file

要显示有关文件系统的信息，请使用 **show file** 命令。

show file [**descriptors** | **system** | **information** *filename*]

Syntax Description

descriptors	显示所有打开文件描述符。
information *filename*	显示有关特定文件的信息，包括合作伙伴应用包文件。
system	显示有关磁盘文件系统的大小、可用字节数、介质类型、标志和前缀信息。

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show file system** 命令的输出示例。

```
> show file system
File Systems:
     Size(b)     Free(b)      Type      Flags  Prefixes
* 7935832064    7828107264    disk      rw      disk0: flash:
              -             -  disk      rw      disk1:
              -             -  network   rw      tftp:
              -             -  opaque    rw      system:
              -             -  network   ro      http:
              -             -  network   ro      https:
              -             -  network   rw      scp:
              -             -  network   rw      ftp:
              -             -  network   wo      cluster:
              -             -  stub      ro      cluster_trace:
              -             -  network   rw      smb:
```

以下是 **show file information** 命令的输出示例：

```
> show file information install.log
disk0:/install.log:
  type is ascii text
  file size is 150484 bytes
```

Related Commands

命令	Description
dir	系统随即会显示目录的内容。
pwd	系统随即会显示当前工作目录。

show firewall

要显示当前防火墙模式（路由或透明），请使用 **show firewall** 命令。

show firewall

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show firewall** 命令的输出示例：

```
> show firewall
Firewall mode: Router
```

Related Commands

命令	Description
configure firewall	设置防火墙模式。
show mode	显示当前情景模式（单模式或多模式）。

show flash

要显示内部闪存的内容，请使用 **show flash:** 命令。

show flash: ［**all** | **controller** | **filesys**］

注释 在 threat defense中， **flash** 关键字的别名为 **disk0**。

Syntax Description

all	显示所有闪存信息。
controller	显示文件系统控制器信息。
filesys	显示文件系统信息。

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show flash:** 命令的输出示例：

```
> show flash:
--#--  --length--  -----date/time------  path
   48  107030784   Oct 05 2016 02:10:26  os.img
   49  33          Oct 06 2016 16:15:24  .boot_string
   50  150484      Oct 06 2016 15:36:02  install.log
   11  4096        Oct 06 2016 15:58:16  log
   13  1065        Oct 06 2016 15:59:13  log/asa-appagent.log
   16  4096        Oct 06 2016 15:59:07  crypto_archive
   51  4096        Oct 06 2016 15:59:12  coredumpinfo
   52  59          Oct 06 2016 15:59:12  coredumpinfo/coredump.cfg
   53  36          Oct 06 2016 16:04:47  enable_configure

7935832064 bytes total (7828107264 bytes free)
```

Related Commands

命令	Description
dir	系统随即会显示目录的内容。
show disk0:	显示内部闪存的内容。
show disk1:	显示外部闪存卡的内容。

show flow-export counters

要查看 NetFlow 统计信息和错误数据的运行时间计数器，请使用 **show flow-export counters** 命令。

show flow-export counters

Command History

版本	修改
6.3	引入了此命令。

示例

以下示例显示如何显示 Netflow 运行时间计数器。

```
> show flow-export counters

destination: inside 209.165.200.224 2055
 Statistics:
  packets sent                      1000
 Errors:
  block allocation failure             0
  invalid interface                    0
  template send failure                0
  no route to collector                0
  source port allocation               0
```

Related Commands

命令	Description
clear flow-export counters	将 NetFlow 中的所有运行时间计数器重置为零。

show flow-offload

要查看流、计数器、统计信息以及有关分流的流的信息，请使用 **show flow-offload** 命令。

此命令在 Firepower 4100/9300 机箱的 threat defense 上可用。

show flow-offload {**flow**[**count**|**detail**]|**dynamic**[**count**|**detail**]|**static**[**count**|**detail**]|**info**[**detail**]|**statistics**}

Syntax Description

flow[**dynamic**|**static**]|[**count**|**detail**]	无参数时，显示正在使用的静态和动态流、最大使用量、分流百分比和冲突数量。 添加 **dynamic** 或 **static** 关键字，以分别显示动态或静态流的计数器、统计信息和信息。 您可以选择添加以下关键字： • **count**：已分流的活动流数和已创建的分流流数。 • **detail**：活动的分流数据流及其重写规则和数据。
info[**detail**]	动态数据流分流的当前状态。添加 **detail** 关键字以获取其他信息，例如端口使用情况摘要。
statistics	数据包计数、成功传输和错误。

Command History

版本	修改
6.3	引入了此命令。

使用指南

使用 **show flow-offload** 命令显示流、计数器、统计信息和有关流分流的信息。

使用 **clear flow-offload** 命令清除计数器或统计信息。

以下是 **show flow-offload flow** 命令的输出示例。分流数据流由索引号标识，该索引号通过散列源和目的 IP 地址、端口和协议来计算。当系统尝试分流与当前活动分流的流具有相同索引的流时，会发生 冲突 。在这种情况下，不会分流新的数据流，但第一个数据流会保持分流状态。

```
>show flow-offload flow
Total offloaded flow stats: 1 in use, 5 most used, 100% offloaded, 0 collisions
UDP intfc 103 src 10.1.1.2:41110 dest 20.1.1.2:5001, dynamic, timestamp 162810457, packets
 84040, bytes 127404640
```

以下是 **show flow-offload flow count** 命令的输出示例。

```
>show flow-offload flow count
Total offloaded flow stats:  4 in use, 20 most used, 10% offloaded, 0 collisions
```

以下是 **show flow-offload flow detail** 命令的输出示例。 rw(*number*) 表示已为该特定分流数据流重写标准报头字段，例如 MAC 或 VLAN。

```
>show flow-offload flow detail
Total offloaded flow stats: 2 in use, 6 most used, 100% offloaded, 0 collisions
TCP vlan 711 intfc 101 src 172.16.1.3:21766 dest 9.9.1.3:80, dynamic, timestamp 217959066,
 packets 633139, bytes 43053452
    node 0, ft index 58197, queue_id 727
    rw(0): cmd '  replace', offset  0, bytes 12, data(x) 90E2 BA01 8E29 B0AA 7730 097B
    rw(1): cmd 'increment', offset 46, bytes  4, data(x) 422AC658
```

以下是 **show flow-offload dynamic** 命令的输出示例。

```
>show flow-offload flow dynamic
Dynamically offloaded flow stats: 2 in use, 6 most used, 100% offloaded, 0 collisions
   TCP vlan 711 intfc 101 src 172.16.1.3:21809 dest 9.9.1.3:80, dynamic, timestamp 218392513,
 packets 14741, bytes 1002388
   TCP vlan 911 intfc 102 src 9.9.1.3:80 dest 172.16.1.3:21809, dynamic, timestamp 218392534,
 packets 16794, bytes 23972345
```

以下是 **show flow-offload dynamic count** 命令的输出示例。

```
>show flow-offload flow dynamic count
Dynamically offloaded flow stats: 2 in use, 6 most used, 100% offloaded, 0 collisions
```

以下是 **show flow-offload dynamic detail** 命令的输出示例。

```
>show flow-offload flow dynamic detail
Total offloaded flow stats: 4 in use, 20 most used, 10% offloaded, 0 collisions
TCP intfc 134 src 9.9.1.3:80 dest 192.168.0.3:5240, static, timestamp 142633202, packets
442870, bytes 630342730
TCP intfc 133 src 192.168.0.3:5240 dest 9.9.1.3:80, static, timestamp 142633204, packets
442971, bytes 28350144
TCP intfc 136 src 9.9.1.4:80 dest 192.168.0.4:7240, dynamic, timestamp 142633876, packets
82870, bytes 10342730
TCP intfc 135 src 192.168.0.4:7240 dest 9.9.1.4:80, dynamic, timestamp 142633877, packets
82971, bytes 350144
```

以下是 **show flow-offload info** 命令的输出示例。 **Current running state** 是流分流的当前状态，保留供将来实施（该值当前不可配置）。 **User configured state** 是受管设备重新启动时的数据流分流状态。（目前，这些值将始终相同。） **Dynamic flow offload** 是动态数据流分流的当前状态。

```
>show flow-offload flow info
Current running state        : Enabled
User configured state        : Enabled
Dynamic flow offload         : Enabled
```

以下是 **show flow-offload info detail** 命令的输出示例。

```
> show flow-offload flow info detail
Current running state        : Enabled
User configured state        : Enabled
Dynamic flow offload       : Enabled
Offload App                  : Running
Offload allocated cores      : S0[ 1] S1[ 13]
Offload reserved Nic         : 9 22
Max PKT burst                : 32
Port-0 details :
        RX queue number      :            149
        FQ queue number      :            727
        Keep alive counter   :         142327
Port-1 details :
        RX queue number      :            147
```

```
        FQ queue number      :            725
        Keep alive counter   :         142328
```

以下是 **show flow-offload statistics** 命令的输出示例。 **VNIC** 指在其上分流动态数据流的硬件。

```
> show flow-offload statistics
Packet stats of port : 0
    Tx Packet count                 :      16483549549
    Rx Packet count                 :      16483549549
    Dropped Packet count            :                0
    VNIC transmitted packet         :      16483549549
    VNIC transmitted bytes          :   12389816183297
    VNIC Dropped packets            :                0
    VNIC erroneous received         :                0
    VNIC CRC errors                 :                0
    VNIC transmit failed            :                0
    VNIC multicast received         :                0
```

Related Commands

命令	Description
configure flow-offload	启用或禁用动态数据流分流。
clear flow-offload	清除动态数据流分流计数器或统计信息。

show flow-offload-ipsec

要显示有关 IP sec 数据流分流的信息，请使用 **show flow-offload-ipsec**。

show flow-offload-ipsec { **info** | **option-table** | **statistics** }

Syntax Description

info	显示有关 IPsec 流分流的当前配置状态的信息。
option-table	显示 IPsec 数据流分流中使用的内容可寻址内存 (CAM) 的表信息。此信息仅用于调试，对最终用户没有意义。
statistics	显示分流数据流的内容可寻址内存 (CAM) 统计信息。

Command History

版本	修改
7.2	引入了此命令。

示例

以下示例显示 IPsec 流分流的当前配置状态。

```
ciscoasa# show flow-offload-ipsec info
IPSec offload : Enabled
Egress optimization: Enabled
```

以下示例显示统计信息。

```
> show flow-offload-ipsec statistics

        Packet stats of Pipe 0
        ----------------------
        Rx Packet count                          :               0
        Tx Packet count                          :               0
        Error Packet count                       :               0
        Drop Packet count                        :               0

        CAM stats of Pipe 0
        -----------------------
        Option ID Table CAM Hit Count            :              38
        Option ID Table CAM Miss Count           :             154
        Tunnel Table CAM Hit Count               :               0
        Tunnel Table CAM Miss Count              :               0
        6-Tuple CAM Hit Count                    :               0
        6-Tuple CAM Miss Count                   :              38
```

以下示例显示选项表。

```
> show flow-offload-ipsec option-table
        instance_id:256 interface_id:124 action:0 logic_id_opt:0 subinterface_id_opt:0
```

```
instance_id:256 interface_id:123 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:122 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:121 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:120 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:119 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:118 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:117 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:156 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:157 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:158 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:159 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:112 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:111 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:110 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:109 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:108 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:107 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:106 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:105 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:104 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:103 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:102 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:101 action:0 logic_id_opt:0 subinterface_id_opt:0
```

Related Commands

命令	Description
clear flow-offload-ipsec	清除 IPsec 流量分流统计信息。

show fqdn

要显示有关完全限定域名 (FQDN) 网络对象名称解析的故障排除信息，请使用 **show fqdn** 命令。

show fqdn ［**id** ［*fqdn_id*］ | **ip** ［*ip_address*］］

Syntax Description

id [*fqdn_id*]	根据与 FQDN 网络对象关联的 ID 编号显示信息。ID 由系统分配。您可以选择包含 ID 值，通过检查 **show running-config** 命令的输出即可找到该值。例如，以下对象的 ID 编号为 1001。
	
	`object network www.example.com`
	` fqdn www.example.com id 1001`

ip [*ip_address*]	根据从 DNS 服务器获取的 IP 地址显示信息。您可以选择输入 IP 地址。

Command History

版本	修改
6.3	引入了此命令。

使用指南

使用此命令进行故障排除。如果要查看 FQDN 如何映射到 IP 地址，请使用 **show dns** 命令而不是此命令。

show fqdn 命令提供通过系统提供的每个对象的 ID 编号将名称解析与特定网络对象关联的详细信息。

示例

以下示例显示如何查看对象 ID 和 IP 地址的 FQDN 映射。

```
> show fqdn

FQDN IP Table:
ip=10.1.45.1, object=Testobj-1, domain=www.cisco.com, hits=10,
           id=45893456,63987645

ip=2001::134, object=Testobj-1, domain=www.cisco.com, hits=10,
          id=45893456

FQDN ID Table:
id=45893456, object=Testobj-1, domain=www.cisco.com
           ip=10.1.45.1, ip=34.12.45.189
           ip6=2001::134

id=23987645, object=Testobj-2, domain=www.google.com
           ip=20.11.65.121, ip=101.2.4.69
```

Related Commands

命令	Description
clear dns	删除 FQDN 网络对象 DNS 解析。
show dns	显示 FQDN 网络对象 DNS 解析。
show running-config	显示运行配置。

show fragment

要显示 IP 分片重组模块的操作数据，请输入 **show fragment**。

show fragment ［*interface*］

Syntax Description

interface	（可选）指定 threat defense 接口。

Command Default

如果未指定接口，则此命令应用于所有接口。

Command History

版本	修改
6.1	引入了此命令。
6.7	增强了 **show fragment** 命令的输出，包括 IP 分段相关丢包和错误计数器。

示例

以下示例展示如何显示 IP 分段重组模块的操作数据：

```
> show fragment
Interface: inside
Configuration: Size: 200, Chain: 24, Timeout: 5, Reassembly: virtual
Run-time stats: Queue: 0, Full assembly: 12
Drops: Size overflow: 0, Timeout: 0,
Chain overflow: 0, Fragment queue threshold exceeded: 0,
Small fragments: 0, Invalid IP len: 0,
Reassembly overlap: 26595, Fraghead alloc failed: 0,
SGT mismatch: 0, Block alloc failed: 0,
Invalid IPV6 header: 0
```

其中：

- 大小：在已配置为默认值的任何给定点，允许驻留在分段数据库中的最大块数（每个接口）。
- 链 - 可将一个完整 IP 数据包分段为分片的最大数量。默认为 24。
- 超时 - 等待整个分段数据包到达的最大秒数。默认值为 5 秒。
- 重组：虚拟或完整。默认值为虚拟重组。在 ASA 处终止或需要在应用级别进行检测的 IP 分段将完全（物理）重组。如有必要，完全（物理）重组的数据包可以在出口接口上再次分片。
- 大小溢出：已达到任何给定点允许驻留在分段数据库中的最大块数。溢出计数器测量由于达到分段数据库的默认大小而导致的丢包。此计数器不包括由于队列大小（最大数据库大小的2/3）而丢弃的分段数。
- 超时：片段链在重组完成之前已超时。
- 链限制：已达到单个分片链限制。

- 超出分段队列阈值：已超出分段数据库阈值，即每个接口的队列大小的 2/3。
- 小分片：分片偏移量大于 0 但小于 16 时。
- 数据包长度无效：IP 数据包长度无效（例如，长度大于 65535）。
- 重组重叠：检测到重复或重叠的片段。
- 分段标题分配失败：无法分配分段标题。分段标题维护 IP 数据包的所有分段链。
- SGT 不匹配：相同 IP 数据包的分段之间的 SGT 值不匹配。
- 块分配失败：完全重组的分配失败。
- 无效的 IPV6 信头：在完全重组期间遇到无效的 IPV6 信头。

Related Commands

命令	Description
clear configure fragment	清除 IP 分段重组配置并重置默认值。
clear fragment	清除 IP 分段重组模块的运行数据。
show running-config fragment	显示 IP 分段重组配置。

show gc

要显示垃圾收集进程统计信息，请使用 **show gc** 命令。

show gc

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show gc** 命令的输出示例：

```
> show gc

Garbage collection process stats:
Total tcp conn delete response             :            0
Total udp conn delete response             :            0
Total number of zombie cleaned             :            0
Total number of embryonic conn cleaned     :            0
Total error response                       :            0
Total queries generated                    :            0
Total queries with conn present response   :            0
Total number of sweeps                     :          946
Total number of invalid vcid               :            0
Total number of zombie vcid                :            0
```

Related Commands

命令	Description
clear gc	删除垃圾回收进程统计信息。

show h225

show h225 命令显示有关通过 threat defense 设备建立的 H.225 会话的信息。

show h225

Command History

版本	修改
6.1	引入了此命令。

使用指南

show h225 命令显示有关通过设备建立的 H.225 会话的信息。

如果存在异常大量的连接，请根据默认超时值或设置的超时值检查会话是否超时。如果未超时，则需要调查问题。

示例

以下是 **show h225** 命令的输出示例：

```
> show h225
Total H.323 Calls: 1
1 Concurrent Call(s) for
    Local:   10.130.56.3/1040   Foreign: 172.30.254.203/1720
    1. CRV 9861
    Local:   10.130.56.3/1040   Foreign: 172.30.254.203/1720
0 Concurrent Call(s) for
    Local:   10.130.56.4/1050   Foreign: 172.30.254.205/1720
```

此输出表示目前有 1 个活动 H.323 呼叫正通过本地终端 10.130.56.3 与外部主机 172.30.254.203 之间的 threat defense，而且对于这些特定终端，在它们之间有 1 个并发呼叫，该呼叫的 CRV 为 9861。

对于本地终端 10.130.56.4 和外部主机 172.30.254.205，有 0 个并发呼叫。这意味着即使 H.225 会话仍然存在，终端之间也没有活动呼叫。如果在执行 **show h225** 命令时呼叫已结束但 H.225 会话尚未删除，就可能会发生这种情况。它也可能意味着两个终端之间还有开启的 TCP 连接，因为这些终端将“maintainConnection”设置为 TRUE，所以在这些终端将“maintainConnection”重新设置为 FALSE 或在会话根据您配置中的 H.225 超时值超时之前，会话保持开启。

Related Commands

命令	Description
show h245	显示关于终端使用缓慢启动在设备范围内建立的 H.245 会话的信息。
show h323 ras	显示关于在设备范围内建立的 H.323 RAS 会话的信息。

show h245

要显示关于终端使用缓慢启动在 threat defense 设备范围内建立的 H.245 会话的信息，请使用 **show h245** 命令。

show h245

Command History

版本	修改
6.1	引入了此命令。

使用指南

show h245 命令显示关于终端使用缓慢启动在 threat defense 设备范围内建立的 H.245 会话的信息。（当呼叫的两个终端打开 H.245 的另一个 TCP 控制信道时，即为慢启动。当 H.245 消息作为 H.225 消息的一部分在 H.225 控制信道上交换时，即为快启动。

示例

以下是 **show h245** 命令的输出示例：

```
> show h245
Total: 1
        LOCAL           TPKT    FOREIGN         TPKT
1       10.130.56.3/1041        0       172.30.254.203/1245    0
        MEDIA: LCN 258 Foreign 172.30.254.203 RTP 49608 RTCP 49609
                       Local   10.130.56.3 RTP 49608 RTCP 49609
        MEDIA: LCN 259 Foreign 172.30.254.203 RTP 49606 RTCP 49607
                       Local   10.130.56.3 RTP 49606 RTCP 49607
```

目前有一个跨 threat defense 设备的 H.245 控制会话处于活动状态。本地终端是 10.130.56.3，来自此终端的下一个数据包预计将会包含 TPKT 报头，因为 TPKT 值为 0。（TKTP 信头是位于每条 H.225/H.245 消息之前的 4 字节信头。TKTP 信头提供消息长度，包括 4 字节信头在内。）外部主机终端是 172.30.254.203，来自此终端的下一个数据包预计将会包含 TPKT 报头，因为 TPKT 值为 0。

在这些终端之间协商的媒体的 LCN（逻辑信道编号） 为 258，该 LCN 的外部 RTP IP 地址/端口对为 172.30.254.203/49608，RTCP IP 地址/端口对为 172.30.254.203/49609，本地 RTP IP 地址/端口对为 10.130.56.3/49608，RTCP 端口为 49609。

第二个 LCN 为 259，该 LCN 的外部 RTP IP 地址/端口对为 172.30.254.203/49606，RTCP IP 地址/端口对为 172.30.254.203/49607，本地 RTP IP 地址/端口对为 10.130.56.3/49606，RTCP 端口为 49607。

Related Commands

命令	Description
show h245	显示关于终端使用缓慢启动在 threat defense 设备范围内建立的 H.245 会话的信息。
show h323 ras	显示关于在 threat defense 设备范围内建立的 H.323 RAS 会话的信息。

show h323

要显示 H.323 连接的信息，请使用 **show h323** 命令。

show h323 {**ras** | **gup**}

Syntax Description

ras	显示在网守与其 H.323 终端之间跨 threat defense 设备建立的 H323 RAS 会话。
gup	显示有关 H323 网关更新的协议连接的信息。

Command History

版本	修改
6.1	引入了此命令。

使用指南

show h323 ras 命令显示有关越过 threat defense 设备在网守与其 H.323 终端之间建立的 H.323 RAS 会话的连接信息。

示例

以下是 **show h323 ras** 命令的输出示例：

```
> show h323 ras

Total: 1
        GK                      Caller
        172.30.254.214          10.130.56.14
```

此输出显示网守 172.30.254.214 与其客户端 10.130.56.14 之间有一个活动注册。

Related Commands

命令	Description
show h245	显示关于终端使用缓慢启动在 threat defense 设备范围内建立的 H.245 会话的信息。

show hardware-bypass

要显示 ISA 3000 上的当前硬件绕行状态，请使用 **show hardware-bypass** 命令。

show hardware-bypass

Command History

版本	修改
6.3	引入了此命令。

示例

以下是 **show hardware-bypass** 命令的输出示例。

```
> show hardware-bypass
                          Status              Powerdown           Powerup
GigabitEthernet 1/1-1/2   Disable             Disable             Disable
GigabitEthernet 1/3-1/4   Disable             Disable             Disable

Pairing supported on these interfaces: gig1/1 & gig1/2, gig1/3 & gig1/4
```

show high-availability config

要查看有关高可用性（故障切换）配置的信息，请使用 **show high-availability config** 命令。

show high-availability config

Command History

版本	修改
6.1	引入了此命令。

使用指南

show high-availability config 命令是 **show failover** 命令的别名。有关详细信息，请参阅 **show failover** 的参考页面。

示例

以下示例显示了处于主用/备用故障切换模式的设备的故障切换配置。

```
> show high-availability config
Failover On
Failover unit Primary
Failover LAN Interface: failover GigabitEthernet0/2 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 61 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.7(0)74, Mate 9.7(0)74
Serial Number: Ours 9A41CKDXQJU, Mate 9A3MFP0H1CP
Last Failover at: 19:23:17 UTC Oct 26 2016
        This host: Primary - Active
                Active time: 2009 (sec)
                slot 0: empty
                  Interface diagnostic (0.0.0.0): Normal (Waiting)
                  Interface outside (192.168.77.1): Normal (Waiting)
                  Interface inside (192.168.87.1): Normal (Waiting)
                slot 1: snort rev (1.0)  status (up)
                slot 2: diskstatus rev (1.0)  status (up)
        Other host: Secondary - Standby Ready
                Active time: 0 (sec)
                  Interface diagnostic (0.0.0.0): Normal (Waiting)
                  Interface outside (0.0.0.0): Normal (Waiting)
                  Interface inside (0.0.0.0): Normal (Waiting)
                slot 1: snort rev (1.0)  status (up)
                slot 2: diskstatus rev (1.0)  status (up)

Stateful Failover Logical Update Statistics
        Link : failover GigabitEthernet0/2 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         235        0          234        0
        sys cmd         234        0          234        0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        0          0          0          0
```

```
UDP conn        0          0          0          0
ARP tbl         0          0          0          0
Xlate_Timeout   0          0          0          0
IPv6 ND tbl     0          0          0          0
VPN IKEv1 SA    0          0          0          0
VPN IKEv1 P2    0          0          0          0
VPN IKEv2 SA    0          0          0          0
VPN IKEv2 P2    0          0          0          0
VPN CTCP upd    0          0          0          0
VPN SDI upd     0          0          0          0
VPN DHCP upd    0          0          0          0
SIP Session     0          0          0          0
SIP Tx          0          0          0          0
SIP Pinhole     0          0          0          0
Route Session   0          0          0          0
Router ID       0          0          0          0
User-Identity   1          0          0          0
CTS SGTNAME     0          0          0          0
CTS PAC         0          0          0          0
TrustSec-SXP    0          0          0          0
IPv6 Route      0          0          0          0
STS Table       0          0          0          0

Logical Update Queue Information
                Cur     Max     Total
Recv Q:         0       10      234
Xmit Q:         0       11      1200
```

以下示例显示了设备当前未配置故障切换的情况。第一行表示故障切换已关闭，是此输出中唯一有意义的部分。

```
> show high-availability config
Failover Off
Failover unit Secondary
Failover LAN Interface: not Configured
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 12 of 160 maximum
MAC Address Move Notification Interval not set
```

Related Commands

命令	Description
show failover	显示故障转移（高可用性）配置。

show https-access-list

show https-access-list 命令显示设备上配置的 HTTPS 访问列表。

show https-access-list

Command History

版本	修改
6.1	引入了此命令。

使用指南

HTTPS 访问列表确定哪些地址可以与使用 **configure network ipv4**/**ipv6** 命令配置的管理接口建立 HTTPS 连接。使用 HTTPS 连接以使用本地管理器、 设备管理器来配置和管理设备。

此访问列表不控制通过设备的流量或对数据接口的 HTTPS 访问。

示例

以下示例显示管理接口的 HTTPS 访问列表。

```
> show https-access-list
ACCEPT     tcp  --  anywhere             anywhere             state NEW tcp dpt:https
ACCEPT     tcp      anywhere             anywhere             state NEW tcp dpt:https
```

Related Commands

命令	Description
configure https-access-list	在管理接口上配置 HTTPS 访问列表。

show i

show idb

要显示有关接口描述符块状态的信息（表示接口资源的内部数据结构），请使用 **show idb** 命令。

show idb

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show idb** 命令的输出示例：

```
> show idb
Maximum number of Software IDBs 2252.  In use(total) 16. In use(active) 16

                    HWIDBs     SWIDBs
              Active 15         15
            Inactive 1          1
          Total IDBs 16         16
 Size each (bytes) 984        1512
        Total bytes 15744      24192

HWIDB#  1 0xdacf1420  Virtual0
HWIDB#  2 0xdac4da20  GigabitEthernet1/1
HWIDB#  3 0xdac5aa20  GigabitEthernet1/2
HWIDB#  4 0xdac651b0  GigabitEthernet1/3
HWIDB#  5 0xdac6f940  GigabitEthernet1/4
HWIDB#  6 0xdac7a0d0  GigabitEthernet1/5
HWIDB#  7 0xdac84860  GigabitEthernet1/6
HWIDB#  8 0xdac8eff0  GigabitEthernet1/7
HWIDB#  9 0xdac99780  GigabitEthernet1/8
HWIDB# 10 0xdacbda00  Internal-Control1/1
HWIDB# 11 0xdaca3f10  Internal-Data1/1
HWIDB# 12 0xdacb3260  Internal-Data1/2
HWIDB# 13 0xdacc81a0  Internal-Data1/3
HWIDB# 14 0xd409e4e0  Internal-Data1/4
HWIDB# 15 0xd409d090  Management1/1

SWIDB#  1 0xdacf1840 0x00000041 Virtual0 UP UP
SWIDB#  2 0xdac4de40 0x00000002 GigabitEthernet1/1 UP DOWN
SWIDB#  3 0xdac5ae40 0x00000003 GigabitEthernet1/2 UP DOWN
SWIDB#  4 0xdac655d0 0xffffffff GigabitEthernet1/3 DOWN DOWN
SWIDB#  5 0xdac6fd60 0xffffffff GigabitEthernet1/4 DOWN DOWN
SWIDB#  6 0xdac7a4f0 0xffffffff GigabitEthernet1/5 DOWN DOWN
SWIDB#  7 0xdac84c80 0xffffffff GigabitEthernet1/6 DOWN DOWN
SWIDB#  8 0xdac8f410 0xffffffff GigabitEthernet1/7 DOWN DOWN
SWIDB#  9 0xdac99ba0 0xffffffff GigabitEthernet1/8 DOWN DOWN
SWIDB# 10 0xdacbde20 0x0000003f Internal-Control1/1 UP UP
SWIDB# 11 0xdaca4330 0x00000043 Internal-Data1/1 UP UP
SWIDB# 12 0xdacb3680 0xffffffff Internal-Data1/2 UP UP
SWIDB# 13 0xdacc85c0 0x00000044 Internal-Data1/3 UP UP
SWIDB# 14 0xdacae210 0x00000045 Internal-Data1/4 UP UP
SWIDB# 15 0xd409d4b0 0x00000004 Management1/1 UP UP
```

下表对每个字段进行了说明。

表 *35: show idb stats* 字段

字段	Description
HWIDB	显示所有 HWIDB 的统计信息。为系统中的每个硬件端口创建 HWIDB。
SWIDB	显示所有 SWIDB 的统计信息。为系统中的每个主接口和子接口以及分配给情景的每个接口创建 SWIDB。 其他一些内部软件模块还会创建 IDB。
HWIDB#	指定硬件接口条目。IDB 序列号、地址和接口名称显示在每行中。
SWIDB#	指定软件接口条目。IDB 序列号、地址、对应的 vPif ID 和接口名称显示在每行中。
PEER IDB#	指定分配给情景的接口。IDB 序列号、地址、对应的 vPif ID 和接口名称显示在每行中。

Related Commands

命令	Description
show interface	显示接口的运行时间状态和统计信息。

show igmp groups

要显示其接收器直接连接到 threat defense 设备并且通过 IGMP 获知的组播组，请使用 **show igmp groups** 命令。

show igmp groups [[**reserved** | *group*] [*if_name*] [**detail**]] | **summary**]

Syntax Description

detail	（可选）提供源的详细说明。
group	（可选）IGMP 组的地址。包括此可选参数可限制只显示指定的组。
if_name	（可选）显示指定接口的组信息。
reserved	（可选）显示有关预留组的信息。
summary	（可选）显示组加入汇总信息。

Command History

版本	修改
6.1	引入了此命令。

使用指南

如果省略所有可选参数和关键字，则 **show igmp groups** 命令会按组地址、接口类型和接口号显示所有直接连接的组播组。

示例

以下是 **show igmp groups** 命令的输出示例：

```
> show igmp groups

IGMP Connected Group Membership
Group Address    Interface            Uptime    Expires   Last Reporter
224.1.1.1        inside               00:00:53  00:03:26  192.168.1.6
```

Related Commands

命令	Description
show igmp interface	显示接口的组播信息。

show igmp interface

要显示接口的组播信息，请使用 **show igmp interface** 命令。

show igmp interface ［*if_name*］

Syntax Description

if_name	（可选）显示选定接口的 IGMP 组信息。

Command History

版本	修改
6.1	引入了此命令。

使用指南

如果省略可选 *if_name* 参数，则 **show igmp interface** 命令会显示有关所有接口的信息。

示例

以下是 **show igmp interface** 命令的输出示例：

```
> show igmp interface inside

inside is up, line protocol is up
 Internet address is 192.168.37.6, subnet mask is 255.255.255.0
 IGMP is enabled on interface
 IGMP query interval is 60 seconds
 Inbound IGMP access group is not set
 Multicast routing is enabled on interface
 Multicast TTL threshold is 0
 Multicast designated router (DR) is 192.168.37.33
 No multicast groups joined
```

Related Commands

命令	Description
show igmp groups	显示其接收器直接连接到 threat defense 设备并且通过 IGMP 获知的组播组。

show igmp traffic

要显示 IGMP 流量统计信息，请使用 **show igmp traffic** 命令。

show igmp traffic

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show igmp traffic** 命令的输出示例：

```
> show igmp traffic

IGMP Traffic Counters
Elapsed time since counters cleared: 00:02:30
                               Received     Sent
Valid IGMP Packets                3           6
Queries                           2           6
Reports                           1           0
Leaves                            0           0
Mtrace packets                    0           0
DVMRP packets                     0           0
PIM packets                       0           0

Errors:
Malformed Packets                 0
Martian source                    0
Bad Checksums                     0
```

Related Commands

命令	Description
clear igmp counters	清除所有 IGMP 统计信息计数器。
clear igmp traffic	清除 IGMP 流量计数器。

show inline-set

要查看有关设备上配置的内联集（仅 IPS 接口）的信息，请使用 **show inline-set** 命令。

show inline-set ［*inline-set-name* | **mac-address-table**］

Syntax Description

inline-set-name	（可选）显示有关指定内联集的信息。如果不包括名称，则显示所有内联集。
mac-address-table	（可选）显示内联集的 MAC 地址网桥表。

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show inline-set** 命令的输出示例：

```
> show inline-set
Inline-set ips-inline
  Mtu is 1500 bytes
  Fail-open for snort down is on
  Fail-open for snort busy is off
  Tap mode is off
  Propagate-link-state option is off
  hardware-bypass mode is disabled
  Interface-Pair[1]:
    Interface: GigabitEthernet0/3 "inline-inside"
      Current-Status: UP
    Interface: GigabitEthernet0/4 "inline-outside"
      Current-Status: DOWN
    Bridge Group ID: 504
```

show interface

要查看接口统计信息，请使用 **show interface** 命令。

show interface [{*physical_interface* | **redundant***number*}[**.***subinterface*] | *interface_name* | **BVI** *ID* |] [**summary** | **stats** | **detail**]

Syntax Description

BVI *id*	（可选）显示指定网桥虚拟接口 (BVI) 的统计信息。输入 BVI 编号（1-250）。
detail	（可选）显示接口详细信息，包括添加接口的顺序、配置状态、真实状态和非对称路由统计信息（如果已启用）。 如果显示所有接口，则还会看到有关用于系统通信的内部接口的信息。用户无法配置内部接口，该信息只用于调试目的。
interface_name	（可选）按逻辑名称标识接口。
physical_interface	（可选）标识接口 ID，例如 **gigabitethernet0/1**。可用接口因设备型号而异。使用不带参数的 show interface 命令查看设备上可用的名称。
redundant*number*	（可选）标识冗余接口 ID，例如 **redundant1**。
stats	（默认）显示接口信息和统计信息。此关键字是默认值，而且是可选的。
summary	（可选）显示有关接口的摘要信息。
subinterface	（可选）识别一个介于 1 到 4294967293 之间整数，用以指定逻辑子接口。

Command Default

如果您不标识任何选项，则此命令显示除内部接口外的所有接口的基础统计。

Command History

版本	修改
6.1	引入了此命令。
6.2	添加了 **BVI** 关键字。
6.7	在数据接口上配置访问 管理中心 权限时，已将输出添加到 Internal-Data0/1 "nlp_int_tap" 接口的 **detail** 关键字中。

使用指南

为子接口显示的统计信息数是为物理接口显示的统计信息数的子集。

注释 硬件中传输或接收的字节数计数和流量统计信息计数不同。

在硬件计数中，数量直接从硬件检索，并反映第 2 层数据包大小。而在流量统计信息中，它反映第 3 层数据包大小。

计数差异因接口卡硬件的具体设计而有所不同。

例如，对于快速以太网卡，因为它包括以太网信头，所以第 2 层计数比流量计数大 14 字节。对于千兆位以太网卡，因为它包括以太网信头和 CRC，所以第 2 层计数比流量计数大 18 字节。

请参阅“示例”部分，了解显示输出的说明。

示例

以下是 **show interface** 命令的输出示例：

```
> show interface
Interface GigabitEthernet1/1 "outside", is down, line protocol is down
  Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex, Auto-Speed
        Input flow control is unsupported, output flow control is off
        MAC address e865.49b8.97f2, MTU 1500
        IP address unassigned
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (2047/2047)
        output queue (blocks free curr/low): hardware (2047/2047)
  Traffic Statistics for "outside":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet1/2 "inside", is down, line protocol is down
  Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex, Auto-Speed
        Input flow control is unsupported, output flow control is off
        MAC address e865.49b8.97f3, MTU 1500
        IP address 192.168.45.1, subnet mask 255.255.255.0
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
```

```
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (2047/2047)
        output queue (blocks free curr/low): hardware (2047/2047)
  Traffic Statistics for "inside":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet1/3 "", is administratively down, line protocol is down
  Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex, Auto-Speed
        Input flow control is unsupported, output flow control is off
        Available but not configured via nameif
        MAC address e865.49b8.97f4, MTU not set
        IP address unassigned
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (2047/2047)
        output queue (blocks free curr/low): hardware (2047/2047)
Interface GigabitEthernet1/4 "", is administratively down, line protocol is down
  Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex, Auto-Speed
        Input flow control is unsupported, output flow control is off
        Available but not configured via nameif
        MAC address e865.49b8.97f5, MTU not set
        IP address unassigned
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (2047/2047)
        output queue (blocks free curr/low): hardware (2047/2047)
Interface GigabitEthernet1/5 "", is administratively down, line protocol is down
  Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex, Auto-Speed
        Input flow control is unsupported, output flow control is off
        Available but not configured via nameif
        MAC address e865.49b8.97f6, MTU not set
        IP address unassigned
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
```

```
        0 pause input, 0 resume input
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (2047/2047)
        output queue (blocks free curr/low): hardware (2047/2047)
Interface GigabitEthernet1/6 "", is administratively down, line protocol is down
  Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex, Auto-Speed
        Input flow control is unsupported, output flow control is off
        Available but not configured via nameif
        MAC address e865.49b8.97f7, MTU not set
        IP address unassigned
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (2047/2047)
        output queue (blocks free curr/low): hardware (2047/2047)
Interface GigabitEthernet1/7 "", is administratively down, line protocol is down
  Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex, Auto-Speed
        Input flow control is unsupported, output flow control is off
        Available but not configured via nameif
        MAC address e865.49b8.97f8, MTU not set
        IP address unassigned
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (2047/2047)
        output queue (blocks free curr/low): hardware (2047/2047)
Interface GigabitEthernet1/8 "", is administratively down, line protocol is down
  Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex, Auto-Speed
        Input flow control is unsupported, output flow control is off
        Available but not configured via nameif
        MAC address e865.49b8.97f9, MTU not set
        IP address unassigned
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
```

```
       input queue (blocks free curr/low): hardware (2047/2047)
       output queue (blocks free curr/low): hardware (2047/2047)
Interface Management1/1 "diagnostic", is up, line protocol is up
  Hardware is en_vtun rev00, BW 1000 Mbps, DLY 10 usec
       Auto-Duplex(Full-duplex), Auto-Speed(1000 Mbps)
       Input flow control is unsupported, output flow control is off
       MAC address e865.49b8.97f1, MTU 1500
       IP address unassigned
       14247681 packets input, 896591753 bytes, 0 no buffer
       Received 0 broadcasts, 0 runts, 0 giants
       0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
       0 pause input, 0 resume input
       0 L2 decode drops
       0 packets output, 0 bytes, 0 underruns
       0 pause output, 0 resume output
       0 output errors, 0 collisions, 0 interface resets
       0 late collisions, 0 deferred
       0 input reset drops, 0 output reset drops
       input queue (blocks free curr/low): hardware (0/0)
       output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "diagnostic":
       14247685 packets input, 697121911 bytes
       0 packets output, 0 bytes
       5054964 packets dropped
     1 minute input rate 2 pkts/sec,  131 bytes/sec
     1 minute output rate 0 pkts/sec,  0 bytes/sec
     1 minute drop rate, 0 pkts/sec
     5 minute input rate 2 pkts/sec,  108 bytes/sec
     5 minute output rate 0 pkts/sec,  0 bytes/sec
     5 minute drop rate, 0 pkts/sec
       Management-only interface. Blocked 0 through-the-device packets
```

下表显示每个字段的说明。

表 *36: show interface* 字段

字段	Description
Interface ID	接口 ID。
“*interface_name*”	逻辑接口名称。如果不配置名称，则在硬件行之后会出现以下消息： `Available but not configured via nameif`
is *state*	管理状态，如下所示： • up - 接口没有关闭。 • administratively down - 人为地关闭接口。
Line protocol is state	线路状态，如下所示： • up - 工作电缆插入网络接口。 • down - 电缆不正确或未插入接口连接器。
VLAN identifier	对于子接口，是 VLAN ID。

字段	Description
Hardware	接口类型、最大带宽、延迟、复用和速度。在链路断开时，复用和速度显示配置的值。当链路连通时，这些字段显示配置的值，并在括号中包含实际设置。
Media-type	（并非始终显示）显示接口介质类型，例如 RJ-45 或 SFP。
message area	在某些情况下可能显示消息。请参阅以下示例： • 如果不配置名称，您会看到以下消息：Available but not configured via nameif • 如果接口是冗余接口的成员，您会看到以下消息：Active member of Redundant5
MAC address	接口 MAC 地址。
Site Specific MAC address	对于群集技术， 显示正在使用的站点特定 MAC 地址。
MTU	此接口上允许的最大数据包大小（以字节表示）。如果没有设置接口名称，此字段显示“MTU not set”（未设置 MTU）。
IP address	接口 IP 地址，静态或从 DHCP 服务器接收。
Subnet mask	IP 地址的子网掩码。
Packets input	此接口上接收的数据包数。
Bytes	此接口上接收的字节数。
No buffer	块分配的失败数。
Received:	
Broadcasts	接收的广播数。
Input errors	输入错误总数，包括如下所示的类型。其他与输入有关的错误也可能导致输入错误计数增加，并且一些数据报可能有多个错误；因此，这个总数可能超过以下类型列出的错误数。
Runts	由于小于最小数据包大小（64 字节）而丢弃的数据包数。超短帧通常是由冲突引起的。也可能是由接线不良和电子干扰引起的。
Giants	由于超出最大数据包大小而丢弃的数据包数。例如，大于 1518 字节的所有以太网数据包均被视为超长帧。

字段	Description
CRC	循环冗余检查错误数。当站发送帧时，会将 CRC 附加到帧尾。此 CRC 是使用算法基于帧中的数据生成的。如果在源和目的地之间更改了帧，系统会注意到 CRC 不匹配。CRC 数量过大通常是冲突或站传输错误数据引起的。
Frame	帧错误数。错误的帧包含长度不正确或帧校验和错误的数据包。此错误通常是冲突或以太网设备故障引起的。
Overrun	因输入速度超出接口处理数据的能力而导致接口无法将接收的数据传递至硬件缓冲区的次数。
Ignored	不使用此字段。值始终为 0。
Abort	不使用此字段。值始终为 0。
L2 decode drops	因未配置名称或接收具有无效 VLAN ID 的帧而丢弃的数据包。在冗余接口配置中的备用接口上，此计数器的数值可能因该接口没有配置名称而增加。
Packets output	在此接口上发送的数据包数。
Bytes	在此接口上发送的字节数。
Underruns	发射器运行速度比接口处理速度更快的次数
Output Errors	因超过已配置的最大冲突数而未传输的帧数。在网络流量巨大时，此计数器的数值只会增加。
Collisions	由于以太网冲突（单一和多个冲突）而重新传输的消息数。这通常发生在过度扩展的 LAN（以太网或收发器电缆太长、站之间超过两个中继器或层叠的多端口收发器太多）上。输出数据包仅对发生冲突的数据包计数一次。
Interface resets	接口已重置的次数。如果接口在三秒内无法传输，系统会重置接口以重启传输。在此时间间隔内，保持连接状态。接口环回或关闭时，也会出现接口重置。
Babbles	未使用。（“babble”意味着发射器在接口上的时间大于传输最大帧所花费的时间。）

字段	Description
Late collisions	因冲突发生在正常冲突时间范围之外而未传输的帧数。延迟冲突是在传输数据包中延迟检测到的冲突。通常，这些不应该发生。当两台以太网主机同时尝试通信时，它们应在数据包的早期阶段发生冲突且双方都退出，或者第二台主机应看到第一台正在通信和等待。 如果遇到延迟冲突，设备将迅速行动并尝试在以太网上发送数据包，而 threat defense 设备已部分完成发送数据包。 threat defense 设备不重新发送数据包，因为它可能已释放保留数据包第一部分的缓冲区。这不是真正的问题，因为网络协议设计为通过重新发送数据包来解决冲突。但是，延迟冲突指示您的网络中存在问题。常见问题是运行着大量重复的网络和以太网络，超出了指定范围。
Deferred	在传输之前由于链路上的活动而延迟的帧数。
input reset drops	当发生重置时，计算 RX 环中丢弃的数据包数。
output reset drops	当发生重置时，计算 RX 环中丢弃的数据包数。
Rate limit drops	将接口配置为非千兆位速度而尝试传输超过 10 Mbps 或 100 Mbps（具体取决于配置）时丢弃的数据包数。
Lost carrier	在传输期间载波信号丢失的次数。
No carrier	未使用。
Input queue (curr/max packets):	输入队列中数据包的当前数和最大数。
Hardware	硬件队列中的数据包数。
Software	软件队列中的数据包数。对千兆位以太网接口不可用。
Output queue (curr/max packets):	输出队列中数据包的当前数和最大数。
Hardware	硬件队列中的数据包数。
Software	软件队列中的数据包数。
input queue (blocks free curr/low)	当前/低条目指示接口的接收（输入）描述符环上当前可用和始终可用的最低插槽数。这些数值由主 CPU 更新，因此最低（直到接口统计信息清除或设备重新加载）水印不是十分准确。
output queue (blocks free curr/low)	当前/低条目指示接口的接收传输（输出）描述符环上当前可用和始终可用的最低插槽数。这些数值由主 CPU 更新，因此最低（直到接口统计信息清除或设备重新加载）水印不是十分准确。
Traffic Statistics:	接收、传输或丢弃的数据包数。

字段	Description
Packets input	The number of packets received and the number of bytes.
Packets output	传输的数据包数和字节数。
Packets dropped	丢弃的数据包数。通常，当加速安全路径(ASP)上丢弃数据包（例如，如果数据包由于访问列表拒绝而被丢弃）时，此计数器数值会增加。 有关接口上潜在丢弃的原因，请参阅 **show asp drop** 命令。
1 minute input rate	在过去一分钟内接收的数据包数（包/秒和字节/秒）。
1 minute output rate	在过去一分钟内传输的数据包数（包/秒和字节/秒）。
1 minute drop rate	在过去一分钟内丢弃的数据包数（包/秒）。
5 minute input rate	在过去 5 分钟内接收的数据包数（包/秒和字节/秒）。
5 minute output rate	在过去 5 分钟内传输的数据包数（包/秒和字节/秒）。
5 minute drop rate	在过去 5 分钟内丢弃的数据包数（包/秒）。
Redundancy Information:	对冗余接口，显示成员的物理接口。主用接口在接口ID后有“(Active)”。 如果您尚未指定成员，您会看到以下输出： `Members unassigned`
Last switchover	对冗余接口，显示上次主用接口故障切换到备用接口的时间。

注释 **show interface detail** 命令结果中的输入和输出速率可能与 管理中心 用户界面的接口模块中显示的输入和输出流量速率不同。

接口模块根据 Snort 性能监控的值显示流量速率。Snort 性能监控和接口统计信息的采样间隔不同。这种采样间隔的差异会导致 管理中心 用户界面和 **show interface detail** 命令结果中的吞吐量值不同。

以下是 **show interface detail** 命令的输出示例。以下示例展示所有接口的详细接口统计信息，包括内部接口（如果针对您的平台存在）和非对称路由统计信息（如果已启用）：

```
> show interface detail
Interface GigabitEthernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 1000 usec
        Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
        MAC address 000b.fcf8.c44e, MTU 1500
        IP address 10.86.194.60, subnet mask 255.255.254.0
        1330214 packets input, 124580214 bytes, 0 no buffer
        Received 1216917 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
```

```
        9 L2 decode drops
        124863 packets output, 86956597 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        input queue (curr/max packets): hardware (0/7)
        output queue (curr/max packets): hardware (0/13)
  Traffic Statistics for "outside":
        1330201 packets input, 99995120 bytes
        124863 packets output, 84651382 bytes
        525233 packets dropped
  Control Point Interface States:
        Interface number is 1
        Interface config status is active
        Interface state is active
Interface Internal-Data0/0 "", is up, line protocol is up
  Hardware is i82547GI rev00, BW 1000 Mbps, DLY 1000 usec
        (Full-duplex), (1000 Mbps)
        MAC address 0000.0001.0002, MTU not set
        IP address unassigned
        6 packets input, 1094 bytes, 0 no buffer
        Received 6 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops, 0 demux drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        input queue (curr/max packets): hardware (0/2) software (0/0)
        output queue (curr/max packets): hardware (0/0) software (0/0)
   Control Point Interface States:
        Interface number is unassigned
Interface Internal-Data0/1 "nlp_int_tap", is up, line protocol is up
  Hardware is en_vtun rev00, BW Unknown Speed-Capability, DLY 1000 usec
 (Full-duplex), (1000 Mbps)
 Input flow control is unsupported, output flow control is unsupported
 MAC address 0000.0100.0001, MTU 1500
 IP address 169.254.1.1, subnet mask 255.255.255.248
 37 packets input, 2822 bytes, 0 no buffer
 Received 0 broadcasts, 0 runts, 0 giants
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
 0 pause input, 0 resume input
 0 L2 decode drops
 5 packets output, 370 bytes, 0 underruns
 0 pause output, 0 resume output
 0 output errors, 0 collisions, 0 interface resets
 0 late collisions, 0 deferred
 0 input reset drops, 0 output reset drops
 input queue (blocks free curr/low): hardware (0/0)
 output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "nlp_int_tap":
 37 packets input, 2304 bytes
 5 packets output, 300 bytes
 37 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
  Control Point Interface States:
 Interface number is 14
 Interface config status is active
 Interface state is active
[...]
```

下表说明 **show interface detail** 命令显示的其他字段。

表 *37: show interface detail* 字段

字段	Description
Demux drops	（仅在内部数据接口上）因 threat defense 设备无法多路复用来自其他接口的数据包而丢弃的数据包数。
Control Point Interface States:	
Interface number	用于调试的编号，指示此接口创建的顺序，从 0 开始。
Interface config status	管理状态，如下所示： • active - 该接口没有关闭。 • not active - 接口被有意关闭。
Interface state	接口的实际状态。在大多数情况下，此状态与上述配置状态匹配。如果配置高可用性，则可能不匹配，因为 threat defense 设备会根据需要打开或关闭接口。
Asymmetrical Routing Statistics:	
Received X1 packets	在此接口上接收的 ASR 数据包数。
Transmitted X2 packets	在此接口上发送的 ASR 数据包数。
Dropped X3 packets	在此接口上丢弃的ASR数据包数。当尝试转发数据包时，如果接口关闭，则可能丢弃数据包。

Related Commands

命令	Description
clear interface	清除 **show interface** 命令的计数器。
show interface ip brief	显示接口 IP 地址和状态。

show interface ip brief

要查看接口 IP 地址和状态，请使用 **show interface ip brief** 命令。

show interface [[*physical_interface*[**.***subinterface*] | *interface_name* | **BVI** *ID* |] **ip brief**

Syntax Description

BVI *id*	（可选）显示指定网桥虚拟接口 (BVI) 的统计信息。输入 BVI 编号（1-250）。
interface_name	（可选）标识接口 ID。
physical_interface	（可选）标识接口 ID，例如 **gigabitethernet0/1**。
subinterface	（可选）识别一个介于 1 到 4294967293 之间整数，用以指定逻辑子接口。

Command Default

如果不指定接口， 命令会显示所有接口，包括内部接口。

Command History

版本	修改
6.1	引入了此命令。
6.2	添加了 **BVI** 关键字。

示例

以下是 **show ip brief** 命令的输出示例：

```
> show interface ip brief
    Interface                  IP-Address      OK? Method  Status                Protocol
    Control0/0                 127.0.1.1       YES CONFIG  up                    up
    GigabitEthernet0/0         209.165.200.226 YES CONFIG  up                    up
    GigabitEthernet0/1         unassigned      YES unset   administratively down down
    GigabitEthernet0/2         10.1.1.50       YES manual  administratively down down
    GigabitEthernet0/3         192.168.2.6     YES DHCP    administratively down down
    Management0/0              209.165.201.3   YES CONFIG  up
```

以下示例显示大多数接口属于 BVI 时的寻址。成员接口与父 BVI 具有相同的地址。

```
> show interface ip brief
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet1/1         unassigned      YES DHCP   down                  down
GigabitEthernet1/2         192.168.1.1     YES unset  down                  down
GigabitEthernet1/3         192.168.1.1     YES unset  down                  down
GigabitEthernet1/4         192.168.1.1     YES unset  down                  down
GigabitEthernet1/5         192.168.1.1     YES unset  down                  down
GigabitEthernet1/6         192.168.1.1     YES unset  down                  down
GigabitEthernet1/7         192.168.1.1     YES unset  down                  down
GigabitEthernet1/8         192.168.1.1     YES unset  down                  down
Internal-Control1/1        127.0.1.1       YES unset  up                    up
Internal-Data1/1           unassigned      YES unset  up                    up
```

```
Internal-Data1/2           unassigned      YES unset  down                  down
Internal-Data1/3           unassigned      YES unset  up                    up
Internal-Data1/4           169.254.1.1     YES unset  up                    up
Management1/1              unassigned      YES unset  up                    up
BVI1                       192.168.1.1     YES manual up                    up
```

下表对输出字段进行了说明。

表 *38: show interface ip brief* 字段

字段	Description
Interface	接口 ID。 如果显示所有接口，则还会看到有关用于系统通信的内部接口的信息。用户无法配置内部接口，该信息只用于调试目的。
IP-Address	接口 IP 地址。
OK?	此列没有使用并始终显示为“Yes”。
Method	接口接收 IP 地址的方法。值包括以下各项： • unset - 未配置 IP 地址。 • manual - 接口具有静态地址。 • CONFIG - 已从启动配置载入。 • DHCP — 从 DHCP 服务器接收。
Status	管理状态，如下所示： • up - 接口没有关闭。 • down - 接口未启动，也未有意关闭。 • administratively down - 人为地关闭接口。
Protocol	线路状态，如下所示： • up - 工作电缆插入网络接口。 • down - 电缆不正确或未插入接口连接器。

Related Commands

命令	Description
show interface	显示接口的运行时间状态和统计信息。

show inventory

要显示有关安装在网络设备中并指定了产品标识符 (PID)、版本标识符 (VID) 和序列号 (SN) 的思科产品的所有信息，请在用户 EXEC 模式或特权 EXEC 模式下使用 **show inventory** 命令。

show inventory ［*slot_id*］

Syntax Description

slot_id	（可选）指定模块 ID 或插槽号码 0-3。

Command Default

如果在显示项目的库存时不指定插槽，则会显示所有模块（包括电源）的库存信息。

Command History

版本	修改
6.1	引入了此命令。

使用指南

show inventory 命令检索和显示有关每个思科产品的库存信息，这些产品的形式为 UDI，是以下三个不同数据元素的组合：产品标识符 (PID)、版本标识符 (VID) 和序列号 (SN)。

PID 是可以用来订购产品的名称；过去称为“产品名称”或“部件号”。这是您订购精确替换部件时使用的标识符。

VID 是产品的版本。每当修订产品后，VID 即根据 Telcordia GR-209-CORE（管理产品更改通知的行业标准）的严格流程来递增。

SN 是供应商提供的唯一产品序列号。每个产品都具有工厂指定的唯一序列号，无法在实际应用中更改。序列号是用于标识各具体产品实例的方法。对于设备的不同组件，序列号的长度可以不同。

UDI 将每个产品作为一个实体。部分实体（如机箱）具有子实体（像插槽）。每个实体以逻辑排序呈现方式显示在思科实体分层排列的单独行上。

使用 **show inventory** 命令（不带选项）可显示安装在网络设备中并分配了 PID 的思科实体列表。

如果未对思科实体分配 PID，则不会检索或显示该实体。

由于 ASA 5500-X 系列的硬件限制，序列号可能不显示。对于这些型号中 PCI-E I/O (NIC) 选项卡的 UDI 显示，根据机箱类型有六种可能的输出，尽管只有两种不同类型的卡。这是因为根据指定的机箱使用了不同的 PCI-E 支架组件。以下示例展示每个 PCI-E I/O 卡组装的预期输出。例如，如果检测到 Silicom SFP NIC 卡，则 UDI 显示取决于安装该 UDI 的设备。VID 和 S/N 值为 N/A，因为没有这些值的电子存储。

对于 ASA 5512-X 或 5515-X 中的 6 端口 SFP 以太网 NIC 卡：

```
Name: "module1", DESCR: "ASA 5512-X/5515-X Interface Card 6-port GE SFP, SX/LX"
PID: ASA-IC-6GE-SFP-A    , VID: N/A, SN: N/A
```

对于 ASA 5525-X 中的 6 端口 SFP 以太网 NIC 卡：

```
Name: "module1", DESCR: "ASA 5525-X Interface Card 6-port GE SFP, SX/LX"
```

```
PID: ASA-IC-6GE-SFP-B    , VID: N/A, SN: N/A
```

对于 ASA 5545-X 或 5555-X 中的 6 端口 SFP 以太网 NIC 卡：

```
Name: "module1", DESCR: "ASA 5545-X/5555-X Interface Card 6-port GE SFP, SX/LX"
PID: ASA-IC-6GE-SFP-C    , VID: N/A, SN: N/A
```

对于 ASA 5512-X 或 5515-X 中的 6 端口铜缆以太网 NIC 卡：

```
Name: "module1", DESCR: "ASA 5512-X/5515-X Interface Card 6-port 10/100/1000, RJ-45"
PID: ASA-IC-6GE-CU-A    , VID: N/A, SN: N/A
```

对于 ASA 5525-X 中的 6 端口铜缆以太网 NIC 卡：

```
Name: "module1", DESCR: "ASA 5525-X Interface Card 6-port 10/100/1000, RJ-45"
PID: ASA-IC-6GE-CU-B    , VID: N/A, SN: N/A
```

对于 ASA 5545-X 或 5555-X 中的 6 端口铜缆以太网 NIC 卡：

```
Name: "module1", DESCR: "ASA 5545-X/5555-X Interface Card 6-port 10/100/1000, RJ-45"
PID: ASA-IC-6GE-CU-C    , VID: N/A, SN: N/A
```

示例

以下是没有任何关键字或参数的 **show inventory** 命令的输出示例。此示例输出显示 threat defense 设备中安装的思科实体的列表，每个实体都分配了 PID。

```
> show inventory
Name: "Chassis", DESCR: "ASA 5508-X with FirePOWER services, 8GE, AC, DES"
PID: ASA5508           , VID: V01     , SN: JMX1923408S

Name: "Storage Device 1", DESCR: "ASA 5508-X SSD"
PID: ASA5508-SSD       , VID: N/A     , SN: MXA184205MC
```

下表介绍了显示屏中显示的字段。

表 *39: show inventory* 的字段说明

字段	Description
Name	分配给思科实体的物理名称（文本字符串）。例如，控制台、SSP或简单组件号（端口或模块号，如“1”）取决于设备的物理组件的命名语法。相当于 RFC 2737 中的 entPhysicalName MIB 变量。
DESCR	用于描述对象的思科实体的物理说明。相当于 RFC 2737 中的 entPhysicalName MIB 变量。
PID	实体的产品标识符。相当于 RFC 2737 中的 entPhysicalModelName MIB 变量。

字段	Description
VID	实体的版本标识符。相当于 RFC 2737 中的 entPhysicalHardwareRev MIB 变量。
SN	实体的序列号。相当于 RFC 2737 中的 entPhysicalSerialNum MIB 变量。

show ip address

要查看接口 IP 地址，或在透明模式下查看管理 IP 地址，请使用 **show ip address** 命令。

show ip address [[*physical_interface*[**.***subinterface*] | *interface_name* |]

Syntax Description

interface_name	（可选）标识接口 ID。
physical_interface	（可选）标识接口 ID，例如 **gigabit**ethernet0/1。
subinterface	（可选）识别一个介于 1 到 4294967293 之间整数，用以指定逻辑子接口。

Command Default

如果不指定接口，则输出显示所有接口的 IP 地址。

Command History

版本	修改
6.1	引入了此命令。

使用指南

此命令显示主要 IP 地址（在显示屏幕中称为“System”，适用于配置高可用性时）以及当前 IP 地址。如果设备处于主用状态，则系统和当前 IP 地址匹配。如果设备处于备用状态，则当前 IP 地址显示备用地址。

IP 地址仅用于数据接口。此命令不会在诊断接口（与透明模式管理接口）上的管理接口上显示系统的 IP 地址。信息将包括诊断接口的 IP 地址信息（如果已配置）。要查看管理接口上有关的信息，请使用 **show network** 命令。

示例

以下是 **show ip address** 命令的输出示例：

```
> show ip address
System IP Addresses:
Interface               Name         IP address      Subnet mask       Method
GigabitEthernet0/0      mgmt         10.7.12.100     255.255.255.0     CONFIG
GigabitEthernet0/1      inside       10.1.1.100      255.255.255.0     CONFIG
GigabitEthernet0/2.40   outside      209.165.201.2   255.255.255.224   DHCP
GigabitEthernet0/3      dmz          209.165.200.225 255.255.255.224   manual
Current IP Addresses:
Interface               Name         IP address      Subnet mask       Method
GigabitEthernet0/0      mgmt         10.7.12.100     255.255.255.0     CONFIG
GigabitEthernet0/1      inside       10.1.1.100      255.255.255.0     CONFIG
GigabitEthernet0/2.40   outside      209.165.201.2   255.255.255.224   DHCP
GigabitEthernet0/3      dmz          209.165.200.225 255.255.255.224   manual
```

下表对每个字段进行了说明。

表 *40: show ip address* 字段

字段	Description
Interface	接口 ID。
Name	接口名称。
IP address	接口 IP 地址。
Subnet mask	IP 地址子网掩码。
Method	接口接收 IP 地址的方法。值包括以下各项： • unset - 未配置 IP 地址。 • manual - 接口具有静态地址。 • CONFIG - 已从启动配置载入。 • DHCP — 从 DHCP 服务器接收。

Related Commands

命令	Description
show interface	显示接口的运行时间状态和统计信息。
show interface ip brief	显示接口 IP 地址和状态。

show ip address dhcp

要查看接口的 DHCP 租用或服务器的详细信息，请使用 **show ip address dhcp** 命令。

show ip address {*physical_interface*[**.***subinterface*] | *interface_name*} **dhcp server**
show ip address {*physical_interface*[**.***subinterface*] | *interface_name*} **dhcp lease** [**proxy** | **server**] [**summary**]

Syntax Description

interface_name	标识接口名称。
lease	显示有关 DHCP 租用的信息。
physical_interface	标识接口 ID，例如 **gigabitethernet0/1**。
proxy	显示 IPL 表中的代理条目。
server	显示 IPL 表中的服务器条目。
subinterface	识别一个介于 1 到 4294967293 之间整数，用以指定逻辑子接口。
summary	显示条目的汇总。

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show ip address dhcp lease** 命令的输出示例：

```
> show ip address outside dhcp lease
Temp IP Addr:209.165.201.57 for peer on interface:outside
Temp sub net mask:255.255.255.224
   DHCP Lease server:209.165.200.225, state:3 Bound
   DHCP Transaction id:0x4123
   Lease:259200 secs, Renewal:129600 secs, Rebind:226800 secs
   Temp default-gateway addr:209.165.201.1
   Temp ip static route0: dest 10.9.0.0 router 10.7.12.255
   Next timer fires after:111797 secs
   Retry count:0, Client-ID:cisco-0000.0000.0000-outside
   Proxy: TRUE  Proxy Network: 10.1.1.1
   Hostname: device1
```

下表对每个字段进行了说明。

表 *41: show ip address dhcp lease* 字段

字段	Description
Temp IP Addr	分配给接口的 IP 地址。
Temp sub net mask	分配给接口的子网掩码。
DHCP Lease server	DHCP 服务器地址。
state	DHCP 租用的状态，如下所示： • Initial - 初始化状态，设备启动获取租用流程。当租用结束或租用协商失败时，也会显示此状态。 • Selecting - 设备正在等待检索来自一个或多个 DHCP 服务器的 DHCPOFFER 消息，从而可从中选择一个。 • Requesting - 设备正在等待接收所发送请求的目标服务器的回应。 • Purging - 设备正在删除租用，因为客户端已释放 IP 地址或出现其他错误。 • Bound - 设备具有有效租用且正在正常运行。 • Renewing - 设备正在尝试续订租用。它定期将 DHCPREQUEST 消息发送到当前 DHCP 服务器，然后等待回复。 • Rebinding - 设备无法对原始服务器的租用续约，现在发送 DHCPREQUEST 消息，直到收到任何服务器的回复或租用结束。 • Holddown - 设备已启动用于删除租用的流程。 • Releasing - 设备将释放消息发送到服务器，指示不再需要 IP 地址。
DHCP transaction id	客户端选择的随机号码，供客户端和服务器用来关联请求消息。
Lease	DHCP 服务器指定的时间长度，接口可在该时间段内使用此 IP 地址。
Renewal	接口自动尝试续订此租用之前的时间长度。
Rebind	threat defense 设备尝试重新绑定 DHCP 服务器之前的时间长度。如果设备无法与原始 DHCP 服务器通信且租用时间已超过 87.5%，就会进行重新绑定。然后，设备尝试通过广播 DHCP 请求与任何可用的 DHCP 服务器联系。
Temp default-gateway addr	DHCP 服务器提供的默认网关地址。
Temp ip static route0	默认静态路由。
Next timer fires after	内部计时器触发之前的秒数。

字段	Description
Retry count	如果 threat defense 设备正在尝试建立租用，则此字段显示设备已尝试发送 DHCP 消息的次数。例如，如果设备处于 Selecting（选择中）状态，则此值显示设备已发送发现消息的次数。如果设备处于 Requesting（请求中）状态，则此值显示设备已发送请求消息的次数。
Client-ID	在与服务器的所有通信中使用的客户端 ID。
Proxy	指定此接口是否为 VPN 客户端的代理 DHCP 客户端，值为 True 或 False。
Proxy Network	请求的网络。
Hostname	客户端主机名称。

以下是 **show ip address dhcp server** 命令的输出示例：

```
> show ip address outside dhcp server
   DHCP server: ANY (255.255.255.255)
    Leases:   0
    Offers:   0      Requests: 0     Acks: 0     Naks: 0
    Declines: 0      Releases: 0     Bad:  0

   DHCP server: 40.7.12.6
    Leases:   1
    Offers:   1      Requests: 17     Acks: 17     Naks: 0
    Declines: 0      Releases: 0     Bad:  0
    DNS0:   171.69.161.23,   DNS1:  171.69.161.24
    WINS0:  172.69.161.23,   WINS1: 172.69.161.23
    Subnet: 255.255.0.0   DNS Domain: cisco.com
```

下表对每个字段进行了说明。

***表 42: show ip address dhcp server* 字段**

字段	Description
DHCP server	向此接口提供租用的 DHCP 服务器的地址。顶部条目（“ANY”）是默认服务器并始终存在。
Leases	从服务器获取的租用数。对于一个接口，租用数通常是 1。如果服务器为正在运行 VPN 代理的接口提供地址，会有数个租用。
Offers	服务器所提供的项的数量。
Requests	发送至服务器的请求数。
Acks	从服务器接收的确认数。
Naks	从服务器接收的否定确认数。
Declines	从服务器接收的拒绝数。

字段	Description
Releases	发送至服务器的释放数。
Bad	从服务器接收的错误数据包数。
DNS0	从 DHCP 服务器获取的主要 DNS 服务器地址。
DNS1	从 DHCP 服务器获取的辅助 DNS 服务器地址。
WINS0	从 DHCP 服务器获取的主要 WINS 服务器地址。
WINS1	从 DHCP 服务器获取的辅助 WINS 服务器地址。
Subnet	从 DHCP 服务器获取的子网地址。
DNS Domain	从 DHCP 服务器获取的域。

Related Commands

命令	Description
show interface ip brief	显示接口 IP 地址和状态。
show ip address	显示接口的 IP 地址。

show ip address pppoe

要查看有关 PPPoE 连接的详细信息，请使用 **show ip address pppoe** 命令。

show ip address {*physical_interface*[**.***subinterface*] | *interface_name* | } **pppoe**

Syntax Description

interface_name	标识接口名称。
physical_interface	标识接口 ID，例如 **gigabitethernet0/1**。
subinterface	识别一个介于 1 到 4294967293 之间整数，用以指定逻辑子接口。

Command History

版本	修改
6.1	引入了此命令。

Related Commands

命令	Description
show interface ip brief	显示接口 IP 地址和状态。
show ip address	显示接口的 IP 地址。

show ip audit count

要在将审核策略应用于接口时显示签名匹配数，请使用 **show ip audit count** 命令。

show ip audit count ［**global** | **interface** *interface_name*］

Syntax Description

global	（默认）显示所有接口的匹配数。
interface *interface_name*	（可选）显示指定接口的匹配数。

Command History

版本	修改
6.1	引入了此命令。

使用指南

通常不配置审核策略，但如果使用 FlexConfig 进行配置，则可以查看相关统计信息。

Related Commands

命令	Description
clear ip audit count	清除 IP 审核的统计信息。
show running-config ip audit name	显示 **ip audit name** 命令的配置。除 **name**外，您可以检查 **interface** 和 **signature** 配置。

show ip local pool

要显示 IPv4 地址池信息，请使用 **show ip local pool** 命令。

show ip local pool *pool_name*

Syntax Description

pool_name	IPv6 地址池的名称。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用此命令可查看 IPv4 地址池的内容。这些池用于远程访问 VPN 和集群技术。使用 **show ipv6 local pool** 以查看IPv6 地址池。

示例

以下是 **show ip local pool** 命令的输出示例：

```
> show ip local pool test-ipv4-pool
Begin           End             Mask            Free     Held     In use
10.100.10.10    10.100.10.254   255.255.255.0     245        0        0

Available Addresses:
10.100.10.10
10.100.10.11
10.100.10.12
10.100.10.13
10.100.10.14
10.100.10.15
10.100.10.16
... (remaining output redacted)...
```

show ip verify statistics

要显示因单播拟向转发 (RPF) 功能而丢弃的数据包数，请使用 **show ip verify statistics** 命令。

show ip verify statistics ［**interface** *interface_name*］

Syntax Description

interface *interface_name*	（可选）显示指定接口的统计信息。

Command Default

此命令显示所有接口的统计信息。

Command History

版本	修改
6.1	引入了此命令。

使用指南

ip verify reverse-path 功能通常未配置，但如果使用 FlexConfig 进行配置，则可以查看相关统计信息。

示例

以下是 **show ip verify statistics** 命令的输出示例：

```
> show ip verify statistics
interface outside: 2 unicast rpf drops
interface inside: 1 unicast rpf drops
interface intf2: 3 unicast rpf drops
```

Related Commands

命令	Description
clear ip verify statistics	清除单播 RPF 统计信息。
show running-config ip verify reverse-path	显示 **ip verify reverse-path** 配置。

show ipsec df-bit

要显示指定接口的 IPsec 数据包的 IPsec 不分片（DF 位）策略，请使用 **show ipsec df-bit** 命令。您还可以使用 **show crypto ipsec df-bit** 命令同义词。

show ipsec df-bit *interface*

Syntax Description

interface	指定接口名称。

Command History

版本	修改
6.1	引入了此命令。

使用指南

df-bit 设置确定系统如何处理封装信头中的不分片 (DF) 位。IP 信头中的 DF 位确定是否允许设备对数据包分段。根据此设置，系统在应用加密时会清除、设置或复制明文数据包的 DF 位设置，也可以将其复制到外 IPsec 信头。

示例

以下示例展示名为 inside 的接口的 IPsec DF 位策略：

```
> show ipsec df-bit inside
df-bit inside copy
```

Related Commands

命令	Description
show ipsec fragmentation	显示 IPsec 数据包的分段策略。

show ipsec fragmentation

要显示 IPsec 数据包的分段策略，请使用 **show ipsec fragmentation** 命令。您还可以使用 **show crypto ipsec fragmentation** 命令同义词。

show ipsec fragmentation *interface*

Syntax Description

interface	指定接口名称。

Command History

版本	修改
6.1	引入了此命令。

使用指南

为 VPN 加密数据包时，系统会将数据包长度与出站接口的 MTU 进行比较。如果加密数据包将超过 MTU，则必须对数据包进行分段。此命令显示系统是在数据包加密后（加密后）还是加密前（加密前）对数据包进行分片。在加密之前对数据包进行分片也称为预分片，这是默认的系统行为，因为它可以提高整体加密性能。

示例

以下示例显示名为 inside 的接口的 IPsec 分段策略：

```
> show ipsec fragmentation inside
fragmentation inside before-encryption
```

Related Commands

命令	Description
show ipsec df-bit	显示指定接口的 DF 位策略。

show ipsec policy

要显示为 OSPFv3 配置的 IPsec 安全套接字 API (SS API) 安全策略，请使用 **show ipsec policy** 命令。您还可以使用此命令的替代形式： **show crypto ipsec policy**。

show ipsec policy

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例显示 OSPFv3 身份验证和加密策略。

```
> show ipsec policy
Crypto IPsec client security policy data

Policy name:      OSPFv3-1-256
Policy refcount:  1
Policy flags:     0x00000000
SA handles:       sess 268382208 (0xfff3000) / in 55017 (0xd6e9) / out 90369 (0x16101)
Inbound  ESP SPI:        256 (0x100)
Outbound ESP SPI:        256 (0x100)
Inbound  ESP Auth Key:   12345678901234567890123456789012345678901234567890
Outbound ESP Auth Key:   12345678901234567890123456789012345678901234567890
Inbound  ESP Cipher Key: 123456789012345678901234567890123456789012
Outbound ESP Cipher Key: 123456789012345678901234567890123456789012
Transform set:    esp-aes esp-sha-hmac
```

Related Commands

命令	Description
show crypto sockets	显示安全套接字信息。
show ipv6 ospf interface	显示有关 OSPFv3 接口的信息。

show ipsec sa

要显示 IPsec 安全关联 (SA) 列表，请使用 **show ipsec sa** 命令。您还可以使用此命令的替代形式：**show crypto ipsec sa**。

show ipsec sa [**assigned-address** *hostname_or_IP_address* | **entry** | **identity** | **inactive** | **map** *map-name* | **peer** *peer-addr* | **spi** *spi-num*] [**detail**]

Syntax Description

assigned-address *hostname_or_IP_address*	（可选）显示指定的主机名或 IP 地址的 IPsec SA。
detail	（可选）显示有关所显示内容的详细错误信息。
entry	（可选）显示按对等设备地址排序的 IPsec SA
identity	（可选）显示按身份排序的 IPsec SA，不包括 ESP。这是简洁形式。
inactive	（可选）显示无法传递流量的 IPsec SA。
map *map-name*	（可选）显示指定加密映射的 IPsec SA。
peer *peer-addr*	（可选）显示指定对等设备 IP 地址的 IPsec SA。
spi *spi-num*	（可选）显示 SPI 的 IPsec SA。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例显示 IPsec SA，包括分配的 IPv6 地址以及传输模式和 GRE 封装指示。

```
> show ipsec sa
interface: outside
    Crypto map tag: def, seq num: 1, local addr: 75.2.1.23

      local ident (addr/mask/prot/port): (75.2.1.23/255.255.255.255/47/0)
      remote ident (addr/mask/prot/port): (75.2.1.60/255.255.255.255/47/0)
      current_peer: 75.2.1.60, username: rashmi
      dynamic allocated peer ip: 65.2.1.100
      dynamic allocated peer ip(ipv6): 2001:1000::10

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 18, #pkts decrypt: 18, #pkts verify: 18
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #post-frag successes: 0, #post-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
```

```
      #send errors: 0, #recv errors: 4

     local crypto endpt.: 75.2.1.23/4500, remote crypto endpt.: 75.2.1.60/64251
      path mtu 1342, ipsec overhead 62(44), override mtu 1280, media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: D9C00FC2
      current inbound spi : 4FCB6624

    inbound esp sas:
      spi: 0x4FCB6624 (1338730020)
         transform: esp-3des esp-sha-hmac no compression
         in use settings ={RA, Transport,  NAT-T-Encaps, GRE, IKEv2, }
         slot: 0, conn_id: 8192, crypto-map: def
         sa timing: remaining key lifetime (sec): 28387
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x0003FFFF 0xFFFFFFFF
    outbound esp sas:
      spi: 0xD9C00FC2 (3653242818)
         transform: esp-3des esp-sha-hmac no compression
         in use settings ={RA, Transport,  NAT-T-Encaps, GRE, IKEv2, }
         slot: 0, conn_id: 8192, crypto-map: def
         sa timing: remaining key lifetime (sec): 28387
         IV size: 8 bytes
        replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

以下示例显示 IPsec SA，包括用于将隧道标识为 OSPFv3 的使用中设置。

```
> show ipsec sa
interface: outside2
    Crypto map tag: def, local addr: 10.132.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (172.20.0.21/255.255.255.255/0/0)
      current_peer: 172.20.0.21
      dynamic allocated peer ip: 10.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1145, #pkts decrypt: 1145, #pkts verify: 1145
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 2, #pre-frag failures: 1, #fragments created: 10
      #PMTUs sent: 5, #PMTUs rcvd: 2, #decapstulated frags needing reassembly: 1
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 10.132.0.17, remote crypto endpt.: 172.20.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={L2L, Transport, Manual key (OSPFv3),}
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 548
         IV size: 8 bytes
         replay detection support: Y
```

```
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={L2L, Transport, Manual key (OSPFv3), }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 548
         IV size: 8 bytes
         replay detection support: Y

    Crypto map tag: def, local addr: 10.132.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
```

注释 如果 IPsec SA 策略表明在 IPsec 处理前进行碎片整理，则碎片整理统计信息为碎片整理前统计信息。如果 SA 策略表明在 IPsec 处理后进行碎片整理，则显示碎片整理后统计信息。

以下示例在全局配置模式下输入，显示名为 def 的加密映射的 IPsec SA。

```
> show ipsec sa map def
cryptomap: def
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1146, #pkts decrypt: 1146, #pkts verify: 1146
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 480
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 480
         IV size: 8 bytes
         replay detection support: Y

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
```

```
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73672, #pkts encrypt: 73672, #pkts digest: 73672
      #pkts decaps: 78824, #pkts decrypt: 78824, #pkts verify: 78824
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73672, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 263
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 263
         IV size: 8 bytes
         replay detection support: Y
```

以下示例显示 **entry** 关键字的 IPsec SA。

```
> show ipsec sa entry
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 429
         IV size: 8 bytes
         replay detection support: Y
```

```
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 429
         IV size: 8 bytes
         replay detection support: Y
peer address: 10.135.1.8
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73723, #pkts encrypt: 73723, #pkts digest: 73723
      #pkts decaps: 78878, #pkts decrypt: 78878, #pkts verify: 78878
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73723, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 212
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 212
         IV size: 8 bytes
         replay detection support: Y
```

以下示例显示带有 **entry detail** 关键字的 IPsec SA。

```
> show ipsec sa entry detail
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1148, #pkts decrypt: 1148, #pkts verify: 1148
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
```

```
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 322
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 322
         IV size: 8 bytes
         replay detection support: Y

peer address: 10.135.1.8
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73831, #pkts encrypt: 73831, #pkts digest: 73831
      #pkts decaps: 78989, #pkts decrypt: 78989, #pkts verify: 78989
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73831, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 104
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
```

```
          slot: 0, conn_id: 4, crypto-map: def
          sa timing: remaining key lifetime (sec): 104
          IV size: 8 bytes
          replay detection support: Y
>
```

以下示例显示带有 **identity** 关键字的 IPsec SA。

```
> show ipsec sa identity
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73756, #pkts encrypt: 73756, #pkts digest: 73756
      #pkts decaps: 78911, #pkts decrypt: 78911, #pkts verify: 78911
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73756, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
```

以下示例显示具有关键字 **identity** 和 **detail** 的 IPsec SA。

```
> show ipsec sa identity detail
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
```

```
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73771, #pkts encrypt: 73771, #pkts digest: 73771
      #pkts decaps: 78926, #pkts decrypt: 78926, #pkts verify: 78926
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73771, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
```

以下示例展示基于分配 IPv6 地址的 IPSec SA：

```
> show ipsec sa assigned-address 2001:1000::10
assigned address: 2001:1000::10
    Crypto map tag: def, seq num: 1, local addr: 75.2.1.23

      local ident (addr/mask/prot/port): (75.2.1.23/255.255.255.255/47/0)
      remote ident (addr/mask/prot/port): (75.2.1.60/255.255.255.255/47/0)
      current_peer: 75.2.1.60, username: rashmi
      dynamic allocated peer ip: 65.2.1.100
      dynamic allocated peer ip(ipv6): 2001:1000::10

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 326, #pkts decrypt: 326, #pkts verify: 326
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #post-frag successes: 0, #post-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 35

      local crypto endpt.: 75.2.1.23/4500, remote crypto endpt.: 75.2.1.60/64251
      path mtu 1342, ipsec overhead 62(44), override mtu 1280, media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
```

```
  ICMP error validation: disabled, TFC packets: disabled
  current outbound spi: D9C00FC2
  current inbound spi : 4FCB6624

inbound esp sas:
  spi: 0x4FCB6624 (1338730020)
     transform: esp-3des esp-sha-hmac no compression
     in use settings ={RA, Transport,  NAT-T-Encaps, GRE, IKEv2, }
     slot: 0, conn_id: 8192, crypto-map: def
     sa timing: remaining key lifetime (sec): 28108
     IV size: 8 bytes
     replay detection support: Y
     Anti replay bitmap:
      0xFFFFFFFF 0xFFFFFFFF
outbound esp sas:
  spi: 0xD9C00FC2 (3653242818)
     transform: esp-3des esp-sha-hmac no compression
     in use settings ={RA, Transport,  NAT-T-Encaps, GRE, IKEv2, }
     slot: 0, conn_id: 8192, crypto-map: def
     sa timing: remaining key lifetime (sec): 28108
     IV size: 8 bytes
     replay detection support: Y
     Anti replay bitmap:
      0x00000000 0x00000001
```

Related Commands

命令	Description
clear isakmp sa	清除 IKE 运行时间 SA 数据库。
show running-config isakmp	显示所有活动的 ISAKMP 配置。

show ipsec sa summary

要显示 IPsec SA 摘要，请使用 **show ipsec sa summary**命令。

show ipsec sa summary

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例按以下连接类型显示 IPsec SA 摘要：

- IPSec
- IPsec over UDP
- IPsec over NAT-T
- IPsec over TCP
- IPsec VPN 负载平衡

```
> show ipsec sa summary
Current IPsec SA's:           Peak IPsec SA's:
IPsec            :     2        Peak Concurrent SA  :    14
IPsec over UDP   :     2        Peak Concurrent L2L :     0
IPsec over NAT-T :     4        Peak Concurrent RA  :    14
IPsec over TCP   :     6
IPsec VPN LB     :     0
Total            :    14
```

Related Commands

命令	Description
clear ipsec sa	全部或基于特定参数删除 IPsec SA。
show ipsec sa	显示 IPsec SA 列表。
show ipsec stats	显示 IPsec 统计信息列表。

show ipsec stats

要显示 IPsec 统计信息列表，请使用 **show ipsec stats** 命令。

show ipsec stats

Command History

版本	修改
6.1	引入了此命令。

使用指南

下表说明了输出条目指示的内容。

输出（续）	说明（续）
IPsec Global Statistics	此部分显示 threat defense 设备支持的 IPsec 隧道总数。
Active tunnels	当前连接的 IPsec 隧道数。
Previous tunnels	已连接的 IPsec 隧道数，包括主用隧道。
入站	此部分显示通过 IPsec 隧道接收的入站加密流量。
Bytes	接收的加密流量的字节数。
解压缩的字节	执行解压缩之后接收的加密流量的字节数（如果适用）。如果未启用压缩，此计数器应始终等于前一个计数器。
数据包	接收的加密 IPsec 数据包数。
已丢弃的数据包	已接收但由于错误而丢弃的加密 IPsec 数据包数。
重播故障	对接收的加密 IPsec 数据包检测到的反重播故障数。
身份验证	对接收的加密 IPsec 数据包执行的身份验证成功数。
身份验证失败	对接收的加密 IPsec 数据包检测到的身份验证失败数。
解密	对接收的加密 IPsec 数据包执行的解密成功数。
解密失败	对接收的加密 IPsec 数据包检测到的解密失败数。
需要重组地解封分段	包括要重组的 IP 分段的解密 IPsec 数据包数。
发送	此部分显示要通过 IPsec 流量传输的出站明文流量。
Bytes	要通过 IPsec 隧道加密并传输的明文流量字节数。
未压缩字节数	要通过IPsec隧道加密并传输的未压缩明文流量字节数。如果未启用压缩，此计数器应始终等于前一个计数器。

输出（续）	说明（续）
数据包	要通过 IPsec 隧道加密并传输的明文流量字节数据包。
已丢弃的数据包	要通过IPsec隧道加密并传输而由于错误已丢弃的明文数据包数。
身份验证	对要通过 IPsec 隧道传输的数据包执行的身份验证成功数。
身份验证失败	对要通过IPsec隧道传输的数据包检测到的身份验证失败数。
加密	对要通过 IPsec 隧道传输的数据包执行的加密成功数。
加密失败	对要通过 IPsec 隧道传输的数据包检测到的加密失败数。
分段成功	作为出站IPsec数据包转换的一部分执行的分段操作成功数。
预分段成功	作为出站 IPsec 数据包转换的一部分执行的预分段操作成功数。预分段发生在将明文数据包加密和封装为一个或多个 IPsec 数据包之前。
后分段成功	作为出站 IPsec 数据包转换的一部分执行的预分段操作成功数。后分段发生在明文数据包加密和封装为 IPsec 数据包之后，会导致多个 IP 分段。必须在解密之前重组这些分段。
分段失败	出站 IPsec 数据包转换时发生的分段失败数。
预分段失败	出站IPsec数据包转换时发生的预分段失败数。预分段发生在将明文数据包加密和封装为一个或多个 IPsec 数据包之前。
后分段失败	出站IPsec数据包转换时发生的后分段失败数。后分段发生在明文数据包加密和封装为 IPsec 数据包之后，会导致多个 IP 分段。必须在解密之前重组这些分段。
创建的分段	IPsec 转换过程中创建的分段数。
发送的PMTU	IPsec 系统发送的路径 MTU 消息数。IPsec 将 PMTU 消息发送至内部主机，此主机正在发送封装后由于太大而无法通过 IPsec 隧道传输的数据包。PMTU 消息用于请求主机降低其 MTU 和发送更小的数据包以通过 IPsec 隧道传输。
接收的 PMTU	IPsec 系统接收的路径 MTU 消息数。如果通过隧道发送的数据包太大而无法遍历下游网络元素，IPsec将接收来自该网络元素的路径 MTU 消息。当接收路径 MTU 消息时，IPsec 通常会降低其隧道 MTU。
协议失败	接收的错误 IPsec 数据包数。
遗漏 SA 失败	因指定 IPsec 安全关联不存在而请求的 IPsec 操作数。

输出（续）	说明（续）
系统容量失败	因 IPsec 系统容量不足以支持数据速率而无法完成的 IPsec 操作数。

示例

以下示例在全局配置模式下输入，显示 IPsec 统计信息：

```
> show ipsec stats

IPsec Global Statistics
-----------------------
Active tunnels: 2
Previous tunnels: 9
Inbound
    Bytes: 4933013
    Decompressed bytes: 4933013
    Packets: 80348
    Dropped packets: 0
    Replay failures: 0
    Authentications: 80348
    Authentication failures: 0
    Decryptions: 80348
    Decryption failures: 0
    Decapsulated fragments needing reassembly: 0
Outbound
    Bytes: 4441740
    Uncompressed bytes: 4441740
    Packets: 74029
    Dropped packets: 0
    Authentications: 74029
    Authentication failures: 0
    Encryptions: 74029
    Encryption failures: 0
    Fragmentation successes: 3
        Pre-fragmentation successes:2
        Post-fragmentation successes: 1
    Fragmentation failures: 2
        Pre-fragmentation failures:1
        Post-fragmentation failures: 1
    Fragments created: 10
    PMTUs sent: 1
    PMTUs recvd: 2
Protocol failures: 0
Missing SA failures: 0
System capacity failures: 0
```

在支持 IPsec 流分流的平台上，输出显示已分流的流的计数器，而常规计数器显示已分流和未分流的流的总数。

```
> show ipsec stats

IPsec Global Statistics
-----------------------
Active tunnels: 1
Previous tunnels: 1
Inbound
    Bytes: 93568
```

```
    Decompressed bytes: 0
    Packets: 86
    Dropped packets: 0
    Replay failures: 0
    Authentications: 0
    Authentication failures: 0
    Decryptions: 86
    Decryption failures: 0
    TFC Packets: 0
    Decapsulated fragments needing reassembly: 0
    Valid ICMP Errors rcvd: 0
    Invalid ICMP Errors rcvd: 0
Outbound
    Bytes: 93568
    Uncompressed bytes: 90472
    Packets: 86
    Dropped packets: 0
    Authentications: 0
    Authentication failures: 0
    Encryptions: 86
    Encryption failures: 0
    TFC Packets: 0
    Fragmentation successes: 0
        Pre-fragmentation successes: 0
        Post-fragmentation successes: 0
    Fragmentation failures: 0
        Pre-fragmentation failures: 0
        Post-fragmentation failures: 0
    Fragments created: 0
    PMTUs sent: 0
    PMTUs rcvd: 0
Offloaded Inbound
    Bytes: 93568
    Packets: 86
    Authentications: 0
    Decryptions: 86
Offloaded Outbound
    Bytes: 93568
    Packets: 86
    Authentications: 0
    Encryptions: 86
Protocol failures: 0
Missing SA failures: 0
System capacity failures: 0
Inbound SA delete requests: 0
Outbound SA delete requests: 0
Inbound SA destroy calls: 0
Outbound SA destroy calls: 0
```

Related Commands

命令	Description
clear ipsec sa	基于指定的参数清除 IPsec SA 或计数器。
show ipsec sa	根据指定参数显示 IPsec SA。
show ipsec sa summary	显示 IPsec SA 摘要。

show ipv6 access-list

此命令用于 threat defense不支持的功能。IPv6 访问控制已集成到标准访问控制策略中。查看管理器中的策略，或使用以下命令：

- **show access-list**
- **show access-control-config**

show ipv6 dhcp

要显示 DHCPv6 信息，请使用 **show ipv6 dhcp** 命令。

show ipv6 dhcp ［**client** ［**pd**］ **statistics** | **interface** ［*interface_name* ［**statistics**］］ | **ha statistics** | **server statistics** | **pool** ［*pool_name*］］

Syntax Description

client ［**pd**］ **statistics**	显示DHCPv6客户端统计信息，并显示已发送和已接收的消息数量的输出结果。添加 **pd** 关键字以显示 DHCPv6 前缀委派客户端统计信息。
interface ［*interface_name* ［**statistics**］］	显示所有接口或指定接口的 DHCPv6 信息（可选）。如果接口配置用于DHCPv6无状态服务器配置，则此命令将列出该服务器正在使用的DHCPv6池。如果接口包含DHCPv6地址客户端或前缀委派客户端配置，则此命令将显示各个客户端的状态，以及从该服务器收到的值。 如果指定接口名称，则可以添加 **statistics** 以查看该接口的 DHCP 服务器或客户端的消息统计信息。
ha statistics	显示故障转移设备之间的事务处理统计信息，包括在DUID信息各个设备之间的同步次数。
server statistics	显示 DHCPv6 无状态服务器统计信息。
pool ［*pool_name*］	显示所有 DHCPv6 池或（可选）指定的池。

Command History

版本	修改
6.2.1	引入了此命令。

使用指南

如果不指定任何参数，此命令将显示 DHCPv6 客户端或服务器正在使用的设备 DUID。

示例

以下是 **show ipv6 dhcp** 命令的输出示例：

```
> show ipv6 dhcp
This device's DHCPv6 unique identifier(DUID): 00030001377E8FD91020
```

以下是 **show ipv6 dhcp pool** 命令的输出示例：

```
> show ipv6 dhcp pool
DHCPv6 pool: Sample-Pool
  Imported DNS server: 2004:abcd:abcd:abcd::2
  Imported DNS server: 2004:abcd:abcd:abcd::4
  Imported Domain name: relay.com
  Imported Domain name: server.com
  SIP server address: 2001::abcd:1
```

```
  SIP server domain name: sip.xyz.com
```

以下是 **show ipv6 dhcp interface** 命令的输出示例：

```
> show ipv6 dhcp interface
GigabitEthernet1/1 is in server mode
  Using pool: Sample-Pool

GigabitEthernet1/2 is in client mode
  Prefix State is OPEN
  Renew will be sent in 00:03:46
  Address State is OPEN
  Renew for address will be sent in 00:03:47
  List of known servers:
    Reachable via address: fe80::20c:29ff:fe96:1bf4
    DUID: 000100011D9D1712005056A07E06
    Preference: 0
    Configuration parameters:
      IA PD: IA ID 0x00030001, T1 250, T2 400
        Prefix: 2005:abcd:ab03::/48
                preferred lifetime 500, valid lifetime 600
                expires at Nov 26 2014 03:11 PM (577 seconds)
      IA NA: IA ID 0x00030001, T1 250, T2 400
        Address: 2004:abcd:abcd:abcd:abcd:abcd:abcd:f2cb/128
                preferred lifetime 500, valid lifetime 600
                expires at Nov 26 2014 03:11 PM (577 seconds)
      DNS server: 2004:abcd:abcd:abcd::2
      DNS server: 2004:abcd:abcd:abcd::4
      Domain name: relay.com
      Domain name: server.com
      Information refresh time: 0
  Prefix name: Sample-PD

Management1/1 is in client mode
  Prefix State is IDLE
  Address State is OPEN
  Renew for address will be sent in 11:26:44
  List of known servers:
    Reachable via address: fe80::4e00:82ff:fe6f:f6f9
    DUID: 000300014C00826FF6F8
    Preference: 0
    Configuration parameters:
      IA NA: IA ID 0x000a0001, T1 43200, T2 69120
        Address: 2308:2308:210:1812:2504:1234:abcd:8e5a/128
                preferred lifetime INFINITY, valid lifetime INFINITY
      Information refresh time: 0
```

以下是 **show ipv6 dhcp interface outside** 命令的输出示例：

```
> show ipv6 dhcp interface outside
GigabitEthernet1/2 is in client mode


 Prefix State is OPEN
 Renew will be sent in 00:02:05
 Address State is OPEN
 Renew for address will be sent in 00:02:06
 List of known servers:
   Reachable via address: fe80::20c:29ff:fe96:1bf4
   DUID: 000100011D9D1712005056A07E06
   Preference: 0
```

```
   Configuration parameters:
     IA PD: IA ID 0x00030001, T1 250, T2 400
       Prefix: 2005:abcd:ab03::/48
               preferred lifetime 500, valid lifetime 600
               expires at Nov 26 2014 03:11 PM (476 seconds)
     IA NA: IA ID 0x00030001, T1 250, T2 400
       Address: 2004:abcd:abcd:abcd:abcd:abcd:abcd:f2cb/128
               preferred lifetime 500, valid lifetime 600
               expires at Nov 26 2014 03:11 PM (476 seconds)
     DNS server: 2004:abcd:abcd:abcd::2
     DNS server: 2004:abcd:abcd:abcd::4
     Domain name: relay.com
     Domain name: server.com
     Information refresh time: 0
 Prefix name: Sample-PD
```

以下是 **show ipv6 dhcp interface outside statistics** 命令的输出示例：

```
> show ipv6 dhcp interface outside statistics
DHCPV6 Client PD statistics:

Protocol Exchange Statistics:


 Number of Solicit messages sent:              1
 Number of Advertise messages received:        1
 Number of Request messages sent:              1
 Number of Renew messages sent:                45
 Number of Rebind messages sent:               0
 Number of Reply messages received:            46
 Number of Release messages sent:              0
 Number of Reconfigure messages received:      0
 Number of Information-request messages sent:  0

Error and Failure Statistics:


 Number of Re-transmission messages sent:                 1
 Number of Message Validation errors in received messages: 0

DHCPV6 Client address statistics:

Protocol Exchange Statistics:


 Number of Solicit messages sent:              1
 Number of Advertise messages received:        1
 Number of Request messages sent:              1
 Number of Renew messages sent:                45
 Number of Rebind messages sent:               0
 Number of Reply messages received:            46
 Number of Release messages sent:              0
 Number of Reconfigure messages received:      0
 Number of Information-request messages sent:  0

Error and Failure Statistics:


 Number of Re-transmission messages sent:                 1
 Number of Message Validation errors in received messages: 0
```

以下是 **show ipv6 dhcp client statistics** 命令的输出示例：

```
> show ipv6 dhcp client statistics

Protocol Exchange Statistics:
  Total number of Solicit messages sent:              4
  Total number of Advertise messages received:        4
  Total number of Request messages sent:              4
  Total number of Renew messages sent:                92
  Total number of Rebind messages sent:               0
  Total number of Reply messages received:            96
  Total number of Release messages sent:              6
  Total number of Reconfigure messages received:      0
  Total number of Information-request messages sent:  0

Error and Failure Statistics:
  Total number of Re-transmission messages sent:                  8
  Total number of Message Validation errors in received messages: 0
```

以下是 **show ipv6 dhcp client pd statistics** 命令的输出示例：

```
> show ipv6 dhcp client pd statistics

Protocol Exchange Statistics:


 Total number of Solicit messages sent:              1
 Total number of Advertise messages received:        1
 Total number of Request messages sent:              1
 Total number of Renew messages sent:                92
 Total number of Rebind messages sent:               0
 Total number of Reply messages received:            93
 Total number of Release messages sent:              0
 Total number of Reconfigure messages received:      0
 Total number of Information-request messages sent:  0

Error and Failure Statistics:


 Total number of Re-transmission messages sent:                 1
 Total number of Message Validation errors in received messages: 0
```

以下是 **show ipv6 dhcp server statistics** 命令的输出示例：

```
> show ipv6 dhcp server statistics

Protocol Exchange Statistics:
  Total number of Solicit messages received:             0
  Total number of Advertise messages sent:               0
  Total number of Request messages received:             0
  Total number of Renew messages received:               0
  Total number of Rebind messages received:              0
  Total number of Reply messages sent:                   10
  Total number of Release messages received:             0
  Total number of Reconfigure messages sent:             0
  Total number of Information-request messages received: 10
  Total number of Relay-Forward messages received:       0
  Total number of Relay-Reply messages sent:             0

Error and Failure Statistics:
```

```
  Total number of Re-transmission messages sent:                  0
  Total number of Message Validation errors in received messages: 0
```

以下是 **show ipv6 dhcp ha statistics** 命令的输出示例：

```
> show ipv6 dhcp ha statistics

DHCPv6 HA global statistics:
  DUID sync messages sent:              1
  DUID sync messages received:          0

DHCPv6 HA error statistics:
  Send errors:                          0
```

以下是备用设备上 **show ipv6 dhcp ha statistics** 命令的输出示例：

```
> show ipv6 dhcp ha statistics

DHCPv6 HA global statistics:
  DUID sync messages sent:              0
  DUID sync messages received:          1

DHCPv6 HA error statistics:
  Send errors:                          0
```

Related Commands

命令	Description
clear ipv6 dhcp	清除 DHCPv6 统计信息。

show ipv6 dhcprelay binding

使用 **show ipv6 dhcprelay binding** 命令以显示中继代理创建的中继绑定条目。

show ipv6 dhcprelay binding

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show ipv6 dhcprelay binding** 命令的输出示例：

```
> show ipv6 dhcprelay binding
1 in use, 2 most used

Client: fe80::204:23ff:febb:b094 (inside)
  DUID: 000100010f9a59d1000423bbb094, Timeout in 60 seconds

Above binding is created for client with link local address of fe80::204:23ff:febb:b094 on
the inside interface using DHCPv6 id of 000100010f9a59d1000423bbb094, and will timeout in
60 seconds.

There will be limit of 1000 bindings for each context.
```

Related Commands

命令	Description
show ipv6 dhcprelay statistics	显示 IPv6 DHCP 中继代理信息。

show ipv6 dhcprelay statistics

要显示 IPv6 DHCP 中继代理统计信息，请使用 **show ipv6 dhcprelay statistics** 命令。

show ipv6 dhcprelay statistics

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show ipv6 dhcprelay statistics** 命令的输出示例：

```
> show ipv6 dhcprelay statistics
Relay Messages:
  SOLICIT                                     1
  ADVERTISE                                   2
  REQUEST                                     1
  CONFIRM                                     1
  RENEW                                     496
  REBIND                                      0
  REPLY                                     498
  RELEASE                                     0
  DECLINE                                     0
  RECONFIGURE                                 0
  INFORMATION-REQUEST                         0
  RELAY-FORWARD                             499
  RELAY-REPLY                               500

Relay Errors:
  Malformed message:                          0
  Block allocation/duplication failures:      0
  Hop count limit exceeded:                   0
  Forward binding creation failures:          0
  Reply binding lookup failures:              0
  No output route:                            0
  Conflict relay server route:                0
  Failed to add server NP rule:               0
  Unit or context is not active:              0

Total Relay Bindings Created:               498
```

Related Commands

命令	Description
show ipv6 dhcprelay binding	显示中继代理创建的中继绑定条目。

show ipv6 general-prefix

要显示 IPv6 通用前缀，请使用 **show ipv6 general-prefix** 命令。

show ipv6 general-prefix

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用 **show ipv6 general-prefix** 命令可查看有关 IPv6 通用前缀的信息。

示例

以下是 **show ipv6 general-prefix** 命令的输出示例：

```
> show ipv6 general-prefix
IPv6 Prefix my-prefix, acquired via 6to4
2002:B0B:B0B::/48
 Loopback42 (Address command)
Codes: A - Address, P - Prefix-Advertisement, O - Pool
       U - Per-user prefix, D - Default       N - Not advertised, C - Calendar

AD      fec0:0:0:a::/64 [LA] Valid lifetime 2592000, preferred lifetime 604800
```

show ipv6 icmp

要显示在所有接口上配置的 ICMPv6 访问规则，请使用 **show ipv6 icmp** 命令。

show ipv6 icmp

Command History

版本	修改
6.1	引入了此命令。

使用指南

ICMPv6 规则控制流向设备接口的 ICMPv6 流量。它们不控制通过设备的流量。您可以使用这些规则来控制哪些地址可以向接口发送 ICMPv6 命令（例如 ping），以及可以发送哪些类型的 ICMPv6 命令。使用 **show ipv6 icmp** 命令查看这些规则。

示例

以下是 **show ipv6 icmp** 命令的输出示例。

```
> show ipv6 icmp
ipv6 icmp permit any inside
```

show ipv6 interface

要显示为 IPv6 配置的接口的状态，请使用 **show ipv6 interface** 命令。

show ipv6 interface ［**brief**］［*if_name* ［**prefix**］］

Syntax Description

brief	显示每个接口的 IPv6 状态和配置的简短汇总。
if_name	（可选）内部或外部接口名称。仅显示指定接口的状态和配置。 如果显示所有接口，则还会看到有关用于系统通信的内部接口的信息。用户无法配置内部接口，该信息只用于调试目的。
prefix	（可选）从本地 IPv6 前缀池生成的前缀。前缀是 IPv6 地址的网络部分。

Command Default

显示所有 IPv6 接口。

Command History

版本	修改
6.1	引入了此命令。

使用指南

show ipv6 interface 命令的输出类似于 **show interface** 命令的输出，唯一不同之处是，前者显示的信息是IPv6特定信息。如果接口硬件可用，会将接口标记为up。如果接口可以提供双向通信，会将线路协议标记为 up。

当未指定接口名称时，会显示所有 IPv6 接口的信息。指定接口名称则会显示有关指定接口的信息。

示例

以下是 **show ipv6 interface** 命令的输出示例：

```
> show ipv6 interface outside
interface ethernet0 “outside” is up, line protocol is up
  IPv6 is enabled, link-local address is 2001:0DB8::/29 [TENTATIVE]
  Global unicast address(es):
    2000::2, subnet is 2000::/64
  Joined group address(es):
    FF02::1
    FF02::1:FF11:6770
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
```

以下是使用 **brief** 关键字输入的 **show ipv6 interface** 命令的输出示例：

```
> show ipv6 interface brief
outside [up/up]
    unassigned
inside [up/up]
    fe80::20d:29ff:fe1d:69f0
    fec0::a:0:0:a0a:a70
vlan101 [up/up]
    fe80::20d:29ff:fe1d:69f0
    fec0::65:0:0:a0a:6570
dmz-ca [up/up]
    unassigned
```

以下是 **show ipv6 interface** 命令的输出示例。它显示已从地址生成前缀的接口的特征。

```
> show ipv6 interface inside prefix
IPv6 Prefix Advertisements inside
Codes: A - Address, P - Prefix-Advertisement, O - Pool
       U - Per-user prefix, D - Default       N - Not advertised, C - Calendar

AD      fec0:0:0:a::/64 [LA] Valid lifetime 2592000, preferred lifetime 604800
```

show ipv6 local pool

要显示 IPv6 地址池信息，请使用 **show ipv6 local pool** 命令。

show ipv6 local pool *pool_name*

Syntax Description

pool_name	IPv6 地址池的名称。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用此命令可查看 IPv6 地址池的内容。这些池用于 远程访问 VPN 和 集群技术。使用 **show ip local pool** 以查看IPv4 地址池。

示例

以下是 **show ipv6 local pool** 命令的输出示例：

```
> show ipv6 local pool test-ipv6-pool
IPv6 Pool test-ipv6-pool
Begin Address: 2001:db8::db8:800:200c:417a
End Address: 2001:db8::db8:800:200c:4188
Prefix Length: 64
Pool Size: 15
Number of used addresses: 0
Number of available addresses: 15

Available Addresses:
2001:db8::db8:800:200c:417a
2001:db8::db8:800:200c:417b
2001:db8::db8:800:200c:417c
2001:db8::db8:800:200c:417d
2001:db8::db8:800:200c:417e
2001:db8::db8:800:200c:417f
2001:db8::db8:800:200c:4180
2001:db8::db8:800:200c:4181
2001:db8::db8:800:200c:4182
2001:db8::db8:800:200c:4183
2001:db8::db8:800:200c:4184
2001:db8::db8:800:200c:4185
2001:db8::db8:800:200c:4186
2001:db8::db8:800:200c:4187
2001:db8::db8:800:200c:4188
```

show ipv6 mld traffic

要显示组播侦听程序发现 (MLD) 流量计数器信息，请使用 **show ipv6 mld traffic** 命令。

show ipv6 mld traffic

Command History

版本	修改
6.1	引入了此命令。

使用指南

show ipv6 mld traffic 命令允许您检查是否已接收和发送预计的 MLD 消息数。以下信息是由 **show ipv6 mld traffic** 命令提供信息：

- 清除计数器以后经过的时间 - 自清除计数器以来的时间量。
- 有效 MLD 数据包 - 接收和发送的有效 MLD 数据包数。
- 查询 - 接收和发送的有效查询数。
- 报告 - 接收和发送的有效报告数。
- 保留 - 接收和发送的有效保留数。
- Mtrace 数据包 - 接收和发送的组播跟踪数据包数。
- Errors（错误）- 错误类型和发生的错误数。

示例

以下是 **show ipv6 mld traffic** 命令的输出示例：

```
> show ipv6 mld traffic
show ipv6 mld traffic
MLD Traffic Counters
Elapsed time since counters cleared: 00:01:19
                  Received          Sent
Valid MLD Packets  1                 3
Queries            1                 0
Reports            0                 3
Leaves             0                 0
Mtrace packets     0                 0
Errors:
Malformed Packets  0
Martian source     0
Non link-local source 0
Hop limit is not equal to 1 0
```

Related Commands

命令	Description
clear ipv6 mld traffic	重置所有 MLD 流量计数器。

show ipv6 neighbor

要显示 IPv6 邻居发现缓存信息，请使用 **show ipv6 neighbor** 命令。

show ipv6 neighbor ［*if_name* | 地址］

Syntax Description

地址	（可选）仅显示提供的 IPv6 地址的邻居发现缓存信息。
if_name	（可选）显示所提供接口名称的缓存信息。 如果显示所有接口，则还会看到有关用于系统通信的内部接口的信息。用户无法配置内部接口，该信息只用于调试目的。

Command History

版本	修改
6.1	引入了此命令。

使用指南

以下信息是由 **show ipv6 neighbor** 命令提供信息：

- IPv6 地址 - 邻居或接口的 IPv6 地址。
- Age（时间）- 自确认地址可到达以来的时间（以分钟为单位）。连字符 (-) 指示静态条目。
- 链路层地址 - MAC 地址。如果地址未知，则显示连字符 (-)。
- 状态 - 邻居缓存条目的状态。

注释 连通性检测不会应用于 IPv6 邻居发现缓存中的静态条目；因此，对于动态和静态缓存条目，INCMP（未完成）和 REACH（可达）状态的说明不同。

以下是 IPv6 邻居发现缓存中动态条目的可能状态：

- INCMP -（未完成）正在对条目执行地址解析。邻居请求消息已发送至目标的请求节点组播地址，但是尚未收到对应的邻居通告消息。
- REACH -（可达）在最后 ReachableTime 毫秒内收到正面确认，指示邻居的转发路径运行正常。在 REACH 状态下，由于数据包已发送，设备不执行任何特殊操作。
- STALE-自设备收到表明转发路径运行正常的最后一个正面确认之后，已经历了超过 ReachableTime 毫秒。在 STALE 状态下，设备在数据包发送完成之前不执行任何操作。
- DELAY-自设备收到表明转发路径运行正常的最后一个正面确认之后，已经历了超过 ReachableTime 毫秒。数据包在最后 DELAY_FIRST_PROBE_TIME 秒内已发送。在进入 DELAY 状态的 DELAY_FIRST_PROBE_TIME 秒内，如果未收到确定性确认，则发送邻居请求消息并将状态更改为 PROBE。

- PROBE - 通过每 RetransTimer 毫秒后重新发送邻居请求消息，积极寻找连通性确认，直至收到可达性确认。
- ???? - 未知状态。

以下是 IPv6 邻居发现缓存中静态条目的可能状态：

- INCMP -（未完成）此条目的接口关闭。
- REACH -（可达）此条目的接口开启。

- Interface

  可从中访问地址的接口。

示例

以下是输入具有接口的 **show ipv6 neighbor** 命令时的输出示例：

```
> show ipv6 neighbor inside
IPv6 Address                              Age Link-layer Addr State Interface
2000:0:0:4::2                               0 0003.a0d6.141e  REACH inside
FE80::203:A0FF:FED6:141E                    0 0003.a0d6.141e  REACH inside
3001:1::45a                                 - 0002.7d1a.9472  REACH inside
```

以下是输入具有 IPv6 地址的 **show ipv6 neighbor** 命令时，该命令的输出示例：

```
> show ipv6 neighbor 2000:0:0:4::2
IPv6 Address                              Age Link-layer Addr State Interface
2000:0:0:4::2                               0 0003.a0d6.141e  REACH inside
```

Related Commands

命令	Description
clear ipv6 neighbors	删除 IPv6 邻居发现缓存中除静态条目以外的所有条目。

show ipv6 ospf

要显示有关 OSPFv3 路由流程的一般信息，请使用 **show ipv6 ospf** 命令。

show ipv6 ospf ［*process_id*］［*area_id*］

Syntax Description

area_id	（可选）仅显示有关指定区域的信息。
process_id	（可选）指定本地分配的内部ID，可以是任何正整数。启用OSPFv3路由流程时，此 ID 是管理性分配的号码。

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show ipv6 ospf** 命令的输出示例：

```
> show ipv6 ospf
Routing Process “ospfv3 1” with ID 10.9.4.1
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
It is an autonomous system boundary router
Redistributing External Routes from,
   ospf 2
Initial SPF schedule delay 5000 msecs
Minimum hold time between two consecutive SPFs 10000 msecs
Maximum wait time between two consecutive SPFs 10000 msecs
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msecs
```

Related Commands

命令	Description
show ipv6 ospf border-routers	显示区域边界路由器(ABR)和自主系统边界路由器(ASBR)的内部OSPFv3路由表条目。
show ipv6 ospf database	显示与特定路由器 OSPFv3 数据库相关的信息列表。

show ipv6 ospf border-routers

要显示区域边界路由器 (ABR) 和自治系统边界路由器 (ASBR) 的内部 OSPFv3 路由表条目，请使用 **show ipv6 ospf border-routers** 命令。

show ipv6 ospf ［*process_id*］ **border-routers**

Syntax Description

process_id	（可选）指定本地分配的内部ID，可以是任何正整数。启用OSPFv3路由流程时，此 ID 是管理性分配的号码。

Command History

版本	修改
6.1	引入了此命令。

使用指南

show ipv6 ospf border-routers 命令列出以下设置：

- 区域内路由
- 区域间路由
- IPv6 地址
- 接口类型
- 区域 ID
- SPF 编号

示例

以下是 **show ipv6 ospf border-routers** 命令的输出示例：

```
> show ipv6 ospf border-routers
OSPFv3 Process 1 internal Routing Table

Codes: i - Intra-area route, I - Inter-area route

i 172.16.4.4 [2] via FE80::205:5FFF:FED3:5808, FastEthernet0/0, ABR, Area 1, SPF 13
i 172.16.4.4 [1] via FE80::205:5FFF:FED3:5406, POS4/0, ABR, Area 0, SPF 8
i 172.16.3.3 [1] via FE80::205:5FFF:FED3:5808, FastEthernet0/0, ASBR, Area 1, SPF 3
```

Related Commands

命令	Description
show ipv6 ospf	显示 OSPFv3 路由流程中的所有 IPv6 设置。
show ipv6 ospf database	显示与特定路由器 OSPFv3 数据库相关的信息列表。

show ipv6 ospf database

要显示与特定路由器 OSPFv3 数据库相关的信息列表，请使用 **show ipv6 ospf database** 命令。

show ipv6 ospf ［*process_id*］［*area_id*］ **database** ［**external** | **inter-area prefix** | **inter-area-router** | **network** | **nssa-external** | **router** | **area** | **as** | **ref-lsa** | ［*destination-router-id*］［**prefix** *ipv6-prefix*］［*link-state-id*］］［**link** ［**interface** *interface-name*］［**adv-router** *router-id*］ | **self-originate**］［**internal**］［**database-summary**］

Syntax Description

adv-router *router-id*	（可选）显示通告路由器的所有 LSA。路由器 ID 必须是 RFC 2740 中记录的形式，其中地址以使用冒号分隔 16 位值的十六进制格式指定。
area	（可选）仅显示有关区域 LSA 的信息。
area_id	（可选）仅显示有关指定区域的信息。
as	（可选）过滤未知自主系统 (AS) LSA。
database-summary	（可选）显示数据库中每个区域的每种类型的 LSA 数以及总数。
destination-router-id	（可选）仅显示有关指定目标路由器的信息。
external	（可选）仅显示有关外部 LSA 的信息。
interface	（可选）显示有关依据接口情景过滤的 LSA 的信息。
interface-name	（可选）指定 LSA 接口名称。
internal	（可选）仅显示有关内部 LSA 的信息。
inter-area prefix	（可选）仅显示有关基于区域间前缀的 LSA 的信息。
inter-area router	（可选）仅显示有关基于区域间路由器 LSA 的 LSA 的信息。
link	（可选）显示有关链路 LSA 的信息。当后面有 **unknown** 关键字时， **link** 关键字会过滤链路范围 LSA。
link-state-id	（可选）指定用于区分 LSA 的整数。在网络和链路 LSA 中，链路状态 ID 与接口索引匹配。
network	（可选）显示有关网络 LSA 的信息。
nssa-external	（可选）仅显示有关末节区域 (NSSA) 外部 LSA 的信息。
prefix *ipv6-prefix*	（可选）显示邻居的本地链路 IPv6 地址。IPv6 前缀必须采用 RFC 2373 规定的格式，其中地址以十六进制的 16 位值指定，各个值之间用冒号分隔。
process_id	（可选）指定本地分配的内部 ID，可以是任何正整数。启用 OSPF 路由流程时，此 ID 是管理性分配的号码。

ref-lsa	（可选）进一步过滤前缀 LSA 类型。
router	（可选）显示有关路由器 LSA 的信息。
self-originate	（可选）仅显示来自本地路由器的自发 LSA。

Command History

版本	修改
6.1	引入了此命令。

使用指南

多种形式的命令提供有关不同 OSPFv3 LSA 的信息。

示例

以下是 **show ipv6 ospf database** 命令的输出示例：

```
> show ipv6 ospf database

            OSPFv3 Router with ID (172.16.4.4) (Process ID 1)

                Router Link States (Area 0)

ADV Router         Age         Seq#        Fragment ID   Link count  Bits
172.16.4.4         239         0x80000003  0             1           B
172.16.6.6         239         0x80000003  0             1           B

            Inter Area Prefix Link States (Area 0)

ADV Router         Age         Seq#        Prefix
172.16.4.4         249         0x80000001  FEC0:3344::/32
172.16.4.4         219         0x80000001  FEC0:3366::/32
172.16.6.6         247         0x80000001  FEC0:3366::/32
172.16.6.6         193         0x80000001  FEC0:3344::/32
172.16.6.6         82          0x80000001  FEC0::/32

            Inter Area Router Link States (Area 0)

ADV Router         Age         Seq#        Link ID    Dest RtrID
172.16.4.4         219         0x80000001  50529027   172.16.3.3
172.16.6.6         193         0x80000001  50529027   172.16.3.3

            Link (Type-8) Link States (Area 0)

ADV Router         Age         Seq#        Link ID    Interface
172.16.4.4         242         0x80000002  14         PO4/0
172.16.6.6         252         0x80000002  14         PO4/0

            Intra Area Prefix Link States (Area 0)

ADV Router         Age         Seq#        Link ID    Ref-lstype  Ref-LSID
172.16.4.4         242         0x80000002  0          0x2001      0
172.16.6.6         252         0x80000002  0          0x2001      0
```

Related Commands

命令	Description
show ipv6 ospf	显示 OSPFv3 路由流程中的所有 IPv6 设置。
show ipv6 ospf border-routers	显示区域边界路由器 (ABR) 和自主系统边界路由器 (ASBR) 的内部 OSPFv3 路由表条目。

show ipv6 ospf events

要显示 OSPFv3 内部事件信息，请使用 **show ipv6 ospf events** 命令。

show ipv6 ospf ［*process_id*］ **events** ［*type*］

Syntax Description

process_id	（可选）指定本地分配的内部ID，可以是任何正整数。启用OSPF路由流程时，此 ID 是管理性分配的号码。
type	（可选）要查看的事件类型的列表。如果不指定一种或多种类型，则会看到所有事件。您可以过滤以下类型： • **generic**-通用事件。 • **interface**- 接口状态更改事件。 • **lsa**- LSA 到达和 LSA 生成事件。 • **neighbor**- 邻居状态更改事件。 • **reverse**- 以相反的顺序显示事件。 • **rib**- 路由器信息库更新、删除和重新分发事件。 • **spf**- SPF 计划和 SPF 运行事件。

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show ipv6 ospf events** 命令的输出示例：

```
> show ipv6 ospf events

OSPFv3 Router with ID (10.1.3.2) (Process ID 10)

   1 Jul 9  18:49:34.071: Timer Exp:  ospfv3_if_ack_delayed  0xda05fad8
   2 Jul 9  18:49:31.571: Rcv Unchanged Type-0x2001 LSA, LSID 0.0.0.0, Adv-Rtr 10.1.1.2,

Seq# 80000008, Age 1, Area 10
   3 Jul 9  18:48:13.241: Generate Changed Type-0x8 LSA, LSID 2.0.0.0, Seq# 80000004,
Age    0, Area 10
   4 Jul 9  18:48:13.241: Generate Changed Type-0x2001 LSA, LSID 0.0.0.0, Seq# 80000005,

Age 0, Area 10
   5 Jul 9  18:41:18.901: End of SPF, SPF time 0ms, next wait-interval 10000ms
   6 Jul 9  18:41:18.902: Starting External processing in area 10
   7 Jul 9  18:41:18.902: Starting External processing
   8 Jul 9  18:41:18.902: Starting Inter-Area SPF in area 10
```

```
   9 Jul 9  18:41:18.902: Generic:  post_spf_intra  0x0
  10 Jul 9  18:41:18.902: RIB Delete (All Paths), Prefix 2002::/64, type Intra
  11 Jul 9  18:41:18.902: RIB Update, Prefix 5005::/64, gw ::, via inside, type Intra
  12 Jul 9  18:41:18.902: Starting Intra-Area SPF in Area 10
  13 Jul 9  18:41:18.903: Starting SPF, wait-interval 5000ms
  14 Jul 9  18:41:16.403: Timer Exp:  ospfv3_if_ack_delayed  0xda05fad8
  15 Jul 9  18:41:13.903: Schedule SPF, Area 10, Change in LSA type PLSID 0.8.0.0,
Adv-Rtr   50.100.168.192
  16 Jul 9  18:41:13.903: Rcv Changed Type-0x2009 LSA, LSID 0.8.0.0, Adv-Rtr 10.1.2.3,
Seq# 80000003, Age 1, Area 10
```

Related Commands

命令	Description
show ipv6 ospf	显示 OSPFv3 路由流程中的所有 IPv6 设置。
show ipv6 ospf border-routers	显示区域边界路由器(ABR)和自主系统边界路由器(ASBR)的内部OSPFv3路由表条目。

show ipv6 ospf flood-list

要显示等待通过接口泛洪的 OSPFv3 LSA 列表，请使用 **show ipv6 ospf flood-list** 命令。

show ipv6 ospf ［*process_id*］［*area_id*］ **flood-list** *interface-type interface-number*

Syntax Description

area_id	（可选）仅显示有关指定区域的信息。
interface-number	指定泛洪 LSA 所在的接口号。
interface-type	指定泛洪 LSA 所在的接口类型。
process_id	（可选）指定本地分配的内部ID，可以是任何正整数。启用OSPFv3路由流程时，此 ID 是管理性分配的号码。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用此命令可显示 OSPFv3 数据包节奏信息。

示例

以下是 **show ipv6 ospf flood-list** 命令的输出示例：

```
> show ipv6 ospf flood-list

OSPFv3 Router with ID (172.16.6.6) (Process ID 1)

 Interface POS4/0, Queue length 1
 Link state retransmission due in 14 msec

 Type    LS ID           ADV RTR         Seq NO      Age    Checksum
 0x2001  0               172.16.6.6      0x80000031  0      0x1971

 Interface FastEthernet0/0, Queue length 0

 Interface ATM3/0, Queue length 0
```

Related Commands

命令	Description
show ipv6 ospf	显示 OSPFv3 路由流程中的所有 IPv6 设置。
show ipv6 ospf border-routers	显示区域边界路由器(ABR)和自主系统边界路由器(ASBR)的内部OSPFv3路由表条目。

show ipv6 ospf graceful-restart

要显示有关 OSPFv3 graceful-restart 的信息，请使用 **show ipv6 ospf graceful-restart** 命令。

show ipv6 ospf graceful-restart

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show ipv6 ospf graceful-restart** 命令的输出示例：

```
> show ipv6 ospf graceful-restart
Routing Process "ospfv3 10"
  Graceful Restart enabled
    restart-interval limit: 240 sec
    Clustering is not configured in spanned etherchannel mode
  Graceful Restart helper support enabled
    Number of neighbors performing Graceful Restart is 0
```

Related Commands

命令	Description
show ipv6 ospf	显示 OSPFv3 路由流程中的所有 IPv6 设置。

show ipv6 ospf interface

要显示 OSPFv3 相关的接口信息，请使用 **show ipv6 ospf interface** 命令。

show ipv6 ospf ［*process_id*］［*area_id*］ **interface** ［*type-number*］［**brief**］

Syntax Description

area_id	（可选）仅显示有关指定区域的信息。
brief	（可选）显示路由器上OSPFv3接口、状态、地址和掩码以及区域的简要概述信息。
process_id	（可选）指定本地分配的内部ID，可以是任何正整数。启用OSPF路由流程时，此 ID 是管理性分配的号码。
type-number	（可选）指定接口类型和号码。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用此命令可显示路由器上 OSPFv3 接口、状态、地址和掩码以及区域的概述信息。

示例

以下是 **show ipv6 ospf interface** 命令的输出示例：

```
> show ipv6 ospf interface
ATM3/0 is up, line protocol is up
  Link Local Address 2001:0DB1:205:5FFF:FED3:5808, Interface ID 13
  Area 1, Process ID 1, Instance ID 0, Router ID 172.16.3.3
  Network Type POINT_TO_POINT, Cost: 1
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
  Index 1/2/2, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 12, maximum is 12
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 172.16.4.4
  Suppress hello for 0 neighbor(s)
FastEthernet0/0 is up, line protocol is up
  Link Local Address 2001:0DB1:205:5FFF:FED3:5808, Interface ID 3
  Area 1, Process ID 1, Instance ID 0, Router ID 172.16.3.3
  Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 172.16.6.6, local address 2001:0DB1:205:5FFF:FED3:6408
  Backup Designated router (ID) 172.16.3.3, local address 2001:0DB1:205:5FFF:FED3:5808
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
```

```
Last flood scan length is 12, maximum is 12
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
  Adjacent with neighbor 172.16.6.6  (Designated Router)
Suppress hello for 0 neighbor(s)
```

Related Commands

命令	Description
show ipv6 ospf	显示 OSPFv3 路由流程中的所有 IPv6 设置。
show ipv6 ospf border-routers	显示区域边界路由器(ABR)和自主系统边界路由器(ASBR)的内部OSPFv3路由表条目。

show ipv6 ospf request-list

要显示路由器已请求的所有 LSA 的列表，请使用 **show ipv6 ospf request-list** 命令。

show ipv6 ospf ［*process_id*］［*area_id*］ **request-list** ［*neighbor*］［*interface*］［*interface-neighbor*］

Syntax Description

area_id	（可选）仅显示有关指定区域的信息。
interface	（可选）指定路由器从此接口请求的所有 LSA 的列表。
interface-neighbor	（可选）指定路由器在此接口上从此邻居请求的所有 LSA 的列表。
neighbor	（可选）指定路由器从此邻居请求的所有 LSA 的列表。
process_id	（可选）指定本地分配的内部ID，可以是任何正整数。启用OSPF路由流程时，此 ID 是管理性分配的号码。

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show ipv6 ospf request-list** 命令的输出示例：

```
> show ipv6 ospf request-list

            OSPFv3 Router with ID (192.168.255.5) (Process ID 1)

 Neighbor 192.168.255.2, interface Ethernet0/0 address
FE80::A8BB:CCFF:FE00:6600

 Type    LS ID           ADV RTR         Seq NO      Age    Checksum
  1      0.0.0.0         192.168.255.3   0x800000C2  1      0x0014C5
  1      0.0.0.0         192.168.255.2   0x800000C8  0      0x000BCA
  1      0.0.0.0         192.168.255.1   0x800000C5  1      0x008CD1
  2      0.0.0.3         192.168.255.3   0x800000A9  774    0x0058C0
  2      0.0.0.2         192.168.255.3   0x800000B7  1      0x003A63
```

Related Commands

命令	Description
show ipv6 ospf	显示 OSPFv3 路由流程中的所有 IPv6 设置。
show ipv6 ospf border-routers	显示区域边界路由器(ABR)和自主系统边界路由器(ASBR)的内部OSPFv3路由表条目。

show ipv6 ospf retransmission-list

要显示等待重新发送的所有 LSA 的列表，请使用 **show ipv6 ospf retransmission-list** 命令。

show ipv6 ospf ［*process_id*］［*area_id*］ **retransmission-list** ［*neighbor*］［*interface*］［*interface-neighbor*］

Syntax Description

area_id	（可选）仅显示有关指定区域的信息。
interface	（可选）指定在此接口上等待重新发送的所有 LSA 的列表。
interface-neighbor	（可选）指定针对此接口等待从此邻居重新发送的所有 LSA 的列表。
neighbor	（可选）指定等待针对此邻居重新发送的所有 LSA 的列表。
process_id	（可选）指定本地分配的内部ID，可以是任何正整数。启用OSPF路由流程时，此 ID 是管理性分配的号码。

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show ipv6 ospf retransmission-list** 命令的输出示例：

```
> show ipv6 ospf retransmission-list

        OSPFv3 Router with ID (192.168.255.2) (Process ID 1)

 Neighbor 192.168.255.1, interface Ethernet0/0
 Link state retransmission due in 3759 msec, Queue length 1

 Type    LS ID           ADV RTR         Seq NO      Age    Checksum
 0x2001  0               192.168.255.2   0x80000222  1      0x00AE52
```

Related Commands

命令	Description
show ipv6 ospf	显示 OSPFv3 路由流程中的所有 IPv6 设置。
show ipv6 ospf border-routers	显示区域边界路由器(ABR)和自主系统边界路由器(ASBR)的内部OSPFv3路由表条目。

show ipv6 ospf statistic

使用 **show ipv6 ospf statistic** 命令以显示各种 OSPFv3 统计信息，例如 SPF 的执行次数、原因和持续时间。

show ipv6 ospf ［*process_id*］ **statistic** ［**detail**］

Syntax Description

detail	（可选）指定详细 SPF 信息，包括触发点。
process_id	（可选）指定本地分配的内部ID，可以是任何正整数。启用OSPF路由流程时，此 ID 是管理性分配的号码。

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show ipv6 ospf statistic** 命令的输出示例：

```
> show ipv6 ospf 10 statistic detail
Area 10: SPF algorithm executed 6 times

SPF 1 executed 04:36:56 ago, SPF type Full
  SPF calculation time (in msec):
  SPT    Prefix D-Int  Sum    D-Sum  Ext    D-Ext  Total
       0      0      0      0      0      0      0 0
  RIB manipulation time (in msec):
  RIB Update    RIB Delete
                0             0
  LSIDs processed R:1 N:0 Prefix:0 SN:0 SA:0 X7:0
  Change record R L
  LSAs changed 2
  Changed LSAs. Recorded is Advertising Router, LSID and LS type:
  49.100.168.192/0(R) 49.100.168.192/2(L)

SPF 2 executed 04:35:50 ago, SPF type Full
  SPF calculation time (in msec):
  SPT    Prefix D-Int  Sum    D-Sum  Ext    D-Ext  Total
       0      0      0      0      0      0      0 0
  RIB manipulation time (in msec):
  RIB Update    RIB Delete
                0             0
  LSIDs processed R:2 N:1 Prefix:0 SN:0 SA:0 X7:0
  Change record R N L
  LSAs changed 5
  Changed LSAs. Recorded is Advertising Router, LSID and LS type:
  50.100.168.192/0(R) 50.100.168.192/2(L) 49.100.168.192/0(R) 50.100.168.192/0(R)
  50.100.168.192/2(N)
```

show ipv6 ospf summary-prefix

要显示在 OSPFv3 流程下配置的所有汇总地址重新分发信息的列表，请使用 **show ipv6 ospf summary-prefix** 命令。

show ipv6 ospf ［*process_id*］ **summary-prefix**

Syntax Description

process_id	（可选）指定本地分配的内部ID，可以是任何正整数。启用OSPF路由流程时，此 ID 是管理性分配的号码。

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show ipv6 ospf summary-prefix** 命令的输出示例：

```
> show ipv6 ospf summary-prefix

OSPFv3 Process 1, Summary-prefix

FEC0::/24 Metric 16777215, Type 0, Tag 0
```

Related Commands

命令	Description
show ipv6 ospf	显示 OSPFv3 路由流程中的所有 IPv6 设置。
show ipv6 ospf border-routers	显示区域边界路由器(ABR)和自主系统边界路由器(ASBR)的内部OSPFv3路由表条目。

show ipv6 ospf timers

要显示 OSPFv3 计时器信息，请使用 **show ipv6 ospf timers** 命令。

show ipv6 ospf ［*process_id*］ **timers** ［**lsa-group** | **rate-limit**］

Syntax Description

lsa-group	（可选）指定 OSPFv3 LSA 组信息。
process_id	（可选）指定本地分配的内部ID，可以是任何正整数。启用OSPF路由流程时，此 ID 是管理性分配的号码。
rate-limit	（可选）指定 OSPFv3 LSA 速率限制信息。

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show ipv6 ospf timers lsa-group** 命令的输出示例：

```
> show ipv6 ospf timers lsa-group

OSPFv3 Router with ID (10.10.13.101) (Process ID 1)

Group size 5, Head 2, Search Index 4, Interval 240 sec
Next update due in 0:00:13
Current time 96532
Index 0 Timestamp 96546
Index 1 Timestamp 96788
Index 2 Timestamp 97048
Index 3 Timestamp 97293
Index 4 Timestamp 97548

Failure Head 0, Last 0 LSA group failure logged

            OSPFv3 Router with ID (10.10.10.102) (Process ID 5709)

Group size 5, Head 2, Search Index 4, Interval 240 sec
Next update due in 0:00:22
Current time 96532
Index 0 Timestamp 96555
Index 1 Timestamp 96801
Index 2 Timestamp 97041
Index 3 Timestamp 97287
Index 4 Timestamp 97546

Failure Head 0, Last 0 LSA group failure logged
```

show ipv6 ospf traffic

要显示当前可用接口的 OSPFv3 流量相关统计信息，请使用 **show ipv6 ospf traffic** 命令。

show ipv6 ospf ［*process_id*］ **traffic** ［*interface_name*］

Syntax Description

interface_name	（可选）指定接口名称。使用此选项将流量隔离至特定接口。
process_id	（可选）指定本地分配的内部ID，可以是任何正整数。启用OSPF路由流程时，此 ID 是管理性分配的号码。

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show ipv6 ospf traffic** 命令的输出示例：

```
> show ipv6 ospf 10 traffic inside
Interface inside

Last clearing of interface traffic counters never

OSPFv3 packets received/sent
  Type          Packets               Bytes
  RX Invalid                      0 0
  RX Hello                     1232 53132
  RX DB des                      27 896
  RX LS req                       3 216
  RX LS upd                      28 2436
  RX LS ack                      14 1064
  RX Total                     1304 57744

  TX Failed                       0 0
  TX Hello                      753 32072
  TX DB des                      27 1056
  TX LS req                       2 92
  TX LS upd                       9 1128
  TX LS ack                      15 900
  TX Total                      806 35248
```

Related Commands

命令	Description
show ipv6 ospf	显示 OSPFv3 路由流程中的所有 IPv6 设置。
show ipv6 ospf border-routers	显示区域边界路由器(ABR)和自主系统边界路由器(ASBR)的内部OSPFv3路由表条目。

show ipv6 ospf virtual-links

要显示 OSPFv3 虚拟链路的参数和当前状态，请使用 **show ipv6 ospf virtual-links** 命令。

show ipv6 ospf virtual-links

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show ipv6 ospf virtual-links** 命令的输出示例：

```
> show ipv6 ospf virtual-links

Virtual Link OSPF_VL0 to router 172.16.6.6 is up
  Interface ID 27, IPv6 address FEC0:6666:6666::
  Run as demand circuit
  DoNotAge LSA allowed.
  Transit area 2, via interface ATM3/0, Cost of using 1
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
```

Related Commands

命令	Description
show ipv6 ospf	显示 OSPFv3 路由流程中的所有 IPv6 设置。
show ipv6 ospf border-routers	显示区域边界路由器 (ABR) 和自主系统边界路由器 (ASBR) 的内部 OSPFv3 路由表条目。

show ipv6 prefix-list

要列出配置为匹配 IPv6 流量的前缀列表，请使用 **show ipv6 prefix-list** 命令。

show ipv6 prefix-list ［**detail** | **summary**］［*prefix_list_name* ［**seq** *sequence_number* | *network/length* ［**longer** | **first-match**］］］

Syntax Description

detail	显示有关前缀列表的详细信息。
summary	显示前缀列表摘要。
prefix_list_name	前缀列表的名称。
seq *sequence-number*	（可选）仅显示指定前缀列表中具有指定序列号的前缀列表条目。
network/length [**longer** | **first-match**]	（可选）显示使用此网络地址和前缀长度（以位为单位）的指定前缀列表中的所有条目。 您可以选择包含以下关键字之一： • **longer** 显示与给定 network/length 匹配或比其更具体的指定前缀列表的所有条目。 • **first-match** 显示与给定 network/length 匹配的指定前缀列表的第一个条目。

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show ipv6 prefix-list** 命令的输出示例。

```
> show ipv6 prefix-list
ipv6 prefix-list test-ipv6-prefix: 1 entries
   seq 5 permit 2001:db8:0:cd30::/64
```

以下是汇总输出的示例。

```
> show ipv6 prefix-list summary
Prefix-list with the last deletion/insertion: test-ipv6-prefix
ipv6 prefix-list test-ipv6-prefix:   count: 1, range entries: 0,
sequences: 5 - 5, refcount: 2
```

以下是详细输出示例。

```
> show ipv6 prefix-list detail
Prefix-list with the last deletion/insertion: test-ipv6-prefix
ipv6 prefix-list test-ipv6-prefix:   count: 1, range entries: 0,
sequences: 5 - 5, refcount: 2
```

Related Commands

命令	Description
clear ipv6 prefix-list	重置 IPv6 前缀列表的命中计数。
show bgp prefix-list	显示在边界网关协议情景下有关前缀列表或前缀列表条目的信息。
show prefix-list	显示有关 IPv4 前缀列表的信息。

show ipv6 route

要显示 IPv6 路由表的内容，请使用 **show ipv6 route** 命令。

show ipv6 route ［**vrf** *name* | **all**］ ［**management-only**］［**failover**］［**cluster**］［**interface** *name*］［**ospf**］［**summary**］

Syntax Description

managment-only	显示 IPv6 管理路由表中的路由。
cluster	（可选）显示集群中的IPv6路由表序号、IPv6重新收敛计时器状态和IPv6路由条目序号。
failover	（可选）显示 IPv6 路由表序号、IPv6 重新收敛计时器状态和 IPv6 路由条目序号。
interface *name*	（可选）显示 IPv6 接口特定的路由。
ospf	（可选）显示 OSPFv3 路由。
summary	（可选）显示 IPv6 路由汇总。
［**vrf** *name*	**all**］	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将视图限制为特定虚拟路由器。如果要查看所有虚拟路由器的路由表，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则命令会显示全局 VRF 虚拟路由器的路由表。

Command History

版本	修改
6.1	引入了此命令。
6.6	添加了 ［**vrf** *name*	**all**］ 关键字。

使用指南

show ipv6 route 命令的输出类似于 **show route** 命令的输出，唯一不同之处是，前者显示的信息是 IPv6 特定信息。

以下信息出现在 IPv6 路由表中：

- 代码 - 指示派生路由的协议。值如下所示：
  - C - 连接
  - L - 本地
  - S - 静态
  - R - 派生的 RIP
  - B - 派生的 BGP

- I1 - ISIS L1 - 派生的集成 IS-IS 级别 1
- I2 - ISIS L2 - 派生的集成 IS-IS 级别 2
- IA - ISIS interarea - 派生的集成 ISIS interarea

- fe80::/10 - 指示远程网络的 IPv6 前缀。
- [0/0] - 中括号中的第一个数字是信息源的管理距离；第二个数字是路由的指标。
- via :: - 指定到远程网络的下一个路由器的地址。
- inside - 指定可到达所指定网络的下一个路由器所使用的接口。

示例

以下是 **show ipv6 route** 命令的输出示例：

```
> show ipv6 route

IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
L   fe80::/10 [0/0]
     via ::, inside
     via ::, vlan101
L   fec0::a:0:0:a0a:a70/128 [0/0]
     via ::, inside
C   fec0:0:0:a::/64 [0/0]
     via ::, inside
L   fec0::65:0:0:a0a:6570/128 [0/0]
     via ::, vlan101
C   fec0:0:0:65::/64 [0/0]
     via ::, vlan101
L   ff00::/8 [0/0]
     via ::, inside
     via ::, vlan101
S   ::/0 [0/0]
     via fec0::65:0:0:a0a:6575, vlan101
```

以下是 **show ipv6 route failover** 命令的输出示例：

```
> show ipv6 route failover

IPv6 Routing Table - 6 entries
Codes: C - Connected, L - Local, S - Static
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
           ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
IPv6 Routing table seq num 0
IPv6 Reconvergence timer expired

O   2009::1/128 [110/10]
     via fe80::217:94ff:fe85:4401, inside seq 0
OE2  2011::/64 [110/20]
     via fe80::217:94ff:fe85:4401, inside seq 0
```

```
S   4001::1/128 [0/0]
     via 4001::2, inside seq 0
C   7001::1/128 [0/0]
     via ::, outside seq 0
L   fe80::/10 [0/0]
     via ::, inside seq 0
     via ::, outside seq 0
L   ff00::/8 [0/0]
     via ::, inside seq 0
     via ::, outside seq 0
```

以下是主设备上 s**how ipv6 route cluster** 命令的输出示例：

```
> show ipv6 route cluster

IPv6 Routing Table - 5 entries
Codes: C - Connected, L - Local, S - Static
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
            ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
IPv6 Routing table seq num 2
IPv6 Reconvergence timer expired

OE2  2001::/58 [110/20]
     via fe80::21f:9eff:fe2a:78ba, inside seq 2
...
```

以下是角色更改期间辅助设备上 **show ipv6 route cluster** 命令的输出示例：

```
> cluster master
INFO: Wait for existing master to quit. Use "show cluster info"
to check status. Use "cluster remove unit <name>" to force
master unit out of the cluster if for some reason it refuses
to quit within reasonable time
> show ipv6 route cluster

IPv6 Routing Table - 5 entries
Codes: C - Connected, L - Local, S - Static
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
            ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
IPv6 Routing table seq num 3
IPv6 Reconvergence timer expires in 61 secs

OE2  2001::/58 [110/20]
     via fe80::21f:9eff:fe2a:78ba, inside seq 2
...
```

以下示例显示名为 red 的虚拟路由器的路由。请注意，泄漏到其他虚拟路由器的静态路由使用密钥 SI 表示。

```
> show ipv6 route vrf red

Codes: C - Connected, L - Local, S - Static, SI - Static InterVRF
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
            ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, B - BGP, V - VPN
            I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary

IPv6 Routing Table : red - 5 entries
L   2301::/128 [0/0]
     via ::, gig0
C   2301::/64 [0/0]
```

```
     via ::, gig0
SI  2304::/64 [1/0]
     via ::, gig3
L   fe80::/10 [0/0]
     via ::, gig0
L   ff00::/8 [0/0]
     via ::, gig0
```

Related Commands

命令	Description
show route	显示 IPv4 路由表。
show vrf	显示系统上的虚拟路由器。

show ipv6 routers

要显示从链路上的路由器接收的 IPv6 路由器通告信息，请使用 **show ipv6 routers** 命令。

show ipv6 routers ［*if_name*］

Syntax Description

if_name	（可选）要显示相关信息的内部或外部接口名称。

Command History

版本	修改
6.1	引入了此命令。

使用指南

当未指定接口名称时，会显示所有 IPv6 接口的信息。指定接口名称则会显示有关指定接口的信息。

示例

以下是输入时没有接口名称的 **show ipv6 routers** 命令的输出示例：

```
> show ipv6 routers
Router FE80::83B3:60A4 on outside, last update 3 min
  Hops 0, Lifetime 6000 sec, AddrFlag=0, OtherFlag=0
  Reachable time 0 msec, Retransmit time 0 msec
  Prefix 3FFE:C00:8007::800:207C:4E37/96 autoconfig
    Valid lifetime -1, preferred lifetime -1
Router FE80::290:27FF:FE8C:B709 on inside, last update 0 min
  Hops 64, Lifetime 1800 sec, AddrFlag=0, OtherFlag=0
  Reachable time 0 msec, Retransmit time 0 msec
```

Related Commands

命令	Description
ipv6 route	将静态条目添加至 IPv6 路由表。

show ipv6 traffic

要显示有关 IPv6 流量的统计信息，请使用 **show ipv6 traffic** 命令。

show ipv6 traffic

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用 **clear ipv6 traffic** 命令清除流量计数器。

示例

以下是 **show ipv6 traffic** 命令的输出示例：

```
> show ipv6 traffic
IPv6 statistics:
  Rcvd:  545 total, 545 local destination
         0 source-routed, 0 truncated
         0 format errors, 0 hop count exceeded
         0 bad header, 0 unknown option, 0 bad source
         0 unknown protocol, 0 not a router
         218 fragments, 109 total reassembled
         0 reassembly timeouts, 0 reassembly failures
  Sent:  228 generated, 0 forwarded
         1 fragmented into 2 fragments, 0 failed
         0 encapsulation failed, 0 no route, 0 too big
  Mcast: 168 received, 70 sent

ICMP statistics:
  Rcvd: 116 input, 0 checksum errors, 0 too short
        0 unknown info type, 0 unknown error type
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 60 router advert, 0 redirects
        31 neighbor solicit, 25 neighbor advert
  Sent: 85 output, 0 rate-limited
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 18 router advert, 0 redirects
        33 neighbor solicit, 34 neighbor advert

UDP statistics:
  Rcvd: 109 input, 0 checksum errors, 0 length errors
        0 no port, 0 dropped
  Sent: 37 output

TCP statistics:
```

```
Rcvd: 85 input, 0 checksum errors
Sent: 103 output, 0 retransmitted
```

Related Commands

命令	Description
clear ipv6 traffic	清除 IPv6 流量计数器。

show isakmp sa

要显示 IKE 运行时间 SA 数据库，请使用 **show isakmp sa** 命令。

show isakmp sa ［**detail**］

Syntax Description

detail	显示关于 SA 数据库的详细输出。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例显示有关 SA 数据库的详细信息：

```
> show isakmp sa detail

IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
1 209.165.200.225 User  Resp  No   AM_Active  3des    SHA   preshrd 86400

IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
2 209.165.200.226 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
3 209.165.200.227 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
4 209.165.200.228 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400
```

Related Commands

命令	Description
clear isakmp sa	清除 IKE 运行时间 SA 数据库。
show running-config isakmp	显示所有活动的 ISAKMP 配置。

show isakmp stats

要显示运行时间统计信息，请使用 **show isakmp stats** 命令。

威胁防御

show isakmp stats

Command History

版本	修改
6.1	引入了此命令。

使用指南

每个计数器都映射到一个关联的 cikePhase1GW 计数器。有关每个计数器的详细信息，请参阅 CISCO-IPSEC-FLOW-MONITOR-MIB.my。

- 主用/备用隧道数 - cikePhase1GWActiveTunnels
- 先前隧道数 - cikePhase1GWPreviousTunnels
- 输入八位组 - cikePhase1GWInOctets
- 输入数据包数 - cikePhase1GWInPkts
- 输入丢弃数据包数 - cikePhase1GWInDropPkts
- 输入通知数 - cikePhase1GWInNotifys
- 输入 P2 交换数 - cikePhase1GWInP2Exchgs
- 输入 P2 交换无效次数 - cikePhase1GWInP2ExchgInvalids
- 输入 P2 交换拒绝次数 - cikePhase1GWInP2ExchgRejects
- 输入 P2 Sa 删除请求数 - cikePhase1GWInP2SaDelRequests
- 输出八位组 - cikePhase1GWOutOctets
- 输出数据包数 - cikePhase1GWOutPkts
- 输出丢弃数据包数 - cikePhase1GWOutDropPkts
- 输出通知数 - cikePhase1GWOutNotifys
- 输出 P2 交换数 - cikePhase1GWOutP2Exchgs
- 输出 P2 交换无效次数 - cikePhase1GWOutP2ExchgInvalids
- 输出 P2 交换拒绝次数 - cikePhase1GWOutP2ExchgRejects
- 输出 P2 Sa 删除请求数 - cikePhase1GWOutP2SaDelRequests
- 发起方隧道数 - cikePhase1GWInitTunnels
- 发起方失败次数 - cikePhase1GWInitTunnelFails

- 响应方失败次数 - cikePhase1GWRespTunnelFails
- 系统容量故障次数 - cikePhase1GWSysCapFails
- 验证失败次数 - cikePhase1GWAuthFails
- 解密失败次数 - cikePhase1GWDecryptFails
- 散列有效失败次数 - cikePhase1GWHashValidFails
- 无 Sa 故障次数 - cikePhase1GWNoSaFails

示例

以下示例显示 ISAKMP 统计信息：

```
> show isakmp stats
Global IKE Statistics
Active Tunnels: 132
Previous Tunnels: 132
In Octets: 195471
In Packets: 1854
In Drop Packets: 925
In Notifys: 0
In P2 Exchanges: 132
In P2 Exchange Invalids: 0
In P2 Exchange Rejects: 0
In P2 Sa Delete Requests: 0
Out Octets: 119029
Out Packets: 796
Out Drop Packets: 0
Out Notifys: 264
Out P2 Exchanges: 0
Out P2 Exchange Invalids: 0
Out P2 Exchange Rejects: 0
Out P2 Sa Delete Requests: 0
Initiator Tunnels: 0
Initiator Fails: 0
Responder Fails: 0
System Capacity Fails: 0
Auth Fails: 0
Decrypt Fails: 0
Hash Valid Fails: 0
No Sa Fails: 0
```

Related Commands

命令	Description
clear isakmp sa	清除 IKE 运行时间 SA 数据库。
show running-config isakmp	显示所有活动的 ISAKMP 配置。

show isis database

要显示 IS-IS 链路状态数据库，请使用 **show isis database** 命令。

show isis database ［{**detail** | **verbose**} ［**ip** ［**unicast**］ | **ipv6** ［**unicast**］］ ［**topology base**］］ ［**level-1** | **level-2**］

Syntax Description

level-1	（可选）显示级别 1 的 IS-IS 链路状态数据库。
level-2	（可选）显示级别 2 的 IS-IS 链路状态数据库。
ip	（可选）显示 IPv4 地址系列的 IS-IS 链路状态数据库
ipv6	（可选）显示 IPv6 地址系列的 IS-IS 链路状态数据库
detail	（可选）显示每个链路状态数据包 (LSP) 的内容。
verbose	（可选）显示有关中间 IS-IS 数据库的其他信息。
topology base	（可选）显示 MTR 拓扑。
unicast	（可选）显示单播地址系列。

Command History

版本	修改
6.3	引入了此命令。

使用指南

下表对此命令的输出进行了解释。

表 *43: IS-IS* 数据库输出中的字段

字段	Description
LSPID	链路状态数据包 (LSP) 标识符。前六个八位组构成发起 LSP 的路由器的系统 ID。 下一个八位组是伪节点 ID。当此字节为非零值时，LSP 描述来自系统的链路。当它为零时，LSP 是所谓的非伪节点 LSP。此机制类似于开放最短路径优先 (OSPF) 协议中的路由器链路状态通告 (LSA)。LSP 将描述始发路由器的状态。 对于每个 LAN，该 LAN 的指定路由器将创建并泛洪伪节点 LSP，描述连接到该 LAN 的所有系统。 最后一个八位组是 LSP 编号。如果数据超过单个 LSP 的容量，LSP 将被划分为多个 LSP 分段。每个分段将具有不同的 LSP 编号。星号 (*) 表示 LSP 是由发出此命令的系统发起的。
LSP Seq Num	LSP 的序列号，允许其他系统确定它们是否已收到来自源的最新信息。

字段	Description
LSP Checksum	整个 LSP 数据包的校验和。
LSP Holdtime	LSP 保持有效的时间（以秒为单位）。LSP 保持时间为 0 表示此 LSP 已清除，并正在从所有路由器的链路状态数据库 (LSDB) 中删除。该值表示被清除的 LSP 在被完全删除之前将在 LSDB 中保留多长时间。
ATT	附加位。此位表示路由器也是第 2 级路由器，可以到达其他区域。仅 1 级路由器和与其他 2 级路由器失去连接的 1-2 级路由器将使用“连接”位来查找最近的 2 级路由器。它们会将默认路由指向最近的 2 级路由器。
P	P 位。检测中间系统是否支持区域分区修复。Cisco 和其他供应商不支持区域分区修复。
OL-	超载位。确定 IS 是否拥塞。如果设置了过载位，则其他路由器在计算路由器时不会将此系统用作中转路由器。只有目的地直接连接到过载路由器的数据包才会发送到此路由器。
Area Address (Detail and Verbose output only.)	可从路由器访问的区域地址。对于 1 级 LSP，这些是在源路由器上手动配置的区域地址。对于 2 级 LSP，这些是此路由器所属区域的所有区域地址。
NLPID (Detail and Verbose output only.)	网络层协议标识符。
Hostname (Detail and Verbose output only.)	节点的主机名。
Router ID (Detail and Verbose output only.)	节点的流量工程路由器标识符。
IP Address (Detail and Verbose output only.)	接口的 IPv4 地址。
Metric (Detail and Verbose output only.)	源路由器与通告邻居之间的邻接开销的 IS-IS 度量，或从通告路由器到通告目的地（可以是 IP 地址、终端系统 (ES)、或无连接网络服务 [CLNS] 前缀）。
Affinity （仅限 Verbose 输出。）	被泛洪的链路属性标志。

字段	Description
Physical BW （仅限 Verbose 输出。）	链路带宽容量（以位/秒为单位）。
Reservable BW （仅限 Verbose 输出。）	此链路上的可预留带宽量。
BW Unreserved （仅限 Verbose 输出。）	可用于预留的带宽量。

示例

以下示例显示 IS-IS 数据库。

```
> show isis database

IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
c1.00-00              0xea19d300     0x3d0d              674                0/0/0
routerA.00-00     0x1b541556     0xa349              928                0/0/0
c3.00-00              0x9257c979     0x9952              759                0/0/0
c2.00-00             *0xef11e977     0x3188              489                0/0/0
c2.01-00             *0xa8333f03     0xd6ea              829                0/0/0
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
c1.00-00              0x63871f24      0xaba2              526                0/0/0
routerA.00-00     0x0d540b55      0x81d7              472                0/0/0
routerA.00-01     0xffffff01          0xe20b              677                0/0/0
c3.00-00              0x002e5434      0xb20a              487                0/0/0
c2.00-00             *0x74fd1227      0xbb0f              742                0/0/0
c2.01-00             *0x7ee72c1a      0xb506              968                0/0/0
```

以下示例显示 IS-IS 数据库的详细输出。详细输出显示每个 LSP 的内容。

```
> show isis database detail

IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
c1.00-00              0xea19d301      0x3b0e              1189               0/0/0
  Area Address: 49.0001
  NLPID:        0xcc
  Hostname: c1
  IP Address:   10.22.22.1
  Metric:         10 IP 10.22.22.0 255.255.255.0
  Metric:         10 IS c2.01
routerA.00-00      0x1b541556     0xa349              642                0/0/0
  Area Address: 49.0001
  NLPID:        0xcc
  Hostname: routerA
  IP Address:   10.22.22.5
```

```
  Metric:         10 IP 10.22.22.0 255.255.255.0
  Metric:         10 IS c2.01
```

以下示例仅显示级别 2 LSP 的详细输出。区域地址 39.0001 是路由器所在区域的地址。

```
> show isis database 12 detail

IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
c1.00-00              0x63871f25      0xa9a3              1076                     0/0/0
  Area Address: 49.0001
  NLPID:        0xcc
  Hostname: c1
  IP Address:   10.22.22.1
  Metric:         10 IS c2.01
routerA.00-00     0x0d540b56     0x7fd8                941                      0/0/0
  Area Address: 49.0001
  NLPID:        0xcc
  Hostname: routerA
  IP Address:   10.22.22.5
  Metric:         10 IS c2.01
  Metric:          0 IP-External 1.1.1.0 255.255.255.0
  Metric:          0 IP-External 2.1.1.0 255.255.255.0
  Metric:          0 IP-External 2.2.2.0 255.255.255.0
  Metric:          0 IP-External 3.1.1.0 255.255.255.0
```

以下示例显示了详细输出。

```
> show isis database verbose

IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
c1.00-00             *0xea19d301   0x3b0e        644               0/0/0
  Area Address: 49.0001
  NLPID:        0xcc
  Hostname: c1
  IP Address:   22.22.22.1
  Metric:         10 IP 22.22.22.0 255.255.255.0
  Metric:         10 IS c2.01
routerA.00-00         0x1b541557   0xa14a        783               0/0/0
  Area Address: 49.0001
  NLPID:        0xcc
  Hostname: routerA
  IP Address:   22.22.22.5
  Metric:         10 IP 22.22.22.0 255.255.255.0
  Metric:         10 IS c2.01
```

Related Commands

命令	Description
clear isis	清除 IS-IS 数据结构。
show clns	显示 CLNS 特定信息。
show route isis	显示 IS-IS 路由。

show isis hostname

要显示 IS-IS 路由器的路由器名称到系统 ID 映射表条目，请使用 **show isis hostname** 命令。

show isis hostname

Command History

版本	修改
6.3	引入了此命令。

使用指南

在 IS-IS 路由域中，使用系统 ID 代表每个路由器。系统 ID 是为每个 IS-IS 路由器配置的网络实体名称 (NET) 的一部分。例如，NET 配置为 49.0001.0023.0003.000a.00 的路由器的系统 ID 为 0023.0003.000a。对于网络管理员而言，在路由器上进行维护以及故障排除期间，很难记住路由器名称与系统 ID 的映射。输入 **show isis hostname** 命令可显示路由器名称与系统 ID 映射表中的条目。

示例

以下示例显示动态主机映射表。动态主机映射表显示思科threat defense、c2、c3 和名为 routerA 的本地路由器的路由器名称到系统 ID 的映射表条目。该表还显示，c3 是级别 1 路由器，其主机名由级别 1 (L1) 链路状态协议 (LSP) 通告。C2 是第 2 层路由器，其主机名由 L2 LSP 通告。思科threat defense 的“级别”下显示的 * 符号表示这是系统的路由器名称到系统 ID 的映射信息。

```
> show isis hostname

Level  System ID       Dynamic Hostname  (c1)
     * 0050.0500.5005   ciscoASA
    1  0050.0500.5007   c3
    2  0050.0500.5006   routerA
    2  0050.0500.5008   c2
```

Related Commands

命令	Description
clear isis	清除 IS-IS 数据结构。
show clns	显示 CLNS 特定信息。
show route isis	显示 IS-IS 路由。

show isis lsp-log

要显示触发新链路状态数据包 (LSP) 的接口的第 1 级和第 2 级 IS-IS LSP 日志，请使用 **show isis lsp-log** 命令。

show isis lsp-log

Command History

版本	修改
6.3	引入了此命令。

使用指南

使用此命令以要显示触发新链路状态数据包 (LSP) 的接口的第 1 级和第 2 级 IS-IS LSP 日志。输出包括以下信息：

- 时间 - 自生成 LSP 以来经过的时间。
- 计数 - 此时发生的事件数。
- 接口 - 导致 LSP 重新生成的接口。
- 触发器 - 触发 LSP 泛洪的事件。LSP 的可能触发器如下：
  - AREASET - 活动区域集已更改。
  - ATTACHFLAG - 附加位更改状态。
  - CLEAR - 发出了某种形式的手动清除命令。
  - CONFIG - 任何配置更改。
  - DELADJ - 邻接关系关闭。
  - DIS - DIS 已更改或伪节点已更改。
  - ES - 终端系统邻接关系已更改。
  - HIPPITY — LSPDB 过载位已更改状态。
  - IF_DOWN - 需要新的 LSP。
  - IP_DEF_ORIG - 默认信息来源已更改。
  - IPDOWN - 直连 IP 前缀关闭。
  - IP_EXTERNAL - 重新分发的 IP 路由出现或消失。
  - IPIA - 区域间 IP 路由出现或消失。
  - IPUP - 直连 IP 前缀开启。
  - NEWADJ — 建立新的邻接关系。
  - REDIST — 已更改的 2 级 CLNS 路由已更改。

- RRR_INFO - RRR 带宽资源信息。

示例

以下是 **show isis lsp-log** 命令的输出示例：

```
> show isis lsp-log

  Level 1 LSP log
When       Count       Interface         Triggers
04:16:47     1         subint             CONFIG NEWADJ DIS
03:52:42     2         subint             NEWADJ DIS
03:52:12     1         subint             ATTACHFLAG
03:31:41     1         subint             IPUP
03:30:08     2         subint             CONFIG
03:29:38     1         subint             DELADJ
03:09:07     1         subint             DIS ES
02:34:37     2         subint             NEWADJ
02:34:07     1         subint             NEWADJ DIS

  Level 2 LSP log
When       Count       Interface         Triggers
03:09:27     1         subint             CONFIG NEWADJ
03:09:22     1         subint             NEWADJ
02:34:57     2         subint             DIS
02:34:50     1                                IPUP
02:34:27     1         subint             CONFIG DELADJ
02:13:57     1         subint             DELADJ
02:13:52     1         subint             NEWADJ
01:35:58     2         subint             IPIA
01:35:51     1                               AREASET IPIA
```

Related Commands

命令	Description
clear isis	清除 IS-IS 数据结构。
show clns	显示 CLNS 特定信息。
show route isis	显示 IS-IS 路由。

show isis neighbors

要显示有关 IS-IS 邻居的信息，请使用 **show isis neighbors** 命令：

show isis neighbors ［**detail**］

Syntax Description

detail	（可选）显示 IS-IS 邻居的更多详细信息。

Command History

版本	修改
6.3	引入了此命令。

使用指南

下表解释 IS-IS 邻居信息。

表 *44: IS-IS* 邻居信息

字段	Description
System Id	标识区域中的系统的六字节值。
Type	级别类型。指示 IS-IS 邻居是 1 级、1-2 级还是 2 级路由器。
Interface	从中获知系统的接口。
IP Address	邻居路由器的 IP 地址。
State	指示 IS-IS 邻居的状态是开启还是关闭。
Holdtime	链路状态数据包 (LSP) 保持时间。LSP 保持有效的时间（以秒为单位）。
Circuit Id	IS-IS 邻居路由器的端口位置，指示其如何连接到本地路由器。
Area Address(es)	可从路由器访问的区域地址。对于 1 级 LSP，这些是在源路由器上手动配置的区域地址。对于 2 级 LSP，这些是此路由器所属区域的所有区域地址。
SNPA	子网连接点。这是数据链路地址。
State Changed	状态更改的时间。
LAN Priority	LAN 的优先级。
Remote TID	邻居路由器拓扑 ID。
Local TID	本地路由器拓扑 ID。

示例

以下示例显示基本 IS-IS 邻居信息。

```
> show isis neighbors

System Id      Type Interface   IP Address      State Holdtime Circuit Id
routerA          L1    subint   10.22.22.5        UP    21          c2.01
routerA          L2    subint   10.22.22.5        UP    22          c2.01
c2               L1    subint   10.22.22.3        UP     9          c2.01
c2               L2    subint   10.22.22.3        UP     9          c2.01
```

以下示例显示了详细的 IS-IS 邻居信息。

```
> show isis neighbors detail

System Id      Type Interface   IP Address      State Holdtime Circuit Id
routerA          L1    subint   10.22.22.5        UP    23          c2.01
  Area Address(es): 49.0001
  SNPA:       0025.8407.f2b0
  State Changed: 00:03:03
  LAN Priority: 64
  Format: Phase V
  Remote TID: 0
  Local TID:  0
  Interface name: subint
routerA          L2    subint   10.22.22.5        UP    22         c2.01
  Area Address(es): 49.0001
  SNPA:       0025.8407.f2b0
  State Changed: 00:03:03
  LAN Priority: 64
  Format: Phase V
  Remote TID: 0
  Local TID:  0
  Interface name: subint
```

Related Commands

命令	Description
clear isis	清除 IS-IS 数据结构。
show clns	显示 CLNS 特定信息。
show route isis	显示 IS-IS 路由。

show isis rib

要显示存储在 IP 本地路由信息库 (RIB) 中的特定路由或主网络下所有路由的路径，请使用 **show isis rib** 命令。

show isis ［***** | **ip** ［**unicast**］ | **ipv6** ［**unicast**］］ **rib** ［**redistribution** ［**level-1** | **level-2**］］ ［*network_ip* ［*mask*］］

Syntax Description

*****	（可选）显示所有 IS-IS 地址系列。
ip	（可选）显示 IPv4 地址系列。
ipv6	（可选）显示 IPv6 地址系列。
level-1	（可选）显示 1 级重新分发 RIB。
level-2	（可选）显示第 2 级重新分发 RIB
network_ip [*mask*]	（可选）显示网络的 RIB 信息。
redistribution	（可选）显示 IS-IS IP 重新分发 RIB 信息
unicast	（可选）显示单播地址系列。

Command History

版本	修改
6.3	引入了此命令。

使用指南

使用此命令可验证 IP 全局 RIB 中存在的 IP 前缀更新是否也已在 IS-IS 本地 RIB 中更新。

示例

以下示例显示了存储在 IS-IS 本地 RIB 中的所有路由。

```
> show isis rib

IPv4 local RIB for IS-IS process

IPV4 unicast topology base (TID 0, TOPOID 0x2) = = = = = = = = = = = = = =

10.10.0.0 255.255.0.0
  [115/L2/10] via 10.22.22.5(subint), from 10.22.22.5, tag 0, LSP[12/524]


10.1.2.0 255.255.255.0
  [115/L2/10] via 10.22.22.5(subint), from 10.22.22.5, tag 0, LSP[12/524]


10.3.2.0 255.255.255.0
  [115/L2/10] via 10.22.22.5(subint), from 10.22.22.5, tag 0, LSP[13/149]
```

以下示例显示了主网络 10.0.0.0 下 IP 地址为 10.3.2.0 且存储在 IS-IS 本地 RIB 中的所有路由。

```
> show isis rib 10.3.2.0

IPv4 local RIB for IS-IS process

IPV4 unicast topology base (TID 0, TOPOID 0x2) = = = = = = = = = = = = =
Routes under majornet 10.0.0.0 255.0.0.0:

10.1.2.0 255.255.255.0
  [115/L2/10] via 10.22.22.5(subint), from 10.22.22.5, tag 0, LSP[12/524]


10.3.2.0 255.255.255.0
  [115/L2/10] via 10.22.22.5(subint), from 10.22.22.5, tag 0, LSP[13/149]
```

以下示例显示了在 IS-IS 本地 RIB 中存储的 IP 地址和掩码为 10.3.2.0 255.255.255.0 的网络下的所有路由。

```
> show isis rib 10.3.2.0 255.255.255.0

IPv4 local RIB for IS-IS process

IPV4 unicast topology base (TID 0, TOPOID 0x2) = = = = = = = = = = = = =

10.3.2.0 255.255.255.0
  [115/L2/10] via 10.22.22.5(subint), from 10.22.22.5, tag 0, LSP[13/149]
```

Related Commands

命令	Description
clear isis	清除 IS-IS 数据结构。
show clns	显示 CLNS 特定信息。
show route isis	显示 IS-IS 路由。

show isis spf-log

要显示路由器运行完整最短路径优先 (SPF) 计算的频率和原因，请使用 **show isis spf-log** 命令。

show isis ［***** | **ip** ［**unicast**］ | **ipv6** ［**unicast**］］ **spf-log**

Syntax Description

*****	（可选）显示所有 IS-IS 地址系列。
ip	（可选）显示 IPv4 地址系列。
ipv6	（可选）显示 IPv6 地址系列。
unicast	（可选）显示单播地址系列。

Command History

版本	修改
6.3	引入了此命令。

使用指南

此命令显示路由器运行完整最短路径优先 (SPF) 计算的频率和原因。下表对输出字段进行了解释。

字段	Description
When	多久前（小时：分钟：秒）进行了完整的 SPF 计算。记录最近 20 次发生的事件。
Duration	完成此SPF运行所需的毫秒数。已用时间是挂钟时间，而不是CPU时间。
Nodes	构成此 SPF 运行中计算的拓扑的路由器和伪节点 (LAN) 的数量。
Count	触发此SPF运行的事件数。当拓扑发生变化时，通常会在短时间内收到多个链路状态数据包 (LSP)。路由器在运行完整 SPF 之前会等待 5 秒，因此它可以包含所有新信息。此计数表示路由器在运行完整SPF之前等待5秒时发生的事件数（例如接收新的 LSP）。
First Trigger LSP	每当新 LSP 到达时触发完整的 SPF 计算，路由器就会存储 LSP ID。LSP ID 可以提供有关区域中路由不稳定来源的线索。如果多个 LSP 导致 SPF 运行，则仅记住最后接收的 LSP 的 LSP ID。
Triggers	触发完整 SPF 计算的所有原因的列表。有关触发器，请参阅下一个表。

下表解释了可能的触发器。

触发器	Description
ATTACHFLAG	此路由器现在已连接到第 2 级中枢，或者刚刚失去与第 2 级中枢的联系。
ADMINDIST	此路由器上为 IS-IS 流程配置了另一个管理距离。

触发器	Description
AREASET	此区域中的已获知区域地址集已更改。
BACKUPOVFL	IP 前缀消失。路由器知道有另一种方法可以到达该前缀，但尚未存储该备份路由。查找替代路由的唯一方法是通过完整的 SPF 运行。
DBCHANGED	**clear isis *** 命令在此路由器上发出。
IPBACKUP	IP 路由消失了，该路由不是通过 IS-IS 获知的，而是通过具有更好管理距离的另一个协议获知的。IS-IS 将运行完整的 SPF，为消失的 IP 前缀安装 IS-IS 路由。
IPQUERY	**clear ip route** 命令在此路由器上发出。
LSPEXPIRED	链路状态数据库 (LSDB) 中的某些 LSP 已过期。
LSPHEADER	LSP 信头中的 ATT/P/OL 位或 is-type 已更改。
NEWADJ	此路由器与另一台路由器建立了新的邻接关系。
NEWAREA	已在此路由器上配置新区域（通过网络实体标题 [NET]）。
NEWLEVEL	已在此路由器上配置新级别（通过 is-type）。
NEWLSP	拓扑中出现新的路由器或伪节点。
NEWMETRIC	在此路由器的接口上配置了新的度量。
NEWSYSID	已在此路由器上配置新的系统 ID（通过 NET）。
PERIODIC	通常，路由器每隔 15 分钟运行一次完整的 SPF 计算。
RTCLEARED	**clear clns route** 命令在此路由器上发出。
TLVCODE	TLV 代码不匹配，表示 LSP 的最新版本中包含不同的 TLV。
TLVCONTENT	TLV 内容已更改。这通常表示该区域中某处的邻接关系已建立或关闭。“第一个触发 LSP”列指示可能发生不稳定的位置。

示例

以下是 **show isis ipv6 spf-log** 命令的输出示例：

```
> show isis ipv6 spf-log

      TID 0 level 1 SPF log
  When   Duration  Nodes  Count     First trigger LSP   Triggers
00:15:46    3124     40      1          milles.00-00  TLVCODE
00:15:24    3216     41      5          milles.00-00  TLVCODE NEWLSP
00:15:19    3096     41      1          deurze.00-00  TLVCODE
00:14:54    3004     41      2          milles.00-00  ATTACHFLAG LSPHEADER
```

```
00:14:49    3384     41      1          milles.00-01  TLVCODE
00:14:23    2932     41      3          milles.00-00  TLVCODE
00:05:18    3140     41      1                        PERIODIC
00:03:54    3144     41      1          milles.01-00  TLVCODE
00:03:49    2908     41      1          milles.01-00  TLVCODE
00:03:28    3148     41      3           bakel.00-00  TLVCODE TLVCONTENT
00:03:15    3054     41      1          milles.00-00  TLVCODE
00:02:53    2958     41      1          mortel.00-00  TLVCODE
00:02:48    3632     41      2          milles.00-00  NEWADJ TLVCODE
00:02:23    2988     41      1          milles.00-01  TLVCODE
00:02:18    3016     41      1          gemert.00-00  TLVCODE
00:02:14    2932     41      1           bakel.00-00  TLVCONTENT
00:02:09    2988     41      2           bakel.00-00  TLVCONTENT
00:01:54    3228     41      1          milles.00-00  TLVCODE
00:01:38    3120     41      3            rips.03-00  TLVCONTENT
```

Related Commands

命令	Description
clear isis	清除 IS-IS 数据结构。
show clns	显示 CLNS 特定信息。
show route isis	显示 IS-IS 路由。

show isis topology

要显示所有区域中所有连接的路由器的列表，请使用 **show isis topology** 命令。

show isis ［***** | **ip** ［**unicast**］ | **ipv6** ［**unicast**］］ **topology** ［**level-1** | **level-2**］

Syntax Description

*****	（可选）显示所有 IS-IS 地址系列。
ip	（可选）显示 IPv4 地址系列。
ipv6	（可选）显示 IPv6 地址系列。
level-1	（可选）显示 1 级重新分发 RIB。
level-2	（可选）显示第 2 级重新分发 RIB
unicast	（可选）显示单播地址系列。

Command History

版本	修改
6.3	引入了此命令。

使用指南

使用 **show isis topology** 命令以验证所有区域中所有路由器的存在性及其连接性。在下表中对字段进行了说明。

字段	Description
System Id	标识区域中的系统的六字节值。
Metric	源路由器与通告邻居之间的邻接关系开销的 IS-IS 度量，或从通告路由器到通告目的地的开销度量（可以是 IP 地址、终端系统 [ES]、或 CLNS 前缀）。
Next-Hop	下一跳路由器的 IP 地址
Interface	从中获知系统的接口。
SNPA	子网连接点。这是数据链路地址。

示例

以下示例显示 **show isis topology** 命令的输出示例。

```
> show isis topology

IS-IS TID 0 paths to level-1 routers
System Id            Metric     Next-Hop             Interface   SNPA
cisco1                  --
```

```
routerA                 10       routerA                 subint  0025.8407.f2b0
c3                      10
c2                      10            c2                subint  c08c.60e6.986f

IS-IS TID 0 paths to level-2 routers
System Id            Metric     Next-Hop             Interface   SNPA
cisco1                  --
routerA                 10       routerA                 subint  0025.8407.f2b0
c3                      10
c2                      10            c2                subint  c08c.60e6.986f
```

Related Commands

命令	Description
clear isis	清除 IS-IS 数据结构。
show clns	显示 CLNS 特定信息。
show route isis	显示 IS-IS 路由。

show j - show o

show jumbo-frame reservation

要查看是否为所有接口启用巨帧，请使用 **show jumbo-frame reservation** 命令。

show jumbo-frame reservation

Command History

版本	修改
6.1	引入了此命令。

使用指南

只要将任何接口的 MTU 增加到 1500 以上，就会启用巨帧预留。当您将所有 MTU 恢复为 1500 或更低时，它会自动禁用。

示例

以下是启用巨帧支持时 **show jumbo-frame reservation** 命令的输出示例：

```
> show jumbo-frame-reservation
Jumbo Frame Support is currently enabled
```

show kernel

要显示 Linux brctl 实用程序提供的可用于调试的信息，请使用 **show kernel** 命令。

show kernel {**process** | **bridge** [**mac-address** *bridge_name*] | **cgroup-controller** [**cpu** | **cpuset** | **memory**] [**detail**] | **ifconfig** | **module**}

Syntax Description

bridge [**mac-address** *bridge_name*]	显示Linux tap网桥、其成员端口以及在每个端口获知的可用于调试的MAC地址（包括远程 MAC 地址）。可以使用 **mac-address** 关键字查看有关特定网桥的 MAC 地址详细信息。使用不带关键字的命令查看可用的网桥名称，例如 br0。
cgroup-controller [**cpu** | **cpuset** | **memory**] [**detail**]	显示 cgroup-controller 统计信息。 **cpu**、 **cpuset** 和 **memory** 关键字允许您根据要求过滤 cgroup-controller 统计信息。使用 detail 关键字可查看额外信息。
ifconfig	显示 tap 和网桥接口统计信息。
module	显示已安装并且正在运行的模块。
process	显示设备上运行的活动内核进程的当前状态。

Command History

版本	修改
6.1	引入了此命令。

使用指南

此命令显示内核中运行的各个进程的统计信息。

示例

以下示例显示 **show kernel process** 命令的输出：

```
> show kernel process
PID PPID PRI NI      VSIZE      RSS      WCHAN STAT  RUNTIME COMMAND
  1    0  16  0     991232      268 3725684979    S       78 init
  2    1  34 19          0        0 3725694381    S        0 ksoftirqd/0
  3    1  10 -5          0        0 3725736671    S        0 events/0
  4    1  20 -5          0        0 3725736671    S        0 khelper
  5    1  20 -5          0        0 3725736671    S        0 kthread
  7    5  10 -5          0        0 3725736671    S        0 kblockd/0
  8    5  20 -5          0        0 3726794334    S        0 kseriod
 66    5  20  0          0        0 3725811768    S        0 pdflush
 67    5  15  0          0        0 3725811768    S        0 pdflush
 68    1  15  0          0        0 3725824451    S        2 kswapd0
 69    5  20 -5          0        0 3725736671    S        0 aio/0
171    1  16  0     991232       80 3725684979    S        0 init
172  171  19  0     983040      268 3725684979    S        0 rcS
201  172  21  0    1351680      344 3725712932    S        0 lina_monitor
202  201  16  0 1017602048   899932 3725716348    S      212 lina
203  202  16  0 1017602048   899932          0    S        0 lina
```

```
204  203  15  0 1017602048   899932          0    S        0 lina
205  203  15  0 1017602048   899932 3725712932    S        6 lina
206  203  25  0 1017602048   899932          0    R 13069390 lina
>
```

下表对每个字段进行了说明。

表 *45: show kernel process* 字段

字段	Description
PID	进程 ID。
PPID	父进程 ID。
PRI	进程的优先级。
Nexus Dashboard Insights	友好值，用于优先级计算。值范围为 19（最友好）到 -19（对其他进程不友好）。
VSIZE	虚拟内存大小（以字节为单位）。
RSS	进程的驻留集大小（以千字节为单位）。
WCHAN	进程处于等待状态时所处的通道。
STAT	进程的状态： • R - 正在运行 • S - 在可中断等待状态下休眠 • D - 在不可中断磁盘休眠状态下等待 • Z - 僵停 • T - 跟踪或停止（基于信号） • P - 分页
运行时间	进程在用户模式和内核模式中已计划的节拍数。运行时是 utime 和 stime 的总和。
COMMAND	进程名。

以下示例显示 **show kernel module** 命令的输出：

```
> show kernel module

Module                  Size  Used by    Tainted: P
cpp_base              861808  2
kvm_intel              44104  8
kvm                   174304  1 kvm_intel
msrif                   4180  0
```

```
tscsync                 3852  0
```

以下示例显示 **show kernel ifconfig** 命令的输出：

```
> show kernel ifconfig

br0       Link encap:Ethernet  HWaddr 42:9E:B8:6C:1F:23
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:43 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1708 (1.6 KiB)  TX bytes:0 (0.0 B)

br1       Link encap:Ethernet  HWaddr 6A:03:EC:BA:89:26
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.255.255.255
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

tap0      Link encap:Ethernet  HWaddr 6A:0C:48:32:FE:F4
          inet addr:127.0.2.2  Bcast:127.255.255.255  Mask:255.0.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:148 errors:0 dropped:0 overruns:0 frame:0
          TX packets:186 errors:0 dropped:13 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:10320 (10.0 KiB)  TX bytes:12452 (12.1 KiB)

tap1      Link encap:Ethernet  HWaddr 8E:E7:61:CF:E9:BD
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:259 errors:0 dropped:0 overruns:0 frame:0
          TX packets:187 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:19368 (18.9 KiB)  TX bytes:14638 (14.2 KiB)

tap2      Link encap:Ethernet  HWaddr 6A:03:EC:BA:89:26
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

tap3      Link encap:Ethernet  HWaddr 42:9E:B8:6C:1F:23
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:187 errors:0 dropped:0 overruns:0 frame:0
          TX packets:256 errors:0 dropped:3 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:14638 (14.2 KiB)  TX bytes:19202 (18.7 KiB)

tap4      Link encap:Ethernet  HWaddr 6A:5C:60:BC:9C:ED
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
```

```
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

以下示例显示 **show kernel bridge** 命令的输出：

```
> show kernel bridge

bridge name     bridge id               STP enabled     interfaces
br0             8000.000000040001       no              tap1
                                                        tap3
br1             8000.84b261b192bd       no              tap2
                                                        tap4
                                                        tap5
```

以下示例显示 **show kernel bridge mac-address** 命令的输出：

```
> show kernel bridge mac-address br1

port no    mac addr       is local?   ageing timer
 1    00:21:d8:cb:dc:f7    no          12.93
 3    00:22:bd:d8:7d:da    no          12.93
 2    26:d2:9f:51:a4:90    yes          0.00
 1    4e:a4:e0:73:1f:ab    yes          0.00
 3    52:04:38:3d:79:c0    yes          0.00
```

Related Commands

命令	Description
show module	显示有关设备中安装的模块的信息。

show lacp

要显示流量统计信息、系统标识符和邻居详细信息等 EtherChannel LACP 信息，请输入此命令。

show lacp {*channel_group_number* {**counters** | **internal** [**detail**] | **neighbor** [**detail**]} | **neighbor** [**detail**] | **sys-id**}

Syntax Description

channel_group_number	指定 EtherChannel 通道组编号（介于 1 到 48 之间）并且仅显示有关此通道组的信息。
counters	显示用于已发送和接收的 LACPDU 和标记数量的计数器。
detail	显示项目的其他详细信息。
internal	显示内部信息。
neighbor	显示邻居信息。
sys-id	Shows the LACP system ID.

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show lacp sys-id** 命令的输出示例：

```
> show lacp sys-id
32768,001c.c4e5.cfee
```

以下是 **show lacp counters** 命令的输出示例：

```
> show lacp counters

              LACPDUs         Marker      Marker Response    LACPDUs
Port       Sent   Recv     Sent   Recv     Sent    Recv      Pkts Err
--------------------------------------------------------------------
Channel group: 1
Gi3/1      736    728      0      0        0       0         0
Gi3/2      739    730      0      0        0       0         0
Gi3/3      739    732      0      0        0       0         0
```

以下是 **show lacp internal** 命令的输出示例：

```
> show lacp internal

Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs
```

```
        A - Device is in Active mode       P - Device is in Passive mode

Channel group 1
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
--------------------------------------------------------------------------------
Gi3/1     SA      bndl      32768         0x1       0x1     0x302       0x3d
Gi3/2     SA      bndl      32768         0x1       0x1     0x303       0x3d
Gi3/3     SA      bndl      32768         0x1       0x1     0x304       0x3d
```

以下是 **show lacp neighbor** 命令的输出示例：

```
> show lacp neighbor

Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs
        A - Device is in Active mode       P - Device is in Passive mode

Channel group 1 neighbors

Partner's information:
          Partner Partner    LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State      Port Priority Admin Key Oper Key Port Number Port State
--------------------------------------------------------------------------------
Gi3/1     SA      bndl       32768         0x0       0x1      0x306       0x3d
Gi3/2     SA      bndl       32768         0x0       0x1      0x303       0x3d
Gi3/3     SA      bndl       32768         0x0       0x1      0x302       0x3d
```

Related Commands

命令	Description
show port-channel	在详细的单行摘要表单中显示 EtherChannel 信息。此命令还显示端口和端口信道信息。
show port-channel load-balance	显示端口通道负载均衡信息以及为给定的一组参数选择的散列结果和成员接口。

show lacp cluster

要显示 cLACP 系统 MAC 和 ID，请使用 **show lacp cluster** 命令

show lacp cluster {**system-mac** | **system-id**}

Syntax Description

system-mac	显示系统 ID 以及它是自动生成还是手动输入的。
system-id	显示系统 ID 和优先级。

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show lacp cluster system-mac** 命令的输出示例：

```
> show lacp cluster system-mac
lacp cluster system MAC is automatically generated: a300.010a.010a.
```

以下是 **show lacp cluster system-id** 命令的输出示例：

```
> show lacp cluster system-id
5    ,a300.010a.010a
```

show last-upgrade status

要显示有关上次系统软件升级的状态的信息，请使用 **show last-upgrade status** 命令。

show last-upgrade status

Command History

版本	修改
6.7	引入了此命令。

示例

以下示例显示上次升级成功。在实际输出中，xy0 将替换为实际版本号。

```
> show last-upgrade status
Upgrade from 6.7.0 to x.y.0 was successful.
Time started: Tue Dec  3 23:50:31 UTC 2020
```

以下示例显示上次升级已取消。在实际输出中，xy0 将替换为实际版本号。

```
> show last-upgrade status
Upgrade from 6.7.0 to x.y.0 failed.
Time started: Tue Dec  3 23:50:31 UTC 2020
Cancel Upgrade was successful.
```

Related Commands

命令	Description
show upgrade	显示有关当前系统软件升级的信息。
upgrade	取消、恢复或重试系统软件升级。

show lisp eid

要查看 EID 表，请使用 **show lisp eid** 命令。

show lisp eid ［**site-id** *ID*］

Syntax Description

site-id *id*	仅查看特定站点的 EID。

Command History

版本	修改
6.1	引入了此命令。

使用指南

设备维护着一个将 EID 和站点 ID 相关联的 EID 表。

示例

以下是 **show lisp eid** 命令的输出示例：

```
> show lisp eid
LISP EID       Site ID
10.44.33.105        2
10.44.33.201        2
192.168.11.1        4
192.168.11.2        4
```

Related Commands

命令	Description
clear cluster info flow-mobility counters	清除流移动性计数器。
clear lisp eid	从 ASA EID 表中删除 EID。
show cluster info flow-mobility counters	显示流移动性计数器。
show conn	显示受 LISP 流移动性影响的流量。
show service-policy	显示服务策略。

show lldp

要显示接口的链路层发现协议 (LLDP) 状态，请使用 **show lldp** 命令。

注释 LLDP 仅受 Firepower 1100 支持

show lldp { **neighbors** | **statistics** | **status** } *interface_id*

Syntax Description

interface_id	指定接口 ID。
neighbors	显示是否已建立 LLDP 邻居关系。
statistics	显示 LLDP 统计信息。
status	显示是否已启用 LLDP。

Command History

版本	修改
7.1	引入了此命令。

使用指南

如果 LLDP 处于活动状态，则 **通过** 字段显示；如果 LLDP 已禁用或不起作用，则显示未知。

示例

以下是 **show lldp neighbors** 命令的输出示例：

```
> show lldp neighbors

------------------------------------------------------------------------------
LLDP neighbors:
------------------------------------------------------------------------------
Interface: lldp-Eth1_6, via: LLDP, RID: 1, Time: 0 day, 00:00:18
  Chassis:
    ChassisID: mac 8c:60:4f:58:c1:ac
    SysName: ruintpo
    SysDescr: Cisco Nexus Operating System (NX OS) Software 7.0(1)N1(1)
 TAC support: http://www.cisco.com /tac
 Copyright (c) 2002-2014, Cisco Systems, Inc. All rights reserved.
    MgmtIP: 10.225.126.91
    Capability: Bridge, on
  Port:
    PortID: local Eth1/37
    PortDescr: Ethernet1/37
    TTL: 30
------------------------------------------------------------------------------
```

以下是 **show lldp statistics** 命令的输出示例：

```
> show lldp statistics interface Ethernet 1/6
------------------------------------------------------------------------------
LLDP statistics:
------------------------------------------------------------------------------
Interface: lldp-Eth1_6
  Transmitted: 115
  Received: 116
  Discarded: 0
  Unrecognized: 0
  Ageout: 0
  Inserted: 0
  Deleted: 0
------------------------------------------------------------------------------
```

以下是 **show lldp status** 命令的输出示例：

```
> show lldp status interface Ethernet 1/6
------------------------------------------------------------------------------
LLDP interfaces:
------------------------------------------------------------------------------
Interface: lldp-Eth1_6, via: unknown, Time: 18795 days, 05:38:39
  Chassis:
    ChassisID: mac 42:8f:14:a8:2f:c5
    SysName: firepower
    SysDescr: Cisco Firepower 1150 Threat Defense 7.1.0 1558
    MgmtIP: 127.128.254.1
    MgmtIP: fd00:0:0:1::3
    Capability: Bridge, on
    Capability: Router, off
    Capability: Wlan , off
    Capability: Station, off
  Port:
    PortID: mac 34:12:78:56:01:03
    PortDescr: Ethernet1/6
    TTL: 120
------------------------------------------------------------------------------
```

Related Commands

命令	Description
show interface	显示接口统计信息。

show local-host

要显示本地主机的网络状态，请使用 **show local-host** 命令。

show local-host ［*hostname* | *ip_address*］［**detail**］［**all**］［**brief**］［**connection** {**sctp** | **tcp** | **udp** | **embryonic**} *start*［*-end*］］［**zone**］

Syntax Description

all	（已弃用） 包括连接到设备和从设备连接的本地主机。
brief	（可选）显示有关本地主机的简要信息。
connection {**sctp** | **tcp** | **udp** | **embryonic**} *start*[*-end*]	（已弃用） 根据连接的数量和类型应用过滤器：初期、TCP、UDP 或 SCTP。起始编号表示该类型的最小连接数。包括 -end 数字以指定范围，例如 10-100。这些过滤器可以单独使用也可以联合使用。
detail	（可选）显示本地主机信息的详细网络状态，包括有关活动 xlate 和网络连接的详细信息。
hostname | *ip_address*	（可选）指定本地主机名或 IPv4/IPv6 地址。
zone	（可选）指定每个区域或内联集的本地主机。

Command History

版本	修改
6.1	引入了此命令。
7.0	以下关键字已弃用： **all**、 **connection**。

使用指南

要显示本地主机的网络状态，请使用 **show local-host** 命令。对于任何将流量转发到 threat defense 设备或通过其转发流量的主机，将为其创建一个本地主机。

对于运行 7.0 及更高版本的系统，请考虑使用 **show conn address** 命令而不是此命令。

此命令可显示本地主机的转换和连接插槽。转换信息包括分配给主机的任何 PAT 端口块。

此命令还显示连接限制值。如果未设置连接限制，值将显示为 0 并且不应用限制。

发生 SYN 攻击（已配置 TCP 拦截）时， **show local-host** 命令输出将已拦截连接数包括在使用计数中。此字段通常仅显示完全开放的连接。

在 **show local-host** 命令输出中，为使用静态连接的主机配置了最大初期限制（TCP 拦截水印）时使用 **TCP embryonic count to host counter** 。此计数器显示从其他主机到该主机的初期连接总数。如果此总数超过配置的最大限制，将对到主机的新连接应用 TCP 拦截。

示例

以下是 **show local-host** 命令的输出示例：

```
> show local-host

Interface mgmt: 2 active, 2 maximum active, 0 denied
local host: <10.24.250.191>,
    SCTP flow count/limit = 0/unlimited
    TCP flow count/limit = 1/unlimited
    TCP embryonic count to host = 0
    TCP intercept watermark = unlimited
    UDP flow count/limit = 0/unlimited
local host: <10.44.64.65>,
    SCTP flow count/limit = 0/unlimited
    TCP flow count/limit = 1/unlimited
    TCP embryonic count to host = 1
    TCP intercept watermark = unlimited
    UDP flow count/limit = 5/unlimited
Interface inside: 0 active, 0 maximum active, 0 denied
Interface outside: 0 active, 0 maximum active, 0 denied
Interface any: 0 active, 0 maximum active, 0 denied
```

以下示例展示本地主机的网络状态：

```
> show local-host all

Interface outside: 1 active, 2 maximum active, 0 denied
local host: <11.0.0.4>,
SCTP flow count/limit = 0/unlimited
TCP flow count/limit = 0/unlimited
TCP embryonic count to host = 0
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited
Conn:
105 out 11.0.0.4 in 11.0.0.3 idle 0:01:42 bytes 4464
105 out 11.0.0.4 in 11.0.0.3 idle 0:01:44 bytes 4464
Interface inside: 1 active, 2 maximum active, 0 denied
local host: <17.3.8.2>,
SCTP flow count/limit = 0/unlimited
TCP flow count/limit = 0/unlimited
TCP embryonic count to host = 0
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited
Conn:
105 out 17.3.8.2 in 17.3.8.1 idle 0:01:42 bytes 4464
105 out 17.3.8.2 in 17.3.8.1 idle 0:01:44 bytes 4464
Interface NP Identity Ifc: 2 active, 4 maximum active, 0 denied
local host: <11.0.0.3>,
SCTP flow count/limit = 0/unlimited
TCP flow count/limit = 0/unlimited
TCP embryonic count to host = 0
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited
Conn:
105 out 11.0.0.4 in 11.0.0.3 idle 0:01:44 bytes 4464
105 out 11.0.0.4 in 11.0.0.3 idle 0:01:42 bytes 4464
local host: <17.3.8.1>,
SCTP flow count/limit = 0/unlimited
TCP flow count/limit = 0/unlimited
TCP embryonic count to host = 0
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited
Conn:
105 out 17.3.8.2 in 17.3.8.1 idle 0:01:44 bytes 4464
```

```
105 out 17.3.8.2 in 17.3.8.1 idle 0:01:42 bytes 4464
```

以下示例显示有关特定主机的信息，后跟该主机的详细信息。

```
> show local-host 10.1.1.91
Interface third: 0 active, 0 maximum active, 0 denied
Interface inside: 1 active, 1 maximum active, 0 denied
local host: <10.1.1.91>,
SCTP flow count/limit = 0/unlimited
TCP flow count/limit = 1/unlimited
TCP embryonic count to (from) host = 0 (0)
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited

Xlate:
PAT Global 192.150.49.1(1024) Local 10.1.1.91(4984)

Conn:
TCP out 192.150.49.10:21 in 10.1.1.91:4984 idle 0:00:07 bytes 75 flags UI Interface
outside: 1 active, 1 maximum active, 0 denied

> show local-host 10.1.1.91 detail
Interface third: 0 active, 0 maximum active, 0 denied
Interface inside: 1 active, 1 maximum active, 0 denied
local host: <10.1.1.91>,
SCTP flow count/limit = 0/unlimited
TCP flow count/limit = 1/unlimited
TCP embryonic count to (from) host = 0 (0)
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited

Xlate:
TCP PAT from inside:10.1.1.91/4984 to outside:192.150.49.1/1024 flags ri

Conn:
TCP outside:192.150.49.10/21 inside:10.1.1.91/4984 flags UI Interface outside: 1 active,
1 maximum active, 0 denied
```

以下示例展示具有至少 4 个 UDP 连接以及同时具有 1 到 10 个 TCP 连接的所有主机：

```
> show local-host connection udp 4 tcp 1-10
Interface mng: 0 active, 3 maximum active, 0 denied
Interface INSIDE: 4 active, 5 maximum active, 0 denied
local host: <10.1.1.11>,
       TCP flow count/limit = 1/unlimited TCP embryonic count to host = 0 TCP intercept
       watermark = unlimited UDP flow count/limit = 4/unlimited
Xlate:
       Global 192.168.1.24 Local 10.1.1.11 Conn: UDP out 192.168.1.10:80 in
       10.1.1.11:1730 idle 0:00:21 bytes 0 flags - UDP out 192.168.1.10:80 in
       10.1.1.11:1729 idle 0:00:22 bytes 0 flags - UDP out 192.168.1.10:80 in
       10.1.1.11:1728 idle 0:00:23 bytes 0 flags - UDP out 192.168.1.10:80 in
       10.1.1.11:1727 idle 0:00:24 bytes 0 flags - TCP out 192.168.1.10:22 in
       10.1.1.11:27337 idle 0:01:55 bytes 2641 flags UIO Interface OUTSIDE: 3 active, 5
       maximum active, 0 denied
```

Related Commands

命令	Description
clear local-host	释放通过 **show local-host** 命令显示的本地主机的网络连接。

show log-events-to-ramdisk

要显示将连接事件记录到 RAM 磁盘的状态，请使用 **show log-events-to-ramdisk** 命令。

show log-events-to-ramdisk

Command History

版本	修改
6.1	引入了此命令。

使用指南

此命令显示您是将连接事件记录到RAM磁盘还是固态驱动器(SSD)。并非所有硬件型号都支持RAM磁盘日志记录。使用 **configure log-events-to-ramdisk** 命令配置 RAM 磁盘日志记录。

示例

以下示例显示此硬件型号不支持将日志记录到 RAM 磁盘。

```
> show log-events-to-ramdisk
This command is not available on this platform.
```

Related Commands

命令	Description
configure log-events-to-ramdisk	启用或禁用将连接事件记录到 RAM 磁盘。

show logging

要显示缓冲区中的日志或其他日志记录设置，请使用 **show logging** 命令。

show logging [**message** [*syslog_id* | **all**] | **asdm** | **flow-export-syslogs** | **queue** | **setting** | **unified-client** [**statistics**]]

Syntax Description

all	（可选）显示所有系统日志消息 ID，以及它们是启用还是禁用。
asdm	（可选）此关键字不适用于 设备管理器。它与配置ASA 软件设备的ASDM 相关。
flow-export-syslogs	（可选。显示其信息也由 NetFlow 捕获的所有系统日志消息。
message [*syslog_id* | **all**]	（可选）如果不指定系统日志 ID 或全部，则此关键字显示非默认级别的消息。您还可以按 ID 显示消息，或查看有关所有系统日志消息的信息。
queue	（可选）显示系统日志消息队列。
setting	（可选）显示日志记录设置，而不显示日志记录缓冲区。
syslog_id	（可选）指定要显示的消息编号。
unified-client [**statistics**]	显示有关系统日志客户端状态的详细统计信息，包括 loggerD 服务状态、系统日志客户端注册信息、loggerD 心跳详细信息以及系统日志客户端控制/数据和错误统计信息，

Command History

版本	修改
6.1	引入了此命令。
6.3	添加了 **unified-client** [**statistics**] 关键字。

使用指南

如果启用日志记录到内部缓冲区，则不带任何关键字的 **show logging** 命令会显示当前消息缓冲区和当前设置。

show logging queue 命令允许您显示以下内容：

- 队列中的消息数量
- 队列中记录的最大消息数量
- 由于块内存无法处理而被丢弃的消息数量
- 用于陷阱和其他系统日志消息的单独队列

注释 零是可接受的已配置队列大小，表示允许最大队列大小。如果配置的队列大小为零， **show logging queue** 命令的输出将显示实际队列大小。

show logging flow-export-syslogs 命令显示以下系统日志是已启用还是已禁用。使用 Netflow 时，您可以选择禁用这些系统日志，因为它们是冗余的。

系统日志消息	Description
106015	TCP 流被拒绝，因为第一个数据包不是 SYN 数据包。
106023	被连接到接口的入口 ACL 或出口 ACL 拒绝的流。
106100	ACL 允许或拒绝的流。
302013 and 302014	TCP 连接和删除。
302015 and 302016	UDP 连接和删除。
302017 and 302018	GRE 连接和删除。
302020 and 302021	ICMP 连接和删除。
313001	发送到 threat defense 设备的 ICMP 数据包被拒绝。
313008	发送到 threat defense 设备的 ICMPv6 数据包被拒绝。
710003	连接到 threat defense 的尝试被拒绝。

示例

以下是 **show logging** 命令的输出示例：

```
> show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: enabled
    Standby logging:disabled
    Debug-trace logging: disabled
    Console logging: level informational, 3962 messages logged
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: level informational, facility 20, 20549 messages logged
        Logging to inside 10.2.5.3 tcp/50001 connected
    Permit-hostdown state
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: disabled
```

注释 系统日志记录的可能值包括已启用、已禁用、已禁用-屏蔽和已禁用-不屏蔽。

以下是配置了安全系统日志服务器后 **show logging** 命令的输出示例：

```
> show logging
Syslog logging: disabled
    Facility:
    Timestamp logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: level debugging, 135 messages logged
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: list show _syslog, facility, 20, 21 messages logged
        Logging to inside 10.0.0.1 tcp/1500 SECURE
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging disabled
```

以下是 **show logging queue** 命令的输出示例：

```
> show logging queue
Logging Queue length limit: 512 msg(s)
0 msg(s) discarded due to queue overflow
0 msg(s) discarded due to memory allocation failure
Current 0 msgs on queue, 0 msgs most on queue
```

以下是 **show logging message all** 命令的输出示例：

```
> show logging message all
syslog 111111: default-level alerts (enabled)
syslog 101001: default-level alerts (enabled)
syslog 101002: default-level alerts (enabled)
syslog 101003: default-level alerts (enabled)
syslog 101004: default-level alerts (enabled)
syslog 101005: default-level alerts (enabled)
syslog 102001: default-level alerts (enabled)
syslog 103001: default-level alerts (enabled)
syslog 103002: default-level alerts (enabled)
syslog 103003: default-level alerts (enabled)
syslog 103004: default-level alerts (enabled)
syslog 103005: default-level alerts (enabled)
syslog 103011: default-level alerts (enabled)
syslog 103012: default-level informational (enabled)
```

以下是 **show logging unified-client** 命令的输出示例：

```
> show logging unified-client
Log client details:
 Name : Lina
 Id : 1331
 Init time : Fri Sep 7 07:20:14 2018
 Status : Registered
```

以下是 **show logging unified-client statistics** 命令的输出示例：

```
> show logging unified-client statistics
Log client details:
  Name                                          : Lina
  Id                                            : 1331
  Init time                                     : Fri Sep  7 07:20:14 2018
  Status                                        : Registered

Loggerd service up/down statistics:
  Service status                                : Up
  Instance-id                                   : 4602
  Last service down time                        : Wed Sep 12 05:17:43 2018

Log client register/unregister statistics:
  Total register messages Tx                    : 1222
  Total unregister messages Tx                  : 0
  Last register message Tx time                 : Wed Sep 12 05:40:16 2018
  Total register-ack messages Rx                : 39
  Last register-ack Rx time                     : Wed Sep 12 05:40:17 2018
  Total configuration sent messages Tx          : 14
  Number of configuration pushes                : 38

Heartbeat statistics:
  Last heartbeat Tx time                        : Wed Sep 12 06:38:33 2018
  Last Tx seqnum                                : 10019
  Total heartbeat Tx                            : 9981

Loggerd heartbeat statistics:
  Last heartbeat Rx time                        : Wed Sep 12 06:38:36 2018
  Last hearbeat Rx seqnum                       : 701
  Total heartbeat Rx                            : 5977
  Miss count                                    : 1

Log client data messages details:
  Syslogs Tx for ngfw-management                : 6554
  Syslogs Rx for data ports                     : 0
  Syslogs Tx drops for ngfw-management          : 0

Log client Control/Data channel statistics:
  Total control messages Tx                     : 11757
  Total service messages Rx                     : 98
  Total notify messages Rx                      : 6020
  Total data messages Rx                        : 0

Log-client error statistics:
  Register messages Tx                          : 2373
  Register-ack messages Rx                      : 5921
  Configuration push Tx                         : 1
  Heartbeat Tx                                  : 0
  Control channel Rx                            : 0
  Data channel Rx                               : 0
  Syslogs Rx for data ports                     : 0
```

show mac-address-table

要显示 MAC 地址表，请使用 **show mac-address-table** 命令。

show mac-address-table [*interface_name* | **count** | **static**]

Syntax Description

count	（可选）列出动态和静态条目的总数。
interface_name	（可选）标识要查看其 MAC 地址表条目的接口名称。
static	（可选）仅列出静态条目。

Command Default

如果不指定接口，将显示所有接口 MAC 地址条目。

Command History

版本	修改
6.1	添加了此命令。
6.2	使用集成路由和桥接时，我们在路由防火墙模式下添加了支持。

示例

以下是 **show mac-address-table** 命令的输出示例：

```
> show mac-address-table
interface    mac address     type      Time Left
-----------------------------------------------------
outside      0009.7cbe.2100  static    -
inside       0010.7cbe.6101  static    -
inside       0009.7cbe.5101  dynamic   10
```

以下是 **show mac-address-table count** 命令的输出示例：

```
> show mac-address-table count
Static     mac-address bridges (curr/max): 0/65535
Dynamic    mac-address bridges (curr/max): 103/65535
```

show mac-learn

要显示为每个接口启用还是禁用 MAC 学习，请使用 **show mac-learn** 命令。

show mac-learn

Command History

版本	修改
6.1	添加了此命令。
6.2	使用集成路由和桥接时，我们在路由防火墙模式下添加了支持。

使用指南

默认情况下，每个接口会自动获悉进入流量的MAC地址，并且系统会将对应的条目添加到MAC地址表中。您可以禁用每个接口的 MAC 学习。

示例

以下是 **show mac-learn** 命令的输出示例。

```
> show mac-learn
no mac-learn flood
interface                          mac learn
-------------------------------------------
 outside                             enabled
 inside1_2                           enabled
 inside1_3                           enabled
 inside1_4                           enabled
 inside1_5                           enabled
 inside1_6                           enabled
 inside1_7                           enabled
 inside1_8                           enabled
 diagnostic                          enabled
 inside                              enabled
```

show managers

要显示管理设备配置的当前管理器，请使用 **show managers** 命令。

show managers

Command History

版本	修改
6.1	引入了此命令。
7.2	对多个安装管理器加强支持。输出现在包括 管理中心 显示名称、标识符和管理类型（配置或分析）。

使用指南

使用 **show managers** 命令确定定义了哪个应用来管理设备配置。然后，您可以使用网络浏览器登录管理器。

使用 **configure manager add** 命令为设备配置远程管理器 管理中心时，输出会显示主机地址和注册状态。仅在注册处于待处理状态时，才会显示注册密钥和NAT ID。如果设备已注册到高可用性对，将会同时显示有关两个管理管理中心的信息。如果设备被配置为堆叠配置中的次要设备，将会同时显示有关管理管理中心和主设备的信息。

示例

以下示例显示已完成的远程管理器 管理中心 注册。

```
> show managers
Type                      : Manager
Host                      : 10.10.1.4
Display name              : 10.10.1.4
Identifier                : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration              : Completed
Management type           : Configuration
```

以下示例显示启用了本地管理器 设备管理器。

```
> show managers
Managed locally.
```

以下示例显示当前未配置管理器。必须先使用 configure manager add 或 configure manager local 启用一个，然后才能配置设备。

```
> show managers
No managers configured.
```

以下示例显示三个管理器：一个处于待处理状态，当前未在使用；一个是主配置管理器 (CDO)；一个是本地分析专用管理器。

```
> show managers
Type                      : Manager
Host                      : 1.2.3.4
Display name              : 1.2.3.4
Identifier                : 1.2.3.4
Registration              : Pending

Type                      : Manager
Host                      : 10.10.1.4
Display name              : 10.10.1.4
Identifier                : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration              : Completed
Management type           : Configuration

Type                      : Manager
Host                      : 10.10.2.7
Display name              : 10.10.2.7
Identifier                : 6d3df56e-bf16-11ec-972b-b07a16ffdd03
Registration              : Completed
Management type           : Analytics
```

Related Commands

命令	Description
configure manager add	添加远程管理器 管理中心。
configure manager delete	删除当前管理器并进入无管理器模式。
configure manager local	启用本地管理器 设备管理器。

show memory

要显示可供操作系统使用的最大物理内存量和当前可用内存量的摘要，请使用 **show memory** 命令。

show memory [**api** | **app-cache** | **binsize** *size* | **caller-address** | **detail** | **region** | **system** | **top-usage** [*num*]]

Syntax Description

api	（可选）显示在系统中注册的 malloc 堆栈 API。 如果开启任意内存调试功能（即无延迟毒化器、内存记录器、内存跟踪器或内存分析器），其 API 将显示在输出中。
app-cache	（可选）按应用显示内存使用情况。
binsize *size*	（可选）显示有关为特定 bin 大小分配的数据块（内存块）的摘要信息。bin 大小来自 **show memory detail** 命令输出的“分段大小”列。
caller-address	显示与 **memory caller-address** 网络配置相关的信息。
detail	（可选）显示空闲和已分配的系统内存的详细视图。
region	显示流程映射。
system	显示设备的总内存、使用中内存和可用内存。
top-usage [*num*]	显示通过 **show memory detail** 命令分配的最大分片大小。您可以选择指定要列出的 bin 大小的数量，范围为 1-64。默认值为 10。

Command History

版本	修改
6.1	引入了此命令。
6.2.2	**show memory** 和 **show memory detail** 的输出已更改。

使用指南

show memory 命令让您显示可供操作系统使用的最大物理内存量和当前可用内存量的摘要。内存会根据需要进行分配。

还可以使用 SNMP 显示 **show memory** 命令的信息。

您可以使用带有 **show memory binsize** 命令的 **show memory detail** 输出来调试内存泄漏。

show memory detail 命令输出可分为三个部分：摘要、DMA 内存和 HEAP 内存。摘要显示内存的总体分配方式。未绑定到 DMA 或保留的内存被视为 HEAP 内存。可用内存值是 HEAP 中的未使用内存。使用中的已分配内存值是已分配的 HEAP 数量。HEAP 分配的细目随后显示在输出中。保留内存和 DMA 保留内存主要被 VPN 服务使用，也被不同的系统进程使用。

可用内存分为两部分：可用内存堆和可用内存系统。可用内存堆是glibc堆中的可用内存量。当glibc堆按需增长和缩减时，空闲堆内存的量并不指示系统中剩余的总内存。可用内存系统表示ASA可用的可用内存量。

保留内存 (DMA) 是为 DMA 池保留的内存量。内存开销是各种运行进程的 glibc 开销和进程开销。

在 **show memory detail** 命令输出中，已分配内存统计合计（字节）列中显示的值未反映实际值 (MEMPOOL_GLOBAL_SHARED POOL STATS)。

注释 MEMPOOL_GLOBAL_SHARED 在启动期间不会占用所有系统内存，但会在需要时向底层操作系统请求内存。同样，当释放大量内存时，它会将内存返还给系统。因此，MEMPOOL_GLOBAL_SHARED 的大小似乎根据需求增长和缩小。MEMPOOL_GLOBAL_SHARED 中保留了最少量的可用内存，以加快分配速度。

输出表明，先分配了大小为 49,152 的块，随后该块返回到空闲池，并分配了另一个大小为 131,072 的块。在这种情况下，您会认为可用内存减少了 131,072-49,152=81,920 字节，但实际上减少了 100,000 字节（请参阅 Free memory 行）。

```
> show memory detail
MEMPOOL_GLOBAL_SHARED POOL STATS:            MEMPOOL_GLOBAL_SHARED POOL STATS:
Non-mmapped bytes allocated =   1862270976   Non-mmapped bytes allocated =   1862270976
Number of free chunks       =           99   Number of free chunks       =          100
Number of mmapped regions   =            0   Number of mmapped regions   =            0
Mmapped bytes allocated     =            0   Mmapped bytes allocated     =            0
Max memory footprint        =   1862270976   Max memory footprint        =   1862270976
Keepcost                    =   1762019304   Keepcost                    =   1761869256
Max contiguous free mem     =   1762019304   Max contiguous free mem     =   1761869256
Allocated memory in use     =    100133944   Allocated memory in use     =    100233944
Free memory                 =   1762137032   Free memory                 =   1762037032
----- fragmented memory statistics -----     ----- fragmented memory statistics -----
 fragment size       count          total     fragment size       count          total
    (bytes)                       (bytes)        (bytes)                       (bytes)
---------------  ----------  -------------- ---------------  ----------  --------------
        32768             1          33176           32768             1          33176
                                                      49152             1          50048
   1762019304             1     1762019304*     1761869256             1     1761869256*
----- allocated memory statistics -----      ----- allocated memory statistics -----
 fragment size       count          total     fragment size       count          total
    (bytes)                       (bytes)        (bytes)                       (bytes)
---------------  ----------  -------------- ---------------  ----------  --------------
        49152            10         491520           49152             9         442368
        65536           125        8192000           65536           125        8192000
        98304             3         294912           98304             3         294912
       131072            18        2359296          131072            19        2490368
```

以下输出确认分配了大小为 150,000 而不是 131,072 的块：

```
> show memory binsize 131072
MEMPOOL_DMA pool bin stats:
MEMPOOL_GLOBAL_SHARED pool bin stats:
pc = 0x8eda524, size = 150000   , count = 1
pc = 0x8f08054, size = 163904   , count = 1
pc = 0x846e477, size = 139264   , count = 1
pc = 0x8068691, size = 393216   , count = 3
pc = 0x8eea09b, size = 131072   , count = 1
pc = 0x88ca830, size = 141212   , count = 1
pc = 0x9589e93, size = 593580   , count = 4
pc = 0x9589bd2, size = 616004   , count = 4
pc = 0x8f2e060, size = 327808   , count = 2
```

```
pc = 0x8068284, size = 182000   , count = 1

0x8eda524 <logger_buffer_init_int+148 at syslog/main.c:403>
```

按照设计， **show memory detail** 命令输出中显示的总字节数是近似值。这有两个原因：

- 对于每个分段大小，如果您需要获取所有分段的总和，将会影响性能，因为可能有大量分配对应单个分段大小，要获得准确值，需要查遍数千个数据块。
- 对于每个 binsize，您需要查遍双重链接的分配列表，并且可能有多个分配。在这种情况下，您不能长时间占用 CPU，需要定期暂停分配。在恢复分配之后，其他进程可能已分配或取消分配内存，内存状态可能已发生变化。因此，总字节数列提供近似值而不是实际值。

示例

以下是 **show memory** 命令的输出示例：

```
> show memory
Free memory:        2986716635 bytes (64%)
Used memory:        1646723072 bytes (36%)
-------------     ------------------
Total memory:       4633439707 bytes (100%)

Note: Free memory is the free system memory. Additional memory may
      be available from memory pools internal to the ASA process.
      Use 'show memory detail' to see this information, but use it
      with care since it may cause CPU hogs and packet loss under load.
>
```

以下示例显示如何显示系统级内存使用情况。

```
> show memory system
             total       used       free     shared    buffers     cached
Mem:       3982640    3014544     240200          0     159932     567964
-/+ buffers/cache:    3014544     968096
Swap:      3998716     137704    3861012
```

以下是 **show memory detail** 命令的输出示例：

```
> show memory detail

Heap Memory:
   Free Memory:
      Heapcache Pool:                      3804848 bytes (  0% )
      Global Shared Pool:                 67372768 bytes (  1% )
      System:                           2986716635 bytes ( 64% )
   Used Memory:
      Heapcache Pool:                    308670800 bytes (  7% )
      Global Shared Pool:                     6432 bytes (  0% )
      Reserved (Size of DMA Pool):       499122176 bytes ( 11% )
      Reserved for messaging:              2097152 bytes (  0% )
      System Overhead:                   765648896 bytes ( 17% )
-----------------------------------     ----------------
   Total Memory:                        4633439707 bytes ( 100% )
```

```
Warning:  The information reported here is computationally expensive to
          determine, and may result in CPU hogs and performance impact.

------------------------------------------------------------------------
MEMPOOL_MSGLYR POOL STATS:

Non-mmapped bytes allocated =      2097152
Number of free chunks       =            1
Number of mmapped regions   =            0
Mmapped bytes allocated     =            0
Max memory footprint        =      2097152
Keepcost                    =      2092768
Max contiguous free mem     =      2092768
Allocated memory in use     =         4288
Free memory                 =      2092864

----- fragmented memory statistics -----

(...Remaining output truncated...)
```

以下示例显示分配给 bin 大小为 8192 的数据块。

```
> show memory binsize 8192
MEMPOOL_HEAPCACHE_0 pool bin stats:
pc = 0x7efc3f80e508, size = 773406   , count = 92
pc = 0x7efc3e3c5013, size = 189152   , count = 23
pc = 0x7efc405df64f, size = 287036   , count = 32
pc = 0x7efc3f9ef622, size = 8128     , count = 1
pc = 0x7efc3f4fd5f5, size = 871744   , count = 106
pc = 0x7efc3f4fd8b7, size = 82240    , count = 10
pc = 0x7efc3f18c3e6, size = 20272    , count = 2
pc = 0x7efc3f557139, size = 8192     , count = 1
pc = 0x7efc3e3f1697, size = 8344     , count = 1
pc = 0x7efc3e0506f6, size = 8192     , count = 1
MEMPOOL_DMA pool bin stats:
pc = 0x7efc3e1cca68, size = 10240    , count = 1
MEMPOOL_GLOBAL_SHARED pool bin stats:
```

以下是 **show memory api** 命令的输出示例。它显示内存跟踪器和延迟释放毒物内存功能处于活动状态。

```
> show memory api
Resource Manager (0) ->
Tracking (0) ->
Delayed-free-poisoner (0) ->
Core malloc package (0)
```

以下示例显示如何显示系统级内存使用情况。

```
> show memory system
             total       used       free     shared    buffers     cached
Mem:       3982640    3014544     240200          0     159932     567964
-/+ buffers/cache:    3014544     968096
Swap:      3998716     137704    3861012
```

Related Commands

命令	Description
show memory profile	显示 threat defense 内存使用情况（分析）的信息。

show memory all

要显示 lina 和 Snort 的可供操作系统使用的最大物理内存量和当前可用内存量的摘要，请使用 **show memory all** 命令。

show memory all

Command History

版本	修改
7.0	引入了此命令。

使用指南

show memory all 命令让您显示可供操作系统使用的最大物理内存量和当前可用内存量的摘要。内存会根据需要进行分配。

```
> show memory all
Data Path:
Free memory:        3161408675 bytes (72%)
Used memory:        1203826208 bytes (28%)
-------------     ------------------
Total memory:       4365234883 bytes (100%)
Inspection Engine:
Free memory:                  0 bytes ( 0%)
Used memory:                  0 bytes ( 0%)
-------------     ------------------
Total memory:                 0 bytes (100%)
System:
Free memory:                  0 bytes ( 0%)
Used memory:                  0 bytes ( 0%)
-------------     ------------------
Total memory:                 0 bytes (100%)
```

show memory delayed-free-poisoner

要显示 **memory delayed-free-poisoner** 队列使用情况摘要，请使用 **show memory delayed-free-poisoner** 命令。

show memory delayed-free-poisoner

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用 **memory delayed-free-poisoner enable** 命令启用此功能。使用 **clear memory delayed-free-poisoner** 命令清除队列和统计信息。

示例

以下是 **show memory delayed-free-poisoner** 命令的输出示例：

```
> memory delayed-free-poisoner enable
> show memory delayed-free-poisoner
delayed-free-poisoner settings:
 delayed-free-poisoner threshold 100
 delayed-free-poisoner desired-fragment-size 102400
 delayed-free-poisoner desired-fragment-count 16
 delayed-free-poisoner watchdog-percent 50
delayed-free-poisoner statistics:
                  136064:  current memory in queue
                     500:  current queue length
                       0:  frees dequeued
                     280:  frees not queued for size
                       0:  frees not queued for locking
                       0:  successful validate runs
                       0:  aborted validate runs
                   never:  time of last validate
                       0:  threshold defragment operations
                       0:  size and/or count defragment operations
                       0:  watchdog-aborts
```

show memory logging

要显示内存使用情况日志记录，请使用 **show memory logging** 命令。

show memory logging ［**wrap** | **brief** | **include** ［选项］］

Syntax Description

brief	（可选）显示缩写的内存使用情况日志记录。
include *option*	（可选）仅包含输出中的指定字段。您可以按任意顺序指定字段的关键词，但它们始终以下列顺序显示。如果不包括选项，则输出与指定了**brief**而不是 **include**。 • **process** • **time** • **operator** (free/malloc/etc.) • **address** • **size** • **callers** 输出格式如下： process=[XXX] time=[XXX] oper=[XXX] address=0xXXXXXXXX size=XX @ XXXXXXXX XXXXXXX XXXXXXX XXXXXXX 最多显示4个主叫方地址。操作类型列于示例所示的输出（...的数量）中。
wrap	（可选）显示内存使用情况日志记录包装的数据，在您输入此命令后，这些数据将被清除，因此不会出现重复的数据，也不会保存这些数据。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用 **show memory logging** 命令查看内存日志信息。您必须先使用 **memory logging** 命令启用此日志记录。

示例

以下是 **show memory logging** 命令的输出示例。

```
> memory logging 1024
> show memory logging
```

```
Number of free                          203989
Number of calloc                        83703
Number of malloc                        120286
Number of realloc-new                   0
Number of realloc-free                  0
Number of realloc-null                  0
Number of realloc-same                  0
Number of calloc-fail                   0
Number of malloc-fail                   0
Number of realloc-fail                  0
Total operations 407978
Buffer size: 1024 (73816 x2 bytes)
process=[cli_xml_server] time=[19:23:42.030] oper=[malloc] addr=0x00007efc358373c0 size=72

@ 0x00007efc3f8e9404 0x00007efc3f80e508 0x00007efc3f4d3cea 0x00007efc3e037f0c
process=[cli_xml_server] time=[19:23:42.030] oper=[free] addr=0x00007efc358373c0 size=72
@ 0x00007efc3f80e9c0 0x00007efc3f4d3fb8 0x00007efc3e037fb0 0x00007efc3f4d537d
(...Remaining output truncated...)
```

以下是 **show memory logging brief** 命令的输出示例。

```
> show memory logging brief
Number of free                          223195
Number of calloc                        91624
Number of malloc                        131572
Number of realloc-new                   0
Number of realloc-free                  0
Number of realloc-null                  0
Number of realloc-same                  0
Number of calloc-fail                   0
Number of malloc-fail                   0
Number of realloc-fail                  0
Total operations 446391
Buffer size: 1024 (73816 x2 bytes)
```

Related Commands

命令	Description
memory logging	启用内存日志记录。

show memory profile

要显示有关 threat defense 设备内存使用情况（分析）的信息，请使用 **show memory profile** 命令。

show memory profile ［**status** | **peak** ［**detail** | **collated**］］

Syntax Description

collated	（可选）整理显示的内存信息。
detail	（可选）显示详细内存信息。
peak	（可选）显示峰值捕获缓冲区而不是“使用中”缓冲区。
status	（可选）显示内存分析和峰值捕获缓冲区的当前状态。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用 **show memory profile** 命令可对内存使用级别和内存泄漏进行故障排除。即使内存分析已停止，您仍然可以查看分析缓冲区内容。开始内存分析将自动清除该缓冲区。

注释 启用内存分析时， threat defense 设备的性能可能会临时下降。

示例

以下是 **show memory profile** 命令的输出示例：

```
> show memory profile
Range: start = 0x004018b4, end = 0x004169d0, increment = 00000004
Total = 0
```

show memory profile detail 命令的输出分为六个数据列和最左侧的一个信头列。与第一个数据列对应的内存桶的地址在信头列给定（十六进制数字）。数据本身是通过桶地址中的文本/代码保存的字节数。数据列中的句点 (.) 表示此内存桶处的文本未保留内存。行中的其他列对应于大于前一列增量的桶地址。例如，第一行中第一个数据列的地址桶为 0x001069e0。第一行中第二个数据列的地址桶为 0x001069e4，依此类推。通常信头列地址是下一个桶地址；即，前一行的最后一个数据列的地址加上增量。所有未使用的行都不会显示。若不显示多个连续的此类行，用信头列中的三个句点 (...) 指示。

以下是 **show memory profile peak detail** 命令的输出示例，其中显示了峰值捕获缓冲区和通过相应桶地址中的文本/代码保存的字节数：

```
> show memory profile peak detail
Range: start = 0x00100020, end = 0x00e006e0, increment = 00000004
```

```
Total = 48941152
...
0x001069e0 . 24462 . . . .
...
0x00106d88 . 1865870 . . . .
...
0x0010adf0 . 7788 . . . .
...
0x00113640 . . . . 433152 .
...
0x00116790 2480 . . . . .
(...output truncated...)
```

以下是 **show memory profile peak collated** 命令的输出示例：

```
> show memory profile peak collated
Range: start = 0x00100020, end = 0x00e006e0, increment = 00000004
Total = 48941152
24462 0x001069e4
1865870 0x00106d8c
7788 0x0010adf4
433152 0x00113650
2480 0x00116790
<More>
```

以下是 **show memory profile peak** 命令的输出示例，其中显示了峰值捕获缓冲区：

```
> show memory profile peak
Range: start = 0x004018b4, end = 0x004169d0, increment = 00000004
Total = 102400
```

以下是 **show memory profile status** 命令的输出示例，其中显示了内存分析和峰值捕获缓冲区的当前状态：

```
> show memory profile status
InUse profiling: ON
Peak profiling: OFF
Memory used by profile buffers: 11518860 bytes
Profile:
0x00100020-0x00bfc3a8(00000004)
```

Related Commands

命令	Description
memory profile enable	启用对内存使用（内存分析）的监控。
memory profile text	配置要分析的内存的程序文本范围。
clear memory profile	清除内存分析功能保留的缓冲区。

show memory tracking

要显示该工具跟踪的当前已分配内存，请使用 **show memory tracking** 命令。

show memory tracking [**address** | **detail** | **dump** *tracked_address*]

Syntax Description

address	（可选）按地址显示内存跟踪。
detail	（可选）显示内存跟踪状态。
dump *tracked_address*	（可选）显示指定内存跟踪地址 0-4294967295 的转储。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用 **show memory tracking** 命令以要显示该工具跟踪的当前已分配内存。您必须先使用 **memory tracking enable**，然后才能看到此信息。

示例

以下是 **show memory tracking** 命令的输出示例：

```
> show memory tracking
memory tracking by caller:
  bytes-threshold:        0
  allocates-by-threshold: 0
         65406 bytes from    49 allocates by 0x00007efc3f80e508
          3000 bytes from     1 allocates by 0x00007efc3f4e1278
           159 bytes from     1 allocates by 0x00007efc3fe9ee13
            17 bytes from     1 allocates by 0x00007efc3fe9ef4e
```

以下是 **show memory tracking address** 命令的输出示例：

```
> show memory tracking address
memory tracking by caller:
  bytes-threshold:        0
  allocates-by-threshold: 0
         58918 bytes from    49 allocates by 0x00007efc3f80e508
          3000 bytes from     1 allocates by 0x00007efc3f4e1278
           167 bytes from     1 allocates by 0x00007efc3fe9ee13
            17 bytes from     1 allocates by 0x00007efc3fe9ef4e
memory tracking address pool:
            32 byte region @ 0x00007efc358a06e0 allocated by 0x00007efc3f80e508
            96 byte region @ 0x00007efc351d0880 allocated by 0x00007efc3f80e508
           896 byte region @ 0x00007efc35f121c0 allocated by 0x00007efc3f80e508
          8192 byte region @ 0x00007efc35832e20 allocated by 0x00007efc3f80e508
            96 byte region @ 0x00007efc30483910 allocated by 0x00007efc3f80e508
            88 byte region @ 0x00007efc359e3960 allocated by 0x00007efc3f80e508
          1036 byte region @ 0x00007efc35f04680 allocated by 0x00007efc3f80e508
            76 byte region @ 0x00007efc36024890 allocated by 0x00007efc3f80e508
```

```
  24 byte region @ 0x00007efc35fd48a0 allocated by 0x00007efc3f80e508
  32 byte region @ 0x00007efc35f04ad0 allocated by 0x00007efc3f80e508
  34 byte region @ 0x00007efc35e54e00 allocated by 0x00007efc3f80e508
8192 byte region @ 0x00007efc35834e70 allocated by 0x00007efc3f80e508
  40 byte region @ 0x00007efc36005cc0 allocated by 0x00007efc3f80e508
  11 byte region @ 0x00007efc360061e0 allocated by 0x00007efc3f80e508
  76 byte region @ 0x00007efc357a6dd0 allocated by 0x00007efc3f80e508
1024 byte region @ 0x00007efc358574f0 allocated by 0x00007efc3f80e508
  88 byte region @ 0x00007efc365b7ef0 allocated by 0x00007efc3f80e508
  56 byte region @ 0x00007efc365b7f90 allocated by 0x00007efc3f80e508
 168 byte region @ 0x00007efc365b8210 allocated by 0x00007efc3f80e508
 112 byte region @ 0x00007efc365b8300 allocated by 0x00007efc3f80e508
 112 byte region @ 0x00007efc365b83c0 allocated by 0x00007efc3f80e508
  16 byte region @ 0x00007efc365b8560 allocated by 0x00007efc3f80e508
 167 byte region @ 0x00007efc365b85c0 allocated by 0x00007efc3fe9ee13
2048 byte region @ 0x00007efc357a8610 allocated by 0x00007efc3f80e508
  88 byte region @ 0x00007efc35728be0 allocated by 0x00007efc3f80e508
  88 byte region @ 0x00007efc357a8e60 allocated by 0x00007efc3f80e508
4112 byte region @ 0x00007efc35fe90c0 allocated by 0x00007efc3f80e508
  17 byte region @ 0x00007efc365b95a0 allocated by 0x00007efc3fe9ef4e
  72 byte region @ 0x00007efc365b9600 allocated by 0x00007efc3f80e508
  72 byte region @ 0x00007efc365b9690 allocated by 0x00007efc3f80e508
  72 byte region @ 0x00007efc365b9720 allocated by 0x00007efc3f80e508
  40 byte region @ 0x00007efc365b97b0 allocated by 0x00007efc3f80e508
  24 byte region @ 0x00007efc365b9820 allocated by 0x00007efc3f80e508
   2 byte region @ 0x00007efc365b9880 allocated by 0x00007efc3f80e508
  76 byte region @ 0x00007efc35ff9aa0 allocated by 0x00007efc3f80e508
 776 byte region @ 0x00007efc35f19df0 allocated by 0x00007efc3f80e508
 512 byte region @ 0x00007efc3585a0a0 allocated by 0x00007efc3f80e508
 936 byte region @ 0x00007efc357aaea0 allocated by 0x00007efc3f80e508
  24 byte region @ 0x00007efc357ab290 allocated by 0x00007efc3f80e508
 568 byte region @ 0x00007efc3592bc40 allocated by 0x00007efc3f80e508
 512 byte region @ 0x00007efc35e5c8a0 allocated by 0x00007efc3f80e508
  40 byte region @ 0x00007efc35f2cae0 allocated by 0x00007efc3f80e508
1665 byte region @ 0x00007efc359fcda0 allocated by 0x00007efc3f80e508
 168 byte region @ 0x00007efc34fccf60 allocated by 0x00007efc3f80e508
 112 byte region @ 0x00007efc35ffd0e0 allocated by 0x00007efc3f80e508
4112 byte region @ 0x00007efc356bd340 allocated by 0x00007efc3f80e508
8208 byte region @ 0x00007efc3643d3e0 allocated by 0x00007efc3f80e508
 386 byte region @ 0x00007efc359fd470 allocated by 0x00007efc3f80e508
  72 byte region @ 0x00007efc35e4d570 allocated by 0x00007efc3f80e508
8208 byte region @ 0x00007efc359fd840 allocated by 0x00007efc3f80e508
4112 byte region @ 0x00007efc3592ded0 allocated by 0x00007efc3f80e508
3000 byte region @ 0x00007efc357ee5c0 allocated by 0x00007efc3f4e1278
  32 byte region @ 0x00007efc351be6d0 allocated by 0x00007efc3f80e508
  16 byte region @ 0x00007efc359de790 allocated by 0x00007efc3f80e508
1036 byte region @ 0x00007efc3524f080 allocated by 0x00007efc3f80e508
 512 byte region @ 0x00007efc357ff290 allocated by 0x00007efc3f80e508
 360 byte region @ 0x00007efc357ef360 allocated by 0x00007efc3f80e508
  24 byte region @ 0x00007efc357ff4e0 allocated by 0x00007efc3f80e508
```

Related Commands

命令	Description
clear memory tracking	清除所有当前已收集的信息。
memory tracking	启用内存跟踪。

show memory webvpn

要生成 WebVPN 的内存使用情况统计信息，请使用 **show memory webvpn** 命令。

show memory webvpn ［**allobjects** | **blocks** | **dumpstate** *filename* | **pools** | **usedobjects**］
show memory webvpn profile ［**clear** | **dump** *filename* | **start** | **stop**］

Syntax Description

allobjects	显示池、块以及所有已使用和已释放对象的 WebVPN 内存消耗详细信息。
blocks	显示内存块的 WebVPN 内存消耗详细信息。
clear	清除 WebVPN 内存配置。
dump *filename*	将 WebVPN 内存配置文件放入指定的文件中。文件名应包括位置，可以是 disk0:、disk1:、flash:、ftp:、tftp:。
dumpstate *filename*	将 WebVPN 内存状态放入指定文件。文件名应包括位置，可以是 disk0:、disk1:、flash:、ftp:、tftp:。
pools	显示内存池的 WebVPN 内存消耗详细信息。
profile	获取 WebVPN 内存配置并将其放入文件。
start	开始收集 WebVPN 内存分析。
stop	停止获取 WebVPN 内存分析。
usedobjects	显示已使用对象的 WebVPN 内存消耗详细信息。

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show memory webvpn allobjects** 命令的输出示例：

```
> show memory webvpn allobjects
Arena 0x36b14f8 of 4094744 bytes (61 blocks of size 66048), maximum 134195200
130100456 free bytes (97%; 1969 blocks, zone 0)
Arena is dynamically allocated, not contiguous
Features: GroupMgmt: SET, MemDebugLog: unset
Pool 0xd719a78 ("cp_entries" => "pool for class cpool entries") (next 0xd6d91d8)
Size: 66040 (1% of current, 0% of limit)
Object frame size: 32
Load related limits: 70/50/30
Callbacks: !init/!prep/!f2ca/!dstr/!dump
Blocks in use:
Block 0xd719ac0..0xd729cb8 (size 66040), pool "cp_entries"
Watermarks { 0xd7098f8 <= 0xd70bb60 <= 0xd719a60 } = 57088 ready
```

```
Block size 66040 not equal to arena block 66048 (realigned-to-8)
Used objects: 0
Top allocated count: 275
Objects dump:
0. Object 0xd70bb50: FREED (by "jvclass_pool_free")
```

show mfib

要显示组播转发信息库中的信息，请使用 **show mfib** 命令。

show mfib [*source_or_group* [*group*]] [**cluster** | **count** | **verbose**]
show mfib [**active** [*kbps*] | **cluster-stats** | **interface** | **status** | **summary**]
show mfib reserved [**active** [*kbps*] | **cluster** | **count** | **verbose**]

Syntax Description

[**active** [*kbps*]	（可选）显示活动组播源。您可以指定千位/秒，将显示限制为大于或等于此值的组播流。默认值为 4，范围为 0-4294967295。
cluster	（可选）显示MFIB日期和当前计时器值。如果同时指定源和组，则无法指定 **cluster** 。
cluster-stats	（可选）显示 MFIB 集群同步统计信息。
count	（可选）显示MFIB路由和数据包计数数据。此命令显示数据包丢弃统计信息。
interface	（可选）显示与 MFIB 流程相关的接口的数据包统计信息。
reserved	（可选）显示保留组的 MFIB 条目，范围为 224.0.0.0 到 224.0.0.225。
source_or_group [*group*]	（可选）源或组 IPv4、IPv6 或名称。如果同时指定两者，请先指定源。源地址为单播地址。
status	（可选）显示常规 MFIB 配置和运行状态。
summary	（可选）显示有关 MFIB 条目和接口数量的摘要信息。
verbose	显示有关转发条目和接口的详细信息

Command Default

如果没有可选参数，则显示所有组的信息。

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show mfib** 命令的输出示例：

```
> show mfib 224.0.2.39
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop
Forwarding counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface flags: A - Accept, F - Forward, NS - Negate Signalling
```

```
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,224.0.1.39) Flags: S K
  Forwarding: 0/0/0/0, Other: 0/0/0
```

以下是 **show mfib verbose** 命令的输出示例：

```
> show mfib verbose
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop
Forwarding counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface flags: A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,224.0.1.39) Flags: S K
  Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.1.40) Flags: S K
  Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.0.0/8) Flags: K
  Forwarding: 0/0/0/0, Other: 0/0/0
```

以下是 **show mfib count** 命令的输出示例：

```
> show mfib count
MFIB global counters are :
* Packets [no input idb] : 0
* Packets [failed route lookup] : 0
* Packets [Failed idb lookup] : 0
* Packets [Mcast disabled on input I/F] : 0
```

以下是 **show mfib active** 命令的输出示例。输出显示速率 PPS 的正数或负数。当 RPF 数据包发生故障或路由器观察到具有传出接口 (OIF) 列表的 RPF 数据包时，命令显示负数。此类型的活动可能指示组播路由问题。

```
> show mfib active
Active IP Multicast Sources - sending >= 4 kbps

Group: 224.2.127.254, (sdr.cisco.com)
   Source: 192.168.28.69 (mbone.ipd.anl.gov)
     Rate: 1 pps/4 kbps(1sec), 4 kbps(last 1 secs), 4 kbps(life avg)

Group: 224.2.201.241, ACM 97
   Source: 192.168.52.160 (webcast3-e1.acm97.interop.net)
     Rate: 9 pps/93 kbps(1sec), 145 kbps(last 20 secs), 85 kbps(life avg)

Group: 224.2.207.215, ACM 97
   Source: 192.168.52.160 (webcast3-e1.acm97.interop.net)
     Rate: 3 pps/31 kbps(1sec), 63 kbps(last 19 secs), 65 kbps(life avg)
```

以下是 **show mfib interface** 命令的输出示例：

```
> show mfib interface
IP Multicast Forwarding (MFIB) status:
```

```
    Configuration Status: enabled
    Operational Status: running
MFIB interface       status    CEF-based output
                               [configured,available]
           Ethernet0   up    [        no,       no]
           Ethernet1   up    [        no,       no]
           Ethernet2   up    [        no,       no]
```

以下是 **show mfib status** 命令的输出示例：

```
> show mfib status
IP Multicast Forwarding (MFIB) status:
    Configuration Status: enabled
    Operational Status: running
```

以下是 **show mfib summary** 命令的输出示例：

```
> show mfib summary
IPv6 MFIB summary:

  54     total entries [1 (S,G), 7 (*,G), 46 (*,G/m)]

  17     total MFIB interfaces
```

以下是 **show mfib reserved** 命令的输出示例：

```
> show mfib reserved
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface Flags: A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,224.0.0.0/4) Flags: C K
   Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.0.0/24) Flags: K
   Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.0.1) Flags:
   Forwarding: 0/0/0/0, Other: 0/0/0
   outside Flags: IC
   dmz Flags: IC
   inside Flags: IC
```

Related Commands

命令	Description
clear mfib counters	清除 MFIB 路由器数据包计数器。
show mroute active	显示活动的组播流。
show mroute count	显示组播路由计数器。
show mroute summary	显示组播路由表摘要信息。

show mgcp

要显示媒体网关控制协议 (MGCP) 配置和会话信息，请使用 **show mgcp** 命令。

show mgcp {commands | **sessions**} [**detail**]

Syntax Description

commands	列出命令队列中 MGCP 命令的数量。
detail	（可选）在输出中列出每个命令或会话的附加信息。
sessions	列出现有 MGCP 会话的数量。

Command History

版本	修改
6.2.1	引入了此命令。

使用指南

要显示 MGCP 信息，必须检查 MGCP 流量。要检查 MGCP 流量，您需要在 管理中心中配置 FlexConfig。

示例

以下是 **show mgcp** 命令选项的示例：

```
> show mgcp commands
1 in use, 1 most used, 200 maximum allowed
CRCX, gateway IP: host-pc-2, transaction ID: 2052, idle: 0:00:07

> show mgcp commands detail
1 in use, 1 most used, 200 maximum allowed
CRCX, idle: 0:00:10
       Gateway IP | host-pc-2
       Transaction ID  2052
       Endpoint name | aaln/1
       Call ID | 9876543210abcdef
       Connection ID |
       Media IP | 192.168.5.7
       Media port | 6058

> show mgcp sessions
1 in use, 1 most used
Gateway IP host-pc-2, connection ID 6789af54c9, active 0:00:11

> show mgcp sessions detail
1 in use, 1 most used
Session active 0:00:14
       Gateway IP | host-pc-2
       Call ID | 9876543210abcdef
       Connection ID | 6789af54c9
       Endpoint name | aaln/1
       Media lcl port  6166
       Media rmt IP | 192.168.5.7
```

```
Media rmt port  6058
```

show mini-coredump status

要显示迷你核心转储生成的设置，请输入 **show mini-coredump status** 命令。

show mini-coredump status

Command History

版本	修改
7.0	引入了此命令。

使用指南

默认情况下，迷你核心转储生成处于启用状态。

由于其多线程性质，Snort 3 流程会转储巨大的核心文件。这些转储需要一段时间才能写入硬盘。在写入核心并启动新流程之前，Snort 的流量检查会中断。创建迷你核心转储可避免时间延迟。迷你核心转储具有有助于调试的堆栈和内存值的基本详细信息。

示例

以下示例显示迷你核心转储生成已禁用。

```
> show mini-coredump status
minicoredump feature status : Disabled
```

Related Commands

命令	Description
configure mini-coredump	启用或禁用迷你核心转储生成。

show mode

要显示系统的安全情景模式，请使用 **show mode** 命令。

show mode

Command History

版本	修改
6.1	引入了此命令。

使用指南

threat defense 设备仅支持单情景模式。不支持多情景模式。

示例

以下示例显示如何显示安全情景模式。

```
> show mode
Security context mode: single
```

show model

要显示设备的硬件型号，请使用 **show model** 命令。

show model

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例显示了设备型号。

```
> show model
Cisco ASA5516-X Threat Defense
```

Related Commands

命令	Description
show serial-number	显示设备序列号。
show version	显示软件和其他设备版本信息。

show module

要显示有关 threat defense 设备上安装的模块的信息，请在用户 EXEC 模式下使用 **show module** 命令。

show module ［*ID* ［**details** | **recover** | **log console**］］ | **all**］

Syntax Description

all	（默认）显示所有模块的信息。这是默认值。
details	（可选）显示附加信息，包括模块的远程管理配置。
ID	指定模块 ID。使用不带参数的 show module 查看可用插槽号，通常为 0 和 1。
log console	（可选）显示模块的日志信息。此选项可能并非对每个模块都有效。
recover	（可选）显示用于恢复模块的设置。

Command Default

默认情况下，显示所有模块的信息。

Command History

版本	修改
6.1	引入了此命令。

使用指南

此命令显示有关 threat defense 设备中安装的模块的信息。 threat defense 本身也会以模块形式出现在显示中（在插槽 0 中）。设备是否支持其他模块因设备型号而异。

show module details 命令的输出会根据已安装的模块而有所不同。

对于允许配置软件模块的型号， **show module** 命令会列出所有可能的模块。状态消息指示是否已安装其中一个模块。

示例

以下示例输出适用于运行 threat defense 软件的 ASA 5516-X。对于此设备，插槽 1 未知是正常的，因为 threat defense 不支持任何软件模块。

```
> show module

Mod  Card Type                                    Model              Serial No.
---- ------------------------------------------- ------------------ -----------
   0 ASA 5516-X with FirePOWER services, 8GE, AC, ASA5516            JAD19390056I
   1 Unknown                                     N/A                JAD19390056I

Mod  MAC Address Range                 Hw Version   Fw Version   Sw Version
---- --------------------------------- ------------ ------------ ---------------
   0 84b2.61b1.92be to 84b2.61b1.92c6  1.0          1.1.3        97.1(0)60
   1 84b2.61b1.92bd to 84b2.61b1.92bd  N/A          N/A
```

```
Mod  SSM Application Name           Status           SSM Application Version
---- ------------------------------ ---------------- --------------------------
   1 Unknown                        No Image Present Not Applicable

Mod  Status             Data Plane Status     Compatibility
---- ------------------ --------------------- -------------
   0 Up Sys             Not Applicable
   1 Unresponsive       Not Applicable
```

下表说明了输出中列出的每个字段。

表 *46: show module* 输出字段

字段	Description
Mod	模块编号，0 或 1。
Card Type	卡类型。对于模块 0 中显示的设备，类型为平台型号。对于插槽 1，它将是额外的模块（如果有）。
Model	此模块的型号。
Serial No.	序列号。
MAC Address Range	此模块上接口的 MAC 地址范围。
Hw Version	硬件版本。
Fw Version	固件版本。
Sw Version	软件版本。这不是 threat defense 版本。相反，它是 ASA 软件版本，是 threat defense 软件的组件。使用 **show version** 命令查看 threat defense 版本。
SSM Application Name	在安全服务模块上运行的应用的名称。
SSM Application Version	在安全服务模块上运行的应用的版本。

字段	Description
Status	对于模块 0 中的设备，状态为 Up Sys。模块 1 中的模块的状态可以是以下状态之一： • Initializing（正在初始化）- 检测到模块，并且设备正在初始化控制通信。 • Up（开启）- 模块已完成设备初始化。 • Unresponsive（无响应）- 设备在与此模块通信时遇到错误。 • Reloading（正在重新加载）- 模块正在重新加载。 • Shutting Down（正在关闭）- 模块正在关闭。 • Down（关闭）- 模块已关闭。 • Recover（恢复）- 模块正在尝试下载恢复映像。 • No Image Present（不存在映像）- 模块软件尚未安装。
Data Plane Status	数据层面的当前状态。
Compatibility	模块相对于设备其余部分的兼容性。

show monitor-interface

要显示有关故障转移监控接口的信息，请使用 **show monitor-interface** 命令。

show monitor-interface

Command History

版本	修改
6.1	引入了此命令。

使用指南

由于一个接口上可配置多个 IPv6 地址，因此 **show monitor-interface** 命令只显示本地链路的地址。如果接口上配置了 IPv4 和 IPv6 地址，则两个地址都会出现在输出中。如果接口上未配置 IPv4 地址，则输出中的 IPv4 地址会显示为 0.0.0.0。如果接口上未配置 IPv6 地址，则输出中会直接省略地址。

监测的故障切转移口可以具有以下状态：

- (Waiting) 加上任何其他状态，例如 Unknown (Waiting) - 接口尚未从对等体设备上的相应接口收到 hello 数据包。
- Unknown - 初始状态。此状态也可能意味着状态无法确定。
- Normal - 接口正在接收流量。如果状态为正常（等待），请检查该接口是否配置了备 IP 地址，且两个接口之间是否连接。
- Testing - 接口上有 5 个轮询时间未收听到 Hello 消息。
- Link Down - 接口或 VLAN 通过管理方式关闭。
- No Link - 接口的物理链路关闭。
- Failed - 在接口上没有收到流量，但在对等体接口上收听到流量。

示例

以下是 **show monitor-interface** 命令的输出示例：

```
> show monitor-interface
 This host: Primary - Active
  Interface inside (192.168.1.13): Normal (Monitored)
  Interface outside (192.168.2.13): Normal (Monitored)
 Other host: Secondary - Standby Ready
  Interface inside (192.168.1.14): Normal (Monitored)
  Interface outside (192.168.2.14): Normal (Monitored)
```

show mrib client

要显示有关 MRIB 客户端连接的信息，请使用 **show mrib client** 命令。

show mrib client ［**filter**］［**name** *client_name*］

Syntax Description

filter	（可选）显示客户端过滤器。用于查看有关每个客户端拥有的MRIB标志以及每个客户端感兴趣的标志的信息。
name *client_name*	（可选）用作 MRIB 客户端的组播路由协议的名称，如 PIM 或 IGMP。

Command History

版本	修改
6.1	引入了此命令。

使用指南

filter 选项用于显示各 MRIB 客户端已注册的路由和接口级别标志更改。此命令选项还显示哪些标志由 MRIB 客户端所有。

示例

以下是使用 **filter** 关键字的 **show mrib client** 命令的输出示例：

```
> show mrib client filter
MFWD:0 (connection id 0)
interest filter:
entry attributes: S C IA D
interface attributes: F A IC NS DP SP
groups:
include 0.0.0.0/0
interfaces:
include All
ownership filter:
groups:
include 0.0.0.0/0
interfaces:
include All
igmp:77964 (connection id 1)
ownership filter:
interface attributes: II ID LI LD
groups:
include 0.0.0.0/0
interfaces:
include All
pim:49287 (connection id 5)
interest filter:
entry attributes: E
interface attributes: SP II ID LI LD
groups:
include 0.0.0.0/0
interfaces:
include All
ownership filter:
entry attributes: L S C IA D
```

```
interface attributes: F A IC NS DP
groups:
include 0.0.0.0/0
interfaces:
include All
```

Related Commands

命令	Description
show mrib route	显示 MRIB 表条目。

show mrib route

要显示 MRIB 表中的条目，请使用 **show mrib route** 命令。

show mrib route [[[*source* | *****] [*group*[/*prefix-length*]]] | **summary**]

Syntax Description

*****	（可选）显示共享树条目。
/*prefix-length*	（可选）MRIB 路由的前缀长度。是一个十进制值，表示构成前缀（地址的网络部分）的地址高位的连续位数。十进制值前面必须有斜线标记。
group	（可选）组的 IP 地址或名称。
source	（可选）路由源的 IP 地址或名称。
summary	显示 MRIB 表条目的摘要。

Command History

版本	修改
6.1	引入了此命令。

使用指南

MFIB 表维护从 MRIB 更新的条目和标志子集。标志根据组播数据包的转发规则集来确定转发和信令行为。

除了接口和标志的列表外，每个路由条目都显示各种计数器。字节数是转发的总字节数。数据包数是针对此条目接收的数据包数。 **show mfib count** 命令显示与路由无关的全局计数器。

示例

以下是 **show mrib route** 命令的输出示例：

```
> show mrib route
IP Multicast Routing Information Base
Entry flags: L - Domain-Local Source, E - External Source to the Domain,
    C - Directly-Connected Check, S - Signal, IA - Inherit Accept, D - Drop
Interface flags: F - Forward, A - Accept, IC - Internal Copy,
    NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,
    II - Internal Interest, ID - Internal Disinterest, LI - Local Interest,
LD - Local Disinterest
(*,224.0.0.0/4) RPF nbr: 10.11.1.20 Flags: L C
   Decapstunnel0 Flags: NS

(*,224.0.0.0/24) Flags: D

(*,224.0.1.39) Flags: S

(*,224.0.1.40) Flags: S
   POS0/3/0/0 Flags: II LI

(*,238.1.1.1) RPF nbr: 10.11.1.20 Flags: C
   POS0/3/0/0 Flags: F NS LI
```

```
   Decapstunnel0 Flags: A

(*,239.1.1.1) RPF nbr: 10.11.1.20 Flags: C
   POS0/3/0/0 Flags: F NS
   Decapstunnel0 Flags: A
```

Related Commands

命令	Description
show mfib count	显示 MFIB 表的路由和数据包计数数据。

show mroute

要显示 IPv4 组播路由表，请使用 **show mroute** 命令。

show mroute [*group* [*source*] | **reserved**] [**active** [*rate*] | **count** | **pruned** | **summary**]

Syntax Description

active *rate*	（可选）仅显示活动组播源。活动源是正在以指定 *rate* 或更高速率发送的源。如果未指定 *rate* ，则活动源是正在以 4 kbps 或更高速率发送的源。
count	（可选）显示有关组和源的统计信息，包括数据包数、每秒数据包数，平均数据包大小和 bps。
group	（可选）组播组的 IP 地址或名称，如 DNS 主机表中所定义。
pruned	（可选）显示修剪的路由。
reserved	（可选）显示预留组。
source	（可选）源主机名或 IP 地址。
summary	（可选）在组播路由表中显示每个条目的单行缩写摘要。

Command History

版本	修改
6.1	引入了此命令。

使用指南

show mroute 命令显示组播路由表的内容。设备通过创建基于 PIM 协议消息、IGMP 报告和流量的 (S,G) 和 (*,G) 条目来填充组播路由表。星号 (*) 指所有源地址，“S”指单个源地址，“G”是目标组播组地址。在创建 (S, G) 条目时，软件使用在单播路由表中找到的到该目标组的最佳路径（通过 RPF）。

要查看运行配置中的 **mroute** 命令，请使用 **show running-config mroute** 命令。

示例

以下是 **show mroute** 命令的输出示例：

```
> show mroute

Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, State

(*, 239.1.1.40), 08:07:24/never, RP 0.0.0.0, flags: DPC
  Incoming interface: Null
```

```
  RPF nbr: 0.0.0.0
  Outgoing interface list:
    inside, Null, 08:05:45/never
    tftp, Null, 08:07:24/never

(*, 239.2.2.1), 08:07:44/never, RP 140.0.0.70, flags: SCJ
  Incoming interface: outside
  RPF nbr: 140.0.0.70
  Outgoing interface list:
    inside, Forward, 08:07:44/never
```

show mroute 输出中显示以下字段：

- Flags - 提供有关条目的信息。
  - D - 密集。条目在密集模式下工作。
  - S - 稀疏。条目在稀疏模式下工作。
  - B - 双向组。指示组播组在双向模式下工作。
  - s - SSM 组。指示组播组在 IP 地址的 SSM 范围内。如果 SSM 范围更改，此标志将重置。
  - C - 已连接。组播组的成员出现在直接连接的接口上。
  - L - 本地。设备本身是组播组的成员。通过 igmp join-group 命令以本地方式加入组（对于已配置的组）。
  - I - 已接收源特定主机报告。指示通过 (S, G) 报告创建了 (S, G) 条目。此 (S, G) 报告可能通过 IGMP 创建。此标志仅在 DR 上设置。
  - P - 已修剪。路由已修剪。软件将保留此信息，以便下游成员加入源。
  - R - RP 位已设置。指示 (S, G) 条目指向 RP。
  - F - 注册标志。指示软件正在注册组播源。
  - T - SPT 未已设置。指示已在最短路径源树上收到数据包。
  - J - 联合 SPT。对于 (*, G) 条目，指示流量流下共享树的速率超过为组设置的 SPT 阈值。（默认 SPT 阈值设置为 0 kbps。）当设置 J - Join 最短路径树 (SPT) 标志后，在共享树收到的下一个 (S, G) 数据包将触发源方向上的 (S, G) 加入，从而使设备加入源树。

    对于 (S, G) 条目，指示由于超过了组的 SPT 阈值而创建了条目。当为 (S, G) 条目设置 J - Join SPT 标志后，设备监控源树上的流量速率，并在源树上的流量速率低于组的 SPT 阈值超过 1 分钟时尝试切换回此源的共享树。

注释 设备会测量共享树上的流量速率，并将测量出的速率与组的 SPT 阈值进行比较，每秒比较一次。如果流量速率超过 SPT 阈值，将在 (*, G) 条目上设置 J - Join SPT 标志，直到下一次测量流量速率。当下一个数据包到达共享树并且开始新的测量间隔时，清除该标志。

如果组使用默认 SPT 阈值 0 Kbps，将始终在 (*, G) 条目上设置 J - Join SPT 标志，并且不会清除。当使用默认 SPT 阈值时，如果收到来自新源的流量，设备会立即切换到最短路径源树。

- 计时器：正常运行时间/到期时间 - 正常运行时间针对接口指示条目在 IP 组播路由表中的时长（以小时、分钟和秒为单位）。到期时间针对接口指示从 IP 组播路由表中删除条目之前的时长（以小时、分钟和秒为单位）。
- 接口状态 - 指示传入或传出接口的状态。
  - 接口 - 传入或传出接口列表中列出的接口名称。
  - 状态 - 指示数据包在接口上被转发、修剪还是变空，具体取决于是否因访问列表或生存时间 (TTL) 阈值而存在限制。
- (*, 239.1.1.40) 和 (* , 239.2.2.1) - IP 组播路由表中的条目。条目包含源的 IP 地址，后面紧跟组播组的 IP 地址。用星号 (*) 代替源则表示所有源。
- RP - RP 的地址。对于在稀疏模式下运行的路由器和访问服务器，此地址始终为 224.0.0.0。
- 传入接口 - 来自源的组播数据包的预期接口。如果在此接口上未接收到数据包，系统会将其丢弃。
- RPF nbr - 上游路由器相对于源的 IP 地址。
- 传出接口 — 通过其转发数据包的接口。

Related Commands

命令	Description
show running-config mroute	显示已配置的组播路由。

show nameif

要查看接口的逻辑名称，请使用 **show nameif** 命令。

show nameif [*physical_interface*[**.***subinterface*] | **zone**]

Syntax Description

physical_interface	（可选）标识接口 ID，例如 **gigabitethernet0/1**。
subinterface	（可选）识别一个介于 1 到 4294967293 之间整数，用以指定逻辑子接口。
zone	（可选）显示区域和内联集名称。

Command Default

如果不指定接口，此命令将显示所有接口名称。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用此命令可显示分配给接口的名称。必须为接口命名才能在任何配置设置中使用它。它还显示接口的安全级别， threat defense始终为 0。

如果添加**zone**关键字，则“区域名称”列指示接口所属的内联集或流量区域。流量区域与安全区域不同，因此如果没有被动接口或内联集，即使接口属于路由或交换安全区域，该列也可能为空。使用设备管理器确定哪些安全区域包含每个接口。

示例

以下是 **show nameif** 命令的输出示例：

```
> show nameif
Interface                Name                    Security
GigabitEthernet1/1       outside                   0
GigabitEthernet1/2       inside1_2                 0
GigabitEthernet1/3       inside1_3                 0
GigabitEthernet1/4       inside1_4                 0
GigabitEthernet1/5       inside1_5                 0
GigabitEthernet1/6       inside1_6                 0
GigabitEthernet1/7       inside1_7                 0
GigabitEthernet1/8       inside1_8                 0
Management1/1            diagnostic                0
BVI1                     inside                    0
```

以下是显示区域成员身份的示例输出。在本示例中，2个接口位于内联集中，一个接口位于被动流量区域。

```
> show nameif zone
Interface                Name                    Zone Name           Security
GigabitEthernet0/0       passive                 passive-security-zone
                                                                       0
GigabitEthernet0/1       in                      is-154              0
```

```
GigabitEthernet0/2      out                    is-154              0
Management0/0           diagnostic                                 0
```

show nat

要显示 NAT 策略的统计信息，请使用 **show nat** 命令。

show nat [**interface** *name*] [*ip_addr* [*mask*] | {**object** | **object-group**} *name*] [**translated** [**interface** *name*] {*ip_addr* [*mask*] | {**object** | **object-group**} *name*}] [**detail**]

Syntax Description

detail	（可选）包括对象字段更详细的扩展。
interface *name*	（可选）指定源接口。
ip_addr [*mask*]	（可选）指定 IP 地址和子网掩码。
object *name*	（可选）指定网络对象或服务对象。
object-group *name*	（可选）指定网络对象组
translated	（可选）指定转换参数。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用 **show nat** 命令以显示 NAT 策略的运行时间表示。使用 **detail** 可选关键字以展开对象并查看对象值。使用其他选择器字段以限制 **show nat** 命令输出。

输出显示所有 NAT 命令，甚至是隐藏的命令。例如，如果将管理接口配置为使用数据接口作为网关，则会为隐藏的虚拟接口（例如，nlp_int_tap）创建隐藏的 NAT 规则，以启用管理接口和每个数据接口之间的通信。这些规则不会反映在 设备管理器中的 NAT 表中。您还将看到允许与数据接口建立管理连接的任何 HTTPS/SSH 管理访问规则的隐藏规则，这些规则会反映在 设备管理器的管理访问表中，但不会反映在 NAT 表中。从版本 7.0 开始，系统为自己创建的任何规则都列在第 0 部分中。

示例

以下是 **show nat** 命令的输出示例：

```
> show nat
   Manual NAT Policies (Section 1)
   1 (any) to (any) source dynamic S S' destination static D' D
       translate_hits = 0, untranslate_hits = 0

   Auto NAT Policies (Section 2)
   1 (inside) to (outside) source dynamic A 2.2.2.2
       translate_hits = 0, untranslate_hits = 0

   Manual NAT Policies (Section 3)
   1 (any) to (any) source dynamic C C' destination static B' B service R R'
       translate_hits = 0, untranslate_hits = 0
```

```
> show nat detail
   Manual NAT Policies (Section 1)
   1 (any) to (any) source dynamic S S' destination static D' D
       translate_hits = 0, untranslate_hits = 0
       Source - Real: 1.1.1.2/32, Mapped: 2.2.2.3/32
       Destination - Real: 10.10.10.0/24, Mapped: 20.20.20.0/24

   Auto NAT Policies (Section 2)
   1 (inside) to (outside) source dynamic A 2.2.2.2
       translate_hits = 0, untranslate_hits = 0
       Source - Real: 1.1.1.1/32, Mapped: 2.2.2.2/32

   Manual NAT Policies (Section 3)
   1 (any) to (any) source dynamic C C' destination static B' B service R R'
       translate_hits = 0, untranslate_hits = 0
       Source - Real: 11.11.11.10-11.11.11.11, Mapped: 192.168.10.10/32
       Destination - Real: 192.168.1.0/24, Mapped: 10.75.1.0/24
       Service - Real: tcp source eq 10 destination eq ftp-data , Mapped: tcp source eq
       100 destination eq 200
```

以下是 **show nat detail** 命令在 IPv6 与 IPv4 之间的输出示例：

```
> show nat detail
1 (in) to (outside) source dynamic inside_nw outside_map destination static inside_map any
translate_hits = 0, untranslate_hits = 0
Source - Origin: 2001::/96, Translated: 192.168.102.200-192.168.102.210
Destination - Origin: 2001::/96, Translated: 0.0.0.0/0
```

以下示例显示第 0 部分中系统定义的规则。

```
> show nat detail
Manual NAT Policies Implicit (Section 0)
1 (nlp_int_tap) to (inside) source static nlp_server_0_snmp_intf3 interface  service udp
snmp snmp
    translate_hits = 1, untranslate_hits = 1
    Source - Origin: 169.254.1.2/32, Translated: 10.1.1.122/24
    Service - Protocol: udp Real: snmp Mapped: snmp
2 (nlp_int_tap) to (inside) source dynamic nlp_client_0_intf3 interface
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 169.254.1.2/32, Translated: 10.1.1.122/24

Manual NAT Policies (Section 1)
1 (inside) to (any) source dynamic obj_man interface
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 10.3.3.3/32, Translated: 10.1.1.122/24
```

Related Commands

命令	Description
clear nat counters	清除 NAT 策略计数器。

show nat divert-table

要显示 NAT 转向表的统计信息，请使用 **show nat divert-table** 命令。

show nat divert-table ［**ipv6**］［**interface** *interface_name*］

Syntax Description

divert-table	显示 NAT 转移表。
ipv6	（可选）显示转移表中的 IPv6 条目。
interface *interface_name*	（可选）将输出限制为指定的源接口。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用 **show nat divert-table** 命令显示 NAT 代理 NAT 转移表的运行时表示。使用 **ipv6** 可选关键字以查看转移表中的 IPv6 条目。使用 **interface** 可选关键字以查看特定源接口的 NAT 转向表。

转向表显示所有NAT命令，甚至是隐藏的命令。例如，如果将管理接口配置为使用数据接口作为网关，则会为隐藏的虚拟接口（例如，nlp_int_tap）创建隐藏的 NAT 规则，以启用管理接口和每个数据接口之间的通信。这些规则不会反映在 设备管理器中的 NAT 表中。

示例

以下是 **show nat divert-table** 命令的输出示例：

```
> show nat divert-table
Divert Table
id=0xad1521b8, domain=twice-nat section=1 ignore=no
        type=none, hits=0, flags=0x9, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0-0
        dst ip/id=10.86.119.255, mask=255.255.255.255, port=0-0
        input_ifc=outside, output_ifc=NP Identity Ifc
id=0xad1523a8, domain=twice-nat section=1 ignore=no
        type=none, hits=0, flags=0x9, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0-0
        dst ip/id=10.86.116.0, mask=255.255.255.255, port=0-0
        input_ifc=outside, output_ifc=NP Identity Ifc
id=0xad1865c0, domain=twice-nat section=1 ignore=no
        type=none, hits=0, flags=0x9, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0-0
        dst ip/id=192.168.255.255, mask=255.255.255.255, port=0-0
        input_ifc=amallio-wizard, output_ifc=NP Identity Ifc
id=0xad1867b0, domain=twice-nat section=1 ignore=no
        type=none, hits=0, flags=0x9, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0-0
        dst ip/id=192.168.0.0, mask=255.255.255.255, port=0-0
        input_ifc=amallio-wizard, output_ifc=NP Identity Ifc
id=0xad257bf8, domain=twice-nat section=1 ignore=no
        type=none, hits=0, flags=0x9, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0-0
```

```
        dst ip/id=172.27.48.255, mask=255.255.255.255, port=0-0
        input_ifc=folink, output_ifc=NP Identity Ifc
id=0xad257db8, domain=twice-nat section=1 ignore=no
        type=none, hits=0, flags=0x9, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0-0
        dst ip/id=172.27.48.0, mask=255.255.255.255, port=0-0
        input_ifc=folink, output_ifc=NP Identity Ifc
```

以下是 **show nat divert ipv6** 命令的输出示例：

```
> show nat divert ipv6
Divert Table
id=0xcb9ea518, domain=divert-route
type=static, hits=0, flags=0x21, protocol=0
src ip/id=2001::/ffff:ffff:ffff:ffff:ffff:ffff::, port=0-0
dst ip/id=2001::/ffff:ffff:ffff:ffff:ffff:ffff::, port=0-0
input_ifc=in, output_ifc=outside
id=0xcf24d4b8, domain=divert-route
type=static, hits=0, flags=0x20, protocol=0
src ip/id=::/::, port=0-0
dst ip/id=2222::/ffff:ffff:ffff:ffff:ffff:ffff::, port=0-0
input_ifc=in, output_ifc=mgmt
```

Related Commands

命令	Description
clear nat counters	清除 NAT 策略计数器。
show nat	显示 NAT 策略的运行时间表示。

show nat pool

要显示 NAT 池使用情况的统计信息，请使用 **show nat pool** 命令。

show nat pool ［ **interface** *if-name* ［ **ip** *address* ］ | **ip** *address* | **detail** ］

show nat pool cluster ［ **summary** | **interface** *if-name* ［ **ip** *address* ］ | **ip** *address* ］

Syntax Description

cluster	（可选）启用群集技术后，将显示当前分配到所有者设备和备用设备的 PAT 地址。 (6.7+) 包括 **summary** 关键字，以查看集群中设备之间的端口块分布情况。
interface *if_name*	将显示限制为指定接口的池。您可以选择包含 **ip** 关键字以进一步限制视图。
ip 地址	将显示限制为 PAT 池中的指定 IP 地址。
detail	显示与集群内端口块的使用和分布相关的信息。仅当设备是集群成员时，才会显示此关键字。不能将其与集群关键字一起使用。

Command History

版本	修改
6.1	引入了此命令。
6.7	添加了以下关键字： **interface**、 **ip**、 **detail**、 **summary**。

使用指南

(Pre-6.7) 为每个映射的协议/IP 地址/端口范围创建 NAT 池，其中端口范围默认为 1-511、512-1023 和 1024-65535。如果将 PAT 池配置为使用平面范围的端口，则会看到更少、更大的范围。

(6.7+) 从 6.7 开始，端口范围默认为平面，您可以选择在池中包含保留的端口 1-1023。对于集群系统，PAT 池以 512 个端口为一组分布在集群成员之间。

每个 NAT 池在上次使用后存在至少 10 分钟。如果您使用 **clear xlate**清除转换，则 10 分钟抑制计时器将被取消。

示例

以下是 **show running-config object network** 命令显示的动态 PAT 规则创建的 NAT 池的输出示例。

```
> show running-config object network
object network myhost
 host 10.10.10.10
 nat (pppoe2,inside) dynamic 10.76.11.25

> show nat pool
TCP inside, address 10.76.11.25, range 1-511, allocated 0
TCP inside, address 10.76.11.25, range 512-1023, allocated 0
```

```
TCP inside, address 10.76.11.25, range 1024-65535, allocated 1
```

以下是 **show nat pool** 命令展示如何使用 PAT 池 **flat** 选项的输出示例。如果没有 **include-reserve** 关键字，则显示两个范围；低于 1024 的源端口映射到同一端口时使用较低的范围。

```
> show nat pool
ICMP PAT pool dynamic-pat, address 172.16.2.200, range 1-65535, allocated 2
TCP PAT pool dynamic-pat, address 172.16.2.200, range 1-1024, allocated 0
TCP PAT pool dynamic-pat, address 172.16.2.200, range 1024-65535, allocated 2
UDP PAT pool dynamic-pat, address 172.16.2.200, range 1-1024, allocated 0
UDP PAT pool dynamic-pat, address 172.16.2.200, range 1024-65535, allocated 2
```

以下是 **show nat pool** 命令的输出示例，显示了 PAT 池 **flat include-reserve** 选项的使用。

```
> show nat pool
ICMP PAT pool dynamic-pat, address 172.16.2.200, range 1-65535, allocated 2
TCP PAT pool dynamic-pat, address 172.16.2.200, range 1-65535, allocated 2
UDP PAT pool dynamic-pat, address 172.16.2.200, range 1-65535, allocated 2
```

(Pre-6.7) 以下是 **show nat pool** 命令的输出示例，其中显示了 PAT 池 **extended flat include-reserve** 选项的使用。重要的项目是括号内的地址。这些是用于扩展 PAT 的目标地址。

```
ICMP PAT pool dynamic-pat, address 172.16.2.200, range 1-65535, allocated 0
ICMP PAT pool dynamic-pat, address 172.16.2.200(172.16.2.99), range 1-65535,
allocated 2
TCP PAT pool dynamic-pat, address 172.16.2.200(172.16.2.100), range 1-65535,
allocated 1
UDP PAT pool dynamic-pat, address 172.16.2.200(172.16.2.100), range 1-65535,
allocated 1
TCP PAT pool dynamic-pat, address 172.16.2.200, range 1-65535, allocated 0
ICMP PAT pool dynamic-pat, address 172.16.2.200(172.16.2.100), range 1-65535,
allocated 1
TCP PAT pool dynamic-pat, address 172.16.2.200(172.16.2.99), range 1-65535,
allocated 2
UDP PAT pool dynamic-pat, address 172.16.2.200, range 1-65535, allocated 0
```

(6.7+) 以下示例显示了端口块的分布情况（显示端口范围）及其在集群中的使用情况，包括拥有该块的设备和该块的备用设备。

```
> show nat pool cluster
IP outside_a:src_map_a 174.0.1.20
               [1536  -  2047], owner A, backup B
               [8192  -  8703], owner A, backup B
               [4089  -  4600], owner B, backup A
               [11243  -  11754], owner B, backup A
IP outside_a:src_map_a 174.0.1.21
               [1536  -  2047], owner A, backup B
               [8192  -  8703], owner A, backup B
               [4089  -  4600], owner B, backup A
               [11243  -  11754], owner B, backup A
IP outside_b:src_map_b 174.0.1.22
               [6656 - 7167], owner A, backup B
               [13312 - 13823], owner A, backup B
```

```
               [20480 - 20991], owner B, backup A
               [58368 - 58879], owner B, backup A
IP outside_b:src_map_b 174.0.1.23
               [46592 - 47103], owner A, backup B
               [52224 - 52735], owner A, backup B
               [62976 - 63487], owner B, backup A
```

(6.7+) 以下示例显示集群中的池分配摘要。

```
> show nat pool cluster summary
port-blocks count display order: total, unit-A, unit-B, unit-C, unit-D
IP outside_a:src_map_a, 174.0.1.20 (128 - 32/32/32/32)
IP outside_a:src_map_a, 174.0.1.21 (128 - 36/32/32/28)
IP outside_b:src_map_b, 174.0.1.22 (128 - 31/32/32/33)
```

(6.7+) 以下示例显示了集群中池的 PAT 池的详细使用情况。查看详细输出时，备份端口范围用星号表示。例如：范围 63464-62975，已分配 27 *

```
> show nat pool detail
TCP PAT pool outside_a, address 174.0.1.1
                 range 1536-2047, allocated 56
                 range 8192-8703, allocated 16
UDP PAT pool outside_a, address 174.0.1.1
                 range 1536-2047, allocated 12
                 range 8192-8703, allocated 25
 TCP PAT pool outside_b, address 174.0.2.1
                 range 47104-47615, allocated 39
                 range 62464-62975, allocated 9
UDP PAT pool outside_b, address 174.0.2.1
                 range 47104-47615, allocated 35
                 range 62464-62975, allocated 27
```

(6.7+) 以下示例显示如何将视图限制为特定设备上的特定接口。

```
> show nat pool interface outside_b ip 174.0.2.1
TCP PAT pool outside_b, address 174.0.2.1, range 1-511, allocated 0
TCP PAT pool outside_b, address 174.0.2.1, range 512-1023, allocated 12
TCP PAT pool outside_b, address 174.0.2.1, range 1024-65535, allocated 48
UDP PAT pool outside_b, address 174.0.2.1, range 1-511, allocated 6
UDP PAT pool outside_b, address 174.0.2.1, range 512-1023, allocated 8
UDP PAT pool outside_b, address 174.0.2.1, range 1024-65535, allocated 62
```

Related Commands

命令	Description
show nat	显示 NAT 策略统计信息。

show nat proxy-arp

要显示 NAT 代理 ARP 表，请使用 **show nat proxy-arp** 命令。

show nat proxy-arp ［**ipv6**］［**interface** *name*］

Syntax Description

ipv6	（可选）显示代理 ARP 表中的 IPv6 条目。
interface *name*	（可选）将输出限制为指定的源接口。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用 **show nat proxy-arp** 命令显示 NAT 代理 ARP 表的运行时间表示。

代理 ARP 表显示所有 NAT 命令，甚至是隐藏的命令。例如，如果将管理接口配置为使用数据接口作为网关，则会为隐藏的虚拟接口（例如，nlp_int_tap）创建隐藏的 NAT 规则，以启用管理接口和每个数据接口之间的通信。这些规则不会反映在 设备管理器中的 NAT 表中。

示例

以下是 **show nat proxy-arp** 命令的输出示例：

```
> show nat proxy-arp
Nat Proxy-arp Table
id=0x00007f4ce491a010, ip/id=0.0.0.0, mask=255.255.255.255 ifc=outside
        config:(inside1_8) to (outside) source dynamic any-ipv4 interface
id=0x00007f4cdc6138d0, ip/id=0.0.0.0, mask=255.255.255.255 ifc=outside
        config:(inside1_7) to (outside) source dynamic any-ipv4 interface
id=0x00007f4ce491d2e0, ip/id=0.0.0.0, mask=255.255.255.255 ifc=outside
        config:(inside1_6) to (outside) source dynamic any-ipv4 interface
id=0x00007f4cdc618a10, ip/id=0.0.0.0, mask=255.255.255.255 ifc=outside
        config:(inside1_5) to (outside) source dynamic any-ipv4 interface
id=0x00007f4d019c9e70, ip/id=0.0.0.0, mask=255.255.255.255 ifc=outside
        config:(inside1_4) to (outside) source dynamic any-ipv4 interface
id=0x00007f4cdc61b300, ip/id=0.0.0.0, mask=255.255.255.255 ifc=outside
        config:(inside1_3) to (outside) source dynamic any-ipv4 interface
id=0x00007f4ce49261f0, ip/id=0.0.0.0, mask=255.255.255.255 ifc=outside
        config:(inside1_2) to (outside) source dynamic any-ipv4 interface
```

Related Commands

命令	Description
clear nat counters	清除 NAT 策略计数器。
show nat	显示 NAT 策略的运行时间表示。

show network

要显示管理接口的属性，请使用 **show network** 命令。

show network

Command History

版本	修改
6.1	引入了此命令。
6.7	此命令现在显示管理和 管理中心 访问数据接口网络设置。

使用指南

使用此命令可查看使用 **configure network** 命令设置的管理接口属性。

如果将管理地址配置为使用数据接口作为网关，则网关显示为“数据接口”。

示例

以下是 **show network** 命令的输出示例。

```
> show network
===============[ System Information ]===============
Hostname                : 5516X-4
DNS Servers             : 208.67.220.220,208.67.222.222
Management port         : 8305
IPv4 Default route
  Gateway               : data-interfaces
IPv6 Default route
  Gateway               : data-interfaces

=====================[ br1 ]=====================
State                   : Enabled
Link                    : Up
Channels                : Management & Events
Mode                    : Non-Autonegotiation
MDI/MDIX                : Auto/MDIX
MTU                     : 1500
MAC Address             : 28:6F:7F:D3:CB:8D
---------------------[ IPv4 ]---------------------
Configuration           : Manual
Address                 : 10.99.10.4
Netmask                 : 255.255.255.0
Gateway                 : 10.99.10.1
---------------------[ IPv6 ]---------------------
Configuration           : Disabled

===============[ Proxy Information ]================
State                   : Disabled
Authentication          : Disabled

======[ System Information - Data Interfaces ]======
DNS Servers             :
Interfaces              : GigabitEthernet1/1

===============[ GigabitEthernet1/1 ]===============
```

```
State                       : Enabled
Link                        : Up
Name                        : outside
MTU                         : 1500
MAC Address                 : 28:6F:7F:D3:CB:8F
----------------------[ IPv4 ]----------------------
Configuration               : Manual
Address                     : 10.89.5.29
Netmask                     : 255.255.255.192
Gateway                     : 10.89.5.1
----------------------[ IPv6 ]----------------------
Configuration               : Disabled
```

show network-dhcp-server

要在管理接口上显示 DHCP 服务器的状态，请使用 **show network-dhcp-server** 命令。

show network-dhcp-server

Command History

版本	修改
6.2	引入了此命令。

使用指南

使用此命令可查看管理接口的可选 DHCP 服务器的状态。要配置 DHCP 服务器，请使用 **configure network ipv4 dhcp-server-enable** 命令。

输出显示 DHCP 服务器是已启用还是已禁用。如果启用，它还会显示地址池。

示例

以下示例显示如何配置 DHCP 服务器并显示其状态。

```
> show network-dhcp-server
DHCP Server Disabled
> configure network ipv4 dhcp-server-enable 192.168.45.46 192.168.45.254
DHCP Server Enabled
> show network-dhcp-server
DHCP Server Enabled
192.168.45.46-192.168.45.254
```

Related Commands

命令	Description
configure network ipv4 dhcp-server-enable	配置管理接口上的 DHCP 服务器。
configure network ipv4 dhcp-server-disable	禁用管理接口上的 DHCP 服务器。

show network-static-routes

要显示管理接口配置的静态路由，请使用 **show network-static-routes** 命令。

show network-static-routes

Command History

版本	修改
6.1	引入了此命令。

使用指南

配置多个管理接口时，使用管理接口的静态路由。这些路由不包括默认网关。如果使用单个管理接口，通常不会有其他静态路由。

使用此命令显示的路由仅适用于管理接口。任何数据接口都不使用它们。它们不用于通过设备的流量。

示例

以下示例显示管理接口没有其他静态路由。默认网关是唯一的路由。

```
> show network-static-routes
No static routes currently configured.
```

以下示例显示一个静态路由。

```
> show network-static-routes
---------------[ IPv4 Static Routes ]---------------
Interface                : br1
Destination              : 10.1.1.0
Gateway                  : 192.168.0.254
Netmask                  : 255.255.255.0
```

Related Commands

命令	Description
configure network static-routes	为管理接口配置静态路由。

show ntp

要显示当前的网络时间协议 (NTP) 服务器和配置，请使用 **show ntp** 命令。

show ntp

Command History

版本	修改
6.1	引入了此命令。

使用指南

此命令显示有关 NTP 服务器的基本信息。如果您需要更全面的信息，请使用 **system support ntp** 命令，包括此命令的输出以及标准 NTP 命令 **ntpq**（该命令记录在 NTP 协议中）的输出。

示例

以下示例显示如何显示 NTP 配置。

```
> show ntp
NTP Server                : 209.208.79.69
Status                    : Available
Offset                    : -1.614 (milliseconds)
Last Update               : 578 (seconds)

NTP Server                : 45.127.112.2  (clocka.ntpjs.org)
Status                    : Available
Offset                    : -1.355 (milliseconds)
Last Update               : 874 (seconds)

NTP Server                : 198.58.105.63  (ha81.smatwebdesign.com)
Status                    : Not Available
Offset                    : -4.942 (milliseconds)
Last Update               : 369 (seconds)

NTP Server                : 204.9.54.119  (ntp.your.org)
Status                    : Being Used
Offset                    : 0.312 (milliseconds)
Last Update               : 962 (seconds)
```

以下示例显示如何使用 **system support ntp** 命令获取其他信息。如果需要确认 NTP 同步，请使用此命令。

查找“Results of ‘ntpq -pn’”部分。例如，您可能会看到类似如下的内容：

```
> system support ntp
... output redacted ...
Results of 'ntpq -pn'
remote                    : +216.229.0.50
refid                     : 129.7.1.66
st                        : 2
t                         : u
when                      : 704
poll                      : 1024
reach                     : 377
```

```
delay                       : 90.455
offset                      : 2.954
jitter                      : 2.473
... remaining output redacted ...
```

在本例中，NTP 服务器地址前的 + 表示作为潜在候选者。此处的星号 * 表示当前的时间源对等体。

NTP 后台守护程序 (NTPD) 使用每个对等体中的八个示例的滑动窗口，并选出一个示例，然后根据时钟选择确定正确的报时器和错误的断续器。然后，NTPD 会确定往返距离（候补者的偏移不得超过往返延迟的一半）。如果连接延迟、丢包或服务器问题导致一个或全部候补者被拒绝，则同步中会出现较长的延迟。而且，该调整很长一段时间后才会完成：时钟偏移和振荡器错误必须通过时钟训练算法解决，这可能会需要数小时的时间。

注释 如果 refid 是 .LOCL.，则表明对等体是一个未经训练的本地时钟，也即它只使用其本地时钟来设置时间。如果所选的对等体是 .LOCL.，则 设备管理器 始终将 NTP 连接标为黄色（未同步）。如果还有更好的证书，NTP 通常不会选择 .LOCL. 证书，这就是应配置至少三个服务器的原因所在。

Related Commands

命令	Description
system support ntp	显示 NTP 的详细故障排除信息。

show object

要显示有关网络服务对象的信息（包括命中计数和 IP 地址），请使用 **show object** 命令。

show object [**id** *object_name* | **network-service** [**detail**]]

Syntax Description

id *name*	（可选）要查看的对象的名称。大小写很重要。例如，“object-name”与“Object-Name”不匹配。
network-service [**detail**]	（可选。）显示所有网络服务对象。包括细节关键字以查看与对象成员关联的缓存 IP 地址。

Command Default

如果没有参数，则显示所有对象。

Command History

版本	修改
7.1	引入了此命令。

示例

以下示例显示名为 Cisco 的网络服务对象的详细信息。app-id（应用 ID）是内部编号。hitcnt（命中计数）是显示的唯一相关指标。

```
> show object id Cisco
object network-service "Cisco" dynamic
 description Official website for Cisco.
 app-id 2655
 domain cisco.com (bid=0) ip (hitcnt=0)
```

Related Commands

命令	Description
clear object	清除网络服务对象命中计数。
show object-groups	显示网络服务对象组和命中计数。

show object-group

要显示对象组信息和相关命中计数（如果对象组为 network 或 network-service object-group 类型），请使用 **show object-group** 命令。使用不带参数的 命令可查看所有类型的对象组。

show object-group [**count** | **interface** | **network** | **security** | **service** | **id** *name*]

show object-group network-service [*group_name* [**network-service-member** *member_name* [**dns** *domain_name*]] [**detail**]

Syntax Description

count	（可选。）显示与对象组数量和这些组中的对象数量相关的统计信息，以及它们的使用方式。
detail	对于网络服务对象，显示与对象成员关联的缓存 IP 地址。
dns *domain_name*	（可选。）对于按名称和成员指定的网络服务对象，将信息限制为该成员的特定域。例如 example.com。
id *name*	（可选）按名称标识对象组。
interface	（可选）接口类型对象
network	（可选）网络类型对象。
network-service [*group_name*]	（可选。）网络服务对象。您可以指定对象名称以将信息限制为单个对象。
network-service-member *member_name*	（可选。）对于按名称指定的网络服务对象，将信息限制为该对象的特定成员。
security	（可选）安全类型对象
service	（可选）服务类型对象。

Command History

版本	修改
6.1	引入了此命令。
7.1	我们添加了 **network-service** 关键字及其关联的参数。
7.2	添加了 **count** 关键字。

示例

以下是 **show object-group** 命令的输出示例，显示关于名为“Anet”的网络对象组的信息：

```
> show object-group id Anet
```

```
Object-group network Anet (hitcnt=10)
   Description OBJ SEARCH ALG APPLIED
   network-object 1.1.1.0 255.255.255.0 (hitcnt=4)
   network-object 2.2.2.0 255.255.255.0 (hitcnt=6)
```

以下是 **show object-group** 命令的输出示例，显示关于服务组的信息：

```
> show object-group service
object-group service B-Serobj
   description its a service group
   service-object tcp eq bgp
```

以下示例显示了网络服务对象及其命中计数。网络服务组 ID (nsg-id)、应用 ID (app-id) 和出价等各种标识符是可以忽略的内部索引编号。

```
> show object-group network-service FMC_NSG_4294969442
object-group network-service FMC_NSG_4294969442 (nsg-id 512/1)
 network-service-member "Facebook" dynamic
  description Facebook is a social networking service.
  app-id 629
  domain connect.facebook.net (bid=214491) ip (hitcnt=0)
  domain facebook.com (bid=370809) ip (hitcnt=0)
  domain fbcdn.net (bid=490321) ip (hitcnt=0)
  domain fbcdn-photos-a.akamaihd.net (bid=548791) ip (hitcnt=0)
  domain fbcdn-photos-e-a.akamaihd.net (bid=681143) ip (hitcnt=0)
  domain fbcdn-photos-b-a.akamaihd.net (bid=840741) ip (hitcnt=0)
  domain fbstatic-a.akamaihd.net (bid=1014669) ip (hitcnt=0)
  domain fbexternal-a.akamaihd.net (bid=1098051) ip (hitcnt=0)
  domain fbcdn-profile-a.akamaihd.net (bid=1217875) ip (hitcnt=0)
  domain fbcdn-creative-a.akamaihd.net (bid=1379985) ip (hitcnt=0)
  domain channel.facebook.com (bid=1524617) ip (hitcnt=0)
  domain fbcdn-dragon-a.akamaihd.net (bid=1683343) ip (hitcnt=0)
  domain contentcache-a.akamaihd.net (bid=1782703) ip (hitcnt=0)
  domain facebook.net (bid=1868733) ip (hitcnt=0)
 network-service-member "Google+ Videos" dynamic
  description Video sharing among Google+ community.
  app-id 2881
  domain plus.google.com (bid=2068293) ip (hitcnt=0)
 network-service-member "Instagram" dynamic
  description Mobile phone photo sharing.
  app-id 1233
  domain instagram.com (bid=2176667) ip (hitcnt=0)
 network-service-member "LinkedIn" dynamic
  description Career oriented social networking.
  app-id 713
  domain linkedin.com (bid=2317259) ip (hitcnt=0)
>
```

以下示例显示了对象计数，以便您了解对象组的数量、组中包含的对象数量以及ACL、NAT等中使用的对象数量。此信息与对象组搜索功能的性能相关。

```
ciscoasa(config)# show object-group count

Object Group Name                     Group Count Dyn Count V4 CNT     V6 CNT     ACL CNT
    NAT CNT    OG in OG
network    i28Z-route                 68          0          68         0          0
      0          0
network    i28Z-VRF-BGP-PEERS         4           0          4          0          2
      0          0
network    EXCH-BGP-PEERS             4           0          4          0          2
```

```
      0          0
network    obgr_SUBNETS_NO_ACL         112          0           112          0          0
      0          0
network    obgr_SUBNETS_ACL_ASAMgmt    1            0           1            0          0
      0          0
network    obgr_CLIENTS_ACL_ASAMgmt    8            0           8            0          1
      0          0
network    obgr_SUBNETS_CGS_vMotion    1            0           1            0          0
      0          0
network    obgr_CLIENTS_CGS_vMotion    9            0           9            0          1
      0          0
network    obgr_SUBNETS_UPMCOD_CGS     17           0           17           0          0
      0          0
network    obgr_CLIENTS_UPMCOD_CGS     90           0           90           0          1
      0          0
network    obgr_CLIENTS_10.68.0.0_16   2            0           2            0          1
      0          0
network    obgr_CLIENTS_10.68.1.198_31 4            0           4            0          1
      0          0
network    obgr_CLIENTS_10.68.73.133   7            0           7            0          1
      0          0
network    asa_zabbix_proxies          4            0           4            0          1
      0          0

Total Summary
Object-group count                          14
Object-group object count                   331
Object-group Dynamic count                  0
Object-group IPv4 count                     331
Object-group IPv6 count                     0
Object-group Used in ACL                    9
Object-group Used in NAT                    0
Object-group Unused                         5
Object-group Internal                       0
Object-group Dummy                          0
Redundant object-group in Network           4
Redundant object-group in IfC               0
```

Related Commands

命令	Description
clear object-group	清除指定对象组的网络对象命中计数。
show access-list	显示所有访问列表、相关扩展访问列表条目以及命中计数。
show object	显示网络服务对象和命中计数。

show ospf

要显示有关 OSPF 路由流程的一般信息，请使用 **show ospf** 命令。

show ospf ［**vrf** *name* | **all**］ ［*pid* ［*area_id*］］

Syntax Description

area_id	（可选）与 OSPF 地址范围关联的区域的 ID。
pid	（可选）OSPF 流程的 ID。
［**vrf** *name*	**all**］	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将该命令限制为特定虚拟路由器。如果您希望 命令影响所有虚拟路由器，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则 命令适用于全局 VRF 虚拟路由器。

Command History

版本	修改
6.1	引入了此命令。
6.6	添加了 ［**vrf** *name*	**all**］ 关键字。

示例

以下是 **show ospf** 命令的输出示例，展示如何显示关于特定 OSPF 路由流程的一般信息：

```
> show ospf 5
 Routing Process "ospf 5" with ID 127.0.0.1 and Domain ID 0.0.0.5
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x     0
 Number of opaque AS LSA 0. Checksum Sum 0x     0
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 0. 0 normal 0 stub 0 nssa
 External flood list length 0
```

以下是 **show ospf** 命令的输出示例，展示如何显示关于所有 OSPF 路由流程的一般信息：

```
> show ospf
 Routing Process "ospf 5" with ID 127.0.0.1 and Domain ID 0.0.0.5
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x     0
 Number of opaque AS LSA 0. Checksum Sum 0x     0
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
```

```
Number of areas in this router is 0. 0 normal 0 stub 0 nssa
External flood list length 0

Routing Process "ospf 12" with ID 172.23.59.232 and Domain ID 0.0.0.12
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x     0
Number of opaque AS LSA 0. Checksum Sum 0x     0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 0. 0 normal 0 stub 0 nssa
External flood list length 0
```

show ospf border-routers

要向 ABR 和 ASBR 显示内部 OSPF 路由表条目，请使用 **show ospf border-routers** 命令。

show ospf border-routers ［**vrf** *name* | **all**］

Syntax Description

［**vrf** *name*	**all**］	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将该命令限制为特定虚拟路由器。如果您希望 命令影响所有虚拟路由器，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则 命令适用于全局 VRF 虚拟路由器。

Command History

版本	修改
6.1	引入了此命令。
6.6	添加了 ［**vrf** *name*	**all**］ 关键字。

示例

以下是 **show ospf border-routers** 命令的输出示例：

```
> show ospf border-routers

OSPF Process 109 internal Routing Table

Codes: i - Intra-area route, I - Inter-area route

i 192.168.97.53 [10] via 192.168.1.53, fifth, ABR, Area 0, SPF 20
i 192.168.103.51 [10] via 192.168.96.51, outside, ASBR, Area 192.168.12.0, SPF 14
i 192.168.103.52 [10] via 192.168.96.51, outside, ABR/ASBR, Area 192.168.12.0, SPF 14
```

show ospf database

要显示 OSPF 拓扑数据库中包含的信息，请使用 **show ospf database** 命令。

show ospf ［**vrf** *name* | **all**］ ［*pid* ［*area_id*］］ **database** ［**router** | **network** | **summary** | **asbr-summary** | **external** | **nssa-external**］［*lsid*］［**internal**］［**self-originate** | **adv-router** *addr*］
show ospf ［*pid* ［*area_id*］］ **database database-summary**

Syntax Description

addr	（可选）路由器地址。
adv-router	（可选）通告的路由器。
area_id	（可选）与 OSPF 地址范围关联的区域的 ID。
asbr-summary	（可选）显示 ASBR 列表摘要。
database	显示数据库信息。
database-summary	（可选）显示完整的数据库摘要列表。
external	（可选）显示指定自主系统外部的路由。
internal	（可选）指定自主系统内部的路由。
lsid	（可选）LSA ID。
network	（可选）显示有关网络 LSA 的信息。
nssa-external	（可选）显示外部末节区域列表。
pid	（可选）OSPF 进程的 ID。
router	（可选）显示路由器。
self-originate	（可选）显示指定自主系统的信息。
summary	（可选）显示列表的摘要。
［**vrf** *name*	**all**］	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将该命令限制为特定虚拟路由器。如果您希望 命令影响所有虚拟路由器，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则 命令适用于全局 VRF 虚拟路由器。

Command History

版本	修改
6.1	引入了此命令。
6.6	添加了 ［**vrf** *name*	**all**］ 关键字。

示例

以下是 **show ospf database** 命令的输出示例：

```
> show ospf database
OSPF Router with ID(192.168.1.11) (Process ID 1)

                Router Link States(Area 0)
Link ID   ADV Router   Age   Seq# Checksum Link count
192.168.1.8 192.168.1.8 1381 0x8000010D    0xEF60 2
192.168.1.11 192.168.1.11 1460 0x800002FE    0xEB3D 4
192.168.1.12 192.168.1.12 2027 0x80000090    0x875D 3
192.168.1.27 192.168.1.27 1323 0x800001D6    0x12CC 3

                Net Link States(Area 0)
Link ID ADV Router   Age   Seq# Checksum
172.16.1.27 192.168.1.27 1323 0x8000005B    0xA8EE
172.17.1.11 192.168.1.11 1461 0x8000005B    0x7AC

                Type-10 Opaque Link Area Link States (Area 0)
Link ID ADV Router   Age Seq# Checksum Opaque ID
10.0.0.0 192.168.1.11 1461 0x800002C8    0x8483   0
10.0.0.0 192.168.1.12 2027 0x80000080    0xF858   0
10.0.0.0 192.168.1.27 1323 0x800001BC    0x919B   0
10.0.0.1 192.168.1.11 1461 0x8000005E    0x5B43   1
```

以下是 **show ospf database asbr-summary** 命令的输出示例：

```
> show ospf database asbr-summary
OSPF Router with ID(192.168.239.66) (Process ID 300)
Summary ASB Link States(Area 0.0.0.0)
Routing Bit Set on this LSA
LS age: 1463
Options: (No TOS-capability)
LS Type: Summary Links(AS Boundary Router)
Link State ID: 172.16.245.1 (AS Boundary Router address)
Advertising Router: 172.16.241.5
LS Seq Number: 80000072
Checksum: 0x3548
Length: 28
Network Mask: 0.0.0.0
TOS: 0 Metric: 1
```

以下是 **show ospf database router** 命令的输出示例：

```
> show ospf database router
OSPF Router with id(192.168.239.66) (Process ID 300)
Router Link States(Area 0.0.0.0)
Routing Bit Set on this LSA
LS age: 1176
Options: (No TOS-capability)
LS Type: Router Links
Link State ID: 10.187.21.6
Advertising Router: 10.187.21.6
LS Seq Number: 80002CF6
Checksum: 0x73B7
Length: 120
AS Boundary Router
```

```
Number of Links: 8
Link connected to: another Router (point-to-point)
(link ID) Neighboring Router ID: 10.187.21.5
(Link Data) Router Interface address: 10.187.21.6
Number of TOS metrics: 0
TOS 0 Metrics: 2
```

以下是 **show ospf database network** 命令的输出示例：

```
> show ospf database network
OSPF Router with id(192.168.239.66) (Process ID 300)
Displaying Net Link States(Area 0.0.0.0)
LS age: 1367
Options: (No TOS-capability)
LS Type: Network Links
Link State ID: 10.187.1.3 (address of Designated Router)
Advertising Router: 192.168.239.66
LS Seq Number: 800000E7
Checksum: 0x1229
Length: 52
Network Mask: 255.255.255.0
Attached Router: 192.168.239.66
Attached Router: 10.187.241.5
Attached Router: 10.187.1.1
Attached Router: 10.187.54.5
Attached Router: 10.187.1.5
```

以下是 **show ospf database summary** 命令的输出示例：

```
> show ospf database summary
OSPF Router with id(192.168.239.66) (Process ID 300)
Displaying Summary Net Link States(Area 0.0.0.0)
LS age: 1401
Options: (No TOS-capability)
LS Type: Summary Links(Network)
Link State ID: 10.187.240.0 (summary Network Number)
Advertising Router: 10.187.241.5
LS Seq Number: 80000072
Checksum: 0x84FF
Length: 28
Network Mask: 255.255.255.0 TOS: 0 Metric: 1
```

以下是 **show ospf database external** 命令的输出示例：

```
> show ospf database external
OSPF Router with id(192.168.239.66) (Autonomous system 300)

                  Displaying AS External Link States
LS age: 280
Options: (No TOS-capability)
LS Type: AS External Link
Link State ID: 172.16.0.0 (External Network Number)
Advertising Router: 10.187.70.6
LS Seq Number: 80000AFD
Checksum: 0xC3A
Length: 36
Network Mask: 255.255.0.0

      Metric Type: 2 (Larger than any link state path)
```

```
TOS: 0
Metric: 1
Forward Address: 0.0.0.0
External Route Tag: 0
```

show ospf events

要显示 OSPF 内部事件信息，请使用 **show ospf events** 命令。

show ospf ［**vrf** *name* | **all**］ ［*process_id*］ **events** ［*type*］

Syntax Description

process_id	（可选）指定本地分配的内部ID，可以是任何正整数。启用OSPF路由流程时，此 ID 是管理性分配的号码。
type	（可选）要查看的事件类型的列表。如果不指定一种或多种类型，则会看到所有事件。您可以过滤以下类型： • **generic**-通用事件。 • **interface**- 接口状态更改事件。 • **lsa**- LSA 到达和 LSA 生成事件。 • **neighbor**- 邻居状态更改事件。 • **reverse**- 以相反的顺序显示事件。 • **rib**- 路由器信息库更新、删除和重新分发事件。 • **spf**- SPF 计划和 SPF 运行事件。
［**vrf** *name*	**all**］	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将该命令限制为特定虚拟路由器。如果您希望 命令影响所有虚拟路由器，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则 命令适用于全局 VRF 虚拟路由器。

Command History

版本	修改
6.1	引入了此命令。
6.6	添加了 ［**vrf** *name*	**all**］ 关键字。

示例

以下是 **show ospf events** 命令的输出示例：

```
> show ospf events

            OSPF Router with ID (192.168.77.1) (Process ID 5)

  1 Apr 27 16:33:23.556: RIB Redist, dest 0.0.0.0, mask 0.0.0.0, Up
  2 Apr 27 16:33:23.556: Rescanning RIB:  0x00x0
  3 Apr 27 16:33:23.556: Service Redist scan:  0x00x0
```

Related Commands

命令	Description
show ospf	显示 OSPF 路由流程中的所有设置。
show ospf border-routers	显示区域边界路由器 (ABR) 和自主系统边界路由器 (ASBR) 的内部 OSPF 路由表条目。

show ospf flood-list

要显示等待通过接口泛洪的 OSPF LSA 列表，请使用 **show ospf flood-list** 命令。

show ospf flood-list ［**vrf** *name* | **all**］ *interface_name*

Syntax Description

interface_name	要显示邻居信息的接口的名称。
［**vrf** *name*	**all**］	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将该命令限制为特定虚拟路由器。如果您希望 命令影响所有虚拟路由器，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则 命令适用于全局 VRF 虚拟路由器。

Command History

版本	修改
6.1	引入了此命令。
6.6	添加了 ［**vrf** *name*	**all**］ 关键字。

示例

以下是 **show ospf flood-list** 命令的输出示例：

```
> show ospf flood-list outside

  Interface outside, Queue length 20
  Link state flooding due in 12 msec

  Type  LS ID          ADV RTR          Seq NO       Age   Checksum
     5  10.2.195.0     192.168.0.163    0x80000009   0     0xFB61
     5  10.1.192.0     192.168.0.163    0x80000009   0     0x2938
     5  10.2.194.0     192.168.0.163    0x80000009   0     0x757
     5  10.1.193.0     192.168.0.163    0x80000009   0     0x1E42
     5  10.2.193.0     192.168.0.163    0x80000009   0     0x124D
     5  10.1.194.0     192.168.0.163    0x80000009   0     0x134C
```

show ospf interface

要显示 OSPF 相关接口信息，请使用 **show ospf interface** 命令。

show ospf interface ［**vrf** *name* | **all**］ ［*interface_name*］

Syntax Description

interface_name	（可选）要显示 OSPF 相关信息的接口的名称。
［**vrf** *name*	**all**］	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将该命令限制为特定虚拟路由器。如果您希望 命令影响所有虚拟路由器，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则 命令适用于全局 VRF 虚拟路由器。

Command Default

当不指定接口名称时，则会显示所有接口的 OSPF 信息。

Command History

版本	修改
6.1	引入了此命令。
6.6	添加了 ［**vrf** *name*	**all**］ 关键字。

示例

以下是 **show ospf interface** 命令的输出示例：

```
> show ospf interface outside
out is up, line protocol is up
  Internet Address 10.0.3.4 mask 255.255.255.0, Area 0
  Process ID 2, Router ID 10.0.3.4, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State WAITING, Priority 1
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10 msec, Dead 1, Wait 1, Retransmit 5
    Hello due in 5 msec
    Wait time before Designated router selection 0:00:11
  Index 1/1, flood queue length 0
  Next 0x00000000(0)/0x00000000(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

show ospf neighbor

要显示每个接口上的 OSPF 邻居信息，请使用 **show ospf neighbor** 命令。

show ospf neighbor ［**vrf** *name* | **all**］ ［**detail** | *interface_name* ［*nbr_router_id*］］

Syntax Description

detail	（可选）列出指定路由器的详细信息。
interface_name	（可选）要显示邻居信息的接口的名称。
nbr_router_id	（可选）邻居路由器的路由器 ID。
［**vrf** *name*	**all**］	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将该命令限制为特定虚拟路由器。如果您希望 命令影响所有虚拟路由器，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则 命令适用于全局 VRF 虚拟路由器。

Command History

版本	修改
6.1	引入了此命令。
6.6	添加了 ［**vrf** *name*	**all**］ 关键字。

示例

以下是 **show ospf neighbor** 命令的输出示例。它基于每个接口展示如何显示 OSPF 邻居信息。

```
> show ospf neighbor outside

Neighbor 192.168.5.2, interface address 10.225.200.28
    In the area 0 via interface outside
    Neighbor priority is 1, State is FULL, 6 state changes
    DR is 10.225.200.28 BDR is 10.225.200.30
    Options is 0x42
    Dead timer due in 00:00:36
    Neighbor is up for 00:09:46
  Index 1/1, retransmission queue length 0, number of retransmission 1
    First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
    Last retransmission scan length is 1, maximum is 1
    Last retransmission scan time is 0 msec, maximum is 0 msec
```

以下是 **show ospf neighbor detail** 命令的输出示例。它展示如何显示指定 OSPF 邻居的详细信息。

```
> show ospf neighbor detail

Neighbor 25.1.1.60, interface address 15.1.1.60
    In the area 0 via interface inside
```

```
Neighbor priority is 1, State is FULL, 46 state changes
DR is 15.1.1.62 BDR is 15.1.1.60
Options is 0x12 in Hello (E-bit, L-bit)
Options is 0x52 in DBD (E-bit, L-bit, O-bit)
LLS Options is 0x1 (LR), last OOB-Resync 00:03:07 ago
Dead timer due in 0:00:24
Neighbor is up for 01:42:15
Index 5/5, retransmission queue length 0, number of retransmission 0
First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
Last retransmission scan length is 0, maximum is 0
Last retransmission scan time is 0 msec, maximum is 0 msec
```

show ospf nsf

要显示 OSPFv2 相关的 NSF 信息，请使用 **show ospf nsf** 命令。

show ospf nsf ［**vrf** *name* | **all**］

Syntax Description

［**vrf** *name*	**all**］	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将该命令限制为特定虚拟路由器。如果您希望 命令影响所有虚拟路由器，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则 命令适用于全局 VRF 虚拟路由器。

Command History

版本	修改
6.1	引入了此命令。
6.6	添加了 ［**vrf** *name*	**all**］ 关键字。

示例

以下是 **show ospf nsf** 命令的输出示例：

```
> show ospf nsf
Routing Process "ospf 10"
Non-Stop Forwarding enabled
    Clustering is not configured in spanned etherchannel mode
IETF NSF helper support enabled
Cisco NSF helper support enabled
    OSPF restart state is
    Handle 1, Router ID 25.1.1.60, checkpoint Router ID 0.0.0.0
    Config wait timer interval 10, timer not running
    Dbase wait timer interval 120, timer not running
```

show ospf request-list

要显示路由器请求的所有 LSA 的列表，请使用 **show ospf request-list** 命令。

show ospf request-list ［**vrf** *name* | **all**］ *nbr_router_id interface_name*

Syntax Description

interface_name	要显示邻居信息的接口的名称。显示路由器从此接口请求的所有 LSA 的列表。
nbr_router_id	邻居路由器的路由器 ID。显示路由器从此邻居请求的所有 LSA 的列表。
［**vrf** *name*	**all**］	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将该命令限制为特定虚拟路由器。如果您希望 命令影响所有虚拟路由器，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则 命令适用于全局 VRF 虚拟路由器。

Command History

版本	修改
6.1	引入了此命令。
6.6	添加了 ［**vrf** *name*	**all**］ 关键字。

示例

以下是 **show ospf request-list** 命令的输出示例：

```
> show ospf request-list 192.168.1.12 inside

         OSPF Router with ID (192.168.1.11) (Process ID 1)

 Neighbor 192.168.1.12, interface inside address 172.16.1.12

 Type   LS ID          ADV RTR        Seq NO       Age   Checksum
    1   192.168.1.12   192.168.1.12   0x8000020D   8     0x6572
```

Related Commands

命令	Description
show ospf retransmission-list	显示等待重新发送的所有 LSA 的列表。

show ospf retransmission-list

要显示等待为特定邻居和接口重新发送的所有 LSA 的列表，请使用 **show ospf retransmission-list** 命令。

show ospf retransmission-list ［**vrf** *name* | **all**］ *nbr_router_id interface_name*

Syntax Description

interface_name	要显示邻居信息的接口的名称。
nbr_router_id	邻居路由器的路由器 ID。
［**vrf** *name* | **all**］	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将该命令限制为特定虚拟路由器。如果您希望 命令影响所有虚拟路由器，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则 命令适用于全局 VRF 虚拟路由器。

Command History

版本	修改
6.1	引入了此命令。
6.6	添加了 ［**vrf** *name* | **all**］ 关键字。

示例

以下是外部接口上 192.168.1.11 邻居路由器的 **show ospf retransmission-list** 命令输出示例。

```
> show ospf retransmission-list 192.168.1.11 outside

         OSPF Router with ID (192.168.1.12) (Process ID 1)

 Neighbor 192.168.1.11, interface outside address 172.16.1.11

 Link state retransmission due in 3764 msec, Queue length 2
 Type   LS ID          ADV RTR        Seq NO       Age   Checksum
    1   192.168.1.12   192.168.1.12   0x80000210   0     0xB196
```

Related Commands

命令	Description
show ospf request-list	显示路由器请求的所有 LSA 的列表。

show ospf rib

要显示 OSPF 路由器信息库 (RIB)，请使用 **show ospf rib** 命令。

show ospf ［**vrf** *name* | **all**］ ［*process_id* ［*area_id*］］ **rib** ［*network_prefix* ［*network_mask*］］ | **detail** | **redistribution** ［*network_prefix* ［*network_mask*］］ | **detail**］］

Syntax Description

process_id	（可选）OSPF 流程的 ID。
area_id	（可选）与 OSPF 地址范围关联的区域的 ID。
network_prefix [*network_mask*]	（可选）要查看的路由的网络前缀和掩码（可选），例如： 10.100.10.1 10.100.10.0 255.255.255.0
detail	（可选）显示有关 RIB 的详细信息。
redistribution	（可选）显示重新分发信息。您还可以在重新分发 **detail** 关键字后指定网络前缀和掩码或关键字。
［**vrf** *name*	**all**］	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将该命令限制为特定虚拟路由器。如果您希望 命令影响所有虚拟路由器，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则 命令适用于全局 VRF 虚拟路由器。

Command History

版本	修改
6.1	引入了此命令。
6.6	添加了 ［**vrf** *name*	**all**］ 关键字。

show ospf statistics

使用 **show ospf statistics** 命令以显示各种 OSPF 统计信息，例如 SPF 的执行次数、原因和持续时间。

show ospf ［**vrf** *name* | **all**］ ［*process_id*］ **statistics** ［**detail**］

Syntax Description

detail	（可选）指定详细 SPF 信息，包括触发点。
process_id	（可选）指定本地分配的内部ID，可以是任何正整数。启用OSPF路由流程时，此 ID 是管理性分配的号码。
［**vrf** *name*	**all**］	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将该命令限制为特定虚拟路由器。如果您希望 命令影响所有虚拟路由器，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则 命令适用于全局 VRF 虚拟路由器。

Command History

版本	修改
6.1	引入了此命令。
6.6	添加了 ［**vrf** *name*	**all**］ 关键字。

示例

以下是 **show ospf statistics** 命令的输出示例：

```
> show ospf 10 statistics detail
Area 10: SPF algorithm executed 6 times

SPF 1 executed 04:36:56 ago, SPF type Full
  SPF calculation time (in msec):
  SPT    Prefix D-Int  Sum    D-Sum  Ext    D-Ext  Total
       0      0      0      0      0      0      0 0
  RIB manipulation time (in msec):
  RIB Update    RIB Delete
                0             0
  LSIDs processed R:1 N:0 Prefix:0 SN:0 SA:0 X7:0
  Change record R L
  LSAs changed 2
  Changed LSAs. Recorded is Advertising Router, LSID and LS type:
  49.100.168.192/0(R) 49.100.168.192/2(L)

SPF 2 executed 04:35:50 ago, SPF type Full
  SPF calculation time (in msec):
  SPT    Prefix D-Int  Sum    D-Sum  Ext    D-Ext  Total
       0      0      0      0      0      0      0 0
  RIB manipulation time (in msec):
  RIB Update    RIB Delete
                0             0
  LSIDs processed R:2 N:1 Prefix:0 SN:0 SA:0 X7:0
  Change record R N L
  LSAs changed 5
```

```
Changed LSAs. Recorded is Advertising Router, LSID and LS type:
50.100.168.192/0(R) 50.100.168.192/2(L) 49.100.168.192/0(R) 50.100.168.192/0(R)
50.100.168.192/2(N)
```

show ospf summary-address

要显示在OSPF流程下配置的所有汇总地址重新分发信息的列表，请使用**show ospf summary-address**命令。

show ospf summary-address ［**vrf** *name* | **all**］

Syntax Description

［**vrf** *name* | **all**］	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将该命令限制为特定虚拟路由器。如果您希望 命令影响所有虚拟路由器，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则 命令适用于全局 VRF 虚拟路由器。

Command History

版本	修改
6.1	引入了此命令。
6.6	添加了 ［**vrf** *name* | **all**］ 关键字。

示例

以下显示 **show ospf summary-address** 命令的输出示例。它展示如何在为 ID 为 5 的 OSPF 流程配置摘要地址之前显示所有摘要地址重分布信息的列表。

```
> show ospf 5 summary-address

OSPF Process 2, Summary-address

10.2.0.0/255.255.0.0 Metric -1, Type 0, Tag 0
10.2.0.0/255.255.0.0 Metric -1, Type 0, Tag 10
```

show ospf traffic

要显示已由特定 OSPF 实例处理（发送或接收）的不同类型数据包的列表，请使用 **show ospf traffic** 命令。

show ospf traffic ［**vrf** *name* | **all**］

Syntax Description

［**vrf** *name*	**all**］	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将该命令限制为特定虚拟路由器。如果您希望 命令影响所有虚拟路由器，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则 命令适用于全局 VRF 虚拟路由器。

Command History

版本	修改
6.1	引入了此命令。
6.6	添加了 ［**vrf** *name*	**all**］ 关键字。

使用指南

通过此命令，您可以获取处理的不同类型 OSPF 数据包的快照而无需启用调试。如果配置了两个 OSPF 实例，则 **show ospf traffic** 命令会显示两个实例的统计信息及每个实例的流程 ID。您还可以通过使用 **show ospf** *process_id* **traffic** 命令显示单一实例的统计信息。

示例

以下显示 **show ospf traffic** 命令的输出示例。

```
> show ospf traffic

OSPF statistics (Process ID 70):

       Rcvd: 244 total, 0 checksum errors
             234 hello, 4 database desc, 1 link state req
             3 link state updates, 2 link state acks
       Sent: 485 total
             472 hello, 7 database desc, 1 link state req
             3 link state updates, 2 link state acks
```

Related Commands

命令	Description
show ospf virtual-links	显示 OSPF 虚拟链路的参数和当前状态。

show ospf virtual-links

要显示 OSPF 虚拟链路的参数和当前状态，请使用 **show ospf virtual-links** 命令。

show ospf virtual-links ［**vrf** *name* | **all**］

Syntax Description

［**vrf** *name* | **all**］	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将该命令限制为特定虚拟路由器。如果您希望 命令影响所有虚拟路由器，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则 命令适用于全局 VRF 虚拟路由器。

Command History

版本	修改
6.1	引入了此命令。
6.6	添加了 ［**vrf** *name* | **all**］ 关键字。

示例

以下是 **show ospf virtual-links** 命令的输出示例：

```
> show ospf virtual-links

Virtual Link to router 192.168.101.2 is up
Transit area 0.0.0.1, via interface Ethernet0, Cost of using 10
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 0:00:08
Adjacency State FULL
```

show p - show r

show packet tracer

要显示有关 pcap trace 输出的信息，请使用 **show packet tracer** 命令。

show packet-tracer pcap trace ［ **packet-number** *number* | **summary** | **detailed** | **status** ］

Syntax Description

packet-number	（可选）显示 pcap 中单个数据包的跟踪输出。
summary	（可选）显示 pcap 摘要。
detailed	（可选）显示 pcap 中所有数据包的跟踪输出。
status	（可选）显示 pcap trace 的当前执行状态。

Command Default

无默认行为或值。

Command History

版本	修改
7.1	该命令已增强，包括 pcap trace 的输出。

使用指南

show packet-tracer 命令显示数据包跟踪器输出。 **pcap trace** 命令允许您显示最近在 PCAP 文件上运行的 packet-tracer 的跟踪缓冲区输出。

示例

以下是 **show packet-tracer pcap trace summary** 命令的输出示例：

```
> show packet-tracer pcap trace summary
      1: 02:38:01.265123       6.1.1.100.51944 > 9.1.1.100.80: S 542888804:542888804(0) win
 29200 <mss 1460,sackOK,timestamp 2526545680 0,nop,wscale 7>
      2: 02:38:01.271317       9.1.1.100.80 > 6.1.1.100.51944: S 2281169942:2281169942(0)
ack 542888805 win 28960 <mss 1380,sackOK,timestamp 2526520070 2526545680,nop,wscale 7>
      3: 02:38:01.271638       6.1.1.100.51944 > 9.1.1.100.80: . ack 2281169943 win 229
<nop,nop,timestamp 2526545682 2526520070>

                Total packets: 3
       Packets replayed: 3
       Result: Allow
       Start time: Mar 28 04:51:54
       Total time taken: 10247935ns
     show packet-tracer pcap trace packet-number 1 detailed
     1: 02:38:01.265123 0050.56a9.81e5 0050.56a9.60e1 0x0800 Length: 74
      6.1.1.100.51944 > 9.1.1.100.80: S [tcp sum ok] 542888804:542888804(0) win 29200 <mss
 1460,sackOK,timestamp 2526545680 0,nop,wscale 7> (DF) (ttl 64, id 54388)
      Phase: 1
      Type: ACCESS-LIST
      Subtype:
      Result: ALLOW
      Time Spent: 12345 ns
      Config:
      Implicit Rule
      Additional Information:
```

```
Forward Flow based lookup yields rule:
 in  id=0x154523db3ce0, priority=1, domain=permit, deny=false
                hits=92, user_data=0x0, cs_id=0x0, l3_type=0x8
                src mac=0000.0000.0000, mask=0000.0000.0000
                dst mac=0000.0000.0000, mask=0100.0000.0000
                input_ifc=inside, output_ifc=any
 ...
 ...
```

Related Commands

命令	Description
packet tracer	根据防火墙的当前配置生成 5 到 6 元组数据包

show packet-statistics

要显示 Secure Firewall 3100上有关非策略相关数据包丢弃的信息，请使用 **show packet-statistics** 命令。在 威胁防御上，在系统诊断模式下运行此命令。

show packet-statistics { **interface id** *slot port* } [**breakout** *port* | { **brief** | **no brief** }]

Syntax Description

interface id*slotport*	显示统计信息的带有插槽号和端口号的接口名称。
breakout	（可选）以太网端口号的分支。
brief	（可选）显示不包括零计数器值的输出。

Command Default

无默认行为或值。

Command History

版本	修改
7.2	引入了此命令。

使用指南

show packet-statistics 命令会整理并显示来自多个来源的丢包数据。输出有助于确定数据包被丢弃的位置。此命令整合了以下调试命令的输出：

- **show portmanager counters ethernet <slot> <port>**
- **show queuing interface ethernet <slot> <port>**
- **show portmanager counters internal <slot> <port>**
- **show queuing interface internal <slot> <port>**
- **show portmanager switch counters packet-trace**
- **show npu-accel statistics**
- **show interface detail**
- **show asp drop**

当流量到达设备时，合并的输出按数据路径的顺序排列。此外，输出不会被其他 CLI 的输出中断或中断。

slot/port and **breakout***port* 用于限制特定接口的输出。这些变量和关键字仅适用于外部交换机端口和 Lina 接口。对于其他接口，这些变量将被忽略。

示例

以下是 **show packet-statistics** 命令的输出示例：

```
$ show packet-statistics ethernet 2/1/1 no brief

====================== show portmanager switch counters packet-trace ======================


       Counter                              Description
---------------------- ------------------------------------------------------
goodOctetsRcv          Number of ethernet frames received that are not bad
                       ethernet frames or MAC Control pkts
badOctetsRcv           Sum of lengths of all bad ethernet frames received
gtBrgInFrames          Number of packets received
gtBrgVlanIngFilterDisc Number of packets discarded due to VLAN Ingress Filtering
gtBrgSecFilterDisc     Number of packets discarded due to
                       Security Filtering measures
gtBrgLocalPropDisc     Number of packets discarded due to reasons other than
                       VLAN ingress and Security filtering
dropCounter            Ingress Drop Counter
outUcFrames            Number of unicast packets transmitted
outMcFrames            Number of multicast packets transmitted. This includes
                       registered multicasts, unregistered multicasts
                       and unknown unicast packets
outBcFrames            Number of broadcast packets transmitted
brgEgrFilterDisc       Number of IN packets that were Bridge Egress filtered
txqFilterDisc          Number of IN packets that were filtered
                       due to TxQ congestion
outCtrlFrames          Number of out control packets
                       (to cpu, from cpu and to  analyzer)
egrFrwDropFrames       Number of packets dropped due to egress
                       forwarding restrictions
goodOctetsSent         Sum of lengths of all good ethernet
                       frames sent from this MAC


        Counter            Source port- 0/0    Destination port- 0/0
-----------------------  ---------------------  ---------------------
goodOctetsRcv                     ---                    ---
badOctetsRcv                       ---                    ---

                                       Ingress counters
gtBrgInFrames                    9515                    9515
gtBrgVlanIngFilterDisc             0                       0
gtBrgSecFilterDisc                 0                       0
gtBrgLocalPropDisc                 0                       0
dropCounter                      319           Only for source-port

                                       Egress counters
outUcFrames                       12                      12
outMcFrames                     8176                    8176
outBcFrames                     1008                    1008
brgEgrFilterDisc                   0                       0
txqFilterDisc                      0                       0
outCtrlFrames                      0                       0
egrFrwDropFrames                   0                       0

goodOctetsSent                    ---                     ---

Error at clearing mac counters0/0: GT_BAD_PARAM = Illegal parameter in function called


------------------------------------------------------------

====================== show npu-accel statistics ======================
module: kc25-pcie, pipe: 0
```

```
--------------------------
reg_pcie_rcv_reg_access_rd_tlp_cnt = 28374275
reg_pcie_rcv_reg_access_wr_tlp_cnt = 3810207

module: kc25-eth, pipe: 0
-------------------------
stat_rx_bip_err_0 = 0
stat_rx_bip_err_1 = 0
stat_rx_bip_err_2 = 0
stat_rx_bip_err_3 = 0
stat_rx_framing_err_0 = 0
stat_rx_framing_err_1 = 0
stat_rx_framing_err_2 = 0
stat_rx_framing_err_3 = 0
stat_rx_bad_code = 0
stat_tx_frame_error = 0
stat_tx_total_packets = 0
stat_tx_total_good_packets = 0
stat_tx_total_bytes = 0
stat_tx_total_good_bytes = 0
stat_tx_packet_64_bytes = 0
stat_tx_packet_65_127_bytes = 0
stat_tx_packet_128_255_bytes = 0
stat_tx_packet_256_511_bytes = 0
stat_tx_packet_512_1023_bytes = 0
stat_tx_packet_1024_1518_bytes = 0
stat_tx_packet_1519_1522_bytes = 0
stat_tx_packet_1523_1548_bytes = 0
stat_tx_packet_1549_2047_bytes = 0
stat_tx_packet_2048_4095_bytes = 0
stat_tx_packet_4096_8191_bytes = 0
stat_tx_packet_8192_9215_bytes = 0
stat_tx_packet_large = 0
stat_tx_packet_small = 0
stat_tx_bad_fcs = 0
stat_tx_unicast = 0
stat_tx_multicast = 0
stat_tx_broadcast = 0
stat_tx_vlan = 0
stat_tx_pause = 0
stat_tx_user_pause = 0
stat_rx_total_packets = 964
stat_rx_total_good_packets = 964
stat_rx_total_bytes = 264439
stat_rx_total_good_bytes = 264439
stat_rx_packet_64_bytes = 0
stat_rx_packet_65_127_bytes = 35
stat_rx_packet_128_255_bytes = 0
stat_rx_packet_256_511_bytes = 929
stat_rx_packet_512_1023_bytes = 0
stat_rx_packet_1024_1518_bytes = 0
stat_rx_packet_1519_1522_bytes = 0
stat_rx_packet_1523_1548_bytes = 0
stat_rx_packet_1549_2047_bytes = 0
stat_rx_packet_2048_4095_bytes = 0
stat_rx_packet_4096_8191_bytes = 0
stat_rx_packet_8192_9215_bytes = 0
stat_rx_packet_large = 0
stat_rx_undersize = 0
stat_rx_fragment = 0
stat_rx_oversize = 0
stat_rx_toolong = 0
stat_rx_jabber = 0
stat_rx_bad_fcs = 0
```

```
stat_rx_packet_bad_fcs = 0
stat_rx_stomped_fcs = 0
stat_rx_unicast = 0
stat_rx_multicast = 0
stat_rx_broadcast = 964
stat_rx_vlan = 0
stat_rx_pause = 0
stat_rx_user_pause = 0
stat_rx_inrangeerr = 0
stat_rx_truncated = 0
eth_tx_good_pkt_cnt = 0
eth_tx_err_pkt_cnt = 0
eth_rx_good_pkt_cnt = 964
eth_tx_fifo_sbit_err_cnt = 0
eth_tx_fifo_dbit_err_cnt = 0
eth_rx_fifo_sbit_err_cnt = 0
eth_rx_fifo_dbit_err_cnt = 0

module: kc25-nic, pipe: 0
-------------------------
nic_top_in_pkt_cnt = 964
nic_top_tm_out_pkt_cnt = 971
nic_top_inband_flow_tbl_pkt_cnt = 7
nic_top_inband_stat_pkt_cnt = 0
tm_shared_mem_sbiterr_pkt_cnt = 0
tm_shared_mem_dbiterr_pkt_cnt = 0
tm_pkt_buf_sbiterr_pkt_cnt = 0
tm_pkt_buf_dbiterr_pkt_cnt = 0
tm_out_fifo_sbiterr_pkt_cnt = 0
tm_out_fifo_dbiterr_pkt_cnt = 0
tm_qm_mem_parerr_pkt_cnt = 0
tm_budm_mem_parerr_pkt_cnt = 0
tm_qm_taildrop_pkt_cnt = 0
tm_h2c_desc_mem_sbiterr_pkt_cnt = 0
tm_h2c_desc_mem_dbiterr_pkt_cnt = 0
tm_c2h_desc_mem_sbiterr_pkt_cnt = 0
tm_c2h_desc_mem_dbiterr_pkt_cnt = 0
tm_inband_fifo_sbiterr_pkt_cnt = 0
tm_inband_fifo_dbiterr_pkt_cnt = 0
tm_egr_fifo_sbiterr_pkt_cnt = 0
tm_egr_fifo_dbiterr_pkt_cnt = 0

Traffic Manager per Q statistics
qid             input pkts           output pkts   input tail-drop cnt
  0                     49                    49                     0
  1                      0                     0                     0
  2                     66                    66                     0
  3                      0                     0                     0
  4                     42                    42                     0
  5                      0                     0                     0
  6                     64                    64                     0
  7                      0                     0                     0
  8                      0                     0                     0
  9                     42                    42                     0
 10                      0                     0                     0
 11                     64                    64                     0
 12                      0                     0                     0
 13                     64                    64                     0
 14                      0                     0                     0
 15                     64                    64                     0
 16                      0                     0                     0
 17                     88                    88                     0
 18                      0                     0                     0
 19                     24                    24                     0
```

```
 20                      0                       0                       0
 21                     64                      64                       0
 22                     40                      40                       0
 23                     64                      64                       0
 24                     42                      42                       0
 25                     42                      42                       0
 26                     42                      42                       0
 27                      0                       0                       0
 28                      0                       0                       0
 29                     39                      39                       0
 30                     64                      64                       0
 31                      0                       0                       0
 32                      0                       0                       0
 33                      0                       0                       0
 34                      0                       0                       0
 35                      0                       0                       0
 36                      0                       0                       0
 37                      0                       0                       0
 38                      0                       0                       0
 39                      0                       0                       0
 40                      0                       0                       0
 41                      0                       0                       0
 42                      0                       0                       0
 43                      0                       0                       0
 44                      0                       0                       0
 45                      0                       0                       0
 46                      0                       0                       0
 47                      0                       0                       0
 48                      0                       0                       0
 49                      0                       0                       0
 50                      0                       0                       0
 51                      0                       0                       0
 52                      0                       0                       0
 53                      0                       0                       0
 54                      0                       0                       0
 55                      0                       0                       0
 56                      0                       0                       0
 57                      0                       0                       0
 58                      0                       0                       0
 59                      0                       0                       0
 60                      0                       0                       0
 61                      0                       0                       0
 62                      0                       0                       0
 63                      0                       0                       0

module: kc25-ingress-pkt-classifier, pipe: 0
-------------------------------------------
cla_opt_tbl_hit_cmd_cnt = 0
cla_opt_tbl_miss_cmd_cnt = 958
cla_tunnel_tbl_hit_cmd_cnt = 0
cla_tunnel_tbl_miss_cmd_cnt = 0
cla_6_tuple_tbl_hit_cmd_cnt = 0
cla_6_tuple_tbl_miss_cmd_cnt = 0
cla_4_tuple_tbl_hit_cmd_cnt = 0
cla_4_tuple_tbl_miss_cmd_cnt = 0
cla_bypass_in_cmd_cnt = 6
cla_non_bypass_in_cmd_cnt = 958
cla_rss_lookup_cmd_cnt = 958
cla_rss_bypass_cmd_cnt = 6
cla_opt_tbl_sbiterr_pkt_cnt = 0
cla_opt_tbl_dbiterr_pkt_cnt = 0
cla_tunnel_tbl_sbiterr_pkt_cnt = 0
cla_tunnel_tbl_dbiterr_pkt_cnt = 0
cla_6_tuple_tbl_sbiterr_pkt_cnt = 0
```

```
cla_6_tuple_tbl_dbiterr_pkt_cnt = 0
cla_4_tuple_tbl_sbiterr_pkt_cnt = 0
cla_4_tuple_tbl_dbiterr_pkt_cnt = 0
cla_vf_dma_qid_ram_dbiterr_pkt_cnt = 0
inbf_ram_sbiterr_cnt = 0
inbf_ram_dbiterr_cnt = 0
inbf_rx_request_pkt_cnt = 270327
inbf_tx_response_pkt_cnt = 7
inbf_parser_regrd_cnt = 1
inbf_cmdgen_regrd_cnt = 1
inbf_cmdgen_regwr_cnt = 302068967
inbf_rx_err0_pkt_cnt = 0
inbf_rx_err1_pkt_cnt = 0
inbf_rx_err2_pkt_cnt = 0
inbf_rx_err3_pkt_cnt = 0
inbf_rx_err4_pkt_cnt = 0
inbf_exec_cmd_err_cnt = 0
inbf_wdata_err_cnt = 0
inbf_act_tbl_timeout_cnt = 0
cla_ipsec_sn_tbl_parerr_pkt_cnt = 0
stat_fifo_parerr_pkt_cnt = 0
stat_ag_ram_dbiterr_pkt_cnt = 0
stat_acc_ram_dbiterr_pkt_cnt = 0
stat_ddr_rl_ram_dbiterr_pkt_cnt = 0
stat_ag_ram_sbiterr_pkt_cnt = 0
stat_acc_ram_sbiterr_pkt_cnt = 0
stat_ddr_rl_ram_sbiterr_pkt_cnt = 0
inbs_ram_dbiterr_cnt = 0
stat_in_rx_pkt_cnt = 0
acc_cache_access_col_cnt = 0
acc_cache_insert_fail_cnt = 0
acc_cache_replace_cnt = 0
acc_cache_cpu_col_cnt = 0
ddr_rx_pkt_cnt = 0
ddr_rl_cache_insert_fail_cnt = 0
ddr_rl_cache_insert_update_cnt = 0
ddr_read_cnt = 0
ddr_write_cnt = 0
inbs_rx_request_pkt_cnt = 0
inbs_tx_response_pkt_cnt = 0
inbs_stat_collect_cnt = 0
inbs_rx_err0_pkt_cnt = 0
inbs_rx_err1_pkt_cnt = 0
inbs_rx_err2_pkt_cnt = 0
inbs_rx_err3_pkt_cnt = 0
inbs_rx_err4_pkt_cnt = 0
inbs_exec_cmd_err_cnt = 0
inbs_stat_collect_timeout_err_cnt = 0
key_tbl_dbiterr_pkt_cnt = 0
ts_tbl_dbiterr_pkt_cnt = 0
act_tbl_sbiterr_pkt_cnt = 0
act_tbl_dbiterr_pkt_cnt = 0

module: kc25-ingress-pkt-processor, pipe: 0
-------------------------------------------
proc_pkt_in_cnt = 964
proc_nic_pkt_out_cnt = 964
proc_egr_pkt_out_cnt = 0
proc_ilk_pkt_out_cnt = 0
proc_cap_be_pkt_out_cnt = 0
proc_cap_ae_pkt_out_cnt = 0
proc_cap_tail_drop_cnt = 0
proc_instr_drop_pkt_cnt = 0
proc_err_ar_drop_pkt_cnt = 0
```

```
proc_pkt_in_fifo_sbiterr_pkt_cnt = 0
proc_pkt_in_fifo_dbiterr_pkt_cnt = 0
proc_rwe_data_fifo_sbiterr_pkt_cnt = 0
proc_rwe_data_fifo_dbiterr_pkt_cnt = 0
proc_pkt_out_fifo_sbiterr_pkt_cnt = 0
proc_pkt_out_fifo_dbiterr_pkt_cnt = 0
proc_cap_be_pkt_fifo_sbiterr_pkt_cnt = 0
proc_cap_be_pkt_fifo_dbiterr_pkt_cnt = 0
proc_cap_ae_pkt_fifo_sbiterr_pkt_cnt = 0
proc_cap_ae_pkt_fifo_dbiterr_pkt_cnt = 0
proc_cks_chk_tcp_udp_err_pkt_cnt = 0
proc_cks_chk_ip_err_pkt_cnt = 0
proc_cks_chk_both_err_pkt_cnt = 0

module: kc25-ingress-pkt-parser, pipe: 0
----------------------------------------
par_hi_pri_q_good_pkt_cnt = 0
par_hi_pri_q_err_pkt_cnt = 0
par_hi_pri_q_taildrop_pkt_cnt = 0
par_md_pri_q_good_pkt_cnt = 0
par_md_pri_q_err_pkt_cnt = 0
par_md_pri_q_taildrop_pkt_cnt = 0
par_lo_pri_q_good_pkt_cnt = 964
par_lo_pri_q_err_pkt_cnt = 0
par_lo_pri_q_taildrop_pkt_cnt = 0
par_hi_pri_q_sbiterr_pkt_cnt = 0
par_hi_pri_q_dbiterr_pkt_cnt = 0
par_md_pri_q_sbiterr_pkt_cnt = 0
par_md_pri_q_dbiterr_pkt_cnt = 0
par_lo_pri_q_sbiterr_pkt_cnt = 0
par_lo_pri_q_dbiterr_pkt_cnt = 0

module: kc25-egress-scheduler, pipe: 0
---------------------------------------
egr_rx_ingr_good_pkt_cnt = 0
egr_rx_octeon_good_pkt_cnt = 0
egr_rx_all_good_pkt_cnt = 0
egr_rx_ingr_err_pkt_cnt = 0
egr_rx_octeon_err_pkt_cnt = 0
egr_rx_ingr_drop_pkt_cnt = 0
egr_rx_octeon_drop_pkt_cnt = 0
egr_tx_ingr_pkt_cnt = 0
egr_tx_octeon_pkt_cnt = 0
egr_tx_all_pkt_cnt = 0
egr_ingr_pktbuf_ecc_sbiterr_cnt = 0
egr_ingr_pktbuf_ecc_dbiterr_cnt = 0
egr_ingr_schefifo_ecc_sbiterr_cnt = 0
egr_ingr_schefifo_ecc_dbiterr_cnt = 0
egr_octeon_pktbuf_ecc_sbiterr_cnt = 0
egr_octeon_pktbuf_ecc_dbiterr_cnt = 0
egr_octeon_schefifo_ecc_sbiterr_cnt = 0
egr_octeon_schefifo_ecc_dbiterr_cnt = 0


------------------------------------------------------------

======================      show asp drop       ======================

Frame drop:
  Slowpath security checks failed (sp-security-failed)                    148
  FP L2 rule drop (l2_acl)                                                493
  Interface is down (interface-down)                                        2

Last clearing: Never
```

```
Flow drop:

Last clearing: Never

======================  show interface detail   ======================

Interface Ethernet1/1 "outside", is down, line protocol is down
  Hardware is EtherSVI, BW 1000 Mbps, DLY 10 usec
 Full-Duplex, 1000 Mbps
 MAC address 6c13.d509.5194, MTU 1500
 IP address unassigned
 Auto-Negotiation is turned on
 0 packets input, 0 bytes, 0 no buffer
 Received 0 broadcasts, 0 runts, 0 giants
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
 0 pause input, 0 resume input
 0 packets output, 0 bytes, 0 underruns
 0 pause output, 0 resume output
 0 output errors, 0 collisions, 0 interface resets
 0 late collisions, 0 deferred
 0 input reset drops, 0 output reset drops
  Traffic Statistics for "outside":
 0 packets input, 0 bytes
 0 packets output, 0 bytes
 0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
  Control Point Interface States:
 Interface number is 5
 Interface config status is active
 Interface state is not active
```

show pager

要显示CLI会话的当前页面长度，即在输出暂停并显示--More--指示之前显示的行数，请使用**show pager** 命令。

show pager

注释 不能为 threat defense CLI 设置页面长度。

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show pager** 命令的输出示例。由于您无法在 threat defense CLI 中设置页面长度，因此输出指示没有分页程序。

```
> show pager
no pager
```

show packet debugs

要从数据库中检索和查看存储的调试日志，请使用 **show packet debugs** 命令。在某些版本中，此命令可能带有连字符： **show packet-debugs**

show packet debugs ［ **match** ［ *protocol* ］ ［ *source-ip* ］［ *source-port* ］［ *dest-ip* ］ ［ *dest-port* ］［ **module** *module-id* ］ ［ **packet-id** *packet-id* ］ ［ **severity** *0-7* ］［ **time-start** *time* ］ ［ **time-end** *time* ］］

Syntax Description

match	匹配为过滤连接而输入的以下一个或多个选项：源IP、目的IP、源端口、目标端口或协议。
protocol	协议的名称。
source-ip	源 IP 地址。
source-port	源端口号。
dest-ip	目标 IP 地址。
dest-port	目标端口号。
module *module-id*	用于过滤调试日志的模块名称。
packet-id *packet-id*	用于过滤调试日志的唯一数据包 ID。
severity *0-7*	以下严重性级别之一： • 0（应急）- 系统不可用 • 1（警报）- 需要立即采取措施 • 2（严重）- 严重情况 • 3（错误）- 错误情况 • 4（警告）- 警告情况 • 5（通知）- 正常，但重大的情况 • 6（说明性）- 仅信息性消息 • 7（调试）- 仅调试消息
time-start *time*	返回指定开始时间之后的所有日志。
time-end *time*	返回指定时间之前的所有日志。

Command History

版本	修改
6.4	引入了此命令。

使用指南

使用 **show packet debugs** 命令从数据库中检索和查看存储的调试日志。

[] 中的所有关键字都是可选的。如果未输入特定关键字，则该关键字将被视为 any。所有调试都按时间戳的升序显示。

示例

以下示例启用 TCP 调试，然后显示调试状态。

```
> show packet debugs
```

Related Commands

命令	Description
debug	启用调试。

show parser dump

show parser dump 命令供内部或思科技术支持使用。

show password encryption

要显示密码加密配置设置，请使用 **show password encryption** 命令。

show password encryption

Command History

版本	修改
6.1	引入了此命令。

使用指南

threat defense 不允许配置主密码加密，因此此命令应始终显示密码加密已禁用，并且未设置主密钥散列。

如果密钥已保存，则密钥散列旁边会显示“已保存”。如果没有密钥或者密钥已从运行配置中删除，将会显示“Not set”而不是哈希值。

示例

以下是 **show password encryption** 命令的输出示例：

```
> show password encryption
Password Encryption: Disabled
Master key hash: Not set(saved)
```

show path-monitoring

要显示有关路径监控输出的信息，请使用 **show path monitoring** 命令。

show path-monitoring ［ **interface** *name* ］［ **detail** ］

Syntax Description

Interface*name*	显示路径监控指标的接口
detail	（可选）显示有关路径监控指标的详细信息。

Command Default

无默认行为或值。

Command History

版本	修改
7.1	引入命令是为了显示指定接口的路径监控详细信息。

使用指南

show path-monitoring 命令显示指定出口接口的路径监控输出。

示例

以下是 *outside 1* 接口的 **show path-monitoring** 命令的输出示例：

```
firepower# show path-monitoring interface outside1
Interface: outside1
Remote peer: 90.2.1.1
    Version: 14275
    Remote peer reachable: Yes
    RTT average: 1407 microsecond(s)
    Jitter: 1218 microsecond(s)
    Packet loss: 0%
    MOS: 4.40
    Last updated: 1 second(s) ago
```

以下是 *outside 1* 接口的 **show path-monitoring detail** 命令的输出示例：

```
firepower#
firepower# show path-monitoring interface outside1 detail
Interface: outside1
Remote peer: 90.2.1.1
    Version: 14275
    Remote peer reachable: Yes
    RTT average: 1407 microsecond(s)
    Jitter: 1218 microsecond(s)
    Packet loss: 0%
    MOS: 4.40
    Last updated: 8 second(s) ago

    Internal data:
        Total probes sent: 418553
        Total probes pending: 0
        Current probes pending: 0
        Current RTT sum: 51674
```

```
Current RTT square sum: 154410282
Flags: 0x2
Current queue index: 14
Index:  0, Timestamp:              0, RTT:     962
Index:  1, Timestamp:              0, RTT:    1096
Index:  2, Timestamp:              0, RTT:    1056
Index:  3, Timestamp:              0, RTT:    1457
Index:  4, Timestamp:              0, RTT:    1078
Index:  5, Timestamp:              0, RTT:    1114
Index:  6, Timestamp:              0, RTT:    1570
Index:  7, Timestamp:              0, RTT:    6865
Index:  8, Timestamp:              0, RTT:    1035
Index:  9, Timestamp:              0, RTT:    1334
Index: 10, Timestamp:              0, RTT:    1090
Index: 11, Timestamp:              0, RTT:    1099
Index: 12, Timestamp:              0, RTT:    1429
Index: 13, Timestamp:              0, RTT:    1048
Index: 14, Timestamp:              0, RTT:     985
Index: 15, Timestamp:              0, RTT:    1002
Index: 16, Timestamp:              0, RTT:    1013
Index: 17, Timestamp:              0, RTT:    1741
Index: 18, Timestamp:              0, RTT:    1231
Index: 19, Timestamp:              0, RTT:    1517
Index: 20, Timestamp:              0, RTT:    7780
Index: 21, Timestamp:              0, RTT:    1018
Index: 22, Timestamp:              0, RTT:    1036
Index: 23, Timestamp:              0, RTT:    2369
Index: 24, Timestamp:              0, RTT:    1120
Index: 25, Timestamp:              0, RTT:    1062
Index: 26, Timestamp:              0, RTT:    1088
Index: 27, Timestamp:              0, RTT:    1073
Index: 28, Timestamp:              0, RTT:    1060
Index: 29, Timestamp:              0, RTT:    1071
Index: 30, Timestamp:              0, RTT:    1116
Index: 31, Timestamp:              0, RTT:    1075
Index: 32, Timestamp:              0, RTT:    1084
```

Related Commands

命令	Description
policy-route	在接口上配置策略型路由。

show pclu

show pclu 命令供内部或思科技术支持使用。

show perfmon

要显示有关设备性能的信息，请使用 **show perfmon** 命令。

show perfmon ［**detail**］

Syntax Description

detail	（可选）显示其他统计信息。这些统计信息与思科统一防火墙 MIB 的全局和单一协议连接对象收集的统计信息相一致。

Command History

版本	修改
6.1	引入了此命令。

使用指南

perfmon 命令按定义的时间间隔持续显示性能统计信息。使用 **show perfmon** 命令可立即显示这些信息。

示例

以下是 **show perfmon detail** 命令的输出示例：

```
> show perfmon detail
PERFMON STATS:    Current      Average
Xlates               0/s          0/s
Connections          0/s          0/s
TCP Conns            0/s          0/s
UDP Conns            0/s          0/s
URL Access           0/s          0/s
URL Server Req       0/s          0/s
TCP Fixup            0/s          0/s
HTTP Fixup           0/s          0/s
FTP Fixup            0/s          0/s
AAA Authen           0/s          0/s
AAA Author           0/s          0/s
AAA Account          0/s          0/s
TCP Intercept        0/s          0/s
SETUP RATES:
Connections for 1 minute = 0/s; 5 minutes = 0/s
TCP Conns for 1 minute = 0/s; 5 minutes = 0/s
UDP Conns for 1 minute = 0/s; 5 minutes = 0/s
```

Related Commands

命令	Description
perfmon	按定义的时间间隔显示详细的性能监控信息。

show perfstats

要显示有关设备性能的统计信息，请使用 **show perfstats** 命令。

show perfstats

Command History

版本	修改
6.1	引入了此命令。

使用指南

show perfstats 命令显示检测引擎的性能信息。命令会显示可用引擎的列表，您可以选择要查看其统计信息的引擎。然后，您会看到许多配置文件；选择要查看的内容。

这些文件对管理中心远程管理的系统有意义。对于使用本地管理器设备管理器管理的系统，这些文件通常没有内容。

如果您决定不想查看完整的文件，请使用 Crtl+C 停止显示。文件内容可能很长。

示例

```
> show perfstats
Available DEs:
  1 - Primary Detection Engine (703006f4-8ff6-11e6-bb6e-8f2d5febf243)
  0 - Cancel and return to CLI

Select a DE to profile: 1
Available now files:
  1 - /var/sf/detection_engines/f24ce56c-8ff6-11e6-b914-515e5febf243/2016-10-13
  2 - /var/sf/detection_engines/f24ce56c-8ff6-11e6-b914-515e5febf243/2016-10-16
  3 - /var/sf/detection_engines/f24ce56c-8ff6-11e6-b914-515e5febf243/2016-10-11
  4 - /var/sf/detection_engines/f24ce56c-8ff6-11e6-b914-515e5febf243/2016-10-15
  5 - /var/sf/detection_engines/f24ce56c-8ff6-11e6-b914-515e5febf243/2016-10-14
  6 - /var/sf/detection_engines/f24ce56c-8ff6-11e6-b914-515e5febf243/2016-10-12
  7 - /var/sf/detection_engines/f24ce56c-8ff6-11e6-b914-515e5febf243/instance-1/now
  0 - Cancel and return to DE selection

Select a now file: 7
Mon Oct 17 00:05:00 2016
                 Pkts Recv: 162
                 Pkts Drop: 0
            Block Verdicts: 0
                 Mbits/Sec: 0.001
                 Drop Rate: 0%
                Alerts/Sec: 0
          Total Alerts/Sec: 0
(...remaining content truncated...)
```

show pim bsr-router

要显示引导路由引导程序 (BSR) 信息，请使用 **show pim bsr-router** 命令。

show pim bsr-router

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show pim bsr-router** 命令的输出示例：

```
> show pim bsr-router
PIMv2 Bootstrap information
This system is a candidate BSR
  Candidate BSR interface GigabitEthernet0/0 is down - BSR messages not originated
  Candidate RP: 4.4.4.1(GigabitEthernet0/0), GigabitEthernet0/0 is down - not advertised
```

show pim df

要显示汇聚点 (RP) 或接口的双向 DF“优胜者”，请使用 **show pim df** 命令。

show pim df ［**winner**］［*rp_address* | *interface_name*］

Syntax Description

rp_address	可以是以下各项之一： • RP 的名称，如域名系统 (DNS) 主机表中所定义。 • RP 的 IP 地址。这是采用四点分十进制符号的组播 IP 地址。
interface_name	物理或逻辑接口名称。
winner	（可选）显示每个 RP 的每个接口在 DF 选定中的获胜者。

Command History

版本	修改
6.1	引入了此命令。

使用指南

此命令还显示适用于 RP 的优胜衡量标准。

示例

以下是 **show pim df** 命令的输出示例：

```
> show pim df
RP           Interface   DF Winner   Metrics

172.16.1.3   Loopback3   172.17.3.2  [110/2]
172.16.1.3   Loopback2   172.17.2.2  [110/2]
172.16.1.3   Loopback1   172.17.1.2  [110/2]
172.16.1.3   inside      10.10.2.3   [0/0]
172.16.1.3   inside      10.10.1.2   [110/2]
```

show pim group-map

要显示组到协议的映射表，请使用 **show pim group-map** 命令。

show pim group-map ［**info-source** | **rp-timers**］［*group*］

Syntax Description

group	（可选）可以是以下各项之一： • 组播组的名称，如 DNS 主机表中所定义。 • 组播组的 IPv4 或 IPV6 地址。
info-source	（可选）显示组范围信息源。
rp-timers	（可选）显示组到 RP 映射的正常运行时间和到期计时器。

Command Default

显示所有组的组-协议映射。

Command History

版本	修改
6.1	引入了此命令。

使用指南

此命令显示 RP 的所有组协议地址映射。在设备上从不同的客户端获知映射。

在设备上实施 PIM 会在映射表中填充各种特殊条目。自动 RP 组范围会从稀疏模式组范围中专门排除。SSM 组范围也不属于稀疏模式范围。链路本地组播组（224.0.0.0 至 224.0.0.225，由 224.0.0.0/24 定义）也会从稀疏模式组范围中排除。最后一个条目使用给定 RP 在稀疏模式下显示所有剩余的组。

示例

以下是 **show pim group-map** 命令的输出示例：

```
> show pim group-map
Group Range      Proto   Client Groups   RP address   Info

224.0.1.39/32*   DM      static 1        0.0.0.0
224.0.1.40/32*   DM      static 1        0.0.0.0
224.0.0.0/24*    NO      static 0        0.0.0.0
232.0.0.0/8*     SSM     config 0        0.0.0.0
224.0.0.0/4*     SM      autorp 1        10.10.2.2    RPF: POS01/0/3,10.10.3.2
```

在行 1 和行 2 中，自动 RP 组范围会从稀疏模式组范围中专门排除。

在行 3 中，链路本地组播组（224.0.0.0 至 224.0.0.255，由 224.0.0.0/24 定义）也会从稀疏模式组范围中排除。

在行 4 中，PIM 源特定组播 (PIM-SSM) 组范围映射到 232.0.0.0/8。

最后一个条目显示，所有剩余的组都处于稀疏模式并映射到 RP 10.10.3.2。

show pim interface

要显示 PIM 的接口特定信息，请使用 **show pim interface** 命令。

show pim interface ［*interface_name* | **state-off** | **state-on**］

Syntax Description

interface_name	（可选）接口的名称。包含此参数会限制向指定接口显示的信息。
state-off	（可选）显示禁用了 PIM 的接口。
state-on	（可选）显示启用了 PIM 的接口。

Command Default

如果不指定接口，将会显示所有接口的 PIM 信息。

Command History

版本	修改
6.1	引入了此命令。

使用指南

threat defense 设备本身就是 PIM 邻居。因此，此命令的输出中的“邻居数”列显示的邻居数会比实际邻居数大 1。

示例

以下示例展示内部接口的 PIM 信息：

```
> show pim interface inside
Address    Interface      Ver/     Nbr     Query      DR     DR
                          Mode     Count   Intvl      Prior
172.16.1.4 inside         v2/S     2       100 ms     1      172.16.1.4
```

show pim join-prune statistic

要显示 PIM 加入/删除汇聚统计信息，请使用 **show pim join-prune statistic** 命令。

show pim join-prune statistic ［*interface_name*］

Syntax Description

interface_name	（可选）接口的名称。包含此参数会限制向指定接口显示的信息。

Command Default

如果不指定接口，此命令将会显示所有接口的联接/修剪统计信息。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用 **clear pim counters** 命令清除 PIM 加入/删除统计信息。

示例

以下是 **show pim join-prune statistic** 命令的输出示例：

```
> show pim join-prune statistic
PIM Average Join/Prune Aggregation for last (1K/10K/50K) packets
Interface          Transmitted             Received
            inside   0 /    0 /    0         0 /    0 /    0
   GigabitEthernet1   0 /    0 /    0         0 /    0 /    0
          Ethernet0   0 /    0 /    0         0 /    0 /    0
          Ethernet3   0 /    0 /    0         0 /    0 /    0
   GigabitEthernet0   0 /    0 /    0         0 /    0 /    0
          Ethernet2   0 /    0 /    0         0 /    0 /    0
```

Related Commands

命令	Description
clear pim counters	清除 PIM 流量计数器。

show pim neighbor

要显示 PIM 邻居表中的条目，请使用 **show pim neighbor** 命令。

show pim neighbor ［**count** | **detail**］［*interface*］

Syntax Description

interface	（可选）接口的名称。包含此参数会限制向指定接口显示的信息。
count	（可选）显示 PIM 邻居总数以及每个接口的 PIM 邻居数。
detail	（可选）显示通过上游检测问候选项获知的邻居的其他地址。

Command History

版本	修改
6.1	引入了此命令。

使用指南

此命令用于确定路由器通过 PIM 问候消息获知的 PIM 邻居。此外，此命令还指明哪个接口是指定路由器 (DR) 以及邻居何时能够双向运行。

threat defense 设备本身就是 PIM 邻居。因此， threat defense 接口会显示在此命令的输出中。 threat defense 设备的 IP 地址旁边带有一个星号。

示例

以下是 **show pim neighbor** 命令的输出示例：

```
> show pim neighbor inside
Neighbor Address    Interface    Uptime     Expires   DR  pri  Bidir
10.10.1.1           inside       03:40:36   00:01:41  1        B
10.10.1.2*          inside       03:41:28   00:01:32  1   (DR) B
```

show pim range-list

要显示 PIM 的范围列表信息，请使用 **show pim range-list** 命令。

show pim range-list ［**config**］［*rp_address*］

Syntax Description

config	显示 PIM CLI 范围列表信息。
rp_address	可以是以下各项之一： • 汇聚点 (RP) 的名称，如域名系统 (DNS) 主机表中所定义。 • RP 的 IP 地址。这是采用四点分十进制符号的组播 IP 地址。

Command History

版本	修改
6.1	引入了此命令。

使用指南

此命令用于确定组映射的组播转发模式。此命令的输出还指明范围的集合点(RP)地址（如果适用）。

示例

以下是 **show pim range-list** 命令的输出示例：

```
> show pim range-list
config SSM Exp: never Src: 0.0.0.0
  230.0.0.0/8 Up: 03:47:09
config BD RP: 172.16.1.3 Exp: never Src: 0.0.0.0
  239.0.0.0/8 Up: 03:47:16
config BD RP: 172.18.1.6 Exp: never Src: 0.0.0.0
  239.100.0.0/16 Up: 03:47:10
config SM RP: 172.18.2.6 Exp: never Src: 0.0.0.0
  235.0.0.0/8 Up: 03:47:09
```

Related Commands

命令	Description
show pim group-map	显示组到 PIM 模式的映射和活动 RP 信息。

show pim topology

要显示 PIM 拓扑表信息，请使用 **show pim topology** 命令。

show pim topology ［**reserved** | **route-count** ［**detail**］ | *group* ［*source*］］

Syntax Description

reserved	显示保留组的 PIM 拓扑表信息。
route-count	显示 PIM 拓扑表中的路由数量。
detail	（可选）显示每个组更详细的计数信息。
group	（可选）可以是以下各项之一： • 组播组的名称，如 DNS 主机表中所定义。 • 组播组的 IPv4 或 IPV6 地址。
source	（可选）可以是以下各项之一： • 组播源的名称，如 DNS 主机表中所定义。 • 组播源的 IPv4 或 IPV6 地址。

Command Default

显示所有组和源的拓扑信息。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用 PIM 拓扑表可显示给定组、(*, G)、(S, G) 和 (S, G)RPT（它们分别有自己的接口列表）的各个条目。

PIM 通过 MRIB 传达这些条目的内容；MRIB 是组播路由协议（例如 PIM）、本地成员协议（例如互联网组管理协议 [IGMP]）和系统的组播转发引擎之间的通信中介。

MRIB 显示对于给定 (S, G) 条目应在哪个接口接收数据包以及应在哪个接口转发数据包。此外，在转发过程中会使用组播转发信息库 (MFIB) 表，以决定每个数据包的转发操作。

注释 有关转发信息，请使用 **show mfib route** 命令。

示例

以下是 **show pim topology** 命令的输出示例：

```
> show pim topology
IP PIM Multicast Topology Table
Entry state: (*/S,G)[RPT/SPT] Protocol Uptime Info
Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive,
    RA - Really Alive, LH - Last Hop, DSS - Don't Signal Sources,
    RR - Register Received, SR
(*,224.0.1.40) DM Up: 15:57:24 RP: 0.0.0.0
JP: Null(never) RPF: ,0.0.0.0 Flags: LH DSS
  outside            15:57:24  off LI LH

(*,224.0.1.24) SM Up: 15:57:20 RP: 0.0.0.0
JP: Join(00:00:32) RPF: ,0.0.0.0 Flags: LH
  outside            15:57:20  fwd LI LH

(*,224.0.1.60) SM Up: 15:57:16 RP: 0.0.0.0
JP: Join(00:00:32) RPF: ,0.0.0.0 Flags: LH
  outside            15:57:16  fwd LI LH
```

以下是 **show pim topology reserved** 命令的输出示例：

```
> show pim topology reserved
IP PIM Multicast Topology Table
Entry state: (*/S,G)[RPT/SPT] Protocol Uptime Info
Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive,
    RA - Really Alive, LH - Last Hop, DSS - Don't Signal Sources,
    RR - Register Received, SR - Sending Registers, E - MSDP External,
    DCC - Don't Check Connected
Interface state: Name, Uptime, Fwd, Info
Interface flags: LI - Local Interest, LD - Local Disinterest,
    II - Internal Interest, ID - Internal Disinterest,
    LH - Last Hop, AS - Assert, AB - Admin Boundary

(*,224.0.0.1) L-Local Up: 00:02:26 RP: 0.0.0.0
JP: Null(never) RPF: ,0.0.0.0 Flags:
  outside            00:02:26  off II

(*,224.0.0.3) L-Local Up: 00:00:48 RP: 0.0.0.0
JP: Null(never) RPF: ,0.0.0.0 Flags:
  inside             00:00:48  off II
```

以下是 **show pim topology route-count** 命令的输出示例：

```
> show pim topology route-count
PIM Topology Table Summary
  No. of group ranges = 5
  No. of (*,G) routes = 0
  No. of (S,G) routes = 0
  No. of (S,G)RPT routes = 0
```

Related Commands

命令	Description
show mrib route	显示 MRIB 表。

show pim traffic

要显示 PIM 流量计数器，请使用 **show pim traffic** 命令。

show pim traffic

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用 **clear pim counters** 命令清除 PIM 流量计数器。

示例

以下是 **show pim traffic** 命令的输出示例：

```
> show pim traffic

PIM Traffic Counters
Elapsed time since counters cleared: 3d06h

                                Received     Sent
Valid PIM Packets                      0        9485
Hello                                  0        9485
Join-Prune                             0           0
Register                               0           0
Register Stop                          0           0
Assert                                 0           0
Bidir DF Election                      0           0

Errors:
Malformed Packets                                  0
Bad Checksums                                      0
Send Errors                                        0
Packet Sent on Loopback Errors                     0
Packets Received on PIM-disabled Interface         0
Packets Received with Unknown PIM Version          0
```

Related Commands

命令	Description
clear pim counters	清除 PIM 流量计数器。

show pim tunnel

要显示有关 PIM 隧道接口的信息，请使用 **show pim tunnel** 命令。

show pim tunnel ［*interface_name*］

Syntax Description

interface_name	（可选）接口的名称。包含此参数会限制向指定接口显示的信息。

Command Default

如果不指定接口，此命令会显示所有接口的 PIM 隧道信息。

Command History

版本	修改
6.1	引入了此命令。

使用指南

PIM 注册数据包通过虚拟封装隧道接口从源第一跳 DR 路由器发送到交汇点 (RP)。在 RP 上，虚拟解封隧道用于代表 PIM 注册数据包的接收接口。此命令显示这两种接口的隧道信息。

注册隧道是通过共享树从源发送到 RP 以供分布的（PIM 注册消息中的）封装组播数据包。注册仅适用于 SM，而不适用于 SSM 和双向 PIM。

示例

以下是 **show pim tunnel** 命令的输出示例：

```
> show pim tunnel

Interface     RP Address    Source Address

Encapstunne   l0 10.1.1.1   10.1.1.1
Decapstunne   l0 10.1.1.1   -
```

Related Commands

命令	Description
show pim topology	显示 PIM 拓扑表。

show policy-list

要显示有关已配置的策略列表和策略列表条目的信息，请使用 **show policy-list** 命令。

show policy-list ［*policy_list_name*］

Syntax Description

policy_list_name	（可选）显示有关指定策略列表的信息。

Command History

版本	修改
6.1	引入了此命令。

使用指南

策略列表在 BGP 路由中用作路由地图的匹配条件。

示例

以下是 **show policy-list** 命令的输出示例：

```
> show policy-list

policy-list policy_list_2 permit
  Match clauses:
    ip address prefix-lists: prefix_1

policy-list policy_list_1 permit
  Match clauses:
    ip address (access-lists): test
    interface inside
```

show policy-route

要显示基于策略的路由配置，请使用 **show policy-route** 命令。

show policy-route

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show policy-route** 命令的输出示例：

```
> show policy-route
Interface Route map
GigabitEthernet0/0   equal-access
```

show port-channel

要以详细的单行摘要形式显示 EtherChannel 信息，或显示端口和端口通道信息，请使用 **show port-channel** 命令。

show port-channel [*channel_group_number*] [**brief** | **detail** | **port** | **protocol** | **summary**]

Syntax Description

brief	（默认设置）显示简要信息。
channel_group_number	（可选）指定 EtherChannel 通道组编号（介于 1 到 48 之间）并且仅显示有关此通道组的信息。
detail	（可选）显示详细信息。
port	（可选）显示每个接口的信息。
protocol	（可选）显示 EtherChannel 协议，例如 LACP（如果已启用）。
summary	（可选）显示端口通道摘要。

Command Default

默认值为 **brief**。

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show port-channel** 命令的输出示例：

```
> show port-channel
        Channel-group listing:
        ----------------------

Group: 1
----------
Ports: 3   Maxports = 16
Port-channels: 1 Max Port-channels = 48
Protocol: LACP/ active
Minimum Links: 1
Maximum Bundle: 8
Load balance: src-dst-ip
```

以下是 **show port-channel summary** 命令的输出示例：

```
> show port-channel summary

Number of channel-groups in use: 1
Group  Port-channel  Protocol    Ports
```

```
------+-------------+-----------+-----------------------------------------------
1      Po1             LACP    Gi3/1   Gi3/2   Gi3/3
```

以下是 **show port-channel detail** 命令的输出示例：

```
> show port-channel detail
        Channel-group listing:
        ----------------------

Group: 1
----------
Ports: 3   Maxports = 16
Port-channels: 1 Max Port-channels = 48
Protocol: LACP/ active
Minimum Links: 1
Maximum Bundle: 8
Load balance: src-dst-ip

       Ports in the group:
       -------------------
Port: Gi3/1
------------
Port state    = bndl
Channel group =    1        Mode = LACP/ active
Port-channel  = Po1

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.

Local information:
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State      Priority      Key       Key     Number      State
--------------------------------------------------------------------------------
Gi3/1     SA      bndl       32768         0x1       0x1     0x302       0x3d

Partner's information:
          Partner Partner    LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State      Port Priority Admin Key Oper Key Port Number Port State
--------------------------------------------------------------------------------
Gi3/1     SA      bndl       32768         0x0       0x1      0x306       0x3d

Port: Gi3/2
------------
Port state    = bndl
Channel group =    1        Mode = LACP/ active
Port-channel  = Po1

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.

Local information:
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State      Priority      Key       Key     Number      State
--------------------------------------------------------------------------------
Gi3/2     SA      bndl       32768         0x1       0x1     0x303       0x3d

Partner's information:
          Partner Partner    LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State      Port Priority Admin Key Oper Key Port Number Port State
--------------------------------------------------------------------------------
Gi3/2     SA      bndl       32768         0x0       0x1      0x303       0x3d
```

```
Port: Gi3/3
------------
Port state    = bndl
Channel group =    1        Mode = LACP/ active
Port-channel  = Po1

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.

Local information:
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
-------------------------------------------------------------------------------
Gi3/3     SA      bndl      32768         0x1       0x1     0x304       0x3d

Partner's information:
          Partner Partner    LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State      Port Priority Admin Key Oper Key Port Number Port State
-------------------------------------------------------------------------------
Gi3/3     SA      bndl       32768         0x0       0x1      0x302       0x3d
```

以下是 **show port-channel port** 命令的输出示例：

```
> show port-channel port
        Channel-group listing:
        ----------------------

Group: 1
----------
       Ports in the group:
       -------------------
Port: Gi3/1
------------
Port state    = bndl
Channel group =    1        Mode = LACP/ active
Port-channel  = Po1

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.

Local information:
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
-------------------------------------------------------------------------------
Gi3/1     SA      bndl      32768         0x1       0x1     0x302       0x3d

Partner's information:
          Partner Partner    LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State      Port Priority Admin Key Oper Key Port Number Port State
-------------------------------------------------------------------------------
Gi3/1     SA      bndl       32768         0x0       0x1      0x306       0x3d

Port: Gi3/2
------------
Port state    = bndl
Channel group =    1        Mode = LACP/ active
Port-channel  = Po1

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.

Local information:
```

```
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
--------------------------------------------------------------------------------
Gi3/2     SA      bndl      32768         0x1       0x1     0x303       0x3d

Partner's information:
          Partner Partner   LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State     Port Priority Admin Key Oper Key Port Number Port State
--------------------------------------------------------------------------------
Gi3/2     SA      bndl      32768         0x0       0x1      0x303       0x3d

Port: Gi3/3
------------
Port state    = bndl
Channel group =    1        Mode = LACP/ active
Port-channel  = Po1

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.

Local information:
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
--------------------------------------------------------------------------------
Gi3/3     SA      bndl      32768         0x1       0x1     0x304       0x3d

Partner's information:
          Partner Partner   LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State     Port Priority Admin Key Oper Key Port Number Port State
--------------------------------------------------------------------------------
Gi3/3     SA      bndl      32768         0x0       0x1      0x302       0x3d
```

以下是 **show port-channel protocol** 命令的输出示例：

```
> show port-channel protocol
        Channel-group listing:
        ----------------------
Group: 1
----------
Protocol: LACP
```

Related Commands

命令	Description
show lacp	显示 LACP 信息（例如流量统计信息）、系统标识符和邻居详细信息。
show port-channel load-balance	显示端口通道负载均衡信息以及为给定的一组参数选择的散列结果和成员接口。

show port-channel load-balance

对于 EtherChannel，要显示当前的端口信道负载平衡算法，或者要查看为给定参数集选择的成员接口，请使用 **show port-channel load-balance** 命令。

show port-channel *channel_group_number* **load-balance** [**hash-result** {{**ip** | **ipv6** | **mac** | **l4port** | **mixed**} *parameters* | **vlan-only** *number*}]

Syntax Description

channel_group_number	指定 EtherChannel 信道组编号（1 到 48）。
hash-result	（可选）显示在为当前负载平衡算法输入的散列值之后选择的成员接口。
ip	（可选）指定 IPv4 数据包参数。
ipv6	（可选）指定 IPv6 数据包参数。
l4port	（可选）指定端口数据包参数。
mac	（可选）指定 MAC 地址数据包参数。
mixed	（可选）指定 IP 或 IPv6 参数的组合以及端口和/或 VLAN ID。
parameters	（可选）数据包参数（取决于类型）。例如，对于 ip，可以指定源 IP 地址、目标 IP 地址和/或 VLAN ID。
vlan-only *number*	（可选）指定数据包的 VLAN ID，范围为 0-4095。

Command History

版本	修改
6.1	引入了此命令。

使用指南

默认情况下，设备根据数据包的源 IP 地址和目标 IP 地址 (**src-dst-ip**) 来均衡接口上的数据包负载。

使用此命令可查看当前负载平衡算法；如果与 **hash-result** 关键字结合使用，此命令还可以测试将为带有给定参数的数据包选择哪个成员接口。此命令仅测试当前负载平衡算法。例如，如果算法是 src-dst-ip，请输入 IPv4 或 IPv6 源 IP 地址和目标 IP 地址。如果您输入当前算法没有使用的其他参数，这些参数将被忽略，且当前算法实际使用的而您没有输入的值将会默认为 0。例如，如果算法是 vlan-src-ip，请输入：

```
show port-channel 1 load-balance hash-result ip source 10.1.1.1 vlan 5
```

如果您输入以下内容，则 vlan-src-ip 算法会假设使用的是源 IP 地址 0.0.0.0 和 VLAN 0，并会忽略您输入的值：

```
show port-channel 1 load-balance hash-result l4port source 90 destination 100
```

示例

以下是 **show port-channel 1 load-balance** 命令的输出示例：

```
> show port-channel 1 load-balance
EtherChannel Load-Balancing Configuration:
       src-dst-ip

EtherChannel Load-Balancing Addresses UsedPer-Protocol:
Non-IP: Source XOR Destination MAC address
 IPv4: Source XOR Destination IP address
 IPv6: Source XOR Destination IP address
```

以下是 **show port-channel 1 load-balance hash-result** 命令的输出示例，其中输入的参数与当前算法 (src-dst-ip) 匹配：

```
> show port-channel 1 load-balance hash-result ip source 10.1.1.1 destination 10.5.5.5
Would select GigabitEthernet2/1 based on algorithm src-dst-ip
```

以下是 **show port-channel 1 load-balance hash-result** 命令的输出示例，其中输入的参数与当前算法 (src-dst-ip) 不匹配，且使用的散列值为 0：

```
> show port-channel 1 load-balance hash-result l4port source 5
Would select GigabitEthernet3/2 of Port-channel1 based on algorithm src-dst-ip
```

Related Commands

命令	Description
show lacp	显示 LACP 信息（例如流量统计信息）、系统标识符和邻居详细信息。
show port-channel	在详细的单行摘要表单中显示 EtherChannel 信息。此命令还显示端口和端口信道信息。

show power inline

对于带 PoE 接口的型号，使用 **show power inline** 命令显示接口的电源状态。

注释 仅支持 Firepower 1010。

show power inline

Command History

版本	修改
6.5	引入了此命令。

使用指南

可以使用 PoE 接口连接需要电源的设备，例如 IP 电话或无线接入点。对于 Firepower 1010，以太网 1/7 和 1/8 支持 PoE+。

示例

以下是 Firepower 1010 的 **show power inline** 命令的输出示例：

```
> show power inline
   Interface     Power   Class   Current (mA)   Voltage (V)
   ---------     -----   -----   ------------   -----------
   Ethernet1/1   n/a     n/a     n/a            n/a
   Ethernet1/2   n/a     n/a     n/a            n/a
   Ethernet1/3   n/a     n/a     n/a            n/a
   Ethernet1/4   n/a     n/a     n/a            n/a
   Ethernet1/5   n/a     n/a     n/a            n/a
   Ethernet1/6   n/a     n/a     n/a            n/a
   Ethernet1/7   On      4       121.00         53.00
   Ethernet1/8   On      4       88.00          53.00
```

下表显示每个字段的说明：

表 47: show power inline Fields

字段	Description
Interface	显示 threat defense上的所有接口（包括没有 PoE 可用的接口）。
Power	显示电源是否已开启。如果设备不需要电源，或者该接口上没有设备，或者接口已关闭，则值为 Off。如果接口不支持 PoE，则值为 n/a。
Class	显示所连接设备的 PoE 类。
Current (mA)	显示正在使用的电流。
Voltage (V)	显示正在使用的电压。

show prefix-list

要列出配置为匹配 IPv4 流量的前缀列表，请使用 **show prefix-list** 命令。

show prefix-list ［**detail** | **summary**］［*prefix_list_name* ［**seq** *sequence_number* | *network/length* ［**longer** | **first-match**］］］

Syntax Description

detail	显示有关前缀列表的详细信息。
summary	显示前缀列表摘要。
prefix_list_name	前缀列表的名称。
seq *sequence-number*	（可选）仅显示指定前缀列表中具有指定序列号的前缀列表条目。
network/length [**longer** | **first-match**]	（可选）显示使用此网络地址和网络掩码长度（以位为单位）的指定前缀列表中的所有条目。网络掩码的长度可以是 0 到 32。 您可以选择包含以下关键字之一： • **longer** 显示与给定 network/length 匹配或比其更具体的指定前缀列表的所有条目。 • **first-match** 显示与给定 network/length 匹配的指定前缀列表的第一个条目。

Command History

版本	修改
6.1	引入了此命令。

示例

以下是带有名为 "test" 的前缀列表的 **show prefix-list** 命令的输出示例：

```
> show prefix-list detail test

prefix-list test:   Description: test-list
   count: 1, range entries: 0, sequences: 1 - 1, refcount: 3

   seq 1 permit 2.0.0.0/8 (hit count: 0, refcount: 1)
```

Related Commands

命令	Description
clear prefix-list	重置 IP 前缀列表的命中计数。
show bgp prefix-list	显示在边界网关协议情景下有关前缀列表或前缀列表条目的信息。
show ipv6 prefix-list	显示有关 IPv6 前缀列表的信息。

show priority-queue

要显示某个接口的优先级队列配置或统计信息，请使用 **show priority-queue** 命令。

show priority-queue {**config** | **statistics**} [*interface_name*]

Syntax Description

config	显示接口优先级队列的队列和 TX 环限制。
interface_name	（可选）指定要显示配置或尽力而为队列和低延迟队列详细统计信息的接口的名称。
statistics	显示尽力而为和低延迟队列的统计详细信息。

Command History

版本	修改
6.3	引入了此命令。

示例

此示例显示名为 test 的接口的统计信息。在以下输出中，BE 表示“尽力而为”队列，LLQ 表示低延迟队列：

```
> show priority-queue statistics test

Priority-Queue Statistics interface test

Queue Type         = BE
Packets Dropped    = 0
Packets Transmit   = 0
Packets Enqueued   = 0
Current Q Length   = 0
Max Q Length       = 0

Queue Type         = LLQ
Packets Dropped    = 0
Packets Transmit   = 0
Packets Enqueued   = 0
Current Q Length   = 0
Max Q Length       = 0
```

以下示例显示所有已配置接口上的优先级队列的配置。

```
> show priority-queue config

Priority-Queue Config interface inside
                current          default          range
queue-limit     0                2048             0 - 2048
tx-ring-limit   4294967295               511              3 - 511

Priority-Queue Config interface test
                current          default          range
queue-limit     0                2048             0 - 2048
```

```
tx-ring-limit   4294967295              511             3 - 511

Priority-Queue Config interface outside
                current         default         range
queue-limit     0               2048            0 - 2048
tx-ring-limit   4294967295              511             3 - 511

Priority-Queue Config interface bgmember1
                current         default         range
queue-limit     0               2048            0 - 2048
tx-ring-limit   4294967295              511             3 - 511
```

命令	Description
clear priority-queue statistics	将优先级队列统计信息重置为零。

show processes

要显示设备上正在运行的流程列表，请使用 **show processes** 命令。

show processes ［**cpu-hog** | **cpu-usage** ［**non-zero**］［**sorted**］ | **internals** | **memory** | **system**］

Syntax Description

cpu-hog	显示正在大量占用 CPU（即使用 CPU 超过 100 毫秒）的流程的数量及详细信息。
cpu-usage	显示在最近的 5 秒、1 分钟和 5 分钟内每个流程的 CPU 使用率。
internals	显示每个流程的内部详细信息。
memory	显示每个流程的内存分配。
non-zero	（可选）显示 CPU 使用率不是 0 的流程。
sorted	（可选）显示已排序的流程 CPU 使用率。
system	（可选）显示有关系统上当前运行的流程的信息。

Command History

版本	修改
6.1	引入了此命令。

使用指南

流程是只需要几个指令的轻量级线程。 **show processes** 命令显示设备上正在运行的流程列表，如下所示：

命令	显示的数据	Description
show processes	PC	程序计数器。
show processes	SP	堆栈指针。
show processes	省/自治区	线程队列的地址。
show processes	运行时间	线程根据 CPU 时钟周期已运行的毫秒数。对于基于 CPU 时钟周期（小于 10 纳秒分辨率）而非时钟计时周期（10 毫秒分辨率）的完整、准确的流程 CPU 使用率计算，准确性达到 1 毫秒以内。
show processes	SBASE	堆栈基址。
show processes	产品	当前使用中的字节数以及堆栈的总大小。
show processes	流程	线程的功能。
show processes cpu-usage	MAXHOG	最大 CPU 大量占用运行时间，以毫秒为单位。

命令	显示的数据	Description
show processes cpu-usage	NUMHOG	CPU 大量占用运行次数。
show processes cpu-usage	LASTHOG	上一次 CPU 大量占用运行时间，以毫秒为单位。
show processes cpu-usage	PC	CPU 占用流程的指令指针。
show processes cpu-usage	Traceback	CPU 大量占用流程的堆栈跟踪。最多可回溯 14 个地址。
show processes internals	Invoked Calls	调度程序运行流程的次数。
show processes internals	Giveups	流程将 CPU 归还给调度程序的次数。

使用 **show processes cpu-usage** 命令可缩小设备上可能正在使用 CPU 的特定流程的范围。您可以使用 **sorted** 和 **non-zero** 命令进一步自定义 **show processes cpu-usage** 命令的输出。

借助调度程序和总摘要行，您可以连续运行两个 **show proccesses** 命令，并比较输出以确定：

- CPU 占用率。
- 每个线程的CPU使用率（通过将具体线程的运行时间增量与总运行时间增量作比较来确定）。

设备作为具有许多不同执行线程的单个流程运行。此命令的输出实际上显示了每个线程的内存分配和可用内存。由于这些线程协同处理与设备操作相关的数据流和其他操作，因此一个线程可能会分配内存块，而另一个线程可能会释放该内存块。输出的最后一行包含所有线程的总数。通过监控分配和可用内存之间的差异，仅此行可用于跟踪潜在的内存泄漏。

示例

以下示例展示如何显示正在运行的流程的列表：命令输出自动换行。

```
> show processes
    PC                 SP                 STATE                 Runtime               SBASE

Stack Process TID
Mwe 0x00007f9ae994881e 0x00007f9acb9d6e18 0x00007f9b027e1340          0 0x00007f9acb9cf030
32000/32768 zone_background_idb 140
Mwe 0x00007f9ae91d64ae 0x00007f9ae7659cd8 0x00007f9b027e1340          0 0x00007f9ae7652030
27568/32768 WebVPN KCD Process 14
Msi 0x00007f9aea3f8c04 0x00007f9acba86e48 0x00007f9b027e1340       2917 0x00007f9acba7f030
29944/32768 vpnlb_timer_thread 131
```

以下示例显示如何列出系统流程。

```
> show processes system
  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
23302 root       0 -20 1896m 558m 101m S  198  7.1  16939:07 lina
 8330 admin     20   0 15240 1188  852 R    2  0.0   0:00.01 top
23148 root      20   0 29780 2876 1268 S    2  0.0  41:27.25 UEChanneld
(...output truncated...)
```

以下示例展示如何显示每个流程的 CPU 使用率：

```
> show processes cpu-usage non-zero
PC         Thread       5Sec     1Min     5Min   Process
0x00007f9ae8abcc76   0x00007f9ad04cf7a0     0.2%     0.0%     0.0%   Environment Monitor
Process
```

以下示例展示如何显示正在大量占用 CPU 的流程的数量及详细信息：

```
> show processes cpu-hog
Process:      cli_xml_server, NUMHOG: 12, MAXHOG: 30, LASTHOG: 2
LASTHOG At:   17:37:08 UTC Oct 28 2016
PC:           0x00007f9ae9b11539 (suspend)
Call stack:   0x00007f9ae9b11539  0x00007f9ae9caf084  0x00007f9ae9caf9d0
              0x00007f9ae8736425  0x00007f9ae9b13346  0x00007f9ae9b15ab4
              0x00007f9ae8730ead  0x00007f9ae87663ec  0x00007f9ae6eccde0
              0x00007f9ac4a46120  0x31223d646920696c
(...output truncated...)
```

以下示例展示如何显示每个流程的内存分配：

```
> show processes memory

------------------------------------------------------------------------------
Allocs      Allocated             Frees       Freed                 Process
             (bytes)                           (bytes)
------------------------------------------------------------------------------
0           0                     0           0                     *System Main*
0           0                     0           0                     QoS Support Module
0           0                     0           0                     SSL
0           0                     0           0                     vpnfol_thread_sync
22          8636                  78          3728                  DHCP Network Scope
Monitor
7           40459                 0           0                     Integrity FW Task
0           0                     0           0                     uauth_urlb clean
2           64                    0           0                     arp_timer
8450        233220                0           0                     HDD Health Monitor
14638       1659384               14509       1570750               PTHREAD-23518
0           0                     6           1926                  DHCP Client
(...output truncated...)
```

以下示例展示如何显示每个流程的内部详细信息：

```
> show processes internals
     Invoked      Giveups  Max_Runtime  Process
           1            0        0.002  zone_background_idb
           2            0        0.163  WebVPN KCD Process
      507512            0        0.060  vpnlb_timer_thread
           2            0        0.057  vpnlb_thread
     2029820            0        0.130  vpnfol_thread_unsent
      507455            0        0.137  vpnfol_thread_timer
(...output truncated...)
```

show process-tree

要以树关系显示系统流程，请使用 **show process-tree** 命令。

show process-tree

Command History

版本	修改
6.1	引入了此命令。

使用指南

此命令的输出主要供思科技术支持人员使用。

示例

以下是显示流程树的示例。

```
> show process-tree
init(1)-+-acpid(23138)
        |-agetty(23726)
        |-crond(23141)
        |-dbus-daemon(23119)
        |-login(23727)---clish(6394)
        |-nscd(14445)-+-{nscd}(14448)
        |             |-{nscd}(14449)
        |             |-{nscd}(14450)
        |             |-{nscd}(14451)
        |             |-{nscd}(14452)
        |             `-{nscd}(14453)
(...remaining output truncated...)
```

show ptp

要显示精确时间协议 (PTP) 统计信息和时钟信息，请使用 **show ptp** 命令。

show ptp {**clock** | **port** [*interface_name*]}

Syntax Description

clock	显示 PTP 时钟属性。
port [*interface_name*]	显示接口的PTP端口信息。您可以选择指定接口名称，以仅查看有关该接口的信息。

Command History

版本	修改
6.5	引入了此命令。

示例

以下示例显示未配置 PTP。PTP 数据包可以通过设备，但设备不使用 PTP 时钟。

```
> show ptp clock
 No clock information is available in PTP forwarding mode.
> show ptp port
 No clock information is available in PTP forwarding mode.
```

以下示例显示了 PTP 时钟属性：

```
> show ptp clock
PTP CLOCK INFO
PTP Device Type: Transparent Clock
Operation mode: One Step
Clock Identity: 0:8:2F:FF:FE:E8:43:81
Clock Domain: 0
Number of PTP ports: 4
```

以下示例显示所有启用 PTP 的接口的 PTP 端口信息：

```
> show ptp port
PTP PORT DATASET: GigabitEthernet1/1
Port identity: clock identity: 0:8:2F:FF:FE:E8:43:81
Port identity: port number: 1
PTP version: 2
Port state: Enabled

PTP PORT DATASET: GigabitEthernet1/2
Port identity: clock identity: 0:8:2F:FF:FE:E8:43:81
Port identity: port number: 2
PTP version: 2
Port state: Disabled

PTP PORT DATASET: GigabitEthernet1/3
Port identity: clock identity: 0:8:2F:FF:FE:E8:43:81
Port identity: port number: 3
```

```
PTP version: 2
Port state: Disabled

PTP PORT DATASET: GigabitEthernet1/4
Port identity: clock identity: 0:8:2F:FF:FE:E8:43:81
Port identity: port number: 4
PTP version: 2
Port state: Enabled
```

show quota

要显示当前会话的配额统计信息，请使用 **show quota** 命令。

show quota ［**management-session**］

Syntax Description

management-session	显示当前管理会话的统计信息。

Command History

版本	修改
6.1	引入了此命令。

使用指南

您无法在 threat defense上配置管理会话配额。此命令应始终显示无限制。

示例

以下示例显示配额统计信息。

```
> show quota
quota management-session limit 0
quota management-session warning level 0
quota management-session level 0
quota management-session high water 0
quota management-session errors 0
quota management-session warnings 0
```

show raid

要查看 RAID 中 SSD 的状态，请使用 **show raid** 命令。

注释 仅在 Secure Firewall 3100 上支持此命令。

show raid

Command History

版本	修改
7.1	引入了此命令。

示例

以下示例显示了 RAID 中的两个 SSD：

```
> show raid
Virtual Drive
ID:                           1
Size (MB):                    858306
Operability:                  operable
Presence:                     equipped
Lifecycle:                    available
Drive State:                  optimal
Type:                         raid
Level:                        raid1
Max Disks:                    2
Meta Version:                 1.0
Array State:                  active
Sync Action:                  idle
Sync Completed:               unknown
Degraded:                     0
Sync Speed:                   none

RAID member Disk:
Device Name:                  nvme0n1
Disk State:                   in-sync
Disk Slot:                    1
Read Errors:                  0
Recovery Start:               none
Bad Blocks:
Unacknowledged Bad Blocks:

Device Name:                  nvme1n1
Disk State:                   in-sync
Disk Slot:                    2
Read Errors:                  0
Recovery Start:               none
Bad Blocks:
Unacknowledged Bad Blocks:
```

以下示例显示了 RAID 中的一个 SSD； disk2 不存在，并且 RAID 显示为“已降级”：

```
> show raid
Virtual Drive
ID:                           1
Size (MB):                    858306
Operability:                  degraded
Presence:                     equipped
Lifecycle:                    available
Drive State:                  degraded
Type:                         raid
Level:                        raid1
Max Disks:                    2
Meta Version:                 1.0
Array State:                  active
Sync Action:                  idle
Sync Completed:               unknown
Degraded:                     1
Sync Speed:                   none

RAID member Disk:
Device Name:                  nvme0n1
Disk State:                   in-sync
Disk Slot:                    1
Read Errors:                  0
Recovery Start:               none
Bad Blocks:
Unacknowledged Bad Blocks:
```

Related Commands

命令	Description
configure raid	在 RAID 中添加或删除 SSD。
show ssd	显示 SSD 状态。

show random-password, random-strong-password

要生成可在更改密码时使用的密码，请使用以下命令之一

show { **random-password** | **random-strong-password** } *length*

Syntax Description

random-password	生成不包含特殊字符的随机密码。
random-strong-password	生成强随机密码，即包含特殊字符的密码。
length	指定要生成的密码的长度，8-127 个字符。

Command History

版本	修改
7.0	引入了此命令。

使用指南

生成密码仅适用于FXOS平台。如果您不想设置自己的密码，可以将这些命令与更改密码结合使用。

输入命令后，系统将显示随机密码。您可以复制/粘贴或记下密码。在任何类型的下一次按键时，密码将从输出中擦除，以便其他用户无法获取密码。

示例

以下示例显示如何使用生成的密码更改 joeuser 的密码。首先，使用 **show user** 确定最小密码长度以及是否需要强密码。在这种情况下，最小长度 (MinL) 为 8 个字符，密码强度 (Str) 为“已启用”。接下来，我们将生成 12 个字符的强密码（超过最小长度）。将其复制到剪贴板，然后将其粘贴到更改密码命令中，当更改另一个用户的密码时为 **configure user password**，当更改您登录的账户的密码时则为 **configure password**。

```
> show user
Login       UID   Auth Access  Enabled Reset   Exp  Warn    Grace MinL Str Lock Max
joeuser    1001  Local Config  Enabled   Yes   180     7  Disabled    8 Ena   No   5
> show random-strong-password 12
4j9@!GEhnL>V
> configure user password joeuser
Enter new password for user joeuser: <paste not shown>
Confirm new password for user joeuser: <paste not shown>
```

以下示例显示了尝试在非 FXOS 平台上或 FXOS 版本不支持随机密码生成的 FXOS 平台上生成密码时所看到的内容。

```
> show random-strong-password 12
Password generator is not available.
```

命令	Description
configure password	设置已登录用户的密码。

命令	Description
configure user minpasswdlength	添加新用户。
configure user password	为指定用户设置密码。
configure user strength-check	设置强密码要求。
show user	显示用户账号。

show resource types

要查看设备跟踪使用情况的资源类型，请使用 **show resource types** 命令。

show resource types

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例展示资源类型：

```
> show resource types
Rate limited resource types:
  Conns                     Connections/sec
  Inspects                  Inspects/sec
  Syslogs                   Syslogs/sec

Absolute limit types:
  Conns                     Connections
  Hosts                     Hosts
  IPSec                     IPSec Mgmt Tunnels
  Mac-addresses             MAC Address table entries
  ASDM                      ASDM Connections
  SSH Client                SSH Client Sessions
  SSH Server                SSH Server Sessions
  Storage                   Storage Limit Size of context directory in MB
  Telnet                    Telnet Sessions
  Xlates                    XLATE Objects
  Routes                    Routing Table Entries
  All                       All Resources
  Other VPN Sessions        Other VPN Sessions
  Other VPN Burst           Allowable burst for Other VPN Sessions
  AnyConnect                AnyConnect Premium licensed sessions
  AnyConnect Burst          Allowable burst for AnyConnect Premium licensed sessions
  IKEv1 in-negotiation      Allowable in negotiation IKEv1 SAs
```

Related Commands

命令	Description
clear resource usage	清除资源使用统计信息
show resource usage	显示设备的资源使用情况。

show resource usage

要在多模式 或每个情景的资源使用情况，请使用 **show resource usage** 命令。

show resource usage ［**all** | **detail**］［**resource** {［**rate**］ *resource_name* | **all**}］［**counter** *counter_name* ［*count_threshold*］］

Syntax Description

all	所有类型。
count_threshold	设置要显示资源须达到的资源使用量下限。默认值为 1。如果资源的使用率低于所设置的数字，则不会显示资源。如果为计数器名称指定 all，则 count_threshold 适用于当前使用情况。要显示所有资源，请将 count_threshold 设置为 0。
counter *counter_name*	显示以下计数器类型的计数： • **current**- 显示活动并发实例数或资源的当前使用率。 • **peak**- 显示自上一次清除统计信息（使用 **clear resource usage** 命令或由于设备重启）以来，峰值并发实例数或资源的峰值使用率。 • **denied**- 显示由于超过 Limit 列中所示的资源限制而被拒绝的实例的数量。 • **all**-（默认）显示所有统计信息。
detail	显示所有资源（包括不能管理的资源）的使用情况。例如，可以查看 TCP 拦截次数。
resource {[**rate**] *resource_name* | **all**}	显示特定资源的使用情况。为所有资源指定 **all** 。指定使用率可显示资源的使用率。按使用率衡量的资源包括 **conns**、 **inspects**和 **syslogs**。对于这些资源类型，必须指定 **rate** 关键字。 **conns** 资源也可以按并发连接数来测量；要查看每秒连接数，必须使用 rate 关键字。请参阅使用指南部分。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用 **resource** 关键字时，资源包括以下类型：

- **asdm**- threat defense不支持与此关键字相关的功能。
- **conns**—任意两台主机之间的 TCP 或 UDP 连接数，包括一台主机和多台其他主机之间的连接。
- **hosts**- 可以通过 threat defense 设备连接的主机。
- **ipsec**- IPSec 管理隧道

- **mac-addresses**-对于透明防火墙模式，表示 MAC 地址表中允许的 MAC 地址数量。
- **rate**- 按使用率测量的资源。指定 **conns**、 **inspects**或 **syslogs**。
- **routes**-路由表条目。
- **ssh**-SSH 会话。
- **storage**-情景目录 (以 MB 为单位)。
- **telnet**-Telnet 会话。
- **vpn** - VPN 资源。
- **vpn anyconnect**-AnyConnect 高级许可证限制。
- **vpn ikev1 in-negotiation**- 可以协商的 IKEv1 会话数。
- **VPN Other** - 站点间 VPN 会话。
- **VPN Burst Other** - 站点间 VPN 突发会话。
- **xlates**—NAT 转换。

示例

以下是 **show resource usage** 命令的样本输出，其中显示所有资源的资源使用情况。设备处于单情景模式，因此情景显示为系统。

```
> show resource usage
Resource                Current         Peak      Limit         Denied Context
Syslogs [rate]                0          144        N/A              0 System
Conns                         0            5     100000              0 System
Xlates                        0            5        N/A              0 System
Hosts                         0            8        N/A              0 System
Conns [rate]                  0            1        N/A              0 System
Inspects [rate]               0            3        N/A              0 System
Mac-addresses                 0            4      16384              0 System
Routes                        9            9  unlimited              0 System
```

Related Commands

命令	Description
clear resource usage	清除资源使用统计信息
show resource types	显示资源类型列表。

show rip database

要显示 RIP 拓扑数据库中存储的信息，请使用 **show rip database** 命令。

show rip database ［*ip_addr* ［*mask*］］

Syntax Description

ip_addr	（可选）限制要为指定网络地址显示的路由。
mask	（可选）指定可选网络地址的网络掩码。

Command History

版本	修改
6.1	引入了此命令。

使用指南

RIP 数据库包含通过 RIP 获知的所有路由。在该数据库中出现的路由不一定出现在路由表中。

示例

以下是 **show rip database** 命令的输出示例：

```
> show rip database

10.0.0.0/8    auto-summary
10.11.11.0/24    directly connected, GigabitEthernet0/2
10.1.0.0/8    auto-summary
10.11.0.0/16    int-summary
10.11.10.0/24    directly connected, GigabitEthernet0/3
192.168.1.1/24
    [2] via 10.11.10.5, 00:00:14, GigabitEthernet0/3
```

以下是 **show rip database** 命令的输出示例，其中包含网络地址和网络掩码：

```
> show rip database 172.19.86.0 255.255.255.0
172.19.86.0/24
    [1] via 172.19.67.38, 00:00:25, GigabitEthernet0/2
    [2] via 172.19.70.36, 00:00:14, GigabitEthernet0/3
```

show rollback-status

要显示从 管理中心发送的最新回滚作业（如有）的状态，请使用 **show rollback-status** 命令。

show rollback-status

Command History

版本	修改
6.3	引入了此命令。

使用指南

如果 管理中心 需要在部署作业期间回滚配置更改，它会向设备发送请求，然后重置 管理中心 与设备的管理连接。您可以使用此命令查看回滚作业的状态。

回滚作业仅与运行配置文件中配置的命令相关；它不会回滚 Snort 配置。

如果设备在高可用性模式下运行，请仅在主用设备上使用此命令。在集群中，只能在主设备上使用命令。

信息包括以下内容：

- 状态- 最近的回滚作业的状态。
  - 无 - 未曾请求回滚作业。
  - 正在进行 - 系统已收到回滚请求，并且正在执行回滚作业。
  - 成功 - 回滚已成功完成。
  - 已恢复 - 回滚到从 设备管理器 发送的配置失败。系统将恢复为上次保存的配置。
  - 失败 - 回滚已完成，但出现错误。
- 开始时间/结束时间 - 作业的开始和结束时间。N/A 表示没有作业；对于结束时间，N/A 也可能意味着作业仍在进行中。

示例

以下示例显示了未请求回滚作业的正常情况。

```
> show rollback-status
        Status      : None
        Start Time  : N/A
        End Time    : N/A
```

Related Commands

命令	Description
show running-config	显示在运行配置文件中定义的配置。

show route

要显示数据接口的路由表，请使用 **show route** 命令。

show route ［ **vrf** *name* ｜ **all** ］ **summary** ［ **management-only** ］ ［ **cluster** ｜ **failover** ｜ *ip_address* ［ *mask* ］ ［ **longer-prefixes** ］ ｜ **bgp** ［ *as_number* ］ ｜ **connected** ｜ **eigrp** ［ *process_id* ］ ｜ **isis** ｜ **ospf** ［ *process_id* ］ ｜ **rip** ｜ **static** ｜ **summary** ｜ **zone** ］

Syntax Description

bgp *as_number*	（可选）显示BGP路由的路由信息库(RIB)代编号（序列号）、当前计时器值以及网络描述符块代编号（序列号）。AS 编号将显示限制为使用指定 AS 编号的路由条目。
cluster	（可选）显示路由信息库 (RIB) 代编号（序列号）、当前计时器值以及网络描述符块代编号（序列号）。
connected	（可选）显示已连接的路由。
eigrp *process_id*	（可选）显示 EIGRP 路由。但是， threat defense 不支持 EIGRP。
failover	（可选）显示出现故障转移且备用设备变为主用设备后的当前路由表序列号和路由条目数。
interface_name	（可选）要显示使用指定接口的路由条目。
ip_address mask	（可选）显示通往指定目的地的路由。
isis	（可选）显示 IS-IS 路由。
longer-prefixes	（可选）仅显示与指定的 IP 地址/掩码对匹配的路由
management-only	（可选）显示 IPv4 管理路由表中的路由。
ospf *process_id*	（可选）显示 OSPF 路由。
rip	（可选）显示 RIP 路由。
static	（可选）显示静态路由。
summary	（可选）显示路由表的当前状态。
［**vrf***name* ｜ **all**］ **summary**	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将视图限制为特定虚拟路由器。如果要查看所有虚拟路由器的路由表，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则命令会显示全局 VRF 虚拟路由器的路由表。摘要关键字可用于查看所有 VRF 的路由信息。
zone	（可选）显示区域接口的路由。

Command History

版本	修改
6.1	引入了此命令。
6.6	添加了 ［**vrf** *name*	**all**］ 关键字。

使用指南

show route 命令的输出类似于 **show ipv6 route** 命令的输出，唯一不同之处是，前者显示的信息是IPv4特定信息。所示路由仅适用于数据接口，不适用于虚拟管理接口。要查看管理接口的默认网关，请使用 **show network** 命令。要查看管理接口上的路由，请使用 **show network-static-routes** 命令。

注释 除非在 threat defense 设备上配置了这些功能，否则不会显示 **clustering** 和 **failover** 关键字。

show route 命令列出可用于新连接的“最佳”路由。如果您将允许的 TCP SYN 发送到备用接口，threat defense 设备只能使用同一个接口作出响应。如果该接口上的 RIB 中没有默认路由，设备将会由于没有邻接而丢弃数据包。 **show running-config route** 命令中所示的所有配置将保留在系统的某些数据结构中。

使用 **show asp table routing** 命令可查看特定于后端接口的路由表。这一设计类似于 OSPF 或 EIGRP，其中的协议特定路由数据库不同于全局路由表，后者仅显示“最佳”路由。此行为是有意设计的行为。

示例

以下是 **show route** 命令的输出示例：

```
> show route

Codes: L - Local, C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, E - EGP, EX - EIGRP external, O - OSPF, I - IGRP, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, su - IS-IS summary, U - per-user static route, o - ODR
       P - periodic downloaded static route, + - replicated route

Gateway of last resort is 10.86.194.1 to network 0.0.0.0

C    10.86.194.0 255.255.255.0 is directly connected, outside
C    10.40.10.0 255.255.255.0 is directly connected, inside
C    192.168.2.0 255.255.255.0 is directly connected, faillink
C    192.168.3.0 255.255.255.0 is directly connected, statelink
```

以下是 **show route failover** 命令的输出示例，其中显示在故障转移后 OSPF 和 EIGRP 路由与备用设备之间的同步情况：

```
> show route failover

Codes: L - Local, C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, E - EGP, EX - EIGRP external, O - OSPF, I - IGRP, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, su - IS-IS summary, U - per-user static route, o - ODR
       P - periodic downloaded static route, + - replicated route

Gateway of last resort is 10.86.194.1 to network 0.0.0.0
Routing table sequence number 1
Reconvergence timer 00.20 (Running)

S    10.10.10.0 255.0.0.0 [1/0] via 10.10.10.1, mgmt, seq 1
                        [1/0] via 10.10.10.2, mgmt, seq 1
D    209.165.200.224 255.255.255.0 [90/28416] via 200.165.200.225, 0:00:15, outside, seq 1

O   198.51.100.0 255.255.255.0 [110/28416] via 198.51.100.10, 0:24:45, inside, seq 0

D   10.65.68.220 255.255.255.255 [1/0] via 10.76.11.1, mgmt, seq 1
```

以下是 **show route cluster** 命令的输出示例：

```
> show route cluster
Codes: L - Local, C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, E - EGP, EX - EIGRP external, O - OSPF, I - IGRP, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, su - IS-IS summary, U - per-user static route, o - ODR
       P - periodic downloaded static route, + - replicated route

Gateway of last resort is not set

Routing table seq num 2
Reconvergence timer expires in 52 secs

C    70.0.0.0 255.255.255.0 is directly connected, cluster, seq 1
C    172.23.0.0 255.255.0.0 is directly connected, tftp, seq 1
C    200.165.200.0 255.255.255.0 is directly connected, outside, seq 1
C    198.51.100.0 255.255.255.0 is directly connected, inside, seq 1
O   198.51.100.0 255.255.255.0 [110/28416] via 198.51.100.10, 0:24:45, inside, seq 2
D   209.165.200.224 255.255.255.0 [90/28416] via 200.165.200.225, 0:00:15, outside, seq 2
```

以下是 **show route summary** 命令的输出示例：

```
> show route summary

IP routing table maximum-paths is 3
Route Source    Networks    Subnets     Replicates  Overhead    Memory (bytes)
connected       0           2           0           176         576
static          1           0           0           88          288
bgp 2           0           0           0           0           0
  External: 0 Internal: 0 Local: 0
internal        1                                               408
Total           2           2           0           264         1272
```

以下示例显示已启用虚拟路由和转发 (VRF) 时所有虚拟路由器中的路由。在本例中，除了首先显示的全局路由器之外，还有两个虚拟路由器（test1 和 test2）。

```
> show route all

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
```

```
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF
Gateway of last resort is not set

C        192.168.0.0 255.255.255.0 is directly connected, inside1
L        192.168.0.100 255.255.255.255 is directly connected, inside1


Routing Table: test1
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF
Gateway of last resort is not set

C        10.10.10.0 255.255.255.0 is directly connected, outside
L        10.10.10.10 255.255.255.255 is directly connected, outside


Routing Table: test2
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF
Gateway of last resort is not set

C        20.20.20.0 255.255.255.0 is directly connected, inside
L        20.20.20.20 255.255.255.255 is directly connected, inside
```

以下示例显示名为 red 的虚拟路由器的路由。请注意，泄漏到其他虚拟路由器的静态路由使用密钥 SI 表示。

```
> show route vrf red

Routing Table: red
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF
Gateway of last resort is not set

C        2.1.1.0 255.255.255.0 is directly connected, gig0
L        2.1.1.2 255.255.255.255 is directly connected, gig0
S        7.0.0.0 255.0.0.0 [1/0] via 8.1.1.1, gig0
SI       11.0.0.0 255.0.0.0 [1/0] is directly connected, gig3
```

以下示例显示所有 VRF 的路由摘要。

```
> show route all summary
IP routing table maximum-paths is 8
Route Source    Networks    Subnets     Replicates  Overhead    Memory (bytes)
connected            0           4           0           352         1184
static               1           0           0           88          296
ospf 1               0           0           0           0           0
  Intra-area: 0 Inter-area: 0 External-1: 0 External-2: 0
  NSSA External-1: 0 NSSA External-2: 0
internal                 2                                           792
Total                    3           4           0           440         2272


Routing Table: v1
IP routing table maximum-paths is 8
Route Source    Networks    Subnets     Replicates  Overhead    Memory (bytes)
connected            0           2           0           176         592
static               0           0           0           0           0
ospf 12              0           0           0           0           0
  Intra-area: 0 Inter-area: 0 External-1: 0 External-2: 0
  NSSA External-1: 0 NSSA External-2: 0
internal                 1                                           416
Total                    1           2           0           176         1008


Routing Table: v2
IP routing table maximum-paths is 8
Route Source    Networks    Subnets     Replicates  Overhead    Memory (bytes)
connected            0           2           0           176         592
static               0           0           0           0           0
ospf 13              0           0           0           0           0
  Intra-area: 0 Inter-area: 0 External-1: 0 External-2: 0
  NSSA External-1: 0 NSSA External-2: 0
internal                 1                                           416
Total                    1           2           0           176         1008
```

Related Commands

命令	Description
show ipv6 route	显示 IPv6 路由表。
show vrf	显示系统上的虚拟路由器。

show route-map

要显示路由地图信息，请使用 **show route-map** 命令。

show route-map [**all** | **dynamic** [**application** [*application*] | **detail** | *route_map*] | *route_map*]

Syntax Description

all	显示有关静态和动态路由地图的信息。
dynamic	仅显示有关动态路由地图的信息。
application *application*	创建路由地图的应用。
route_map	为路由地图命名。

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show route-map dynamic** 命令的输出示例：

```
> show route-map dynamic
route-map MIP-10/24/06-05:23:46.091-1-MPATH_1, permit, sequence 0, identifier 54943520
  Match clauses:
    ip address (access-lists): VOICE
  Set clauses:
    interface Tunnel0
  Policy routing matches: 0 packets, 0 bytes
 Current active dynamic routemaps = 1
```

show rule hits

要显示所有评估的访问控制策略和预过滤器策略的规则命中信息，请使用 **show rule hits** 命令。

show rule hits [**id** *number* | **raw** | **cumulative** | **node-wise**] [**gt** *#hit-count* | **lt** *#hit-count* | **range** *#hit-count1 #hit-count2*]

Syntax Description

cumulative	（可选。）显示所有集群或高可用性 (HA) 节点中规则命中的累计总和。命中计数是按节点计算的，因此总和显示整个集群或HA对的总命中数。
id*number*	（可选）规则的 ID。包含此参数会限制向指定规则显示的信息。指定 ID 时不能指定任何其他选项。 使用 **show access-list** 命令标识规则 ID。
node-wise	（可选。）显示集群或 HA 对中每台设备的当前命中计数。
raw	（可选）以 .csv 格式显示规则命中信息。
gt *#hit-count*	（可选）显示命中计数大于 *#hit-count*的所有规则。
lt *#hit-count*	（可选）显示命中计数小于 *#hit-count*的所有规则。
range *#hit-count1 #hit-count2*	（可选）显示命中计数介于 *#hit-count1* 和 *#hit-count2*之间的所有规则。

Command Default

如果不指定规则 ID，则会显示所有规则的规则命中信息。

Command History

版本	修改
6.4	引入了此命令。
7.2	添加了 **cumulative** 和 **node-wise** 关键字。

使用指南

规则命中信息仅涵盖访问控制规则和预过滤器规则。

查看访问控制或预过滤策略时，可以使用本地或远程设备管理器更轻松地查看规则命中信息。请注意，此命令中显示的规则命中信息基于实际规则，而不是为部分实施规则而生成的任何ACL中的任何访问控制条目 (ACE)。因此，此命令显示的命中计数信息不等同于 **show access-list** 命令显示的命中计数。

使用**show access-list** 命令标识规则ID。但是，此命令的输出中并未列出所有规则。对于管理中心受管设备，您可以对以下 URL 使用 REST API GET 操作来查看所有规则及其 ID：

- `/api/fmc_config/v1/domain/{domainUUID}/policy/accesspolicies/{containerUUID}/operational/hitcounts?filter="deviceId:{deviceId}"&expanded=true`
- `/api/fmc_config/v1/domain/{domainUUID}/policy/prefilterpolicies/{containerUUID}`

```
/operational/hitcounts?filter="deviceId:{deviceId}"&expanded=true
```

示例

以下示例显示规则命中信息：

```
> show rule hits
RuleID            Hit Count       First Hit Time(UTC)       Last Hit Time(UTC)
--------------------------------------------------------------------------------
268436979            1            22:01:39 Jan 25 2019      22:01:39 Jan 25 2019
268436980            1            22:01:51 Jan 25 2019      22:01:51 Jan 25 2019
268436981            2            22:02:00 Jan 25 2019      22:02:02 Jan 25 2019
268436925            2            22:01:53 Jan 25 2019      22:04:51 Jan 25 2019
```

以下示例显示集群或 HA 对中所有设备的摘要命中计数。

```
> show rule hits cumulative

RuleID               Hit Count           First Hit Time(UTC)     Last Hit Time(UTC)
--------------------------------------------------------------------------------
111116               2                   10:03:55 Apr 12 2021     10:04:02 Apr 12 2021

111117               1                   10:03:59 Apr 12 2021     10:03:59 Apr 12 2021
111119               1                   10:04:05 Apr 12 2021     10:04:05 Apr 12 2021
```

以下示例显示集群或 HA 对中每台设备的命中计数。为每个设备单独保存命中计数。

```
> show rule hits node-wise

Active/Control node rule hits:

RuleID               Hit Count           First Hit Time(UTC)     Last Hit Time(UTC)
--------------------------------------------------------------------------------
111116               1                   10:03:55 Apr 12 2021     10:03:55 Apr 12 2021

111117               1                   10:03:59 Apr 12 2021     10:03:59 Apr 12 2021

Standby/Data node rule hits:

RuleID               Hit Count           First Hit Time(UTC)     Last Hit Time(UTC)
--------------------------------------------------------------------------------

111116               1                   10:04:02 Apr 12 2021     10:04:02 Apr 12 2021

111119               1                   10:04:05 Apr 12 2021     10:04:05 Apr 12 2021
```

Related Commands

命令	Description
clear rule hits	清除访问控制策略和预过滤器策略的所有评估规则的规则命中信息，并将其重置为零。
show cluster rule hits	以汇总格式显示来自集群所有节点的访问控制策略和预过滤器策略的所有评估规则命中信息。

命令	Description
cluster exec show rule hits	以隔离的格式显示集群中每个节点的访问控制策略和预过滤器策略的所有评估规则命中信息。
cluster exec clear rule hits	从集群中的所有节点清除访问控制策略和预过滤器策略的所有评估规则的规则命中信息，并将其重置为零。

show running-config

要显示设备上当前运行的配置，请使用 **show running-config** 命令。

show running-config ［**all**］［*command*］

Syntax Description

all	显示整个运行配置，包括默认设置。
command	显示与特定命令关联的配置。有关可用 命令，请参阅 **show running-config ?**CLI 帮助。 **注释** threat defense 不直接支持 CLI 帮助中列出的每个命令。给定选项可能没有任何配置。某些选项只能使用 管理中心的 FlexConfig 进行配置。

Command History

版本	修改
6.1	引入了此命令。

使用指南

show running-config 命令用于显示设备上的内存中的活动配置（包括保存的配置更改）。您不能直接配置这些命令。相反，它们由控制设备的管理器配置，例如 管理中心 或 设备管理器。

但是，这是部分配置。它仅显示可使用 ASA 软件配置命令配置的内容，但某些命令可能特定于 threat defense。这些命令移植到 threat defense。因此，您应仅将运行配置中的信息用作故障排除辅助工具。使用 管理中心设备管理器作为分析设备配置的主要方法。

示例

以下是 **show running-config** 命令的输出示例：

```
> show running-config
: Saved

:
: Serial Number: XXXXXXXXXXX
: Hardware:   ASA5512, 4096 MB RAM, CPU Clarkdale 2793 MHz, 1 CPU (2 cores)
:
NGFW Version 6.1.0
!
hostname firepower
enable password $sha512$5000$Col980QPR9VVq/VYoAkGJw==$ZvzuZDNpcvvEP/DGbBqytA== pbkdf2
strong-encryption-disable
names

!
interface GigabitEthernet0/0
 nameif outside
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
```

```
 security-level 0
 ip address 192.168.10.1 255.255.255.0
 ipv6 enable
!
interface GigabitEthernet0/1
 shutdown
 nameif inside
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 security-level 0
 ip address 192.168.1.1 255.255.255.0
 ipv6 enable
!
interface GigabitEthernet0/2
 shutdown
 nameif dmz
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 security-level 0
 ip address 192.168.2.1 255.255.255.0
 ipv6 enable
!
interface GigabitEthernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/4
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/5
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 management-only
 no nameif
 no security-level
 no ip address
!
ftp mode passive
ngips conn-match vlan-id
access-list CSM_FW_ACL_ remark rule-id 9998: PREFILTER POLICY: Default Tunnel and Priority
 Policy
access-list CSM_FW_ACL_ remark rule-id 9998: RULE: DEFAULT TUNNEL ACTION RULE
access-list CSM_FW_ACL_ advanced permit ipinip any any rule-id 9998
access-list CSM_FW_ACL_ advanced permit 41 any any rule-id 9998
access-list CSM_FW_ACL_ advanced permit gre any any rule-id 9998
access-list CSM_FW_ACL_ advanced permit udp any eq 3544 any range 1025 65535 rule-id 9998
access-list CSM_FW_ACL_ advanced permit udp any range 1025 65535 any eq 3544 rule-id 9998
access-list CSM_FW_ACL_ remark rule-id 268434432: ACCESS POLICY: Initial AC Policy - Default/1
access-list CSM_FW_ACL_ remark rule-id 268434432: L4 RULE: DEFAULT ACTION RULE
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268434432
access-list CSM_IPSEC_ACL_1 extended permit ip any6 any6
!
tcp-map UM_STATIC_TCP_MAP
```

```
  tcp-options range 6 7 allow
  tcp-options range 9 18 allow
  tcp-options range 20 255 allow
  tcp-options md5 clear
  urgent-flag allow
!
no pager
logging enable
logging timestamp rfc5424
logging buffered informational
logging flash-minimum-free 1024
logging flash-maximum-allocation 3076
no logging message 106015
no logging message 313001
no logging message 313008
no logging message 106023
no logging message 710003
no logging message 106100
no logging message 302015
no logging message 302014
no logging message 302013
no logging message 302018
no logging message 302017
no logging message 302016
no logging message 302021
no logging message 302020
mtu outside 1500
mtu inside 1500
mtu dmz 1500
no failover
no monitor-interface service-module
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
arp rate-limit 8192
access-group CSM_FW_ACL_ global
as-path access-list 2 deny 100$
as-path access-list 2 permit 200$
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:00:30
timeout floating-conn 0:00:00
timeout conn-holddown 0:00:15
aaa proxy-limit disable
no snmp-server location
no snmp-server contact
no snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
no sysopt connection permit-vpn
crypto ipsec ikev1 transform-set CSM_TS_1 esp-des esp-sha-hmac
crypto ipsec security-association pmtu-aging infinite
crypto map CSM_outside_map 1 match address CSM_IPSEC_ACL_1
crypto map CSM_outside_map 1 set peer 10.10.10.10
crypto map CSM_outside_map 1 set ikev1 transform-set CSM_TS_1
crypto map CSM_outside_map 1 set reverse-route
crypto map CSM_outside_map interface outside
crypto ca trustpool policy
crypto ikev1 enable outside
crypto ikev1 policy 160
 authentication pre-share
```

```
 encryption des
 hash sha
 group 5
 lifetime 86400
telnet timeout 5
console timeout 0
dynamic-access-policy-record DfltAccessPolicy
tunnel-group 10.10.10.10 type ipsec-l2l
tunnel-group 10.10.10.10 ipsec-attributes
 ikev1 pre-shared-key *****
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map type inspect ip-options UM_STATIC_IP_OPTIONS_MAP
 parameters
  eool action allow
  nop action allow
  router-alert action allow
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options UM_STATIC_IP_OPTIONS_MAP
 class class-default
  set connection advanced-options UM_STATIC_TCP_MAP
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:167911f11cbf1140edeffcb0f9b17f01
: end
>
```

要查看 BFD 全局配置设置，请使用输出修饰符过滤 BFD 相关配置。以下是使用输出修饰器 **show running-config bfd** 命令的输出示例：。

```
ciscoftd# show running-config bfd
bfd map ipv4 1.1.1.1/24 1.1.1.2/32 name2
```

以下是使用输出修饰器 **show running-config bfd-template** 命令的输出示例：。

```
ciscoftd# show running-config bfd-template
bfd-template single-hop bfd_template
interval min-tx 50 min-rx 50 multiplier 3
```

```
!
bfd-template single-hop bfd_template_auth
interval min-tx 50 min-rx 50 multiplier 3
authentication md5 ***** key-id 8
!
```

Related Commands

命令	Description
show access-control-config	显示有关访问控制策略的摘要信息。

show s - sz

show sctp

要显示当前的流控制传输协议 (SCTP) Cookie 和关联，请使用 **show sctp** 命令。

show sctp ［**detail**］

Syntax Description

detail	显示 SCTP 关联的详细信息。

Command History

版本	修改
6.1	引入了此命令。

使用指南

命令显示有关 SCTP Cookie 和关联的信息。**show sctp**

如果使用 管理中心FlexConfig 启用 SCTP 检测，则此命令可以显示 SCTP 信息。

示例

以下是 **show sctp** 命令的输出示例：

```
> show sctp

AssocID: 2279da7a
Local:  192.168.107.11/20001 (ESTABLISHED)
Remote: 192.168.108.11/40174 (ESTABLISHED)

AssocID: 4924f520
Local:  192.168.107.11/20001 (ESTABLISHED)
Remote: 192.168.108.11/40200 (ESTABLISHED)
```

以下是 **show sctp detail** 命令的输出示例：

```
> show sctp detail

AssocID: 8b7e3ffb
Local:  192.168.100.56/3868 (ESTABLISHED)
    Receiver Window: 48000
    Cumulative TSN: 5cb6cd9b
    Next TSN: 5cb6cd9c
    Earliest Outstanding TSN: 5cb6cd9c
    Out-of-Order Packet Count: 0
Remote: 192.168.200.78/3868 (ESTABLISHED)
    Receiver Window: 114688
    Cumulative TSN: 5cb6cd98
    Next TSN: 0
    Earliest Outstanding TSN: 5cb6cd9c
    Out-of-Order Packet Count: 0
```

Related Commands

命令	Description
show local-host	显示主机上有关使连接在每个接口上通过设备的信息。
show service-policy inspect sctp	显示 SCTP 检测统计信息。
show traffic	显示每个接口的连接和检测统计信息

show serial-number

要显示印刷电路板 (PCB) 序列号，请使用 **show serial-number** 命令。此命令不适用于虚拟设备。

show serial-number

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用 **show serial-number** 命令查看印刷电路板的序列号。此信息也显示在 **show version system** 和 **show running-config** 输出中。

使用 **show inventory** 命令查看机箱序列号

示例

以下示例显示如何显示序列号。此示例中的数字已更改为无效。

```
> show serial-number
XXX175078X5
```

show service-policy

要显示服务策略统计信息，请使用 **show service-policy** 命令。

show service-policy [**global** | **interface** *intf*] [**cluster flow-mobility** | **inspect** *inspection* [*arguments*] | **police** | **priority** | **set connection** [**details**] | **sfr** | **shape** | **user-statistics**]
show service-policy [**global** | **interface** *intf*] [**flow** *protocol* {**host** *src_host* | *src_ip src_mask*} [**eq** *src_port*] {**host** *dest_host* | *dest_ip dest_mask*} [**eq** *dest_port*] [*icmp_number* | *icmp_control_message*]]

Syntax Description

cluster flow-mobility	（可选。）显示有关 threat defense 集群中流移动性的状态信息。
dest_ip dest_mask	对应 **flow** 关键字，指流量流的目标 IP 地址和子网掩码。
details	（可选）对应 **set connection** 关键字，如果启用每客户端连接限制，则显示每客户端连接信息。
eq *dest_port*	（可选）对应 **flow** 关键字，等于流的目标端口。
eq *src_port*	（可选）对应 **flow** 关键字，等于流的源端口。
flow 协议	（可选）显示与通过 5 元组（协议、源 IP 地址、源端口、目标 IP 地址、目标端口）标识的特定流匹配的策略。您可以使用此命令检查服务策略配置是否将提供特定连接所需的服务。
global	（可选）限制全局策略的输出。
host *dest_host*	对应 **flow** 关键字，指流量流的主机目标 IP 地址。
host *src_host*	对应 **flow** 关键字，指流量流的主机源 IP 地址。
icmp_control_message	（可选）对应 **flow** 关键字，当指定 ICMP 作为协议时，指定流量流的 ICMP 控制消息。
icmp_number	（可选）对应 **flow** 关键字，当指定 ICMP 作为协议时，指定流量流的 ICMP 协议编号。
inspect *inspection* [*arguments*]	（可选）显示有关包括 **inspect** 命令的策略的详细信息。并非所有 **inspect** 命令都受到详细输出支持。要查看所有检测，请使用 **show service-policy inspect ?** 命令。各个检查的可用参数各不相同；请参阅 CLI 帮助以获取更多信息。
interface *intf*	（可选）显示应用到通过 *intf* 参数指定的接口的策略，其中 *intf* 是接口名称。
police	（可选）显示有关包括 **police** 命令的策略的详细信息。
priority	（可选）显示有关包括 **priority** 命令的策略的详细信息。

set connection	（可选）显示有关包括 **set connection** 命令的策略的详细信息。
sfr	（可选）显示有关 ASA FirePOWER 模块策略的详细信息。此关键字对 threat defense无意义。
shape	（可选）显示有关包括 **shape** 命令的策略的详细信息。
src_ip src_mask	对应 **flow** 关键字，指流量流中使用的源 IP 地址和子网掩码。
user-statistics	（可选）显示有关包括 **user-statistics** 命令的策略的详细信息。此关键字对 threat defense无意义。

Command Default

如果不指定任何参数，此命令将显示所有全局接口策略。

Command History

版本	修改
6.1	引入了此命令。

使用指南

show service-policy 命令输出中显示的初期连接数表示与为流量类定义的流量匹配的接口的当前初期连接数。“embryonic-conn-max”字段显示为流量类配置的最大初期限制。如果所显示的当前初期连接数等于或超过最大值，将对与流量类型相匹配的新 TCP 连接应用 TCP 拦截。

当对配置进行服务策略更改后，所有新连接都将使用新的服务策略。现有连接将继续使用在连接建立时配置的策略。**show** 命令输出不会包含有关旧连接的数据。要确保所有连接都使用新策略，需要断开当前连接，以便使用新策略重新连接。请参阅 **clear conn** 或 **clear local-host** 命令。

不能直接使用 管理中心 或 设备管理器配置服务策略。编辑各种连接设置或配置 QoS 策略时，会间接进行一些更改。您还可以使用 **configure inspection** 命令调整启用的默认检测。如果在 管理中心 中使用 FlexConfig 配置服务策略，则此命令显示与配置相关的统计信息 。

注释 对于 **inspect icmp** 和 **inspect icmp error** 策略，数据包计数仅包括回应请求和应答数据包。

示例

以下是 **show service-policy** 命令的输出示例。

```
> show service-policy
Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: dns preset_dns_map, packet 0, lock fail 0, drop 0, reset-drop 0,
5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: ftp, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: h323 h225 _default_h323_map, packet 0, lock fail 0, drop 0, reset-drop 0,
5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: h323 ras _default_h323_map, packet 0, lock fail 0, drop 0, reset-drop 0,
```

```
5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: rsh, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: rtsp, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: esmtp _default_esmtp_map, packet 0, lock fail 0, drop 0, reset-drop 0,
5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: sqlnet, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: skinny , packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: sunrpc, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: xdmcp, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: sip , packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: netbios, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: tftp, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: ip-options UM_STATIC_IP_OPTIONS_MAP, packet 0, lock fail 0, drop 0,
reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
    Class-map: class-default
      Default Queueing      Set connection policy:         drop 0
      Set connection advanced-options: UM_STATIC_TCP_MAP
        Retransmission drops: 0                   TCP checksum drops : 0
        Exceeded MSS drops  : 0                   SYN with data drops: 0
        Invalid ACK drops   : 0                   SYN-ACK with data drops: 0
        Out-of-order (OoO) packets : 0            OoO no buffer drops: 0
        OoO buffer timeout drops : 0              SEQ past window drops: 0
        Reserved bit cleared: 0                   Reserved bit drops : 0
        IP TTL modified     : 0                   Urgent flag cleared: 0
        Window varied resets: 0
        TCP-options:
          Selective ACK cleared: 0                Timestamp cleared  : 0
          Window scale cleared : 0
          Other options cleared: 0
          Other options drops: 0
```

对于具有多个 CPU 核心的设备，有一个锁定失败计数器。锁定机制用于保护共享数据结构和变量，因为它们可以被多个核心使用。当核心获取锁失败时，它会尝试再次获取锁。每次尝试失败时，锁定失败计数器都会递增。

```
> show service-policy
Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      ...
      Inspect: esmtp _default_esmtp_map, packet 96716502, lock fail 7, drop 25,
reset-drop 0
      Inspect: sqlnet, packet 2526511491, lock fail 21, drop 2362, reset-drop 0
```

以下命令显示 GTP 检查的统计信息。示例后面的表中对输出进行了说明。

```
> show service-policy inspect gtp statistics
GPRS GTP Statistics:
  version_not_support               0     msg_too_short             0
```

```
unknown_msg                     0     unexpected_sig_msg        0
unexpected_data_msg             0     ie_duplicated             0
mandatory_ie_missing            0     mandatory_ie_incorrect    0
optional_ie_incorrect           0     ie_unknown                0
ie_out_of_order                 0     ie_unexpected             0
total_forwarded                67     total_dropped             1
signalling_msg_dropped          1     data_msg_dropped          0
signalling_msg_forwarded       67     data_msg_forwarded        0
total created_pdp              33     total deleted_pdp        32
total created_pdpmcb           31     total deleted_pdpmcb     30
total dup_sig_mcbinfo           0     total dup_data_mcbinfo    0
no_new_sgw_sig_mcbinfo          0     no_new_sgw_data_mcbinfo   0
pdp_non_existent                1
```

表 *48: GPRS GTP Statistics*

列标题	Description
version_not_support	显示具有不支持的 GTP 版本字段的数据包。
msg_too_short	显示长度小于 8 字节的数据包。
unknown_msg	显示未知类型消息。
unexpected_sig_msg	显示意外的信令消息。
unexpected_data_msg	显示意外数据消息。
mandatory_ie_missing	显示缺少必需信息元素 (IE) 的消息。
mandatory_ie_incorrect	显示具有格式不正确的必需信息元素 (IE) 的消息。
optional_ie_incorrect	显示可选信息元素 (IE) 无效的消息。
ie_unknown	显示具有未知信息元素 (IE) 的消息。
ie_out_of_order	显示具有失序信息元素 (IE) 的消息。
ie_unexpected	显示具有意外信息元素 (IE) 的消息。
ie_duplicated	显示具有重复信息元素 (IE) 的邮件。
optional_ie_incorrect	显示具有格式不正确的可选信息元素 (IE) 的消息。
total_dropped	显示丢弃的消息总数。
signalling_msg_dropped	显示丢弃的信令消息数。
data_msg_dropped	显示丢弃的数据消息数。
total_forwarded	显示转发的消息总数。
signalling_msg_forwarded	显示转发的信令消息数。

列标题	Description
data_msg_forwarded	显示转发的数据消息数。
total created_pdp	显示所创建的数据包数据协议 (PDP) 承载情景总数。
total deleted_pdp	显示所创建的数据包数据协议 (PDP) 承载情景总数。
total created_pdpmcb total deleted_pdpmcb total dup_sig_mcbinfo total dup_data_mcbinfo no_new_sgw_sig_mcbinfo no_new_sgw_data_mcbinfo	这些字段与 PDP 主控制块的使用相关，这是一项实施功能。这些计数器由思科技术支持人员用于故障排除，最终用户并不直接感兴趣。
pdp_non_existent	显示为不存在的 PDP 情景接收的消息数。

以下命令显示有关 PDP 情景的信息：

```
> show service-policy inspect gtp pdp-context
4 in use, 5 most used
Version v1,   TID 050542012151705f,  MS Addr 2005:a00::250:56ff:fe96:eec,
SGSN Addr 10.0.203.22,      Idle 0:52:01,   Timeout 3:00:00,   APN ssenoauth146
Version v2,   TID 0505420121517056,  MS Addr 100.100.100.102,
SGW Addr 10.0.203.24,       Idle 0:00:05,   Timeout 3:00:00,   APN ssenoauth146
Version v2,   TID 0505420121517057,  MS Addr 100.100.100.103,
SGW Addr 10.0.203.25,       Idle 0:00:04,   Timeout 3:00:00,   APN ssenoauth146
Version v2,   TID 0505420121517055,  MS Addr 100.100.100.101,
SGW Addr 10.0.203.23,       Idle 0:00:06,   Timeout 3:00:00,   APN ssenoauth146
```

下表介绍了 **show service-policy inspect gtp pdp-context** 命令的输出。

表 *49: PDP* 情景

列标题	Description
Version	显示 GTP 版本。
TID	显示隧道标识符。
MS Addr	显示移动站地址。
SGSN Addr SGW Addr	显示服务网关服务节点 (SGSN) 或服务网关 (SGW)。
Idle	显示未使用 PDP 或承载情景的时间。
APN	显示接入点名称。

Related Commands

命令	Description
clear service-policy	清除所有服务策略统计信息。
configure inspection	启用或禁用默认检测。
show running-config service-policy	显示在运行配置中配置的服务策略。

show shun

要显示避开信息，请使用 **show shun** 命令。

show shun ［*src_ip* | **statistics**］

Syntax Description

src_ip	（可选）显示该地址的信息。
statistics	（可选）显示接口规避统计信息。

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show shun** 命令的输出示例：

```
> show shun
shun (outside) 10.1.1.27 10.2.2.89 555 666 6
shun (inside1) 10.1.1.27 10.2.2.89 555 666 6
```

Related Commands

命令	Description
clear shun	禁用当前启用的所有 shun 并清除 shun 统计信息。
shun	阻止新连接并禁止通过任何现有连接传输数据包，从而允许对攻击主机作出动态响应。

show sip

要显示 SIP 会话，请使用 **show sip** 命令。

show sip

Command History

版本	修改
6.1	引入了此命令。

使用指南

show sip 命令显示有关通过 threat defense 设备建立的 SIP 会话的信息。

示例

以下是 **show sip** 命令的输出示例：

```
> show sip
Total: 2
call-id c3943000-960ca-2e43-228f@10.130.56.44
 | state Call init, idle 0:00:01
call-id c3943000-860ca-7e1f-11f7@10.130.56.45
 | state Active, idle 0:00:06
```

此示例显示 threat defense 设备中的两个活动 SIP 会话（如 Total 字段中所示）。每个呼叫 ID 代表一个呼叫。

第一个会话（其呼叫 ID 为 c3943000-960ca-2e43-228f@10.130.56.44）处于 Call Init 状态，这意味着会话仍处于呼叫建立阶段。只有看到 ACK 时，才说明呼叫设置完成。此会话已空闲 1 秒。

第二个会话处于 Active 状态，这表示呼叫建立已完成，且终端正在交换媒体。此会话已空闲 6 秒。

Related Commands

命令	Description
show conn	显示不同连接类型的连接状态。

show skinny

要显示 SCCP（瘦客户端）会话的信息，请使用 **show skinny** 命令。

show skinny ［**audio** | **video**］

Syntax Description

audio	显示 SCCP 音频会话
video	显示 SCCP 视频会话

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show skinny** 命令在以下情况时的输出示例。设备中设置了两个活动瘦客户端会话。第一个建立在位于本地地址 10.0.0.11 的内部思科 IP 电话与位于 172.18.1.33 的外部思科统一通信管理器之间。TCP 端口 2000 是思科统一通信管理器。第二个建立在位于本地地址 10.0.0.22 的另一个内部思科 IP 电话与同一思科统一通信管理器之间。

```
> show skinny
MEDIA 10.0.0.22/20798         172.18.1.11/22948
LOCAL                    FOREIGN                 STATE
-----------------------------------------------------------------
1       10.0.0.11/52238         172.18.1.33/2000                1
  MEDIA 10.0.0.11/22948         172.18.1.22/20798
2       10.0.0.22/52232         172.18.1.33/2000                1
  MEDIA 10.0.0.22/20798         172.18.1.11/22948
```

输出表明已在两个内部思科 IP 电话之间建立呼叫。第一个电话和第二个电话的 RTP 侦听端口分别为 UDP 22948 和 20798。

Related Commands

命令	Description
show conn	显示不同连接类型的连接状态。

show sla monitor

要显示有关互联网协议服务水平协议 (IP SLA) 的信息，请使用 **show sla monitor** 命令。

show sla monitor {**configuration** | **operational-state**} [*sla_id*]

Syntax Description

configuration	显示 SLA 配置值，包括默认值。
operational-state	显示 SLA 操作的运行状态。
sla_id	（可选）SLA 操作的 ID 编号。有效值范围为 1 至 2147483647。

Command Default

如果未指定 SLA ID，将显示所有 SLA 操作的配置值。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用 **show running-config sla monitor** 命令查看运行配置中的 SLA 操作命令。

示例

以下是 **show sla monitor configuration** 命令的输出示例。它显示 SLA 操作 124 的配置值。**show sla monitor configuration** 命令输出之后是相同 SLA 操作的 **show running-config sla monitor** 命令输出。

```
> show sla monitor configuration 124

SA Agent, Infrastructure Engine-II
Entry number: 124
Owner:
Tag:
Type of operation to perform: echo
Target address: 10.1.1.1
Interface: outside
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 1000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 3
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:

> show running-config sla monitor 124

sla monitor 124
```

```
 type echo protocol ipIcmpEcho 10.1.1.1 interface outside
 timeout 1000
 frequency 3
sla monitor schedule 124 life forever start-time now
```

以下是 **show sla monitor operational-state** 命令的输出示例：

```
> show sla monitor operational-state

Entry number: 124
Modification time: 14:42:23.607 EST Wed Mar 22 2006
Number of Octets Used by this Entry: 1480
Number of operations attempted: 4043
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: TRUE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): NoConnection/Busy/Timeout
Latest operation start time: 18:04:26.609 EST Wed Mar 22 2006
Latest operation return code: Timeout
RTT Values:
RTTAvg: 0       RTTMin: 0       RTTMax: 0
NumOfRTT: 0     RTTSum: 0       RTTSum2: 0
```

Related Commands

命令	Description
show running-config sla monitor	显示运行配置中的 SLA 操作配置命令。

show snmp-server

要显示有关设备上配置的 SNMP 服务器的信息，请使用 **show snmp-server** 命令。

show snmp-server {**engineID** | **group** | **host** | **statistics** | **user** [*username*]}

Syntax Description

engineID	显示 SNMP 引擎的标识。
group	显示已配置的SNMP组的名称、正在使用的安全模型、不同视图的状态以及每个组的存储类型。
host	显示属于主机组的已配置SNMP主机的名称、正在使用的接口以及正在使用的 SNMP 版本。
statistics	显示 SNMP 服务器统计信息。
user [*username*]	显示有关SNMP用户的特征的信息。您可以选择指定用户名，以将信息限制为该用户。

Command History

版本	修改
6.1	引入了此命令。

使用指南

SNMP 引擎是可以驻留在本地设备上的 SNMP 副本。引擎 ID 是为每个 SNMP 代理分配的唯一值。引擎 ID 不能配置。引擎 ID 的长度为 25 字节，用于生成加密密码。在故障转移对中，引擎 ID 与对等设备同步。

根据 SNMP 的基于视图的访问控制模型 (VACM) 来使用 SNMP 用户和组。SNMP 组确定要使用的安全模型。SNMP 用户应当符合 SNMP 组的安全模型。每个 SNMP 组名称/安全级别对必须唯一。

注释 统计信息显示有关 SNMP 模块的输入和输出数据包的信息。数据包被输出并不意味着它们到达目的地。路由问题、干预防火墙、拔出接口等可能会阻止输出数据包的传输。如果数据包未到达 SNMP 服务器，请使用 **show asp drop** 和 **show logging** 等命令检查其他问题。

示例

以下是 **show snmp-server engineid** 命令的输出示例：

```
> show snmp-server engineid
Local SNMP engineID: 80000009fe85f8fd882920834a3af7e4ca79a0a1220fe10685
```

以下是 **show snmp-server group** 命令的输出示例：

```
> show snmp-server group
```

```
groupname: public                           security model:v1
readview : <no readview specified>          writeview: <no writeview specified>
notifyview: <no readview specified>
row status: active

groupname: public                           security model:v2c
readview : <no readview specified>          writeview: <no writeview specified>
notifyview: *<no readview specified>
row status: active

groupname: privgroup                    security model:v3 priv
readview : def_read_view                writeview: <no writeview specified>
notifyview: def_notify_view
row status: active
```

以下是 **show snmp-server host** 命令的输出示例，其中仅显示轮询设备的活动主机：

```
> show snmp-server host
host ip = 10.10.10.3, interface = mgmt  poll community ***** version 2c
host ip = 10.10.10.6, interface = mgmt  poll community ***** version 2c
```

以下是 **show snmp-server user** 命令的输出示例：

```
> show snmp-server user authuser
User name: authuser
Engine ID: 000000090200000000C025808
storage-type: nonvolatile       active access-list: N/A
Rowstatus: active
Authentication Protocol: MD5
Privacy protocol: DES
Group name: VacmGroupName
```

输出提供以下信息：

- 用户名，是标识 SNMP 用户名称的字符串。
- 引擎 ID，是标识设备上的 SNMP 副本的字符串。
- 存储类型，指示在设备上的易失性或临时内存中还是在非易失性或永久内存中设定设置，如果为后者，则关闭设备再重新开启后，设置仍然保留。
- 活动访问列表，是与 SNMP 用户关联的标准 IP 访问列表。
- Rowstatus，指示其是否处于活动状态。
- 身份验证协议，标识正在使用哪种身份验证协议。选项为 MD5、SHA 或无。如果您的软件映像不支持身份验证，则此字段不显示。
- 隐私协议，指示是否启用 DES 数据包加密。如果您的软件映像不支持隐私，则此字段不显示。
- 组名称，指示用户所属的 SNMP 组。SNMP 组按照基于视图的访问控制模型 (VACM) 进行定义。

Related Commands

命令	Description
clear snmp-server statistics	清除 SNMP 数据包输入和输出计数器。
show running-config snmp-server	显示 SNMP 服务器配置。

show snort counters

要显示 Snort 预处理器连接的统计信息，请使用 **show snort counters** 命令。

show snort counters {**action** | **stream** | **sip** | **ssl** | **smtp** | **vrf**} {**all** | **instance** *x*}

Syntax Description

action	显示操作、限制和判定的 Snort 实例级统计信息。
stream	显示数据流预处理器的统计信息。
sip	显示 SIP 预处理器的统计信息。
ssl	显示 SSL 预处理器的统计信息。
smtp	显示 SMTP 预处理器的统计信息。
vrf	显示通过每个虚拟路由器的实时会话数。
all	显示系统中所有 Snort 实例的统计信息。例如，**show snort counters action all**、 **show snort counters smtp all**等。
instance *x*	显示系统中所选 Snort 实例的统计信息。例如，**show snort counters smtp instance 11**。使用 **show snort instances** 命令确定可用的实例编号。

Command History

版本	修改
6.3	引入了此命令。
6.6	添加了 **vrf** 关键字。

使用指南

使用此命令可显示系统中 Snort 实例的统计信息。您可以将这些统计信息用于提供信息和调试目的。请咨询思科 TAC 以帮助您使用此命令调试您的系统。使用 **show snort counters action all** 命令查看系统中所有 Snort 实例的操作、限制和判定的 Snort 实例级统计信息。使用 **show snort instances** 命令确定可用的实例编号。

以下示例显示系统中所有 Snort 实例的操作、限制和判定的 Snort 实例级统计信息。

```
> show snort counters action all
Instance : 1
------------

Action Stats are not available
 Total Action Processed:           0

...

================================================================================

Instance : 16
```

```
------------

Action Stats:
     Alerts:            0 (  0.000%)
     Logged:            0 (  0.000%)
     Passed:            0 (  0.000%)
Limits:
      Match:            0
      Queue:            0
        Log:            0
      Event:            0
      Alert:            0
Verdicts:
      Allow:       220009 (100.000%)
      Block:         5076 (  2.307%)
    Replace:            0 (  0.000%)
  Whitelist:            0 (  0.000%)
  Blacklist:            0 (  0.000%)
     Ignore:            0 (  0.000%)
      Retry:            0 (  0.000%)

================================================================================
```

以下示例显示了 Steam 统计信息。

```
> show snort counters stream all
Instance : 1
------------

Stream statistics not available
 Total sessions: 0
================================================================================

...

Instance : 16
------------

Stream statistics:
            Total sessions: 665
              TCP sessions: 665
              UDP sessions: 0
             ICMP sessions: 0
               IP sessions: 0
                TCP Prunes: 0
                UDP Prunes: 0
               ICMP Prunes: 0
                 IP Prunes: 0
TCP StreamTrackers Created: 0
TCP StreamTrackers Deleted: 0
              TCP Timeouts: 661
              TCP Overlaps: 0
       TCP Segments Queued: 0
     TCP Segments Released: 0
       TCP Rebuilt Packets: 0
         TCP Segments Used: 0
              TCP Discards: 0
                  TCP Gaps: 0
      UDP Sessions Created: 0
      UDP Sessions Deleted: 0
```

```
               UDP Timeouts: 0
               UDP Discards: 0
                     Events: 0
            Internal Events: 0
            TCP Port Filter
                   Filtered: 0
                  Inspected: 0
                    Tracked: 910736
            UDP Port Filter
                   Filtered: 0
                  Inspected: 0
                    Tracked: 0

===============================================================================
```

以下示例显示了 Snort 实例 1 的 SMTP 统计信息。

```
> show snort counters smtp instance 1
Instance : 1
------------

SMTP Preprocessor Statistics
  Total sessions                                  : 80
  Max concurrent sessions                         : 1
  Base64 attachments decoded                      : 0
  Total Base64 decoded bytes                      : 0
  Quoted-Printable attachments decoded            : 0
  Total Quoted decoded bytes                      : 0
  UU attachments decoded                          : 0
  Total UU decoded bytes                          : 0
  Non-Encoded MIME attachments extracted          : 0
  Total Non-Encoded MIME bytes extracted          : 0

===============================================================================
```

Related Commands

命令	Description
clear snort statistics	清除 Snort 检测统计信息。
show snort statistics	显示 Snort 检查流量时与各种 Snort 判定匹配的数据包数。
show snort tls-offload	显示与硬件中的检测引擎 (Snort) 加密和解密的数据包相关的统计信息。

show snort instances

要显示可在其他 **show snort** 命令中使用的 Snort 实例编号列表，请使用 **show snort instances** 命令。

show snort instances

Command History

版本	修改
6.3	引入了此命令。

示例

以下示例显示 Snort 实例列表。

```
> show snort instances
Total number of instances available - 2

+----------+---------+
| INSTANCE |   PID   |
+----------+---------+
|    1     |   2787  |
|    2     |   2788  |
+----------+---------+
```

show snort preprocessor-memory-usage

要显示每个 Snort 实例的 Snort 预处理器的内存使用情况统计信息，请使用 **show snort preprocessor-memory-usage** 命令。

show snort preprocessor-memory-usage 实例*_ID* {**all** | **imap** | **pop** | **smtp**}

Syntax Description

实例*_ID*	Snort 实例的 ID 编号。使用 **show snort instances** 命令获取系统上活动的实例 ID 编号的列表。
all	显示所有预处理器的统计信息。
imap	仅显示 IMAP 预处理器的统计信息。
pop	仅显示 POP 预处理器的统计信息。
smtp	仅显示 SMTP 预处理器的统计信息。

Command History

版本	修改
6.3	引入了此命令。

示例

以下示例显示 Snort 实例 1 的 SMTP 预处理器的统计信息。系统将提示您输入管理员密码。

```
> show snort preprocessor-memory-usage 1 smtp

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

Password:

Snort Memory Usage for: Instance-1
----------------------------------


Memory Statistics of SMTP on: Fri Jul 12 09:13:02 2019

SMTP Session Statistics:
       Total Sessions seen: 0
   Max concurrent sessions: 0
   Current Active sessions: 0

   Memory Pool:
        Free Memory:
            SMTP Mime Pool:       17968000 bytes
                 SMTP Pool:              0 bytes
```

```
        Used Memory:
            SMTP Mime Pool:              0 bytes
                 SMTP Pool:              0 bytes
        -------------------       ---------------
        Total Memory:             17968000 bytes

   Heap Memory:
                      Session:              0 bytes
                Configuration:          16784 bytes
                --------------         ------------
                 Total Memory:          16784 bytes
                 No of allocs:             38 times
                  IP sessions:             30 times
-----------------------------------------------------
```

show snort statistics

要在 Snort 检查流量时显示与各种 Snort 判定匹配的数据包数，请使用 **show snort statistics** 命令。

show snort statistics

Command History

版本	修改
6.0.1	引入了此命令。

使用指南

使用此命令可显示访问策略和入侵规则配置的 Snort 检查结果。此命令通常用于调试意外的 Snort 检查行为。统计信息包括以下内容：

- 通过的数据包数 - 从 Lina 发送到 Snort 的数据包数。
- 阻止的数据包数 - 在 Lina 中阻止且未发送到 Snort 的数据包数量。
- 注入的数据包-Snort 创建并添加到流量流的数据包数。例如，如果配置具有重置操作的阻止，Snort 会生成数据包以重置连接。
- 绕过的数据包数（Snort 关闭或 Snort 繁忙）- 如果将系统配置为允许需要 Snort 检测的数据包，而 Snort 无法执行检测，则这些计数器是当 Snort 关闭或太忙而无法处理检测时绕过检测的数据包的数量数据包。

⚠

注意 当流被绕过（未经检查而通过）时，这些繁忙和关闭计数器会增加，直到被绕过的会话结束，即使 Snort 不再繁忙或关闭，也会发生这种情况。例如，如果持续数天的 TCP 连接在 Snort 繁忙或关闭时发送数据包，然后在 Snort 恢复后继续连接，则计数器可能会增加数天。

- 快速转发流-由策略快速转发并因此未检查的流的数量。
- 黑名单流-Snort 在策略配置中丢弃的流数。
- 流开始事件-当数据平面流程快速传输流而不将其发送到 Snort 时，Lina 进程会向 Snort 发送流开始事件。这些事件有助于 Snort 跟踪连接并报告连接事件。
- 流结束事件-当快速路径流结束时，Lina 流程会向 Snort 发送流结束事件。
- 拒绝流事件-当数据平面决定在将流发送到 Snort 之前丢弃流时，Lina 流程会向 Snort 发送拒绝流事件。
- 丢弃前转发到 Snort 的帧数 - 仅适用于 NGIPS 接口。这是转发到 Snort 的待丢弃数据包数。当 Lina 流程因某种原因（TCP 信头长度无效、UDP 长度无效或 IP 长度无效）而决定丢弃帧时，这些帧也会发送到 Snort 进行查看。
- 丢弃的注入数据包-Snort 添加到已丢弃的流量流的数据包数。

示例

以下示例脚本显示了 **show snort statistics** 命令显示的信息：

```
show snort statistics
Packet Counters:
  Passed Packets                                         6
  Blocked Packets                                        321
  Injected Packets                                       284
  Packets bypassed (Snort Down)                          0
  Packets bypassed (Snort Busy)                          0

Flow Counters:
  Fast-Forwarded Flows                                   0
  Blacklisted Flows                                      0

Miscellaneous Counters:
  Start-of-Flow events                                   0
  End-of-Flow events                                     0
  Denied flow events                                     0
  Frames forwarded to Snort before drop                  0
  Inject packets dropped                                 0
```

在下面的示例中，请考虑将访问控制策略配置为阻止并重置所有流量的情况。Lina无法处理重置，因此它将数据包升级到 Snort 以阻止并将重置注入客户端和服务器。

- 通过的数据包 - 显示从 Lina 传递到 Snort 的八个数据包。
- 注入的数据包 - 显示发送到客户端和服务器的两个数据包。
- 列入黑名单的流 - 显示 Snort 要求 Lina 阻止的流。

注释 本例中没有 被阻止的 数据包。

```
> show snort statistics
Packet Counters:
  Passed Packets                                         8
  Blocked Packets                                        0
  Injected Packets                                       2
  Packets bypassed (Snort Down)                          0
  Packets bypassed (Snort Busy)                          0

Flow Counters:
  Fast-Forwarded Flows                                   0
  Blacklisted Flows                                      3

Miscellaneous Counters:
  Start-of-Flow events                                   0
  End-of-Flow events                                     0
  Denied flow events                                     0
  Frames forwarded to Snort before drop                  0
  Inject packets dropped                                 0
```

在下面的示例中，请考虑以下情况：访问控制策略有一个规则与 FTP 端口匹配并具有阻止操作，另一个规则与 HTTP 应用匹配并具有允许操作。

- 通过的数据包 - 显示 60 个 HTTP 数据包，因为 Lina 将允许规则的数据包发送到 Snort。
- 拒绝流事件 - 显示 Lina 使用 FTP 端口匹配处理的两个数据和控制信道数据包。

注释 本例中没有 被阻止的 数据包。

```
> show snort statistics
Packet Counters:
  Passed Packets                                   60
  Blocked Packets                                  0
  Injected Packets                                 0
  Packets bypassed (Snort Down)                    0
  Packets bypassed (Snort Busy)                    0

Flow Counters:
  Fast-Forwarded Flows                             0
  Blacklisted Flows                                0

Miscellaneous Counters:
  Start-of-Flow events                             0
  End-of-Flow events                               0
  Denied flow events                               2
  Frames forwarded to Snort before drop            0
  Inject packets dropped                           0
```

Related Commands

命令	Description
clear snort statistics	清除 Snort 检测统计信息。
configure snort preserve-connection	决定是否在 Snort 流程关闭时保留路由和透明接口上的现有 TCP/UDP 连接。

show snort tls-offload

要在硬件中显示与检测引擎 (Snort) 加密和解密的数据包相关的统计信息，请使用 **show snort tls-offload** 命令。此命令仅在以下支持 SSL 硬件加速的受管设备上可用：

- 采用 威胁防御 的 Firepower 2100
- 采用 威胁防御的 Firepower 4100/9300

  有关 TLS 加密加速Firepower 4100/9300 支持威胁防御 容器实例的信息，请参阅 *FXOS* 配置指南。

所有虚拟设备或除前面所述设备之外的任何硬件上都不支持 TLS 加密加速。

show snort tls-offload [proxy | tracker | description]

Syntax Description

proxy	（可选。）仅显示代理的统计信息。
tracker	（可选。）仅显示跟踪器的统计信息。
description	（可选。）显示代理和跟踪器的计数器说明。

Command History

版本	修改
6.2.3	引入了此命令。

使用指南

使用此命令可显示Snort的代理和跟踪器组件的详细统计信息。您可以将这些统计信息用于提供信息和调试目的。使用 **show snort tls-offload description** 命令查看计数器的说明。请咨询思科 TAC 以帮助您使用此命令调试您的系统。

以下是 **show snort tls-offload** 命令示例：

```
====== Tracker Statistics ======
TOTAL_CONNECTION                 2774
TOTAL_RSA_KEY_EXCHANGE_4K        2774
TOTAL_CIPHER_SUITE_ENCR_AES      2774
TOTAL_CIPHER_SUITE_HASH_SHA1     2774
TOTAL_CKE_PMS_DECRYPTED          2774
TOTAL_RECORD_DECRYPTED           363001
TOTAL_RECORD_ENCRYPTED           363001
TOTAL_CONNECTION_W_DUR (<0.5s)   2771
AVG_CONNECTION_DURATION  (ms)    184
AVG_HANDSHAKE_TIME       (ms)    37
AVG_CKE_PMS_DECRYPT_TIME (us)    21402
AVG_RECORD_DECRYPT_TIME  (us)    619
AVG_RECORD_ENCRYPT_TIME  (us)    477
PEAK_CONNECTION_DURATION (ms)    400
PEAK_HANDSHAKE_TIME      (ms)    62
CONCURRENT_CONNECTION/Peak       3/3
CPS_ATTEMPTED/Peak               7/8
CPS_COMPLETED/Peak               8/8
```

```
CKE_PMS_DECRYPTING_Q/Peak        0/2
SKE_DH_PARAM_SIGNING_Q/Peak      0/0
RECORD_ENCRYPTING_Q/Peak         1/25
RECORD_DECRYPTING_Q/Peak         1/2
======= Proxy Statistics =======
TOTAL_CONNECTION(LW+FP)          15855
TOTAL_CONNECTION_FP              15853
CONNECTION_FP_RECV_FIN           31697
CONNECTION_FP_RECV_RST           27
CONNECTION_LW_RECV_FIN           2
CONCURRENT_CONNECTION_LW/Peak    0/2
CONCURRENT_CONNECTION_FP/Peak    3/7
BYPASS_NOT_ENOUGH_MEM            0
```

Related Commands

命令	Description
clear snort tls-offload	清除统计信息计数器。
debug snort tls-offload	显示所有 Snort 流程的所有类型的错误调试消息。

show software authenticity

要显示软件真实性信息，请使用 **show software authenticity** 命令。

show software authenticity {**development** | **file** *filename* | **keys** | **running**}

Syntax Description

development	显示是否已启用或禁用开发密钥签名映像的加载。
file *filename*	显示与特定映像文件的软件身份验证有关的数字签名信息。
keys	显示有关存储在 SPI 闪存中的开发密钥和释放密钥的信息。
running	显示与当前运行的映像文件的软件身份验证相关的数字签名信息。

Command History

版本	修改
6.1	引入了此命令。

使用指南

文件和运行映像的输出提供以下信息。

- 文件名，是内存中文件的名称。
- 映像类型，是所显示映像的类型。
- 签名者信息指定签名信息，其中包括以下内容：
  - 公用名称，是软件制造商的名称。
  - 组织单位，指示部署软件映像的硬件。
  - 组织名称，是软件映像的所有者。
- 证书序列号，是数字签名的证书序列号。
- 散列算法，指示数字签名验证中使用的散列算法类型。
- 签名算法，标识数字签名验证中使用的签名算法类型。
- 密钥版本，指示用于验证的密钥版本。

示例

以下是 **show software authenticity development** 命令的输出示例：

```
> show software authenticity development
Loading of development images is disabled
```

以下是 **show software authenticity file** 命令的输出示例。在本例中，文件是开发映像。对于当前在设备上运行的映像文件，您会看到相同的 **show software authenticity running** 输出。

```
> show software authenticity file os.img
File Name                     : disk0:/os.img
Image type                    : Development
    Signer Information
        Common Name           : abraxas
        Organization Unit     : NCS_Kenton_ASA
        Organization Name     : CiscoSystems
    Certificate Serial Number : 57F4610F
    Hash Algorithm            : SHA2 512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A
```

以下是 show software authenticity keys 命令的输出示例：

```
> show software authenticity keys
Public Key #1 Information
-------------------------
Key Type              : Release (Primary)
Public Key Algorithm  : 2048-bit RSA
Modulus :
        96:A2:E6:E4:51:4D:4A:B0:F0:EF:DB:41:82:A6:AC:D0:
        FC:11:40:C2:F0:76:10:19:CE:D0:16:7D:26:73:B1:55:
        FE:42:FE:5D:5F:4D:A5:D5:29:7F:91:EC:91:4D:9B:33:
        54:4B:B8:4D:85:E9:11:2D:79:19:AA:C5:E7:2C:22:5E:
        F6:66:27:98:1C:5A:84:5E:25:E7:B9:09:80:C7:CD:F4:
        13:FB:32:6B:25:B5:22:DE:CD:DC:BE:65:D5:6A:99:02:
        95:89:78:8D:1A:39:A3:14:C9:32:EE:02:4C:AB:25:D0:
        38:AD:E4:C9:C6:6B:28:FE:93:C3:0A:FE:90:D4:22:CC:
        FF:99:62:25:57:FB:A7:C6:E4:A5:B2:22:C7:35:91:F8:
        BB:2A:19:42:85:8F:5E:2E:BF:A0:9D:57:94:DF:29:45:
        AA:31:56:6B:7C:C4:5B:54:FE:DE:30:31:B4:FC:4E:0C:
        9D:D8:16:DB:1D:3D:8A:98:6A:BB:C2:34:8B:B4:AA:D1:
        53:66:FF:89:FB:C2:13:12:7D:5B:60:16:CA:D8:17:54:
        7B:41:1D:31:EF:54:DB:49:40:1F:99:FB:18:38:03:EE:
        2D:E8:E1:9F:E6:B2:C3:1C:55:70:F4:F3:B2:E7:4A:5A:
        F5:AA:1D:03:BD:A1:C3:9F:97:80:E6:63:05:27:F2:1F
Exponent              : 65537
Key Version           : A
Public Key #2 Information
-------------------------
Key Type              : Development (Primary)
Public Key Algorithm  : 2048-bit RSA
Modulus :
        E1:61:22:18:6D:0D:A3:D8:C8:54:62:0D:8D:9A:0E:09:
        05:C8:02:5C:B6:51:47:C7:23:AF:1D:1E:AC:8D:9D:0E:
        DD:30:3C:50:26:F6:E8:26:F9:D7:69:D2:1E:DA:4E:24:
        99:D4:A5:A6:13:68:8D:B0:53:39:02:61:64:81:70:94:
        27:A3:31:A5:05:95:63:AF:EA:EB:26:AB:39:8C:31:6A:
        DD:13:22:22:41:A7:3A:FC:19:80:BE:FC:13:2A:C1:39:
        E0:E6:70:1B:DE:4F:69:EB:92:84:34:23:61:AE:46:53:
        C4:68:4E:DE:A3:98:F6:2E:5A:B5:AC:18:05:90:37:80:
        7C:3E:08:E3:03:83:91:30:11:29:E3:12:B0:26:23:AC:
        0A:C0:DE:31:9D:4B:14:D8:A6:78:B8:B5:84:04:EA:C7:
        FB:CF:C1:DD:16:75:82:FC:1B:5C:FF:B7:C0:36:88:E3:
        3E:BE:44:82:65:2F:66:FF:25:1A:FA:2C:B2:03:17:16:
        0D:C8:33:4F:13:C6:62:D8:53:FC:11:1A:9C:3C:10:EE:
        09:32:FE:38:C2:A2:E2:56:E5:ED:93:89:40:46:B9:E4:
        B3:9C:68:76:B0:BF:0D:FD:33:E6:F6:8C:26:D9:FF:F9:
```

```
        DA:B5:D4:86:81:B4:D1:3B:5E:81:1E:20:9F:BE:6E:B7
Exponent              : 65537
Key Version           : A
Public Key #3 Information
--------------------------
Key Type              : Release (Backup)
Public Key Algorithm  : 2048-bit RSA
Modulus :
        96:A2:E6:E4:51:4D:4A:B0:F0:EF:DB:41:82:A6:AC:D0:
        FC:11:40:C2:F0:76:10:19:CE:D0:16:7D:26:73:B1:55:
        FE:42:FE:5D:5F:4D:A5:D5:29:7F:91:EC:91:4D:9B:33:
        54:4B:B8:4D:85:E9:11:2D:79:19:AA:C5:E7:2C:22:5E:
        F6:66:27:98:1C:5A:84:5E:25:E7:B9:09:80:C7:CD:F4:
        13:FB:32:6B:25:B5:22:DE:CD:DC:BE:65:D5:6A:99:02:
        95:89:78:8D:1A:39:A3:14:C9:32:EE:02:4C:AB:25:D0:
        38:AD:E4:C9:C6:6B:28:FE:93:C3:0A:FE:90:D4:22:CC:
        FF:99:62:25:57:FB:A7:C6:E4:A5:B2:22:C7:35:91:F8:
        BB:2A:19:42:85:8F:5E:2E:BF:A0:9D:57:94:DF:29:45:
        AA:31:56:6B:7C:C4:5B:54:FE:DE:30:31:B4:FC:4E:0C:
        9D:D8:16:DB:1D:3D:8A:98:6A:BB:C2:34:8B:B4:AA:D1:
        53:66:FF:89:FB:C2:13:12:7D:5B:60:16:CA:D8:17:54:
        7B:41:1D:31:EF:54:DB:49:40:1F:99:FB:18:38:03:EE:
        2D:E8:E1:9F:E6:B2:C3:1C:55:70:F4:F3:B2:E7:4A:5A:
        F5:AA:1D:03:BD:A1:C3:9F:97:80:E6:63:05:27:F2:1F
Exponent              : 65537
Key Version           : A
Public Key #4 Information
--------------------------
Key Type              : Development (Backup)
Public Key Algorithm  : 2048-bit RSA
Modulus :
        E1:61:22:18:6D:0D:A3:D8:C8:54:62:0D:8D:9A:0E:09:
        05:C8:02:5C:B6:51:47:C7:23:AF:1D:1E:AC:8D:9D:0E:
        DD:30:3C:50:26:F6:E8:26:F9:D7:69:D2:1E:DA:4E:24:
        99:D4:A5:A6:13:68:8D:B0:53:39:02:61:64:81:70:94:
        27:A3:31:A5:05:95:63:AF:EA:EB:26:AB:39:8C:31:6A:
        DD:13:22:22:41:A7:3A:FC:19:80:BE:FC:13:2A:C1:39:
        E0:E6:70:1B:DE:4F:69:EB:92:84:34:23:61:AE:46:53:
        C4:68:4E:DE:A3:98:F6:2E:5A:B5:AC:18:05:90:37:80:
        7C:3E:08:E3:03:83:91:30:11:29:E3:12:B0:26:23:AC:
        0A:C0:DE:31:9D:4B:14:D8:A6:78:B8:B5:84:04:EA:C7:
        FB:CF:C1:DD:16:75:82:FC:1B:5C:FF:B7:C0:36:88:E3:
        3E:BE:44:82:65:2F:66:FF:25:1A:FA:2C:B2:03:17:16:
        0D:C8:33:4F:13:C6:62:D8:53:FC:11:1A:9C:3C:10:EE:
        09:32:FE:38:C2:A2:E2:56:E5:ED:93:89:40:46:B9:E4:
        B3:9C:68:76:B0:BF:0D:FD:33:E6:F6:8C:26:D9:FF:F9:
        DA:B5:D4:86:81:B4:D1:3B:5E:81:1E:20:9F:BE:6E:B7
Exponent              : 65537
Key Version           : A
```

Related Commands

命令	Description
show version	显示软件版本、硬件配置、许可证密钥和相关运行时间数据。

show ssd

要查看 SSD 的状态，请使用 **show ssd** 命令。

注释 仅在 Secure Firewall 3100 上支持此命令。

show ssd

Command History

版本	修改
7.1	引入了此命令。

示例

以下示例显示了有关 SSD 的信息：

```
> show ssd
Local Disk: 1
Name: nvme0n1
Size(MB): 858306
Operability:
operable
Presence:
equipped
Model: Micron_7300_MTFDHBE960TDF
Serial: MSA244302N0
Drive State: online
SED Support:
yes
SED State:
unlocked
SED Auth Status: ok
RAID action: none
```

Related Commands

命令	Description
configure raid	在 RAID 中添加或删除 SSD。
show raid	显示 RAID 状态。

show ssh-access-list

要显示管理接口的 SSH 访问列表设置，请使用 **show ssh-access-list** 命令。

show ssh-access-list

Command History

版本	修改
6.0.1	引入了此命令。

使用指南

使用此命令可显示管理接口的 SSH 访问列表设置。访问列表确定用户可以从哪些 IP 地址尝试与管理 IP 地址建立 SSH 连接。此列表不控制对任何数据接口的 SSH 访问。

示例

以下示例是 **show ssh-access-list** 命令的默认输出。此访问列表允许从任何 IP 地址到管理 IP 地址的 SSH 连接。任何用户都必须提供有效的用户名/密码才能实际完成 SSH 连接。

```
> show ssh-access-list
ACCEPT     tcp  --  anywhere            anywhere            state NEW tcp dpt:ssh
ACCEPT     tcp      anywhere            anywhere            state NEW tcp dpt:ssh
```

Related Commands

命令	Description
configure ssh-access-list	配置管理接口的 SSH 访问列表。

show ssl

要显示有关活动 SSL 会话和可用密码的信息，请使用 **show ssl** 命令。

show ssl ［**cache** | **ciphers** ［*level*］ | **errors** ［**trace**］ | **mib** ［**64**］ | **objects**］

Syntax Description

cache	（可选）显示 SSL 会话缓存统计信息。
ciphers	（可选）显示可用的 SSL 密码。包含 level 关键字以仅查看可用于给定级别的密码，这表示密码强度。以下是按强度递增的可能级别。 • **all** • **low** • **medium**（如果未指定级别，则为默认值） • **fips** • **high**（仅适用于 TLSv1.2）
errors [**trace**]	（可选）显示SSL错误。包括trace关键字，以包括每个错误的跟踪信息。
mib [**64**]	（可选）显示 SSL MIB 统计信息。包括 64 关键字以查看 64 位计数器统计信息。
objects	（可选）显示 SSL 对象统计信息。

Command History

版本	修改
6.1	引入了此命令。

使用指南

此命令显示有关当前 SSLv3 或更高会话的信息，包括启用的密码顺序、禁用了哪些密码、正在使用的 SSL 信任点，以及是否启用证书身份验证。这些设置适用于数据接口上的 SSL 连接，而不是管理接口上的 SSL 连接。

示例

以下是 **show ssl** 命令的输出示例：

```
> show ssl
Accept connections using SSLv3 or greater and negotiate to TLSv1 or greater
Start connections using TLSv1 and negotiate to TLSv1 or greater
SSL DH Group: group2 (1024-bit modulus)
SSL ECDH Group: group19 (256-bit EC)

SSL trust-points:
  Self-signed (RSA 2048 bits RSA-SHA256) certificate available
  Self-signed (EC 256 bits ecdsa-with-SHA256) certificate available
```

```
Certificate authentication is not enabled
```

以下是 **show ssl ciphers** 命令的输出示例。

```
> show ssl ciphers
Current cipher configuration:
default (medium):
  ECDHE-ECDSA-AES256-GCM-SHA384
  ECDHE-RSA-AES256-GCM-SHA384
  DHE-RSA-AES256-GCM-SHA384
  AES256-GCM-SHA384
  ECDHE-ECDSA-AES256-SHA384
  ECDHE-RSA-AES256-SHA384
  DHE-RSA-AES256-SHA256
  AES256-SHA256
  ECDHE-ECDSA-AES128-GCM-SHA256
  ECDHE-RSA-AES128-GCM-SHA256
  DHE-RSA-AES128-GCM-SHA256
  AES128-GCM-SHA256
  ECDHE-ECDSA-AES128-SHA256
  ECDHE-RSA-AES128-SHA256
  DHE-RSA-AES128-SHA256
  AES128-SHA256
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
  DES-CBC3-SHA
tlsv1 (medium):
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
  DES-CBC3-SHA
tlsv1.1 (medium):
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
  DES-CBC3-SHA
tlsv1.2 (medium):
  ECDHE-ECDSA-AES256-GCM-SHA384
  ECDHE-RSA-AES256-GCM-SHA384
  DHE-RSA-AES256-GCM-SHA384
  AES256-GCM-SHA384
  ECDHE-ECDSA-AES256-SHA384
  ECDHE-RSA-AES256-SHA384
  DHE-RSA-AES256-SHA256
  AES256-SHA256
  ECDHE-ECDSA-AES128-GCM-SHA256
  ECDHE-RSA-AES128-GCM-SHA256
  DHE-RSA-AES128-GCM-SHA256
  AES128-GCM-SHA256
  ECDHE-ECDSA-AES128-SHA256
  ECDHE-RSA-AES128-SHA256
  DHE-RSA-AES128-SHA256
  AES128-SHA256
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
  DES-CBC3-SHA
```

```
dtlsv1 (medium):
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
  DES-CBC3-SHA
>
```

show ssl-policy-config

要显示当前应用的 SSL 策略配置有关的信息，包括策略说明、默认日志记录设置、所有已启用的 SSL 规则和规则配置、受信任 CA 证书以及无法解密的流量操作，请使用 **show ssl-policy-config** 命令。

show ssl-policy-config

Command History

版本	修改
6.1	引入了此命令。

使用指南

在 管理中心 中配置 SSL 策略并将其附加到分配给设备的访问控制策略。您可以使用此命令查看有关为通过设备的流量进行 SSL 解密而配置的操作的信息。

示例

以下示例显示未为设备配置 SSL 策略时所显示的内容。

```
> show ssl-policy-config
SSL policy not yet applied.
```

以下示例显示已配置的 SSL 策略。

```
> show ssl-policy-config
===============[ General SSL Policy ]===============

=================[ Default Action ]=================
Default Action            : Do Not Decrypt

======[ Category: admin_category (Built-in) ]=======

=====[ Category: standard_category (Built-in) ]=====

----------[ Block unwanted applications ]-----------
State                     : Enabled
Action                    : Block
Source Zones              : outside_zone
Destination Zones         : dmz_zone
Applications              : HTTP/SSL Tunnel (3860)

=======[ Category: root_category (Built-in) ]=======

============[ Trusted CA Certificates ]=============

Cisco-Trusted-Authorities (group)
                              thawte-Primary-Root-CA
                              UTN-DATACorp-SGC
                              Chambers-of-Commerce-Root-2008
                              Izenpe.com-1
                              A-Trust-Qual-02
                              A-Trust-nQual-03
                              Common-Policy
```

```
                                Starfield-Root-Certificate-Authority-G2
                                GeoTrust-Primary-Certification-Authority
                                Certum-Trusted-Network-CA
                                UTN-USERFirst-Object

C_US-O_VeriSign-Inc.-OU_Class-3-Public-Primary-Certification-Authority-G2-OU_
c-1998-VeriSign-Inc.-For-authorized-use-only-OU_VeriSign-Trust-Network
                                CA-Disig-Root-R1
                                C_US-O_Equifax-OU_Equifax-Secure-Certificate-Authority
                                Thawte-Server-CA-1
                                VeriSign-Class-3-Public-Primary-Certification-Authority-G3
                                COMODO-Certification-Authority
                                VeriSign-Class-3-Public-Primary-Certification-Authority-G5
                                UTN-USERFirst-Client-Authentication-and-Email
                                TC-TrustCenter-Universal-CA-III
                                Cisco-Root-CA-2048
                                Staat-der-Nederlanden-Root-CA-G2

(...Remaining trusted CA certificates removed...)

=============[ Undecryptable Actions ]==============
Unsupported Cipher Suite  : Inherit Default Action
Unknown Cipher Suite      : Inherit Default Action
Compressed Session        : Inherit Default Action
Uncached Session ID       : Inherit Default Action
SSLv2 Session             : Inherit Default Action
Handshake Error           : Inherit Default Action
Decryption Error          : Block
```

Related Commands

命令	Description
show access-policy-config	显示有关当前配置的访问控制策略的信息。

show ssl-protocol

要显示当前为 HTTPS 访问本地设备管理器 () 而配置的 SSL 协议，请使用 设备管理器**show ssl-protocol** 命令。

show ssl-protocol

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用此命令可查看为管理接口配置的 SSL 协议。这些是 HTTPS 连接允许的协议，用于打开本地管理器 设备管理器。这些协议不用于远程管理器。

使用 **configure ssl-protocol** 命令配置这些协议。

示例

以下示例显示使用本地管理器时如何查看当前定义的 SSL 协议。

```
> show ssl-protocol
The supported ssl protocols are TLSv1.1 TLSv1.2
```

Related Commands

命令	Description
configure ssl-protocol	配置用于 HTTPS 访问管理接口的 SSL 协议。

show startup-config

要显示启动配置或在启动配置加载时显示任何错误，请使用 **show startup-config** 命令。

show startup-config ［**errors**］

Syntax Description

errors	（可选）显示当加载启动配置时生成的任何错误。

Command History

版本	修改
6.1	引入了此命令。

使用指南

show startup-config 命令可显示启动系统配置信息。您不能直接配置这些命令。相反，它们由控制设备的管理器配置，例如 管理中心 或 设备管理器。

但是，这是部分配置。它仅显示可使用 ASA 软件配置命令配置的内容，但某些命令可能特定于 threat defense。这些命令移植到 threat defense。因此，您应仅将启动配置中的信息用作故障排除辅助工具。使用设备管理器作为分析设备配置的主要方法。

示例

以下是 **show startup-config** 命令的输出示例：

```
> show startup-config
: Saved

:
: Serial Number: JAD192100RG
: Hardware:   ASA5508, 8192 MB RAM, CPU Atom C2000 series 2000 MHz, 1 CPU (8 cores)
: Written by enable_1 at 20:39:10.749 UTC Tue Jun 28 2016
!
NGFW Version 6.1.0
!
hostname firepower
enable password 8Ry2YjIyt7RRXU24 encrypted
names

(...Output Truncated...)
```

Related Commands

命令	Description
show running-config	显示运行配置。

show summary

要显示有关设备的最常用信息（版本、类型、UUID 等）的摘要，请使用 **show summary** 命令。

show summary

Command History

版本	修改
6.1	引入了此命令。

使用指南

摘要信息包括基本 **show version** 输出以及应用的策略列表和 Snort 版本信息。

示例

以下是显示摘要信息的示例。

```
> show summary
--------[ ftd1.example.com ]---------
Model                     : Cisco ASA5512-X Threat Defense (75) Version 6.1.0 (Build 2007)
UUID                      : 703006f4-8ff6-11e6-bb6e-8f2d5febf243
Rules update version      : 2016-03-28-001-vrt
VDB version               : 271
-----------------------------------------------------

------------------[ policy info ]--------------------
Access Control Policy     : Initial AC Policy
Intrusion Policy          : Balanced Security and Connectivity

-----------------------------------------------------

---------------[ snort version info ]---------------
Snort Version             : 2.9.10 GRE (Build 20)
libpcap Version           : 1.1.1
PCRE Version              : 7.6 2008-01-28
ZLIB Version              : 1.2.8
-----------------------------------------------------
```

show sunrpc-server active

要显示为 Sun RPC 服务打开的针孔，例如 NFS 和 NIS，请使用**show sunrpc-server active** 命令。

show sunrpc-server active

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show sunrpc-server active** 命令的输出示例：

```
> show sunrpc-server active
        LOCAL           FOREIGN                 SERVICE TIMEOUT
        ------------------------------------------------
        192.168.100.2/0 209.165.200.5/32780     100005 00:10:00
```

LOCAL 列中的条目显示内部接口上客户端或服务器的 IP 地址，而 FOREIGN 列中的值则显示外部接口上客户端或服务器的 IP 地址。

Related Commands

命令	Description
clear sunrpc-server active	清除为 Sun RPC 服务（如 NFS 或 NIS）开放的针孔。
show running-config sunrpc-server	显示有关 SunRPC 服务配置的信息。

show switch mac-address-table

要查看交换机 MAC 地址表，请使用 **show switch mac-address-table** 命令。

注释 仅支持 Firepower 1010。

show switch mac-address-table

Command History

版本	修改
6.5	引入了此命令。

使用指南

交换机 MAC 地址表为交换机硬件中的每个 VLAN 内的流量维护 MAC 地址到交换机端口的映射。网桥 MAC 地址表为 VLAN 之间传递的流量维护 MAC 地址到 VLAN 接口的映射。

MAC 地址条目的有效期为 5 分钟。

示例

以下是 **show switch mac-address-table** 命令的输出示例。

```
> show switch mac-address-table
Legend: Age - entry expiration time in seconds
 Mac Address | VLAN | Type | Age | Port
-----------------------------------------------------
 000e.0c4e.2aa4 | 0001 | dynamic | 287 | Et1/1
 0012.d927.fb03 | 0001 | dynamic | 287 | Et1/1
 0013.c4ca.8a8c | 0001 | dynamic | 287 | Et1/1
 00b0.6486.0c14 | 0001 | dynamic | 287 | Et1/1
 00d0.2bff.449f | 0001 | static | - | In0/1
 0100.5e00.000d | 0001 | static multicast | - | In0/1,Et1/1-8
Total Entries: 6
```

下表显示每个字段的说明：

表 *50: show switch mac-address-table* 字段

字段	Description
Mac Address	显示 MAC 地址。
VLAN	显示与 MAC 地址关联的 VLAN。
Type	显示 MAC 地址是动态获知、作为静态组播地址获知还是静态获知的。唯一的静态条目用于内部背板接口。
Age	显示 MAC 地址表中的动态条目的期限。

字段	Description
Port	显示用于通过 MAC 地址访问主机的交换机端口。

Related Commands

命令	Description
show switch vlan	显示 VLAN 和物理 MAC 地址关联。

show switch vlan

要查看 VLAN 和关联的交换机端口，请使用 **show switch vlan** 命令。

注释 仅支持 Firepower 1010。

show switch vlan

Command History

版本	修改
6.5	引入了此命令。

使用指南

此命令仅适用于具有内置交换机的型号。对于其他型号，请使用 **show vlan** 命令。

示例

以下是 **show switch vlan** 命令的输出示例。

```
> show switch vlan

VLAN Name                            Status    Ports
---- --------------------------------- --------- -------------
100  inside                          up        Et1/1, Et1/2
200  outside                         up        Et1/8
300  -                               down      Et1/2, Et1/3
400  backup                          down      Et1/4
```

下表显示每个字段的说明：

表 *51: show switch vlan* 字段

字段	Description
VLAN	显示 VLAN 编号。
Name	显示 VLAN 接口的名称。如果未设置名称，或者没有 VLAN 接口，则显示屏会显示破折号 (-)。
Status	显示状态（up 或 down）以从/向交换机中的 VLAN 接收/发送流量。VLAN 中需要至少一个交换机端口处于 up 状态才能使 VLAN 处于 up 状态。
Ports	显示为每个 VLAN 分配的交换机端口。如果某个交换机端口为多个 VLAN 列出，则该端口是中继端口。上面的输出示例显示 Ethernet 1/2 是承载 VLAN 100 和 VLAN 300 的中继端口。

Related Commands

命令	Description
show switch mac-address-table	显示交换机 MAC 地址表。

show tcpstat

要显示 TCP 协议栈的状态以及在设备上终止的 TCP 连接（用于调试），请使用 **show tcpstat** 命令。

show tcpstat

Command History

版本	修改
6.1	引入了此命令。

使用指南

show tcpstat 命令可用于显示 TCP 堆栈和设备上终止的 TCP 连接的状态。下表介绍了所显示的 TCP 统计信息。

表 ***52: Show tcpstat*** 命令中的 ***TCP*** 统计信息

统计信息	Description
tcb_cnt	TCP 用户数。
proxy_cnt	TCP 代理数。TCP 代理被用户授权使用。
tcp_xmt pkts	TCP 堆栈发送的数据包数。
tcp_rcv good pkts	TCP 堆栈接收的良好数据包数。
tcp_rcv drop pkts	TCP 堆栈丢弃的已接收数据包数。
tcp bad chksum	校验和错误的已接收数据包数。
tcp user hash add	已添加到散列表的 TCP 用户数。
tcp user hash add dup	当尝试添加新用户时发现散列表中已存在 TCP 用户的次数。
tcp user srch hash hit	当搜索时在散列表中找到 TCP 用户的次数。
tcp user srch hash miss	当搜索时在散列表中未找到 TCP 用户的次数。
tcp user hash delete	从散列表中删除 TCP 用户的次数。
tcp user hash delete miss	当尝试删除 TCP 用户时在散列表中找不到该用户的次数。
lip	TCP 用户的本地 IP 地址。
fip	TCP 用户的外部 IP 地址。
lp	TCP 用户的本地端口。
fp	TCP 用户的外部端口。

统计信息	Description
st	TCP 用户的状态（请参阅 RFC 793）。可能值如下： 1 CLOSED 2 LISTEN 3 SYN_SENT 4 SYN_RCVD 5 ESTABLISHED 6 FIN_WAIT_1 7 FIN_WAIT_2 8 CLOSE_WAIT 9 CLOSING 10 LAST_ACK 11 TIME_WAIT
rexqlen	TCP 用户的重新传输队列的长度。
inqlen	TCP 用户的输入队列的长度。
tw_timer	TCP 用户的 time_wait 计时器的值（以毫秒为单位）。
to_timer	TCP 用户的非活动超时计时器的值（以毫秒为单位）。
cl_timer	TCP 用户的关闭请求计时器的值（以毫秒为单位）。
per_timer	TCP 用户的持续计时器的值（以毫秒为单位）。
rt_timer	TCP 用户的重新传输计时器的值（以毫秒为单位）。
tries	TCP 用户的重新传输计数。

示例

以下示例展示如何显示 TCP 堆栈的状态：

```
> show tcpstat
                CURRENT MAX     TOTAL
tcb_cnt         2       12      320
proxy_cnt       0       0       160

tcp_xmt pkts = 540591
tcp_rcv good pkts = 6583
tcp_rcv drop pkts = 2
tcp bad chksum = 0
tcp user hash add = 2028
tcp user hash add dup = 0
tcp user srch hash hit = 316753
tcp user srch hash miss = 6663
tcp user hash delete = 2027
tcp user hash delete miss = 0

lip = 203.0.113.45 fip = 192.0.2.12 lp = 443 fp = 2567 st = 4 rexqlen = 0
in0
```

```
tw_timer = 0 to_timer = 179000 cl_timer = 0 per_timer = 0
rt_timer = 0 tries 0
```

命令	Description
show conn	显示使用的连接和可用的连接。

show tech-support

要显示由技术支持分析师用于诊断的信息，请使用 **show tech-support** 命令。

show tech-support

Command History

版本	修改
6.1	引入了此命令。
7.1	添加了 **show access-list element-count** 和 **show asp rule-engine** 的输出。

使用指南

show tech-support 命令可列出技术支持分析师帮助您诊断问题时所需的信息。

示例

以下示例展示如何显示用于技术支持分析的信息。输出已缩短，仅显示其开头。输出非常长，需要很长时间才能浏览结果。

```
> show tech-support

-------------[ ftd1.example.com ]--------------
Model                     : Cisco ASA5508-X Threat Defense (75) Version 6.1.0 (B
uild 226)
UUID                      : 43235986-2363-11e6-b278-aff0a43948fe
Rules update version      : 2016-03-28-001-vrt
VDB version               : 270
------------------------------------------------

Cisco Adaptive Security Appliance Software Version 9.6(1)72

Compiled on Fri 20-May-16 13:36 PDT by builders
System image file is "disk0:/os.img"
Config file at boot was "startup-config"

firepower up 3 days 16 hours

Hardware:   ASA5508, 8192 MB RAM, CPU Atom C2000 series 2000 MHz, 1 CPU (8 cores
)
Internal ATA Compact Flash, 8192MB
BIOS Flash M25P64 @ 0xfed01000, 16384KB
Encryption hardware device : Cisco ASA Crypto on-board accelerator (revision 0x1
)
(...Remaining output truncated...)
```

show threat-detection memory

要显示由运行配置中的 **threat-detection statistics** 命令启用的高级威胁检测统计信息使用的内存，请使用 **show threat-detection memory** 命令。

show threat-detection memory

Command History

版本	修改
6.3	引入了此命令。

使用指南

某些统计可使用大量内存，并会影响系统性能。此命令可监控内存使用情况，以便您在必要时调整配置。

使用 FlexConfig 配置 **threat-detection statistics** 命令。

示例

以下是 **show threat-detection memory** 命令的输出示例：

```
> show threat-detection memory
Cached chunks:
       CACHE TYPE             BYTES USED
TD Host                         70245888
TD Port                             2724
TD Protocol                         1476
TD ACE                               728
TD Shared counters                 14256
============================
Subtotal TD Chunks              70265072


Regular memory                BYTES USED
TD Port                             33824
TD Control block                   162064
============================
Subtotal Regular Memory            195888


Total TD memory:                70460960
```

命令	Description
show running-config all threat-detection	显示威胁检测配置，包括默认速率设置（如果没有单独配置）。
show threat-detection statistics host	显示主机统计信息。
show threat-detection statistics port	显示端口统计信息。

命令	Description
show threat-detection statistics protocol	显示协议统计信息。
show threat-detection statistics top	显示前 10 个统计信息。

show threat-detection rate

使用 **threat-detection basic-threat** 命令（使用 FlexConfig）启用基本威胁检测时，可以使用 **show threat-detection rate** 命令查看统计信息。

show threat-detection rate ［**min-display-rate** *events_per_second*］［**acl-drop** | **bad-packet-drop** | **conn-limit-drop** | **dos-drop** | **fw-drop** | **icmp-drop** | **inspect-drop** | **interface-drop** | **scanning-threat** | **syn-attack**］

Syntax Description

acl-drop	（可选）显示由于访问列表拒绝而产生丢弃数据包的速率。
bad-packet-drop	（可选）显示由于数据包格式错误（如 invalid-ip-header 或 invalid-tcp-hdr-length）而被拒绝所产生丢弃数据包的速率。
conn-limit-drop	（可选）显示由于超过连接限制（系统范围的资源限制和配置中设置的限制）而产生丢弃数据包的速率。
dos-drop	（可选）显示由于检测到 DoS 攻击（如无效的 SPI，状态防火墙检查失败）而产生丢弃数据包的速率。
fw-drop	（可选）显示由于基本防火墙检查失败而产生丢弃数据包的速率。此选项是包括此命令中所有防火墙相关数据包丢弃的组合速率。它不包括非防火墙相关丢包（例如 interface-drop、inspect-drop 和 scanning-threat）。
icmp-drop	（可选）显示由于检测到可疑 ICMP 数据包而被拒绝所产生丢弃数据包的速率。
inspect-drop	（可选）显示由于数据包导致应用检查失败而产生丢弃数据包的速率限制。
interface-drop	（可选）显示由于接口过载而产生丢弃数据包的速率限制。
min-display-rate *events_per_second*	（可选）将显示限制为超过最小显示速率（以每秒事件数为单位， 0 - 2147483647）的统计信息。
scanning-threat	（可选）显示由于检测到扫描攻击而产生丢弃数据包的速率。此选项监控扫描攻击；例如，第一个 TCP 数据包并非 SYN 数据包，或者 TCP 连接未通过三方握手。例如，完整扫描威胁检测采用此扫描攻击频率信息，通过将主机分类为攻击者并自动避开这些主机，从而根据此信息采取行动。
syn-attack	（可选）显示由于会话不完整（如 TCP SYN 攻击或无返回数据 UDP 会话攻击）而产生丢弃数据包的速率。

Command History

版本	修改
6.3	引入了此命令。

使用指南

显示内容输出显示以下内容：

- 固定时间段内的平均速率（单位：事件数/秒）。
- 上一个完整突发间隔（平均速率间隔的 1/30 或 10 秒，两者中取较大的一个）内的当前突发速率（单位：事件数/秒）。
- 超过速率的次数。
- 固定时间段内的事件总数。

系统会在平均速率间隔内计算30次事件计数，换句话说，系统在每个突发周期的末尾检查速率，总共检查30个完整突发间隔。当前进行的未完成突发间隔不包括在平均速率中。例如，如果平均速率间隔为 10 分钟，则突发间隔为 10 秒。如果上一个突发间隔为 3:00:00 至 3:00:10，并且您在 3:00:15 使用 **show** 命令，则最后 5 秒不会包含在输出中。

此规则的唯一例外是，当计算总事件数时，未完成突发间隔内的事件数已超过最早突发间隔（30 个的第 1 个）内的事件数。在这种情况下，系统会将最后 59 个完整间隔的事件数加上未完成突发间隔中到目前为止的事件数作为总事件数。此例外可让您实时监控事件的大幅增加。

示例

以下是 **show threat-detection rate** 命令的输出示例：

```
> show threat-detection rate

                        Average(eps)    Current(eps) Trigger         Total events
10-min ACL  drop:                  0               0       0                   16
1-hour ACL  drop:                  0               0       0                  112
1-hour SYN attck:                  5               0       2                21438
10-min  Scanning:                  0               0      29                  193
1-hour  Scanning:                106               0      10               384776
1-hour Bad  pkts:                 76               0       2               274690
10-min  Firewall:                  0               0       3                   22
1-hour  Firewall:                 76               0       2               274844
10-min DoS attck:                  0               0       0                    6
1-hour DoS attck:                  0               0       0                   42
10-min Interface:                  0               0       0                  204
1-hour Interface:                 88               0       0               318225
```

Related Commands

命令	Description
clear threat-detection rate	清除基本威胁检测统计信息。
show running-config all threat-detection	显示威胁检测配置，包括默认速率设置（如果没有单独配置）。
show threat-detection statistics	显示威胁检测统计信息。

show threat-detection scanning-threat

如果使用 **threat-detection scanning-threat** 命令启用扫描威胁检测（使用 FlexConfig），则使用 **show threat-detection scanning-threat** 命令查看归类为攻击者和目标的主机。

show threat-detection scanning-threat ［**attacker** | **target**］

Syntax Description

attacker	（可选）显示攻击主机 IP 地址。
target	（可选）显示目标主机 IP 地址。

Command History

版本	修改
6.3	引入了此命令。

示例

以下是 **show threat-detection scanning-threat** 命令的输出示例：

```
> show threat-detection scanning-threat
Latest Target Host & Subnet List:
    192.168.1.0 (l2l)
    192.168.1.249 (l2l)
Latest Attacker Host & Subnet List:
    192.168.10.234 (outside)
    192.168.10.0 (outside)
    192.168.10.2 (outside)
    192.168.10.3 (outside)
    192.168.10.4 (outside)
    192.168.10.5 (outside)
    192.168.10.6 (outside)
    192.168.10.7 (outside)
    192.168.10.8 (outside)
    192.168.10.9 (outside)
```

Related Commands

命令	Description
clear threat-detection scanning-threat	清除扫描威胁攻击者和目标的列表。
show running-config all threat-detection	显示威胁检测配置，包括默认速率设置（如果没有单独配置）。
show threat-detection statistics	显示威胁检测统计信息。
shun	阻止来自指定主机的连接，例如扫描威胁攻击者。

show threat-detection shun

如果使用 **threat-detection scanning-threat** 命令（使用 FlexConfig）启用扫描威胁检测，并自动避开攻击主机，则使用 **show threat-detection shun** 命令查看当前避开的主机。

show threat-detection scanning-host

Command History

版本	修改
6.3	引入了此命令。

使用指南

要释放回避的主机，请使用 **clear threat-detection shun** 命令。

示例

以下是 **show threat-detection shun** 命令的输出示例：

```
> show threat-detection shun
Shunned Host List:
(outside) src-ip=10.0.0.13 255.255.255.255
(inside) src-ip=10.0.0.13 255.255.255.255
```

Related Commands

命令	Description
clear threat-detection shun	清除自动避开的主机列表。
show running-config all threat-detection	显示威胁检测配置，包括默认速率设置（如果没有单独配置）。
show threat-detection scanning-threat	显示扫描威胁攻击者和目标。
show threat-detection statistics	显示威胁检测统计信息。
shun	阻止来自指定主机的连接，例如扫描威胁攻击者。

show threat-detection statistics

如果使用 **threat-detection statistics** 命令（使用 FlexConfig）启用威胁统计信息，请使用 **show threat-detection statistics** 命令查看统计信息。为清楚起见，下图中分别显示了主要关键字和选项。

show threat-detection statistics ［**min-display-rate** *eps*］ **host** ［*ip_address* ［*mask*］］

show threat-detection statistics ［**min-display-rate** *eps*］ **port** ［*start_port*［*-end_port*］］

show threat-detection statistics ［**min-display-rate** *eps*］ **protocol** ［*number* | *name*］

show threat-detection statistics ［**min-display-rate** *EPS*］ **top** ［**access-list** | **host** | **port-protocol**］［**rate-1** | **rate-2** | **rate-3**］ | **tcp-intercept** ［**all**］［**detail**］［**long**］］

Syntax Description

host [*ip_address* [*mask*]]	显示主机统计信息。您可以选择指定 IP 地址以显示特定主机的统计信息。可以包括主机的子网掩码。 通过使用 FlexConfig 配置 **threat-detection statistics host** 命令来启用主机统计信息。
min-display-rate *eps*	（可选）将显示限制为超过最小显示速率（以每秒事件数为单位， 0 - 2147483647）的统计信息。
port [*start_port*[*-end_port*]]	显示 TCP/UDP 端口统计信息。您可以选择指定一个端口或一系列端口，范围介于 0 和 65535 之间。 通过使用 FlexConfig 配置 **threat-detection statistics port** 命令来启用端口统计信息。
protocol [*number* | *name*]	显示协议统计信息。您可以选择按编号或名称指定协议。数字可以是 0 - 255。名称可以是下列项目之一：ah、eigrp、esp、gre、icmp、icmp6、igmp、igrp、ip、ipinip、ipsec、nos、ospf、pcp、pim、pptp、snp、tcp、udp。 通过使用 FlexConfig 配置 **threat-detection statistics protocol** 命令来启用协议统计信息。

top [**access-list** | **host** | **port-protocol**] [**rate-1** | **rate-2** | **rate-3**]	根据启用统计信息的选项，显示前 10 个访问规则、主机和端口/协议。您可以使用以下关键字缩小视图范围： • **access-list** 显示与数据包匹配的前 10 名 ACE，包括允许和拒绝 ACE。如果使用 **threat-detection basic-threat** 命令启用基本威胁检测，则可以使用 **show threat-detection rate access-list** 命令跟踪访问列表拒绝。 • **host** 显示每个固定时间段的前 10 名主机统计信息。由于威胁检测算法的原因，用于故障转移链路或状态链路的接口可能显示为前 10 名主机之一。当将一个接口同时用于故障转移和状态链路时，更有可能出现这种情况。这是预期行为，您可以在显示中忽略此 IP 地址。 • **port-protocol** 显示 TCP/UDP 端口和 IP 协议类型的前 10 名合并统计信息。TCP（协议 6）和 UDP（协议 17）未包含在 IP 协议的显示内容中。 • **rate-1**、 **rate-2**、 **rate-3** 仅显示指定固定速率周期的统计信息，其中 1 表示最小间隔，3 表示最大间隔。例如，如果显示最近 1 小时、8 小时和 24 小时的统计信息，则速率 1 为 1 小时，速率 2 为 8 小时，速率 3 为 24 小时。
top tcp-intercept [**all**] [**detail**] [**long**]	显示 TCP 拦截统计信息。显示内容包含受到攻击的前 10 台受保护服务器。可以包括以下关键字： • **all** 显示所有被跟踪服务器的历史数据。 • **detail** 显示历史采样数据。 • **long** 以长格式显示统计历史记录，其中包含服务器的实际 IP 地址和转换后的 IP 地址。

Command History

版本	修改
6.3	引入了此命令。

使用指南

威胁检测统计信息显示允许和丢弃的流量速率。

显示内容输出显示以下内容：

- 固定时间段内的平均速率（单位：事件数/秒）。
- 上一个完整突发间隔（平均速率间隔的 1/30 或 10 秒，两者中取较大的一个）内的当前突发速率（单位：事件数/秒）。
- 超过速率的次数（仅适用于丢弃流量统计信息）
- 固定时间段内的事件总数。

系统会在平均速率间隔内计算30次事件计数，换句话说，系统在每个突发周期的末尾检查速率，总共检查30个完整突发间隔。当前进行的未完成突发间隔不包括在平均速率中。例如，如果平均速率

间隔为 20 分钟，则突发间隔为 20 秒。如果上一个突发间隔为 3:00:00 至 3:00:20，并且您在 3:00:25 使用 **show** 命令，则最后 5 秒不会包含在输出中。

此规则的唯一例外是，当计算总事件数时，未完成突发间隔内的事件数已超过最早突发间隔（30 个的第 1 个）内的事件数。在这种情况下，系统会将最后 29 个完整间隔的事件数加上未完成突发间隔中到目前为止的事件数作为总事件数。此例外可让您实时监控事件的大幅增加。

下表说明了除 TCP 拦截视图之外的所有命令的输出。有关该输出的说明，请参阅 TCP 拦截示例。

字段	Description
Top Name, ID	对于排名靠前的报告，此列显示访问控制条目的名称或编号、主机的 IP 地址或端口或协议的名称/ID 编号。 条目按固定速率间隔分组，并在时间段内排名，从 [0]（最高计数）到 [9]（最低计数）。对于所有 10 个位置，您可能没有足够的统计信息，因此在给定时间间隔内显示的项目可能少于 10 个。 对于主机和端口协议，按固定间隔发送和接收的字节和数据包进行分组。
Average(eps)	显示每个时间段内的平均速率（单位：事件数/秒）。 系统在每个突发时段结束时，为共计 30 个已完成突发间隔存储计数。当前进行的未完成突发间隔不包括在平均速率中。例如，如果平均速率间隔为 20 分钟，则突发间隔为 20 秒。如果上一个突发间隔为 3:00:00 至 3:00:20，并且您在 3:00:25 使用 show 命令，则最后 5 秒不会包含在输出中。 此规则的唯一例外是，当计算总事件数时，未完成突发间隔内的事件数已超过最早突发间隔（30 个的第 1 个）内的事件数。在这种情况下，系统会将最后 29 个完整间隔的事件数加上未完成突发间隔中到目前为止的事件数作为总事件数。此例外可让您实时监控事件的大幅增加。
Current(eps)	显示上一个完整突发间隔（平均速率间隔的 1/30 或 10 秒，两者中取较大的一个）内的当前突发速率（单位：事件数/秒）对于 Average(eps) 说明中指定的示例，当前速率为 3:19:30 至 3:20:00 的速率
触发器	显示超出丢弃数据包速率限制的次数。对于发送和接收的字节和数据包行中标识的有效流量，此值始终为 0，因为对触发有效流量没有速率限制。
Total events	显示每个速率间隔内的事件总数。当前进行的未完成突发间隔不包括在事件总数中。此规则的唯一例外是，当计算总事件数时，未完成突发间隔内的事件数已超过最早突发间隔（30 个的第 1 个）内的事件数。在这种情况下，系统会将最后 29 个完整间隔的事件数加上未完成突发间隔中到目前为止的事件数作为总事件数。此例外可让您实时监控事件的大幅增加。

字段	Description
条目标题	统计信息按标题下的固定间隔分组。标题可以包括以下各行中解释的信息。通常，条目标题以以下内容开头： • 带有主机 IP 地址的主机。 • 端口号/名称。例如，80/HTTP。 • 协议编号或名称。例如，ICMP。 • 对于排名靠前的报告，为固定间隔和统计信息类型。对于访问列表，标题表示这是针对 ACL 命中的。
tot-ses	显示自主机、端口或协议添加到数据库后的该主机会话总数。
act-ses	显示主机、端口或协议当前参与的活动会话总数。
fw-drop (Host only.)	显示防火墙丢弃数。防火墙丢包是一个组合速率，其中包括在基本威胁检测中跟踪的与防火墙有关的所有丢包，包括访问列表拒绝的数据包、错误数据包、超出连接限制的数据包、DoS 攻击数据包、可疑 ICMP 数据包、TCP SYN 攻击数据包以及无返回数据 UDP 会话攻击数据包。它不包括非防火墙相关丢弃，如接口过载、使应用检查失败的数据包以及检测到的扫描攻击。
insp-drop (Host only.)	显示因为数据包未通过应用检查而被丢弃的数据包的数量。
null-ses (Host only.)	显示空会话数量，空会话是指在 30 秒超时内未完成的 TCP SYN 会话，以及在会话开始后 3 秒内没有其服务器发送的任何数据的 UDP 会话。
bad-acc (Host only.)	显示对处于关闭状态的主机端口的不良访问尝试次数。当确定某个端口处于空会话时（请参阅上文），该主机的端口状态设置为 HOST_PORT_CLOSE。任何访问该主机端口的客户端都会被立即分类为错误访问，无需等待超时。
20-min, 1-hour, 8-hour, and 24-hour	显示这些固定速率间隔的统计信息。 • Sent byte, sent pkts - 显示从主机、端口或协议成功发送的字节数或数据包数。 • Sent drop - 显示已从主机、端口或协议发送但因为是扫描攻击的一部分而被丢弃的数据包数。 • Recv byte, pkts - 显示主机、端口或协议成功接收的字节数或数据包数。 • Sent drop - 显示已从主机、端口或协议发送但因为是扫描攻击的一部分而被丢弃的数据包数。

示例

以下是 **show threat-detection statistics host** 命令的输出示例：

```
> show threat-detection statistics host

                          Average(eps)    Current(eps) Trigger         Total events
Host:10.0.0.1: tot-ses:289235 act-ses:22571 fw-drop:0 insp-drop:0 null-ses:21438 bad-acc:0
  1-hour Sent byte:               2938               0       0             10580308
  8-hour Sent byte:                367               0       0             10580308
 24-hour Sent byte:                122               0       0             10580308
  1-hour Sent pkts:                 28               0       0               104043
  8-hour Sent pkts:                  3               0       0               104043
 24-hour Sent pkts:                  1               0       0               104043
  20-min Sent drop:                  9               0       1                10851
  1-hour Sent drop:                  3               0       1                10851
  1-hour Recv byte:               2697               0       0              9712670
  8-hour Recv byte:                337               0       0              9712670
 24-hour Recv byte:                112               0       0              9712670
  1-hour Recv pkts:                 29               0       0               104846
  8-hour Recv pkts:                  3               0       0               104846
 24-hour Recv pkts:                  1               0       0               104846
  20-min Recv drop:                 42               0       3                50567
  1-hour Recv drop:                 14               0       1                50567
Host:10.0.0.0: tot-ses:1 act-ses:0 fw-drop:0 insp-drop:0 null-ses:0 bad-acc:0
  1-hour Sent byte:                  0               0       0                  614
  8-hour Sent byte:                  0               0       0                  614
 24-hour Sent byte:                  0               0       0                  614
  1-hour Sent pkts:                  0               0       0                    6
  8-hour Sent pkts:                  0               0       0                    6
 24-hour Sent pkts:                  0               0       0                    6
  20-min Sent drop:                  0               0       0                    4
  1-hour Sent drop:                  0               0       0                    4
  1-hour Recv byte:                  0               0       0                  706
  8-hour Recv byte:                  0               0       0                  706
 24-hour Recv byte:                  0               0       0                  706
  1-hour Recv pkts:                  0               0       0                    7
```

以下是 **show threat-detection statistics port** 命令的输出示例：

```
> show threat-detection statistics port

                          Average(eps)    Current(eps) Trigger         Total events
80/HTTP: tot-ses:310971 act-ses:22571
  1-hour Sent byte:               2939               0       0             10580922
  8-hour Sent byte:                367           22043       0             10580922
 24-hour Sent byte:                122            7347       0             10580922
  1-hour Sent pkts:                 28               0       0               104049
  8-hour Sent pkts:                  3             216       0               104049
 24-hour Sent pkts:                  1              72       0               104049
  20-min Sent drop:                  9               0       2                10855
  1-hour Sent drop:                  3               0       2                10855
  1-hour Recv byte:               2698               0       0              9713376
  8-hour Recv byte:                337           20236       0              9713376
 24-hour Recv byte:                112            6745       0              9713376
  1-hour Recv pkts:                 29               0       0               104853
  8-hour Recv pkts:                  3             218       0               104853
 24-hour Recv pkts:                  1              72       0               104853
  20-min Recv drop:                 24               0       2                29134
  1-hour Recv drop:                  8               0       2                29134
```

以下是 **show threat-detection statistics protocol** 命令的输出示例：

```
> show threat-detection statistics protocol

                          Average(eps)    Current(eps) Trigger         Total events
ICMP: tot-ses:0 act-ses:0
  1-hour Sent byte:                  0               0       0                 1000
  8-hour Sent byte:                  0               2       0                 1000
 24-hour Sent byte:                  0               0       0                 1000
  1-hour Sent pkts:                  0               0       0                   10
  8-hour Sent pkts:                  0               0       0                   10
 24-hour Sent pkts:                  0               0       0                   10
```

以下是 **show threat-detection statistics top access-list** 命令的输出示例：

```
> show threat-detection statistics top access-list

                   Top    Average(eps)    Current(eps) Trigger         Total events
  1-hour ACL hits:
              100/3[0]             173               0       0               623488
              200/2[1]              43               0       0               156786
              100/1[2]              43               0       0               156786
  8-hour ACL hits:
              100/3[0]              21            1298       0               623488
              200/2[1]               5             326       0               156786
              100/1[2]               5             326       0               156786
```

以下是 **show threat-detection statistics top port-protocol** 命令的输出示例：

```
> show threat-detection statistics top port-protocol

Top          Name   Id    Average(eps)    Current(eps) Trigger      Total events
  1-hour Recv byte:
 1         gopher   70              71               0       0          32345678
 2  btp-clnt/dhcp   68              68               0       0          27345678
 3         gopher   69              65               0       0          24345678
 4    Protocol-96 * 96              63               0       0          22345678
 5      Port-7314 7314              62               0       0          12845678
 6 BitTorrent/trc 6969              61               0       0          12645678
 7     Port-8191-65535              55               0       0          12345678
 8           SMTP  366              34               0       0           3345678
 9         IPinIP *  4              30               0       0           2345678
10          EIGRP * 88              23               0       0           1345678
  1-hour Recv pkts:
...
...
  8-hour Recv byte:
...
...
  8-hour Recv pkts:
...
...
 24-hour Recv byte:
...
...
 24-hour Recv pkts:
...
...

Note: Id preceded by * denotes the Id is an IP protocol type
```

以下是 **show threat-detection statistics top host** 命令的输出示例：

```
> show threat-detection statistics top host

                    Top    Average(eps)    Current(eps) Trigger         Total events
  1-hour Sent byte:
          10.0.0.1[0]            2938               0       0             10580308
  1-hour Sent pkts:
          10.0.0.1[0]              28               0       0               104043
  20-min Sent drop:
          10.0.0.1[0]               9               0       1                10851
  1-hour Recv byte:
          10.0.0.1[0]            2697               0       0              9712670
  1-hour Recv pkts:
          10.0.0.1[0]              29               0       0               104846
  20-min Recv drop:
          10.0.0.1[0]              42               0       3                50567
  8-hour Sent byte:
          10.0.0.1[0]             367               0       0             10580308
  8-hour Sent pkts:
          10.0.0.1[0]               3               0       0               104043
  1-hour Sent drop:
          10.0.0.1[0]               3               0       1                10851
  8-hour Recv byte:
          10.0.0.1[0]             337               0       0              9712670
  8-hour Recv pkts:
          10.0.0.1[0]               3               0       0               104846
  1-hour Recv drop:
          10.0.0.1[0]              14               0       1                50567
 24-hour Sent byte:
          10.0.0.1[0]             122               0       0             10580308
 24-hour Sent pkts:
          10.0.0.1[0]               1               0       0               104043
 24-hour Recv byte:
          10.0.0.1[0]             112               0       0              9712670
 24-hour Recv pkts:
          10.0.0.1[0]               1               0       0               104846
```

以下是 **show threat-detection statistics top tcp-intercept** 命令的输出示例：

```
> show threat-detection statistics top tcp-intercept

Top 10 protected servers under attack (sorted by average rate)
Monitoring window size: 30 mins    Sampling interval: 30 secs
<Rank> <Server IP:Port> <Interface> <Ave Rate> <Cur Rate> <Total> <Source IP (Last Attack
Time)>
------------------------------------------------------------------------------------
1    192.168.1.2:5000 inside 1249 9503 2249245 <various> Last: 10.0.0.3 (0 secs ago)
2    192.168.1.3:5000 inside 10 10 6080 10.0.0.200 (0 secs ago)
3    192.168.1.4:5000 inside 2 6 560 10.0.0.200 (59 secs ago)
4    192.168.1.5:5000 inside 1 5 560 10.0.0.200 (59 secs ago)
5    192.168.1.6:5000 inside 1 4 560 10.0.0.200 (59 secs ago)
6    192.168.1.7:5000 inside 0 3 560 10.0.0.200 (59 secs ago)
7    192.168.1.8:5000 inside 0 2 560 10.0.0.200 (59 secs ago)
8    192.168.1.9:5000 inside 0 1 560 10.0.0.200 (59 secs ago)
9    192.168.1.10:5000 inside 0 0 550 10.0.0.200 (2 mins ago)
10   192.168.1.11:5000 inside 0 0 550 10.0.0.200 (5 mins ago)
```

下表对 TCP 截取输出进行了解释。

字段	Description
Monitoring window size	显示系统采样统计信息的时间段。默认值为 30 分钟。您可以使用 FlexConfig 的 **threat-detection statistics tcp-intercept rate-interval** 命令更改此设置。系统在此间隔内采样 30 次数据。
Sampling interval	显示采样的间隔。此值始终为速率间隔除以 30。
Rank	显示排名 1 到 10，其中 1 是最受攻击的服务器，10 是最不受攻击的服务器。
Server IP:Port	显示正受到攻击的服务器 IP 地址和端口。
Interface	显示服务器受到攻击的接口。
Ave Rate	显示采样期间内的平均攻击速率（以攻击数/秒为单位）。
Cur Rate	显示当前攻击速率（以攻击数/秒为单位）。
Total	显示攻击总数。
Source IP	显示攻击者 IP 地址。
Last Attack Time	显示上一次攻击发生的时间。

以下是 **show threat-detection statistics top tcp-intercept long** 命令的输出示例，括号中为实际服务器 IP 地址：

```
> show threat-detection statistics top tcp-intercept long

Top 10 protected servers under attack (sorted by average rate)
Monitoring window size: 30 mins    Sampling interval: 30 secs
<Rank> <Server IP:Port (Real IP:Real Port)> <Interface> <Ave Rate> <Cur Rate> <Total> <Source
 IP (Last Attack Time)>
--------------------------------------------------------------------------------
1    10.1.0.2:6025 (209.165.200.227:6025) inside 18 709 33911 10.0.0.201 (0 secs ago)
2    10.1.0.2:6026 (209.165.200.227:6026) inside 18 709 33911 10.0.0.201 (0 secs ago)
3    10.1.0.2:6027 (209.165.200.227:6027) inside 18 709 33911 10.0.0.201 (0 secs ago)
4    10.1.0.2:6028 (209.165.200.227:6028) inside 18 709 33911 10.0.0.201 (0 secs ago)
5    10.1.0.2:6029 (209.165.200.227:6029) inside 18 709 33911 10.0.0.201 (0 secs ago)
6    10.1.0.2:6030 (209.165.200.227:6030) inside 18 709 33911 10.0.0.201 (0 secs ago)
7    10.1.0.2:6031 (209.165.200.227:6031) inside 18 709 33911 10.0.0.201 (0 secs ago)
8    10.1.0.2:6032 (209.165.200.227:6032) inside 18 709 33911 10.0.0.201 (0 secs ago)
9    10.1.0.2:6033 (209.165.200.227:6033) inside 18 709 33911 10.0.0.201 (0 secs ago)
10   10.1.0.2:6034 (209.165.200.227:6034) inside 18 709 33911 10.0.0.201 (0 secs ago)
```

以下显示 **show threat-detection statistics top tcp-intercept detail** 命令的输出示例，这显示采样数据。采样数据显示 30 个采样周期中每个周期的攻击次数。

```
> show threat-detection statistics top tcp-intercept detail

Top 10 Protected Servers under Attack (sorted by average rate)
Monitoring Window Size: 30 mins    Sampling Interval: 30 secs
<Rank> <Server IP:Port> <Interface> <Ave Rate> <Cur Rate> <Total> <Source IP (Last Attack
Time)>
```

```
--------------------------------------------------------------------------------
1     192.168.1.2:5000 inside 1877 9502 3379276 <various> Last: 10.0.0.45 (0 secs ago)
      Sampling History (30 Samplings):
              95348       95337       95341       95339       95338       95342
              95337       95348       95342       95338       95339       95340
              95339       95337       95342       95348       95338       95342
              95337       95339       95340       95339       95347       95343
              95337       95338       95342       95338       95337       95342
              95348       95338       95342       95338       95337       95343
              95337       95349       95341       95338       95337       95342
              95338       95339       95338       95350       95339       95570
              96351       96351       96119       95337       95349       95341
              95338       95337       95342       95338       95338       95342
......
```

Related Commands

命令	Description
clear threat-detection statistics	清除威胁检测统计信息。
show running-config all threat-detection	显示威胁检测配置，包括默认速率设置（如果没有单独配置）。

show time

要显示设备的 UTC 和本地时间和日期，请使用 **show time** 命令。

show time

Command History

版本	修改
6.0.1	引入了此命令。

示例

以下是 **show time** 命令的输出示例。

```
> show time
UTC -       Wed Aug  3 17:04:06 UTC 2016
Localtime - Wed Aug 03 13:04:06 EDT 2016
```

show time-range

要显示所有时间范围对象的配置，请使用 **show time-range** 命令。

注释 此命令不显示设备时间。要查看设备时间，请使用 显示时间。

show time-range timezone ［ 名称 ］

Syntax Description

name	（可选）仅显示此时间范围对象的信息。
timezone	要查看为时间范围策略配置的时区，请使用时区。

Command History

版本	修改
6.3	引入了此命令。
6.6	添加了时区关键字。

示例

此示例显示如何显示时间范围对象的配置。在本示例中，有一个名为 work-hours 的对象。非活动意味着对象未被使用。

```
> show time-range

time-range entry: work-hours (inactive)
   periodic weekdays 9:00 to 17:00
```

以下是 **show time-range timezone** 命令的输出示例：

```
> show time-range timezone
Time-range Clock:
------------------------------
13:20:22.852 tzname Tue Aug 18 2020
```

show tls-proxy

要显示加密检测的 TLS 代理和会话信息，请使用 **show tls-proxy** 命令。

show tls-proxy [*tls_name* | **session** [**host** *host_address* | **detail** [**cert-dump**] | **count** | **statistics**]]

Syntax Description

count	仅显示会话计数器。
detail [**cert-dump**]	显示详细 TLS 代理信息，包括每个 SSL 段和 LDC 的密码。添加 **cert-dump** 关键字以获取本地动态证书 (LDC) 的十六进制转储。 您还可以将这些关键字与 **host** 选项配合使用。
host *host_address*	指定特定主机的 IPv4 或 IPv6 地址，以显示关联的会话。
session	显示活动 TLS 代理会话。
statistics	显示监控和管理 TLS 会话的统计信息。
tls_name	要显示的 TLS 代理的名称。

Command History

版本	修改
6.3	引入了此命令。

使用指南

您可以使用此命令查看的 TLS 代理是仅为加密应用检测配置的代理。它们适用于 SIP、SCCP (Skinny) 或 Diameter 检测。这些 TLS 代理与 SSL 解密或 VPN 策略无关。

示例

以下是 **show tls-proxy** 命令的输出示例：

```
> show tls-proxy
TLS-Proxy 'proxy': ref_cnt 1, seq#1
      Server proxy:
            Trust-point: local_ccm
      Client proxy:
            Local dynamic certificate issuer: ldc_signer
            Local dynamic certificate key-pair: phone_common
            Cipher-suite <unconfigured>
      Run-time proxies:
            Proxy 0x448b468: Class-map: skinny_ssl, Inspect: skinny
                  Active sess 1, most sess 4, byte 3244
```

以下是 **show tls-proxy session** 命令的输出示例：

```
> show tls-proxy session
outside 133.9.0.211:51291 inside 195.168.2.200:2443 P:0x4491a60(proxy)
S:0x482e790 byte 3388
```

以下是 **show tls-proxy session detail** 命令的输出示例：

```
> show tls-proxy session detail
1 in use, 1 most used
outside 133.9.0.211:50433 inside 195.168.2.200:2443 P:0xcba60b60(proxy) S:0xcbc10748 byte
1831704
      Client: State SSLOK  Cipher AES128-SHA Ch 0xca55efc8 TxQSize 0 LastTxLeft 0 Flags 0x1

      Server: State SSLOK  Cipher AES128-SHA Ch 0xca55efa8 TxQSize 0 LastTxLeft 0 Flags 0x9
Local Dynamic Certificate
      Status: Available
      Certificate Serial Number: 29
      Certificate Usage: General Purpose
      Public Key Type: RSA (1024 bits)
      Issuer Name:
             cn=TLS-Proxy-Signer
      Subject Name:
             cn=SEP0002B9EB0AAD
             o=Cisco Systems Inc
             c=US
      Validity Date:
            start date: 00:47:12 PDT Feb 27 2007
            end   date: 00:47:12 PDT Feb 27 2008
      Associated Trustpoints:
```

以下是 **show tls-proxy session statistics** 命令的输出示例：

```
> show tls-proxy session stastics
TLS Proxy Sessions (Established: 600)
    Mobility:                                      0
Per-Session Licensed TLS Proxy Sessions
(Established: 222, License Limit: 3000)
    SIP:                                           2
    SCCP:                                         20
    DIAMETER:                                    200
Total TLS Proxy Sessions
    Established:                                 822
    Platform Limit:                             1000
```

show track

要显示有关安全级别协议 (SLA) 跟踪流程跟踪的对象的信息，请使用 **show track** 命令。

show track ［*track-id*］

Syntax Description

track-id	跟踪条目对象 ID 编号，范围为 1 到 500。

Command History

版本	修改
6.3	引入了此命令。

示例

以下是 **show track** 命令的输出示例：

```
> show track

Track 5
      Response Time Reporter 124 reachability
      Reachability is UP
      2 changes, last change 03:41:16
      Latest operation return code: OK
      Tracked by:
                 STATIC-IP-ROUTING 0
```

show traffic

要显示接口传输和接收活动，请使用 **show traffic** 命令。

show traffic

Command History

版本	修改
6.1	引入了此命令。

使用指南

show traffic 命令列出了自上次输入 **show traffic** 命令以来或设备上线以来通过每个接口的数据包和字节数。秒数是设备自上次重启以来的在线持续时间，除非自上次重启以来输入过 **clear traffic** 命令。如果是这种情况，则秒数是自输入命令以来的持续时间。

统计信息首先根据接口名称显示。在指定接口之后，将根据物理接口显示统计信息。接口可以包括系统用于内部通信的隐藏虚拟接口。

示例

以下是 **show traffic** 命令的简短输出示例，显示单个接口的统计信息。每个接口显示相同的统计信息。

```
> show traffic
...
diagnostic:
        received (in 102.080 secs):
                2048 packets     204295 bytes
                20 pkts/sec      2001 bytes/sec
        transmitted (in 102.080 secs):
                2048 packets       204056 bytes
                20 pkts/sec      1998 bytes/sec
      1 minute input rate 122880 pkts/sec,  5775360 bytes/sec
      1 minute output rate 122887 pkts/sec,  5775389 bytes/sec
      1 minute drop rate, 3 pkts/sec
      5 minute input rate 118347 pkts/sec,  5562309 bytes/sec
      5 minute output rate 119221 pkts/sec,  5603387 bytes/sec
      5 minute drop rate, 11 pkts/sec
...
```

Related Commands

命令	Description
clear traffic	重置用于发送和接收活动的计数器。

show upgrade

要显示有关系统软件升级的信息，请使用 **show upgrade** 命令。

show upgrade { **revert-info** | **status** [**detail**] [**continuous**] }

Syntax Description

revert-info	显示您可以恢复使用的系统版本（如果有任何版本可用于恢复）。如果没有可用的恢复版本，则无法使用 **upgrade revert** 命令。
status	显示升级的状态。可以包含以下可选关键字： • **detail** 除摘要状态信息外，还显示升级日志。 • **continuous** 显示生成的升级消息。您可以单独使用此关键字，也可以将其与detail关键字结合使用。

Command History

版本	修改
6.7	引入了此命令。

使用指南

可能的状态包括：

- 未在进行升级。
- 正在进行主要升级。
- 正在进行补丁升级。
- 正在进行修复程序。
- 主要升级失败。运行 “cancel” 进行恢复。

  重新启动可能会发生，也可能不会发生，具体取决于升级失败阶段。
- 主要升级失败。重新启动设备以进行恢复。

示例

以下示例显示当前正在进行的升级的状态。要查看已完成升级的状态，请使用 **show last-upgrade status** 命令。

```
> show upgrade status
Upgrade from 6.3.0 to 6.7.0 in progress (11% progress, time remaining 8 mins)
Time started: Tue Dec  3 23:50:31 UTC 2020
Current state: Tue Dec  3 23:51:01 UTC 2020 Running script 200_pre/001_check_reg.pl...
```

以下示例显示恢复信息。在本示例中，确实存在您可以恢复的版本。如果没有可用的版本，则消息为“没有可用于恢复的版本”。

```
> show upgrade revert-info
You can revert to version 6.4.0-102
at 2020-03-20T22:49:43+0000

It uses 4946MB of disk space.

Version 6.4.0-102 is available for revert.
```

Related Commands

命令	Description
show last-upgrade status	显示有关上次系统软件升级的信息。
upgrade	取消、恢复或重试系统软件升级。

show user

要显示用于访问设备上的命令行接口 (CLI) 的用户账号，请使用 **show user** 命令。

show user ［*username1* ［*usernam2*］［...］］

Syntax Description

username1 [*usernam2*] [...]	（可选。）一个或多个空格分隔的用户名。如果不指定任何名称，则会显示所有用户。

Command History

版本	修改
6.1	引入了此命令。

使用指南

系统将为每个用户显示以下信息。使用 **configure user add** 命令创建用户账号。

- Login - 登录名。
- UID - 数字用户 ID。
- Auth - 如何对用户进行身份验证，本地或远程（通过目录服务器）。
- Access — 用户的权限级别，基础或配置。使用 **configure user access** 命令更改其设置。
- 已启用 - 用户是否处于活动状态，已启用或已禁用。使用 **configure user enable**/**disable** 命令更改此设置。
- Reset - 用户下次登录时是否必须更改账户密码，是或否。使用 **configure user forcereset** 命令更改此设置。
- Exp- 还剩下多少天必须更改用户密码。从不表示密码不会过期。使用 **configure user aging** 命令更改其设置。
- Warn - 在密码到期前警告用户更改密码的天数。N/A 表示警告不适用。使用 **configure user aging** 命令更改其设置。
- 宽限期 - 宽限期，即密码到期后用户可以更改的天数。禁用意味着没有宽限期。宽限期仅适用于运行 FXOS 的设备。使用 **configure user aging** 命令更改其设置。
- Str - 用户密码是否必须符合强度检查标准，Dis (禁用) 或 Ena (启用)。使用 **configure user strengthcheck** 命令配置此选项。
- Lock - 用户账户是否因登录失败太多次而被锁定，是或否。使用 **configure user unlock** 命令以解锁用户账号。
- Max - 用户账户被锁定前允许的最多登录失败次数。N/A 表示永远无法锁定账户。使用 configure user maxfailedlogins 命令更改此设置。

示例

以下示例显示如何显示为 CLI 访问定义的用户。

```
> show user
Login              UID   Auth Access  Enabled Reset    Exp Warn  Str Lock Max
admin             1000  Local Config  Enabled    No  Never  N/A  Dis   No N/A
admin2            1001  Local Config  Enabled    No  Never  N/A  Dis   No   5
```

以下示例包括外部用户和宽限期。

```
> show user
Login          UID   Auth Access  Enabled Reset   Exp   Warn    Grace  MinL Str Lock Max
admin          100  Local Config  Enabled    No  10000     7  Disabled    8 Ena   No N/A
extuser        501 Remote Config Disabled   N/A  99999     7  Disabled    1 Dis   No N/A
joeuser       1000  Local Config  Enabled   Yes    180     7         7    8 Dis   No   5
```

Related Commands

命令	Description
configure user add	添加用于 CLI 访问的用户账号。

show version

要显示硬件型号、软件版本、UUID、入侵规则更新版本和 VDB 版本，请使用 **show version** 命令。

show version ［**detail** | **system**］

Syntax Description

detail	**show version** 和 **show version detail** 显示相同的信息。
system	此关键字将其他系统信息附加到 **show version**显示的信息。

Command History

版本	修改
6.1	引入了此命令。
7.1	有关启动（引导）系统所需时间的信息已添加到输出中。

使用指南

show version 命令和 **show version detail** 命令显示相同的基本系统信息。 **show version system** 命令显示此信息以及其他系统信息，例如自上次重新启动以来的运行时间和更具体的硬件信息。

示例

以下示例显示了 **show version** 的基础输出：

```
> show version
-------------------[ firepower ]--------------------
Model : Secure Firewall Management Center for VMware (66) Version 7.2.0 (Build 1405)
UUID : 78ddf634-3754-11ec-87dd-ace5f9ec4cdc
Rules update version : 2022-01-11-001-vrt
LSP version : lsp-rel-20220111-1030
VDB version : 348
----------------------------------------------------
```

show version system 命令的以下示例输出附加了与 **show version** 命令相同的输出以及其他信息。

```
> show version system
-------------[ example-sfr.example.com ]--------------
Model                     : Cisco ASA5508-X Threat Defense (75) Version 6.1.0 (Build 226)
UUID                      : 43235986-2363-11e6-b278-aff0a43948fe
Rules update version      : 2016-03-28-001-vrt
VDB version               : 270
----------------------------------------------------

Cisco Adaptive Security Appliance Software Version 9.6(1)72

Compiled on Fri 20-May-16 13:36 PDT by builders
System image file is "disk0:/os.img"
Config file at boot was "startup-config"

firepower up 36 days 21 hours
```

```
Hardware:   ASA5508, 8192 MB RAM, CPU Atom C2000 series 2000 MHz, 1 CPU (8 cores
)
Internal ATA Compact Flash, 8192MB
BIOS Flash M25P64 @ 0xfed01000, 16384KB

Encryption hardware device : Cisco ASA Crypto on-board accelerator (revision 0x1
)
                             Number of accelerators: 1

 1: Ext: GigabitEthernet1/1  : address is e865.49b8.97f2, irq 255
 2: Ext: GigabitEthernet1/2  : address is e865.49b8.97f3, irq 255
 3: Ext: GigabitEthernet1/3  : address is e865.49b8.97f4, irq 255
 4: Ext: GigabitEthernet1/4  : address is e865.49b8.97f5, irq 255
 5: Ext: GigabitEthernet1/5  : address is e865.49b8.97f6, irq 255
 6: Ext: GigabitEthernet1/6  : address is e865.49b8.97f7, irq 255
 7: Ext: GigabitEthernet1/7  : address is e865.49b8.97f8, irq 255
 8: Ext: GigabitEthernet1/8  : address is e865.49b8.97f9, irq 255
 9: Int: Internal-Data1/1    : address is e865.49b8.97f1, irq 255
10: Int: Internal-Data1/2    : address is 0000.0001.0002, irq 0
11: Int: Internal-Control1/1 : address is 0000.0001.0001, irq 0
12: Int: Internal-Data1/3    : address is 0000.0001.0003, irq 0
13: Ext: Management1/1       : address is e865.49b8.97f1, irq 0
14: Int: Internal-Data1/4    : address is 0000.0100.0001, irq 0

Serial Number: JAD192100RG
Configuration register is 0x1
Image type              : Release
Key Version             : A
Configuration last modified by enable_1 at 12:44:37.849 UTC Mon Jul 25 2016
```

从版本 7.1 开始，您可以看到启动系统所需的时间。该信息位于系统运行时间的状态之后。

```
> show version system
----------------------[ ftdv1 ]-----------------------
Model                     : Cisco Firepower Threat Defense for VMware (75) Version 7.1.0
(Build 1519)
UUID                      : b964ed5e-92c0-11eb-aaa2-cfab359c2436
LSP version               : lsp-rel-20210310-2255
VDB version               : 338
------------------------------------------------------

Cisco Adaptive Security Appliance Software Version 99.17(1)135
SSP Operating System Version 82.11(1.277i)

Compiled on Thu 25-Mar-21 00:49 GMT by builders
System image file is "boot:/asa99171-135-smp-k8.bin"
Config file at boot was "startup-config"

ftdv1 up 6 days 22 hours
Start-up time 5 secs

(remaining output redacted)
```

show vlan

要显示 threat defense 设备上配置的所有 VLAN，请使用 **show vlan** 命令。

show vlan ［**mapping** ［*primary_id*］］

Syntax Description

mapping	（可选）显示映射到主 VLAN 的辅助 VLAN。
primary_id	（可选）显示特定主 VLAN 的辅助 VLAN。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例展示已配置的 VLAN：

```
> show vlan
10-11,30,40,300
```

以下示例显示映射到每个主 VLAN 的辅助 VLAN：

```
> show vlan mapping
Interface                       Secondary VLAN ID                   Mapped VLAN ID
0/1.100                         200                                            300
0/1.100                         201                                            300
0/2.500                         400                                            200
```

Related Commands

命令	Description
clear interface	清除 **show interface** 命令的计数器。
show interface	显示接口的运行时间状态和统计信息。

show vm

要显示 threat defense virtual 设备上的虚拟平台信息，请使用 **show vm** 命令。

show vm

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例显示如何显示有关 VMware 的信息：

```
> show vm

Virtual Platform Resource Status
--------------------------------
Number of vCPUs           :  4
Processor Memory          :  8192 MB
Hypervisor                :  VMware
```

show vpdn

要显示虚拟专用拨号网络 (VPDN) 连接（例如 PPPoE 或 L2TP）的状态，请使用 **show vpdn** 命令。

show vpdn {**group** *name* | **pppinterface id** *number* | **session** {**l2tp** | **pppoe**} **id** *number* {**packets** | **state** | **window**} | **tunnel** {**l2tp** | **pppoe**} **id** *number* {**packets** | **state** | **summary** | **transport**} | **username** *name*}

Syntax Description

group *name*	显示 VPDN 组配置。
id *number*	（可选）显示有关具有指定 ID 的 VPDN 会话的信息。
l2tp	（可选）显示有关 L2TP 的会话或隧道信息。
packets	显示会话或隧道数据包信息。
pppinterface	显示 PPP 接口信息。
pppoe	（可选）显示有关 PPPoE 的会话或隧道信息。
session	显示会话信息。
state	显示会话或隧道状态信息。
summary	显示隧道摘要。
transport	显示隧道传输信息。
tunnel	显示隧道信息。
username *name*	显示用户信息。
window	显示会话窗口信息。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用此命令可对 VPDN PPPoE 或 L2TP 连接进行故障排除。

示例

以下是 **show vpdn session** 命令的输出示例：

```
> show vpdn session
```

```
PPPoE Session Information (Total tunnels=1 sessions=1)
Remote Internet Address is 10.0.0.1
  Session state is SESSION_UP
    Time since event change 65887 secs, interface outside
    PPP interface id is 1
    6 packets sent, 6 received, 84 bytes sent, 0 received
```

以下是 **show vpdn tunnel** 命令的输出示例：

```
> show vpdn tunnel
PPPoE Tunnel Information (Total tunnels=1 sessions=1)
Tunnel id 0, 1 active sessions
   time since change 65901 secs
   Remote Internet Address 10.0.0.1
   Local Internet Address 199.99.99.3
```

show vpn load-balancing

请勿使用此命令。它与 threat defense不支持的功能相关。

show vpn-sessiondb

要显示有关 VPN 会话的信息，请使用以下 **show vpn-sessiondb** 命令之一。

show vpn-sessiondb ［**detail**］［**full**］｛**anyconnect** | **l2l** | **ra-ikev1-ipsec** | **ra-ikev2-ipsec**｝［**filter** *criteria*］［**sort** *criteria*］
show vpn-sessiondb ［**detail**］［**full**］ **index** *indexnumber*
show vpn-sessiondb failover
show vpn-sessiondb ospfv3 ［**filter ipaddress** *IP_address*］［**sort ipaddress**］

Syntax Description

anyconnect	显示 AnyConnect VPN 客户端会话。
detail	（可选）显示会话的相关扩展详细信息。例如，detail 选项用于 IPsec 会话，会显示其他详细信息，例如 IKE 散列算法、身份验证模式和再生密钥时间间隔。 如果您选择 detail 和 full 选项，则 threat defense 设备以机器可读格式显示详细输出。
failover	显示故障转移 IPsec 隧道的会话信息。
filter *filter_criteria*	（可选）根据指定的过滤器选项过滤输出。有关选项列表，请参阅使用指南部分。
full	（可选）显示流式未截断输出。在记录之间用 | 字符和 || 字符串对输出进行分段。
index *indexnumber*	按索引编号显示单个会话。指定会话的索引编号（范围为 1 - 65535）。
l2l	显示 VPN LAN-to-LAN 会话信息。
ospfv3	显示 OSPFv3 会话信息。
ra-ikev1-ipsec	显示 IPsec IKEv1 会话。
ra-ikev2-ipsec	显示 IKEv2 远程访问客户端连接的详细信息。
sort *sort_criteria*	（可选）根据您指定的排序选项将输出排序。有关选项列表，请参阅使用指南部分。

Command History

版本	修改
6.1	引入了此命令。

使用指南

您可以使用以下选项对会话显示进行过滤和排序：可以过滤和排序的值因列出的会话类型而异。

Filter/Sort 选项	Description
filter a-ipaddress *IP_address*	过滤输出以仅显示指定的分配 IP 地址的信息。 配合使用： **anyconnect**、 **ra-ikev2-ipsec**
sort a-ipaddress	按分配的 IP 地址排序显示。 配合使用： **anyconnect**、 **ra-ikev2-ipsec**
filter a-ipversion {**v4** | **v6**}	过滤输出，仅显示已分配 IPv4 或 IPv6 地址的会话。 配合使用： **anyconnect**、 **ra-ikev2-ipsec**
filter encryption *encryption_algorithm*	过滤输出以仅显示使用指定加密算法的会话的信息。使用 ? 查看可用的方法。 配合使用： **anyconnect**、 **l2l**、 **ra-ikev2-ipsec**
sort encryption	按会话中使用的加密算法对输出进行排序。 配合使用： **anyconnect**、 **l2l**、 **ra-ikev2-ipsec**
filter inactive	过滤空闲和可能失去连接（由于休眠、移动设备断开连接等等）的非活动会话。从 threat defense 设备发送 TCP 保持连接而没有收到来自 AnyConnect 客户端的响应时，非活动会话数量会增长。用 SSL 隧道丢弃时间为每个会话加上时间戳。如果会话主动通过 SSL 隧道传输流量，则显示 00:00m:00s。 配合使用： **anyconnect** 注释 threat defense 设备不会将 TCP 保持连接发送到一些设备（例如 iPhone、iPad 和 iPod）以延长电池续航时间，因此故障检测无法区分断开连接与休眠。因此，按照设计，非活动状态计数器将保持为 00:00:00。
sort inactivity	将非活动会话排序。 配合使用： **anyconnect**
filter ipaddress *IP_address*	过滤输出以仅显示内部分配 IP 地址的信息。 配合使用： **l2l**、 **ospfv3**
sort ipaddress	按内部 IP 地址将显示排序。 配合使用： **l2l**、 **ospfv3**
filter ipversion {**v4** | **v6**}	过滤输出，仅显示源自具有 IPv4 或 IPv6 地址的终端的会话。 配合使用： **l2l**
filter name *username*	过滤输出以显示指定用户名的会话。 配合使用： **anyconnect**、 **l2l**、 **ra-ikev2-ipsec**

Filter/Sort 选项	Description
sort name	按用户名的字母顺序将显示排序。 配合使用： **anyconnect**、 **l2l**、 **ra-ikev2-ipsec**
filter p-ipaddress *IP_address*	过滤输出以仅显示公共外部分配 IP 地址的信息。 配合使用： **anyconnect**、 **ra-ikev2-ipsec**
sort p-ipaddress	按公共外部 IP 地址对显示内容进行排序。 配合使用： **anyconnect**、 **ra-ikev2-ipsec**
filter p-ipversion {**v4** | **v6**}	过滤输出，仅显示来自具有公共 IPv4 或 IPv6 地址的终端的会话。 配合使用： **anyconnect**、 **ra-ikev2-ipsec**
filter protocol *name*	过滤输出以仅显示使用指定协议的会话的信息。使用 ? 查看可用的协议。 配合使用： **anyconnect**、 **l2l**、 **ra-ikev2-ipsec**
sort protocol	按协议将显示排序。 配合使用： **anyconnect**、 **l2l**、 **ra-ikev2-ipsec**

下表对可能看到的输出字段进行了解释。

字段	Description
Auth Mode	用于身份验证该会话的协议或模式。
Bytes Rx	系统从远程对等设备或客户端接收的字节总数。
Bytes Tx	系统传输到远程对等设备或客户端的字节数。
Client Type	在远程对等设备上运行的客户端软件（如果可用）。
Client Ver	在远程对等设备上运行的客户端软件的版本。
Connection	连接或专用 IP 地址的名称。
D/H Group	Diffie-Hellman 组。用于生成 IPsec SA 加密密钥的算法和密钥大小。
Duration	会话登录时间与上次屏幕刷新之间的已用时间 (HH:MM:SS)。
EAPoUDP Session Age	上次成功的状态验证以来的秒数。
Encapsulation	用于应用 IPsec ESP（封装安全负载协议）加密和身份验证的模式（即，应用了 ESP 的原始 IP 数据包的一部分）。
Encryption	此会话使用的数据加密算法（如果有）。
EoU Age (T)	EAPoUDP Session Age 上次成功的状态验证以来的秒数。

字段	Description
Filter Name	指定的用来限制会话信息显示的用户名。
Hashing	用于创建数据包的散列的算法，该算法用于 IPsec 数据身份验证。
Hold Left (T)	Hold-Off Time Remaining. 如果上一状态验证成功，则为 0 秒。否则，为下一终端安全评估验证尝试之前剩余的秒数。
剩余的延缓时间	如果上一状态验证成功，则为 0 秒。否则，为下一终端安全评估验证尝试之前剩余的秒数。
IKE Neg Mode	用于交换密钥信息和设施 SA 的 IKE（IPsec 阶段 1）模式：积极或主要。
IKE Sessions	IKE（IPsec 阶段 1）会话数；通常为 1。这些会话为 IPsec 流量建立隧道。
Index	此记录的唯一标识符。
IP Addr	为此会话分配给远程客户端的专用 IP 地址。这也称为“内部”或“虚拟”IP 地址。它允许客户端在专用网络中显示为主机。
IPsec Sessions	IPsec（阶段 2）会话数，即通过隧道的数据流量会话。每个 IPsec 远程访问会话可以有两个 IPsec 会话：一个包含隧道终端，而另一个包含可通过隧道访问的专用网络。
License Information	显示关于共享 SSL VPN 许可证的信息。
Local IP Addr	分配给隧道本地终端（这是系统上的接口）的 IP 地址。
Login Time	会话登录的日期和时间 (MMM DD HH:MM:SS)。时间以 24 小时制显示。
NAC Result	网络准入控制状态验证的状态。它可以是下列类型之一： • Accepted - ACS 已成功验证远程主机的终端安全评估。 • Rejected - ACS 未能成功验证远程主机的终端安全评估。 • Exempted - 根据 threat defense 设备上配置的 Posture Validation Exception 列表，远程主机已被豁免终端安全评估验证。 • Non-Responsive - 远程主机没有响应 EAPoUDP Hello 消息。 • Hold-off - threat defense 设备在终端安全评估验证成功后丢失与远程主机的 EAPoUDP 通信。 • N/A - 根据 VPN NAC 组策略，已为远程主机禁用 NAC。 • Unknown - 终端安全评估验证正在进行中。
NAC Sessions	网络准入控制（EAPoUDP）会话数。
Packets Rx	系统从远程对等设备接收的数据包的数量。

字段	Description
Packets Tx	系统传输到远程对等设备的数据包数。
PFS Group	完全转发保密组编号。
Posture Token	访问控制服务器上可配置的信息文本字符串。ACS将安全评估令牌下载至系统，以实现协助系统监控、报告、调试和记录的参考用途。典型的安全评估令牌标记为正常、检查、隔离、感染或未知。
Protocol	会话使用的协议。
Public IP	分配给客户端的公共可路由 IP 地址。
Redirect URL	在安全状态验证或无客户端身份验证后，ACS将会话的访问策略下载到系统。Redirect URL 是访问策略负载的可选部分。系统将此远程主机的所有 HTTP（端口 80）和 HTTPS（端口 443）请求重定向至 Redirect URL（如果有）。如果访问策略不包含 Redirect URL， threat defense 设备不会重定向来自远程主机的 HTTP 和 HTTPS 请求。 重定向URL保持有效，直到IPsec会话结束或直到终端安全评估重新验证为止，对此，ACS 下载新的访问策略，其中可以包含其他重新定向 URL 或不包含重定向 URL。
Rekey Int (T or D)	IPsec（IKE）SA 加密密钥的生命期。T 值是持续时间，D 值是传输的数据。仅显示远程访问 VPN 的 T 值。
Rekey Left (T or D)	IPsec（IKE）SA加密密钥的剩余生命期。T值是持续时间，D值是传输的数据。仅显示远程访问 VPN 的 T 值。
Rekey Time Interval	IPsec（IKE）SA 加密密钥的生命期。
Remote IP addr	分配给隧道的远程终端（即远程对等设备上的接口）的 IP 地址。
Reval Int (T)	Revalidation Time Interval. 每次成功的状态验证之间所需的时间间隔（以秒为单位）。
Reval Left (T)	到下次重新验证的时间。如果上一状态验证尝试失败，则为 0。否则，为重新验证时间间隔与上次成功终端安全评估验证以来的秒数之间的差值。
重新验证时间间隔	每次成功的状态验证之间所需的时间间隔（以秒为单位）。
Session ID	会话组件（子会话）的标识符。每个 SA 都有自己的标识符。
Session Type	会话的类型：LAN-to-LAN 或 Remote
SQ Int (T)	Status Query Time Interval. 每次成功的状态验证或状态查询响应与下一次状态查询响应之间允许的时间（以秒为单位。状态查询是系统向远程主机发出的请求，指示主机在上次终端安全评估验证后是否有任何终端安全评估更改。

字段	Description
状态查询时间间隔	每次成功的状态验证或状态查询响应与下一次状态查询响应之间允许的时间（以秒为单位。状态查询是系统向远程主机发出的请求，指示主机在上次终端安全评估验证后是否有任何终端安全评估更改。
Time Until Next Revalidation	如果上一状态验证尝试失败，则为 0。否则，为重新验证时间间隔与上次成功终端安全评估验证以来的秒数之间的差值。
Tunnel Group	此隧道针对属性值引用的隧道组的名称。
UDP Dst Port or UDP Destination Port	远程对等设备用于 UDP 的端口号。
UDP Src Port or UDP Source Port	用于 UDP 的端口号。
Username	建立会话所使用的用户登录名称。
VLAN	分配给此会话的出口 VLAN 接口。系统将所有流量转发到此 VLAN。以下元素之一指定值：组策略或继承的组策略

示例

以下是 **show vpn-sessiondb** 命令的输出示例：

```
> show vpn-sessiondb
--------------------------------------------------------------------------------
VPN Session Summary
--------------------------------------------------------------------------------
                            Active : Cumulative : Peak Concur : Inactive
                           ------------------------------------------------
AnyConnect Client           :      1 :         12 :           3 :        0
  SSL/TLS/DTLS              :      1 :         12 :           3 :        0
Clientless VPN              :      0 :          6 :           2
  Browser                   :      0 :          6 :           2
--------------------------------------------------------------------------------
Total Active and Inactive   :      1             Total Cumulative :     18
Device Total VPN Capacity   :    250
Device Load                 :     0%
--------------------------------------------------------------------------------

--------------------------------------------------------------------------------
Tunnels Summary
--------------------------------------------------------------------------------
                            Active : Cumulative : Peak Concurrent
                           ------------------------------------------------
Clientless                  :      0 :          7 :               2
AnyConnect-Parent           :      1 :         11 :               3
SSL-Tunnel                  :      1 :         12 :               3
DTLS-Tunnel                 :      1 :         12 :               3
```

```
-------------------------------------------------------------------------------
Totals                        :      3 :         42
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
IPv6 Usage Summary
-------------------------------------------------------------------------------
Active : Cumulative : Peak Concurrent
-----------------------------------------------
AnyConnect SSL/TLS/DTLS : : :
IPv6 Peer : 1 : 41 : 2
Tunneled IPv6 : 1 : 70 : 2
AnyConnect IKEv2 : : :
IPv6 Peer : 0 : 4 : 1
Clientless : : :
IPv6 Peer : 0 : 1 : 1
-------------------------------------------------------------------------------
```

以下是 **show vpn-sessiondb detail** 命令的输出示例：

```
> show vpn-sessiondb detail
-------------------------------------------------------------------------------
VPN Session Summary
-------------------------------------------------------------------------------
                            Active : Cumulative : Peak Concur : Inactive
                           ----------------------------------------------
AnyConnect Client           :      1 :         12 :           3 :        0
  SSL/TLS/DTLS              :      1 :         12 :           3 :        0
Clientless VPN              :      0 :          6 :           2
  Browser                   :      0 :          6 :           2
-------------------------------------------------------------------------------
Total Active and Inactive   :      1             Total Cumulative :     18
Device Total VPN Capacity   :    250
Device Load                 :     0%
-------------------------------------------------------------------------------

-------------------------------------------------------------------------------
Tunnels Summary
-------------------------------------------------------------------------------
                            Active : Cumulative : Peak Concurrent
                           ----------------------------------------------
Clientless                  :      0 :          7 :               2
AnyConnect-Parent           :      1 :         11 :               3
SSL-Tunnel                  :      1 :         12 :               3
DTLS-Tunnel                 :      1 :         12 :               3
-------------------------------------------------------------------------------
Totals                      :      3 :         42
-------------------------------------------------------------------------------
```

以下是 **show vpn-sessiondb detail l2l** 命令的输出示例：

```
> show vpn-sessiondb detail l2l
Session Type: LAN-to-LAN Detailed

Connection : 172.16.0.0
Index : 1
IP Addr : 172.16.0.0
Protocol : IKEv2 IPsec
Encryption : IKEv2: (1)AES256 IPsec: (1)AES256
Hashing : IKEv2: (1)SHA1 IPsec: (1)SHA1
Bytes Tx : 240 Bytes Rx : 160
Login Time : 14:50:35 UTC Tue May 1 2017
```

```
Duration : 0h:00m:11s
IKEv2 Tunnels: 1
IPsec Tunnels: 1

IKEv2:
Tunnel ID : 1.1
UDP Src Port : 500 UDP Dst Port : 500
Rem Auth Mode: preSharedKeys
Loc Auth Mode: preSharedKeys
Encryption : AES256 Hashing : SHA1
Rekey Int (T): 86400 Seconds Rekey Left(T): 86389 Seconds
PRF : SHA1 D/H Group : 5
Filter Name :
IPv6 Filter :

IPsec:
Tunnel ID : 1.2
Local Addr : 10.0.0.0/255.255.255.0
Remote Addr : 209.165.201.30/255.255.255.0
Encryption : AES256 Hashing : SHA1
Encapsulation: Tunnel PFS Group : 5
Rekey Int (T): 120 Seconds Rekey Left(T): 107 Seconds
Rekey Int (D): 4608000 K-Bytes Rekey Left(D): 4608000 K-Bytes
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Bytes Tx : 240 Bytes Rx : 160
Pkts Tx : 3 Pkts Rx : 2

NAC:
Reval Int (T): 0 Seconds Reval Left(T): 0 Seconds
SQ Int (T) : 0 Seconds EoU Age(T) : 13 Seconds
Hold Left (T): 0 Seconds Posture Token:
Redirect URL :
```

以下是 **show vpn-sessiondb detail index 1** 命令的输出示例：

```
> show vpn-sessiondb detail index 1

Session Type: Remote Detailed

Username : user1
Index : 1
Assigned IP : 192.168.2.70 Public IP : 10.86.5.114
Protocol : IPsec Encryption : AES128
Hashing : SHA1
Bytes Tx : 0 Bytes Rx : 604533
Client Type : WinNT Client Ver : 4.6.00.0049
Tunnel Group : bxbvpnlab
Login Time : 15:22:46 EDT Tue May 10 2005
Duration : 7h:02m:03s
Filter Name :
NAC Result : Accepted
Posture Token: Healthy
VM Result : Static
VLAN : 10

IKE Sessions: 1 IPsec Sessions: 1 NAC Sessions: 1

IKE:
Session ID : 1
UDP Src Port : 500 UDP Dst Port : 500
IKE Neg Mode : Aggressive Auth Mode : preSharedKeysXauth
Encryption : 3DES Hashing : MD5
```

```
Rekey Int (T): 86400 Seconds Rekey Left(T): 61078 Seconds
D/H Group : 2

IPsec:
Session ID : 2
Local Addr : 0.0.0.0
Remote Addr : 192.168.2.70
Encryption : AES128 Hashing : SHA1
Encapsulation: Tunnel
Rekey Int (T): 28800 Seconds Rekey Left(T): 26531 Seconds
Bytes Tx : 0 Bytes Rx : 604533
Pkts Tx : 0 Pkts Rx : 8126

NAC:
Reval Int (T): 3000 Seconds Reval Left(T): 286 Seconds
SQ Int (T) : 600 Seconds EoU Age (T) : 2714 Seconds
Hold Left (T): 0 Seconds Posture Token: Healthy
Redirect URL : www.cisco.com
```

以下是 **show vpn-sessiondb ospfv3** 命令的输出示例：

```
> show vpn-sessiondb ospfv3

Session Type: OSPFv3 IPsec

Connection :
Index : 1 IP Addr : 0.0.0.0
Protocol : IPsec
Encryption : IPsec: (1)none Hashing : IPsec: (1)SHA1
Bytes Tx : 0 Bytes Rx : 0
Login Time : 15:06:41 EST Wed Feb 1 2017
Duration : 1d 5h:13m:11s
```

以下是 **show vpn-sessiondb detail ospfv3** 命令的输出示例：

```
> show vpn-sessiondb detail ospfv3

Session Type: OSPFv3 IPsec Detailed

Connection :
Index : 1 IP Addr : 0.0.0.0
Protocol : IPsec
Encryption : IPsec: (1)none Hashing : IPsec: (1)SHA1
Bytes Tx : 0 Bytes Rx : 0
Login Time : 15:06:41 EST Wed Feb 1 2017
Duration : 1d 5h:14m:28s
IPsec Tunnels: 1

IPsec:
Tunnel ID : 1.1
Local Addr : ::/0/89/0
Remote Addr : ::/0/89/0
Encryption : none Hashing : SHA1
Encapsulation: Transport
Idle Time Out: 0 Minutes Idle TO Left : 0 Minutes
Bytes Tx : 0 Bytes Rx : 0
Pkts Tx : 0 Pkts Rx : 0
NAC:
Reval Int (T): 0 Seconds Reval Left(T): 0 Seconds
SQ Int (T) : 0 Seconds EoU Age(T) : 105268 Seconds
Hold Left (T): 0 Seconds Posture Token:
```

```
Redirect URL :
```

以下是 **show vpn-sessiondb detail anyconnect** 命令的输出示例：

```
> show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : userab Index : 2
Assigned IP : 65.2.1.100 Public IP : 75.2.1.60
Assigned IPv6: 2001:1000::10
Protocol : IKEv2 IPsecOverNatT AnyConnect-Parent
License : AnyConnect Premium
Encryption : IKEv2: (1)3DES IPsecOverNatT: (1)3DES AnyConnect-Parent: (1)none
Hashing : IKEv2: (1)SHA1 IPsecOverNatT: (1)SHA1 AnyConnect-Parent: (1)none
Bytes Tx : 0 Bytes Rx : 21248
Pkts Tx : 0 Pkts Rx : 238
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : DfltGrpPolicy Tunnel Group : test1
Login Time : 22:44:59 EST Tue Aug 13 2017
Duration : 0h:02m:42s
Inactivity : 0h:00m:00s
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none

IKEv2 Tunnels: 1
IPsecOverNatT Tunnels: 1
AnyConnect-Parent Tunnels: 1

AnyConnect-Parent:
Tunnel ID : 2.1
Public IP : 75.2.1.60
Encryption : none Hashing : none
Auth Mode : userPassword
Idle Time Out: 400 Minutes Idle TO Left : 397 Minutes
Conn Time Out: 500 Minutes Conn TO Left : 497 Minutes
Client OS : Windows
Client Type : AnyConnect
Client Ver : 3.1.05050

IKEv2:
Tunnel ID : 2.2
UDP Src Port : 64251 UDP Dst Port : 4500
Rem Auth Mode: userPassword
Loc Auth Mode: rsaCertificate
Encryption : 3DES Hashing : SHA1
Rekey Int (T): 86400 Seconds Rekey Left(T): 86241 Seconds
PRF : SHA1 D/H Group : 2
Filter Name : mixed1
Client OS : Windows

IPsecOverNatT:
Tunnel ID : 2.3
Local Addr : 75.2.1.23/255.255.255.255/47/0
Remote Addr : 75.2.1.60/255.255.255.255/47/0
Encryption : 3DES Hashing : SHA1
Encapsulation: Transport, GRE
Rekey Int (T): 28400 Seconds Rekey Left(T): 28241 Seconds
Idle Time Out: 400 Minutes Idle TO Left : 400 Minutes
Conn Time Out: 500 Minutes Conn TO Left : 497 Minutes
Bytes Tx : 0 Bytes Rx : 21326
Pkts Tx : 0 Pkts Rx : 239
```

```
NAC:
Reval Int (T): 0 Seconds Reval Left(T): 0 Seconds
SQ Int (T) : 0 Seconds EoU Age(T) : 165 Seconds
Hold Left (T): 0 Seconds Posture Token:
Redirect URL :
```

以下是 **show vpn-sessiondb ra-ikev2-ipsec** 命令的输出示例：

```
> show vpn-sessiondb detail ra-ikev2-ipsec

Session Type: Generic Remote-Access IKEv2 IPsec Detailed

Username : IKEV2TG Index : 1
Assigned IP : 95.0.225.200 Public IP : 85.0.224.12
Protocol : IKEv2 IPsec
License : AnyConnect Essentials
Encryption : IKEv2: (1)3DES IPsec: (1)AES256
Hashing : IKEv2: (1)SHA1 IPsec: (1)SHA1
Bytes Tx : 0 Bytes Rx : 17844
Pkts Tx : 0 Pkts Rx : 230
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : GroupPolicy_IKEV2TG Tunnel Group : IKEV2TG
Login Time : 11:39:54 UTC Tue May 6 2017
Duration : 0h:03m:17s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 5f00e105000010005368ca0a
Security Grp : none

IKEv2 Tunnels: 1
IPsec Tunnels: 1
```

以下是 **show vpn-sessiondb anyconnect** 命令的输出示例：

```
> show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : user1                  Index        : 19576
Assigned IP  : 192.168.3.243          Public IP    : 192.168.10.61
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256  DTLS-Tunnel: (1)AES256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 15060                  Bytes Rx     : 20631
Group Policy : DfltGrpPolicy          Tunnel Group : Ad_group
Login Time   : 09:24:53 UTC Fri Apr 7 2017
Duration     : 0h:03m:20s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : c0a8013804c7800058e75ae5
Security Grp : none                   Tunnel Zone  : 0
```

Related Commands

命令	Description
clear vpn-sessiondb statistics	清除 VPN 会话统计信息。

命令	Description
show vpn-sessiondb ratio	显示 VPN 会话加密或协议比率。
show vpn-sessiondb summary	显示会话摘要，包括当前会话总数、每种类型的当前会话、峰值和累积总值、最大并发会话数。

show vpn-sessiondb ratio

要按协议或加密算法以百分比形式显示当前会话的比率，请使用 **show vpn-sessiondb ratio** 命令。

show vpn-sessiondb ratio {**encryption** | **protocol**} [**filter** *groupname*]

Syntax Description

encryption	显示使用每种加密方法的会话数和会话百分比。
protocol	显示使用每个 VPN 协议的会话数和会话百分比。
filter *groupname*	（可选。）过滤输出以仅包含所指定的隧道组的会话比率。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例显示如何根据加密显示会话比率。

```
> show vpn-sessiondb ratio encryption

Filter Group         : All
Total Active Sessions: 5
Cumulative Sessions  : 9
Encryption               Tunnels        Percent
none                     0                0%
DES                      0                0%
3DES                     0                0%
RC4                      0                0%
AES128                   4               80%
AES192                   1               20%
AES256                   0                0%
AES-GCM-128              0                0%
AES-GCM-192              0                0%
AES-GCM-256              0                0%
AES-GMAC-128             0                0%
AES-GMAC-192             0                0%
AES-GMAC-256             0                0%
```

以下示例显示如何根据协议显示会话比率。

```
> show vpn-sessiondb ratio protocol

Filter Group         : All
Total Active Tunnels : 3
Cumulative Tunnels   : 42

Protocol                 Tunnels        Percent
IKEv1                    0                0%
IKEv2                    0                0%
IPsec                    0                0%
```

```
IPsecLAN2LAN              0               0%
IPsecLAN2LANOverNatT      0               0%
IPsecOverNatT             0               0%
IPsecOverTCP              0               0%
IPsecOverUDP              0               0%
L2TPOverIPsec             0               0%
L2TPOverIPsecOverNatT     0               0%
Clientless                0               0%
Port-Forwarding           0               0%
IMAP4S                    0               0%
POP3S                     0               0%
SMTPS                     0               0%
AnyConnect-Parent         1              33%
SSL-Tunnel                1              33%
DTLS-Tunnel               1              33%
```

Related Commands

命令	Description
show vpn-sessiondb	显示有关 VPN 会话的信息。
show vpn-sessiondb summary	显示会话摘要，包括当前会话总数、每种类型的当前会话、峰值和累积总值、最大并发会话数。

show vpn-sessiondb summary

要显示活动会话数的摘要，请使用 **show vpn-sessiondb summary** 命令。

show vpn-sessiondb summary

Command History

版本	修改
6.1	引入了此命令。

使用指南

下表解释了活动会话和会话信息摘要中的字段：

字段	Description
Concurrent Limit	此系统上允许的并发活动会话的最大数量。
Cumulative Sessions	自上次启动或重置系统以来所有类型的会话数。
LAN-to-LAN	当前处于活动状态的 IPsec LAN-to-LAN 会话数。
Peak Concurrent	自上次启动或重置系统以来并发活动的所有类型会话的最大数量。
Percent Session Load	使用中的 VPN 会话分配的百分比。此值等于活动会话总数除以可用会话的最大数量（以百分比形式显示）。
Remote Access	ra-ikev1-ipsec - IKEv1 IPsec 远程访问用户数、L2TP over IPsec 以及通过当前活动的 NAT 会话的 IPsec。
Total Active Sessions	当前处于活动状态的所有类型会话的数量。

示例

以下是 **show vpn-sessiondb summary** 命令的输出示例：

```
> show vpn-sessiondb summary
-------------------------------------------------------------------------
VPN Session Summary
-------------------------------------------------------------------------
Active : Cumulative : Peak Concur : Inactive
-----------------------------------------------
OSPFv3 IPsec : 1 : 1 : 1
-------------------------------------------------------------------------
Total Active and Inactive : 1 Total Cumulative : 1
Device Total VPN Capacity : 10000
Device Load : 0%
-------------------------------------------------------------------------
```

以下是常规 IKEv2 IPsec 远程访问会话的 **show vpn-sessiondb summary** 命令的输出示例：

```
> show vpn-sessiondb summary
-------------------------------------------------------------------------------
VPN Session Summary
-------------------------------------------------------------------------------
Active : Cumulative : Peak Concur : Inactive
----------------------------------------------
Generic IKEv2 Remote Access : 1 : 1 : 1
-------------------------------------------------------------------------------
Total Active and Inactive : 1 Total Cumulative : 1
Device Total VPN Capacity : 250
Device Load : 0%
-------------------------------------------------------------------------------

-------------------------------------------------------------------------------
Tunnels Summary
-------------------------------------------------------------------------------
Active : Cumulative : Peak Concurrent
----------------------------------------------
IKEv2 : 1 : 1 : 1
IPsec : 1 : 1 : 1
-------------------------------------------------------------------------------
Totals : 2 : 2
-------------------------------------------------------------------------------
```

Related Commands

命令	Description
show vpn-sessiondb	显示有关 VPN 会话的信息。
show vpn-sessiondb ratio	显示 VPN 会话加密或协议比率。

show vrf

要显示有关系统上定义的虚拟路由器的信息，请使用 **show vrf** 命令。

show vrf ［**counters** | **lock**］

Syntax Description

counters	（可选）显示此系统上允许的用户定义的最大虚拟路由器数量，以及配置的实际虚拟路由器数量。最大计数文档不包括全局虚拟路由器：例如，如果最大计数为 4，则总数限制为 5。
lock	（可选）显示 VRF 锁定信息。

Command Default

如果不使用关键字， 命令会显示当前虚拟路由器以及分配给每个虚拟路由器的接口。

Command History

版本	修改
6.6	引入了此命令。

使用指南

如果启用了虚拟路由和转发 (VRF)，请使用 **show vrf** 命令查看有关系统上定义的虚拟路由器的基本信息。要查看每个虚拟路由器的路由表，请对 IPv4 路由表使用 。 **show route vrf** 名称 命令，对 IPv6 路由表使用 **show ipv6 route vrf** 名称 。

示例

以下示例显示了虚拟路由器和分配给每个路由器的接口：

```
> show vrf

Name            VRF ID          Description             Interfaces
vrf1            1                                       inside
                                                        inside_2
vrf2            2                                       inside_3
                                                        inside_4
```

以下示例显示了此系统上允许的最大虚拟路由器数量，以及当前虚拟路由器的数量。虚拟路由器是 IPv4、IPv6 还是两者兼有，取决于您为每个虚拟路由器内的接口分配的 IP 地址。请注意，最大数量是指用户定义的虚拟路由器；在本示例中，对于 VMware 系统，允许的总限制为 15，其中一个用于全局虚拟路由器，14 个用于用户定义的路由器。

```
> show vrf counters
Maximum number of VRFs supported: 14
Maximum number of IPv4 VRFs supported: 14
Maximum number of IPv6 VRFs supported: 14
Current number of VRFs: 2
Current number of VRFs in delete state: 0
```

以下示例显示 VRF 锁定信息。

```
> show vrf lock

VRF Name: single_vf; VRF id = 0 (0x0)
VRF lock count: 1
VRF Name: vrf1; VRF id = 1 (0x1)
VRF lock count: 2
VRF Name: vrf2; VRF id = 2 (0x2)
VRF lock count: 2
```

Related Commands

命令	Description
show ipv6 route	显示 IPv6 路由表。
show route	显示 IPv4 路由表。

show wccp

要显示与 Web 缓存通信协议 (WCCP) 相关的全局统计信息，请使用 **show wccp** 命令。

show wccp {**web-cache** | *service_number*} [**buckets** | **detail** | **service** | **view** | **hash** *dest_addr source_addr dest_port source_port*]
show wccp [**interfaces** [**detail**]]

Syntax Description

buckets	（可选）显示服务组存储桶分配。
detail	（可选）显示关于路由器和所有 Web 缓存的信息。
hash *dest_addr source_addr dest_port source_port*	（可选）显示指定连接的 WCCP 散列： • *dest_addr* 是目的主机的 IP 地址。 • *source_addr* 是源主机的 IP 地址。 • *Dest_port* 是目标主机的端口。 • *source_port* 是源主机的端口。
interfaces [**detail**]	（可选）显示 WCCP 重定向接口。包括用于接口配置的 detail 关键字。
service	（可选）显示服务组定义信息。
service-number	缓存所控制的 Web 缓存服务组的标识号。数字可以是 0 到 254。对于使用 Cisco Cache Engine 的 Web 缓存，以值 99 指示反向代理服务。
view	（可选）显示已检测或尚未检测特定服务组的其他成员。
web-cache	指定 Web 缓存服务的统计信息。

Command History

版本	修改
6.2	引入了此命令。

示例

以下示例展示如何显示 WCCP 信息：

```
> show wccp
Global WCCP information:
    Router information:
        Router Identifier:                  -not yet determined-
        Protocol Version:                   2.0
    Service Identifier: web-cache
        Number of Cache Engines:            0
        Number of routers:                  0
```

```
Total Packets Redirected:           0
Redirect access-list:               foo
Total Connections Denied Redirect:  0
Total Packets Unassigned:           0
Group access-list:                  foobar
Total Messages Denied to Group:     0
Total Authentication failures:      0
Total Bypassed Packets Received:    0
```

Related Commands

命令	Description
clear wccp	清除统计数据。

show webvpn

要查看有关远程接入 VPN 的信息，请使用 **show webvpn** 命令。

show webvpn {**anyconnect** | **debug-condition** | **group-alias** [*tunnel_group*] | **group-url** [*tunnel_group*] | **statistics**}

Syntax Description

anyconnect	显示有关可下载到客户端终端的 AnyConnect 映像的信息。
debug-condition	显示 **debug webvpn condition** 命令设置的当前调试条件。
group-alias [*tunnel_group*]	显示隧道组的别名（连接配置文件）。您可以选择指定隧道组的名称，以仅查看有关该组的信息。每个组可以有多个别名或甚至没有别名。
group-url [*tunnel_group*]	显示隧道组（连接配置文件）的 URL。您可以选择指定隧道组的名称，以仅查看有关该组的信息。每个组可以有多个 URL 或甚至没有 URL。
statistics	显示有关 WebVPN 事件的数据。

Command History

版本	修改
6.2.1	引入了此命令。
7.1	有关外部浏览器软件包的信息已添加到 AnyConnect 输出中。

示例

以下示例显示 **show webvpn anyconnect** 命令的输出示例：

```
> show webvpn anyconnect
1. disk0:/csm/anyconnect-win-4.2.06014-k9.pkg 1 cfg-regex=/Windows/
  CISCO STC win2k+
  4,2,06014
  Hostscan Version 4.2.06014
  Thu 10/06/2016 14:40:31.34

1 AnyConnect Client(s) installed
```

以下 **show webvpn anyconnect** 示例包括外部浏览器软件包（如果与 SAML 身份验证配合使用）。

```
> show webvpn anyconnect
1. disk0:/anyconnpkgs/anyconnect-win-4.10.01075-webdeploy-k9.pkg 2 dyn-regex=/Windows NT/
  CISCO STC win2k+
  4,10,01075
  Hostscan Version 4.10.01075
  Wed 04/28/2021 12:36:03.98

1 AnyConnect Client(s) installed
```

```
2. disk0:/externalbrowserpkgs/external-sso-98.161.00015-webdeploy-k9.pkg
  Cisco AnyConnect External Browser Headend Package
  98.161.00015
  Wed 05/05/21 15:49:27.817381
```

以下示例显示 **show webvpn debug-condition** 命令的输出示例：

```
> show webvpn debug-condition
INFO: Webvpn conditional debug is turned ON
INFO: IP address filters:
INFO: 10.100.10.10/32
```

以下示例显示 **show webvpn group-alias** 命令的输出示例：

```
> show webvpn group-alias
Tunnel Group: Ad_group   Group Alias: ad_group enabled
Tunnel Group: Radius_group   Group Alias: Radius_group enabled
Tunnel Group: Cert_auth   Group Alias: cert_auth enabled
```

以下示例显示 **show webvpn group-url** 命令的输出示例：

```
> show webvpn group-url
http://www.cisco.com
https://ger1.example.com
https://ger2.example.com
```

以下示例显示 **show webvpn statistics** 命令的输出示例：

```
> show webvpn statistics
Total number of objects served  0
 html                           0
 js                             0
 css                            0
 vb                             0
 java archive                   0
 java class                     0
 image                          0
 undetermined                   0
Server compression statistics
 Decompression success from server                  0
 Unsolicited compression from server                0
 Unsupported compression algorithm used by server   0
 Decompression failure for server responses         0
IOBuf failure statistics
 uib_create_with_channel                            0
 uib_create_with_string                             0
 uib_create_with_string_and_channel                 0
 uib_transfer                                       0
 uib_add_filter                                     0
 uib_yyread                                         0
 uib_read                                           0
 uib_set_buffer_max                                 0
 uib_set_eof_symbol                                 0
 uib_get_capture_handle                             0
 uib_set_capture_handle                             0
 uib_buflen                                         0
 uib_bufptr                                         0
```

```
uib_buf_endptr                                0
uib_get_buf_offset                            0
uib_get_buf_offset_addr                       0
uib_get_nth_char                              0
uib_consume                                   0
uib_advance_bufptr                            0
uib_eof                                       0
```

show xlate

要显示有关 NAT 会话（转换或转换）的信息，请使用 **show xlate** 命令。

show xlate ［**global** *ip1*［*-ip2*］［**netmask** *mask*］］［**local** *ip1*［*-ip2*］［**netmask** *mask*］］［**gport** *port1*［*-port2*］］［**lport** *port1*［*-port2*］］［**interface** *if_name*］［**type** *type*］
show xlate count

Syntax Description

count	显示转换计数。
global *ip1*[*-ip2*]	（可选）按映射 IP 地址或地址范围显示活动的转换。
gport *port1*[*-port2*]	按映射端口或端口范围显示活动的转换。
interface *if_name*	（可选）按接口显示活动转换。
local *ip1*[*-ip2*]	（可选）按实际 IP 地址或地址范围显示活动的转换。
lport *port1*[*-port2*]	按实际端口或端口范围显示活动的转换。
netmask *mask*	（可选）指定用于限定映射的或实际 IP 地址的网络掩码。
type *type*	（可选）按类型显示活动的转换。您可以输入以下一个或多个类型： • **static** • **portmap** • **dynamic** • **twice-nat** （也称为手动 NAT） 指定多个类型时，请用空格来分隔类型。

Command History

版本	修改
6.1	引入了此命令。

使用指南

show xlate 命令显示转换槽的内容。转换可以包括为内部接口生成的转换，这些转换不会显示在设备管理器的 NAT 规则表中。这些是内部处理所必需的。

当 VPN 客户端配置已启用且内部主机发出 DNS 请求时， **show xlate** 命令可以为静态转换列出多个 xlate。

在集群环境中，可将最多三个 xlate 复制到集群中的不同节点以处理 PAT 会话。在拥有该连接的设备上创建了一个 xlate。在其他设备上创建一个 xlate 以备份 PAT 地址。最后，导向器上存在一个可复制该流的 xlate。在备用和导向器是同一设备的情况下，可能创建两个（而不是三个）xlate。

示例

以下是 **show xlate** 命令的输出示例。nlp_int_tap 的初始 PAT 转换与允许 设备管理器 访问 192.168.1.1 而非管理接口地址的 HTTPS 访问规则相关。这些是内部 NAT 转换，其规则不会显示在设备管理器的 NAT 表中。

```
> show xlate
13 in use, 14 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
       s - static, T - twice, N - net-to-net
TCP PAT from nlp_int_tap:169.254.1.2 443-443 to inside1_2:192.168.1.1 443-443
    flags sr idle 124:39:20 timeout 0:00:00
TCP PAT from nlp_int_tap:169.254.1.2 443-443 to inside1_3:192.168.1.1 443-443
    flags sr idle 124:39:20 timeout 0:00:00
TCP PAT from nlp_int_tap:169.254.1.2 443-443 to inside1_4:192.168.1.1 443-443
    flags sr idle 124:39:20 timeout 0:00:00
TCP PAT from nlp_int_tap:169.254.1.2 443-443 to inside1_5:192.168.1.1 443-443
    flags sr idle 124:39:20 timeout 0:00:00
TCP PAT from nlp_int_tap:169.254.1.2 443-443 to inside1_6:192.168.1.1 443-443
    flags sr idle 124:39:20 timeout 0:00:00
TCP PAT from nlp_int_tap:169.254.1.2 443-443 to inside1_7:192.168.1.1 443-443
    flags sr idle 124:39:20 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside1_8:0.0.0.0/0
    flags sIT idle 0:30:10 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside1_7:0.0.0.0/0
    flags sIT idle 124:39:20 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside1_6:0.0.0.0/0
    flags sIT idle 124:39:20 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside1_5:0.0.0.0/0
    flags sIT idle 124:39:20 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside1_4:0.0.0.0/0
    flags sIT idle 124:39:20 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside1_3:0.0.0.0/0
    flags sIT idle 124:39:20 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside1_2:0.0.0.0/0
    flags sIT idle 124:39:20 timeout 0:00:00
```

以下是来自 **show xlate** 命令的输出示例，其中显示从 IPv4 到 IPv6 的转换

```
> show xlate
14 in use, 14 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
       s - static, T - twice, N - net-to-net
(...other entries removed...)
NAT from outside:0.0.0.0/0 to inside1_8:2001:db8::/96
    flags s idle 0:01:36 timeout 0:00:00
```

Related Commands

命令	Description
clear xlate	清除当前转换和连接信息。
show conn	显示所有活动连接。
show local-host	显示本地主机网络信息。

show zone

要显示流量区域信息，请使用 **show zone** 命令。

show zone [*name*]

Syntax Description

name	（可选）流量区域的名称。

Command History

版本	修改
6.1	引入了此命令。

使用指南

流量区域与安全区域不完全相同。虽然被动安全区域也会自动生成为流量区域，但路由和交换安全区域不会自动生成。流量区域用以实现流量负载均衡（使用等价多路径 (ECMP) 路由）、路由冗余以及多个接口之间的不对称路由。

要查看区域配置的其余部分，请使用 **show running-config zone** 和 **show running-config interface** 命令。

示例

以下示例显示已配置的流量区域。在本示例中，流量区域用于被动接口。如果区域用于等价多路径路由，则区域类型将为 ecmp。接口配置如下。 **zone-member** 命令将接口配置为区域的成员。

```
> show zone passive-security-zone
Zone: passive-security-zone passive
    Security-level: 0
    Zone member(s): 1
      passive                       GigabitEthernet0/0

> show running-config interface gigabitethernet0/0
!
interface GigabitEthernet0/0
 mode passive
 nameif passive
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 zone-member krjones-passive-security-zone
```

Related Commands

命令	Description
clear conn zone	清除区域连接。
clear local-host zone	清除区域主机。
show interface	显示接口的运行时间状态和统计信息。

命令	Description
show local-host zone	显示区域内本地主机的网络状态。
show nameif zone	显示接口的区域或内联集成员身份。

shun

要阻止来自攻击主机的连接，请使用 **shun** 命令。要禁用 shun，请使用此命令的 **no** 形式。

shun *source_ip* ［*dest_ip source_port dest_port* ［*protocol*］］［**vlan** *vlan_id*］
no shun *source_ip* ［**vlan** *vlan_id*］

Syntax Description

dest_port	（可选）指定当您在源 IP 地址上放置 shun 时要丢弃的当前连接的目标端口。
dest_ip	（可选）指定当您在源 IP 地址上放置 shun 时要丢弃的当前连接的目标地址。
protocol	（可选）指定当您在源 IP 地址上放置 shun 时要丢弃的当前连接的 IP 协议，例如 UDP 或 TCP。默认情况下，protocol 为 0（任何协议）。
source_ip	指定攻击主机的地址。如果仅指定源 IP 地址，则以后来自此地址的所有连接都将被丢弃；当前连接保持不变。要丢弃当前连接并同时放置 shun，请指定连接的其他参数。请注意，shun 适用于后面所有来自源 IP 地址的连接，无论目标参数为何。
source_port	（可选）指定当您在源 IP 地址上放置 shun 时要丢弃的当前连接的源端口。
vlan *vlan_id*	（可选）指定源主机所在的 VLAN ID。

Command Default

默认协议是 0（任何协议）。

Command History

版本	修改
6.1	引入了此命令。

使用指南

shun 命令可以阻止来自攻击主机的连接。后面来自源 IP 地址的所有连接都将被丢弃并记录，直到手动取消阻止功能。无论使用指定主机地址的连接当前是否为活动状态， **shun** 命令的阻止功能都适用。

如果您指定目标地址、来源和目标端口以及协议，则会丢弃匹配的连接以及在后面所有来自源 IP 地址的连接上放置 shun；将会避开后面所有的连接，而不只是与这些特定连接参数匹配的连接。

对每个源 IP 地址只能使用一个 **shun** 命令。

由于 **shun** 命令用于动态阻止攻击，因此不会显示在 threat defense 设备配置中。

只要删除接口配置，所有附加到该接口的 shun 也会一同删除。

示例

以下示例展示攻击主机 (10.1.1.27) 使用 TCP 与受攻击主机 (10.2.2.89) 建立连接。 threat defense 设备连接表中的连接如下所示：

```
10.1.1.27, 555-> 10.2.2.89, 666 PROT TCP
```

使用以下选项应用 **shun** 命令：

```
> shun 10.1.1.27 10.2.2.89 555 666 tcp
Shun 10.1.1.27 added in context: single_vf
Shun 10.1.1.27 successful
```

此命令将从 threat defense 设备连接表删除特定的当前接通，同时禁止来自 10.1.1.27 的所有后续数据包通过 threat defense 设备。

Related Commands

命令	Description
clear shun	禁用当前启用的所有 shun 并清除 shun 统计信息。
show conn	显示所有活动连接。
show shun	显示 shun 信息。

shutdown

要关闭设备，请使用 **shutdown** 命令。

shutdown

Command History

版本	修改
6.0.1	引入了此命令。

示例

以下示例是关闭设备时 **shutdown** 命令的输出示例：

```
> shutdown
This command will shutdown the system.  Continue?
Please enter 'YES' or 'NO': YES
```

Related Commands

命令	Description
reboot	重启设备。

system access-control clear-rule-counts

要将访问控制规则命中次数重置为 0，请使用 **system access-control clear-rule-counts** 命令。

system access-control clear-rule-counts

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例显示 **system access-control clear-rule-counts** 命令的输出示例：

```
> system access-control clear-rule-counts
Are you sure that you want to clear the rule hit counters? (y/n): y
Clearing the rule hit counters.
Success.
```

Related Commands

命令	Description
show access-control-config	显示访问控制策略摘要和命中计数。

system generate-troubleshoot

要在思科技术支持部门要求时生成故障排除数据以供分析，请使用 **system generate troubleshoot** 命令。

system generate-troubleshoot 选项

Syntax Description

选项	显示要生成的故障排除数据的类型。您可以输入一个或多个选项。使用空格隔开多个选项。 • **ALL**-运行以下所有选项。 • **SNT**-Snort 性能和配置。 • **PER**-硬件性能和日志。- • **SYS**-系统配置、策略和日志。 • **DES**-检测配置、策略和日志。 • **NET**-接口和网络相关数据。 • **VDB**-发现、感知、VDB 数据和日志。 • **UPG**-升级数据和日志。 • **DBO**-所有数据库数据。 • **LOG**-所有日志数据。 • **NMP**-网络映射信息。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例显示如何为 Snort 和硬件性能生成故障排除数据。

```
> system generate-troubleshoot SNT PER
Starting /usr/local/sf/bin/sf_troubleshoot.pl...
Please, be patient.  This may take several minutes.
the troubleshoot options codes specified are SNT,PER.
getting filenames from [/ngfw/usr/local/sf/etc/db_updates/index]
getting filenames from [/ngfw/usr/local/sf/etc/db_updates/base-6.2.0]
Troubleshooting information successfully created at /ngfw/var/common/results-10-14-201
6--181112.tar.gz
```

Related Commands

命令	Description
copy	从系统复制文件或将文件复制到系统。
delete	从系统中删除文件。

system lockdown-sensor

要删除对专家模式和 Bash Shell 的访问，请使用 **system lockdown-sensor** 命令。

system lockdown-sensor

Command History

版本	修改
6.2.1	引入了此命令。

使用指南

注意 不能撤销此命令。如果您需要恢复对专家模式的访问，您必须联系思科技术支持中心并获取热补丁。

expert 命令提供对 Bash shell 的访问，为管理用户提供对系统操作环境的广泛访问。安全认证机制（例如通用标准 (CC) 或统一功能批准产品列表 (UC APL)）强加了限制系统用户可用的访问权限和信息的要求。使用 **system lockdown-sensor** 命令可删除对 **expert** 命令的访问，以帮助满足这些认证要求。

注释 使用此命令后， **expert** 命令在当前 SSH 会话中仍然可用。您必须注销并重新登录，以验证该命令是否已删除且不再有效。在您使用 命令后登录的任何其他人也将无法使用专家模式。

示例

以下示例删除对专家模式的访问，以满足安全要求。

```
> system lockdown-sensor
This action will remove the 'expert' command from your system for all
future CLI sessions, rendering the bash shell inaccessible.

This cannot be reversed without a support call.
Continue and remove the 'expert' command?

Please enter 'YES' or 'NO': YES
>
```

system support commands

大多数系统支持命令用于在思科技术支持中心的帮助下进行调试和故障排除。您应在思科支持人员的指导下使用这些命令，但以下命令除外，这些命令是通用的。

system support ssl-client-hello- commands

这些命令允许您确定传输层安全 (TLS) 1.3 降级到 TLS 1.2 的行为。由于受管设备不支持 TLS 1.3 加密或解密，因此客户端和服务器之间的 TLS 1.3 会话可能会中断，从而导致客户端网络浏览器中出现如下错误：

ERR_SSL_PROTOCOL_ERROR

SEC_ERROR_BAD_SIGNATURE

ERR_SSL_VERSION_INTERFERENCE

当客户端连接到服务器并且 TLS 检查确定已修改为降级的连接与 **不解密** SSL 规则操作匹配时，可能会发生错误。

我们建议您在咨询思科 TAC 之后再使用这些命令。

system support ssl-client-hello-enabled aggressive_tls13_downgrade { **true** | **false** }

Syntax Description

true	默认值。每当需要执行解密时，TLS 1.3 连接都会降级。但是，如果在 ClientHello 消息之后收到的数据导致会话匹配 **不解密** 规则，则会话可能会失败。
false	仅当合理确定会话与 **不解密** 规则不匹配时，才会降级 TLS 1.3 连接。在某些情况下，需要解密的 TLS 连接可能不会降级。在这些情况下，流量不会被解密。改为执行 SSL 策略中 **无法解密的操作** 的 **会话未缓存** 设置指定的操作。

Command History

版本	修改
6.2.3.7	引入了此命令。

system support diagnostic-cli

要进入诊断 CLI（包括其他 show 和其他故障排除命令），请使用 **system support diagnostic-cli** 命令。

system support diagnostic-cli

Command History

版本	修改
6.1	引入了此命令。

使用指南

诊断 CLI 包含可用于对系统进行故障排除的其他 show 和其他命令。诊断 CLI 中的命令来自 ASA 软件。常规 threat defense CLI 包含许多相同的命令，因此您可能不需要诊断 CLI 的额外命令。

当您进入诊断 CLI 时，您将处于与常规 threat defense CLI 不同的会话中。

提示符会更改为包括系统主机名。有两种模式，提示符指示您所处的模式。对于用户 EXEC 模式，提示符为：

```
hostname>
```

对于特权 EXEC 模式（也称为启用模式），提示符如下。使用 enable 命令进入此模式。虽然系统会提示您输入密码，但只需按 Enter 键即可，默认情况下无需密码即可进入此模式。

```
hostname#
```

使用诊断 CLI 时，请记住以下提示：

- 要退出诊断 CLI 并返回到常规 CLI，请按 Ctrl+a，然后按 d。
- 使用 **exit** 命令以退出特权 EXEC 模式。

  每种模式下可用的命令各不相同。特权 EXEC 模式包含的命令明显多于用户 EXEC 模式。使用 **?** 查看可用的命令。您可以在 ASA 软件命令参考中找到使用信息：

  - 思科 ASA 系列命令参考，A - H 命令，http://www.cisco.com/c/en/us/td/docs/security/asa/asa-command-reference/A-H/cmdref1.html
  - 思科 ASA 系列命令参考，I - R 命令，http://www.cisco.com/c/en/us/td/docs/security/asa/asa-command-reference/I-R/cmdref2.html
  - 思科 ASA 系列命令参考，S 命令，http://www.cisco.com/c/en/us/td/docs/security/asa/asa-command-reference/S/cmdref3.html
  - 思科 ASA 系列命令参考，ASASM 的 T-Z 命令和 IOS 命令，http://www.cisco.com/c/en/us/td/docs/security/asa/asa-command-reference/T-Z/cmdref4.html

- 诊断 CLI 可以包含对 threat defense无意义的命令。如果您尝试不提供有意义（或任何）信息的命令，则 threat defense可能未配置或不支持相关功能。

- 诊断 CLI 不允许您进入配置模式。您无法使用 CLI 配置设备。
- 当您从诊断 CLI 中分离时，下次进入时，您将处于与上次分离时相同的模式。
- 在 ASA 5506W-X 上，您可以使用 **session wlan** 命令打开与无线模块的连接，并使用其 CLI 配置无线接入点。必须在特权 EXEC 模式下。

示例

以下示例显示如何进入诊断 CLI 和特权 EXEC 模式。输入 **enable** 命令后出现密码提示时，只需按 Enter 键即可。默认情况下，没有进入特权 EXEC 模式的密码。

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
firepower> enable
Password: <press enter, do not enter a password>
firepower#
```

system support ssl-hw- commands

这些命令允许您对版本 6.2.3 和 6.3 中称为 *TLS/SSL* 硬件加速，以及版本 6.4 中称为 *TLS* 加密加速 的功能执行各种操作。可用的关键字取决于 threat defense 软件版本。

支持的设备以及默认情况下是启用还是禁用功能还取决于软件版本。有关详细信息，请参阅 管理中心 配置指南。

版本 6.2.3 和 6.3 的语法：

system support {**ssl-hw-status** | **ssl-hw-supported-ciphers** | **ssl-hw-offload enable** | **ssl-hw-offload disable**}

版本 6.4 的语法：

system support ssl-hw-supported-ciphers

Syntax Description

ssl-hw-status	显示 SSL 硬件加速的当前状态。默认状态为： • 6.2.3：禁用 • 6.3 和 6.4：已启用
ssl-hw-supported-ciphers	显示 SSL 硬件加速支持的密码列表。此命令非常有用，因为 SSL 硬件加速不支持 SSL 软件加速支持的所有密码（特别是不支持解密 SEED 和 Camellia 密码）。
ssl-hw-offload enable	启用 SSL 硬件加速；系统将提示您重新启动设备。
ssl-hw-offload disable	禁用 SSL 硬件加速；系统将提示您重新启动设备。

Command History

版本	修改
6.4	功能名称由 TLS/SSL 硬件加速 更改为 TLS 加密加速。 已删除以下关键字： **ssl-hw-offload enable** **ssl-hw-offload disable** **ssl-hw-status**
6.3	默认情况下启用此功能。
6.2.3	引入了此命令。默认情况下会禁用此功能。

使用指南

注释 在本节讨论的命令中， **system support ssl-hw-offload-supported ciphers** 仅适用于版本 6.4。

使用这些命令可显示有关 SSL 硬件加速 的信息，或者启用或禁用该功能。

启用 SSL 硬件加速以提高加密和解密性能。

禁用 SSL 硬件加速以使用其不支持的任何功能，或者在启用 SSL 策略的情况下遇到意外流量中断。

SSL 硬件加速不支持的功能包括：

- 启用了 威胁防御 容器实例 的托管设备。
- 如果检测引擎配置为保留连接，并且检测引擎意外出现故障，则 TLS/SSL流量将被丢弃，直到引擎重启。

  此行为受 **configure snort preserve-connection {enable | disable}** 命令控制。

使用 **system support ssl-hw-status** 命令显示当前状态。

使用 **system support ssl-hw-supported-ciphers** 命令显示 SSL 硬件加速支持的密码列表。

示例

以下是查看 SSL 硬件加速的当前状态的示例：

```
> system support ssl-hw-status
Hardware Offload configuration set to Disabled
```

以下是启用 SSL 硬件加速并提示重启设备的示例：

```
If you enable SSL hardware acceleration, you cannot:
    1.    Decrypt passive or inline tap traffic.
    2.    Preserve Do Not Decrypt connections when the inspection engine restarts.
Continue? (y/n) [n]: y


Enabling or disabling SSL hardware acceleration reboots the system. Continue? (y/n) [n]: y

SSL hardware acceleration will be enabled on system boot.
```

在重新启动设备之前，您需要确认所有上述内容。

以下是 SSL 硬件加速支持的部分密码列表：

```
> system support ssl-hw-supported-ciphers
CID     Cipher Suite Name                                CH_mod Keep     Support Inline
Support Passive
-------------------------------------------------------------------------------------------------
0x0004  TLS_RSA_WITH_RC4_128_MD5                         Yes             Yes             Yes
0x0005  TLS_RSA_WITH_RC4_128_SHA                         Yes             Yes             Yes
0x0009  TLS_RSA_WITH_DES_CBC_SHA                         Yes             Yes             Yes
```

```
0x000a  TLS_RSA_WITH_3DES_EDE_CBC_SHA                Yes             Yes             Yes
0x000c  TLS_DH_DSS_WITH_DES_CBC_SHA                  No              No              No
0x000d  TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA             No              No              No
0x000f  TLS_DH_RSA_WITH_DES_CBC_SHA                  No              No              No
0x0010  TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA             No              No              No
0x0012  TLS_DHE_DSS_WITH_DES_CBC_SHA                 No              No              No
0x0013  TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA            No              No              No
0x0015  TLS_DHE_RSA_WITH_DES_CBC_SHA                 Yes             Yes             No
0x0016  TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA            Yes             Yes             No
0x0018  TLS_DH_Anon_WITH_RC4_128_MD5                 No              Yes             No
0x001a  TLS_DH_Anon_WITH_DES_CBC_SHA                 No              Yes             No
0x001b  TLS_DH_Anon_WITH_3DES_EDE_CBC_SHA            No              Yes             No
0x001e  TLS_KRB5_WITH_DES_CBC_SHA                    No              No              No
0x001f  TLS_KRB5_WITH_3DES_EDE_CBC_SHA               No              No              No
0x0020  TLS_KRB5_WITH_RC4_128_SHA                    No              No              No
0x0024  TLS_KRB5_WITH_RC4_128_MD5                    No              No              No
0x002f  TLS_RSA_WITH_AES_128_CBC_SHA                 Yes             Yes             Yes
0x0030  TLS_DH_DSS_WITH_AES_128_CBC_SHA              No              No              No
0x0031  TLS_DH_RSA_WITH_AES_128_CBC_SHA              No              No              No
⋯ more
```

system support view-files

要在与思科技术支持中心 (TAC) 合作解决问题时查看系统日志内容，请使用 **system support view-files** 命令。

system support view-files

Command History

版本	修改
6.1	引入了此命令。

使用指南

system support view-files 命令可打开系统日志。请在配合思科技术支持中心 (TAC) 解决问题时使用此命令，以便他们帮助您解释输出内容并选择要查看的相应日志。

该命令将显示一个菜单供您选择日志。请使用以下命令在向导中导航：

- 要更改为子目录，请键入该目录的名称并按 Enter 键。
- 要选择欲查看的文件，请在提示符后输入 **s**。然后系统将提示您输入文件名。请键入完整名称，并注意区分大小写。文件列表会显示日志的大小，您最好考虑一下再打开非常大的日志。
- 看到 --More-- 时，按空格键可查看下一页日志条目；按 Enter 键仅查看下一个日志条目。到达日志末尾后，即会转到主菜单。--More-- 行会显示日志的大小和已查看部分的大小。**如果不想翻阅完整个日志，请使用 Ctrl+C 关闭日志并退出命令**。
- 键入 **b** 返回菜单结构的上一级。

如果要保持日志打开以便及时看到添加的新消息，请使用 **tail-logs** 命令而非 。

示例

以下示例显示如何查看 ngfw.log 文件。文件列表首先在顶部列出目录，然后列出当前目录下的文件。

```
> system support view-files

===View Logs===

============================
Directory: /ngfw/var/log
----------sub-dirs----------
cisco
mojo
removed_packages
setup
connector
sf
scripts
packages
removed_scripts
httpd
-----------files------------
```

```
2016-10-14 18:12:04.514783 | 5371       | SMART_STATUS_sda.log
2016-10-14 18:12:04.524783 | 353        | SMART_STATUS_sdb.log
2016-10-11 21:32:23.848733 | 326517     | action_queue.log
2016-10-06 16:00:56.620019 | 1018       | br1.down.log

<list abbreviated>

2016-10-06 15:38:22.630001 | 9194       | ngfw.log

<list abbreviated>

([b] to go back or [s] to select a file to view, [Ctrl+C] to exit)
Type a sub-dir name to list its contents: s

Type the name of the file to view ([b] to go back, [Ctrl+C] to exit)
> ngfw.log
2016-10-06 15:38:03 Starting Cisco Firepower Threat Defense ...
2016-10-06 15:38:03 Found USB flash drive /dev/sdb
2016-10-06 15:38:03 Found hard drive(s):  /dev/sda

<remaining log truncated>
```

Related Commands

命令	Description
tail-logs	打开日志并保持打开状态。

第 III 部分

T - Z 命令

t - z

tail-logs

要打开系统日志以查看在与思科技术支持中心 (TAC) 合作解决问题时编写的消息，请使用 **tail-logs** 命令。

tail-logs

Command History

版本	修改
6.1	引入了此命令。

使用指南

tail-logs 命令会打开系统日志，以便您可以查看写入的消息。请在配合思科技术支持中心 (TAC) 解决问题时使用此命令，以便他们帮助您解释输出内容并选择要查看的相应日志。

命令会显示一个列出所有可用日志的菜单。按照命令提示符选择日志。如果日志很长，您将看到 More 行；按 Enter 键一次前进一行，按 Space 键一次进入一页。查看完日志后，按 Ctrl+C 返回命令提示符。

示例

以下示例显示了如何跟踪 ngfw.log 文件。文件列表首先在顶部列出目录，然后列出当前目录下的文件。

```
> tail-logs
===Tail Logs===
============================
Directory: /ngfw/var/log
----------sub-dirs----------
cisco
mojo
removed_packages
setup
connector
sf
scripts
packages
removed_scripts
httpd
-----------files------------
2016-10-14 18:12:04.514783 | 5371       | SMART_STATUS_sda.log
2016-10-14 18:12:04.524783 | 353        | SMART_STATUS_sdb.log
2016-10-11 21:32:23.848733 | 326517     | action_queue.log
2016-10-06 16:00:56.620019 | 1018       | br1.down.log

<list abbreviated>

2016-10-06 15:38:22.630001 | 9194       | ngfw.log

<list abbreviated>

([b] to go back or [s] to select a file to view, [Ctrl+C] to exit)
Type a sub-dir name to list its contents: s
```

```
Type the name of the file to view ([b] to go back, [Ctrl+C] to exit)
> ngfw.log
2016-10-06 15:38:22 Running [rm -rf /etc/logrotate-dmesg.conf /etc/logrotate.conf
/etc/logrotate.d
/etc/logrotate_ssp.conf /etc/logrotate_ssp.d] ... success
2016-10-06 15:38:22 Running [ln -sf /ngfw/etc/logrotate-size.conf /etc/] ... success
2016-10-06 15:38:22 Running [ln -sf /ngfw/etc/logrotate-size.d /etc/] ... success
2016-10-06 15:38:22 Running [ln -sf /ngfw/etc/logrotate.conf /etc/] ... success
2016-10-06 15:38:22 Running [ln -sf /ngfw/etc/logrotate.d /etc/] ... success
2016-10-06 15:38:22 Running [rm -f /usr/sbin/ntpd] ... success
```

Related Commands

命令	Description
system support view-files	打开日志文件。

test aaa-server

要检查设备是否能够使用特定 AAA 服务器验证或授权用户，请使用 **test aaa-server** 命令。

test aaa-server {**authentication** *groupname* [**host** *ip_address*] [**username** *username*] [**password** *password*] | **authorization** *groupname* [**host** *ip_address*] [**username** *username*}

Syntax Description

groupname	指定 AAA 服务器组或领域名称。
host *ip-address*	指定服务器 IP 地址。如果没有在命令中指定 IP 地址，系统将提示您输入地址。
password *password*	指定用户密码。如果没有在命令中指定密码，系统将提示您输入密码。
username *username*	指定用于测试 AAA 服务器设置的帐户的用户名。确保 AAA 服务器中存在该用户名；否则，测试将失败。如果没有在命令中指定用户名，系统将提示您输入用户名。

Command History

版本	修改
6.2.1	引入了此命令。

使用指南

此命令允许您验证系统是否可以使用特定AAA服务器对用户进行身份验证或授权。此命令可让您测试 AAA 服务器而无需尝试验证的实际用户。它还可帮助您隔离 AAA 故障是由于 AAA 服务器参数配置错误、AAA 服务器连接问题还是其他配置错误。

示例

以下是成功进行身份验证的示例：

```
> test aaa-server authentication svrgrp1 host 192.168.3.4 username bogus password mypassword
INFO: Attempting Authentication test to IP address <10.77.152.85> (timeout: 12 seconds)
INFO: Authentication Successful
```

以下是不成功的身份验证尝试：

```
> test aaa-server authentication svrgrp1
Server IP Address or name: 192.168.3.4
Username: bogus
Password: mypassword
INFO: Attempting Authentication test to IP address <192.168.3.4> (timeout: 10
          seconds)
ERROR: Authentication Rejected: Unspecified
```

Related Commands

命令	Description
aaa-server active **aaa-server fail**	重新激活标记为发生故障的 AAA 服务器或使活动 AAA 服务器失效。
clear aaa-server statistics	清除 AAA 服务器统计信息。
show aaa-server	显示 AAA 服务器统计信息。

traceroute

要确定通过数据接口将传送至其目标的路由数据包，请使用 **traceroute** 命令。要确定数据包经过管理IP地址时到达目的地的路由，请使用 **traceroute system** 命令。

traceroute *destination* [**source** {*source_ip* | *source-interface*}] [**numeric**] [**timeout** *timeout_value*] [**probe** *probe_num*] [**ttl** *min_ttl max_ttl*] [**port** *port_value*] [**use-icmp**]
traceroute system *destination*

Syntax Description

destination	要跟踪的主机的 IPv4 或 IPv6 地址或主机名。例如，10.100.10.10 或 www.example.com。必须配置 DNS 服务器才能解析主机名。 使用 **system** 关键字的跟踪使用为管理接口配置的 DNS 服务器。其他跟踪使用为数据接口配置的 DNS 服务器。如果没有为数据接口定义 DNS，请先使用 **nslookup** 命令确定主机的 IP 地址，然后使用 IP 地址而不是 FQDN。
numeric	指定只输出打印中间网关的 IP 地址。如果未指定此关键字，跟踪路由会尝试查找跟踪时到达的网关主机名。
port *port_value*	用户数据报协议 (UDP) 探测消息使用的目标端口。默认值为 33434。
probe *probe_num*	在每个 TTL 级别要发送的探测次数。默认计数为 3。
source {*source_ip* | *source_interface*}	指定 IP 地址或接口将用作跟踪数据包的源。此 IP 地址必须是其中一个数据接口的 IP 地址。在透明模式下，它必须是管理 IP 地址。如果指定接口名称，则使用接口的 IP 地址。
system	表示跟踪路由应通过管理接口，而不是数据接口。
timeout *timeout_value*	指定在连接超时前等待响应的时间（秒）。默认值为 3 秒。
ttl *min_ttl max_ttl*	指定探测中要使用的“生存时间”值范围。 • *min_ttl*-第一次探测的 TTL 值。默认值为 1，但也可以设置为更高的值来抑制已知跃点的显示。 • *max-ttl*-可以使用的最大 TTL 值。默认值为 30。此命令在跟踪路由数据包到达目标或达到该值时终止。
use-icmp	指定使用 ICMP 探测数据包而不是 UDP 探测数据包。

Command History

版本	修改
6.1	引入了此命令。

使用指南

traceroute 命令可打印发送的每个探测的结果。每行输出以递增顺序对应一个 TTL 值。以下是 **traceroute** 命令打印的输出符号：

输出符号	Description
*	在超时期限内未收到对探测的响应。
nn msec	各节点指定探测数的往返时间（以毫秒为单位）。
!N.	无法访问 ICMP 网络。
!H	无法访问 ICMP 主机。
!P	ICMP 协议不可达。
!A	管理性禁止 ICMP。
?	未知 ICMP 错误。

示例

以下示例展示指定了目标 IP 地址时产生的跟踪路由输出：

```
> traceroute 209.165.200.225
Tracing the route to 209.165.200.225
 1  10.83.194.1 0 msec 10 msec 0 msec
 2  10.83.193.65 0 msec 0 msec 0 msec
 3  10.88.193.101 0 msec 10 msec 0 msec
 4  10.88.193.97 0 msec 0 msec 10 msec
 5  10.88.239.9 0 msec 10 msec 0 msec
 6  10.88.238.65 10 msec 10 msec 0 msec
 7 172.16.7.221 70 msec 70 msec 80 msec
 8 209.165.200.225 70 msec 70 msec 70 msec
```

以下示例显示了通过管理接口到主机名的跟踪路由。

```
> traceroute system www.example.com
traceroute to www.example.com (172.163.4.161), 30 hops max, 60 byte packets
 1  192.168.0.254 (192.168.0.254)  0.213 ms  0.310 ms  0.328 ms
 2  10.88.127.1 (10.88.127.1)  0.677 ms  0.739 ms  0.899 ms
 3  lab-gw1.example.com (10.89.128.25)  0.638 ms  0.856 ms  0.864 ms
 4  04-bb-gw1.example.com (10.152.240.65)  1.169 ms  1.355 ms  1.409 ms
 5  wan-gw1.example.com (10.152.240.33)  0.712 ms  0.722 ms  0.790 ms
 6  wag-gw1.example.com (10.152.240.73)  13.868 ms  10.760 ms  11.187 ms
 7  rbb-gw2.example.com (172.30.4.85)  7.202 ms  7.301 ms  7.101 ms
 8  rbb-gw1.example.com (172.30.4.77)  8.162 ms  8.225 ms  8.373 ms
 9  sbb-gw1.example.com (172.16.16.210)  7.396 ms  7.548 ms  7.653 ms
10  corp-gw2.example.com (172.16.16.58)  7.413 ms  7.310 ms  7.431 ms
11  dmzbb-gw2.example.com (172.16.0.78)  7.835 ms  7.705 ms  7.702 ms
12  dmzdcc-gw2.example.com (172.16.0.190)  8.126 ms  8.193 ms  11.559 ms
13  dcz05n-gw1.example.com (172.16.2.106)  11.729 ms  11.728 ms  11.939 ms
14  www1.example.com (172.16.4.161)  11.645 ms  7.958 ms  7.936 ms
```

Related Commands

命令	Description
capture	捕获数据包信息，包括跟踪数据包。

命令	Description
show capture	在未指定选项时显示捕获配置。
packet-tracer	启用数据包跟踪功能。

undebug

要禁用给定功能调试，请使用 **undebug** 命令。此命令与 **no debug** 命令的效果相同。

undebug {*feature* [*subfeature*] [*level*] | **all**}

Syntax Description

all	禁用所有功能调试。
feature	指定要为其禁用调试的功能。若要查看可用功能，请使用 **undebug ?** 命令获取 CLI 帮助。
subfeature	（可选）根据功能，您可以为一项或多项子功能禁用调试消息。使用 ? 查看可用的子功能。
level	（可选）指定调试级别。级别可能并非对所有功能都适用。使用 ? 可查看可用的级别。

Command History

版本	修改
6.1	引入了此命令。

使用指南

由于调试输出在CPU进程中享有高优先级，因此可导致系统不可用。为此，应仅在对特定问题进行故障排除或与思科 Technical Assistance Center (TAC) 进行故障排除会话时使用 **debug** 命令。此外，最好在网络流量较低和用户较少时使用 **debug** 命令。在这些时段进行调试会减少因 **debug** 命令处理开销增加而影响系统使用的可能性。

您只能在 CLI 会话中查看调试输出。在连接到控制台端口的情况下，或者在诊断 CLI 中，您可以直接查看输出结果（输入 **system support diagnostic-cli**）。此外，您也可以使用 **show console-output** 命令在常规 threat defense CLI 中查看输出。

示例

以下示例禁用所有已启用调试的调试。

```
> undebug all
>
```

Related Commands

命令	Description
debug	启用功能调试。
show debug	显示当前活动的调试设置。

upgrade

要重试、取消或恢复系统软件升级，请使用 **upgrade** 命令。

upgrade { **cancel** | **cleanup-revert** | **revert** | **retry** }

Syntax Description

cancel	取消主要升级的安装。如果升级失败，但系统认为升级仍在进行中，则必须取消升级，才能将作业状态更改为可以重试升级的状态。在大多数情况下，系统应该能够自动取消失败的升级。
cleanup-revert	永久删除以前的版本以释放磁盘空间。如果清理可恢复版本，则无法使用 **revert** 关键字返回到该可恢复版本。
revert	如果有可恢复的版本，则通过返回到上一个版本来撤消系统软件升级。首先使用 **show upgrade revert-info** 命令验证是否存在可恢复版本，以及它是哪个版本。如果该版本可接受，则可以使用此命令恢复为该版本。 在高可用性/可扩展性 部署中，当所有设备同时恢复时，恢复更成功。使用CLI恢复时，打开所有设备的会话，验证每个设备是否可以恢复，然后同时启动进程。 恢复后，必须向智能软件管理器重新注册设备。 在版本 6.7 至 7.1 中， **upgrade revert** 仅可用于本地管理的系统。您不能在 管理中心管理的系统上使用此命令。 在版本 7.2+ 中， 如果 管理中心和设备之间的通信中断，则在 管理中心 部署中支持此命令。 注意 从 CLI 恢复可能会导致设备和管理中心之间的配置不同步，具体取决于您在升级后所做的更改。这可能会导致进一步的通信和部署问题。
retry	重试未能完成的主要升级。升级必须被系统视为失败，而不是正在进行。您可能需要输入 **upgrade cancel** ，然后才能重试升级。

Command History

版本	修改
6.7	引入了此命令。
7.0	**upgrade revert** 命令现在会自动从智能软件管理器注销设备。恢复升级后，必须重新注册设备。
7.2	如果管理中心和设备之间的通信中断， 管理中心 部署中现在支持 **upgrade revert** 命令。

示例

以下示例显示如何取消正在进行的系统软件更新。升级取消成功完成后，设备将自动重启。

```
> upgrade cancel
Warning: Upgrade in progress (11%,  8 mins remaining).
Are you sure you want to cancel it(yes/no)? yes
```

以下示例显示如何重试失败的升级。您需要先更正导致升级失败的问题，如失败消息所示。您可能需要使用 **upgrade cancel**，然后才能重试升级。并非所有失败的升级都可以重试。

```
> upgrade retry
Tue Dec  3 23:50:31 UTC 2020: Resuming upgrade for
Cisco_FTD_Upgrade-6.7.0-32.sh.REL.tar
```

以下示例显示如何在本地管理的系统上恢复到以前的版本。使用 **show upgrade revert-info** 命令确定是否有可用于恢复的版本。

```
> upgrade revert
Current version is 6.7.0.50
Detected previous version 6.6.1.20
Are you sure you want to revert (Yes/No)? Yes
```

以下示例显示如何删除以前的版本以清理磁盘空间。使用此命令后，您将无法恢复到以前的版本。

```
> upgrade cleanup-revert
Version 6.6 was cleaned up successfully.
```

Related Commands

命令	Description
show last-upgrade status	显示有关上次系统软件升级的信息。
show upgrade	显示有关当前系统软件升级的信息。

verify

要检验文件的校验和，请使用 **verify** 命令。

verify ［**sha-512** | **/signature**］ *path*
verify/md5 *path* ［*md5-value*］

Syntax Description

/md5	（可选）计算并显示指定软件映像的 MD5 值。将此值与 Cisco.com 上此映像的可用值进行比较。
sha-512	（可选）计算并显示指定软件映像的 SHA-512 值。将此值与 Cisco.com 上此映像的可用值进行比较。
/signature	（可选）验证存储在闪存中的映像的签名。
md5-value	（可选）指定映像的已知 MD5 值。在此命令中指定 MD5 值后，系统将计算指定映像的 MD5 值并显示一条验证 MD5 值匹配或不匹配的消息。

path	• *filename* 当前目录中的文件的名称。使用 **dir** 查看目录内容， **cd** 以更改目录。 • **disk0:**/[*path*/]*filename* 此选项表示内部闪存。您还可以使用 **flash:** 代替 **disk0**；它们是别名。 • **disk1:**/[*path*/]*filename* 此选项表示外部闪存卡。 • **flash:**/[*path*/]*filename* 此选项表示内部闪存卡。对于 ASA 5500 系列， **flash** 是 **disk0:** 的别名。 • **ftp:**//[*user*[**:***password*]**@**]*server*[: *port*]/[*path*/]*filename*[**;type=***xx*] **type** 可以是以下关键字之一： • **ap**- ASCII 被动模式 • **an**- ASCII 正常模式 • **ip**-（默认）二进制被动模式 • **in**- 二进制正常模式 • **http**[**s**]**:**//[*user*[:*password*] **@**]*server*[: *port*]/[*path*/]*filename* • **tftp:**//[*user*[:*password*]@]*server*[: *port*]/[*path*/]*filename*[**;int=***interface_name*] 如果要覆盖到服务器地址的路由，请指定接口名称。路径名不能包含空格。

Command Default

当前的闪存设备是默认文件系统。

注释 在指定 **/md5** 选项时，可使用网络文件（如 FTP、HTTP 和 TFTP）作为源。不带 **verify** 选项的 **/md5** 命令仅允许验证闪存中的本地映像。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用 **verify** 命令验证文件的校验和，然后再使用文件。

分布在磁盘上的每个软件映像对整个映像使用单个校验和。当映像复制到闪存中时才显示此校验和；当映像文件从一个磁盘复制到另一个磁盘时，不会显示。

在加载或复制新的映像之前，记录映像的校验和与MD5信息，以便当您将映像复制到闪存中或服务器上时可验证校验和。Cisco.com 上提供多种映像信息。

要显示闪存的内容，请使用 **show flash:** 命令。闪存的内容列表不包含各个文件的校验和。要重新计算和验证映像复制到闪存后的校验和，请使用**verify**命令。但请注意，当文件保存到文件系统之后，**verify** 命令才检查其完整性。损坏的映像可能会传输到设备并保存在文件系统中，不进行检测。如果损坏的映像成功传输到设备，则软件无法识别映像已损坏，而文件将成功验证。

要使用消息摘要 5 (MD5) 散列算法确保文件验证，请使用带 **/md5** 选项的 **verify** 命令。MD5 是一种通过创建唯一的 128 位消息摘要来验证数据完整性的算法（在 RFC 1321 中定义）。 **verify** 命令的 **/md5** 选项通过将映像的MD5校验和值与该映像的已知MD5校验和值进行比较，检查安全设备软件映像的完整性。目前 Cisco.com 提供了所有安全设备软件映像的 MD5 值，以供与本地系统映像值进行比较。

要执行 MD5 完整性检查，请执行使用 **/md5** 关键字的 **verify** 命令。例如，执行 **verify /md5 flash:cdisk.bin** 命令将计算并显示软件映像的 MD5 值。将此值与 Cisco.com 上此映像的可用值进行比较。

或者，您可以先从 Cisco.com 获取 MD5 值，然后在命令语法中指定此值。例如，执行 **verify /md5 flash:cdisk.bin 8b5f3062c4cacdbae72571440e962233** 命令将显示验证 MD5 值匹配或不匹配的消息。MD5 值不匹配表示映像已损坏或输入了错误的 MD5 值。

示例

以下示例验证映像文件。如果包含 **/signature** 关键字，则会看到相同的结果。

```
> verify os.img
Verifying file integrity of disk0:/os.img
Computed Hash   SHA2: 4916c9b70ad368feb02a0597fbef798e
                      ca360037fc0bb596c78e7ef916c6c398
                      e238e2597eab213d5c48161df3e6f4a7
                      66e4ec15a7b327ee26963b2fd6e2b347
Embedded Hash   SHA2: 4916c9b70ad368feb02a0597fbef798e
                      ca360037fc0bb596c78e7ef916c6c398
                      e238e2597eab213d5c48161df3e6f4a7
                      66e4ec15a7b327ee26963b2fd6e2b347
Digital signature successfully validated
```

以下示例计算映像的 MD5 值。为简洁起见，大多数感叹号已被删除。

```
> verify /md5 os.img
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!Done!
verify /MD5 (disk0:/os.img) = 0940c6c71d3d43b3ba495f7290f4f276
>
```

以下示例计算 MD5 值并将其与预期值进行比较。在这种情况下，决策为“已验证”，即计算值与预期值匹配。

```
> verify /md5 os.img 0940c6c71d3d43b3ba495f7290f4f276
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!Done!
```

```
Verified (disk0:/os.img) = 0940c6c71d3d43b3ba495f7290f4f276
>
```

以下示例计算映像的 SHA-512 值。

```
> verify /sha-512 os.img
!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!Done!
verify /SHA-512 (disk0:/os.img) = 77421c0f6498976fbe5300e62bd8b7e8140b52a851f055265080
a392299848a77227d6047827192f34d969d36944abf2bddd215ec4127f9503173f82a2d6c7e2
```

Related Commands

命令	Description
copy	复制文件。
dir	列出系统中的文件。

vpn-sessiondb logoff

要注销所有或选定的 VPN 会话，请使用 **vpn-sessiondb logoff** 命令。

vpn-sessiondb logoff {**all** | **index** *index_number* | **ipaddress** *IPaddr* | **l2l** | **name** *username* | **protocol** *protocol-name* | **tunnel-group** *groupname*} **noconfirm**

Syntax Description

all	注销所有 VPN 会话。
index *index_number*	按索引编号注销单个会话。您可以使用 **show vpn-sessiondb detail** 命令查看每个会话的索引编号。
ipaddress *IPaddr*	注销您指定的 IP 地址的会话。
l2l	注销所有 LAN 到 LAN 会话。
name *username*	注销您指定的用户名的会话。
protocol *protocol-name*	注销您指定的协议的会话。这些协议包括： • **ikev1**-互联网密钥交换第 1 版 (IKEv1) 会话。 • **ikev2**-互联网密钥交换第 2 版 (IKEv2) 会话。 • **ipsec**-使用 IKEv1 或 IKEv2 的 IPsec 会话。 • **ipseclan2lan**—IPsec LAN-to-LAN 会话。 • **ipseclan2lanovernatt**—IPsec LAN-to-LAN-over NAT-T 会话。
tunnel-group *groupname*	注销您指定的隧道组（连接配置文件）会话。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例显示如何注销企业隧道组（连接配置文件）的会话。

```
> vpn-sessiondb logoff tunnel-group Corporate noconfirm
INFO: Number of sessions from TunnelGroup "Corporate" logged off : 1
```

write net

要将运行配置保存到 TFTP 服务器，请使用 **write net** 命令。

write net ［**interface** *if_name*］ *server***:**［*filename*］

Syntax Description

:*filename*	指定路径和文件名。
interface *if_name*	可以通过其访问服务器的接口的名称。
*server***:**	设置 TFTP 服务器的 IP 地址或名称。

Command History

版本	修改
6.1	引入了此命令。

使用指南

运行配置是内存中当前运行配置。

示例

以下示例通过内部接口将运行配置复制到 TFTP 服务器。

```
> write net interface inside 10.1.1.1:/configs/contextbackup.cfg
```

Related Commands

命令	Description
show running-config	显示运行配置。

write terminal

要在终端上显示运行配置，请使用 **write terminal** 命令。

write terminal

Command History

版本	修改
6.1	引入了此命令。

使用指南

此命令与 **show running-config** 命令等效：

示例

以下示例将运行配置写入终端：

```
> write terminal
: Saved
:
: Serial Number: XXXXXXXXXXX
: Hardware:   ASA5516, 8192 MB RAM, CPU Atom C2000 series 2416 MHz, 1 CPU (8 cores)
:
NGFW Version 6.2.0
!
hostname firepower
(...remaining output deleted...)
```

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。