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。

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。