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 *1:* 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 *2:* 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 *3: 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 *4:* 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 *5:* 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 *6:* 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 7: 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 *8:* 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
```

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。