



show d - show h

- [show database](#) , 第 3 页
- [show ddns update](#) , 第 4 页
- [show debug](#) , 第 6 页
- [show debug](#) , 第 7 页
- [show dhcpd](#) , 第 8 页
- [show dhcprelay](#) , 第 10 页
- [show diameter](#) , 第 11 页
- [show disk](#) , 第 12 页
- [show disk-manager](#) , 第 14 页
- [show dns](#) , 第 15 页
- [show dns-hosts](#) , 第 17 页
- [show eigrp events](#) , 第 19 页
- [show eigrp interfaces](#) , 第 21 页
- [show eigrp neighbors](#) , 第 23 页
- [show eigrp topology](#) , 第 27 页
- [show eigrp traffic](#) , 第 30 页
- [show environment](#) , 第 32 页
- [show facility-alarm](#) , 第 36 页
- [show failover](#) , 第 38 页
- [show failover exec](#) , 第 51 页
- [show file](#) , 第 52 页
- [show firewall](#) , 第 53 页
- [show flash](#) , 第 54 页
- [show flow-export counters](#) , 第 55 页
- [show flow-offload](#) , 第 56 页
- [show flow-offload-ipsec](#) , 第 59 页
- [show fqdn](#) , 第 61 页
- [show fragment](#) , 第 63 页
- [show gc](#) , 第 65 页
- [show h225](#) , 第 66 页

- [show h245](#) , 第 67 页
- [show h323](#) , 第 68 页
- [show hardware-bypass](#) , 第 69 页
- [show high-availability config](#) , 第 70 页
- [show https-access-list](#) , 第 72 页

show database

要显示有关系统数据库的信息，请使用 **show database** 命令。

show database { **processes** | **slow-query-log** }

Syntax Description	processes	显示有关当前正在运行的数据库查询的信息。
	slow-query-log	显示数据库的慢查询日志。
Command History	版本	修改
	6.1	引入了此命令。

示例

以下示例显示如何显示数据库进程信息。

```
> show database processes
Database Processes:
  Id : 3
  User : barnyard
  Host : localhost
  Database : sfsnort
  Command : Sleep
  Time : 6
  State : Null
  Info : Null
-----
(...Remaining output truncated...)
```

show ddns update

要显示有关 DDNS 更新方法的信息，请使用 **show ddns update interface** 命令。

```
show ddns update { interface [interface-name] | method [method-name] }
```

Syntax Description	interface [interface-name]	method [method-name]
	显示分配给 threat defense 接口的方法。您可以选择指定接口名称，以仅查看有关该接口的信息。	显示有关 DDNS 更新方法的信息。您可以选择输入方法的名称，以仅查看有关该方法的信息。
Command History	版本	修改
	6.1	引入了此命令。
	6.7	对于 Web 更新方法， interface 关键字的输出包括上次成功更新的 FQDN/IP 地址映射。对于 method 关键字，添加了 Web 更新方法的输出。

示例

以下示例展示分配给内部接口的 DDNS 方法：

```
> show ddns update interface inside
Dynamic DNS Update on inside:
  Update Method Name      Update Destination
  ddns-2                  not available
>
```

以下示例显示 Web 类型更新成功：

```
> show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name      Update Destination
  test                    not available

Last Update attempted on 09:01:52.729 UTC Mon Mar 23 2020
Status : Success
FQDN : ftdl.example.com
IP addresses(s): 10.10.32.45,2001:DB8::1
```

以下示例显示 Web 类型故障：

```
> show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name      Update Destination
  test                    not available
```

```
Last Update attempted on 09:01:52.729 UTC Mon Mar 23 2020
Status : Failed
Reason : Could not establish a connection to the server
```

以下示例显示 DNS 服务器返回 Web 类型更新错误:

```
> show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name      Update Destination
  test                    not available

Last Update attempted on 09:01:52.729 UTC Mon Mar 23 2020
Status : Failed
Reason : Server error (Error response from server)
```

以下示例显示, 由于 IP 地址未配置或 DHCP 请求失败, 尚未尝试 Web 更新, 例如:

```
> show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name      Update Destination
  test                    not available

Last Update Not attempted
```

以下示例展示名为 ddns-2 的 DDNS 方法:

```
> show ddns update method ddns-2
Dynamic DNS Update Method: ddns-2
  IETF standardized Dynamic DNS 'A' and 'PTR' records update
  Maximum update interval: 0 days 0 hours 10 minutes 0 seconds
>
```

以下示例显示有关 Web 更新方法的详细信息:

```
> show ddns update method web1

Dynamic DNS Update Method: web1
Dynamic DNS updated via HTTP(s) protocols
URL used to update record: https://cdarwin:*****@ddns.cisco.com/update?hostname=<h>&myip=<a>
```

Related Commands

命令	Description
show running-config ddns	显示运行的配置中所有配置 DDNS 方法的类型和间隔。

show debug

要显示当前调试配置，请使用 **show debug** 命令。

show debug [命令 [关键词]]

Syntax Description	command	(可选) 指定要查看其当前配置的 debug 命令。
	关键词	(可选) 对于每个命令，命令后跟的关键词与关联 debug 命令支持的关键词完全相同。
Command History	版本	修改
	6.1	引入了此命令。

使用指南

对于每个命令，命令后跟的关键词与关联 **debug** 命令支持的关键词完全相同。有关支持的语法的信息，请输入 ? 在关键字位置。

例如：

- **show debug ?** 列出可用的命令。
- **show debug tcp ?** 列出可用于 TCP 调试的关键字。

示例

以下示例启用 TCP 调试，然后显示调试状态。

```
> debug tcp
debug tcp enabled at level 1
> show debug tcp
debug tcp enabled at level 1
debug tcp enabled at level 1 (persistent)
```

Related Commands	命令	Description
	debug	启用调试。

show debug

要显示当前调试配置，请使用 **show debug** 命令。

show debug [命令 [关键词]]

Syntax Description	command	(可选) 指定要查看其当前配置的 debug 命令。
	关键词	(可选) 对于每个命令，命令后跟的关键词与关联 debug 命令支持的关键词完全相同。
Command History	版本	修改
	6.1	引入了此命令。

使用指南

对于每个命令，命令后跟的关键词与关联 **debug** 命令支持的关键词完全相同。有关支持的语法的信息，请输入 ? 在关键字位置。

例如：

- **show debug ?** 列出可用的命令。
- **show debug tcp ?** 列出可用于 TCP 调试的关键字。

示例

以下示例启用 TCP 调试，然后显示调试状态。

```
> debug tcp
debug tcp enabled at level 1
> show debug tcp
debug tcp enabled at level 1
debug tcp enabled at level 1 (persistent)
```

Related Commands	命令	Description
	debug	启用调试。

show dhcpd

要查看 DHCP 绑定、状态和统计信息，请使用 **show dhcpd** 命令。

```
show dhcpd {binding [IP_address] | state | statistics}
```

Syntax Description	binding	显示指定服务器 IP 地址的绑定信息及其关联客户端硬件地址和租用时长。
	<i>IP_address</i>	显示指定 IP 地址的绑定信息。
	state	显示 DHCP 服务器的状态，例如在当前情景下是否已启用以及在每个接口上是否已启用。
	statistics	显示统计信息，例如地址池、绑定、过期绑定、格式不正确的消息、已发送消息和已接收消息的数量。
Command History	版本	修改
	6.1	引入了此命令。

使用指南

如果您在 **show dhcpd binding** 命令中包含了可选的 IP 地址，则仅显示该 IP 地址的绑定。

示例

以下是 **show dhcpd binding** 命令的输出示例：

```
> show dhcpd binding
IP Address Client-id Lease Expiration Type
10.0.1.100 0100.a0c9.868e.43 84985 seconds automatic
```

以下是 **show dhcpd state** 命令的输出示例。在本例中，外部接口是 DHCP 客户端，而许多其他接口充当 DHCP 服务器。

```
> show dhcpd state
Context Configured as DHCP Server
Interface outside, Configured for DHCP CLIENT
Interface inside1_2, Configured for DHCP SERVER
Interface inside1_3, Configured for DHCP SERVER
Interface inside1_4, Configured for DHCP SERVER
Interface inside1_5, Configured for DHCP SERVER
Interface inside1_6, Configured for DHCP SERVER
Interface inside1_7, Configured for DHCP SERVER
Interface inside1_8, Not Configured for DHCP
Interface diagnostic, Not Configured for DHCP
Interface inside, Configured for DHCP SERVER
```

以下是 **show dhcpd statistics** 命令的输出示例：

> show dhcpd statistics

DHCP UDP Unreachable Errors: 0
 DHCP Other UDP Errors: 0

```

Address pools          1
Automatic bindings    1
Expired bindings      1
Malformed messages    0

Message                Received
BOOTREQUEST           0
DHCPDISCOVER          1
DHCPCREQUEST          2
DHCPCDECLINE          0
DHCPCRELEASE          0
DHCPCINFORM           0

Message                Sent
BOOTREPLY              0
DHCPOFFER             1
DHCPCACK              1
DHCPCNAK              1
  
```

Related Commands

命令	Description
clear dhcpd	清除 DHCP 服务器绑定和统计计数器。
show running-config dhcpd	显示当前 DHCP 服务器配置。

show dhcprelay

要查看 DHCP 中继代理状态和统计信息，请使用 **show dhcprelay state** 命令。

show dhcprelay {state | statistics}

Syntax Description	state	显示每个接口的 DHCP 中继代理的状态。
	statistics	显示 DHCP 中继统计信息。
Command History	版本	修改
	6.1	引入了此命令。

示例

以下是 **show dhcprelay state** 命令的输出示例：

```
> show dhcprelay state

Context Configured as DHCP Relay
Interface outside, Not Configured for DHCP
Interface infrastructure, Configured for DHCP RELAY SERVER
Interface inside, Configured for DHCP RELAY
```

以下显示 **show dhcprelay statistics** 命令的输出示例。

```
> show dhcprelay statistics

DHCP UDP Unreachable Errors: 0
DHCP Other UDP Errors: 0

Packets Relayed
BOOTREQUEST          0
DHCPCDISCOVER        7
DHCPREQUEST          3
DHCPDECLINE          0
DHCPRELEASE          0
DHCPINFORM           0

BOOTREPLY            0
DHCPPOFFER           7
DHCPACK              3
DHCPNAK              0
```

Related Commands	命令	Description
	clear dhcprelay statistics	清除 DHCP 中继代理统计计数器。
	show dhcpd	显示 DHCP 服务器统计信息和状态信息。

show diameter

要显示每个 Diameter 连接的状态信息，请使用 **show diameter** 命令。

show diameter

Command History

版本	修改
6.2	引入了此命令。

使用指南

要显示 Diameter 连接状态信息，必须检查 Diameter 流量。要检查 Diameter 流量，您需要在管理中心配置 FlexConfig。

示例

以下显示 **show diameter** 命令的输出示例。

```
> show diameter
Total active diameter sessions: 5
Session 3638
=====
ref_count: 1 val = .; 1096298391; 2461;
  Protocol : diameter Context id : 0
  From inside:211.1.1.10/45169 to outside:212.1.1.10/3868
...
```

Related Commands

命令	Description
clear service-policy	清除服务策略统计信息。

show disk

要仅显示 threat defense 设备的闪存内容，请使用 **show disk** 命令。

show disk

show {**disk0:** | **disk1:**} [**filesystem** | **all** | **controller**]

Syntax Description	{disk0: disk1:}	指定内部闪存 (disk0:) 或外部闪存 (disk1:)。如果输入不带数字的 show disk 命令，则会看到有关文件系统的信息。
	all	显示闪存内容以及文件系统和控制器信息。
	controller	显示闪存控制器型号。
	filesystem	显示关于紧凑型闪存卡的信息。
Command Default		默认情况下，此命令显示文件系统信息。
Command History	版本	修改
	6.1	引入了此命令。

示例

以下示例显示有关文件系统的信息。

```
> show disk
Filesystem      Size  Used Avail Use% Mounted on
tmpfs           3.9G  440K  3.9G   1% /run
tmpfs           3.9G  168K  3.9G   1% /var/volatile
none            3.8G   9.4M  3.8G   1% /dev
/dev/sdb1       7.4G  104M  7.3G   2% /mnt/disk0
/dev/mapper/root 3.7G  943M  2.6G  27% /ngfw
/dev/mapper/var  81G   4.0G   73G   6% /home
tmpfs           3.9G   0    3.9G   0% /dev/cgroups
```

以下是 **show disk0:** 命令的输出示例：

```
> show disk0:
--#--  --length--  -----date/time-----  path
 48  107030784  Oct 05 2016 02:10:26  os.img
 49   33      Oct 11 2016 21:32:16  .boot_string
 50  150484    Oct 06 2016 15:36:02  install.log
 11  4096      Oct 06 2016 15:58:16  log
 13  1544     Oct 13 2016 18:59:06  log/asa-appagent.log
 16  4096     Oct 06 2016 15:59:07  crypto_archive
 51  4096     Oct 06 2016 15:59:12  coredumpinfo
 52  59       Oct 06 2016 15:59:12  coredumpinfo/coredump.cfg
 53  36       Oct 06 2016 16:04:47  enable_configure
 56  507281   Oct 20 2016 18:10:20  crashinfo-test_20161020_181021.UTC
```

```
7935832064 bytes total (7827599360 bytes free)
```

以下是 **show disk0: fileys** 命令的输出示例:

```
> show disk0: fileys
***** Flash Card Geometry/Format Info *****

COMPACT FLASH CARD GEOMETRY
Number of Heads:      245
Number of Cylinders  1022
Sectors per Cylinder   62
Sector Size          512
Total Sectors        15524180
```

以下是 **show disk0: controller** 命令的输出示例:

```
> show disk0: controller

Flash Model: ATA Micron_M500DC_MT
```

Related Commands

命令	Description
dir	系统随即会显示目录的内容。

show disk-manager

要显示系统每个部分（包括孤岛、低水位线和高水位线）的磁盘使用情况详细信息，请使用 **show disk-manager** 命令。

show disk-manager

Command History

版本	修改
6.1	引入了此命令。

示例

以下是磁盘管理器信息的示例。

```
> show disk-manager
Silo                               Used           Minimum       Maximum
Temporary Files                   0 KB           499.197 MB   1.950 GB
Action Queue Results               0 KB           499.197 MB   1.950 GB
User Identity Events               0 KB           499.197 MB   1.950 GB
UI Caches                           4 KB           1.462 GB     2.925 GB
Backups                             0 KB           3.900 GB     9.750 GB
Updates                             0 KB           5.850 GB     14.625 GB
Other Detection Engine             0 KB           2.925 GB     5.850 GB
Performance Statistics             33 KB          998.395 MB   11.700 GB
Other Events                       0 KB           1.950 GB     3.900 GB
IP Reputation & URL Filtering       0 KB           2.437 GB     4.875 GB
Archives & Cores & File Logs       0 KB           3.900 GB     19.500 GB
Unified Low Priority Events         1.329 MB       4.875 GB     24.375 GB
RNA Events                         0 KB           3.900 GB     15.600 GB
File Capture                       0 KB           9.750 GB     19.500 GB
Unified High Priority Events       0 KB           14.625 GB    34.125 GB
IPS Events                         0 KB           11.700 GB    29.250 GB
```

show dns

要显示完全限定域名 (FQDN) 网络对象的当前已解析 DNS 地址或管理接口上的 DNS 服务器配置，请使用 **show dns** 命令。

show dns [**host** *fqdn* | **system**]

Syntax Description

host *fqdn* 仅显示有关指定的完全限定域名 (FQDN) 的信息。

system 显示为管理接口配置的 DNS 服务器和搜索域。

Command Default

如果不包括 **system** 关键字，该命令将显示访问控制规则中使用的所有 FQDN 网络对象的 DNS 解析。

Command History

版本	修改
6.1	引入了此命令。
6.3	添加了对基于 FQDN 的访问控制规则的支持。

示例

以下示例显示管理地址的 DNS 配置。

```
> show dns system
search example.com
nameserver 72.163.47.11
```

以下示例显示访问控制规则中使用的 FQDN 网络对象的 DNS 解析。仅当在规则中使用 FQDN 对象时才会对其进行解析：仅定义对象不会启动名称的 DNS 查找。

```
> show dns
Name: www.example1.com
  Address: 10.1.3.1           TTL 00:03:01
  Address: 10.1.3.3           TTL 00:00:36
  Address: 10.4.1.2           TTL 00:01:01
Name: www.example2.com
  Address: 10.2.4.1           TTL 00:25:13
  Address: 10.5.2.1           TTL 00:25:01
Name: server.ddns-exampleuser.com
  Address: fe80::21e:8cff:feb5:4faa  TTL 00:00:41
  Address: 10.10.10.2         TTL 00:25:01
```

以下是 **show dns host** 命令的输出示例：

```
> show dns host www.example1.com
Name: www.example1.com
  Address: 10.1.3.1           TTL 00:03:01
  Address: 10.1.3.3           TTL 00:00:36
  Address: 10.4.1.2           TTL 00:01:01
```

Related Commands	命令	Description
	clear dns	删除 FQDN 网络对象 DNS 解析。
	show network	显示管理接口的配置。

show dns-hosts

要显示 DNS 缓存，请使用 **show dns-hosts** 命令。DNS 缓存包括从 DNS 服务器动态获知的条目以及手动输入的名称和 IP 地址。

show dns-hosts

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show dns-hosts** 命令的输出示例：

```
> show dns-hosts
Host                Flags      Age Type  Address(es)
ns2.example.com    (temp, OK) 0   IP    10.102.255.44
ns1.example.com    (temp, OK) 0   IP    192.168.241.185
snowmass.example.com (temp, OK) 0   IP    10.94.146.101
server.example.com (temp, OK) 0   IP    10.94.146.80
```

下表对每个字段进行了说明。

表 1: *show dns-hosts* 字段

字段	Description
Host	显示主机名。
Flags	显示条目状态为以下各项的组合： <ul style="list-style-type: none"> • temp - 由于来自 DNS 服务器，此条目是临时的。设备会在 72 小时不活动后删除此条目。 • perm - 由于使用 name 命令添加，此条目是永久的。 • OK - 此条目有效。 • ?? - 此条目可疑并需要重新验证。 • EX - 此条目已过期。
Age	显示自此条目上次引用后经过的小时数。
Type	显示 DNS 记录的类型；该值始终为 IP。
Address(es)	IP 地址。

Related Commands

命令	Description
clear dns-hosts	清除 DNS 缓存。

show eigrp events

要显示 EIGRP 事件日志，请使用 **show eigrp events** 命令。

```
show eigrp [as-number] events [{start end} | type]
```

Syntax Description	<i>as_number</i>	(可选) 指定您查看事件日志的 EIGRP 流程的自主系统编号。由于 threat defense 设备仅支持一个 EIGRP 路由流程，因此，无需指定自主系统编号。
	<i>end</i>	(可选) 限制以 <i>start</i> 索引号开头并以 <i>end</i> 索引号结尾的条目的输出。
	<i>start</i>	(可选) 指定日志条目索引号的数字。指定起始编号将导致输出以指定的事件开头并以通过 <i>end</i> 参数指定的事件结尾。有效值范围为 1 至 500。
	<i>type</i>	(可选) 显示所记录的事件。
Command Default	如果没有指定 <i>start</i> 和 <i>end</i> ，则显示所有日志条目。	
Command History	版本	修改
	6.1	引入了此命令。

使用指南

show eigrp events 输出最多显示 500 个事件。达到最大事件数后，新事件将添加到输出底部，并且旧事件将从输出顶部删除。

您可以使用 **clear eigrp events** 命令清除 EIGRP 事件日志。

show eigrp events type 命令显示 EIGRP 事件的日志记录状态。默认情况下，将记录邻居变更、邻居警告和 DUAL FSM 消息。您无法禁用 DUAL FSM 事件的日志记录。

示例

以下是 **show eigrp events** 命令的输出示例：

```
> show eigrp events

Event information for AS 100:
1   12:11:23.500 Change queue emptied, entries: 4
2   12:11:23.500 Metric set: 10.1.0.0/16 53760
3   12:11:23.500 Update reason, delay: new if 4294967295
4   12:11:23.500 Update sent, RD: 10.1.0.0/16 4294967295
5   12:11:23.500 Update reason, delay: metric chg 4294967295
6   12:11:23.500 Update sent, RD: 10.1.0.0/16 4294967295
7   12:11:23.500 Route install: 10.1.0.0/16 10.130.60.248
8   12:11:23.500 Find FS: 10.1.0.0/16 4294967295
9   12:11:23.500 Rcv update met/succmet: 53760 28160
10  12:11:23.500 Rcv update dest/nh: 10.1.0.0/16 10.130.60.248
11  12:11:23.500 Metric set: 10.1.0.0/16 4294967295
```

以下是定义了起始和停止编号的 **show eigrp events** 命令的输出示例:

```
> show eigrp events 3 8
```

```
Event information for AS 100:
3   12:11:23.500 Update reason, delay: new if 4294967295
4   12:11:23.500 Update sent, RD: 10.1.0.0/16 4294967295
5   12:11:23.500 Update reason, delay: metric chg 4294967295
6   12:11:23.500 Update sent, RD: 10.1.0.0/16 4294967295
7   12:11:23.500 Route install: 10.1.0.0/16 10.130.60.248
8   12:11:23.500 Find FS: 10.1.0.0/16 4294967295
```

以下是 EIGRP 事件日志中没有条目时 **show eigrp events** 命令的输出示例:

```
> show eigrp events
```

```
Event information for AS 100: Event log is empty.
```

以下是 **show eigrp events type** 命令的输出示例:

```
> show eigrp events type
```

```
EIGRP-IPv4 Event Logging for AS 100:
  Log Size           500
  Neighbor Changes   Enable
  Neighbor Warnings  Enable
  Dual FSM           Enable
```

Related Commands

命令	Description
clear eigrp events	清除 EIGRP 事件日志记录缓冲区。

show eigrp interfaces

要显示参与 EIGRP 路由的接口，请使用 **show eigrp interfaces** 命令。

show eigrp [*as-number*] **interfaces** [*if-name*] [**detail**]

Syntax Description		
<i>as-number</i>	(可选) 指定您显示活动接口的 EIGRP 流程的自主系统编号。由于 threat defense 设备仅支持一个 EIGRP 路由流程，因此，无需指定自主系统编号。	
detail	(可选) 显示详细信息。	
<i>if-name</i>	(可选) 接口的名称。指定限制指定接口显示的接口名称。	
Command Default	如果没有指定接口名称，则显示所有 EIGRP 接口的信息。	
Command History	版本	修改
	6.1	引入了此命令。

使用指南 使用 **show eigrp interfaces** 命令确定哪些接口上的 EIGRP 处于活动状态，并了解与这些接口相关的 EIGRP 的信息。

如果指定了接口，则仅显示该接口。否则将显示正在运行 EIGRP 的所有接口。

如果指定了自主系统，则仅显示该指定自主系统的路由流程。否则将显示所有 EIGRP 流程。

示例

以下是 **show eigrp interfaces** 命令的输出示例：

```
> show eigrp interfaces

EIGRP-IPv4 interfaces for process 100

Interface    Peers    Xmit Queue    Mean    Pacing Time    Multicast    Pending
             Un/Reliable  SRTT         Un/Reliable    Flow Timer   Routes
-----
mgmt         0         0/0           0        11/434         0           0
outside     1         0/0           337      0/10           0           0
inside      1         0/0           10       1/63           103          0
```

下表描述屏幕上展示的重要字段。

表 2: **show eigrp interfaces** 字段说明

字段	Description
process	EIGRP 路由流程的自主系统编号。
Peers	直连对等设备的数量。

字段	Description
Xmit Queue Un/Reliable	不可靠队列和可靠传输队列中包含的数据包数量。
Mean SRTT	平均顺利往返时间间隔（以秒为单位）。
Pacing Time Un/Reliable	用于确定 EIGRP 数据包应何时发出接口（不可靠和可靠数据包）的定步计时（以秒为单位）。
Multicast Flow Timer	threat defense 设备将发送组播 EIGRP 数据包的最大秒数。
Pending Routes	等待发送的传输队列中的数据包内的路由数。

show eigrp neighbors

要显示 EIGRP 邻居表，请使用 **show eigrp neighbors** 命令。

show eigrp [*as-number*] **neighbors** [**detail** | **static**] [*if-name*]

Syntax Description

<i>as_number</i>	(可选) 指定要删除邻居条目的 EIGRP 流程的自主系统编号。由于 threat defense 设备仅支持一个 EIGRP 路由流程，因此，无需指定自主系统编号。
detail	(可选) 显示详细邻居信息。
<i>if-name</i>	(可选) 接口的名称。指定接口名称将显示通过该接口获知的所有邻居表条目。
static	(可选) 显示静态定义的 EIGRP 邻居。

Command Default

如果没有指定接口名称，则显示通过所有接口获知的邻居。

Command History

版本	修改
6.1	引入了此命令。

使用指南

您可以使用 **clear eigrp neighbors** 命令清除从 EIGRP 邻居表动态获知的邻居。除非您使用 **static** 关键字，否则静态邻居不包含在输出中。

示例

以下是 **show eigrp neighbors** 命令的输出示例：

```
> show eigrp neighbors

EIGRP-IPv4 Neighbors for process 100

Address                Interface    Holdtime  Uptime    Q      Seq  SRTT  RTO
                   (secs)     (h:m:s)  Count    Num  (ms)  (ms)
172.16.81.28           Ethernet1    13        0:00:41   0      11   4     20
172.16.80.28           Ethernet0    14        0:02:01   0      10  12     24
172.16.80.31           Ethernet0    12        0:02:02   0       4   5     20
```

下表描述屏幕上展示的重要字段。

表 3: **show eigrp neighbors** 字段说明

字段	Description
process	EIGRP 路由流程的自主系统编号。
Address	EIGRP 邻居的 IP 地址。

字段	Description
Interface	threat defense 设备在其上接收来自邻居的问候数据包的接口。
Holdtime	threat defense 设备在宣告关闭之前等待从邻居收到消息的时长（以秒为单位）。此保持时间从问候数据包中的邻居接收，然后开始减少，直到从邻居接收另一个问候数据包。 如果邻居使用默认保持时间，此数值将小于 15。如果对等设备配置了非默认的保持时间，则会显示非默认的保持时间。 如果该值达到 0，则 threat defense 设备认为邻居不可访问。
Uptime	自 threat defense 设备初次从邻居收到消息后的已用时间（小时:分钟:秒钟格式）。
Q Count	等待 threat defense 设备发送的 EIGRP 数据包（更新、查询和应答）数。
Seq Num	从邻居接收到的最后一个更新数据包、查询数据包或应答数据包的顺序号。
SRTT	顺利往返时间。EIGRP 数据包发送到此邻居和 threat defense 设备接收该数据包确认所需的毫秒数。
RTO	重新传输超时（以毫秒为单位）。这是 threat defense 设备将数据包从重新传输队列重新发送到邻居之前等待的时间量。

以下是 `show eigrp neighbors static` 命令的输出示例：

```
> show eigrp neighbors static

EIGRP-IPv4 neighbors for process 100
Static Address          Interface
192.168.1.5            management
```

下表描述屏幕上展示的重要字段。

表 4: `show ip eigrp neighbors static` 字段说明

字段	Description
process	EIGRP 路由流程的自主系统编号。
Static Address	EIGRP 邻居的 IP 地址。
Interface	threat defense 设备在其上接收来自邻居的问候数据包的接口。

以下是 `show eigrp neighbors detail` 命令的输出示例：

```
> show eigrp neighbors detail

EIGRP-IPv4 neighbors for process 100
H   Address                Interface          Hold Uptime   SRTT   RTO   Q Seq Tye
```



```

                                (sec)      (ms)      Cnt Num
3  1.1.1.3                      Et0/0      12 00:04:48 1832 5000 0 14
  Version 12.2/1.2, Retrans: 0, Retries: 0
  Restart time 00:01:05
0  10.4.9.5                      Fa0/0      11 00:04:07 768 4608 0 4 S
  Version 12.2/1.2, Retrans: 0, Retries: 0
2  10.4.9.10                     Fa0/0      13 1w0d          1 3000 0 6 S
  Version 12.2/1.2, Retrans: 1, Retries: 0
1  10.4.9.6                      Fa0/0      12 1w0d          1 3000 0 4 S
  Version 12.2/1.2, Retrans: 1, Retries: 0

```

下表描述屏幕上展示的重要字段。

表 5: *show ip eigrp neighbors details* 字段说明

字段	Description
process	EIGRP 路由流程的自主系统编号。
H	该列列出了与指定邻居建立对等会话的顺序。该顺序由从 0 开始的有序编号指定。
Address	EIGRP 邻居的 IP 地址。
Interface	threat defense 设备在其上接收来自邻居的问候数据包的接口。
Holdtime	<p>threat defense 设备在宣告关闭之前等待从邻居收到消息的时长（以秒为单位）。此保持时间从问候数据包中的邻居接收，然后开始减少，直到从邻居接收另一个问候数据包。</p> <p>如果邻居使用默认保持时间，此数值将小于 15。如果对等设备配置了非默认的保持时间，则会显示非默认的保持时间。</p> <p>如果该值达到 0，则 threat defense 设备认为邻居不可访问。</p>
Uptime	自 threat defense 设备初次从邻居收到消息后的已用时间（小时:分钟:秒钟格式）。
SRTT	顺利往返时间。EIGRP 数据包发送到此邻居和 threat defense 设备接收该数据包确认所需的毫秒数。
RTO	重新传输超时（以毫秒为单位）。这是 threat defense 设备将数据包从重新传输队列重新发送到邻居之前等待的时间量。
Q Count	等待 threat defense 设备发送的 EIGRP 数据包（更新、查询和应答）数。
Seq Num	从邻居接收到的最后一个更新数据包、查询数据包或应答数据包的序号。
Version	指定的对等设备运行的软件版本。
Retrans	数据包已重传的次数。
Retries	重传数据包的尝试次数。

字段	Description
Restart time	指定从邻居重启之后的已用时间（格式：小时:分钟:秒）。

show eigrp topology

要显示 EIGRP 拓扑表，请使用 **show eigrp topology** 命令。

show eigrp [*as-number*] **topology** [*ip-addr* [*mask*] | **active** | **all-links** | **pending** | **summary** | **zero-successors**]

Syntax Description	
active	(可选) 仅显示 EIGRP 拓扑表中的活动条目。
all-links	(可选) 显示 EIGRP 拓扑表中的所有路由，即使并非可行后续路由。
<i>as_number</i>	(可选) 指定 EIGRP 流程的自主系统编号。由于 threat defense 设备仅支持一个 EIGRP 路由流程，因此，无需指定自主系统编号。
<i>ip-addr</i>	(可选) 定义要显示的拓扑表 IP 地址。使用掩码指定时，将提供条目的详细说明。
<i>mask</i>	(可选) 定义要应用于 <i>ip-addr</i> 参数的网络掩码。
pending	(可选) 显示等待来自邻居的更新或等待回复邻居的 EIGRP 拓扑表中的所有条目。
summary	(可选) 显示 EIGRP 拓扑表的摘要。
zero-successors	(可选) 显示 EIGRP 拓扑表中可用的路由。

Command Default 仅显示可行后续路由。使用 **all-links** 关键字以显示所有路由，包括并非可行后续的路由。

Command History	版本	修改
	6.1	引入了此命令。

使用指南 您可以使用 **clear eigrp topology** 命令删除拓扑表的动态条目。

示例

以下是 **show eigrp topology** 命令的输出示例：

```
EIGRP-IPv4 Topology Table for AS(100)/ID(192.168.1.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 10.2.1.0 255.255.255.0, 2 successors, FD is 0
   via 10.16.80.28 (46251776/46226176), Ethernet0
   via 10.16.81.28 (46251776/46226176), Ethernet1
P 10.2.1.0 255.255.255.0, 1 successors, FD is 307200
   via Connected, Ethernet1
   via 10.16.81.28 (307200/281600), Ethernet1
```

```
via 10.16.80.28 (307200/281600), Ethernet0
```

下表描述屏幕上展示的重要字段。

表 6: `show eigrp topology` 字段说明

字段	Description
Codes	此拓扑表条目的状态。 <code>passive</code> （被动）和 <code>active</code> （主动）指与该目标相关的 EIGRP 状态； <code>update</code> （更新）、 <code>query</code> （查询）和 <code>reply</code> （应答）指所发送的数据包的类型。
P - Passive	路由已知良好并且没有对此目标执行任何 EIGRP 计算。
A - Active	对此目标执行 EIGRP 计算。
U - Update	表示向此目标发送了一个更新数据包。
Q - Query	表示向此目标发送了一个查询数据包。
R - Reply	表示向此目标发送了一个应答数据包。
r - Reply status	在软件发送查询之后等待应答期间所设置的标志。
address mask	目标 IP 地址和掩码。
successors	后继路由数量。该数字对应 IP 路由表中的下一跳数量。如果“successors”为大写，则路由或下一跳处于过渡状态。
FD	可行距离。可行距离是到达目的地的最佳度量，或是路由进入活动状态后所获知的最佳度量。该值用于检查可行性条件。如果路由器的报告距离（斜杠后的度量）小于可行距离，则符合可行性条件，该路径为可行后继路由。软件确定其有可行后续路由后，无需发送该目标的查询。
via	将关于此目标的信息告知软件的对等设备 IP 地址。前 n 个条目（其中 n 为后继路由数）为当前后继路由。列表上其余的条目是可行后继路由。
(cost/adv_cost)	第一个数字为 EIGRP 度量，表示到达目标的成本。第二个数字是此对等设备所通告的 EIGRP 度量。
interface	获知该信息所使用的接口。

以下是 `show eigrp topology` 使用的 IP 地址的输出示例。所示输出适用于内部路由。

```
> show eigrp topology 10.2.1.0 255.255.255.0
EIGRP-IPv4 (AS 100): Topology Default-IP-Routing-Table(0) entry for entry for 10.2.1.0
255.255.255.0

    State is Passive, Query origin flag is 1, 1 Successor(s), FD is 281600
    Routing Descriptor Blocks:
      0.0.0.0 (Ethernet0/0), from Connected, Send flag is 0x0
        Composite metric is (281600/0), Route is Internal
```

```

Vector metric:
  Minimum bandwidth is 10000 Kbit
  Total delay is 1000 microseconds
  Reliability is 255/255
  Load is 1/255
  Minimum MTU is 1500
  Hop count is 0

```

以下是 **show eigrp topology** 使用的 IP 地址的输出示例。所示输出适用于外部路由。

```

> show eigrp topology 10.4.80.0 255.255.255.0
EIGRP-IPv4 (AS 100): Topology Default-IP-Routing-Table(0) entry for entry for 10.4.80.0
255.255.255.0

State is Passive, Query origin flag is 1, 1 Successor(s), FD is 409600
Routing Descriptor Blocks:
  10.2.1.1 (Ethernet0/0), from 10.2.1.1, Send flag is 0x0
    Composite metric is (409600/128256), Route is External
    Vector metric:
      Minimum bandwidth is 10000 Kbit
      Total delay is 6000 microseconds
      Reliability is 255/255
      Load is 1/255
      Minimum MTU is 1500
      Hop count is 1
    External data:
      Originating router is 10.89.245.1
      AS number of route is 0
      External protocol is Connected, external metric is 0
      Administrator tag is 0 (0x00000000)

```

Related Commands

命令	Description
clear eigrp topology	清除从 EIGRP 拓扑表动态查找的条目。

show eigrp traffic

要显示发送和接收的 EIGRP 数据包的数量，请使用 **show eigrp traffic** 命令。

show eigrp [*as-number*] **traffic**

Syntax Description	<i>as_number</i>	(可选) 指定您查看事件日志的 EIGRP 流程的自主系统编号。由于 threat defense 设备仅支持一个 EIGRP 路由流程，因此，无需指定自主系统编号。
---------------------------	------------------	---

Command History	版本	修改
	6.1	引入了此命令。

使用指南 您可以使用 **clear eigrp traffic** 命令清除 EIGRP 流量统计信息。

示例

以下是 **show eigrp traffic** 命令的输出示例：

```
> show eigrp traffic
EIGRP-IPv4 Traffic Statistics for AS 100
  Hellos sent/received: 218/205
  Updates sent/received: 7/23
  Queries sent/received: 2/0
  Replies sent/received: 0/2
  Acks sent/received: 21/14
  Input queue high water mark 0, 0 drops
  SIA-Queries sent/received: 0/0
  SIA-Replies sent/received: 0/0
  Hello Process ID: 1719439416
  PDM Process ID: 1719439824
```

下表描述屏幕上展示的重要字段。

表 7: **show eigrp traffic** 字段说明

字段	Description
process	EIGRP 路由流程的自主系统编号。
Hellos sent/received	发送和接收的问候数据包数。
Updates sent/received	发送和接收的更新数据包数。
Queries sent/received	发送和接收的查询数据包数。
Replies sent/received	发送和接收的回复数据包数。
Acks sent/received	发送和接收的确认数据包数。

字段	Description
Input queue high water mark/drops	接近最大接收阈值的发送数据包数和丢弃数据包数。
SIA-Queries sent/received	发送和接收的 Stuck-in-active 查询。
SIA-Replies sent/received	发送和接收的 Stuck-in-active 回复。

show environment

要显示系统组件的系统环境信息，请使用 **show environment** 命令。



注释 Firepower 2100、4100 和 9300 系列设备不支持此命令。连接到 FXOS CLI 并使用 **show env** 命令而不是此命令。

```
show environment [alarm-contact | driver | fans | power-supplies | power_consumption |
voltage | temperature [accelerator | chassis | cpu | io-hub | mother-board |
power-supply]]
```

Syntax Description

alarm-contact	(可选) 显示 ISA 3000 设备上输入警报触点的运行状态。
driver	(可选) 显示环境监控 (IPMI) 驱动程序状态。驱动程序状态可为以下各项之一： <ul style="list-style-type: none"> • 运行 - 驱动程序正常运行。 • 已停止 - 错误导致驱动程序停止。
fans	(可选) 显示冷却风扇的运行状态。状态为以下之一： <ul style="list-style-type: none"> • 正常 - 风扇正常运行。 • 故障 - 风扇出现故障并应进行更换。
power-supplies	(可选) 显示电源设备的运行状态。每个电源设备的状态均为以下各项之一： <ul style="list-style-type: none"> • 正常 - 电源设备正常运行。 • 故障 - 电源设备出现故障并应进行更换。 • 不存在 - 指定的电源设备未安装。 <p>电源设备冗余状态也将显示。冗余状态为以下各项之一：</p> <ul style="list-style-type: none"> • 正常 - 设备以完整资源正常运行。 • 丢失 - 设备已丢失冗余但以最低资源正常运行。任何进一步的故障都将导致系统关闭。 • 不适用 - 设备未配置电源设备冗余。
power_consumption	(可选) 显示功耗值
voltage	(可选) 显示 CPU 电压通道 1-24 的值。不包括运行状态。

temperature (可选) 显示处理器和机箱的温度和状态。温度单位为摄氏度。您可以包含关键字以将输出限制为特定区域: **accelerator**、**chassis**、**cpu**、**io-hub**、**motherboard**、**power-supply**。

状态为以下之一:

- 正常 - 温度在正常工作范围内, 低于 70 摄氏度。
- 严重 - 温度超出正常操作范围。70-80 被认为是温暖的; 80-90 为严重, 大于 90 被视为不可恢复。

Command Default

如果没有指定关键字, 则显示所有运行信息 (驱动程序除外)。

Command History

版本	修改
6.1	引入了此命令。
6.3	我们为 ISA 3000 添加了 alarm-contact 关键字。

使用指南

您可以显示设备中物理组件的运行环境信息。此信息包括风扇和电源设备的运行状态, 以及 CPU 和机箱的温度和状态。对于 ISA 3000 设备, 它包括有关输入警报触点的信息。

示例

以下是 **show environment** 命令的常规输出示例:

```
> show environment
Cooling Fans:
-----
Power Supplies:
-----
Left Slot (PS0): 6900 RPM - OK (Power Supply Fan)
Right Slot (PS1): 7000 RPM - OK (Power Supply Fan)
Power Supplies:
-----
Power Supply Unit Redundancy: OK
Temperature:
-----
Left Slot (PS0): 26 C - OK (Power Supply Temperature)
Right Slot (PS1): 27 C - OK (Power Supply Temperature)
Cooling Fans:
-----
Left Slot (PS0): 6900 RPM - OK (Power Supply Fan)
Right Slot (PS1): 7000 RPM - OK (Power Supply Fan)
Temperature:
-----
Processors:
-----
Processor 1: 44.0 C - OK (CPU1 Core Temperature)
Processor 2: 45.0 C - OK (CPU2 Core Temperature)
Chassis:
-----
Ambient 1: 28.0 C - OK (Chassis Front Temperature)
Ambient 2: 40.5 C - OK (Chassis Back Temperature)
Ambient 3: 28.0 C - OK (CPU1 Front Temperature)
```

```

Ambient 4: 36.50 C - OK (CPU1 Back Temperature)
Ambient 5: 34.50 C - OK (CPU2 Front Temperature)
Ambient 6: 43.25 C - OK (CPU2 Back Temperature)
Power Supplies:
-----
Left Slot (PS0): 26 C - OK (Power Supply Temperature)
Right Slot (PS1): 27 C - OK (Power Supply Temperature)

```

以下是 **show environment driver** 命令的输出示例:

```

> show environment driver
Cooling Fans:
-----
Chassis Fans:
-----
Cooling Fan 1: 5888 RPM - OK
Cooling Fan 2: 5632 RPM - OK
Cooling Fan 3: 5888 RPM - OK
Power Supplies:
-----
Left Slot (PS0): N/A
Right Slot (PS1): 8448 RPM - OK
Power Supplies:
-----
Left Slot (PS0): Not Present
Right Slot (PS1): Present
Left Slot (PS0): N/A
Right Slot (PS1): 33 C - OK
Left Slot (PS0): N/A
Right Slot (PS1): 8448 RPM - OK
Temperature:
-----
Processors:
-----
Processor 1: 70.0 C - OK
Chassis:
-----
Ambient 1: 36.0 C - OK (Chassis Back Temperature)
Ambient 2: 31.0 C - OK (Chassis Front Temperature)
Ambient 3: 39.0 C - OK (Chassis Back Left Temperature)
Power Supplies:
-----
Left Slot (PS0): N/A
Right Slot (PS1): 33 C - OK
Voltage:
-----
Channel 1: 1.168 V - (CPU Core 0.46V-1.4V)
Channel 2: 11.954 V - (12V)
Channel 3: 4.998 V - (5V)
Channel 4: 3.296 V - (3.3V)
Channel 5: 1.496 V - (DDR3 1.5V)
Channel 6: 1.048 V - (PCH 1.5V)

```

以下是 **show environment alarm-contact** 命令的输出示例。

```

> show environment alarm-contact
ALARM CONTACT 1
  Status:      not asserted
  Description: external alarm contact 1
  Severity:    minor
  Trigger:     closed
ALARM CONTACT 2

```

```
Status:      not asserted
Description: external alarm contact 2
Severity:    minor
Trigger:     closed
```

Related Commands

命令	Description
clear facility-alarm output	断开输出继电器并清除 LED 的警报状态。
show facility-alarm	显示已触发警报的状态信息。
show version	显示硬件和软件版本。

show facility-alarm

要显示 ISA 3000 设备中触发的警报，请使用 **show facility-alarm** 命令。

show facility-alarm {**relay** | **status** [**major** | **minor** | **info**]}

Syntax Description

relay	显示已激活报警输出继电器的报警。
status [major minor info]	显示已触发的所有警报。您可以添加以下关键字来限制列表： <ul style="list-style-type: none"> • major- 显示所有主要严重性警报。 • minor- 显示所有次要严重性警报。 • info- 显示所有警报。此关键字提供与不使用关键字时相同的视图。

Command History

版本	修改
6.3	引入了此命令。

使用指南

使用 **relay** 关键字可仅查看已激活警报输出继电器的警报。输出警报继电器根据您是否配置触发警报来激活它。启动报警输出中继，激活连接的设备，比如蜂鸣器或闪烁灯的外部警报。

使用 **status** 关键字查看已触发的所有警报，无论警报操作是否触发了外部警报输出继电器。

下表对输出列进行了解释。

列	Description
Source	从中触发报警的设备。这通常是在该设备上配置的主机名。
Severity	严重或轻微。
Description	触发的报警的类型。例如，温度、外部警报接触或冗余电源。
Relay	外部报警输出继电器是通电还是断电。根据您的警报配置触发外部输出警报。
Time	触发的报警的时间戳。

示例

以下是 **show facility-alarm relay** 命令的输出示例：

```
> show facility-alarm relay
Source      Severity  Description                                Relay      Time
firepower  minor     external alarm contact 1 triggered      Energized  06:56:50 UTC Mon Sep
22 2014
```

以下是 **show facility-alarm status** 命令的输出示例:

```
> show facility-alarm status info
Source      Severity  Description                               Relay      Time
firepower  minor    external alarm contact 1 triggered      Energized  06:56:50 UTC Mon Sep 22
2014
firepower  minor    Temp below Secondary Threshold          De-energized 06:56:49 UTC Mon Sep 22
2014
firepower  major    Redundant pwr missing or failed         De-energized 07:00:19 UTC Mon Sep 22
2014
firepower  major    Redundant pwr missing or failed         De-energized 07:00:19 UTC Mon Sep 22
2014

> show facility-alarm status major
Source      Severity  Description                               Relay      Time
firepower  major      Redundant pwr missing or failed         De-energized 07:00:19 UTC Mon Sep
22 2014
firepower  major      Redundant pwr missing or failed         De-energized 07:00:19 UTC Mon Sep
22 2014

> show facility-alarm status minor
Source      Severity  Description                               Relay      Time
firepower  minor      external alarm contact 1 triggered      Energized  06:56:50 UTC Mon Sep
22 2014
firepower  minor      Temp below Secondary Threshold          De-energized 06:56:49 UTC Mon Sep
22 2014
```

Related Commands

命令	Description
clear facility-alarm output	断开输出继电器并清除 LED 的警报状态。
show alarm settings	显示所有全局报警设置。
show environment alarm-contact	显示输入警报触点的状态。

show failover

要显示有关设备的故障转移状态的信息，请使用 **show failover** 命令。

```
show failover [ group num | history [ details ] | interface | state | trace [ options ] | statistics | details ]
```

Syntax Description							
group num	显示指定的故障转移组的运行状态。						
history [details]	<p>显示故障转移历史记录。故障转移历史记录显示已结束故障转移状态更改和状态更改的原因。此信息可帮助进行故障排除。</p> <p>添加 details 关键字可显示对等体的故障转移历史记录。这包括故障转移状态更改和对等设备发生状态更改的原因。</p> <p>历史记录信息会随设备重启而被清除。</p>						
interface	显示故障转移和有状态链路信息。						
state	显示两个故障切换设备的故障转移状态。显示的信息包括设备的主要或辅助状态、设备的主用/备用状态以及最新报告的故障转移原因。即使清除了故障的原因，故障原因信息也会保留在输出中。						
trace [options]	<p>(可选) 显示故障转移事件跟踪。选项包括按级别 (1-5) 显示故障转移事件跟踪：</p> <ul style="list-style-type: none"> • critical - 过滤故障转移关键事件跟踪 (级别 = 1) • debugging- 过滤故障转移调试跟踪 (调试级别 = 5) • error- 过滤故障转移内部异常 (级别 = 2) • informational- 过滤故障转移信息跟踪 (级别 = 4) • warning- 过滤故障转移警告 (级别 = 3) 						
statistics	显示故障转移命令接口的传输和接收数据包计数。						
details	显示高可用性对中的故障转移详细信息。						
Command History	<table border="1"> <thead> <tr> <th>版本</th> <th>修改</th> </tr> </thead> <tbody> <tr> <td>6.1</td> <td>引入了此命令。</td> </tr> <tr> <td>6.2.3</td> <td>添加了 history details 关键字。</td> </tr> </tbody> </table>	版本	修改	6.1	引入了此命令。	6.2.3	添加了 history details 关键字。
版本	修改						
6.1	引入了此命令。						
6.2.3	添加了 history details 关键字。						

版本	修改
6.4	添加了以下对象静态计数。 <ul style="list-style-type: none"> • 规则数据库 B 同步 • 规则数据库 P-Sync • 规则数据库删除
7.0	添加了 details 关键字。

使用指南

show failover 命令显示动态故障转移信息、接口状态和有状态故障转移统计信息。

如果接口上配置了 IPv4 和 IPv6 地址，则两个地址都会出现在输出中。由于一个接口上可配置多个 IPv6 地址，因此只显示本地链路的地址。如果接口上未配置 IPv4 地址，则输出中的 IPv4 地址会显示为 0.0.0.0。如果接口上未配置 IPv6 地址，则输出中会直接省略地址。

只有在启用有状态故障转移时，才会出现有状态故障切换逻辑更新统计信息输出。“xerr”和“rerr”值并不指示故障转移中的错误数，而是指示数据包传输或接收错误数。

在 **show failover** 命令输出中，有状态故障转移字段包含以下值：

- 有状态对象具有以下值：
 - xmit - 指示传输的数据包数。
 - xerr - 指示传输错误数。
 - rcv - 指示接收的数据包数。
 - rerr - 指示接收错误数。
- 每行是针对特定对象的静态计数，如下所示：
 - General - 指示所有有状态对象的总和。
 - sys cmd - 指逻辑更新系统命令，例如 **login** 或 **stay alive**。
 - up time - 指示 threat defense 设备正常工作时间的值，即主用 threat defense 设备传递到备用 threat defense 设备的时间。
 - RPC services - 远程过程调用连接信息。
 - TCP conn - 动态 TCP 连接信息。
 - UDP conn - 动态 UDP 连接信息。
 - ARP tbl - 动态 ARP 表信息。
 - Xlate_Timeout - 指示连接转换超时信息。
 - IPv6 ND tbl - IPv6 邻居发现表信息。
 - VPN IKE upd - IKE 连接信息。

- VPN IPSEC upd - IPsec 连接信息。
- VPN CTCP upd - cTCP 隧道连接信息。
- VPN SDI upd - SDI AAA 连接信息。
- VPN DHCP upd - 隧道化 DHCP 连接信息。
- SIP Session - SIP 信令会话信息。
- Route Session - 路由同步更新的 LU 统计信息
- Rule DB B-Sync - 指示执行规则数据库批量同步的次数以及相应的错误（如有）
- Rule DB P-Sync - 指示规则数据库定期同步的次数以及此操作的错误（如有）
- Rule DB Delete - 指示发送规则数据库删除消息的次数以及此操作的错误（如有）

如果不输入故障转移 IP 地址，则 **show failover** 命令显示 IP 地址为 0.0.0.0，且接口的监控仍处于“等待”状态。您必须设置一个故障转移 IP 地址，故障转移才能工作。

下表介绍了故障转移的接口状态。

表 8: 故障转移接口状态

State	Description
Normal	接口正在运行并正在接收来自对等设备上相应接口的问候数据包。
Normal (Waiting)	接口已打开，但尚未从对等设备上的对应接口接收欢迎数据包。验证已为接口配置备用 IP 地址，并且两个接口之间存在连接。 当故障转移接口关闭时，您也可以看到此状态。
Normal (Not-Monitored)	接口正在运行，但故障转移进程并未监控它。未受监控的接口发生故障时不会触发故障转移。
No Link	物理链路断开。
No Link (Waiting)	物理链路断开，且接口尚未收到来自对等设备上相应接口的问候数据包。在恢复链路后，验证已为接口配置备用 IP 地址，并且两个接口之间存在连接。
No Link (Not-Monitored)	物理链路断开，但故障转移进程并未监控它。未受监控的接口发生故障时不会触发故障转移。
Link Down	物理链路处于工作状态，但是接口处于管理性关闭状态。
Link Down (Waiting)	物理链路处于工作状态，但是接口处于管理性关闭状态，且接口尚未收到来自对等设备上相应接口的问候数据包。将接口启动后，请检查该接口是否配置了备用 IP 地址，并且两个接口之间是否连接。

State	Description
Link Down (Not-Monitored)	物理链路处于工作状态，但是接口处于管理性关闭状态，且故障转移流程并未监控它。未受监控的接口发生故障时不会触发故障转移。
Testing	接口由于丢失来自对等设备上相应接口的问候数据包而处于测试模式。
Failed	接口测试失败，并且接口标记为发生故障。如果接口故障符合故障转移条件，则接口故障会导致故障转移到备用设备或故障转移组。

示例

以下是主用/备用故障转移的 **show failover** 命令的输出示例。

```

Failover unit Primary
Failover LAN Interface: failover GigabitEthernet0/2 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Failover On
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 61 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.7(0)74, Mate 9.7(0)74
Serial Number: Ours 9A41CKDXQJU, Mate 9A3MFP0H1CP
Last Failover at: 19:23:17 UTC Oct 26 2016
  This host: Primary - Active
    Active time: 589 (sec)
    slot 0: empty
      Interface diagnostic (0.0.0.0): Normal (Waiting)
      Interface outside (192.168.77.1): Normal (Waiting)
      Interface inside (192.168.87.1): Normal (Waiting)
    slot 1: snort rev (1.0) status (up)
    slot 2: diskstatus rev (1.0) status (up)
  Other host: Secondary - Standby Ready
    Active time: 0 (sec)
    Interface diagnostic (0.0.0.0): Normal (Waiting)
    Interface outside (0.0.0.0): Normal (Waiting)
    Interface inside (0.0.0.0): Normal (Waiting)
    slot 1: snort rev (1.0) status (up)
    slot 2: diskstatus rev (1.0) status (up)
Stateful Failover Logical Update Statistics
Link : failover GigabitEthernet0/2 (up)
Stateful Obj      xmit      xerr      rcv      rerr
General           45         0         44         0
sys cmd           44         0         44         0
up time           0          0          0          0
RPC services      0          0          0          0
TCP conn          0          0          0          0
UDP conn          0          0          0          0
ARP tbl           0          0          0          0
Xlate_Timeout     0          0          0          0
IPv6 ND tbl       0          0          0          0
VPN IKEv1 SA      0          0          0          0
VPN IKEv1 P2      0          0          0          0
VPN IKEv2 SA      0          0          0          0

```

```

VPN IKEv2 P2      0      0      0      0
VPN CTCP upd     0      0      0      0
VPN SDI upd      0      0      0      0
VPN DHCP upd     0      0      0      0
SIP Session      0      0      0      0
SIP Tx           0      0      0      0
SIP Pinhole      0      0      0      0
Route Session    0      0      0      0
Router ID        0      0      0      0
User-Identity    1      0      0      0
CTS SGTNAME      0      0      0      0
CTS PAC          0      0      0      0
TrustSec-SXP     0      0      0      0
IPv6 Route       0      0      0      0
STS Table        0      0      0      0
Rule DB B-Sync   0      0      1      0
Rule DB P-Sync   5      0      1      0
Rule DB Delete   12     0      5      0

Logical Update Queue Information
          Cur  Max  Total
Recv Q:   0   10   44
Xmit Q:   0   11  238

```

以下是主用-备用设置的 **show failover state** 命令的输出示例。

```

> show failover state

State          Last Failure Reason      Date/Time
This host -    Primary
               Negotiation             Backplane Failure       15:44:56 UTC Jun 20 2016
Other host -   Secondary
               Not Detected           Comm Failure             15:36:30 UTC Jun 20 2016

====Configuration State====
      Sync Done
====Communication State====
      Mac set

```

下表介绍了 **show failover state** 命令的输出。

表 9: show failover state 输出说明

字段	Description
Configuration State	<p>显示配置同步状态。</p> <p>以下是备用设备的可能配置状态：</p> <ul style="list-style-type: none"> • Config Syncing - STANDBY- 在执行同步配置时设置。 • Interface Config Syncing - STANDBY • Sync Done - STANDBY- 当备用设备完成从主用设备的配置同步时设置。 <p>以下是主用设备的可能配置状态：</p> <ul style="list-style-type: none"> • Config Syncing- 在主用设备执行与备用设备的配置同步时在主用设备上设置。 • Interface Config Syncing • Sync Done- 在主用设备已成功完成到备用设备的配置同步时设置。 • Ready for Config Sync- 在备用设备发出准备好接收配置同步的信号时在主用设备上设置。
Communication State	<p>显示 MAC 地址同步状态。</p> <ul style="list-style-type: none"> • Mac set- MAC 地址已完成从对等设备至此设备的同步。 • Updated Mac- 在 MAC 地址已更新并需要同步到另一设备时使用。在设备正在更新从对等设备同步的本地 MAC 地址的过渡期间也使用此状态。
Date/Time	显示故障的日期和时间戳。
Last Failure Reason	<p>显示最后报告故障的原因。此信息不会清除，即使故障情况已清除。只有发生故障转移时，此信息才会变更。</p> <p>以下是可能的故障原因：</p> <ul style="list-style-type: none"> • Interface Failure- 发生故障的接口数量符合故障切换条件并导致故障转移。 • Comm Failure- 故障转移链路发生故障或对等体关闭。 • Backplane Failure
State	显示设备的主要/辅助和主用/备用状态。
This host/Other host	此主机指示被执行命令的设备的信息。其他主机指示故障转移配对中的另一个设备的信息。

以下是主设备上 **show failover history** 命令的输出示例:

```
> show failover history
=====
From State          To State          Reason
=====
14:29:59 UTC Nov 11 2017
Not Detected          Negotiation          No Error

14:30:36 UTC Nov 11 2017
Negotiation           Cold Standby         Detected an Active mate

14:30:38 UTC Nov 11 2017
Cold Standby         Sync Config          Detected an Active mate

14:30:47 UTC Nov 11 2017
Sync Config          Sync File System     Detected an Active mate

14:30:47 UTC Nov 11 2017
Sync File System     Bulk Sync            Detected an Active mate

14:31:00 UTC Nov 11 2017
Bulk Sync            Standby Ready        Detected an Active mate

14:31:39 UTC Nov 11 2017
Standby Ready        Failed               Interface check
This host:1
single_vf: OUTSIDE
Other host:0

14:31:46 UTC Nov 11 2017
Failed               Standby Ready        Interface check
This host:0
Other host:0

14:33:36 UTC Nov 11 2017
Standby Ready        Just Active          HELLO not heard from mate

14:33:36 UTC Nov 11 2017
Just Active          Active Drain          HELLO not heard from mate

14:33:36 UTC Nov 11 2017
Active Drain          Active Applying Config HELLO not heard from mate

14:33:36 UTC Nov 11 2017
Active Applying Config Active Config Applied HELLO not heard from mate

14:33:36 UTC Nov 11 2017
Active Config Applied Active               HELLO not heard from mate
=====
```

以下是辅助设备上 **show failover history** 命令的输出示例:

```
> show failover history
=====
From State          To State          Reason
=====
17:17:29 UTC Nov 10 2017
Not Detected          Negotiation          No Error
```

```

17:18:06 UTC Nov 10 2017
Negotiation          Cold Standby          Detected an Active mate

17:18:08 UTC Nov 10 2017
Cold Standby        Sync Config           Detected an Active mate

17:18:17 UTC Nov 10 2017
Sync Config         Sync File System      Detected an Active mate

17:18:17 UTC Nov 10 2017
Sync File System    Bulk Sync             Detected an Active mate

17:18:30 UTC Nov 10 2017
Bulk Sync           Standby Ready         Detected an Active mate

17:19:09 UTC Nov 10 2017
Standby Ready       Failed                Interface check
This host:1
single_vf: OUTSIDE
Other host:0

17:19:21 UTC Nov 10 2017
Failed              Standby Ready         Interface check
This host:0
Other host:0

```

```
=====
```

每个条目提供状态更改的时间和日期、初始状态、结果状态和状态更改的原因。最新的条目位于显示画面的底部。较旧的条目显示在顶部。最多可以显示 60 个条目。一旦到达条目数上限，随着新条目添加至底部，最旧的条目就会从输出的顶部移除。

失败原因包括有助于进行故障排除的详细信息。其中包括接口检查、故障转移状态检查、状态进程故障和服务模块故障。

以下是 **show failover history details** 命令的输出示例：

```

>show failover history details
=====
From State          To State          Reason
=====
09:58:07 UTC Jan 18 2017
Not Detected        Negotiation        No Error

09:58:10 UTC Jan 18 2017
Negotiation         Just Active        No Active unit found

09:58:10 UTC Jan 18 2017
Just Active         Active Drain       No Active unit found

09:58:10 UTC Jan 18 2017
Active Drain        Active Applying Config No Active unit found

09:58:10 UTC Jan 18 2017
Active Applying Config Active Config Applied No Active unit found

09:58:10 UTC Jan 18 2017
Active Config Applied Active              No Active unit found
=====

```

```

PEER History Collected at 09:58:54 UTC Jan 18 2017
=====PEER-HISTORY=====
From State          To State          Reason
=====PEER-HISTORY=====
09:57:46 UTC Jan 18 2017
Not Detected        Negotiation        No Error

09:58:19 UTC Jan 18 2017
Negotiation         Cold Standby       Detected an Active mate

09:58:21 UTC Jan 18 2017
Cold Standby        Sync Config         Detected an Active mate

09:58:29 UTC Jan 18 2017
Sync Config         Sync File System    Detected an Active mate

09:58:29 UTC Jan 18 2017
Sync File System    Bulk Sync           Detected an Active mate

09:58:42 UTC Jan 18 2017
Bulk Sync           Standby Ready       Detected an Active mate

=====PEER-HISTORY=====

```

show failover history details 命令会请求对等体的故障转移历史记录，并打印设备故障转移历史记录以及对等体的最新故障转移历史记录。如果对等体在一秒内未响应，则会显示上次收集的故障转移历史记录信息。

下表显示了故障转移状态。有稳定和临时两种状态类型。稳定状态是发生如故障之类的情况而导致状态更改之前设备可保持的状态。临时状态是设备达到稳定状态时所经过的状态。

表 10: 故障转移状态

状态	Description
Disabled	禁用故障转移。这是稳定状态。
Failed	设备处于故障状态。这是稳定状态。
Negotiation	设备建立与对等设备的连接，并与其协商确定软件版本兼容性和主用/备用角色。根据协商的角色，设备将经历备用设备状态或主用设备状态，或进入故障状态。这是临时状态。
Not Detected	ASA 无法检测到对等设备的存在。若 ASA 启动并启用故障转移而对等设备不存在或关闭，会发生这种情况。
备用设备状态	
Cold Standby	设备等待对等设备进入主用状态。当对等设备进入主用状态时，此设备进入备用配置状态。这是临时状态。
Sync Config	设备请求来自对等设备的运行配置。如果配置同步时发生错误，设备会回到初始化状态。这是临时状态。
Sync File System	设备与对等设备同步文件系统。这是临时状态。

状态	Description
Bulk Sync	设备接收对等设备状态信息。只有启用有状态故障转移时，才会出现此状态。这是临时状态。
Standby Ready	设备已准备好在主用设备发生故障时接管。这是稳定状态。
主用设备状态	
Just Active	设备成为主用设备时进入的第一个状态。在此状态时会向对等设备发送消息，向对等设备警报该设备成为主用设备并为接口设置IP地址和MAC地址。这是临时状态。
Active Drain	丢弃来自对等设备的消息队列。这是临时状态。
Active Applying Config	设备正在应用系统配置。这是临时状态。
Active Config Applied	设备已完成应用系统配置。这是临时状态。
Active	设备处于主用状态并在处理流量。这是稳定状态。

每个状态更改后面都附带状态更改原因。在设备从临时状态过渡到稳定状态时，原因通常保持相同。以下是可能的状态更改原因：

- 未出现错误
- 通过 CI config 命令设置
- 故障转移状态检查
- 故障转移接口恢复正常
- 未收到对方的问候消息
- 另一设备具有不同的软件版本
- 另一设备操作模式不同
- 另一设备许可证不同
- 另一设备机箱配置不同
- 另一设备卡配置不同
- 另一设备要本设备成为主用设备
- 另一设备要本设备成为备用设备
- 另一设备报告本设备已发生故障
- 另一设备报告该设备已发生故障
- 配置不匹配
- 检测到主用对等设备

- 未找到主用设备
- 已完成配置同步
- 已从通信故障恢复
- 另一设备具有不同的 VLAN 组配置
- 无法验证 VLAN 配置
- 配置同步未完成
- 配置同步失败
- 接口检查
- 我的通信失败
- 针对故障转移消息没有收到 ACK
- 另一设备在同步后进入卡机状态
- 从对等设备中检测不到电源
- 没有故障转移电缆
- 高可用性状态进度失败
- 检测服务卡故障
- 另一设备中的服务卡发生故障
- 本设备与对等设备的服务卡都正常
- LAN 接口变成未配置
- 对等设备刚刚重新加载
- 从串行电缆切换到基于 LAN 的故障切换
- 无法验证配置同步的状态
- 自动更新请求
- 未知原因

以下是 **show failover interface** 命令的输出示例。设备已对故障转移接口配置 IPv6 地址。

```
> show failover interface
      interface folink GigabitEthernet0/2
          System IP Address: 2001:a0a:b00::a0a:b70/64
          My IP Address      : 2001:a0a:b00::a0a:b70
          Other IP Address   : 2001:a0a:b00::a0a:b71
```

以下是来自高可用性对上的对等设备的 **show failover details** 命令的输出示例。

> show failover details

```

Failover On
Failover unit Secondary
Failover LAN Interface: HA-LINK GigabitEthernet0/3 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
1 Hold Interval Success: 12 Failure: 0
2 Hold Interval Success: 15 Failure: 0
3 Hold Interval Success: 15 Failure: 0
4 Hold Interval Success: 15 Failure: 0
5 Hold Interval Success: 15 Failure: 0
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 1 of 311 maximum
Interface: management
  1 Hold Success: 0 Failure: 0
  2 Hold Success: 0 Failure: 0
  3 Hold Success: 0 Failure: 0
  4 Hold Success: 0 Failure: 0
  5 Hold Success: 0 Failure: 0
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 99.16(2)10, Mate 99.16(2)10
Serial Number: Ours 9A7WJNE35T5, Mate 9A3497TXPU6
Last Failover at: 06:56:25 UTC Jan 25 2021
  This host: Secondary - Standby Ready
    Active time: 0 (sec)
    slot 0: ASAv hw/sw rev (/99.16(2)10) status (Up Sys)
      Interface management (203.0.113.130/fe80::250:56ff:feb7:4927): Unknown
    (Waiting)
    slot 1: snort rev (1.0) status (up)
    snort poll success:2877 miss:0
    slot 2: diskstatus rev (1.0) status (up)

    disk poll success:2877 miss:0
  Other host: Primary - Active
    Active time: 2910 (sec)
    Interface management (203.0.113.130): Unknown (Waiting)
    slot 1: snort rev (1.0) status (up)
    peer snort poll success:2877 miss:0
    slot 2: diskstatus rev (1.0) status (up)

    peer disk poll success:2877 miss:0

Stateful Failover Logical Update Statistics
Link : HA-LINK GigabitEthernet0/3 (up)
Stateful Obj   xmit   xerr   rcv    rerr
General        379    0      380    0
sys cmd        379    0      379    0
up time        0      0      0      0
RPC services   0      0      0      0
TCP conn       0      0      0      0
UDP conn       0      0      0      0
ARP tbl        0      0      0      0
Xlate_Timeout  0      0      0      0
IPv6_ND_tbl    0      0      0      0
VPN IKEv1 SA   0      0      0      0
VPN IKEv1 P2   0      0      0      0
VPN IKEv2 SA   0      0      0      0
VPN IKEv2 P2   0      0      0      0
VPN CTCP upd   0      0      0      0
VPN SDI upd    0      0      0      0
VPN DHCP upd   0      0      0      0

```

```

SIP Session      0          0          0          0
SIP Tx 0         0          0          0
SIP Pinhole      0          0          0          0
Route Session    0          0          0          0
Router ID        0          0          0          0
User-Identity    0          0          1          0
CTS SGTNAME      0          0          0          0
CTS PAC          0          0          0          0
TrustSec-SXP     0          0          0          0
IPv6 Route       0          0          0          0

```

以下是 **show failover trace** 命令的故障转移警告示例：

```

> show failover trace warning
Warning:Output can be huge. Displaying in pager mode
Oct 14 UTC 20:56:56.345 [CABLE] [ERROR]fover: peer rcvd down ifcs info
Oct 14 UTC 20:56:56.345 [CABLE] [ERROR]fover: peer has 1 down ifcs
Oct 14 UTC 20:56:56.345 [CABLE] [ERROR]fover: peer rcvd down ifcs info
Oct 14 UTC 20:56:56.345 [CABLE] [ERROR]fover: peer has 1 down ifcs
Oct 14 UTC 20:56:56.345 [CABLE] [ERROR]fover: peer rcvd down ifcs info

```

Related Commands

命令	Description
show running-config failover	在当前配置中显示 failover 命令。

show failover exec

要显示指定设备的 **failover exec** 命令模式，请使用 **show failover exec** 命令。

```
show failover exec { active | standby | mate }
```

Syntax Description	active	显示主用设备的 failover exec 命令模式。
	mate	显示对等设备的 failover exec 命令模式。
	standby	显示备用设备的 failover exec 命令模式。
Command History	版本	修改
	6.1	引入了此命令。

使用指南

failover exec 命令会创建与指定设备的会话。默认情况下，该会话处于全局配置模式，即使 **threat defense** 不支持 CLI 配置。模式信息与 **threat defense** 无关。

show failover exec 命令显示指定设备上的命令模式，通过 **failover exec** 命令发送的命令在该设备中执行。

示例

以下是 **show failover exec** 命令的输出示例。

```
> show failover exec mate
Standby unit Failover EXEC is at config mode
```

Related Commands	命令	Description
	failover exec	在故障切换对中的指定设备上执行提供的命令。

show file

要显示有关文件系统的信息，请使用 **show file** 命令。

show file [**descriptors** | **system** | **information filename**]

Syntax Description	descriptors	显示所有打开文件描述符。
	information filename	显示有关特定文件的信息，包括合作伙伴应用包文件。
	system	显示有关磁盘文件系统的大小、可用字节数、介质类型、标志和前缀信息。
Command History	版本	修改
	6.1	引入了此命令。

示例

以下是 **show file system** 命令的输出示例。

```
> show file system
File Systems:
  Size(b)      Free(b)      Type      Flags  Prefixes
* 7935832064  7828107264  disk      rw     disk0: flash:
-             -            disk      rw     disk1:
-             -            network   rw     tftp:
-             -            opaque    rw     system:
-             -            network   ro     http:
-             -            network   ro     https:
-             -            network   rw     scp:
-             -            network   rw     ftp:
-             -            network   wo     cluster:
-             -            stub      ro     cluster_trace:
-             -            network   rw     smb:
```

以下是 **show file information** 命令的输出示例：

```
> show file information install.log
disk0:/install.log:
  type is ascii text
  file size is 150484 bytes
```

Related Commands	命令	Description
	dir	系统随即会显示目录的内容。
	pwd	系统随即会显示当前工作目录。

show firewall

要显示当前防火墙模式（路由或透明），请使用 **show firewall** 命令。

show firewall

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show firewall** 命令的输出示例：

```
> show firewall
Firewall mode: Router
```

Related Commands

命令	Description
configure firewall	设置防火墙模式。
show mode	显示当前情景模式（单模式或多模式）。

show flash

要显示内部闪存的内容，请使用 **show flash:** 命令。

show flash: [all | controller | fileys]



注释 在 threat defense 中，**flash** 关键字的别名为 **disk0**。

Syntax Description

all	显示所有闪存信息。
controller	显示文件系统控制器信息。
fileys	显示文件系统信息。

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show flash:** 命令的输出示例：

```
> show flash:
--#-- --length-- -----date/time----- path
 48 107030784 Oct 05 2016 02:10:26 os.img
 49 33 Oct 06 2016 16:15:24 .boot_string
 50 150484 Oct 06 2016 15:36:02 install.log
 11 4096 Oct 06 2016 15:58:16 log
 13 1065 Oct 06 2016 15:59:13 log/asa-appagent.log
 16 4096 Oct 06 2016 15:59:07 crypto_archive
 51 4096 Oct 06 2016 15:59:12 coredumpinfo
 52 59 Oct 06 2016 15:59:12 coredumpinfo/coredump.cfg
 53 36 Oct 06 2016 16:04:47 enable_configure

7935832064 bytes total (7828107264 bytes free)
```

Related Commands

命令	Description
dir	系统随即会显示目录的内容。
show disk0:	显示内部闪存的内容。
show disk1:	显示外部闪存卡的内容。

show flow-export counters

要查看 NetFlow 统计信息和错误数据的运行时间计数器，请使用 **show flow-export counters** 命令。

show flow-export counters

Command History

版本	修改
6.3	引入了此命令。

示例

以下示例显示如何显示 Netflow 运行时间计数器。

```
> show flow-export counters
destination: inside 209.165.200.224 2055
Statistics:
  packets sent                1000
Errors:
  block allocation failure    0
  invalid interface          0
  template send failure      0
  no route to collector      0
  source port allocation      0
```

Related Commands

命令	Description
clear flow-export counters	将 NetFlow 中的所有运行时间计数器重置为零。

show flow-offload

要查看流、计数器、统计信息以及有关分流的流的信息，请使用 **show flow-offload** 命令。

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

show flow-offload { **flow** [**count** | **detail**] | **dynamic** [**count** | **detail**] | **static** [**count** | **detail**] | **info** [**detail**] | **statistics** }

Syntax Description

flow [**dynamic** | **static**] | [**count** | **detail**] 无参数时，显示正在使用的静态和动态流、最大使用量、分流百分比和冲突数量。

添加 **dynamic** 或 **static** 关键字，以分别显示动态或静态流的计数器、统计信息和信息。

您可以选择添加以下关键字：

- **count**: 已分流的的活动流数和已创建的分流流数。
- **detail**: 活动的分流数据流及其重写规则和数据。

info [**detail**] 动态数据流分流的当前状态。添加 **detail** 关键字以获取其他信息，例如端口使用情况摘要。

statistics 数据包计数、成功传输和错误。

Command History

版本	修改
6.3	引入了此命令。

使用指南

使用 **show flow-offload** 命令显示流、计数器、统计信息和有关流分流的信息。

使用 **clear flow-offload** 命令清除计数器或统计信息。

以下是 **show flow-offload flow** 命令的输出示例。分流数据流由索引号标识，该索引号通过散列源和目的 IP 地址、端口和协议来计算。当系统尝试分流与当前活动分流的流具有相同索引的流时，会发生冲突。在这种情况下，不会分流新的数据流，但第一个数据流会保持分流状态。

```
>show flow-offload flow
Total offloaded flow stats: 1 in use, 5 most used, 100% offloaded, 0 collisions
UDP intf0 103 src 10.1.1.2:41110 dest 20.1.1.2:5001, dynamic, timestamp 162810457, packets
  84040, bytes 127404640
```

以下是 **show flow-offload flow count** 命令的输出示例。

```
>show flow-offload flow count
Total offloaded flow stats: 4 in use, 20 most used, 10% offloaded, 0 collisions
```


以下是 **show flow-offload flow detail** 命令的输出示例。rw(number) 表示已为该特定分流数据流重写标准报头字段，例如 MAC 或 VLAN。

```
>show flow-offload flow detail
Total offloaded flow stats: 2 in use, 6 most used, 100% offloaded, 0 collisions
TCP vlan 711 intfc 101 src 172.16.1.3:21766 dest 9.9.1.3:80, dynamic, timestamp 217959066,
  packets 633139, bytes 43053452
  node 0, ft index 58197, queue_id 727
  rw(0): cmd ' replace', offset 0, bytes 12, data(x) 90E2 BA01 8E29 B0AA 7730 097B
  rw(1): cmd 'increment', offset 46, bytes 4, data(x) 422AC658
```

以下是 **show flow-offload dynamic** 命令的输出示例。

```
>show flow-offload flow dynamic
Dynamically offloaded flow stats: 2 in use, 6 most used, 100% offloaded, 0 collisions
  TCP vlan 711 intfc 101 src 172.16.1.3:21809 dest 9.9.1.3:80, dynamic, timestamp 218392513,
  packets 14741, bytes 1002388
  TCP vlan 911 intfc 102 src 9.9.1.3:80 dest 172.16.1.3:21809, dynamic, timestamp 218392534,
  packets 16794, bytes 23972345
```

以下是 **show flow-offload dynamic count** 命令的输出示例。

```
>show flow-offload flow dynamic count
Dynamically offloaded flow stats: 2 in use, 6 most used, 100% offloaded, 0 collisions
```

以下是 **show flow-offload dynamic detail** 命令的输出示例。

```
>show flow-offload flow dynamic detail
Total offloaded flow stats: 4 in use, 20 most used, 10% offloaded, 0 collisions
TCP intfc 134 src 9.9.1.3:80 dest 192.168.0.3:5240, static, timestamp 142633202, packets
442870, bytes 630342730
TCP intfc 133 src 192.168.0.3:5240 dest 9.9.1.3:80, static, timestamp 142633204, packets
442971, bytes 28350144
TCP intfc 136 src 9.9.1.4:80 dest 192.168.0.4:7240, dynamic, timestamp 142633876, packets
82870, bytes 10342730
TCP intfc 135 src 192.168.0.4:7240 dest 9.9.1.4:80, dynamic, timestamp 142633877, packets
82971, bytes 350144
```

以下是 **show flow-offload info** 命令的输出示例。 **Current running state** 是流分流的当前状态，保留供将来实施（该值当前不可配置）。 **User configured state** 是受管设备重新启动时的数据流分流状态。（目前，这些值将始终相同。） **Dynamic flow offload** 是动态数据流分流的当前状态。

```
>show flow-offload flow info
Current running state      : Enabled
User configured state     : Enabled
Dynamic flow offload      : Enabled
```

以下是 **show flow-offload info detail** 命令的输出示例。

```
> show flow-offload flow info detail
Current running state      : Enabled
User configured state     : Enabled
Dynamic flow offload      : Enabled
Offload App                : Running
Offload allocated cores   : S0[ 1] S1[ 13]
Offload reserved Nic      : 9 22
Max PKT burst             : 32
Port-0 details :
  RX queue number         :          149
  FQ queue number         :          727
  Keep alive counter      :        142327
Port-1 details :
  RX queue number         :          147
```

```

FQ queue number      :          725
Keep alive counter   :        142328

```

以下是 **show flow-offload statistics** 命令的输出示例。VNIC 指在其上分流动态数据流的硬件。

```

> show flow-offload statistics
Packet stats of port : 0
Tx Packet count      :        16483549549
Rx Packet count      :        16483549549
Dropped Packet count :              0
VNIC transmitted packet :        16483549549
VNIC transmitted bytes :    12389816183297
VNIC Dropped packets :              0
VNIC erroneous received :              0
VNIC CRC errors      :              0
VNIC transmit failed :              0
VNIC multicast received :              0

```

Related Commands

命令	Description
configure flow-offload	启用或禁用动态数据流分流。
clear flow-offload	清除动态数据流分流计数器或统计信息。

show flow-offload-ipsec

要显示有关 IPsec 数据流分流的信息，请使用 **show flow-offload-ipsec**。

show flow-offload-ipsec { **info** | **option-table** | **statistics** }

Syntax Description	
info	显示有关 IPsec 流分流的当前配置状态的信息。
option-table	显示 IPsec 数据流分流中使用的内容可寻址内存 (CAM) 的表信息。此信息仅用于调试，对最终用户没有意义。
statistics	显示分流数据流的内容可寻址内存 (CAM) 统计信息。

Command History	版本	修改
	7.2	引入了此命令。

示例

以下示例显示 IPsec 流分流的当前配置状态。

```
ciscoasa# show flow-offload-ipsec info
IPSec offload : Enabled
Egress optimization: Enabled
```

以下示例显示统计信息。

```
> show flow-offload-ipsec statistics

Packet stats of Pipe 0
-----
Rx Packet count           :           0
Tx Packet count           :           0
Error Packet count        :           0
Drop Packet count         :           0

CAM stats of Pipe 0
-----
Option ID Table CAM Hit Count           :           38
Option ID Table CAM Miss Count          :          154
Tunnel Table CAM Hit Count              :           0
Tunnel Table CAM Miss Count             :           0
6-Tuple CAM Hit Count                   :           0
6-Tuple CAM Miss Count                   :           38
```

以下示例显示选项表。

```
> show flow-offload-ipsec option-table
instance_id:256 interface_id:124 action:0 logic_id_opt:0 subinterface_id_opt:0
```

```

instance_id:256 interface_id:123 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:122 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:121 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:120 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:119 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:118 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:117 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:156 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:157 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:158 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:159 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:112 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:111 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:110 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:109 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:108 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:107 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:106 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:105 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:104 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:103 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:102 action:0 logic_id_opt:0 subinterface_id_opt:0
instance_id:256 interface_id:101 action:0 logic_id_opt:0 subinterface_id_opt:0

```

Related Commands

命令	Description
clear flow-offload-ipsec	清除 IPsec 流量分流统计信息。

show fqdn

要显示有关完全限定域名 (FQDN) 网络对象名称解析的故障排除信息，请使用 **show fqdn** 命令。

```
show fqdn [id [fqdn_id] | ip [ip_address]]
```

Syntax Description

id [fqdn_id] 根据与 FQDN 网络对象关联的 ID 编号显示信息。ID 由系统分配。您可以选择包含 ID 值，通过检查 **show running-config** 命令的输出即可找到该值。例如，以下对象的 ID 编号为 1001。

```
object network www.example.com
fqdn www.example.com id 1001
```

ip [ip_address] 根据从 DNS 服务器获取的 IP 地址显示信息。您可以选择输入 IP 地址。

Command History

版本	修改
6.3	引入了此命令。

使用指南

使用此命令进行故障排除。如果要查看 FQDN 如何映射到 IP 地址，请使用 **show dns** 命令而不是此命令。

show fqdn 命令提供通过系统提供的每个对象的 ID 编号将名称解析与特定网络对象关联的详细信息。

示例

以下示例显示如何查看对象 ID 和 IP 地址的 FQDN 映射。

```
> show fqdn

FQDN IP Table:
ip=10.1.45.1, object=Testobj-1, domain=www.cisco.com, hits=10,
    id=45893456,63987645

ip=2001::134, object=Testobj-1, domain=www.cisco.com, hits=10,
    id=45893456

FQDN ID Table:
id=45893456, object=Testobj-1, domain=www.cisco.com
    ip=10.1.45.1, ip=34.12.45.189
    ip6=2001::134

id=23987645, object=Testobj-2, domain=www.google.com
    ip=20.11.65.121, ip=101.2.4.69
```

Related Commands

命令	Description
clear dns	删除 FQDN 网络对象 DNS 解析。
show dns	显示 FQDN 网络对象 DNS 解析。
show running-config	显示运行配置。

show fragment

要显示 IP 分片重组模块的操作数据，请输入 **show fragment**。

show fragment [*interface*]

Syntax Description	<i>interface</i> (可选) 指定 threat defense 接口。						
Command Default	如果未指定接口，则此命令应用于所有接口。						
Command History	<table border="1"> <thead> <tr> <th>版本</th> <th>修改</th> </tr> </thead> <tbody> <tr> <td>6.1</td> <td>引入了此命令。</td> </tr> <tr> <td>6.7</td> <td>增强了 show fragment 命令的输出，包括 IP 分段相关丢包和错误计数器。</td> </tr> </tbody> </table>	版本	修改	6.1	引入了此命令。	6.7	增强了 show fragment 命令的输出，包括 IP 分段相关丢包和错误计数器。
版本	修改						
6.1	引入了此命令。						
6.7	增强了 show fragment 命令的输出，包括 IP 分段相关丢包和错误计数器。						

示例

以下示例展示如何显示 IP 分段重组模块的操作数据：

```
> show fragment
Interface: inside
Configuration: Size: 200, Chain: 24, Timeout: 5, Reassembly: virtual
Run-time stats: Queue: 0, Full assembly: 12
Drops: Size overflow: 0, Timeout: 0,
Chain overflow: 0, Fragment queue threshold exceeded: 0,
Small fragments: 0, Invalid IP len: 0,
Reassembly overlap: 26595, Fraghead alloc failed: 0,
SGT mismatch: 0, Block alloc failed: 0,
Invalid IPV6 header: 0
```

其中：

- 大小：在已配置为默认值的任何给定点，允许驻留在分段数据库中的最大块数（每个接口）。
- 链 - 可将一个完整 IP 数据包分段为分片的最大数量。默认为 24。
- 超时 - 等待整个分段数据包到达的最大秒数。默认值为 5 秒。
- 重组：虚拟或完整。默认值为虚拟重组。在 ASA 处终止或需要在应用级别进行检测的 IP 分段将完全（物理）重组。如有必要，完全（物理）重组的数据包可以在出口接口上再次分片。
- 大小溢出：已达到任何给定点允许驻留在分段数据库中的最大块数。溢出计数器测量由于达到分段数据库的默认大小而导致的丢包。此计数器不包括由于队列大小（最大数据库大小的 2/3）而丢弃的分段数。
- 超时：片段链在重组完成之前已超时。
- 链限制：已达到单个分片链限制。

- 超出分段队列阈值：已超出分段数据库阈值，即每个接口的队列大小的 2/3。
- 小分片：分片偏移量大于 0 但小于 16 时。
- 数据包长度无效：IP 数据包长度无效（例如，长度大于 65535）。
- 重组重叠：检测到重复或重叠的片段。
- 分段标题分配失败：无法分配分段标题。分段标题维护 IP 数据包的所有分段链。
- SGT 不匹配：相同 IP 数据包的分段之间的 SGT 值不匹配。
- 块分配失败：完全重组的分配失败。
- 无效的 IPV6 信头：在完全重组期间遇到无效的 IPV6 信头。

Related Commands

命令	Description
clear configure fragment	清除 IP 分段重组配置并重置默认值。
clear fragment	清除 IP 分段重组模块的运行数据。
show running-config fragment	显示 IP 分段重组配置。

show gc

要显示垃圾收集进程统计信息，请使用 **show gc** 命令。

show gc

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show gc** 命令的输出示例：

```
> show gc
```

```
Garbage collection process stats:
Total tcp conn delete response      :          0
Total udp conn delete response      :          0
Total number of zombie cleaned      :          0
Total number of embryonic conn cleaned :          0
Total error response                 :          0
Total queries generated              :          0
Total queries with conn present response :          0
Total number of sweeps               :         946
Total number of invalid vcid         :          0
Total number of zombie vcid         :          0
```

Related Commands

命令	Description
clear gc	删除垃圾回收进程统计信息。

show h225

show h225 命令显示有关通过 threat defense 设备建立的 H.225 会话的信息。

show h225

Command History

版本	修改
6.1	引入了此命令。

使用指南

show h225 命令显示有关通过设备建立的 H.225 会话的信息。

如果存在异常大量的连接，请根据默认超时值或设置的超时值检查会话是否超时。如果未超时，则需要调查问题。

示例

以下是 **show h225** 命令的输出示例：

```
> show h225
Total H.323 Calls: 1
1 Concurrent Call(s) for
  Local: 10.130.56.3/1040 Foreign: 172.30.254.203/1720
  1. CRV 9861
  Local: 10.130.56.3/1040 Foreign: 172.30.254.203/1720
0 Concurrent Call(s) for
  Local: 10.130.56.4/1050 Foreign: 172.30.254.205/1720
```

此输出表示目前有 1 个活动 H.323 呼叫正通过本地终端 10.130.56.3 与外部主机 172.30.254.203 之间的 threat defense，而且对于这些特定终端，在它们之间有 1 个并发呼叫，该呼叫的 CRV 为 9861。

对于本地终端 10.130.56.4 和外部主机 172.30.254.205，有 0 个并发呼叫。这意味着即使 H.225 会话仍然存在，终端之间也没有活动呼叫。如果在执行 **show h225** 命令时呼叫已结束但 H.225 会话尚未删除，就可能会发生这种情况。它也可能意味着两个终端之间还有开启的 TCP 连接，因为这些终端将 “maintainConnection” 设置为 TRUE，所以在这些终端将 “maintainConnection” 重新设置为 FALSE 或在会话根据您配置中的 H.225 超时值超时之前，会话保持开启。

Related Commands

命令	Description
show h245	显示关于终端使用缓慢启动在设备范围内建立的 H.245 会话的信息。
show h323 ras	显示关于在设备范围内建立的 H.323 RAS 会话的信息。

show h245

要显示关于终端使用缓慢启动在 threat defense 设备范围内建立的 H.245 会话的信息，请使用 **show h245** 命令。

show h245

Command History

版本	修改
6.1	引入了此命令。

使用指南

show h245 命令显示关于终端使用缓慢启动在 threat defense 设备范围内建立的 H.245 会话的信息。（当呼叫的两个终端打开 H.245 的另一个 TCP 控制信道时，即为慢启动。当 H.245 消息作为 H.225 消息的一部分在 H.225 控制信道上交换时，即为快启动。

示例

以下是 **show h245** 命令的输出示例：

```
> show h245
Total: 1
      LOCAL          TPKT    FOREIGN          TPKT
1     10.130.56.3/1041    0      172.30.254.203/1245    0
      MEDIA: LCN 258 Foreign 172.30.254.203 RTP 49608 RTCP 49609
              Local   10.130.56.3 RTP 49608 RTCP 49609
      MEDIA: LCN 259 Foreign 172.30.254.203 RTP 49606 RTCP 49607
              Local   10.130.56.3 RTP 49606 RTCP 49607
```

目前有一个跨 threat defense 设备的 H.245 控制会话处于活动状态。本地终端是 10.130.56.3，来自此终端的下一个数据包预计将会包含 TPKT 报头，因为 TPKT 值为 0。（TKTP 信头是位于每条 H.225/H.245 消息之前的 4 字节信头。TKTP 信头提供消息长度，包括 4 字节信头在内。）外部主机终端是 172.30.254.203，来自此终端的下一个数据包预计将会包含 TPKT 报头，因为 TPKT 值为 0。

在这些终端之间协商的媒体的 LCN（逻辑信道编号）为 258，该 LCN 的外部 RTP IP 地址/端口对为 172.30.254.203/49608，RTCP IP 地址/端口对为 172.30.254.203/49609，本地 RTP IP 地址/端口对为 10.130.56.3/49608，RTCP 端口为 49609。

第二个 LCN 为 259，该 LCN 的外部 RTP IP 地址/端口对为 172.30.254.203/49606，RTCP IP 地址/端口对为 172.30.254.203/49607，本地 RTP IP 地址/端口对为 10.130.56.3/49606，RTCP 端口为 49607。

Related Commands

命令	Description
show h245	显示关于终端使用缓慢启动在 threat defense 设备范围内建立的 H.245 会话的信息。
show h323 ras	显示关于在 threat defense 设备范围内建立的 H.323 RAS 会话的信息。

show h323

要显示 H.323 连接的信息，请使用 **show h323** 命令。

show h323 {ras | gup}

Syntax Description	ras	gup
	显示在网守与其 H.323 终端之间跨 threat defense 设备建立的 H323 RAS 会话。	显示有关 H323 网关更新的协议连接的信息。
Command History	版本	修改
	6.1	引入了此命令。

使用指南

show h323 ras 命令显示有关越过 threat defense 设备在网守与其 H.323 终端之间建立的 H.323 RAS 会话的连接信息。

示例

以下是 **show h323 ras** 命令的输出示例：

```
> show h323 ras

Total: 1
      GK                               Caller
      172.30.254.214                   10.130.56.14
```

此输出显示网守 172.30.254.214 与其客户端 10.130.56.14 之间有一个活动注册。

Related Commands	命令	Description
	show h245	显示关于终端使用缓慢启动在 threat defense 设备范围内建立的 H.245 会话的信息。

show hardware-bypass

要显示 ISA 3000 上的当前硬件绕行状态，请使用 **show hardware-bypass** 命令。

show hardware-bypass

Command History

版本	修改
6.3	引入了此命令。

示例

以下是 **show hardware-bypass** 命令的输出示例。

```
> show hardware-bypass
      Status           Powerdown           Powerup
GigabitEthernet 1/1-1/2  Disable            Disable            Disable
GigabitEthernet 1/3-1/4  Disable            Disable            Disable

Pairing supported on these interfaces: gig1/1 & gig1/2, gig1/3 & gig1/4
```

show high-availability config

要查看有关高可用性（故障切换）配置的信息，请使用 **show high-availability config** 命令。

show high-availability config

Command History

版本	修改
6.1	引入了此命令。

使用指南

show high-availability config 命令是 **show failover** 命令的别名。有关详细信息，请参阅 **show failover** 的参考页面。

示例

以下示例显示了处于主用/备用故障切换模式的设备的故障切换配置。

```
> show high-availability config
Failover On
Failover unit Primary
Failover LAN Interface: failover GigabitEthernet0/2 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 61 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.7(0)74, Mate 9.7(0)74
Serial Number: Ours 9A41CKDXQJU, Mate 9A3MFP0H1CP
Last Failover at: 19:23:17 UTC Oct 26 2016
  This host: Primary - Active
    Active time: 2009 (sec)
    slot 0: empty
      Interface diagnostic (0.0.0.0): Normal (Waiting)
      Interface outside (192.168.77.1): Normal (Waiting)
      Interface inside (192.168.87.1): Normal (Waiting)
    slot 1: snort rev (1.0) status (up)
    slot 2: diskstatus rev (1.0) status (up)
  Other host: Secondary - Standby Ready
    Active time: 0 (sec)
    Interface diagnostic (0.0.0.0): Normal (Waiting)
    Interface outside (0.0.0.0): Normal (Waiting)
    Interface inside (0.0.0.0): Normal (Waiting)
    slot 1: snort rev (1.0) status (up)
    slot 2: diskstatus rev (1.0) status (up)

Stateful Failover Logical Update Statistics
Link : failover GigabitEthernet0/2 (up)
Stateful Obj  xmit      xerr      rcv        rerr
General      235         0         234        0
sys cmd      234         0         234        0
up time      0           0         0          0
RPC services 0           0         0          0
TCP conn     0           0         0          0
```

```

UDP conn          0          0          0          0
ARP tbl           0          0          0          0
Xlate_Timeout    0          0          0          0
IPv6 ND tbl      0          0          0          0
VPN IKEv1 SA     0          0          0          0
VPN IKEv1 P2    0          0          0          0
VPN IKEv2 SA     0          0          0          0
VPN IKEv2 P2    0          0          0          0
VPN CTCP upd     0          0          0          0
VPN SDI upd      0          0          0          0
VPN DHCP upd     0          0          0          0
SIP Session      0          0          0          0
SIP Tx           0          0          0          0
SIP Pinhole      0          0          0          0
Route Session    0          0          0          0
Router ID        0          0          0          0
User-Identity    1          0          0          0
CTS SGTNAME      0          0          0          0
CTS PAC          0          0          0          0
TrustSec-SXP     0          0          0          0
IPv6 Route       0          0          0          0
STS Table        0          0          0          0

```

Logical Update Queue Information

```

          Cur      Max      Total
Recv Q:   0       10      234
Xmit Q:   0       11     1200

```

以下示例显示了设备当前未配置故障切换的情况。第一行表示故障切换已关闭，是此输出中唯一有意义的部分。

```

> show high-availability config
Failover Off
Failover unit Secondary
Failover LAN Interface: not Configured
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 12 of 160 maximum
MAC Address Move Notification Interval not set

```

Related Commands

命令	Description
show failover	显示故障转移（高可用性）配置。

show https-access-list

show https-access-list 命令显示设备上配置的 HTTPS 访问列表。

show https-access-list

Command History

版本	修改
6.1	引入了此命令。

使用指南

HTTPS 访问列表确定哪些地址可以与使用 **configure network ipv4/ipv6** 命令配置的管理接口建立 HTTPS 连接。使用 HTTPS 连接以使用本地管理器、设备管理器来配置和管理设备。

此访问列表不控制通过设备的流量或对数据接口的 HTTPS 访问。

示例

以下示例显示管理接口的 HTTPS 访问列表。

```
> show https-access-list
ACCEPT tcp -- anywhere          anywhere          state NEW tcp dpt:https
ACCEPT tcp      anywhere          anywhere          state NEW tcp dpt:https
```

Related Commands

命令	Description
configure https-access-list	在管理接口上配置 HTTPS 访问列表。

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。