pa - pn

packet-tracer

可在特权 EXEC 模式下使用 packet-tracer 命令，以根据防火墙的当前配置生成 5 到 6 元组数据包。为了清楚起见，数据包跟踪器语法分别针对 ICMP、TCP/UDP/SCTP 和 IP 数据包建模显示。您可以使用 **pcap** 关键字重放多个数据包并跟踪完整的工作流程。

packet-tracer input*ifc_name* [**vlan-id***vlan_id*] **icmp** [**inline-tag***tag*]
{*src_ip* | **user***username* | **security-group** {**name***name* | **tag***tag*} | **fqdn***fqdn_string*} *icmp_value* [*icmp_code*]
[*dmac*] {*dst_ip* | **security-group** {**name***name* | **tag***tag*} | **fqdn***fqdn_string*} [**detailed**] [**xml**]

packet-tracer input*ifc_name* [**vlan-id***vlan_id*] **rawip** [**inline-tag***tag*]
{*src_ip* | **user***username* | **security-group** {**name***name* | **tag***tag*} | **fqdn***fqdn_string*} 协议 [*dmac*]
{*dst_ip* | **security-group** {**name***name* | **tag***tag*} | **fqdn***fqdn_string*} [**detailed**] [**xml**]

packet-tracer input*ifc_name* [**vlan-id***vlan_id*] {**tcp** | **udp** | **sctp**}
[**inline-tag***tag*] {*src_ip* | **user***username* | **security-group** {**name***name* | **tag***tag*}
| **fqdn***fqdn_string*} *src_port* [*dmac*]
{*dst_ip* | **security-group** {**name***name* | **tag***tag*} | **fqdn***fqdn_string*} *dst_port* [选项] [**detailed**] [**xml**]

packet-tracer
input*ifc_name* **pcap***pcap_filename* [**bypass-checks** | **decrypted** | **detailed** | **persist** | **transmit** | **xml** | **json** | **force**]

Syntax Description

bypass-checks	（可选）绕过针对模拟数据包的安全检查。
decrypted	（可选）将模拟数据包视为 IPsec/SSL VPN 解密。
detailed	（可选）提供详细的跟踪结果信息。
dmac	指定目的MAC地址。通过显示输出接口选择以及由于未知目标MAC地址而导致的丢包，提供交换数据包整个生命周期的全过程。
dst_ip	指定数据包跟踪的目标 IPv4 或 IPv6 地址。
dst_port	指定 TCP/UDP/SCTP 数据包跟踪的目标端口。根据端口，您可能有其他选项，包括 **vxlan**和 **geneve**内部数据包。
fqdn*fqdn_string*	指定主机的完全限定域名，该主机可以是源 IP 地址和目标 IP 地址。仅支持 IPv4 的 FQDN。
force	删除现有的 pcap 跟踪并执行新的 pcap 文件。
icmp	指定要使用的协议为 ICMP。
icmp_type	指定 ICMP 数据包跟踪的 ICMP 代码。确保使用 ICMPv6 数据包跟踪器的 V6 类型。
icmp_code	指定与ICMP数据包跟踪器的类型对应的ICMP代码。确保使用ICMPv6数据包跟踪器的 V6 代码。

input*ifc_name*	指定数据包的入口接口。
inline-tag*tag*	指定要嵌入第 2 层 CMD 信头中的安全组标记值。有效值范围为 0 – 65533。
json	（可选）以 JSON 格式显示跟踪结果。
pcap	指定 pcap 作为输入。
pcap_filename	包含要跟踪的数据包的 pcap 文件名。
protocol	指定原始 IP 数据包跟踪的协议编号，从 0 到 255。
persist	（可选）启用长期跟踪，并在集群中进行跟踪。
rawip	指定要使用的协议为原始 IP。
sctp	指定要使用的协议为 SCTP。
security-group {**name***name* | **tag***tag* }	指定基于用于 Trustsec 的 IP-SGT 查找的源安全组和目标安全组。您可以指定安全组名称或标签编号。
src_port	指定 TCP/UDP/SCTP 数据包跟踪的源端口。
src_ip	指定数据包跟踪的源 IPv4 或 IPv6 地址。
tcp	指定要使用的协议为 TCP。
transmit	（可选）允许从设备传输模拟数据包
type	指定 ICMP 数据包跟踪的 ICMP 代码。
udp	指定要使用的协议为 UDP。
user用户名	如果要将用户指定为源 IP 地址，请以“域\用户”格式指定用户身份。跟踪中使用最近为用户映射的地址（如有）。
vlan-id*vlan_id*	（可选）指定数据流的 VLAN 身份。值的范围是 1 - 4096。
xml	（可选）以 XML 格式显示跟踪结果。

Command Default 此命令没有默认设置。

Command Modes 下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
特权执行模式	• 是	• 支持	• 支持	• 支持	• 支持

Command History

版本	修改
7.2(1)	添加了此命令。
8.4(2)	增加了两个关键字-参数对：user *username* 和 fqdn *fqdn_ string* 。重命名和重新定义了多个关键字。添加了对 IPv6 源地址的支持。
9.0(1)	增加了对用户身份的支持。仅支持 IPv4 完全限定域名 (FQDN)。
9.3(1)	添加了 **inline-tag**标记 关键字-参数对，以支持嵌入到第 2 层 CMD 报头中的安全组标记值。
9.4(1)	增加了两个关键字参数对： **vlan-id***vlan_id* 和 **vxlan-inner***vxlan_inner_tag* 。
9.5(2)	已添加 sctp 关键字。
9.7(1)	支持透明防火墙模式。引入了用于目标 MAC 地址的新跟踪模块。
9.9.(1)	引入了对集群持久跟踪的支持。使用该功能可跟踪集群设备上的数据包。添加了新的选项：persistent、bypass-checks、decrypted、transmit、id 和 origin。
9.14(1)	增强了数据包跟踪器输出，以提供在路由数据包时允许/丢弃数据包的具体原因。
9.17(1)	增强了 packet-tracer 命令，以允许 pcap 文件作为跟踪的输入。还添加了对 **geneve**的支持。
7.6	启用对象组搜索后，对象组搜索阶段中会添加更多详细信息。

使用指南

除了使用捕获命令捕获数据包之外，还可以通过ASA跟踪数据包的生命周期，以查看其是否按预期运行。packet-tracer 命令使您能够执行以下操作：

- 调试生产网络中的所有数据包丢失。
- 验证配置是否达到预期。
- 显示适用于数据包和导致规则添加的 CLI 行的所有规则。
- 显示数据路径中数据包更改时间线。

- 将跟踪数据包注入数据路径。
- 根据用户身份和 FQDN 搜索 IPv4 或 IPv6 地址。
- 跨集群节点调试数据包。

该**packet-tracer**命令提供有关数据包以及 ASA 如何处理它们的详细信息。该实用程序的强大之处在于能够通过使用协议和端口信息指定源地址和目标地址来模拟真实世界的流量。 **packet-tracer**允许防火墙管理员将虚拟数据包注入安全设备并跟踪从入口到出口的流量。在此过程中，将根据流和路由查找、协议检查和 NAT 对数据包进行评估。

记住
- 在现有连接上执行数据包跟踪器时，跟踪器不会查阅 ACL。
- 在集群环境中，必须在入口、出口、asp 和 集群上执行同时数据包捕获。

可选的 **vlan-id** 关键字允许数据包跟踪器进入父接口，父接口稍后会重定向到与 VLAN 身份匹配的子接口。VLAN 身份是仅适用于非子接口的可选条目。管理接口是一个例外，其中父管理专用接口只能有管理专用子接口。

可以进行目的 MAC 地址查找。

在透明防火墙模式下，当输入接口为VTEP时，如果在VLAN中输入一个值，则可以选择性地启用目标MAC地址。而在网桥组成员接口中，目标 MAC 地址为必填字段，但在输入 vlan-id 时则为可选字段。

在路由防火墙模式下，当输入接口为桥接组成员接口时，vlan-id 关键字和 dmac 参数是可选的。

下表提供了分别在透明和路由防火墙模式下有关 VLAN 身份和目标 MAC 地址的接口相关行为的完整信息。

Transparentfirewallmode:

接口	**VLAN**	目标 **MAC** 地址
管理	已启用（可选）	禁用
VTEP	已启用（可选）	已禁用。当用户在VLAN中输入值时，系统将启用目的MAC地址，但该地址是可选的。
网桥虚拟接口(BVI)	已启用（可选）	已启用（强制）。当用户在 VLAN 中输入值时，目的 MAC 地址为可选。

Routedfirewallmode:

接口	**VLAN**	目标 **MAC** 地址
管理	已启用（可选）	禁用

接口	VLAN	目标 MAC 地址
路由接口	已启用（可选）	禁用
桥接组成员	已启用（可选）	已启用（可选）

当您使用输入入口接口运行 **packet-tracer** 命令时，如果数据包未被丢弃，则数据包会经历不同的阶段，例如 UN-NAT、ACL、NAT、IP-OPTIONS 和 FLOW-CREATION。系统将显示生成的消息：“ALLOW”。

在防火墙配置可能导致实时流量被丢弃的情况下，模拟的跟踪器数据包也将被丢弃。在某些情况下，将会提供特定丢弃原因。例如，如果由于无效的标头验证而丢弃数据包，则会出现以下消息：“由于错误的 IP 标头（原因）而丢弃数据包。”如果目标 MAC 地址未知，则交换顺序中的数据包会被丢弃。它启动 ASA 以搜索目标 MAC 地址。如果找到目标 MAC 地址，则可以再次执行 packet-tracer，并且 L2 查找成功。

通过 packet-tracer 中的 VXLAN 和 Geneve 支持，您可以指定内部数据包第 2 层源和目标 MAC 地址、第 3 层源和目标 IP 地址、第 4 层协议、第 4 层源和目标端口号以及虚拟网络接口 (VNI)。号码。内部数据包仅支持 TCP、SCTP、UDP、原始 IP 和 ICMP。

您可以使用域/用户格式为源指定用户身份。ASA 搜索用户的 IP 地址并将其用于数据包跟踪测试。如果用户映射到多个 IP 地址，则使用最新的登录 IP 地址，并且输出显示存在更多 IP 地址-用户映射。如果在此命令的源部分指定了用户身份，则 ASA 将根据用户输入的目标地址类型搜索用户的 IPv4 或 IPv6 地址。

您可以指定安全组名称或安全组标记作为源。ASA 会根据安全组名称或安全组标记搜索 IP 地址，并在数据包跟踪测试中使用该地址。如果安全组标记或安全组名称映射到多个 IP 地址，则使用其中一个 IP 地址，输出显示存在更多 IP 地址到安全组标记映射。

您还可以将 FQDN 指定为源地址和目标地址。ASA 先执行 DNS 查找，然后为数据包构建检索第一个返回的 IP 地址。

对于第 3 层到桥接虚拟接口以及桥接虚拟接口到桥接虚拟接口等流量场景（其中目标 IP 是通过 ASA 上的 BVI 接口进行的下一跳），数据包跟踪器会执行双重 ROUTE-LOOKUP。此外，也不会创建流。

在清除 ARP 和 MAC 地址表条目的情况下，数据包跟踪器始终执行两次 ROUTE-LOOKUP，然后解析目标 MAC 地址并将其存储在数据库中。而对于任何其他流量场景则不是这种情况。如果目标 MAC 地址为 L3 接口，则永远不会解析该地址并将其存储在数据库中。由于 BVI 接口是使用 *nameif* 进行配置并具有 L3 属性，因此不应执行 DMAC 查找。

此行为仅在第一次尝试、没有 MAC 地址和 ARP 条目时出现。显示 DMAC 的条目后，数据包跟踪器输出将符合预期。系统将创建流。

通过持久跟踪，可以跟踪在集群设备之间传递的数据包。必须使用 persist 选项注入您想要跨集群单元跟踪的数据包。每个数据包的持久跟踪配备数据包 id 和跳数，可以通过集群节点确定注入的数据包来源和数据包跳数阶段。packet-id 是下列各项的组合<node name of the device where the packet originated>和一个递增编号。对于在节点上首次接收的每个新数据包，数据包 ID 是唯一的。每当数据包从一个集群成员移动到另一个集群成员时，都会填充跳数计数。例如，集群中的数据包根据外部负载均衡编号列表到达成员。Host-1 向 Host-2 发送数据包。注入的数据包在发送到 Host-2 之前，

会在集群节点之间重定向。元数据输出分别显示 Tracer origin-id B:7 hop 0、Tracer origin-id B:7 hop 1 和 Tracer origin-id B:7 hop 2。其中 B 是数据包源自的集群节点的名称。7 是递增的数字，表示这是源自此集群节点的第 7 个数据包。此数字随着从此节点发出的每个新数据包而增加。“B”和“7”一起构成用于标识数据包的唯一 id。集群设备本地名称对于通过此设备传递的每个数据包都是相同的。当全局缓冲区使用 unique-id 和跳数时，可区分每个数据包。跟踪数据包后，每个节点上将提供持久跟踪，直到您手动丢弃它们以释放一些内存。情景中已启用的持久跟踪存储在每个情景的缓冲区中。将来源所有者 ID（两个值<origin-owner><id>），以便在跟踪集中查找跟踪。

可以允许模拟数据包离开 ASA。通过 packet-tracer 使用传输选项，可以在网络上传输数据包。默认情况下，数据包跟踪器会在传输数据包之前丢弃该数据包。传出数据包后，会在流表中生成流。

通过 packet-tracer 使用 bypass-checks 选项，可以绕过 ACL、VPN 过滤器、uRPF 和 IPsec 欺骗检查。它同时适用于入口和出口条件，并且不会丢弃模拟的 IPsec 数据包。

可以将已解密的数据包注入 VPN 隧道，这是通用的，适用于 IPSec 和 TLS。还可以模拟通过 VPN 隧道的数据包。模拟的“已解密”数据包将与现有的VPN隧道进行匹配，并应用关联的隧道策略。但是，此功能不适用于基于路由的 VPN 隧道。

packet-tracer 注入和跟踪单个数据包时，使用 **pcap** 关键字可使数据包跟踪器重放多个数据包（最多 100 个数据包）并跟踪整个数据流。您可以提供 pcap 文件作为输入，并以 XML 或 JSON 格式获取结果以进行进一步分析。要清除跟踪输出，请使用 **clear packet-tracer** 的 **pcap trace** 子命令。在跟踪过程中，您无法使用跟踪输出。

当您重放包含 Dot1q 标记数据包的 **pcap** 时，请确保数据包包含在防火墙上配置的传输子接口的标签。

以下示例显示当前行为：

```
------ INSIDE (VLAN 100) FTD (VLAN 200) OUTSIDE ------
```

如果在 INSIDE 子接口上注入 TCP SYN 数据包，则该数据包的 Dot1q 标记必须为 VLAN 100。同样，返回流量（例如，TCP SYN/ACK）的 Dot1q 标记中必须包含 VLAN 200。

注释 如果重放 INSIDE 接口上的捕获，并且所有数据包的 Dot1q 标签中都有 VLAN 100，则重放将失败（SYN/ACK 也将注入 INSIDE 子接口）。

以下示例显示如何使用 pcap 文件作为输入运行 packet-tracer：

```
ciscoasa# packet-tracer input inside pcap http_get.pcap detailed xml
```

以下示例显示如何通过清除现有的 pcap 跟踪缓冲区并提供 pcap 文件作为输入来运行 packet-tracer：

```
ciscoasa# packet-tracer input inside pcap http_get.pcap force
```

CR_Examples

以下示例跟踪来自内部接口的 ICMP 数据包。结果表明，由于反向路径验证失败（RPF），数据包被丢弃。失败的原因可能是流量从路由表已知但与内部接口关联的地址进入外部接

口。同样，如果流量从未知源地址进入内部接口，则设备会丢弃数据包，因为匹配的路由（默认路由）指示外部接口。

```
ciscoasa#  packet-tracer input inside icmp 10.15.200.2 8 0$

Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0xd793b4a0, priority=12, domain=capture, deny=false
        hits=621531641, user_data=0xd7bbe720, cs_id=0x0, l3_type=0x0
        src mac=0000.0000.0000, mask=0000.0000.0000
        dst mac=0000.0000.0000, mask=0000.0000.0000

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0xd7dc31d8, priority=1, domain=permit, deny=false
        hits=23451445222, user_data=0x0, cs_id=0x0, l3_type=0x8
        src mac=0000.0000.0000, mask=0000.0000.0000
        dst mac=0000.0000.0000, mask=0100.0000.0000

Phase: 3
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in   10.15.216.0     255.255.252.0   inside

Phase: 4
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in   0.0.0.0         0.0.0.0         outside


Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: inside
output-status: up
output-line-status: up
Action: drop
Drop-reason: (rpf-violated) Reverse-path verify failed
```

以下示例跟踪从 201.1.1.1 到 202.1.1.1 的 HTTP 端口的 TCP 数据包。

```
ciscoasa# packet-tracer input inside tcp 201.1.1.1 13 202.1.1.1 324 000c.29a3.b07a detailed
Result:
Action: drop
Drop-reason: (dst-l2_lookup-fail) Dst MAC L2 Lookup Failed
```

```
ciscoasa# packet-tracer input inside tcp 201.1.1.1 13 202.1.1.1 324 000c.29a3.b07a detailed
Phase: 1
Type: L2-EGRESS-IFC-LOOKUP
Subtype: Destination MAC Address Lookup
Result: ALLOW
Config:
Additional Information:
Destination MAC address lookup resulted in egress ifc outside
Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
Forward Flow based lookup yields rule:
in  id=0x7fdbe83542f0, priority=1, domain=permit, deny=false
hits=7313, user_data=0x0, cs_id=0x0, l3_type=0x8
src mac=0000.0000.0000, mask=0000.0000.0000
dst mac=0000.0000.0000, mask=0100.0000.0000
input_ifc=inside, output_ifc=any
Phase: 3
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group ALLOW global
access-list ALLOW extended permit ip any any
Additional Information:
Forward Flow based lookup yields rule:
in  id=0x7fdbd94026a0, priority=12, domain=permit, deny=false
hits=8, user_data=0x7fdbf07cbd00, cs_id=0x0, use_real_addr,
flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=any, output_ifc=any
Phase: 4
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in  id=0x7fdbd90a2990, priority=0, domain=nat-per-session, deny=false
hits=10, user_data=0x0, cs_id=0x0, reverse, use_real_addr,
flags=0x0, protocol=6
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=any, output_ifc=any
Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in  id=0x7fdbe8363790, priority=0, domain=inspect-ip-options, deny=true
hits=212, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=inside, output_ifc=any
Phase: 6
Type: NAT
       Subtype: per-session
```

```
Result: ALLOW
Config:
Additional Information:

Reverse Flow based lookup yields rule:
in  id=0x7fdbd90a2990, priority=0, domain=nat-per-session, deny=false
hits=12, user_data=0x0, cs_id=0x0, reverse, use_real_addr,
flags=0x0, protocol=6
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Reverse Flow based lookup yields rule:
in  id=0x7fdbd93dfc10, priority=0, domain=inspect-ip-options, deny=true
hits=110, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=outside, output_ifc=any
Phase: 8
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 221, packet dispatched to next module
Module information for forward flow …
snp_fp_tracer_drop
snp_fp_inspect_ip_options
snp_fp_tcp_normalizer
snp_fp_translate
snp_fp_tfw
snp_fp_fragment
snp_ifc_stat
Module information for reverse flow …
snp_fp_tracer_drop
snp_fp_inspect_ip_options
snp_fp_tcp_normalizer
snp_fp_translate
snp_fp_tfw
snp_fp_fragment
snp_ifc_stat
Result:
input-interface: inside
input-status: up
input-line-status: up
Action: allow
44# command example
ciscoasa(config)# command example
resulting screen display here
<Text omitted.>
```

以下示例跟踪从 10.100.10.10 到 10.100.11.11 的 HTTP 端口的 TCP 数据包。结果表明隐式拒绝访问规则将丢弃该数据包。

```
ciscoasa(config)# packet-tracer input outside tcp 10.100.10.10  80 10.100.11.11 80
Phase: 1
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
```

```
Config:
Additional Information:
found next-hop 10.86.116.1 using egress ifc  outside
Phase: 2
Type: ACCESS-LIST
Subtype:
Result: DROP
Config:
Implicit Rule
Additional Information:
Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
output-status: up
output-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule
```

以下示例显示如何使用用户名 CISCOabc 跟踪从内部主机 10.0.0.2 到外部主机 20.0.0.2 的数据包：

```
ciscoasa# packet-tracer input inside icmp user CISCO\abc 0 0 1 20.0.0.2
Source: CISCO\abc 10.0.0.2
Phase: 1
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in 20.0.0. 255.255.255.0 outside
...
Result:
input-interface: inside
input-status: up
input-line-status: up
output-interfce: outside
output-status: up
output-line-status: up
Action: allow
```

以下示例显示如何跟踪来自用户名为 CISCO\abc 的内部主机 20.0.0.2 的数据包，并以 XML 格式显示跟踪结果：

```
<Source>
<user>CISCO\abc</user>
<user-ip>10.0.0.2</user-ip>
<more-ip>1</more-ip>
</Source>
<Phase>
<id>1</id>
<type>ROUTE-LOOKUP</type>
<subtype>input</subtype>
<result>ALLOW</result>
<config>
</config>
<extra>
in 20.0.0.0 255.255.255.0 outside
</extra>
</Phase>
```

以下示例显示如何跟踪从内部主机 xyz.example.com 到外部主机 abc.example.com 的数据包。

```
ciscoasa# packet-tracer input inside tcp fqdn xyz.example.com 1000 fqdn abc.example.com 23
Mapping FQDN xyz.example.com to IP address 10.0.0.2
(More IP addresses resolved. Please run “show dns-host” to check.)
Mapping FQDN abc.example.com to IP address 20.0.0.2
(More IP addresses resolved. Please run “show dns-host” to check.)
Phase: 1
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
```

以下示例显示该命令的 **packet-tracer**输出，以显示安全组标签映射到 IP 地址：

```
ciscoasa# packet-tracer input inside tcp security-group name alpha 30 security-group tag
31 300
Mapping security-group 30:alpha to IP address 10.1.1.2.
Mapping security-group 31:bravo to IP address 192.168.1.2.
Phase: 1
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in 192.168.1.0 255.255.255.0 outside....
----------------More---------------------
```

以下示例显示 **packet-tracer** 命令的输出，显示第 2 层 SGT 实施：

```
ciscoasa# packet-tracer input inside tcp inline-tag 100 10.1.1.2 30 192.168.1.2 300
```

以下示例概述 VXLAN 对 UDP/TCP 和 ICMP 内部数据包的支持

```
packet-tracer in inside udp 30.0.0.2 12345 30.0.0.100 vxlan vxlan-inner 1234 1.1.1.1 11111
 2.2.2.2 22222 aaaa.bbbb.cccc aaaa.bbbb.dddd detailedOuter packet: UDP from 30.0.0.2 to
30.0.0.100 (vtep/nve source-interface IP) with default vxlan destination port.
Inner packet: VXLAN in-tag 1234, UDP from 1.1.1.1/11111 to 2.2.2.2/22222 with smac
aaaa.bbbb.cccc and dmac aaaa.bbbb.dddd
```

以下示例显示在集群设备之间传递持久跟踪时的输出：

```
ciscoasa# cluster exec show packet-tracer
B(LOCAL):**********************************************************
tracer 10/8 (allocate/freed), handle 10/8 (allocated/freed), error 0
=======  Tracer origin-id B:7, hop 0 =======
packet-id: icmp src inside:15.11.1.122 dst 15.11.2.124 (type 0, code 0)
<Snipping phase 1-3: CAPTURE, ACCESS-LIST, ROUTE-LOOKUP>
Phase: 4
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'inside'
Flow type: NO FLOW
I (1) am asking director (0).
Phase: 5
Type: CLUSTER-EVENT
```

```
Subtype: forward
Result: ALLOW
Config:
Additional Information:
To A(0), cq_type CQ_FLOW_OWNER_REQUEST(17), flags 0, frag-cnt 0, trace-options 0x10
=======  Tracer origin-id B:7, hop 2 =======
packet-id: icmp src inside:15.11.1.122 dst 15.11.2.124 (type 0, code 0)
<Snipping phase 1-3: CAPTURE, ACCESS-LIST, ROUTE-LOOKUP>
Phase: 1
Type: CLUSTER-EVENT
Subtype: receive
Result: ALLOW
Config:
Additional Information:
From A(0), cq_type CQ_FLOW_OWNER_REPLY(18), flags 0, frag-cnt 0, trace-options 0x10
<Snipping phase 2-4: CAPTURE, ACCESS-LIST, ROUTE-LOOKUP>
Phase: 5
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'inside'
Flow type: NO FLOW
I (1) have been elected owner by (0).
<Snipping phase 6-16: ACCESS-LIST, NAT, IP-OPTIONS, INSPECT, INSPECT, FLOW-CREATION,
ACCESS-LIST, NAT, IP-OPTIONS, ROUTE-LOOKUP, ADJACENCY-LOOKUP>
A:*********************************************************************
tracer 6/5 (allocate/freed), handle 6/5 (allocated/freed), error 0
=======  Tracer origin-id B:7, hop 1 =======
packet-id: icmp src inside:15.11.1.122 dst 15.11.2.124 (type 0, code 0)
Phase: 1
Type: CLUSTER-EVENT
Subtype: receive
Result: ALLOW
Config:
Additional Information:
From B(1), cq_type CQ_FLOW_OWNER_REQUEST(17), flags 0, frag-cnt 0, trace-options 0x10
<Snipping phase 2-7: CAPTURE, ACCESS-LIST, ROUTE-LOOKUP, ACCESS-LIST, NAT, IP-OPTIONS>
Phase: 8
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'inside'
Flow type: NO FLOW
I (0) am director, not creating dir flow for ICMP pkt recvd by (1).
Phase: 9
Type: CLUSTER-EVENT
Subtype: forward
Result: ALLOW
Config:
Additional Information:
To B(1), cq_type CQ_FLOW_OWNER_REPLY(18), flags 0, frag-cnt 0, trace-options 0x10
ciscoasa#
```

以下示例显示使用 origin 和 id 选项从集群节点跟踪数据包时的输出：

```
cluster2-asa5585a# cluster exec show packet-tracer | i origin-id
b(LOCAL):*********************************************************
=======  Tracer origin-id b:2, hop 0 =======
=======  Tracer origin-id b:2, hop 2 =======
a:*********************************************************************
```

```
=======  Tracer origin-id a:17, hop 0 =======
=======  Tracer origin-id b:2, hop 1 =======
=======  Tracer origin-id b:2, hop 3 =======
cluster2-asa5585a#
cluster2-asa5585a# cluster exec show packet-tracer ori
cluster2-asa5585a# cluster exec show packet-tracer origin b id 2
b(LOCAL):************************************************************
tracer 3/1 (allocate/freed), handle 3/1 (allocated/freed), error 0
=======  Tracer origin-id b:2, hop 0 =======
packet-id: icmp src outside2:212.1.1.9 dst 214.1.1.10 (type 8, code 0)
Phase: 1
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list
Phase: 2
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 214.1.1.10 using egress ifc  identity
Phase: 3
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'outside2'
Flow type: NO FLOW
I (1) am asking director (0).
Phase: 4
Type: CLUSTER-EVENT
Subtype: forward
Result: ALLOW
Config:
Additional Information:
To a(0), cq_type CQ_FLOW_OWNER_REQUEST(17), flags 0, frag-cnt 0, trace-options 0x10
Result:
input-interface: outside2
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
Action: allow
=======  Tracer origin-id b:2, hop 2 =======
packet-id: icmp src outside2:212.1.1.9 dst 214.1.1.10 (type 0, code 0)

Phase: 1
Type: CLUSTER-EVENT
Subtype: receive
Result: ALLOW
Config:
Additional Information:
From a(0), cq_type CQ_FLOW_OWNER_REPLY(18), flags 0, frag-cnt 0, trace-options 0x10
Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
```

```
MAC Access list
Phase: 3
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 214.1.1.10 using egress ifc  identity
Phase: 4
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'outside2'
Flow type: NO FLOW
I (1) have been elected owner by (0).
Phase: 5
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 8
Type: CLUSTER-REDIRECT
Subtype: cluster-redirect
Result: ALLOW
Config:
Additional Information:
Phase: 9
Type:
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 10
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
Phase: 11
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
Phase: 12
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
```

```
Config:
Additional Information:
Phase: 13
Type: CLUSTER-REDIRECT
Subtype: cluster-redirect
Result: ALLOW
Config:
Additional Information:
Phase: 14
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'outside2'
Flow type: FULL
I (1) am redirecting to (0) due to matching action (1).
Phase: 15
Type: CLUSTER-EVENT
Subtype: forward
Result: ALLOW
Config:
Additional Information:
To a(0), cq_type CQ_FLOW(1), flags 0, frag-cnt 0, trace-options 0x10
Result:
input-interface: outside2
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
Action: allow
a:**********************************************************************
tracer 20/17 (allocate/freed), handle 20/17 (allocated/freed), error 0
=======  Tracer origin-id b:2, hop 1 =======
packet-id: icmp src outside2:212.1.1.9 dst 214.1.1.10 (type 0, code 0)
Phase: 1
Type: CLUSTER-EVENT
Subtype: receive
Result: ALLOW
Config:
Additional Information:
From b(1), cq_type CQ_FLOW_OWNER_REQUEST(17), flags 0, frag-cnt 0, trace-options 0x10
Phase: 2
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 214.1.1.10 using egress ifc  identity
Phase: 3
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
Phase: 4
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Phase: 5
Type: IP-OPTIONS
Subtype:
```

```
Result: ALLOW
Config:
Additional Information:
Phase: 6
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'outside2'
Flow type: NO FLOW
I (0) am director, found static rule to classify owner as (253).
Phase: 7
Type: CLUSTER-EVENT
Subtype: forward
Result: ALLOW
Config:
Additional Information:
To b(1), cq_type CQ_FLOW_OWNER_REPLY(18), flags 0, frag-cnt 0, trace-options 0x10
Result:
input-interface: outside2
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
Action: allow
=======  Tracer origin-id b:2, hop 3 =======
packet-id: icmp src outside2:212.1.1.9 dst 214.1.1.10 (type 0, code 0)
Phase: 1
Type: CLUSTER-EVENT
Subtype: receive
Result: ALLOW
Config:
Additional Information:
From b(1), cq_type CQ_FLOW(1), flags 0, frag-cnt 0, trace-options 0x10
Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list
Phase: 3
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 214.1.1.10 using egress ifc  identity
Phase: 4
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'outside2'
Flow type: NO FLOW
I (0) have been elected owner by (0).
Phase: 5
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
```

```
Additional Information:

Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 8
Type: CLUSTER-REDIRECT
Subtype: cluster-redirect
Result: ALLOW
Config:
Additional Information:
Phase: 9
Type:
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 10
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
Phase: 11
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
Phase: 12
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 13
Type: CLUSTER-REDIRECT
Subtype: cluster-redirect
Result: ALLOW
Config:
Additional Information:
Phase: 14
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
Phase: 15
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
Phase: 16
Type: VPN
```

```
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 17
Type:
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 18
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 70, packet dispatched to next module
Phase: 19
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 0.0.0.0 using egress ifc  identity
Phase: 20
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop IP address to MAC
Result: ALLOW
Config:
Additional Information:
found adjacency entry for Next-hop 0.0.0.0 on interface  outside
adjacency Active
mac address 0000.0000.0000 hits 1730 reference 6
Phase: 21
Type: SUBOPTIMAL-LOOKUP
Subtype: suboptimal next-hop
Result: ALLOW
Config:
Additional Information:
Input route lookup returned ifc  inside is not same as existing ifc  outside
Doing adjacency lookup lookup on existing ifc outside2
Result:
input-interface: outside2
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
Action: allow
cluster2-asa5585a#
cluster2-asa5585a#
cluster2-asa5585a#
cluster2-asa5585a# cluster exec show packet-tracer origin a
b(LOCAL):**************************************************************
tracer 3/1 (allocate/freed), handle 3/1 (allocated/freed), error 0
a:**************************************************************
tracer 20/17 (allocate/freed), handle 20/17 (allocated/freed), error 0
=======  Tracer origin-id a:17, hop 0 =======
packet-id: icmp src outside2:212.1.1.9 dst 214.1.1.10 (type 8, code 0)
Phase: 1
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 214.1.1.10 using egress ifc  identity
```

```
Phase: 2
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'outside2'
Flow type: NO FLOW
I (0) am becoming owner
Phase: 3
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
Phase: 4
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 6
Type: CLUSTER-REDIRECT
Subtype: cluster-redirect
Result: ALLOW
Config:
Additional Information:
Phase: 7
Type:
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 8
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
Phase: 9
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
Phase: 10
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 11
Type: CLUSTER-REDIRECT
Subtype: cluster-redirect
Result: ALLOW
Config:
Additional Information:
```

```
Phase: 12
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:

Phase: 13
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
Phase: 14
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 15
Type:
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 16
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 69, packet dispatched to next module
Phase: 17
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 0.0.0.0 using egress ifc  identity
Phase: 18
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop IP address to MAC
Result: ALLOW
Config:
Additional Information:
found adjacency entry for Next-hop 0.0.0.0 on interface  outside
adjacency Active
mac address 0000.0000.0000 hits 1577 reference 6
Result:
input-interface: outside2
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
Action: allow
cluster2-asa5585a#
cluster2-asa5585a# cluster exec show packet-tracer id 17
b(LOCAL):************************************************************
tracer 3/1 (allocate/freed), handle 3/1 (allocated/freed), error 0
a:************************************************************
tracer 20/17 (allocate/freed), handle 20/17 (allocated/freed), error 0
=======  Tracer origin-id a:17, hop 0 =======
packet-id: icmp src outside2:212.1.1.9 dst 214.1.1.10 (type 8, code 0)
Phase: 1
Type: ROUTE-LOOKUP
```

```
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 214.1.1.10 using egress ifc  identity
Phase: 2
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'outside2'
Flow type: NO FLOW
I (0) am becoming owner
Phase: 3
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
Phase: 4
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 6
Type: CLUSTER-REDIRECT
Subtype: cluster-redirect
Result: ALLOW
Config:
Additional Information:
Phase: 7
Type:
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 8
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
Phase: 9
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
Phase: 10
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 11
```

```
Type: CLUSTER-REDIRECT
Subtype: cluster-redirect
Result: ALLOW
Config:
Additional Information:
Phase: 12
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:

Phase: 13
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
Phase: 14
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 15
Type:
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 16
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 69, packet dispatched to next module
Phase: 17
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
Found next-hop 0.0.0.0 using egress ifc  identity
Phase: 18
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop IP address to MAC
Result: ALLOW
Config:
Additional Information:
found adjacency entry for Next-hop 0.0.0.0 on interface  outside
adjacency Active
mac address 0000.0000.0000 hits 1577 reference 6
Result:
input-interface: outside2
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
Action: allow
cluster2-asa5585a#
```

以下示例概述了如何从集群节点中清除持久跟踪：

```
ciscoasa# cluster exec clear packet-tracer
```

要在 IPSec 隧道中注入解密的数据包，需要满足一些条件。如果未协商 IPSec 隧道，系统会显示错误消息。第二次协商 IPSec 隧道后，数据包通过。

以下示例说明何时 **not** 协商 IPSec 隧道以注入解密数据包：

```
cluster2-asa5585a(config)# packet-tracer input outside tcp 211.1.1.1 5050 213.1.1.2 21
decrypted
  ********************************************************************
  WARNING: An existing decryption SA was not found. Please confirm the
  IPsec Phase 2 SA or Anyconnect Tunnel is established.
  ********************************************************************
  Phase: 1
  Type: ACCESS-LIST
  Subtype:
  Result: ALLOW
  Config:
  Implicit Rule
  Additional Information:
  MAC Access list
  Phase: 2
  Type: ROUTE-LOOKUP
  Subtype: Resolve Egress Interface
  Result: ALLOW
  Config:
  Additional Information:
  found next-hop 214.1.1.9 using egress ifc  outside2
  Phase: 3
  Type: CLUSTER-EVENT
  Subtype:
  Result: ALLOW
  Config:
  Additional Information:
  Input interface: 'outside'
  Flow type: NO FLOW
  I (0) got initial, attempting ownership.
  Phase: 4
  Type: CLUSTER-EVENT
  Subtype:
  Result: ALLOW
  Config:
  Additional Information:
  Input interface: 'outside'
  Flow type: NO FLOW
  I (0) am becoming owner
  Phase: 5
  Type: ACCESS-LIST
  Subtype: log
  Result: ALLOW
  Config:
  access-group ALLOW global
  access-list ALLOW extended permit ip any any
  Additional Information:
  Phase: 6
  Type: NAT
  Subtype: per-session
  Result: ALLOW
  Config:
  Additional Information:
  Phase: 7
  Type: IP-OPTIONS
  Subtype:
  Result: ALLOW
  Config:
```

```
  Additional Information:
  Phase: 8
  Type: INSPECT
  Subtype: inspect-ftp
  Result: ALLOW
  Config:
  class-map inspection_default
  match default-inspection-traffic
  policy-map global_policy
  class inspection_default
  inspect ftp
  service-policy global_policy global
  Additional Information:
  Phase: 9
  Type: VPN
  Subtype: ipsec-tunnel-flow
  Result: DROP
  Config:
  Additional Information:
  Result:
  input-interface: outside
  input-status: up
  input-line-status: up
  output-interface: outside2
  output-status: up
  output-line-status: up
  Action: drop
  Drop-reason: (acl-drop) Flow is denied by configured rule
  cluster2-asa5585a(config)#
```

以下示例说明何时协商 IPSec 隧道以注入解密数据包：

```
cluster2-asa5585a# packet-tracer input outside tcp 211.1.1.1 5050 213.1.1.2 21 decrypted
  Phase: 1
  Type: ROUTE-LOOKUP
  Subtype: Resolve Egress Interface
  Result: ALLOW
  Config:
  Additional Information:
  found next-hop 214.1.1.9 using egress ifc  outside2
  Phase: 2
  Type: CLUSTER-EVENT
  Subtype:
  Result: ALLOW
  Config:
  Additional Information:
  Input interface: 'outside'
  Flow type: NO FLOW
  I (0) got initial, attempting ownership.
  Phase: 3
  Type: CLUSTER-EVENT
  Subtype:
  Result: ALLOW
  Config:
  Additional Information:
  Input interface: 'outside'
  Flow type: NO FLOW
  I (0) am becoming owner
  Phase: 4
  Type: ACCESS-LIST
  Subtype: log
  Result: ALLOW
  Config:
  access-group ALLOW global
```

```
access-list ALLOW extended permit ip any any
Additional Information:
Phase: 5
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Phase: 6
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 7
Type: INSPECT
Subtype: inspect-ftp
Result: ALLOW
Config:
class-map inspection_default
 match default-inspection-traffic
policy-map global_policy
 class inspection_default
  inspect ftp
service-policy global_policy global
Additional Information:
Phase: 8
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 9
Type: INSPECT
Subtype: inspect-ftp
Result: ALLOW
Config:
class-map inspection_default
 match default-inspection-traffic
policy-map global_policy
 class inspection_default
  inspect ftp
service-policy global_policy global
Additional Information:
Phase: 10
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 11
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:
Phase: 12
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:
Phase: 13
Type: VPN
```

```
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 14
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Phase: 15
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 16
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 17
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Phase: 18
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 19
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:
Phase: 20
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:
Phase: 21
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 1099, packet dispatched to next module
Phase: 22
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 214.1.1.9 using egress ifc  outside2
Phase: 23
Type: ACCESS-LIST
Subtype:
Result: ALLOW
```

```
  Config:
  Implicit Rule
  Additional Information:
  Phase: 24
  Type: ACCESS-LIST
  Subtype:
  Result: ALLOW
  Config:
  Implicit Rule
  Additional Information:
  Phase: 25
  Type: FLOW-CREATION
  Subtype:
  Result: ALLOW
  Config:
  Additional Information:
  New flow created with id 1100, packet dispatched to next module
  Phase: 26
  Type: ROUTE-LOOKUP
  Subtype: Resolve Egress Interface
  Result: ALLOW
  Config:
  Additional Information:
  found next-hop 214.1.1.9 using egress ifc  outside2
Phase: 27
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop IP address to MAC
Result: ALLOW
Config:
Additional Information:
found adjacency entry for next-hop 214.1.1.9 on interface  outside
adjacency Active
mac address 4403.a74a.9a32 hits 99 reference 2
  Result:
  input-interface: outside
  input-status: up
  input-line-status: up
  output-interface: outside2
  output-status: up
  output-line-status: up
  Action: allow
```

以下示例使用传输 选项来允许模拟的数据包传出并在传出接口上捕获模拟的数据包：

```
cluster2-asa5585a(config)# packet-tracer input outside icmp 211.1.1.10 8 0 213.1.1.10
transmit
  Phase: 1
  Type: CAPTURE
  Subtype:
  Result: ALLOW
  Config:
  Additional Information:
  MAC Access list
  Phase: 2
  Type: ACCESS-LIST
  Subtype:
  Result: ALLOW
  Config:
  Implicit Rule
  Additional Information:
  MAC Access list
  Phase: 3
  Type: ROUTE-LOOKUP
  Subtype: Resolve Egress Interface
```

```
Result: ALLOW
Config:
Additional Information:
found next-hop 214.1.1.9 using egress ifc  outside2

Phase: 4
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'outside'
Flow type: NO FLOW
I (0) am becoming owner
Phase: 5
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group ALLOW global
access-list ALLOW extended permit ip any any
Additional Information:
Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 8
Type:
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 9
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
Phase: 10
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 11
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
Phase: 12
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
```

```
Phase: 13
Type:
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 14
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 6449, packet dispatched to next module
Phase: 15
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group ALLOW global
access-list ALLOW extended permit ip any any
Additional Information:
Phase: 16
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Phase: 17
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 18
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 214.1.1.9 using egress ifc  outside2
Phase: 19
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop IP address to MAC
Result: ALLOW
Config:
Additional Information:
found adjacency entry for next-hop 214.1.1.9 on interface  outside
adjacency Active
mac address 4403.a74a.9a32 hits 15 reference 1
Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: outside2
output-status: up
output-line-status: up
Action: allow
cluster2-asa5585a(config)#
```

以下示例概述在传出接口上捕获的 ICMP 数据包：

```
cluster2-asa5585a(config)# cluster exec show capture test | i icmp
  a(LOCAL):*******************************************************
    14: 02:18:16.717736      802.1Q vlan#212 P0 211.1.1.10 > 213.1.1.10: icmp: echo request
```

```
  cluster2-asa5585a(config)#
```

数据包跟踪器的绕行检查选项的示例将通过所列的以下阶段进行概述。下面为每种情况提供了具体示例：

- 分支和集线器之间未创建 IPSec 隧道。
- 两个设备之间的 IPSec 隧道必须协商，并且初始数据包触发隧道建立。
- IPSec 协商完成，隧道启动。
- 隧道启动后，注入的数据包将通过隧道发送。将绕过或跳过与数据包路径一起提供的安全检查（ACL、VPN 过滤等）。

未创建 IPSec 隧道：

```
cluster2-asa5585a(config)# sh crypto ipsec sa
  There are no ipsec sas
  cluster2-asa5585a(config)#
```

隧道协商过程开始：

```
cluster2-asa5585a(config)# packet-tracer input outside tcp 211.1.1.1 5050 213.1.1.2 21
bypass-checks
  Phase: 1
  Type: CAPTURE
  Subtype:
  Result: ALLOW
  Config:
  Additional Information:
  MAC Access list
  Phase: 2
  Type: ACCESS-LIST
  Subtype:
  Result: ALLOW
  Config:
  Implicit Rule
  Additional Information:
  MAC Access list
  Phase: 3
  Type: ROUTE-LOOKUP
  Subtype: Resolve Egress Interface
  Result: ALLOW
  Config:
  Additional Information:
  found next-hop 214.1.1.9 using egress ifc  outside2

  Phase: 4
  Type: CLUSTER-EVENT
  Subtype:
  Result: ALLOW
  Config:
  Additional Information:
  Input interface: 'outside'
  Flow type: NO FLOW
  I (0) got initial, attempting ownership.
  Phase: 5
  Type: CLUSTER-EVENT
  Subtype:
  Result: ALLOW
```

```
Config:
Additional Information:
Input interface: 'outside'
Flow type: NO FLOW
I (0) am becoming owner
Phase: 6
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group ALLOW global
access-list ALLOW extended permit ip any any
Additional Information:
Phase: 7
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Phase: 8
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 9
Type: INSPECT
Subtype: inspect-ftp
Result: ALLOW
Config:
class-map inspection_default
 match default-inspection-traffic
policy-map global_policy
 class inspection_default
  inspect ftp
service-policy global_policy global
Additional Information:
Phase: 10
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 11
Type: INSPECT
Subtype: inspect-ftp
Result: ALLOW
Config:
class-map inspection_default
 match default-inspection-traffic
policy-map global_policy
 class inspection_default
  inspect ftp
service-policy global_policy global
Additional Information:
Phase: 12
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 13
Type: VPN
Subtype: encrypt
```

```
  Result: DROP
  Config:
  Additional Information:
  Result:
  input-interface: outside
  input-status: up
  input-line-status: up
  output-interface: outside2
  output-status: up
  output-line-status: up
  Action: drop
  Drop-reason: (acl-drop) Flow is denied by configured rule
  cluster2-asa5585a(config)#
```

协商 IPSec 隧道并且隧道启动后：

```
cluster2-asa5585a#
  cluster2-asa5585a(config)# sh crypto ipsec sa
  interface: outside2
      Crypto map tag: crypto-map-peer4, seq num: 1, local addr: 214.1.1.10
        access-list toPeer4 extended permit ip host 211.1.1.1 host 213.1.1.2
        local ident (addr/mask/prot/port): (211.1.1.1/255.255.255.255/0/0)
        remote ident (addr/mask/prot/port): (213.1.1.2/255.255.255.255/0/0)
        current_peer: 214.1.1.9
        #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
        #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
        #pkts compressed: 0, #pkts decompressed: 0
        #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
        #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
        #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
        #TFC rcvd: 0, #TFC sent: 0
        #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
        #send errors: 0, #recv errors: 0
        local crypto endpt.: 214.1.1.10/500, remote crypto endpt.: 214.1.1.9/500
        path mtu 1500, ipsec overhead 74(44), media mtu 1500
        PMTU time remaining (sec): 0, DF policy: copy-df
        ICMP error validation: disabled, TFC packets: disabled
        current outbound spi: A642726D
        current inbound spi : CF1E8F90

      inbound esp sas:
        spi: 0xCF1E8F90 (3474886544)
           SA State: active
           transform: esp-aes-256 esp-sha-hmac no compression
           in use settings ={L2L, Tunnel, IKEv2, }
           slot: 0, conn_id: 2, crypto-map: crypto-map-peer4
           sa timing: remaining key lifetime (kB/sec): (4285440/28744)
           IV size: 16 bytes
           replay detection support: Y
           Anti replay bitmap:
            0x00000000 0x00000001
      outbound esp sas:
        spi: 0xA642726D (2789372525)
           SA State: active
           transform: esp-aes-256 esp-sha-hmac no compression
           in use settings ={L2L, Tunnel, IKEv2, }
           slot: 0, conn_id: 2, crypto-map: crypto-map-peer4
           sa timing: remaining key lifetime (kB/sec): (4239360/28744)
           IV size: 16 bytes
           replay detection support: Y
           Anti replay bitmap:
            0x00000000 0x00000001
  cluster2-asa5585a(config)#
```

隧道启动后，允许数据包通过，并且由于应用了 bypass-checks 选项，因此会跳过安全检查：

```
cluster2-asa5585a# packet-tracer input outside tcp 211.1.1.1 5050 213.1.1.2 21 bypass-checks

  Phase: 1
  Type: ROUTE-LOOKUP
  Subtype: Resolve Egress Interface
  Result: ALLOW
  Config:
  Additional Information:
  found next-hop 214.1.1.9 using egress ifc  outside2
  Phase: 2
  Type: CLUSTER-EVENT
  Subtype:
  Result: ALLOW
  Config:
  Additional Information:
  Input interface: 'outside'
  Flow type: NO FLOW
  I (0) got initial, attempting ownership.
  Phase: 3
  Type: CLUSTER-EVENT
  Subtype:
  Result: ALLOW
  Config:
  Additional Information:
  Input interface: 'outside'
  Flow type: NO FLOW
  I (0) am becoming owner
  Phase: 4
  Type: ACCESS-LIST
  Subtype: log
  Result: ALLOW
  Config:
  access-group ALLOW global
  access-list ALLOW extended permit ip any any
  Additional Information:
  Phase: 5
  Type: NAT
  Subtype: per-session
  Result: ALLOW
  Config:
  Additional Information:
  Phase: 6
  Type: IP-OPTIONS
  Subtype:
  Result: ALLOW
  Config:
  Additional Information:
  Phase: 7
  Type: INSPECT
  Subtype: inspect-ftp
  Result: ALLOW
  Config:
  class-map inspection_default
   match default-inspection-traffic
  policy-map global_policy
   class inspection_default
    inspect ftp
  service-policy global_policy global
  Additional Information:
  Phase: 8
  Type: VPN
```

```
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 9
Type: INSPECT
Subtype: inspect-ftp
Result: ALLOW
Config:
class-map inspection_default
 match default-inspection-traffic
policy-map global_policy
 class inspection_default
  inspect ftp
service-policy global_policy global
Additional Information:
Phase: 10
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 11
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:
Phase: 12
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:
Phase: 13
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 14
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Phase: 15
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 16
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 17
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
```

```
Phase: 18
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 19
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:
Phase: 20
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:
Phase: 21
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 1099, packet dispatched to next module
Phase: 22
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 214.1.1.9 using egress ifc  outside2
Phase: 23
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
Phase: 24
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
Phase: 25
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 1100, packet dispatched to next module
Phase: 26
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 214.1.1.9 using egress ifc  outside2
Phase: 27
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop IP address to MAC
Result: ALLOW
```

```
Config:
Additional Information:
found adjacency entry for next-hop 214.1.1.9 on interface  outside
adjacency Active
mac address 4403.a74a.9a32 hits 99 reference 2
Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: outside2
output-status: up
output-line-status: up
Action: allow
```

以下示例跟踪具有下一跳 ARP 条目的直连主机中的 TCP 数据包。

```
ciscoasa# packet-tracer input inside tcp 192.168.100.100 12345 192.168.102.102 80 detailed

Phase: 1
Type: ROUTE-LOOKUP
Subtype: No ECMP load balancing
Result: ALLOW
Config:
Additional Information:
Destination is locally connected. No ECMP load balancing.
Found next-hop 192.168.102.102 using egress ifc  outside(vrfid:0)

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group TEST global
access-list TEST advanced trust ip any any
Additional Information:
Forward Flow based lookup yields rule:
in  id=0x2ae2a8aa5e90, priority=12, domain=permit, trust
hits=17, user_data=0x2ae29aabc100, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any, vlan=0, dscp=0x0
input_ifc=any, output_ifc=any
Phase: 3
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in  id=0x2ae2a69a7240, priority=0, domain=nat-per-session, deny=false
hits=34, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=6
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=any, output_ifc=any

Phase: 4
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in  id=0x2ae2a8488800, priority=0, domain=inspect-ip-options, deny=true
hits=22, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
```

```
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=inside(vrfid:0), output_ifc=any

Phase: 5
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Reverse Flow based lookup yields rule:
in  id=0x2ae2a69a7240, priority=0, domain=nat-per-session, deny=false
hits=36, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=6
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=any, output_ifc=any

Phase: 6
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Reverse Flow based lookup yields rule:
in  id=0x2ae2a893e230, priority=0, domain=inspect-ip-options, deny=true
hits=10, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=outside(vrfid:0), output_ifc=any

Phase: 7
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 21, packet dispatched to next module
Module information for forward flow ...
snp_fp_inspect_ip_options
snp_fp_tcp_normalizer
snp_fp_translate
snp_fp_adjacency
snp_fp_fragment
snp_fp_tracer_drop
snp_ifc_stat

Module information for reverse flow ...
snp_fp_inspect_ip_options
snp_fp_translate
snp_fp_tcp_normalizer
snp_fp_adjacency
snp_fp_fragment
snp_fp_tracer_drop
snp_ifc_stat

Phase: 8
Type: INPUT-ROUTE-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP
Subtype: Resolve Preferred Egress interface
Result: ALLOW
Config:
Additional Information:
Found next-hop 192.168.102.102 using egress ifc  outside(vrfid:0)

Phase: 9
```

```
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop IP address to MAC
Result: ALLOW
Config:
Additional Information:
found adjacency entry for next-hop 192.168.102.102 on interface  outside
Adjacency :Active
mac address 0aaa.0bbb.00cc hits 5 reference 1

Result:
input-interface: inside(vrfid:0)
input-status: up
input-line-status: up
output-interface: outside(vrfid:0)
output-status: up
output-line-status: up
Action: allow
```

以下示例跟踪由于缺少有效的下一跳 ARP 条目而被丢弃的 TCP 数据包。请注意，丢弃原因提供了检查 ARP 表的提示。

```
<Displays same phases as in the previous example till Phase 8>
Result:
input-interface: inside(vrfid:0)
input-status: up
input-line-status: up
output-interface: outside(vrfid:0)
output-status: up
output-line-status: up
Action: drop
Drop-reason: (no-v4-adjacency) No valid V4 adjacency. Check ARP table (show arp) has entry
 for nexthop., Drop-location: frame snp_fp_adj_process_cb:200 flow (NA)/NA
```

以下示例描述了使用 NAT 和可访问的下一跳进行次优路由的数据包跟踪器。

```
ciscoasa# sh run route
route inside 0.0.0.0 0.0.0.0 192.168.100.100 1
route outside 0.0.0.0 0.0.0.0 192.168.102.102 10

ciscoasa# sh nat detail
Manual NAT Policies (Section 1)
1 (outside) to (dmz) source static src_real src_mapped  destination static dest_real
dest_mapped
translate_hits = 3, untranslate_hits = 3
Source - Origin: 9.9.9.0/24, Translated: 10.10.10.0/24
Destination - Origin: 192.168.104.0/24, Translated: 192.168.104.0/24
ciscoasa# packet-tracer input dmz tcp 192.168.104.104 12345 10.10.10.10 80 detailed

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (outside,dmz) source static src_real src_mapped destination static dest_real dest_mapped
Additional Information:
NAT divert to egress interface outside(vrfid:0)
Untranslate 10.10.10.10/80 to 9.9.9.10/80

Phase: 2
Type: ACCESS-LIST
Subtype: log
```

```
Result: ALLOW
Config:
access-group TEST global
access-list TEST advanced trust ip any any
Additional Information:
Forward Flow based lookup yields rule:
in  id=0x2ae2a8aa5e90, priority=12, domain=permit, trust
hits=20, user_data=0x2ae29aabc100, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any, vlan=0, dscp=0x0
input_ifc=any, output_ifc=any

Phase: 3
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (outside,dmz) source static src_real src_mapped destination static dest_real dest_mapped
Additional Information:
Static translate 192.168.104.104/12345 to 192.168.104.104/12345
Forward Flow based lookup yields rule:
in  id=0x2ae2a8aa4ff0, priority=6, domain=nat, deny=false
hits=4, user_data=0x2ae2a8a9d690, cs_id=0x0, flags=0x0, protocol=0
src ip/id=192.168.104.0, mask=255.255.255.0, port=0, tag=any
dst ip/id=10.10.10.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
input_ifc=dmz(vrfid:0), output_ifc=outside(vrfid:0)

Phase: 4
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in  id=0x2ae2a69a7240, priority=0, domain=nat-per-session, deny=false
hits=40, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=6
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=any, output_ifc=any

Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in  id=0x2ae2a89de1b0, priority=0, domain=inspect-ip-options, deny=true
hits=4, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=dmz(vrfid:0), output_ifc=any

Phase: 6
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
nat (outside,dmz) source static src_real src_mapped destination static dest_real dest_mapped
Additional Information:
Forward Flow based lookup yields rule:
out id=0x2ae2a8aa53d0, priority=6, domain=nat-reverse, deny=false
hits=5, user_data=0x2ae2a8a9d580, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
src ip/id=192.168.104.0, mask=255.255.255.0, port=0, tag=any
```

```
dst ip/id=9.9.9.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
input_ifc=dmz(vrfid:0), output_ifc=outside(vrfid:0)

Phase: 7
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Reverse Flow based lookup yields rule:
in  id=0x2ae2a69a7240, priority=0, domain=nat-per-session, deny=false
hits=42, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=6
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=any, output_ifc=any
Phase: 8
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Reverse Flow based lookup yields rule:
in  id=0x2ae2a893e230, priority=0, domain=inspect-ip-options, deny=true
hits=13, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=outside(vrfid:0), output_ifc=any

Phase: 9
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 24, packet dispatched to next module
Module information for forward flow ...
snp_fp_inspect_ip_options
snp_fp_tcp_normalizer
snp_fp_translate
snp_fp_adjacency
snp_fp_fragment
snp_fp_tracer_drop
snp_ifc_stat

Module information for reverse flow ...
snp_fp_inspect_ip_options
snp_fp_translate
snp_fp_tcp_normalizer
snp_fp_adjacency
snp_fp_fragment
snp_fp_tracer_drop
snp_ifc_stat

Phase: 10
Type: INPUT-ROUTE-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP
Subtype: Resolve Preferred Egress interface
Result: ALLOW
Config:
Additional Information:
Found next-hop 192.168.100.100 using egress ifc  inside(vrfid:0)

Phase: 11
Type: SUBOPTIMAL-LOOKUP
Subtype: suboptimal next-hop
```

```
Result: ALLOW
Config:
Additional Information:
Input route lookup returned ifc  inside is not same as existing ifc  outside
Doing adjacency lookup lookup on existing ifc outside

Phase: 12
Type: NEXTHOP-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP
Subtype: Lookup Nexthop on interface
Result: ALLOW
Config:
Additional Information:
Found next-hop 192.168.102.102 using egress ifc  outside(vrfid:0)

Phase: 13
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop IP address to MAC
Result: ALLOW
Config:
Additional Information:
found adjacency entry for Next-hop 192.168.102.102 on interface  outside
Adjacency :Active
mac address 0aaa.0bbb.00cc hits 5 reference 1

Result:
input-interface: dmz(vrfid:0)
input-status: up
input-line-status: up
output-interface: outside(vrfid:0)
output-status: up
output-line-status: up
Action: allow
The following example depicts packet tracer for sub-optimal routing with NAT, where, the
packet is dropped due to non-reachable nexthop.
ciscoasa# sh run route
route inside 0.0.0.0 0.0.0.0 192.168.100.100 1

ciscoasa# sh nat detail
Manual NAT Policies (Section 1)
1 (outside) to (dmz) source static src_real src_mapped  destination static dest_real
dest_mapped
translate_hits = 3, untranslate_hits = 3
Source - Origin: 9.9.9.0/24, Translated: 10.10.10.0/24
Destination - Origin: 192.168.104.0/24, Translated: 192.168.104.0/24


<Displays same phases as in the previous example till Phase 11>
Result:
input-interface: dmz(vrfid:0)
input-status: up
input-line-status: up
output-interface: outside(vrfid:0)
output-status: up
output-line-status: up
Action: drop
Drop-reason: (no-adjacency) No valid adjacency, Drop-location: frame
snp_fp_adjacency_internal:5890 flow (NA)/NA
```

启用对象组搜索时，跟踪包括对象查找步骤。从 9.22(1) 开始，这些信息包括源对象表和目标对象表中的查找总数、总体查找计数以及对象查找阶段所花费的总时间。以下是对象组搜索信息的示例。

```
Phase: 2
```

```
Type: OBJECT_GROUP_SEARCH
Subtype:
Result: ALLOW
Elapsed time: 47005 ns
Config:
Additional Information:
 Source object-group match count:          2
 Source NSG match count:                   0
 Destination NSG match count:              0
 Classify table lookup count:              4
 Total lookup count:                       3
 Duplicate key pair count:                 0
 Classify table match count:               3
```

Related Commands

命令	说明
capture	捕获数据包信息，包括跟踪数据包。
show capture	在未指定选项时显示捕获配置。
show packet-tracer	显示最近在PCAP文件上运行的数据包跟踪器的跟踪缓冲区输出。

pager

要设置在 Telnet 会话出现“ ---More--- ”提示符之前页面上显示的默认行数，请在全局配置模式下使用 **pager** 命令。

pager [**lines**] *lines*

Syntax Description

[**lines**]*lines*	设置在出现“ ---更多--- ”提示之前页面上的行数。默认值为 24 行； 0 表示无页面限制。范围是 0 到 2147483647 行。 **lines** 关键字是可选的，并且无论有或没有该关键字，命令的功能都是相同的。

Command Default

默认值为 24 行。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	• 支持	• 支持

Command History

版本	修改
7.0(1)	此命令已从特权 EXEC 模式命令更改为全局配置模式命令。 **terminalpager** 命令被添加为特权 EXEC 模式命令。

使用指南

此命令更改 Telnet 会话的默认寻呼线路设置。如果只想暂时更改当前会话的设置，请使用**terminalpager** 命令。

如果您通过 Telnet 进入管理上下文，则当您切换到其他上下文时，寻呼机线路设置将跟随您的 **pager** 会话，即使给定上下文中的命令具有不同的设置。要更改当前分页器设置，请输入带有新设置的 **terminalpager** 命令，也可以在当前上下文中输入该 **pager**命令。除了将新的寻呼机设置保存到上下文配置之外，该 **pager**命令还将新设置应用于当前 Telnet 会话。

CR_Examples

以下示例将显示的行数更改为 20：

```
ciscoasa(config)# pager 20
```

Related Commands

命令	说明
clear configure terminal	清除终端显示宽度设置。

命令	说明
show running-config terminal	显示当前终端设置。
terminal	允许系统日志消息显示在 Telnet 会话中。
terminal pager	设置在“ ---more--- ”提示之前在 Telnet 会话中显示的行数。此命令不会保存到配置中。
terminal width	在全局配置模式中设置终端显示宽度。

page style

要定制 WebVPN 用户连接到安全设备时显示的 WebVPN 页面，请在 webvpn 定制配置模式下使用该 **pagestyle** 命令。要从配置中删除命令并导致值被继承，请使用此命令的 **no**形式。

page style 值
［**no**］**page style** *value*

Syntax Description

value 级联样式表 (CSS) 参数（最多 256 个字符）。

Command Default

默认页面样式为background-colour:white;font-family:Arial,Helv,sans-serif

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
Webvpn 自定义配置	• 是	—	• 是	—	—

Command History

版本	修改
7.1(1)	添加了此命令。

使用指南

该 **style**选项表示为任何有效的层叠样式表 (CSS) 参数。描述这些参数已超出本文档的范围。有关 CSS 参数的更多信息，请查阅万维网联盟 (W3C) 网站 www.w3.org 上的 CSS 规范。CSS 2.1 规范的附录 F 包含 CSS 参数的便捷列表，且在 www.w3.org/TR/CSS21/propidx.html 上提供。

以下是对 WebVPN 页面进行最常见更改（页面颜色）的一些技巧：

- 您可以使用逗号分隔的 RGB 值、HTML 颜色值或颜色的名称（如果已在 HTML 中标识）。
- RGB 格式是 0,0,0，每种颜色（红色、绿色、蓝色）的范围是从 0 到 255 的十进制数字；逗号分隔的条目表示每种颜色与其他颜色相结合的强度级别。
- HTML 格式是 #000000，十六进制格式的六位数；第一和第二个数字代表红色，第三和第四个数字代表绿色，第五和第六个数字代表蓝色。

注释 要轻松定制 WebVPN 页面，我们建议您使用 ASDM，它具有配置样式元素的便捷功能，包括色样和预览功能。

CR_Examples

以下示例将页面样式自定义为large：

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# page style font-size:large
```

Related Commands

命令	说明
logo	定制 WebVPN 页面上的徽标。
title	自定义 WebVPN 页面的标题

parameters

要进入参数配置模式以为检测策略映射设置参数，请在策略映射配置模式下使用 **parameters** 命令。

parameters

Syntax Description

此命令没有任何参数或关键字。

Command Default

没有默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
策略映射配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.2(1)	添加了此命令。

使用指南

通过模块化策略框架，您可以为许多应用检测配置特殊操作。当您使用第 3/4 层策略映射中的 **inspect** 命令（ **policy-map** 命令）启用检测引擎时，您还可以选择启用 **policy-maptypeinspect** 命令创建的检测策略映射中定义的操作。例如，输入 **inspectdnsdns_policy_map** 命令，其中 dns_policy_map 是检测策略映射的名称。

检测策略映射可能支持一个或多个 **parameters** 命令。参数影响检查引擎的行为。参数配置模式下可用的命令取决于应用。

CR_Examples

以下示例显示如何在默认检测策略映射中设置 DNS 数据包的最大消息长度：

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# message-length maximum 512
```

Related Commands

命令	说明
class	在策略映射中标识类映射名称。
class-maptypeinspect	创建检查类映射以匹配特定于应用的流量。
policy-map	创建第 3/4 层策略映射。

命令	说明
showrunning-configpolicy-map	显示所有当前的策略映射配置。

participate

要强制设备加入虚拟负载均衡集群，请在VPN负载均衡配置模式下使用**participate**命令。要取消设备对集群的参与，请使用此命令的 **no** 形式。

participate
no participate

Syntax Description

此命令没有任何参数或关键字。

Command Default

默认行为是，设备不加入 VPN 负载均衡集群。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
VPN 负载平衡配置	• 是	—	• 是	—	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

您必须先使用 **interface** 和 **nameif** 命令配置接口，然后使用 **vpnload-balancing**命令进入 VPN 负载均衡模式。您还必须先前使用该命令配置集群 IP 地址 **clusterip**，并配置虚拟集群 IP 地址所引用的接口。

此命令会强制此设备加入虚拟负载均衡集群。必须显式发出此命令启用设备的参与。

参与集群的所有设备必须共享相同的集群特定值：IP 地址、加密设置、加密密钥和端口。

注释 使用加密时，您必须事先配置命令 **isakmpenable***inside*，其中 *inside*指定负载平衡内部接口。如果未在负载均衡内部接口上启用isakmp，您会在尝试配置集群加密时收到错误消息。如果isakmp在配置 **clusterencryption** 命令时已启用，但在配置 **participate** 命令之前已被禁用，则您 **participate** 会出现错误消息，并且本地设备不会加入集群。

CR_Examples

以下是一个VPN负载均衡命令序列示例，其中包含使当前设备能够加入VPN负载均衡集群的 **participate** 命令：

```
ciscoasa(config)# interface GigabitEthernet 0/1
ciscoasa(config-if)# ip address 209.165.202.159 255.255.255.0
ciscoasa(config)# nameif test
ciscoasa(config)# interface GigabitEthernet 0/2
ciscoasa(config-if)# ip address 209.165.201.30 255.255.255.0
ciscoasa(config)# nameif foo
ciscoasa(config)# vpn load-balancing
ciscoasa(config-load-balancing)# interface lbpublic test
ciscoasa(config-load-balancing)# interface lbprivate foo
ciscoasa(config-load-balancing)# cluster ip address 209.165.202.224
ciscoasa(config-load-balancing)# participate
```

Related Commands

命令	说明
vpnload-balancing	进入 VPN 负载均衡模式。

passive-interface (ipv6 router ospf)

要抑制在接口上或使用 OSPFv3 进程的所有接口上发送和接收路由更新，请在 ipv6 router ospf 配置模式下使用 **passive-interface**命令。要在接口上或在使用 OSPFv3 进程的所有接口上重新启用路由更新，请使用此命令的 **no** 形式。

passive-interface [*interface_name*]
no passive-interface [*interface_name*]

Syntax Description

interface_name	（可选）指定运行 OSPFv3 进程的接口名称。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
Ipv6 路由器 ospf 配置	• 是	—	• 是	—	—

Command History

版本	修改
9.0(1)	添加了此命令。

使用指南

此命令可在接口上启用被动路由。

CR_Examples

以下示例抑制内部接口上路由更新的发送和接收。

```
ciscoasa(config)# ipv6 router ospf 10
ciscoasa(config-rtr)# passive-interface interface
ciscoasa(config-rtr)#
```

Related Commands

命令	说明
showrunning-configrouter	显示运行配置中的路由器配置命令。

passive-interface (isis)

要选择接口上的 ISIS hello 数据包和路由更新，同时仍将接口地址包含在拓扑数据库中，请在 **passive-interface**路由器 isis 配置模式下使用该命令。要重新启用传出呼叫数据包和路由更新，请使用此命令的 **no** 形式。

passive-interface [**default** | **inside** | **management** | **management2**]
no passive-interface [**default** | **inside** | **management** | **management2**]

Syntax Description

default	抑制所有接口上的路由更新。
inside	接口 GigabithEthernet0/0 的名称。
management	接口 Management0/0 的名称。
management2	接口 Management0/1 的名称。

Command Default

默认设置是抑制所有接口上的路由更新。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
路由器 isis 配置	• 是	—	• 是	• 支持	—

Command History

版本	修改
9.6(1)	添加了此命令。

使用指南

此命令可在接口上启用被动路由。

CR_Examples

以下示例抑制内部接口上路由更新的发送和接收。

```
ciscoasa(config)# router isis
ciscoasa(config-router)# passive-interface inside
```

Related Commands

命令	说明
advertisepassive-only	配置 ASA 以通告被动接口。

命令	说明
area-password	配置 IS-IS 区域身份验证密码。
authenticationkey	全局启用 IS-IS 身份验证。
authenticationmode	指定IS-IS实例全局使用的IS-IS报文认证方式。
authenticationsend-only	全局配置 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。
clearisis	清除 IS-IS 数据结构。
default-information originate	在 IS-IS 路由域中生成默认路由。
distance	定义分配给 IS-IS 协议发现的路由的管理距离。
domain-password	配置 IS-IS 域身份验证密码。
fast-flood	将 IS-IS LSP 配置为完整的。
hellopadding	将 IS-IS hello 配置为完整 MTU 大小。
hostnamedynamic	启用 IS-IS 动态主机名功能。
ignore-lsp-errors	配置 ASA 忽略收到的带有内部校验和错误的 IS-IS LSP，而不是清除 LSP。
isisadjacency-filter	过滤 IS-IS 邻接关系的建立。
isisadvertiseprefix	在 IS-IS 接口上的 LSP 通告中通告所连接网络的 IS-IS 前缀。
isisauthenticationkey	启用接口的身份验证。
isisauthenticationmode	指定每个接口的 IS-IS 实例的 IS-IS 数据包中使用的身份验证模式类型
isisauthenticationsend-only	配置每个接口的 IS-IS 实例，仅对发送（而不是接收）的 IS-IS 数据包执行身份验证。
isiscircuit-type	配置用于 IS-IS 的邻接类型。
isiscsnp-interval	配置在广播接口上发送周期性 CSNP 数据包的间隔。
isishello-interval	指定 IS-IS 发送的连续 hello 数据包之间的时间长度。
isishello-multiplier	指定在 ASA 宣布邻接关系关闭之前邻居必须错过的 IS-IS hello 数据包的数量。
isishellopadding	将 IS-IS hello 配置为每个接口的完整 MTU 大小。
isislsp-interval	配置每个接口连续 IS-IS LSP 传输之间的时间延迟。

命令	说明
isismetric	配置 IS-IS 度量的值。
isispassword	配置接口的认证密码。EXTEN
isispriority	配置接口上指定 ASA 的优先级。
isisprotocolshutdown	禁用每个接口的 IS-IS 协议。
isisretransmit-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isisretransmit-throttle-interval	配置接口上每个 IS-IS LSP 重新传输之间的时间量。
isistag	当 IP 前缀放入 LSP 时，在为接口配置的 IP 地址上设置标签。
is-type	为 IS-IS 路由进程分配路由级别。
log-adjacency-changes	使 ASA 能够在 NLSP IS-IS 邻接关系改变状态（启动或关闭）时生成日志消息。
lsp-fullsuppress	配置当 PDU 已满时哪些路由会被抑制。
lsp-gen-interval	定制 IS-IS 对 LSP 生成的限制。
lsp-refresh-interval	设置LSP刷新间隔。
max-area-addresses	为 IS-IS 区域配置额外的手动地址。
max-lsp-lifetime	设置 LSP 在 ASA 数据库中持续存在而不被刷新的最长时间。
maximum-paths	为 IS-IS 配置多路径负载共享。
metric	全局更改所有 IS-IS 接口的度量值。
metric-style	配置运行 IS-IS 的 ASA，使其生成且仅接受新式长度值对象 (TLV)。
net	指定路由过程的NET。
passive-interface	配置被动接口。
prc-interval	定制 PRC 的 IS-IS 限制。
protocolshutdown	全局禁用 IS-IS 协议，使其无法在任何接口上形成任何邻接，并将清除 LSP 数据库。
redistributeisis	将 IS-IS 路由从第 1 级重新分配到第 2 级或从第 2 级重新分配到第 1 级。
routeprioorityhigh	为 IS-IS IP 前缀分配高优先级。
routerisis	启用 IS-IS 路由。

命令	说明
set-attached-bit	指定第 1 级至第 2 级路由器应设置其附加位的约束。
set-overload-bit	配置 ASA 以向其他路由器发出信号，不要在其 SPF 计算中将其用作中间跳。
showclns	显示 CLNS 特定信息。
showisis	显示 IS-IS 信息。
showrouteisis	显示 IS-IS 路由。
spf-interval	自定义 IS-IS 对 SPF 计算的限制。
summary-address	为 IS-IS 创建聚合地址。

passive-interface (router eigrp)

要禁用接口上 EIGRP 路由更新的发送和接收，请在 **passive-interface** 路由器 eigrp 配置模式下使用该命令。要重新启用接口上的路由更新，请使用此命令的 **no** 形式。

passive-interface { **default** | *if_name* }
no passive-interface { **default** | *if_name* }

Syntax Description

default	（可选）将所有接口设置为被动模式。
if_name	（可选）由 **nameif** 命令指定的接口名称，用于禁用路由更新。

Command Default

当为该接口启用路由时，所有接口都针对活动路由启用（发送和接收路由更新）。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
路由器 eigrp 配置	• 是	—	• 是	—	—

Command History

版本	修改
7.2(1)	添加了此命令。
8.0(2)	添加了对 EIGRP 路由的支持。
9.20(1)	增加了对 EIGRP IPv6 路由的支持。

使用指南

在接口上启用被动路由。对于 EIGRP，这会禁用该接口上路由更新的传输和接收。

您可以在 EIGRP 配置中使用多个 **passive-interface** 命令。您可以使用 **passive-interfacedefault** 命令在所有接口上禁用 EIGRP 路由，然后使用 **nopassive-interface** 命令在特定接口上启用 EIGRP 路由。

CR_Examples

以下示例将外部接口设置为被动 EIGRP。安全设备上的其他接口会发送和接收 EIGRP 更新。

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# passive-interface outside
```

以下示例将除内部接口之外的所有接口设置为被动 EIGRP。只有内部接口会发送和接收 EIGRP 更新。

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# passive-interface default
ciscoasa(config-router)# no passive-interface inside
```

Related Commands

命令	说明
showrunning-configrouter	显示运行配置中的路由器配置命令。

passive-interface (router rip)

要禁用接口上的 RIP 路由更新传输，请在 **passive-interface** 路由器 RIP 配置模式下使用该命令。要在接口上重新启用 RIP 路由更新，请使用此命令的 **no** 形式。

passive-interface { **default** | *if_name* }
no passive-interface { **default** | *if_name* }

Syntax Description

default	（可选）将所有接口设置为被动模式。
if_name	（可选）将指定接口设置为被动模式。

Command Default

如果启用了 RIP，系统会为活动 RIP 启用所有接口。

如果未指定接口或 **default** 关键字，则命令默认为 **default**，并在配置中显示为 passive-interface default。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
路由器 RIP 配置	• 是	—	• 是	• 支持	—

Command History

版本	修改
7.2(1)	添加了此命令。
9.0(1)	增加了多情景模式支持。

使用指南

在接口上启用被动 RIP。该接口侦听 RIP 路由广播并使用该信息填充路由表，但不会广播路由更新。

CR_Examples

以下示例将外部接口设置为被动 RIP。安全设备上的其他接口会发送和接收 RIP 更新。

```
ciscoasa(config)# router rip
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# passive-interface outside
```

Related Commands

命令	说明
clearconfigurerip	从运行配置中清除所有 RIP 命令。
routerrip	启用 RIP 路由进程并进入 RIP 路由器配置模式。

命令	说明
showrunning-configrip	显示运行配置中的 RIP 命令。

passwd

要设置Telnet的登录密码，请在**passwd** 全局配置模式下使用该命令。要重置密码，请使用此命 **no**令的形式。

passwd*password* ［**encrypted**］
no passwd密码

Syntax Description

encrypted	（可选）指定密码为加密形式。密码以加密形式保存在配置中，因此在输入原始密码后无法查看原始密码。如果由于某种原因您需要将密码复制到另一个 ASA 但不知道原始密码，则可以输入带 **passwd**有加密密码和此关键字的命令。通常，只有在输入命令时才会看到这个关 **showrunning-configpasswd**键字。
password	将密码设置为最多 80 个字符的字符串，区分大小写。密码不得包含空格。

Command Default

9.1(1)：默认密码是“cisco”。

9.1(2): 无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。
8.3(1)	删除了别名 **password** 命令；仅支持 **passwd** 。
8.4(2)	SSH 默认用户名不再受支持；您无法再使用带有 **pix**或 **asa**用户名和登录密码的 SSH 连接到 ASA。
9.0(2)、9.1(2)	默认密码“cisco”已被删除；您必须主动设置登录密码。使用**nopasswd**或 **clearconfigurepasswd**命令可删除密码；默认情况下）。从前 会将其重置为默认值“cisco”。

使用指南

当您使用 **telnet** 命令启用 Telnet 时，您可以使用 **passwd** 命令设置的密码登录。输入登录密码后，您将处于用户 EXEC 模式。如果使用 **aaaauthenticationtelnetconsole** 命令为 Telnet 配置每用户 CLI 身份验证，则不会使用此密码。

此密码也用于从交换机到 ASASM 的 Telnet 会话（参见命 **session**令）。

CR_Examples

以下示例将密码设置为 Pa$$w0rd：

```
ciscoasa(config)# passwd Pa$$w0rd
```

以下示例将 password 设置为您从另一个 ASA 复制的加密密码：

```
ciscoasa(config)# passwd jMorNbK0514fadBh encrypted
```

Related Commands

命令	说明
clearconfigurepasswd	清除登录密码。
enable	进入特权 EXEC 模式。
enablepassword	设置启用密码。
showcurpriv	显示当前登录的用户名和用户权限级别。
showrunning-configpasswd	以加密形式显示登录密码。

password (crypto ca trustpoint)

要指定在注册期间向 CA 注册的质询短语，请在 crypto ca trustpoint 配置模式下使用 **password** 命令。要恢复默认设置，请使用此命 **no**令的形式。

password字符串
no password字符串

Syntax Description

string 将密码的名称指定为字符串。第一个字符不能为数字。该字符串可以包含任何字母数字字符（包括空格），最多 80 个字符。您不能以数字-空格-任何格式指定密码。数字后有空格会导致问题。例如，“hello 21”是合法密码，但“21 hello”不是。密码检查区分大小写。例如，密码“Secret”与密码“secret”不同。

Command Default

默认设置为不包含密码。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
Crypto ca trustpoint 配置	• 是	• 支持	• 支持	• 支持	• 支持

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

此命令允许您在实际证书注册开始之前指定证书的吊销密码。当 ASA 将更新的配置写入 NVRAM 时，指定的密码将被加密。

CA 通常使用质询短语来验证后续的撤销请求。

如果启用此命令，则在证书注册期间系统不会提示您输入密码。

CR_Examples

以下示例进入 trustpoint Central 的 crypto CA trustpoint 配置模式，并且在 trustpoint Central 的注册请求中包含向 CA 注册的质询短语：

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# password zzxxyy
```

Related Commands

命令	说明
cryptocatrustpoint	进入 trustpoint 配置模式。
defaultenrollment	将注册参数还原为其默认值。

password encryption aes

要使用主密码启用密码加密，请在全局配置模式下使用 **passwordencryptionaes** 命令。要禁用密码加密，请使用此命 **no**令的形式。

password encryption aes
no password encryption aes

Syntax Description

此命令没有任何参数或关键字。

Command Default

没有默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	—	• 是

Command History

版本	修改
8.3(1)	添加了此命令。

使用指南

您必须以任意顺序输入 **keyconfig-keypassword-encrypt** 命令和 **passwordencryptionaes**命令才能触发密码加密。输入 **writememory** ，以将加密密码保存到启动配置。否则，启动配置中的密码可能仍然可见。在多情景模式下，请在系统执行空间中使用 **writememoryall** 保存所有情景配置。如果您稍后使用该命令禁用密码加密，则所有现有的 **nopasswordencryptionaes**加密密码都将保持不变，并且只要主密码存在，就会根据应用程序的要求解密加密密码。

此命令仅在安全会话中被接受，例如通过控制台、SSH 或通过 HTTPS 的 ASDM。

在主用/备用故障转移中启用或 **writestandby**更改密码加密会导致将主用配置复制到备用单元。如果不进行此复制操作，即使主用设备和备用设备使用相同的密码，备用设备上经过加密的密码也不会不同；配置复制可确保两者的配置相同。对于主动/主动故障转移，您必须手动输入。 **writestandby** A 可 **writestandby**能会导致主动/主动模式下的流量中断，因为在同步新配置之前，辅助设备上的配置已被清除。您应该使用 **failoveractivegroup1** 和**failoveractivegroup2** 命令使主 ASA 上的所有上下文处于活动状态 **writestandby**，输入，然后使用命令将第 2 组上下文恢复到辅助单 **nofailoveractivegroup2**元。

write擦除命令（后跟reload命令）将删除主密码和所有配置（如果其丢失）。

CR_Examples

以下示例设置用于生成加密密钥的密码，并启用密码加密：

```
ciscoasa
(config)#
 key config-key password-encryption
Old key: bumblebee
New key: haverford
Confirm key: haverford
ciscoasa(config)# password encryption aes
ciscoasa(config)# write memory
```

Related Commands

命令	说明
keyconfig-keypassword-encryption	设置用于生成加密密钥的密码。
write erase	如果主密码在其后跟 reload 命令时丢失，则将其删除。

password-history

当您启用 **password-policyreuse-interval** 命令且用户不可配置时，此命令出现在 **usernameattributes** 命令的配置中。它以加密形式存储以前的密码。

password-history散列 *1*,散列 *2*,散列 *3*...

Syntax Description

散列 *1*,散列 *2*,散列 *3*...	显示已使用 PBKDF2（基于密码的密钥派生功能 2）进行散列处理的先前密码。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
用户名属性配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
9.8(1)	我们引入了此命令。

使用指南

此命令不可由用户配置，并且仅在启用 **password-policyreuse-interval** 命令时才会显示在 show 输出中。

CR_Examples

以下示例将密码更改两次，然后显示以前的散列密码：

```
ciscoasa(config)# username test password pw1
ciscoasa(config)# show running-config username test
username test password $sha512$5000$4tAPQTnL3WG1aa4xrfGMjA==$wbi1ks6eo381Km1qOiwqnQ== pbkdf2
ciscoasa(config)# username test password pw2
ciscoasa(config)# show running-config username test
username test password $sha512$5000$d8ebNCK2oTyzSiHjSh2T6w==$urDQ/+9sOPwi4IUftWFMcw== pbkdf2
username test attributes
  password-history $sha512$5000$4tAPQTnL3WG1aa4xrfGMjA==$wbi1ks6eo381Km1qOiwqnQ==
ciscoasa(config)# username test password pw3
ciscoasa(config)# show running-config username test
username test password $sha512$5000$o8WLa1qnLdp2Js4OlW+NdQ==$4Be4eHtPmOxdpfH6j+F4qQ== pbkdf2
username test attributes
  password-history
$sha512$5000$d8ebNCK2oTyzSiHjSh2T6w==$urDQ/+9sOPwi4IUftWFMcw==,$sha512$5000$4tAPQTnL3WG1aa4xrfGMjA==$wbi1ks6eo381Km1qOiwqnQ==
ciscoasa(config)#
```

Related Commands

命令	说明
aaaauthenticationlogin-history	保存本地 **username** 登录历史。
password-history	存储以前的**username**密码。用户无法配置此命令。
password-policyreuse-interval	禁止重复使用**username**密码。
password-policyusername-check	禁止使用与 **username**名称匹配的密码。
showaaalogin-history	显示本地 **username** 登录历史记录。
username	配置本地用户。

password-management

要启用密码管理，请在 tunnel-group general-attributes 配置模式下使用**password-management** 命令。要禁用密码管理，请使用此命 **no**令的形式。要将天数重置为默认值，请使用命令的 **no** 形式并指定 **password-expire-in-days** 关键字。

password-management [**password-expire-in-days**天]
nopassword-management
nopassword-managementpassword-expire-in-days [*days*]

Syntax Description

天	指定当前密码到期前的天数（0 至 180）。如果指定 **password-expire-in-days** 关键字，则需要此参数。
password-expire-in-days	（可选）表示紧随其后的参数指定 ASA 在当前密码到期之前多少天开始警告用户有关即将到期的情况。此选项仅对 LDAP 服务器有效。请参阅使用说明部分以了解更多信息。

Command Default

默认设置为无密码管理。如果没有为 LDAP 服务器指定 **password-expire-in-days** 关键字，则在当前密码到期之前，默认开始警告的时间长度为 14 天。如果禁用此功能，ASA 将使用密码身份验证协议 (PAP) 的身份验证方法。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
隧道组常规属性配置	• 是	—	• 是	—	—

Command History

版本	修改
7.1(1)	添加了此命令。

使用指南

ASA 支持 RADIUS 和 LDAP 协议的密码管理。对于 LDAP，它仅支持“password-expire-in-days”选项。

可以为 IPsec 远程访问和 SSL VPN 隧道组配置密码管理。

当您配置密码管理命令时，ASA 会在远程用户登录时通知用户当前密码即将过期或已过期。然后，ASA 为用户提供机会更改密码。如果当前密码尚未到期，用户仍可使用该密码登录。

此命令对于支持此类通知的AAA服务器有效；即，对于LDAP服务器和RADIUS服务器本身有效，代理到 NT 4.0 或 Active Directory 服务器。如果尚未配置 RADIUS 或 LDAP 身份验证，ASA 将忽略此命令。

注释 某些支持 MSCHAP 的 RADIUS 服务器当前不支持 MSCHAPv2。此命令需要 MSCHAPv2，因此请与您的供应商核实。

使用 LDAP 或支持 MS-CHAPv2 的任何 RADIUS 配置进行身份验证时，ASA 版本 7.1 及更高版本通常支持以下连接类型的密码管理：

- AnyConnect VPN 客户端（ASA 软件 8.0 及更高版本）
- IPsec VPN 客户端
- 无客户端 SSL VPN（ASA 软件版本 8.0 及更高版本）WebVPN（ASA 软件版本 7.1 至 7.2.x）
- SSL VPN 客户端 全隧道客户端

这些 RADIUS 配置包括使用 LOCAL 身份验证的 RADIUS、使用 Active Directory/Kerberos Windows DC 的 RADIUS、使用 NT/4.0 域的 RADIUS 以及使用 LDAP 的 RADIUS。

对于 Kerberos/Active Directory（Windows 密码）或 NT 4.0 域，所有这些连接类型都不支持密码管理。RADIUS 服务器（例如，思科 ACS）可能会将身份验证请求以代理方式发送到另一个身份验证服务器。但是， ASA 仅与 RADIUS 服务器通信。

注释 对于 LDAP，市场上不同的 LDAP 服务器有专有的密码更改方法。目前，ASA 仅对 Microsoft Active Directory 和 Sun LDAP 服务器实施专有密码管理逻辑。

本机 LDAP 需要 SSL 连接。在尝试执行 LDAP 密码管理之前，必须先启用基于 SSL 的 LDAP。默认情况下，LDAP 使用端口 636。

请注意，此命令不会改变密码过期前的天数，而是改变ASA在密码即将过期前多少天开始警告用户密码即将过期。

如果指定 **password-expire-in-days** 关键字，还必须指定天数。

指定此命令且天数设置为 0 会禁用此命令。ASA 不会通知用户密码即将到期，但是用户可以在密码到期后更改密码。

注释 Radius 不提供密码更改，也不提供密码更改提示。

CR_Examples

以下示例对于 WebVPN 隧道组“testgroup”，将距离密码到期以开始警告用户即将到期的警告设置为 90：

```
ciscoasa(config)# tunnel-group testgroup type webvpn
ciscoasa(config)# tunnel-group testgroup general-attributes
ciscoasa(config-tunnel-general)# password-management password-expire-in-days 90
ciscoasa(config-tunnel-general)#
```

以下示例使用默认值，即距离密码到期14天开始警告用户IPsec远程访问隧道组“QAgroup”即将到期：

```
ciscoasa(config)# tunnel-group QAgroup type ipsec-ra
ciscoasa(config)# tunnel-group QAgroup general-attributes
ciscoasa(config-tunnel-general)# password-management
ciscoasa(config-tunnel-general)#
```

Related Commands

命令	说明
clearconfigurepasswd	清除登录密码。
passwd	设置登录密码。
radius-with-expiry	在RADIUS身份验证期间启用密码更新协商（已弃用）。
showrunning-configpasswd	以加密形式显示登录密码。
tunnel-group general-attributes	配置隧道组常规属性值。

password-parameter

要指定必须提交用户密码以进行 SSO 身份验证的 HTTP POST 请求参数的名称，请在 **password-parameter** aaa-server-host 配置模式下使用该命令。这是使用 HTTP 表单命令的 SSO。

password-parameter*字符串*

注释 要正确配置 HTTP 的 SSO，您必须具备有关身份验证和 HTTP 交换的全面工作知识。

Syntax Description

string HTTP POST 请求中包含的密码参数的名称。密码最大长度为 128 个字符。

Command Default

没有默认值或行为。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
Aaa-server-host 配置	• 是	—	• 是	—	—

Command History

版本	修改
7.1(1)	添加了此命令。

使用指南

ASA 的 WebVPN 服务器使用 HTTP POST 请求向身份验证 Web 服务器提交单点登录身份验证请求。必需命 **password-parameter**令指定 POST 请求必须包含用于 SSO 身份验证的用户密码参数。

注释 登录时，用户输入实际密码值，该密码值输入到 POST 请求中并传递给身份验证 Web 服务器。

CR_Examples

以下示例在 aaa-server-host 配置模式下指定名为 user_password 的 password 参数：

```
ciscoasa(config)# aaa-server testgrp1 host example.com
ciscoasa(config-aaa-server-host)# password-parameter user_password
```

Related Commands

命令	说明
action-uri	指定要接收用于单点登录身份验证的用户名和密码的网络服务器 URI。
auth-cookie-name	指定身份验证 Cookie 的名称。
hidden-parameter	创建用于与身份验证网络服务器交换的隐藏参数。
start-url	指定用于提取登录前 Cookie 的 URL。
user-parameter	指定 HTTP POST 请求参数的名称，其中必须提交用户名以进行 SSO 身份验证。

password-policy authenticate enable

要确定是否允许用户修改其自己的用户账号，请在全局配置模式下使用 **password-policyauthenticateenable**命令。要将对应的密码策略属性设置为其默认值，请使用此命令的 **no** 形式。

password-policy authenticate enable
no password-policy authenticate enable

Syntax Description

此命令没有任何参数或关键字。

Command Default

默认情况下，身份验证是禁用的。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	—	• 是	• 支持	—

Command History

版本	修改
9.1(2)	添加了此命令。

使用指南

如果启用身份验证， **username** 命令不允许用户更改自己的密码或删除自己的帐户。此外，**clearconfigureusername** 命令不允许用户删除自己的帐户。

CR_Examples

以下示例显示如何使用户能够修改其用户账户：

```
ciscoasa(config)# password-policy authenticate enable
```

Related Commands

命令	说明
password-policyminimum-changes	设置新旧密码之间必须更改的最小字符数。
password-policyminimumlength	设置密码的最小长度。
password-policy minimum-lowercase	设置密码可以包含的最小小写字符数。

password-policy lifetime

要为当前情景设置密码策略和密码过期的间隔（天），请在全局配置模式下使用 **password-policylifetime** 命令。要将对应的密码策略属性设置为其默认值，请使用此命令的 **no** 形式。

password-policy lifetime值
no password-policy lifetime值

Syntax Description

value	指定密码有效期。有效值范围为 0 至 65535 天。

Command Default

默认生命周期值为 0 天。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	—	• 是	• 支持	—

Command History

版本	修改
9.1(2)	添加了此命令。

使用指南

密码具有指定的最长有效期限。0 天的生命周期间隔指定本地用户密码永不过期。请注意，密码将在有效期到期后的次日上午 12:00 到期。

CR_Examples

以下示例指定密码有效期值为 10 天：

```
ciscoasa(config)# password-policy lifetime 10
```

Related Commands

命令	说明
password-policyminimum-changes	设置新旧密码之间必须更改的最小字符数。
password-policyminimumlength	设置密码的最小长度。
password-policy minimum-lowercase	设置密码可以包含的最小小写字符数。

password-policy minimum-changes

如要设置新密码和旧密码必须更改的最小字符数，请在全局配置模式下使用 **password-policyminimum-changes** 命令。要将对应的密码策略属性设置为其默认值，请使用此命令的 **no** 形式。

password-policy minimum-changes*值*
no password-policy minimum-changes*值*

Syntax Description

value	指定新旧密码之间必须更改的字符数。有效值范围为 0 到 64 个字符。

Command Default

更改的字符数默认为 0。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	—	• 是	• 支持	—

Command History

版本	修改
9.1(2)	添加了此命令。

使用指南

新密码必须在当前密码的基础上至少更改4个字符，并且仅当它们未出现在当前密码的任何位置时，才会被视为已更改。

CR_Examples

以下示例指定新旧密码之间最小字符更改数（6 个字符）：

```
ciscoasa(config)# password-policy minimum-changes 6
```

Related Commands

命令	说明
password-policylifetime	设置密码有效期（以天为单位，在该天后密码将到期）。
password-policyminimum-length	设置密码的最小长度。
password-policy minimum-lowercase	设置密码可以包含的最小小写字符数。

password-policy minimum-length

要设置密码最小长度，请在全局配置模式下使用 **password-policyminimum-length** 命令。要将对应的密码策略属性设置为其默认值，请使用此命令的 **no** 形式。

password-policy minimum-length*值*
no password-policy minimum-length*值*

Syntax Description

value	指定密码的最小长度。有效值范围为 3 到 32 个字符。

Command Default

默认最小长度为 3。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	—	• 是	• 支持	—

Command History

版本	修改
9.1(2)	添加了此命令。

使用指南

如果最小长度小于任何其他最小属性（更改、小写字母、大写字母、数字和特殊字符），则会显示错误消息，并且不会更改最小长度。建议密码长度为 8 个字符。

CR_Examples

以下示例将密码的最小字符数指定为 8：

```
ciscoasa(config)# password-policy minimum-length 8
```

Related Commands

命令	说明
password-policylifetime	设置密码有效期值，以天为单位，在该值后密码到期。
password-policyminimum-changes	设置旧密码和新密码之间允许的最小已更改字符数。
password-policy minimum-lowercase	设置密码可以包含的最小小写字符数。

password-policy minimum-lowercase

要设置密码可能包含的最小小写字符数，请在全局配置模式下使用**password-policyminimum-lowercase**命令。要将对应的密码策略属性设置为其默认值，请使用此命令的 **no** 形式。

password-policy minimum-lowercase*值*
no password-policy minimum-lowercase*值*

Syntax Description

value	指定密码的最小小写字符数。有效值范围为 0 到 64 个字符。

Command Default

默认的最小小写字符数为 0，表示没有最低要求。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	—	• 是	• 支持	—

Command History

版本	修改
9.1(2)	添加了此命令。

使用指南

此命令设置密码可以包含的最小小写字符数。有效值范围为 0 到 64 个字符。

CR_Examples

以下示例将密码可具有的最小小写字符数指定为 6：

```
ciscoasa(config)# password-policy minimum-lowercase 6
```

Related Commands

命令	说明
password-policylifetime	设置密码有效期值，以天为单位，在该值后密码到期。
password-policyminimum-changes	设置新旧密码之间必须更改的最小字符数。
password-policy minimum-length	设置密码的最小长度。

password-policy minimum-numeric

要设置密码可包含的最小数字字符数，请在全局配置模式下使用 **password-policyminimum-numeric** 命令。要将对应的密码策略属性设置为其默认值，请使用此命令的 **no** 形式。

password-policy minimum-numeric*值*
no password-policy minimum-numeric*值*

Syntax Description

value	指定密码的最小数字字符数。有效值范围为 0 到 64 个字符。

Command Default

默认的最小数字字符数为 0，表示没有最小字符数。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	—	• 是	• 支持	—

Command History

版本	修改
9.1(2)	添加了此命令。

使用指南

此命令设置密码可以包含的最小数字字符数。有效值范围为 0 到 64 个字符。

CR_Examples

以下示例指定密码可包含的最小数字字符数为 8：

```
ciscoasa(config)# password-policy minimum-numeric 8
```

Related Commands

命令	说明
password-policylifetime	设置密码有效期值，以天为单位，在该值后密码到期。
password-policyminimum-changes	设置新旧密码之间必须更改的最小字符数。
password-policy minimum-length	设置密码的最小长度。

password-policy minimum-special

要设置密码可包含的最小特殊字符数，请在全局配置模式下使用 **password-policyminimum-special** 命令。要将对应的密码策略属性设置为其默认值，请使用此命令的 **no** 形式。

password-policy minimum-special*值*
no password-policy minimum-special*值*

Syntax Description

value	指定密码的最小特殊字符数。有效值范围为 0 到 64 个字符。

Command Default

默认的最小特殊字符数为 0，表示没有最小字符数。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	—	• 是	• 支持	—

Command History

版本	修改
9.1(2)	添加了此命令。

使用指南

此命令设置密码可以包含的特殊字符的最小数量。特殊字符包括以下字符：!、@、#、$、%、^、%、*、“(”和“)”。

CR_Examples

以下示例将密码可具有的最小特殊字符数指定为 2：

```
ciscoasa(config)# password-policy minimum-special 2
```

Related Commands

命令	说明
password-policylifetime	设置密码有效期值，以天为单位，在该值后密码到期。
password-policyminimum-changes	设置新旧密码之间必须更改的最小字符数。
password-policy minimum-length	设置密码的最小长度。

password-policy minimum-uppercase

要设置密码可包含的最小大写字符数，请在全局配置模式下使用**password-policyminimum-uppercase**命令。要将对应的密码策略属性设置为其默认值，请使用此命令的 **no** 形式。

password-policy minimum-uppercase*值*
no password-policy minimum-uppercase*值*

Syntax Description

value	指定密码的最小大写字符数。有效值范围为 0 到 64 个字符。

Command Default

默认的最小大写字符数为 0，表示没有最小字符数。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	—	• 是	• 支持	—

Command History

版本	修改
9.1(2)	添加了此命令。

使用指南

此命令设置密码可以包含的最小大写字符数。有效值范围为 0 到 64 个字符。

CR_Examples

以下示例将密码可包含的最小大写字符数指定为 4：

```
ciscoasa(config)# password-policy minimum-uppercase 4
```

Related Commands

命令	说明
password-policylifetime	设置密码有效期值，以天为单位，在该值后密码到期。
password-policyminimum-changes	设置新旧密码之间必须更改的最小字符数。
password-policy minimum-length	设置密码的最小长度。

password-policy reuse-interval

要禁止对本地用户名重复使用密码，请在全局配置模式下使用**password-policyreuse-interval** 命令。要删除此限制，请使用此**no**命令的形式。

password-policy reuse-interval值
no password-policy reuse-interval[*value*]

Syntax Description

value	设置创建新密码时可使用的先前密码的数量，该值介于2到7之间。

Command Default

此命令默认禁用。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
9.8(1)	我们引入了此命令。

使用指南

您可以禁止重复使用与以前使用过的密码相匹配的密码。先前的密码使用该命令以加密形式存储**username**在每个配置 **password-history**下；此命令不是用户可配置的。

CR_Examples

以下示例将密码续用间隔设置为 5：

```
ciscoasa(config)# password-policy reuse-interval 5
```

Related Commands

命令	说明
aaaauthenticationlogin-history	保存本地 **username** 登录历史。
password-history	存储以前的**username**密码。用户无法配置此命令。
password-policyreuse-interval	禁止重复使用**username**密码。
password-policyusername-check	禁止使用与 **username**名称匹配的密码。
showaaalogin-history	显示本地 **username** 登录历史记录。

命令	说明
username	配置本地用户。

密码策略用户名检查

要禁止与用户名匹配的密码，请在全局配置模式下使用**password-policyusername-check** 命令。要删除此限制，请使用此**no**命令的形式。

password-policy username-check
no password-policy username-check

Syntax Description

此命令没有任何参数或关键字。

Command Default

此命令默认禁用。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
9.8(1)	我们引入了此命令。

使用指南

可以禁止使用与 **username** 命令中的名称匹配的密码。

CR_Examples

以下示例限制密码与用户名 john_crichton 匹配：

```
ciscoasa(config)# password-policy username-check
ciscoasa(config)# username john_crichton password moya privilege 15
ciscoasa(config)# username aeryn_sun password john_crichton privilege 15
ERROR: Password must contain:
ERROR:  a value that complies with the password policy
ERROR: Username addition failed.
ciscoasa(config)#
```

Related Commands

命令	说明
aaaauthenticationlogin-history	保存本地 **username** 登录历史。
password-history	存储以前的**username**密码。用户无法配置此命令。
password-policyreuse-interval	禁止重复使用**username**密码。
password-policyusername-check	禁止使用与 **username**名称匹配的密码。

命令	说明
showaaalogin-history	显示本地 **username** 登录历史记录。
username	配置本地用户。

password-storage

要让用户在客户端系统上存储他们的登录密码，请在 **password-storageenable** 策略组配置模式或用户名配置模式下使用该命令。要禁用密码存储，请使用该 **password-storagedisable** 命令。

要从运行配置中删除密码存储属性，请使用此**no**命令的形式。这使得可以从另一个组策略继承密码存储的值。

password-storage { **enable** | **disable** }
no password-storage

Syntax Description

disable	禁用密码存储。
enable	启用密码存储。

Command Default

密码存储已禁用。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
组策略配置	• 是	—	• 是	—	—
用户名配置	• 是	—	• 是	—	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

仅在已知处于安全站点中的系统上启用密码存储。

此命令与交互式硬件客户端身份验证或硬件客户端的个人用户身份验证无关。

CR_Examples

以下示例显示如何为名为FirstGroup 的组策略启用密码存储：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# password-storage enable
```

peer-group

要标识 VXLAN 集群控制链路的 ASA virtual 集群节点，请在 nve 配置模式下使用 **peer-group** 命令。要删除对等组，请使用此命 **no**令的形式。

peer-group*network_object_name*
no peer-group*network_object_name*

Syntax Description

network_object_name	标识 **object-group network** 命令定义的网络对象。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
Nve 配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
9.17(1)	添加了此命令。

使用指南

通过使用命令创建网络对象组来识别 VTEP 对 **object-group network**等 IP 地址。

VTEP之间的基础IP网络独立于VNI接口使用的集群控制链路网络。VTEP网络可能包含其他设备，VTEP 对等体甚至可能不在同一子网中。

VTEP 源接口 IP 地址应作为对等体之一包含在网络对象组中。

CR_Examples

以下是使用内联定义的主机来创建网络对象组的示例：

```
ciscoasa(config)# object-group network cluster-peers
ciscoasa(network-object-group)# network-object host 10.6.6.51
ciscoasa(network-object-group)# network-object host 10.6.6.52
ciscoasa(network-object-group)# network-object host 10.6.6.53
ciscoasa(network-object-group)# network-object host 10.6.6.54
```

以下是创建引用独立网络对象的网络对象组的示例：

```
ciscoasa(config)# object network xyz
ciscoasa(config-network-object)# range 10.6.6.51 10.6.6.54
```

```
ciscoasa(config)# object-group network cluster-peers
ciscoasa(network-object-group)# network-object object xyz
```

以下示例将千兆以太网接口 0/7 定义为集群控制链路 VTEP 源接口，并将 cluster-peers 网络对象组标识为 peer-group：

```
interface gigabitethernet 0/7
    nve-only cluster
    nameif ccl
    ip address 10.6.6.51 255.255.255.0
    no shutdown

nve 1
    source-interface ccl
    peer-group cluster-peers

interface vni 1
    segment-id 1000
    vtep-nve 1
```

Related Commands

命令	说明
debugvxlan	调试 VXLAN 流量。
encapsulationvxlan	将 NVE 实例设置为 VXLAN 封装。
inspectvxlan	强制遵守标准 VXLAN 报头格式。
interfacevni	创建用于 VXLAN 标记的 VNI 接口。
nve	指定网络虚拟化终端实例。
nve-only cluster	指定 NVE 用于集群控制链路。
segment-id	指定 VNI 接口的 VXLAN 网段 ID。
showinterfacevni	显示 VNI 接口的参数、状态和统计信息，其桥接接口（如果已配置）的状态，以及与其关联的 NVE 接口。
shownve	显示 NVE 接口的参数、状态和统计信息，其载频接口（源接口）的状态，承载接口的 IP 地址，已将此 NVE 用作 VXLAN VTEP 的 VNI，以及与此 NVE 接口相关联的对等体 VTEP IP 地址。
source-interface	指定 VTEP 源接口。
vtep-nve	将 VNI 接口与 VTEP 源接口相关联。
vxlanport	设置 VXLAN UDP 端口。默认情况下，VTEP 源接口接收发往 UDP 端口 4789 的 VXLAN 流量。

peer-id-validate

要指定是否使用对等方的证书验证对等方的身份，请在**peer-id-validate**隧道组 ipsec-attributes 模式下使用该命令。要返回默认值，请使用此**no**命令形式。

peer-id-validate*option*
no peer-id-validate

Syntax Description

选项	指定以下选项之一： • ： **req**必需的 • ：**cert**如果有证书支持 • **nocheck**：不检查

Command Default

此命令的默认设置为 **req**。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
隧道组 ipsec 属性	• 是	—	• 是	—	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

您可以将此属性应用于所有 IPsec tunnel-group 类型。

CR_Examples

以下示例在 config-ipsec 配置模式下需要使用名为 209.165.200.225 的 IPsec LAN 间隧道组的对等体证书标识来验证对等体：

```
ciscoasa(config)# tunnel-group 209.165.200.225 type IPsec_L2L
ciscoasa(config)# tunnel-group 209.165.200.225 ipsec-attributes
ciscoasa(config-tunnel-ipsec)# peer-id-validate req
ciscoasa(config-tunnel-ipsec)#
```

Related Commands

命令	说明
clear-configuretunnel-group	清除所有配置的隧道组。
showrunning-configtunnel-group	显示所有隧道组或特定隧道组的隧道组配置。
tunnel-group ipsec-attributes	配置该组的隧道组 ipsec 属性。

peer ip

要手动指定对等体 VXLAN 隧道终端 (VTEP) IP 地址，请在 nve 配置模式下使用 **peerip**命令。要删除对等地址，请使用此命 **no**令的形式。

peer ip*ip_address*
no peer ip

Syntax Description

ip_address	设置对等体 VTEP IP 地址，包括 IPv4 或 IPv6。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
Nve 配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
9.4(1)	添加了此命令。
9.20(1)	此命令现在支持 IPv6。

使用指南

如果指定对等体 IP 地址，则无法使用组播组发现。在多情景模式中不支持组播，因此只能选择手动配置。只能为 VTEP 指定一个对等体。

CR_Examples

以下示例将 GigabitEthernet 1/1 接口配置为 VTEP 源接口，并指定对等 IP 地址为 10.1.1.2：

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# nve 1
ciscoasa(cfg-nve)# source-interface outside
ciscoasa(cfg-nve)# peer ip 10.1.1.2
```

Related Commands

命令	说明
debugvxlan	调试 VXLAN 流量。
default-mcast-group	为与 VTEP 源接口关联的所有 VNI 接口指定默认组播组。

命令	说明
encapsulationvxlan	将 NVE 实例设置为 VXLAN 封装。
inspectvxlan	强制遵守标准 VXLAN 报头格式。
interfacevni	创建用于 VXLAN 标记的 VNI 接口。
mcast-group	为 VNI 接口设置组播组地址。
nve	指定网络虚拟化终端实例。
nve-only	将 VXLAN 源接口指定为仅限 NVE。
peerip	手动指定对等 VTEP IP 地址。
segment-id	指定 VNI 接口的 VXLAN 网段 ID。
showarpvtep-mapping	显示 VNI 接口上缓存的与远程网段域中的 IP 地址和远程 VTEP IP 地址对应的 MAC 地址。
showinterfacevni	显示 VNI 接口的参数、状态和统计信息，其桥接接口（如果已配置）的状态，以及与其关联的 NVE 接口。
showmac-address-tablevtep-mapping	使用远程 VTEP IP 地址在 VNI 接口上显示第 2 层转发表（MAC 地址表）。
shownve	显示 NVE 接口的参数、状态和统计信息，其载频接口（源接口）的状态，承载接口的 IP 地址，已将此 NVE 用作 VXLAN VTEP 的 VNI，以及与此 NVE 接口相关联的对等体 VTEP IP 地址。
showvnivlan-mapping	显示透明模式下的 VNI 网段 ID 与 VLAN 接口或物理接口之间的映射。
source-interface	指定 VTEP 源接口。
vtep-nve	将 VNI 接口与 VTEP 源接口相关联。
vxlanport	设置 VXLAN UDP 端口。默认情况下，VTEP 源接口接收发往 UDP 端口 4789 的 VXLAN 流量。

perfmon

要显示性能信息，请在 **perfmon**特权 EXEC 模式下使用该命令。

perfmon{**verbose** | **interval**秒 | **quiet** | **settings**}[详细信息]

Syntax Description

verbose	在ASA控制台上显示性能监视器信息。
interval*seconds*	指定控制台上刷新性能显示前的秒数。
quiet	禁用性能监控显示。
settings	显示间隔以及它是安静的还是详细的。
detail	显示有关性能的详细信息。

Command Default

seconds 是 120 秒。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
特权 EXEC	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0	在ASA上添加了对此命令的支持。
7.2(1)	增加了对关 **detail**键字的支持。

使用指南

perfmon 命令允许您监控 ASA 的性能。使用 show perfmon 命令立即显示信息。使用 perfmon verbose 命令可每 2 分钟显示一次此信息。将 perfmon interval seconds 命令与 perfmon verbose 命令配合使用，每隔指定的秒数显示一次该信息。

系统显示性能信息示例，如下所示：

PERFMON统计信息：	当前	平均
Xlate	33/s	20/s
连接	110/s	10/s

TCP Conns	50/s	42/s
WebSns Req	4/s	2/s
TCP Fixup	20/s	15/s
HTTP 修复	5/s	5/s
FTP 修复	7/s	4/s
AAA 身份验证	10/s	5/s
AAA 创建者	9/s	5/s
AAA帐户	3/s	3/s

此信息列出每秒发生的转换、连接、Websense 请求、地址转换（称为“修复”）和 AAA 事务的数量。

CR_Examples

此示例显示如何在 ASA 控制台上每 30 秒显示一次性能监视器统计数据：

```
ciscoasa(config)# perfmon interval 120
ciscoasa(config)# perfmon quiet
ciscoasa(config)# perfmon settings
interval: 120 (seconds)
quiet
```

Related Commands

命令	说明
showperfmon	显示性能信息。

periodic

要为支持时间范围功能的功能指定重复（每周）时间范围，请在 **periodic** 时间范围配置模式下使用该命令。要禁用此功能，请使用此命令的 **no** 形式。

periodic*days-of-the-weektime***to** [*days-of-the-week*] *time*
no periodic*days-of-the-weektime***to** [*days-of-the-week*] *time*

Syntax Description

一周内某天	（可选）此参数第一次出现是关联时间范围生效的开始日期或星期几。第二次出现是指关联对账单生效的结束日期或星期几。 此参数是任意单日或多日组合：星期一、星期二、星期三、星期四、星期五、星期六和星期日。其他可能的值包括： • day - 星期一到星期日 • weekdays - 星期一至星期五 • Weekend - 星期六和星期日 如果一周的结束日期与一周的开始日期相同，则可以省略它们。
time	以 HH:MM 格式指定时间。例如，8:00 表示上午 8:00，20:00 表示晚上 8:00。
to	要填写“从开始时间到结束时间”的范围，需要输入 **to** 关键字。

Command Default

如果未与 **periodic** 命令一起输入值，则根据 **time-range** 命令定义对 ASA 的访问立即生效并始终有效。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
时间范围配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

要实现基于时间的 **time-range**ACL，请使用命令定义一天和一周的特定时间。然后使用命令将时 **access-listextendedtime-range**间范围绑定到 ACL。

periodic 命令是指定时间范围生效的方法之一。另一种方法是使用 **absolute** 命令指定绝对时间段。在 **time-range** 全局配置命令（该命令指定时间范围的名称）后使用这些命令。每个 **time-range** 命令允许多个 **periodic** 条目。

如果结束 days-of-the-week 值与开始值相同，则可以省略它们。

如果 **time-range**命令同时指定了 **absolute**和 **periodic**值，则仅在 **periodic**达到 **absolutestart**时间后评估命令，并且在达到 **absoluteend**时间后不会进一步评估。

时间范围功能依赖于 ASA 的系统时钟；但是，该功能与 NTP 同步配合使用效果最佳。

CR_Examples

以下是一些示例：

如果需要：	输入：
仅限星期一至星期五，上午 8:00 至下午 6:00	**periodicweekdays8:00to18:00**
仅限一周中的每天上午 8:00 至下午 6:00	**periodicdaily8:00to18:00**
从星期一上午 8:00 到星期五晚上 8:00 每分钟一次	**periodicmonday8:00tofriday20:00**
所有周末，从星期六早上到星期日晚上	**periodicweekend00:00to23:59**
星期六和星期日，从中午到午夜	**periodicweekend12:00to23:59**

以下示例显示如何允许仅在星期一至星期五的上午 8:00 至下午 6:00 访问 ASA：

```
ciscoasa(config-time-range)# periodic weekdays 8:00 to 18:00
ciscoasa(config-time-range)#
```

以下示例显示如何允许在特定日期（星期一、星期二和星期五）上午 10:30 至下午 12:30 访问 ASA：

```
ciscoasa(config-time-range)# periodic Monday Tuesday Friday 10:30 to 12:30
ciscoasa(config-time-range)#
```

Related Commands

命令	说明
absolute	定义时间范围生效时的绝对时间。
access-list extended	配置允许或拒绝 IP 流量通过 ASA 的策略。
default	恢复命令 **absolute**和 **periodic**关**time-range**键字的默认设置。
time-range	基于时间定义对 ASA 的访问控制。

periodic-authentication certificate

要启用定期证书验证，请使用 **periodic-authentication certificate**命令。要从默认组策略继承设置，请使用此命令的 **no** 形式。

periodic-authentication certificate<*time in hours*>**none**
no periodic-authentication certificate<*time in hours*>**none**

Syntax Description

时间（小时）	设置介于 1 和 168 小时之间的间隔。
none	禁用定期身份验证。

Command Default

定期证书验证默认处于禁用状态。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
默认策略组配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
9.4(1)	添加了此命令。

使用指南

默认情况下，对于默认组策略， 命令将为 **periodic-authenticationcertificatenone** 。其他组策略会从默认策略继承该设置，除非做出更改。

CR_Examples

```
100(config-group-policy)# periodic-authentication ?
group-policy mode commands/options:
  certificate  Configure periodic certificate authentication
100(config-group-policy)# periodic-authentication certificate ?
group-policy mode commands/options:
  <1-168>  Enter periodic authentication interval in hours
  none     Disable periodic authentication
100(config-group-policy)# periodic-authentication certificate ?
group-policy mode commands/options:
  <1-168>  Enter periodic authentication interval in hours
  none     Disable periodic authentication
100(config-group-policy)# help periodic-authentication
```

permit-errors

要允许无效 GTP 数据包或否则会解析失败并被丢弃的数据包，请在策略映射参数配置模式下使用 **permit-errors** 命令。返回到默认行为，其中所有无效数据包或解析失败的数据包都将被丢弃。请使用此命令的 **no** 形式。

permit-errors
no permit-errors

Syntax Description

此命令没有任何参数或关键字。

Command Default

默认情况下，所有无效数据包或解析失败的数据包都会被丢弃。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
参数配置	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

在 GTP 检测策略映射参数中使用 **permit-errors** 命令，以允许通过 ASA 发送消息检测期间无效或遇到错误的任何数据包，而不是丢弃这些数据包。根据在策略映射中定义的操作，仍然可以丢弃数据包。

CR_Examples

以下示例允许包含无效数据包或解析失败的数据包的流量通过：

```
ciscoasa(config)# policy-map type inspect gtp gtp-policy
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# permit-errors
```

Related Commands

命令	说明
policy-maptypeinspectgtp	定义 GTP 检查策略图。
inspectgtp	适用于特定的GTP映射，以用于应用检查。

permit-response

要配置 GSN 或 PGW 池，请在策略映射参数配置模式下使用 permit-response 命令。使用此命令的 **no** 形式可删除共享关系。

permit-responseto-object-group*to_obj_group_id***from-object-group***from_obj_group_id*
no permit-responseto-object-group*to_obj_group_id***from-object-group***from_obj_group_id*

Syntax Description

from-object-group源对象组 *ID*	标识 GSN/PGW 终端的网络对象组。这必须是对象组（**object-group** 命令）。这些终端可以向 **to-object-group**发送请求并接收响应。 从版本 9.5(1) 开始，对象组可以包含 IPv6 地址，而不仅仅是 IPv4 地址。
to-object-group目标对象组 *ID*	标识SGSN/SGW 的网络对象组。这必须是对象组（**object-group** 命令）。这些地址可以接收来自 **from-object-group**中标识的终端集的响应。 从版本 9.5(1) 开始，对象组可以包含 IPv6 地址，而不仅仅是 IPv4 地址。

Command Default

ASA 会丢弃 GTP 请求中未指定的 GSN 或 PGW 的 GTP 响应。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
参数配置模式	• 是	• 支持	• 支持	• 支持	—

Command History

版本	修改
7.0(4)	添加了此命令。GTP 检查仅支持 IPv4 地址。
9.5(1)	增加了对 IPv6 地址的支持。

使用指南

当 ASA 执行 GTP 检测时，ASA 默认会丢弃来自 GSN 或 PGW 而 GTP 请求中未指定的 GTP 响应。在 GSN 或 PGW 池中使用负载均衡来提供 GPRS 的效率和扩展性时，会发生这种情况。

要创建 GSN/PGW 轮询以便支持负载均衡，请创建一个指定 GSN/PGW 终端的网络对象组，并在 from-object-group 参数中指定该组。同样，为 SGSN/SGW 创建一个网络对象组并在 to-object-group 参数中选择该组。如果 GSN/PGW 响应与 GTP 请求被发送到的 GSN/PGW 属于同一个对象组，并且 SGSN/SGW 位于允许响应 GSN/PGW 向其发送 GTP 响应的对象组中，则 ASA 允许该响应。

网络对象组可通过主机地址或包含终端的子网标识它们。

CR_Examples

以下示例允许从 192.168.32.0 网络上的任何主机到 IP 地址为 192.168.112.57 的主机的 GTP 响应：

```
ciscoasa(config)# object-group network gsnpool32
ciscoasa(config-network)# network-object 192.168.32.0 255.255.255.0
ciscoasa(config)# object-group network sgsn1

ciscoasa(config-network)# network-object host 192.168.112.57
ciscoasa(config-network)# exit

ciscoasa(config)# policy-map type inspect gtp gtp-policy

ciscoasa(config-pmap)# parameters

ciscoasa(config-pmap-p)# permit-response to-object-group sgsn1 from-object-group gsnpool32
```

Related Commands

命令	说明
policy-maptypeinspectgtp	定义 GTP 检查策略图。
inspectgtp	适用于特定的GTP映射，以用于应用检查。
showservice-policyinspectgtp	显示 GTP 配置。

pfs

要启用 PFS，请在 **pfsenable** 策略组配置模式下使用该命令。要禁用 PFS，请使用该 **pfsdisable** 命令。要从运行配置中删除 PFS 属性，请使用此命令的 **no**形式。

pfs {**enable** | **disable**}
no pfs

Syntax Description

disable	禁用 PFS。
enable	启用 PFS。

Command Default

PFS 已禁用。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
组策略配置	• 是	—	• 是	—	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

VPN 客户端和 ASA 上的 PFS 设置必须匹配。

使用此命令的 **no** 形式可允许从其他组策略继承 PFS 的值。

在 IPsec 协商中，PFS 确保每个新的加密密钥与任何先前的密钥无关。

CR_Examples

以下示例显示如何为名为 FirstGroup 的组策略设置 PFS：

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# pfs enable
```

phone-proxy (已弃用)

要配置电话代理实例，请在 **phone-proxy**全局配置模式下使用该命令。

要删除电话代理实例，请使用此命 **no**令的形式。

phone-proxy*Phone_proxy_name*
no phone-proxy*Phone_proxy_name*

Syntax Description

Phone_proxy_name	指定电话代理实例的名称。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	—	• 是	—	—

Command History

版本	修改
8.0(4)	命令已添加。
9.4(1)	此命令已弃用。

使用指南

只能在 ASA 上配置一个电话代理实例。

如果为 HTTP 代理服务器配置了 NAT，则与 IP 电话相关的 HTTP 代理服务器的全局或映射 IP 地址将写入电话代理配置文件。

CR_Examples

以下示例显示如何使 **phone-proxy** 用命令配置电话代理实例：

```
ciscoasa
(config)# phone-proxy asa_phone_proxy
ciscoasa(config-phone-proxy)# tftp-server address 128.106.254.8 interface outside
ciscoasa
(config-phone-proxy)#
media-termination address 192.0.2.25 interface inside
ciscoasa
(config-phone-proxy)#
media-termination address 128.106.254.3 interface outside
ciscoasa(config-phone-proxy)# tls-proxy asa_tlsp
ciscoasa
```

```
(config-phone-proxy)#
ctl-file asactl
ciscoasa
(config-phone-proxy)#
cluster-mode nonsecure
ciscoasa
(config-phone-proxy)#
timeout secure-phones 00:05:00
ciscoasa
(config-phone-proxy)#
disable service-settings
```

Related Commands

命令	说明
ctl-file(global)	指定要为电话代理配置创建的 CTL 文件，或指定要从闪存中解析的 CTL 文件。
ctl-file(phone-proxy)	指定用于电话代理配置的 CTL 文件。
tls-proxy	配置 TLS 代理实例。

pim

要重新启用接口上的 PIM，请在接口配置模式下使用 **pim** 命令。要禁用 PIM，请使用此命 **no**令的形式。

pim
no pim

Syntax Description

此命令没有任何参数或关键字。

Command Default

默认情况下， **multicast-routing** 命令会在所有接口上启用 PIM。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
接口配置	• 是	—	• 是	—	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

默认情况下， **multicast-routing** 命令会在所有接口上启用 PIM。仅 **no** 命令的 **pim** 形式会保存在配置中。

注释 PAT 不支持 PIM。PIM 协议不使用端口，而 PAT 仅适用于使用端口的协议。

CR_Examples

以下示例在所选接口上禁用 PIM：

```
ciscoasa(config-if)# no pim
```

Related Commands

命令	说明
multicast-routing	在 ASA 上启用组播路由。

pim accept-register

要配置 ASA 以筛选 PIM 注册消息，请在全局配置模式下使用 **pim accept-register** 命令。要删除过滤，请使用此命 **no**令的形式。

pimaccept-register{**list***acl* | **route-map**映射名称}
no pim accept-register

Syntax Description

list*acl*	指定访问列表名称或编号。使用此命令时只能使用扩展主机ACL。
route-map*map-name*	指定 route-map 名称。在引用的路由映射中使用扩展主机 ACL。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	—	• 是	—	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

此命令用于防止未授权的源向 RP 注册。如果未授权的源向 RP 发送注册消息，ASA 将立即发回注册停止消息。

CR_Examples

以下示例将 PIM 注册消息限制为来自名为“no-ssm-range”的访问列表中定义的源的注册消息：

```
ciscoasa(config)# pim accept-register list no-ssm-range
```

Related Commands

命令	说明
multicast-routing	在 ASA 上启用组播路由。

pim bidir-neighbor-filter

要控制哪些支持 bidir 的邻居可参与 DF 选举，请在接口配置模式下使用 **pim bidir-neighbor-filter** 命令。要删除过滤，请使用此命 **no**令的形式。

pim bidir-neighbor-filter*acl*
no pim bidir-neighbor-filter*acl*

Syntax Description

acl	指定访问列表名称或编号。此访问列表定义可以参与 bidir DF 选举的邻居。在此命令中仅使用标准 ACL；不支持扩展 ACL。

Command Default

所有路由器都被视为支持 bidir。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
接口配置	• 是	—	• 是	—	—

Command History

版本	修改
7.2(1)	添加了此命令。

使用指南

双向 PIM 允许组播路由器保持减少的状态信息。要选择 DF，必须为 bidir 双向启用分片中的所有组播路由器。

该命令允许您指定应参与 DF **pimbidir-neighbor-filter**选举的路由器，同时仍允许所有路由器参与稀疏模式域，从而实现从仅稀疏模式网络到双向网络的转换。支持 bidir 的路由器可以从它们本身当中选择 DF，即使分片上有非 bidir 路由器。非 bidir 路由器上的组播边界可防止 bidir 组中的 PIM 消息和数据泄漏到 bidir 子集云中或从 bidir 子集云泄漏出去。

启用该 **pimbidir-neighbor-filter**命令后，ACL 允许的路由器将被视为具有 bidir 功能。因此：

- 如果允许的邻居不支持 bidir，则不会发生 DF 选举。
- 如果被拒绝的邻居支持 bidir，则不会发生 DF 选举。
- 如果一个被拒绝的邻居不支持 bidir，可能会发生 DF 选举。

CR_Examples

以下示例允许 10.1.1.1 成为 PIM bidir 邻居：

```
ciscoasa(config)# access-list bidir_test permit 10.1.1.1 255.255.255.55
ciscoasa(config)# access-list bidir_test deny any
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# pim bidir-neighbor-filter bidir_test
```

Related Commands

命令	说明
multicastboundary	为管理范围的多播地址定义多播边界。
multicast-routing	在 ASA 上启用组播路由。

pim bsr-border

要阻止通过接口发送或接收自举路由器 (BSR) 消息，请在接口配置模式下使用 pim bsr-border 命令。

注释 对于 PIM 稀疏模式 (PIM-SM) 域中的边界接口，需要采取特殊的预防措施，以避免与可通过该接口访问的相邻域交换某些流量，尤其是在该域同时运行 PIM-SM 的情况下。

pim bsr-border
no pim bsr-border

Syntax Description

此命令没有任何参数或关键字。

Command Default

该命令默认为禁用。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
接口配置	• 是	—	• 是	—	—

Command History

版本	修改
9.5(2)	添加了此命令。

使用指南

当在接口上配置此命令时，将不会通过该接口发送或接收任何 PIM 版本 2 BSR 消息。使用此命令配置与另一个 PIM 域邻接的接口，以避免在两个域之间交换 BSR 消息。不应在不同的域之间交换 BSR 消息，因为一个域中的路由器可能会选举另一个域中的交汇点 (RP)，从而导致协议故障或失去域之间的隔离。

注释 此命令不会设置组播边界。它仅设置 PIM 域 BSR 消息边界。

CR_Examples

以下示例将接口配置为 PIM 域边界：

```
ciscoasa(config)# interface gigabit 0/0
ciscoasa(config-if)# pim bsr-border
ciscoasa(config)# show runn interface gigabitEthernet 0/0
!
```

```
interface GigabitEthernet0/0
 nameif outsideA
 security-level 0
 ip address 2.2.2.2 255.255.255.0
 pim bsr-border
```

Related Commands

命令	说明
multicast-routing	在ASA上启用组播路由。
pim bsr-candidate	将 ASA 配置为候选 BSR

pim bsr-candidate

要配置路由器宣布其作为引导程序路由器 (BSR) 的候选，请在全局配置模式下使用 pim bsr-candidate 命令。要删除此路由器作为引导程序路由器的候选者，请使用此命令的 no 形式。

pim bsr-candidate*interface-name* [*hash-mask-length* [*priority*]]
nopim bsr-candidate

Syntax Description

interface-name	从其派生 BSR 地址的此路由器上的接口名称。此地址在 BSR 消息中发送。
散列掩码长度	（可选）在调用 PIMv2 哈希函数之前，要与组地址进行“与”运算的掩码长度（最多 32 位）。所有具有相同种子哈希的组都对应相同的会合点 (RP)。 例如，如果此值为 24，则组地址只有前 24 位起作用。散列掩码长度允许一个 RP 用于多个组。 默认散列掩码长度为 0。
priority	（可选）候选 BSR (C-BSR) 的优先级。范围是从 0 到 255。优先选择具有最高优先级值的 C-BSR。如果优先级值相同，则 IP 地址较大的路由器是 BSR。 默认优先级为 0。

Command Default

该命令默认为禁用。

当将设备配置为没有散列长度和优先级的 bsr 候选者时，它假设默认散列长度为 0，优先级为 0。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	—	• 是	—	—

Command History

版本	修改
9.5(2)	添加了此命令。

使用指南

此命令导致 ASA 将引导程序消息发送到其所有 PIM 邻居，其中指定接口的地址作为 BSR 地址。每个邻居会将 BSR 地址与它从先前引导程序消息（不必在同一接口上接收）中获取的地址进行比较。如果当前地址是相同或更高的地址，则它缓存当前地址并转发引导程序消息。否则，它会丢弃引导程序消息。

此 ASA 将继续作为 BSR，直到收到来自另一个候选 BSR 的引导程序消息，表明自己具有更高的优先级（或者，如果优先级相同，则具有更高的 IP 地址）。

CR_Examples

以下示例将 ASA 配置为内部接口上的候选自举路由器 (C-BSR)，散列长度为 30，优先级为 10：

```
ciscoasa(config)# pim bsr-candidate inside 30 10
ciscoasa(config)# sh runn pim
pim bsr-candidate inside 30 10
```

Related Commands

命令	说明
multicast-routing	在ASA上启用组播路由。
pim bsr-border	将 ASA 配置为边界 BSR

pim dr-priority

要在 ASA 上配置用于指定路由器选举的邻居优先级，请在接口配置模式下使用 **pimdr-priority** 命令。要恢复默认优先级，请使用此命 **no**令的形式。

pim dr-priority编号
no pim dr-priority

Syntax Description

number	介于 0 到 4294967294 之间的数字。在确定指定路由器时，此数字用于确定设备的优先级。指定 0 可防止 ASA 成为指定路由器。

Command Default

默认值为 1。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
接口配置	• 是	—	• 是	—	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

接口上具有最大优先级值的设备将成为 PIM 指定路由器。如果多台设备具有相同的指定路由器优先级，则具有最高 IP 地址的设备将成为 DR。如果设备在 Hello 消息中未包含 DR-Priority 选项，则该设备会被视为优先级最高的设备并成为指定路由器。如果多台设备未在其Hello消息中包含此选项，则具有最高 IP 地址的设备将成为指定路由器。

CR_Examples

以下示例将接口的 DR 优先级设置为 5：

```
ciscoasa(config-if)# pim dr-priority 5
```

Related Commands

命令	说明
multicast-routing	在ASA上启用组播路由。

pim hello-interval

如要配置 PIM 呼叫消息的频率，请在接口配置模式下使用 **pimhello-interval** 命令。要将 hello-interval 恢复为默认值，请使用此命令的 **no**形式。

pim hello-interval秒
no pim hello-interval [秒]

Syntax Description

seconds	ASA 在发送 hello 消息之前等待的秒数。值的范围为 1 到 3600 秒。默认值为 30 秒。

Command Default

间隔默认为30秒。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
接口配置	• 是	—	• 是	—	—

Command History

版本	修改
7.0(1)	添加了此命令。

CR_Examples

以下示例将 PIM 呼叫间隔设置为 1 分钟：

```
ciscoasa(config-if)# pim hello-interval 60
```

Related Commands

命令	说明
multicast-routing	在 ASA 上启用组播路由。

pim join-prune-interval

如要配置 PIM 加入/删除间隔，请在接口配置模式下使用 **pimjoin-prune-interval** 命令。要将间隔恢复为默认值，请使用此命令的 **no**形式。

pimjoin-prune-interval秒
no pimjoin-prune-interval [*seconds*]

Syntax Description

seconds	ASA 在发送加入/删除消息之前等待的秒数。有效值范围为 10 至 600 秒。默认值为 60 秒。

Command Default

默认间隔为 60 秒

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
接口配置	• 是	—	• 是	—	—

Command History

版本	修改
7.0(1)	添加了此命令。

CR_Examples

以下示例将 PIM 加入/删除间隔设置为 2 分钟：

```
ciscoasa(config-if)# pim join-prune-interval 120
```

Related Commands

命令	说明
multicast-routing	在ASA上启用组播路由。

pim neighbor-filter

要控制哪些邻居路由器可以加入 PIM，请在接口配置模式下使用 **pimneighbor-filter** 命令。要删除过滤，请使用此命 **no**令的形式。

pim neighbor-filter*acl*
no pim neighbor-filter*acl*

Syntax Description

acl	指定访问列表名称或编号。在此命令中仅使用标准 ACL；不支持扩展 ACL。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
接口配置	• 是	—	• 是	—	—

Command History

版本	修改
7.2(1)	添加了此命令。

使用指南

此命令定义了可以参与 PIM 的邻居路由器。如果配置中不存在此命令，则没有限制。

必须启用组播路由和 PIM，此命令才会显示在配置中。如果禁用组播路由，则会从配置中删除此命令。

CR_Examples

以下示例允许 IP 地址为 10.1.1.1 的路由器成为接口 GigabitEthernet 0/2 上的 PIM 邻居：

```
ciscoasa(config)# access-list pim_filter permit 10.1.1.1 255.255.255.55
ciscoasa(config)# access-list pim_filter deny any
ciscoasa(config)# interface gigabitEthernet0/2
ciscoasa(config-if)# pim neighbor-filter pim_filter
```

Related Commands

命令	说明
multicast-routing	在 ASA 上启用组播路由。

pim old-register-checksum

要在使用旧注册校验和方法的交汇点 (RP) 上实现向后兼容，请在全局配置模式下使用 **pim old-register-checksum** 命令。要生成符合 PIM RFC 标准的寄存器，请使用此命令的 **no** 形式。

pim old-register-checksum
no pim old-register-checksum

Syntax Description

此命令没有任何参数或关键字。

Command Default

ASA 可生成符合 PIM RFC 标准的寄存器。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	—	• 是	—	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

ASA 软件接受在 PIM 报头以及仅接下来 4 个字节上包含校验和的注册消息，而不是使用思科 IOS 方法 - 接受具有所有 PIM 消息类型的完整 PIM 消息的注册消息。 **pimold-register-checksum** 命令生成与 Cisco IOS 软件兼容的寄存器。

CR_Examples

以下示例将 ASA 配置为使用旧校验和计算：

```
ciscoasa(config)# pim old-register-checksum
```

Related Commands

命令	说明
multicast-routing	在 ASA 上启用组播路由。

pim rp-address

要配置 PIM 交汇点 (RP) 的地址，请在全局配置模式下使用 **pimrp-address** 命令。输入重试计数器值，即轮询代理服务器以检查其可用性之前等待的 **no**时间。

pim rp-address*ip_address*[*acl*] [**bidir**]
no pim rp-address*ip_address*

Syntax Description

acl	（可选）定义 RP 应与哪些多播组一起使用的标准访问列表的名称或编号。请勿在使用此命令时一起使用主机 ACL。
bidir	（可选）指示指定的组播组将在双向模式下运行。如果配置 命令时不使用此选项，则指定的组将在 PIM 稀疏模式下运行。
ip_address	将成为 PIM RP 的路由器的 IP 地址。这是一个由四部分点分十进制表示的单播 IP 地址。

Command Default

未配置 PIM RP 地址。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	—	• 是	—	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

公共 PIM 稀疏模式 (PIM-SM) 或 bidir 域内的所有路由器都需要了解众所周知的 PIM RP 地址。使用此命令静态配置地址。

注释 ASA 不支持自动 RP；您必须使 **pimrp-address**用命令指定 RP 地址。

您可以配置单个 RP 来为多个组提供服务。访问列表中指定的组范围决定了 PIM RP 组映射。如果未指定访问列表，则该组的 RP 将应用于整个 IP 多播组范围 (224.0.0.0/4)。

注释 无论实际的 bidir 配置如何，ASA 始终在 PIM hello 消息中通告 bidir 功能。

CR_Examples

以下示例将所有组播组的 PIM RP 地址设置为 10.0.0.1：

```
ciscoasa(config)# pim rp-address 10.0.0.1
```

Related Commands

命令	说明
pimaccept-register	配置候选RP，过滤PIM注册消息。

pim spt-threshold infinity

要更改最后一跳路由器的行为以始终使用共享树且从不执行最短路径树 (SPT) 切换，请在全局配置模式下使用 **pim spt-threshold infinity** 命令。要恢复默认值，请使用此命 **no**令的形式。

pim spt-threshold infinity [**group-list***acl*]
no pim spt-threshold

Syntax Description

group-list*acl*	（可选）指示受访问列表限制的源组。*acl* 参数必须指定标准 ACL；不支持扩展 ACL。

Command Default

默认情况下，最后一跳 PIM 路由器切换到最短路径源树。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
全局配置	• 是	—	• 是	—	—

Command History

版本	修改
7.0(1)	添加了此命令。

使用指南

如果未使用 **group-list** 关键字，则此命令适用于所有组播组。

CR_Examples

以下示例导致最后一跳 PIM 路由器始终使用共享树而不是切换到最短路径源树：

```
ciscoasa(config)# pim spt-threshold infinity
```

Related Commands

命令	说明
multicast-routing	在 ASA 上启用组播路由。

ping

要测试从指定接口到 IP 地址的连接，请在 **ping**特权 EXEC 模式下使用该命令。与 TCP ping 相比，常规的基于 ICMP 的 ping 可用的参数有所不同。输入不带参数的命令，系统会提示输入值，包括不能用作参数的特征。

ping [*if_name*] *host* [**repeat***count*] [**timeout***seconds*] [**data***pattern*] [**size***bytes* [**validate**]
ping tcp [*if_name*] *host port* [**repeat***count*] [**timeout***seconds*] [**source***host port*]
ping

注释 source 和 port 选项仅与 tcp 选项配合使用； data、size 和 validate 选项不适用于 tcp 选项。

Syntax Description

data*pattern*	（可选，仅限 ICMP。）指定十六进制格式的 16 位数据模式，范围为 0 到 FFFF。默认值为 0xabcd。
host	指定要 ping 的主机的 IPv4 地址或名称。对于 ICMP ping，可以指定 IPv6 地址（TCP ping 不支持该地址）。 使用主机名时，名称可以是 DNS 名称或使用 **name** 命令分配的名称。DNS 名称的最大字符数为 128，使用 **name** 命令创建的名称的最大字符数为 63。必须配置 DNS 服务器以使用 DNS 名称。
if_name	（可选）指定用于 ping 源的 IP 地址的接口名称；但实际的出口接口是通过使用数据路由表的路由查找来确定的。
port	（仅限 TCP。）为您正在 ping 的主机指定 TCP 端口号 (1-65535)。
repeat计数	（可选）指定重复 ping 请求的次数。默认值为 5。
size*bytes*	（可选，仅限 ICMP。）指定数据报大小（以字节为单位）。默认值为 100。
source*hostport*	（可选，仅限 TCP。）指定从其发送 ping 的某个 IP 地址和端口（对于随机端口，使用端口 = 0）。源地址不会影响数据包的路由方式。
tcp	（可选）测试基于 TCP 的连接（默认为 ICMP）。TCP ping 发送 SYN 数据包，如果目标发送了 SYN-ACK 数据包，则认为 ping 取得了成功。您还可以同时运行最多 2 个 TCP ping 操作。
timeout*seconds*	（可选）指定超时间隔的秒数。默认值为 2 秒。
validate	（可选，仅限 ICMP。）验证回复数据。

Command Default

无默认行为或值。

Command Modes

下表展示可输入命令的模式：

命令模式	防火墙模式		安全情景		
	路由	透明	一个	多个	
				情景	系统
特权 EXEC	• 是	• 支持	• 支持	• 支持	• 支持

Command History

版本	修改
7.0(1)	添加了此命令。
7.2(1)	添加了对 DNS 名称的支持。
8.4(1)	添加了 **tcp** 选项。
9.18(2)	如果您在命令中指定接口，则源IP地址与指定的接口IP地址匹配，但实际出口接口将由使用数据路由表的路由查找来确定。

使用指南

该 **ping**命令允许您确定 ASA 是否具有连接或网络上是否有主机可用。

当使用基于 ICMP 的常规 ping 时，请确保您没有禁止这些数据包的 **icmp**规则（如果您不使用 ICMP 规则，则允许所有 ICMP 流量）。如果希望内部主机通过 ICMP 对外部主机 ping 操作，必须执行以下操作之一：

- 创建用于回应应答的 ICMP **access-list** 命令；例如，要为所有主机提供 ping 访问权限，请使用 **access-listacl_grppermiticmpanyany** 命令，然后将 **access-list** 命令绑定到要使用 **access-group** 命令测试的接口。
- 使用 **inspecticmp** 命令配置 ICMP 检测引擎。例如，将 **inspecticmp** 命令添加到全局服务策略的 **classdefault_inspection** 类，将允许通过 ASA 对内部主机发起的回应请求进行回应。

使用 TCP ping 时，您必须确保访问策略允许在您指定的端口上的 TCP 流量。

需要此配置来允许 ASA 响应并接受从命令生成的 **ping**消息。 **ping** 命令输出显示是否接收了响应。如果输入 **ping** 命令后主机未响应，将出现如下所示的类似消息：

```
ciscoasa(config)# ping 10.1.1.1

Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
?????
Success rate is 0 percent (0/5)
```

ASA 会使用数据路由表来路由ping数据包，并且仅当数据表中没有匹配的路由时才会回退到管理路由表。为 TCP ping 指定源 IP 地址不会影响数据包的路由方式。例如，即使您手动指定源地址来匹配接口 IP 地址，也不会从该接口发出 ping。出口接口仅由 路由查找确定。

使用该 **showinterface**命令确保 ASA 已连接到网络并正在传输流量。指定 *if_name* 的地址用作 ping 的源地址，除非指定了其他源地址（仅限 TCP ping）。

您还可以输入不带参数的 **ping** 来执行扩展 ping。系统将提示您输入参数，包括一些不能用作关键字的特征。

CR_Examples

以下示例显示如何确定其他 IP 地址对 ASA 是否可见：

```
ciscoasa# ping 171.69.38.1
Sending 5, 100-byte ICMP Echos to 171.69.38.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

以下示例使用 DNS 名称指定主机：

```
ciscoasa# ping www.example.com
Sending 5, 100-byte ICMP Echos to www.example.com, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

以下是扩展 ping 的示例：

```
ciscoasa# ping
TCP [n]:
Interface: outside
Target IP address: 171.69.38.1
Repeat count: [5]
Datagram size: [100]
Timeout in seconds: [2]
Extended commands [n]:
Sweep range of sizes [n]:
Sending 5, 100-byte ICMP Echos to 171.69.38.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
The following are examples of the ping tcp command:
ciscoasa# ping
TCP [n]: yes
Interface: dmz
Target IP address: 10.0.0.1
Target IP port: 21
Specify source? [n]: y
Source IP address: 192.168.2.7

Source IP port: [0] 465

Repeat count: [5]
Timeout in seconds: [2] 5

Type escape sequence to abort.
Sending 5 TCP SYN requests to 10.0.0.1 port 21
from 192.168.2.7 starting port 465, timeout is 5 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
ciscoasa# ping tcp 10.0.0.1 21
Type escape sequence to abort.
No source specified. Pinging from identity interface.
Sending 5 TCP SYN requests to 10.0.0.1 port 21
from 10.0.0.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
ciscoasa# ping tcp 10.0.0.1 21 source 192.168.1.1 2002 repeat 10
Type escape sequence to abort.
Sending 10 TCP SYN requests to 10.0.0.1 port 21
```

```
from 192.168.1.1 starting port 2002, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 1/2/2 ms
ciscoasa(config)# ping tcp www.example.com 80
Type escape sequence to abort.
No source specified. Pinging from identity interface.
Sending 5 TCP SYN requests to 74.125.19.103 port 80
from 171.63.230.107, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/4/4 ms
ciscoasa# ping tcp 192.168.1.7 23 source 192.168.2.7 24966
Type escape sequence to abort.
Source port 24966 in use! Using port 24967 instead.
Sending 5 TCP SYN requests to 192.168.1.7 port 23
from 192.168.2.7 starting port 24967, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Related Commands

命令	说明
icmp	为在接口终止的ICMP流量配置访问规则。
showinterface	显示有关 VLAN 配置的信息。

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。