在ASA 5500系列上配置TCP状态旁路功能

目录

简介

本文档介绍如何配置TCP状态旁路功能，该功能允许出站和入站流量通过单独的Cisco ASA 5500系列自适应安全设备(ASA)。

先决条件

要求

Cisco ASA必须至少安装基本许可证，才能继续执行本文档中描述的配置。

使用的组件

本文档中的信息基于运行软件版本9.x的Cisco ASA 5500系列。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

背景信息

本节概述TCP状态绕行功能和相关支持信息。

TCP状态绕行功能概述

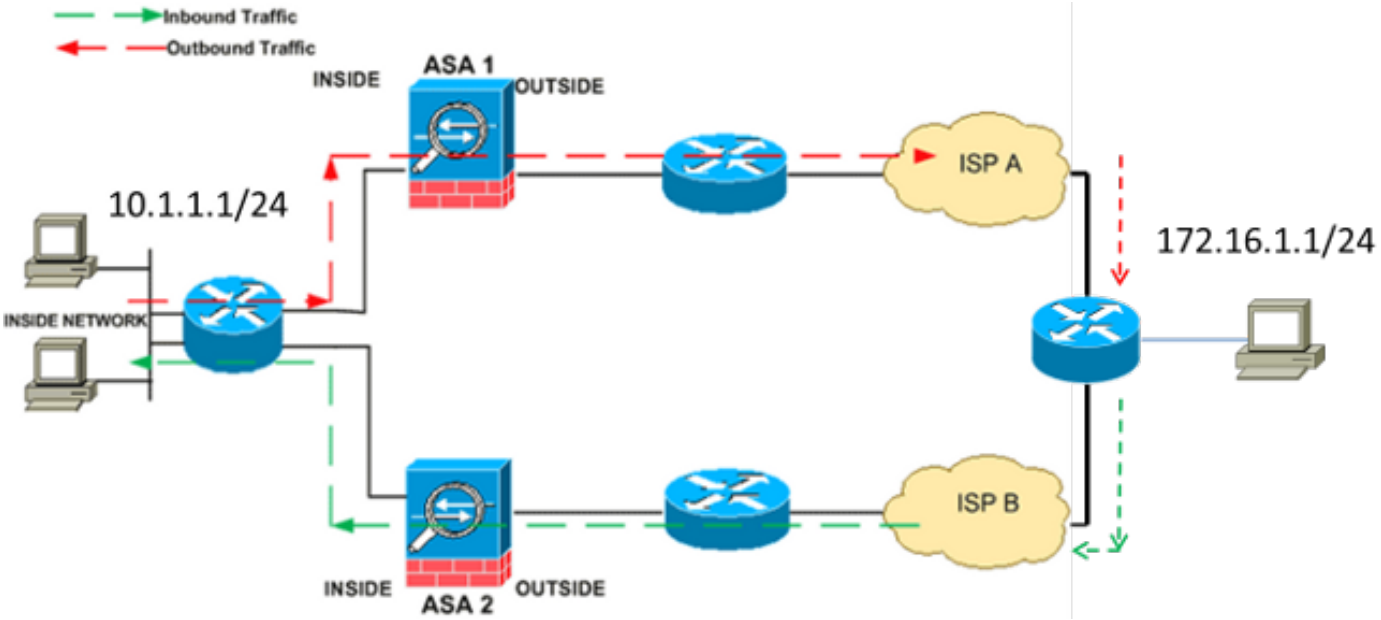
默认情况下，通过ASA的所有流量都通过自适应安全算法进行检查，并根据安全策略允许或丢弃。为了最大限度地提高防火墙性能，ASA检查每个数据包的状态（例如，它检查它是新连接还是已建立连接），并将其分配给会话管理路径(新连接同步(SYN)数据包)、快速路径（已建立连接）或控制平面路径（高级检查）。

匹配快速路径中当前连接的TCP数据包可以通过ASA，而无需重新检查安全策略的每个方面。此功能可最大限度地提高性能。但是，在快速路径（使用SYN数据包）中建立会话所使用的方法和在快速路径（如TCP序列号）中发生的检查可能会阻碍非对称路由解决方案；连接的出站和入站流量必须通过同一ASA。

例如，新连接将转到*ASA 1*。SYN数据包将通过会话管理路径，并且连接的条目将添加到快速路径表中。如果此连接上的后续数据包通过*ASA 1*，则数据包与快速路径中的条目匹配并通过。如果后续数据包转到*ASA 2*，且没有SYN数据包通过会话管理路径，则快速路径中没有用于连接的条目，并且数据包将被丢弃。

如果在上游路由器上配置了非对称路由，并且流量在两个ASA之间交替，则可以为特定流量配置TCP状态绕行功能。TCP状态绕行功能改变会话在快速路径中建立的方式并禁用快速路径检查。此功能处理TCP流量的方式与处理UDP连接的方式相同：当与指定网络匹配的非SYN数据包进入ASA，且没有快速路径条目时，该数据包将通过会话管理路径以在快速路径中建立连接。进入快速路径后，流量会绕过快速路径检查。

此映像提供非对称路由示例，其中出站流量通过与入站流量不同的ASA:



注意：默认情况下，Cisco ASA 5500系列上禁用TCP状态旁路功能。此外，如果TCP状态旁路配置未正确实施，则可能导致大量连接。

支持信息

本节介绍TCP状态旁路功能的支持信息。

- **上下文模式** - - TCP状态绕行功能在单情景和多情景模式下受支持。
- **防火墙模式** - TCP状态绕行功能在路由和透明模式下受支持。
- **故障转移** — TCP状态绕行功能支持故障转移。

使用TCP状态旁路功能时，不支持以下功能：

- **应用检测** - Application检测要求入站和出站流量都通过同一ASA，因此TCP状态绕行功能不支持应用检测。
- **身份验证、授权和记帐(AAA)已验证会话** - 当用户使用一个ASA进行身份验证时，通过另一个ASA返回的流量将被拒绝，因为用户未使用该ASA进行身份验证。
- **TCP拦截、最大初期连接限制、TCP序列号随机化** Â A ASA不跟踪连接状态，因此不应用这些功能。
- **TCP规范化** — TCP规范器已禁用。
- 安全服务模块(SSM)和安全服务卡(SSC)功能 — 您不能将TCP状态绕行功能用于在SSM或SSC上运行的任何应用，如IPS或内容安全(CSC)。

  注意：由于转换会话是为每个ASA单独建立的，请确保在两个ASA上为TCP状态绕行流量配置静态网络地址转换(NAT)。如果使用动态NAT，则为ASA 1上的会话选择的地*址将*与为ASA 2上的会话选择的地*址不同*。

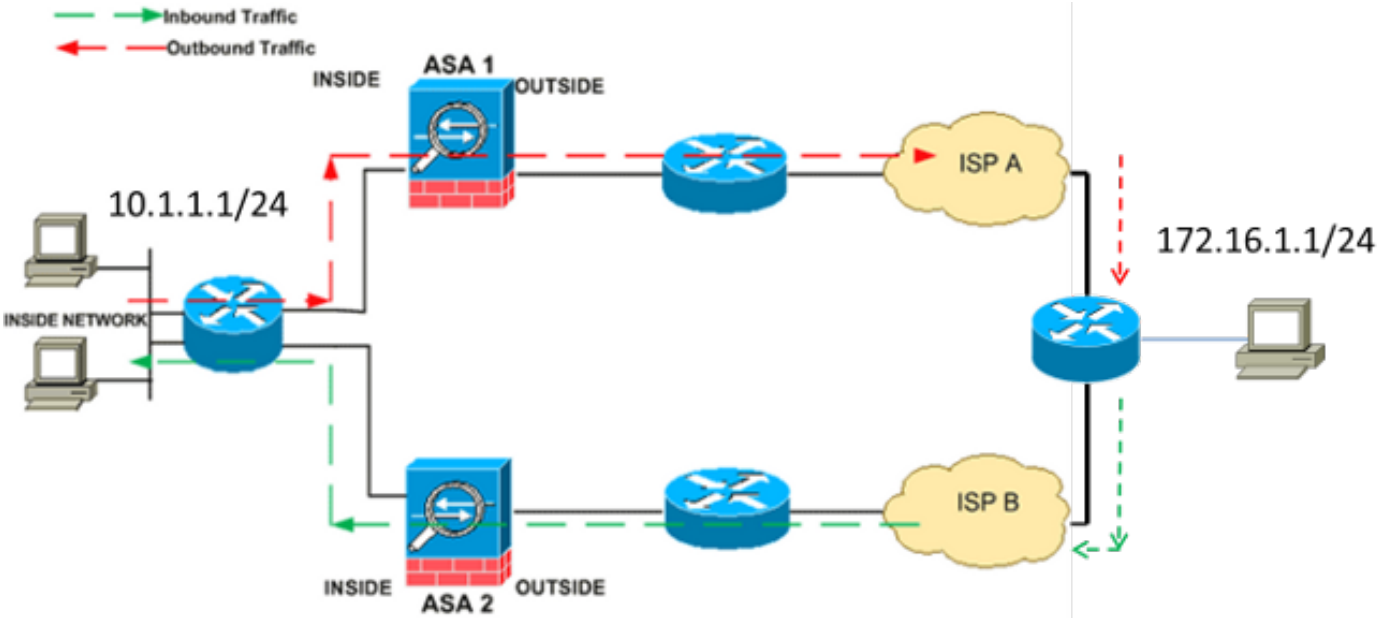
配置

本节介绍如何在两种不同场景中配置ASA 5500系列的TCP状态旁路功能。

注意：使用命令查找工具(仅注册客户)可获取有关本节中使用的命令的详细信息。

场景 1

这是用于第一个场景的拓扑：



注意：您必须将本节中介绍的配置应用到两个ASA。

要配置TCP状态旁路功能，请完成以下步骤：

1. 输入class-map class_map_name命令以创建类*映射*。类映射用于标识要禁用状态防火墙检测的流量。**注意**：本示例中使用的类映射是**tcp_bypass**。
```
ASA(config)#class-map tcp_bypass
```
2. 输入match parameter命令以指定类映射中关注的流量。使用模块化策略框架时，请在*类映射配置模式*下使用**match access-list** 命令，以便使用访问列表识别要应用操作的流量。以下是此配置的示例：

```
ASA(config)#class-map tcp_bypass
ASA(config-cmap)#match access-list tcp_bypass
```
注意：**tcp_bypass**是本示例中使用的访问列表的名称。有关如何指定所关注流量的详细信息，*请参阅Cisco ASA 5500系列配置指南8.2的识别流量（第3/4层类映射）部分。*
3. 输入policy-map name命令以添加策略映射或编辑策略映射（已存在），该策略映射为指定的类映射流量分配要执行的操作。在使用模块化策略框架时，请在全局配置模式下使用policy-map命令(不带*type*关键字)，以便为使用第3/4层类映射标识的流量分配操作(*class-map*或class-map type management命令)。 在本示例中，策略映射为**tcp_bypass_policy**:

```
ASA(config-cmap)#policy-map tcp_bypass_policy
```
4. 在*policy-map configuration* 模式下输入class 命令，以便将已创建的类映射(*tcp_bypass*)分配到策略映射(*tcp_bypass_policy*)，以便您可以将操作分配到类映射流量。在本例中，类映射为**tcp_bypass**:

```
ASA(config-cmap)#policy-map tcp_bypass_policy
ASA(config-pmap)#class tcp_bypass
```
5. 在类配置模式下输入set connection advanced-options tcp-state-bypass命令以*启用TCP状态绕行功能*。此命令在8.2(1)版中引入。 可从*策略映射配置模式*访问类配置模式，如本示例所示：

```
ASA(config-cmap)#policy-map tcp_bypass_policy
ASA(config-pmap)#class tcp_bypass
ASA(config-pmap-c)#set connection advanced-options tcp-state-bypass
```

6. 输入service-policy policymap_name [global | interface *intf*]命令，以便在所有接口或目标接口上全局激活策略映射。要禁用服务策略，请使用此**命令**的no形式。输入**service-policy**命令以在接口上启用一组策略。**global**关键字将策略映射应用于所有接口，而**interface**关键字将策略映射仅应用于一个接口。仅允许有一个全局策略。要覆盖接口上的全局策略，可以将服务策略应用到该接口。您只能将一个策略映射应用到每个接口。示例如下：

```
ASA(config-pmap-c)#service-policy tcp_bypass_policy outside
```

以下是ASA1上TCP状态绕行功能的*示例配置*:

```
!--- Configure the access list to specify the TCP traffic
!--- that needs to by-pass inspection to improve the performance.

ASA1(config)#access-list tcp_bypass extended permit tcp 10.1.1.0 255.255.255.0
172.16.1.0 255.255.255.0

!--- Configure the class map and specify the match parameter for the
!--- class map to match the interesting traffic.

ASA1(config)#class-map tcp_bypass
ASA1(config-cmap)#description "TCP traffic that bypasses stateful firewall"
ASA1(config-cmap)#match access-list tcp_bypass

!--- Configure the policy map and specify the class map
!--- inside this policy map for the class map.

ASA1(config-cmap)#policy-map tcp_bypass_policy
ASA1(config-pmap)#class tcp_bypass

!--- Use the set connection advanced-options tcp-state-bypass
!--- command in order to enable TCP state bypass feature.

ASA1(config-pmap-c)#set connection advanced-options tcp-state-bypass

!--- Use the service-policy policymap_name [ global | interface intf ]
!--- command in global configuration mode in order to activate a policy map
!--- globally on all interfaces or on a targeted interface.

ASA1(config-pmap-c)#service-policy tcp_bypass_policy outside

!--- NAT configuration

ASA1(config)#object network obj-10.1.1.0
ASA1(config-network-object)#subnet 10.1.1.0 255.255.255.0
ASA1(config-network-object)#nat(inside,outside) static 192.168.1.0
```

以下是ASA2上TCP状态旁路功能的*配置示例*:

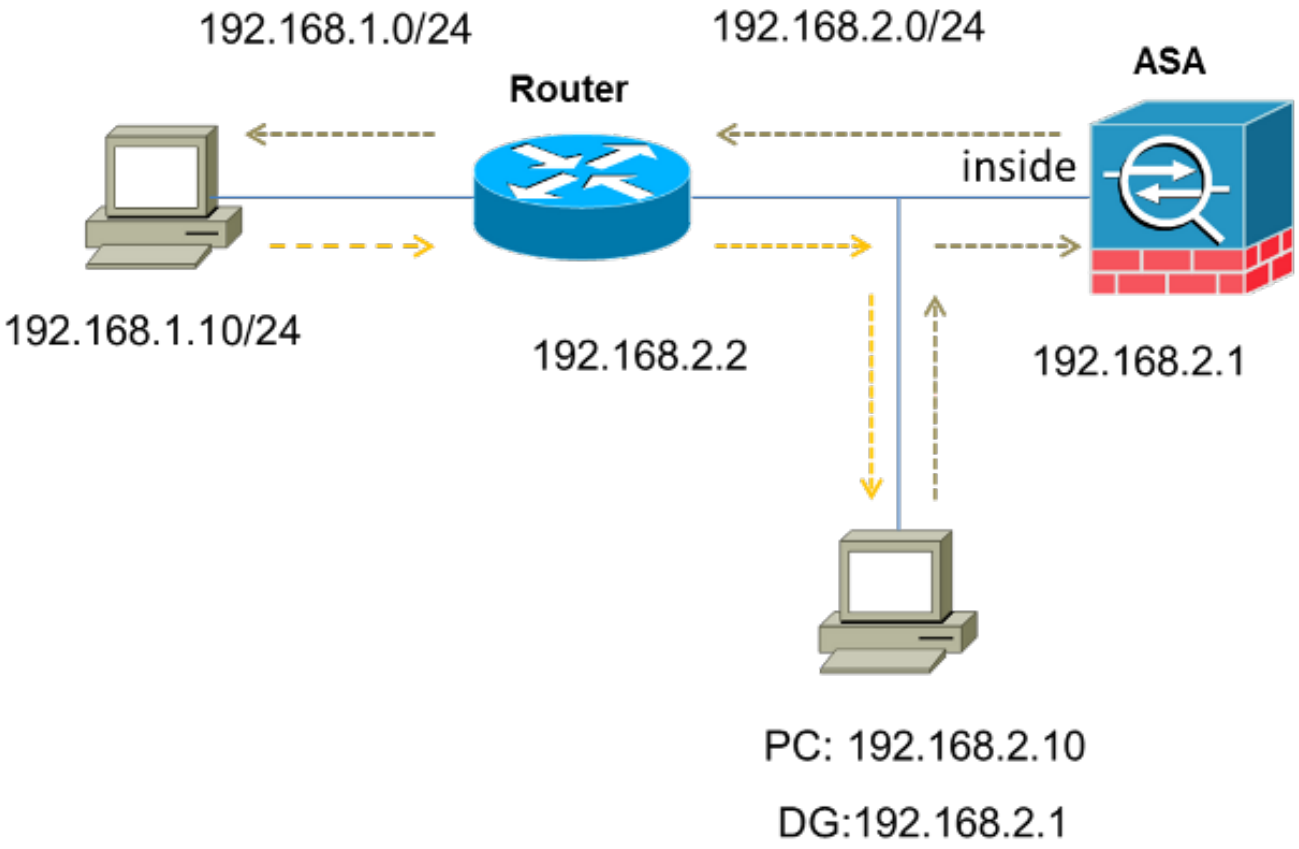
```
!--- Configure the access list to specify the TCP traffic
!--- that needs to by-pass inspection to improve the performance.

ASA2(config)#access-list tcp_bypass extended permit tcp 172.16.1.0 255.255.255.0
10.1.1.0 255.255.255.0

!--- Configure the class map and specify the match parameter for the
!--- class map to match the interesting traffic.
```

```
ASA2(config)#class-map tcp_bypass
ASA2(config-cmap)#description "TCP traffic that bypasses stateful firewall"
ASA2(config-cmap)#match access-list tcp_bypass

!--- Configure the policy map and specify the class map
!--- inside this policy map for the class map.

ASA2(config-cmap)#policy-map tcp_bypass_policy
ASA2(config-pmap)#class tcp_bypass

!--- Use the set connection advanced-options tcp-state-bypass
!--- command in order to enable TCP state bypass feature.

ASA2(config-pmap-c)#set connection advanced-options tcp-state-bypass

!--- Use the service-policy policymap_name [ global | interface intf ]
!--- command in global configuration mode in order to activate a policy map
!--- globally on all interfaces or on a targeted interface.

ASA2(config-pmap-c)#service-policy tcp_bypass_policy outside

!--- NAT configuration

ASA2(config)#object network obj-10.1.1.0
ASA2(config-network-object)#subnet 10.1.1.0 255.255.255.0
ASA1(config-network-object)#nat(inside,outside) static 192.168.1.0
```

场景 2

本节介绍如何在ASA上为使用非对称路由的场景配置TCP状态绕行功能，在这种情况下，流量会从同一接口(u-*turning*)进入和离开ASA。

以下是本场景中使用的拓扑：



要配置TCP状态旁路功能，请完成以下步骤：

1. 创建*access-list*以匹配应绕过TCP检测的流量：

```
ASA(config)#access-list tcp_bypass extended permit tcp 192.168.2.0 255.255.255.0
192.168.1.0 255.255.255.0
```

2. 输入class-map class_map_name命令以创建类*映射*。类映射用于标识要禁用状态防火墙检测的流量。**注意**：本示例中使用的类映射是**tcp_bypass**。

```
ASA(config)#class-map tcp_bypass
```

3. 输入match parameter命令以指定类映射中关注的流量。使用模块化策略框架时，请在*类映射配置模式*下使用**match access-list** 命令，以便使用访问列表识别要应用操作的流量。以下是此配置的示例：

```
ASA(config)#class-map tcp_bypass
ASA(config-cmap)#match access-list tcp_bypass
```

注意：**tcp_bypass**是本示例中使用的访问列表的名称。有关如何指定所关注流量的详*细信息，请参阅Cisco ASA 5500系列配置指南8.2的识别流量（第3/4层类映射）部分。*

4. 输入policy-map name命令以添加策略映射或编辑策略映射（已存在），该策略映射设置对指定类映射流量执行的操作。在使用模块化策略框架时，请在全局配置模式下使用policy-map命令(不带*type*关键字)，以便将操作分配给您使用第3/4层类映射标识的流量(类映射或*类映射类型管理命令)*。 在本示例中，策略映射为**tcp_bypass_policy**:

```
ASA(config-cmap)#policy-map tcp_bypass_policy
```

5. 在*policy-map configuration* 模式下输入class命令，以便将已创建的类映射(*tcp_bypass*)分配到策略映射(*tcp_bypass_policy*)，以便可以为类映射流量分配操作。在本例中，类映射为**tcp_bypass**:

```
ASA(config-cmap)#policy-map tcp_bypass_policy
```

```
ASA(config-pmap)#class tcp_bypass
```

6. 在类配置模式下输入set connection advanced-options tcp-state-bypass命令以*启用TCP状态绕行功能*。此命令在8.2(1)版中引入。 可从*策略映*射配置模式*访问类配*置模式，如以下示例所示：

```
ASA(config-cmap)#policy-map tcp_bypass_policy
ASA(config-pmap)#class tcp_bypass
ASA(config-pmap-c)#set connection advanced-options tcp-state-bypass
```

7. 输入service-policy policymap_name [global | interface *intf*]命令，以便在所有接口或目标接口上全局激活策略映射。要禁用服务策略，请使用此**命令**的no形式。输入**service-policy**命令以在接口上启用一组策略。**global**关键字将策略映射应用于所有接口，而**interface**关键字将策略仅应用于一个接口。仅允许有一个全局策略。要覆盖接口上的全局策略，可以将服务策略应用到该接口。您只能将一个策略映射应用到每个接口。示例如下：

```
ASA(config-pmap-c)#service-policy tcp_bypass_policy inside
```

8. 允许ASA上流量的相同安全级别：

```
ASA(config)#same-security-traffic permit intra-interface
```

以下是ASA上TCP状态绕行功能的示例配置：

```
!--- Configure the access list to specify the TCP traffic
!--- that needs to bypass inspection to improve the performance.

ASA(config)#access-list tcp_bypass extended permit tcp 192.168.2.0 255.255.255.0
192.168.1.0 255.255.255.0

!--- Configure the class map and specify the match parameter for the
!--- class map to match the interesting traffic.

ASA(config)#class-map tcp_bypass
ASA(config-cmap)#description "TCP traffic that bypasses stateful firewall"
ASA(config-cmap)#match access-list tcp_bypass

!--- Configure the policy map and specify the class map
!--- inside this policy map for the class map.

ASA(config-cmap)#policy-map tcp_bypass_policy
ASA(config-pmap)#class tcp_bypass

!--- Use the set connection advanced-options tcp-state-bypass
!--- command in order to enable TCP state bypass feature.

ASA(config-pmap-c)#set connection advanced-options tcp-state-bypass

!--- Use the service-policy policymap_name [ global | interface intf ]
!--- command in global configuration mode in order to activate a policy map
!--- globally on all interfaces or on a targeted interface.

ASA(config-pmap-c)#service-policy tcp_bypass_policy inside

!--- Permit same security level traffic on the ASA to support U-turning

ASA(config)#same-security-traffic permit intra-interface
```

验证

输入 show conn 命令，以查看活动TCP和UDP连接的数量以及各种类型连接的相关信息。要显示指定连接类型的连接状态，请输入 show conn 命令*的IPv6*模式。

> **注意**：此命令支持 IPv4 和 IPv6 地址。为使用TCP状态旁路功能的连接显示的输出包括标**志 b**。

下面是示例输出：

```
ASA(config)show conn
1 in use, 3 most used
TCP tcp 10.1.1.1:49525 tcp 172.16.1.1:21, idle 0:01:10, bytes 230, flags b
```

故障排除

此功能没有特定的故障排除信息。有关一般连接故障排除信息，请参阅以下文档：

- 通过 CLI 和 ASDM 配置实现 ASA 数据包捕获示例
- ASA 8.2：通过Cisco ASA防火墙的数据包流

> **注意**：TCP状态旁路连接不会复制到故障转移对中的备用设备。

错误消息

ASA在启用TCP状态绕行功能后显示以下错误消息：

```
%PIX|ASA-4-313004:Denied ICMP type=icmp_type, from source_address oninterface
interface_name to dest_address:no matching session
```

由于状态ICMP功能添加的安全检查，ASA会丢弃Internet控制消息协议(ICMP)数据包。这些通常是ICMP回*应*应答，没有在ASA上已传递的有效*回应请求*，或ICMP错误消息，与ASA中当前建立的任何TCP、UDP或ICMP会话无关。

ASA显示此日志，即使TCP状态绕行功能已启用，因为无法禁用此功能(即，检查连接表中第3类的ICMP返*回*条目)。但是，TCP状态旁路功能工作正常。

输入此命令以防止出现以下消息：

```
hostname(config)#no logging message 313004
```

相关信息

- Cisco 自适应安全设备管理器
- Cisco ASA 5500 系列自适应安全设备

- 请求注解 (RFC)
- 技术支持和文档 - Cisco Systems