在ASA 5500系列上配置TCP狀態旁路功能

目錄

[簡介](#)
[必要條件](#)
[需求](#)
[採用元件](#)
[慣例](#)
[背景資訊](#)
[TCP狀態略過功能概述](#)
[支援資訊](#)
[設定](#)
[案例 1](#)
[案例 2](#)
[驗證](#)
[疑難排解](#)
[錯誤消息](#)
[相關資訊](#)

簡介

本檔案介紹如何設定TCP狀態略過功能，此功能允許傳出和傳入流量通過單獨的Cisco ASA 5500系列調適型安全裝置(ASA)。

必要條件

需求

Cisco ASA必須至少安裝基本許可證，然後才能繼續本文檔中所述的配置。

採用元件

本文檔中的資訊基於運行軟體版本9.x的Cisco ASA 5500系列。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

背景資訊

本節概述TCP狀態略過功能和相關支援資訊。

TCP狀態略過功能概述

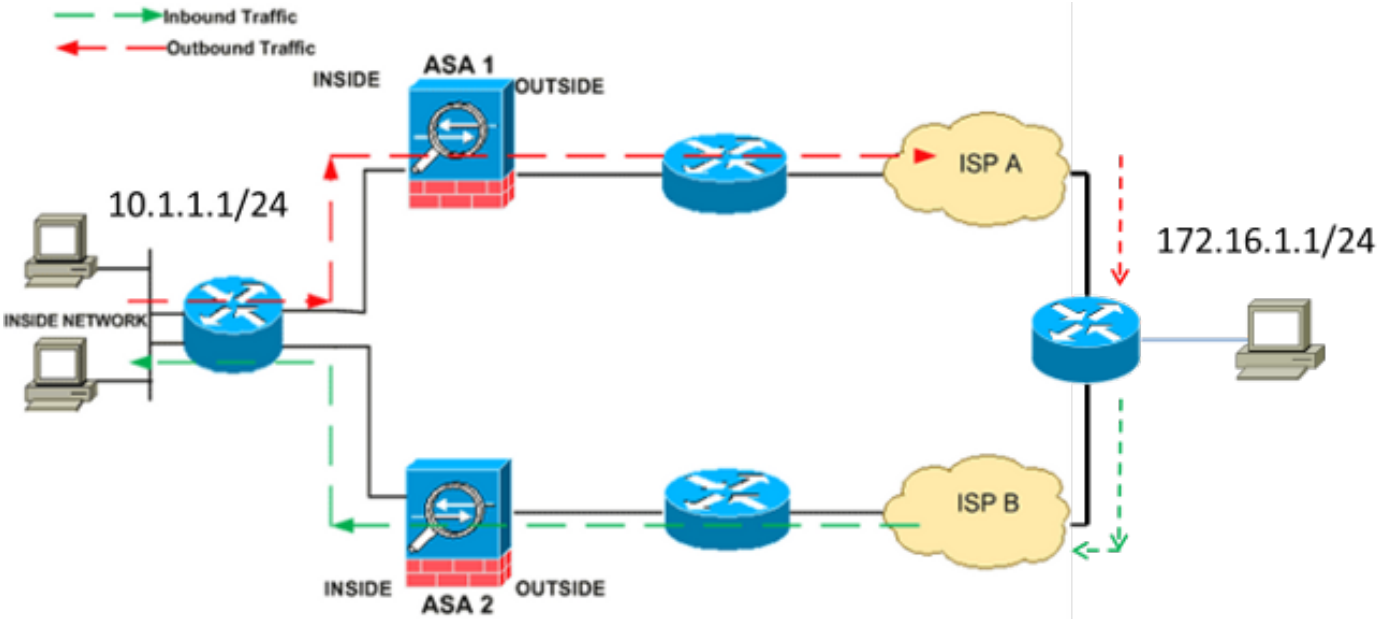
預設情況下，所有通過ASA的流量都會通過自適應安全演算法進行檢查，並根據安全策略允許通過或丟棄。為了最大限度地提高防火牆效能，ASA會檢查每個資料包的狀態（例如，它檢查它是新連線還是已建立的連線），並將其分配給會話管理路徑(新的連線同步(SYN)資料包)、快速路徑（已建立的連線）或控制平面路徑（高級檢查）。

與快速路徑中的當前連線匹配的TCP資料包可以通過ASA，而無需重新檢查安全策略的各個方面。此功能可最大限度地提高效能。然而，用於在快速路徑中建立作業階段的方法（使用SYN封包）和在快速路徑中進行的檢查（例如TCP序號）可以阻止非對稱路由解決方案；連線的出站和入站流都必須通過同一個ASA。

例如，新連線進入*ASA 1*。SYN資料包通過會話管理路徑，並且連線條目新增到快速路徑表中。如果此連線上的後續資料包通過*ASA 1*，則這些資料包與快速路徑中的條目匹配，並且被通過。如果後續資料包進入*ASA 2*，其中沒有經過會話管理路徑的SYN資料包，則快速路徑中沒有用於連線的條目，資料包將被丟棄。

如果在上游路由器上配置了非對稱路由，且流量在兩個ASA之間交替，則可以為特定流量配置TCP狀態旁路功能。TCP狀態略過功能會變更在快速路徑中建立作業階段的方式，並停用快速路徑檢查。此功能處理TCP流量的方式與處理UDP連線的方式相同：當與指定網路匹配的非SYN資料包進入ASA且沒有快速路徑條目時，該資料包將通過會話管理路徑以在快速路徑中建立連線。進入快速路徑後，流量會繞過快速路徑檢查。

此圖提供非對稱路由的示例，其中出站流量通過與入站流量不同的ASA:



附註：Cisco ASA 5500系列預設禁用TCP狀態旁路功能。此外，如果未正確實施TCP狀態旁路配置，可能會導致大量連線。

支援資訊

本節介紹TCP狀態略過功能的支援資訊。

- **Context Mode** â âAâTCP狀態略過功能在單情景和多情景模式下受支援。
- **防火牆模**â式â TCPâ狀態略過功能在路由和透明模式下支援。
- **故障切**â換ââ TCP狀態旁路功能支援故障切換。

使用TCP狀態略過功能時，不支援以下功能：

- **應用檢**â測âApplicationâ 檢測要求入站和出站流量都通過同一個ASA，因此TCP狀態旁路功能不支援應用檢測。
- **身份驗證、授權和記帳(AAA)已驗證的會話**âAuthentication， Authorization， and Accounting(AAA)Authenticated sessionsâA â **當使用者使用一個ASA進行身份驗證時，由於使用者未使用該ASA進行身份驗證，因此通過另一個ASA返回的流量被拒絕。**
- **TCP攔截、最大初始連線限制、TCP序列號**â隨ââASA不跟蹤連線狀態，因此這些功能未應用。
- **TCP規範化**ââ âTCP規范化器已禁用。
- **安全服務模組(SSM)和安全服務卡(SSC)功能**âââ不能在SSM或SSC上執行的任何應用程式(例如IPS或內容安全(CSC))上使用TCP狀態略過功能。

  附註：由於轉換會話是單獨為每個ASA建立的，因此請確保在兩個ASA上為TCP狀態繞過流量配置靜態網路地址轉換(NAT)。如果使用動態NAT，為*ASA 1*上的會話選擇的地址將與*ASA 2上的會話選擇的地址不*同。

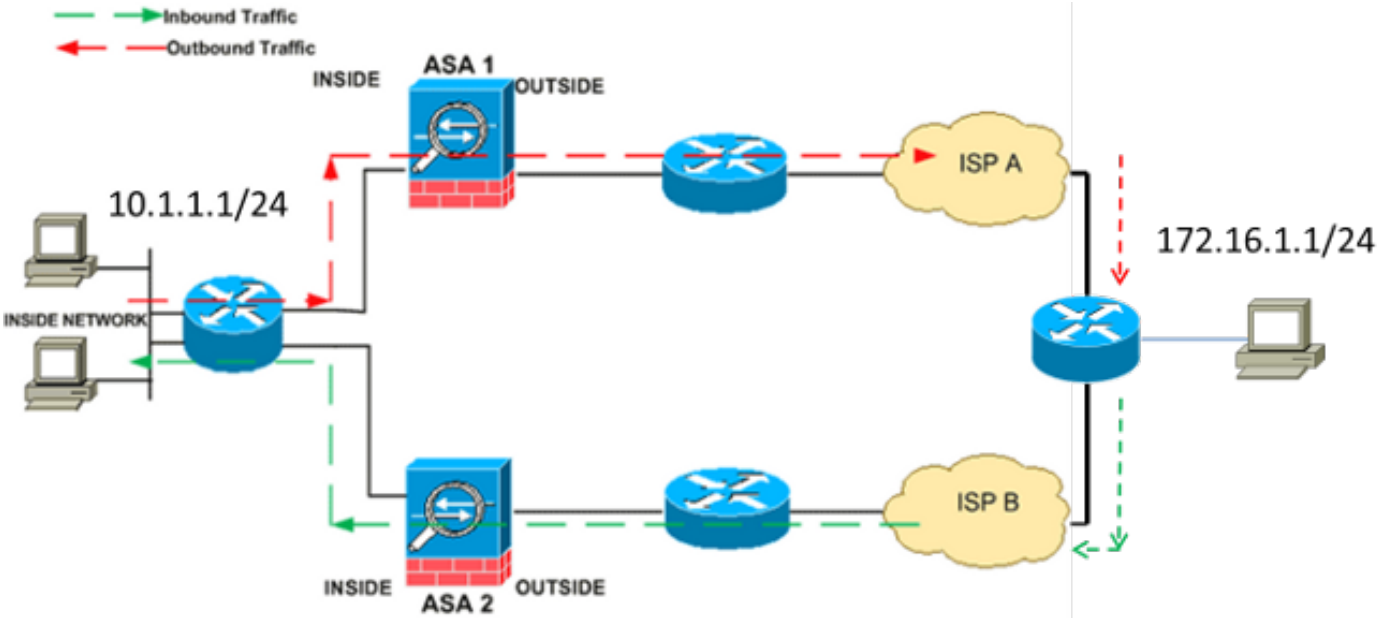
設定

本節介紹如何在兩種不同情況下在ASA 5500系列上配置TCP狀態旁路功能。

附註：使用命令查詢工具(僅供註冊客戶使用)可獲取本節中使用的命令的更多資訊。

案例 1

這是用於第一個場景的拓撲：



附註：您必須將本節所述的配置應用到兩個ASA。

完成以下步驟即可設定TCP狀態略過功能：

1. 輸入class-map class_map_name命令以建立類*對映*。類對映用於標識要為其禁用狀態防火牆檢測的流量。**附註**：本示例中使用的類對映是**tcp_bypass**。
   ```
   ASA(config)#class-map tcp_bypass
   ```
2. 輸入match parameter命令以指定類對映中的相關流量。使用模組化策略框架時，請在*class-map配置*模式下使用**match access-list**命令，以便使用訪問清單來標識要對其應用操作的流量。以下是此組態的範例：

   ```
   ASA(config)#class-map tcp_bypass
   ASA(config-cmap)#match access-list tcp_bypass
   ```
   附註：**tcp_bypass**是本範例中使用的存取清單的名稱。有關如何指定相關流量的詳細資訊，請參閱*使用CLI 8.2的Cisco ASA 5500系列配置指南*的識別流量（第3/4層類對映）部分。
3. 輸入policy-map name命令以新增策略對映或編輯策略對映（已經存在），該策略對映分配針對指定類對映流量要採取的操作。使用模組化策略框架時，請在*全域性配置*模式下使用policy-map命令(不帶*type*關鍵字)將操作分配給使用第3/4層類對映標識的流量(class-map或**class-map type management**命令)。 在本示例中，策略對映為**tcp_bypass_policy**:

   ```
   ASA(config-cmap)#policy-map tcp_bypass_policy
   ```
4. 在*policy-map configuration*模式下輸入class命令，以將建立的類對映(*tcp_bypass*)分配到策略對映(*tcp_bypass_policy*)，以便可以將操作分配到類對映流量。在本示例中，類對映是**tcp_bypass**:

   ```
   ASA(config-cmap)#policy-map tcp_bypass_policy
   ASA(config-pmap)#class tcp_bypass
   ```
5. 在*class configuration*模式下輸入set connection advanced-options tcp-state-bypass命令以啟用TCP狀態略過功能。此命令在8.2(1)版中匯入。 通過*policy-map*配置模式可以訪問類配置模式，如下例所示：

   ```
   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. 輸入service-policy policymap_name [global | interface *intf*]命令*在*全局配置模式下，以便在所有介面或目標介面上全域性啟用策略對映。若要停用服務原則，請使用此命令的no形式。輸入service-policy命令以在介面上啟用一組策略。global關鍵字將策略對映應用於所有介面，而interface關鍵字將策略對映僅應用於一個介面。只允許一個全域性策略。要覆蓋介面上的全域性策略，可以將服務策略應用於該介面。您只能對每個介面應用一個策略對映。以下是範例：

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

*ASA*1上的TCP狀態旁路功能配置示*例如下*:

```
!--- 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
```

*ASA*2上的TCP狀態旁路功能配置示*例如下*:

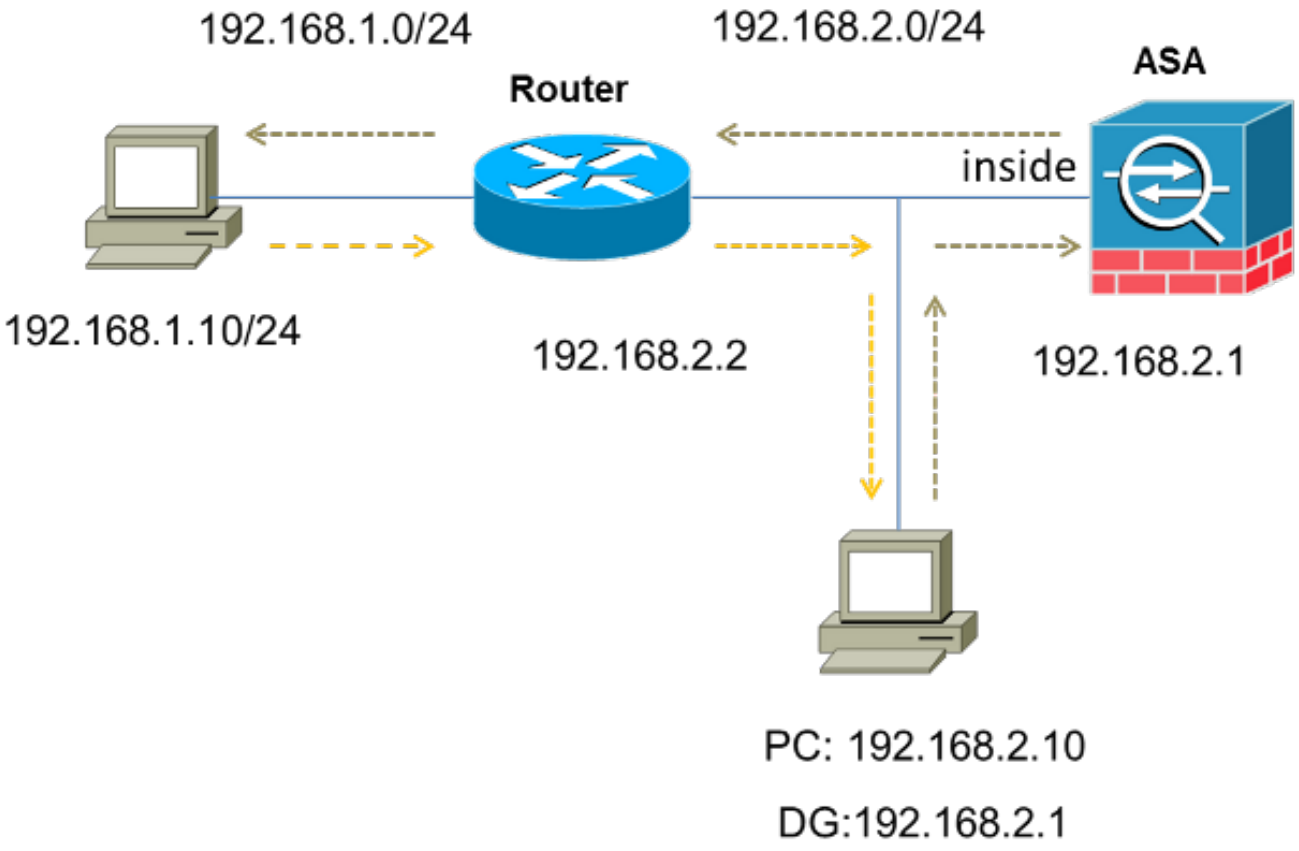
```
!--- Configure the access list to specify the TCP traffic
!--- that needs to by-pass inspection to improve the performance.

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
```

案例 2

本節介紹如何在ASA上為使用非對稱路由的方案(流量從同一介面進入或離開ASA(*u-turning*))*配置TCP狀態旁路功*能。

以下是此案例中使用的拓撲：



完成以下步驟即可設定TCP狀態略過功能：

1. 建立*access-list*以與應繞過TCP檢查的流量相符：

```
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. 輸入class-map class_map_name命令以建立類*對映*。類對映用於標識要為其禁用狀態防火牆檢測的流量。**附註**：本示例中使用的類對映是**tcp_bypass**。

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

3. 輸入match parameter命令以指定類對映中的相關流量。使用模組化策略框架時，請在*class-map配置*模式下使用**match access-list**命令，以便使用訪問清單來標識要對其應用操作的流量。以下是此組態的範例：

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

附註：**tcp_bypass**是本範例中使用的存取清單的名稱。有關如何指定相關流量的詳細資訊，請參閱*使用CLI 8.2的Cisco ASA 5500系列配置指南*的識別流量（第3/4層類對映）部分。

4. 輸入policy-map name命令以新增策略對映或編輯策略對映（已經存在），策略對映設定針對指定類對映流量要執行的操作。使用模組化策略框架時，請在*全域性配置*模式下使用policy-map命令(不帶*type*關鍵字)將操作分配給使用第3/4層類對映標識的流量(class-map或**class-map type management**命令)。 在本示例中，策略對映為**tcp_bypass_policy**:

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

5. 在*policy-map configuration*模式下輸入class命令，以將建立的類對映(*tcp_bypass*)分配到策略對映(*tcp_bypass_policy*)，以便可以為類對映流量分配操作。在本示例中，類對映為**tcp_bypass**:

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

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

6. 在*class configuration*模式下輸入**set connection advanced-options tcp-state-bypass**命令以啟用TCP狀態略過功能。此命令在8.2(1)版中匯入。 可以從*policy-map configuration*模式訪問*類配置模式，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. 輸入**service-policy policymap_name [global | interface *intf*]**命令*在*全域性配置模式下，以便在所有介面或目標介面上全域性啟用策略對映。若要停用服務原則，請使用此命令的**no**形式。輸入**service-policy**命令以在介面上啟用一組策略。**global**關鍵字將策略對映應用於所有介面，而**interface**關鍵字僅將策略應用於一個介面。只允許一個全域性策略。要覆蓋介面上的全域性策略，可以將服務策略應用於該介面。您只能對每個介面應用一個策略對映。以下是範例：

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

8. 允許ASA上的流量具有相同的安全級別：

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

以下是ASA上TCP狀態旁路功能的配置示例：

```
!--- 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
```

驗證

輸入 show conn 命令可檢視活動TCP和UDP連線的數量和有關各種連線型別的資訊。要顯示指定連線型別的連線狀態，請輸入 show conn 命令*的EXEC*模式。

附註：此命令支援IPv4和IPv6地址。為使用TCP狀態旁路功能的連線顯示的輸出包括標誌**b**。

以下是輸出範例：

```
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
```

疑難排解

此功能沒有特定的故障排除資訊。有關一般連線疑難排解資訊，請參閱以下文檔：

- 使用CLI和ASDM的ASA資料包捕獲配置示例
- ASA 8.2:通過Cisco ASA防火牆的資料包流

附註：TCP狀態旁路連線不會複製到故障轉移對中的備用裝置。

錯誤消息

即使啟用TCP狀態旁路功能，ASA仍會顯示以下錯誤消息：

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

由於有狀態ICMP功能新增了安全檢查，ASA丟棄了網際網路控制消息協定(ICMP)資料包。這些錯誤消息通常是沒有通過ASA的有效回應請求的ICMP *echo*應答，或者是與ASA中當前建立的任何TCP、UDP或ICMP會話無關的ICMP錯誤消息。

即使由於無法禁用此功能(即檢查連線表中型別3的ICMP *return*條目)而啟用了TCP狀態旁路功能，ASA也會顯示此日誌。但是，TCP狀態略過功能可以正常工作。

輸入以下命令可防止出現以下訊息：

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

相關資訊

- 思科調適型資安裝置管理員
- Cisco ASA 5500系列調適型安全裝置
- 要求建議 (RFC)

- 技術支援與文件 - Cisco Systems