Configure o recurso de desvio de estado TCP no ASA 5500 Series

Contents

Introduction

Este documento descreve como configurar o recurso de desvio de estado TCP, que permite que o tráfego de saída e de entrada flua por meio de dispositivos de segurança adaptáveis (ASAs) Cisco ASA 5500 Series separados.

Prerequisites

Requirements

O Cisco ASA deve ter pelo menos a licença básica instalada antes que você possa prosseguir com a configuração descrita neste documento.

Componentes Utilizados

As informações neste documento são baseadas no Cisco ASA 5500 Series que executa o software versão 9.x.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

Esta seção fornece uma visão geral do recurso de desvio de estado TCP e as informações de suporte relacionadas.

Visão geral do recurso de desvio de estado TCP

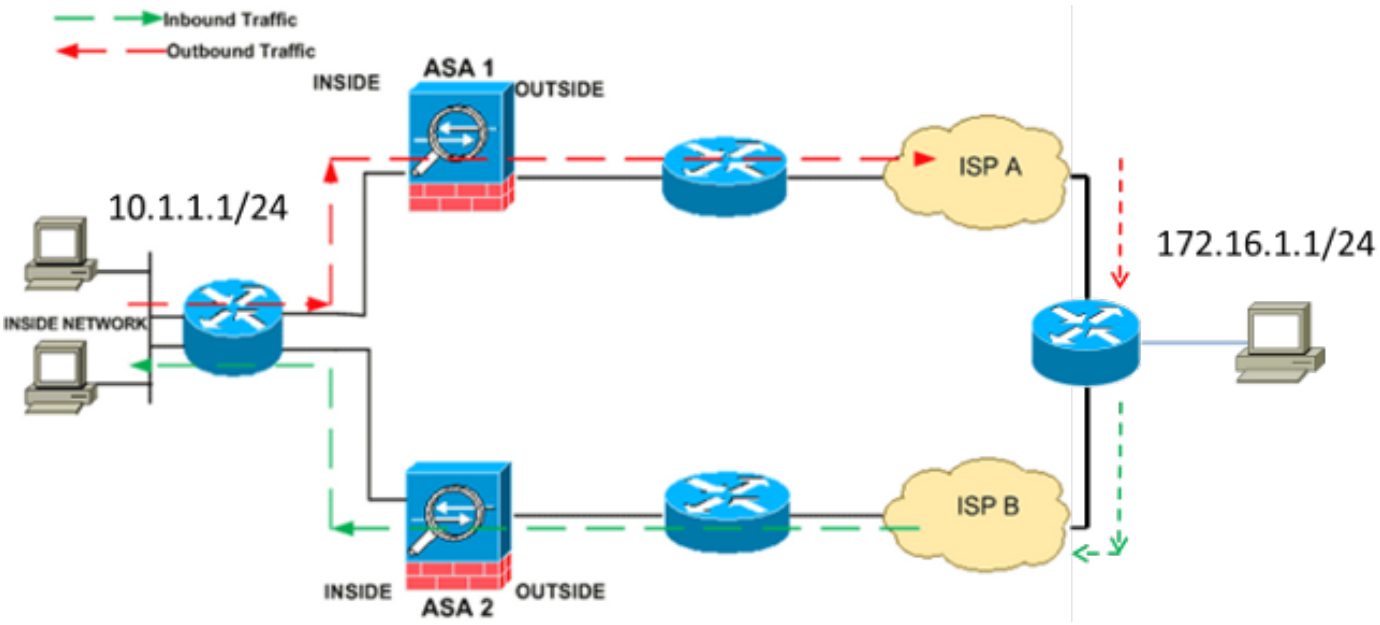
Por padrão, todo o tráfego que passa pelo ASA é inspecionado por meio do algoritmo de segurança adaptável e é permitido atravessar ou ser descartado com base na política de segurança. Para maximizar o desempenho do Firewall, o ASA verifica o estado de cada pacote (por exemplo, verifica se é uma nova conexão ou uma conexão estabelecida) e o atribui ao caminho de gerenciamento da sessão (um novo pacote de sincronização de conexão (SYN)), ao caminho rápido (uma conexão estabelecida) ou ao caminho do plano de controle (inspeção avançada).

Os pacotes TCP que correspondem às conexões atuais no caminho rápido podem passar pelo ASA sem uma reverificação de cada aspecto da política de segurança. Este recurso maximiza o desempenho. No entanto, o método usado para estabelecer a sessão no caminho rápido (que usa o pacote SYN) e as verificações que ocorrem no caminho rápido (como o número de sequência TCP) podem atrapalhar as soluções de roteamento assimétrico; os fluxos de saída e de entrada de uma conexão devem passar pelo mesmo ASA.

Por exemplo, uma nova conexão vai para o *ASA 1*. O pacote SYN passa pelo caminho de gerenciamento da sessão e uma entrada para a conexão é adicionada à tabela de caminho rápido. Se os pacotes subsequentes nesta conexão passarem pelo *ASA 1*, os pacotes corresponderão à entrada no caminho rápido e serão passados. Se os pacotes subsequentes forem para o *ASA 2*, onde não havia um pacote SYN que passasse pelo caminho de gerenciamento da sessão, então não há entrada no caminho rápido para a conexão e os pacotes serão descartados.

Se você tiver o roteamento assimétrico configurado nos roteadores upstream e o tráfego alternar entre dois ASAs, você poderá configurar o recurso de desvio de estado TCP para tráfego específico. O recurso de desvio de estado do TCP altera a forma como as sessões são estabelecidas no caminho rápido e desabilita as verificações de caminho rápido. Este recurso trata o tráfego TCP da mesma forma que trata uma conexão UDP: quando um pacote não-SYN que corresponde às redes especificadas entra no ASA e não há entrada de caminho rápido, o pacote passa pelo caminho de gerenciamento da sessão para estabelecer a conexão no caminho rápido. Uma vez no caminho rápido, o tráfego ignora as verificações de caminho rápido.

Essa imagem fornece um exemplo de roteamento assimétrico, em que o tráfego de saída passa por um ASA diferente do tráfego de entrada:



Note: O recurso de desvio de estado TCP é desativado por padrão no Cisco ASA 5500 Series. Além disso, a configuração de desvio de estado do TCP pode causar um alto número de conexões se não for implementada corretamente.

Informações de suporte

Esta seção descreve as informações de suporte para o recurso de desvio de estado TCP.

- **Modo de contexto** â Â A característica de desvio de estado TCP é suportada em modos de contexto único e múltiplo.
- **Modo de firewall** â Â O recurso de desvio de estado TCP é suportado em modos roteados e transparentes.
- **Failover** â Â O recurso de desvio de estado TCP suporta failover.

Esses recursos não são suportados quando você usa o recurso de desvio de estado TCP:

- **A inspeção de aplicativos** â Â inspeção de aplicativos exige que o tráfego de entrada e saída passe pelo mesmo ASA, portanto, a inspeção de aplicativos não é suportada com o recurso de desvio de estado do TCP.
- **Sessões autenticadas de Autenticação, Autorização e Auditoria (AAA)** Â Quando um usuário se autentica com um ASA, o tráfego que retorna através do outro ASA é negado porque o usuário não se autentica com esse ASA.
- **Interceptação de TCP, limite máximo de conexão embrionária, randomização do número de sequência TCP** â Â O ASA não rastreia o estado da conexão, portanto esses recursos não são aplicados.

- **Normalização do TCP** â Â O normalizador TCP está desativado.
- **Funcionalidade de Módulo de Serviços de Segurança (SSM) e Placa de Serviços de Segurança (SSC)** â Â Você não pode usar o recurso de desvio de estado TCP com nenhum aplicativo executado em um SSM ou SSC, como IPS ou Segurança de Conteúdo (CSC).

Note: Como a sessão de conversão é estabelecida separadamente para cada ASA, certifique-se de configurar a NAT (Network Address Translation, tradução estática de endereço de rede) em ambos os ASAs para o tráfego de desvio de estado do TCP. Se você usar NAT dinâmico, o endereço escolhido para a sessão no *ASA 1* será diferente do endereço escolhido para a sessão no *ASA 2*.

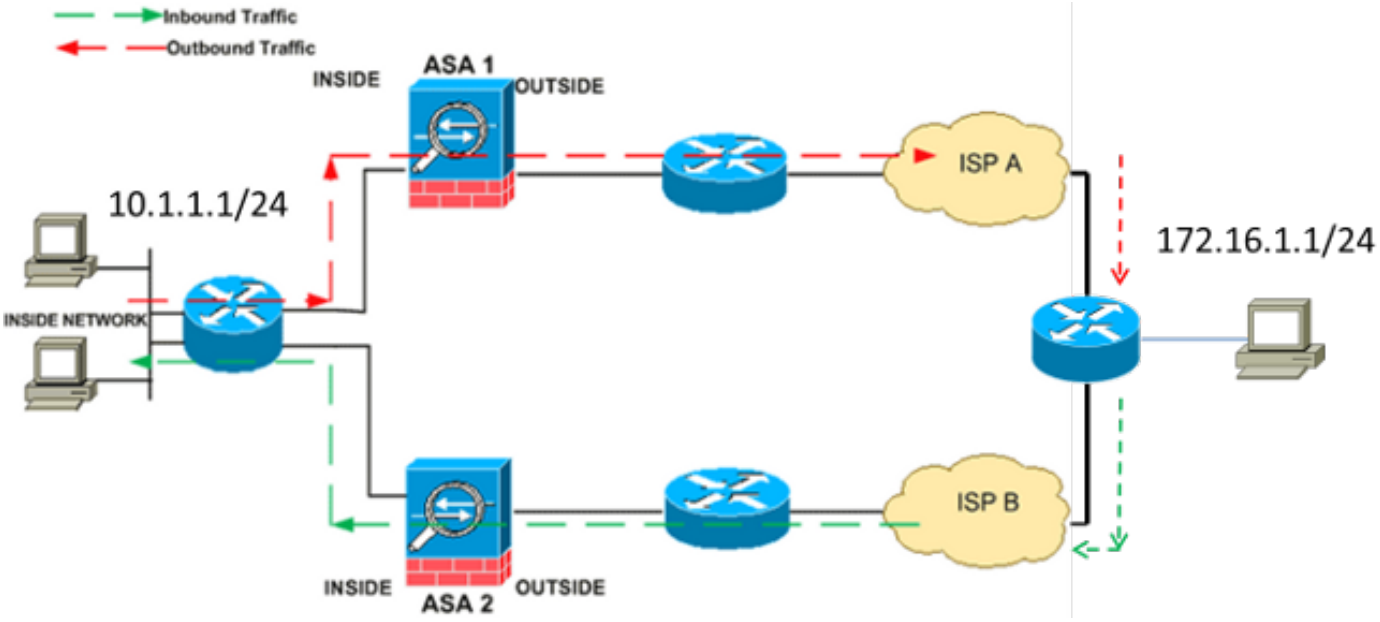
Configurar

Esta seção descreve como configurar o recurso de desvio de estado TCP no ASA 5500 Series em dois cenários diferentes.

Note: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Cenário 1

Esta é a topologia usada para o primeiro cenário:



Note: Você deve aplicar a configuração descrita nesta seção a ambos os ASAs.

Conclua estes passos para configurar o recurso de desvio de estado TCP:

1. Insira o comando class-map class_map_name para criar um *mapa de classes*. O mapa de

classes é usado para identificar o tráfego para o qual você deseja desativar a inspeção de firewall stateful.**Note**: O mapa de classes usado neste exemplo é **tcp_bypass**.

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

2. Insira o comando match parameter para especificar o tráfego de interesse no mapa de classes. Ao usar a Estrutura de política modular, use o comando **match access-list** no modo de *configuração class-map* para usar uma lista de acesso para identificar o tráfego ao qual deseja aplicar as ações. Aqui está um exemplo desta configuração:

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

Note: O **tcp_bypass** é o nome da lista de acesso usada neste exemplo. Consulte a seção Identificação de Tráfego (Mapa de Classe da Camada 3/4) do *Guia de Configuração do Cisco ASA 5500 Series usando CLI, 8.2* para obter mais informações sobre como especificar o tráfego de interesse.

3. Insira o comando policy-map name para adicionar um mapa de política ou editar um mapa de política (que já esteja presente) que atribua as ações a serem tomadas em relação ao tráfego de mapa de classe especificado. Quando você usa a Estrutura de Política Modular, use o comando policy-map (sem a palavra-chave *type*) no modo de *configuração global* para atribuir ações ao tráfego identificado com um mapa de classe de Camada 3/4 (o **comando class-map** ou **class-map type management**). Neste exemplo, o mapa de política é **tcp_bypass_policy**:

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

4. Insira o comando class no modo *de configuração do mapa de políticas* para atribuir o mapa de classes criado (*tcp_bypass*) ao mapa de políticas (*tcp_bypass_policy*) para que você possa atribuir as ações ao tráfego do mapa de classes. Neste exemplo, o mapa de classes é **tcp_bypass**:

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

5. Insira o comando set connection advanced-options tcp-state-bypass no modo de *configuração de classe* para habilitar o recurso TCP state bypass. Esse comando foi introduzido na versão 8.2(1). O modo de *configuração de classe* pode ser acessado no modo *de configuração de mapa de política*, como mostrado neste exemplo:

```
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. Digite o service-policy policymap_name [global comando | interface *intf*] no *modo de configuração global* para ativar um mapa de políticas globalmente em todas as interfaces ou em uma interface de destino. Para desabilitar a política de serviço, use a forma **no** desse comando. Insira o comando **service-policy** para ativar um conjunto de políticas em uma interface. A palavra-chave **global** aplica o mapa de políticas a todas as interfaces, e a palavra-chave **interface** aplica o mapa de políticas a apenas uma interface. Apenas uma política global é permitida. Para substituir a política global em uma interface, você pode aplicar uma política de serviço a essa interface. Você pode aplicar apenas um mapa de política a cada interface. Aqui está um exemplo:

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

Aqui está um exemplo de configuração para o recurso de desvio de estado TCP no *ASA1*:

```
!--- 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
```

Aqui está um exemplo de configuração para o recurso de desvio de estado TCP no *ASA2*:

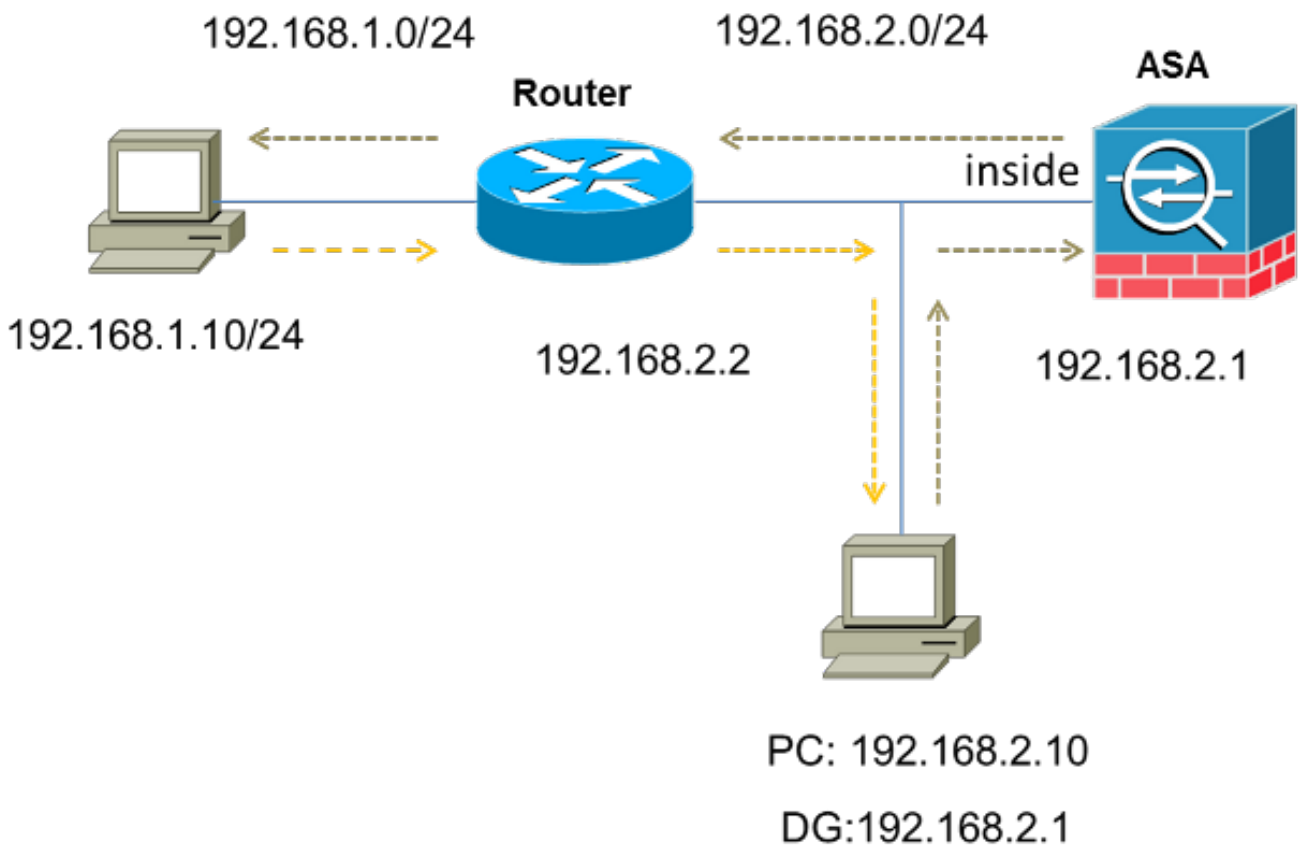
```
!--- Configure the access list to specify the TCP traffic
!--- that needs to by-pass inspection to improve the performance.

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
```

Cenário 2

Esta seção descreve como configurar o recurso de desvio de estado TCP no ASA para cenários que usam roteamento assimétrico, em que o tráfego entra e sai do ASA da mesma interface (*reativação*).

Esta é a topologia usada neste cenário:



Conclua estes passos para configurar o recurso de desvio de estado TCP:

1. Crie uma *lista de acesso* para corresponder ao tráfego que deve ignorar a inspeção TCP:

```
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. Insira o comando class-map class_map_name para criar um *mapa de classes*. O mapa de classes é usado para identificar o tráfego para o qual você deseja desativar a inspeção de firewall stateful.**Note**: O mapa de classes usado neste exemplo é **tcp_bypass**.
```
ASA(config)#class-map tcp_bypass
```
3. Insira o comando match parameter para especificar o tráfego de interesse no mapa de classes. Ao usar a Estrutura de política modular, use o comando **match access-list** no modo de *configuração class-map* para usar uma lista de acesso para identificar o tráfego ao qual deseja aplicar as ações. Aqui está um exemplo desta configuração:

```
ASA(config)#class-map tcp_bypass
ASA(config-cmap)#match access-list tcp_bypass
```
Note: O **tcp_bypass** é o nome da lista de acesso usada neste exemplo. Consulte a seção Identificação de Tráfego (Mapa de Classe da Camada 3/4) do *Guia de Configuração do Cisco ASA 5500 Series usando CLI, 8.2* para obter mais informações sobre como especificar o tráfego de interesse.
4. Insira o comando policy-map name para adicionar um mapa de política ou editar um mapa de política (que já esteja presente) que defina as ações a serem tomadas em relação ao tráfego de mapa de classe especificado. Quando você usa a Estrutura de Política Modular, use o comando policy-map (sem a palavra-chave *type*) no modo de *configuração global* para atribuir as ações ao tráfego identificado com um mapa de classe de Camada 3/4 (o **comando class-map** ou **class-map type management**). Neste exemplo, o mapa de política é **tcp_bypass_policy**:

```
ASA(config-cmap)#policy-map tcp_bypass_policy
```
5. Insira o comando class no modo *de configuração do mapa de políticas* para atribuir o mapa de classes criado (*tcp_bypass*) ao mapa de políticas (*tcp_bypass_policy*) para que você possa atribuir ações ao tráfego do mapa de classes. Neste exemplo, o mapa de classes é **tcp_bypass**:

```
ASA(config-cmap)#policy-map tcp_bypass_policy
ASA(config-pmap)#class tcp_bypass
```
6. Insira o comando set connection advanced-options tcp-state-bypass no modo de *configuração de classe* para habilitar o recurso TCP state bypass. Esse comando foi introduzido na versão 8.2(1). O modo de *configuração de classe* pode ser acessado no modo de *configuração de mapa de política*, como mostrado neste exemplo:

```
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. Digite o service-policy policymap_name [global comando | interface *intf*] no modo *de configuração global* para ativar um mapa de políticas globalmente em todas as interfaces ou em uma interface de destino. Para desabilitar a política de serviço, use a forma **no** desse comando. Insira o comando **service-policy** para ativar um conjunto de políticas em uma interface. A palavra-chave **global** aplica o mapa de políticas a todas as interfaces, e a palavra-chave **interface** aplica a política a apenas uma interface. Apenas uma política global é permitida. Para substituir a política global em uma interface, você pode aplicar uma política de serviço a essa interface. Você pode aplicar apenas um mapa de política a cada interface. Aqui está um exemplo:

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

8. Permita o mesmo nível de segurança para o tráfego no ASA:

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

Aqui está um exemplo de configuração para o recurso de desvio de estado TCP no ASA:

```
!--- 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
```

Verificar

Digite o **show conn** para visualizar o número de conexões TCP e UDP ativas e informações sobre as conexões de vários tipos. Para exibir o estado da conexão para o tipo de conexão designado, insira o comando **show conn** no modo *EXEC privilegiado*.

> **Note**: Esse comando oferece suporte aos endereços IPv4 e IPv6. A saída exibida para as conexões que usam o recurso de desvio de estado TCP inclui o flag **b**.

Aqui está um exemplo de saída:

```
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
```

Troubleshoot

Não há informações específicas de solução de problemas para este recurso. Consulte estes documentos para obter informações gerais sobre solução de problemas de conectividade:

- Exemplo de captura de pacote ASA com CLI e configuração ASDM
- ASA 8.2: Fluxo de pacotes pelo firewall Cisco ASA

  Note: As conexões de desvio de estado TCP não são replicadas para a unidade de standby em um par de failover.

Mensagens de erro

O ASA exibe esta mensagem de erro mesmo depois que o recurso de desvio de estado do TCP está ativado:

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

Os pacotes ICMP (Internet Control Message Protocol) são descartados pelo ASA devido às verificações de segurança adicionadas pelo recurso ICMP stateful. Geralmente, essas são respostas de *eco* ICMP sem uma *solicitação de eco* válida já passada pelo ASA ou mensagens de erro ICMP que não estão relacionadas a nenhuma sessão TCP, UDP ou ICMP estabelecida atualmente no ASA.

O ASA exibe esse log mesmo se o recurso de desvio de estado do TCP estiver habilitado porque a desativação dessa funcionalidade (ou seja, verificações das entradas de *retorno* do ICMP para o Tipo 3 na tabela de conexão) não é possível. No entanto, o recurso de desvio de estado do TCP funciona corretamente.

Insira este comando para evitar a aparência destas mensagens:

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

Informações Relacionadas

- Cisco Adaptive Security Device Manager
- Dispositivos de segurança adaptáveis Cisco ASA 5500 Series
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems