Configurar a característica do desvio do estado TCP no 5500 Series ASA

Índice

Introdução

Este documento descreve como configurar a característica do desvio do estado TCP, que permite que o tráfego de saída e entrada corra através do Dispositivos de segurança adaptáveis Cisco ASA série 5500 separado (ASA).

Pré-requisitos

Requisitos

Cisco ASA deve ter pelo menos a licença baixa instalada antes que você possa continuar com a configuração que está descrita neste documento.

Componentes Utilizados

A informação neste documento é baseada no 5500 Series de Cisco ASA que executa a versão de software 9.x.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

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

Informações de Apoio

Esta seção fornece uma vista geral da característica do desvio do estado TCP e da informação da sustentação relacionada.

Visão geral de características do desvio do estado TCP

Àrevelia, todo o tráfego que passa com o ASA é inspecionado através do algoritmo de segurança adaptável e é reservado completamente ou deixado cair baseado na política de segurança. A fim maximizar o desempenho do Firewall, o ASA verifica o estado de cada pacote (por exemplo, verifica se seja uma nova conexão ou uma conexão estabelecida) e atribui-lhe ao um ou outro o trajeto do gerenciamento de sessão (um pacote do sincronizar da nova conexão (SYN)), o caminho rápido (uma conexão estabelecida), ou o trajeto do plano do controle (inspeção avançada).

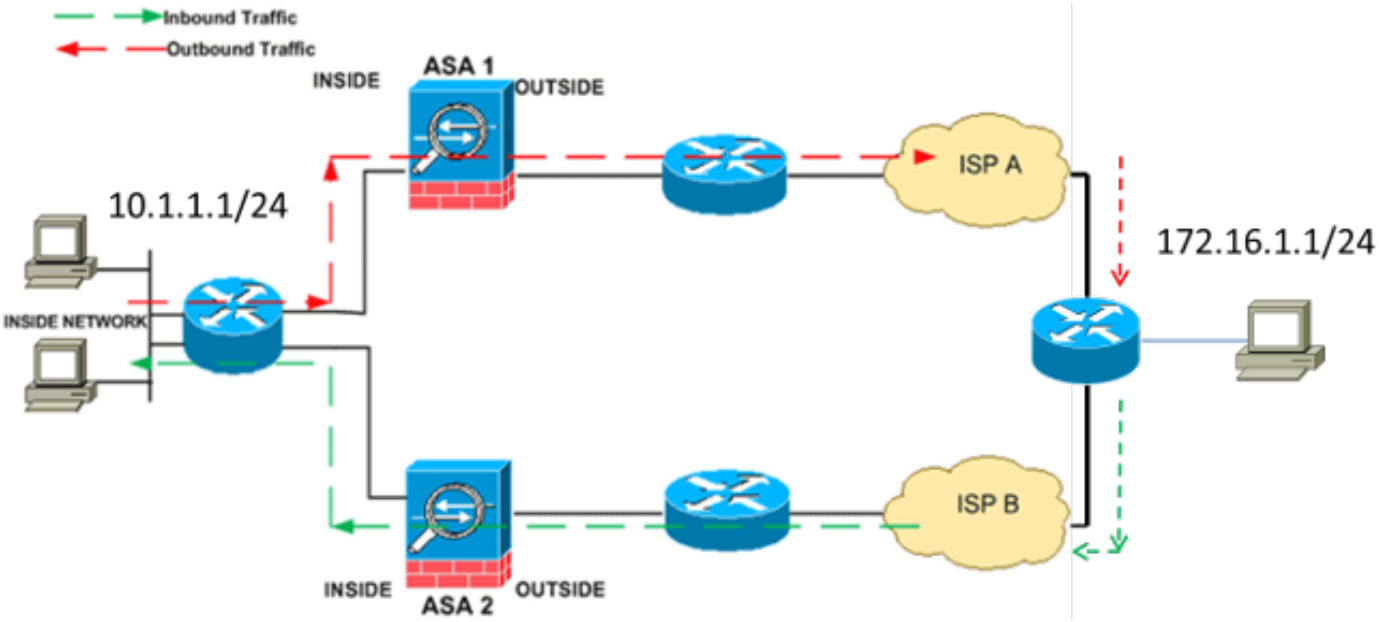
Os pacotes de TCP que combinam as conexões atual no caminho rápido podem passar com o ASA sem uma reverificação de cada aspecto da política de segurança. Esta característica maximiza o desempenho. Contudo, o método que é usado a fim estabelecer a sessão no caminho rápido (que usa o pacote SYN) e as verificações que ocorrem no caminho rápido (tal como o número de sequência TCP) pode estar na maneira de soluções assimétricas do roteamento; os fluxos de partida e de entrada de uma conexão devem passar com o mesmo ASA.

Por exemplo, uma nova conexão vai a *ASA 1.* O pacote SYN passa através do trajeto do gerenciamento de sessão, e uma entrada para a conexão é adicionada à tabela do caminho rápido. Se os pacotes subsequente nesta conexão atravessam *ASA 1*, os pacotes combinam a entrada no caminho rápido e estão passados completamente. Se os pacotes subsequente vão a *ASA 2*, onde não havia um pacote SYN que atravesse o trajeto do gerenciamento de sessão, a seguir não há nenhuma entrada no caminho rápido para a conexão, e os pacotes são deixados cair.

Se você tem o roteamento assimétrico configurado nos roteadores fluxo acima, e o tráfego alterna entre dois ASA, a seguir você pode configurar a característica do desvio do estado TCP para o tráfego específico. A característica do desvio do estado TCP altera a maneira que as sessões estão estabelecidas no caminho rápido e desabilita as verificações do caminho rápido. Esta característica trata o tráfego TCP muito enquanto trata uma conexão de UDP: quando um pacote NON-SYN que combine as redes especificadas não incorpora o ASA, e lá é nenhuma entrada do caminho rápido, a seguir o pacote atravessa o trajeto do gerenciamento de sessão a fim estabelecer a conexão no caminho rápido. Uma vez no caminho rápido, o tráfego contorneia as

verificações do caminho rápido.

Esta imagem fornece um exemplo do roteamento assimétrico, aonde o tráfego de saída atravessa um ASA diferente do que o tráfego de entrada:



> Nota: A característica do desvio do estado TCP é desabilitada à revelia no 5500 Series de Cisco ASA. Adicionalmente, a configuração do desvio do estado TCP pode causar um alto número de conexões se não é executada corretamente.

Informação da sustentação

Esta seção descreve a informação da sustentação para a característica do desvio do estado TCP.

- O do Â do âÂ do **modo do contexto a** característica do desvio do estado TCP é apoiado em único e em modos de contexto múltiplo.
- O do Â do âÂ do **modo de firewall a** característica do desvio do estado TCP é apoiado em roteado e em modos transparente.
- do Â do âÂ do **Failover o** Failover dos suportes de recurso do desvio do estado TCP.

Estas características não são apoiadas quando você usa a característica do desvio do estado TCP:

- A inspeção de aplicativo do do Â do âÂ da **inspeção de aplicativo** exige que ambos que o tráfego de entrada e de saída passa com o mesmo ASA, assim que a inspeção de aplicativo não é apoiada com a característica do desvio do estado TCP.
- **O Authentication, Authorization, and Accounting (AAA) autenticou o** do Â do âÂ das **sessões** quando um usuário autentica com um ASA, o tráfego que os retornos através do outro ASA são negados porque o usuário não autenticou com esse ASA.
- **O TCP Intercept, limite máximo da conexão embriônica,** do Â do âÂ do **randomization do**

número de sequência TCP O ASA não faz trilha do estado da conexão, assim que estas características não são aplicadas.

- O do Â do âÂ da **normalização TCP o** normalizador TCP é desabilitado.
- **O módulo de Serviços de segurança (SS) e do cartão dos Serviços de segurança** do Â do âÂ da **funcionalidade (SSC)** você não pode usar a característica do desvio do estado TCP com nenhuns aplicativos que são executado em um SS ou em SSC, tal como a Segurança IPS ou de índice (CSC).

Nota: Porque a sessão de conversão é estabelecida separadamente para cada ASA, assegure-se de que você configure a tradução de endereço da rede estática (NAT) em ambos os ASA para o tráfego do desvio do estado TCP. Se você usa o NAT dinâmico, o endereço que é escolhido para a sessão em *ASA 1* diferirá do endereço que é escolhido para a sessão em *ASA 2.*

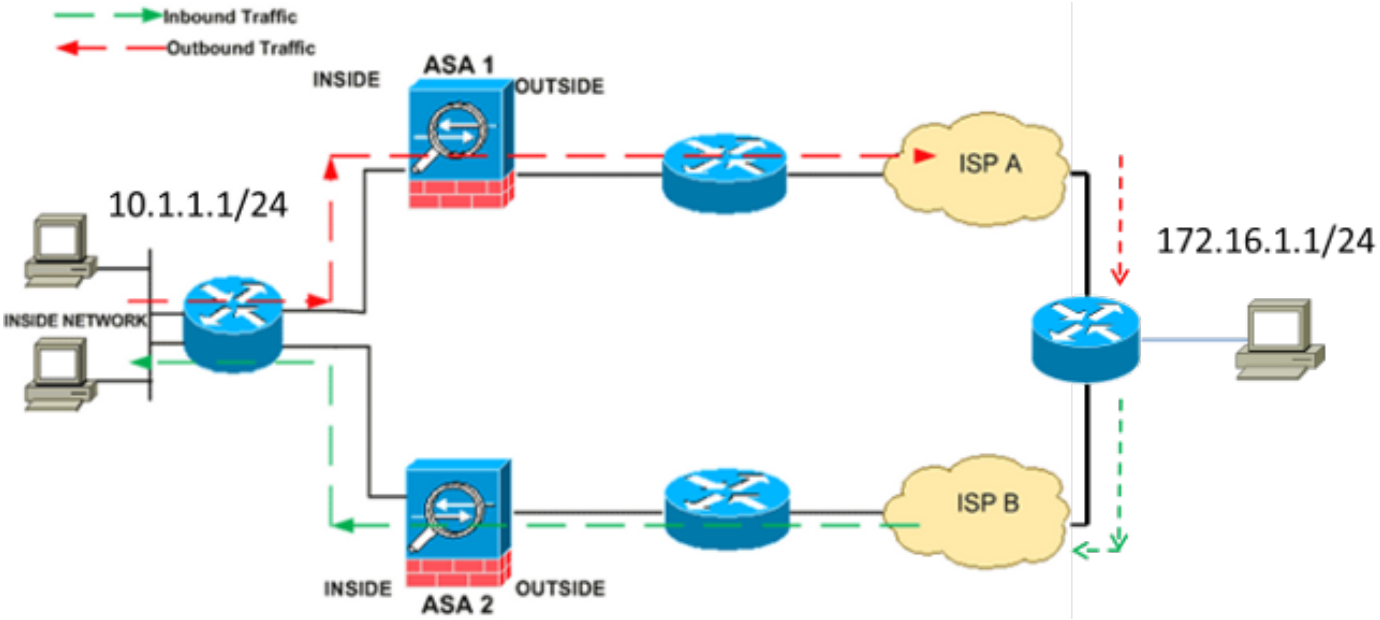
Configurar

Esta seção descreve como configurar a característica do desvio do estado TCP no 5500 Series ASA em duas encenações diferentes.

Nota: Use a ferramenta de consulta de comandos (clientes registrados somente) a fim obter mais informação nos comandos que são usados nesta seção.

Cenário 1

Esta é a topologia que é usada para a primeira encenação:



Nota: Você deve aplicar a configuração que é descrita nesta seção a ambos os ASA.

Termine estas etapas a fim configurar a característica do desvio do estado TCP:

1. Incorpore o comando do class_map_name do mapa de classe a fim criar um *mapa da classe*. O mapa da classe é usado a fim identificar o tráfego para que você quer desabilitar a inspeção do firewall stateful.Nota: O mapa da classe que é usado neste exemplo é **tcp_bypass**.`ASA(config)#class-map tcp_bypass`
2. Inscreva o comando parameter do fósforo a fim especificar o tráfego do interesse dentro do mapa da classe. Quando você usa a estrutura de política modular, use o **comando access-list do fósforo no** modo da *configuração de mapa de classe* a fim usar uma lista de acessos para a identificação do tráfego a que você quer aplicar ações. Está aqui um exemplo desta configuração:

   ```
   ASA(config)#class-map tcp_bypass
   ASA(config-cmap)#match access-list tcp_bypass
   ```
   Nota: **Os tcp_bypass** são o nome da lista de acesso que é usada neste exemplo. Refira a seção de identificação do tráfego (mapa da classe da camada 3/4) do *manual de configuração do 5500 Series de Cisco ASA usando o CLI, 8.2* para obter mais informações sobre de como especificar o tráfego do interesse.
3. Inscreva o comando name do mapa de política a fim adicionar um mapa de política ou editar um mapa de política (de que está já atual) que atribui as ações para ser considerações recolhidas ao tráfego do mapa da classe especificada. Quando você usa a estrutura de política modular, use o **comando policy-map** (sem o *tipo* palavra-chave) no *modo de configuração global* a fim atribuir ações ao tráfego que você identificou com um mapa da classe da camada 3/4 (o **mapa de classe** ou o **tipo comando management do mapa de classe**). Neste exemplo, o mapa de política é **tcp_bypass_policy**:
   ```
   ASA(config-cmap)#policy-map tcp_bypass_policy
   ```
4. Inscreva o comando class no modo da *configuração de mapa de política* a fim atribuir o mapa criado da classe (*tcp_bypass*) ao mapa de política (*tcp_bypass_policy*) de modo que você possa atribuir as ações ao tráfego do mapa da classe. Neste exemplo, o mapa da classe é **tcp_bypass**:
   ```
   ASA(config-cmap)#policy-map tcp_bypass_policy
   ASA(config-pmap)#class tcp_bypass
   ```
5. Incorpore o comando do TCP-estado-desvio das avançado-opções da conexão do grupo ao *modo de configuração de classe* a fim permitir a característica do desvio do estado TCP. Este comando foi introduzido na versão 8.2(1). *O modo de configuração de classe* é acessível do modo da *configuração de mapa de política*, segundo as indicações deste 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. Incorpore o policymap_name da serviço-política [global | conecte o comando do *intf*] no *modo de configuração global* a fim ativar globalmente um mapa de política em todas as relações ou em uma relação visada. A fim desabilitar a política de serviços, não use **nenhum** formulário deste comando. Inscreva o **comando service-policy** a fim permitir um grupo de políticas em uma relação. A palavra-chave **global** aplica o mapa de política a todas as relações, e a palavra-chave da **relação** aplica o mapa de política a somente uma relação. Somente uma política global é permitida. A fim cancelar a política global em uma relação, você pode aplicar uma política de serviços a essa relação. Você pode aplicar somente um mapa de política a cada relação. Aqui está um exemplo:
   ```
   ASA(config-pmap-c)#service-policy tcp_bypass_policy outside
   ```

Está aqui um exemplo de configuração para a característica do desvio do estado TCP em *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
```

Está aqui um exemplo de configuração para a característica do desvio do estado TCP em *ASA2*:

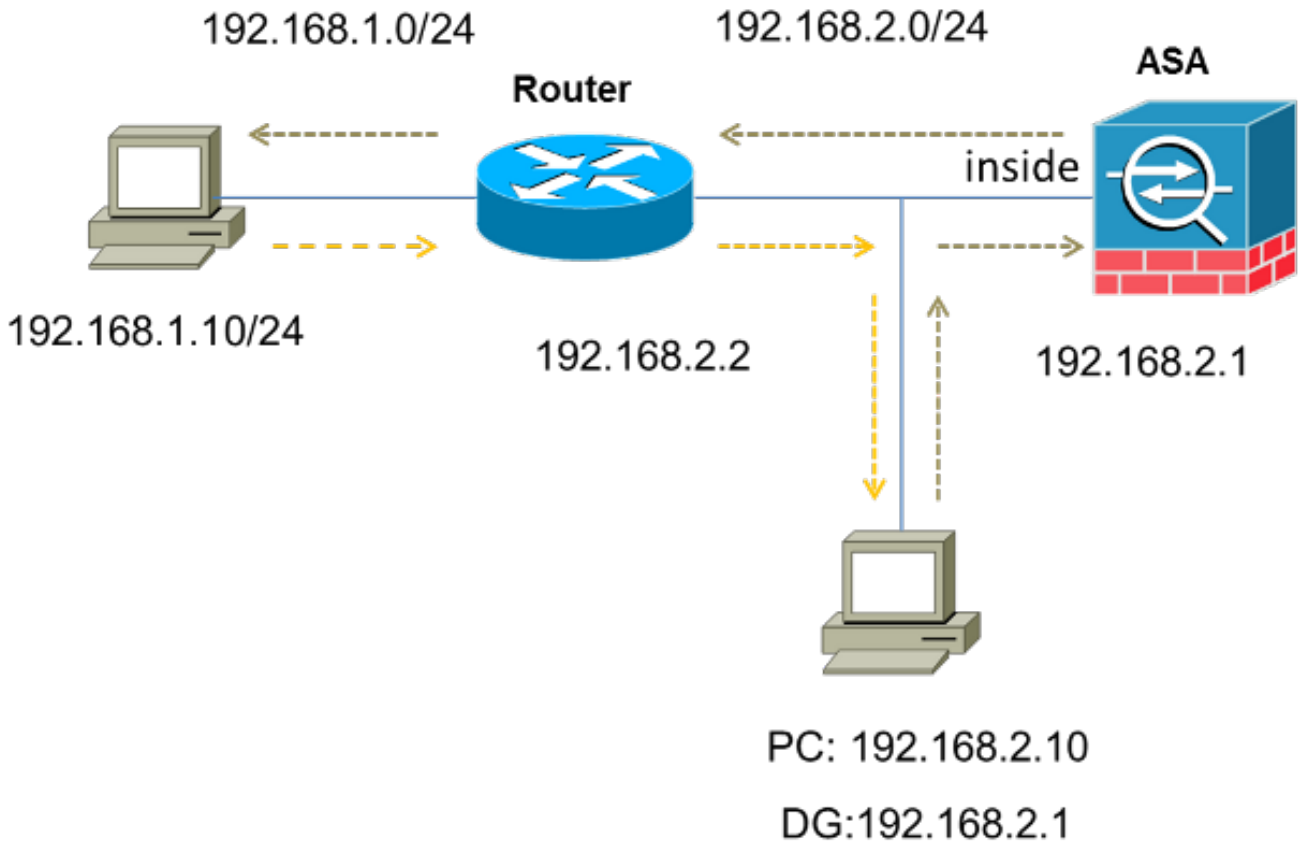
```
!--- Configure the access list to specify the TCP traffic
!--- that needs to by-pass inspection to improve the performance.

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 a característica do desvio do estado TCP no ASA para as encenações que usam o roteamento assimétrico, onde o tráfego incorpora e sae do ASA da mesma relação (u-*gerencio*).

Está aqui a topologia que é usada nesta encenação:



Termine estas etapas a fim configurar a característica do desvio do estado TCP:

1. Crie uma *lista de acesso* a fim combinar o tráfego que deve contornear 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. Incorpore o comando do class_map_name do mapa de classe a fim criar um *mapa da classe*. O mapa da classe é usado a fim identificar o tráfego para que você quer desabilitar a inspeção do firewall stateful.Nota: O mapa da classe que é usado neste exemplo é **tcp_bypass**.`ASA(config)#class-map tcp_bypass`

3. Inscreva o comando parameter do fósforo a fim especificar o tráfego do interesse no mapa da classe. Quando você usa a estrutura de política modular, use o **comando access-list do fósforo no** modo da *configuração de mapa de classe* a fim usar uma lista de acessos para a identificação do tráfego a que você quer aplicar ações. Está aqui um exemplo desta configuração:
   ```
   ASA(config)#class-map tcp_bypass
   ASA(config-cmap)#match access-list tcp_bypass
   ```
   Nota: **Os tcp_bypass** são o nome da lista de acesso que é usada neste exemplo. Refira a identificação da seção do tráfego (mapa da classe da camada 3/4) do *manual de configuração do 5500 Series de Cisco ASA usando o CLI, 8.2* para obter mais informações sobre de como especificar o tráfego do interesse.
4. Inscreva o comando name do mapa de política a fim adicionar um mapa de política ou editar um mapa de política (de que está já atual) esse ajusta as ações para ser considerações recolhidas ao tráfego do mapa da classe especificada. Quando você usa a estrutura de política modular, use o **comando policy-map** (sem o *tipo* palavra-chave) no *modo de configuração global* a fim atribuir as ações ao tráfego que você identificou com um mapa da classe da camada 3/4 (o **mapa de classe** ou o **tipo comando management do mapa de classe**). Neste exemplo, o mapa de política é **tcp_bypass_policy**:
   ```
   ASA(config-cmap)#policy-map tcp_bypass_policy
   ```
5. Inscreva o comando class no modo da *configuração de mapa de política* a fim atribuir o mapa criado da classe (*tcp_bypass*) ao mapa de política (*tcp_bypass_policy*) de modo que você possa atribuir ações ao tráfego do mapa da classe. Neste exemplo, o mapa da classe é **tcp_bypass**:
   ```
   ASA(config-cmap)#policy-map tcp_bypass_policy
   ASA(config-pmap)#class tcp_bypass
   ```
6. Incorpore o comando do TCP-estado-desvio das avançado-opções da conexão do grupo ao *modo de configuração de classe* a fim permitir a característica do desvio do estado TCP. Este comando foi introduzido na versão 8.2(1). *O modo de configuração de classe* é acessível do modo da *configuração de mapa de política*, segundo as indicações deste 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. Incorpore o policymap_name da serviço-política [global | conecte o comando do *intf*] no *modo de configuração global* a fim ativar globalmente um mapa de política em todas as relações ou em uma relação visada. A fim desabilitar a política de serviços, não use **nenhum** formulário deste comando. Inscreva o **comando service-policy** a fim permitir um grupo de políticas em uma relação. A palavra-chave **global** aplica o mapa de política a todas as relações, e a palavra-chave da **relação** aplica a política a somente uma relação. Somente uma política global é permitida. A fim cancelar a política global em uma relação, você pode aplicar uma política de serviços a essa relação. Você pode aplicar somente um mapa de política a cada relação. 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
   ```

Está aqui um exemplo de configuração para a característica do desvio do 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

Inscreva o comando show conn a fim ver o número de TCP ativo e de conexões de UDP e a informação sobre as conexões de vários tipos. A fim indicar o estado de conexão para o tipo de conexão designado, inscreva o comando show conn no *modo de exec privilegiado*.

> Nota: Esse comando oferece suporte aos endereços IPv4 e IPv6. A saída que é indicada para as conexões que usam a característica do desvio do estado TCP inclui a bandeira **B.**

Estão aqui umas saídas de exemplo:

```
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
```

Troubleshooting

Não há nenhuma informação de Troubleshooting específica para esta característica. Refira estes documentos para a informação de Troubleshooting geral da Conectividade:

- Capturas de pacote de informação ASA com CLI e exemplo da configuração ASDM
- ASA 8.2: O pacote corre através do Firewall de Cisco ASA

> Nota: As conexões do desvio do estado TCP não replicated à unidade em standby em um

par de failover.

Mensagens de erro

O ASA indica este Mensagem de Erro mesmo depois que a característica do desvio do estado TCP é permitida:

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

Os pacotes do Internet Control Message Protocol (ICMP) são deixados cair pelo ASA devido às verificações de segurança que são adicionadas pela característica do stateful ICMP. Estes são geralmente respostas de eco ICMP sem uma *requisição de eco* válida já passada através do ASA, ou mensagens de erro ICMP que não são relacionados a nenhuma sessão TCP, UDP, ou ICMP estabelecida atualmente no ASA.

O ASA indica este log mesmo se a característica do desvio do estado TCP é permitida porque a incapacidade desta funcionalidade (isto é, verifica das entradas do *retorno* ICMP para ver se há o tipo 3 na tabela de conexão) não é possível. Contudo, a característica do desvio do estado TCP trabalha corretamente.

Incorpore este comando a fim impedir a aparência destas mensagens:

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

Informações Relacionadas

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