Het configureren van de TCP-statelijke omzeilingsfunctie in de ASA 5500 Series

Inhoud

Inleiding

Dit document beschrijft hoe u de TCP-statustbypass-functie kunt configureren, waardoor het uitgaande en inkomende verkeer door afzonderlijke Cisco ASA 5500 Series adaptieve security applicaties (ASA's) kan stromen.

Voorwaarden

Vereisten

De Cisco ASA moet minimaal de basislicentie hebben geïnstalleerd voordat u kunt verdergaan met de configuratie die in dit document wordt beschreven.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco ASA 5500 Series die software versie 9.x uitvoeren.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Achtergrondinformatie

Deze sectie verschaft een overzicht van de TCP-statelijke omzeilingsfunctie en de verwante ondersteuningsinformatie.

Overzicht van TCP-statelijke omzeilingsfuncties

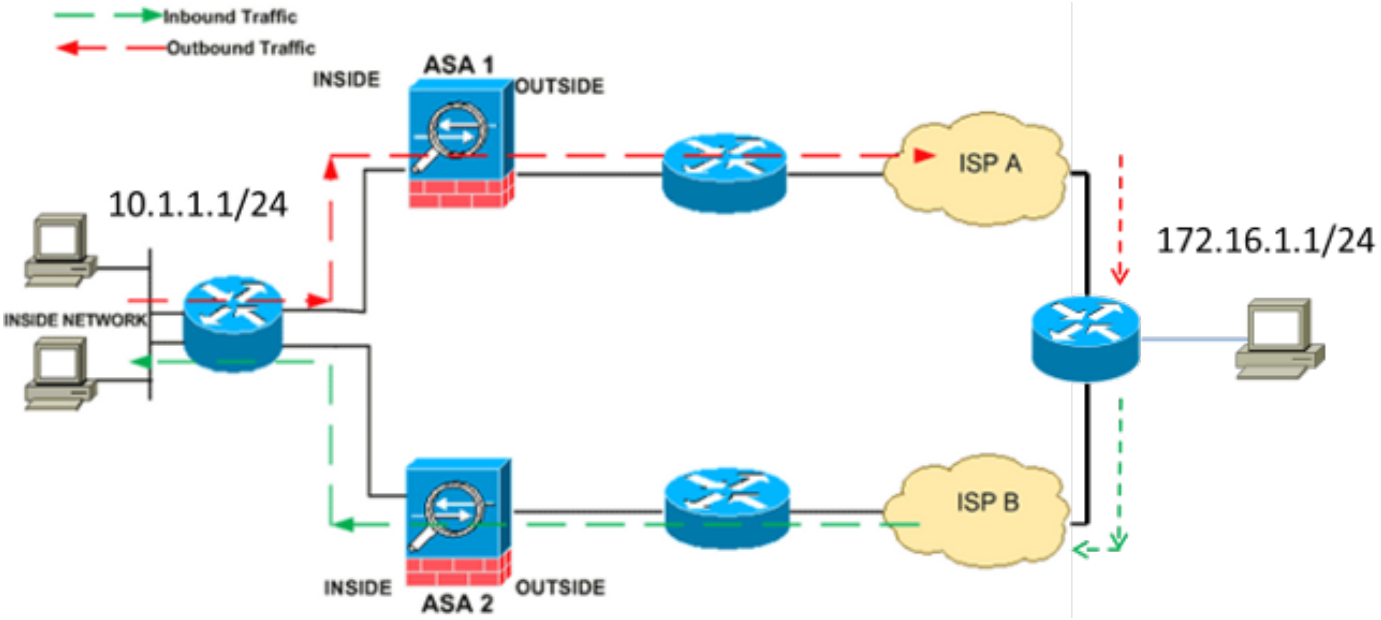
Standaard wordt al het verkeer dat door de ASA passeert geïnspecteerd via het adaptieve security algoritme en op basis van het beveiligingsbeleid toegestaan of laten vallen. Om de prestaties van de Firewall te maximaliseren, controleert de ASA de staat van elk pakje (bijvoorbeeld, controleert het of het een nieuwe verbinding of een gevestigde verbinding is) en wijst het toe aan of het sessiebeheerpad (een nieuw verbinding synchroon (SYN) pakje), het snelle pad (een gevestigde verbinding) of het besturingsplanpad (geavanceerde inspectie).

De TCP-pakketten die overeenkomen met de huidige verbindingen in het snelle pad kunnen door de ASA gaan zonder een controle van elk aspect van het beveiligingsbeleid. Deze functie maximaliseert de prestaties. Maar de methode die wordt gebruikt om de sessie in het snelle pad (die het SYN-pakket gebruikt) en de controles die in het snelle pad (zoals het TCP-sequentienummer) voorkomen kan asymmetrische routingoplossingen in de weg staan; zowel de uitgaande als inkomende stromen van een verbinding moeten door dezelfde ASA gaan.

Een nieuwe verbinding gaat bijvoorbeeld naar *ASA 1*. Het SYN-pakket gaat door het sessiebeheerpad en een ingang voor de verbinding wordt toegevoegd aan de snelle pad tabel. Als volgende pakketten op deze verbinding door *ASA 1* gaan, komen de pakketten overeen met de ingang in het snelle pad en worden doorgegeven. Als volgende pakketten naar *ASA 2* gaan, waar er geen SYN-pakket was dat door het sessiebeheerpad ging, dan is er geen ingang in het snelle pad voor de verbinding en worden de pakketten ingetrokken.

Als u asymmetrische routing op de upstream routers hebt ingesteld en verkeerswisselingen tussen twee ASA's zijn uitgevoerd, dan kunt u de TCP-state bypass-functie voor specifiek verkeer configureren. De TCP status bypass functie verandert de manier waarop de sessies in het fast pad worden ingesteld en schakelt de fast path controles uit. Deze eigenschap behandelt veel TCP verkeer zoals het een UDP verbinding behandelt: wanneer een niet-SYN-pakket dat met de gespecificeerde netwerken overeenkomt, de ASA invoert en er geen snelle pad is, gaat het pakket door het sessiebeheerpad om de verbinding in het snelle pad op te zetten. Eenmaal in het snelle pad passeert het verkeer de snelle controles van het pad.

Dit beeld biedt een voorbeeld van asymmetrische routing, waar het uitgaande verkeer door een andere ASA gaat dan het inkomende verkeer:



Opmerking: De TCP-status bypass-functie is standaard uitgeschakeld in Cisco ASA 5500 Series. Daarnaast kan de TCP-status bypass-configuratie een groot aantal verbindingen veroorzaken als deze niet correct wordt uitgevoerd.

Ondersteuningsinformatie

In dit gedeelte wordt de ondersteuningsinformatie voor de TCP-statustoorbypass-functie beschreven.

- **Context Mode** Hiermee wordt de TCP-omleidingsfunctie ondersteund in één en meerdere context modi.
- **Firewallmodus** ß de de TCP-statustoorfunctie wordt ondersteund in routed en transparante modi.
- **Failover** Hiermee de TCP-overloopfunctie ondersteunt failover.

Deze functies worden niet ondersteund wanneer u de TCP status bypass-functie gebruikt:

- **Toepassingsinspectie**-ß-Application-inspectie vereist dat zowel het inkomende als het uitgaande verkeer door dezelfde ASA passeert, zodat de toepassingsinspectie niet wordt ondersteund met de TCP-statustbypass-functie.
- **Verificatie, autorisatie en accounting (AAA) geauthentiseerde sessies** ß$ Wanneer een gebruiker authenticeert met een ASA, wordt het verkeer dat retourneert via de andere ASA afgewezen omdat de gebruiker niet echt authentiek was met die ASA.
- **TCP-onderschepping, maximale embryonale verbindingsgrens, TCP sequentienummer randomisatie** ß XIVThe ASA volgt de staat van de verbinding niet, dus deze functies worden niet toegepast.
- **TCP-normalisatie**-ßH-H**wordt** de TCP-normalizer uitgeschakeld.

- **Security Services Module (SSM) en Security Services Card (SSC) functionaliteit**, u kunt de TCP-bypass-functie niet gebruiken bij toepassingen die op een SSM of SSC draaien, zoals IPS of Content Security (CSC).

  Opmerking: Omdat de vertaalsessie afzonderlijk voor elke ASA wordt ingesteld, zorg er dan voor dat u statische netwerkadresomzetting (NAT) op beide ASA's voor de TCP-statustomboeking op een andere manier configureren. Als u dynamisch NAT gebruikt, zal het adres dat geselecteerd is voor de sessie op *ASA 1* verschillen van het adres dat geselecteerd is voor de sessie op *ASA 2*.

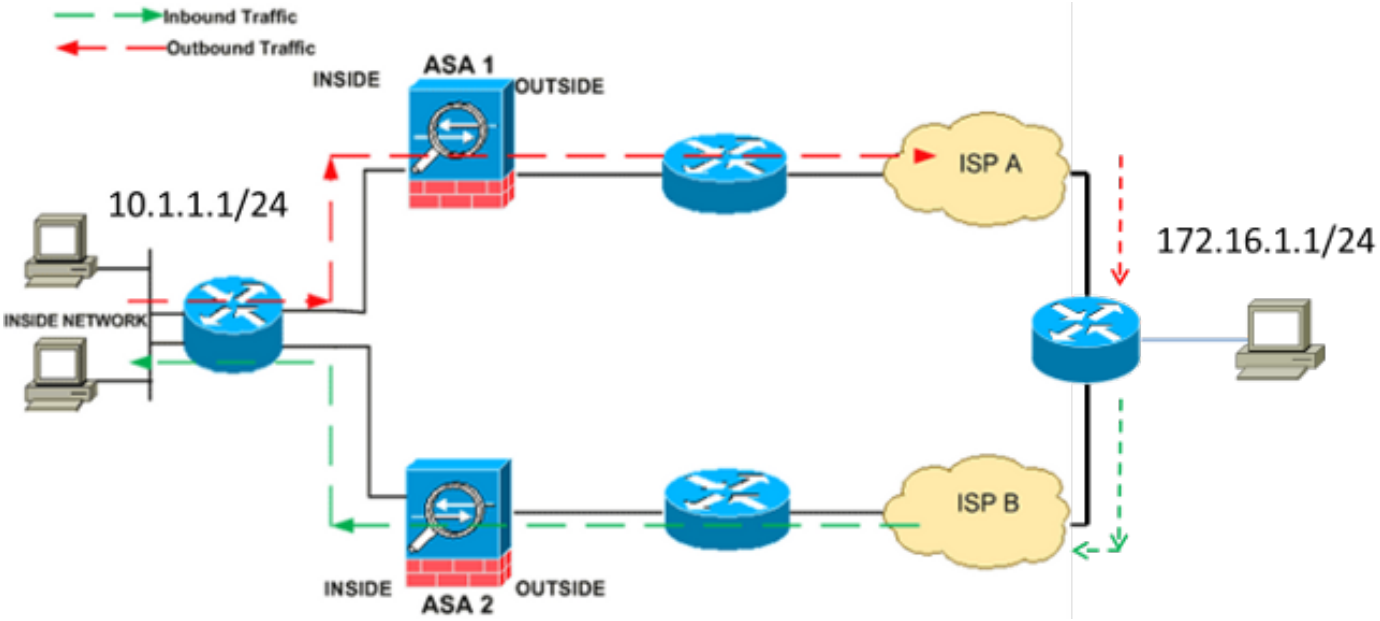
Configureren

In deze sectie wordt beschreven hoe u de TCP state bypass-functie op de ASA 5500 Series-serie in twee verschillende scenario's kunt configureren.

Opmerking: Gebruik het Opdrachtupgereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Scenario 1

Dit is de topologie die voor het eerste scenario wordt gebruikt:



Opmerking: U moet de configuratie die in deze sectie wordt beschreven op beide ASA's toepassen.

Voltooi deze stappen om de TCP status bypass-functie te configureren:

1. Voer de class-map class_map_name opdracht in om een *class map* te maken. De class map wordt gebruikt om het verkeer te identificeren waarvoor u stateful Firewall inspection wilt

uitschakelen.Opmerking: De class map die gebruikt wordt in dit voorbeeld is **tcp_bypass**.

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

2. Voer de opdracht match parameter in om het verkeer van belang binnen de class map op te geven. Wanneer u het Modulaire Kader van het Beleid gebruikt, gebruik de **van de toegangs-lijst** opdracht in *class-map configuratie* modus om een toegangslijst voor identificatie van het verkeer te gebruiken waarop u acties wilt toepassen. Hier is een voorbeeld van deze configuratie:

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

Opmerking: De **tcp_bypass** is de naam van de access-list die in dit voorbeeld gebruikt wordt. Raadpleeg het gedeelte Identificatie van verkeer (Layer 3/4 Class Map) van de *Cisco ASA 5500 Series Configuration Guide met behulp van de CLI, 8.2* voor meer informatie over hoe u het verkeer van belang wilt specificeren.

3. Typ de opdracht beleidsmap-map om een beleidsplan toe te voegen of een beleidsplan (dat reeds aanwezig is) te bewerken dat de acties toewijst die moeten worden ondernomen in verband met het gespecificeerde class map verkeer. Wanneer u het Modulaire Kader van het Beleid gebruikt, gebruik de **beleid-kaart** opdracht (zonder het *type* sleutelwoord) in *mondiale* configuratie modus om acties aan het verkeer toe te wijzen dat u met een Layer 3/4 klasse kaart (de **class-map** of **class-map type management opdracht) hebt geïdentificeerd.** In dit voorbeeld, is de beleidslijn **tcp_bypass_policy**:

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

4. Voer de opdracht class in *policy-map configuratie* mode in om de gemaakte class map (*tcp_bypass*) toe te wijzen aan de *beleidsplan (tcp_bypass_policy*) zodat u de acties kunt toewijzen aan het class map traffic. In dit voorbeeld is de class map **tcp_bypass**:

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

5. Voer de ingestelde opdracht voor geavanceerde verbindingen in tussen TCP en state-bypass in *class configuratie* mode om de TCP staat bypass-functie in te schakelen. Deze opdracht is ingevoerd in versie 8.2(1). De configuratie-modus van de klasse is toegankelijk vanuit de configuratie-modus *voor de beleidskaart*, zoals in dit voorbeeld wordt getoond:

```
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. Voer de service-beleidsmap_name in [global | interface *intf*] opdracht in de *mondiale* configuratiemodus om wereldwijd een beleidskaart op alle interfaces of op een gerichte interface te activeren. Gebruik het **geen** formulier van deze opdracht om het servicebeleid uit te schakelen. Typ de opdracht **Service-beleid** om een verzameling beleid op een interface in te schakelen. Het **mondiale** sleutelwoord past de beleidskaart op alle interfaces toe, en het **interface** sleutelwoord past de beleidskaart op slechts één interface toe. Er is slechts één algemeen beleid toegestaan. Om het algemene beleid op een interface te negeren, kunt u een servicebeleid op die interface toepassen. U kunt slechts één beleidskaart op elke interface toepassen. Hierna volgt een voorbeeld:

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

Hier is een voorbeeldconfiguratie voor de TCP status bypass optie op *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
```

Hier is een voorbeeldconfiguratie voor de TCP status bypass optie op *ASA2*:

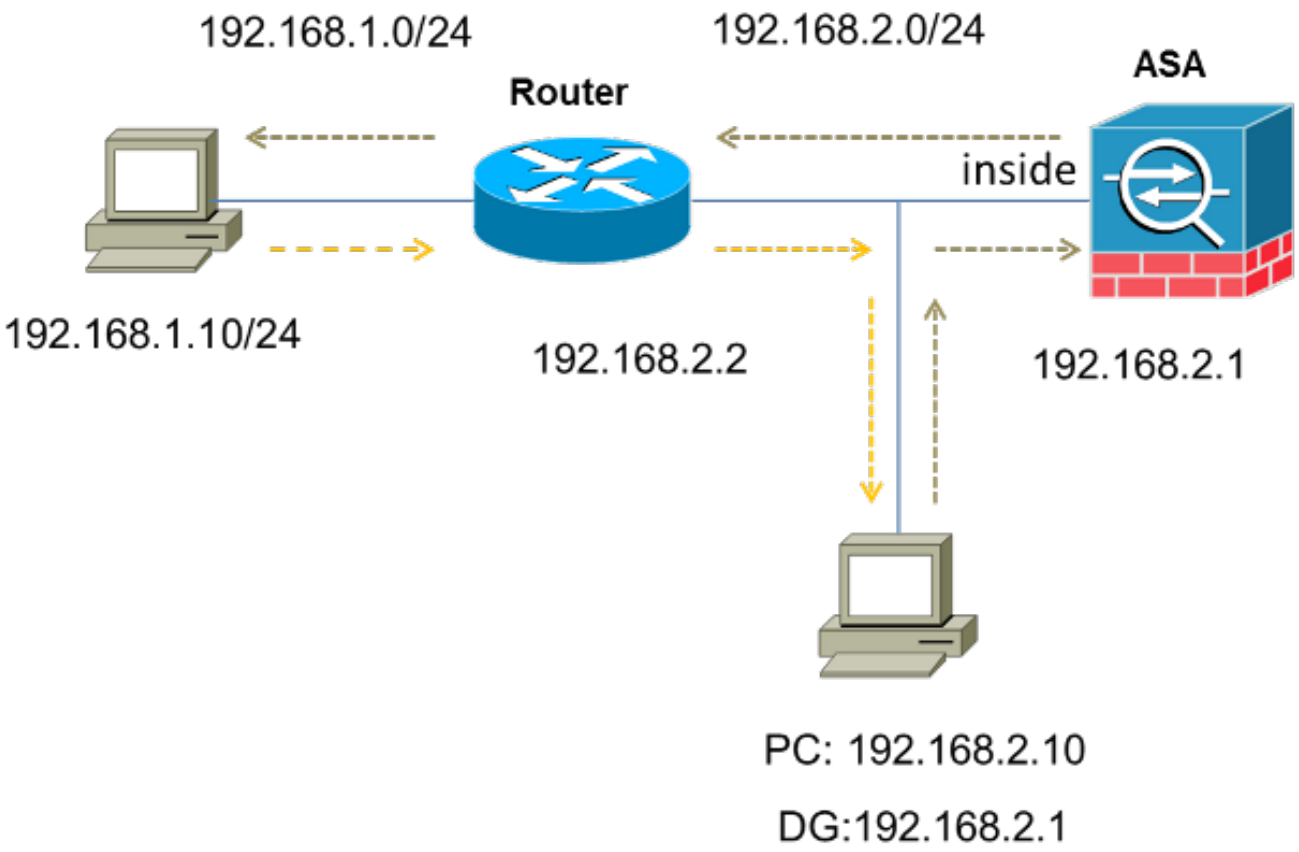
```
!--- Configure the access list to specify the TCP traffic
!--- that needs to by-pass inspection to improve the performance.

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
```

Scenario 2

In deze sectie wordt beschreven hoe u de TCP-bypass-functie op de ASA-software kunt configureren voor scenario's die asymmetrische routing gebruiken, waarbij het verkeer de ASA ingaat en verlaat vanuit dezelfde interface (*u-draaien*).

Hier is de topologie die in dit scenario wordt gebruikt:



Voltooi deze stappen om de TCP status bypass-functie te configureren:

1. Maak een *toegangslijst* om het verkeer aan te passen dat de TCP-inspectie zou moeten omzeilen:

```
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. Voer de class-map class_map_name opdracht in om een *class map* te maken. De class map wordt gebruikt om het verkeer te identificeren waarvoor u stateful Firewall inspection wilt uitschakelen.Opmerking: De class map die gebruikt wordt in dit voorbeeld is **tcp_bypass**.
```
ASA(config)#class-map tcp_bypass
```
3. Voer de opdracht match parameter in om het verkeer van belang in de class map op te geven. Wanneer u het Modulaire Kader van het Beleid gebruikt, gebruik de **van de** verbindingstoegang **tot lijst** opdracht in *class-map configuratie* modus om een toegangslijst voor identificatie van het verkeer te gebruiken waarop u acties wilt toepassen. Hier is een voorbeeld van deze configuratie:

```
ASA(config)#class-map tcp_bypass
ASA(config-cmap)#match access-list tcp_bypass
```
Opmerking: De **tcp_bypass** is de naam van de access-list die in dit voorbeeld gebruikt wordt. Raadpleeg het gedeelte Identificatie van verkeer (Layer 3/4 Class Map) van de *Cisco ASA 5500 Series Configuration Guide met behulp van de CLI, 8.2* voor meer informatie over het specificeren van het verkeer van belang.
4. Voer de beleids-map opdracht in om een beleidsplan toe te voegen of een beleidsplan (dat reeds aanwezig is) te bewerken dat de acties bepaalt die moeten worden ondernomen in verband met het gespecificeerde class map verkeer. Wanneer u het Modulaire Kader van het Beleid gebruikt, gebruik de **beleid-kaart** opdracht (zonder het *type* sleutelwoord) in *mondiale* configuratie modus om de acties aan het verkeer toe te wijzen dat u met een Layer 3/4 klas kaart (de **class-map** of **class-map type management opdracht) hebt geïdentificeerd.** In dit voorbeeld, is de beleidslijn **tcp_bypass_policy**:

```
ASA(config-cmap)#policy-map tcp_bypass_policy
```
5. Voer de opdracht class in *policy-map configuratie* mode in om de gemaakte class map (*tcp_bypass*) toe te wijzen aan de beleidslijn (*tcp_bypass_policy*), zodat u acties kunt toewijzen aan het class map traffic. In dit voorbeeld is de class map **tcp_bypass**:

```
ASA(config-cmap)#policy-map tcp_bypass_policy
ASA(config-pmap)#class tcp_bypass
```
6. Voer de ingestelde opdracht voor geavanceerde verbindingen in tussen TCP en state-bypass in *class configuratie* mode om de TCP staat bypass-functie in te schakelen. Deze opdracht is ingevoerd in versie 8.2(1). De configuratie-modus van de *klasse* is toegankelijk vanuit de configuratie-modus *voor de beleidskaart*, zoals in dit voorbeeld wordt getoond:

```
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. Voer de service-beleidsmap_name in [global | interface *intf*] opdracht in *mondiale configuratie*-modus om wereldwijd een beleidskaart op alle interfaces of op een gerichte interface te activeren. Gebruik het **geen** formulier van deze opdracht om het servicebeleid uit te schakelen. Typ de opdracht **Service-beleid** om een verzameling beleid op een interface in te schakelen. Het **mondiale** sleutelwoord past de beleidskaart op alle interfaces toe, en het **interface** sleutelwoord past het beleid op slechts één interface toe. Er is slechts één algemeen beleid toegestaan. Om het algemene beleid op een interface te negeren, kunt u een servicebeleid op die interface toepassen. U kunt slechts één beleidskaart op elke interface toepassen. Hierna volgt een voorbeeld:

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

8. Hetzelfde veiligheidsniveau voor het verkeer op de ASA toestaan:

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

Hier is een voorbeeldconfiguratie voor de TCP status bypass optie op de 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
```

Verifiëren

Voer het **show conn** opdracht om het aantal actieve TCP- en UDP-verbindingen en informatie over de verbindingen van verschillende typen te bekijken. Voer de **show conn** Opdracht in *bevoorrechte EXEC* modus.

> Opmerking: Deze opdracht ondersteunt IPv4- en IPv6-adressen. De output die wordt weergegeven voor de verbindingen die de TCP state bypass optie gebruiken omvat de flag **b**.

Hier wordt een voorbeeld uitgevoerd:

```
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
```

Problemen oplossen

Er is geen specifieke informatie over probleemoplossing voor deze functie. Raadpleeg deze documenten voor informatie over probleemoplossing bij algemene connectiviteit:

- ASA Packet Capture met CLI en ASDM Configuratievoorbeeld
- ASA 8.2: PacketFlow via Cisco ASA-firewall

  Opmerking: De TCP-status bypass-verbindingen worden niet gerepliceerd naar de standby-unit in een failover-paar.

Foutberichten

ASA toont deze foutmelding zelfs nadat de TCP state bypass optie is ingeschakeld:

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

De pakketten Internet Control Message Protocol (ICMP) worden door de ASA ingetrokken vanwege de beveiligingscontroles die door de stateful ICMP-functie worden toegevoegd. Dit zijn meestal *echo*-antwoorden van ICMP zonder een geldig *echo-verzoek* dat al over de ASA is verspreid of ICMP-foutmeldingen die geen verband houden met een TCP-, UDP- of ICMP-sessie die momenteel in de ASA is ingesteld.

ASA toont dit logbestand zelfs als de TCP status bypass optie is ingeschakeld omdat de disablement van deze functionaliteit (dat wil zeggen, controles van de ICMP *return* items voor Type 3 in de verbindingstabel) niet mogelijk is. Maar de TCP status bypass functie werkt correct.

Typ deze opdracht om de weergave van deze berichten te voorkomen:

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

Gerelateerde informatie

- Cisco adaptieve security apparaatbeheer
- Cisco ASA 5500 Series adaptieve security applicaties
- Verzoeken om opmerkingen (RFC's)
- Technische ondersteuning en documentatie – Cisco Systems