ASA 8.2.X Configuratievoorbeeld van TCP-statelijke omzeilingfuncties

Inhoud

Inleiding

Dit document beschrijft hoe u de TCP status bypass-functie kunt configureren. Deze optie maakt uitgaande en inkomende stromen door afzonderlijke Cisco ASA 5500 Series adaptieve security applicaties mogelijk.

Voorwaarden

Licentievereisten

De Cisco ASA 5500 Series adaptieve security applicaties moeten ten minste de basislicentie hebben.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco adaptieve security applicatie (ASA) met versie 8.2(1) en hoger.

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 informatie over documentconventies.

TCP-Statusbypass

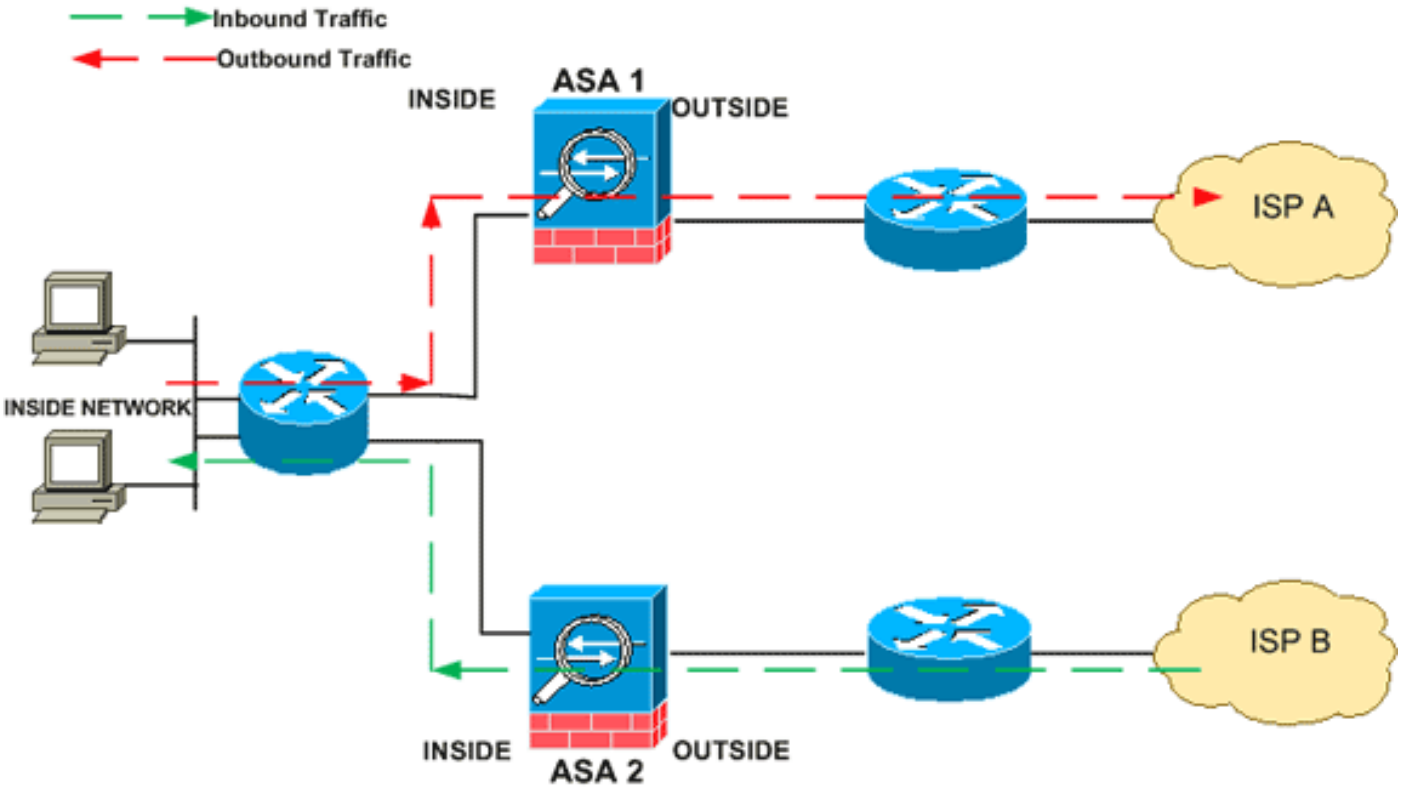
Standaard wordt al het verkeer dat door de Cisco adaptieve security applicatie (ASA) passeert, geïnspecteerd met behulp van het adaptieve security algoritme en is het toegestaan of laten vallen op basis van het beveiligingsbeleid. Om de firewallprestaties te maximaliseren, controleert de ASA de staat van elk pakje (bijvoorbeeld is dit een nieuwe verbinding of een gevestigde verbinding?) en wijst de ASA de status toe aan ofwel het sessiebeheerpad (een nieuw verbinding SYN-pakket), het snelle pad (een gevestigde verbinding) of het besturingsplanpad (geavanceerde inspectie).

TCP-pakketten die overeenkomen met bestaande verbindingen in het snelle pad kunnen door het adaptieve security apparaat lopen zonder alle aspecten van het beveiligingsbeleid opnieuw te controleren. Deze functie maximaliseert de prestaties. Nochtans, kan de methode die wordt gebruikt om de zitting in het snelle pad (dat het pakket SYN gebruikt) en de controles te vestigen die in het snelle pad (zoals TCP sequentienummer) in de weg van asymmetrische routingoplossingen staan: zowel de uitgaande als inkomende stroom van een verbinding moet 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 van deze verbinding door *ASA 1* gaan, zullen de pakketten de ingang in het snelle pad aanpassen en door 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 upstream routers hebt ingesteld en verkeerswisselaars tussen twee ASA's, dan kunt u TCP-statustbypass configureren voor specifiek verkeer. De TCP-statustbypass verandert de manier waarop de sessies in het snelpad 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 de gespecificeerde netwerken aansluit, de ASA ingaat en er geen snelle padingang 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 optie TCP-statustoorbypass is standaard uitgeschakeld aan de Cisco ASA 5500 Series adaptieve security applicaties.

Ondersteuningsinformatie

Deze sectie verschaft de ondersteuningsinformatie voor de TCP-statustoorbypass-functie.

- Context Mode — ondersteund in enkele en meerdere context-modus.
- Firewallmodus — ondersteund in routed en transparant.
- failover-ondersteunt failover.

Deze functies worden niet ondersteund wanneer u TCP-statustbypass gebruikt:

- Toepassingsinspectie-toepassingsinspectie vereist zowel inkomend als uitgaand verkeer om door de zelfde ASA door te gaan, dus de toepassingsinspectie wordt niet ondersteund met de TCP-statustbypass.
- AAA geauthentiseerde sessies-wanneer een gebruiker authentiek verklaart met één ASA, zal verkeer dat via de andere ASA terugkeert worden ontkend omdat de gebruiker niet echt bevestig met die ASA.
- TCP-onderschepping, maximum embryonale verbinding limiet, TCP sequentienummer randomisatie-De ASA houdt geen spoor van de staat van de verbinding, dus deze functies worden niet toegepast.
- TCP-normalisatie-de TCP-normalisatie is uitgeschakeld.
- SSM en SSC functionaliteit—U kunt geen TCP-state bypass en elke toepassing die op een SSM of SSC wordt uitgevoerd, zoals IPS of CSC gebruiken.

NAT-richtsnoeren: Omdat de vertaalsessie afzonderlijk voor elke ASA wordt ingesteld, dient u statische NAT op beide ASA's te configureren voor TCP-bypassverkeer; Als u dynamisch NAT gebruikt, zal het adres dat voor de sessie op *ASA 1* is gekozen verschillen van het adres dat voor de sessie op *ASA 2* is gekozen.

Configureren

In deze sectie wordt beschreven hoe u de TCP-statelijke omzeilingfunctie kunt configureren op Cisco ASA 5500 Series adaptieve security applicatie (ASA).

Configuratie van TCP-statelijke omzeilingsfuncties

Voltooi deze stappen om de optie TCP-state bypass te configureren op de Cisco ASA 5500 Series adaptieve security applicatie:

1. Gebruik de opdracht class-map class_map_name **om een** *class map* te maken. De class map wordt gebruikt om het verkeer te identificeren waarvoor u stateful firewall-inspectie wilt uitschakelen. De class map die gebruikt wordt in dit voorbeeld is *tcp_bypass*.
   ```
   ASA(config)#class-map tcp_bypass
   ```

2. Gebruik de opdracht match parameter **om interessant verkeer in de class map op te geven.** Wanneer u het modulaire beleidskader gebruikt, gebruik de opdracht **matchen access-list** in class-map configuratie modus om een toegangslijst te gebruiken om verkeer te identificeren 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
   ```

   tcp_bypass is de naam van de toegangslijst die in dit voorbeeld gebruikt wordt. Raadpleeg het Identificeren van verkeer (Layer 3/4 Class Map) voor meer informatie over het specificeren van het interessante verkeer.
3. Gebruik de opdracht beleidsmap-map **om een beleidsplan toe te voegen of een beleidsplan (dat reeds aanwezig is) te bewerken dat de acties instelt die moeten worden ondernomen met het reeds gespecificeerde class map verkeer.** Wanneer u het modulaire Kader van het Beleid gebruikt, gebruik de **beleid-kaart** opdracht (zonder het type sleutelwoord) in mondiale configuratiewijze om acties aan verkeer toe te wijzen dat u met een Layer 3/4 class kaart (de class-map of class-map-type managementopdracht) hebt geïdentificeerd. In dit voorbeeld, is de beleidslijn *tcp_bypass_policy*:
   ```
   ASA(config-cmap)#policy-map tcp_bypass_policy
   ```

4. Gebruik de opdracht van de class **in beleid-kaart configuratie modus om de class map (***tcp_bypass*) die al aan de beleidsplan (*tcp_bypass_policy*) is toegevoegd, toe te wijzen waar 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
   ```

5. Gebruik de ingestelde verbinding met geavanceerde opties TCP-staat-bypass **opdracht in** class configuratie mode om de TCP-state bypass-functie in te schakelen. Deze opdracht werd ingevoerd in versie 8.2(1). De class configuratie mode is toegankelijk vanuit de policy-map configuratiemodus zoals in dit voorbeeld:
   ```
   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. Gebruik de service-**beleidsmap**_name [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. Gebruik de opdracht **Service-beleid** om een reeks beleid op een interface mogelijk te maken.**global** past de beleidskaart op alle interfaces toe, en **interface** past het beleid op één interface toe. Er is slechts één algemeen beleid toegestaan. Je kunt het mondiale beleid omzeilen op een interface door een dienstenbeleid op die interface toe te passen. U kunt slechts één beleidskaart op elke interface toepassen.

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

Hier is een voorbeeldconfiguratie voor TCP state bypass:

```
!--- Configure the access list to specify the TCP traffic !--- that needs to by-pass inspection
to improve the performance. ASA(config)#access-list tcp_bypass extended permit tcp 10.1.1.0
255.255.255.224 any

!--- 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 outside

ASA(config-pmap-c)#static (inside,outside) 192.168.1.224 10.1.1.0 netmask
255.255.255.224
```

Verifiëren

De opdracht tonen **bevat** het aantal actieve TCP- en UDP-verbindingen en geeft informatie over verbindingen van verschillende typen. Om de verbindingsstaat voor het aangewezen connectietype te tonen, gebruik de show conn **opdracht in bevoorrechte EXEC modus.** Deze opdracht ondersteunt IPv4- en IPv6-adressen. De uitvoerweergave voor verbindingen die **TCP state bypass** gebruiken omvat de vlag **b**.

Problemen oplossen

Fout

ASA toont deze foutmelding zelfs nadat de TCP-staat-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
```

ICMP-pakketten zijn door het security apparaat verwijderd vanwege beveiligingscontroles die door de stateful ICMP-functie zijn toegevoegd, maar die meestal een ICMP-echo-reactie zijn zonder een geldig echo-verzoek dat al door het security apparaat is doorgegeven, of een ICMP-foutmelding die geen verband houdt met een TCP-, UDP- of ICMP-sessie die al in het security apparaat is ingesteld.

ASA geeft dit logbestand weer, zelfs als de TCP state bypass is ingeschakeld omdat het uitschakelen van deze functionaliteit (dat wil zeggen, het controleren van de ICMP return angen voor Type 3 in verbindingstabel) niet mogelijk is. Maar de TCP status bypass optie werkt correct.

Gebruik deze opdracht om te voorkomen dat deze berichten verschijnen:

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

Gerelateerde informatie

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