ASA 8.3: Connectiviteit met Cisco security applicatie vaststellen en oplossen

Inhoud

Inleiding

Wanneer een adaptieve security applicatie van Cisco (ASA) aanvankelijk is geconfigureerd, heeft deze een standaard beveiligingsbeleid waar iedereen aan de binnenkant uit kan komen en niemand van buiten erin kan krijgen. Als uw site een ander beveiligingsbeleid vereist, kunt u externe gebruikers toestaan om via de ASA verbinding te maken met uw webserver.

Zodra u basisconnectiviteit door de Cisco ASA installeert, kunt u configuratieveranderingen in de firewall aanbrengen. Zorg ervoor dat alle configuratiewijzigingen in de ASA in overeenstemming zijn met uw beveiligingsbeleid.

Raadpleeg PIX/ASA: Connectiviteit met Cisco security applicatie voor de oplossing van problemen voor de identieke configuratie op Cisco ASA met versies 8.2 en eerder.

Voorwaarden

Vereisten

Dit document gaat ervan uit dat bepaalde basisconfiguraties al zijn voltooid in Cisco ASA. Raadpleeg deze documenten voor voorbeelden van een eerste ASA-configuratie:

- ASA 8.3(x): Sluit één intern netwerk aan op internet
- De PPPoE-client configureren op een Cisco adaptieve security applicatie (ASA)

Gebruikte componenten

De informatie in dit document is gebaseerd op een Cisco adaptieve security applicatie (ASA) die versie 8.3 en hoger uitvoert.

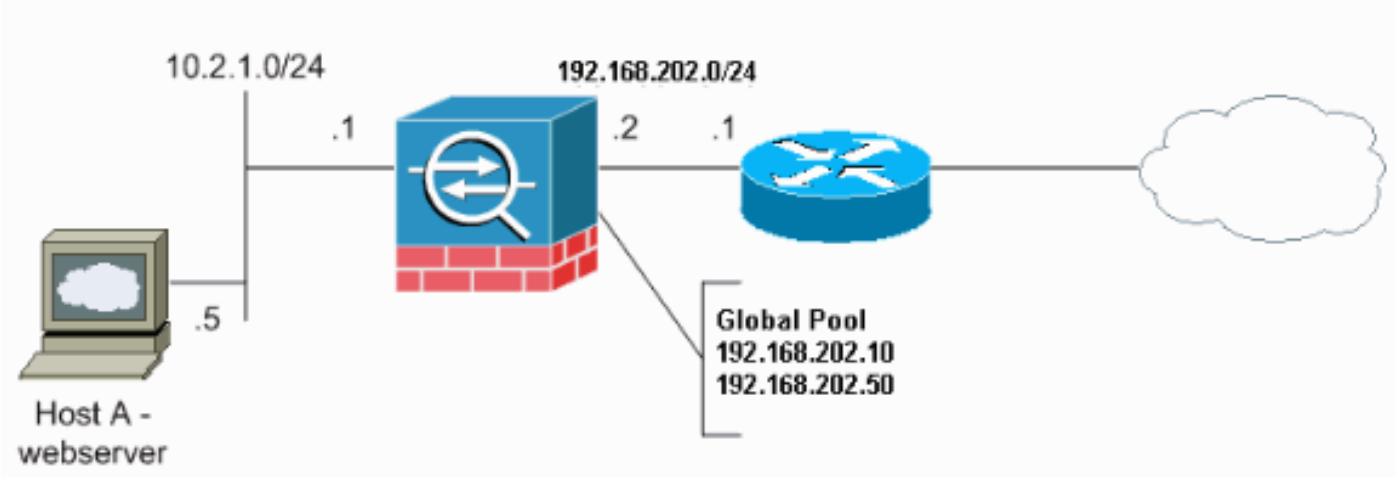
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

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

Hoe connectiviteit via de ASA-systemen werkt

In dit netwerk is Host A de webserver met een intern adres van 10.2.1.5. De webserver krijgt een extern (vertaald) adres van 192.168.202.5 toegewezen. Internetgebruikers moeten naar 192.168.202.5 wijzen om toegang te krijgen tot de webserver. De DNS-ingang voor uw webserver moet dat adres zijn. Er zijn geen andere verbindingen via het internet toegestaan.



Opmerking: de IP-adresseringsschema's die in deze configuratie worden gebruikt, zijn niet wettelijk routeerbaar op het internet. Het zijn RFC 1918 adressen die in een labomgeving gebruikt zijn.

Connectiviteit met Cisco ASA configureren

Voltooi deze stappen om connectiviteit met de ASA te configureren:

1. Maak een netwerkobject dat het interne net en een ander netwerkobject voor het IP-poolbereik definieert. Configureer de NAT met deze netwerkobjecten:

```
object network inside-net
subnet 0.0.0.0 0.0.0.0
object network outside-pat-pool
range 192.168.202.10 192.168.202.50
nat (inside,outside) source dynamic inside-net  outside-pat-pool
```

2. Toewijzen van een statisch vertaald adres voor de interne host waartoe internetgebruikers toegang hebben.

```
object network obj-10.2.1.5
  host 10.2.1.5
  nat (inside,outside) static 192.168.202.5
```

3. Gebruik de opdracht **toegangslijst** om externe gebruikers door de Cisco ASA toe te staan. Gebruik altijd het vertaalde adres in de opdracht **toegangslijst**.

```
access-list 101 permit tcp any host 192.168.202.5 eq www
  access-group 101 in interface outside
```

ARP-breedbandverkeer toestaan

Het security apparaat sluit hetzelfde netwerk aan op de binnen- en buitenkant van het apparaat. Omdat de firewall geen routed hop is, kunt u gemakkelijk een transparante firewall aan een bestaand netwerk introduceren. IP-adressering is niet nodig. IPv4-verkeer wordt automatisch via de transparante firewall toegestaan via een hogere beveiligingsinterface naar een lagere beveiligingsinterface zonder toegangslijst. Adresresoluties (ARP's) zijn toegestaan via de transparante firewall in beide richtingen zonder toegangslijst. ARP-verkeer kan worden geregeld door ARP-inspectie. Voor Layer 3 verkeer dat van een lage naar een hoge veiligheidsinterface reist, is een uitgebreide toegangslijst vereist.

Opmerking: het transparante mode security apparaat gaat niet via CDP-pakketten (Cisco Discovery Protocol) of IPv6-pakketten of pakketten die geen geldig EtherType hoger dan of gelijk aan 0x600 hebben. U kunt bijvoorbeeld geen IS-IS-pakketten overdragen. Er wordt een uitzondering gemaakt voor BPDU's (bridge Protocol Data Unit), die worden ondersteund.

Toegestaan MAC-adressen

Deze MAC-adressen van de bestemming zijn toegestaan door de transparante firewall. MAC-adressen die niet in deze lijst staan, worden niet meer vermeld:

- TRUE broadcast-MAC-adres, gelijk aan FFFF.FFFF.FFFF
- IPv4 multicast MAC-adressen van 100.5E00.000 tot 100.5EFE.FFFF
- IPv6 multicast MAC-adressen van 333.000.000 tot 333.FFFF.FFFF
- BPDU multicast adres, gelijk aan 100.0CCC.CCD
- AppleTalk multicast MAC-adressen van 0900.0700.000 tot 0900.07FF.FFFF

Verkeer toegestaan om niet in routermodus te passeren

In routermodus kunnen bepaalde typen verkeer niet door het security apparaat lopen, zelfs niet indien u het in een toegangslijst toestaat. De transparante firewall kan echter bijna elk verkeer toestaan door gebruik te maken van een uitgebreide toegangslijst (voor IP-verkeer) of een EtherType-toegangslijst (voor niet-IP-verkeer).

U kunt bijvoorbeeld routingnabijheden van protocollen maken door een transparante firewall. U

kunt Open Shortest Path First (OSPF), Routing Information Protocol (RIP), Enhanced Interior Gateway Routing Protocol (DHCP) of Border Gateway Protocol (BGP) doorsturen op basis van een uitgebreide toegangslijst. Op dezelfde manier kunnen protocollen zoals Hot Standby Router Protocol (HSRP) of Virtual Router Redundancy Protocol (VRRP) door het security apparaat lopen.

Niet-IP verkeer (bijvoorbeeld AppleTalk, IPX, BPDU's en MPLS) kan worden geconfigureerd om door te gaan in het gebruik van een EtherType-toegangslijst.

Voor functies die niet direct op de transparante firewall worden ondersteund, kunt u verkeer toestaan om door te gaan zodat upstream- en downstreamrouters de functionaliteit kunnen ondersteunen. Door een uitgebreide toegangslijst te gebruiken, kunt u bijvoorbeeld het verkeer van Dynamic Host Configuration Protocol (DHCP) (in plaats van de niet-ondersteunde DHCP-relais) of het multicastverkeer toestaan zoals dat wordt gecreëerd door IP/TV.

Problemen oplossen

Als internetgebruikers geen toegang hebben tot uw website, Voltooi de volgende stappen:

1. Zorg ervoor dat u de configuratieadressen correct hebt ingevoerd:Geldig extern adresCorrect intern adresExterne DNS heeft een vertaald adres
2. Controleer de externe interface op fouten.Cisco security applicatie is vooraf ingesteld om de snelheid en duplexinstellingen op een interface automatisch te detecteren. Er bestaan echter verschillende situaties die ervoor kunnen zorgen dat het automatische onderhandelingsproces mislukt. Dit resulteert in onjuistheden of dubbele onjuistheden (en prestatiekwesties). Voor missie-kritieke netwerkinfrastructuur, codeert Cisco handmatig de snelheid en de duplex op elke interface zodat er geen kans op een fout is. Deze apparaten bewegen over het algemeen niet rond. Daarom moet u, als u ze correct configureren, ze niet wijzigen.**Voorbeeld:**
```
asa(config)#interface ethernet 0/0
asa(config-if)#duplex full
asa(config-if)#speed 100
asa(config-if)#exit
```

   In bepaalde situaties, leidt het hardcoderen van de snelheid en de duplexinstellingen tot het genereren van fouten. Om deze reden moet u de interface met de standaardinstelling van de auto-detectiemodus configureren zoals dit voorbeeld laat zien:**Voorbeeld:**
```
asa(config)#interface ethernet 0/0
asa(config-if)#duplex auto
asa(config-if)#speed auto
asa(config-if)#exit
```

3. Als het verkeer niet door de interface van de ASA of de head-end router stuurt of ontvangt, probeer dan de ARP statistieken te wissen.
```
asa#clear arp
```

4. Gebruik het **tonen run object** en **tonen statische** opdrachten om er zeker van te zijn dat statische vertaling is ingeschakeld.**Voorbeeld:**

```
object service www
service tcp source eq www
object network 192.168.202.2
host 192.168.202.2
```

```
object network 10.2.1.5
host 10.2.1.5
object service 1025
service tcp source eq 1025
nat (inside,outside) source static 10.2.1.5 192.168.202.2 service 1025 www
```

In dit scenario wordt het externe IP-adres gebruikt als het in kaart gebrachte IP-adres voor de webserver.

```
nat (inside,outside) source dynamic 10.2.1.5 interface service 1025 www
```

5. Controleer of de standaardroute op de webserver op de interne interface van de ASA wijst.
6. Controleer de vertaaltabel met behulp van de opdracht **Show** Exlate om te zien of de vertaling gemaakt is.
7. Gebruik de **gebufferde** opdracht **houtkap** om de logbestanden te controleren om te zien of er ontkenningen voorkomen. (Kijk naar het vertaalde adres en controleer of u eventuele ontkenningen ziet.)
8. Gebruik de opdracht **Opnemen**:

```
access-list webtraffic permit tcp any host 192.168.202.5

capture capture1 access-list webtraffic interface outside
```

Opmerking: deze opdracht genereert een aanzienlijke hoeveelheid output. Het kan een router veroorzaken om onder zware verkeersladingen te hangen of te herladen.

9. Als pakketten het aan de ASA maken, zorg er dan voor dat uw route naar de webserver van de ASA correct is. (Controleer de routeopdrachten in uw ASA-configuratie.)
10. Controleer of proxy-ARP is uitgeschakeld. Geef het **show in werking stellen-in-stellingssysteem opdracht in ASA 8.3 uit.**Hier, proxy ARP is uitgeschakeld door de **sysopt noproxyarp buiten** opdracht:

```
ciscoasa#show running-config sysopt
no sysopt connection timewait
sysopt connection tcpmss 1380
sysopt connection tcpmss minimum 0
no sysopt nodnsalias inbound
no sysopt nodnsalias outbound
no sysopt radius ignore-secret
sysopt noproxyarp outside
sysopt connection permit-vpn
```

Om proxy ARP opnieuw in te schakelen voert u deze opdracht in de mondiale configuratiemodus:

```
ciscoasa(config)#no sysopt noproxyarp outside
```

Wanneer een host IP-verkeer naar een ander apparaat op hetzelfde Ethernet-netwerk stuurt, moet de host het MAC-adres van het apparaat kennen. ARP is een Layer 2-protocol dat een IP-adres naar een MAC-adres oplost. Een host stuurt een ARP-aanvraag en vraagt "Wie is dit IP-adres?" Het apparaat dat het IP-adres bezit antwoordt, "Ik bezit dat IP-adres; Hier is mijn MAC-adres."Proxy ARP stelt het security apparaat in staat om op een ARP-verzoek te antwoorden namens hosts achter het scherm. Dit gebeurt door op ARP verzoeken om de statische in kaart gebrachte adressen van die hosts te antwoorden. Het security apparaat reageert op het verzoek met zijn eigen MAC-adres en stuurt de IP-pakketten naar de juiste binnenhost.In het diagram in dit document, bijvoorbeeld, wanneer

een ARP-verzoek wordt ingediend voor het globale IP-adres van de webserver, 192.168.202.5, reageert het security apparaat met zijn eigen MAC-adres. Als proxy-ARP in deze situatie niet is ingeschakeld, kunnen hosts op het externe netwerk van het security apparaat niet de webserver bereiken door een ARP-verzoek op te geven voor adres 192.168.202.5. Raadpleeg de opdrachtreferentie voor meer informatie over de sysopt-opdracht.

11. Als alles correct lijkt te zijn en de gebruikers nog steeds geen toegang tot de webserver hebben, kunt u een case openen met Cisco Technical Support.

Foutbericht - %ASA-4-07001:

Een paar hosts geen verbinding kunnen maken met het internet en de `foutmelding - %ASA-4-407001: Deny traffic for local-host interface_name:binnenkant_address, licentielimiet van aantal overschreden` foutmelding wordt in de syslog ontvangen. Hoe is deze fout opgelost?

Deze foutmelding wordt ontvangen wanneer het aantal gebruikers de gebruikerslimiet van de licentie overschrijdt. upgrade van de licentie naar een hoger aantal gebruikers om deze fout op te lossen. Dit kan een 50, 100 of onbeperkte gebruikerslicentie zijn, zoals vereist.

Gerelateerde informatie

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