ASA heeft een hoge CPU-gebruik door een verkeerslijn wanneer VPN-clients worden losgekoppeld

Inhoud

Inleiding

Dit document beschrijft een veelvoorkomend probleem dat zich voordoet wanneer VPN-clients de verbinding verbroken hebben met een Cisco adaptieve security applicatie (ASA) die werkt als een head-end head-end externe toegang van VPN. Dit document beschrijft ook de situatie waarin een verkeerslijn optreedt wanneer VPN-gebruikers de verbinding met een ASA-firewall verbroken hebben. Dit document beslaat niet de manier waarop u externe toegang tot VPN kunt configureren of instellen, alleen de specifieke situatie die voortvloeit uit bepaalde gemeenschappelijke routingconfiguraties.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Remote Access VPN-configuratie voor ASA
- Basis Layer 3-routing

Gebruikte componenten

De informatie in dit document is gebaseerd op een ASA model 5520 met ASA-code versie 9.1(1).

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.

Verwante producten

Dit document kan met deze hardware- en softwareversies worden gebruikt:

- Elk ASA-model
- Elke ASA-codversie

Achtergrondinformatie

Wanneer een gebruiker op ASA als een externe VPN-concentrator aan de ASA verbindt, installeert de ASA een op host gebaseerde route in de ASA-routingtabel die het verkeer naar die VPN-client vanuit de externe interface (naar het internet) routeert. Wanneer die gebruiker de verbinding verbreekt, wordt de route uit de tabel verwijderd en kunnen de pakketten op het binnennetwerk (bestemd voor die niet-aangesloten VPN-gebruiker) tussen de ASA en een intern routingapparaat lopen.

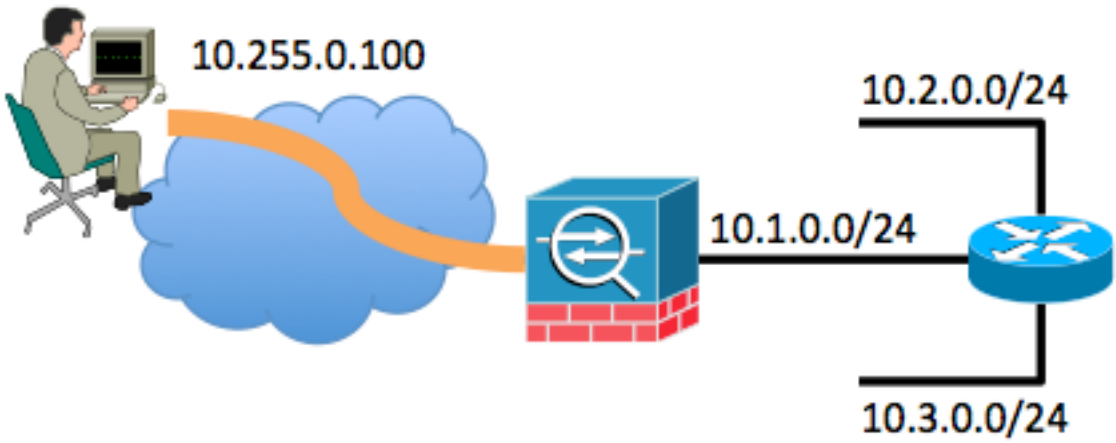
Een ander probleem is dat de geregisseerde (netwerk) uitzendingspakketten (die door de verwijdering van de VPN-clients worden gegenereerd) door de ASA als een unicastframe naar het interne netwerk kunnen worden doorgestuurd. Dit zou het terug naar de ASA kunnen doorsturen, wat ervoor zorgt dat het pakje van een loopje wordt voorzien tot de Tijd om te leven (TTL) verstrijkt.

Dit document legt deze problemen uit en toont welke configuratietechnieken kunnen worden gebruikt om het probleem te voorkomen.

Probleem: Packet bedoeld voor een los VPN-clientlaag binnen het interne netwerk

Wanneer een gebruiker van VPN-toegang op afstand een ASA-firewall ontkoppelt, zijn de pakketten nog steeds aanwezig op het interne netwerk (bestemd voor de niet-verbonden gebruikers) en het toegewezen IP VPN-adres kan binnen het interne netwerk van een netwerk worden voorzien. Deze pakketlijnen kunnen het CPU-gebruik in de ASA doen toenemen tot de lus stopt met ofwel de IP TTL-waarde in de IP-pakketheader-decreatie naar 0, of de gebruiker herverbindt en het IP-adres wordt opnieuw toegewezen aan een VPN-client.

Om dit scenario beter te begrijpen, overweeg deze topologie:



In dit voorbeeld is de externe toegangsclient toegewezen aan het IP-adres van 10.255.0.100. De ASA in dit voorbeeld is verbonden met het zelfde binnen netwerk segment samen met een router. De router heeft twee extra Layer 3 netwerksegmenten die ermee zijn verbonden. De relevante interface (routing) en VPN-configuraties van de ASA en router worden in de voorbeelden weergegeven.

ASA configuratie-hoogtepunten worden in dit voorbeeld getoond:

```
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 198.51.100.100 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.1.0.1 255.255.255.0
!
same-security-traffic permit intra-interface
!
ip local pool VPNpool 10.255.0.1-10.255.0.255
!
route outside 0.0.0.0 0.0.0.0 198.51.100.1
route inside 10.0.0.0 255.0.0.0 10.1.0.2
```

De hoogtepunten van de routerconfiguratie worden in dit voorbeeld getoond:

```
interface FastEthernet0
description connected to the inside interface of the ASA G0/1
ip address 10.1.0.2 255.255.255.0
!
interface FastEthernet1
 description connected to network segment
 ip address 10.2.0.1 255.255.255.0
!
interface FastEthernet2
 description connected to other network segment
 ip address 10.3.0.1 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 10.1.0.1
```

De routingtabel van de router die op de binnenkant van de ASA is aangesloten heeft eenvoudigweg een standaardroute die op de ASA binneninterface van 10.1.0.1 is gericht.

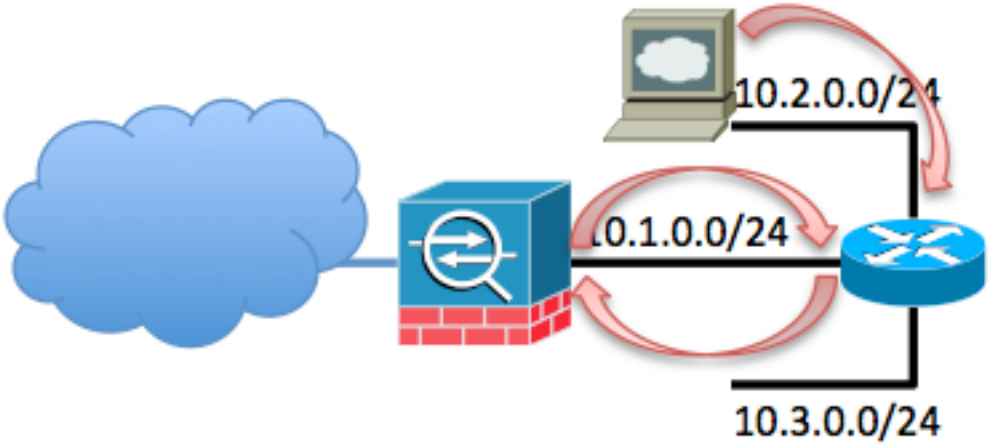
Terwijl de gebruiker via VPN op de ASA-routingtabel wordt aangesloten, toont de ASA-routingtabel als volgt:

```
ASA# show route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is 198.51.100.1 to network 0.0.0.0
S 10.255.0.100 255.255.255.255 [1/0] via 198.51.100.1, outside
S 10.0.0.0 255.0.0.0 [1/0] via 10.1.0.2, inside
C 198.51.100.0 255.255.255.0 is directly connected, outside
C 10.1.0.0 255.255.255.0 is directly connected, inside
S* 0.0.0.0 0.0.0.0 [1/0] via 198.51.100.1, outside
```

Het probleem doet zich voor wanneer de VPN-gebruiker van de externe toegang de VPN-verbinding verbreekt. Op dit punt wordt de op host gebaseerde route verwijderd van de ASA routingtabel. Als een host binnen het netwerk probeert verkeer naar de VPN-client te verzenden, wordt dat verkeer door de router naar de ASA-binneninterface routeerd. Deze serie stappen komt voor:

1. Het pakket dat is bestemd voor 10.255.0.100 wordt geleverd op de interne interface van de ASA.
2. Standaard ACL-controles worden uitgevoerd.
3. De ASA routing table wordt gecontroleerd om de spanning-interface voor dit verkeer te bepalen.
4. De bestemming van het pakket past de brede 10.0.0.0/8 route aan die uit de interne interface naar de router wijst.
5. De ASA controleert of het verkeer met haarspelden is toegestaan - hij zoekt naar **de veilige intra-interface** en stelt vast dat dit is toegestaan.
6. Een verbinding wordt van en naar de binneninterface gemaakt en het pakket wordt naar de router teruggestuurd als volgende hop.
7. De router ontvangt een pakket dat voor 10.255.0.100 is bestemd op de interface die met de ASA wordt geconfronteerd. De router controleert zijn routingtabel voor een geschikte volgende hop. De router vindt dat de volgende hop de ASA binneninterface zou zijn, en het pakje wordt naar de ASA verzonden.
8. Ga terug naar stap 1.

Hier wordt een voorbeeld getoond:



Deze lus treedt op tot de TTL van dit pakket stappen tot 0. Let op dat de ASA Firewall de TTL-waarde **niet** standaard **bepaalt** wanneer het een pakje verwerkt. De router neemt de TTL af terwijl het het pakje leidt. Dit voorkomt het voorkomen van deze lus voor onbepaalde tijd, maar deze lijn verhoogt de verkeersbelasting op de ASA en veroorzaakt het gebruik van CPU om te pieken.

Probleem: GERICHT (netwerk) broadcast-pakketten die door VPN-clients zijn gegenereerd, zijn geladen op een binnen netwerk

Deze kwestie lijkt op het eerste probleem. Als een VPN-client een geregisseerd broadcast-pakket genereert naar zijn toegewezen IP-subtype (10.255.0.255 in het vorige voorbeeld), dan kan dat pakket door de ASA naar de interne router worden doorgestuurd als een unicastframe. De binnenrouter kan het dan terugsturen naar de ASA, die het pakket veroorzaakt om te lus tot de TTL verlopen.

Deze serie gebeurtenissen komt voor:

1. De VPN clientmachine genereert een pakje dat is bestemd voor het netwerkadres 10.255.0.255 en het pakje komt in de ASA aan.
2. ASA behandelt dit pakje als een enkel frame (door de routingtabel) en stuurt het naar de binnenrouter.

3. De binnenrouter, die het pakket ook als een unicastframe behandelt, beslist de TTL van het pakket en zendt het terug naar de ASA.

4. Het proces wordt herhaald totdat de TTL van het pakket tot 0 wordt verminderd.

Oplossingen voor het probleem

Er zijn verschillende mogelijke oplossingen voor deze kwestie. Afhankelijk van de netwerktopologie en de specifieke situatie, zou één oplossing gemakkelijker te implementeren kunnen zijn dan een andere.

Oplossing 1-Statische route voor Null0-interface (ASA versie 9.2.1 en hoger)

Wanneer u verkeer naar een **Null0-**interface stuurt, worden de pakketten die bestemd zijn voor het gespecificeerde netwerk, verbroken. Deze optie is handig wanneer u op afstand geactiveerd Zwart gat (RTBH) voor Border Gateway Protocol (BGP) vormt. In deze situatie, als u een route naar Null0 voor het netwerk van de afstandstoegangsclient vormt, dwingt dit de ASA om verkeer te laten vallen dat bestemd is voor hosts in dat netwerk als er geen specifiekere route (voorzien door omgekeerde routeinjectie) aanwezig is.

```
route Null0 10.255.0.0 255.255.255.0
```

Oplossing 2 - Gebruik een andere IP-pool voor VPN-clients

Deze oplossing is om de verre gebruikers van VPN een IP adres toe te wijzen dat niet met interne netwerkverkenner overlapt. Dit zou voorkomen dat de ASA pakketten die bestemd zijn voor dat VPN-net terugsturen naar de binnenrouter als de VPN-gebruiker niet was verbonden.

Oplossing 3 - Maak de ASA-routingtabel specifieker voor interne routers

Deze oplossing is om te verzekeren de routingtabel van de ASA geen zeer brede routes heeft die met de VPN IP pool overlapt. Voor dit specifieke netwerkvoorbeeld, verwijder de 10.0.0.0/8 route van de ASA en vorm meer specifieke statische routes voor de subnetten die van de binneninterface wonen. Afhankelijk van het aantal subnetten en de topologie van het netwerk, zou dit een groot aantal statische routes kunnen zijn en het zou niet mogelijk kunnen zijn.

Oplossing 4 - Voeg een specifiekere route voor het VPN-subnet terug uit de externe interface toe

Deze oplossing is gecompliceerder dan de andere in dit document beschreven oplossingen. Cisco raadt u aan om de andere oplossingen eerst te gebruiken vanwege de situatie die in de Opmerking later in deze sectie wordt beschreven. Deze oplossing is om te voorkomen dat de ASA IP-pakketten die van VPN IP-SUBNET zijn afgeleid, naar de interne router doorstuurt; U kunt dit doen als u een specifiekere route voor VPN-subnet uit de externe interface toevoegt. Aangezien deze IP-telefoon is gereserveerd voor externe VPN-gebruikers, moeten IP-pakketten met een bronadres uit dit VPN-subprogramma nooit binnenkomend op de ASA-binneninterface aankomen. De makkelijkste manier om dit te bereiken is een route voor de externe toegang VPN IP-pool uit de externe interface met een volgende hop-IP-adres van de upstream ISP-router toe te voegen.

In dit voorbeeld van de netwerktopologie zou die route er als volgt uitzien:

```
route outside 10.255.0.0 255.255.255.0 198.51.100.1
```

Naast deze route, voeg het **IP verify-pad in** opdracht toe om de ASA te veroorzaken om binnenkomende pakketten op de interne interface die van VPN IP-subnet zijn afgeleid te laten vallen vanwege de meer geprefereerde route die op de externe interface bestaat:

```
ip verify reverse-path inside
```

Nadat deze opdrachten zijn geïmplementeerd, ziet de ASA-routingtabel er precies zo uit als bij de gebruiker:

```
ASA# show route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 198.51.100.1 to network 0.0.0.0

S 10.255.0.100 255.255.255.255 [1/0] via 198.51.100.1, outside
S 10.0.0.0 255.0.0.0 [1/0] via 10.1.0.2, inside
S 10.255.0.0 255.255.255.0 [1/0] via 198.51.100.1, outside
C 198.51.100.0 255.255.255.0 is directly connected, outside
C 10.1.0.0 255.255.255.0 is directly connected, inside
S* 0.0.0.0 0.0.0.0 [1/0] via 198.51.100.1, outside
```

Wanneer de VPN-client is aangesloten, is de op host gebaseerde route naar dat VPN IP-adres aanwezig in de tabel en heeft de voorkeur. Wanneer de VPN-client wordt afgesloten, wordt het verkeer dat afkomstig is van dat client-IP-adres dat op de interne interface aankomt, gecontroleerd tegen de routingtabel en gevallen vanwege de **ip verify-pad binnen de** opdracht.

Als de VPN-client een geregisseerde netwerkuitzending naar VPN IP-telefoon genereert, dan wordt dat pakket naar de interne router verzonden en door de router teruggestuurd naar de ASA, waar het is gevallen door de **ip verify-pad in** opdracht.

> Opmerking: Nadat deze oplossing is geïmplementeerd, als de opdracht voor **dezelfde beveiligingslicentie binnen-interface** aanwezig is in de configuratie en het toegangsbeleid deze, kan verkeer dat is afkomstig van een VPN-gebruiker die is bestemd voor een IP-adres in de VPN IP-pool voor een gebruiker die geen verbinding heeft, in duidelijke tekst uit de externe interface worden teruggeleid. Dit is een zeldzame situatie en kan worden verzacht door het gebruik van VPN-filters binnen het VPN-beleid. Deze situatie doet zich alleen voor als de opdracht **voor** het **instellen van de ASA**-interface met **dezelfde beveiliging** aanwezig is.
>
> Op dezelfde manier, als interne hosts verkeer genereren dat bestemd is voor een IP-adres in de VPN-pool en dat IP-adres niet is toegewezen aan een externe VPN-gebruiker, kan dat verkeer de buitenkant van de ASA in duidelijk-tekst bereiken.