Begrijp Crypto ACL-tellers binnen op beleid gebaseerde VPN-tunnels

Inhoud

Inleiding

Dit document beschrijft het gedrag van tellers van de crypto-toegangscontrolelijst (ACL) binnen op beleid gebaseerde VPN-tunnels.

Voorwaarden

Vereisten

Cisco raadt kennis van deze onderwerpen aan:

- Op beleid gebaseerde site-to-site VPN op Cisco IOS®/Cisco IOS® XE-platform
- Toegangscontrolelijsten op Cisco IOS/Cisco IOS XE-platform

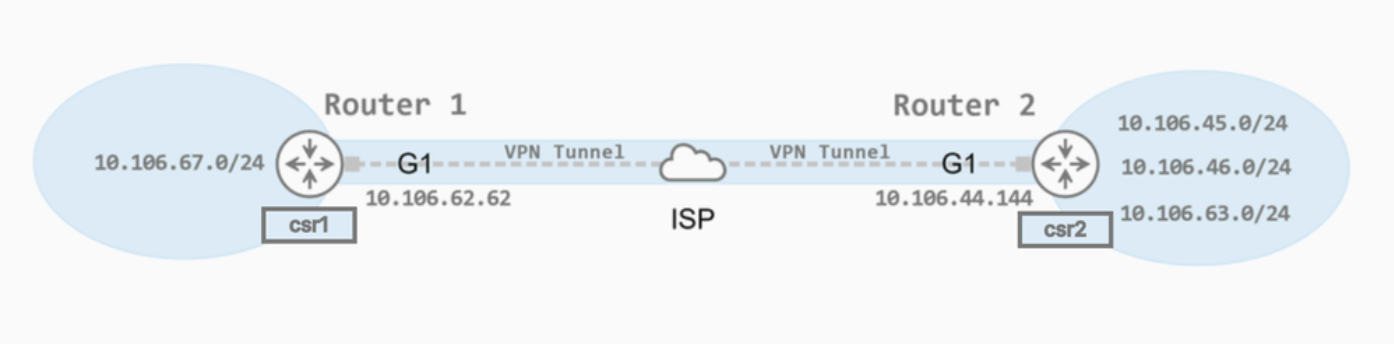
Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco C8kv, versie 17.12.04(MD)

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 zorgen dat u de potentiële impact van elke opdracht begrijpt.

Topologie



Topologie

Scenario's

Door twee verschillende scenario's te bekijken, proberen we te begrijpen hoe ACL-treffers worden beïnvloed wanneer verkeer wordt geïnitieerd vanuit verschillende peers en wanneer tunnels worden gereset.

1. Scenario één: Verkeer geïnitieerd vanaf router 1 terwijl de VPN-tunnel inactief is

   In dit scenario worden de wijzigingen in ACL-hit tellingen geanalyseerd wanneer de VPN-tunnel aanvankelijk is ingedrukt en wordt verkeer gestart vanaf router 1. Deze analyse helpt de eerste installatie te begrijpen en hoe de crypto ACL-tellers reageren op de eerste poging tot verkeersdoorstroming.

2. Scenario twee: Verkeer geïnitieerd vanuit router2 terwijl de VPN-tunnel actief is

   In dit scenario is de VPN-tunnel al tot stand gebracht en wordt het verkeer vanaf router2 verkend. Dit scenario biedt inzichten in hoe ACL-tellers zich gedragen wanneer de tunnel actief is en er verkeer wordt geïntroduceerd vanuit een andere peer.

Door deze scenario's te vergelijken, kunnen we een uitgebreid begrip van de dynamiek van ACL-tellers in VPN-tunnels onder verschillende omstandigheden verkrijgen.

Configuratie

We hebben een op beleid gebaseerde site-to-site VPN-tunnel geconfigureerd tussen twee Cisco

C8kv-routers, aangeduid als peers. Router1 wordt "csr1" genoemd en router2 wordt "csr2" genoemd.

Crypto configuratie op router1

```
csr1#sh ip int br
Interface              IP-Address      OK?   Method   Status  Protocol
GigabitEthernet1       10.106.62.62    YES   NVRAM    up      up
GigabitEthernet2       10.106.67.27    YES   NVRAM    up      up
```

```
csr1#sh run | sec crypto map
crypto map nigarapa_map 100 ipsec-isakmp
   set peer 10.106.44.144
   set transform-set new_ts
   set ikev2-profile new_profile
   match address new_acl
```

```
csr1#sh ip access-lists new_acl
Extended IP access list new_acl
   10 permit ip 10.106.67.0 0.0.0.255 10.106.45.0 0.0.0.255 log
   20 permit ip 10.106.67.0 0.0.0.255 10.106.46.0 0.0.0.255
   30 permit ip 10.106.67.0 0.0.0.255 10.106.63.0 0.0.0.255 log
```

```
csr1#sh run int GigabitEthernet1
Building configuration...

Current configuration : 162 bytes
!
interface GigabitEthernet1
ip address 10.106.62.62 255.255.255.0
ip nat outside
negotiation auto
no mop enabled
no mop sysid
crypto map nigarapa_map
end
```

Crypto configuratie op router2

```
csr2#sh ip int br
Interface              IP-Address        OK?     Method       Status     Protocol
GigabitEthernet1       10.106.44.144     YES     NVRAM        up         up
GigabitEthernet2       10.106.45.145     YES     NVRAM        up         up
GigabitEthernet3       10.106.46.146     YES     NVRAM        up         up
```

```
GigabitEthernet4      10.106.63.13      YES      NVRAM        up          up
```

```
csr2#sh run | sec crypto map
crypto map nigarapa_map 100 ipsec-isakmp
   set peer 10.106.62.62
   set transform-set new_ts
   set ikev2-profile new_profile
   match address new_acl
```

```
csr2#sh ip access-lists new_acl
Extended IP access list new_acl
   10 permit ip 10.106.45.0 0.0.0.255 10.106.67.0 0.0.0.255
   20 permit ip 10.106.46.0 0.0.0.255 10.106.67.0 0.0.0.255
   30 permit ip 10.106.63.0 0.0.0.255 10.106.67.0 0.0.0.255
```

```
csr2#sh run int GigabitEthernet1
Building configuration...

Current configuration : 163 bytes
!
interface GigabitEthernet1
ip address 10.106.44.144 255.255.255.0
ip nat outside
negotiation auto
no mop enabled
no mop sysid
crypto map nigarapa_map
end
```

Gedragsanalyse van tellers van crypto-toegangscontrolelijsten binnen VPN-tunnels

Aanvankelijk, hebben beide apparaten een ACL klaptelling van nul op hun respectieve crypto toegangslijsten.

Access Control List slaat op het aantal nul op hun respectieve cryptotoegangslijsten op beide peer-apparaten.

Scenario één: Verkeer geïnitieerd vanaf router 1 terwijl de VPN-tunnel inactief is

Begintoestand:

De VPN-tunnel die router1 (IP: 10.106.67.27) en router2 (IP: 10.106.45.145) is momenteel niet actief.

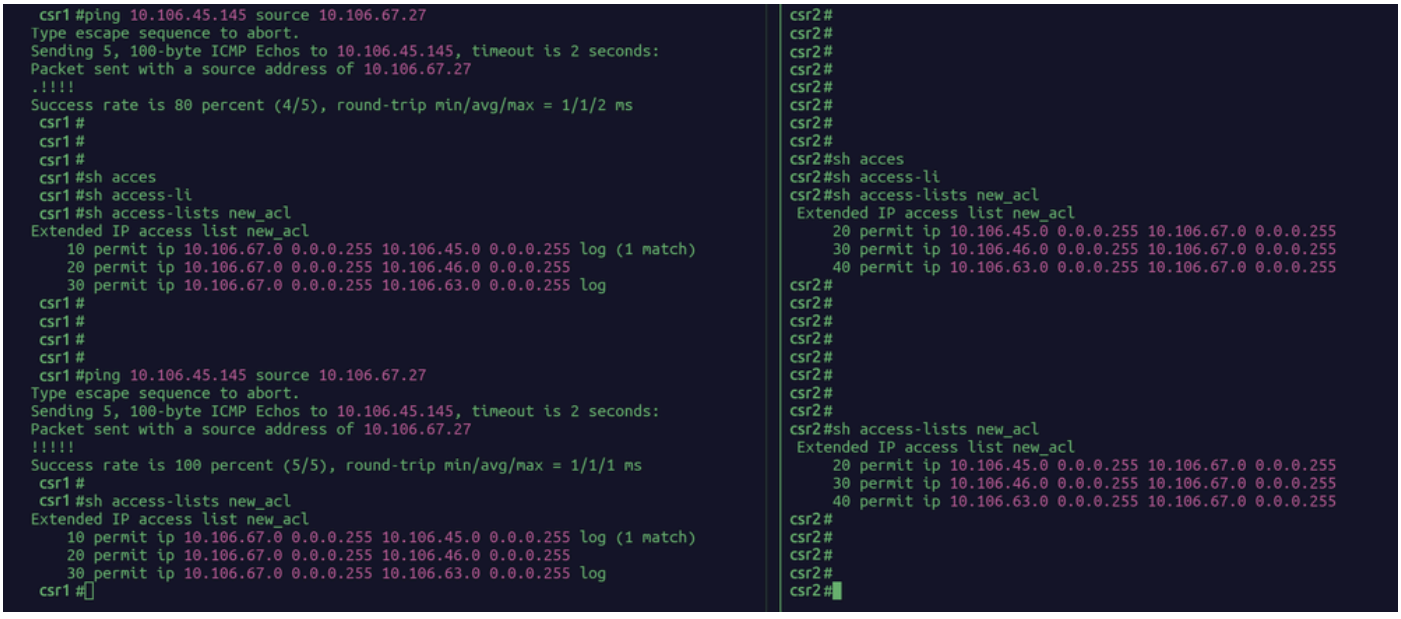
Genomen maatregelen:

Het verkeer wordt geïnitieerd vanaf router1, bedoeld om communicatie met router2 tot stand te brengen.

Opmerkingen:

1. ACL-tellergedrag:
   a. Op het initiëren van verkeer van Router1, is er een merkbare toename in de teller van de Toegangscontrolelijst (ACL) op Router1. Deze verhoging komt slechts eenmaal voor op het ogenblik dat de tunnel probeert te vestigen.
   b. De stijging in de ACL-teller wordt exclusief waargenomen op de initiërende router, die in dit scenario Router1 is. Router2 weerspiegelt geen veranderingen in zijn ACL teller op dit stadium.
2. Tunnelinstallatie:
   a. Na de aanvankelijke verhoging die aan de verkeersinitiatie beantwoordt, vestigt de tunnel tussen eerste en Router2 met succes.
   b. Na de installatie van de tunnel stabiliseert de ACL-teller op router1 en toont geen verdere stappen, wat aangeeft dat de ACL-regel is aangepast en dat er nu consistent verkeer door de ingestelde tunnel wordt toegestaan.
3. Tunnelherstart:
   De ACL-teller op Router1 ervaart alleen een andere toename als de tunnel daalt en opnieuw moet worden ingesteld. Dit suggereert dat de ACL-regel wordt geactiveerd door de eerste verkeersinitiatie die probeert om de tunnel te vestigen, in plaats van door doorlopende gegevensoverdracht zodra de tunnel actief is.

Samengevat, toont dit scenario aan dat de ACL-teller op Router1 gevoelig is voor de eerste verkeerspogingen voor tunnelcreatie maar statisch blijft zodra de VPN-tunnel is geopend en operationeel is.



Scenario twee:verkeer geïnitieerd vanuit router2 terwijl de VPN-tunnel actief is

Begintoestand:

De VPN-tunnel die router1 (IP: 10.106.67.27) en router2 (IP: 10.106.45.145) is momenteel actief en operationeel.

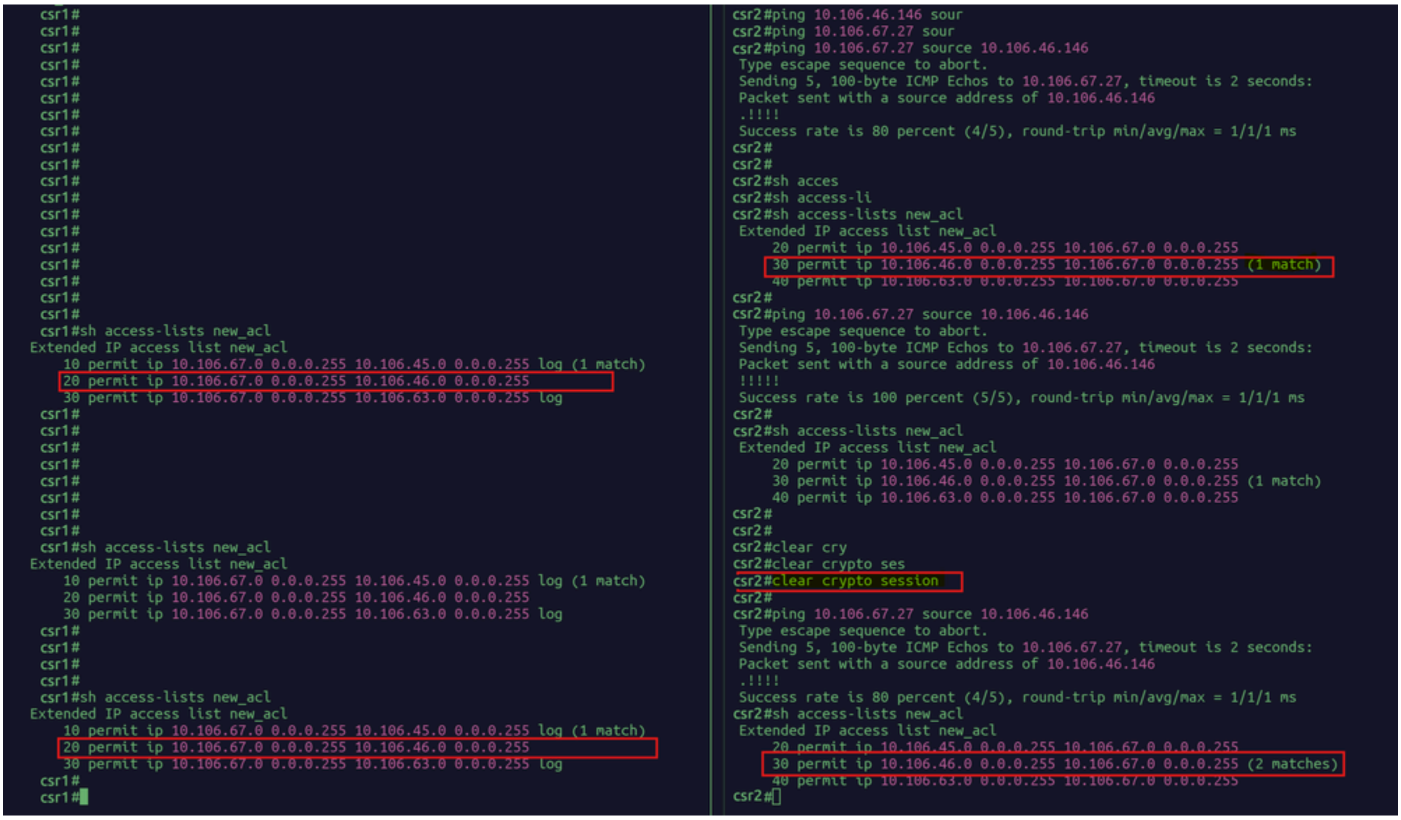
Genomen maatregelen:

1. Het verkeer wordt geïnitieerd van router2 naar router1 terwijl de tunnel omhoog is.
2. Vervolgens wordt de tunnel doelbewust ontruimd (of gereset).
3. Nadat de tunnel is gewist, start Router2 opnieuw verkeer om de verbinding opnieuw tot stand te brengen.

Opmerkingen:

1. Eerste verkeersinitiatie:
   a. Wanneer het verkeer voor het eerst wordt geïnitieerd vanaf router2 terwijl de tunnel al is opgezet, is er geen onmiddellijke wijziging in de teller van de toegangscontrolelijst (ACL).
   b. Dit geeft aan dat doorlopend verkeer binnen een reeds ingestelde tunnel niet leidt tot de toename van de ACL-teller.
2. Tunnelreiniging en herstart:
   a. Op het ontruimen van de tunnel, wordt de gevestigde verbinding tussen eerste en Router2 tijdelijk onderbroken. Dit vereist een herstelproces voor alle daaropvolgende verkeer.
   b. Wanneer het verkeer opnieuw wordt geïnitieerd van router2 nadat de tunnel is ontruimd, is er een waarneembare toename in de ACL-teller op router2. Deze toename betekent dat de ACL-regels opnieuw worden ingeschakeld om de vorming van de tunnel te vergemakkelijken.
3. Specificiteit ACL-teller:
   De toename in de ACL-teller vindt alleen plaats aan de kant die het verkeer initieert, wat in dit geval router2 is. Dit gedrag benadrukt de rol van de ACL bij het bewaken en controleren van processen voor verkeersinitiatie aan de kant van oorsprong, terwijl de ACL-teller van router 1 onaangetast blijft tijdens deze fase.

Samengevat, illustreert dit scenario dat de ACL-teller op Router2 op de initiatie van verkeer reageert wanneer u een VPN-tunnel opnieuw installeert. De teller stijgt niet met regelmatige verkeersstroom binnen een actieve tunnel, maar reageert op de behoefte aan het herstel van de tunnel, waardoor een nauwkeurige opvolging van tunnelinitiatiegebeurtenissen wordt verzekerd.



Scenario 2

Conclusie:

Het gedrag van de crypto ACL tellers onthult dat zij klaptellingen registreren uitsluitend tijdens de initiatieffase van de VPN-tunnel.

Initiatorspecifieke verhoging: Wanneer de tunnel van Router1 in werking wordt gesteld, wordt de verhoging van de klaptelling waargenomen alleen op Router1. Op dezelfde manier als de initiatie van Router2 voorkomt, stijgt de klaptelling slechts op Router2. Dit benadrukt de rol van ACL in de controle van het proces van de verkeersinitiatie bij de bron.

Stabiliteit na vestiging: Zodra de tunnel met succes wordt gevestigd, blijven de ACL-tellers op beide peers onveranderd, wat op geen verdere hits wijst. Deze stabiliteit blijft bestaan tot de tunnel of ontruimd of teruggesteld wordt, en de verkeersinitiatie wordt opnieuw geprobeerd.
Dit gedrag onderstreept de functionaliteit van toegangscontrolelijsten in het volgen en controleren van de eerste fase van tunnelcreatie, ervoor zorgend dat de volgende gegevensstroom binnen de gevestigde tunnel de klaptellingen niet beïnvloedt.

Belangrijkste afhaalpunten:

ACL-tellergedrag: De ACL-tellers registreren toename uitsluitend aan de initiatorkant tijdens het tunnelinitiatieproces. Dit geeft aan dat de tellers zijn ontworpen om het initiële verkeer dat de tunnelvestiging activeert te bewaken.

Statische tellers na vestiging: Zodra de tunnel actief en gevestigd is, blijven de ACL-tellers ongewijzigd. Zij wijzen niet op enige verdere activiteit tenzij de tunnel opnieuw wordt ingesteld en

opnieuw moet worden geïnitieerd, waarbij de nadruk wordt gelegd op de eerste verkeersgebeurtenissen.

Specificiteit voor traffic initiation: De ACL-hit tellingen zijn specifiek voor de peer die de tunnel initieert. Deze specificiteit zorgt voor een nauwkeurige tracering van welke kant verantwoordelijk is voor het initiëren van de VPN-verbinding, waardoor nauwkeurige bewaking en controle mogelijk is.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.