Workround voordat u AVC-verkeer doorlaat door IPSec-tunnelinterface

Inhoud

Inleiding

Dit document beschrijft de configuratie die vereist is voor het doorgeven van AVC-verkeer door een IPSEC-tunnel naar de collector. Standaard kan AVC-informatie niet via een IPSEC-tunnel naar de verzamelaar worden geëxporteerd

Voorwaarden

Cisco raadt u aan de basiskennis van deze onderwerpen te hebben:

- Application Visibility and Control (AVC)
- Easy Performance Monitor (EzPM)

Achtergrondinformatie

De functie Cisco AVC wordt gebruikt om meerdere toepassingen te herkennen, te analyseren en te controleren. Met toepassingsbewustzijn dat in de netwerkinfrastructuur is ingebouwd, plus zichtbaarheid in de prestaties van toepassingen die op het netwerk actief zijn, maakt AVC beleid

per toepassing mogelijk voor granulaire controle van het gebruik van de bandbreedte, wat resulteert in een betere ervaring van de eindgebruiker. Hier kun je meer details over deze technologie vinden.

EzPM is een snellere en makkelijkere manier om de traditionele prestatiebewaking te configureren. Momenteel biedt EzPM niet de volledige flexibiliteit van het traditionele model voor het configureren van prestatiemonitor. Hier vind je meer informatie over de EzPM.

Beperking

Op dit moment ondersteunt AVC het aantal passthrough tunneling-protocollen niet, hier zijn meer details te vinden.

Internet Protocol Security (IPSec) is een van de niet-ondersteunde doorvoertunneling-protocollen voor AVC en dit document richt zich op de mogelijke tijdelijke oplossing voor deze beperking.

Configureren

In dit deel wordt de volledige configuratie beschreven die wordt gebruikt om de gegeven beperking te simuleren.

Netwerkdiagram

In dit netwerkdiagram hebben alle routers bereikbaarheid aan elkaar door de statische routes te gebruiken. R1 wordt geconfigureerd met de EzPM-configuratie en heeft één IPSec-tunnel die is ingesteld met R2-router. R3 werkt hier als exporteur, wat Cisco Prime kan zijn of een andere soort exporteur die de prestatiegegevens kan verzamelen.

AVC-verkeer wordt gegenereerd door R1 en wordt via R2 naar de exporteur verzonden. R1 verstuurt het AVC-verkeer naar R2 via een IPSec-tunnelinterface.

Eerste configuratie

In dit deel wordt de eerste configuratie voor R1 tot en met R3 beschreven.

R1

```
!
interface-Loopback-up0
ip-adres 1.1.1.1 255.255.255.255
!

interface Gigabit Ethernet0/1

 ip-adres 172.16.1.1 255.255.255.0

 duplex auto

 snelheid auto
```

!

ip-route 0.0.0.0 0.0.0.0 172.16.1.2

!

R2

!

interface Gigabit Ethernet0/0/0

 ip-adres 172.16.2.2 255.255.255.0

 onderhandelings-auto

 !

interface Gigabit Ethernet0/0/1

 ip-adres 172.16.1.2 255.255.255.0

 onderhandelings-auto

!

R3

!

interface Gigabit Ethernet0/0

 ip-adres 172.16.2.1 255.255.255.0

 duplex auto

 snelheid auto

!

ip-route 0.0.0.0 0.0.0.0 172.16.2.2

!

IPsec-configuratie

In dit gedeelte wordt de IPSec-configuratie voor R1 en R2-router beschreven.

R1

!

```
Uitgebreide IP-toegangslijst voor IPSec_matching
 autorisatie ip elke host 172.16.2.1
!
crypto isakmp - beleid 1
 encr aes 256
 hak md5
 controle vooraf
 groep 2
crypto isakmp-toets cisco123 adres 172.16.1.2
!
!
crypto ipsec transformatie-set2 esp-aes 256 esp-sha-hmac
 modemtunnel
!
!
crypto kaart VPN 10 ipsec-isakmp
 ingesteld peer 172.16.1.2
 set transformatie-set2 instellen
 matchadres IPSec_matching
!
interface Gigabit Ethernet0/1
 ip-adres 172.16.1.1 255.255.255.0
 duplex auto
 snelheid auto
 crypto-kaart VPN
!
```

R2

```
!
Uitgebreide IP-toegangslijst voor IPSec_matching
 vergunning ip 172.16.2.1
!
crypto isakmp - beleid 1
 encr aes 256
 hak md5
 controle vooraf
 groep 2
crypto isakmp-toets cisco123 adres 172.16.1.1
!
!
crypto ipsec transformatie-set2 esp-aes 256 esp-sha-hmac
 modemtunnel
!
!
crypto kaart VPN 10 ipsec-isakmp
 ingesteld peer 172.16.1.1
 set transformatie-set2 instellen
 matchadres IPSec_matching
 omgekeerde route
!
interface Gigabit Ethernet0/0/1
 ip-adres 172.16.1.2 255.255.255.0
 onderhandelings-auto
```

```
 cdp mogelijk

 crypto-kaart VPN

!
```

Om te verifiëren of de IPSec-configuratie werkt zoals verwacht of niet, controleer de uitvoer voor **show crypto isakmp sa**

```
R1#show crypto isakmp

IPv4-encryptie met ISAKMP SA

Dst-src status van conn-id

IPv6-encryptie met ISAKMP SA
```

Om de veiligheidsorganisaties op te richten, de exporteur (R3, 172.16.2.1) te pingelen uit R1.

```
R1#ping 172.16.2.1

Typ de ontsnappingsvolgorde om te stoppen.

Verzendtijd 5, 100-byte ICMP Echos naar 172.16.2.1, de tijd is 2
seconden:

!!!!!

Succespercentage is 100% (5/5), min/avg/max = 1/1/4 ms

R1#
```

Nu zal de router een actieve veiligheidsvereniging hebben, die bevestigt dat het verkeer dat van R1 komt en bestemd is voor de exporteur ESP ingekapseld is.

```
R1#show crypto isakmp

IPv4-encryptie met ISAKMP SA

Dst-src status van conn-id

172.16.1.2 172.16.1.1 QM_IDLE 1002 ACTIEF

IPv6-encryptie met ISAKMP SA
```

EzPM-configuratie

In dit gedeelte wordt de EzPM-configuratie voor de R1-router beschreven.

R1

```
!
```

class-map match-all perf-mon-acl

Beschrijving PrimeAM-gegenereerde entiteit - wijzig deze entiteit niet en gebruik deze niet

IP-protocol

!

performance monitor context Performance-Monitor profiel, toepassingservaring

bestemming van de exporteur 172.16.2.1 bron Gigabit Ethernet0/1 transport via de IP-poort 9991

op de verkeerstoepassingsstaten gebaseerde verkeerstoepassingen

gesprekken tussen verkeerslieden en opstandelingen ipv4

traffic-monitor applicatie-responsietijd ipv4

IPv4-ingangen voor verkeersbewakingsmedia

verkeers- en bewakingsmedia ipv4-uitgang

verkeersmonitor versie ipv4 class-replace perf-mon-acl

!

Pas het EzPM-profiel toe op de te controleren interface; hier volgen we de " loopback 0 " - interface .

R1

!

interface-Loopback-up0

ip-adres 1.1.1.1 255.255.255.255

performance monitor context Performance-Monitor

!

Werken

Als de bovenstaande configuratie is geïnstalleerd, neem dan de uitvoer voor **show performance monitor** *contextcontext*-**naam exporteur**.

Schakel de optie **Uitloopfuncties** in op de status van de optie **Uitvoer**. Deze optie is standaard **ingeschakeld**. Dit is een verwacht gedrag en daarom wordt het AVC-verkeer niet ingekapseld of versleuteld.

Om het AVC-verkeer door de IPsec-tunnelinterface te laten passeren, wordt de optie **Uitloopeigenschappen** gebruikt. Om dat te doen, moet het expliciet in flow-exporteurs profiel

worden ingeschakeld. Hieronder vindt u de stap voor stap gedetailleerde procedure om deze optie mogelijk te maken.

Stap 1

Neem de volledige uitvoer voor **show performance monitor context** *context-name* **configuratie** opdracht en bewaar deze in noteblok. Hieronder staat het fragment voor deze uitvoer.

```
R1#show performance monitor-configuratie van context Performance Monitor

=======================================================================
=======================================================================
=======================================================================

!            Gelijkwaardige configuratie van Context Performance-
Monitor!

=======================================================================
=======================================================================
=======================================================================

!Exporters

==========!

!

uitvoer van stroom Performance-Monitor-1

 beschrijving van de prestatiebewaking van de context Prestatie-Monitor
exporteur

 bestemming 172.16.2.1

 bron Gigabit Ethernet0/1

 vervoer udp 9991

 exportprotocol-oplossing

 sjabloon gegevens timeout 300

 optie interface-tabel timeout 300

 optie vrf-tabel timeout 300

 optie c3pl-class-table timeout 300

 optie c3pl-beleidstabeltijd 300

 optie-monsternemertijd 300
```

```
 optie toepassing-tabel timeout 300

 optie-applicatie-eigenschappen timeout 300

 optie-sub-application-table timeout 300

—snip—
```

Stap 2

Voeg de optie **uitvoerfuncties** expliciet toe onder het profiel van de stroomexporteur. Na het toevoegen van de optie "outputeigenschappen" moet het profiel van de stroomexporteur er zo uitzien;

uitvoer van stroom Performance-Monitor-1

beschrijving van de prestatiebewaking van de context Prestatie-Monitor exporteur

bestemming 172.16.2.1

bron Gigabit Ethernet0/1

vervoer udp 9991

exportprotocol-oplossing

sjabloon gegevens timeout 300

uitvoerfuncties

optie interface-tabel timeout 300

optie vrf-tabel timeout 300

optie c3pl-class-table timeout 300

optie c3pl-beleidstabeltijd 300

optie-monsternemertijd 300

optie toepassing-tabel timeout 300

optie-applicatie-eigenschappen timeout 300

optie-sub-application-table timeout 300

Laat de rest van de uitvoer ongewijzigd zoals deze is, Wijzig GEEN andere wijzigingen in de uitvoer.

Stap 3

Verwijder nu het EzPM-profiel van de interface en ook van de router.

!

Interfaceback 0

geen prestatiemonitor voor context Performance Monitor

uitgang

!

!

geen ervaring met prestatiebewaking van context Performance-Monitor profieltoepassing

!

Stap 4

Pas de aangepaste configuratie op de R1-router toe. Zorg dat er geen enkele opdracht wordt gemist, omdat dit onverwacht gedrag kan veroorzaken.

Verifiëren

In dit gedeelte wordt de verificatiemethode beschreven die in dit document wordt gebruikt voor de controle van de inhoud en hoe deze bewerking heeft bijgedragen aan het overwinnen van de limieten voor AVC-pakketten die hier worden genoemd.

Voordat u het werkvenster toepast, worden de pakketten die door de IPSec peer router (R2) zijn ontvangen, ingetrokken. Dit bericht wordt ook gegenereerd:

```
%IPSEC-3-RECVD_PKT_NOT_IPSEC: Rec'd-pakket geen IPSEC-pakket, dest_addr=
172.16.2.1, src_addr= 172.16.1.1, poort= 17
```

Hier verwacht R2 dat de in ESP ingekapselde pakketten die voor 172.16.2.1 bestemd zijn, maar de ontvangen pakketten zijn gewone UDP-pakketten (prot=17) en het is verwacht dat deze pakketten worden gedroogd. Hieronder toont de pakketvastlegging aan dat het bij R2 ontvangen pakket een leeg UDP-pakket is in plaats van een ingekapselde ESP-pakketvastlegging, wat een standaardgedrag voor AVC is.

```
Internet Protocol Version 4, Src: 172.16.1.1 (172.16.1.1), Dst: 172.16.2.1 (172.16.2.1)
  Version: 4
  Header Length: 20 bytes
⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
  Total Length: 1348
  Identification: 0x961a (38426)
⊞ Flags: 0x00
  Fragment offset: 0
  Time to live: 255
  Protocol: UDP (17)
⊞ Header checksum: 0xc56b [validation disabled]
  Source: 172.16.1.1 (172.16.1.1)
  Destination: 172.16.2.1 (172.16.2.1)
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
User Datagram Protocol, Src Port: 50208 (50208), Dst Port: 9991 (9991)
  Source Port: 50208 (50208)
  Destination Port: 9991 (9991)
  Length: 1328
⊞ Checksum: 0xb7ec [validation disabled]
  [Stream index: 0]
Data (1320 bytes)
```

Na het toepassen van het tijdelijke beeld wordt uit de onderstaande pakketvastlegging duidelijk zichtbaar dat de AVC-pakketten die bij R2 worden ontvangen, zijn ingekapseld in ESP en dat er geen meer foutmeldingen meer worden weergegeven op R2.

```
Internet Protocol Version 4, Src: 172.16.1.1 (172.16.1.1), Dst: 172.16.1.2 (172.16.1.2)
  Version: 4
  Header Length: 20 bytes
⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
  Total Length: 1448
  Identification: 0x0114 (276)
⊞ Flags: 0x00
  Fragment offset: 0
  Time to live: 255
  Protocol: Encap Security Payload (50)
⊞ Header checksum: 0x5aec [validation disabled]
  Source: 172.16.1.1 (172.16.1.1)
  Destination: 172.16.1.2 (172.16.1.2)
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
Encapsulating Security Payload
  ESP SPI: 0x804c46a3 (2152482467)
  ESP Sequence: 203
```

Probleemoplossing

Er is momenteel geen specifieke informatie over probleemoplossing beschikbaar voor deze configuratie.