EEM voorbeelden voor verschillende VPN-scenario's op ASA

Inhoud

Inleiding

De Cisco IOS® Software Embedded Event Manager (EEM) is een krachtig en flexibel subsysteem dat real-time detectie van netwerkgebeurtenissen en automatisering aan boord biedt. Dit document geeft u voorbeelden van waar EEM kan helpen in verschillende VPN-scenario's

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van de ASA EEM-functie.

Gebruikte componenten

Dit document is gebaseerd op de Cisco adaptieve security applicatie (ASA) die of later software versie 9.2(1) draait.

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.

Achtergrondinformatie

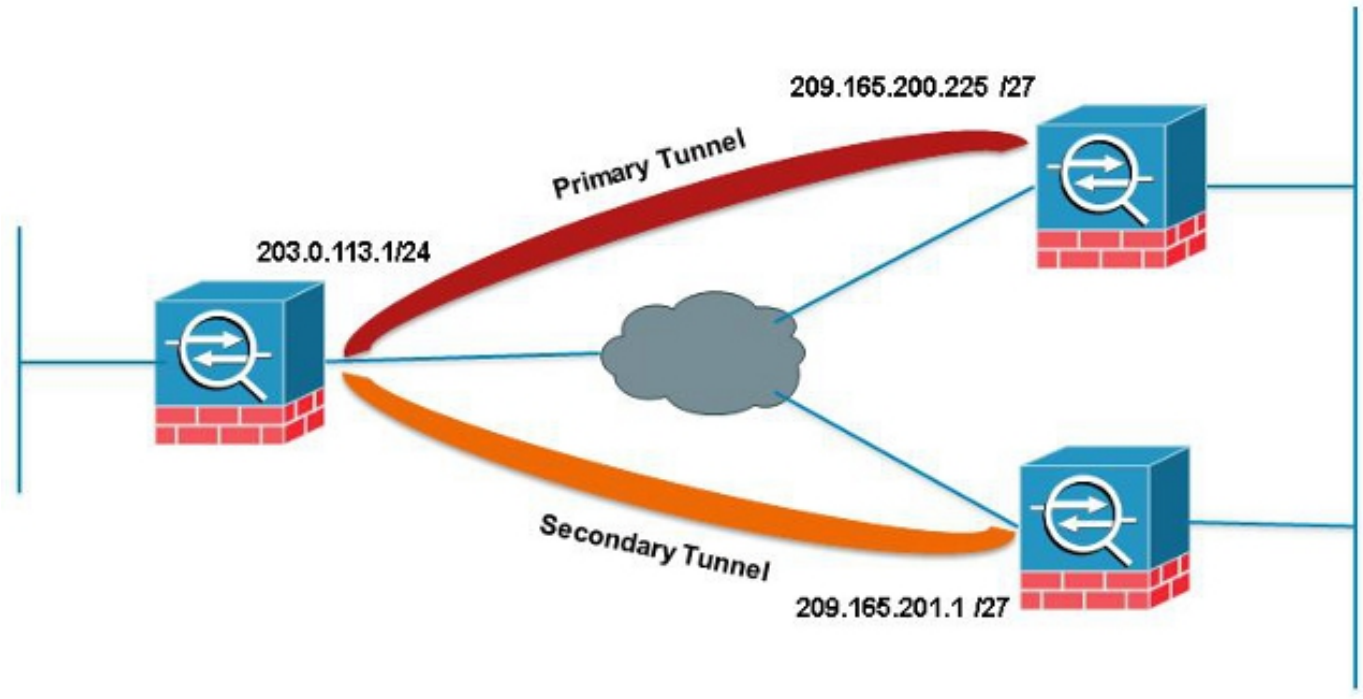
Embedded Event Manager werd oorspronkelijk "achtergrond-debug" genoemd in de ASA en was een eigenschap gebruikt om een specifiek probleem te debug. Na review bleek het vergelijkbaar genoeg te zijn met Cisco IOS-software EMM, zodat het werd bijgewerkt om aan die CLI te voldoen.

Met de EEM-functie kunt u problemen oplossen en algemene vastlegging voor probleemoplossing bieden. Het EEM reageert op gebeurtenissen in het EEM - systeem door maatregelen uit te voeren. Er zijn twee onderdelen: gebeurtenissen die het EEM in gang zet, en gebeurtenissen die de beheerder toepast die acties definiëren. U kunt meerdere gebeurtenissen toevoegen aan elke applicatie van de eventmanager, waardoor het wordt geactiveerd om de acties op te roepen die er ingesteld zijn.

VPN-preventie

Als u VPN met meerdere peer IP adressen voor een crypto ingang vormt, wordt VPN gevestigd met de backup peer IP zodra de primaire peer daalt. Zodra de primaire peer echter terugkomt, loopt VPN niet vooruit op het primaire IP-adres. U moet de bestaande SA handmatig wissen om de onderhandeling van VPN te heropenen om het over te switches naar het primaire IP adres.

```
ASA 1
crypto map outside_map 10 match address outside_cryptomap_20
crypto map outside_map 10 set peer 209.165.200.225 209.165.201.1
crypto map outside_map 10 set transform-set ESP-AES-256-SHA
crypto map outside_map interface outside
```



In dit voorbeeld wordt een IP site level aggregation (SLA) gebruikt om de Primaire tunnel te controleren. Als die peer faalt, neemt de backup peer de zaak over, maar de SLA controleert de primaire; Zodra de Primaire terugkomt, zal de gegenereerde slang de EEM in gang zetten om de secundaire tunnel te ontruimen, zodat de ASA opnieuw met de Primaire kan onderhandelen.

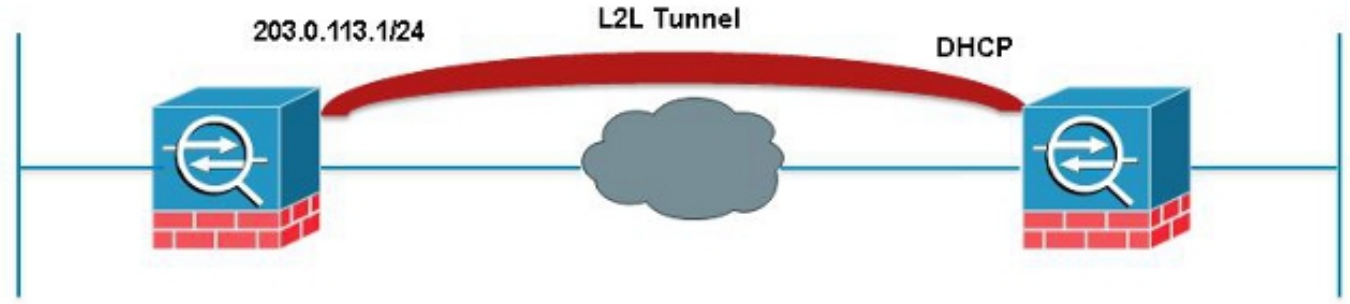
```
sla monitor 123
type echo protocol ipIcmpEcho 209.165.200.225 interface outside
```

```
num-packets 3
frequency 10

sla monitor schedule 123 life forever start-time now

track 1 rtr 123 reachability

route outside 209.165.200.225 255.255.255.0 203.0.113.254 1 track 1

event manager applet PREEMPT
event syslog id 622001 occurs 2
action 1 cli command "clear crypto ipsec sa peer 209.165.101.1"
output none
```

Dynamisch-naar-statische L2L altijd omhoog

Wanneer u een LAN-to-LAN tunnel maakt, moet het IP-adres van beide IPSec-peers bekend zijn. Als een van de IP-adressen niet bekend is omdat deze dynamisch is, d.w.z. via DHCP verkregen, is het enige alternatief het gebruik van een dynamische crypto-kaart. De tunnel kan slechts van het apparaat met het dynamische IP worden geïnitieerd aangezien de andere peer geen idee heeft van IP die wordt gebruikt.

Dit is een probleem voor het geval niemand achter het toestel zit met de dynamische IP om de tunnel op te halen voor het geval dat deze naar beneden gaat; de noodzaak van deze tunnel is dus altijd groter . Zelfs als je de ongebruikte tijdspanne op **geen** zet, zal dit de kwestie niet aanpakken omdat, op een rekensom, als er geen verkeer is dat de tunnel passeert, zal dalen. Op dat moment is de enige manier om de tunnel weer op te halen het verkeer van het apparaat met de dynamische IP te sturen. Hetzelfde geldt als de tunnel omlaag gaat om een onverwachte reden zoals de DPD.



Deze EEM zal elke 60 seconden een ping door de tunnel sturen die overeenkomt met de gewenste SA om de verbinding op te houden.

```
event manager applet VPN-Always-UP
event timer watchdog time 60
action 1 cli command "ping inside 192.168.20.1"
output none
```

Koppel alle VPN-bestaande verbindingen op een bepaald moment los

ASA heeft geen manier om een harde cut-off tijd in te stellen voor VPN-sessies. U doet dit echter met EEM. Dit voorbeeld laat zien hoe u zowel VPN-clients als AnyConnect-clients vanaf 5:00 uur kunt onderscheiden

```
event manager applet VPN-Disconnect
event timer absolute time 17:00:00
action 1 cli command "vpn-sessiondb logoff ra-ikev1-ipsec noconfirm"
action 2 cli command "vpn-sessiondb logoff anyconnect noconfirm"
output none
```