ASA FAQ: Hoe kan ik de ASA bron interface voor syslogs specificeren die via een VPN toonl worden verstuurd?

Inhoud

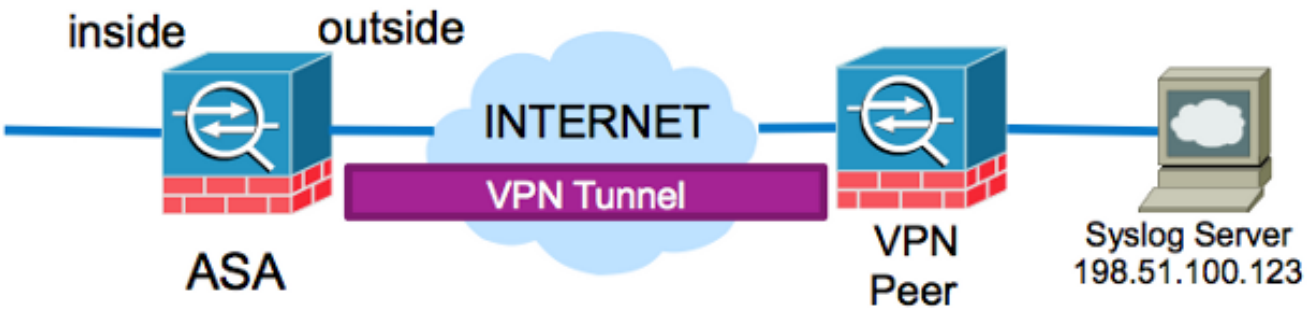
Inleiding

Dit document beschrijft hoe u de Cisco adaptieve security applicatie (ASA) dient te configureren om systemen via een LAN-to-LAN VPN-tunnel te verzenden en deze signalen vanaf het IP-adres van de binnenkant te bron.

Hoe kan ik de ASA bron interface voor systemen specificeren die via een VPN-tunnel worden verstuurd?

Om de interface te specificeren van wie om het syslogverkeer te bron dat over de tunnel wordt verzonden, voer de **beheer-toegang** opdracht in.

Als uw systeem deze topologie en configuratie heeft, voer dan de opdrachten in die volgen.




```
ASA# show run logging
logging enable
logging timestamp
logging trap debugging
logging host outside 198.51.100.123
```

Deze configuratie probeert het actieve verkeer te bron vanaf het IP-adres van de ASA. Dit vereist dat het externe IP-adres aan de crypto toegangslijst wordt toegevoegd om het verkeer via de tunnel te versleutelen. Deze configuratieverandering zou niet optimaal kunnen zijn, vooral als het verkeer dat van het binnen interface IP adres komt dat voor syslog serversubnet bestemd is reeds is ingesteld om door de crypto access-list te worden ingesloten.

ASA kan worden geconfigureerd om het syslogverkeer te starten dat bestemd is voor de server om over de VPN-tunnel te worden verzonden vanuit de interface die met de **beheertoegang** opdracht is gespecificeerd.

Om deze configuratie voor dit specifieke voorbeeld uit te voeren, verwijder eerst de huidige configuratie van de **houtkap**:

```
no logging host outside 198.51.100.123
```

Plaats de logserver opnieuw met de opgegeven interne interface en de opdracht **beheertoegang**:

```
logging host inside 198.51.100.123
management-access inside
```