VPN-migratie configureren tussen FTD's die worden beheerd door één FMC

Inhoud

Inleiding

Dit document beschrijft het migreren van een Site-to-Site VPN van de ene FTD naar de andere, beheerd door dezelfde FMC, terwijl de VPN-verbinding met de router behouden blijft.

Voorwaarden

Vereisten

Om het migratieproces effectief uit te voeren, raadt Cisco aan om vertrouwd te raken met de gegeven onderwerpen:
· FTD-registratie bij FMC: begrijpen hoe u Firepower Threat Defense (FTD)-apparaten kunt registreren bij het Firepower Management Center (FMC).
· Site-to-Site VPN-configuratie: Ervaring met het configureren van site-to-site VPN's op FTD-apparaten die worden beheerd door FMC.

Gebruikte componenten

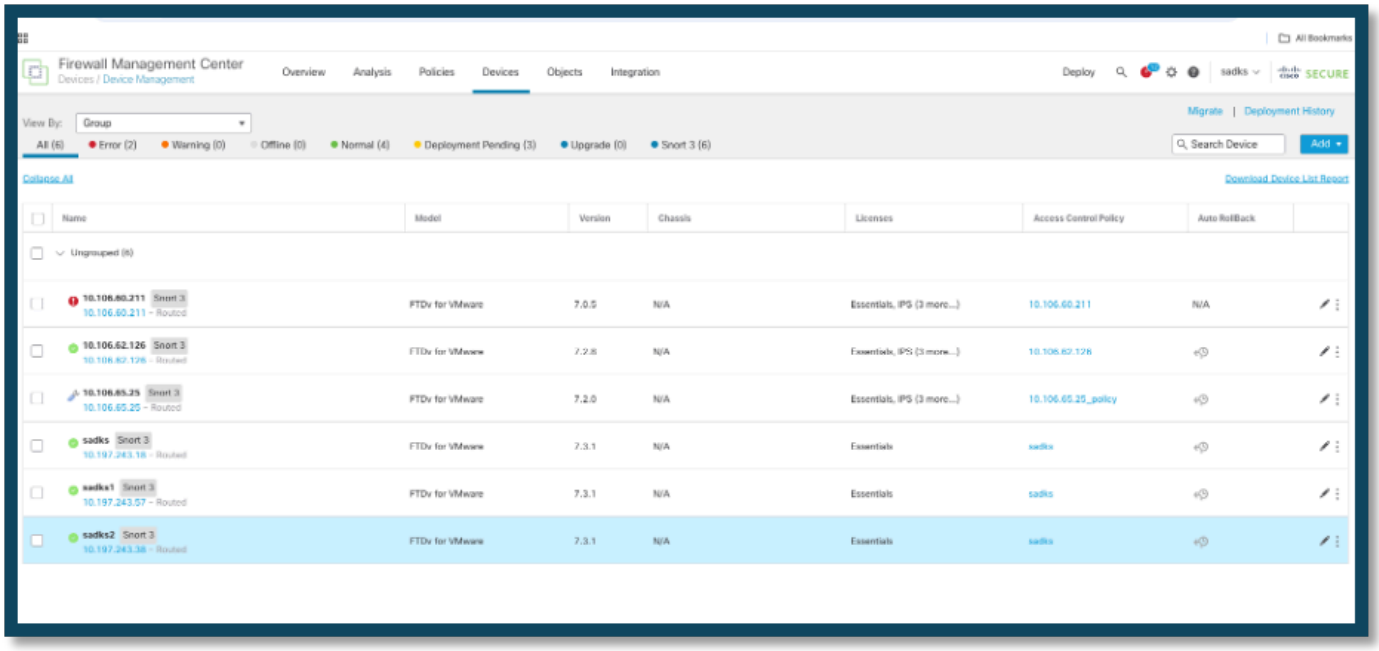
Dit document is gebaseerd op de opgegeven software- en hardwareversies:
· Firepower Threat Defense Virtual (FTDv): twee instanties met versie 7.3.1.
· Firepower Management Center (FMC): versie 7.4.0.

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.

Configureren

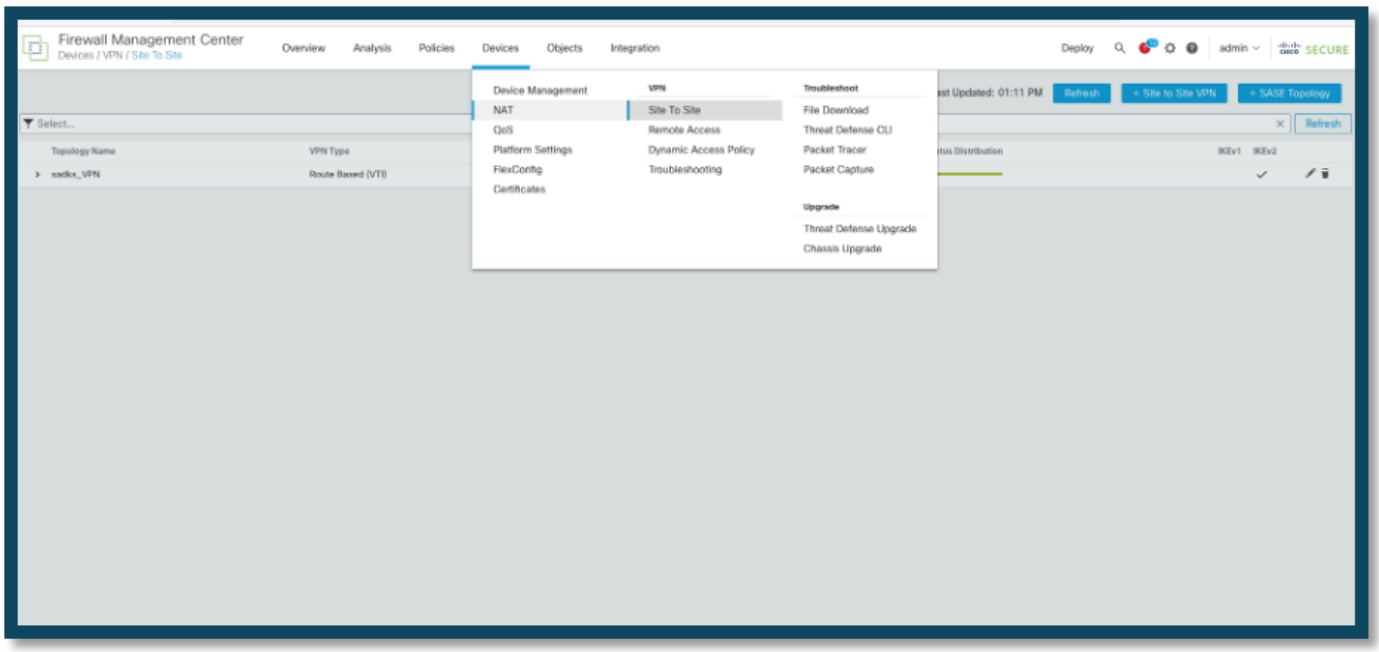
Procedure

1. Registreer het nieuwe FTD bij het VCC:
   · Begin met het registreren van het nieuwe Firepower Threat Defense (FTD)-apparaat in het Firepower Management Center (FMC) onder Apparaten > Apparaatbeheer.
   · In dit voorbeeld wordt het nieuwe geregistreerde apparaat "sadks2" genoemd.



Nieuw FTD geregistreerd

2. Toegang tot de site-to-site tunnelconfiguratie:
   · Navigeer naar de site-to-site tunnelinstellingen door naar Apparaten > Site-to-site te gaan in de FMC-interface.

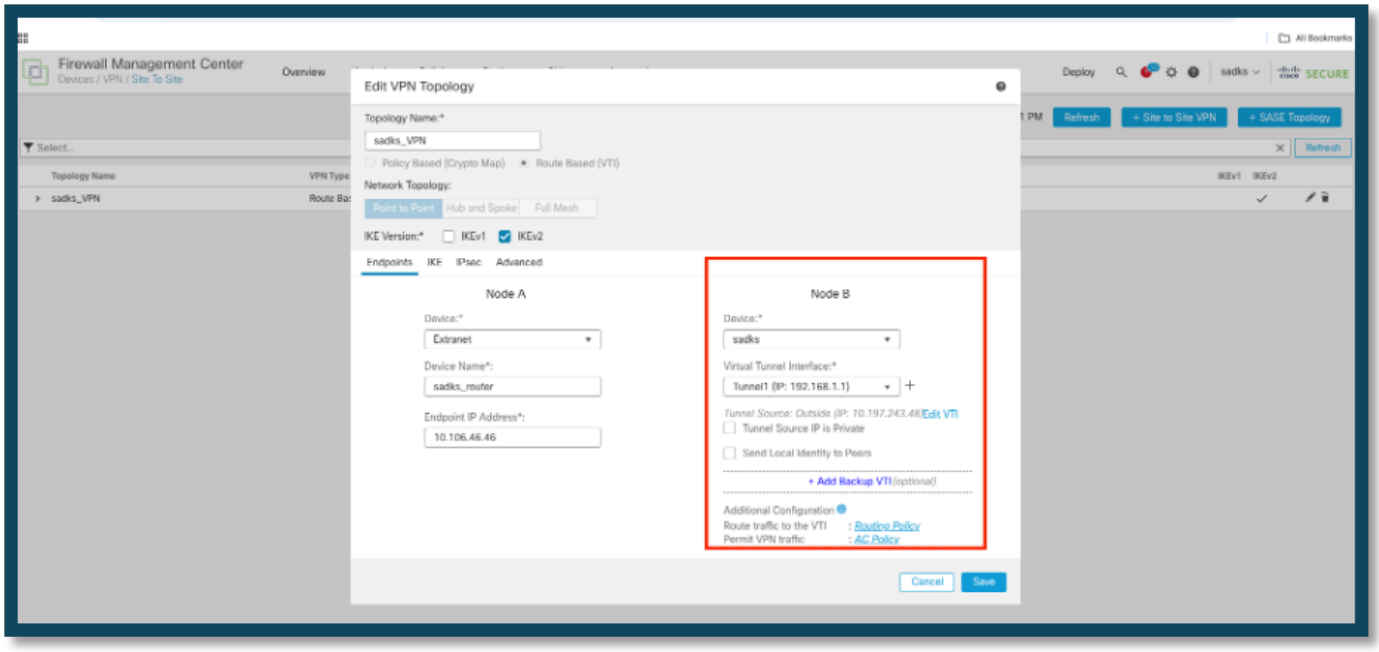


Navigeer naar VPN Config

3. Wijzig de VPN-configuratie:

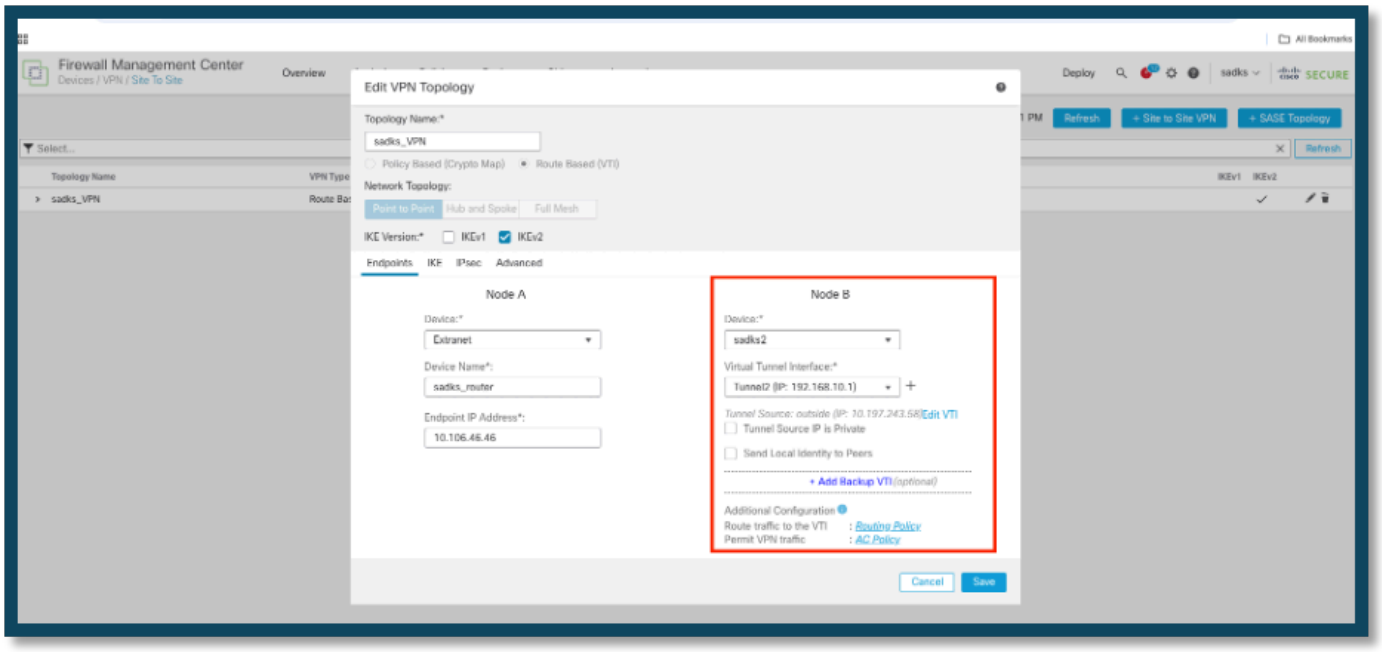
· Selecteer de VPN-configuratie die u wilt bijwerken.

· Voorbeeld: In dit scenario omvat de VPN-configuratie een FTD-apparaat en een router. Hier vertegenwoordigt knooppunt B het FTD-apparaat en is de configuratie bijgewerkt om de apparaatkoppeling van "schijven" naar "sadks2" te wijzigen.



Oud FTD-apparaat

in



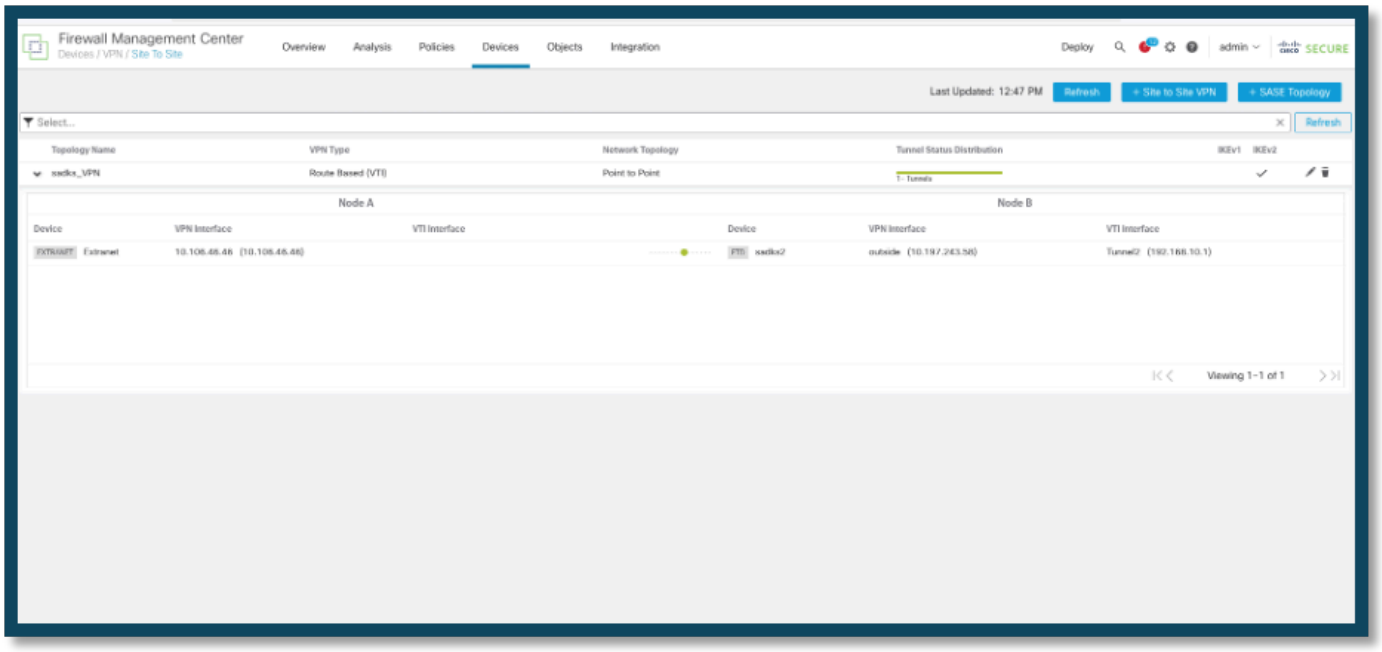
Nieuw FTD-apparaat

4. De configuratie opslaan en implementeren:

· Nadat u de nodige wijzigingen hebt aangebracht, slaat u de configuratie op en implementeert u deze om de updates te activeren.

Verifiëren

De tunnel komt tevoorschijn als hij eenmaal is ingezet.



tunnelstatus

Problemen oplossen

Aanvankelijke connectiviteitsproblemen

Bij het bouwen van een VPN zijn er twee partijen die onderhandelen over de tunnel. Daarom is het het beste om beide kanten van het gesprek te krijgen wanneer u problemen oplost met elk type tunnelstoring. Een gedetailleerde gids over het debuggen van IKEv2-tunnels is hier te vinden: Hoe IKEv2 VPN's te debuggen

De meest voorkomende oorzaak van tunnelstoringen is een connectiviteitsprobleem. De beste manier om dit te bepalen is om pakketopnames op het apparaat te maken. Gebruik deze opdracht om pakketopnames op het apparaat te maken:

<#root>

capture capout interface outside match ip host 10.106.46.46 host 10.197.243.58

Zodra de opname op zijn plaats is, probeer dan verkeer over de VPN te verzenden en te controleren op bi-directioneel verkeer in de pakketopname.

Bekijk de pakketopname met deze opdracht:

<#root>

show cap capout

Verkeersspecifieke kwesties

Veelvoorkomende verkeersproblemen die u ondervindt zijn:

- Routeringsproblemen achter de FTD -- het interne netwerk kan pakketten niet terugleiden naar de toegewezen IP-adressen en VPN-clients.
- Toegangscontrolelijsten blokkeren verkeer.
- Netwerkadresvertaling wordt niet omzeild voor VPN-verkeer.

Voor meer informatie over VPN's op de FTD beheerd door FMC, kunt u de volledige configuratiehandleiding hier vinden: FTD beheerd door FMC configuratiehandleiding

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.