Naadloze overgang: migratie van Palo Alto Firewall naar Cisco FTD

Inhoud

Inleiding

Dit document beschrijft het proces van de overgang van een Palo Alto firewall naar een Cisco FTD-systeem met behulp van de FMT versie 6.0.

Voorwaarden

Vereisten

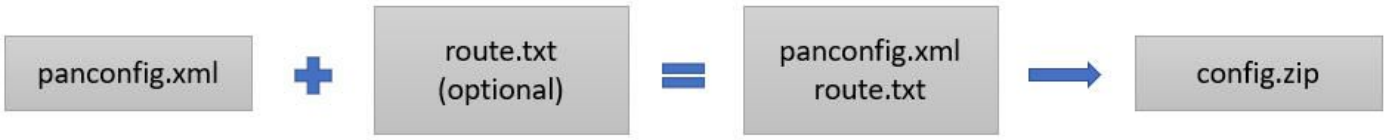
Cisco raadt kennis van de volgende onderwerpen aan:

- De huidige actieve configuratie exporteren vanuit de Palo Alto-firewall in XML-indeling (*.xml).
- De Palo Alto Firewall CLI openen en de opdracht routeringsroute tonen uitvoeren, waarna de uitvoer als tekstbestand wordt opgeslagen (*.txt).
- Zowel het configuratiebestand (*.xml) als het uitvoerbestand (*.txt) worden gecomprimeerd tot één ZIP-archief (*.zip).

Gebruikte componenten

De informatie in dit document is gebaseerd op Palo Alto Firewall versie 8.4.x of hoger.

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.



Firepower Migration Tool (FMT)

De FMT helpt technische teams bij de overgang van bestaande Vendor-firewalls naar Ciscos Next-Generation Firewall (NGFW) / Firepower Threat Defense (FTD). Zorg ervoor dat u de nieuwste versie van FMT gebruikt, gedownload van de Cisco-website.

migratierichtlijn

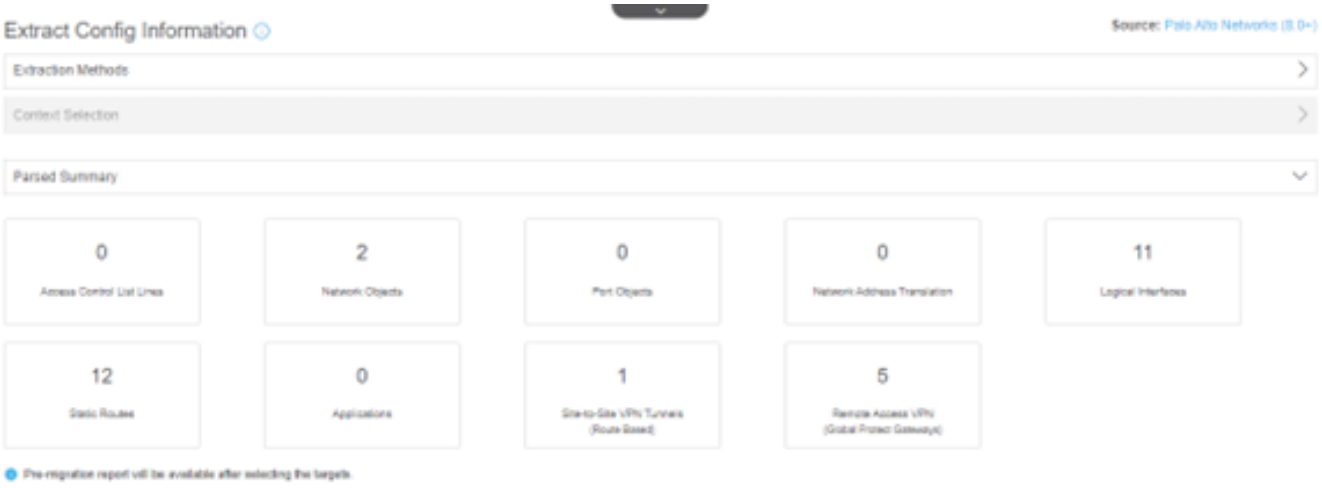
1. Controlelijst vóór de migratie

- Zorg ervoor dat het FTD aan het VCC is toegevoegd voordat het migratieproces wordt gestart.
- Er is een nieuwe gebruikersaccount met beheerdersrechten gemaakt in de FMC.
- Geëxporteerd Palo Alto met configuratie file.xml moet worden gezipt met een extensie van .zip.
- NGFW/FTD moet hetzelfde aantal fysieke of subinterface of poortkanaal hebben als Palo Alto Firewall-interfaces.

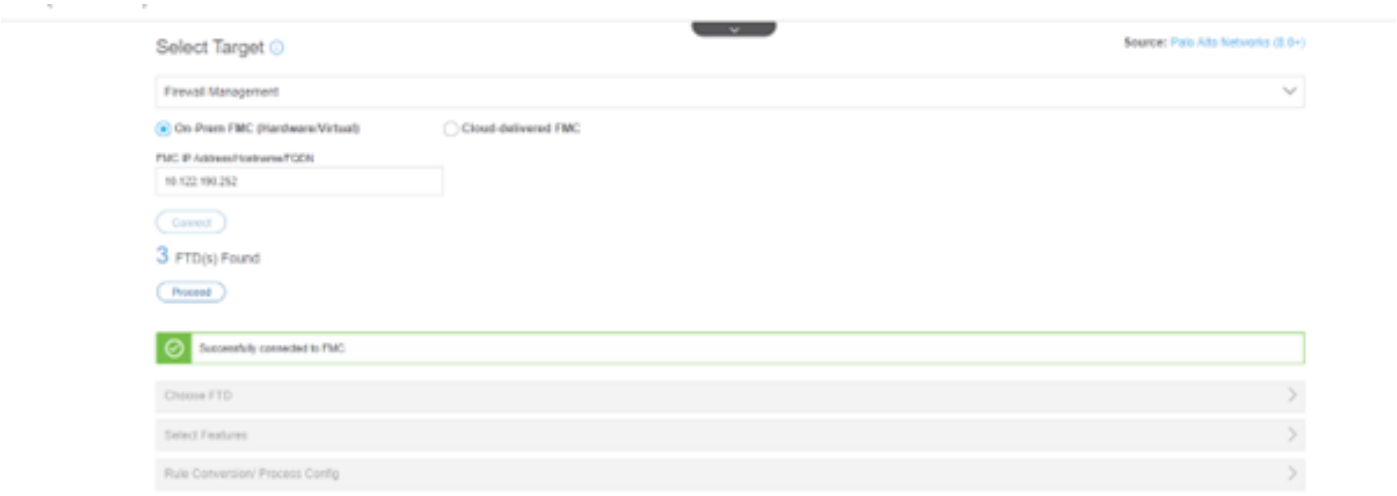
2. Gebruik van migratietools

- Download de FMT tool .exe en voer uit als beheerder.
- FMT heeft een CEC-ID of een Cisco-gebruikersaccount nodig om in te loggen.
- Na Succesvolle aanmelding toont de tool een dashboard waar u een firewallleverancier kunt kiezen en het bijbehorende *.zip-bestand kunt uploaden; raadpleeg de volgende afbeelding.

- Bekijk de instructies aan de rechterkant zorgvuldig voordat u doorgaat met de migratie.
- Klik op Migratie starten zodra u klaar bent om te beginnen.
- Upload het opgeslagen *.zip-bestand met de configuratie-instellingen van uw Palo Alto-firewall.
- Zodra het configuratiebestand is geüpload, kunt u een ontleed overzicht van de inhoud zien en op volgende klikken; raadpleeg de volgende afbeelding.

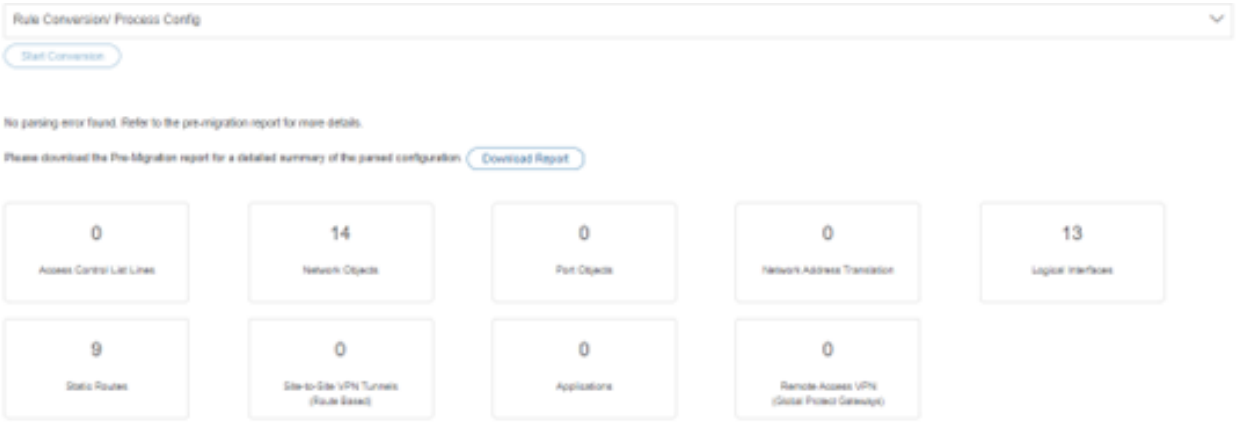


- Voer het IP-adres van de FMC in en log in.
- De tool zal zoeken naar een actieve FTD die is geregistreerd bij het FMC.
- Kies de FTD die u wilt migreren en klik op Doorgaan, zoals weergegeven in de volgende afbeelding.

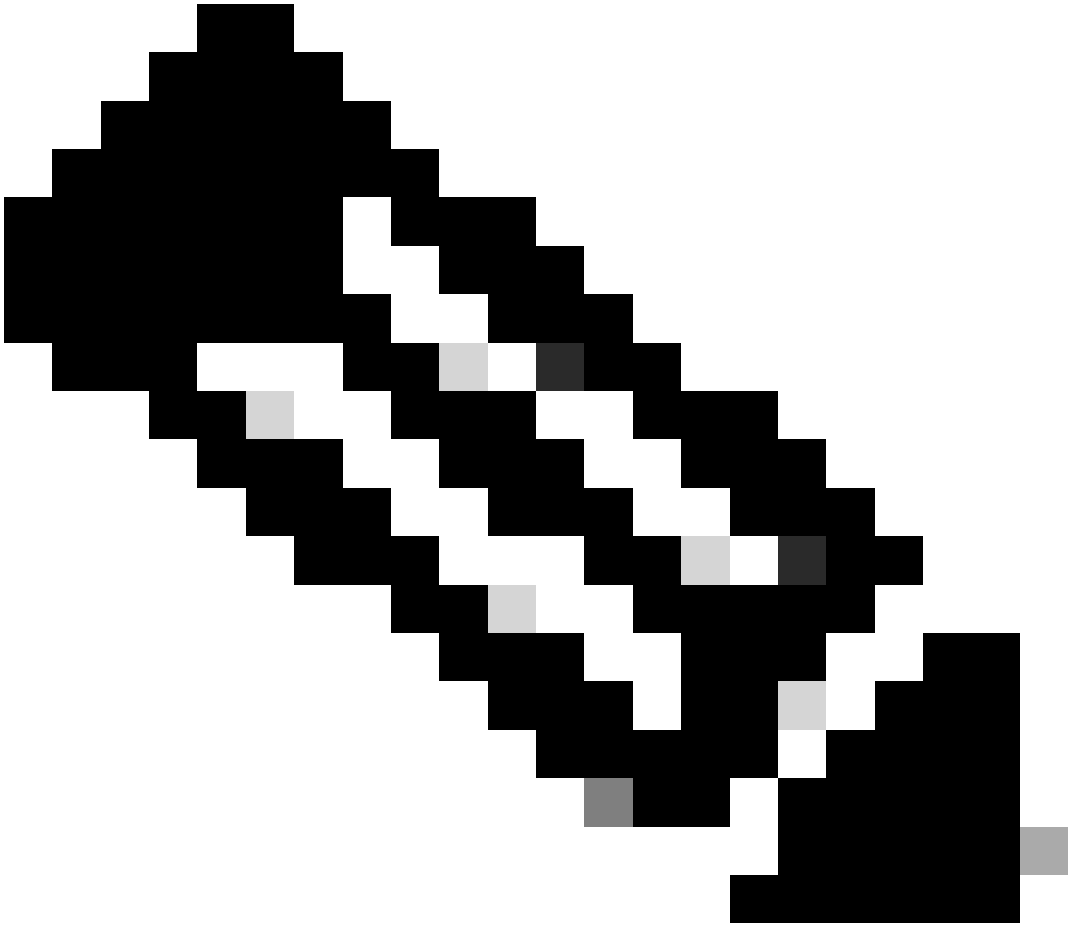


- Kies de specifieke functies om te migreren op basis van de vereisten van de klant. Merk op dat Palo Alto-firewalls een andere functieset hebben in vergelijking met FTD.
- Klik op Doorgaan en raadpleeg de volgende afbeelding ter referentie.

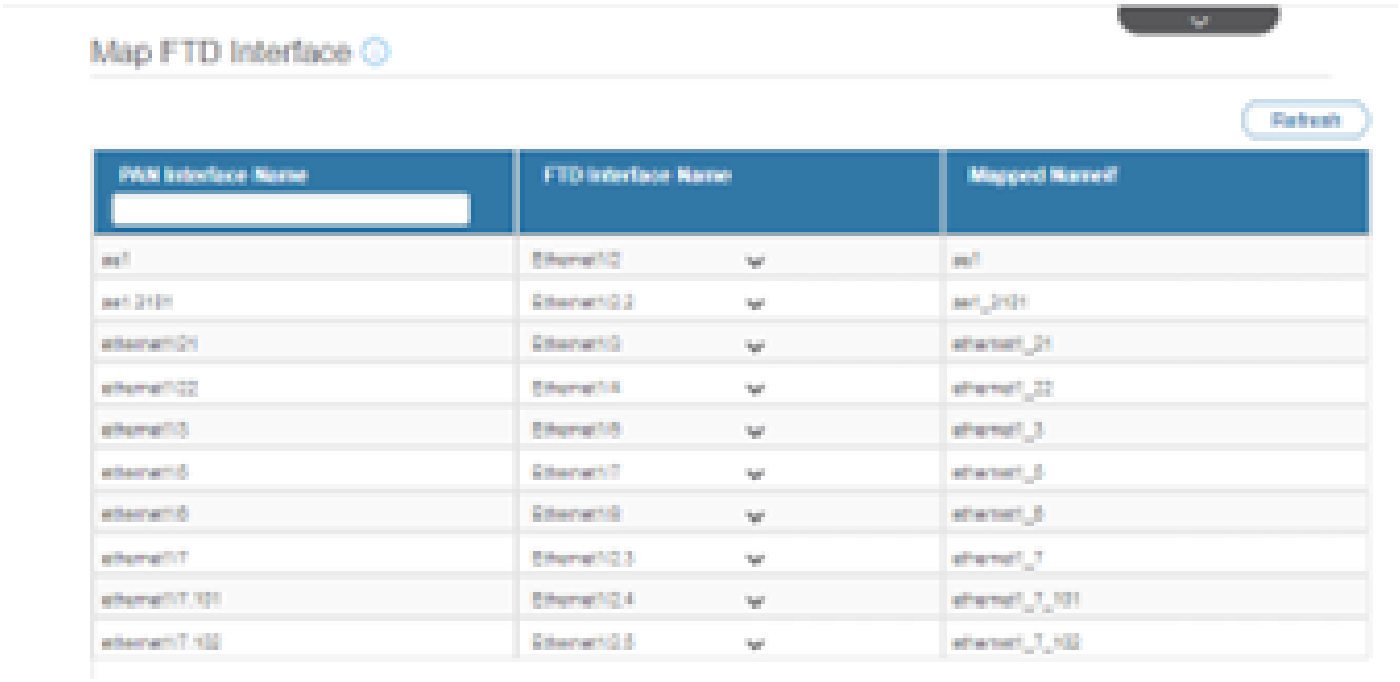
- De FMT voert de conversie uit volgens uw selecties. Controleer de wijzigingen in het rapport vóór migratie en klik op Doorgaan. Zie de volgende afbeelding voor meer informatie.



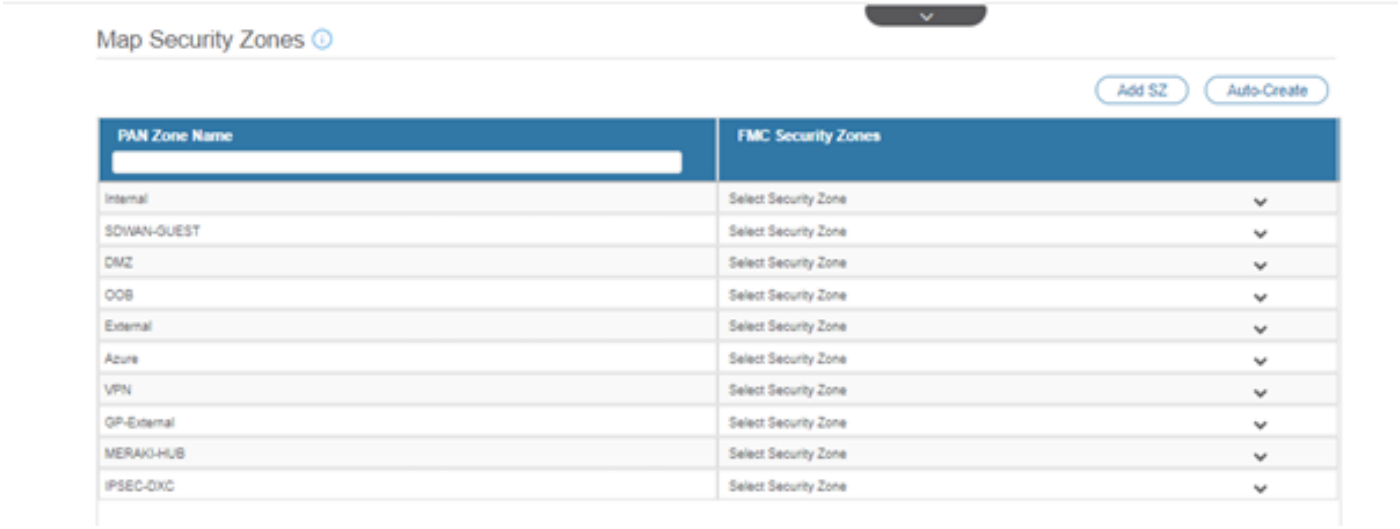
  - Breng de interfaces van de Palo Alto-firewall in kaart met die op de FTD. Raadpleeg de volgende afbeelding voor meer informatie.



Opmerking: NGFW/FTD moet hetzelfde aantal fysieke of subinterface of poortkanaal hebben als Palo Alto Firewall-interfaces, inclusief subinterfaces.



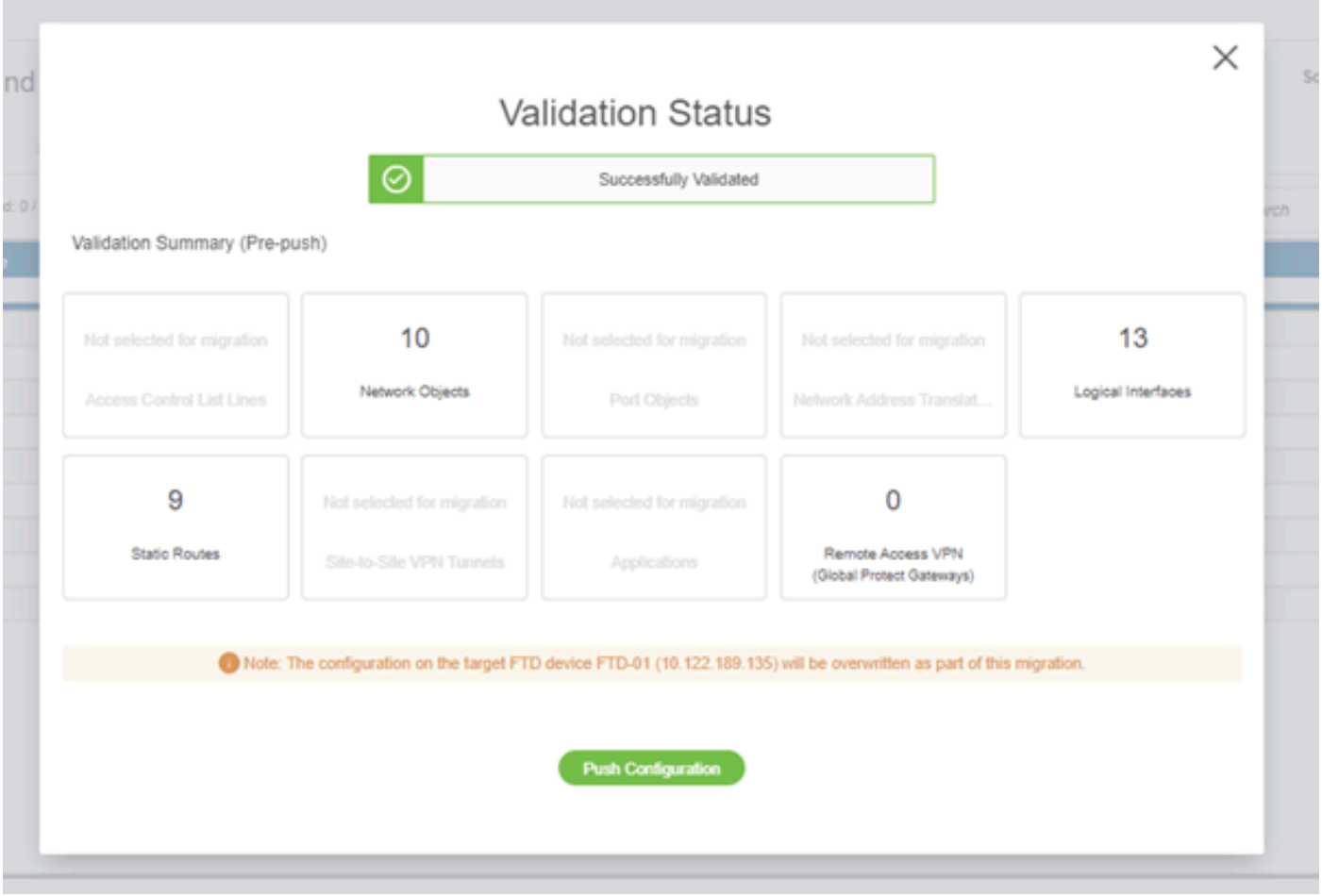
- Bepaal de toewijzing voor zones, die handmatig of met behulp van de functie Automatisch maken kan worden gedaan. Voor visualisatie verwijzen we naar de volgende afbeelding.



- Wijs uw profiel voor het blokkeren van toepassingen toe. Aangezien dit een laboratoriumapparaat is zonder toewijzing van toepassingen, kunt u doorgaan met de standaardinstellingen en kunt u doorgaan. Klik op Volgende en raadpleeg de afbeelding die wordt geleverd.

- Optimaliseer ACL's, objecten, interfaces en routes indien nodig. Aangezien dit een labopstelling is met minimale configuraties, kunt u doorgaan met de standaardopties. Klik vervolgens op Valideren, verwijzend naar de volgende afbeelding.

- Na succesvolle validatie is de configuratie klaar om te worden geïmplementeerd in de beoogde FTD. Zie de volgende afbeelding voor verdere instructies.



- De Push Configuration slaat de gemigreerde configuraties op in FMC en wordt automatisch in de FTD geïmplementeerd.
- In geval van een probleem tijdens de migratie, voel je vrij om een TAC geval te openen voor verdere hulp.

3. Validatie na migratie

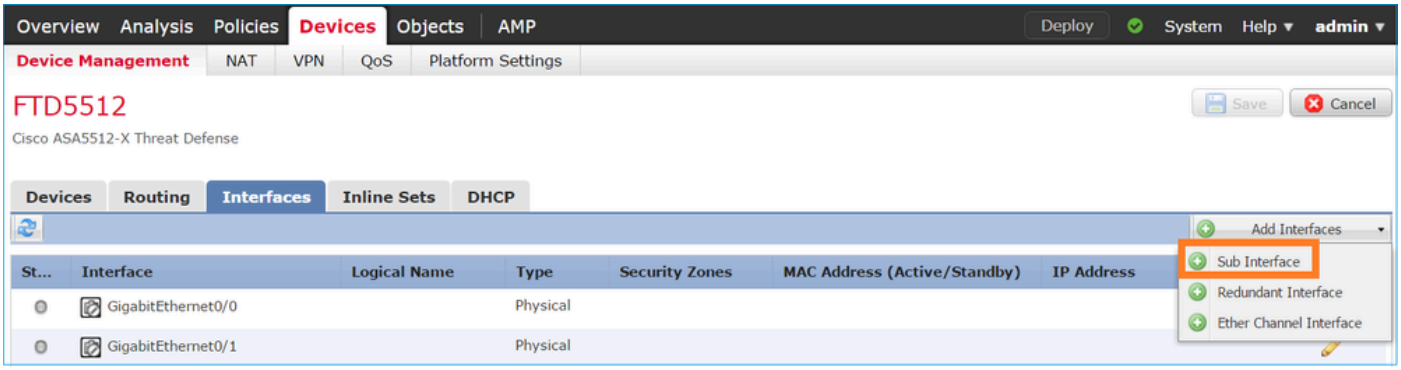
- De configuratie valideren op de FTD en de FMC.
- De ACL's, het beleid, de connectiviteit en andere geavanceerde functies van het apparaat testen.
- Maak een terugdraaipunt voordat u wijzigingen uitvoert.
- De migratie in de laboratoriumomgeving testen voordat Go-Live in de productieomgeving wordt uitgevoerd.

Bekende problemen

1. Ontbrekende interfaces op FTD

- Meld u aan bij de Palo Alto CLI en voer de interface voor alle shows uit. U moet een gelijk of groter aantal interfaces in FTD hebben.
- Maak een gelijk of groter aantal interfaces - subinterface, poortkanaal of fysieke interface via FMC GUI.
- Navigeer naar FMC GUI Device > Device Management, klik op de FTD waarin de vereiste

interface moet worden gemaakt. Kies in het vervolgkeuzemenu Rechterhoek onder Interface de optie Create Sub-interface/BVI dienovereenkomstig en maak de interface en koppel de bijbehorende interfaces. Sla de configuratie op en synchroniseer met het apparaat.



- Controleer of interfaces op FTD zijn gemaakt door IP-briefing van de interface tonen uit te voeren en door te gaan met migratie voor toewijzing van de interface.

2. Routeringstabel

- Verifieer de routeringstabel op de Palo Alto-firewall door de routeringroute tonen of het routeringoverzicht tonen uit te voeren.
- Voordat u de routes naar FTD migreert, controleert u de tabel en kiest u de vereiste routes volgens de projectbehoefte.
- Valideer dezelfde routeringstabel in de FTD door alle routes weer te geven en een routeoverzicht weer te geven.

3. Optimaliseren

- Het deelvenster Objecten optimaliseren is grijs weergegeven. Soms moet u een handmatig object in FMC maken en toewijzen. Als u het object in FTD wilt bekijken, gebruikt u Uitvoeren weergeven | in objecten en in Palo Alto, gebruikt u Adres <objectnaam weergeven>.
- Toepassingsmigratie vereist een audit van de Palo Alto-firewall vóór de migratie, FTD heeft een speciaal IPS-apparaat of u kunt de functie in FTD inschakelen, zodat u de toepassingsmigratietaak moet plannen volgens de klantvereisten.
- NAT-configuratie van Palo Alto firewall moet worden geverifieerd door show running nat-policy en u moet een aangepast NAT-beleid in FTD hebben, dat kan worden bekeken in FTD door Show Running nat.

Conclusie

De Palo Alto-firewall is met succes gemigreerd naar Cisco FTD met behulp van FMT. In het geval van een probleem na de migratie op FTD en voor het oplossen van problemen, opent u verder een TAC-zaak.

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.