Beveiligde toegang configureren met Secure Firewall Threat Defense voor privétoegang met op beleid gebaseerde routering

Inhoud

Inleiding

In dit document wordt beschreven hoe u Veilige toegang met FTD via IPsec configureert voor Veilige privétoegang met beleidsgebaseerde routering.

Voorwaarden

Vereisten

- Cisco Secure Access-kennis
- Cisco Secure Access-dashboard/tenant
- Kennis van het Secure Firewall Threat Defense and Firewall Management Center
- IPsec-kennis
- Beleidsgebaseerde routeringskennis

Gebruikte componenten

- Secure Firewall Running 7.7.10 code
- Het door de cloud geleverde Firewall Management Center. Configuratie is ook van toepassing voor de typische virtuele FMC
- Cisco Secure Access-dashboard

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.

Achtergrondinformatie

Netwerktunnels in Secure Access kunnen worden gebruikt voor twee primaire doeleinden: Secure Internet Access en Secure Private Access.

Voor Secure Private Access kunnen organisaties gebruikmaken van Zero Trust Access (ZTA) en/of VPN as a Service (VPNaaS) om gebruikers te verbinden met privébronnen zoals interne toepassingen of datacenters. IPsec-tunnels spelen een belangrijke rol in deze architectuur door het netwerkverkeer tussen gebruikers en privébronnen veilig te coderen en ervoor te zorgen dat gevoelige gegevens beschermd blijven terwijl ze door niet-vertrouwde netwerken gaan. Door IPsec-tunnels te integreren met ZTA of VPNaaS kunnen organisaties naadloze en veilige toegang bieden tot interne bronnen met behoud van robuuste beveiligingscontroles en zichtbaarheid.

In dit document wordt beschreven hoe u Secure Access configureert met Secure Firewall Threat Defense (FTD) via IPsec voor Secure Private Access.
Daarnaast bevat deze handleiding stappen voor het configureren van op beleid gebaseerde routering.

Hoewel dit document betrekking heeft op de configuratie van IPsec-tunnels voor beveiligde privétoegang, valt de installatie van Zero Trust Access (ZTA) of VPN as a Service (VPNaaS) voor toegang tot privétoepassingen buiten het toepassingsgebied van deze handleiding.

Configureren

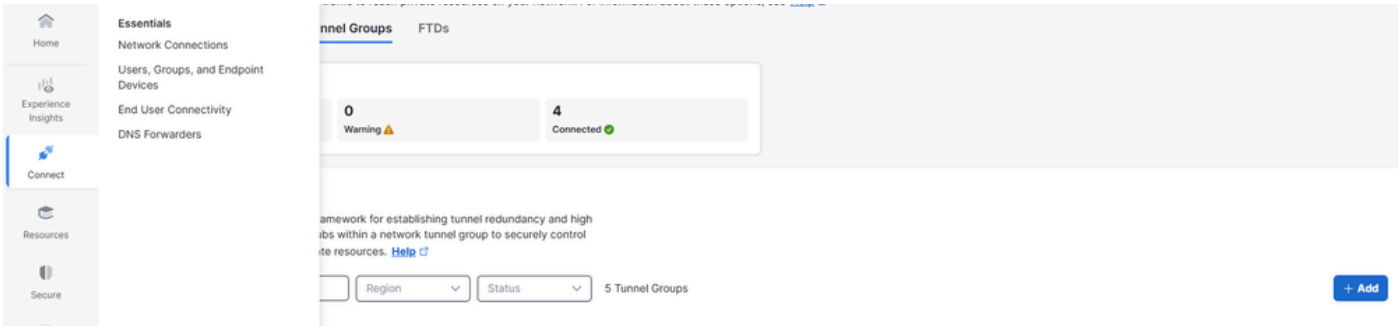
Beveiligde toegangsconfiguratie

Configuratie netwerktunnelgroep

1. Navigeer naar het beheerderspaneel van Secure Access.

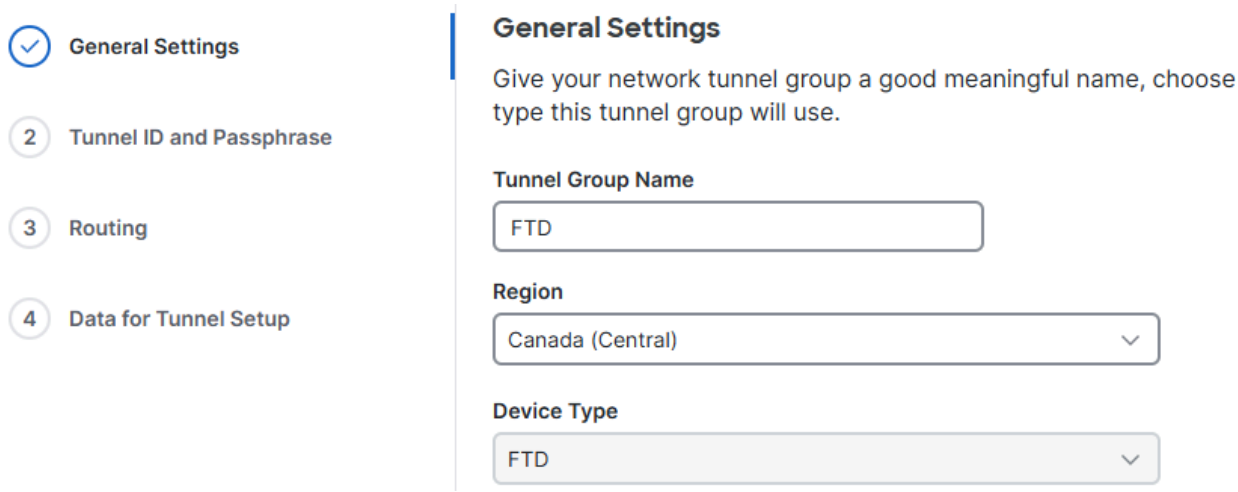
2. Voeg een netwerktunnelgroep toe.

- Klik opConnect> Network Connections
  - Klik onder Network Tunnel Groups op > Add



3. General Settings Configuratie.

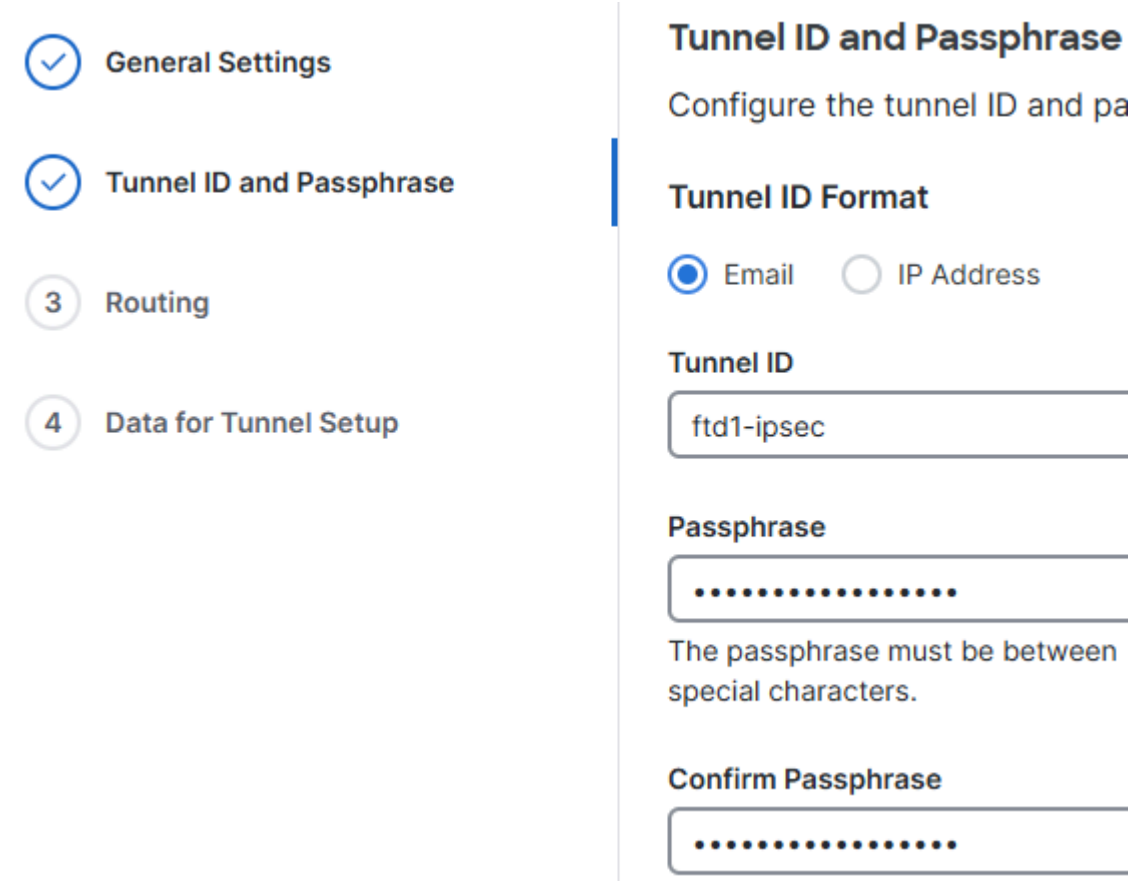
- Configureer de Tunnel Group Nameen **Region** de Device Type
  - Klik op de knop Next



Algemene instellingen

4. Configureren Tunnel ID en Passphraseinstellen.

- Configureer de **Tunnel ID**enPassphrase. Deze ID is belangrijk, omdat deze vereist is voor de FTD-configuratie
- Klik op Next



ID en PSK

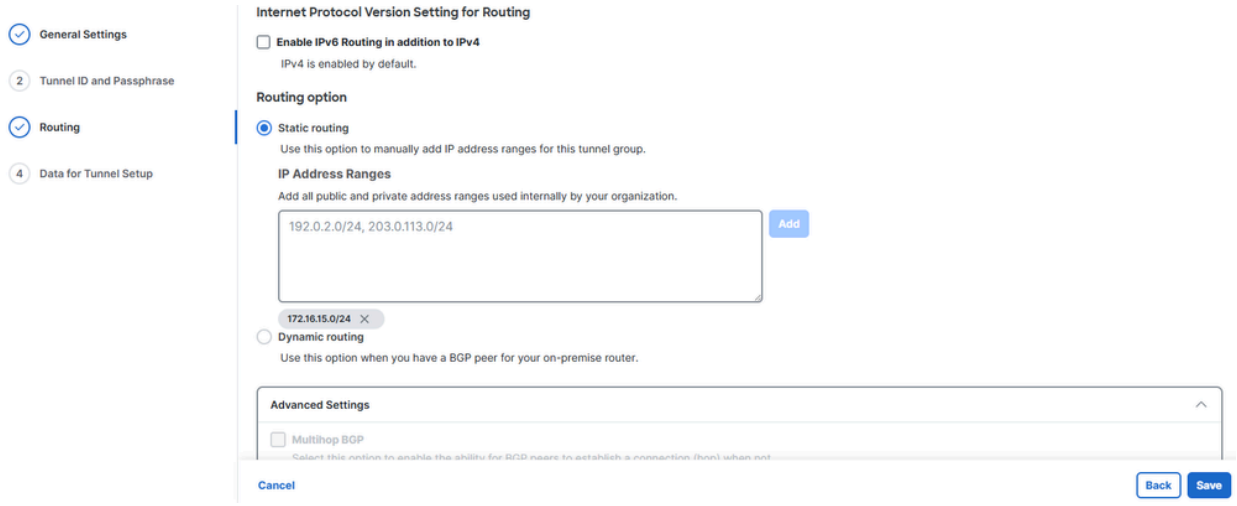
5. Statische routering configureren.

beveiligde toegangsroutering

op beleid gebaseerde routering

Voeg het netwerk (de netwerken) toe dat wordt beveiligd door de FTD en waartoe u externe gebruikers toegang wilt geven via ZTA en/of VPNaaS en klik op Opslaan.

- Klik op Routing> **Static routing**
  - Voeg de IP-adresbereiken of hosts toe die u in uw netwerk hebt geconfigureerd en die het verkeer via Secure Access willen doorgeven, en klik opAdd
  - Klik opSave

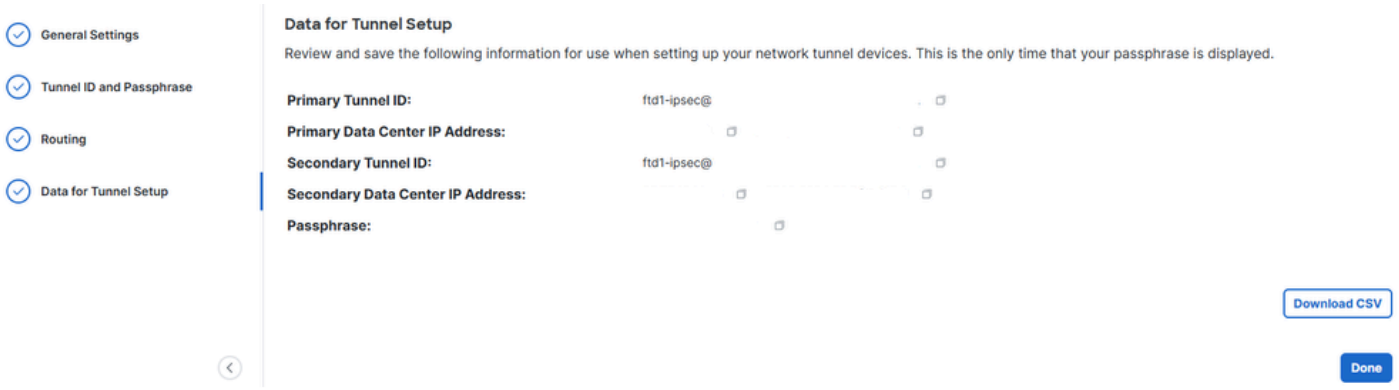


statische CSA-routering

Configuratie netwerktunnelgroep opslaan

Download en sla de tunnelinstallatiegegevens op, zoals deze nodig zijn voor de FTD-configuratie.

- Klik op Download CSV
- Klik op Done



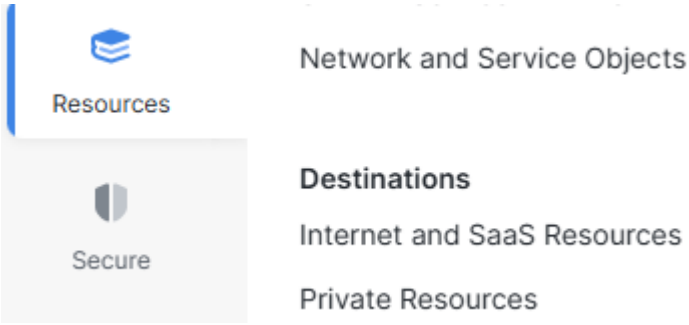
NTG-gegevens

Een privé-bron maken

Privébronnen zijn interne toepassingen, netwerken of subnetten die worden gehost in uw datacenter- of privécloudomgeving. Deze bronnen zijn niet openbaar toegankelijk en worden beschermd achter de infrastructuur van uw organisatie.

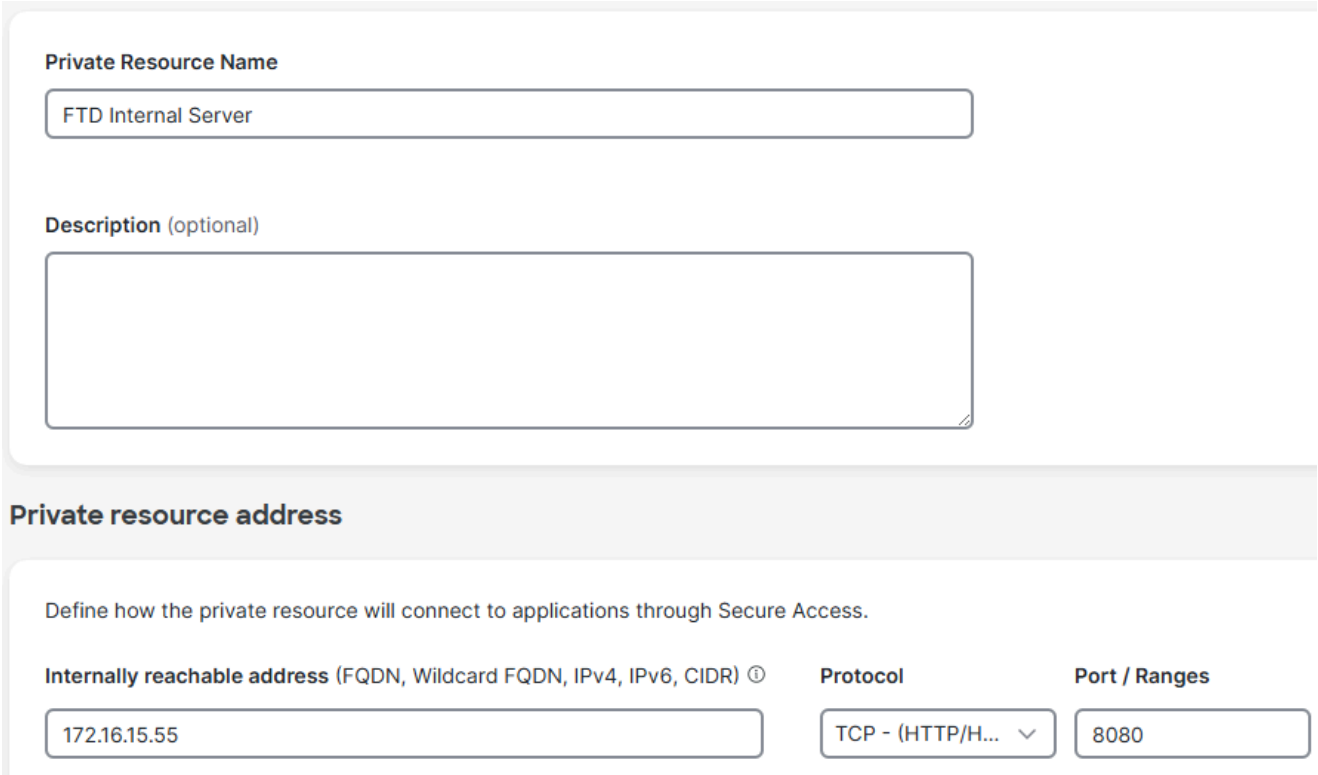
Door ze te definiëren als Private Resources in Secure Access, kunt u gecontroleerde toegang inschakelen via oplossingen zoals Zero Trust Access (ZTA) of VPN as a Service (VPNaaS). Dit zorgt ervoor dat gebruikers veilig verbinding kunnen maken met interne systemen op basis van identiteit, apparaathouding en toegangsbeleid, zonder de bronnen rechtstreeks aan het internet bloot te stellen.

Navigeer naar **Resources** > **Private Resources**> klik opAdd.



PR

- Specificeer de **Private Resource Name**, Internally reachable address, Protocol, Port/Ranges. Geef poorten en protocollen op en voeg indien nodig extra privébronnen toe
- Selecteer de gewenste verbinding Connection Method op basis van uw behoefte, bijvoorbeeld Zero-trust-verbindingen en/of VPN-verbindingen, volgens uw vereisten
- Klik op Save



particuliere hulpbron

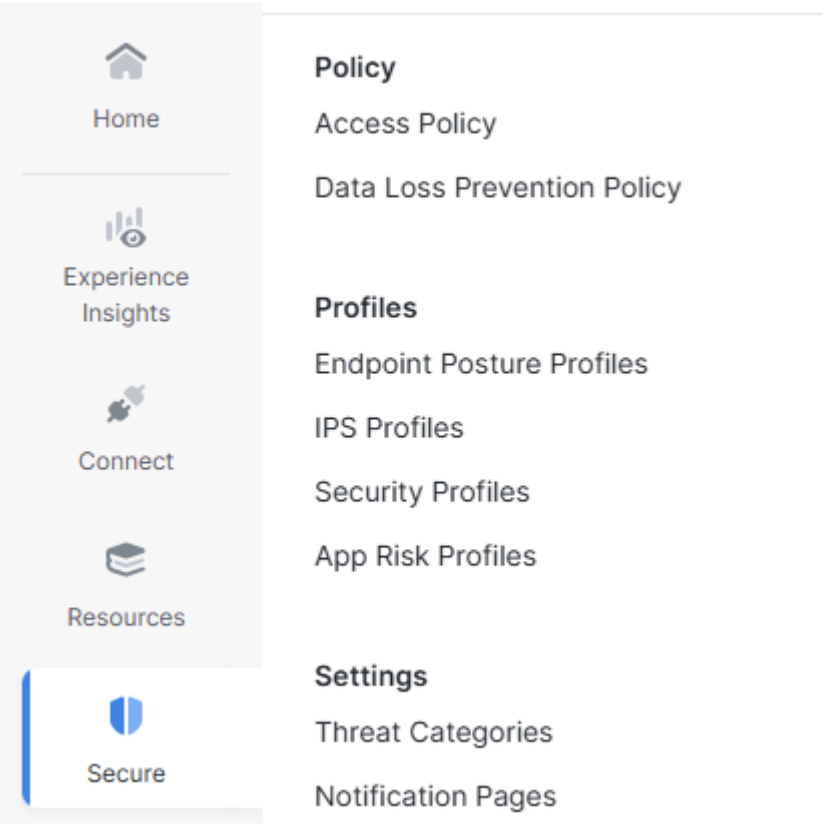
Een regel voor toegangsbeleid maken

Privé-toegangsregels bepalen hoe gebruikers veilig verbinding kunnen maken met interne bronnen en toepassingen die niet openbaar toegankelijk zijn.

Deze regels handhaven de beveiliging door te bepalen wie toegang heeft tot specifieke privébronnen op basis van factoren zoals gebruikersidentiteit, groepslidmaatschap, apparaathouding, locatie of andere beleidsvoorwaarden. Dit zorgt ervoor dat gevoelige interne systemen beschermd blijven tegen algemene publieke toegang, terwijl ze nog steeds veilig

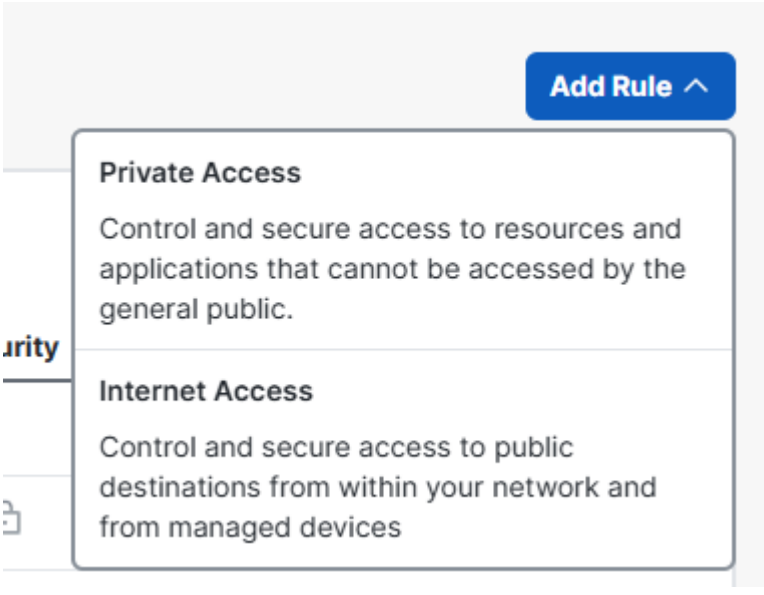
beschikbaar zijn voor geautoriseerde gebruikers via ZTA of VPNaaS.

Navigeer naar Secure>Access Policy



ACS

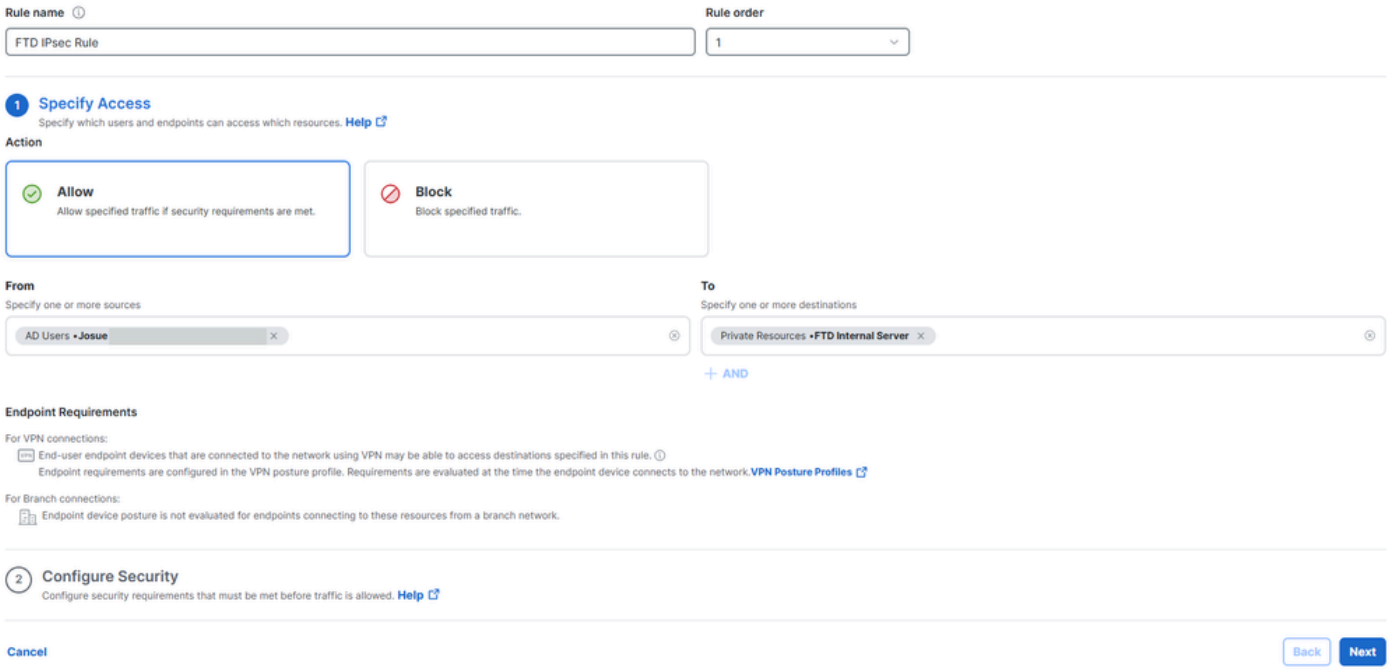
- Klik op Add Rule
  - Klik op Private Access



ACP toevoegen

- Klik erop Rule Name en geef het een naam

- Klik opActionen selecteer Allowom dit verkeer toe te staan
- KlikFromop en geef de gebruikers op die toestemming hebben gekregen
- Klik op Toen geef de toegang op die gebruikers hebben op basis van deze regel
- Klik opNexten dan Saveop de volgende pagina



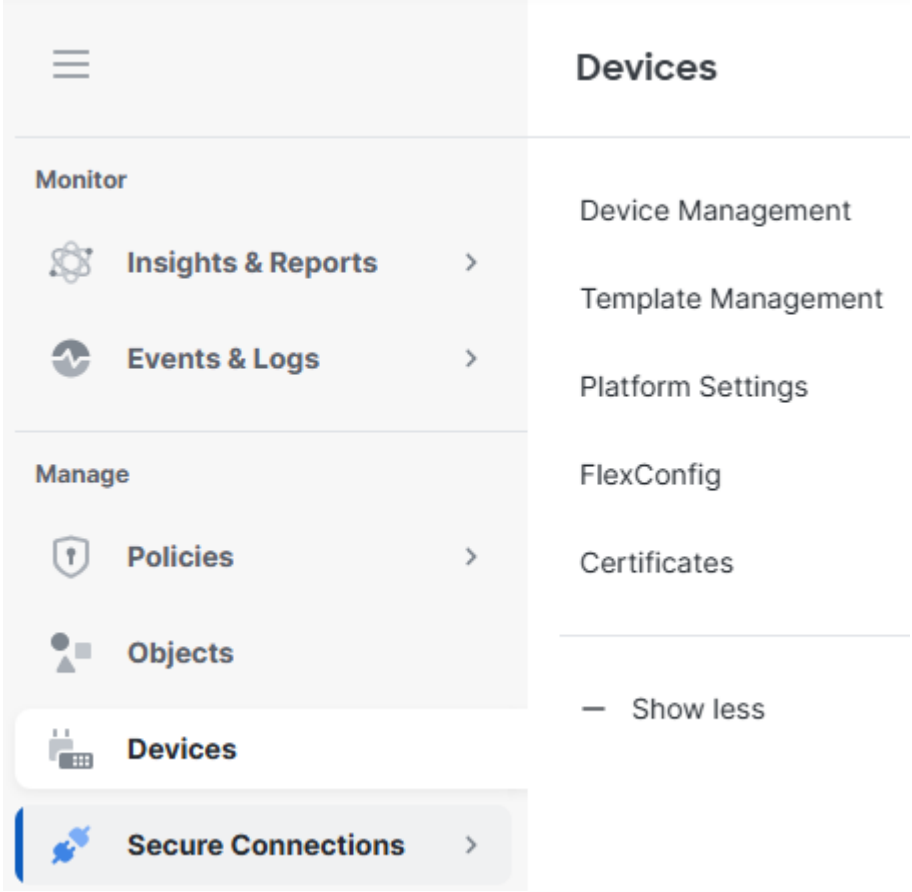
ACS-configuratie

Beveiligde Firewall Threat Defense (FTD)-configuratie

Configuratie van virtuele tunnelinterfaces

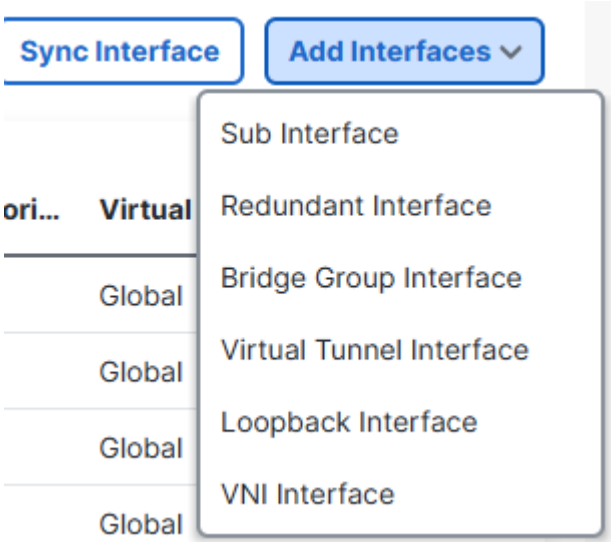
Een Virtual Tunnel Interface (VTI) op FTD is een logische Layer 3-interface die wordt gebruikt om routegebaseerde IPsec VPN-tunnels te configureren.

1. Navigeer naar Devices> Device Management.



FTD-apparaten

- Klik op het FTD-apparaat, Interfaces
  - Klik op Add Interfaces
  - Klik op Virtual Tunnel Interface
  - Maak twee Virtual Tunnel Interfaces, één voor de primaire beveiligde toegangshub en een andere voor de secundaire beveiligde toegangshub

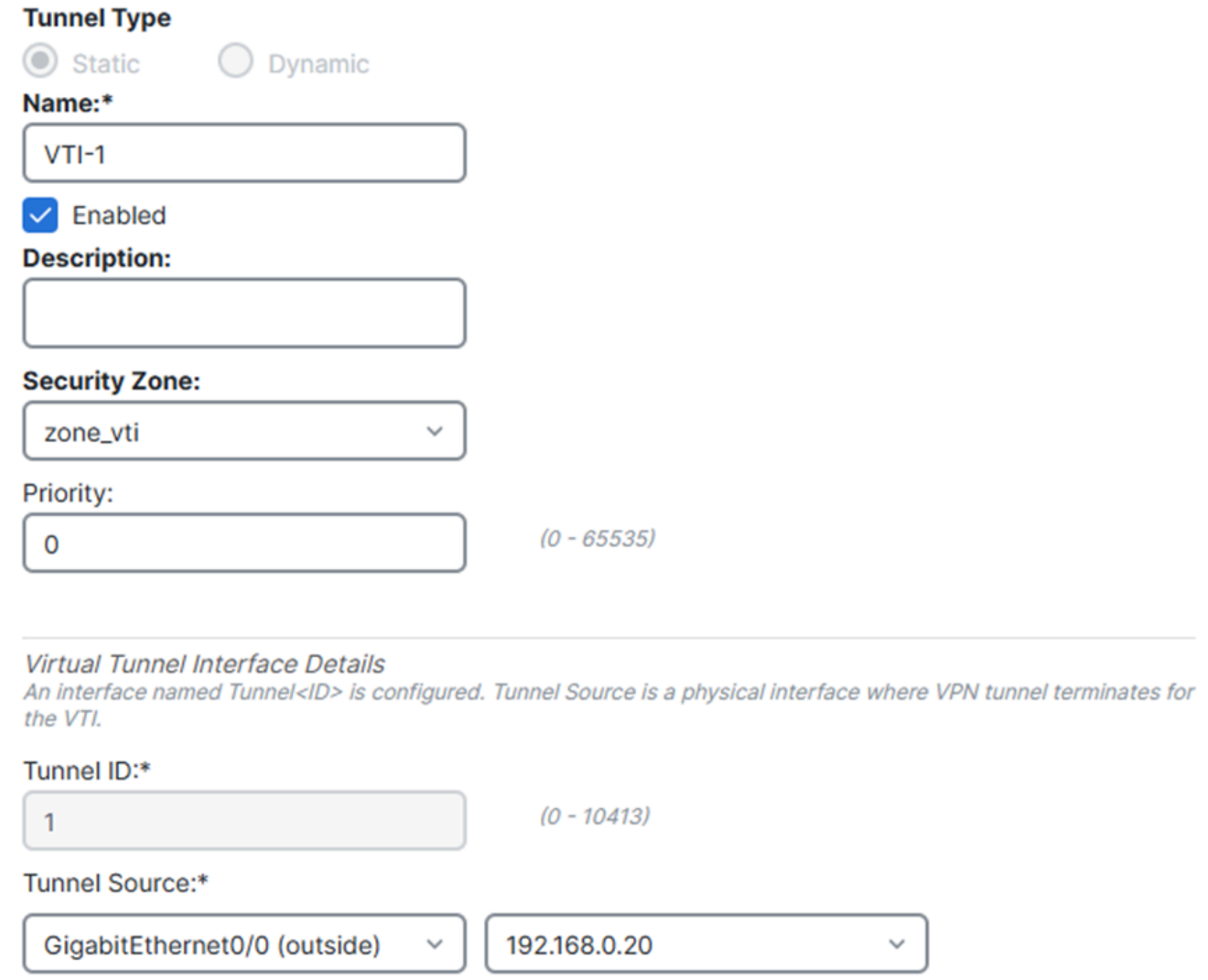


VTI's toevoegen

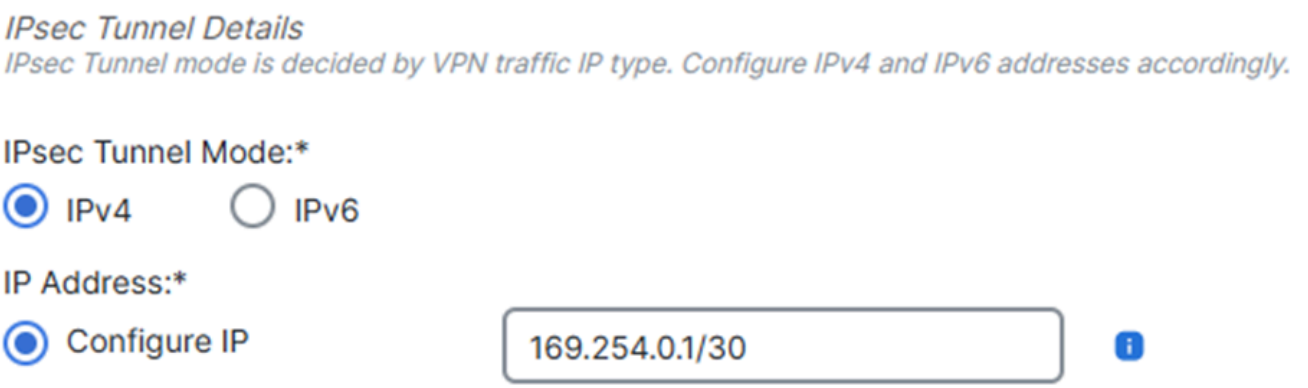
Virtual Tunnel Interface 1:

- Geef het een naam, klik op Enable

- Selecteer of maak een Security Zone
- Klik erop Tunnel ID en geef het een waarde.
- Klik op en specificeer Tunnel Source de WAN-interface van waaruit de tunnel wordt ingesteld
- Klik op IPsec Tunnel Modeen selecteerIPv4
- Klik op IP Address en configureer het IP-adres voor de VTI
- Klik opOK



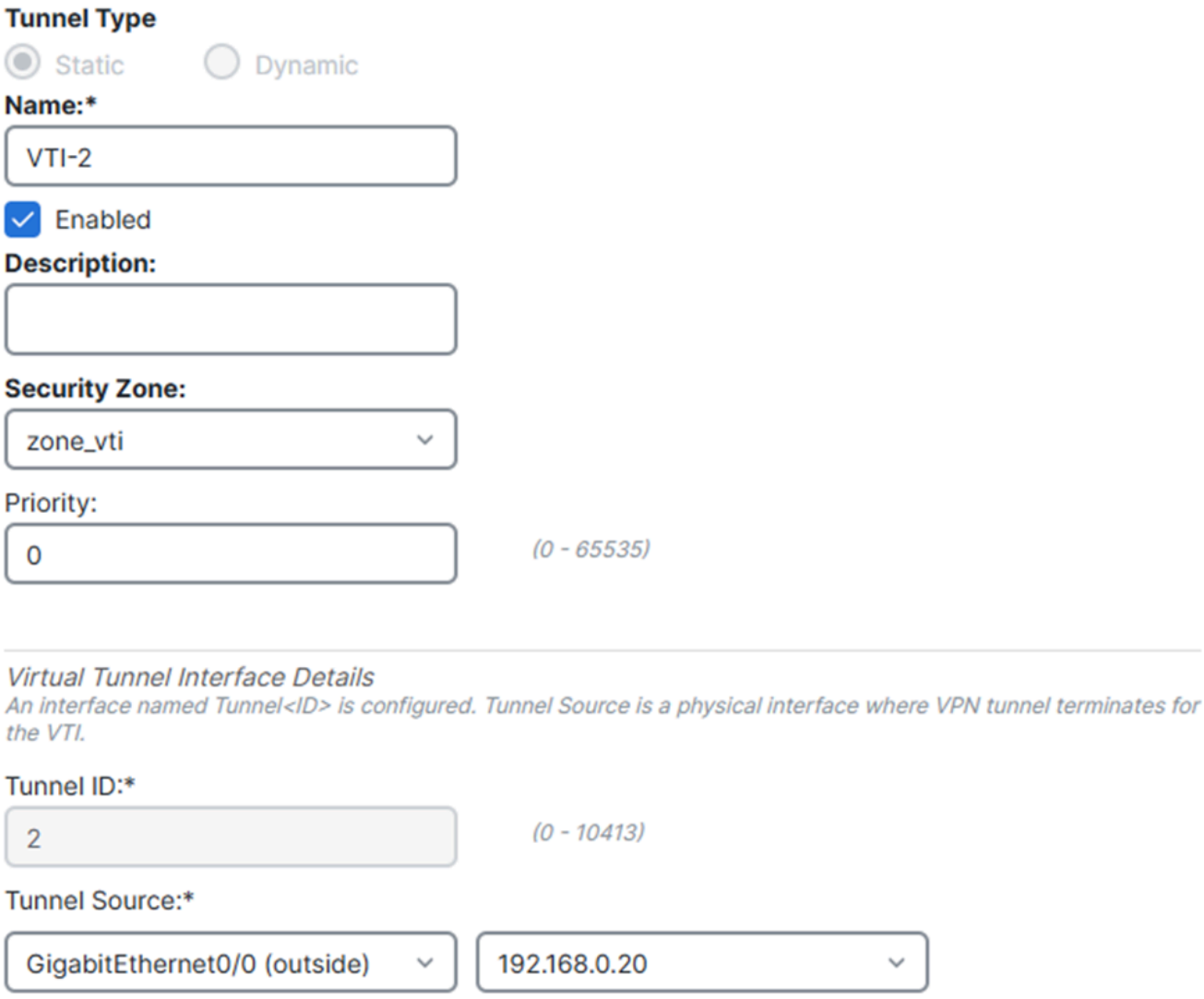
VTI1,1



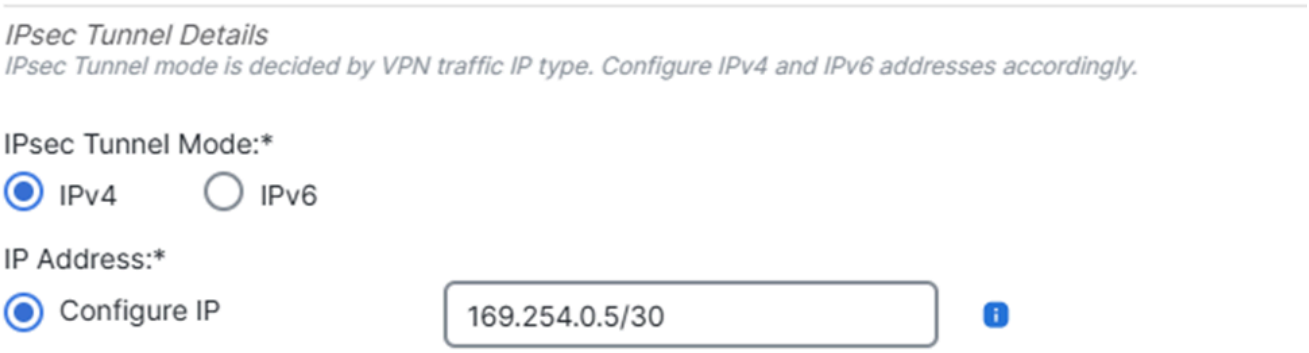
VTI1,2

Virtual Tunnel Interface 2:

- Geef het een naam, klik op Enable
- Selecteer of maak een Security Zone
- Klik erop Tunnel ID en geef het een waarde
- Klik op en specificeer Tunnel Source de WAN-interface van waaruit de tunnel wordt ingesteld
- Klik op IPsec Tunnel Modeen selecteerIPv4
- Klik op IP Address en configureer het IP-adres voor de VTI
- Klik opOK

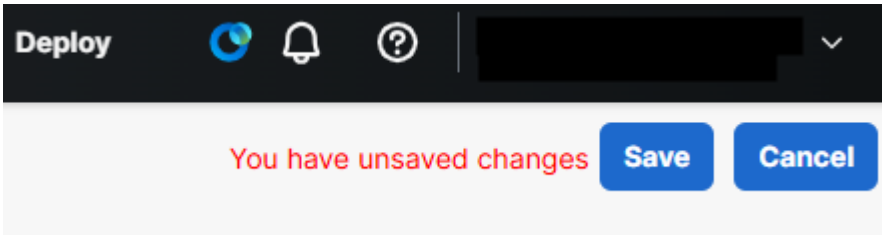


VTI2,1



VTI2,2

- Klik op Opslaan.

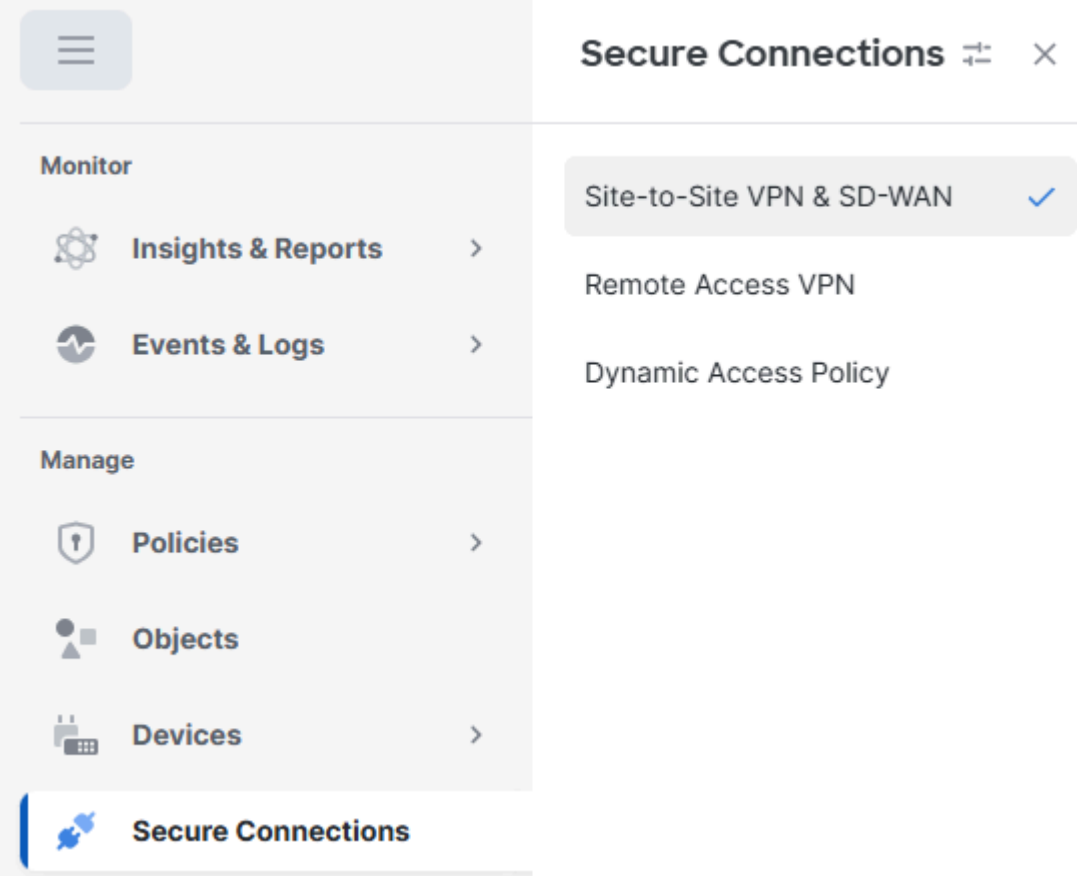


VTI-wijzigingen opslaan

IPsec-tunnelconfiguratie

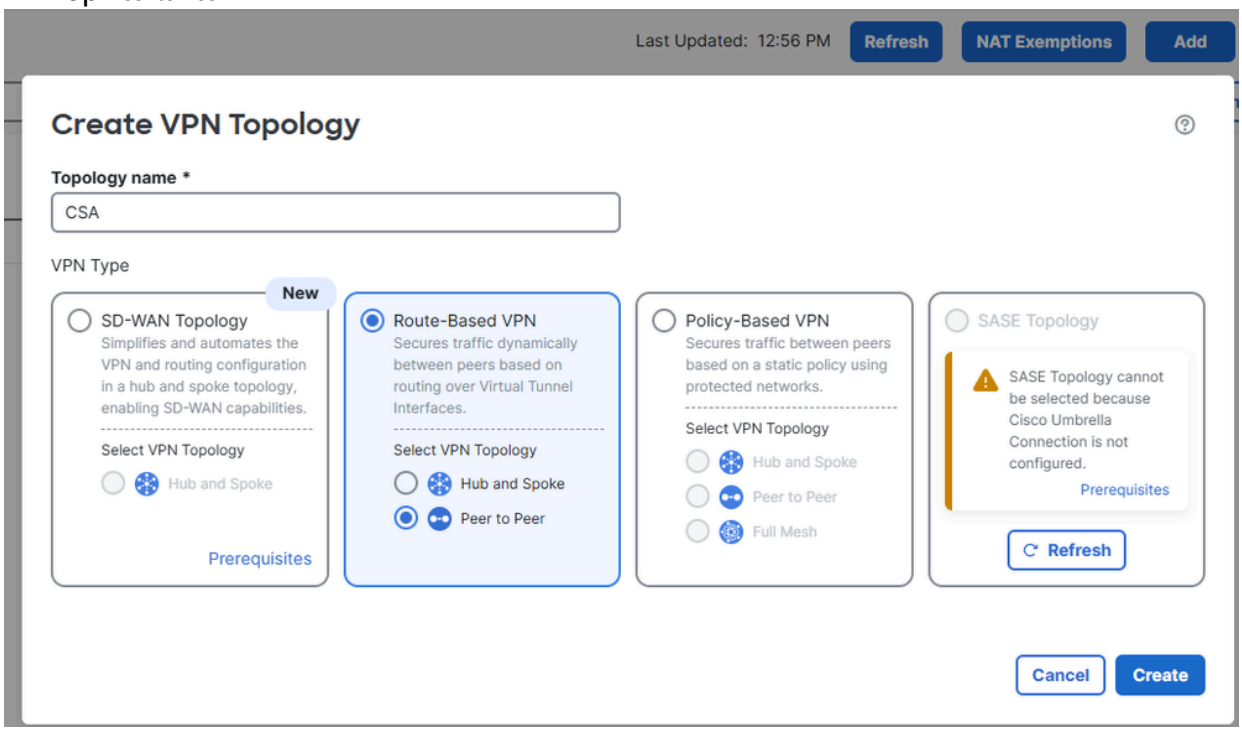
Navigeer naar uw cdFMC-dashboard.

- Klik op Secure Connection> Site-to-Site VPN & SD-WAN



S2S

- Klik opAdd
  - Klik op Route-Based VPN
  - Klik op Peer to Peer

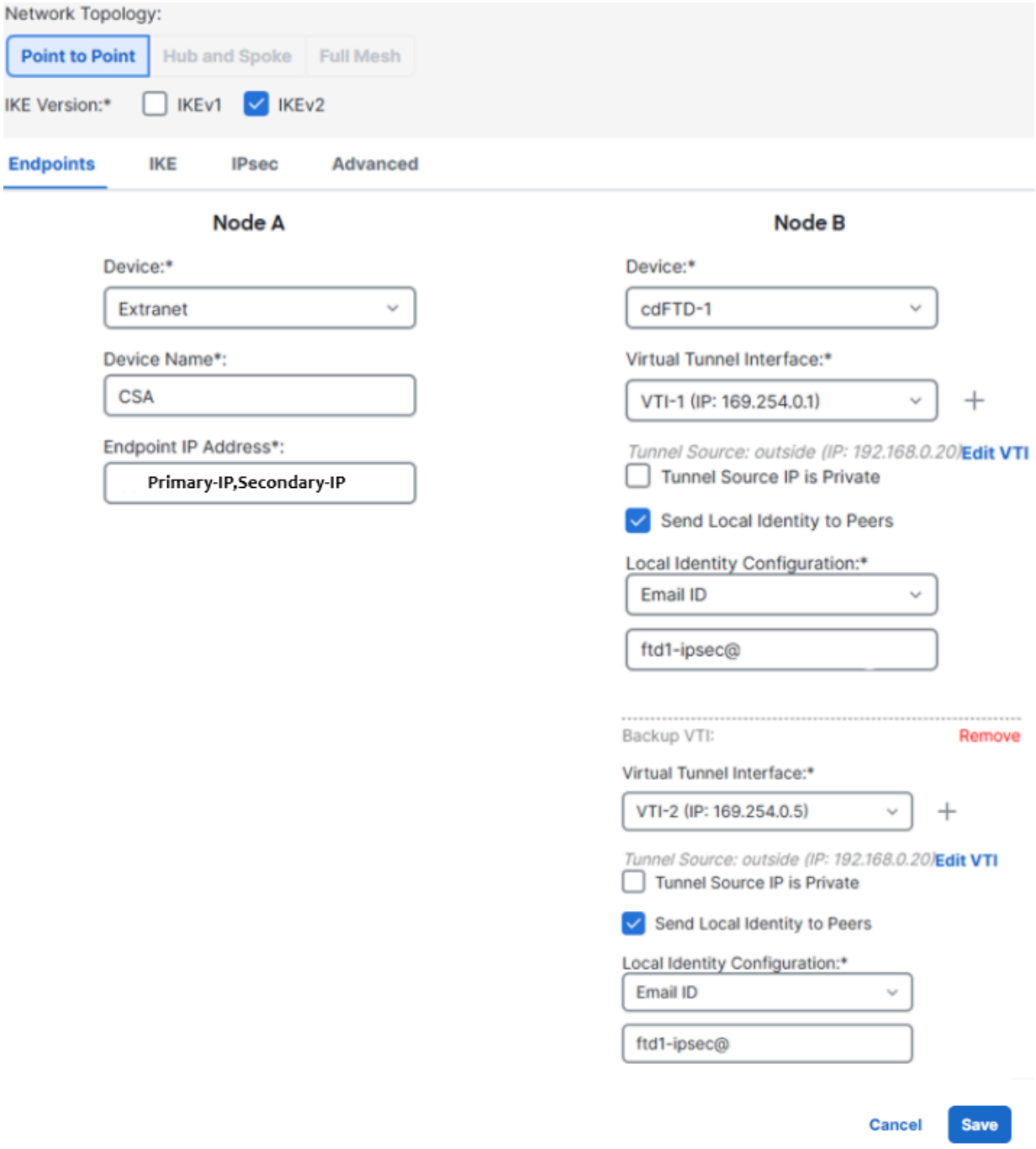


VPN toevoegen

- Verzamel in stap 5 van de Secure Access-configuratie de tunnel-ID's en IP-adressen voor de

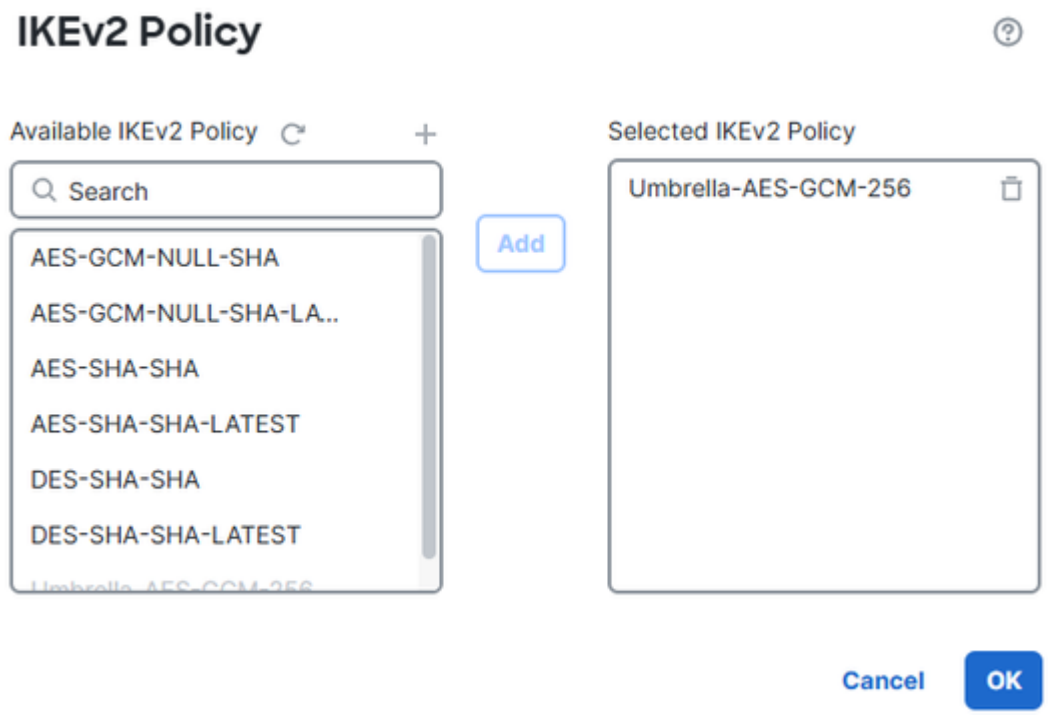
primaire en secundaire datacenters

- Klik opEndpoints
  - Klik onderNode Aaan enDeviceselecteer Extranet
  - Klik op Device Nameen geef het een naam
  - Klik op Enpoint IP Addresses en voer de primaire en secundaire IP-adressen voor beveiligde toegang in, gescheiden door een komma (van "Configuratie netwerktunnelgroep opslaan" onder de optie Beveiligde toegang)
    Configuratie)
  - Klik onder Node Baan Deviceen selecteer uw FTD-apparaat
  - Klik op Virtual Tunnel Interface en selecteer de eerste VTI-interface die in de vorige stap is gemaakt
  - Klik op de optie Send Local Identity to Peers en selecteer Email ID, voer de primaire tunnel-ID in (van "Save Network Tunnel Group Configuration" onder de Secure Access Configuration)
  - Klik op Add Backup VTI
  - Klik op Virtual Tunnel Interface en selecteer de tweede VTI-interface die in de vorige stap is gemaakt
  - KlikSend Local Identity to Peersop optie en selecteer Email ID, voer de secundaire tunnel-ID in (van "Save Network Tunnel Group Configuration" onder de Secure Access Configuration)
  - Klik op Opslaan



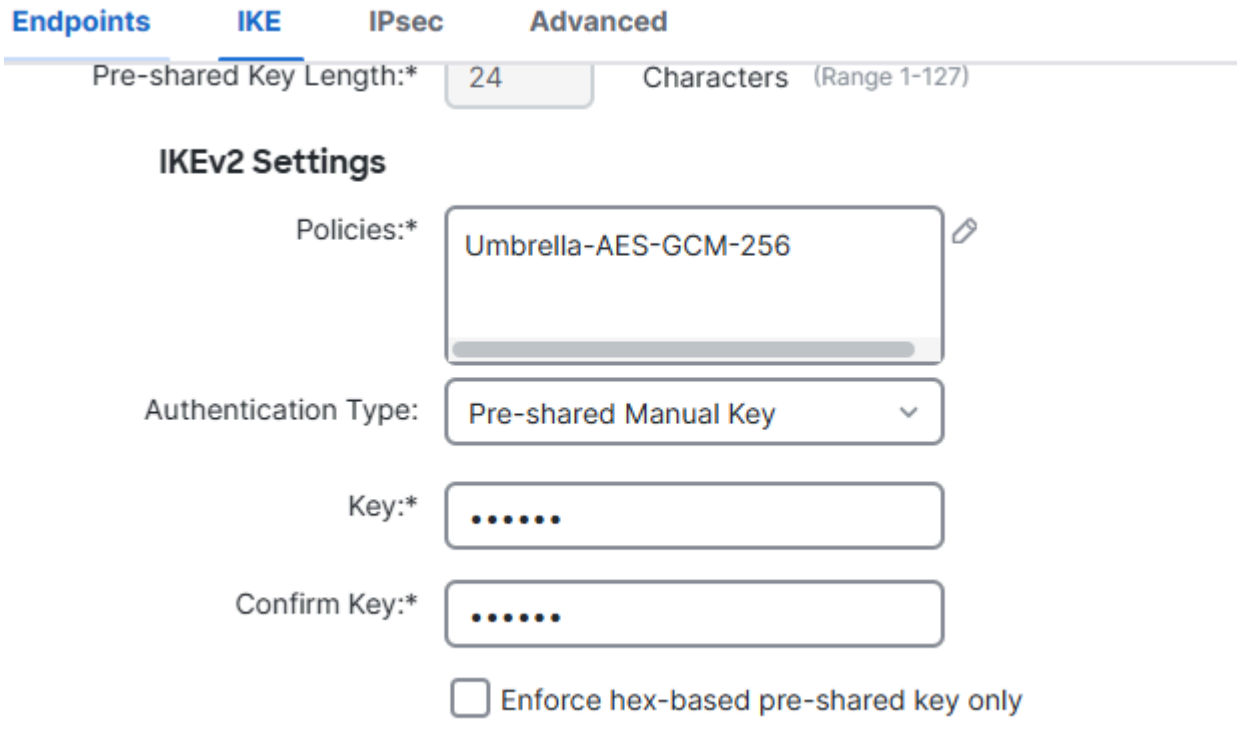
FTD VTI-configuratie

- Klik opIKE
  - Klik op **IKEv2 Settings >** Policies
  - Selecteer deUmbrella-AES-GCM-256optie
  - Klik op OK



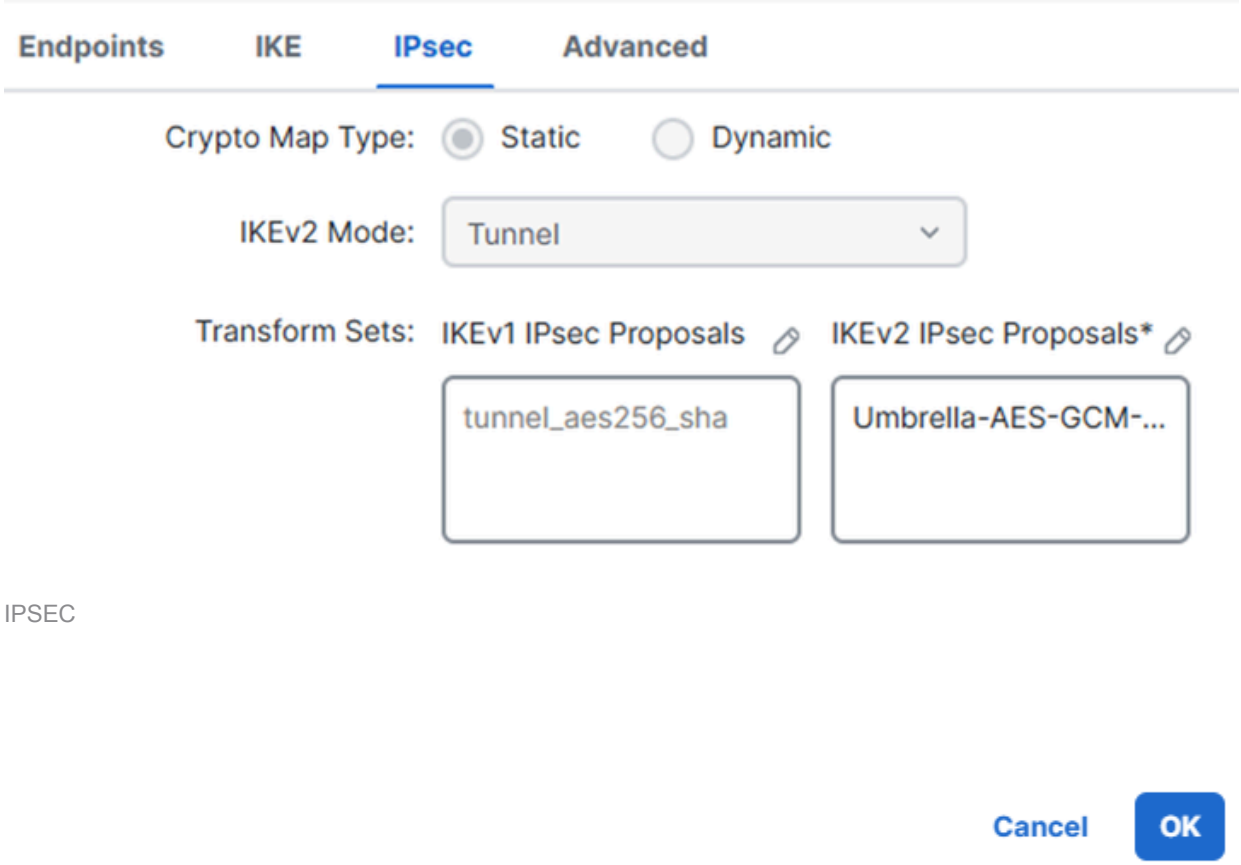
IKEv2-beleid

- Klik op Authentication Type en selecteerPre Shared Manual Keyde PSK die is geconfigureerd in Secure Access (wachtwoordgroep)



IKE

- Klik op IPSEC
  - Klik op IKEv2 Proposals
  - selecteren Umbrella-AES-GCM-256
  - Klik op OK



IKEv2-voorstellen opslaan

FTD-routeringsconfiguratie

Met Policy-Based Routing (PBR) kunt u het doorsturen van verkeer beheren op basis van criteria die verder gaan dan alleen het IP-adres van de bestemming. In plaats van alleen te vertrouwen op de routeringstabel, kan PBR verkeer routeren op basis van bron, toepassing, protocol, poorten of ander gedefinieerd beleid.

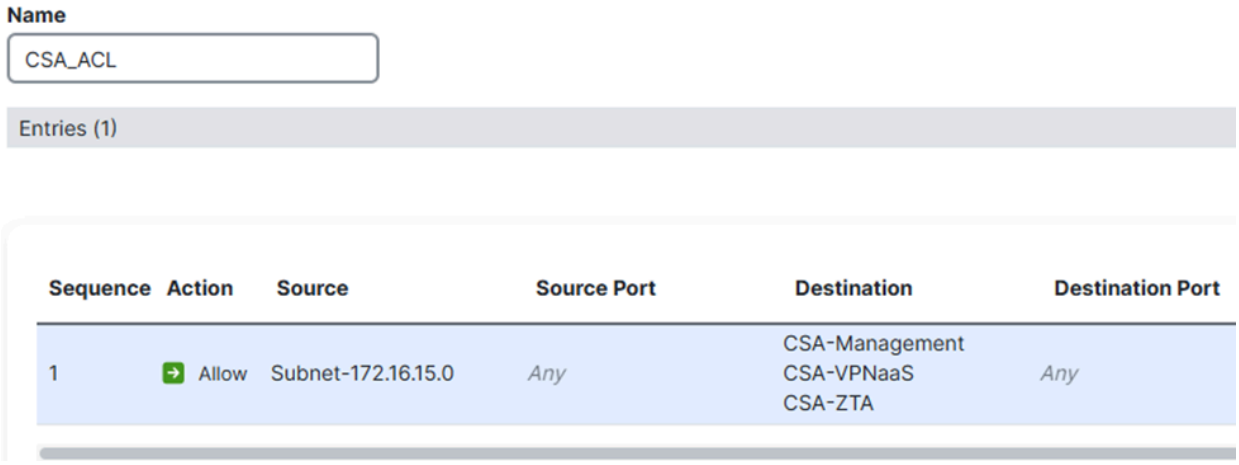
Dit stelt organisaties in staat om specifiek of hoog prioritair verkeer via voorkeurslinks te sturen (zoals een hoge bandbreedte of directe internetlink), de prestaties te optimaliseren en geselecteerde applicaties veilig uit te breken zonder al het verkeer door een VPN-tunnel te sturen.

op beleid gebaseerde routering

- Navigeer naarObjects
  - Klik op Access List
  - Klik op Extended
  - Klik opAdd Extended Access List

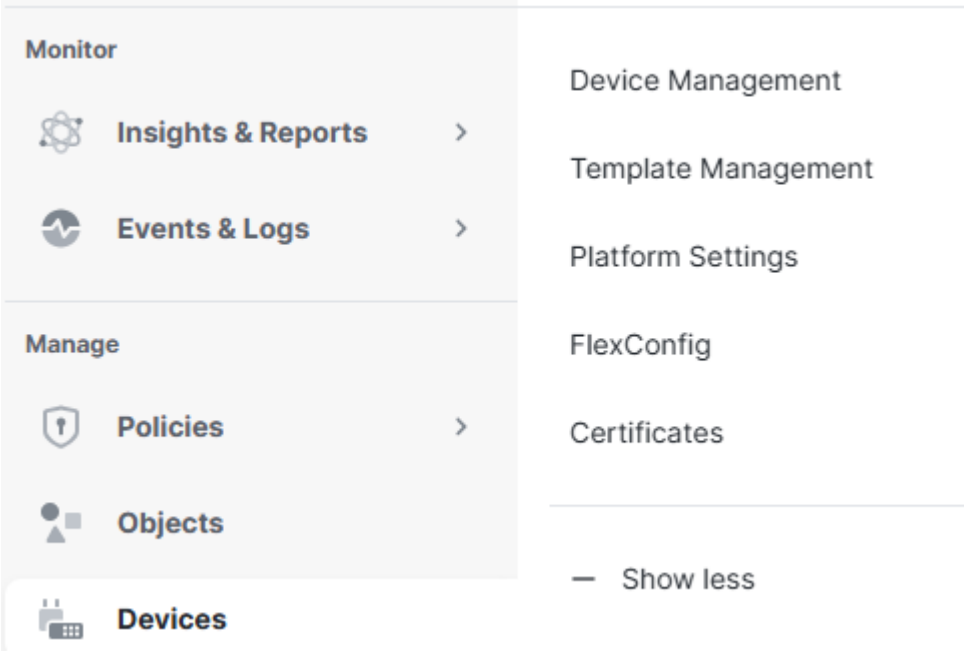
ACL toevoegen

Maak een uitgebreide toegangscontrolelijst (ACL) die overeenkomt met uw bronnetwerk dat wordt beschermd door de FTD (bijvoorbeeld 172.16.15.0/24) om door de tunnel te worden verzonden. Voeg voor de bestemming de netwerken toe die worden gebruikt door ZTA (CGNAT-bereik) en het netwerk dat wordt gebruikt door uw VPNaaS (controleer Virtual Private Network IP Pool).



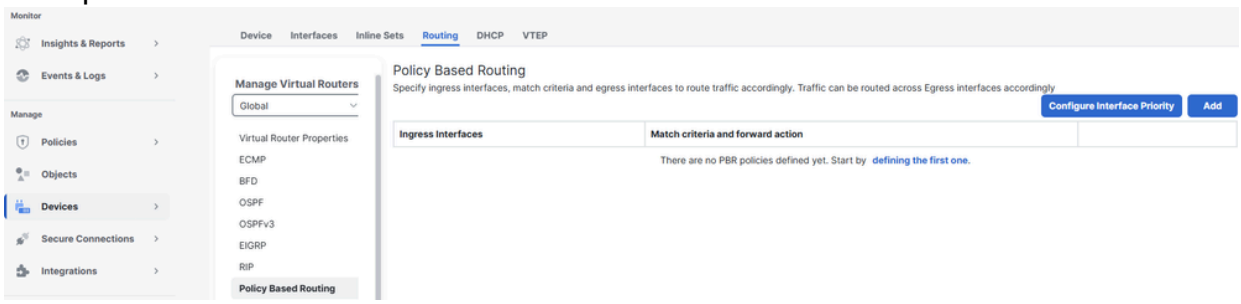
ACL

- Klik op Devices> Device Management



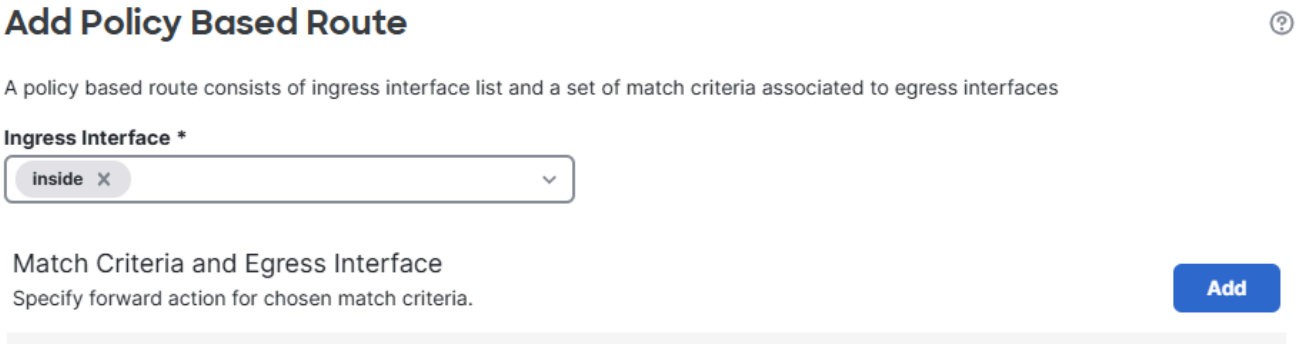
Apparaat

- Klik op de FTD
  - Klik opRouting
  - Klik op Policy Based Routing
  - Klik op Add



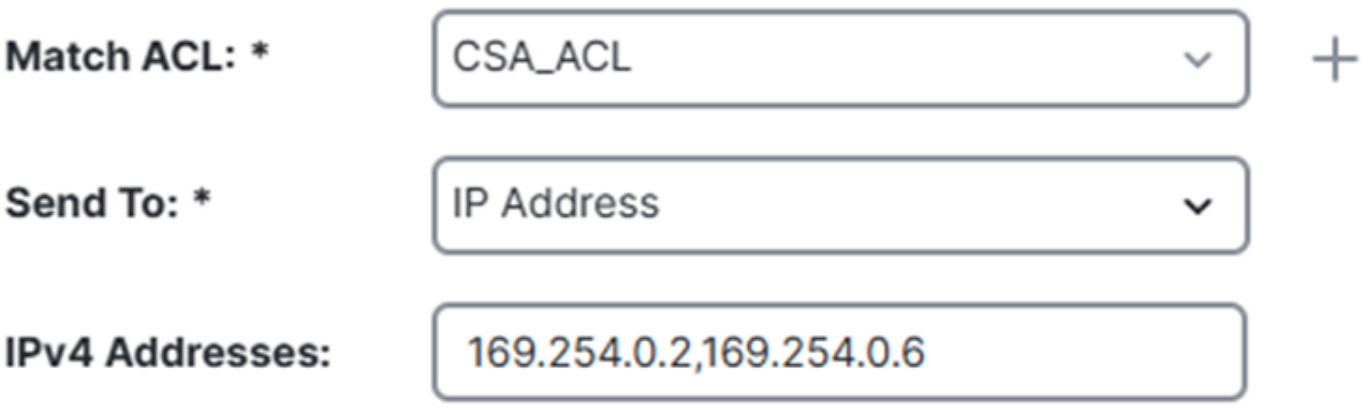
PBR toevoegen

- Klik op Ingress Interface en selecteer de ingangsinterface waar verkeer van interne netwerken binnenkomt
- Klik onder Overeenstemmingscriteria en Uitgangs-interface op Add



Ingress-interface

- Klik op Match ACL en selecteer de uitgebreide ACL die eerder is gemaakt
- Klik op Send To and select IP Address
- Klik op IPv4 Addresses en stel als volgende stappen de IP-adressen in de VTI-interfacesubnetten in die eerder in de FTD zijn geconfigureerd (169.254.0.2 en 169.254.0.6)
- Klik op Save



PBR opslaan

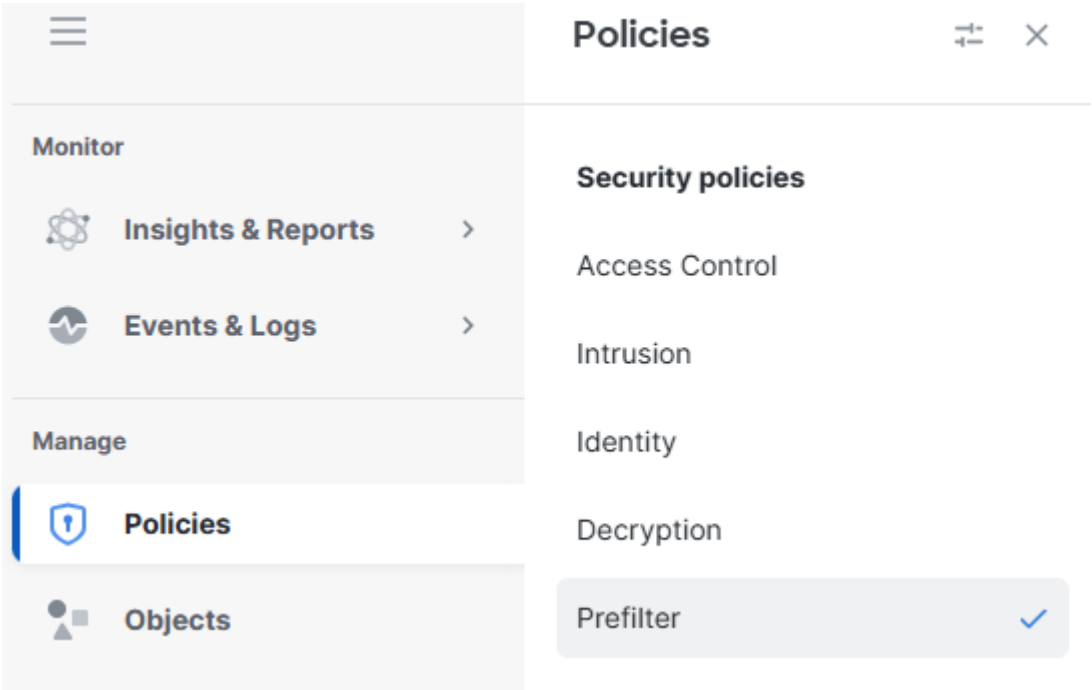
Selecteer de optie Send To > IP Address en niet de Egress Interface optie.

Configuratie toegangsbeleid

Om verkeer op een Cisco Firepower Threat Defense (FTD) mogelijk te maken en toegang tot privébronnen mogelijk te maken, moet het verkeer eerst door de eerste fase van toegangscontrole gaan die bekend staat als Prefiltering.

Prefiltering wordt verwerkt voordat diepere inspectie plaatsvindt en is ontworpen om eenvoudig en snel te zijn. Het evalueert verkeer met behulp van basis-criteria voor de buitenste koptekst (zoals bron- en bestemmings-IP-adressen en -poorten) om snel verkeer toe te staan, te blokkeren of te omzeilen. Wanneer verkeer in dit stadium is toegestaan, kan het meer resource-intensieve inspecties zoals diepe pakketinspectie of inbraakbeleid overslaan, waardoor de prestaties worden verbeterd terwijl de beveiligingscontrole behouden blijft.

- Navigeer naar Policies> Prefilter

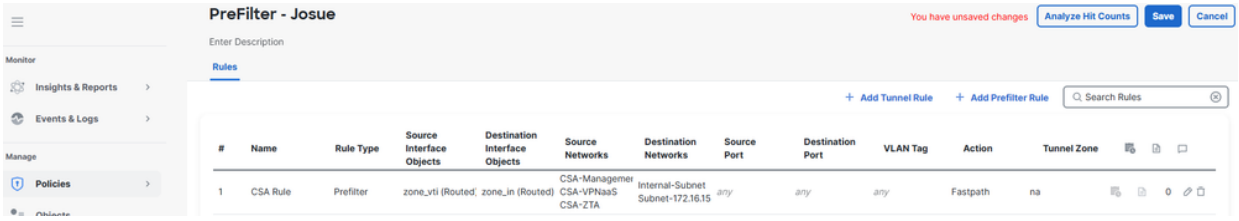


voorfilter

- Klik op het beleid Voorfilter bewerken dat wordt gebruikt in uw toegangsbeleid

Klik op Prefilter

- Klik op Add Tunnel Rule
  - Voeg het verkeer van het VPNaaS-netwerk en/of het ZTA-subnet toe aan uw privébronnen
  - Klik opSave



Regel opslaan

Zodra de configuratie op de FTD is voltooid en geverifieerd, kunt u doorgaan met de implementatie. Na de implementatie komen de IPsec-tunnels met succes tevoorschijn, wat bevestigt dat een veilige verbinding met de privébronnen tot stand is gebracht.

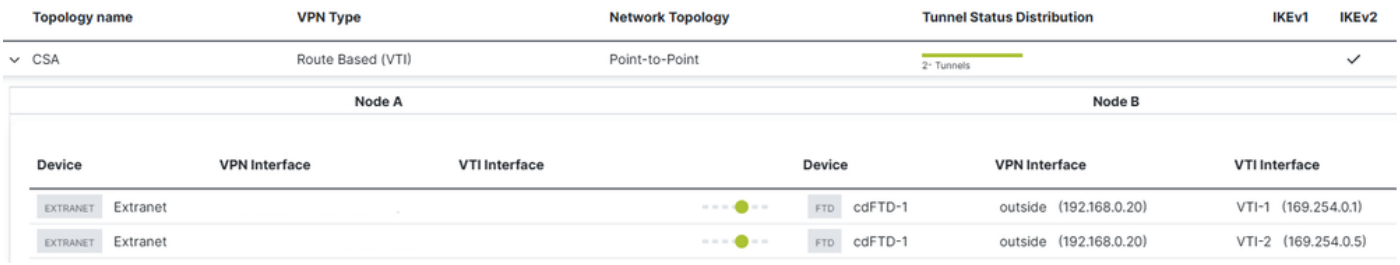
Verifiëren

Controleren in FTD

De tunnelstatus in FTD

U kunt de huidige status van de tunnel bekijken, inclusief of deze omhoog of omlaag is. Dit helpt om te controleren of de IPsec-tunnel correct is ingesteld.

- Klik op Beveiligde verbindingen.
- Klik op Site-to-Site VPN en SD-WAN.
- Klik op de naam van de topologie.



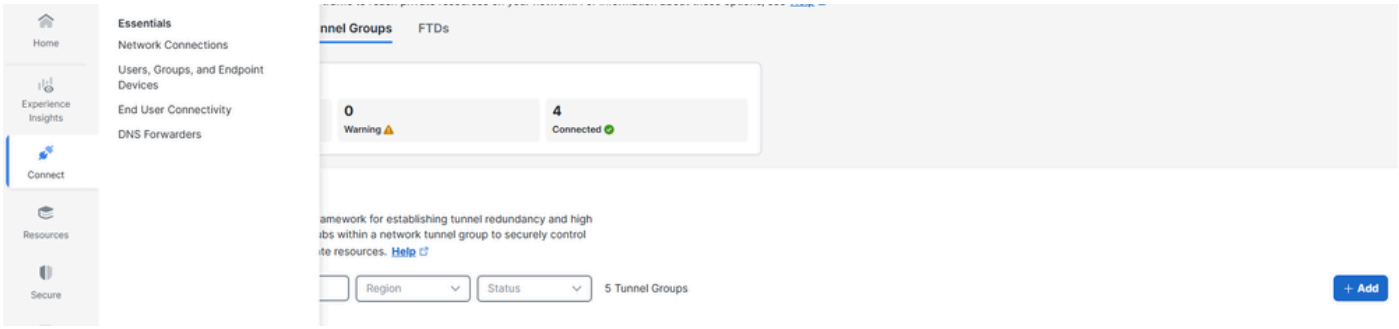
FTD-tunnelstatus

Verifiëren bij beveiligde toegang

Tunnel Status in Veilige Toegang

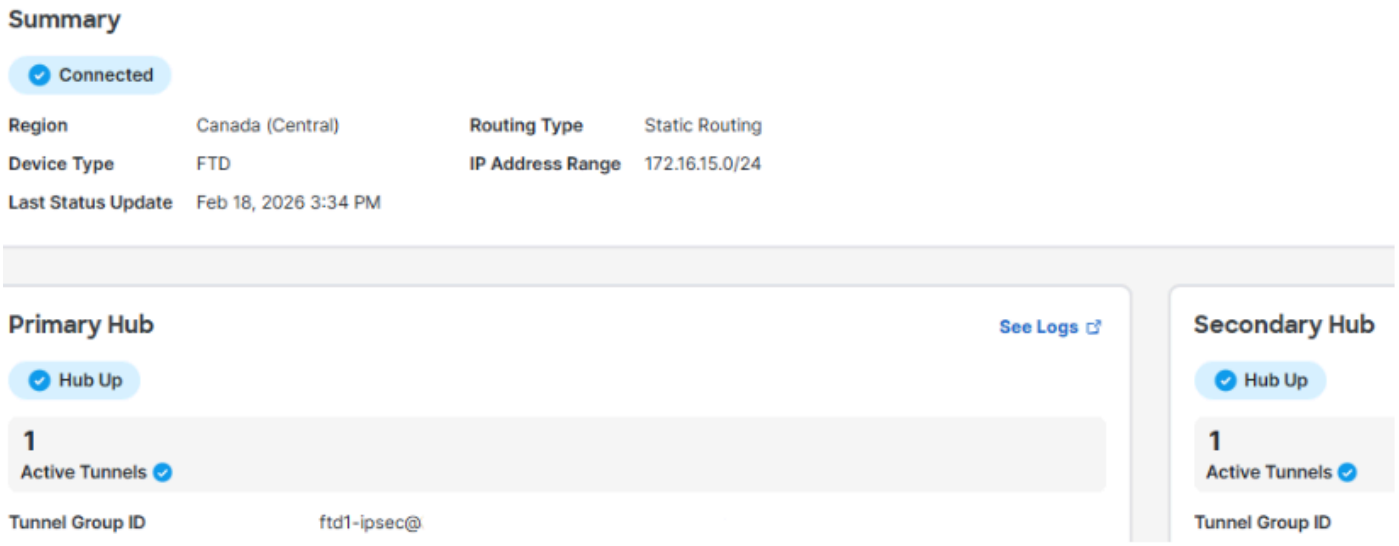
U kunt de huidige status van de tunnel bekijken, inclusief of de tunnel is losgekoppeld, gewaarschuwd of verbonden. Dit helpt om te controleren of de IPsec-tunnel correct is ingesteld.

- Klik op Verbinden > Netwerk verbindingen
- Klik op Network Tunnel Groups



NTG controleren

- Klik op de Netwerktunnelgroep

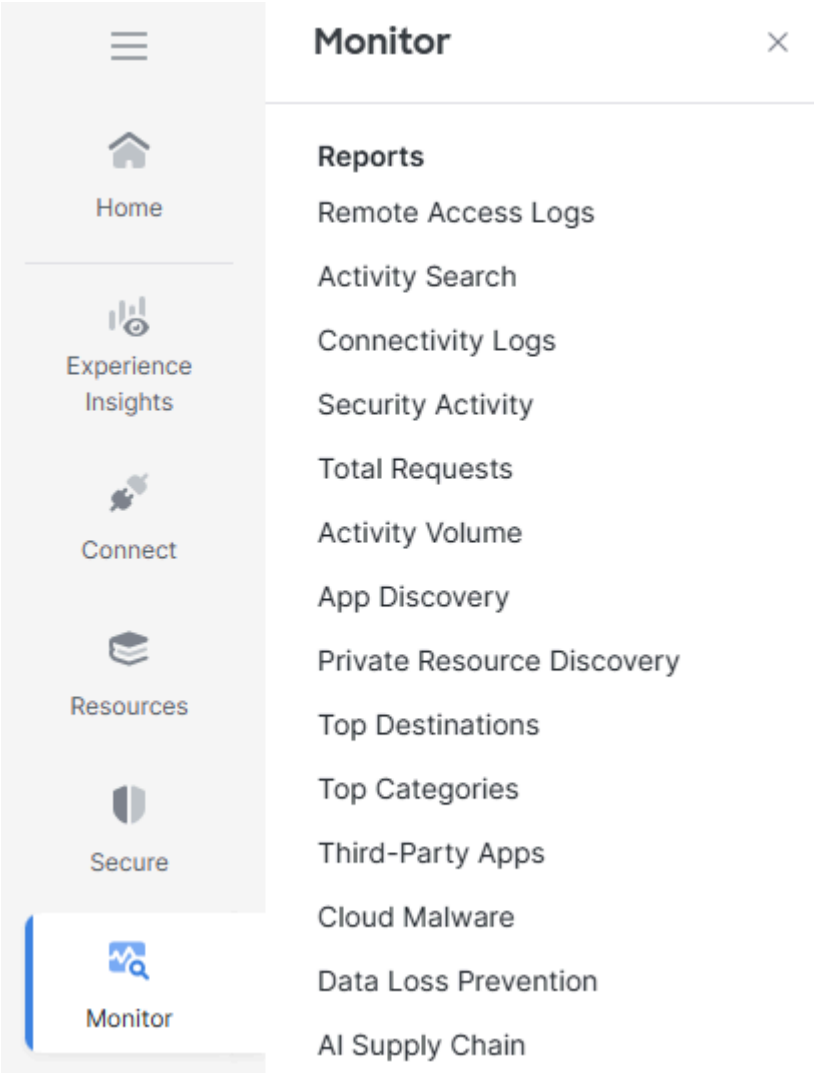


CSA-tunnelstatus

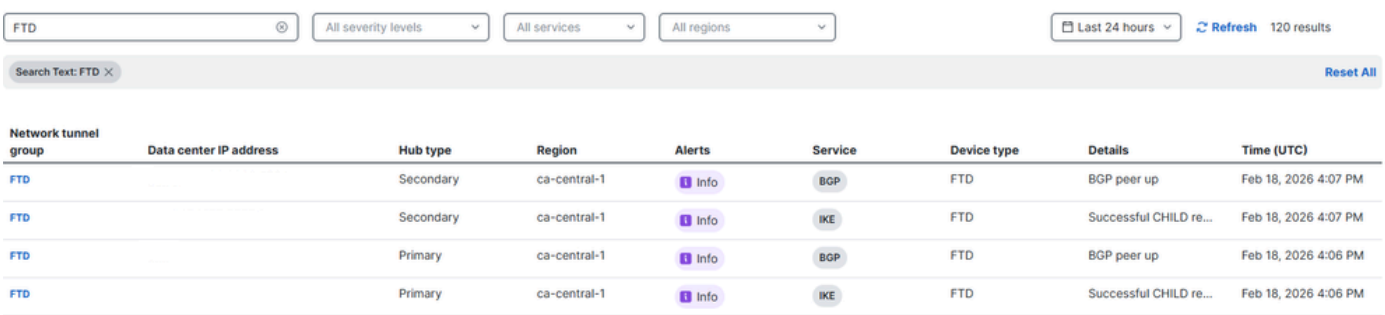
Evenementen in Secure Access

U kunt tunnelgebeurtenissen bekijken en bevestigen of de status van de IPsec-tunnels is ingesteld en stabiel is.

Klik op Monitor > Netwerk connectiviteit.

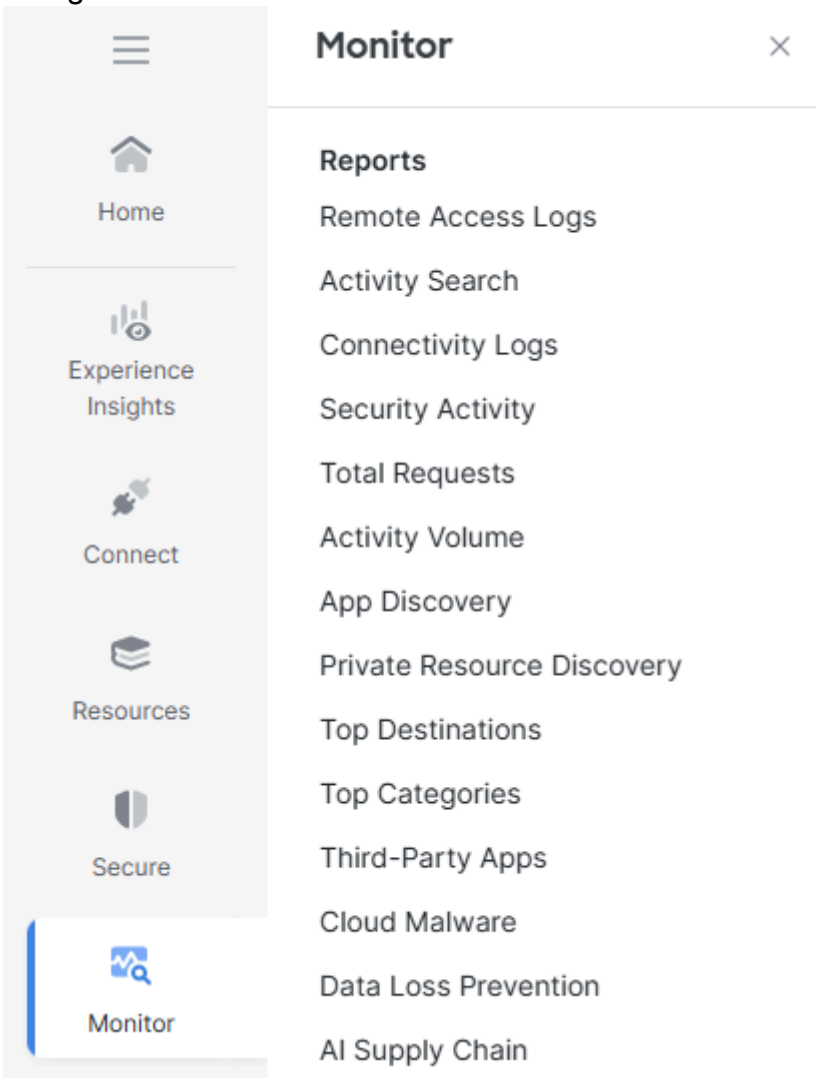


Conn-logboeken bewaken



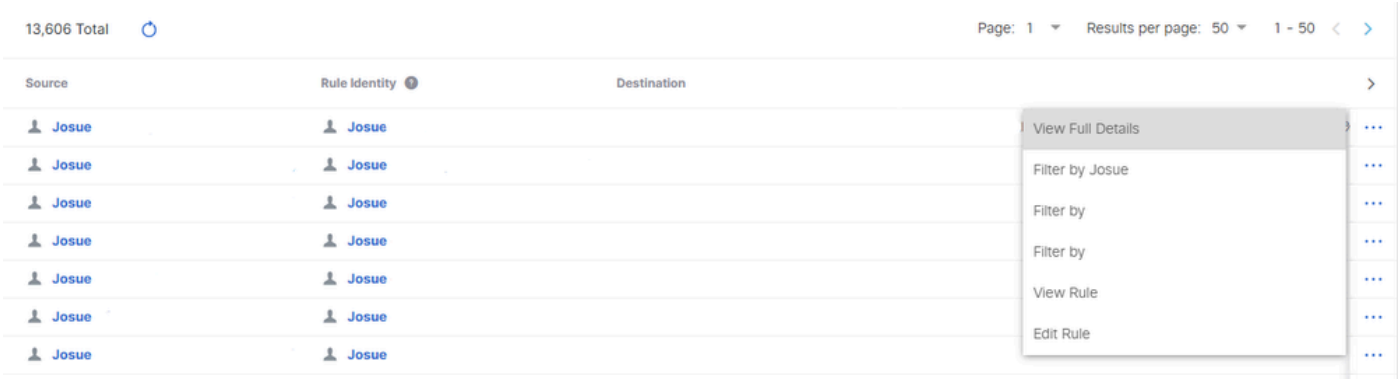
Conn Logs

Navigeer naar Monitor > Activiteit zoeken.

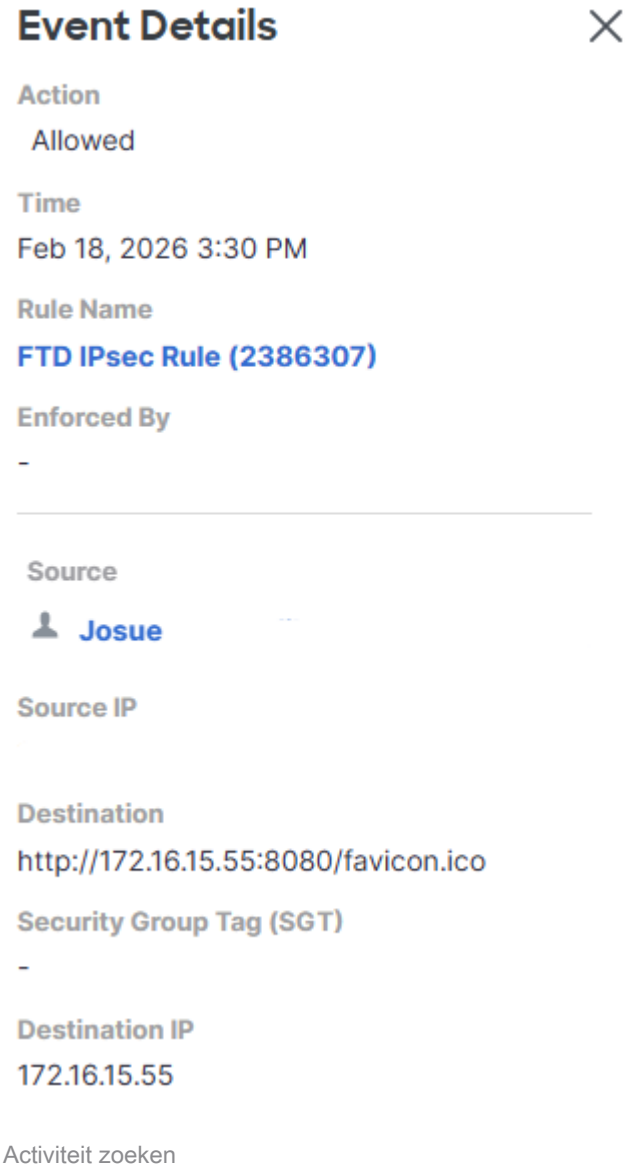


Conn-logboeken bewaken

Klik op een van de gerelateerde gebeurtenissen op Volledige details bekijken.



Volledige details



Gerelateerde informatie

- Cisco Technical Support en downloads
- Apparaatconfiguratiehandleiding Cisco Secure Firewall Management Center, 7.7

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.