

Configureer beveiligde toegang met beveiligde firewall met hoge beschikbaarheid

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Netwerkdigram](#)

[Configureren](#)

[VPN bij beveiligde toegang configureren](#)

[Gegevens voor tunnelinstelling](#)

[De tunnel op Secure Firewall configureren](#)

[De tunnelinterface configureren](#)

[Statische route voor de secundaire interface configureren](#)

[VPN configureren voor beveiligde toegang in VTI-modus](#)

[Configuratie van endpoints](#)

[IKE-configuratie](#)

[IPSEC-configuratie](#)

[Geavanceerde configuratie](#)

[Configuratiescenario's voor toegangsbeleid](#)

[Internet Access Scenario](#)

[RA-VPN-scenario](#)

[CLAP-BAP ZTNA-scenario](#)

[Configuratie van beleidsbasisrouting](#)

[Internettoegangsbeleid configureren voor beveiligde toegang](#)

[Private Resource Access configureren voor ZTNA en RA-VPN](#)

[Problemen oplossen](#)

[Controleer fase 1 \(IKEv2\)](#)

[Controleer fase 2 \(IPSEC\)](#)

[Functie met hoge beschikbaarheid](#)

[Controleer de routing van het verkeer voor beveiligde toegang](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u Secure Access met Secure Firewall met hoge beschikbaarheid kunt configureren.

Voorwaarden

- [Gebruikersprovisioning configureren](#)
- [Configuratie ZTNA SSO-verificatie](#)
- [Beveiligde toegang tot VPN configureren](#)

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Firepower Management Center 7.2
- Firepower Threat Defence 7.2
- Beveiligde toegang
- Cisco Secure-client - VPN
- Cisco Secure-client - ZTNA
- Clientloze ZTNA

Gebruikte componenten

De informatie in dit document is gebaseerd op:

- Firepower Management Center 7.2
- Firepower Threat Defence 7.2
- Beveiligde toegang
- Cisco Secure-client - VPN
- Cisco Secure-client - ZTNA

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



CISCO

Secure

Access

Secure Firewall

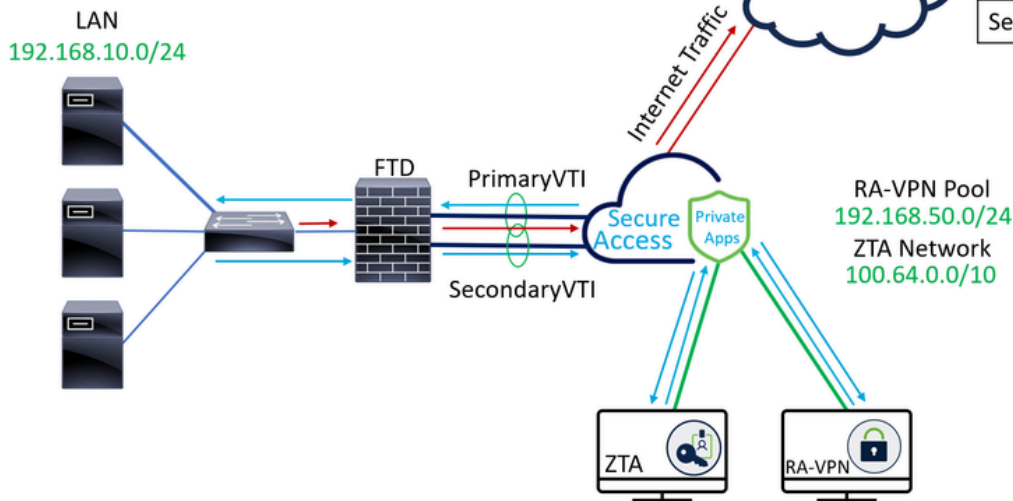
FTD

Cisco heeft Secure Access ontworpen om toegang tot particuliere toepassingen te beschermen en te bieden, zowel op locatie als in de cloud. Het beschermt ook de verbinding van het netwerk met het internet. Dit wordt bereikt door de implementatie van meerdere beveiligingsmethoden en -lagen, die allemaal gericht zijn op het bewaren van de informatie zoals ze deze via de cloud benaderen.

Netwerkdigram

Internet Access Traffic — (red line)
 Private Apps Traffic — (blue line)

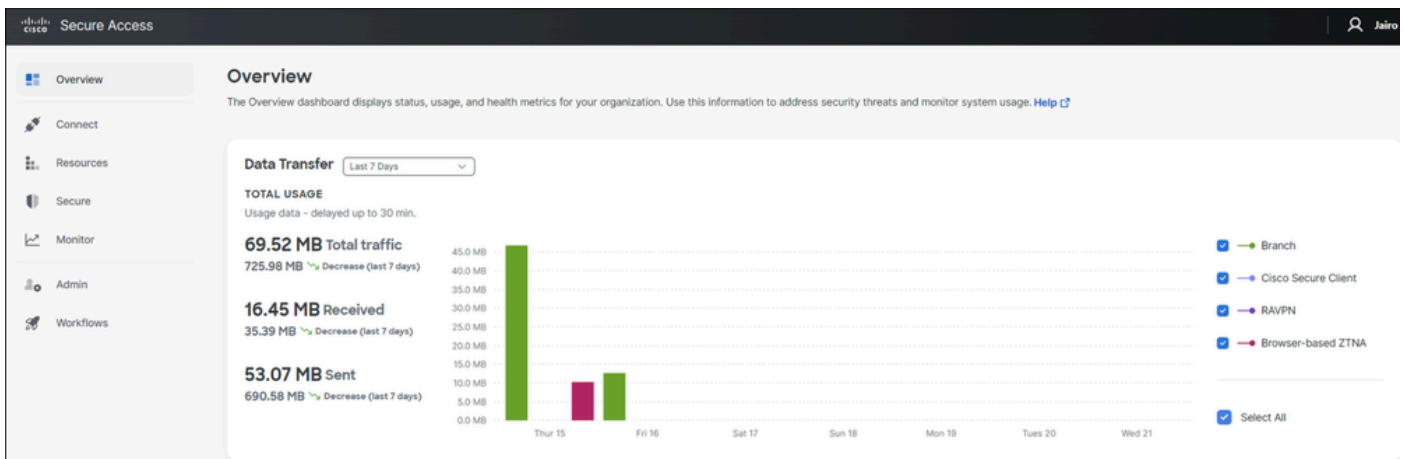
INTERFACE	IP
PrimaryWAN	192.168.30.5
PrimaryVTI	169.254.2.1
SecondaryWAN	192.168.0.202
SecondaryVTI	169.254.3.1



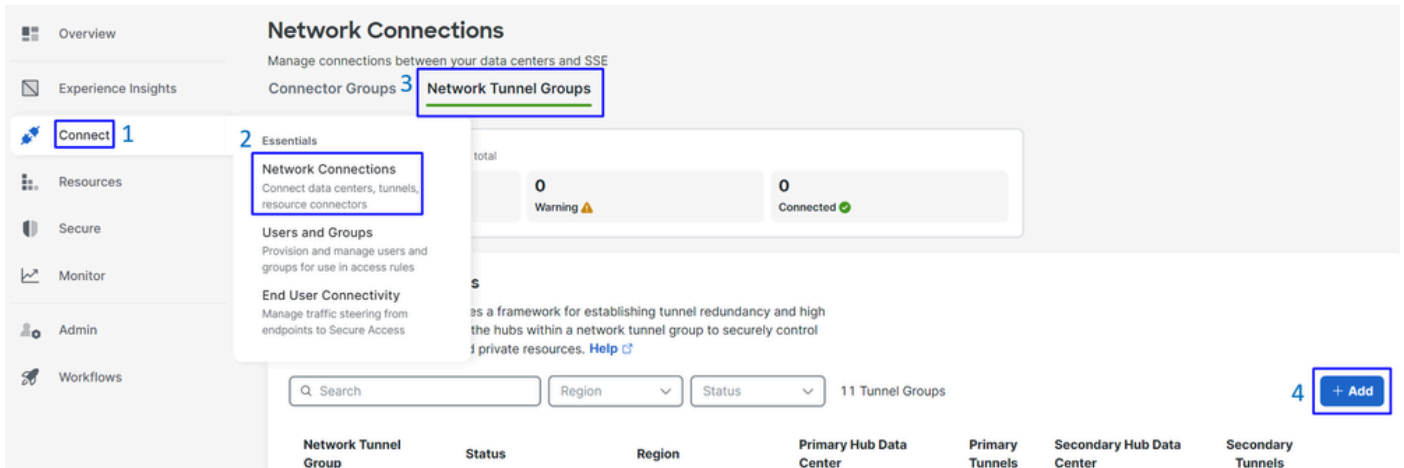
Configureren

VPN bij beveiligde toegang configureren

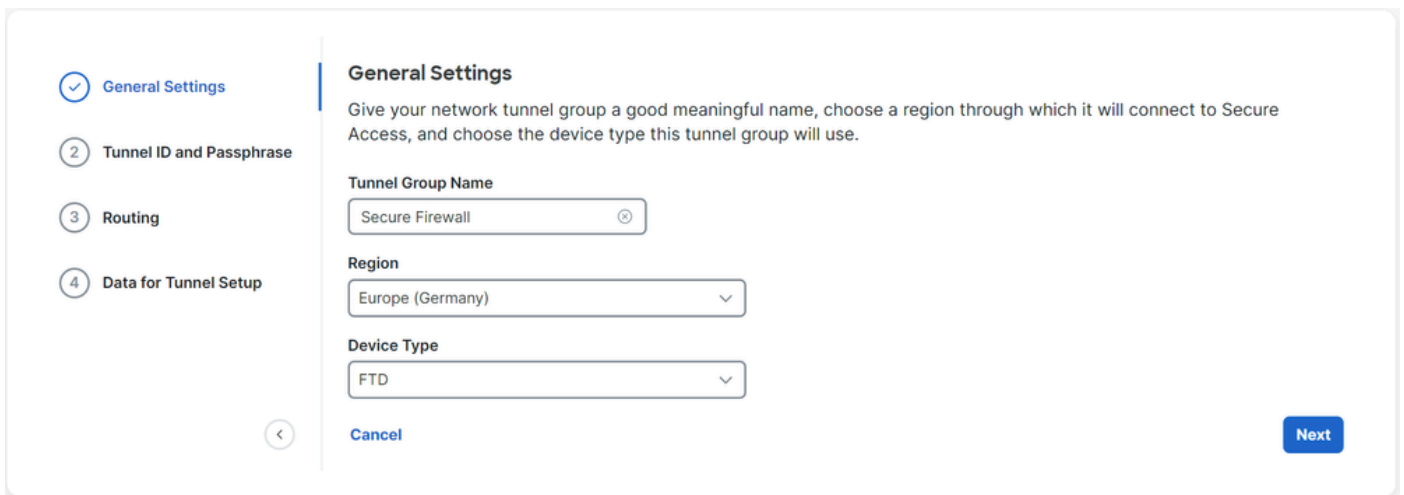
Navigeer naar het beheerderspaneel van [Beveiligde toegang](#).



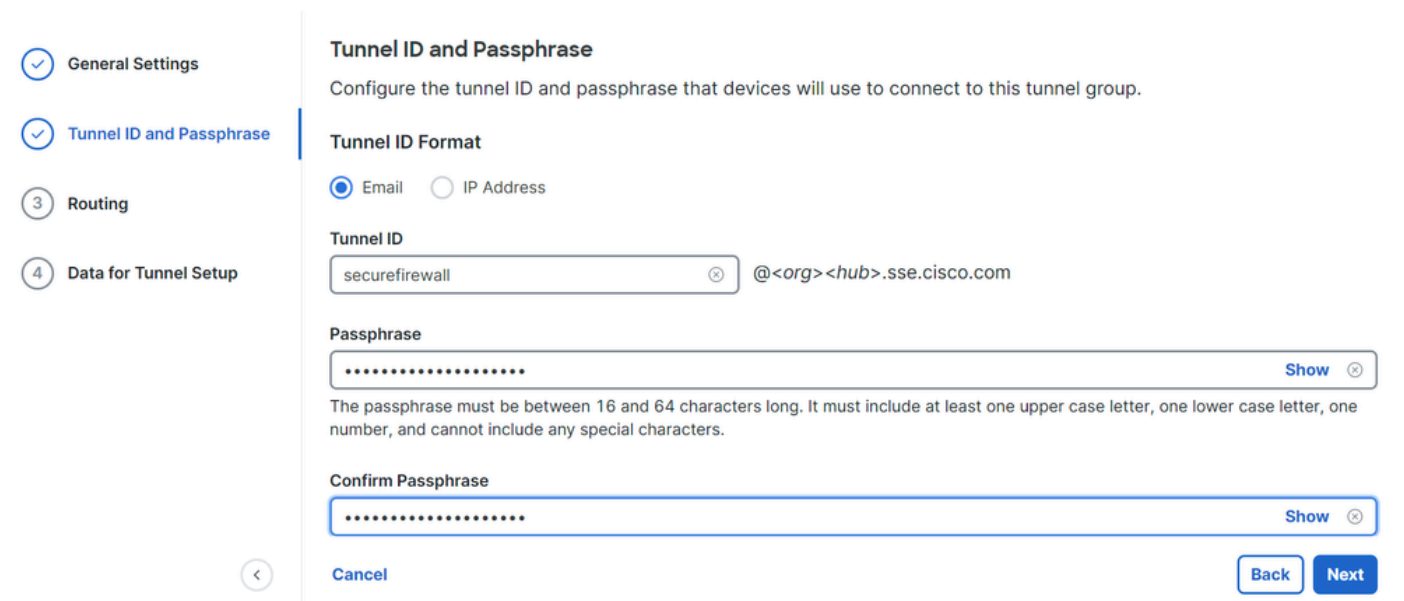
- Klik op Connect > Network Connections
- Onder Network Tunnel Groups klik op + Add



- Configureer Tunnel Group Name, Region en Device Type
- Klik op de knop Next



- Configureer de Tunnel ID Format en Passphrase
- Klik op de knop Next



- Configureer de IP-adresbereiken of hosts die u op uw netwerk hebt geconfigureerd en u wilt

het verkeer via beveiligde toegang doorgeven

- Klik op de knop **Save**

Routing option

Static routing

Use this option to manually add IP address ranges for this tunnel group.

IP Address Ranges

Add all public and private address ranges used internally by your organization. For example, 128.66.0.0/16, 192.0.2.0/24.

128.66.0.0/16, 192.0.2.0/24 **Add**

192.168.0.0/24 X 192.168.10.0/24 X

Dynamic routing

Use this option when you have a BGP peer for your on-premise router.

[Cancel](#)

[Back](#) [Save](#)

Save Nadat u op de informatie over de tunnel wordt weergegeven, slaat u die informatie op voor de volgende stap. **Configure the tunnel on Secure Firewall.**

Gegevens voor tunnelinstelling

General Settings

Tunnel ID and Passphrase

Routing

Data for Tunnel Setup

Data for Tunnel Setup

Review and save the following information for use when setting up your network tunnel devices. This is the only time that your passphrase is displayed.

Primary Tunnel ID: securefirewall@[redacted]-sse.cisco.com

Primary Data Center IP Address: 18.156.145.74

Secondary Tunnel ID: securefirewall@[redacted]-sse.cisco.com

Secondary Data Center IP Address: 3.120.45.23

Passphrase: [redacted]

[Download CSV](#)

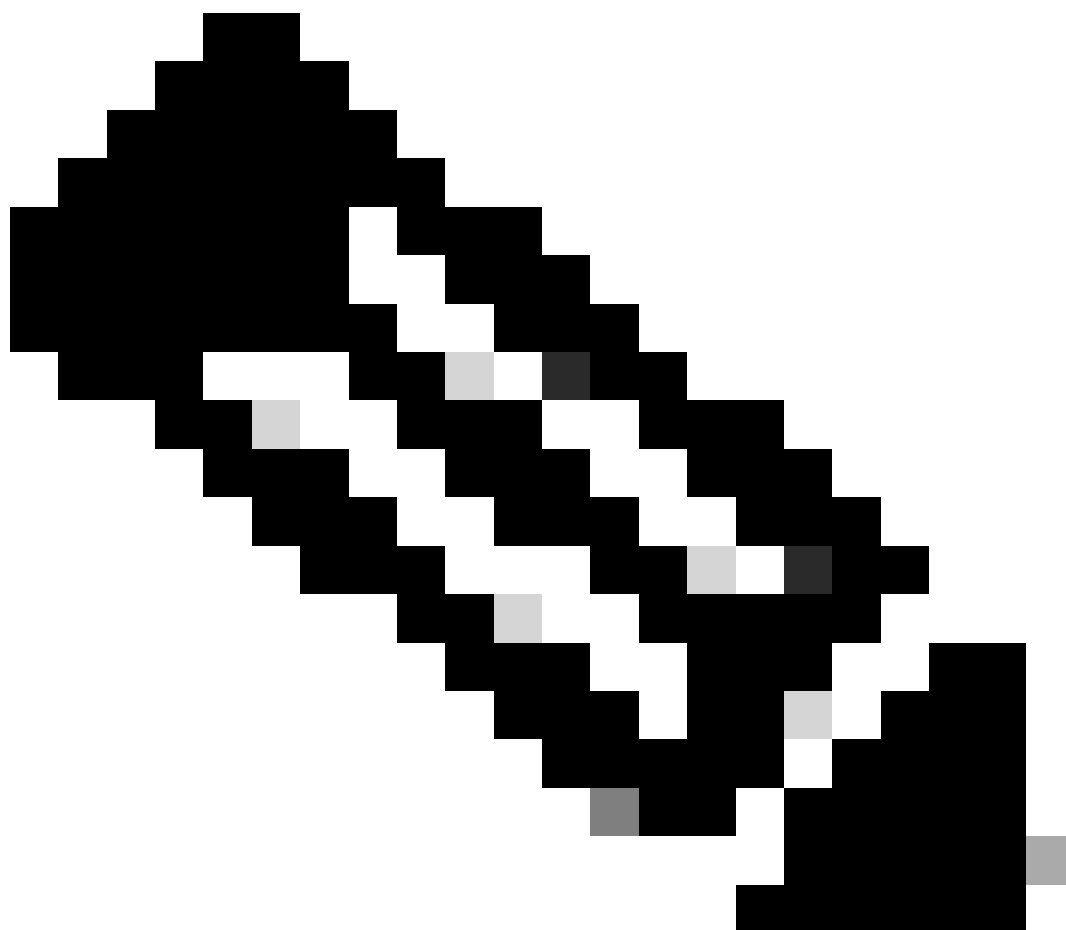
[Done](#)

De tunnel op Secure Firewall configureren

De tunnelinterface configureren

Voor dit scenario gebruikt u de Virtual Tunnel Interface (VTI)-configuratie op Secure Firewall om dit doel te bereiken. Onthoud, in dit geval heb je dubbele ISP, en we willen HA hebben als een van je ISP's faalt.

INTERFACES	ROL
Primair WAN	Belangrijkste WAN-interfacekaart
Secundair WAN	Secundair internet WAN
Primaire VTI	Gekoppeld om het verkeer door de Principal Internet WAN naar Secure Access te verzenden
Secundair VTI	Gekoppeld om het verkeer door de Secondary Internet WAN naar Secure Access te verzenden



Opmerking: 1. U moet een statische route toevoegen of toewijzen aan het **Primary or Secondary Datacenter IP** systeem om beide tunnels te kunnen laten oplopen.



Opmerking: 2. Als u ECMP hebt ingesteld tussen de interfaces, hoeft u geen statische route naar de **Primary or Secondary Datacenter IP tunnels** te maken om beide tunnels te kunnen laten oplopen.

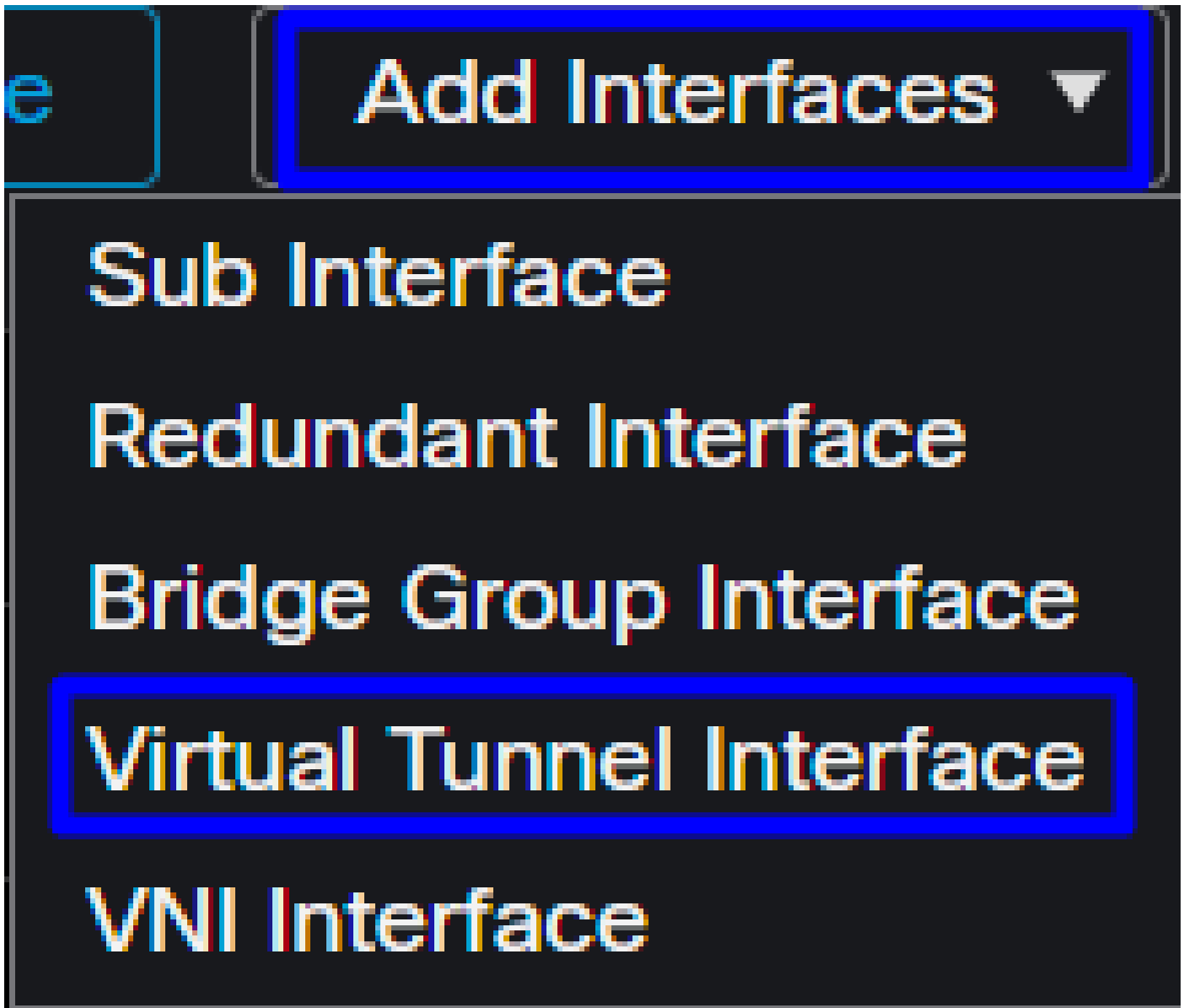
Gebaseerd op het scenario, hebben wij **PrimaryWAN** en **SecondaryWAN**, die wij moeten gebruiken om de VTI interfaces te creëren.

Navigeer naar **uWFirepower Management Center > Devices**.

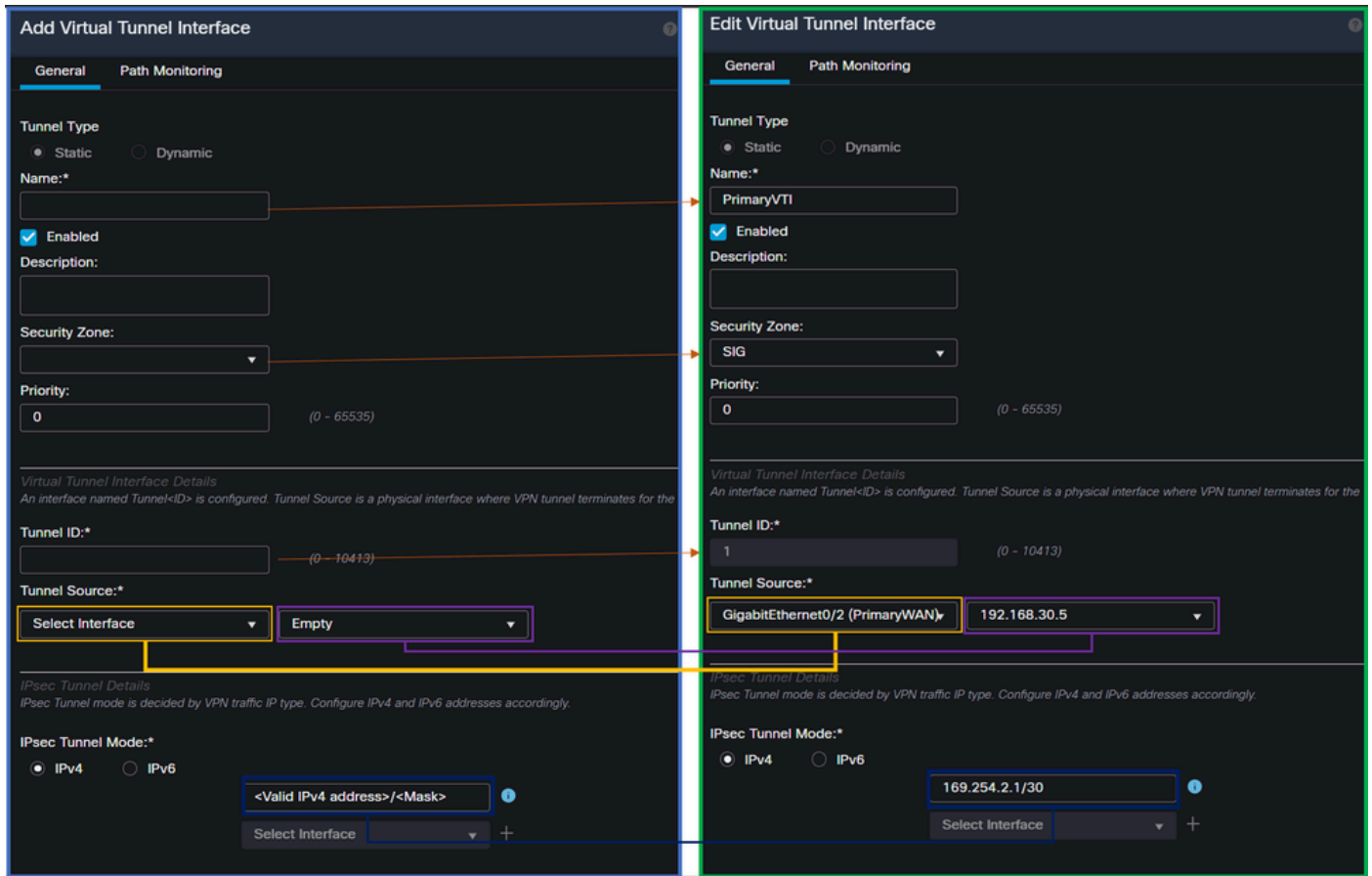
- Kies uw **FTD**
- Kies **Interfaces**

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
Diagnostic0/0	diagnostic	Physical			
GigabitEthernet0/0	SecondaryWAN	Physical	SecondaryWAN		192.168.0.202/24(Static)
GigabitEthernet0/1	LAN	Physical	LAN		192.168.10.1/24(Static)
GigabitEthernet0/2	PrimaryWAN	Physical	PrimaryWAN		192.168.30.5/24(Static)

- Klik op **Add Interfaces > Virtual Tunnel Interface**



- Configureer de interface op basis van de volgende informatie



- **Name** : Configureer een naam die verwijst naar de **PrimaryWAN interface**
- **Security Zone** : U kunt een andere hergebruiken, **Security Zone** maar het maken van een nieuwe voor **Secure Access-verkeer** is beter
- **Tunnel ID** : Een nummer toevoegen voor de tunnelid
- **Tunnel Source** : Kies uw interface **PrimaryWAN interface** en kies de privé of openbare IP van uw interface
- **IPsec Tunnel Mode** : Kies **IPv4** en vorm een niet routable IP in uw netwerk met masker 30



Opmerking: Voor de VTI-interface moet u een niet-routeerbaar IP gebruiken. Als u bijvoorbeeld twee VTI-interfaces hebt, kunt u 169.254.2.1/30 gebruiken voor de **Primary** VTI en 169.254.3.1/30 voor de **Secondary** VTI.

Daarna moet je hetzelfde doen voor de **Secondary** WAN interface VTI, en je hebt alles ingesteld voor de VTI High Availability, en als gevolg daarvan heb je het volgende resultaat:

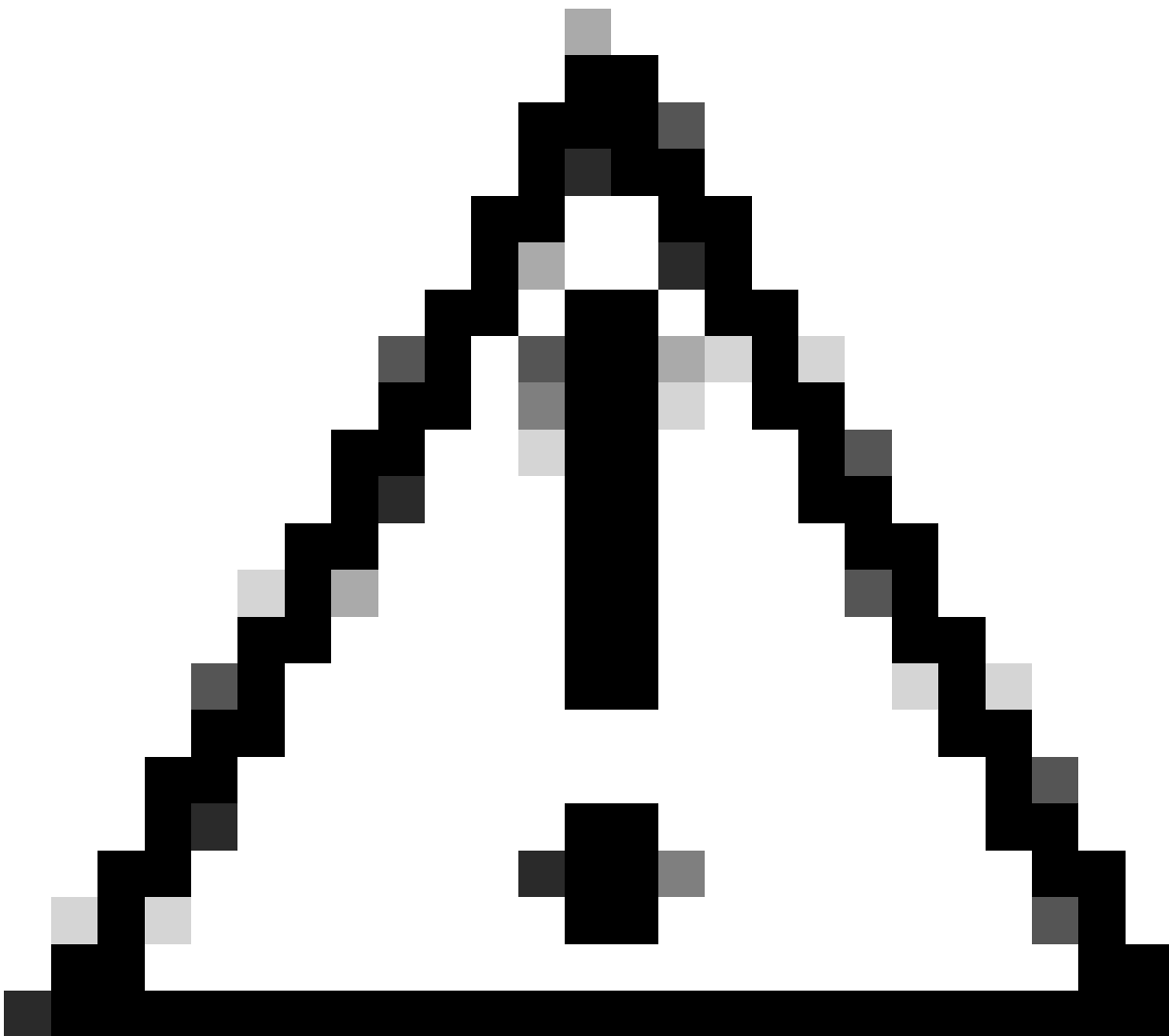
Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
Diagnostic0/0	diagnostic	Physical			
GigabitEthernet0/0	SecondaryWAN	Physical	SecondaryWAN		192.168.0.202/24(Static)
Tunnel2	SecondaryVTI	VTI	SIG		169.254.3.1/30(Static)
GigabitEthernet0/1	LAN	Physical	LAN		192.168.10.1/24(Static)
GigabitEthernet0/2	PrimaryWAN	Physical	PrimaryWAN		192.168.30.5/24(Static)
Tunnel1	PrimaryVTI	VTI	SIG		169.254.2.1/30(Static)

Voor dit scenario zijn de gebruikte IP's:

VTI IP-configuratie		
Logische naam	IP	Bereik
Primaire VTI	169.254.2.1/30	169.254.2.1-169.254.2.2
Secundair VTI	169.254.3.1/30	169.254.3.1-169.254.3.2

Statische route voor de secundaire interface configureren

Om het verkeer van de **Secondary WAN interface** te bereiken **Secondary Datacenter IP Address** moet u een statische route naar het datacenter IP configureren. U kunt het met metriek van één (1) vormen om het bovenop de routingstabel te maken; Specificeer ook het IP als host.



Voorzichtig: Dit is alleen nodig als u geen ECMP-instelling hebt tussen de WAN-kanalen;

als u ECMP hebt geconfigureerd, kunt u naar de volgende stap springen.

Naar navigeren **Device > Device Management**

- Klik op uw FTD-apparaat
- Klik op **Routing**
- Kiezen **Static Route > + Add Route**

Edit Static Route Configuration




Type: IPv4 IPv6

Interface*

SecondaryWAN

Choose the SecondaryWAN interface

(Interface starting with this icon  signifies it is available for route leak)


Available Network  +

Search

Add

192.168.0.150
192.168.10.153
any-ipv4
ASA_GW
CSA_Primary
GWT1

Selected Network

SecureAccessTunnel 

Choose the Secondary Datacenter IP

Ensure that egress virtualrouter has route to that destination

Gateway

Outside_GW

Choose the SecondaryWAN Gateway

Metric:

1

(1 - 254)

Tunneled: (Used only for default Route)

Route Tracking:

Cancel

OK

- Interface: Kies de secundaire WAN-interface
- Gateway: Kies de secundaire WAN-gateway
- Selected Network: Voeg het secundaire datacenter IP toe als host; u kunt de informatie over de gegeven informatie vinden wanneer u de tunnel op de Veilige stap van de Toegang, [Gegevens voor de Opstelling van de Tunnel](#) vormt

- Metric: Gebruik één (1)
- Klik op en Save voer de informatie op om deze op te slaan, en implementeer vervolgens.

Network	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked
▼ IPv4 Routes						
SecureAccessTunnel	SecondaryWAN	Global	Outside_GW	false	1	
any-ipv4	PrimaryWAN	Global	ASA_GW	false	1	
▼ IPv6 Routes						

VPN configureren voor beveiligde toegang in VTI-modus

Om VPN te configureren navigeer je naar je firewall:

- Klik op **Devices > Site to Site**
- Klik op **+ Site to Site VPN**

Configuratie van endpoints

Om de stap Endpoints te configureren, moet u de informatie gebruiken die onder de stap [Data for Tunnel Setup is](#) geleverd.

Create New VPN Topology

Topology Name:*

Policy Based (Crypto Map) Route Based (VTI)

Network Topology:

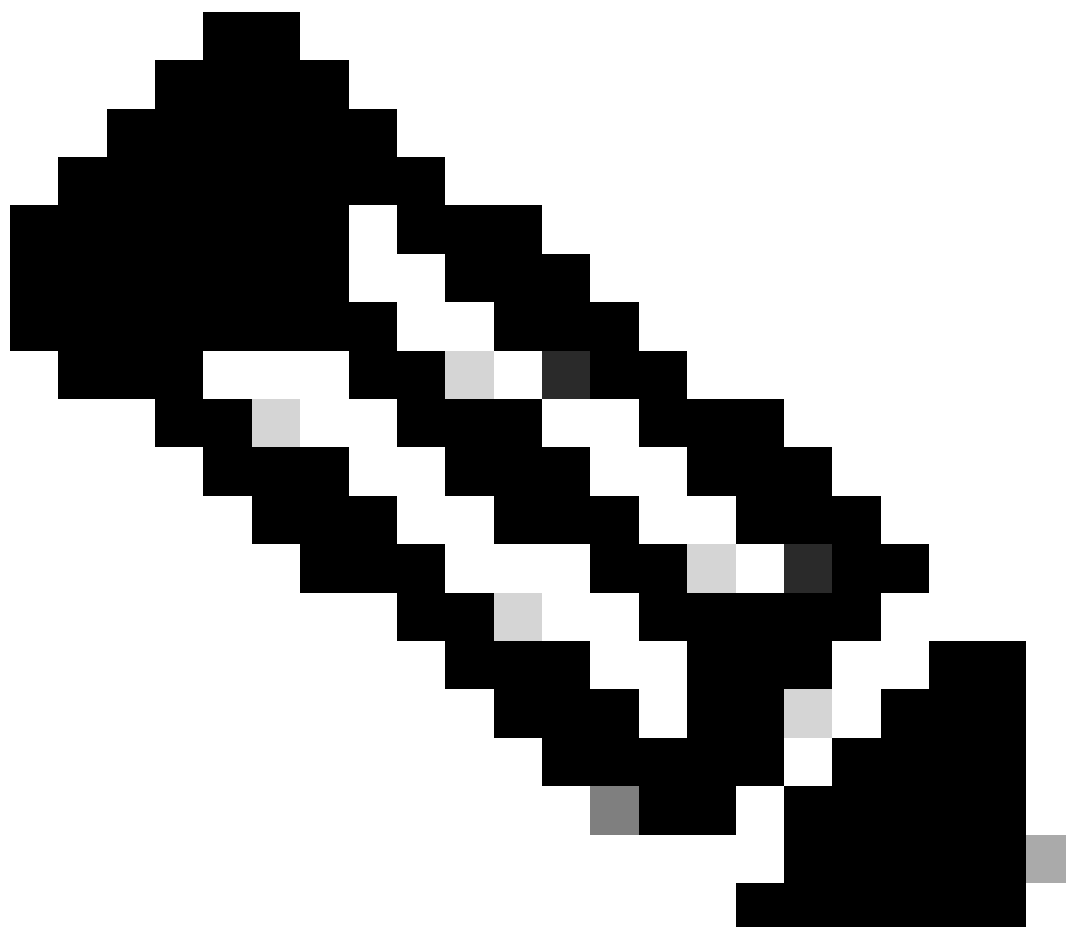
IKE Version:* IKEv1 IKEv2

Endpoints | IKE | IPsec | Advanced

Node A	Node B
Device:* <input type="text" value="FTD_HOME"/>	Device:* <input type="text" value="Extranet"/>
Virtual Tunnel Interface:* <input type="text" value="PrimaryVTI (IP: 169.254.2.1)"/>	Device Name*: <input type="text" value="SecureAccess"/>
Tunnel Source: PrimaryWAN (IP: 192.168.30.5) Edit VTI <input type="checkbox"/> Tunnel Source IP is Private <input checked="" type="checkbox"/> Send Local Identity to Peers	Endpoint IP Address*: <input type="text" value="18.156.145.74,3.120.45.23"/>
Local Identity Configuration:* <input type="text" value="Email ID"/> <input type="text" value="jairohome@8195126-615626006-"/>	
Backup VTI: Remove	

- Naam topologie: Een naam maken met betrekking tot de integratie Secure Access
- Kiezen Routed Based (VTI)

- Kiezen **Point to Point**
 - IKE Version: Kies **IKEv2**
-



Opmerking: IKEv1 wordt niet ondersteund voor integratie met Secure Access.

Onder het **Node A** menu moet u de volgende parameters configureren:

Node A

Device:*

FTD_HOME ▼

Virtual Tunnel Interface:*

PrimaryVTI (IP: 169.254.2.1) ▼



Tunnel Source: PrimaryWAN (IP: 192.168.30.5) [Edit VTI](#)

Tunnel Source IP is Private

Send Local Identity to Peers

Local Identity Configuration:*

Email ID ▼

jairohome@ [redacted]

[+ Add Backup VTI \(optional\)](#)

- **Device:** Kies uw FTD-apparaat
- **Virtual Tunnel Interface:** Kies de VTI met betrekking tot de PrimaryWAN Interface.
- Schakel het selectievakje in voor **Send Local Identity to Peers**
- **Local Identity Configuration:** Kies e-mail-id en vul de informatie in op basis van de informatie die u in uw configuratie hebt **Primary Tunnel ID** opgegeven voor de stap, [Data for Tunnel Setup](#)

Nadat u de informatie over de PrimaryVTI klik hebt geconfigureerd [+ Add Backup VTI](#):

Backup VTI:

Remove

Virtual Tunnel Interface:*

SecondaryVTI (IP: 169.254.3.1) ▼



Tunnel Source: SecondaryWAN (IP: 192.168.0.202) [Edit VTI](#)

Tunnel Source IP is Private

Send Local Identity to Peers

Local Identity Configuration:*

Email ID ▼

jairohome@

- **Virtual Tunnel Interface:** Kies de VTI met betrekking tot de PrimaryWAN Interface.
- Schakel het selectievakje in voor **Send Local Identity to Peers**
- **Local Identity Configuration:** Kies e-mail-id en vul de informatie in op basis van de informatie die u in uw configuratie hebt **Secondary Tunnel ID** opgegeven voor de stap, [Data for Tunnel Setup](#)

Onder het **Node B** menu moet u de volgende parameters configureren:

Node B

Device:*

Extranet

Device Name*:

SecureAccess

Endpoint IP Address*:

18.156.145.74, 3.120.45.23

- Device: Extranet
- Device Name: Kies een naam om beveiligde toegang te herkennen als de bestemming.
- Endpoint IP Address: De configuratie voor primair en secundair moet Primair zijn Datacenter IP, Secondary Datacenter IP, kunt u die informatie in de stap, [Gegevens voor de Opstelling van de Tunnel](#) vinden

Daarna is uw configuratie voor Endpoints voltooid en kunt u nu naar de stap, IKE Configuration gaan.

IKE-configuratie

Klik op **IKE** om de IKE-parameters te configureren.

Endpoints

IKE

IPsec

Advanced

Onder moet IKE, u de volgende parameters configureren:

Endpoints **IKE** IPsec Advanced

IKEv2 Settings

Policies:* Umbrella-AES-GCM-256

Authentication Type: Pre-shared Manual Key

Key:*

Confirm Key:*

Enforce hex-based pre-shared key only

- Policies: U kunt de standaard Umbrella configuratie gebruiken Umbrella-AES-GCM-256 of u kunt een andere parameters configureren op basis van de [Supported IKEv2 and IPSEC Parameters](#)
- Authentication Type: Vooraf gedeelde handmatige sleutel
- Key en Confirm Key: Passphrase U vindt de informatie in de stap, [Data for Tunnel Setup](#)

Daarna is uw configuratie voor IKE voltooid en kunt u nu naar de stap, IPSEC Configuration gaan.

IPSEC-configuratie

Klik op IPSEC om de IPSEC-parameters te configureren.

Endpoints

IKE



IPsec

Advanced

Onder moet IPSEC, u de volgende parameters configureren:

Crypto Map Type: Static Dynamic

IKEv2 Mode: Tunnel

Transform Sets: IKEv1 IPsec Proposals  IKEv2 IPsec Proposals* 

tunnel_aes256_sha	Umbrella-AES-GCM-256
-------------------	-----------------------------

Enable Security Association (SA) Strength Enforcement

Enable Perfect Forward Secrecy

Modulus Group: 14

Lifetime Duration*: 28800 Seconds (Range 120-2147483647)

Lifetime Size: 4608000 Kbytes (Range 10-2147483647)

- Policies: U kunt de standaard Umbrella configuratie gebruiken **Umbrella-AES-GCM-256** of u kunt een andere parameters configureren op basis van de [Supported IKEv2 and IPSEC Parameters](#)



Opmerking: Voor IPSEC is verder niets vereist.

Daarna is uw configuratie voor IPSEC voltooid en kunt u nu naar de stap, Advanced Configuration gaan.

Geavanceerde configuratie

Om de geavanceerde parameters te configureren klikt u op Geavanceerd.

Endpoints

IKE

IPsec

Advanced

Onder moet **Advanced**, u de volgende parameters configureren:

ISAKMP Settings

IKE Keepalive: Enable

Threshold: 10 Seconds (Range 10 - 3600)

Retry Interval: 2 Seconds (Range 2 - 10)

Identity Sent to Peers: autoOrDN

Peer Identity Validation: Do not check

Enable Aggressive Mode

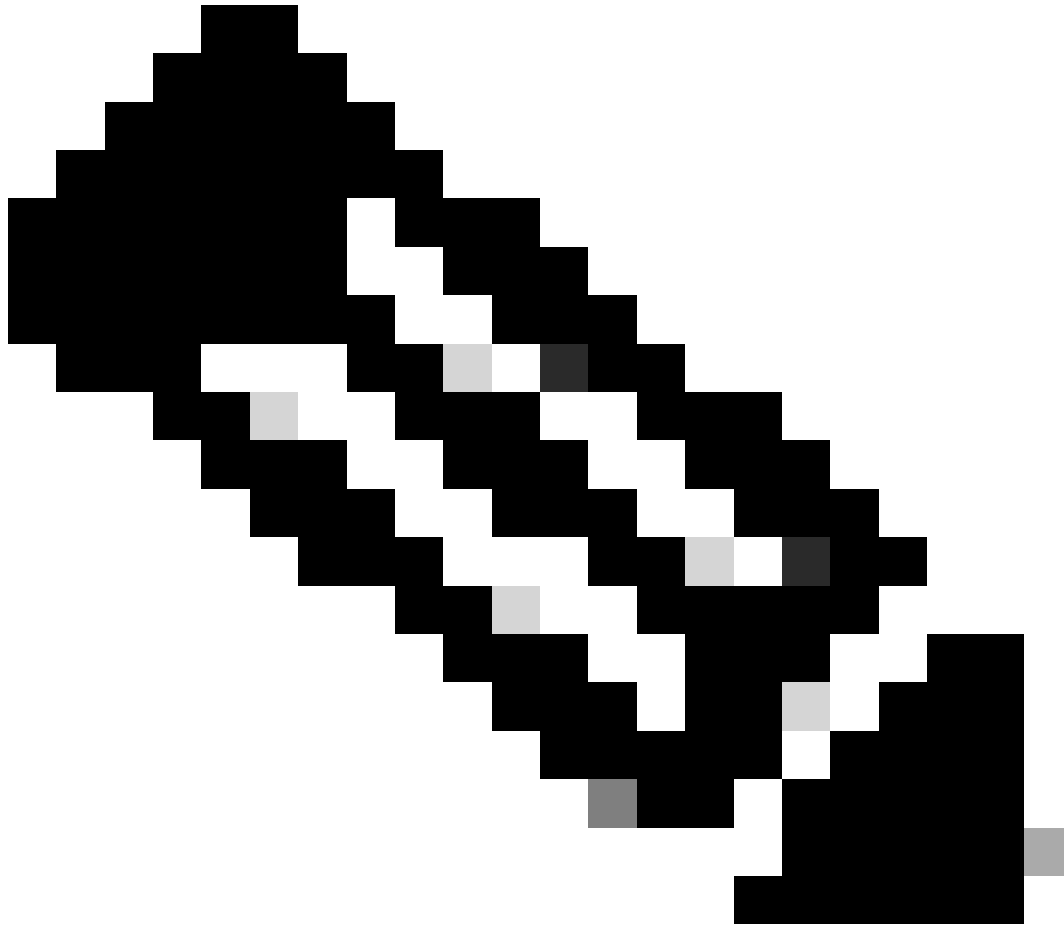
Enable Notification on Tunnel Disconnect

IKEv2 Security Association (SA) Settings

Cookie Challenge: custom

- IKE Keepalive: Inschakelen
- Threshold: 10
- Retry Interval: 2
- Identity Sent to Peers: autoORDN
- Peer Identity Validation: Niet controleren

Daarna kunt u op **Save** en **Deploy**.



Opmerking: Na een paar minuten ziet u de VPN die voor beide knooppunten is gemaakt.

Topology Name	VPN Type	Network Topology	Tunnel Status Distribution	IKEv1	IKEv2
SecureAccess	Route Based (VTI)	Point to Point	2 - Tunnels	✓	✗
Node A			Node B		
Device	VPN Interface	VTI Interface	Device	VPN Interface	VTI Interface
EXTRANET	Extranet	3.120.4... (3.120.45.23)	FTD	FTD_HOME	Secon... (192.168.0.202) Seconda... (169.254.3.1)
EXTRANET	Extranet	18.15... (18.156.145.74)	FTD	FTD_HOME	Primary... (192.168.30.5) PrimaryVTI (169.254.2.1)

Daarna is uw configuratie voor het VPN to Secure Access in VTI Mode systeem voltooid en kunt u nu naar de stap gaan, **Configure Policy Base Routing**.



Waarschuwing: Verkeer naar beveiligde toegang wordt alleen naar de primaire tunnel doorgestuurd wanneer beide tunnels worden opgezet; als de primaire wordt neergehaald, maakt Secure Access het mogelijk dat het verkeer door de secundaire tunnel wordt doorgestuurd.

Opmerking: de failover op de Secure Access-site is gebaseerd op de DPD-waarden die zijn gedocumenteerd in de [gebruikershandleiding](#) voor ondersteunde IPsec-waarden.

Configuratiescenario's voor toegangsbeleid

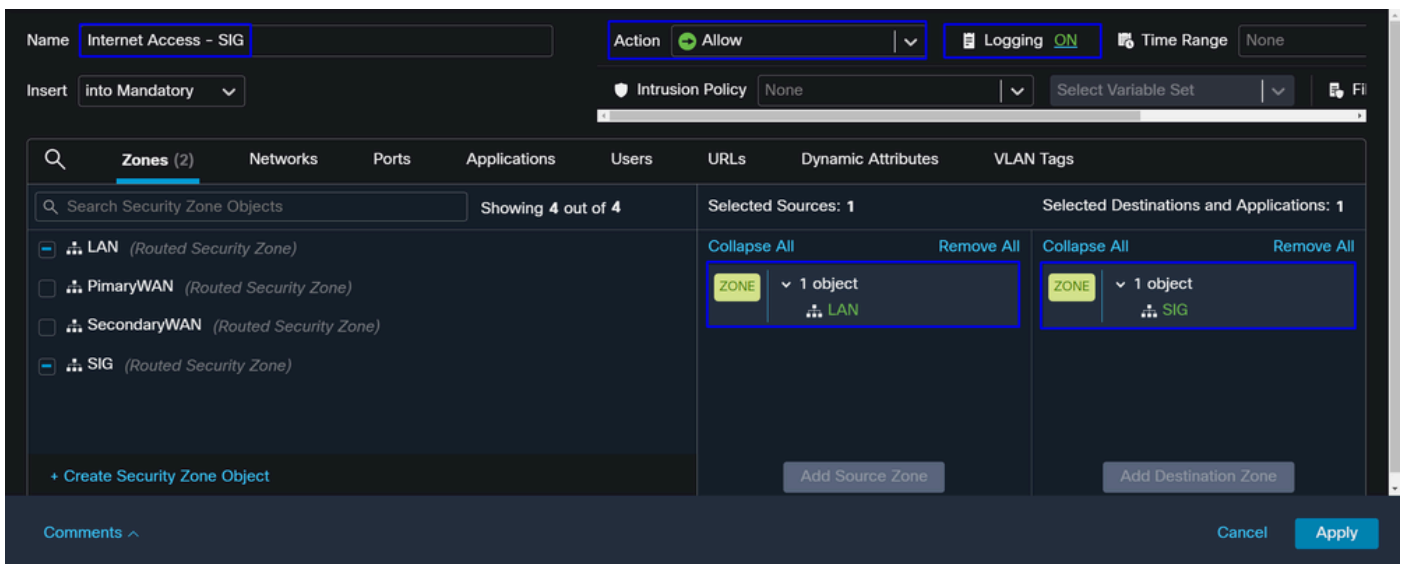
De vastgestelde regels voor het toegangsbeleid zijn gebaseerd op:

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
● GigabitEthernet0/0	SecondaryWAN	Physical	SecondaryWAN		192.168.0.202/24(Static)
● Tunnel2	SecondaryVTI	VTI	SIG		169.254.3.1/30(Static)
● GigabitEthernet0/1	LAN	Physical	LAN		192.168.10.1/24(Static)
● GigabitEthernet0/2	PrimaryWAN	Physical	PrimaryWAN		192.168.30.5/24(Static)
● Tunnel1	PrimaryVTI	VTI	SIG		169.254.2.1/30(Static)

Interface	Gebied
Primaire VTI	SIG
Secundair VTI	SIG
LAN	LAN

Internet Access Scenario

Om toegang tot het internet te bieden aan alle bronnen die u vormt op de Policy Base Routing, moet u bepaalde toegangsregels en ook een aantal beleidsregels in beveiligde toegang configureren, dus laat me uitleggen hoe u dat in dit scenario kunt bereiken:



Deze regel geeft toegang tot het LAN internet, en in dit geval is het internet dat SIG.

RA-VPN-scenario

Om toegang te bieden van de RA-VPN-gebruikers, moet u deze configureren op basis van het bereik dat u hebt toegewezen aan de RA-VPN-pool.



Opmerking: Om uw RA-VPNaaS-beleid te configureren, kunt u via [Virtual Private Networks beheren](#)

Hoe verifieert u de IP-pool van uw VPNaaS?

Navigeer naar uw [Secure Access Dashboard](#)

- Klik op **Connect** > End User Connectivity
- Klik op **Virtual Private Network**
- Klik onder **Manage IP Pool** het kopje **Manage**

End User Connectivity

↓ Cisco Secure Client

Manage DNS Servers (2)

End user connectivity lets you define how your organization's traffic is steered from endpoints to Secure Access or to the internet. [Help](#)

Zero Trust **Virtual Private Network** Internet Security

Global FQDN

fb57.vpn.sse.cisco.com [Copy](#)

Manage IP Pools

2 Regions mapped

Manage

- U ziet uw zwembad onder **Endpoint IP Pools**

Pop Name	Display Name	Endpoint IP Pools	Management IP Pools	DNS Servers
Europe (Germany)	RA VPN 1	192.168.50.0/24 256 user connections	192.168.60.0/24 256 user connections	House

- U moet dit bereik toestaan onder SIG, maar u moet het ook toevoegen onder de ACL die u in uw PBR vormt.

Configuratie van toegangsregels

Als u alleen Secure Access configureert om deze te gebruiken met de mogelijkheden om toegang te krijgen tot de bronnen van particuliere toepassingen, kan uw toegangsregel er zo uitzien:

The screenshot shows the configuration of an Access Control List (ACL) rule. The rule name is "Private APP". The action is set to "Allow", logging is enabled, and the time range is "None". The rule is inserted "into Mandatory". The intrusion policy is "None".

The configuration is set for "Networks". The "Selected Sources" list includes:

- ZONE: 1 object (SIG)
- NET: 1 object (192.168.50.0/24)

The "Selected Destinations and Applications" list includes:

- ZONE: 1 object (LAN)

The "Networks" table shows the following objects:

Networks	Geolocations
<input type="checkbox"/> 192.168.0.150 (Host Object)	192.168.0.150
<input type="checkbox"/> 192.168.10.153 (Host Object)	192.168.10.153
<input type="checkbox"/> any (Network Group)	0.0.0.0::/0
<input type="checkbox"/> any-ipv4 (Network Object)	0.0.0.0/0
<input type="checkbox"/> any-ipv6 (Host Object)	::/0

Buttons at the bottom include "Add Source Network" and "Add Destination Network". The "Apply" button is highlighted.

Deze regel maakt verkeer van de RA-VPN Pool 192.168.50.0/24 naar uw LAN mogelijk; U kunt indien nodig meer opgeven.

ACL-configuratie

Om het routingverkeer van SIG naar uw LAN toe te laten, moet u het onder de ACL toevoegen om het onder de PBR te laten werken.

Sequence	Action	Source	Source Port	Destination	Destination Port	Application	Users	SGT	
1	Allow	192.168.10.0/24	Any	192.168.50.0/24	Any	Any	Any		
2	Block	Any	Any	Any	Any	Any	Any		

CLAP-BAP ZTNA-scenario

U moet uw netwerk configureren op basis van CGNAT-bereik 100.64.0.0/10 om toegang te bieden tot uw netwerk vanuit de ZTA- of ZTA-gebruikers van de clientbase of de ZTA-gebruikers van de browserbasis.

Configuratie van toegangsregels

Als u alleen Secure Access configureert om deze te gebruiken met de mogelijkheden om toegang te krijgen tot de bronnen van particuliere toepassingen, kan uw toegangsregel er zo uitzien:

Name: ZTNA Access - IN Action: Allow Logging: ON Time Range: None Rule Enabled: ON

Insert: into Mandatory Intrusion Policy: None Select Variable Set: File Policy: None

Showing 27 out of 27

Networks	Geolocations
<input type="checkbox"/> 192.168.0.150 (Host Object)	192.168.0.150
<input type="checkbox"/> 192.168.10.153 (Host Object)	192.168.10.153
<input type="checkbox"/> any (Network Group)	0.0.0.0/0::/0
<input type="checkbox"/> any-ipv4 (Network Object)	0.0.0.0/0
<input type="checkbox"/> any-ipv6 (Host Object)	::/0
<input type="checkbox"/> ASA_GW (Host Object)	192.168.30.1
<input type="checkbox"/> CSA_Primary (Host Object)	18.156.145.74
<input type="checkbox"/> GWT1 (Host Object)	169.254.2.2

Selected Sources: 2

- ZONE 1 object: SIG
- NET 1 object: 100.64.0.0/10 (CGNAT RANGE)

Selected Destinations and Applications: 1

- ZONE 1 object: LAN

Die regel maakt verkeer van de ZTNA CGNAT Range 100.64.0.0/10 naar uw LAN mogelijk.

ACL-configuratie

Om het routingverkeer van SIG met CGNAT naar uw LAN toe te laten, moet u dit onder de ACL toevoegen om het onder de PBR te laten werken.

Sequence	Action	Source	Source Port	Destination	Destination Port	Application	Users	SGT	
1	Allow	192.168.10.0/24	Any	100.64.0.0/10	Any	Any	Any		
2	Block	Any	Any	Any	Any	Any	Any		

Configuratie van beleidsbasisrouting

Om toegang tot interne resources en het internet via beveiligde toegang te bieden, moet u routes via Policy Base Routing (PBR) maken die het routing van het verkeer van de bron naar de bestemming vergemakkelijken.

- Naar navigeren **Devices > Device Management**
- Kies het FTD-apparaat waar u de route maakt

<input type="checkbox"/>	Name	Model	Version
<input type="checkbox"/>	Ungrouped (1)		
<input type="checkbox"/>	<div style="border: 2px solid blue; padding: 2px;"> ✔ FTD_HOME Snort 3 192.168.0.201 - Routed </div>	FTDv for VMware	7.2.5

- Klik op **Routing**
- Kiezen **Policy Base Routing**
- Klik op de knop **Add**

Policy Based Routing
 Specify Ingress interfaces, match criteria and egress interfaces to route traffic accordingly. Traffic can be routed across Egress Interfaces accordingly

[Configure Interface Priority](#)
[Add](#)

In dit scenario selecteert u alle interfaces die u als bron gebruikt om verkeer te routeren naar beveiligde toegang of om gebruikersverificatie te bieden aan beveiligde toegang met RA-VPN of clientgebaseerde of browsergebaseerde ZTA-toegang tot de interne netwerkbronnen:

- Selecteer onder **Ingress Interface** alle interfaces die verkeer via **Secure Access** verzenden:

Edit Policy Based Route

A policy based route consists of ingress interface list and a set of match criteria associated to egress interfaces

Ingress Interface*

LAN

- Onder Match Criteria en uitgaande interface definieert u de volgende parameters nadat u op **Add** hebt geklikt:

Match Criteria and Egress Interface
Specify forward action for chosen match criteria. Add

Add Forwarding Actions

Match ACL:* Select... +

Send To:* IP Address

IPv4 Addresses: For example, 192.168.0.1, 10.10.1.2

IPv6 Addresses: For example, 2001:db8::, 2002:db8::1

Don't Fragment: None

Internal Sources

Match ACL:* ACL

Send To:* IP Address

IPv4 Addresses: 169.254.2.2, 169.254.3.2

IPv6 Addresses: For example, 2001:db8::, 2002:db8::1

Don't Fragment: None

- **Match ACL:** Voor deze ACL configureert u alles dat u naar Secure Access routeert:

Traffic to the destination 208.67.222.222 or 208.67.220.220 over DNS using TCP or UDP will not be routed to Secure Access

✗ REJECT

Name: SSPT_FTD_ACL

Entries (2)

Sequence	Action	Source	Source Port	Destination	Destination Port
1	Block	Any	Any	208.67.222.222 208.67.222.220	Any
2	Allow	192.168.10.0/24	Any	Any	Any

Traffic from the source 192.168.10.0/24 will be routed to Secure Access

Depends how you play with the ACL, you can define how the traffic must be routed to Secure Access

✓ ACCEPT

- **Send To:** IP-adres kiezen
- **IPv4 Addresses:** U moet de volgende IP gebruiken onder het masker 30 dat op beide VTI is geconfigureerd; u kunt controleren dat onder de stap, [VTI Interface Config](#)

Interface	IP	GW
Primaire VTI	169.254.2.1/30	169.254.2.2

Secundair VTI	169.254.3.1/30	169.254.3.2
---------------	----------------	-------------



Nadat je het zo hebt geconfigureerd, heb je het volgende resultaat en kun je verder gaan met klikken **Save**:

Save Daarna moet u het opnieuw, en je hebt het geconfigureerd op de volgende manier:

A policy based route consists of ingress interface list and a set of match criteria associated to egress interfaces

Ingress Interface*
 LAN

Match Criteria and Egress Interface
 Specify forward action for chosen match criteria. Add

Match ACL	Forwarding Action
ACL	Send through 169.254.2.2 169.254.3.2 → Send the traffic to the PrimaryVTI

If PrimaryVTI fail it will send the traffic to the SecondaryVTI



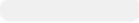


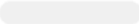


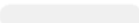


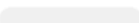


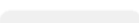


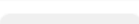


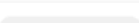

Cancel Save

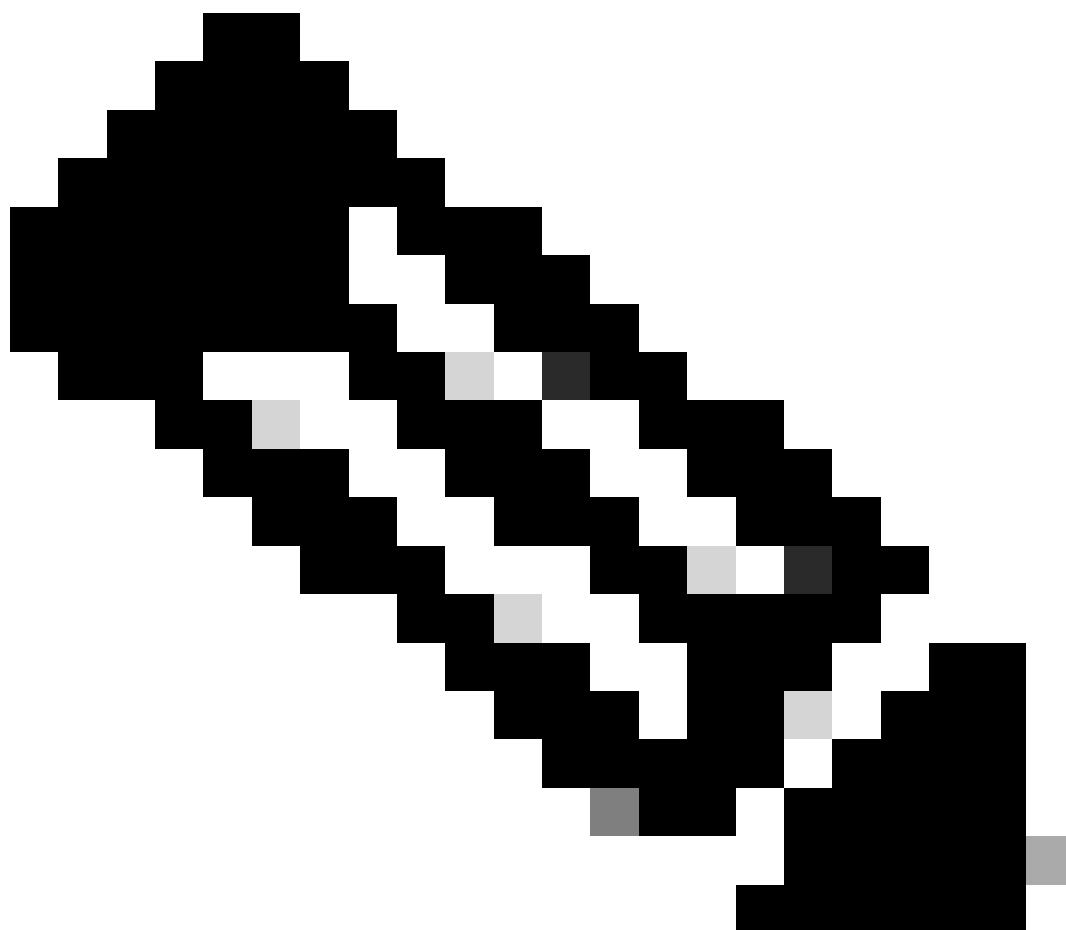
Daarna kunt u implementeren en u ziet het verkeer van de machines die op de ACL zijn geconfigureerd en het verkeer naar beveiligde toegang routing:

Vanuit het **Conexion Events VCC**:

<input type="checkbox"/>	Action x	Initiator IP x	Responder IP x	↓ Application Risk x	Access Control Policy x	Ingress Interface x	Egress Interface x
▼ <input type="checkbox"/>	Allow	192.168.10.40	8.8.8.8	Medium	HOUSE	LAN	PrimaryVTI
▼ <input type="checkbox"/>	Allow	192.168.10.40	8.8.8.8	Medium	HOUSE	LAN	PrimaryVTI
▼ <input type="checkbox"/>	Allow	192.168.10.40	8.8.8.8	Medium	HOUSE	LAN	PrimaryVTI
▼ <input type="checkbox"/>	Allow	192.168.10.40	8.8.8.8	Medium	HOUSE	LAN	PrimaryVTI
▼ <input type="checkbox"/>	Allow	192.168.10.40	8.8.8.8	Medium	HOUSE	LAN	PrimaryVTI
▼ <input type="checkbox"/>	Allow	192.168.10.40	8.8.8.8	Medium	HOUSE	LAN	PrimaryVTI

Vanaf het **Activity Search** tabblad Beveiligde toegang:

Request	Source	Rule Identity 	Destination	Destination IP	Internal IP	External IP	Action	Categories	Res
	⇌ HomeFTD	⇌ HomeFTD		8.8.8.8	192.168.10.40		 Allowed	Uncategorized	
	⇌ HomeFTD	⇌ HomeFTD		8.8.8.8	192.168.10.40		 Allowed	Uncategorized	
	⇌ HomeFTD	⇌ HomeFTD		8.8.8.8	192.168.10.40		 Allowed	Uncategorized	
	⇌ HomeFTD	⇌ HomeFTD		8.8.8.8	192.168.10.40		 Allowed	Uncategorized	
	⇌ HomeFTD	⇌ HomeFTD		8.8.8.8	192.168.10.40		 Allowed	Uncategorized	
	⇌ HomeFTD	⇌ HomeFTD		8.8.8.8	192.168.10.40		 Allowed	Uncategorized	
	⇌ HomeFTD	⇌ HomeFTD		8.8.8.8	192.168.10.40		 Allowed	Uncategorized	

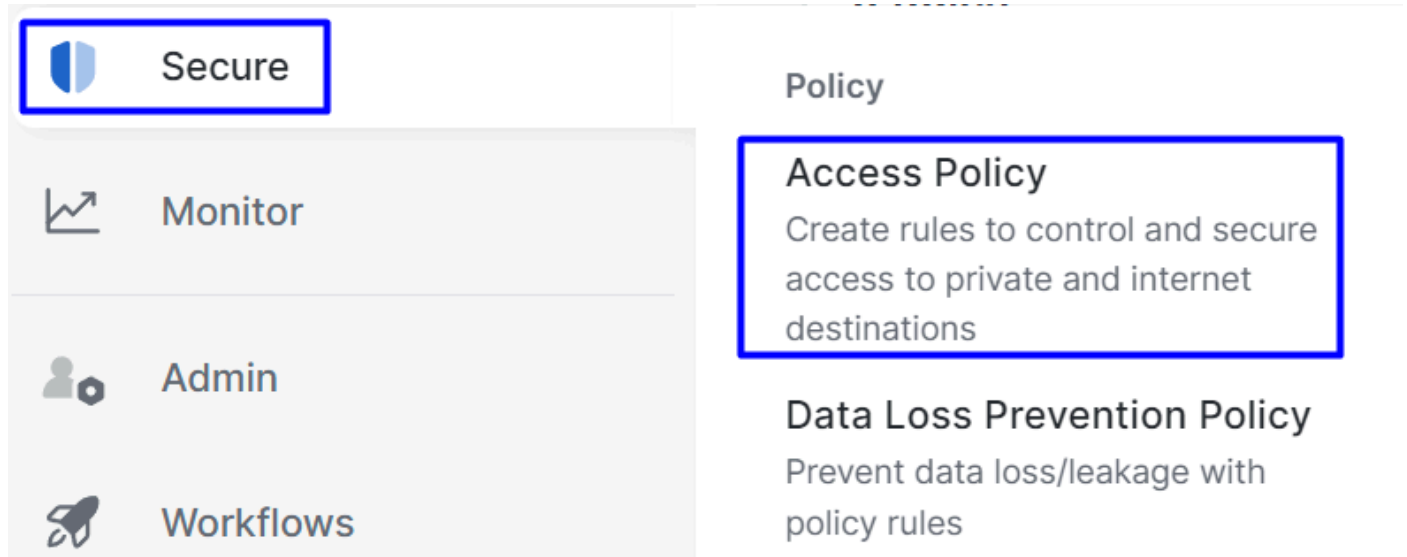


Opmerking: Standaard staat het standaard Secure Access Policy verkeer naar het internet toe. Om toegang tot privé toepassingen te verlenen, moet u privé middelen tot stand brengen en hen toevoegen aan het toegangsbeleid voor privé middeltoegang.

Internettoegangsbeleid configureren voor beveiligde toegang

Om de toegang voor internettoegang te configureren, moet u het beleid op uw [Secure Access Dashboard](#) maken:

- Klik op **Secure > Access Policy**



- Klik op **Add Rule > Internet Access**

Add Rule ^

Private Access

Control and secure access to resources and applications that cannot be accessed by the general public.

Internet Access

Control and secure access to public destinations from within your network and from managed devices

Daar kunt u de bron als de tunnel specificeren, en aan de bestemming, kunt u om het even welk, afhankelijk van wat u op het beleid wilt vormen kiezen. Controleer of u de [Secure Access-gebruikershandleiding hebt](#).

Private Resource Access configureren voor ZTNA en RA-VPN

Om de toegang voor privé-bronnen te configureren, moet u eerst de bronnen maken onder het [Secure Access Dashboard](#):

Klik op **Resources > Private Resources**

The screenshot shows the Secure Access Dashboard interface. On the left is a navigation menu with the following items: Resources (highlighted with a blue box), Secure, Monitor, Admin, and Workflows. The main content area is divided into two columns. The left column is titled 'Sources and destinations' and contains three sections: 'Registered Networks' (Point your networks to our servers), 'Internal Networks' (Define internal network segments to use as sources in access rules), and 'Roaming Devices' (Mac and Windows). The right column is titled 'Destinations' and contains two sections: 'Internet and SaaS Resources' (Define destinations for internet access rules) and 'Private Resources' (Define internal applications and other resources for use in access rules). The 'Private Resources' section is highlighted with a blue box.

- Klik vervolgens op **ADD**

Onder de configuratie, vindt u de volgende secties om te vormen: **General**, **Communication with Secure Access Cloud and Endpoint Connection Methods**.

Algemeen

General

Private Resource Name

Description (optional)

- Private Resource Name : **Maak een naam voor de bron die u toegang verleent via Secure Access naar uw netwerk**

Methoden voor endpointverbinding

Zero-trust connections
Allow endpoints to connect to this resource from outside your network without requiring a VPN connection. [Help](#)

Client-based connection
Allow connections from endpoints that have the Secure Client installed. Enable this option for maximum control over endpoint security requirements (posture).

Remotely Reachable Address (FQDN, Wildcard FQDN, IP Address) ⓘ

[+ FQDN or IP Address](#)

Browser-based connection
Allow browser-based connections from endpoints that do not have the Secure Client installed. Enable this option when devices that your organization does not manage must connect to this resource. Fewer endpoint security checks are possible.

Public URL for this resource ⓘ

https:// ⓘ

Protocol **Server Name Indication (SNI)** (optional) ⓘ

HTTPS ▾

Validate Application Certificate ⓘ

- **Zero Trust Connections:** Markeer het vakje.
- **Client-based connection:** Als u deze functie inschakelt, kunt u de Secure Client - Zero Trust Module gebruiken om toegang via de clientgebaseerde modus mogelijk te maken.
- **Remote Reachable Address (FQDN, Wildcard FQDN, IP Address) :** Configureer de bronnen IP of FQDN; als u FQDN vormt, moet u DNS toevoegen om de naam op te lossen.
- **Browser-based connection:** Als u deze inschakelt, kunt u toegang krijgen tot uw bronnen via de browser (Voeg alleen bronnen toe met HTTP- of HTTPS-communicatie)
- **Public URL for this resource:** Configureer de openbare URL die u gebruikt via de browser; Secure Access beschermt deze bron.
- **Protocol:** Selecteer het protocol (HTTP of HTTPS)

VPN connections
 Allow endpoints to connect to this resource when connected to the network using VPN.

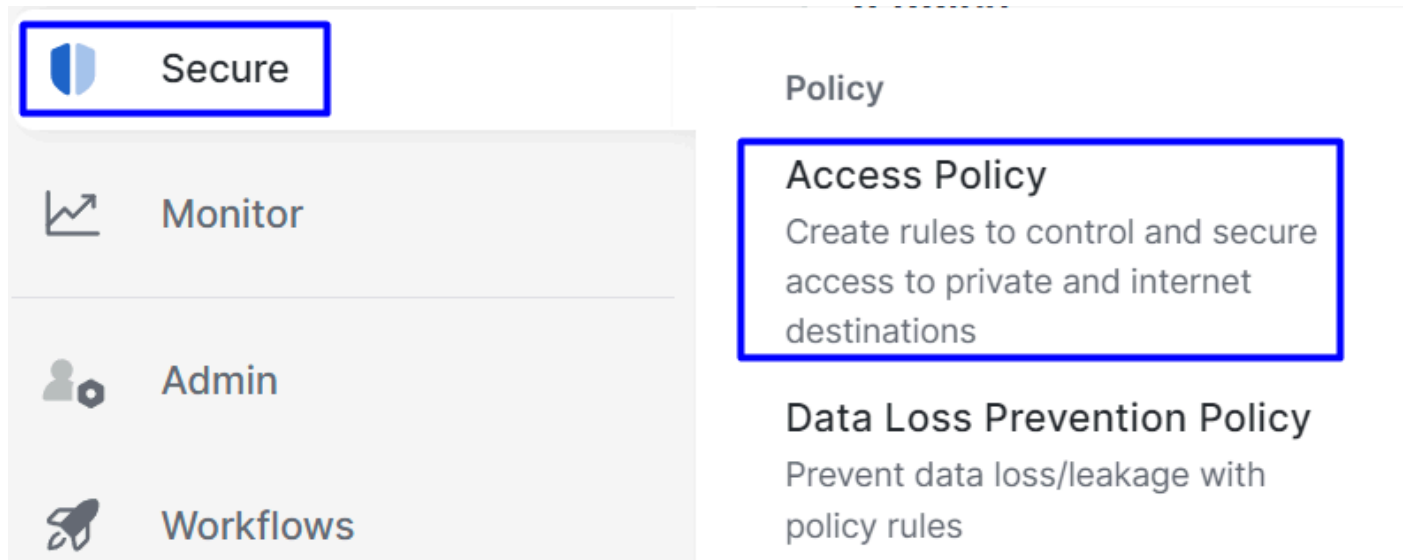
VPN Connection: Markeer het aanvinkvakje om toegang via RA-VPNaaS in te schakelen.

Daarna klikt u op **Save** en kunt u die bron aan de **Access Policy** pagina toevoegen.

Het toegangsbeleid configureren

Wanneer u de resource maakt, moet u deze toewijzen aan een van de beveiligingstoegangsregels:

- Klik op **Secure > Access Policy**



- Klik op de knop **Add > Private Resource**

Add Rule ^

Private Access

Control and secure access to resources and applications that cannot be accessed by the general public.

Internet Access

Control and secure access to public destinations from within your network and from managed devices

Voor deze Private Access-regel, vormt u de standaardwaarden om toegang te verlenen tot de bron. Om meer te weten te komen over beleidsconfiguraties, raadpleegt u de [Gebruikersgids](#).

1 Specify Access

Specify which users and endpoints can access which resources. [Help](#)

Action

<input checked="" type="radio"/> Allow Allow specified traffic if security requirements are met.	<input type="radio"/> Block Block specified traffic.
--	--

From

Specify one or more sources.

vpn user (vpnuser@ciscospt.es) x

Information about sources, including selecting multiple sources. [Help](#)

To

Specify one or more destinations.

SplunkFTD x

Information about destinations, including selecting multiple destinations. [Help](#)

- **Action** : Kies Toestaan om toegang te verlenen tot de bron.
- **From** : Specificeer de gebruiker die kan worden gebruikt om in te loggen op de resource.
- **To** : Kies de resource die u wilt openen via Secure Access.

Endpoint Requirements

For zero-trust connections, if endpoints do not meet the specified requirements, this rule will not match the traffic. [Help](#)

Zero-Trust Client-based Posture Profile Rule Defaults

Requirements for end-user devices on which the Cisco Secure Client is installed.

System provided (Client-based)

Private Resources: **SplunkFTD**

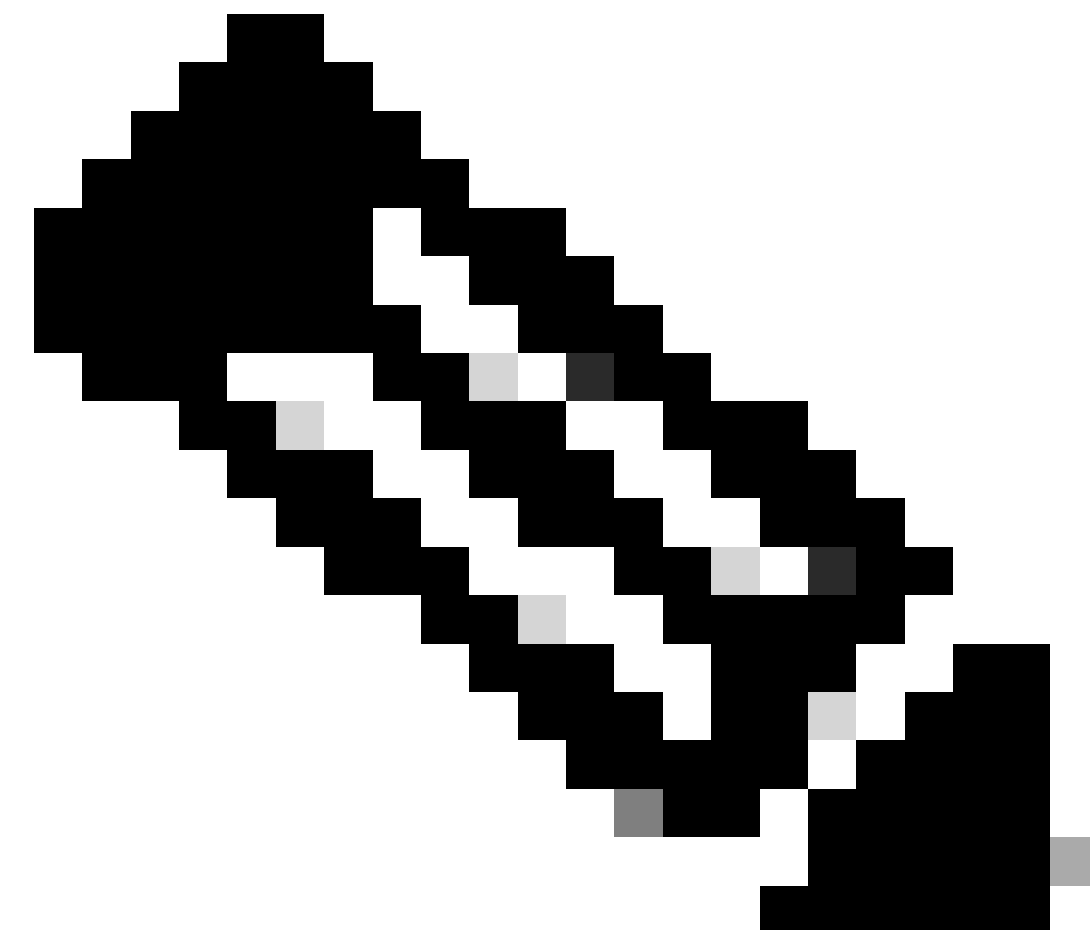
Zero Trust Browser-based Posture Profile Rule Defaults

Requirements for end-user devices on which the Cisco Secure Client is NOT installed.

System provided (Browser-based)

Private Resources: **SplunkFTD**

- **Zero-Trust Client-based Posture Profile:** Kies het standaardprofiel voor toegang op clientbasis
- **Zero-Trust Browser-based Posture Profile:** Kies de standaardprofiel browser basis toegang



Opmerking: Als u meer wilt weten over het postuur, raadpleegt u de [gebruikershandleiding](#) voor Secure Access.

Na dat, klik `Next` en `Save` en uw configuratie, en u kunt proberen om tot uw middelen door RA-VPN en de Basis ZTNA van de Cliënt of Browser Basis ZTNA toegang te hebben.

Problemen oplossen

Om problemen op te lossen op basis van de communicatie tussen Secure Firewall en Secure Access, kunt u controleren of fase1 (IKEv2) en fase2 (IPSEC) zonder probleem tussen de apparaten tot stand zijn gebracht.

Controleer fase 1 (IKEv2)

Om te controleren of Phase1 u de volgende opdracht op de CLI van uw FTD moet uitvoeren:

```
show crypto isakmp sa
```

In dit geval is de gewenste uitvoer twee **IKEv2 SAs** tot stand gebracht aan de Datacenter IP's van Secure Access en de gewenste status als **READY**:

There are no IKEv1 SAs

IKEv2 SAs:

Session-id:3, Status:UP-ACTIVE, IKE count:1, CHILD count:1

```
Tunnel-id Local Remote
52346451 192.168.0.202/4500 3.120.45.23/4500
    Encr: AES-GCM, keysize: 256, Hash: N/A, DH Grp:20, Auth sign: PSK, Auth verify: PSK
    Life/Active Time: 86400/4009 sec
Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535
          remote selector 0.0.0.0/0 - 255.255.255.255/65535
          ESP spi in/out: 0xfb34754c/0xc27fd2ba
```

IKEv2 SAs:

Session-id:2, Status:UP-ACTIVE, IKE count:1, CHILD count:1

```
Tunnel-id Local Remote
52442403 192.168.30.5/4500 18.156.145.74/4500
    Encr: AES-GCM, keysize: 256, Hash: N/A, DH Grp:20, Auth sign: PSK, Auth verify: PSK
    Life/Active Time: 86400/3891 sec
Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535
          remote selector 0.0.0.0/0 - 255.255.255.255/65535
          ESP spi in/out: 0x4af761fd/0xfbca3343
```

Controleer fase 2 (IPSEC)

Om fase2 te verifiëren, moet u de volgende opdracht uitvoeren op de CLI van uw FTD:

interface: PrimaryVTI

Crypto map tag: __vti-crypto-map-Tunnel1-0-1, seq num: 65280, local addr: 192.168.30.5

Protected vrf (ivrf): Global

local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)

remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)

current_peer: 18.156.145.74

#pkts encaps: 71965, #pkts encrypt: 71965, #pkts digest: 71965

#pkts decaps: 91325, #pkts decrypt: 91325, #pkts verify: 91325

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 71965, #pkts comp failed: 0, #pkts decomp failed: 0

#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0

#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0

#TFC rcvd: 0, #TFC sent: 0

#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0

#send errors: 0, #recv errors: 0

local crypto endpt.: 192.168.30.5/4500, remote crypto endpt.: 18.156.145.74/4500

path mtu 1500, ipsec overhead 63(44), media mtu 1500

PMTU time remaining (sec): 0, DF policy: copy-df

ICMP error validation: disabled, TFC packets: disabled

current outbound spi: FBCA3343

current inbound spi : 4AF761FD

inbound esp sas:

spi: 0x4AF761FD (1257726461)

SA State: active

transform: esp-aes-gcm-256 esp-null-hmac no compression

in use settings ={L2L, Tunnel, NAT-T-Encaps, IKEv2, VTI, }

slot: 0, conn_id: 2, crypto-map: __vti-crypto-map-Tunnel1-0-1

sa timing: remaining key lifetime (kB/sec): (3916242/27571)

IV size: 8 bytes

replay detection support: Y

Anti replay bitmap:

0xFFFFFFFF 0xFFFFFFFF

outbound esp sas:

spi: 0xFBCA3343 (4224332611)

SA State: active

transform: esp-aes-gcm-256 esp-null-hmac no compression

in use settings ={L2L, Tunnel, NAT-T-Encaps, IKEv2, VTI, }

slot: 0, conn_id: 2, crypto-map: __vti-crypto-map-Tunnel1-0-1

sa timing: remaining key lifetime (kB/sec): (4239174/27571)

IV size: 8 bytes

replay detection support: Y

Anti replay bitmap:

0x00000000 0x00000001

interface: SecondaryVTI

Crypto map tag: __vti-crypto-map-Tunnel2-0-2, seq num: 65280, local addr: 192.168.0.202

Protected vrf (ivrf): Global

local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)

remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)

current_peer: 3.120.45.23

#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0

#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0

#pkts compressed: 0, #pkts decompressed: 0

```
#pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0
```

```
local crypto endpt.: 192.168.0.202/4500, remote crypto endpt.: 3.120.45.23/4500
path mtu 1500, ipsec overhead 63(44), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: C27FD2BA
current inbound spi : FB34754C
```

inbound esp sas:

```
spi: 0xFB34754C (4214519116)
SA State: active
transform: esp-aes-gcm-256 esp-null-hmac no compression
in use settings ={L2L, Tunnel, NAT-T-Encaps, IKEv2, VTI, }
slot: 0, conn_id: 20, crypto-map: __vti-crypto-map-Tunnel2-0-2
sa timing: remaining key lifetime (kB/sec): (4101120/27412)
IV size: 8 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001
```

outbound esp sas:

```
spi: 0xC27FD2BA (3263156922)
SA State: active
transform: esp-aes-gcm-256 esp-null-hmac no compression
in use settings ={L2L, Tunnel, NAT-T-Encaps, IKEv2, VTI, }
slot: 0, conn_id: 20, crypto-map: __vti-crypto-map-Tunnel2-0-2
sa timing: remaining key lifetime (kB/sec): (4239360/27412)
IV size: 8 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001
```

In de laatste output, kunt u beide tunnels zien worden gevestigd; wat niet gewenst is, is de volgende uitvoer onder het pakketencapsendecaps.

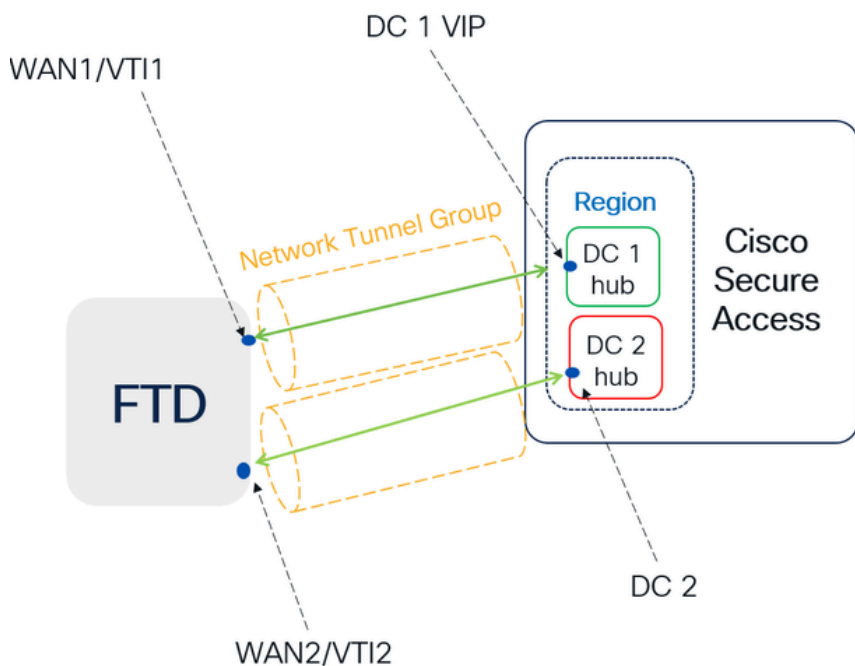
```
#pkts encaps: 71965, #pkts encrypt: 71965, #pkts digest: 71965 → Packets forwarded to Secure Access
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0 → No packets forwarded from Secure
#pkts compressed: 0, #pkts decompressed: 0 → Access to your firewall
#pkts not compressed: 71965, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0
```

Als u dit scenario hebt, open een case met TAC.

Functie met hoge beschikbaarheid

De functie van de tunnels met beveiligde toegang communiceren met het datacenter in de cloud is actief/passief, wat betekent dat alleen de deur voor DC 1 open zal zijn om verkeer te ontvangen; de DC 2-deur is gesloten tot tunnel nummer 1 omlaag komt.

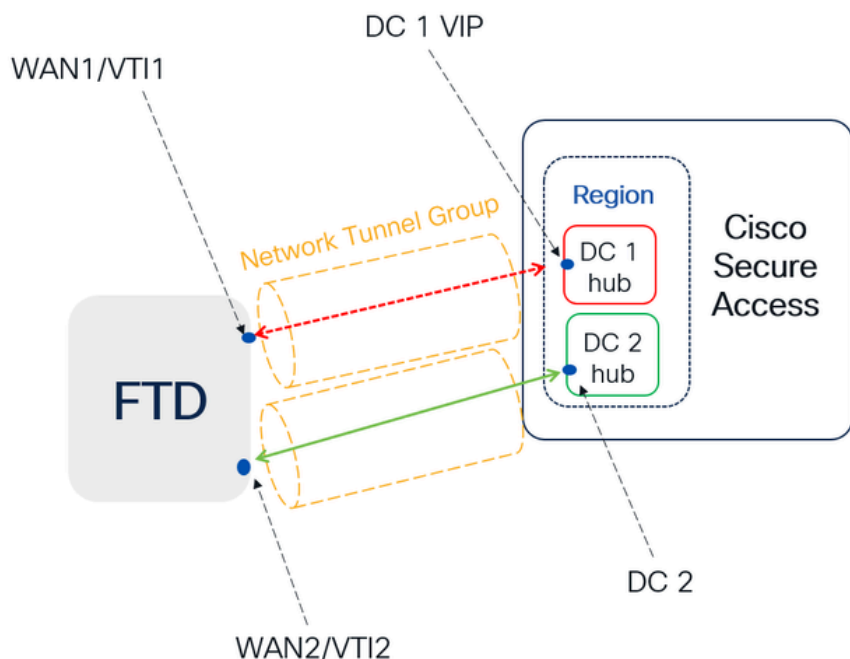
Normal Behavior



Secure Access default behavior

- DC2 is **passive** when DC1 is **active**
- Data Centers operating in High Availability (HA) mode ensure that only one tunnel receives traffic at a time. The other tunnel remains on standby and will drop any packets sent through it while in standby mode.

HA Behavior



Secure Access HA Behavior

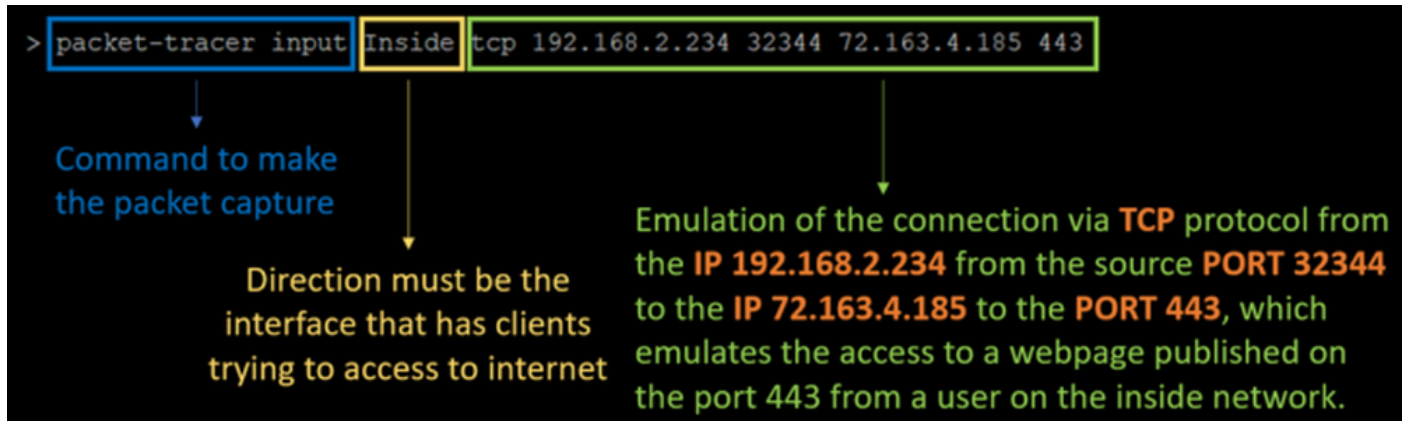
- DC2 is **Active** when DC1 or WAN1 peer is **Down**
- High availability is implemented to address failures in the WAN1 channel on the Firewall, ensuring operational continuity in the **region** and mitigating potential issues in DC1

Controleer de routing van het verkeer voor beveiligde toegang

In dit voorbeeld, gebruiken wij de bron als machine op het firewallnetwerk:

- Bron: 192.168.10.40
- Bestemming: 146.112.255.40 (IP voor beveiligde toegangsbewaking)

Voorbeeld:



Opdracht:

```
packet-tracer input LAN tcp 192.168.10.40 3422 146.112.255.40 80
```

Uitvoer:

```
Phase: 1
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Elapsed time: 14010 ns
Config:
Implicit Rule
Additional Information:
MAC Access list
```

```
Phase: 2
Type: PBR-LOOKUP
Subtype: policy-route
Result: ALLOW
Elapsed time: 21482 ns
Config:
route-map FMC_GENERATED_PBR_1707686032813 permit 5
  match ip address ACL
  set ip next-hop 169.254.2.2 169.254.3.2
Additional Information:
  Matched route-map FMC_GENERATED_PBR_1707686032813, sequence 5, permit
  Found next-hop 169.254.2.2 using egress ifc PrimaryVTI
```

```
Phase: 3
Type: OBJECT_GROUP_SEARCH
Subtype:
Result: ALLOW
Elapsed time: 0 ns
Config:
Additional Information:
  Source Object Group Match Count: 0
  Destination Object Group Match Count: 0
```

Object Group Search: 0

Phase: 4

Type: ACCESS-LIST

Subtype: log

Result: ALLOW

Elapsed time: 233 ns

Config:

access-group CSM_FW_ACL_ global

access-list CSM_FW_ACL_ advanced permit ip any ifc PrimaryVTI any rule-id 268434435

access-list CSM_FW_ACL_ remark rule-id 268434435: ACCESS POLICY: HOUSE - Mandatory

access-list CSM_FW_ACL_ remark rule-id 268434435: L7 RULE: New-Rule-#3-ALLOW

Additional Information:

This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 5

Type: CONN-SETTINGS

Subtype:

Result: ALLOW

Elapsed time: 233 ns

Config:

class-map class_map_Any

match access-list Any

policy-map policy_map_LAN

class class_map_Any

set connection decrement-ttl

service-policy policy_map_LAN interface LAN

Additional Information:

Phase: 6

Type: NAT

Subtype: per-session

Result: ALLOW

Elapsed time: 233 ns

Config:

Additional Information:

Phase: 7

Type: IP-OPTIONS

Subtype:

Result: ALLOW

Elapsed time: 233 ns

Config:

Additional Information:

Phase: 8

Type: VPN

Subtype: encrypt

Result: ALLOW

Elapsed time: 18680 ns

Config:

Additional Information:

Phase: 9

Type: VPN

Subtype: ipsec-tunnel-flow

Result: ALLOW

Elapsed time: 25218 ns

Config:

Additional Information:

Phase: 10

Type: NAT
Subtype: per-session
Result: ALLOW
Elapsed time: 14944 ns
Config:
Additional Information:

Phase: 11
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Elapsed time: 0 ns
Config:
Additional Information:

Phase: 12
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Elapsed time: 19614 ns
Config:
Additional Information:
New flow created with id 23811, packet dispatched to next module

Phase: 13
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Elapsed time: 27086 ns
Config:
Additional Information:
Application: 'SNORT Inspect'

Phase: 14
Type: SNORT
Subtype: appid
Result: ALLOW
Elapsed time: 28820 ns
Config:
Additional Information:
service: (0), client: (0), payload: (0), misc: (0)

Phase: 15
Type: SNORT
Subtype: firewall
Result: ALLOW
Elapsed time: 450193 ns
Config:
Network 0, Inspection 0, Detection 0, Rule ID 268434435
Additional Information:
Starting rule matching, zone 1 -> 3, geo 0 -> 0, vlan 0, src sgt: 0, src sgt type: unknown, dst sgt: 0,
Matched rule ids 268434435 - Allow

Result:
input-interface: LAN(vrfid:0)
input-status: up
input-line-status: up
output-interface: PrimaryVTI(vrfid:0)
output-status: up
output-line-status: up
Action: allow
Time Taken: 620979 ns

Hier, kan veel dingen ons context geven over de communicatie en weten of alles correct is onder de PBR configuratie om het verkeer correct te leiden naar Secure Access:

```
Phase: 2
Type: PBR-LOOKUP
Subtype: policy-route
Result: ALLOW
Elapsed time: 21482 ns
Config:
route-map FMC_GENERATED_PBR_1707686032813 permit 5
  match ip address ACL
  set ip next-hop 169.254.2.2 169.254.3.2
Additional Information:
  Matched route-map FMC_GENERATED_PBR_1707686032813, sequence 5, permit
  Found next-hop 169.254.2.2 using egress ifc PrimaryVTI
```

Fase 2 geeft aan dat het verkeer wordt doorgestuurd naar de PrimaryVTI interface, wat correct is omdat, op basis van de configuraties in dit scenario, het internetverkeer moet worden doorgestuurd naar Secure Access via de VTI.

Phase: 8

Type: VPN

Subtype: encrypt

Result: ALLOW

Elapsed time: 18680 ns

Config:

Additional Information:

Phase: 9

Type: VPN

Subtype: ipsec-tunnel-flow

Result: ALLOW

Elapsed time: 25218 ns

Config:

Additional Information:

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.