

Konfigurieren eines sicheren Zugriffs mit einer sicheren Firewall mit hoher Verfügbarkeit

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Netzwerkdigramm](#)

[Konfigurieren](#)

[Konfigurieren des VPN für sicheren Zugriff](#)

[Daten für Tunnel-Setup](#)

[Konfigurieren des Tunnels auf einer sicheren Firewall](#)

[Konfigurieren der Tunnelschnittstelle](#)

[Konfigurieren einer statischen Route für die sekundäre Schnittstelle](#)

[Konfigurieren des VPN für sicheren Zugriff im VTI-Modus](#)

[Endgerätekonfiguration](#)

[IKE-Konfiguration](#)

[IPSEC-Konfiguration](#)

[Erweiterte Konfiguration](#)

[Szenarien für die Konfiguration von Zugriffsrichtlinien](#)

[Szenario mit Internetzugriff](#)

[RA-VPN-Szenario](#)

[CLAP-BAP-ZTNA-Szenario](#)

[Richtlinienbasierte Weiterleitung konfigurieren](#)

[Konfigurieren der Internet-Zugriffsrichtlinie für sicheren Zugriff](#)

[Konfigurieren des Zugriffs auf private Ressourcen für ZTNA und RA-VPN](#)

[Fehlerbehebung](#)

[Phase 1 überprüfen \(IKEv2\)](#)

[Phase 2 \(IPSEC\) überprüfen](#)

[Hochverfügbarkeitsfunktion](#)

[Überprüfen der Datenverkehrsweiterleitung für den sicheren Zugriff](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie sicheren Zugriff mit einer sicheren Firewall mit hoher Verfügbarkeit konfigurieren.

Voraussetzungen

- [Konfiguration der Benutzerbereitstellung](#)
- [Konfiguration der ZTNA SSO-Authentifizierung](#)
- [Konfigurieren des sicheren Remotezugriff-VPN](#)

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Firepower Management Center 7.2
- FirePOWER Threat Defense 7.2
- Sicherer Zugriff
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA
- Clientless-ZTNA

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf:

- Firepower Management Center 7.2
- FirePOWER Threat Defense 7.2
- Sicherer Zugriff
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

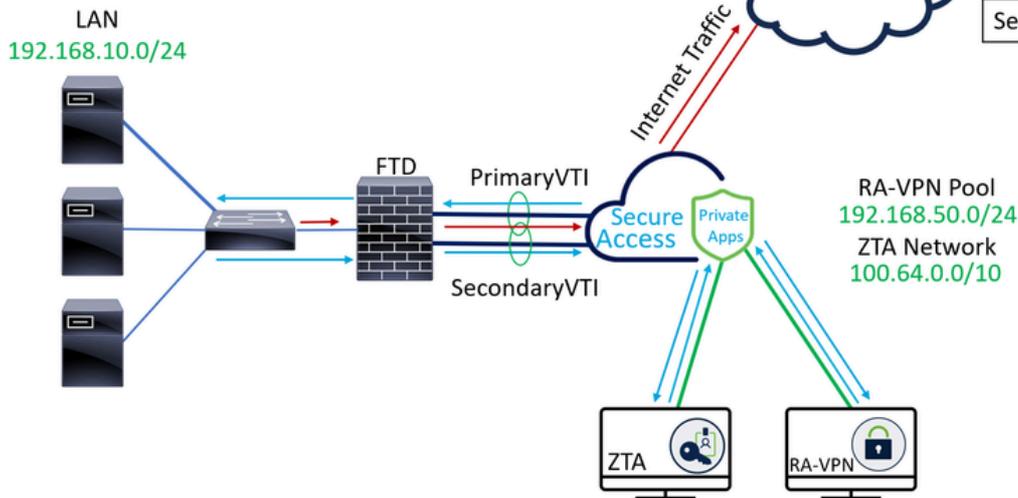


Cisco hat Secure Access entwickelt, um den Zugriff auf private Anwendungen vor Ort und in der Cloud zu schützen. Außerdem wird die Verbindung vom Netzwerk zum Internet gesichert. Dies wird durch die Implementierung mehrerer Sicherheitsmethoden und -ebenen erreicht, die alle darauf abzielen, die Informationen beim Zugriff über die Cloud zu erhalten.

Netzwerkdiagramm

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

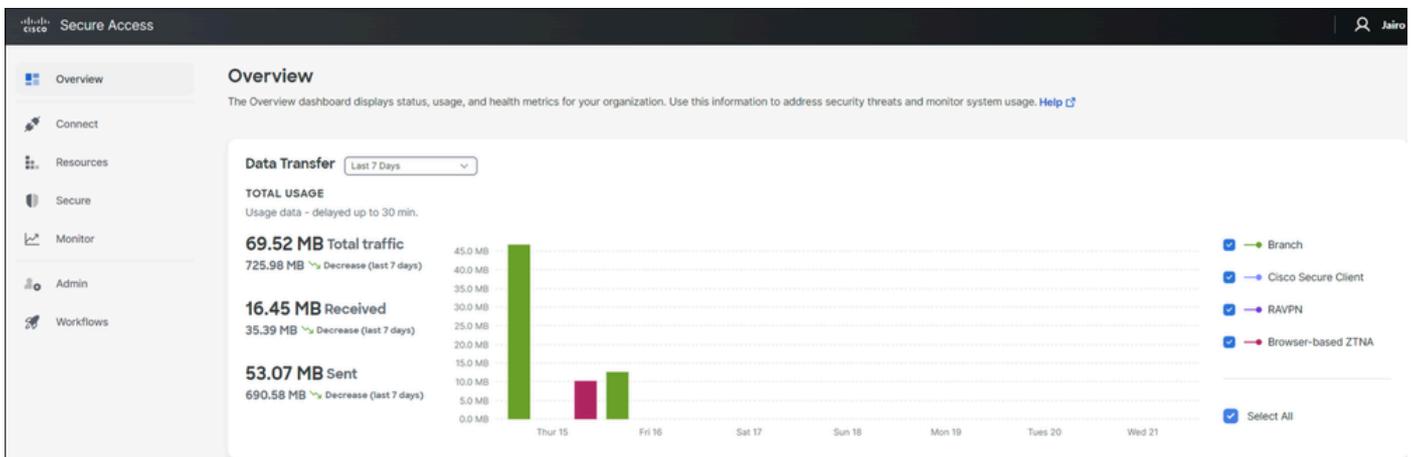
INTERFACE	IP
PrimaryWAN	192.168.30.5
PrimaryVTI	169.254.2.1
SecondaryWAN	192.168.0.202
SecondaryVTI	169.254.3.1



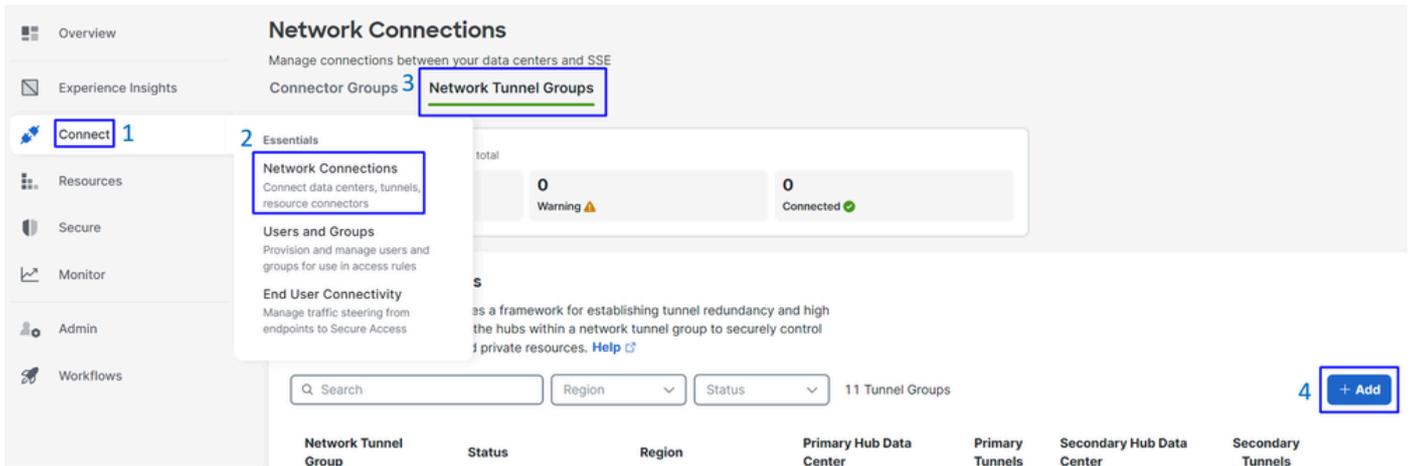
Konfigurieren

Konfigurieren des VPN für sicheren Zugriff

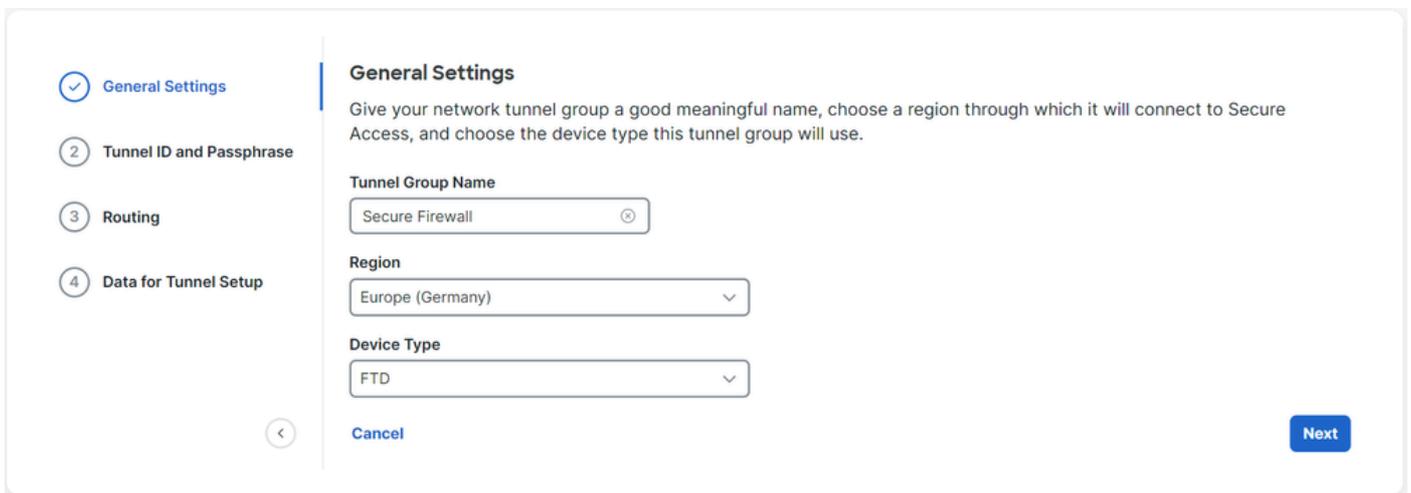
Navigieren Sie zum Admin-Bereich von [Sicherer Zugriff](#).



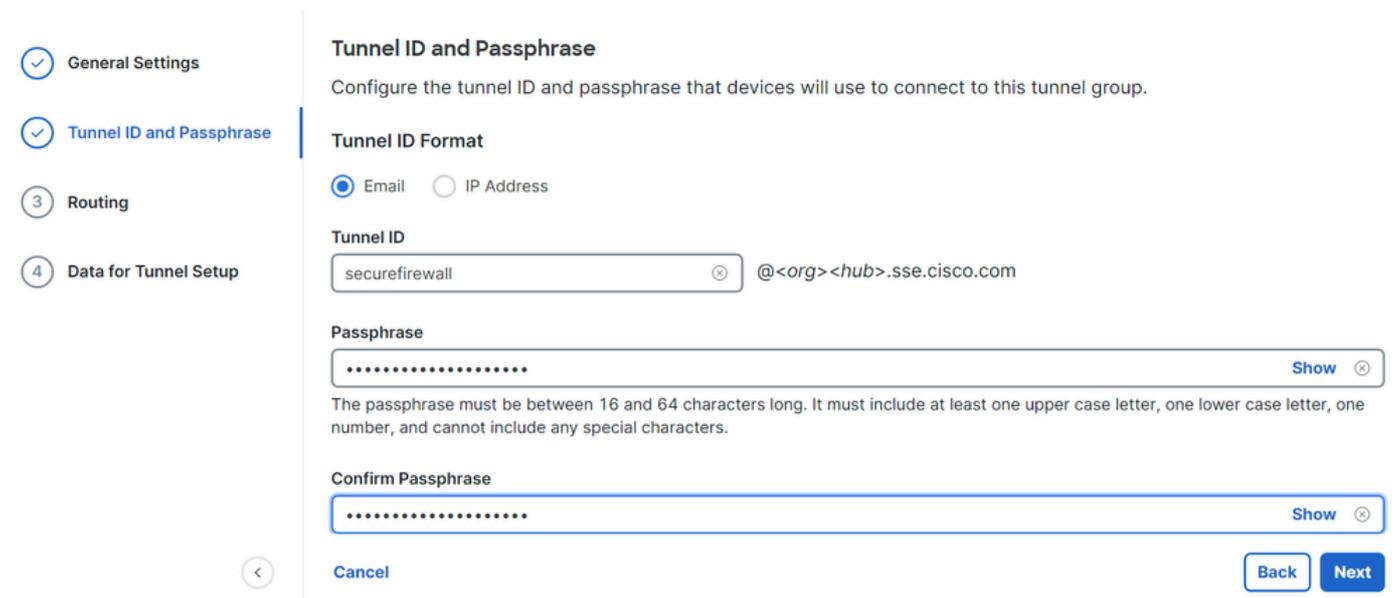
- Klicken Sie Connect > Network Connections
- Klicken Sie unter Network Tunnel Groups auf + Add



- Konfigurieren Sie die Tunnel Group Name, Region und Device Type
- Klicken Sie auf Next



- Konfigurieren Sie die Tunnel ID Format und Passphrase
- Klicken Sie auf Next



- Konfigurieren Sie die IP-Adressbereiche oder Hosts, die Sie in Ihrem Netzwerk konfiguriert

haben, und leiten Sie den Datenverkehr über sicheren Zugriff weiter.

- Klicken Sie auf **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.

192.168.0.0/24

192.168.10.0/24

Dynamic routing

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

[Cancel](#)

Nachdem Sie auf **save** die Informationen über den Tunnel angezeigt wird, bitte speichern Sie diese Informationen für den nächsten Schritt, **Configure the tunnel on Secure Firewall**.

Daten für Tunnel-Setup

- 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.

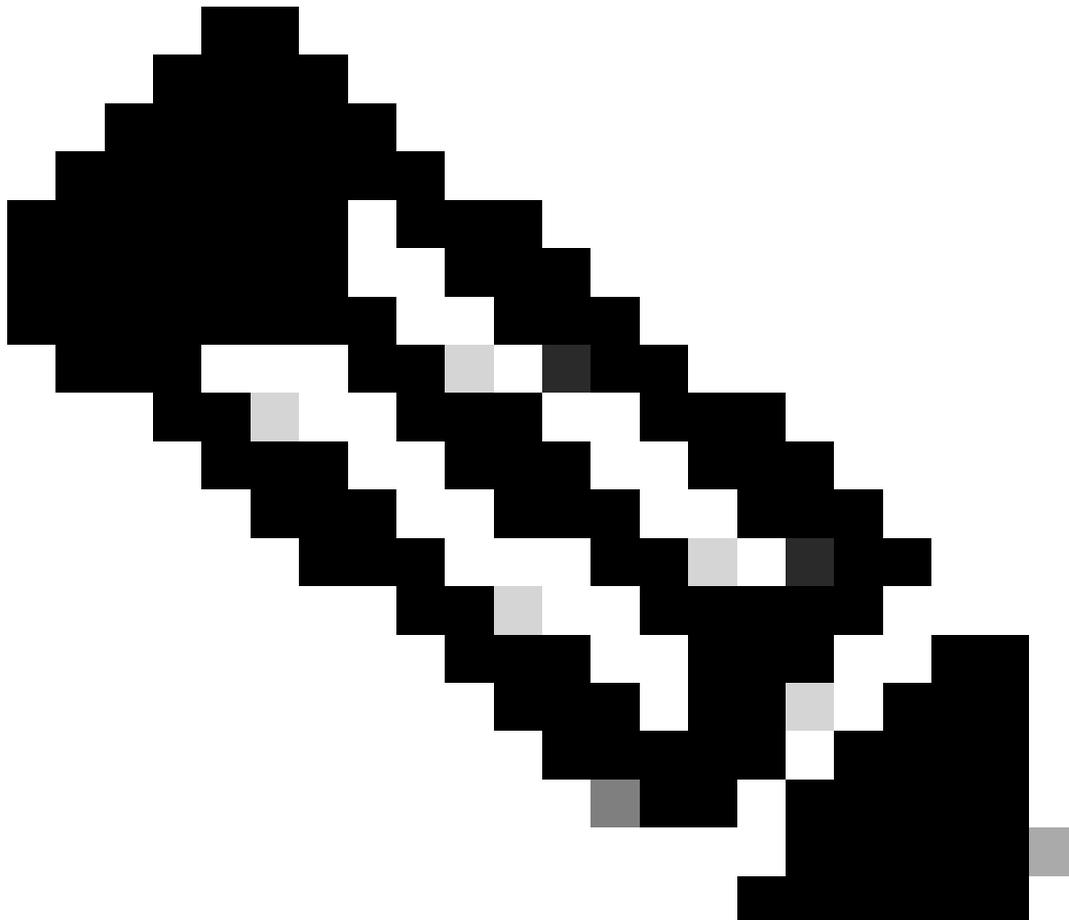
Primary Tunnel ID:	securefirewall@[redacted]-sse.cisco.com <input type="button" value="copy"/>
Primary Data Center IP Address:	18.156.145.74 <input type="button" value="copy"/>
Secondary Tunnel ID:	securefirewall@[redacted]-sse.cisco.com <input type="button" value="copy"/>
Secondary Data Center IP Address:	3.120.45.23 <input type="button" value="copy"/>
Passphrase:	[redacted] <input type="button" value="copy"/>

Konfigurieren des Tunnels auf einer sicheren Firewall

Konfigurieren der Tunnelschnittstelle

In diesem Szenario verwenden Sie die VTI-Konfiguration (Virtual Tunnel Interface) auf der sicheren Firewall, um dieses Ziel zu erreichen. Denken Sie daran, dass Sie in diesem Fall einen doppelten ISP haben, und dass wir Hochverfügbarkeit benötigen, wenn einer Ihrer ISPs ausfällt.

SCHNITTSTELLEN	ROLLE
PrimärWAN	Principal Internet WAN
Sekundäres WAN	Sekundäres Internet-WAN
PrimärVTI	Verlinkt zum Senden des Datenverkehrs an Secure Access über Principal Internet WAN das
Sekundäre VTI	Verlinkt zum Senden des Datenverkehrs an Secure Access über Secondary Internet WAN das



Anmerkung: 1. Sie müssen eine statische Route zur hinzufügen oder der **Primary or Secondary Datacenter IP** zuweisen, damit beide Tunnel verfügbar sind.



Anmerkung: 2. Wenn zwischen den Schnittstellen ECMP konfiguriert ist, müssen Sie keine statische Route zu erstellen, **Primary or Secondary Datacenter IP** damit beide Tunnel verfügbar sind.

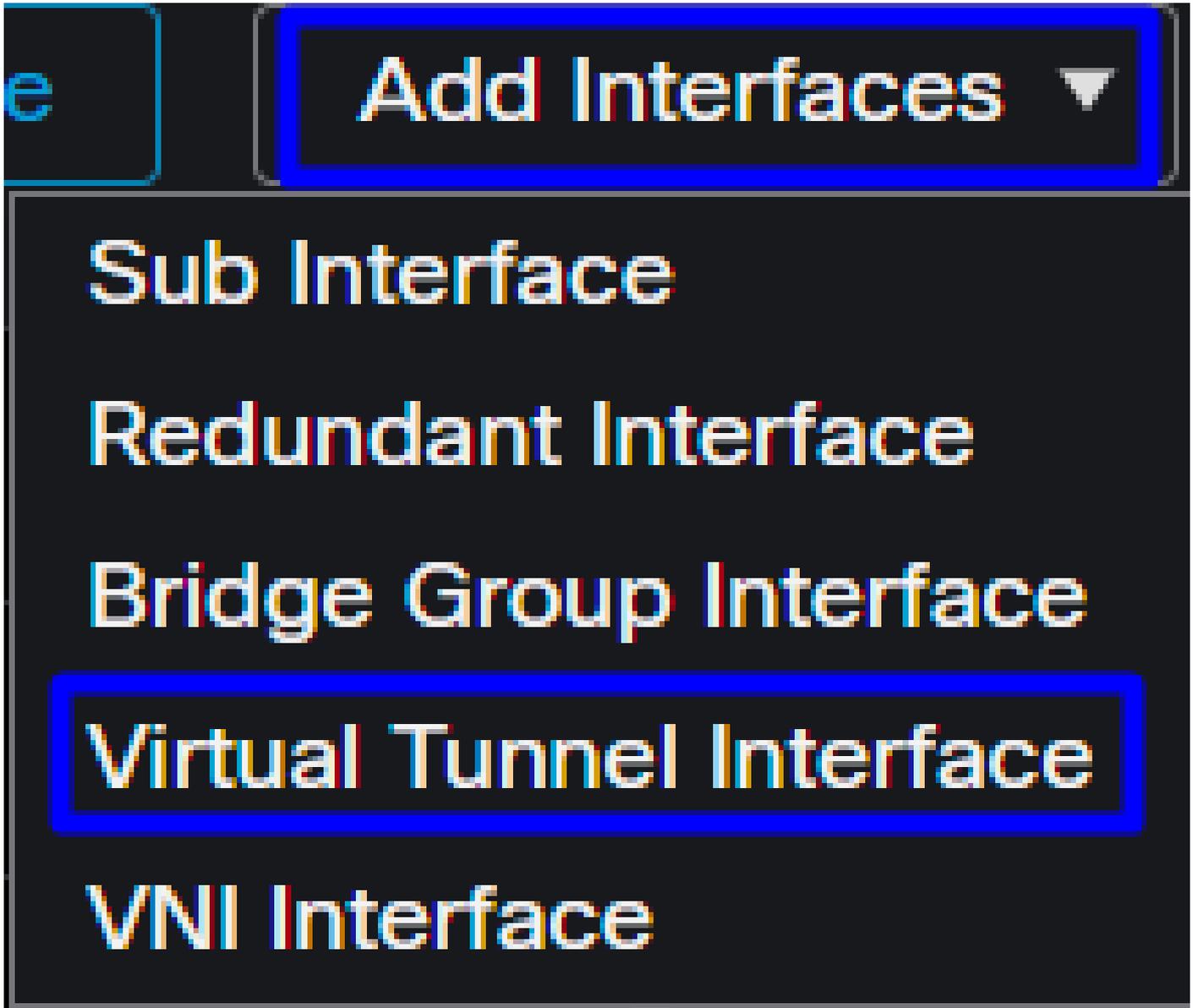
Basierend auf dem Szenario verfügen wir über **PrimaryWAN** und **SecondaryWAN**, mit denen wir die VTI-Schnittstellen erstellen müssen.

Navigieren Sie zu Ihrem **Firepower Management Center > Devices**.

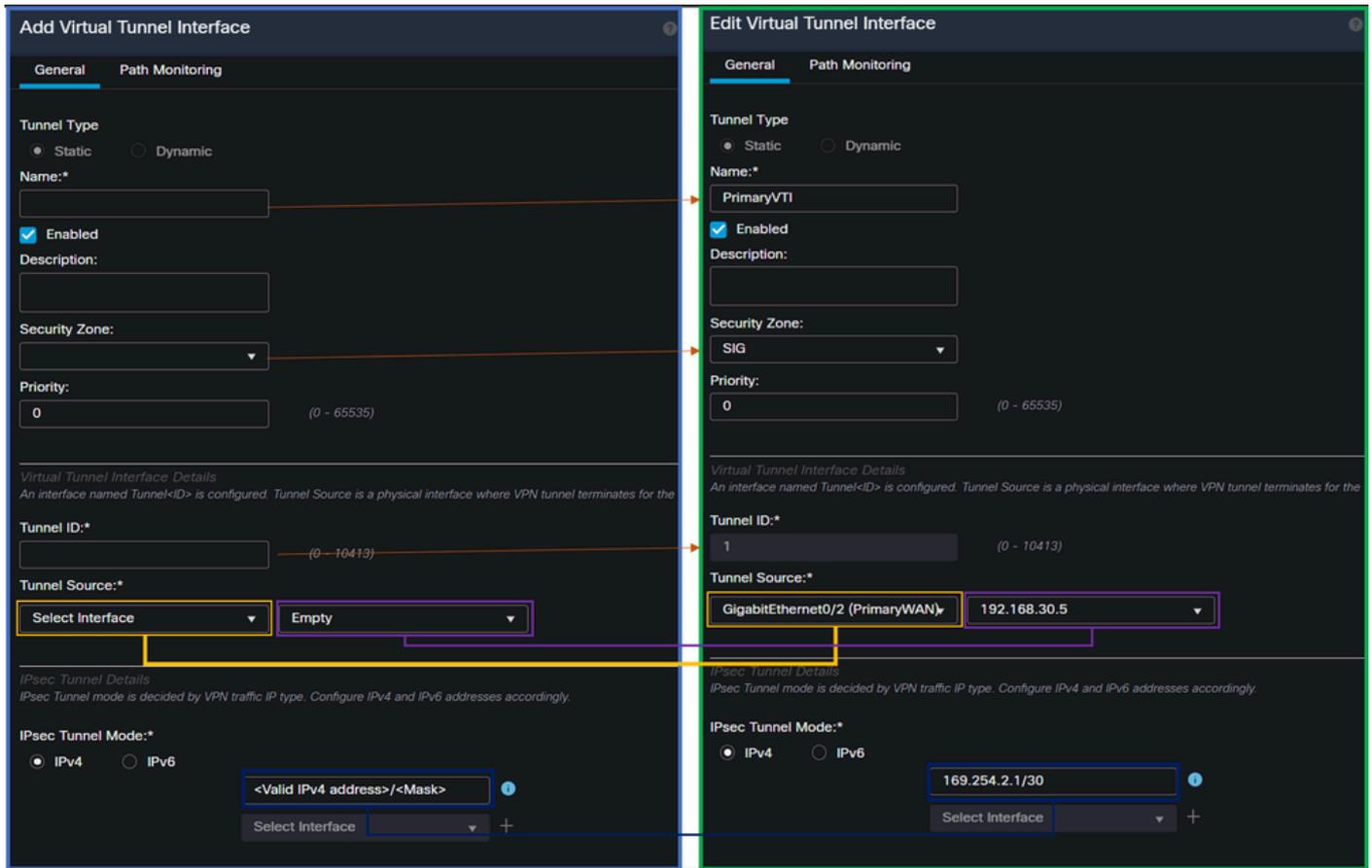
- Wählen Sie Ihren FTD
- Auswählen **Interfaces**

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)

- Klicken Sie **Add Interfaces > Virtual Tunnel Interface**



- Konfigurieren Sie die Schnittstelle anhand der nächsten Informationen.



- **Name** : Konfigurieren Sie einen Namen, der sich auf **PrimaryWAN interface**
- **Security Zone** : Sie können einen anderen **Security Zone** verwenden, aber es ist besser, einen neuen für den sicheren Datenverkehr zu erstellen.
- **Tunnel ID** : Nummer für Tunnel-ID hinzufügen
- **Tunnel Source** : Wählen Sie Ihre **PrimaryWAN interface** , und wählen Sie die private oder öffentliche IP-Adresse Ihrer Schnittstelle aus.
- **IPsec Tunnel Mode** : Wählen **IPv4** und konfigurieren Sie eine nicht routbare IP in Ihrem Netzwerk mit Maske 30



Anmerkung: Für die VTI-Schnittstelle muss eine nicht routbare IP-Adresse verwendet werden. Wenn Sie beispielsweise über zwei VTI-Schnittstellen verfügen, können Sie 169.254.2.1/30 für die **PrimaryVTI** und 169.254.3.1/30 für die **SecondaryVTI** verwenden.

Danach müssen Sie das Gleiche für die **tun**, **SecondaryWAN interface** und Sie haben alles für die VTI High Availability eingerichtet, und als Ergebnis haben Sie das nächste Ergebnis:

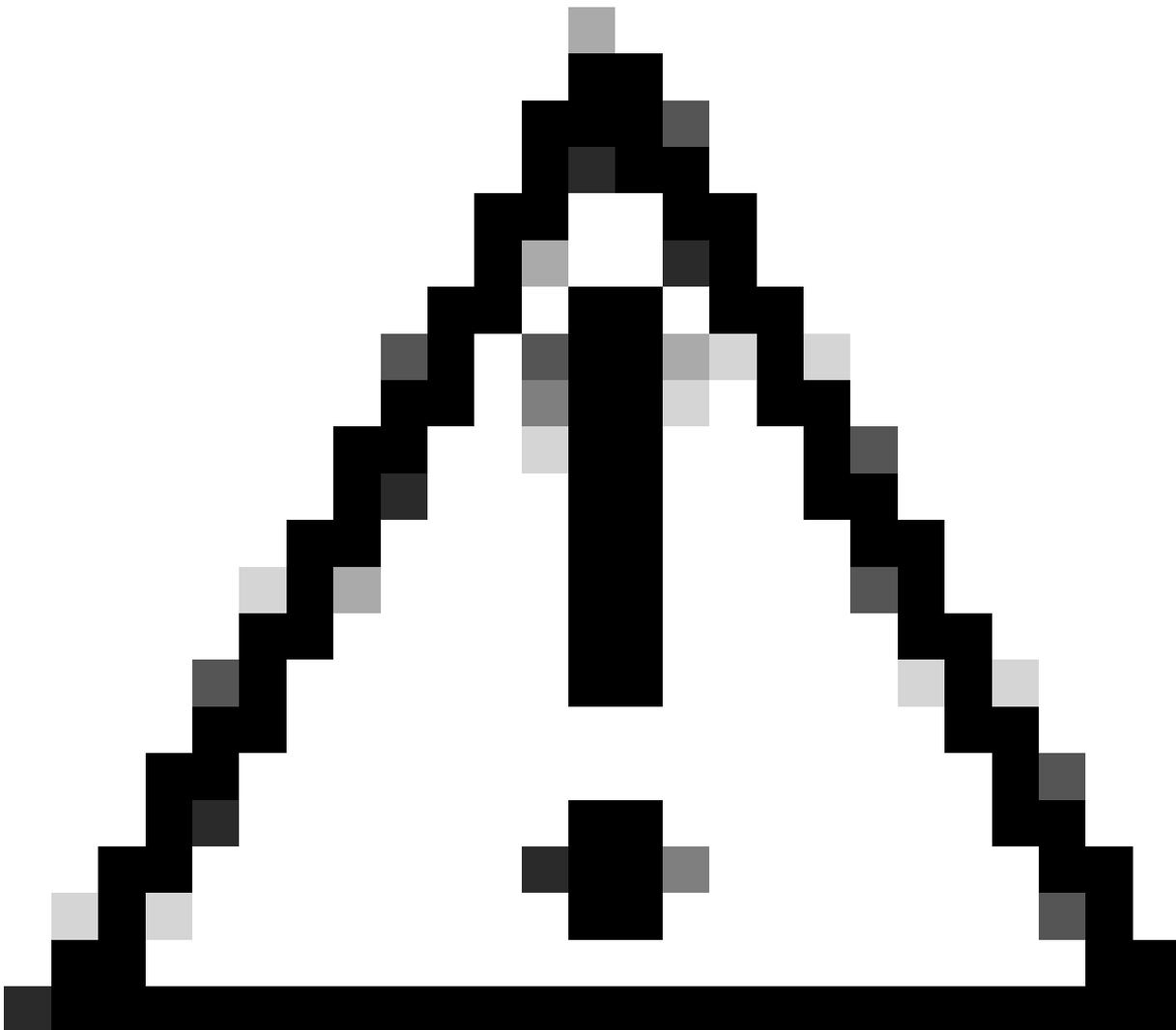
Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
Diagnostic0/0	diagnostic	Physical			
GigabitEthernet0/0	SecondaryWAN	Physical	SecondaryWAN		192.168.0.202/24(Static)
Tunnel2	SecondaryVTI	VTI	SIG		169.254.3.1/30(Static)
GigabitEthernet0/1	LAN	Physical	LAN		192.168.10.1/24(Static)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

Für dieses Szenario werden folgende IPs verwendet:

VTI IP-Konfiguration		
Logischer Name	IP	Bereich
PrimärVTI	169.254.2.1/30	169.254.2.1-169.254.2.2
Sekundäre VTI	169.254.3.1/30	169.254.3.1-169.254.3.2

Konfigurieren einer statischen Route für die sekundäre Schnittstelle

Damit der Datenverkehr der **Secondary WAN interface** die erreichen kann, müssen Sie eine statische Route zur IP-Adresse des **Secondary Datacenter IP Address** Rechenzentrums konfigurieren. Sie können ihn mit einer Metrik von eins (1) konfigurieren, um ihn an die Spitze der Routing-Tabelle zu setzen. Geben Sie außerdem die IP als Host an.



Vorsicht: Dies ist nur erforderlich, wenn zwischen den WAN-Kanälen kein ECMP eingerichtet wurde. Wenn Sie ECMP konfiguriert haben, können Sie mit dem nächsten Schritt fortfahren.

Navigieren Sie zu **Device > Device Management**

- Klicken Sie auf Ihr FTD-Gerät.
- Klicken Sie **Routing**
- Auswählen **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

Selected Network

SecureAccessTunnel 

Choose the Secondary Datacenter IP

192.168.0.150

192.168.10.153

any-ipv4

ASA_GW

CSA_Primary

GWT1

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:** Wählen Sie die sekundäre WAN-Schnittstelle aus
- **Gateway:** Wählen Sie das sekundäre WAN-Gateway aus
- **Selected Network:** Fügen Sie die sekundäre Rechenzentrums-IP als Host hinzu. finden Sie die Informationen zu den Informationen, die Sie beim Konfigurieren des Tunnels im Schritt Sicherer Zugriff, [Daten für Tunnleinrichtung, erhalten haben.](#)

- **Metric:** Eine verwenden (1)
- **OK** Klicken Sie **Save** auf und, um die Informationen zu speichern und dann bereitzustellen.

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						

Konfigurieren des VPN für sicheren Zugriff im VTI-Modus

Um das VPN zu konfigurieren, navigieren Sie zu Ihrer Firewall:

- Klicken Sie **Devices > Site to Site**
- Klicken Sie **+ Site to Site VPN**

Endgerätekonfiguration

Zum Konfigurieren des Schritts "Endgeräte" müssen Sie die Informationen aus dem Schritt "[Daten für Tunnleinrichtung](#)" verwenden.

Create New VPN Topology

Topology Name:*

Policy Based (Crypto Map) Route Based (VTI)

Network Topology:

IKE Version:* IKEv1 IKEv2

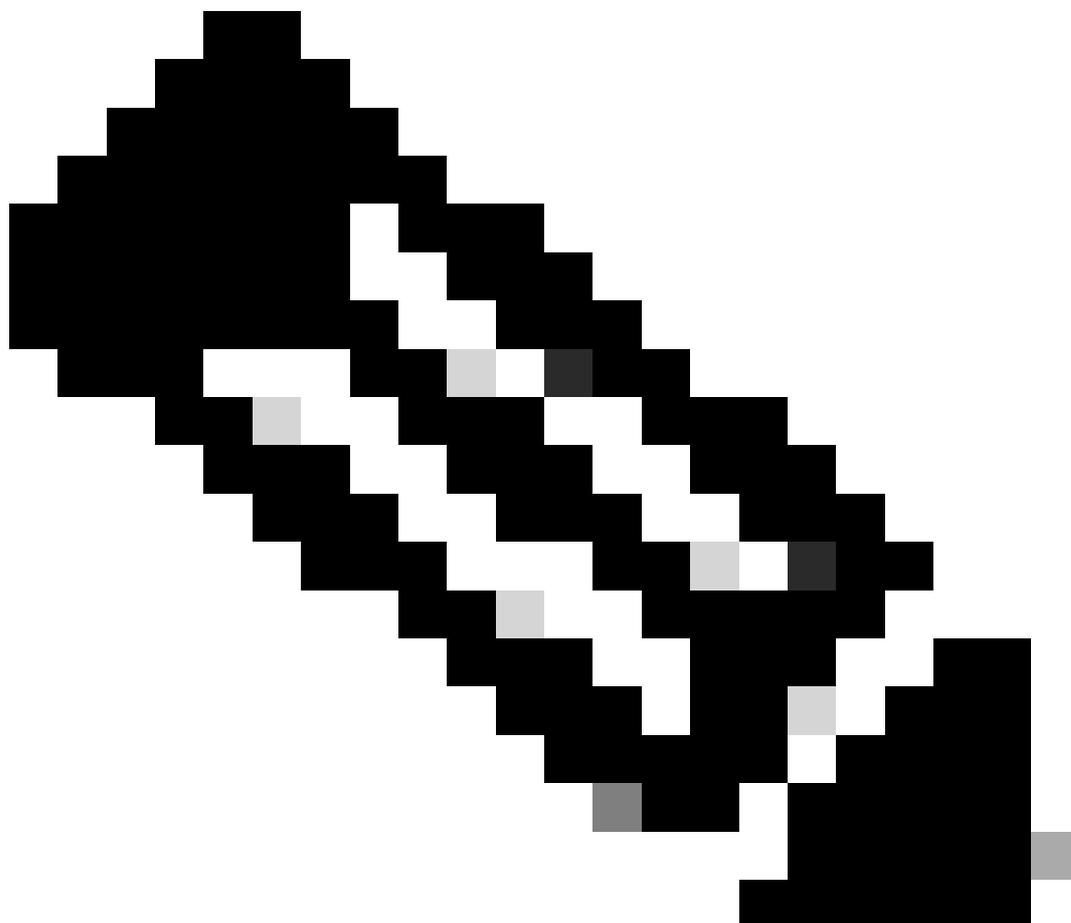
Endpoints | IKE | IPsec | Advanced

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](#)

- Topologienname: Erstellen eines Namens für die Secure Access-Integration
- Auswählen **Routed Based (VTI)**

- Auswählen **Point to Point**
 - IKE Version: IKEv2 auswählen
-



Anmerkung: IKEv1 wird für die Integration mit Secure Access nicht unterstützt.

Unter **Node A**müssen Sie die folgenden Parameter konfigurieren:

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@

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

- **Device:** Wählen Sie Ihr FTD-Gerät
- **Virtual Tunnel Interface:** Wählen Sie den VTI aus, der mit der PrimaryWAN Interface Verknüpft ist.
- Aktivieren Sie das Kontrollkästchen für **Send Local Identity to Peers**
- **Local Identity Configuration:** Wählen Sie die E-Mail-ID aus, und geben Sie die Informationen gemäß den Angaben in Ihrer Konfiguration im Schritt "[Daten für Tunnel-Setup](#)" Primary Tunnel ID ein.

Nachdem Sie die Informationen konfiguriert haben, klicken Sie auf den PrimaryVTI folgenden Link **+ 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:** Wählen Sie den VTI aus, der mit der PrimaryWAN Interface verknüpft ist.
- Aktivieren Sie das Kontrollkästchen für **Send Local Identity to Peers**
- **Local Identity Configuration:** Wählen Sie die E-Mail-ID aus, und geben Sie die Informationen gemäß den Angaben in Ihrer Konfiguration im Schritt "[Daten für Tunnel-Setup](#)" Secondary Tunnel ID ein.

Unter **Node B** müssen Sie die folgenden Parameter konfigurieren:

Node B

Device:*

Extranet

Device Name*:

SecureAccess

Endpoint IP Address*:

18.156.145.74, 3.120.45.23

- **Device:** Extranet
- **Device Name:** Wählen Sie einen Namen aus, um Secure Access als Ziel zu erkennen.
- **Endpoint IP Address:** Die Konfiguration für die primäre und sekundäre Konfiguration muss die primäre sein. Diese Informationen finden Sie **Datacenter IP, Secondary Datacenter IP** im Schritt "[Daten für Tunnel-Setup](#)".

Danach ist die Konfiguration für abgeschlossen, und Sie können **Endpoints** mit dem Schritt "IKE-Konfiguration" fortfahren.

IKE-Konfiguration

Um die IKE-Parameter zu konfigurieren, klicken Sie auf **IKE**.

Endpoints

IKE

IPsec

Advanced

Unter müssen IKE, Sie die nächsten Parameter konfigurieren:

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:** Sie können die Standard-Umbrella-Konfiguration verwenden `Umbrella-AES-GCM-256` oder auf der Grundlage des [Supported IKEv2 and IPSEC Parameters](#)
- **Authentication Type:** Vorinstallierter manueller Schlüssel
- **Key** und **Confirm Key:** Sie finden die **Passphrase** Informationen im Schritt [Daten für Tunneleinrichtung](#).

Danach ist Ihre Konfiguration für abgeschlossen, und Sie können **IKE** mit dem Schritt "IPSEC-Konfiguration" fortfahren.

IPSEC-Konfiguration

Um die IPSEC-Parameter zu konfigurieren, klicken Sie auf IPSEC.

Endpoints

IKE

IPsec

Advanced

Unter müssen IPSEC, Sie die nächsten Parameter konfigurieren:

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: Sie können die Standard-Umbrella-Konfiguration verwenden Umbrella-AES-GCM-256 oder auf der Grundlage des [Supported IKEv2 and IPSEC Parameters](#)

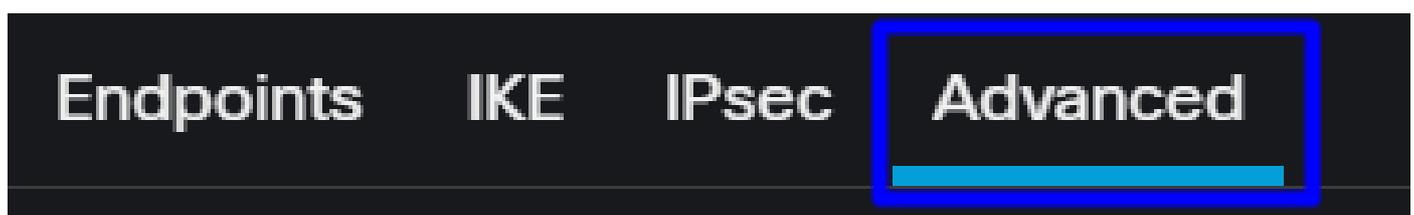


Anmerkung: Für IPSEC ist nichts anderes erforderlich.

Danach ist Ihre Konfiguration für abgeschlossen, und Sie können nun **IPSEC** mit dem Schritt "Erweiterte Konfiguration" fortfahren.

Erweiterte Konfiguration

Um die erweiterten Parameter zu konfigurieren, klicken Sie auf **Erweitert**.



Unter müssen **Advanced**, Sie die nächsten Parameter konfigurieren:

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

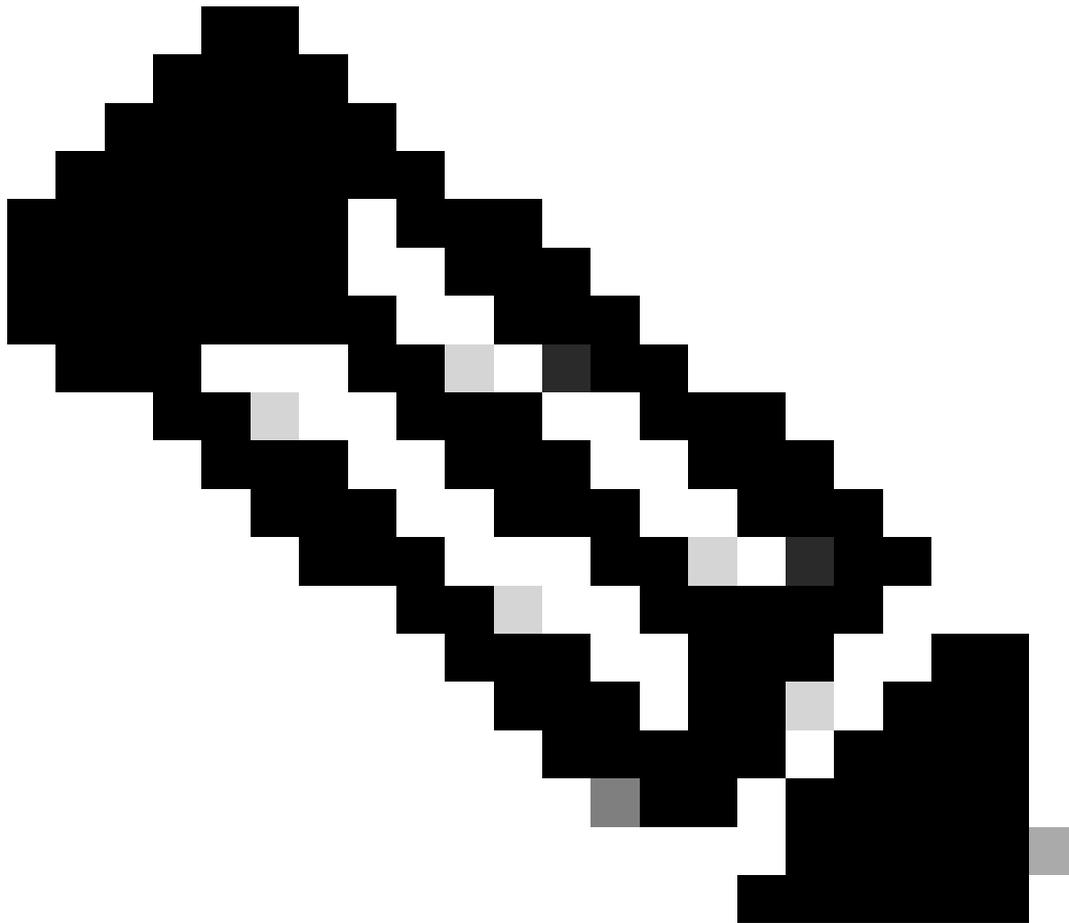
Enable Notification on Tunnel Disconnect

IKEv2 Security Association (SA) Settings

Cookie Challenge: custom

- IKE Keepalive: Enable
- Threshold: 10
- Retry Interval: 2
- Identity Sent to Peers: AutoOderDN
- Peer Identity Validation: Nicht prüfen

Danach können Sie auf **Save** und **Deploy** klicken.



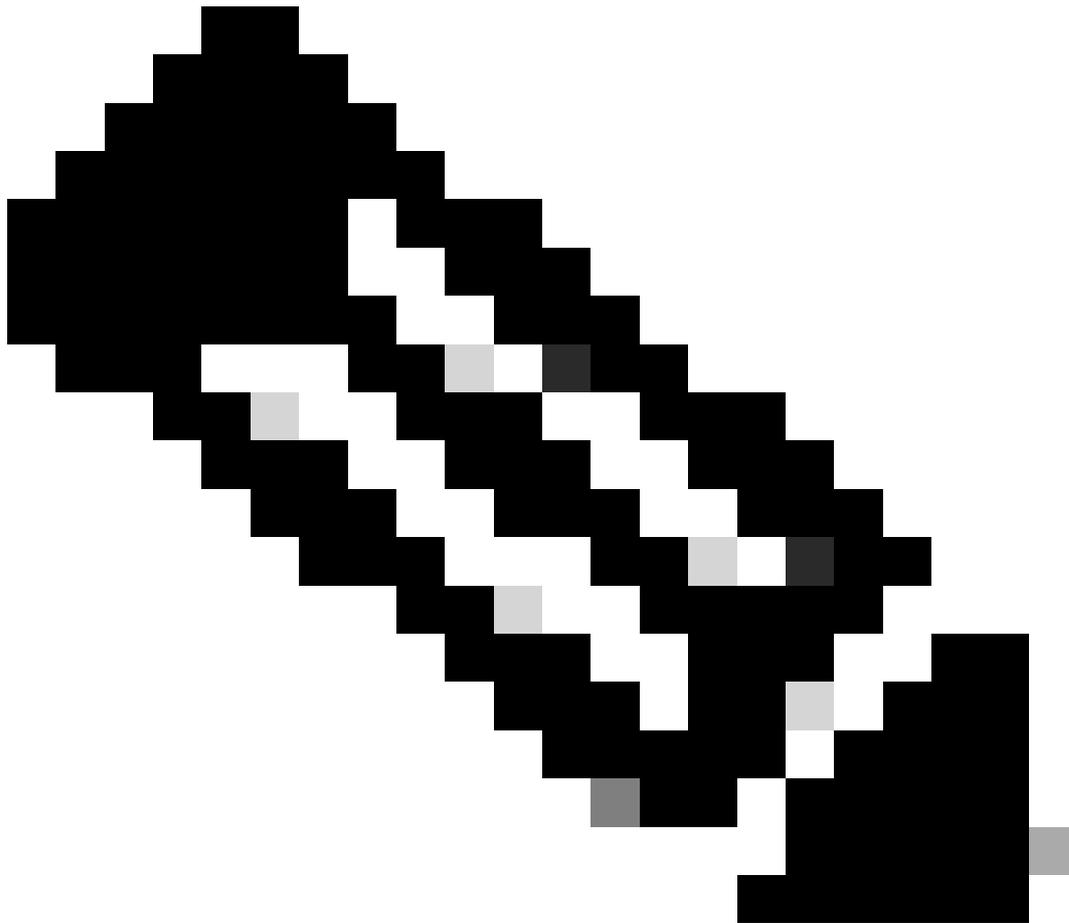
Anmerkung: Nach einigen Minuten wird das VPN für beide Knoten eingerichtet.

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)

Danach ist Ihre Konfiguration für den abgeschlossen, und Sie können VPN to Secure Access in VTI Mode nun mit dem Schritt fortfahren **Configure Policy Base Routing**.



Warnung: Der Datenverkehr zu Secure Access wird nur dann an den primären Tunnel weitergeleitet, wenn beide Tunnel eingerichtet sind. Wenn der primäre Tunnel ausfällt, lässt Secure Access die Weiterleitung des Datenverkehrs durch den sekundären Tunnel zu.



Hinweis: Das Failover am Secure Access-Standort basiert auf den DPD-Werten, die im [Benutzerhandbuch](#) für unterstützte IPsec-Werte dokumentiert sind.

Szenarien für die Konfiguration von Zugriffsrichtlinien

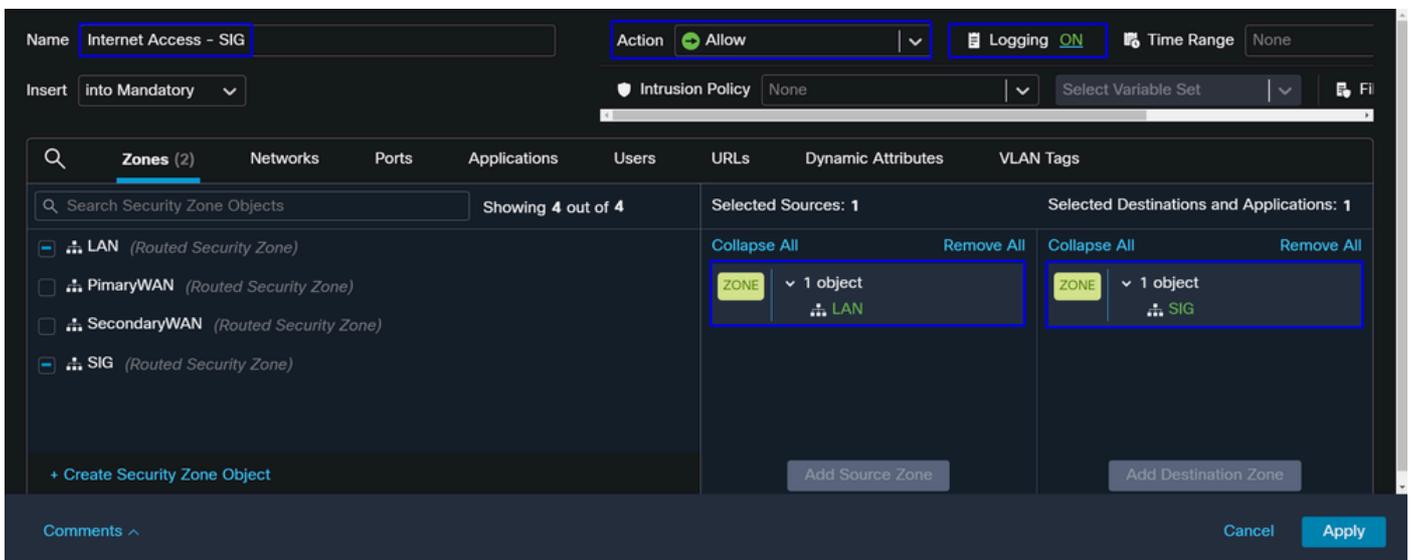
Die definierten Zugriffsrichtlinienregeln basieren auf:

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)

Schnittstelle	Zone
PrimärVTI	SIGNIEREN
Sekundäre VTI	SIGNIEREN
LAN	LAN

Szenario mit Internetzugriff

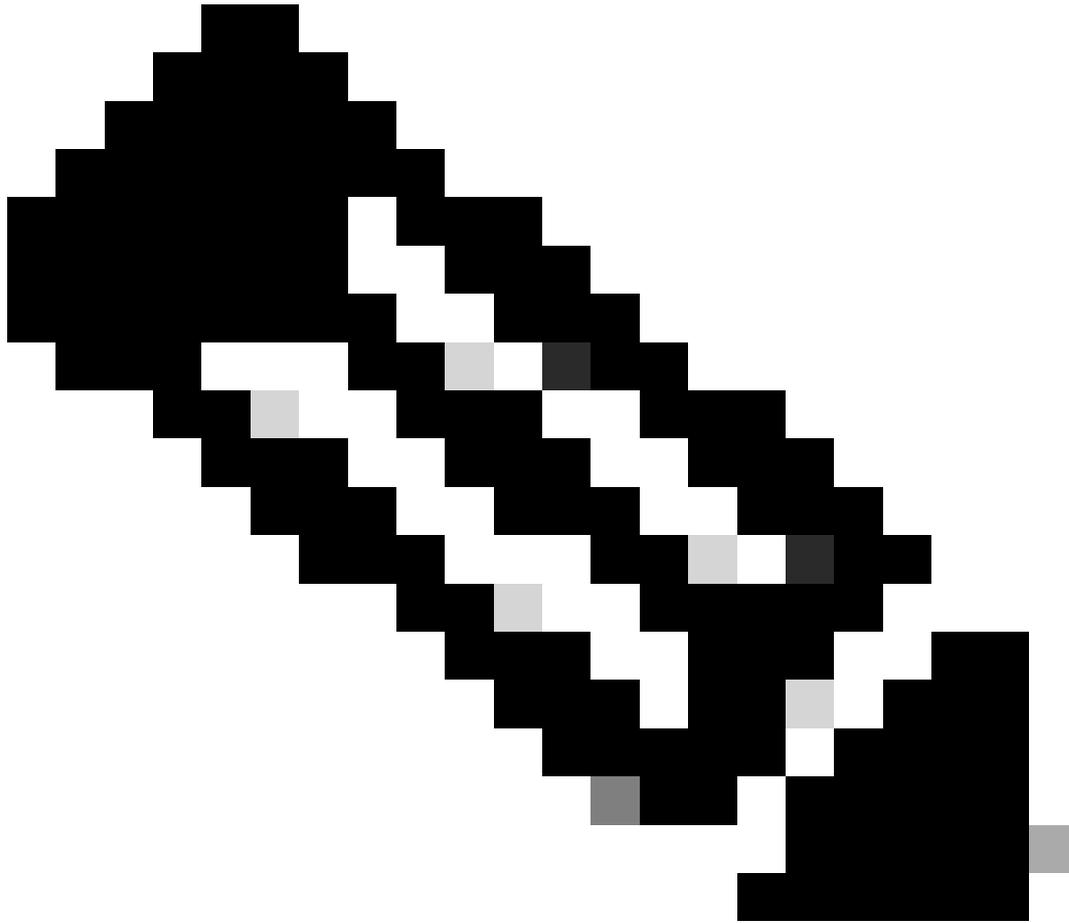
Um allen Ressourcen, die Sie auf dem richtlinienbasierten Routing konfigurieren, Zugriff auf das Internet zu ermöglichen, müssen Sie einige Zugriffsregeln sowie einige Richtlinien für sicheren Zugriff konfigurieren. Lassen Sie mich daher erklären, wie Sie dies in diesem Szenario erreichen:



Diese Regel ermöglicht den Zugriff auf das LAN Internet, in diesem Fall auf das Internet SIG.

RA-VPN-Szenario

Um den Zugriff durch die RA-VPN-Benutzer zu ermöglichen, muss dieser auf der Grundlage des Bereichs konfiguriert werden, den Sie dem RA-VPN-Pool zugewiesen haben.



Anmerkung: Die RA-VPNaaS-Richtlinie können Sie über "[Manage Virtual Private Networks](#)" (Virtuelle private Netzwerke verwalten) konfigurieren.

Wie überprüfen Sie den IP-Pool Ihres VPNaaS?

Navigieren Sie zu Ihrem [Dashboard für sicheren Zugriff](#).

- Klicken Sie **Connect** > End User Connectivity
- Klicken Sie **Virtual Private Network**
- Klicken Sie **Manage IP Pools** unter auf **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

- Du siehst dein Becken unter **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

- Sie müssen diesen Bereich unter SIG zulassen, ihn aber auch unter der ACL hinzufügen, die Sie in Ihrem PBR konfigurieren.

Konfiguration von Zugriffsregeln

Wenn Sie Secure Access nur so konfigurieren, dass es mit den Funktionen für den Zugriff auf private Anwendungsressourcen verwendet wird, kann Ihre Zugriffsregel wie folgt aussehen:

The screenshot shows the configuration of a rule named 'Private APP'. The rule is set to 'Allow' with logging on. The source is configured with two selected networks: 192.168.50.0/24 (under a NET object) and 192.168.10.153 (under a ZONE object). The destination is configured with one selected network: LAN (under a ZONE object). The rule is applied to the 'Mandatory' zone.

Diese Regel lässt Datenverkehr vom RA-VPN-Pool 192.168.50.0/24 zu Ihrem LAN zu. können Sie bei Bedarf weitere angeben.

ACL-Konfiguration

Um den Routing-Verkehr von SIG zu Ihrem LAN zuzulassen, müssen Sie ihn unter der ACL hinzufügen, damit er unter dem PBR funktioniert.

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-Szenario

Sie müssen Ihr Netzwerk auf der Grundlage des CGNAT-Bereichs 100.64.0.0/10 konfigurieren, um den Zugriff auf Ihr Netzwerk über die Client Base ZTA- oder Browser Base ZTA-Benutzer zu ermöglichen.

Konfiguration von Zugriffsregeln

Wenn Sie Secure Access nur so konfigurieren, dass es mit den Funktionen für den Zugriff auf private Anwendungsressourcen verwendet wird, kann Ihre Zugriffsregel wie folgt aussehen:

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

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

Search Network and Geolocation Objects 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 Selected Destinations and Applications: 1

Selected Sources:

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

Selected Destinations and Applications:

- ZONE 1 object: LAN

+ Create Network Object Manually Enter IP: Add Source Network Add Destination Network

Diese Regel lässt Datenverkehr von der ZTNA CGNAT-Reihe 100.64.0.0/10 zu Ihrem LAN zu.

ACL-Konfiguration

Um den Routing-Datenverkehr von SIG über CGNAT zu Ihrem LAN zuzulassen, müssen Sie ihn unter der ACL hinzufügen, damit er unter dem PBR funktioniert.

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		

Richtlinienbasierte Weiterleitung konfigurieren

Um den Zugriff auf interne Ressourcen und das Internet über sicheren Zugriff zu ermöglichen, müssen Sie Routen über Policy Base Routing (PBR) erstellen, die das Routing des Datenverkehrs von der Quelle zum Ziel vereinfachen.

- Navigieren Sie zu **Devices > Device Management**
- Wählen Sie das FTD-Gerät, auf dem Sie die Route erstellen.

<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

- Klicken Sie **Routing**
- Auswählen **Policy Base Routing**
- Klicken Sie auf **Add**

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

In diesem Szenario wählen Sie alle Schnittstellen aus, die Sie als Quelle für das Routing des Datenverkehrs zu Secure Access oder für die Benutzerauthentifizierung zu Secure Access verwenden, indem Sie RA-VPN oder Client- oder browserbasierten ZTA-Zugriff auf die internen Netzwerkressourcen verwenden:

- Wählen Sie unter **Ingress Interface (Eingangsschnittstelle)** alle Schnittstellen aus, die Datenverkehr über Secure Access senden:

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

- Unter Match Criteria and Egress Interface definieren Sie die nächsten Parameter, nachdem Sie auf **Add** klicken:

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:** Für diese ACL konfigurieren Sie alle Elemente, die Sie an Secure Access weiterleiten:

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-Adresse auswählen
- **IPv4**

Addresses: Sie müssen die nächste IP unter der Maske 30 verwenden, die auf beiden VTI konfiguriert wurde. können Sie überprüfen, ob unter dem Schritt [VTI Interface Config](#)

Schnittstelle	IP	GW
PrimärVTI	169.254.2.1/30	169.254.2.2
Sekundäre VTI	169.254.3.1/30	169.254.3.2



Nachdem Sie es so konfiguriert haben, haben Sie das nächste Ergebnis, und Sie können fortfahren, um zu klicken **Save**:

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**

Default Interface

IPv4 settings IPv6 settings

Recursive: For example, 192.168.0.1

Default: For example, 192.168.0.1, 10.10.10.1

Peer Address

Verify Availability +

Cancel Save

Danach müssen Sie **Save** es erneut durchführen, und Sie haben es wie folgt konfiguriert:

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 → Send the traffic to the PrimaryVTI 169.254.3.2 If PrimaryVTI fail it will send the traffic to the SecondaryVTI

Cancel Save

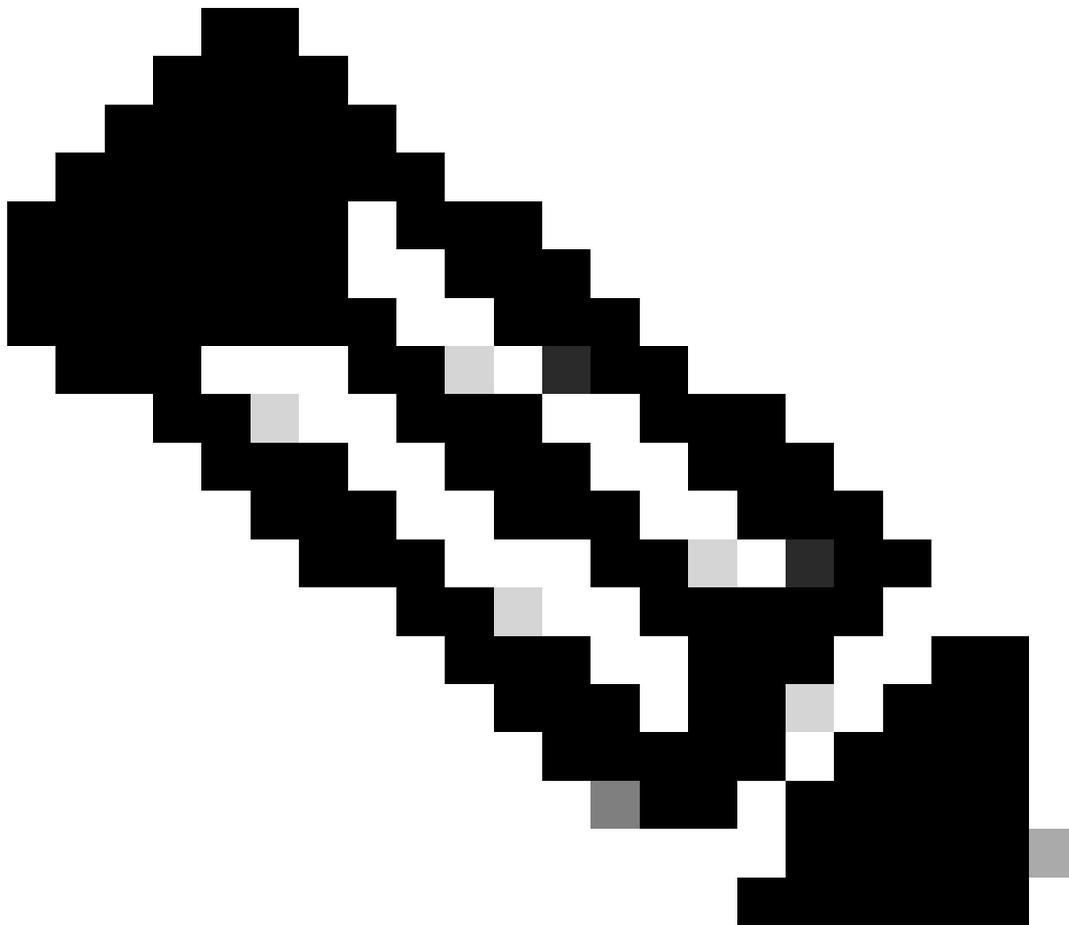
Anschließend können Sie die Bereitstellung durchführen und den Datenverkehr der auf der ACL konfigurierten Computer sehen, der den Datenverkehr an den sicheren Zugriff weiterleitet:

Aus dem **Conexion Events** im FÜZ:

<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

Über die **Activity Search** in Sicherer Zugriff:

Request	Source	Rule Identity ?	Destination	Destination IP	Internal IP	External IP	Action	Categories	Res
FW	⇌ HomeFTD	⇌ HomeFTD		8.8.8.8	192.168.10.40	<div style="width: 100%; height: 10px; background-color: #ccc;"></div>	✔ Allowed	Uncategorized	
FW	⇌ HomeFTD	⇌ HomeFTD		8.8.8.8	192.168.10.40	<div style="width: 100%; height: 10px; background-color: #ccc;"></div>	✔ Allowed	Uncategorized	
FW	⇌ HomeFTD	⇌ HomeFTD		8.8.8.8	192.168.10.40	<div style="width: 100%; height: 10px; background-color: #ccc;"></div>	✔ Allowed	Uncategorized	
FW	⇌ HomeFTD	⇌ HomeFTD		8.8.8.8	192.168.10.40	<div style="width: 100%; height: 10px; background-color: #ccc;"></div>	✔ Allowed	Uncategorized	
FW	⇌ HomeFTD	⇌ HomeFTD		8.8.8.8	192.168.10.40	<div style="width: 100%; height: 10px; background-color: #ccc;"></div>	✔ Allowed	Uncategorized	
FW	⇌ HomeFTD	⇌ HomeFTD		8.8.8.8	192.168.10.40	<div style="width: 100%; height: 10px; background-color: #ccc;"></div>	✔ Allowed	Uncategorized	
FW	⇌ HomeFTD	⇌ HomeFTD		8.8.8.8	192.168.10.40	<div style="width: 100%; height: 10px; background-color: #ccc;"></div>	✔ Allowed	Uncategorized	

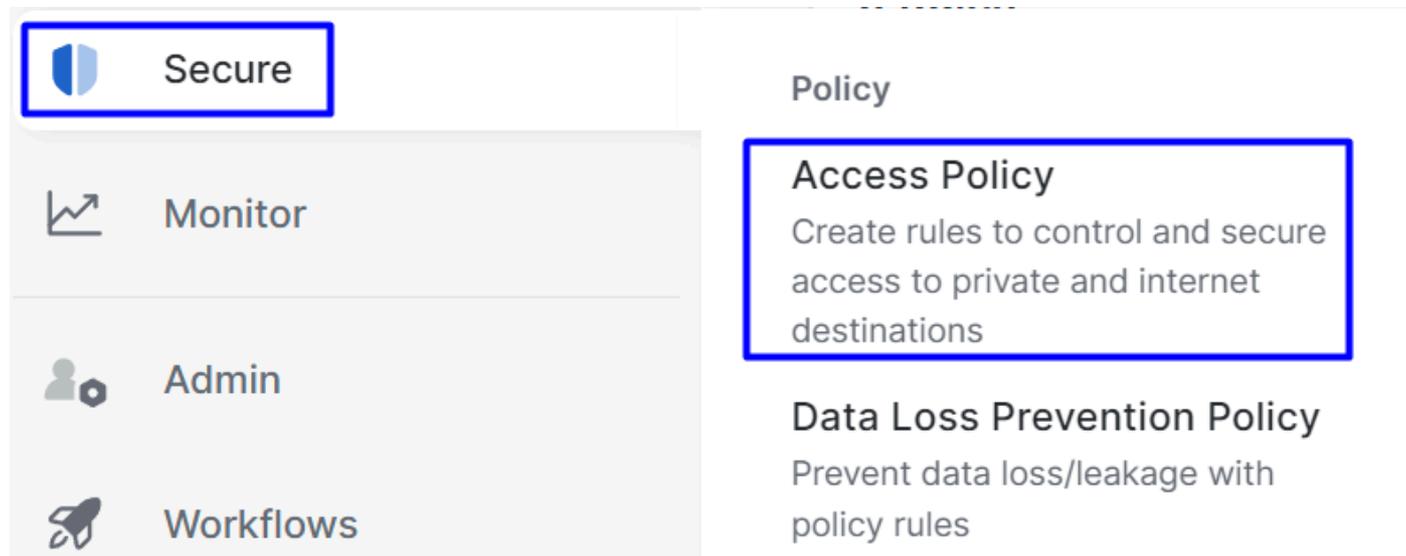


Anmerkung: Standardmäßig lässt die Richtlinie für sicheren Zugriff Datenverkehr zum Internet zu. Um den Zugriff auf private Anwendungen zu ermöglichen, müssen Sie private Ressourcen erstellen und sie der Zugriffsrichtlinie für den Zugriff auf private Ressourcen hinzufügen.

Konfigurieren der Internet-Zugriffsrichtlinie für sicheren Zugriff

Um den Zugriff für den Internetzugang zu konfigurieren, müssen Sie die Richtlinie auf Ihrem [Secure Access Dashboard](#) erstellen:

- Klicken Sie **Secure > Access Policy**



- Klicken Sie **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

Dort können Sie die Quelle als Tunnel angeben, und zum Ziel können Sie einen beliebigen Tunnel auswählen, je nachdem, was Sie in der Richtlinie konfigurieren möchten. Weitere Informationen finden Sie im [Secure Access-Benutzerhandbuch](#).

Konfigurieren des Zugriffs auf private Ressourcen für ZTNA und RA-VPN

Um den Zugriff für private Ressourcen zu konfigurieren, müssen Sie die Ressourcen zuerst im [Dashboard für sicheren Zugriff](#) erstellen:

Klicken Sie **Resources > Private Resources**

The screenshot shows the SAG 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.

- Klicken Sie anschließend auf **ADD**

Im Abschnitt "Konfiguration" finden Sie die nächsten zu konfigurierenden Abschnitte:
General, Communication with Secure Access Cloud and Endpoint Connection Methods.

Allgemein

General

Private Resource Name

Description (optional)

- Private Resource Name : Erstellen Sie einen Namen für die Ressource, auf die Sie über den sicheren Zugriff auf Ihr Netzwerk zugreifen

Endgeräteverbindungsmethoden

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 ⓘ
 ⓘ

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

Validate Application Certificate ⓘ

- **Zero Trust Connections:** Aktivieren Sie das Kontrollkästchen.
- **Client-based connection:** Wenn Sie es aktivieren, können Sie das Secure Client - Zero Trust Module verwenden, um den Zugriff über den Client-Basismodus zu ermöglichen.
- **Remote Reachable Address (FQDN, Wildcard FQDN, IP Address) :** Konfigurieren Sie die Ressourcen IP oder FQDN. Wenn Sie FQDN konfigurieren, müssen Sie den DNS hinzufügen, um den Namen aufzulösen.
- **Browser-based connection:** Wenn Sie diese Option aktivieren, können Sie über einen Browser auf Ihre Ressourcen zugreifen (fügen Sie nur Ressourcen mit HTTP- oder HTTPS-Kommunikation hinzu)
- **Public URL for this resource:** Konfigurieren Sie die öffentliche URL, die Sie über den Browser verwenden. Diese Ressource wird durch sicheren Zugriff geschützt.
- **Protocol:** Protokoll auswählen (HTTP oder HTTPS)

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

VPN Connection: Aktivieren Sie das Kontrollkästchen, um den Zugriff über RA-VPNaaS zu aktivieren.

Klicken Sie anschließend auf **save**, und Sie können diese Ressource der hinzufügen **Access Policy**.

Konfigurieren der Zugriffsrichtlinie

Wenn Sie die Ressource erstellen, müssen Sie sie einer der Richtlinien für den sicheren Zugriff zuweisen:

- Klicken Sie **Secure > Access Policy**

The screenshot shows the Azure portal interface. On the left, a navigation menu is visible with the following items: **Secure** (highlighted with a blue box), **Monitor**, **Admin**, and **Workflows**. On the right, under the heading **Policy**, there are two policy options: **Access Policy** (highlighted with a blue box) with the description "Create rules to control and secure access to private and internet destinations", and **Data Loss Prevention Policy** with the description "Prevent data loss/leakage with policy rules".

- Klicken Sie auf **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

Für diese Private Access-Regel konfigurieren Sie die Standardwerte, um den Zugriff auf die Ressource zu ermöglichen. Weitere Informationen zu Richtlinienkonfigurationen finden Sie im [Benutzerhandbuch](#).

1 Specify Access [Help](#)

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

Action

Allow
Allow specified traffic if security requirements are met.

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** : Wählen Sie Erlauben, um den Zugriff auf die Ressource zuzulassen.
- **From** : Geben Sie den Benutzer an, mit dem Sie sich bei der Ressource anmelden können.
- **To** : Wählen Sie die Ressource aus, auf die Sie über sicheren Zugriff zugreifen möchten.

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**

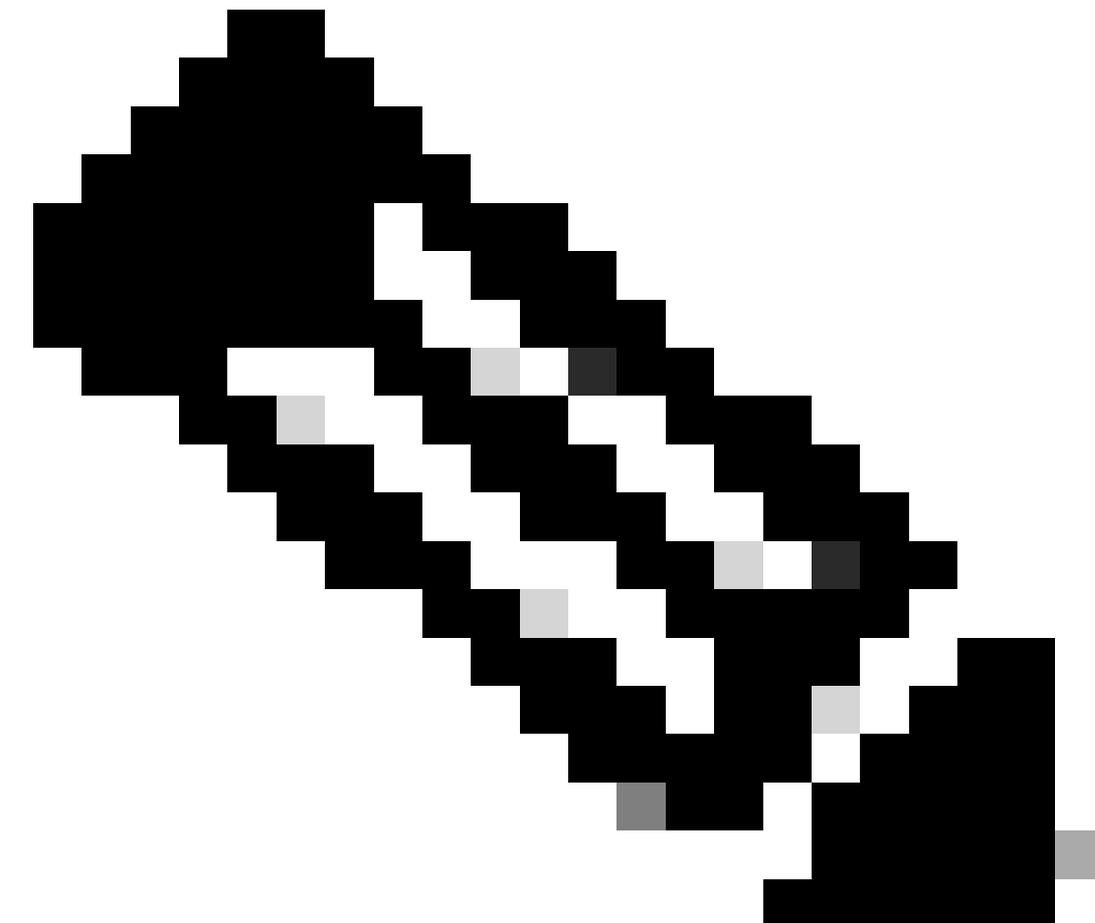
Zero Trust Browser-based Posture Profile **Rule Defaults**

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:** Standardprofil für Client-Basiszugriff auswählen
- **Zero-Trust Browser-based Posture Profile:** Standardprofil-Browser für Basiszugriff auswählen



Anmerkung: Weitere Informationen zur Statusrichtlinie finden Sie im [Benutzerhandbuch](#) für sicheren Zugriff.

Klicken Sie anschließend auf `Next` und `Save` und Ihre Konfiguration, und Sie können versuchen, über RA-VPN und Client Base ZTNA oder Browser Base ZTNA auf Ihre Ressourcen zuzugreifen.

Fehlerbehebung

Um eine Fehlerbehebung basierend auf der Kommunikation zwischen der sicheren Firewall und sicherem Zugriff durchzuführen, können Sie problemlos überprüfen, ob Phase 1 (IKEv2) und Phase 2 (IPSEC) zwischen den Geräten eingerichtet wurde.

Phase 1 überprüfen (IKEv2)

Um Phase 1 zu überprüfen, müssen Sie den nächsten Befehl in der CLI Ihres FTD ausführen:

```
show crypto isakmp sa
```

In diesem Fall ist die gewünschte Ausgabe zwei, die für die Rechenzentrum-IPs von Secure Access **IKEv2 SAs** eingerichtet sind, und der gewünschte Status lautet **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
```

Phase 2 (IPSEC) überprüfen

Um Phase 2 zu überprüfen, müssen Sie den nächsten Befehl in der CLI Ihres FTD ausführen:

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 der letzten Ausgabe können Sie sehen, dass beide Tunnel eingerichtet sind. was nicht erwünscht ist, ist die nächste Ausgabe unter dem Paketencapsunddecaps.

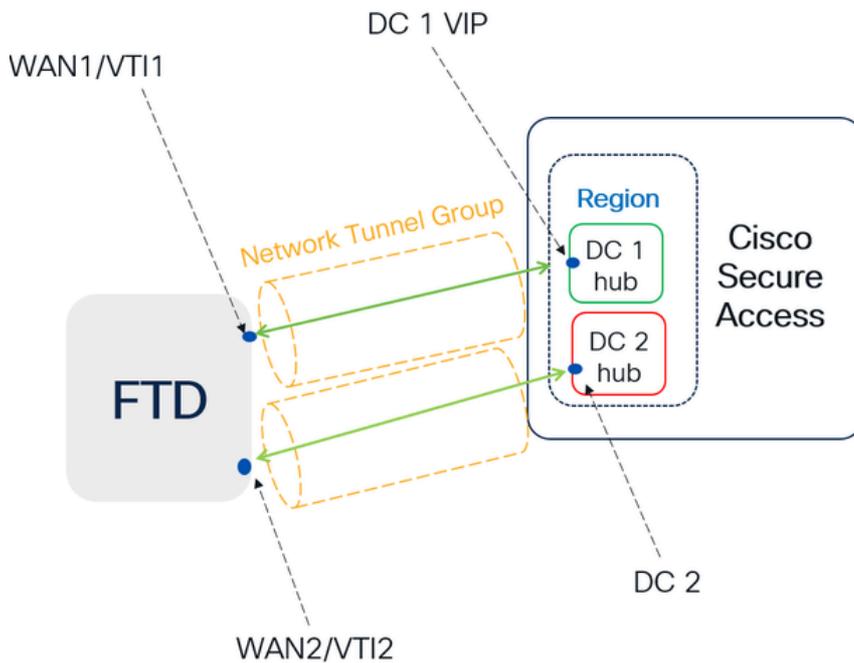
```
#pkts encaps: 71965, #pkts encrypt: 71965, #pkts digest: 71965 → Packets forwarded to Secure Access
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0 → No packets forwarded from Secure
#pkts compressed: 0, #pkts decompressed: 0 → Access to your firewall
#pkts not compressed: 71965, #pkts comp failed: 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
```

In diesem Szenario erstellen Sie ein Ticket beim TAC.

Hochverfügbarkeitsfunktion

Die Funktion der Tunnel mit sicherem Zugriff, die mit dem Rechenzentrum in der Cloud kommunizieren, ist aktiv/passiv, d. h. nur das Rechenzentrum 1 kann Datenverkehr empfangen. die Tür des DC 2 ist geschlossen, bis Tunnel Nummer 1 ausfällt.

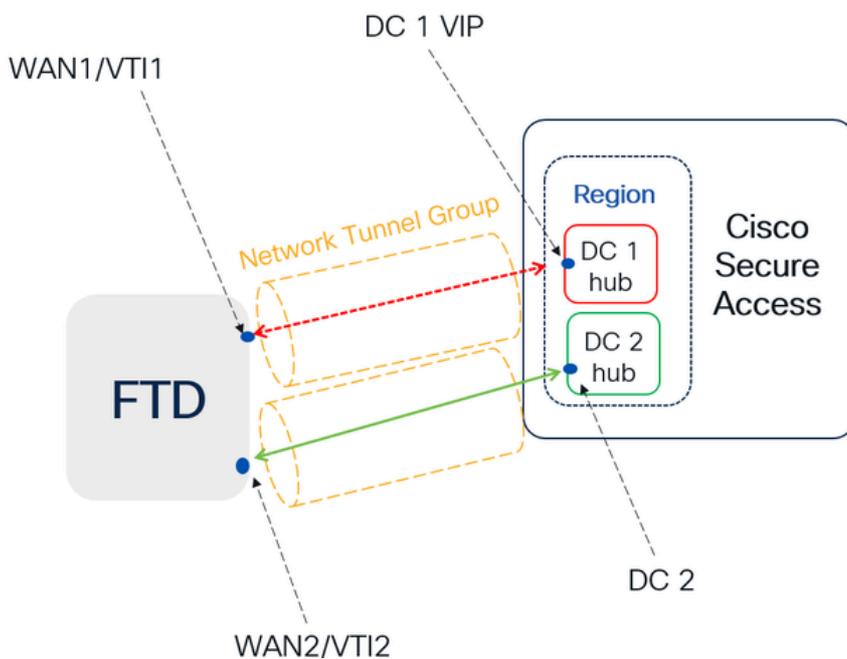
Normal Behavior



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

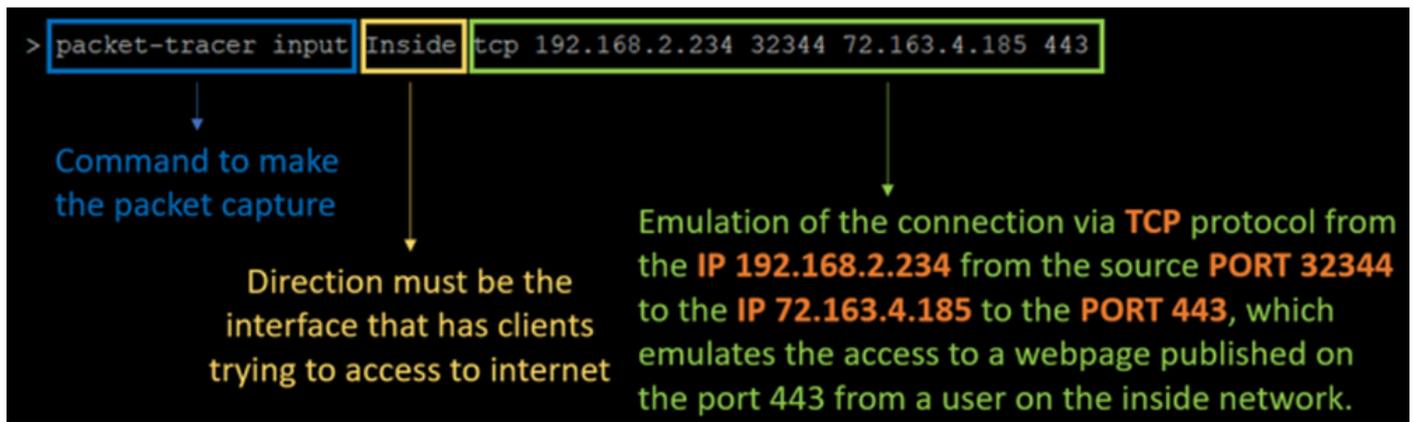
- DC2 is **Active** when DC1 or WAN1 peer is **Down**
- High availability is implemented to address failures in the WAN1 channel on the Firewall, ensuring operational continuity in the **region** and mitigating potential issues in DC1

Überprüfen der Datenverkehrsweiterleitung für den sicheren Zugriff

In diesem Beispiel verwenden wir die Quelle als Rechner im Firewall-Netzwerk:

- Quelle: 192.168.10.40
- Ziel: 146.112.255.40 (Sicherer Zugriff, Überwachungs-IP)

Beispiel:



Command:

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

Output:

```
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 können uns viele Dinge einen Kontext zur Kommunikation liefern und wissen, ob alles richtig unter der PBR-Konfiguration ist, um den Datenverkehr richtig zu Secure Access zu routen:

```
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 2 gibt an, dass der Datenverkehr an die `PrimaryVTI` Schnittstelle weitergeleitet wird. Dies ist richtig, da der Internetdatenverkehr basierend auf den Konfigurationen in diesem Szenario über den VTI an Secure Access weitergeleitet werden muss.

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:

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.