

# Configurazione di Secure Access con Secure Firewall ad alta disponibilità

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Esempio di rete](#)

[Configurazione](#)

[Configurare la VPN su accesso sicuro](#)

[Dati per configurazione tunnel](#)

[Configurare il tunnel su Secure Firewall](#)

[Configurazione dell'interfaccia del tunnel](#)

[Configura route statica per l'interfaccia secondaria](#)

[Configurare la VPN per l'accesso sicuro in modalità VTI](#)

[Configurazione degli endpoint](#)

[Configurazione IKE](#)

[Configurazione IPSEC](#)

[Configurazione avanzata](#)

[Scenari di configurazione dei criteri di accesso](#)

[Scenario di accesso Internet](#)

[RA-VPN Escenario](#)

[CLAP-BAP ZTNA Escenario](#)

[Configura Policy Base Routing](#)

[Configura i criteri di accesso a Internet per l'accesso protetto](#)

[Configurazione dell'accesso alle risorse private per ZTNA e RA-VPN](#)

[Risoluzione dei problemi](#)

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

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

[Funzione High Availability](#)

[Verifica del routing del traffico per l'accesso sicuro](#)

[Informazioni correlate](#)

---

## Introduzione

In questo documento viene descritto come configurare Secure Access con Secure Firewall con alta disponibilità.

## Prerequisiti

- [Configura assegnazione ruoli utente](#)
- [Configurazione autenticazione SSO ZTNA](#)
- [Configura accesso sicuro VPN di accesso remoto](#)

## Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Firepower Management Center 7.2
- Firepower Threat Defense 7.2
- Accesso sicuro
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA
- ZTNA senza client

## Componenti usati

Le informazioni fornite in questo documento si basano su:

- Firepower Management Center 7.2
- Firepower Threat Defense 7.2
- Accesso sicuro
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Premesse

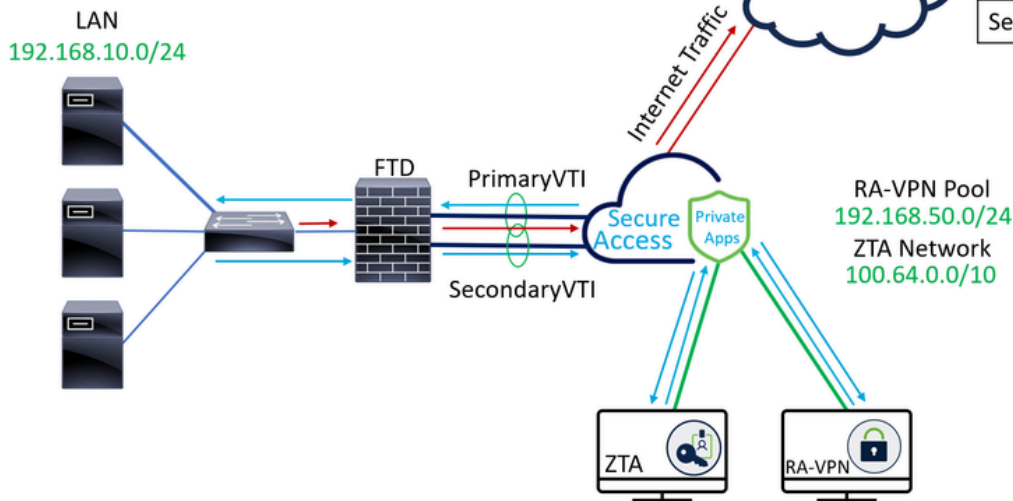


Cisco ha progettato Secure Access per proteggere e fornire accesso alle applicazioni private, sia in sede che basate su cloud. Inoltre, garantisce il collegamento dalla rete a Internet. Questo risultato è ottenuto attraverso l'implementazione di più metodi e livelli di sicurezza, il tutto finalizzato a preservare le informazioni mentre vi accedono tramite il cloud.

Esempio di rete

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

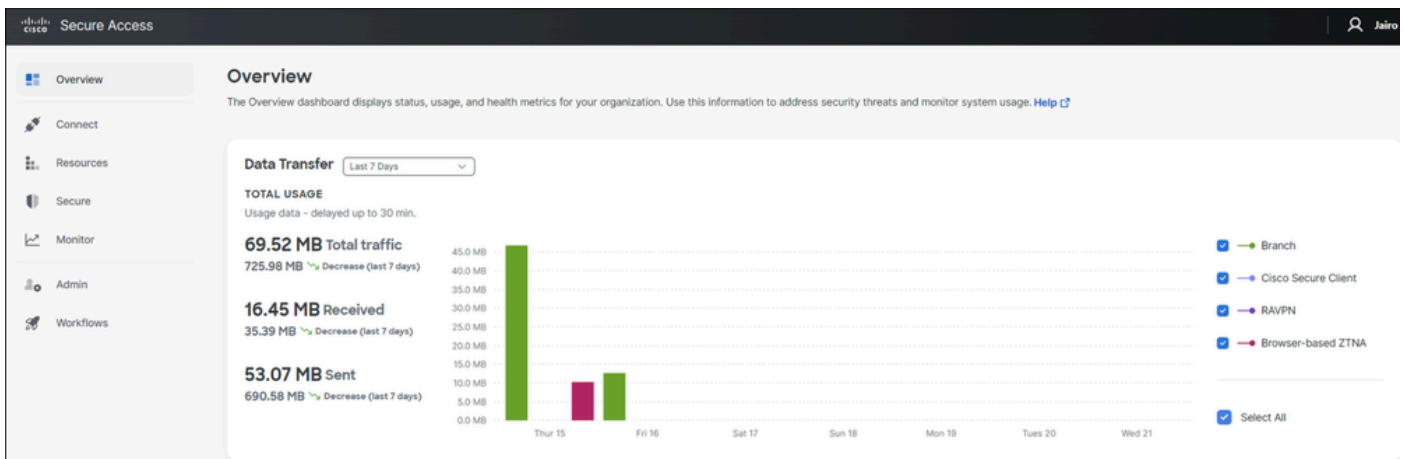
INTERFACE	IP
PrimaryWAN	192.168.30.5
PrimaryVTI	169.254.2.1
SecondaryWAN	192.168.0.202
SecondaryVTI	169.254.3.1



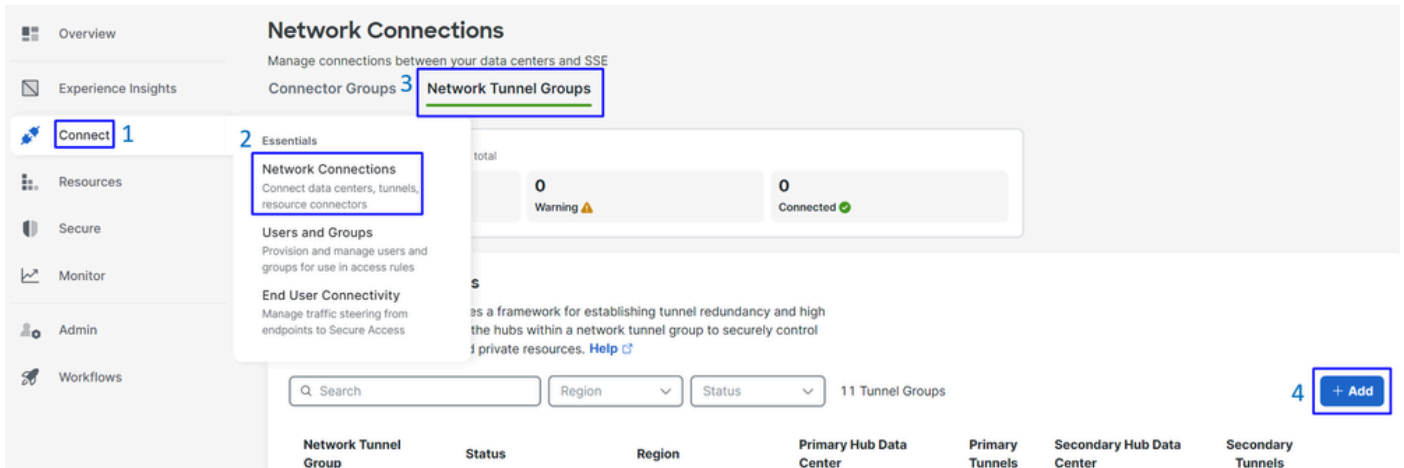
## Configurazione

### Configurare la VPN su accesso sicuro

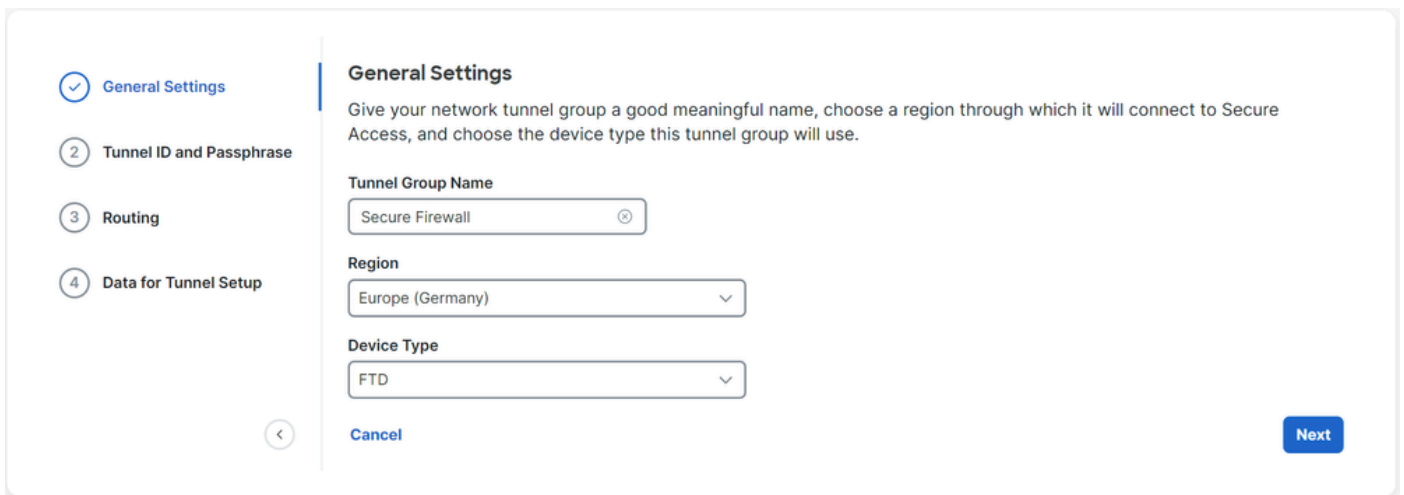
Passare al pannello di amministrazione di [Accesso sicuro](#).



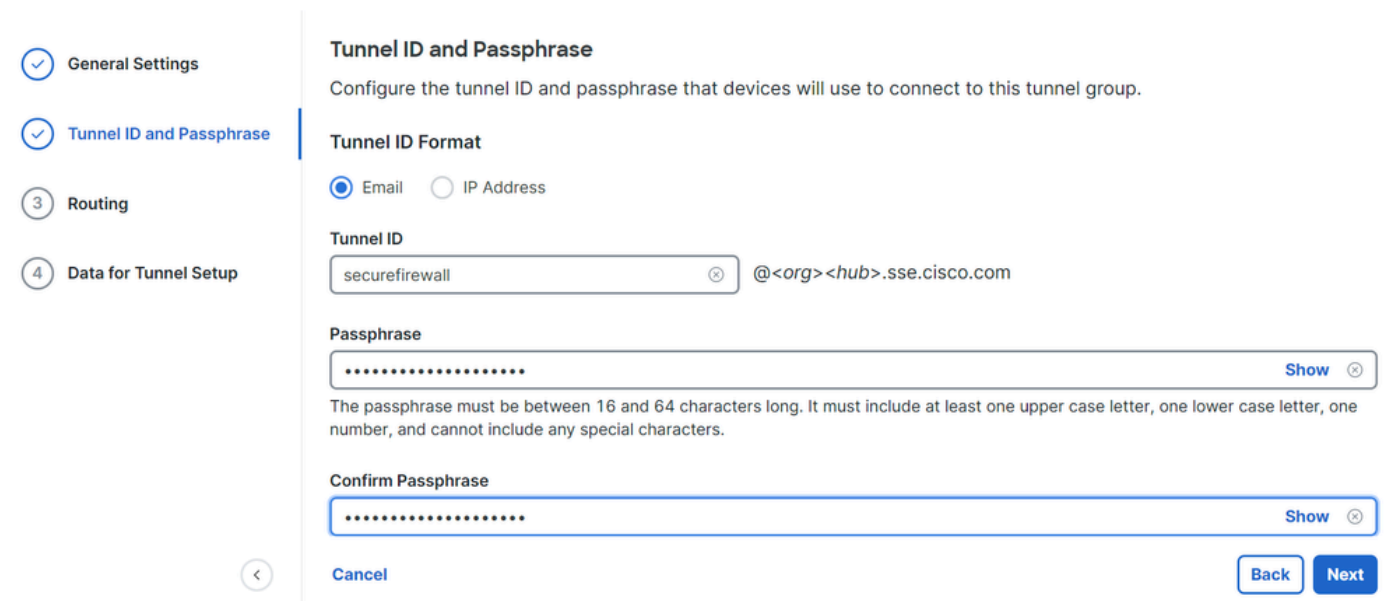
- Fare clic su **Connect > Network Connections**
- In **Network Tunnel Groups** clic su **+ Add**



- Configurazione Tunnel Group Name, Region e Device Type
- Fare clic su Next



- Configurare Tunnel ID Format e Passphrase
- Fare clic su Next



- Configurare gli intervalli di indirizzi IP o gli host configurati nella rete e che si desidera

passare il traffico attraverso l'accesso sicuro

- Fare clic su **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**

Dopo aver fatto clic sulle informazioni relative al **save tunnel** che vengono visualizzate, salvarle per il passaggio successivo, **Configure the tunnel on Secure Firewall**.

### Dati per configurazione tunnel

**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**

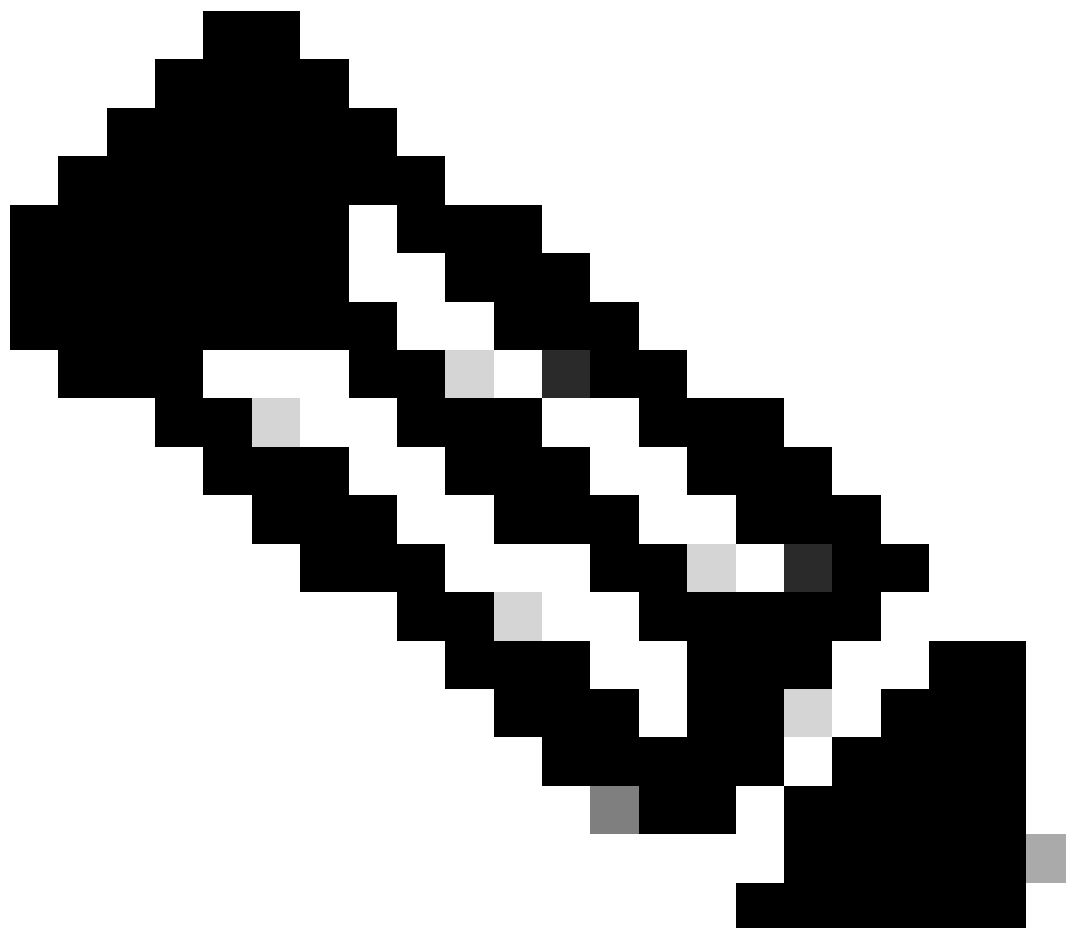
**Done**

## Configurare il tunnel su Secure Firewall

### Configurazione dell'interfaccia del tunnel

Per questo scenario, è necessario utilizzare la configurazione VTI (Virtual Tunnel Interface) su Secure Firewall; in questo caso, si dispone di un doppio ISP e si desidera avere HA se uno dei propri ISP ha esito negativo.

INTERFACCE	RUOLO
PrimaryWAN	Principal Internet WAN
Secondary WAN	WAN Internet secondaria
PrimaryVTI	Collegato per inviare il traffico attraverso il <b>Principal Internet WAN</b> router ad accesso protetto
VTI secondario	Collegato per inviare il traffico attraverso il <b>Secondary Internet WAN</b> router ad accesso protetto



Nota: 1. Per avere entrambi i tunnel, è necessario aggiungere o assegnare un percorso statico alla **Primary or Secondary Datacenter IP** rete.

---

Nota: 2. Se l'ECMP è stato configurato tra le interfacce, non è necessario creare un percorso statico all'Primary or Secondary Datacenter IP interfaccia per poter avere entrambi i tunnel attivi.

---

In base allo scenario, abbiamo PrimaryWAN e SecondaryWAN, che dobbiamo utilizzare per creare le interfacce VTI.

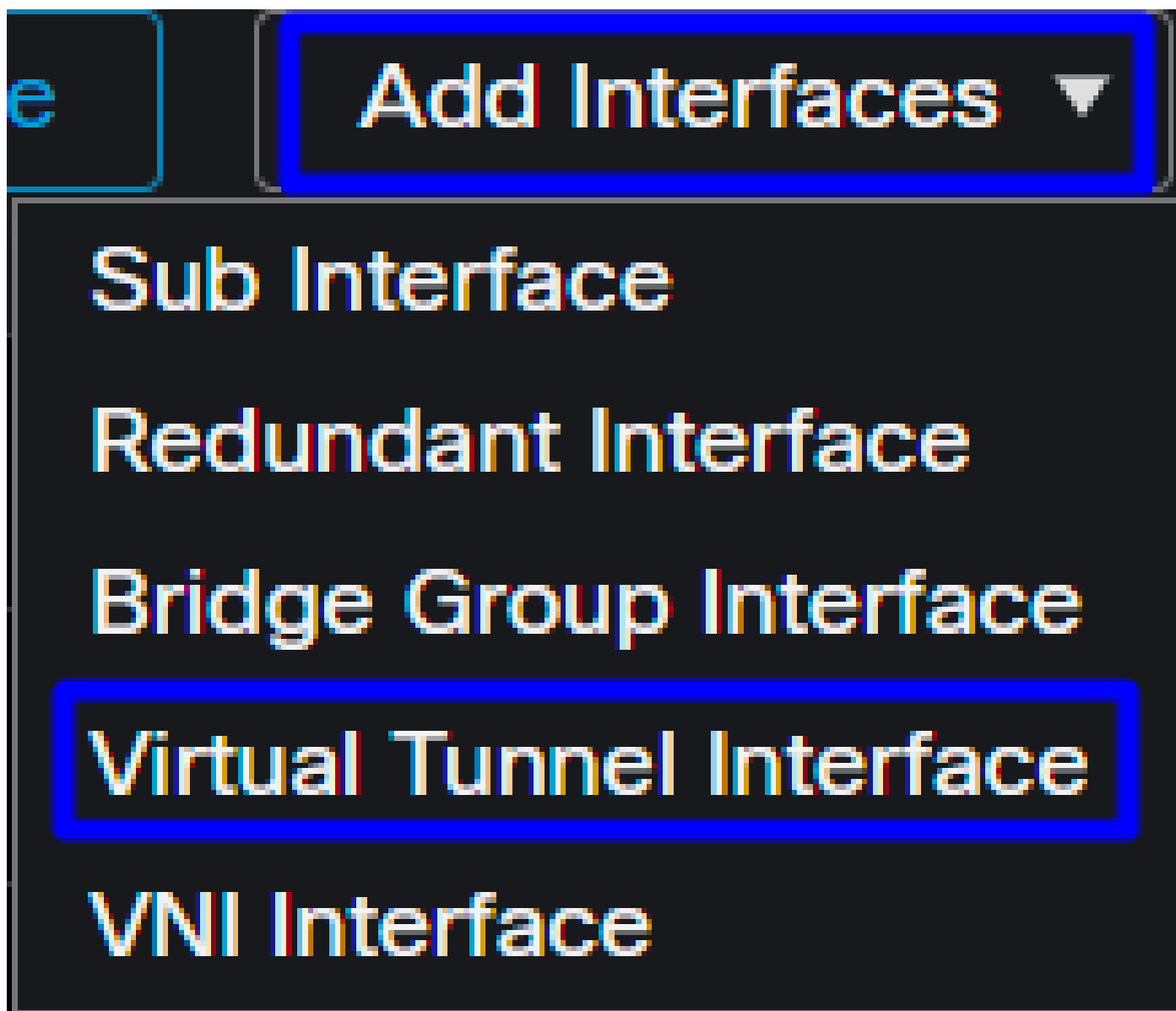
Passare alla Firepower Management Center > Devices pagina.

- Scegli il tuo FTD
- Scegli Interfaces

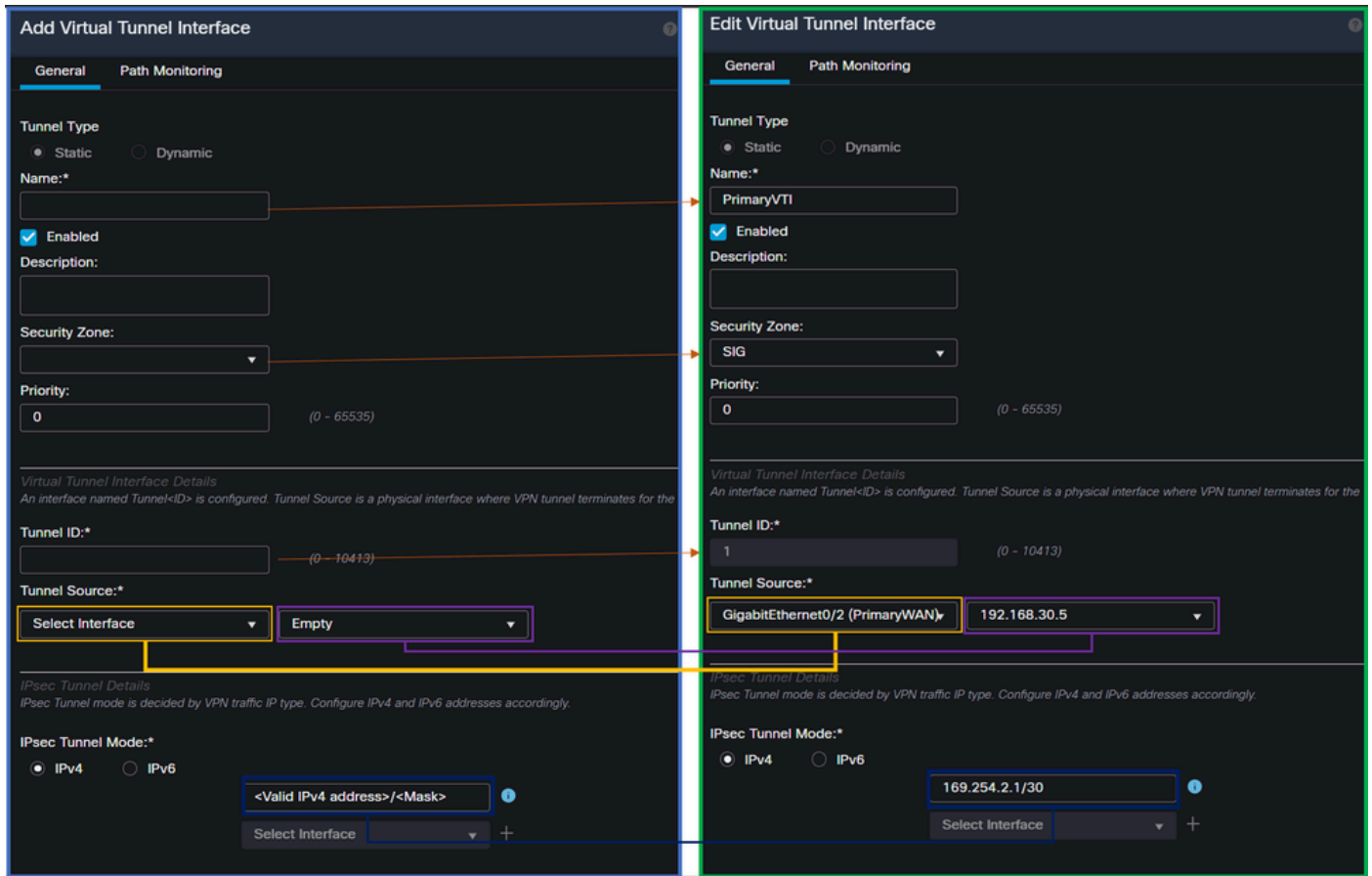
Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
Diagnostic0/0	diagnostic	Physical			
GigabitEthernet0/0	SecondaryWAN	Physical	SecondaryWAN		192.168.0.202/24(Static)
GigabitEthernet0/1	LAN	Physical	LAN		192.168.10.1/24(Static)
GigabitEthernet0/2	PrimaryWAN	Physical	PrimaryWAN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



- Fare clic su **Add Interfaces > Virtual Tunnel Interface**



- Configurare l'interfaccia in base alle informazioni seguenti



- **Name** : Configurare un nome che faccia riferimento al **PrimaryWAN** interface
- **Security Zone** : È possibile riutilizzarne un altro security Zonema è preferibile crearne uno nuovo per il traffico di accesso sicuro
- **Tunnel ID** : Aggiungere un numero per l'ID tunnel
- **Tunnel Source** : Scegliere l'indirizzo IP pubblico o privato **PrimaryWAN** interface dell'interfaccia
- **IPsec Tunnel Mode** : Selezionare **IPv4** e configurare un indirizzo IP non instradabile nella rete con la maschera 30



Nota: Per l'interfaccia VTI, è necessario usare un indirizzo IP non instradabile; ad esempio, se si hanno due interfacce VTI, è possibile usare 169.254.2.1/30 per PrimaryVTI e 169.254.3.1/30 per SecondaryVTI.

In seguito, è necessario eseguire la stessa operazione per il SecondaryWAN interfaceVTI e tutte le impostazioni sono configurate per l'alta disponibilità VTI, con il risultato seguente:

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)

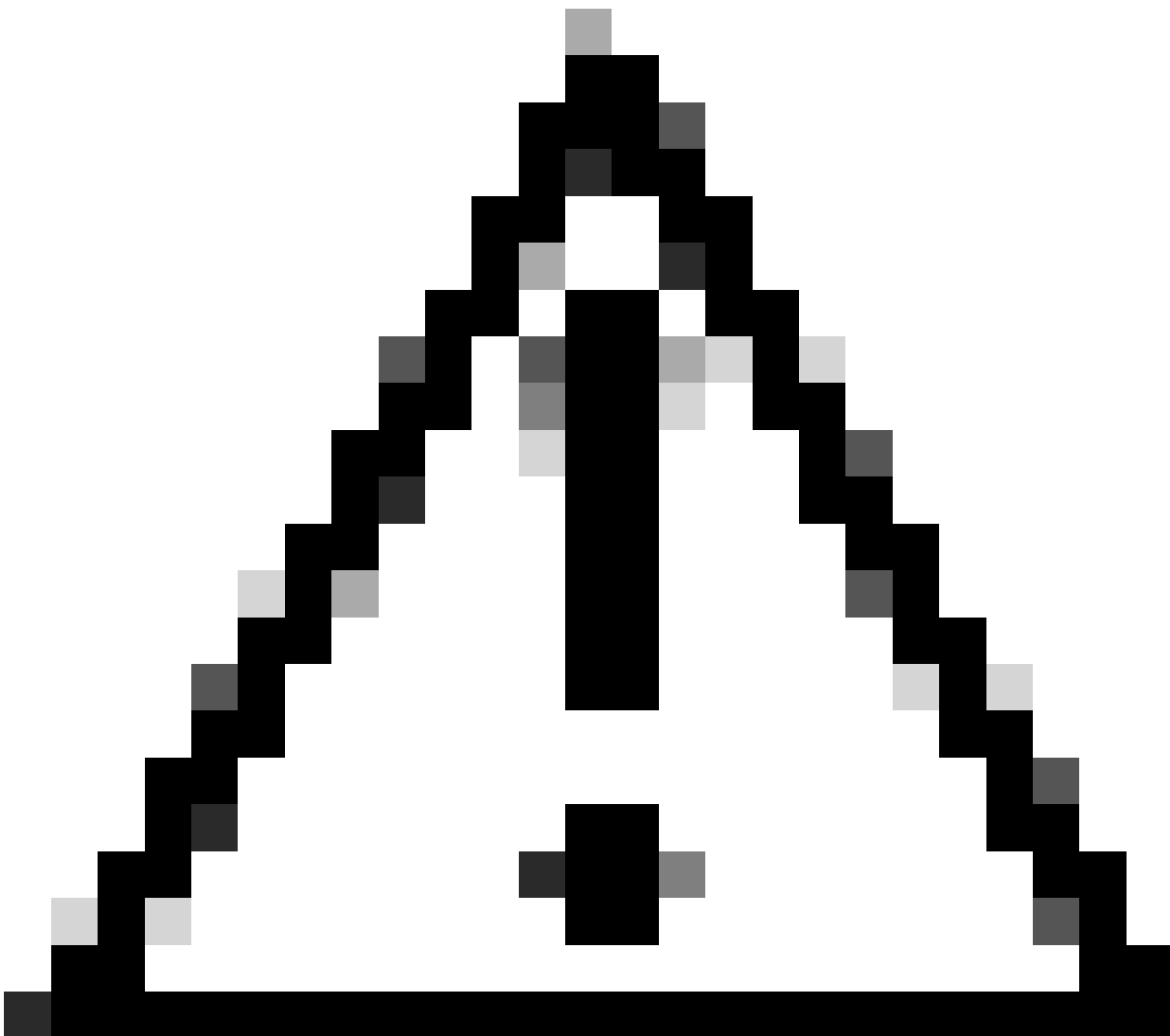
Per questo scenario, vengono utilizzati i seguenti IP:

Configurazione IP VTI		
Nome logico	IP	Intervallo
PrimaryVTI	169.254.2.1/30	169.254.2.1-169.254.2.2
VTI secondario	169.254.3.1/30	169.254.3.1-169.254.3.2

## Configura route statica per l'interfaccia secondaria

Per consentire al traffico del **SecondaryWAN interface router** di raggiungere l'**Secondary Datacenter IP Address host**, è necessario configurare una route statica all'indirizzo IP del centro dati. È possibile configurarla con una metrica di uno (1) per collocarla sopra la tabella di routing; inoltre, specificare l'indirizzo IP come host.

---



---

Attenzione: Questa operazione è necessaria solo se non si dispone di una configurazione ECMP tra i canali WAN; se è stato configurato ECMP, è possibile passare alla fase successiva.

---

Passa a **Device > Device Management**

- Fare clic sul dispositivo **FTD**
- Fare clic su **Routing**
- Scegli **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: Scelta dell'interfaccia WAN secondaria
- Gateway: Scelta del gateway WAN secondario
- Selected Network: Aggiungere l'indirizzo IP del centro dati secondario come host; le informazioni sono reperibili nella procedura di configurazione del tunnel su accesso sicuro, [Dati per configurazione tunnel](#)

- **Metric:** Usa uno (1)
- **OK** Fare clic su **and save** per salvare le informazioni, quindi su **deploy** (distribuisci).

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						

## Configurare la VPN per l'accesso sicuro in modalità VTI

Per configurare la VPN, passare al firewall:

- Fare clic su **Devices > Site to Site**
- Fare clic su **+ Site to Site VPN**

### Configurazione degli endpoint

Per configurare il passaggio Endpoint, è necessario utilizzare le informazioni fornite nel passaggio [Dati per configurazione tunnel](#).

### Create New VPN Topology

Topology Name:\*

Policy Based (Crypto Map)  Route Based (VTI)

Network Topology:

IKE Version:\*  IKEv1  IKEv2

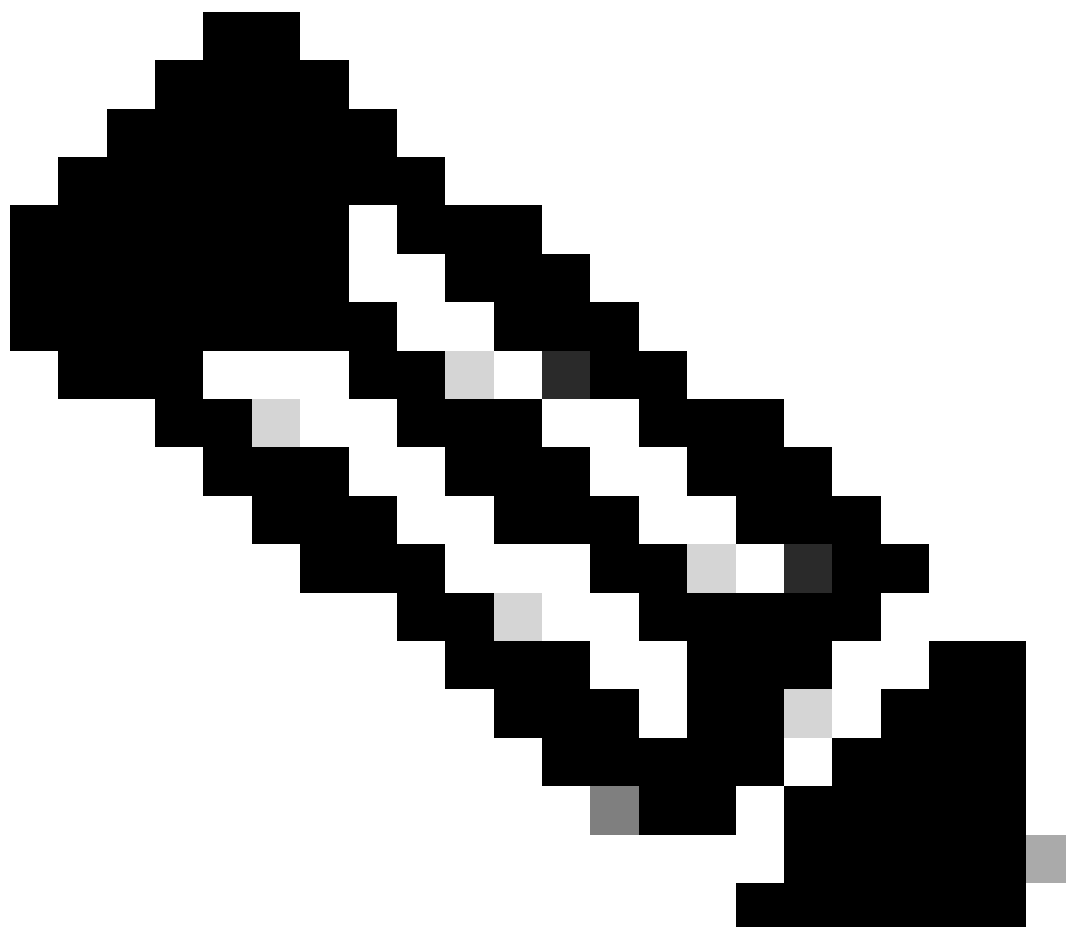
**Endpoints** | IKE | IPsec | Advanced

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) <a href="#">Edit VTI</a> <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](#)

- Nome topologia: Crea un nome correlato all'integrazione di Accesso sicuro
- Scegli **Routed Based (VTI)**

- Scegli **Point to Point**
  - IKE Version: Scegli **IKEv2**
- 



Nota: IKEv1 non è supportato per l'integrazione con Secure Access.

---

In è **Node A** necessario configurare i parametri successivi:



## 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:** Scegli il dispositivo FTD
- **Virtual Tunnel Interface:** Scegliere la VTI correlata alla PrimaryWAN Interface VLAN.
- Selezionare la casella di controllo **Send Local Identity to Peers**
- **Local Identity Configuration:** Scegliere l'ID e-mail e immettere le informazioni in base a quanto **Primary Tunnel ID** fornito nella configurazione nella fase [Data for Tunnel Setup](#)

Dopo aver configurato le informazioni sul PrimaryVTI clic SU + 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:** Scegliere la VTI correlata alla PrimaryWAN InterfaceVLAN.
- Selezionare la casella di controllo **Send Local Identity to Peers**
- **Local Identity Configuration:** Scegliere l'ID e-mail e immettere le informazioni in base a quanto **Secondary Tunnel ID** fornito nella configurazione nella fase [Data for Tunnel Setup](#)

In è **Node B** necessario configurare i parametri successivi:

# Node B

Device:\*

Extranet

Device Name\*:

SecureAccess

Endpoint IP Address\*:

18.156.145.74, 3.120.45.23

- **Device:** Extranet
- **Device Name:** Scegliere un Nome per riconoscere Accesso protetto come destinazione.
- **Endpoint IP Address:** La configurazione per primario e secondario deve essere Primario **Datacenter IP**,**Secondary Datacenter IP**. Queste informazioni sono disponibili nel passo [Dati per configurazione tunnel](#)

Al termine, la configurazione di **Endpoints** è stata completata ed è ora possibile passare alla fase Configurazione IKE.

Configurazione IKE

Per configurare i parametri IKE, fare clic su **IKE**.

Endpoints

IKE

IPsec

Advanced

In è IKE, necessario configurare i parametri successivi:

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: È possibile utilizzare la configurazione Umbrella predefinita Umbrella-AES-GCM-256 oppure configurare parametri diversi in base alla [Supported IKEv2 and IPSEC Parameters](#)
- Authentication Type: Chiave manuale già condivisa
- Key e Confirm Key Le informazioni sono disponibili nel Passphrase passo [Dati per configurazione tunnel](#)

Al termine, la configurazione di IKE è stata completata ed è ora possibile passare alla fase Configurazione IPSEC.

Configurazione IPSEC

Per configurare i parametri IPSEC, fare clic su IPSEC.

Endpoints

IKE



IPsec

Advanced

In è IPSEC, necessario configurare i parametri successivi:

Crypto Map Type:  Static  Dynamic

IKEv2 Mode: Tunnel

Transform Sets: IKEv1 IPsec Proposals  IKEv2 IPsec Proposals\* 

tunnel_aes256_sha	<b>Umbrella-AES-GCM-256</b>
-------------------	-----------------------------

Enable Security Association (SA) Strength Enforcement

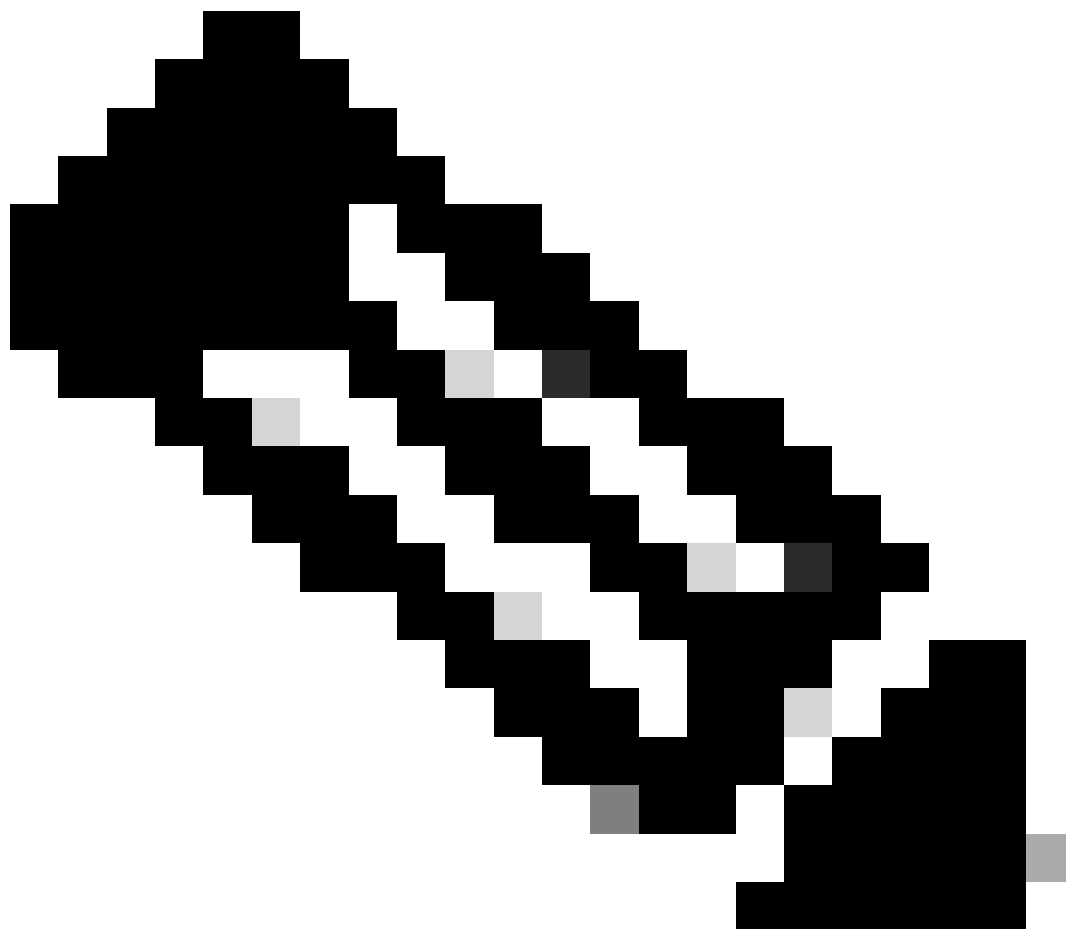
Enable Perfect Forward Secrecy

Modulus Group: 14

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

Lifetime Size: 4608000 Kbytes (Range 10-2147483647)

- Policies: È possibile utilizzare la configurazione Umbrella predefinita Umbrella-AES-GCM-256 oppure configurare parametri diversi in base alla [Supported IKEv2 and IPSEC Parameters](#)



Nota: Su IPSEC non è richiesto altro.

---

Al termine, la configurazione di IPSEC è stata completata ed è ora possibile passare alla fase Configurazione avanzata.

Configurazione avanzata

Per configurare i parametri avanzati, fare clic su Avanzate.

Endpoints

IKE

IPsec

Advanced

In è **Advanced**, necessario configurare i parametri successivi:

**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

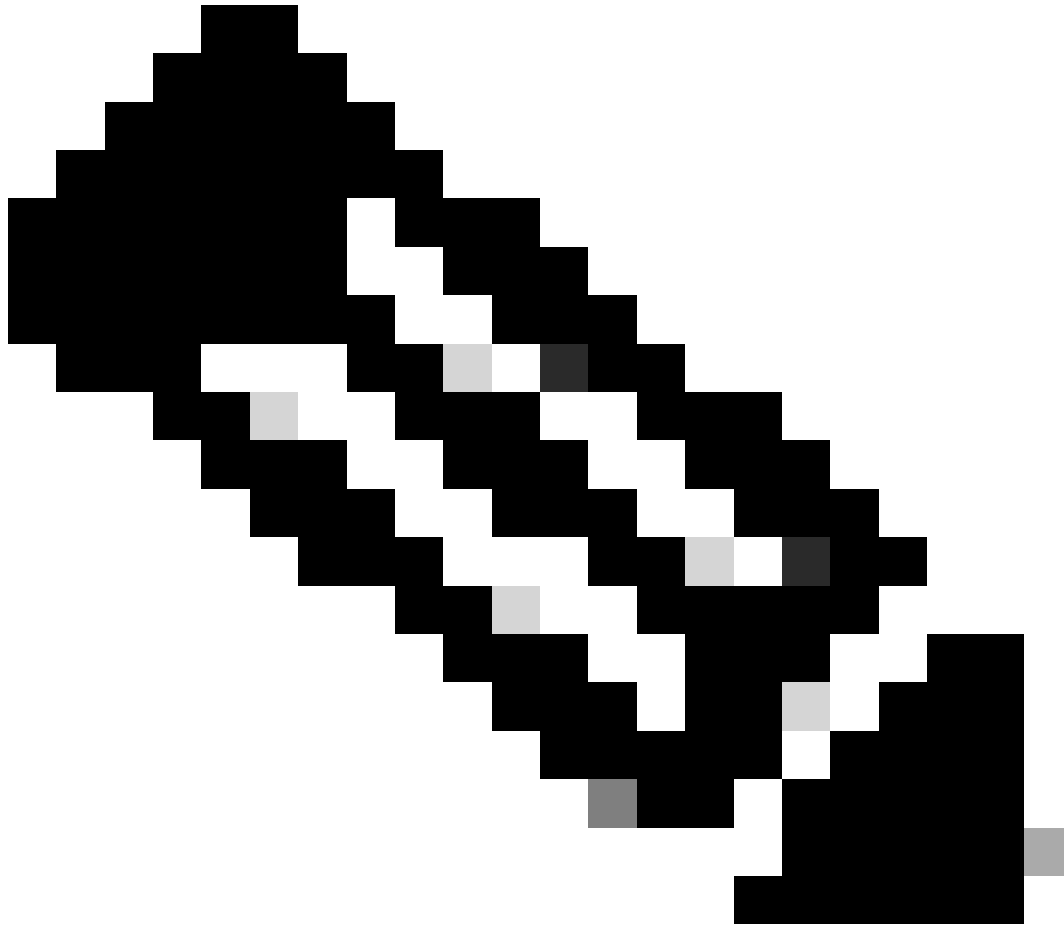
Enable Notification on Tunnel Disconnect

**IKEv2 Security Association (SA) Settings**

Cookie Challenge: custom

- IKE Keepalive: Abilita
- Threshold: 10
- Retry Interval: 2
- Identity Sent to Peers: AutoOrDN
- Peer Identity Validation: Non controllare

Dopodiché, è possibile fare clic su **Save** e su **Deploy**.



Nota: Dopo alcuni minuti, verrà visualizzata la VPN stabilita per entrambi i nodi.

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)

Al termine, la configurazione del VPN to Secure Access in VTI Mode file è stata completata ed è possibile procedere alla procedura Configure Policy Base Routing.

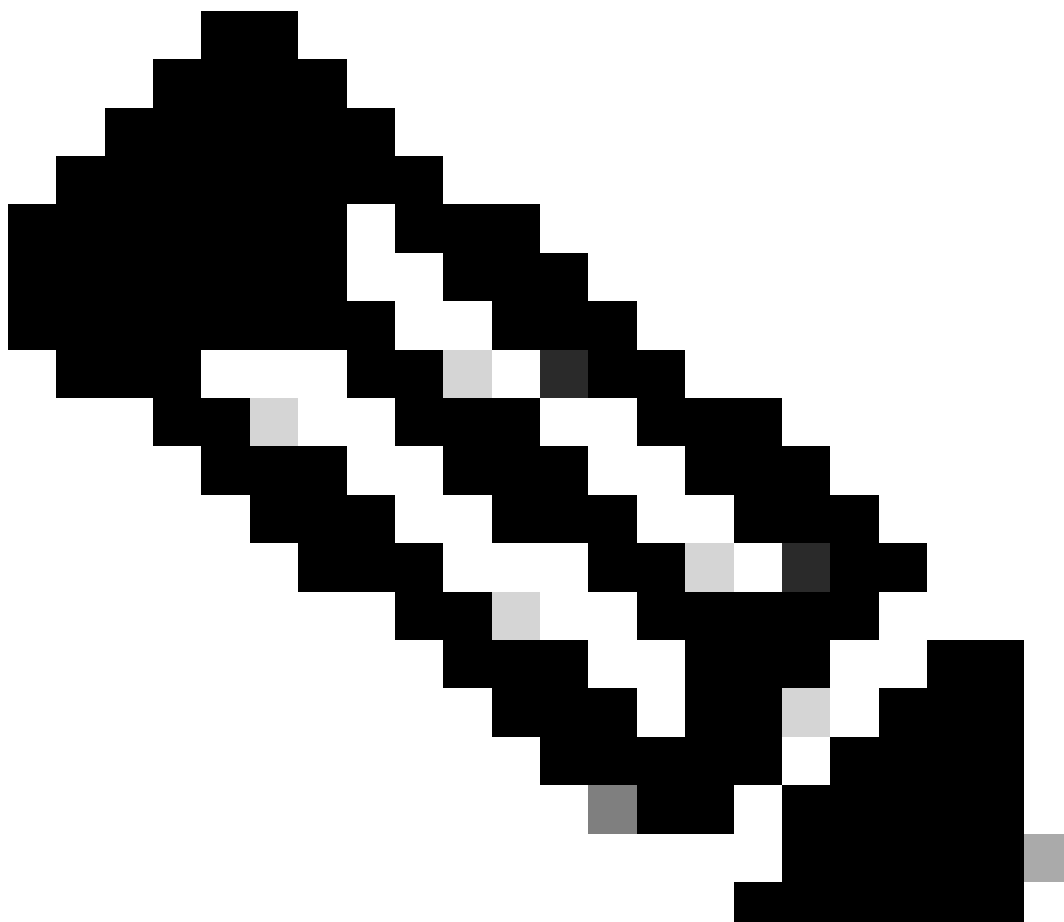




Avviso: il traffico diretto all'accesso sicuro viene inoltrato solo al tunnel primario quando sono stabiliti entrambi i tunnel; se il server primario non è attivo, Secure Access consente l'inoltro del traffico attraverso il tunnel secondario.

---

---



Nota: il failover sul sito Secure Access è basato sui valori DPD documentati nella [guida per l'utente](#) per i valori IPsec supportati.

---

## Scenari di configurazione dei criteri di accesso

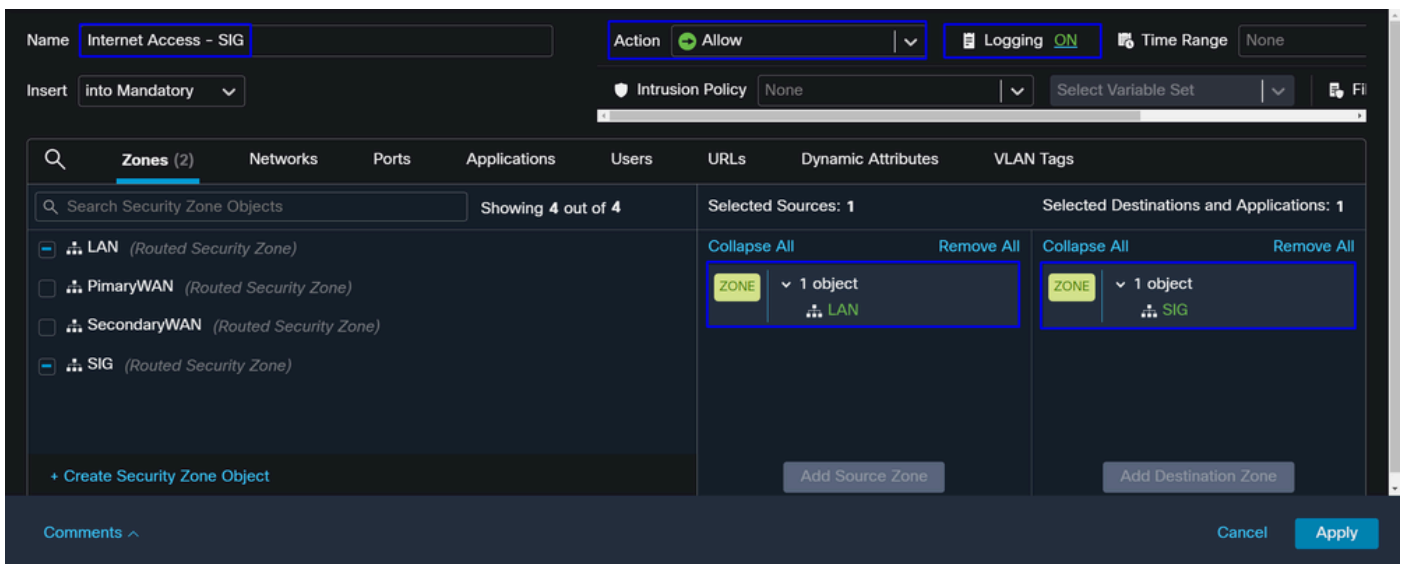
Le regole dei criteri di accesso definite si basano su:

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)

Interfaccia	Zona
PrimaryVTI	SIG
VTI secondario	SIG
LAN	LAN

### Scenario di accesso Internet

Per consentire l'accesso a Internet a tutte le risorse configurate nel Policy Base Routing, è necessario configurare alcune regole di accesso e alcuni criteri in accesso sicuro. In questo scenario verranno illustrate le modalità per ottenere questo risultato:



Questa regola fornisce l'accesso a LAN Internet e, in questo caso, Internet è SIGprotetto.

### RA-VPN Escenario

Per fornire l'accesso dagli utenti RA-VPN, è necessario configurarlo in base all'intervallo assegnato al pool RA-VPN.



Nota: Per configurare il criterio RA-VPNaaS, è possibile passare alla sezione [Gestione reti private virtuali](#)

---

Come è possibile verificare il pool IP della VPNaaS?

Passare al [Dashboard di accesso protetto](#)

- Fare clic su **Connect > End User Connectivity**
- Fare clic su **Virtual Private Network**
- In **Manage IP Pools**, fare clic su **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

- Vedi la tua piscina sotto **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

- È necessario autorizzare questo intervallo in SIG, ma è necessario aggiungerlo anche nell'ACL configurato nel PBR.

## Configurazione regola di accesso

Se si configura Accesso sicuro solo per utilizzarlo con le funzionalità di accesso alle risorse delle applicazioni private, la regola di accesso può avere il seguente aspetto:

The screenshot shows the configuration of an Access Rule named 'Private APP'. The rule is set to 'Allow' with logging enabled. The source is configured with two selected networks: '192.168.10.153' (Host Object) and '192.168.50.0/24' (Network Object). The destination is configured with one selected network: 'LAN' (Network Object). The rule is applied to the 'SIG' zone.

Name	Action	Logging	Time Range
Private APP	Allow	ON	None

Insert	Intrusion Policy	Select Variable Set
into Mandatory	None	

Networks	Geolocations	Selected Sources: 2	Selected Destinations and Applications: 1
<input type="checkbox"/> 192.168.0.150 (Host Object)	192.168.0.150	<input checked="" type="checkbox"/> ZONE 1 object SIG	<input checked="" type="checkbox"/> ZONE 1 object LAN
<input type="checkbox"/> 192.168.10.153 (Host Object)	192.168.10.153	<input checked="" type="checkbox"/> NET 1 object 192.168.50.0/24	
<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		

Questa regola consente il traffico dal pool RA-VPN 192.168.50.0/24 alla rete LAN; se necessario, è possibile specificare altre opzioni.

## Configurazione ACL

Per consentire il routing del traffico da SIG alla LAN, è necessario aggiungerlo all'ACL in modo che funzioni nel PBR.

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 Escenario

È necessario configurare la rete in base all'intervallo CGNAT 100.64.0.0/10 per consentire l'accesso alla rete da parte degli utenti ZTA di base client o ZTA di base browser.

### Configurazione regola di accesso

Se si configura Accesso sicuro solo per utilizzarlo con le funzionalità di accesso alle risorse delle applicazioni private, la regola di accesso può avere il seguente aspetto:

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

Showing 27 out of 27  
Selected Sources: 2  
Selected Destinations and Applications: 1

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"/> GWWT1 (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)

Questa regola consente il traffico dall'intervallo CGNAT ZTNA 100.64.0.0/10 alla LAN.

### Configurazione ACL

Per consentire il routing del traffico da SIG alla LAN tramite CGNAT, è necessario aggiungerlo nell'ACL in modo che funzioni nel PBR.

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	

## Configura Policy Base Routing

Per consentire l'accesso alle risorse interne e a Internet tramite l'accesso sicuro, è necessario creare route tramite Policy Base Routing (PBR) che facilitino il routing del traffico dall'origine alla destinazione.

- Passa a **Devices > Device Management**
- Scegliere il dispositivo FTD in cui creare il ciclo di lavorazione

<input type="checkbox"/>	Name	Model	Version
<input type="checkbox"/>	Ungrouped (1)		
<input type="checkbox"/>	<b>FTD_HOME</b> Snort 3 192.168.0.201 - Routed	FTDv for VMware	7.2.5

- Fare clic su **Routing**
- Scegli **Policy Base Routing**
- Fare clic su **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 questo scenario, è possibile selezionare tutte le interfacce utilizzate come origine per instradare il traffico verso l'accesso sicuro o per fornire l'autenticazione utente all'accesso sicuro mediante RA-VPN o l'accesso ZTA basato su client o browser alle risorse interne della rete:

- In **Interfaccia in ingresso** selezionare tutte le interfacce che inviano il traffico tramite l'accesso sicuro:

**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 x

- In **Criteri di corrispondenza e interfaccia in uscita (Match Criteria and Egress Interface)**, definire i parametri successivi dopo aver fatto clic su **Add**:

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

[Add](#)

**Add Forwarding Actions**

Match ACL:\*  +

Send To:\*

IPv4 Addresses:

IPv6 Addresses:

Don't Fragment:

Internal Sources

Match ACL:\*

Send To:\*

IPv4 Addresses:

IPv6 Addresses:

Don't Fragment:

- **Match ACL:** Per questo ACL, è possibile configurare tutti gli elementi indirizzati a Secure Access:

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:

Entries (2)

Sequence	Action	Source	Source Port	Destination	Destination Port
1	Block	Any	Any	208.67.222.222 208.67.220.220	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:** Scegli indirizzo IP
- **IPv4 Addresses:** È necessario usare l'IP successivo sotto la maschera 30 configurata su entrambe le VTI; è possibile controllare che al di sotto della fase, [VTI Interface Config](#)

Interfaccia	IP	GW
PrimaryVTI	169.254.2.1/30	169.254.2.2
VTI secondario	169.254.3.1/30	169.254.3.2

IPv4 Addresses:  →



Dopo aver configurato il file in questo modo, si otterrà il risultato successivo e sarà possibile fare clic su **Save**:

The screenshot shows a configuration window with the following fields and options:

- Match ACL:\***: A dropdown menu set to **ACL**.
- Send To:\***: A dropdown menu set to **IP Address**.
- IPv4 Addresses:**: A text input field containing **169.254.2.2,169.254.3.2**.
- IPv6 Addresses:**: A text input field with the placeholder text "For example, 2001:db8::, 2002:db8::1".
- Don't Fragment:**: A dropdown menu set to **None**.
- Default Interface**
- Two tabs: **IPv4 settings** (active) and **IPv6 settings**.
- Recursive:** A text input field with the placeholder text "For example, 192.168.0.1".
- Default:** A text input field with the placeholder text "For example, 192.168.0.1, 10.10.10.1".
- Peer Address**
- Verify Availability** with a plus icon (+).

At the bottom right, there are **Cancel** and **Save** buttons.

Dopo di che, è necessario **save** di nuovo e lo avete configurato nel modo seguente:

The screenshot shows a configuration window for a policy based route with the following details:

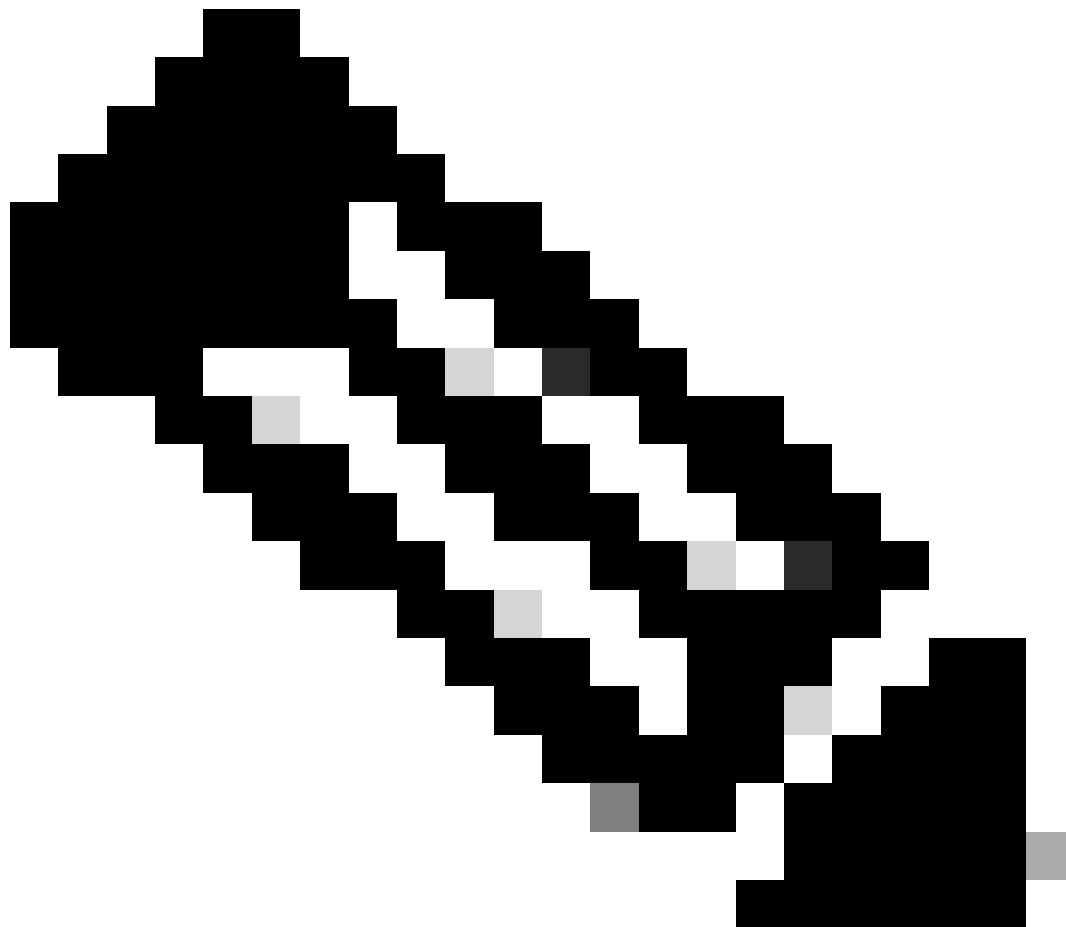
- Ingress Interface\***: A dropdown menu set to **LAN**.
- Match Criteria and Egress Interface**: A section with an **Add** button and the instruction "Specify forward action for chosen match criteria."
- Match ACL**: A table with the following content:

Match ACL	Forwarding Action
ACL	Send through 169.254.2.2 169.254.3.2 → Send the traffic to the PrimaryVTI
- Forwarding Action**: A text description: "If PrimaryVTI fail it will send the traffic to the SecondaryVTI".

At the bottom right, there are **Cancel** and **Save** buttons.

Quindi, è possibile eseguire la distribuzione e visualizzare il traffico dei computer configurati sull'ACL che instrada il traffico a Secure Access:





Nota: Per impostazione predefinita, i criteri di accesso protetto predefiniti consentono il traffico verso Internet. Per consentire l'accesso alle applicazioni private, è necessario creare risorse private e aggiungerle ai criteri di accesso per l'accesso alle risorse private.

---

Configura i criteri di accesso a Internet per l'accesso protetto

Per configurare l'accesso per l'accesso a Internet, è necessario creare il criterio nel [Dashboard di accesso sicuro](#):

- Fare clic su **Secure > Access Policy**



Secure



Monitor



Admin



Workflows

Policy

### Access Policy

Create rules to control and secure access to private and internet destinations

### Data Loss Prevention Policy

Prevent data loss/leakage with policy rules

- Fare clic su **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

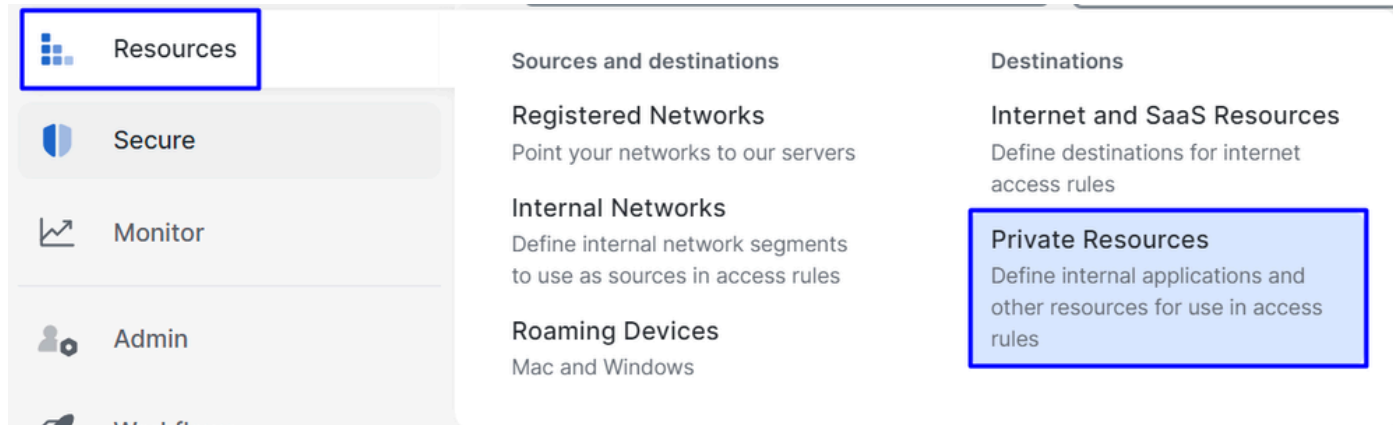
Control and secure access to public destinations from within your network and from managed devices

In questa finestra è possibile specificare l'origine come tunnel e la destinazione come destinazione è possibile scegliere qualsiasi, a seconda di ciò che si desidera configurare in base al criterio. Consultare la [Guida dell'utente di Secure Access](#).

## Configurazione dell'accesso alle risorse private per ZTNA e RA-VPN

Per configurare l'accesso per le risorse private, è necessario innanzitutto creare le risorse nel [Dashboard accesso sicuro](#):

Fare clic su **Resources > Private Resources**



- Quindi fare clic su **ADD**

Nella configurazione sono disponibili le sezioni successive da configurare: **General**, **Communication with Secure Access Cloud and Endpoint Connection Methods**.

### Informazioni generali

## General

**Private Resource Name**

**Description (optional)**

- Private Resource Name : Creare un nome per la risorsa alla quale si fornisce l'accesso tramite l'accesso sicuro alla rete

### Metodi di connessione degli endpoint

**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://  -8195126.ztna.sse.cisco.io

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

**Validate Application Certificate** ⓘ

- **Zero Trust Connections:** Contrassegnare la casella di controllo.
- **Client-based connection:** Se viene attivato, è possibile utilizzare il modulo Secure Client - Zero Trust per abilitare l'accesso tramite la modalità basata su client.
- **Remote Reachable Address (FQDN, Wildcard FQDN, IP Address) :** Configurare l'indirizzo IP o FQDN delle risorse. se si configura FQDN, è necessario aggiungere il DNS per risolvere il nome.
- **Browser-based connection:** se la si abilita, sarà possibile accedere alle risorse tramite browser (aggiungere solo risorse con comunicazione HTTP o HTTPS)
- **Public URL for this resource:** Configurare l'URL pubblico da utilizzare con il browser; La risorsa è protetta da Accesso sicuro.
- **Protocol:** Selezionare il protocollo (HTTP o HTTPS)

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

**VPN Connection:** Selezionare la casella di controllo per abilitare l'accesso tramite RA-VPNaaS.

Quindi, fare clic su **Save** per aggiungere la risorsa alla **Access Policy** cartella.

Configurare i criteri di accesso

Quando si crea la risorsa, è necessario assegnarla a uno dei criteri di accesso sicuro:

- Fare clic su **Secure > Access Policy**



Secure



Monitor



Admin



Workflows

Policy

### Access Policy

Create rules to control and secure access to private and internet destinations

### Data Loss Prevention Policy

Prevent data loss/leakage with policy rules

- Fare clic su **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

Per questa regola di accesso privato è necessario configurare i valori predefiniti per consentire l'accesso alla risorsa. Per ulteriori informazioni sulle configurazioni dei criteri, consultare la [Guida dell'utente](#).

## 1 Specify Access

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) ×

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

### To

Specify one or more destinations.

SplunkFTD ×

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

- **Action** : Scegliere Consenti per consentire l'accesso alla risorsa.
- **From** : Specificare l'utente che può essere utilizzato per accedere alla risorsa.
- **To** : Scegliere la risorsa a cui si desidera accedere tramite Accesso protetto.

### 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**

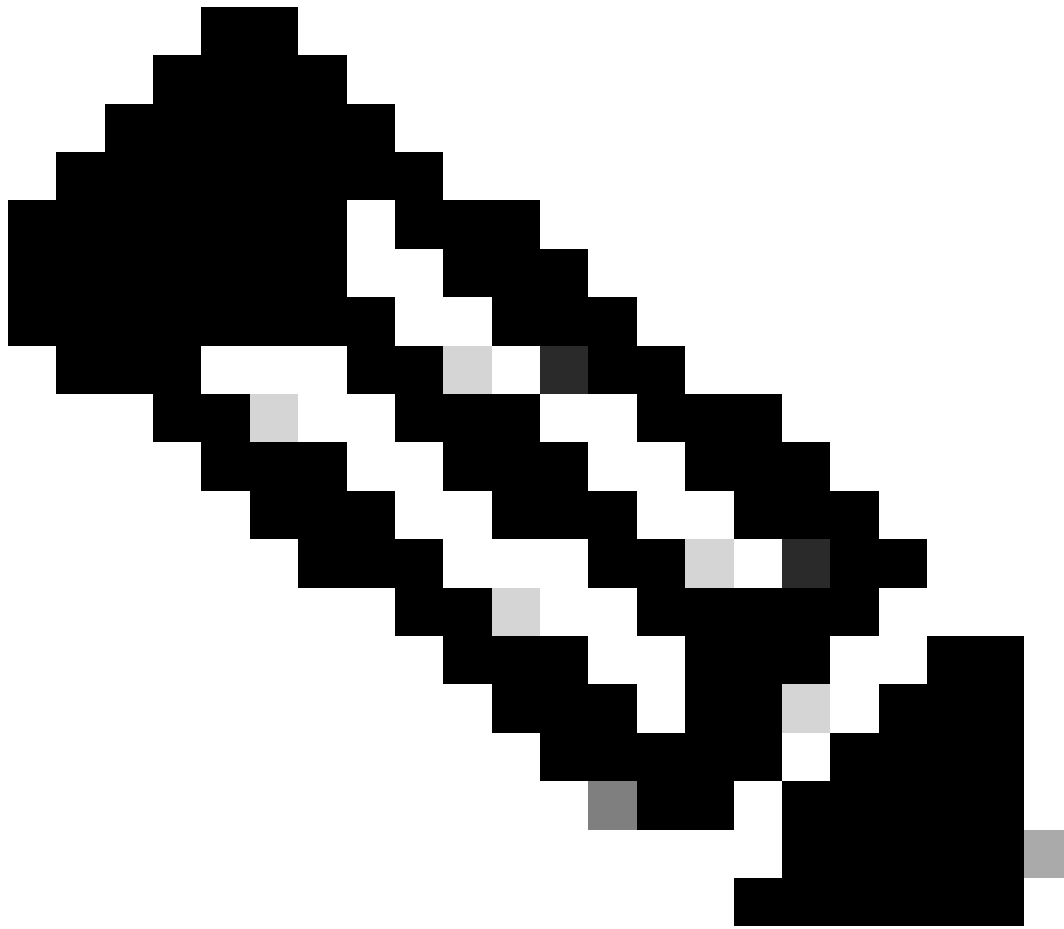
---

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**: Scegliere il profilo predefinito per l'accesso alla base client
- **Zero-Trust Browser-based Posture Profile**: Scegliere l'accesso di base predefinito al browser dei profili





Nota: Per ulteriori informazioni sui criteri di postura, consultare la [guida dell'utente](#) per l'accesso sicuro.

---

Quindi, fare clic su `Next and Save` e sulla configurazione, quindi provare ad accedere alle risorse tramite RA-VPN e Client Base ZTNA o Browser Base ZTNA.

## Risoluzione dei problemi

Per risolvere i problemi in base alla comunicazione tra Secure Firewall e Secure Access, è possibile verificare se la fase 1 (IKEv2) e la fase 2 (IPSEC) sono state stabilite tra i dispositivi senza alcun problema.

### Verifica fase 1 (IKEv2)

Per verificare la fase 1, è necessario eseguire il comando successivo sulla CLI dell'FTD:

```
show crypto isakmp sa
```

In questo caso, l'output desiderato è due **IKEv2 SAs** stabilito per gli indirizzi IP dei data center di accesso sicuro e lo stato desiderato come **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
```

## Verifica fase 2 (IPSEC)

Per verificare la fase 2, è necessario eseguire il comando successivo sulla CLI dell'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

```

Nell'ultimo output, è possibile vedere entrambi i tunnel stabiliti; ciò che non si desidera è l'output successivo sotto il pacchetto `encaps` e `decaps`.

```

#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

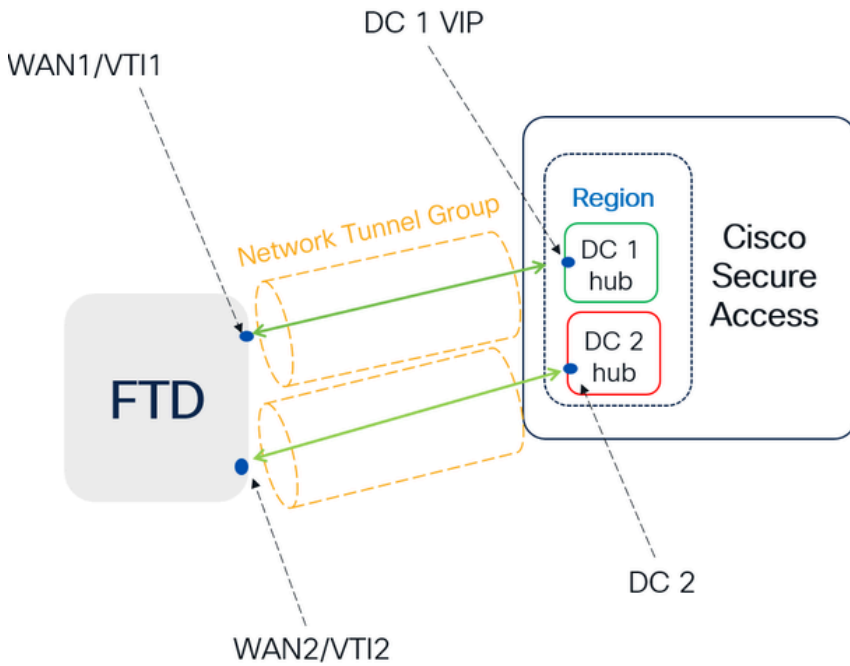
```

In questo caso, aprire una richiesta con TAC.

## Funzione High Availability

La funzione dei tunnel con accesso sicuro che comunicano con il centro dati nel cloud è attiva/passiva, il che significa che solo la porta per DC 1 sarà aperta per ricevere il traffico; lo sportello CC 2 è chiuso finché non scende il tunnel numero 1.

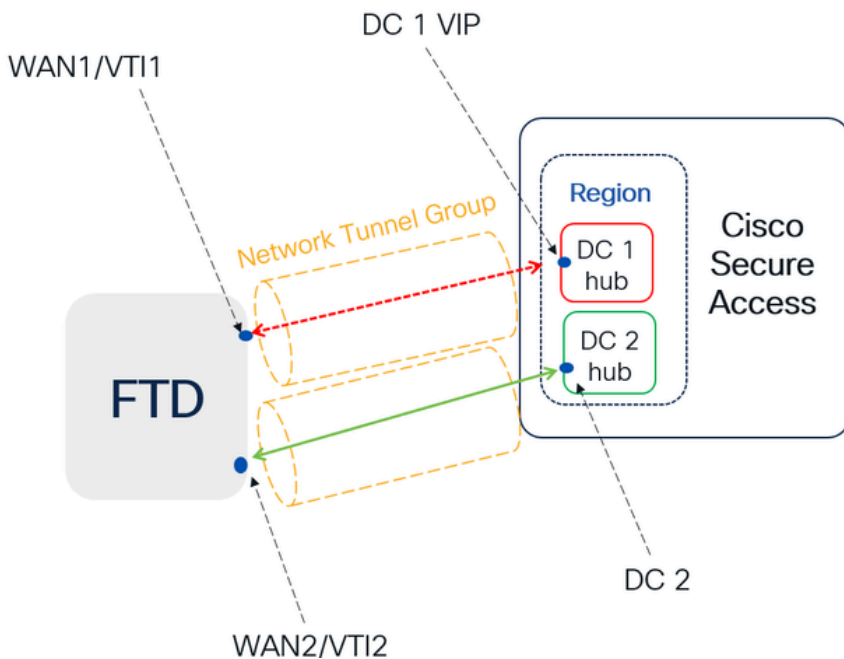
# Normal Behavior



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

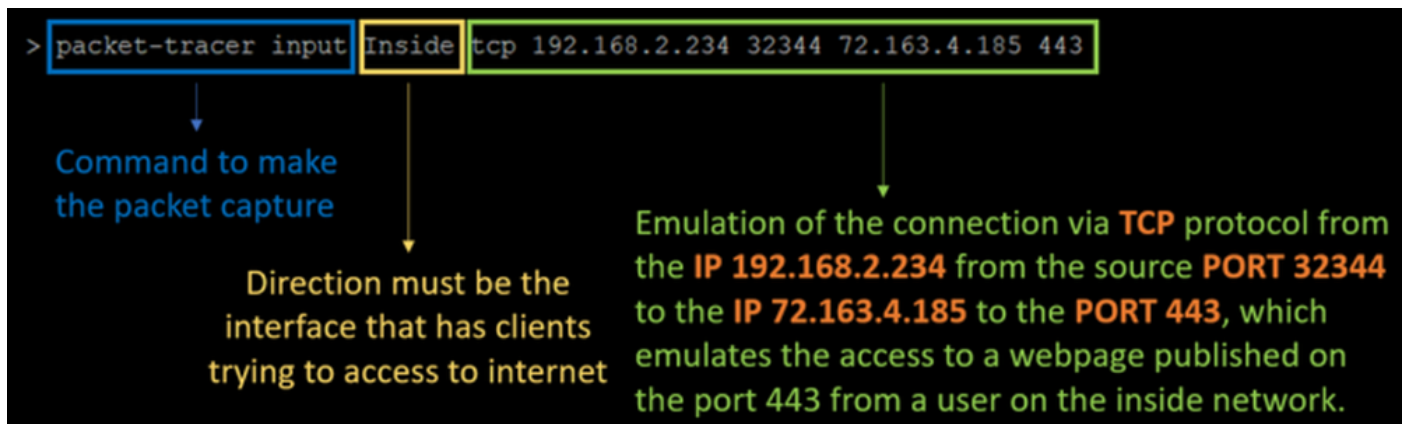
- DC2 is **Active** when DC1 or WAN1 peer is **Down**
- High availability is implemented to address failures in the WAN1 channel on the Firewall, ensuring operational continuity in the **region** and mitigating potential issues in DC1

Verifica del routing del traffico per l'accesso sicuro

In questo esempio, viene utilizzata l'origine come computer sulla rete del firewall:

- Fonte: 192.168.10.40
- Destinazione: 146.112.255.40 (Secure Access Monitoring IP)

Esempio:



Comando:

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

Uscita:

```
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



In questo caso, molte cose possono fornire un contesto relativo alla comunicazione e sapere se tutto è correttamente nella configurazione PBR per indirizzare correttamente il traffico verso 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
```

La fase 2 indica che il traffico viene inoltrato all'PrimaryVTIinterfaccia, e questa operazione è corretta perché, in base alle configurazioni di questo scenario, il traffico Internet deve essere inoltrato a Secure Access tramite 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:

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).