

使用高可用性安全防火牆配置安全訪問

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[網路圖表](#)

[設定](#)

[在安全訪問中配置VPN](#)

[用於隧道設定的資料](#)

[在安全防火牆上配置隧道](#)

[設定通道介面](#)

[配置輔助介面的靜態路由](#)

[在VTI模式下將VPN配置為安全訪問](#)

[終端配置](#)

[IKE組態](#)

[IPSEC組態](#)

[高級配置](#)

[訪問策略配置方案](#)

[Internet訪問場景](#)

[RA-VPN環境](#)

[CLAP-BAP ZTNA Escenario](#)

[配置策略基礎路由](#)

[在安全訪問中配置Internet訪問策略](#)

[配置ZTNA和RA-VPN的專用資源訪問](#)

[疑難排解](#)

[驗證階段1\(IKEv2\)](#)

[驗證階段2\(IPSEC\)](#)

[高可用性功能](#)

[驗證安全訪問的流量路由](#)

[相關資訊](#)

簡介

本文檔介紹如何使用高可用性安全防火牆配置安全訪問。

必要條件

- [配置使用者調配](#)
- [ZTNA SSO身份驗證配置](#)

- [配置遠端訪問VPN安全訪問](#)

需求

思科建議您瞭解以下主題：

- Firepower管理中心7.2
- Firepower威脅防禦7.2
- 安全訪問
- Cisco安全使用者端 — VPN
- 思科安全使用者端 — ZTNA
- 無客戶端ZTNA

採用元件

本檔案中的資訊是根據：

- Firepower管理中心7.2
- Firepower威脅防禦7.2
- 安全訪問
- Cisco安全使用者端 — VPN
- 思科安全使用者端 — ZTNA

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊



CISCO

Secure

Access

Secure Firewall

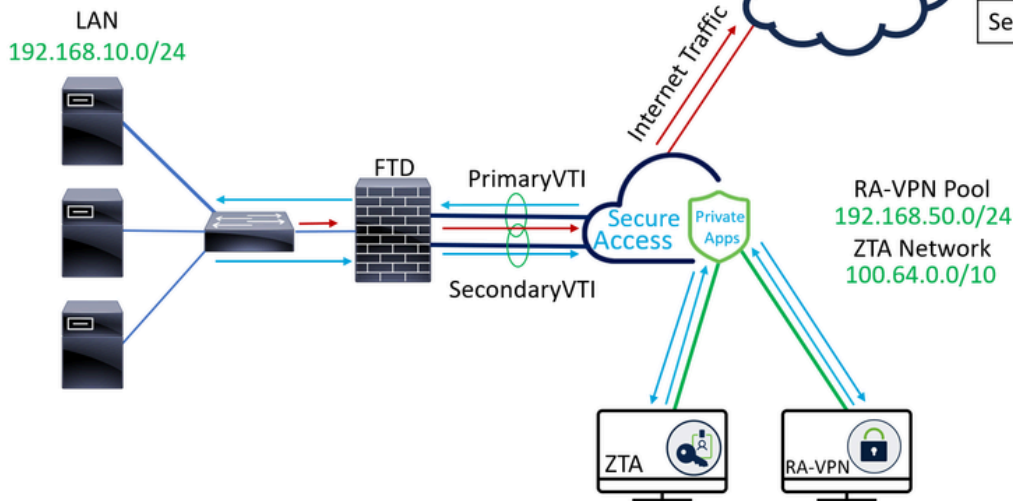
FTD

思科設計了安全訪問，可保護和提供對內部和基於雲的私有應用的訪問。它還保護從網路到 Internet 的連線。這是通過實施多種安全方法和層實現的，所有這些方法都旨在保護通過雲訪問資訊時的資訊。

網路圖表

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

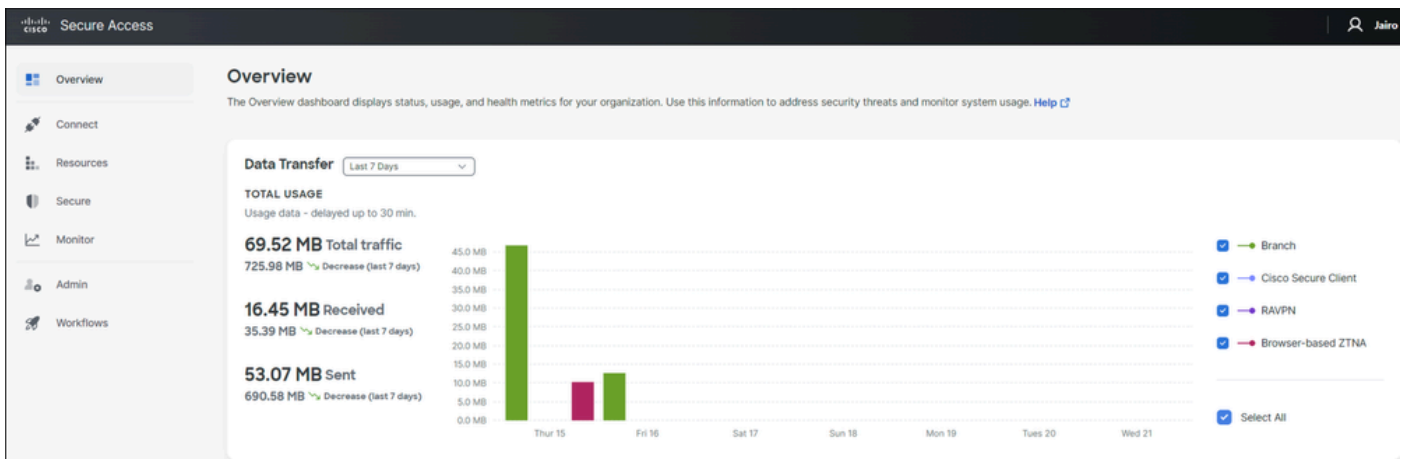
INTERFACE	IP
PrimaryWAN	192.168.30.5
PrimaryVTI	169.254.2.1
SecondaryWAN	192.168.0.202
SecondaryVTI	169.254.3.1



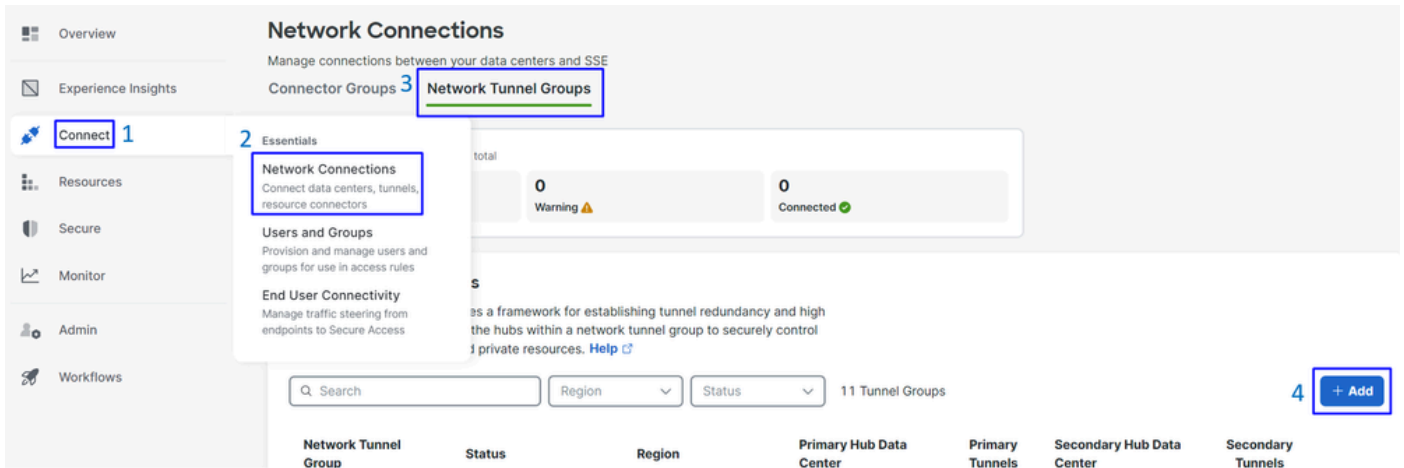
設定

在安全訪問中配置VPN

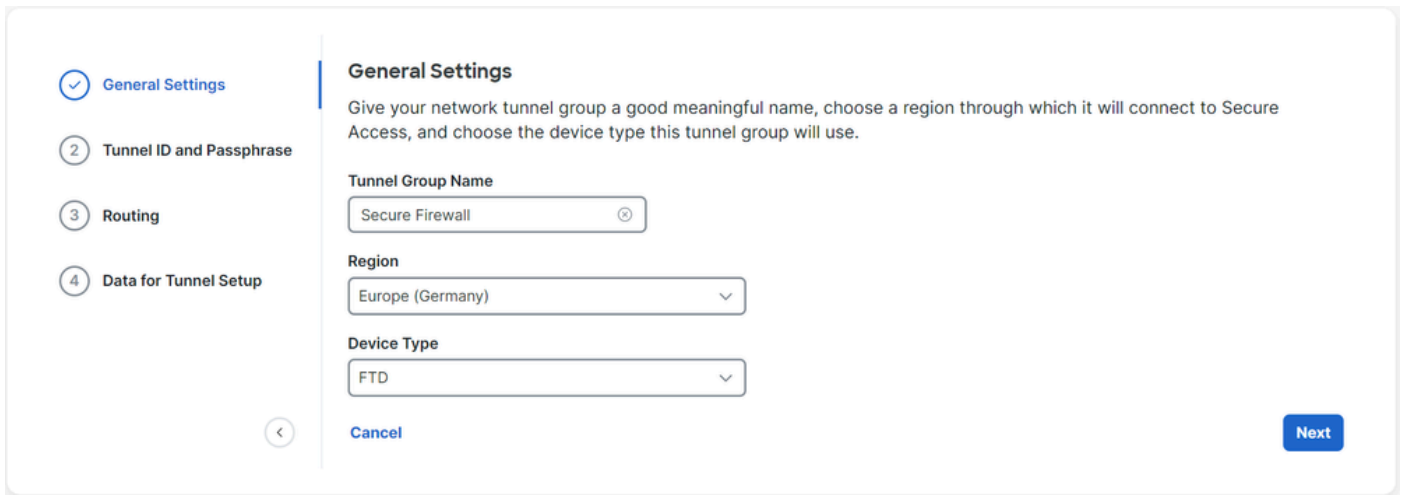
導航到的管理面板 [安全訪問](#).



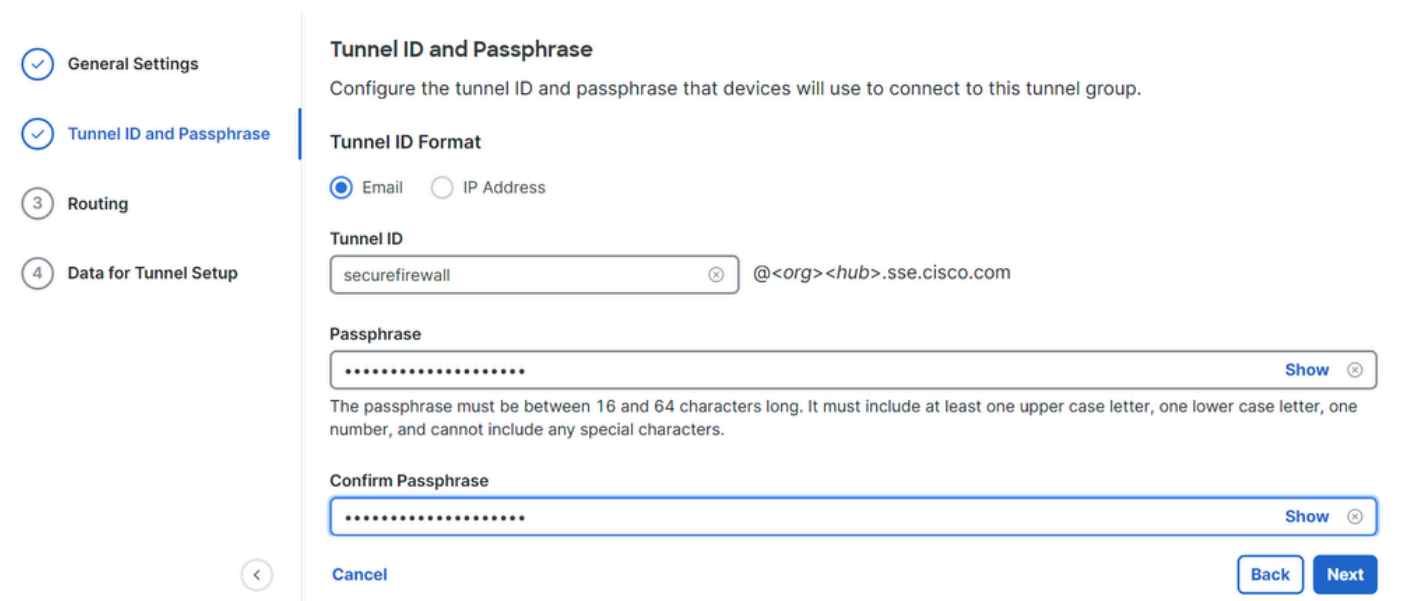
- 按一下 Connect > Network Connections
- 在Network Tunnel Groups 下，按一下 + Add



- **Configure** Tunnel Group Name, Region 和 Device Type
- 按一下 **Next**



- **配置** Tunnel ID Format 和 Passphrase
- 按一下 **Next**



- 配置在網路上已配置且希望通過安全訪問傳遞流量的IP地址範圍或主機

- 按一下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.

Add

192.168.0.0/24 X192.168.10.0/24 X

Dynamic routing

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

[Cancel](#)

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

按一下顯示的Save「通道資訊」後，請儲存下一步的相關資訊。 **Configure the tunnel on Secure Firewall.**

用於隧道設定的資料

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

Download CSV
Done

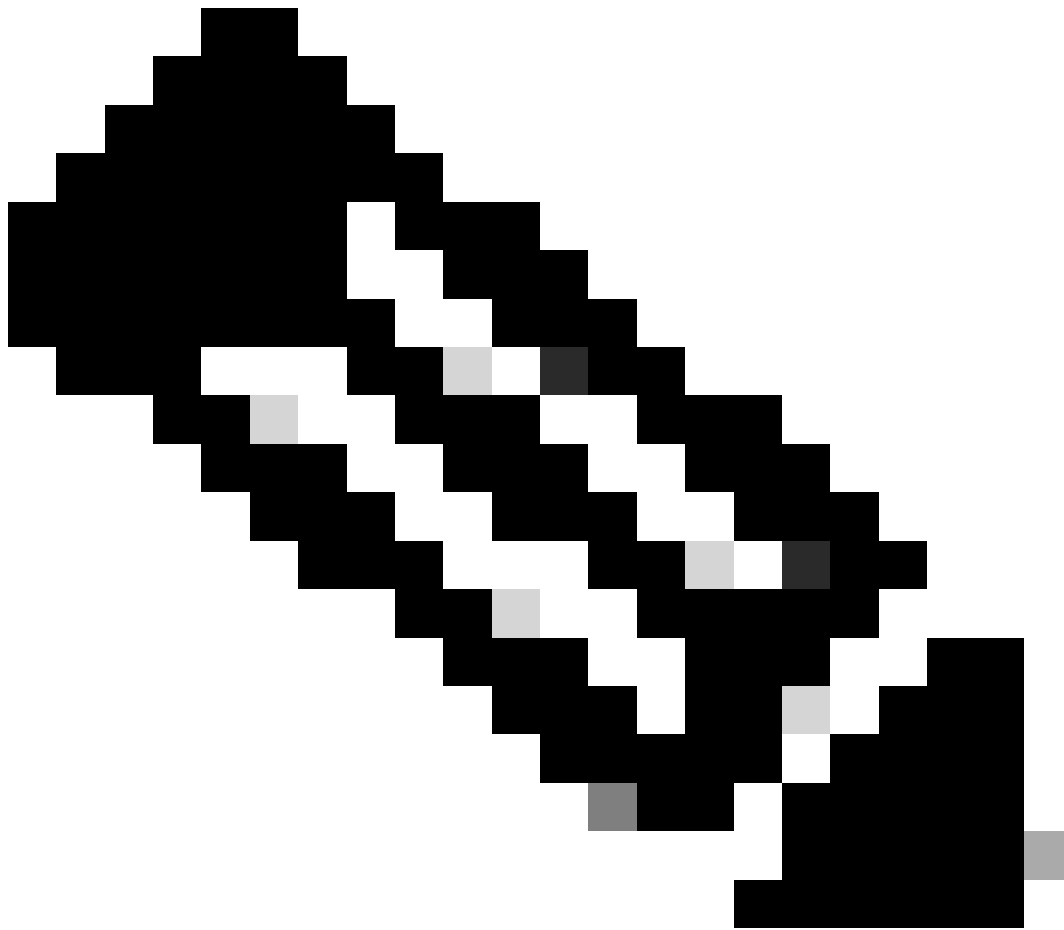
在安全防火牆上配置隧道

設定通道介面

在此案例中，您使用安全防火牆上的虛擬通道介面(VTI)組態來實現此目標；請記住，在這種情況下，您有兩個ISP，如果其中一個ISP發生故障，我們希望有HA。

介面	角色
----	----

主要WAN	主要網際網路WAN
輔助WAN	輔助網際網路WAN
PrimaryVTI	連結以將流量通過傳送到Principal Internet WAN安全訪問
輔助VTI	連結以將流量通過傳送到Secondary Internet WAN安全訪問



附註：1.需要向新增靜態路由或為其分配靜態路由 Primary or Secondary Datacenter IP，才能啟用兩個隧道。



附註：2.如果在介面之間配置了ECMP，則無需建立到的任何靜態路由，即可啟用兩個隧道
Primary or Secondary Datacenter IP。

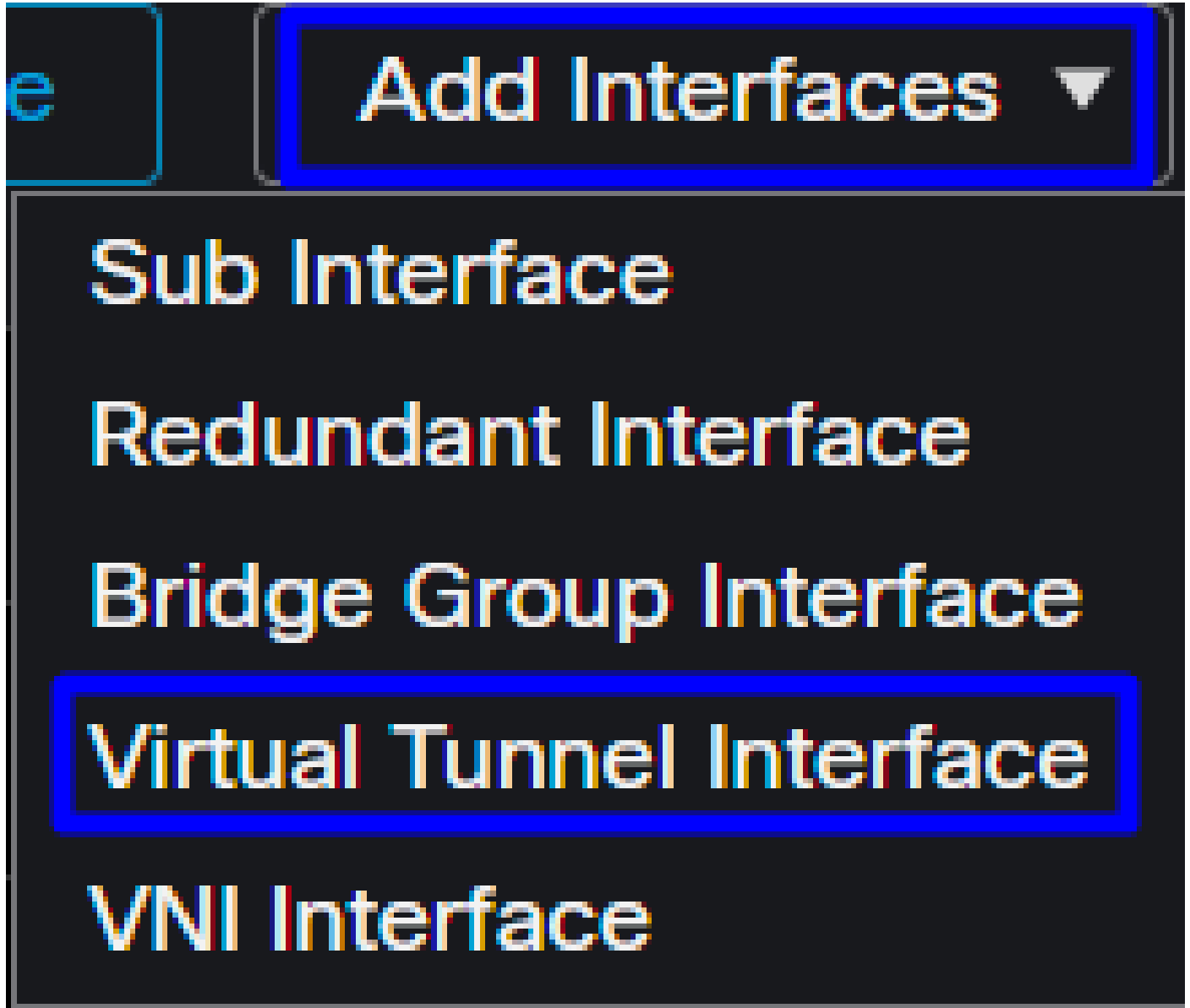
根據場景，我們有PrimaryWAN和，SecondaryWAN必須使用這些來建立VTI介面。

導航到您的Firepower Management Center > Devices。

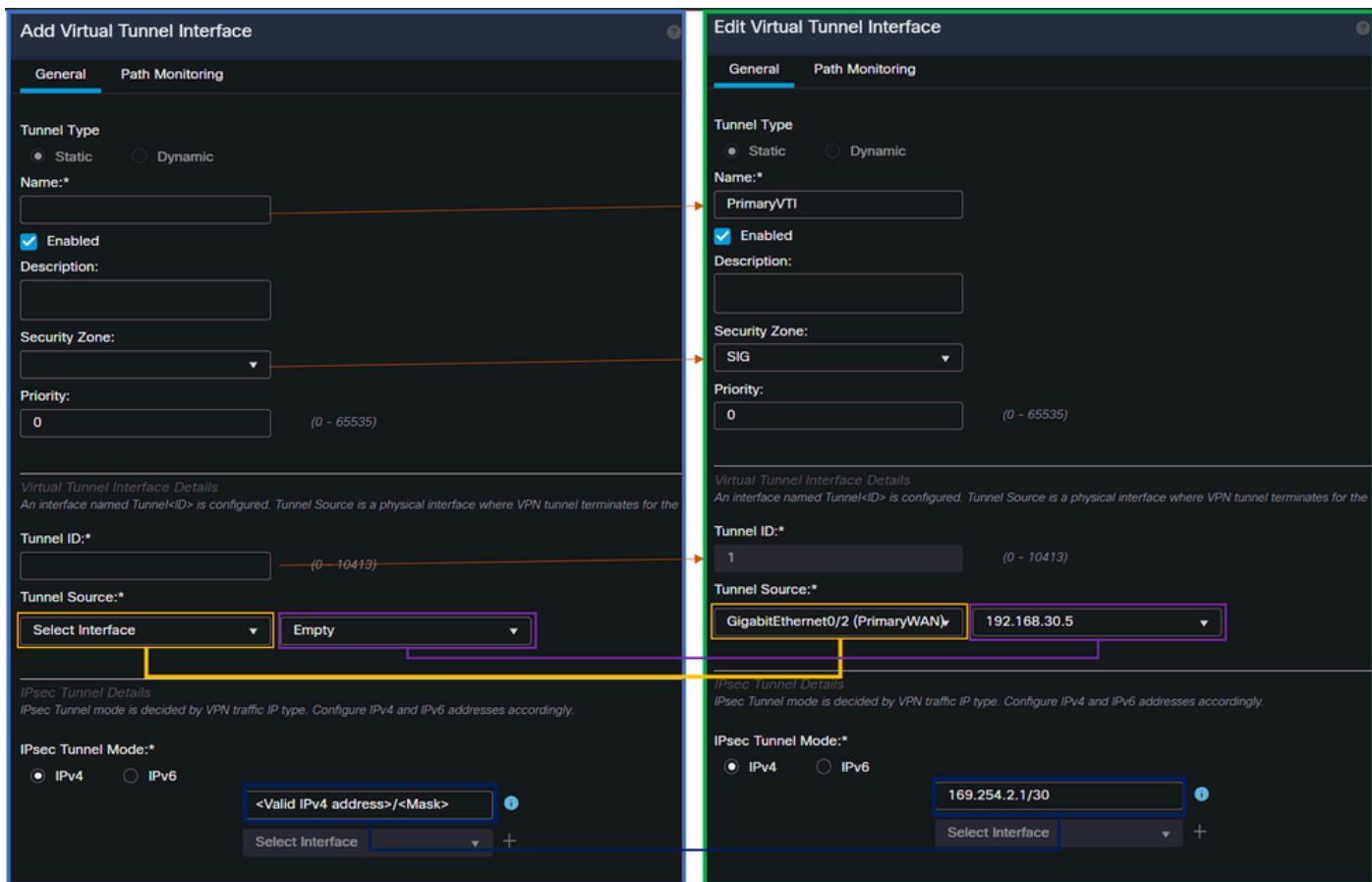
- 選擇您的FTD
- 選擇 Interfaces

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)

- 按一下 Add Interfaces > Virtual Tunnel Interface



- 根據下一個資訊配置介面



- Name :配置一個名稱，該名稱引用 PrimaryWAN interface
- Security Zone :您可以重複使用另一Security Zone個流量，但是為安全訪問流量建立新的流量會更好
- Tunnel ID :為通道ID新增一個數字
- Tunnel Source :選擇PrimaryWAN interface並選擇介面的專用或公用IP
- IPsec Tunnel Mode :選擇IPv4並配置網路中帶有掩碼30的不可路由IP

附註：對於VTI介面，必須使用不可路由的IP;例如，如果您有兩個VTI介面，則可以將169.254.2.1/30用PrimaryVTI於，將169.254.3.1/30用SecondaryVTI於。

之後，您需要對執行相同的操作，並且已為VTI高可用性做好了各項設定，因此，您將得到下一個結SecondaryWAN interface果：

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)

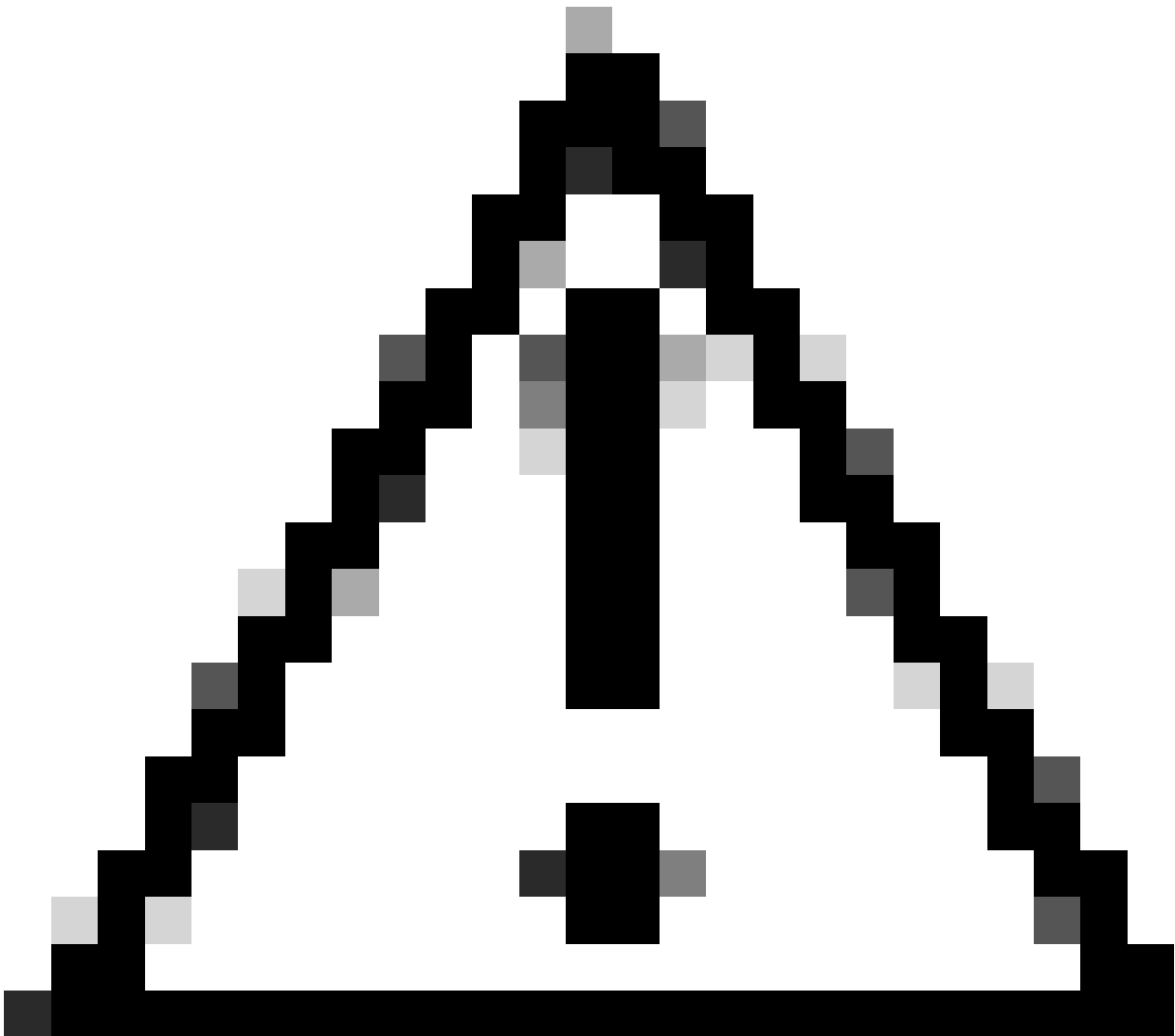
在此案例中，使用的IP如下：

VTI IP配置

邏輯名稱	IP	範圍
PrimaryVTI	169.254.2.1/30	169.254.2.1-169.254.2.2
輔助VTI	169.254.3.1/30	169.254.3.1-169.254.3.2

配置輔助介面的靜態路由

要允許流量到達Secondary WAN interface 的流量Secondary Datacenter IP Address，您需要配置到資料中心IP的靜態路由。可以使用度量一(1)進行配置，使其位於路由表之上；此外，請指定IP作為主機。



注意：僅當在WAN通道之間沒有ECMP設定時，才需要這樣做；如果已配置ECMP，則可以跳至下一步。

- 按一下FTD裝置
- 按一下 Routing
- 選擇 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 ↻ +

192.168.0.150

192.168.10.153

any-ipv4

ASA_GW

CSA_Primary

GWWT1

Add

Selected Network

SecureAccessTunnel

↓

Choose the Secondary Datacenter IP

Cancel
OK

- Interface: 選擇輔助WAN介面

- Gateway: 選擇輔助WAN網關
- Selected Network: 新增輔助資料中心IP作為主機；在安全訪問步驟中配置隧道時，您可以找到相關資訊，如[Data for Tunnel Setup](#)
- Metric: 使用-(1)
- OK 按一下Save並儲存資訊，然後進行部署。

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						

在VTI模式下將VPN配置為安全訪問

要配置VPN，請導航到您的防火牆：

- 按一下 **Devices > Site to Site**
- 按一下 **+ Site to Site VPN**

終端配置

要配置終端步驟，您需要使用步驟[Data for Tunnel Setup](#)中提供的資訊。

Create New VPN Topology

Topology Name:*
SecureAccess

Policy Based (Crypto Map) Route Based (VTI)

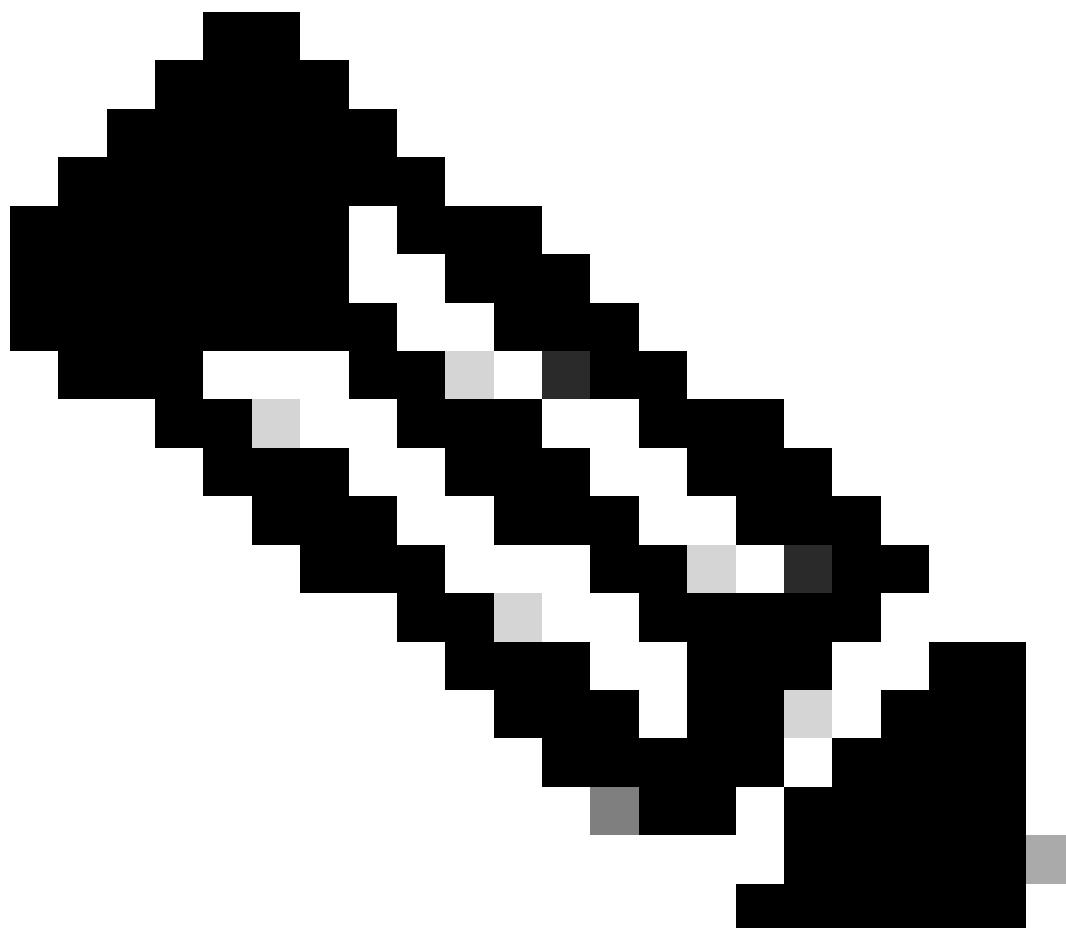
Network Topology:

IKE Version:* IKEv1 IKEv2

Endpoints | IKE | IPsec | Advanced

Node A	Node B
Device:* FTD_HOME	Device:* Extranet
Virtual Tunnel Interface:* PrimaryVTI (IP: 169.254.2.1) +	Device Name*: 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*: 18.156.145.74,3.120.45.23
Local Identity Configuration:* Email ID jairohome@8195126-615626006-	
Backup VTI: Remove	

- 拓撲名稱：建立與安全訪問整合相關的名稱
 - 選擇 **Routed Based (VTI)**
 - 選擇 **Point to Point**
 - IKE Version:選擇IKEv2
-



附註：與Secure Access整合不支援IKEv1。

在下Node A面，您需要配置以下引數：

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:選擇FTD裝置
- Virtual Tunnel Interface:選擇與相關的PrimaryWAN InterfaceVTI。
- 選中覈取方塊 Send Local Identity to Peers
- Local Identity Configuration:選擇Email ID (電子郵件ID) , 然後根據步驟Primary Tunnel IDData for Tunnel Setup (隧道設定的資料) 中提供的資訊填寫

在配置上的資訊後 , PrimaryVTI請單+ Add Backup VTI擊 :

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:選擇與相關的PrimaryWAN InterfaceVTI。
- 選中竅取方塊 Send Local Identity to Peers
- Local Identity Configuration:選擇Email ID (電子郵件ID) ，然後根據步驟Secondary Tunnel IDData for Tunnel Setup (隧道設定的資料) 中提供的資訊填寫

在下Node B面，您需要配置以下引數：

Node B

Device:*

Extranet

Device Name*:

SecureAccess

Endpoint IP Address*:

18.156.145.74, 3.120.45.23

- Device: Extranet
- Device Name: 選擇名稱以將Secure Access識別為目標。
- Endpoint IP Address: 主要和輔助的配置必須為主要，Datacenter IP, Secondary Datacenter IP您可以在步驟 [Data for Tunnel Setup](#)中找到該資訊

完成後，您的配Endpoints置即完成，現在您可以轉到步驟IKE Configuration。

IKE組態

要配置IKE引數，請點選IKE。

Endpoints

IKE

IPsec

Advanced

在IKE, 下，您需要配置以下引數：

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: 您可以使用預設的Umbrella配Umbrella-AES-GCM-256置，也可以根據 [Supported IKEv2 and IPSEC Parameters](#)
- Authentication Type: 預共用手動金鑰
- Key和: Confirm Key 您可以在步驟 [Passphrase Data for Tunnel Setup](#) 中找到資訊

完成後，您的配IKE置即完成，現在您可以轉到步驟IPSEC Configuration。

IPSEC組態

要配置IPSEC引數，請按一下IPSEC。

Endpoints

IKE



IPsec

Advanced

在IPSEC, 下，您需要配置以下引數：

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

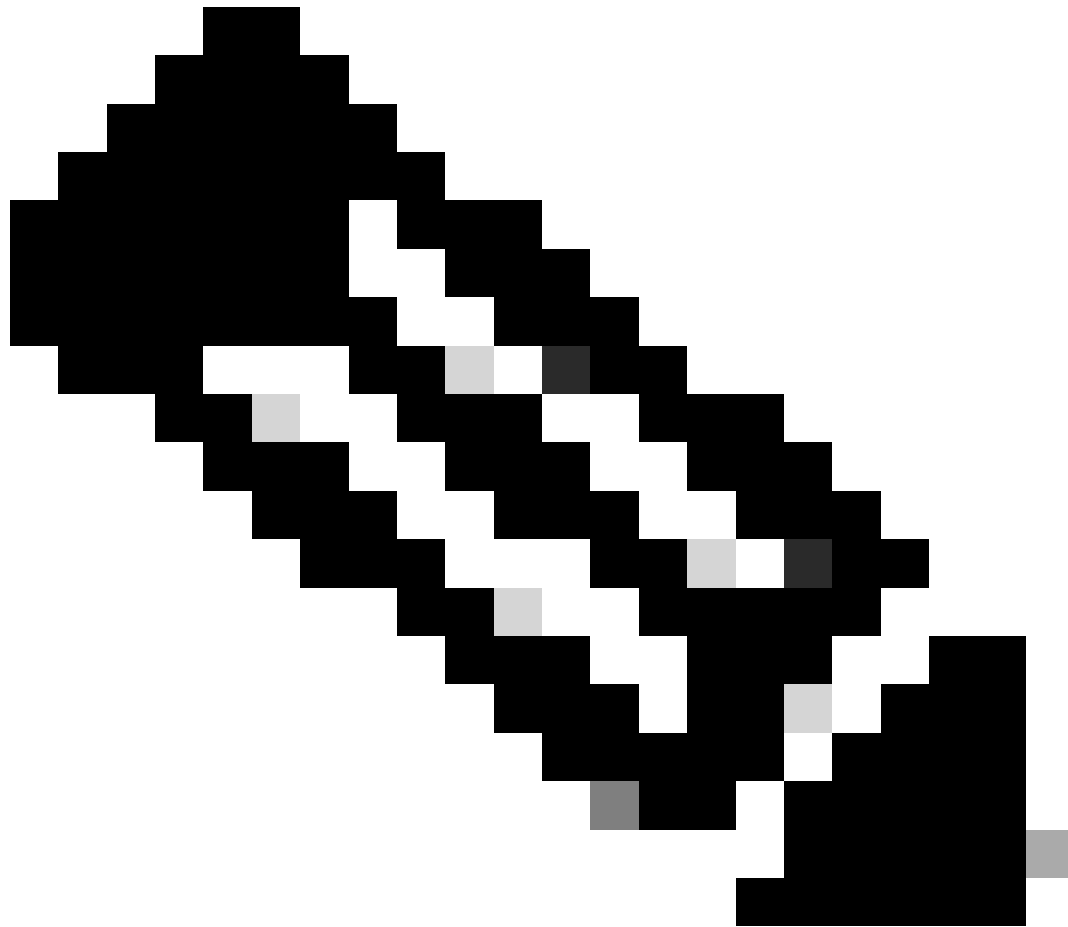
Enable Perfect Forward Secrecy

Modulus Group: 14

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

Lifetime Size: 4608000 Kbytes (Range 10-2147483647)

- Policies: 您可以使用預設的Umbrella配Umbrella-AES-GCM-256置，也可以根據 [Supported IKEv2 and IPSEC Parameters](#)



附註：IPSEC不需要其他任何內容。

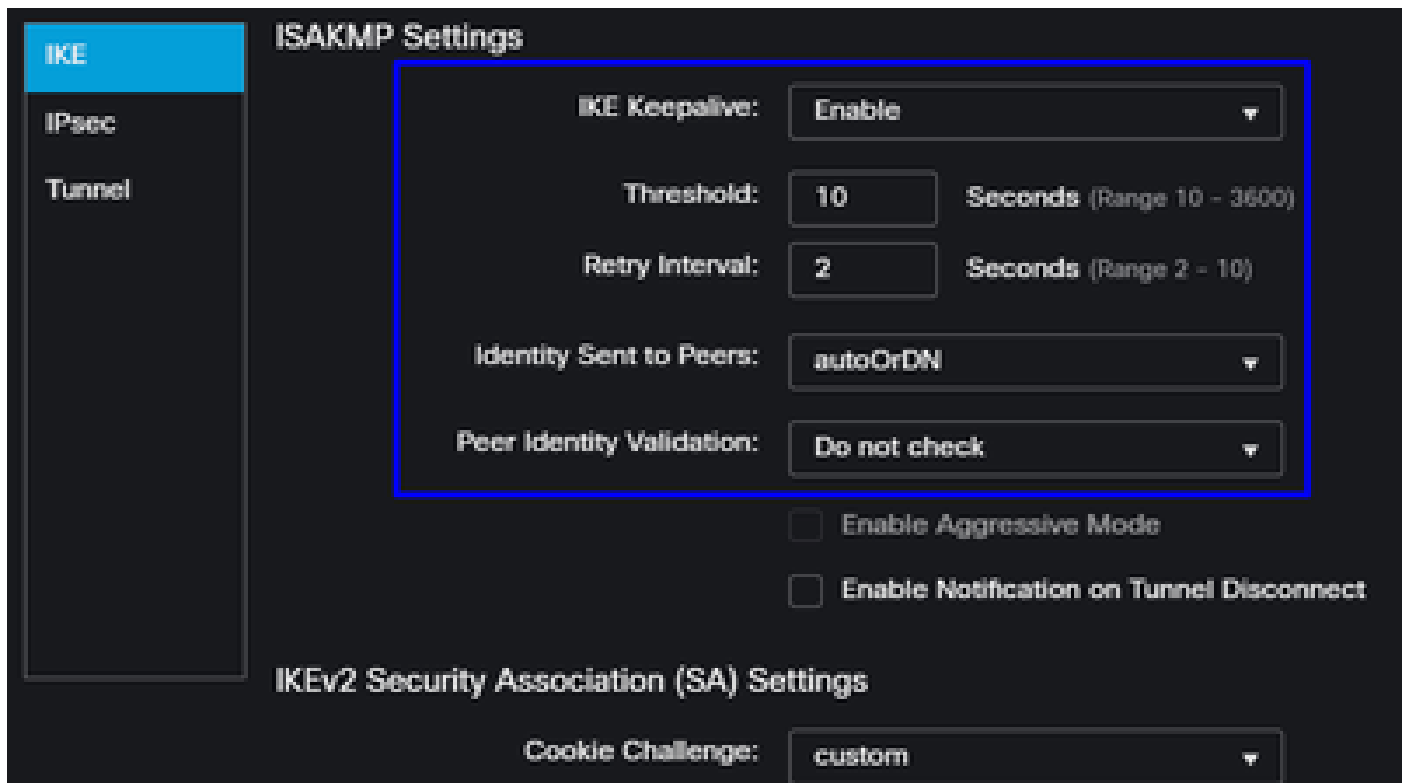
完成後，您的配IPSEC置即完成，現在您可以轉到高級配置步驟。

高級配置

要配置高級引數，請按一下高級。



在Advanced, 下，您需要配置以下引數：



- IKE Keepalive: 啟用
- Threshold: 10
- Retry Interval: 2
- Identity Sent to Peers: autoOrDN
- Peer Identity Validation: 不檢查

之後，您可以點選SaveDeploy 和。



附註：幾分鐘後，您會看到為兩個節點建立的VPN。

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)

完成後，您的配VPN to Secure Access in VTI Mode置完成，現在您可以轉到第步Configure Policy Base Routing。



警告：建立兩個通道時，前往安全存取的流量僅轉送到主通道；如果主隧道關閉，安全訪問允許通過輔助隧道轉發流量。

注意：安全訪問站點上的故障轉移基於使用手冊中記錄的DPD值來確定支援的IPsec值。

訪問策略配置方案

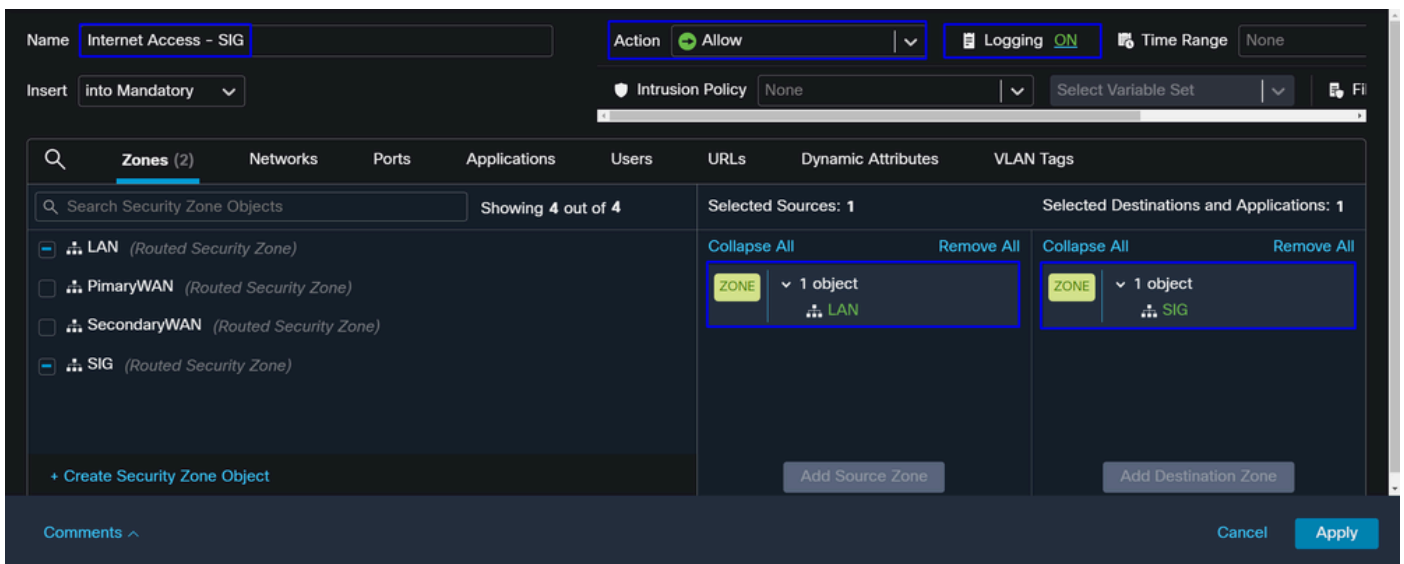
定義的訪問策略規則基於：

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)

介面	區域
PrimaryVTI	SIG
輔助VTI	SIG
LAN	LAN

Internet訪問場景

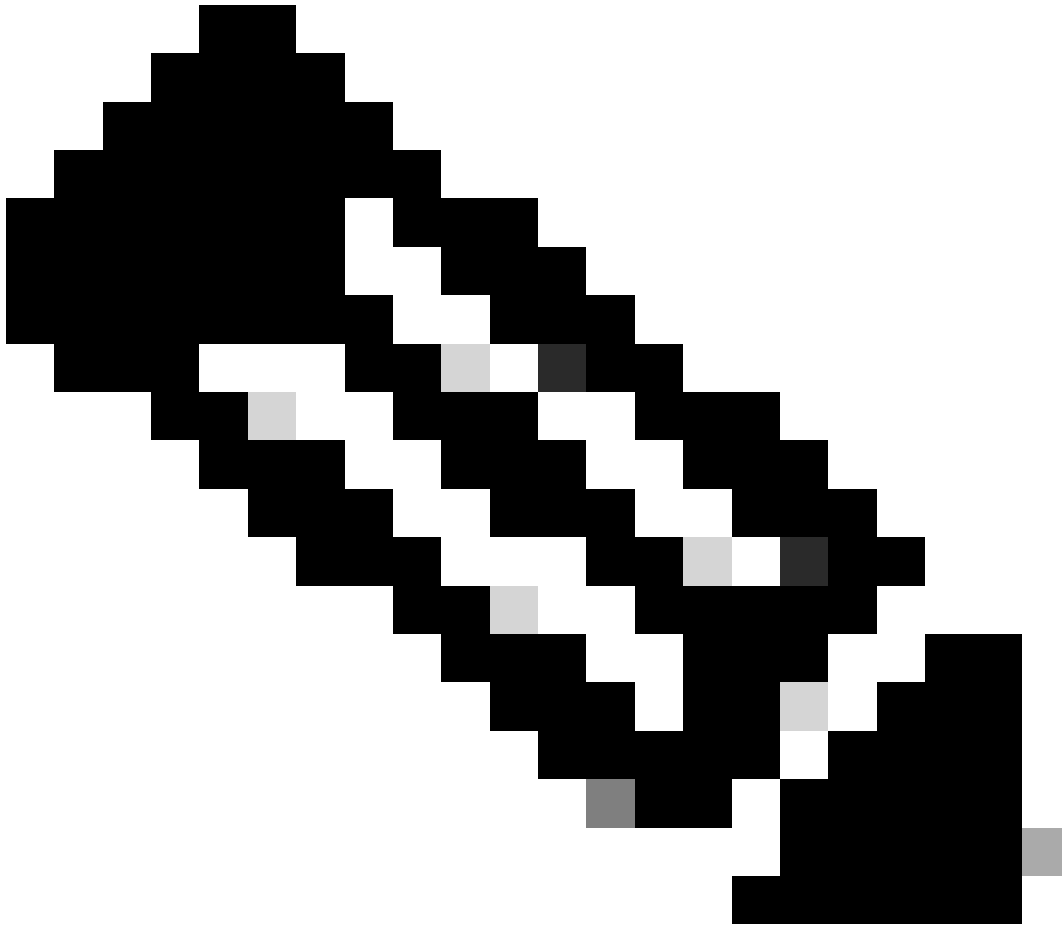
要提供對您在Policy Base Routing上配置的所有資源的網際網路訪問，您需要配置一些訪問規則以及安全訪問中的某些策略，因此讓我解釋一下在此場景中如何實現這一目標：



此規則提供對LANInternet的訪問，在本例中為Internet訪SIG問。

RA-VPN環境

要提供RA-VPN使用者的訪問許可權，您需要根據在RA-VPN池上分配的範圍對其進行配置。



附註：要配置RA-VPNaaS策略，可以通過[管理虛擬專用網路](#)

如何驗證VPN的IP池？

導航到您的[Secure Access Dashboard](#)

- 按一下 Connect > End User Connectivity
- 按一下 Virtual Private Network
- 在Manage IP Pools下，按一下 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

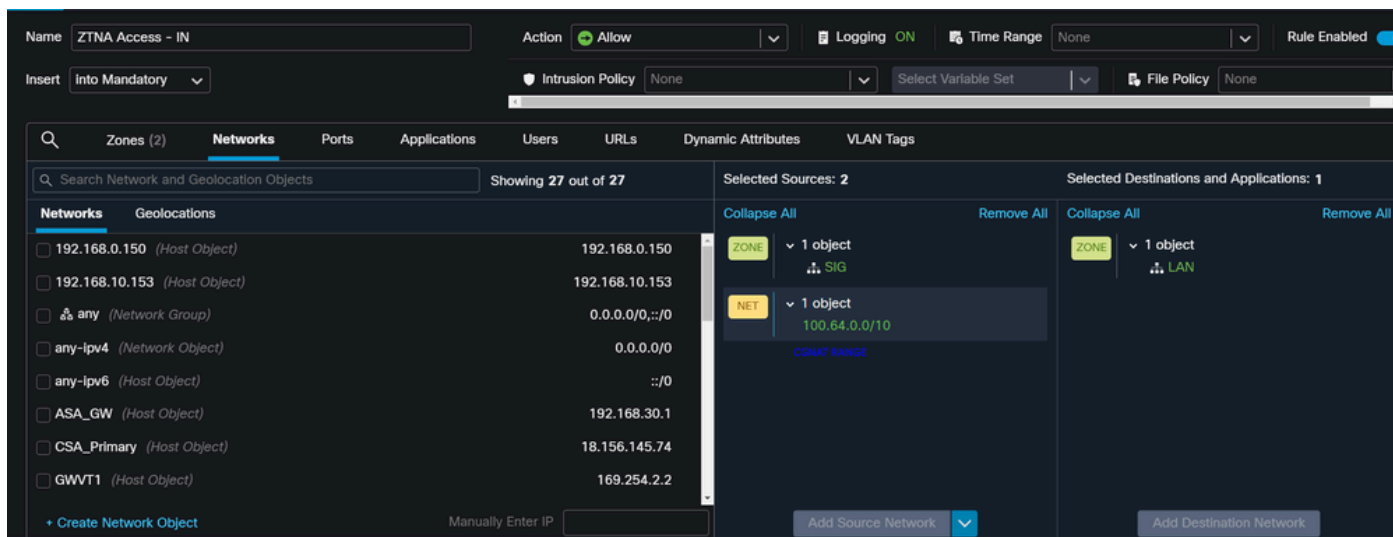
Manage

CLAP-BAP ZTNA Escenario

您必須根據CGNAT範圍100.64.0.0/10配置您的網路，以便從客戶端基礎ZTA或瀏覽器基礎ZTA使用者訪問您的網路。

訪問規則配置

如果僅將Secure Access配置為使用它以及訪問專用應用程式資源的功能，則您的訪問規則可能如下所示：

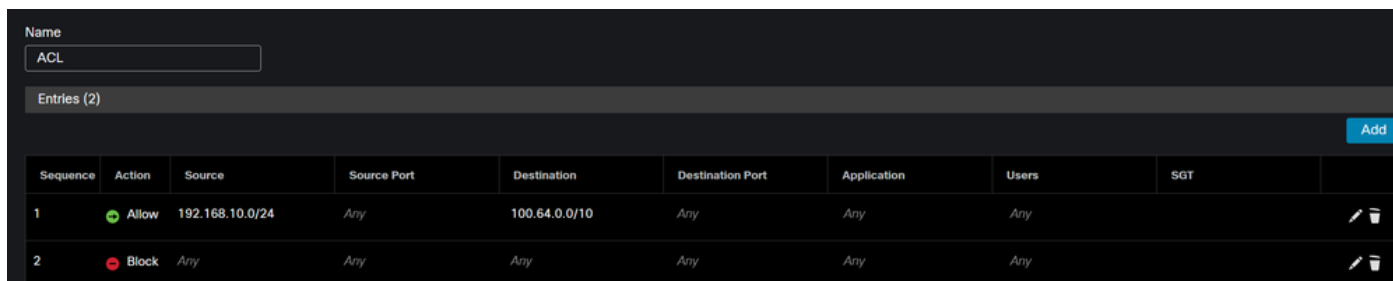


The screenshot shows the configuration for a rule named "ZTNA Access - IN". The rule is enabled and has an "Allow" action with logging turned on. The source is configured with "any" and "any-ipv4". The destination is configured with "any-ipv4" and "any-ipv6". The rule is applied to the "LAN" zone.

此規則允許從ZTNA CGNAT範圍100.64.0.0/10到您的LAN的流量。

ACL配置

要允許使用CGNAT從SIG到LAN的路由流量，您必須將其新增到ACL下使其在PBR下工作。



The screenshot shows the configuration for an ACL named "ACL". It has two entries:

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	

配置策略基礎路由

要通過Secure Access提供對內部資源和Internet的訪問，您必須通過策略基礎路由(PBR)建立路由，以便於將流量從源路由到目標。

- 導航至 **Devices > Device Management**
- 選擇您建立路由的FTD裝置

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

- 按一下 **Routing**
- 選擇 **Policy Base Routing**
- 按一下 **Add**

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

在此場景中，您選擇所有用作源以路由流量到安全訪問的介面，或者為使用RA-VPN對網路內部資源進行安全訪問或基於客戶端或基於瀏覽器的ZTA訪問提供使用者身份驗證：

- 在Ingress Interface下，選擇所有通過Secure Access傳送流量的介面：

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

- 在「匹配條件」(Match Criteria)和「輸出介面」(Egress Interface)下，按一下Add後定義下一個引數：

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

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:對於此ACL，您可以配置路由到安全訪問的所有內容：

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	208.67.222.222 208.67.220.220	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:選擇IP地址
- IPv4 Addresses:您必須使用兩個VTI上所設定之遮罩30下的下一個IP;您可以在步驟[VTI Interface Config](#)中

介面	IP	GW
PrimaryVTI	169.254.2.1/30	169.254.2.2
輔助VTI	169.254.3.1/30	169.254.3.2

IPv4 Addresses: For example, 192.168.0.1, 10.10.1.2

➔

IPv4 Addresses: 169.254.2.2, 169.254.3.2

進行這樣的配置後，您將得到下一個結果，您可以繼續按一下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

之後，您需要再次Save進行配置，然後採用以下方式對其進行配置：

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.

Match ACL	Forwarding Action
ACL	<p>Send through</p> <p>169.254.2.2 → Send the traffic to the PrimaryVTI</p> <p>169.254.3.2</p>

If PrimaryVTI fail it will send the traffic to the SecondaryVTI

之後，您可以進行部署，並看到在ACL上配置的電腦的流量將流量路由到安全訪問：

在FMCConexion Events中：



附註：預設情況下，預設的安全訪問策略允許流量通過Internet。要提供對專用應用程式的訪問，您需要建立專用資源並將其新增到專用資源訪問的訪問策略中。

在安全訪問中配置Internet訪問策略

要配置網際網路訪問的訪問，您需要在[Secure Access Dashboard](#)上創建策略：

- 按一下 **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

- 按一下 [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

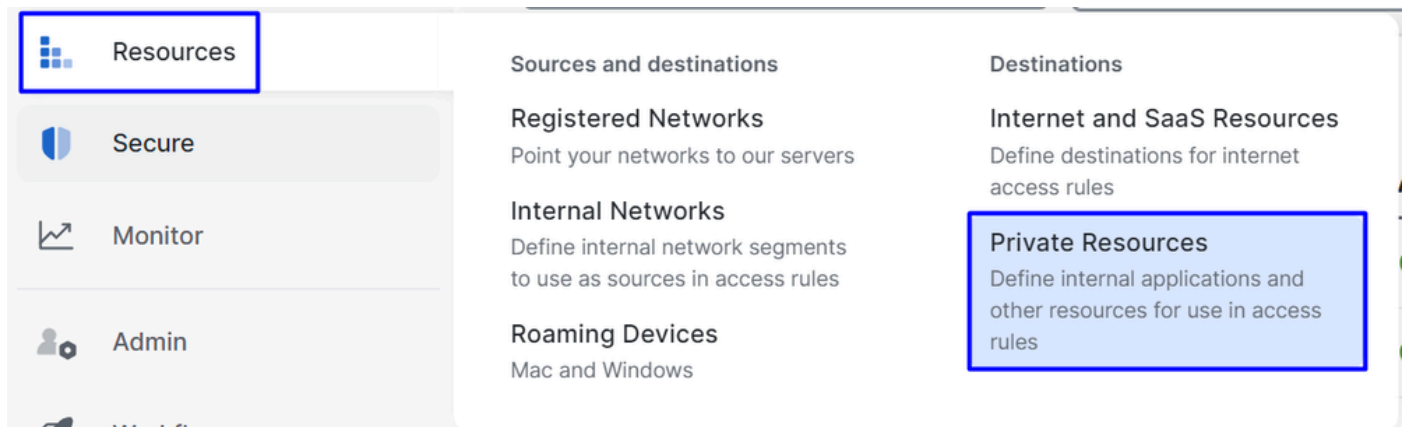
Control and secure access to public destinations from within your network and from managed devices

您可以在此處將源指定為隧道，而至目標，您可以選擇任意，具體取決於要在策略上配置的內容。請檢視[Secure Access使用手冊](#)。

配置ZTNA和RA-VPN的專用資源訪問

要配置專用資源的訪問，您需要首先在[Secure Access Dashboard](#)下建立資源：

按一下 **Resources > Private Resources**



- 然後按一下 **ADD**

在配置下，您可以找到要配置的以下各節：**General, Communication with Secure Access Cloud and Endpoint Connection Methods.**

一般

General

Private Resource Name

Description (optional)

- Private Resource Name : 為通過安全訪問網路提供訪問許可權的資源建立名稱

端點連線方法

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:**選中覈取方塊。
- **Client-based connection:**如果啟用該功能，則可以使用安全客戶端 — 零信任模組啟用通過客戶端基礎模式的訪問。
- **Remote Reachable Address (FQDN, Wildcard FQDN, IP Address) :**配置資源IP或FQDN;如果配置FQDN，則需要新增DNS以解析名稱。
- **Browser-based connection :** 如果啟用該功能，則可以通過瀏覽器訪問資源（請僅通過HTTP或HTTPS通訊新增資源）
- **Public URL for this resource:**透過瀏覽器設定您使用的公用URL;Secure Access可保護此資源。
- **Protocol:**選擇協定（HTTP或HTTPS）

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

VPN Connection:選中此覈取方塊可啟用通過RA-VPNaaS的訪問。

然後，單Save擊，即可將該資源新增到Access Policy。

配置訪問策略

建立資源時，需要將其分配給安全訪問策略之一：

- 按一下 **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

- 按一下 [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

對於此專用訪問規則，可以配置預設值以提供對資源的訪問。要瞭解有關策略配置的詳細資訊，請檢視[使用手冊](#)。

1 Specify Access

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

Action

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

From

Specify one or more sources.

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

To

Specify one or more destinations.

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

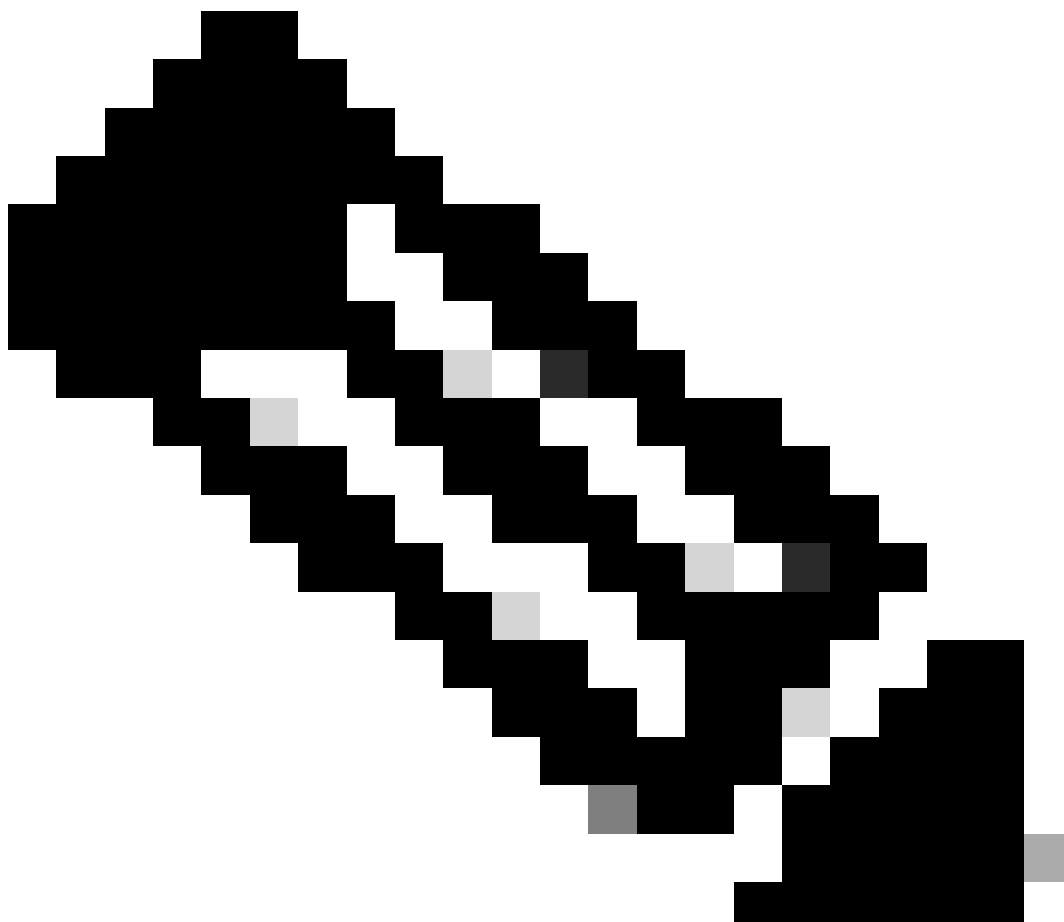
- **Action** :選擇Allow以提供對資源的訪問。
- **From** :指定可用於登入到資源的使用者。
- **To** :選擇要通過Secure Access訪問的資源。

Endpoint Requirements

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

<input type="checkbox"/> Zero-Trust Client-based Posture Profile Rule Defaults Requirements for end-user devices on which the Cisco Secure Client is installed. <input type="text" value="System provided (Client-based)"/> Private Resources: SplunkFTD
<input type="checkbox"/> Zero Trust Browser-based Posture Profile Rule Defaults Requirements for end-user devices on which the Cisco Secure Client is NOT installed. <input type="text" value="System provided (Browser-based)"/> Private Resources: SplunkFTD

- **Zero-Trust Client-based Posture Profile**:選擇客戶端基本訪問的預設配置檔案
- **Zero-Trust Browser-based Posture Profile** : 選擇預設配置檔案瀏覽器基本訪問許可權



附註：要瞭解有關狀態策略的更多資訊，請檢視[安全訪問](#)使用手冊。

然後，點選Next和Save 和您的配置，您可以嘗試通過RA-VPN和客戶端基礎ZTNA或瀏覽器基礎ZTNA訪問您的資源。

疑難排解

要根據安全防火牆和安全訪問之間的通訊進行故障排除，您可以驗證裝置之間是否建立第1階段(IKEv2)和第2階段(IPSEC)而沒有問題。

驗證階段1(IKEv2)

若要驗證Phase1，您需要在FTD的CLI上執行下一個命令：

```
show crypto isakmp sa
```


在這種情況下，所需的輸出是建立到數IKEv2 SAs據中心安全訪問IP的兩個輸出，並且所需的狀態如READY下：

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
```

驗證階段2(IPSEC)

若要驗證Phase2，您需要在FTD的CLI上執行下一個命令：

```
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
```

在上次輸出中，您可以看到兩個通道已建立；不需要的只是資料包encaps和decaps下的下一個輸出。

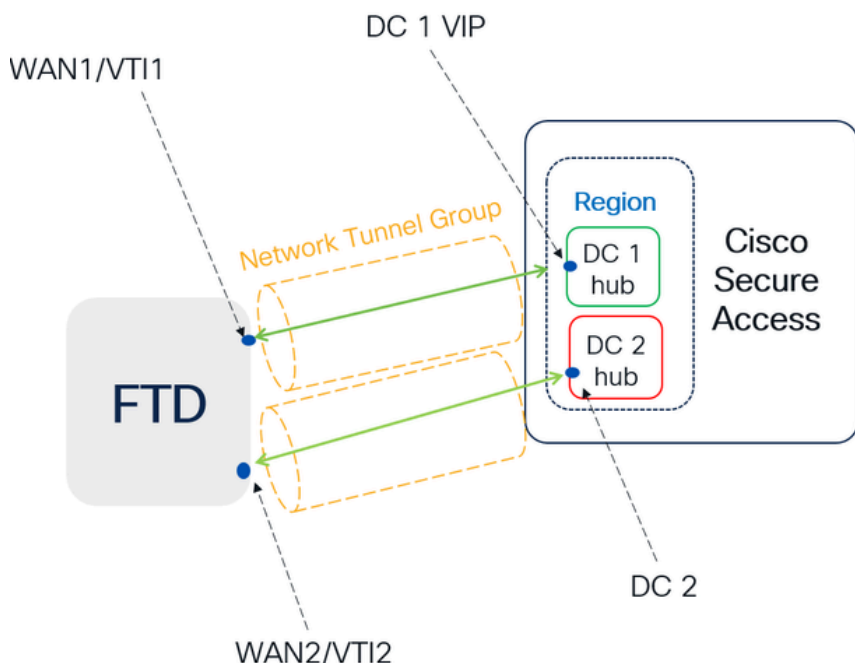
```
#pkts encaps: 71965, #pkts encrypt: 71965, #pkts digest: 71965 → Packets forwarded to Secure Access
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0 → No packets forwarded from Secure
#pkts compressed: 0, #pkts decompressed: 0 → Access to your firewall
#pkts not compressed: 71965, #pkts comp failed: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

遇到此情況時，請透過TAC開啟案例。

高可用性功能

安全訪問隧道與雲中的資料中心通訊的功能是主動/被動，這意味著只有DC 1的門才會開啟以接收流量；一直關閉著DC 2的門，直到一號隧道關閉。

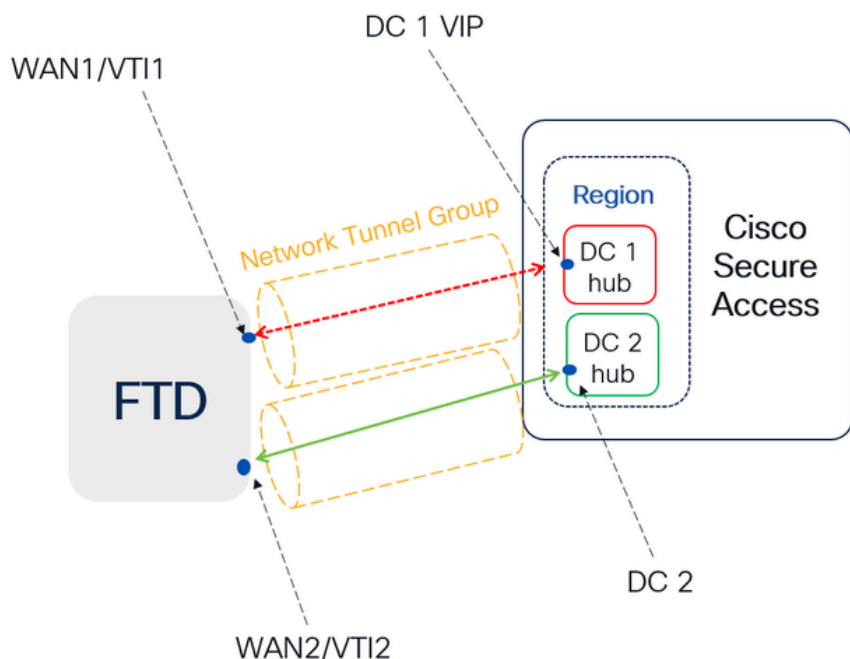
Normal Behavior



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

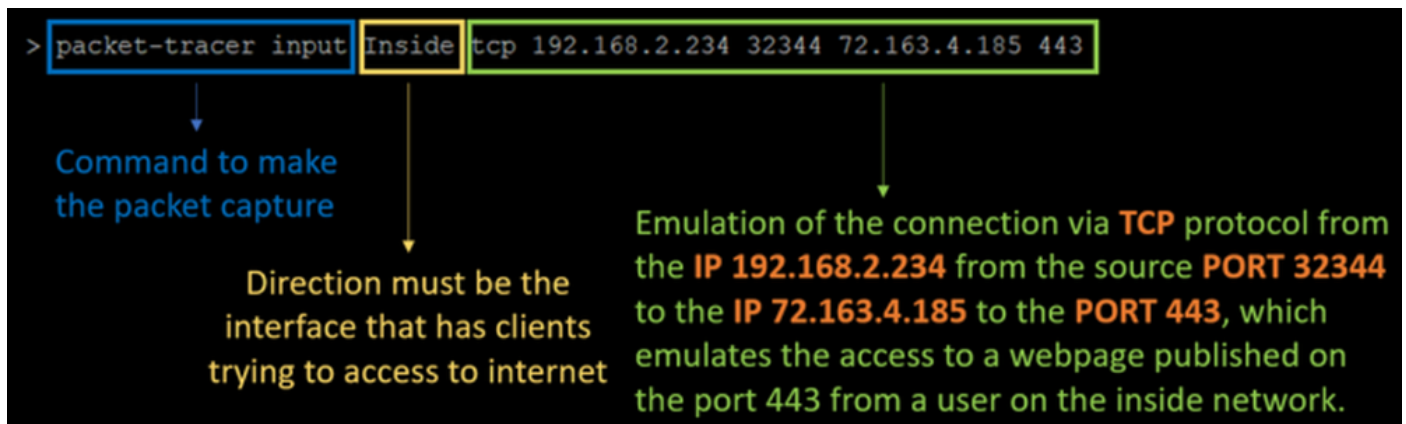
- DC2 is **Active** when DC1 or WAN1 peer is **Down**
- High availability is implemented to address failures in the WAN1 channel on the Firewall, ensuring operational continuity in the **region** and mitigating potential issues in DC1

驗證安全訪問的流量路由

在本例中，我們使用來源作為防火牆網路上的機器：

- 來源：192.168.10.40
- 目標:146.112.255.40 (安全訪問監控IP)

範例：



指令：

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

輸出：

```
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

在這裡，許多因素都可以為我們提供有關通訊的情景，並知道在PBR配置下是否一切都正確，以將流量正確路由到安全訪問：

```
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
```

第2階段表示流量將轉送到介面，這是正確PrimaryVTI的，因為根據此場景中的配置，必須通過VTI將網際網路流量轉送到安全訪問。

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:

連線中的加密階段，在此階段對流量進行評估並授權進行加密，以確保可以安全地傳輸資料。另一方面，第9階段側重於對VPN IPSec隧道內的流量進行特定管理，確認已加密的流量正確路由並允許通過已建立的隧道。

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
```

要最終確定，在流結果的末尾，您可以看到從到將流LAN量轉PrimaryVTI發到安全訪問的流量。該操作allow可確認流量路由沒有問題。

相關資訊

- [思科技術支援與下載](#)
- [Cisco Secure Access幫助中心](#)
- [虛擬可信平台模組概述](#)
- [零信任存取模組](#)
- [對安全訪問錯誤「註冊服務沒有響應」進行故障排除。聯絡您的IT服務檯」](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。