

使用防禦性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](#)

[設定](#)

[在安全訪問上配置VPN](#)

[通道資料](#)

[配置VPN站點到站點防禦工事](#)

[網路](#)

[驗證](#)

[第1階段建議](#)

[第2階段建議](#)

[配置隧道介面](#)

[配置策略路由](#)

[驗證](#)

簡介

本文檔介紹如何使用防禦性防火牆配置安全訪問。

必要條件

- [設定使用者啟動設定](#)
- [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：

- Fortigate 7.4.x版防火牆
- 安全存取
- Cisco安全使用者端- VPN
- 思科安全使用者端- ZTNA
- 無客戶端ZTNA

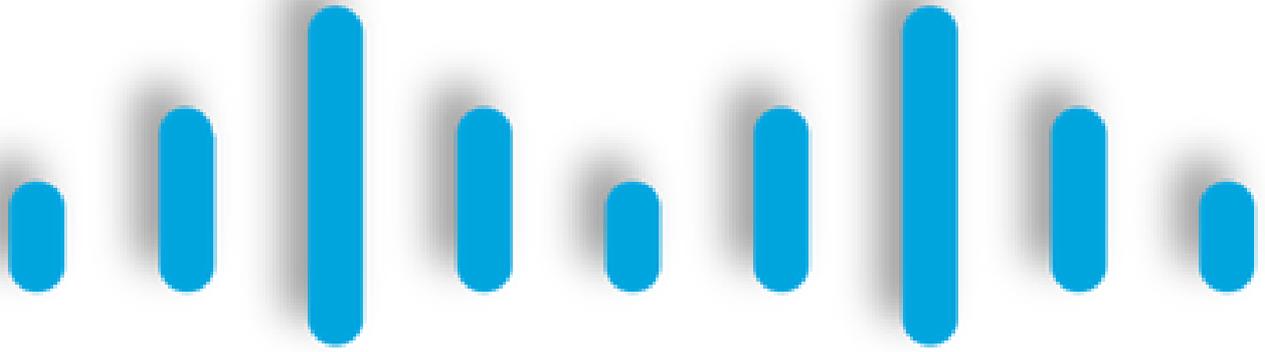
採用元件

本文檔中的資訊基於：

- Fortigate 7.4.x版防火牆
- 安全存取
- 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

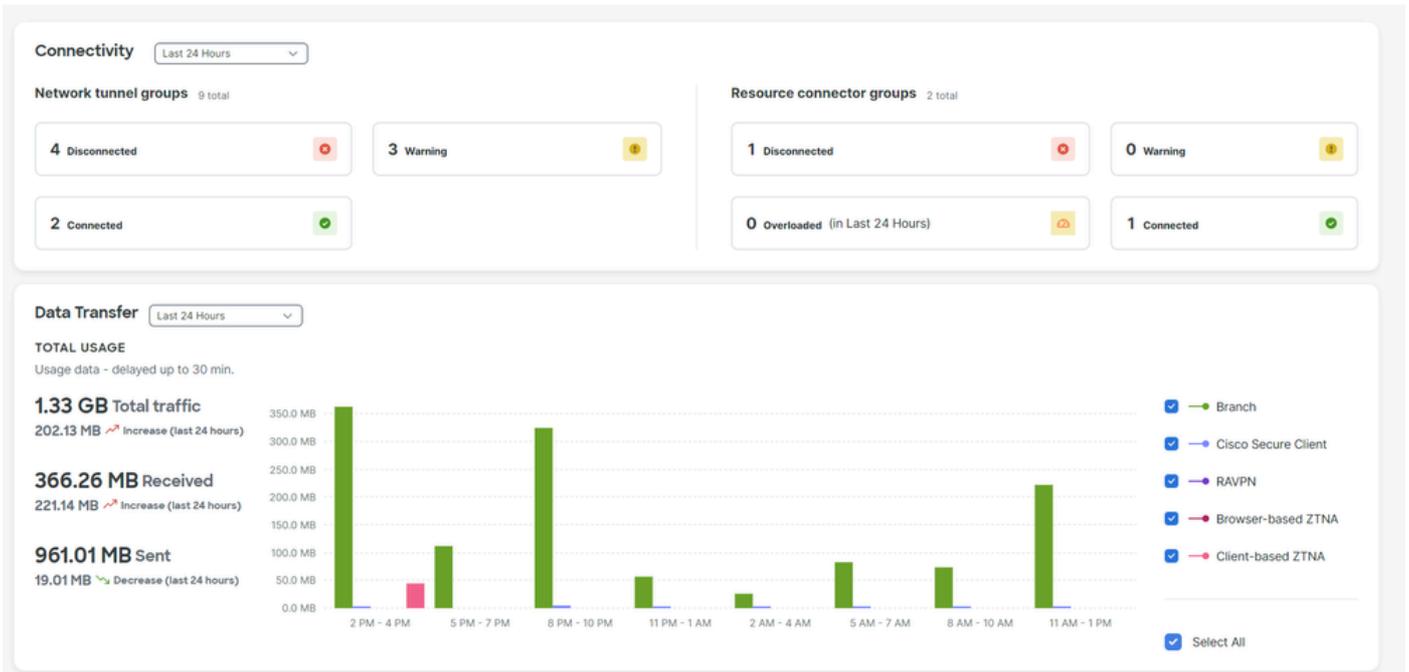
FORTINET®

思科設計了安全訪問，可保護並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。這透過實施多種安全方法和層來實現，所有這些方法都旨在保護透過雲訪問資訊時所需的資訊。

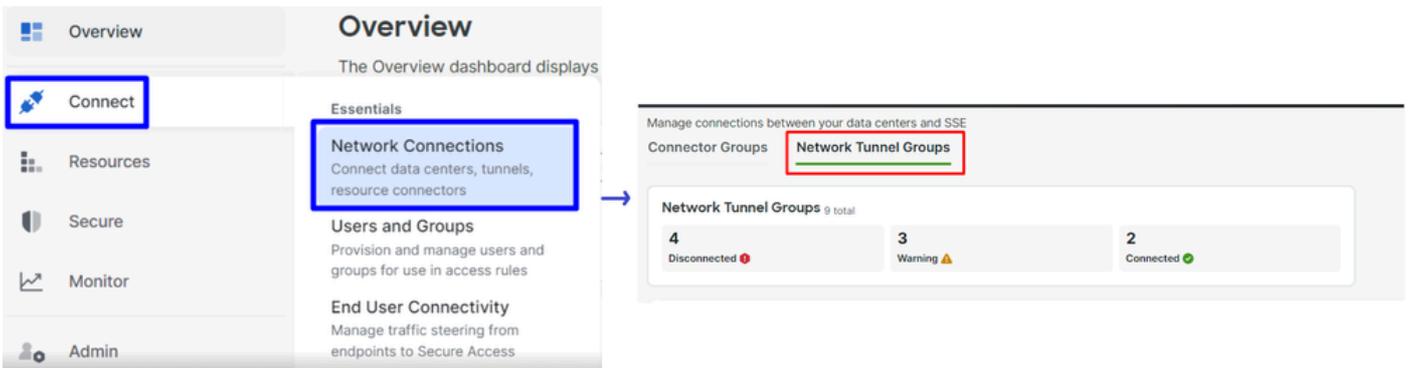
設定

在安全訪問上配置VPN

導航到[安全訪問](#)的管理面板。



- 按一下 [Connect](#) > [Network Connections](#) > [Network Tunnels Groups](#)



- 在Network Tunnel Groups下，按一下 + Add

Network Tunnel Groups

A network tunnel group provides a framework for establishing tunnel redundancy and high availability. Connect tunnels to the hubs within a network tunnel group to securely control user access to the Internet and private resources. [Help](#)

Search Region Status 9 Tunnel Groups

+ Add

- 配置Tunnel Group Name、Region和 Device Type
- 按一下 Next

✓ General Settings

2 Tunnel ID and Passphrase

3 Routing

4 Data for Tunnel Setup



General Settings

Give your network tunnel group a good meaningful name, choose a region through which it will connect to Secure Access, and choose the device type this tunnel group will use.

Tunnel Group Name

Region

Device Type

Cancel

Next



附註：選擇最接近防火牆位置的區域。

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

- ✓ General Settings
- ✓ Tunnel ID and Passphrase
- 3 Routing
- 4 Data for Tunnel Setup

Tunnel ID and Passphrase

Configure the tunnel ID and passphrase that devices will use to connect to this tunnel group.

Tunnel ID Format

Email IP Address

Tunnel ID

fortigate @<org>
<hub>.sse.cisco.com

Passphrase

.....

The passphrase must be between 16 and 64 characters long. It must include at least one upper case letter, one lower case letter, one number, and cannot include any special characters.

Confirm Passphrase

.....



Cancel

Back

Next

- 配置已在網路上配置且希望透過安全訪問傳輸流量的IP地址範圍或主機
- 按一下Save

- ✓ General Settings
- ✓ Tunnel ID and Passphrase
- 3 Routing
- 4 Data for Tunnel Setup

Routing options and network overlaps

Configure routing options for this tunnel group.

Network subnet overlap

Enable NAT / Outbound only

Select if the IP address space of the subnet behind this tunnel group overlaps with other IP address spaces in your network. When selected, private applications behind these tunnels are not accessible.

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

192.168.100.0/24

Dynamic routing

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



Cancel

Back

Save

按一下顯示Save 的隧道資訊後，請儲存該資訊以用於下一步。 **Configure the VPN Site to Site on Fortigate.**

Data for Tunnel Setup

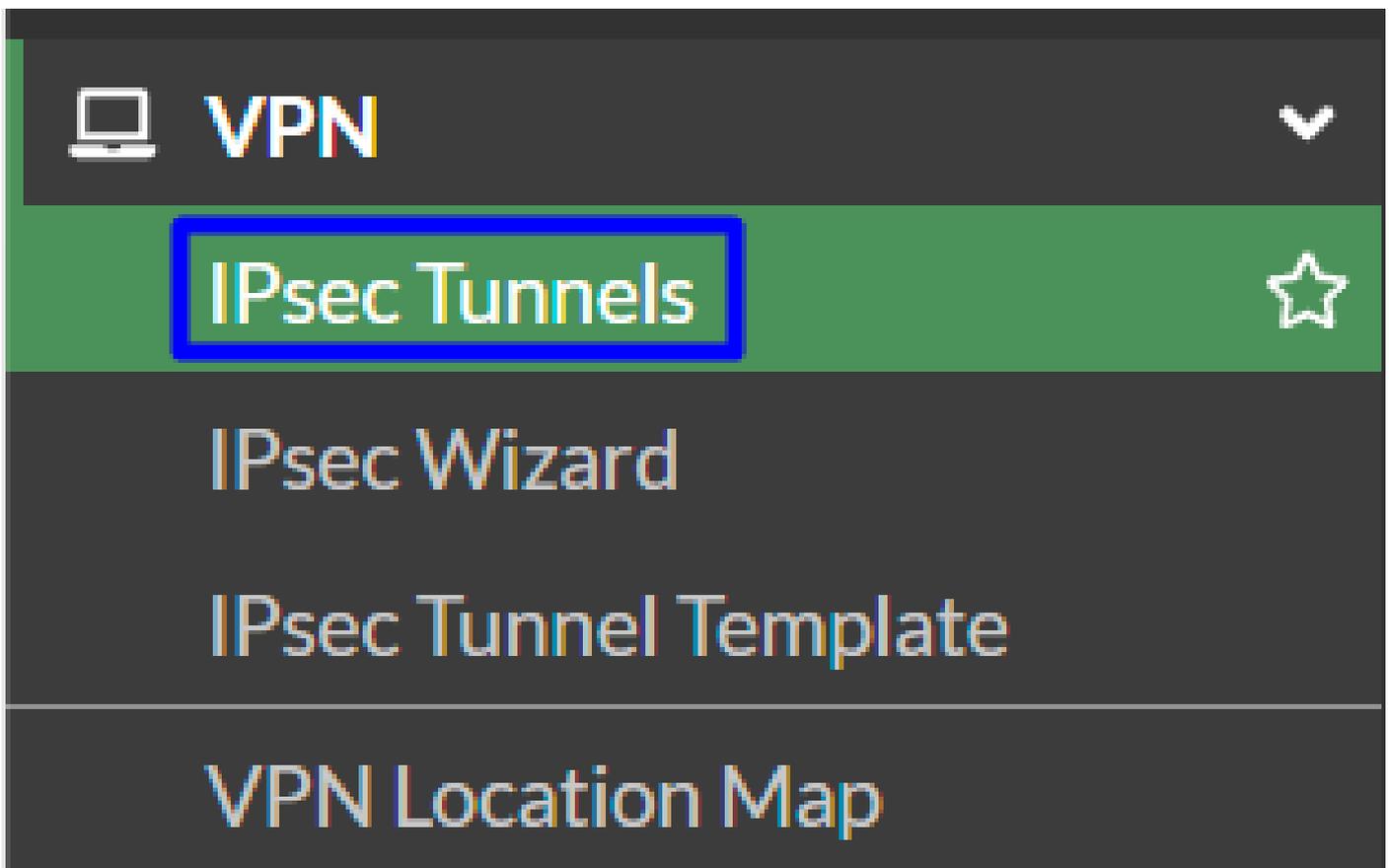
Review and save the following information for use when setting up your network tunnel devices. This is the only time that your passphrase is displayed.

Primary Tunnel ID:	@	-sse.cisco.com	📄
Primary Data Center IP Address:	18.156.145.74		📄
Secondary Tunnel ID:	@	-sse.cisco.com	📄
Secondary Data Center IP Address:	3.120.45.23		📄
Passphrase:		CP	📄

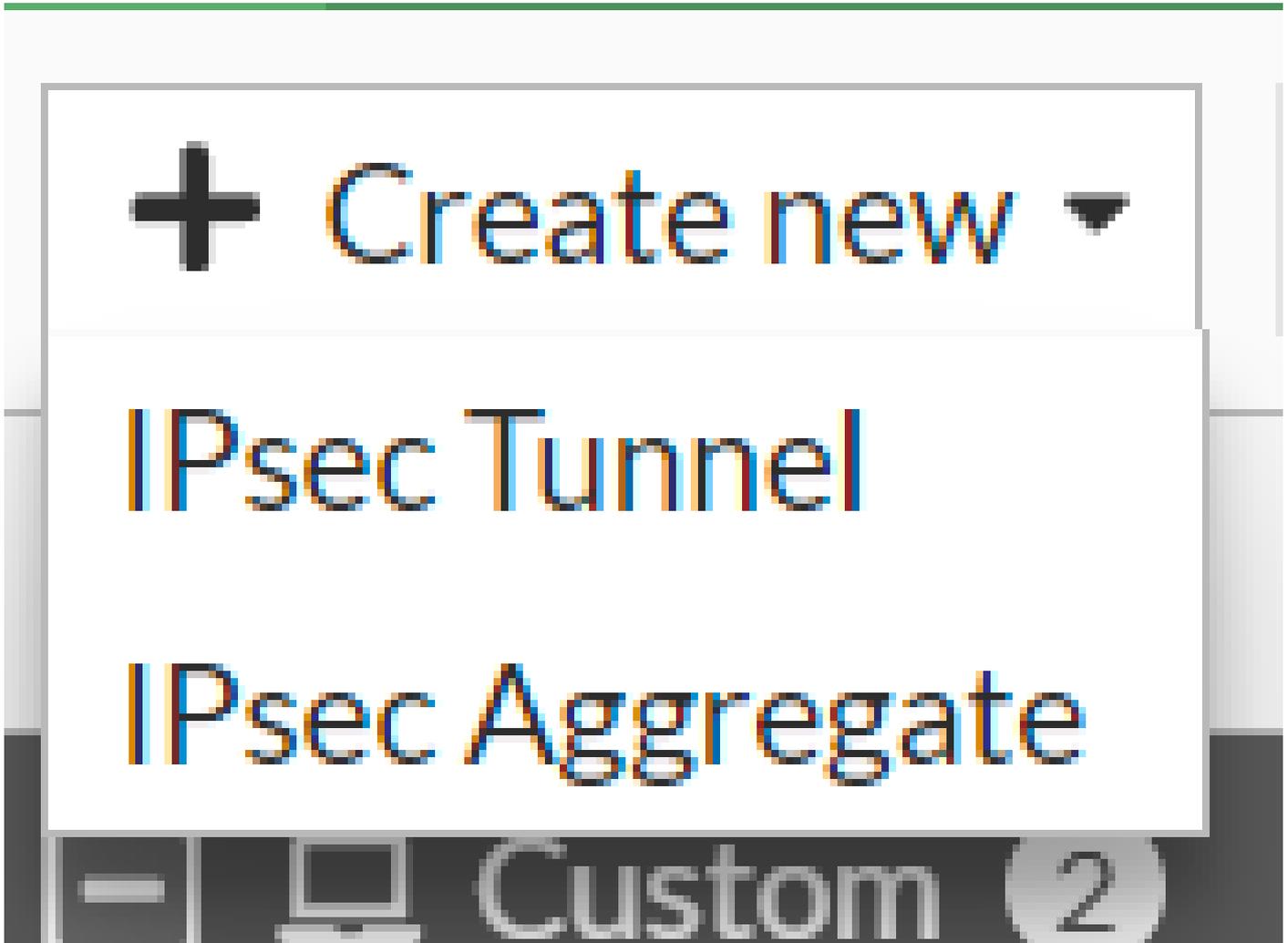
配置VPN站點到站點防禦工事

導航到您的Fortigate控制台。

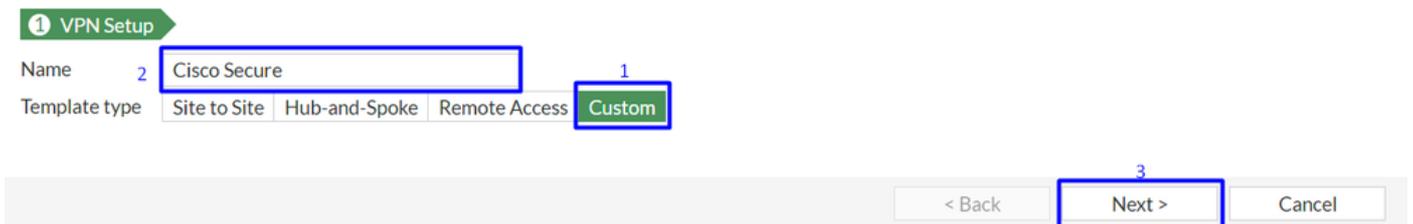
- 按一下 VPN > IPsec Tunnels



- 按一下 Create New > IPsec Tunnels

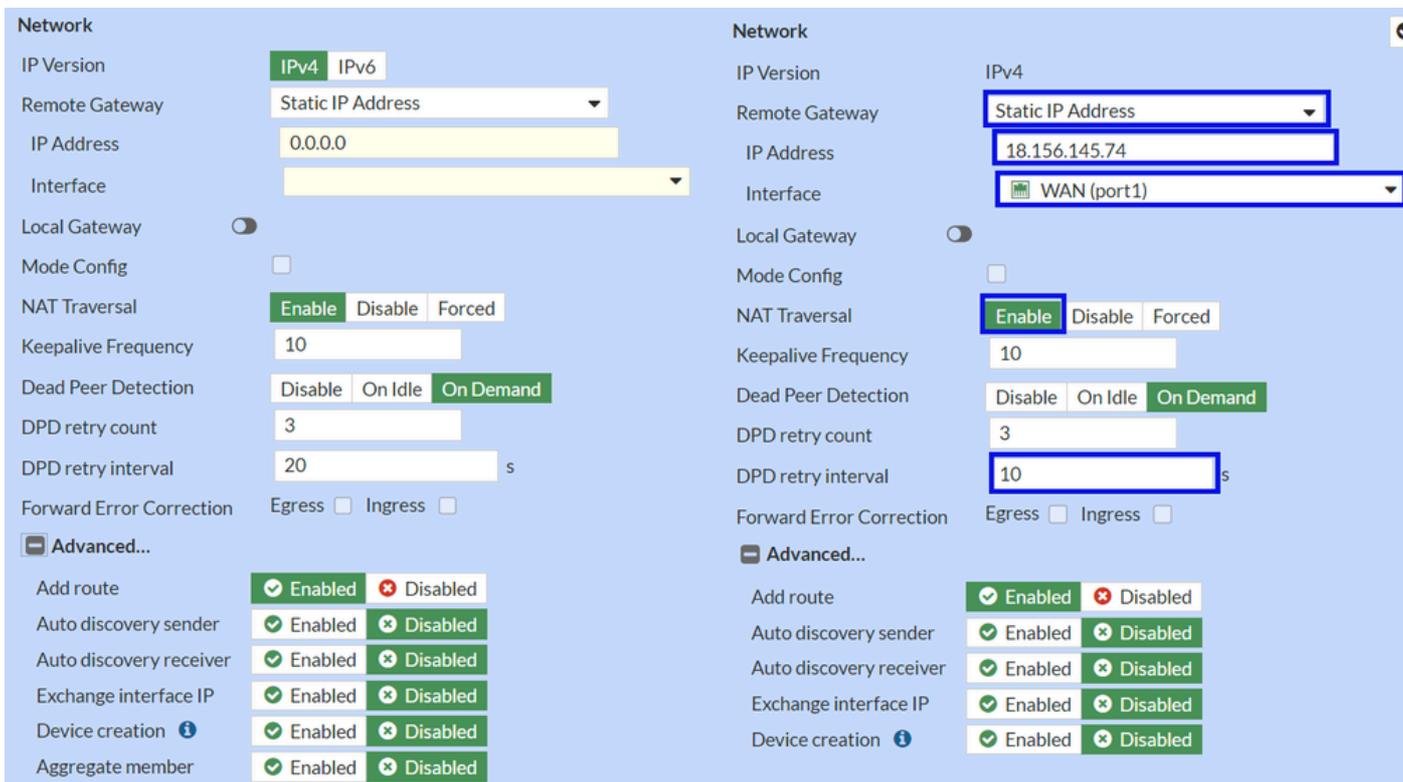


- 按一下 Custom，配置 Name 並按一下 Next。



在下一個影像中，您會看到您需要如何設定零 Network 件的設定。

網路



- Network

- IP Version : IPv4

- **Remote Gateway** : 靜態IP地址
Primary IP Datacenter IP Address,
- **IP Address** : 使用 [隧道資料](#) 步驟中指定的IP
- **Interface** : 選擇您計畫用於建立隧道的WAN介面
- **Local Gateway** : 停用為預設值
- **Mode Config** : 停用為預設值
- **NAT Traversal** : 啟用
- **Keepalive Frequency** :10
- **Dead Peer Detection** : 點播
- **DPD retry count** :3
- **DPD retry interval** :10
- **Forward Error Correction** : 請勿勾選任何方塊。
- **Advanced...** : 將其配置為映像。

現在配置IKE Authentication。

驗證

Authentication		Authentication	
Method	Pre-shared Key	Method	Pre-shared Key
Pre-shared Key		Pre-shared Key	••••••••
IKE		IKE	
Version	1 2	Version	1 2
Mode	Aggressive Main (ID protection)		

- **Authentication**

- **Method** : 預共用金鑰作為預設值

- **Pre-shared Key** : 使用[隧道資料](#)步驟中給出的Passphrase命令

- **IKE**

- **Version** : 選擇版本2。



注意：安全訪問僅支援IKEv2

現在配置 **Phase 1 Proposal**。

第1階段建議

The image displays two screenshots of a Phase 1 Proposal configuration interface. The left screenshot shows a list of four proposals with encryption and authentication settings. The right screenshot shows a detailed view of a proposal with encryption set to AES256, authentication to SHA256, Diffie-Hellman Groups 19 and 20 selected, Key Lifetime set to 86400, and Local ID set to fortigate@8195126-621099508-sse.ci.

- Phase 1 Proposal

- Encryption : 選擇AES256

- Authentication : 選擇SHA256
- Diffie-Hellman Groups : 選中框19和20
- Key Lifetime (seconds) : 86400為預設值
- Local ID : 使用[Tunnel Data](#)步驟中提供的 Primary Tunnel ID

現在配置 **Phase 2 Proposal**。

第2階段建議

New Phase 2

Name: CSA

Comments: Comments

Local Address: addr_subnet 0.0.0.0/0.0.0.0

Remote Address: addr_subnet 0.0.0.0/0.0.0.0

Advanced...

Phase 2 Proposal **Add**

Encryption	AES128	Authentication	SHA1	X
Encryption	AES256	Authentication	SHA1	X
Encryption	AES128	Authentication	SHA256	X
Encryption	AES256	Authentication	SHA256	X
Encryption	AES128GCM			X
Encryption	AES256GCM			X
Encryption	CHACHA20POLY1305			X

Enable Replay Detection

Enable Perfect Forward Secrecy (PFS)

Diffie-Hellman Group: 32 31 30 29 28 27 21 20 19 18 17 16 15 14 5 2 1

Local Port: All

Remote Port: All

Protocol: All

Auto-negotiate:

Autokey Keep Alive:

Key Lifetime: Seconds 43200

New Phase 2

Name: CSA

Comments: Comments

Local Address: addr_subnet 0.0.0.0/0.0.0.0

Remote Address: addr_subnet 0.0.0.0/0.0.0.0

Advanced...

Phase 2 Proposal **Add**

Encryption: AES128 Authentication: SHA256

Enable Replay Detection

Enable Perfect Forward Secrecy (PFS)

Local Port: All

Remote Port: All

Protocol: All

Auto-negotiate:

Autokey Keep Alive:

Key Lifetime: Seconds 43200

- New Phase 2
 - **Name** : 預設為 (取自您的VPN名稱)
 - **Local Address** : 設為預設值(0.0.0.0/0.0.0.0)
 - **Remote Address** : 設為預設值(0.0.0.0/0.0.0.0)

- Advanced
 - **Encryption** : 選擇AES128
 - **Authentication** : 選擇SHA256
 - **Enable Replay Detection** : 設為預設值 (啟用)
 - **Enable Perfect Forward Secrecy (PFS)** : 取消選中釐取方塊
 - **Local**

Port : 設為預設值 (啟用)

- **Remote Port** : 設為預設值 (啟用)
- **Protocol** : 設為預設值 (啟用)
- **Auto-negotiate** : 設為預設值 (未標籤)
- **Autokey Keep Alive** : 設為預設值 (未標籤)
- **Key Lifetime** : 設為預設值 (秒)
- **Seconds** : 設為預設值(43200)

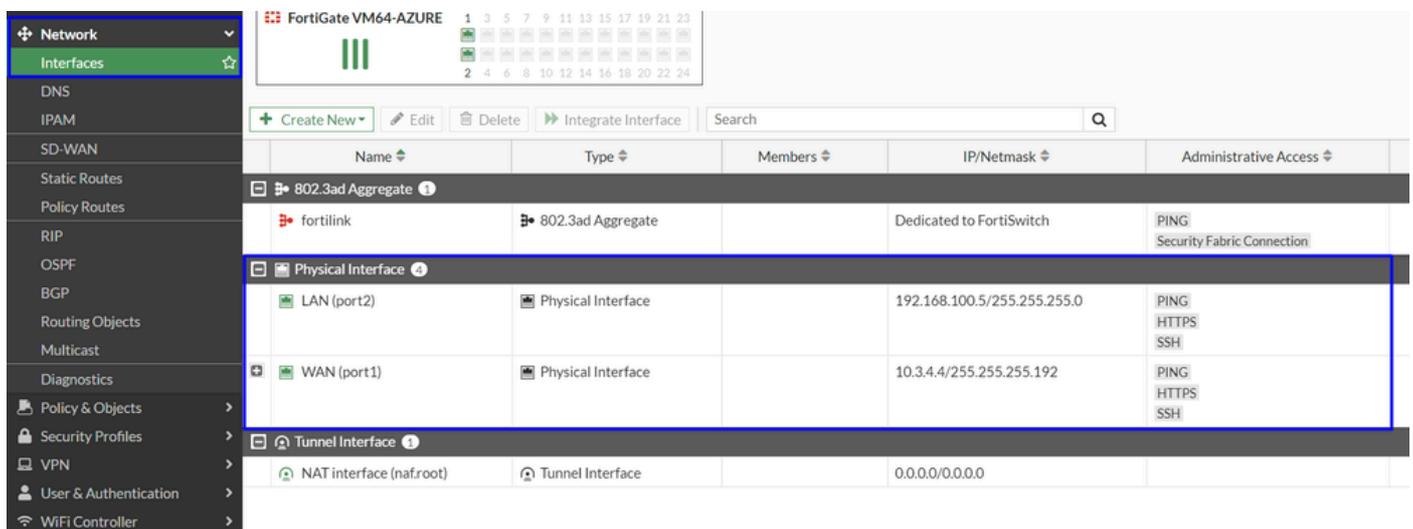
之後，按一下「確定」。幾分鐘後您會看到VPN已使用安全訪問建立，您可以繼續下一步，**Configure the Tunnel Interface**。



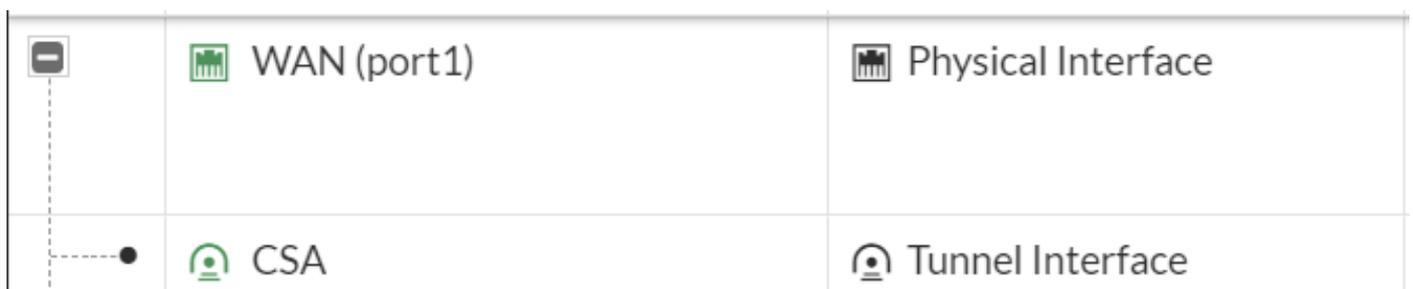
配置隧道介面

隧道建立後，您會注意到您正在用作與Secure Access通訊的WAN介面的埠後面有一個新介面。

要檢查這一點，請導航到 **Network > Interfaces**。



展開您用於與Secure Access進行通訊的埠；在本例中為WAN 介面。



- 按一下您的Tunnel Interface 並按一下 Edit

+ Create New ▾		Edit	🗑 Delete	▶ Integrate Interface	Search
Name ↕		Type ↕			
802.3ad Aggregate 1					
fortilink		802.3ad Aggregate			
Physical Interface 4					
LAN (port2)		Physical Interface			
WAN (port1)		Physical Interface			
CSA		Tunnel Interface			

- 您需要配置下一個映像

Name [CSA](#)

Alias

Type [Tunnel Interface](#)

Interface [WAN \(port1\)](#)

VRF ID ⓘ

Role ⓘ

Name [CSA](#)

Alias

Type [Tunnel Interface](#)

Interface [WAN \(port1\)](#)

VRF ID ⓘ

Role ⓘ

Address

Addressing mode Manual

IP

Netmask 255.255.255.255

Remote IP/Netmask

Address

Addressing mode Manual

IP

Netmask 255.255.255.255

Remote IP/Netmask

- Interface Configuration
- IP : 配置網路中沒有的可路由IP (169.254.0.1)
- Remote IP/Netmask : 將遠端IP配置為介面IP的下一個IP，網路掩碼為30 (169.254.0.2 255.255.255.252)

之後，按一下**OK** 儲存配置，然後繼續執行下一步Configure Policy Route (Origin-based routing)。

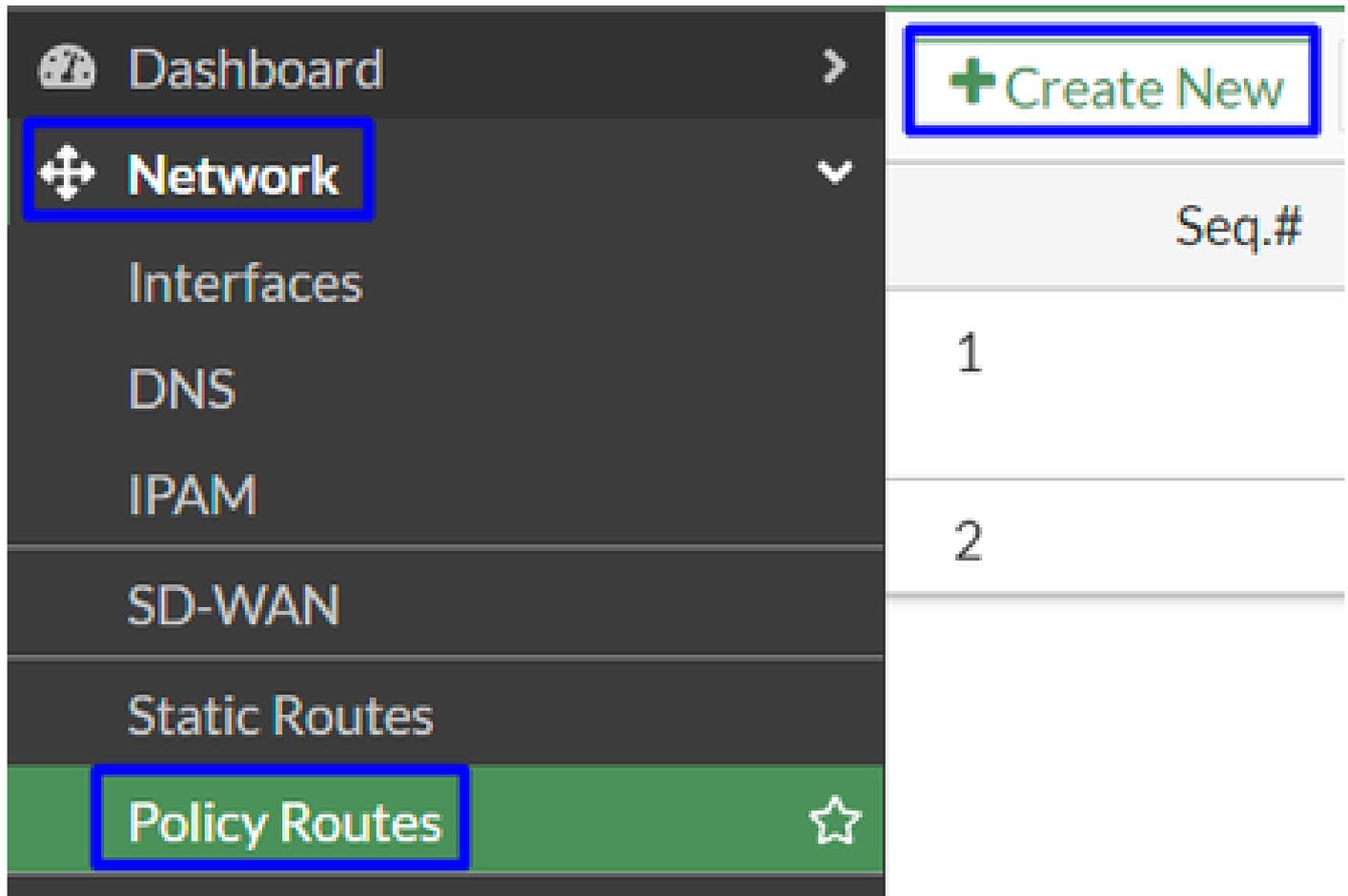


警告：完成此部分後，必須在FortiGate上配置防火牆策略，以允許或允許來自裝置的資料流進行安全訪問，以及來自安全訪問的資料流訪問要路由資料流的網路。

配置策略路由

此時，您的VPN已配置為安全訪問；現在，您必須將流量重新路由到安全訪問，以保護您的流量或對FortiGate防火牆後方的專用應用的訪問。

- 導覽至 Network > Policy Routes



The screenshot shows the FortiGate web interface. On the left is a dark navigation menu with the following items: Dashboard, Network (highlighted with a blue box), Interfaces, DNS, IPAM, SD-WAN, Static Routes, and Policy Routes (highlighted with a blue box and a star icon). On the right, a table is visible with a header 'Seq.#' and two rows containing the numbers '1' and '2'. Above the table, a green button with a plus sign and the text '+ Create New' is highlighted with a blue box.

- 配置策略

If incoming traffic matches:	If incoming traffic matches:
Incoming interface <input type="text" value=""/>	Incoming interface <input type="text" value="LAN (port2)"/>
Source Address	Source Address
IP/Netmask <input type="text" value=""/>	IP/Netmask <input type="text" value="192.168.100.0/255.255.255.0"/>
Addresses <input type="text" value=""/>	Addresses <input type="text" value=""/>
Destination Address	Destination Address
IP/Netmask <input type="text" value=""/>	IP/Netmask <input type="text" value=""/>
Addresses <input type="text" value=""/>	Addresses <input type="text" value="all"/>
Internet service <input type="text" value=""/>	Internet service <input type="text" value=""/>
Protocol <input type="text" value="TCP"/> <input type="text" value="UDP"/> <input type="text" value="SCTP"/> <input checked="" type="text" value="ANY"/> <input type="text" value="Specify"/>	Protocol <input type="text" value="TCP"/> <input type="text" value="UDP"/> <input type="text" value="SCTP"/> <input checked="" type="text" value="ANY"/> <input type="text" value="Specify"/>
Type of service <input type="text" value="0"/>	Type of service <input type="text" value="0"/>
<input type="text" value="0x00"/> Bit Mask <input type="text" value="0x00"/>	<input type="text" value="0x00"/> Bit Mask <input type="text" value="0x00"/>
Then:	Then:
Action <input checked="" type="text" value="Forward Traffic"/> <input type="text" value="Stop Policy Routing"/>	Action <input checked="" type="text" value="Forward Traffic"/> <input type="text" value="Stop Policy Routing"/>
Outgoing interface <input checked="" type="radio"/> <input type="radio"/> <input type="text" value="CSA"/>	Outgoing interface <input checked="" type="radio"/> <input type="radio"/> <input type="text" value="CSA"/>
Gateway address <input type="text" value=""/>	Gateway address <input type="text" value="169.254.0.2"/>
Comments <input type="text" value="Write a comment..."/>	Comments <input type="text" value="Write a comment..."/>
Status <input checked="" type="text" value="Enabled"/> <input type="text" value="Disabled"/>	Status <input checked="" type="text" value="Enabled"/> <input type="text" value="Disabled"/>

- If Incoming traffic matches

- Incoming Interface : 選擇您計畫從哪個介面將流量重新路由到安全訪問 (流量的源)

- Source Address

- IP/Netmask : 如果僅路由介面的子網，則使用此選項
- Addresses : 如果建立了對象，並且流量源來自多個介面和多個子網，則使用此選項

- Destination Addresses

- Addresses:選擇 all

- Protocol:選擇 ANY

- Then
 - Action : **Choose Forward Traffic**

- Outgoing Interface : 選擇在步驟[配置隧道介面](#)中修改的隧道介面
- Gateway Address : 配置在步驟[RemoteIPetmask](#)中配置的遠端IP
- Status : 選擇「啟用」

點選OK 儲存配置，您現在即可驗證您的裝置流量是否已重新路由到安全訪問。

驗證

為了驗證電腦的流量是否被重新路由到安全訪問，您有兩個選項：可以在網際網路上檢查並檢查公共IP，或者使用curl運行下一個命令：

```
<#root>
```

```
C:\Windows\system32>curl ipinfo.io { "ip": "151.186.197.1", "city": "Frankfurt am Main", "region": "Hes
```

您可以檢視流量的公共範圍是：

```
Min Host:151.186.176.1
```

```
Max Host :151.186.207.254
```



注意：這些IP可能會發生變化，這意味著思科將來可能會擴大此範圍。

如果您看到您的公共IP發生更改，這意味著您受到安全訪問的保護，現在您可以在安全訪問控制台上配置您的專用應用，以便從VPNaaS或ZTNA訪問您的應用。

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）。