

Configurare l'accesso sicuro con il firewall Fortigate

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Configurare la VPN su accesso sicuro](#)

[Dati tunnel](#)

[Configurare il sito VPN su sito in Fortigate](#)

[Rete](#)

[Autenticazione](#)

[Proposta fase 1](#)

[Proposta fase 2](#)

[Configurazione dell'interfaccia del tunnel](#)

[Configura route criteri](#)

[Verifica](#)

Introduzione

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

Prerequisiti

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

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Firewall versione 7.4.x avanzata
- Accesso sicuro
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA
- ZTNA senza client

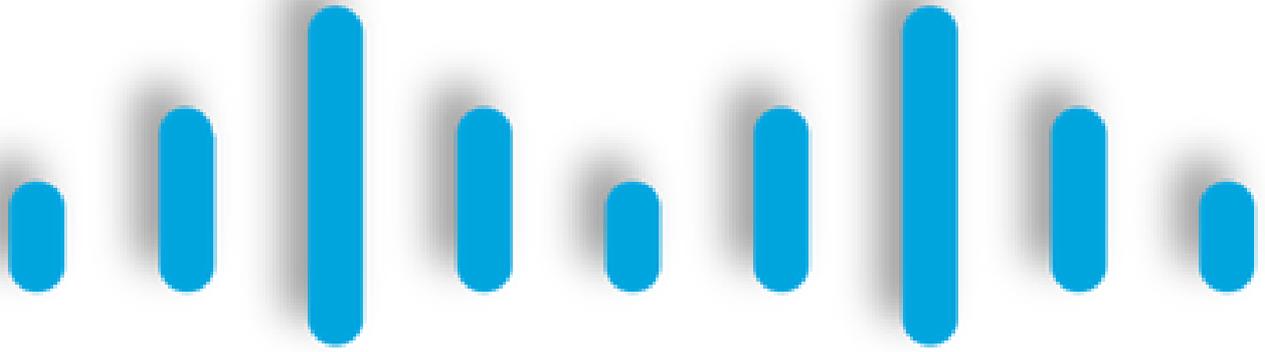
Componenti usati

Le informazioni fornite in questo documento si basano su:

- Firewall versione 7.4.x avanzata
- 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

Secure

Access

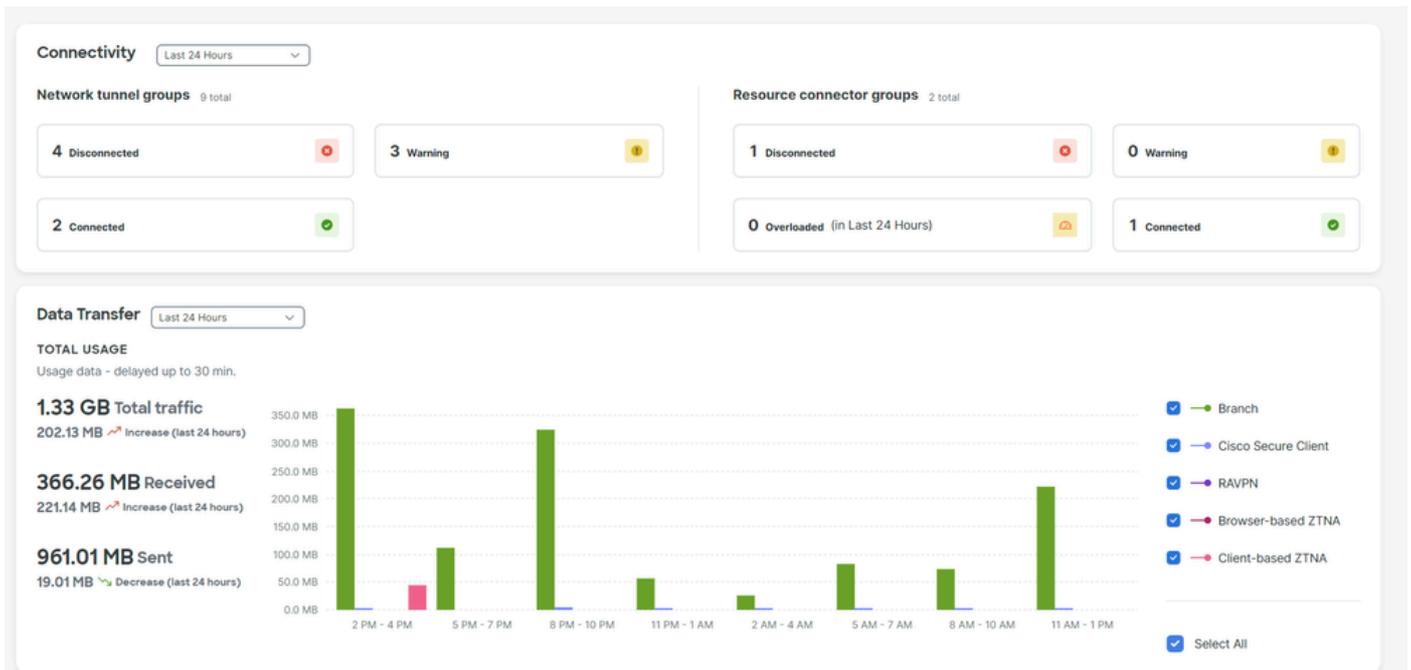
FORTINET®

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.

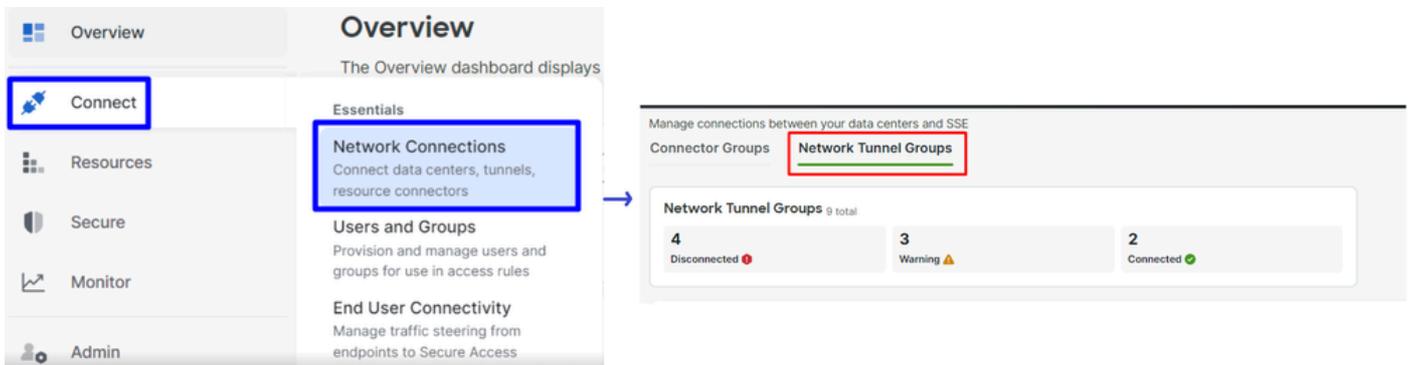
Configurazione

Configurare la VPN su accesso sicuro

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



- Fare clic su **Connect** > **Network Connections** > **Network Tunnel Groups**



- In fare Network Tunnel Groups clic su **+ 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 security control user access to the Internet and private resources. [Help](#)

Q Search Region Status 9 Tunnel Groups



- Configurazione Tunnel Group Name, Regione Device Type
- Fare clic su **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



Nota: scegliere la regione più vicina alla posizione del firewall.

-
- Configurare Tunnel ID Formate Passphrase
 - Fare clic su 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

- 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**

- 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

Dopo aver fatto clic sulle informazioni **Save** del tunnel che vengono visualizzate, salvare le informazioni per il passaggio successivo, **Configure the VPN Site to Site on Fortigate**.

Dati tunnel

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		

Configurare il sito VPN su sito in Fortigate

Passare al pannello di controllo Fortigate.

- Fare clic su VPN > IPsec Tunnels



VPN



IPsec Tunnels

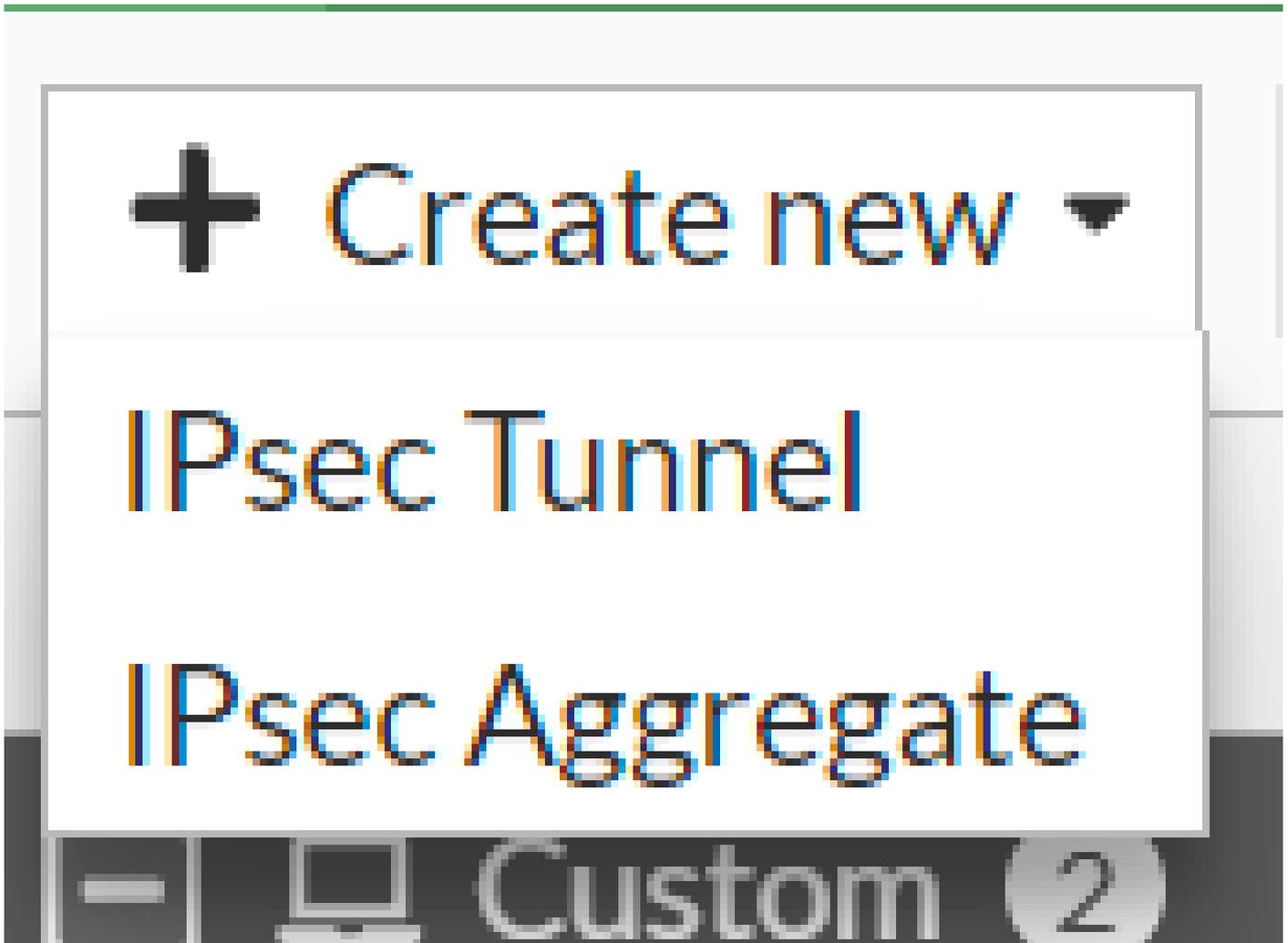


IPsec Wizard

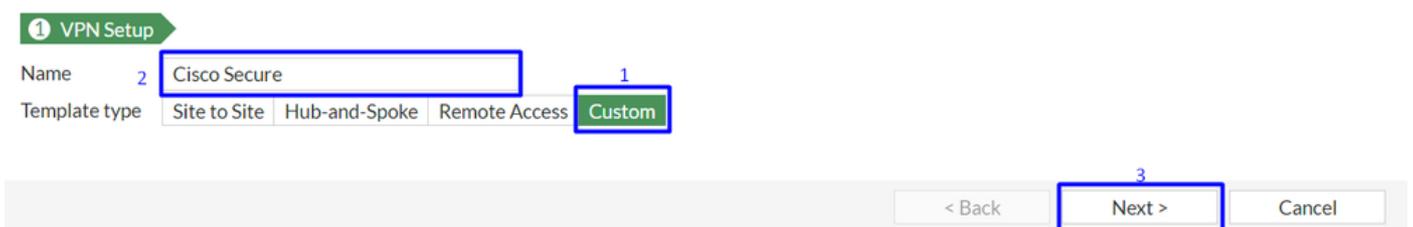
IPsec Tunnel Template

VPN Location Map

- Fare clic su [Create New > IPsec Tunnels](#)

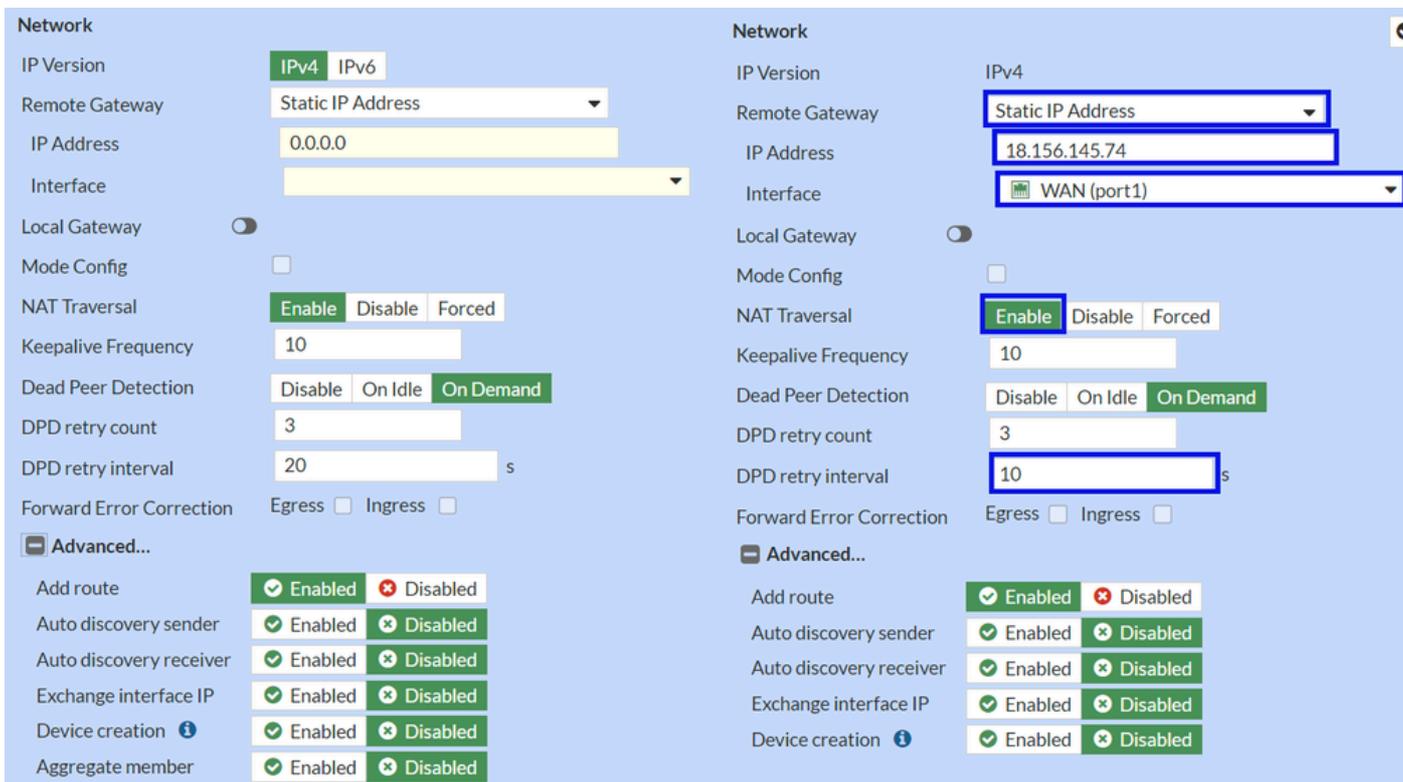


- Fare clic su Custom , configurare una **Name** e fare clic su **Next**.



Nell'immagine seguente viene illustrato come configurare le impostazioni per la **Network** parte.

Rete



- Network

- IP Version :IPv4

- **Remote Gateway** :Indirizzo IP statico
- IP Address: utilizzare l'IP di Primary IP Datacenter IP Address,specificato nella fase [Dati tunnel](#)
- **Interface** : selezionare l'interfaccia WAN che si desidera utilizzare per stabilire il tunnel
- **Local Gateway** : disabilita come impostazione predefinita
- **Mode Config** : disabilita come impostazione predefinita
- **NAT Traversal** : Abilita
- **Keepalive Frequency** :10
- Dead Peer Detection : su richiesta
- **DPD retry count** :3
- **DPD retry interval** :10
- **Forward Error Correction** : non selezionare alcuna casella.
- **Advanced...:** configurarla come immagine.

A questo punto configurare la **Authentication** porta IKE.

Autenticazione

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** : chiave già condivisa come predefinita

- **Pre-shared Key** : utilizzare i dati **Passphrase** forniti nella fase [Tunnel Data](#)

- **IKE**

- **Version** : scegliere la versione 2.



Nota: Secure Access supporta solo IKEv2

A questo punto configurare il **Phase 1 Proposal**router.

Proposta fase 1

The image shows two screenshots of a configuration interface for Phase 1 Proposal. 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 specific settings highlighted by blue boxes.

Left Screenshot:

- Phase 1 Proposal **+ Add**
- Encryption: AES128, Authentication: SHA256, [X]
- Encryption: AES256, Authentication: SHA256, [X]
- Encryption: AES128, Authentication: SHA1, [X]
- Encryption: AES256, Authentication: SHA1, [X]
- Diffie-Hellman Groups: 32 31 30 29 28 27 21 20 19 18 17 16 15 14 5 2 1
- Key Lifetime (seconds): 86400
- Local ID: [Empty]

Right Screenshot:

- Phase 1 Proposal **+ Add** [Checkmark] [Refresh]
- Encryption: **AES256**, Authentication: **SHA256**
- Diffie-Hellman Groups: 32 31 30 29 28 27 21 20 19 18 17 16 15 14 5 2 1
- Key Lifetime (seconds): 86400
- Local ID: **fortigate@8195126-621099508-sse.ci**

- Phase 1 Proposal

- Encryption : scegliere AES256

- Authentication : scelta di SHA256
- Diffie-Hellman Groups : selezionare le caselle 19 e 20
- Key Lifetime (seconds) : 86400 come valore predefinito
- Local ID : utilizzare Primary Tunnel ID, come indicato nella fase [Dati tunnel](#)

A questo punto configurare il **Phase 2 Proposal**router.

Proposta fase 2

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

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

Seconds: 43200

- New Phase 2
 - **Name** : Impostazione predefinita (tratto dal nome della VPN)
 - **Local Address** : impostazione predefinita (0.0.0.0/0.0.0.0)
 - **Remote Address** : impostazione predefinita (0.0.0.0/0.0.0.0)

- Advanced
 - **Encryption** : scegliere AES128
 - **Authentication** : scelta di SHA256
 - **Enable Replay Detection** : Consenti come predefinito (Attivato)
 - **Enable Perfect Forward Secrecy (PFS)** : Deselezionare la casella di controllo
 - **Local Port** : Consenti come predefinito (Attivato)

- **Remote Port**: Consenti come predefinito (Attivato)
- **Protocol** : Consenti come predefinito (Attivato)
- **Auto-negotiate** : impostato come predefinito (non contrassegnato)
- **Autokey Keep Alive** : impostato come predefinito (non contrassegnato)
- **Key Lifetime** : Impostazione predefinita (secondi)
- **Seconds** : impostato come predefinito (43200)

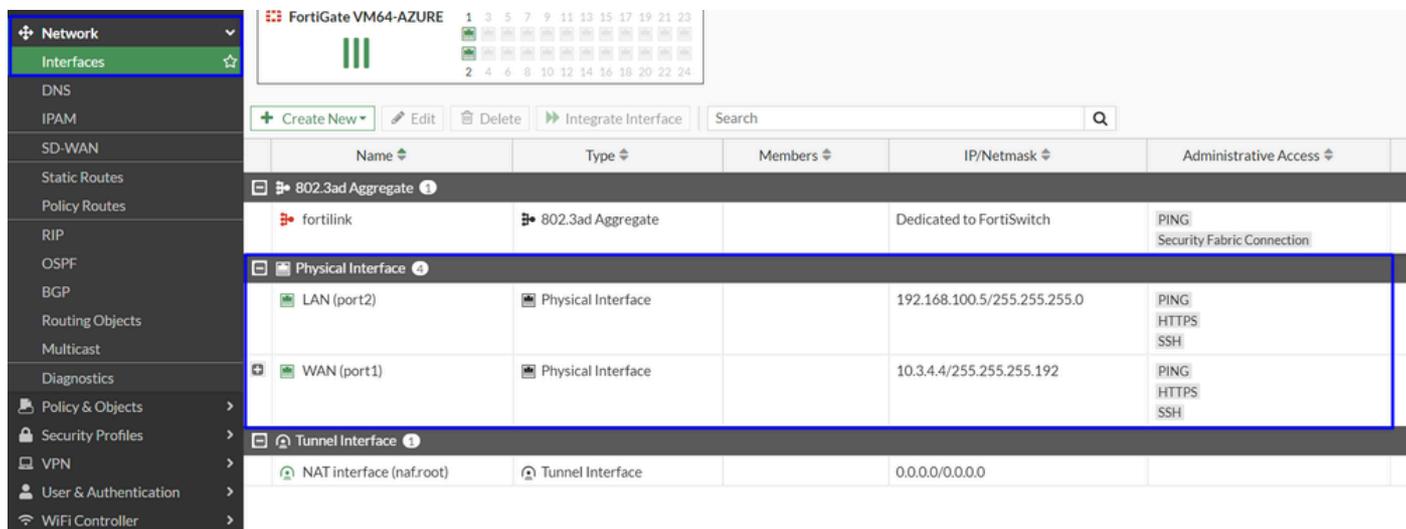
Quindi fare clic su OK. Dopo alcuni minuti la VPN è stata stabilita con Accesso sicuro ed è possibile continuare con il passaggio successivo, **Configure the Tunnel Interface**.



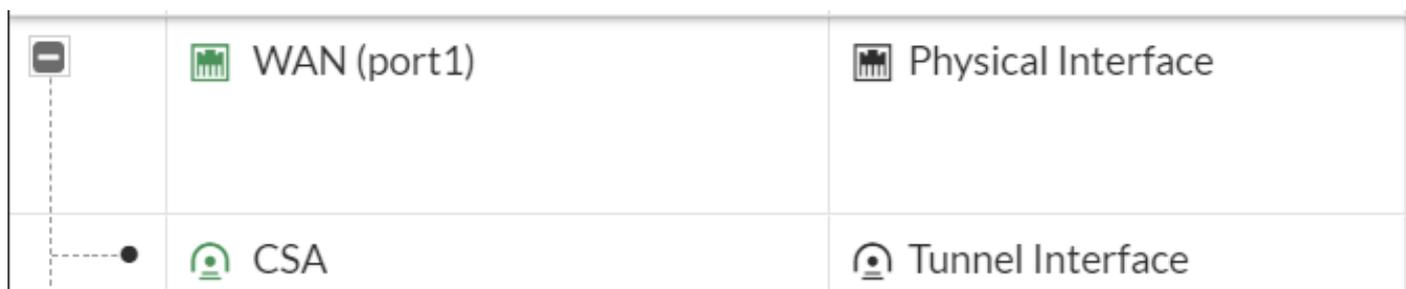
Configurazione dell'interfaccia del tunnel

Dopo aver creato il tunnel, si nota che esiste una nuova interfaccia dietro la porta che si sta utilizzando come interfaccia WAN per comunicare con Secure Access.

Per verificare questa condizione, passare alla **Network > Interfacesezione**.



Espandere la porta utilizzata per comunicare con Secure Access; in questo caso, l'**WAN** interfaccia.



- Fare clic su **Tunnel Interface** e selezionare **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

- È necessario configurare l'immagine successiva

Name CSA
 Alias
 Type Tunnel Interface
 Interface WAN (port1)
 VRF ID 0
 Role Undefined

Name CSA
 Alias
 Type Tunnel Interface
 Interface WAN (port1)
 VRF ID 0
 Role Undefined

Address

Addressing mode Manual

IP

Netmask 255.255.255.255

Remote IP/Netmask

Address

Addressing mode Manual

IP

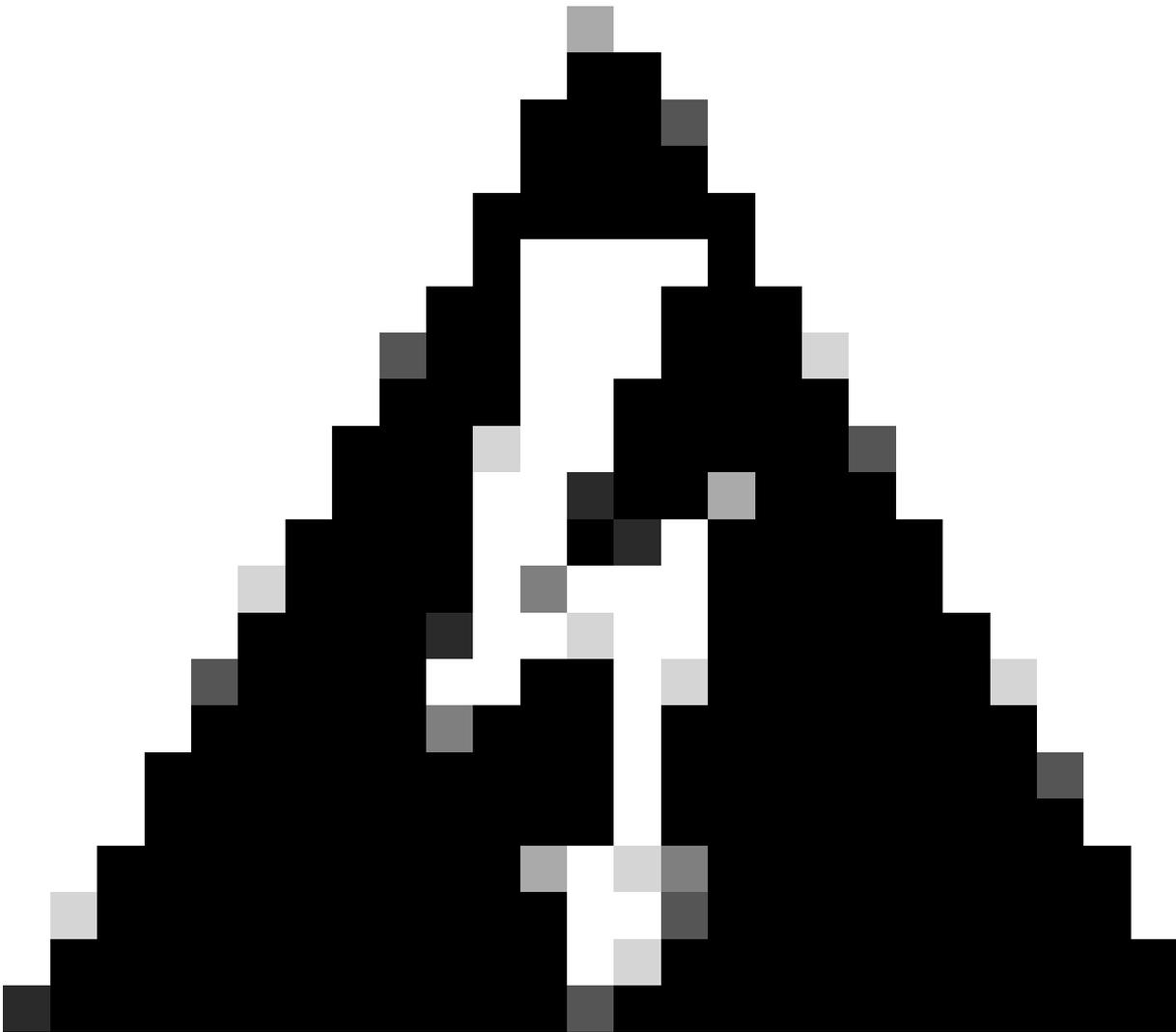
Netmask 255.255.255.255

Remote IP/Netmask

- Interface Configuration

- IP : configurare un indirizzo IP non instradabile non presente nella rete (169.254.0.1)
- Remote IP/Netmask : configurare l'indirizzo IP remoto come indirizzo IP successivo dell'interfaccia IP e con una maschera di rete di 30 (169.254.0.2 255.255.255.252)

Quindi, fare clic su **OK** per salvare la configurazione e procedere con il passaggio successivo, Configure Policy Route (routing basato sull'origine).



Avviso: dopo questa parte, è necessario configurare i criteri firewall sul FortiGate per autorizzare o consentire il traffico proveniente dal dispositivo verso l'accesso sicuro e da Accesso sicuro alle reti alle quali si desidera indirizzare il traffico.

Configura route criteri

A questo punto, la VPN è configurata e stabilita per l'accesso sicuro; ora, è necessario indirizzare nuovamente il traffico ad accesso sicuro per proteggere il traffico o l'accesso alle applicazioni private dietro il firewall FortiGate.

- Passa a Network > Policy Routes

The screenshot shows the FortiGate web interface. On the left, a dark sidebar menu contains 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 green background). On the right, a light-colored panel displays a '+ Create New' button (highlighted with a blue box) and a table with a single column labeled 'Seq.#'. The table contains two rows with the values '1' and '2'.

Seq.#
1
2

- Configurare il criterio

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	TCP UDP SCTP ANY Specify	Protocol	TCP UDP SCTP ANY Specify
Type of service	0	Type of service	0
	0x00 Bit Mask 0x00		0x00 Bit Mask 0x00
Then:		Then:	
Action	Forward Traffic Stop Policy Routing	Action	Forward Traffic Stop Policy Routing
Outgoing interface	<input checked="" type="radio"/> CSA	Outgoing interface	<input checked="" type="radio"/> 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	Enabled Disabled	Status	Enabled Disabled

- If Incoming traffic matches
 - Incoming Interface : scegliere l'interfaccia da cui si desidera instradare nuovamente il traffico per l'accesso sicuro (origine del traffico)

- Source Address
 - IP/Netmask : utilizzare questa opzione se si instrada solo una subnet di un'interfaccia
 - Addresses : utilizzare questa opzione se l'oggetto è stato creato e l'origine del traffico proviene da più interfacce e subnet

- Destination Addresses

- Addresses: Scegli all
- Protocol: Scegli **ANY**
- Then
 - Action: **Choose Forward Traffic**
 - Outgoing Interface : scegliere l'interfaccia tunnel modificata nel passo [Configura interfaccia tunnel](#).
 - Gateway Address: configurare l'indirizzo IP remoto configurato nella fase, [RemoteIPNetmask](#)
 - Status : Scegli abilitato

Fare clic **OK** per salvare la configurazione. È ora possibile verificare se il traffico dei dispositivi è stato reindirizzato ad Accesso sicuro.

Verifica

Per verificare se il traffico del computer è stato reindirizzato ad Accesso sicuro, sono disponibili due opzioni: è possibile controllare su Internet e verificare la presenza dell'IP pubblico oppure eseguire il comando successivo con curl:

<#root>

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

L'intervallo pubblico da cui puoi vedere il traffico è:

Min Host:151.186.176.1

Max Host :151.186.207.254



Nota: questi IP sono soggetti a modifiche, il che significa che Cisco probabilmente estenderà questo intervallo in futuro.

Se viene visualizzata la modifica dell'IP pubblico, ovvero se si è protetti da Accesso sicuro, è ora possibile configurare l'applicazione privata nel dashboard di Accesso sicuro per accedere alle applicazioni da VPNaaS o ZTNA.

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).