

ةيامح رادج مادختساب نمآلا لوصولا نيوكت Fortigate

تايوتحمل

[ةمدقملا](#)

[ةيساسآلا تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[ةيساسآا تامولعم](#)

[نيوكتلا](#)

[نمآلا لوصولا على VPN ةكبش نيوكت](#)

[قفنلا تانايب](#)

[Fortigate على عقوم لىلا VPN عقوم نيوكت](#)

[ةكبشلا](#)

[ةقداصملا](#)

[ىلوالا قلملا جارتقا](#)

[ةينانثلا قلملا جارتقا](#)

[قفنلا ةهجاو نيوكت](#)

[ةسايسللا راسم نيوكت](#)

[ةحصللا نم ققحتلا](#)

ةمدقملا

Fortigate ةيامح رادج مادختساب نمآلا لوصولا نيوكت ةيفيك دننتملا اذه حضوي

ةيساسآلا تابلطتملا

- [مدختسملا ريفوت نيوكت](#)
- [ZTNA SSO ةقداصم نيوكت](#)
- [دعب نع لوصول لىلا نمآلا لوصولا نيوكت](#)

تابلطتملا

ةيلاتلا عيضاوملاب ةفرعم كيديل نوكت نأب Cisco ي صوت

- Fortigate نم 7.4.x رادصالا ةيامح رادج
- نمآلا لوصولا
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA
- اياوز نودب انتز

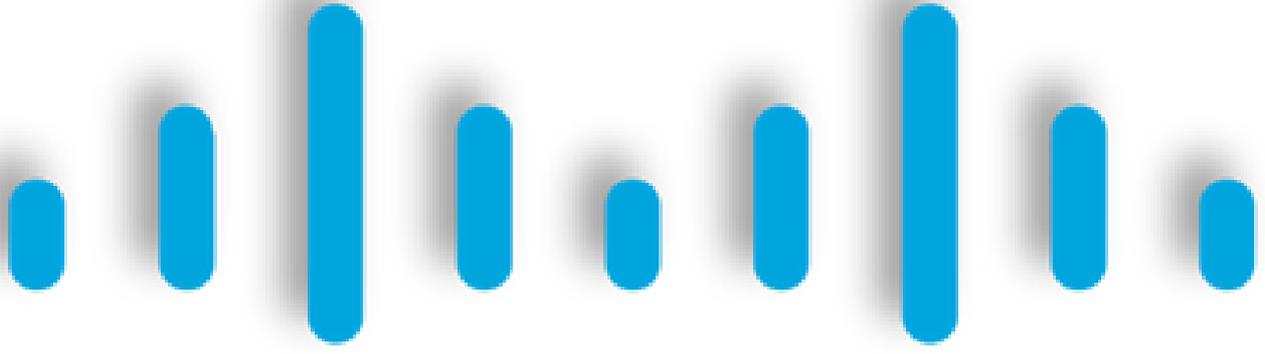
ةمدختسملا تانوكملا

ىل دنن سمل اذه يف ةدراول تامول عمل دنن ستن:

- Fortigate نم 7.4.x رادصل ا ةيامح رادج
- نم آل لوصول
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA

ةصاخ ةيل م عم ةئيب يف ةدوجوم ل ةزهجال نم دنن سمل اذه يف ةدراول تامول عمل اءاشنإ مت تناك اذإ. (يضا رتفا) حوسمم نيوكتب دنن سمل اذه يف ةمدختس مل ةزهجال ا عيمج تادب رما يال لم تحمل الري ثاتلل كمهف نم دكأتف، ليغشتلا دي قكتك بش

ةيساسأ تامول عم



CISCO

Secure

Access

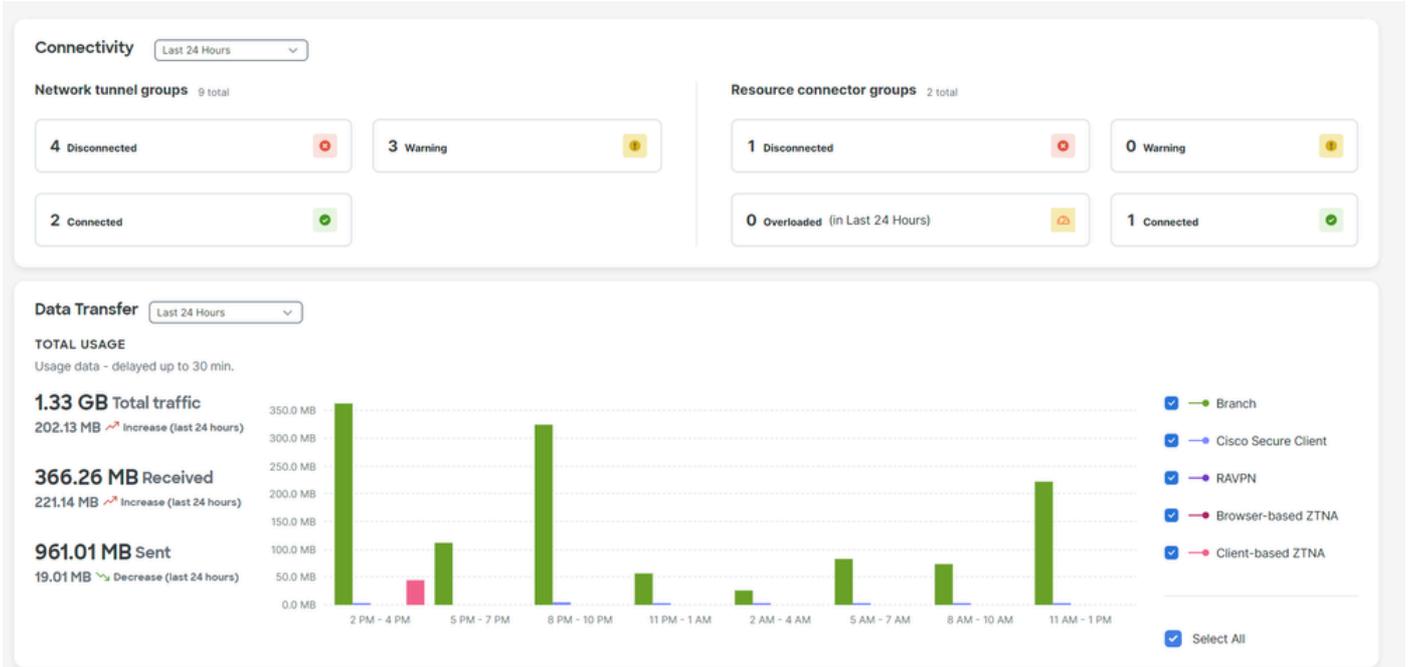
FORTINET®

ساسأ ىلع ،اهىلإ لوصول ريفوتو ةصاخلا تاقببطلال ةيامحل Cisco Secure Access تمم ص ققحتي و. تنرتنإلا ىلإ ةكبشلال نم لاصلتالال نمضي هنأ امك . تاكبشلال ىلع ةمئاقو يلم قىلع ظافحلال ىلإ اهعيمج فدهت ، ةددعتم ةينمأ تاقببطلال ساسأ قىببطلال لالخ نم كلذ ةباحسلال ربع اهىلإ لوصول دنع تامولعملال .

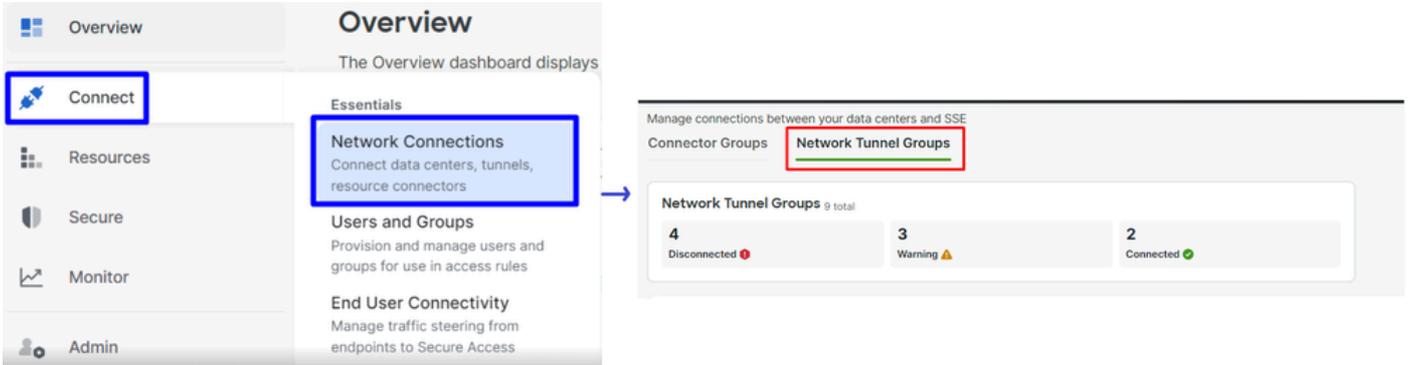
نيوكتال

نمآلا لوصول الی VPN ةكبش نیوكت

ب ةصاخلا ةرادإلا ةحول الی لقتنا [Secure Access](#).



- قوف رقنا Connect > Network Connections > Network Tunnels Groups



- Add + قوف Network Tunnel Groups رقنلا تحت

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](#)

Q Search Region Status 9 Tunnel Groups

+ Add

- Tunnel Group Name، Region و Device Type نیوكتلا
- Next رقنا

✓ 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.

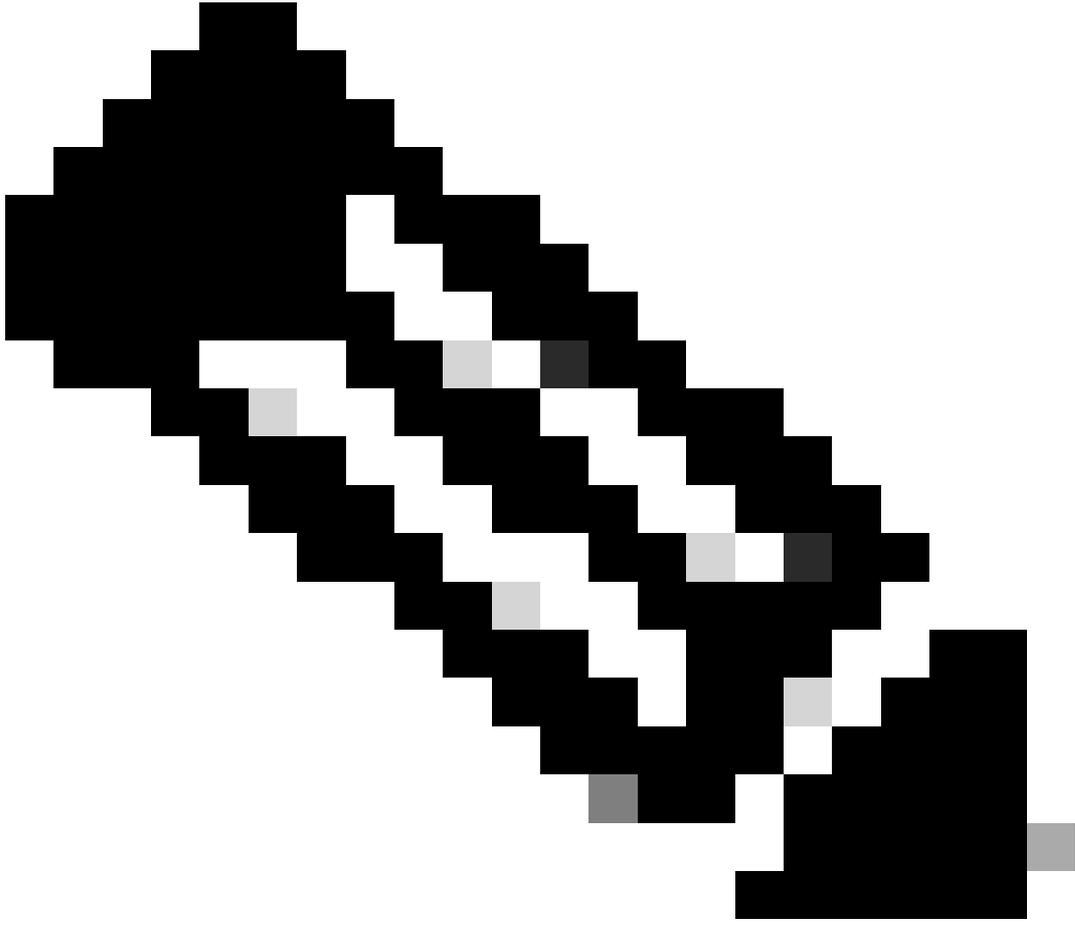
Tunnel Group Name

Region

Device Type

Cancel

Next



ةي امحلا رادج ع قوم ىلا ةقطنم برقا رتخأ :ةظحالم

-
- Tunnel ID Format و Passphrase ني وكتب مق
 - Next رقا

- ✓ 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

- كرح ريرمت ديرتو ةكبشلالا عل اهنيوكتب تمق يئال ةففيضم ال تائيبل وأ IP نيوانع تاقاطن نيوكتب مق نأل لوصول لالغ نم رورملا

- Save رقنا

- ✓ 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

Add

192.168.100.0/24

Dynamic routing

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



Cancel

Back

Save



VPN



IPsec Tunnels



IPsec Wizard

IPsec Tunnel Template

VPN Location Map

- [Create New > IPsec Tunnels](#) رونا

+ Create new ▾

IPsec Tunnel

IPsec Aggregate

Custom 2

- Next رقم او Name a نيو كتيب مق Custom رقمنا

1 VPN Setup

Name 2 Cisco Secure 1
Template type Site to Site Hub-and-Spoke Remote Access Custom

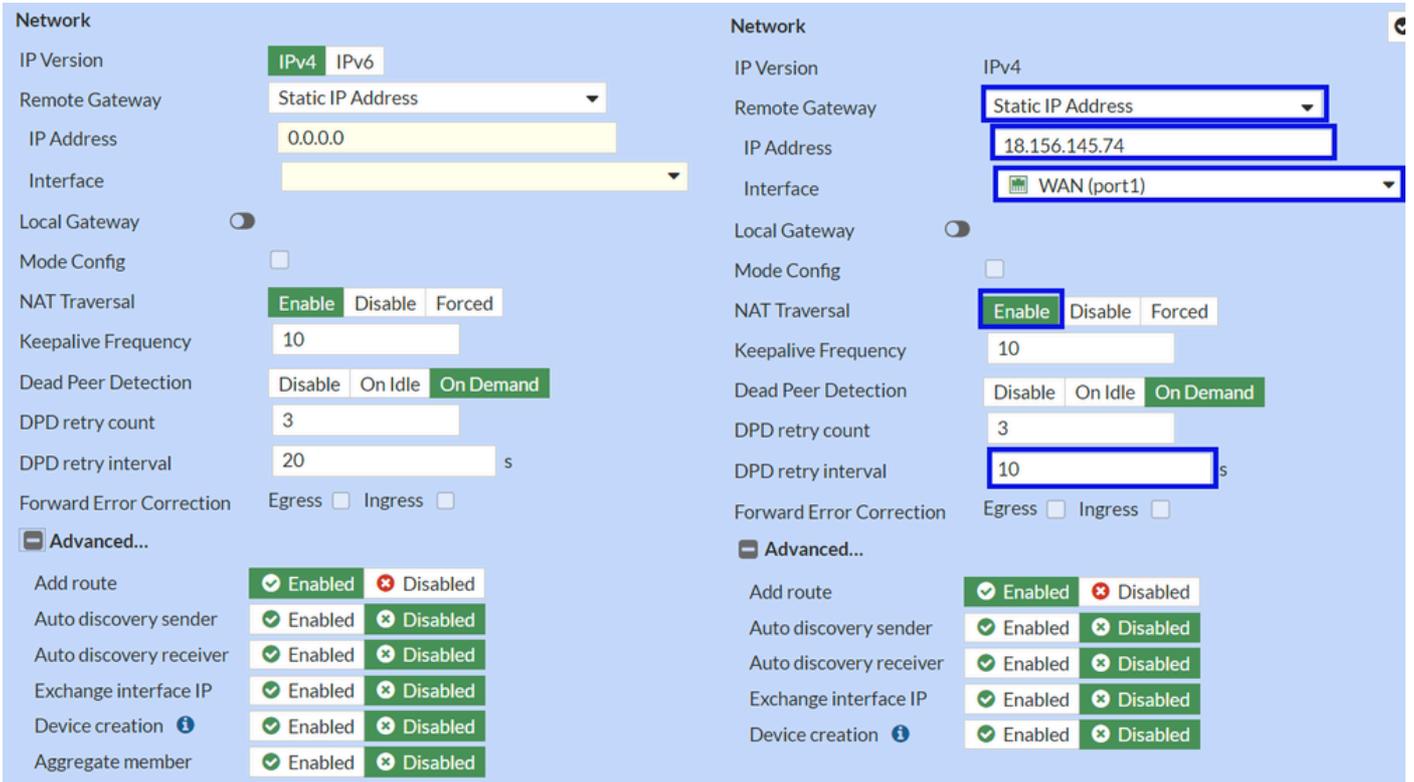
< Back

3
Next >

Cancel

عزجل Network دادع اة لمعمل لكشي نأ جاتحت تنأ فيك تيأر، ة لالتا لة روصلا يف

ة كبشلا



- Network

- IP Version : IPv4

- **Remote Gateway** : تباث ال IP ناوع
- IP Address: ةوطخ ال [قفن تانايب](#) يف ي طعم ل, IP Primary IP Datacenter IP Address, م ادخت س |
- **Interface** : قفن ال عاش ن ال اهم ادخت س ال ت ططخ ي ال WAN ة ه او را ي تخ |
- **Local Gateway** : يضارت فاك لي طعت
- **Mode Config** : يضارت فاك لي طعت
- **NAT Traversal** : نيك مت
- **Keepalive Frequency** : 10
- Dead Peer Detection : بل طال بسح
- **DPD retry count** : 3
- **DPD retry interval** : 10
- **Forward Error Correction** : ع برم ي ا يف ة مال ع عضت ال
- **Advanced...**: ة روصك هن يوك تب مق

IKE Authentication نيوكتب نآل مق

ةقداصلما

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** : مضارتفاك اق بس م كرتشم حاتم

- **Pre-shared Key** : ةوطخلا [قفن تانايب](#) يف يطعمل Passphrase مادختسا

- **IKE**

- **Version** : 2 رادصالا رتخأ

طاقف IKEv لوكوتورب نم ينال رااالصإل Secure Access مع اءى :نظالم

نوكاب نأل مق **Phase 1 Proposal**.

لوالل لارملا ارارا

The screenshot shows two instances of the 'Phase 1 Proposal' configuration interface. The left instance shows a list of four proposals with encryption and authentication settings. The right instance shows a detailed view of a proposal with the following settings:

- Encryption: AES256
- Authentication: SHA256
- Diffie-Hellman Groups: 19 and 20 (checked)
- Key Lifetime (seconds): 86400
- Local ID: fortigate@8195126-621099508-sse.ci

- Phase 1 Proposal

- Encryption : AES256 رتخأ

- Authentication : SHA256 رتخأ

- Diffie-Hellman Groups : ددح 19 و 20 ع برمل

- Key Lifetime (seconds) : 86400 يضا رتفاك

- Local ID : Primary Tunnel ID مادختس | [قف نللا تانايي](#) يف ددح مل

Phase 2 Proposal. نيوكت ب نألا مق

ةينائل ةلحرمل احرارقا

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

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** : كيديل (VPN) ةيره اظلال ةصاخلال ةكبشلال مسا نم اذه ذخأ متي) يضارتفا دادعك :
 - **Local Address** : 0.0.0.0/0.0.0.0 يضارتفا دادعك :
 - **Remote Address** : 0.0.0.0/0.0.0.0 يضارتفا دادعك :

- Advanced
 - **Encryption** : رتخأ AES128
 - **Authentication** : رتخأ SHA256
 - **Enable Replay Detection** : نك مم) يضارتفا لكش ب نك :
 - **Enable Perfect Forward Secrecy (PFS)** : راي تخالال ةناخ دي دحت عاغل :
 - **Local Port** :

(نكمم) يضارتفا لكشپ نك

- **Remote Port:** (نكمم) يضارتفا لكشپ نك
- **Protocol :** (نكمم) يضارتفا لكشپ نك
- **Auto-negotiate :** (ةمالع نودب) ةيضا رتفا ةمي قك نييعت
- **Autokey Keep Alive :** (ةمالع نودب) ةيضا رتفا ةمي قك نييعت
- **Key Lifetime :** (يناوثلاب) ةيضا رتفا ةمي قك نييعت
- **Seconds :** (43200) يضا رتفا لال عصولا نكي ل

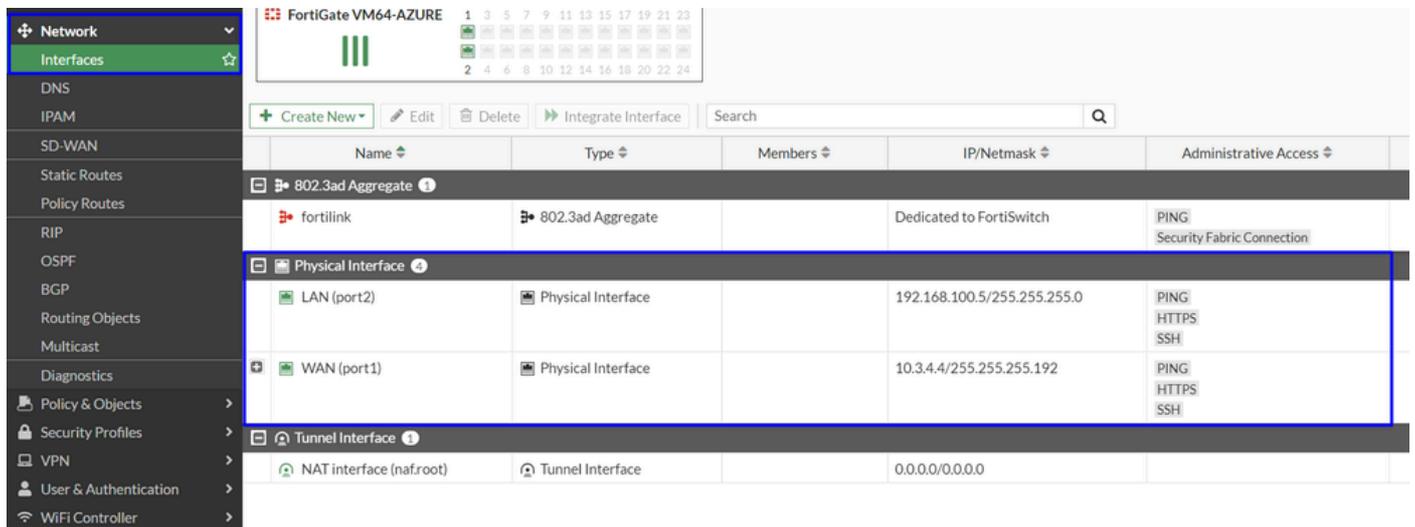
مادختساب اهؤاشن مت دق (VPN) ةيره اظلا ةصاخلا ةكبشلا نأ قئادلا ضعب رورم دعب كنكمي. قفاوم قوف رونا ،كلذ دعب "نمآلا لوصولا" **Configure the Tunnel Interface.** ةيلا لال ةوطخلاب ةعباتملا كنكمي و ،



قفنلا ةهجاو نيوكت

ةنمآلا ذفانم لاب لاصلتال WAN ةهجاوك هم دختست يذلا ذفنم لال فلخ ةديج ةهجاو كي دل نأ ظحالت ،قفنلا عاشن دعب

لل ققحتل **Network > Interfaces** لى للاقنالا اعرجلا ،كلذ نم ققحتل



ةهجاو لال WAN ،ةلا لال هذ ي ف Secure Access: ب لاصلتال هم دختست يذلا ذفنم لال عي سوتب مق



- Edit قوف رونا مٹ Tunnel Interface قوف رونا

+ 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			

- اهنه وكت الى جاتحت يتي التالتي التالتي التالتي التالتي

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 : 169.254.0.1) ةكبشلا ي ف كيدل سيل هيحوتلل لباق ريغ IP نيوكت :
- Remote IP/Netmask : 30 ةكبشلا عانق مادختساب كب ةصاخلا IP ةهجاو ليالاتلا IP ناوئعك دعب نع IP نيوكتب مق : (169.254.0.2 255.255.255.252)

(لصألا ىلا دننتم الما هيحوتلا) Configure Policy Route، ةيالاتلا ةوطخلا ةعباتمو نيوكتلا طفح **OK** رقنا، كلذ دعب



حامسلا وأ زاهاجلا نم رورملا ةكرحل حامسلا ل FortiGate ىلع ةيامحل رادج تاسايس نيوكتب بجي، ءزجال اذه دعب: ريذحت رورملا ةكرح هيحوت ديرت يتلا تاكبشلا ىلا نمألا لوصولو نمو لوصولو نيوماتب اهل

ةسايسلا راسم نيوكت

ةكره هيجوت ةداعا كي لع بجي ،نآلاو ،لوصول نيأتل اهئاشنإو اهنيوكت مت كب ةصاخلا VPN ةكبش كي دل ،ةطقنلا هذو دن ع FortiGate ةيامح راج فلخ كب ةصاخلا ةصاخلا تاقيبطتلا لىل لوصول وأ رورملا ةكره ةيامحل لوصول نيأتل تانايبلا رورم

- لقتنا Network > Policy Routes لىل

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 star icon). On the right, a table displays the Policy Routes configuration. The table has a header row with 'Seq.#' and two data rows with values '1' and '2'. A '+ Create New' button is visible at the top right of the table area.

Seq.#
1
2

- جهنلا نيوكت

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"/>	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"/>	IP/Netmask <input type="text"/>
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"/>
0x00 Bit Mask 0x00	0x00 Bit Mask 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"/>	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

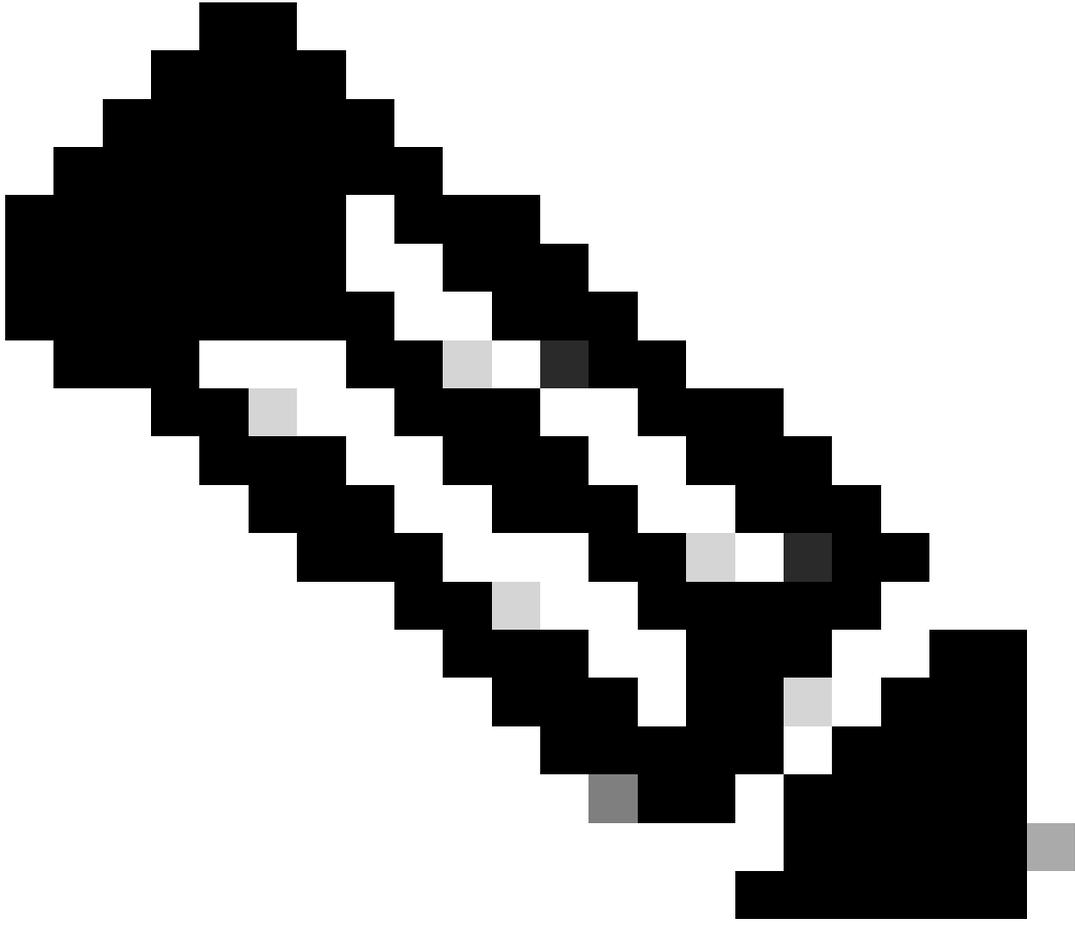
- Incoming Interface : رورملا لوصولو الى رورملا ةكره هي جوت ةداعال ططخت ثيح نم ةهجاو رتخا :

- Source Address

- IP/Netmask : طقف ةهجاو ةيعرف ةكبش هي جوتب تمق اذا راixel اذه مدختسا :

- Addresses : تاهجاو نم يتاي رورملا ةكره رصمو هؤاشن مت يذل نئال كيدل ناك اذا راixel اذه مدختسا : ةدعتم ةيعرف تاكبشو ةدعتم

- Destination Addresses



لجبت سملال يف قاطنلا اذه عيسوتب موقت دق Cisco نأ ينعي ام ،ريغت لل ةضرع هذه IP نيوانع نوكت :تظالم

كب صاخلا قيبتلل نيونك نألا كنكميو ، Secure Access ةطساوب يمحكم كنأ ينعي اذف ،كب صاخلا ماعلا IP ريغت تيأرا اذا
VPNaaS أو ZTNA نم كتاتيبتت لىل لوصولل Secure Access تامولعم ةحول لىل

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا اذ ه Cisco ت مچرت
م ل ا ل ا ا ن ا ع مچ ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل و
ا م ك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ا ة ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا