

ةي امحل رادج مادختساب نم آلا لوصولا نيوكت يلاعلا رفوتلا عم نم آلا

تايوت حمل

ةمدقملا

ةيساس آلا تابلطت ملا

تابلطت ملا

ةمدختس ملا تانوك ملا

ةيساس آلا تامول عم

ةكبش ليل يطي طختلا مسرلا

نيوكت ملا

نم آلا لوصولا يلع VPN ةكبش نيوكت

قفنلا دادعلا تاناب

نم آلا ةي امحل رادج يلع قفنلا نيوكت

قفنلا ةهجاو نيوكت

ةيونانثلا ةهجاو ليل تابلطت ملا راس ملا نيوكت

بولس آ VTI يف ذفنم نم أي نأ VPN ليل تاركش

ةياهنلا طاقن نيوكت

IKE نيوكت

IPSec نيوكت

مدقتم نيوكت

جهن نيوكت تاهو ويرانيس ليل لوصولا

تنترتنالا ليل لوصولا ويرانيس

ويرانيس

ويرانيس انتزت بالك

ةساي سليل ييساس آلا هي جوتلا نيوكت

نم آلا لوصولا يلع تنترتنالا ليل لوصولا جهن نيوكت

RA-VPN و ZTNA ليل ةصاخلا دراوملا ليل لوصولا نيوكت

اهجالص او ءاطخ آلا فاشك تس

(IKEv2) 1 ةلجرملا نم ققحتلا

(IPSec) ةيونانثلا ةلجرملا نم ققحتلا

يلاعلا رفاوتلا ةفيظو

لوصولا نيوكت رورملا ةكرح هي جوت نم ققحتلا

ةلص تاذا تامول عم

ةمدقملا

رفوتلا عم نم آلا ةي امحل رادج مادختساب نم آلا لوصولا نيوكت ةي فيك دنتس ملا اذه حضوي
يلاعلا

ةيساس آلا تابلطت ملا

- [مدخستسملاري فوت نيوكت](#)
- [ZTNA SSO ةقداصم نيوكت](#)
- [دعب نع لوصولل VPN ىل انمآلا لوصولل نيوكت](#)

تابل طتملا

ةيلال عيضاوملاب ةفرعم كي دل نوكت نأب Cisco ي صوت

- Firepower 7.2 ةرادإ زكرم
- 7.2 ةيرانللة قاطلا ديدهت دض عاف دل جم انرب
- نمآلا لوصولل
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA
- اياوز نودب انتز

ةمدخستسملاتانوكملا

ىل دننستسمللا اذه في ةدراولا تامولعمللا دننست

- Firepower 7.2 ةرادإ زكرم
- 7.2 ةيرانللة قاطلا ديدهت دض عاف دل جم انرب
- نمآلا لوصولل
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA

ةصاخة يلمعم ةئييب في ةدوجوملا ةزهجالا نم دننستسمللا اذه في ةدراولا تامولعمللا ءاشنإ مت تناك اذا. (يضا رتفا) حوسمم نيوكتب دننستسمللا اذه في ةمدخستسمللا ةزهجالا عيجمج تادب رما يال لم تحملا ريثأتلل كمهف نم دكأتف، ليغشتللا دي قكتكبش

ةيساسأ تامولعم



CISCO

Secure

Access

Secure Firewall

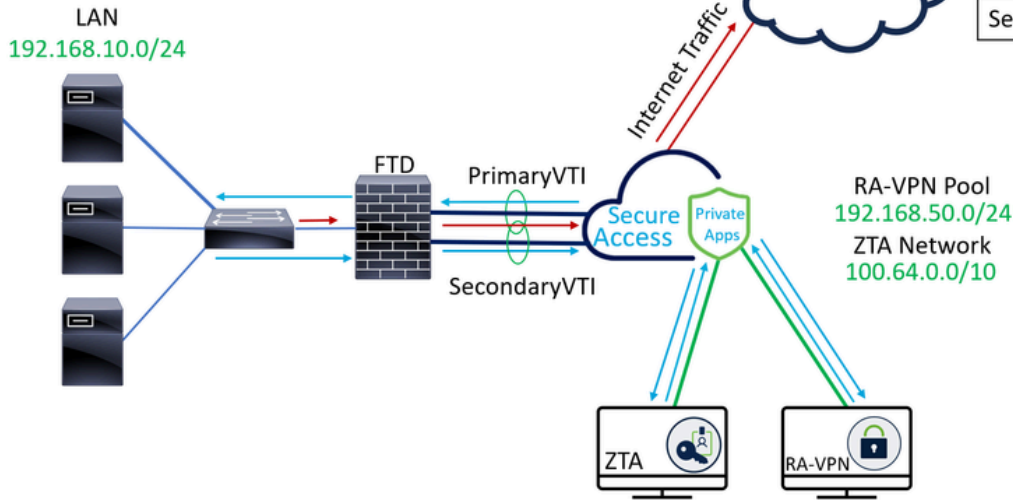
FTD

سأأسأ إلى ع، أهإلإ لوصولأ ريفوتو ةصأخلا تاقببطلأ ةأمحل Cisco Secure Access تممص ققحتي و. تنرتنإلإ إلى ةكبشلأ نم لأصلالأمضي هنأ أمك. تكبشلأ إلى ع ةمئاقو يلحم إلى ع ظافحلأ إلى أهعيمج فدهت، ةددعتم ةينمأ تاقببو بيلاسأ قيببطلأ لآخ نم كلذ ةبأحسلأ ربع أهإلإ لوصولأ دنع تامولعملأ.

ةكبشلل يطيطلأل مسرلأ

Internet Access Traffic —
Private Apps Traffic —

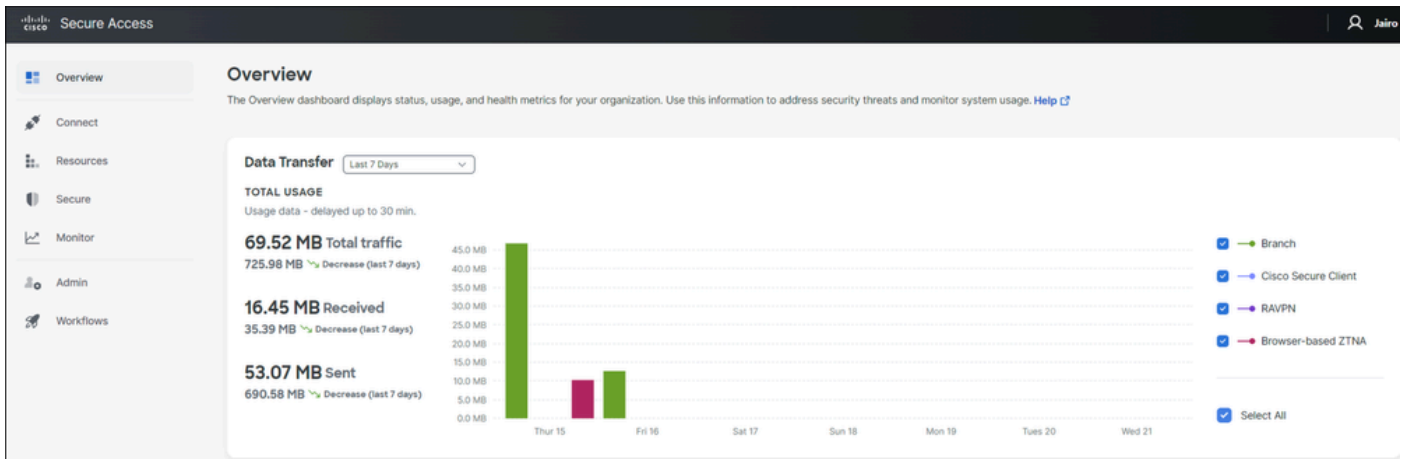
INTERFACE	IP
PrimaryWAN	192.168.30.5
PrimaryVTI	169.254.2.1
SecondaryWAN	192.168.0.202
SecondaryVTI	169.254.3.1



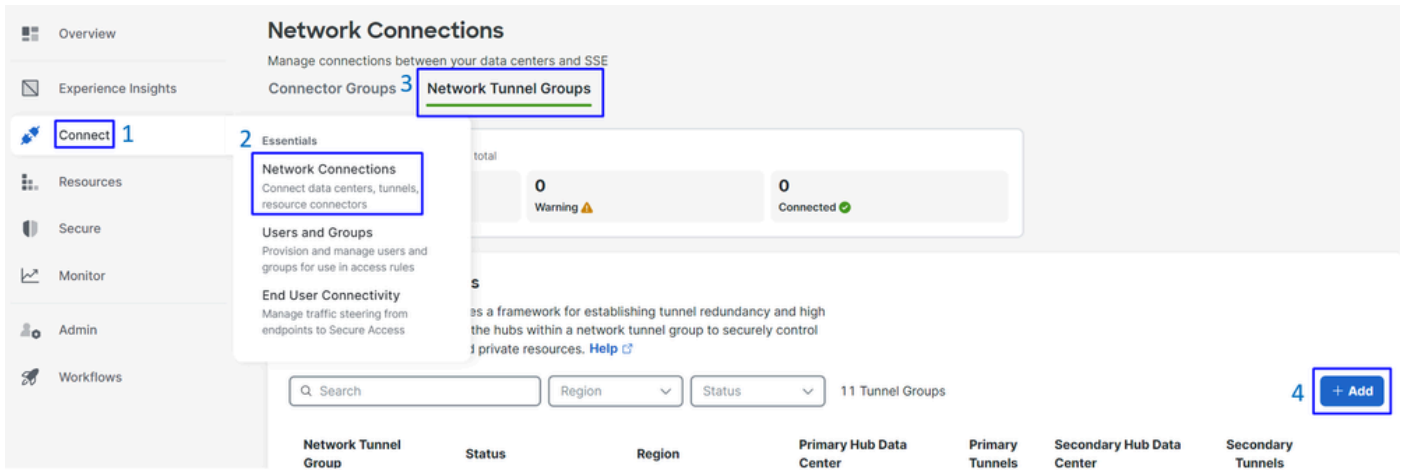
نيوكتالا

نمآلا لوصولا ىل ع VPN ةكبش نيوكت

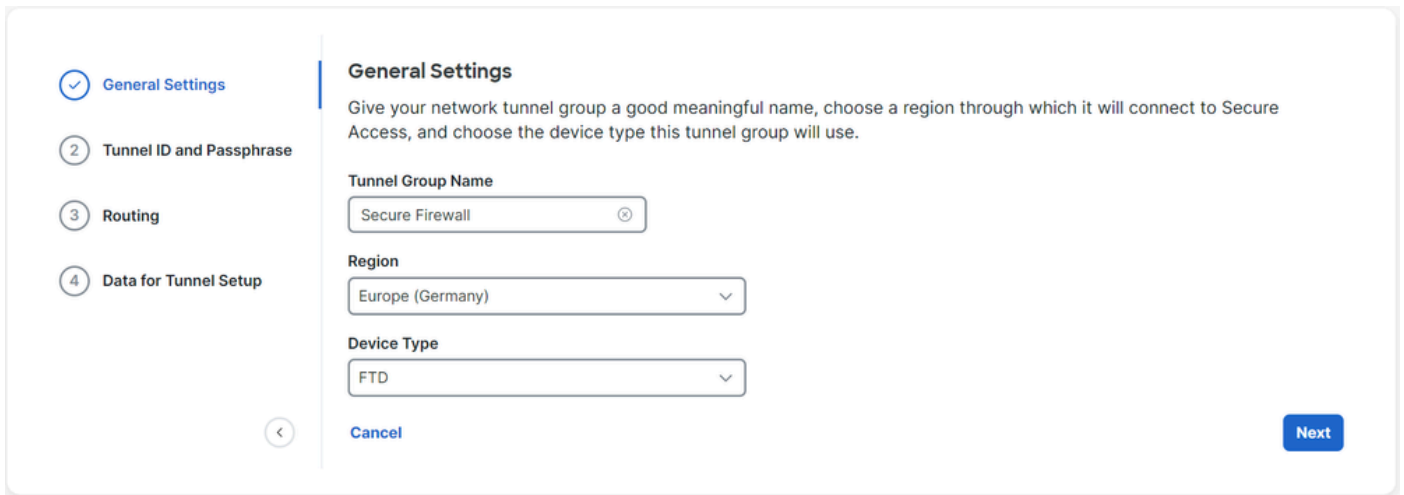
نمآلا لوصولا ةرادا ةحول ىل لقتنا



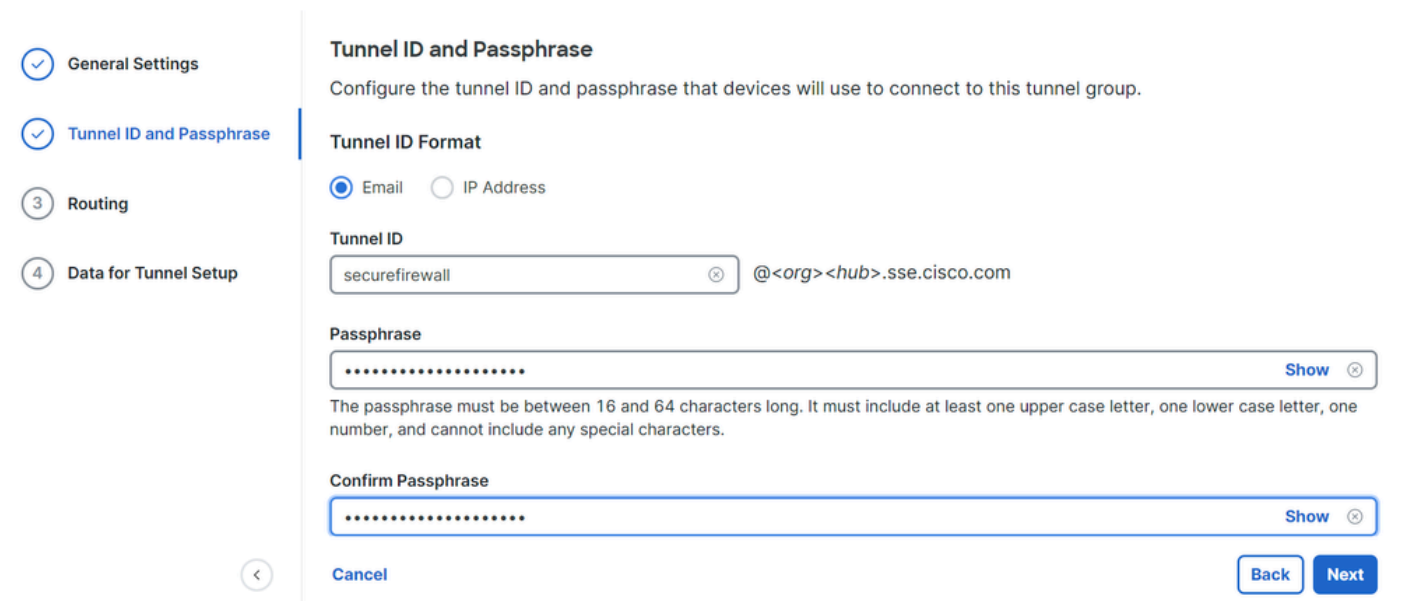
- قوف رقنا Connect > Network Connections
- قوف Network Tunnel Groups رقنلا تحت + Add



- Tunnel Group Name، Region و Device Type نيوكتل
- Next رونا



- Tunnel ID Format و Passphrase نيوكتل مق
- Next رونا



- سلع انه نيوكتل تمق يتللة فيضمال تائيبل وأ IP نيوانع تاقاطن نيوكتل مق

نمآل لوصول لال خ نم رورم لة كرح ريرمت ديرت وة كبش ل

- Save رقنا

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.

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

ة و طخل ل تامول عمل ك لت ظفح عاجر ل، ق فن ل ا ضرع لوح تامول عمل Save قوف رقن ل ا دع ب
ال ل ات ال، Configure the tunnel on Secure Firewall.

ق فن ل ا داع ل ا ت ا ن ا ي ب

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

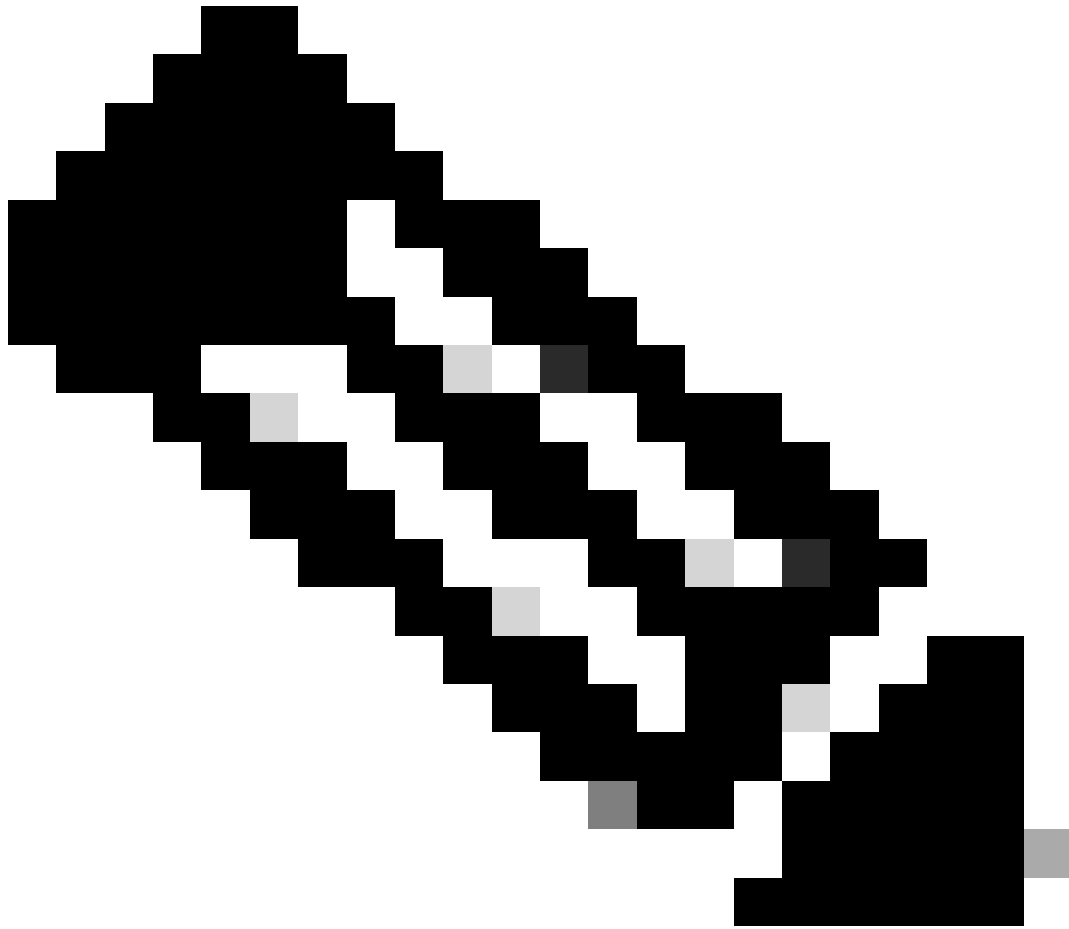
Done

نمآل ة ي ام ح ل ا ر ا د ج ل ع ق فن ل ا ن ي و ك ت

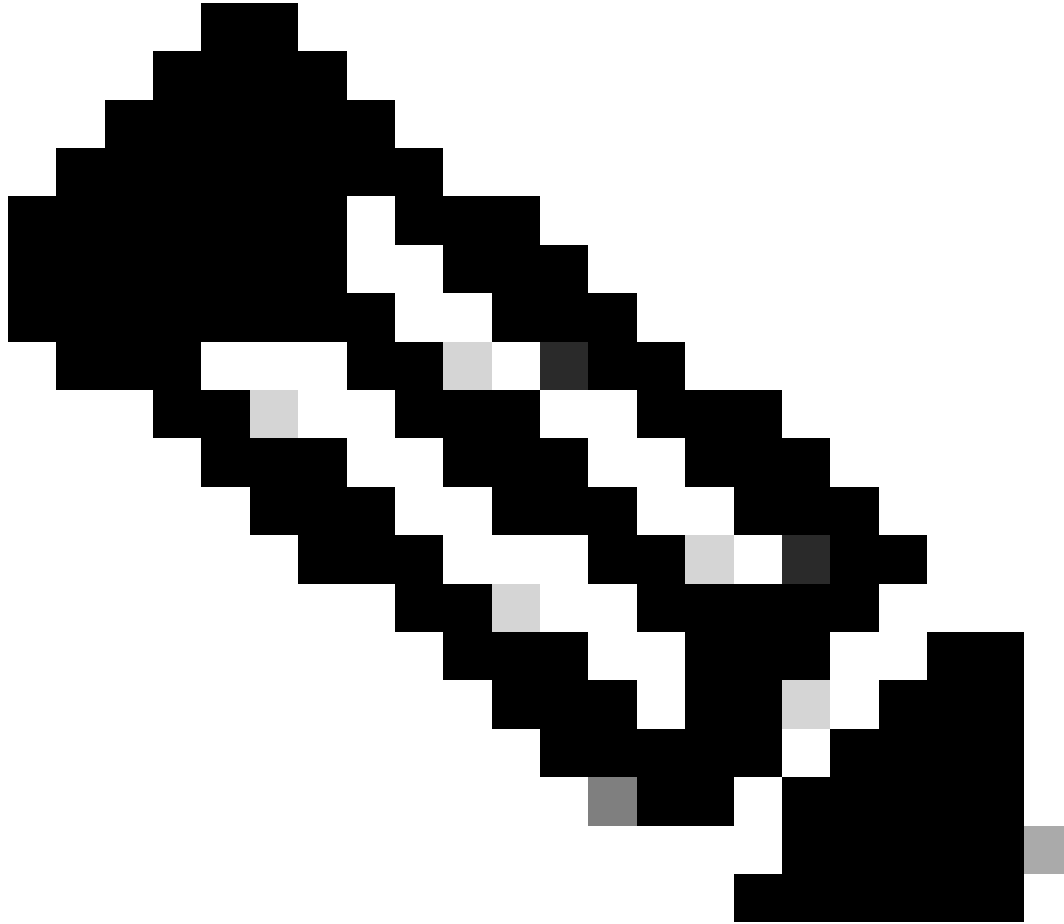
ق فن ل ا ة ه ج ا و ن ي و ك ت

نمآل ة ي ام ح ل ا ر ا د ج ل ع (VTI) ة ي ره ا ظ ل ا ق فن ل ا ة ه ج ا و ن ي و ك ت م د خ ت س ت، و ي ر ا ن ي س ل ا ا ذ ه ل
ن، ج و د ز م (ISP) ت ن ر ت ن ا ل ا ة م د خ ي د و ز م ل ا ج ا ت ح ت ك ن ا، ة ل ا ح ل ا ه ذ ه ي ف ر ك ذ ت؛ ف د ه ل ا ا ذ ه ق ي ق ح ت ل
ك ي د ل ت ن ر ت ن ا ل ا ة م د خ ي د و ز م د ح ا ل ش ف ة ل ا ح ي ف HA ل ع ل و ص ح ل ا ي ف ب غ ر ن و.

تاهجاولا	رود
WAN ةكبش ةيساسألا	تنرتنإلل ةيساسألا WAN ةكبش
WAN ةكبش ةيونألا	يونألا تنرتنإلل WAN ةكبش
PrimaryVTI	لوصولا ىلإ Principal Internet WAN لال خ نم رورملا ةكرح لاسرإل طبترم نمألا
SecondaryVTI	لوصولا ىلإ Secondary Internet WAN لال خ نم رورملا ةكرح لاسرإل طبترم نمألا



Primary or Secondary Datacenter إلى تباث راسم صي صخت وأة فاضا إلى جاتحت 1. :ةظحالم
نيق فنلا الك ليغشت يلع ارداق نوكتل زاوجل IP



جاتحت ال تنأف ،تاهجاولا نيب هنيوكت مت ECMP لوكوتورب كي دل ناك اذا 2. :ةظحالم
يلع ارداق نوكتل لوحملا IP Primary or Secondary Datacenter إلى تباث راسم يءاشن إلى
نيق فنلا الك ءاشن إلى

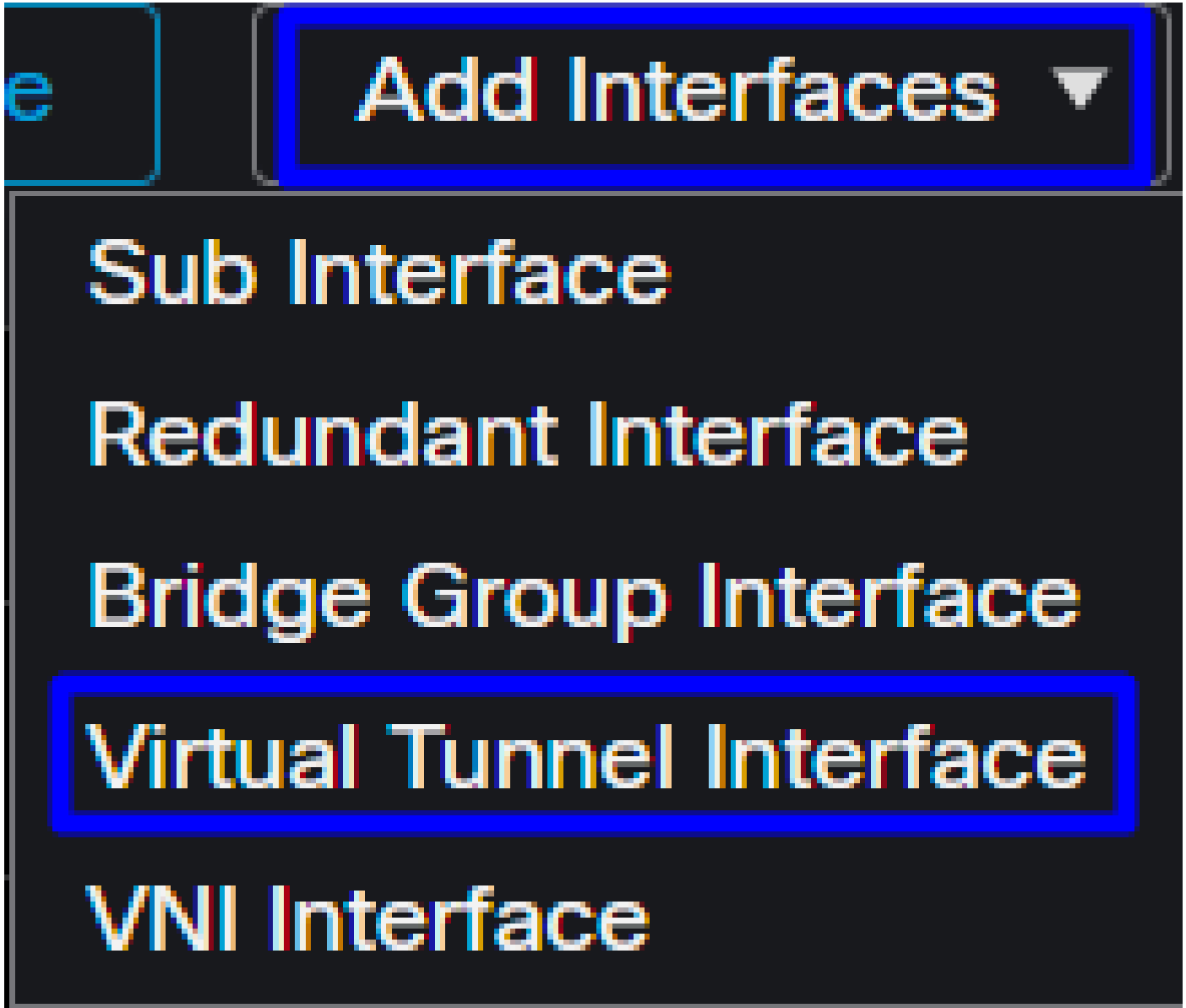
ءاشن إلى هم ادختسإ اني لع بجي يذل SecondaryWAN ، و PrimaryWAN اني دل ،ويرانيسلا إلى ادانتسا
ءاهجاو VTI.

لقتنا Firepower Management Center > Devices إلى لقتنا

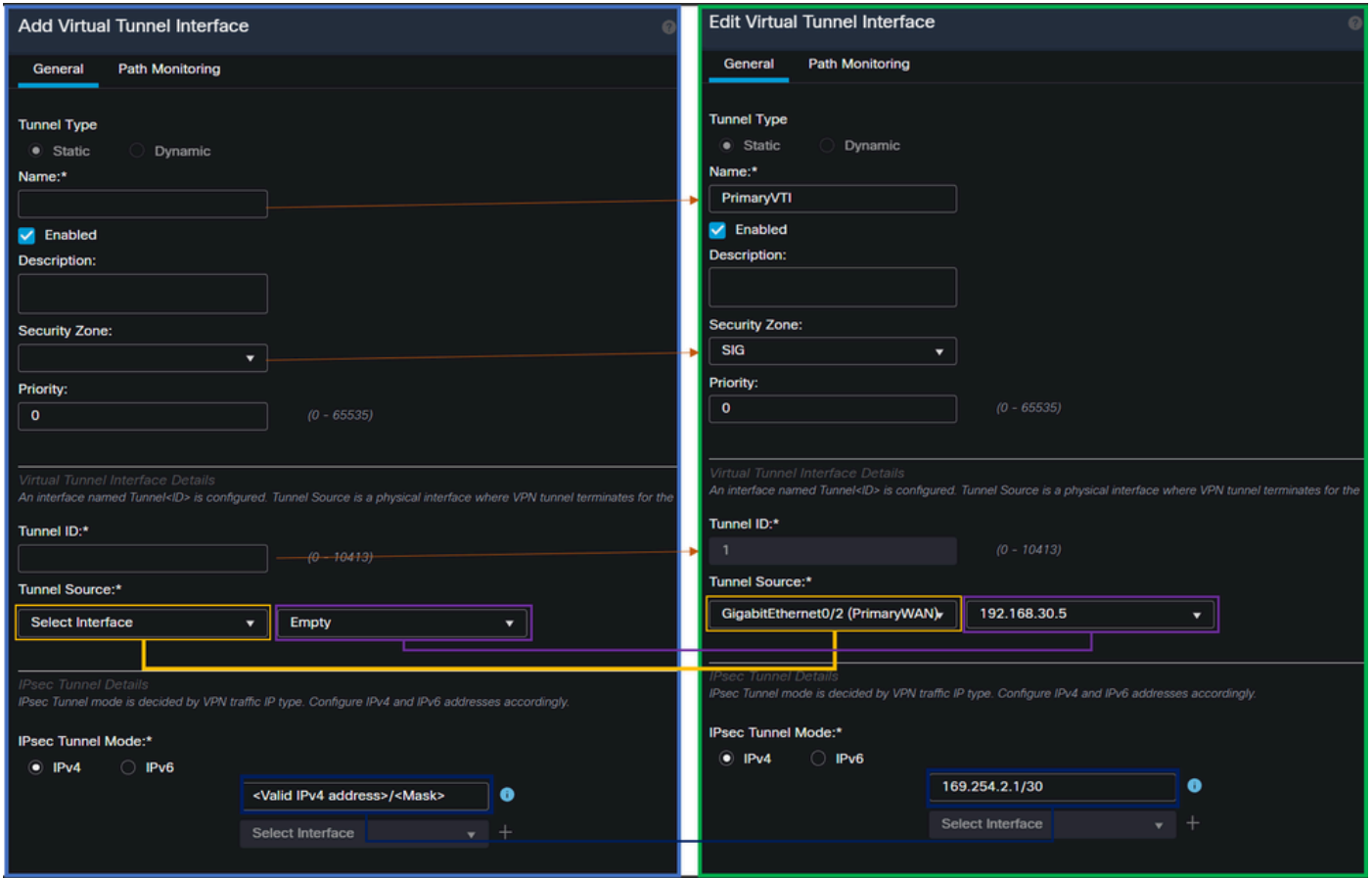
- كب صاخلا FTD راي تخإ
- Interfaces رتخا

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)

- قوف رقنا Add Interfaces > Virtual Tunnel Interface



- قياتل تامول عملال ال ادا نسا ةه جا اولال نيوك ت ب مق



- Name : مق نيوكتب مس ا ريشي لى PrimaryWAN interface
- Security Zone : رورم ة كرحل دي دج دحاو عاشن نكل و Security Zone، رخا مادختسا ةداع كنكمي لصفالا وه نمالا لوصول
- Tunnel ID : قفنلا فرعمل مقرر ةفاضل
- Tunnel Source : ماعالا واصلال IP ناوع رتخاو كب PrimaryWAN interface صاخلال IP ناوع رتخا: مدختسملا ةهجاوب صاخلال
- IPsec Tunnel Mode : 30 عانق عم كتكبش ي ف ip دي دخت جاحسم ريغ تلكشو IPv4 ترتخا:

يقول تي نإ ،ال ثم ؛ ip دي دخت جاح سم ريغ تلمعت سا يغ بن ني تنأ ،نراق VTI لال ل :ةظ حال م
وال ل ل Primary VTI 169.254.2.1/30 تلمعت سا عي طت سي تنأ ،نراق VTI نانثإ تنأ
Secondary VTI ل 169.254.3.1/30

عيش لك كي دلو ، Secondary WAN interface لي لبس نلاب عارجإل س فن ب ما يقو لي إلاتحت ،كلذ دعب
ةي لال ةجيت نال لي ل صحت ،كلذل ةجيت نك و ،رفاوت لاي ل VTI ل دعم

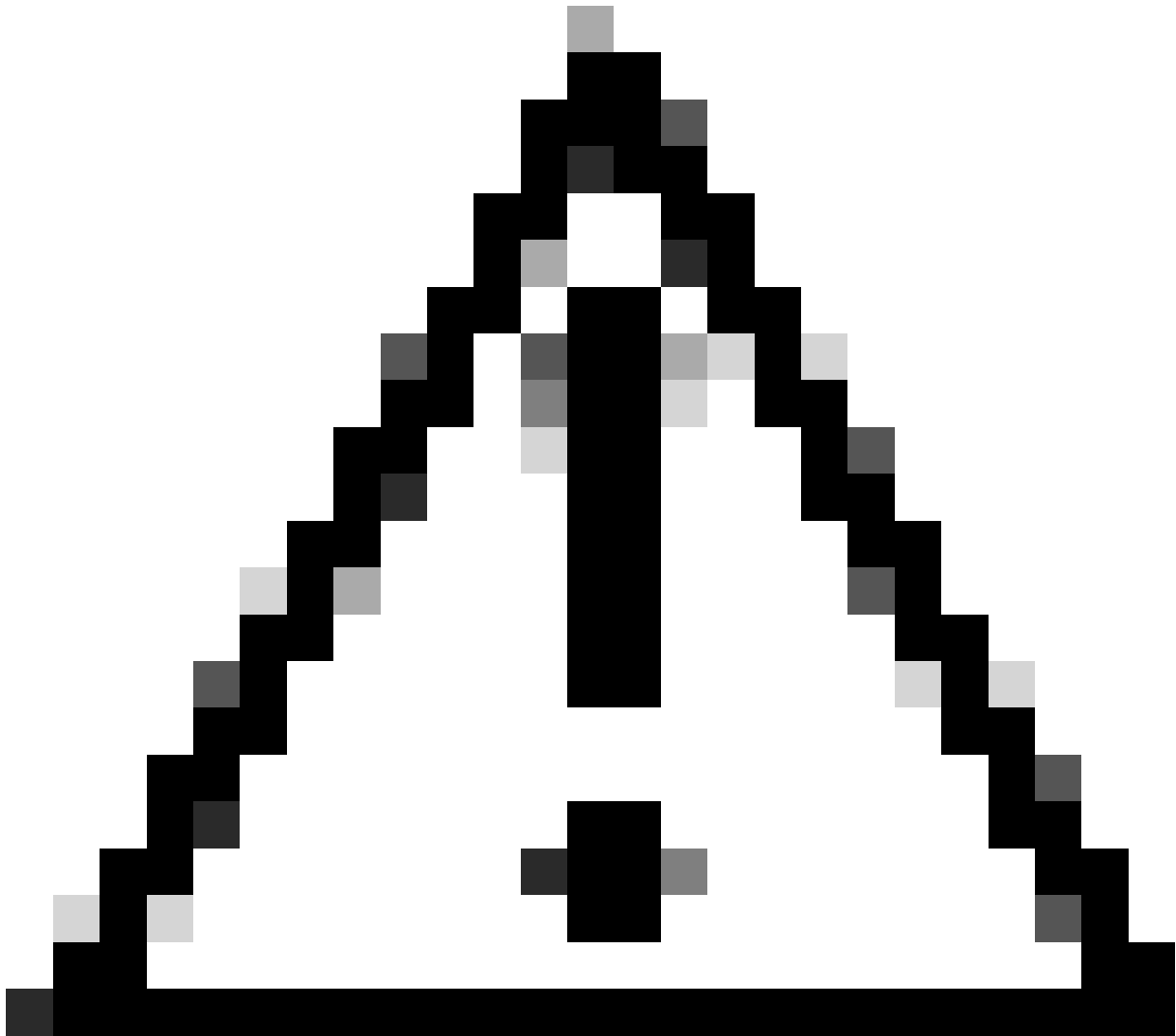
Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
Diagnostic0/0	diagnostic	Physical			
GigabitEthernet0/0	SecondaryWAN	Physical	SecondaryWAN		192.168.0.202/24(Static)
Tunnel2	SecondaryVTI	VTI	SIG		169.254.3.1/30(Static)
GigabitEthernet0/1	LAN	Physical	LAN		192.168.10.1/24(Static)
GigabitEthernet0/2	PrimaryWAN	Physical	PrimaryWAN		192.168.30.5/24(Static)
Tunnel1	PrimaryVTI	VTI	SIG		169.254.2.1/30(Static)

ةمدخت سم ل IP ني وانع نوكت ،وي راني سل اذل

VTI IP نيوكت		
قطنملا مسالا	IP	قطننلا
PrimaryVTI	169.254.2.1/30	169.254.2.1-169.254.2.2
SecondaryVTI	169.254.3.1/30	169.254.3.1-169.254.3.2

ةيوناتللا ةجاولل تباتللا راسملا نيوكت

راسملا Secondary Datacenter IP Address لى لوصول Secondary WAN interface تانايبلا رورم ةكرح ب حاسم لى لى لغأ ي ف هل عجل (1) دحاو سايقم مادختساب اهنيوكت كنكمي . تانايبلا زكرم لى لى تباتللا فىضمك IP دح ، اضيأ ؛ هجوتلا لودج



م ت اذا ؛ WAN تاونق ني ب ECMP دادع لى كيدل نكي مل اذا لى اي رورض اذه نوكي ال : ريذحت

ةيلال ةوطخال لىل لاقتنال كك ميف ، ECMP نيوكت

ىل لقتنا **Device > Device Management**

- فTD زاهج لىل ع رقنا
- روف رقنا Routing
- رتخا 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: أهج او رتخأ WAN ةيون اثل
- Gateway: ةب اوب رتخأ SecondaryWAN
- Selected Network: لى لى روثل ال كن كمى؛ فى ضمك ةيون اثل تان اى ب ال زك رمل IP ةفاضل؛ لوصول ةوطخ لى لى ق فنل لى ني وكت دن ةم دق م ال تامول عملاب ةقل عمل تامول عمل ق فنل لى دادع ل تان اى ب، ن م ال

- Metric: دحاو مادختسا (1)
- OK رشنلاب مق مٹ، تامولعمل ظفحل Save رقن OK.

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						

ببولسا VTI ي ف ذفنم نمأي نا VPN ل تلکش

كب صاخلا ةيامل راج ىل لقتنا، VPN ةكبش نيوكتل

- Devices > Site to Site قوف رقنا
- Site to Site VPN + قوف رقنا

ةياهنلا طاقن نيوكتل

تانايب، ةوطخل نمض ةمدقملا تامولعمل مادختسا ىل جاتحت، ةياهنلا طاقن ةوطخ نيوكتل [قفنلا دادع](#).

Create New VPN Topology

Topology Name:*
SecureAccess

Policy Based (Crypto Map) Route Based (VTI)

Network Topology:
 Point to Point Hub and Spoke Full Mesh

IKE Version:* IKEv1 IKEv2

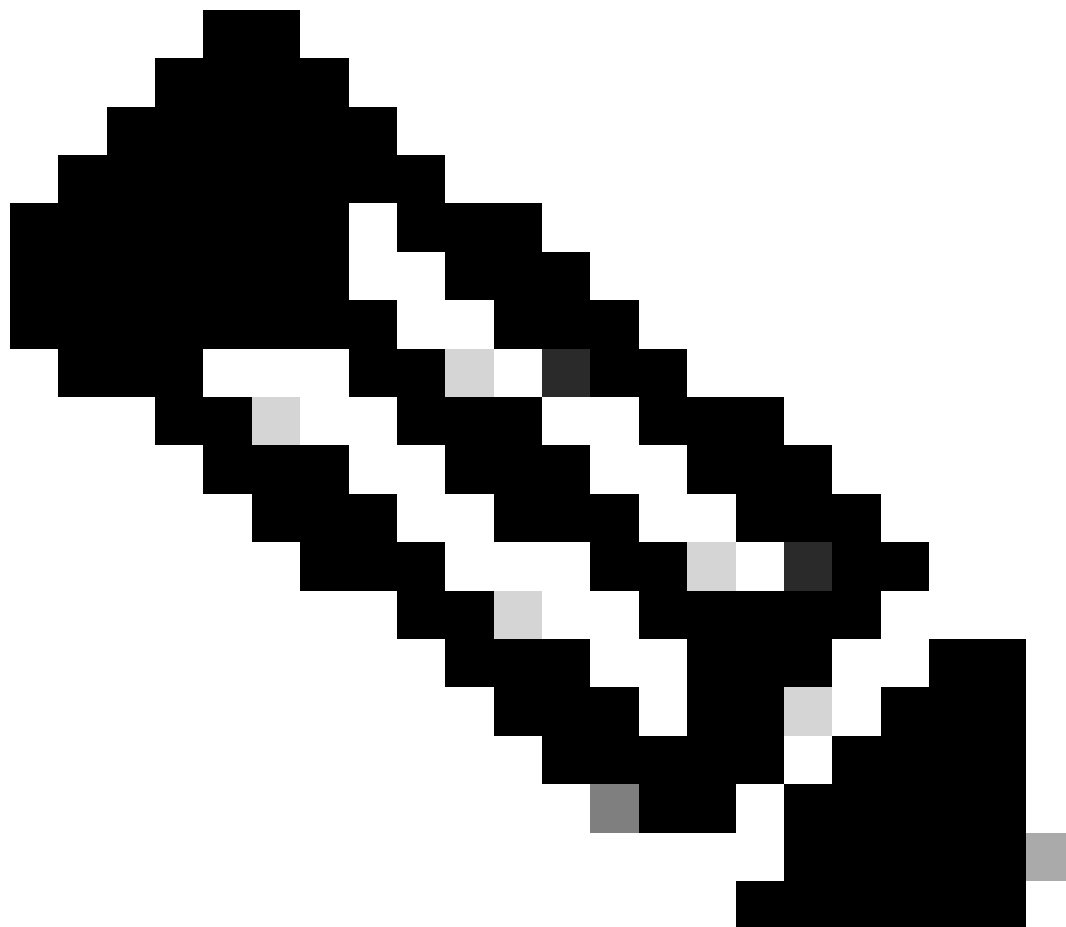
Endpoints IKE IPsec Advanced

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](#)

- نمآلا لوصول لمالك تب قلعتم مسا عاشن: طاخلما مسا
- Routed Based (VTI) رتخا

- رتخا Point to Point
 - IKE Version: رتخا IKEv2
-



Secure Access. عم لم اكل لل موع دم ريغ IKEv1: ةظحالم

ي: لال م ل عم لال لك شي نأ جات تحت Node A تحت

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: كِب صاخال FTD زاهاج رتخأ
- Virtual Tunnel Interface: لآ قلعتم VTI لآ ترتخأ PrimaryWAN Interface.
- Send Local Identity to Peers ل راي تخالا ةناخ دي دحت
- Local Identity Configuration: أرتخأ لآ ادانتسا تامولعملآ لمب مقو، ينورتكلالآ ديرب لآ فرعم رتخأ Primary Tunnel ID تامولعملآ [دادع اتانايب](#)، ةوطخالآ لعل كِب صاخال نيوكتلآ لآ ف ةرفوتملآ Primary Tunnel ID تامولعملآ [قفنلآ](#)

+ Add Backup VTI: قوف PrimaryVTI رقنلآ دنع تامولعملآ نيوكتلآ دعب

Node B

Device:*

Extranet



Device Name*:

SecureAccess

Endpoint IP Address*:

18.156.145.74, 3.120.45.23

- Device: إنارةسك
- Device Name: ةهءوك نمآلا لوصولا ىلع فرعتلل امسا رتخأ.
- Endpoint IP Address: ىساسأ ىونائل او ىساسألا نىوكت نوكى نأ بءى **Datacenter IP,Secondary** [قفنلا دادعلا تاناب](#)، ةوطءلا ىف تامولعمل اءه ىلع روءعلا كنكم ىو **Datacenter IP**

نىوكت، ةوطءلا ىلإ لاقئنا لآلا كنكم ىو، كب صااءلا نىوكئلا لامك ىمئى Endpoints، كلذ ءعب IKE.

IKE نىوكت

IKE قوف رقنا، IKE تامولعمل نىوكئلا

Endpoints

IKE

IPsec

Advanced

ي:للات ملعملال لكشي نأ جاتحت تنأ، تكت IKE

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: كنكمي وأ Umbrella-AES-GCM-256 ي ضارتفالا Umbrella نيوكت مادختسإ كنكمي [Supported IKEv2 and IPSEC Parameters](#) لى اذانتسا ةفلتخم تاملعم نيوكت
- Authentication Type: اقبس م كرتشم يودي جاتقم
- Key: Confirm Key: ةوطخال ي ف تامولعملال Passphrase لى ع روثعلا كنكمي

نيوكت، ةوطخال لى للاقتنال نألا كنكمي، كب صاخلا نيوكتلا لامكإ مت IKE، لكذ دعب IPsec.

نيوكت IPsec

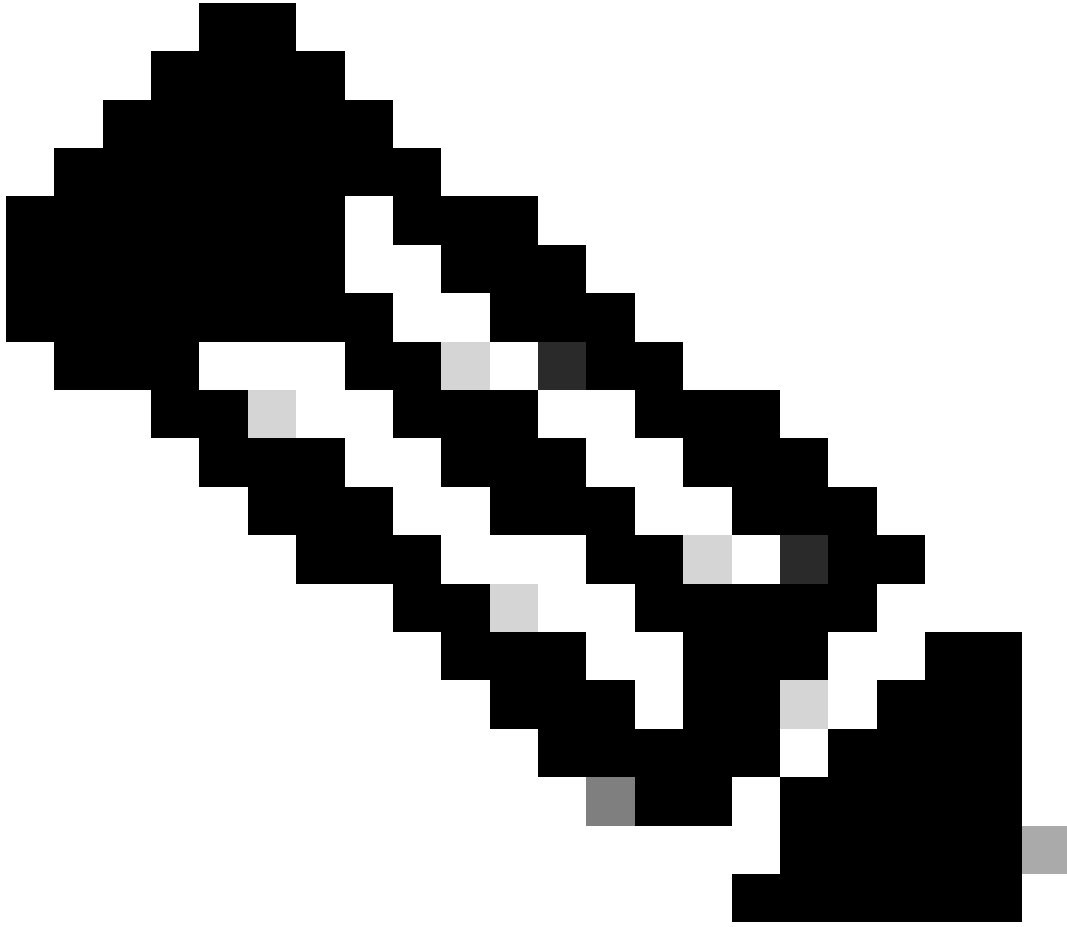
IPsec قوف رونا، IPsec تاملعم نيوكتلا

Endpoints

IKE

IPsec

Advanced



IPSec ىلع بولطم رخآ عيش ال :ةظحال م

نيوكتلاو ةوطخلا ىلإ لاقنتال نآلا كنكميو ،كب صاخلا نيوكتلا لامكإ متي IPSEC ،كلذ دعب مدقتملا

مدقتم نيوكت

"ةمدقتم تاراخي" قوف رقنا ،ةمدقتملا تاملعمل نيوكتل

Endpoints

IKE

IPsec

Advanced

ي:لات ملعمل لكشي نأ جاتحت نأ، Advanced، تحت

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

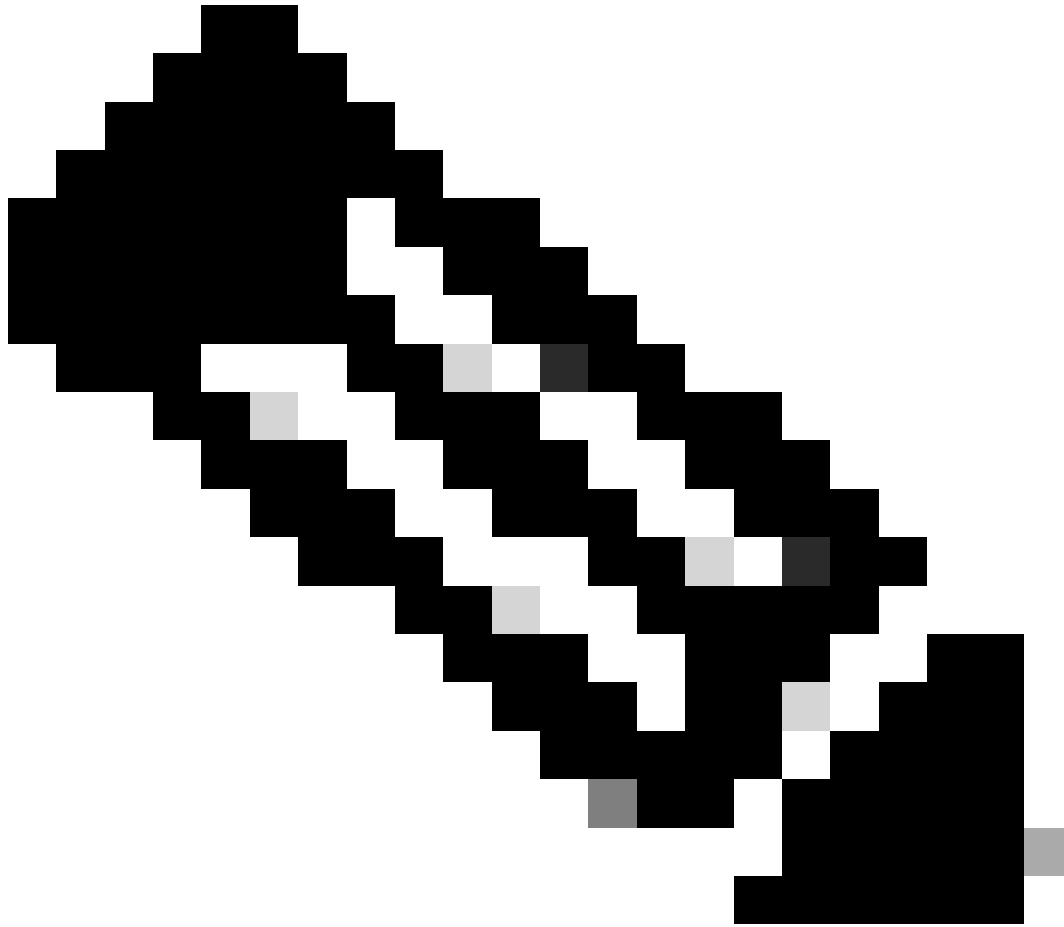
Enable Notification on Tunnel Disconnect

IKEv2 Security Association (SA) Settings

Cookie Challenge: custom

- IKE Keepalive: نيكمت
- Threshold: 10
- Retry Interval: 2
- Identity Sent to Peers: autoOrDN
- Peer Identity Validation: ققحتلا مدع

Save و Deploy طغضلال كنكمي، كلذ دعب.



نم لك اهؤاشنإ مت يتال VPN ةكبش ةدهاشم كنكمي، قئاقد عضب دعب: ةظحالم
دقعال

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)

لاقتنال نآل كنكمي و، كب صاخال نيوكتال لامكإ متي VPN to Secure Access in VTI Mode، كلذ دعب
ةوطخال إلی، Configure Policy Base Routing.



يسئرل قفنل ال طقف لوصول نيمأتل رورملا ةكرح هيجوت ةداعإ متت :ريذحت
ةداعإب "نمآلا لوصول" حمسيف ،يساسألا ضفخنا اذإ ؛نقفنل الك عاشنإ دنع
يوناتل قفنل لالخنم رورملا ةكرح هيجوت.

يف ةقثوم ال DPD ميق ىل Secure Access ع قوم يف لشفلا زواجت دنتسي :ةظحالم
ةم ودم ال IPsec ميق ل [مدختسم ل ليلد](#).

جهن نيوكت تاهويرانيس ىل لوصولا

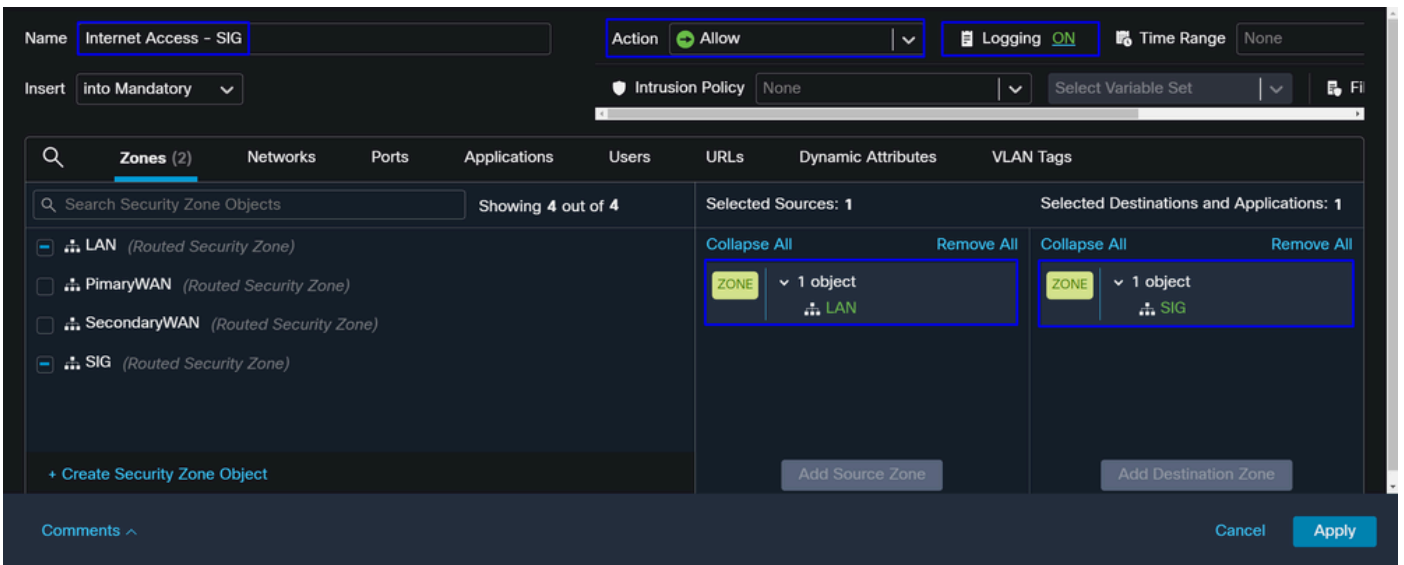
يلې ام ىل ةدحمل لوصولا ةسايس دعاوق دنتست

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)

ةهجاوإا	ةقطنم
PrimaryVTI	ةلخن
SecondaryVTI	ةلخن
LAN	LAN

تنترنتإإا إإا لوصولا ويرانيس

هيجوتلا إلع اهنيوكتب تمق يتلا دراوملا عيمج إإا تنترنتإإا إإا لوصولا ريفوتل لوصولا يف تاسايسلا ضعب كلذكو لوصولا دعاوق ضعب نيوكت كلمزلي، جهنلل ياساسإا ويرانيسلا اذه يف كلذقيقت ةيفيك حرشأ ينعد اذل، نمإا



SIG. ه LAN تنترنتإإا، ةلحال اذه يفو، تنترنتإإا إإا لوصولا ةدعاقلا هذه رفوت

ويرانسإا

تمق يذلا قاطنلا إإا اذانتسا هننيوكت كلمزلي، RA-VPN يمذختسم نم لوصولا ريفوتل RA-VPN عمجت إلع هننيوكتب

[قصا اءلا تاك بشل اءراءا](#) ربء رورملا كئكمي ، RA-VPNaaS ءسايس نيوكئل :ءظءالم
[ءيرءاظلا](#)

VPNaaS ب صا اءلا IP عمءء نم ققءءلا كئكمي فءك

نم آلا لوصولا تامولعم ءءول ىلا لقتنا

- قوف رقنا Connect > End User Connectivity
- قوف رقنا Virtual Private Network
- قوف رقنا Manage IP Pools، ءءء

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

Manage

2 Regions mapped

- Endpoint IP Pools تحت كِب صاخالل ةحابسلا ضوَح یرت

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

- ACL لآ تحت هتفضأ اضیأ یغبنی تنأ نأ ریغ، SIG تحت قاطنلا اذه حمسی نأ آاتحت تنأ نأ ك. PBR یف لكشت تنأ نأ

لوصولا ةدعاق نیوكت

دراوم یلآ لوصولا تاناکم عم هم ادختسال Secure Access نیوكتب طقف موقت تنك اذآ یلی امك كِب ةصاخالل لوصولا ةدعاق ودبت نأ نكمی، ةصاخالل تاقیبطتلا

Name: Private APP
Action: Allow
Logging: ON
Time Range: None
Insert: into Mandatory
Intrusion Policy: None
Select Variable Set:
FI

Search Network and Geolocation Objects

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
<input type="checkbox"/> any-ipv4 (Network Object)	0.0.0.0/0
<input type="checkbox"/> any-ipv6 (Host Object)	::/0

+ Create Network Object Manually Enter IP

Showing 27 out of 27

Selected Sources: 2

- ZONE 1 object SIG
- NET 1 object 192.168.50.0/24

Selected Destinations and Applications: 1

- ZONE 1 object LAN

Comments

Cancel Apply

ةصاخالل LAN ةكِبش یلآ 192.168.50.0/24 RA-VPN عمجت نم رورملا ةكرب حمست ةدعاقلا هذهو رمالا مزلا اذآ دیزملا ددحت كنكمی؛ كِب

(ACL) لوصولا یف مكحتلا ةمئاق نیوكت

يفي مكنحتلا ةمئاق تحت اهتفاضل بجي، LAN ةكبش لىل SIG نم هيچوتلا رورم ةكرب حامسلل
 بجومب لمعت اهلعجل لوصولو 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	

ويرانس انتزب بالك

لىل لوصولو ريفوتل CGNAT 100.64.0.0/10 قاطن لىل اذانتسا كتكبش نيوكت بجي
 ZTA ةسسأل ضرعتسمل ةكبش وأ ZTA لىمعل ةدعاق يمدختسم نم كتكبش

لوصولو ةدعاق نيوكت

دراوم لىل لوصولو تاناكم عم همادختسال Secure Access نيوكتب طقف موقت تنك اذا
 يلى امك كب ةصاخلل لوصولو ةدعاق ودبت نأ نكمي، ةصاخلل تاقىبطلل

Name: ZTNA Access - IN | Action: Allow | Logging: ON | Time Range: None | Rule Enabled: ON

Insert: into Mandatory | Intrusion Policy: None | Select Variable Set: | File Policy: None

Showing 27 out of 27

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

ةيلحمل ةكبش لىل ZTNA cgnat 100.64.0.0/10 قاطن نم رورم ةكرب حمست ةدعاقلل كلت
 كيدل.

(ACL) لوصولو يف مكنحتلا ةمئاق نيوكت

تحت اهتفاضل بجي، LAN ةكبش لىل CGNAT مادختساب SIG نم هيچوتلا رورم ةكرب حامسلل
 PBR تحت لمعت اهلعجل لوصولو يف مكنحتلا ةمئاق

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	

ةساي س ل ل ي س اس ال ا ه ي ج و ت ل ا ن ي و ك ت

ءاشن ا ك ي ل ع ب ج ي ، ن م ال ا ل و ص و ل ا ل ا ل خ ن م ت ن ر ت ن ا ل ا و ة ي ل خ ا د ل ا د ر ا و م ل ا ي ل ا ل و ص و ل ا ر ي ف و ت ل ن م ت ا ن ا ي ب ل ر و ر م ة ك ر ح ه ي ج و ت ل ه س ي ي ذ ل ا (PBR) ت ا س ا ي س ل ا ة د ع ا ق ه ي ج و ت ر ب ع ت ا ر ا س م ة ه ج و ل ا ي ل ا ر د ص م ل ا .

- ا ل ل ق ت ن ا D e v i c e s > D e v i c e M a n a g e m e n t
- ر ا س م ل ا ء ا ش ن ا ب م و ق ت ث ي ح F T D ز ا ه ج ر ت خ ا

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

- R o u t i n g ق و ف ر ق ن ا
- P o l i c y B a s e R o u t i n g ر ت خ ا
- A d d ر ق ن ا

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](#)

ي ل ا ر و ر م ل ا ة ك ر ح ه ي ج و ت ل ر د ص م ك ا ه م د خ ت س ت ي ت ل ا ت ا ه ج ا و ل ا ع ي م ج د د ح ت ، و ي ر ا ن ي س ل ا ا ذ ه ي ف ZTA ل و ص و م ا د خ ت س ا ب ن م ال ا ل و ص و ل ل م د خ ت س م ل ا ة ق د ا ص م ر ي ف و ت ل و ا ن م ال ا ل و ص و ل ا ي ل ا د ن ت س م ل a ZTA ل و ص و و ا R A - V P N ي ل ا د ن ت س م ل ا ل و ص و ل ا و ا ض ر ع ت س م ل ا ي ل ا د ن ت س م ل ا ة : ة ك ب ش ل ل ة ي ل خ ا د ل ا د ر a o m l a ي ل a ل ي م ل a

- ذ ف ن م ن م ا ي ر ب ع ر و ر م ة ك ر ح ل س ر ي ن ا ن ر ا ق a l l t h e ت ن ي ع ، ن ر ا ق ل خ د م ت ح ت :

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

- رقننلا دعب ةيلا لئلا تامل عمل في رعتب موقت ، جورخلا ةهجاو وري اعلمل ةقباطم تحت قوف Add:

Match Criteria and Egress Interface

Specify forward action for chosen match criteria.

Add

Add Forwarding Actions

Match ACL:* Select... +

Send To:* IP Address

IPv4 Addresses: For example, 192.168.0.1, 10.10.1.2

IPv6 Addresses: For example, 2001:db8::, 2002:db8::1

Don't Fragment: None

Internal Sources

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

- موقت ام لك نيوكت كنكمي ، هذه (ACL) لوصولي في مكحتلا ةمئاقل ةبسنلاب Match ACL: نمآلا لوصولي لآهه جوتب:

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

Sequence	Action	Source	Source Port	Destination	Destination Port
1	Block	Any	Any	208.67.222.222 208.67.222.220	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: ناوع رتخأ IP
- IPv4

كنكمي VTI! ال كىل ع لكشي 30 عانقلا تحت ip يلاتل تلمعتسا يغبني تنأ Addresses: [VTI هجاو نيوكت](#)، ةوطخل نمض ك لذ نم ققحتل

طاوا غيغ	IP	هجاو لا
169.254.2.2	169.254.2.1/30	PrimaryVTI
169.254.3.2	169.254.3.1/30	SecondaryVTI



قوف رقنلاب ةعباتملا كنكميو، ةيلاتل ةجيتنلا كيدل، وحنلا اذه لىل اه نيوكت دعب 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 +

Cancel Save

ةيلاتل ةقيرطلاب ه نيوكت لىل جاتحت امك، رخأ ةرم ك لذ Save لىل جاتحت، ك لذ دعب

A policy based route consists of ingress interface list and a set of match criteria associated to egress interfaces

Ingress Interface*

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

Match ACL	Forwarding Action
ACL	Send through 169.254.2.2 169.254.3.2 → Send the traffic to the PrimaryVTI

If PrimaryVTI fail it will send the traffic to the SecondaryVTI

Cancel Save

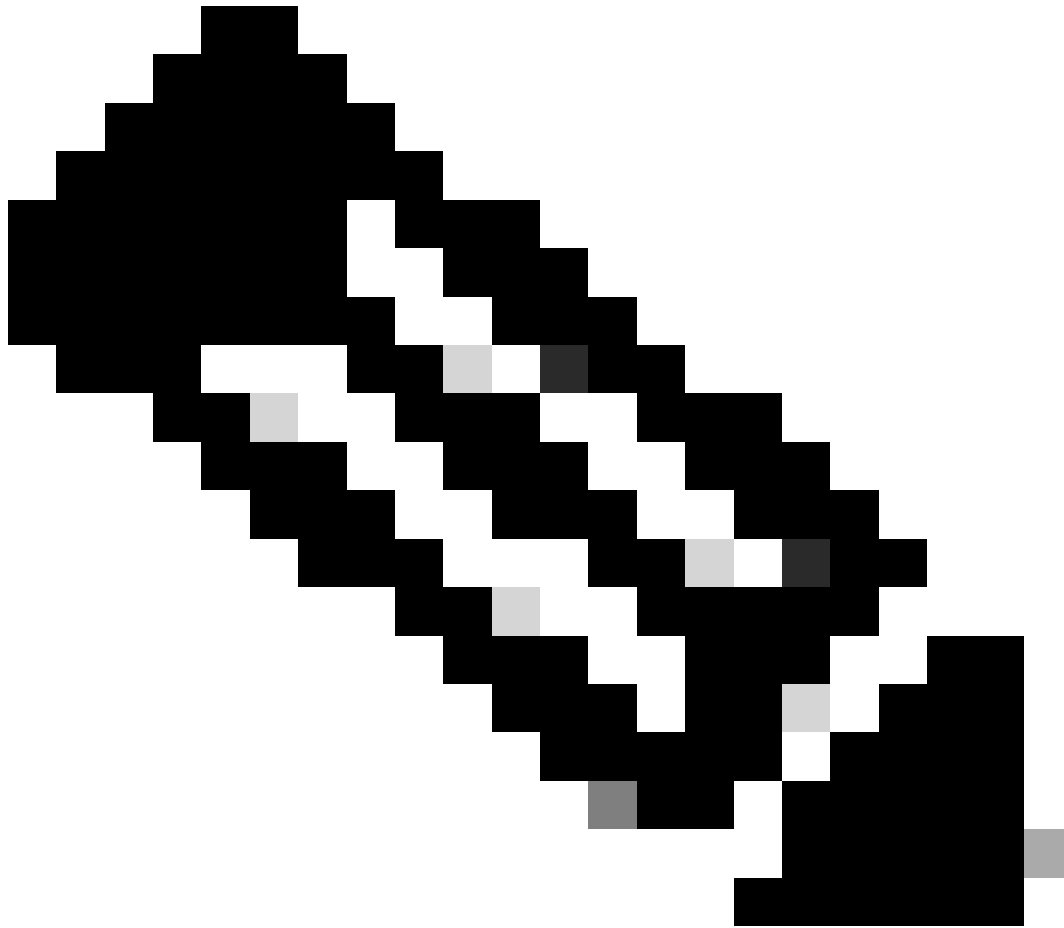
مكحلت الة مئاق ىلع اهنىوكت مت يتي الة زهجالا رورم ةكرح ىرتسو، رشننلا كنكمي، كلذ دعب نمآلا لوصولا ىلا رورملا ةكرح هجوت يتي الة (ACL) لوصولا يف:

ة: لارديفلل Conexion Events تالاصتالا ةرادا زكرم نم

<input type="checkbox"/>	Action x	Initiator IP x	Responder IP x	Application Risk x	Access Control Policy x	Ingress Interface x	Egress Interface x
▼ <input type="checkbox"/>	Allow	192.168.10.40	8.8.8.8	Medium	HOUSE	LAN	PrimaryVTI
▼ <input type="checkbox"/>	Allow	192.168.10.40	8.8.8.8	Medium	HOUSE	LAN	PrimaryVTI
▼ <input type="checkbox"/>	Allow	192.168.10.40	8.8.8.8	Medium	HOUSE	LAN	PrimaryVTI
▼ <input type="checkbox"/>	Allow	192.168.10.40	8.8.8.8	Medium	HOUSE	LAN	PrimaryVTI
▼ <input type="checkbox"/>	Allow	192.168.10.40	8.8.8.8	Medium	HOUSE	LAN	PrimaryVTI
▼ <input type="checkbox"/>	Allow	192.168.10.40	8.8.8.8	Medium	HOUSE	LAN	PrimaryVTI

نمآلا لوصولا لخاد Activity Search نم

Request	Source	Rule Identity	Destination	Destination IP	Internal IP	External IP	Action	Categories	Res
FW	⇒ HomeFTD	⇒ HomeFTD		8.8.8.8	192.168.10.40		✓ Allowed	Uncategorized	
FW	⇒ HomeFTD	⇒ HomeFTD		8.8.8.8	192.168.10.40		✓ Allowed	Uncategorized	
FW	⇒ HomeFTD	⇒ HomeFTD		8.8.8.8	192.168.10.40		✓ Allowed	Uncategorized	
FW	⇒ HomeFTD	⇒ HomeFTD		8.8.8.8	192.168.10.40		✓ Allowed	Uncategorized	
FW	⇒ HomeFTD	⇒ HomeFTD		8.8.8.8	192.168.10.40		✓ Allowed	Uncategorized	
FW	⇒ HomeFTD	⇒ HomeFTD		8.8.8.8	192.168.10.40		✓ Allowed	Uncategorized	
FW	⇒ HomeFTD	⇒ HomeFTD		8.8.8.8	192.168.10.40		✓ Allowed	Uncategorized	



إلى تاناي ب ل رورم ة ك ر ح ل ي ض ا ر ت ف ا ل ا ن م آ ل ا ل و ص و ل ا ج ه ن ح م س ي ، ا ي ض ا ر ت ف ا : ة ظ ح ا ل م ة ص ا خ د ر ا و م ء ا ش ن ا ل ا ج ا ت ح ت ، ة ص ا خ ل ا ت ا ق ي ب ط ت ل ا ل ا ل و ص و ل ا ر ي ف و ت ل . ت ن ر ت ن ا ل ا ة ص ا خ ل ا د ر ا و م ل ا ل ا ل و ص و ل ل ل و ص و ل ا ة س ا ي س ل ا ا ه ت ف ا ض ا و

نمآل لوصول ىلع تنرتنإلإ ىلإ لوصولآ جهن نيوكت

نمآل لوصولآ تامولعم ةحول ىلع جهنلأ ءاشنإ ىلإ ءاتحت، تنرتنإلإ ىلإ لوصولآ نيوكتل
كب ةصاخلا:

- قوف رقنا Secure > Access Policy

The screenshot displays a management interface. On the left, a sidebar contains a 'Secure' menu item (highlighted with a blue box), and below it, 'Monitor', 'Admin', and 'Workflows' options. The main area is titled 'Policy' and lists two policy types: 'Access Policy' (described as 'Create rules to control and secure access to private and internet destinations') and 'Data Loss Prevention Policy' (described as 'Prevent data loss/leakage with policy rules'). The 'Access Policy' item is also highlighted with a blue box.

- قوف رقنا 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

ام بسح، أي ترتخأ عي طتسي تنأ، ةياغلا لىلإو، قف نك ردصملا تنيع عي طتسي تنأ، كانه [Secure Access](#) مدختسم لىلد نم ققحتلا ىجرى. ةسايسلا لىل لكشي نأ ديرت

ت ZTNA و RA-VPN ل ةصاخلا دراوملا لىل لوصول نيوكت

لوصول تامولعم ةحول تحت الوأ دراوملا عاشن لىل جاتحت، ةصاخلا دراوملل لوصول نيوكتل [نمألا](#):

Resources > Private Resources قوف رقنا

The screenshot shows the Microsoft Entra ID console interface. On the left is a navigation pane with 'Resources' selected. The main content area is divided into three columns: 'Sources and destinations', 'Destinations', and 'Private Resources'. The 'Private Resources' section is highlighted with a blue box and contains the text: 'Define internal applications and other resources for use in access rules'.

Sources and destinations	Destinations
Registered Networks Point your networks to our servers	Internet and SaaS Resources Define destinations for internet access rules
Internal Networks Define internal network segments to use as sources in access rules	Private Resources Define internal applications and other resources for use in access rules
Roaming Devices Mac and Windows	

- ADD رقنا مٲ

للكشي نأ يلات مسقلا دجت تنأ، ليكشلتا تحت
General, Communication with Secure Access Cloud and
Endpoint Connection Methods.

ماع

General

Private Resource Name

SplunkFTD

Description (optional)

- Private Resource Name : ككبش ىل نمآلا لوصول لال خ نم هيلا لوصولا ريفوتب موقت يذلا دروملل مسا عاشن |

ةياهنلا ةطقن لاصتا بيلاسا

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 ⓘ
 ⓘ

Protocol Server Name Indication (SNI) (optional) ⓘ

Validate Application Certificate ⓘ

- **Zero Trust Connections:** رايتخاله ؤناخ ؤمالة عضو.
- **Client-based connection:** اهنيكمت ؤلاحي في Client - Secure Client ؤيطمنلا ؤدحوللا مادختسا كنكمي، ؤلاحي في Client-base ؤصوللا لالخي نم لوصوللا نيكمتل Zero Trust Module.
- **Remote Reachable Address (FQDN, Wildcard FQDN, IP Address) :** ؤمق اذلا؛ دراوملل FQDN أو IP نيوكت : مسالال لالخي DNS ؤفاضلا لالخي ؤاتحتس في FQDN نيوكت ب.
- **Browser-based connection:** ؤلاحي في ؤصوللا كنكمي، اهنيكمت ؤلاحي في (HTTPS أو HTTP لاصتا عم طقف دراوم ؤفاضلا ؤلاحي)
- **Public URL for this resource:** لالخي نم هم دختست يذلا ماعلا URL ناوع نيوكت ب مق : ؤصوللا Secure Access يحمي؛ ؤلاحي
- **Protocol:** لوكوتوربلا ديحت (HTTP أو HTTPS)

VPN connections

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

VPN Connection: RA-VPNaaS ؤصوللا نيكمتل رايتخاله ؤناخ لالعي ؤمالة عضو.

Access Policy لالخي دراوملا اذله ؤفاضلا كنكمي و Save رقنا، كلذ دع ب

لوصوللا جهن نيوكت

نم آلا لوصوللا جهن دال هنييغت لالخي ؤاتحت، دراوملا ؤاشن دنع

- **Secure > Access Policy** قوف رقنا

The screenshot shows the Microsoft 365 Security Center interface. On the left, there is a sidebar with four main sections: 'Secure' (highlighted with a blue box), 'Monitor', 'Admin', and 'Workflows'. The 'Secure' section is expanded to show 'Policy'. Under 'Policy', there are two items: 'Access Policy' (highlighted with a blue box) and 'Data Loss Prevention Policy'. The 'Access Policy' description reads: 'Create rules to control and secure access to private and internet destinations'. The 'Data Loss Prevention Policy' description reads: 'Prevent data loss/leakage with policy rules'.

- **Add > Private Resource** رقنا

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

دروملا ىلإ لوصولا ريفوتل ةيضارتفالا ميقلا نيوكتب مق ،هذه "صاخلا لوصولا" ةدعاقل مدختسملال ليلد نم ققحت ،جهنلا تانيوكت لوح ديزملا ةفرعمل

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) x

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

To

Specify one or more destinations.

SplunkFTD x

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

- Action : دروملا ىلإ لوصولا ريفوتل "حامسلا" رتخأ .
- From : دروملا ىلإ لوخدلا ليجستل همادختسإ نكمي يذلا مدختسملال دح .
- To : Secure Access لال خ نم هيلا لوصولا ديرت يذلا دروملا رتخأ .

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**

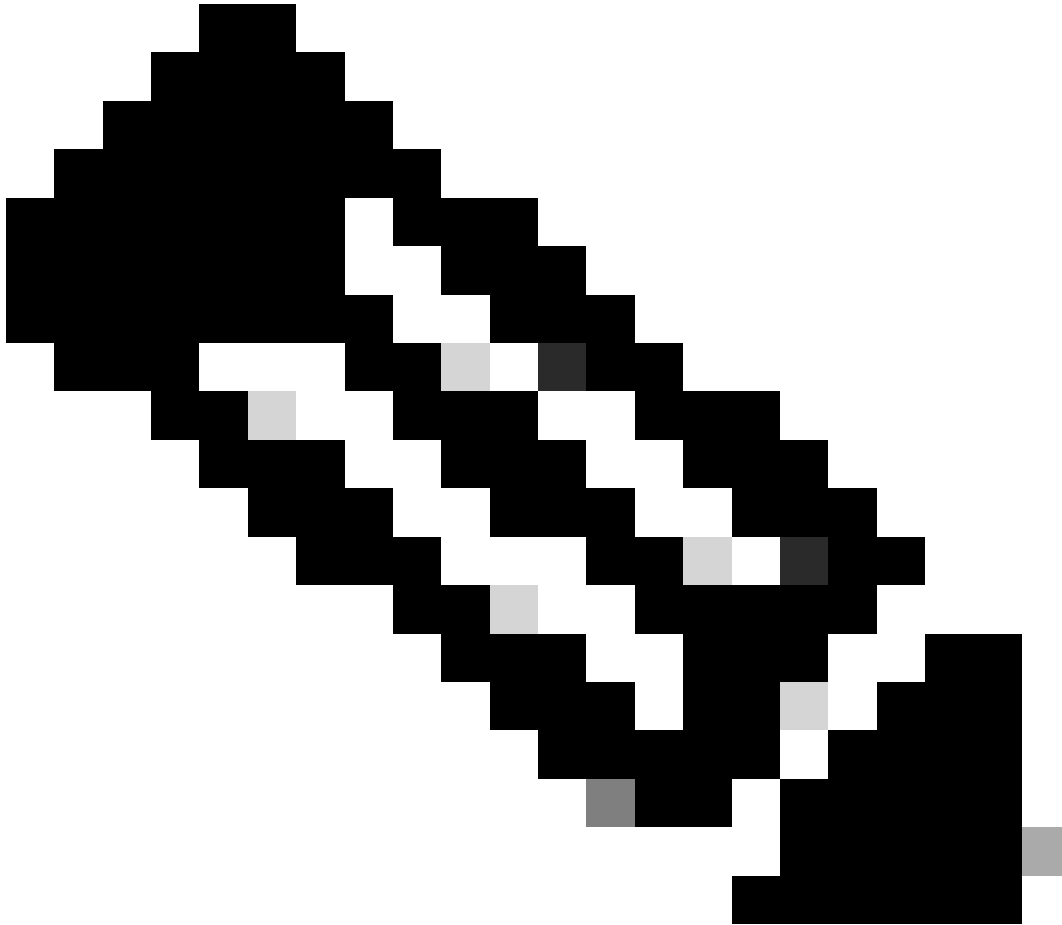
Zero Trust Browser-based Posture Profile Rule Defaults

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:** فيرعتلا فإلا فيرعتلا فلم رتخأ ليمعلا
- **Zero-Trust Browser-based Posture Profile:** فيرعتلا فلم ضرعتسم ل اساسألا لوصول رايتخأ فيرعتلا



لوصول [مدخستسملاليلد](#) نم ققحتلال عاجرلا، عضولا جهن لوح ديزملا ةفرعمل: ةظحالم نمآلا.

دراوملا ىلا لوصوللا ةلواحم كنكمي و، كب صاخلا نيوكتلاو Next Save قوف رقنا، كلذ دعب Browser Base ZTNA و Client Base ZTNA لخالخ نم كب ةصاخلا.

اهحالصإو ءاطخألا فاشكتسا

نمآلا لوصولو نمآلا ةيامحلا رادج نيبل لاصلتالا ىلا اءانتسا اءاطخألا فاشكتسال نود ةزهجألا نيبل (IPSec) ةيناثلا ةلحرملاو (IKEv2) ىلوالا ةلحرملا ءاشنإ نم ققحتلال كنكمي ةلكشم ثودح.

1 (IKEv2) ةلحرملا نم ققحتلال

ب ةصاخلا (رمأوالا رطس ةهجاو) CLI ىلع ىلاتلا رمالا ليغشت بجي 1 ةلحرملا نم ققحتلال FTD:

```
show crypto isakmp sa
```

تانايبلا زكرم ب ةصاخلا IP نيوانع ىلع بولطملا جارخالا ءاشنإ IKEv2 SAs متي، ةلالحا هذه في READY: يلى امك ةبولطملا ةلالحاو نمآلا لوصولل

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
```

ةيناثلا ةلحررلما نم ققحتلا (IPSec)

ةصاخلا (رماؤالا رطس ةهجاو) CLI ىلع ىلاتلا رمالا ليغشت ىلإ جاتحت ، ةلحررلما نم ققحتلا ب 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
```

جاتنا إيلالاتلا وه بغير ب س ي ل ام؛ ني م ئ ا ق ل ل ن ي ق ف ن ل ل ا ل ك ة ي ؤ ر ك ن ك م ي ، ر ي خ أ ل ا ج ا ر خ إ ل ا ي ف
تحت encaps و decaps ط بر ل ا

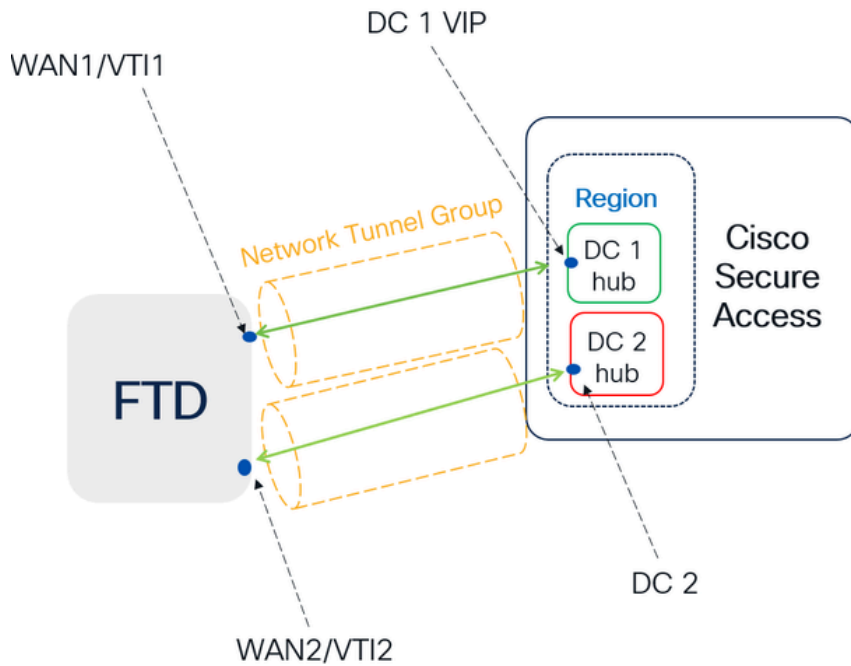
```
#pkts encaps: 71965, #pkts encrypt: 71965, #pkts digest: 71965 → Packets forwarded to Secure Access
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0 → No packets forwarded from Secure
#pkts compressed: 0, #pkts decompressed: 0 → Access to your firewall
#pkts not compressed: 71965, #pkts comp failed: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

TAC مادختساب ةلاح حتفاف ،ويرانيسلا اذه كي دل ناك اذا

يلاعلا رفاوتلا ةفيظو

يه ةباحسلا يف تانايبلا زكرم عم Secure Access لاصتا عم قافنألا ةفيظو ةكرح يقلتلا احوتم نوكتيس طقف DC 1 م كحتلا ةدحو باب نأ ينع ي ام ،"ي بلس/طشن" 1. مقرر قفنلا لازنإ متي يتح DC 2 باب قغالغإ متي ؛رورملا

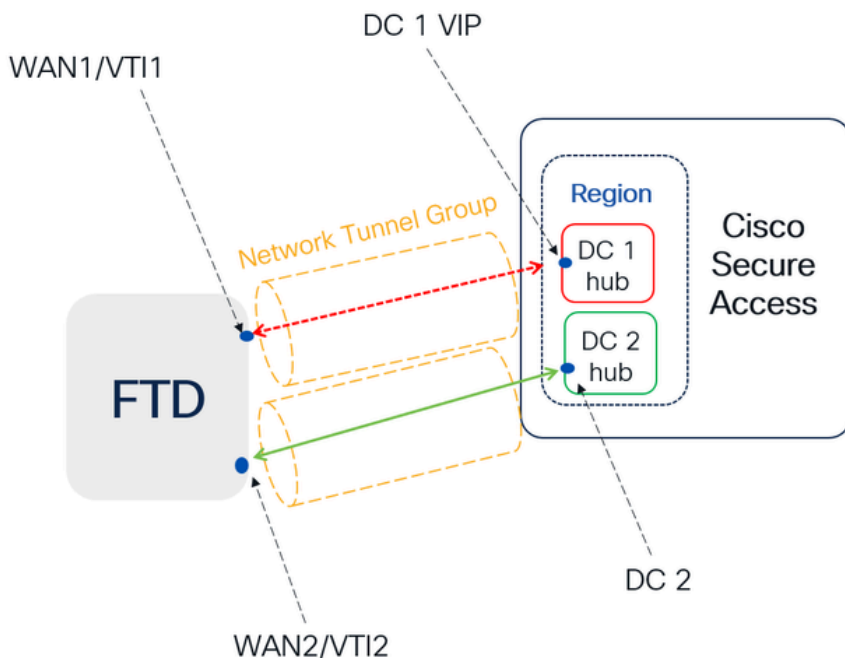
Normal Behavior



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

لوصولنا نيما تال رورملا ةكرح هي جوت نم ققحتال

ةيما حلال راج ةكبش يلع زاهجك ردصملا مدختسن، لاثملا اذه يف:

- ردصملا: 192.168.10.40
- نمآلا لوصولنا ةبقارملا (IP) 146.112.255.40 :ةهجولا

لاثم:

```
> packet-tracer input Inside tcp 192.168.2.234 32344 72.163.4.185 443
```

Command to make the packet capture

Direction must be the interface that has clients trying to access to internet

Emulation of the connection via TCP protocol from the IP 192.168.2.234 from the source PORT 32344 to the IP 72.163.4.185 to the PORT 443, which emulates the access to a webpage published on the port 443 from a user on the inside network.

:

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

جاء اليا

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

ءيش لك ناك اذا ام ةفرعمو لاصتالا لوح قاي س ءايشأل نم دي دعلا اني طعت نأ نكمي ، انه
نمأل لوصولا لىل احيحص لكشب رورملا ةكرح هيجوتل احيحص لكشب PBR نيوكت تحت

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
```

أذهو، ةهءاوا PrimaryVTI إىل إاناىبلا رورم ةكرح هىءوت ةءاعإ مءء هئا إىل 2 ةلءرمل رىشت رورم ةكرح هىءوت ةءاعإ بءى، وىرانىسلا اءه فى ئانىوكئلا إىل اءانئسا، هئاأل ءىءص VTI لالء نم "نمآلا لوصولا" إىل ئنرئناإلا.

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:

لاسرا ةيناكم | نمضي امم ، ريفش تلال اهب ضيوف تلال او رورملا ةكرح ميفيقت متي شي رورملا ةكرح قفدتل ةددحملا ةرادالال ىلع 9 ةلحرملا زكرت ، ىرخأ ةيخان نمو . نم لكشب تانايبلا ححص لكشب اهبهيجوت متي ةرفشملا رورملا ةكرح نأ دكؤي امم ، VPN IPSec قفن لخاد هؤاشن مت يذلال قفنل ربع اهب حامسلاو .

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

هيجوت PrimaryVTI ةداع | LAN نم رورملا ةكرح ةيؤر كنكمي ، قفدتلال ةجيتن ةياهن ي ف ، اهان إل لكاشم نود اهبهيجوت متي رورملا ةكرح نأ allow اءجال دكؤي . نم آلا لوصولال رورملا ةكرح

ةلص تاذا تامولعم

- [Cisco نم تاليزنتلاو ينفلا معدلا](#)
- [Cisco نم نم آلا لوصولال تاميلعت زكرم](#)
- [يرهاظلال هب قوئوملا يساسال اماظنلل ةيظمنلا ةدحولال ىلع ةماع قرظن](#)
- [Zero Trust Access Module ةيظمنلا ةدحولال](#)
- [بتكمب لصلتا . بيجتست ال ليچستلا ةمدخ اءالصل او نم آلا لوصولال اءاخأ فاشكتسأ تامولعملال ةينقت ةدعاسم](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذه Cisco تچرت
ملاعلاء انءمچ يف نيمدختسمل معدى وتحم مي دقتل ةيرشبلاو
امك ةقيد نوك تنل ةللأل ةمچرت لصف انءمچال مچرئى. ةصاغل مهتغب
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه
ىل اءءاد ةوچرلاب يصوت وتامچرتل هذه ةقदन ةتيلوئسم Cisco
Systems (رفوتم طبارلا) يلصلأل يزىلچنل دن تسمل