

ةيامح رادج مادختساب نمآلا لوصولا نيوكت Palo Alto

تايوتحمل

[ةمدقملا](#)

[ةيساسآلا تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[ةيساسآا تامولعم](#)

[نيوكتلا](#)

[نمآلا لوصولا لعلع VPN ةكبش نيوكت](#)

[قفنللا تانايب](#)

[وتلاأ ولابل لعلع قفنللا نيوكت](#)

[قفنللا ةهجاو نيوكت](#)

[IKE ريفش تفيرعت فلم نيوكت](#)

[IKE تابلابل نيوكت](#)

[IPSec ريفش تفيرعت فلم نيوكت](#)

[IPSec قافتأ نيوكت](#)

[ةسايسللا لعلع ةدنتسملا هيچوتلا ةداعل نيوكت](#)

ةمدقملا

Palo Alto ةيامح رادج مادختساب نمآلا لوصولا نيوكت ةيفيك دنتسملا اذه حضوي

ةيساسآلا تابلطتملا

- [مدختسملا ريفوت نيوكت](#)
- [ZTNA SSO ةقداصم نيوكت](#)
- [دعب نعل لوصولل VPN لعلع نمآلا لوصولا نيوكت](#)

تابلطتملا

ةيلاتلا عيضاوملاب ةفرعم كيدل نوكت نأب Cisco ي صوت

- Palo Alto 11.x رادصا ةيامح رادج
- نمآلا لوصولا
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA
- اياوز نودب انتز

ةمدختسملا تانوكملا

ىل دن تسمل اذه يف ة دراو ل تامول عمل دن تس ت

- رادص ا ة يامح رادج Palo Alto 11.x
- نم آلا لوصول
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA

ة صاخ ة يل م عم ة ئب يف ة دوج وملا ة زه آل نم دن تسمل اذه يف ة دراو ل تامول عمل اءاشن ا مت تناك اذ ا . (يضا رتفا) حوس مم نيوك تب دن تسمل اذه يف ة مدختس مل ة زه آل ا عي مج ا دب رم ا ل مل حمل ري ثا تلل كم هف نم دك ا ت ف ، لي غ ش ت ل دي ق ك ت ك ب ش

ة ي س اس ا تامول عم



CISCO

Secure

Access



paloalto®
NETWORKS

ساساً ىلع ،اهيلا لوصول ريفوتو ةصاخلا تاقببطلال ةيامل Cisco Secure Access تمم ص ققحتي و. تنرتنإلا ىلا ةكبشلا نم لاصلال نمضي هنا امك . تاكبشلا ىلع ةمئاقو يلمح ىلع ظافحلا ىلا اعمج فدهت ، ةددم ةي نم أ تاقببو بيلا ساقببطلال لال خ نم كلذ ةباحسلا ربع اهيلا لوصول دنع تامولعمل

نيوكتلا

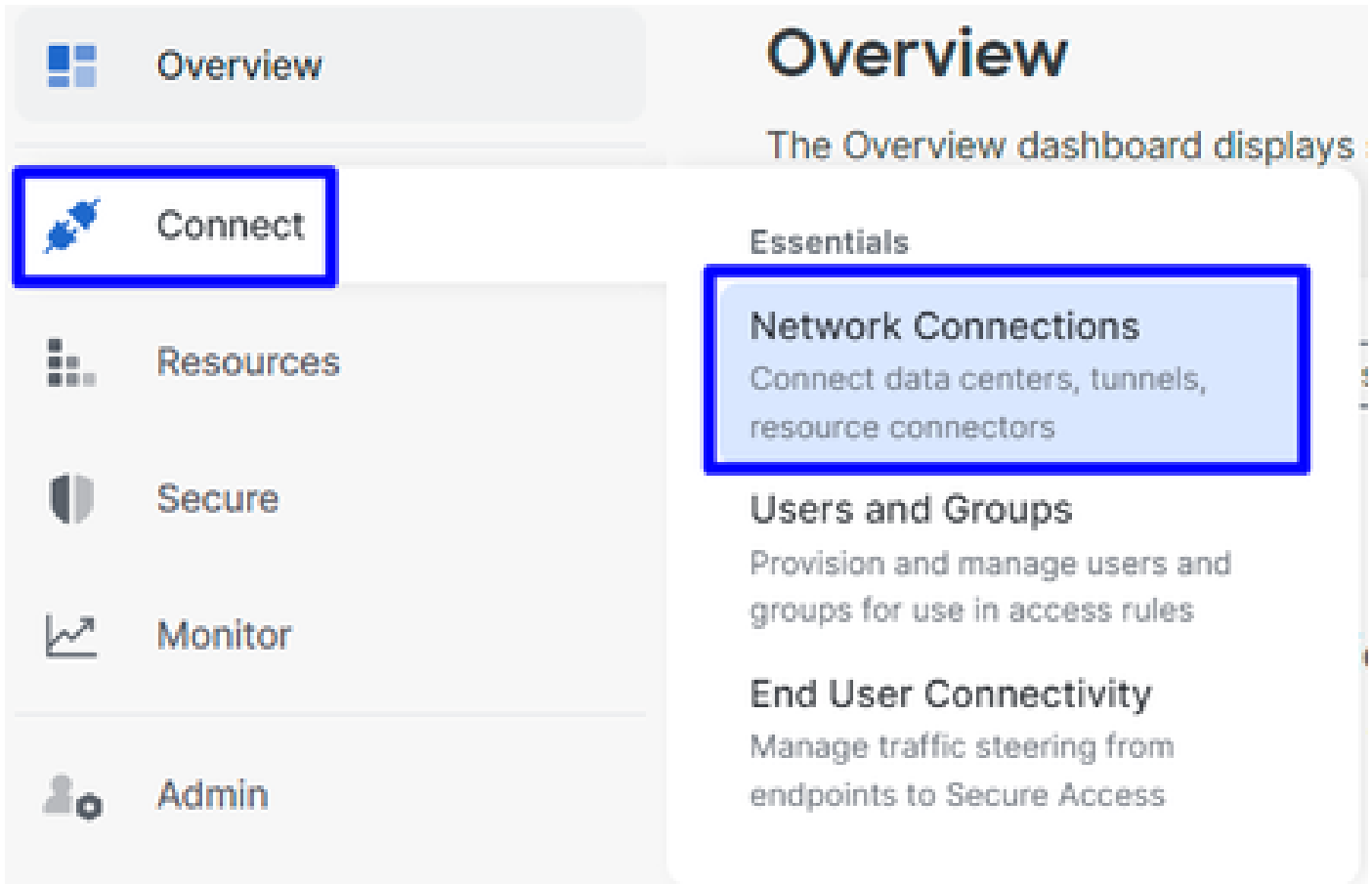
نم آلا لوصول ىلع VPN ةكبش نيوكت

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



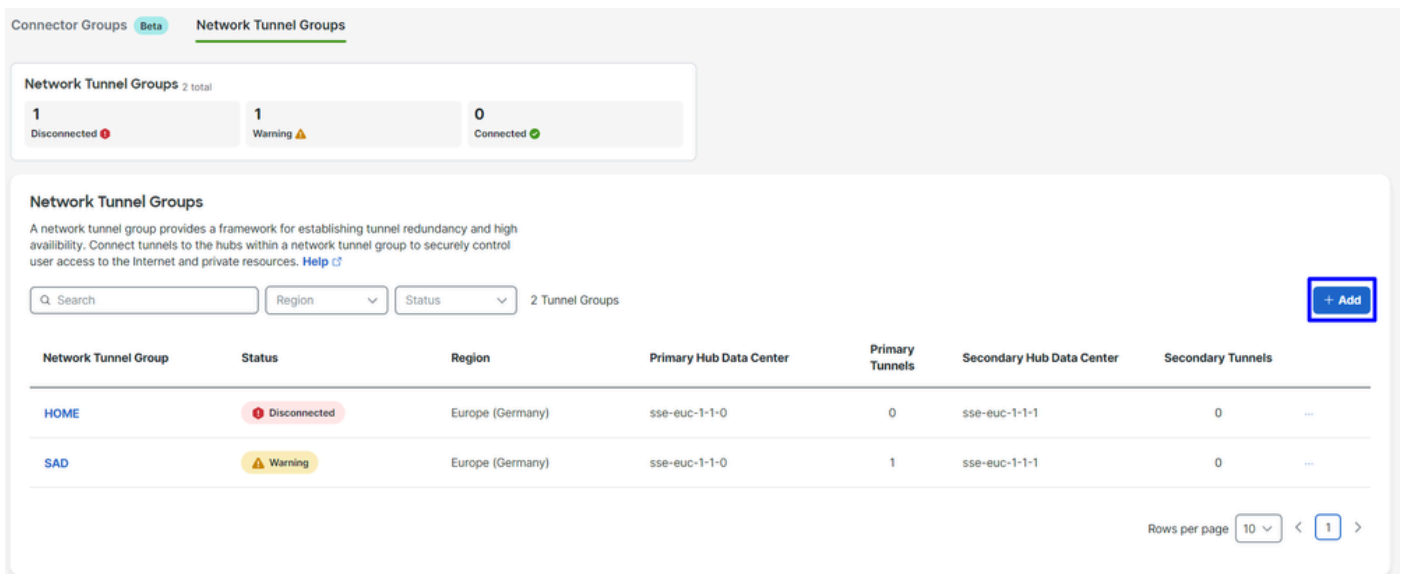
ةيسيئرلا ةحفصل - نم آلا لوصول

- قوف رقنا Connect > Network Connections



ةكبشلا تالاصتا - نمآلا لوصولا

- Add + قوف Network Tunnel Groups رقنلا تحت



ةكبشلا قف ناعومجم - نمآلا لوصولا

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

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

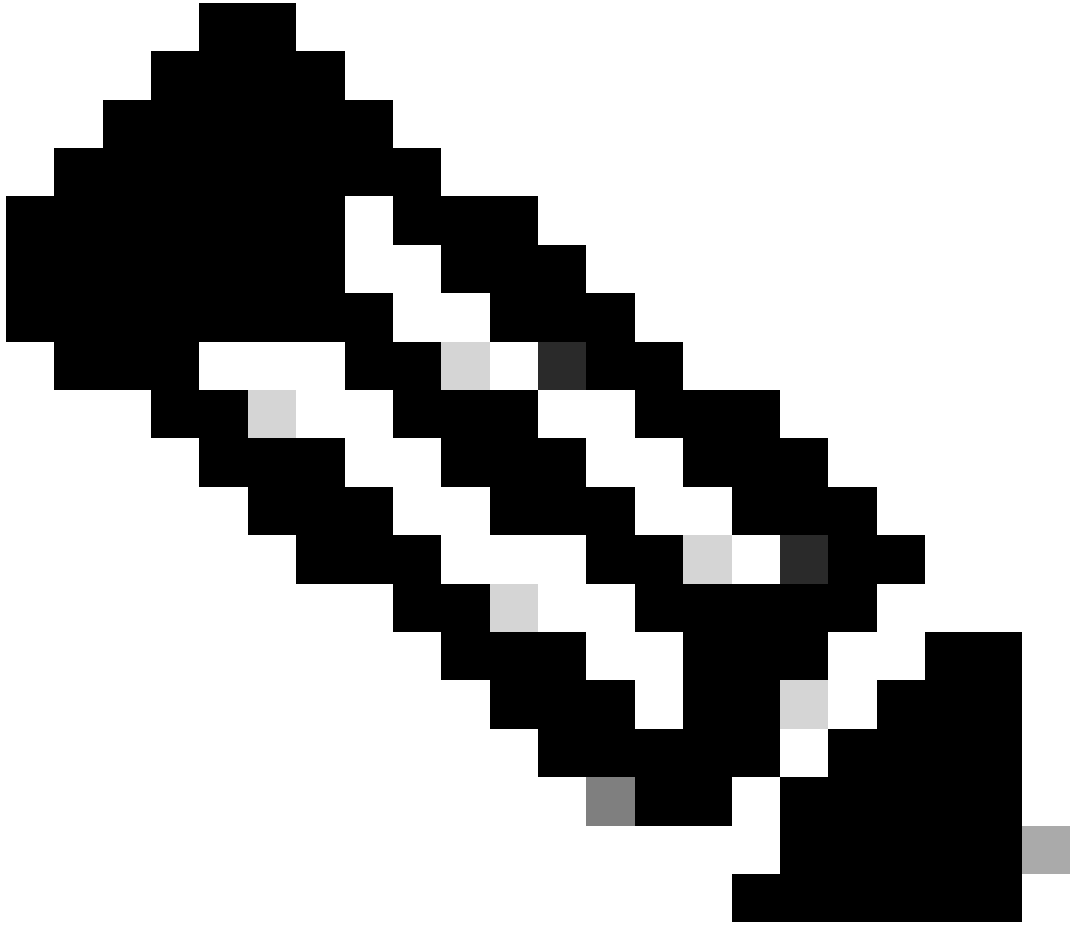
 ∨

Device Type

 ∨

[Cancel](#)

[Next](#)



ةي امحل رادج ع قوم ىل اة قطنم برق ا رتخ ا :ةظحالم

-
- Tunnel ID Format و Passphrase ني وكتب مق
 - Next ر قنا

Tunnel ID Format

Email IP Address

Tunnel ID

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

Passphrase

..... Show

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

..... Show

Cancel

Back Next

- كرح ريرمت ديرتو ةكبشلالى لى اهنيوكتب تمق يتللا ةفيضملا تائيبلا و IP نيوانع تاقاطن نيوكتب مق نم رورملا لوصولال لالخ نم رورملا
- 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.

128.66.0.0/16, 192.0.2.0/24 Add

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

هيجوتلا تاراخي - قافنألا تاعومجم - نمألا لوصولا






Configure the tunnel on، ةيلاتلا ةوطخلل تامولعمللا كلت ظفح عاجرلا، قفنلا ضرع لوح Save تامولعمللا قوف رقنلا دعب

Palo Alto.

قفلنلا تانايب

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

وتلأ ولاب ىلع قفلنلا نيوكت

قفلنلا ةهجاو نيوكت

وتلأ ولاب تامولعم ةحول ىلإ لقتنا

- Network > Interfaces > Tunnel
- Click Add

Ethernet | VLAN | Loopback | **Tunnel** | SD-V

Interfaces

- Zones
- VLANs
- Virtual Wires
- Virtual Routers
- IPSec Tunnels
- GRE Tunnels
- DHCP
- DNS Proxy
- Proxy
- GlobalProtect
- Portals
- Gateways
- MDM
- Clientless Apps

INTERFACE	MANAGEMENT PROFILE	IP ADDRESS
tunnel		none
tunnel.1		Interface_CSA
tunnel.2		169.253.0.1

+ Add - Delete PDF/CSV

- Suffix Number نبيغي وتو، Virtual Router Security Zone نبيوكت ب مق، عمئاق ال Config تحت

Tunnel Interface

Interface Name: tunnel . 1

Comment:

Netflow Profile: None

Config | IPv4 | IPv6 | Advanced

Assign Interface To

Virtual Router: Router

Security Zone: CSA

OK Cancel

- 169.254.0.1/30 م ادخستس | كنكمي، لاثم ال ل بس ىل ع. هيجوت لل ل باق ريغ IP نبيوكت ب مق، IPv4 تحت

- OK رقا

Tunnel Interface

Interface Name: tunnel . 1

Comment:

Netflow Profile: None

Config | **IPv4** | IPv6 | Advanced

IP

169.254.0.1/30

+ Add - Delete ↑ Move Up ↓ Move Down

IP address/netmask. Ex. 192.168.2.254/24

OK Cancel

ليقبل الا اذ نم عيش نيوكت نكمي، كلذ دعبو

Ethernet | VLAN | Loopback | **Tunnel** | SD-WAN

INTERFACE	MANAGEMENT PROFILE	IP ADDRESS	VIRTUAL ROUTER	SECURITY ZONE	FEATURES
tunnel		none	none	CSA	
tunnel.1		169.254.0.1/30	Router	CSA	
tunnel.2		169.253.0.1	Router	CSA	

Configure IKE Crypto Profile، الالاتل ةوطخلاب ةعباتمل او نيوكتال ظفحل Commit رقنلا كنكمي ف، وحنلا اذ ع هنيوكت ب تمق اذا Profile.

IKE فيرقت فيرقت فلم نيوكت

لىلقنا، ريرقتال فيرقت فلم نيوكت

- Network > Network Profile > IKE Crypto
- Add رقنا

PA-VM DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK

Clientless App Groups QoS LLDP Network Profiles GlobalProtect IPSec Crypt IKE Gateways IPSec Crypto IKE Crypto Monitor Interface Mgmt Zone Protection QoS Profile LLDP Profile BFD Profile SD-WAN Interface Profile

4 items

<input type="checkbox"/>	NAME	ENCRYPTION	AUTHENTICATI...	DH GROUP	KEY LIFETI
<input type="checkbox"/>	default	aes-128-cbc, 3des	sha1	group2	8 hours
<input type="checkbox"/>	Suite-B-GCM-128	aes-128-cbc	sha256	group19	8 hours
<input type="checkbox"/>	Suite-B-GCM-256	aes-256-cbc	sha384	group20	8 hours
<input type="checkbox"/>	CSAIKE	aes-256-gcm	non-auth	group19	8 hours

+ Add - Delete Clone PDF/CSV

• تالالت الامل عمل نيوك ت:

◦ Name: فف رتال فلم فف رتال مسا نيوك ت ب مق

- DH GROUP: 19 ةوم جم ال
- AUTHENTICATION: ةق داصم ال رفغ
- ENCRYPTION: زارط AES-256-GCM
- Timers

◦ Key Lifetime: 8 تاع اس

• IKEv2 Authentication:0

• OK قوف رقنا، عفش لك ةئيه ت دع ب

IKE Crypto Profile

Name: CSAIKE

DH GROUP	ENCRYPTION
<input type="checkbox"/> group19	<input type="checkbox"/> aes-256-gcm

+ Add - Delete ↑ Move Up ↓ Move Down

AUTHENTICATION	Timers
<input type="checkbox"/> non-auth	Key Lifetime: Hours <input type="text" value="8"/> Minimum lifetime = 3 mins IKEv2 Authentication Multiple: <input type="text" value="0"/>

+ Add - Delete ↑ Move Up ↓ Move Down

OK Cancel

Configure IKE Gateways، الةوطخاللة عة باتملاو نيوكتلا ظفح Commit رقنلا كنكميف، وحنلا اذه عل هنيوكتت تمق اذا Gateways.

IKE تاباوب نيوكت

IKE تاباوب نيوكتل

- Network > Network Profile > IKE Gateways
- Add رقنا

PA-VM DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK

2 items

	NAME	PEER ADDRESS	Local Address		ID
			INTERFACE	IP	
<input checked="" type="checkbox"/>	CSA_IKE_GW	18.156.145.74	ethernet1/1	192.168.0.204/24	18.156.145.74
<input type="checkbox"/>	CSA_IKE_GW2	3.120.45.23	ethernet1/1	192.168.0.204/24	3.120.45.23

Add Delete Enable Disable PDF/CSV

• ةةللالل تاملل عملال نل وكت :

◦ Name: مق نل وكت ب مسا نل وكت ب مق .

- **Version** : طقف IKEv2 عسو :
- Address Type : IPv4
- **Interface** : تنرتنلال WAN ةهجاو ددح .
- Local IP Address: تنرتنلال WAN ةهجاو ب صال ال IP ددح .
- **Peer IP Address Type** : IP
- Peer Address: ةوطال [قفن تانابل](#) ف مدقملاو ، Primary IP Datacenter IP Address ب صال ال IP مادختس | .
- Authentication: اقبسم كرتشم حاتفم :
- Pre-shared Key : ةوطال [قفن تانابل](#) ف يطعم passphrase مادختس | .
- **Confirm Pre-shared Key** : ةوطال [قفن تانابل](#) ف يطعم passphrase مادختس | .
- **Local Identification** : ةوطال ف يطعمل ال Primary Tunnel ID مادختس او User FQDN (Email address) رائلخ | : [قفنلال تانابل](#) .
- **Peer Identification** : Primary IP Datacenter IP Address مادختس او رائلخ | IP Address .

General | Advanced Options

Name	CSA_IKE_GW		
Version	IKEv2 only mode		
Address Type	<input checked="" type="radio"/> IPv4	<input type="radio"/> IPv6	
Interface	ethernet1/1		
Local IP Address	192.168.0.204/24		
Peer IP Address Type	<input checked="" type="radio"/> IP	<input type="radio"/> FQDN	<input type="radio"/> Dynamic
Peer Address	18.156.145.74		
Authentication	<input checked="" type="radio"/> Pre-Shared Key	<input type="radio"/> Certificate	
Pre-shared Key	●●●●●●●●		
Confirm Pre-shared Key	●●●●●●●●		
Local Identification	User FQDN (email address)	paloalto@	-sse.cisco.c
Peer Identification	IP address	18.156.145.74	
Comment			

OK

Cancel

- Advanced Options رقنا

- **Enable NAT Traversal**

- [IKE ريفشت فيرعت فلم نيوكتب مق](#)، اهواشن امت يت ال **IKE Crypto Profile** ةوطخل ددح
- **Liveness Check** ل راي تخالالا ةناخ ديدحت
- **OK** رقنا

General | **Advanced Options**

Common Options

 Enable Passive Mode Enable NAT Traversal

IKEv2

IKE Crypto Profile CSAIKE

 Strict Cookie Validation Liveness Check

Interval (sec) 5

OK

Cancel

إذا Configure IPSEC Crypto، الة ووطخال اب ة عبات م ل او ني وكت ال ظ فحل Commit ر قن ال كن كم يف ، وحن ال اذه ل ع من ني وكت ب تم ق اذا Crypto.

IPSec ر يف ش ت في ر ع ت ف ل م ني وكت

ل IKE، ت اب او ب ني وكت ل Network > Network Profile > IPSEC Crypto ل ل ق ت نا

- Add ر ق نا

PA-VM DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK

Clientless App Groups 4 items

QoS
LLDP
Network Profiles
GlobalProtect IPSec Crypt
IKE Gateways
IPSec Crypto
IKE Crypto
Monitor
Interface Mgmt
Zone Protection
QoS Profile
LLDP Profile
bfd Profile
SD-WAN Interface Profile

<input type="checkbox"/>	NAME	ESP/AH	ENCRYPTI...	AUTHENTI...	DH GROUP	LIFETIME	LIFE
<input type="checkbox"/>	default	ESP	aes-128-cbc, 3des	sha1	group2	1 hours	
<input type="checkbox"/>	Suite-B-GCM-128	ESP	aes-128-gcm	none	group19	1 hours	
<input type="checkbox"/>	Suite-B-GCM-256	ESP	aes-256-gcm	none	group20	1 hours	
<input type="checkbox"/>	CSA-IPsec	ESP	aes-256-gcm	sha256	no-pfs	1 hours	

+ Add - Delete Clone PDF/CSV

• ﺗﻴﻮﻧﺔ ﺗﺎﻣﻞ ﻋﻤﻞ ﺍﻟﻨﻴﻮﻧﺔ:

◦ **Name:** ﻧﻤﺎﻟﺔ ﻟﻮﺼﻮﻟﻞ IPsec ﻓﻴﺮﻋﺘﻪ ﻓﻠﻢ ﻓﻴﺮﻋﺘﻞ ﻣﺴﺎ ﻣﺎﺩﺧﺘﺴﺎ:

- IPSec Protocol: ESP
- **ENCRYPTION:** ﺯﺍﺭﻃﺔ AES-256-GCM
- DH Group: ﻧﻮﺩﺏ PFS، ﻋﺪﺍﻭﻋﺔ ﻋﺎﺳﺔ

• OK ﺭﻗﻨﺎ

IPSec Crypto Profile ?

Name

IPSec Protocol **ESP**

ENCRYPTION

aes-256-gcm

AUTHENTICATION

sha256

DH Group **no-pfs**

Lifetime **Hours**

Minimum lifetime = 3 mins

Enable

Lifeseize **MB**

Recommended lifeseize is 100MB or greater

إذا تم إعداد التكوين، فسيتم إنشاء النفق. بعد ذلك، يمكنك إجراء التغييرات على النفق. انقر على **Commit** لحفظ التغييرات. إذا كنت بحاجة إلى تغيير الإعدادات، فانقر على **Cancel** لإلغاء التغييرات.

تكوين النفق IPSec

في صفحة **Network > IPSec Tunnels**، انقر على **IPSec Tunnels**، انقر على

- **Add** زر

PA-VM DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK

Interfaces
Zones
VLANs
Virtual Wires
Virtual Routers
IPSec Tunnels
GRE Tunnels
DHCP
DNS Proxy
Proxy
GlobalProtect
Portals
Gateways
MDM
Clientless Apps
Clientless App Groups
QoS
LLDP
Network Profiles
GlobalProtect IPSec Gateway

	NAME	STATUS	TYPE	IKE Gateway/Satellite				INTERFA...
				INTERFA...	LOCAL IP	PEER ADDRESS	STATUS	
<input type="checkbox"/>	CSA	● Tunnel Info	Auto Key	ethernet...	192.168...	18.156.1...	● IKE Info	tunnel.1
<input type="checkbox"/>	CSA2	● Tunnel Info	Auto Key	ethernet...	192.168...	3.120.45...	● IKE Info	tunnel.2

+ Add - Delete Enable Disable PDF/CSV

• قىة اللات الل تامل عمل انى وكت :

◦ **Name:** نم آل لوصول ق فن دى دحت ل مسا مادختس |

• **Tunnel Interface:** ق فن ل ءه جاو رتخ ء ءو طخل ال ع اهنى وكت مت يتل ق فن ل ءه جاو رتخ

• **Type:** ى ئاقتل حات فم

• **Address Type:** IPv4

• **IKE Gateways:** ءو طخل ال ع اهنى وكت مت يتل ال IKE ت اباوب رتخ [IKE ت اباوب نى وكت ب مق](#).

• **IPsec Crypto Profile:** ءو طخل ال ع اهنى وكت مت يتل ال IKE ت اباوب رتخ [رى فشت فى رعت فلم نى وكت ب مق و](#) [IPsec](#)

• **Advanced Options** ل راي ت الخ ال ءناخ دى دحت

◦ **IPSec Mode Tunnel:** ق فن ل راي ت الخ |

- OK رقمنا

IPSec Tunnel

General | Proxy IDs

Name: CSA

Tunnel Interface: tunnel.1

Type: Auto Key Manual Key GlobalProtect Satellite

Address Type: IPv4 IPv6

IKE Gateway: CSA_IKE_GW

IPSec Crypto Profile: CSA-IPsec

Show Advanced Options

Enable Replay Protection Anti Replay Window: 1024

Copy ToS Header

IPSec Mode: Tunnel Transport

Add GRE Encapsulation

Tunnel Monitor

Destination IP:

Profile: None

Comment:

OK **Cancel**

Configure Policy Based Forwarding. ةوطخلال عم ةعباتملا كنكمي، حاجنب كب ةصاخال VPN ةكبش ءاشنا مت نآلا

ةسايسلا لىل ةدنتسملل هيحوتل ةداعل نيوكت

Policy Based Forwarding لىل لقتنل **Policy Based Forwarding**، نيوكتلل

- Add رقمنا

- Destination/Application/Service

- Destination Address: نام آلا لوصولا نيوانع تاقاطن دي دحت كنكمي وأ، يأك اهكرت كنكمي (100.64.0.0/10)

- Forwarding

- Action: مأمألا لىل

- Egress Interface: قفنلأه جاوني وكتب مق، ةوطخلال لىلع اهني وكت مت يتلأ قفنلأه جاورتخأ

- Next Hop: None

- OK و Commit رقنا

Policy Based Forwarding Rule ?

General | Source | Destination/Application/Service | Forwarding

Name

Description

Tags

Group Rules By Tag

Audit Comment

[Audit Comment Archive](#)

Policy Based Forwarding Rule



General | **Source** | Destination/Application/Service | Forwarding

Type	Zone	<input type="checkbox"/> Any	any
<input type="checkbox"/> ZONE ^	<input type="checkbox"/> SOURCE ADDRESS ^	<input type="checkbox"/> SOURCE USER ^	
<input type="checkbox"/> LAN	<input type="checkbox"/> 192.168.30.2		
<input type="checkbox"/> LAN2	<input type="checkbox"/> 192.168.40.3		
<input type="button" value="+ Add"/> <input type="button" value="- Delete"/>	<input type="button" value="+ Add"/> <input type="button" value="- Delete"/>	<input type="button" value="+ Add"/> <input type="button" value="- Delete"/>	

Negate

Policy Based Forwarding Rule



General | Source | **Destination/Application/Service** | Forwarding

<input checked="" type="checkbox"/> Any	<input checked="" type="checkbox"/> Any	any
<input type="checkbox"/> DESTINATION ADDRESS v	<input type="checkbox"/> APPLICATIONS ^	<input type="checkbox"/> SERVICE ^
<input type="button" value="+ Add"/> <input type="button" value="- Delete"/>	<input type="button" value="+ Add"/> <input type="button" value="- Delete"/>	<input type="button" value="+ Add"/> <input type="button" value="- Delete"/>

Negate

Policy Based Forwarding Rule

General | Source | Destination/Application/Service | **Forwarding**

Action: Forward

Egress Interface: tunnel.1

Next Hop: None

Monitor

Profile: [Empty]

Disable this rule if nexthop/monitor ip is unreachable

IP Address: [Empty]

Enforce Symmetric Return

NEXT HOP ADDRESS LIST

[Empty List]

+ Add - Delete

Schedule: None

OK Cancel

أو RA-VPN نيوكت عباتم بجي و، قفالن ااشن نكمي، راسملا نيوكت دعبو، Palo Alto على هنيوكت مت عيش لك كي دل نآلا
 نآلا لوصول تامولعم ةحول على ليمعلا إلى ةدنتسملا ZTA و، ضرعتسملا إلى ةدنتسملا ZTA.

