

Configuración del acceso seguro con el firewall de Palo Alto

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Configuración de la VPN en Secure Access](#)

[Datos del túnel](#)

[Configuración del túnel en Palo Alto](#)

[Configuración de la interfaz de túnel](#)

[Configurar perfil criptográfico IKE](#)

[Configuración de gateways IKE](#)

[Configurar perfil criptográfico IPSEC](#)

[Configuración de túneles IPsec](#)

[Configurar el reenvío basado en políticas](#)

Introducción

Este documento describe cómo configurar Secure Access con el Firewall de Palo Alto.

Prerequisites

- [Configurar aprovisionamiento de usuarios](#)
- [Configuración de Autenticación SSO de ZTNA](#)
- [Configurar acceso seguro VPN de acceso remoto](#)

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Firewall de la versión 11.x de Palo Alto
- Acceso seguro
- Cisco Secure Client - VPN
- Cisco Secure Client: ZTNA
- ZTNA sin cliente

Componentes Utilizados

La información de este documento se basa en:

- Firewall de la versión 11.x de Palo Alto
- Acceso seguro
- Cisco Secure Client - VPN
- Cisco Secure Client: ZTNA

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes



CISCO

Secure

Access



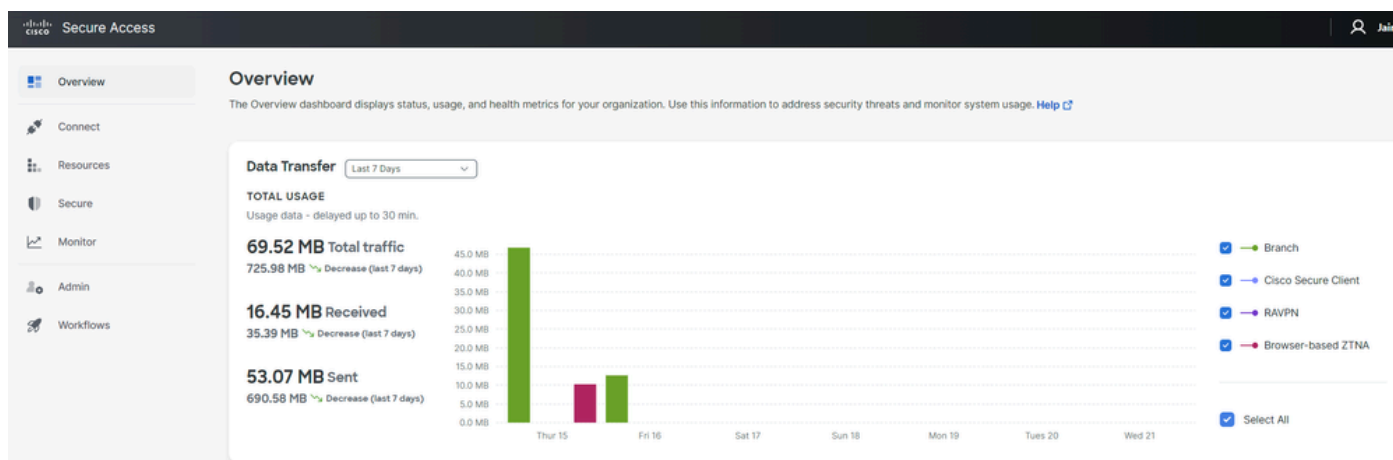
paloalto[®]
NETWORKS

Cisco ha diseñado Secure Access para proteger y proporcionar acceso a aplicaciones privadas, tanto in situ como basadas en la nube. También protege la conexión de la red a Internet. Esto se consigue mediante la implementación de varios métodos y capas de seguridad, todo ello con el objetivo de preservar la información a medida que acceden a ella a través de la nube.

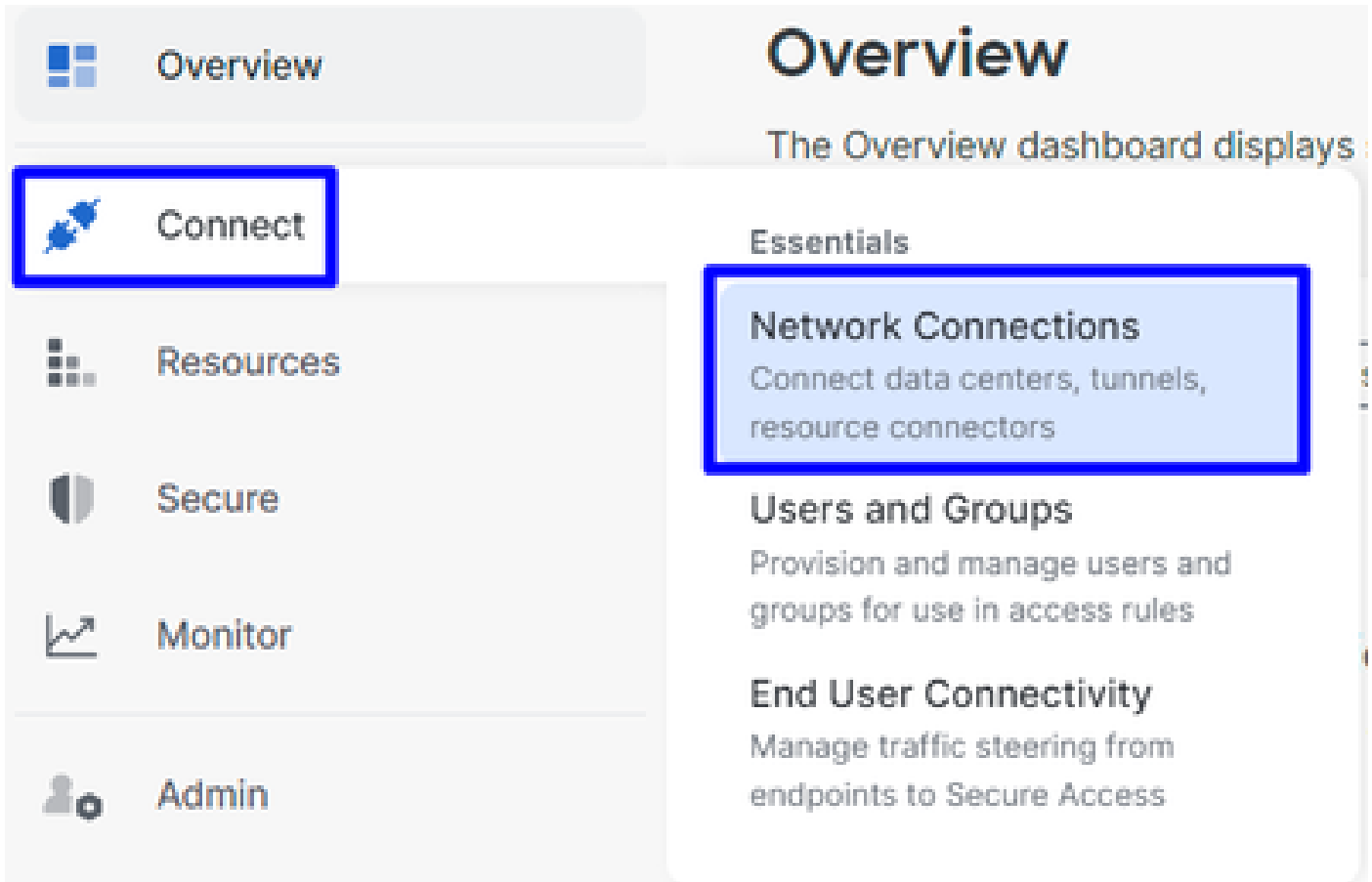
Configurar

Configuración de la VPN en Secure Access

Vaya al panel de administración de [Secure Access](#).

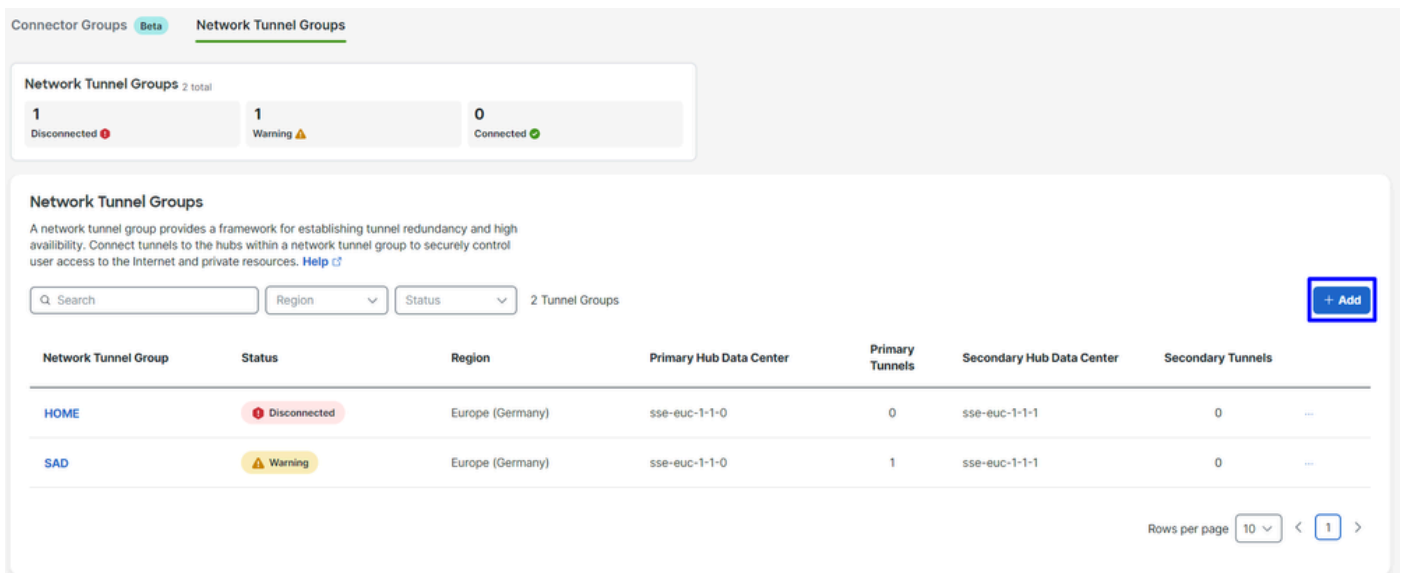


- Haga clic en **Connect > Network Connections**



Acceso seguro - Conexiones de red

- En Network Tunnel Groups haga clic en + Add



Acceso seguro - Grupos de túnel de red

- Configurar Tunnel Group Name, Regiony Device Type
- Haga clic en **Next**

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

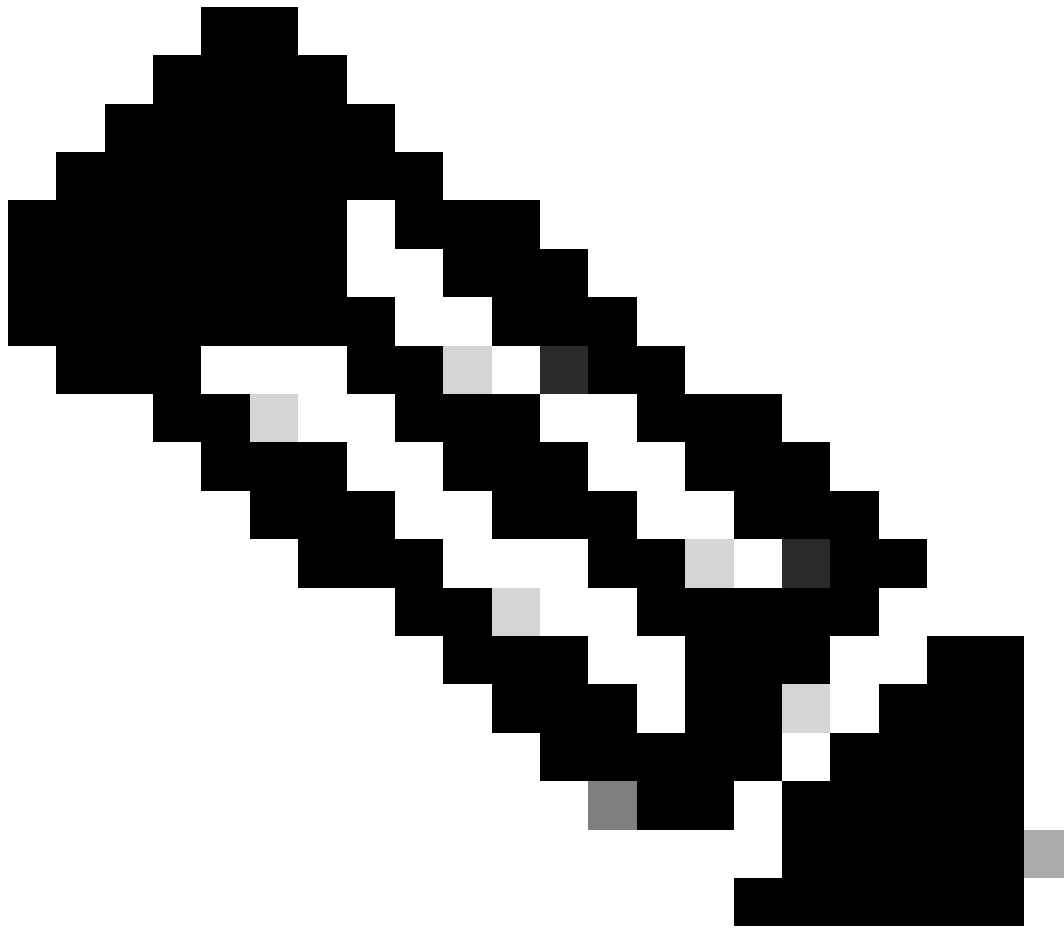
 ∨

Device Type

 ∨

[Cancel](#)

[Next](#)



Nota: Seleccione la región más cercana a la ubicación del firewall.

-
- Configure el Tunnel ID Format y Passphrase
 - Haga clic en Next

Tunnel ID Format

Email IP Address

Tunnel ID

@<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](#)

- Configure los rangos de direcciones IP o los hosts que ha configurado en la red y que desea que el tráfico pase a través de Secure Access
- Haga clic en **Save**

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.

[Add](#)

✕ ✕

Dynamic routing

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

[Cancel](#)

[Back](#)






[Save](#)

Acceso seguro - Grupos de túnel - Opciones de routing

Después de hacer clic en **Save** la información sobre el túnel se muestra, guarde esa información para el siguiente paso, **Configure the tunnel on Palo Alto**.

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	

Configuración del túnel en Palo Alto

Configuración de la interfaz de túnel

Vaya al panel de Palo Alto.

- Network > Interfaces > Tunnel
- Click Add

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

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

- En Config menú, configure el Virtual Router, Security Zone y asigne un Suffix Number

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

- En IPv4, configure una dirección IP no enrutable. Por ejemplo, puede utilizar 169.254.0.1/30
- Haga clic en OK

Tunnel Interface ?

Interface Name .

Comment

Netflow Profile

Config | **IPv4** | IPv6 | Advanced

<input type="checkbox"/>	IP
<input type="checkbox"/>	169.254.0.1/30

IP address/netmask. Ex. 192.168.2.254/24

Después de eso, puede tener algo como esto configurado:

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	

Si la tiene así configurada, puede hacer clic en **Commit** para guardar la configuración y continuar con el siguiente paso, Configure IKE Crypto Profile.

Configurar perfil criptográfico IKE

Para configurar el perfil criptográfico, vaya a:

- Network > Network Profile > IKE Crypto
- Haga clic en Add

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	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

- Configure los siguientes parámetros:
 - **Name:** configure un nombre para identificar el perfil.
 - **DH GROUP:** grupo19
 - **AUTHENTICATION:** sin autenticación
 - **ENCRYPTION:** aes-256-gcm
 - Timers
 - Key Lifetime: 8 horas
 - **IKEv2 Authentication:**0
- Una vez configurado todo, haga clic en **OK**

IKE Crypto Profile

Name

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

+ Add - Delete ↑ Move Up ↓ Move Down

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

+ Add - Delete ↑ Move Up ↓ Move Down

Si la tiene configurada de esta forma, puede hacer clic en **Commit** para guardar la configuración y continuar con el siguiente paso: Configure IKE Gateways.

Configuración de gateways IKE

Para configurar puertas de enlace IKE

- Network > Network Profile > IKE Gateways
- Haga clic en Add

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

- Configure los siguientes parámetros:
 - Name: configure un nombre para identificar las puertas de enlace Ike.
 - **Version** : modo solo IKEv2
 - Address Type :IPv4
 - **Interface** : seleccione la interfaz WAN de Internet.
 - Local IP Address: seleccione la IP de la interfaz WAN de Internet.
 - **Peer IP Address Type** :IP
 - Peer Address: Utilice la dirección IP de Primary IP Datacenter IP Address, indicada en el paso [Tunnel Data](#).
 - Authentication: clave precompartida
 - Pre-shared Key : Utilice el **passphrase** especificado en el paso [Tunnel Data](#).
 - **Confirm Pre-shared Key** : Utilice el **passphrase** especificado en el paso [Tunnel Data](#).
 - **Local Identification** : Elija User FQDN (Email address) y utilice el **Primary Tunnel ID** dato del paso, [Tunnel Data](#).
 - **Peer Identification** : IP Address Elija y utilice el Primary IP Datacenter 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			

- Haga clic en Advanced Options

- **Enable NAT Traversal**

- Seleccione el perfil **IKE Crypto Profile** creado en el paso [Configure IKE Crypto Profile](#)
- Marque la casilla de verificación de **Liveness Check**
- Haga clic en **OK**

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

Si la tiene configurada de esta forma, puede hacer clic en **Commit** para guardar la configuración y continuar con el siguiente paso: Configure IPSEC Crypto.

Configurar perfil criptográfico IPSEC

Para configurar puertas de enlace IKE, vaya a Network > Network Profile > IPSEC Crypto

- Haga clic en Add

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

- Configure los siguientes parámetros:
 - **Name:** utilice un nombre para identificar el perfil IPSec de acceso seguro
 - IPSec Protocol: ESP
 - **ENCRYPTION:** aes-256-gcm
 - DH Group: no-pfs, 1 hora
- Haga clic en OK

IPSec Crypto Profile

Name: CSA-IPsec

IPSec Protocol: ESP

ENCRYPTION

- aes-256-gcm

AUTHENTICATION

- sha256

DH Group: no-pfs

Lifetime: Hours 1

Minimum lifetime = 3 mins

Enable

Lifeseize: MB [1 - 65535]

Recommended lifeseize is 100MB or greater

OK Cancel

Si la tiene configurada de esta forma, puede hacer clic en **Commit** para guardar la configuración y continuar con el siguiente paso: Configure IPSec Tunnels.

Configuración de túneles IPSec

Para configurar **IPSec Tunnels**, vaya a Network > IPSec Tunnels.

- Haga clic en Add

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

- Configure los siguientes parámetros:
 - **Name:** utilice un nombre para identificar el túnel de acceso seguro
 - **Tunnel Interface:** Seleccione la interfaz de túnel configurada en el paso [Configurar la interfaz de túnel](#).
 - **Type:** Clave automática
 - **Address Type:** IPv4
 - **IKE Gateways:** Seleccione las puertas de enlace IKE configuradas en el paso [Configure IKE Gateways](#).
 - **IPsec Crypto Profile:** Seleccione las puertas de enlace IKE configuradas en el paso [Configure IPSEC Crypto Profile](#)
 - Marque la casilla de verificación de **Advanced Options**
 - **IPSec Mode Tunnel:** seleccione Túnel.

- Haga clic en OK

IPSec Tunnel ?

General | Proxy IDs

Name

Tunnel Interface

Type Auto Key Manual Key GlobalProtect Satellite

Address Type IPv4 IPv6

IKE Gateway

IPSec Crypto Profile

Show Advanced Options

Enable Replay Protection Anti Replay Window

Copy ToS Header

IPSec Mode Tunnel Transport

Add GRE Encapsulation

Tunnel Monitor

Destination IP

Profile

Comment

Ahora que la VPN se ha creado correctamente, puede continuar con el paso **Configure Policy Based Forwarding**.

Configurar el reenvío basado en políticas

Para configurar **Policy Based Forwarding**, vaya a Políticas > Policy Based Forwarding.

- Haga clic en Add

PA-VM DASHBOARD ACC MONITOR **POLICIES**

NAT
QoS
Policy Based Forwarding

Policy Optimizer

Rule Usage

- Unused in 30 days 0
- Unused in 90 days 0
- Unused 0

	NAME	TAGS	ZONE/INTERFA
1	CSA	none	LAN LAN2

Object : Addresses + **+** Add - Delete Clone Enable Disable

- Configure los siguientes parámetros:

- General

- **Name:** utilice un nombre para identificar el acceso seguro, el reenvío de base de políticas (routing por origen)

- Source

- **Zone:** seleccione las zonas desde las que tiene planes para enrutar el tráfico en función del origen

- **Source Address:** configure el host o las redes que desea utilizar como origen.

- **Source Users:** configure los usuarios a los que desea enrutar el tráfico (sólo si procede).

- Destination/Application/Service

- Destination Address: puede dejarlo como Any (Cualquiera) o puede especificar los intervalos de direcciones de Secure Access (100.64.0.0/10)

- Forwarding

- **Action:**Reenvío

- **Egress Interface:** Seleccione la interfaz de túnel configurada en el paso [Configurar la interfaz de túnel](#).

- **Next Hop:**Ninguno

- HagaOK clic y Commit

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

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).