

使用Palo Alto防火牆配置安全訪問

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[在安全訪問上配置VPN](#)

[通道資料](#)

[在Palo Alto上配置隧道](#)

[配置隧道介面](#)

[配置IKE加密配置檔案](#)

[配置IKE網關](#)

[配置IPSEC加密配置檔案](#)

[配置IPSec隧道](#)

[配置基於策略的轉發](#)

簡介

本文檔介紹如何使用Palo Alto防火牆配置安全訪問。

必要條件

- [設定使用者啟動設定](#)
- [ZTNA SSO身份驗證配置](#)
- [配置遠端訪問VPN安全訪問](#)

需求

思科建議您瞭解以下主題：

- Palo Alto 11.x版防火牆
- 安全存取
- Cisco安全使用者端- VPN
- 思科安全使用者端- ZTNA
- 無客戶端ZTNA

採用元件

本文檔中的資訊基於：

- Palo Alto 11.x版防火牆

- 安全存取
- Cisco安全使用者端- VPN
- 思科安全使用者端- ZTNA

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊



安全訪問- Palo Alto

思科設計了安全訪問，可保護並提供對內部和基於雲的私有應用的訪問。它還保護從網路到 Internet 的連線。這透過實施多種安全方法和層來實現，所有這些方法都旨在保護透過雲訪問資訊時

所需的資訊。

設定

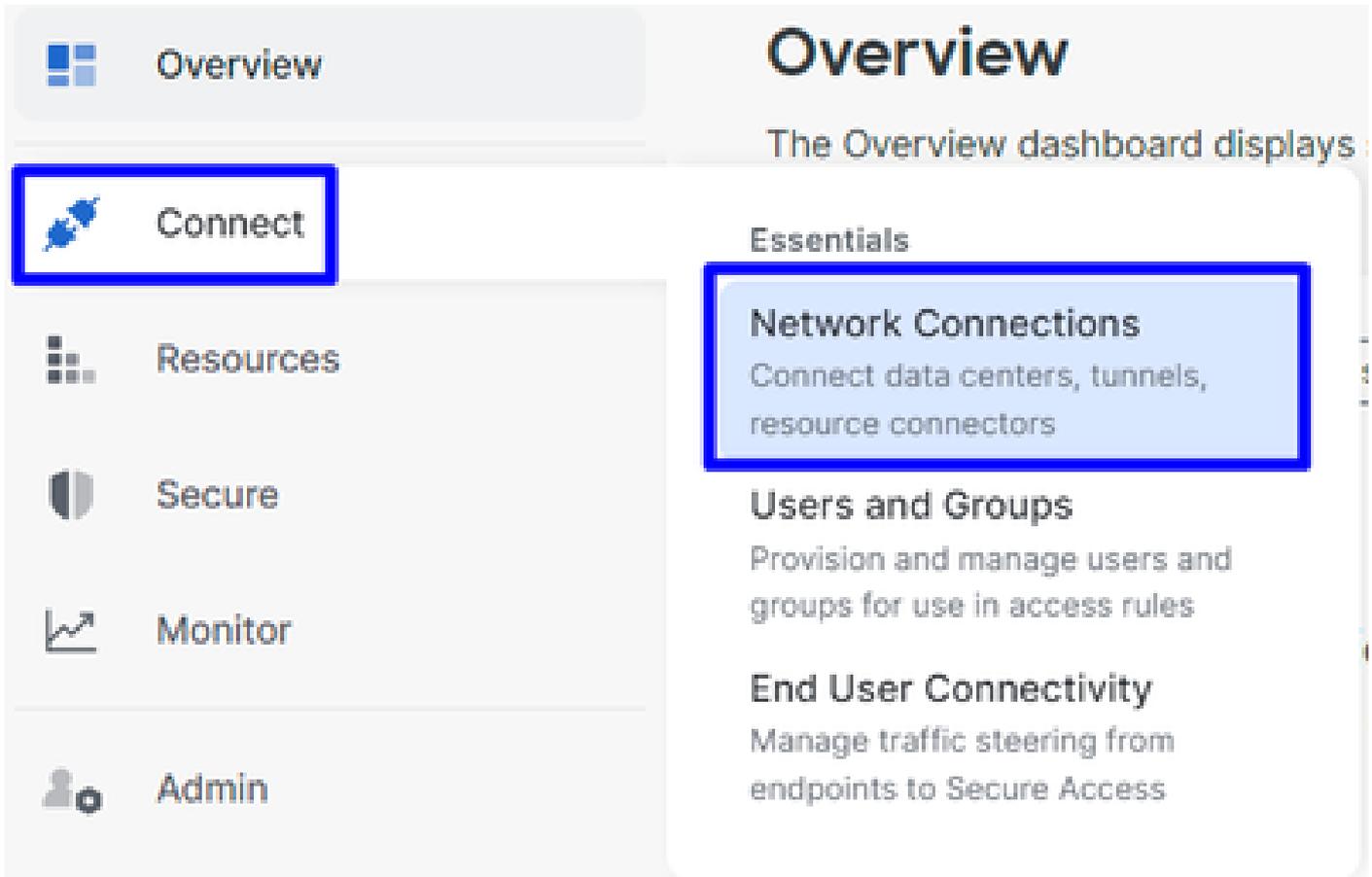
在安全訪問上配置VPN

導航到[安全訪問](#)的管理面板。



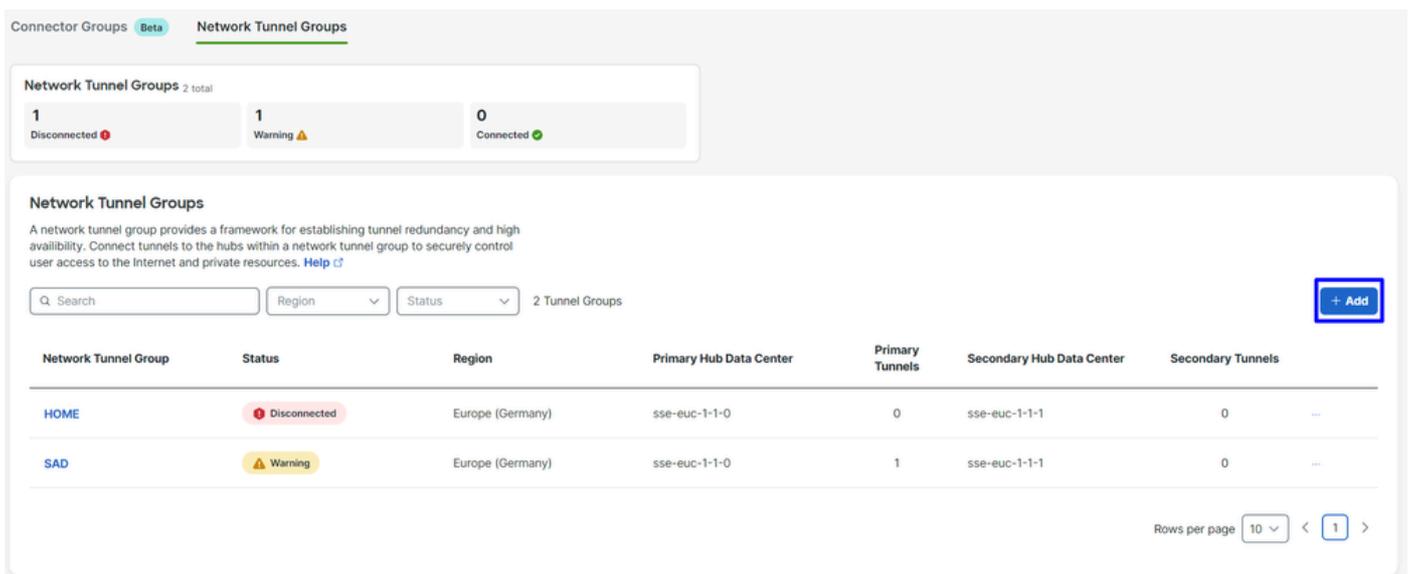
安全存取-首頁

- 按一下 [Connect > Network Connections](#)



安全訪問-網路連線

- 在Network Tunnel Groups下，按一下 + Add



安全訪問-網路隧道組

- 配置Tunnel Group Name、Region和 Device Type
- 按一下 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](#)



附註：選擇最接近防火牆位置的區域。

-
- 配置 Tunnel ID Format 和 Passphrase
 - 按一下 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](#)

- 配置已在網路上配置且希望透過安全訪問傳輸流量的IP地址範圍或主機
- 按一下 **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](#)

安全訪問-隧道組-路由選項

按一下顯示**Save** 的隧道資訊後，請儲存該資訊以用於下一步**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	

在 Palo Alto 上配置隧道

配置隧道介面

導航至 Palo Alto Dashboard。

- 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

- 在Config下，配置Virtual Router、Security Zone並將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

- 在IPv4下，配置一個不可路由的IP。例如，您可以使用 169.254.0.1/30
- 按一下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

之後，您可以設定以下類似設定：

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	

如果已按照如下方式配置該配置，您可以點選**Commit** 儲存配置，然後繼續下一步Configure IKE Crypto Profile。

配置IKE加密配置檔案

要配置加密配置檔案，請導航到：

- Network > Network Profile > IKE Crypto
- 按一下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

- 配置下一個引數：

- **Name**：配置標識配置檔案的名稱。

- **DH GROUP**：組19
- **AUTHENTICATION**：非身份驗證
- **ENCRYPTION**：aes-256-gcm
- Timers

- Key Lifetime：8小時

- **IKEv2 Authentication:0**

- 完成所有配置後，按一下 **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

如果已按照如下方式配置該配置，可以點選Commit 儲存配置，然後繼續下一步，Configure IKE Gateways.

配置IKE網關

配置IKE網關

- Network > Network Profile > IKE Gateways
- 按一下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

- 配置下一個引數：
 - Name：配置用於標識Ike網關的名稱。
 - **Version**：僅IKEv2模式
 - Address Type：IPv4
 - **Interface**：選擇您的Internet WAN介面。
 - Local IP Address：選擇您的Internet WAN介面的IP。
 - **Peer IP Address Type** :IP
 - Peer Address：使用[隧道資料](#)步驟中指定的Primary IP Datacenter IP AddressIP。
 - Authentication：預共用金鑰
 - Pre-shared Key：使用步驟[Tunnel Data](#)中給出的 **passphrase** 命令。
 - **Confirm Pre-shared Key**：使用步驟[Tunnel Data](#)中給出的 **passphrase** 命令。
 - **Local Identification**：選擇User FQDN (Email address) 並使用步驟[Tunnel Data](#)中給出的**Primary Tunnel ID** 命令。
 - **Peer Identification**：選IP Address擇並使用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			

- 按一下Advanced Options
 - **Enable NAT Traversal**
 - 在步驟[Configure IKE Crypto Profile](#)中選擇IKE Crypto Profile 建立的
 - 標示核取方塊 **Liveness Check**
 - 按一下 **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

如果已按照如下方式配置該配置，可以點選**Commit** 儲存配置，然後繼續下一步，Configure IPSEC Crypto.

配置IPSEC加密配置檔案

要配置IKE網關，請導航至 Network > Network Profile > IPSEC Crypto

- 按一下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

- 配置下一個引數：
 - **Name**：使用名稱標識安全訪問IPsec配置檔案
 - IPSec Protocol：ESP
 - **ENCRYPTION**：aes-256-gcm
 - DH Group：無pfs，1小時
- 按一下 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

如果已按照如下方式配置該配置，可以點選Commit 儲存配置，然後繼續下一步，Configure IPSec Tunnels.

配置IPSec隧道

要配置IPSec Tunnels，請導航到Network > IPSec Tunnels。

- 按一下 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

- 配置下一個引數：

- Name：使用名稱標識安全訪問隧道

- Tunnel Interface：選擇在步驟[配置隧道介面](#)上配置的隧道介面。
- Type：自動金鑰
- Address Type：IPv4
- IKE Gateways：在[配置IKE網關](#)步驟中選擇已配置的IKE網關。
- IPsec Crypto Profile：選擇在步驟[配置IPSEC加密配置檔案](#)中配置的IKE網關
- 標示核取方塊 **Advanced Options**

- IPsec Mode Tunnel：選擇隧道。

- 按一下 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

現在已成功建立您的VPN，您可以繼續執行 **Configure Policy Based Forwarding** 步驟。

配置基於策略的轉發

要配置 **Policy Based Forwarding**，請導航到 **Policies > Policy Based Forwarding**。

- 按一下 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

- 配置下一個引數：

- General

- **Name**：使用名稱標識安全訪問、策略基礎轉發（按源路由）

- Source

- **Zone**：選擇您計畫根據源路由流量的區域

- **Source Address**：配置要用作源的主機或網路。
- **Source Users**：配置要路由流量的使用者（僅在適用時）

- Destination/Application/Service

- Destination Address : 您可以將其保留為Any , 也可以指定安全訪問(100.64.0.0/10)的地址範圍

- Forwarding

- Action : 轉發

- Egress Interface : 選擇在步驟[配置隧道介面](#)上配置的隧道介面。

- Next Hop:無

- 按一下OK , 然後 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

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。