

# 使用Palo Alto防火墙配置安全访问

## 目录

---

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[在安全访问中配置VPN](#)

[隧道数据](#)

[在Palo Alto上配置隧道](#)

[配置隧道接口](#)

[配置IKE加密配置文件](#)

[配置IKE网关](#)

[配置IPSEC加密配置文件](#)

[配置IPSec隧道](#)

[配置基于策略的转发](#)

---

## 简介

本文档介绍如何使用Palo Alto防火墙配置安全访问。

## 先决条件

- [配置用户调配](#)
- [ZTNA SSO身份验证配置](#)
- [配置远程访问VPN安全访问](#)

## 要求

Cisco 建议您了解以下主题：

- Palo Alto 11.x版本防火墙
- 安全访问
- 思科安全客户端- VPN
- 思科安全客户端- ZTNA
- 无客户端ZTNA

## 使用的组件

本文档中的信息基于：

- Palo Alto 11.x版本防火墙

- 安全访问
- 思科安全客户端- VPN
- 思科安全客户端- ZTNA

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

## 背景信息



安全访问- Palo Alto

思科设计了安全访问(Secure Access)，用于保护和提供对内部和基于云的私有应用的访问。它还可以保护从网络到Internet的连接。这通过实施多种安全方法和层来实现，所有这些方法都旨在保护通

过云访问信息时所需的信息。

## 配置

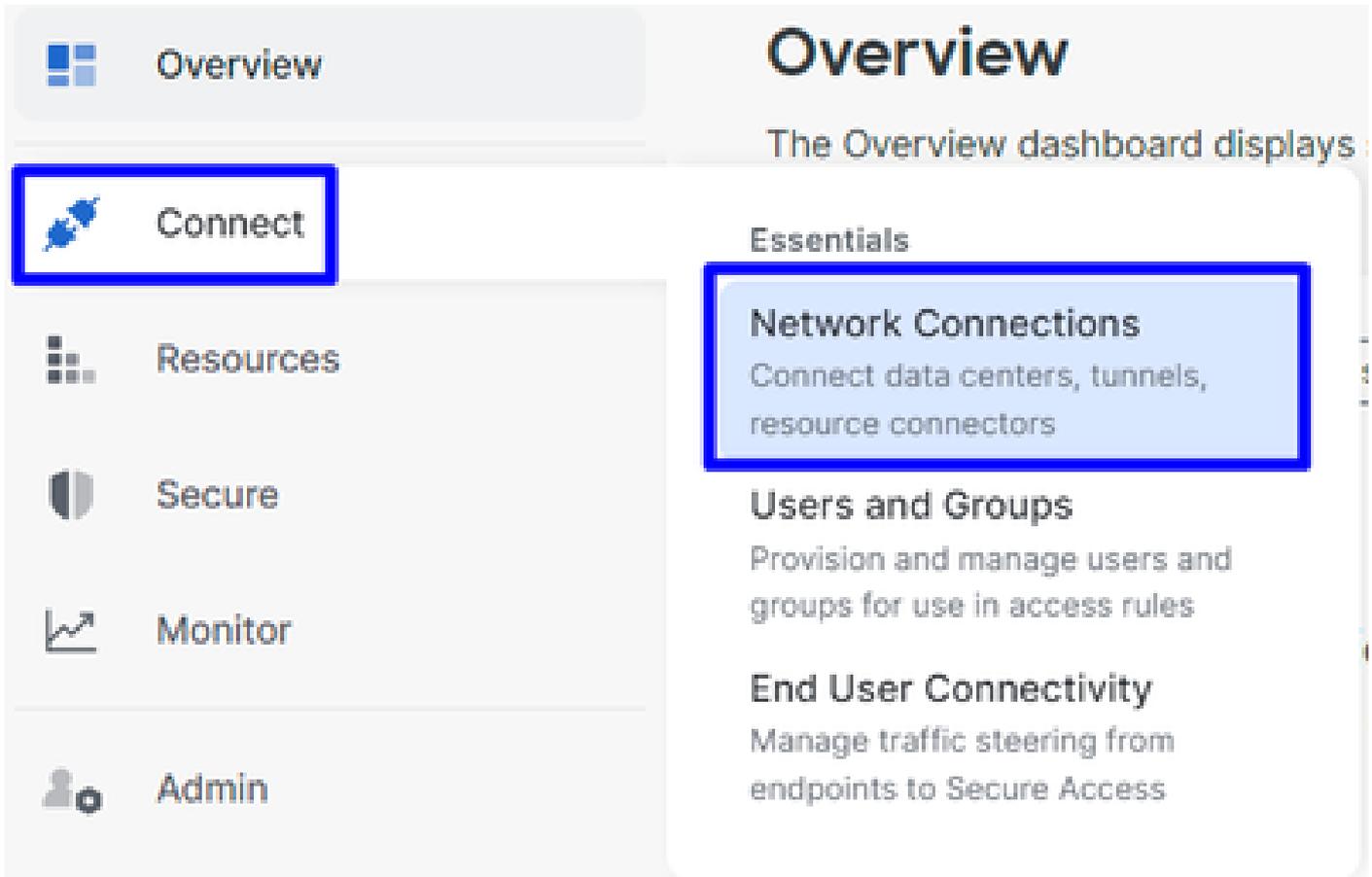
在安全访问中配置VPN

导航到[安全访问](#)的管理面板。



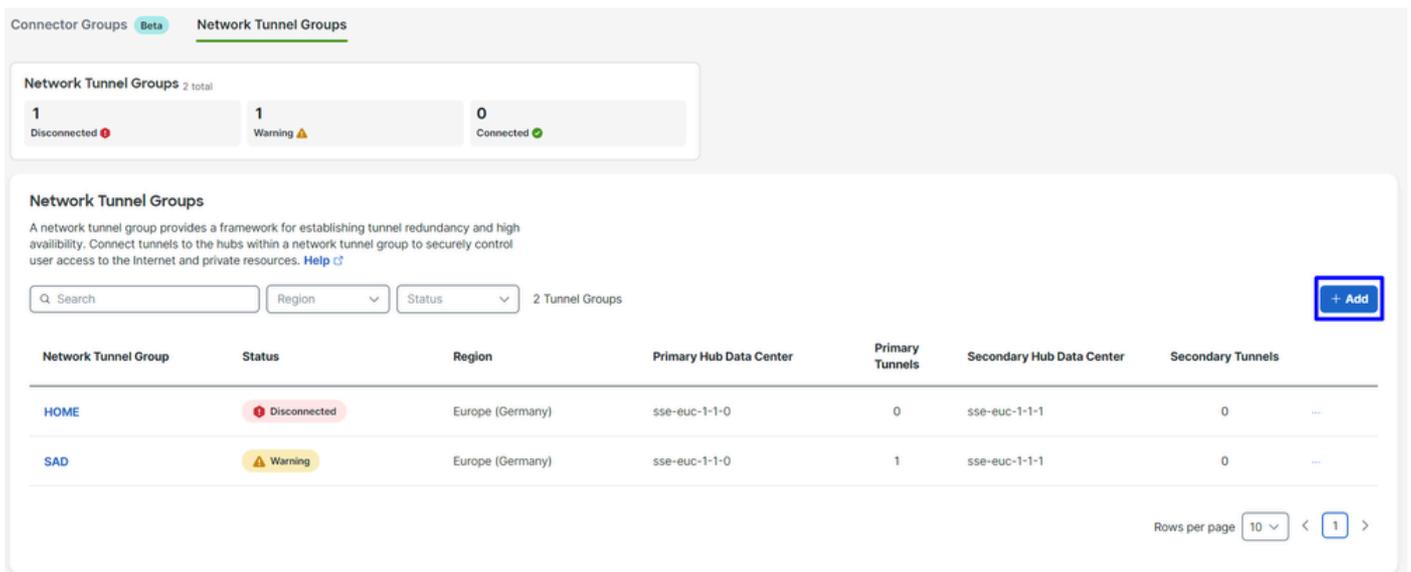
安全访问-主页

- [点击](#) Connect > Network Connections



安全访问-网络连接

- 在Network Tunnel Groups下单击 + Add



安全访问-网络隧道组

- 配置Tunnel Group Name、Region和 Device Type
- 点击 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

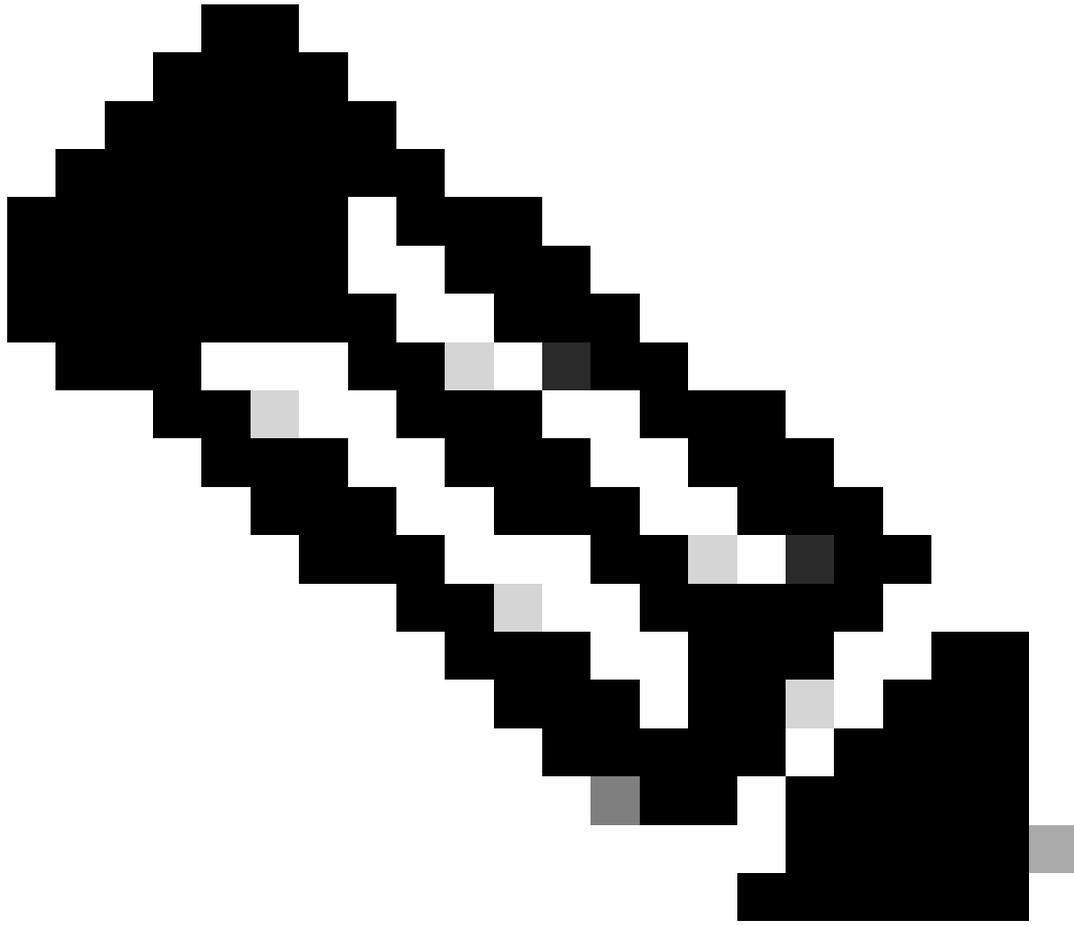
 ∨

### Device Type

 ∨

[Cancel](#)

[Next](#)



注意：选择距离防火墙位置最近的区域。

- 
- 在路由器上配置Tunnel ID Format Passphrase
  - 点击 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](#)

- 配置已在网络上配置并要通过安全访问传递流量的IP地址范围或主机
- 点击 **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](#)

安全访问-隧道组-路由选项

单击显示的**Save** 有关隧道的信息后，请保存该信息，以便执行下一步**Configure the tunnel on Palo Alto**。

## 隧道数据

### 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.

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

在Palo Alto上配置隧道

配置隧道接口

导航至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菜单下，配置Virtual Router、Security Zone并指定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，配置不可路由的IP。例如，您可以使用 169.254.0.1/30
- 点击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

之后，您可以配置如下内容：

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	

如果已按照此方式进行配置，可以点击**Commit** 保存配置并继续执行下一步Configure IKE Crypto Profile。

#### 配置IKE加密配置文件

要配置加密配置文件，请导航至：

- Network > Network Profile > IKE Crypto
- 点击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

- 配置以下参数：

- Name：配置名称以标识配置文件。

- DH GROUP：组19
    - AUTHENTICATION：非身份验证
    - ENCRYPTION：aes-256-gcm
    - Timers

- Key Lifetime:8 小时

- IKEv2 Authentication:0

- 完成所有配置后，单击 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	<b>Timers</b>
<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

如果已按照此方式进行配置，可以点击Commit 保存配置并继续下一步，Configure IKE Gateways.

#### 配置IKE网关

#### 配置IKE网关

- Network > Network Profile > IKE Gateways
- 点击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

- 配置以下参数：

- Name：配置用于标识Ike网关的名称。

- **Version**：仅IKEv2模式
- Address Type：IPv4
- **Interface**：选择您的Internet WAN接口。
- Local IP Address：选择您的Internet WAN接口的IP。
- **Peer IP Address Type** :IP
- Peer Address：使用[隧道数据](#)步骤中给定的Primary IP Datacenter IP Address IP。
- Authentication:预共享密钥
- Pre-shared Key：使用步骤[隧道数据](#)中给定 **passphrase** 的。
- **Confirm Pre-shared Key**：使用步骤[隧道数据](#)中给定 **passphrase** 的。
- **Local Identification**：选择User FQDN (Email address) 并使用步骤[Tunnel Data](#)中给定Primary Tunnel ID 的参数。
- **Peer Identification**：选IP Address择并使用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			

- 点击Advanced Options

- **Enable NAT Traversal**

- 选择在步骤[Configure IKE Crypto Profile](#)上创**IKE Crypto Profile** 建的
- 选中复选框 **Liveness Check**
- 点击 **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

如果已按照此方式进行配置，可以点击**Commit** 保存配置并继续下一步，Configure IPSEC Crypto.

配置IPSEC加密配置文件

要配置IKE网关，请导航至 Network > Network Profile > IPSEC Crypto

- 点击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

- 配置以下参数：
  - Name：使用名称标识安全访问IPsec配置文件
  - IPSec Protocol：ESP
  - ENCRYPTION：aes-256-gcm
  - DH Group：无pfs，1小时
- 点击 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

如果已按照此方式进行配置，可以点击**Commit** 保存配置并继续下一步，Configure IPSec Tunnels.

#### 配置IPSec隧道

要配置**IPSec Tunnels**，请导航到Network > IPSec Tunnels。

- 点击 Add

The screenshot shows the PA-VM Network configuration page. The 'NETWORK' tab is active. The left sidebar lists various network features, with 'IPSec Tunnels' selected. The main content area displays a table of IKE Gateway/Satellite configurations. The table has columns for Name, Status, Type, Interface, Local IP, Peer Address, and Tunnel Interface. Two entries are listed: CSA (Active) and CSA2 (Inactive). At the bottom of the table, there is a toolbar with buttons for '+ Add', '- Delete', 'Enable', 'Disable', and 'PDF/CSV'. The '+ Add' button is highlighted with a red box.

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

• 配置以下参数：

◦ **Name**：使用名称标识安全访问隧道

• **Tunnel Interface**：选择在[配置隧道接口](#)这一步中配置的隧道接口。

• **Type**：自动密钥

• **Address Type**：IPv4

• **IKE Gateways**：选择在[Configure IKE Gateways](#)步骤中配置的IKE网关。

• **IPsec Crypto Profile**：选择在[配置IPSEC加密配置文件](#)步骤中配置的IKE网关

• 选中复选框 **Advanced Options**

◦ **IPSec Mode Tunnel**：选择隧道。

- 点击 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

现在您的VPN已成功创建，您可以继续执行步骤 **Configure Policy Based Forwarding**。

配置基于策略的转发

要配置 **Policy Based Forwarding**，请导航到 **Policies > Policy Based Forwarding**。

- 点击 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

- 配置以下参数：

- General

- Name：使用名称标识安全访问、策略基础转发（按来源路由）

- Source

- Zone：选择您计划根据源路由流量的区域

- Source Address：配置要用作源的一个或多个主机。
- Source Users：配置要路由流量的用户（如果适用）

- Destination/Application/Service

- Destination Address : 您可以将其保留为Any , 也可以指定安全访问(100.64.0.0/10)的地址范围

- Forwarding

- Action : 转发

- Egress Interface : 选择在[配置隧道接口](#)这一步中配置的隧道接口。

- Next Hop:无

- 点击OK , 然后 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

### Policy Based Forwarding Rule

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

Action: Forward

Egress Interface: tunnel.1

Next Hop: None

Monitor

Profile: [ ]

Disable this rule if nexthop/monitor ip is unreachable

IP Address: [ ]

Enforce Symmetric Return

NEXT HOP ADDRESS LIST

[+ Add] [- Delete]

Schedule: None

OK Cancel

现在，您已在Palo Alto上配置所有内容；配置路由后，可以建立隧道，您需要继续在Secure Access Dashboard上配置RA-VPN、基于浏览器的ZTA或客户端基础ZTA。

## 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。