

Configurer un accès sécurisé avec le pare-feu Palo Alto

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Configurer le VPN sur un accès sécurisé](#)

[Données du tunnel](#)

[Configurer le tunnel sur Palo Alto](#)

[Configuration de l'interface du tunnel](#)

[Configuration du profil de chiffrement IKE](#)

[Configuration des passerelles IKE](#)

[Configurer le profil de chiffrement IPSEC](#)

[Configuration des tunnels IPSec](#)

[Configurer le transfert basé sur des stratégies](#)

Introduction

Ce document décrit comment configurer l'accès sécurisé avec Palo Alto Firewall.

Conditions préalables

- [Configurer le provisionnement utilisateur](#)
- [Configuration de l'authentification ZTNA SSO](#)
- [Configuration de l'accès sécurisé VPN à distance](#)

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Pare-feu de version Palo Alto 11.x
- Accès sécurisé
- Client sécurisé Cisco - VPN
- Client sécurisé Cisco - ZTNA
- ZTNA sans client

Composants utilisés

Les informations contenues dans ce document sont basées sur :

- Pare-feu de version Palo Alto 11.x
- Accès sécurisé
- Client sécurisé Cisco - VPN
- Client sécurisé Cisco - ZTNA

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales



CISCO

Secure

Access



paloalto[®]
NETWORKS

Cisco a conçu Secure Access pour protéger et fournir un accès aux applications privées, sur site et dans le cloud. Il protège également la connexion du réseau à Internet. Pour ce faire, plusieurs méthodes et couches de sécurité sont mises en oeuvre, toutes visant à préserver les informations lorsqu'elles y accèdent via le cloud.

Configurer

Configurer le VPN sur un accès sécurisé

Accédez au panneau d'administration de [Secure Access](#).



- Cliquez sur Connect > Network Connections

Overview

The Overview dashboard displays

Connect

Resources

Secure

Monitor

Admin

Essentials

Network Connections
Connect data centers, tunnels, resource connectors

Users and Groups
Provision and manage users and groups for use in access rules

End User Connectivity
Manage traffic steering from endpoints to Secure Access

Accès sécurisé - Connexions réseau

- Sous Network Tunnel Groups cliquez sur + Add

Connector Groups Beta **Network Tunnel Groups**

Network Tunnel Groups 2 total

1 Disconnected ● 1 Warning ▲ 0 Connected ●

Network Tunnel Groups

A network tunnel group provides a framework for establishing tunnel redundancy and high availability. Connect tunnels to the hubs within a network tunnel group to securely control user access to the Internet and private resources. [Help](#)

Q Search Region Status 2 Tunnel Groups + Add

Network Tunnel Group	Status	Region	Primary Hub Data Center	Primary Tunnels	Secondary Hub Data Center	Secondary Tunnels
HOME	● Disconnected	Europe (Germany)	sse-euc-1-1-0	0	sse-euc-1-1-1	0
SAD	▲ Warning	Europe (Germany)	sse-euc-1-1-0	1	sse-euc-1-1-1	0

Rows per page 10 < 1 >

Accès sécurisé - Groupes de tunnels réseau

- Configurer Tunnel Group Name, Region et Device Type
- Cliquer **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

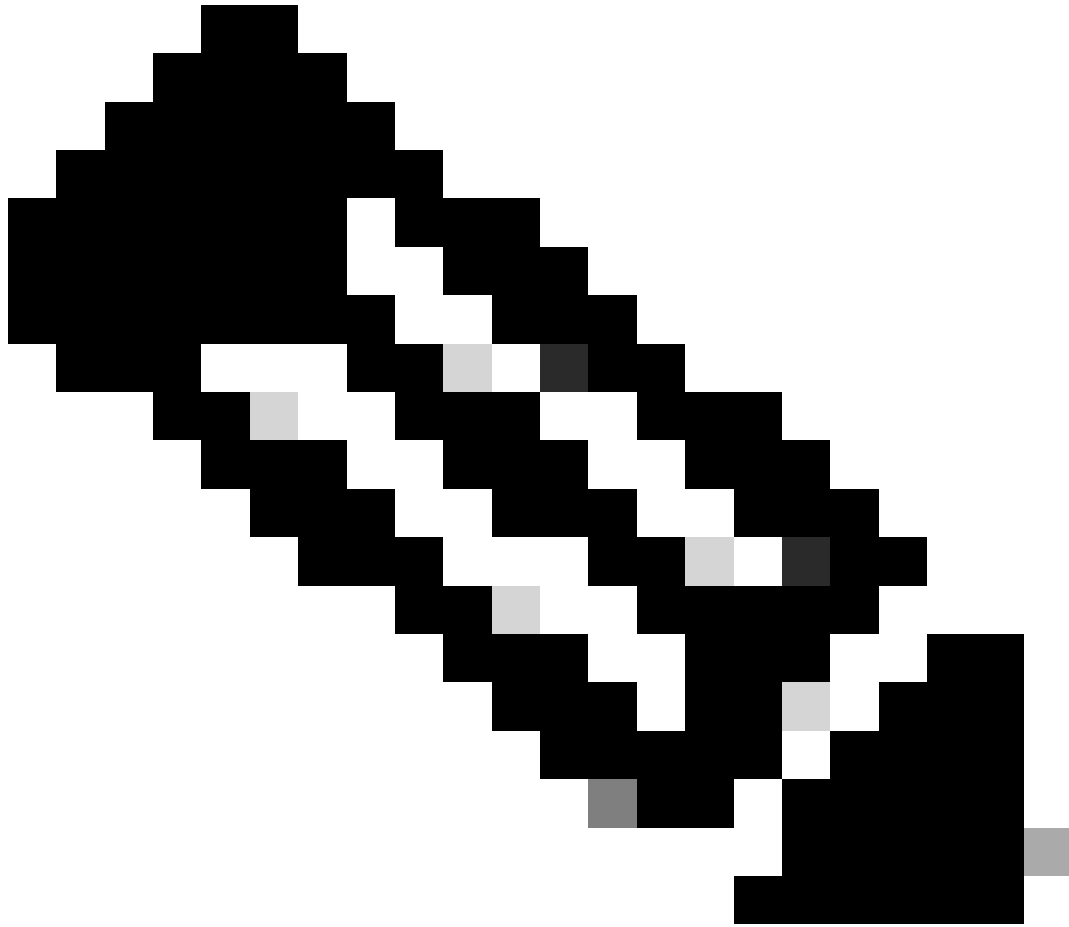
 ∨

Device Type

 ∨

[Cancel](#)

[Next](#)



Remarque : choisissez la région la plus proche de l'emplacement de votre pare-feu.

-
- Configurez les Tunnel ID Format et Passphrase
 - Cliquer 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](#)

- Configurez les plages d'adresses IP ou les hôtes que vous avez configurés sur votre réseau et souhaitez faire passer le trafic par un accès sécurisé
- Cliquer **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](#)

Accès sécurisé - Groupes de tunnels - Options de routage

Après avoir cliqué sur **Save** les informations sur le tunnel s'affiche, veuillez enregistrer ces informations pour l'étape suivante, **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	

Configurer le tunnel sur Palo Alto

Configuration de l'interface du tunnel

Accédez au tableau de bord 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

- Sous Config menu, configurez le Virtual Router, le Security Zone et attribuez 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

- Sous IPv4, configurez une adresse IP non routable. Par exemple, vous pouvez utiliser 169.254.0.1/30
- Cliquer 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

Après cela, vous pouvez configurer quelque chose comme ceci :

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 vous l'avez configuré de cette manière, vous pouvez cliquer sur **Commit** pour enregistrer la configuration et passer à l'étape suivante, Configurer IKE Crypto Profile.

Configuration du profil de chiffrement IKE

Pour configurer le profil de chiffrement, accédez à :

- Network > Network Profile > IKE Crypto
- CliquerAdd

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

- Configurez les paramètres suivants :
 - **Name:** configurez un nom pour identifier le profil.
 - **DH GROUP:** groupe19
 - **AUTHENTICATION:** non-auth
 - **ENCRYPTION:** aes-256-gcm
 - Timers
 - Key Lifetime: 8 heures
 - **IKEv2 Authentication:**0
- Une fois que tout est configuré, cliquez sur **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 vous l'avez configuré de cette manière, vous pouvez cliquer sur **Commit** pour enregistrer la configuration et passer à l'étape suivante, Configure IKE Gateways.

Configuration des passerelles IKE

Pour configurer des passerelles IKE

- Network > Network Profile > IKE Gateways
- CliquerAdd

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

- Configurez les paramètres suivants :
 - Name: configurez un nom pour identifier les passerelles Ike.
 - **Version** : mode IKEv2 uniquement
 - Address Type :IPv4
 - **Interface** : sélectionnez votre interface WAN Internet.
 - Local IP Address: sélectionnez l'adresse IP de votre interface WAN Internet.
 - **Peer IP Address Type** :IP
 - Peer Address: Utilisez l'adresse IP de Primary IP Datacenter IP Address, donnée à l'étape [Données de tunnel](#).
 - Authentication: clé pré-partagée
 - Pre-shared Key : Utilisez la valeur **passphrase** donnée à l'étape [Données de tunnel](#).
 - **Confirm Pre-shared Key** : Utilisez la valeur **passphrase** donnée à l'étape [Données de tunnel](#).
 - **Local Identification** : Choisissez User **FQDN (Email address)** et utilisez la valeur **Primary Tunnel ID** donnée à l'étape, [Tunnel Data](#).
 - **Peer Identification** : IP Address Choisissez et utilisez la 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			

- Cliquer Advanced Options

- **Enable NAT Traversal**

- Sélectionnez le **IKE Crypto Profile** créé à l'étape [Configurer le profil de chiffrement IKE](#)
- Cochez la case correspondant à **Liveness Check**
- Cliquer **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 vous l'avez configuré de cette manière, vous pouvez cliquer sur **Commit** pour enregistrer la configuration et passer à l'étape suivante, Configure IPSEC Crypto.

Configurer le profil de chiffrement IPSEC

Pour configurer les passerelles IKE, accédez à Network > Network Profile > IPSEC Crypto

- CliquerAdd

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

- Configurez les paramètres suivants :
 - **Name:** utilisez un nom pour identifier le profil IPsec d'accès sécurisé
 - IPSec Protocol: ESP
 - **ENCRYPTION:** aes-256-gcm
 - DH Group: no-pfs, 1 heure
- Cliquer 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

Buttons: + Add, - Delete, ↑ Move Up, ↓ Move Down

Buttons: OK, Cancel

Si vous l'avez configuré de cette manière, vous pouvez cliquer sur **Commit** pour enregistrer la configuration et passer à l'étape suivante, Configure IPSec Tunnels.

Configuration des tunnels IPSec

Pour configurer **IPSec Tunnels**, accédez à Network > IPSec Tunnels.

- Cliquer 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...	LOCAL IP	PEER ADDRESS	STATUS
<input type="checkbox"/>	CSA	● Tunnel Info	Auto Key	ethernet...	192.168...	18.156.1...	● IKE Info
<input type="checkbox"/>	CSA2	● Tunnel Info	Auto Key	ethernet...	192.168...	3.120.45...	● IKE Info

+ Add - Delete Enable Disable PDF/CSV

- Configurez les paramètres suivants :
 - **Name:** utilisez un nom pour identifier le tunnel Secure Access
 - **Tunnel Interface:** choisissez l'interface de tunnel configurée à l'étape, [Configurez l'interface de tunnel.](#)
 - **Type:** Clé auto
 - **Address Type:** IPv4
 - **IKE Gateways:** sélectionnez les passerelles IKE configurées à l'étape [Configurer les passerelles IKE.](#)
 - **IPsec Crypto Profile:** sélectionnez les passerelles IKE configurées à l'étape [Configurer le profil de chiffrement IPSEC](#)
 - Cochez la case correspondant à **Advanced Options**
 - **IPSec Mode Tunnel:** sélectionnez Tunnel.

- Cliquer 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

Maintenant que votre VPN est correctement créé, vous pouvez passer à l'étape, **Configure Policy Based Forwarding**.

Configurer le transfert basé sur des stratégies

Pour configurer **Policy Based Forwarding**, accédez à Politiques > Policy Based Forwarding.

- Cliquer 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

- Configurez les paramètres suivants :

- General

- **Name:** utilisez un nom pour identifier l'accès sécurisé, le transfert de base de stratégie (routage par origine)

- Source

- **Zone:** sélectionnez les zones à partir desquelles vous prévoyez d'acheminer le trafic en fonction de l'origine

- **Source Address:** configurez le ou les hôtes que vous souhaitez utiliser comme source.

- **Source Users:** configurez les utilisateurs que vous souhaitez router le trafic (uniquement si applicable)

- Destination/Application/Service

- Destination Address: vous pouvez laisser la valeur Any (Tous) ou spécifier les plages d'adresses d'accès sécurisé (100.64.0.0/10)

- Forwarding

- **Action:** transfert

- **Egress Interface:** choisissez l'interface de tunnel configurée à l'étape, [Configurez l'interface de tunnel](#).

- **Next Hop:** Aucune

- Cliquez sur OK et 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:

Egress Interface:

Next Hop:

Monitor

Profile:

Disable this rule if nexthop/monitor ip is unreachable

IP Address:

Enforce Symmetric Return

NEXT HOP ADDRESS LIST

Schedule:

Maintenant, tout est configuré sur Palo Alto ; après avoir configuré la route, le tunnel peut être établi, et vous devez continuer à configurer le RA-VPN, le ZTA basé sur navigateur ou le ZTA de base client sur le tableau de bord d'accès sécurisé.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.