

Secure Access configureren met firewall van Palo Alto

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[VPN bij beveiligde toegang configureren](#)

[Tunnelgegevens](#)

[Stel de tunnel in op Palo Alto](#)

[De tunnelinterface configureren](#)

[IKE-coderingsprofiel configureren](#)

[IKE-gateways configureren](#)

[IPSEC-coderingsprofiel configureren](#)

[IPsec-tunnels configureren](#)

[Op beleid gebaseerd doorsturen configureren](#)

Inleiding

Dit document beschrijft hoe u Secure Access kunt configureren met de firewall van Palo Alto.

Voorwaarden

- [Gebruikersprovisioning configureren](#)
- [Configuratie ZTNA SSO-verificatie](#)
- [Beveiligde toegang tot VPN configureren](#)

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Firewall van Palo Alto 11.x versie
- Beveiligde toegang
- Cisco Secure-client - VPN
- Cisco Secure-client - ZTNA
- Clientloze ZTNA

Gebruikte componenten

De informatie in dit document is gebaseerd op:

- Firewall van Palo Alto 11.x versie
- Beveiligde toegang
- Cisco Secure-client - VPN
- Cisco Secure-client - ZTNA

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie



CISCO

Secure

Access



paloalto[®]
NETWORKS

Cisco heeft Secure Access ontworpen om toegang tot particuliere toepassingen te beschermen en te bieden, zowel op locatie als in de cloud. Het beschermt ook de verbinding van het netwerk met het internet. Dit wordt bereikt door de implementatie van meerdere beveiligingsmethoden en -lagen, die allemaal gericht zijn op het bewaren van de informatie zoals ze deze via de cloud benaderen.

Configureren

VPN bij beveiligde toegang configureren

Navigeer naar het beheerderspaneel van [Secure Access](#).



Secure Access - hoofdpagina

- **Klik op** 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

Secure Access - netwerkverbindingen

- Onder Network Tunnel Groups klik op + 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 >

Secure Access - netwerktunnelgroepen

- Configureren Tunnel Group Name, Regionen Device Type
- Klik op de knop **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](#)



Opmerking: kies de regio die het dichtst bij de locatie van uw firewall ligt.

-
- Configureer de Tunnel ID Format en Passphrase
 - Klik op de knop 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](#)

- Configureer de IP-adresbereiken of hosts die u op uw netwerk hebt geconfigureerd en u wilt het verkeer via beveiligde toegang doorgeven
- Klik op de knop **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](#)

Secure Access - tunnelgroepen - routingopties

Nadat u op **Save** de informatie over de tunnel wordt weergegeven, bewaar die informatie voor de volgende stap, **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	

Stel de tunnel in op Palo Alto

De tunnelinterface configureren

Navigeer naar het Dashboard van Palo Alto.

- Network > Interfaces > Tunnel
- Click Add

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

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

+ Add - Delete PDF/CSV

- Configureer in hetConfig menu het Virtual Router Security Zone menu en wijs een 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

- Configureer onder IPv4 de optie niet-routeerbare IP. U kunt bijvoorbeeld 169.254.0.1/30
- Klik op de knop 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

Daarna kunt u zoiets als dit instellen:

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	

Als u het zo hebt geconfigureerd, kunt u op klikken **Commit** om de configuratie op te slaan en door te gaan met de volgende stap, Configure IKE Crypto Profile.

IKE-coderingsprofiel configureren

Ga voor het configureren van het crypto-profiel naar:

- Network > Network Profile > IKE Crypto
- Klik op de knop 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

- Configureer de volgende parameters:

- **Name:** Configureer een naam om het profiel te identificeren.

- **DH GROUP:** groep19
- **AUTHENTICATION:** niet-auth
- **ENCRYPTION:** aes-256-gcm
- Timers

- Key Lifetime: 8 uur

- **IKEv2 Authentication:**0

- Nadat u alles hebt geconfigureerd, klikt u op **OK**

IKE Crypto Profile ?

Name

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

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

Als je het zo hebt geconfigureerd, kun je op klikken **Commit** om de configuratie op te slaan en door te gaan met de volgende stap, Configure IKE Gateways.

IKE-gateways configureren

IKE-gateways configureren

- Network > Network Profile > IKE Gateways
- Klik op de knop 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

- Configureer de volgende parameters:
 - Name: Configureer een naam om de Ike-gateways te identificeren.
 - **Version** : alleen IKEv2-modus
 - Address Type :IPv4
 - **Interface** : Selecteer uw Internet WAN-interface.
 - Local IP Address: Selecteer IP van uw WAN-interfacekaart voor internet.
 - **Peer IP Address Type** :IP
 - Peer Address: Gebruik het IP-adres van Primary IP Datacenter IP Address, zoals aangegeven in de stap [Tunnelgegevens](#).
 - Authentication: Vooraf gedeelde sleutel
 - Pre-shared Key : Gebruik de **passphrase** opgegeven waarde in de stap [Tunnelgegevens](#).
 - **Confirm Pre-shared Key** : Gebruik de **passphrase** opgegeven waarde in de stap [Tunnelgegevens](#).
 - **Local Identification** : Kies **User FQDN (Email address)** en gebruik de **Primary Tunnel ID** gegeven in de stap, [Tunnel Data](#).
 - **Peer Identification** : IP AddressKies en gebruik de 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			

OK

Cancel

- Klik op de knop Advanced Options

- **Enable NAT Traversal**

- Selecteer de stappen **IKE Crypto Profile** die u wilt maken, [IKE-coderingsprofiel configureren](#)
- Schakel het selectievakje in voor **Liveness Check**
- Klik op de knop **OK**

IKE Gateway



General | **Advanced Options**

Common Options

Enable Passive Mode

Enable NAT Traversal

IKEv2

IKE Crypto Profile

Strict Cookie Validation

Liveness Check

Interval (sec)

OK

Cancel

Als je het zo hebt geconfigureerd, kun je op klikken **Commit** om de configuratie op te slaan en door te gaan met de volgende stap, Configure IPSEC Crypto.

IPSEC-coderingsprofiel configureren

Om IKE-gateways te configureren, navigeer naar Network > Network Profile > IPSEC Crypto

- Klik op de knop 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

- Configureer de volgende parameters:
 - **Name:** Gebruik een naam om het Secure Access IPsec-profiel te identificeren
 - IPSec Protocol: ESP
 - **ENCRYPTION:** aes-256-gcm
 - DH Group: niet beschikbaar, 1 uur
- Klik op de knop OK

IPSec Crypto Profile



Name

IPSec Protocol

ENCRYPTION

aes-256-gcm

AUTHENTICATION

sha256

DH Group

Lifetime

Minimum lifetime = 3 mins

Enable

Lifeseize

Recommended lifeseize is 100MB or greater

Als je het zo hebt geconfigureerd, kun je op klikken **Commit** om de configuratie op te slaan en door te gaan met de volgende stap, Configure IPSec Tunnels.

IPsec-tunnels configureren

Ga voor het configureren **IPSec Tunnels** naar Network > IPSec Tunnels.

- Klik op de knop Add

	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

- Configureer de volgende parameters:

- **Name:** Gebruik een naam om de Secure Access-tunnel te identificeren

- **Tunnel Interface:** Kies de tunnelinterface die op de stap is geconfigureerd, [configureer de tunnelinterface](#).

- **Type:** Autosleutel

- **Address Type:** IPv4

- **IKE Gateways:** Kies de IKE-gateways die bij de stap zijn geconfigureerd, [IKE-gateways configureren](#).

- **IPsec Crypto Profile:** Kies de IKE-gateways die bij de stap zijn geconfigureerd, [IPSEC-coderingsprofiel configureren](#)

- Schakel het selectievakje in voor **Advanced Options**

- **IPSec Mode Tunnel:** Kies een tunnel.

- Klik op de knop 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

Nu uw VPN met succes is gemaakt, kunt u doorgaan met de stap, **Configure Policy Based Forwarding**.

Op beleid gebaseerd doorsturen configureren

Ga voor het configureren **Policy Based Forwarding** naar Policies > Policy Based Forwarding.

- Klik op de knop 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

- Configureer de volgende parameters:

- General

- **Name:** Gebruik een naam om de Secure Access, Policy Base Forwarding (routing op basis) te identificeren

- Source

- **Zone:** Selecteer de zones waar u plannen hebt om het verkeer te leiden op basis van de oorsprong

- **Source Address:** De host of netwerken configureren die u als bron wilt gebruiken.

- **Source Users:** Configureer de gebruikers die u het verkeer wilt leiden (alleen indien van toepassing)

- Destination/Application/Service

- Destination Address: U kunt het als om het even welk verlaten, of u kunt de waaier van adressen van Veilige Toegang specificeren (100.64.0.0/10)

- Forwarding

- **Action:** Voorwaarts

- **Egress Interface:** Kies de tunnelinterface die op de stap is geconfigureerd, [configureer de tunnelinterface](#).

- **Next Hop:**None

- Klik OK en 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

Nu hebt u alles geconfigureerd op Palo Alto; nadat u de route hebt geconfigureerd, kan de tunnel worden opgezet, en u moet doorgaan met het configureren van de RA-VPN, Browser-Based ZTA, of Client Base ZTA op Secure Access Dashboard.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.