

Sicheren Zugriff mit Palo Alto Firewall konfigurieren

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Konfigurieren des VPN für sicheren Zugriff](#)

[Tunneln](#)

[Konfigurieren Sie den Tunnel auf Palo Alto](#)

[Konfigurieren der Tunnelschnittstelle](#)

[IKE-Verschlüsselungsprofil konfigurieren](#)

[Konfigurieren von IKE-Gateways](#)

[IPSEC-Verschlüsselungsprofil konfigurieren](#)

[Konfigurieren von IPSec-Tunneln](#)

[Richtlinienbasierte Weiterleitung konfigurieren](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie sicheren Zugriff mit der Palo Alto Firewall konfigurieren.

Voraussetzungen

- [Konfiguration der Benutzerbereitstellung](#)
- [Konfiguration der ZTNA SSO-Authentifizierung](#)
- [Konfigurieren des sicheren Remotezugriff-VPN](#)

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Palo Alto 11.x Version Firewall
- Sicherer Zugriff
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA
- Clientless-ZTNA

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf:

- Palo Alto 11.x Version Firewall
- Sicherer Zugriff
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen



CISCO

Secure

Access



paloalto[®]
NETWORKS

Cisco hat Secure Access entwickelt, um den Zugriff auf private Anwendungen vor Ort und in der Cloud zu schützen. Außerdem wird die Verbindung vom Netzwerk zum Internet gesichert. Dies wird durch die Implementierung mehrerer Sicherheitsmethoden und -ebenen erreicht, die alle darauf abzielen, die Informationen beim Zugriff über die Cloud zu erhalten.

Konfigurieren

Konfigurieren des VPN für sicheren Zugriff

Navigieren Sie zum Admin-Bereich von [Secure Access](#).



- Klicken Sie [Connect > Network Connections](#)

Overview

The Overview dashboard displays

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

Connect

Resources

Secure

Monitor

Admin

Sicherer Zugriff - Netzwerkverbindungen

- Klicken Sie unter Network Tunnel Groups auf + 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 >

Sicherer Zugriff - Netzwerk-Tunnelgruppen

- Konfiguration Tunnel Group Name Region und Device Type
- Klicken Sie auf **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](#)



Hinweis: Wählen Sie die Region aus, die dem Standort Ihrer Firewall am nächsten ist.

-
- Konfigurieren Sie die Tunnel ID Format und Passphrase
 - Klicken Sie auf 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](#)

- Konfigurieren Sie die IP-Adressbereiche oder Hosts, die Sie in Ihrem Netzwerk konfiguriert haben, und leiten Sie den Datenverkehr über sicheren Zugriff weiter.
- Klicken Sie auf **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](#)

Sicherer Zugriff - Tunnelgruppen - Routing-Optionen

Nachdem Sie auf **Save** die Informationen über den Tunnel wird angezeigt, speichern Sie diese Informationen für den nächsten Schritt, **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	

Konfigurieren Sie den Tunnel auf Palo Alto

Konfigurieren der Tunnelschnittstelle

Navigieren Sie zum 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

- Konfigurieren Sie Config im Menü die Virtual Router, Security Zone und weisen Sie 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

- Konfigurieren Sie unter IPv4 eine nicht routbare IP-Adresse. Sie können z. B. 169.254.0.1/30
- Klicken Sie auf 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

Danach können Sie etwas wie das hier konfigurieren lassen:

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	

Wenn Sie die Konfiguration auf diese Weise konfiguriert haben, können Sie auf klicken, **Commit** um die Konfiguration zu speichern, und mit dem nächsten Schritt fortfahrenConfigure IKE Crypto Profile.

IKE-Verschlüsselungsprofil konfigurieren

Um das Kryptografieprofil zu konfigurieren, navigieren Sie zu:

- Network > Network Profile > IKE Crypto
- Klicken Sie auf 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

- Konfigurieren Sie die folgenden Parameter:
 - **Name:** Konfigurieren Sie einen Namen zur Identifizierung des Profils.
 - **DH GROUP:** Gruppe19
 - **AUTHENTICATION:** nicht authentifiziert
 - **ENCRYPTION:** aes-256-gcm
 - Timers
 - Key Lifetime: 8 Stunden
 - **IKEv2 Authentication:**0
- Nachdem Sie alle Einstellungen konfiguriert haben, klicken Sie auf **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 Key Lifetime <input type="text" value="Hours"/> ▼ <input type="text" value="8"/> Minimum lifetime = 3 mins IKEv2 Authentication Multiple <input type="text" value="0"/>
<input type="checkbox"/> non-auth	

+ Add - Delete ↑ Move Up ↓ Move Down

Wenn Sie die Konfiguration auf diese Weise konfiguriert haben, können Sie auf klicken, **Commit** um die Konfiguration zu speichern, und mit dem nächsten Schritt fortfahren. Configure IKE Gateways.

Konfigurieren von IKE-Gateways

IKE-Gateways konfigurieren

- Network > Network Profile > IKE Gateways
- Klicken Sie auf 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

- Konfigurieren Sie die folgenden Parameter:

- Name: Konfigurieren Sie einen Namen, um die IKE-Gateways zu identifizieren.

- **Version** : Nur IKEv2-Modus
- Address Type :IPv4
- **Interface** : Wählen Sie Ihre Internet-WAN-Schnittstelle aus.
- Local IP Address: Wählen Sie die IP-Adresse Ihrer Internet-WAN-Schnittstelle aus.
- **Peer IP Address Type** :IP
- Peer Address: Verwenden Sie die IP-Adresse von Primary IP Datacenter IP Address, die im Schritt [Tunnelnamen angeben](#) ist.
- Authentication: Vorläufiger gemeinsamer Schlüssel
- Pre-shared Key : Verwenden Sie die im Schritt [Tunnelnamen](#) passphrase angegebenen [Daten](#).
- **Confirm Pre-shared Key** : Verwenden Sie die im Schritt [Tunnelnamen](#) passphrase angegebenen [Daten](#).
- **Local Identification** : Wählen Sie **User FQDN (Email address)** und verwenden Sie die **Primary Tunnel ID** im Schritt, [Tunnel Data](#).
- **Peer Identification** : IP AddressWählen und verwenden Sie den 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			

- Klicken Sie auf Advanced Options

- **Enable NAT Traversal**

- Wählen Sie die aus dem Schritt [IKE-Verschlüsselungsprofil konfigurieren](#) **IKE Crypto Profile** erstellte aus.
- Aktivieren Sie das Kontrollkästchen für **Liveness Check**
- Klicken Sie auf **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

Wenn Sie die Konfiguration auf diese Weise konfiguriert haben, können Sie auf klicken, **Commit** um die Konfiguration zu speichern, und mit dem nächsten Schritt fortfahren. Configure IPSEC Crypto.

IPSEC-Verschlüsselungsprofil konfigurieren

Zum Konfigurieren von IKE-Gateways navigieren Sie zu Network > Network Profile > IPSEC Crypto

- Klicken Sie auf 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

- Konfigurieren Sie die folgenden Parameter:
 - **Name:** Verwenden Sie einen Namen, um das IPsec-Profil für sicheren Zugriff zu identifizieren.
 - IPSec Protocol: ESP
 - **ENCRYPTION:** aes-256-gcm
 - DH Group: no-pfs, 1 Stunde
- Klicken Sie auf 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

Wenn Sie die Konfiguration auf diese Weise konfiguriert haben, können Sie auf klicken, **Commit** um die Konfiguration zu speichern, und mit dem nächsten Schritt fortfahren. Configure IPSec Tunnels.

Konfigurieren von IPSec-Tunneln

Navigieren Sie zum Konfigurieren **IPSec Tunnels** zu Network > IPSec Tunnels.

- Klicken Sie auf 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

- Konfigurieren Sie die folgenden Parameter:
 - **Name:** Verwenden Sie einen Namen, um den sicheren Zugriffstunnel zu identifizieren.
 - **Tunnel Interface:** Wählen Sie die Tunnelschnittstelle, die im Schritt konfiguriert wurde, [Konfigurieren Sie die Tunnelschnittstelle](#).
 - **Type:** Auto-Taste
 - **Address Type:** IPv4
 - **IKE Gateways:** Wählen Sie die IKE-Gateways aus, die im Schritt konfiguriert wurden, [Konfigurieren Sie IKE-Gateways](#).
 - **IPsec Crypto Profile:** Wählen Sie die IKE-Gateways aus, die auf dem Schritt konfiguriert wurden, und [konfigurieren Sie das IPSEC-Kryptoprofil](#).
 - Aktivieren Sie das Kontrollkästchen für **Advanced Options**
 - **IPsec Mode Tunnel:** Wählen Sie Tunnel aus.

- Klicken Sie auf 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

Nachdem Ihr VPN erfolgreich erstellt wurde, können Sie mit dem Schritt fortfahren **Configure Policy Based Forwarding**.

Richtlinienbasierte Weiterleitung konfigurieren

Navigieren Sie zum Konfigurieren **Policy Based Forwarding** zu Policies > Policy Based Forwarding.

- Klicken Sie auf 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

- Konfigurieren Sie die folgenden Parameter:

- General

- **Name:** Verwenden Sie einen Namen, um den sicheren Zugriff zu identifizieren, Policy Base Forwarding (Routing nach Ursprung)

- Source

- **Zone:** Wählen Sie die Zonen aus, in denen Sie den Datenverkehr basierend auf dem Ursprung weiterleiten möchten.

- **Source Address:** Konfigurieren Sie den Host oder die Netzwerke, die Sie als Quelle verwenden möchten.

- **Source Users:** Konfigurieren Sie die Benutzer, die den Datenverkehr weiterleiten sollen (nur falls zutreffend).

- Destination/Application/Service
 - Destination Address: Sie können es als Any (Beliebig) belassen oder die Adressbereiche von Secure Access (100.64.0.0/10) angeben.
- Forwarding
 - **Action:** Weiterleiten
 - **Egress Interface:** Wählen Sie die Tunnelschnittstelle, die im Schritt konfiguriert wurde, [Konfigurieren Sie die Tunnelschnittstelle](#).
 - **Next Hop:**None
- KlickenOK und 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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.