

Configure o acesso seguro com o firewall Palo Alto

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Configurar a VPN no acesso seguro](#)

[Dados do túnel](#)

[Configurar o túnel em Palo Alto](#)

[Configurar a interface do túnel](#)

[Configurar perfil de criptografia IKE](#)

[Configurar gateways IKE](#)

[Configurar perfil de criptografia IPSEC](#)

[Configurar túneis IPsec](#)

[Configurar Encaminhamento Baseado em Política](#)

Introdução

Este documento descreve como configurar o acesso seguro com o firewall Palo Alto.

Pré-requisitos

- [Configurar Provisionamento de Usuário](#)
- [Configuração de Autenticação ZTNA SSO](#)
- [Configurar o acesso seguro da VPN de acesso remoto](#)

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Firewall da versão Palo Alto 11.x
- Acesso seguro
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA
- ZTNA sem cliente

Componentes Utilizados

As informações neste documento são baseadas em:

- Firewall da versão Palo Alto 11.x
- Acesso seguro
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio



CISCO

Secure

Access



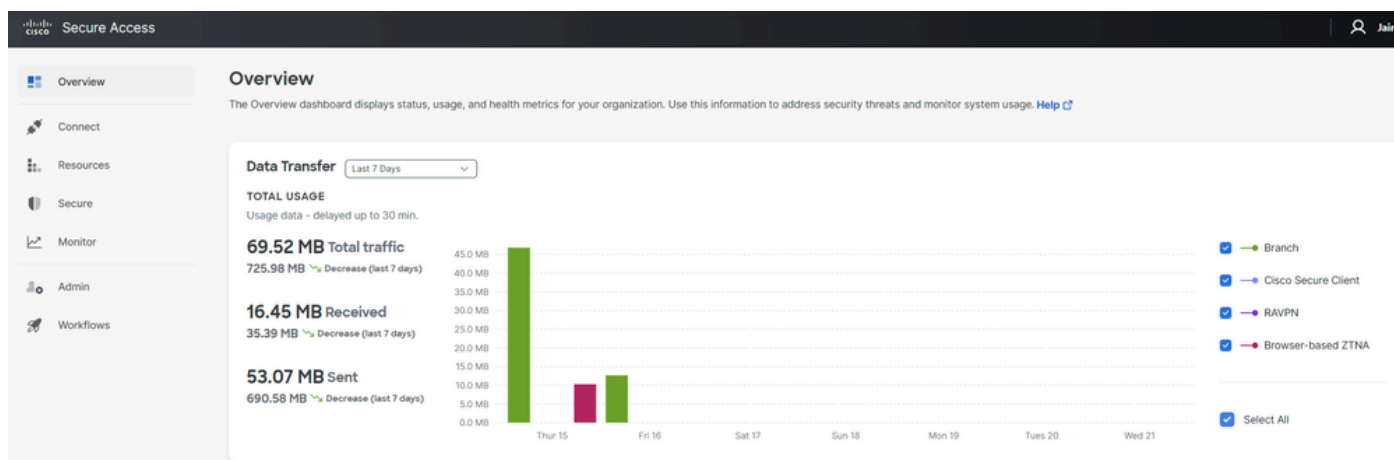
paloalto[®]
NETWORKS

A Cisco projetou o Secure Access para proteger e fornecer acesso a aplicativos privados, no local e baseados em nuvem. Ele também protege a conexão da rede à Internet. Isso é obtido por meio da implementação de vários métodos e camadas de segurança, todos voltados para preservar as informações à medida que elas são acessadas pela nuvem.

Configurar

Configurar a VPN no acesso seguro

Navegue até o painel de administração do [Secure Access](#).



- Clique em **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

Acesso seguro - Conexões de rede

- Em Network Tunnel Groups clique em + 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 >

Acesso seguro - Grupos de túnel de rede

- Configure Tunnel Group Name, Region e Device Type
- Clique em **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](#)



Observação: escolha a região mais próxima ao local do firewall.

-
- Configure o Tunnel ID Format e Passphrase
 - Clique em 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](#)

- Configure os intervalos de endereços IP ou hosts que você configurou na sua rede e deseja passar o tráfego pelo Secure Access
- Clique em **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](#)

Acesso seguro - Grupos de túneis - Opções de roteamento

Depois de clicar nas informações sobre **Save** o túnel que são exibidas, salve essas informações para a próxima etapa, **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	

Configurar o túnel em Palo Alto

Configurar a interface do túnel

Navegue até o Painel 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

- No menuConfig, configure o Virtual Router, Security Zone e atribua um 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

- Em IPv4, configure um IP não roteável. Por exemplo, você pode usar 169.254.0.1/30
- Clique em OK

Tunnel Interface ?

Interface Name: tunnel . 1

Comment:

Netflow Profile: None

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

Depois disso, você pode ter algo assim configurado:

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	

Se tiver configurado dessa forma, você poderá clicar em **Commit** para salvar a configuração e continuar com a próxima etapa, Configure IKE Crypto Profile.

Configurar perfil de criptografia IKE

Para configurar o perfil de criptografia, navegue até:

- Network > Network Profile > IKE Crypto
- Clique em 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

- Configure os próximos parâmetros:
 - **Name:** Configure um nome para identificar o perfil.
 - **DH GROUP:** grupo19
 - **AUTHENTICATION:** não-autenticação
 - **ENCRYPTION:** aes-256-gcm
 - Timers
 - Key Lifetime: 8 horas
 - **IKEv2 Authentication:**0
- Após ter tudo configurado, clique em **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

Se ela estiver configurada dessa forma, você poderá clicar em **Commit** para salvar a configuração e continuar com a próxima etapa, Configure IKE Gateways.

Configurar gateways IKE

Para configurar gateways IKE

- Network > Network Profile > IKE Gateways
- Clique emAdd

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

- Configure os próximos parâmetros:
 - Name: Configure um nome para identificar os Gateways Ike.
 - **Version** : modo somente IKEv2
 - Address Type :IPv4
 - **Interface** : selecione sua interface WAN da Internet.
 - Local IP Address: selecione o IP da interface WAN da Internet.
 - **Peer IP Address Type** :IP
 - Peer Address: Use o IP of Primary IP Datacenter IP Address, fornecido na etapa [Tunnel Data](#).
 - Authentication: Chave pré-compartilhada
 - Pre-shared Key : Use o valor **passphrase** fornecido na etapa [Tunnel Data](#).
 - **Confirm Pre-shared Key** : Use o valor **passphrase** fornecido na etapa [Tunnel Data](#).
 - **Local Identification** : Escolha **User FQDN (Email address)** e use o **Primary Tunnel ID** dado na etapa, [Dados do túnel](#).
 - **Peer Identification** : IP AddressEscolha e use o 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

- Clique em **Advanced Options**

- **Enable NAT Traversal**

- Selecione o **IKE Crypto Profile** criado na etapa, [Configurar perfil de criptografia IKE](#)
- Marcar a caixa de seleção para **Liveness Check**
- Clique em **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

Se ela estiver configurada dessa forma, você poderá clicar em **Commit** para salvar a configuração e continuar com a próxima etapa, Configure IPSEC Crypto.

Configurar perfil de criptografia IPSEC

Para configurar os gateways IKE, navegue até Network > Network Profile > IPSEC Crypto

- Clique em 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

- Configure os próximos parâmetros:
 - **Name:** use um nome para identificar o perfil IPsec de acesso seguro
 - IPSec Protocol: ESP
 - **ENCRYPTION:** aes-256-gcm
 - DH Group: no-pfs, 1 hora
- Clique em 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

Se ela estiver configurada dessa forma, você poderá clicar em **Commit** para salvar a configuração e continuar com a próxima etapa, Configure IPSec Tunnels.

Configurar túneis IPSec

Para configurar **IPSec Tunnels**, navegue até Network > IPSec Tunnels.

- Clique em Add

The screenshot shows the PA-VM Network configuration page. The 'NETWORK' tab is selected in the top navigation bar. In the left sidebar, 'IPSec Tunnels' is highlighted. The main content area displays a table of IKE Gateway/Satellite configurations:

	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

At the bottom of the interface, the 'Add' button is highlighted with a red box. Other buttons include 'Delete', 'Enable', 'Disable', and 'PDF/CSV'.

- Configure os próximos parâmetros:
 - **Name:** use um nome para identificar o túnel de acesso seguro
 - **Tunnel Interface:** Escolha a interface de túnel configurada na etapa, [Configure a interface de túnel](#).
 - **Type:** Chave automática
 - **Address Type:** IPv4
 - **IKE Gateways:** Escolha os gateways IKE configurados na etapa, [Configurar gateways IKE](#).
 - **IPsec Crypto Profile:** Escolha os gateways IKE configurados na etapa, [Configurar perfil de criptografia IPSEC](#)
 - Marcar a caixa de seleção para **Advanced Options**
 - **IPSec Mode Tunnel:** Escolha Túnel.

- Clique em 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

Agora que sua VPN foi criada com êxito, você pode prosseguir com a etapa, **Configure Policy Based Forwarding**.

Configurar Encaminhamento Baseado em Política

Para configurar **Policy Based Forwarding**, navegue até Policies > Policy Based Forwarding.

- Clique em 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

- Configure os próximos parâmetros:

- General

- **Name:** use um nome para identificar o acesso seguro, encaminhamento de base de política (roteamento por origem)

- Source

- **Zone:** selecione as Zonas de onde você tem planos para rotear o tráfego com base na origem

- **Source Address:** configure o host ou as redes que você deseja usar como origem.
- **Source Users:** configure os usuários para os quais deseja rotear o tráfego (somente se aplicável)

- Destination/Application/Service

- Destination Address: Você pode deixá-lo como Qualquer ou pode especificar os intervalos de endereços de Acesso seguro (100.64.0.0/10)

- Forwarding

- **Action:**Encaminhar

- **Egress Interface:** Escolha a interface de túnel configurada na etapa, [Configure a interface de túnel](#).

- **Next Hop:**Nenhum

- Clique OK em e 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: [dropdown]

Disable this rule if nexthop/monitor ip is unreachable

IP Address: [text box]

Enforce Symmetric Return

NEXT HOP ADDRESS LIST

[+ Add] [- Delete]

Schedule: None

OK Cancel

Agora você tem tudo configurado em Palo Alto; depois de configurar a rota, o túnel pode ser estabelecido e você precisa continuar configurando o RA-VPN, o ZTA baseado em navegador ou o ZTA base do cliente no painel de acesso seguro.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.