

Configurazione di Secure Access con Palo Alto Firewall

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Configurare la VPN su accesso sicuro](#)

[Dati tunnel](#)

[Configurazione del tunnel su Palo Alto](#)

[Configurazione dell'interfaccia del tunnel](#)

[Configura profilo di crittografia IKE](#)

[Configurazione gateway IKE](#)

[Configura profilo di crittografia IPSEC](#)

[Configurare i tunnel IPsec](#)

[Configura inoltro basato su criteri](#)

Introduzione

In questo documento viene descritto come configurare Secure Access con Palo Alto Firewall.

Prerequisiti

- [Configura assegnazione ruoli utente](#)
- [Configurazione autenticazione SSO ZTNA](#)
- [Configura accesso sicuro VPN di accesso remoto](#)

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Palo Alto versione 11.x Firewall
- Accesso sicuro
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA
- ZTNA senza client

Componenti usati

Le informazioni fornite in questo documento si basano su:

- Palo Alto versione 11.x Firewall
- Accesso sicuro
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse



CISCO

Secure

Access



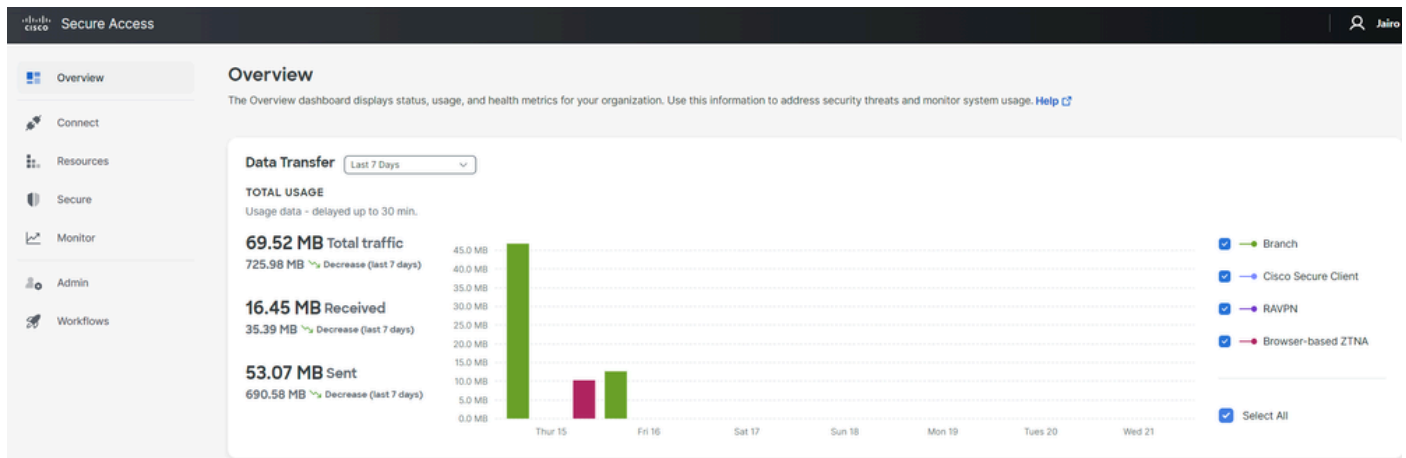
paloalto[®]
NETWORKS

Cisco ha progettato Secure Access per proteggere e fornire accesso alle applicazioni private, sia in sede che basate su cloud. Inoltre, garantisce il collegamento dalla rete a Internet. Questo risultato è ottenuto attraverso l'implementazione di più metodi e livelli di sicurezza, il tutto finalizzato a preservare le informazioni mentre vi accedono tramite il cloud.

Configurazione

Configurare la VPN su accesso sicuro

Passare al pannello di amministrazione di [Accesso sicuro](#).



- Fare clic su **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

Accesso sicuro - Connessioni di rete

- In fareNetwork Tunnel Groups clic su + 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 >

Accesso sicuro - Gruppi di tunnel di rete

- Configurazione Tunnel Group Name, Regione Device Type
- Fare clic su **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](#)



Nota: scegliere la regione più vicina alla posizione del firewall.

-
- Configurare Tunnel ID Formate Passphrase
 - Fare clic su 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](#)

- Configurare gli intervalli di indirizzi IP o gli host configurati nella rete e che si desidera passare il traffico attraverso l'accesso sicuro
- Fare clic su **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](#)

Accesso sicuro - Gruppi di tunnel - Opzioni di routing

Dopo aver fatto clic sulle informazioni **Save** del tunnel che vengono visualizzate, salvare le informazioni per il passaggio successivo, **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	

Configurazione del tunnel su Palo Alto

Configurazione dell'interfaccia del tunnel

Passare al dashboard di 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

- In menu (Menu)Config, configurate le opzioni Virtual Router, Security Zone e assegna aSuffix 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

- In IPv4, configurare un indirizzo IP non instradabile. Ad esempio, è possibile utilizzare 169.254.0.1/30
- Fare clic su 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

In seguito, sarà possibile configurare una soluzione simile alla seguente:

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 la configurazione è stata configurata in questo modo, è possibile fare clic su **Commit** per salvarla e continuare con il passaggio successivo, Configura IKE Crypto Profile.

Configura profilo di crittografia IKE

Per configurare il profilo crittografico, passare a:

- Network > Network Profile > IKE Crypto
- Fare clic su 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

- Configurare i parametri successivi:
 - **Name:** configurare un nome per identificare il profilo.
 - **DH GROUP:** gruppo19
 - **AUTHENTICATION:** non autenticazione
 - **ENCRYPTION:** aes-256-gcm
 - Timers
 - Key Lifetime: 8 ore
 - **IKEv2 Authentication:**0
- Dopo aver configurato tutti gli elementi, fare clic su **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 la configurazione è stata configurata in questo modo, è possibile fare clic su **Commit** per salvarla e continuare con il passaggio successivo, Configure IKE Gateways.

Configurazione gateway IKE

Per configurare i gateway IKE

- Network > Network Profile > IKE Gateways
- Fare clic su 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

- Configurare i parametri successivi:
 - Name: consente di configurare un nome per identificare i gateway Ike.
 - **Version** : modalità solo IKEv2
 - Address Type :IPv4
 - **Interface** : selezionare l'interfaccia WAN Internet.
 - Local IP Address: selezionare l'indirizzo IP dell'interfaccia WAN Internet.
 - **Peer IP Address Type** :IP
 - Peer Address: utilizzare l'indirizzo IP di Primary IP Datacenter IP Address, specificato nella fase [Dati tunnel](#).
 - Authentication: chiave già condivisa
 - Pre-shared Key : utilizzare i dati **passphrase** forniti nella fase [Dati tunnel](#).
 - **Confirm Pre-shared Key** : utilizzare i dati **passphrase** forniti nella fase [Dati tunnel](#).
 - **Local Identification** : scegliere **User FQDN (Email address)** e utilizzare i dati **Primary Tunnel ID** forniti nel passo [Dati tunnel](#).
 - **Peer Identification** : IP AddressScegliere e utilizzare il 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

- Fare clic su Advanced Options

- **Enable NAT Traversal**

- Selezionare il file **IKE Crypto Profile** creato nel passo [Configura profilo di crittografia IKE](#)
- Selezionare la casella di controllo **Liveness Check**
- Fare clic su **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

Se la configurazione è stata configurata in questo modo, è possibile fare clic su **Commit** per salvarla e continuare con il passaggio successivo, Configure IPSEC Crypto.

Configura profilo di crittografia IPSEC

Per configurare i gateway IKE, passare a Network > Network Profile > IPSEC Crypto

- Fare clic su 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

- Configurare i parametri successivi:
 - **Name:** utilizzare un nome per identificare il profilo IPSec di accesso sicuro
 - IPSec Protocol: ESP
 - **ENCRYPTION:** aes-256-gcm
 - DH Group: no-pfs, 1 ora
- Fare clic su 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

Se la configurazione è stata configurata in questo modo, è possibile fare clic su **Commit** per salvarla e continuare con il passaggio successivo, Configure IPSec Tunnels.

Configurare i tunnel IPSec

Per configurare **IPSec Tunnels**, passare a Network > IPSec Tunnels.

- Fare clic su 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

	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

- Configurare i parametri successivi:
 - **Name:** utilizzare un nome per identificare il tunnel Secure Access
 - **Tunnel Interface:** scegliere l'interfaccia del tunnel configurata nel passaggio [Configurazione dell'interfaccia del tunnel](#).
 - **Type:** Tasto automatico
 - **Address Type:** IPv4
 - **IKE Gateways:** scegliere i gateway IKE configurati nel passo [Configurazione gateway IKE](#).
 - **IPsec Crypto Profile:** scegliere i gateway IKE configurati nel passaggio [Configurazione profilo di crittografia IPSEC](#)
 - Selezionare la casella di controllo **Advanced Options**
 - **IPSec Mode Tunnel:** Scegliere Tunnel.

- Fare clic su 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

Ora che la tua VPN è stata creata correttamente, puoi procedere con il passaggio, **Configure Policy Based Forwarding**.

Configura inoltro basato su criteri

Per configurare **Policy Based Forwarding**, passare a Policies > Policy Based Forwarding.

- Fare clic su 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

- Configurare i parametri successivi:

- General

- **Name:** utilizzare un nome per identificare l'accesso sicuro, inoltre base criteri (routing per origine)

- Source

- **Zone:** selezionare le zone da cui si prevede di instradare il traffico in base all'origine

- **Source Address:** configurare l'host o le reti da utilizzare come origine.

- Source Users: configurare gli utenti che si desidera indirizzare il traffico (solo se applicabile)

- Destination/Application/Service

- Destination Address: è possibile lasciare il campo impostato su Qualsiasi oppure specificare gli intervalli di indirizzi di Accesso sicuro (100.64.0.0/10)

- Forwarding

- **Action:** Inoltra

- **Egress Interface:** scegliere l'interfaccia del tunnel configurata nel passaggio [Configurazione dell'interfaccia del tunnel](#).

- **Next Hop:** Nessuna

- Fare clic OK su 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: [Empty]

Disable this rule if nexthop/monitor ip is unreachable

IP Address: [Empty]

Enforce Symmetric Return

NEXT HOP ADDRESS LIST

[Empty List]

+ Add - Delete

Schedule: None

OK Cancel

Ora si dispone di tutto ciò che è stato configurato su Palo Alto; dopo aver configurato il percorso, è possibile stabilire il tunnel e continuare a configurare RA-VPN, ZTA basata su browser o ZTA basata su client su Secure Access Dashboard.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).