

Palo Altoファイアウォールを使用したセキュアアクセスの設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[セキュアアクセスでのVPNの設定](#)

[トンネルデータ](#)

[Palo Altoでのトンネルの設定](#)

[トンネルインターフェイスの設定](#)

[IKE暗号化プロファイルの設定](#)

[IKEゲートウェイの設定](#)

[IPSEC暗号化プロファイルの設定](#)

[IPSecトンネルの設定](#)

[ポリシーベースの転送の設定](#)

はじめに

このドキュメントでは、Palo Altoファイアウォールを使用してセキュアアクセスを設定する方法について説明します。

前提条件

- [ユーザプロビジョニングの設定](#)
- [ZTNA SSO認証設定](#)
- [リモートアクセスVPNセキュアアクセスの設定](#)

要件

次の項目に関する知識があることが推奨されます。

- Palo Alto 11.xバージョンのファイアウォール
- セキュアなアクセス
- Cisco Secure Client - VPN (トンネルモード)
- Cisco Secureクライアント – ZTNA
- クライアントレスZTNA

使用するコンポーネント

このドキュメントの情報は、次のハードウェアに基づくものです。

- Palo Alto 11.xバージョンのファイアウォール
- セキュアなアクセス
- Cisco Secure Client - VPN (トンネルモード)
- Cisco Secureクライアント - ZTNA

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明



CISCO

Secure

Access



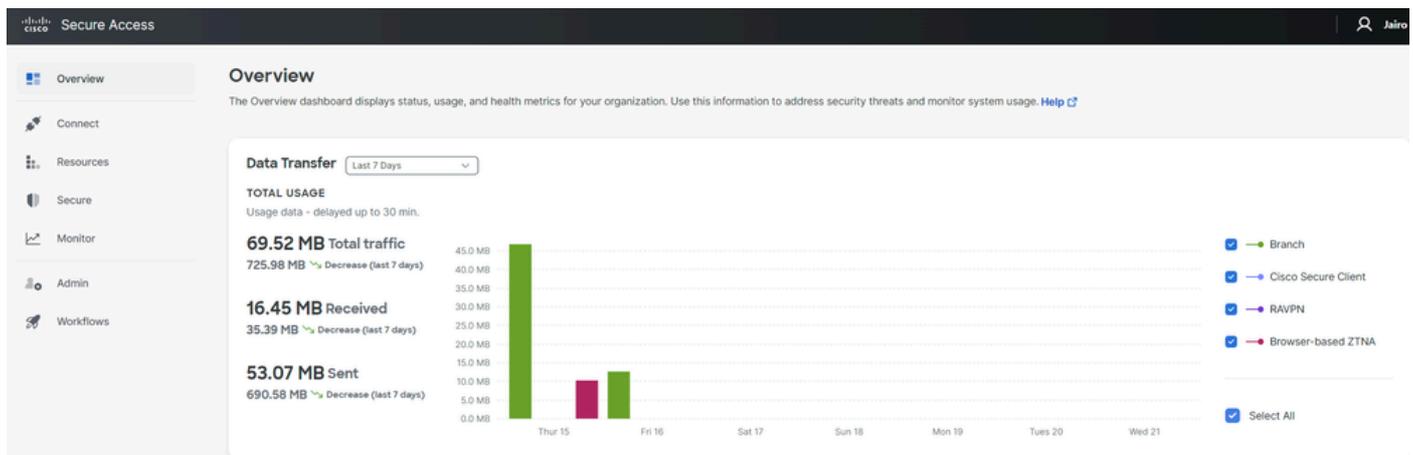
paloalto[®]
NETWORKS

シスコは、プライベートアプリケーション（オンプレミスとクラウドベースの両方）を保護し、アクセスを提供するセキュアなアクセスを設計しました。また、ネットワークからインターネットへの接続も保護します。これは、複数のセキュリティ方式とレイヤの実装によって実現されます。すべての目的は、クラウド経由でアクセスする情報を保持することです。

設定

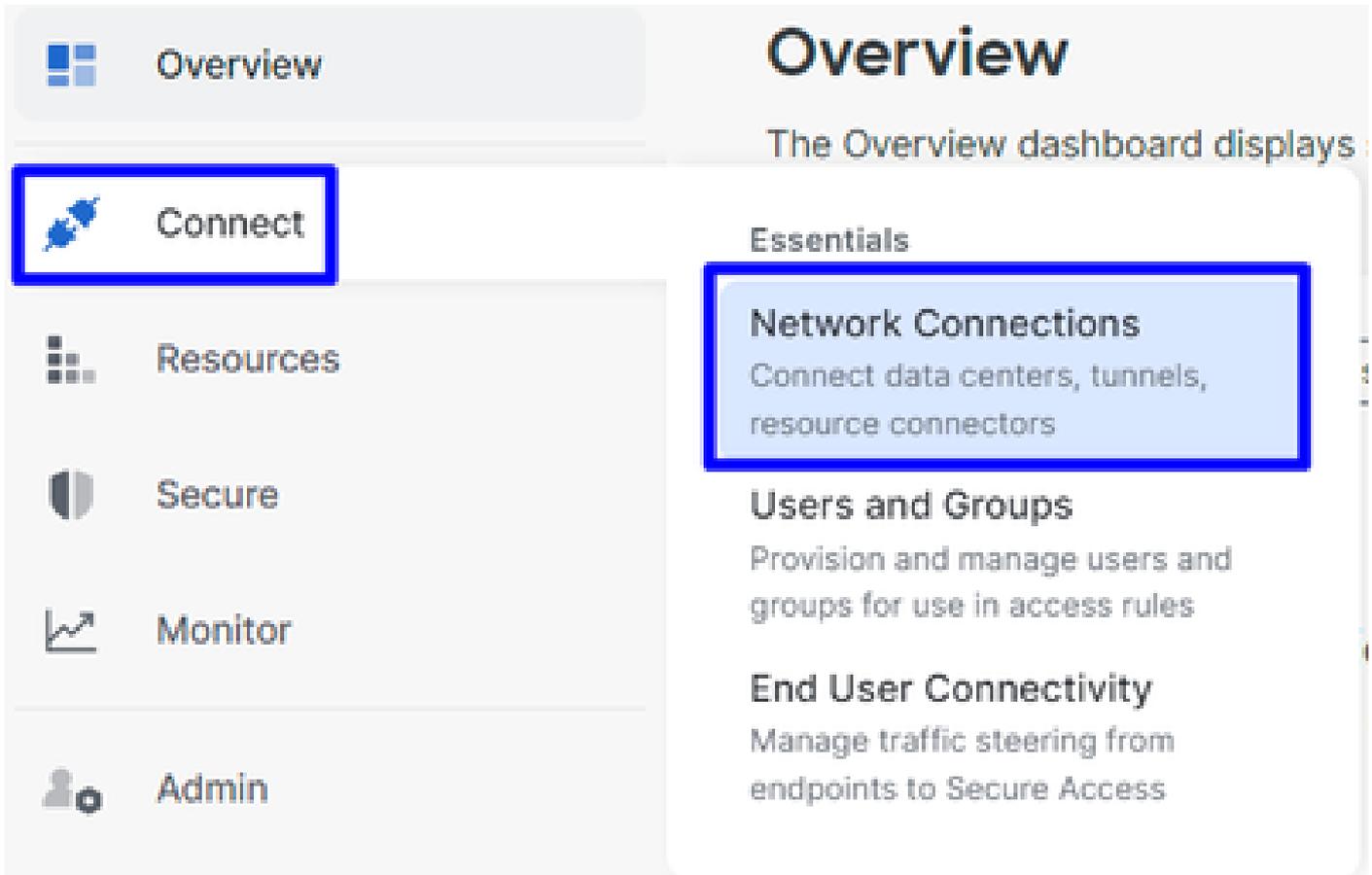
セキュアアクセスでのVPNの設定

[Secure Access](#)の管理パネルに移動します。



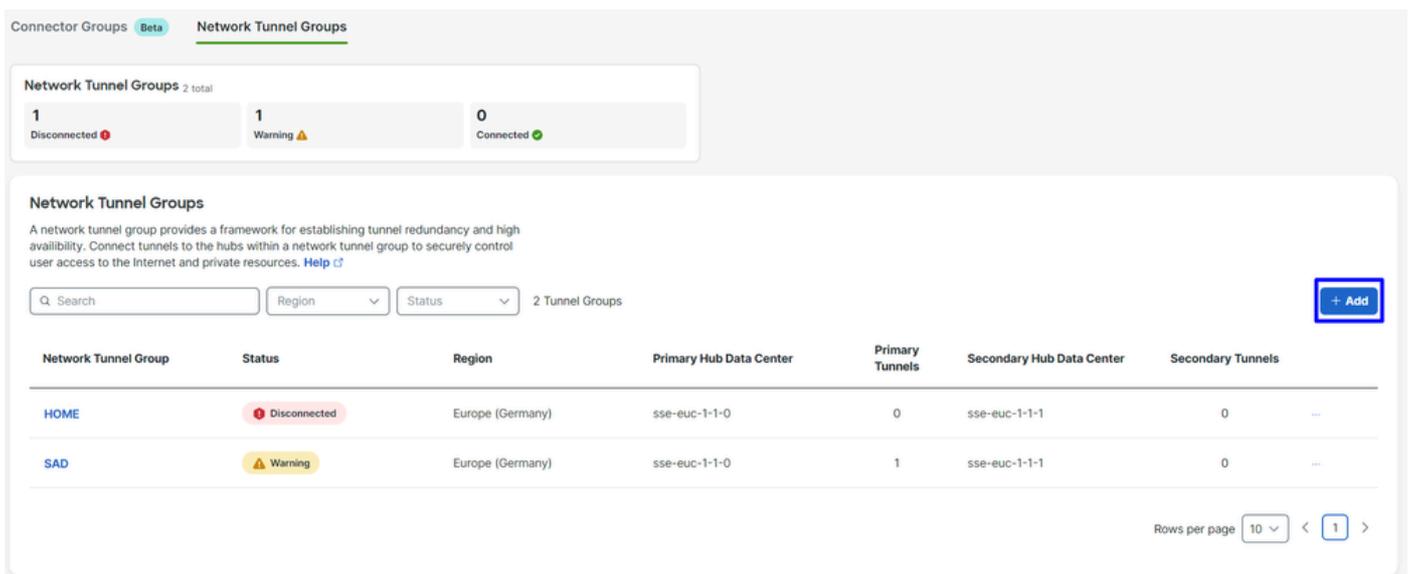
セキュアアクセス – メインページ

- クリック Connect > Network Connections



セキュアアクセス – ネットワーク接続

- 「Network Tunnel Groups」で、+ Add



セキュアアクセス – ネットワークトンネルグループ

- Tunnel Group Name、Regionの設定 Device Type
- クリック 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

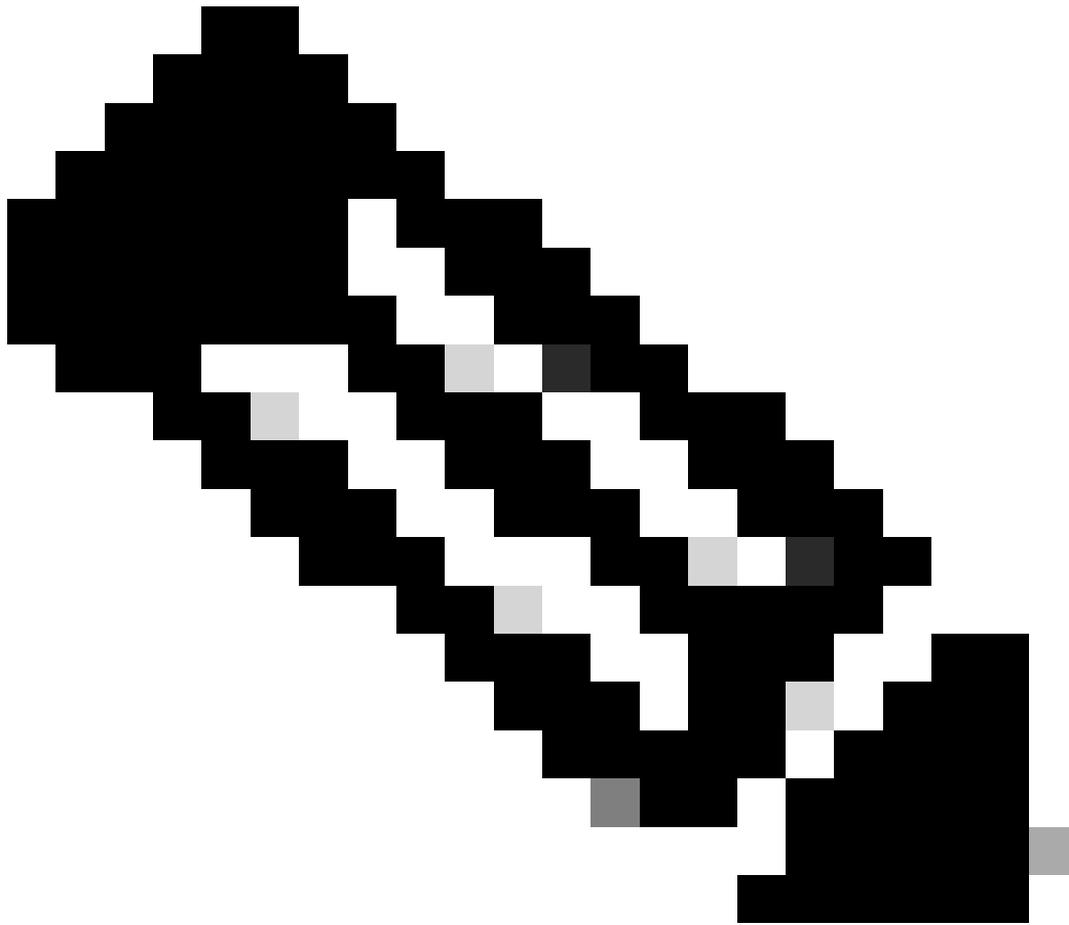
 ∨

Device Type

 ∨

[Cancel](#)

[Next](#)



注：ファイアウォールの場所に最も近い地域を選択します。

Tunnel ID Format

-
- コマンドと Passphrase
 - クリック 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](#)

- ネットワークで設定したIPアドレス範囲またはホストを設定し、トラフィックをセキュアアクセス経由で通過させる
- クリック **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](#)

セキュアアクセス – トンネルグループ – ルーティングオプション

トンネルに関する**Save**る情報をクリックして表示した後、次の手順**Configure the tunnel on Palo Alto**でその情報を保存してください。

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	

Palo Altoでのトンネルの設定

トンネルインターフェイスの設定

Palo Altoダッシュボードに移動します。

- 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

- ConfigメニューでVirtual Router、Security Zoneを設定し、Suffix Number IPv4

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

- の下で、ルーティング不能IPを設定します。たとえば、169.254.0.1/30
- クリック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

その後、次のように設定できます。

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	

このように設定してある場合は、**Commit** をクリックして設定を保存し、次のステップConfigure IKE Crypto Profileに進みます。

IKE暗号化プロファイルの設定

暗号化プロファイルを設定するには、次の場所に移動します。

- Network > Network Profile > IKE Crypto
- クリックAdd

<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

Buttons: **+ Add** (highlighted), - Delete, Clone, PDF/CSV

- 次のパラメータを設定します。

- **Name** : プロファイルを識別するための名前を設定します。

- **DH GROUP** : グループ19
- **AUTHENTICATION** : 非認証
- **ENCRYPTION**: aes-256-gcm
- Timers

- Key Lifetime:8 時間

- **IKEv2 Authentication**:0

- すべての設定が完了したら、**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

このように設定してある場合は、**Commit** をクリックして設定を保存し、次のステップに進みます。 Configure IKE Gateways.

IKEゲートウェイの設定

IKEゲートウェイを設定するには

- Network > Network Profile > IKE Gateways
- クリック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

- 次のパラメータを設定します。

- Name:Ikeゲートウェイを識別するための名前を設定します。

- **Version** : IKEv2専用モード
- Address Type : IPv4
- **Interface** : インターネットWANインターフェイスを選択します。
- Local IP Address : インターネットWANインターフェイスのIPを選択します。
- **Peer IP Address Type** :IP
- Peer Address:手順「[Tunnel Data](#)」で指定したPrimary IP Datacenter IP AddressのIPを使用します。
- Authentication:Pre-Shared Key
- Pre-shared Key : [Tunnel Data](#)の手順で指定した **passphrase** を使用します。
- **Confirm Pre-shared Key** : [Tunnel Data](#)の手順で指定した **passphrase** を使用します。
- **Local Identification** : を選択User FQDN (Email address) し、手順「[Tunnel Data](#)」で指定したPrimary Tunnel IDを使用します。
- **Peer Identification** : IP Addressを選択してPrimary IP Datacenter IP Addressを使用します。

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			

- クリックAdvanced Options

- **Enable NAT Traversal**

- ステップ[Configure IKE Crypto Profile](#)で作IKE Crypto Profile 成した
- チェックボックスをオンにする **Liveness Check**
- クリック **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

このように設定してある場合は、**Commit** をクリックして設定を保存し、次のステップに進みます。 Configure IPSEC Crypto.

IPSEC暗号化プロファイルの設定

IKEゲートウェイを設定するには、 Network > Network Profile > IPSEC Crypto

- クリック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

- 次のパラメータを設定します。
 - **Name** : 名前を使用してセキュアアクセスIPsecプロファイルを識別します。
 - IPSec Protocol:ESP
 - **ENCRYPTION**: aes-256-gcm
 - DH Group: pfsなし、1時間
- クリック 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

このように設定してある場合は、**Commit** をクリックして設定を保存し、次のステップに進みます。Configure IPSec Tunnels.

IPSecトンネルの設定

IPSec Tunnelsを設定するには、Network > IPSec Tunnelsに移動します。

- クリック 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 Crypt

	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

GlobalProtect IPSec Crypt **+ Add** Delete Enable Disable PDF/CSV

- 次のパラメータを設定します。
 - **Name** : セキュアアクセストンネルを識別する名前を使用します。
 - **Tunnel Interface** : ステップ [Configure the tunnel interface](#) で設定したトンネルインターフェイスを選択します。
 - **Type** : オートキー
 - **Address Type**: IPv4
 - **IKE Gateways** : ステップ「[IKEゲートウェイの設定](#)」で設定したIKEゲートウェイを選択します。
 - **IPsec Crypto Profile** : ステップ [Configure IPSEC Crypto Profile](#) で設定したIKEゲートウェイを選択します。
 - チェックボックスをオンにする **Advanced Options**
 - **IPsec Mode Tunnel**: Tunnelを選択します。

- クリック 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

VPNが正常に作成されたら、**Configure Policy Based Forwarding**の手順に進みます。

ポリシーベースの転送の設定

Policy Based Forwardingを設定するには、Policies > Policy Based Forwarding.

- クリック 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

- 次のパラメータを設定します。

- General

- **Name** : 名前を使用して、セキュアアクセス、ポリシーベース転送 (発信元によるルーティング) を識別します。

- Source

- **Zone** : 送信元に基づいてトラフィックをルーティングする計画があるゾーンを選択します。
- **Source Address** : 送信元として使用する1つまたは複数のホストを設定します。
- **Source Users** : トラフィックをルーティングするユーザを設定します (該当する場合のみ) 。

- Destination/Application/Service

- Destination Address : これをAnyのままにしておくか、セキュアアクセス(100.64.0.0/10)のアドレス範囲を指定できます。

- Forwarding

- Action:転送

- Egress Interface : ステップ[Configure the tunnel interface](#)で設定したトンネルインターフェイスを選択します。

- Next Hop:None
OK

- をクリックし、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

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。