

# Fortigate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](#)

#### [FortigateでのVPNサイト間の設定](#)

##### [Network](#)

##### [\[Authentication\]](#)

##### [フェーズ1の提案](#)

##### [フェーズ2の提案](#)

#### [トンネルインターフェイスの設定](#)

#### [ポリシールートの設定](#)

### [確認](#)

---

## はじめに

このドキュメントでは、Fortigate Firewall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。

- Fortigate 7.4.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

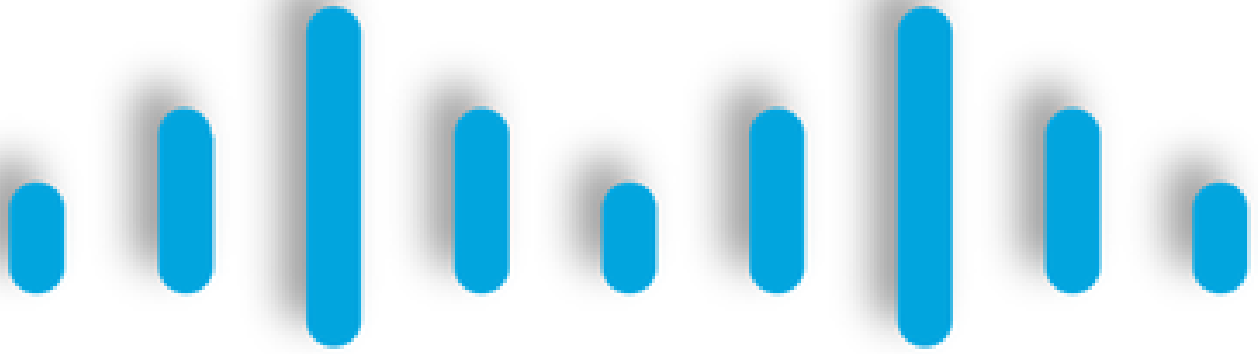
## 使用するコンポーネント

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。

- Fortigate 7.4.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

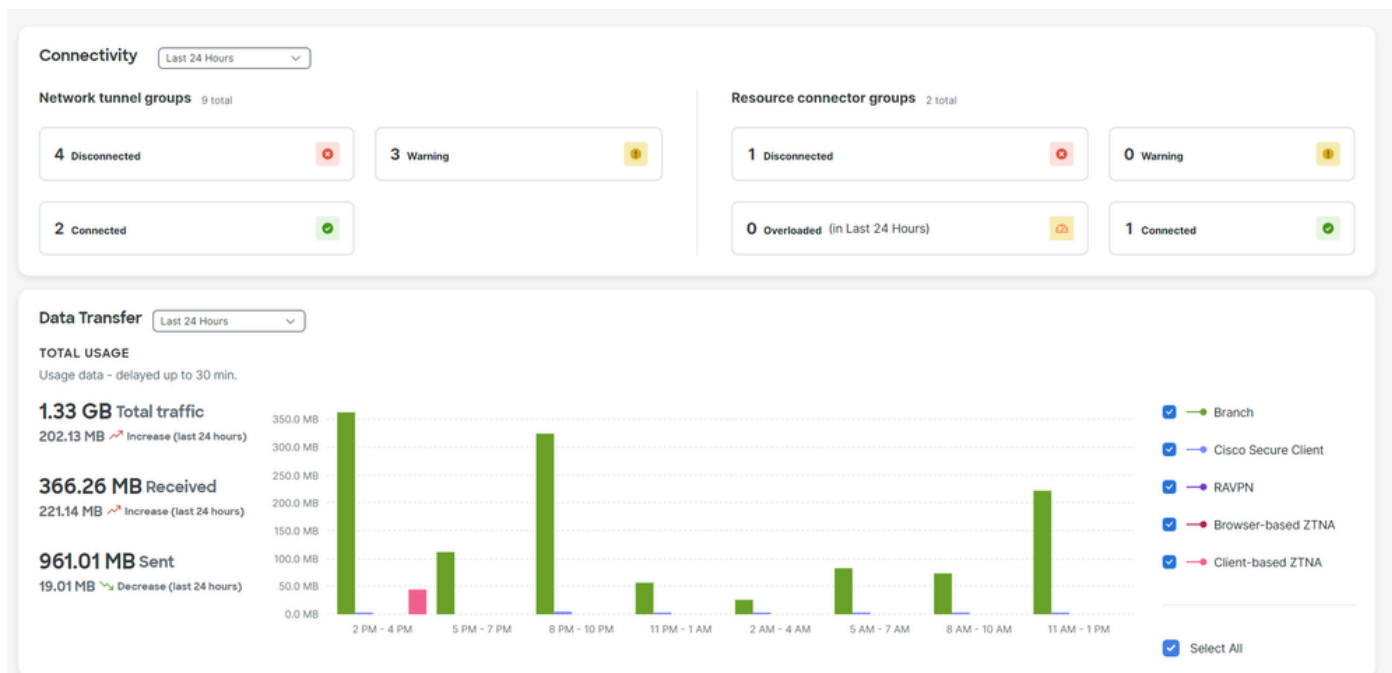
# FORTINET®

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。

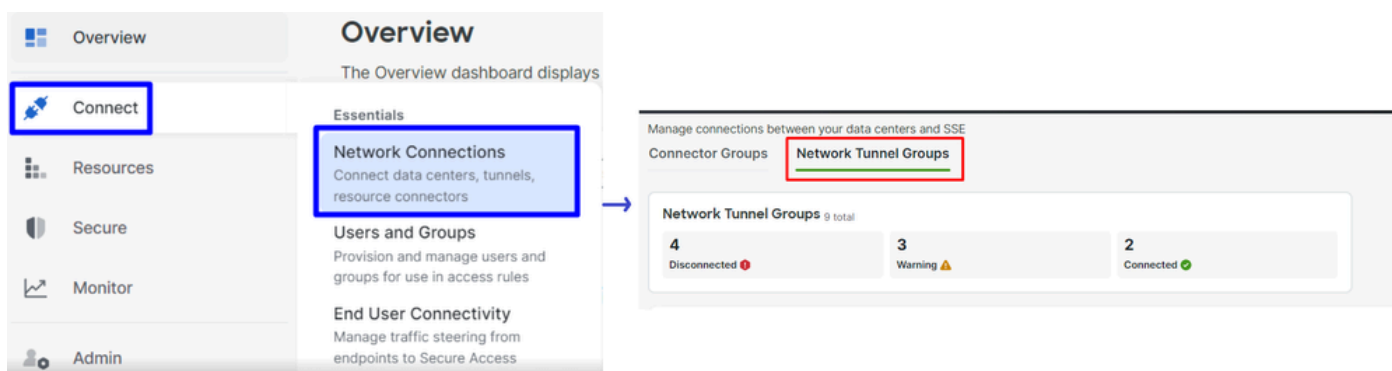
設定

## 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。



- クリック Connect > Network Connections > Network Tunnels Groups



- 「Network Tunnel Groups」で、+ Add Tunnel Group Name

### 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 9 Tunnel Groups

+ Add

- 、Regionの設定 Device Type
- クリック Next

1 **General Settings**

2 Tunnel ID and Passphrase

3 Routing

4 Data for Tunnel Setup



## 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

- ✓ General Settings
- ✓ Tunnel ID and Passphrase
- 3 Routing
- 4 Data for Tunnel Setup

## Tunnel ID and Passphrase

Configure the tunnel ID and passphrase that devices will use to connect to this tunnel group.

### Tunnel ID Format

Email  IP Address

### Tunnel ID

fortigate  @<org>  
<hub>.sse.cisco.com

### Passphrase

.....

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

.....



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

- ✓ General Settings
- ✓ Tunnel ID and Passphrase
- 3 Routing
- 4 Data for Tunnel Setup

## Routing options and network overlaps

Configure routing options for this tunnel group.

### Network subnet overlap

Enable NAT / Outbound only

Select if the IP address space of the subnet behind this tunnel group overlaps with other IP address spaces in your network. When selected, private applications behind these tunnels are not accessible.

### 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.

128.66.0.0/16, 192.0.2.0/24

192.168.100.0/24

Dynamic routing

Use this option when you have a BGP peer for your on-premise router.



Cancel

Back

Save

トンネルに関するSave 情報をクリックして表示した後、次の手順のためにその情報を保存してください。 **Configure the VPN Site**

to Site on Fortigate.

トンネルデータ

## 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.

<b>Primary Tunnel ID:</b>	@	-sse.cisco.com	📄
<b>Primary Data Center IP Address:</b>	18.156.145.74		📄
<b>Secondary Tunnel ID:</b>	@	-sse.cisco.com	📄
<b>Secondary Data Center IP Address:</b>	3.120.45.23		📄
<b>Passphrase:</b>		CP	📄

FortigateでのVPNサイト間の設定

Fortigateダッシュボードに移動します。

- クリック VPN > IPsec Tunnels





VPN



IPsec Tunnels



IPsec Wizard

IPsec Tunnel Template

VPN Location Map

- クリック Create New > IPsec Tunnels

Custom

+ Create new ▾

IPsec Tunnel

IPsec Aggregate

Custom 2

- をクリックし、Name を設定して、Next をクリックします。

#### 1 VPN Setup

Name 2 Cisco Secure

Template type Site to Site Hub-and-Spoke Remote Access Custom 1

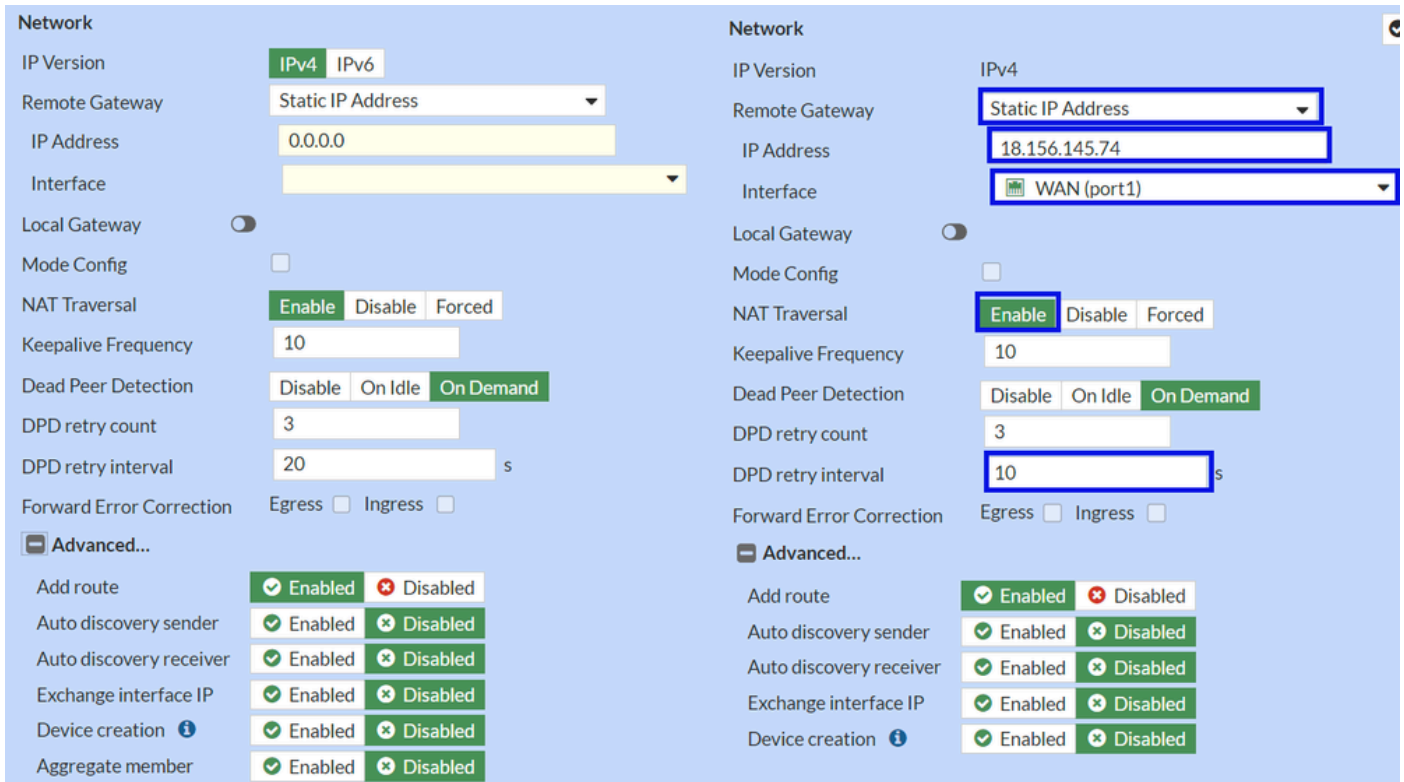
< Back

Next > 3

Cancel

次の図では、パーNetwork ツの設定を構成する方法を示します。

Network



- Network

- IP Version : IPv4

- **Remote Gateway** :スタティック IP アドレス
- **IP Address**:ステップ[Tunnel Data](#)で指定Primary IP Datacenter IP Address,したIPアドレスを使用します。
- **Interface** : トンネルの確立に使用する予定のWANインターフェイスを選択します
- **Local Gateway** : デフォルトで無効
- **Mode Config** : デフォルトで無効
- **NAT Traversal** :Enable
- **Keepalive Frequency** :10
- **Dead Peer Detection** : オンデマンド
- **DPD retry count** :3
- **DPD retry interval** :10
- **Forward Error Correction** : チェックボックスはオンにしないでください。
- **Advanced...** : これをイメージとして設定します。

ここで、IKE Authenticationを設定します。

[Authentication]

Authentication		Authentication	
Method	Pre-shared Key	Method	Pre-shared Key
Pre-shared Key		Pre-shared Key	*****
IKE		IKE	
Version	1 2	Version	1 2
Mode	Aggressive Main (ID protection)		

- **Authentication**

- **Method** : デフォルトの事前共有キー

- **Pre-shared Key** : 手順「[トンネルデータ](#)」で指定したPassphraseを使用します。

- **IKE**

- **Version** : バージョン2を選択します。



注：セキュアアクセスはIKEv2のみをサポートします

---

次に、**Phase 1 Proposal**を設定します。

フェーズ1の提案

The image shows two side-by-side configuration panels for Phase 1 Proposal. The left panel shows a list of four proposals with encryption and authentication methods. The right panel shows a detailed view of a proposal with encryption set to AES256, authentication to SHA256, Diffie-Hellman groups 19 and 20 selected, a key lifetime of 86400 seconds, and a local ID.

- Phase 1 Proposal

- Encryption : AES256を選択

- Authentication : SHA256を選択
- Diffie-Hellman Groups : ボックス19と20をオンにします。
- Key Lifetime (seconds) : デフォルトで86400
- Local ID : Primary Tunnel IDを使用します。これは、[トンネルデータ](#)

次に、 **Phase 2 Proposal**を設定します。

フェーズ2の提案

**New Phase 2**

Name: CSA

Comments: Comments

Local Address: addr\_subnet 0.0.0.0/0.0.0.0

Remote Address: addr\_subnet 0.0.0.0/0.0.0.0

**Advanced...**

Phase 2 Proposal **Add**

Encryption	AES128	Authentication	SHA1	X
Encryption	AES256	Authentication	SHA1	X
Encryption	AES128	Authentication	SHA256	X
Encryption	AES256	Authentication	SHA256	X
Encryption	AES128GCM			X
Encryption	AES256GCM			X
Encryption	CHACHA20POLY1305			X

Enable Replay Detection

Enable Perfect Forward Secrecy (PFS)

Diffie-Hellman Group:  32  31  30  29  28  27  21  20  19  18  17  16  15  14  5  2  1

Local Port: All

Remote Port: All

Protocol: All

Auto-negotiate:

Autokey Keep Alive:

Key Lifetime: Seconds 43200

**New Phase 2**

Name: CSA

Comments: Comments

Local Address: addr\_subnet 0.0.0.0/0.0.0.0

Remote Address: addr\_subnet 0.0.0.0/0.0.0.0

**Advanced...**

Phase 2 Proposal **Add**

Encryption: AES128 Authentication: SHA256

Enable Replay Detection

Enable Perfect Forward Secrecy (PFS)

Local Port: All

Remote Port: All

Protocol: All

Auto-negotiate:

Autokey Keep Alive:

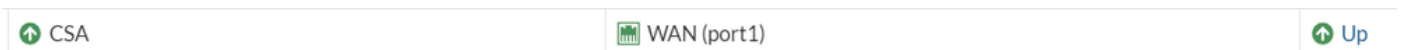
Key Lifetime: Seconds 43200

- New Phase 2
  - **Name** : デフォルトのままにする ( VPNの名前から取得 )
  - **Local Address** : デフォルトで許可(0.0.0.0/0.0.0.0)
  - **Remote Address** : デフォルトで許可(0.0.0.0/0.0.0.0)
  
- Advanced
  - **Encryption** : AES128を選択
  - **Authentication** : SHA256を選択
  - **Enable Replay Detection** : デフォルトで許可 ( 有効 )
  - **Enable Perfect Forward Secrecy (PFS)** : チェックボックスのマークを外す
  - **Local**

**Port** : デフォルトで許可 (有効)

- **Remote Port** : デフォルトで許可 (有効)
- **Protocol** : デフォルトで許可 (有効)
- **Auto-negotiate** : デフォルトにする (マークなし)
- **Autokey Keep Alive** : デフォルトにする (マークなし)
- **Key Lifetime** : デフォルトで許可 (秒)
- **Seconds** : デフォルトで許可(43200)

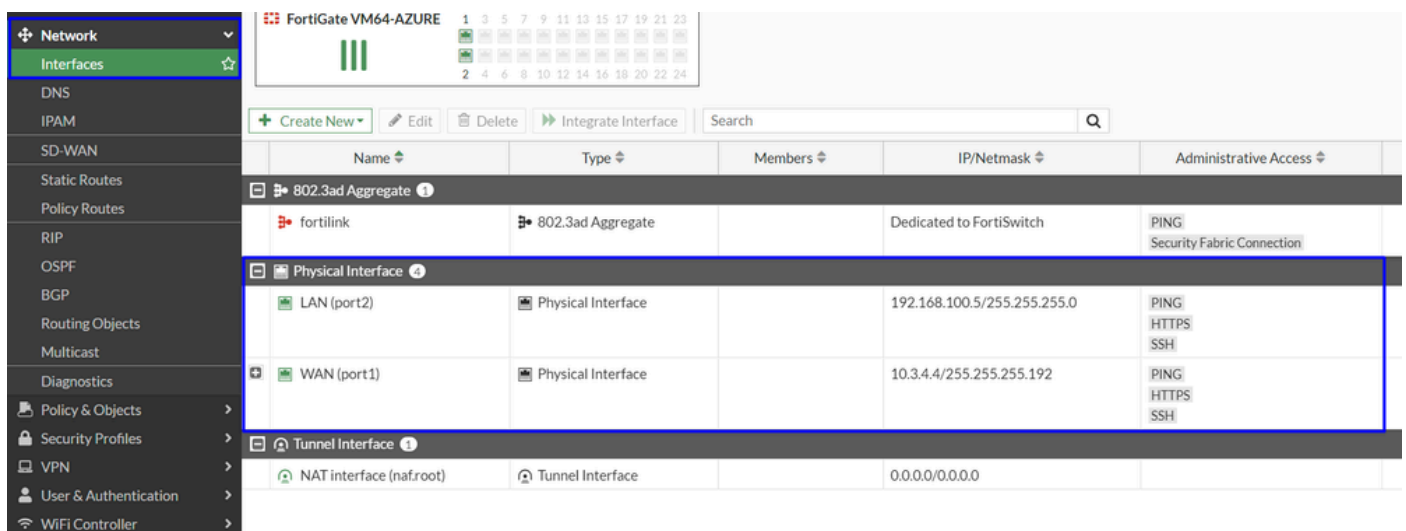
その後、[OK]をクリックします。数分後にセキュアアクセスを使用してVPNが確立されたことが表示され、次の手順に進むことができます。 **Configure the Tunnel Interface.**



トンネルインターフェイスの設定

トンネルが作成された後、セキュアアクセスと通信するためのWANインターフェイスとして使用しているポートの背後に、新しいインターフェイスがあることに気がきます。

これを確認するには、**Network > Interfaces**に移動します。



セキュアアクセスとの通信に使用するポート(この場合はインターフWAN エイス)を展開します。



	WAN (port1)	Physical Interface
	CSA	Tunnel Interface

- **Tunnel Interface** をクリックし、**Edit**

Create New ▾ <b>Edit</b> Delete          Integrate Interface <input type="text" value="Search"/>		
	Name ↕	Type ↕
	802.3ad Aggregate ①	
	fortilink	802.3ad Aggregate
	Physical Interface ④	
	LAN (port2)	Physical Interface
	WAN (port1)	Physical Interface
	CSA	Tunnel Interface

- 次のイメージを設定する必要があります

Name  CSA

Alias

Type  Tunnel Interface


Interface  WAN (port1)

VRF ID  0

Role  Undefined

Name  CSA

Alias

Type  Tunnel Interface

Interface  WAN (port1)

VRF ID  0

Role  Undefined

Address

Addressing mode Manual

IP

Netmask 255.255.255.255

Remote IP/Netmask

Address

Addressing mode Manual

IP

Netmask 255.255.255.255

Remote IP/Netmask

- Interface Configuration
- IP : ネットワークに存在しないルーティング不能IPを設定します(169.254.0.1)。
- Remote IP/Netmask : リモートIPをインターフェイスIPの次のIPとして設定し、ネットマスクを30(169.254.0.2 255.255.255.252)に設定します。

その後、をクリックOK して設定を保存し、次のステップであるConfigure Policy Route ( オリジンベースルーティング ) に進みます。



警告：このパートの後、デバイスからセキュアアクセスへのトラフィック、およびセキュアアクセスからトラフィックをルーティングするネットワークへのトラフィックを許可または許可するために、FortiGateでファイアウォールポリシーを設定する必要があります。

---

## ポリシールートの設定

この時点で、VPNがセキュアアクセスに設定され、確立されています。トラフィックをセキュアアクセスに再ルーティングして、トラフィックまたはFortiGateファイアウォールの背後にあるプライベートアプリケーションへのアクセスを保護する必要があります。

- 移動先 Network > Policy Routes

The image shows a network management interface. On the left is a dark sidebar menu with the following items: Dashboard (with a right arrow), Network (with a plus icon and a dropdown arrow), Interfaces, DNS, IPAM, SD-WAN, Static Routes, and Policy Routes (highlighted with a blue box and a star icon). On the right, there is a table with a header 'Seq.#' and two rows containing the numbers '1' and '2'. Above the table is a button labeled '+ Create New' with a green plus icon, also highlighted with a blue box.

- ポリシーの設定

If incoming traffic matches:	If incoming traffic matches:
Incoming interface <input type="text" value="+"/>	Incoming interface <input type="text" value="LAN (port2)"/>
Source Address	Source Address
IP/Netmask <input type="text"/>	IP/Netmask <input type="text" value="192.168.100.0/255.255.255.0"/>
Addresses <input type="text" value="+"/>	Addresses <input type="text" value="+"/>
Destination Address	Destination Address
IP/Netmask <input type="text"/>	IP/Netmask <input type="text"/>
Addresses <input type="text" value="+"/>	Addresses <input type="text" value="all"/>
Internet service <input type="text" value="+"/>	Internet service <input type="text" value="+"/>
Protocol <input type="text" value="TCP"/> <input type="text" value="UDP"/> <input type="text" value="SCTP"/> <input checked="" type="text" value="ANY"/> <input type="text" value="Specify"/>	Protocol <input type="text" value="TCP"/> <input type="text" value="UDP"/> <input type="text" value="SCTP"/> <input checked="" type="text" value="ANY"/> <input type="text" value="Specify"/>
Type of service <input type="text" value="0"/>	Type of service <input type="text" value="0"/>
<input type="text" value="0x00"/> Bit Mask <input type="text" value="0x00"/>	<input type="text" value="0x00"/> Bit Mask <input type="text" value="0x00"/>
Then:	Then:
Action <input checked="" type="text" value="Forward Traffic"/> <input type="text" value="Stop Policy Routing"/>	Action <input checked="" type="text" value="Forward Traffic"/> <input type="text" value="Stop Policy Routing"/>
Outgoing interface <input checked="" type="radio"/> <input type="radio"/> <input type="text" value="CSA"/>	Outgoing interface <input checked="" type="radio"/> <input type="radio"/> <input type="text" value="CSA"/>
Gateway address <input type="text"/>	Gateway address <input type="text" value="169.254.0.2"/>
Comments <input type="text" value="Write a comment..."/>	Comments <input type="text" value="Write a comment..."/>
Status <input checked="" type="text" value="Enabled"/> <input type="text" value="Disabled"/>	Status <input checked="" type="text" value="Enabled"/> <input type="text" value="Disabled"/>

- If Incoming traffic matches

- Incoming Interface : セキュアアクセス (トラフィックの発信元) へのトラフィックの再ルーティングを計画したインターフェイスを選択します。

- Source Address

- IP/Netmask : このオプションは、インターフェイスのサブネットだけをルーティングする場合に使用します

- Addresses : オブジェクトが作成されていて、トラフィックの送信元が複数のインターフェイスと複数のサブネットにある場合は、このオプションを使用します

- Destination Addresses

- Addresses: 選択 all
  
  - Protocol: 選択 ANY
  
  
  - Then
    - Action: **Choose Forward Traffic**
  
  
    - Outgoing Interface : 手順「[トンネルインターフェイスの設定](#)」で変更したトンネルインターフェイスを選択します。
    - Gateway Address : ステップで設定したリモートIP([RemoteIPNetmask](#))を設定します。
    - Status : Enabledを選択します
- OK**

をクリックして設定を保存すると、デバイストラフィックがセキュアアクセスに再ルーティングされたかどうかを確認できます。

#### 確認

マシンのトラフィックがセキュアアクセスに再ルーティングされたかどうかを確認するには、インターネット上で確認してパブリックIPを確認する方法と、curlで次のコマンドを実行する方法の2つの方法があります。

<#root>

```
C:\Windows\system32>curl ipinfo.io { "ip": "151.186.197.1", "city": "Frankfurt am Main", "region": "Hes
```

トラフィックを確認できるパブリック範囲は次のとおりです。

Min Host:151.186.176.1

Max Host :151.186.207.254



注：これらのIPは変更される可能性があります。つまり、シスコは将来的にこの範囲を拡張する可能性があります。

---

パブリックIPアドレスが変更された場合は、セキュアアクセスによって保護されていることを意味し、セキュアアクセスダッシュボードでプライベートアプリケーションを設定して、VPNaaSまたはZTNAからアプリケーションにアクセスできます。

## 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。