

# Sonicwall Firewall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](#)

[ネットワーク図](#)

[設定](#)

[セキュアアクセスでのネットワークトンネルグループ\(VPN\)の設定](#)

[Sonicwallでのトンネルの設定](#)

[トンネルの設定 - ルールと設定](#)

[VPNトンネルインターフェイスの追加](#)

[ネットワークオブジェクトとグループの追加](#)

[ルートの追加](#)

[アクセスルールの追加](#)

[確認](#)

[トラブルシューティング](#)

[ユーザPC](#)

[セキュアなアクセス](#)

[防音壁](#)

[関連情報](#)

---

## はじめに

このドキュメントでは、スタティックルーティングを使用して、セキュアアクセスから Sonicwall ファイアウォールへの間に IPsec VTI トンネル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。

- Sonicwall ( NSv270 - SonicOSX 7.0.1 ) 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

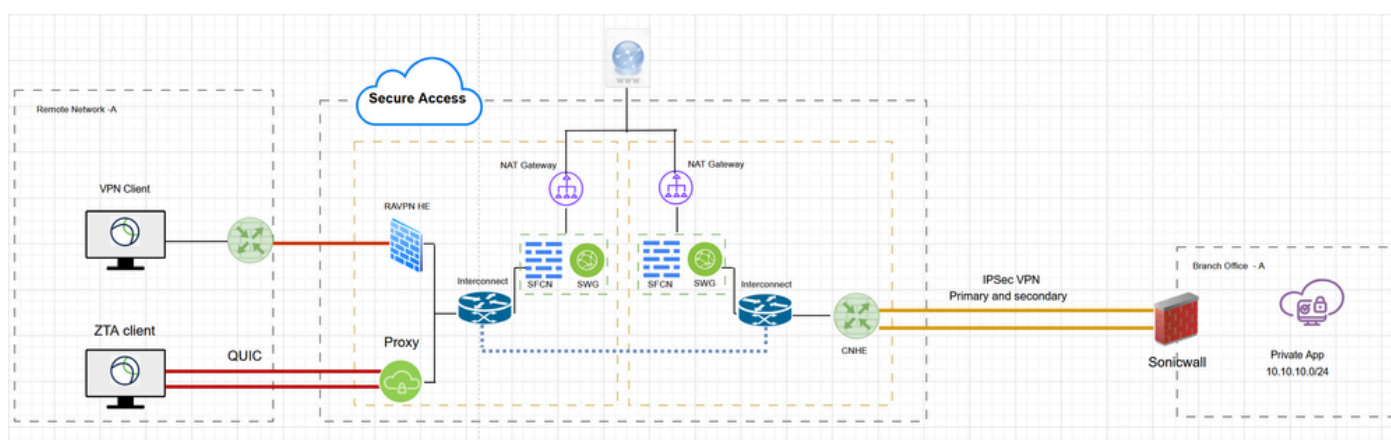
このドキュメントの情報は、次のハードウェアに基づくものです。

- Sonicwall ( NSv270 - SonicOSX 7.0.1 )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

## ネットワーク図



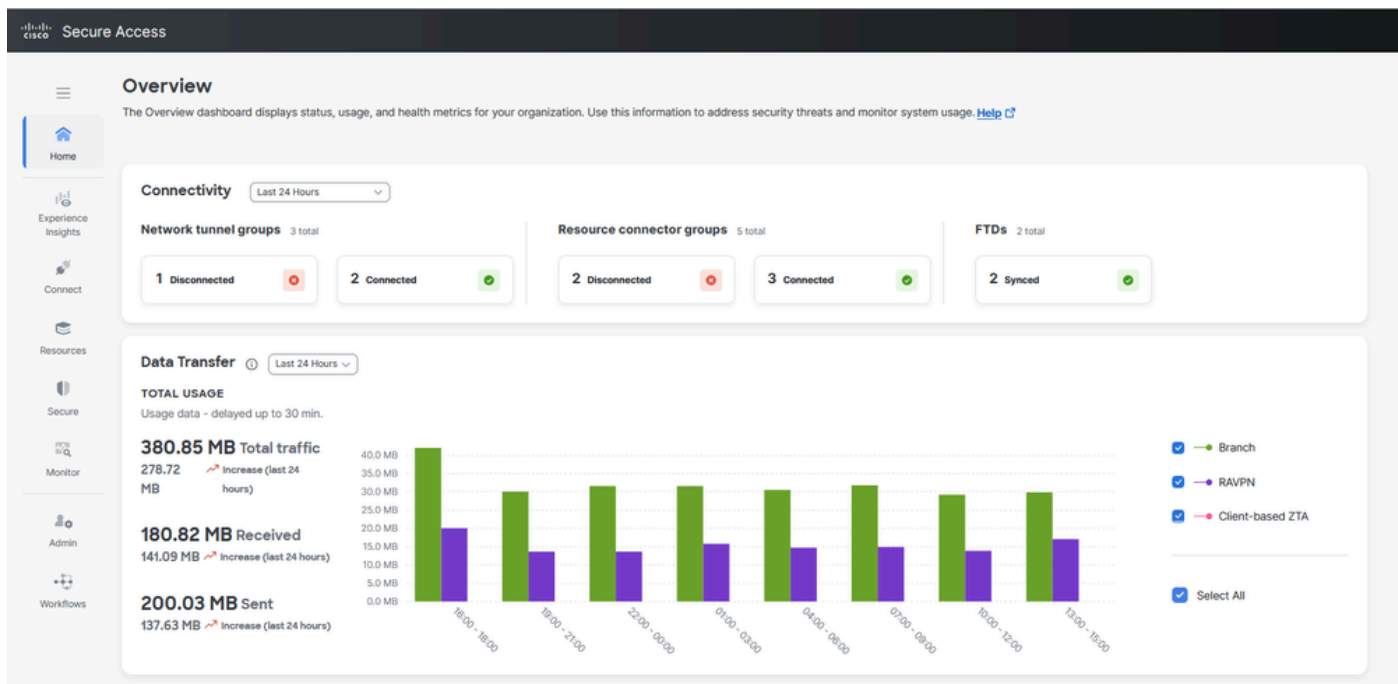
ネットワーク図

## 設定

### セキュアアクセスでのネットワークトンネルグループ(VPN)の設定

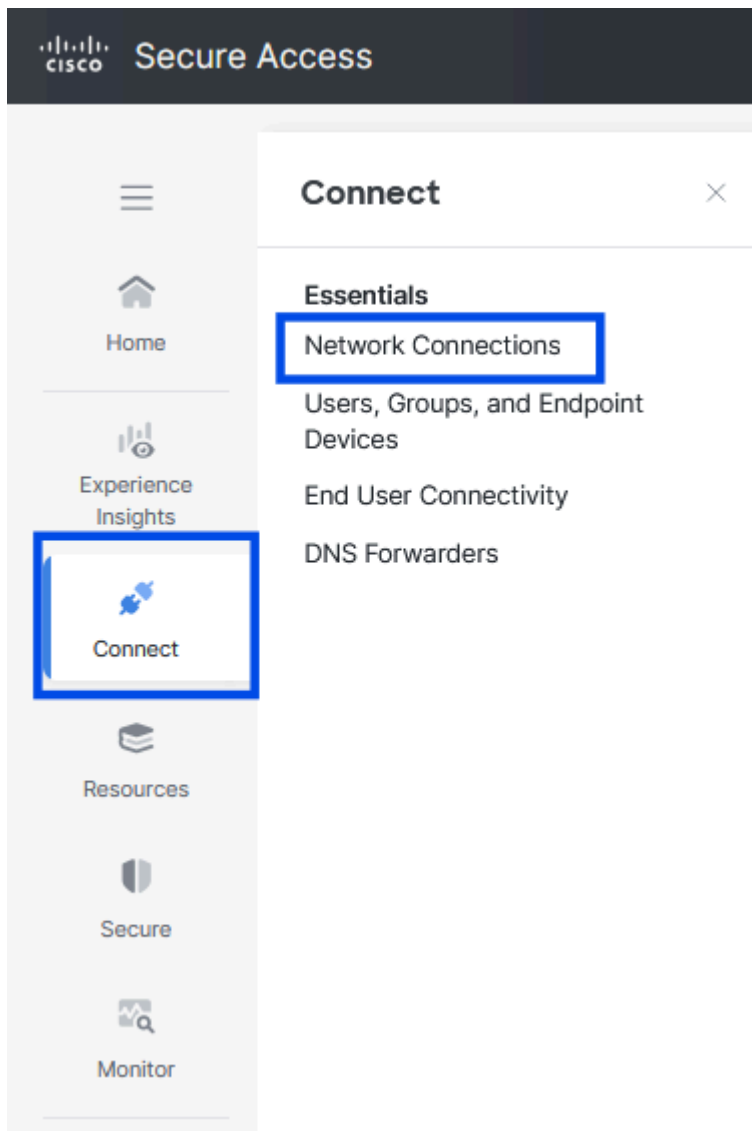
セキュアアクセスとSonicwall間のVPNトンネルを設定するには

- セキュアアクセスの[管理ポータル](#)に移動します



セキュアアクセス - メインページ

- Connect > Network Connectionsの順にクリックします。



セキュアなアクセス：ネットワーク接続

- Network Tunnel Groups の下で、+Addをクリックします。

**Network Connections**  
Manage the connections that allow user traffic to reach private resources on your network. For information about these options, see [Help](#)

Connector Groups **Network Tunnel Groups** FTDs

**Network Tunnel Groups** 2 total

0 Disconnected ❗ 0 Warning ⚠ 2 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
<b>AZURE</b>	<span style="color: green;">✅ Connected</span>	US (Pacific Northwest)	sse-usw-2-1-1	1	sse-usw-2-1-0	1 ...
<b>LAB-BGP</b>	<span style="color: green;">✅ Connected</span>	US (Pacific Northwest)	sse-usw-2-1-1	1	sse-usw-2-1-0	1 ...

Rows per page 10 < 1 >



## セキュアアクセス – トンネルIDとパスフレーズ

- ネットワークに設定したIPアドレス範囲、ホスト、またはサブネットを設定し、トラフィックをセキュアアクセス経由で通過させる
- [Add] をクリックします。
- [Save] をクリックします。

**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 **Add**

10.10.10.0/24 **X**

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

**Advanced Settings**

**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

Saveをクリックすると、トンネルに関する情報が表示されます。次の設定手順のために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.

<b>Primary Tunnel ID:</b>	SonicWall-VPN@i	sse.cisco.com
<b>Primary Data Center IP Address:</b>	44.228.138.150	
<b>Secondary Tunnel ID:</b>	SonicWall-VPN@i	sse.cisco.com
<b>Secondary Data Center IP Address:</b>	52.35.201.56	
<b>Passphrase:</b>		

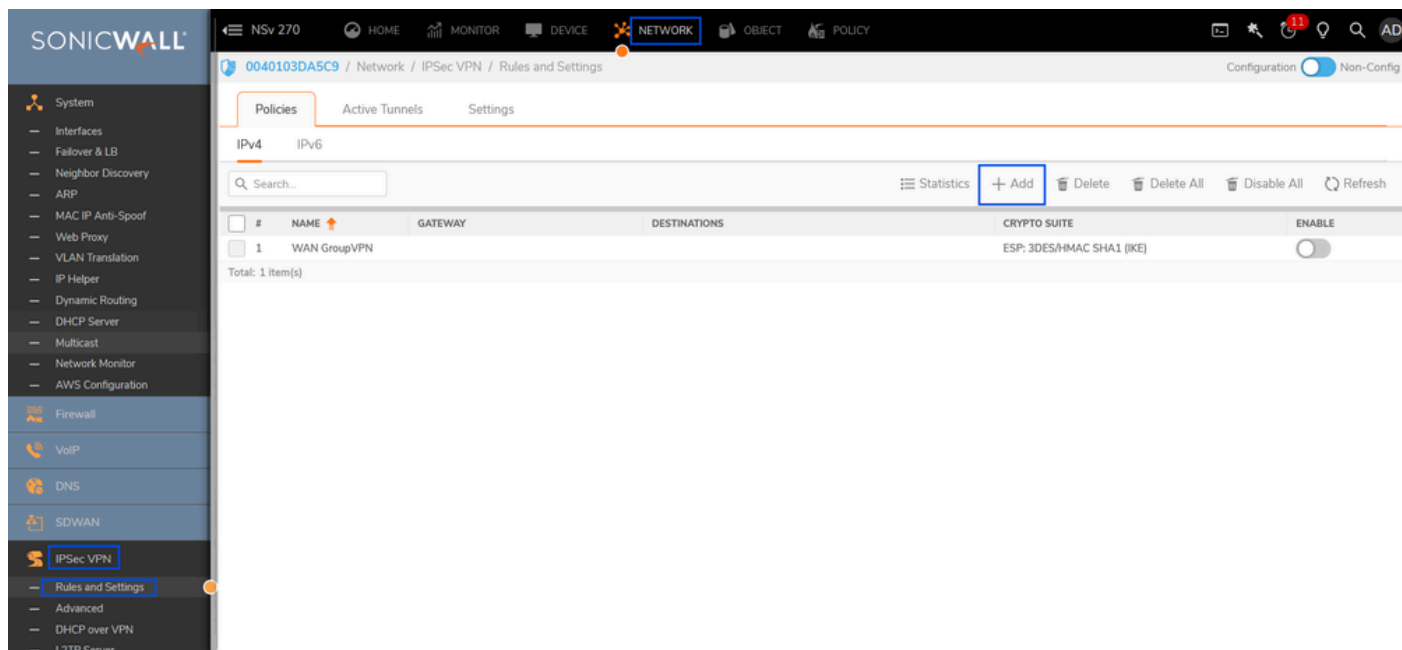
## セキュアアクセス – トンネルセットアップ用データ

### Sonicwallでのトンネルの設定

### トンネルの設定 – ルールと設定

Sonicwall Dashboardに移動します。

- Network > IPsec VPN > Rules and Settings
- +追加をクリックします。



Sonicwall - IPsec VPN – ルールと設定

- VPN Policyの下で、Secure Accessからのトンネルデータと[supported-ipsec-parameters](#)に基づくVPN設定に入力します。

## VPN Policy

General

Proposals

Advanced

SECURITY POLICY

Policy Type

Tunnel Interface

Authentication Method

IKE Using Preshared Secret

Name

SonicWall-CSA

IPsec Primary Gateway Name or Address

44.228.138.150

IKE AUTHENTICATION

Shared Secret

Mask Shared Secret

Confirm Shared Secret

Local IKE ID

E-mail Address

SonicWall-VPN@E

7-ss

Peer IKE ID

IPv4 Address

44.228.138.150

Cancel

Save

# VPN Policy

General   **Proposals**   Advanced

## IKE (PHASE 1) PROPOSAL

Exchange	<div>IKEv2 Mode</div>
DH Group	<div>Group 14</div>
Encryption	<div>AES-256</div>
Authentication	<div>SHA256</div>
Life Time (seconds)	<div>28800</div>

## IPSEC (PHASE 2) PROPOSAL

Protocol	<div>ESP</div>
Encryption	<div>AESGCM16-256</div>
Authentication	<div>None</div>
Enable Perfect Forward Secrecy	<div><input checked="" type="checkbox"/></div>
DH Group	<div>Group 14</div>
Life Time (seconds)	<div>28800</div>

Cancel

Save



# VPN Policy

General

Proposals

Advanced

## ADVANCED SETTINGS

Enable Keep Alive ☒ ⓘ

Disable IPsec Anti-Replay ☐ ⓘ

Allow Advanced Routing ☐

Enable Windows Networking  
(NetBIOS) Broadcast ☐

Enable Multicast ☐

Display Suite B Compliant  
Algorithms Only ☐

Apply NAT Policies ☐

## MANAGEMENT VIA THIS SA

HTTPS ☐

SSH ☐

SNMP ☐

## USER LOGIN VIA THIS SA

HTTP ☐

HTTPS ☐

VPN Policy bound to Interface X1

## IKEV2 SETTINGS

Do not send trigger packet during IKE SA negotiation ☐ ⓘ

Accept Hash & URL Certificate Type ☐

Accept Hash & URL Certificate Type Send Hash & URL Certificate  
Type ☐

Cancel

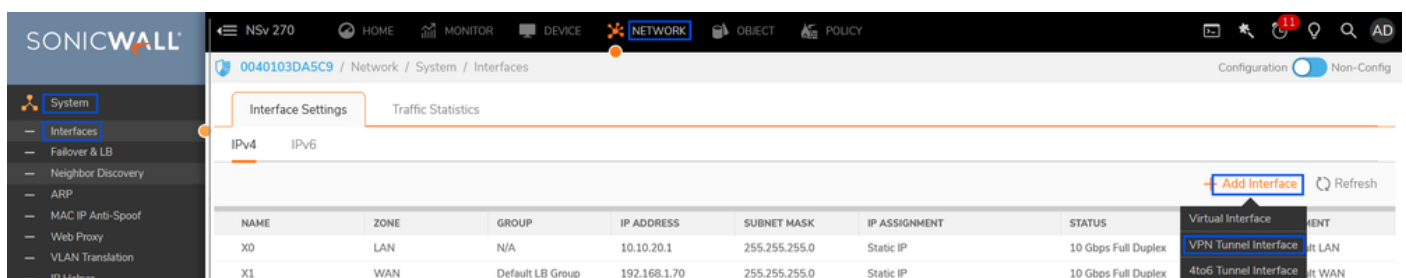
Save

- [Save] をクリックします。

## VPNトンネルインターフェイスの追加

Sonicwall Dashboardに移動します。

- Network > System > Interface
- + Add Interfaceをクリックします。
- VPNトンネルインターフェイスの選択



Sonicwall : インターフェイス

# Add VPN Tunnel Interface

General

Advanced

## INTERFACE SETTINGS

Zone

VPN

VPN Policy

SonicWall-CSA

Name

CSA\_Tunnel1

Mode / IP Assignment

Static IP Mode

IP Address

169.254.0.6

Subnet Mask

255.255.255.252

Interface MTU

Configured automatically via VPN policy

Comment

Tunnel 1 interface - With CSA Primary DC

Domain Name



MANAGEMENT

USER LOGIN

HTTPS



Pina



HTTP



HTTPS



Cancel

OK

- [OK] をクリックします。

The screenshot shows the SonicWall management console with the 'Interface Settings' tab selected. The configuration for 'CSA\_Tunnel1' is visible in the table below.

NAME	ZONE	GROUP	IP ADDRESS	SUBNET MASK	IP ASSIGNMENT	STATUS	ENABLED	COMMENT
X0	LAN	N/A	10.10.20.1	255.255.255.0	Static IP	10 Gbps Full Duplex	<input checked="" type="checkbox"/>	Default LAN
X1	WAN	Default LB Group	192.168.1.70	255.255.255.0	Static IP	10 Gbps Full Duplex	<input checked="" type="checkbox"/>	Default WAN
X2	Unassigned	N/A	0.0.0.0	0.0.0.0		10 Gbps Full Duplex	<input checked="" type="checkbox"/>	N/A
X3	Unassigned	N/A	0.0.0.0	0.0.0.0		10 Gbps Full Duplex	<input checked="" type="checkbox"/>	N/A
X4	Unassigned	N/A	0.0.0.0	0.0.0.0		10 Gbps Full Duplex	<input checked="" type="checkbox"/>	N/A
X5	Unassigned	N/A	0.0.0.0	0.0.0.0		10 Gbps Full Duplex	<input checked="" type="checkbox"/>	N/A
X6	Unassigned	N/A	0.0.0.0	0.0.0.0		10 Gbps Full Duplex	<input checked="" type="checkbox"/>	N/A
X7	Unassigned	N/A	0.0.0.0	0.0.0.0		10 Gbps Full Duplex	<input checked="" type="checkbox"/>	N/A
CSA_Tunnel1	VPN	N/A	169.254.0.6	255.255.255.252	Static IP	Interface Up	<input checked="" type="checkbox"/>	Tunnel 1 interface - With CSA Primary DC

Sonicwall – インターフェイス – VPNトンネルインターフェイス

## ネットワークオブジェクトとグループの追加

Sonicwall Dashboardに移動します。

- Object > Match Objects > Addresses
- アドレスオブジェクト
- +追加をクリックします

0040103DA5C9 / Object / Match Objects / Addresses

Configuration ☒ Non-Config

Address Objects Address Groups

Search... View: All IPv4 & IPv6 + Add Delete Resolve Purge Refresh Column Selection

#	OBJECT NAME	DETAILS	TYPE	IP VERSION	ZONE	REFERENCES	CLASS
1	CSA_Tunnel1 IP	169.254.0.6/255.255.255.255	host	ipv4	VPN		Default
2	CSA_Tunnel1 Subnet	169.254.0.4/255.255.255.252	network	ipv4	VPN		Default
3	Default Active WAN IP	192.168.1.70/255.255.255.255	host	ipv4	WAN		Default

Sonicwall – オブジェクト – アドレスオブジェクト

## Address Object Settings

**Name**  ⓘ

**Zone Assignment**  ▼


**Type**  ▼

**Network**

**Netmask / Prefix Length**


- [Save] をクリックします。

# Address Object Settings

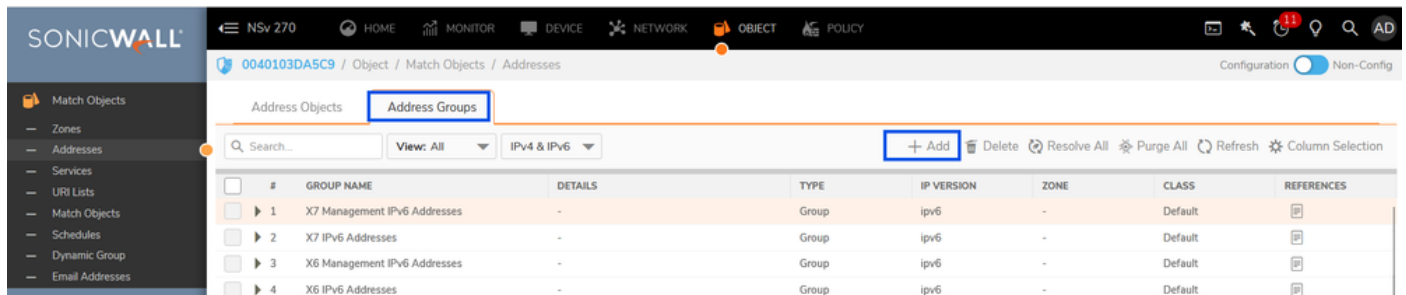
Name	<input type="text" value="CgNAT"/>	
Zone Assignment	<input type="text" value="VPN"/>	▼
Type	<input type="text" value="Network"/>	▼
Network	<input type="text" value="100.64.0.0"/>	
Netmask / Prefix Length	<input type="text" value="255.192.0.0"/>	
<input type="button" value="Cancel"/>		<input type="button" value="Save"/>

- [Save] をクリックします。

# Address Object Settings

Name	<input type="text" value="RAVPNUser-Pool"/>	
Zone Assignment	<input type="text" value="VPN"/>	▼
Type	<input type="text" value="Network"/>	▼
Network	<input type="text" value="10.10.50.0"/>	
Netmask / Prefix Length	<input type="text" value="255.255.255.0"/>	
<input type="button" value="Cancel"/>		<input type="button" value="Save"/>

- [Save] をクリックします。
- アドレスグループの作成
- +Addをクリックします。
- アドレスオブジェクトを選択し、アドレスグループに追加します



Sonicwall – オブジェクト – アドレスグループ

## Add Address Groups

Name CSA-Subnets

SHOW AVAILABLE

☒ All (136) ☒ Hosts (37) ☒ Ranges (0) ☒ Networks (32) ☒ MAC (0) ☒ FQDN (0) ☒ Groups (67)

Not in Group 134 items

Q RAV

No Data

In Group 2 items

Q

CgNAT[NW]

RAVPNUser-Pool[NW]

Cancel

Save

- [Save] をクリックします。

## ルートの追加

Sonicwall Dashboardに移動します。

- Policy > Rules and Policies > Routing Rules
- +追加をクリックします。

SONICWALL

NSv 270

HOME

MONITOR

DEVICE

NETWORK

OBJECT

POLICY

0040103DA5C9 / Policy / Rules and Policies / Routing Rules

Rules and Policies

Access Rules

NAT Rules

Routing Rules

Content Filter Rules

App Rules

Endpoint Rules

DPI-SSL

DPI-SSH

Security Services

Capture ATP

Endpoint Security

Default & Custom

IPv4

Active & Inactive

Used & Unused

GENERAL			LOOKUP				NEXT HOP					
	PR	HITS	NAME	SOURCE	DESTINATION	SERVICE	APP	INTERFACE	GATEWAY	M...	TYPE	PATH
<input type="checkbox"/>	2	0	Route Policy_5	Any	255.255.255.255/32	Any	Any	X0	0.0.0.0	20	Standard	
<input type="checkbox"/>	3	0	Route Policy_7	Any	X1 Default Gateway	Any	Any	X1	0.0.0.0	20	Standard	
<input type="checkbox"/>	4	0	Route Policy_26	Any	CSA_Tunnel1 Subnet	Any	Any	CSA_Tunnel1	0.0.0.0	20	Standard	
<input type="checkbox"/>	7	0	Route Policy_4	Any	X0 Subnet	Any	Any	X0	0.0.0.0	20	Standard	
<input type="checkbox"/>	8	24.9k	Route Policy_6	Any	X1 Subnet	Any	Any	X1	0.0.0.0	20	Standard	
<input type="checkbox"/>	9	3.4k	Route Policy_8	X1 IP	Any	Any	Any	X1	X1 Default Gateway	20	Standard	
<input type="checkbox"/>	10	2.1k	Route Policy_9	Any	0.0.0.0/0	Any	Any	X1	192.168.1.1	20	Standard	

+ Add

Delete

Delete All

Edit

Live Counters

Reset Counters

Sonicwall : ルーティングルール

- ・ ルーティングルールの追加

## Adding Rule

Name

LAN-CSA

Tags

add upto 3 tags, use comma as separator...

Description

provide a short description of your route...

Type

☒ IPv4
☐ IPv6

Lookup

Next Hop

Advanced

Probe

Source

LAN

Destination

CSA-Subnets

☒ Service
☐ App

Service

Any

Show Diagram

☐

Cancel

Add

# Adding Rule

Name

LAN-CSA

Tags

add upto 3 tags, use comma as separator...

Description

provide a short description of your route...

Type

☒ IPv4 ☐ IPv6

Lookup

Next Hop

Advanced

Probe

☒ Standard Route

☐ Multi-Path Route

☐ SD-WAN Rule

Interface

CSA\_Tunnel1

Gateway

0.0.0.0/::

Metric

5

Show Diagram

☐

Cancel

Add

- +追加をクリックします。

SONICWALL

NSv 270

HOME

MONITOR

DEVICE

NETWORK

OBJECT

POLICY

0040103DA5C9 / Policy / Rules and Policies / Routing Rules

Configuration Non-Config

Rules and Policies

Access Rules

NAT Rules

Routing Rules

Content Filter Rules

App Rules

Default & Custom

IPv4

Active & Inactive

Used & Unused

GENERAL				LOOKUP				NEXT HOP				PROBE	OPERATION	
	PR	HITS	NAME	SOURCE	DESTINATION	SERVICE	APP	INTERFACE	GATEWAY	M	TYPE	PATH PROFILE	PROBE	CLASS
<input type="checkbox"/>	1	86	LAN-CSA_27	LAN	CSA-Subnets	Any	Any	CSA_Tunnel1	0.0.0.0	5	Standard			Custom
<input type="checkbox"/>	3	0	Route Policy_5	Any	255.255.255.255/32	Any	Any	X0	0.0.0.0	20	Standard			Default

Sonicwall : ルーティングルール

## アクセスルールの追加

Sonicwall Dashboardに移動します。

- Policy > Rules and Policies > Access Rules
- +追加をクリックします。

SONICWALL

NSv 270

HOME

MONITOR

DEVICE

NETWORK

OBJECT

POLICY

0040103DA5C9

Policy / Rules and Policies / Access Rules

Configuration

Non-Config

Rules and Policies

Access Rules

NAT Rules

Routing Rules

Content Filter Rules

App Rules

Endpoint Rules

DPI-SSL

DPI-SSH

Security Services

Capture ATP

Endpoint Security

Default & Custom

IPv4

All Zones -> All Zones

Active & Inactive

Used & Unused

Max Count

Reset Rules

Settings

	GENERAL			ZONE		ADDRESS		SERVICE	USER		SCHEDULE	
	PI	HITS	NAME	ACTION	SOURCE	DESTINATION	SOURCE	DESTINATION	DESTINATION P...	USER INCL.	USER EXCL.	SCHEDULE
	1 (M)	0	Default Access Rule_2	➔	LAN	LAN	Any	All X0 Management IP	Ping	All	None	Always
	2 (M)	0	Default Access Rule_3	➔	LAN	LAN	Any	All X0 Management IP	SSH Management	All	None	Always
	3 (M)	0	Default Access Rule_4	➔	LAN	LAN	Any	All X0 Management IP	HTTPS Management	All	None	Always
	4 (M)	0	Default Access Rule_5	➔	LAN	LAN	Any	All X0 Management IP	HTTP Management	All	None	Always
	5 (M)	0	Default Access Rule_6	➔	LAN	LAN	Any	Any	Any	All	None	Always
	6 (M)	0	Default Access Rule_9	➔	LAN	VPN	WAN RemoteAccess Networks	Any	Any	All	None	Always
	7 (M)	0	Default Access Rule_124	➔	LAN	VPN	obj_10.10.20.0_24	CSA-Subnets	Any	All	None	Always
	8 (M)	0	Default Access Rule_12	➔	WAN	WAN	Any	All X1 Management IP	Ping	All	None	Always
	9 (M)	0	Default Access Rule_13	➔	WAN	WAN	Any	All X1 Management IP	SSH Management	All	None	Always
	10 (M)	11.4k	Default Access Rule_14	➔	WAN	WAN	Any	All X1 Management IP	HTTPS Management	All	None	Always
	11 (M)	0	Default Access Rule_15	➔	WAN	WAN	Any	All X1 Management IP	HTTP Management	All	None	Always
	12 (A)	2	Default Access Rule_123	➔	WAN	WAN	X1 IP	Any	IKE	All	None	Always
	13 (A)	0	Default Access Rule_122	➔	WAN	WAN	Any	X1 IP	IKE	All	None	Always
	14 (M)	0	Default Access Rule_22	➔	DMZ	DMZ	Any	Any	Any	All	None	Always
	15 (M)	0	Default Access Rule_23	➔	DMZ	VPN	WAN RemoteAccess Networks	Any	Any	All	None	Always

+ Add

Edit

Delete

Move

Enable

Disable

Live Counters

Reset Counters

Displaying 42 of 69 rules

Sonicwall : アクセスルール

## Adding Rule

Name: CSA-Inbound-Allow

Description: Access rule to allow CSA subnets (RAVPN and CgNAT) to access the internal network/s

Action: ☒ Allow ☐ Deny ☐ Discard

Type: ☒ IPv4 ☐ IPv6

Priority: Manual 1

Schedule: Always

Enable: ☒

Source / Destination User & TCP/UDP Security Profiles Traffic Shaping Logging Optional Settings

SOURCE

Zone/Interface: VPN

Address: CSA-Subnets

Port/Services: Any

DESTINATION

Zone/Interface: LAN

Address: LAN

Port/Services: Any

Show Diagram ☐

Cancel Add

- +Addをクリックします。

SONICWALL

NSv 270

HOME

MONITOR

DEVICE

NETWORK

OBJECT

POLICY

0040103DA5C9

/ Policy / Rules and Policies / Access Rules

Configuration 

Non-Config

Rules and Policies

Access Rules

NAT Rules

Routing Rules

CSA

Default & Custom

IPv4

All Zones -> All Zones

Active & Inactive

Used & Unused

Max Count

Reset Rules

Settings

GENERAL				ZONE		ADDRESS		SERVICE	USER		SCHEDULE	
	PI	HITS	NAME	ACTION	SOURCE	DESTINATION	SOURCE	DESTINATION	DESTINATION P...	USER INCL.	USER EXCL.	SCHEDULE
	1 (M)	0	CSA-Inbound-...	VPN	LAN	CSA-Subnets	LAN	Any	All	None	Always	

Sonicwall : アクセスルール



# 確認

- セキュアアクセスのトンネルステータス

← Network Tunnel Groups

## SonicWall-NTG

Review and edit this network tunnel group. Details for each IPsec tunnel added to this group are listed including which tunnel hub it is a member of. [Help](#)

### Summary

**Warning** Primary and secondary hubs mismatch in number of tunnels.

Region US (Pacific Northwest) Routing Type Static Routing  
Device Type Other IP Address Range 10.10.10.0/24

Last Status Update Jul 06, 2025 4:13 PM

#### Primary Hub

Hub Up

1 Active Tunnels

Tunnel Group ID SonicWall-VPN@  
Data Center sse-usw-2-1-1  
IP Address 44.228.138.150

#### Secondary Hub

Hub Down

0 Active Tunnels

Tunnel Group ID SonicWall-VPN@  
Data Center sse-usw-2-1-0  
IP Address 52.35.201.56

### Network Tunnels

Review this network tunnel group's IPsec tunnels. [Help](#)

Tunnels	Peer ID	Peer Device IP Address	Data Center Name	Data Center IP Address	Status	Last Status Update
Primary 1	131073	76.39.159.129	sse-usw-2-1-1	44.228.138.150	Connected	Jul 06, 2025 4:11 PM

セキュアアクセス – ネットワークトンネルグループ – VPNステータス

- Sonicwallファイアウォールのトンネルステータス

SONICWALL

NSv 270 HOME MONITOR DEVICE NETWORK OBJECT POLICY

0040103DA5C9 / Network / IPsec VPN / Rules and Settings

Configuration Non-Config

Policies Active Tunnels Settings

IPv4 IPv6

Search Refresh

#	CREATED	NAME	LOCAL	REMOTE	GATEWAY	COMMENT
1	07/06/2025 08:42:48	SonicWall-CSA	0.0.0.0 - 255.255.255.255	0.0.0.0 - 255.255.255.255	44.228.138.150	

Total: 1 item(s)

System  
Interfaces  
Failover & LB  
Neighbor Discovery  
ARP  
MAC IP Anti-Spoof  
Web Proxy  
VLAN Translation  
IP Helper  
Dynamic Routing  
DHCP Server  
Multicast  
Network Monitor  
AWS Configuration  
Firewall  
VoIP  
DNS  
SDWAN  
IPSec VPN  
Rules and Settings

Sonicwall:IPSec VPNステータス

同じプロセスで、Secure Access SecondaryデータセンターとSonicwall間のトンネルを設定できます

これで、トンネルがセキュアアクセスとSonicwallでアップ状態になったので、RA-VPN、ブラウザベースのZTA、またはクライアントベースのZTAを介したプライベートリソースへのアクセスのセキュアアクセスダッシュボードでの設定を続行できます

# トラブルシューティング

## ユーザPC

- ユーザがRAVPN/ZTNAに正常に接続/登録できるかどうかを確認します。そうでない場合は、コントロールプレーン接続が失敗する原因を詳しくトラブルシューティングします。
- ユーザがアクセスしようとしているネットワークが、RAVPNトンネルまたはZTNA (VPNトンネルインターフェイス) 経由で行くことを想定していることを確認します。そうでない場合は、ヘッドエンド(CMTS)の設定を確認します。

## セキュアなアクセス

- RAVPN接続プロファイルでトラフィックステアリング設定を確認し、宛先ネットワークがトンネル経由でセキュアアクセスに送信するように設定されていることを確認します。
- プライベートリソースが有効なプロトコル/ポートで定義され、ZTNA/RAVPN接続メカニズムがチェックされていることを確認します。
- RAVPN/ZTNAユーザがPrivate Resource Network (PRN; プライベートリソースネットワーク) にアクセスできるようにアクセスポリシーが設定されていて、他のルールが優先されてトラフィックをブロックしていないという順番になっていることを確認します。
- ユーザがアクセスしようとしているプライベートリソースをカバーするスタティックルーティングを介した有効なクライアントルートを示すIPSecトンネルがアップ状態で、セキュアアクセスであることを確認します。

## 防音壁

- IPSecトンネルがアップしているかどうかを確認します (IKEおよびIPSec SA)。
- クライアントルートが適切にアドバタイズされることを確認します。
- RAVPN/ZTNAユーザからSonicwallの背後にあるプライベートリソース宛てのトラフィックの送信元が、Sonicwallでパケットキャプチャを実行することにより、トンネル経由でSonicwallファイアウォールに到達していることを確認します。
- トラフィックがプライベートリソースに到達し、RAVPN/ZTNAクライアントに応答するかどうかを確認します。使用できる場合は、それらのパケットがSonicall X0(LAN)インターフェイスに到達していることを確認します。
- SonicwallがIPSecトンネル経由でSecure Accessにリターントラフィックを転送していることを確認します。

## 関連情報

- [シスコのテクニカルサポートとダウンロード](#)
- [Cisco Secure Accessヘルプセンター](#)
- [ゼロトラストアクセスモジュール](#)
- [Secure Accessエラー「Enrollment Service Is Not Responding.ITヘルプデスクにお問い合わせください」](#)

## 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。