

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](#)

[トラブルシュート](#)

[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

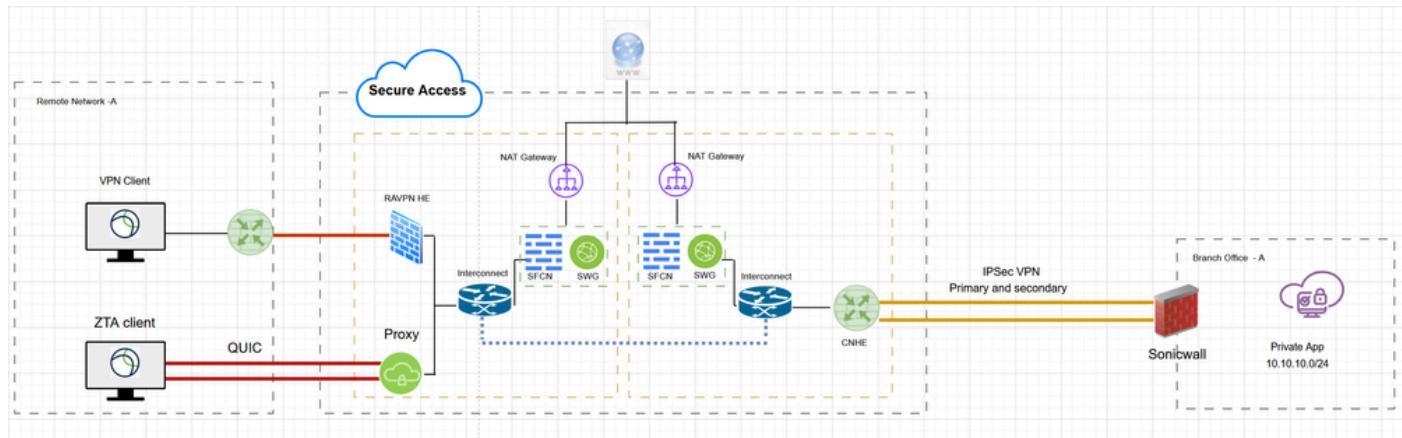
このドキュメントの情報は、次のハードウェアに基づくものです。

- 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



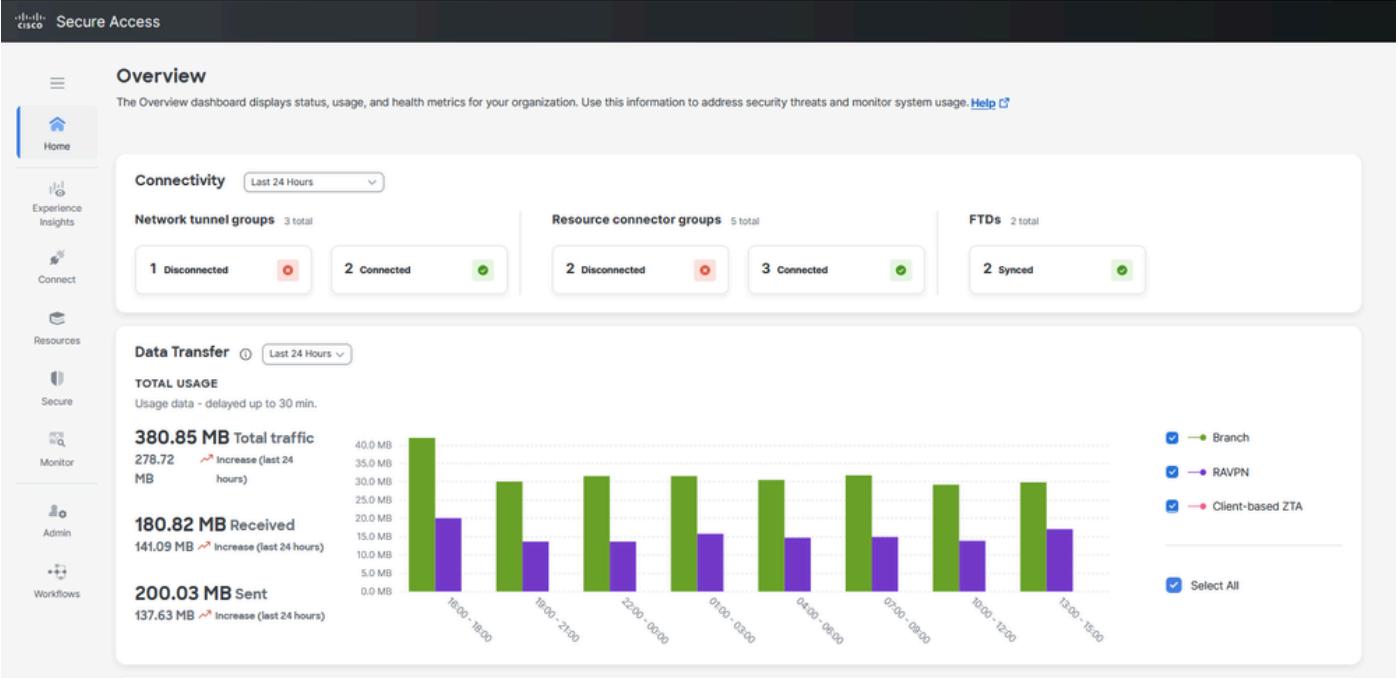
ネットワーク図

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。

The screenshot shows the Cisco Secure Access web interface. On the left, there's a sidebar with icons for Home, Experience Insights, Connect (which is selected and highlighted with a blue border), Resources, Secure, and Monitor. The main content area is titled 'Connect' and has a sub-section titled 'Essentials'. Under 'Essentials', there are four items: 'Network Connections' (highlighted with a blue box), 'Users, Groups, and Endpoint Devices', 'End User Connectivity', and 'DNS Forwarders'.

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。

The screenshot shows the 'Network Tunnel Groups' page. The sidebar on the left includes icons for Experience Insights, Connect (selected), Resources, Secure, Monitor, Admin, and Workflows. The main content area has tabs for 'Connector Groups', 'Network Tunnel Groups' (selected and highlighted with a blue border), and 'FTDs'. Below the tabs, it says 'Network Tunnel Groups 2 total' with three status indicators: 0 Disconnected (red), 0 Warning (yellow), and 2 Connected (green). A table lists two tunnel groups: 'AZURE' and 'LAB-BGP', each with its status, region, primary hub data center, and primary tunnels. At the bottom right, there's a '+ Add' button.

Network Tunnel Group	Status	Region	Primary Hub Data Center	Primary Tunnels	Secondary Hub Data Center	Secondary Tunnels
AZURE	Connected	US (Pacific Northwest)	sse-usw-2-1-1	1	sse-usw-2-1-0	1
LAB-BGP	Connected	US (Pacific Northwest)	sse-usw-2-1-1	1	sse-usw-2-1-0	1

セキュアアクセス – ネットワークトンネルグループ

- ・ トンネルグループ名、リージョン、およびデバイスタイプの設定
- ・ [Next] をクリックします。

← Network Tunnel Groups
Add a Network Tunnel Group

Add a network tunnel group to Secure Access and enable secure network connections to the internet and private resources. Select one of your organization's available network devices to establish this network tunnel group connection. [Help](#)

General Settings

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: SonicWall-NTG

Region: US (Pacific Northwest)

Device Type: Other

[Cancel](#) [Next](#)

セキュアアクセス – ネットワークトンネルグループ – 一般設定



注：ファイアウォールの場所に最も近い地域を選択してください。

- ・ トンネルIDの形式とパスフレーズの設定
- ・ [Next] をクリックします。

← Network Tunnel Groups
Add a Network Tunnel Group

Add a network tunnel group to Secure Access and enable secure network connections to the internet and private resources. Select one of your organization's available network devices to establish this network tunnel group connection. [Help](#)

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: SonicWall-VPN @<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](#) [Next](#)

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。

General Settings
Tunnel ID and Passphrase
Routing
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 **Add**

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

← Network Tunnel Groups
Add a Network Tunnel Group

Add a network tunnel group to Secure Access and enable secure network connections to the internet and private resources. Select one of your organization's available network devices to establish this network tunnel group connection. [Help](#)

General Settings
Tunnel ID and Passphrase
Routing
Data for Tunnel Setup

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: SonicWall-VPN@1 **Primary Data Center IP Address:** 44.228.138.150 **Secondary Tunnel ID:** SonicWall-VPN@1 **Secondary Data Center IP Address:** 52.35.201.56 **Passphrase:**

Back **Save**

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。

The screenshot shows the Sonicwall Dashboard interface. The left sidebar has a tree view with 'System', 'Firewall', 'VoIP', 'DNS', 'SDWAN', and 'IPSec VPN' selected. Under 'IPSec VPN', 'Rules and Settings' is also selected. The main content area is titled '0040103DA5C9 / Network / IPsec VPN / Rules and Settings'. It shows a table with one row: 'WAN GroupVPN'. The table columns include NAME, GATEWAY, DESTINATIONS, CRYPTO SUITE, and ENABLE. The CRYPTO SUITE is set to 'ESP: 3DES/HMAC SHA1 (IKE)'. The ENABLE switch is off. There are buttons for Statistics, Add, Delete, Delete All, Disable All, and Refresh.

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

The screenshot shows the 'General' tab of the 'SECURITY POLICY' configuration. The 'Policy Type' is set to 'Tunnel Interface'. The 'Authentication Method' is 'IKE Using Preshared Secret'. The 'Name' is 'SonicWall-CSA'. The 'IPsec Primary Gateway Name or Address' is '44.228.138.150'. In the 'IKE AUTHENTICATION' section, the 'Shared Secret' field contains a masked password. The 'Mask Shared Secret' toggle is on. The 'Confirm Shared Secret' field also contains a masked password. The 'Local IKE ID' is 'E-mail Address: SonicWall-VPN@E' and the 'Peer IKE ID' is 'IPv4 Address: 44.228.138.150'. At the bottom are 'Cancel' and 'Save' buttons.

VPN Policy

[General](#)[Proposals](#)[Advanced](#)

IKE (PHASE 1) PROPOSAL

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

IPSEC (PHASE 2) PROPOSAL

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

[Cancel](#) [Save](#)

VPN Policy

General Proposals Advanced

ADVANCED SETTINGS

Enable Keep Alive <input checked="" type="checkbox"/>	Display Suite B Compliant Algorithms Only <input type="checkbox"/>
Disable IPsec Anti-Replay <input type="checkbox"/>	Apply NAT Policies <input type="checkbox"/>
Allow Advanced Routing <input type="checkbox"/>	
Enable Windows Networking (NetBIOS) Broadcast <input type="checkbox"/>	
Enable Multicast <input type="checkbox"/>	

MANAGEMENT VIA THIS SA

HTTPS <input type="checkbox"/>	SNMP <input type="checkbox"/>
SSH <input type="checkbox"/>	

USER LOGIN VIA THIS SA

HTTP <input type="checkbox"/>	HTTPS <input type="checkbox"/>
VPN Policy bound to <input type="button" value="Interface X1"/>	

IKEV2 SETTINGS

Do not send trigger packet during IKE SA negotiation <input type="checkbox"/>	Accept Hash & URL Certificate Type <input type="checkbox"/>
Accept Hash & URL Certificate Type Send Hash & URL Certificate Type <input type="checkbox"/>	

- [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

The screenshot shows the Sonicwall NSv 270 dashboard. The left sidebar has 'System' selected, with 'Interfaces' highlighted. The main pane shows 'Interface Settings' for 'Interface X0' (IPv4) and 'Interface X1' (IPv6). On the right, there's a table of interfaces and a 'Virtual Interface' section with buttons for 'Add Interface', 'Edit', and 'Delete'. A tooltip 'Add Interface' is shown over the 'Add Interface' button.

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

HTTPS

Ping

USER LOGIN

HTTP

HTTPS

- [OK] をクリックします。

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

#	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

i

Zone Assignment

LAN

Type

Network

Network

Netmask / Prefix Length

Cancel
Save

- [Save] をクリックします。

Address Object Settings

Name ⓘ

Zone Assignment ▾

Type ▾

Network

Netmask / Prefix Length

- [Save] をクリックします。

Address Object Settings

Name ⓘ

Zone Assignment ▾

Type ▾

Network

Netmask / Prefix Length

- [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

NSv 270 HOME MONITOR DEVICE NETWORK OBJECT POLICY

0040103DASC9 / Object / Match Objects / Addresses

Address Objects Address Groups

Search... View: All IPv4 & IPv6

#	GROUP NAME	DETAILS	TYPE	IP VERSION	ZONE	CLASS	REFERENCES
1	X7 Management IPv6 Addresses	-	Group	ipv6	-	Default	
2	X7 IPv6 Addresses	-	Group	ipv6	-	Default	
3	X6 Management IPv6 Addresses	-	Group	ipv6	-	Default	
4	X6 IPv6 Addresses	-	Group	ipv6	-	Default	

+ Add Delete Resolve All Purge All Refresh Column Selection

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
RAV	
No Data	

In Group	2 items
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 : Rules and Policies

ROUTING RULES

	GENERAL	LOOKUP	NEXT HOP								
	PR ↑ HITS	NAME	SOURCE	DESTINATION	SERVICE	APP	INTERFACE	GATEWAY	M...	TYPE	PATH I
1	2	Route Policy_5	Any	255.255.255.255/32	Any	Any	X0	0.0.0.0	20	Standar	
2	3	Route Policy_7	Any	X1 Default Gateway	Any	Any	X1	0.0.0.0	20	Standar	
3	4	Route Policy_26	Any	CSA_Tunnel1 Subnet	Any	Any	CSA_Tunnel1	0.0.0.0	20	Standar	
4	7	Route Policy_4	X0 Subnet	Any	Any	Any	X0	0.0.0.0	20	Standar	
5	8	Route Policy_6	X1 Subnet	Any	Any	Any	X1	0.0.0.0	20	Standar	
6	9	Route Policy_8	X1 IP	Any	Any	Any	X1	X1 Default Gateway	20	Standar	
7	10	Route Policy_9	0.0.0.0/0	Any	Any	Any	X1	192.168.1.1	20	Standar	

Buttons: + 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 **Type**: IPv4 IPv6

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

Description: provide a short description of your route...

Lookup **Next Hop** **Advanced** **Probe**

Source : LAN	<input type="button" value="edit"/>	<input type="button" value="info"/>
Destination : CSA-Subnets	<input type="button" value="edit"/>	<input type="button" value="info"/>
<input checked="" type="radio"/> Service	<input type="radio"/> App	
Service : Any	<input type="button" value="edit"/>	<input type="button" value="info"/>

Show Diagram

Add **Cancel**

Adding Rule

Name: LAN-CSA Type: IPv4 IPv6

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

Description: provide a short description of your route...

Lookup Next Hop Advanced Probe

Standard Route
 Multi-Path Route
 SD-WAN Rule

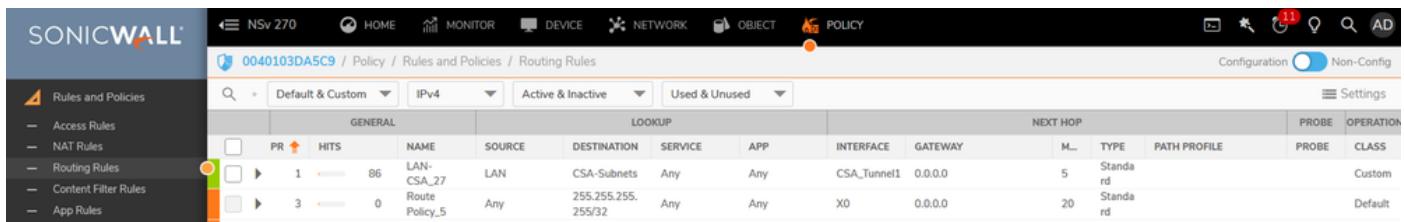
Interface: CSA_Tunnel1

Gateway: 0.0.0.0/0

Metric: 5

Show Diagram Cancel Add

- +追加をクリックします。



The screenshot shows the SonicWall NSv 270 Policy interface. The left sidebar has a 'Rules and Policies' section with 'Access Rules' selected. The main area is titled 'ROUTING RULES' and displays a table of rules. The table has columns for PR, HITS, NAME, SOURCE, DESTINATION, SERVICE, APP, INTERFACE, GATEWAY, Metric, TYPE, PATH PROFILE, PROBE, and OPERATION. There are two entries:

PR	HITS	NAME	SOURCE	DESTINATION	SERVICE	APP	INTERFACE	GATEWAY	Metric	TYPE	PATH PROFILE	PROBE	OPERATION
1	86	LAN-CSA_27	LAN	CSA-Subnets	Any	Any	CSA_Tunnel1	0.0.0.0	5	Standard		Custom	
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 : アクセスルール

Access Rules												
	PI	HITS	NAME	ACTION	SOURCE	DESTINATION	SOURCE	DESTINATION	DESTINATION P...	USER INCL.	USER EXCL.	SCHEDULE
			Default Access Rule_2	Allow	LAN	LAN	Any	All X0 Management IP	Ping	All	None	Always
			Default Access Rule_3	Allow	LAN	LAN	Any	All X0 Management IP	SSH Management	All	None	Always
			Default Access Rule_4	Allow	LAN	LAN	Any	All X0 Management IP	HTTPS Management	All	None	Always
			Default Access Rule_5	Allow	LAN	LAN	Any	All X0 Management IP	HTTP Management	All	None	Always
			Default Access Rule_6	Allow	LAN	LAN	Any	Any	Any	All	None	Always
			Default Access Rule_9	Allow	LAN	VPN	RemoteAccess Networks	Any	Any	All	None	Always
			Default Access Rule_124	Allow	LAN	VPN	obj_10.10.20.0_24	CSA-Subnets	Any	All	None	Always
			Default Access Rule_12	Allow	WAN	WAN	Any	All X1 Management IP	Ping	All	None	Always
			Default Access Rule_13	Allow	WAN	WAN	Any	All X1 Management IP	SSH Management	All	None	Always
			Default Access Rule_14	Allow	WAN	WAN	Any	All X1 Management IP	HTTPS Management	All	None	Always
			Default Access Rule_15	Allow	WAN	WAN	Any	All X1 Management IP	HTTP Management	All	None	Always
			Default Access Rule_13	Allow	WAN	WAN	Any	X1 IP	IKE	All	None	Always
			Default Access Rule_123	Allow	WAN	WAN	Any	X1 IP	IKE	All	None	Always
			Default Access Rule_122	Allow	WAN	WAN	Any	X1 IP	IKE	All	None	Always
			Default Access Rule_22	Allow	DMZ	DMZ	Any	Any	Any	All	None	Always
			Default Access Rule_23	Allow	DMZ	VPN	RemoteAccess Networks	Any	Any	All	None	Always

Adding Rule

Name: CSA-Inbound-Allow

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

Action: Allow

Type: IPv4

Priority: Manual 1

Schedule: Always

Enable: On

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

Add

- +Addをクリックします。

Access Rules												
	PI	HITS	NAME	ACTION	SOURCE	DESTINATION	SOURCE	DESTINATION	DESTINATION P...	USER INCL.	USER EXCL.	SCHEDULE
			CSA-Inbound-Allow_127	Allow	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

The screenshot shows the 'Network Tunnel Groups' section for 'SonicWall-NTG'. It includes a summary table with region (US (Pacific Northwest)), routing type (Static Routing), and device type (Other). The IP address range is listed as 10.10.10.0/24. Below this, there are two sections: 'Primary Hub' (1 active tunnel, status: Hub Up) and 'Secondary Hub' (0 active tunnels, status: Hub Down). A table of network tunnels shows one entry: Tunnel Group ID (SonicWall-VPN@), Data Center (sse-usw-2-1-1), and IP Address (44.228.138.150). The status column indicates 'Connected'.

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

The screenshot shows the 'IPSec VPN / Network / IPSec VPN / Rules and Settings' page on the Sonicwall NSv 270. The 'Active Tunnels' tab is selected. There is one active tunnel listed: SonicWall-CSA, created on 07/06/2025 at 08:42:48. The table columns include Created, Name, Local, Remote, Gateway, and Comment.

#	CREATED	NAME	LOCAL	REMOTE	GATEWAY	COMMENT
1	07/06/2025 08:42:48	SonicWall-CSA	0.0.0 - 255.255.255.255	0.0.0 - 255.255.255.255	44.228.138.150	

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

トラブルシュート

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の背後にい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。