

Configure Secure Access with Sonicwall Firewall

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Network Diagram](#)

[Configure](#)

[Configure Network Tunnel Group \(VPN\) on Secure Access](#)

[Configure the Tunnel on Sonicwall](#)

[Configure the Tunnel - Rules and Settings](#)

[Add VPN Tunnel Interface](#)

[Add Network Object and Groups](#)

[Add Route](#)

[Add Access Rules](#)

[Verify](#)

[Troubleshoot](#)

[User PC](#)

[Secure Access](#)

[Sonicwall](#)

[Related Information](#)

Introduction

This document describes how to configure an IPsec VTI tunnel between Secure Access to Sonicwall firewall using static routing.

Prerequisites

- [Configure User Provisioning](#)
- [ZTNA SSO Authentication Configuration](#)
- [Configure Remote Access VPN Secure Access](#)

Requirements

Cisco recommends that you have knowledge of these topics:

- Sonicwall (NSv270 - SonicOSX 7.0.1) firewall
- Secure Access
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA
- Clientless ZTNA

Components Used

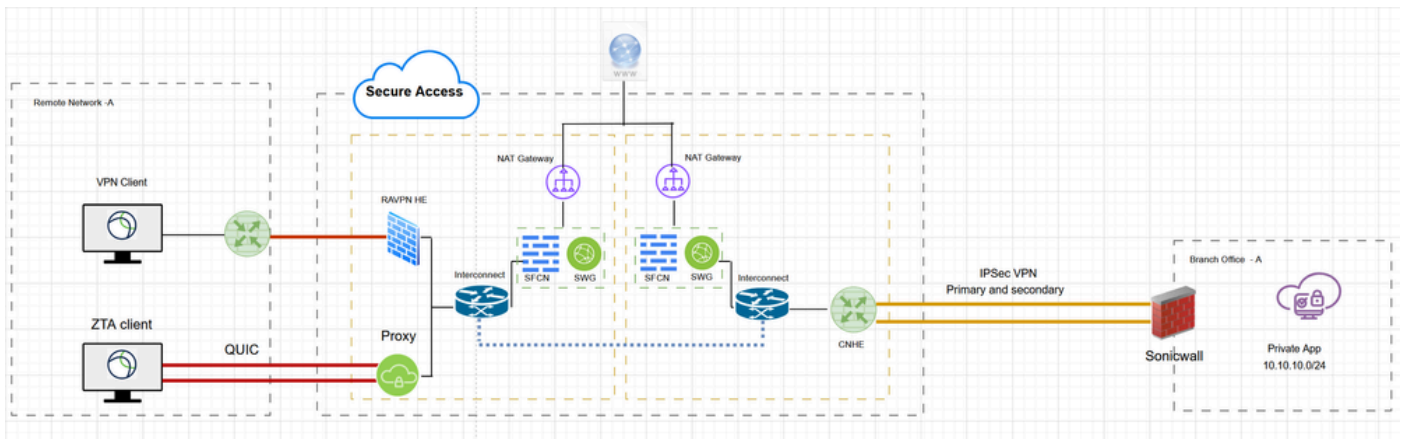
The information in this document is based on:

- Sonicwall (NSv270 - SonicOSX 7.0.1) firewall
- Secure Access
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Network Diagram



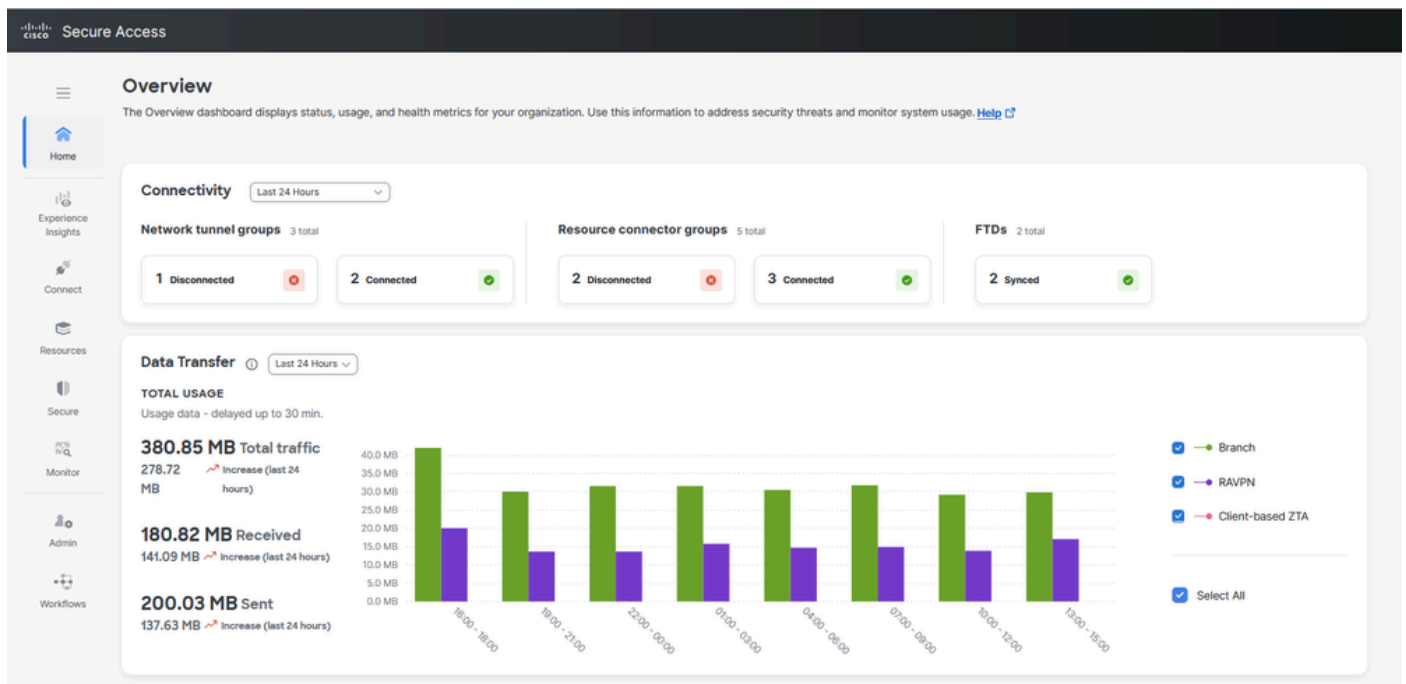
Network Diagram

Configure

Configure Network Tunnel Group (VPN) on Secure Access

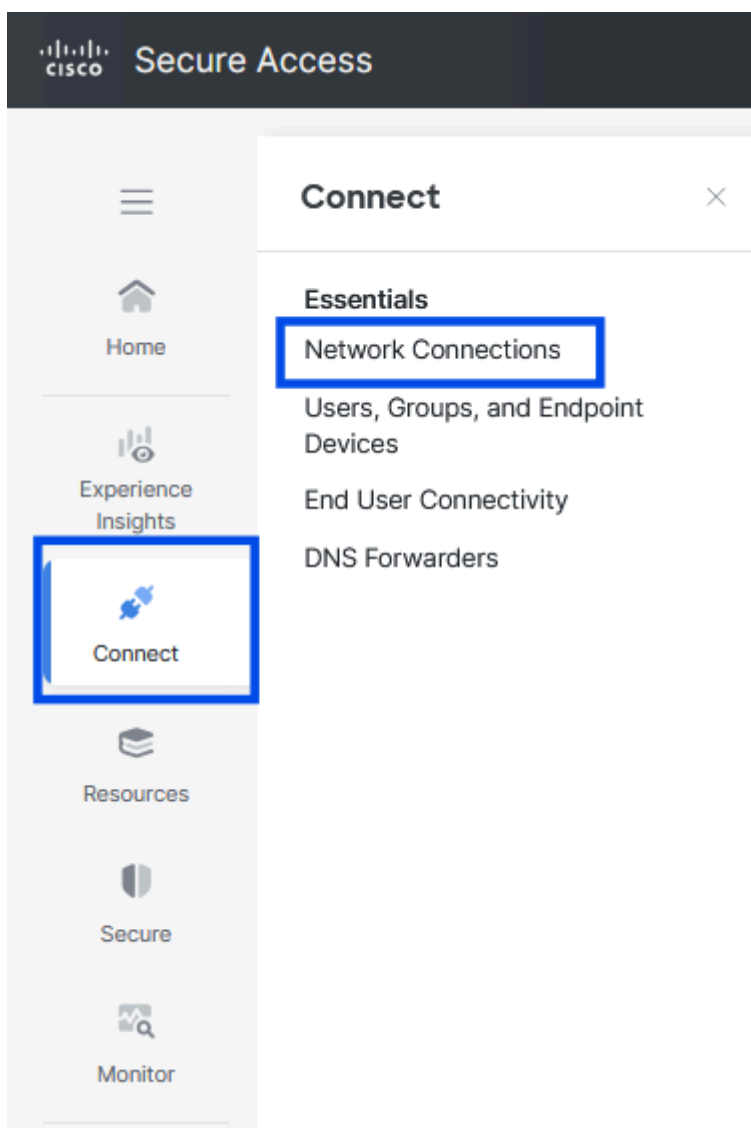
In order to configure VPN tunnel between Secure Access and Sonicwall

- Navigate to the [admin portal](#) of the Secure Access



Secure Access - Main Page

- Click on **Connect > Network Connections**



- Under **Network Tunnel Groups** click on **+ Add**

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
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 ...

Rows per page 10 < 1 >

- Configure **Tunnel Group Name** , **Region** and **Device Typ**
- Click **Next**

← 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

Region

Device Type

[Cancel](#) **Next**



Note: Choose the region nearest to the location of your firewall.

- Configure the **Tunnel ID Fromat** and **Passphrase**
- Click **Next**

← 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

@<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](#)

Secure Access - Tunnel ID and Passphrase

- Configure the IP address ranges, hosts or subnets that you have configured on your network and want to pass the traffic through Secure Access
- Click **Add**
- Click **Save**

General Settings

Tunnel ID and Passphrase

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.

[Add](#)

[X](#)

☐ Dynamic routing

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

Advanced Settings

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

Secure Access - Tunnel Groups - Routing Options

After you click on Save , the information about the tunnel gets displayed. Please save that information for next configuration step

← 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@ sse.cisco.com

Primary Data Center IP Address: 44.228.138.150

Secondary Tunnel ID: SonicWall-VPN@ sse.cisco.com

Secondary Data Center IP Address: 52.35.201.56

Passphrase:

Secure Access - Data for Tunnel Setup

Configure the Tunnel on Sonicwall

Configure the Tunnel - Rules and Settings

Navigate to the Sonicwall Dashboard.

- **Network > IPsec VPN > Rules and Settings**
- Click on + Add

The screenshot shows the SonicWall NSv 270 dashboard. The left sidebar contains a menu with categories like System, Firewall, VoIP, DNS, SD-WAN, and IPsec VPN. The 'IPsec VPN' category is expanded, and 'Rules and Settings' is selected. The main panel shows the 'Rules and Settings' page for IPsec VPN. It includes tabs for Policies, Active Tunnels, and Settings. Under the 'Policies' tab, there are sub-tabs for IPv4 and IPv6. A search bar and action buttons (Statistics, + Add, Delete, Delete All, Disable All, Refresh) are visible. A table lists the existing rule 'WAN GroupVPN' with the following details:

#	NAME	GATEWAY	DESTINATIONS	CRYPTO SUITE	ENABLE
1	WAN GroupVPN			ESP: 3DES/A-MAC SHA1 (IKE)	<input type="checkbox"/>

Total: 1 item(s)

Sonicwall - IPsec VPN - Rules and Settings

- Under VPN Policy , fill out the VPN configuration based on the Tunnel Data from Secure Access and [supported-ipsec-parameters](#)

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@€7-ss

Peer IKE ID

IPv4 Address

44.228.138.150

CancelSave

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

DH Group

Group 14

Life Time (seconds)

28800

CancelSave

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

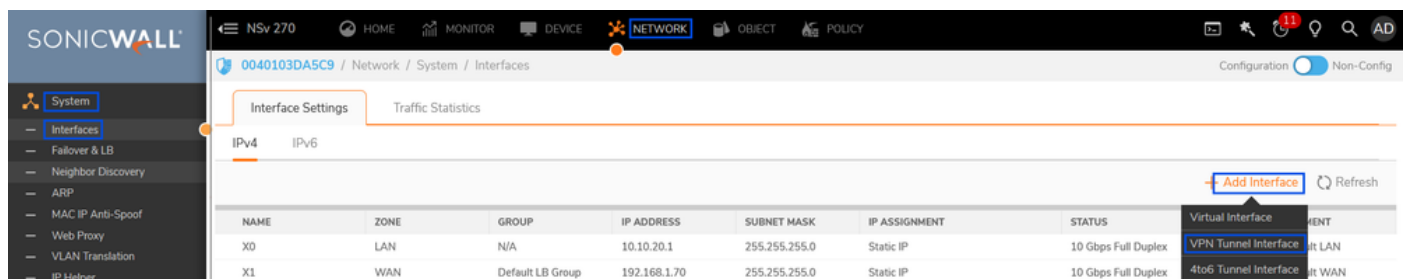
Save

- Click on **Save**

Add VPN Tunnel Interface

Navigate to the Sonicwall Dashboard.

- **Network > System > Interface**
- Click on **+ Add Interface**
- Select **VPN Tunnel Interface**



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

- Click **OK**

SONICWALL

NSv 270

HOME

MONITOR

DEVICE

NETWORK

OBJECT

POLICY

0040103DA5C9 / Network / System / Interfaces

Configuration

Non-Config

Interface Settings

Traffic Statistics

IPv4

IPv6

+ Add Interface

Refresh

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 - Interfaces - VPN Tunnel Interface

Add Network Object and Groups

Navigate to the Sonicwall Dashboard.

- **Object > Match Objects > Addresses**
- **Address Objects**
- Click on **+Add**

0040103DA5C9 / Object / Match Objects / Addresses

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 - Object- Address Objects

Address Object Settings

Name

i

Zone Assignment
 ▼


Type
 ▼

Network

Netmask / Prefix Length


- Click **Save**

Address Object Settings

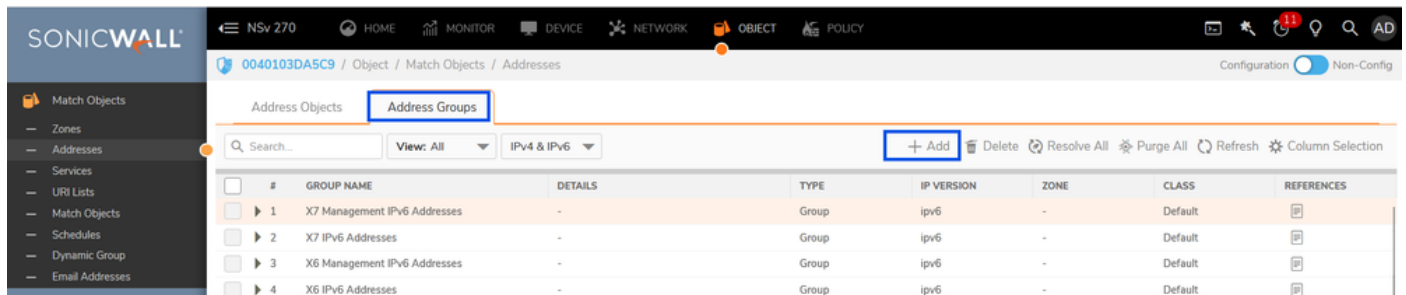
Name	<input type="text" value="CgNAT"/>	
Zone Assignment	<input type="text" value="VPN"/>	▼
Type	<input type="text" value="Network"/>	▼
Network	<input type="text" value="100.64.0.0"/>	
Netmask / Prefix Length	<input type="text" value="255.192.0.0"/>	
<input type="button" value="Cancel"/>		<input type="button"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

- Click **Save**

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"/>

- Click **Save**
- Create Address **Groups**
- Click on **+Add**
- Select the **Address Object** and add them into **Address Groups**



Sonicwall - Object- Address Groups

Add Address Groups

Name

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]

- Click **Save**

Add Route

Navigate to the Sonicwall Dashboard.

- **Policy > Rules and Policies > Routing Rules**
- Click on **+ Add**

SONICWALL

NSv 270

HOME

MONITOR

DEVICE

NETWORK

OBJECT

POLICY

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

0040103DA5C9 / Policy / Rules and Policies / Routing Rules

Q

Default & Custom

IPv4

Active & Inactive

Used & Unused

GENERAL				LOOKUP				NEXT HOP				
<input type="checkbox"/>	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 - Routing Rules

- Add Routing rule

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

- Click on + Add

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

Settings

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

Sonicwall - Routing Rules

Add Access Rules

Navigate to the Sonicwall Dashboard.

- Policy > Rules and Policies > Access Rules
- Click on + Add

- Tunnel Status on Secure Access

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.

Summary
Last Status Update Jul 06, 2025 4:13 PM

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

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

Secondary Hub
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.

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

Secure Access - Network Tunnel Group - VPN status

- Tunnel Status on Sonicwall firewall

SONICWALL
NSv 270 HOME MONITOR DEVICE NETWORK OBJECT POLICY
0040103DA5C9 / Network / IPsec VPN / Rules and Settings
Configuration Non-Config

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

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)

Sonicwall - IPsec VPN status

You can do the same process to configure tunnel between Secure Access Secondary datacenter and Sonicwall

Now , the tunnel is UP on Secure Access and Sonicwall, you can contiue configuring the access to the private resources via RA-VPN , Brosrer-Based ZTA, or Client Based ZTA on Secure Access Dashboard

Troubleshoot

User PC

- Verify User is able to Connect/Enroll to RAVPN/ZTNA successfully or not. If not , troubleshoot further why control plane connection is failing.
- Verify the Network that user is trying to access is supposed to go via RAVPN tunnel or ZTNA . If not , verify configuration on headend .

Secure Access

- Verify traffic steering configuration on RAVPN connection profile to confirm Destination network is configured to send over the tunnel to Secure Access.
- Verify Private Resource is defined with valid protocol/ports and ZTNA/RAVPN connection mechanisms are checked.
- Verify Access-policy is configured to allow RAVPN/ZTNA user to access Private Resource Network and its placed in an order that no other rule is taking precedence to block the traffic.
- Verify IPSec tunnel is UP and Secure Access showing valid Client Routes via static routing which covers Private Resource that user is trying to access.

Sonicwall

- Verify IPSec tunnel is UP or not (IKE & IPSec SA) .
- Verify client route or routes are properly advertised.
- Verify traffic sources from RAVPN/ZTNA user destined to private resource behind Sonicwall is reaching Sonicwall firewall through tunnel by taking packet capture on Sonicwall.
- Verify traffic reached private resource and responding back to RAVPN/ZTNA client or not. If yes, verify those packets are reaching Sonicall X0 (LAN) interface.
- Verify Sonicwall is forwarding the return traffic through IPSec tunnel towards Secure Access.

Related Information

- [Cisco Technical Support & Downloads](#)
- [Cisco Secure Access Help Center](#)
- [Zero Trust Access Module](#)
- [Troubleshoot Secure Access Error "Enrollment Service Is Not Responding. Contact Your IT Help Desk"](#)