

# Configuración de Secure Access con Sonicwall Firewall

## Contenido

---

### [Introducción](#)

### [Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Diagrama de la red](#)

### [Configurar](#)

[Configuración del grupo de túnel de red \(VPN\) en el acceso seguro](#)

[Configuración del túnel en Sonicwall](#)

[Configuración del túnel: reglas y parámetros](#)

[Agregar interfaz de túnel VPN](#)

[Agregar objeto y grupos de red](#)

[Agregar ruta](#)

[Agregar reglas de acceso](#)

### [Verificación](#)

### [Troubleshoot](#)

[PC de usuario](#)

[Acceso seguro](#)

[Sonicwall](#)

### [Información Relacionada](#)

---

## Introducción

Este documento describe cómo configurar un túnel IPsec VTI entre el acceso seguro al firewall Sonicwall usando el ruteo estático.

## Prerequisites

- [Configurar aprovisionamiento de usuarios](#)
- [Configuración de Autenticación SSO de ZTNA](#)
- [Configurar acceso seguro VPN de acceso remoto](#)

## Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Firewall Sonicwall ( NSv270 - SonicOSX 7.0.1 )

- Acceso seguro
- Cisco Secure Client - VPN
- Cisco Secure Client: ZTNA
- ZTNA sin cliente

## Componentes Utilizados

La información de este documento se basa en:

- Firewall Sonicwall ( NSv270 - SonicOSX 7.0.1 )
- Acceso seguro
- Cisco Secure Client - VPN
- Cisco Secure Client: ZTNA

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Antecedentes

## Diagrama de la red

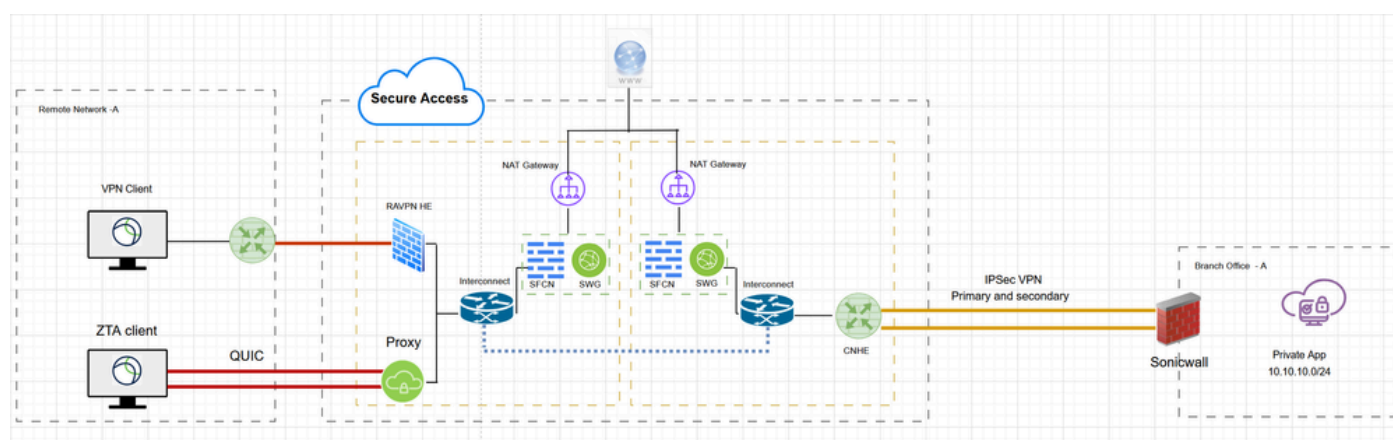


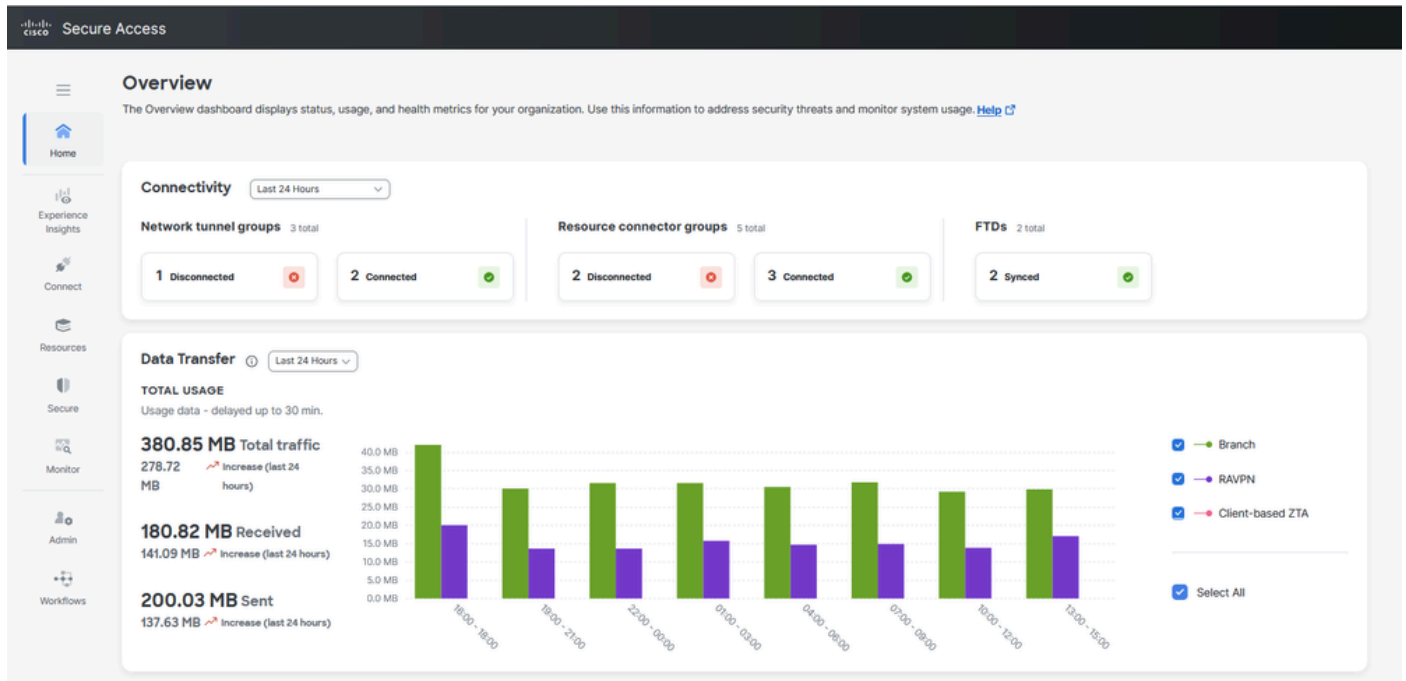
Diagrama de la red

## Configurar

### Configuración del grupo de túnel de red (VPN) en el acceso seguro

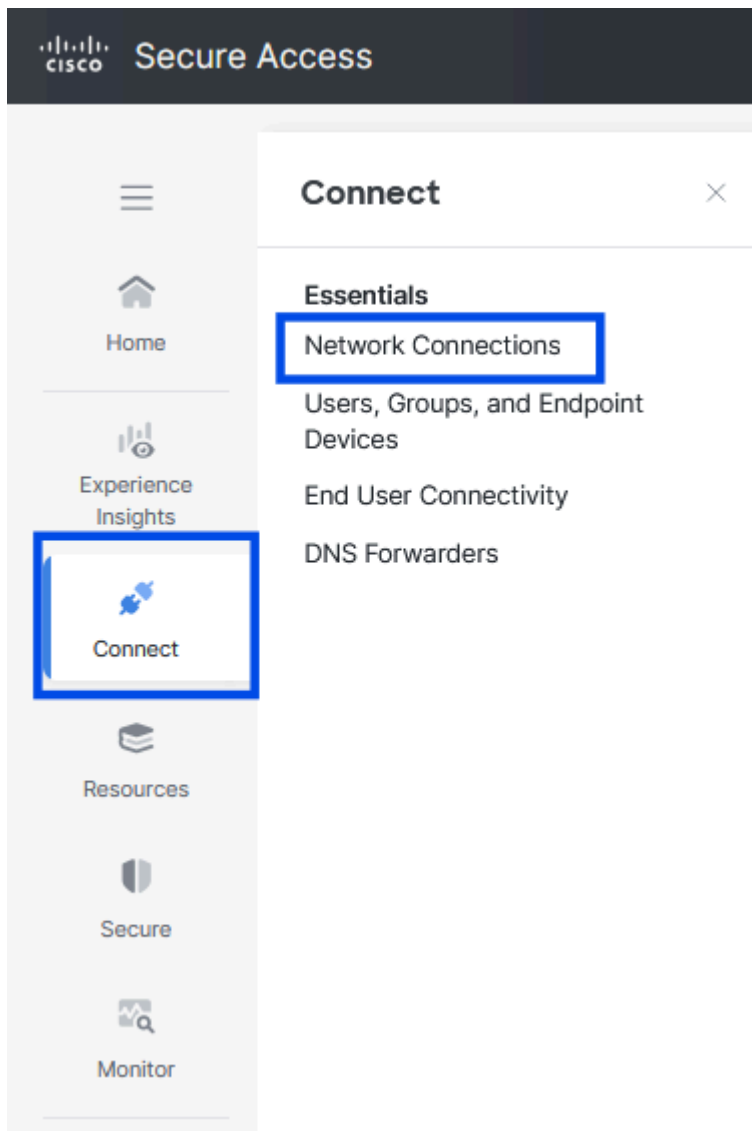
Para configurar el túnel VPN entre Secure Access y Sonicwall

- Vaya al [portal](#) de [administración](#) de Secure Access



Acceso seguro - Página principal

- Haga clic en Connect > Network Connections .



Acceso seguro - Conexiones de red

- En Network Tunnel Groups, haga clic en + Add

The image shows the 'Network Connections' page in the Cisco Secure Access interface. The page has a sub-header 'Network Tunnel Groups' and a description: 'Manage the connections that allow user traffic to reach private resources on your network. For information about these options, see [Help](#)'. Below this is a summary bar showing '0 Disconnected', '0 Warning', and '2 Connected'. The main section is titled 'Network Tunnel Groups' and includes a description: '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](#)'. There is a search bar and filters for 'Region' and 'Status'. A table lists two tunnel groups: 'AZURE' and 'LAB-BGP', both with a status of 'Connected'. The table columns are: Network Tunnel Group, Status, Region, Primary Hub Data Center, Primary Tunnels, Secondary Hub Data Center, and Secondary Tunnels. At the bottom right, there is a '+ Add' button (highlighted with a blue box) and a pagination control showing 'Rows per page 10' and '1'.



- Configure los rangos de direcciones IP, los hosts o las subredes que ha configurado en la red y que desea que el tráfico pase a través de Secure Access
- Haga clic en Add (Agregar)
- Haga clic en Save (Guardar).

**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**

Después de hacer clic en Save (Guardar), se muestra la información sobre el túnel. Guarde esa información para el siguiente paso de configuración

**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](#)

**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.

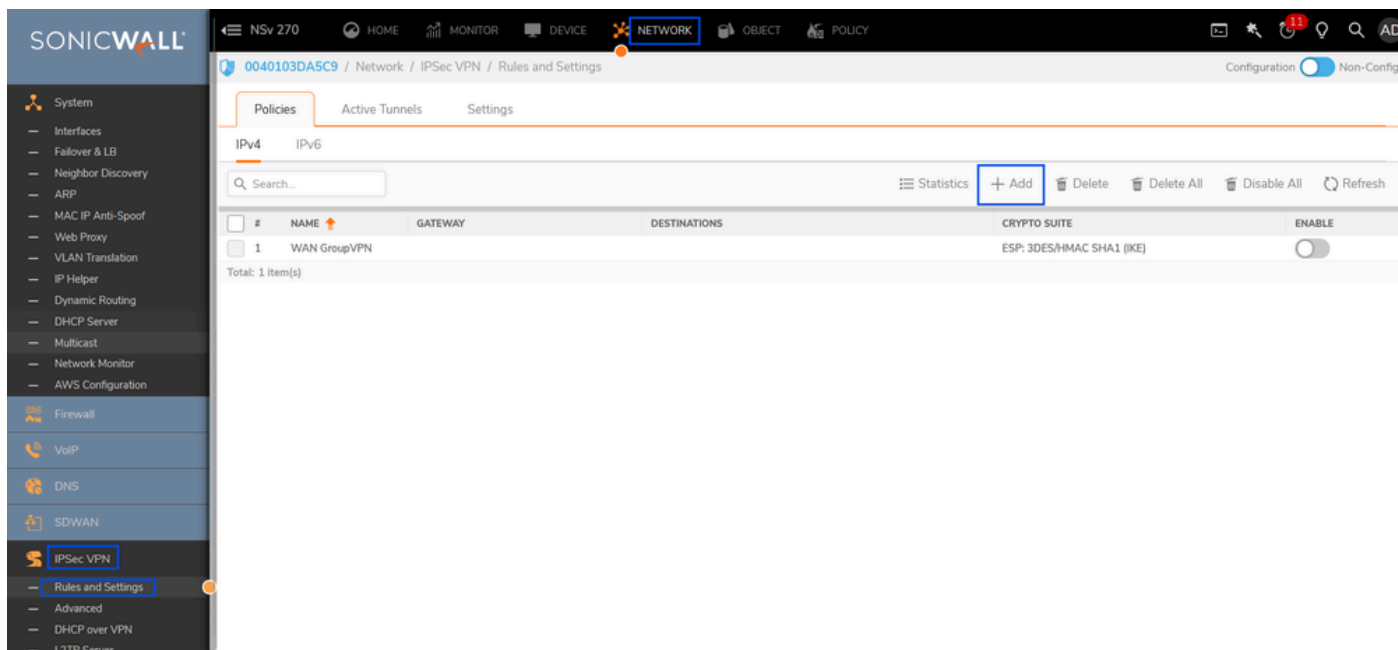
<b>Primary Tunnel ID:</b>	SonicWall-VPN@i	sse.cisco.com
<b>Primary Data Center IP Address:</b>	44.228.138.150	
<b>Secondary Tunnel ID:</b>	SonicWall-VPN@i	sse.cisco.com
<b>Secondary Data Center IP Address:</b>	52.35.201.56	
<b>Passphrase:</b>		

## Configuración del túnel en Sonicwall

### Configuración del túnel: reglas y parámetros

Vaya al panel de Sonicwall.

- Red > VPN IPsec > Reglas y configuración
- Haga clic en + Agregar



Sonicwall - VPN IPsec - Reglas y configuración

- En VPN Policy , complete la configuración VPN basada en los datos del túnel de Secure Access y los [parámetros admitidos de ipsec](#)

## 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

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

ⓘ

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

- Haga clic en Guardar

## Agregar interfaz de túnel VPN

Vaya al panel de Sonicwall.

- Network > System > Interface
- Haga clic en + Agregar interfaz
- Seleccione la interfaz de túnel VPN

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	
X0	LAN	N/A	10.10.20.1	255.255.255.0	Static IP	10 Gbps Full Duplex	Virtual Interface
X1	WAN	Default LB Group	192.168.1.70	255.255.255.0	Static IP	10 Gbps Full Duplex	VPN Tunnel Interface

4to6 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

- Haga clic en OK (Aceptar).

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		Default LAN
X1	WAN	Default LB Group	192.168.1.70	255.255.255.0	Static IP	10 Gbps Full Duplex		Default WAN
X2	Unassigned	N/A	0.0.0.0	0.0.0.0		10 Gbps Full Duplex		N/A
X3	Unassigned	N/A	0.0.0.0	0.0.0.0		10 Gbps Full Duplex		N/A
X4	Unassigned	N/A	0.0.0.0	0.0.0.0		10 Gbps Full Duplex		N/A
X5	Unassigned	N/A	0.0.0.0	0.0.0.0		10 Gbps Full Duplex		N/A
X6	Unassigned	N/A	0.0.0.0	0.0.0.0		10 Gbps Full Duplex		N/A
X7	Unassigned	N/A	0.0.0.0	0.0.0.0		10 Gbps Full Duplex		N/A
CSA_Tunnel1	VPN	N/A	169.254.0.6	255.255.255.252	Static IP	Interface Up		Tunnel 1 interface - With CSA Primary DC

Sonicwall - Interfaces - Interfaz de túnel VPN

Agregar objeto y grupos de red

Vaya al panel de Sonicwall.

- Objeto > Coincidir objetos > Direcciones
- Objetos de dirección
- Haga clic en +Agregar

0040103DA5C9 / Object / Match Objects / Addresses

Configuration ☒ Config ☐ 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 - Objeto- Objetos de dirección

## Address Object Settings

**Name**  ⓘ

**Zone Assignment**  ▼


**Type**  ▼

**Network**

**Netmask / Prefix Length**


- Haga clic en Save (Guardar).

# Address Object Settings

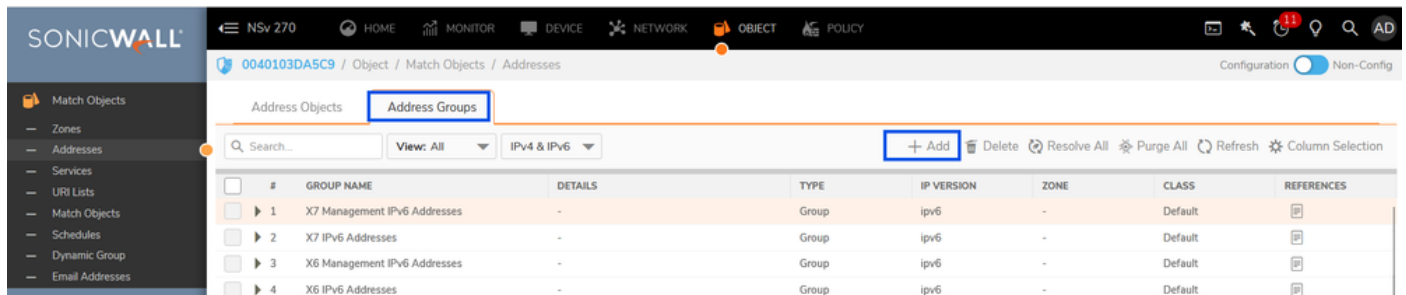
Name	<input type="text" value="CgNAT"/>	
Zone Assignment	<input type="text" value="VPN"/>	▼
Type	<input type="text" value="Network"/>	▼
Network	<input type="text" value="100.64.0.0"/>	
Netmask / Prefix Length	<input type="text" value="255.192.0.0"/>	
<input type="button" value="Cancel"/>		<input type="button"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

- Haga clic en Save (Guardar).

# 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"/>

- Haga clic en Save (Guardar).
- Crear grupos de direcciones
- Haga clic en +Agregar
- Seleccione el objeto de dirección y agréguelo a los grupos de direcciones



Sonicwall - Objeto- Grupos de direcciones

## 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]

Cancel

Save

- Haga clic en Save (Guardar).

## Agregar ruta

Vaya al panel de Sonicwall.

- Directiva > Reglas y políticas > Reglas de enrutamiento
- Haga clic en + Agregar

SONICWALL

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

NSv 270

HOME

MONITOR

DEVICE

NETWORK

OBJECT

POLICY

0040103DA5C9 / Policy / Rules and Policies / Routing Rules

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 - Reglas de enrutamiento

- Agregar regla de enrutamiento

## 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** 0.0.0.0/1

**Metric** 5

**Show Diagram** ☐

Cancel

Add

- Haga clic en + Agregar

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													
GENERAL													
LOOKUP													
NEXT HOP													
PROBE OPERATION													
PR HITS NAME SOURCE DESTINATION SERVICE APP INTERFACE GATEWAY M. TYPE PATH PROFILE PROBE CLASS													
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 - Reglas de enrutamiento

## Agregar reglas de acceso

Vaya al panel de Sonicwall.

- Directiva > Reglas y políticas > Reglas de acceso
- Haga clic en + Agregar

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

Sonicwall - Reglas de acceso

## 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

DESTINATION

Zone/Interface

VPN

Address

CSA-Subnets

Port/Services

Any

Zone/Interface

LAN

Address

LAN

Port/Services

Any

Show Diagram

Cancel

Add

- Haga clic en +Agregar

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-Allow_127	Allow	VPN	LAN	CSA-Subnets	LAN	Any	All	None	Always

Sonicwall - Reglas de acceso



# Verificación

- Estado del túnel en acceso seguro

← 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

Acceso seguro - Grupo de túnel de red - Estado de VPN

- Estado del túnel en el firewall Sonicwall

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

Fallover & 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 - Estado de VPN IPsec

Puede realizar el mismo proceso para configurar el túnel entre el Data Center secundario de acceso seguro y Sonicwall

Ahora, el túnel está ACTIVO en Secure Access y Sonicwall, puede continuar configurando el acceso a los recursos privados a través de RA-VPN , ZTA basado en navegador o ZTA basado en cliente en Secure Access Dashboard

# Troubleshoot

## PC de usuario

- Verifique que el usuario pueda conectarse/inscribirse correctamente a RAVPN/ZTNA o no. Si no es así, solucione más problemas por qué falla la conexión del plano de control.
- Verifique que la red a la que el usuario está intentando acceder se supone que va a través del túnel RAVPN o ZTNA . Si no es así, verifique la configuración en la cabecera .

## Acceso seguro

- Verifique la configuración del direccionamiento del tráfico en el perfil de conexión RAVPN para confirmar que la red de destino está configurada para enviar a través del túnel a Secure Access.
- Verifique que el recurso privado esté definido con protocolos/puertos válidos y que los mecanismos de conexión ZTNA/RAVPN estén verificados.
- Verifique que la política de acceso esté configurada para permitir que el usuario de RAVPN/ZTNA acceda a la Red de Recursos Privados y se coloque en un orden en el que ninguna otra regla tenga prioridad para bloquear el tráfico.
- Verifique que el túnel IPSec esté ACTIVO y que Secure Access muestre las rutas de cliente válidas a través del routing estático que cubre el recurso privado al que el usuario está intentando acceder.

## Sonicwall

- Verifique que el túnel IPSec esté ACTIVO o no ( IKE & IPSec SA) .
- Verifique que la ruta o rutas del cliente estén anunciadas correctamente.
- Verifique que las fuentes de tráfico del usuario de RAVPN/ZTNA destinadas a un recurso privado detrás de Sonicwall estén llegando al firewall de Sonicwall a través del túnel mediante la captura de paquetes en Sonicwall.
- Verifique que el tráfico haya alcanzado el recurso privado y responda al cliente RAVPN/ZTNA o no. Si la respuesta es sí, verifique que esos paquetes estén llegando a la interfaz X0 (LAN) de Sonic.
- Verifique que Sonicwall está reenviando el tráfico de retorno a través del túnel IPSec hacia el acceso seguro.

## Información Relacionada

- [Soporte técnico y descargas de Cisco](#)
- [Centro de ayuda de Cisco Secure Access](#)
- [Módulo de acceso de confianza cero](#)
- [Solucionar El Error De Acceso Seguro "El Servicio De Inscripción No Responde. Póngase en contacto con el soporte técnico de TI"](#)

#### Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).