

# 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](#)

[Aregar interfaz de túnel VPN](#)

[Aregar objeto y grupos de red](#)

[Aregar ruta](#)

[Aregar 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

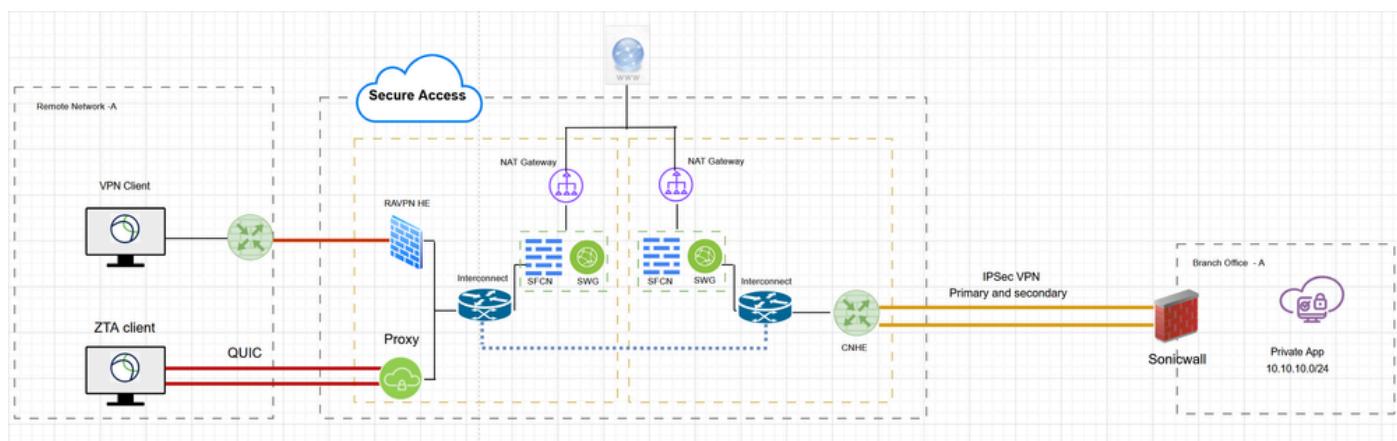
La información de este documento se basa en:

- 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

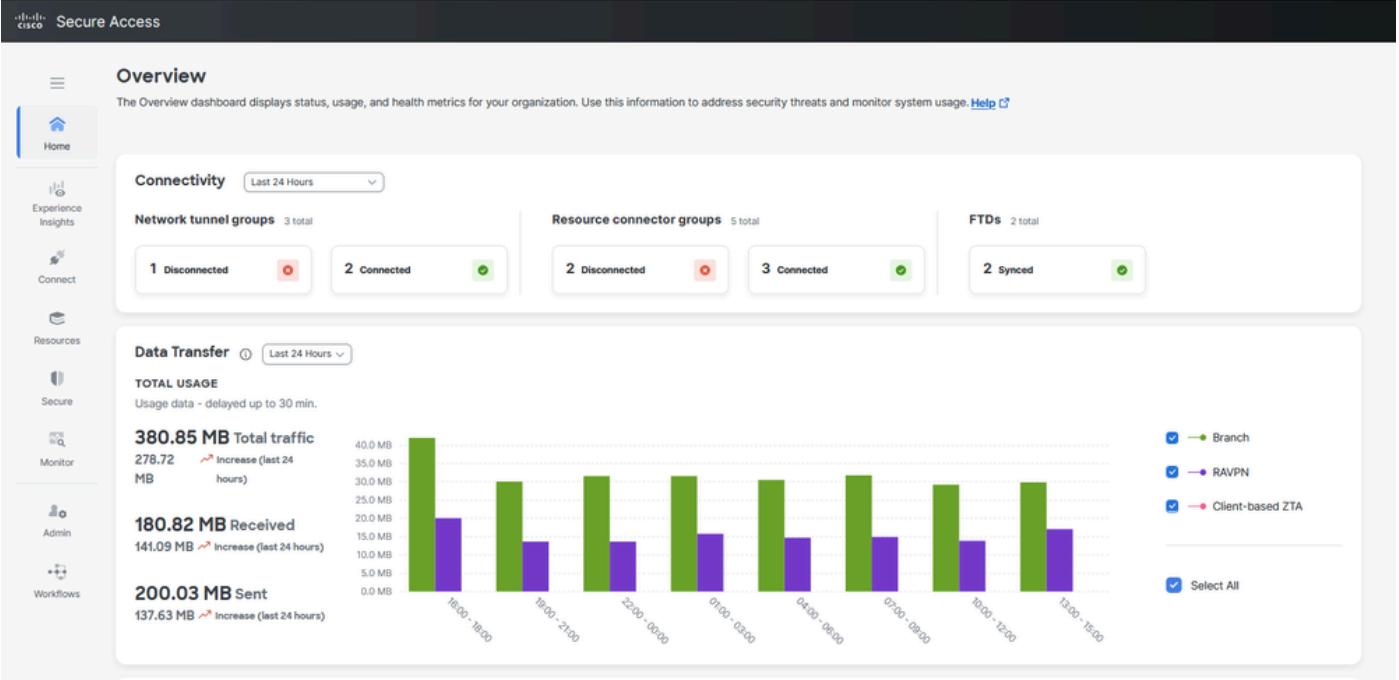


## Configurar

### 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 .

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

Acceso seguro - Conexiones de red

- En Network Tunnel Groups, haga clic en + Add

The screenshot shows the 'Network Tunnel Groups' page in the Cisco Secure Access interface. The left sidebar includes icons for Home, Experience Insights, Connect (selected and highlighted with a blue box), Resources, Secure, Monitor, Admin, and Workflows. The main content area shows a summary of 'Network Tunnel Groups' (2 total) with 0 Disconnected, 0 Warning, and 2 Connected. Below this is a detailed table of 'Network Tunnel Groups' with columns: Network Tunnel Group, Status, Region, Primary Hub Data Center, Primary Tunnels, Secondary Hub Data Center, and Secondary Tunnels. Two entries are listed: 'AZURE' (Connected, US (Pacific Northwest), Primary Hub: sse-usw-2-1-1, Primary Tunnels: 1, Secondary Hub: sse-usw-2-1-0, Secondary Tunnels: 1) and 'LAB-BGP' (Connected, US (Pacific Northwest), Primary Hub: sse-usw-2-1-1, Primary Tunnels: 1, Secondary Hub: sse-usw-2-1-0, Secondary Tunnels: 1). The bottom right corner shows pagination and row selection controls.

- Configuración del nombre del grupo de túneles, la región y el tipo de dispositivo
  - Haga clic en Next (Siguiente)

← 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](#)



Nota: Seleccione la región más cercana a la ubicación del firewall.

- Configuración del Formato de ID de túnel y la Frase de contraseña
  - Haga clic en Next (Siguiente)

Acceso seguro: ID de túnel y frase de paso

- 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 (Aregar)
- Haga clic en Save (Guardar).

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.

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

Acceso seguro - Grupos de túnel - Opciones de routing

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](#)

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:**

Cancel

Back Save

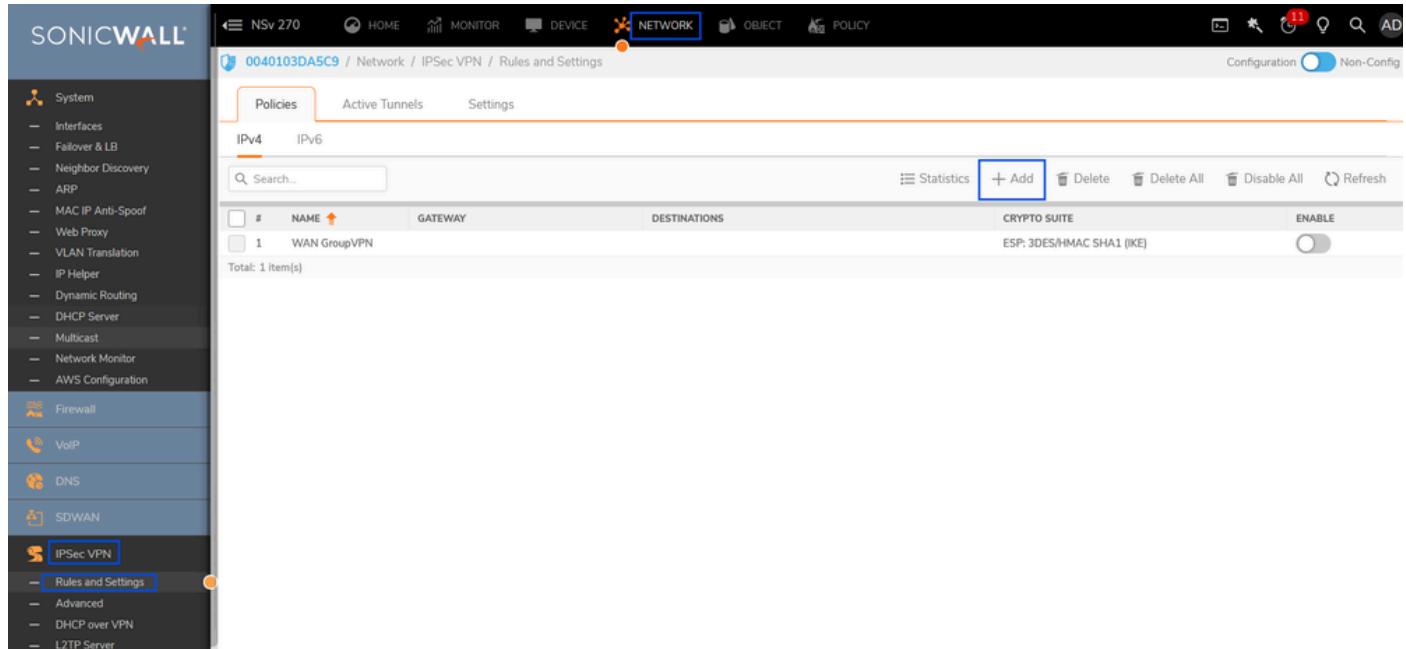
Secure Access - Datos para la configuración del túnel

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

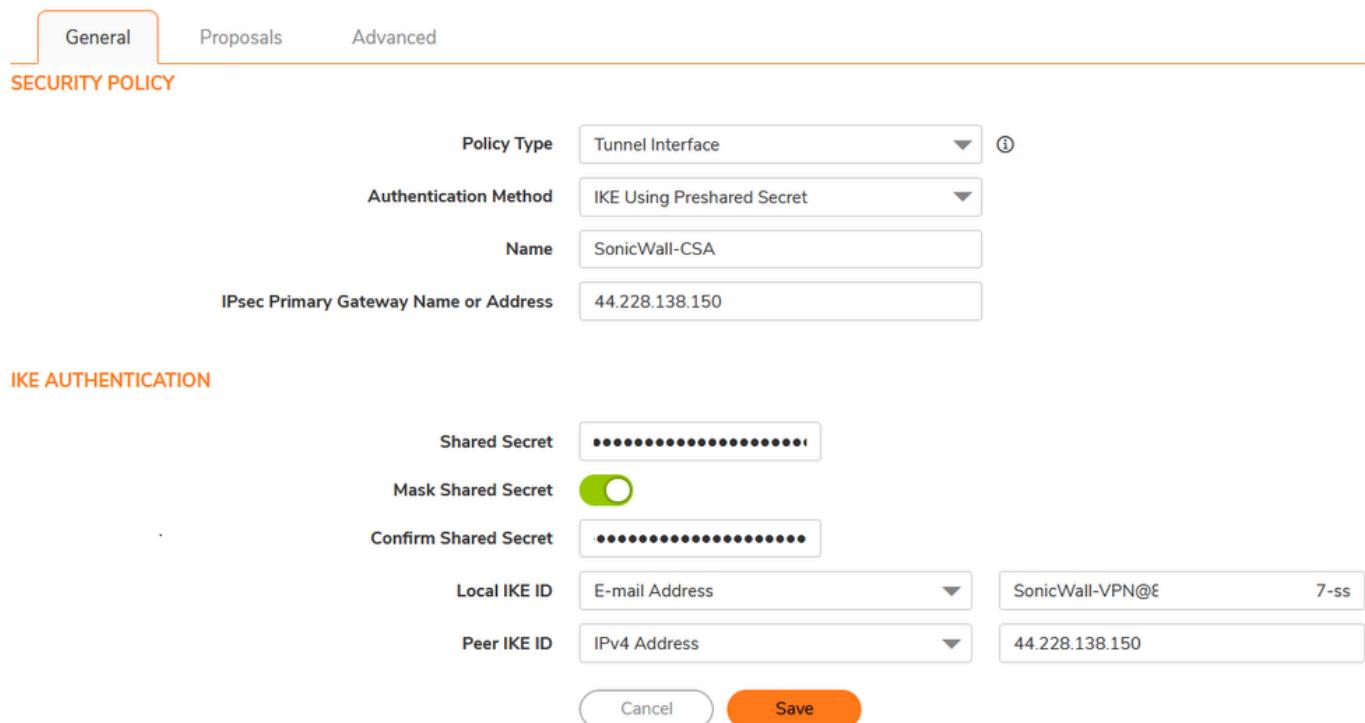


The screenshot shows the Sonicwall interface with the following navigation path: SONICWALL > NSv 270 > HOME > MONITOR > DEVICE > NETWORK > 0040103DA5C9 / Network / IPsec VPN / Rules and Settings. The left sidebar includes sections for System, Firewall, VoIP, DNS, SDWAN, and IPsec VPN (which is selected). Under IPsec VPN, 'Rules and Settings' is also selected. The main content area displays a table of rules, with the first rule 'WAN GroupVPN' selected. The table includes columns for NAME, GATEWAY, DESTINATIONS, CRYPTO SUITE, and ENABLE. The 'CRYPTO SUITE' for the selected rule is 'ESP: 3DES/HMAC SHA1 (IKE)'. A blue box highlights the '+ Add' button in the top right of the table area.

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



The screenshot shows the 'General' tab of the VPN Policy configuration. The 'SECURITY POLICY' section contains the following fields:

- Policy Type: Tunnel Interface
- Authentication Method: IKE Using Preshared Secret
- Name: SonicWall-CSA
- IPsec Primary Gateway Name or Address: 44.228.138.150

The 'IKE AUTHENTICATION' section contains the following fields:

- Shared Secret: (redacted)
- Mask Shared Secret: (on)
- Confirm Shared Secret: (redacted)
- Local IKE ID: E-mail Address: SonicWall-VPN@E, 7-ss
- Peer IKE ID: 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"/>	<small>i</small>	Display Suite B Compliant Algorithms Only	<input type="checkbox"/>
Disable IPsec Anti-Replay	<input type="checkbox"/>	<small>i</small>	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		Interface X1	

**IKEV2 SETTINGS**

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

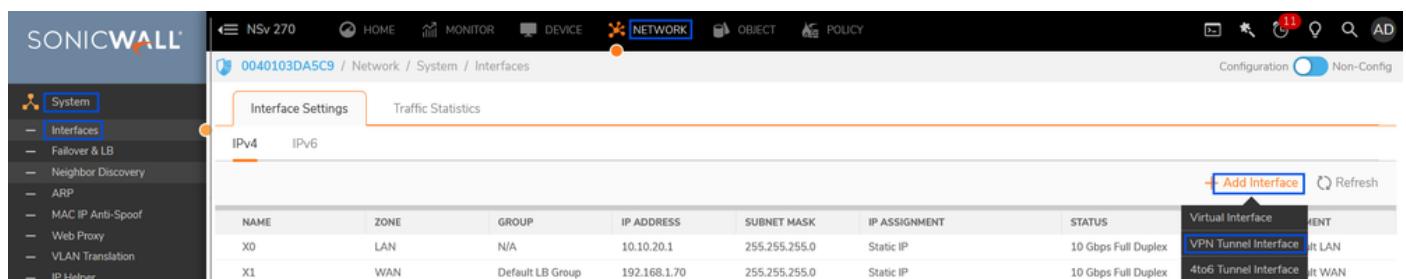
**Buttons:** Cancel, Save

- 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



The screenshot shows the Sonicwall interface with the 'Add Interface' button highlighted in blue. The interface list includes 'Virtual Interface', 'VPN Tunnel Interface', and '4to6 Tunnel Interface'.

Sonicwall - Interfaces

# 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	<input type="checkbox"/>
Port	<input type="checkbox"/>

**USER LOGIN**

HTTP	<input type="checkbox"/>
HTTPS	<input type="checkbox"/>

- Haga clic en OK (Aceptar).

SONICWALL

0040103DASC9 / Network / System / Interfaces

Configuration Non-Config

Interface Settings								
IPv4		IPv6						
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		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

#	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  ⓘ

Zone Assignment  ▾

Type  ▾

Network

Netmask / Prefix Length

- Haga clic en Save (Guardar).

# Address Object Settings

Name  ⓘ

Zone Assignment  ▾

Type  ▾

Network

Netmask / Prefix Length

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

SONICWALL

NSv 270 HOME MONITOR DEVICE NETWORK OBJECT POLICY

0040103DA5C9 / Object / Match Objects / Addresses

Address Objects Address Groups

Search... View: All IPv4 & IPv6

+ Add Delete Resolve All Purge All Refresh Column Selection

#	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	

Sonicwall - Objeto- Grupos de direcciones

## 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

- Haga clic en Save (Guardar).

## Agregar ruta

Vaya al panel de Sonicwall.

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

	GENERAL		LOOKUP				NEXT HOP					
	PR	HITS	NAME	SOURCE	DESTINATION	SERVICE	APP	INTERFACE	GATEWAY	M...	TYPE	PATH
			Route Policy_5	Any	255.255.255.255/32	Any	Any	X0	0.0.0.0	20	Standar	
			Route Policy_7	Any	X1 Default Gateway	Any	Any	X1	0.0.0.0	20	Standar	
			Route Policy_26	Any	CSA_Tunnel1 Subnet	Any	Any	CSA_Tunnel1	0.0.0.0	20	Standar	
			Route Policy_4	X0 Subnet	Any	Any	Any	X0	0.0.0.0	20	Standar	
			Route Policy_6	X1 Subnet	Any	Any	Any	X1	0.0.0.0	20	Standar	
			Route Policy_8	X1 IP	Any	Any	Any	X1	X1 Default Gateway	20	Standar	
			Route Policy_9	0.0.0.0/0	Any	Any	Any	X1	192.168.1.1	20	Standar	

Sonicwall - Reglas de enrutamiento

- Agregar regla de enrutamiento

## Adding Rule

**Name**  **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**

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

**Show Diagram**

## Adding Rule

Form for adding a new route rule:

Name	LAN-CSA	Type	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
Tags	add upto 3 tags, use comma as separator...		
Description	provide a short description of your route...		

Buttons: Lookup, Next Hop (highlighted), Advanced, Probe

Route Type Selection:

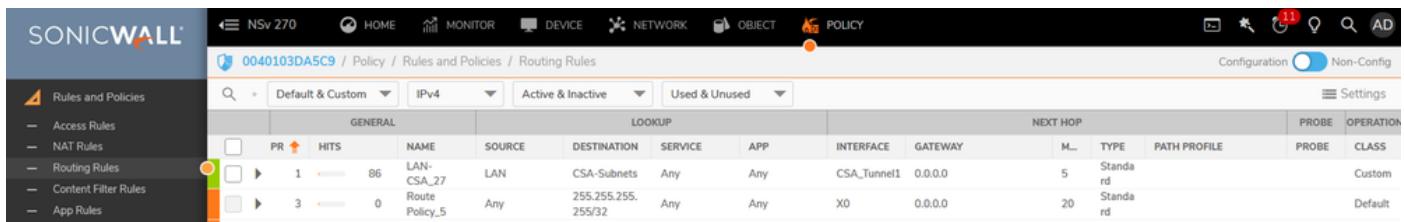
- Standard Route
- Multi-Path Route
- SD-WAN Rule

Fields:

Interface	CSA_Tunnel1
Gateway	0.0.0.0/0
Metric	5

Buttons: Show Diagram, Cancel, Add

- Haga clic en + Agregar



ROUTING 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 enruteamiento

## Agregar reglas de acceso

Vaya al panel de Sonicwall.

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

Sonicwall - Reglas de acceso

Access Rules											
<input type="button" value="Search"/> Default & Custom <input type="button" value="IPv4"/> All Zones -> All Zones Active & Inactive Used & Unused <input type="button" value="Max Count"/> <input type="button" value="Reset Rules"/> <input type="button" value="Settings"/>											
		GENERAL		ZONE		ADDRESS		SERVICE		USER	
PI	HITS	NAME	ACTION	SOURCE	DESTINATION	SOURCE	DESTINATION	DESTINATION P...	USER INCL.	USER EXCL.	SCHEDULE
		Default Access Rule_1	Allow	LAN	LAN	Any	All X0 Management IP	Ping	All	None	Always
		Default Access Rule_2	Allow	LAN	LAN	Any	All X0 Management IP	SSH Management	All	None	Always
		Default Access Rule_3	Allow	LAN	LAN	Any	All X0 Management IP	HTTPS Management	All	None	Always
		Default Access Rule_4	Allow	LAN	LAN	Any	All X0 Management IP	HTTP Management	All	None	Always
		Default Access Rule_5	Allow	LAN	LAN	Any	All X0 Management IP	Management	All	None	Always
		Default Access Rule_6	Allow	LAN	LAN	Any	Any	Any	All	None	Always
		Default Access Rule_7	Allow	VPN	RemoteAccess Networks	Any	Any	All	None	Always	
		Default Access Rule_124	Allow	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	Any	IKE	All	None	Always
		Default Access Rule_123	Allow	WAN	WAN	X1 IP	Any	IKE	All	None	Always
		Default Access Rule_122	Allow	WAN	WAN	Any	X1 IP	Any	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

- Haga clic en +Agregar

Sonicwall - Reglas de acceso

Access Rules											
<input type="button" value="Search"/> Default & Custom <input type="button" value="IPv4"/> All Zones -> All Zones Active & Inactive Used & Unused <input type="button" value="Max Count"/> <input type="button" value="Reset Rules"/> <input type="button" value="Settings"/>											
		GENERAL		ZONE		ADDRESS		SERVICE		USER	
PI	HITS	NAME	ACTION	SOURCE	DESTINATION	SOURCE	DESTINATION	DESTINATION P...	USER INCL.	USER EXCL.	SCHEDULE
		CSA-Inbound-Allow_12	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**

**Primary Hub**

**Secondary Hub**

**Network 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	<span>Connected</span>	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

Configuration  Non-Config

0040103DA5C9 / Network / 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	

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, soluciones 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).