Configuración de Secure Access con Sonicwall Firewall

Contenido

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

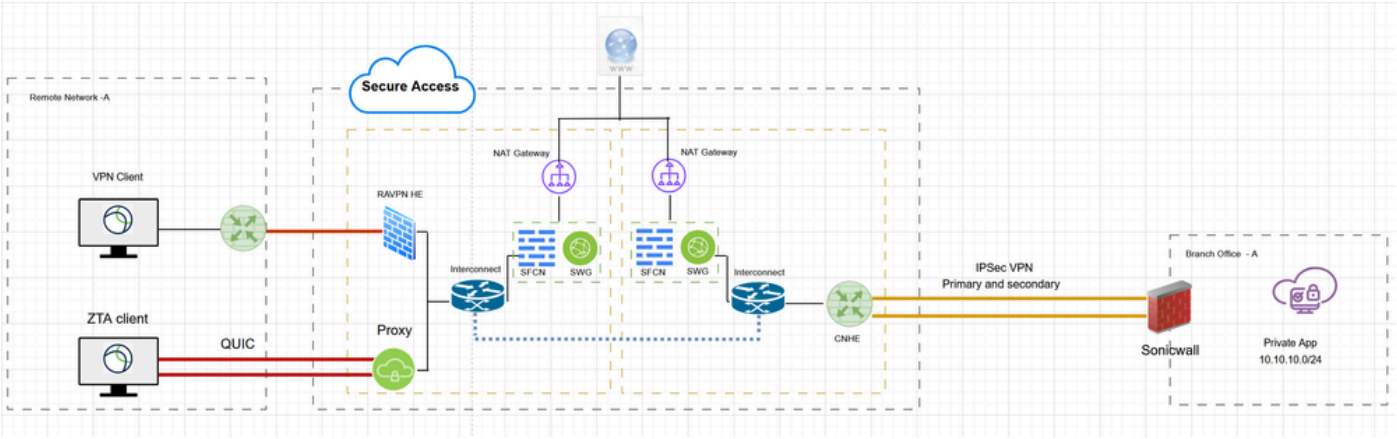


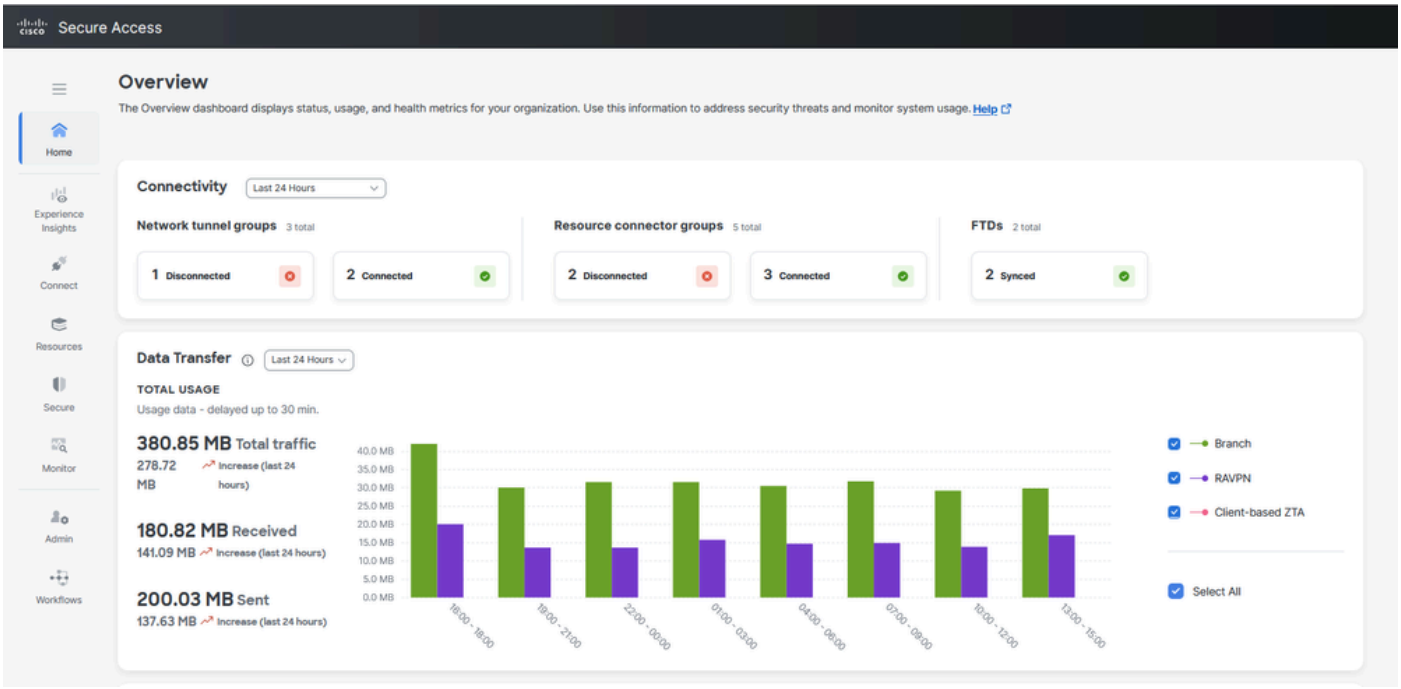
Diagrama de la red

Configurar

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

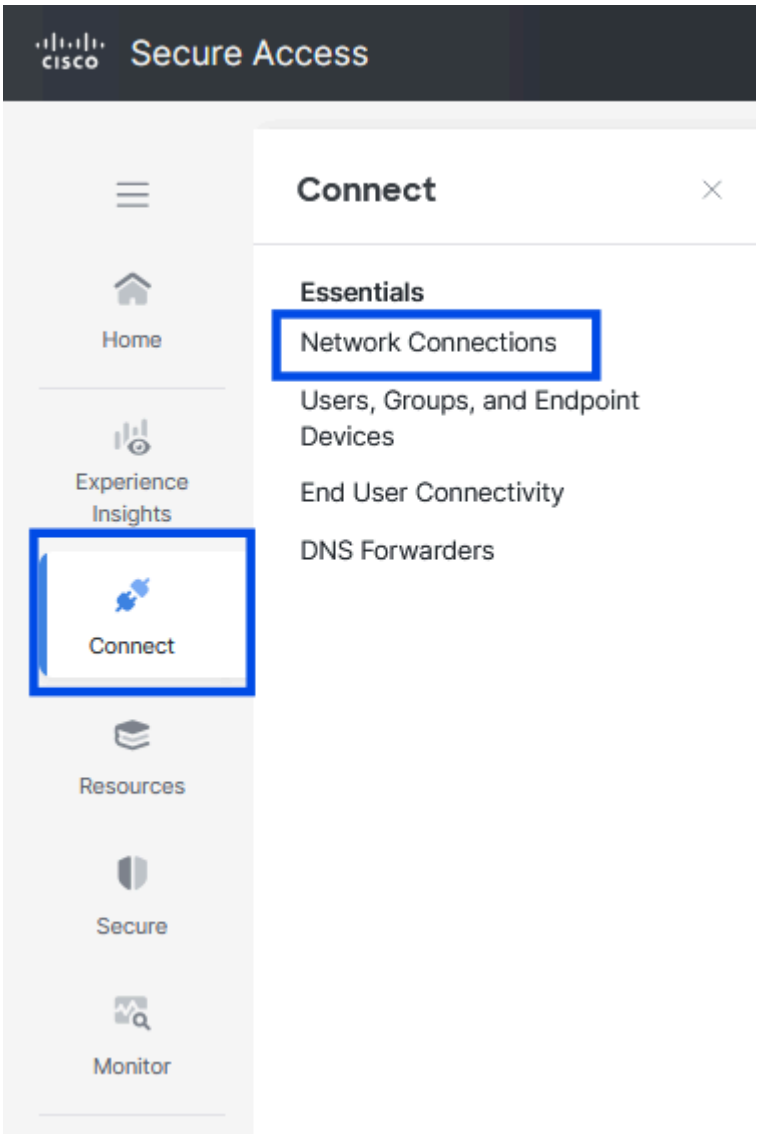
Para configurar el túnel VPN entre Secure Access y Sonicwall

- Vaya al portal de administración de Secure Access



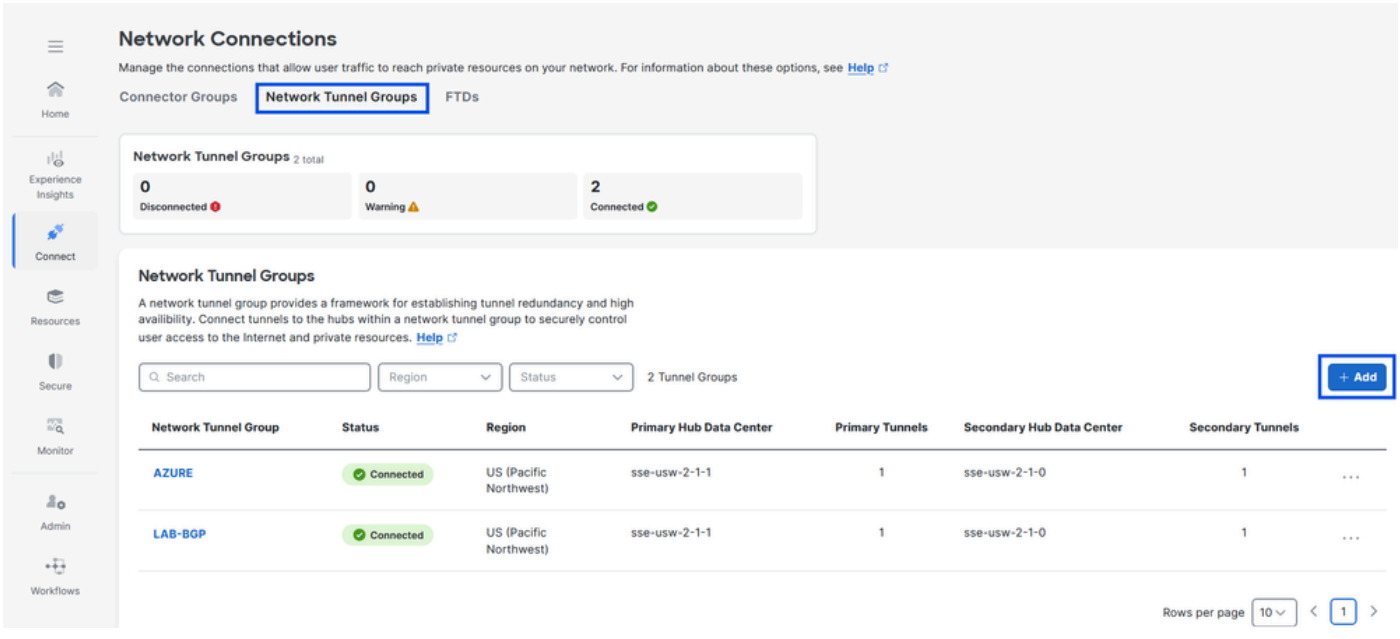
Acceso seguro - Página principal

- Haga clic en Connect > Network Connections .



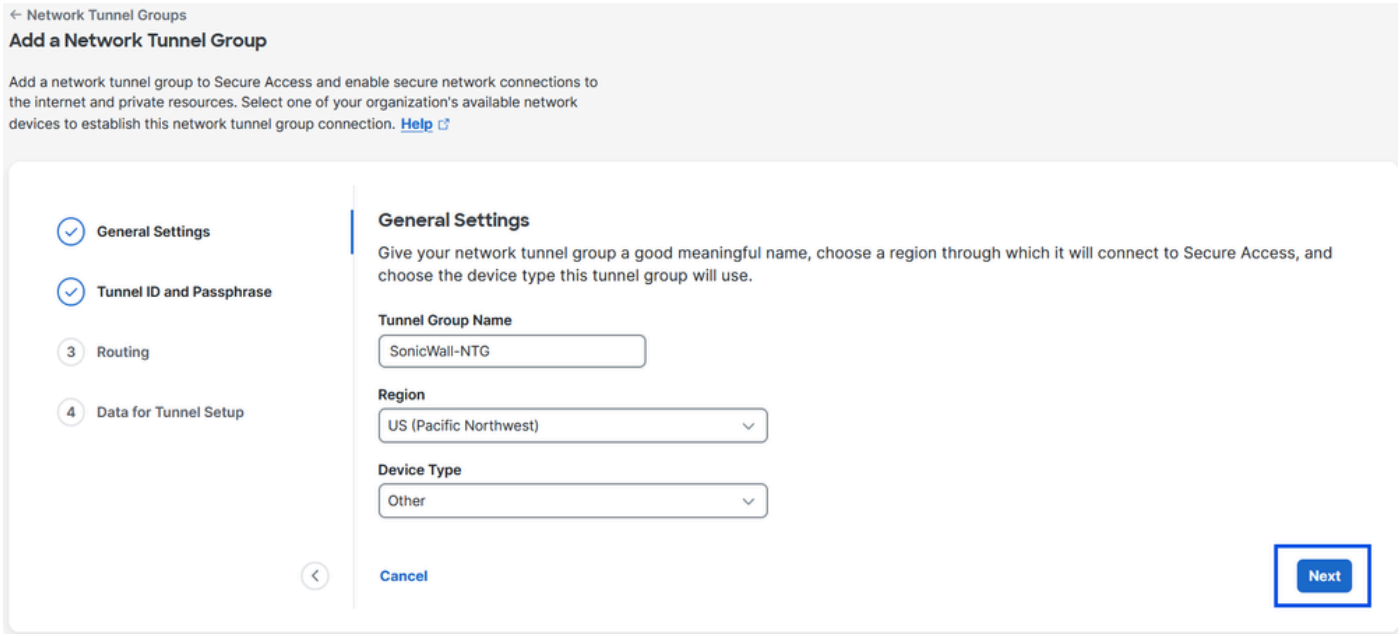
Acceso seguro - Conexiones de red

- En Network Tunnel Groups, haga clic en + Add



Acceso seguro - Grupos de túnel de red

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

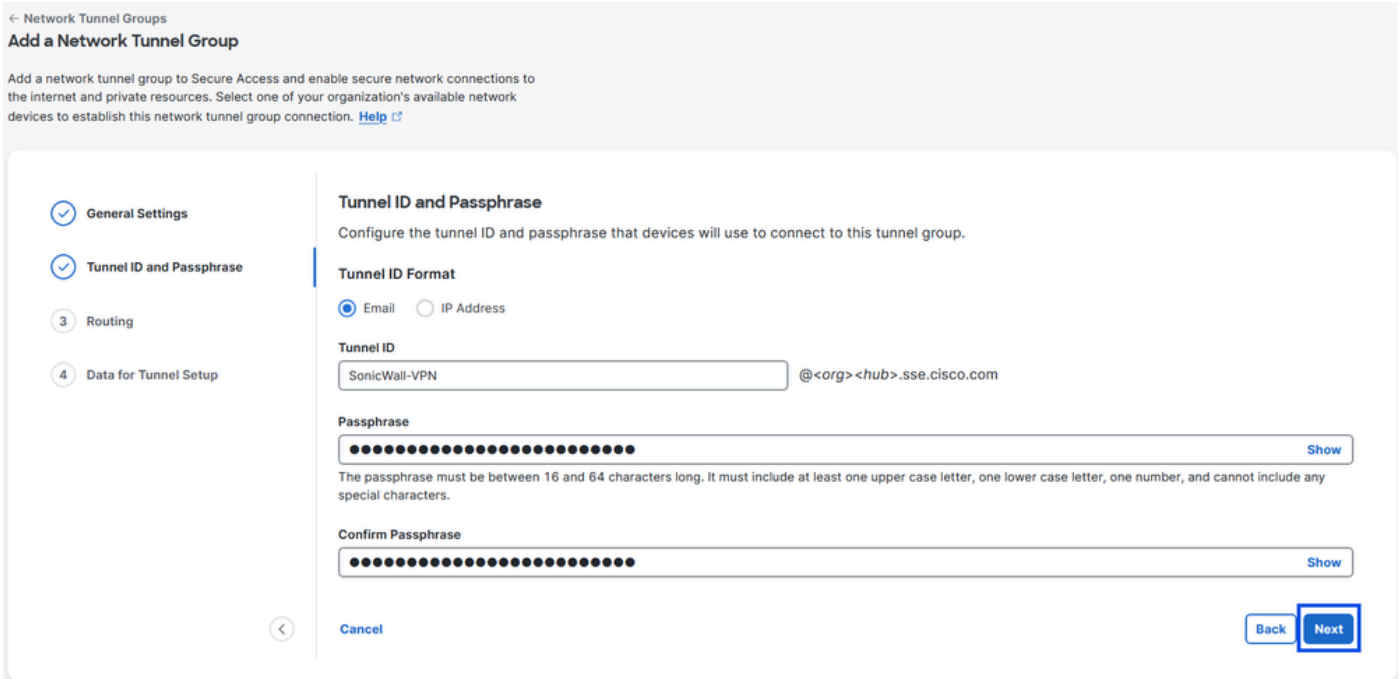


Acceso seguro - Grupo de túnel de red - Configuración general

---

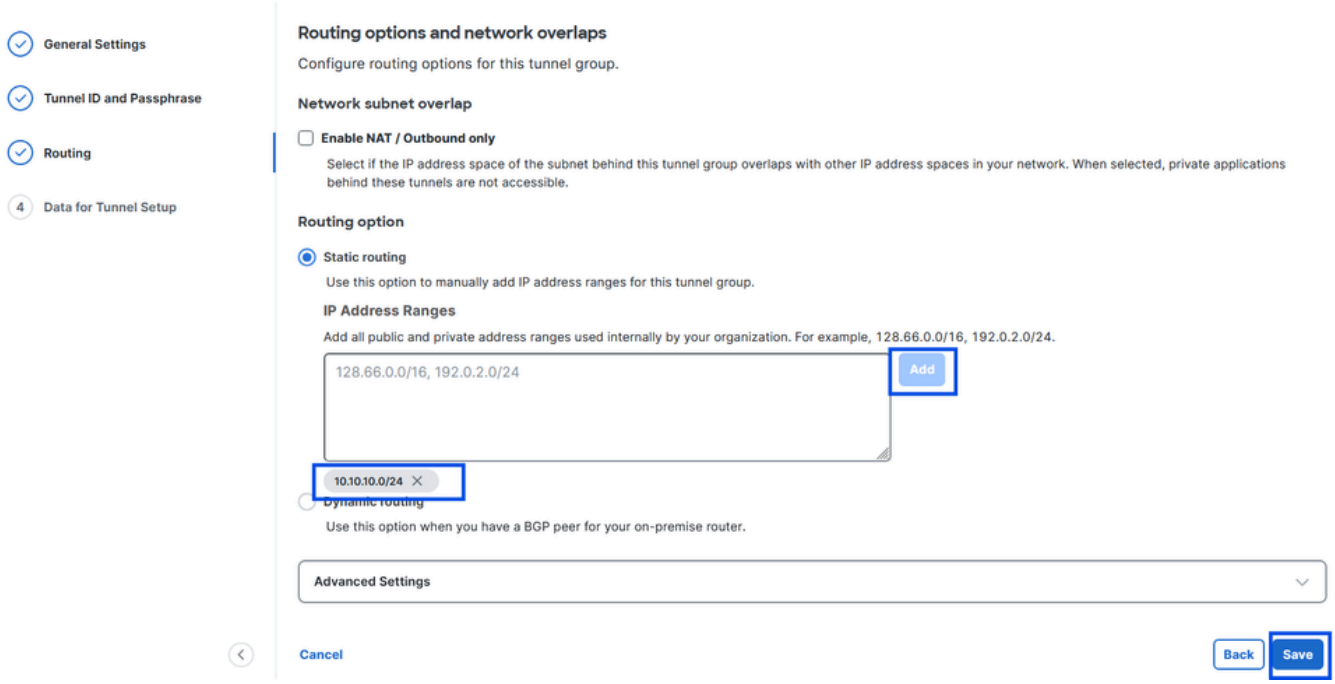
Nota: Seleccione la región más cercana a la ubicación del firewall.

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



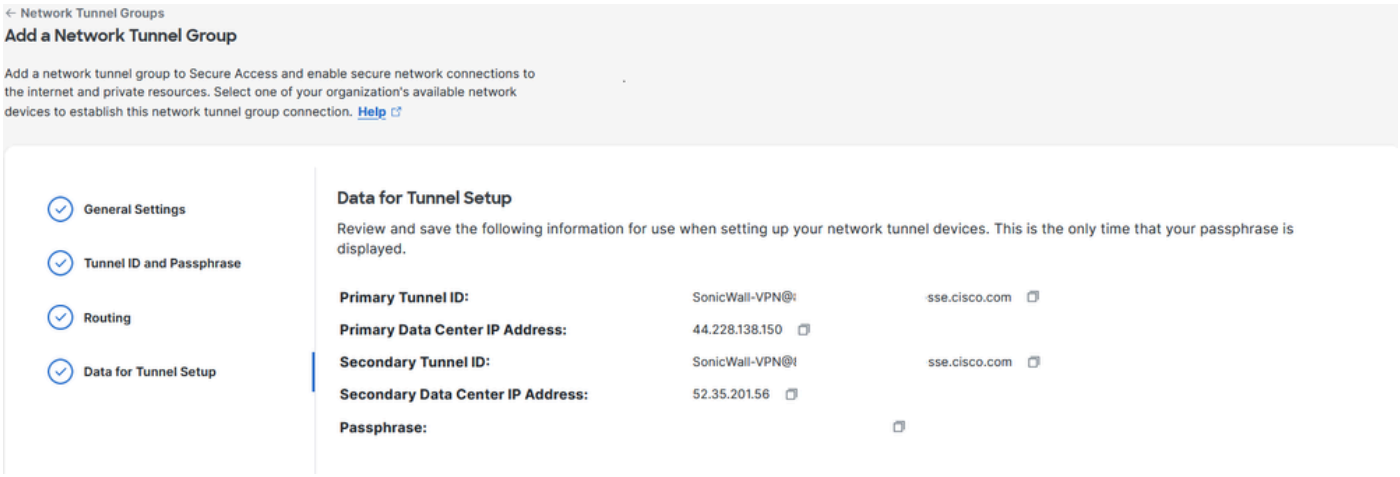
Acceso seguro: ID de túnel y frase de paso

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



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



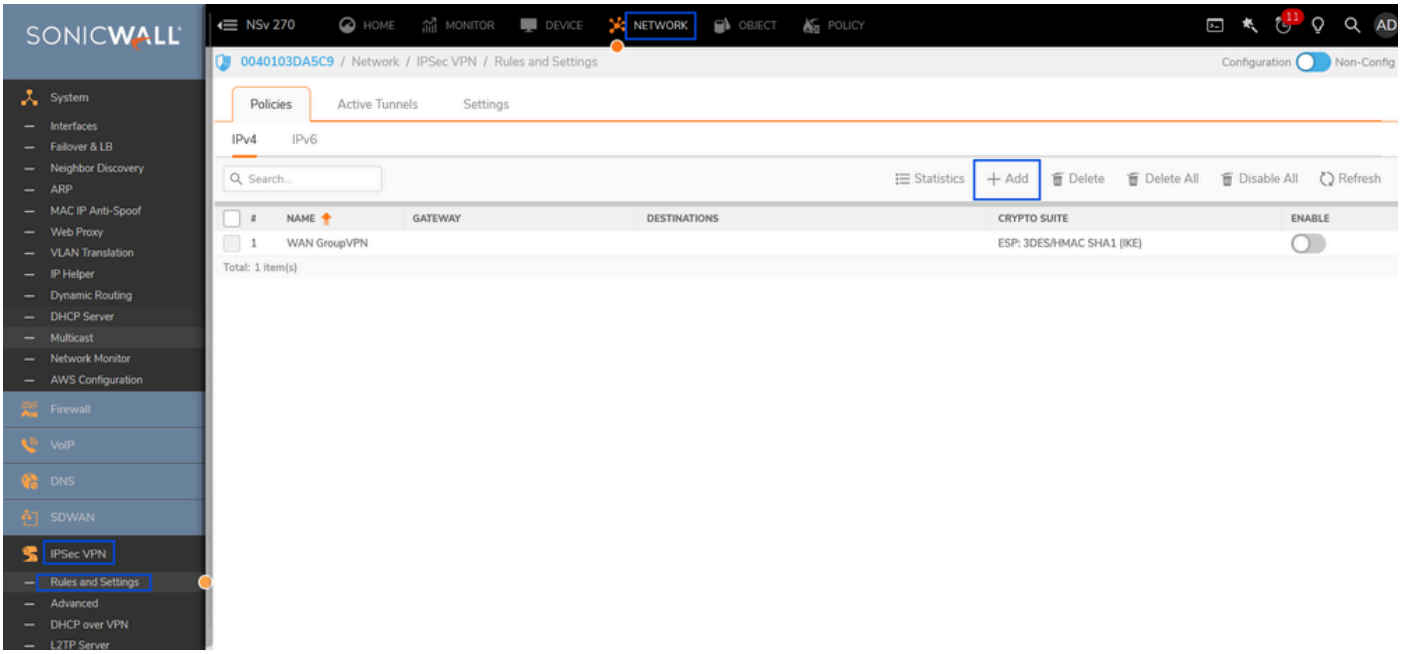
Secure Access - Datos para la configuración del túnel

Configuración del túnel en Sonicwall

Configuración del túnel: reglas y parámetros

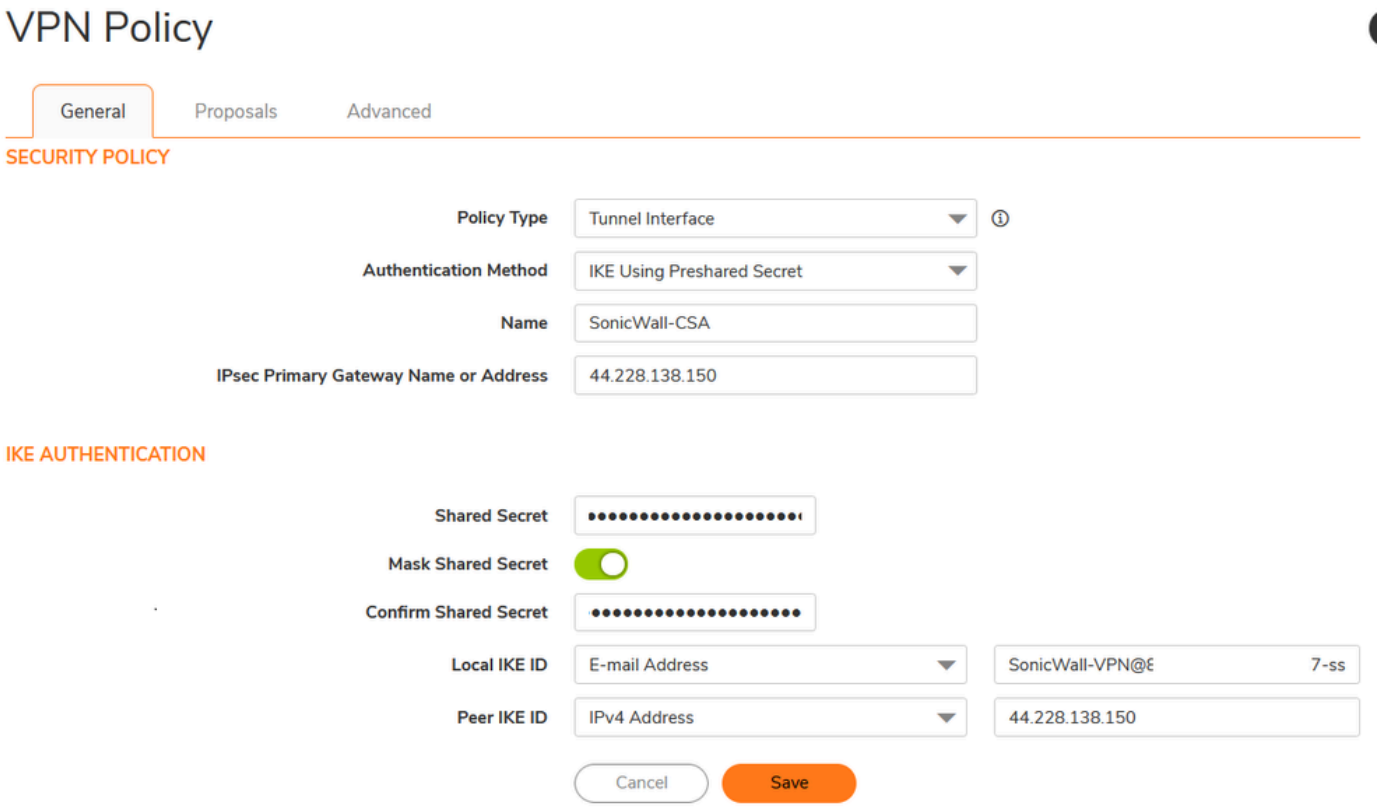
Vaya al panel de Sonicwall.

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



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

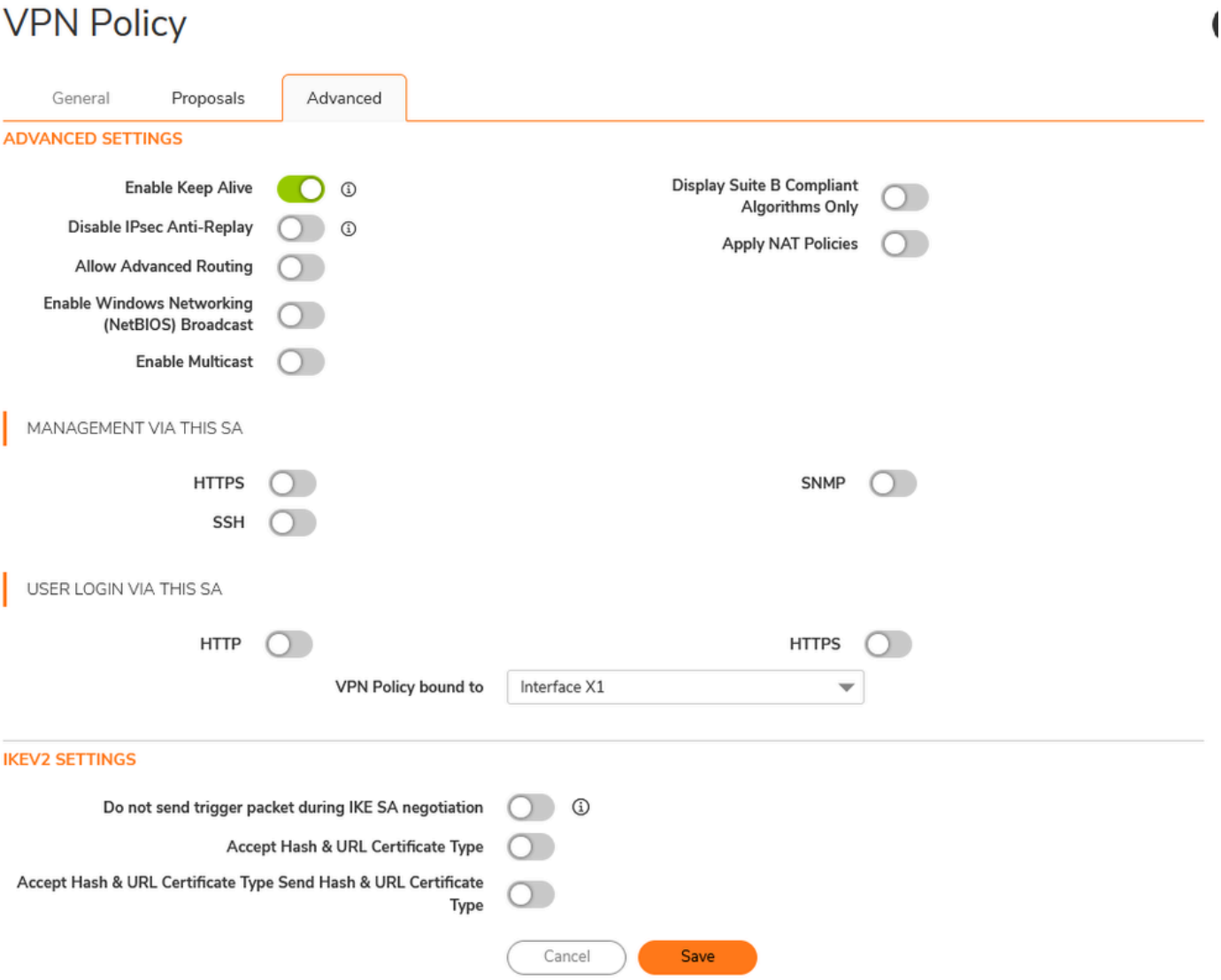
IKE (PHASE 1) PROPOSAL

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

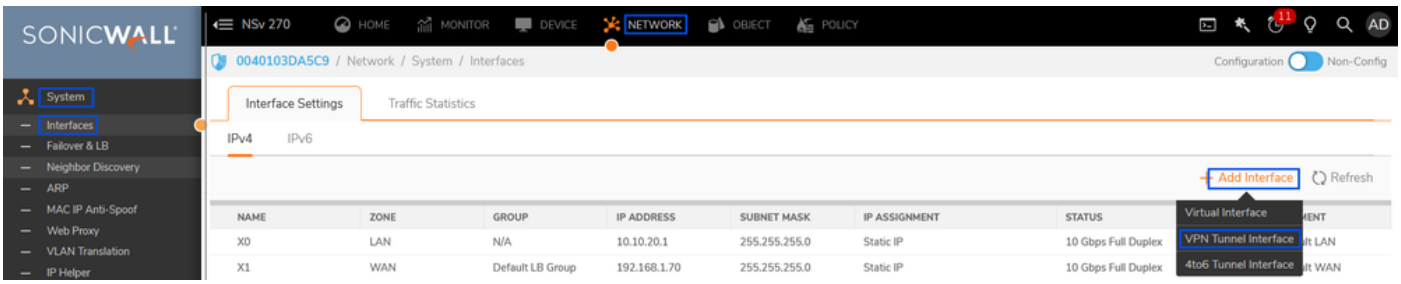


- Haga clic en Guardar

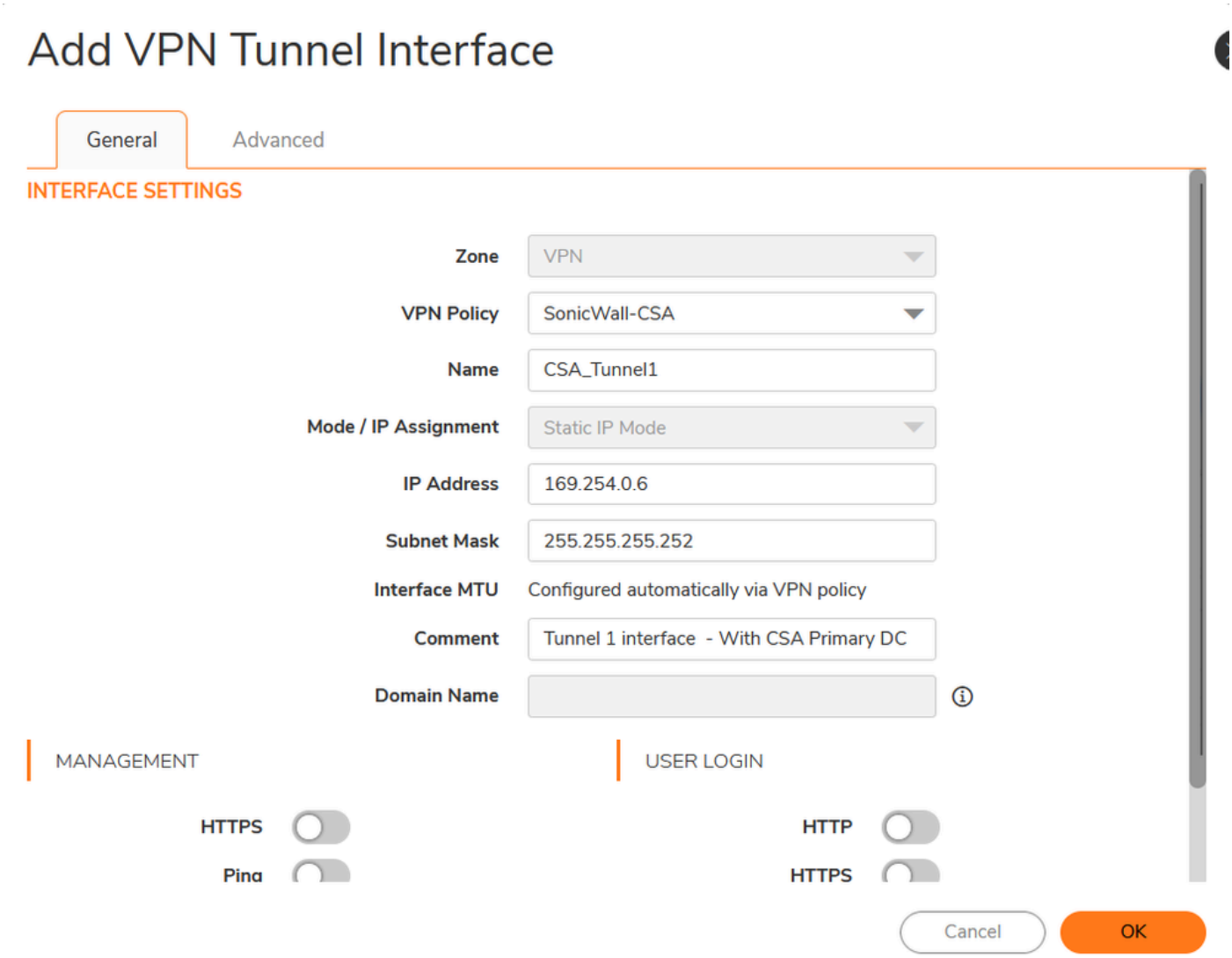
Agregar interfaz de túnel VPN

Vaya al panel de Sonicwall.

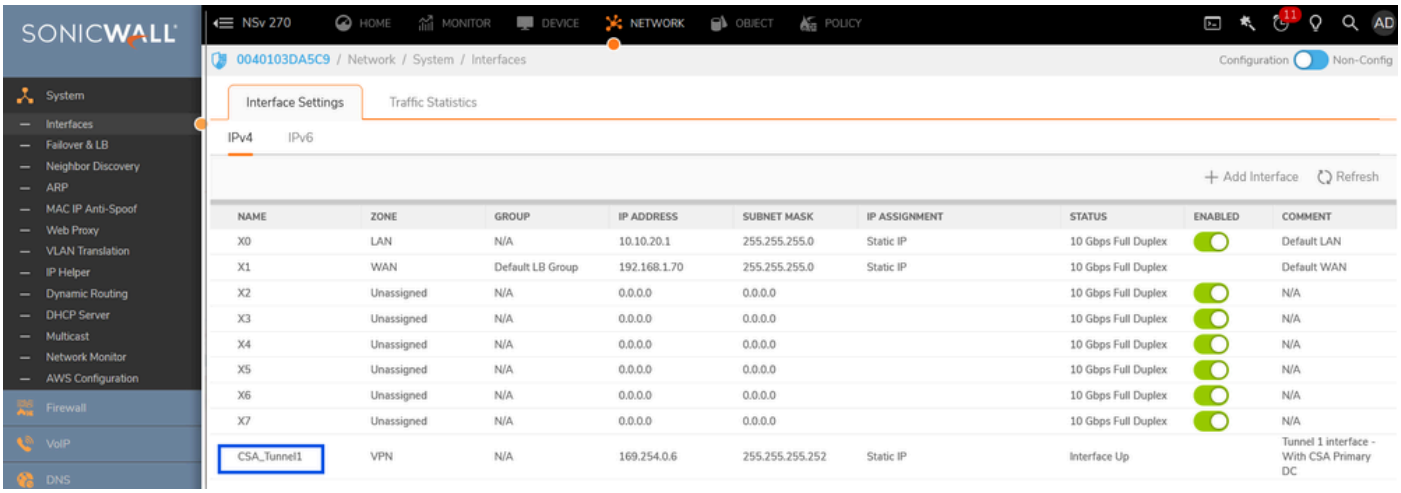
- Network > System > Interface
- Haga clic en + Agregar interfaz
- Seleccione la interfaz de túnel VPN



Sonicwall - Interfaces



- Haga clic en OK (Aceptar).

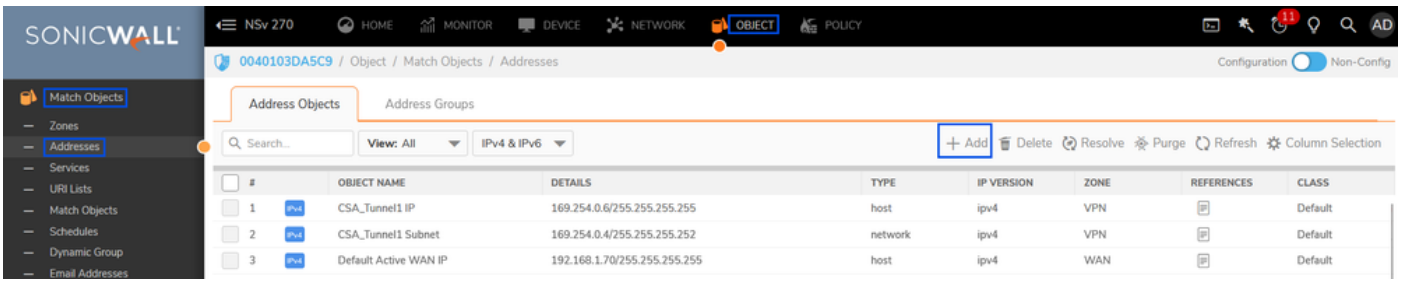


Sonicwall - Interfaces - Interfaz de túnel VPN

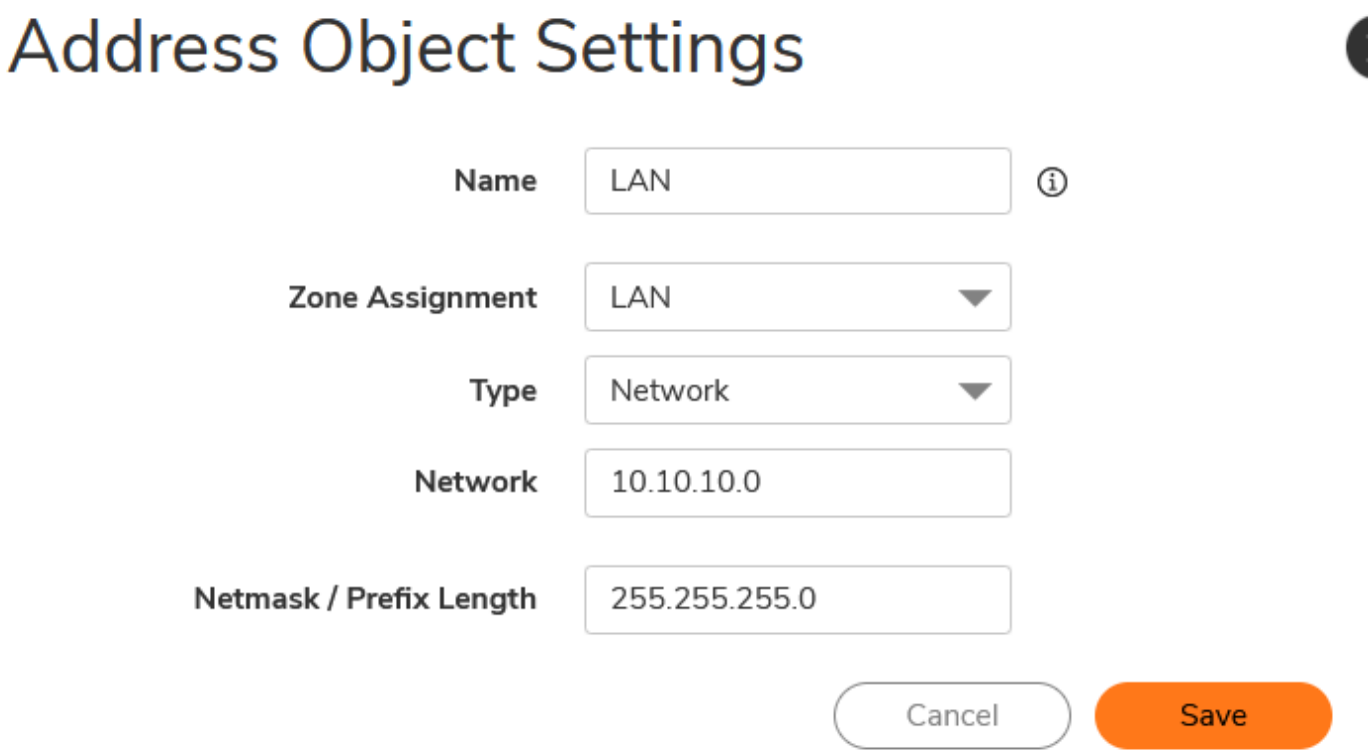
Agregar objeto y grupos de red

Vaya al panel de Sonicwall.

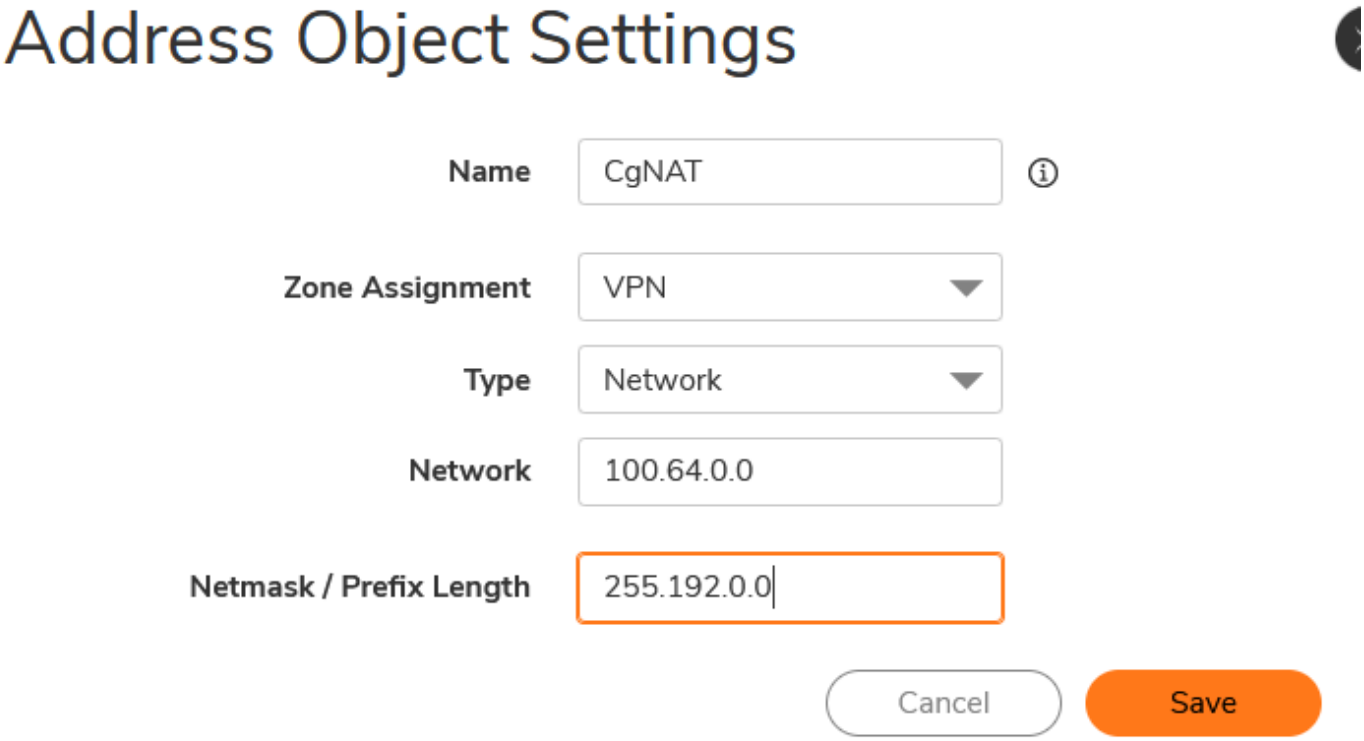
- Objeto > Coincidir objetos >Direcciones
- Objetos de dirección
- Haga clic en +Agregar



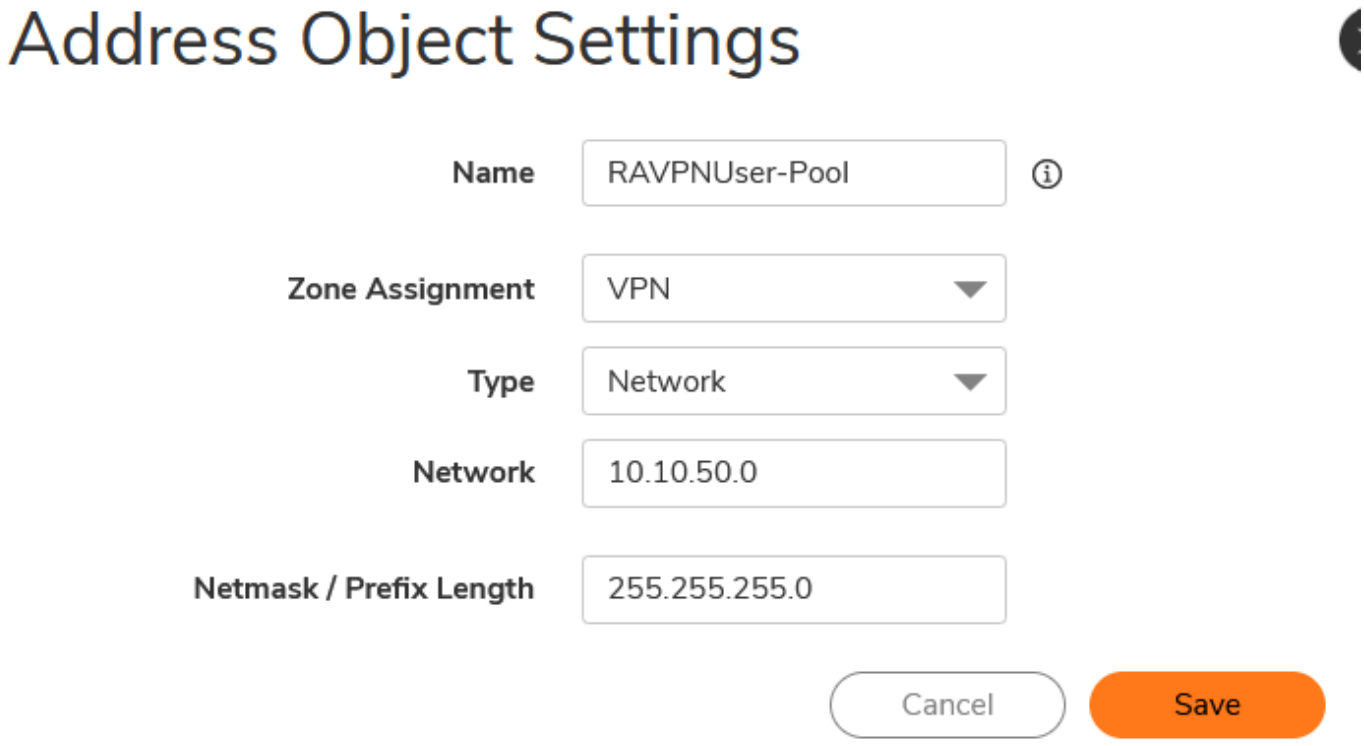
Sonicwall - Objeto- Objetos de dirección



- Haga clic en Save (Guardar).

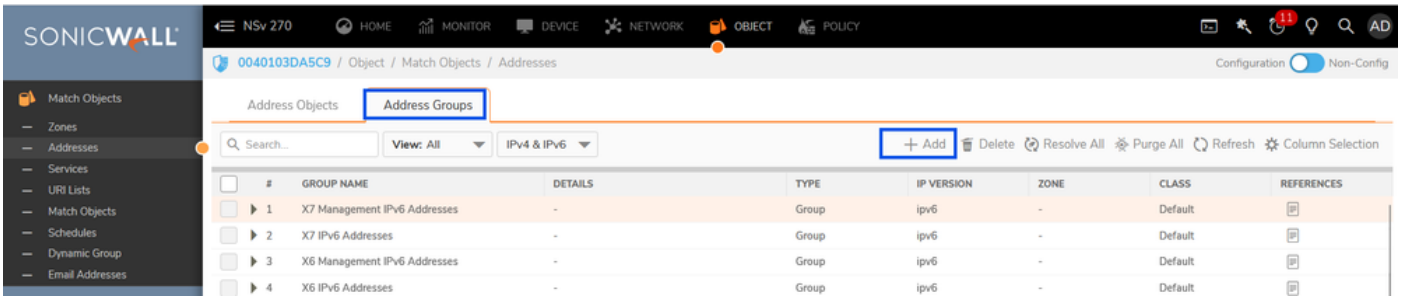


- Haga clic en Save (Guardar).

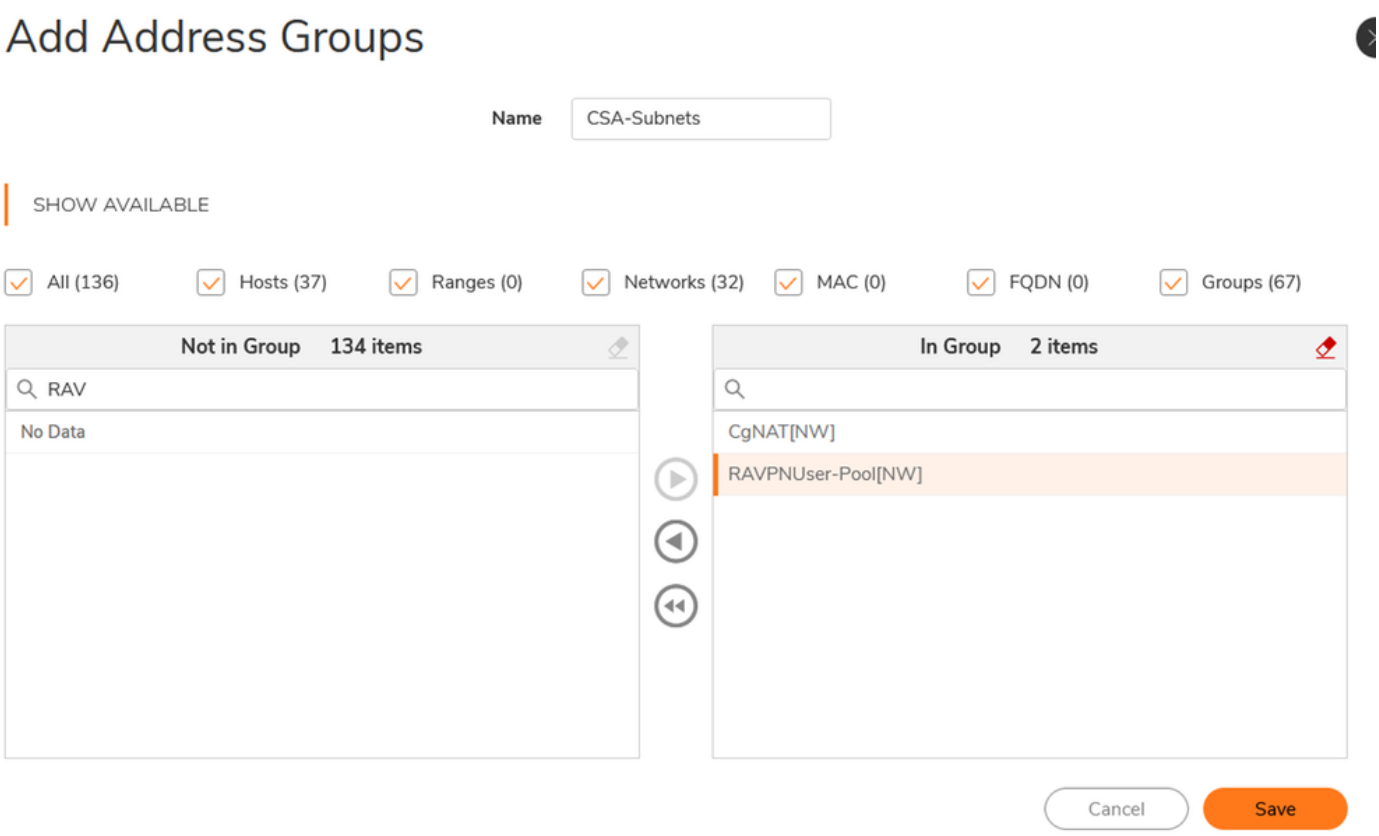


- Haga clic en Save (Guardar).

- 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

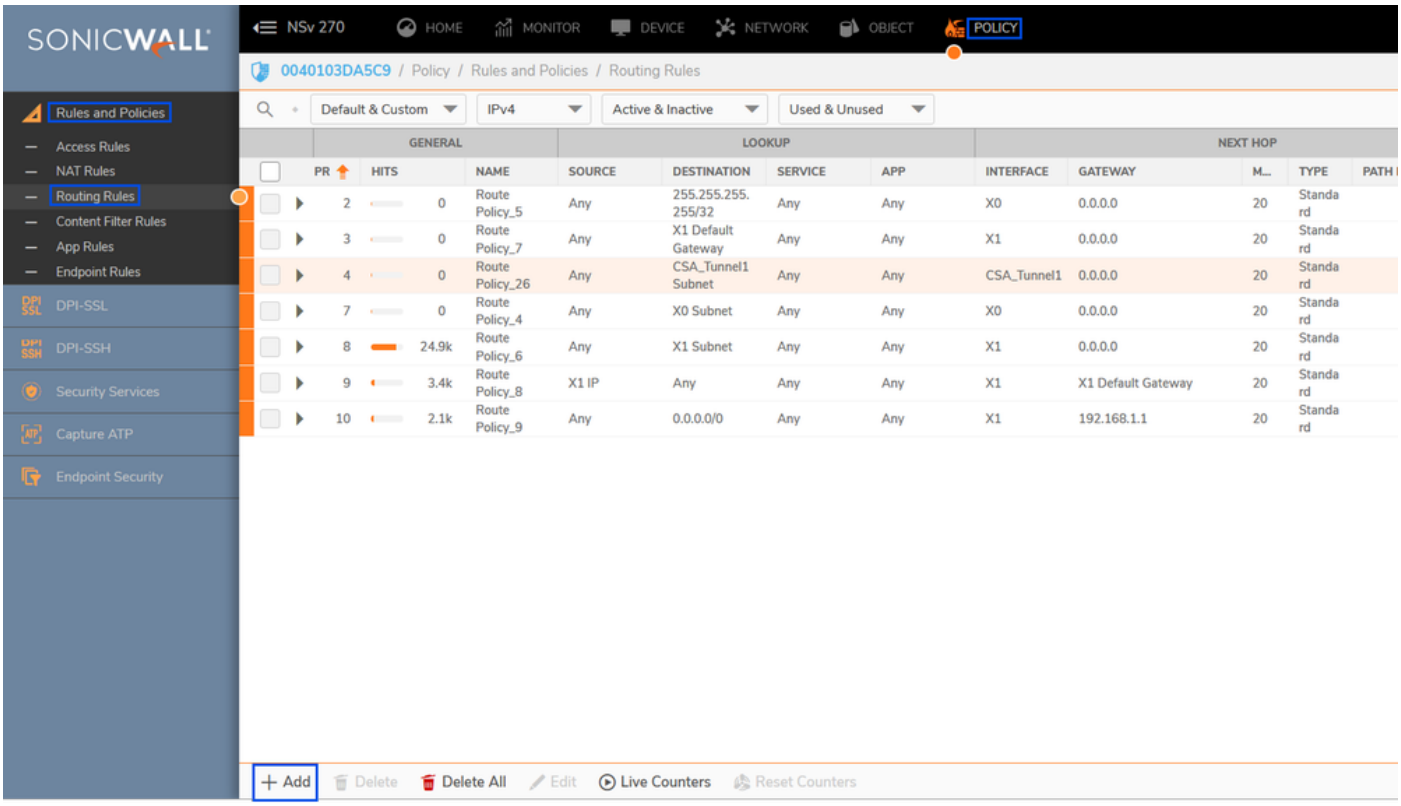


- Haga clic en Save (Guardar).

Agregar ruta

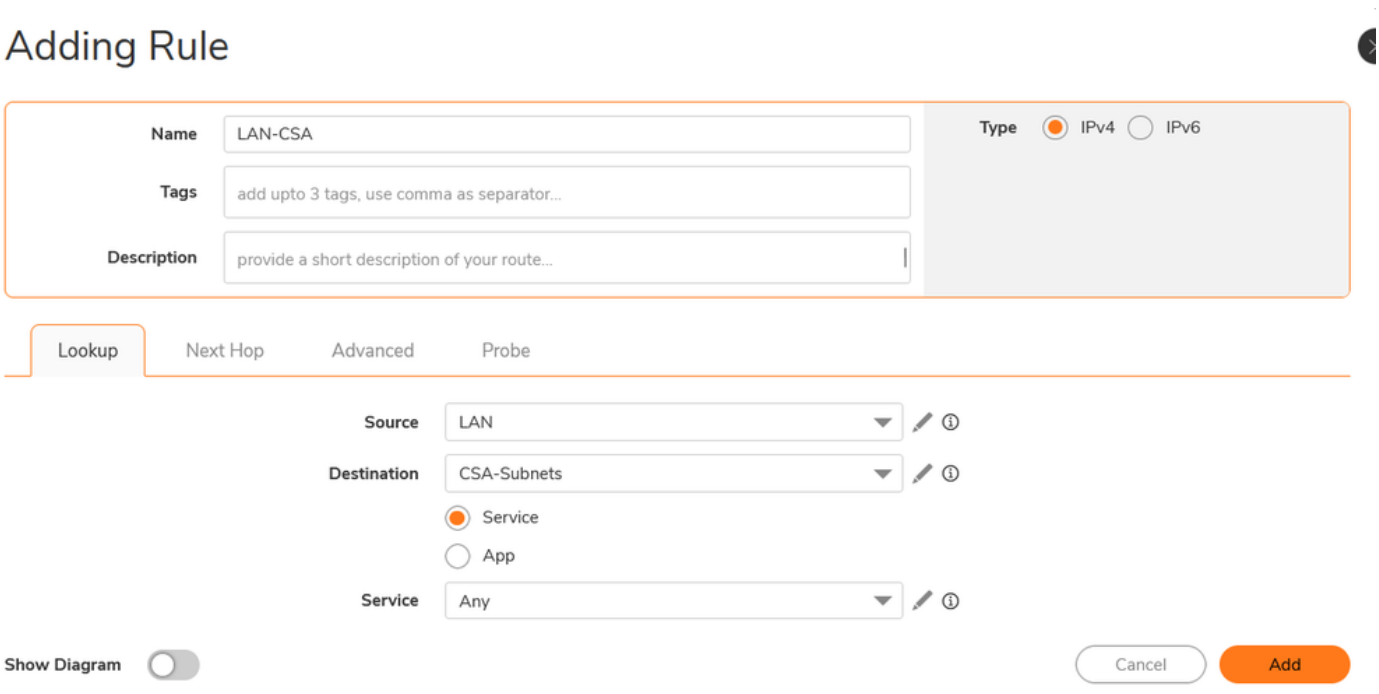
Vaya al panel de Sonicwall.

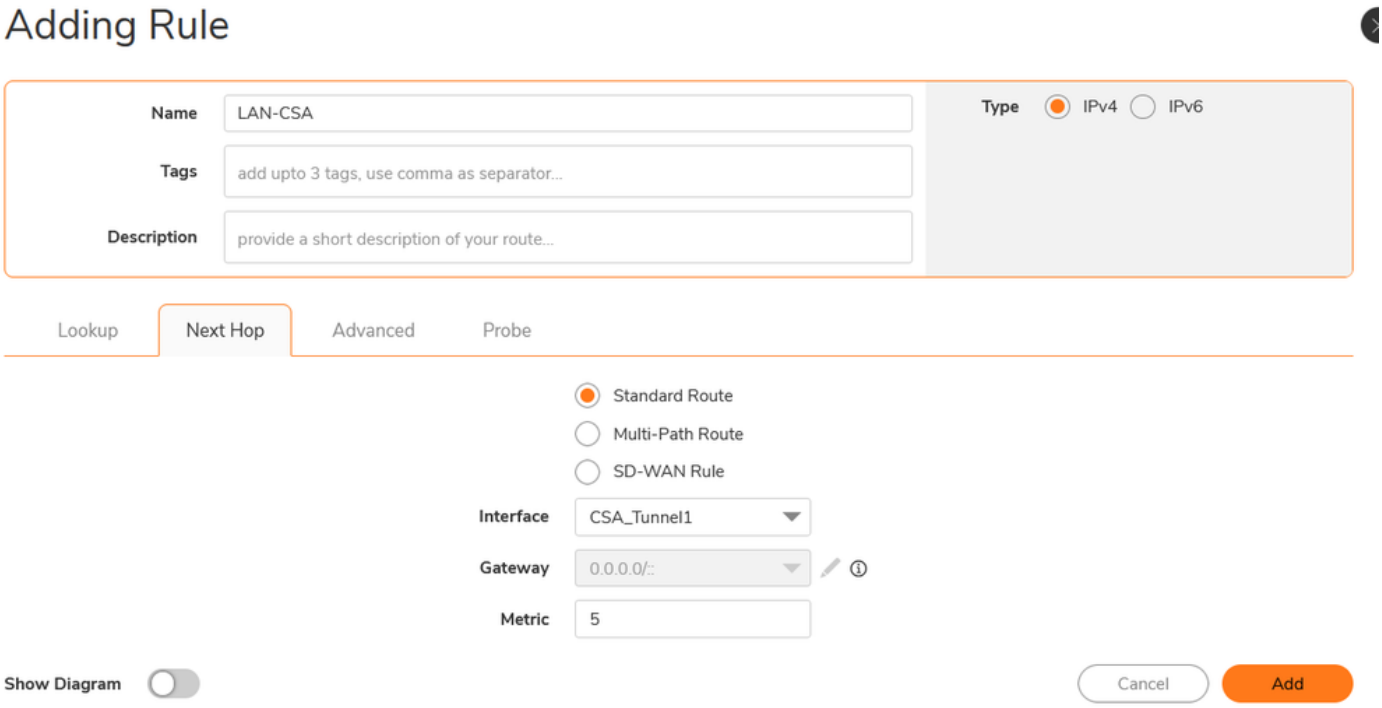
- Directiva > Reglas y políticas > Reglas de enrutamiento
- Haga clic en + Agregar



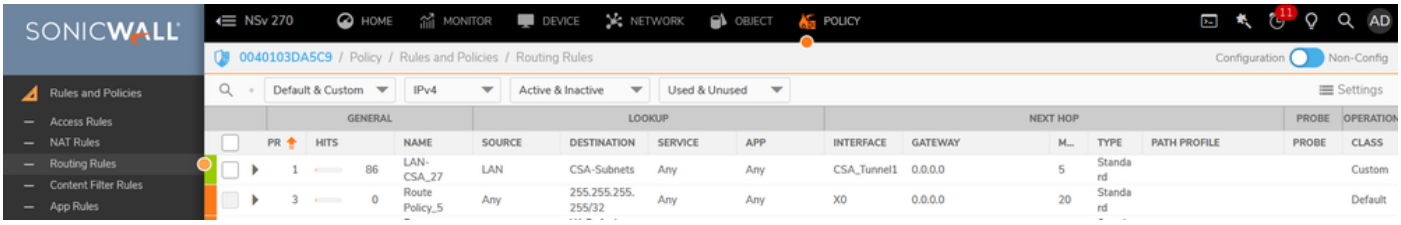
Sonicwall - Reglas de enrutamiento

- Agregar regla de enrutamiento





- Haga clic en + Agregar

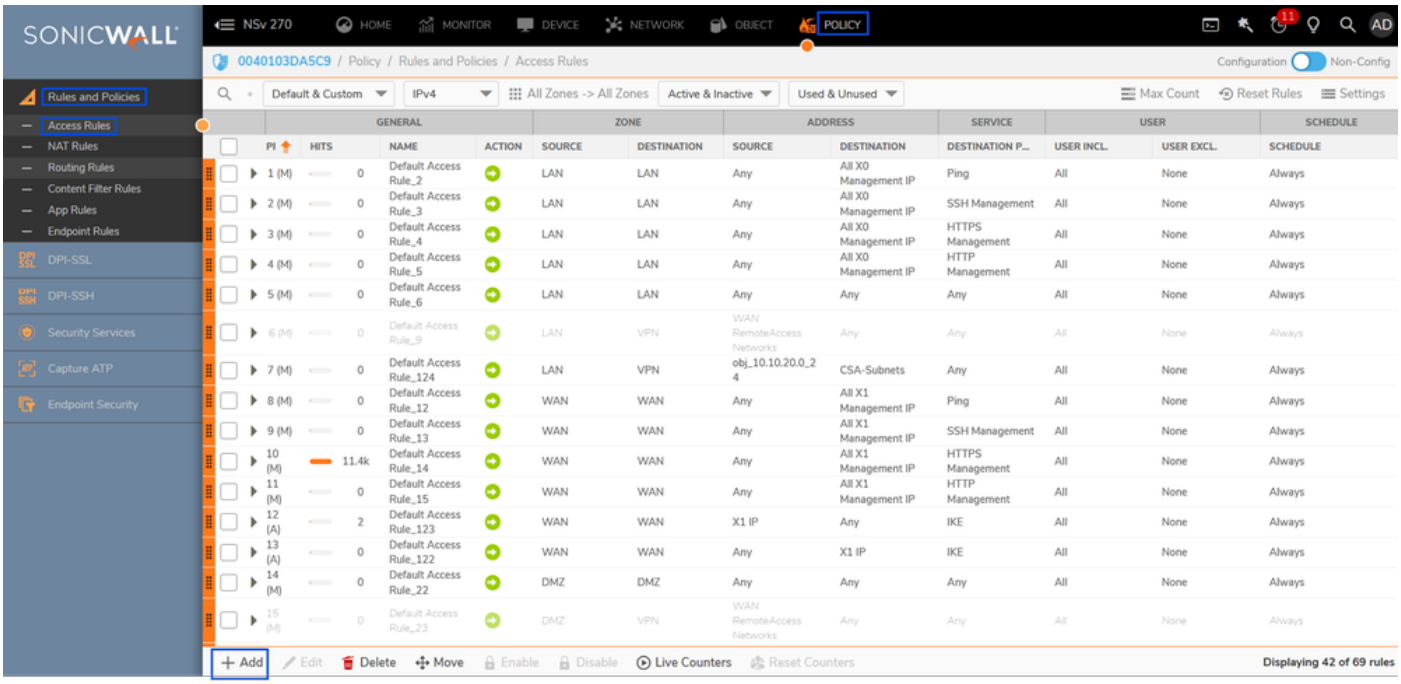


Sonicwall - Reglas de enrutamiento

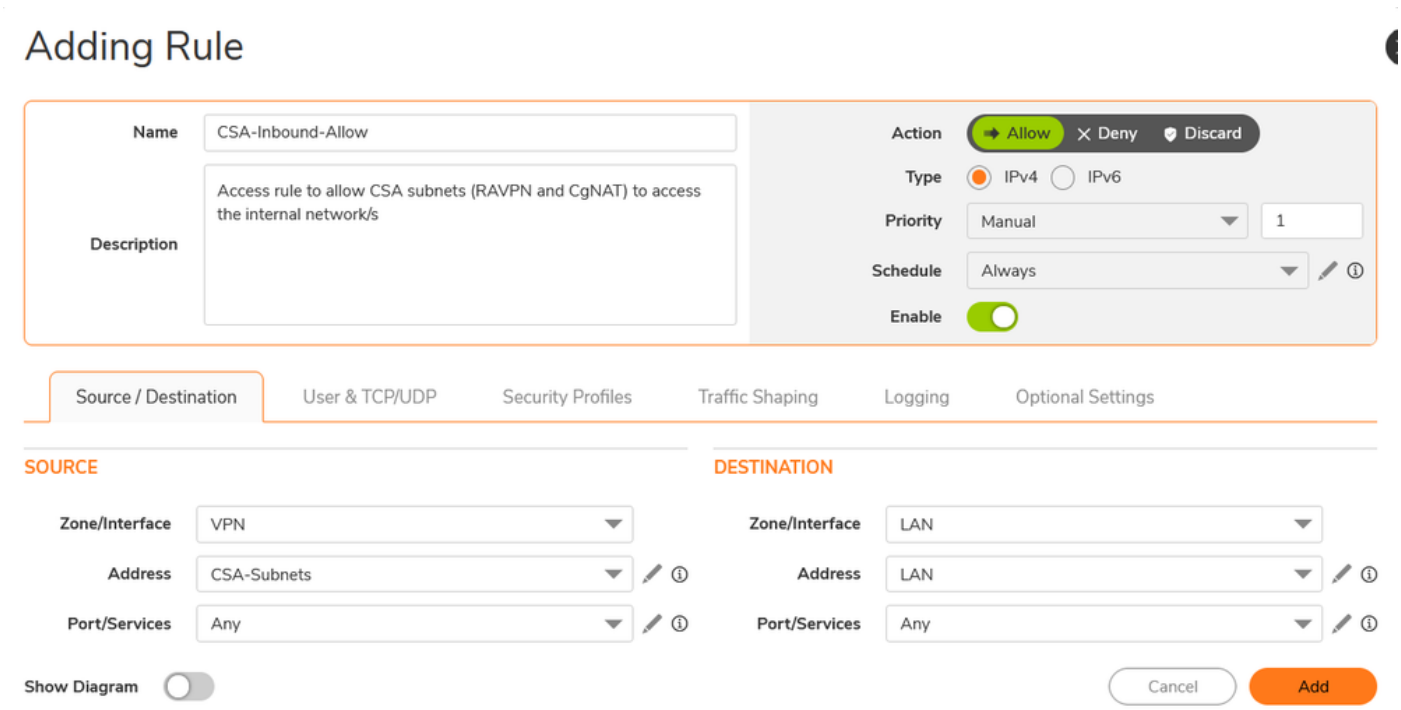
Agregar reglas de acceso

Vaya al panel de Sonicwall.

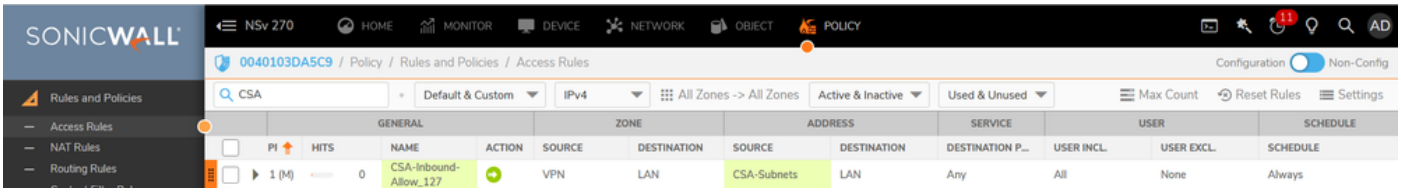
- Directiva > Reglas y políticas > Reglas de acceso
- Haga clic en + Agregar



Sonicwall - Reglas de acceso



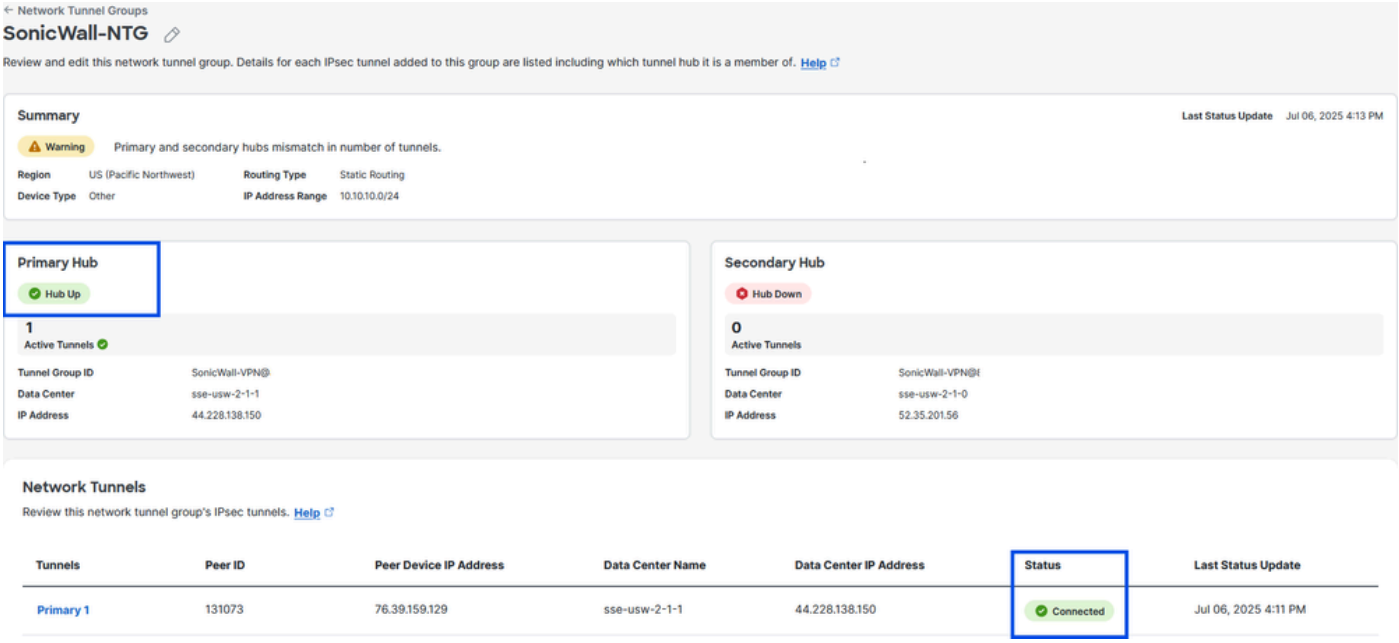
- Haga clic en +Agregar



Sonicwall - Reglas de acceso

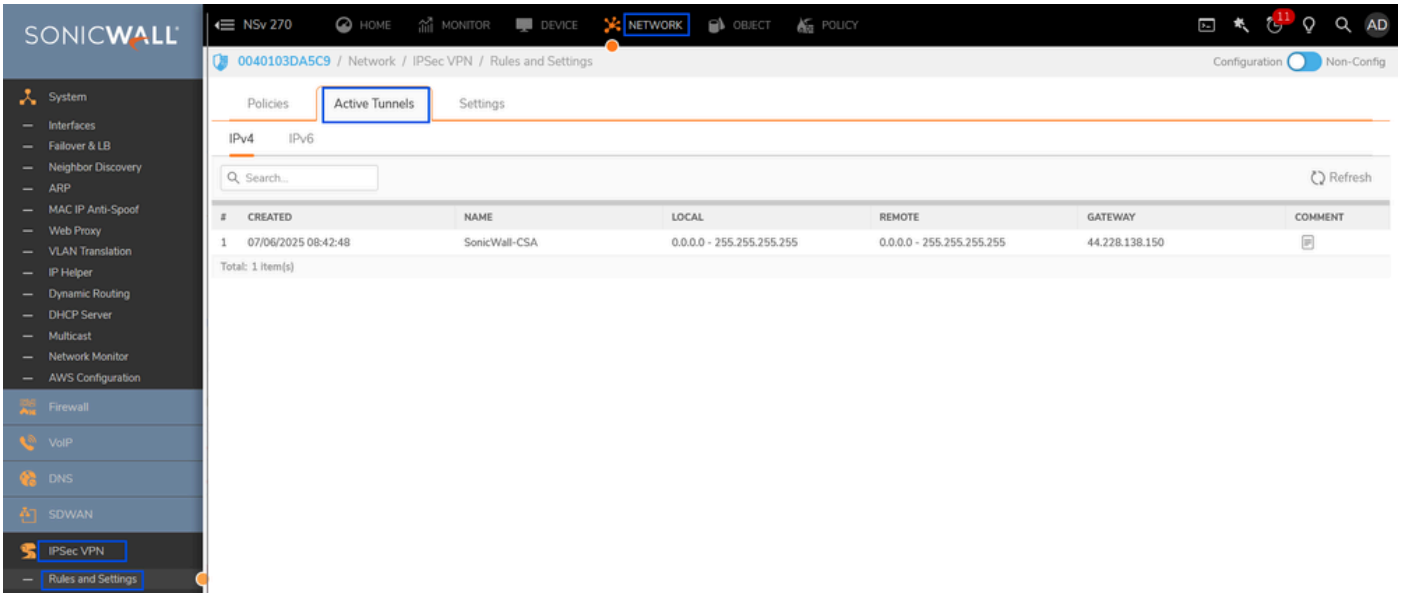
Verificación

- Estado del túnel en acceso seguro



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

- Estado del túnel en el firewall Sonicwall



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).