Configure o acesso seguro com o firewall Sonicwall

Contents

Introdução

Pré-requisitos

- Requisitos
- Componentes Utilizados
- Informações de Apoio
- Diagrama de Rede

Configurar

- Configurar o Network Tunnel Group (VPN) no acesso seguro
- Configure o túnel no Sonicwall
- Configure o túnel - Rules and Settings
- Adicionar interface de túnel VPN
- Adicionar objetos e grupos de rede
- Adicionar rota
- Adicionar regras de acesso

Verificar

Troubleshooting

- PC do usuário
- Acesso seguro
- Sonicwall

Informações Relacionadas

Introdução

Este documento descreve como configurar um túnel IPsec VTI entre o Secure Access e o firewall Sonicwall usando o roteamento estático.

Pré-requisitos

- Configurar Provisionamento de Usuário
- Configuração de Autenticação ZTNA SSO
- Configurar o acesso seguro da VPN de acesso remoto

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Firewall Sonicwall (NSv270 - SonicOSX 7.0.1)

- Acesso seguro
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA
- ZTNA sem cliente

Componentes Utilizados

As informações neste documento são baseadas em:

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Diagrama de Rede

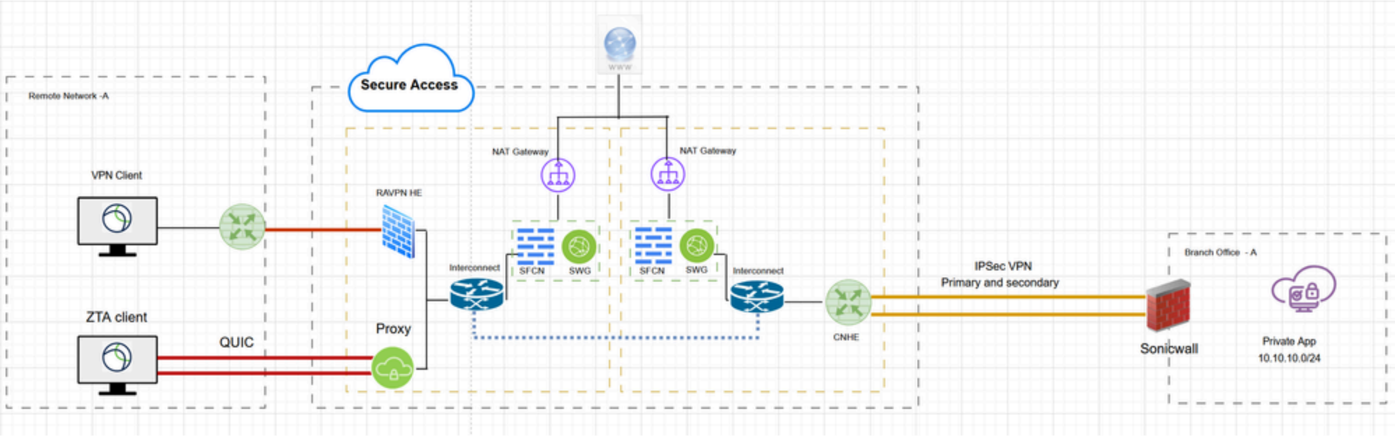


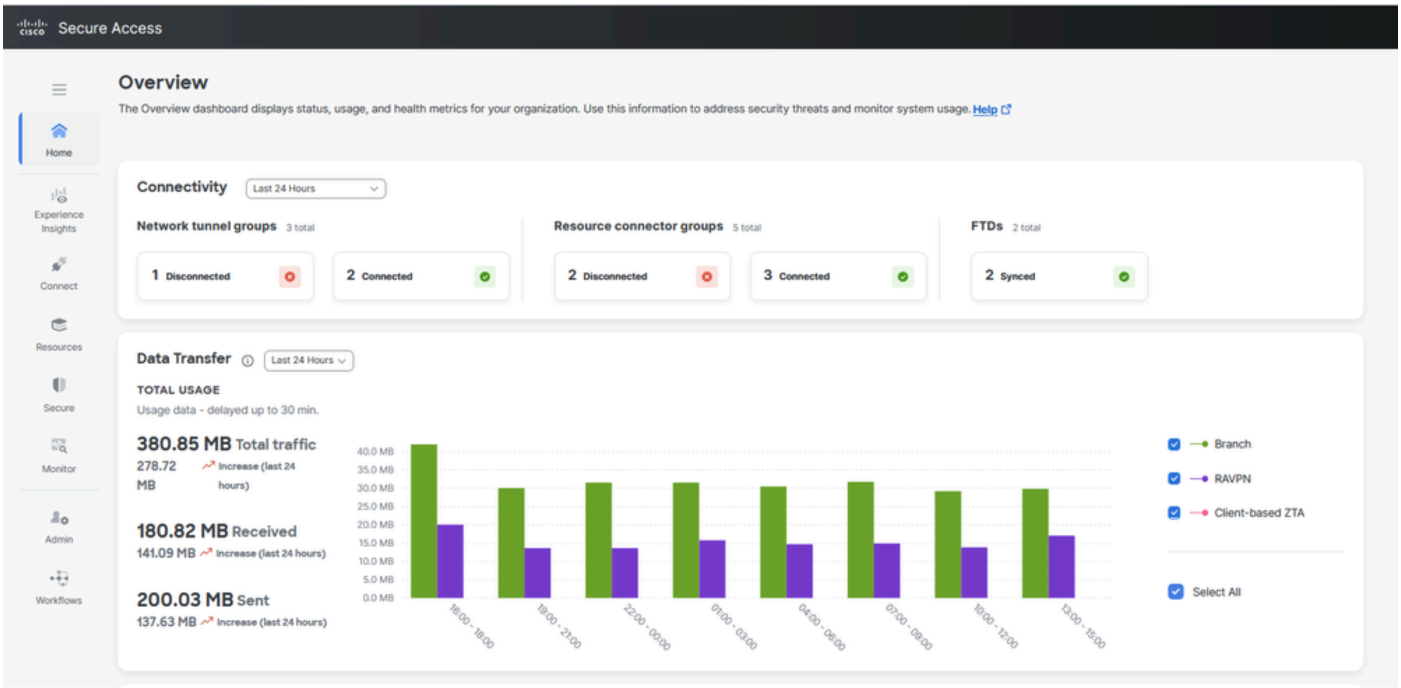
Diagrama de Rede

Configurar

Configurar o Network Tunnel Group (VPN) no acesso seguro

Para configurar o túnel VPN entre o Secure Access e o Sonicwall

- Navegue até o portal admin do Secure Access



Overview

The Overview dashboard displays status, usage, and health metrics for your organization. Use this information to address security threats and monitor system usage. Help

Connectivity — Last 24 Hours

Network tunnel groups 3 total: 1 Disconnected; 2 Connected

Resource connector groups 5 total: 2 Disconnected; 3 Connected

FTDs 2 total: 2 Synced

Data Transfer — Last 24 Hours

TOTAL USAGE

Usage data - delayed up to 30 min.

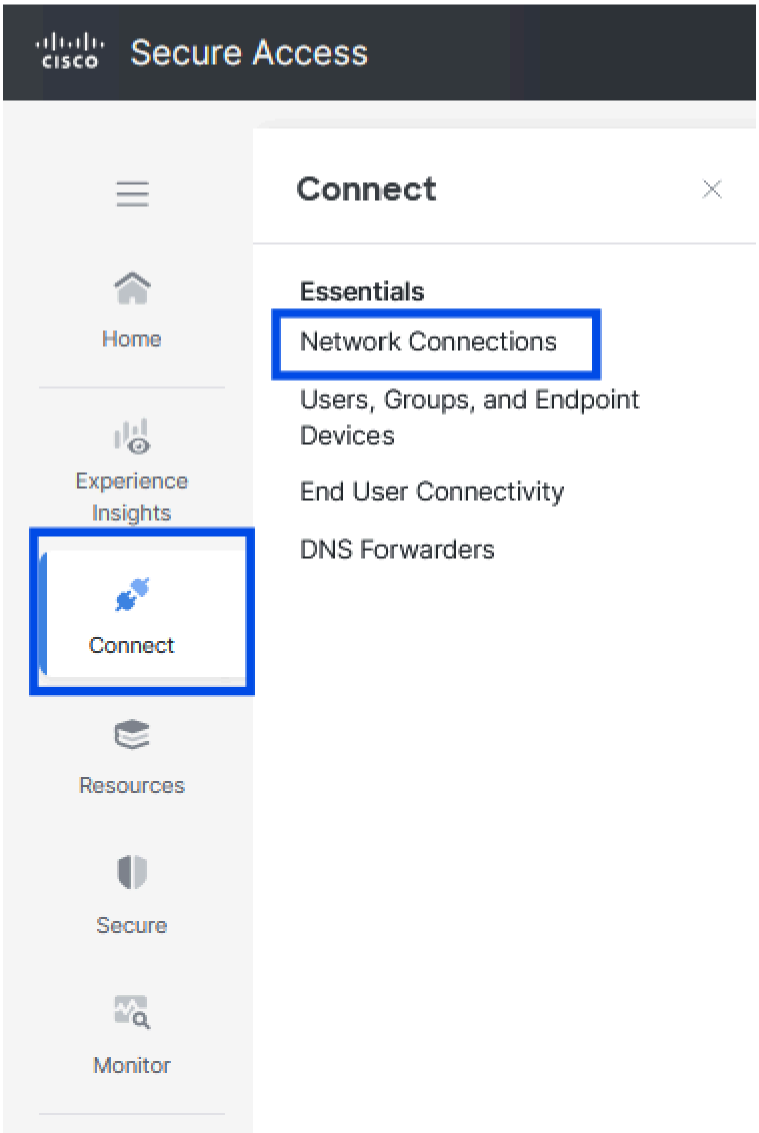
380.85 MB Total traffic
278.72 MB Increase (last 24 hours)

180.82 MB Received
141.09 MB Increase (last 24 hours)

200.03 MB Sent
137.63 MB Increase (last 24 hours)

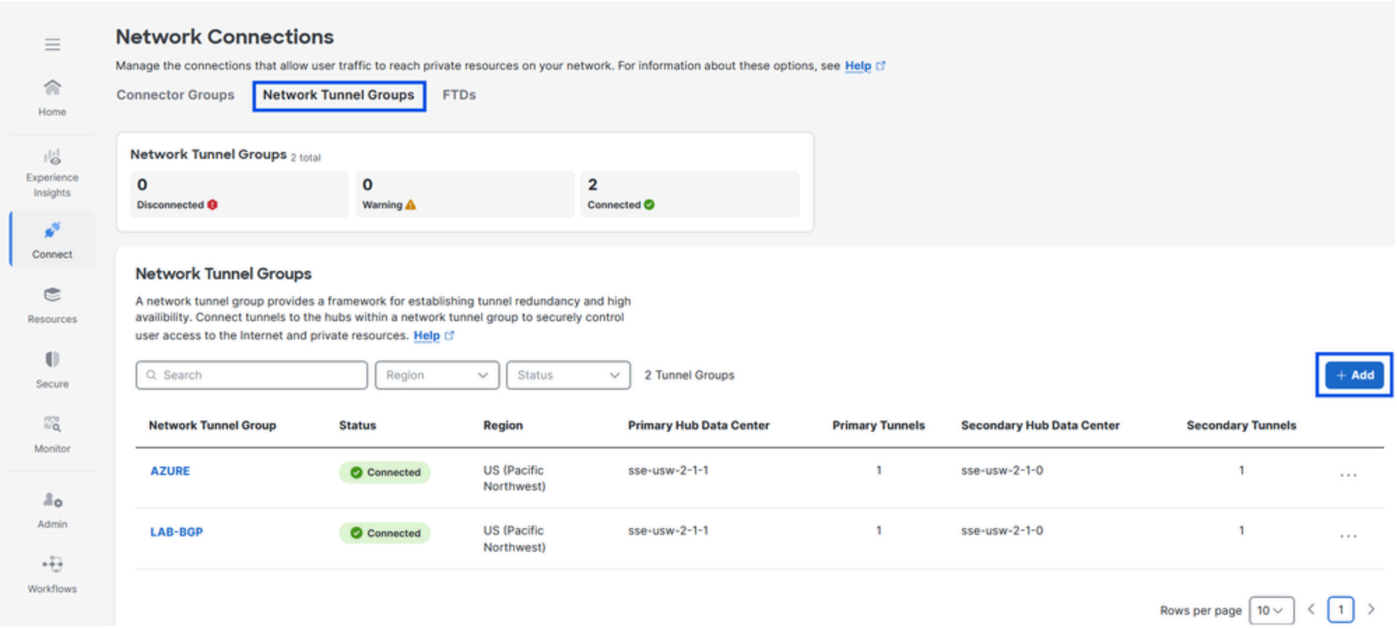
Acesso seguro - Página principal

- Clique em Connect > Network Connections



Acesso seguro - Conexões de rede

- Em Network Tunnel Groups clique em + Add



Network Connections

Manage the connections that allow user traffic to reach private resources on your network. For information about these options, see Help

Network Tunnel Groups 2 total

0 Disconnected

0 Warning

2 Connected

Network Tunnel Groups

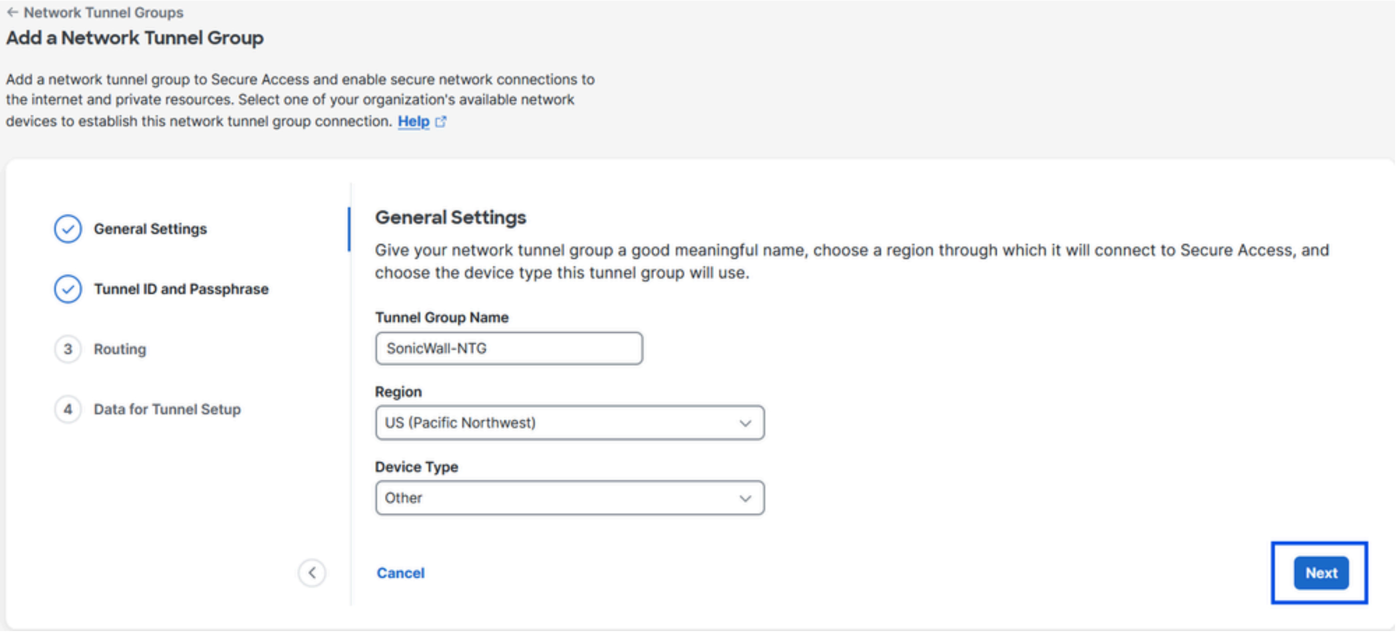
A network tunnel group provides a framework for establishing tunnel redundancy and high availibility. Connect tunnels to the hubs within a network tunnel group to securely control user access to the Internet and private resources. Help

2 Tunnel Groups

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

Acesso seguro - Grupos de túnel de rede

- Configure o nome do grupo de túneis , região e tipo de dispositivo
- Clique em 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

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

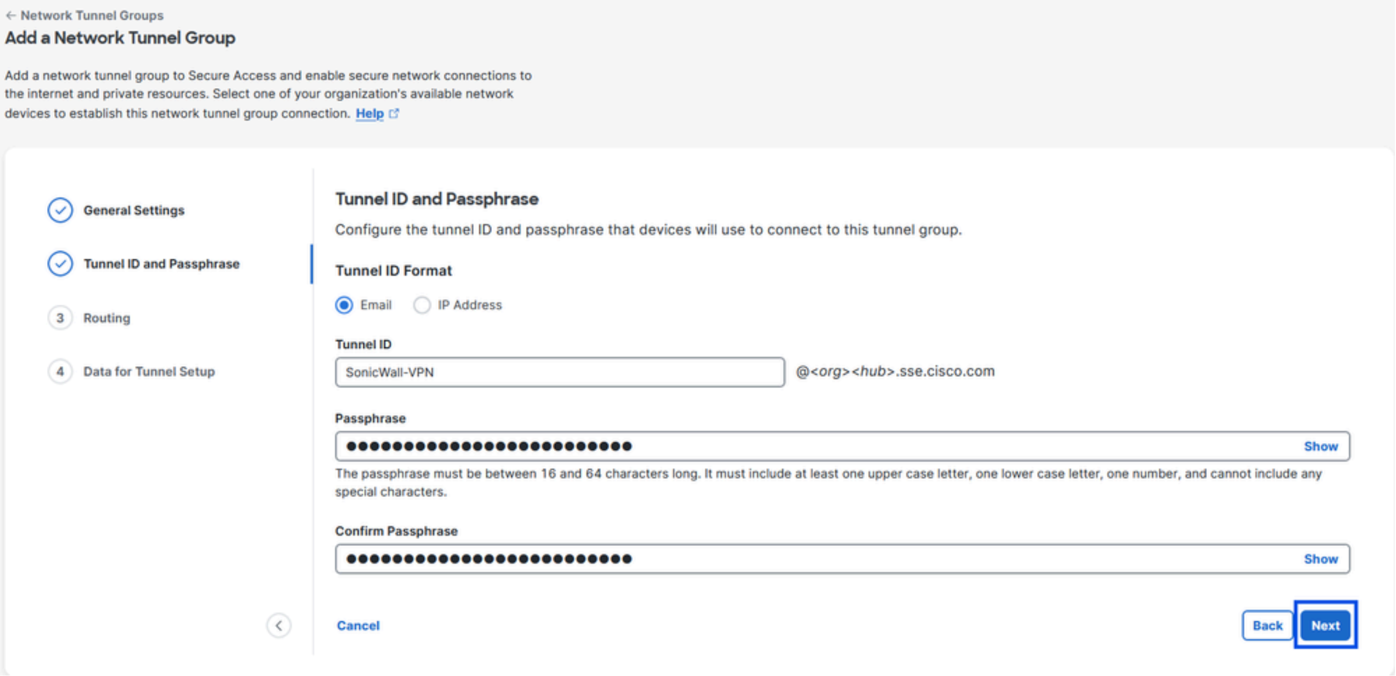
Region: US (Pacific Northwest)

Device Type: Other

Acesso seguro - Grupo de túneis de rede - Configurações gerais

Note: Escolha a região mais próxima ao local do firewall.

- Configure o formato de ID de túnel e a senha
- Clique em 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

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

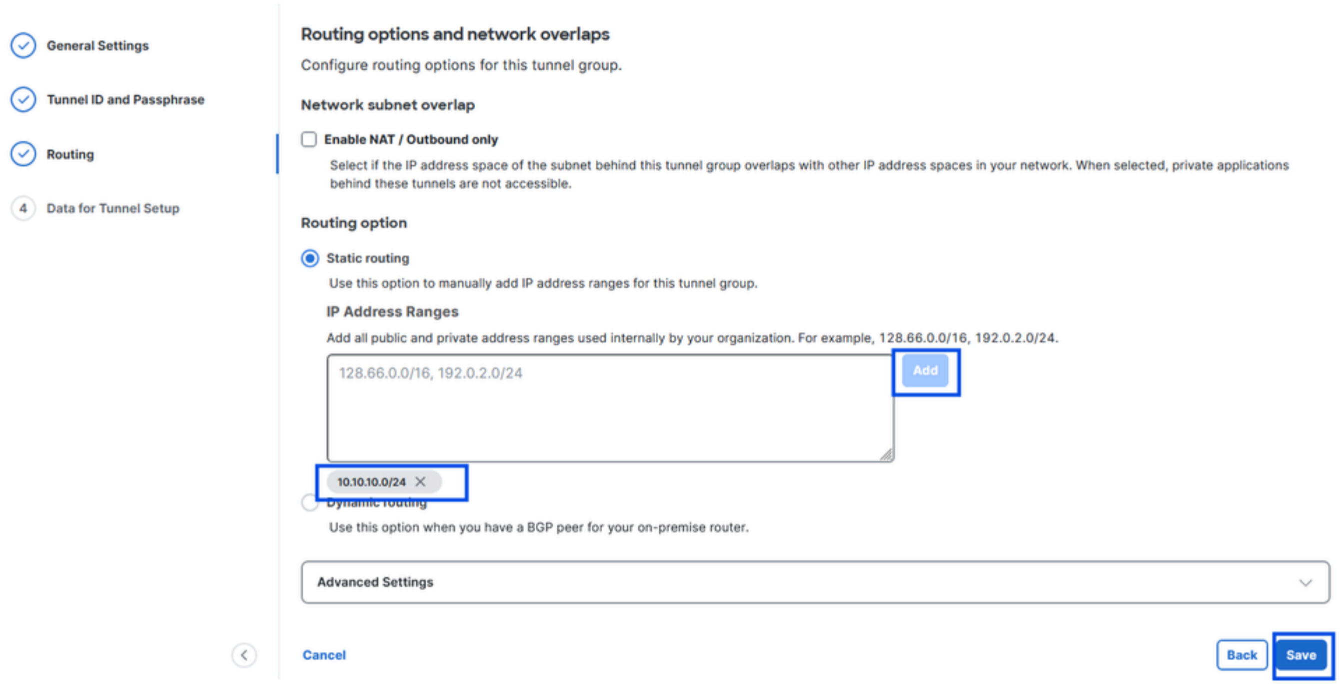
Passphrase: ●●●●●●●●●●●●●●●●●●●●●●●●●●

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: ●●●●●●●●●●●●●●●●●●●●●●●●●●

Acesso seguro - ID e senha do túnel

- Configure os intervalos de endereços IP, hosts ou sub-redes que você configurou em sua rede e deseja passar o tráfego através do Acesso Seguro
- Clique em Add
- Clique em Salvar



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 ✕

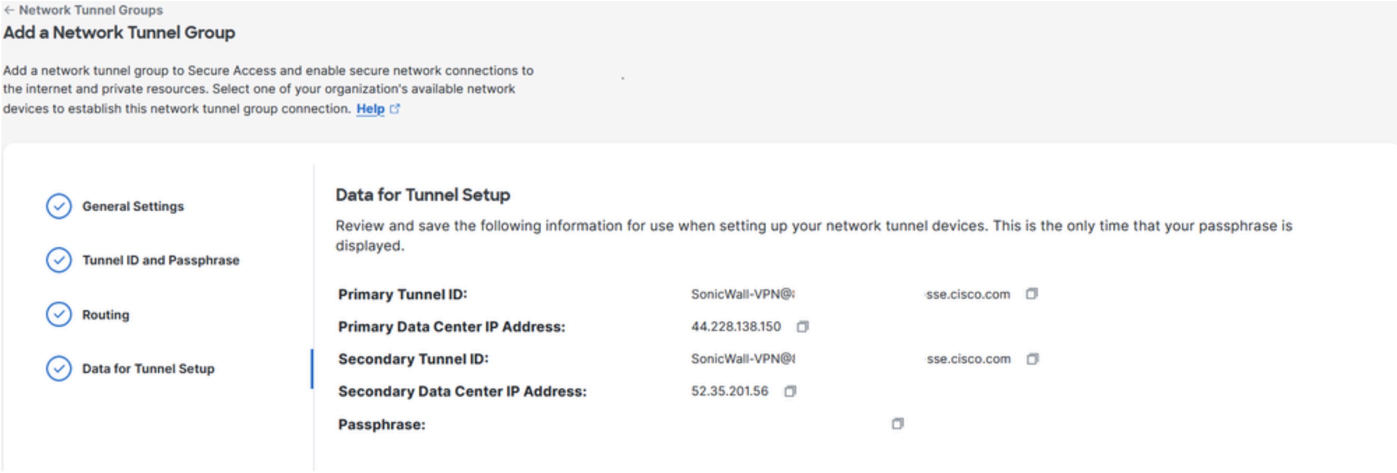
○ Dynamic routing

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

Advanced Settings

Acesso seguro - Grupos de túneis - Opções de roteamento

Depois de clicar em Save , as informações sobre o túnel serão exibidas. Salve essas informações para a próxima etapa da configuração



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.

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:	

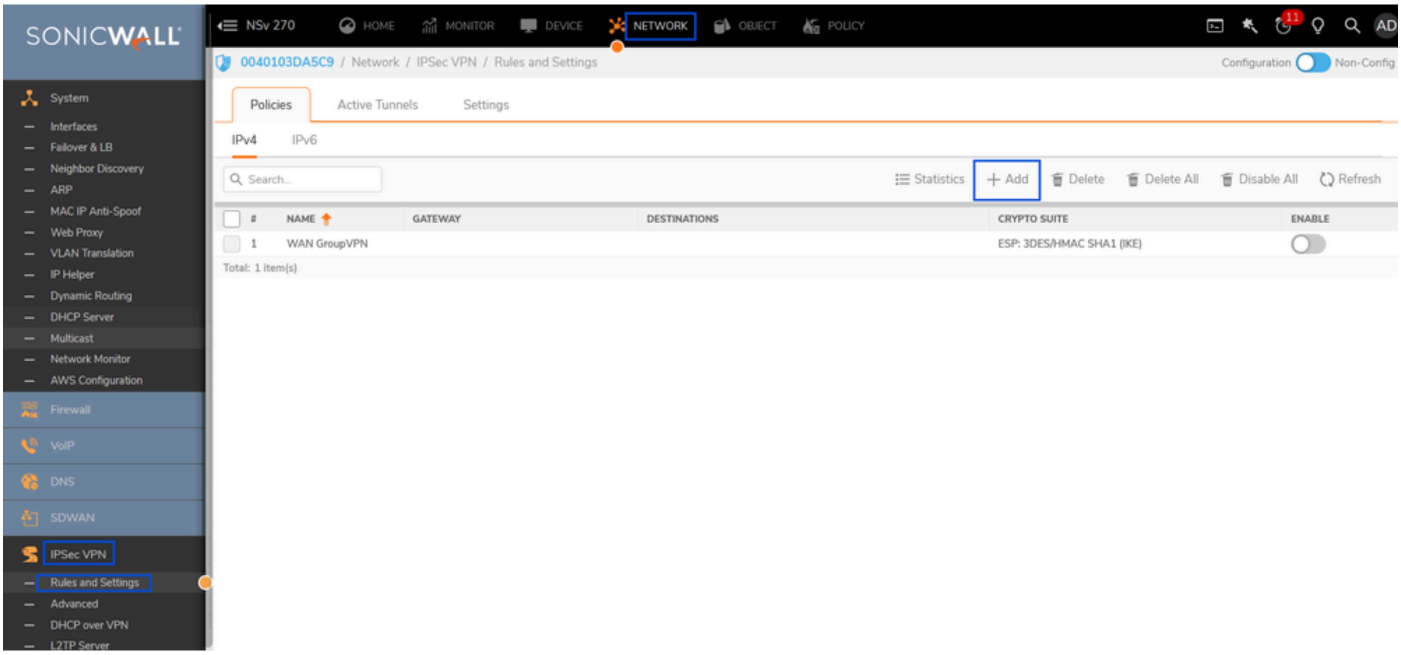
Acesso seguro - Configuração de dados para túnel

Configure o túnel no Sonicwall

Configure o túnel - Rules and Settings

Navegue até o Painel Sonicwall.

- Rede > VPN IPsec > Regras e Configurações
- Clique em + Adicionar

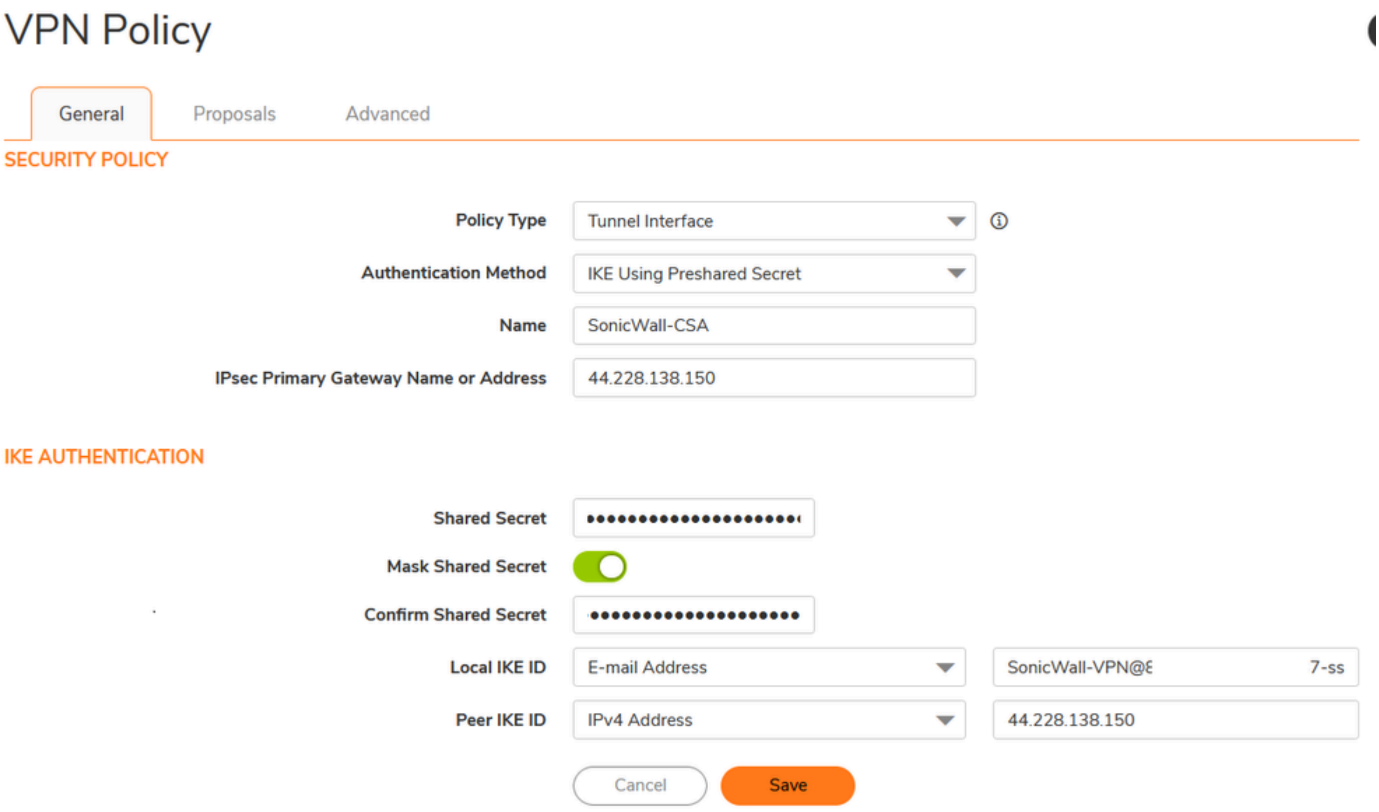


#	NAME	GATEWAY	DESTINATIONS	CRYPTO SUITE	ENABLE
1	WAN GroupVPN			ESP: 3DES/HMAC SHA1 (IKE)	○

Total: 1 item(s)

Sonicwall - IPSec VPN - Regras e configurações

- Em VPN Policy , preencha a configuração de VPN com base nos dados de túnel do acesso seguro e [parâmetros-ipsec suportados]


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: ••••••••••••••••••••••

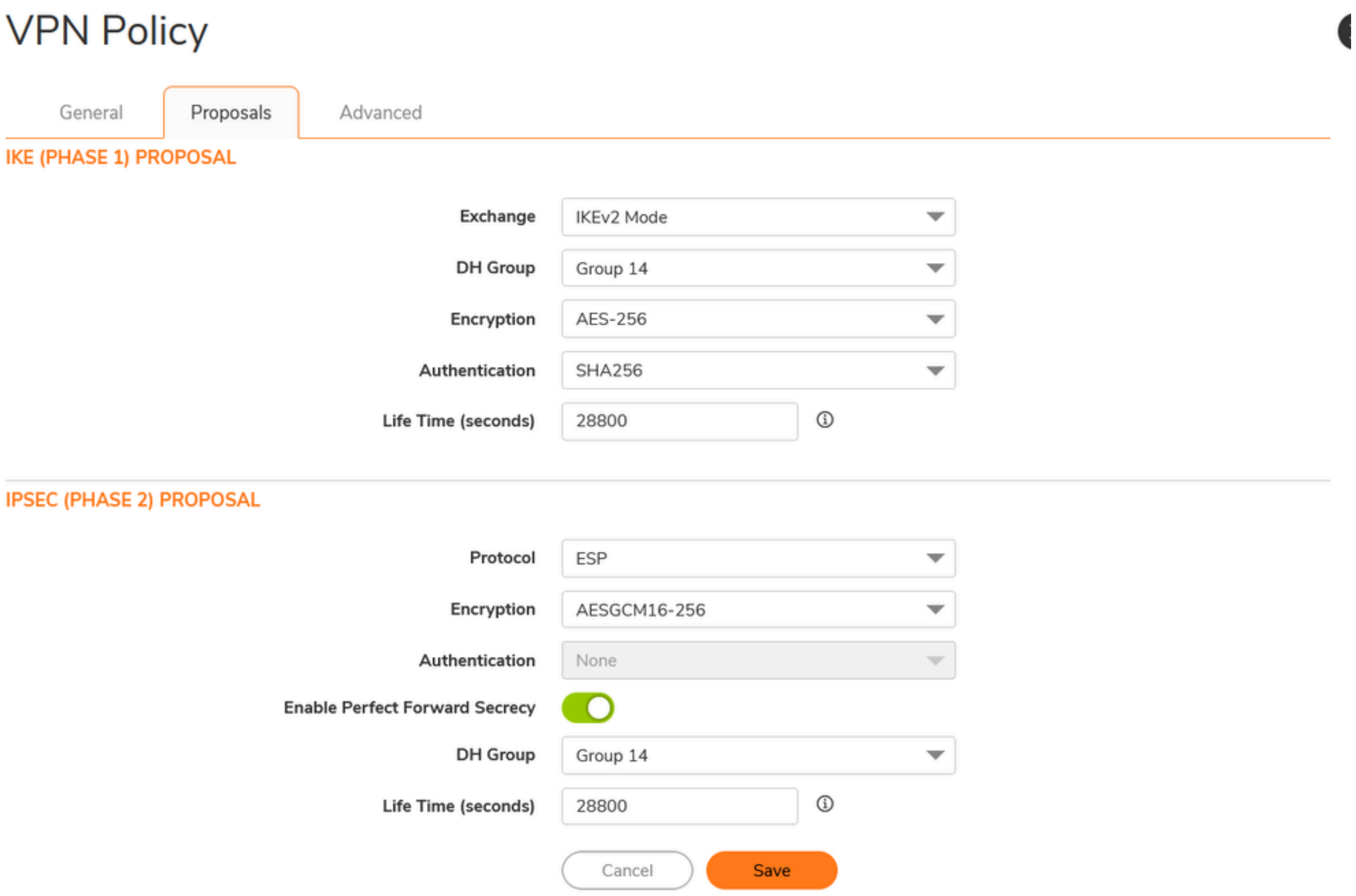
Mask Shared Secret: ●

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



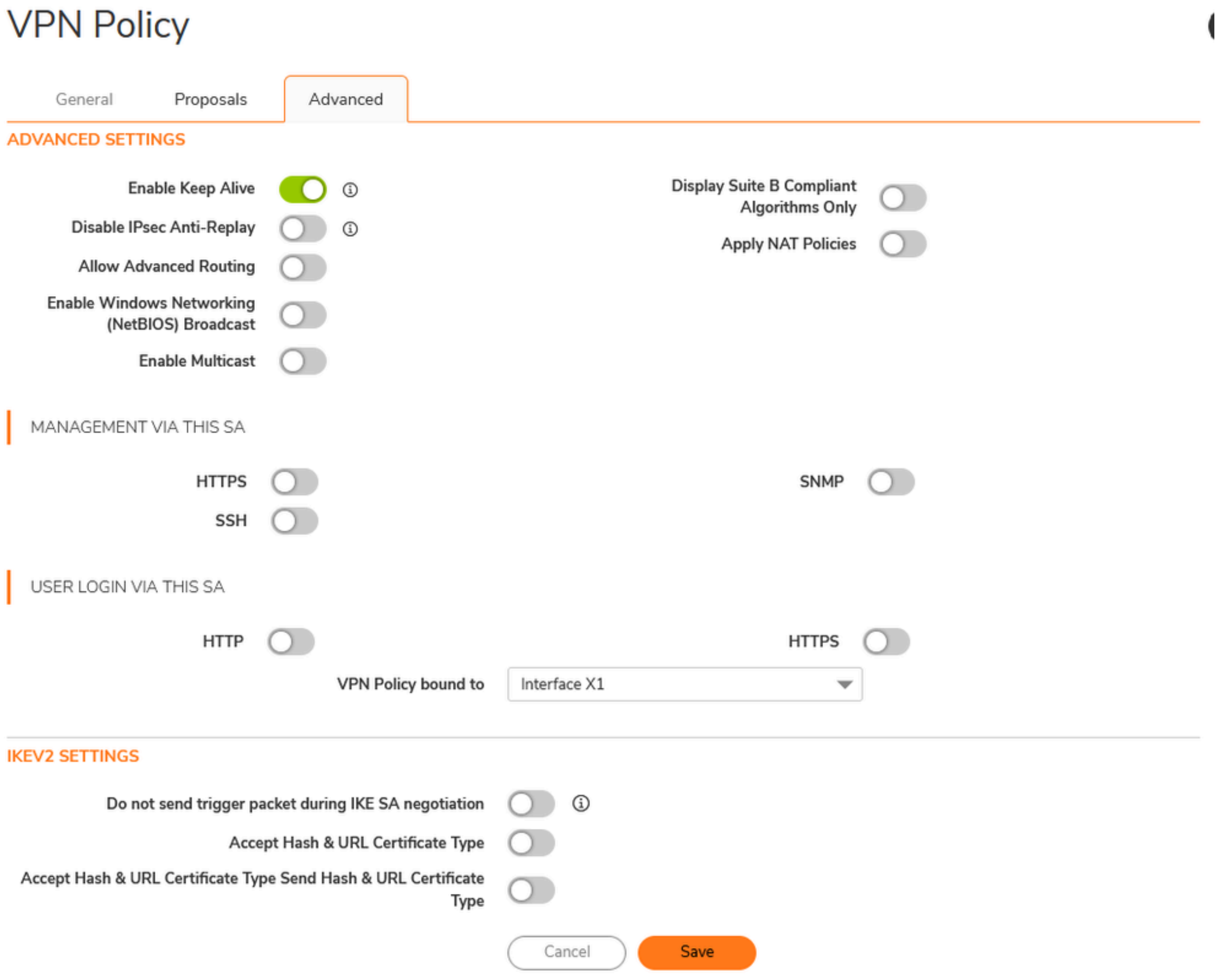
VPN Policy

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



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

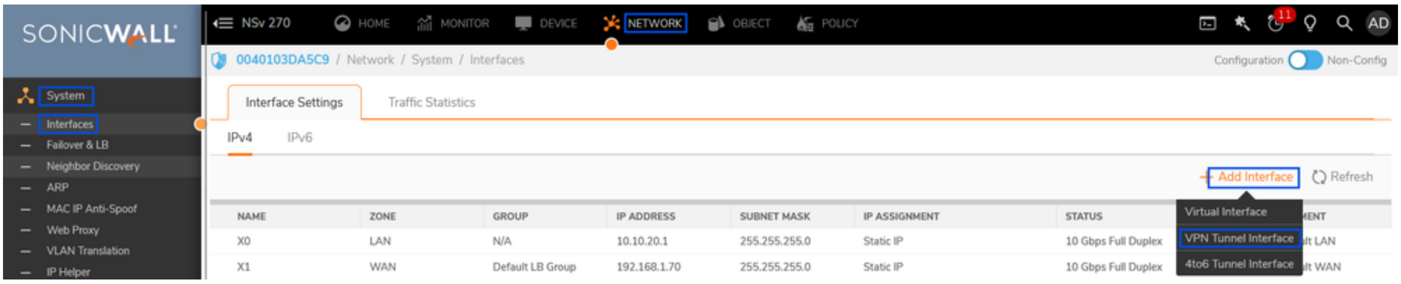
- Do not send trigger packet during IKE SA negotiation ○
- Accept Hash & URL Certificate Type ○
- Accept Hash & URL Certificate Type Send Hash & URL Certificate Type ○

- Clique em Salvar

Adicionar interface de túnel VPN

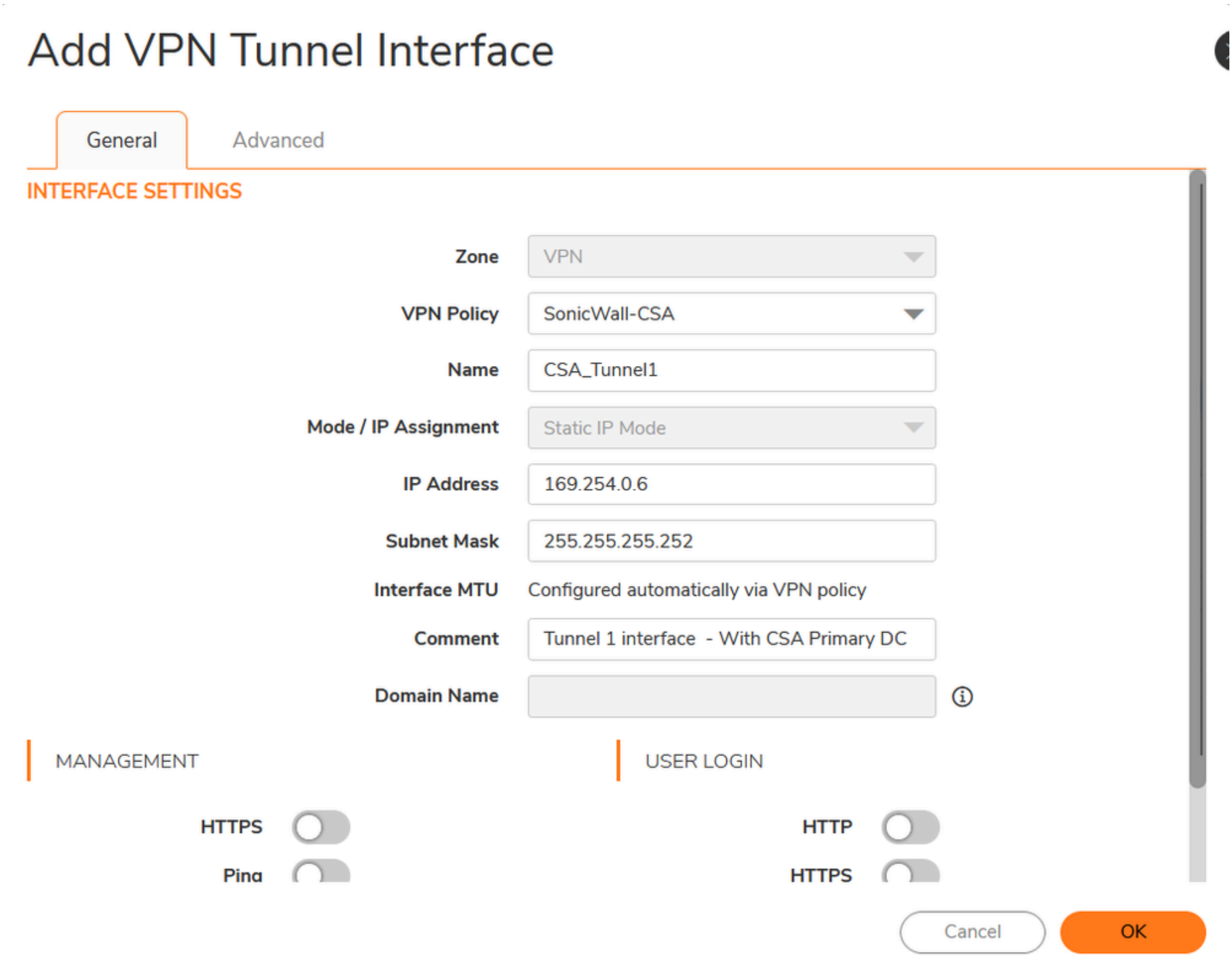
Navegue até o Painel Sonicwall.

- Rede > Sistema > Interface
- Clique em + Adicionar interface
- Selecionar interface de túnel VPN



NAME	ZONE	GROUP	IP ADDRESS	SUBNET MASK	IP ASSIGNMENT	STATUS	ENT
X0	LAN	N/A	10.10.20.1	255.255.255.0	Static IP	10 Gbps Full Duplex	lt LAN
X1	WAN	Default LB Group	192.168.1.70	255.255.255.0	Static IP	10 Gbps Full Duplex	lt WAN

Sonicwall - Interfaces



Add VPN Tunnel Interface

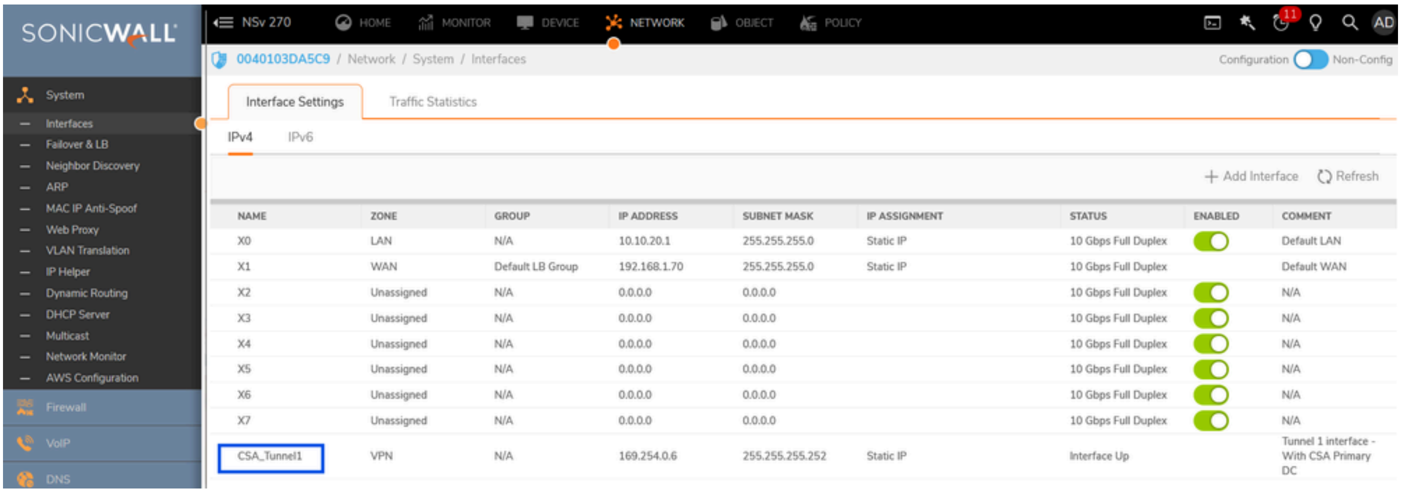
INTERFACE SETTINGS

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

- Clique em OK.



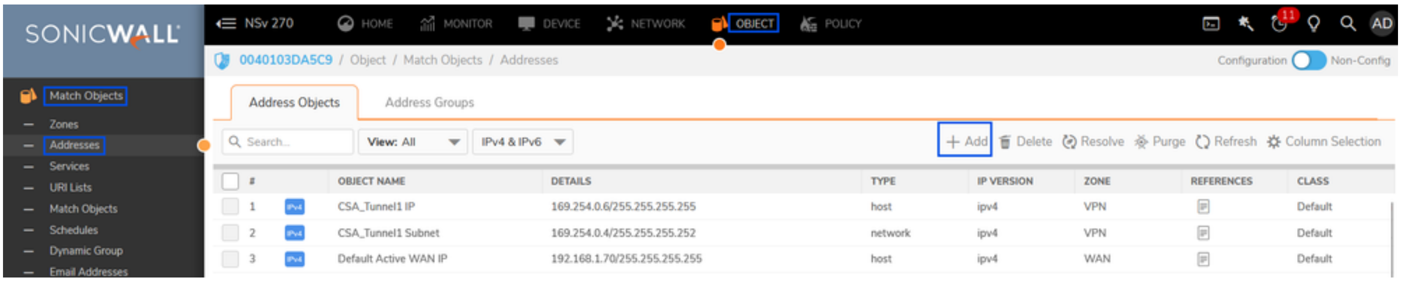
NAME	ZONE	GROUP	IP ADDRESS	SUBNET MASK	IP ASSIGNMENT	STATUS	ENABLED	COMMENT
X0	LAN	N/A	10.10.20.1	255.255.255.0	Static IP	10 Gbps Full Duplex	●	Default LAN
X1	WAN	Default LB Group	192.168.1.70	255.255.255.0	Static IP	10 Gbps Full Duplex		Default WAN
X2	Unassigned	N/A	0.0.0.0	0.0.0.0		10 Gbps Full Duplex	●	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 - Interface de túnel VPN

Adicionar objetos e grupos de rede

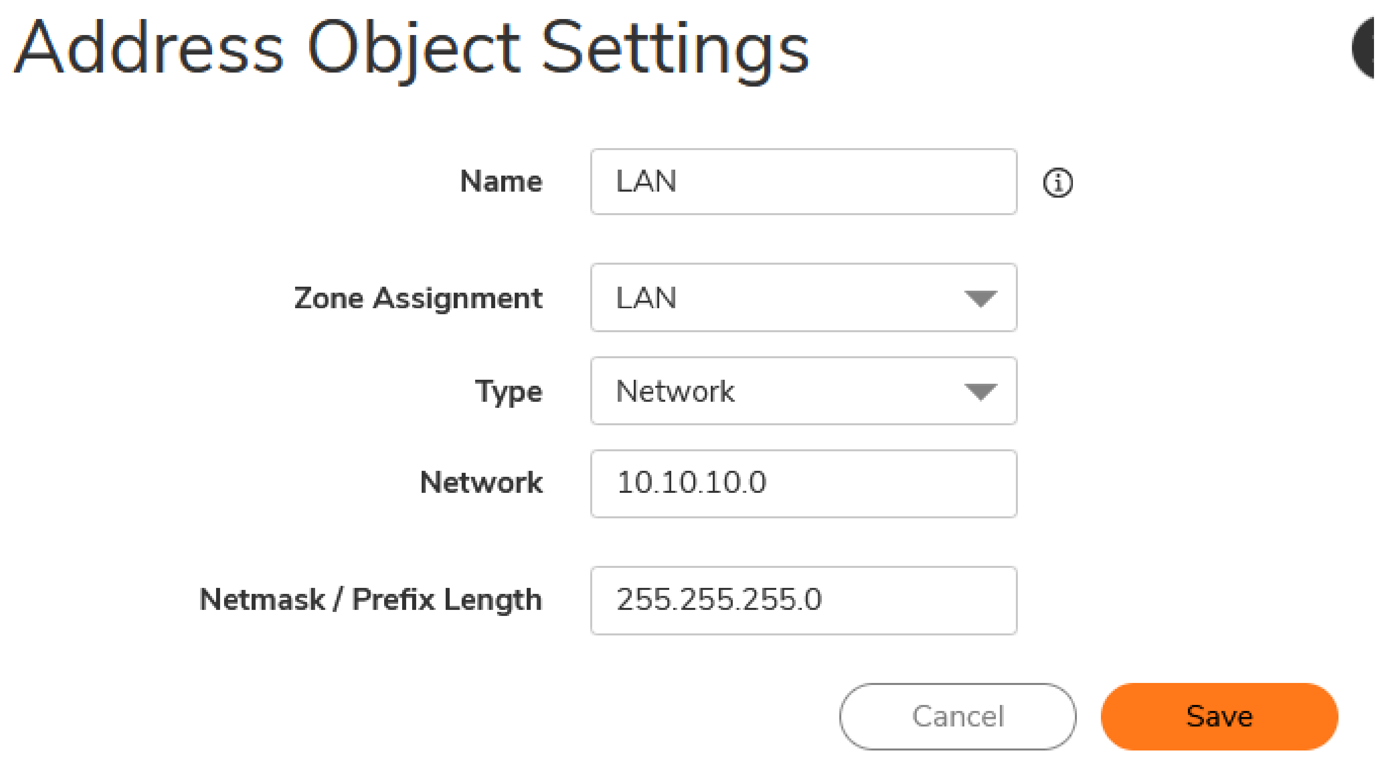
Navegue até o Painel Sonicwall.

- Objeto > Corresponder objetos >Endereços
- Objetos de Endereço
- Clique em +Adicionar



#		OBJECT NAME	DETAILS	TYPE	IP VERSION	ZONE	REFERENCES	CLASS
1	IPv4	CSA_Tunnel1 IP	169.254.0.6/255.255.255.255	host	ipv4	VPN		Default
2	IPv4	CSA_Tunnel1 Subnet	169.254.0.4/255.255.255.252	network	ipv4	VPN		Default
3	IPv4	Default Active WAN IP	192.168.1.70/255.255.255.255	host	ipv4	WAN		Default

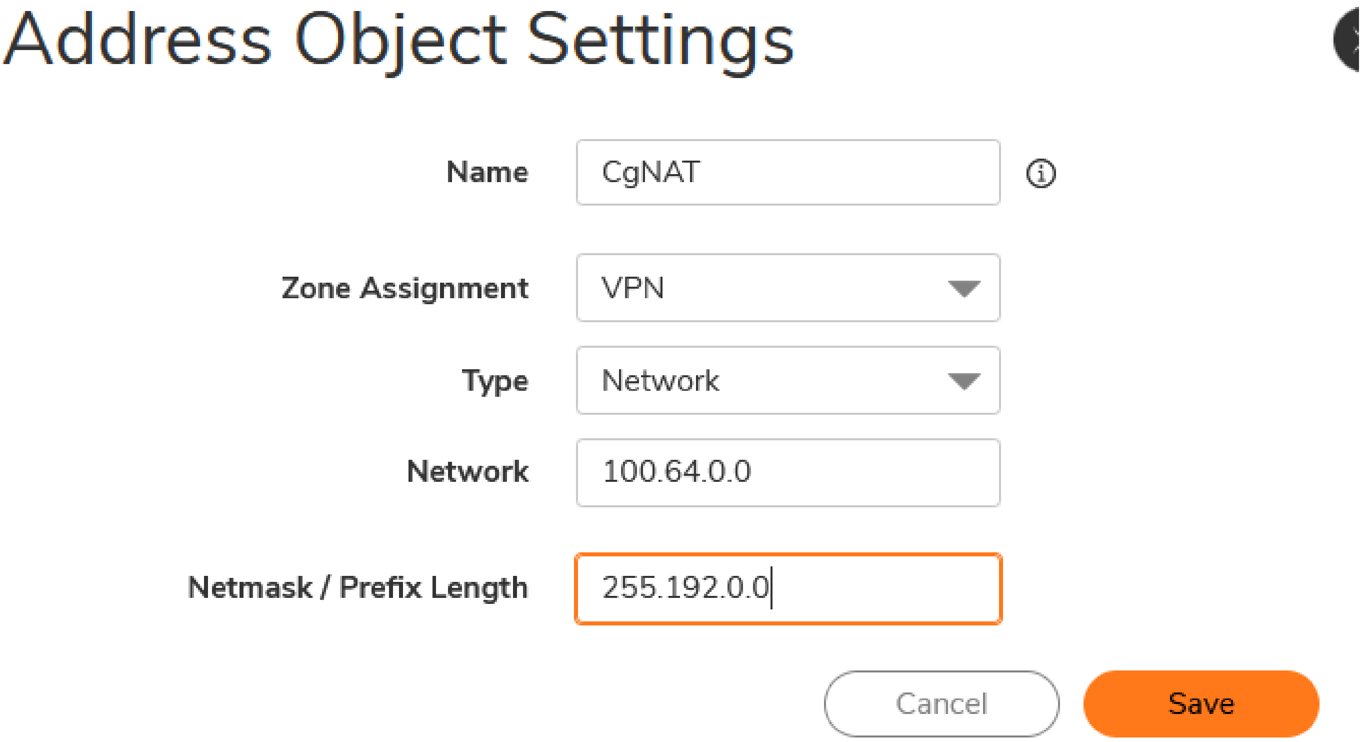
Sonicwall - Object- Objetos de endereço



Address Object Settings

Name	LAN
Zone Assignment	LAN
Type	Network
Network	10.10.10.0
Netmask / Prefix Length	255.255.255.0

- Clique em Salvar



Address Object Settings

Name: CgNAT

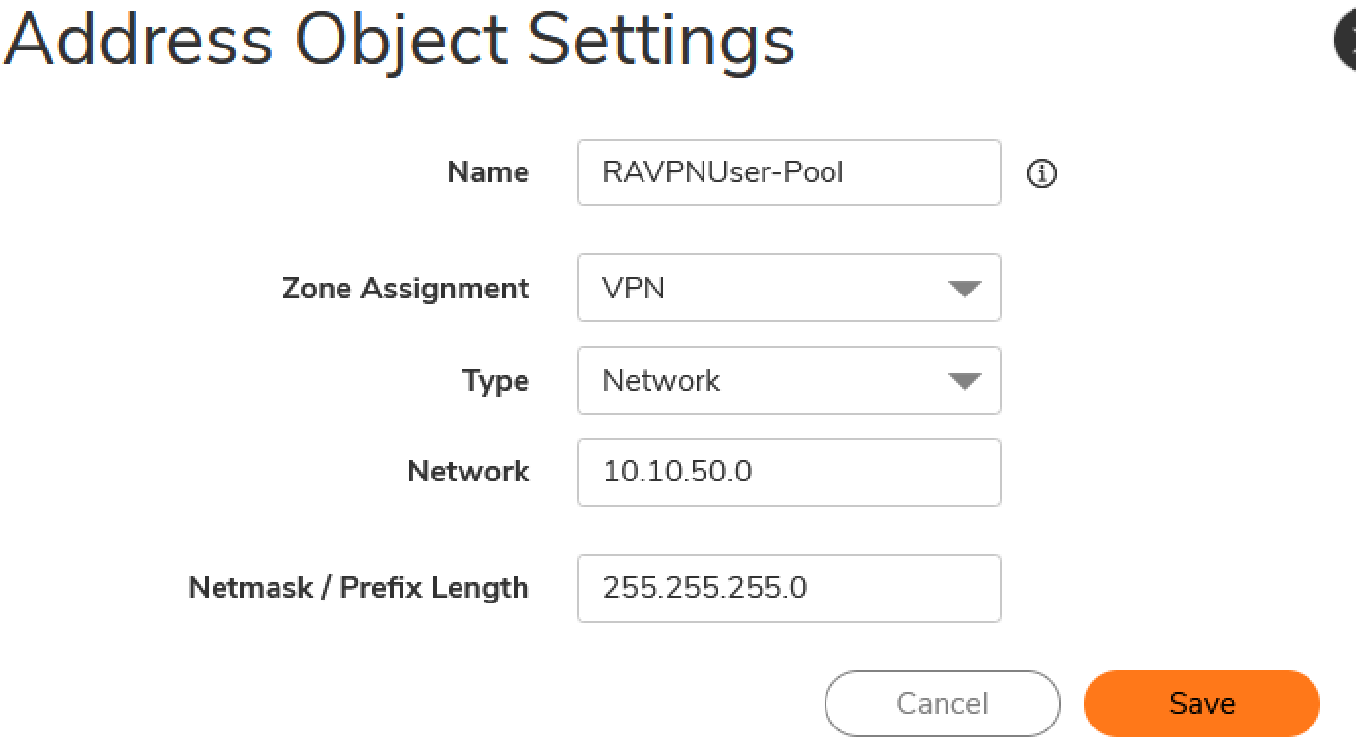
Zone Assignment: VPN

Type: Network

Network: 100.64.0.0

Netmask / Prefix Length: 255.192.0.0

- Clique em Salvar



Address Object Settings

Name: RAVPNUser-Pool

Zone Assignment: VPN

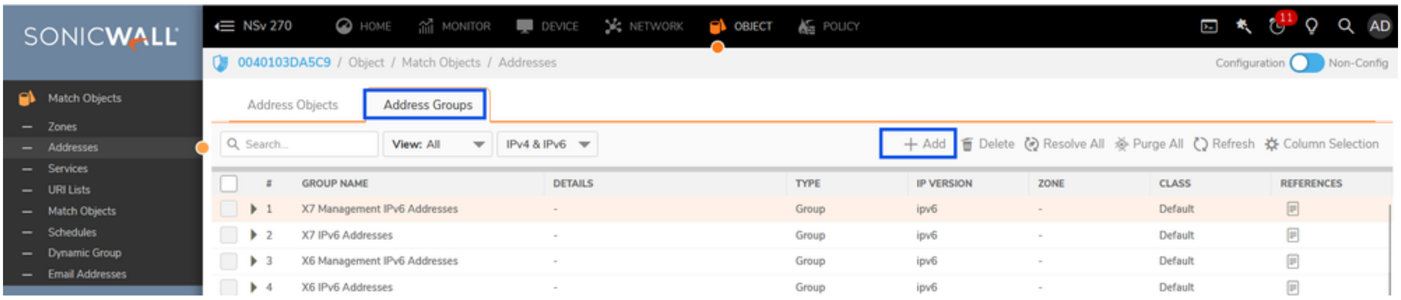
Type: Network

Network: 10.10.50.0

Netmask / Prefix Length: 255.255.255.0

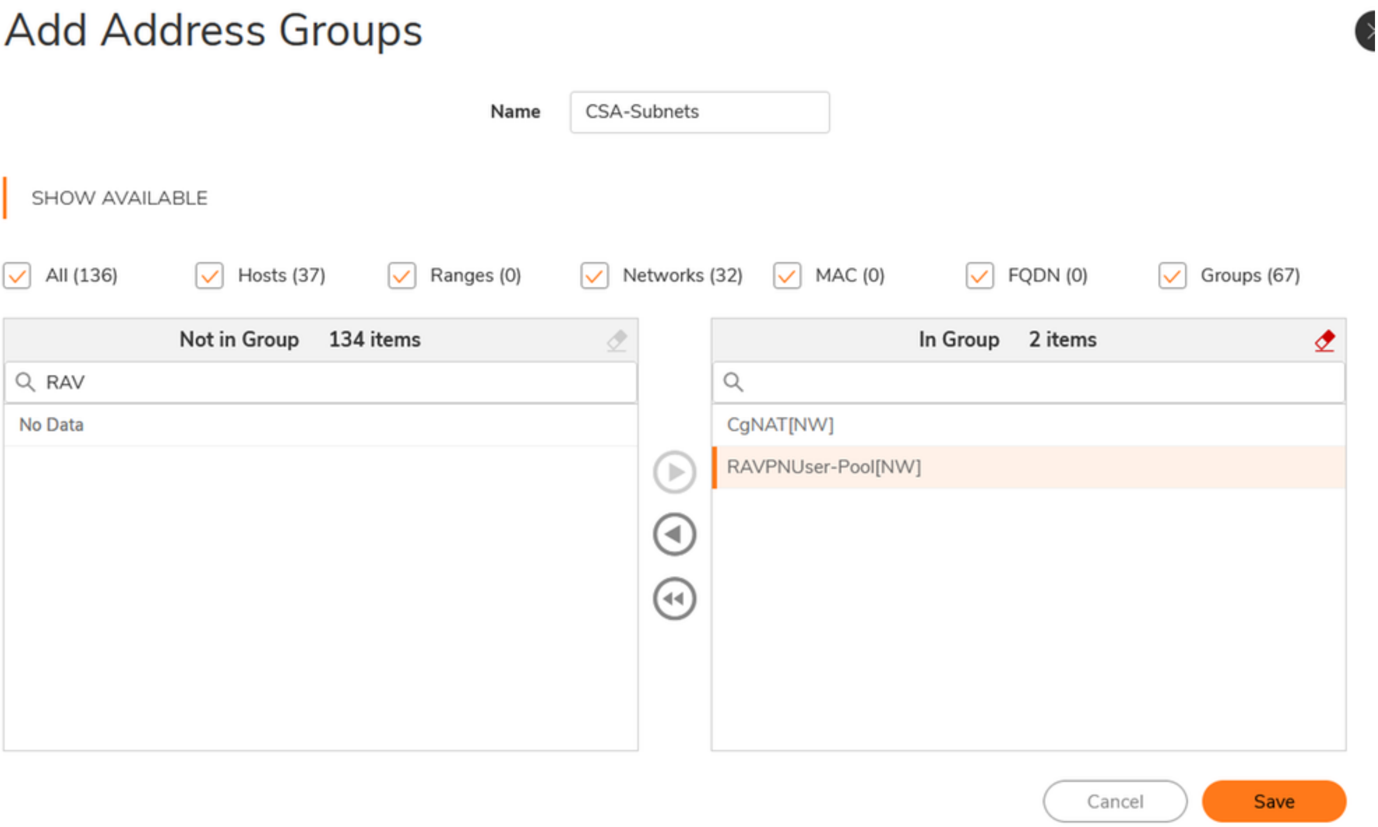
- Clique em Salvar

- Criar grupos de endereços
- Clique em +Adicionar
- Selecione o objeto de endereço e adicione-o aos grupos de endereços



#	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 - Object- Grupos de endereços



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]

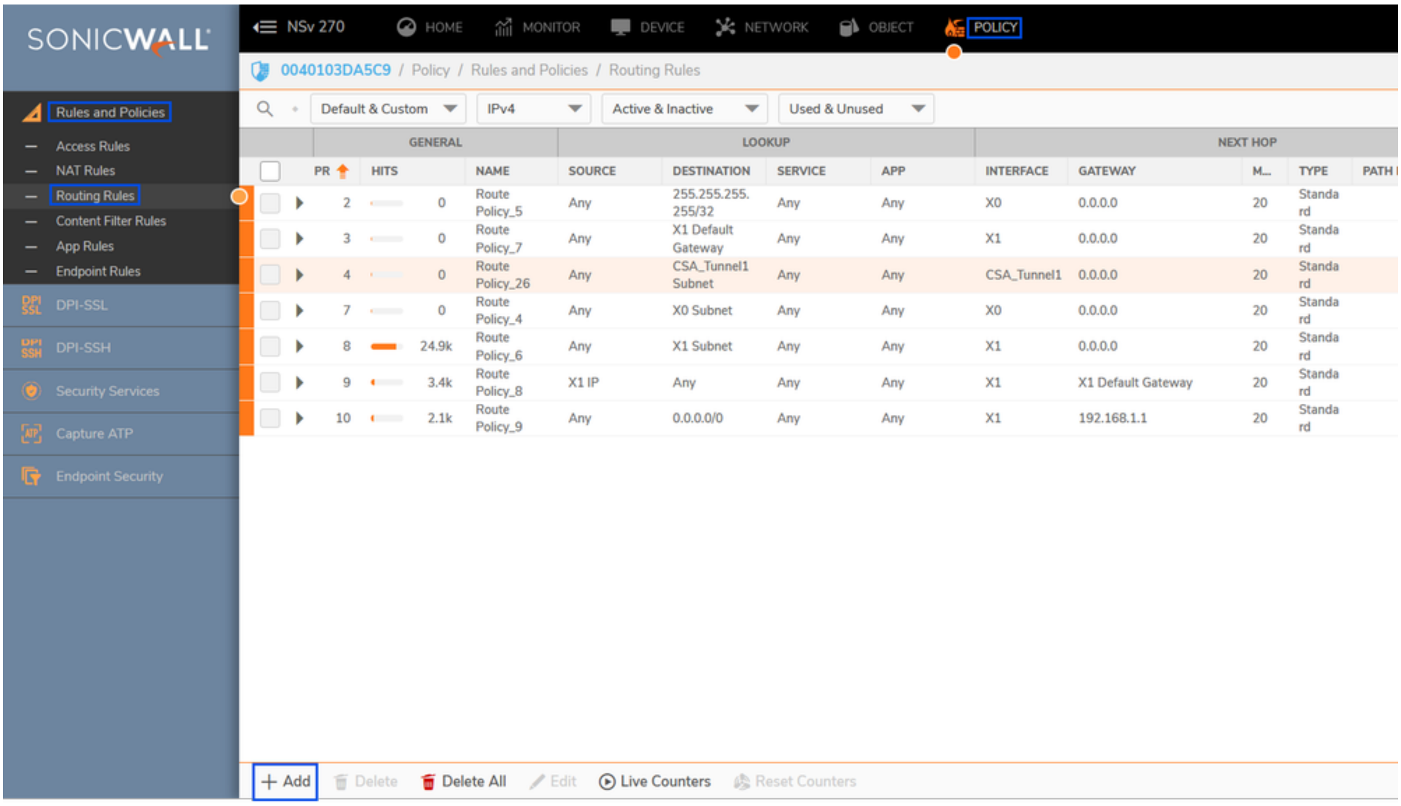
RAVPNUser-Pool[NW]

- Clique em Salvar

Adicionar rota

Navegue até o Painel Sonicwall.

- Política > Regras e Políticas > Regras de Roteamento
- Clique em + Adicionar



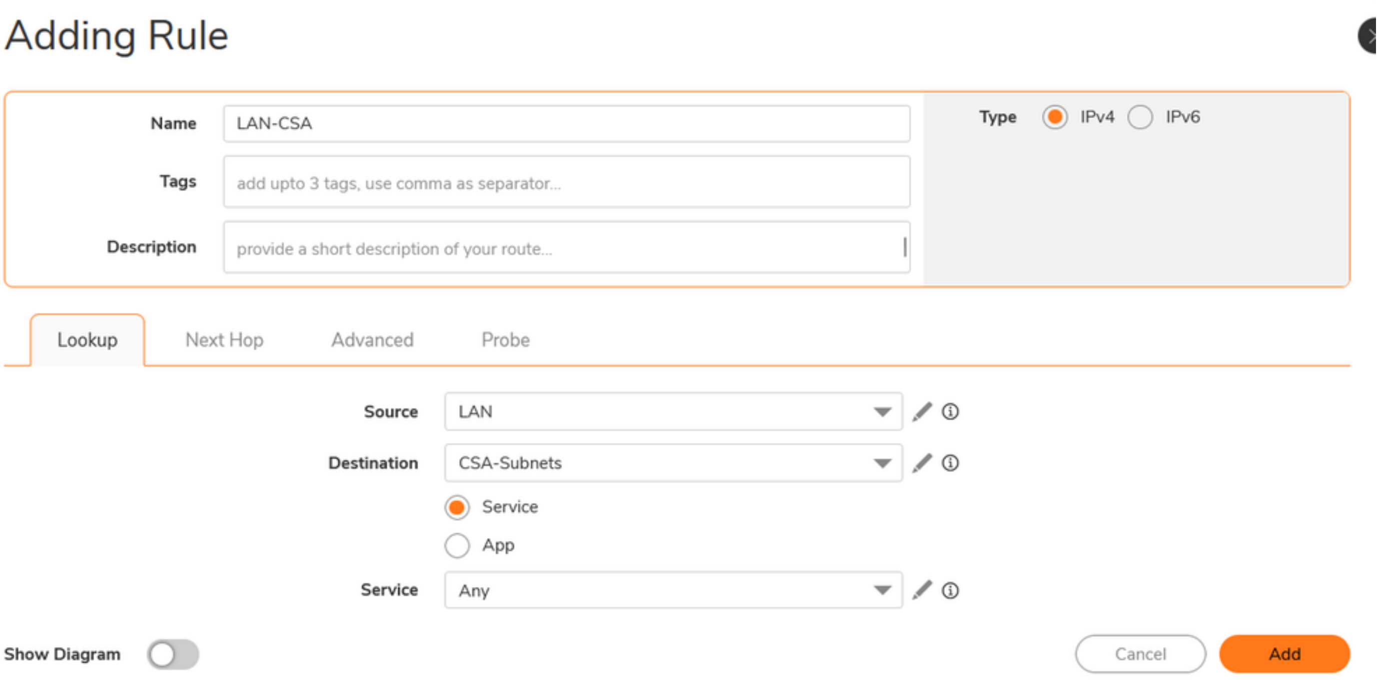
0040103DA5C9 / Policy / Rules and Policies / Routing Rules

Default & Custom | IPv4 | Active & Inactive | Used & Unused

GENERAL			LOOKUP				NEXT HOP				
PR	HITS	NAME	SOURCE	DESTINATION	SERVICE	APP	INTERFACE	GATEWAY	M...	TYPE	PATH
2	0	Route Policy_5	Any	255.255.255.255/32	Any	Any	X0	0.0.0.0	20	Standard	
3	0	Route Policy_7	Any	X1 Default Gateway	Any	Any	X1	0.0.0.0	20	Standard	
4	0	Route Policy_26	Any	CSA_Tunnel1 Subnet	Any	Any	CSA_Tunnel1	0.0.0.0	20	Standard	
7	0	Route Policy_4	Any	X0 Subnet	Any	Any	X0	0.0.0.0	20	Standard	
8	24.9k	Route Policy_6	Any	X1 Subnet	Any	Any	X1	0.0.0.0	20	Standard	
9	3.4k	Route Policy_8	X1 IP	Any	Any	Any	X1	X1 Default Gateway	20	Standard	
10	2.1k	Route Policy_9	Any	0.0.0.0/0	Any	Any	X1	192.168.1.1	20	Standard	

Sonicwall - Regras de roteamento

- Adicionar regra de roteamento



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

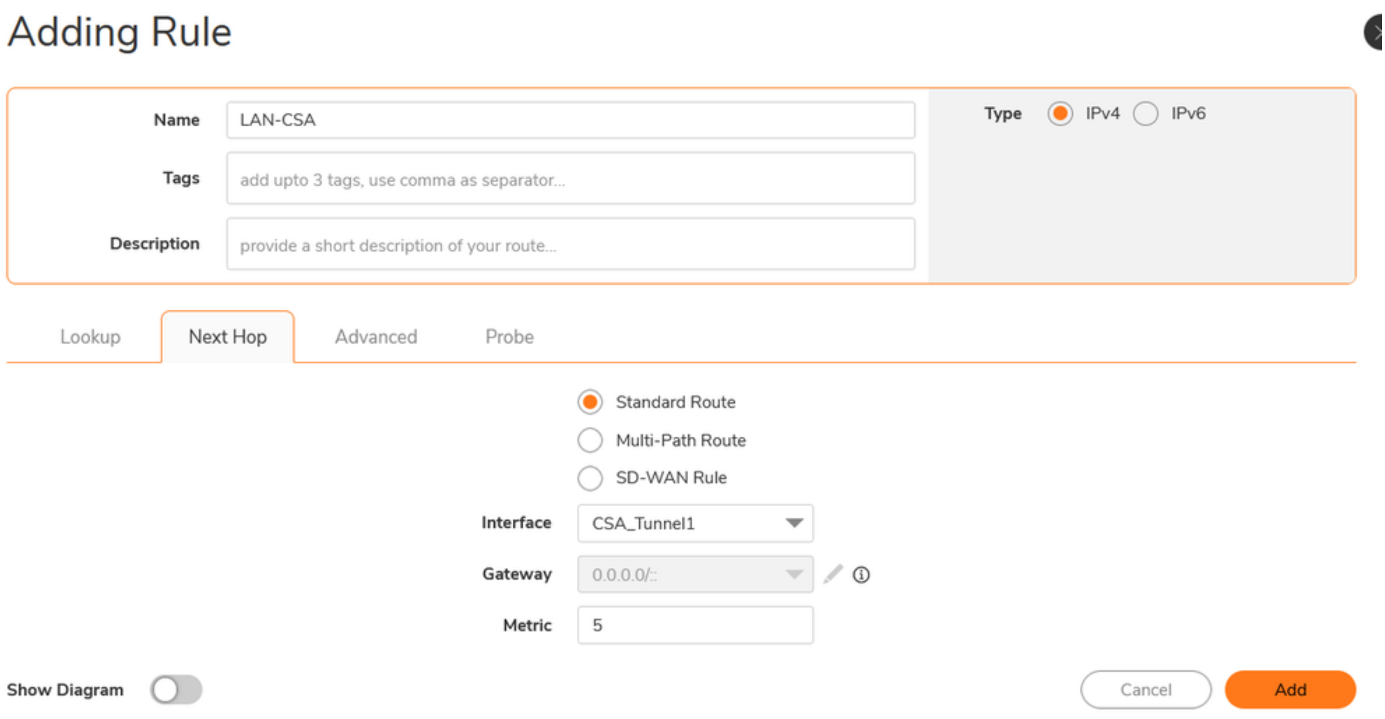
Source: LAN

Destination: CSA-Subnets

● Service
○ App

Service: Any

Show Diagram



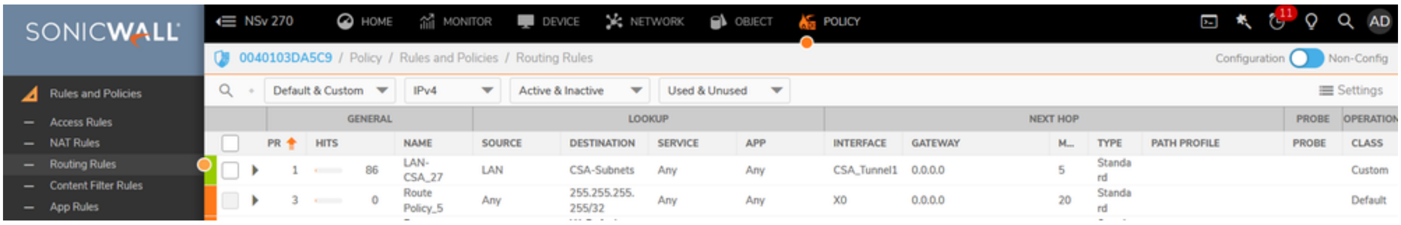
Adding Rule

Name	LAN-CSA
Tags	add upto 3 tags, use comma as separator...
Description	provide a short description of your route...
Type	● IPv4 ○ IPv6

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

Interface	CSA_Tunnel1
Gateway	0.0.0.0/::
Metric	5

- Clique em + Adicionar



0040103DA5C9 / Policy / Rules and Policies / Routing Rules

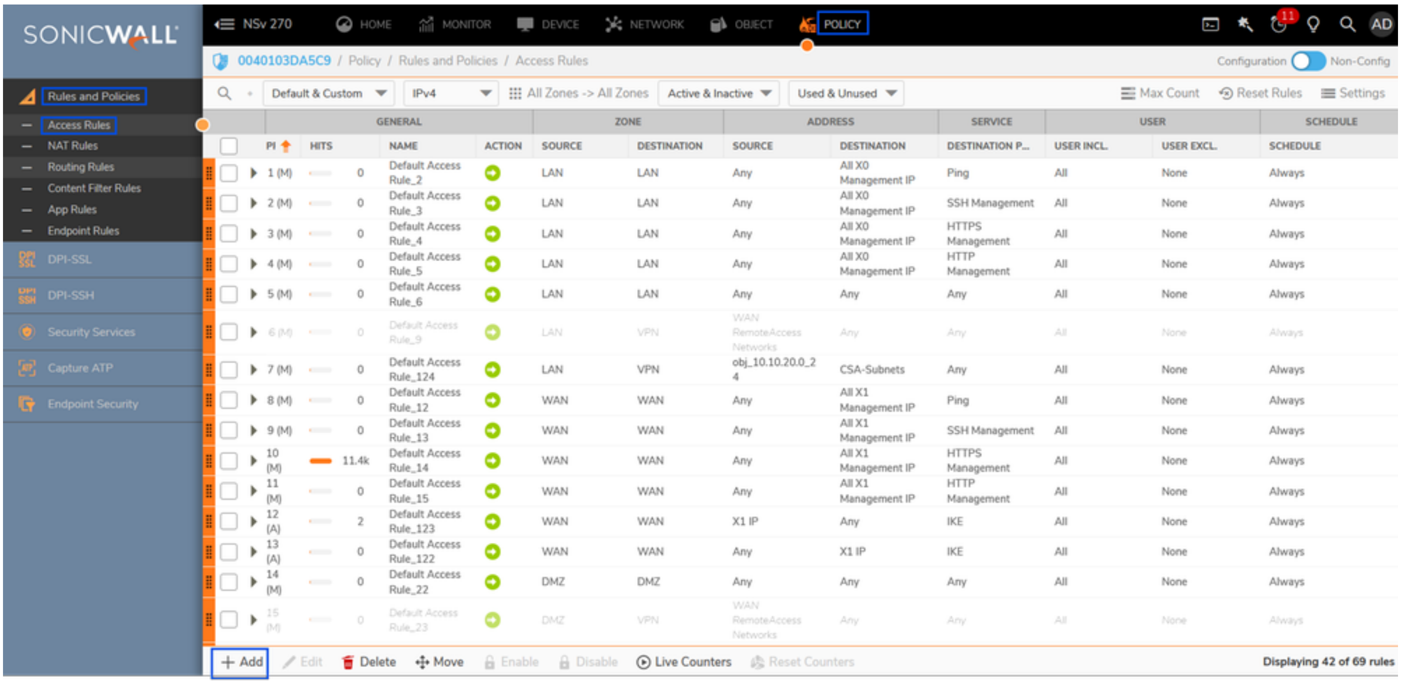
	GENERAL			LOOKUP				NEXT HOP					PROBE	OPERATION
□	PR	HITS	NAME	SOURCE	DESTINATION	SERVICE	APP	INTERFACE	GATEWAY	M...	TYPE	PATH PROFILE	PROBE	CLASS
□	1	86	LAN-CSA_27	LAN	CSA-Subnets	Any	Any	CSA_Tunnel1	0.0.0.0	5	Standard			Custom
□	3	0	Route Policy_5	Any	255.255.255.255/32	Any	Any	X0	0.0.0.0	20	Standard			Default

Sonicwall - Regras de roteamento

Adicionar regras de acesso

Navegue até o Painel Sonicwall.

- Política > Regras e Políticas > Regras de Acesso
- Clique em + Adicionar



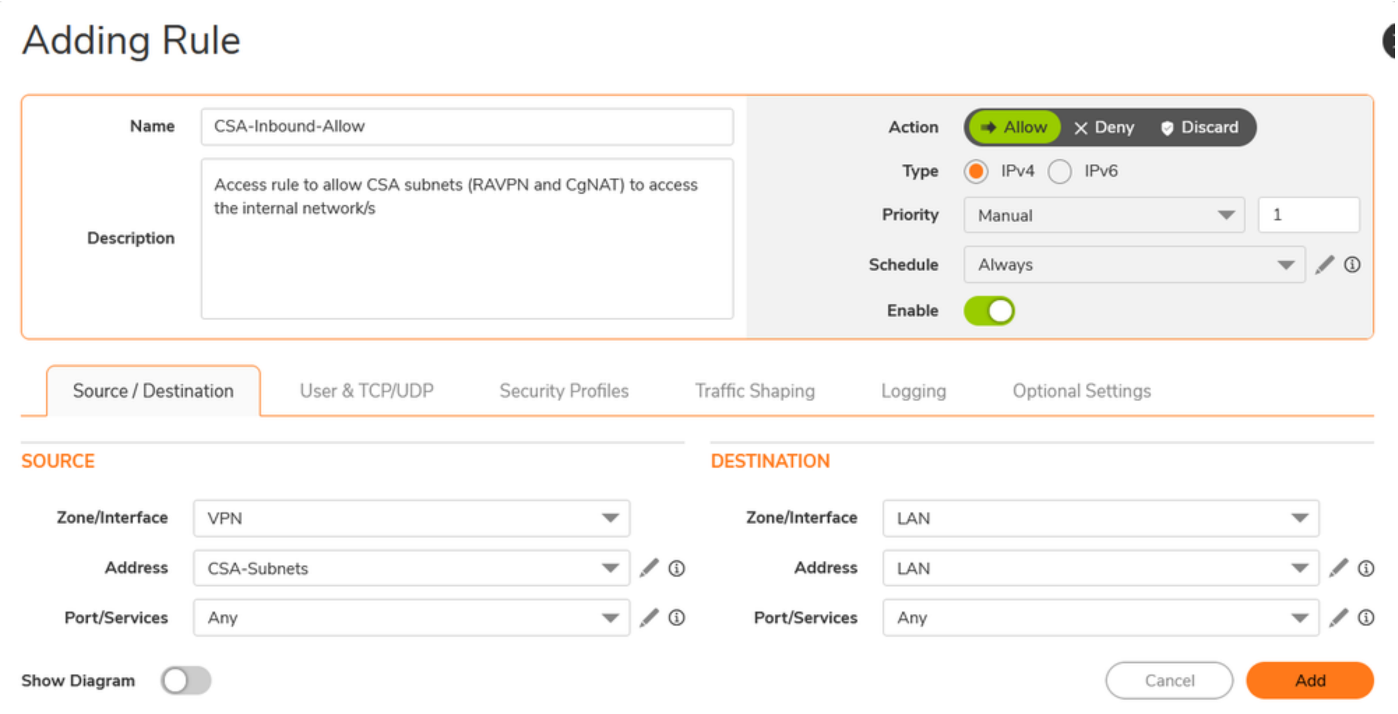
0040103DA5C9 / Policy / Rules and Policies / Access Rules

Default & Custom | IPv4 | All Zones -> All Zones | Active & Inactive | Used & Unused

GENERAL				ZONE		ADDRESS		SERVICE	USER		SCHEDULE
PI	HITS	NAME	ACTION	SOURCE	DESTINATION	SOURCE	DESTINATION	DESTINATION P...	USER INCL.	USER EXCL.	SCHEDULE
1 (M)	0	Default Access Rule_2	➜	LAN	LAN	Any	All X0 Management IP	Ping	All	None	Always
2 (M)	0	Default Access Rule_3	➜	LAN	LAN	Any	All X0 Management IP	SSH Management	All	None	Always
3 (M)	0	Default Access Rule_4	➜	LAN	LAN	Any	All X0 Management IP	HTTPS Management	All	None	Always
4 (M)	0	Default Access Rule_5	➜	LAN	LAN	Any	All X0 Management IP	HTTP Management	All	None	Always
5 (M)	0	Default Access Rule_6	➜	LAN	LAN	Any	Any	Any	All	None	Always
6 (M)	0	Default Access Rule_9	➜	LAN	VPN	WAN RemoteAccess Networks	Any	Any	All	None	Always
7 (M)	0	Default Access Rule_124	➜	LAN	VPN	obj_10.10.20.0_24	CSA-Subnets	Any	All	None	Always
8 (M)	0	Default Access Rule_12	➜	WAN	WAN	Any	All X1 Management IP	Ping	All	None	Always
9 (M)	0	Default Access Rule_13	➜	WAN	WAN	Any	All X1 Management IP	SSH Management	All	None	Always
10 (M)	11.4k	Default Access Rule_14	➜	WAN	WAN	Any	All X1 Management IP	HTTPS Management	All	None	Always
11 (M)	0	Default Access Rule_15	➜	WAN	WAN	Any	All X1 Management IP	HTTP Management	All	None	Always
12 (A)	2	Default Access Rule_123	➜	WAN	WAN	X1 IP	Any	IKE	All	None	Always
13 (A)	0	Default Access Rule_122	➜	WAN	WAN	Any	X1 IP	IKE	All	None	Always
14 (M)	0	Default Access Rule_22	➜	DMZ	DMZ	Any	Any	Any	All	None	Always
15 (M)	0	Default Access Rule_23	➜	DMZ	VPN	WAN RemoteAccess Networks	Any	Any	All	None	Always

Displaying 42 of 69 rules

Sonicwall - Regras de acesso



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 ○ IPv6
Priority	Manual 1
Schedule	Always
Enable	☑

SOURCE

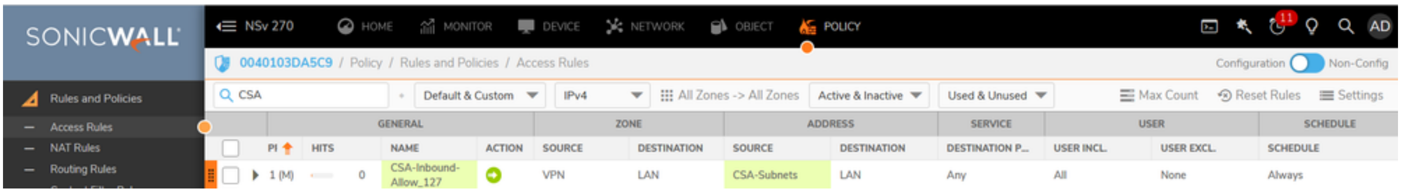
Zone/Interface	VPN
Address	CSA-Subnets
Port/Services	Any

DESTINATION

Zone/Interface	LAN
Address	LAN
Port/Services	Any

Show Diagram ○

- Clique em +Adicionar



0040103DA5C9 / Policy / Rules and Policies / Access Rules

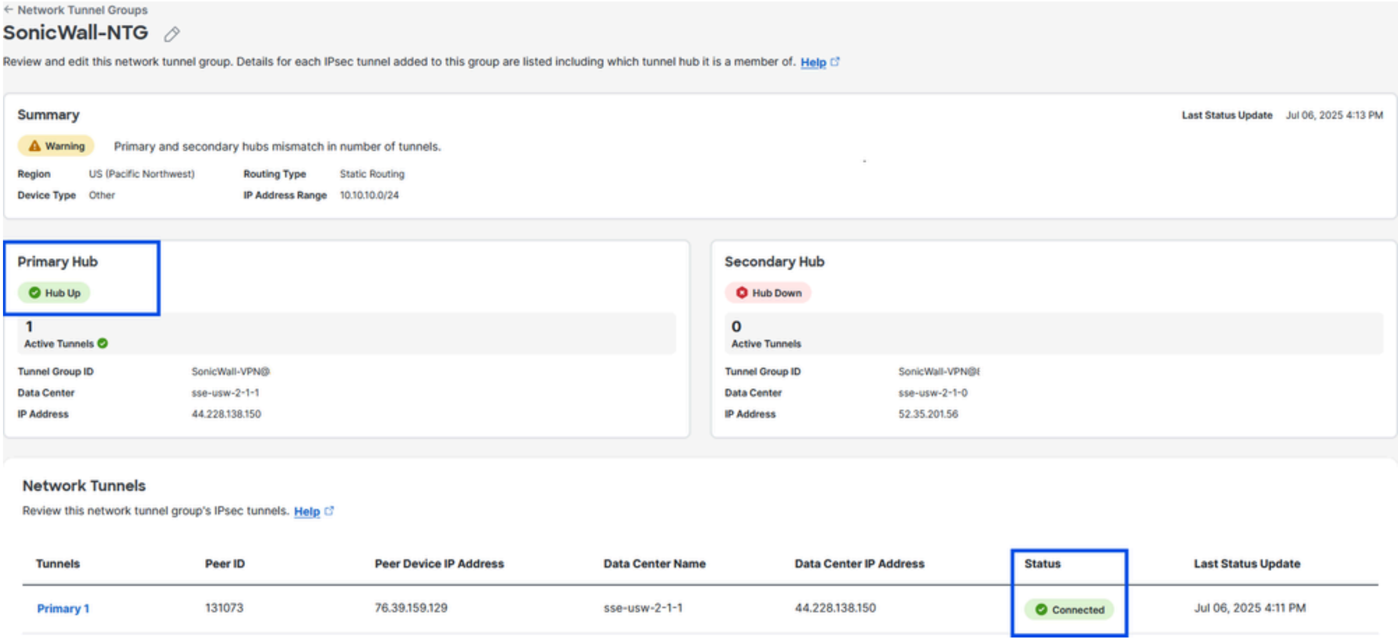
CSA | Default & Custom | IPv4 | All Zones -> All Zones | Active & Inactive | Used & Unused

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	➜	VPN	LAN	CSA-Subnets	LAN	Any	All	None	Always

Sonicwall - Regras de acesso

Verificar

- Status do túnel no acesso 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

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

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

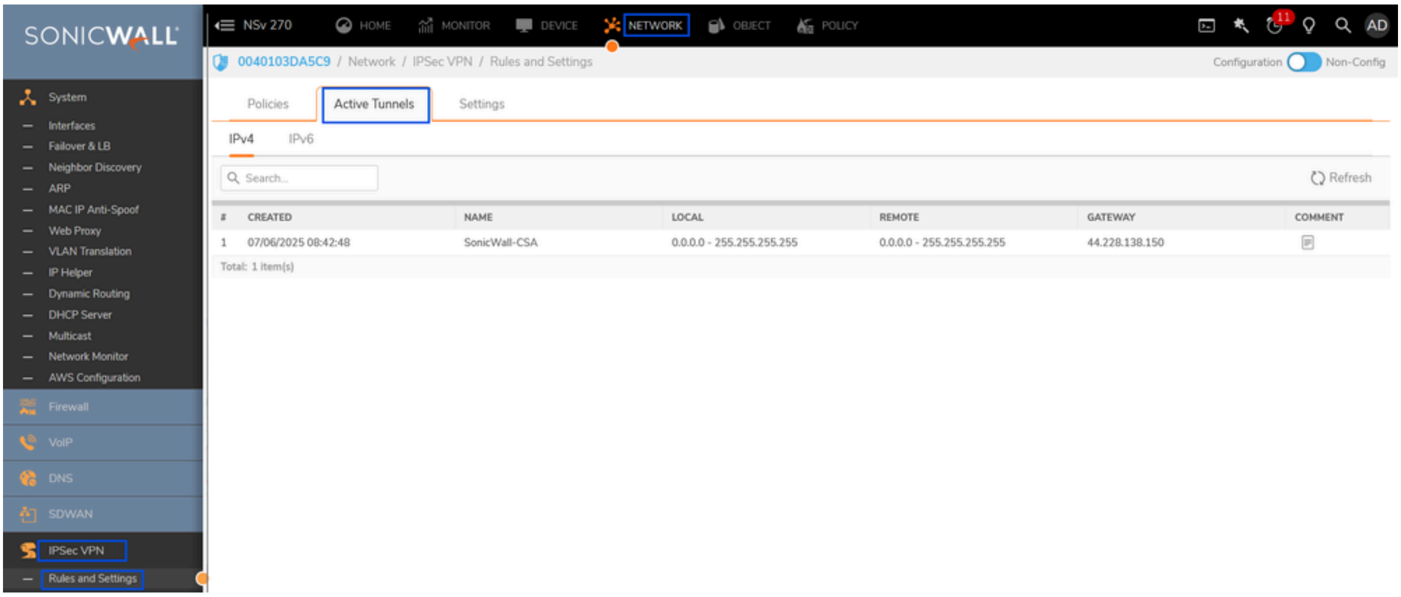
Network Tunnels

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

Acesso seguro - Grupo de túneis de rede - status da VPN

- Status do túnel no firewall Sonicwall



0040103DA5C9 / Network / IPSec VPN / Rules and Settings

#	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 - status de VPN IPSec

Você pode fazer o mesmo processo para configurar o túnel entre o data center secundário de acesso seguro e o Sonicwall

Agora, o túnel está UP no Secure Access e Sonicwall, você pode continuar configurando o acesso aos recursos privados através de RA-VPN , ZTA baseado em navegador ou ZTA baseado em cliente no painel de acesso seguro

Troubleshooting

PC do usuário

- Verifique se o usuário pode se conectar/registrar no RAVPN/ZTNA com êxito ou não. Caso contrário, solucione outros problemas relacionados à falha da conexão do plano de controle.
- Verifique se a rede que o usuário está tentando acessar deve passar pelo túnel RAVPN ou ZTNA . Caso contrário, verifique a configuração no headend .

Acesso seguro

- Verifique a configuração do direcionamento de tráfego no perfil de conexão RAVPN para confirmar se a rede de Destino está configurada para enviar pelo túnel para Acesso Seguro.
- Verifique se o recurso privado está definido com protocolo/portas válidos e se os mecanismos de conexão ZTNA/RAVPN estão verificados.
- Verifique se a política de acesso está configurada para permitir que o usuário RAVPN/ZTNA acesse a Private Resource Network e seja colocado em uma ordem em que nenhuma outra regra tenha precedência para bloquear o tráfego.
- Verifique se o túnel IPSec está UP e Secure Access mostrando rotas de cliente válidas através de roteamento estático que cobre o recurso privado que o usuário está tentando acessar.

Sonicwall

- Verifique se o túnel IPSec está UP ou não (IKE & IPSec SA) .
- Verifique se a rota ou rotas do cliente foram anunciadas corretamente.
- Verifique se as fontes de tráfego do usuário RAVPN/ZTNA destinadas ao recurso privado por trás do Sonicwall estão alcançando o firewall Sonicwall através do túnel, capturando pacotes no Sonicwall.
- Verifique se o tráfego atingiu o recurso privado e respondeu ao cliente RAVPN/ZTNA ou não. Se sim, verifique se esses pacotes estão chegando à interface Sonicall X0 (LAN).
- Verifique se Sonicwall está encaminhando o tráfego de retorno através do túnel IPSec em direção ao acesso seguro.

Informações Relacionadas

- Suporte técnico e downloads da Cisco
- Central de ajuda do Cisco Secure Access
- Módulo de acesso Zero Trust
- Solucione O Erro De Acesso Seguro "O Serviço De Registro Não Está Respondendo. Entre em contato com o help desk de TI"