تكوين الوصول الآمن باستخدام جدار حماية SONICWALL

المحتويات

[المقدمة](#)

[المتطلبات الأساسية](#)

  [المتطلبات](#)

  [المكونات المستخدمة](#)

  [معلومات أساسية](#)

  [الرسم التخطيطي للشبكة](#)

[التكوين](#)

  [تكوين مجموعة نفق الشبكة (VPN) على الوصول الآمن](#)

  [تكوين النفق على Sonicwall](#)

  [تكوين النفق - القواعد والإعدادات](#)

  [إضافة واجهة نفق VPN](#)

  [إضافة كائن شبكة ومجموعات](#)

  [إضافة مسار](#)

  [إضافة قواعد الوصول](#)

[التحقق من الصحة](#)

[استكشاف الأخطاء وإصلاحها](#)

  [كمبيوتر المستخدم](#)

  [الوصول الآمن](#)

  [سونيكوول](#)

[معلومات ذات صلة](#)

المقدمة

يصف هذا المستند كيفية تكوين نفق IPsec VTI بين الوصول الآمن إلى جدار حماية Sonicwall باستخدام التوجيه الثابت.

المتطلبات الأساسية

- تكوين توفير المستخدم
- تكوين مصادقة ZTNA SSO
- تكوين الوصول الآمن إلى VPN للوصول عن بعد

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- جدار حماية Sonicwall (NSv270 - SonicOSX 7.0.1)

- الوصول الآمن
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA
- زتنا بدون زوايا

المكونات المستخدمة

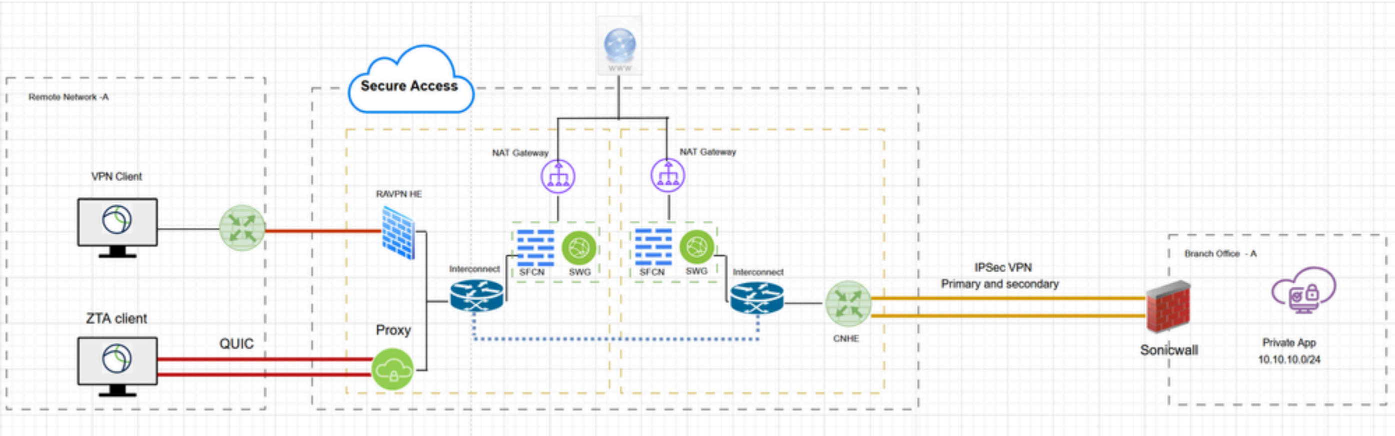
تستند المعلومات الواردة في هذا المستند إلى:

- جدار حماية Sonicwall (NSv270 - SonicOSX 7.0.1)
- الوصول الآمن
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

الرسم التخطيطي للشبكة



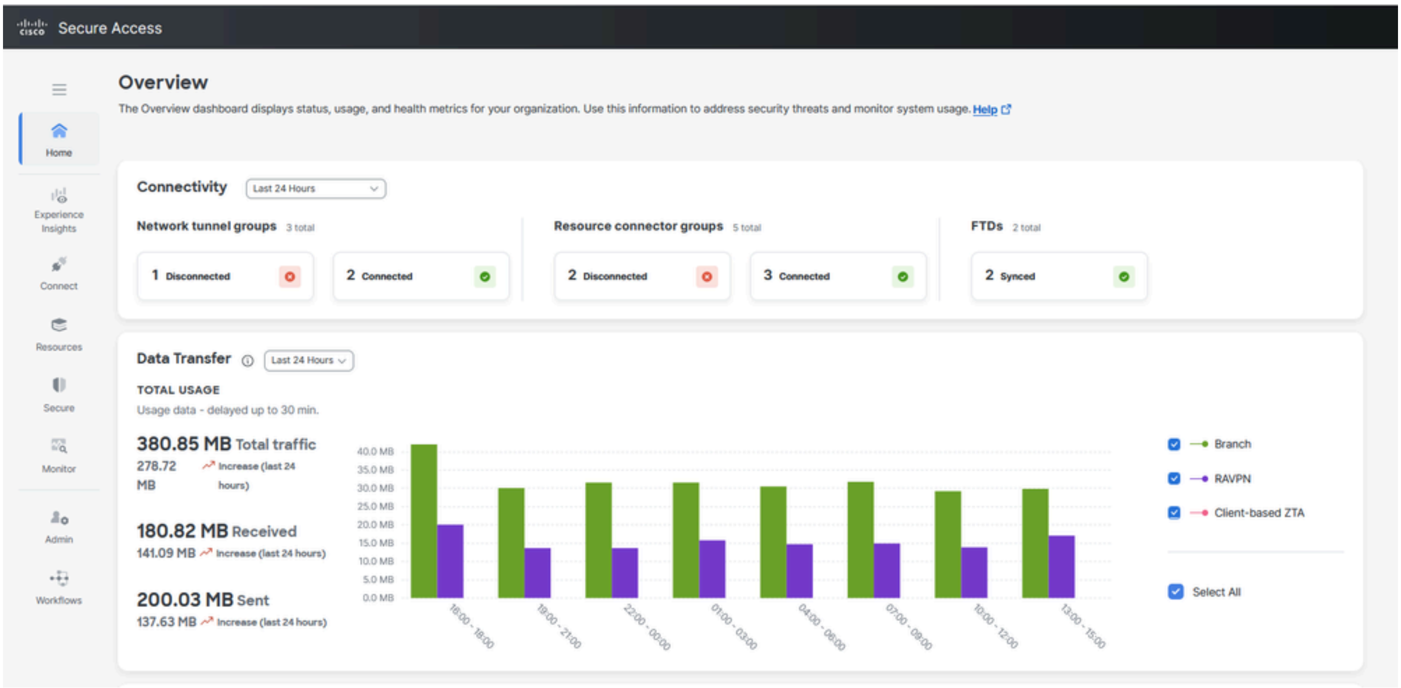
الرسم التخطيطي للشبكة

التكوين

تكوين مجموعة نفق الشبكة (VPN) على الوصول الآمن

لتكوين نفق VPN بين Secure Access و Sonicwall

- انتقل إلى مدخل المسؤول الخاص ب Secure Access



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)

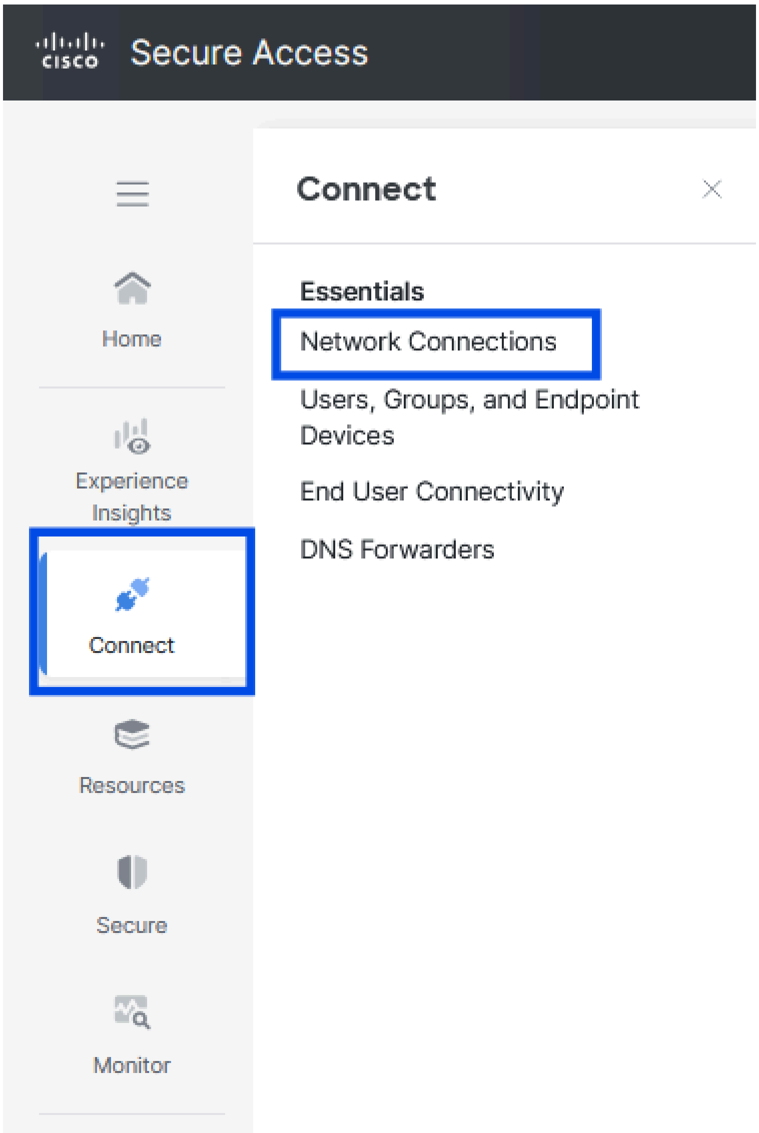
200.03 MB Sent
137.63 MB Increase (last 24 hours)

☑ Branch
☑ RAVPN
☑ Client-based ZTA

☑ Select All

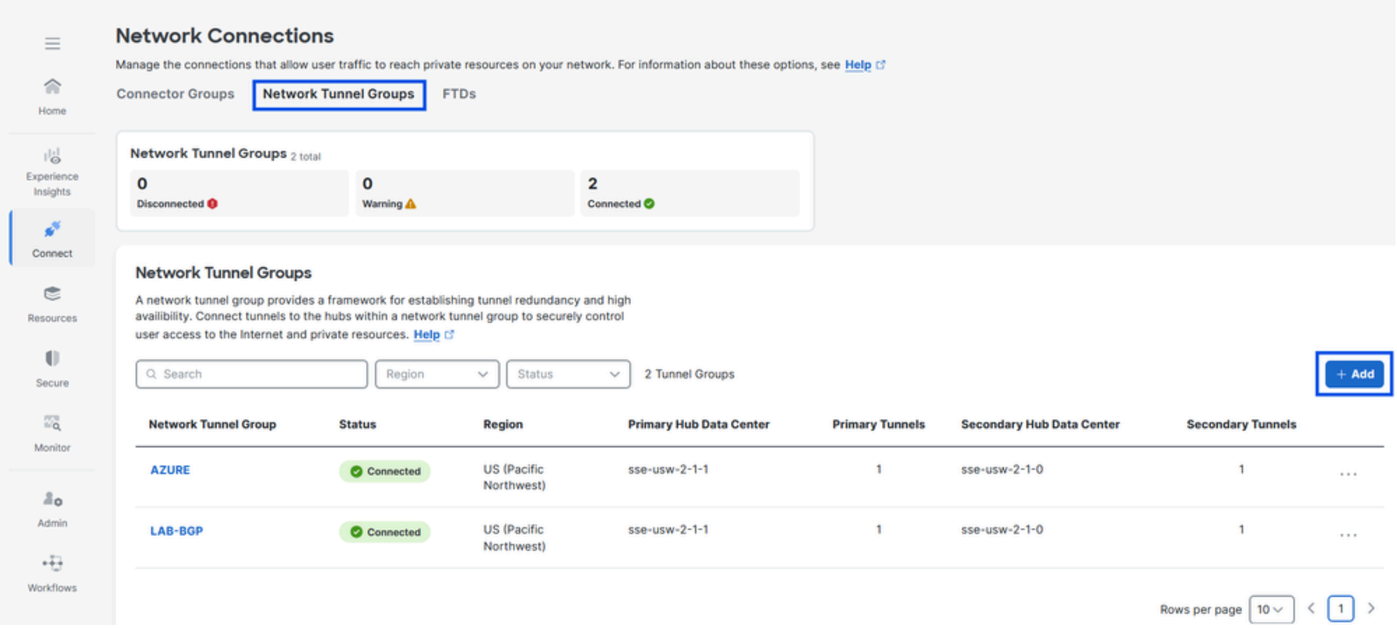
الوصول الآمن - الصفحة الرئيسية

- انقر على توصيل > توصيلات الشبكة



الوصول الآمن - إتصالات الشبكة

- تحت مجموعات أنفاق الشبكة انقر فوق + إضافة



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

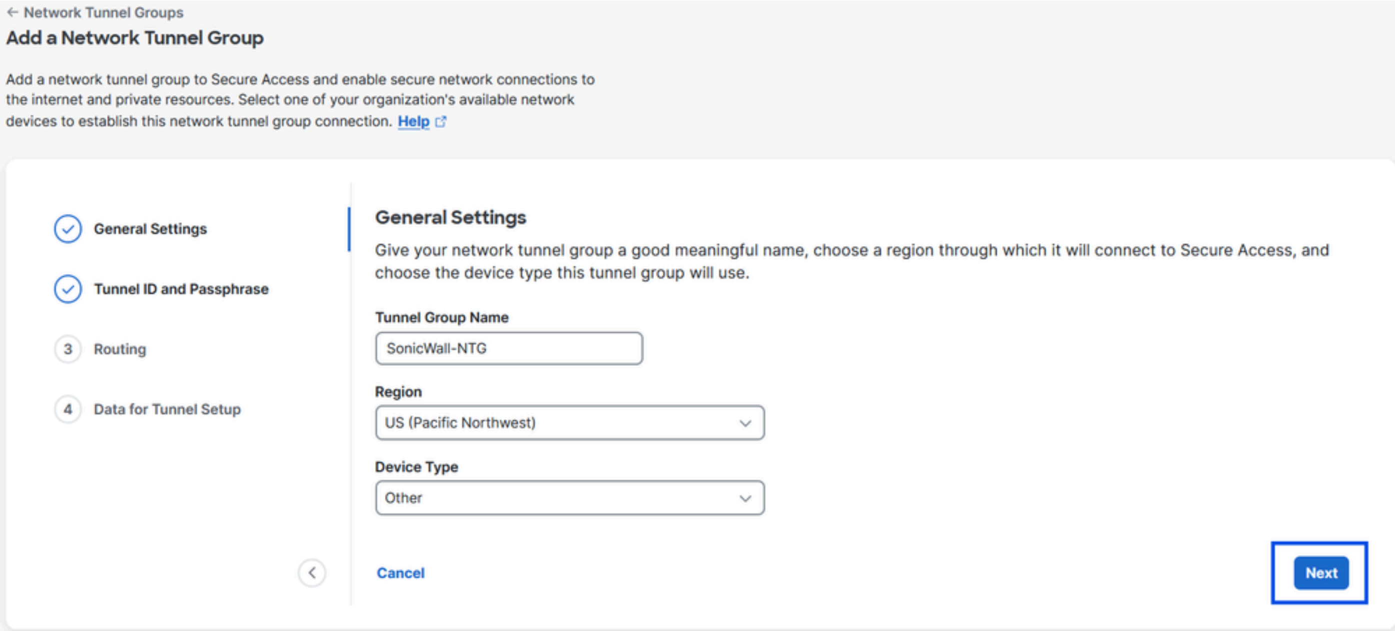
A network tunnel group provides a framework for establishing tunnel redundancy and high availibility. Connect tunnels to the hubs within a network tunnel group to securely control user access to the Internet and private resources. Help

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	...

الوصول الآمن - مجموعات نفق الشبكة

- تكوين اسم مجموعة Tunel والمنطقة ونوع الجهاز
- انقر فوق التالي



← 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

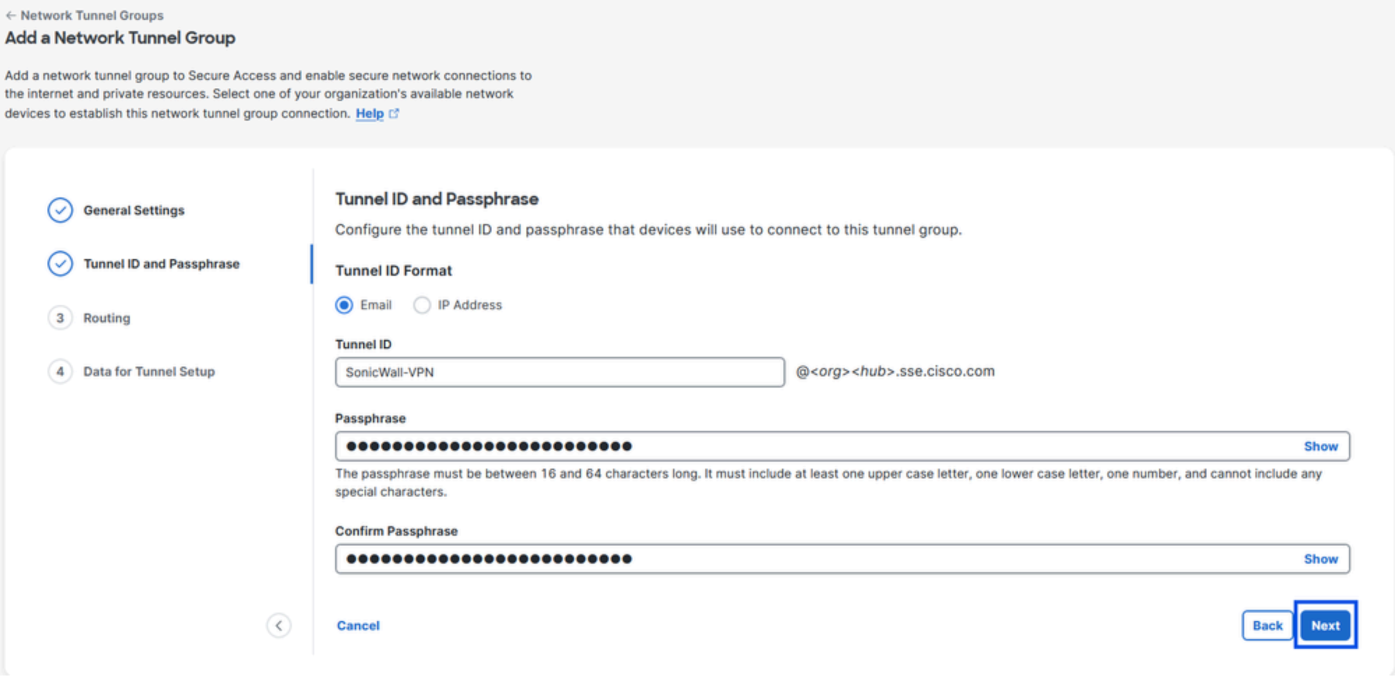
Region: US (Pacific Northwest)

Device Type: Other

الوصول الآمن - مجموعة نفق الشبكة - الإعدادات العامة

ملاحظة: أختر المنطقة الأقرب إلى موقع جدار الحماية.

- تكوين نموذج معرف النفق وعبارة المرور
- انقر فوق التالي



← 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

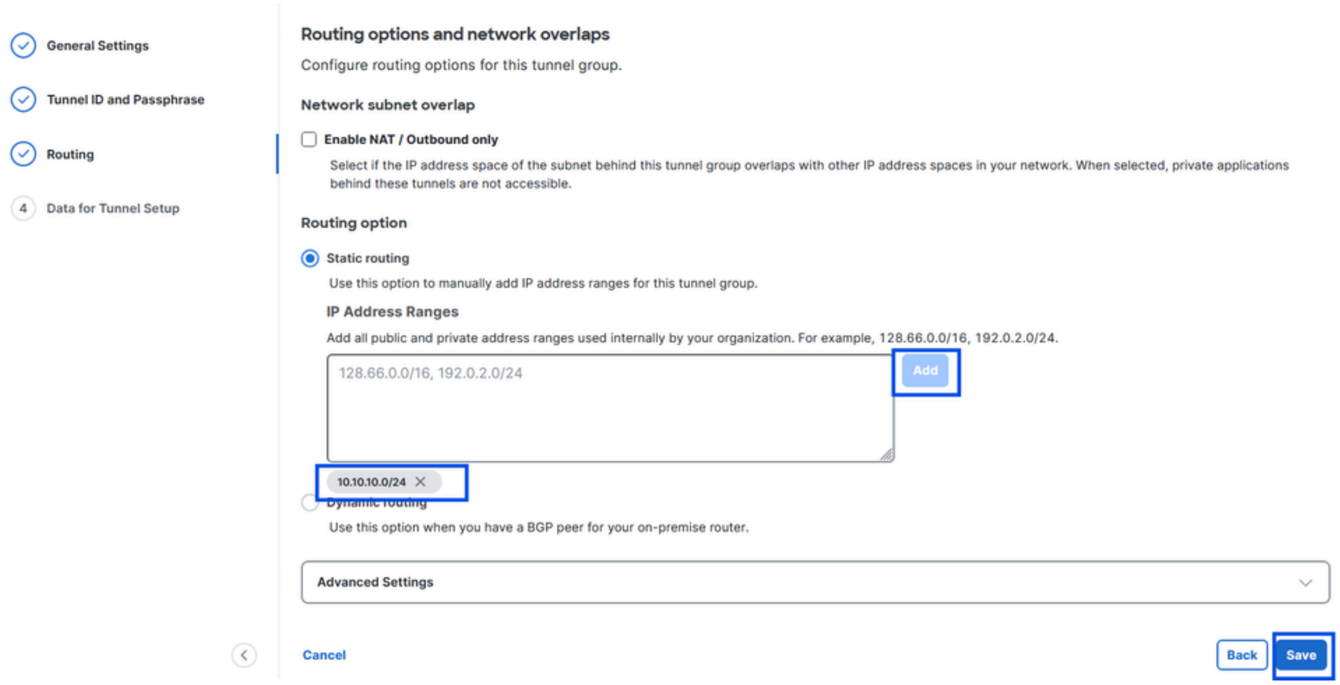
Passphrase: ••••••••••••••••••••••••••

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: ••••••••••••••••••••••••••

الوصول الآمن - معرف النفق عبارة المرور

- قم بتكوين نطاقات عناوين IP أو البيئات المضيفة أو الشبكات الفرعية التي قمت بتكوينها على الشبكة وتريد تمرير حركة المرور من خلال الوصول الآمن
- طقطقة يضيف
- انقر فوق حفظ



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

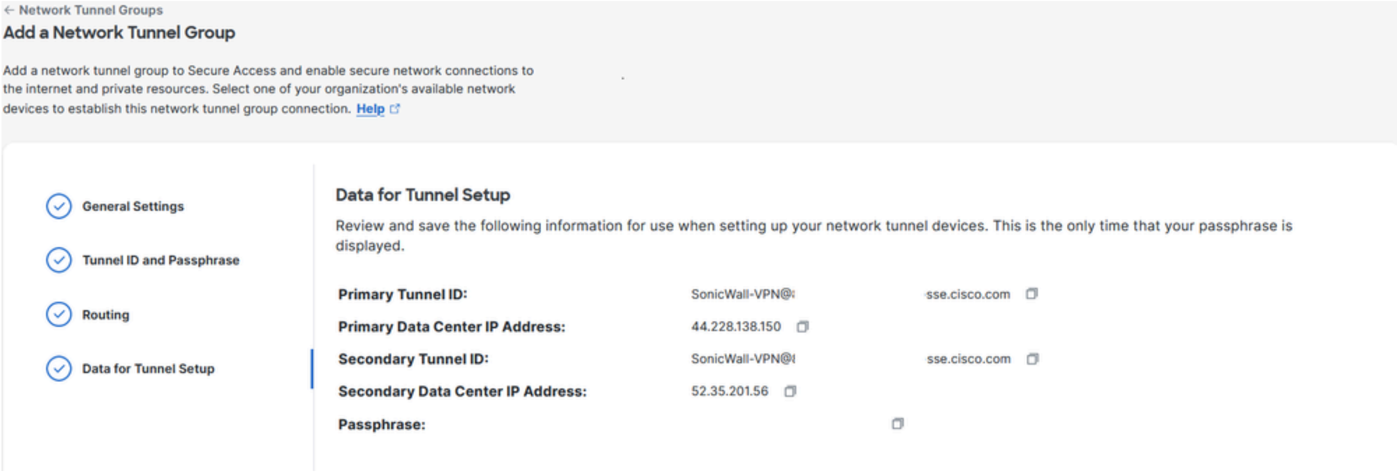
10.10.10.0/24 ✕

○ Dynamic routing

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

الوصول الآمن - مجموعات الأنفاق - خيارات التوجيه

بعد النقر فوق "حفظ"، يتم عرض معلومات حول النفق. يرجى حفظ هذه المعلومات لخطوة التكوين التالية



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:	

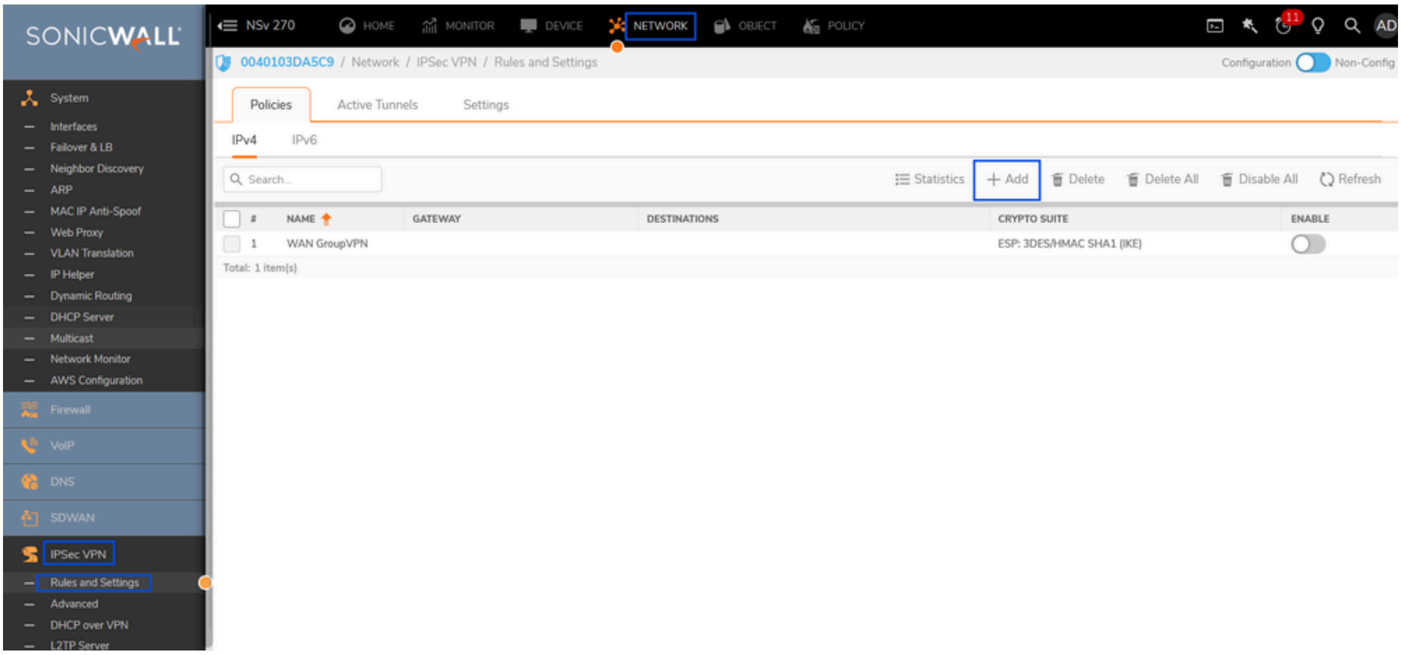
Secure Access - بيانات لإعداد النفق

تكوين النفق على Sonicwall

تكوين النفق - القواعد والإعدادات

انتقل إلى لوحة معلومات Sonicwall.

- الشبكة > IPsec VPN > القواعد والإعدادات
- انقر فوق + إضافة



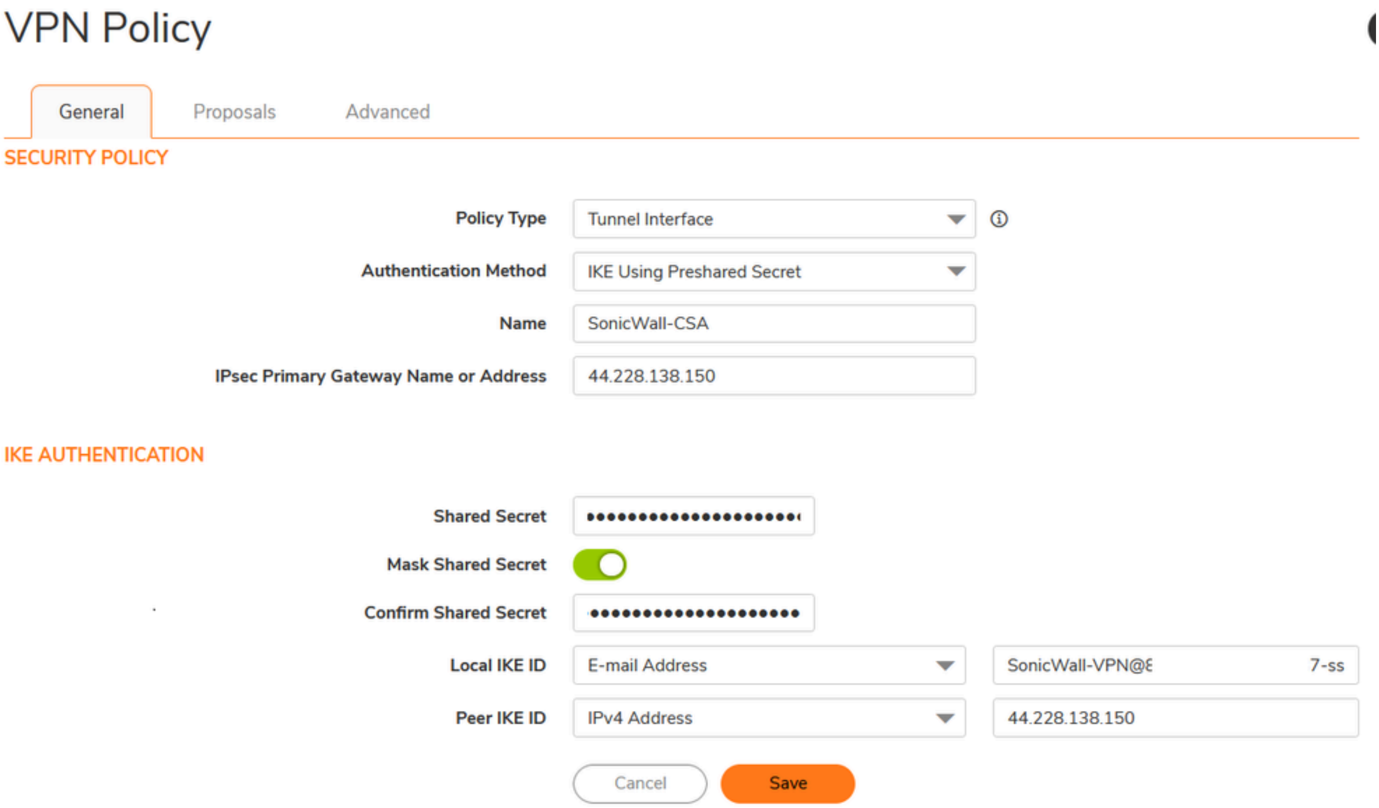
0040103DA5C9 / Network / IPSec VPN / Rules and Settings

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

Total: 1 item(s)

Sonicwall - IPSec VPN - القواعد والإعدادات

- بموجب سياسة الشبكة الخاصة الظاهرية (VPN)، املأ تكوين الشبكة الخاصة الظاهرية (VPN) استنادا إلى بيانات النفق من الوصول الآمن [معلمات IPSec المدعومة]



VPN Policy

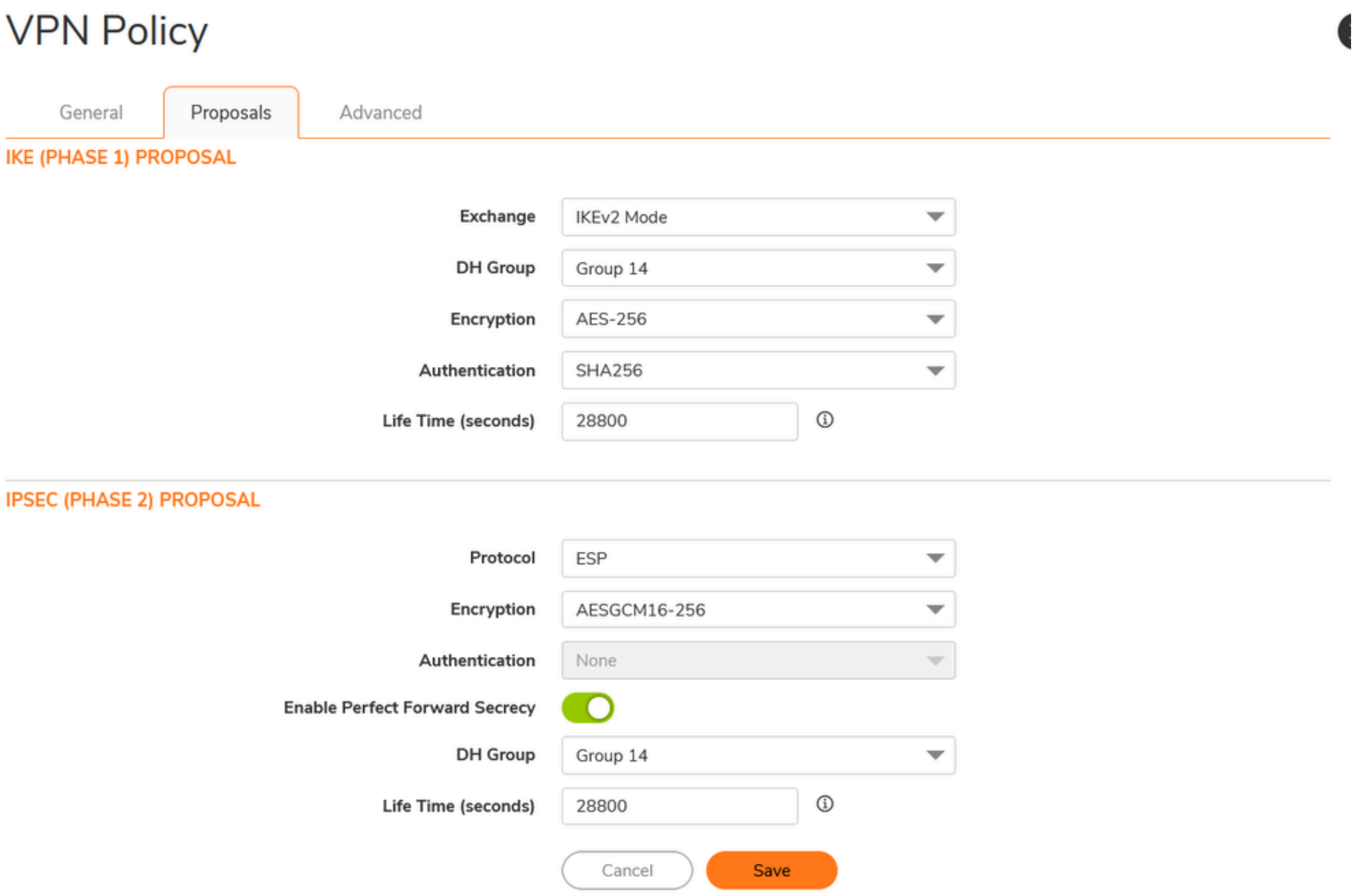
General | Proposals | Advanced

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



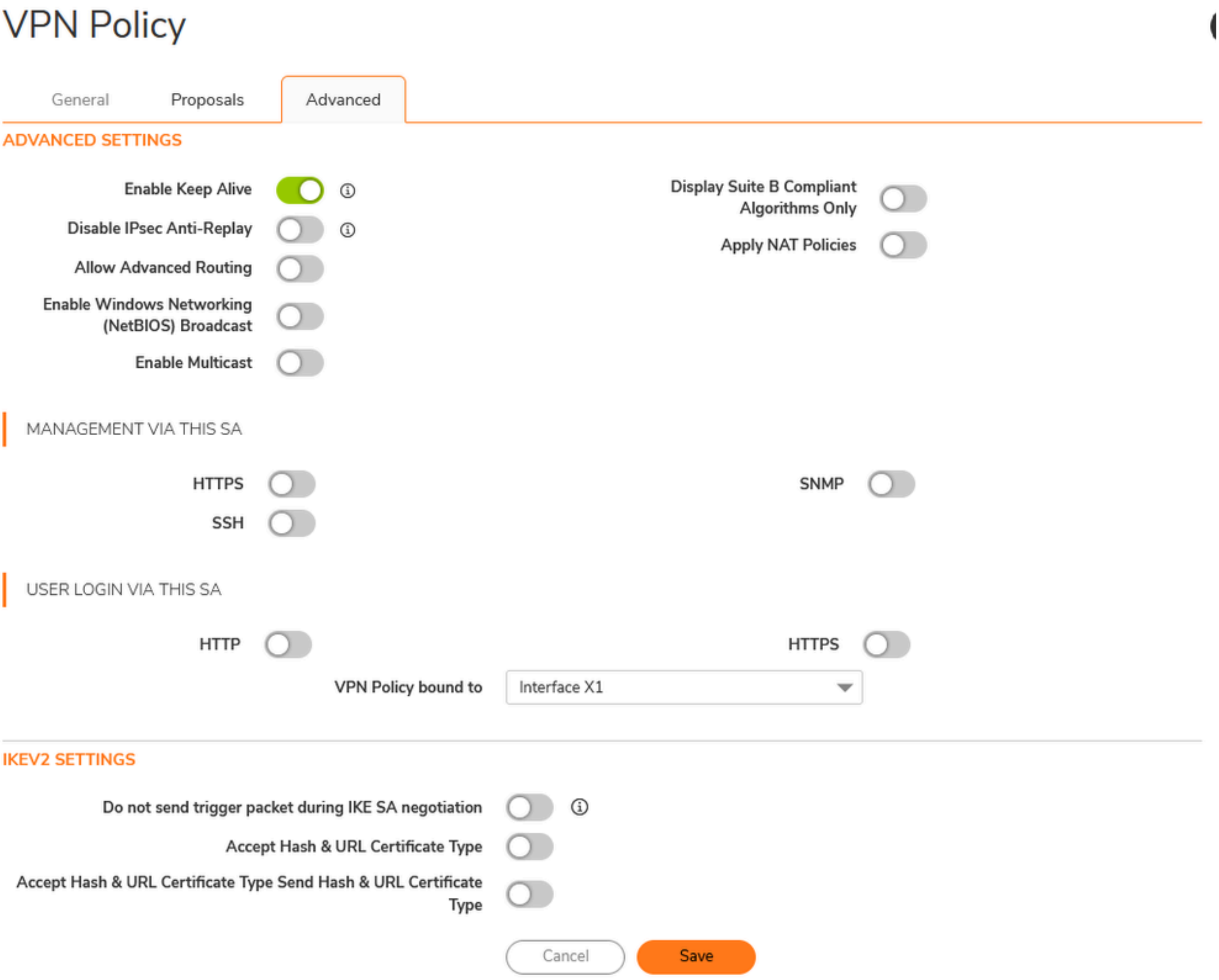
VPN Policy

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

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 ○

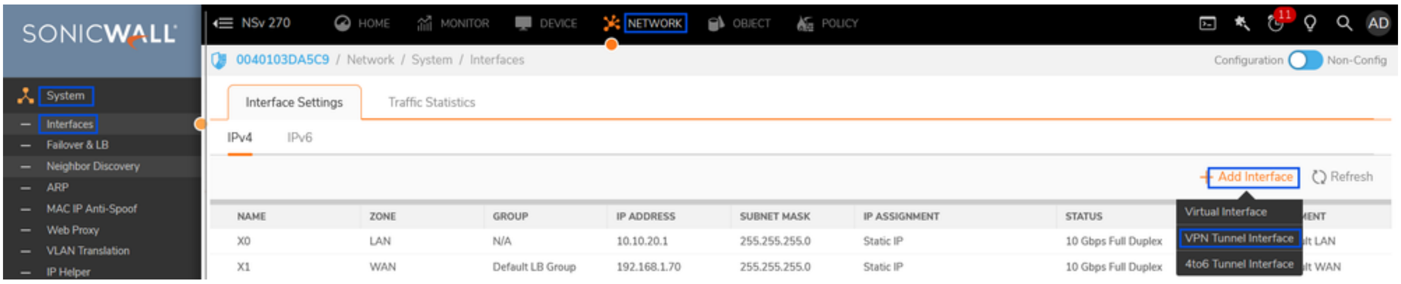
Accept Hash & URL Certificate Type Send Hash & URL Certificate Type ○

- انقر على حفظ

إضافة واجهة نفق VPN

انتقل إلى لوحة معلومات Sonicwall.

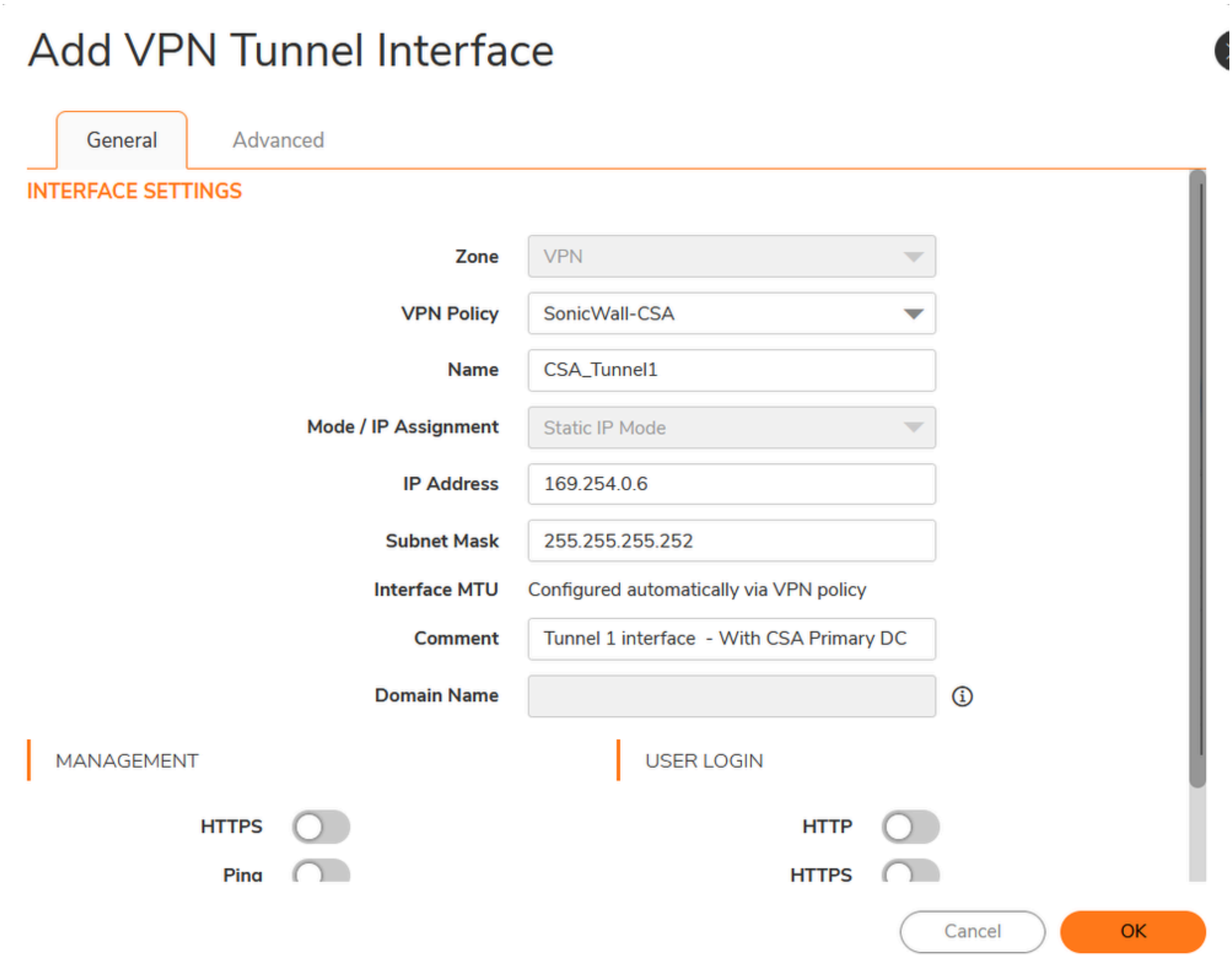
- الشبكة >النظام >الواجهة
- انقر على + إضافة واجهة
- تحديد واجهة نفق VPN



0040103DA5C9 / Network / System / Interfaces

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 - الواجهات



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	

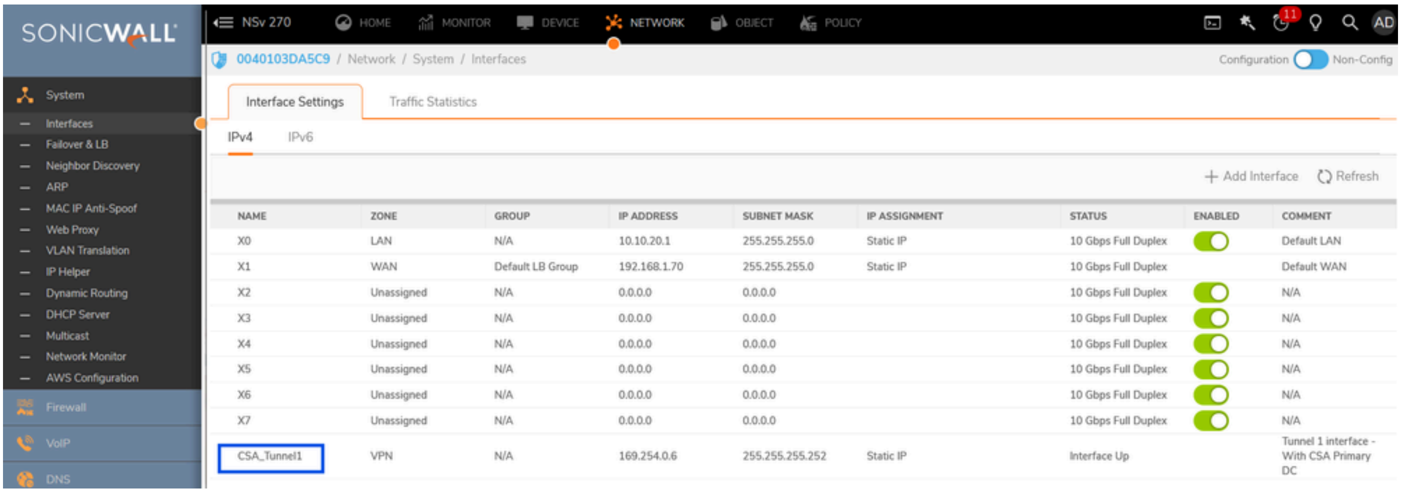
MANAGEMENT

HTTPS ○
Ping ○

USER LOGIN

HTTP ○
HTTPS ○

- ثم انقر فوق موافق



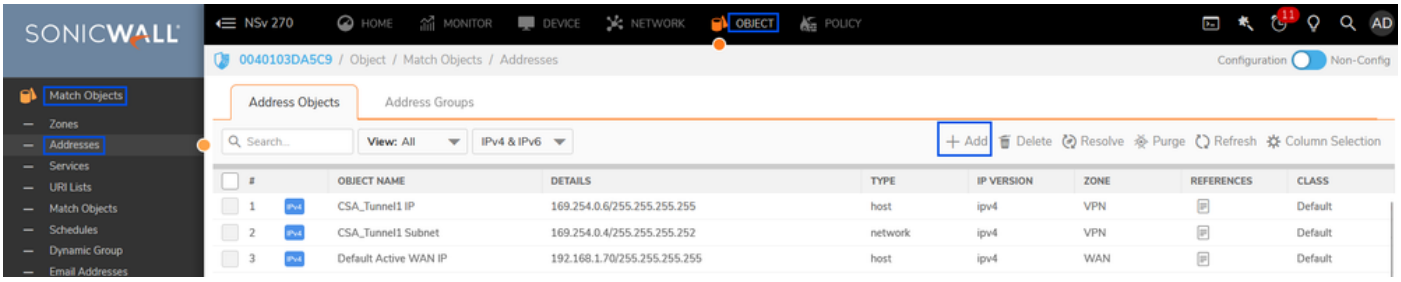
NAME	ZONE	GROUP	IP ADDRESS	SUBNET MASK	IP ASSIGNMENT	STATUS	ENABLED	COMMENT
X0	LAN	N/A	10.10.20.1	255.255.255.0	Static IP	10 Gbps Full Duplex	✓	Default LAN
X1	WAN	Default LB Group	192.168.1.70	255.255.255.0	Static IP	10 Gbps Full Duplex		Default WAN
X2	Unassigned	N/A	0.0.0.0	0.0.0.0		10 Gbps Full Duplex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

إضافة كائن شبكة ومجموعات

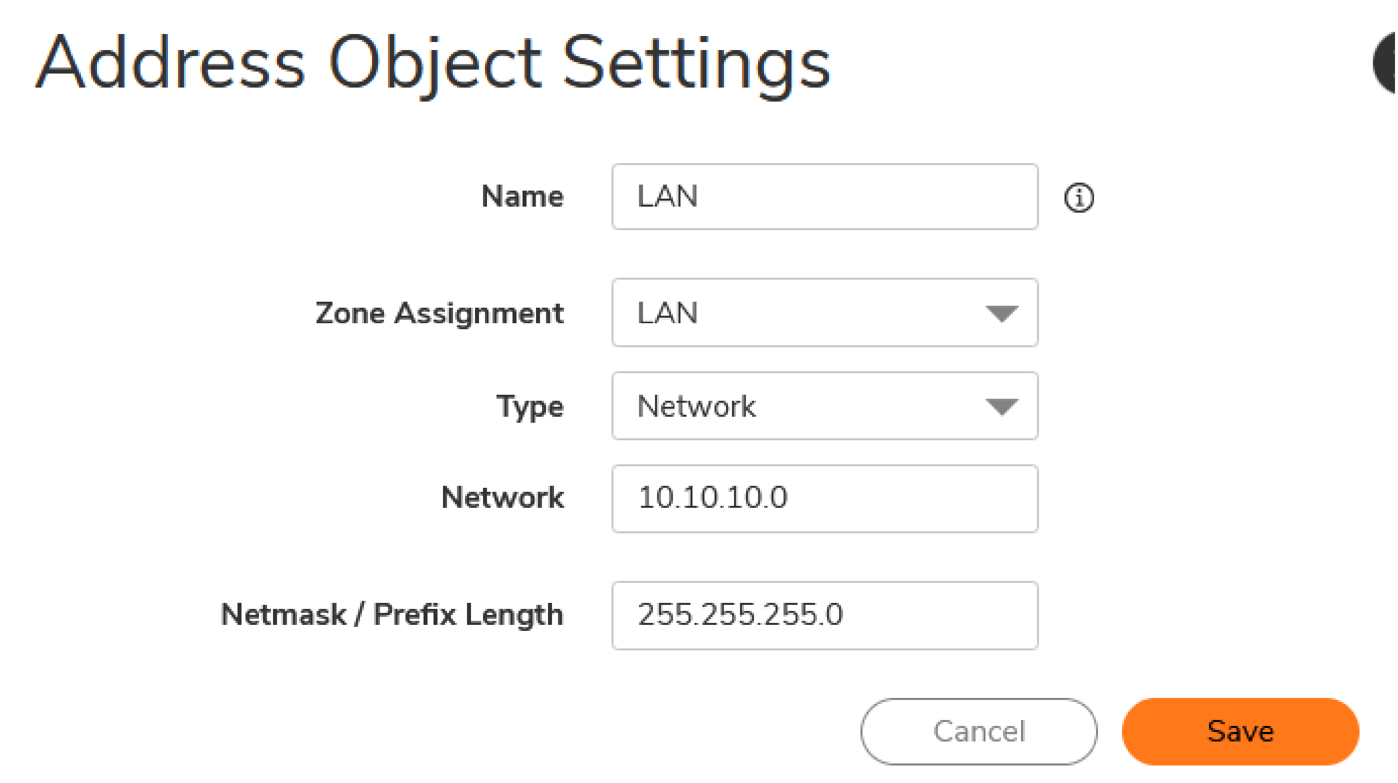
انتقل إلى لوحة معلومات Sonicwall.

- كائن >مطابقة كائنات >عناوين
- كائنات العنوان
- انقر فوق +إضافة



#		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

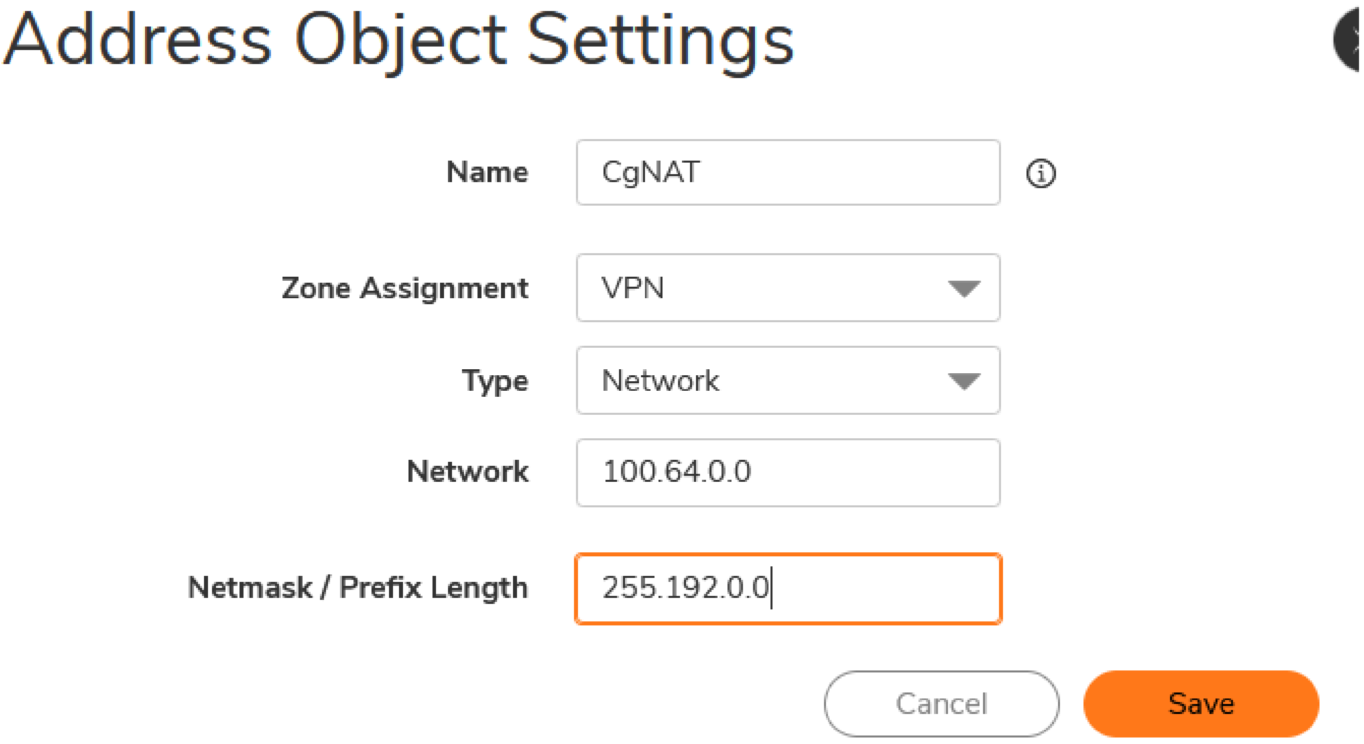
SONICWALL - كائنات عنوان الكائن



Address Object Settings

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

- انقر فوق حفظ



Address Object Settings

Name: CgNAT

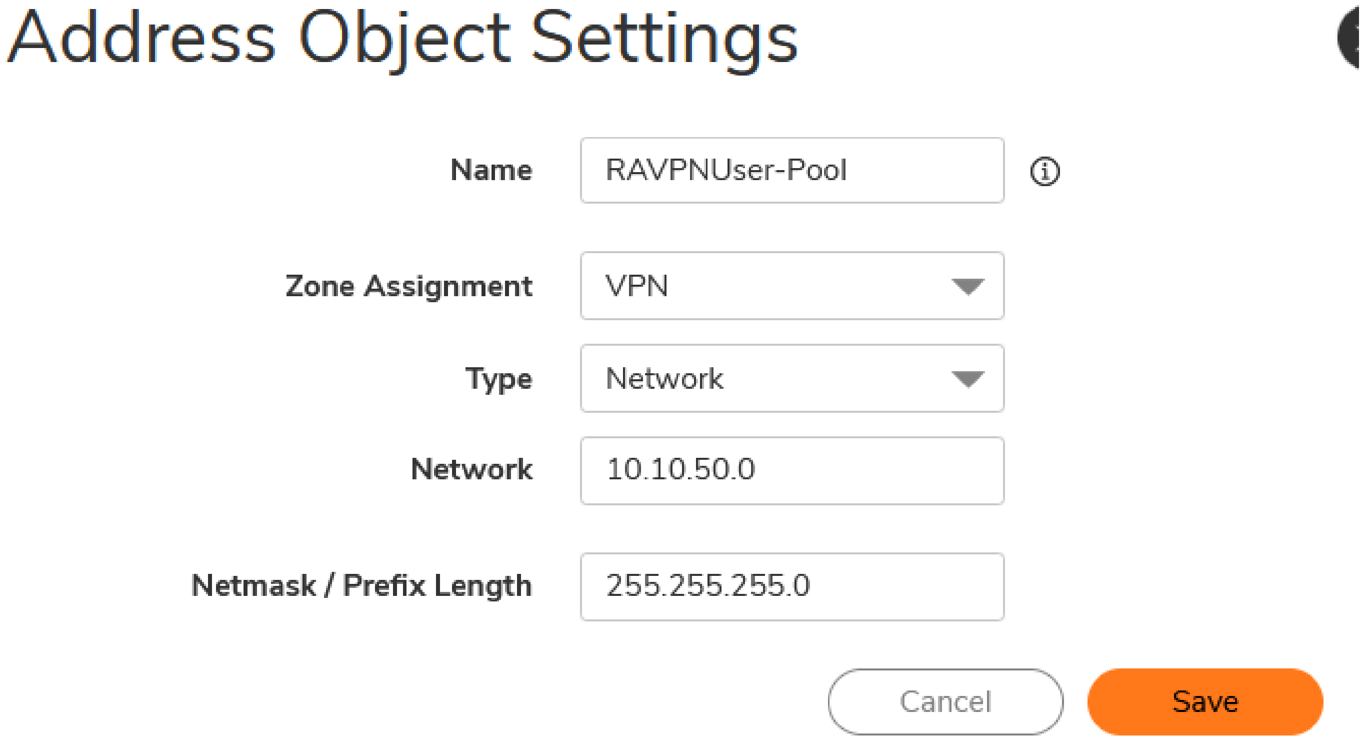
Zone Assignment: VPN

Type: Network

Network: 100.64.0.0

Netmask / Prefix Length: 255.192.0.0

- انقر فوق حفظ



Address Object Settings

Name: RAVPNUser-Pool

Zone Assignment: VPN

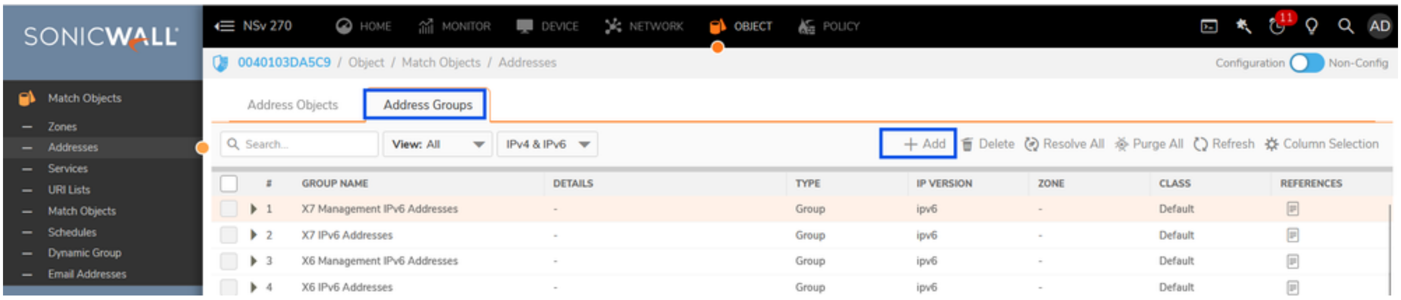
Type: Network

Network: 10.10.50.0

Netmask / Prefix Length: 255.255.255.0

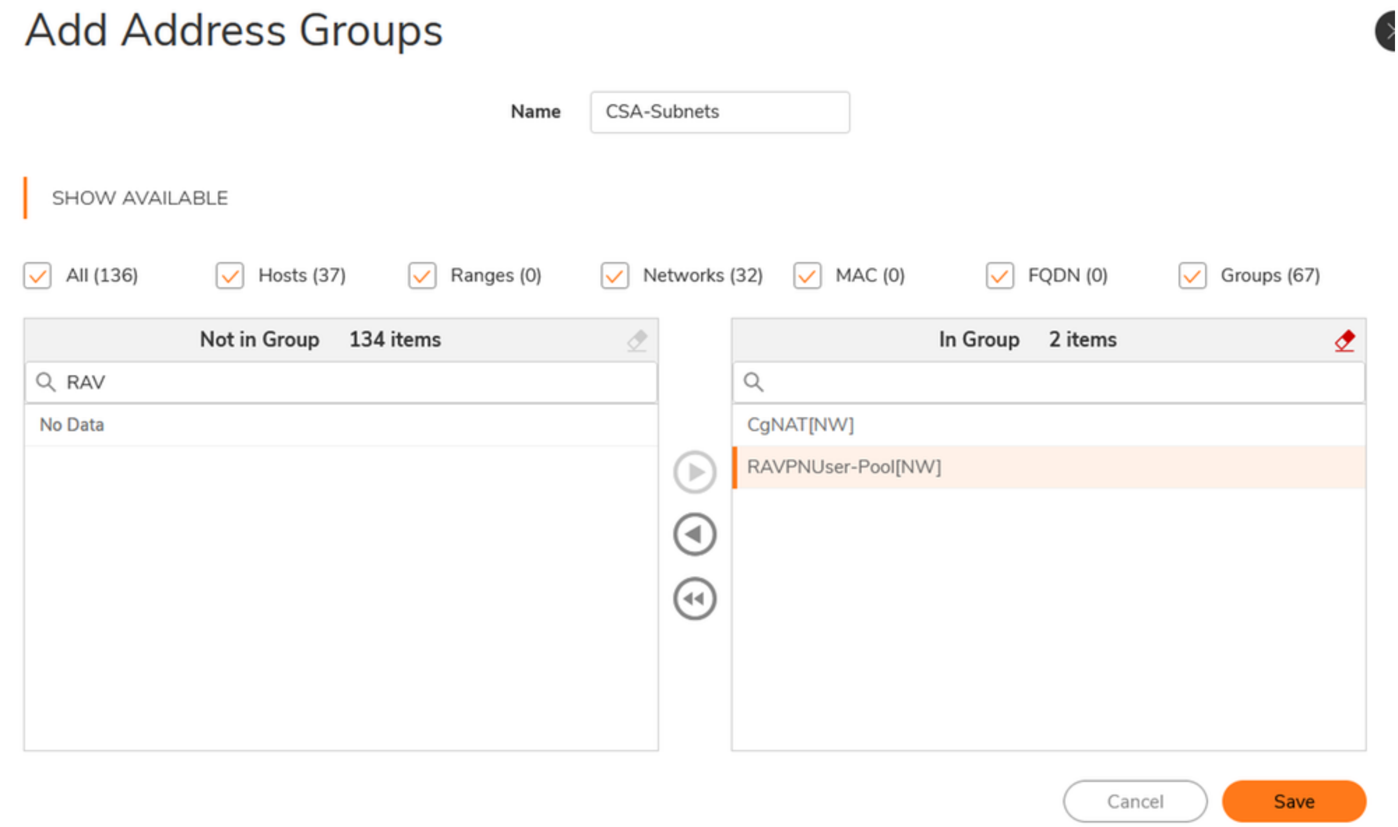
- انقر فوق حفظ

- إنشاء مجموعات عناوين
- انقر فوق +إضافة
- حدد كائن العنوان وقم بإضافتهم إلى مجموعات العناوين



#	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 - مجموعات عناوين الكائنات



Add Address Groups

Name: CSA-Subnets

SHOW AVAILABLE

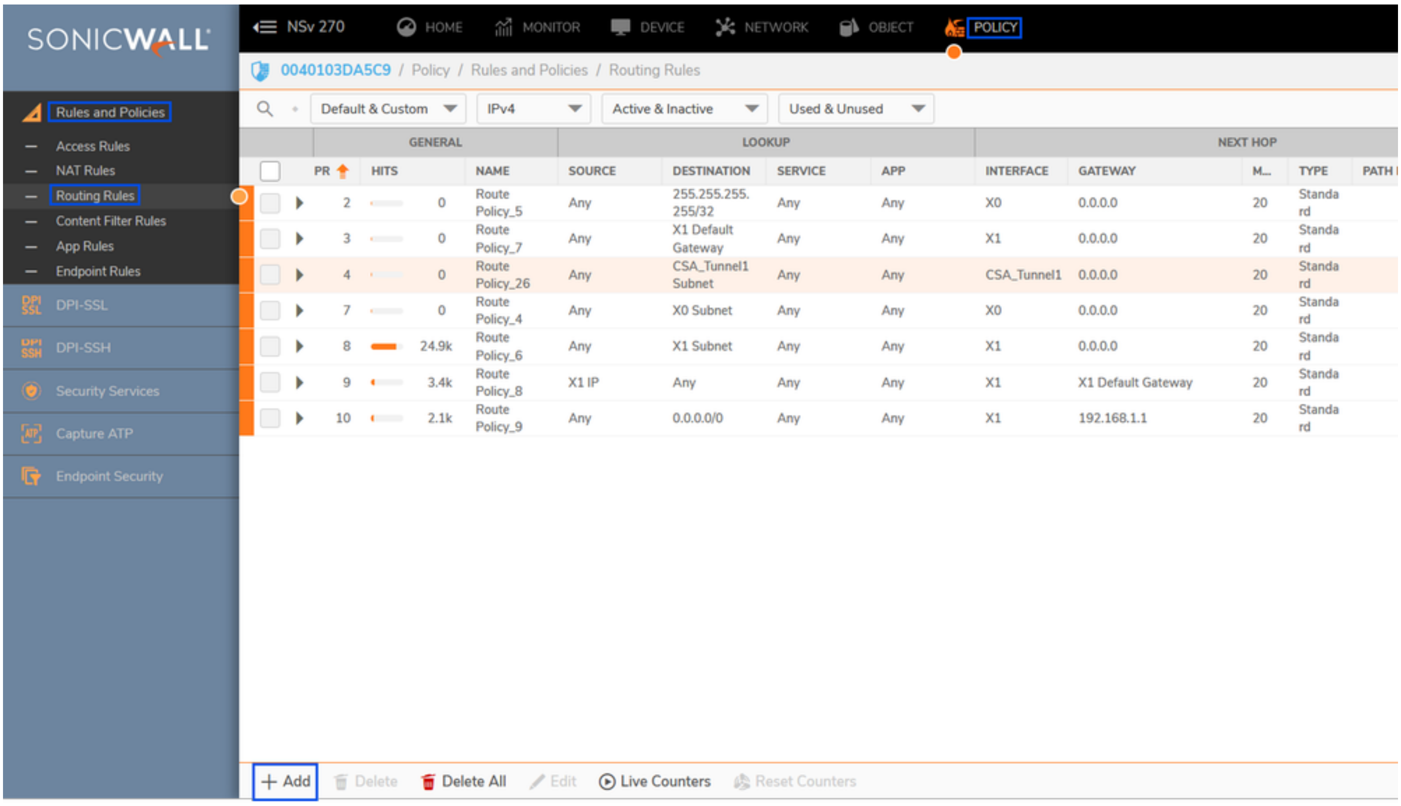
☑ All (136) ☑ Hosts (37) ☑ Ranges (0) ☑ Networks (32) ☑ MAC (0) ☑ FQDN (0) ☑ Groups (67)

- انقر فوق حفظ

إضافة مسار

انتقل إلى لوحة معلومات Sonicwall.

- السياسة>القواعد والسياسات >قواعد التوجيه
- انقر فوق + إضافة



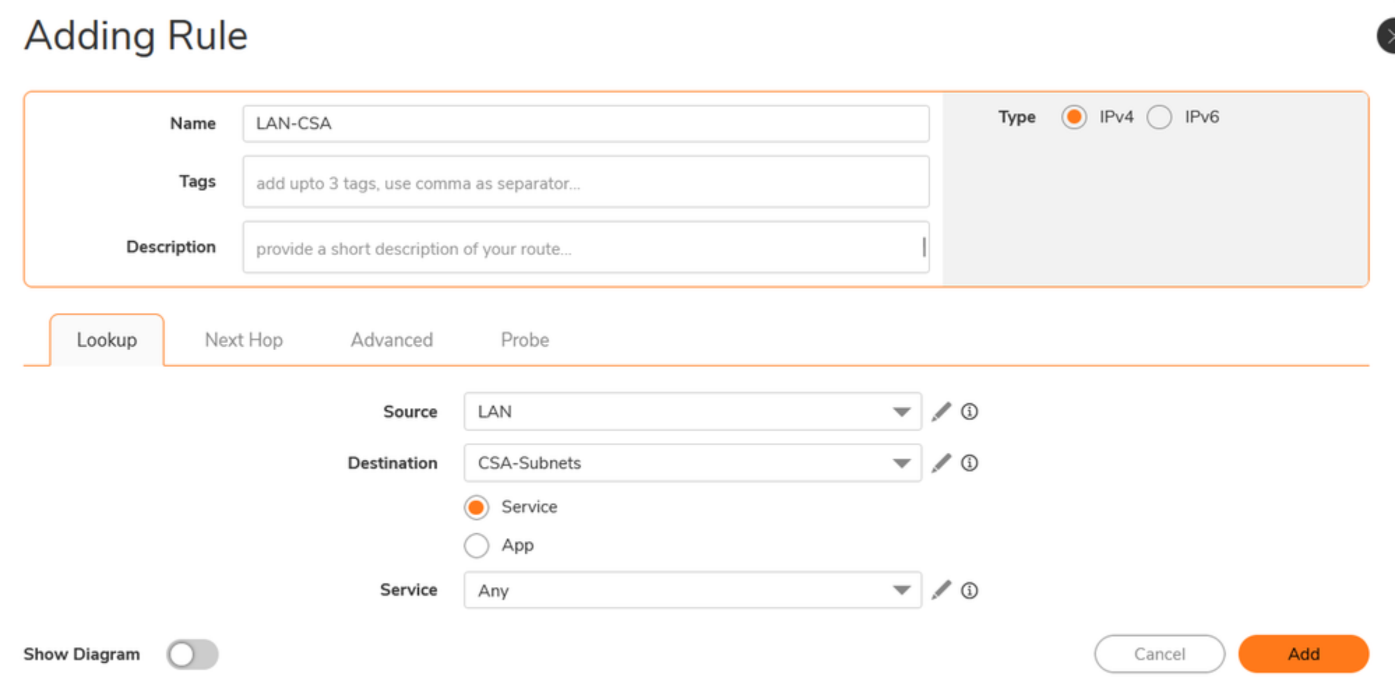
0040103DA5C9 / Policy / Rules and Policies / Routing Rules

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

GENERAL			LOOKUP				NEXT HOP				
PR	HITS	NAME	SOURCE	DESTINATION	SERVICE	APP	INTERFACE	GATEWAY	M...	TYPE	PATH I
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 - قواعد التوجيه

- إضافة قاعدة توجيه



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

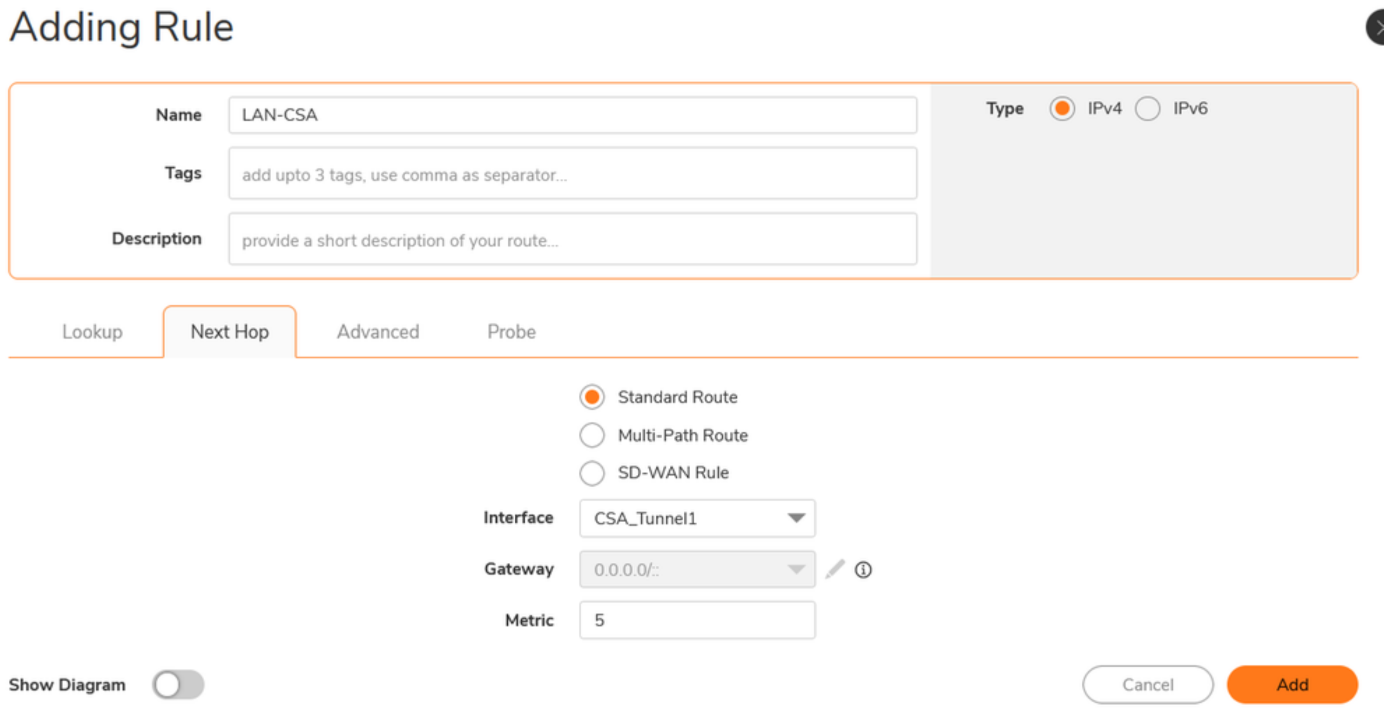
Source: LAN

Destination: CSA-Subnets

● Service
○ App

Service: Any

Show Diagram ○



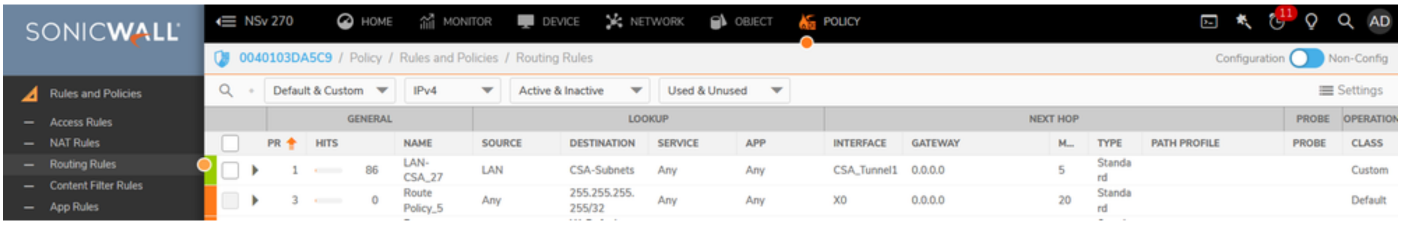
Adding Rule

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

- انقر فوق + إضافة



0040103DA5C9 / Policy / Rules and Policies / Routing Rules

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

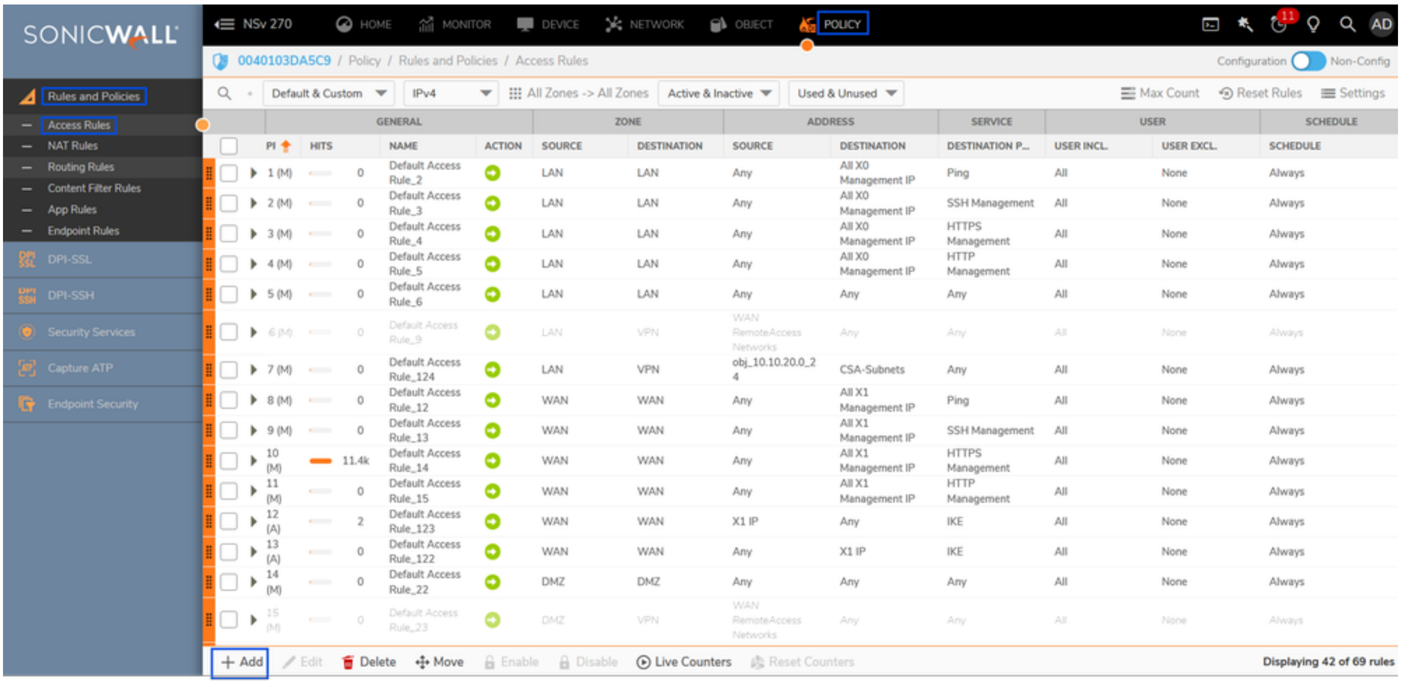
GENERAL			LOOKUP				NEXT HOP					PROBE	OPERATION
PR	HITS	NAME	SOURCE	DESTINATION	SERVICE	APP	INTERFACE	GATEWAY	M...	TYPE	PATH PROFILE	PROBE	CLASS
1	86	LAN-CSA_27	LAN	CSA-Subnets	Any	Any	CSA_Tunnel1	0.0.0.0	5	Standard			Custom
3	0	Route Policy_5	Any	255.255.255.255/32	Any	Any	X0	0.0.0.0	20	Standard		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

Sonicwall - قواعد التوجيه

إضافة قواعد الوصول

انتقل إلى لوحة معلومات Sonicwall.

- السياسة>القواعد والسياسات>قواعد الوصول
- انقر فوق + إضافة



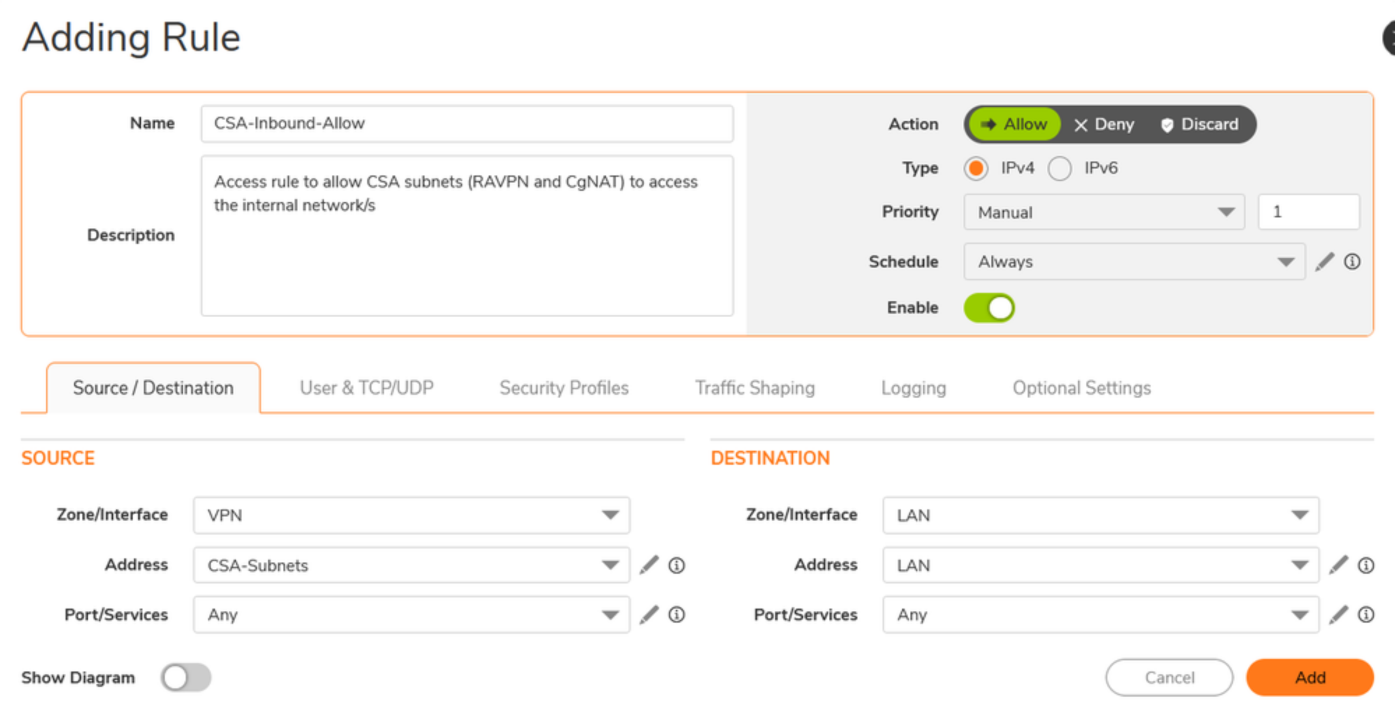
0040103DA5C9 / Policy / Rules and Policies / Access Rules

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 - قواعد الوصول



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	On

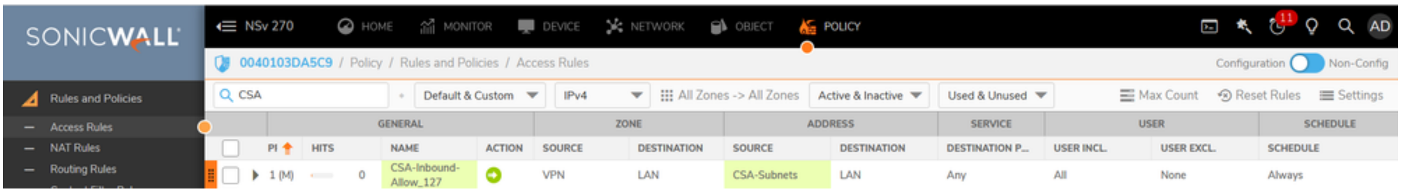
SOURCE

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

DESTINATION

Zone/Interface	LAN
Address	LAN
Port/Services	Any

- انقر فوق +إضافة



0040103DA5C9 / Policy / Rules and Policies / Access Rules

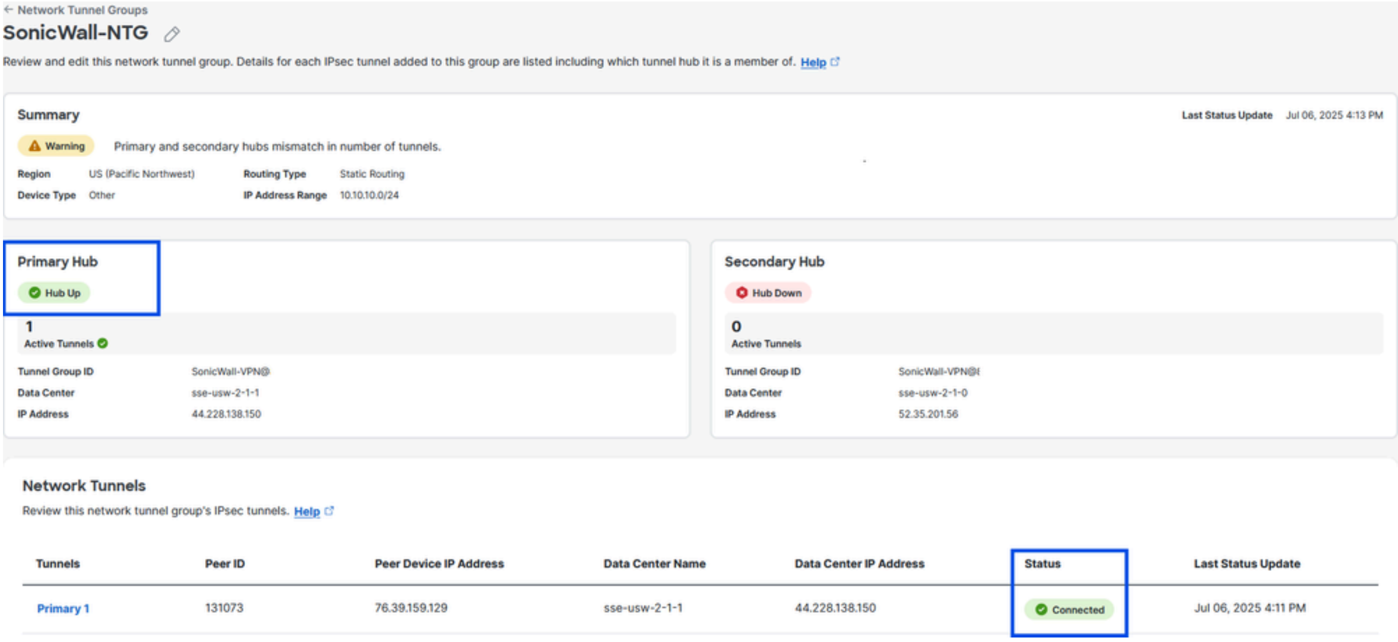
CSA | Default & Custom | IPv4 | All Zones -> All Zones | Active & Inactive | Used & Unused

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 - قواعد الوصول

التحقق من الصحة

- حالة النفق على الوصول الآمن



← 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

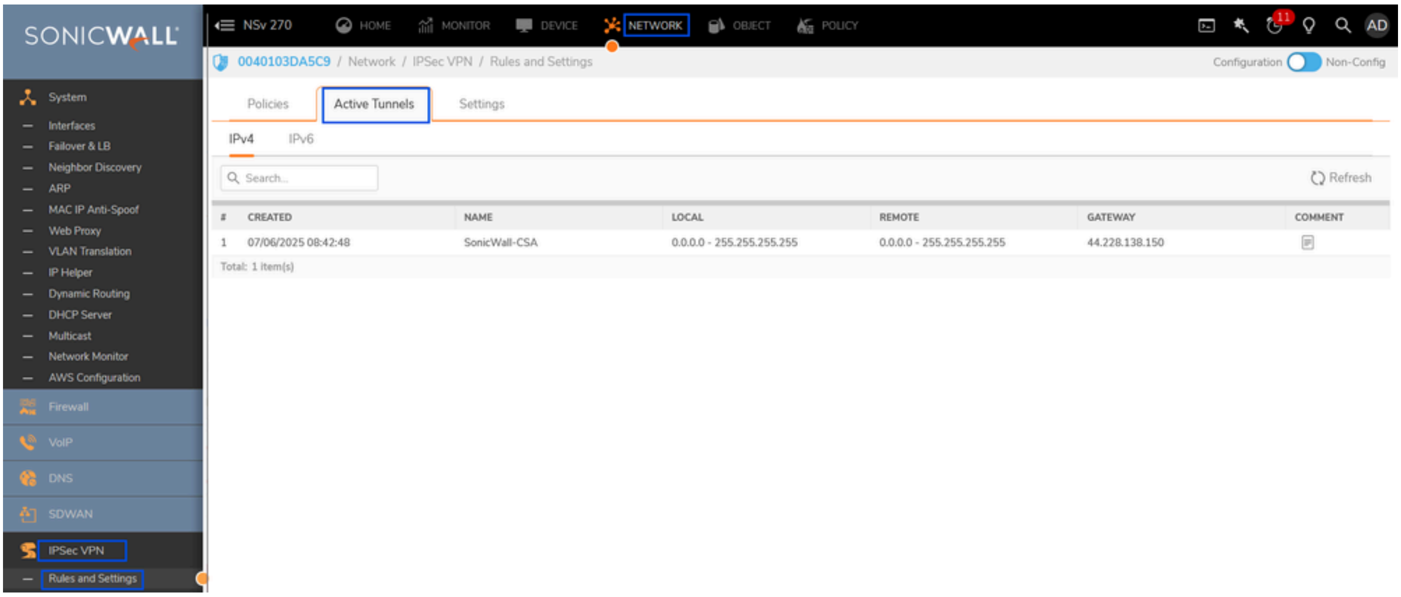
Network Tunnels

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

الوصول الآمن - مجموعة نفق الشبكة - حالة VPN

- حالة النفق على جدار حماية 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 - حالة IPSec VPN

يمكنك تنفيذ نفس العملية لتكوين النفق بين مركز البيانات الثانوي ل Secure Access و Sonicwall

والآن، يتم تشغيل النفق على Secure Access و Sonicwall، ويمكنك مواصلة تكوين الوصول إلى الموارد الخاصة عبر RA-VPN أو ZTA المستندة إلى Broswer أو ZTA المستندة إلى العميل على لوحة معلومات الوصول الآمن

استكشاف الأخطاء وإصلاحها

كمبيوتر المستخدم

- تحقق من قدرة المستخدم على الاتصال/التسجيل إلى RAVPN/ZTNA بنجاح أو لا. وإذا لم تكن هناك مساحة، فعليك أستكشاف الأخطاء وإصلاحها بشكل إضافي بسبب فشل اتصال مستوى التحكم.
- تحقق من أن الشبكة التي يحاول المستخدم الوصول إليها من المفترض أن تمر عبر نفق RAVPN أو ZTNA . إذا لم تكن هناك مساحة، فتحقق من التكوين على وحدة الاستقبال والبث .

الوصول الآمن

- تحقق من تكوين توجيه حركة المرور على ملف تعريف اتصال RAPN لتأكيد تكوين شبكة الوجهة لإرسالها عبر النفق لتأمين الوصول.
- تحقق من تحديد المورد الخاص باستخدام البروتوكول/المنافذ الصالحة وتم التحقق من آليات اتصال ZTNA/RAVPN.
- تحقق من تكوين نهج الوصول للسماح لمستخدم RAPN/ZTNA بالوصول إلى شبكة الموارد الخاصة ووضعها في ترتيب بعدم وجود قاعدة أخرى لها الأسبقية لحظر حركة المرور.
- تحقق من أن نفق IPSec عبارة عن وصول UP وآمن يظهر مسارات عميل صالحة عبر التوجيه الثابت الذي يغطي المورد الخاص الذي يحاول المستخدم الوصول إليه.

سونيكوول

- تحقق من أن نفق IPSec أعلى أم لا (IKE & IPSec SA) .
- تحقق من الإعلان بشكل صحيح عن توجيه العميل أو موجهاته.
- تحقق من وصول مصادر حركة المرور من مستخدم RAPN/ZTNA الموجه إلى المورد الخاص خلف Sonicwall إلى جدار حماية Sonicwall عبر النفق من خلال التقاط الحزم على Sonicwall.
- تحقق من حركة المرور التي وصلت إلى المورد الخاص والاستجابة إلى عميل RAVPN/ZTNA أو لا. إذا كانت نعم، فتحقق من أن الحزم تصل إلى واجهة Sonicall X0 (LAN).
- تحقق من قيام Sonicwall بإعادة توجيه حركة مرور البيانات المرتجعة من خلال نفق IPSec نحو الوصول الآمن.

معلومات ذات صلة

- [الدعم الفني والتنزيلات من Cisco]()
- [مركز تعليمات الوصول الآمن من Cisco]()
- [الوحدة النمطية Zero Trust Access Module]()
- [أستكشاف أخطاء الوصول الآمن وإصلاحها خدمة التسجيل لا تستجيب. اتصل بمكتب مساعدة تقنية المعلومات]()

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية
والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم
بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما
هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco
Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى
المستند الإنجليزي الأصلي (الرابط متوفر).