Sicheren Zugriff mit Sonicwall Firewall konfigurieren

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration eines IPsec-VTI-Tunnels zwischen dem sicheren Zugriff auf die Sonicwall-Firewall mithilfe von statischem Routing beschrieben.

Voraussetzungen

- Konfiguration der Benutzerbereitstellung
- Konfiguration der ZTNA SSO-Authentifizierung
- Konfigurieren des sicheren Remotezugriff-VPN

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Sonicwall-Firewall (NSv270 - SonicOSX 7.0.1)

- Sicherer Zugriff
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA
- Clientless-ZTNA

Verwendete Komponenten

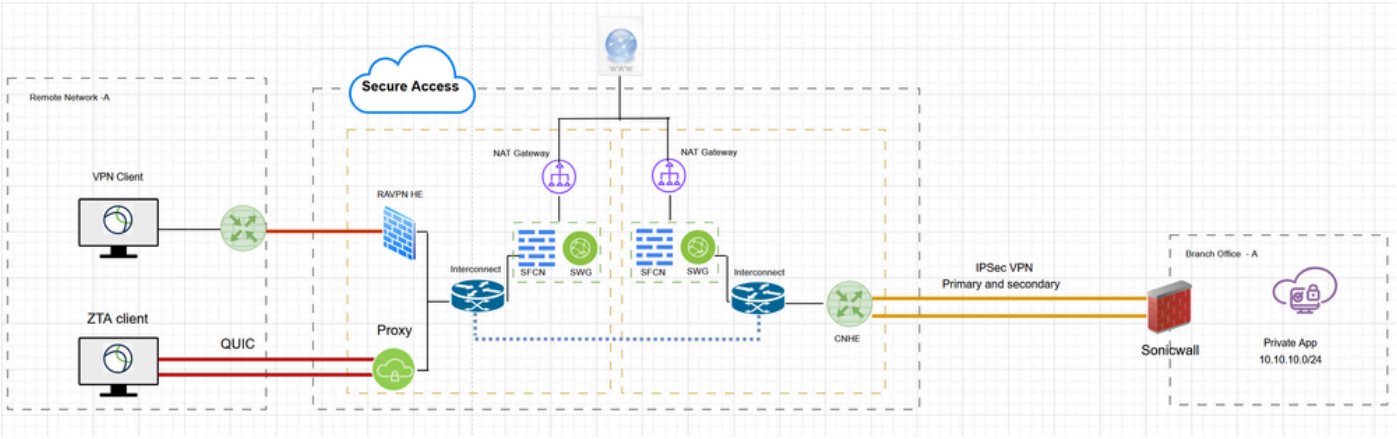
Die Informationen in diesem Dokument basieren auf:

- Sonicwall-Firewall (NSv270 - SonicOSX 7.0.1)
- Sicherer Zugriff
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Netzwerkdiagramm



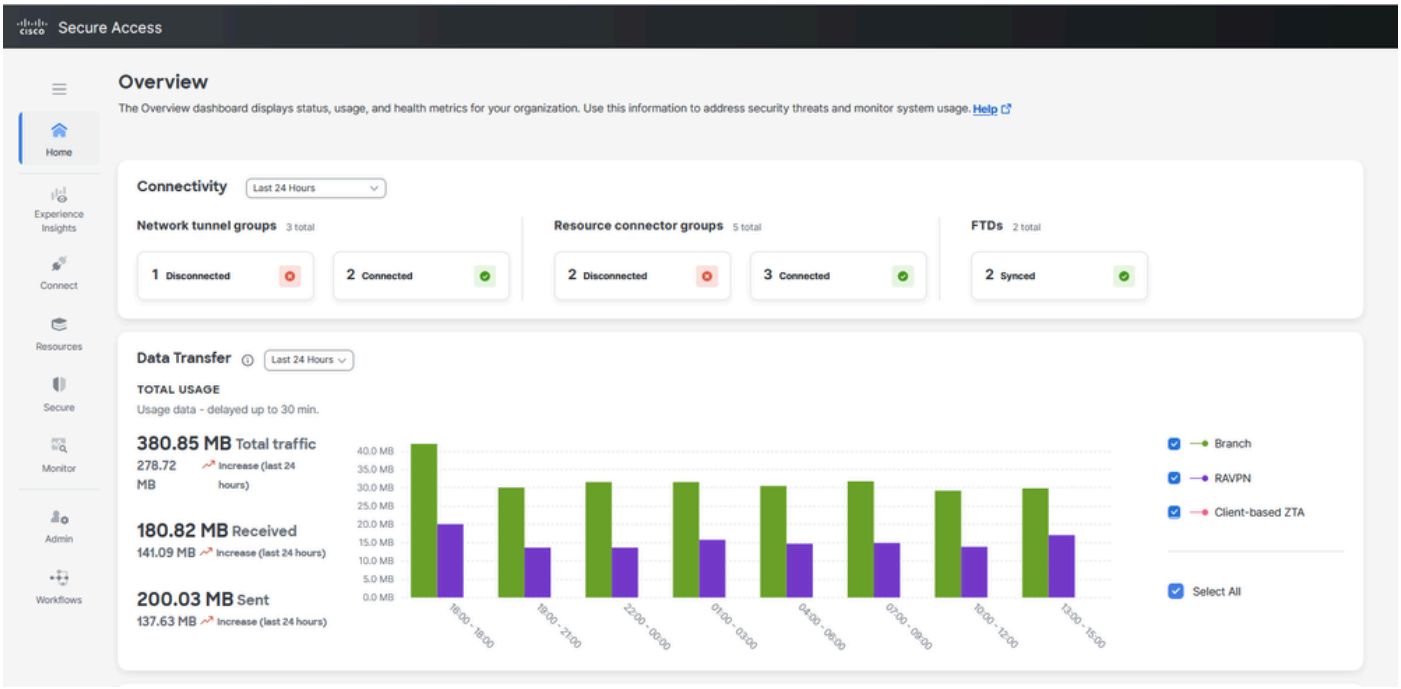
Netzwerkdiagramm

Konfigurieren

Konfigurieren der Netzwerk-Tunnelgruppe (VPN) für sicheren Zugriff

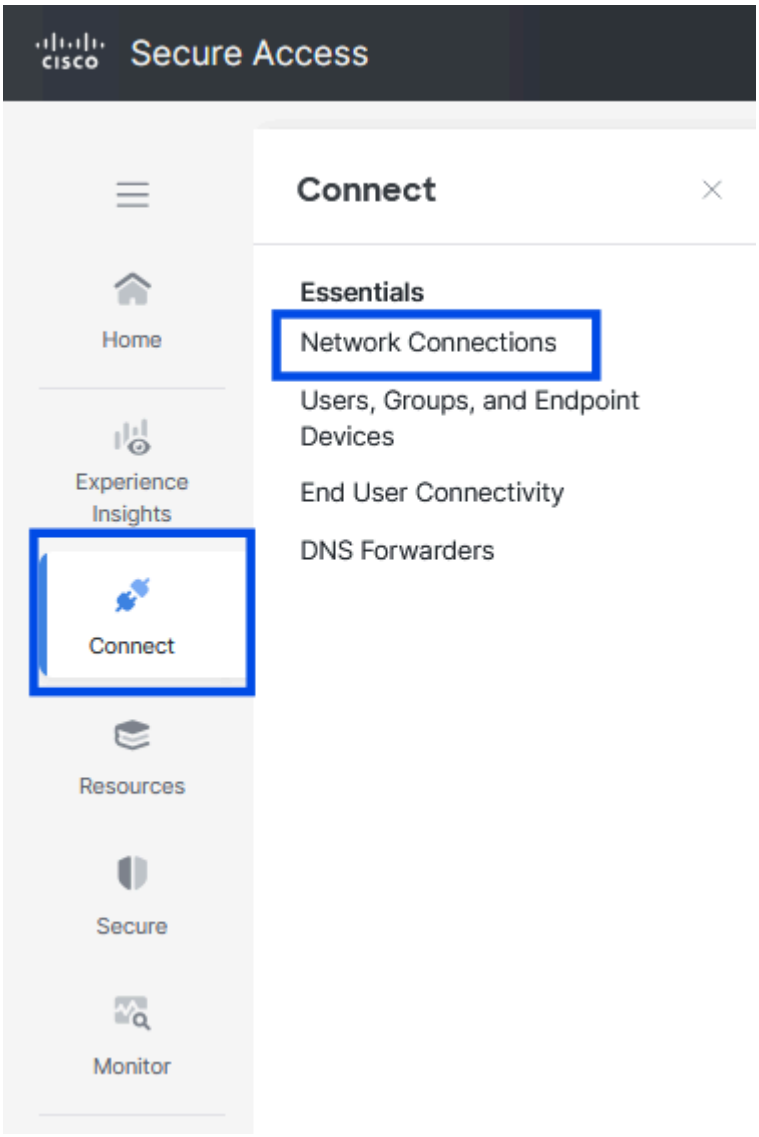
Konfiguration eines VPN-Tunnels zwischen sicherem Zugriff und Sonicwall

- Navigieren Sie zum Admin-Portal des sicheren Zugriffs.



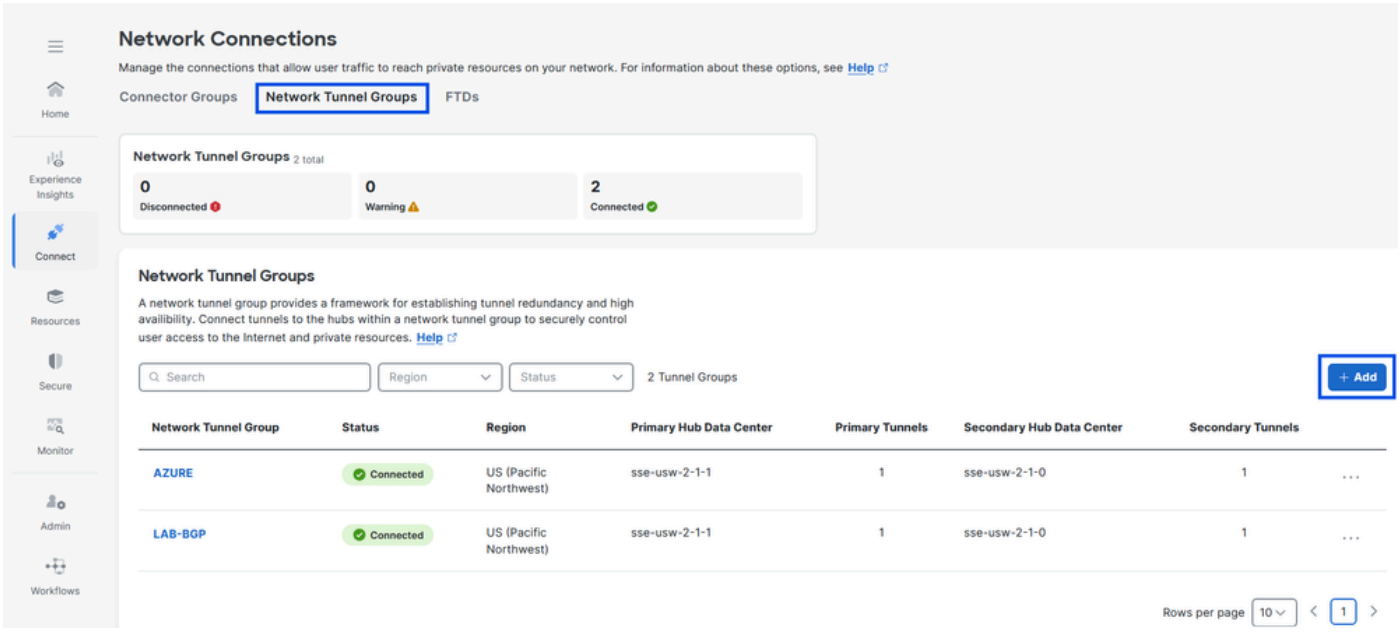
Sicherer Zugriff - Hauptseite

- Klicken Sie auf Verbinden > Netzwerkverbindungen.



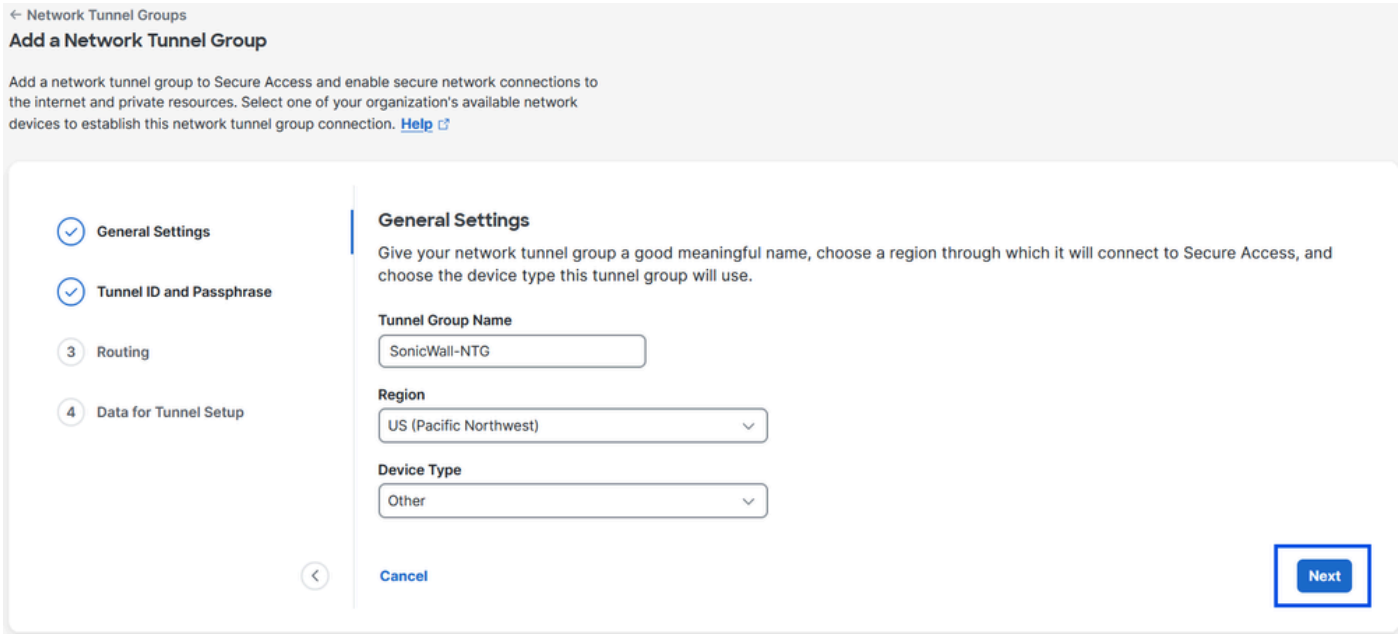
Sicherer Zugriff - Netzwerkverbindungen

- Klicken Sie unter Netzwerk-Tunnelgruppen auf + Hinzufügen



Sicherer Zugriff - Netzwerk-Tunnelgruppen

- Konfigurieren von Tunnelgruppenname, Region und Gerätetyp
- Klicken Sie auf Next (Weiter).

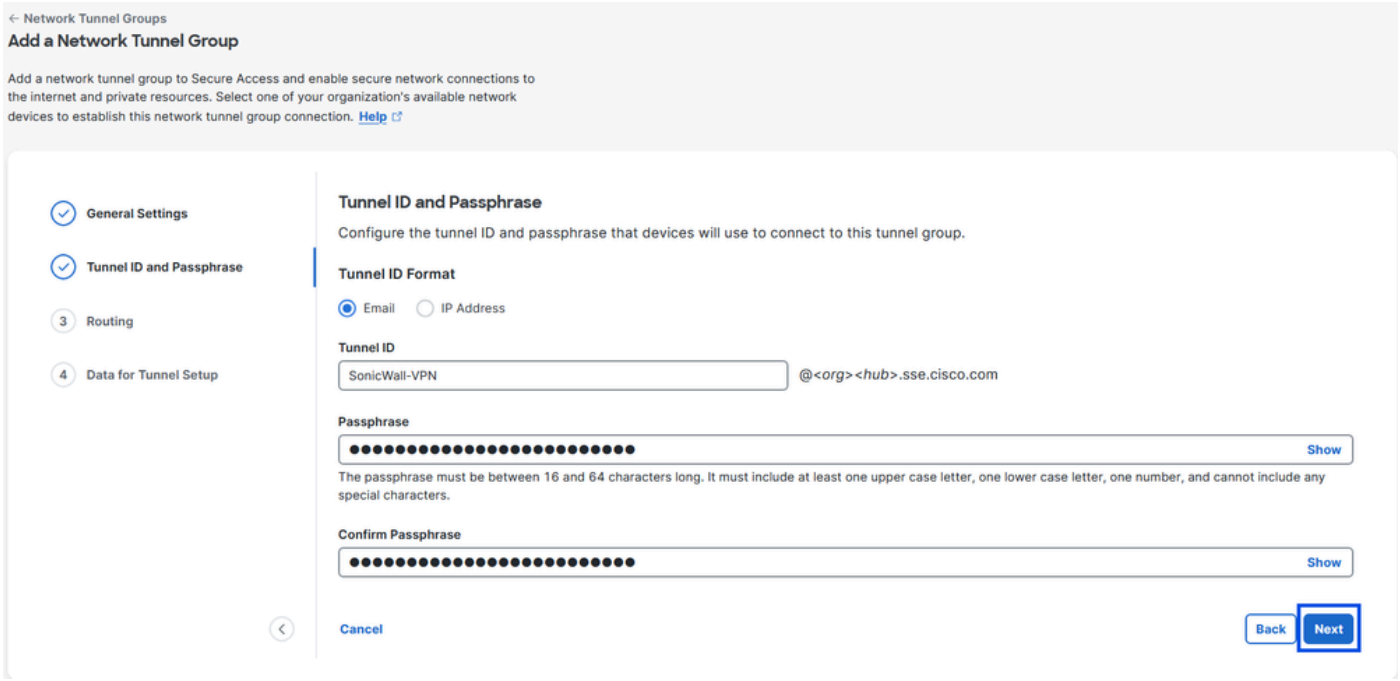


Sicherer Zugriff - Netzwerk-Tunnelgruppe - Allgemeine Einstellungen

---

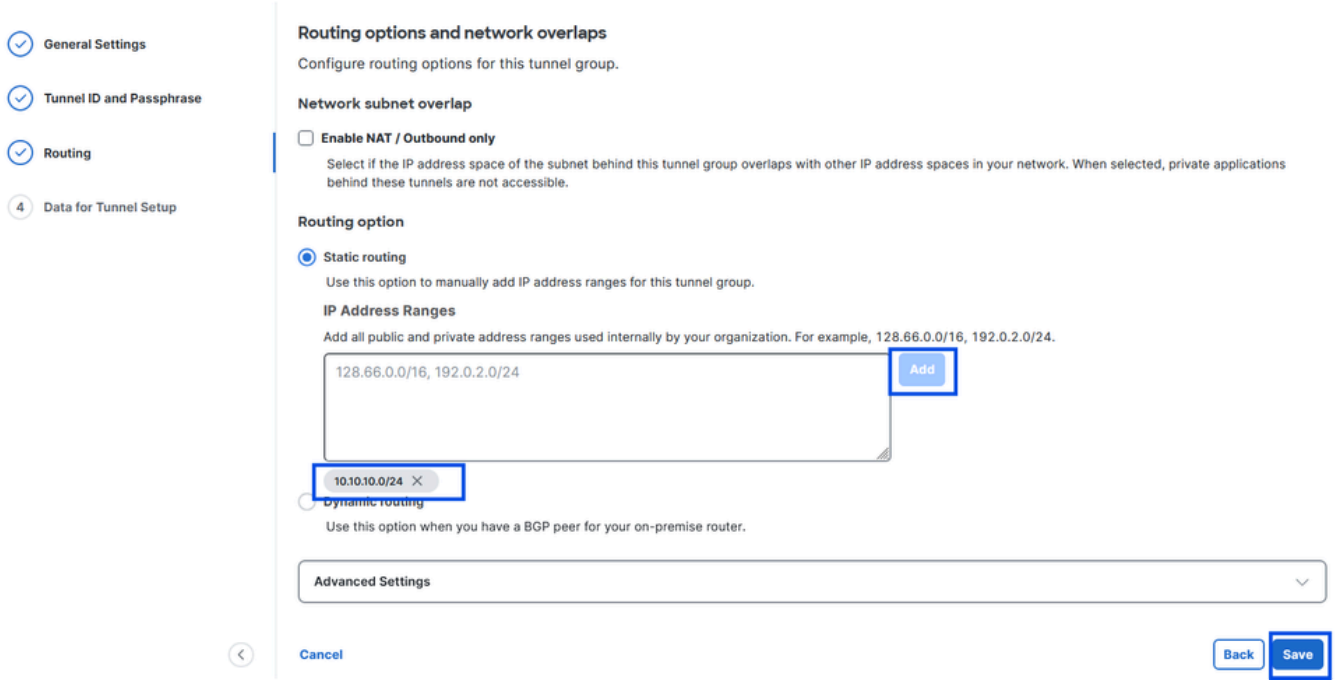
Anmerkung: Wählen Sie die Region aus, die dem Standort Ihrer Firewall am nächsten liegt.

- Konfigurieren des Tunnel-ID-Formats und der Passphrase
- Klicken Sie auf Next (Weiter).



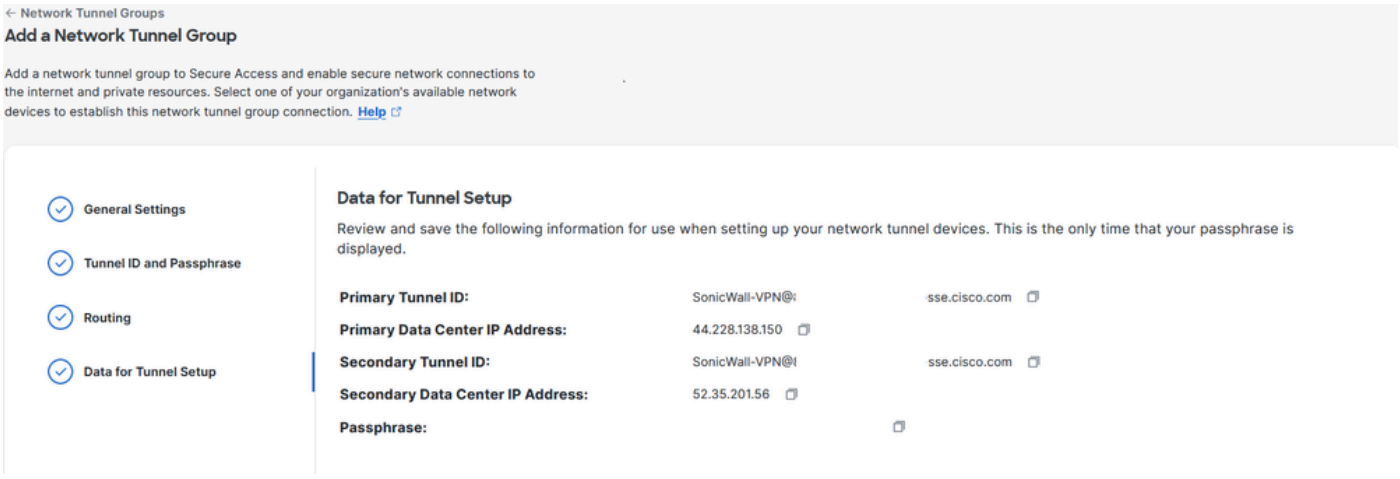
Sicherer Zugriff - Tunnel-ID und Passphrase

- Konfigurieren Sie die IP-Adressbereiche, Hosts oder Subnetze, die Sie in Ihrem Netzwerk konfiguriert haben, und leiten Sie den Datenverkehr über den sicheren Zugriff weiter.
- Klicken Sie auf Hinzufügen
- Klicken Sie auf Save (Speichern).



Sicherer Zugriff - Tunnelgruppen - Routing-Optionen

Nachdem Sie auf Speichern geklickt haben, werden die Informationen zum Tunnel angezeigt. Speichern Sie diese Informationen für den nächsten Konfigurationsschritt.



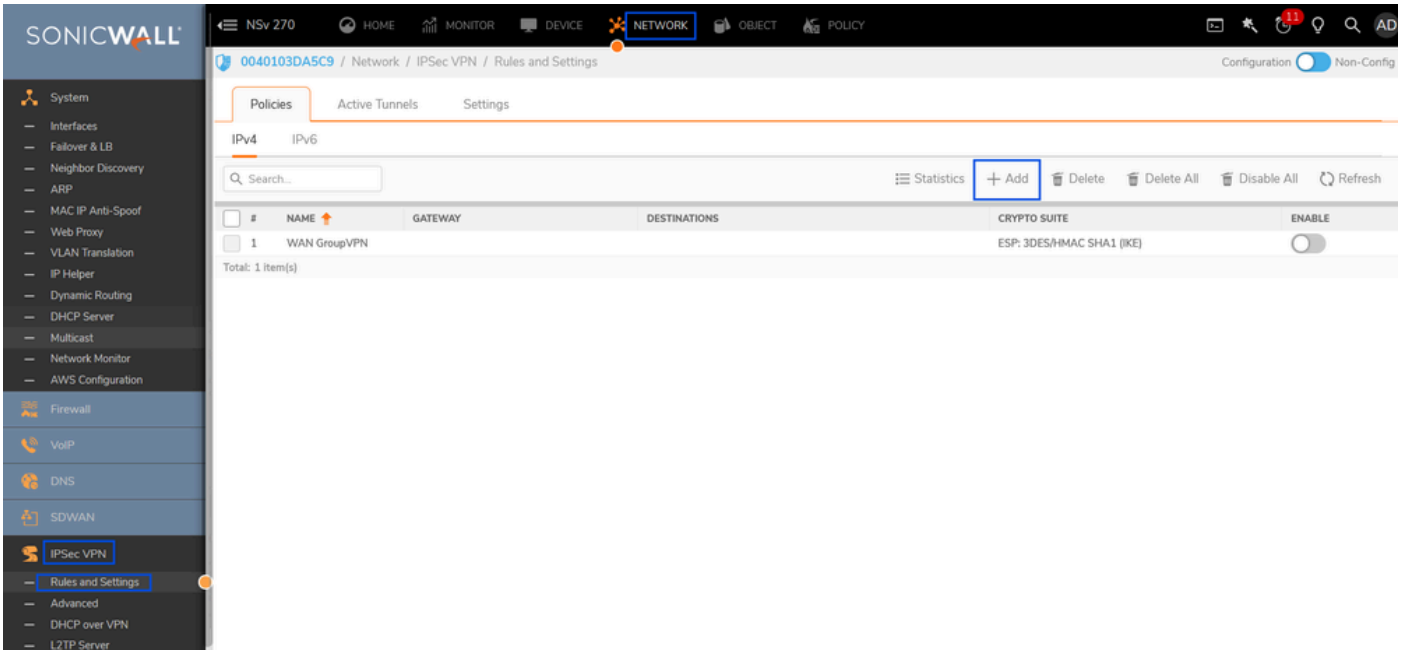
Sicherer Zugriff - Daten für Tunnel-Setup

Konfigurieren des Tunnels auf der Sonicwall

Konfigurieren des Tunnels - Regeln und Einstellungen

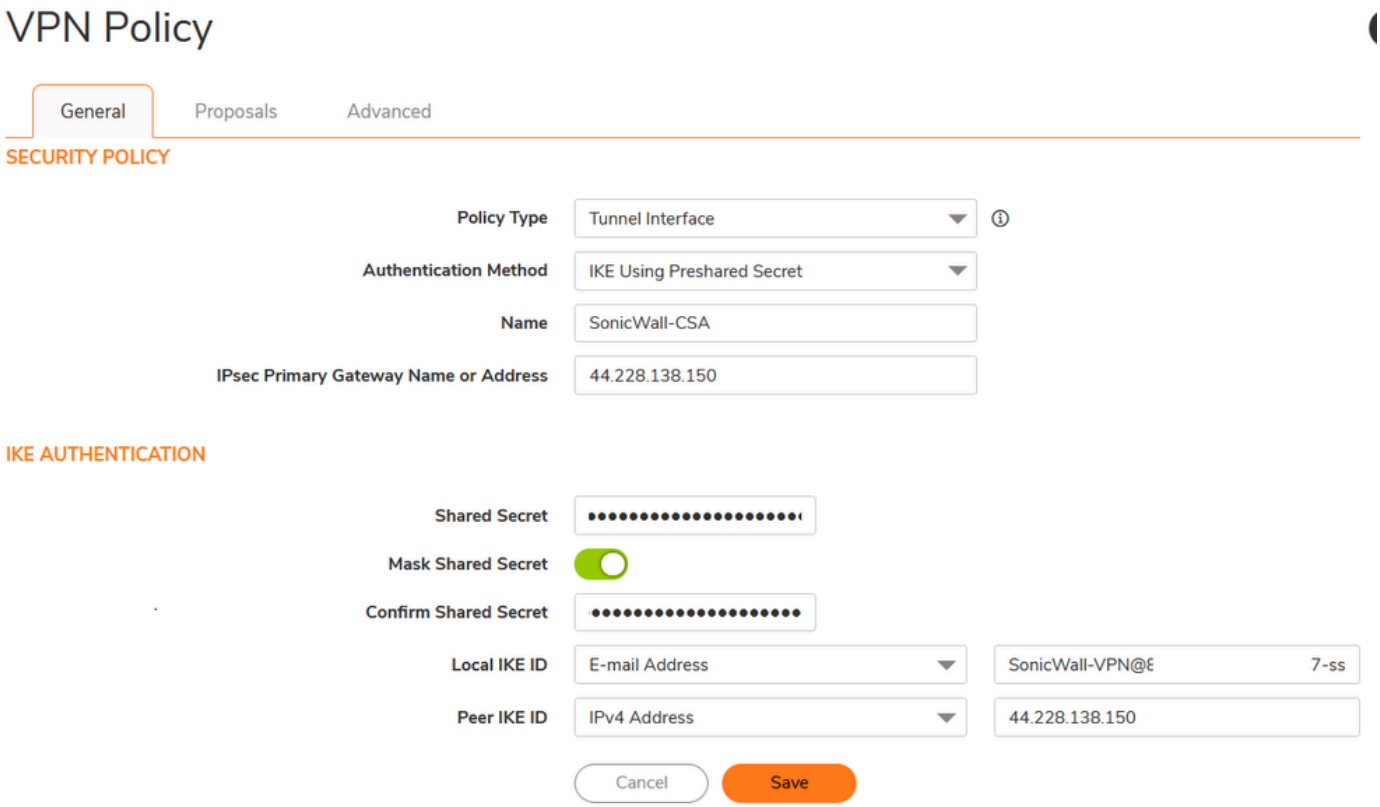
Navigieren Sie zum Sonicwall Dashboard.

- Netzwerk > IPsec VPN > Regeln und Einstellungen
- Klicken Sie auf + Hinzufügen



Sonicwall - IPSec VPN - Regeln und Einstellungen

- Füllen Sie unter VPN Policy (VPN-Richtlinie) die VPN-Konfiguration basierend auf den Tunneldaten von Secure Access und den unterstützten ipsec-Parametern aus.



VPN Policy

General | Proposals | Advanced

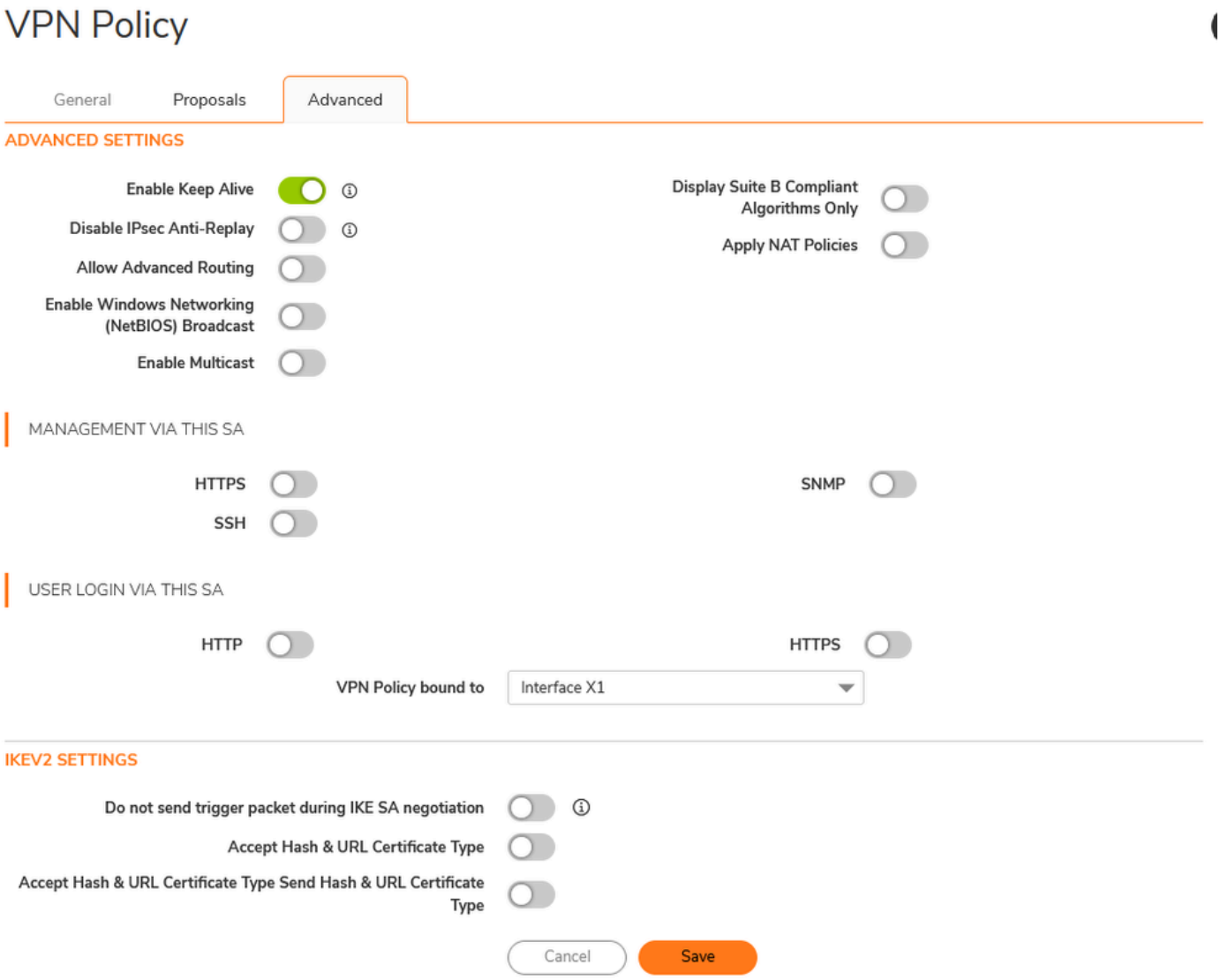
IKE (PHASE 1) PROPOSAL

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

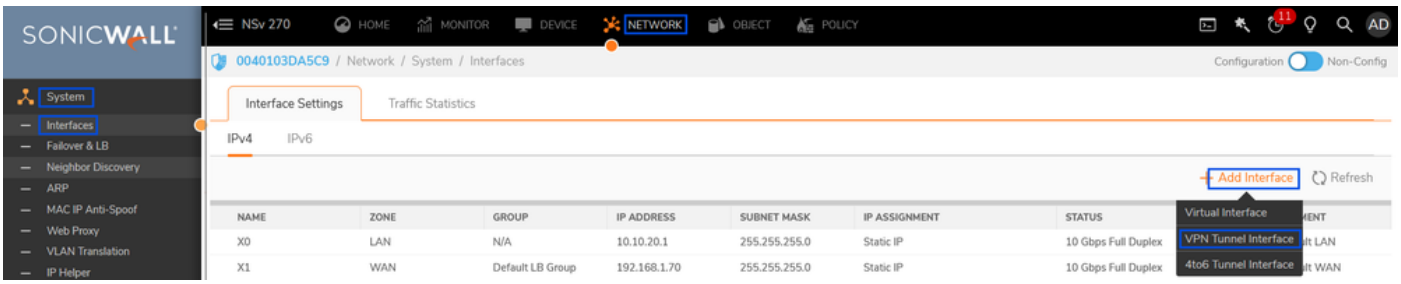


- Klicken Sie auf Speichern

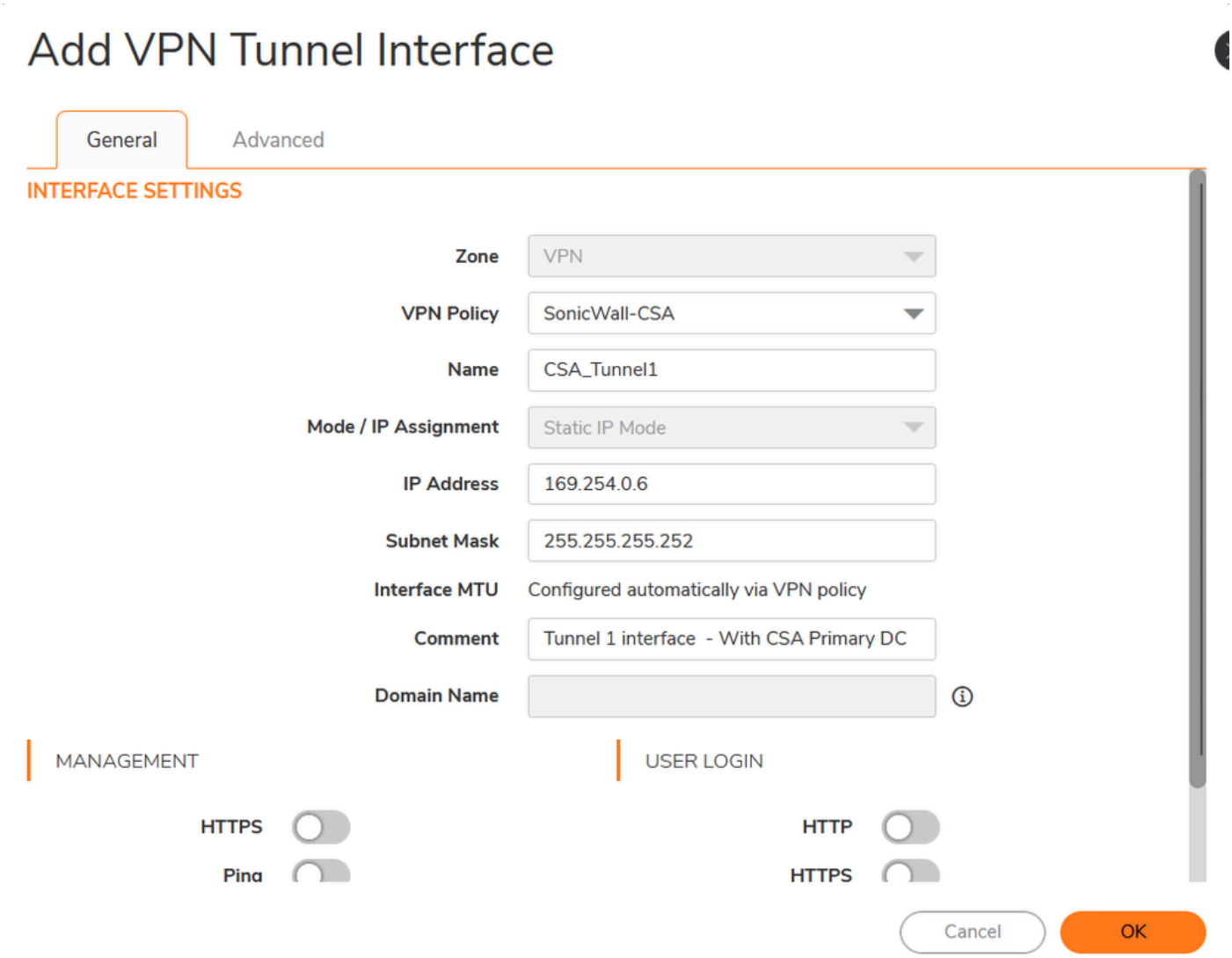
VPN-Tunnelschnittstelle hinzufügen

Navigieren Sie zum Sonicwall Dashboard.

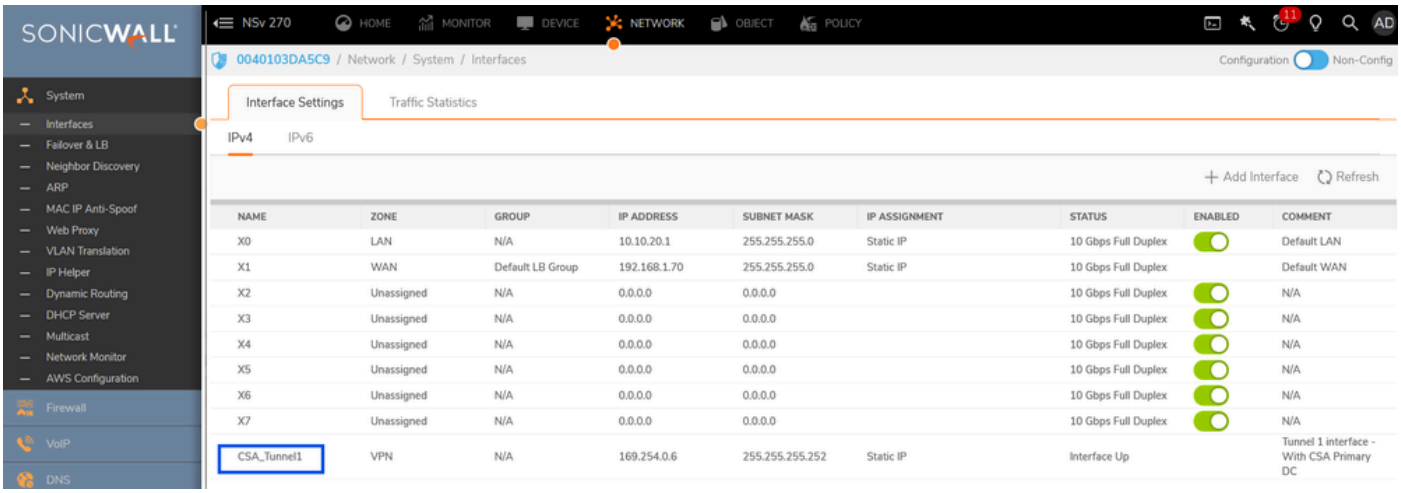
- Netzwerk > System > Schnittstelle
- Klicken Sie auf + Schnittstelle hinzufügen.
- VPN-Tunnelschnittstelle auswählen



Sonicwall - Schnittstellen



- Klicken Sie auf OK.

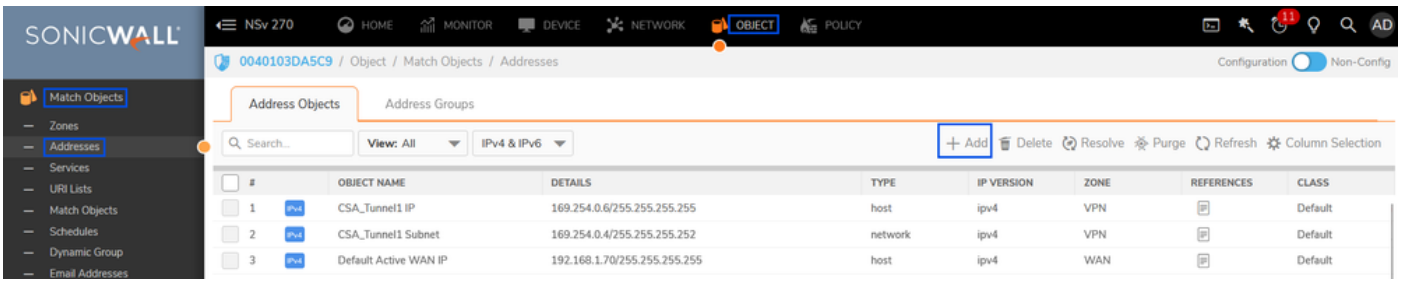


Sonicwall - Schnittstellen - VPN-Tunnelschnittstelle

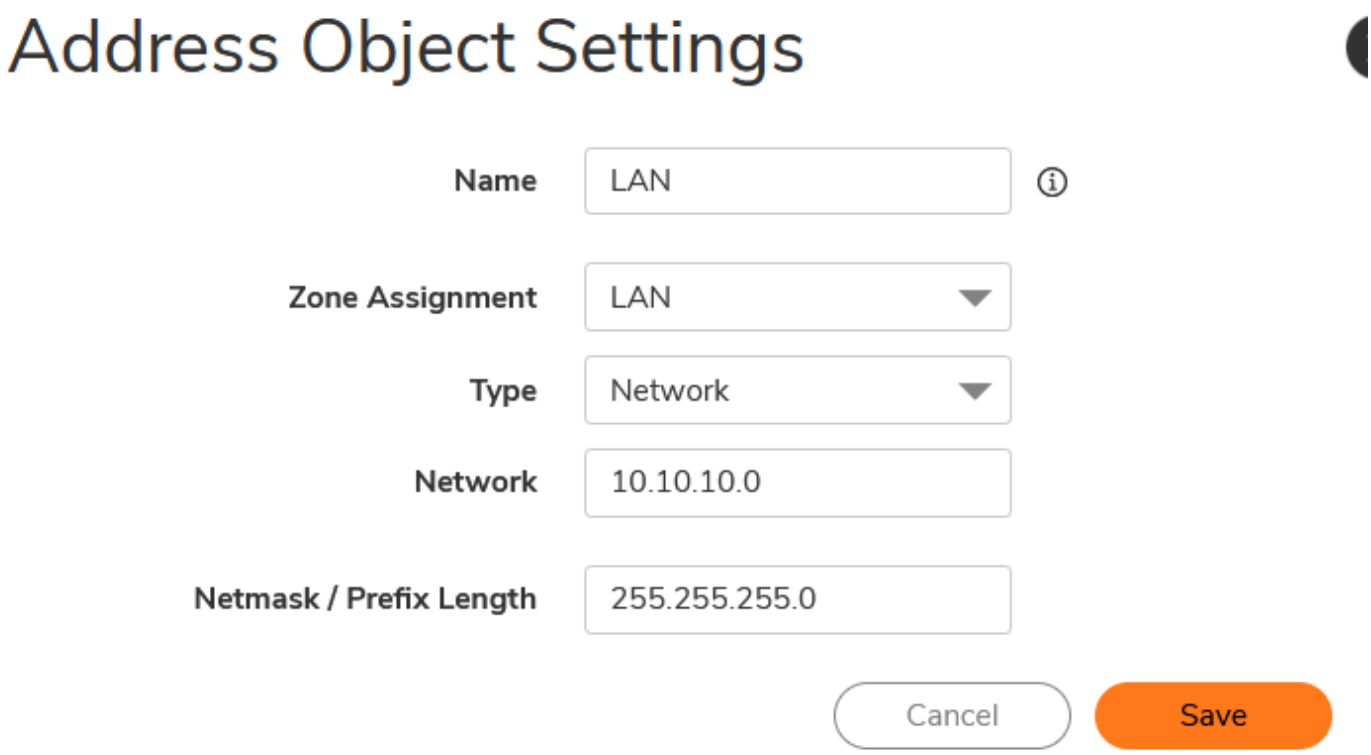
Netzwerkobjekt und Gruppen hinzufügen

Navigieren Sie zum Sonicwall Dashboard.

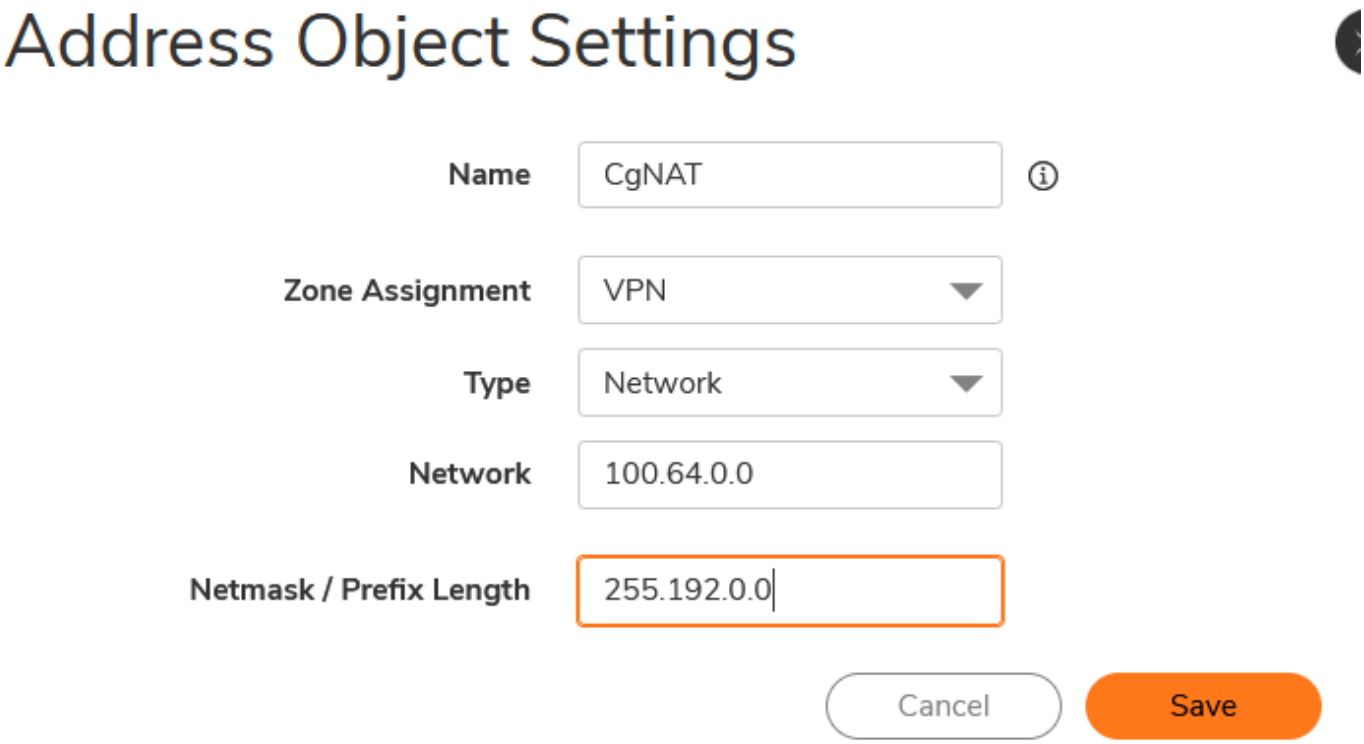
- Objekt > Objekte zuordnen > Adressen
- Adressobjekte
- Klicken Sie auf + Hinzufügen



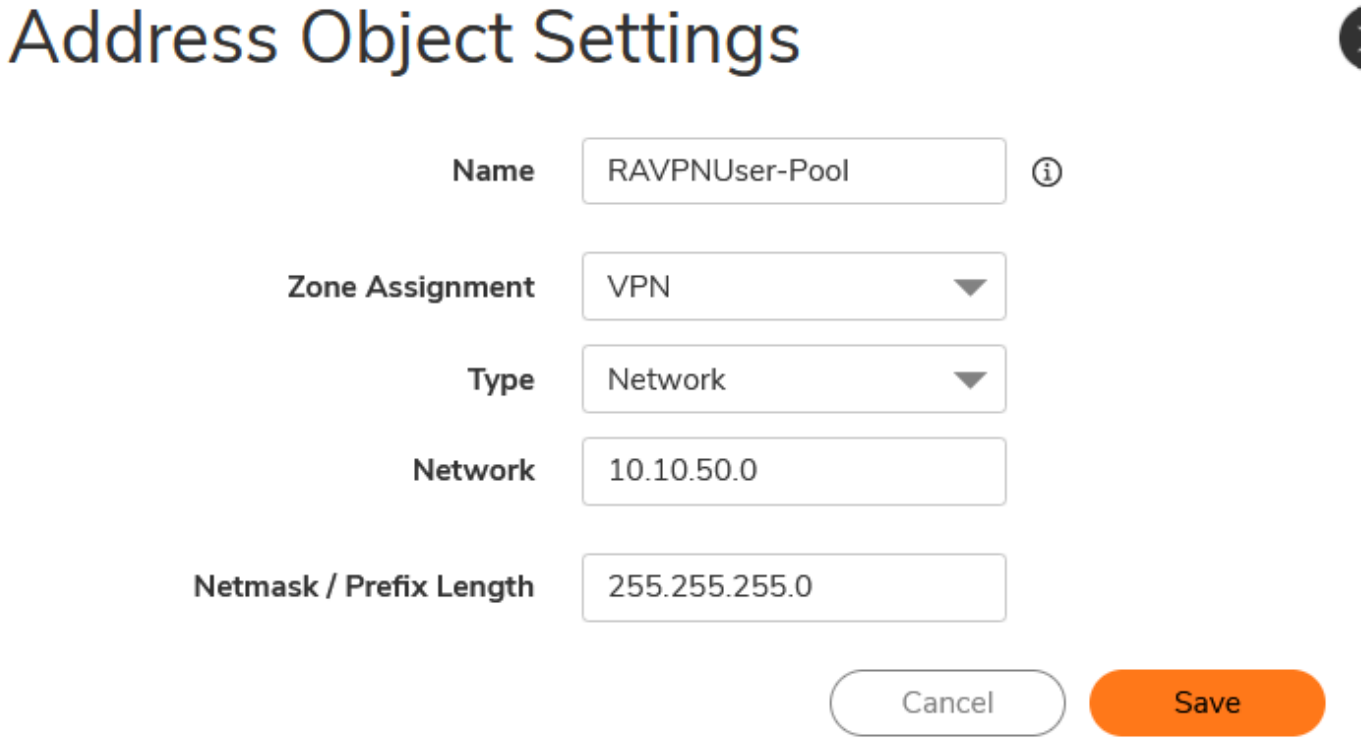
Sonicwall - Objekt - Adressobjekte



- Klicken Sie auf Save (Speichern).

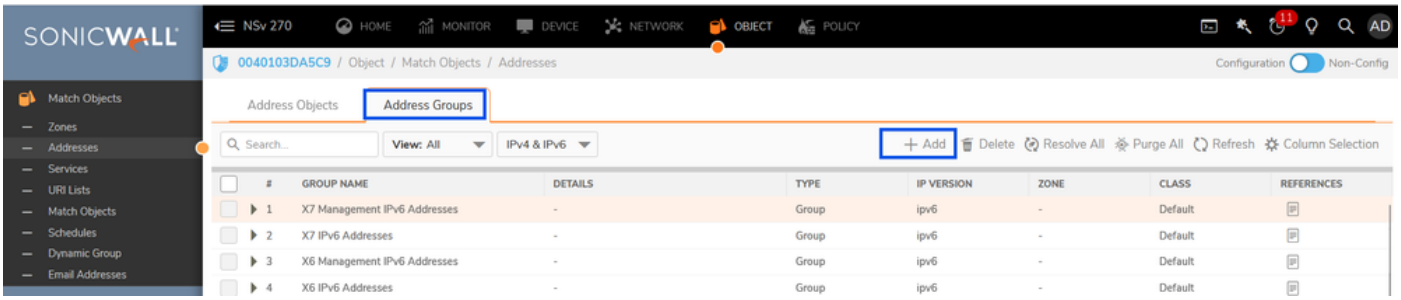


- Klicken Sie auf Save (Speichern).

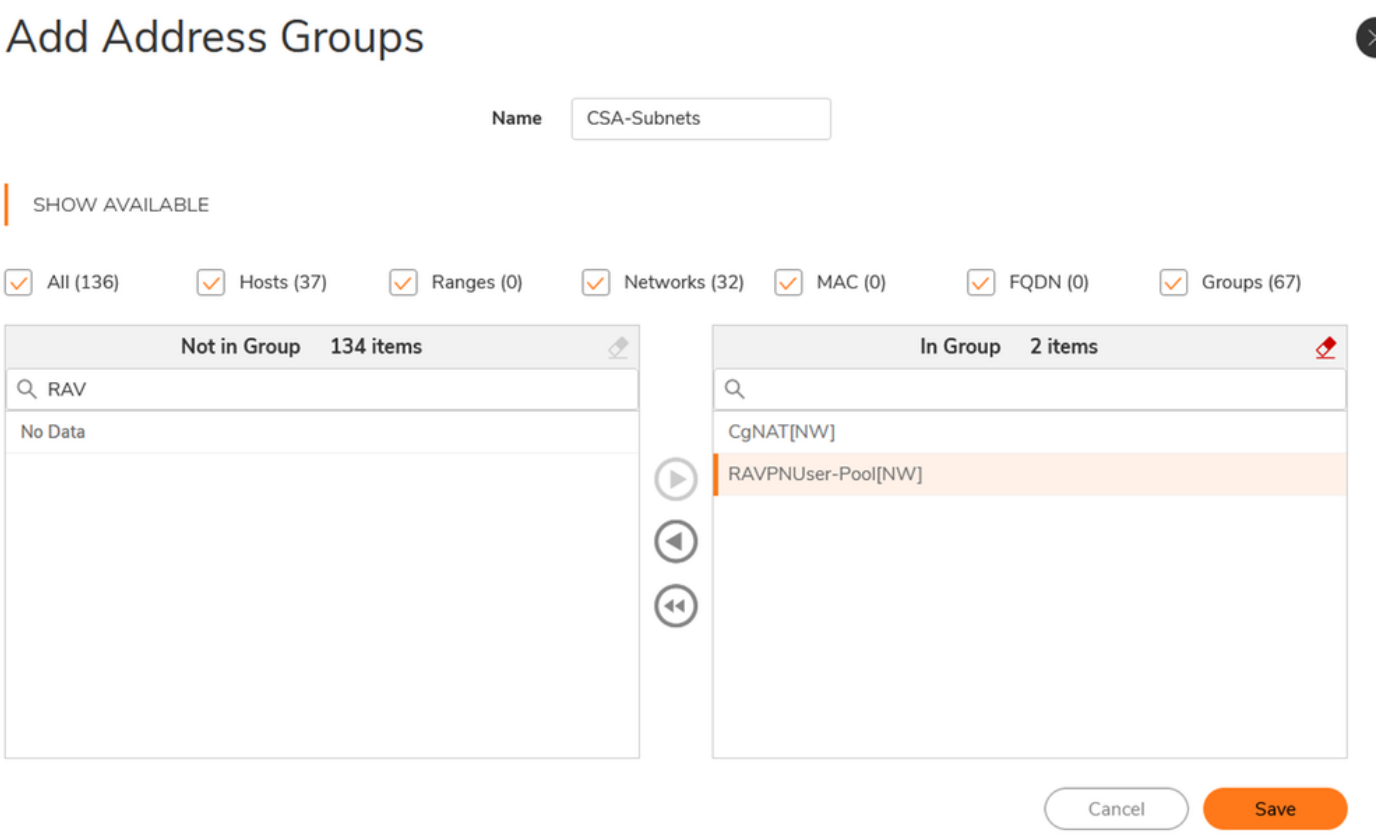


- Klicken Sie auf Save (Speichern).

- Erstellen von Adressgruppen
- Klicken Sie auf +Hinzufügen
- Wählen Sie das Adressobjekt aus, und fügen Sie es zu Adressgruppen hinzu.



Sonicwall - Objekt - Adressgruppen

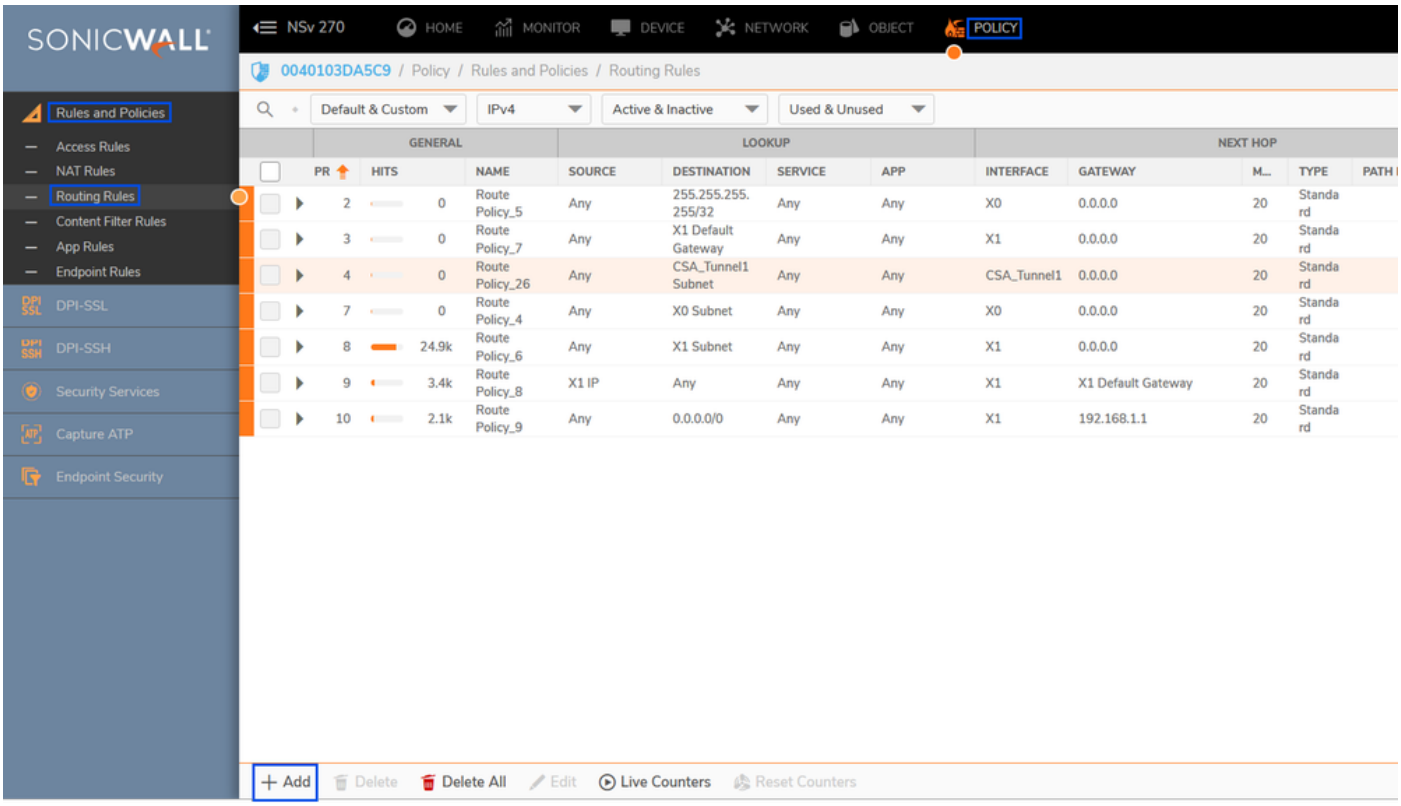


- Klicken Sie auf Save (Speichern).

Route hinzufügen

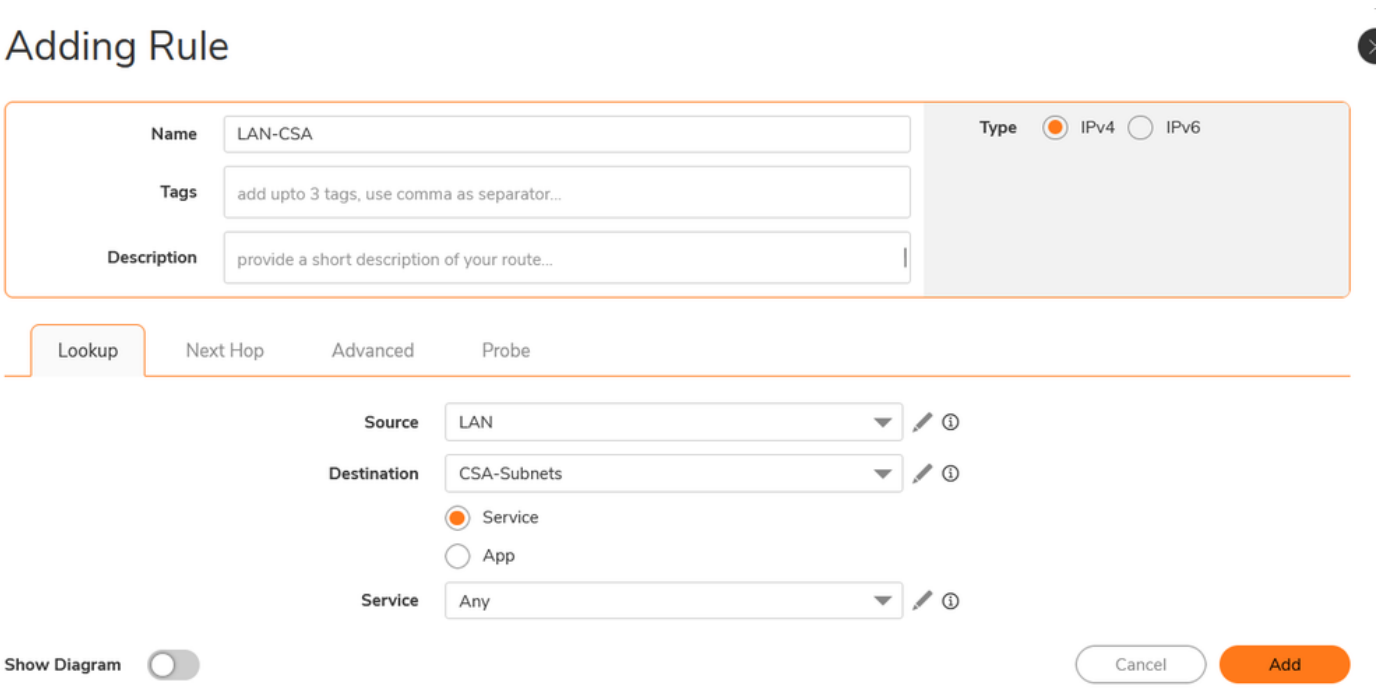
Navigieren Sie zum Sonicwall Dashboard.

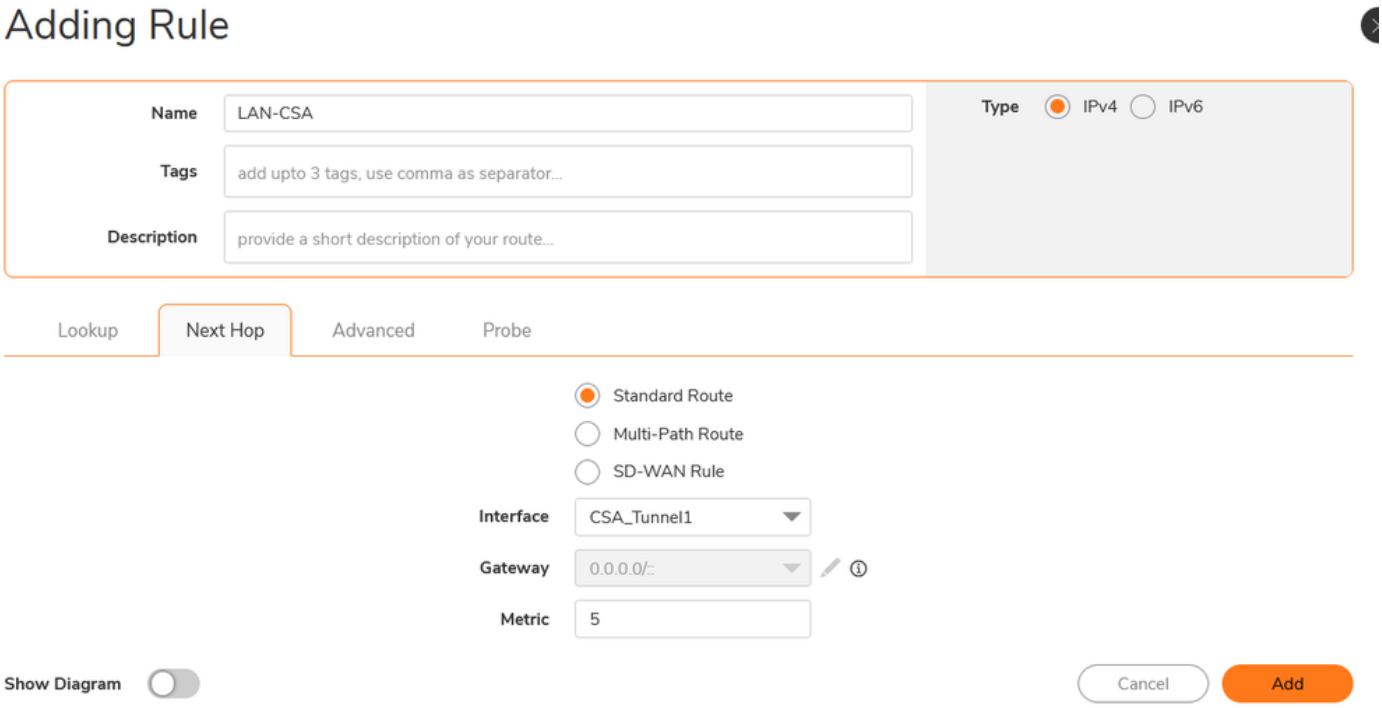
- Richtlinie > Regeln und Richtlinien > Weiterleitungsregeln
- Klicken Sie auf + Hinzufügen



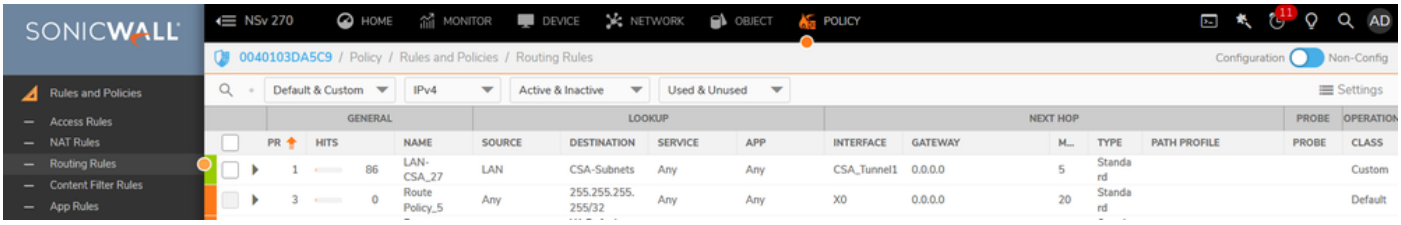
Sonicwall - Routingregeln

- Routingregel hinzufügen





- Klicken Sie auf + Hinzufügen

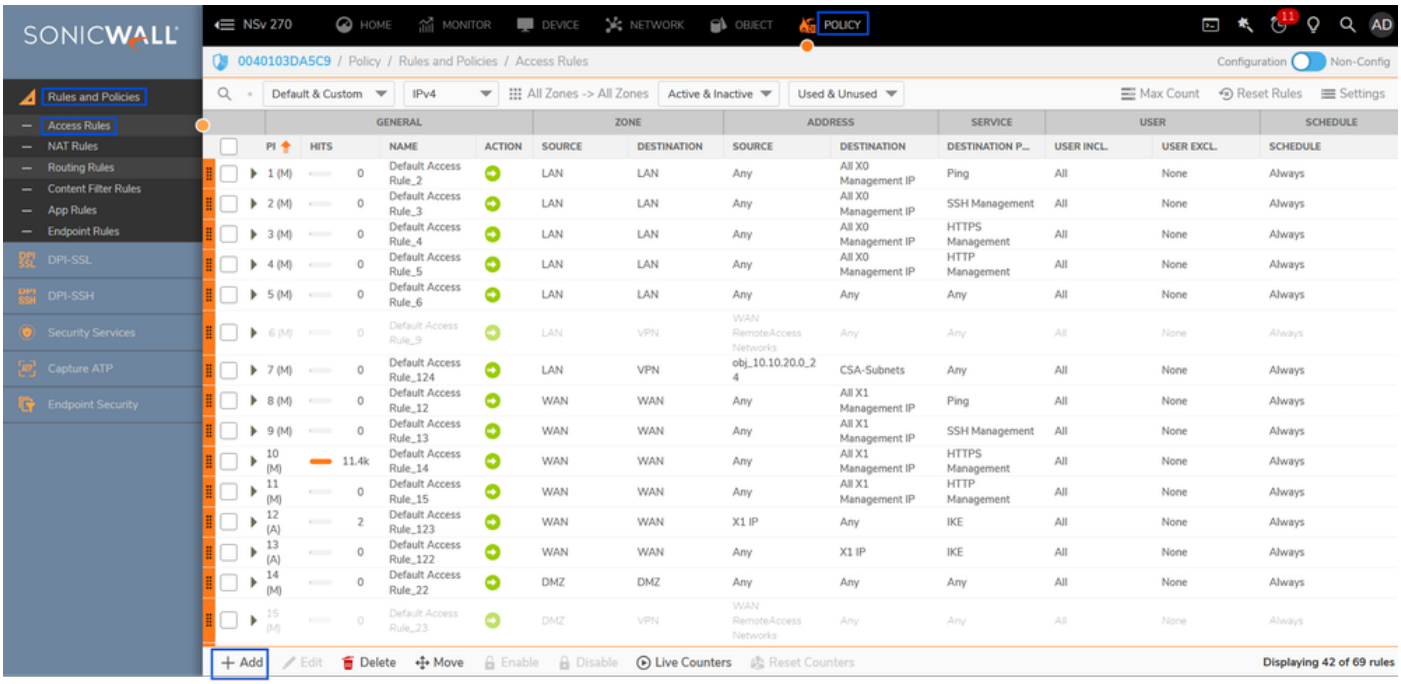


Sonicwall - Routingregeln

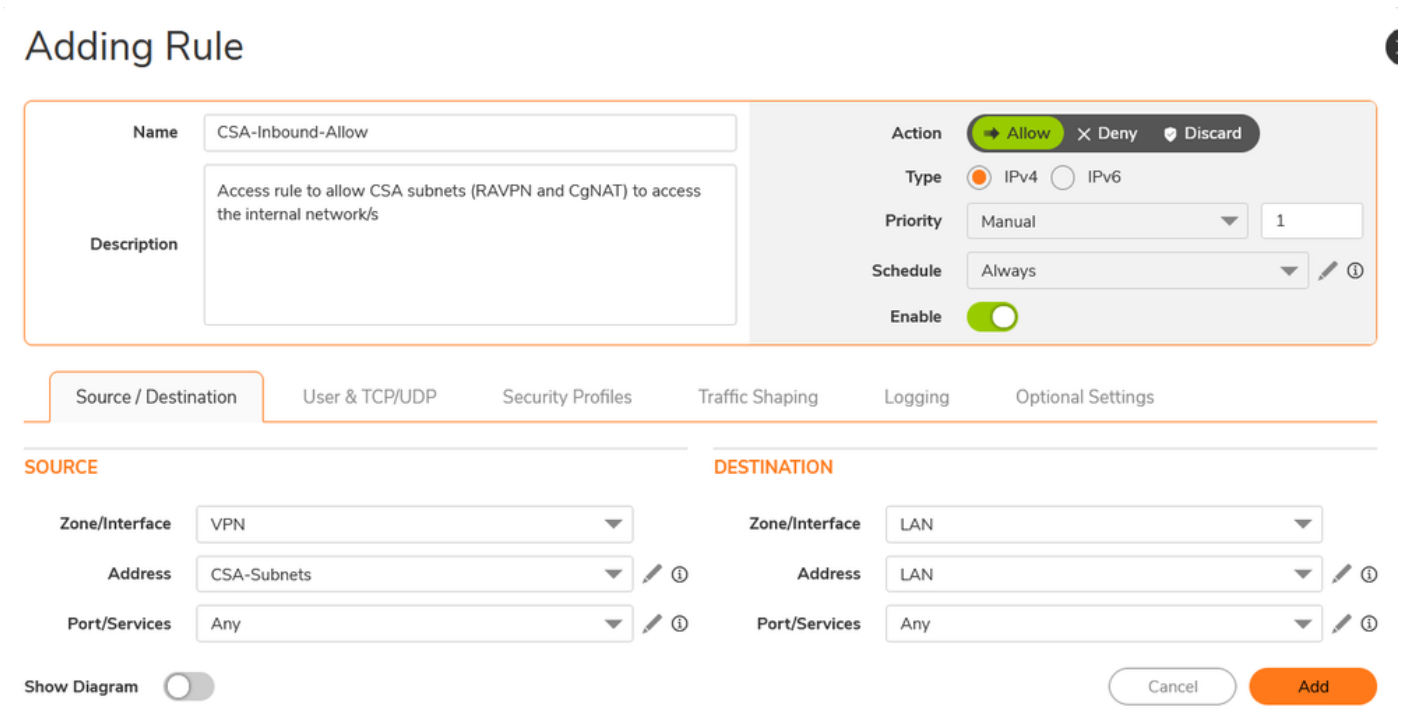
Zugriffsregeln hinzufügen

Navigieren Sie zum Sonicwall Dashboard.

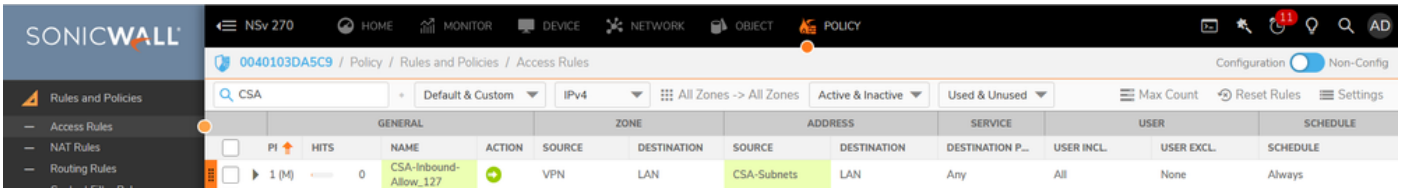
- Richtlinie > Regeln und Richtlinien > Zugriffsregeln
- Klicken Sie auf + Hinzufügen



Sonicwall - Zugriffsregeln



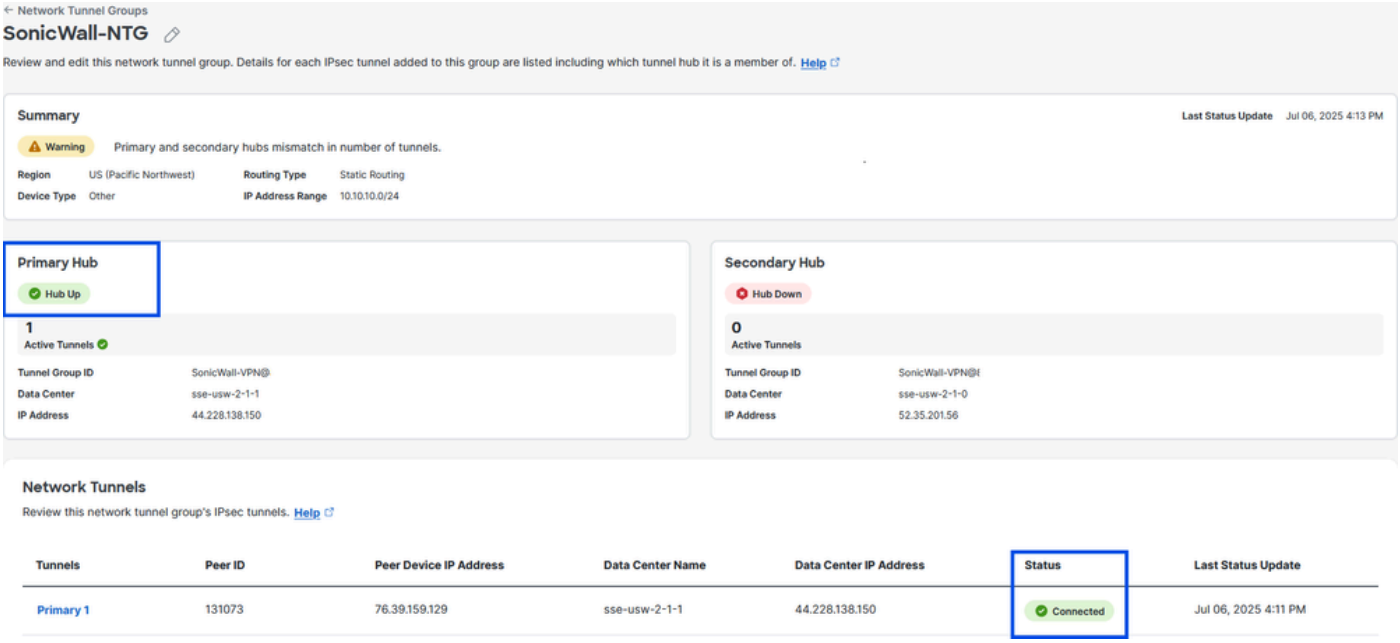
- Klicken Sie auf +Hinzufügen



Sonicwall - Zugriffsregeln

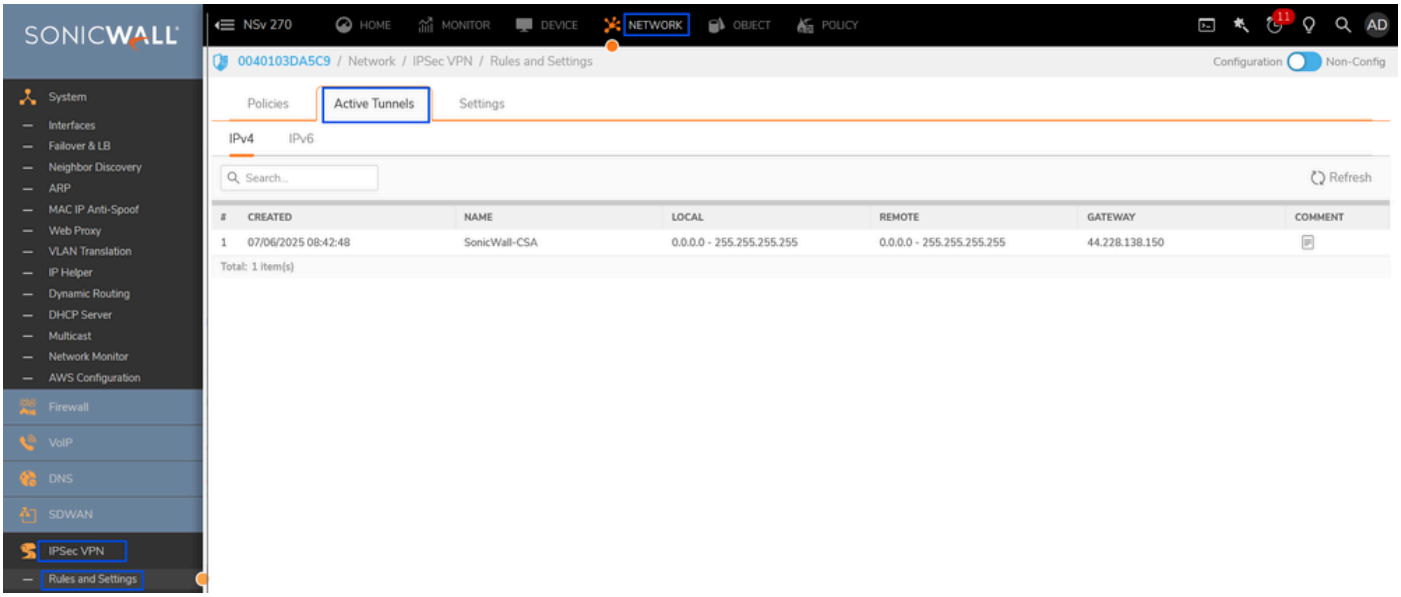
Überprüfung

- Tunnelstatus bei sicherem Zugriff



Sicherer Zugriff - Netzwerk-Tunnelgruppe - VPN-Status

- Tunnelstatus auf Sonicwall-Firewall



Sonicwall - IPSec-VPN-Status

Sie können den gleichen Prozess für die Konfiguration eines Tunnels zwischen dem sekundären Secure Access-Rechenzentrum und Sonicwall ausführen.

Jetzt ist der Tunnel für sicheren Zugriff und Sonicwall aktiviert. Sie können den Zugriff auf die privaten Ressourcen weiterhin über RA-VPN, browserbasiertes ZTA oder clientbasiertes ZTA auf Secure Access Dashboard konfigurieren.

Fehlerbehebung

Benutzer-PC

- Überprüfen Sie, ob der Benutzer erfolgreich eine Verbindung mit RAVPN/ZTNA herstellen/sich anmelden kann. Wenn nicht, suchen Sie weiter nach den Gründen, warum die Verbindung der Kontrollebene fehlschlägt.
- Überprüfen Sie, ob das Netzwerk, auf das der Benutzer zuzugreifen versucht, über einen RAVPN-Tunnel oder ZTNA geleitet werden soll. Wenn nicht, überprüfen Sie die Konfiguration am Headend .

Sicherer Zugriff

- Überprüfen Sie die Konfiguration der Verkehrssteuerung im RAVPN-Verbindungsprofil, um zu bestätigen, dass das Zielnetzwerk für das Senden über den Tunnel an Secure Access konfiguriert ist.
- Überprüfen Sie, ob eine private Ressource mit einem gültigen Protokoll bzw. gültigen Ports definiert ist, und ob die ZTNA-/RAVPN-Verbindungsmechanismen überprüft wurden.
- Überprüfen Sie, ob die Zugriffsrichtlinie so konfiguriert ist, dass RAVPN-/ZTNA-Benutzer auf das private Ressourcennetzwerk zugreifen können, und platzieren Sie sie in einer Reihenfolge, in der keine andere Regel zur Blockierung des Datenverkehrs Vorrang hat.
- Vergewissern Sie sich, dass der IPSec-Tunnel aktiviert ist und für sicheren Zugriff gültige Client-Routen über statisches Routing angezeigt werden, das private Ressourcen abdeckt, auf die der Benutzer zugreifen möchte.

Schallwand

- Überprüfen Sie, ob der IPSec-Tunnel aktiv ist oder nicht (IKE & IPSec SA).
- Überprüfen Sie, ob die Client-Route oder -Routen ordnungsgemäß angekündigt wurden.
- Überprüfen Sie, ob die Datenverkehrsquellen des RAVPN-/ZTNA-Benutzers, die an eine private Ressource hinter Sonicwall gerichtet sind, die Sonicwall-Firewall über einen Tunnel erreichen, indem Sie die Paketerfassung auf Sonicwall durchführen.
- Überprüfen Sie, ob der Datenverkehr die private Ressource erreicht hat und auf den RAVPN-/ZTNA-Client antwortet oder nicht. Wenn ja, stellen Sie sicher, dass diese Pakete die Sonic X0 (LAN)-Schnittstelle erreichen.
- Überprüfen Sie, ob Sonicwall den zurückfließenden Datenverkehr über den IPSec-Tunnel an Secure Access weiterleitet.

Zugehörige Informationen

- Technischer Support und Downloads von Cisco
- Cisco Secure Access-Hilfecenter
- Zugriffsmodul ohne Vertrauen
- Fehler beim sicheren Zugriff: "Der Registrierungsdienst reagiert nicht. Kontaktieren Sie Ihren IT-Helpdesk"

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.