Configurer un accès sécurisé avec le pare-feu Sonicwall

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés
- Informations générales
- Diagramme du réseau

Configurer

- Configurer le groupe de tunnels réseau (VPN) sur l'accès sécurisé
- Configuration du tunnel sur Sonicwall
- Configuration du tunnel - Règles et paramètres
- Ajouter une interface de tunnel VPN
- Ajouter un objet et des groupes réseau
- Ajouter une route
- Ajouter des règles d'accès

Vérifier

Dépannage

- PC utilisateur
- Accès sécurisé
- Paroi Sonique

Informations connexes

Introduction

Ce document décrit comment configurer un tunnel IPsec VTI entre un accès sécurisé au pare-feu Sonicwall à l'aide du routage statique.

Conditions préalables

- Configurer le provisionnement utilisateur
- Configuration de l'authentification ZTNA SSO
- Configuration de l'accès sécurisé VPN à distance

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Pare-feu SonicWall (NSv270 - SonicOSX 7.0.1)

- Accès sécurisé
- Client sécurisé Cisco - VPN
- Client sécurisé Cisco - ZTNA
- ZTNA sans client

Composants utilisés

Les informations contenues dans ce document sont basées sur :

- Pare-feu SonicWall (NSv270 - SonicOSX 7.0.1)
- Accès sécurisé
- Client sécurisé Cisco - VPN
- Client sécurisé Cisco - ZTNA

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Diagramme du réseau

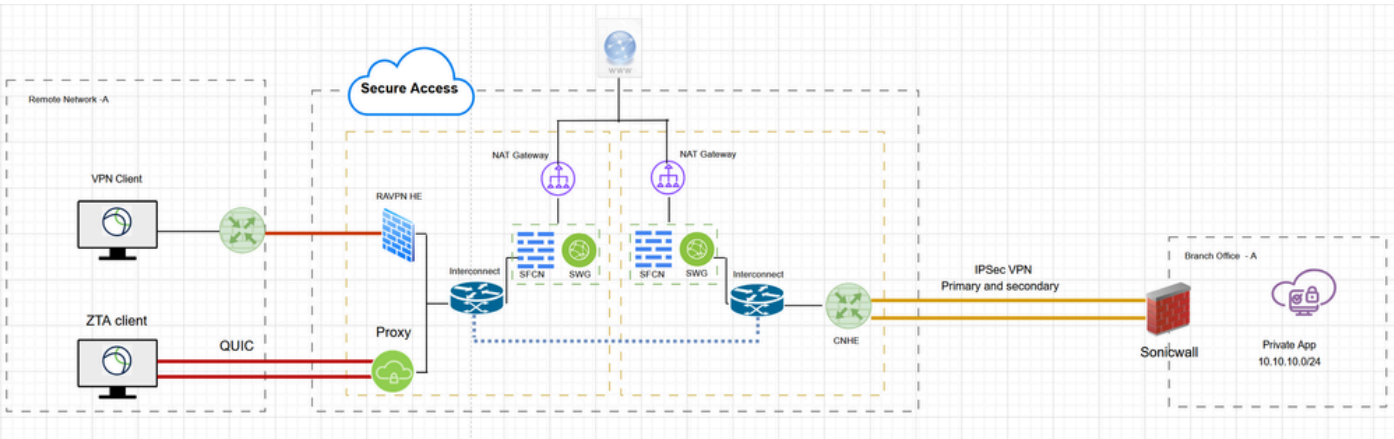


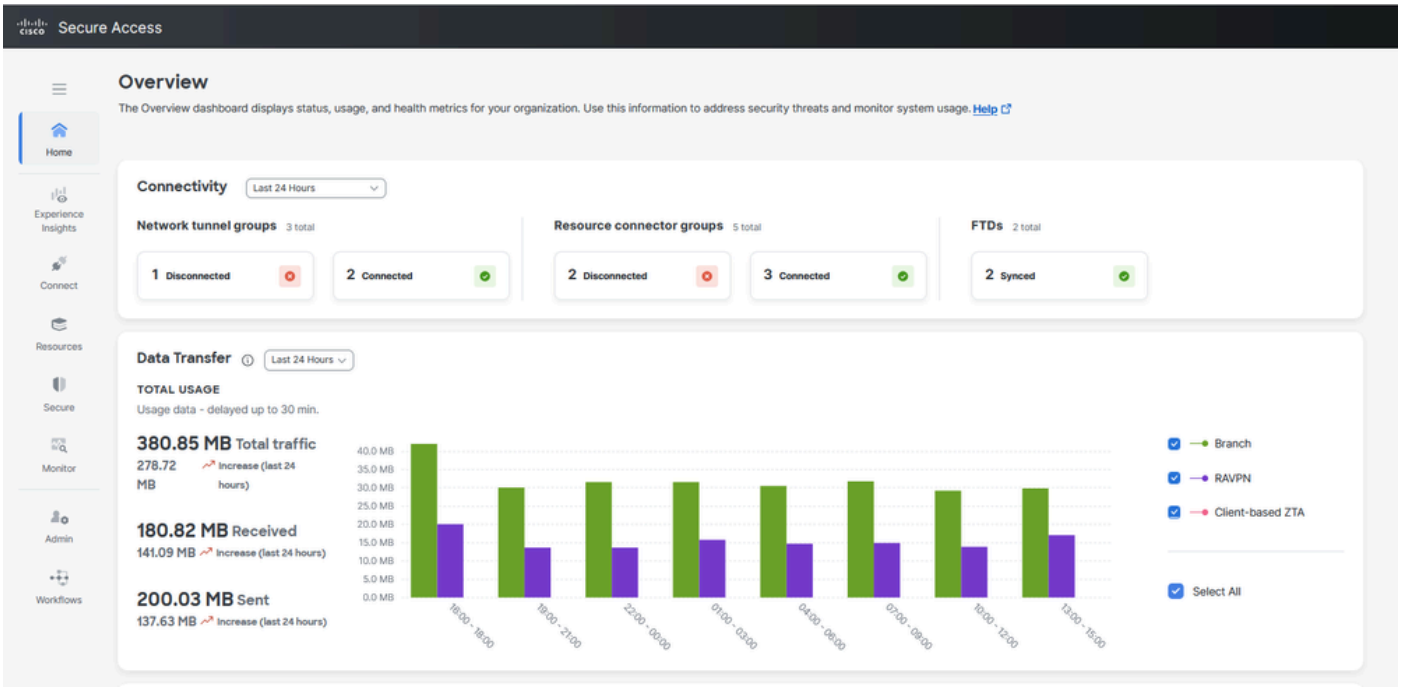
Diagramme du réseau

Configurer

Configurer le groupe de tunnels réseau (VPN) sur l'accès sécurisé

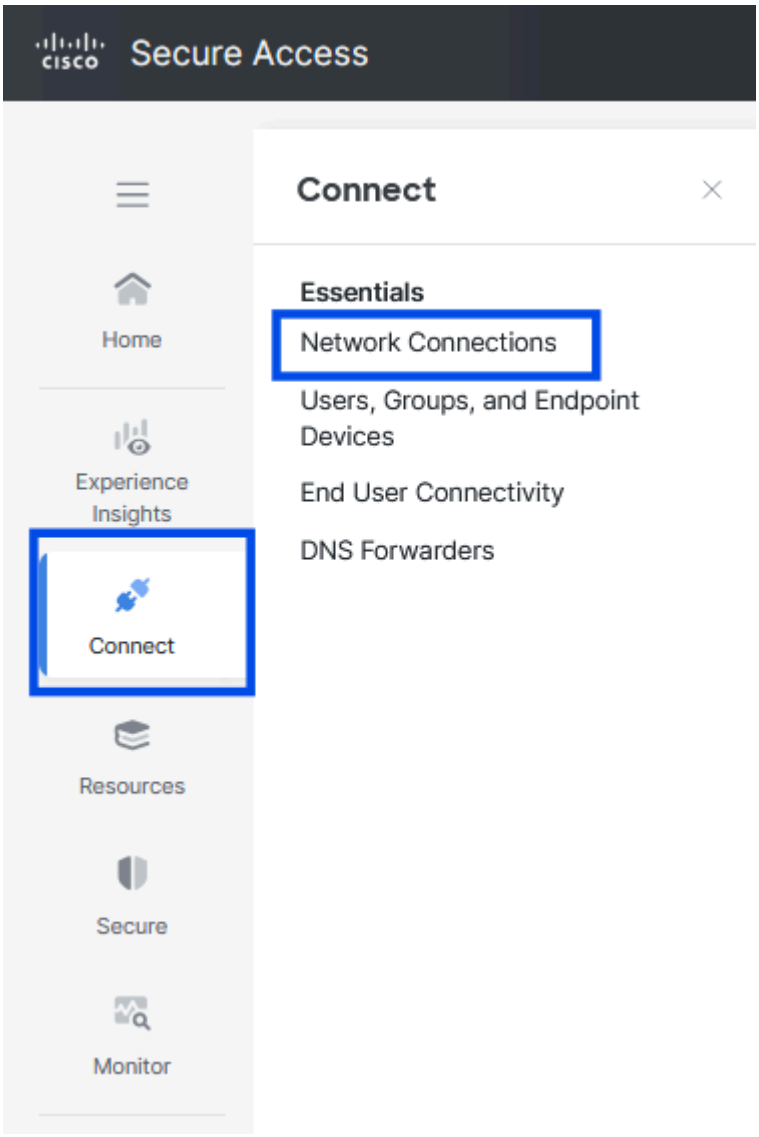
Afin de configurer un tunnel VPN entre Secure Access et Sonicwall

- Accédez au portail d'administration de Secure Access



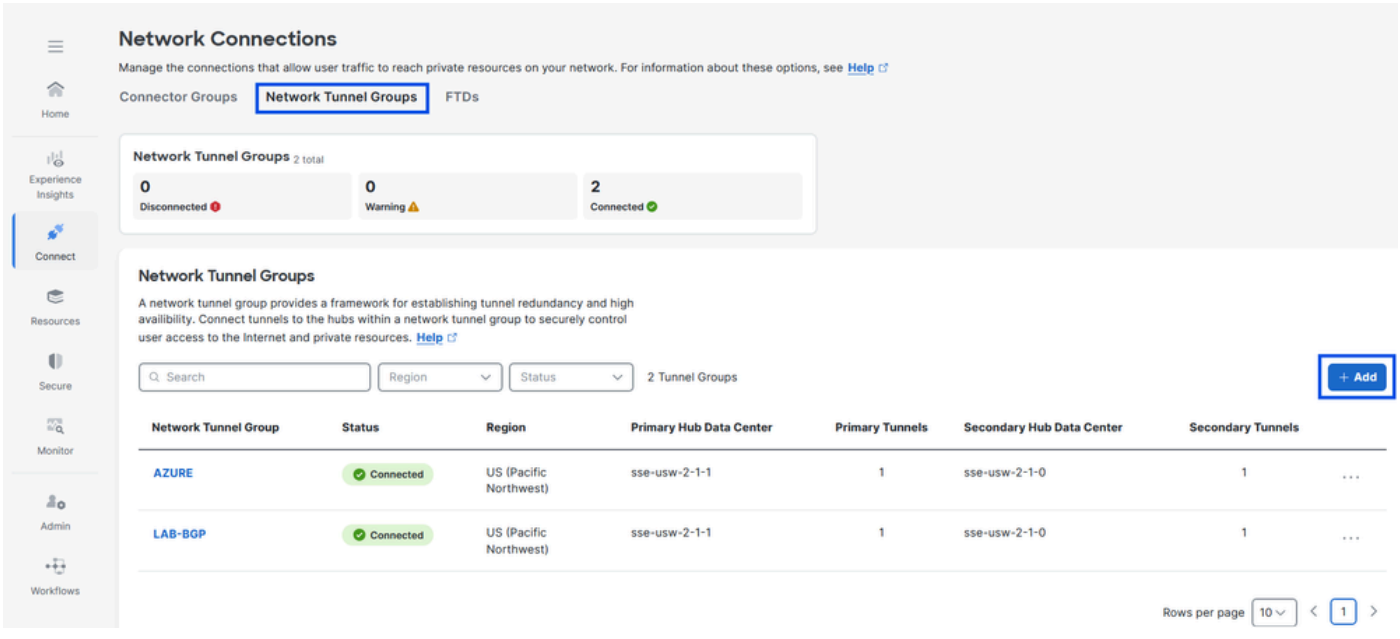
Accès sécurisé - Page principale

- Cliquez sur Connect > Network Connections



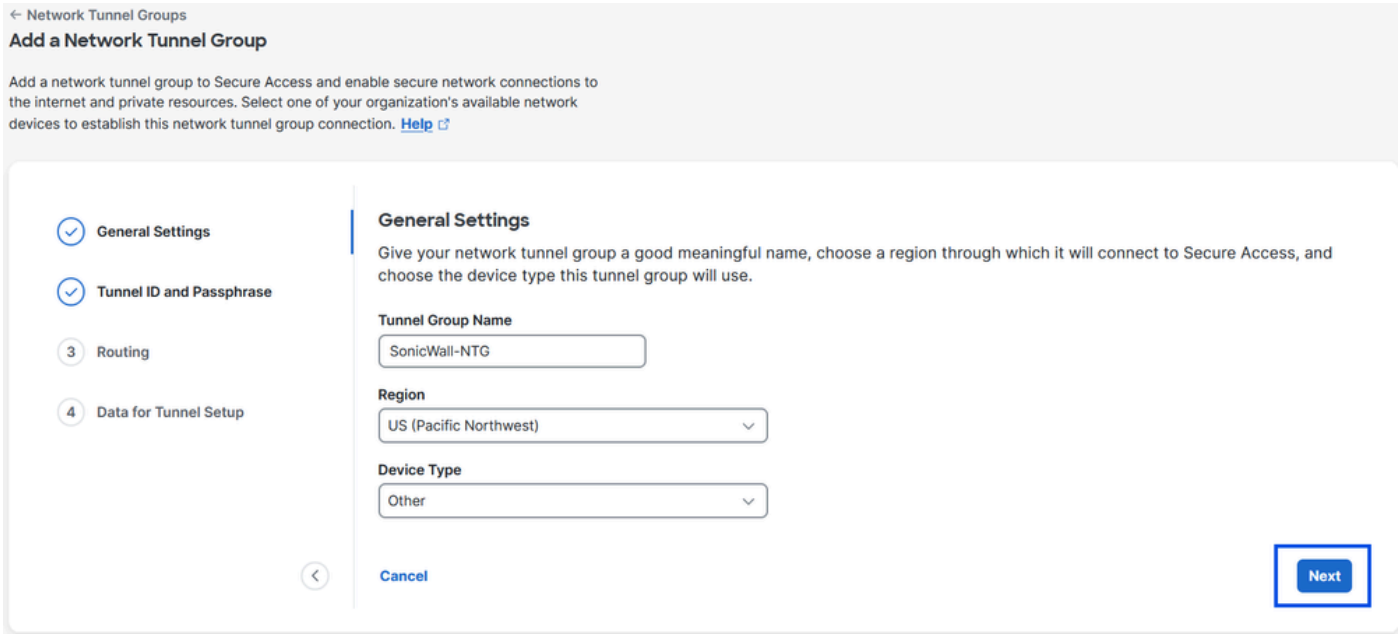
Accès sécurisé - Connexions réseau

- Sous Network Tunnel Groups, cliquez sur + Add



Accès sécurisé - Groupes de tunnels réseau

- Configurer le nom du groupe de tunnels , la région et le type de périphérique
- Cliquez sur Next (suivant).

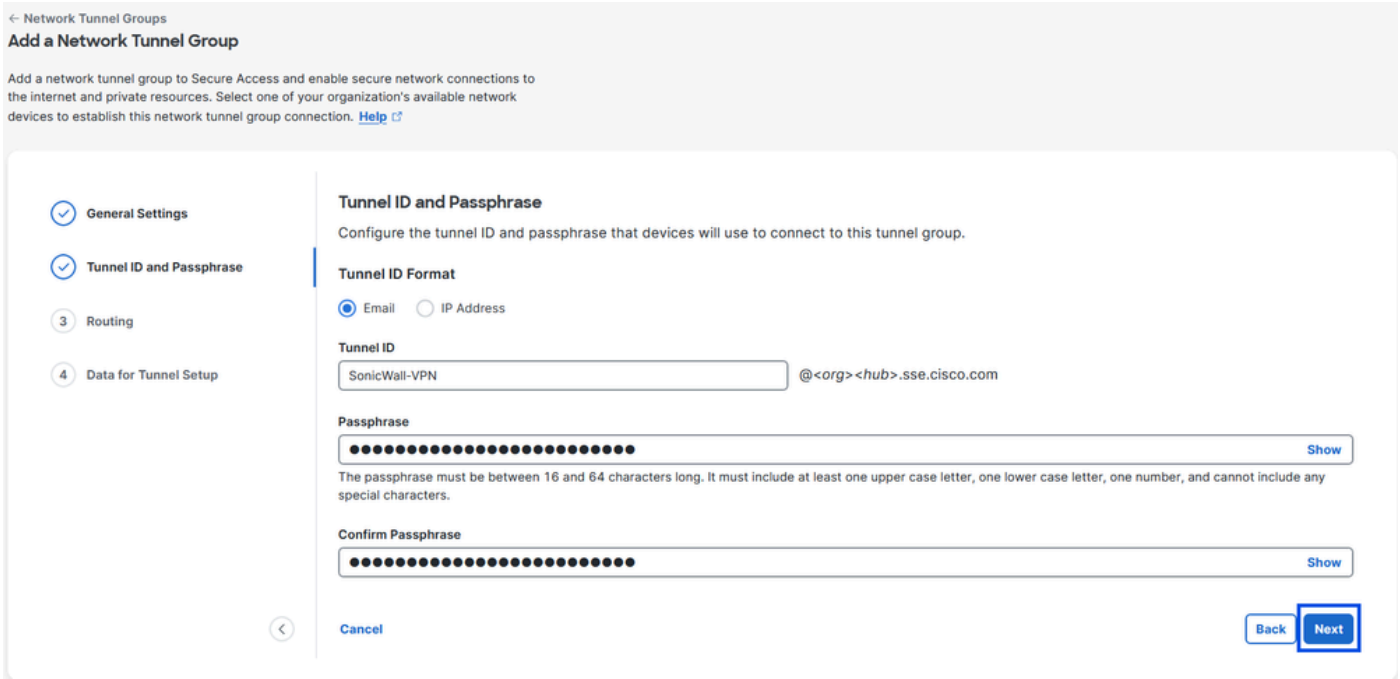


Accès sécurisé - Groupe de tunnels réseau - Paramètres généraux

---

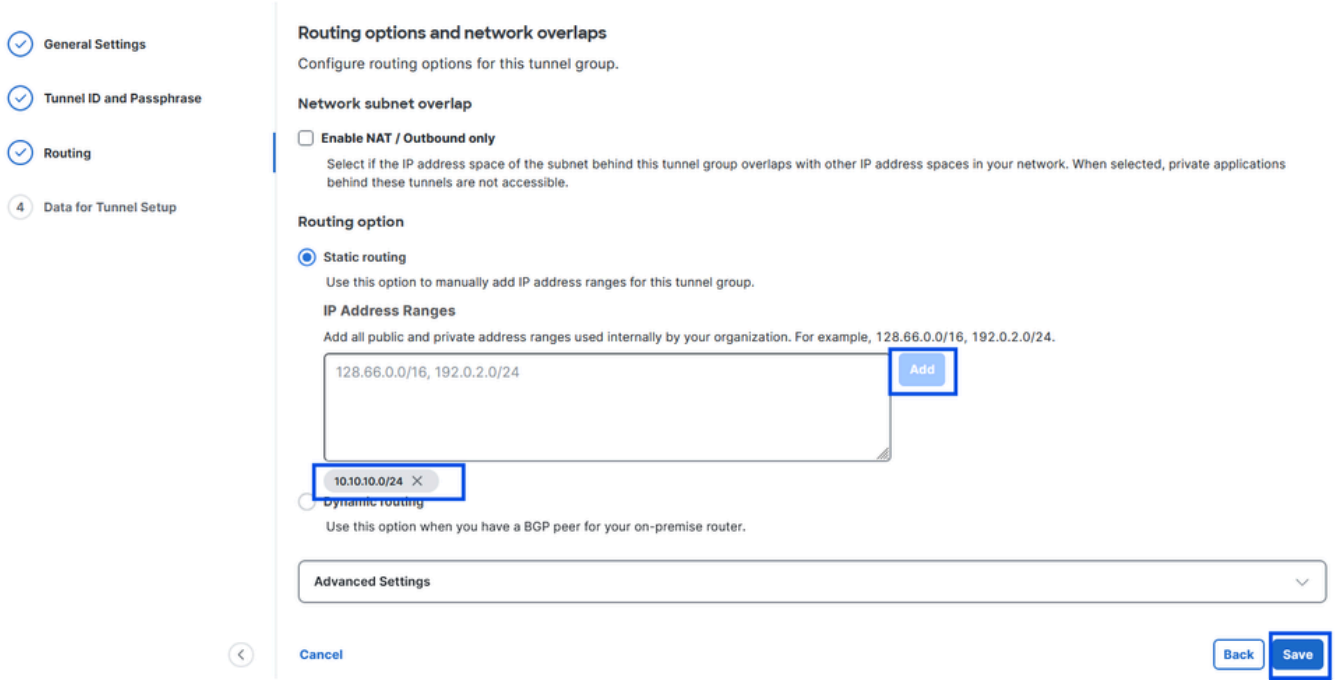
Remarque : Sélectionnez la région la plus proche de l'emplacement de votre pare-feu.

- Configuration du format ID de tunnel et de la phrase de passe
- Cliquez sur Next (suivant).



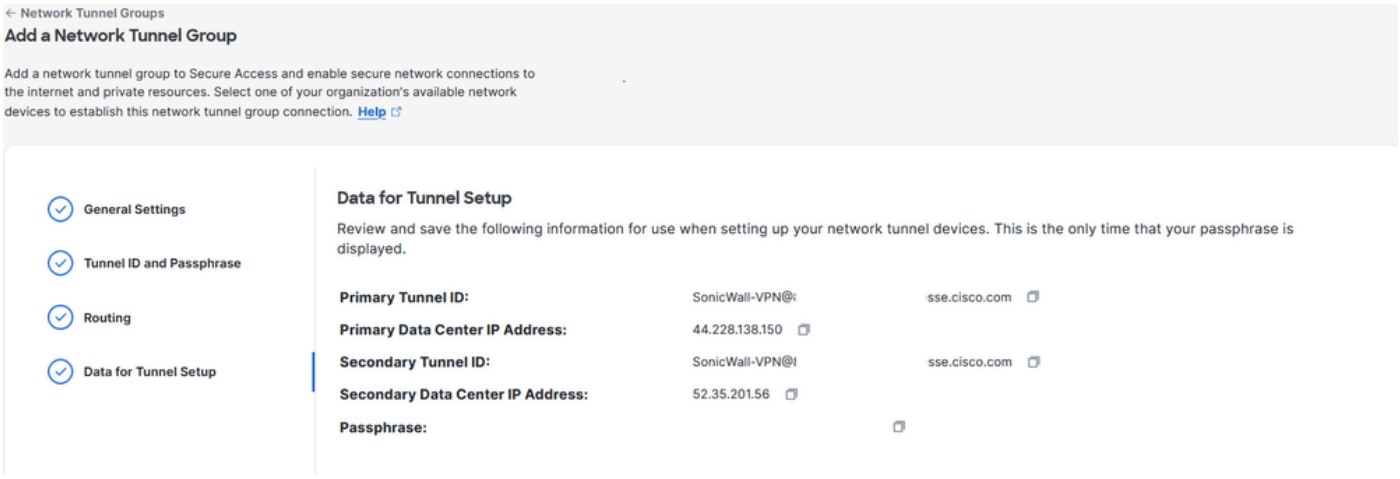
Accès sécurisé - ID de tunnel et phrase de passe

- Configurez les plages d'adresses IP, les hôtes ou les sous-réseaux que vous avez configurés sur votre réseau et souhaitez faire passer le trafic par un accès sécurisé
- Cliquez sur Add
- Cliquez sur Save (enregistrer)



Accès sécurisé - Groupes de tunnels - Options de routage

Après avoir cliqué sur Enregistrer , les informations sur le tunnel s'affichent. Enregistrez ces informations pour l'étape de configuration suivante



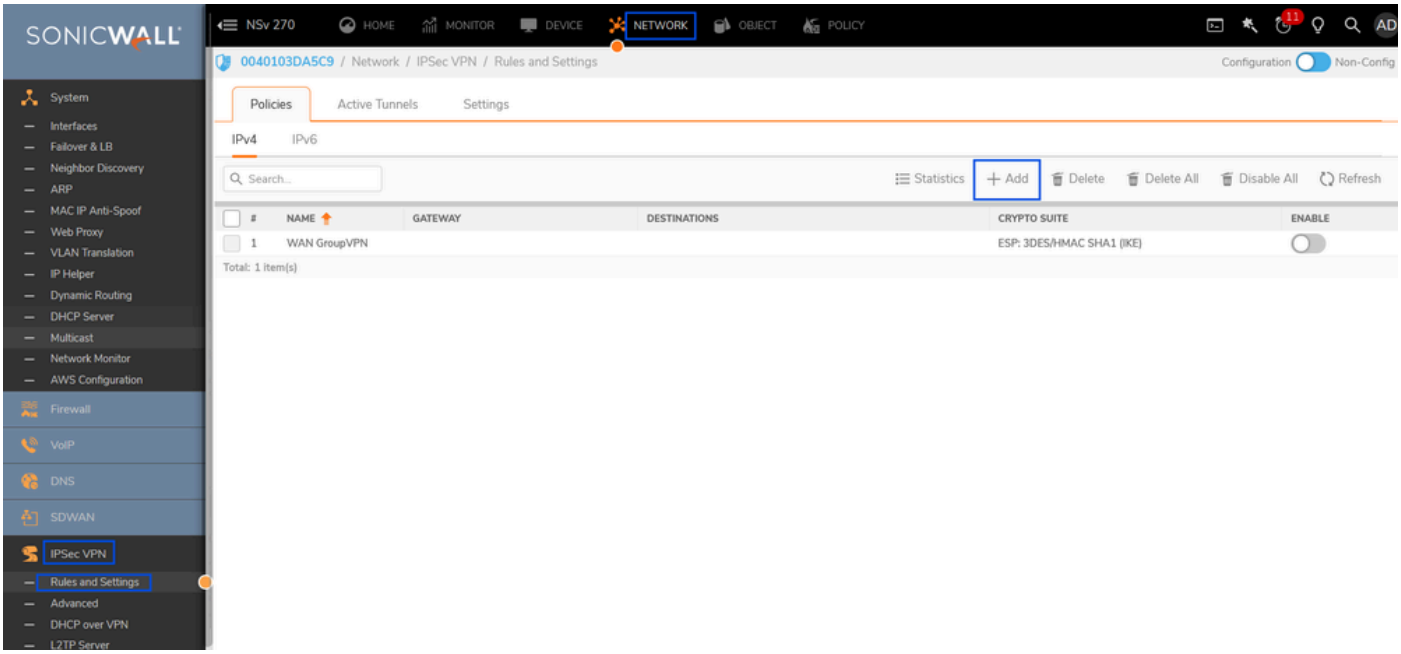
Accès sécurisé - Données pour la configuration du tunnel

Configuration du tunnel sur Sonicwall

Configuration du tunnel - Règles et paramètres

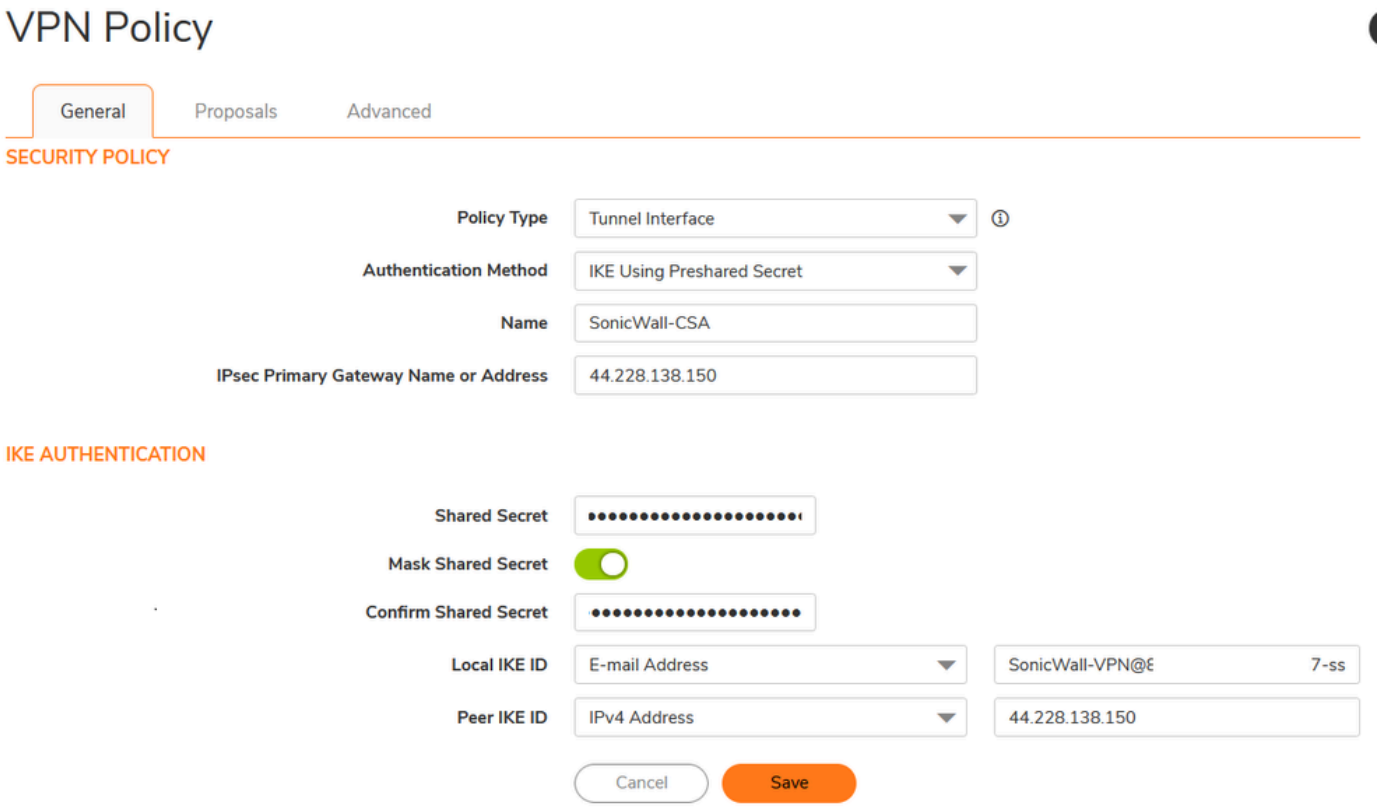
Accédez au tableau de bord Sonicwall.

- Réseau > VPN IPsec > Règles et paramètres
- Cliquez sur + Ajouter



Sonicwall - VPN IPSec - Règles et paramètres

- Sous VPN Policy , complétez la configuration VPN basée sur les données de tunnel de Secure Access et les [paramètres ipsec pris en charge]



VPN Policy

General | Proposals | Advanced

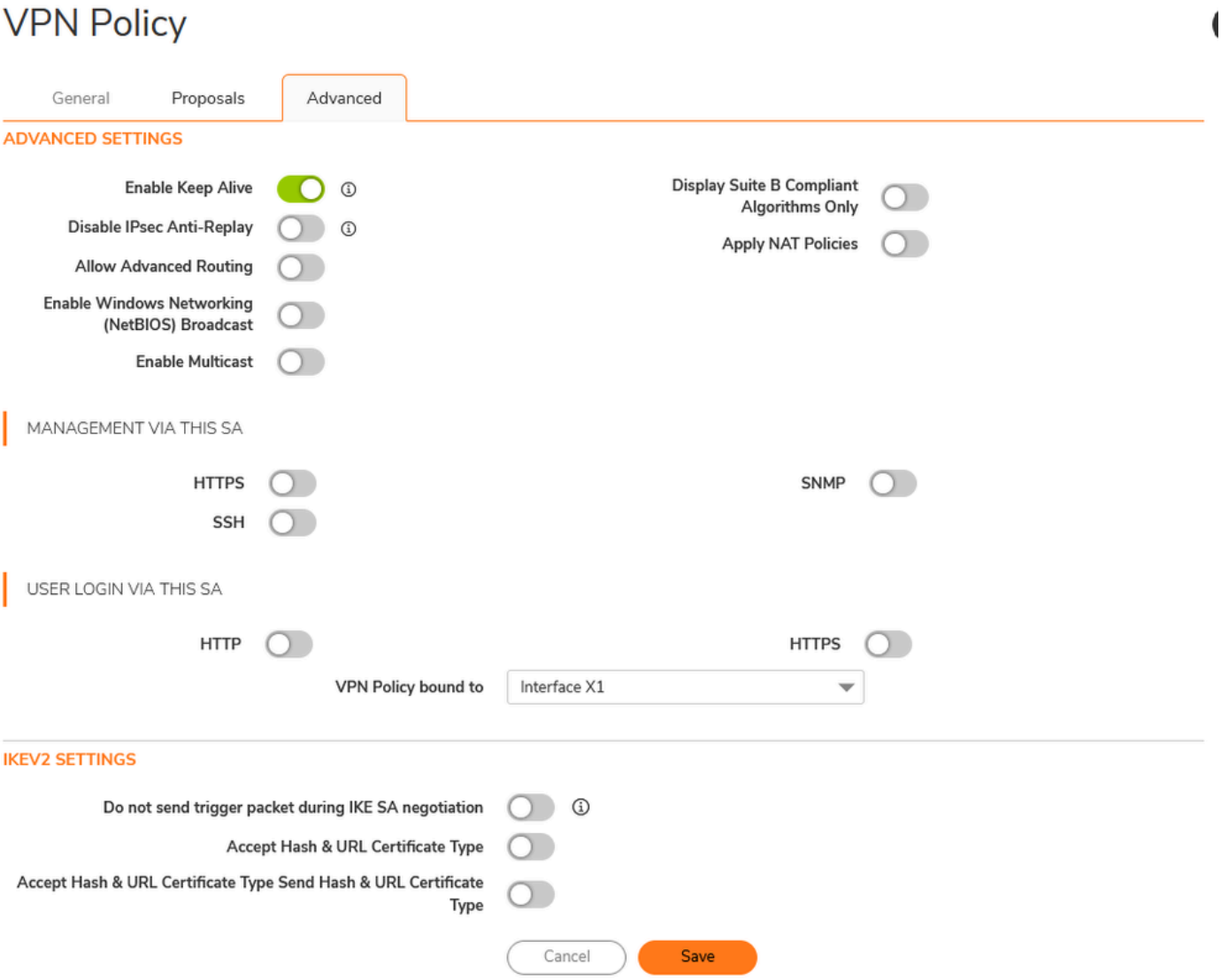
IKE (PHASE 1) PROPOSAL

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

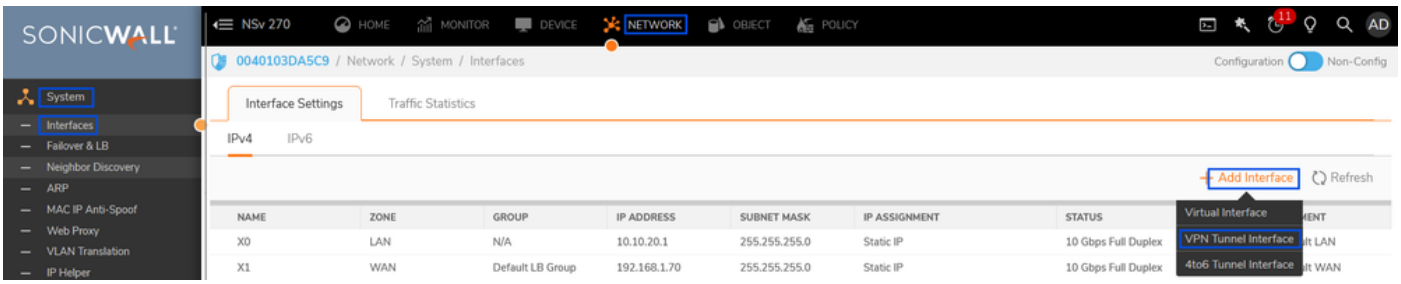


- Cliquez sur Enregistrer

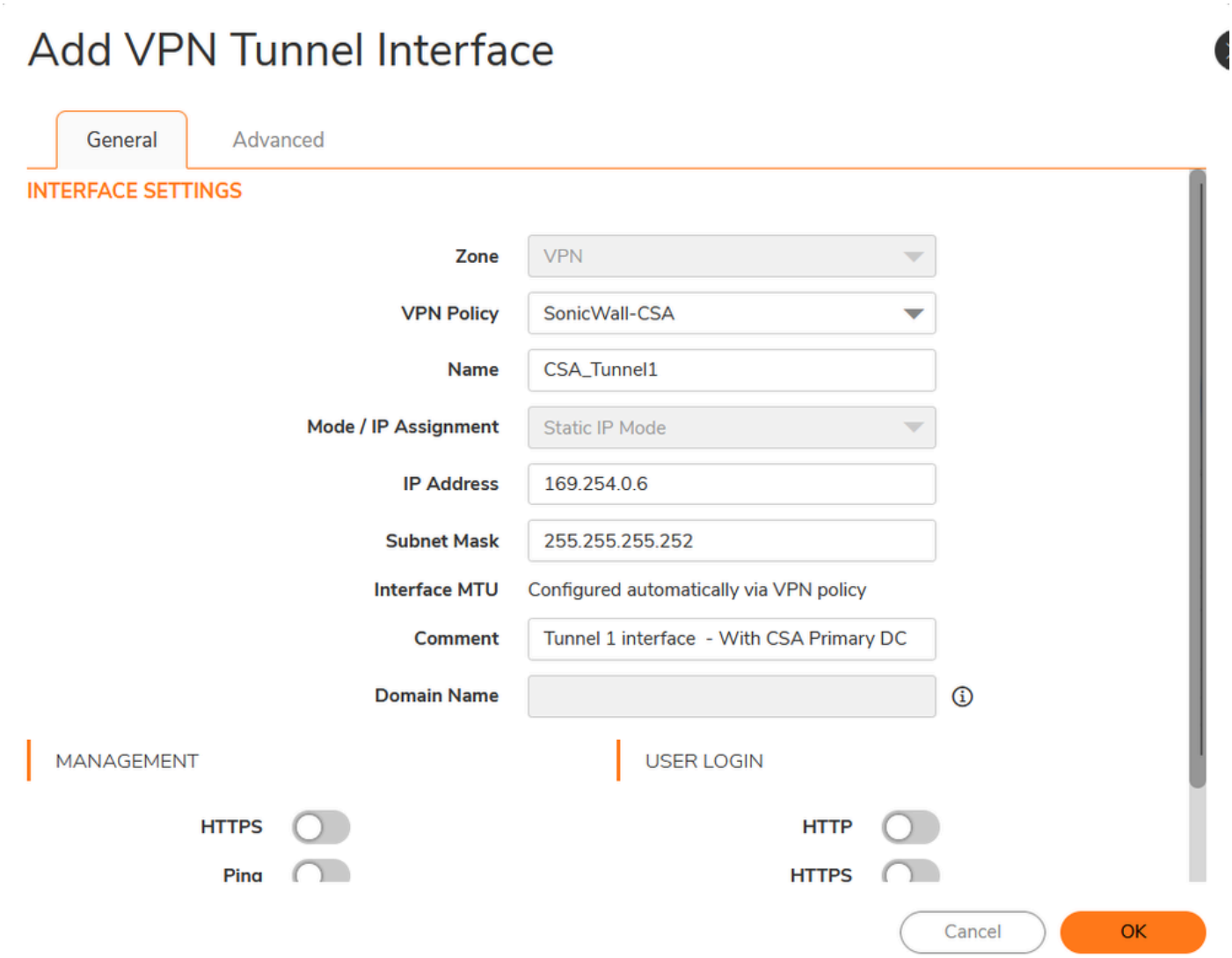
Ajouter une interface de tunnel VPN

Accédez au tableau de bord Sonicwall.

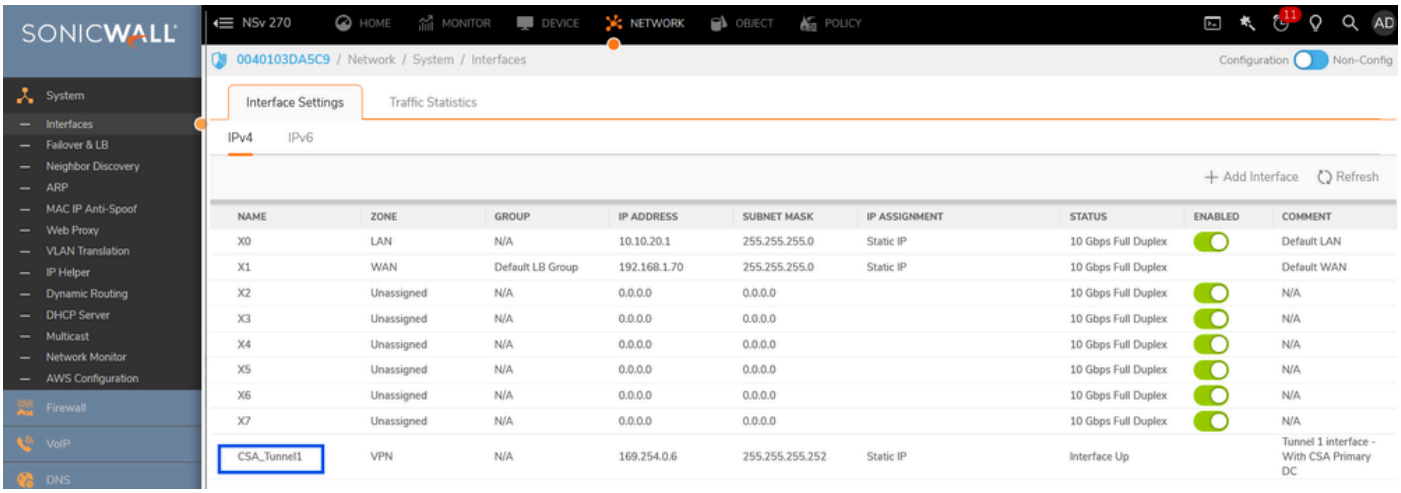
- Réseau > Système > Interface
- Cliquez sur + Ajouter une interface
- Sélectionner une interface de tunnel VPN



Sonicwall - Interfaces



- Click OK

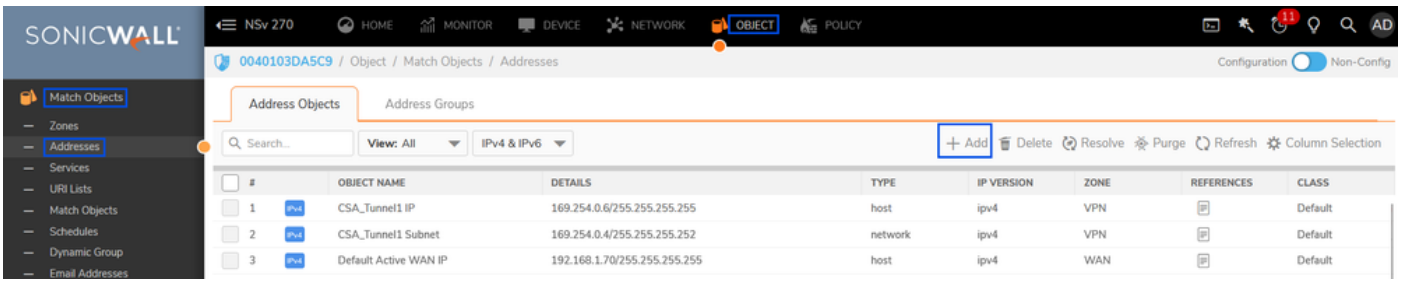


Sonicwall - Interfaces - Interface de tunnel VPN

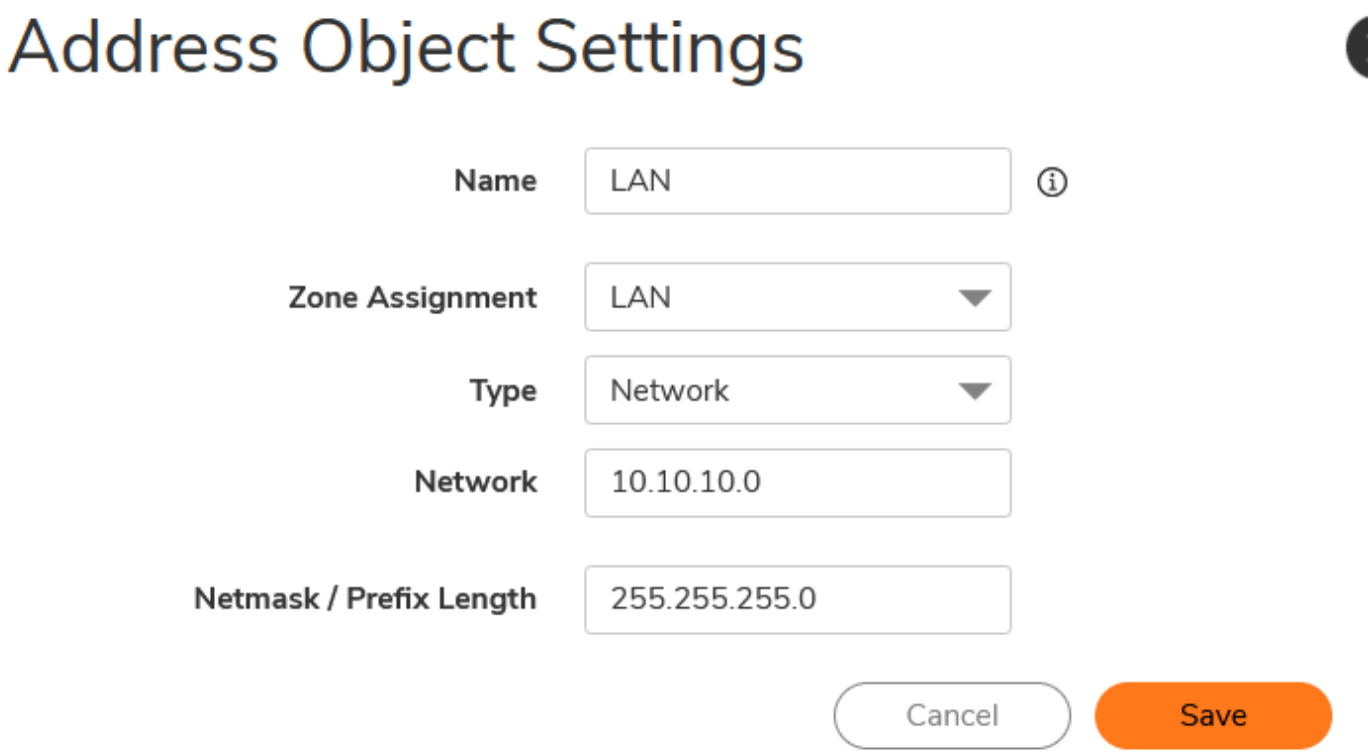
Ajouter un objet et des groupes réseau

Accédez au tableau de bord Sonicwall.

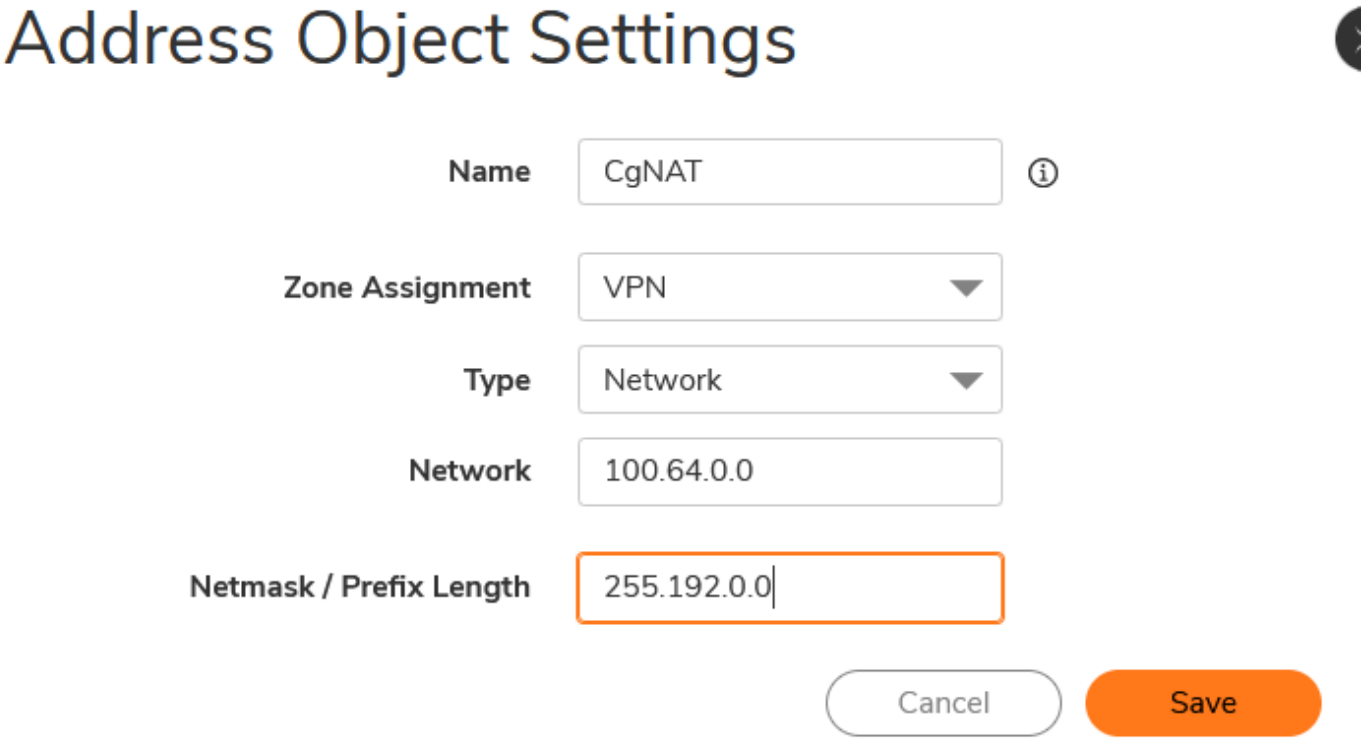
- Objet > Correspondance d'objets >Adresses
- Objets d'adressage
- Cliquez sur +Ajouter



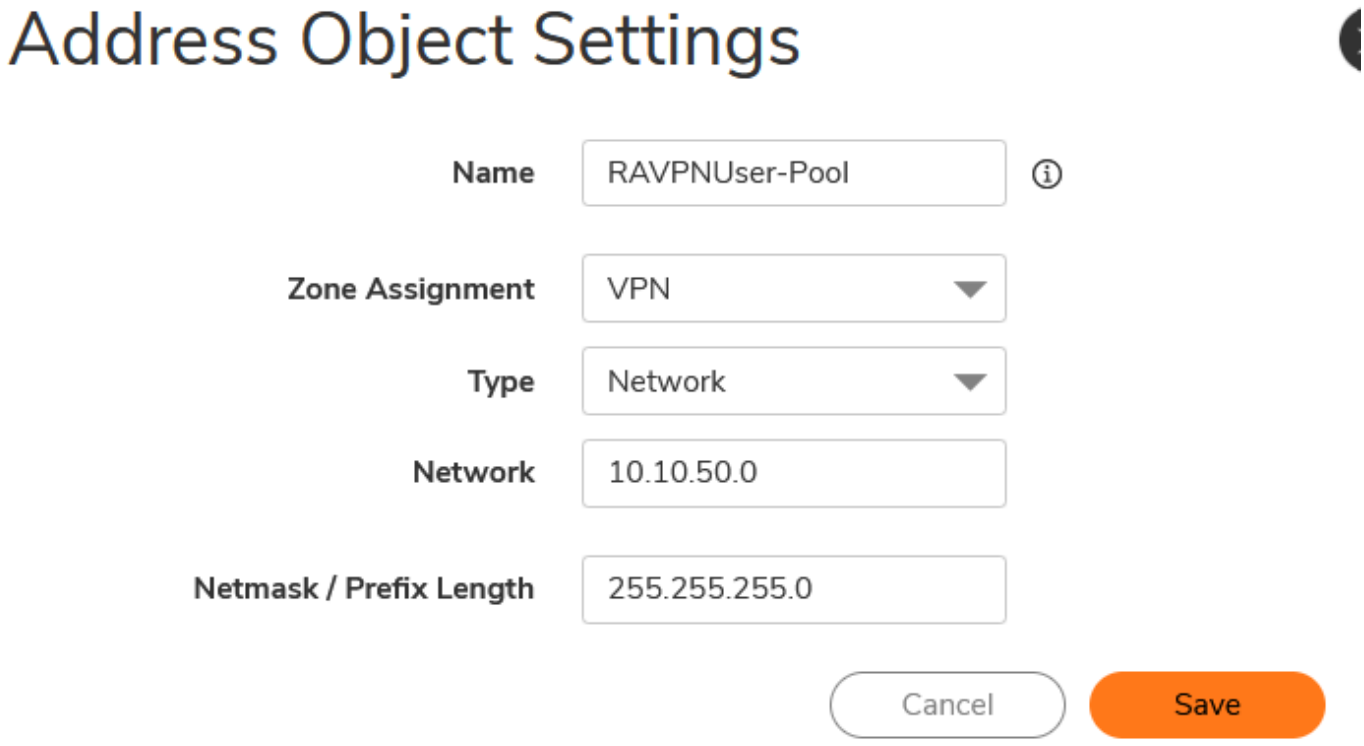
Sonicwall - Objets d'objet-adresse



- Cliquez sur Save (enregistrer)

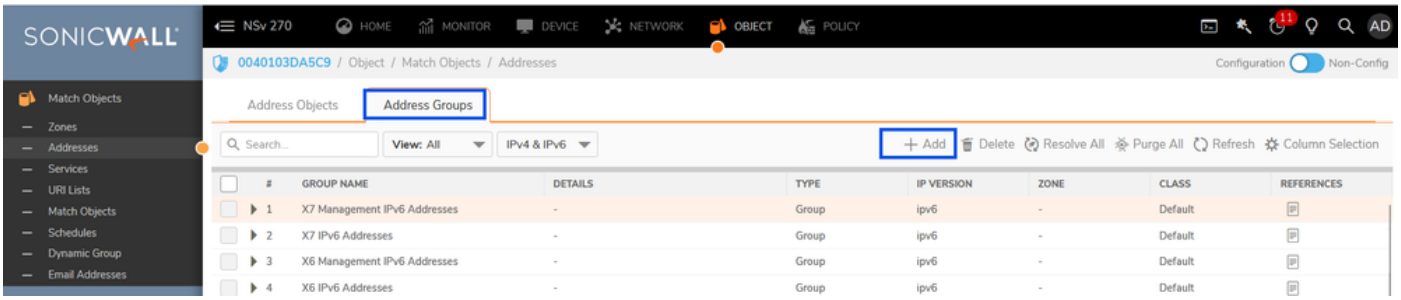


- Cliquez sur Save (enregistrer)

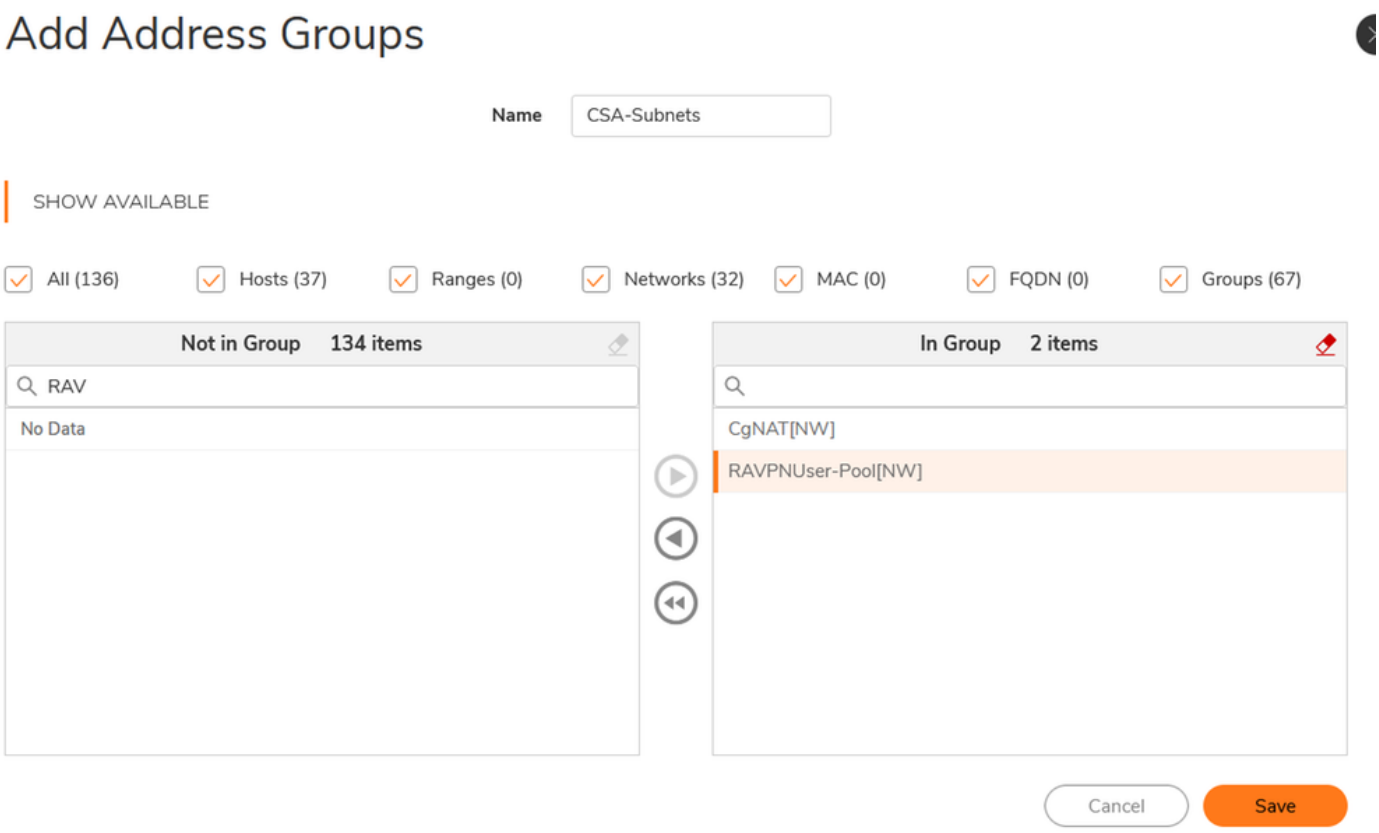


- Cliquez sur Save (enregistrer)

- Créer des groupes d'adresses
- Cliquez sur +Ajouter
- Sélectionnez l'objet d'adresse et ajoutez-les aux groupes d'adresses



Sonicwall - Objet - Groupes d'adresses

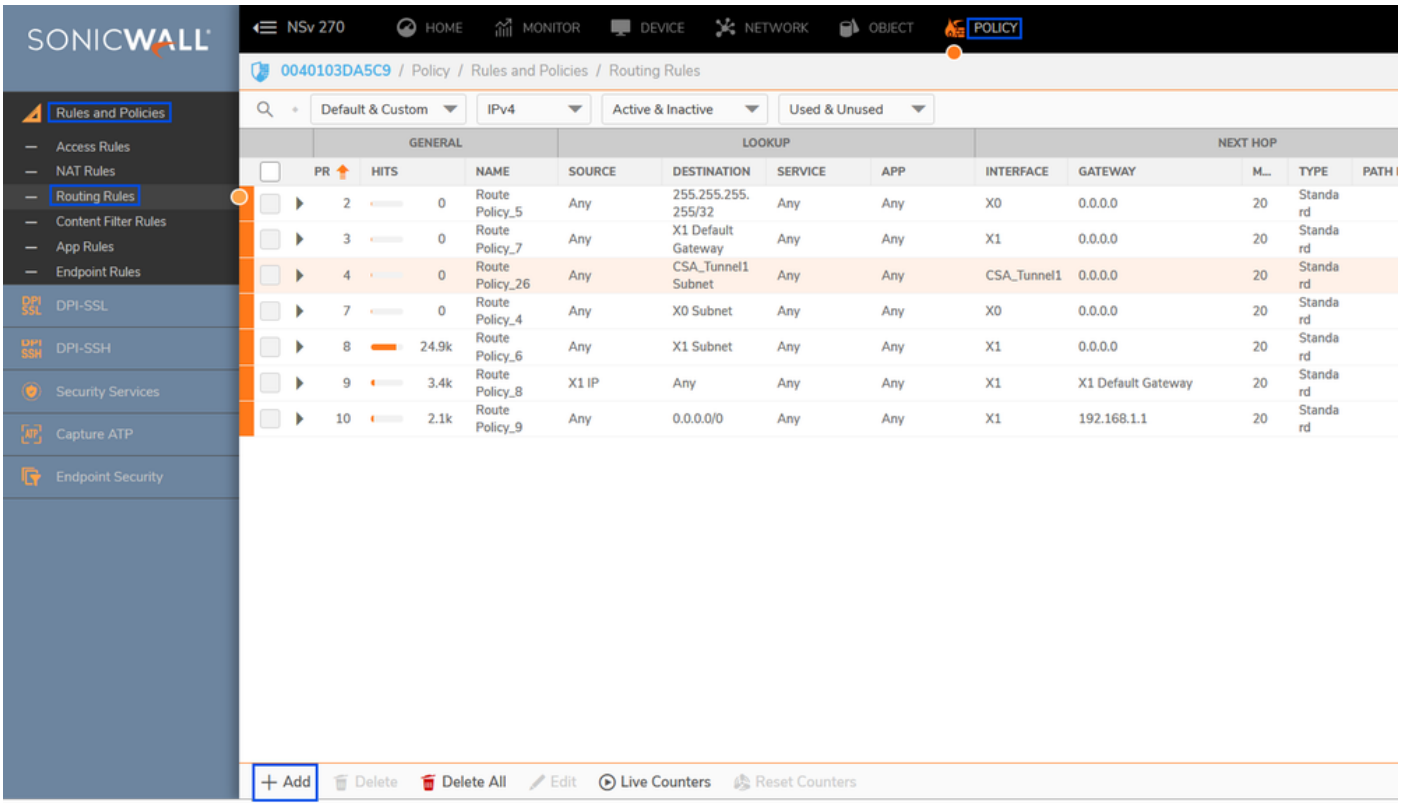


- Cliquez sur Save (enregistrer)

Ajouter une route

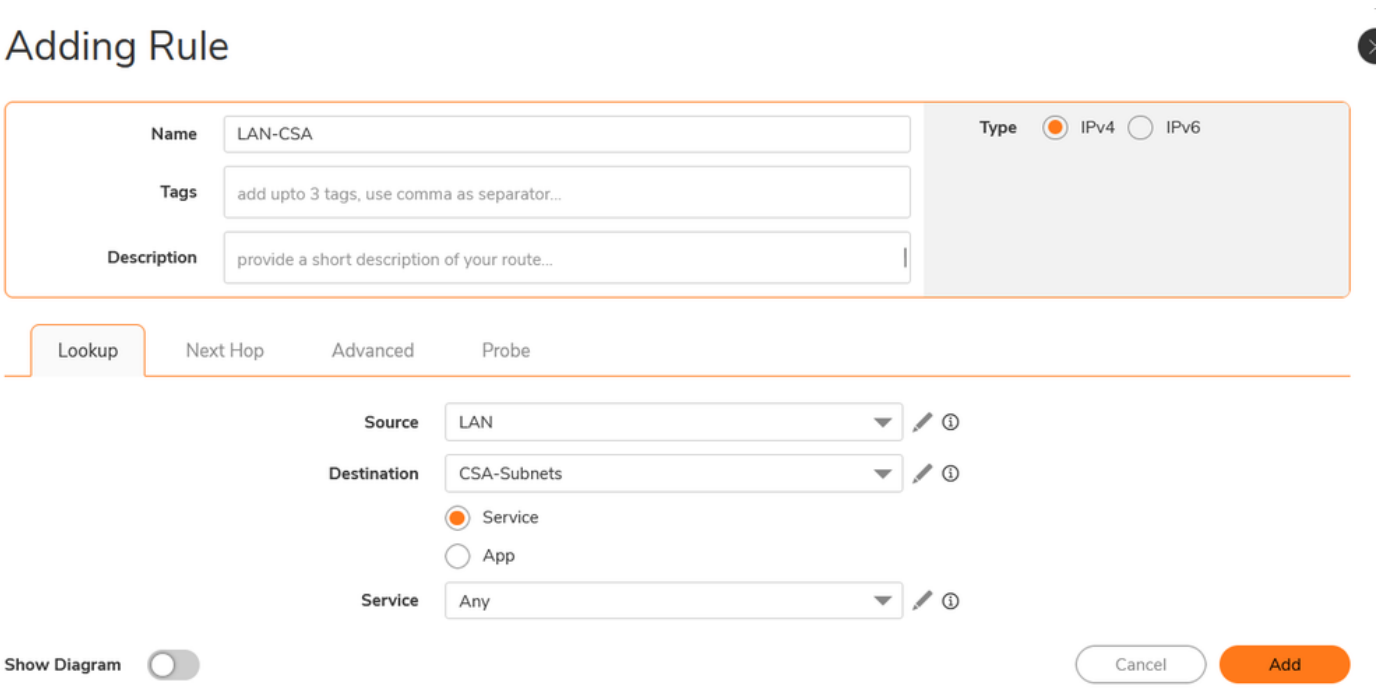
Accédez au tableau de bord Sonicwall.

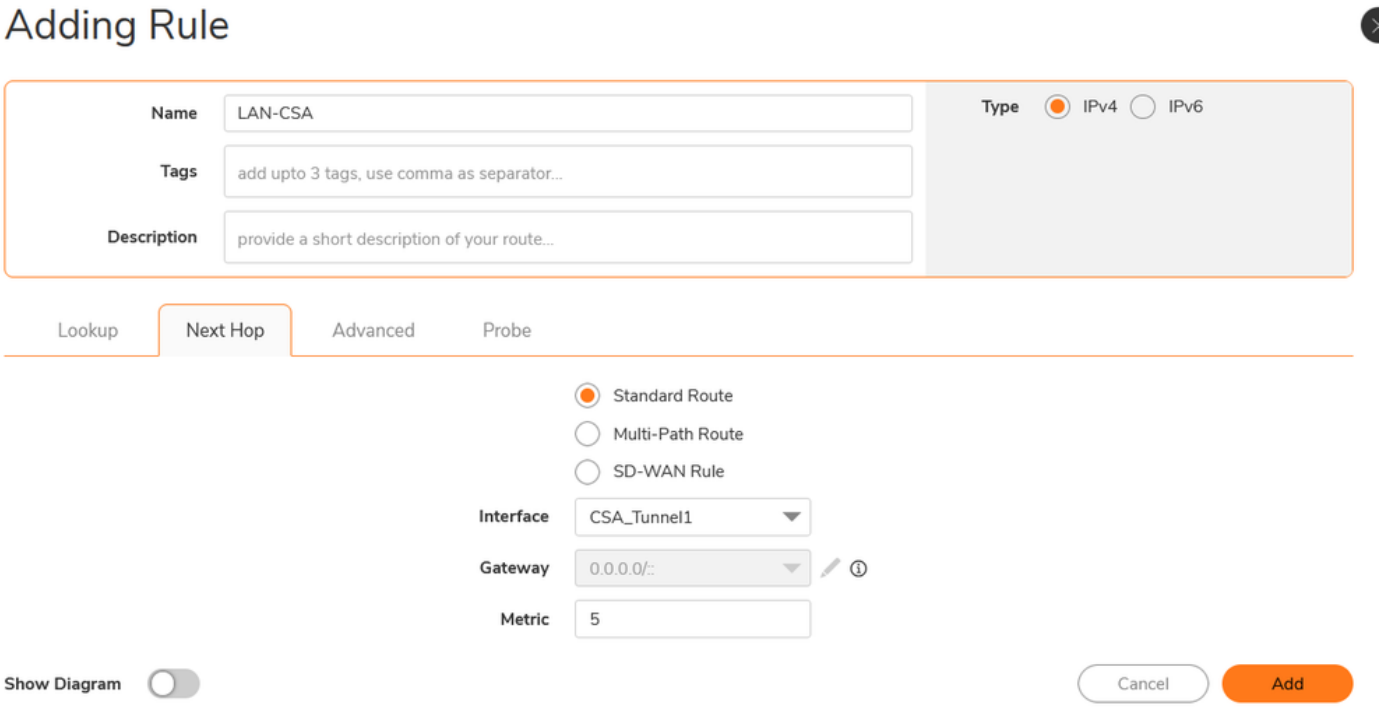
- Stratégie > Règles et stratégies > Règles de routage
- Cliquez sur + Ajouter



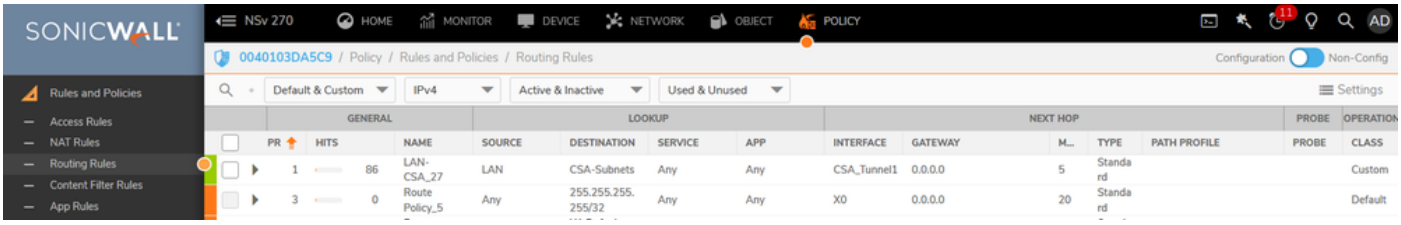
Sonicwall - Règles de routage

- Ajouter une règle de routage





- Cliquez sur + Ajouter

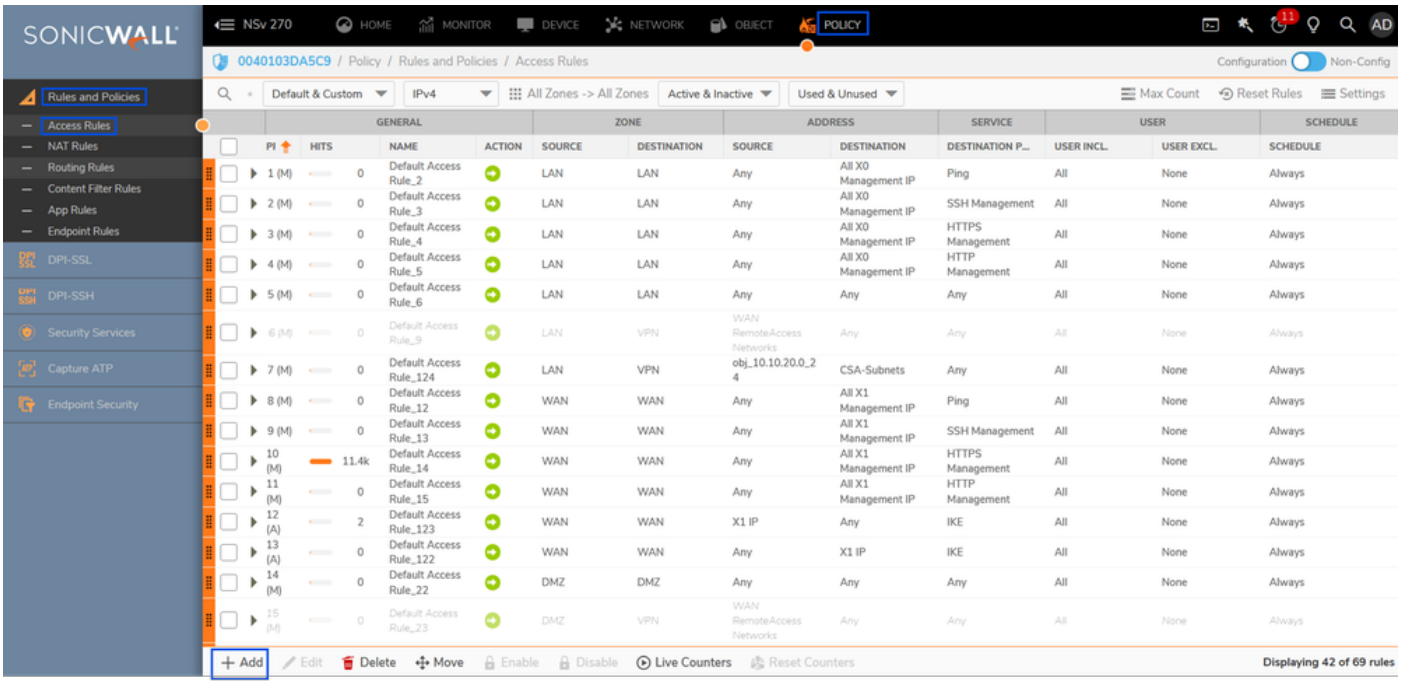


Sonicwall - Règles de routage

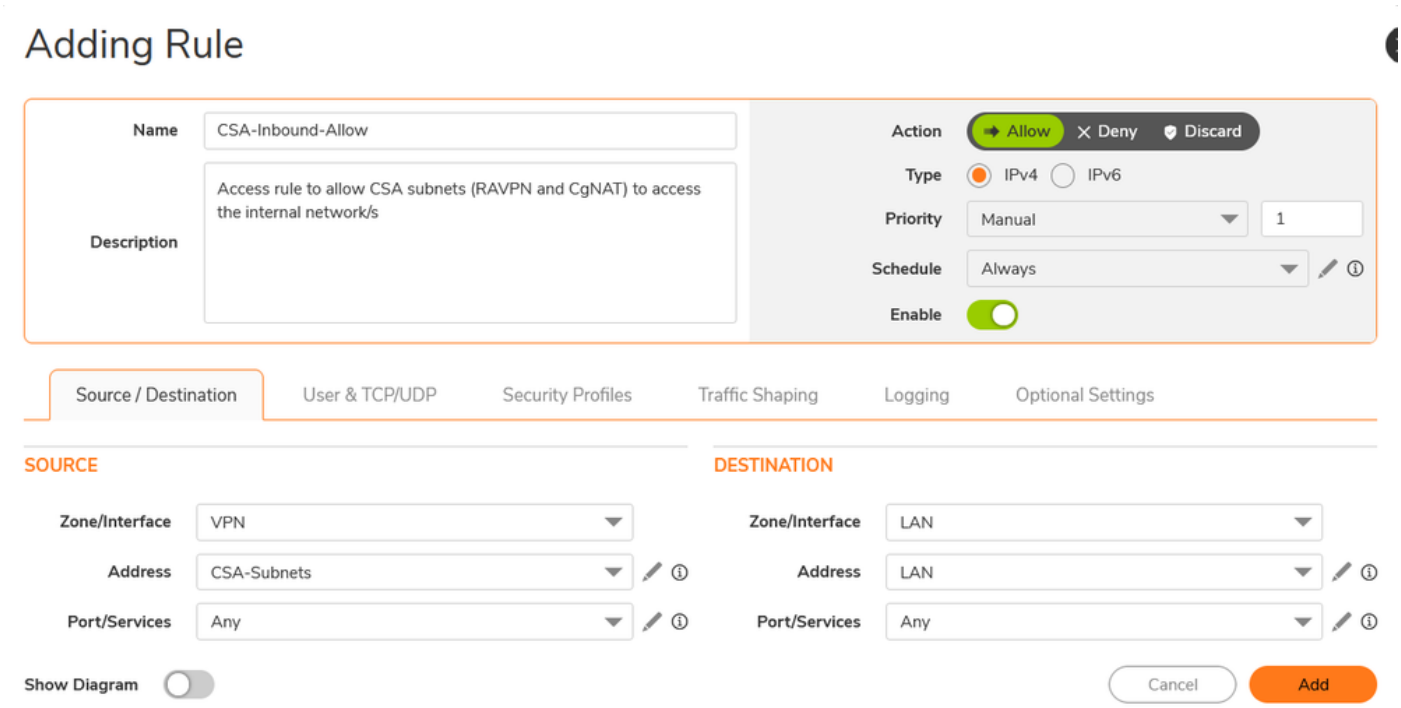
Ajouter des règles d'accès

Accédez au tableau de bord Sonicwall.

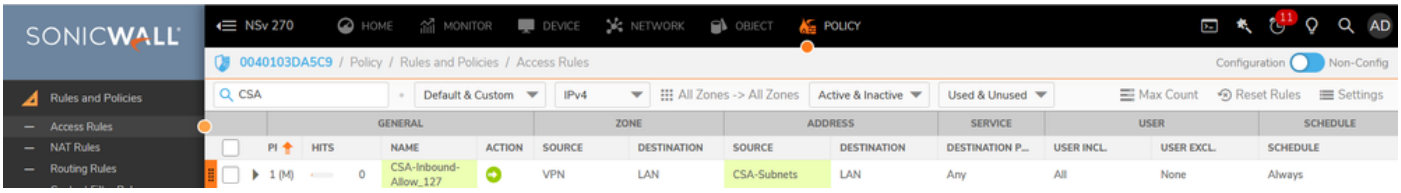
- Stratégie > Règles et stratégies > Règles d'accès
- Cliquez sur + Ajouter



Sonicwall - Règles d'accès



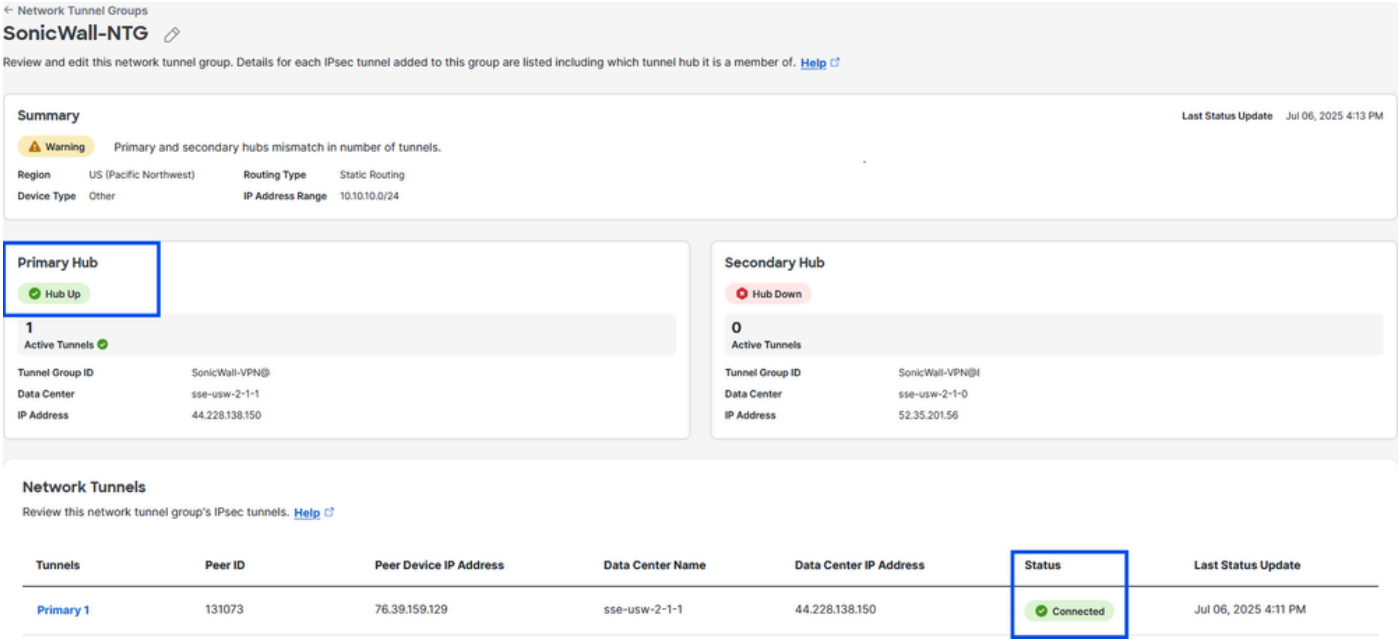
- Cliquez sur +Ajouter



Sonicwall - Règles d'accès

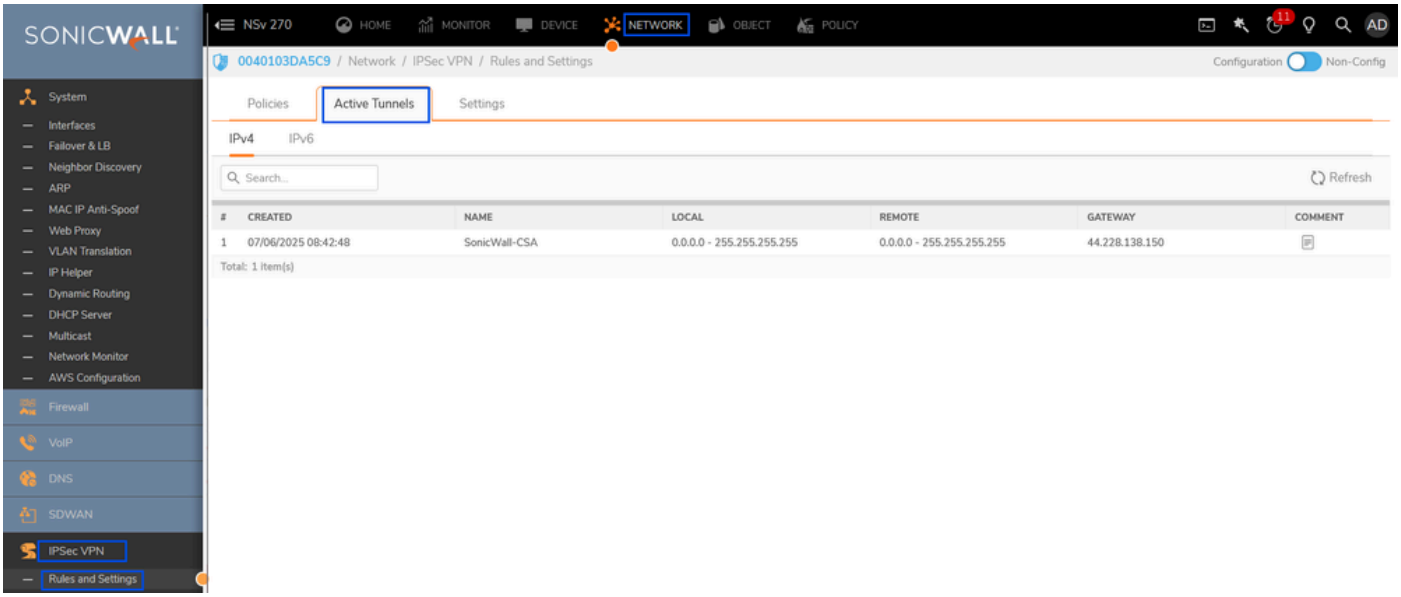
Vérifier

- État du tunnel sur accès sécurisé



Accès sécurisé - Groupe de tunnels réseau - État VPN

- État du tunnel sur le pare-feu Sonicwall



Sonicwall - État VPN IPSec

Vous pouvez effectuer le même processus pour configurer le tunnel entre le data center secondaire Secure Access et Sonicwall

Maintenant , le tunnel est UP sur Secure Access et Sonicwall, vous pouvez continuer à configurer l'accès aux ressources privées via RA-VPN , Browser Based ZTA ou Client Based ZTA sur Secure Access Dashboard

Dépannage

PC utilisateur

- Vérifiez que l'utilisateur peut se connecter/s'inscrire à RAVPN/ZTNA correctement ou non. Si ce n'est pas le cas, identifiez les raisons de la défaillance de la connexion du plan de contrôle.
- Vérifiez que le réseau auquel l'utilisateur tente d'accéder est supposé passer par le tunnel RAVPN ou ZTNA . Sinon, vérifiez la configuration sur la tête de réseau .

Accès sécurisé

- Vérifiez la configuration du pilotage du trafic sur le profil de connexion RAVPN pour confirmer que le réseau de destination est configuré pour envoyer le tunnel vers l'accès sécurisé.
- Vérifiez que la ressource privée est définie avec un protocole/des ports valides et que les mécanismes de connexion ZTNA/RAVPN sont vérifiés.
- Vérifiez que la stratégie d'accès est configurée pour autoriser l'utilisateur RAVPN/ZTNA à accéder au réseau de ressources privées et que son est placé dans un ordre où aucune autre règle n'est prioritaire pour bloquer le trafic.
- Vérifiez que le tunnel IPSec est activé et que l'accès sécurisé indique des routes client valides via le routage statique qui couvre la ressource privée à laquelle l'utilisateur tente d'accéder.

Paroi Sonique

- Vérifiez que le tunnel IPSec est activé ou non (IKE & IPSec SA).
- Vérifiez que la ou les routes client(s) sont correctement annoncées.
- Vérifiez que les sources de trafic de l'utilisateur RAVPN/ZTNA destinées à une ressource privée derrière Sonicwall atteignent le pare-feu Sonicwall via un tunnel en effectuant une capture de paquets sur Sonicwall.
- Vérifiez que le trafic a atteint la ressource privée et répondez au client RAVPN/ZTNA ou non. Si oui, vérifiez que ces paquets atteignent l'interface Sonical X0 (LAN).
- Vérifiez que Sonicwall transfère le trafic de retour via le tunnel IPSec vers Secure Access.

Informations connexes

- Assistance technique de Cisco et téléchargements
- Centre d'aide Cisco Secure Access
- Module d'accès Zero Trust
- Dépannez L'Erreur D'Accès Sécurisé « Le Service D'Inscription Ne Répond Pas. Contactez votre service d'assistance informatique"

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.