Sonicwall Firewallを使用したセキュアアクセスの設定

内容

はじめに

このドキュメントでは、スタティックルーティングを使用して、セキュアアクセスからSonicwallファイアウォールへの間にIPSec VTIトンネルを設定する方法について説明します。

前提条件

- ユーザプロビジョニングの設定
- ZTNA SSO認証設定
- リモートアクセスVPNセキュアアクセスの設定

要件

次の項目に関する知識があることが推奨されます。

- Sonicwall (NSv270 - SonicOSX 7.0.1)ファイアウォール

- セキュアなアクセス
- Cisco Secure Client:VPN（トンネルモード）
- Cisco Secureクライアント – ZTNA
- クライアントレスZTNA

使用するコンポーネント

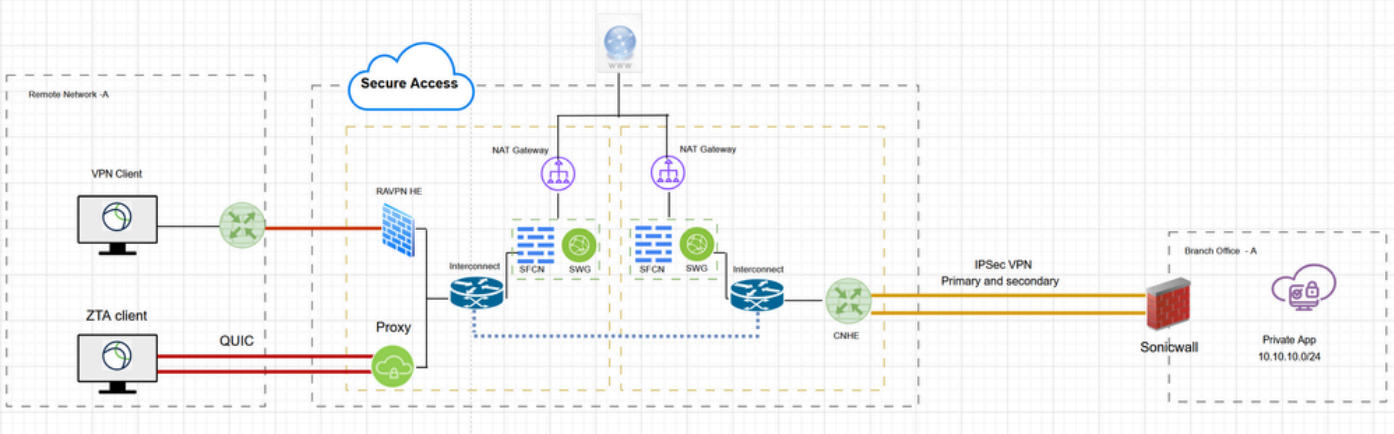
このドキュメントの情報は、次のハードウェアに基づくものです。

- Sonicwall（NSv270 - SonicOSX 7.0.1)ファイアウォール
- セキュアなアクセス
- Cisco Secure Client:VPN（トンネルモード）
- Cisco Secureクライアント – ZTNA

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

ネットワーク図



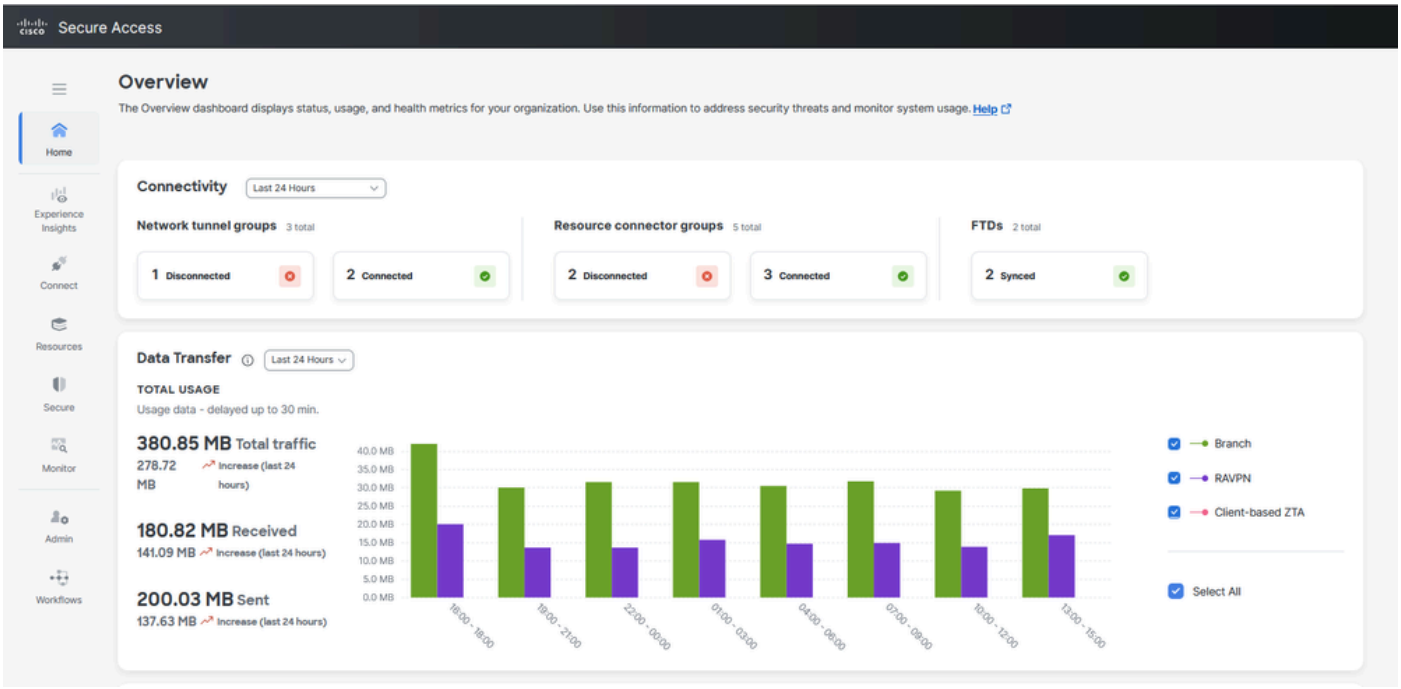
ネットワーク図

設定

セキュアアクセスでのネットワークトンネルグループ(VPN)の設定

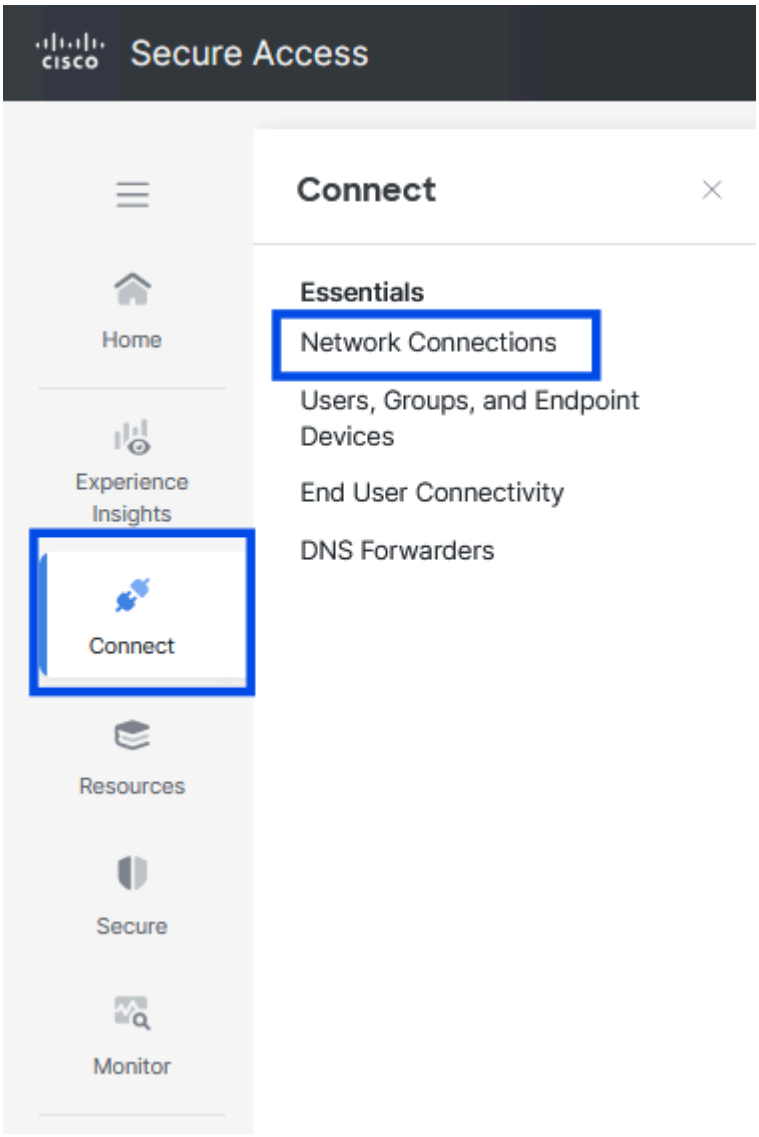
セキュアアクセスとSonicwall間のVPNトンネルを設定するには

- セキュアアクセスの管理ポータルに移動します



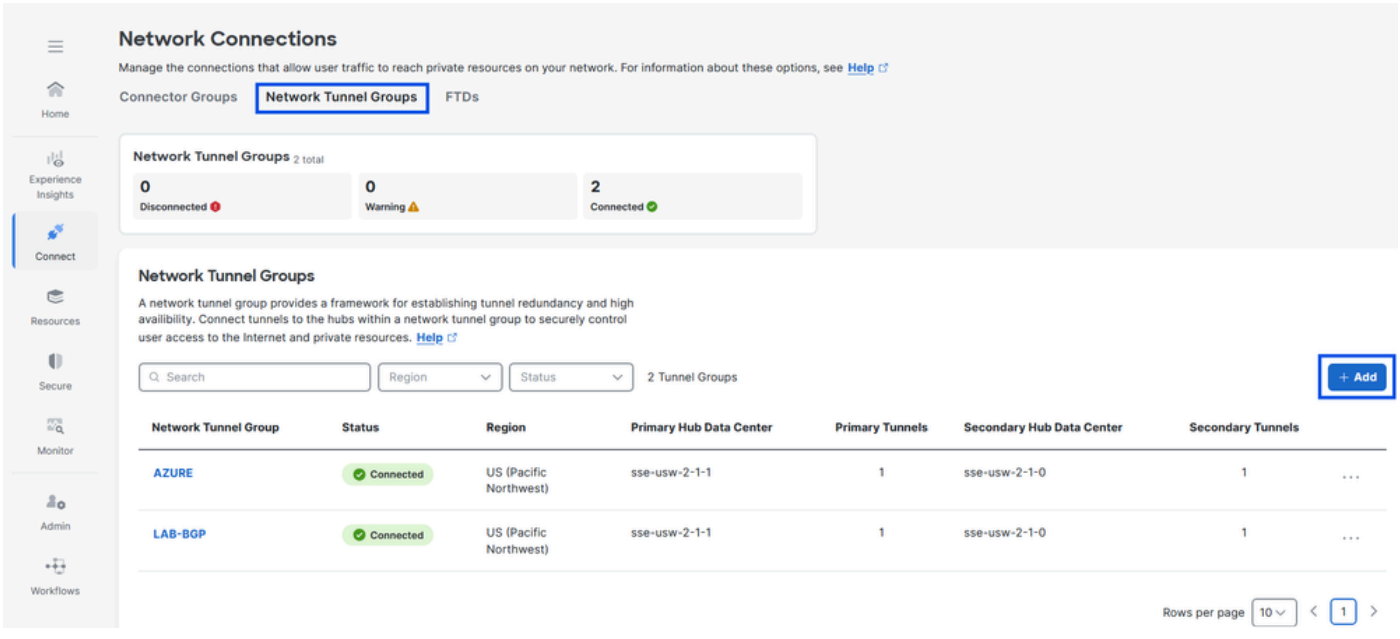
セキュアアクセス – メインページ

- Connect > Network Connectionsの順にクリックします。



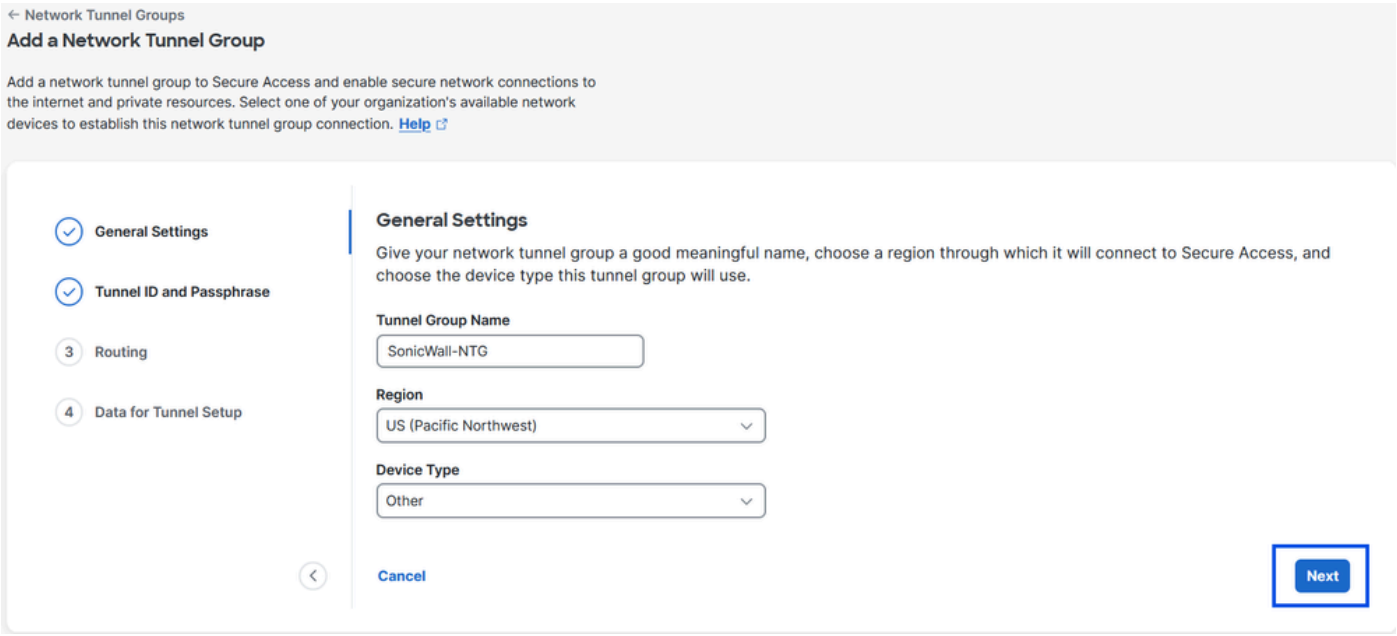
セキュアなアクセス：ネットワーク接続

- Network Tunnel Groups の下で、+Addをクリックします。



セキュアアクセス – ネットワークトンネルグループ

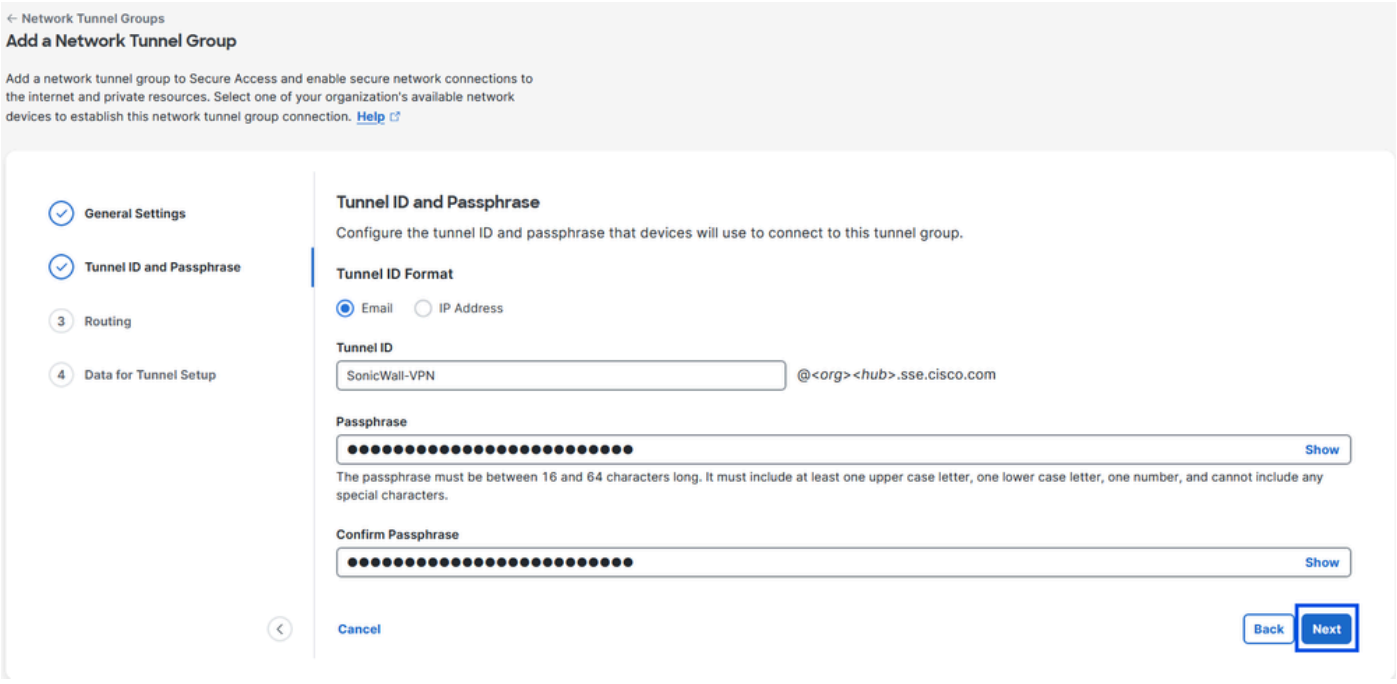
- トンネルグループ名、リージョン、およびデバイスタイプの設定
- [Next] をクリックします。



セキュアアクセス – ネットワークトンネルグループ – 一般設定

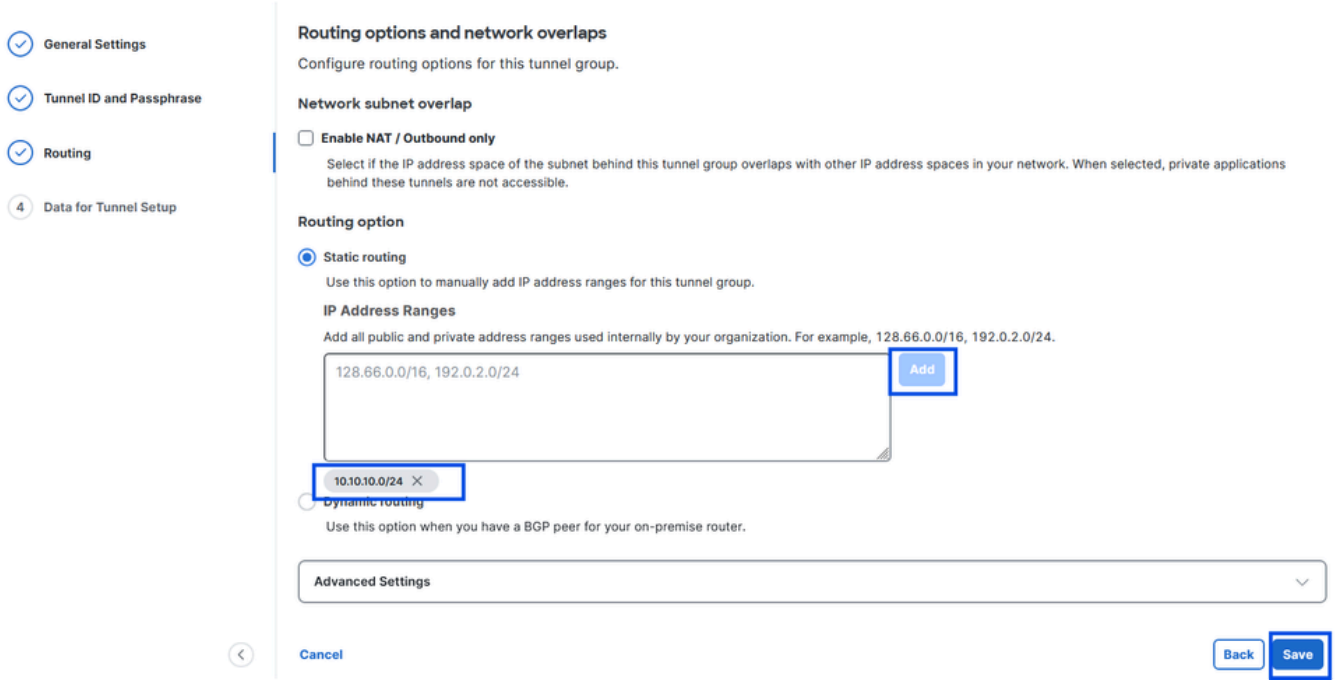
注：ファイアウォールの場所に最も近い地域を選択してください。

- トンネルIDの形式とパスフレーズの設定
- [Next] をクリックします。



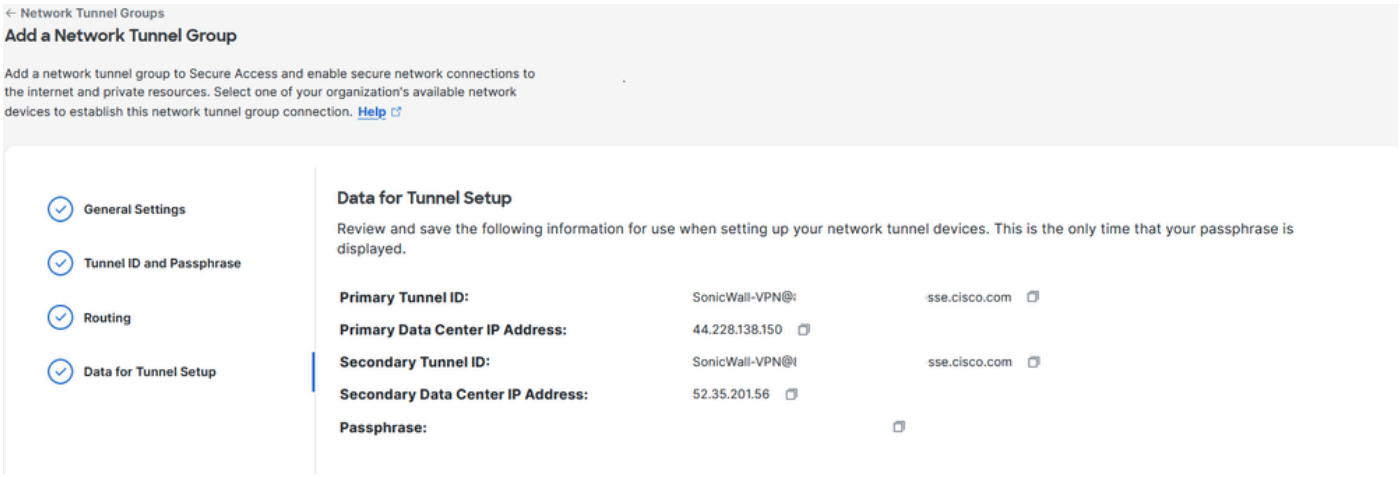
セキュアアクセス – トンネルIDとパスフレーズ

- ネットワークに設定したIPアドレス範囲、ホスト、またはサブネットを設定し、トラフィックをセキュアアクセス経由で通過させる
- [Add] をクリックします。
- [Save] をクリックします。



セキュアアクセス – トンネルグループ – ルーティングオプション

Saveをクリックすると、トンネルに関する情報が表示されます。次の設定手順のためにその情報を保存してください



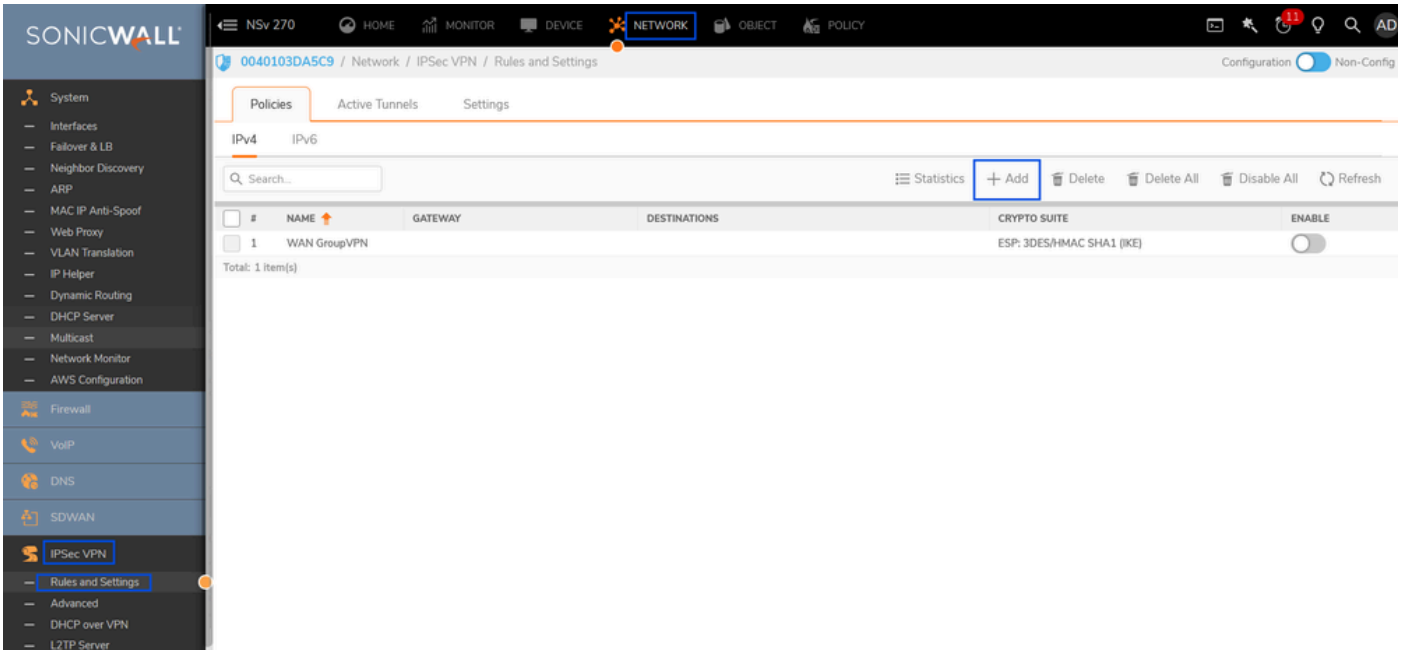
セキュアアクセス – トンネルセットアップ用データ

Sonicwallでのトンネルの設定

トンネルの設定 – ルールと設定

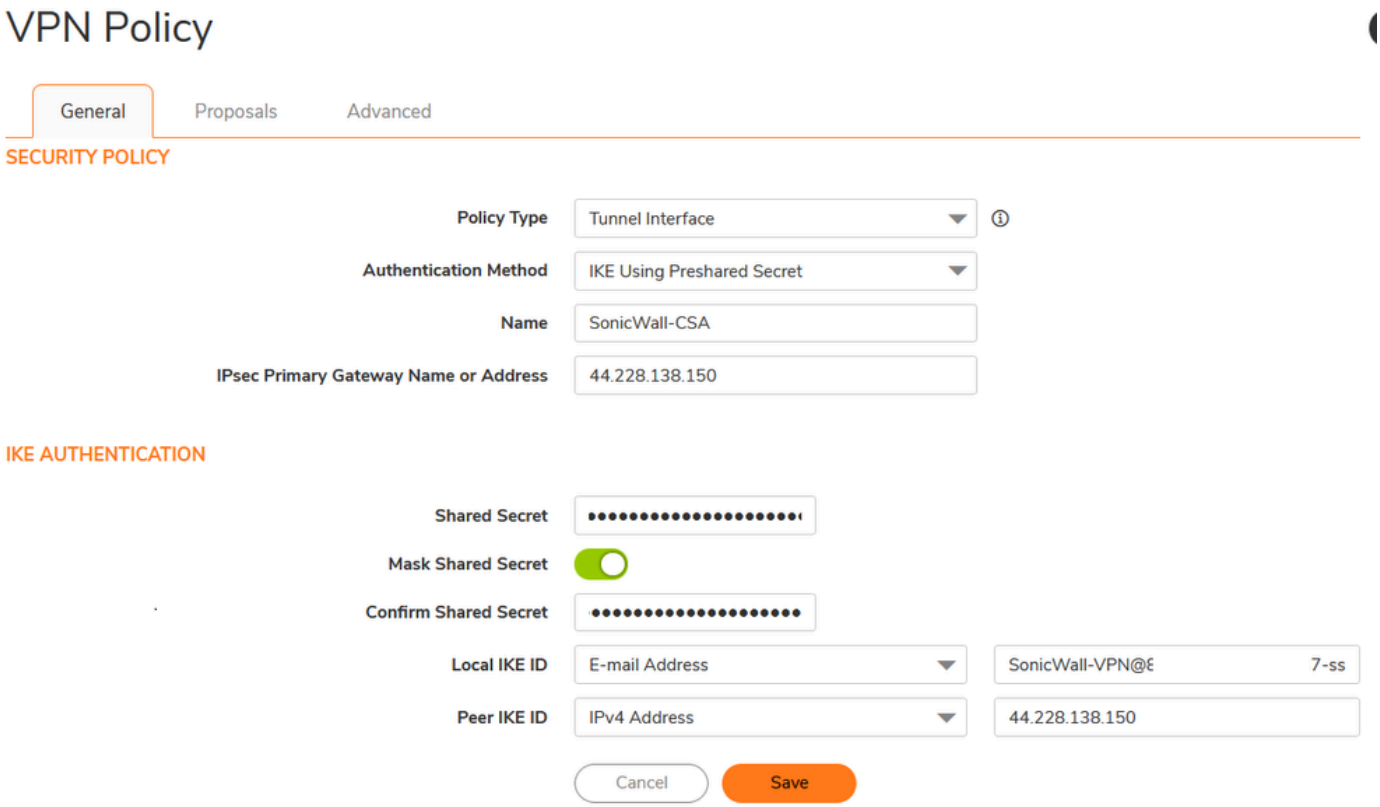
Sonicwall Dashboardに移動します。

- Network > IPsec VPN > Rules and Settings
- +追加をクリックします。



Sonicwall - IPSec VPN – ルールと設定

- VPN Policyの下で、Secure Accessからのトンネルデータと[supported-ipsec-parameters]に基づくVPN設定に入力します。



VPN Policy

General | Proposals | Advanced

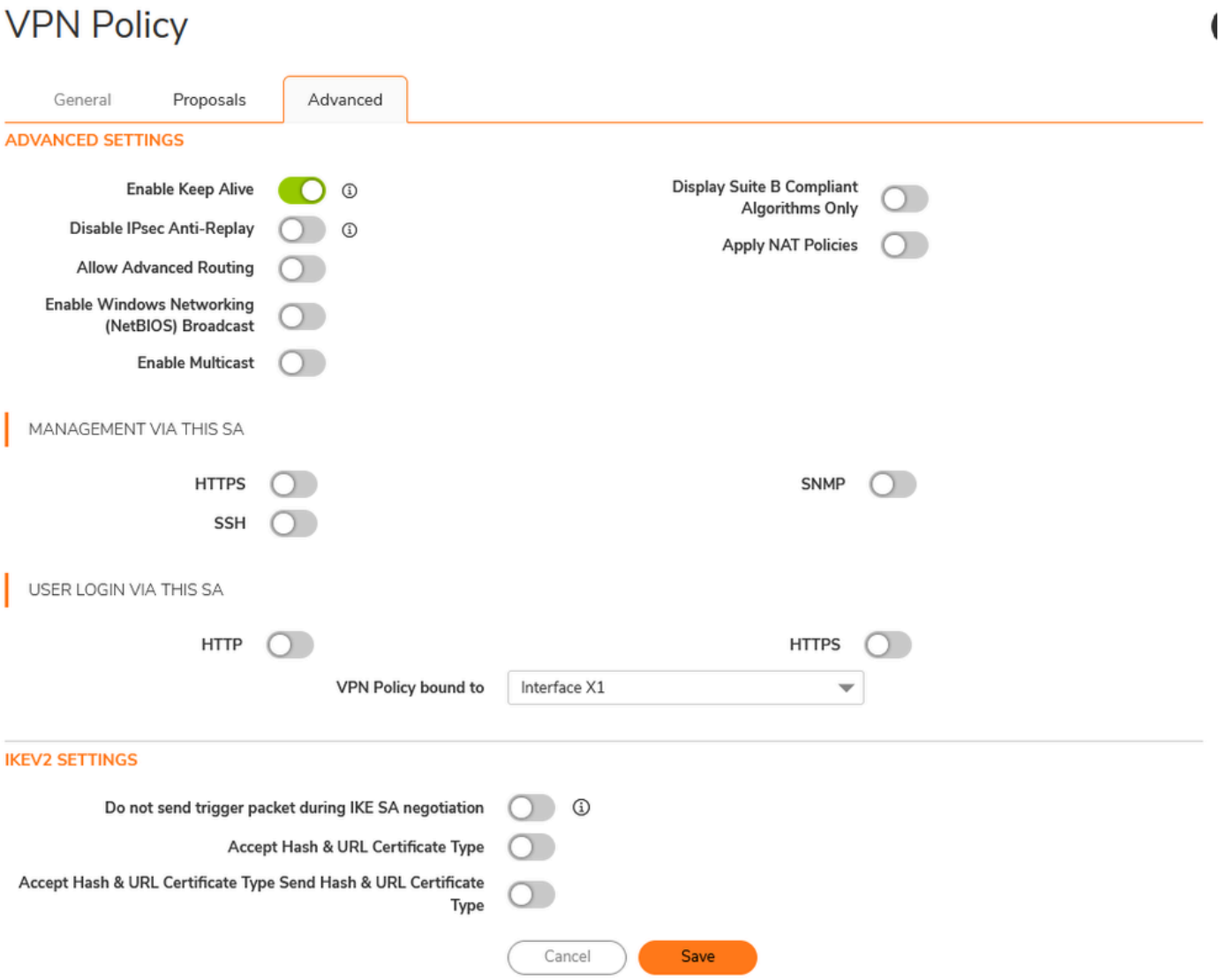
IKE (PHASE 1) PROPOSAL

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

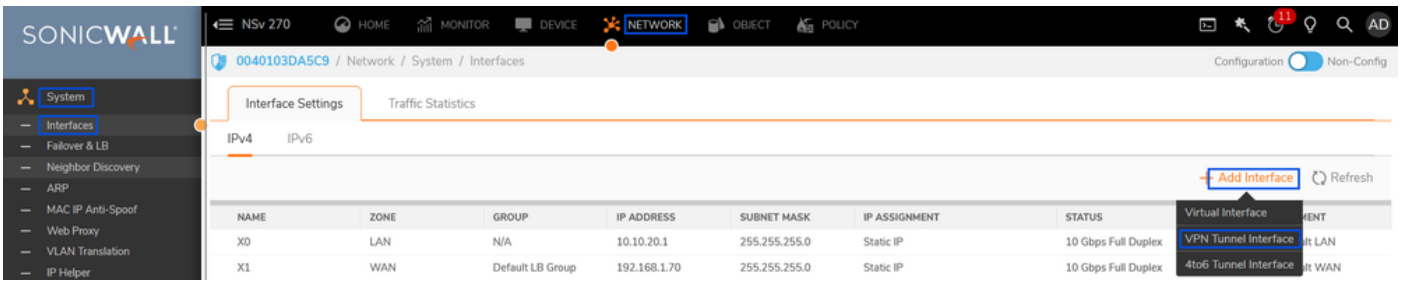


- [Save] をクリックします。

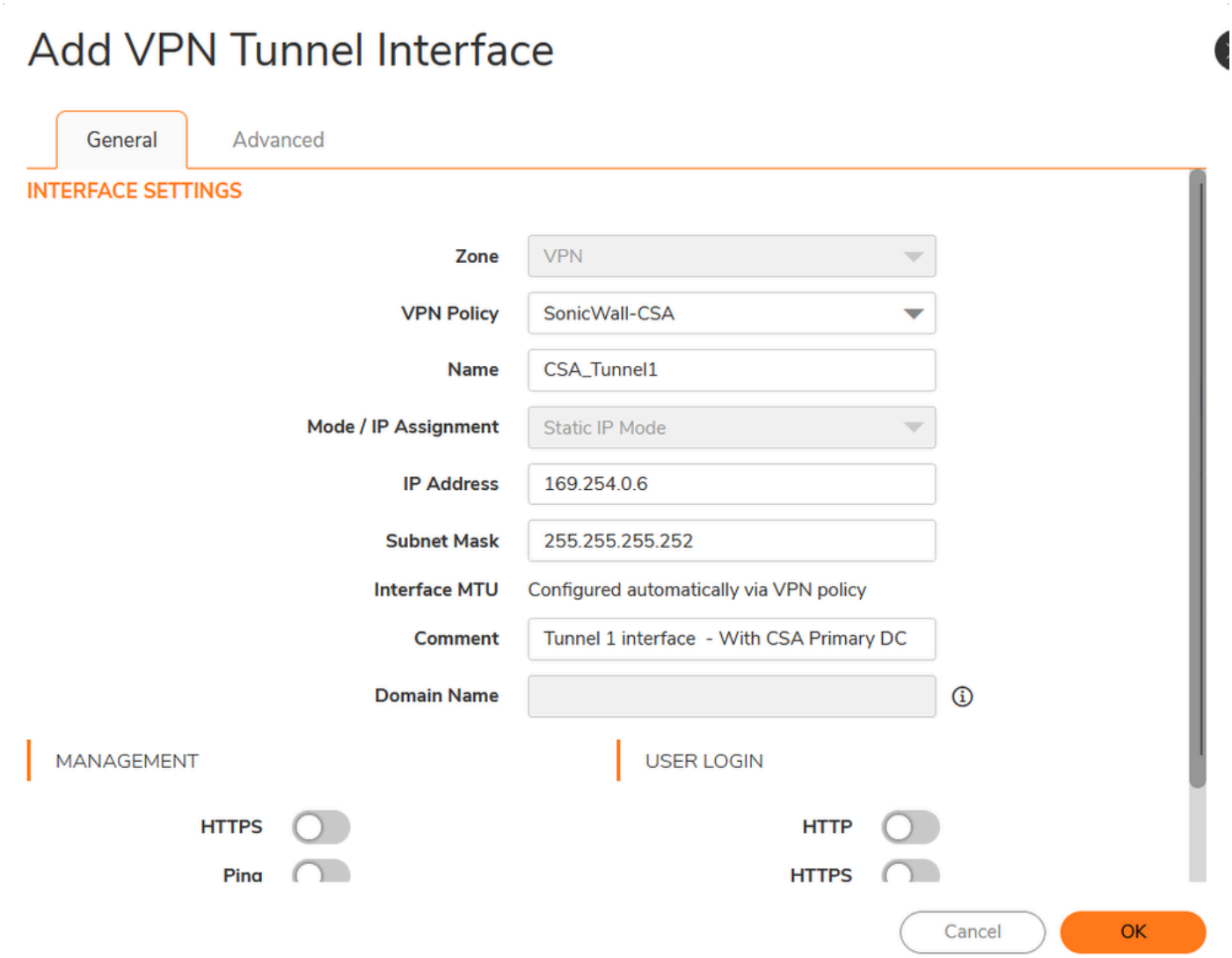
VPNトンネルインターフェイスの追加

Sonicwall Dashboardに移動します。

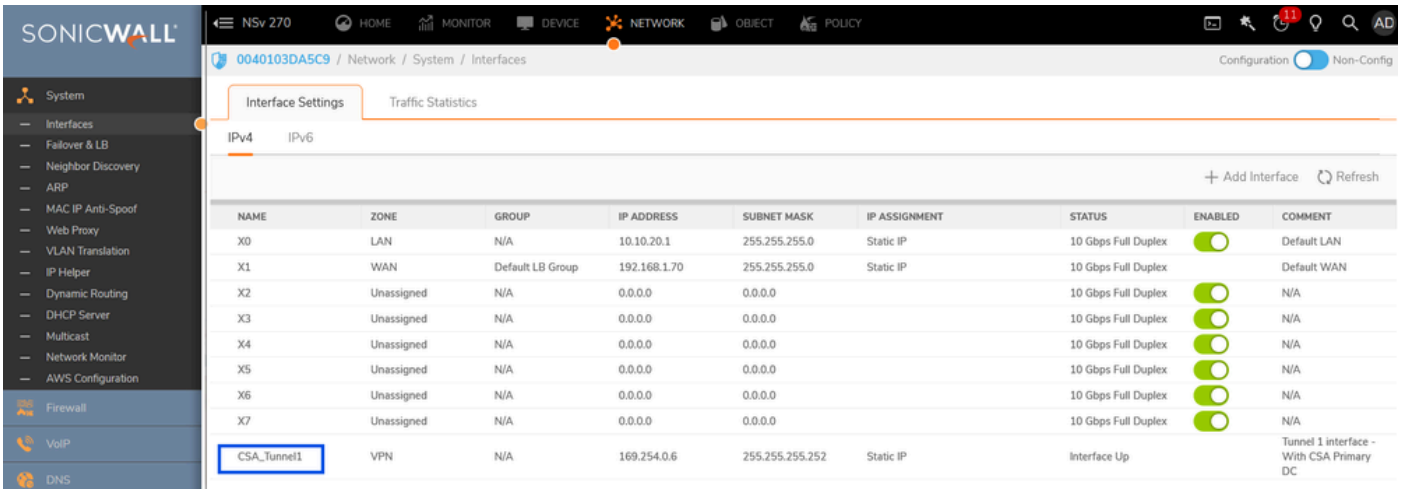
- Network > System > Interface
- + Add Interfaceをクリックします。
- VPNトンネルインターフェイスの選択



Sonicwall：インターフェイス



- [OK] をクリックします。

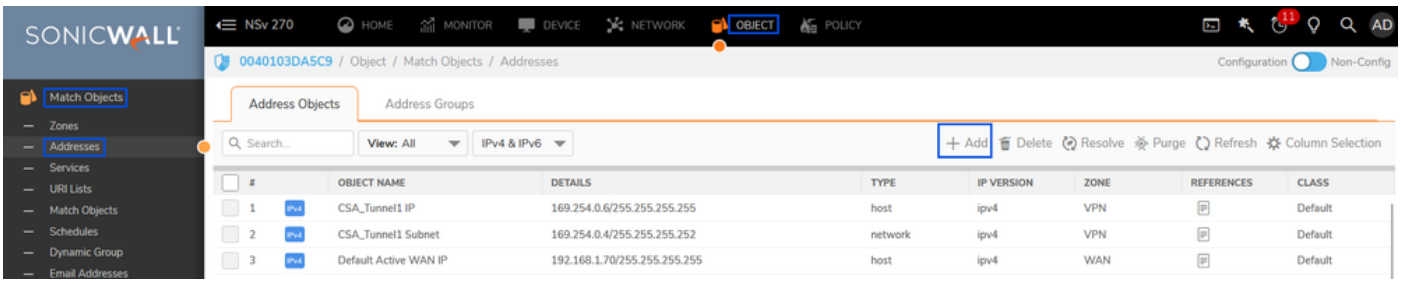


Sonicwall – インターフェイス – VPNトンネルインターフェイス

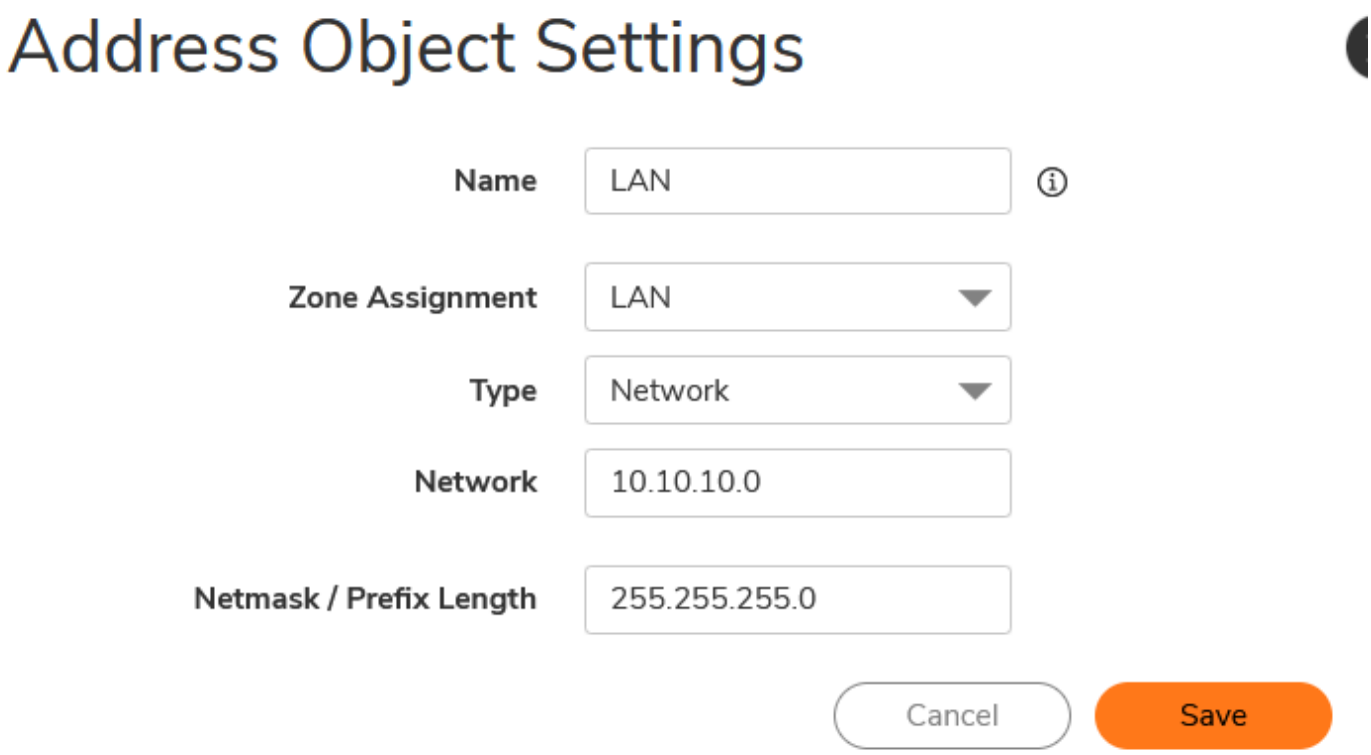
ネットワークオブジェクトとグループの追加

Sonicwall Dashboardに移動します。

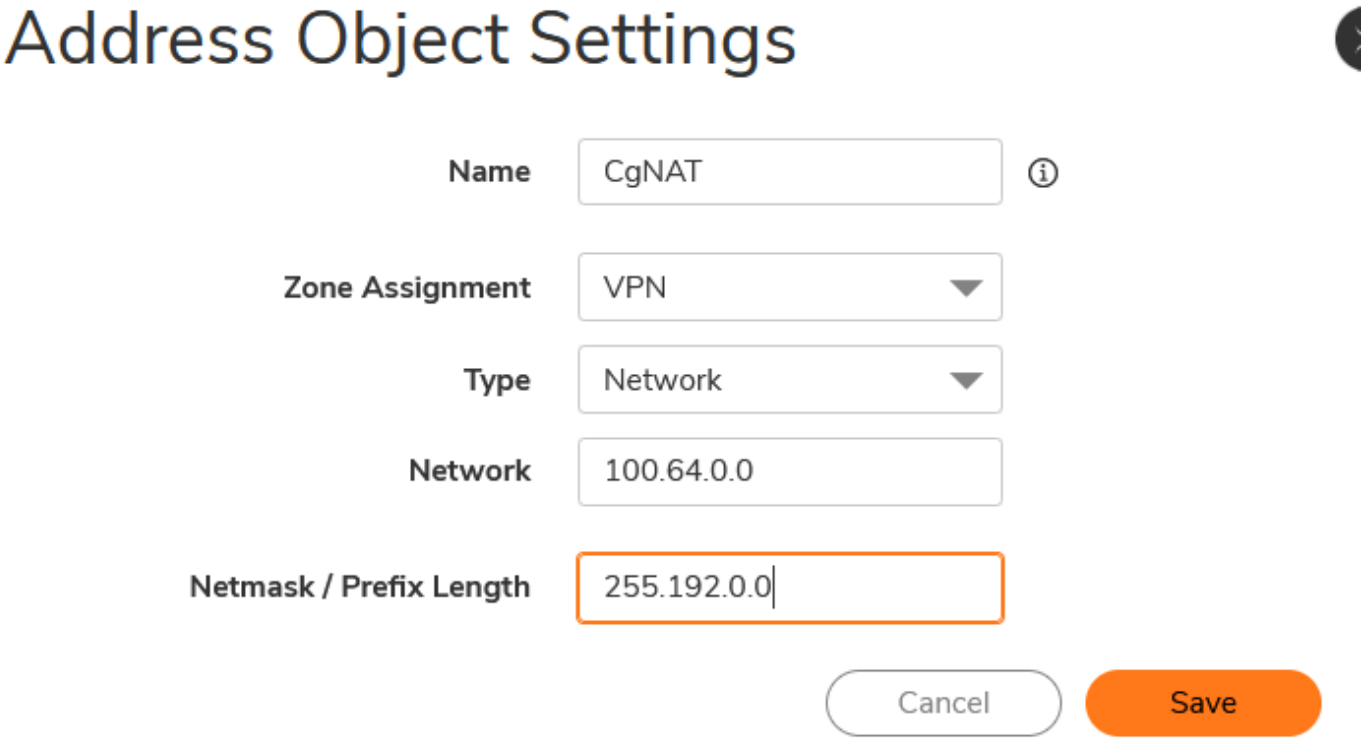
- Object > Match Objects >Addresses
- アドレスオブジェクト
- +追加をクリックします



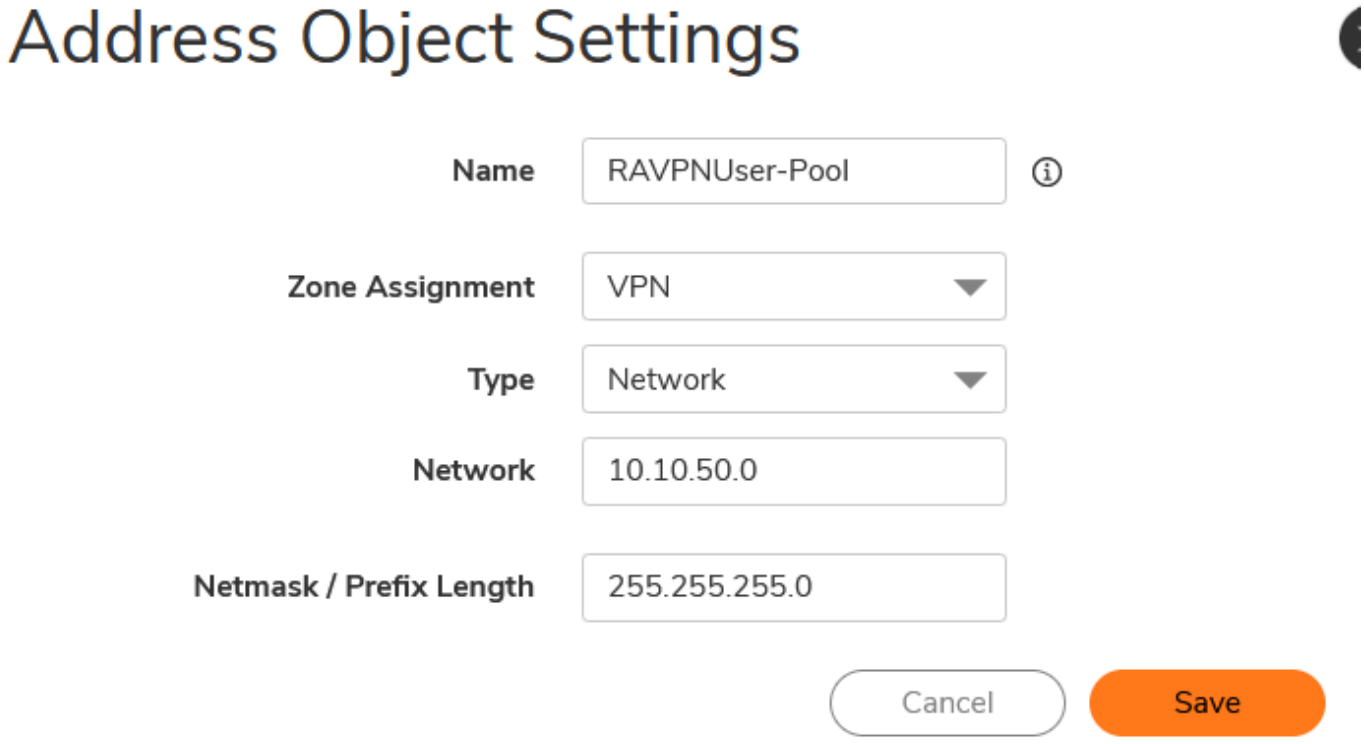
Sonicwall – オブジェクト – アドレスオブジェクト



- [Save] をクリックします。

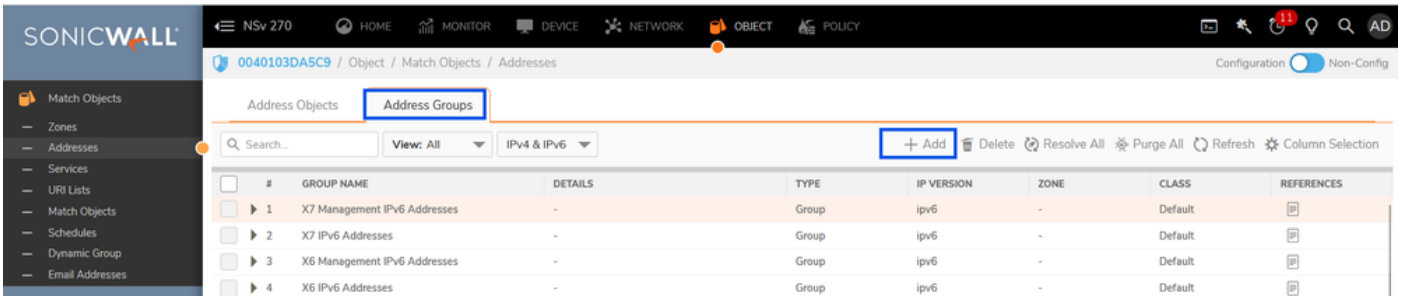


- [Save] をクリックします。

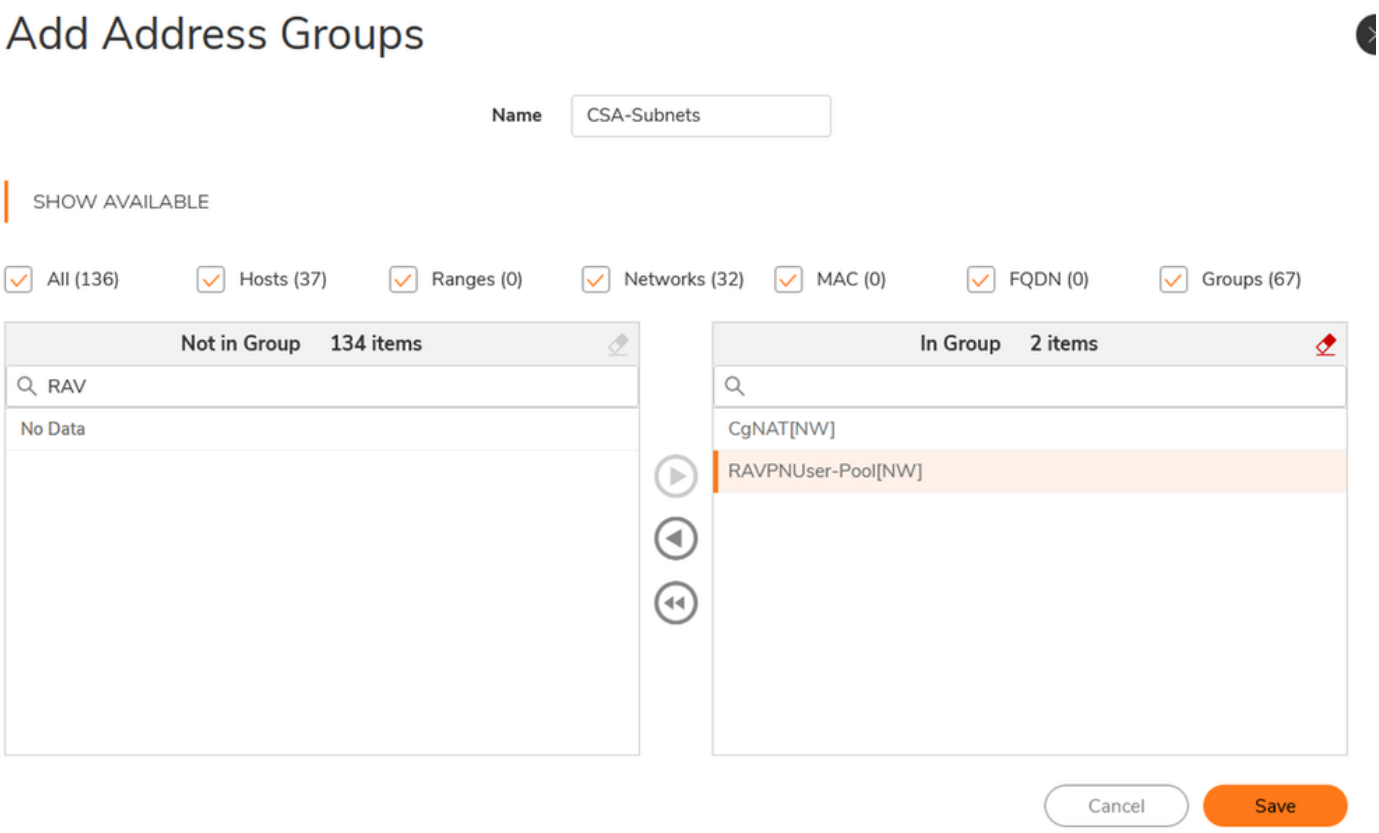


- [Save] をクリックします。

- アドレスグループの作成
- +Addをクリックします。
- アドレスオブジェクトを選択し、アドレスグループに追加します



Sonicwall – オブジェクト – アドレスグループ

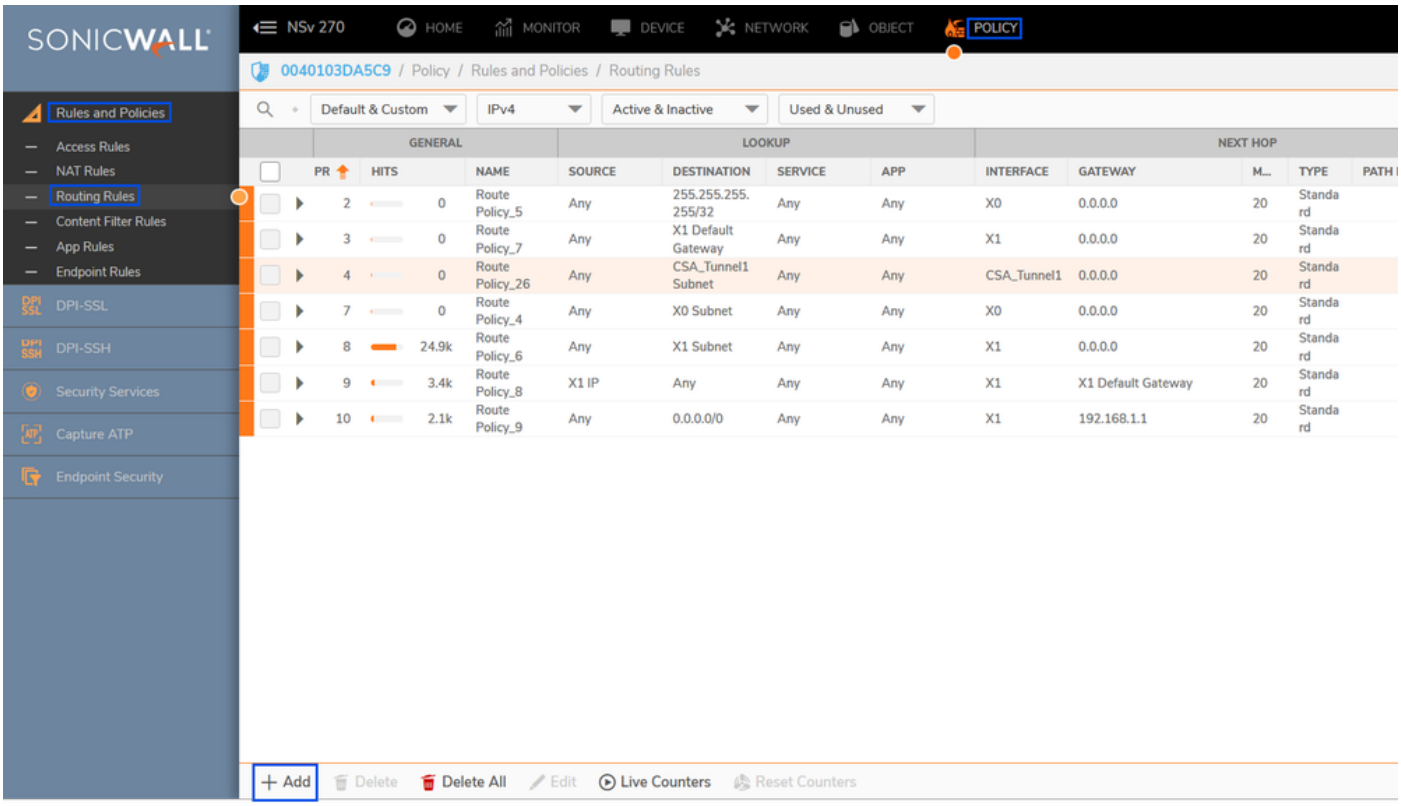


- [Save] をクリックします。

ルートの追加

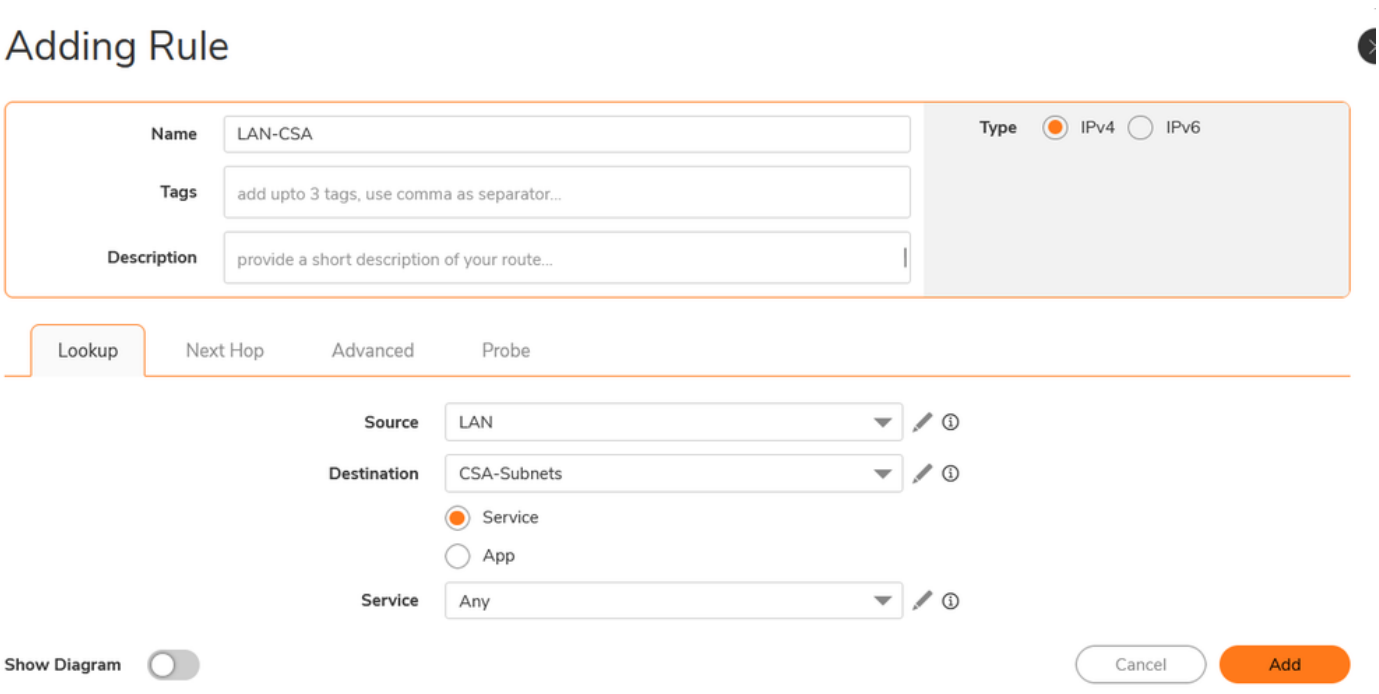
Sonicwall Dashboardに移動します。

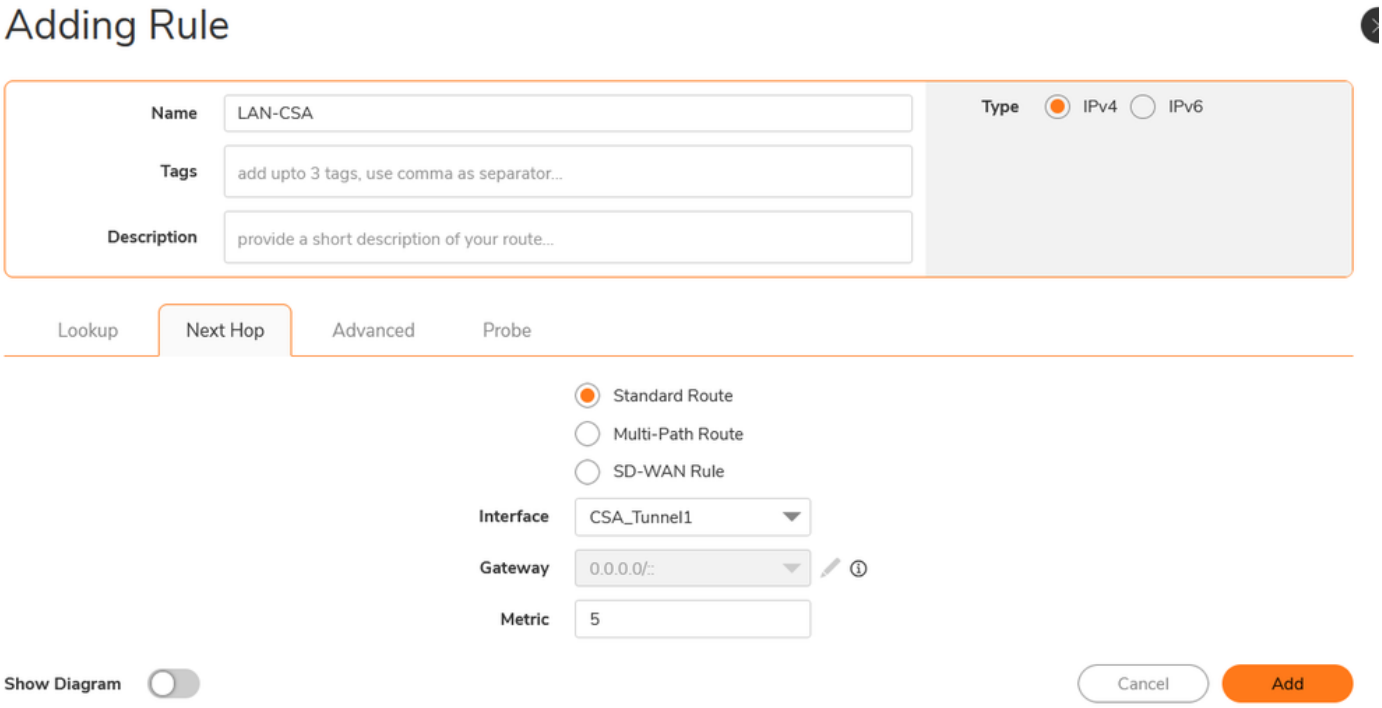
- Policy > Rules and Policies > Routing Rules
- +追加をクリックします。



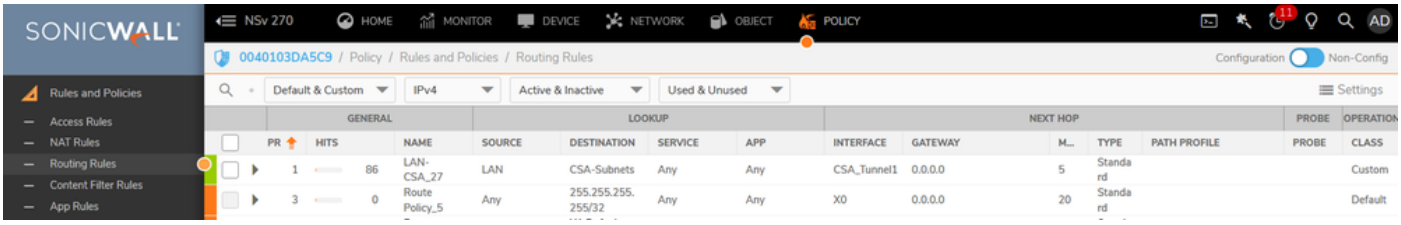
Sonicwall：ルーティングルール

- ルーティングルールの追加





- +追加をクリックします。

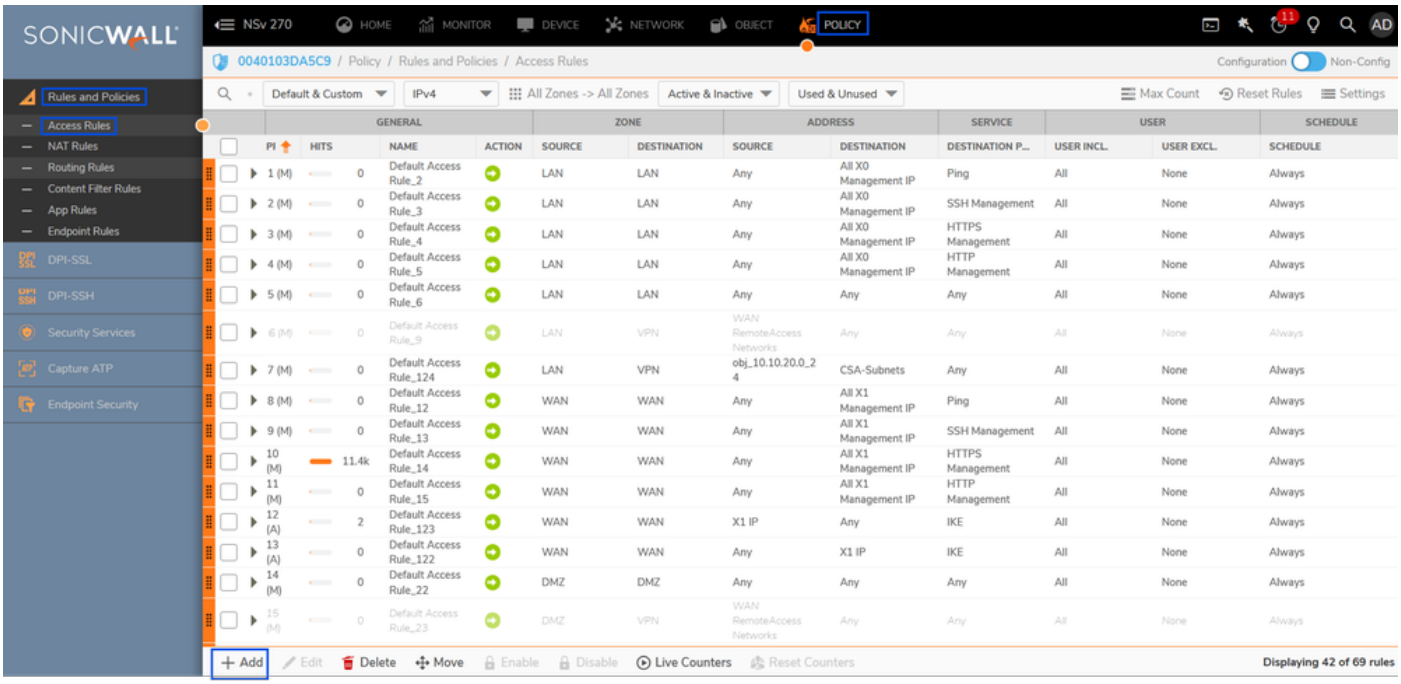


Sonicwall：ルーティングルール

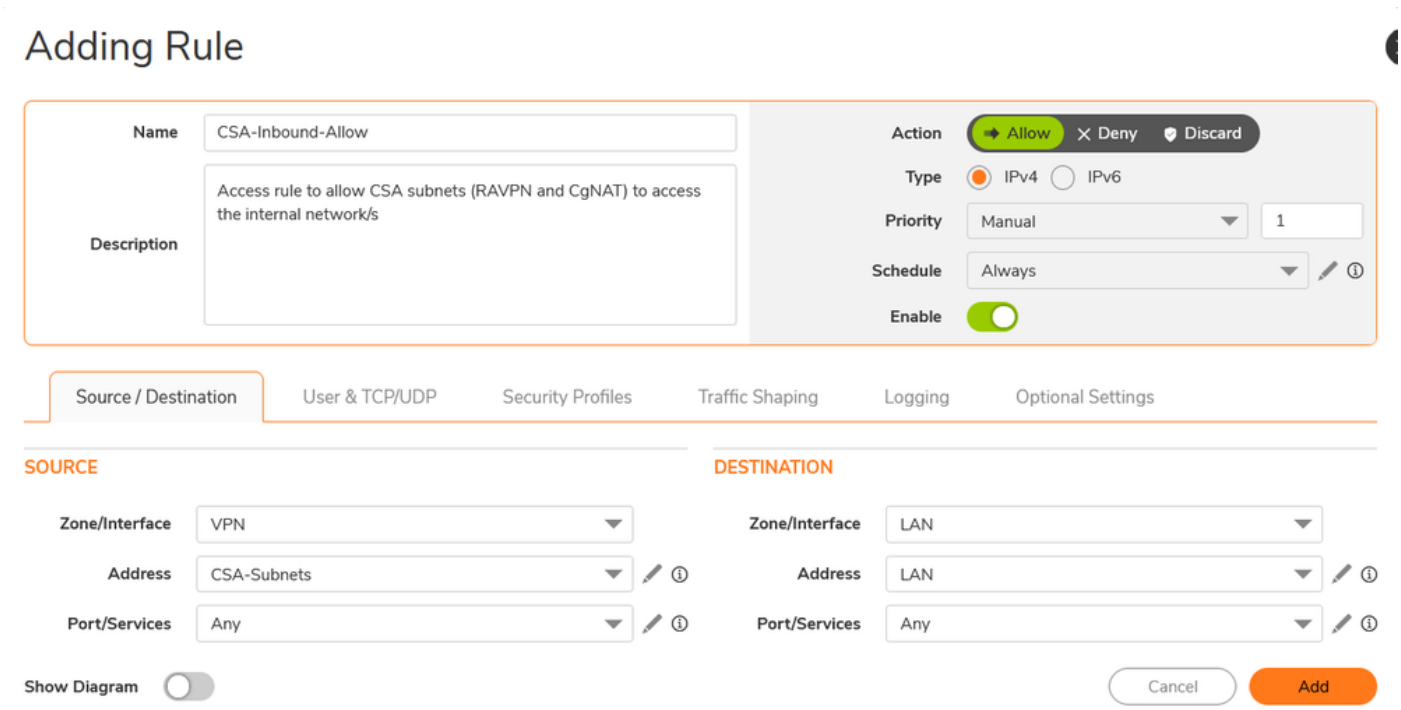
アクセスルールの追加

Sonicwall Dashboardに移動します。

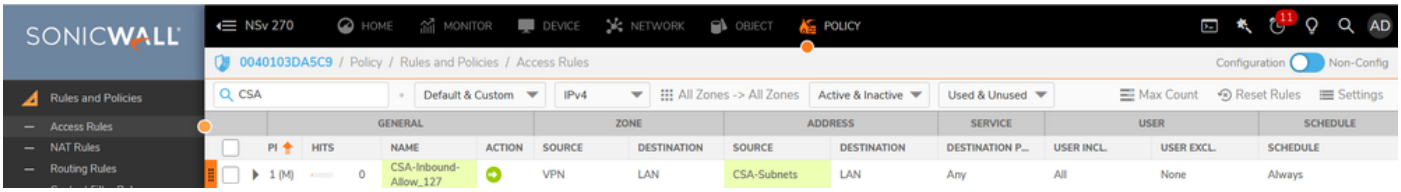
- Policy > Rules and Policies > Access Rules
- +追加をクリックします。



Sonicwall：アクセスルール



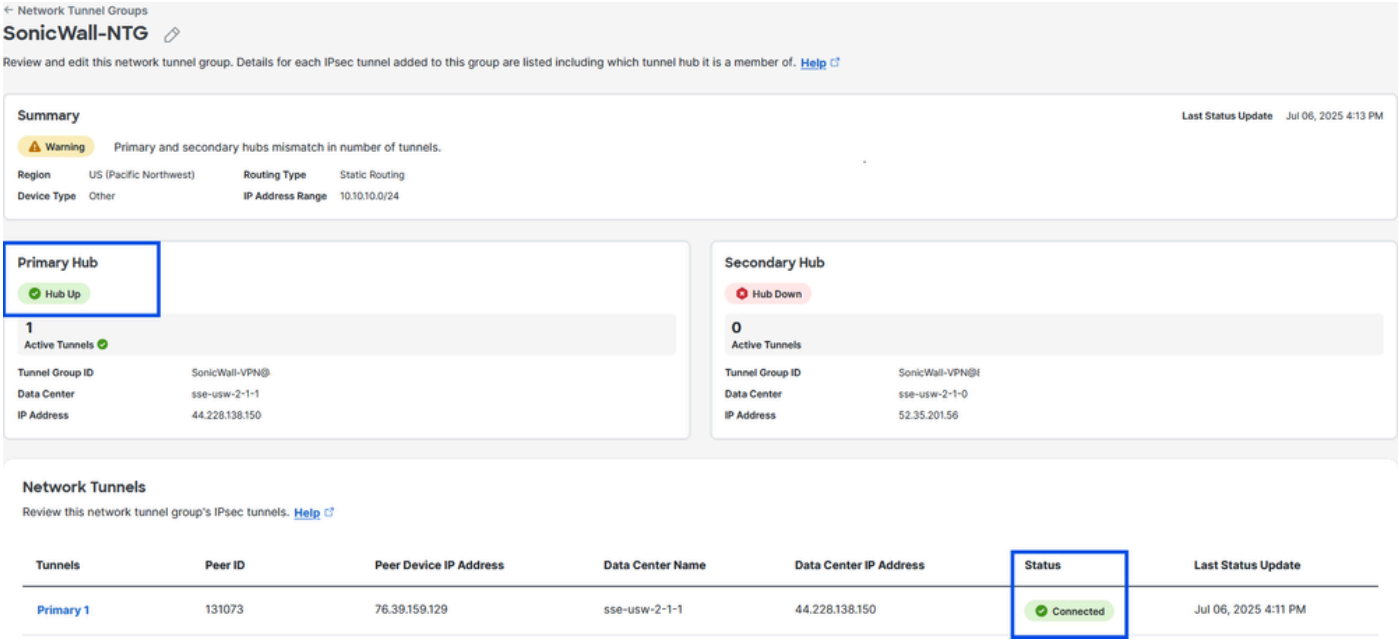
- +Addをクリックします。



Sonicwall：アクセスルール

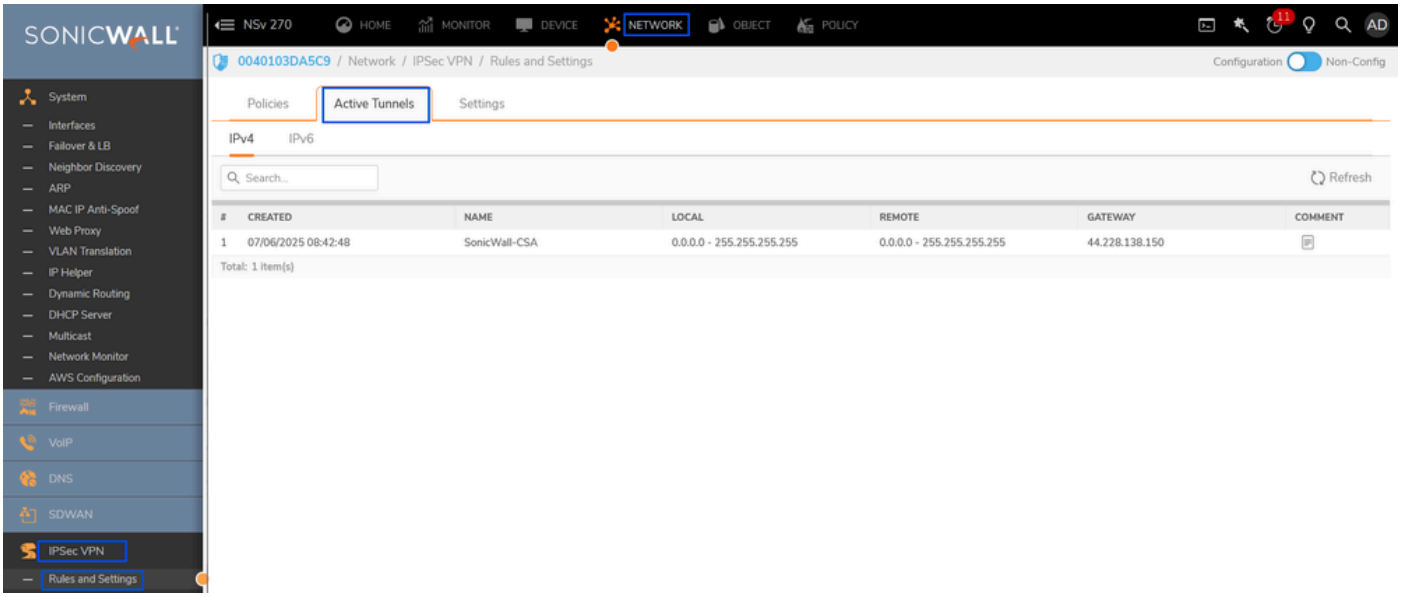
確認

- セキュアアクセスのトンネルステータス



セキュアアクセス – ネットワークトンネルグループ – VPNステータス

- Sonicwallファイアウォールのトンネルステータス



Sonicwall:IPSec VPNステータス

同じプロセスで、Secure Access Secondaryデータセンターと Sonicwall間のトンネルを設定できます

これで、トンネルがセキュアアクセスとSonicwallでアップ状態になったので、RA-VPN、ブラウザベースのZTA、またはクライアントベースのZTAを介したプライベートリソースへのアクセスのセキュアアクセスダッシュボードでの設定を続行できます

トラブルシュート

ユーザPC

- ユーザがRAVPN/ZTNAに正常に接続/登録できるかどうかを確認します。そうでない場合は、コントロールプレーン接続が失敗する原因を詳しくトラブルシューティングします。
- ユーザがアクセスしようとしているネットワークが、RAVPNトンネルまたはZTNA（VPNトンネルインターフェイス）経由で行くことを想定していることを確認します。そうでない場合は、ヘッドエンド(CMTS)の設定を確認します。

セキュアなアクセス

- RAVPN接続プロファイルでトラフィックステアリング設定を確認し、宛先ネットワークがトンネル経由でセキュアアクセスに送信するように設定されていることを確認します。
- プライベートリソースが有効なプロトコル/ポートで定義され、ZTNA/RAVPN接続メカニズムがチェックされていることを確認します。
- RAVPN/ZTNAユーザがPrivate Resource Network（PRN；プライベートリソースネットワーク）にアクセスできるようにアクセスポリシーが設定されていて、他のルールが優先されてトラフィックをブロックしていないという順番になっていることを確認します。
- ユーザがアクセスしようとしているプライベートリソースをカバーするスタティックルーティングを介した有効なクライアントルートを示すIPSecトンネルがアップ状態で、セキュアアクセスであることを確認します。

防音壁

- IPSecトンネルがアップしているかどうかを確認します（IKEおよびIPSec SA）。
- クライアントルートが適切にアドバタイズされることを確認します。
- RAVPN/ZTNAユーザからSonicwallの背後にあるプライベートリソース宛てのトラフィックの送信元が、Sonicwallでパケットキャプチャを実行することにより、トンネル経由でSonicwallファイアウォールに到達していることを確認します。
- トラフィックがプライベートリソースに到達し、RAVPN/ZTNAクライアントに応答するかどうかを確認します。使用できる場合は、それらのパケットがSonicall X0(LAN)インターフェイスに到達していることを確認します。
- SonicwallがIPSecトンネル経由でSecure Accessにリターントラフィックを転送していることを確認します。

関連情報

- シスコのテクニカルサポートとダウンロード
- Cisco Secure Accessヘルプセンター
- ゼロトラストアクセスモジュール
- Secure Accessエラー「Enrollment Service Is Not Responding.ITヘルプデスクにお問い合わせください」

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。