Configurazione di Secure Access con Sonicwall Firewall

Sommario

Introduzione

In questo documento viene descritto come configurare un tunnel VTI IPsec tra un firewall Secure Access to Sonicwall e l'altro utilizzando il routing statico.

Prerequisiti

- Configura assegnazione ruoli utente
- Configurazione autenticazione SSO ZTNA
- Configura accesso sicuro VPN di accesso remoto

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Firewall di Sonicwall (NSv270 - SonicOSX 7.0.1)

- Accesso sicuro
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA
- ZTNA senza client

Componenti usati

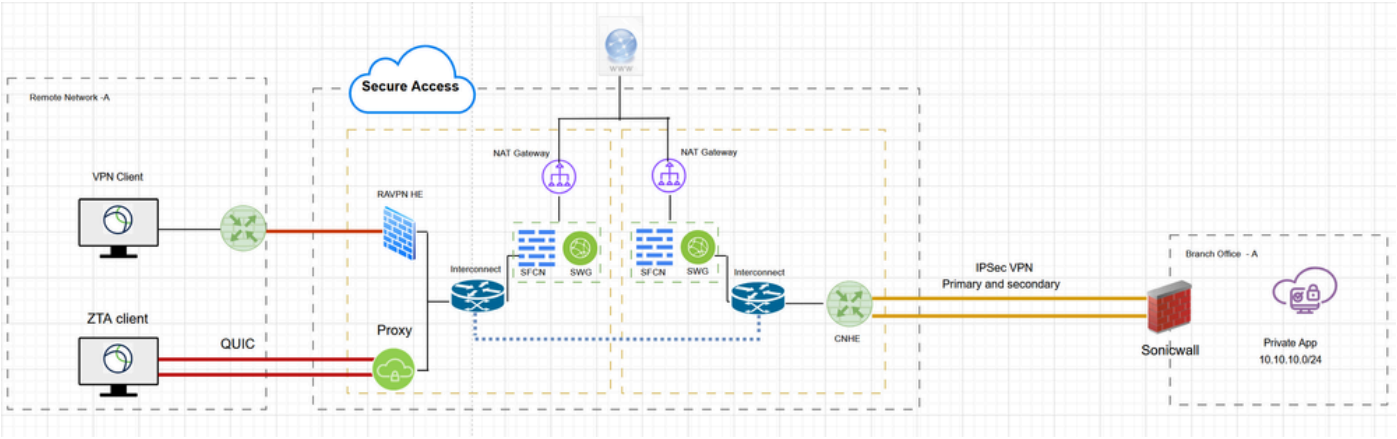
Le informazioni fornite in questo documento si basano su:

- Firewall di Sonicwall (NSv270 - SonicOSX 7.0.1)
- Accesso sicuro
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Esempio di rete



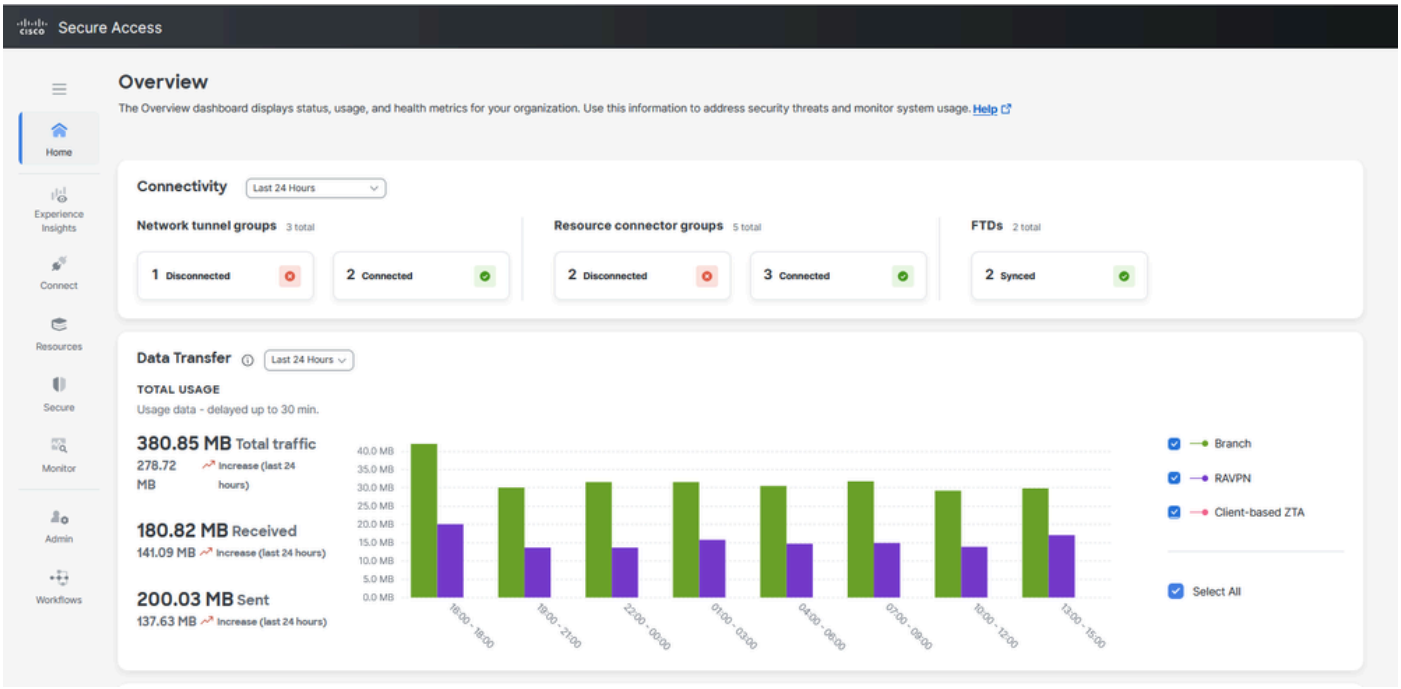
Esempio di rete

Configurazione

Configura Network Tunnel Group (VPN) su Secure Access

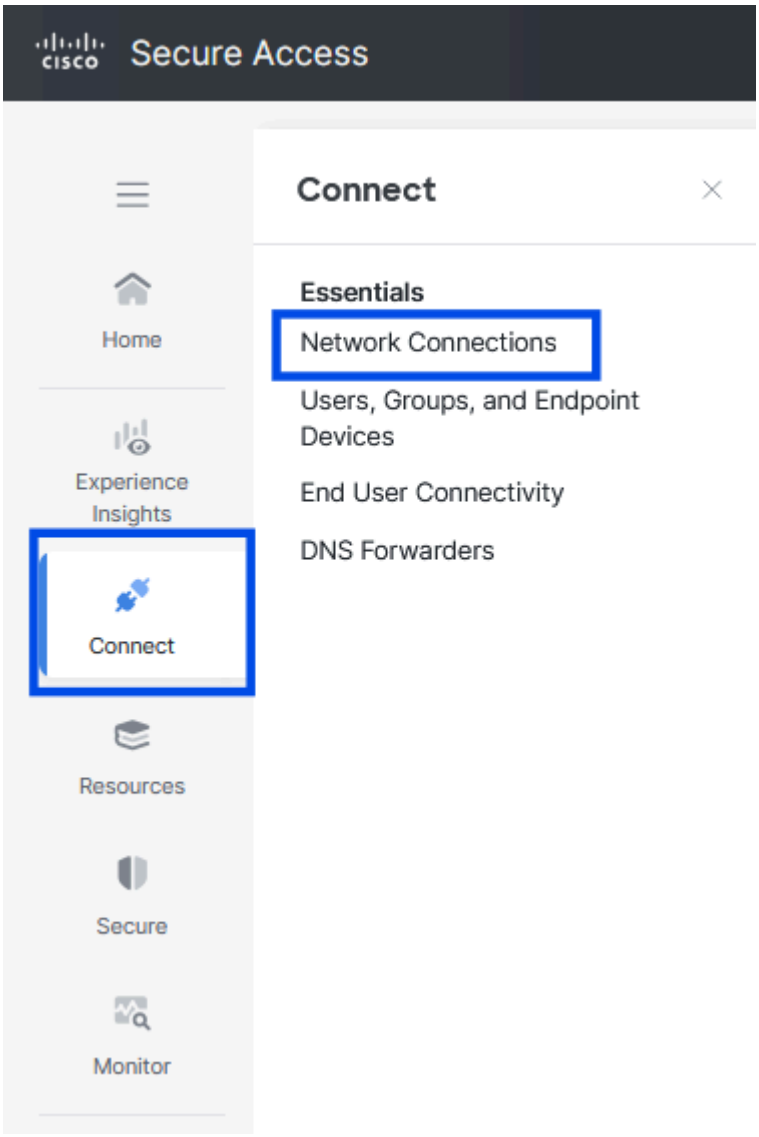
Per configurare il tunnel VPN tra Secure Access e Sonicwall

- Passare al portale di amministrazione di Secure Access



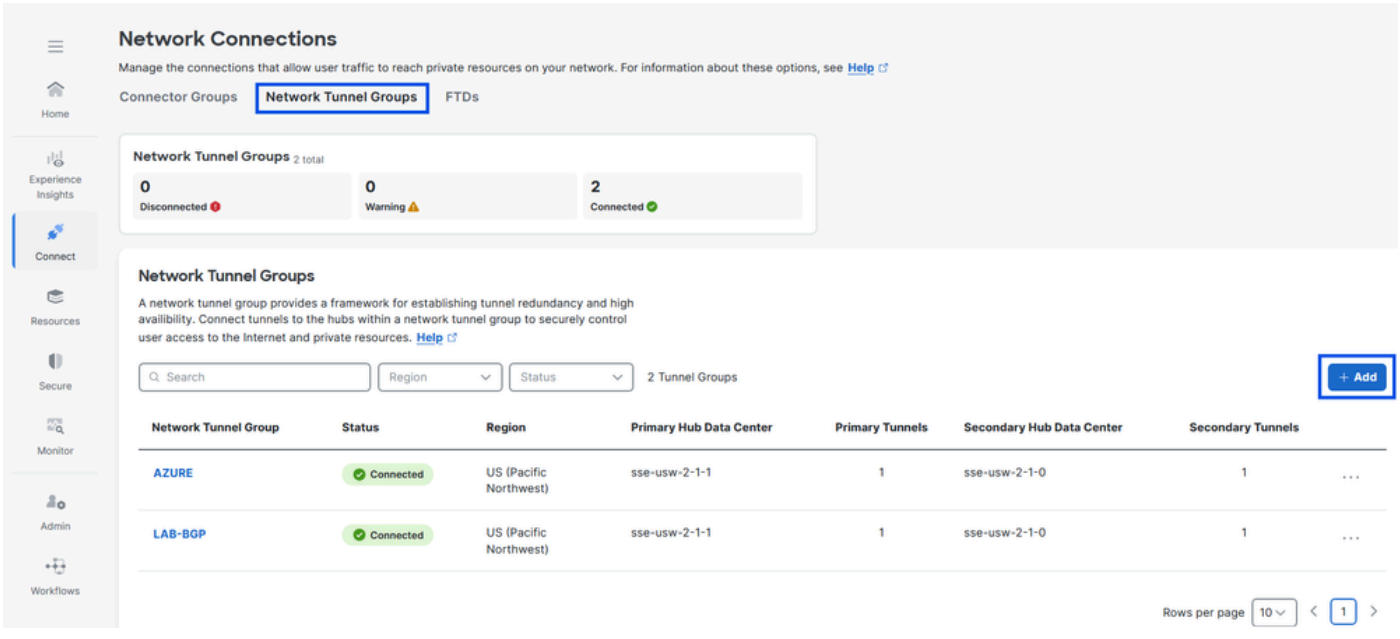
Secure Access - Pagina principale

- Fare clic su Connect > Network Connections



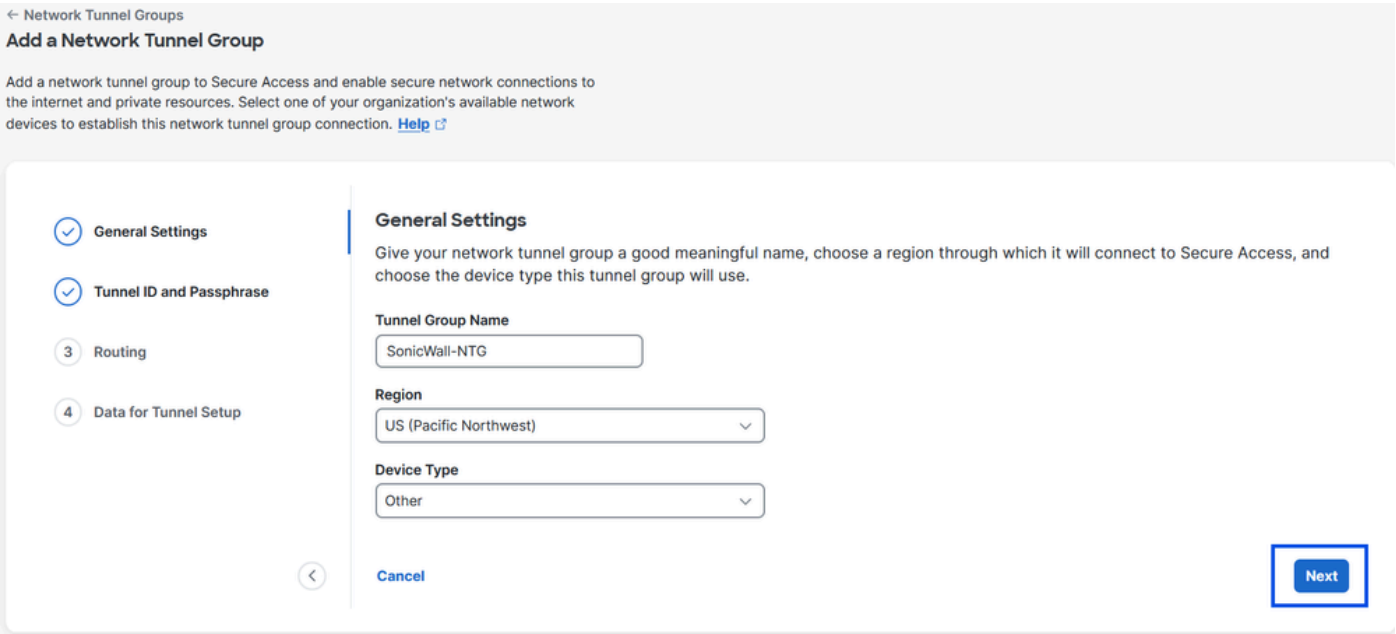
Accesso sicuro - Connessioni di rete

- In Gruppi di tunnel di rete fare clic su + Aggiungi



Accesso sicuro - Gruppi di tunnel di rete

- Configurare il nome del gruppo di tunnel, l'area e il tipo di dispositivo
- Fare clic su Avanti.

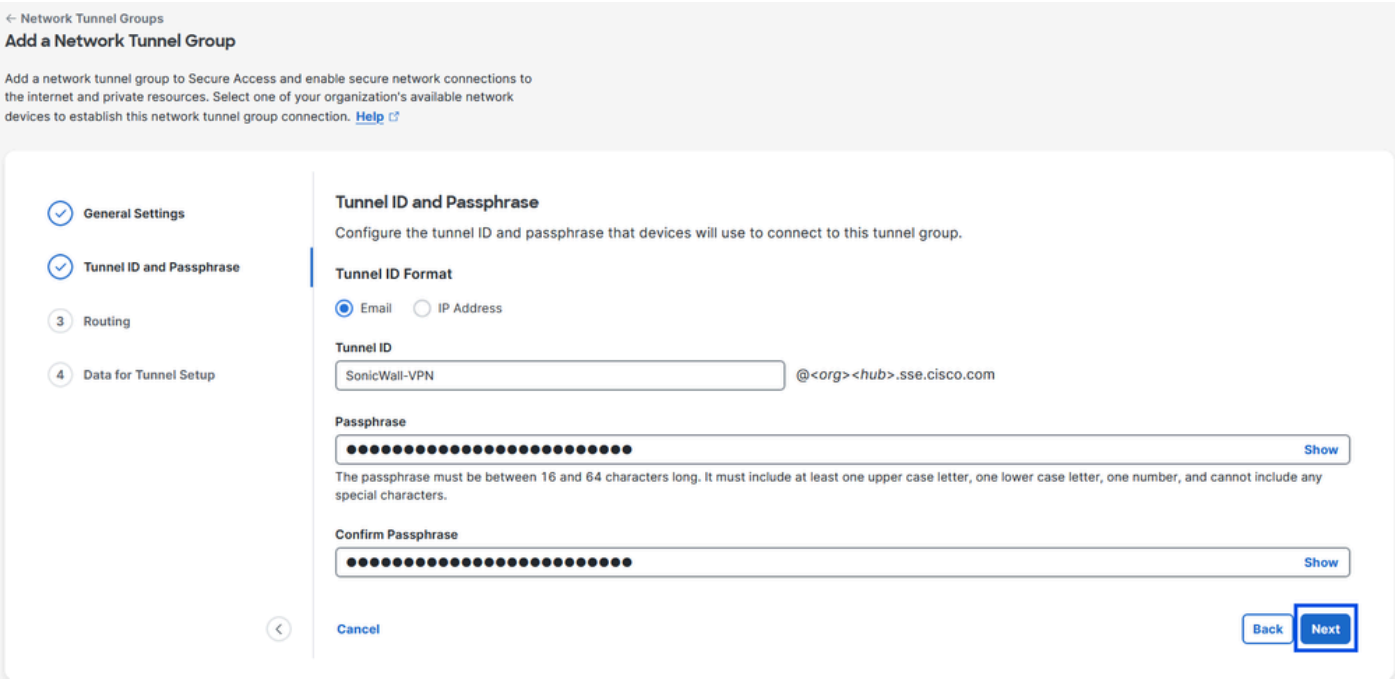


Accesso sicuro - Gruppo tunnel di rete - Impostazioni generali

---

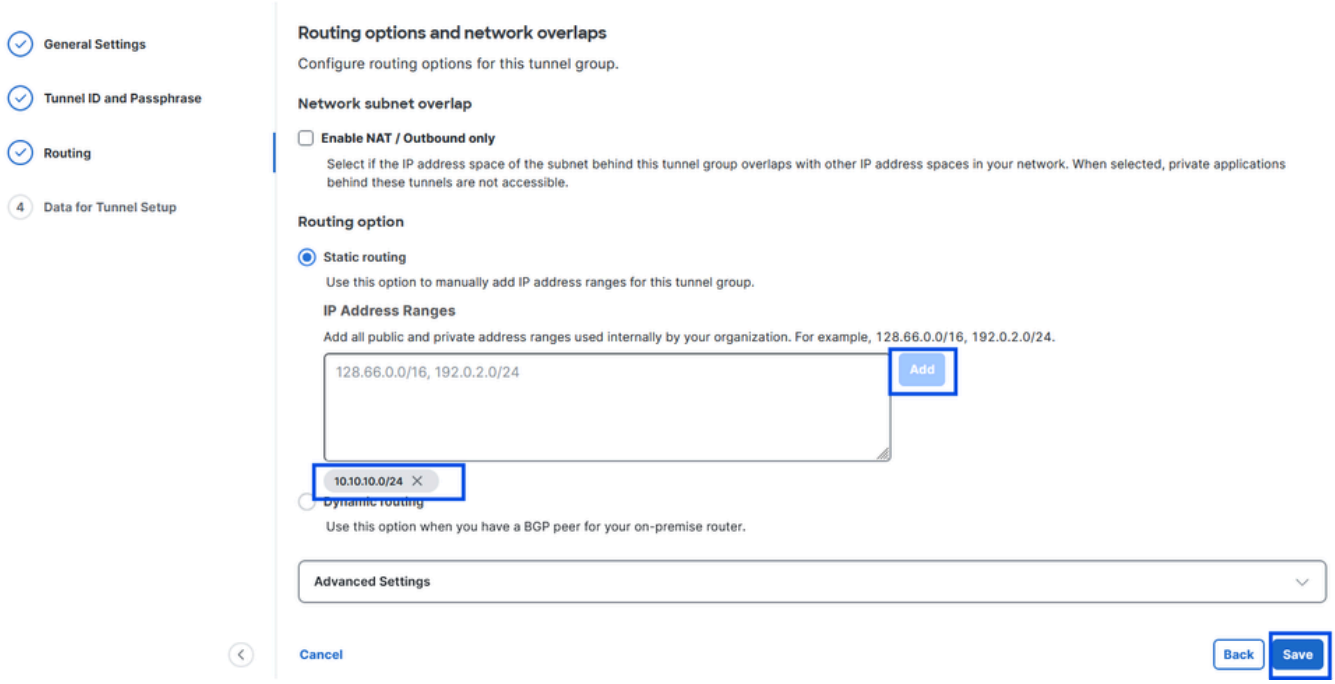
Nota: Scegliere l'area più vicina alla posizione del firewall.

- Configurazione del formato dell'ID del tunnel e della passphrase
- Fare clic su Avanti.



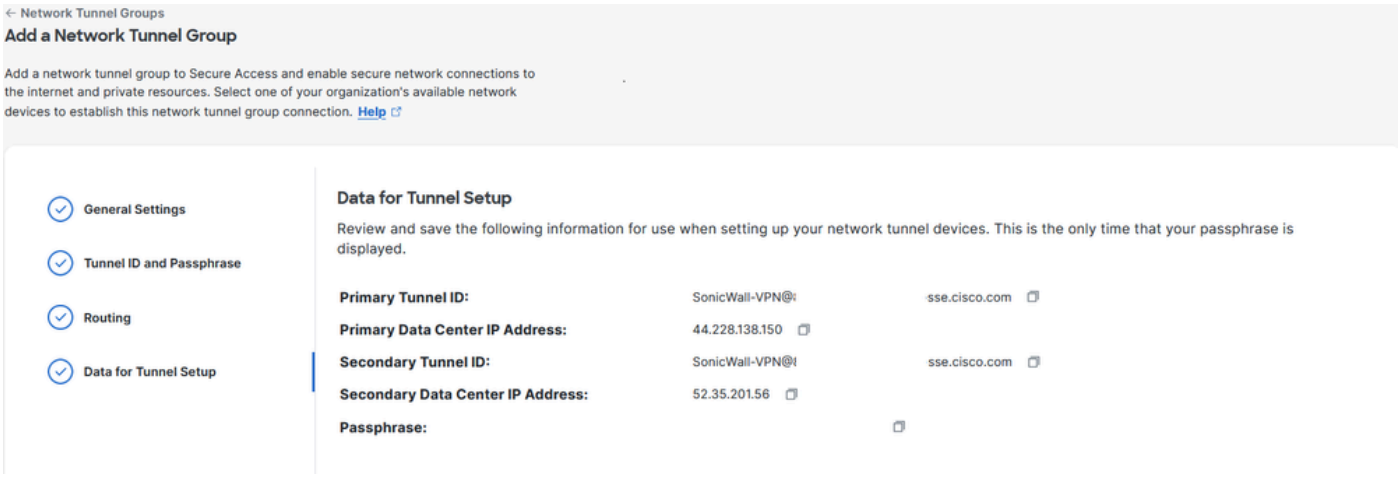
Accesso sicuro - ID tunnel e passphrase

- Configurare gli intervalli di indirizzi IP, gli host o le subnet configurati nella rete e che si desidera passare il traffico attraverso l'accesso protetto
- Fare clic su Aggiungi
- Fare clic su Salva.



Accesso sicuro - Gruppi di tunnel - Opzioni di routing

Dopo aver fatto clic su Save (Salva), vengono visualizzate le informazioni sul tunnel. Salvare le informazioni per il passaggio di configurazione successivo



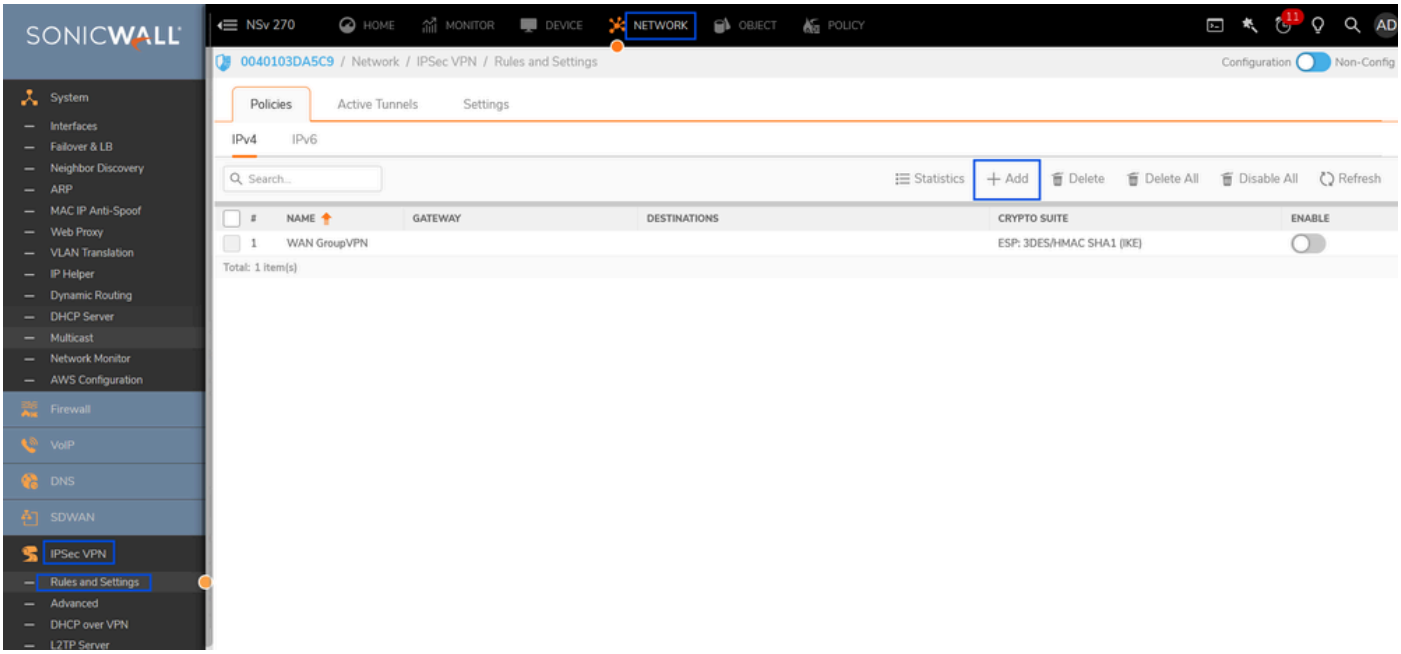
Accesso sicuro - Configurazione dati per tunnel

Configurazione del tunnel su Sonicwall

Configurazione del tunnel - Regole e impostazioni

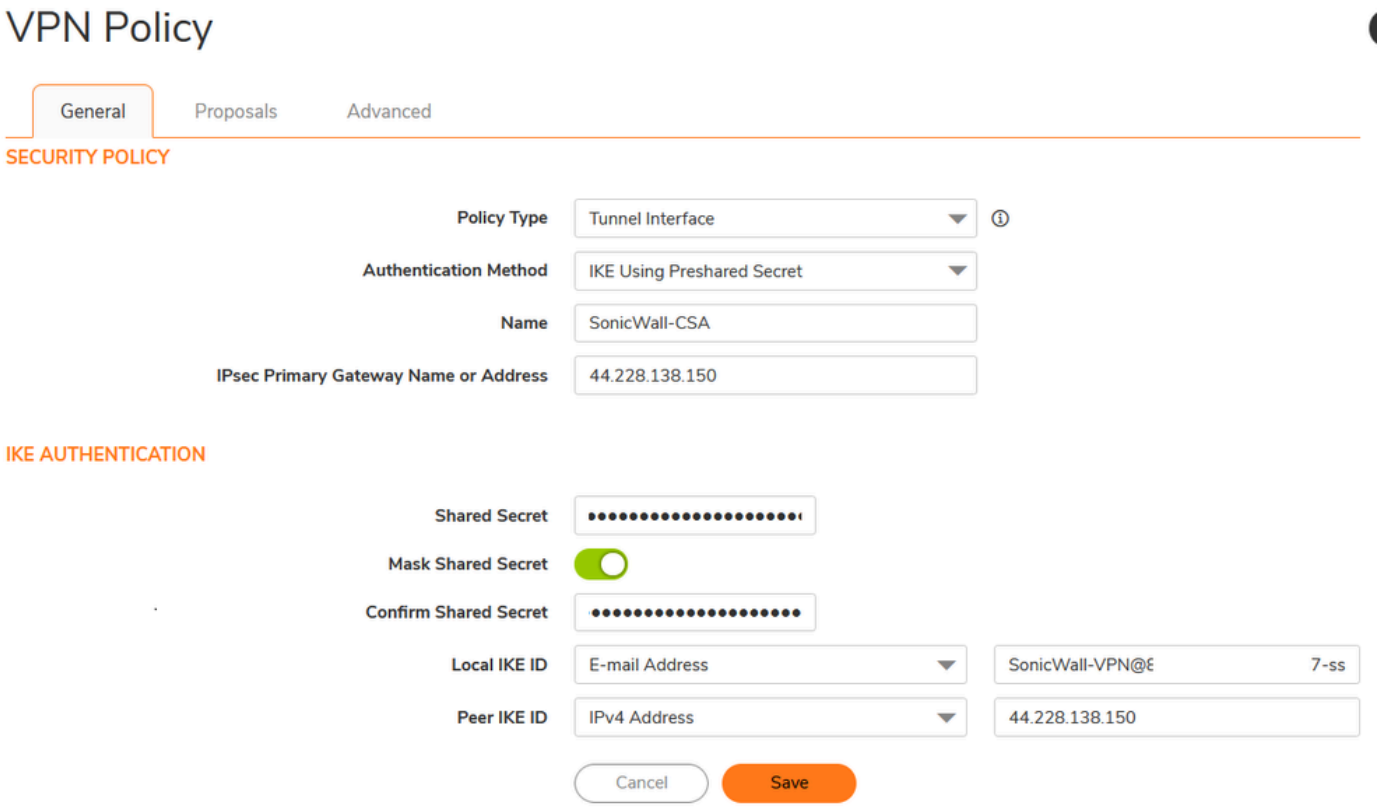
Passare al dashboard di Sonicwall.

- Rete > VPN IPSec > Regole e impostazioni
- Fare clic su + Aggiungi



Sonicwall - IPSec VPN - Regole e impostazioni

- In Criteri VPN, compilare la configurazione della VPN in base ai dati del tunnel di Accesso sicuro e ai [parametri IPSec supportati]



VPN Policy

General | Proposals | Advanced

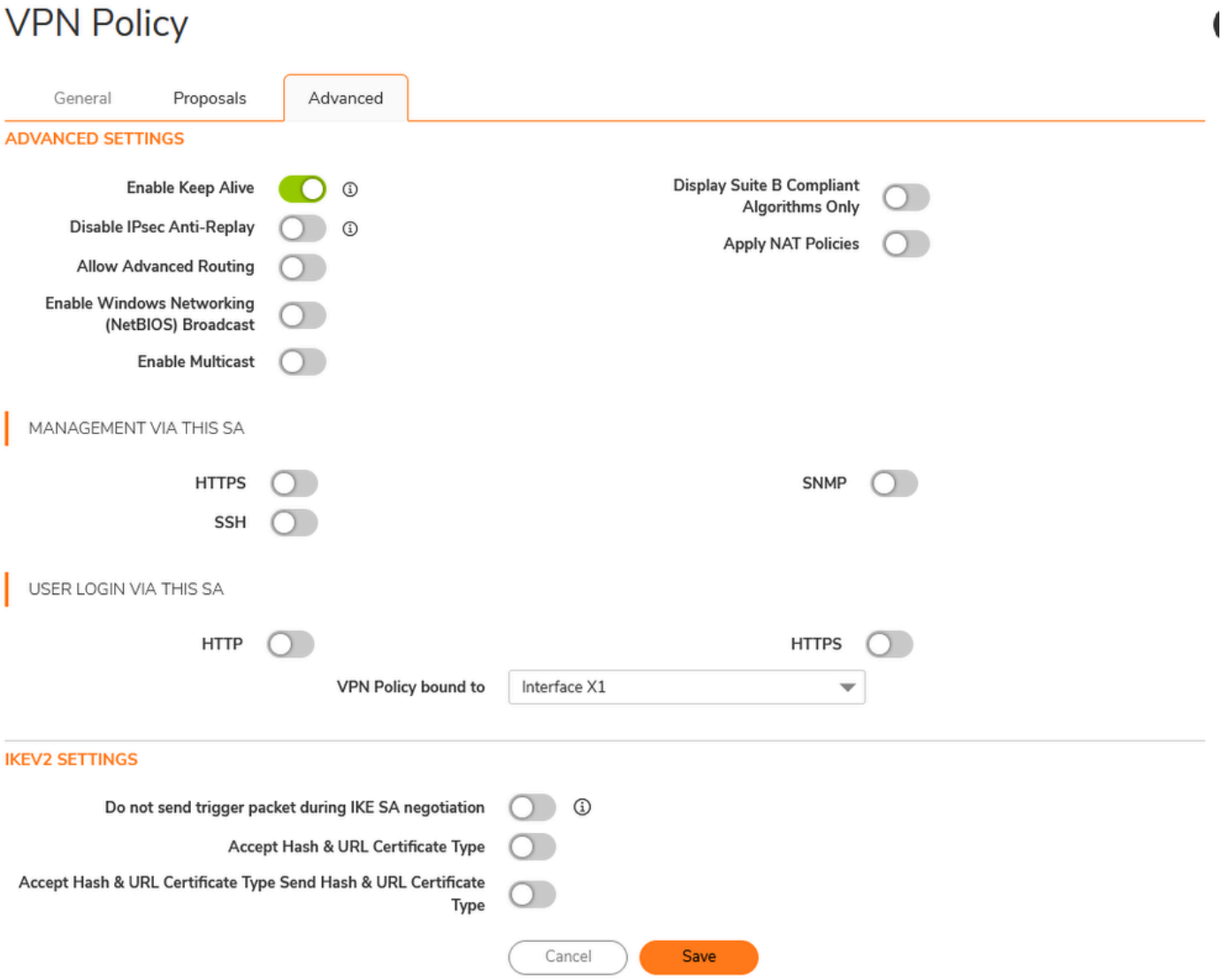
IKE (PHASE 1) PROPOSAL

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

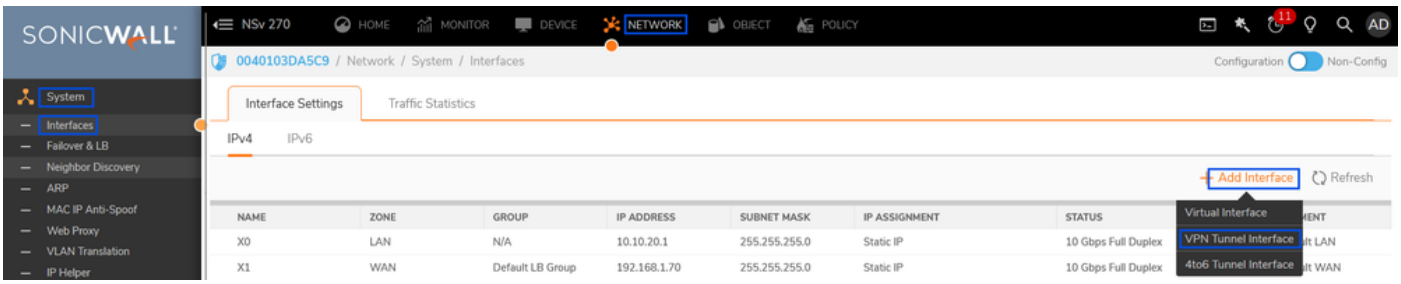


- Fare clic su Salva

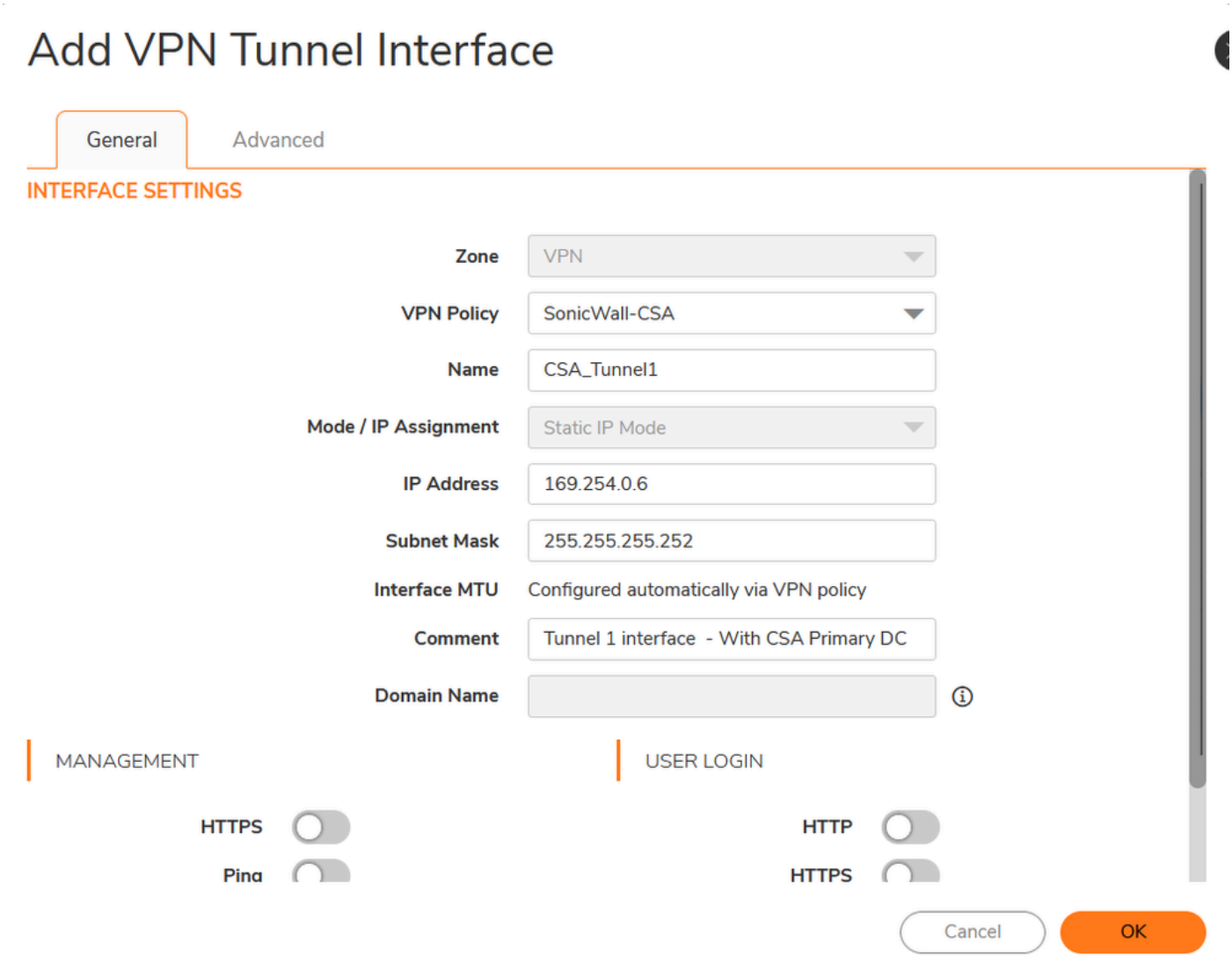
Aggiungi interfaccia tunnel VPN

Passare al dashboard di Sonicwall.

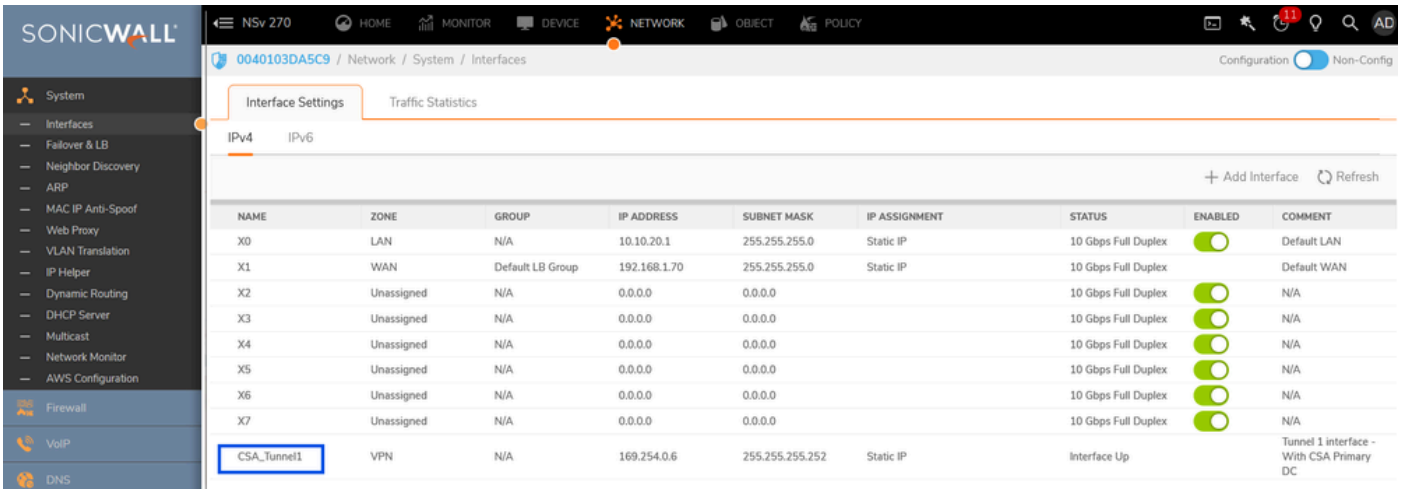
- Rete > Sistema > Interfaccia
- Fare clic su + Aggiungi interfaccia
- Seleziona interfaccia tunnel VPN



Sonicwall - Interfacce



- Fare clic su OK.

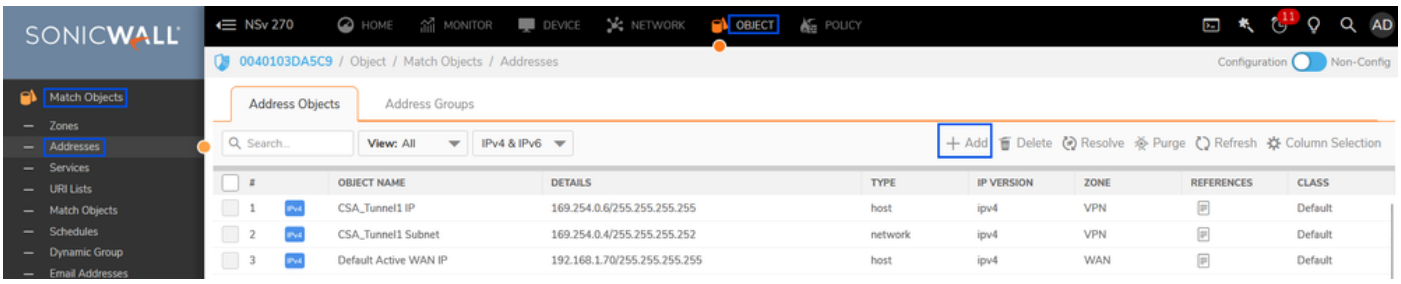


Sonicwall - Interfacce - VPN Tunnel Interface

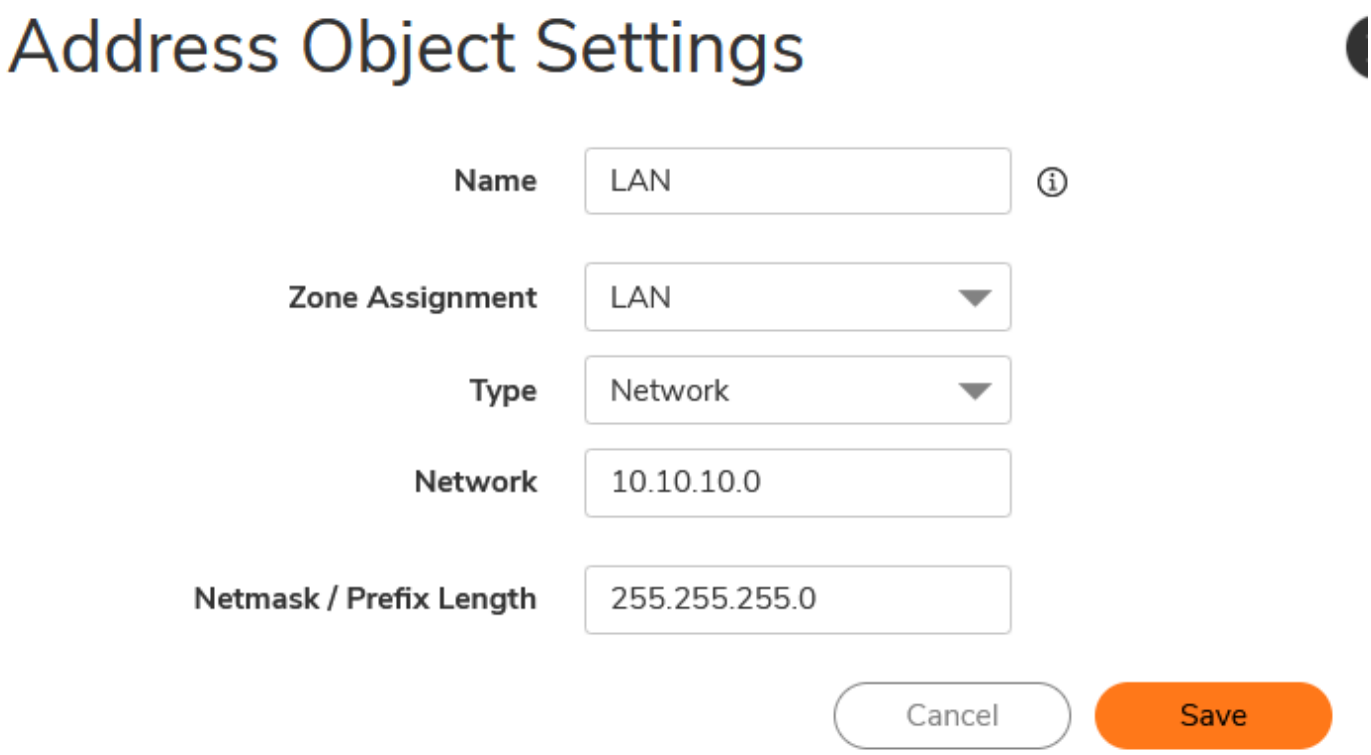
Aggiungi oggetto e gruppi di rete

Passare al dashboard di Sonicwall.

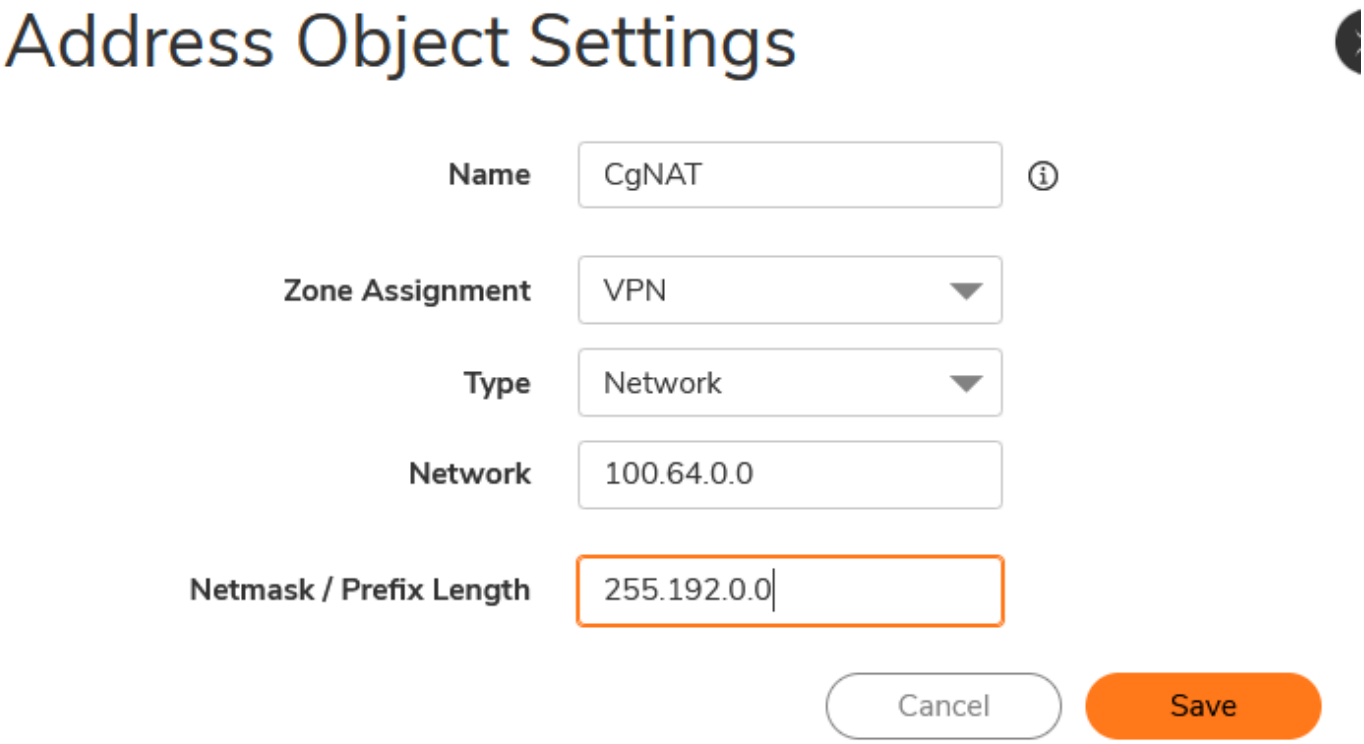
- Oggetto > Corrispondenza oggetti >Indirizzi
- Oggetti Address
- Fare clic su +Aggiungi



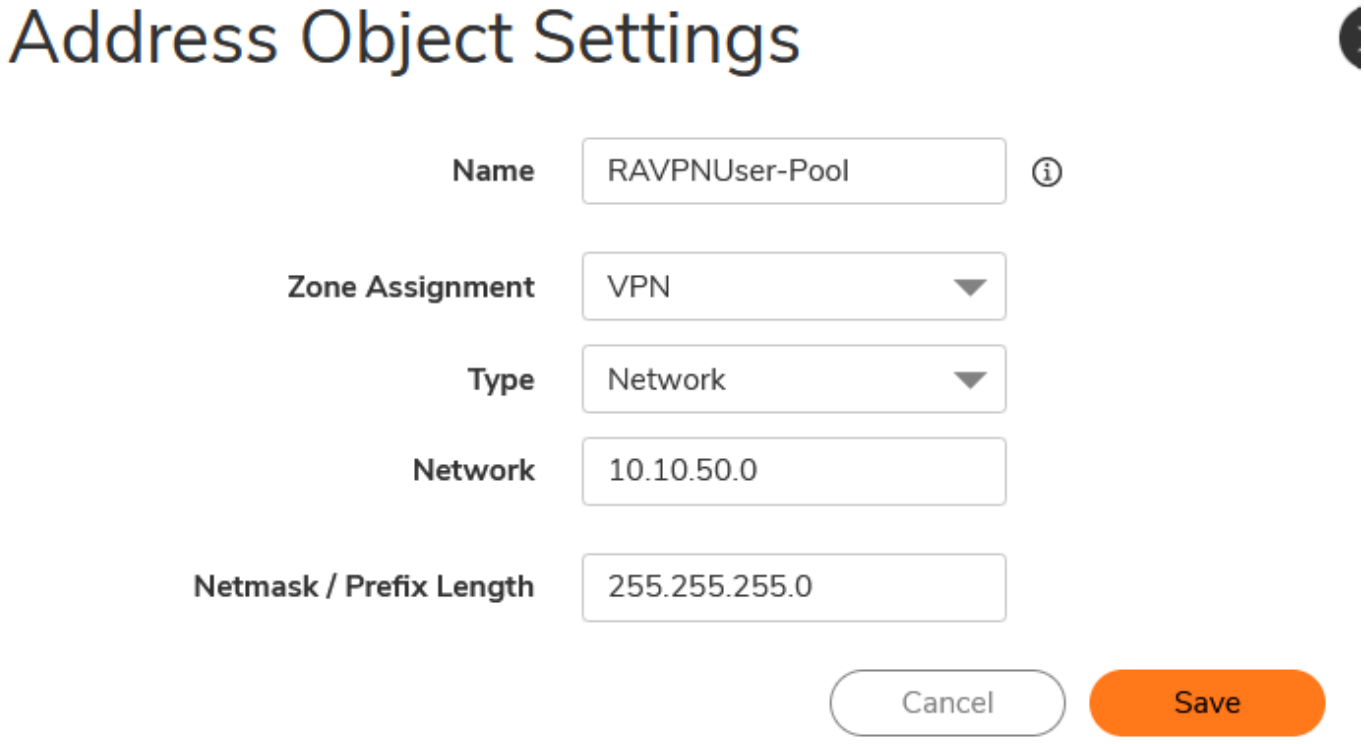
Sonicwall - Oggetto - Oggetti Address



- Fare clic su Salva.

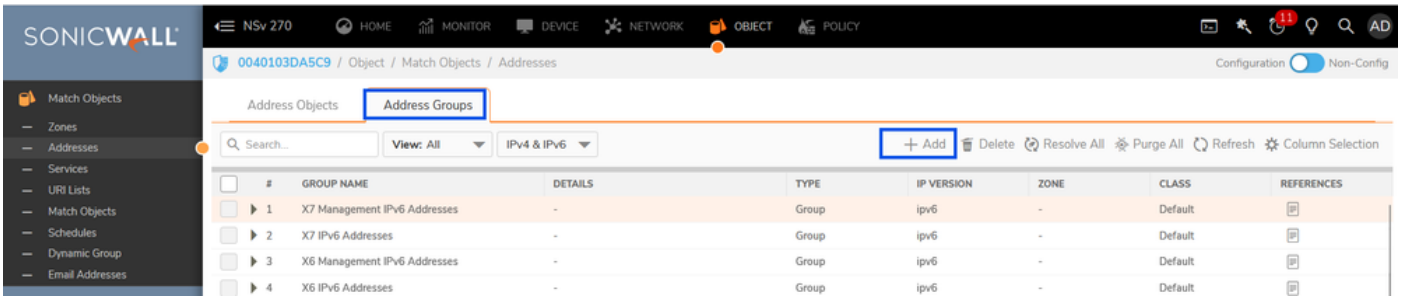


- Fare clic su Salva.

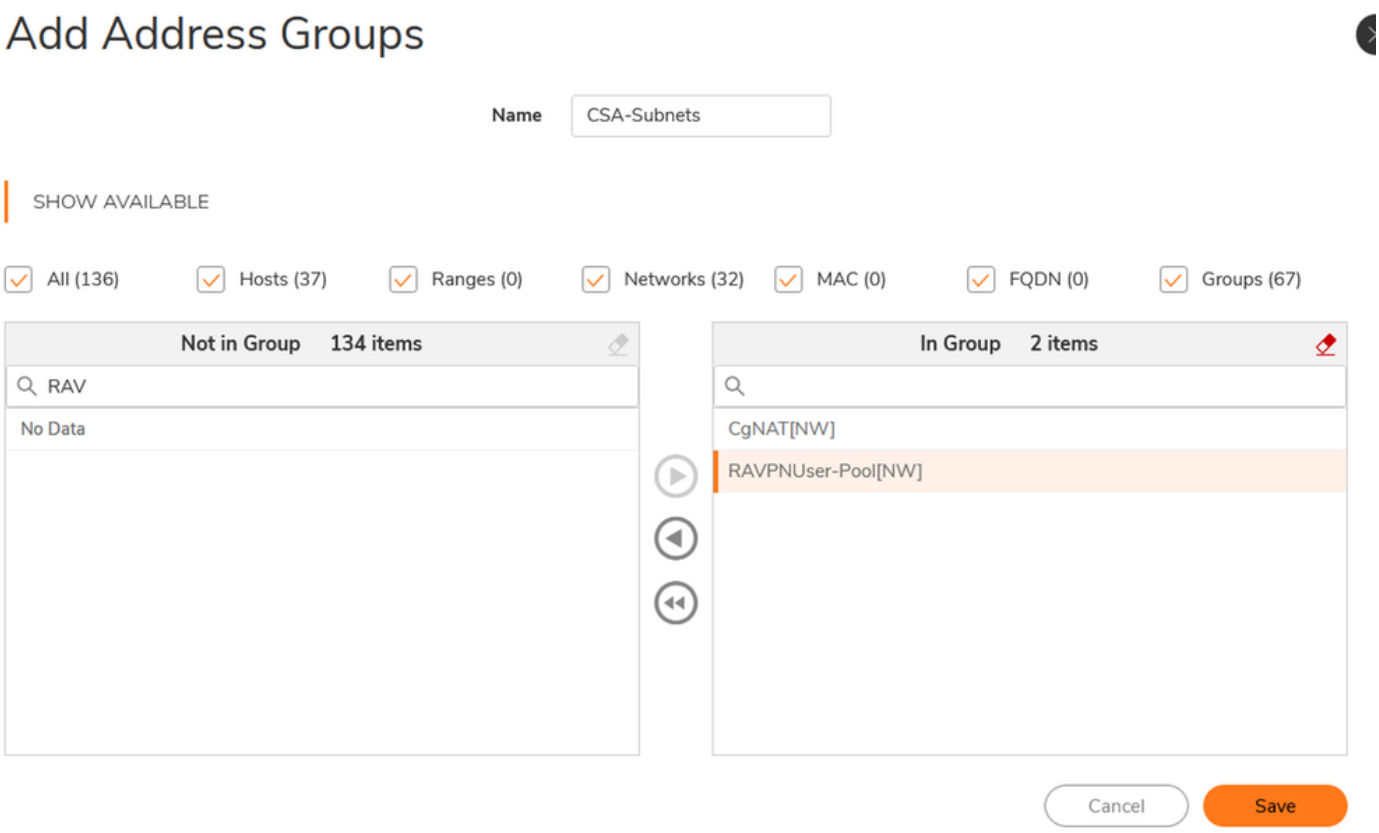


- Fare clic su Salva.

- Crea gruppi di indirizzi
- Fare clic su +Aggiungi
- Selezionare l'oggetto indirizzo e aggiungerlo ai gruppi di indirizzi



Sonicwall - Oggetto - Gruppi di indirizzi

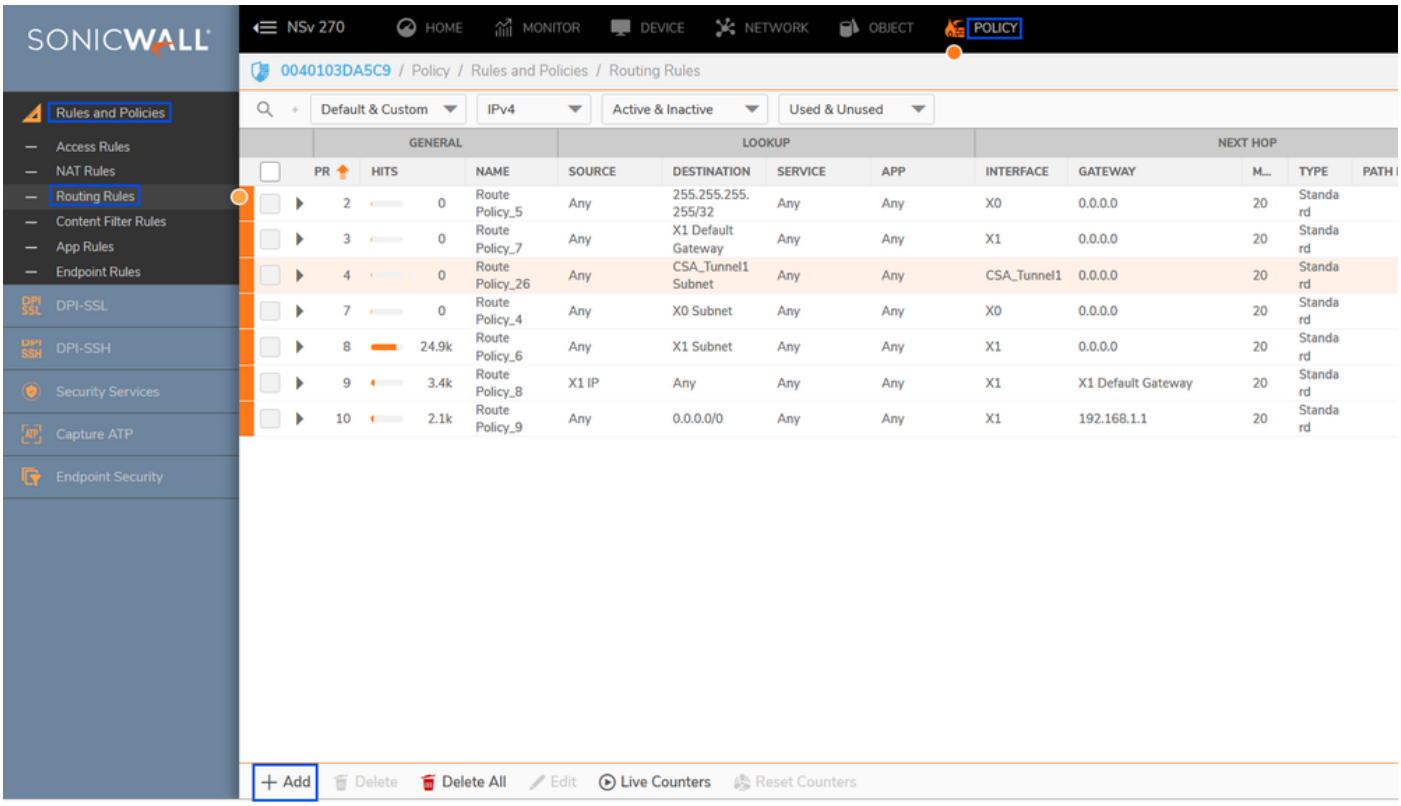


- Fare clic su Salva.

Aggiungi route

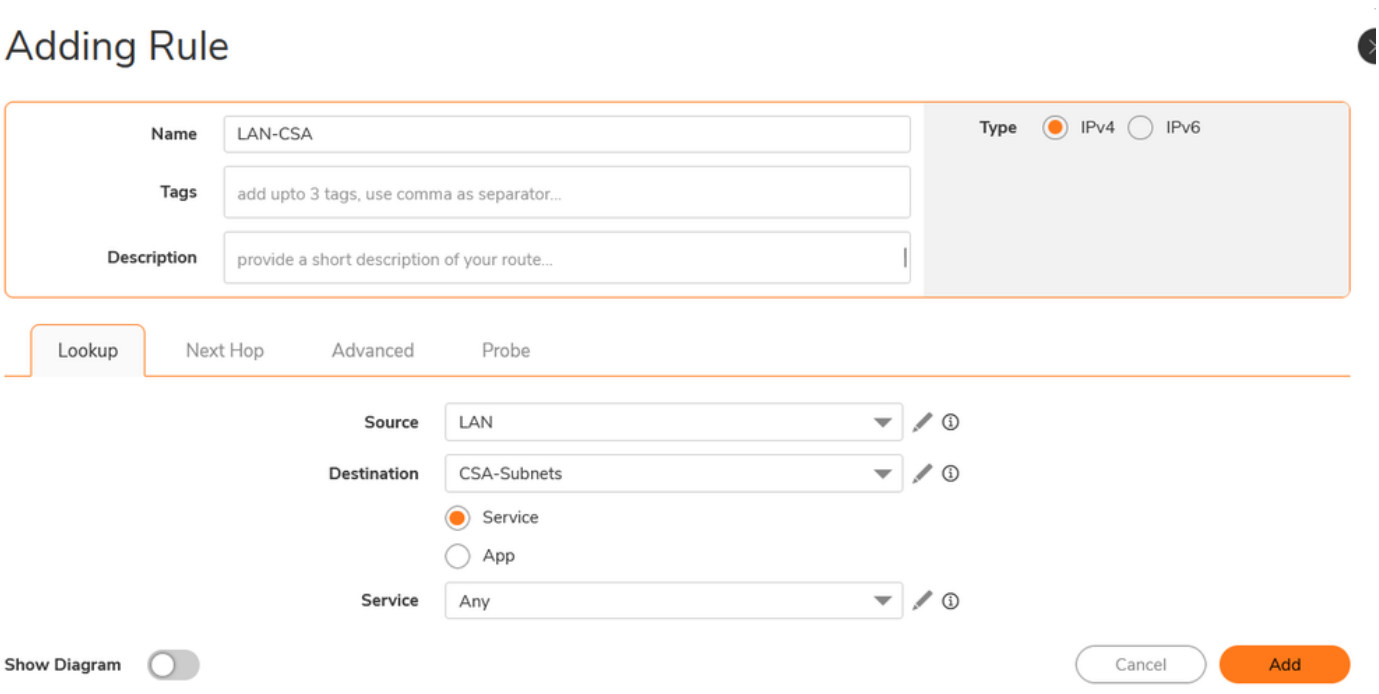
Passare al dashboard di Sonicwall.

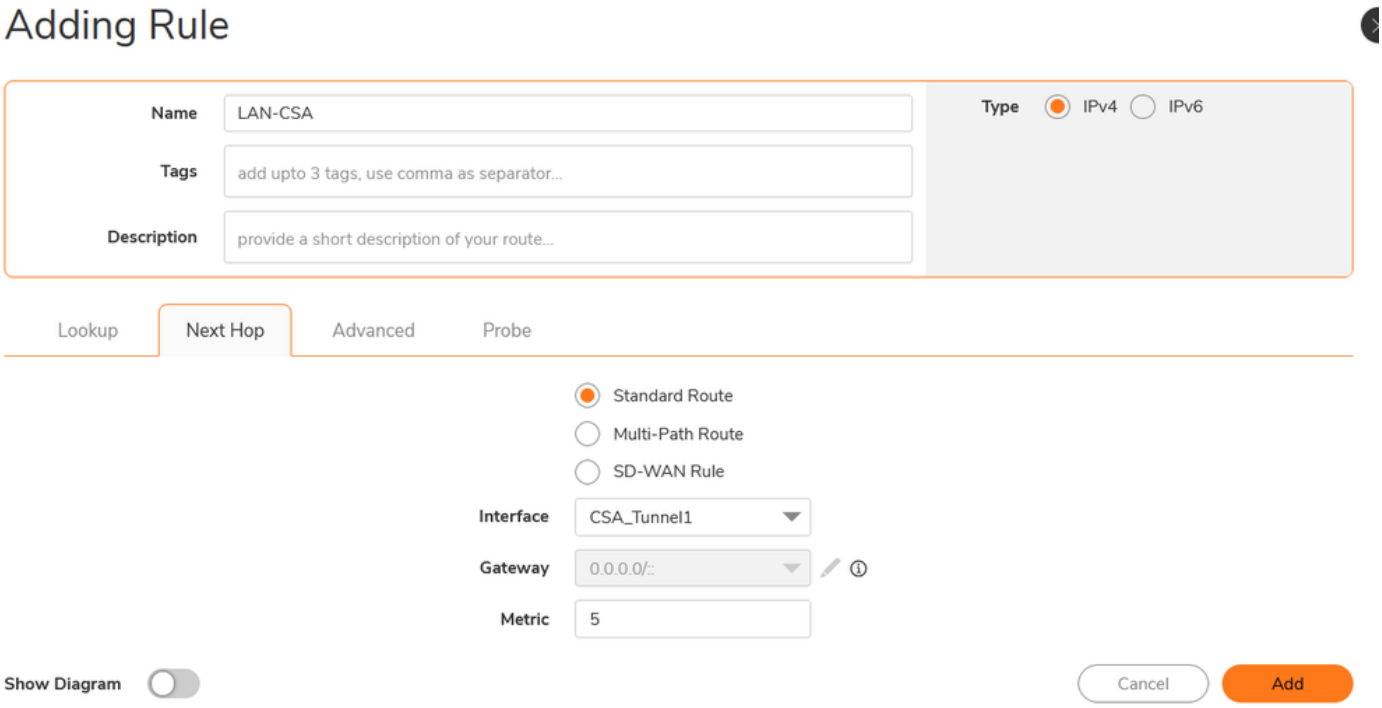
- Criterio > Regole e criteri > Regole di routing
- Fare clic su + Aggiungi



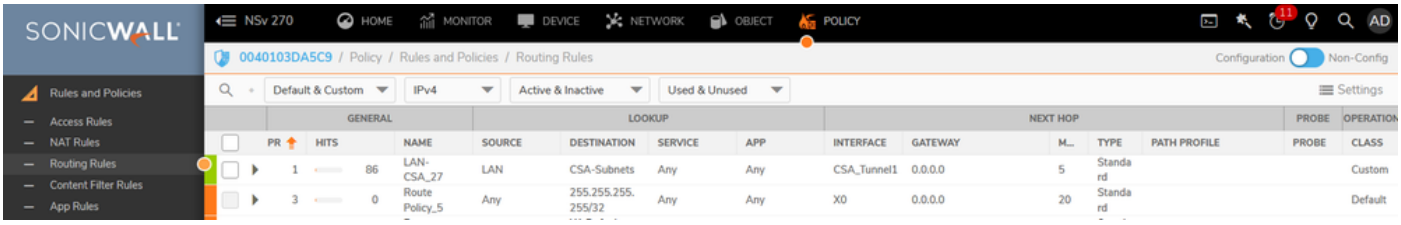
Sonicwall - Regole Di Routing

- Aggiungi regola di routing





- Fare clic su + Aggiungi

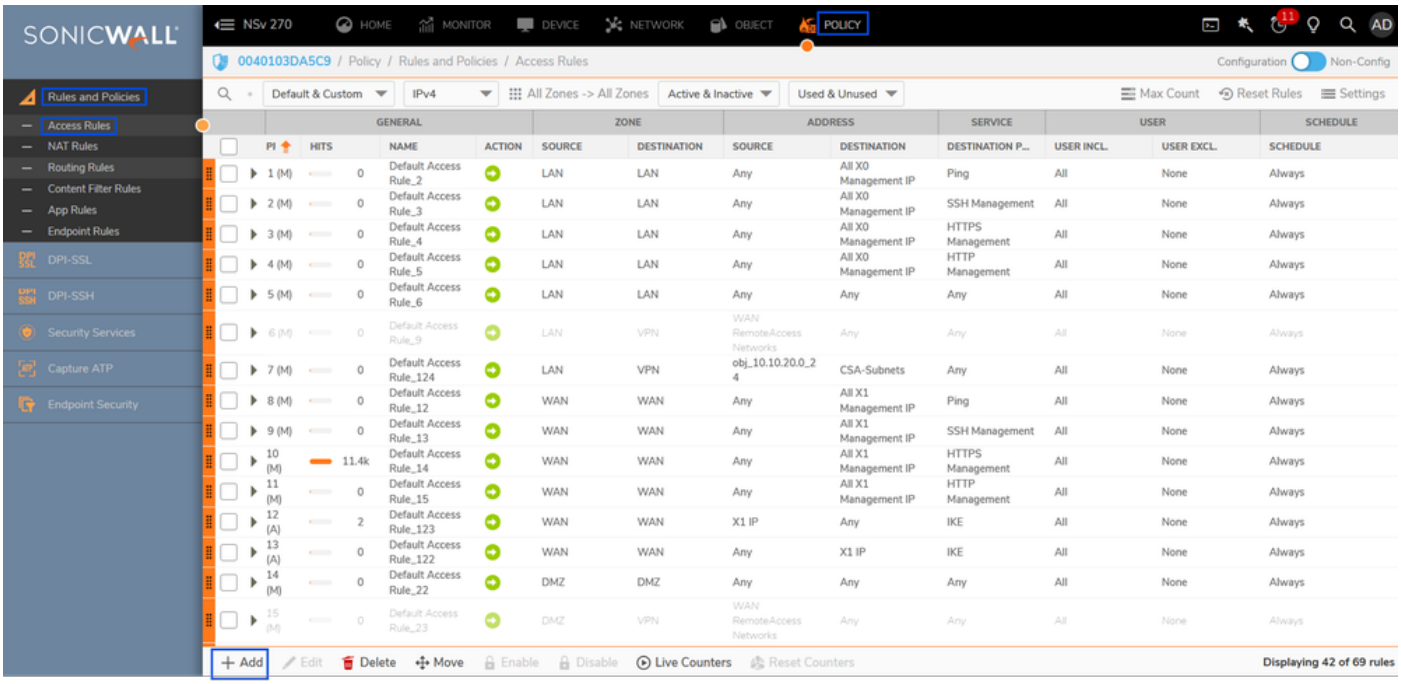


Sonicwall - Regole Di Routing

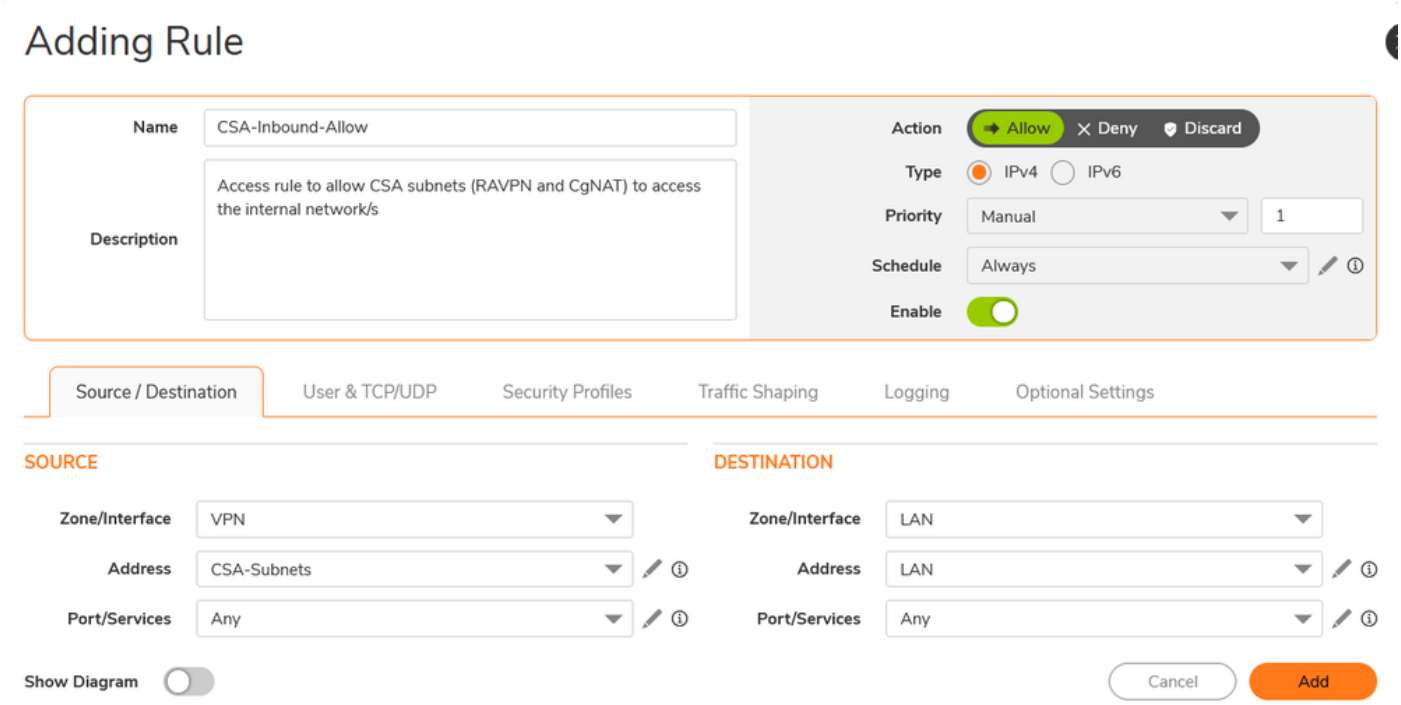
Aggiungi regole di accesso

Passare al dashboard di Sonicwall.

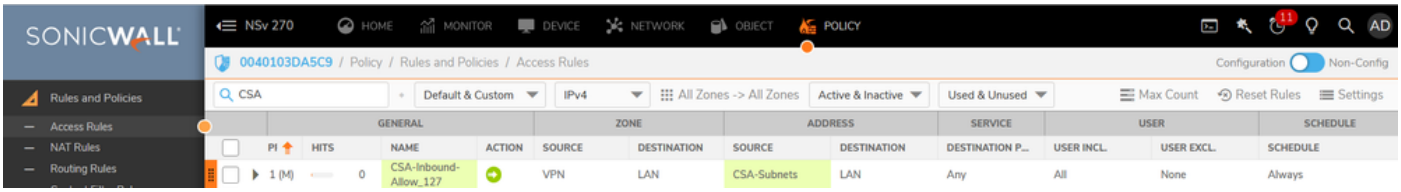
- Criterio > Regole e criteri > Regole di accesso
- Fare clic su + Aggiungi



Sonicwall - Regole di accesso



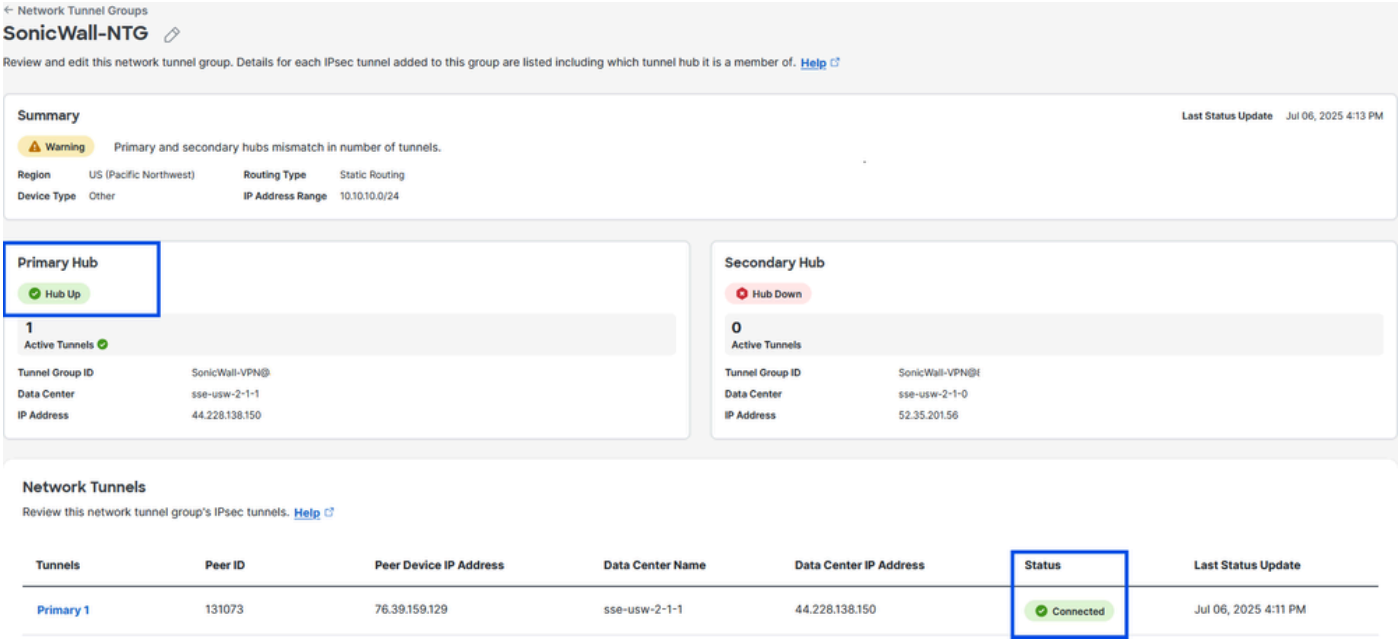
- Fare clic su +Aggiungi



Sonicwall - Regole di accesso

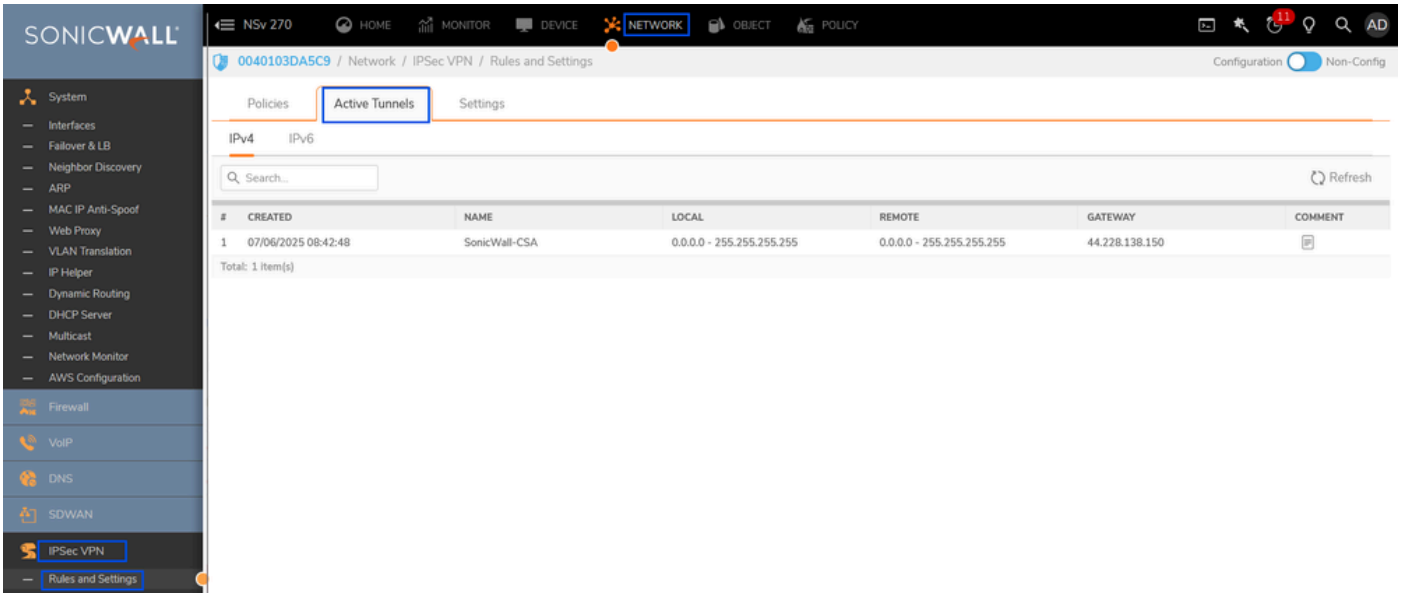
Verifica

- Stato tunnel su accesso sicuro



Accesso sicuro - Gruppo tunnel di rete - Stato VPN

- Stato del tunnel su Sonicwall Firewall



Sonicwall - Stato VPN IPSec

La stessa procedura può essere utilizzata per configurare il tunnel tra il data center secondario di Secure Access e Sonicwall

Ora che il tunnel è attivo su Secure Access e Sonicwall, è possibile continuare a configurare l'accesso alle risorse private tramite RA-VPN, Broswer-Based ZTA o Client Based ZTA su Secure Access Dashboard

Risoluzione dei problemi

PC utente

- Verificare che l'utente sia in grado o meno di connettersi/registrarsi a RAVPN/ZTNA. In caso contrario, risolvere ulteriormente il problema relativo alla mancata connessione del control plane.
- Verificare che la rete a cui l'utente sta tentando di accedere debba passare attraverso il tunnel RAVPN o ZTNA. In caso contrario, verificare la configurazione sull'headend.

Accesso sicuro

- Verificare la configurazione della direzione del traffico nel profilo di connessione RAVPN per confermare che la rete di destinazione è configurata per l'invio tramite il tunnel a Secure Access.
- Verificare che la risorsa privata sia definita con porte/protocolli validi e che i meccanismi di connessione ZTNA/RAVPN siano selezionati.
- Verificare che i criteri di accesso siano configurati in modo da consentire agli utenti RAVPN/ZTNA di accedere alla rete di risorse private e che i criteri siano ordinati in modo che nessun'altra regola abbia la precedenza per bloccare il traffico.
- Verificare che il tunnel IPSec sia attivo e che Accesso sicuro visualizzi le route client valide tramite il routing statico che copre le risorse private a cui l'utente sta tentando di accedere.

Sonicwall

- Verificare che il tunnel IPSec sia attivo o meno (IKE & IPSec SA).
- Verificare che le route del client siano annunciate correttamente.
- Verificare che il traffico proveniente dall'utente RAVPN/ZTNA e destinato a una risorsa privata dietro Sonicwall stia raggiungendo il firewall di Sonicwall attraverso il tunnel acquisendo i pacchetti su Sonicwall.
- Verificare che il traffico abbia raggiunto la risorsa privata e rispondere al client RAVPN/ZTNA o meno. In caso affermativo, verificare che i pacchetti stiano raggiungendo l'interfaccia X0 (LAN) di Sonic.
- Verificare che Sonicwall stia inoltrando il traffico di ritorno attraverso il tunnel IPSec verso l'accesso sicuro.

Informazioni correlate

- Supporto tecnico Cisco e download
- Cisco Secure Access Help Center
- Zero Trust Access Module
- Errore Di Risoluzione Dei Problemi Relativi All'Accesso Sicuro: Il Servizio Di Registrazione Non Risponde. Contatta il tuo help desk IT"

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).