使用Sonicwall防火墙配置安全访问

目录

简介

先决条件

- 要求
- 使用的组件
- 背景信息
- 网络图

配置

- 在安全访问中配置网络隧道组(VPN)
- 在Sonicwall上配置隧道
- 配置隧道 — 规则和设置
- 添加VPN隧道接口
- 添加网络对象和组
- 添加路由
- 添加访问规则

验证

故障排除

- 用户 PC
- 安全访问
- Sonicwall

相关信息

简介

本文档介绍如何使用静态路由在Secure Access to Sonicwall防火墙之间配置IPsec VTI隧道。

先决条件

- 配置用户调配
- ZTNA SSO身份验证配置
- 配置远程访问VPN安全访问

要求

Cisco 建议您了解以下主题：

- Sonicwall(NSv270 - SonicOSX 7.0.1)防火墙
- 安全访问
- 思科安全客户端 — VPN
- 思科安全客户端 — ZTNA

- 无客户端ZTNA

使用的组件

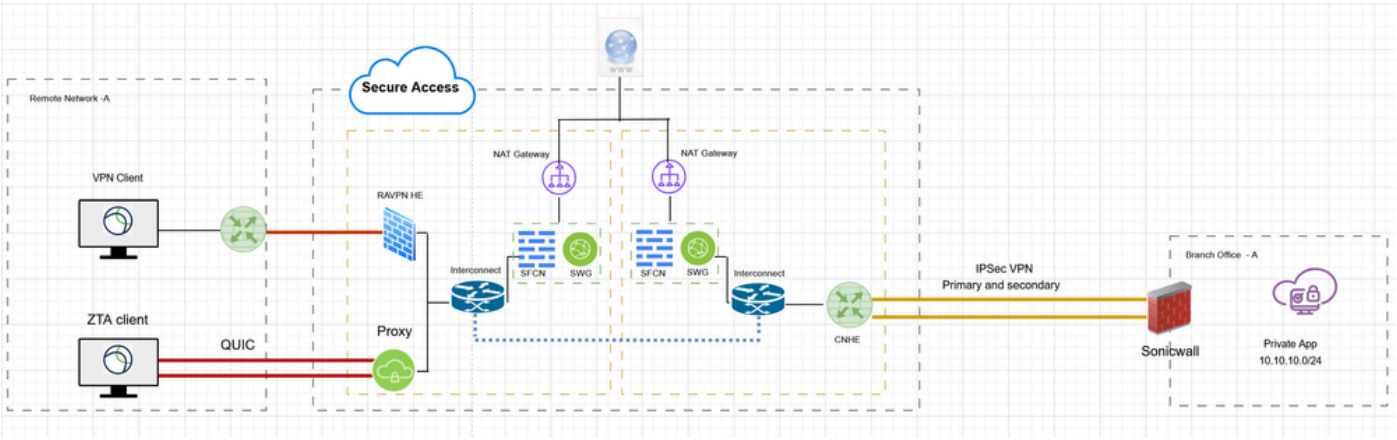
本文档中的信息基于：

- Sonicwall(NSv270 - SonicOSX 7.0.1)防火墙
- 安全访问
- 思科安全客户端 — VPN
- 思科安全客户端 — ZTNA

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

网络图



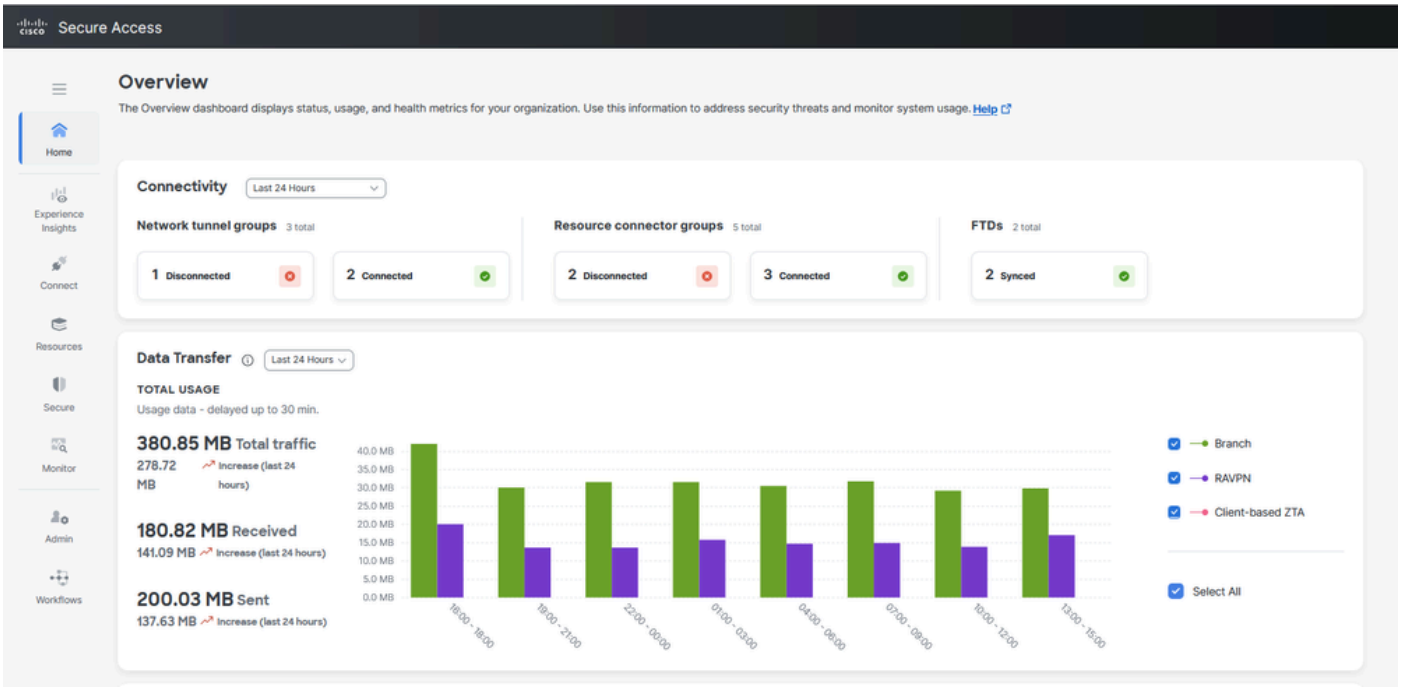
网络图

配置

在安全访问中配置网络隧道组(VPN)

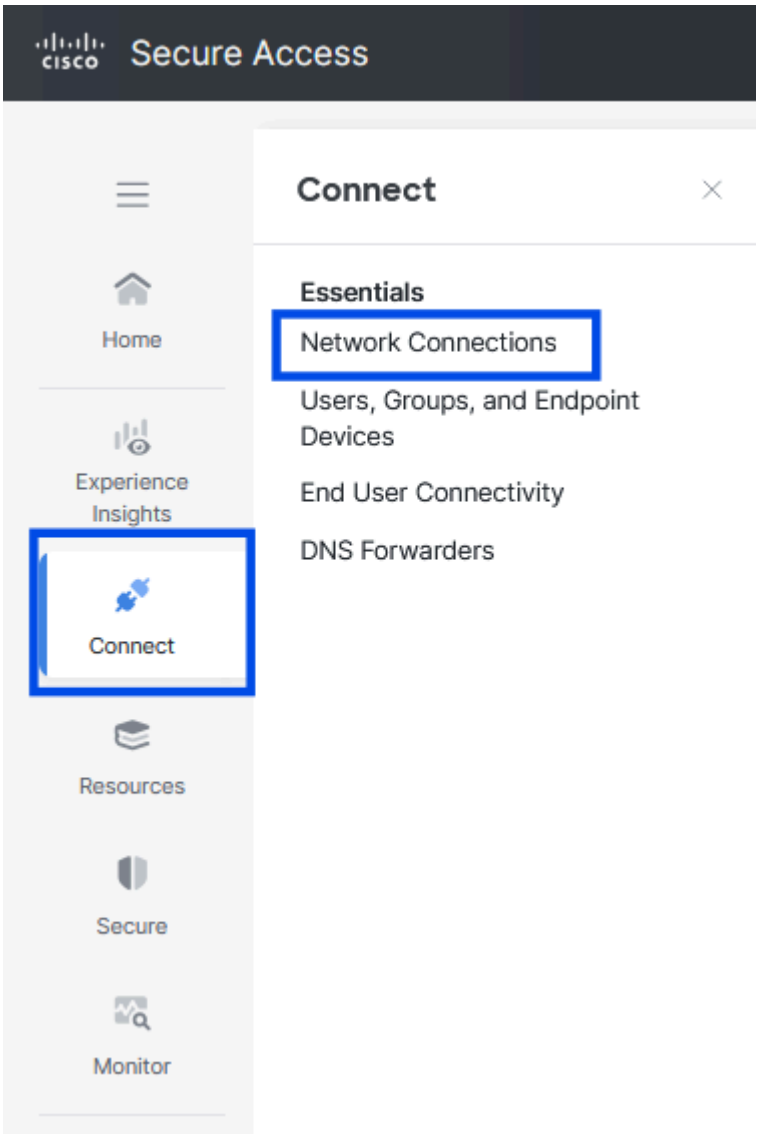
在安全访问和Sonicwall之间配置VPN隧道

- 导航到安全访问的管理员门户



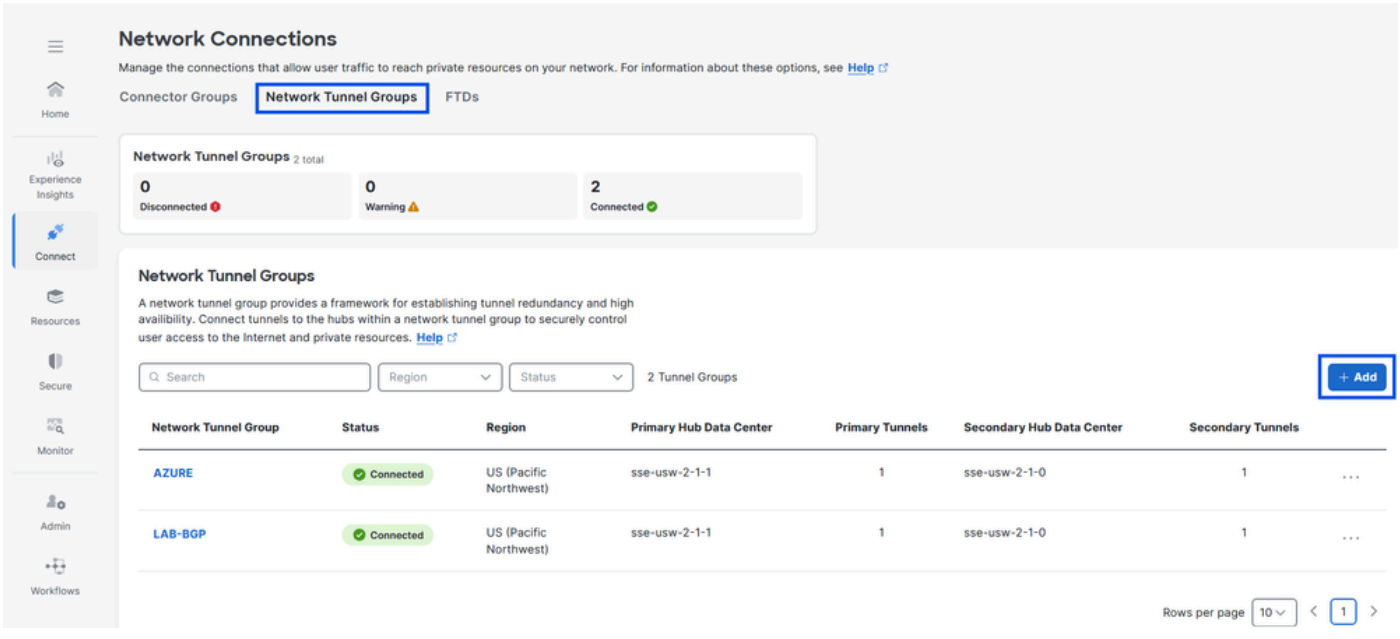
安全访问 — 主页

- 单击Connect > Network Connections



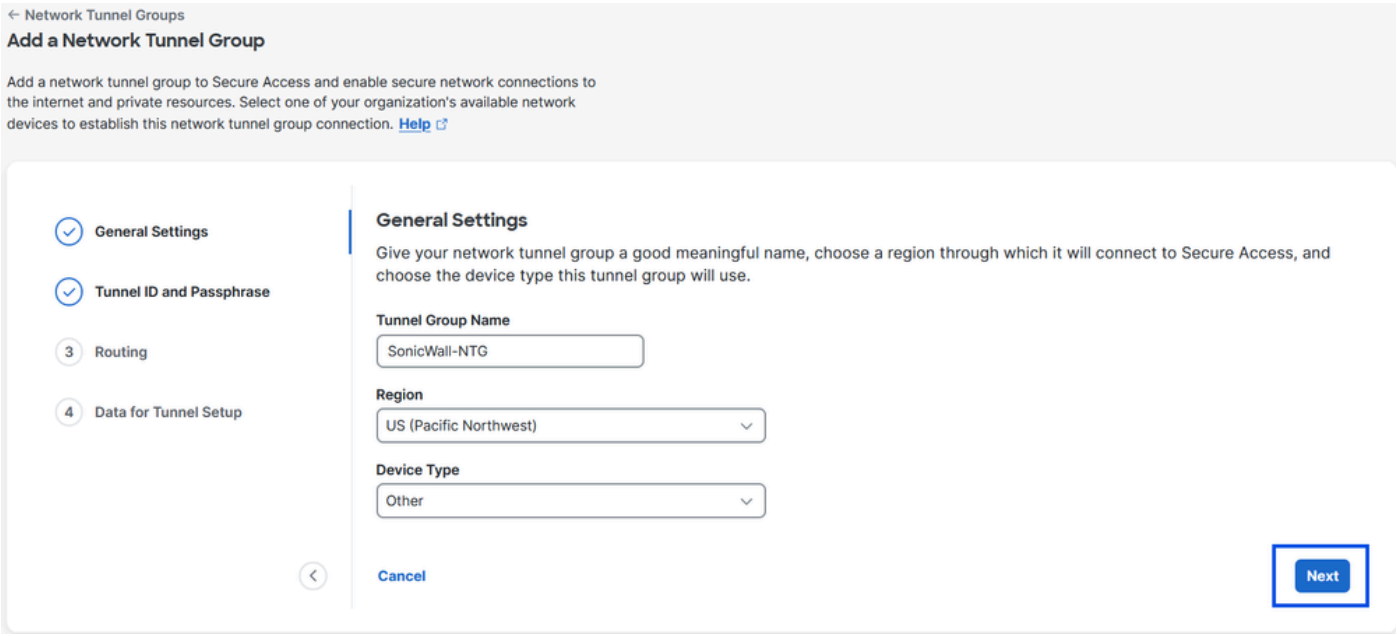
安全访问 — 网络连接

- 在Network Tunnel Groups下，单击+ Add



安全访问 — 网络隧道组

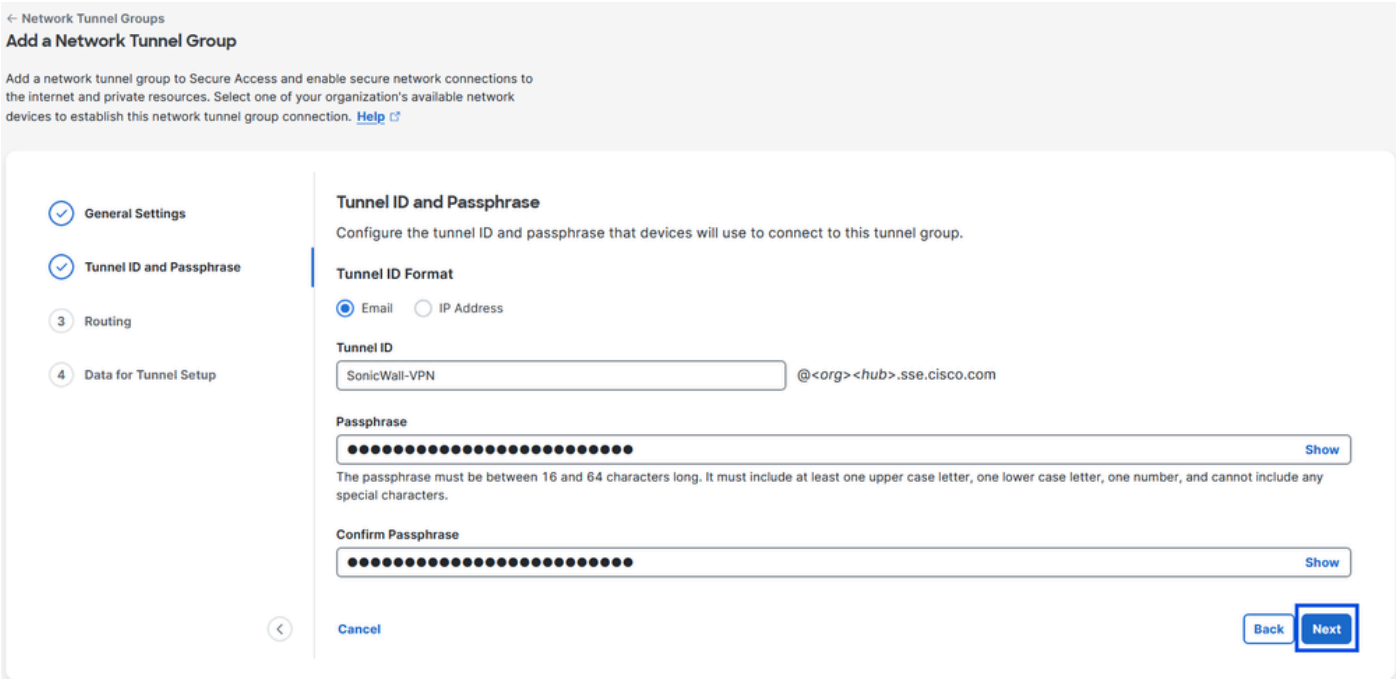
- 配置隧道组名称、区域和设备类型
- 单击“下一步”



安全访问 — 网络隧道组 — 常规设置

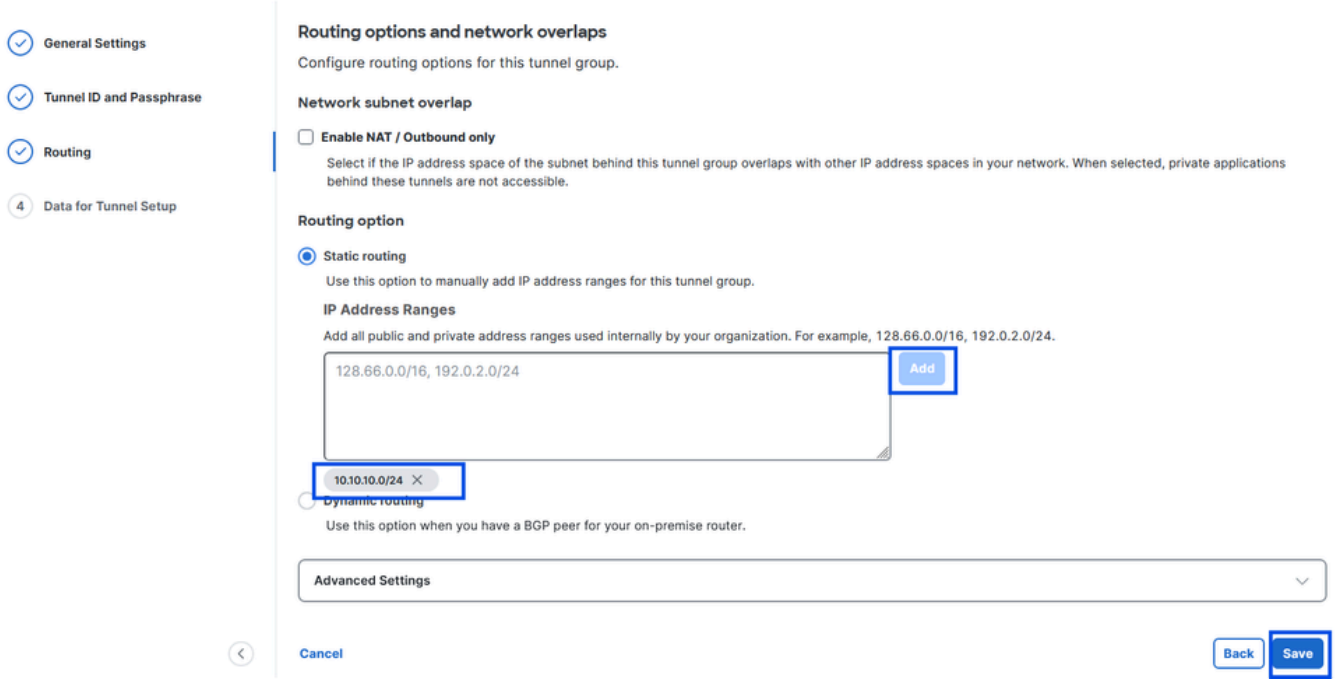
注意：选择距离防火墙位置最近的区域。

- 配置隧道ID格式和密码
- 单击“下一步”



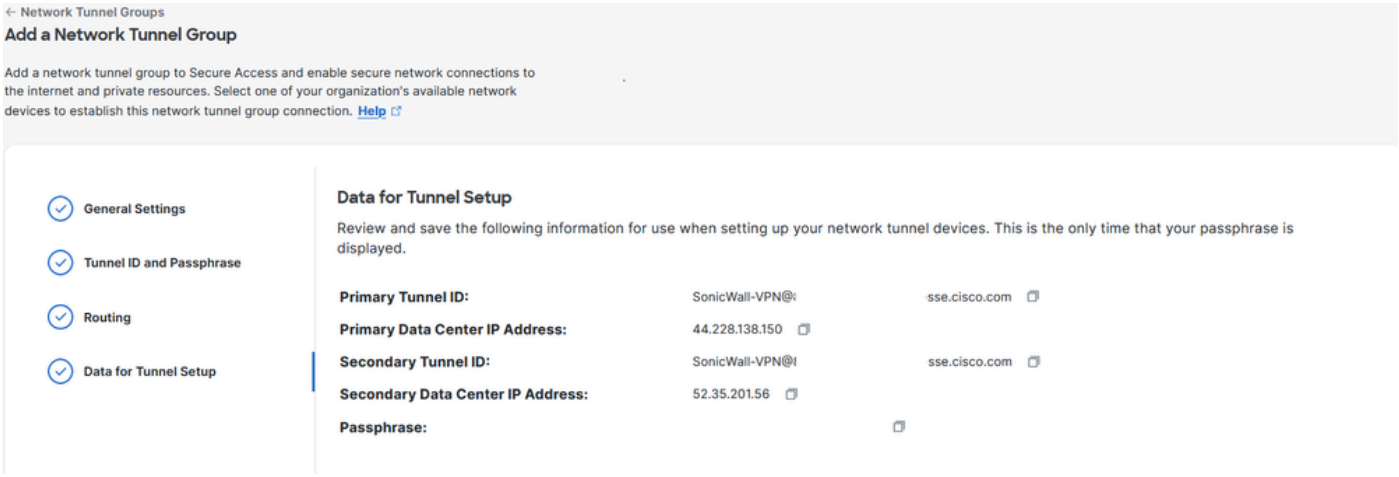
安全访问 — 隧道ID和密码

- 配置网络上已配置并希望通过安全访问传递流量的IP地址范围、主机或子网
- 单击Add
- 点击保存



安全访问 — 隧道组 — 路由选项

点击Save（保存）后，会显示有关隧道的信息。请保存该信息，以便进行下一步配置



安全访问 — 用于隧道设置的数据

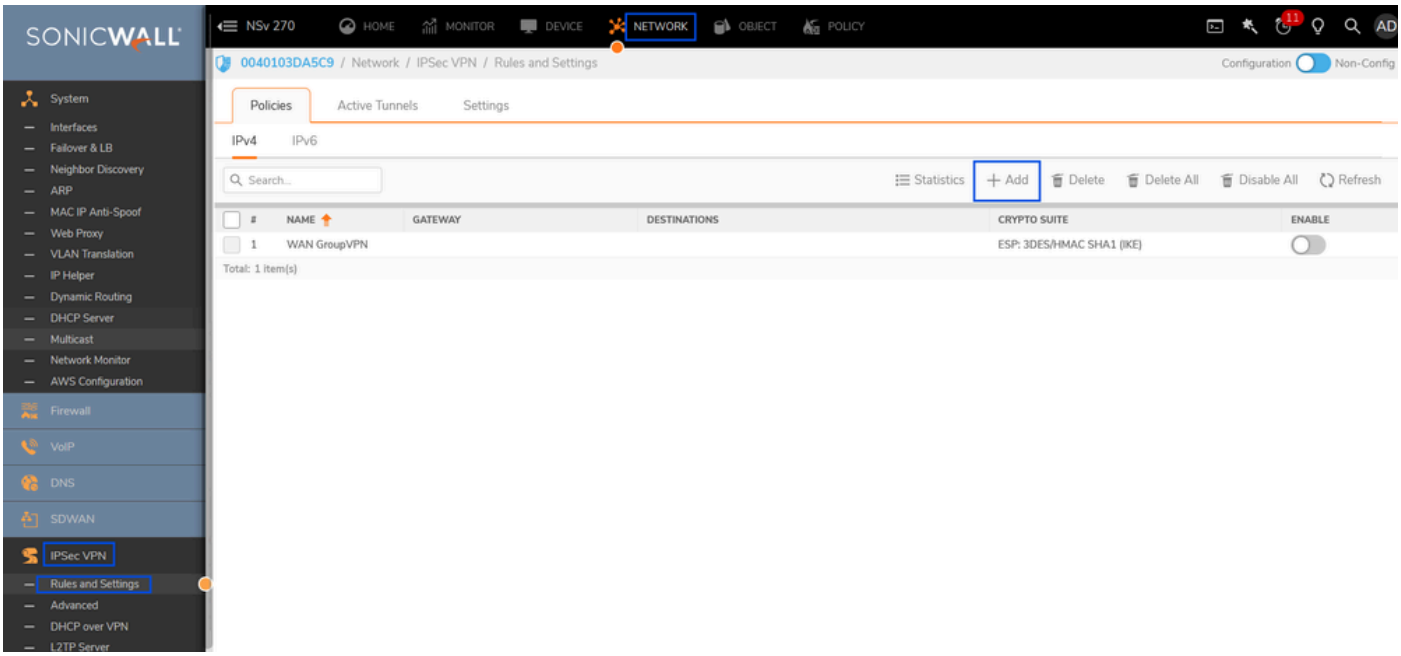
在Sonicwall上配置隧道

配置隧道 — 规则和设置

导航到Sonicwall控制面板。

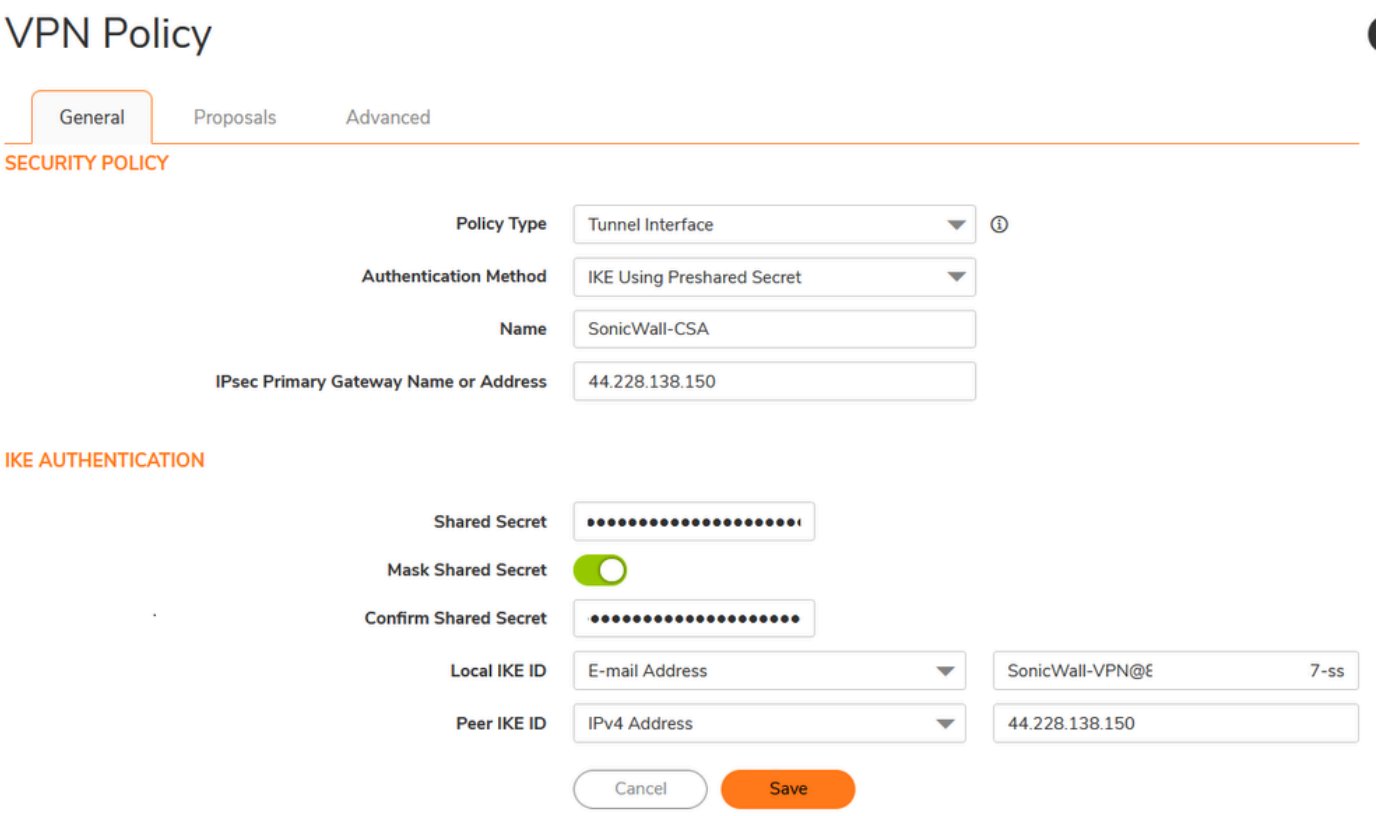
- Network > IPsec VPN > Rules and Settings

- 单击+ Add



Sonicwall - IPSec VPN — 规则和设置

- 在VPN Policy下，根据来自安全访问的隧道数据和supported-ipsec-parameters填充VPN配置



VPN Policy

General | Proposals | Advanced

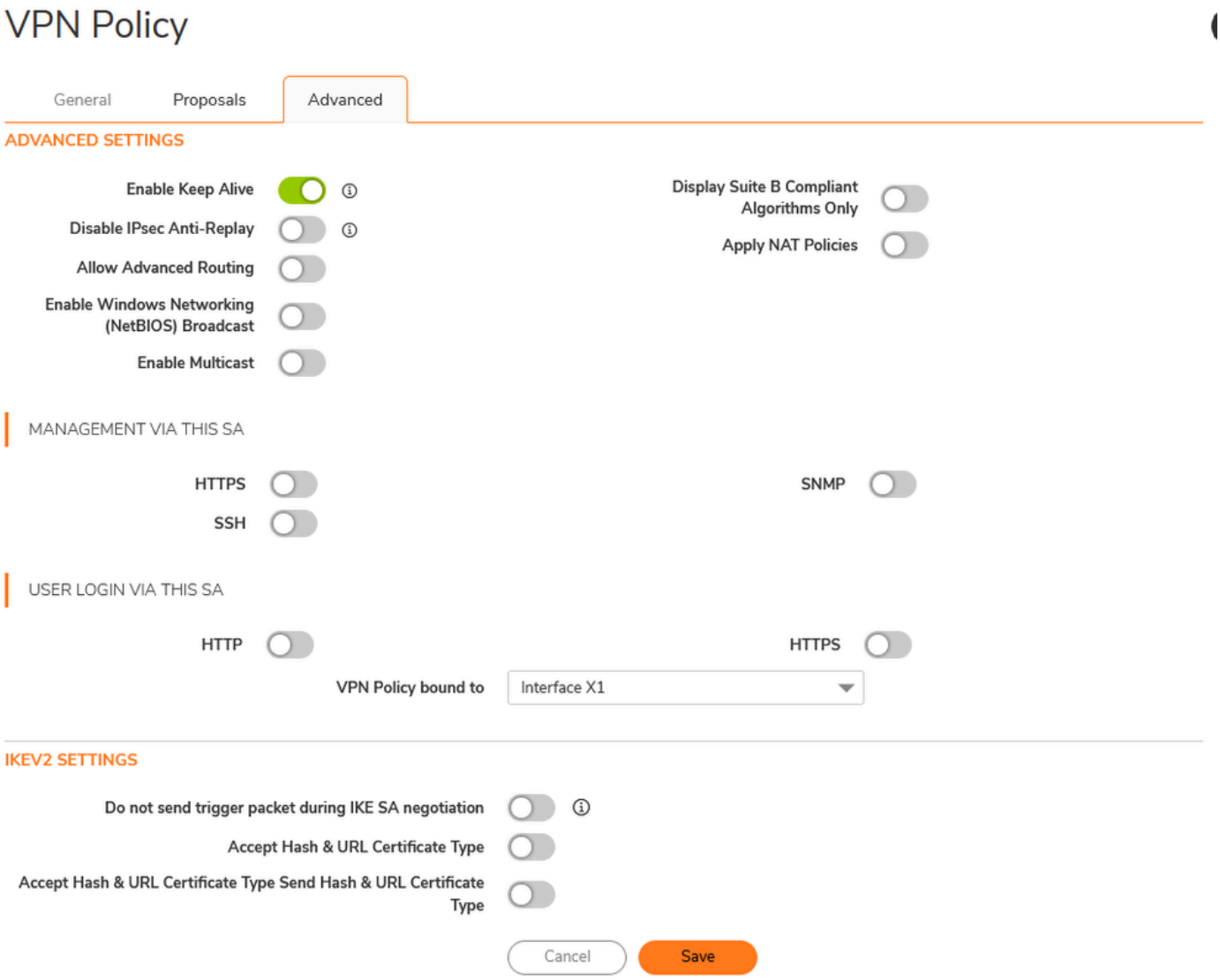
IKE (PHASE 1) PROPOSAL

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

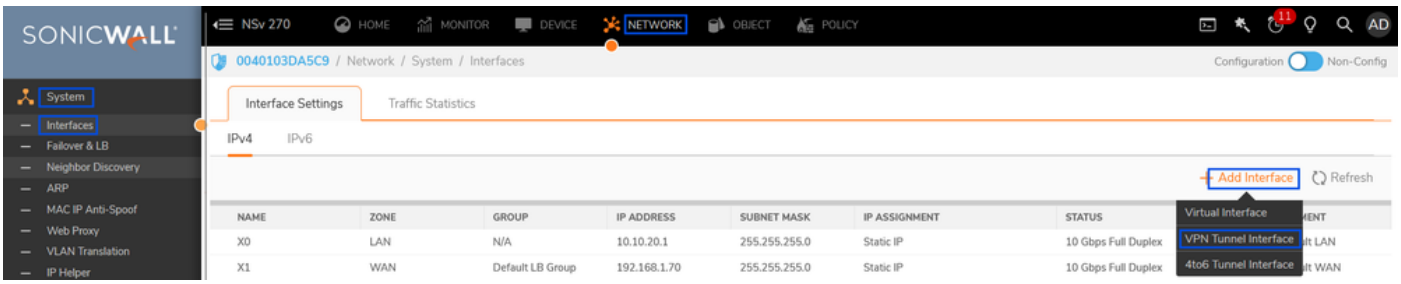


- 单击Save

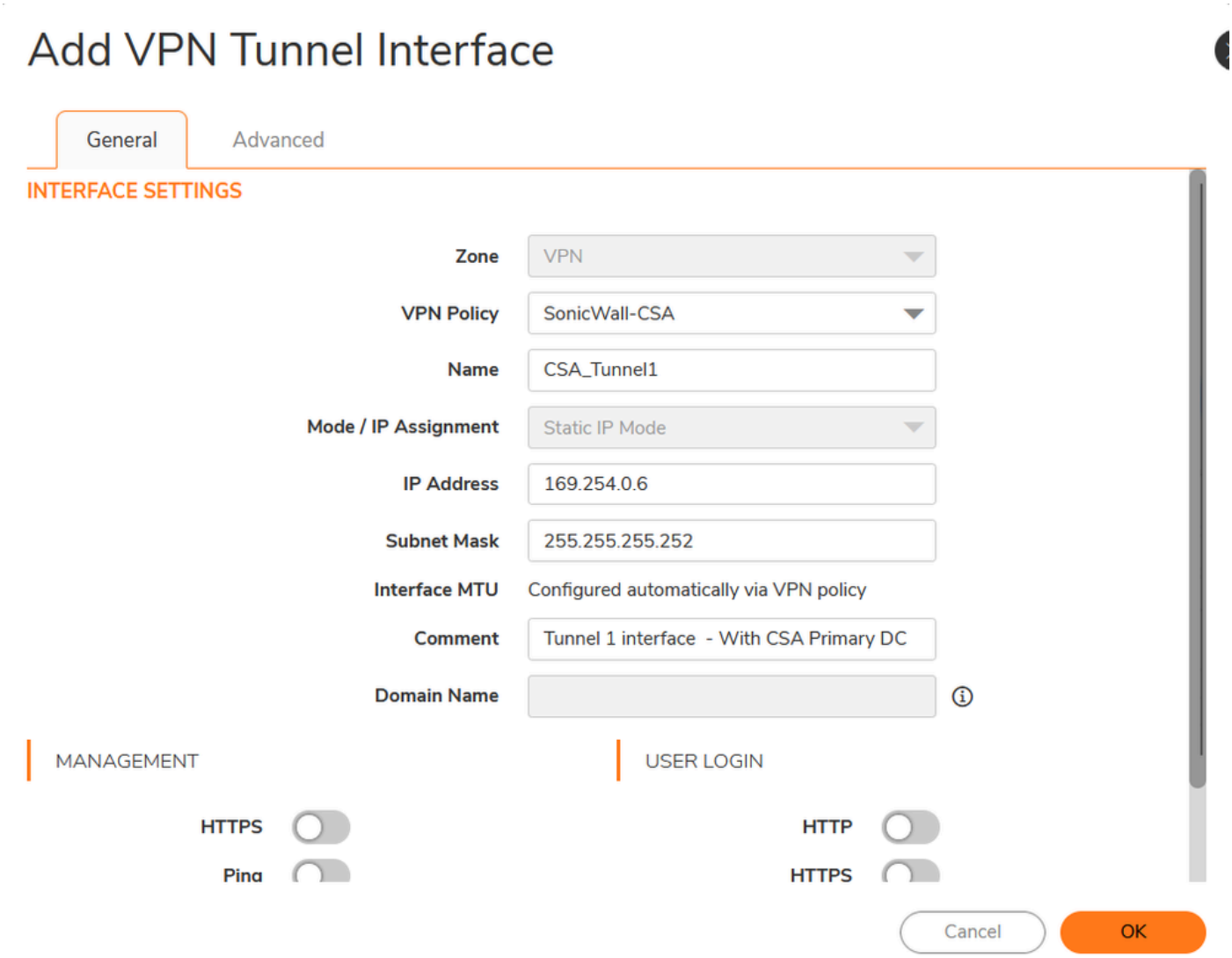
添加VPN隧道接口

导航到Sonicwall控制面板。

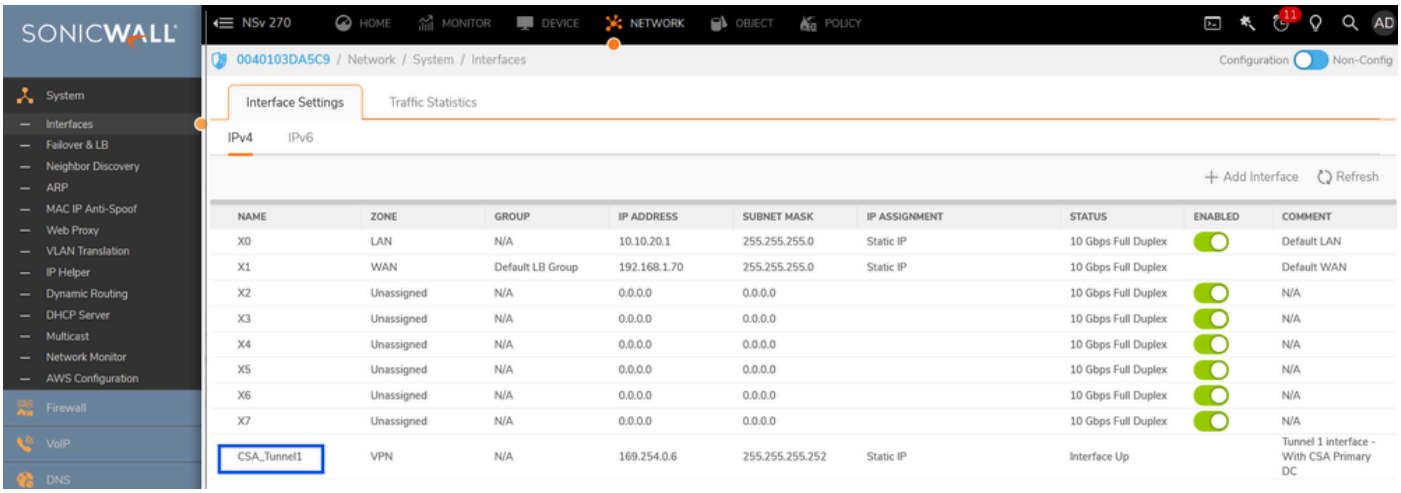
- Network > System > Interface
- 单击+ Add Interface
- 选择VPN隧道接口



Sonicwall — 接口



- 单击 OK

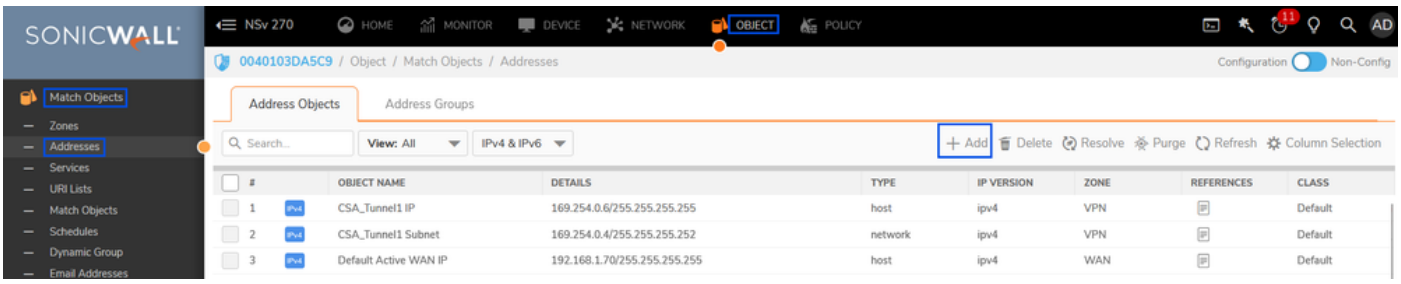


Sonicwall — 接口 — VPN隧道接口

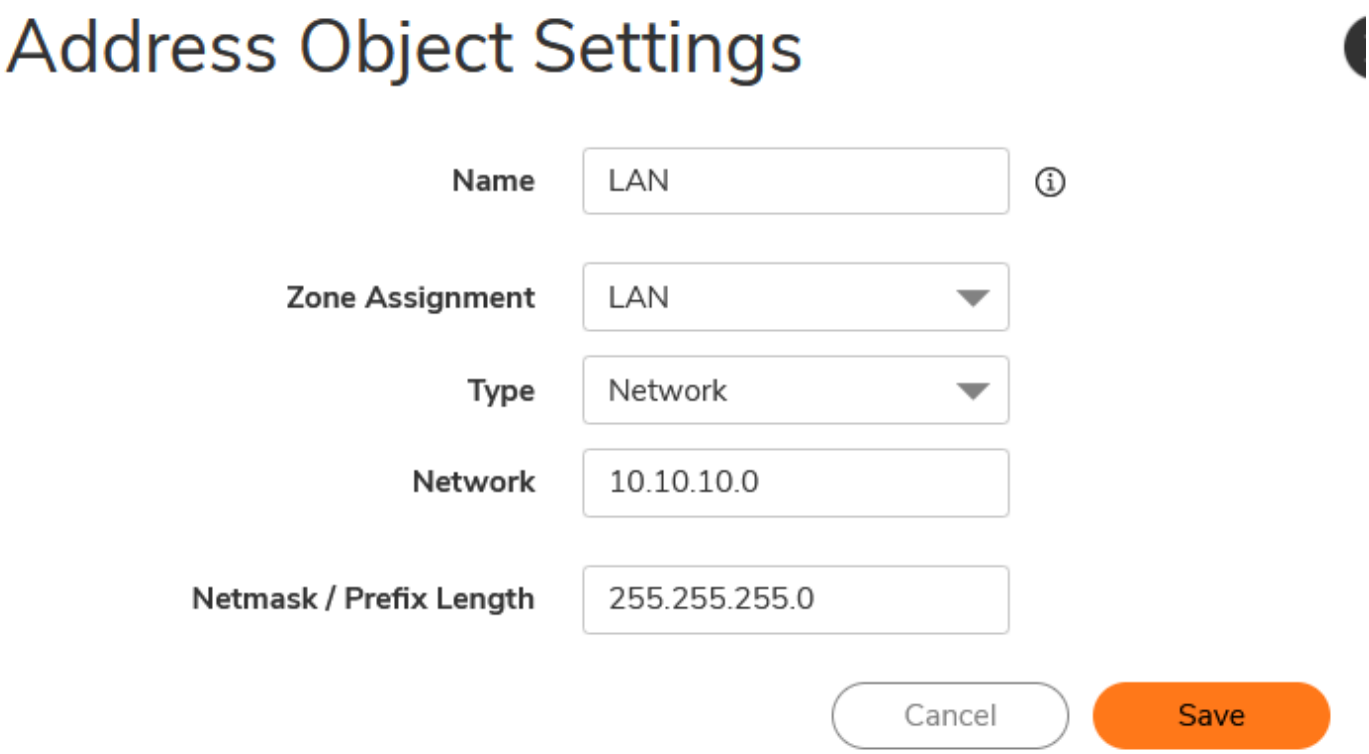
添加网络对象和组

导航到Sonicwall控制面板。

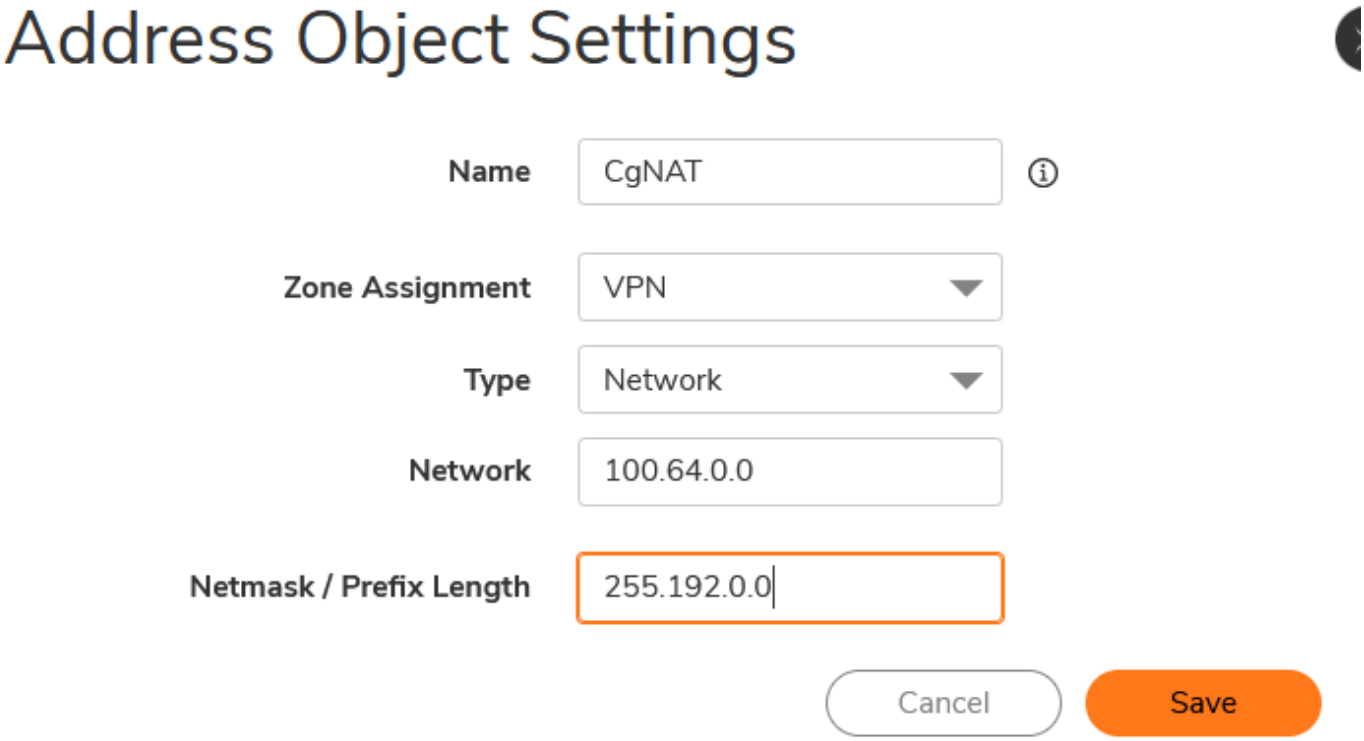
- 对象(Object)>匹配对象(Match Objects)>地址(Addresses)
- 地址对象
- 点击+Add



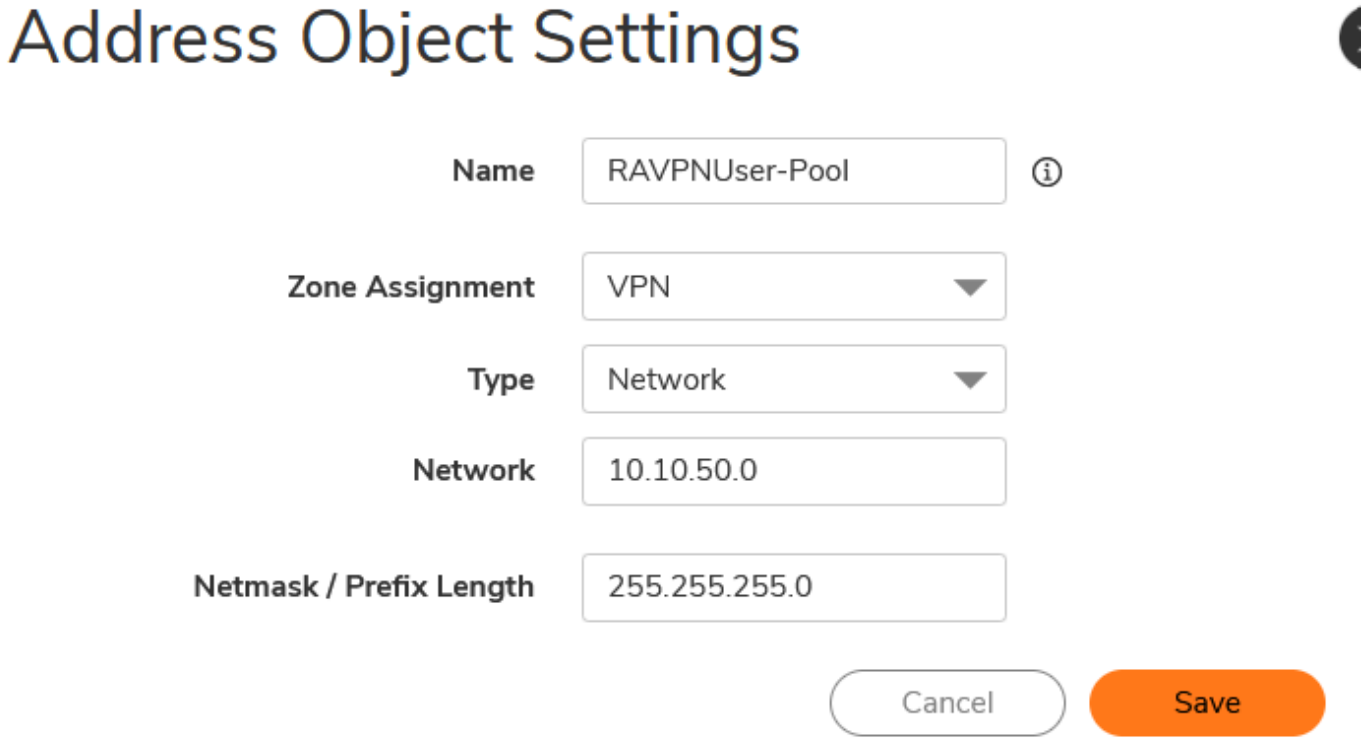
Sonicwall — 对象 — 地址对象



- 点击保存

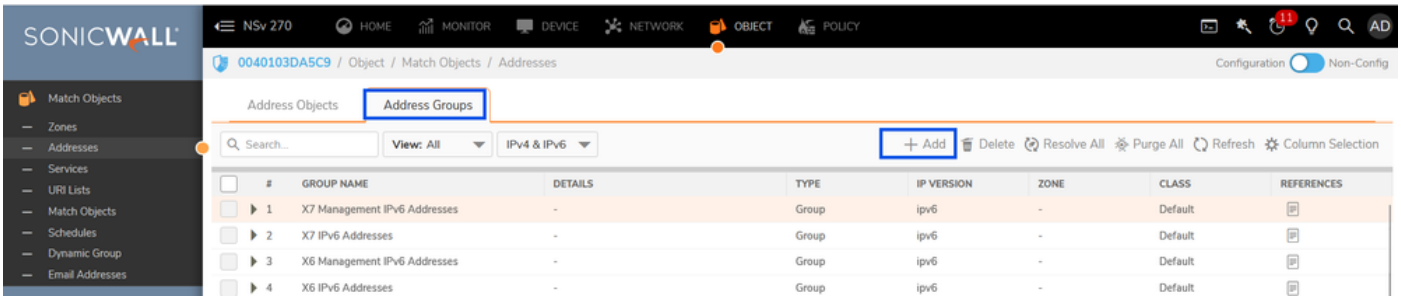


- 点击保存

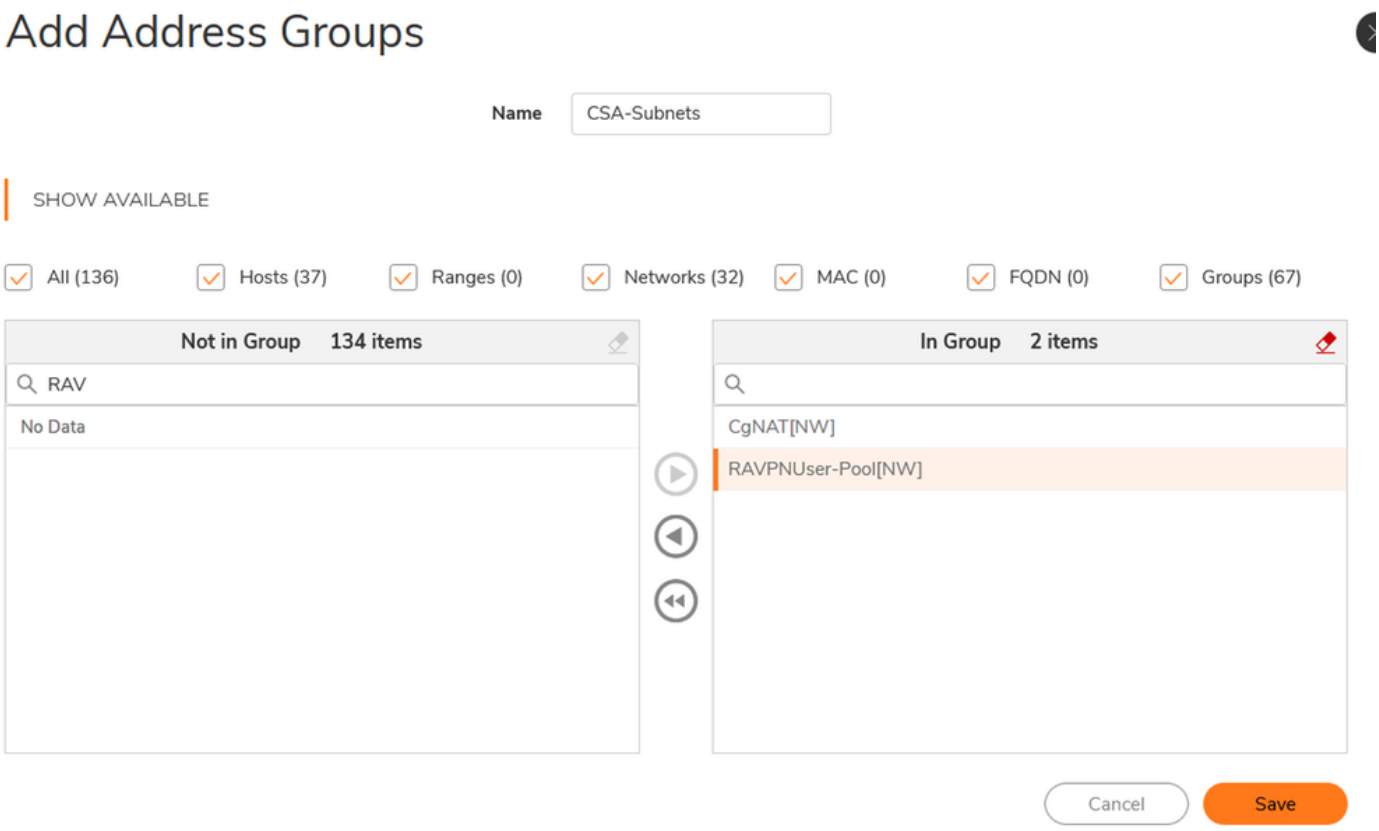


- 点击保存

- 创建地址组
- 单击+Add
- 选择地址对象并将其添加到地址组



Sonicwall — 对象 — 地址组

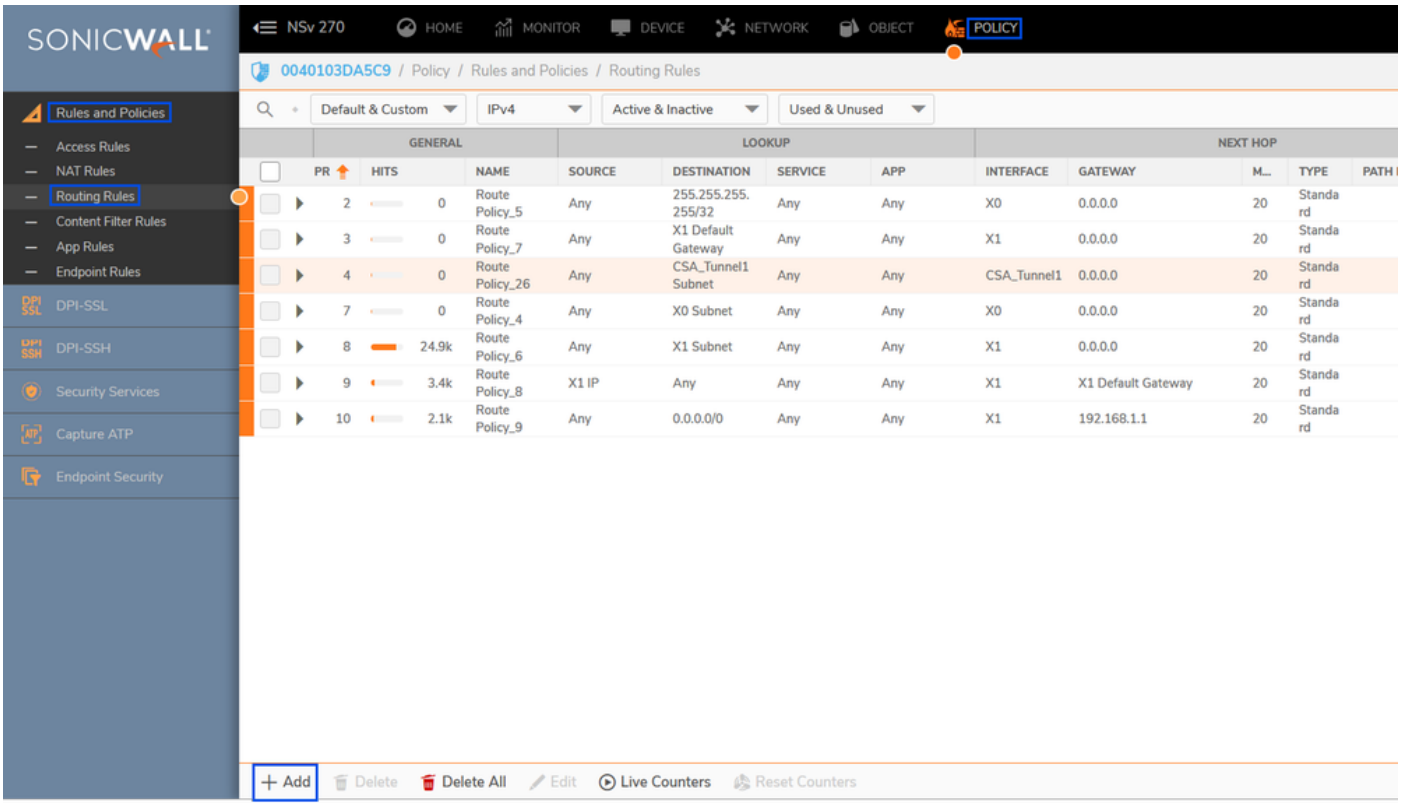


- 点击保存

添加路由

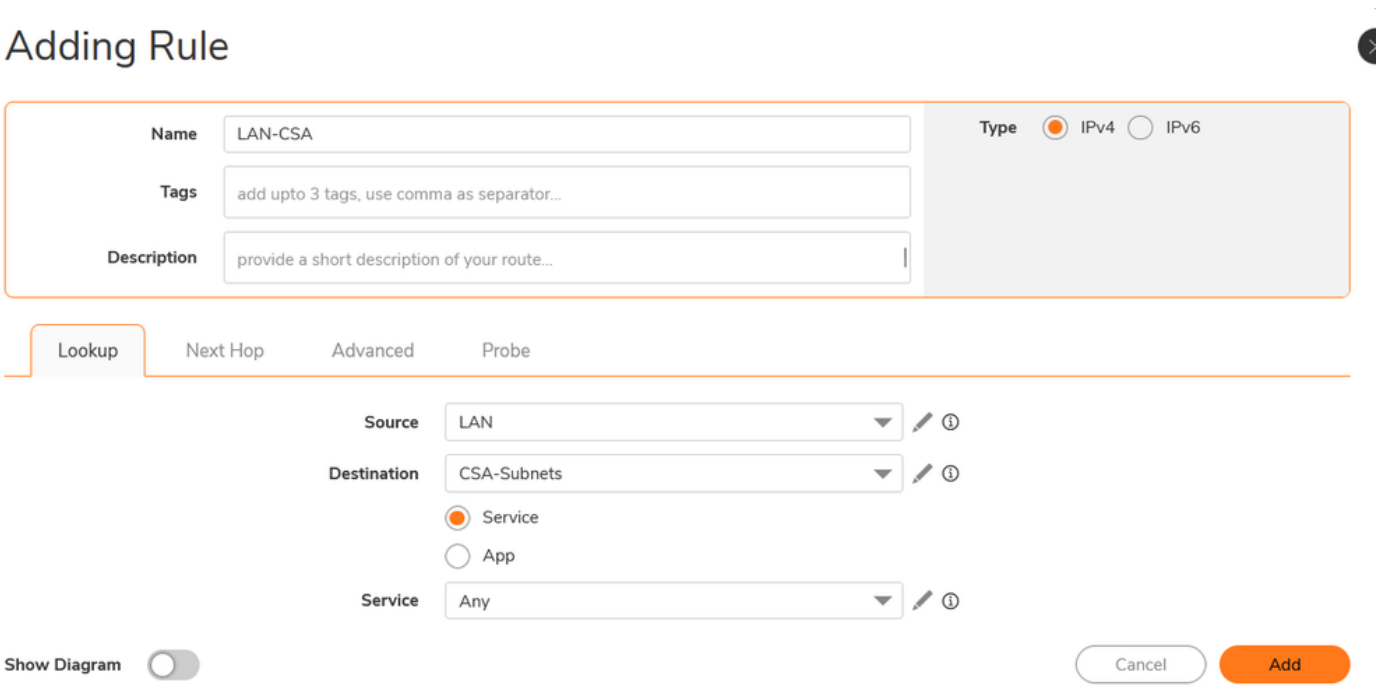
导航到Sonicwall控制面板。

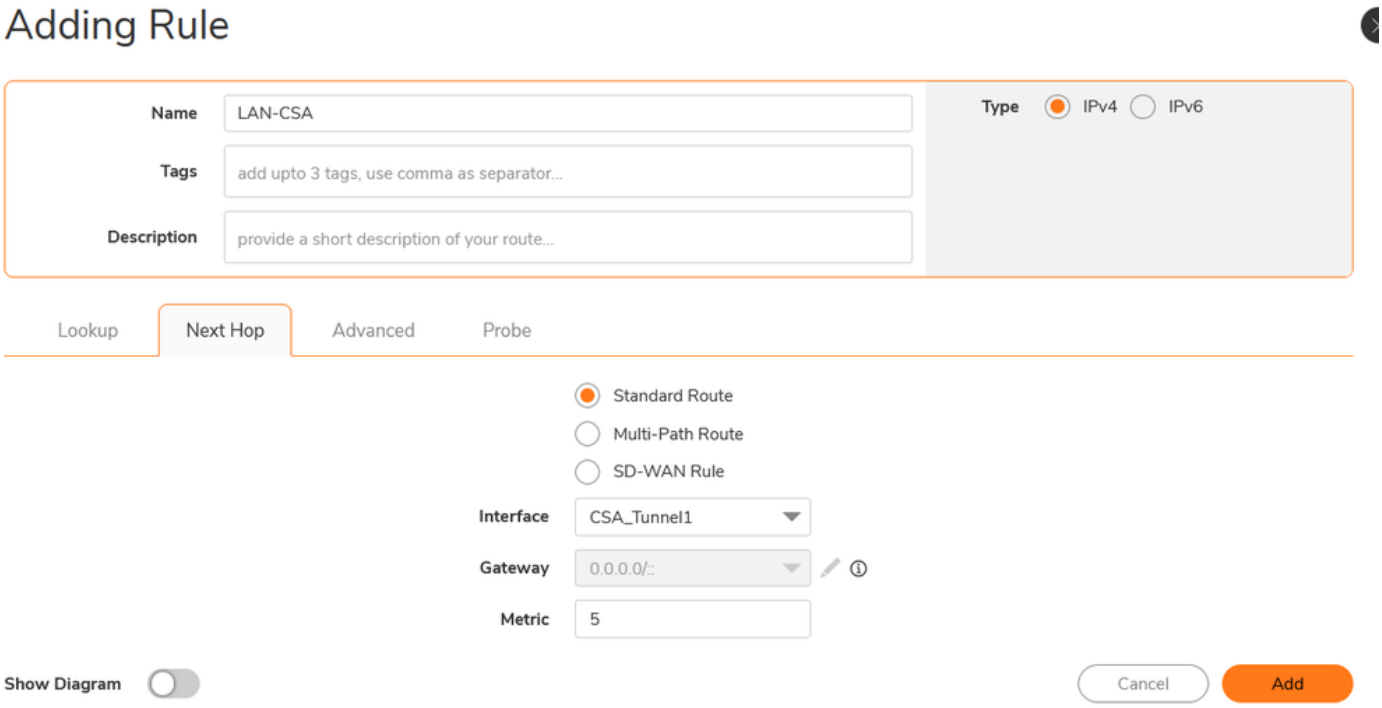
- 策略>规则和策略>路由规则
- 单击+ Add



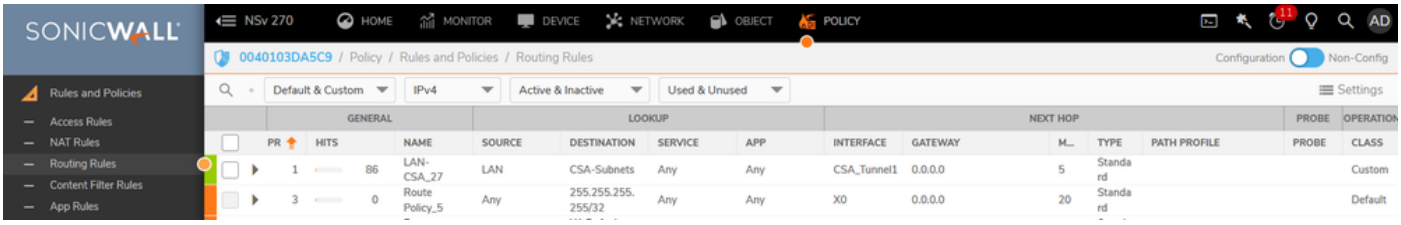
Sonicwall — 路由规则

- 添加路由规则





- 单击+ Add

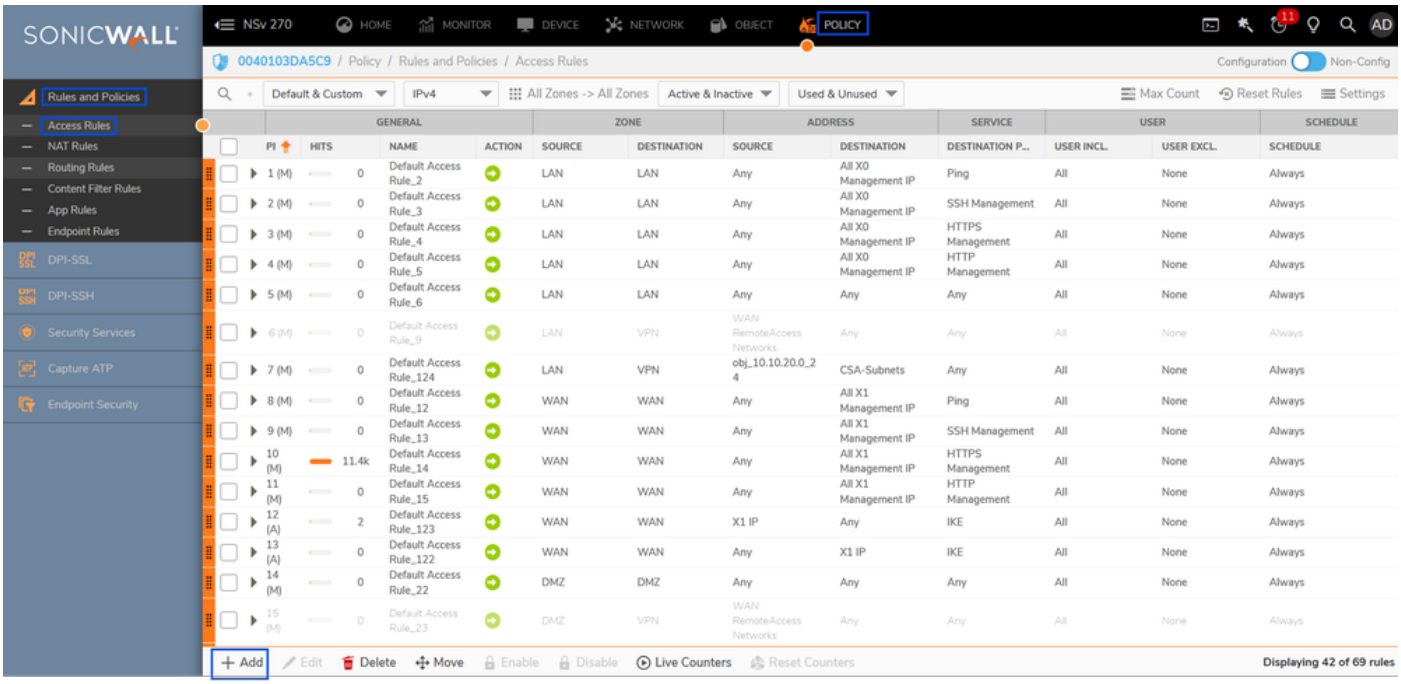


Sonicwall — 路由规则

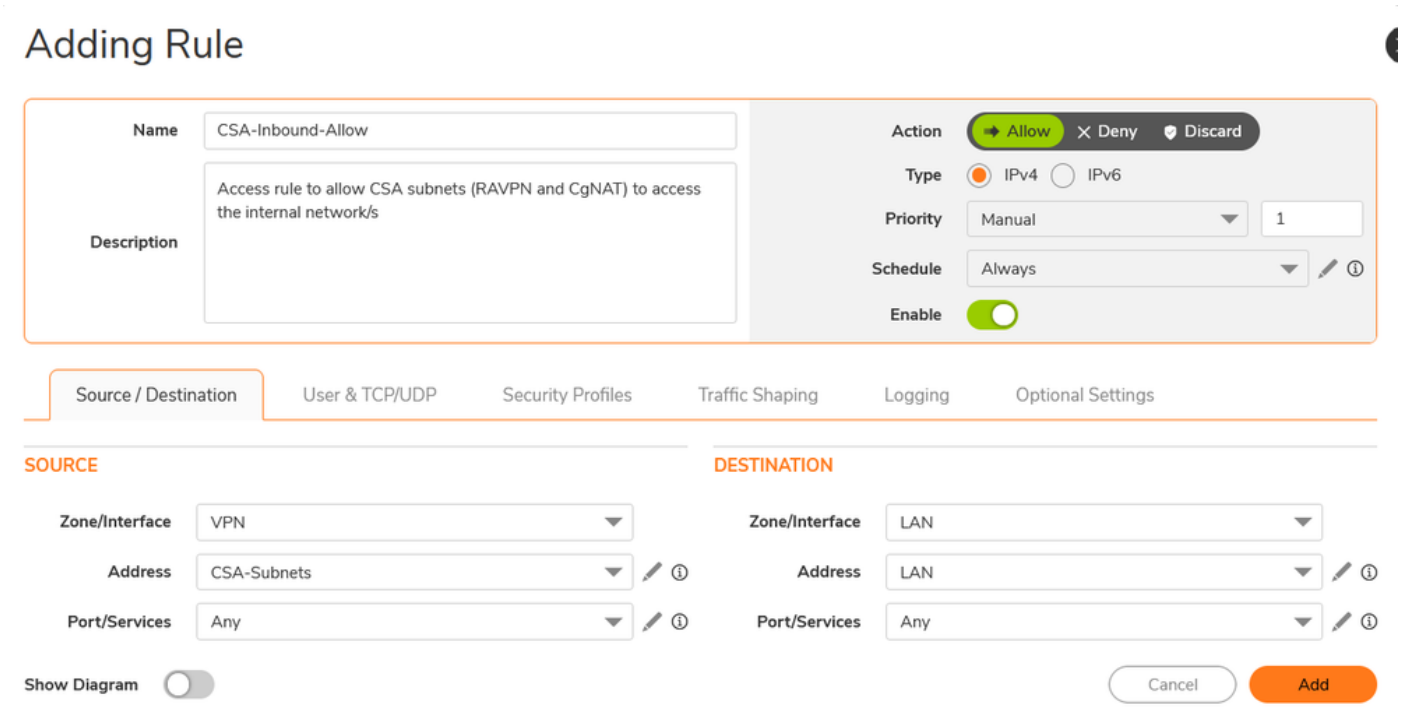
添加访问规则

导航到Sonicwall控制面板。

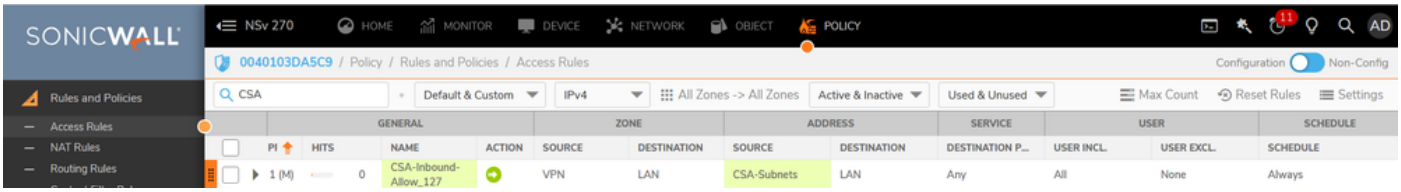
- Policy > Rules and Policies > Access Rules
- 单击+ Add



Sonicwall — 访问规则



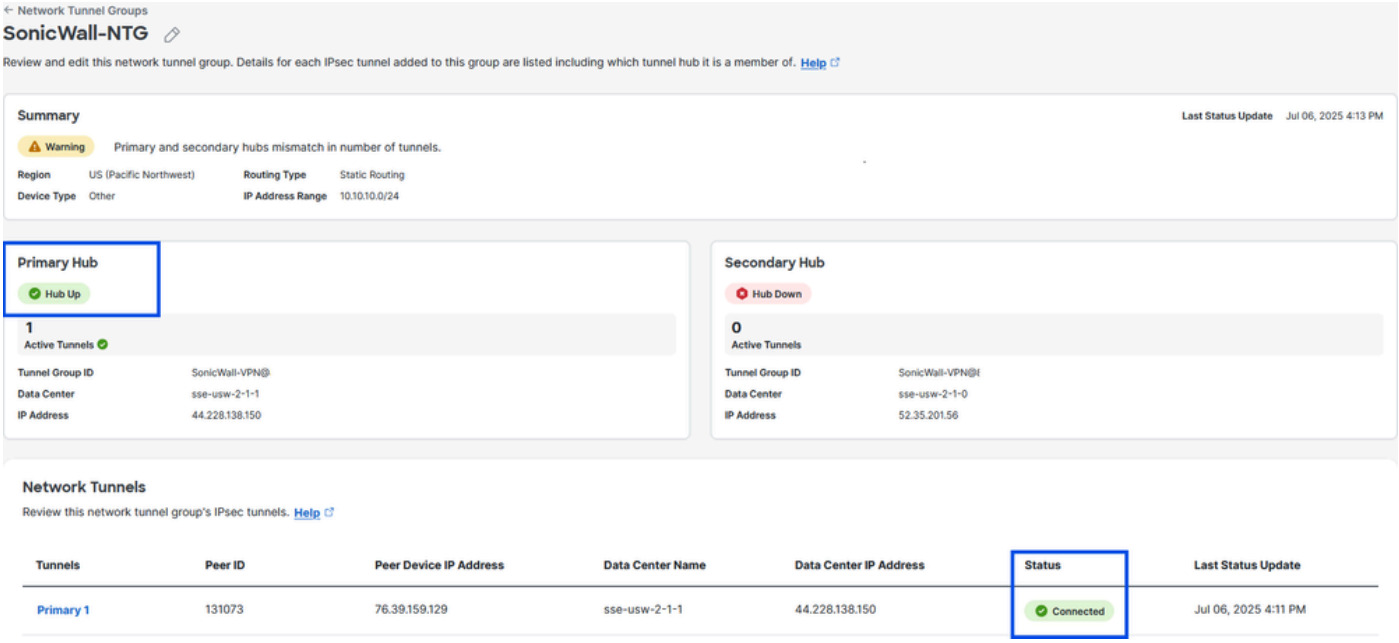
- 单击+Add



Sonicwall — 访问规则

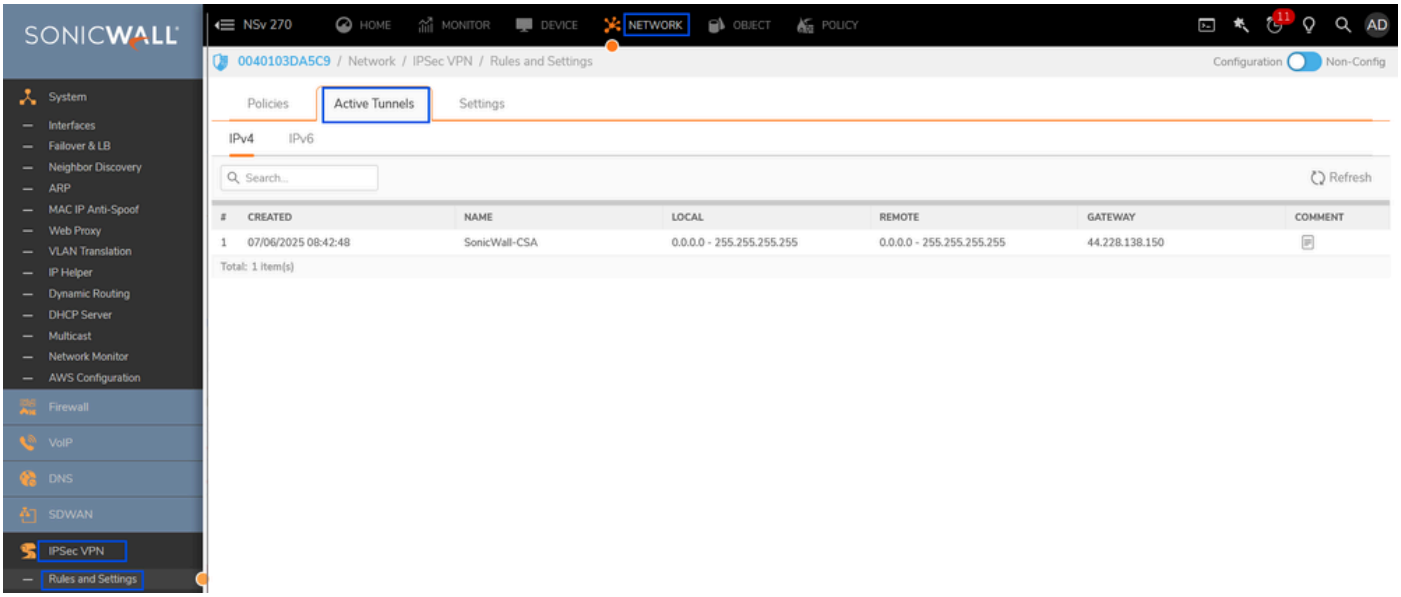
验证

- 安全访问上的隧道状态



安全访问 — 网络隧道组 — VPN状态

- Sonicwall防火墙上的隧道状态



Sonicwall - IPSec VPN状态

您可以执行相同的过程来配置安全访问辅助数据中心和Sonicwall之间的隧道

现在，安全访问和Sonicwall上的隧道为UP，您可以通过RA-VPN、基于浏览器的ZTA或安全访问控制面板上的基于客户端的ZTA继续配置对专用资源的访问

故障排除

用户 PC

- 验证用户是否能够成功连接/注册到RAVPN/ZTNA。如果不是，请进一步排除控制平面连接失败的原因。
- 验证用户尝试访问的网络是否应该通过RAVPN隧道或ZTNA访问。如果不是，请验证头端上的配置。

安全访问

- 验证RAVPN连接配置文件上的流量引导配置，以确认目标网络已配置为通过隧道发送到安全访问。
- 验证私有资源是否定义为具有有效协议/端口，并检查ZTNA/RAVPN连接机制。
- 验证Access-policy已配置为允许RAVPN/ZTNA用户访问私有资源网络及其放置的顺序为没有其他规则优先阻止流量。
- 验证IPSec隧道是否为UP且安全访问显示通过静态路由的有效客户端路由（包括用户尝试访问的私有资源）。

Sonicwall

- 验证IPSec隧道是否启用（IKE和IPSec SA）。
- 验证客户端路由或路由是否正确通告。
- 通过在Sonicwall上捕获数据包，验证从RAVPN/ZTNA用户发往Sonicwall后私有资源的流量源是否通过隧道到达Sonicwall防火墙。
- 验证流量是否到达私有资源并响应回RAVPN/ZTNA客户端。如果是，请验证这些数据包是否到达Sonicall X0(LAN)接口。
- 验证Sonicwall是否通过IPSec隧道将返回流量转发到安全访问。

相关信息

- 思科技术支持和下载
- 思科安全访问帮助中心
- 零信任访问模块
- 对安全访问错误“注册服务未响应”进行故障排除。联系您的IT服务中心”

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。