使用防御性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

配置

- 在安全访问中配置VPN
  - 隧道数据
- 配置VPN站点到防御工事上的站点
  - 网络
  - 身份验证
  - 第1阶段建议
  - 第2阶段建议
- 配置策略路由

验证

简介

本文档介绍如何使用Fortigate防火墙配置安全访问。

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：

- Fortigate 7.4.x版本防火墙
- 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：

- Fortigate 7.4.x版本防火墙
- 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



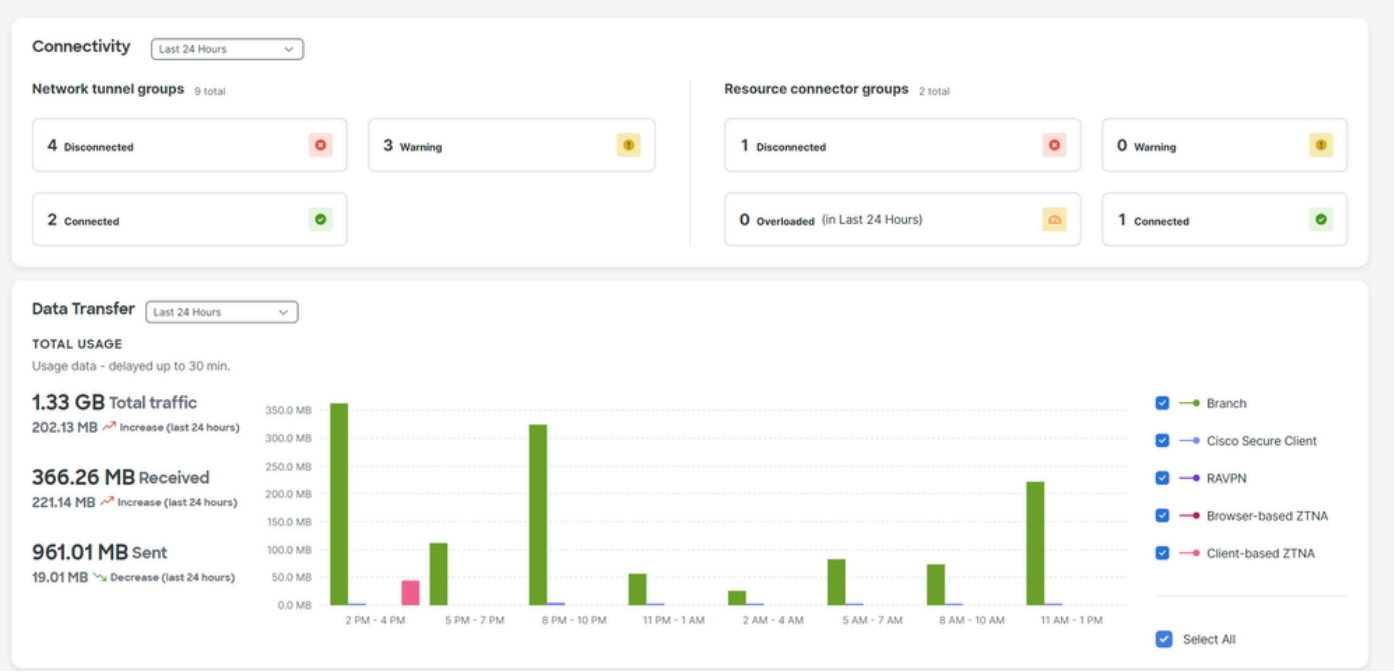
思科设计了安全访问(Secure Access)，用于保护和提供对内部和基于云的私有应用的访问。它还可以保护从网络到Internet的连接。这通过实施多种安全方法和层来实现，所有这些方法都旨在保留通

过云访问的信息。

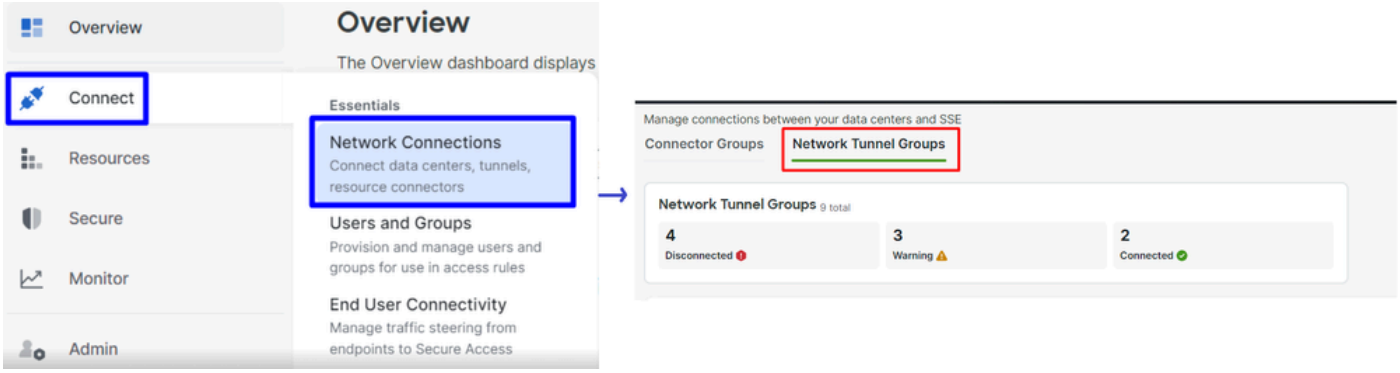
配置

在安全访问中配置VPN

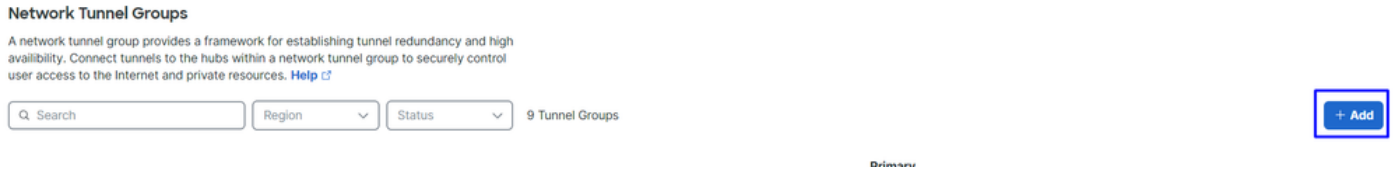
1.导航到Secure Access的管理面板。



2.单击Connect > Network Connections > Network Tunnels Groups。

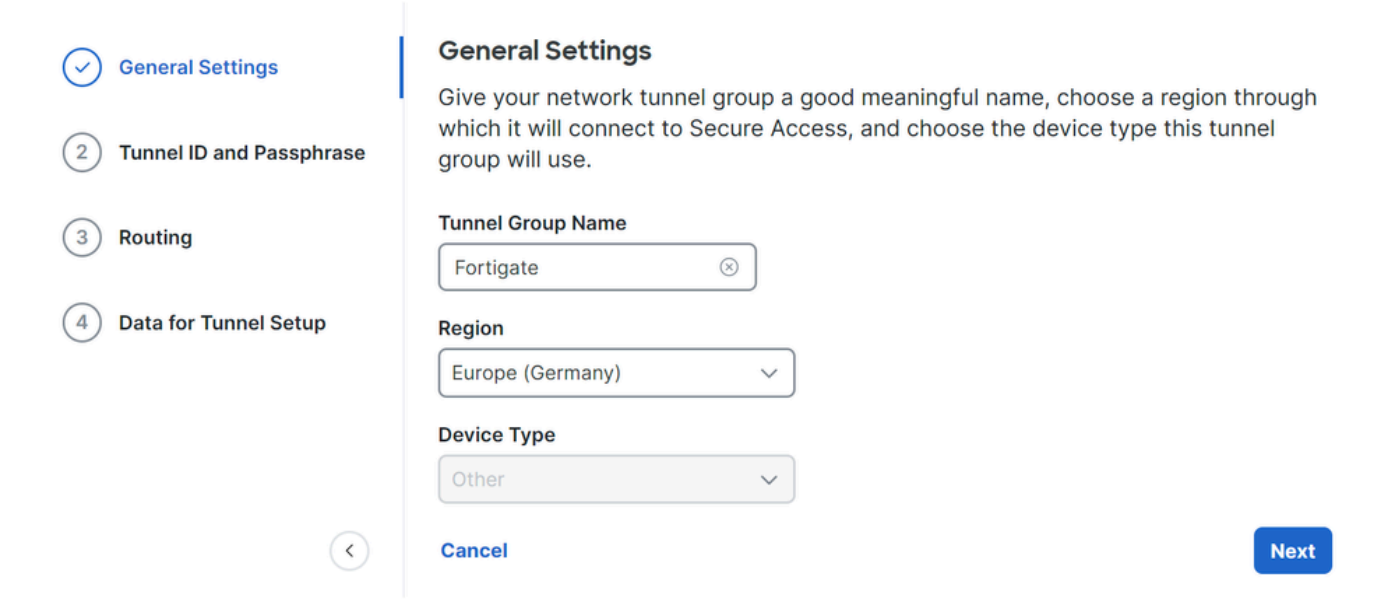


3.在Network Tunnel Groups下，单击+Add。



4.配置隧道组名称、区域和设备类型。

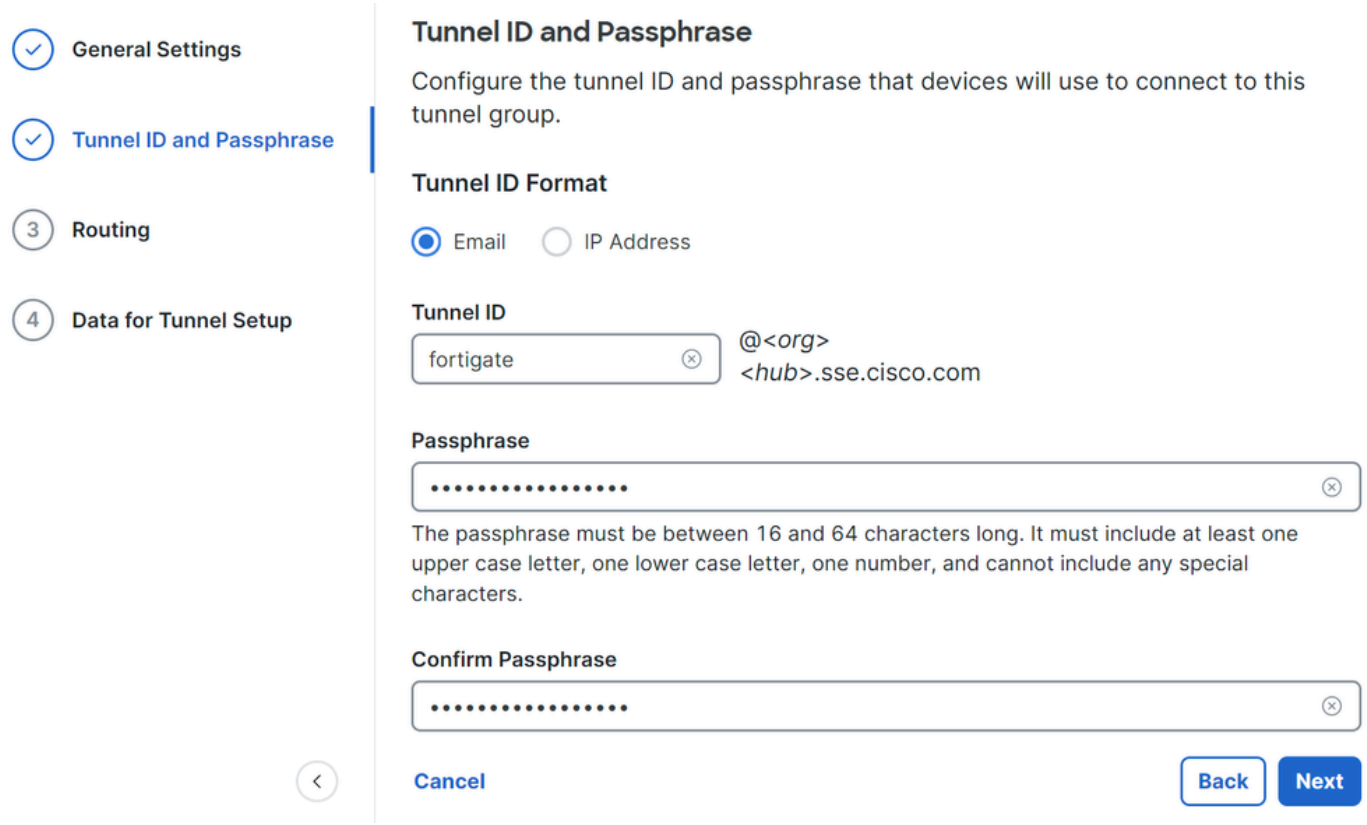
5.单击下一步。



注意：选择距离防火墙位置最近的区域。

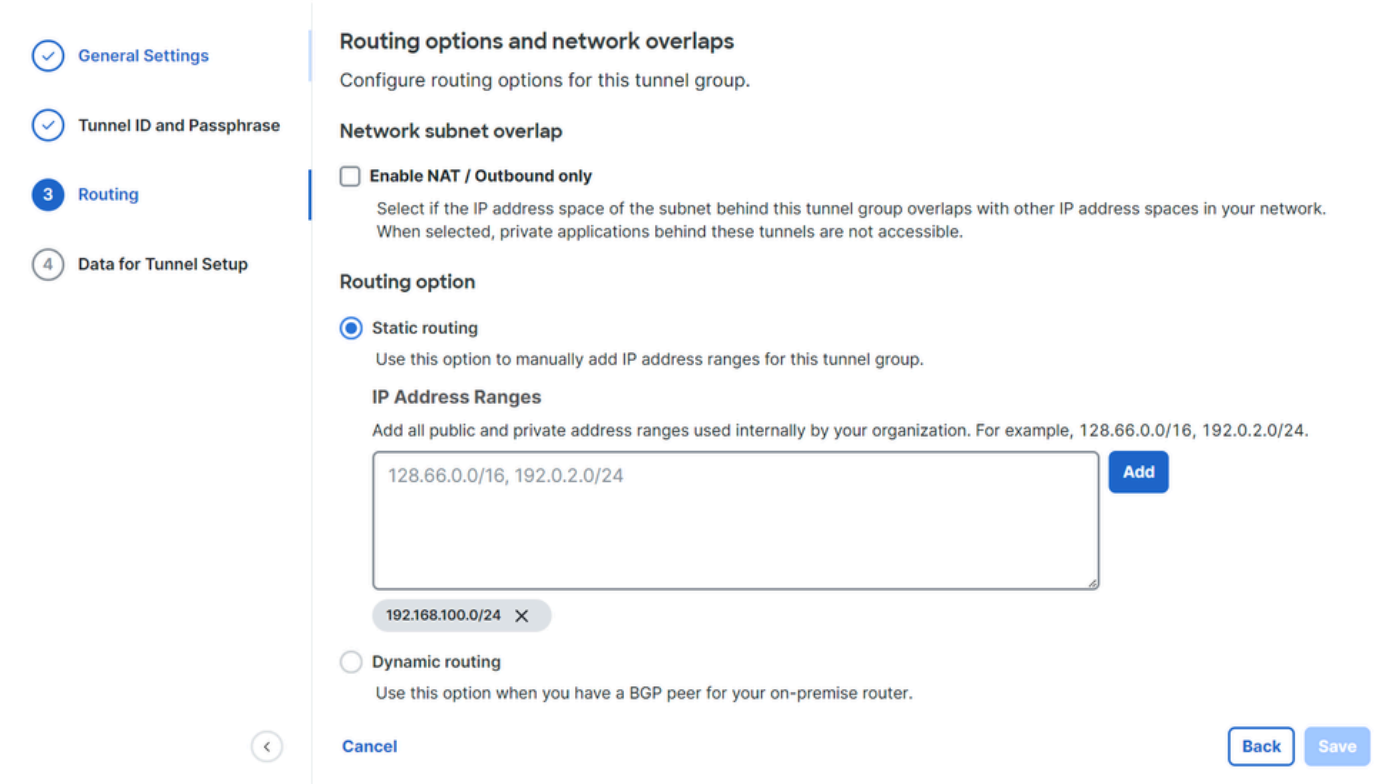
6.配置隧道ID格式和口令。

7.单击下一步。



8.配置在网络上配置的IP地址范围或主机，并希望通过安全访问传递流量。

9.单击保存。



10.保存后，将显示隧道上的信息。保存此信息以供下一步使用；配置VPN站点到防御工事上的站点。

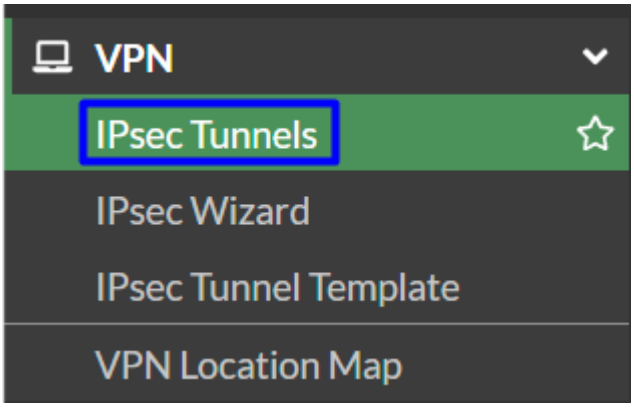
隧道数据



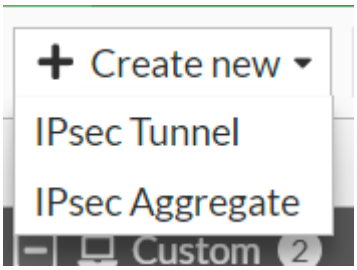
配置VPN站点到防御工事上的站点

1.导航到防御工事控制面板。

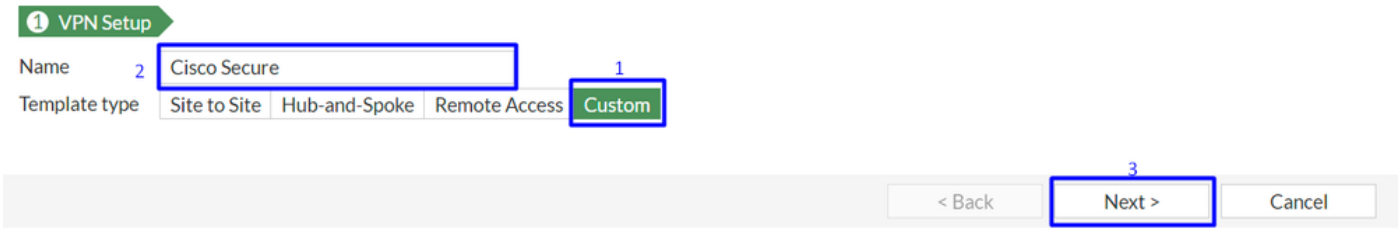
2.单击 VPN > IPsec Tunnels.



3.单击 Create New > IPsec **Tunnels**.

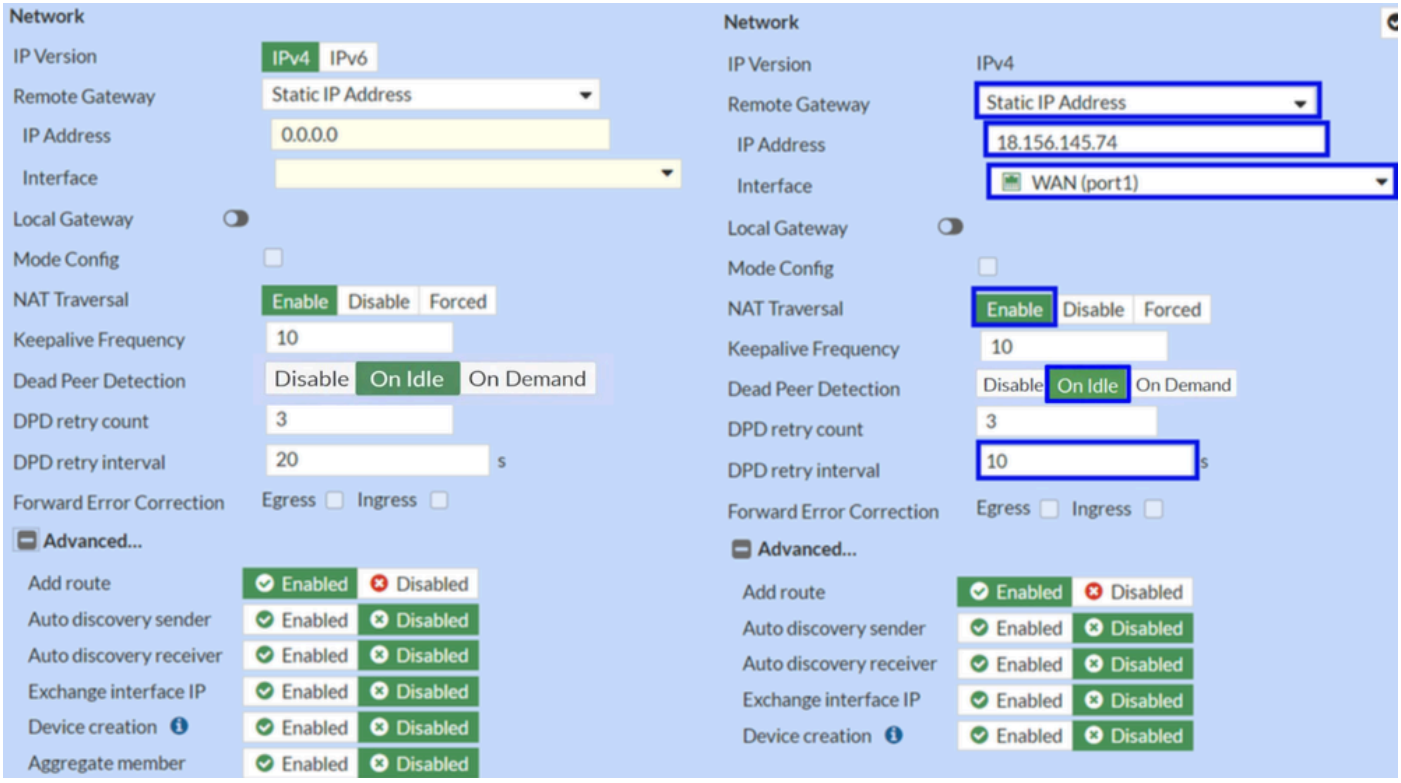


4.单击Custom，配置Name，然后单击Next。



在下一幅图像中，您可以看到如何为配置设Network置。

网络

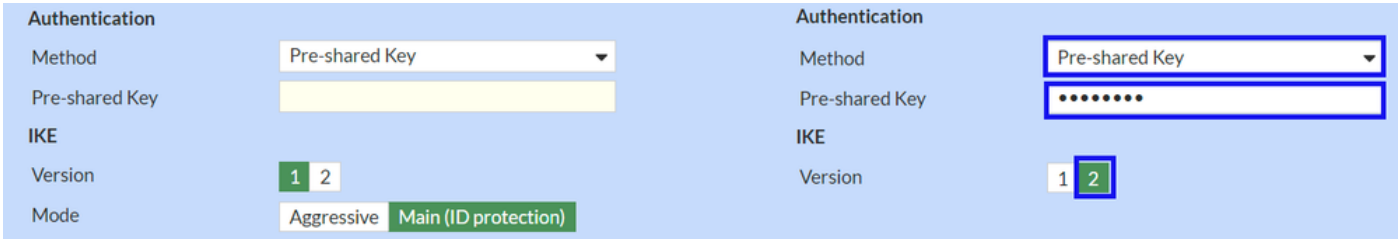


网络

- IP版本:IPv4
- 远程网关:静态 IP 地址
- IP Address:使用隧道数据中提供的主要IP数据中心IP地址的IP地址
- 接口:选择您计划用于建立隧道的WAN接口
- 本地网关:默认情况下禁用
- 模式配置:默认情况下禁用
- NAT穿越:enable
- 保持连接频率：10
- 失效对等项检测:空闲时
- DPD重试计数：3
- DPD重试间隔:10
- 前向纠错:不选中任何复选框
- 高级……:有关配置步骤，请参阅第2阶段

现在，配置IKE**Authentication**。

身份验证

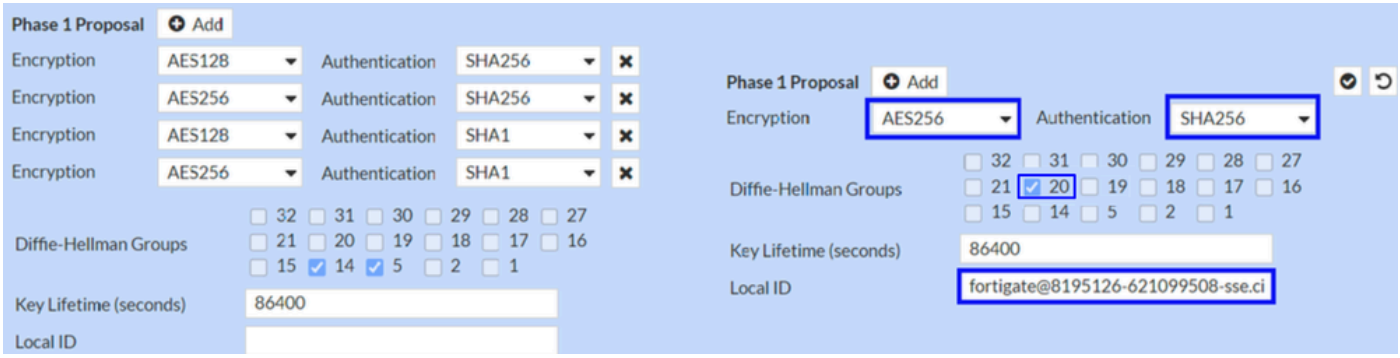


- 身份验证
  - 方法:预共享密钥作为默认值
  - 预共享密钥：使用隧道数据步骤中提供的密码
- IKE
  - 版本:选择版本2

注意：安全访问仅支持IKEv2。

接下来，配置**Phase 1 Proposal**。

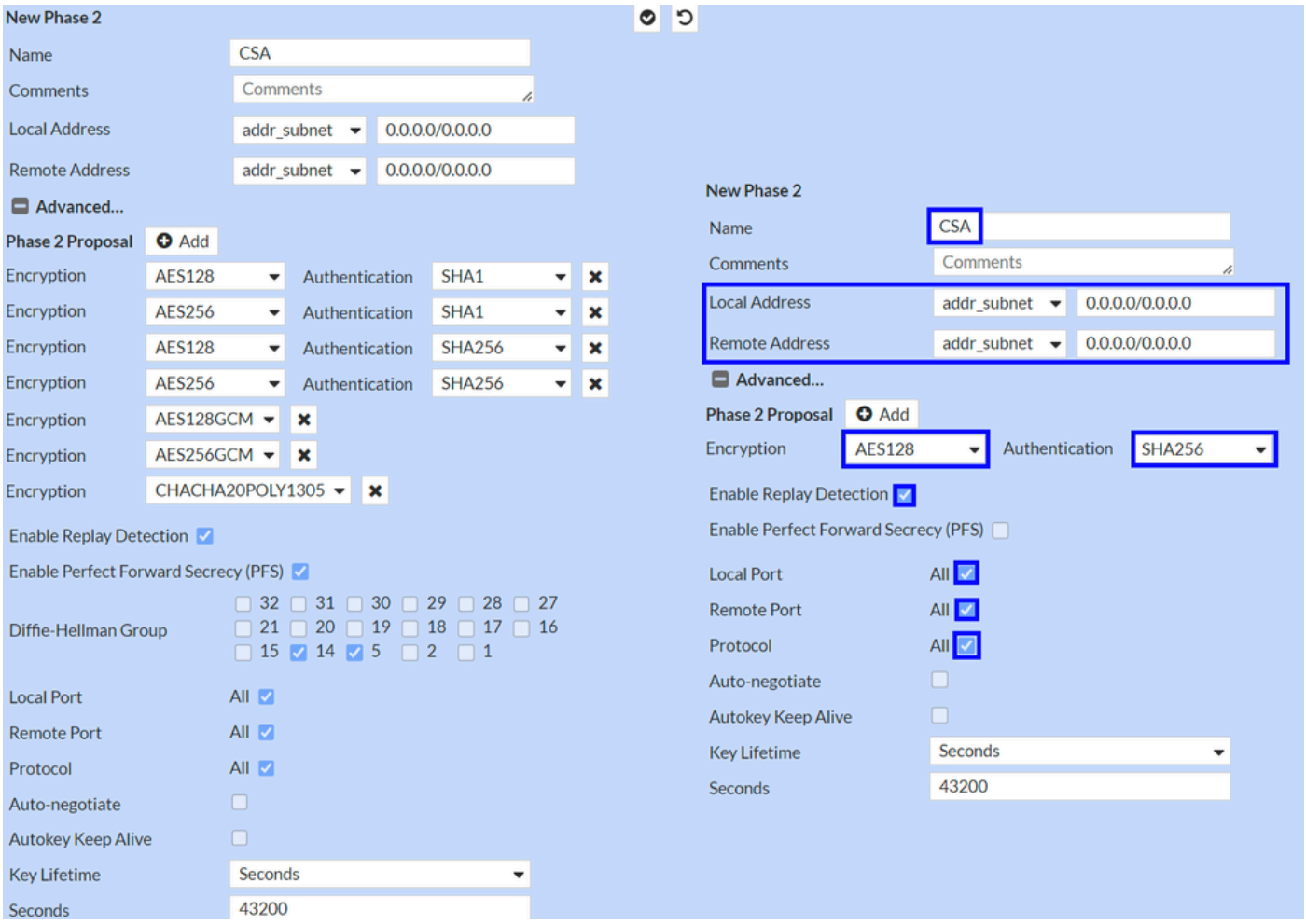
第1阶段建议



- 第1阶段建议
  - 加密 :选择AES256
  - 身份验证:选择SHA256
  - Diffie-Hellman组:仅选择20，如果选择多个选项，您以后可能会遇到问题
  - 密钥生存时间（秒）:86400为默认值
  - 本地ID:使用Tunnel Data步骤中给出的主隧道ID

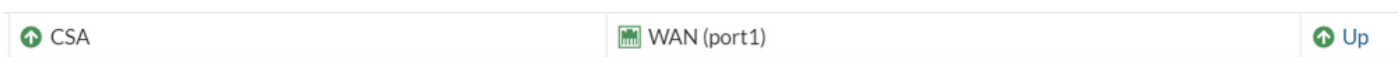
现在配置第2阶段建议。

第2阶段建议



- 新阶段2
  - 名称：保留为默认值（此值与您的VPN连接名称匹配）
  - 本地地址:保留默认值(0.0.0.0/0.0.0.0)
  - 远程地址：默认为(0.0.0.0/0.0.0.0)
- 高级
  - 加密 :选择AES128
  - 身份验证:选择SHA256
  - 启用重播检测:保留为默认值（启用）
  - 启用完全向前保密(PFS) 取消选中复选框
  - 本地端口：保留为默认值（启用）
  - 远程端口:保留为默认值（启用）
  - 协议：保留为默认值（启用）
  - 自动协商：保留为默认值（未标记）
  - Auto-key Keep Alive：保留为默认值（未标记）
  - 密钥生命期:保留为默认值（秒）
  - 秒：保留默认值(43200)

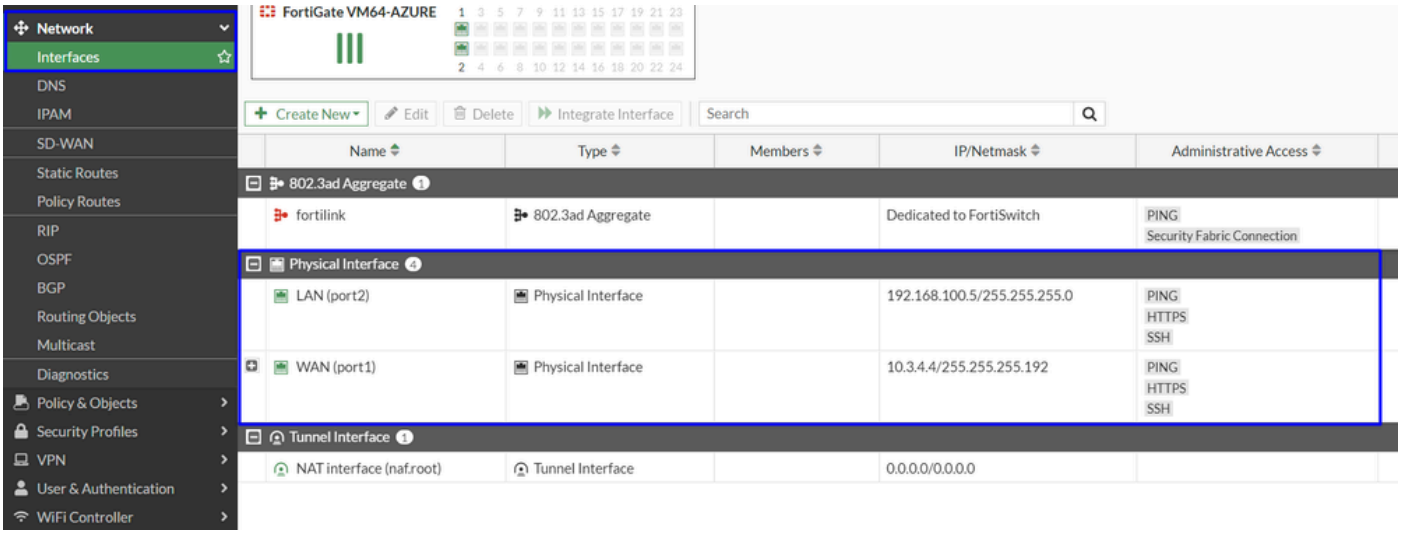
然后，单击OK。您将使用安全访问建立VPN，您可以继续执行下一步；配置隧道接口。



配置隧道接口

创建隧道后，新接口将显示在您用作WAN接口与安全访问通信的端口后面。

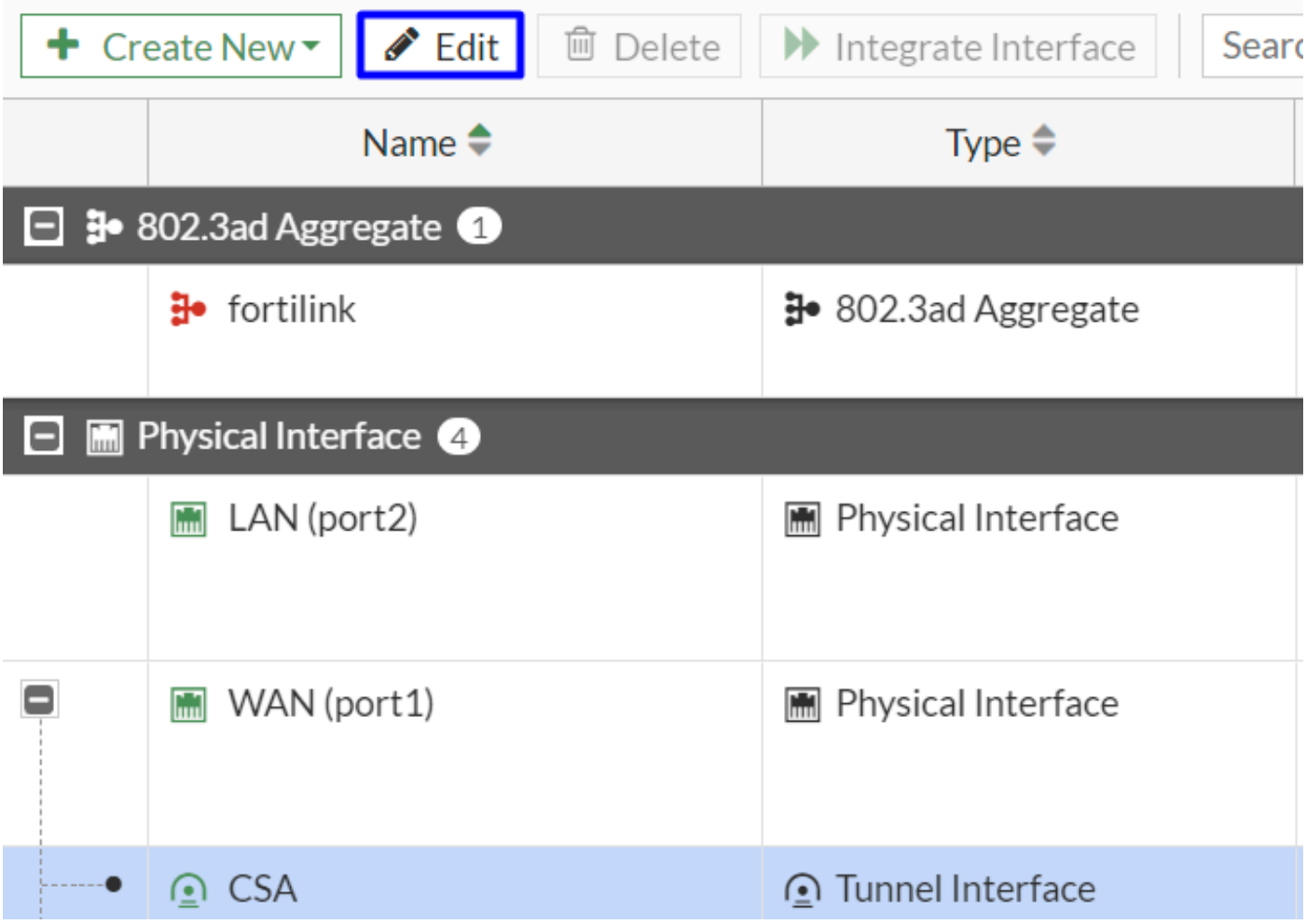
1.要检查此项，请导航至**Network** > **Interfaces**此处。



2.扩展用于与安全访问通信的端口；在本例中是接**WAN**口。



3.单击Tunnel Interface，然后单击Edit。

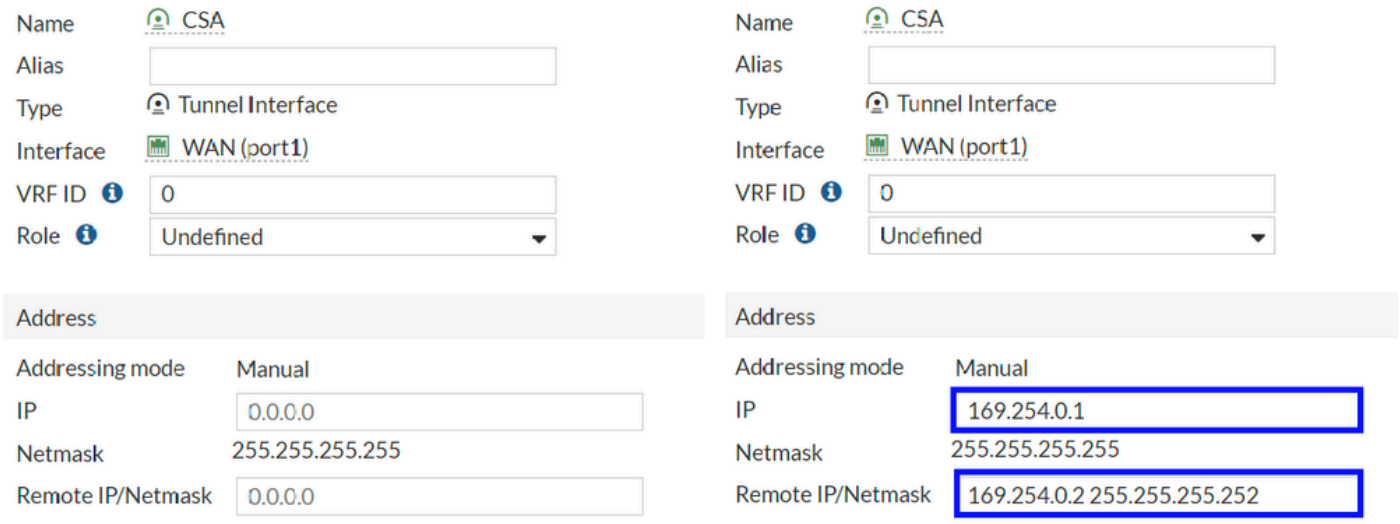


4.请参阅映像以配置设置。

接口配置

- IP :配置不在网络中的不可路由IP（例如，169.254.0.1）。
- 远程IP/网络掩码:将远程IP配置为接口IP的下一个IP，网络掩码为30（例如，169.254.0.2 255.255.255.252）。

5.单击以OK保存配置设置，然后继续执行下一步；配置策略路由（基于源的路由）。

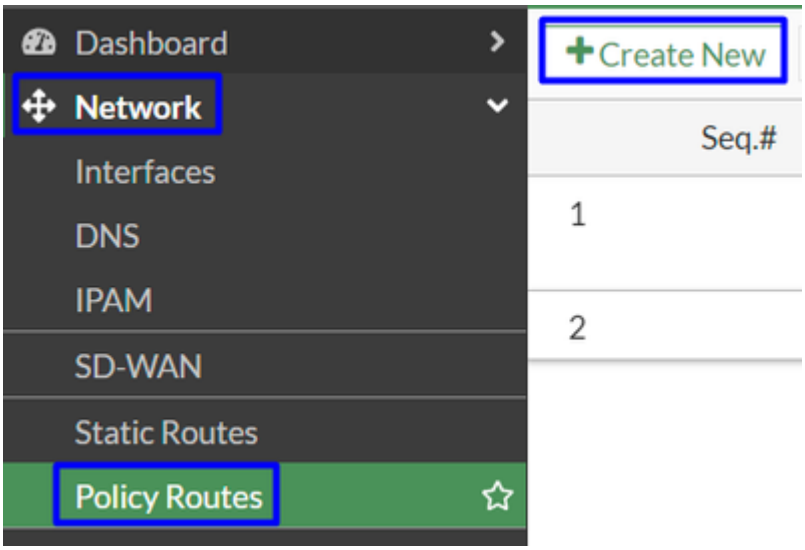


警告：完成后，配置FortiGate防火墙策略以允许从您的设备到安全访问以及从安全访问到目标网络的流量。

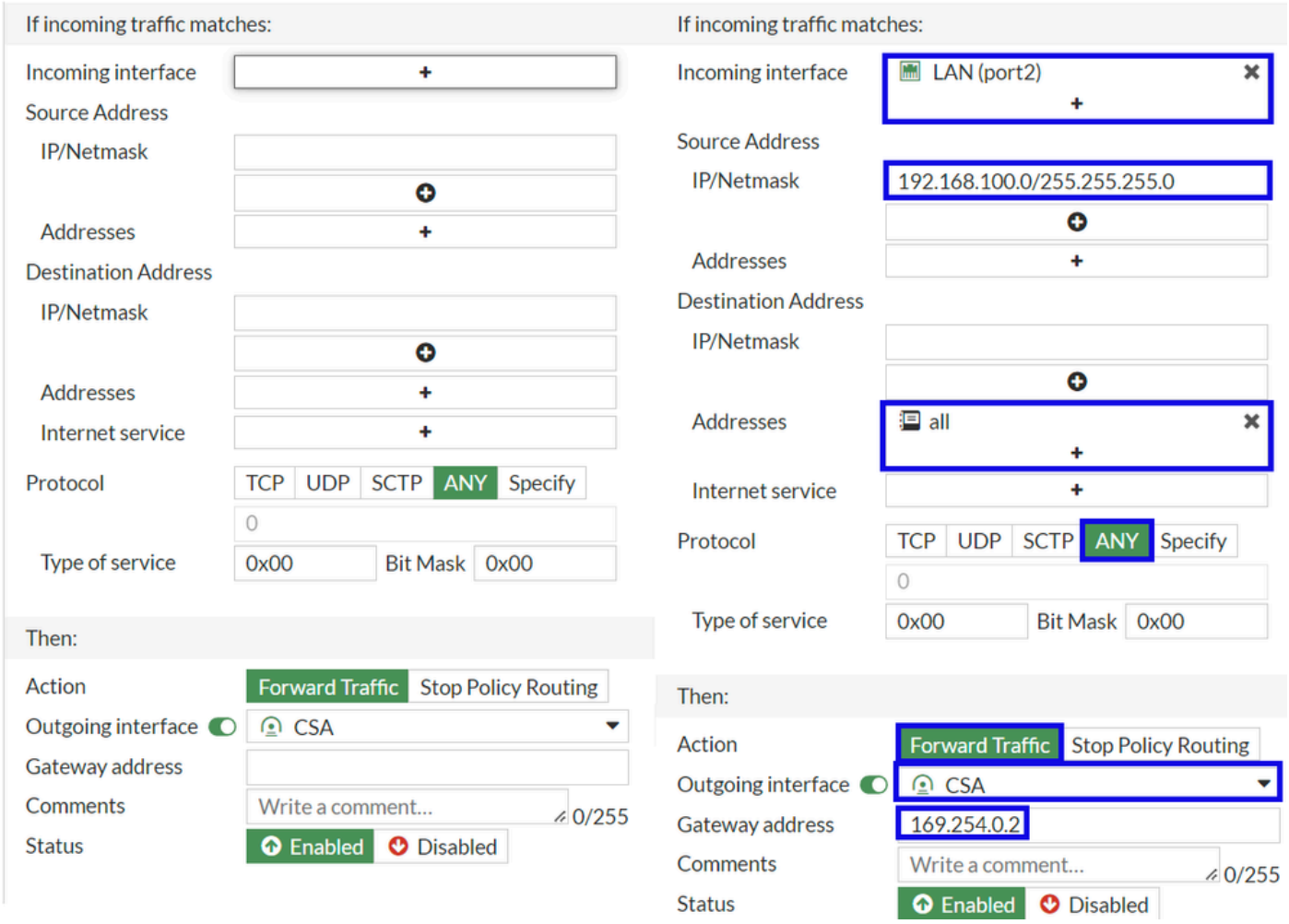
配置策略路由

此时，您已经将VPN配置并设置为安全访问。现在，您必须将流量重新路由到Secure Access，以保护您的流量或对FortiGate防火墙后的专用应用的访问。

1.导航至 Network > Policy **Routes**.



2.配置策略。



- 如果传入流量匹配:
  - 传入接口:选择要将流量重新路由到安全访问（流量来源）的接口。
- 源地址
  - IP/网络掩码:如果仅路由接口的子网，请使用此选项。
  - 地址:如果创建了对象，并且流量的源来自多个接口和多个子网，请使用此选项。
- 目的地址
  - 地址:如果要保护互联网流量，请选择all。如果要进行私有访问，必须添加VPN配置文件IP池和CGNAT范围100.64.0.0/10。
  - 协议：选择ANY。
- 然后
  - 操作：选择转发流量
- 传出接口:选择您在配置隧道接口步骤中修改的Tunnel Interface。
- 网关地址:配置在RemoteIPetmask步骤中配置的远程IP。
- 状态:选择Enabled。

3.单击OK保存配置设置。验证流向设备的流量是否已重新路由到安全访问。

验证

要验证流量是否从重路由到安全访问，您有两个选项：您可以在internet上检查您的公有IP，也可以使用curl运行命令：

```
C:\Windows\system32>curl ipinfo.io
{
  "ip": "151.186.197.1",
  "city": "Frankfurt am Main",
  "region": "Hesse",
  "country": "DE",
  "loc": "50.1112,8.6831",
  "org": "AS16509 Amazon.com, Inc.",
  "postal": "60311",
  "timezone": "Europe/Berlin",
  "readme": "https://ipinfo.io/missingauth"
}
```

您可以查看流量的公共范围是：

- 最小主机:151.186.176.1
- 最大主机：151.186.207.254



注意：这些IP可能会发生变化，思科可以在将来扩展此范围。

如果您看到您的公共IP发生更改，则表示您受到安全访问的保护。您可以在Secure Access控制面板上配置您的专用应用，以便从VPNaaS或ZTNA访问您的应用。

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）。