使用Fortigate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
- 在Fortigate上配置VPN站点到站点
  - 网络
  - 身份验证
  - 第1阶段建议
  - 第2阶段建议
- 配置隧道接口
- 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。

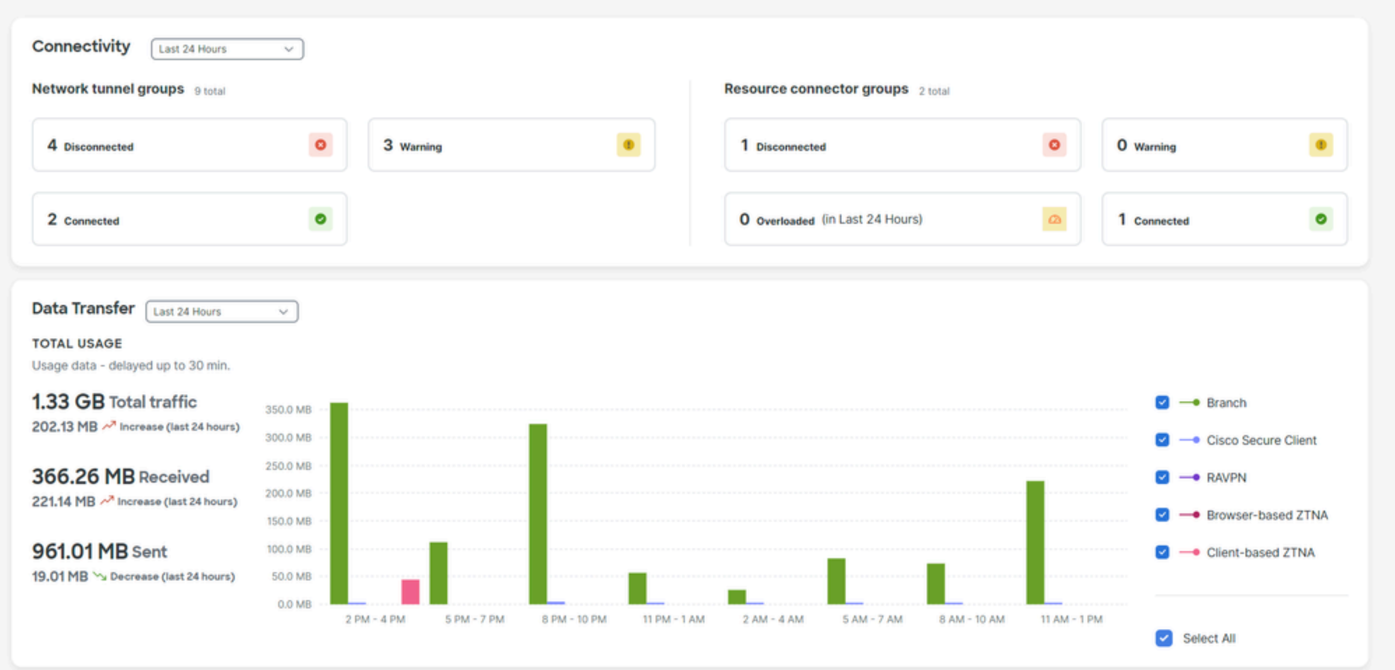
背景信息

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护通过云访问信息时所需的信息。

配置

在安全访问中配置VPN

导航到安全访问的管理面板。



Connectivity Last 24 Hours

Network tunnel groups 9 total

4 Disconnected

3 Warning

2 Connected

Resource connector groups 2 total

1 Disconnected

0 Warning

0 Overloaded (in Last 24 Hours)

1 Connected

Data Transfer Last 24 Hours

TOTAL USAGE

Usage data - delayed up to 30 min.

1.33 GB Total traffic

202.13 MB Increase (last 24 hours)

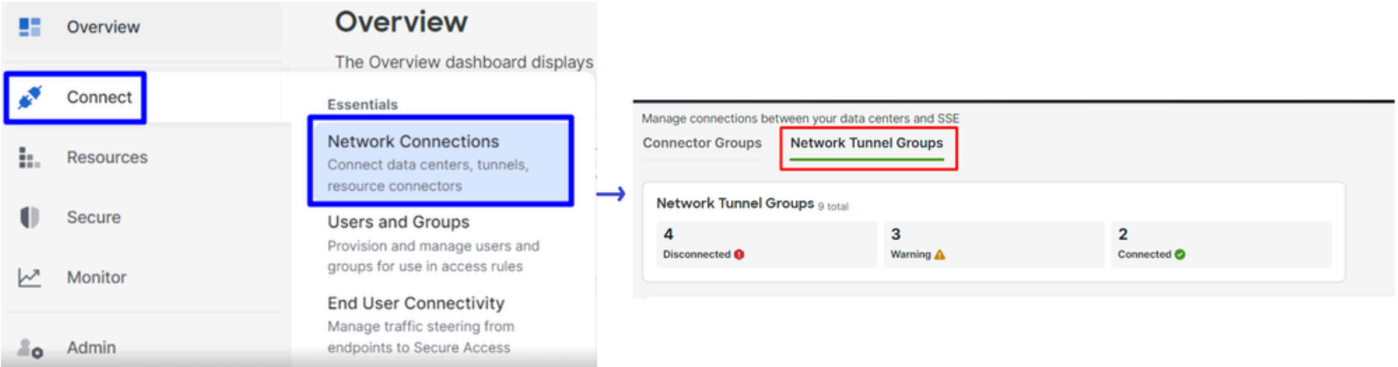
366.26 MB Received

221.14 MB Increase (last 24 hours)

961.01 MB Sent

19.01 MB Decrease (last 24 hours)

- 点击 Connect > Network Connections > Network Tunnels Groups



Overview

The Overview dashboard displays

Essentials

Network Connections

Connect data centers, tunnels, resource connectors

Users and Groups

Provision and manage users and groups for use in access rules

End User Connectivity

Manage traffic steering from endpoints to Secure Access

Manage connections between your data centers and SSE

Connector Groups | Network Tunnel Groups

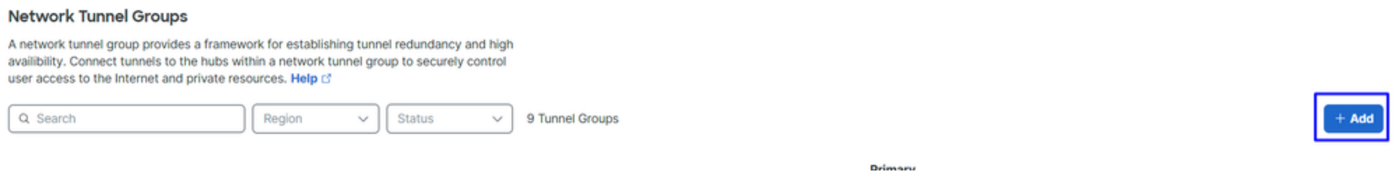
Network Tunnel Groups 9 total

4 Disconnected

3 Warning

2 Connected

- 在Network Tunnel Groups下单击 + Add

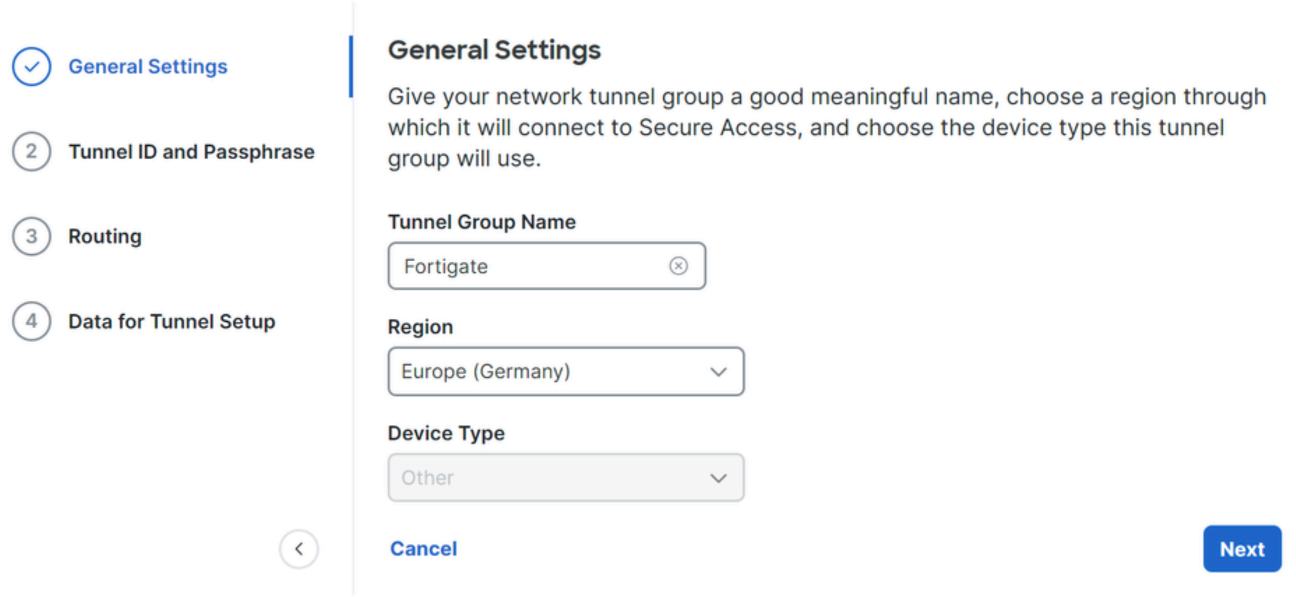


Network Tunnel Groups

A network tunnel group provides a framework for establishing tunnel redundancy and high availibility. Connect tunnels to the hubs within a network tunnel group to securely control user access to the Internet and private resources. Help

- 配置Tunnel Group Name、Region和 Device Type

- 点击 **Next**



General Settings

Give your network tunnel group a good meaningful name, choose a region through which it will connect to Secure Access, and choose the device type this tunnel group will use.

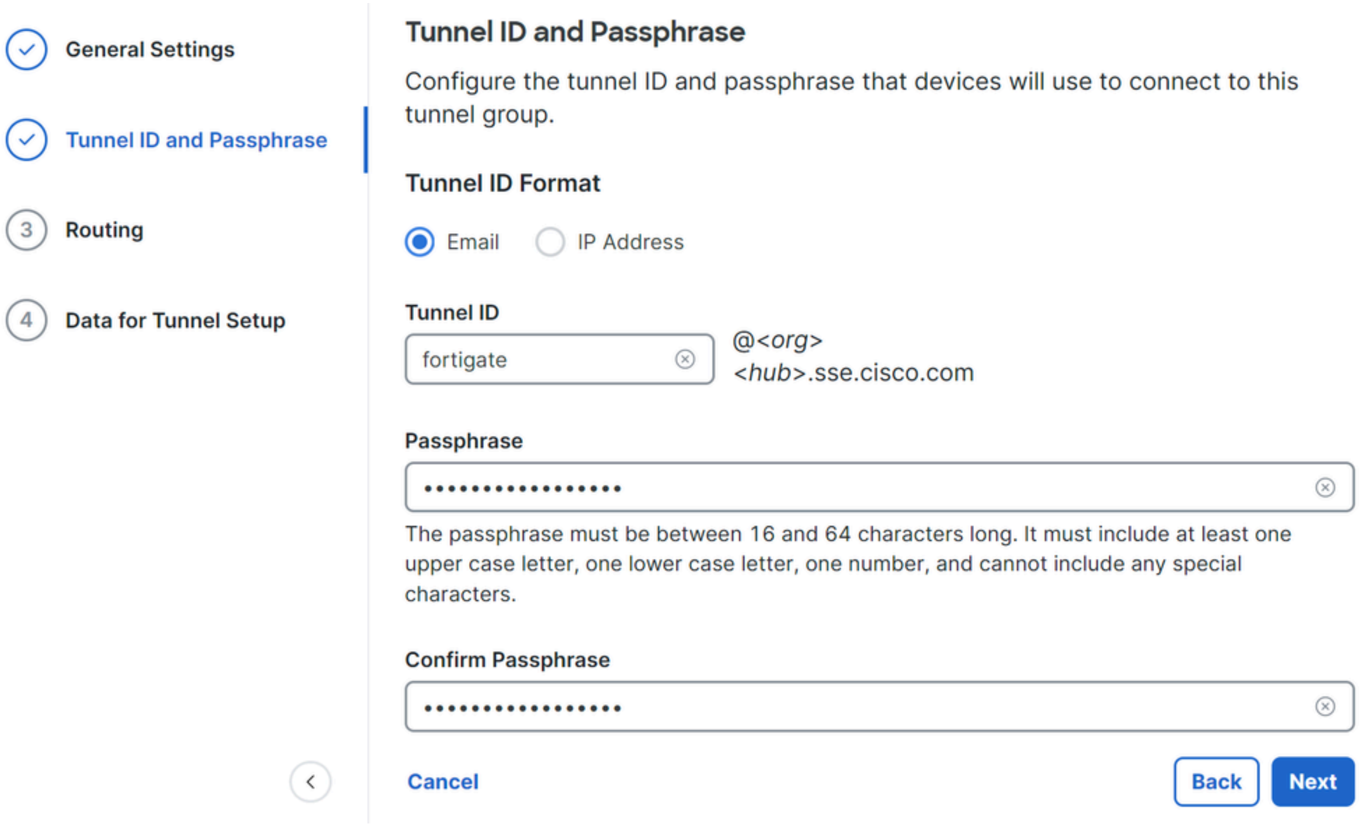
Tunnel Group Name: Fortigate

Region: Europe (Germany)

Device Type: Other

注意：选择距离防火墙位置最近的区域。

- 在路由器上配置Tunnel ID Format Passphrase
- 点击Next



Tunnel ID and Passphrase

Configure the tunnel ID and passphrase that devices will use to connect to this tunnel group.

Tunnel ID Format

● Email ○ IP Address

Tunnel ID

fortigate @<org><hub>.sse.cisco.com

Passphrase

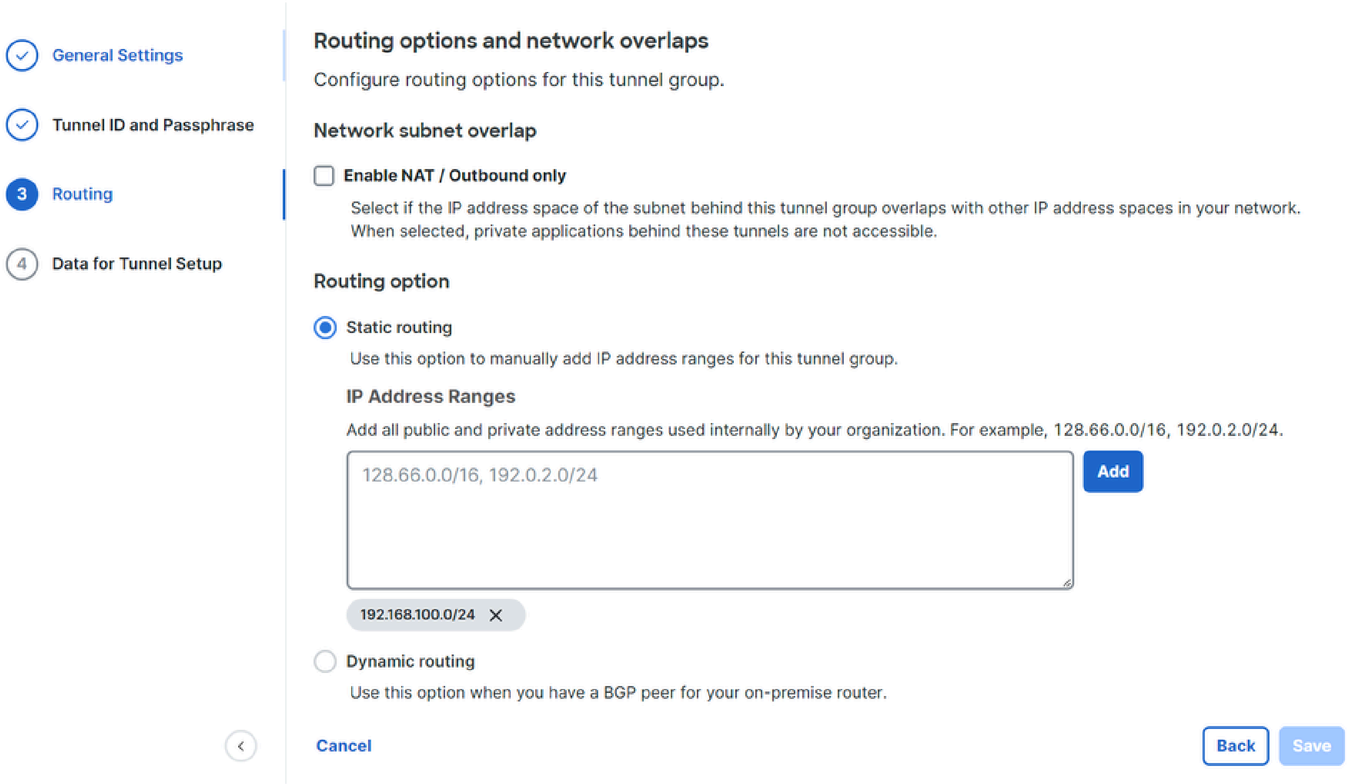
•••••••••••••••••

The passphrase must be between 16 and 64 characters long. It must include at least one upper case letter, one lower case letter, one number, and cannot include any special characters.

Confirm Passphrase

•••••••••••••••••

- 配置已在网络上配置并要通过安全访问传递流量的IP地址范围或主机
- 点击Save



Routing options and network overlaps

Configure routing options for this tunnel group.

Network subnet overlap

□ Enable NAT / Outbound only

Select if the IP address space of the subnet behind this tunnel group overlaps with other IP address spaces in your network. When selected, private applications behind these tunnels are not accessible.

Routing option

● Static routing

Use this option to manually add IP address ranges for this tunnel group.

IP Address Ranges

Add all public and private address ranges used internally by your organization. For example, 128.66.0.0/16, 192.0.2.0/24.

128.66.0.0/16, 192.0.2.0/24

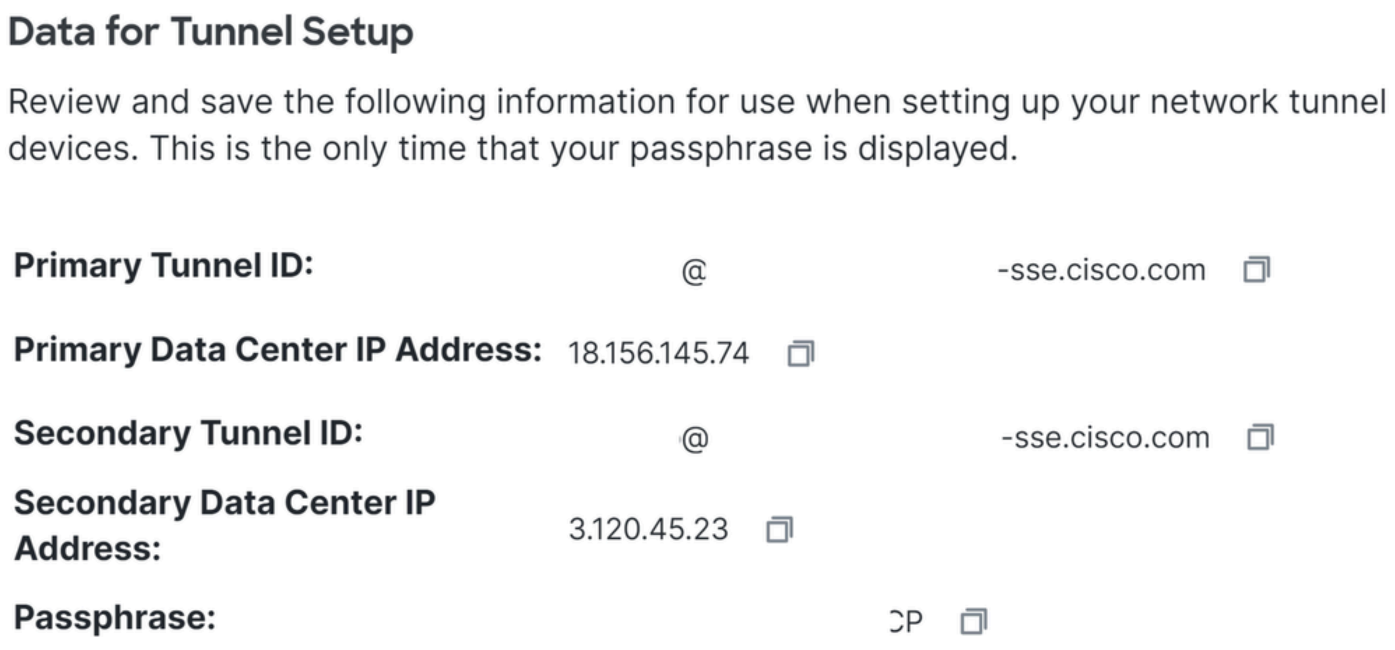
192.168.100.0/24

○ Dynamic routing

Use this option when you have a BGP peer for your on-premise router.

单击显示有Save 关隧道的信息后，请保存该信息以供下一步操作。 **Configure the VPN Site to Site on Fortigate**.

隧道数据



Data for Tunnel Setup

Review and save the following information for use when setting up your network tunnel devices. This is the only time that your passphrase is displayed.

Primary Tunnel ID: @ -sse.cisco.com

Primary Data Center IP Address: 18.156.145.74

Secondary Tunnel ID: @ -sse.cisco.com

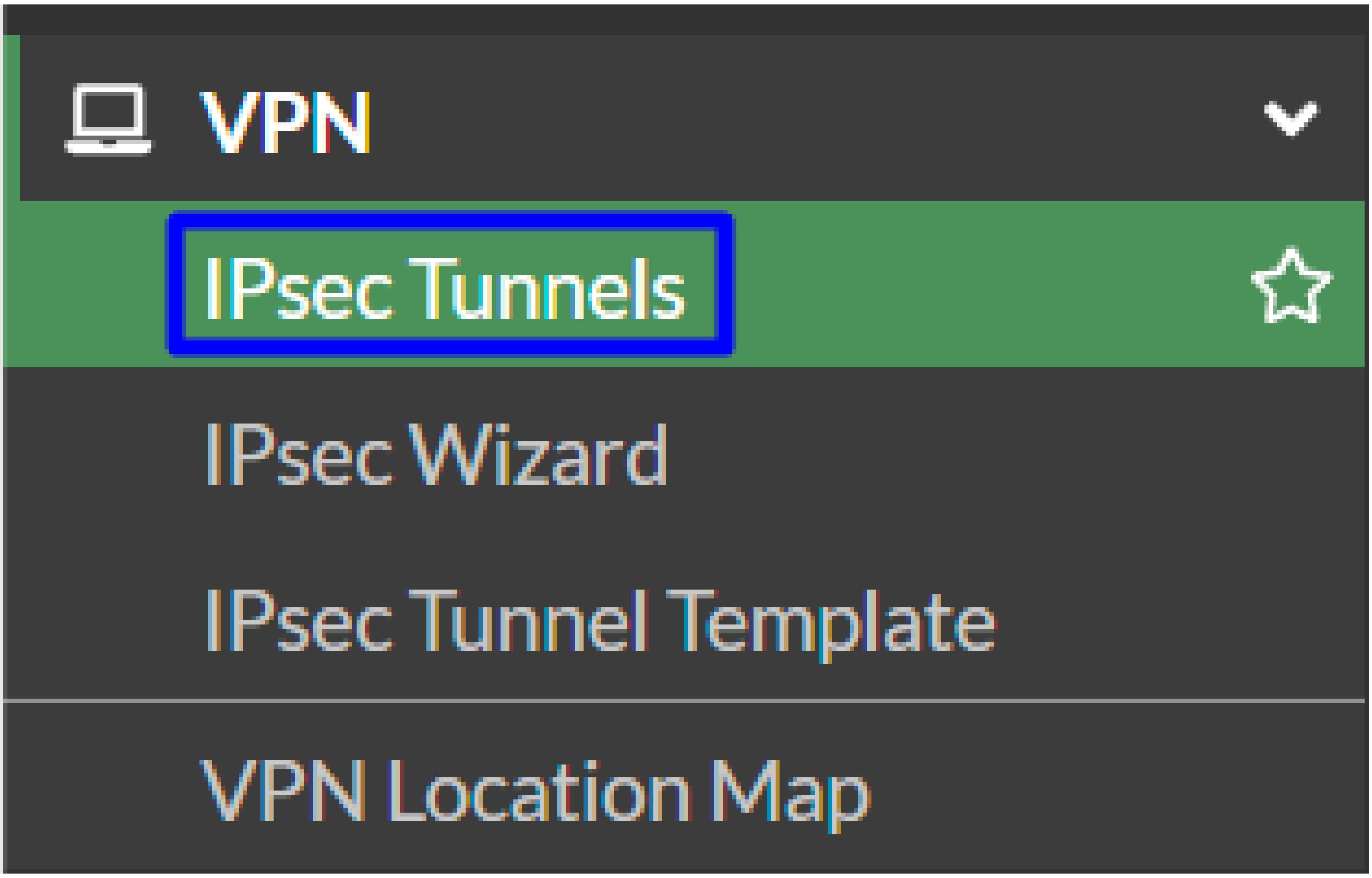
Secondary Data Center IP Address: 3.120.45.23

Passphrase: ɔP

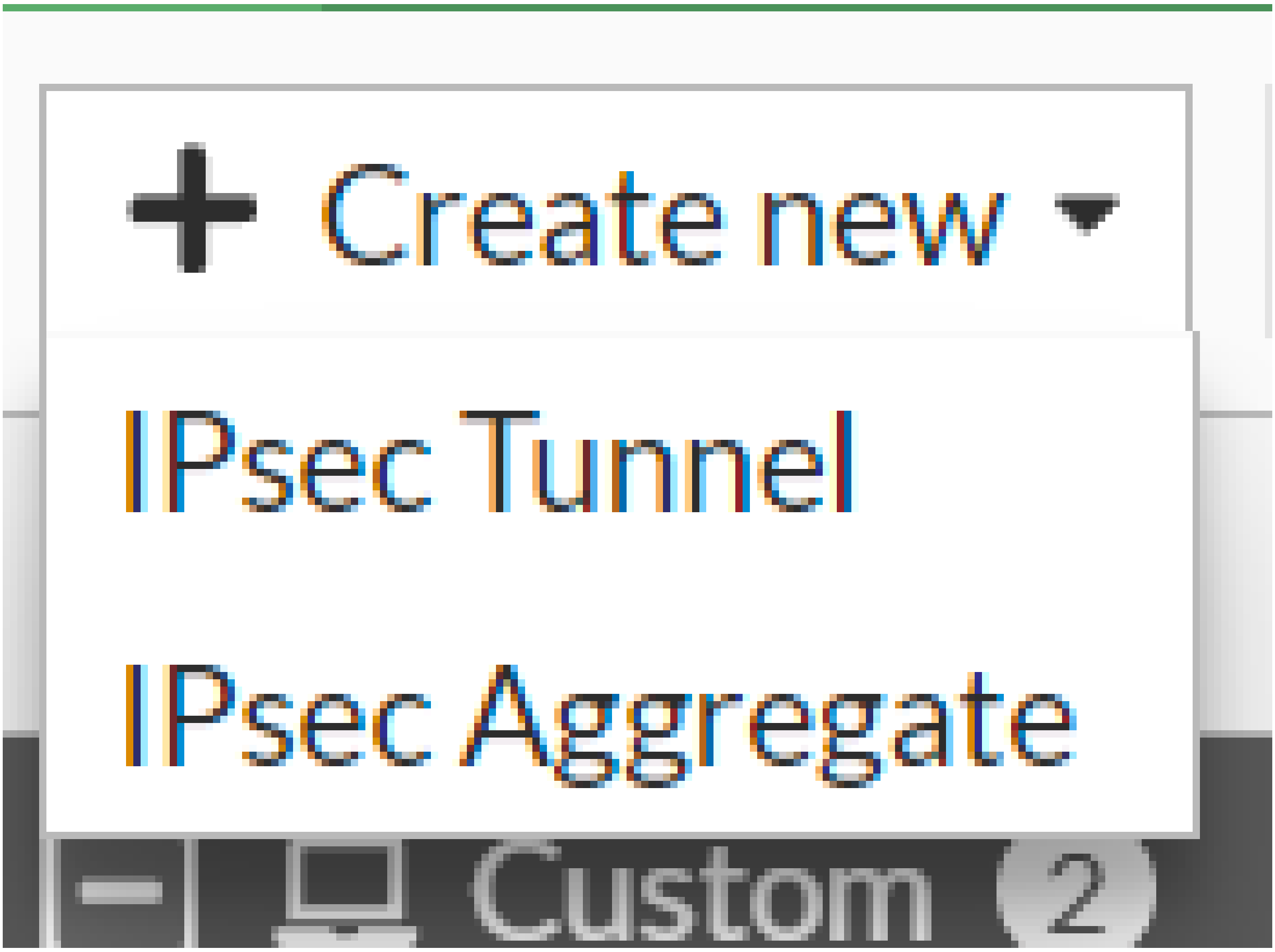
在Fortigate上配置VPN站点到站点

导航到您的Fortigate控制面板。

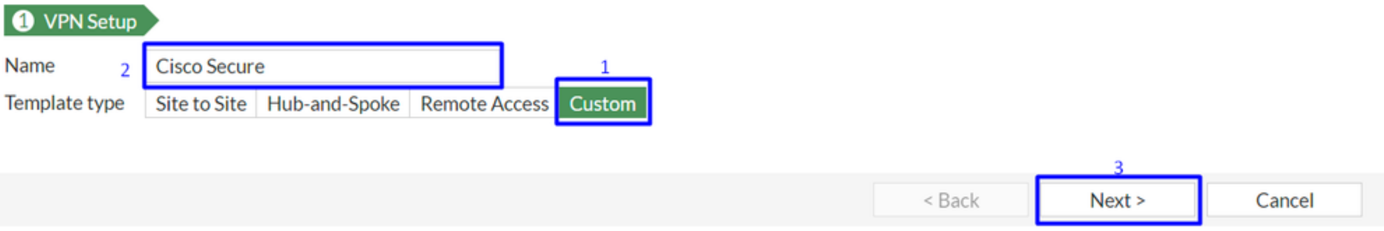
- 点击 VPN > IPsec Tunnels



- 点击 Create New > IPsec Tunnels



- 单击Custom、配置**Name** 并单击**Next**。

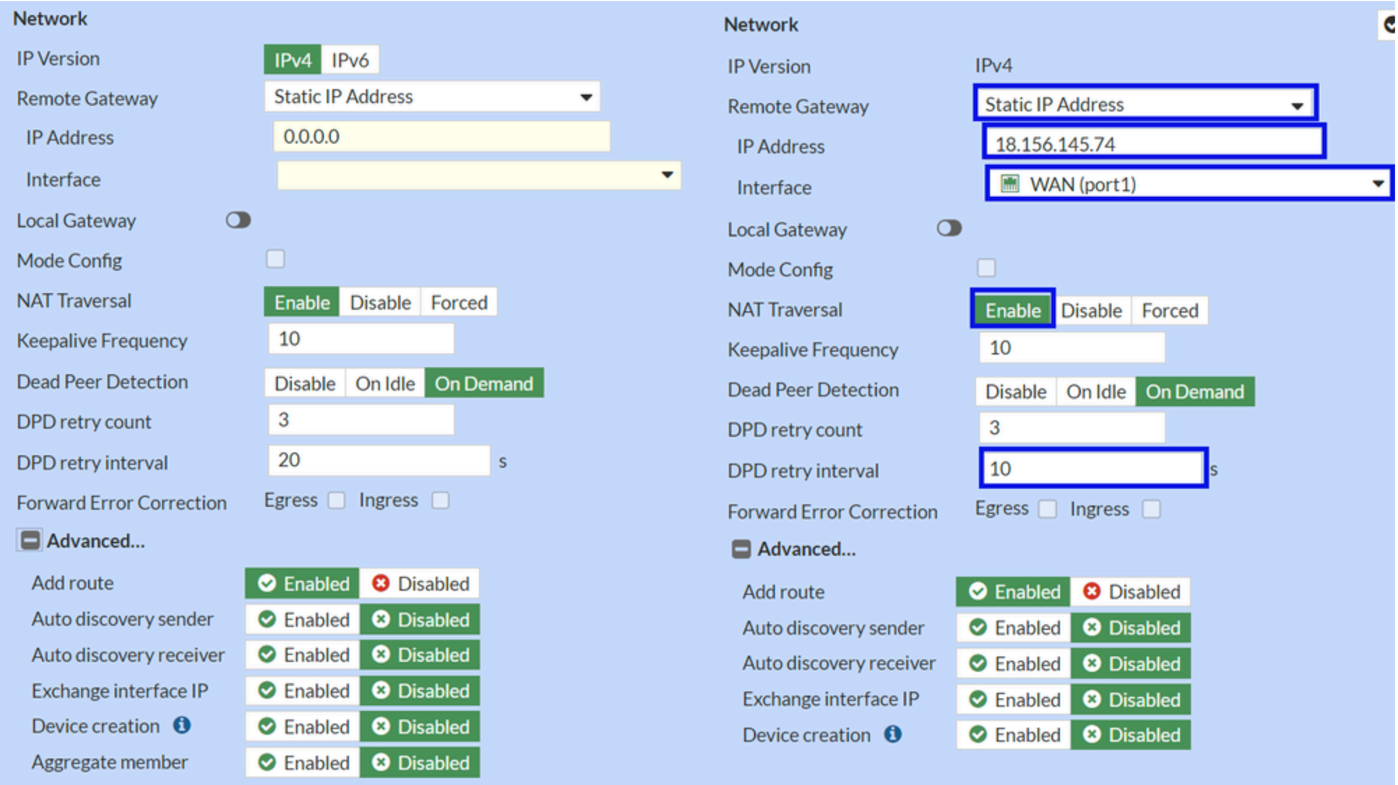


Name: Cisco Secure

Template type: Site to Site | Hub-and-Spoke | Remote Access | Custom

在下一张图中，您将看到需要如何配置**Network** 部件的设置。

网络



Network

IP Version: IPv4 | IPv6

Remote Gateway: Static IP Address

IP Address: 0.0.0.0

Interface:

Local Gateway

Mode Config □

NAT Traversal: Enable | Disable | Forced

Keepalive Frequency: 10

Dead Peer Detection: Disable | On Idle | On Demand

DPD retry count: 3

DPD retry interval: 20 s

Forward Error Correction: Egress □ Ingress □

Advanced...

Add route: Enabled | Disabled

Auto discovery sender: Enabled | Disabled

Auto discovery receiver: Enabled | Disabled

Exchange interface IP: Enabled | Disabled

Device creation: Enabled | Disabled

Aggregate member: Enabled | Disabled

Network

IP Version: IPv4

Remote Gateway: Static IP Address

IP Address: 18.156.145.74

Interface: WAN (port1)

Local Gateway

Mode Config □

NAT Traversal: Enable | Disable | Forced

Keepalive Frequency: 10

Dead Peer Detection: Disable | On Idle | On Demand

DPD retry count: 3

DPD retry interval: 10 s

Forward Error Correction: Egress □ Ingress □

Advanced...

Add route: Enabled | Disabled

Auto discovery sender: Enabled | Disabled

Auto discovery receiver: Enabled | Disabled

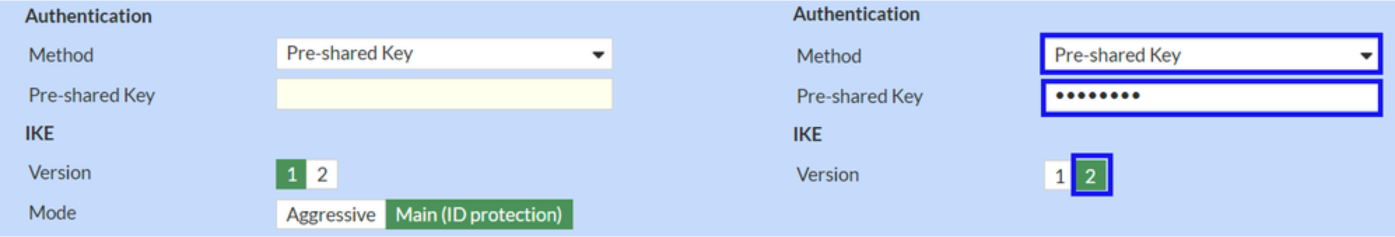
Exchange interface IP: Enabled | Disabled

Device creation: Enabled | Disabled

- Network
  - IP Version ： IPv4
    - **Remote Gateway** :静态 IP 地址
    - IP Address：使用隧道数据步骤Primary IP Datacenter IP Address,中给定的IP
    - **Interface** ：选择您计划用于建立隧道的WAN接口
    - **Local Gateway** ：禁用为默认值
    - **Mode Config** ：禁用为默认值
    - **NAT Traversal** :启用
    - **Keepalive Frequency** :10
    - Dead Peer Detection :按需
    - **DPD retry count** :3
    - **DPD retry interval** :10
    - **Forward Error Correction** ：请勿选中任何复选框。
    - **Advanced...**：将其配置为映像。

现在配置IKE **Authentication**。

身份验证



Authentication

Method	Pre-shared Key
Pre-shared Key	

IKE

Version	[✓ 1] 2
Mode	Aggressive [✓ Main (ID protection)]

Authentication

Method	Pre-shared Key
Pre-shared Key	••••••••

IKE

Version	1 [✓ 2]

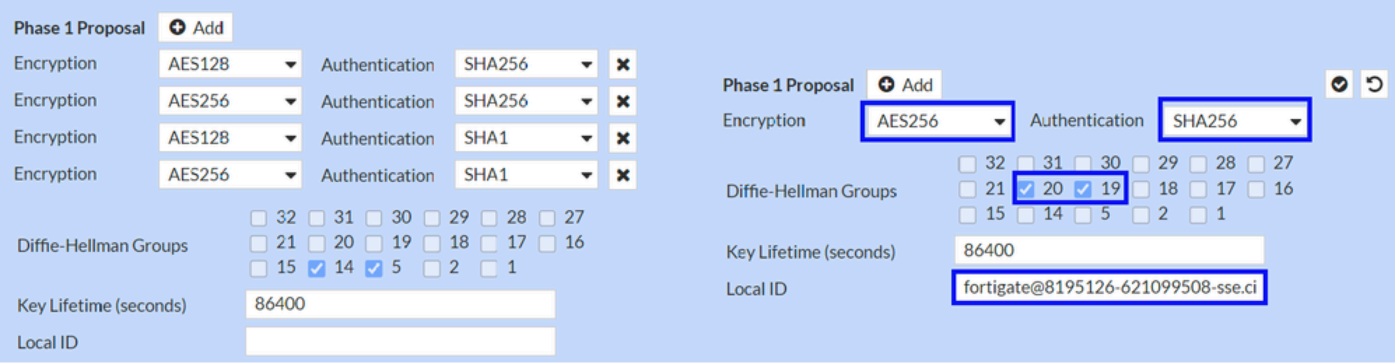
- **Authentication**
  - **Method** ：预共享密钥为默认值
    - **Pre-shared Key** ：使用隧道数据步骤中给定**Passphrase**的

- **IKE**
  - Version ：选择版本2。

注意：安全访问仅支持IKEv2

现在配置 **Phase 1 Proposal**。

第1阶段建议



Phase 1 Proposal ⊕ Add

Encryption	AES128	Authentication	SHA256	✖
Encryption	AES256	Authentication	SHA256	✖
Encryption	AES128	Authentication	SHA1	✖
Encryption	AES256	Authentication	SHA1	✖

Diffie-Hellman Groups
□ 32 □ 31 □ 30 □ 29 □ 28 □ 27
□ 21 □ 20 □ 19 □ 18 □ 17 □ 16
□ 15 ☑ 14 ☑ 5 □ 2 □ 1

Key Lifetime (seconds) 86400

Local ID

Phase 1 Proposal ⊕ Add

Encryption AES256 Authentication SHA256

Diffie-Hellman Groups
□ 32 □ 31 □ 30 □ 29 □ 28 □ 27
□ 21 ☑ 20 ☑ 19 □ 18 □ 17 □ 16
□ 15 □ 14 □ 5 □ 2 □ 1

Key Lifetime (seconds) 86400

Local ID fortigate@8195126-621099508-sse.ci

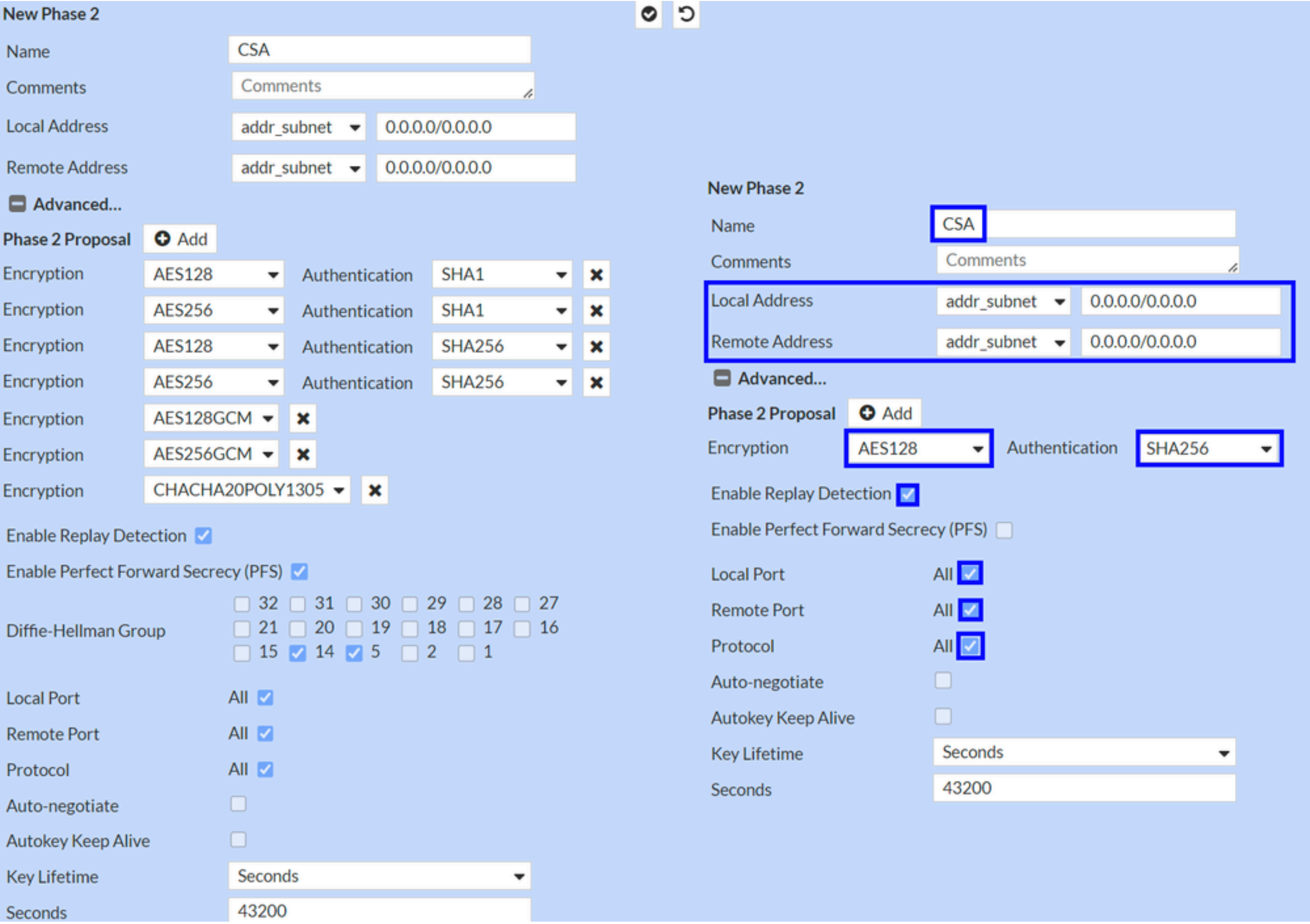
- Phase 1 Proposal

  - Encryption ：选择AES256

    - Authentication ：选择SHA256
    - Diffie-Hellman Groups ：选中框19和20
    - Key Lifetime (seconds) ：86400为默认值
    - Local ID ：使用隧道数据步骤中给定的 Primary Tunnel ID

现在配置 Phase 2 Proposal。

第2阶段建议



New Phase 2

Name	CSA
Comments	Comments
Local Address	addr_subnet ▾ 0.0.0.0/0.0.0.0
Remote Address	addr_subnet ▾ 0.0.0.0/0.0.0.0

Advanced...

Phase 2 Proposal ⊕ Add

Encryption	AES128 ▾	Authentication	SHA1 ▾ ✖
Encryption	AES256 ▾	Authentication	SHA1 ▾ ✖
Encryption	AES128 ▾	Authentication	SHA256 ▾ ✖
Encryption	AES256 ▾	Authentication	SHA256 ▾ ✖
Encryption	AES128GCM ▾ ✖		
Encryption	AES256GCM ▾ ✖		
Encryption	CHACHA20POLY1305 ▾ ✖		

Enable Replay Detection ☑

Enable Perfect Forward Secrecy (PFS) ☑

Diffie-Hellman Group
□ 32 □ 31 □ 30 □ 29 □ 28 □ 27
□ 21 □ 20 □ 19 □ 18 □ 17 □ 16
□ 15 ☑ 14 ☑ 5 □ 2 □ 1

Local Port	All ☑
Remote Port	All ☑
Protocol	All ☑
Auto-negotiate	□
Autokey Keep Alive	□
Key Lifetime	Seconds ▾
Seconds	43200

New Phase 2

Name	CSA
Comments	Comments
Local Address	addr_subnet ▾ 0.0.0.0/0.0.0.0
Remote Address	addr_subnet ▾ 0.0.0.0/0.0.0.0

Advanced...

Phase 2 Proposal ⊕ Add

Encryption	AES128 ▾	Authentication	SHA256 ▾

Enable Replay Detection ☑

Enable Perfect Forward Secrecy (PFS) □

Local Port	All ☑
Remote Port	All ☑
Protocol	All ☑
Auto-negotiate	□
Autokey Keep Alive	□
Key Lifetime	Seconds ▾
Seconds	43200

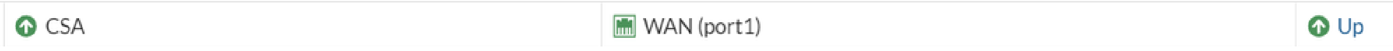
- New Phase 2
  - **Name** ：默认为（取自VPN的名称）
    - **Local Address** ：默认为(0.0.0.0/0.0.0.0)
    - **Remote Address** ：默认为(0.0.0.0/0.0.0.0)

- Advanced
  - **Encryption** ：选择AES128
    - **Authentication** ：选择SHA256
    - **Enable Replay Detection** ：默认为（启用）
    - **Enable Perfect Forward Secrecy (PFS)** ：取消选中复选框
    - **Local**

Port ：默认为（启用）

- **Remote Port**：默认为（启用）
- **Protocol** ：默认为（启用）
- **Auto-negotiate** ：设为默认值（未标记）
- **Autokey Keep Alive** ：设为默认值（未标记）
- **Key Lifetime** ：设为默认值（秒）
- **Seconds** ：默认为(43200)

之后，点击OK。几分钟后，您会看到VPN已使用安全访问建立，您可以继续执行下一步， **Configure the Tunnel Interface.**

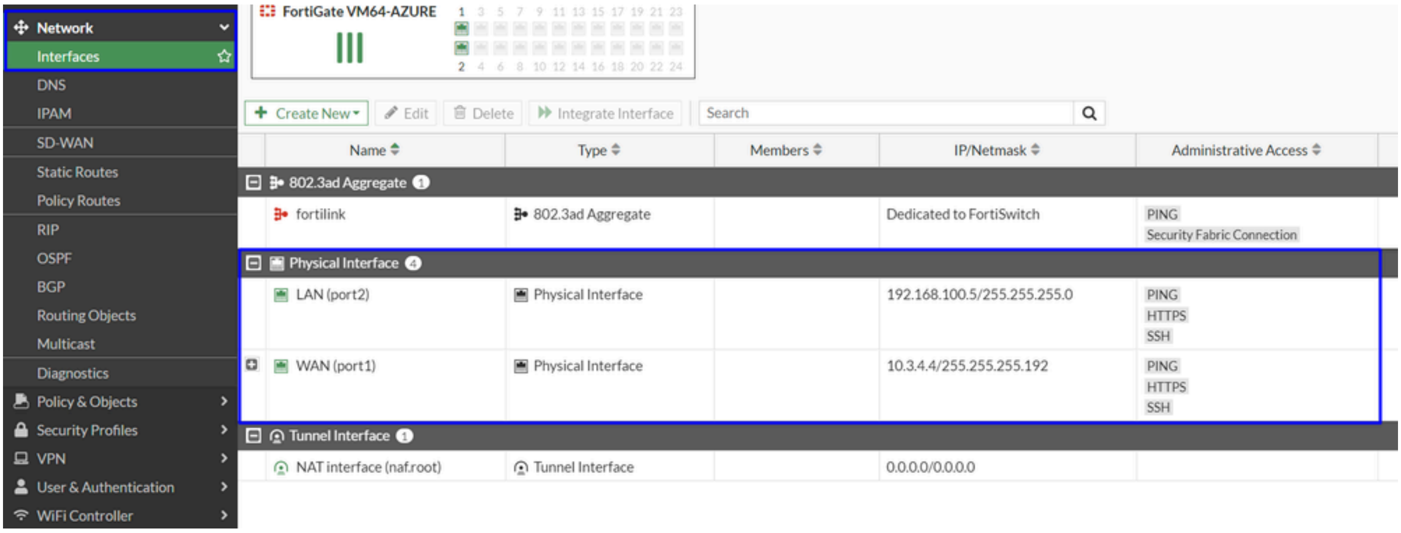


CSA	WAN (port1)	Up

配置隧道接口

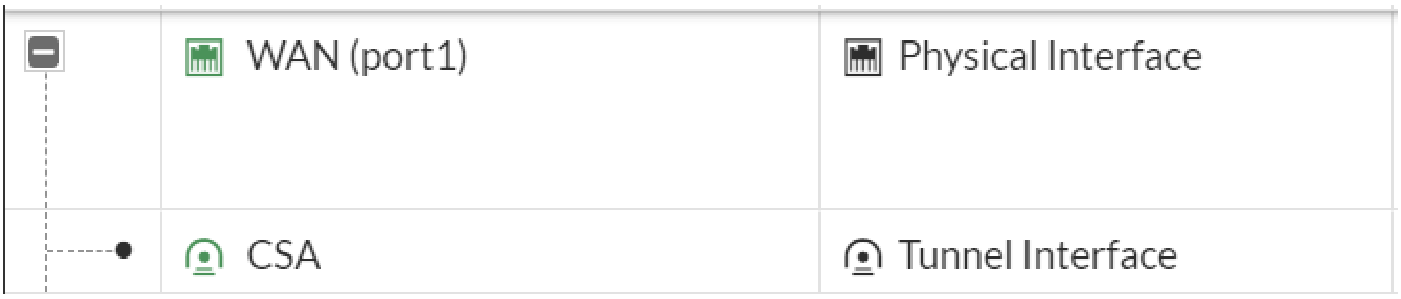
创建隧道后，您会注意到您在端口后面有一个新接口，该端口用作与Secure Access通信的WAN接口。

要检查连通性，请导航到 **Network** > **Interfaces**。



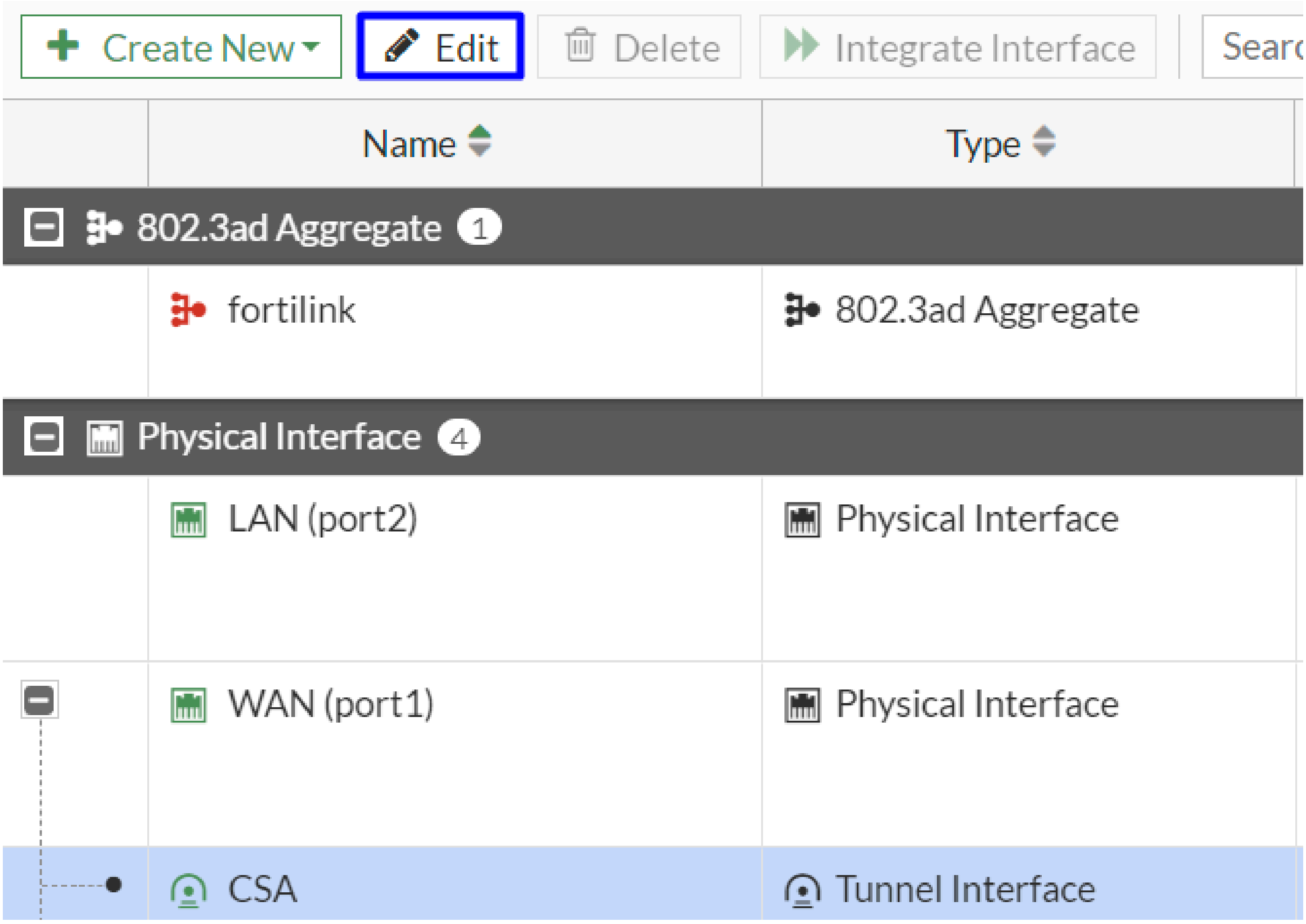
Name	Type	Members	IP/Netmask	Administrative Access
802.3ad Aggregate 1				
fortilink	802.3ad Aggregate		Dedicated to FortiSwitch	PING Security Fabric Connection
Physical Interface 4				
LAN (port2)	Physical Interface		192.168.100.5/255.255.255.0	PING HTTPS SSH
WAN (port1)	Physical Interface		10.3.4.4/255.255.255.192	PING HTTPS SSH
Tunnel Interface 1				
NAT interface (naf.root)	Tunnel Interface		0.0.0.0/0.0.0.0	

展开您用于与安全访问通信的端口；在本例中为**WAN** 接口。



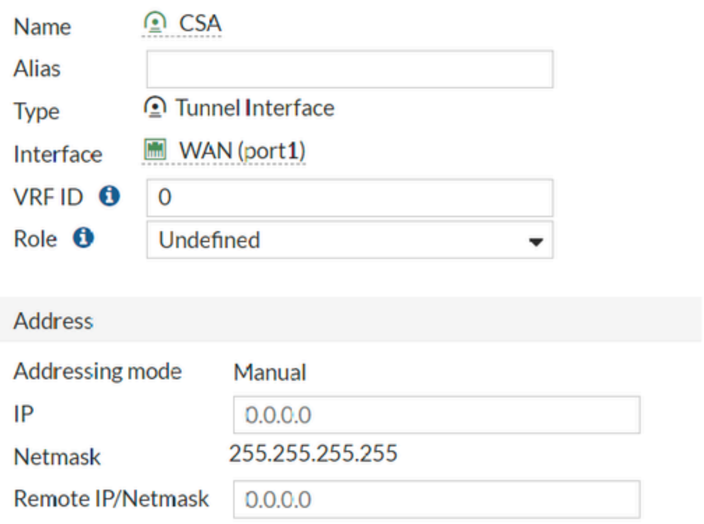
WAN (port1)	Physical Interface
CSA	Tunnel Interface

- 单击您的**Tunnel Interface** 并单击 **Edit**



Name	Type
802.3ad Aggregate 1	
fortilink	802.3ad Aggregate
Physical Interface 4	
LAN (port2)	Physical Interface
WAN (port1)	Physical Interface
CSA	Tunnel Interface

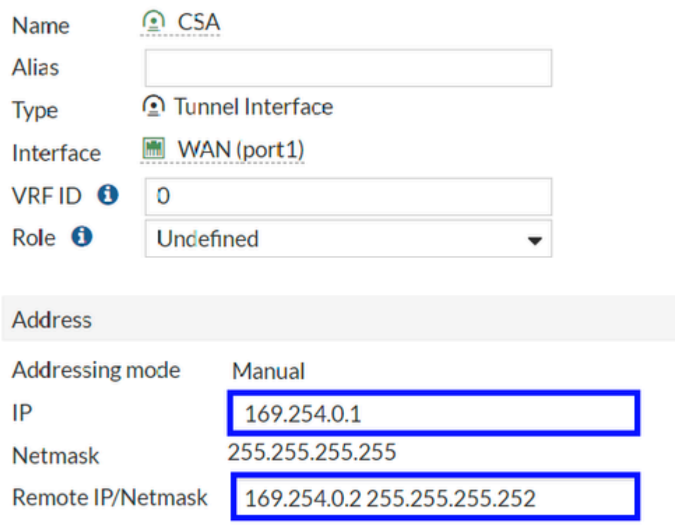
- 您需要配置下一个映像



Name	CSA
Alias	
Type	Tunnel Interface
Interface	WAN (port1)
VRF ID	0
Role	Undefined

Address

Addressing mode	Manual
IP	0.0.0.0
Netmask	255.255.255.255
Remote IP/Netmask	0.0.0.0



Name	CSA
Alias	
Type	Tunnel Interface
Interface	WAN (port1)
VRF ID	0
Role	Undefined

Address

Addressing mode	Manual
IP	169.254.0.1
Netmask	255.255.255.255
Remote IP/Netmask	169.254.0.2 255.255.255.252

  - Interface Configuration

- IP ：配置网络中没有的不可路由IP (169.254.0.1)

- Remote IP/Netmask ：将远程IP配置为接口IP的下一个IP，网络掩码为30 (169.254.0.2 255.255.255.252)

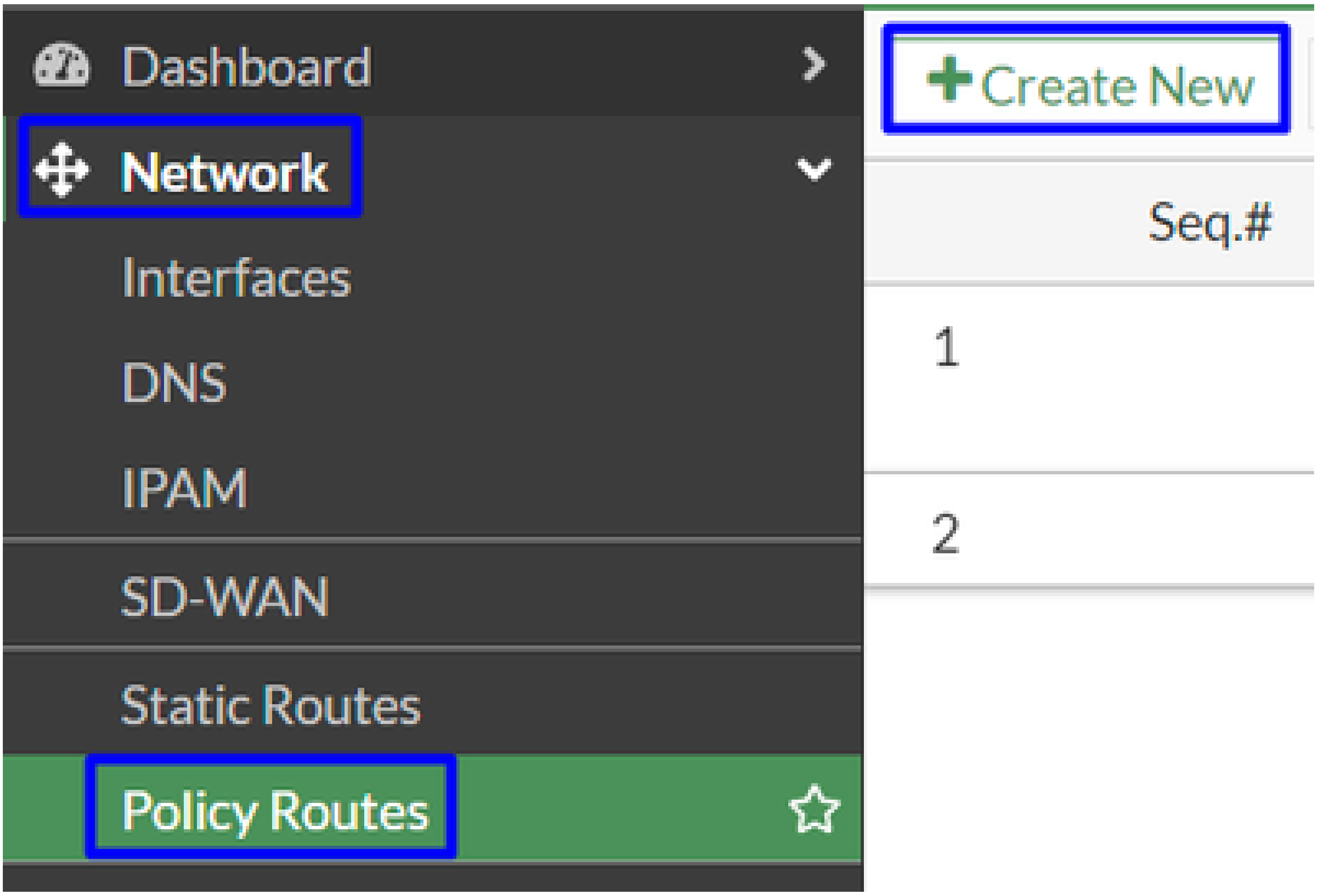
之后，点击**OK** 保存配置并继续下一步，Configure Policy Route （基于源的路由）。

警告：完成此部分后，您必须在FortiGate上配置防火墙策略，以允许或允许来自设备的数据流进行安全访问以及来自安全访问的数据流到达要路由该数据流的网络。

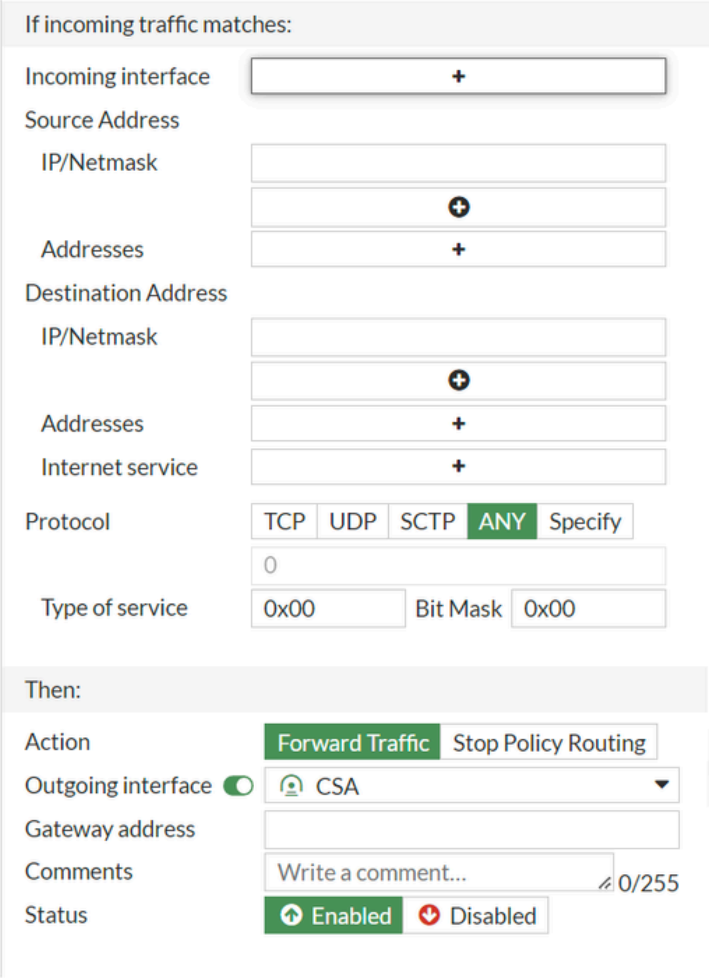
配置策略路由

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

- 导航至 Network > Policy Routes



- 配置策略



If incoming traffic matches:

Incoming interface: +

Source Address

IP/Netmask:

Addresses: +

Destination Address

IP/Netmask:

Addresses: +

Internet service: +

Protocol: TCP | UDP | SCTP | ANY | Specify

0

Type of service: 0x00 Bit Mask 0x00

Then:

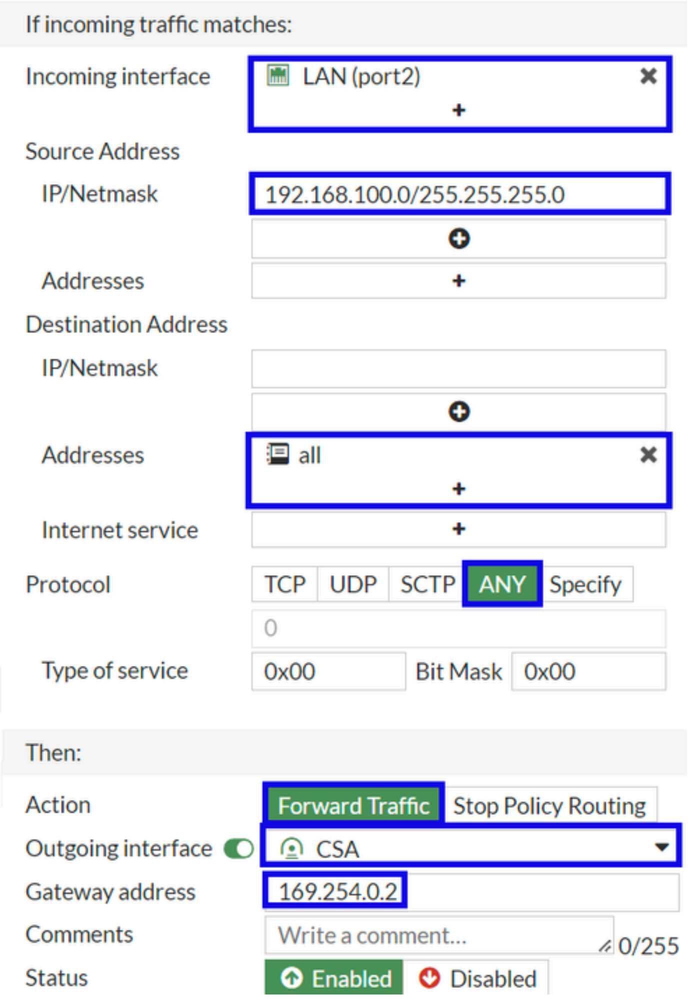
Action: Forward Traffic | Stop Policy Routing

Outgoing interface: CSA

Gateway address:

Comments: Write a comment... 0/255

Status: Enabled | Disabled



If incoming traffic matches:

Incoming interface: LAN (port2)

Source Address

IP/Netmask: 192.168.100.0/255.255.255.0

Addresses: +

Destination Address

IP/Netmask:

Addresses: all

Internet service: +

Protocol: TCP | UDP | SCTP | ANY | Specify

0

Type of service: 0x00 Bit Mask 0x00

Then:

Action: Forward Traffic | Stop Policy Routing

Outgoing interface: CSA

Gateway address: 169.254.0.2

Comments: Write a comment... 0/255

Status: Enabled | Disabled

- If Incoming traffic matches
  - Incoming Interface ：选择计划将流量重新路由至安全访问（流量源）的接口
- Source Address
  - IP/Netmask ：如果仅路由接口的子网，请使用此选项
    - Addresses ：如果已创建对象且流量源来自多个接口和多个子网，则使用此选项
- Destination Addresses
  - Addresses：选择 all

        - Protocol：选择 **ANY**

- Then
    - Action： **Choose Forward Traffic**

- Outgoing Interface ：选择在步骤Configure Tunnel Interface中修改的隧道接口
- Gateway Address：配置在步骤RemoteIPNetmask中配置的远程IP
- Status ：选择已启用

点击**OK** 以保存配置，现在您可以验证是否已将设备流量重新路由到安全访问。

验证

要验证计算机的流量是否已重新路由到安全访问，您有两个选项；您可以在互联网上检查并检查公共IP，或者使用curl运行下一个命令：

<#root>

```
C:\Windows\system32>curl ipinfo.io { "ip": "151.186.197.1", "city": "Frankfurt am Main", "region": "Hes
```

您可以查看流量的公共范围是：

Min Host:151.186.176.1

Max Host :151.186.207.254

注意：这些IP可能会发生变化，这意味着思科可能会在未来扩展此范围。

如果您看到您的公共IP发生更改，这意味着您受到安全访问保护，现在您可以在“安全访问”(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）。