

# 使用安全防火墙配置安全访问使用动态路由的专用访问威胁防御

## 目录

---

### [简介](#)

### [先决条件](#)

#### [要求](#)

#### [使用的组件](#)

### [背景信息](#)

### [配置](#)

#### [安全访问配置](#)

##### [网络隧道组配置](#)

##### [安全访问路由](#)

###### [动态路由\(BGP\)](#)

##### [保存网络隧道组配置](#)

##### [创建专用资源](#)

##### [创建访问策略规则](#)

#### [安全防火墙威胁防御\(FTD\)配置](#)

##### [虚拟隧道接口配置](#)

##### [IPsec隧道配置](#)

##### [FTD路由配置](#)

###### [动态路由\(BGP\)](#)

##### [访问策略配置](#)

### [验证](#)

#### [在FTD中验证](#)

##### [FTD中的隧道状态](#)

##### [安全访问中的隧道状态](#)

##### [安全访问中的事件](#)

### [相关信息](#)

---

## 简介

本文档介绍如何通过IPsec使用FTD配置安全访问，以实现使用动态路由的安全专用访问。

## 先决条件

### 要求

- 思科安全访问知识

- 思科安全访问控制面板/租户
- 安全防火墙威胁防御和防火墙管理中心知识
- IPsec知识
- 动态路由知识

## 使用的组件

- 运行7.7.10代码的安全防火墙
- 云交付的防火墙管理中心。配置也适用于典型的虚拟FMC
- 思科安全访问控制面板

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

安全访问中的网络隧道可用于两个主要用途：安全互联网访问和安全私有访问。

对于安全专用访问，组织可以利用零信任访问(ZTA)和/或VPN即服务(VPNaaS)将用户连接到专用资源（如内部应用程序或数据中心）。IPsec隧道在此架构中扮演着重要角色，它安全地加密用户和私有资源之间的网络流量，确保敏感数据在通过不受信任的网络时仍受到保护。通过将IPsec隧道与ZTA或VPNaaS集成，组织可以无缝安全地访问内部资源，同时保持强大的安全控制和可视性。

本文档介绍如何通过IPsec为安全专用访问配置具有安全防火墙威胁防御(FTD)的安全访问。此外，本指南还提供使用BGP配置动态路由的步骤。

虽然本文档介绍用于安全专用访问的IPsec隧道的配置，但用于访问专用应用程序的零信任访问(ZTA)或VPN即服务(VPNaaS)设置不属于本指南的范围。

## 配置

### 安全访问配置

#### 网络隧道组配置

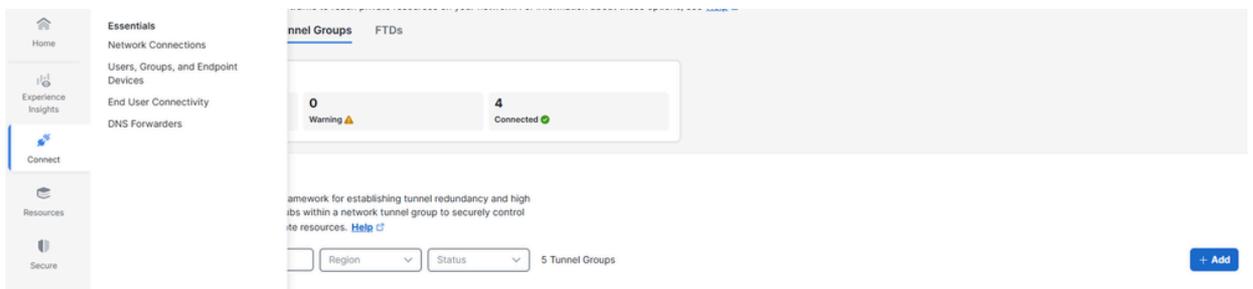
1. 导航至“安全访问”的[管理面板](#)。



CSA控制面板

## 2. 添加网络隧道组。

- 点击Connect > Network Connections
  - 在Network Tunnel Groups下，单击 > Add



检查NTG

## 3. 配置General Settings。

- 配置Tunnel Group Name, Region 和 Device Type
  - 点击 Next

- 1 General Settings
- 2 Tunnel ID and Passphrase
- 3 Routing
- 4 Data for Tunnel Setup

### General Settings

Give your network tunnel group a good meaningful name, choose type this tunnel group will use.

**Tunnel Group Name**  
FTD

**Region**  
Canada (Central)

**Device Type**  
FTD

常规设置

## 4. 配置和Tunnel ID Passphrase。此ID很重要，因为FTD配置需要此ID

- 点击 Next

- ✓ General Settings
- ✓ Tunnel ID and Passphrase
- 3 Routing
- 4 Data for Tunnel Setup

## Tunnel ID and Passphrase

Configure the tunnel ID and pa

### Tunnel ID Format

Email  IP Address

#### Tunnel ID

ftd1-ipsec

#### Passphrase

.....

The passphrase must be between special characters.

#### Confirm Passphrase

.....

ID和PSK

## 5. 配置动态路由。

### 安全访问路由

### 动态路由(BGP)

- 在安全访问中配置BGP对等体时，指定FTD的BGP自主系统(AS)编号。
- 点击Routing > Dynamic routing
  - 点击Device AS Number，然后添加FTD BGP ASN
  - 选中Block default route advertisement复选框
  - 点击 Save

Dynamic routing

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

**Device AS Number**

64513

**Advanced Settings**

**Multihop BGP**

Select this option to enable the ability for BGP peers to establish a connection (hop) when not directly connected.

**Multi-region backhaul**

Use Secure Access as the network backbone and prioritize regions based on origin.

**Block default route advertisement**

Select to block the advertisement of the default route.

CSA BGP配置



注意：由安全访问通告的路由在原始AS路径之前预置以下内容：1表示主隧道，2表示辅助隧道。支持多区域回传场景。有关详细信息，请单击。

## 保存网络隧道组配置

下载并保存隧道设置数据，因为FTD配置需要此数据。

- 点击 Download CSV
- 点击 Done

**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: ftd1-ipsec@

Primary Data Center IP Address:

Secondary Tunnel ID: ftd1-ipsec@

Secondary Data Center IP Address:

Passphrase:

Download CSV

Done

NTG数据

## Summary

✖ Disconnected

|                    |                      |                                       |  |
|--------------------|----------------------|---------------------------------------|--|
| Region             | Canada (Central)     | Routing Type                          | Dynamic Routing (BGP)                                    |
| Device Type        | FTD                  | Device BGP AS                         | 64513  |
| Last Status Update | Feb 18, 2026 3:58 PM | Peer (Secure Access) BGP AS           | 64512  |
|                    |                      | BGP Peer (Secure Access) IP Addresses | 169.254.0.9, 169.254.0.5, 2a04:e4c4:b:c723::b67:0000/120 |
|                    |                      | Multihop BGP Addresses                | —  |
|                    |                      | Multihop TTL                          | —  |

BGP设置



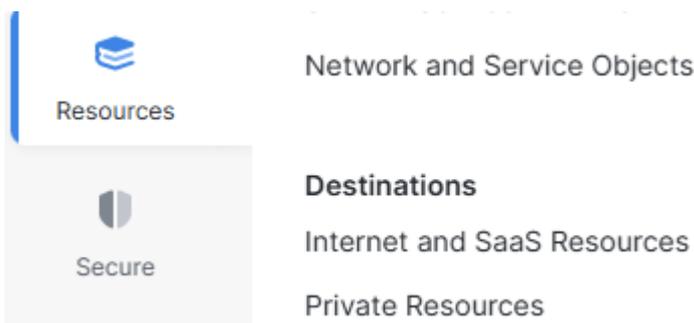
注意：点击Network Tunnel Group以查看BGP AS编号和BGP对等IP地址（稍后在FTD端配置）。

## 创建专用资源

私有资源是指托管在数据中心或私有云环境中的内部应用、网络或子网。这些资源不可公开访问，并且受您组织的基础设施的保护。

通过将它们定义为Secure Access中的专用资源，您可以通过零信任访问(ZTA)或VPN即服务(VPNaaS)等解决方案启用受控访问。这可确保用户根据身份、设备状况和访问策略安全地连接到内部系统，而无需将资源直接暴露到互联网。

导航到Resources Private Resources>>单击Add。



公关

- 指定Private Resource Name、Internally reachable address、ProtocolPort/Ranges。指定端口和协议，并根据需要添加其他专用资源
- 根据需要Connection Method，选择所需的连接，例如零信任连接和/或VPN连接，具体取决于您的要求
- 单击 Save

**Private Resource Name**

**Description (optional)**

**Private resource address**

Define how the private resource will connect to applications through Secure Access.

| <b>Internally reachable address (FQDN, Wildcard FQDN, IPv4, IPv6, CIDR) ⓘ</b> | <b>Protocol</b>                               | <b>Port / Ranges</b>              |
|---|---|-----------------------------------|
| <input type="text" value="172.16.15.55"/>                                     | <input type="text" value="TCP - (HTTP/H..."/> | <input type="text" value="8080"/> |

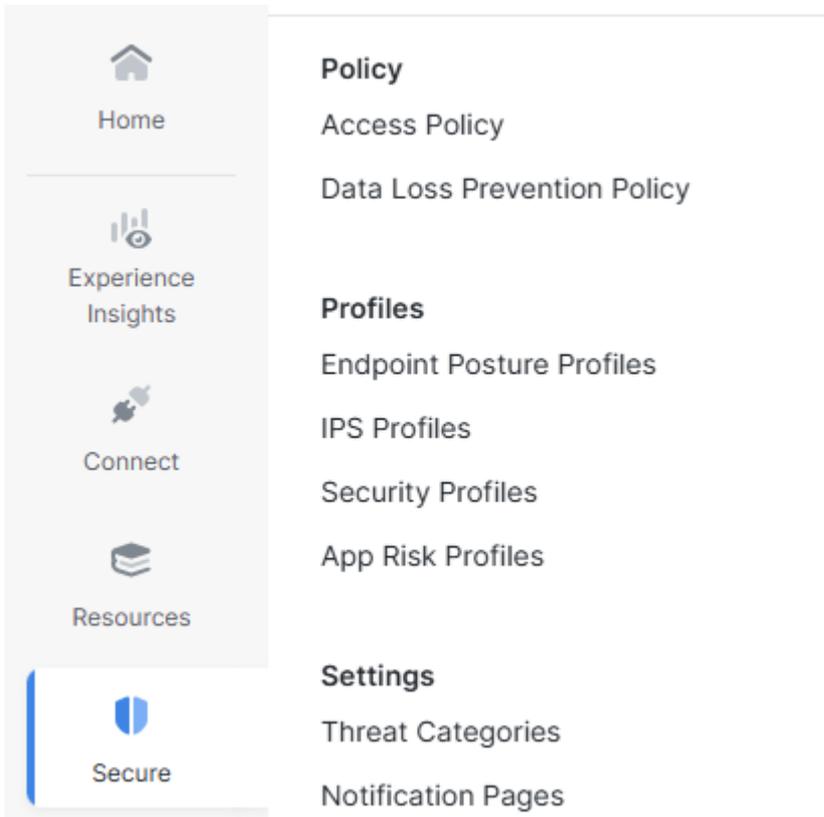
专用资源

## 创建访问策略规则

私有访问规则定义用户如何安全地连接到不可公开访问的内部资源和应用。

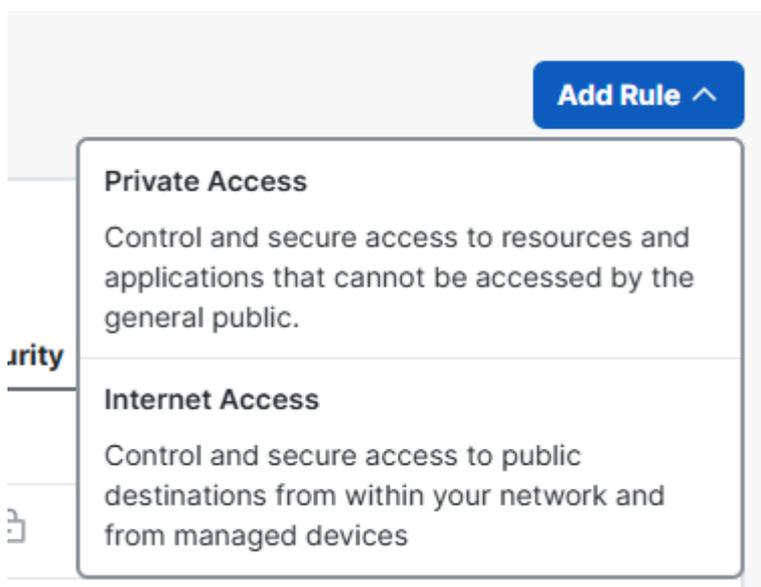
这些规则通过根据用户身份、组成员身份、设备状态、位置或其他策略条件等因素控制谁可以访问特定私有资源来实施安全性。这可确保敏感的内部系统免受一般公共访问的影响，同时仍可通过ZTA或VPNaaS安全地供授权用户使用。

依次导航至 [Secure>Access Policy](#)



ACP

- 点击 Add Rule
  - 点击 Private Access



添加ACP

- 点击 Rule Name ， 并为其命名
- 点击 Action ， 选择 Allow 允许此流量
- 单击 From On 并指定已授予权限的用户
- 点击 To 并指定用户基于此规则拥有的访问权限
- 点击 Next ， 然后 Save 进入下一页

Rule name ⓘ  Rule order

---

**1 Specify Access**  
Specify which users and endpoints can access which resources. [Help](#) 🔗

**Action**

**Allow**  
Allow specified traffic if security requirements are met.

**Block**  
Block specified traffic.

**From**  
Specify one or more sources

**To**  
Specify one or more destinations

+ AND

**Endpoint Requirements**

For VPN connections:  
 End-user endpoint devices that are connected to the network using VPN may be able to access destinations specified in this rule. ⓘ  
Endpoint requirements are configured in the VPN posture profile. Requirements are evaluated at the time the endpoint device connects to the network. [VPN Posture Profiles](#) 🔗

For Branch connections:  
 Endpoint device posture is not evaluated for endpoints connecting to these resources from a branch network.

---

**2 Configure Security**  
Configure security requirements that must be met before traffic is allowed. [Help](#) 🔗

[Cancel](#) [Back](#) [Next](#)

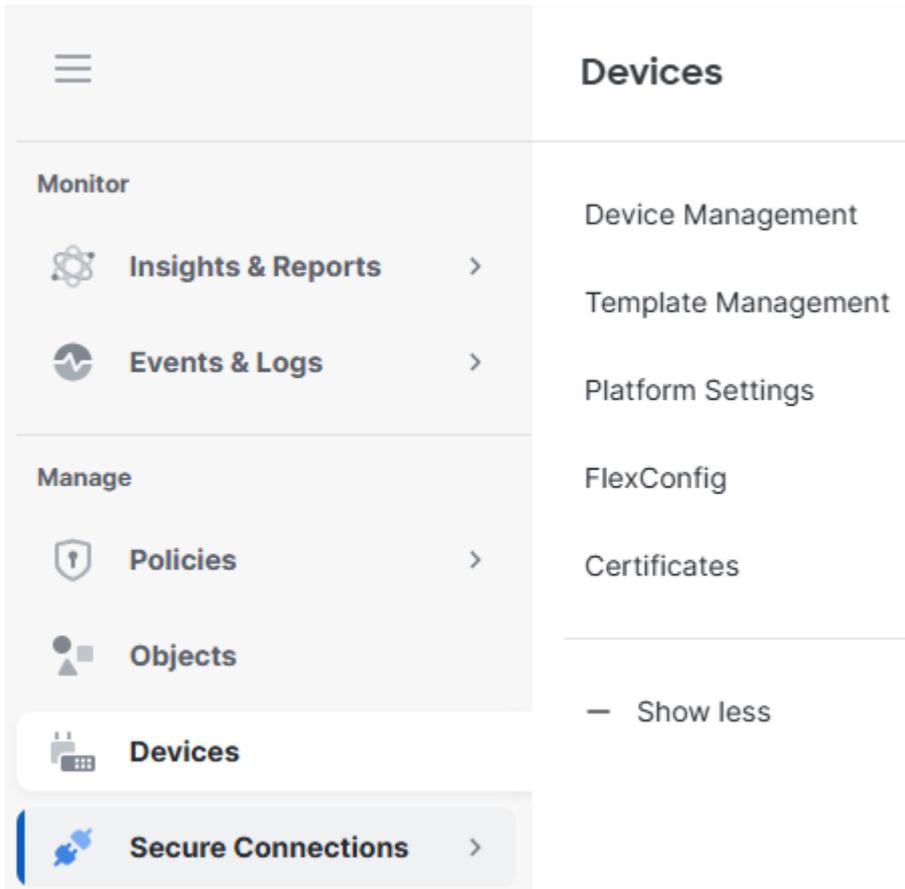
ACP配置

## 安全防火墙威胁防御(FTD)配置

### 虚拟隧道接口配置

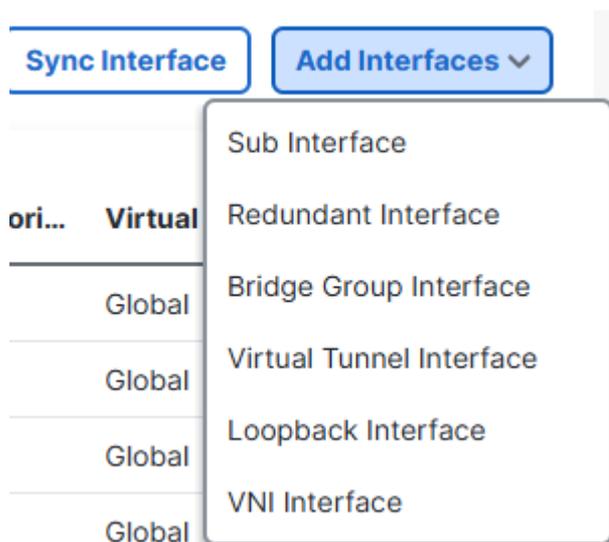
FTD上的虚拟隧道接口(VTI)是用于配置基于路由的IPsec VPN隧道的逻辑第3层接口。

1.定位至Devices>Device Management。



FTD设备

- 点击FTD设备， Interfaces
  - 点击 Add Interfaces
  - 点击 Virtual Tunnel Interface
  - 创建两个虚拟隧道接口，一个用于主安全访问集线器，另一个用于辅助安全访问集线器



添加VTI

虚拟隧道接口1:

- 为其命名，点击 **Enable**
- 选择或创建 **Security Zone**
- 点击 **Tunnel ID**，并为其赋值。
- 点击 **Tunnel Source**，并指定建立隧道的WAN接口
- 点击 **IPsec Tunnel Mode**，选择 **IPv4**
- 点击 **IP Address**，并配置VTI的IP地址

点击OK

### Tunnel Type

Static  Dynamic

Name:\*

VTI-1

Enabled

Description:

Security Zone:

zone\_vti

Priority:

0

(0 - 65535)

---

### Virtual Tunnel Interface Details

An interface named Tunnel<ID> is configured. Tunnel Source is a physical interface where VPN tunnel terminates for the VTI.

Tunnel ID:\*

1

(0 - 10413)

Tunnel Source:\*

GigabitEthernet0/0 (outside)

192.168.0.20

VTI1.1

---

## IPsec Tunnel Details

IPsec Tunnel mode is decided by VPN traffic IP type. Configure IPv4 and IPv6 addresses accordingly.

IPsec Tunnel Mode:\*

IPv4       IPv6

IP Address:\*

Configure IP

169.254.0.1/30



VTI1.2

虚拟隧道接口2:

- 为其命名，点击 `Enable`
- 选择或创建 `Security Zone`
- 点击 `Tunnel ID`，并为其赋值
- 点击 `Tunnel Source`，并指定建立隧道的WAN接口
- 点击 `IPsec Tunnel Mode`，选择IPv4
- 点击 `IP Address`，并配置VTI的IP地址
- 点击OK

### Tunnel Type

Static  Dynamic

Name:\*

VTI-2

Enabled

Description:

Security Zone:

zone\_vti

Priority:

0

(0 - 65535)

---

### Virtual Tunnel Interface Details

An interface named Tunnel<ID> is configured. Tunnel Source is a physical interface where VPN tunnel terminates for the VTI.

Tunnel ID:\*

2

(0 - 10413)

Tunnel Source:\*

GigabitEthernet0/0 (outside)

192.168.0.20

VTI2.1

---

### IPsec Tunnel Details

IPsec Tunnel mode is decided by VPN traffic IP type. Configure IPv4 and IPv6 addresses accordingly.

IPsec Tunnel Mode:\*

IPv4  IPv6

IP Address:\*

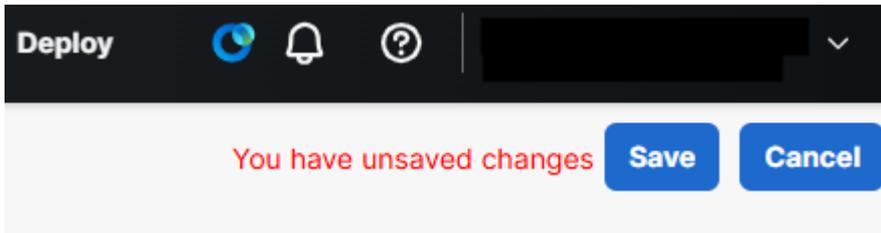
Configure IP

169.254.0.5/30



VTI2.2

单击Save。

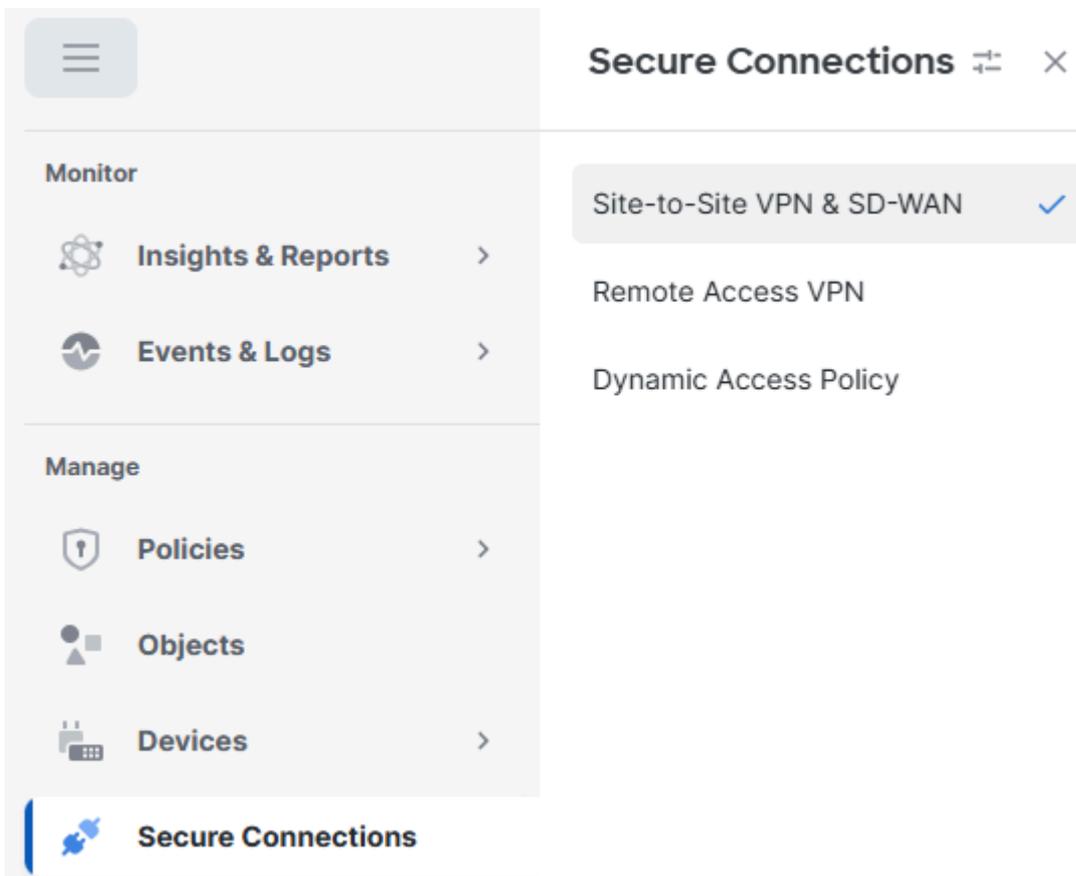


保存VTI更改

## IPsec隧道配置

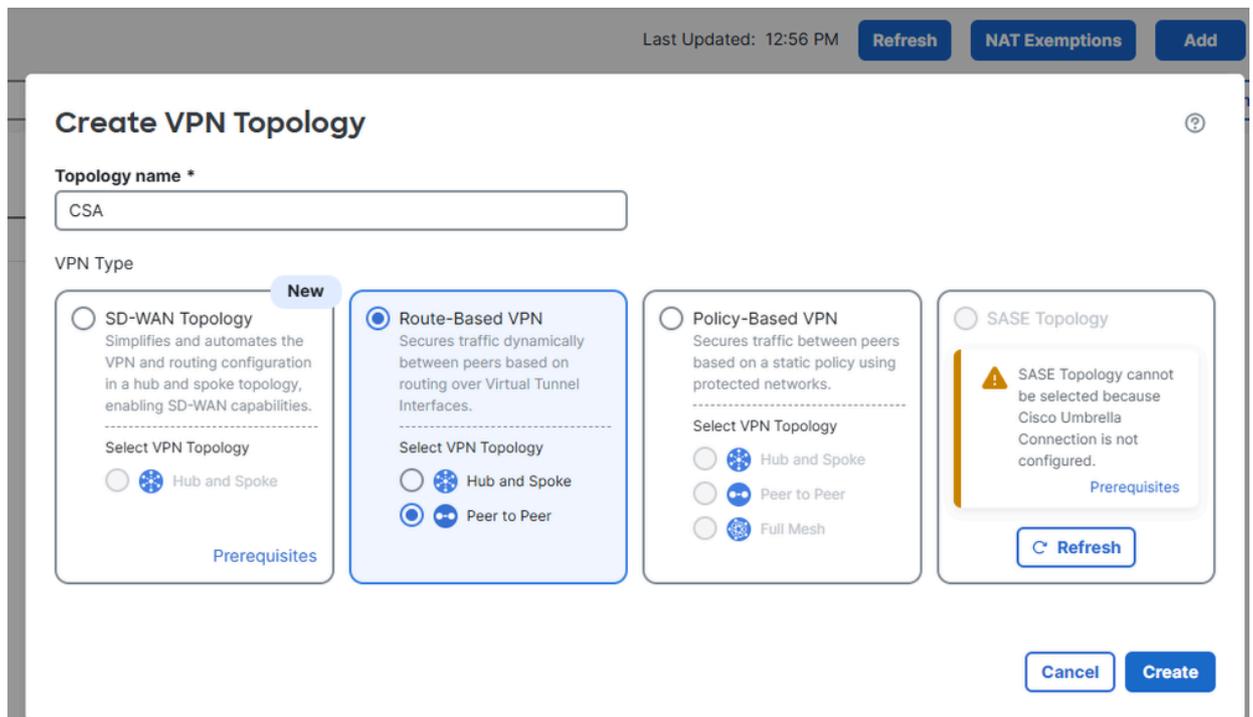
导航到您的cdFMC控制面板。

- 点击Secure Connection> Site-to-Site VPN & SD-WAN



S2

- 点击Add
  - 点击 Route-Based VPN
  - 点击 Peer to Peer



添加VPN

- 从安全访问配置的第5步获取主要和辅助数据中心的隧道ID和IP地址
- 点击Endpoints
  - 在Node A下，单击Device并选择 Extranet
  - 单击Device Name并为其命名
  - 单击Endpoint IP Addresses，在Secure Access（安全访问）下输入Secure Access Primary and Secondary IP Addresses（安全访问主要和辅助IP地址），用逗号分隔（来自“Save Network Tunnel Group Configuration”（保存网络隧道组配置）配置）
  - 在Node B下，单击Device并选择FTD设备
  - 单击Virtual Tunnel Interface，选择上一步中创建的第一个VTI接口
  - 单击Send Local Identity to Peers选项并选择Email ID，输入主隧道ID（从“安全访问配置”下的“保存网络隧道组配置”中）
  - 单击 Add Backup VTI
  - 单击Virtual Tunnel Interface，选择上一步中创建的第二个VTI接口
  - 单击Send Local Identity to Peers选项并选择Email ID，输入辅助隧道ID（从Secure Access Configuration下的“保存网络隧道组配置”）
  - 单击Save

Network Topology:

**Point to Point** Hub and Spoke Full Mesh

IKE Version:\*  IKEv1  IKEv2

**Endpoints** IKE IPsec Advanced

**Node A**

Device:\*

Device Name\*:

Endpoint IP Address\*:

**Node B**

Device:\*

Virtual Tunnel Interface\*  
 +

*Tunnel Source: outside (IP: 192.168.0.20)* [Edit VTI](#)

Tunnel Source IP is Private

Send Local Identity to Peers

Local Identity Configuration\*

---

Backup VTI: Remove

Virtual Tunnel Interface\*  
 +

*Tunnel Source: outside (IP: 192.168.0.20)* [Edit VTI](#)

Tunnel Source IP is Private

Send Local Identity to Peers

Local Identity Configuration\*

Cancel **Save**

FTD VTI配置

- 点击 IKE
  - 点击IKEv2 Settings > Policies
  - 选择选Umbrella-AES-GCM-256项

点击 OK

# IKEv2 Policy



Available IKEv2 Policy ↻ +

Search

- AES-GCM-NULL-SHA
- AES-GCM-NULL-SHA-LA..
- AES-SHA-SHA
- AES-SHA-SHA-LATEST
- DES-SHA-SHA
- DES-SHA-SHA-LATEST
- Umbrella-AES-GCM-256

Add

Selected IKEv2 Policy

Umbrella-AES-GCM-256 ✕

Cancel **OK**

## IKEv2策略

- 点击 Authentication Type ，选择 Pre Shared Manual Key ，输入在安全访问（密码）中配置的PSK

**Endpoints** **IKE** IPsec **Advanced**

Pre-shared Key Length:\* 24 Characters (Range 1-127)

**IKEv2 Settings**

Policies:\* Umbrella-AES-GCM-256 ✎

Authentication Type: Pre-shared Manual Key ▾

Key:\* •••••

Confirm Key:\* •••••

Enforce hex-based pre-shared key only

## IKE

- 点击 IPSEC
  - 点击 IKEv2 Proposals

- 选择 Umbrella-AES-GCM-256
- 点击 OK

Endpoints    IKE    **IPsec**    Advanced

Crypto Map Type:  Static     Dynamic

IKEv2 Mode: Tunnel

Transform Sets: IKEv1 IPsec Proposals     IKEv2 IPsec Proposals\* 

|                   |                      |
|-------------------|----------------------|
| tunnel_aes256_sha | Umbrella-AES-GCM-... |
|-------------------|----------------------|

IPsec

Cancel    **OK**

保存IKEv2提议

## FTD路由配置

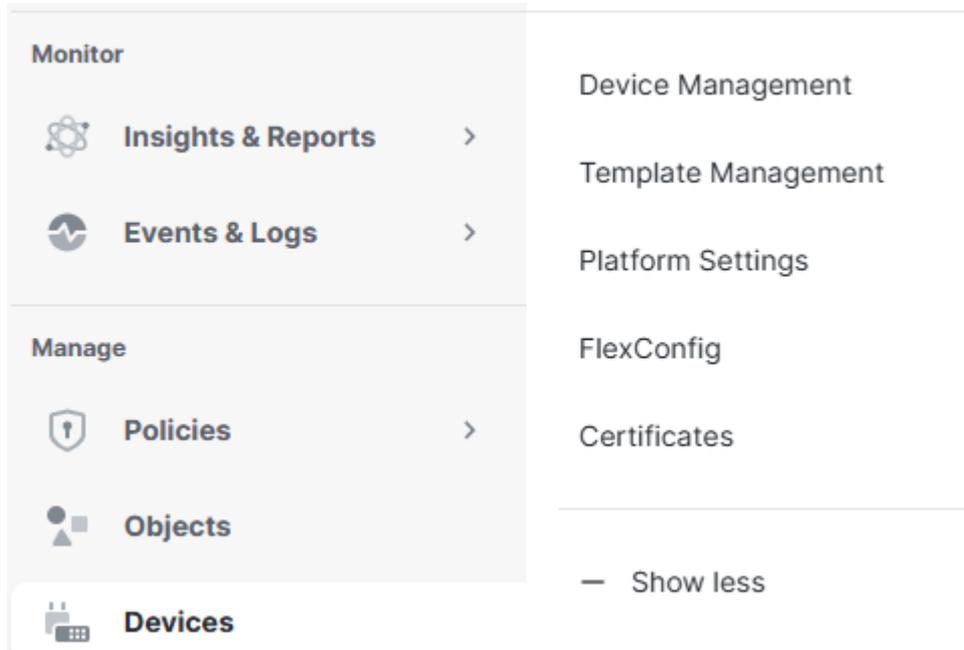
### 动态路由(BGP)

边界网关协议(BGP)是一种动态路由协议，可自动在自治系统(AS)之间交换路由信息。它根据属性和策略确定数据流量的最佳可用路径，而不是依赖静态路由。

通过动态获取和更新路由，BGP提高了可扩展性，优化了路径选择，并在链路或网络发生变化时提供自动故障切换。

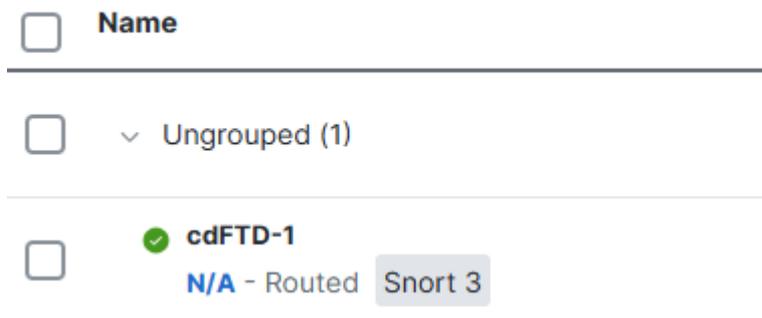
导航到您的cdFMC控制面板。

- 点击Devices > Device Management



设备

- 点击FTD



FTD设备

- 单击Routing > BGP > IPv4 > Enable IPv4
- 单击Neighbor，然后指定安全访问的BGP自治系统(AS)编号以及邻居IP地址  
请参阅安全访问配置下的说明，其中提供了此流程的所有相关配置详细信息。
- 单击Save

cdFTD-1  
Cisco Secure Firewall Threat Defense for VMware

Enable IPv4:  AS Number 64513

General Neighbor Add Aggregate Address Filtering Networks Redistribution Route Injection

| Address     | Remote AS Number | Address Family | Remote Private AS Number | Description |
|-------------|------------------|----------------|--------------------------|-------------|
| 169.254.0.2 | 64512            | Enabled        |                          |             |
| 169.254.0.6 | 64512            | Enabled        |                          |             |

## BGP邻居



注意：从2025年11月开始，所有新创建的安全访问组织默认使32644公共ASN策略在网络隧道组中的BGP对等。在2025年11月之前建立的现有组织继续使用之前为64512全访问BGP对等体保留的私有ASN路由。

- 点击Networks，然后添加要通告给Secure Access的网络
- 点击 Save

cdFTD-1  
Cisco Secure Firewall Threat Defense for VMware

Enable IPv4:  AS Number 64513

General Neighbor Add Aggregate Address Filtering Networks Redistribution Route Injection

| Network            | RouteMap |
|--------------------|----------|
| Subnet-172.16.15.0 |          |

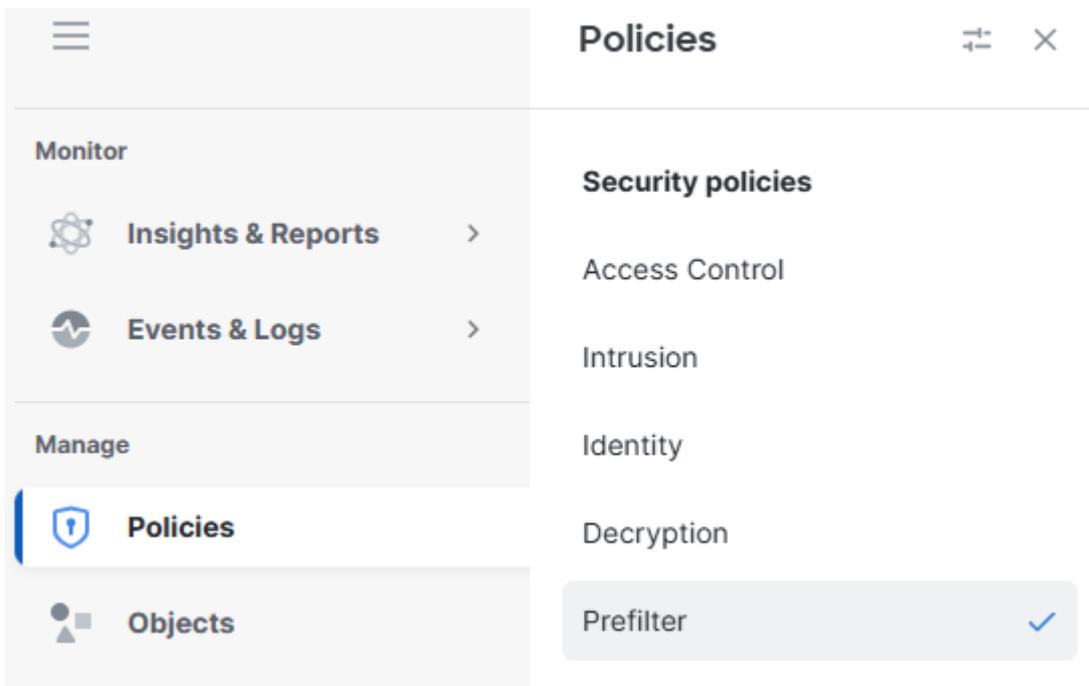
## 添加网络

## 访问策略配置

要允许Cisco Firepower威胁防御(FTD)上的流量并启用对专用资源的访问，流量必须首先通过称为预过滤的访问控制初始阶段。

预过滤是在进行更深的检查之前进行处理，并且设计为简单快速。它使用基本外部报头标准（例如源和目标IP地址和端口）评估流量，以快速允许、阻止或绕过流量。在此阶段允许流量时，可以跳过资源密集型检查（如深度数据包检查或入侵策略），从而在保持安全控制的同时提高性能。

导航至Policies > Prefilter



预过滤器

- 点击编辑您的访问策略使用的预过滤器策略



点击prefilter

- 点击 Add Tunnel Rule
  - 将来自VPNaaS网络和/或ZTA子网的流量添加到您的专用资源，并允许这些流量
  - 点击Save



保存规则

此时，完成并验证FTD上的配置后，您可以继续进行部署。部署后，IPsec隧道和BGP邻居会话均成功启动，确认连接和动态路由按预期运行。

## 验证

## 在FTD中验证

### FTD中的隧道状态

您可以查看隧道的当前状态，包括隧道是up还是down。这有助于检验IPsec隧道是否已正确建立。

- 单击Secure Connections
- 单击Site-to-Site VPN & SD-WAN
- 单击拓扑名称

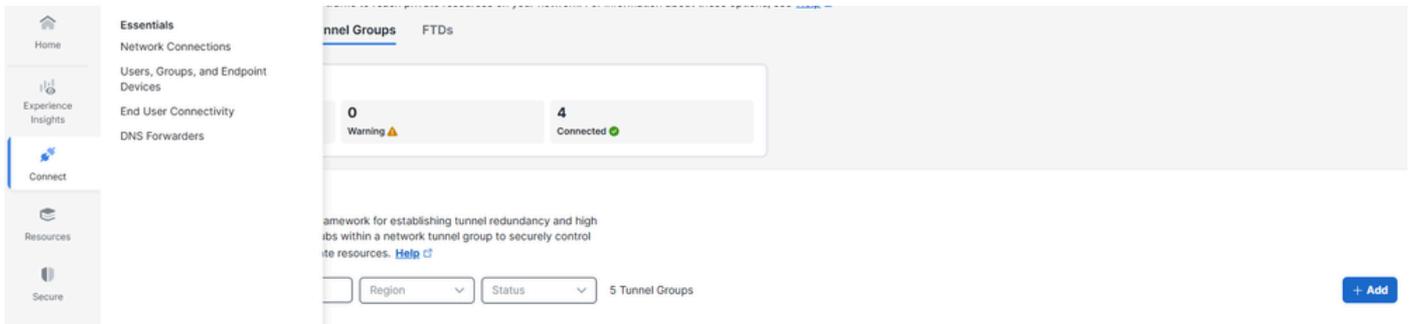
| Topology name     | VPN Type          | Network Topology | Tunnel Status Distribution | IKEv1                  | IKEv2               |
|-------------------|-------------------|------------------|----------------------------|------------------------|---------------------|
| CSA               | Route Based (VTI) | Point-to-Point   | 2 Tunnels                  |                        | ✓                   |
| <b>Node A</b>     |                   |                  |                            |                        |                     |
| <b>Node B</b>     |                   |                  |                            |                        |                     |
| Device            | VPN Interface     | VTI Interface    | Device                     | VPN Interface          | VTI Interface       |
| EXTRANET Extranet |                   |                  | FTD cdFTD-1                | outside (192.168.0.20) | VTI-1 (169.254.0.1) |
| EXTRANET Extranet |                   |                  | FTD cdFTD-1                | outside (192.168.0.20) | VTI-2 (169.254.0.5) |

### FTD隧道状态

### 安全访问中的隧道状态

您可以查看隧道的当前状态，包括它是断开连接、警告连接还是已连接。这有助于检验IPsec隧道是否已正确建立。

- 单击Connect > Network Connections
- 单击Network Tunnel Groups



### 检查NTG

- 点击网络隧道组

## Summary

Connected

|                    |                      |                  |                |
|--------------------|----------------------|------------------|----------------|
| Region             | Canada (Central)     | Routing Type     | Static Routing |
| Device Type        | FTD                  | IP Address Range | 172.16.15.0/24 |
| Last Status Update | Feb 18, 2026 3:34 PM |                  |                |

### Primary Hub

[See Logs](#)

Hub Up

1

Active Tunnels

Tunnel Group ID ftd1-ipsec@

### Secondary Hub

Hub Up

1

Active Tunnels

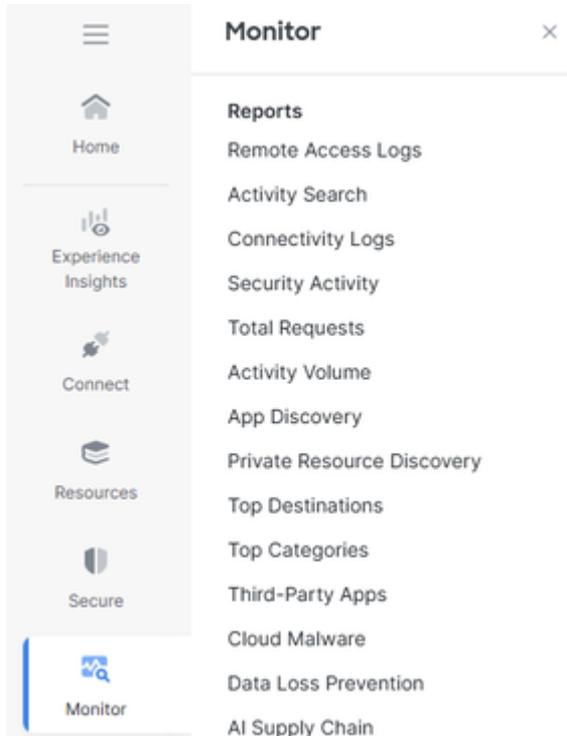
Tunnel Group ID

CSA隧道状态

## 安全访问中的事件

您可以查看隧道和BGP事件，并确认IPsec隧道的状态是否为up且稳定，以及是否建立了BGP会话。

单击Monitor > Network Connectivity。



监控连接日志

| Network tunnel group | Data center IP address | Hub type  | Region       | Alerts | Service | Device type | Details                | Time (UTC)           |
|----------------------|------------------------|-----------|--------------|--------|---------|-------------|------------------------|----------------------|
| FTD                  |                        | Secondary | ca-central-1 | Info   | BGP     | FTD         | BGP peer up            | Feb 18, 2026 4:07 PM |
| FTD                  |                        | Secondary | ca-central-1 | Info   | IKE     | FTD         | Successful CHILD re... | Feb 18, 2026 4:07 PM |
| FTD                  |                        | Primary   | ca-central-1 | Info   | BGP     | FTD         | BGP peer up            | Feb 18, 2026 4:06 PM |
| FTD                  |                        | Primary   | ca-central-1 | Info   | IKE     | FTD         | Successful CHILD re... | Feb 18, 2026 4:06 PM |

NTG日志

导航到监控 > 活动搜索。

- Home
- Experience Insights
- Connect
- Resources
- Secure
- Monitor

## Monitor ×

---

### Reports

- Remote Access Logs
- Activity Search
- Connectivity Logs
- Security Activity
- Total Requests
- Activity Volume
- App Discovery
- Private Resource Discovery
- Top Destinations
- Top Categories
- Third-Party Apps
- Cloud Malware
- Data Loss Prevention
- AI Supply Chain

监控连接日志

在任何相关事件上，点击View Full Details。

| Source | Rule Identity | Destination |                   |
|--------|---------------|-------------|-------------------|
| Josue  | Josue         |             | View Full Details |
| Josue  | Josue         |             | Filter by Josue   |
| Josue  | Josue         |             | Filter by         |
| Josue  | Josue         |             | Filter by         |
| Josue  | Josue         |             | View Rule         |
| Josue  | Josue         |             | Edit Rule         |

完整详情

## Event Details



### Action

Allowed

### Time

Feb 18, 2026 3:30 PM

### Rule Name

**FTD IPsec Rule (2386307)**

### Enforced By

-

---

### Source

 **Josue**

### Source IP

### Destination

http://172.16.15.55:8080/favicon.ico

### Security Group Tag (SGT)

-

### Destination IP

172.16.15.55

活动搜索

## 相关信息

- [思科技术支持和下载](#)
- [思科安全防火墙管理中心设备配置指南, 7.7](#)

## 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）。