使用基于策略的路由为专用访问配置安全访问和安全的防火墙威胁防御

目录

简介

本文档介绍如何通过IPsec使用FTD配置安全访问，以便使用基于策略的路由实现安全专用访问。

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
- 基于策略的路由知识

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，本指南还提供配置基于策略的路由的步骤。

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

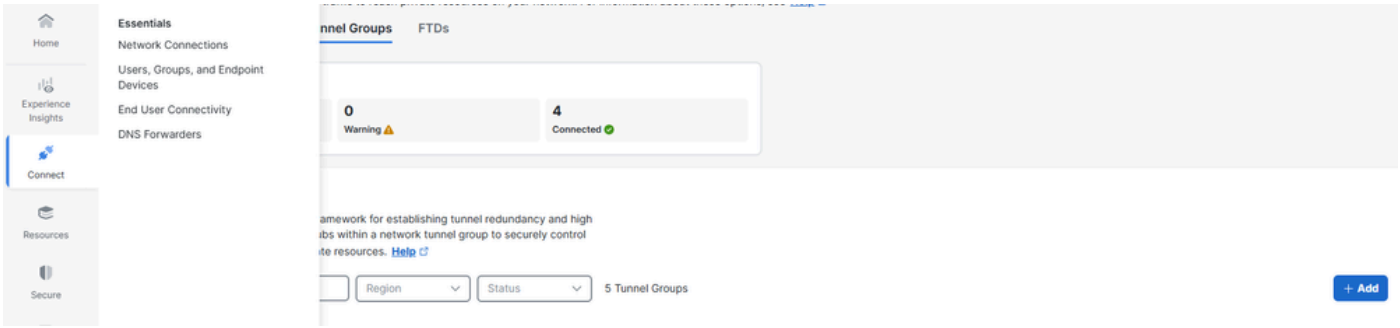
安全访问配置

网络隧道组配置

1.导航至“安全访问”的管理面板。

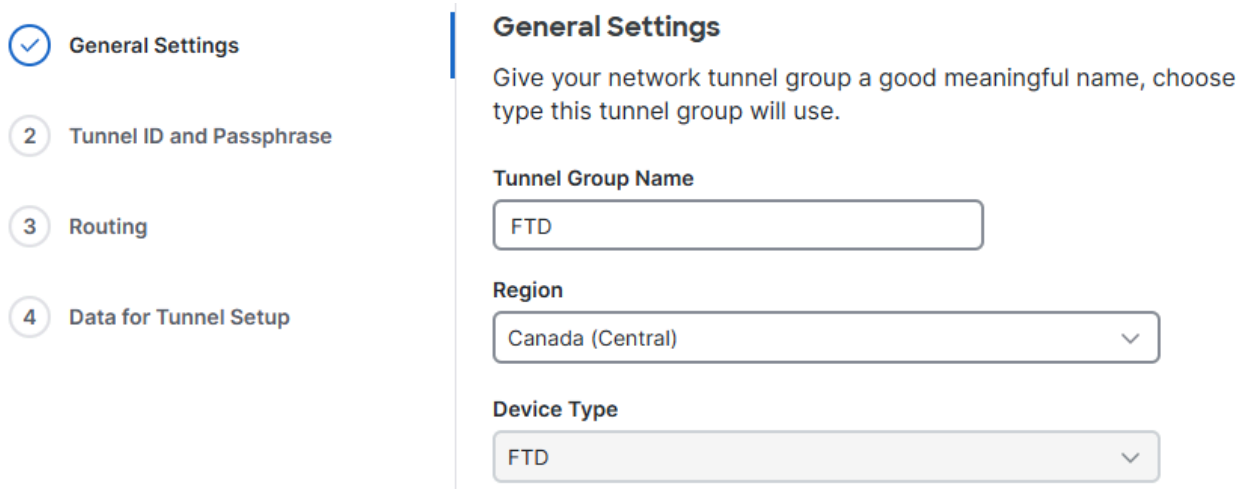
2.添加网络隧道组。

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



3.配置General Settings。

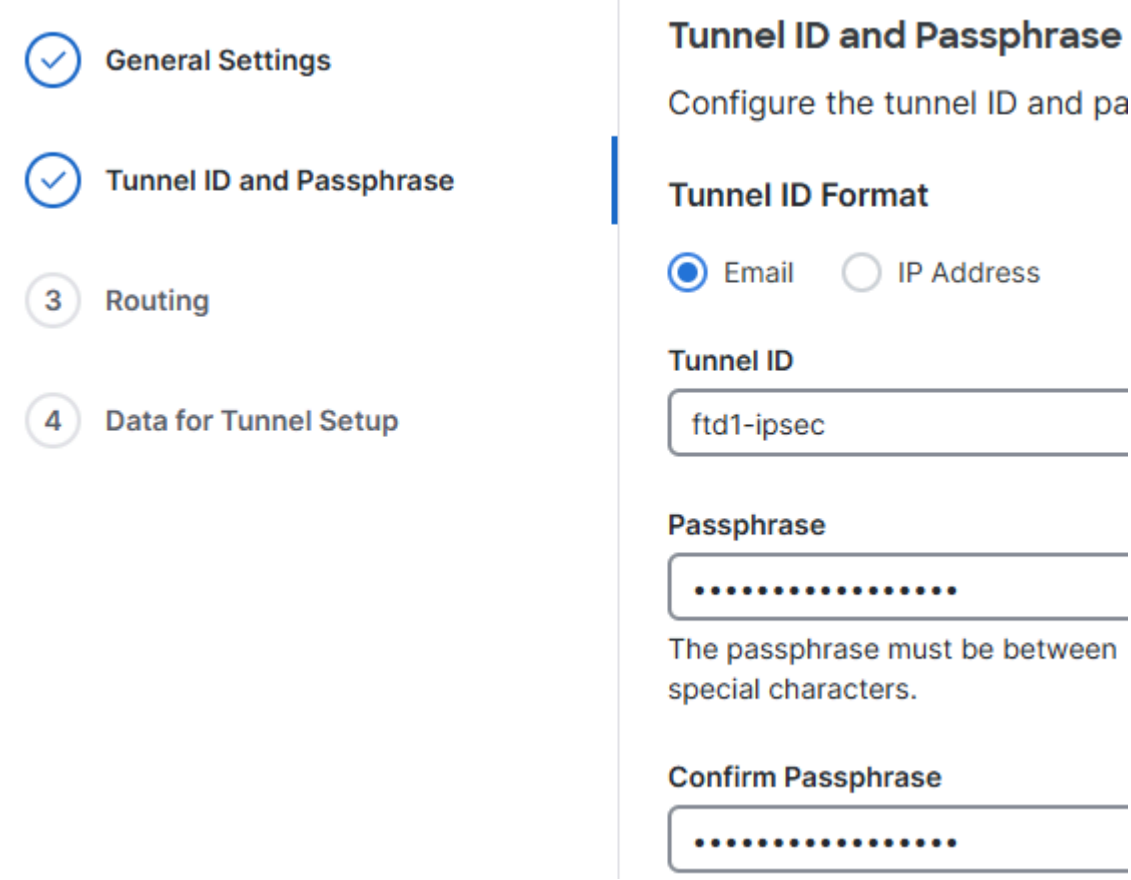
- 配置Tunnel Group Name,**Region** 和 Device Type
  - 点击 Next



常规设置

4.配置Tunnel ID和Passphrase。

- 配置和**Tunnel ID**Passphrase。此ID很重要，因为FTD配置需要此ID
- 点击 Next



ID和PSK

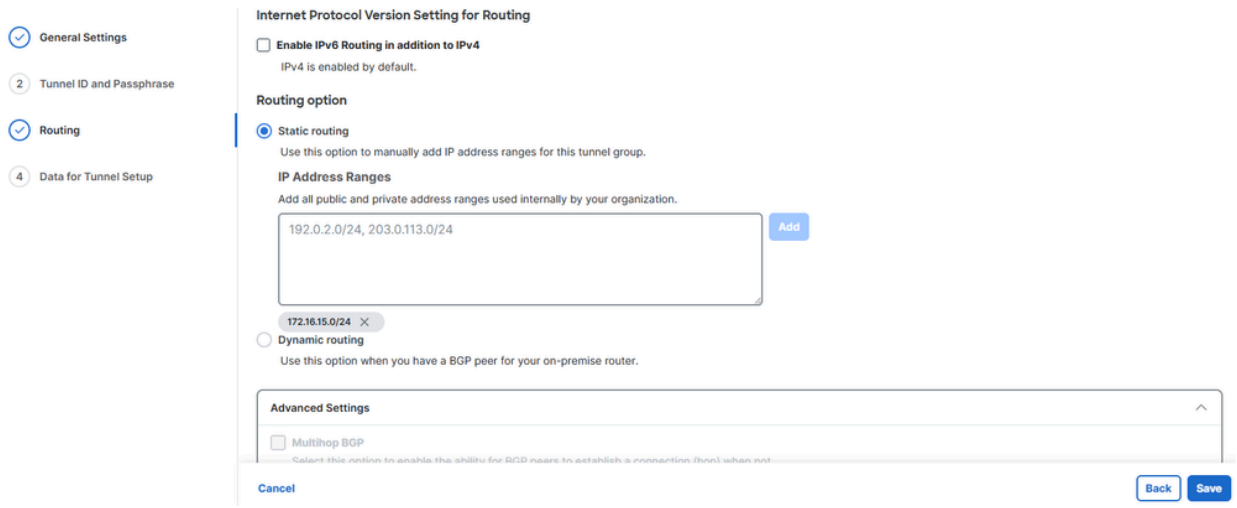
5.配置静态路由。

安全访问路由

基于策略的路由

添加希望远程用户通过ZTA和/或VPNaaS访问的FTD保护的网络，然后点击Save。

- 点击Routing> **Static routing**
  - 添加网络上已配置并希望通过安全访问传递流量的IP地址范围或主机，然后单击Add
  - 点击Save

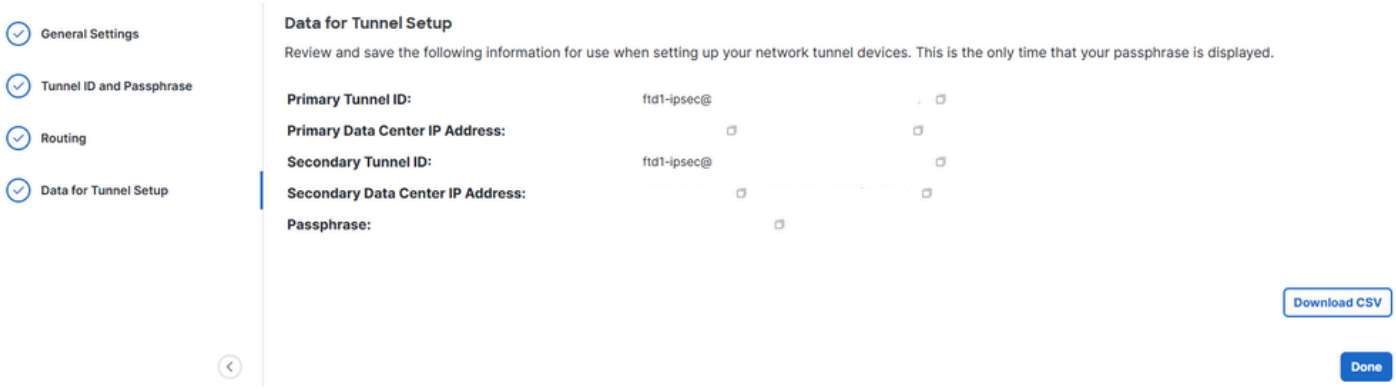


CSA静态路由

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



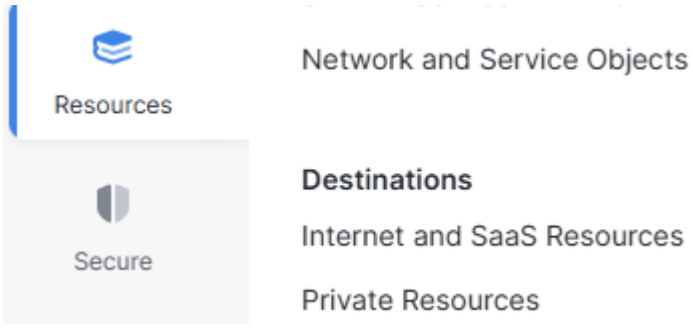
NTG数据

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。

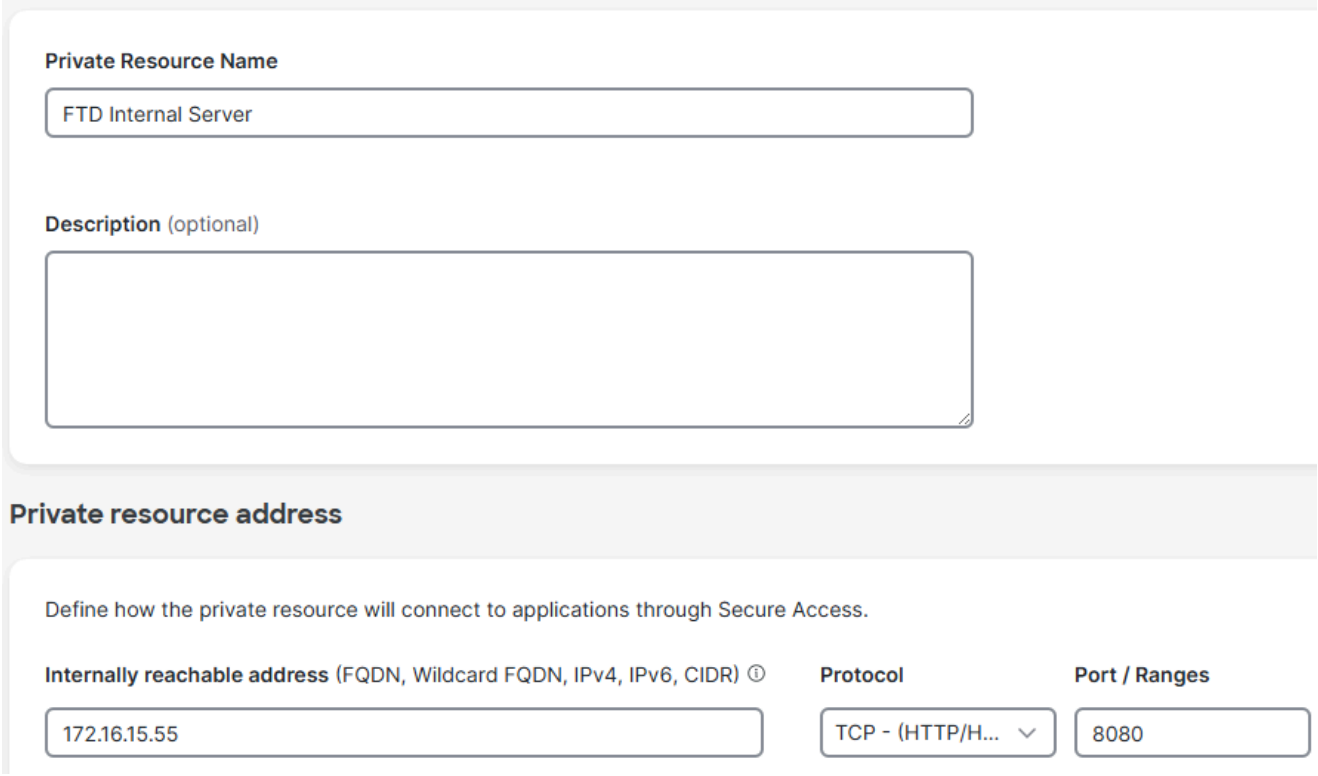
通过将它们定义为Secure Access中的专用资源，您可以通过零信任访问(ZTA)或VPN即服务(VPNaaS)等解决方案启用受控访问。 这可确保用户根据身份、设备状况和访问策略安全地连接到内部系统，而无需将资源直接暴露到互联网。

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
- 点击 Save



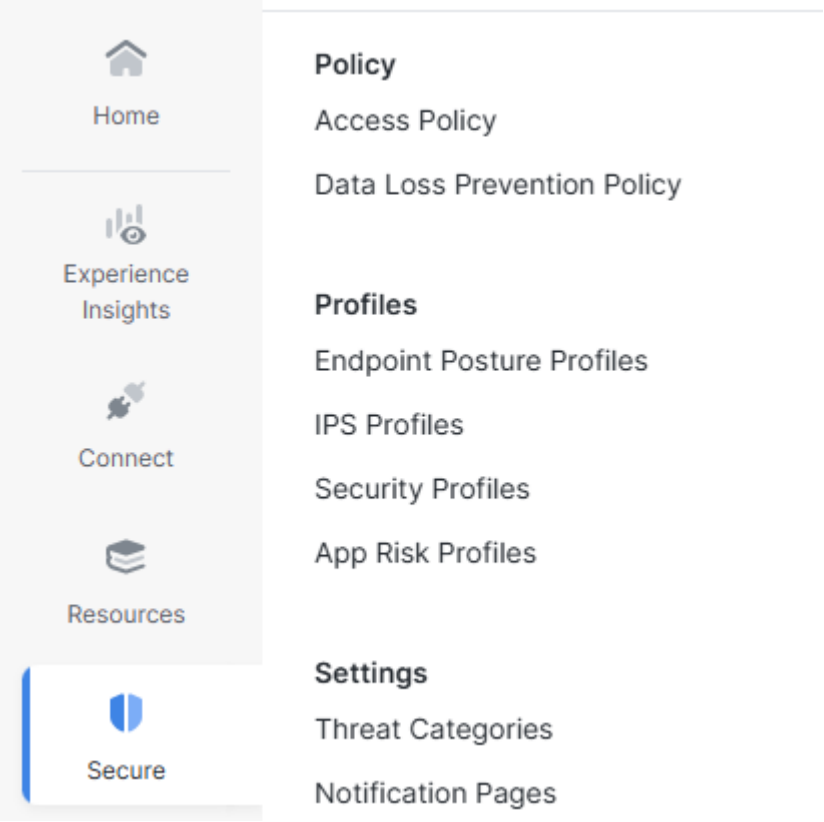
专用资源

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。

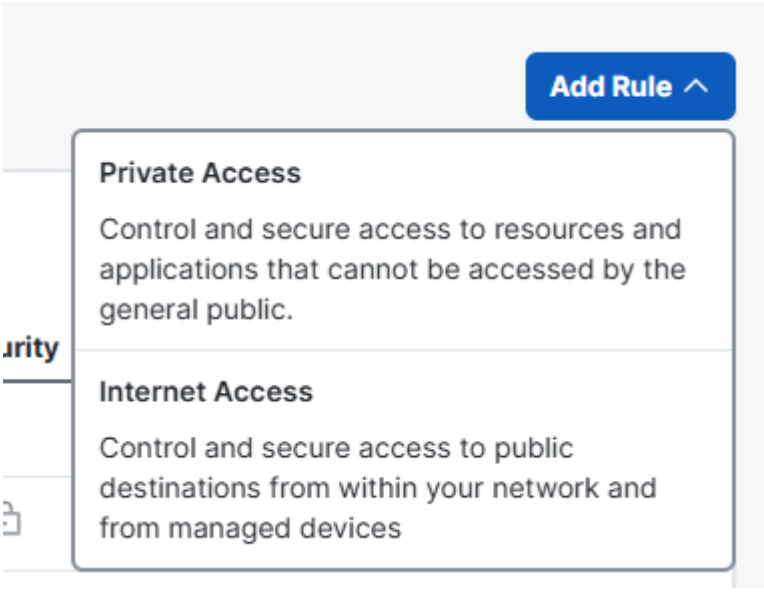
这些规则通过根据用户身份、组成员身份、设备状态、位置或其他策略条件等因素控制谁可以访问特定私有资源来实施安全性。这可确保敏感的内部系统免受一般公共访问的影响，同时仍可通过ZTA或VPNaaS安全地供授权用户使用。

依次导航至 Secure>Access Policy



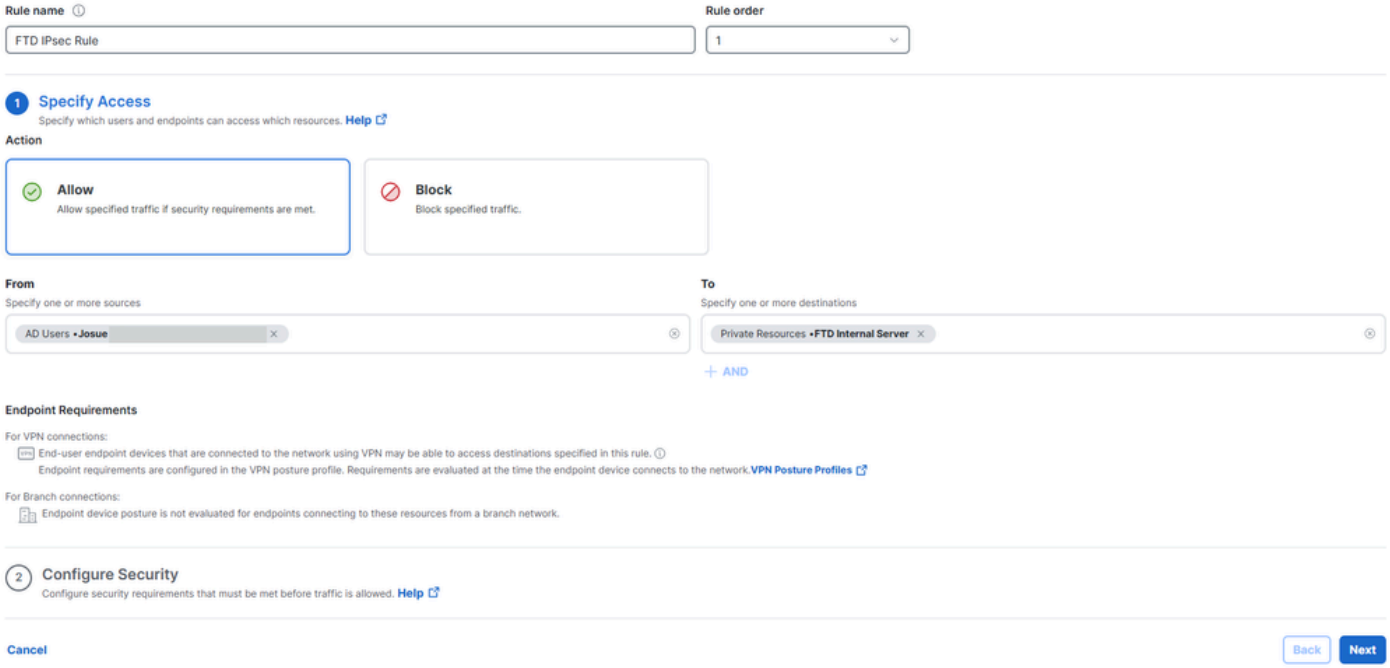
ACP

- 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Fromon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



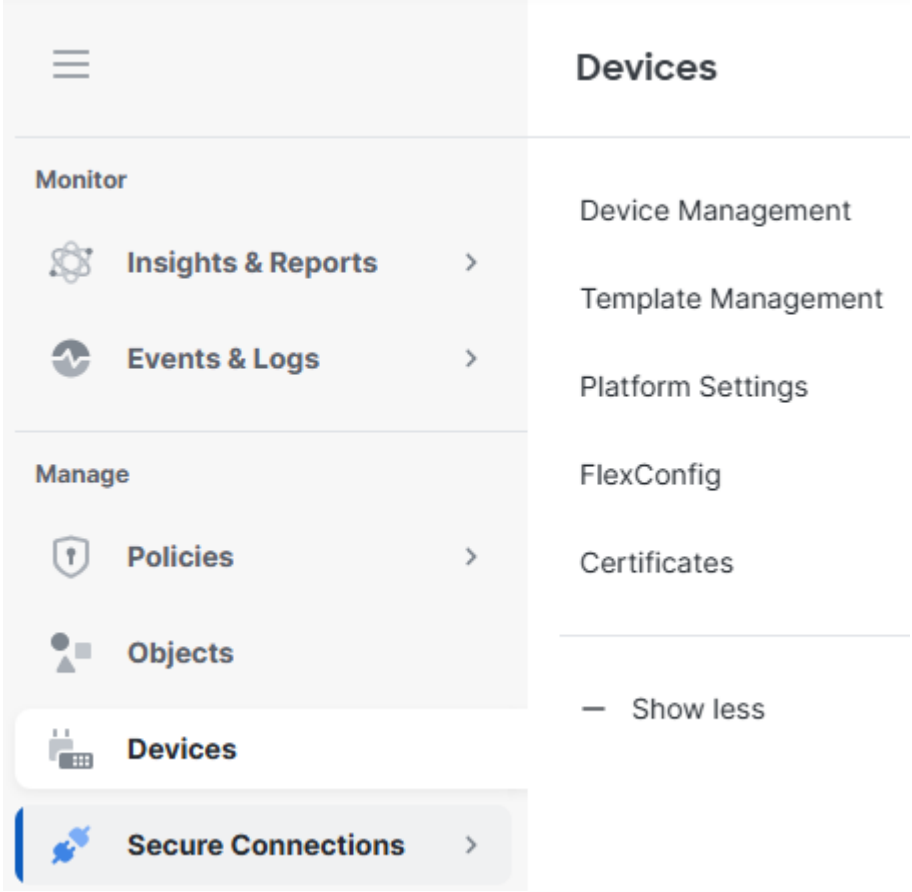
ACP配置

安全防火墙威胁防御(FTD)配置

虚拟隧道接口配置

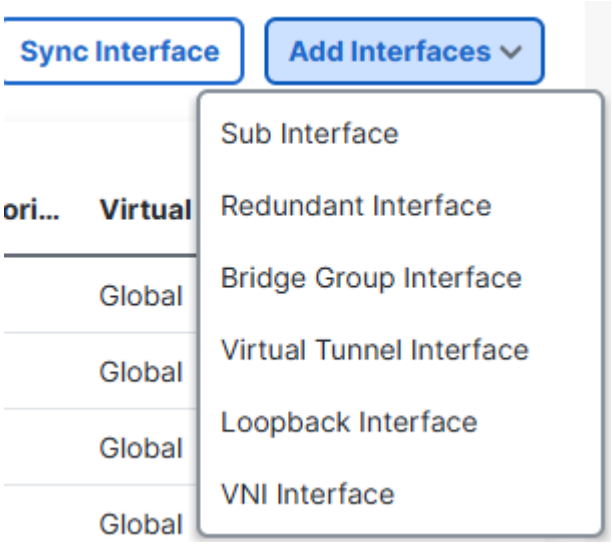
FTD上的虚拟隧道接口(VTI)是用于配置基于路由的IPsec VPN隧道的逻辑第3层接口。

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

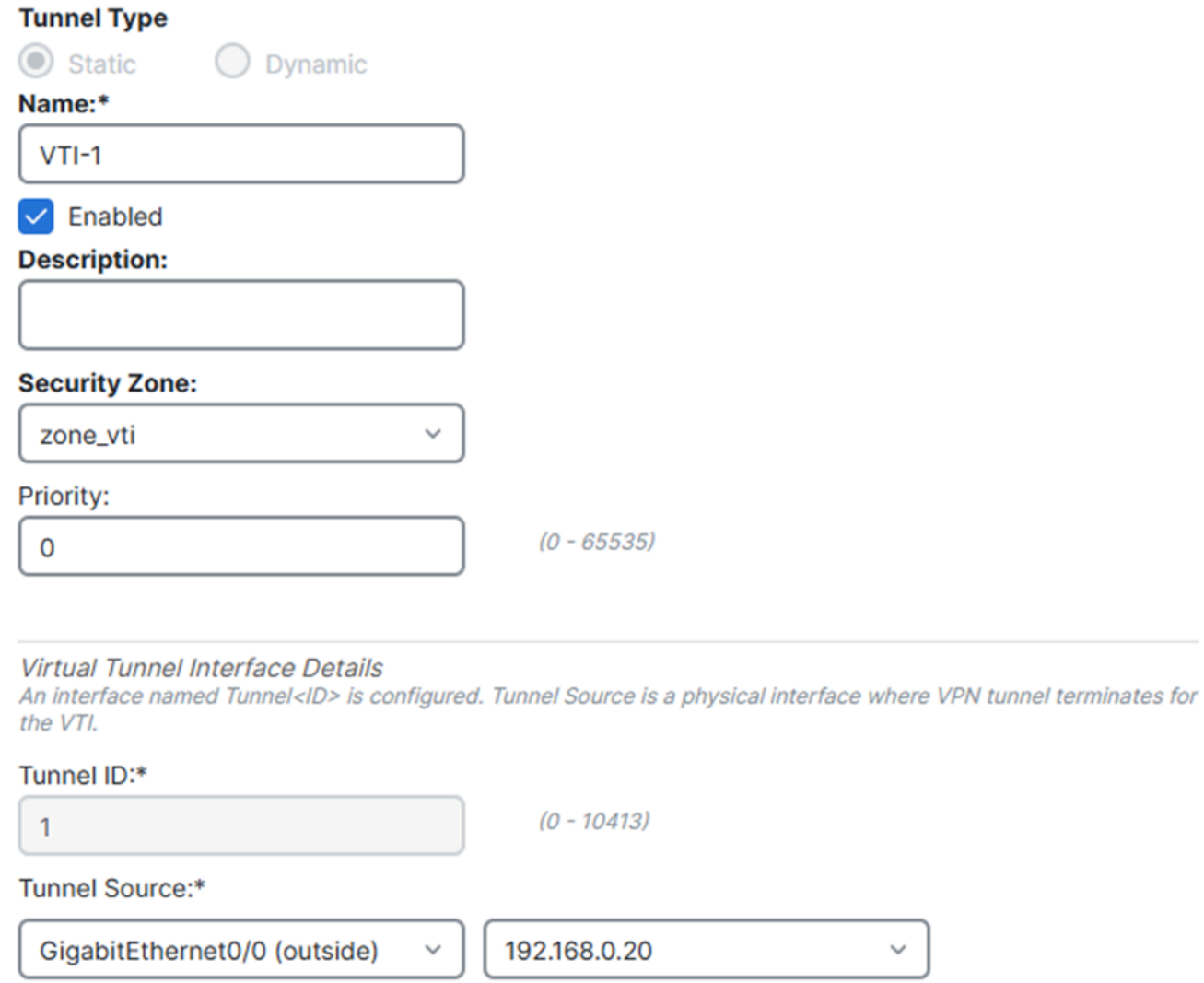


添加VTI

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

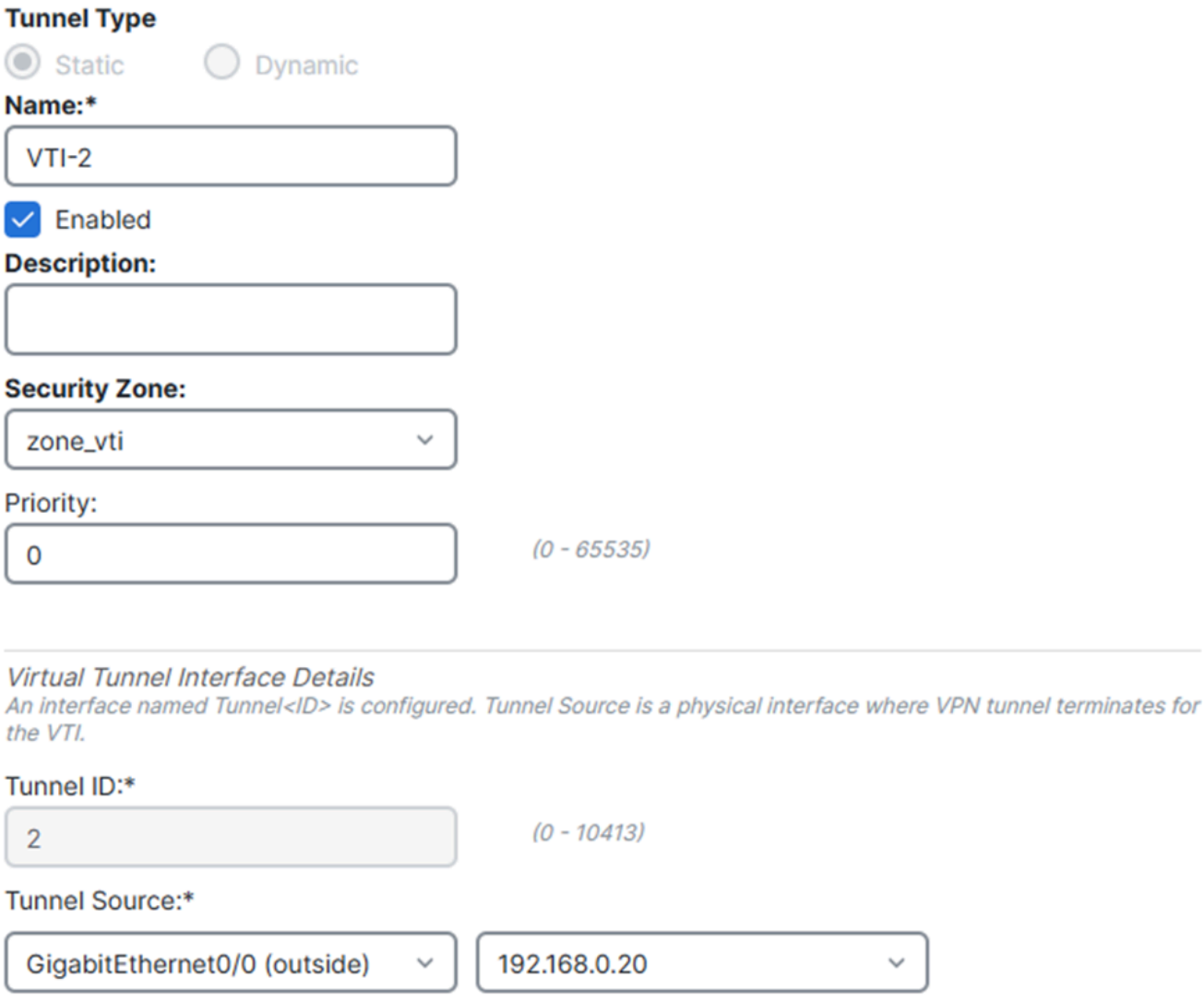


VTI1.1

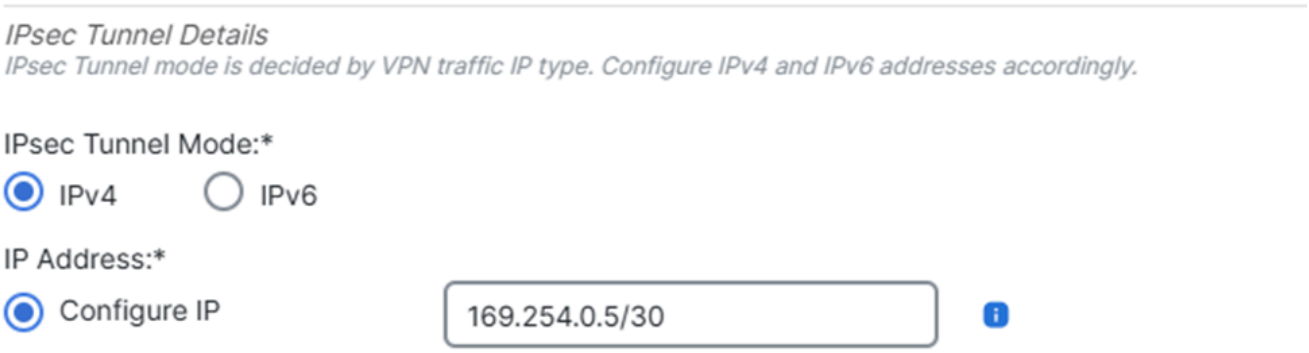
VTI1.2

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

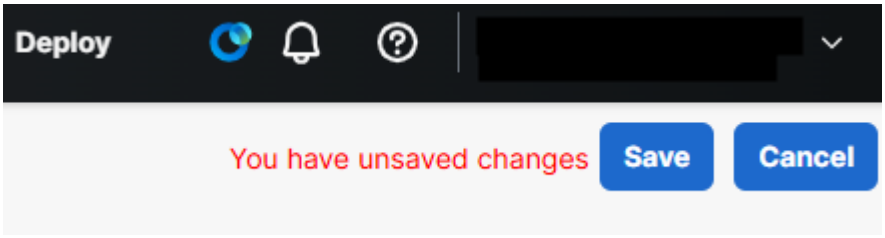


VTI2.1



VTI2.2

- 单击Save。

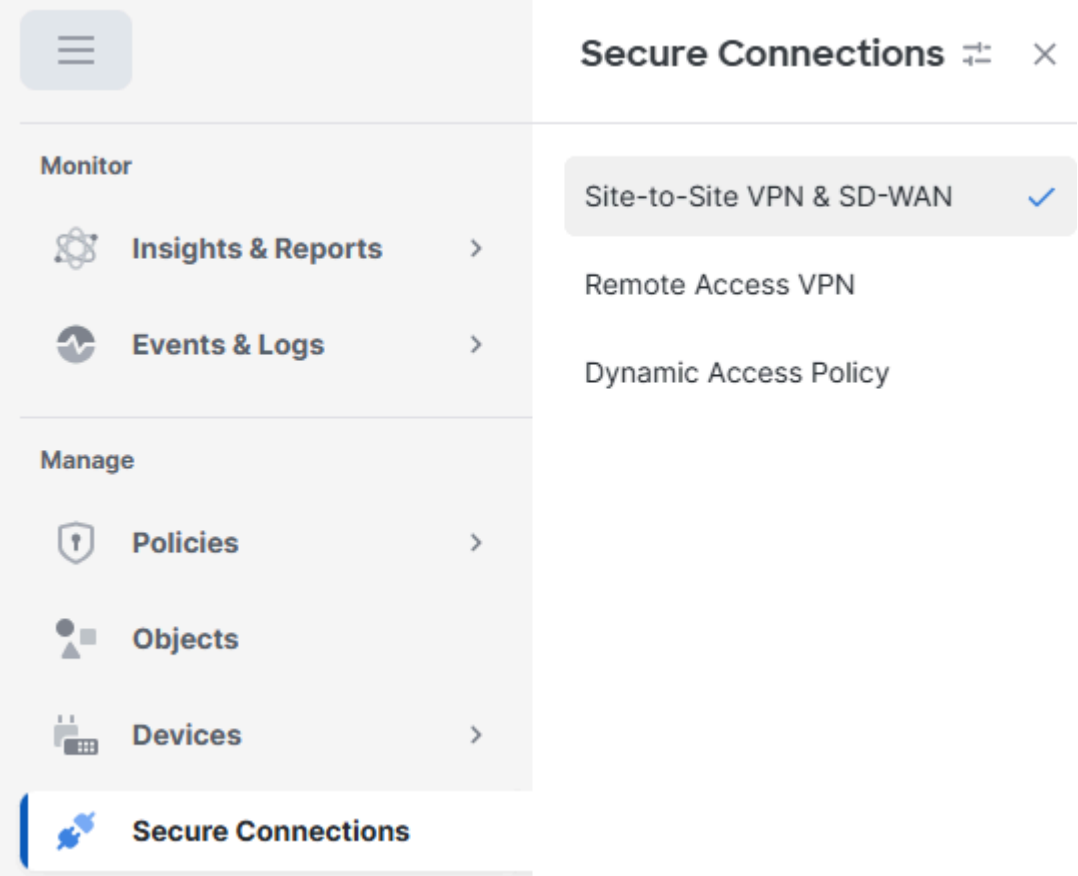


保存VTI更改

IPsec隧道配置

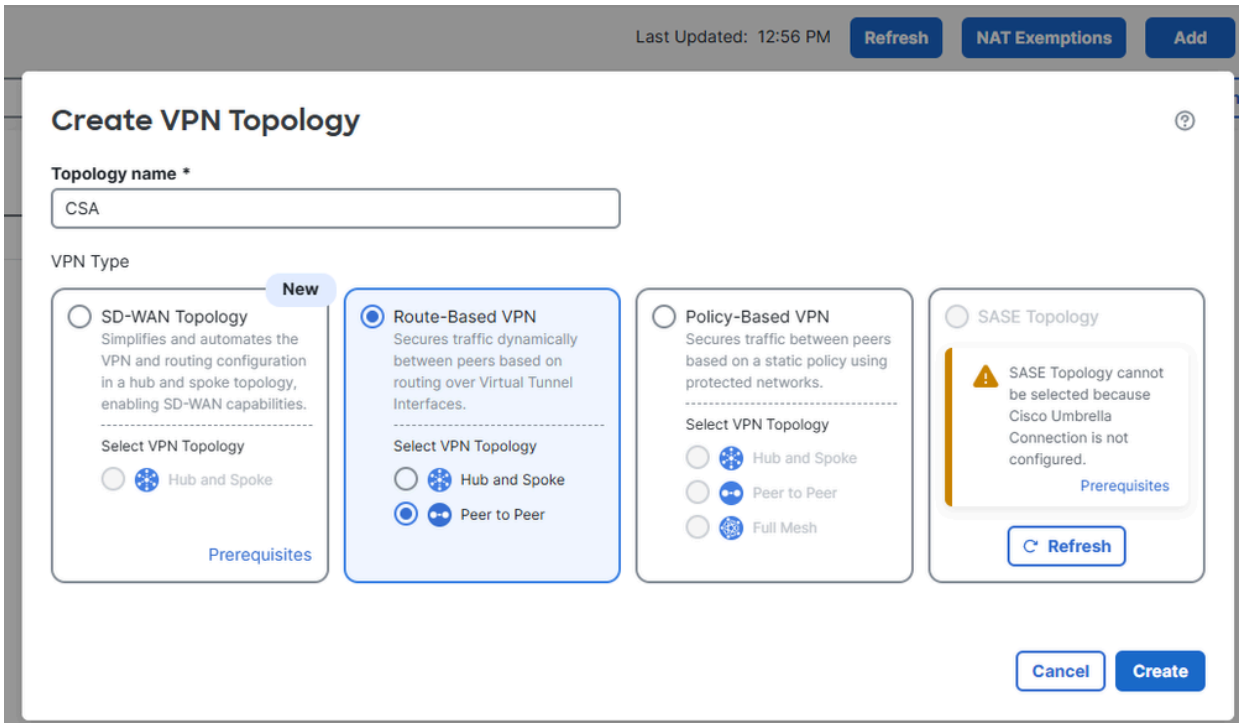
导航到您的cdFMC控制面板。

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



S2

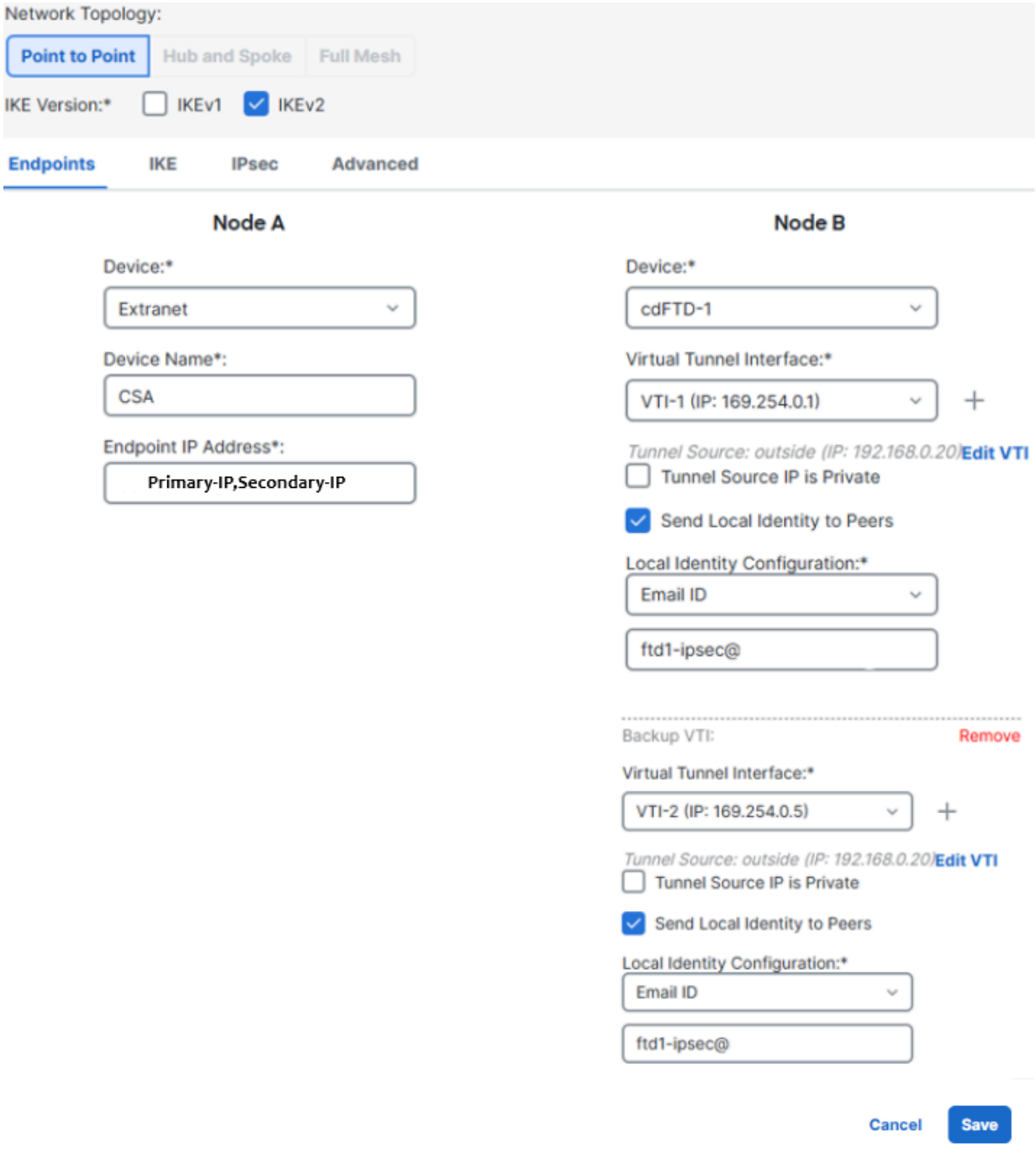
- 点击Add
  - 点击 Route-Based VPN
  - 点击 Peer to Peer



添加VPN

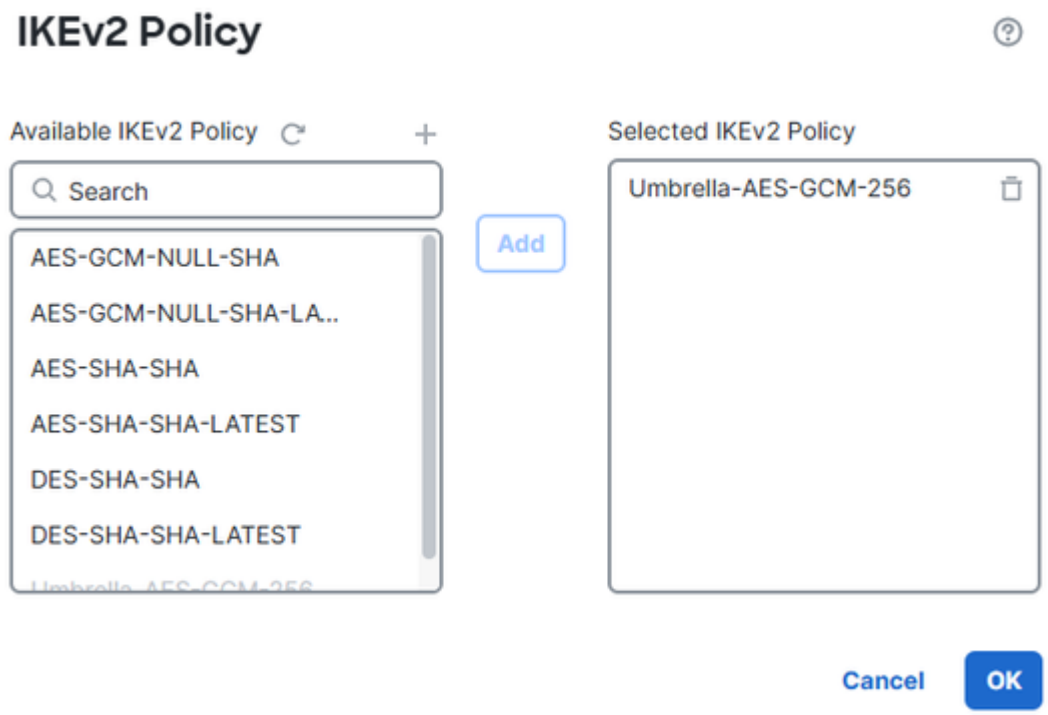
- 从安全访问配置的第5步获取主要和辅助数据中心的隧道ID和IP地址

- 点击Endpoints
  - 在Node A下，单Device击on并选择 Extranet
  - 点击Device Name并为其命名
  - 点击Enpoint 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，点击Device并选择FTD设备
  - 点击Virtual Tunnel Interface，选择上一步中创建的第一个VTI接口
  - 点击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）
  - 点击 Add Backup VTI
  - 点击Virtual Tunnel Interface，选择上一步中创建的第二个VTI接口
  - 单击Send Local Identity to Peersonoption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



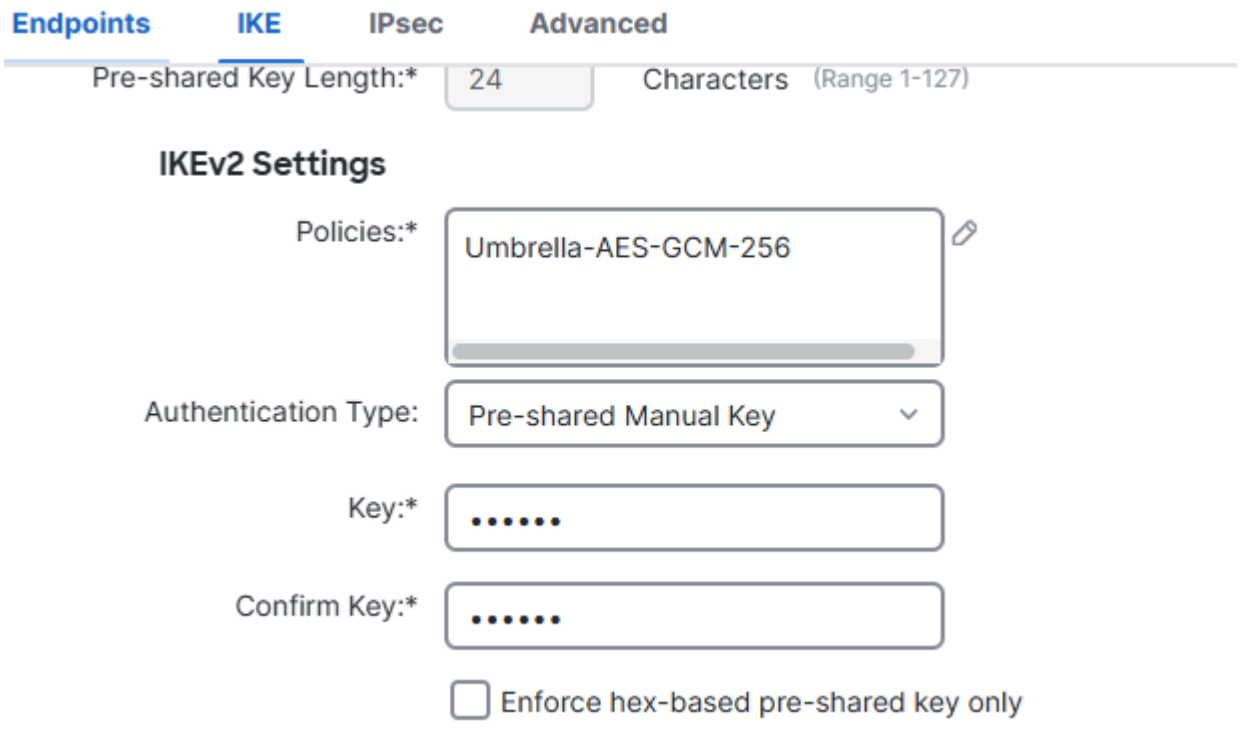
FTD VTI配置

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



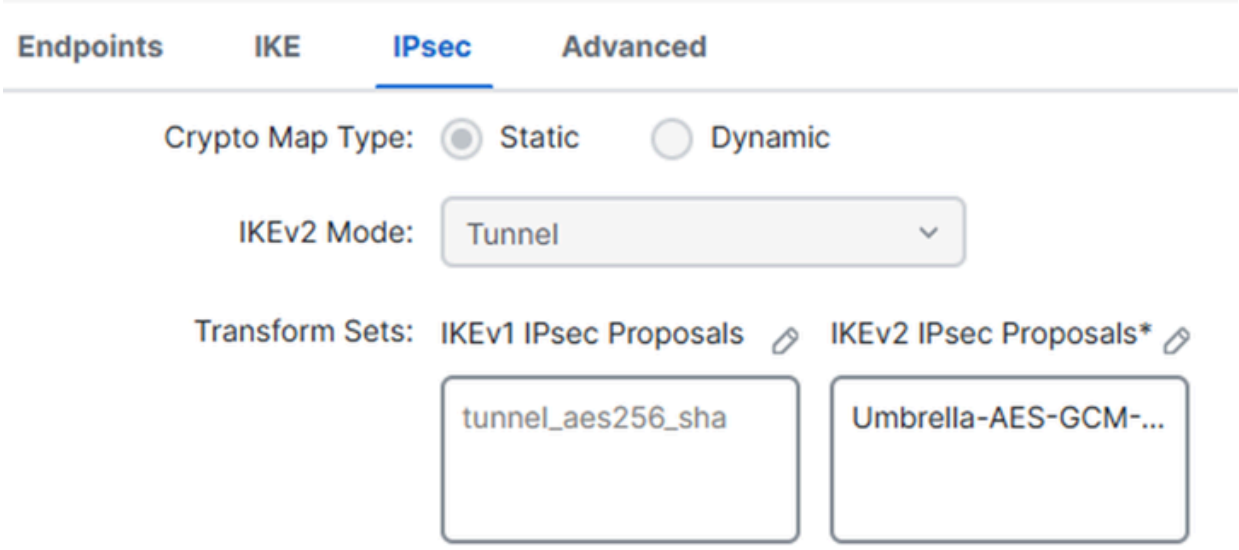
IKEv2策略

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



IKE

- 点击 IPSEC
  - 点击 IKEv2 Proposals
  - 选择 Umbrella-AES-GCM-256
  - 点击 OK



IPsec

保存IKEv2提议

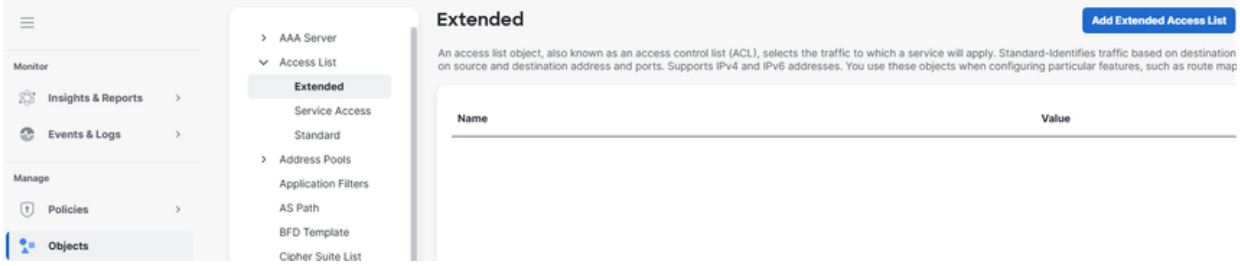
FTD路由配置

基于策略的路由(PBR)允许您根据目标IP地址以外的条件来控制流量转发。PBR可以基于源、应用、协议、端口或其他定义的策略来路由流量，而不是仅依赖路由表。

这使组织能够通过首选链路（例如高带宽或直接互联网链路）控制特定或高优先级的流量，优化性能，并安全地隔离所选应用，而无需通过VPN隧道发送所有流量。

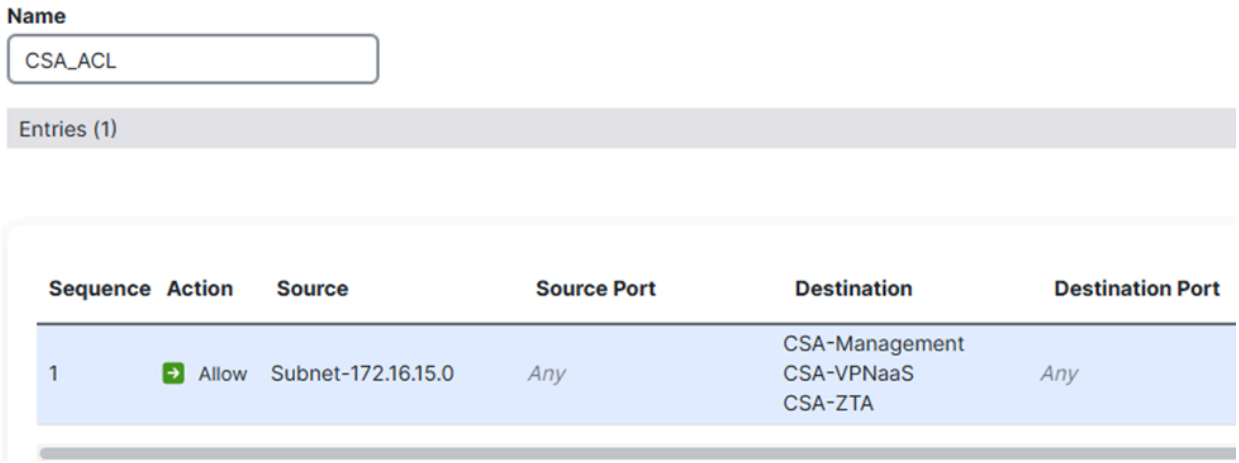
基于策略的路由

- 依次导航至 Objects
  - 点击 Access List
  - 点击 Extended
  - 点击Add Extended Access List



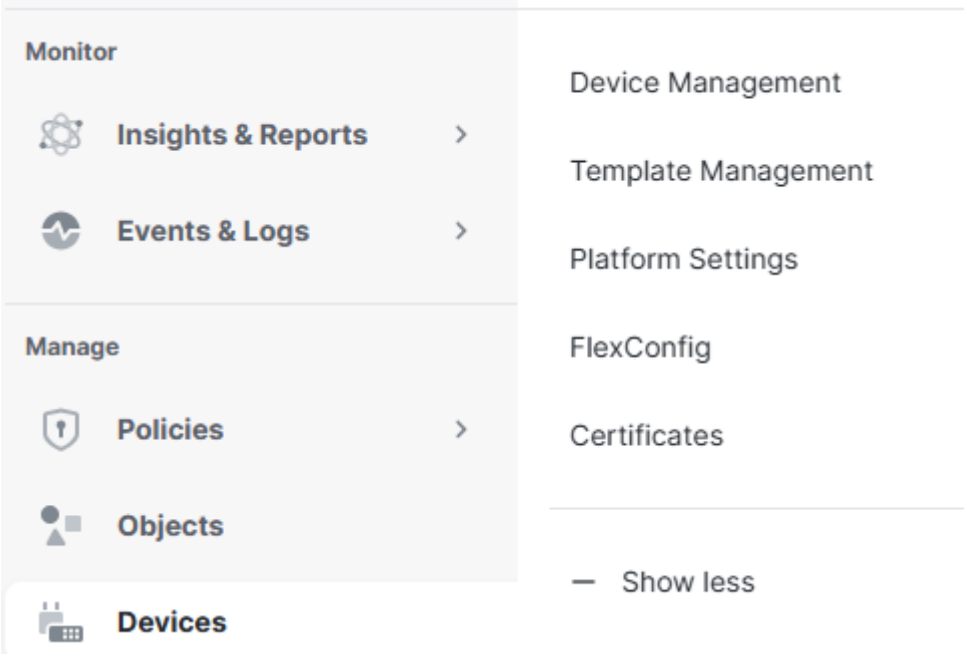
添加ACL

创建与要通过隧道发送的FTD(例如，172.16.15.0/24)保护的源网络匹配的扩展访问控制列表(ACL)。对于目标，添加ZTA使用的网络（CGNAT范围）和VPNaaS使用的网络（选中虚拟专用网络IP池）。



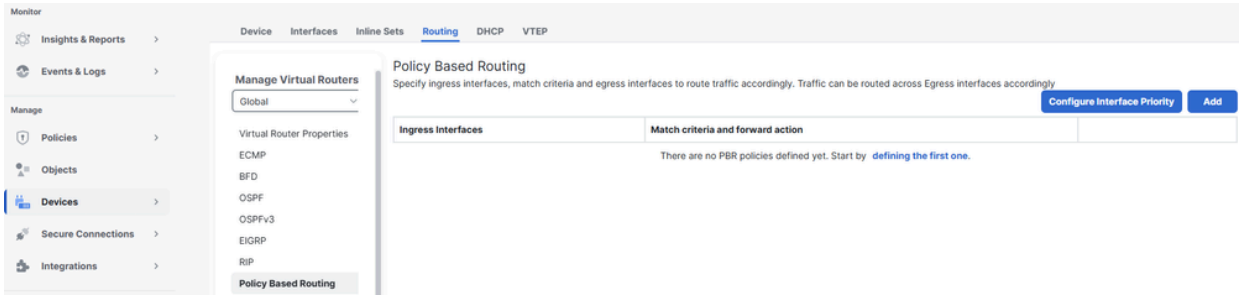
ACL

- 点击Devices> Device Management



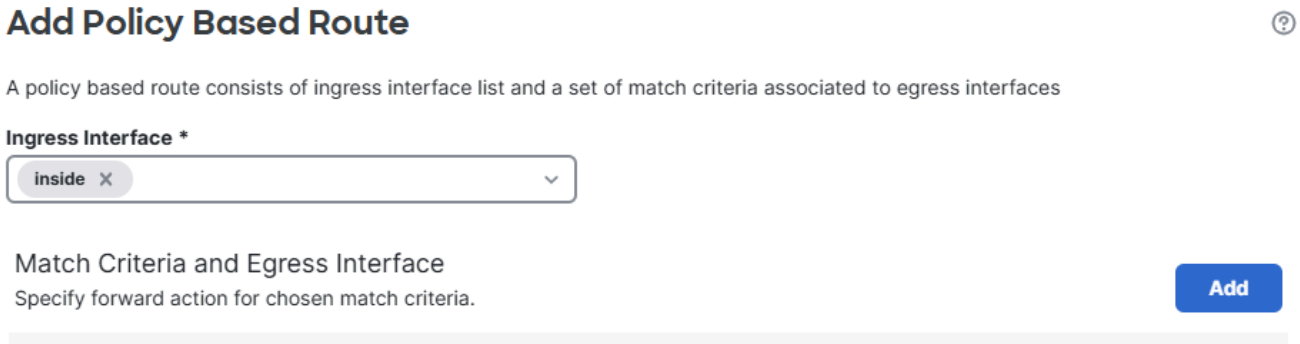
设备

- 点击FTD
  - 点击Routing
  - 点击 Policy Based Routing
  - 点击 Add



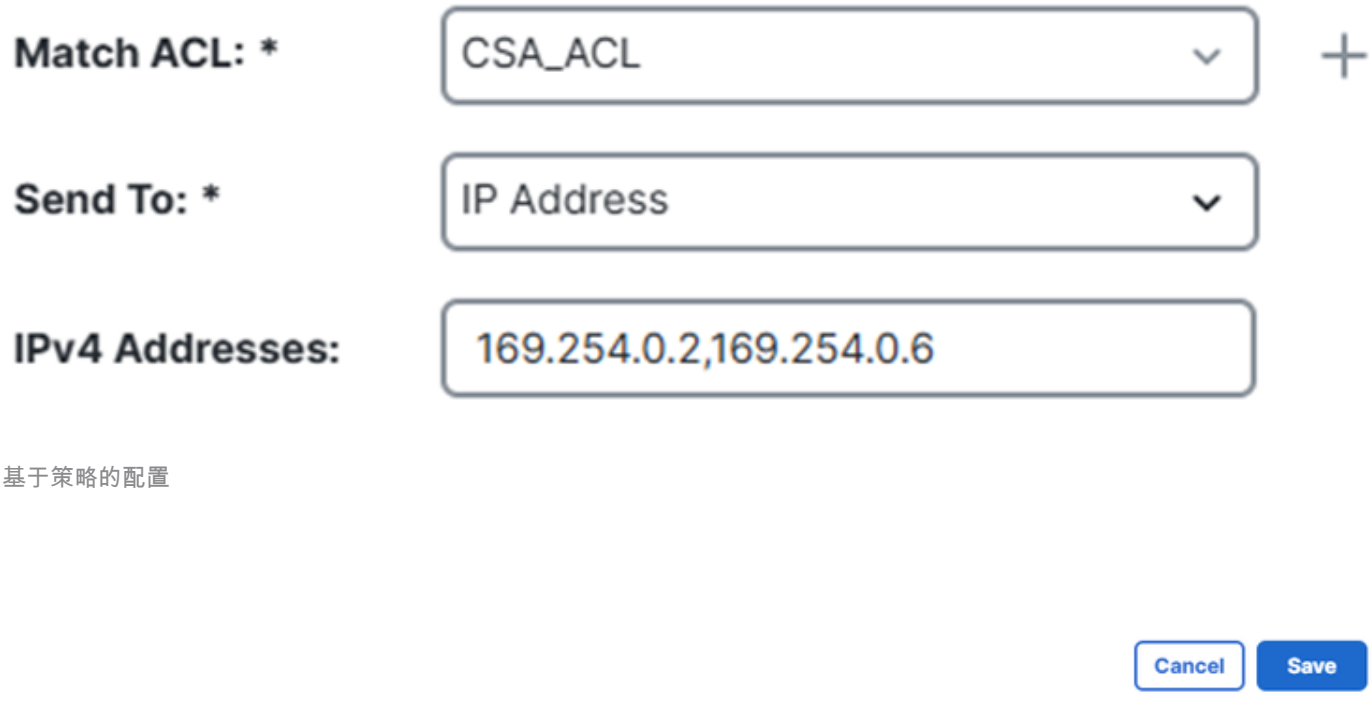
添加PBR

- 点击Ingress Interface，选择来自内部网络的流量进入的入口接口
- 在Match Criteria and Egress Interface下，点击 Add



Ingress 接口

- 点击Match ACL，选择之前创建的扩展ACL
- 点击 Send To and select IP Address
- 点击IPv4 Addresses，将之前在FTD中配置的VTI接口子网内的IP地址（169.254.0.2和169.254.0.6）设置为下一跳
- 点击 Save



基于策略的配置

保存PBR

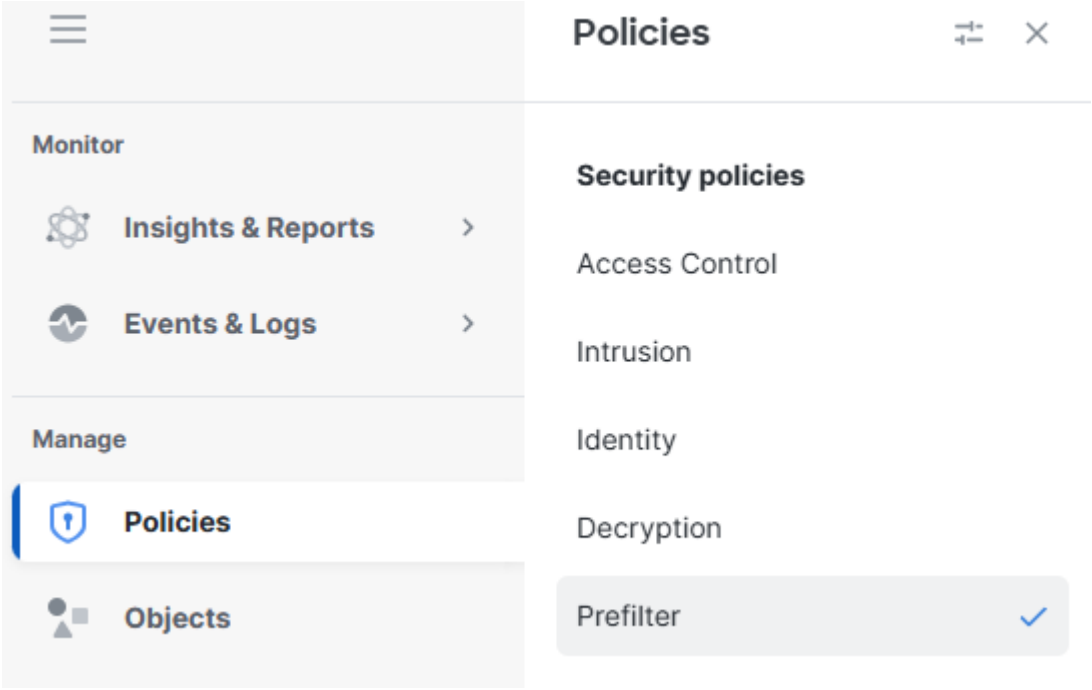
确保选择Send To >选项IP Address ，而不是该选Egress Interface项。

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

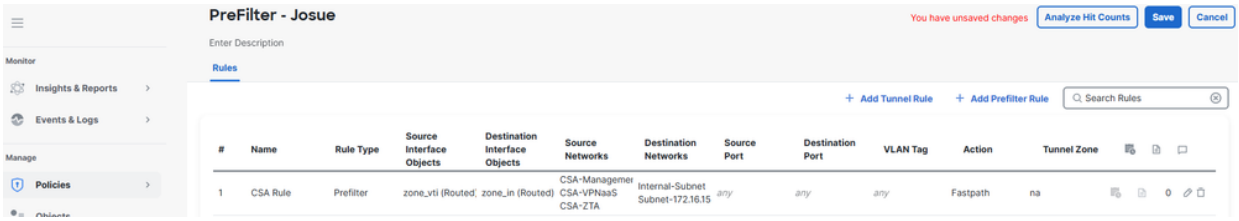


预过滤器

- 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隧道成功建立，确认已建立与专用资源的安全连接。

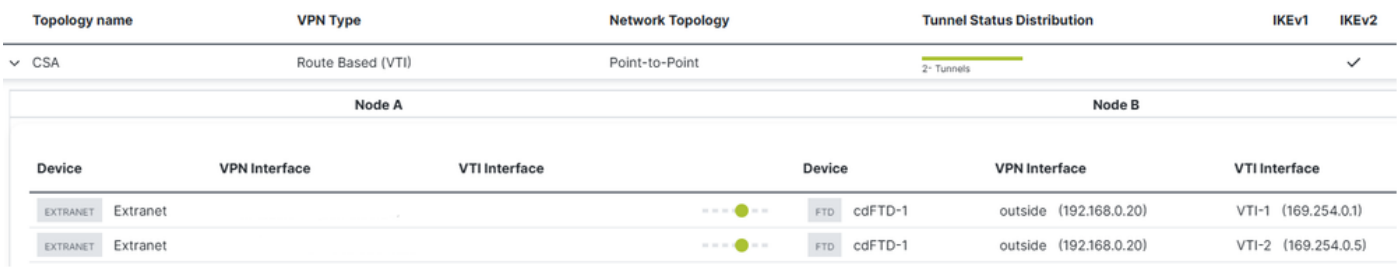
验证

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Topology Name。



FTD隧道状态

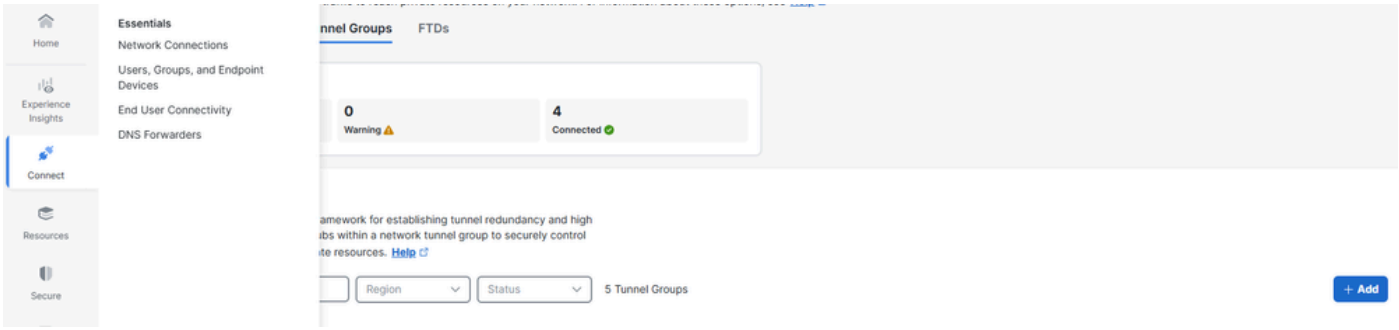
在安全访问中验证

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。

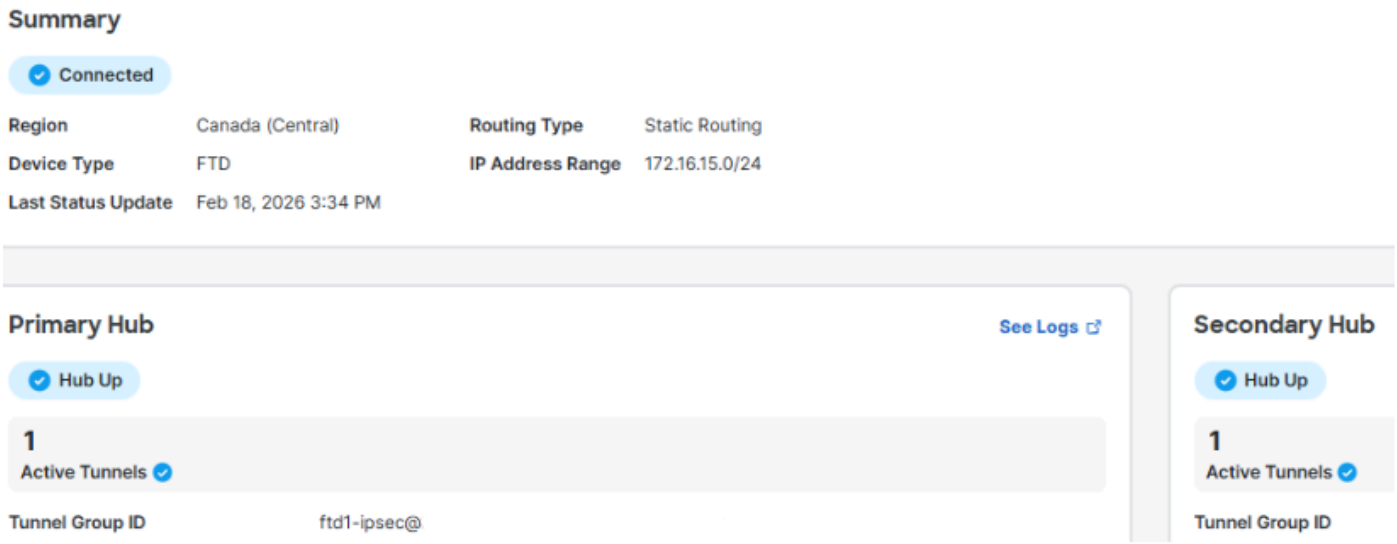
- 单击Connect > Network Connections

- 单击Network Tunnel Groups



检查NTG

- 点击网络隧道组

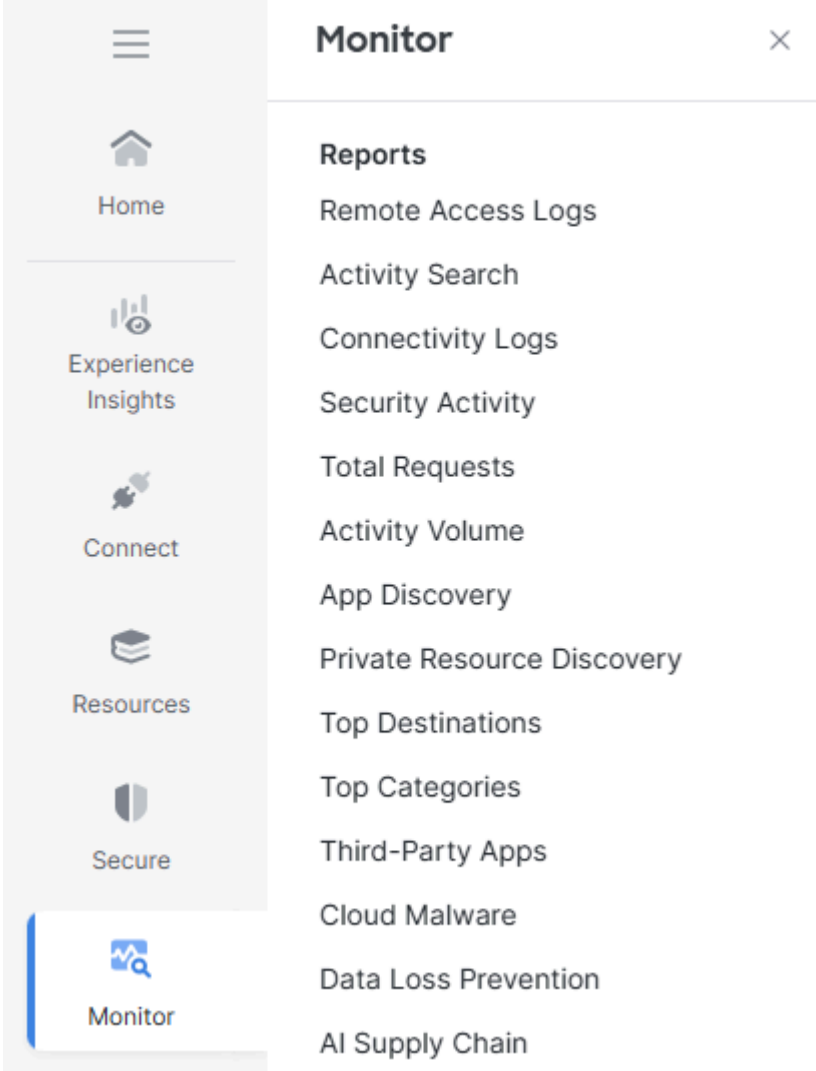


CSA隧道状态

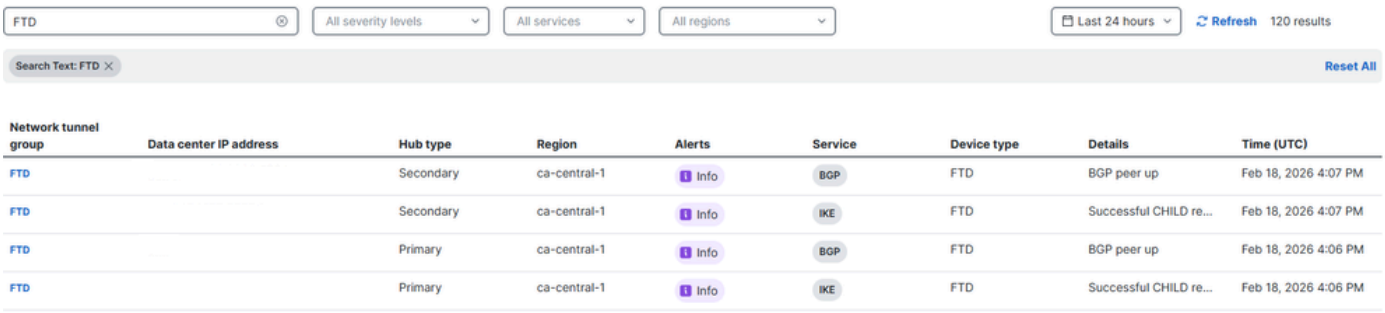
安全访问中的事件

您可以查看Tunnel事件，并确认IPsec隧道的状态是否为up且稳定。

单击Monitor > Network Connectivity。

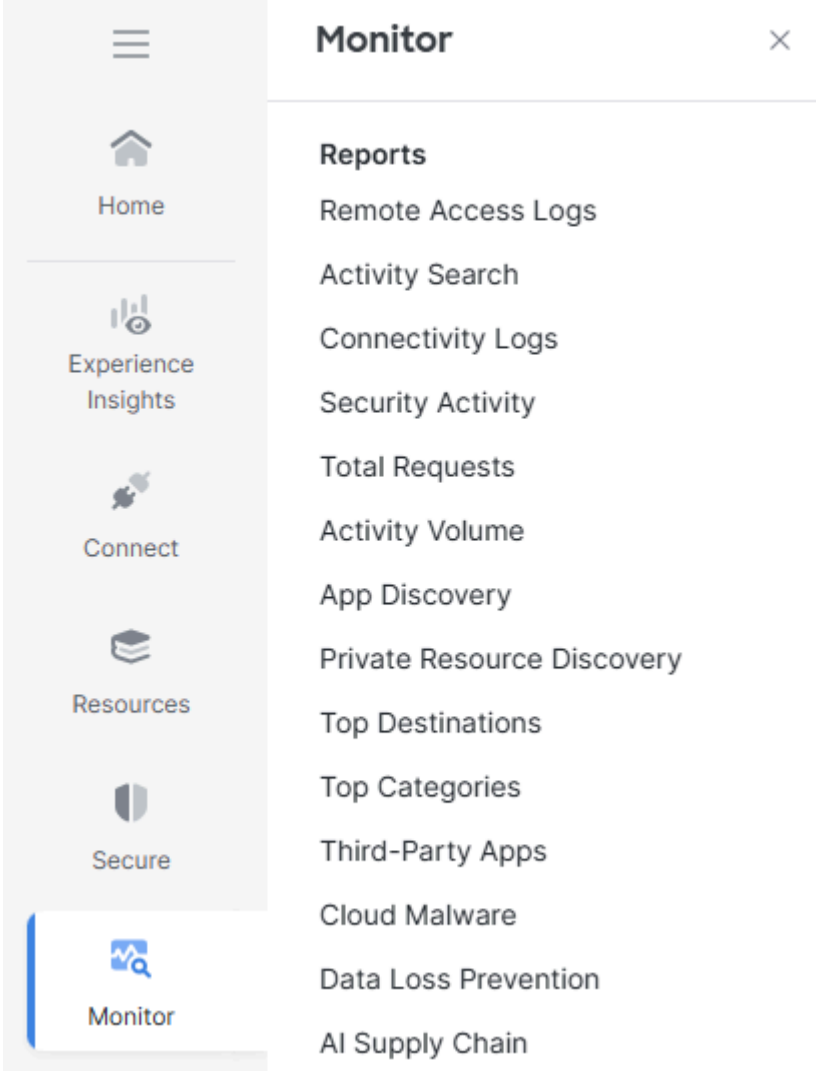


监控连接日志



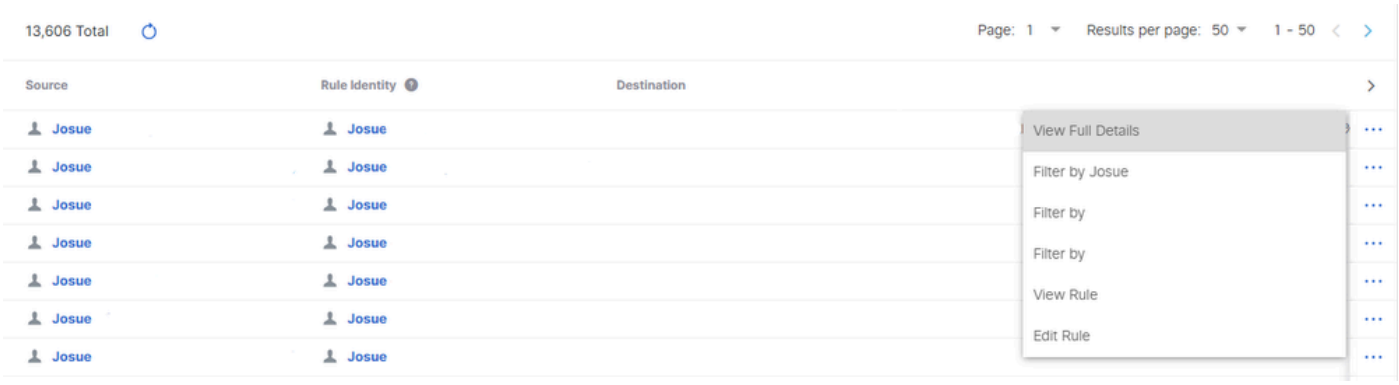
连接日志

导航至监控 > 活动搜索。

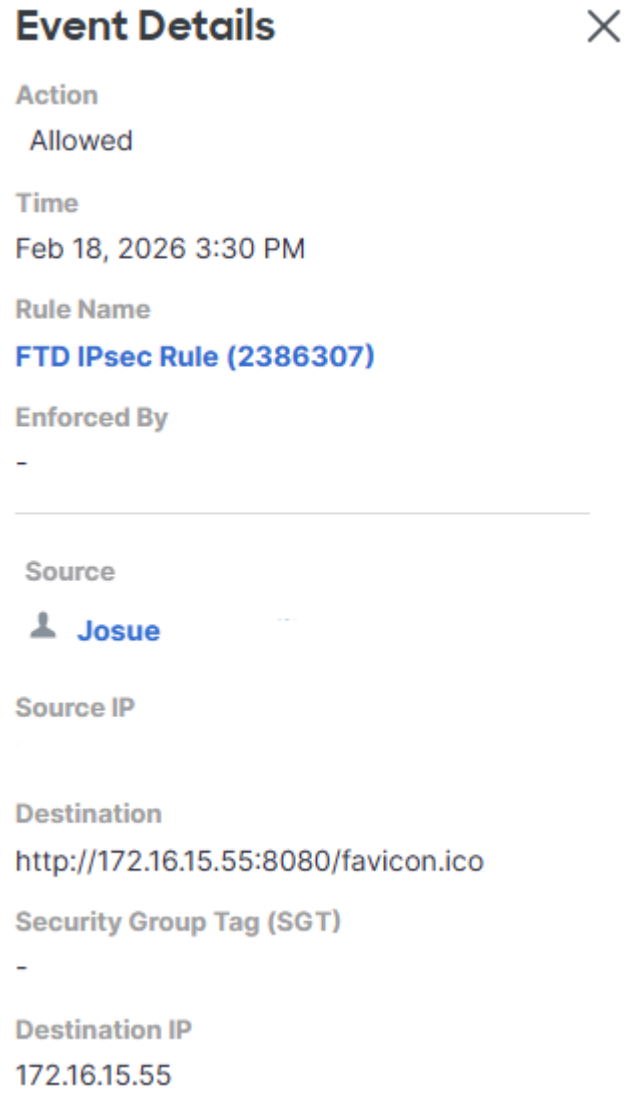


监控连接日志

在任何相关事件上，点击查看完整详细信息。



完整详情



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）。