使用基於策略的路由為專用訪問配置使用安全防火牆威脅防禦的安全訪問

目錄

簡介

本檔案介紹如何透過IPsec使用FTD設定安全存取，以使用基於原則路由實現安全私人存取。

必要條件

需求

- 思科安全訪問知識
- 思科安全訪問控制面板/租戶

- 安全防火牆威脅防禦和防火牆管理中心知識
- IPsec知識
- 基於策略的路由知識

採用元件

- 運行7.7.10代碼的安全防火牆
- 雲交付的防火牆管理中心。配置也適用於典型的虛擬FMC
- Cisco Secure Access控制面板

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

安全訪問中的網路隧道可用於兩個主要用途：安全的網際網路訪問和安全專用訪問。

對於安全專用訪問，組織可以利用零信任訪問(ZTA)和/或VPN即服務(VPNaaS)將使用者連線到專用資源（如內部應用程式或資料中心）。IPsec隧道在此架構中扮演著重要角色，它安全地加密使用者和私有資源之間的網路流量，確保敏感資料在穿越不受信任的網路的過程中始終受到保護。通過將IPsec隧道與ZTA或VPNaaS整合，組織可以無縫安全地訪問內部資源，同時保持強大的安全控制和可視性。

本檔案介紹如何透過IPsec為安全私人存取設定使用安全防火牆威脅防禦(FTD)的安全存取。
此外，本指南還提供了配置基於策略的路由的步驟。

雖然本文檔介紹為安全專用訪問配置IPsec隧道，但設定零信任訪問(ZTA)或用於訪問專用應用程式的VPN即服務(VPNaaS)不在本指南範圍內。

設定

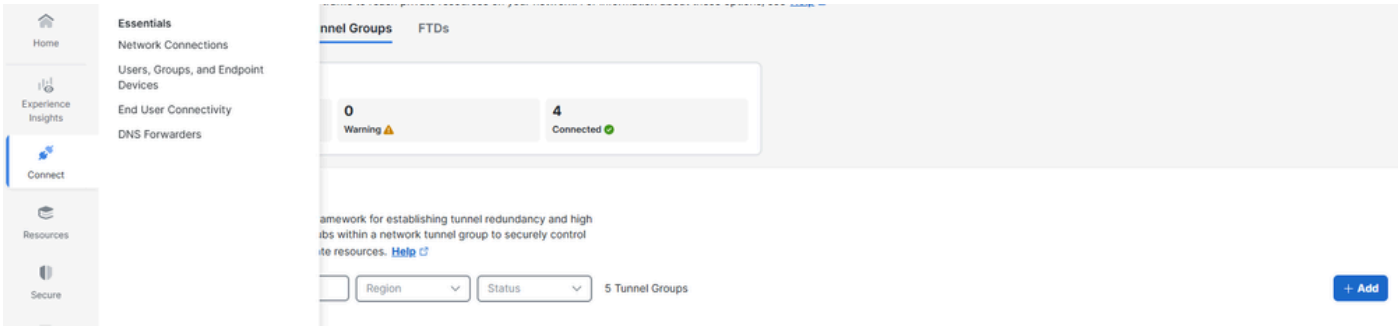
安全訪問配置

網路隧道組配置

1.導航到Secure Access的管理面板。

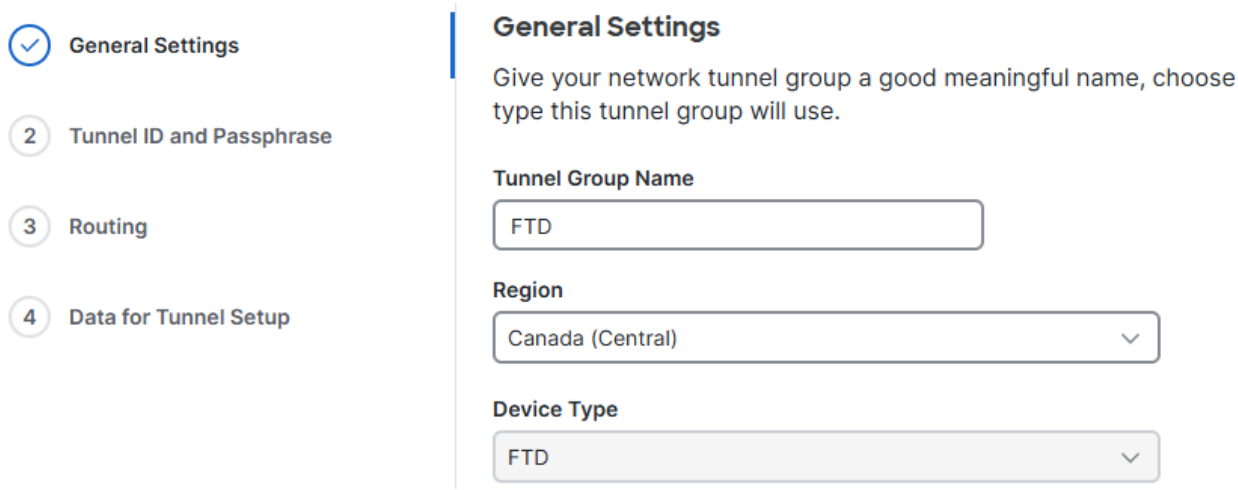
2.新增網路隧道組。

- 按一下Connect> Network Connections
  - 在Network Tunnel Groups下，按一下> Add



3.配置General Settings。

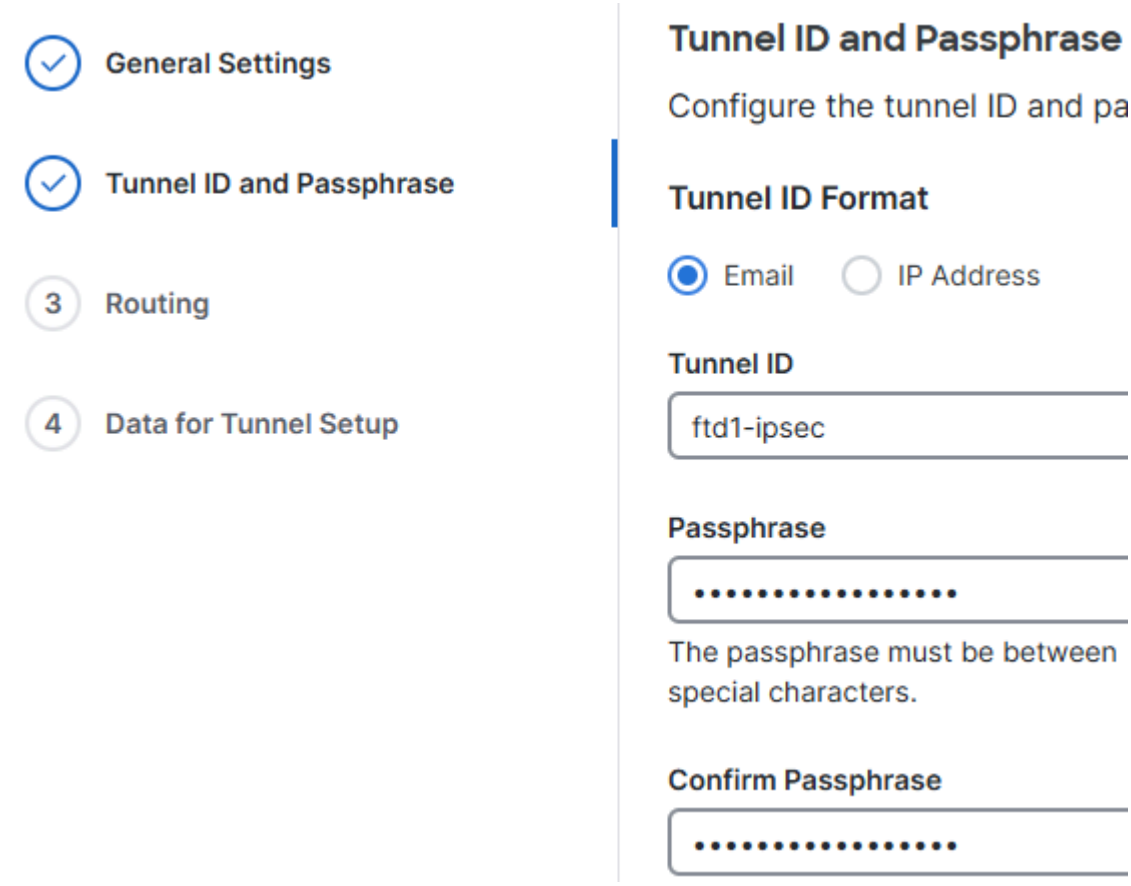
- 配置Tunnel Group Name，以**Region** 及 Device Type
  - 按一下 Next



常規設定

4.配置Tunnel ID和Passphrase。

- 設定和**Tunnel ID**Passphrase。此ID非常重要，因為FTD設定需要此ID
- 按一下 Next



ID和PSK

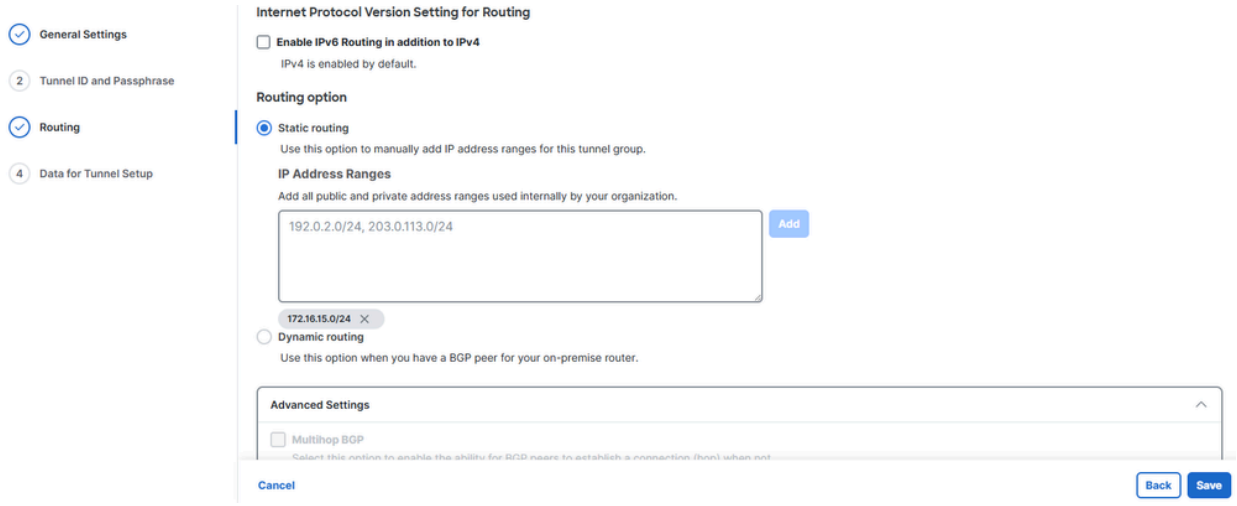
5.配置靜態路由。

安全存取路由

基於原則的路由

新增您想要遠端使用者通過ZTA和/或VPNaaS訪問的FTD保護的網路，然後點選Save。

- 按一下Routing> **Static routing**
  - 新增已在網路上配置且希望通過Secure Access傳遞流量的IP地址範圍或主機，然後按一下Add
  - 按一下Save

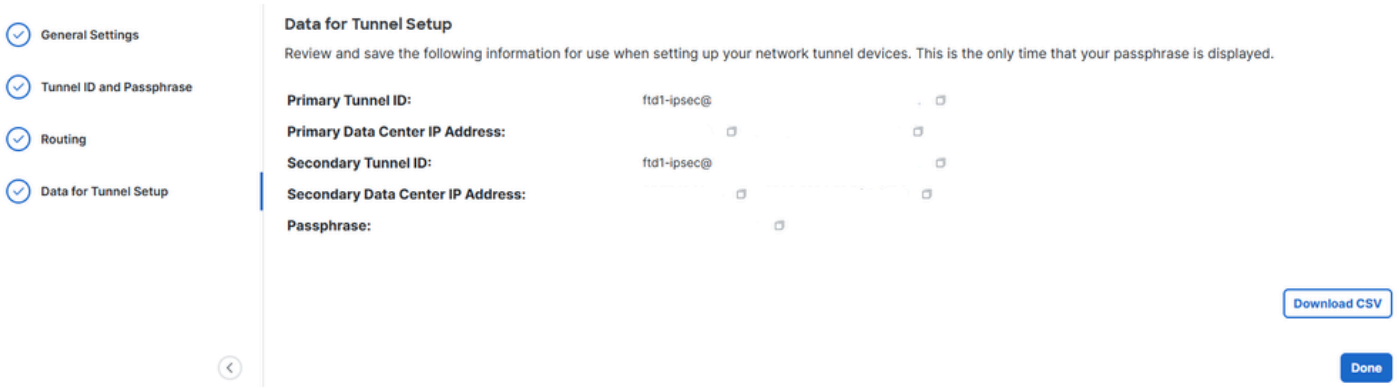


CSA靜態路由

儲存網路隧道組配置

下載並儲存通道設定資料，這是FTD設定所需的資料。

- 按一下 Download CSV
- 按一下 Done



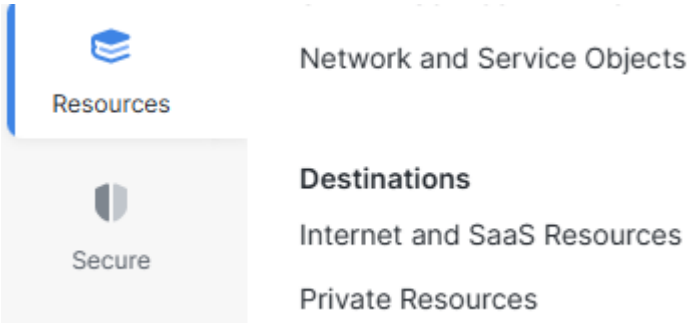
NTG資料

建立專用資源

私有資源是託管在資料中心或私有雲環境中的內部應用程式、網路或子網。這些資源不可公開訪問，並且受您組織的基礎架構保護。

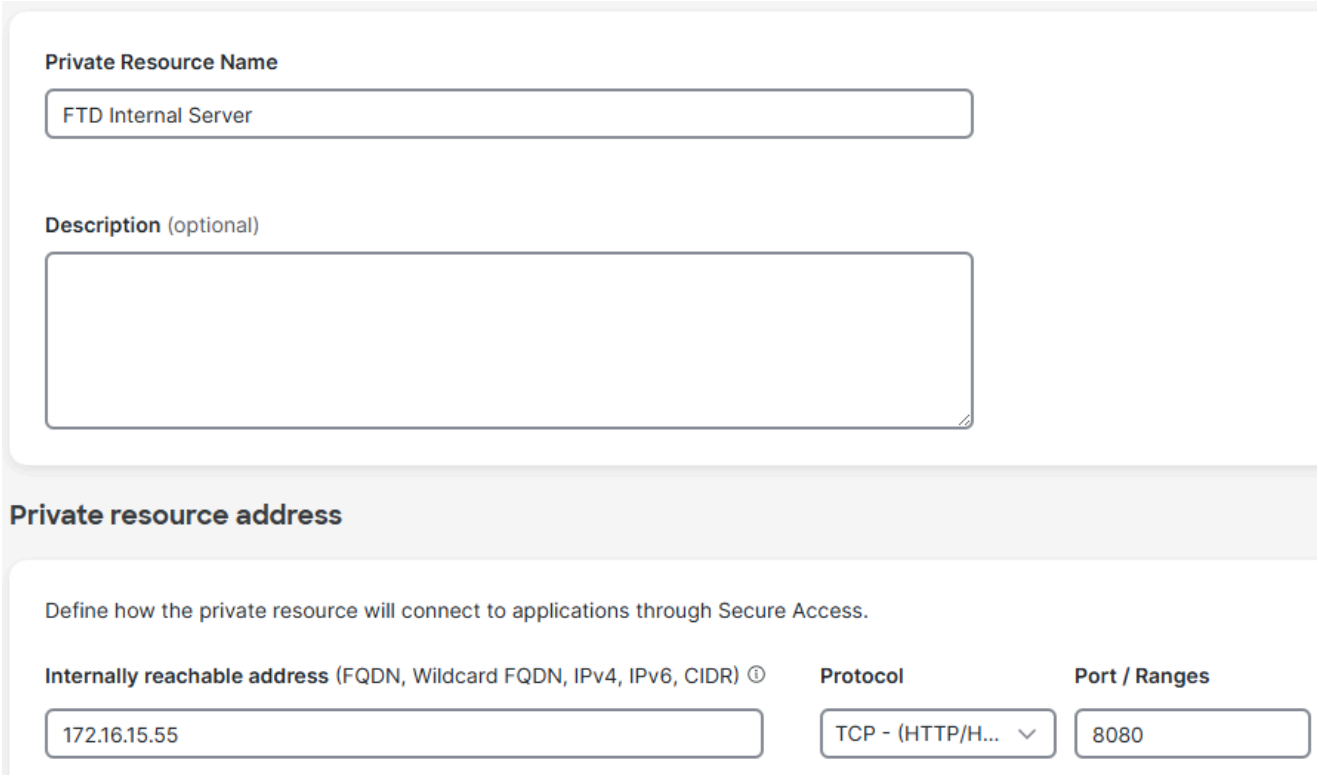
通過在Secure Access中將其定義為私有資源，您可以通過零信任訪問(ZTA)或VPN即服務(VPNaaS)等解決方案啟用受控訪問。 這可確保使用者根據身份、裝置狀態和訪問策略安全地連線到內部系統，而無需將資源直接暴露到網際網路上。

導航到**Resources** > **Private Resources**>按一下Add。



公關

- 指定**Private Resource Name**、 Internally reachable address、 ProtocolPort/Ranges。指定埠和協定，並根據需要新增其他專用資源
- 根據您的需要Connection Method，選擇所需的連線，例如「零信任連線」和/或「VPN連線」（根據您的要求）
- 按一下 Save



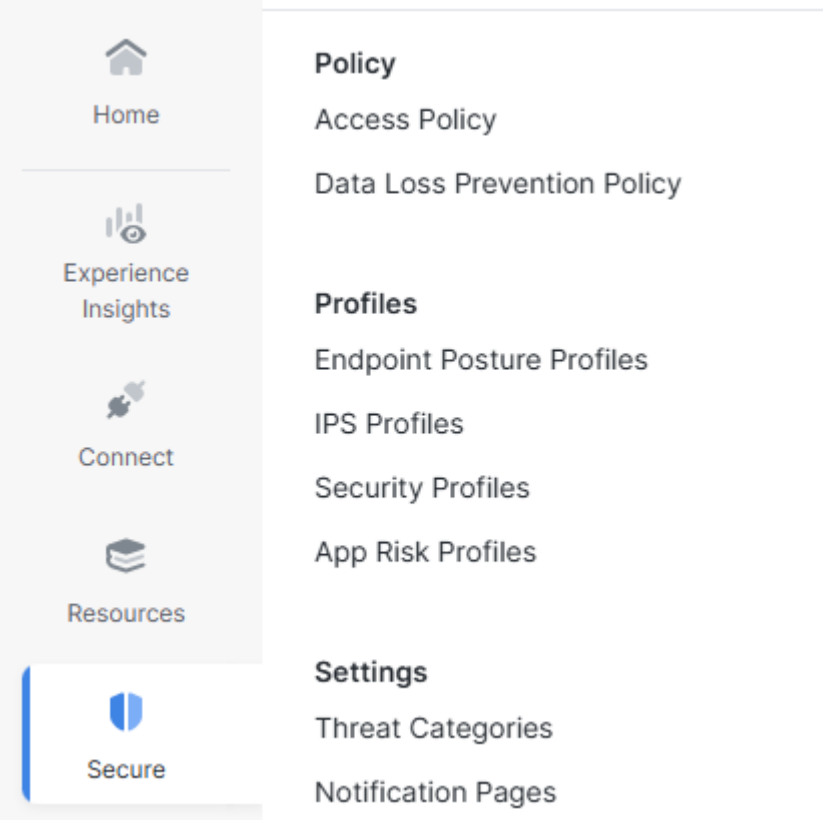
專用資源

建立訪問策略規則

專用訪問規則定義使用者如何安全地連線到不可公開訪問的內部資源和應用程式。

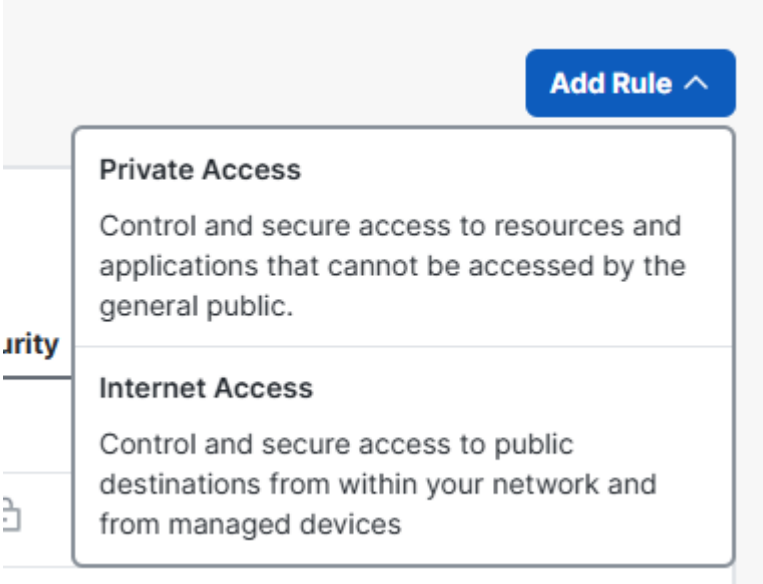
這些規則通過根據使用者身份、組成員身份、裝置狀態、位置或其他策略條件等因素控制誰可以訪問特定私有資源來實施安全性。這可確保敏感的內部系統始終受到保護，不會受到一般公眾訪問，同時仍通過ZTA或VPNaaS安全地可供授權使用者使用。

導航至 Secure>Access Policy



ACP

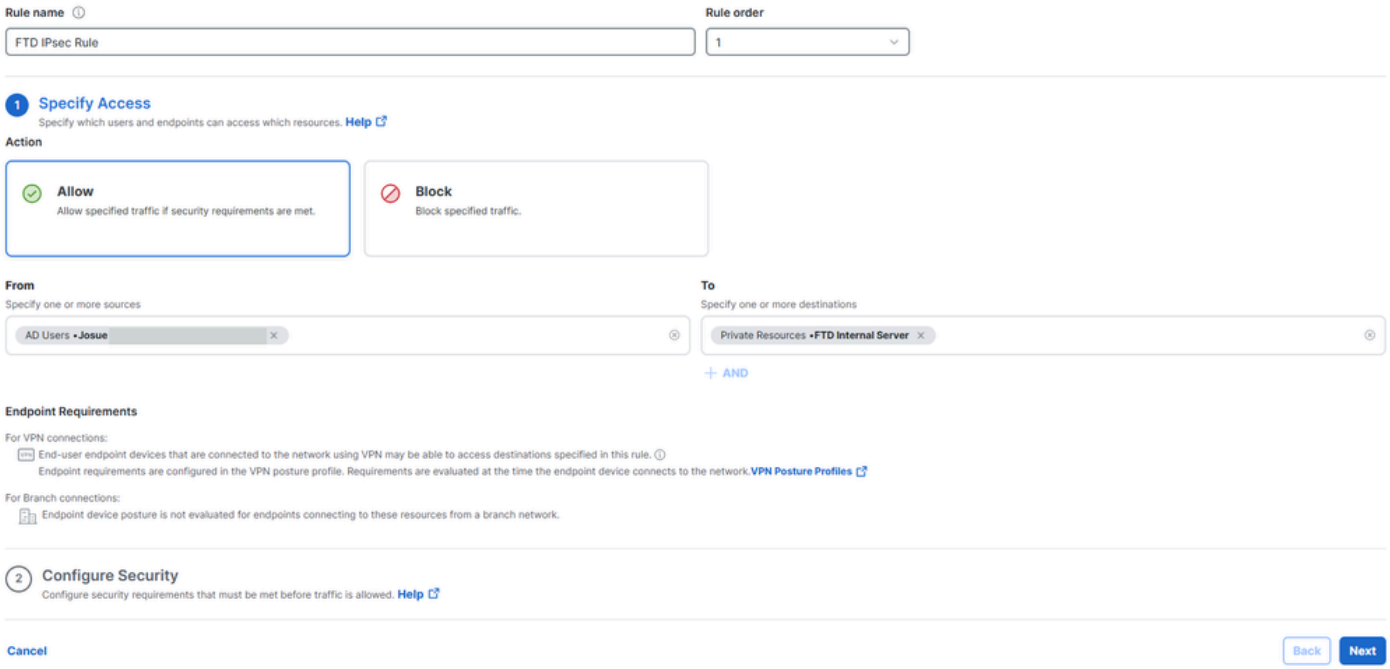
- 按一下 Add Rule
  - 按一下 Private Access



新增ACP

- 按一下Rule Name，然後為其命名
- 按一下Action，選擇Allow允許此流量
- 按一下onFrom並指定具有授予許可權的使用者
- 按一下並To指定使用者基於此規則的訪問許可權

- 按一下Next，然後Save進入下一頁



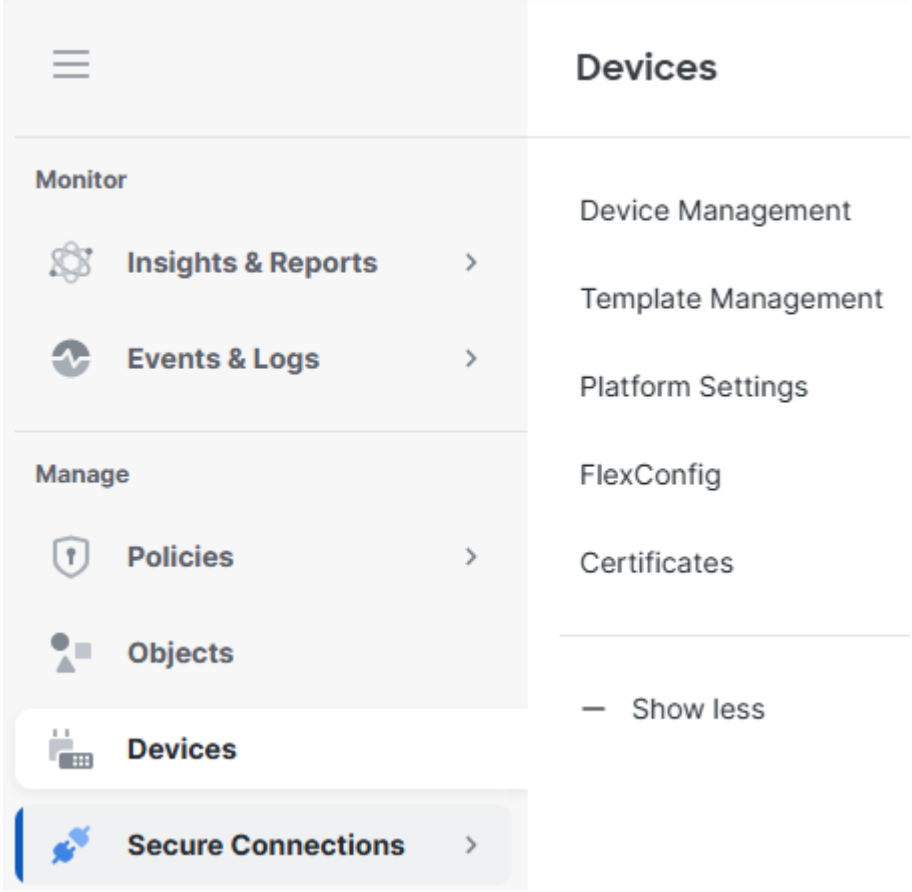
ACP配置

安全防火牆威脅防禦(FTD)組態

虛擬隧道介面配置

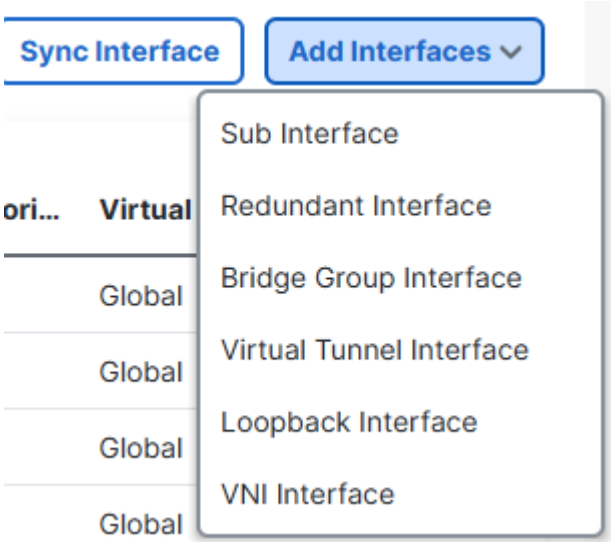
FTD上的虛擬通道介面(VTI)是用來設定路由型IPsec VPN通道的邏輯第3層介面。

1.定位至Devices> Device Management。



FTD裝置

- 按一下「FTD Device， Interfaces
  - 按一下 Add Interfaces
  - 按一下 Virtual Tunnel Interface
  - 建立兩個虛擬通道介面，一個用於主安全訪問中心，另一個用於輔助安全訪問中心

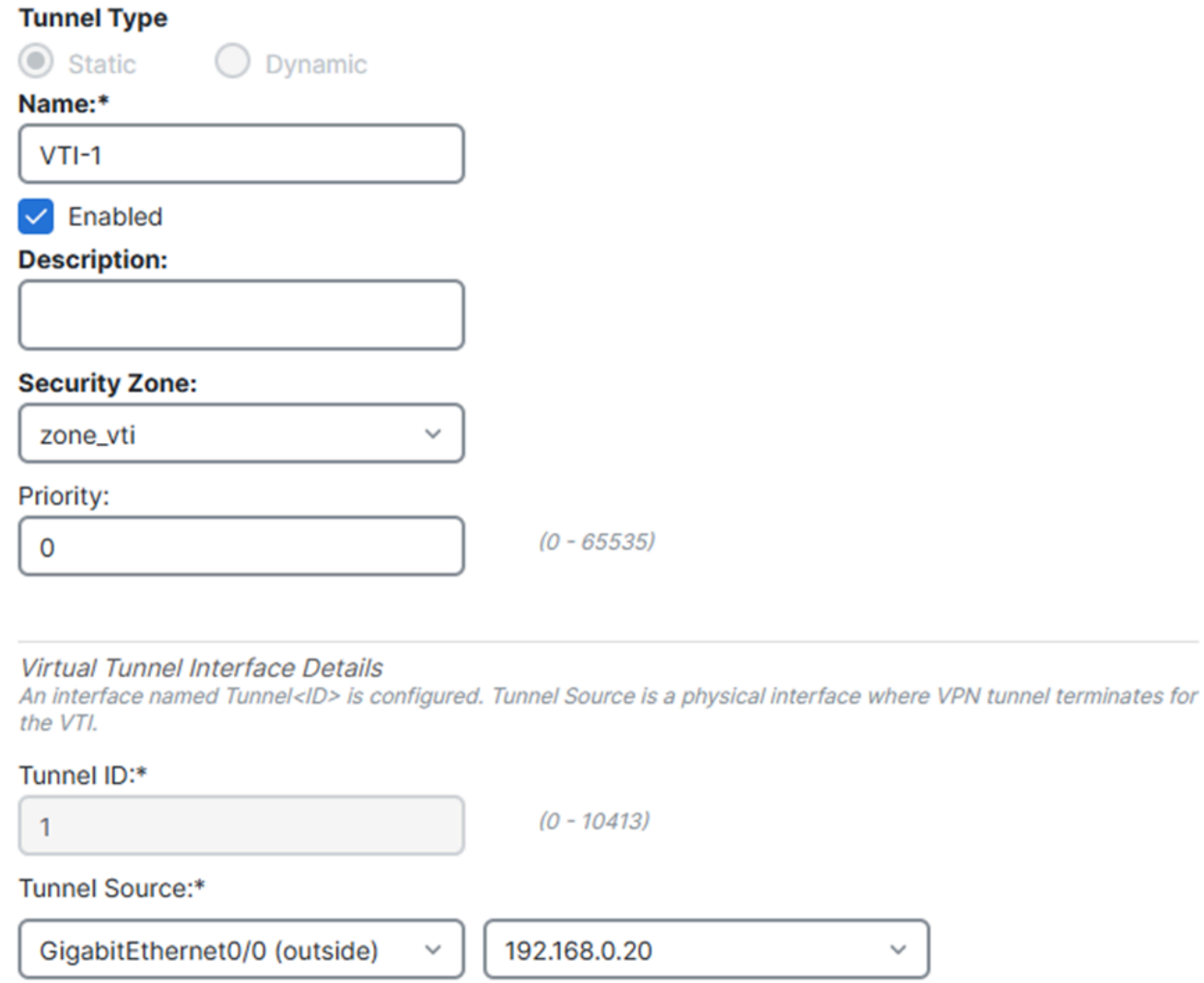


新增VTI

虛擬通道介面1:

- 請為其指定一個名稱，按一下 Enable
- 選擇或建立 Security Zone

- 點選Tunnel ID，並賦予其一個值。
- 點選Tunnel Source，指定隧道要從中建立的WAN介面
- 按一下IPsec Tunnel Mode，選擇IPv4
- 按一下IP Address，然後配置VTI的IP地址
- 按一下OK

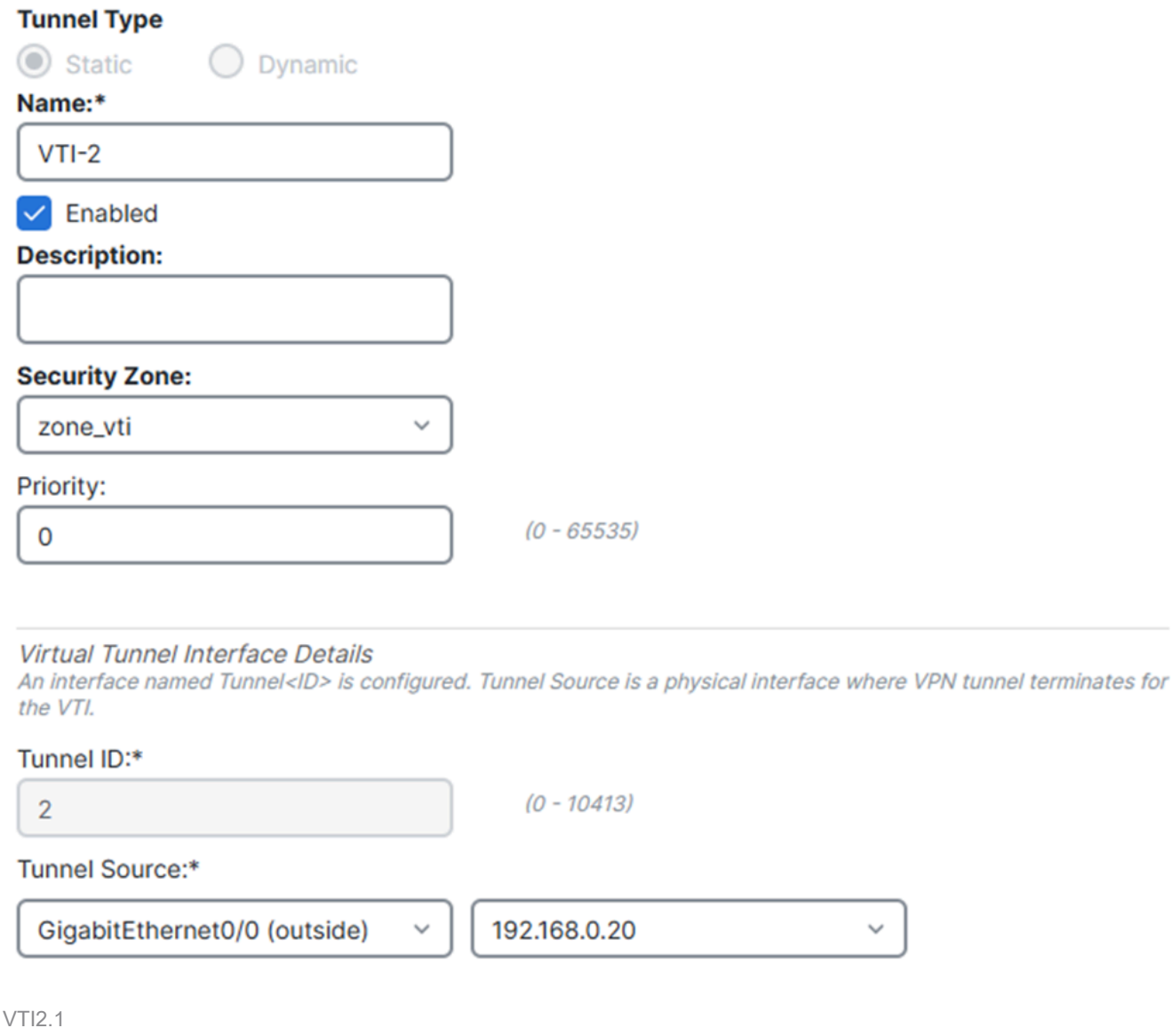


VTI1.1

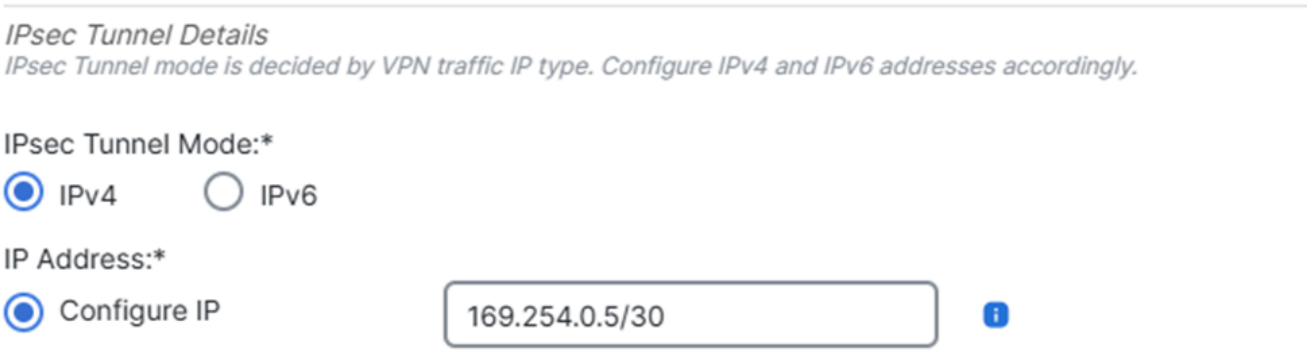
VTI1.2

虛擬通道介面2:

- 請為其指定一個名稱，按一下 Enable
- 選擇或建立 Security Zone
- 點選Tunnel ID，並賦予其一個值
- 點選Tunnel Source，指定隧道要從中建立的WAN介面
- 按一下IPsec Tunnel Mode，選擇IPv4
- 按一下IP Address，然後配置VTI的IP地址
- 按一下OK

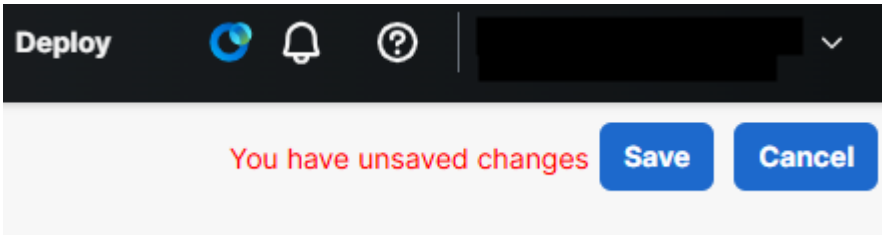


VTI2.1



VTI2.2

- 按一下Save。

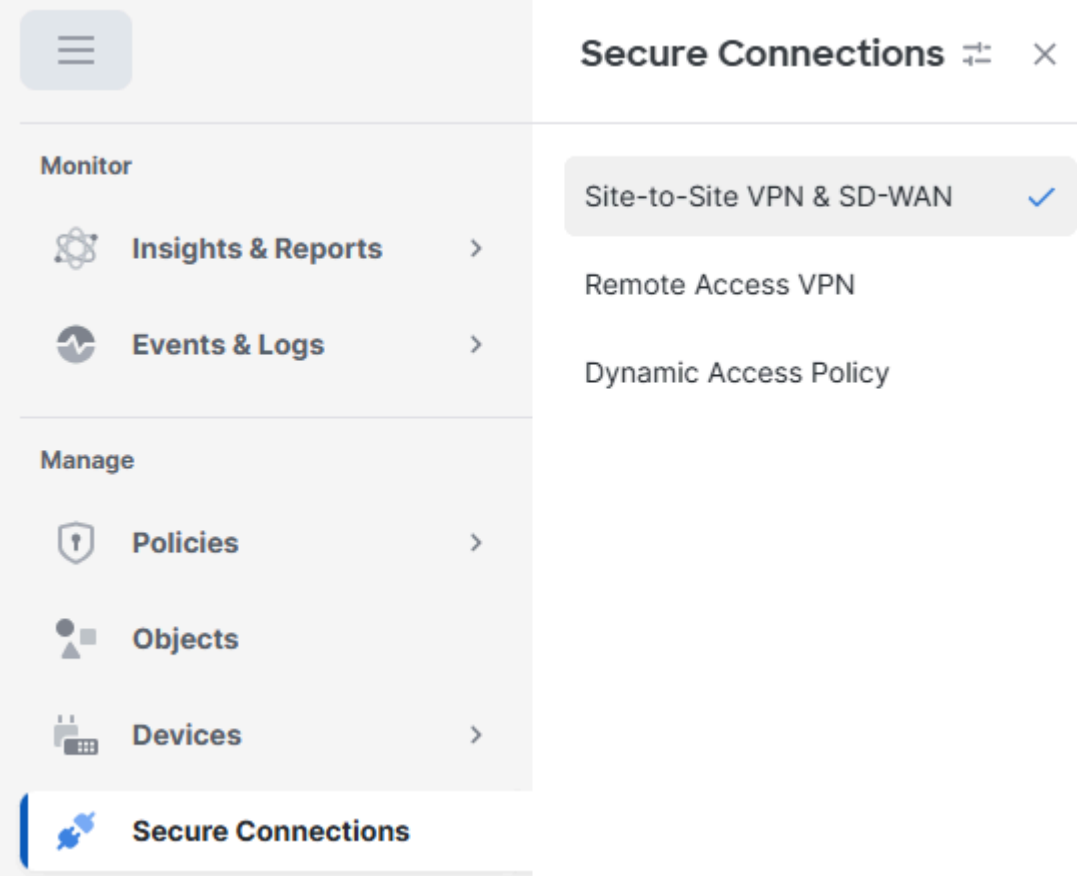


儲存VTI更改

IPsec通道組態

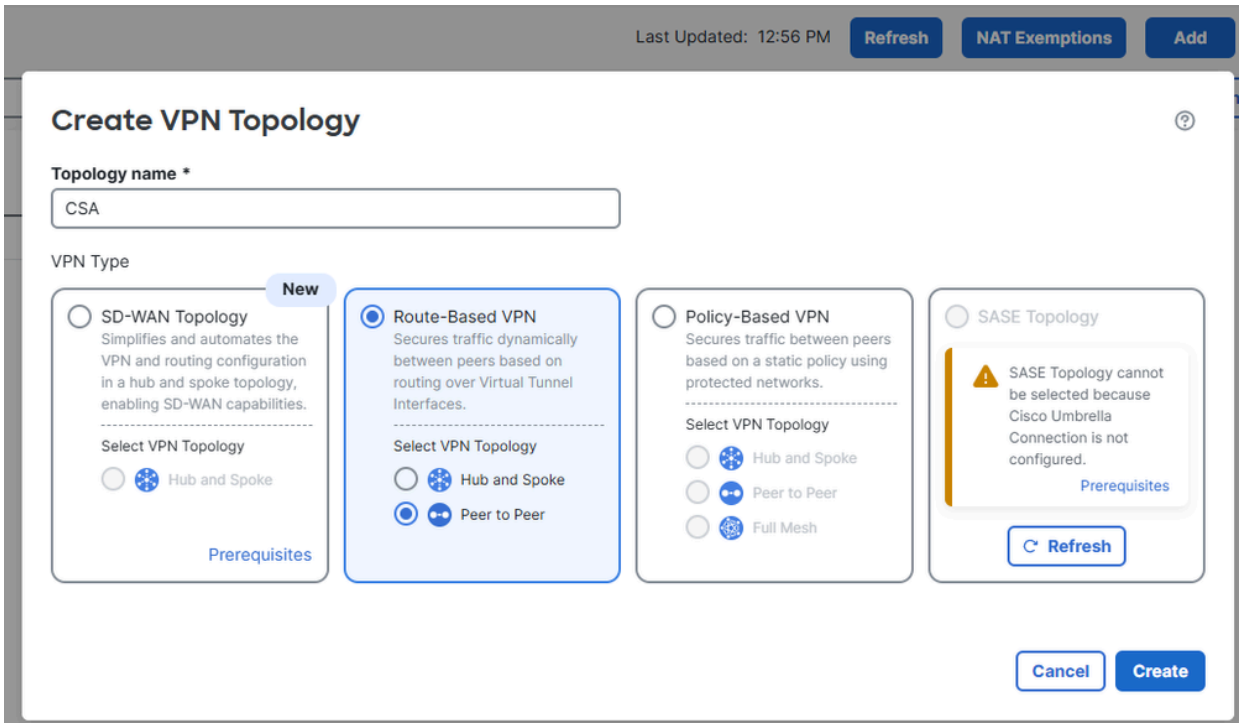
導航到您的cdFMC控制面板。

- 按一下Secure Connection> Site-to-Site VPN & SD-WAN



S2S

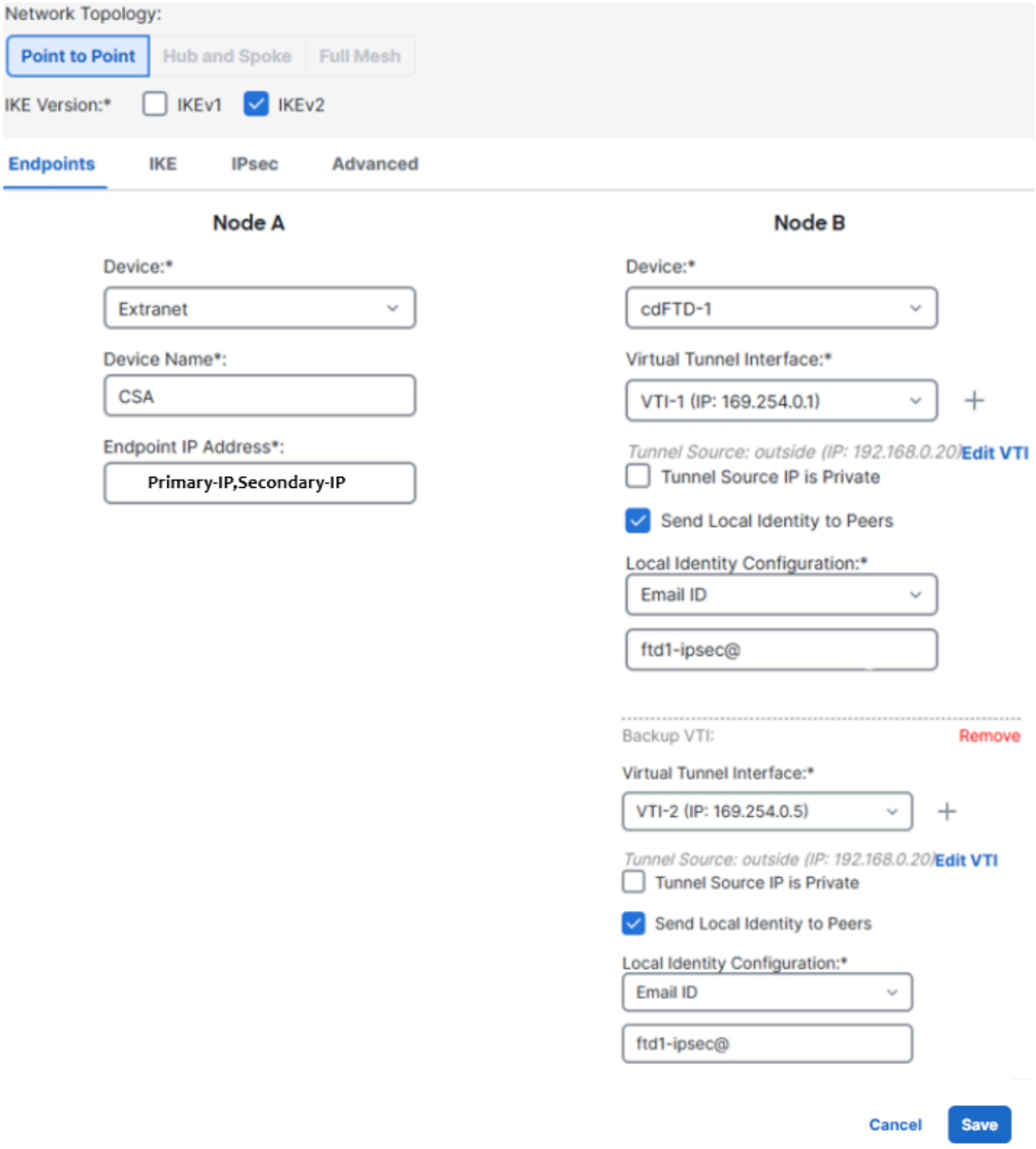
- 按一下Add
  - 按一下 Route-Based VPN
  - 按一下 Peer to Peer



新增VPN

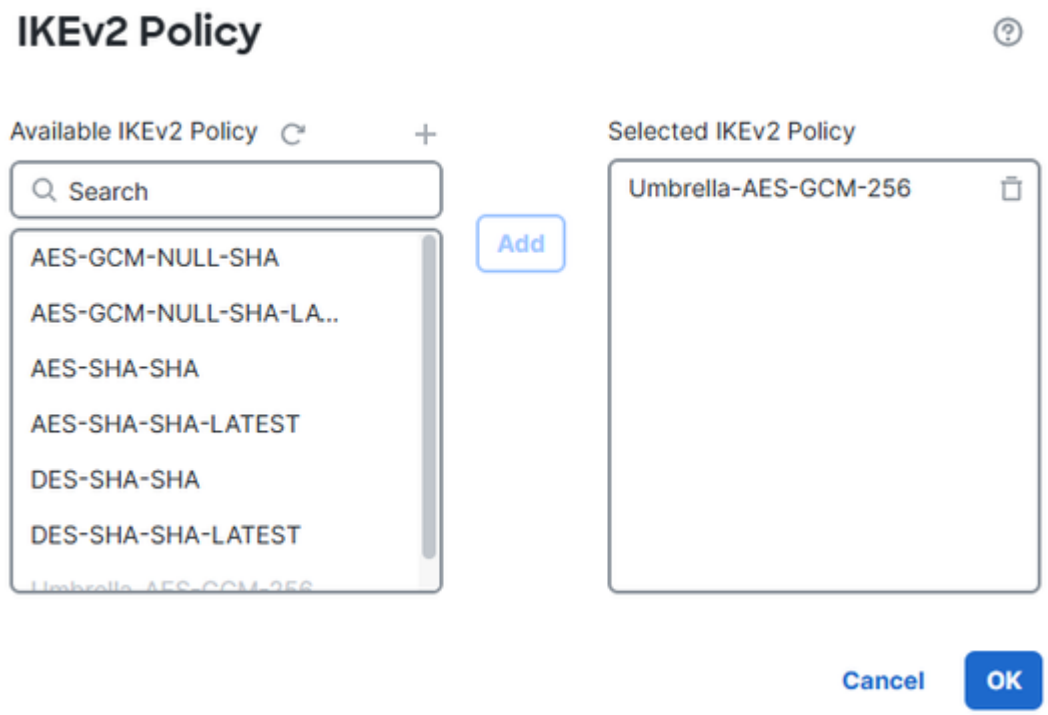
- 從安全訪問配置的第5步獲取主資料中心和輔助資料中心的隧道ID和IP地址

- 按一下Endpoints
  - 在Node A下，按一下Deviceon並選擇 Extranet
  - 點選Device Name並為其命名
  - 點選Enpoint IP Addresses，然後輸入安全訪問主要和輔助IP地址（以逗號分隔），該地址位於Secure Access下的「Save Network Tunnel Group Configuration」中組態)
  - 在Node B下，按一下Device並選擇FTD裝置
  - 按一下Virtual Tunnel Interface，選擇在上一步中建立的第一個VTI介面
  - 按一下Send Local Identity to Peers選項並選擇Email ID，輸入主隧道ID（從「安全訪問配置」下的「儲存網路隧道組配置」中）
  - 按一下 Add Backup VTI
  - 點選Virtual Tunnel Interface，選擇上一步中建立的第二個VTI介面
  - 按一下Send Local Identity to Peersonoption並選擇Email ID，輸入輔助隧道ID（在Secure Access Configuration下的「Save Network Tunnel Group Configuration」中）
  - 按一下Save



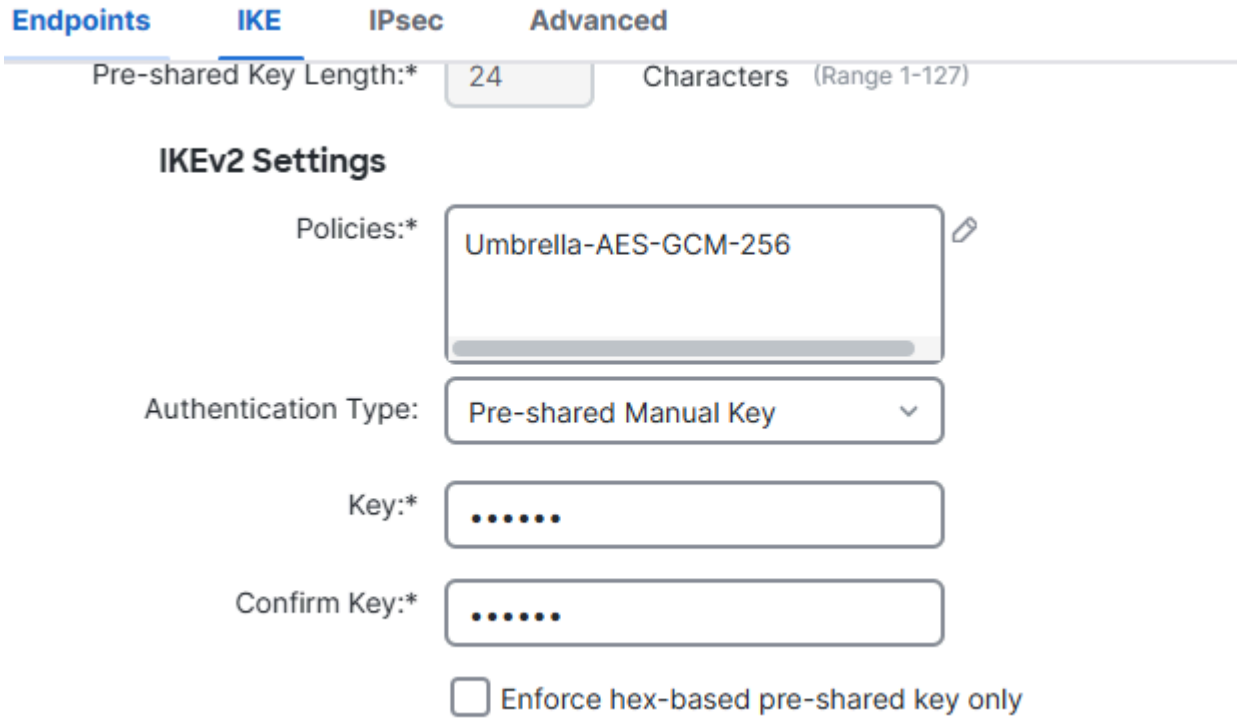
FTD VTI組態

- 按一下IKE
  - 按一下**IKEv2 Settings >** Policies
  - 選擇選Umbrella-AES-GCM-256項
  - 按一下 OK



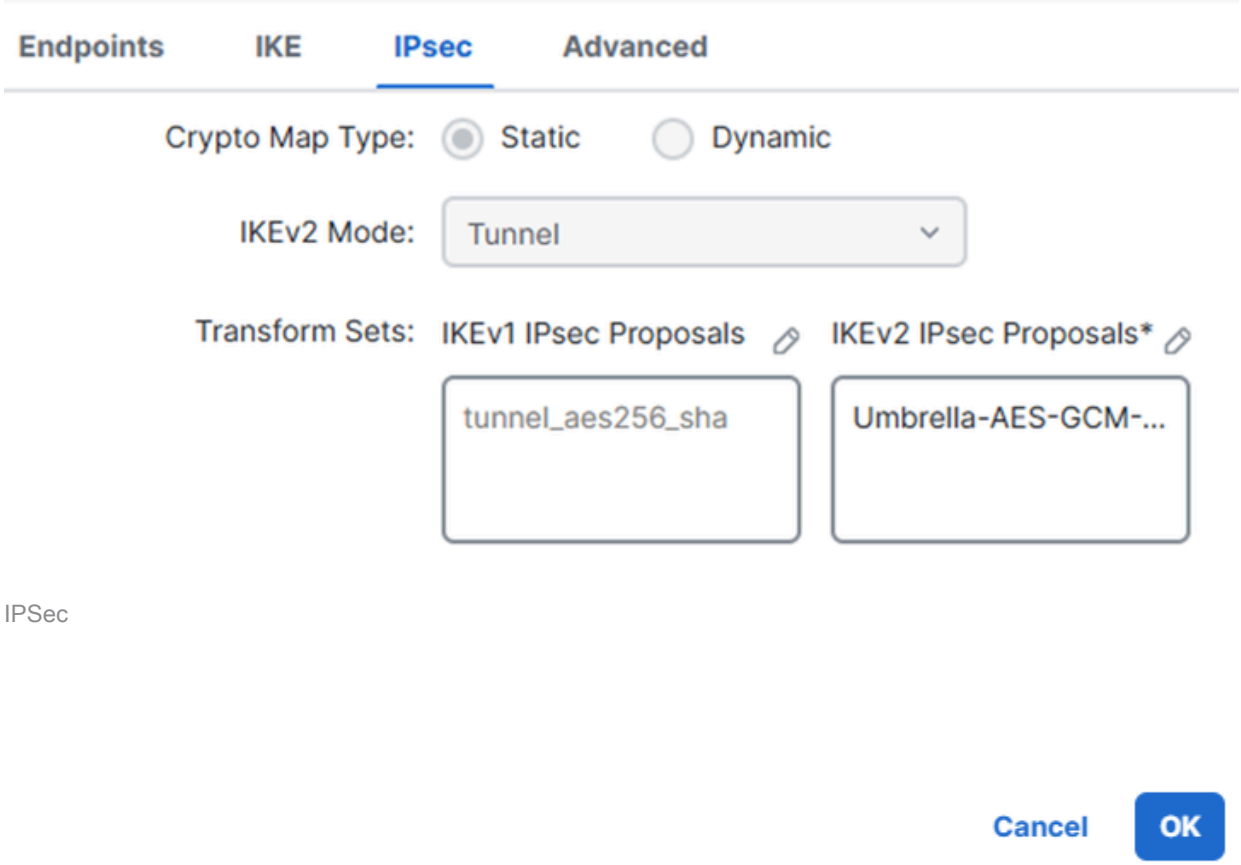
IKEv2原則

- 按一下Authentication Type並選擇Pre Shared Manual Key，輸入在安全訪問（密碼短語）中配置的PSK



IKE

- 按一下 IPSEC
  - 按一下 IKEv2 Proposals
  - 選擇 Umbrella-AES-GCM-256
  - 按一下 OK



IPSec

儲存IKEv2提議

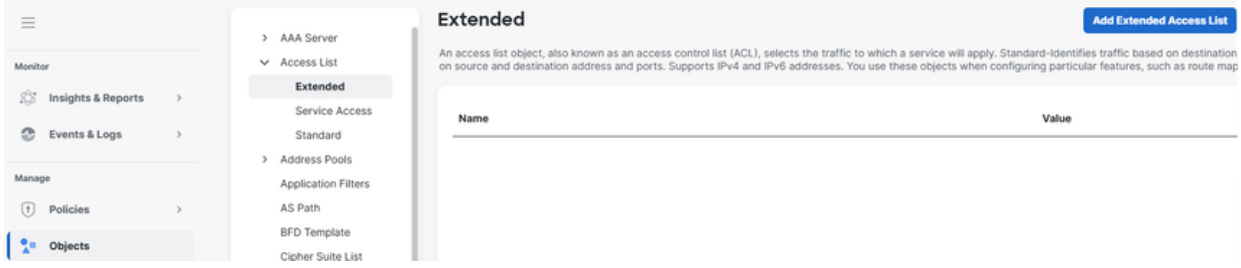
FTD路由組態

透過原則型路由(PBR)，您可以根據除目的地IP位址以外的標準控制流量轉送。PBR可以基於源、應用、協定、埠或其他定義的策略來路由流量，而不是僅依賴路由表。

這使組織能夠通過首選鏈路（例如高頻寬或直接網際網路鏈路）引導特定或高優先順序流量，最佳化效能，並安全地隔離所選應用，而無需通過VPN隧道傳送所有流量。

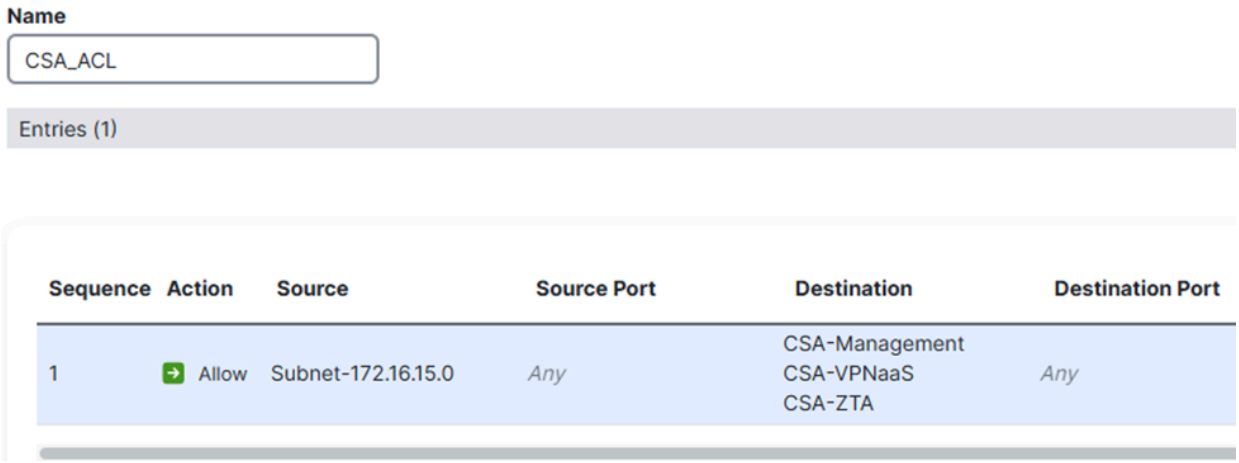
原則型路由

- 導航至Objects
  - 按一下 Access List
  - 按一下 Extended
  - 按一下Add Extended Access List



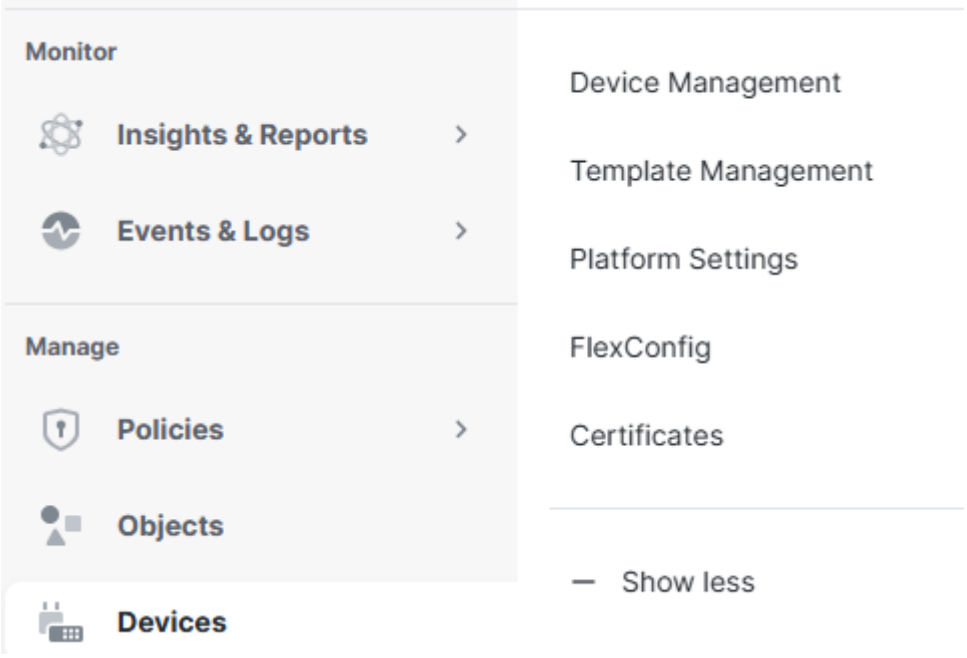
新增ACL

建立延伸存取控制清單(ACL)，與要透過通道傳送的FTD(例如172.16.15.0/24)保護的來源網路相符。對於目標，請新增ZTA使用的網路（CGNAT範圍）和VPNaaS使用的網路（請檢查虛擬專用網路IP池）。



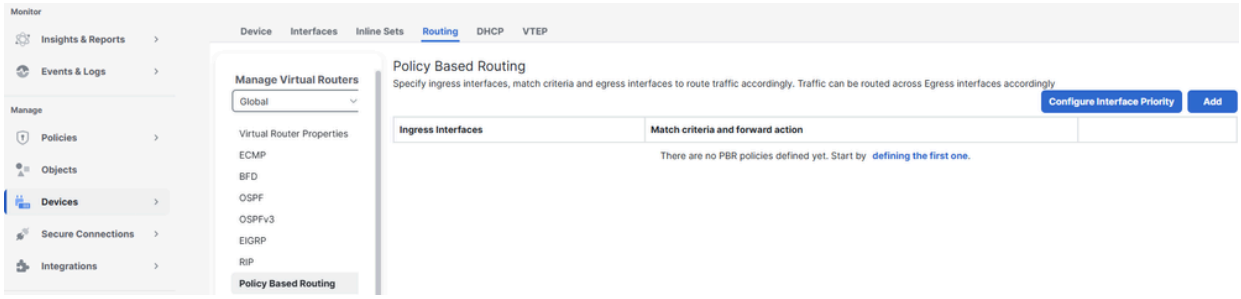
ACL

- 按一下Devices> Device Management



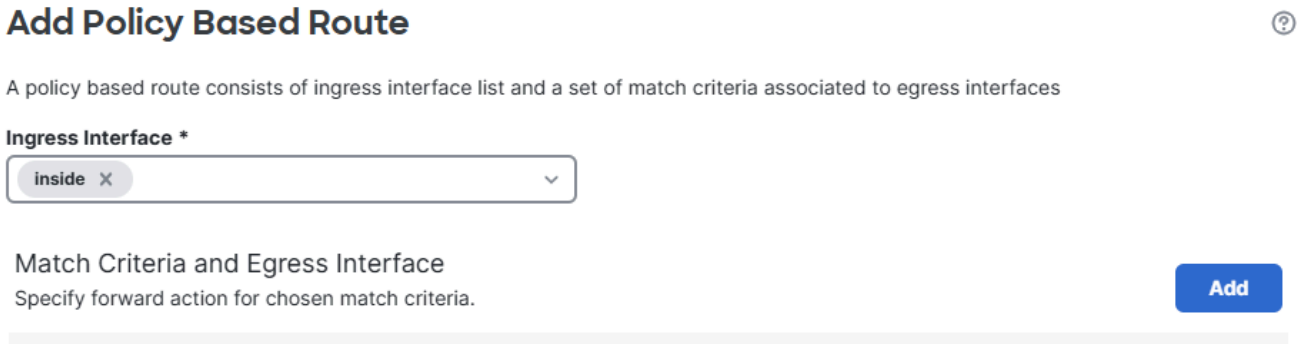
裝置

- 按一下FTD
  - 按一下Routing
  - 按一下 Policy Based Routing
  - 按一下 Add



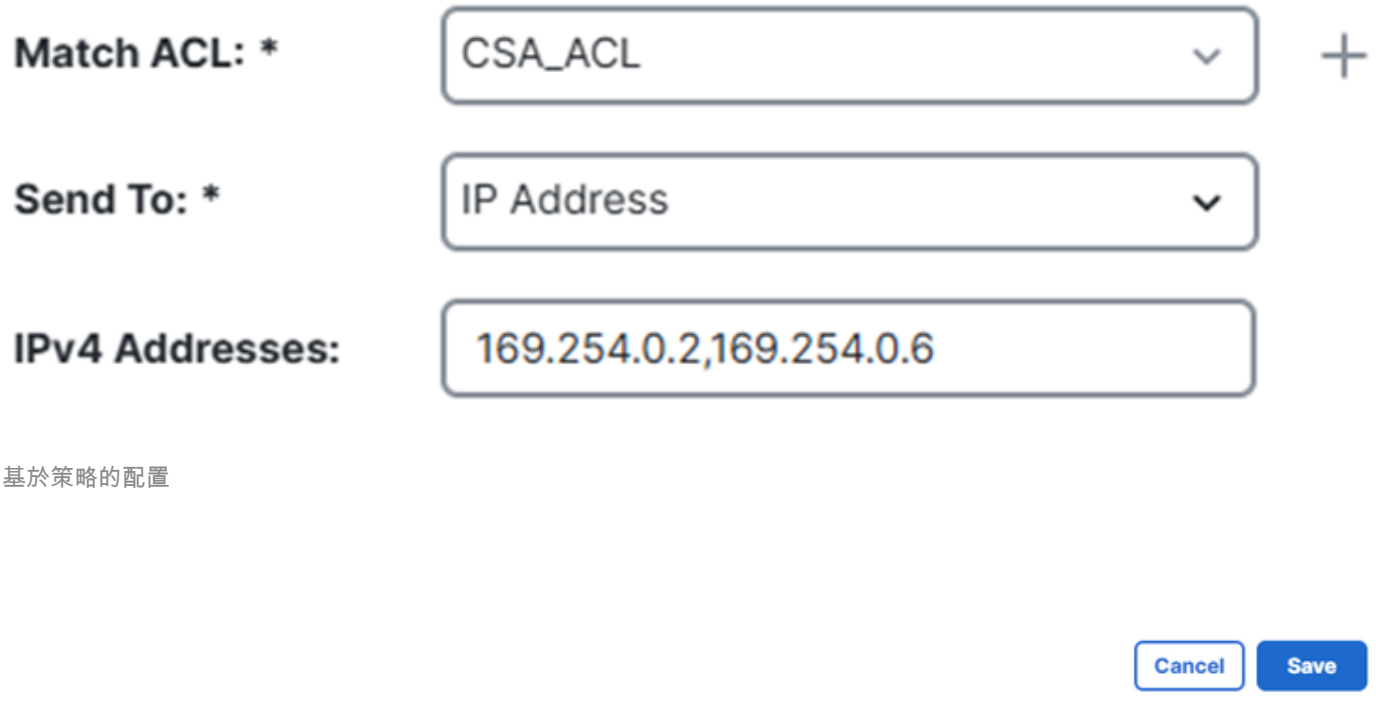
新增PBR

- 按一下Ingress Interface，然後選擇內部網路流量進入的輸入介面
- 在Match Criteria and Egress Interface下，按一下 Add



輸入介面

- 按一下Match ACL，然後選擇先前建立的延伸型ACL
- 按一下 Send To and select IP Address
- 按一下IPv4 Addresses，將VTI介面子網中IP位址在FTD（169.254.0.2和169.254.0.6）中設定為下一跳
- 按一下 Save



基於策略的配置

儲存PBR

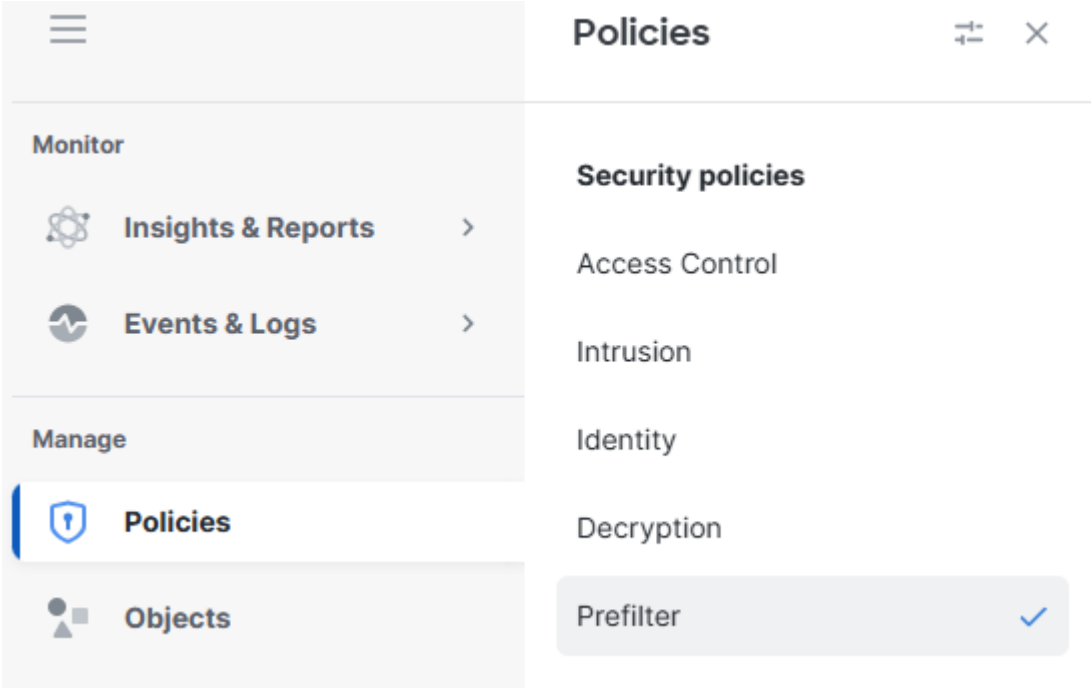
請確保選擇Send To IP Address> 選項，而不是選Egress Interface項。

訪問策略配置

要允許Cisco Firepower威脅防禦(FTD)上的流量並啟用對專用資源的訪問，流量必須首先通過稱為預過濾的訪問控制初始階段。

預濾波是在進行深度檢測之前進行的，設計簡單快速。它使用基本外部報頭標準（如源和目標IP地址和埠）評估流量，以快速允許、阻止或繞過流量。在此階段允許流量時，可以跳過資源密集型檢查（如深度資料包檢查或入侵策略），從而在提高效能的同時保持安全控制。

- 導覽至Policies> Prefilter

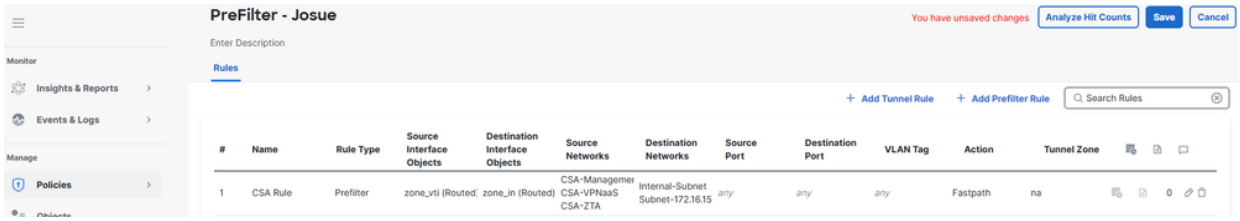


預過濾器

- 點選編輯您的訪問策略正在使用的預過濾器策略

按一下prefilter

- 按一下 Add Tunnel Rule
  - 新增和允許來自VPNaaS網路和/或ZTA子網的流量到您的專用資源
  - 按一下Save



儲存規則

此時，一旦完成並驗證FTD上的組態，就可以繼續部署。部署後，IPsec隧道成功啟動，確認已建立與專用資源的安全連線。

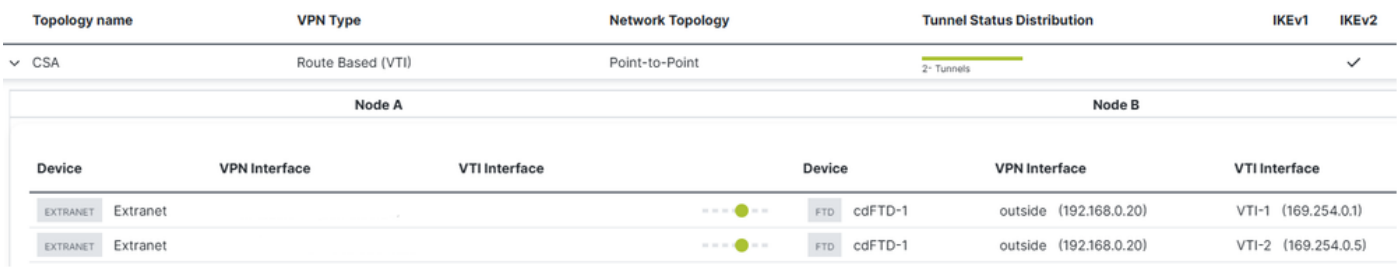
驗證

在FTD中驗證

FTD中的通道狀態

您可以檢視通道的目前狀態，包括up 或down。這有助於檢驗IPsec隧道是否正確建立。

- 按一下Secure Connections。
- 按一下Site-to-Site VPN & SD-WAN。
- 按一下Topology Name。



FTD通道狀態

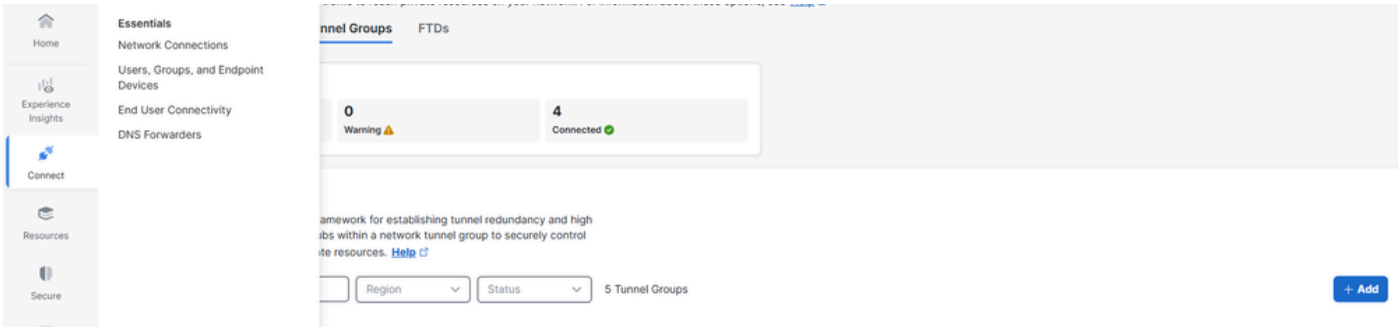
在安全訪問中驗證

安全存取中的通道狀態

您可以檢視通道的目前狀態，包括通道是否已斷開、警告或連線。這有助於檢驗IPsec隧道是否正確建立。

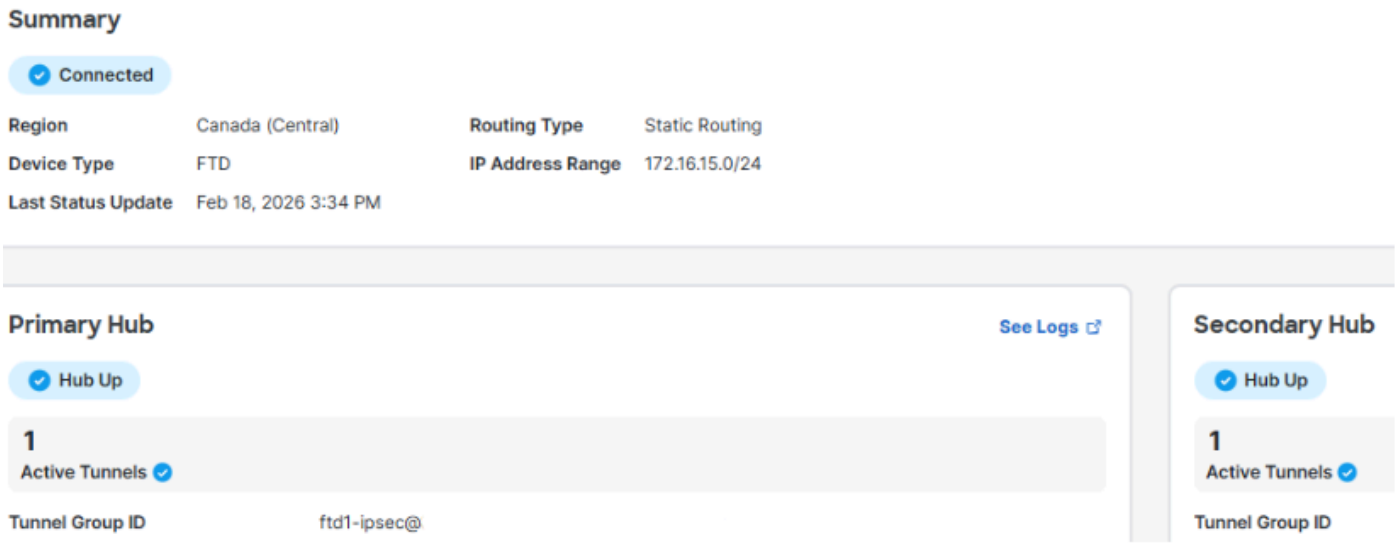
- 按一下Connect > Network Connections

- 按一下「Network Tunnel Groups」



檢查NTG

- 按一下Network Tunnel Group

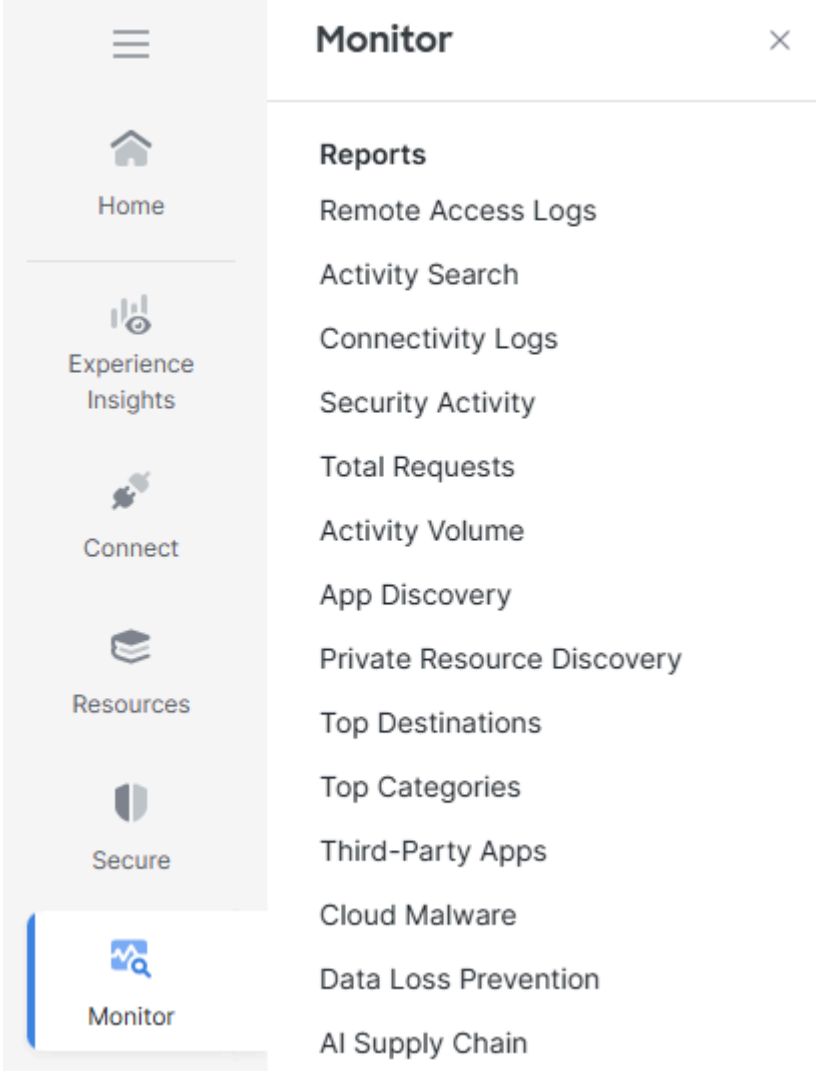


CSA隧道狀態

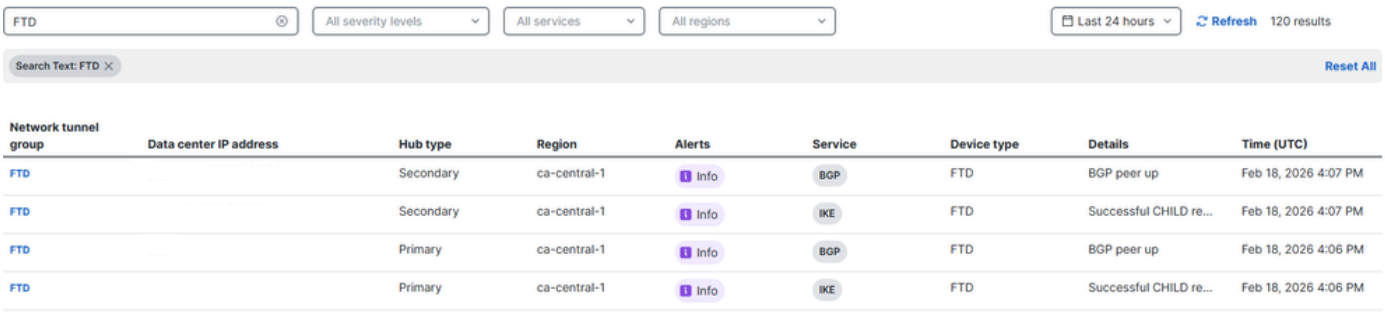
Secure Access中的事件

您可以檢視Tunnel事件，並確認IPsec隧道的狀態是否為up且穩定。

按一下「Monitor」>「Network Connectivity」。

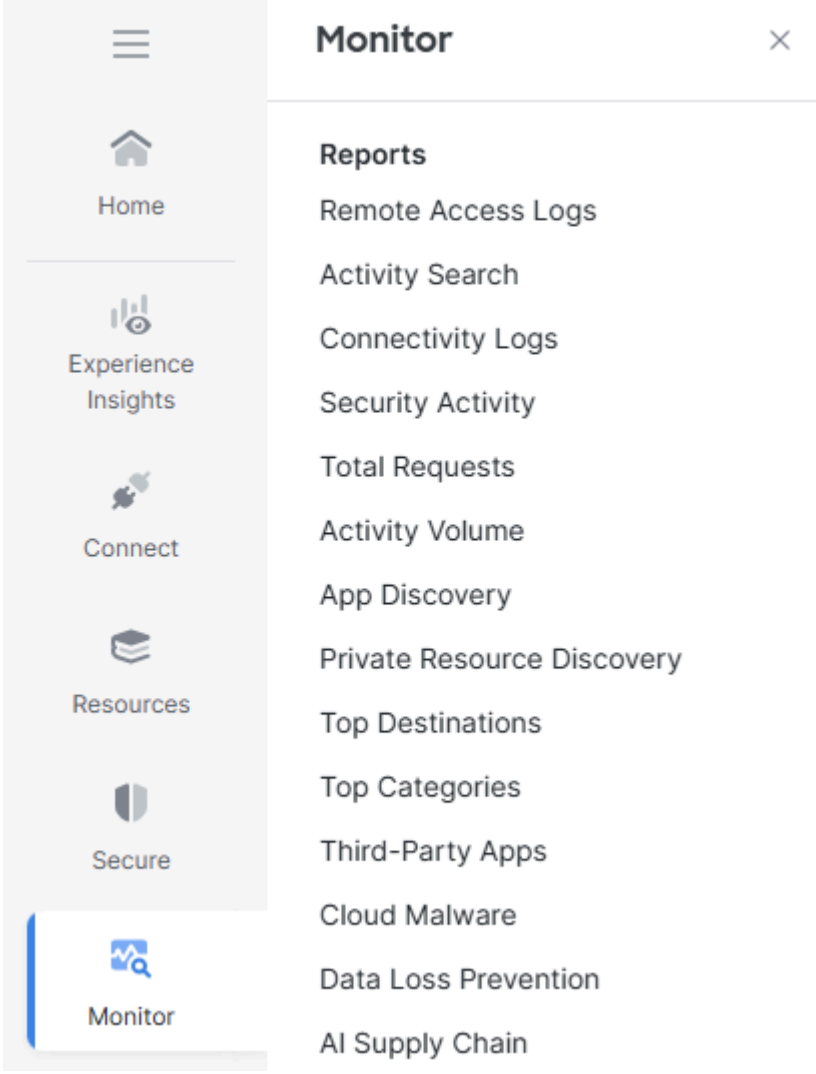


監控連線日誌



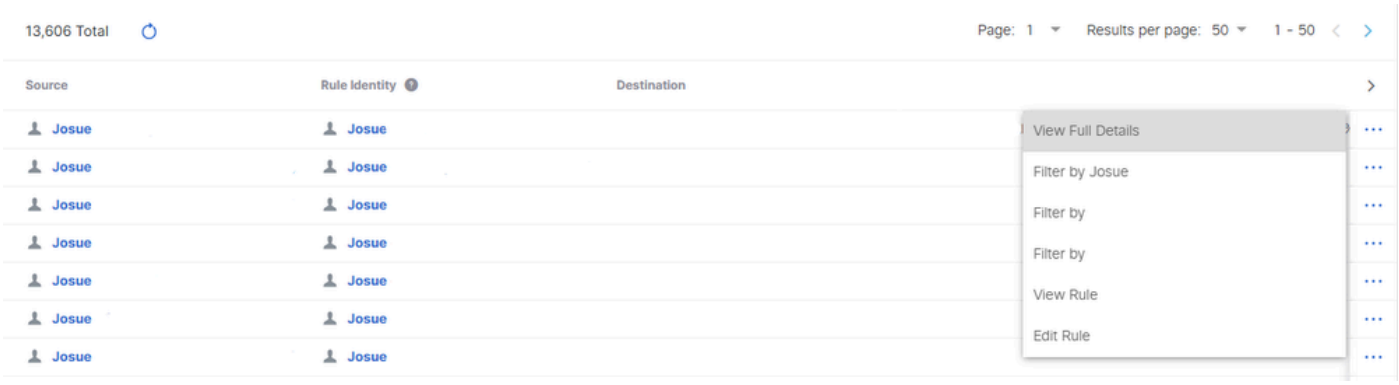
連線日誌

導覽至Monitor > Activity Search。

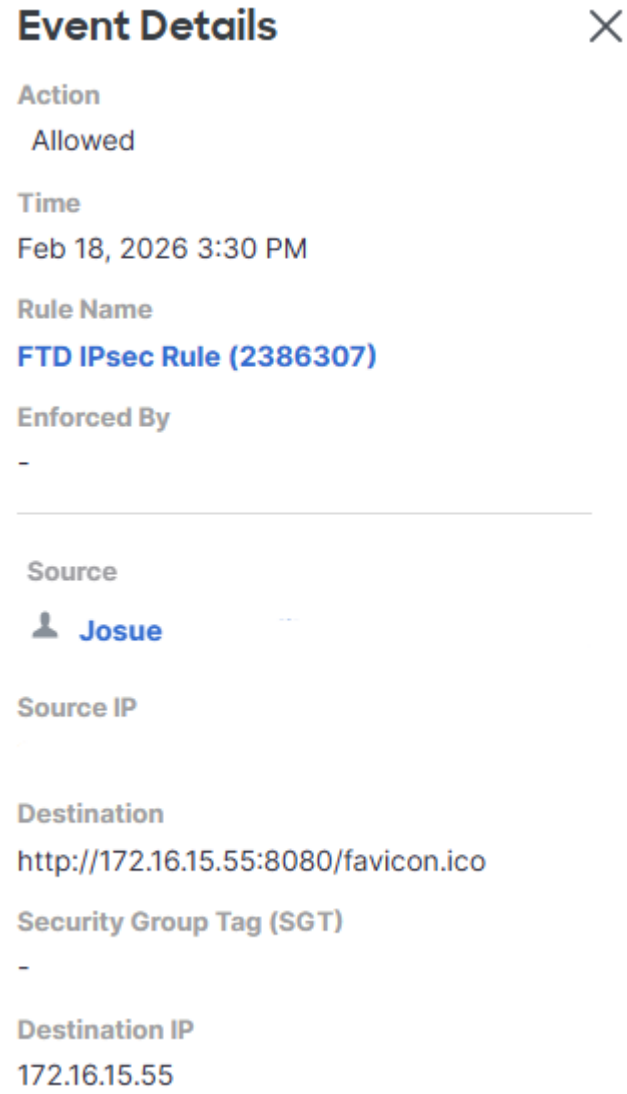


監控連線日誌

在任何相關事件上，點選檢視完整詳細資訊。



完整詳細資訊



活動搜尋

相關資訊

- 思科技術支援與下載
- 思科安全防火牆管理中心裝置配置指南7.7

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。