Konfigurieren von sicherem Zugriff mit sicherem Firewall-Schutz für privaten Zugriff mit richtlinienbasiertem Routing

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie sicheren Zugriff mit FTD über IPsec für sicheren privaten Zugriff mit richtlinienbasiertem Routing konfigurieren.

Voraussetzungen

Anforderungen

- Kenntnisse zu Cisco Secure Access
- Cisco Secure Access Dashboard/Tenant
- Sichere Firewall Threat Defense- und Firewall Management Center-Kenntnisse
- IPsec-Kenntnisse
- Richtlinienbasiertes Routing

Verwendete Komponenten

- Sichere Firewall mit Code 7.7.10
- Cloud-fähiges Firewall-Management-Center. Konfiguration gilt auch für typisches virtuelles FMC
- Cisco Secure Access Dashboard

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Netzwerktunnel in Secure Access können für zwei primäre Zwecke verwendet werden: Sicherer Internetzugriff und sicherer privater Zugriff

Für einen sicheren privaten Zugriff können Unternehmen ZTA (Zero Trust Access) und/oder VPN-as-a-Service (VPNaaS) nutzen, um Benutzer mit privaten Ressourcen wie internen Anwendungen oder Rechenzentren zu verbinden. IPsec-Tunnel spielen eine Schlüsselrolle in dieser Architektur, indem sie den Netzwerkverkehr zwischen Benutzern und privaten Ressourcen sicher verschlüsseln und sicherstellen, dass vertrauliche Daten geschützt bleiben, während sie nicht vertrauenswürdige Netzwerke passieren. Durch die Integration von IPsec-Tunneln mit ZTA oder VPNaaS können Organisationen einen nahtlosen und sicheren Zugriff auf interne Ressourcen bereitstellen und gleichzeitig robuste Sicherheitskontrollen und Transparenz aufrechterhalten.

In diesem Dokument wird beschrieben, wie Sie sicheren Zugriff mit sicherem Firewall-Bedrohungsschutz (FTD) über IPsec für sicheren privaten Zugriff konfigurieren.
Darüber hinaus enthält dieses Handbuch die Schritte zum Konfigurieren von richtlinienbasiertem Routing.

Während in diesem Dokument die Konfiguration von IPsec-Tunneln für sicheren privaten Zugriff behandelt wird, wird die Einrichtung von ZTA (Zero Trust Access) oder VPN-as-a-Service (VPNaaS) für den Zugriff auf private Anwendungen in diesem Leitfaden nicht behandelt.

Konfigurieren

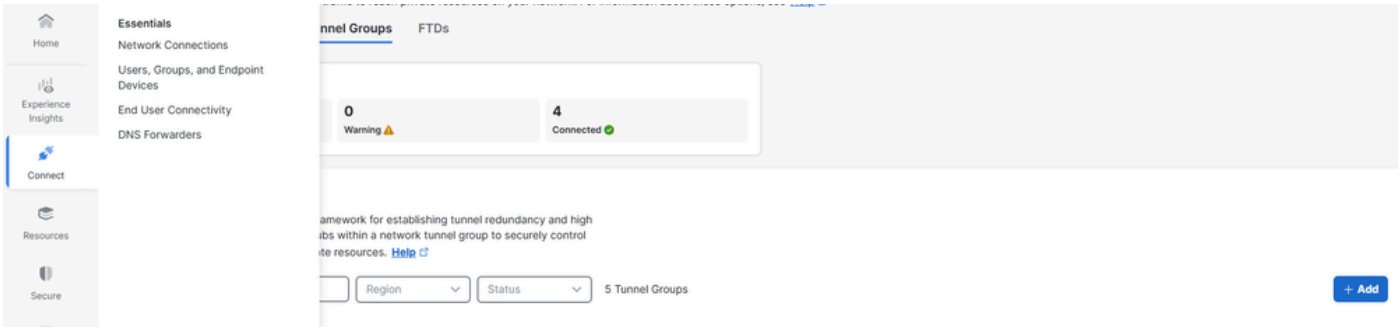
Konfiguration des sicheren Zugriffs

Konfiguration der Netzwerk-Tunnelgruppe

1. Navigieren Sie zum Admin-Bereich von [Sicherer Zugriff.]

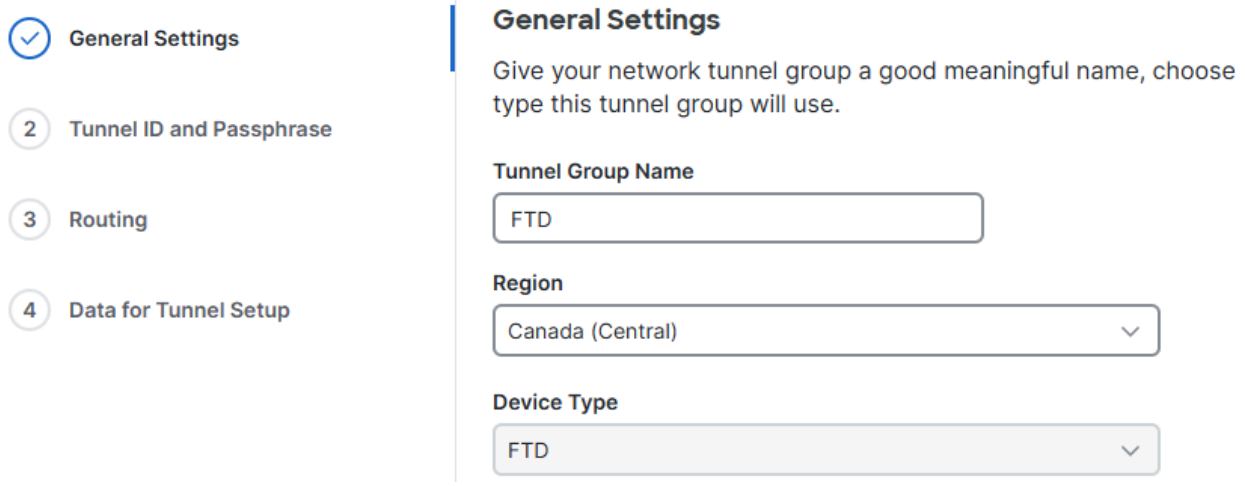
2. Hinzufügen einer Netzwerk-Tunnelgruppe

- Auf Connect > Network Connections
  - Klicken Sie unter Network Tunnel Groups > Add



3. General Settings Konfiguration

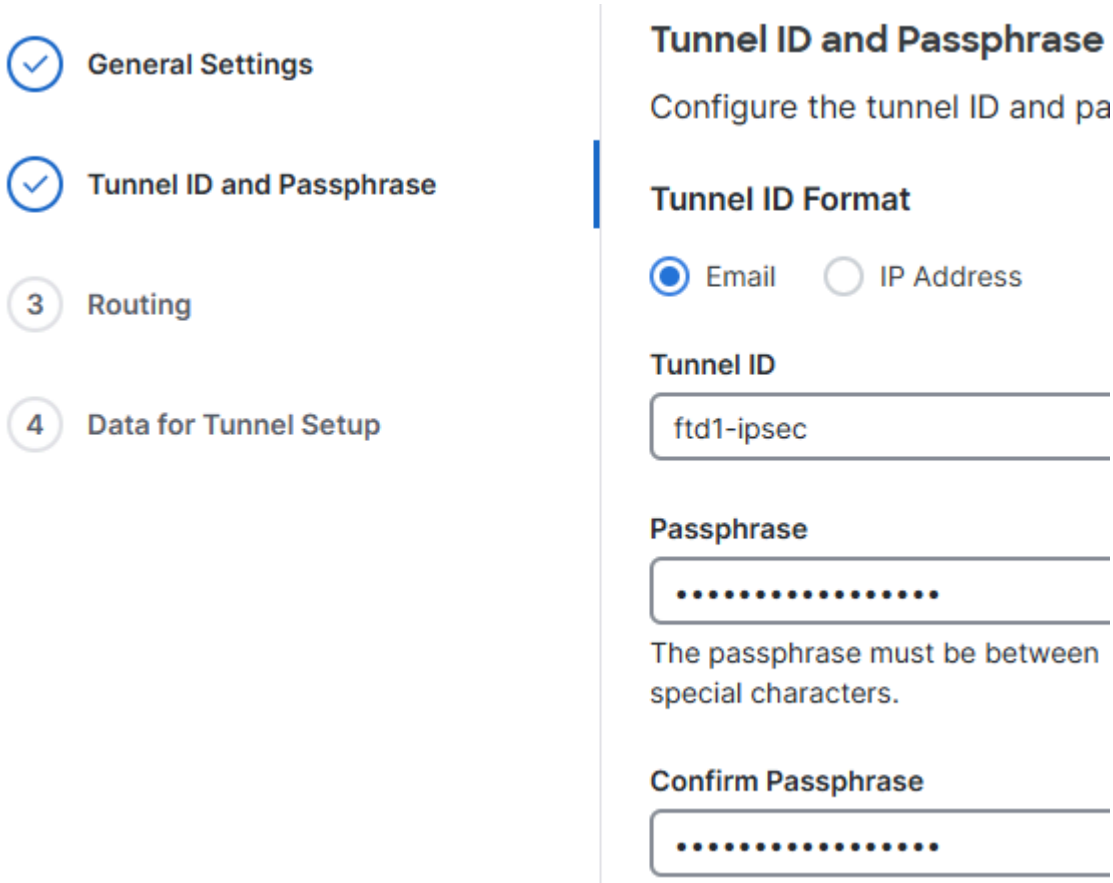
- Konfigurieren Sie Tunnel Group Name und **Region** und Device Type
  - Klicken Sie auf Next



Allgemeine Einstellungen

4. Konfigurieren Tunnel ID und Passphrase.

- Konfigurieren Sie das **Tunnel ID**und Passphrase. Diese ID ist wichtig, da sie für die FTD-Konfiguration erforderlich ist.
- Klicken Sie Next



ID und PSK

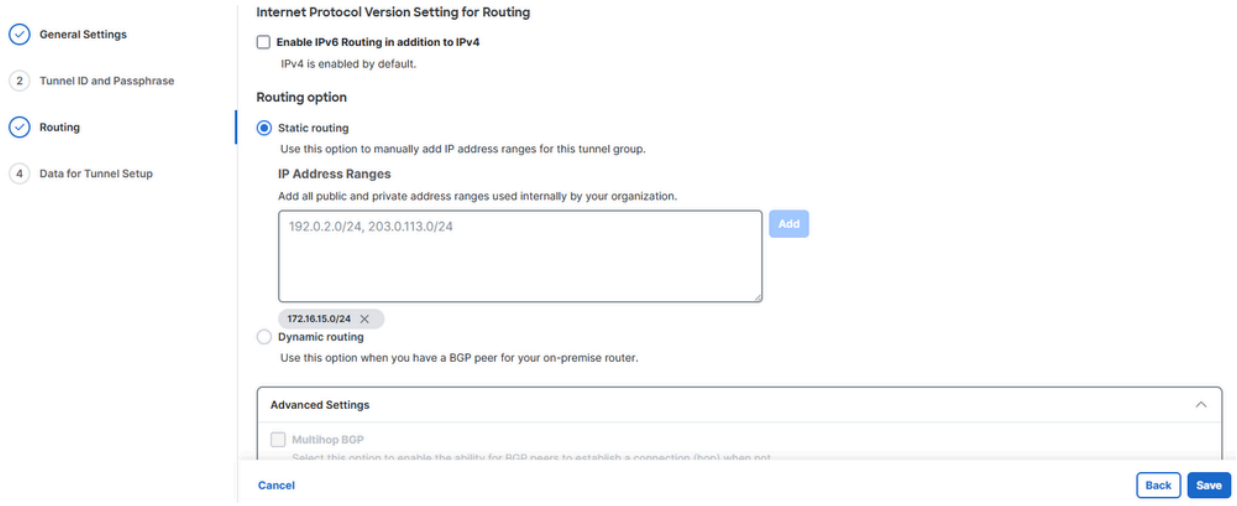
5. Konfigurieren Sie statisches Routing.

Sicheres Access Routing

Richtlinienbasiertes Routing

Fügen Sie die durch die FTD geschützten Netzwerke hinzu, auf die Remote-Benutzer über ZTA und/oder VPNaaS zugreifen sollen, und klicken Sie auf Save (Speichern).

- Auf Routing> **Static routing**
  - Fügen Sie die IP-Adressbereiche oder Hosts hinzu, die Sie in Ihrem Netzwerk konfiguriert haben und den Datenverkehr über Secure Access weiterleiten möchten, und klicken Sie aufAdd
  - Klicken SieSave

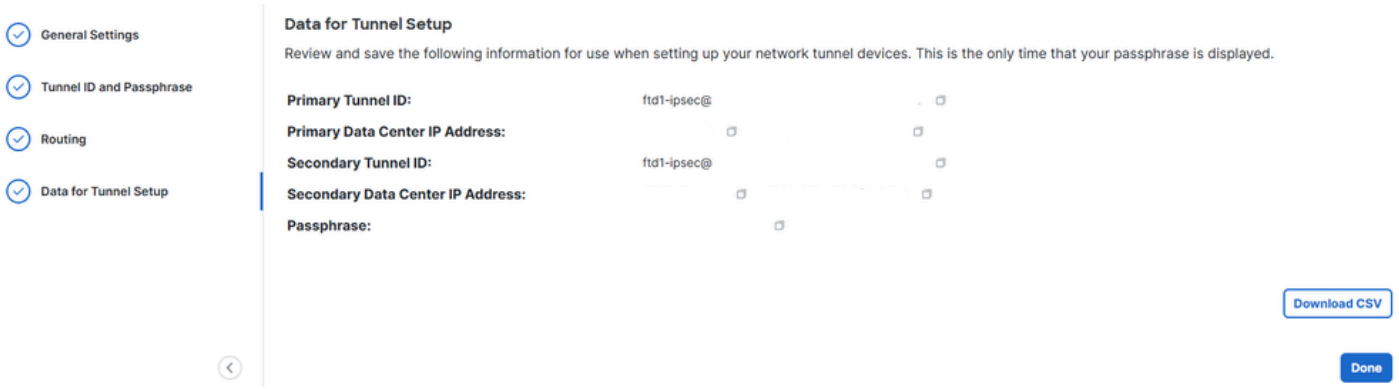


Statisches CSA-Routing

Netzwerk-Tunnelgruppenkonfiguration speichern

Laden Sie die Tunnel-Einrichtungsdaten herunter, und speichern Sie sie, wie es für die FTD-Konfiguration erforderlich ist.

- Klicken Sie Download CSV
- Klicken Sie Done



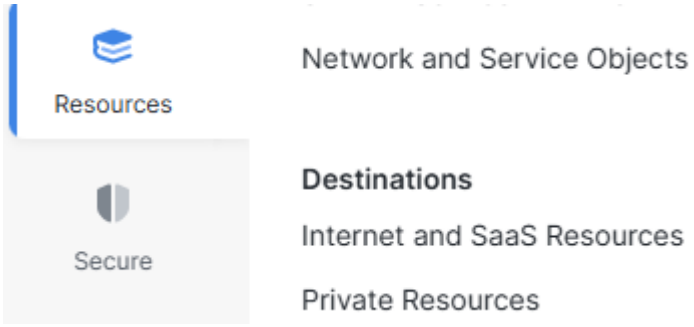
NTG-Daten

Erstellen einer privaten Ressource

Private Ressourcen sind interne Anwendungen, Netzwerke oder Subnetze, die in Ihrem Rechenzentrum oder Ihrer Private Cloud-Umgebung gehostet werden. Diese Ressourcen sind nicht öffentlich zugänglich und werden durch die Infrastruktur Ihres Unternehmens geschützt.

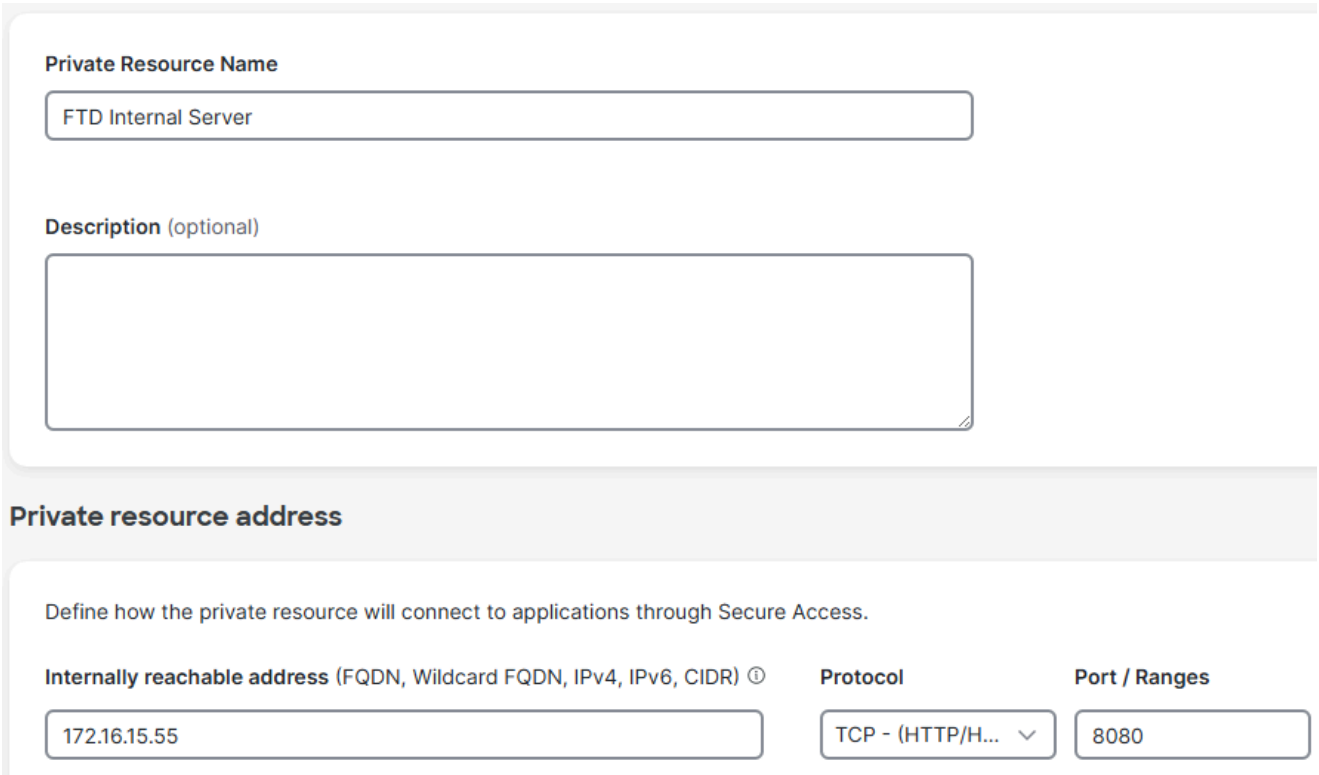
Durch die Definition als private Ressourcen im sicheren Zugriff können Sie einen kontrollierten Zugriff mithilfe von Lösungen wie ZTA (Zero Trust Access) oder VPN-as-a-Service (VPNaaS) ermöglichen. So wird sichergestellt, dass Benutzer basierend auf Identität, Gerätestatus und Zugriffsrichtlinien sicher auf interne Systeme zugreifen können, ohne die Ressourcen direkt dem Internet auszusetzen.

Navigieren Sie zu **Resources** > **Private Resources**> und klicken Sie aufAdd.



PR

- Geben Sie die **Private Resource Name**, Internally reachable address, Protocol, Port/Ranges. Geben Sie Ports und Protokolle an, und fügen Sie bei Bedarf zusätzliche private Ressourcen hinzu.
- Wählen Sie je nach Bedarf die gewünschten Connection Method Verbindungen aus, z. B. Zero-Trust-Verbindungen und/oder VPN-Verbindungen.
- Klicken Sie Save



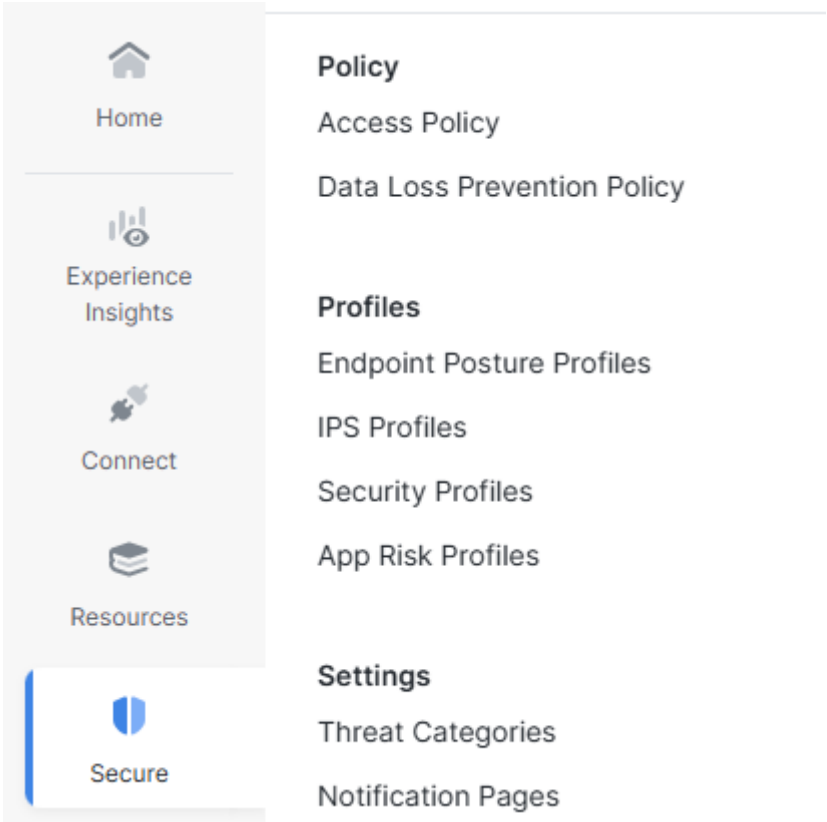
Private Ressource

Erstellen einer Zugriffsrichtlinienregel

Private Zugriffsregeln definieren, wie Benutzer eine sichere Verbindung zu internen Ressourcen und Anwendungen herstellen können, auf die nicht öffentlich zugegriffen werden kann.

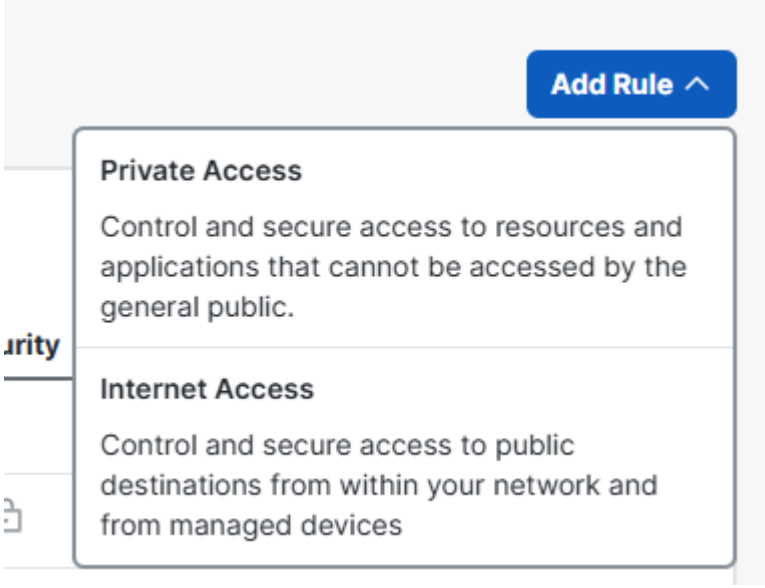
Mit diesen Regeln wird die Sicherheit durchgesetzt, indem gesteuert wird, wer auf bestimmte private Ressourcen zugreifen kann, und zwar basierend auf Faktoren wie der Benutzeridentität, der Gruppenmitgliedschaft, dem Gerätestatus, dem Standort oder anderen Richtlinienbedingungen. So wird sichergestellt, dass sensible interne Systeme vor dem allgemeinen öffentlichen Zugriff geschützt bleiben und gleichzeitig für autorisierte Benutzer über ZTA oder VPNaaS sicher verfügbar sind.

Navigieren Sie zu Secure>Access Policy



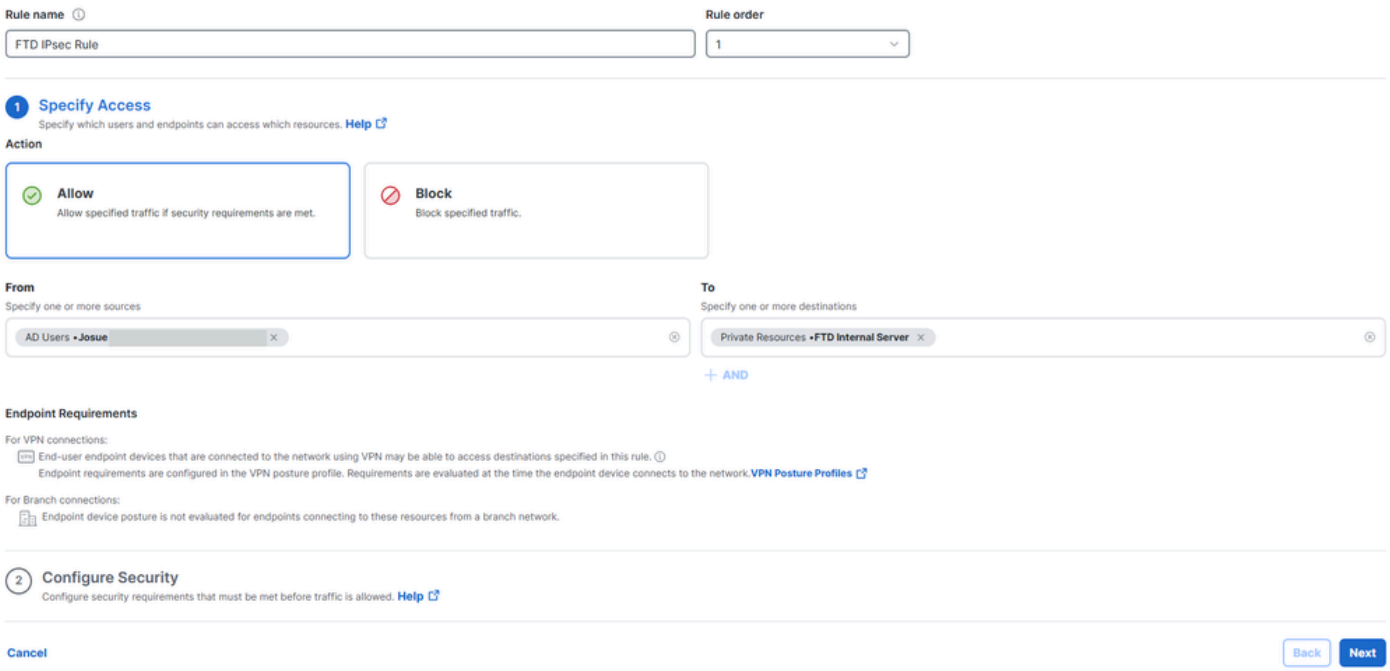
AKP

- Klicken Sie Add Rule
  - Klicken Sie Private Access



ACP hinzufügen

- Klicken Sie auf Rule Name , und geben Sie ihm einen Namen.
- Klicken Sie aufAction, und wählen Sie Allowaus, um diesen Datenverkehr zuzulassen.
- Klicken SieFromauf, und geben Sie die Benutzer an, denen die Berechtigung erteilt wurde.
- Klicken Sie auf Tound geben Sie den Zugriff an, den diese Benutzer basierend auf dieser Regel haben.
- Klicken Sie aufNext, und dann Savein der nächsten Seite



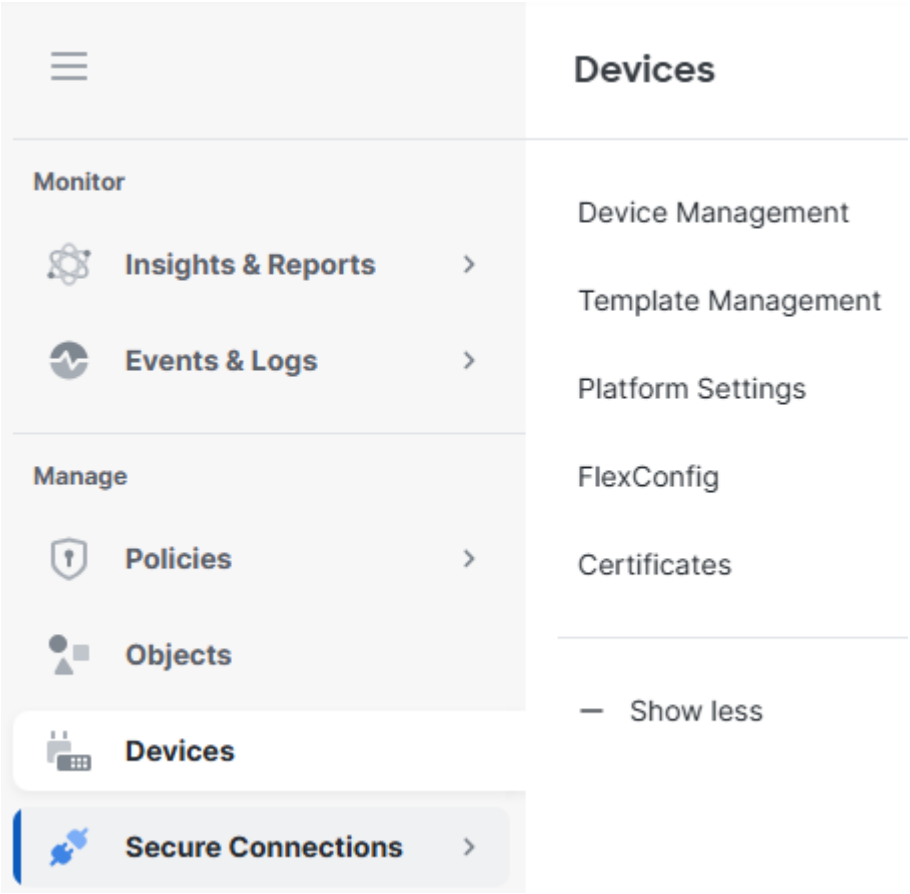
AKP-Konfiguration

Konfiguration der sicheren Firewall-Bedrohungsabwehr (FTD)

Konfiguration der virtuellen Tunnelschnittstellen

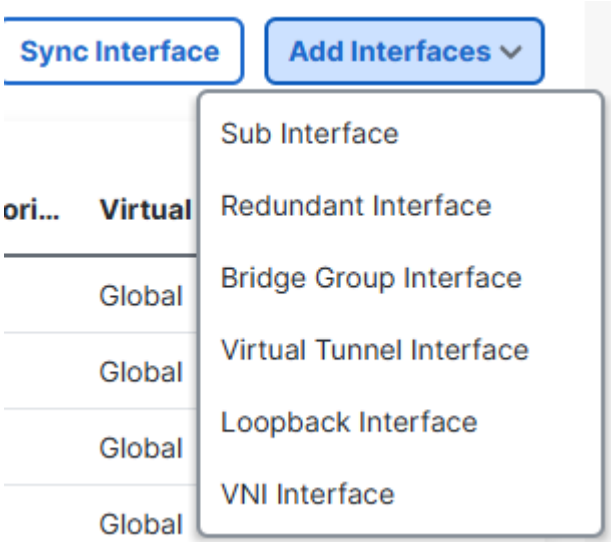
Eine Virtual Tunnel Interface (VTI) auf FTD ist eine logische Layer 3-Schnittstelle, die zum Konfigurieren von routenbasierten IPsec-VPN-Tunneln verwendet wird.

1. Navigieren Sie zu Devices> Device Management.



FTD-Geräte

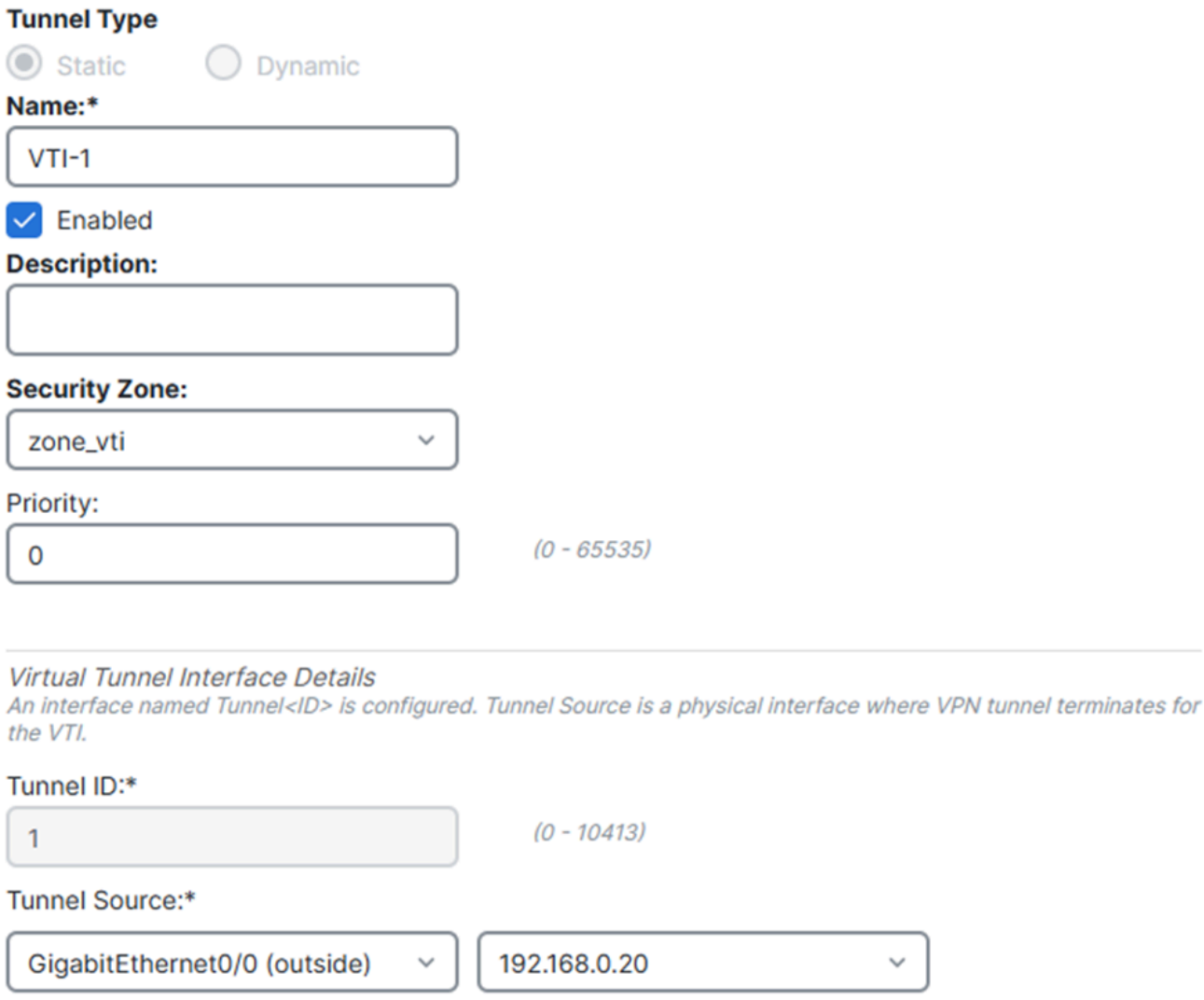
- Klicken Sie auf das FTD-Gerät, Interfaces
  - Klicken Sie Add Interfaces
  - Klicken Sie Virtual Tunnel Interface
  - Erstellung von zwei virtuellen Tunnelschnittstellen, eine für den primären sicheren Access Hub und eine weitere für den sekundären sicheren Access Hub



VTIs hinzufügen

Virtuelle Tunnelschnittstelle 1:

- Gib ihm einen Namen, klicke auf Enable
- Wählen oder erstellen Sie eine Security Zone
- Klicken Sie auf Tunnel ID und geben Sie ihm einen Wert.
- Klicken Sie auf Tunnel Source , und geben Sie die WAN-Schnittstelle an, von der der Tunnel erstellt werden soll.
- Klicken Sie auf IPsec Tunnel Mode, wählen SieIPv4
- Klicken Sie auf IP Address , und konfigurieren Sie die IP-Adresse für den VTI.
- Klicken SieOK

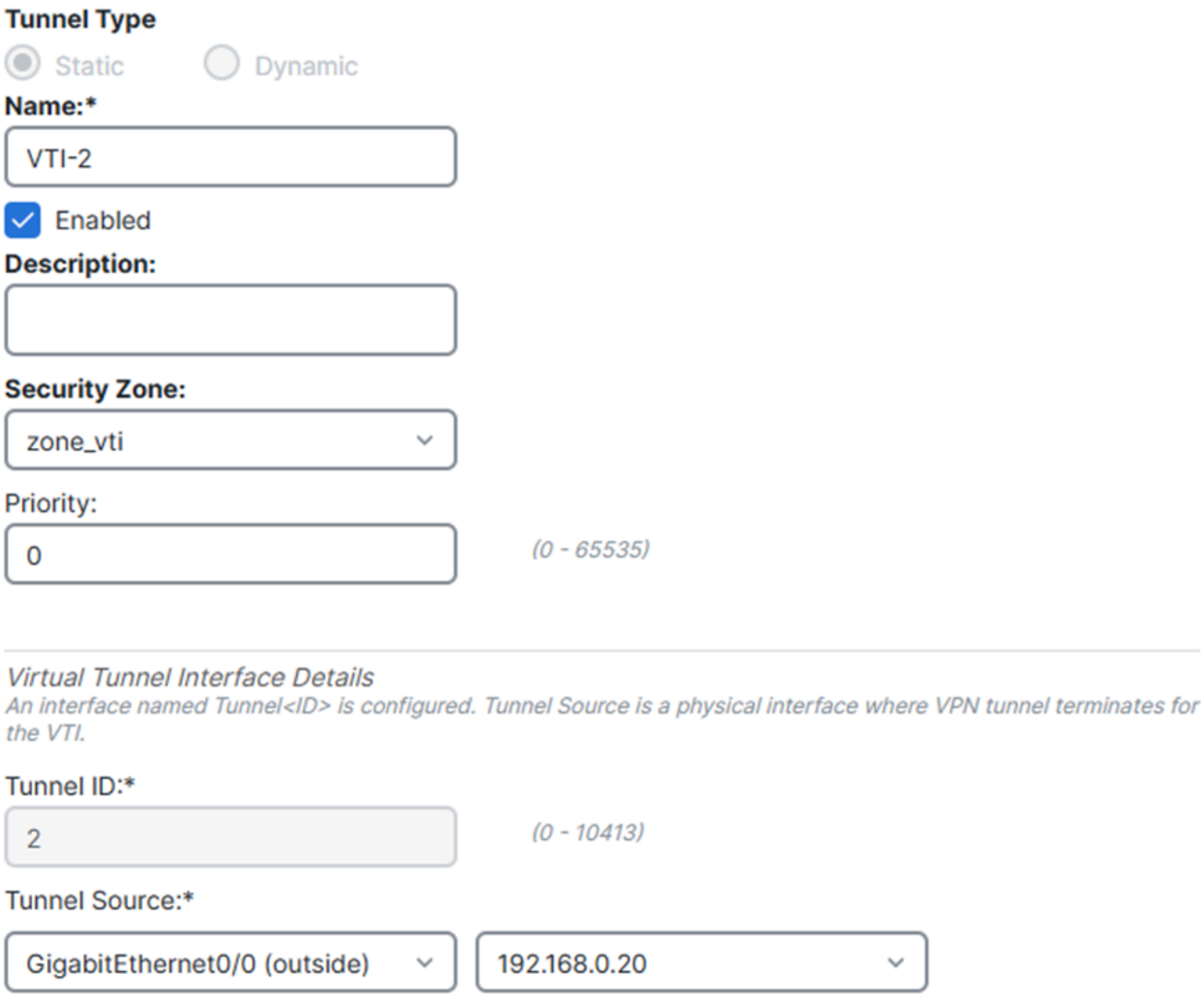


VTI 1.1

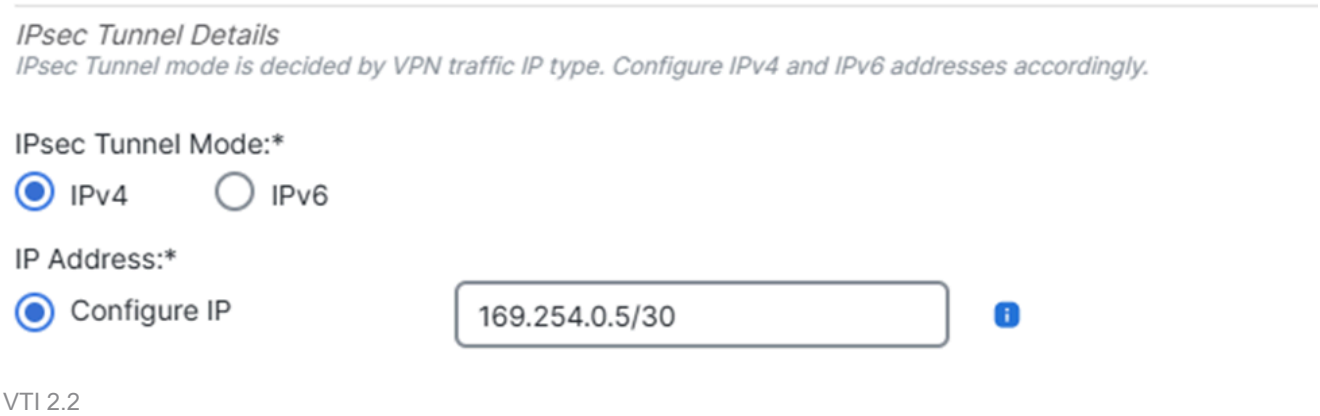
VTI1,2

Virtuelle Tunnelschnittstelle 2:

- Gib ihm einen Namen, klicke auf Enable
- Wählen oder erstellen Sie eine Security Zone
- Klicken Sie auf Tunnel ID , und geben Sie ihm einen Wert
- Klicken Sie auf Tunnel Source , und geben Sie die WAN-Schnittstelle an, von der der Tunnel erstellt werden soll.
- Klicken Sie auf IPsec Tunnel Mode, wählen SieIPv4
- Klicken Sie auf IP Address , und konfigurieren Sie die IP-Adresse für den VTI.
- Klicken SieOK

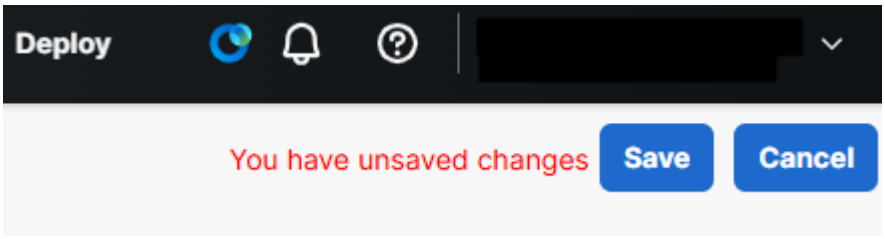


VTI 2.1



VTI 2.2

- Klicken Sie auf Speichern.

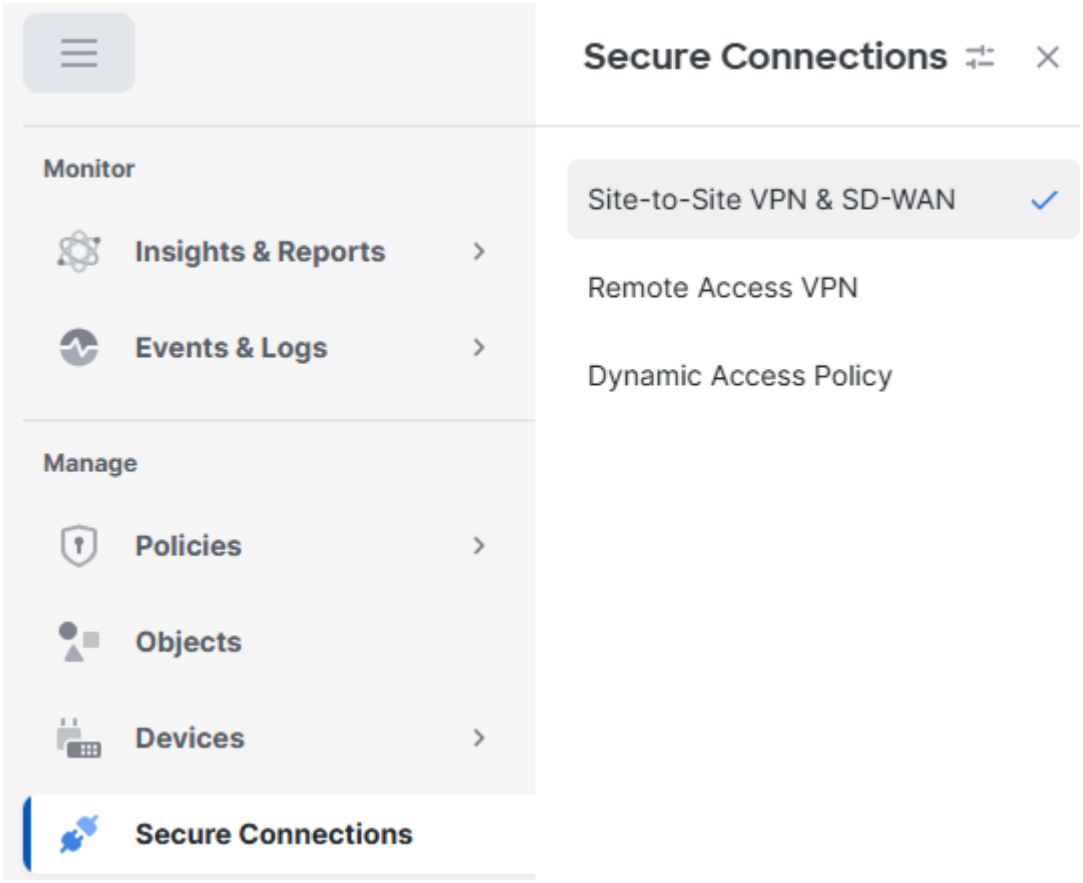


VTI-Änderungen speichern

IPsec-Tunnelkonfiguration

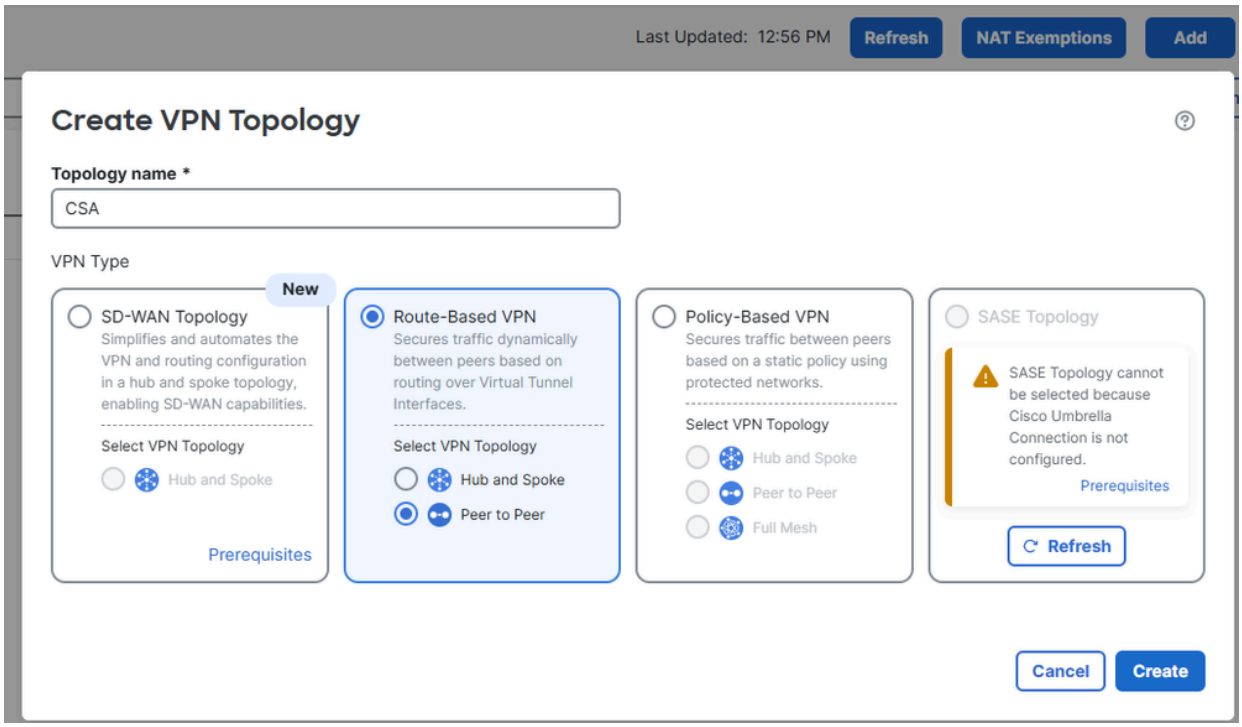
Navigieren Sie zu Ihrem cdFMC-Dashboard.

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



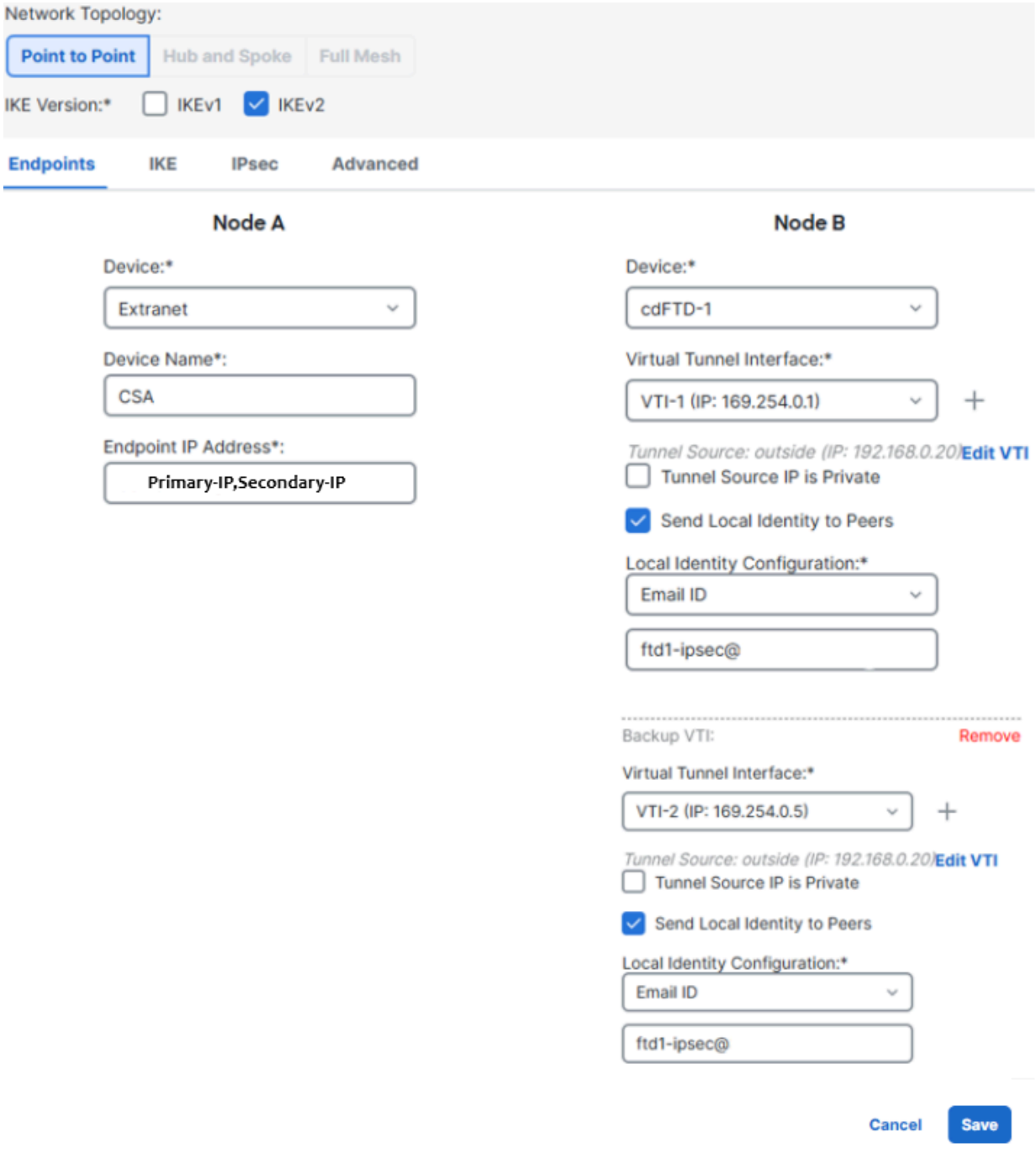
S2S

- Klicken SieAdd
  - Klicken Sie Route-Based VPN
  - Klicken Sie Peer to Peer



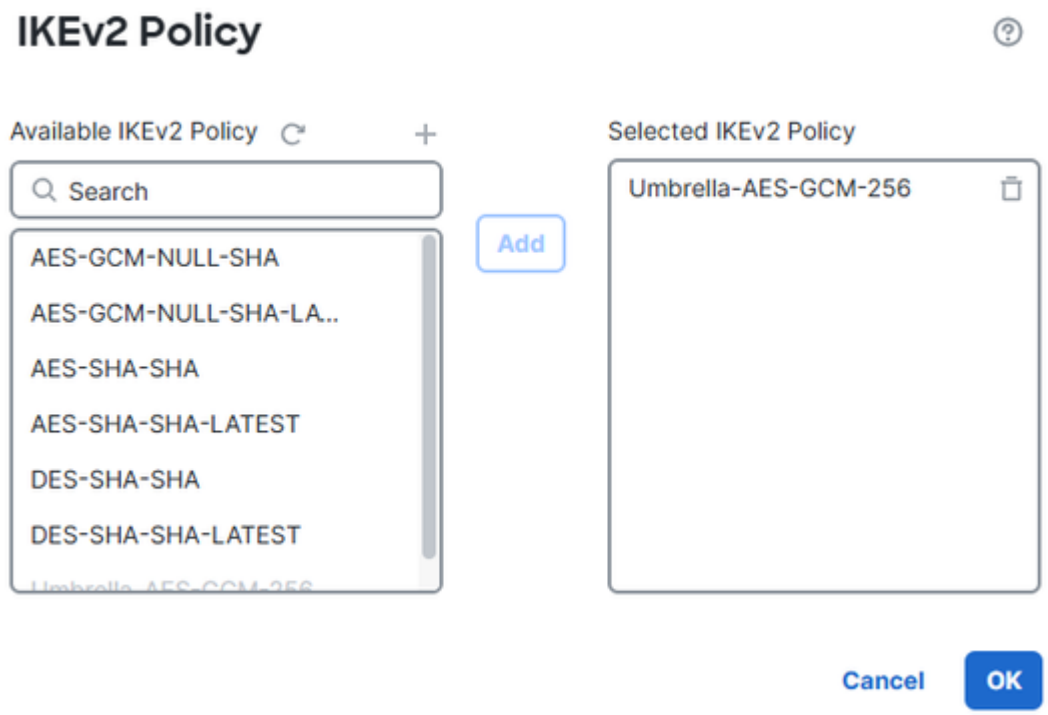
VPN hinzufügen

- Rufen Sie in Schritt 5 der Konfiguration für sicheren Zugriff die Tunnel-IDs und IP-Adressen für das primäre und sekundäre Rechenzentrum ab.
- Klicken SieEndpoints
  - Klicken Sie unterNode Aauf und wählenDeviceSie Extranet
  - Klicken Sie auf Device Nameund geben Sie ihm einen Namen.
  - Klicken Sie auf Enpoint IP Addresses , und geben Sie die primäre und sekundäre IP-Adresse für sicheren Zugriff durch ein Komma getrennt ein (aus "Save Network Tunnel Group Configuration" unter Sicherer Zugriff).
    Konfiguration)
  - Klicken Sie unter Node BaufDeviceund wählen Sie Ihr FTD-Gerät aus.
  - Klicken Sie auf Virtual Tunnel Interface , und wählen Sie die erste im vorherigen Schritt erstellte VTI-Schnittstelle aus.
  - Klicken Sie auf Send Local Identity to Peers Option und wählen Sie Email ID, geben Sie die primäre Tunnel-ID (aus "Save Network Tunnel Group Configuration" unter Secure Access Configuration)
  - Klicken Sie Add Backup VTI
  - Klicken Sie auf Virtual Tunnel Interface , und wählen Sie die zweite im vorherigen Schritt erstellte VTI-Schnittstelle aus.
  - Klicken Sie aufSend Local Identity to Peerseine Option, und wählen Sie Email ID, geben Sie die sekundäre Tunnel-ID ein (unter "Save Network Tunnel Group Configuration" unter Secure Access Configuration).
  - Klicken Sie auf Speichern



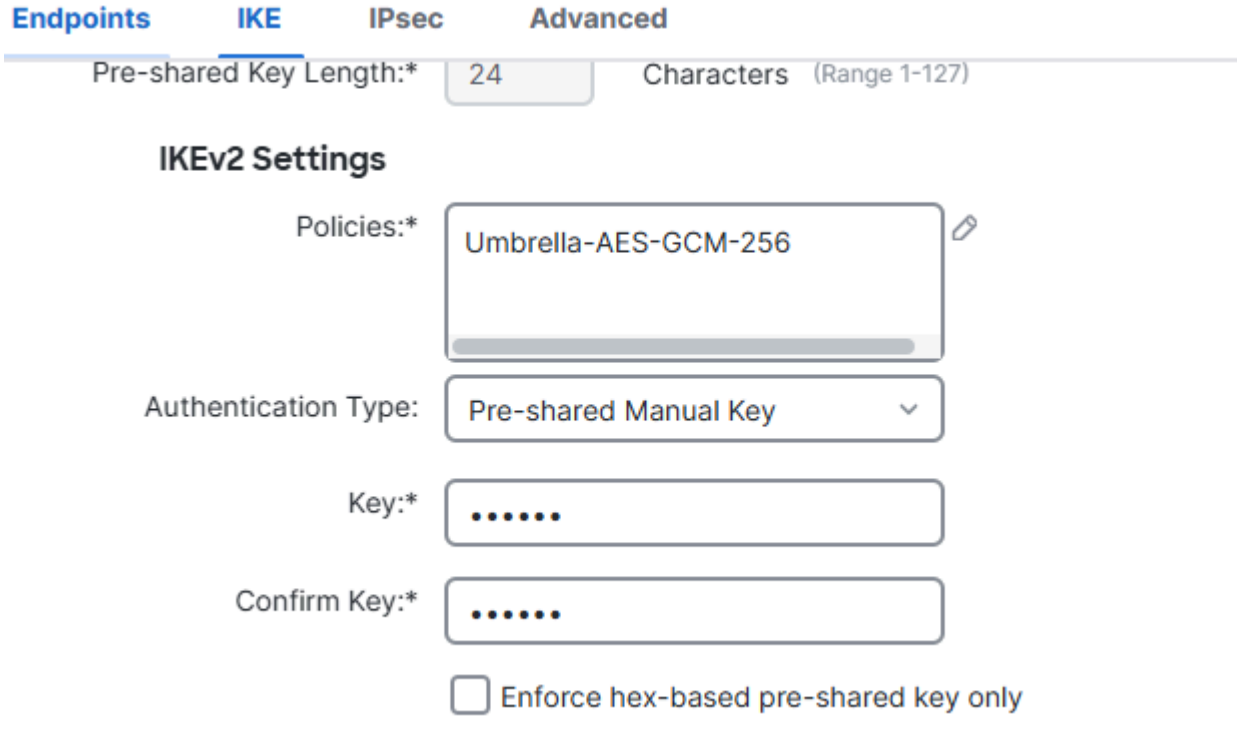
FTD VTI-Konfiguration

- Klicken SieIKE
  - Auf **IKEv2 Settings** > klicken Policies
  - Wählen Sie dieUmbrella-AES-GCM-256Option
  - Klicken Sie OK



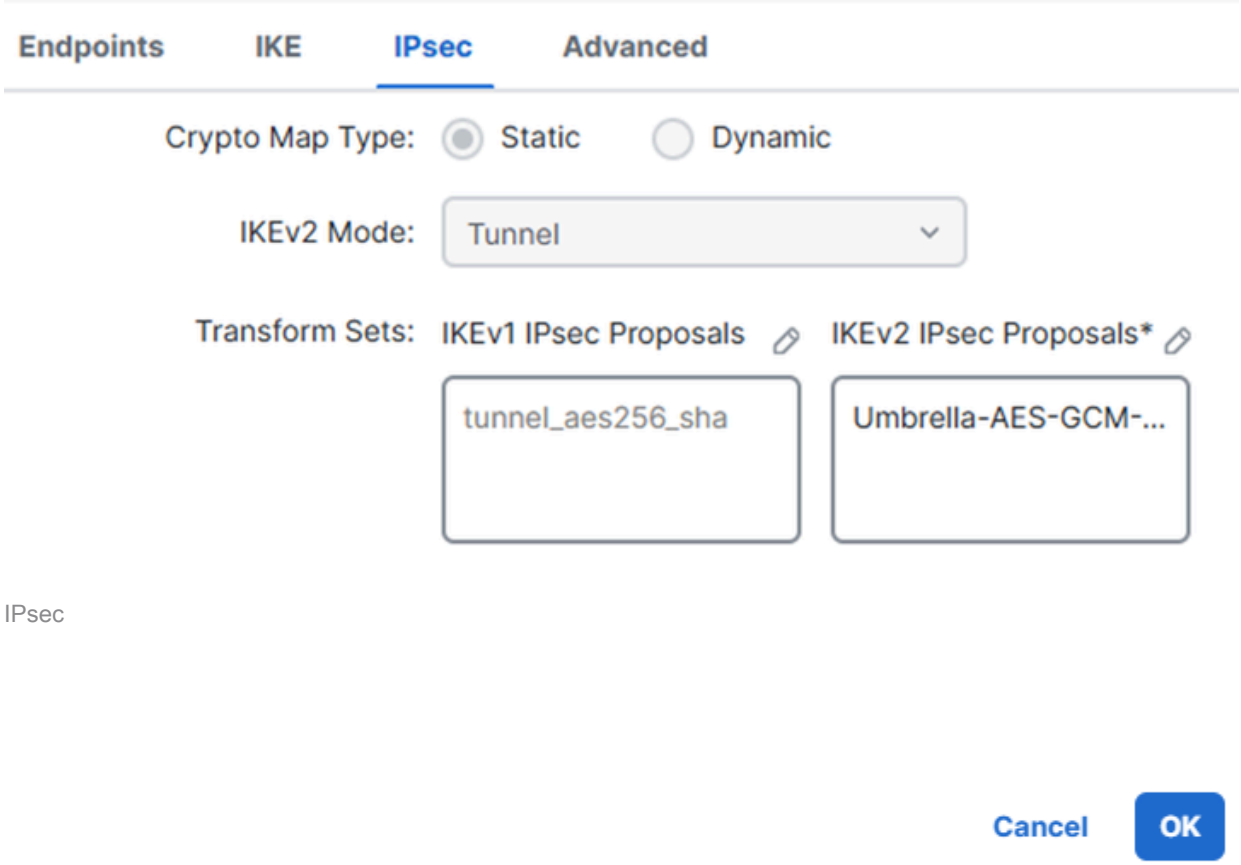
IKEv2-Richtlinie

- Klicken Sie auf Authentication Type , und wählen SiePre Shared Manual Key, geben Sie den PSK ein, der unter Sicherer Zugriff (Passphrase) konfiguriert wurde.



IKE

- Klicken Sie IPSEC
  - Klicken Sie IKEv2 Proposals
  - Auswählen Umbrella-AES-GCM-256
  - Klicken Sie OK



IPsec

IKEv2-Angebote speichern

FTD-Routing-Konfiguration

Mit richtlinienbasiertem Routing (Policy-Based Routing, PBR) können Sie die Weiterleitung von Datenverkehr anhand von Kriterien steuern, die über die Ziel-IP-Adresse hinausgehen. Der PBR verlässt sich nicht mehr ausschließlich auf die Routing-Tabelle, sondern kann den Datenverkehr basierend auf der Quelle, der Anwendung, dem Protokoll, den Ports oder anderen definierten Richtlinien routen.

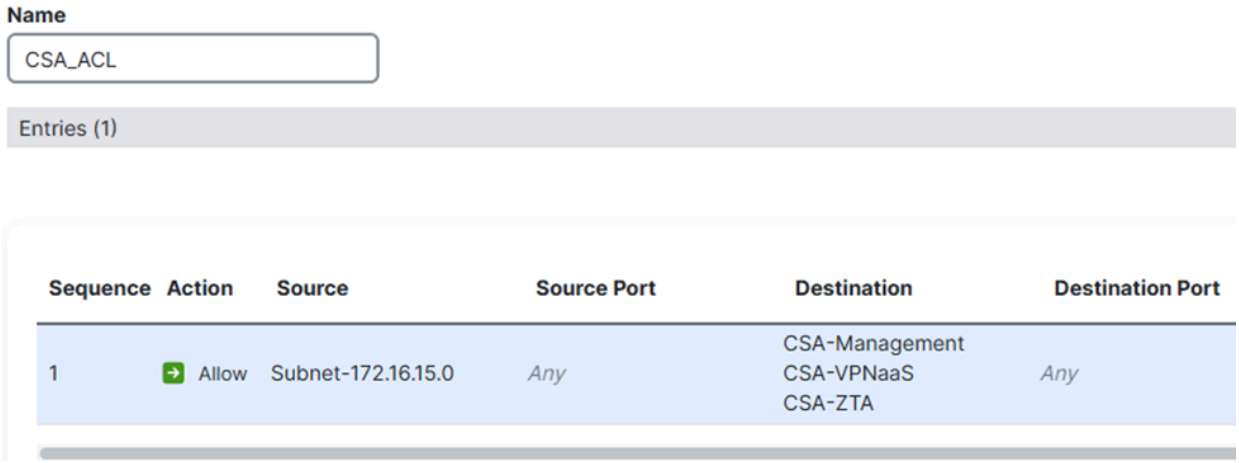
Auf diese Weise können Unternehmen bestimmten oder vorrangigen Datenverkehr über bevorzugte Verbindungen (z. B. eine Verbindung mit hoher Bandbreite oder eine direkte Internetverbindung) steuern, die Leistung optimieren und bestimmte Anwendungen sicher ausbrechen, ohne den gesamten Datenverkehr über einen VPN-Tunnel zu senden.

Richtlinienbasiertes Routing

- Navigieren Sie zu Objects
  - Klicken Sie Access List
  - Klicken Sie Extended
  - Klicken SieAdd Extended Access List

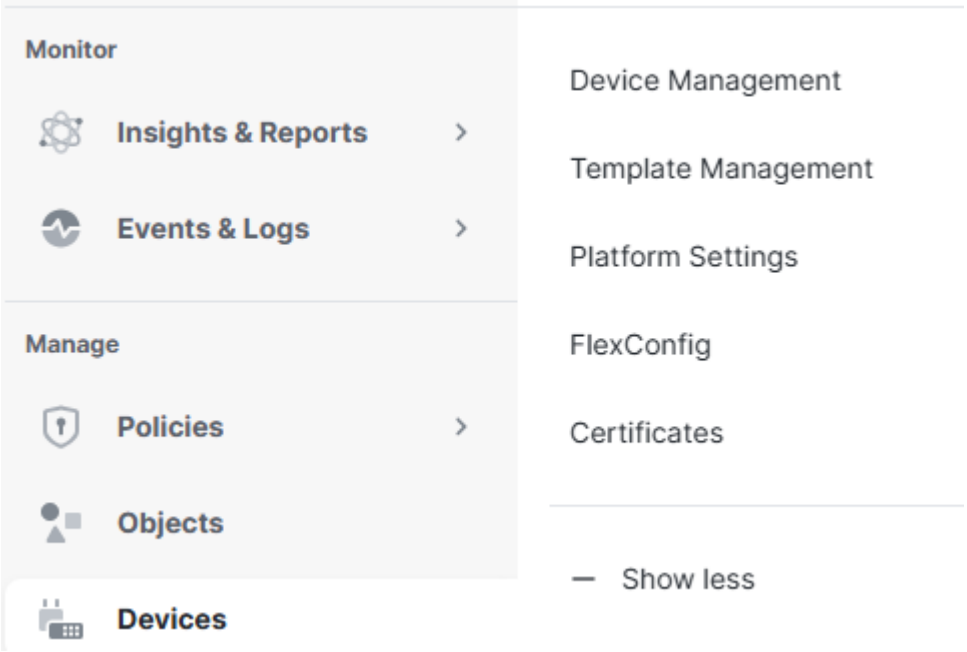
ACL hinzufügen

Erstellen Sie eine erweiterte Zugriffskontrollliste (ACL), die mit dem durch den FTD geschützten Quellnetzwerk (z. B. 172.16.15.0/24) übereinstimmt, das durch den Tunnel gesendet werden soll. Fügen Sie als Ziel die von ZTA verwendeten Netzwerke (CGNAT-Bereich) und das von Ihrem VPNaaS verwendete Netzwerk hinzu (siehe IP-Pool des virtuellen privaten Netzwerks).



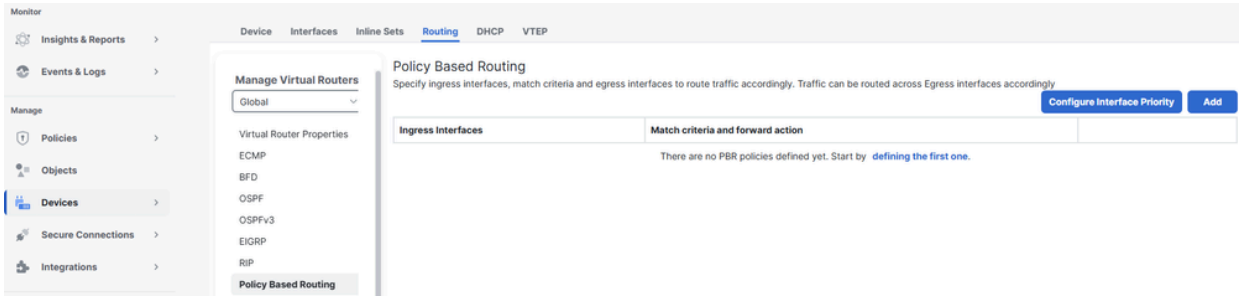
ACL

- Auf Devices> Device Management



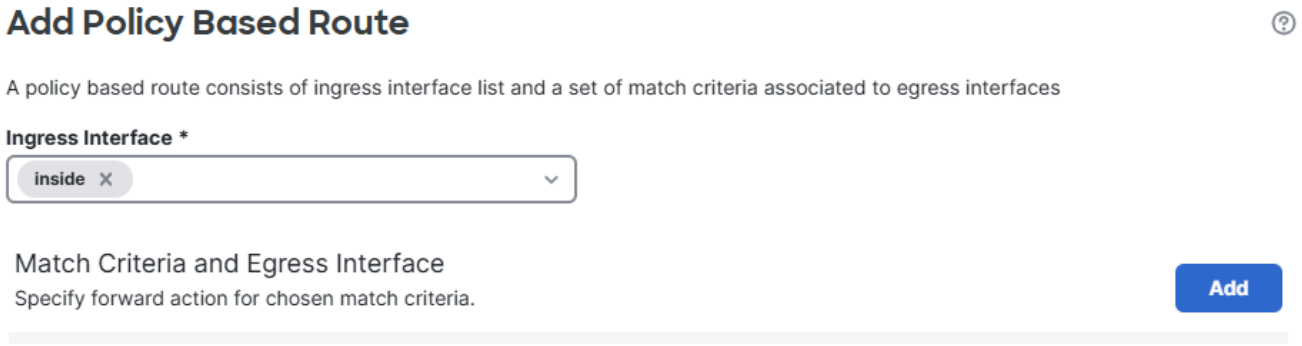
"Slot0:"

- Klicken Sie auf die FTD
  - Klicken SieRouting
  - Klicken Sie Policy Based Routing
  - Klicken Sie Add



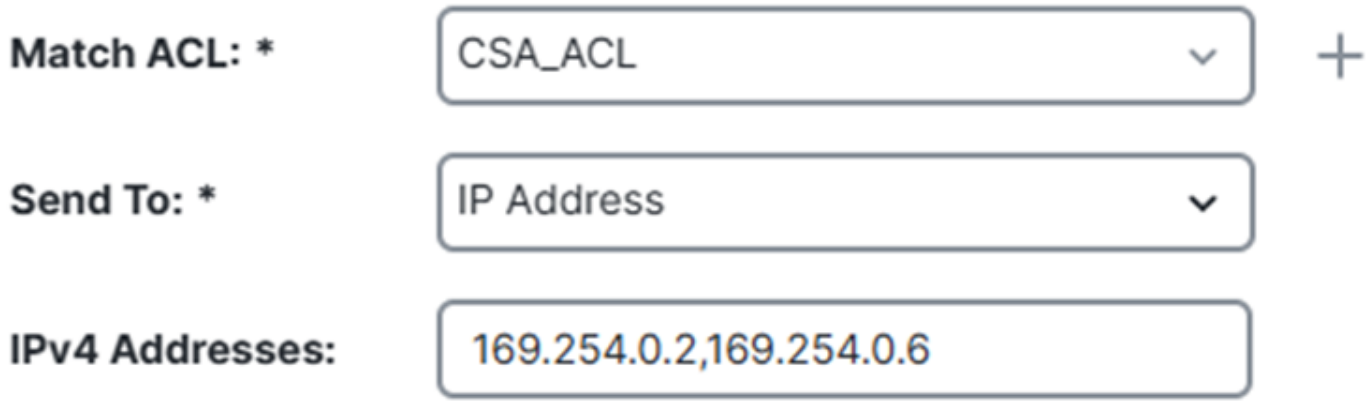
PBR hinzufügen

- Klicken Sie auf Ingress Interface , und wählen Sie die Eingangsschnittstelle aus, über die der Datenverkehr aus internen Netzwerken eingeht.
- Klicken Sie unter "Match Criteria" und "Egress Interface" auf Add



Eingangsschnittstelle

- Klicken Sie auf Match ACL , und wählen Sie die zuvor erstellte erweiterte Zugriffskontrollliste aus.
- Klicken Sie Send To and select IP Address
- Klicken Sie auf IPv4 Addresses , und legen Sie die IP-Adressen in den zuvor im FTD konfigurierten VTI-Schnittstellen-Subnetzen als nächste Hops fest (169.254.0.2 und 169.254.0.6).
- Klicken Sie Save



Richtlinienbasierte Konfiguration

PBR speichern

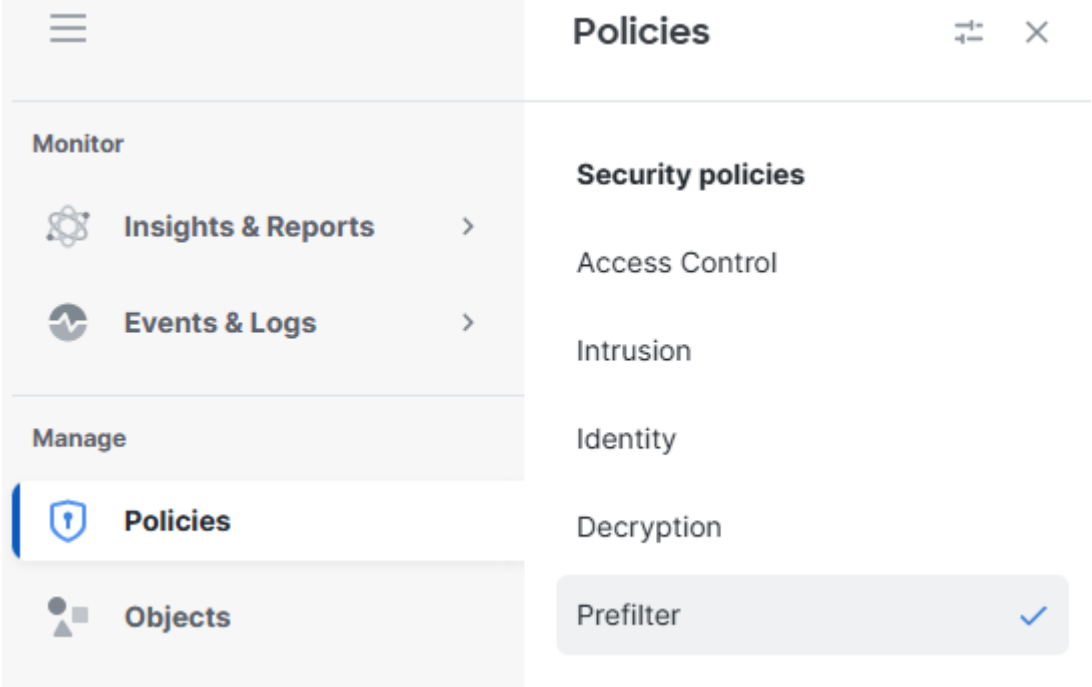
Stellen Sie sicher, dass Sie die Option Send To > IP Address und nicht die Egress Interface Option auswählen.

Konfiguration der Zugriffsrichtlinie

Um Datenverkehr über eine Cisco FirePOWER Threat Defense (FTD) zuzulassen und den Zugriff auf private Ressourcen zu ermöglichen, muss der Datenverkehr zunächst die erste Phase der Zugriffskontrolle passieren, die als Vorfilterung bezeichnet wird.

Die Vorfilterung wird vor der tiefer gehenden Prüfung verarbeitet und ist einfach und schnell konzipiert. Zur Bewertung des Datenverkehrs werden grundlegende Kriterien des äußeren Headers (wie Quell- und Ziel-IP-Adressen und -Ports) herangezogen, um Datenverkehr schnell zuzulassen, zu blockieren oder zu umgehen. Wenn der Datenverkehr in dieser Phase zugelassen wird, können ressourcenintensivere Prüfungen wie Deep Packet Inspection oder Intrusion Policies übersprungen werden, wodurch die Leistung verbessert und gleichzeitig die Sicherheitskontrolle aufrechterhalten wird.

- Navigieren Sie zu Policies> Prefilter



Vorfilter

- Klicken Sie auf die von Ihrer Zugriffsrichtlinie verwendete Vorfilterrichtlinie bearbeiten.

Vorfilter anklicken

- Klicken Sie Add Tunnel Rule
  - Hinzufügen und Zulassen des Datenverkehrs aus dem VPNaaS-Netzwerk und/oder dem ZTA-Subnetz zu Ihren privaten Ressourcen
  - Klicken SieSave

Regel speichern

Sobald die Konfiguration auf dem FTD abgeschlossen und verifiziert wurde, können Sie mit der

Bereitstellung fortfahren. Nach der Bereitstellung werden die IPsec-Tunnel erfolgreich hochgefahren und bestätigen, dass eine sichere Verbindung zu den privaten Ressourcen hergestellt ist.

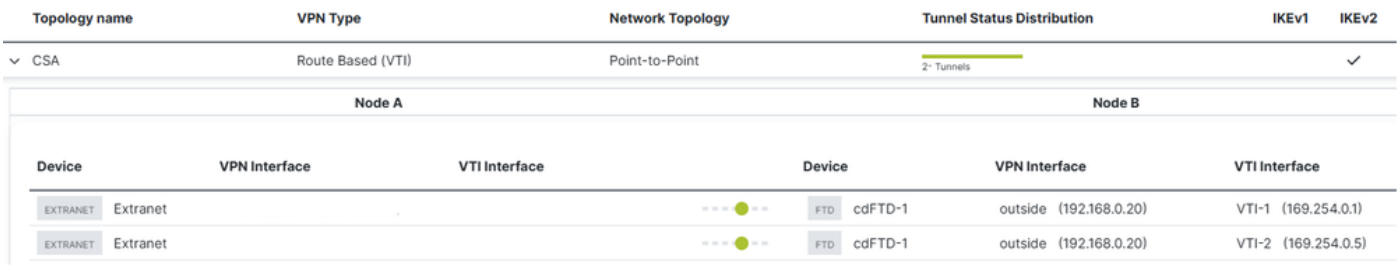
Überprüfung

In FTD überprüfen

Tunnelstatus in FTD

Sie können den aktuellen Status des Tunnels anzeigen, einschließlich dessen, ob er aktiv oder inaktiv ist. Dadurch kann überprüft werden, ob der IPsec-Tunnel ordnungsgemäß eingerichtet ist.

- Klicken Sie auf Sichere Verbindungen.
- Klicken Sie auf Site-to-Site-VPN und SD-WAN.
- Klicken Sie auf den Topologienamen.



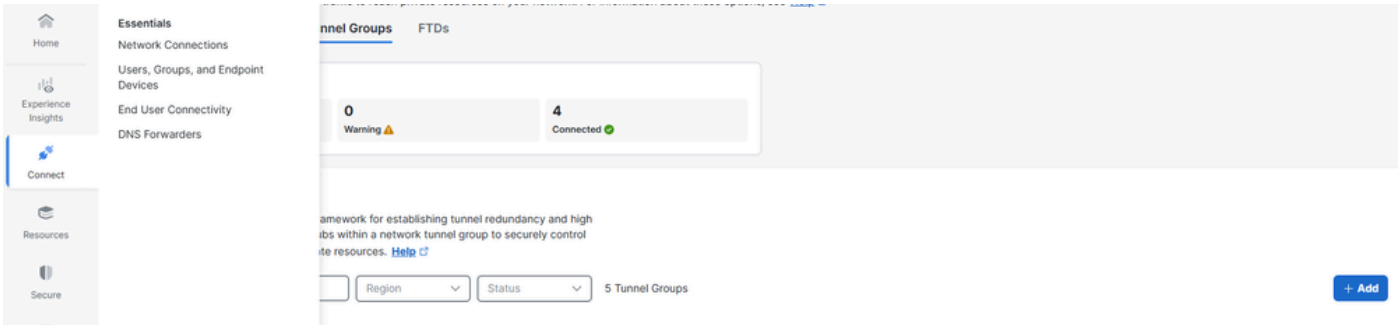
FTD-Tunnelstatus

Überprüfung in sicherem Zugriff

Tunnelstatus bei sicherem Zugriff

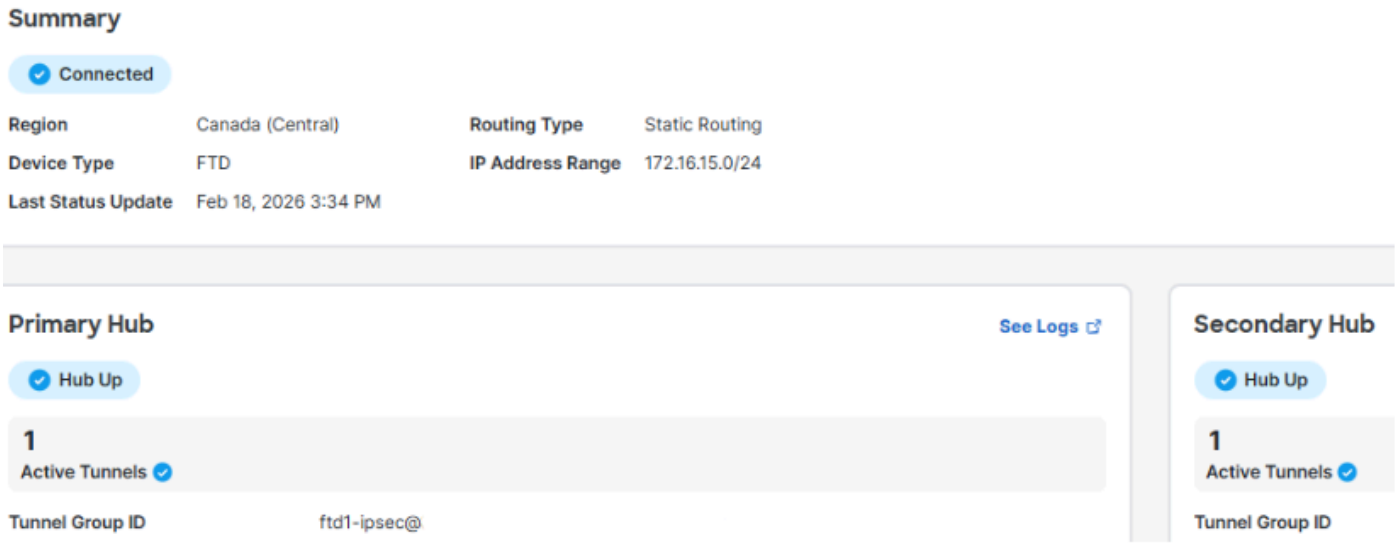
Sie können den aktuellen Status des Tunnels anzeigen, einschließlich ob er "Getrennt", "Warnung" oder "Verbunden" ist. Dadurch kann überprüft werden, ob der IPsec-Tunnel ordnungsgemäß eingerichtet ist.

- Klicken Sie auf Verbinden > Netzwerkverbindungen.
- Klicken Sie auf Network Tunnel Groups (Netzwerktunnelgruppen)



NTG überprüfen

- Klicken Sie auf die Netzwerk-Tunnelgruppe.

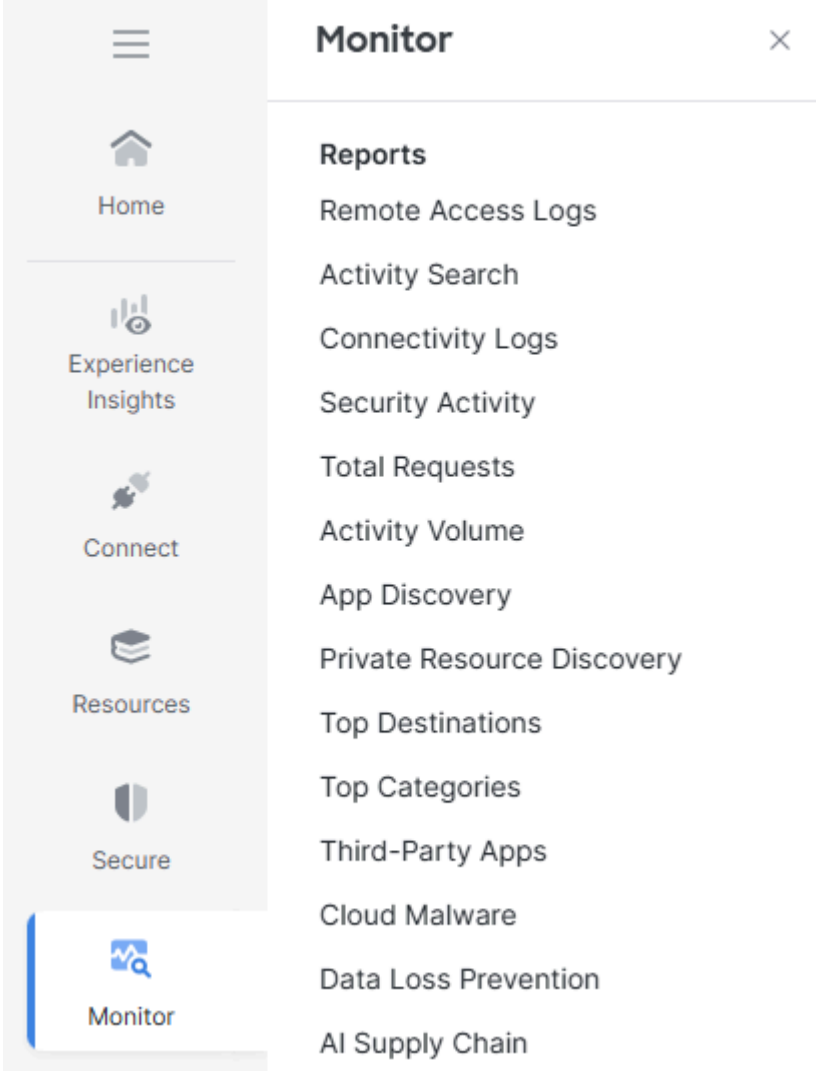


CSA-Tunnelstatus

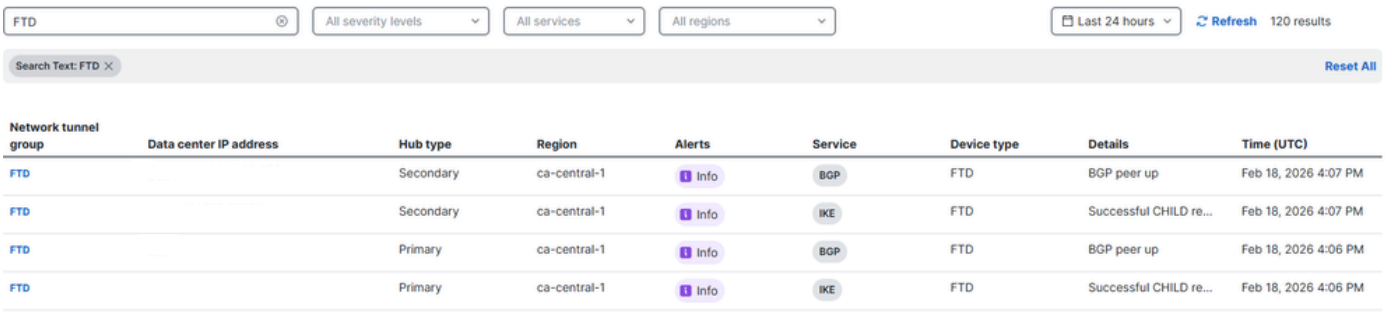
Ereignisse in sicherem Zugriff

Sie können Tunnel-Ereignisse anzeigen und überprüfen, ob der Status der IPsec-Tunnel aktiv und stabil ist.

Klicken Sie auf Monitor > Network Connectivity (Überwachen > Netzwerkverbindung).

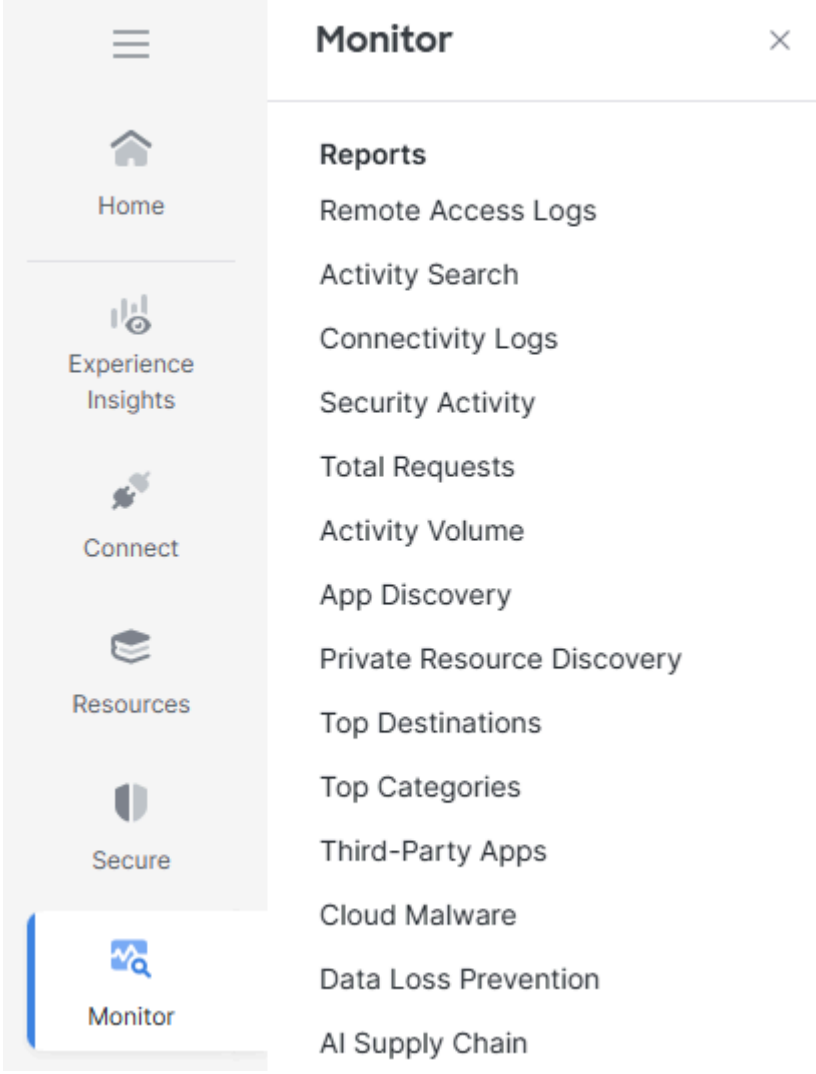


Protokolle überwachen



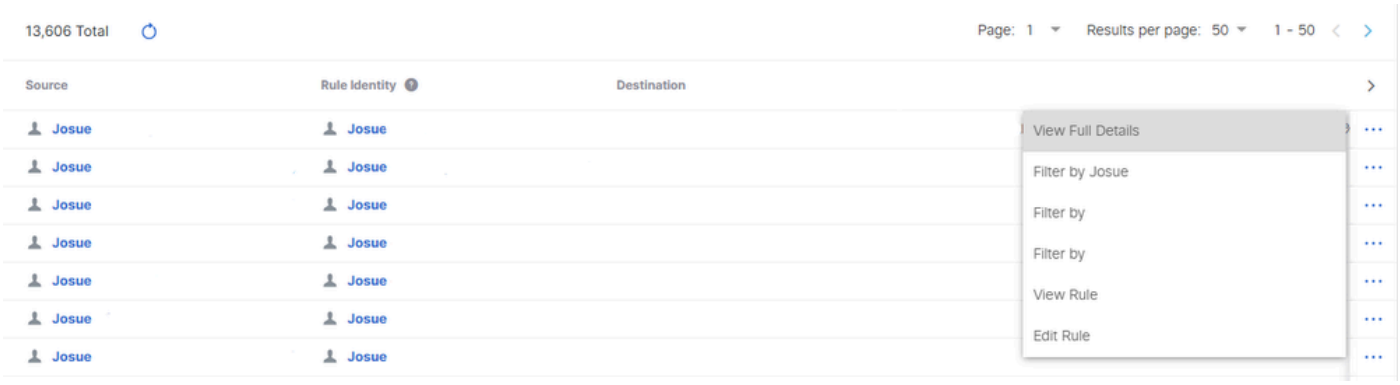
Konn. Protokolle

Navigieren Sie zu auf Monitor > Activity Search.

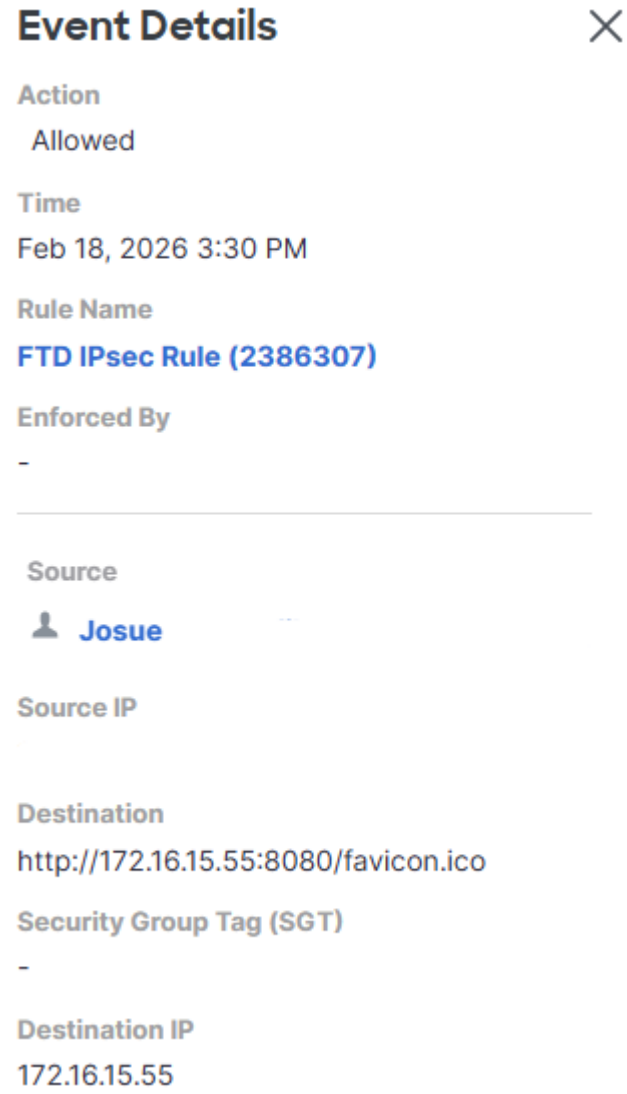


Protokolle überwachen

Klicken Sie bei einem der verwandten Ereignisse auf Alle Details anzeigen.



Vollständige Details



Aktivitätssuche

Zugehörige Informationen

- Technischer Support und Downloads von Cisco
- Konfigurationsanleitung für Cisco Secure Firewall Management Center-Geräte, 7.7

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.