Configurazione di Secure Access con Secure Firewall Threat Defense per l'accesso privato con routing basato su criteri

Sommario

Introduzione

In questo documento viene descritto come configurare Secure Access con FTD tramite IPsec per l'accesso privato sicuro con routing basato su criteri.

Prerequisiti

Requisiti

- Conoscenze Cisco Secure Access
- Dashboard/tenant Cisco Secure Access
- Protezione sicura delle minacce firewall e conoscenza di Centro gestione firewall
- Conoscenza IPSec
- Conoscenze di Routing basate su policy

Componenti usati

- Secure Firewall con codice 7.7.10
- Centro gestione firewall distribuito tramite cloud. La configurazione è valida anche per un tipico FMC virtuale
- Dashboard Cisco Secure Access

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

I tunnel di rete in Secure Access possono essere utilizzati per due scopi principali: Accesso sicuro a Internet e accesso sicuro privato.

Per garantire la protezione dell'accesso privato, le organizzazioni possono utilizzare Zero Trust Access (ZTA) e/o VPN as a Service (VPNaaS) per connettere gli utenti a risorse private quali applicazioni interne o centri dati. I tunnel IPsec svolgono un ruolo chiave in questa architettura grazie alla crittografia protetta del traffico di rete tra gli utenti e le risorse private, che assicura la protezione dei dati sensibili durante l'attraversamento di reti non attendibili. Integrando i tunnel IPsec con ZTA o VPNaaS, le organizzazioni possono fornire un accesso semplice e sicuro alle risorse interne, mantenendo al contempo controlli di sicurezza e visibilità affidabili.

In questo documento viene descritto come configurare Secure Access con Secure Firewall Threat Defense (FTD) tramite IPsec per Secure Private Access.
In questa guida viene inoltre descritto come configurare il routing basato su criteri.

Anche se questo documento descrive la configurazione dei tunnel IPsec per l'accesso privato sicuro, la configurazione di Zero Trust Access (ZTA) o VPN as a Service (VPNaaS) per l'accesso alle applicazioni private esula dalle finalità di questa guida.

Configurazione

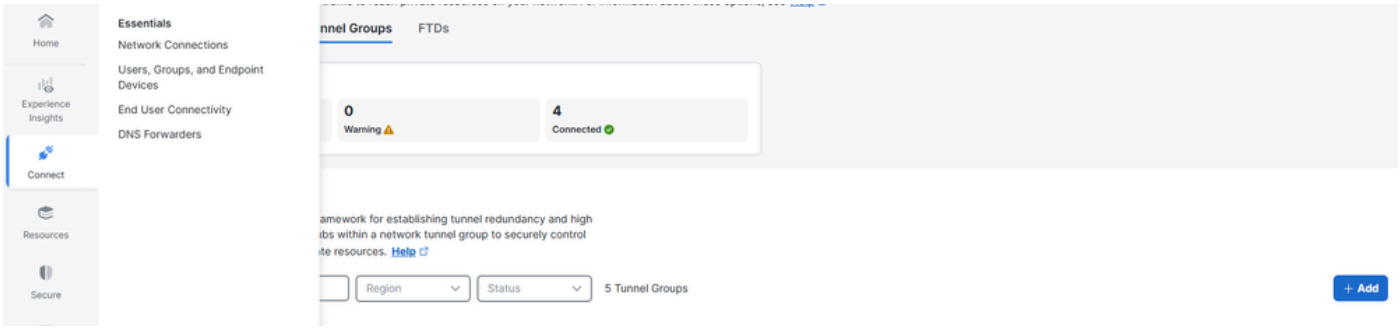
Configurazione accesso sicuro

Configurazione gruppo tunnel di rete

1. Passare al pannello di amministrazione di [Accesso sicuro.](#)

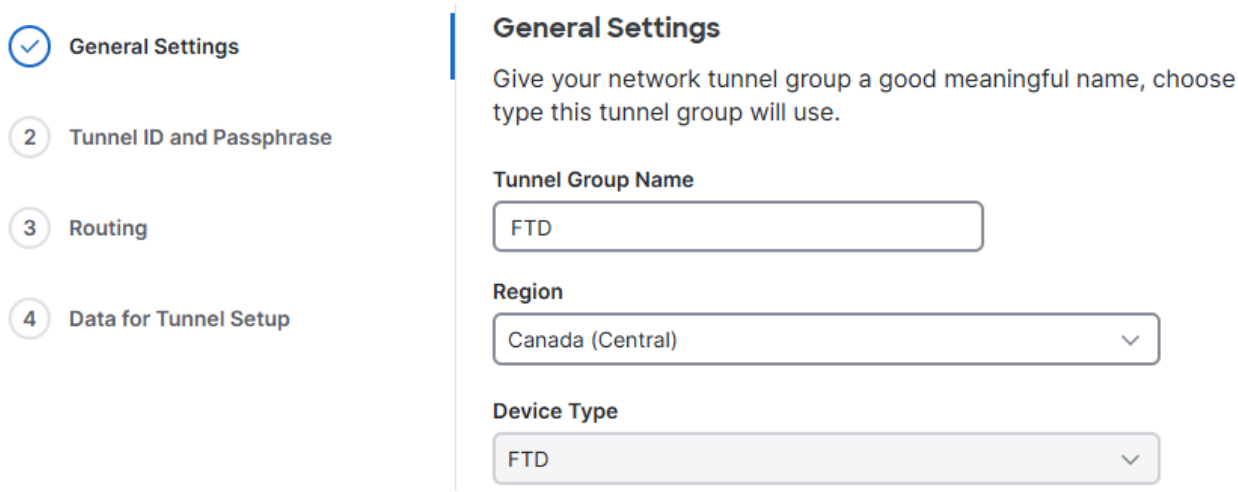
2. Aggiungere un gruppo di tunnel di rete.

- Fai clic suConnect> Network Connections
  - In fare Network Tunnel Groups clic su > Add



3. General Settings Configurazione.

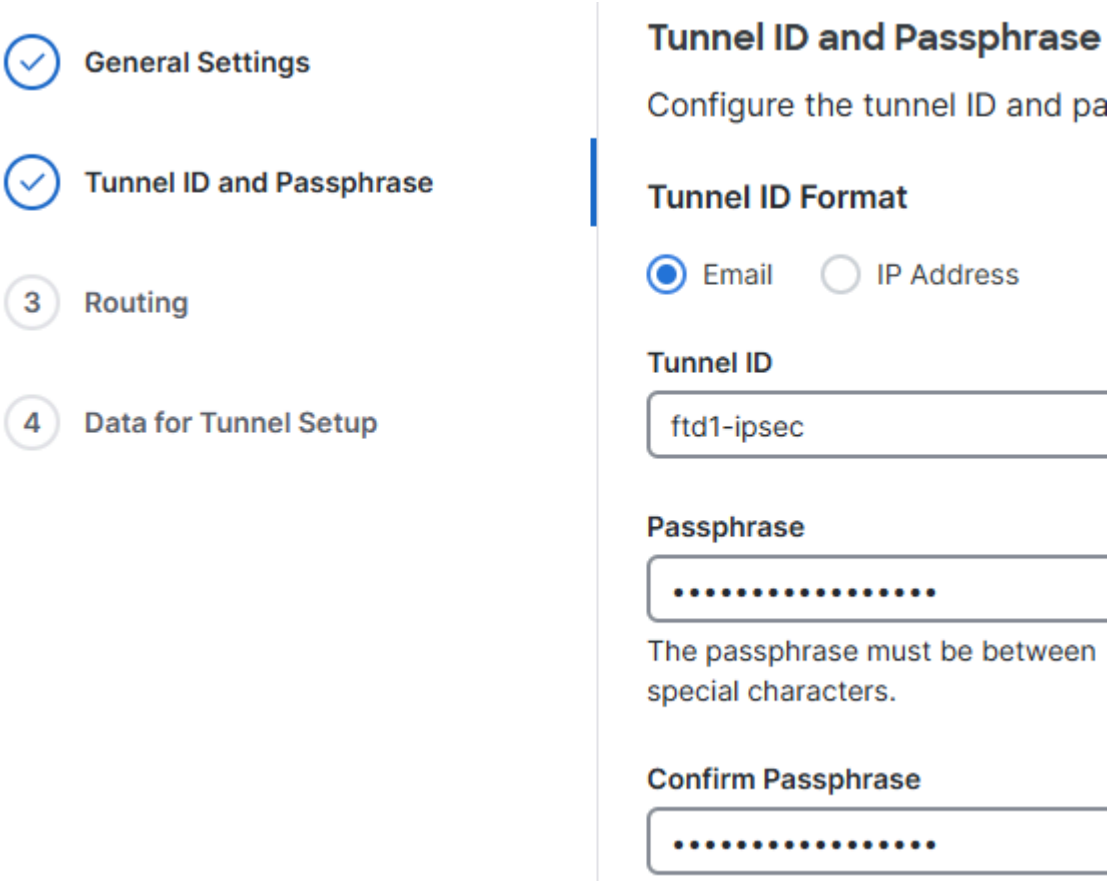
- Configurare Tunnel Group Name, **Region** e Device Type
  - Fare clic su Next



Impostazioni generali

4. Configurare Tunnel ID e Passphrase.

- Configurare l'**Tunnel ID**e Passphrase. Questo ID è importante, in quanto è necessario per la configurazione FTD
- Fare clic su Next



ID e PSK

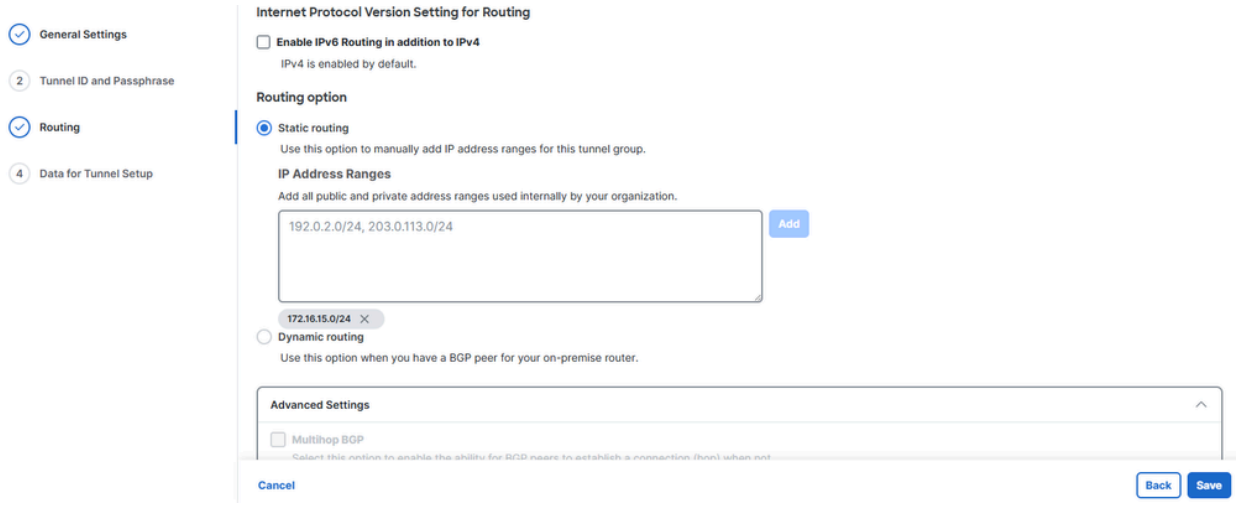
5. Configurare il routing statico.

Secure Access Routing

Policy Based Routing

Aggiungere le reti protette dall'FTD a cui si desidera che gli utenti remoti accedano tramite ZTA e/o VPNaaS e fare clic su Salva.

- Fai clic su Routing> **Static routing**
  - Aggiungere gli intervalli di indirizzi IP o gli host configurati nella rete e passare il traffico attraverso l'accesso sicuro, quindi fare clic suAdd
  - Fare clic suSave

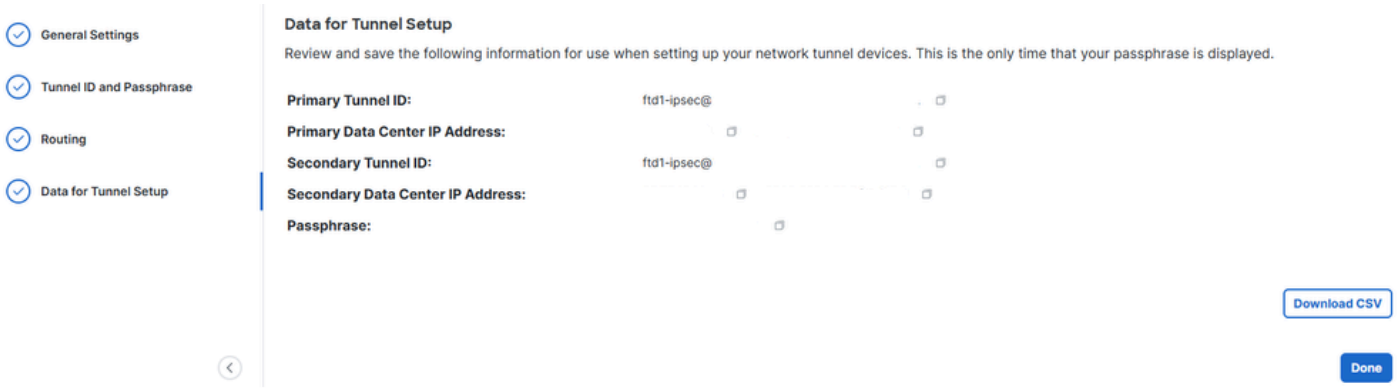


CSA Static Routing

Salva configurazione gruppo tunnel di rete

Scaricare e salvare i dati di configurazione del tunnel come richiesto per la configurazione FTD.

- Fare clic su Download CSV
- Fare clic su Done



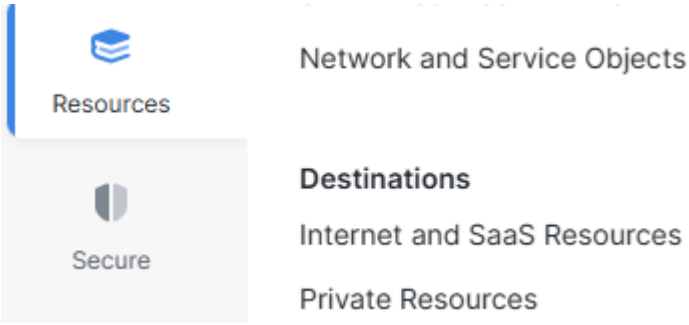
Dati NTG

Crea una risorsa privata

Le risorse private sono applicazioni interne, reti o subnet ospitate nel centro dati o in un ambiente cloud privato. Queste risorse non sono accessibili pubblicamente e sono protette dietro l'infrastruttura dell'organizzazione.

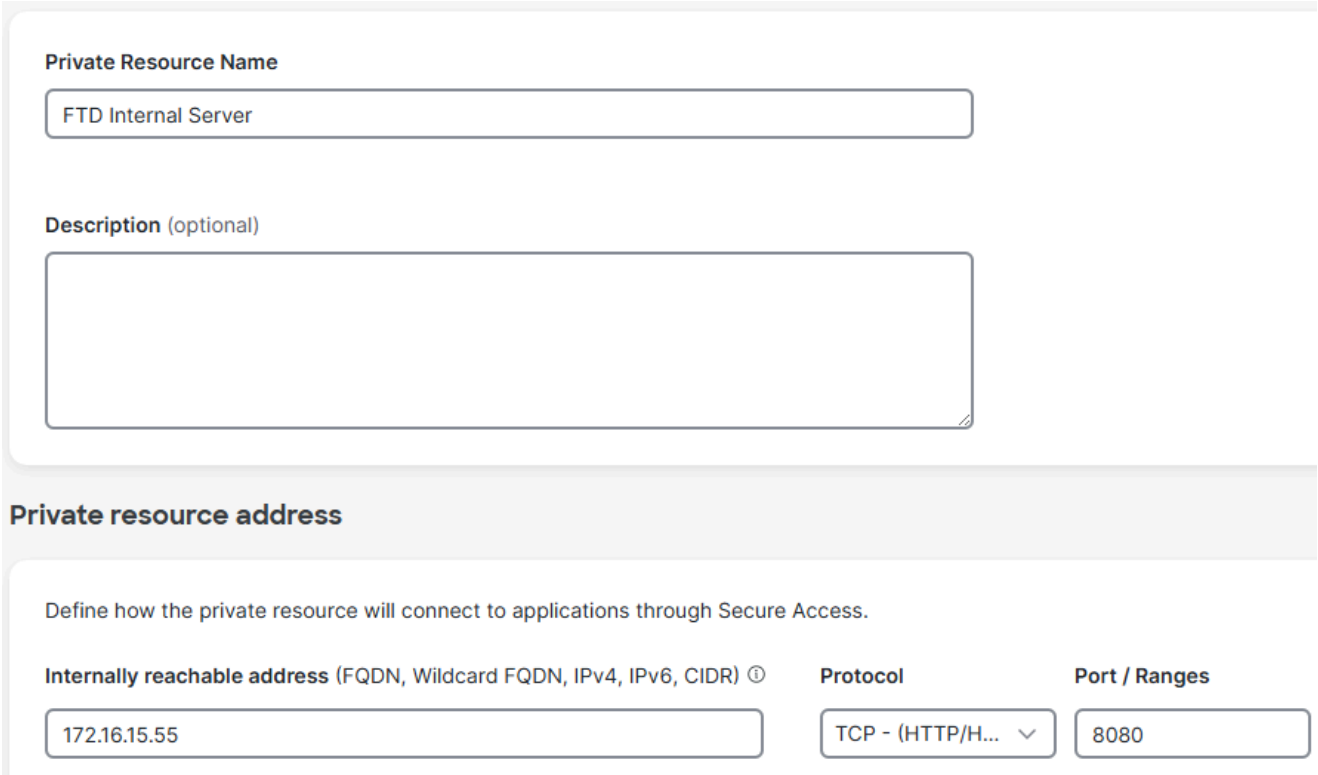
Definendole come risorse private in Secure Access, è possibile abilitare l'accesso controllato tramite soluzioni quali Zero Trust Access (ZTA) o VPN as a Service (VPNaaS). In questo modo gli utenti possono connettersi in modo sicuro ai sistemi interni in base all'identità, alla postura del dispositivo e alle policy di accesso, senza esporre le risorse direttamente a Internet.

Passare a **Resources** > **Private Resources**> fare clic suAdd.



PR

- Specificare il **Private Resource Name**, Internally reachable address, Protocol, Port/Ranges. Specificare porte e protocolli e aggiungere ulteriori risorse private in base alle esigenze
- Selezionare il tipo di connessione desiderato Connection Method in base alle proprie esigenze, ad esempio connessioni Zero Trust e/o VPN, in base alle proprie esigenze
- Fare clic su Save



Risorsa privata

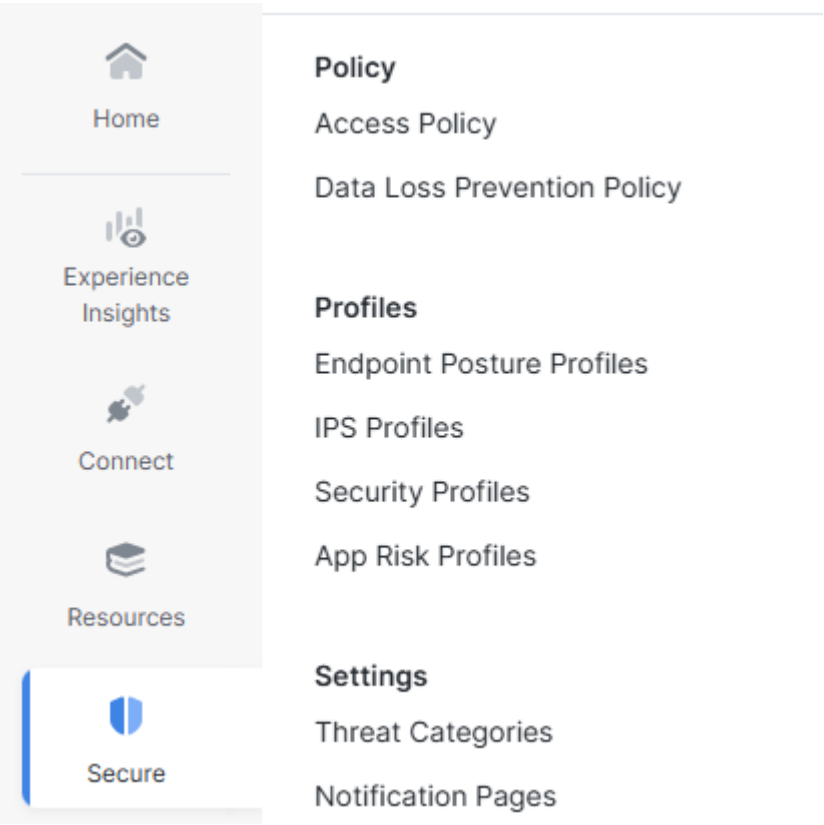
Creare una regola dei criteri di accesso

Le regole di accesso privato definiscono il modo in cui gli utenti possono connettersi in modo sicuro alle risorse e alle applicazioni interne non accessibili pubblicamente.

Queste regole applicano la sicurezza controllando gli utenti che possono accedere a risorse private specifiche in base a fattori quali l'identità degli utenti, l'appartenenza ai gruppi, la postura dei dispositivi, la posizione o altre condizioni dei criteri. Ciò garantisce che i sistemi interni sensibili rimangano protetti dall'accesso del pubblico generale, pur rimanendo al contempo disponibili in

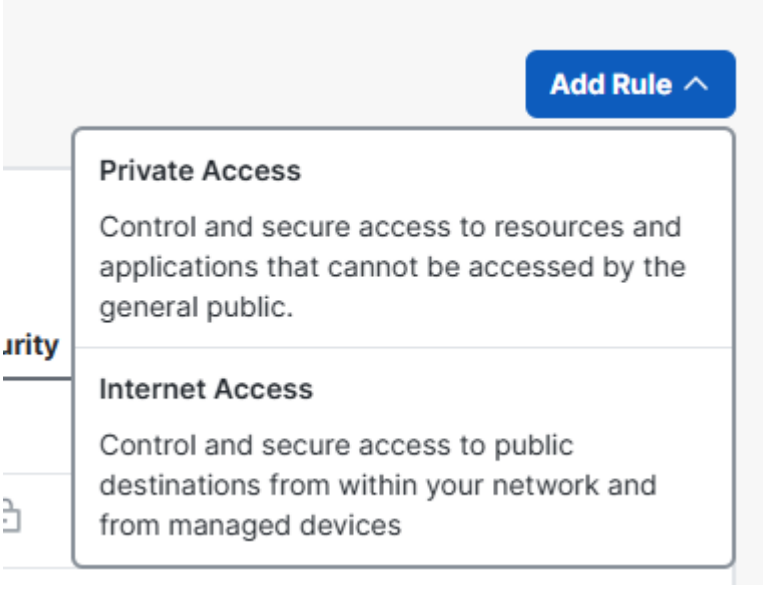
modo sicuro per gli utenti autorizzati tramite ZTA o VPNaaS.

Passa a Secure>Access Policy



ACP

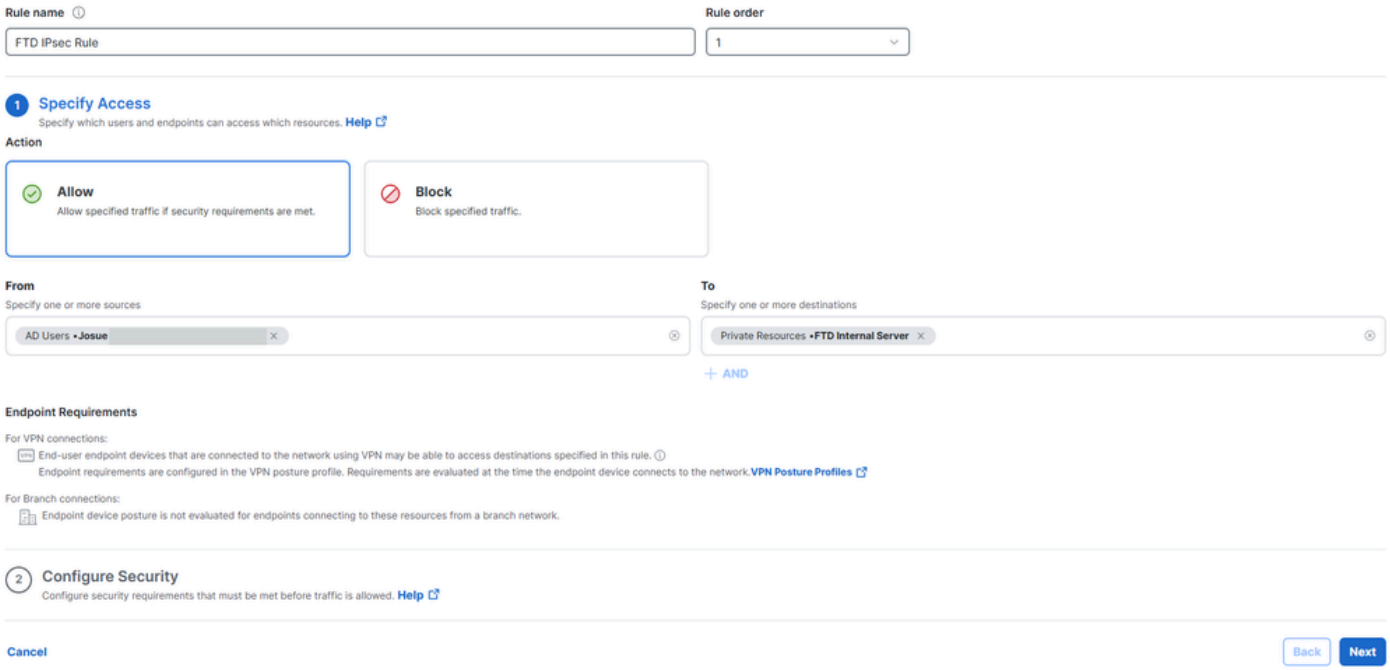
- Fare clic su Add Rule
  - Fare clic su Private Access



Aggiungi ACP

- Fai clic su Rule Name e assegna un nome

- Fare clic suAction, selezionare Allowper autorizzare il traffico
- Fare clic suFromuno e specificare gli utenti a cui vengono concesse le autorizzazioni
- Fare clic su Toe specificare l'accesso di tali utenti in base a questa regola
- Fare clic suNext, quindi Savenella pagina successiva



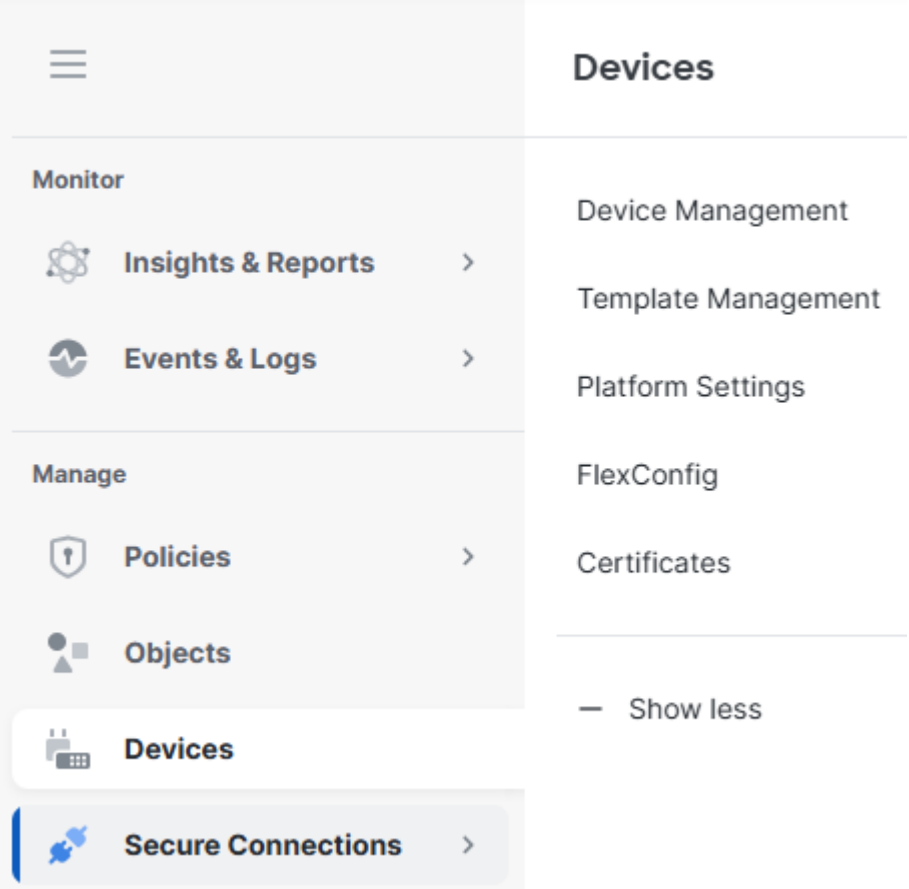
Configurazione ACP

Configurazione Secure Firewall Threat Defense (FTD)

Configurazione interfacce tunnel virtuale

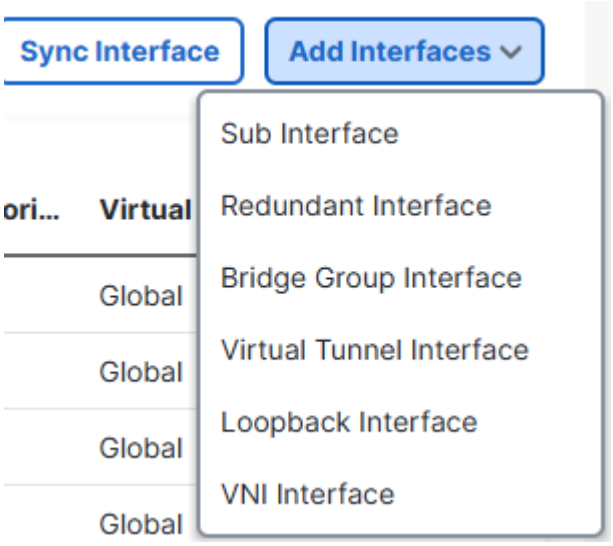
Una VTI (Virtual Tunnel Interface) su FTD è un'interfaccia logica di layer 3 utilizzata per configurare i tunnel VPN IPsec basati su route.

1. Passare a Devices> Device Management.



Dispositivi FTD

- Fare clic sul dispositivo FTD, Interfaces
  - Fare clic su Add Interfaces
  - Fare clic su Virtual Tunnel Interface
  - Creare due interfacce tunnel virtuali, una per l'hub di accesso protetto primario e l'altra per l'hub di accesso protetto secondario

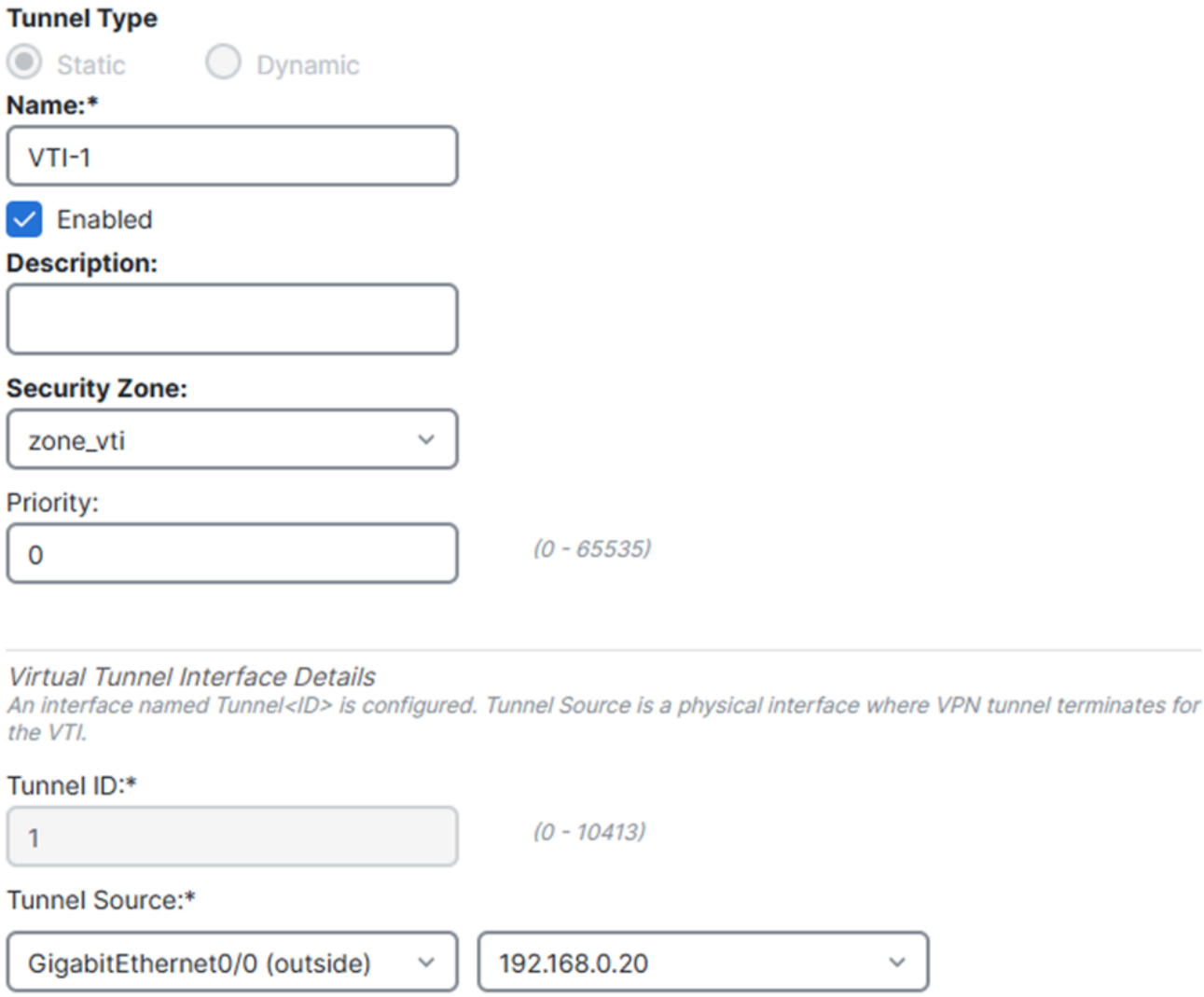


Aggiungi VTI

Virtual Tunnel Interface 1:

- Dai un nome, fai clic su Enable

- Selezionare o creare un Security Zone
- Fare clic su Tunnel ID e assegnare un valore.
- Fare clic su Tunnel Source e specificare l'interfaccia WAN da cui verrà stabilito il tunnel
- Fare clic su IPsec Tunnel Mode, selezionareIPv4
- Fare clic su IP Address e configurare l'indirizzo IP per la VTI
- Fare clic suOK

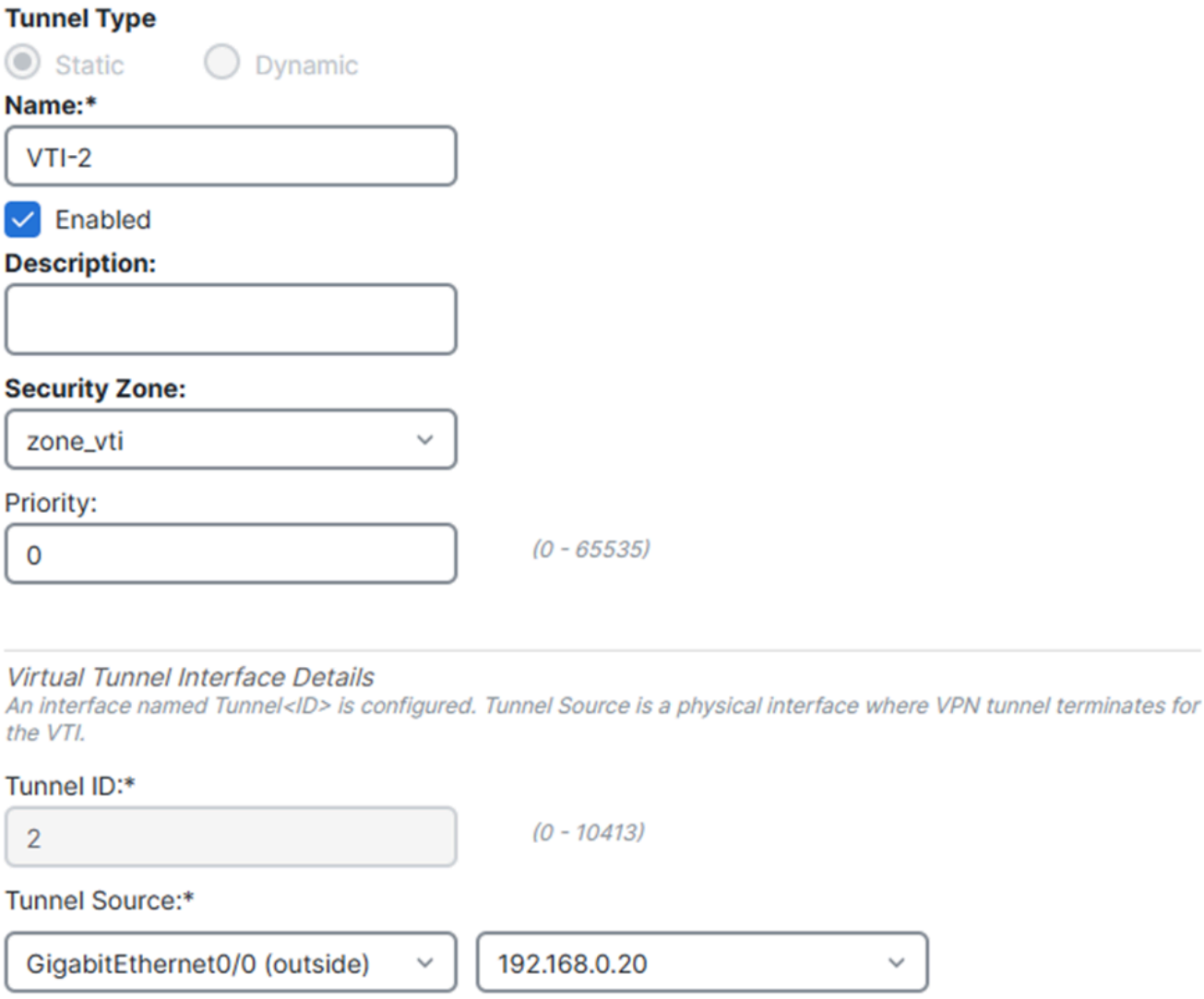


VTI 1.1

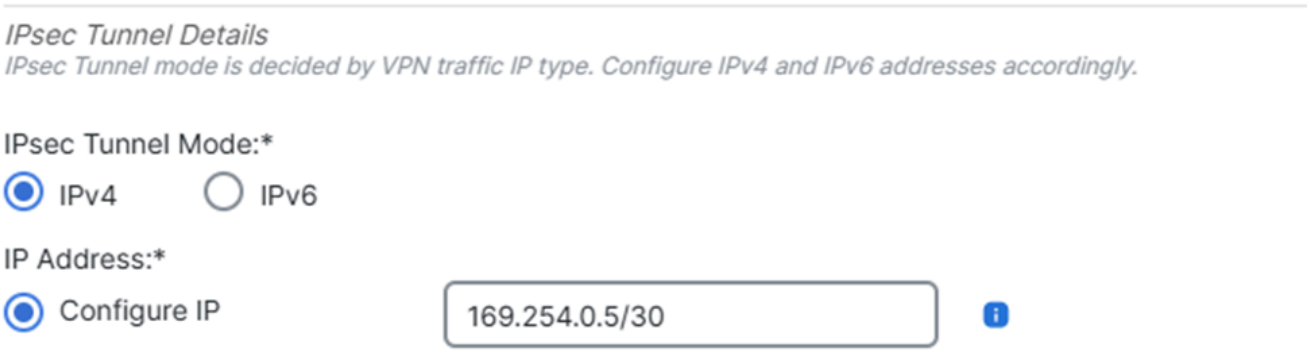
VTI 1.2

Virtual Tunnel Interface 2:

- Dai un nome, fai clic su Enable
- Selezionare o creare un Security Zone
- Fare clic su Tunnel ID e assegnare un valore
- Fare clic su Tunnel Source e specificare l'interfaccia WAN da cui verrà stabilito il tunnel
- Fare clic su IPsec Tunnel Mode, selezionareIPv4
- Fare clic su IP Address e configurare l'indirizzo IP per la VTI
- Fare clic suOK

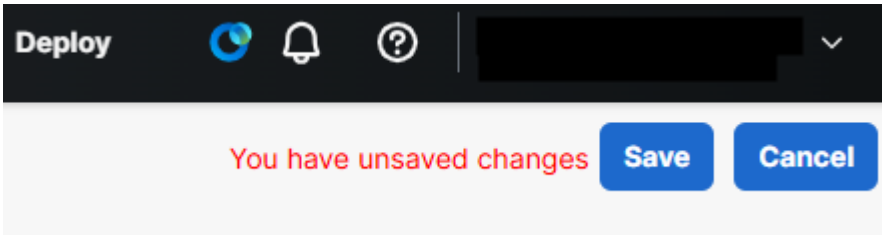


VTI 2.1



VTI 2.2

- Fare clic su Save.

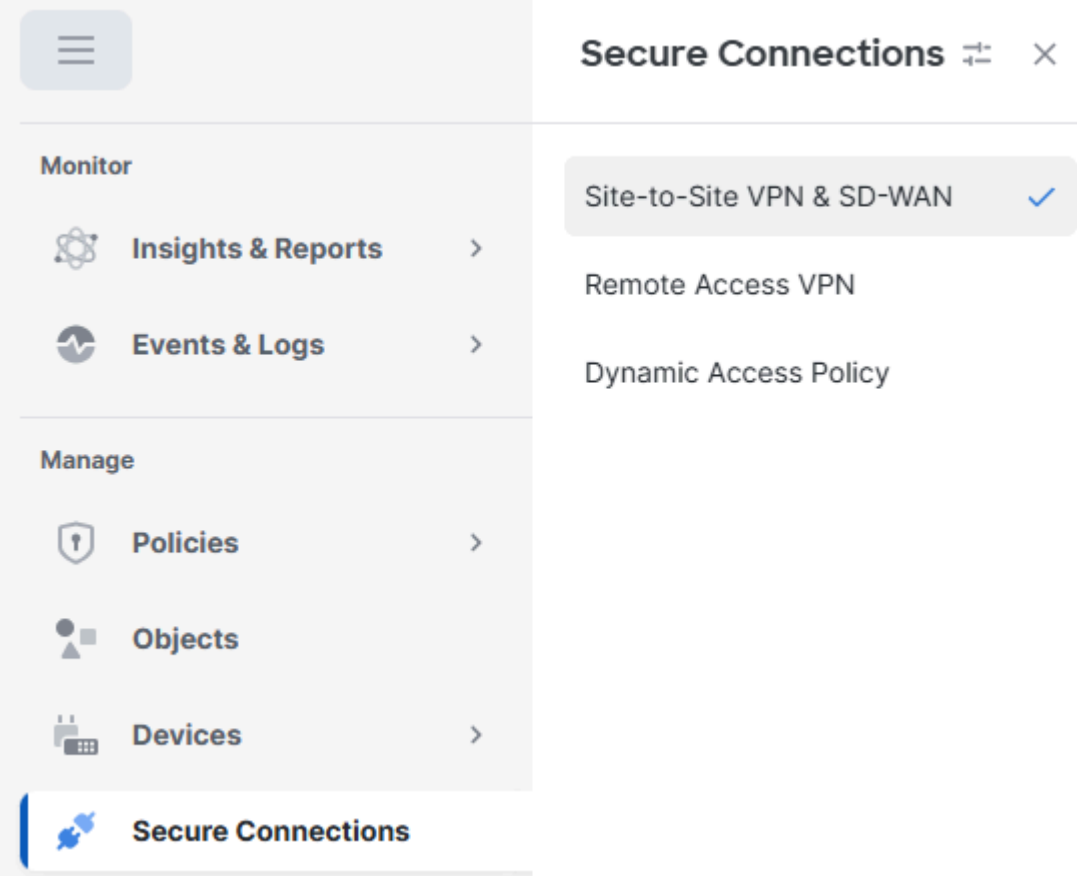


Salva modifiche VTI

Configurazione tunnel IPsec

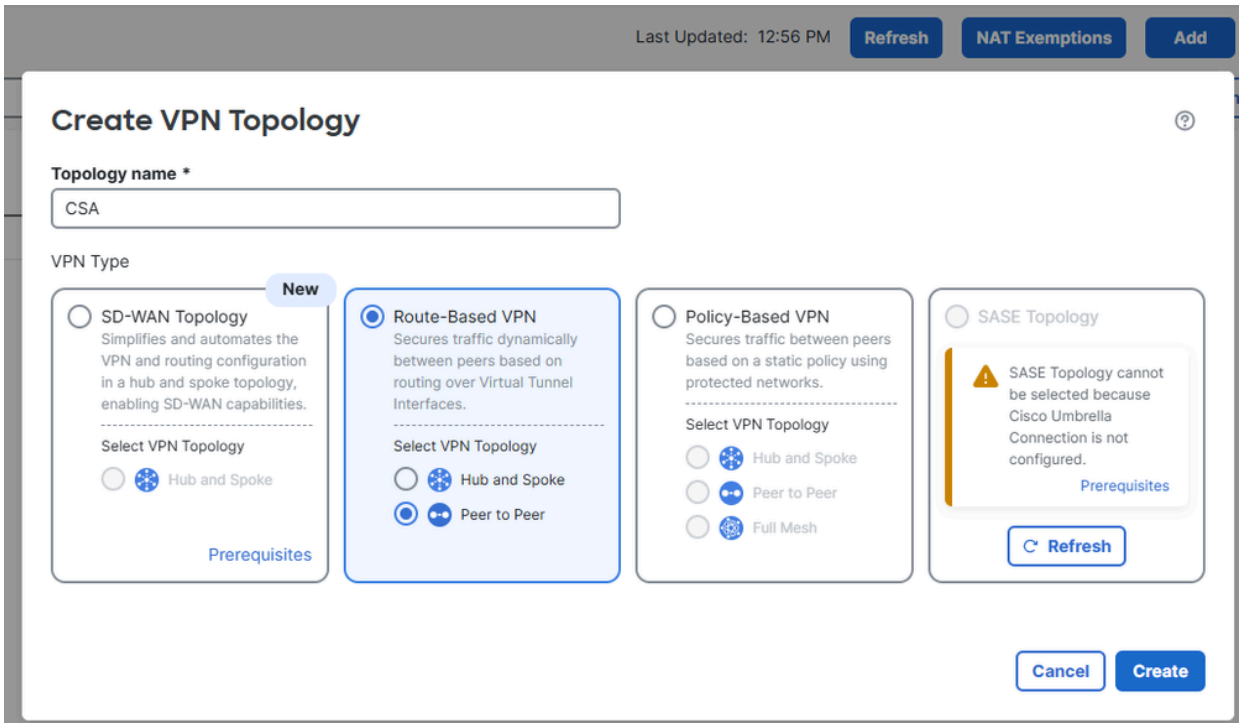
Passare al dashboard di cdFMC.

- Fai clic su Secure Connection> Site-to-Site VPN & SD-WAN



S2S

- Fare clic suAdd
  - Fare clic su Route-Based VPN
  - Fare clic su Peer to Peer

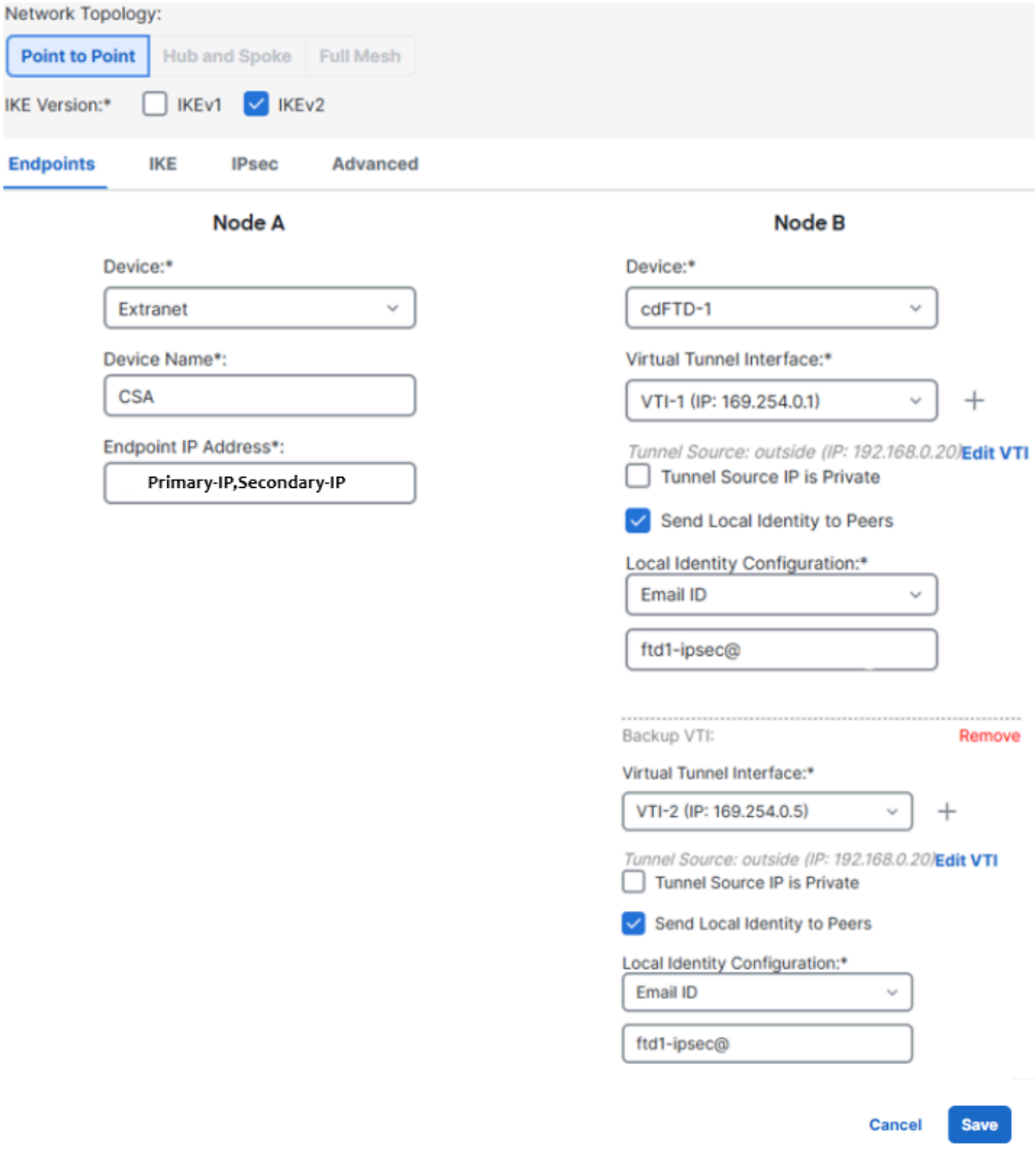


Aggiungi VPN

- Dal passaggio 5 della configurazione Secure Access, ottenere gli ID e gli indirizzi IP del

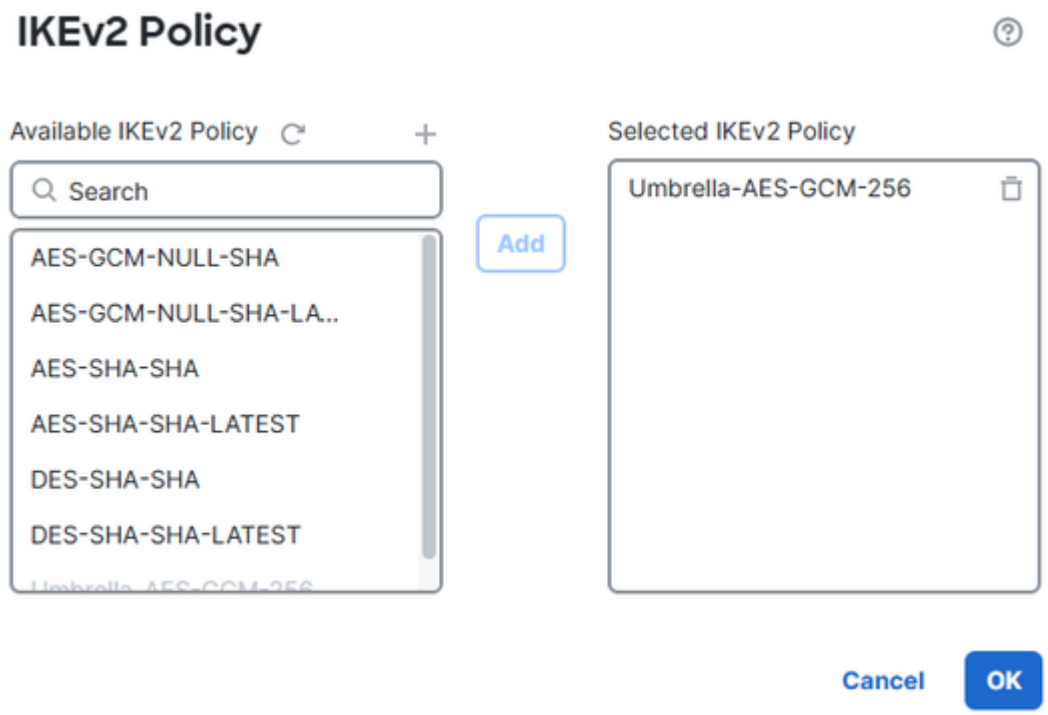
tunnel per i data center primario e secondario

- Fare clic suEndpoints
  - InNode A, fare clic suDeviceuno e selezionare Extranet
  - Fai clic Device Namee assegna un nome
  - Fare clic su Enpoint IP Addresses e immettere gli indirizzi IP primario e secondario di Secure Access separati da una virgola (da "Save Network Tunnel Group Configuration") in Secure Access
    Configurazione)
  - In Node B, fare clic suDevicee selezionare il dispositivo FTD
  - Fare clic su Virtual Tunnel Interface e selezionare la prima interfaccia VTI creata nel passaggio precedente
  - Fare clic sull'opzione Send Local Identity to Peers e selezionareEmail ID, immettere l'ID del tunnel primario (da "Save Network Tunnel Group Configuration" in Secure Access Configuration)
  - Fare clic su Add Backup VTI
  - Fare clic su Virtual Tunnel Interface e selezionare la seconda interfaccia VTI creata nel passaggio precedente
  - Fare clic suSend Local Identity to Peersun'opzione e selezionare Email ID, immettere l'ID del tunnel secondario (da "Save Network Tunnel Group Configuration" in Secure Access Configuration)
  - Fare clic su Salva



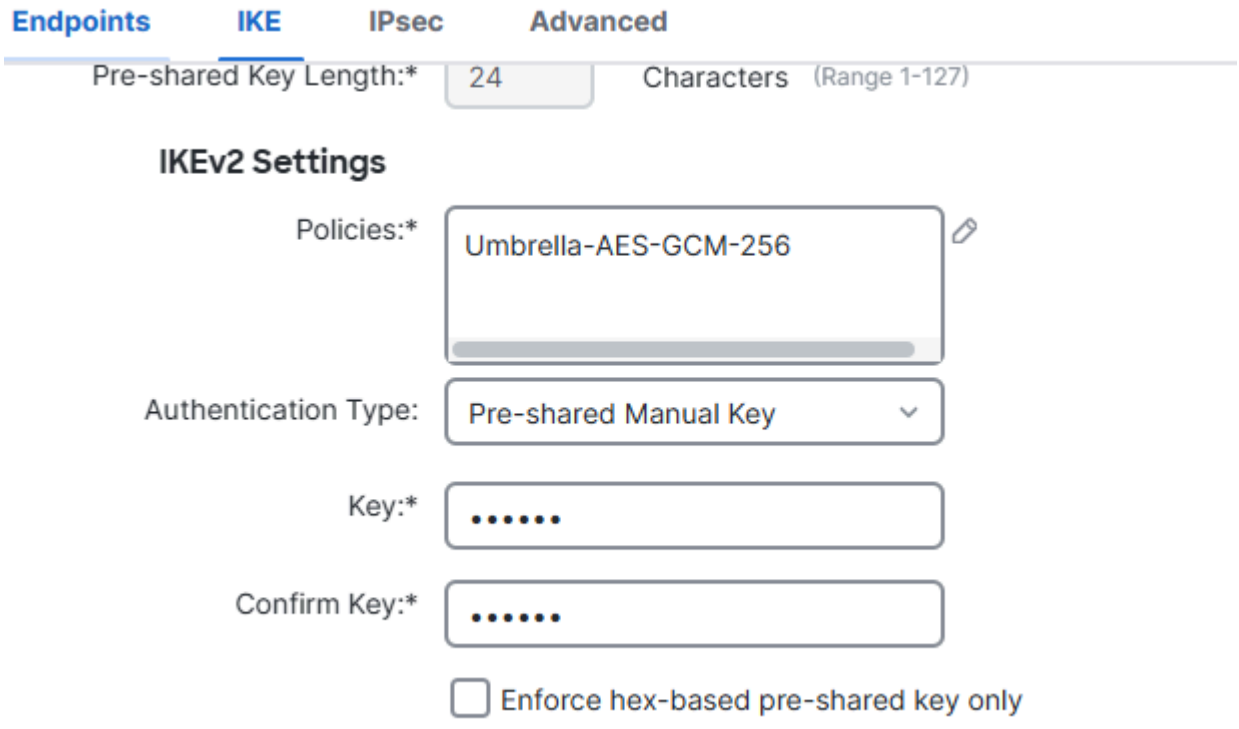
Configurazione VTI FTD

- Fare clic suIKE
  - Fare clic su **IKEv2 Settings >** Policies
  - Selezionare l'Umbrella-AES-GCM-256opzione
  - Fare clic su OK



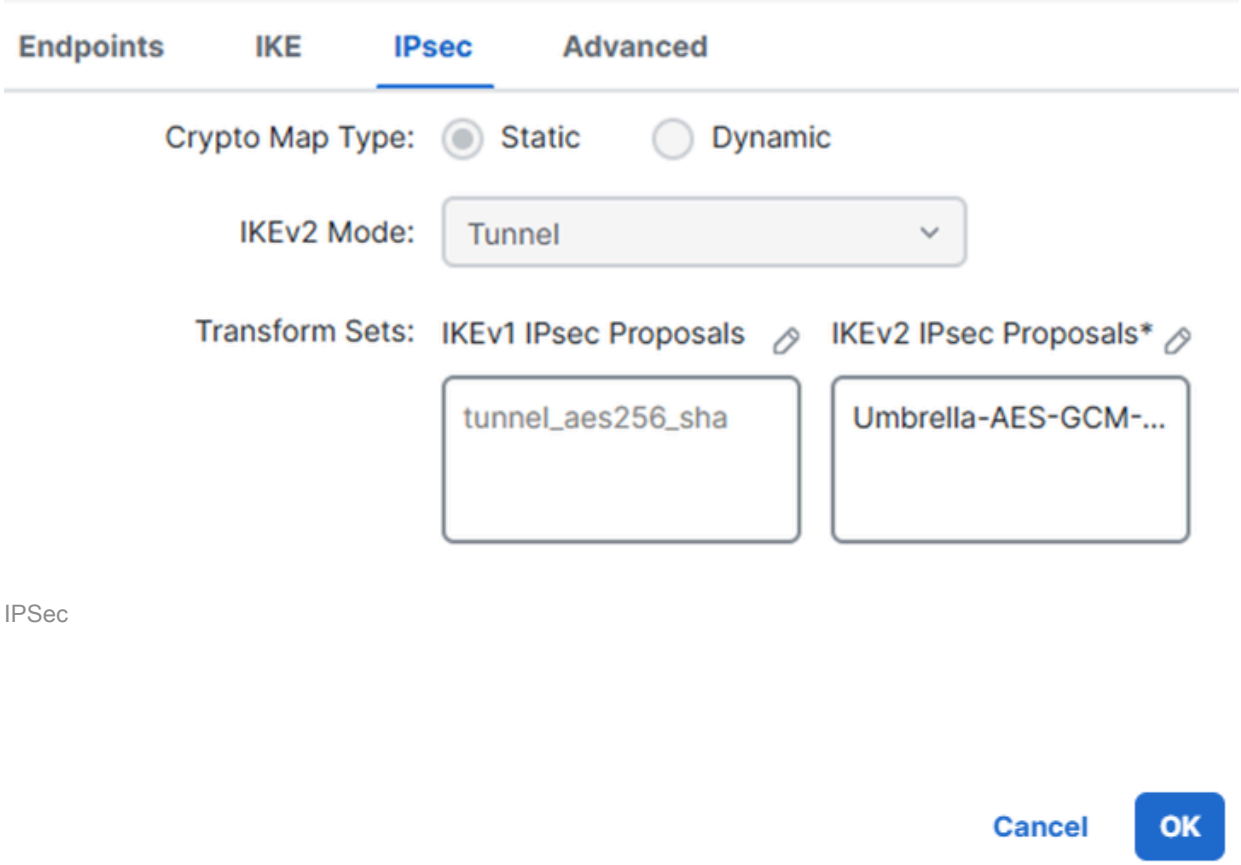
Criterio IKEv2

- Fare clic su Authentication Type e selezionarePre Shared Manual Key, immettere il PSK configurato in Secure Access (passphrase)



IKE

- Fare clic su IPSEC
  - Fare clic su IKEv2 Proposals
  - Seleziona Umbrella-AES-GCM-256
  - Fare clic su OK



IPSec

Salva proposte IKEv2

Configurazione routing FTD

Policy-Based Routing (PBR) consente di controllare l'inoltro del traffico in base a criteri diversi dall'indirizzo IP di destinazione. Anziché basarsi esclusivamente sulla tabella di routing, PBR può indirizzare il traffico in base all'origine, all'applicazione, al protocollo, alle porte o ad altri criteri definiti.

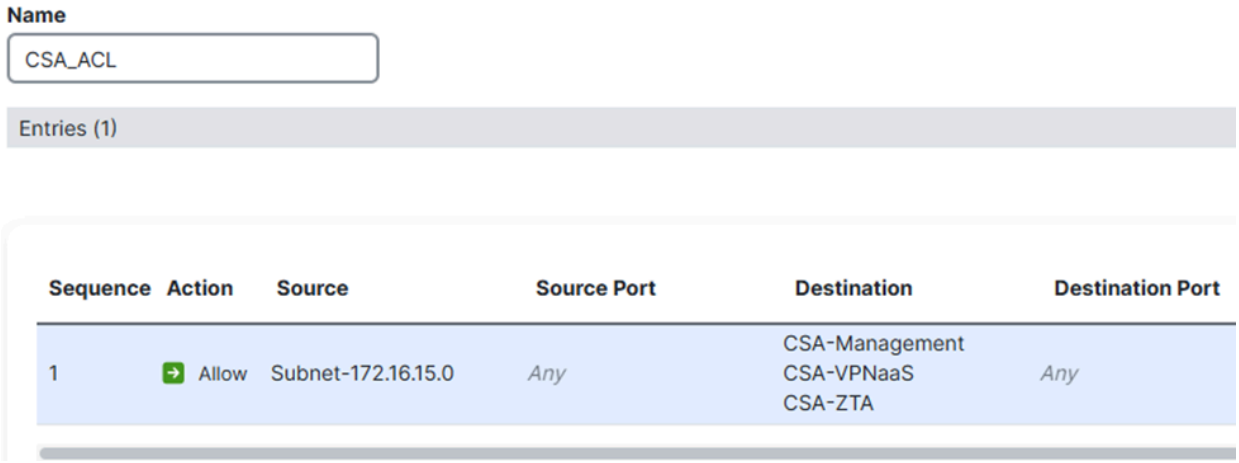
Ciò consente alle organizzazioni di indirizzare il traffico specifico o ad alta priorità sui collegamenti preferiti (ad esempio, un collegamento Internet diretto o ad ampia larghezza di banda), ottimizzare le prestazioni e suddividere in modo sicuro le applicazioni selezionate senza inviare tutto il traffico attraverso un tunnel VPN.

Policy-Based Routing

- Passa aObjects
  - Fare clic su Access List
  - Fare clic su Extended
  - Fare clic suAdd Extended Access List

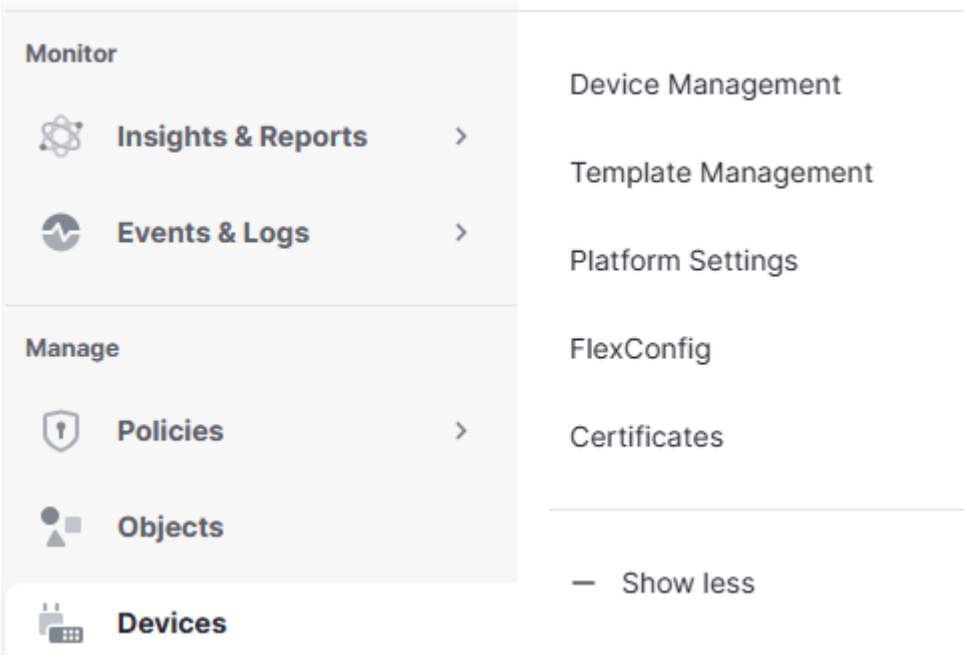
Aggiungi ACL

Creare un elenco di controllo di accesso esteso (ACL) che corrisponda alla rete di origine protetta dall'FTD (ad esempio, 172.16.15.0/24) da inviare tramite il tunnel. Per la destinazione, aggiungere le reti utilizzate da ZTA (intervallo CGNAT) e la rete utilizzata dalla VPNaaS (selezionare Pool IP rete privata virtuale).



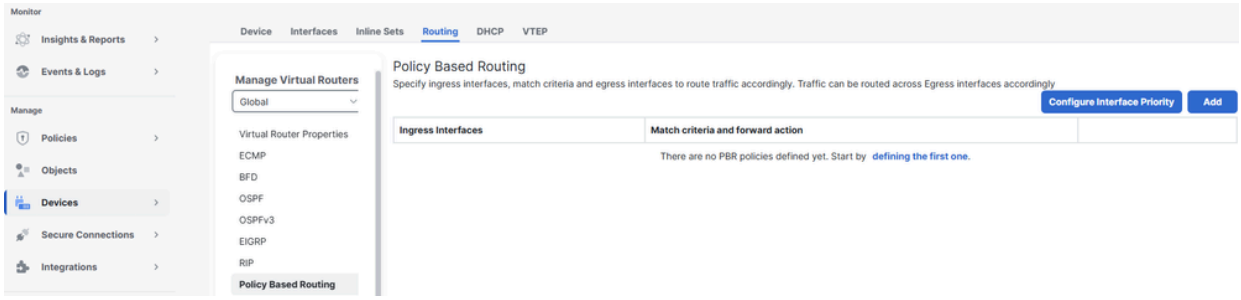
ACL

- Fai clic su Devices> Device Management



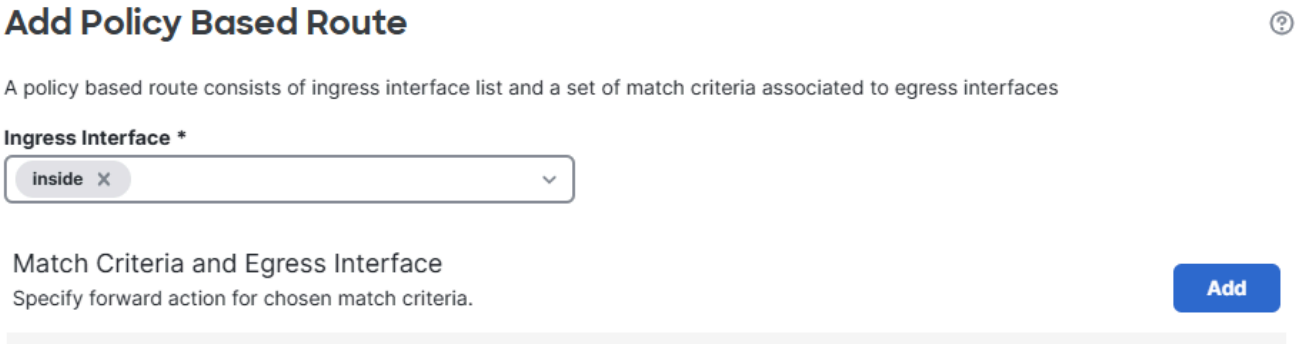
Sul dispositivo bootflash o slot0:

- Fare clic sull'FTD
  - Fare clic suRouting
  - Fare clic su Policy Based Routing
  - Fare clic su Add



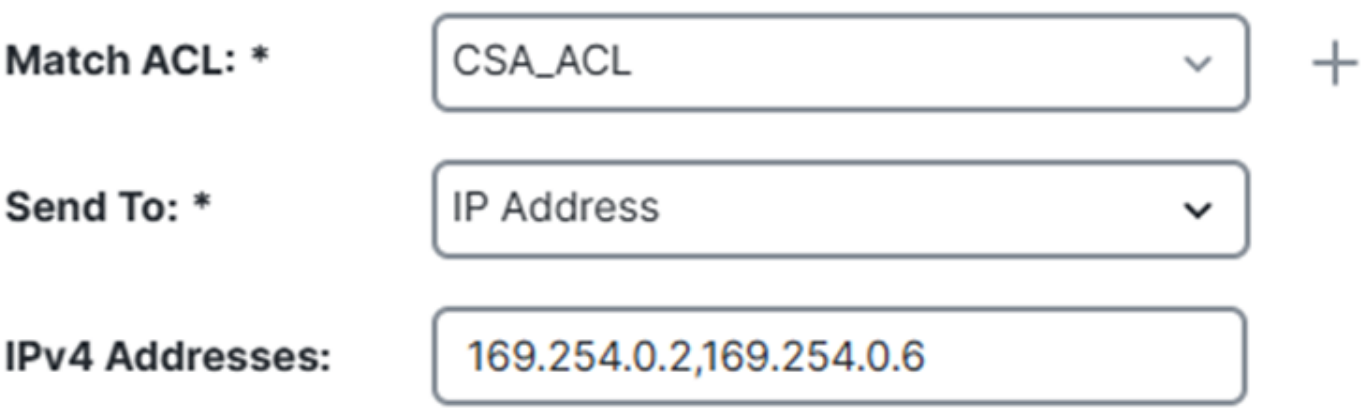
Aggiungi PBR

- Fare clic su Ingress Interface e selezionare l'interfaccia in entrata da cui entra il traffico delle reti interne
- In Criteri di corrispondenza e interfaccia in uscita fare clic su Add



Interfaccia in ingresso

- Fare clic su Match ACL e selezionare l'ACL esteso creato in precedenza
- Fare clic su Send To and select IP Address
- Fare clic su IPv4 Addresses e impostare come hop successivo gli indirizzi IP nelle subnet dell'interfaccia VTI configurate in precedenza nell'FTD (169.254.0.2 e 169.254.0.6)
- Fare clic su Save



Salva PBR

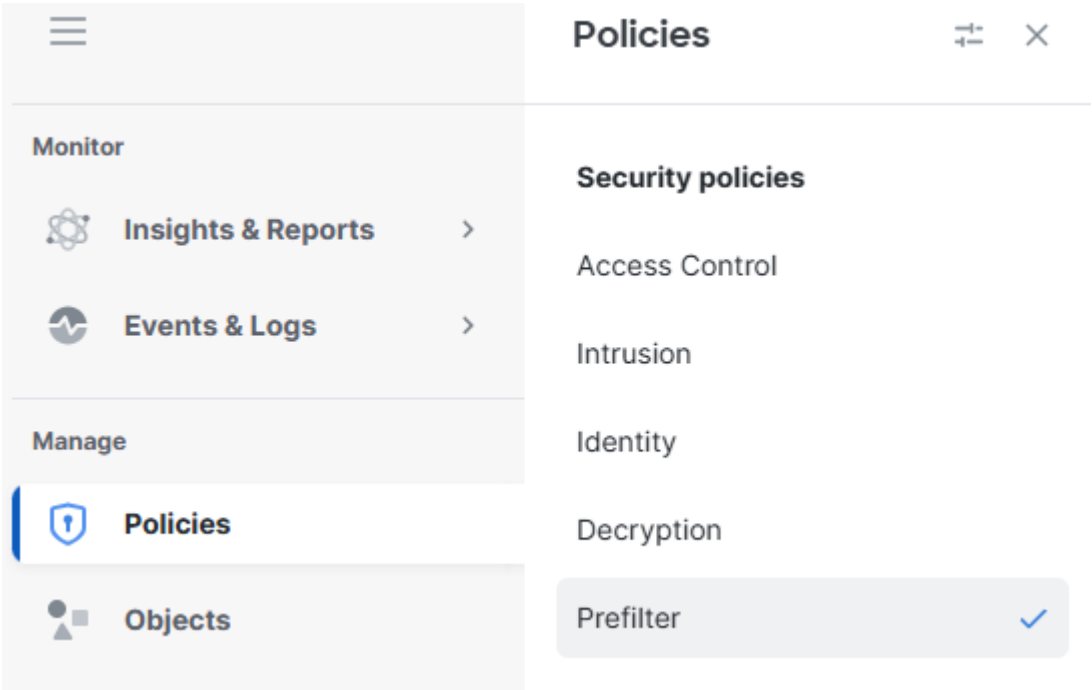
Assicuratevi di selezionare l'opzione Send To > IP Address e non l'Egress Interfaceopzione.

Configurazione criteri di accesso

Per consentire il traffico su un Cisco Firepower Threat Defense (FTD) e l'accesso a risorse private, il traffico deve prima passare attraverso la fase iniziale di controllo dell'accesso nota come prefiltro.

La prefiltrazione viene elaborata prima di un'ispezione più approfondita ed è progettata per essere semplice e veloce. Valuta il traffico utilizzando criteri di base dell'intestazione esterna (come le porte e gli indirizzi IP di origine e destinazione) per consentire, bloccare o ignorare rapidamente il traffico. Quando il traffico è autorizzato in questa fase, può ignorare ispezioni che richiedono un uso intensivo delle risorse, come ad esempio l'ispezione approfondita dei pacchetti o le policy di intrusione, migliorando le prestazioni e mantenendo il controllo della sicurezza.

- Passa a Policies> Prefilter

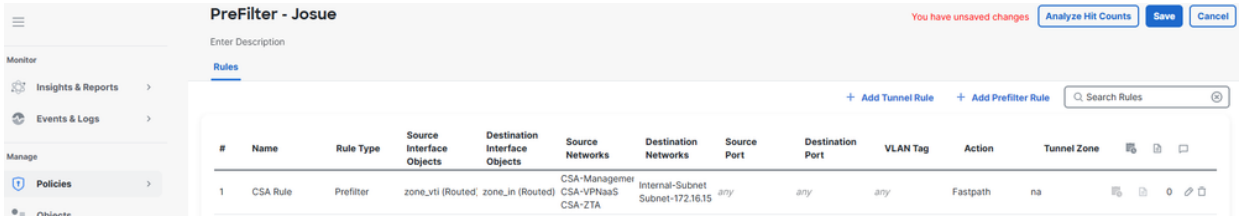


Filtro preliminare

- Fare clic per modificare il criterio di prefiltro utilizzato dal criterio di accesso

fare clic su prefiltro

- Fare clic su Add Tunnel Rule
  - Aggiungere e autorizzare il traffico dalla rete VPNaaS e/o dalla subnet ZTA alle risorse private
  - Fare clic suSave



Salva regola

A questo punto, una volta completata e verificata la configurazione sull'FTD, è possibile procedere con la distribuzione. Dopo la distribuzione, i tunnel IPSec vengono visualizzati correttamente, a conferma che è stata stabilita una connettività protetta alle risorse private.

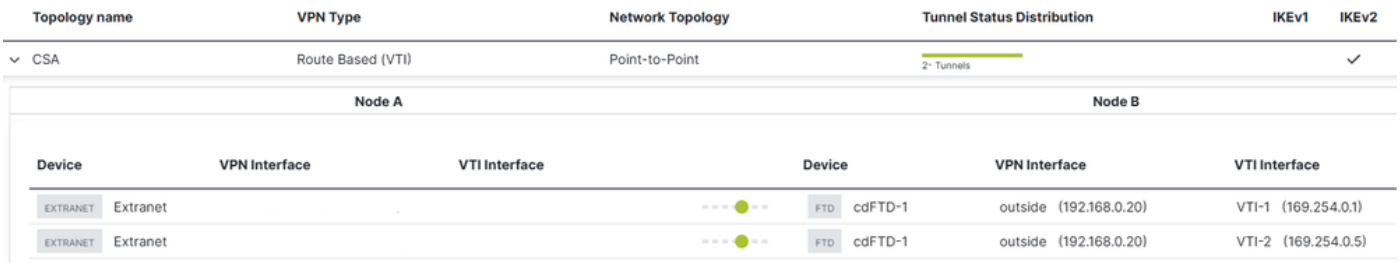
Verifica

Verifica in FTD

Stato tunnel in FTD

È possibile visualizzare lo stato corrente del tunnel, specificando anche se è attivo o inattivo. Ciò consente di verificare che il tunnel IPsec sia stato stabilito correttamente.

- Fare clic su Secure Connections.
- Fai clic su VPN da sito a sito e SD-WAN.
- Fare clic sul nome della topologia.



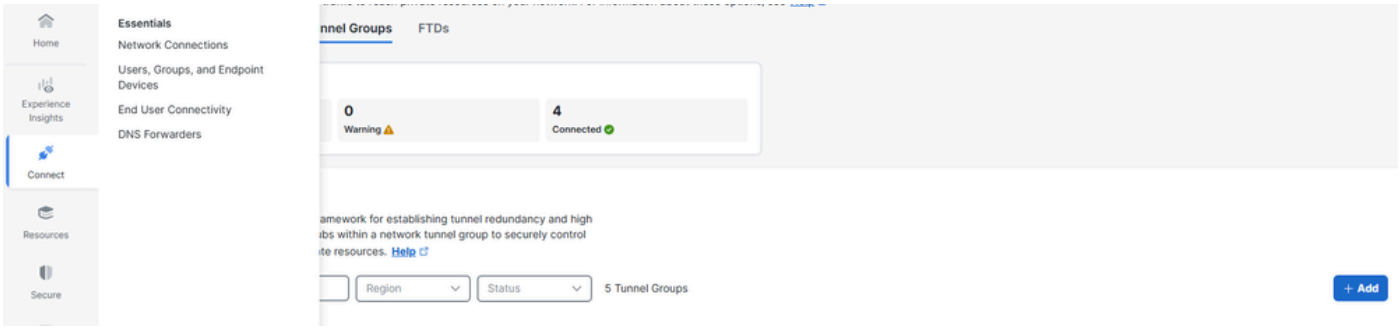
Stato tunnel FTD

Verifica in accesso sicuro

Stato tunnel in accesso sicuro

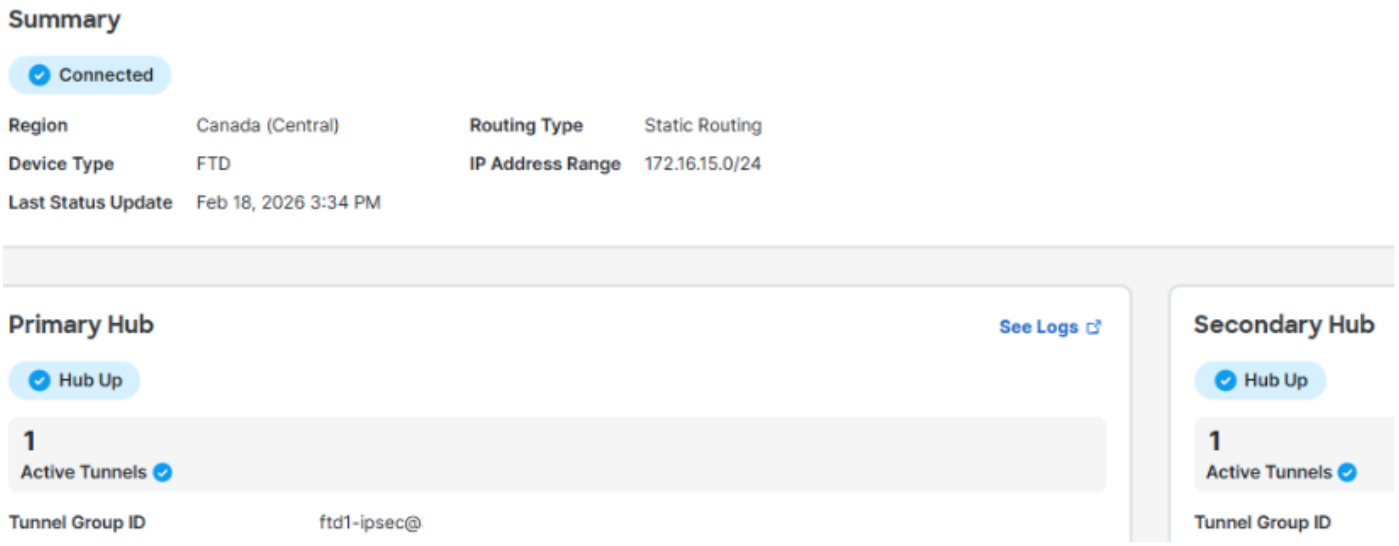
È possibile visualizzare lo stato corrente del tunnel, specificando tra l'altro se è disconnesso, in avviso o connesso. Ciò consente di verificare che il tunnel IPsec sia stato stabilito correttamente.

- Fare clic su Connect > Network Connections
- Fare clic su Network Tunnel Groups



Controlla NTG

- Fare clic su Network Tunnel Group

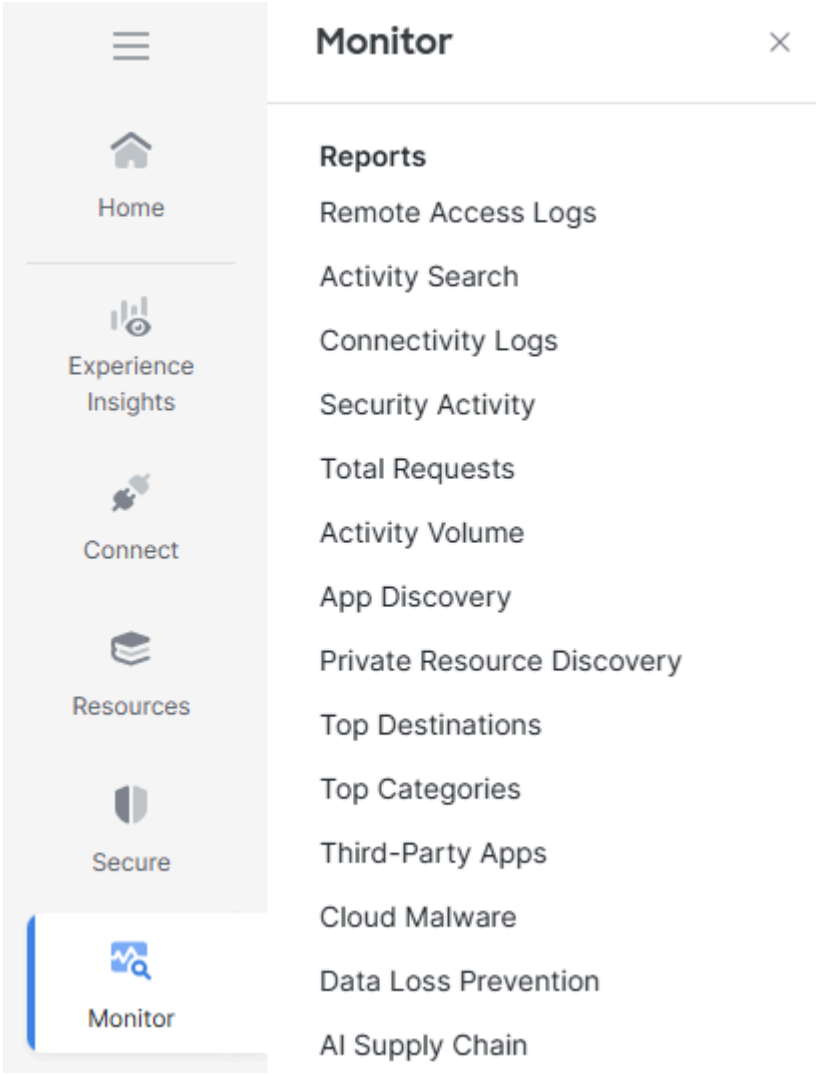


Stato tunnel CSA

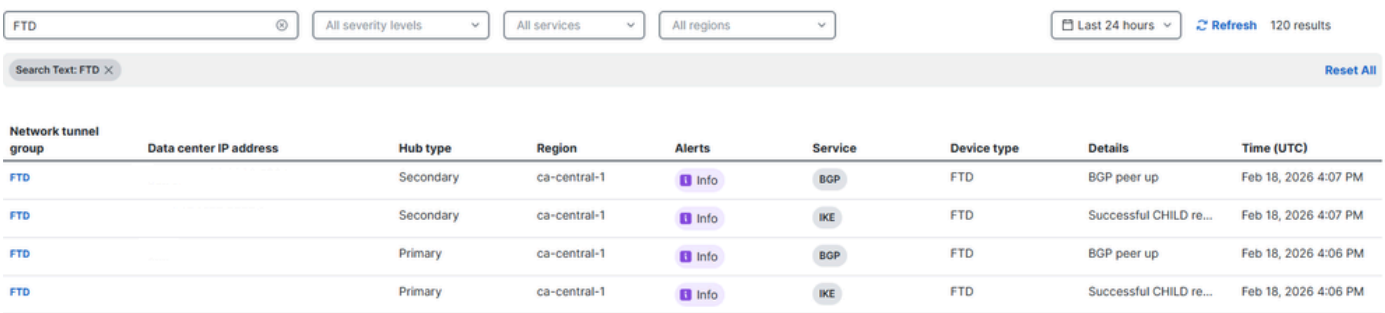
Eventi in accesso sicuro

È possibile visualizzare gli eventi del tunnel e verificare che lo stato dei tunnel IPsec sia attivo e stabile.

Fare clic su Monitor > Network Connectivity.

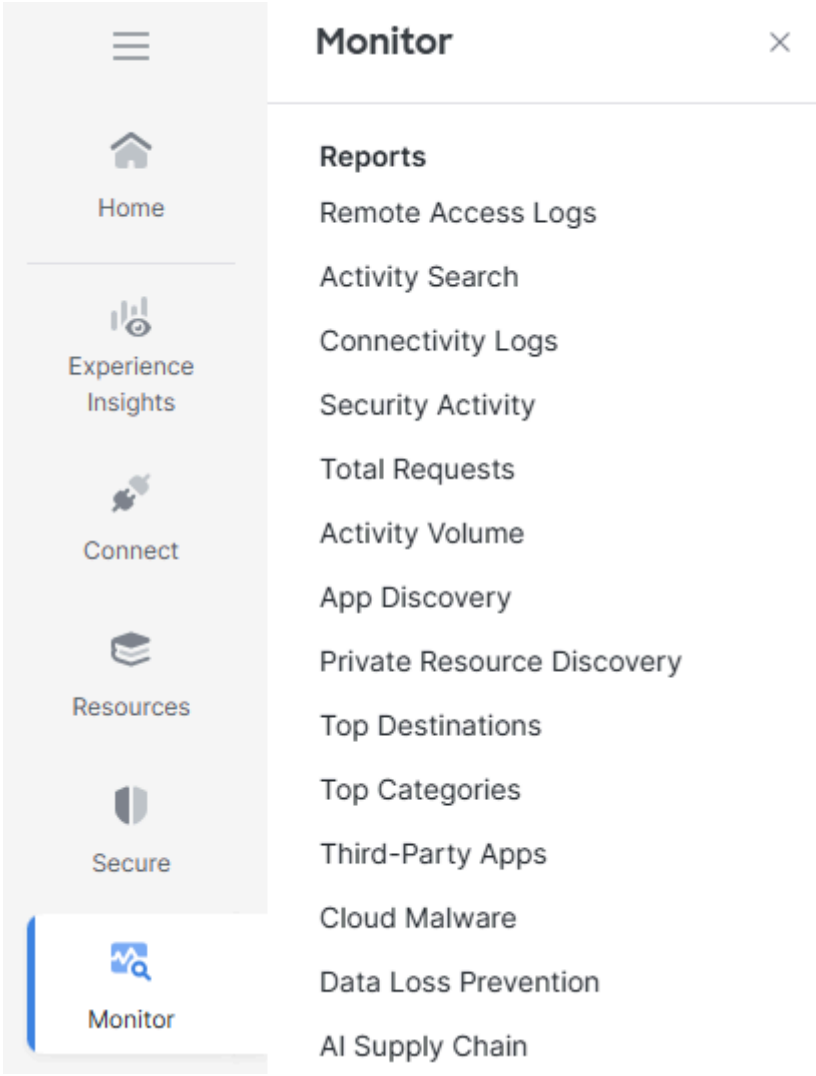


Monitoraggio registri conn



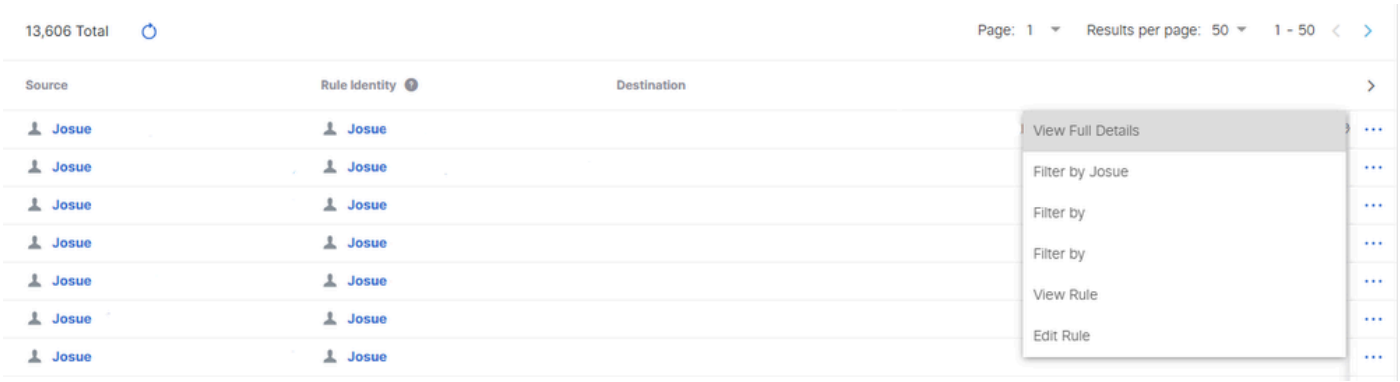
Log Conn

Passare a su Monitor > Ricerca attività.

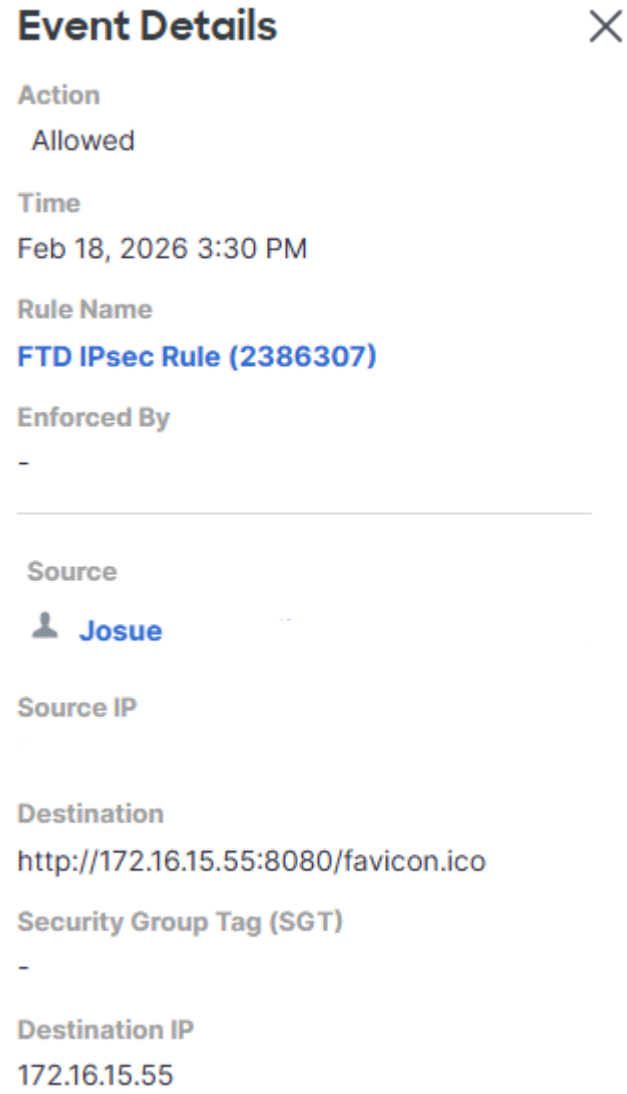


Monitoraggio registri conn

Su uno qualsiasi degli eventi correlati, fare clic su View Full Details (Visualizza dettagli completi).



Dettagli completi



Ricerca attività

Informazioni correlate

- Supporto tecnico Cisco e download
- Guida alla configurazione dei dispositivi di Cisco Secure Firewall Management Center, 7.7

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).