Configurazione di due VTI ISP su FTD Gestito da FMC

Sommario

Introduzione

In questo documento viene descritta la distribuzione di una configurazione con due ISP utilizzando le interfacce tunnel virtuali su un dispositivo FTD gestito da FMC.

Prerequisiti

Requisiti di base

- Una conoscenza di base delle VPN da sito a sito sarebbe vantaggiosa. Questo background aiuta a comprendere il processo di configurazione della VTI, inclusi i concetti e le configurazioni chiave coinvolti.
- È essenziale comprendere i fondamenti della configurazione e della gestione delle VTI sulla piattaforma Cisco Firepower. Ciò comprende la conoscenza del funzionamento delle VTI all'interno dell'FTD e del modo in cui sono controllate tramite l'interfaccia FMC.

Componenti usati

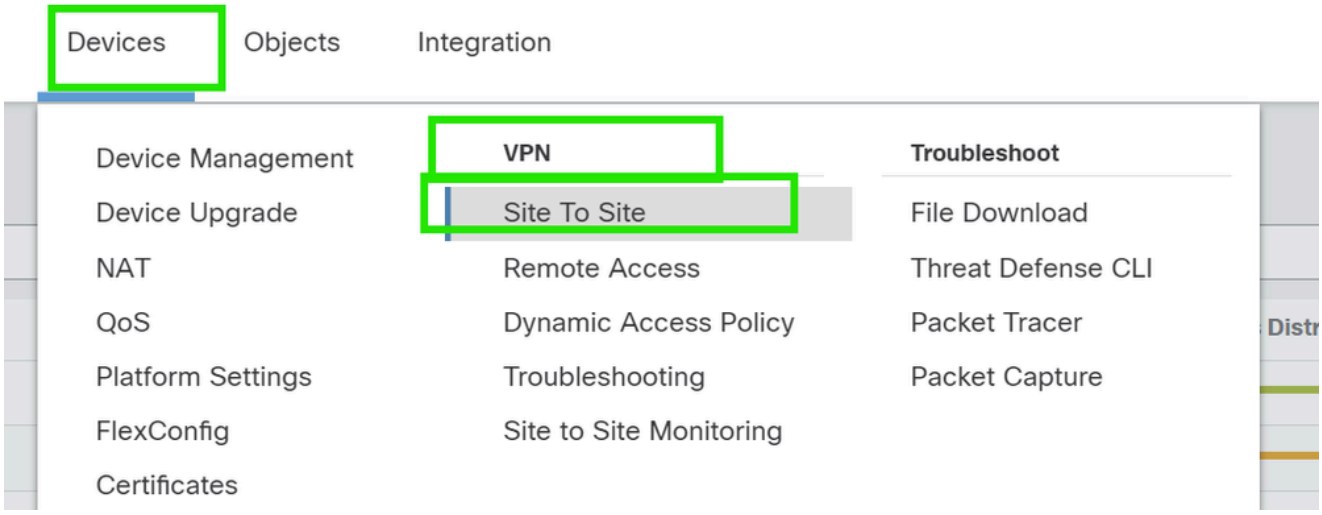
- Cisco Firepower Threat Defense (FTD) per VMware: versione 7.0.0
- Firepower Management Center (FMC): versione 7.2.4 (build 169)

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.

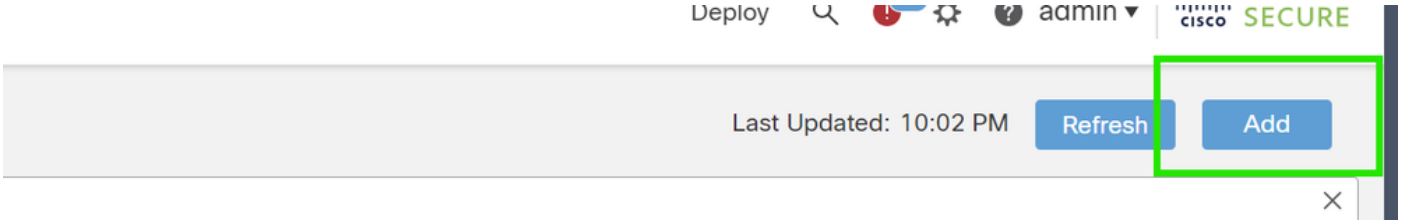
Configurazioni su FMC

Configurazione topologia

1. Passare a Dispositivi >VPN > Da sito a sito.



2. Fare clic su Aggiungi per aggiungere la topologia VPN.



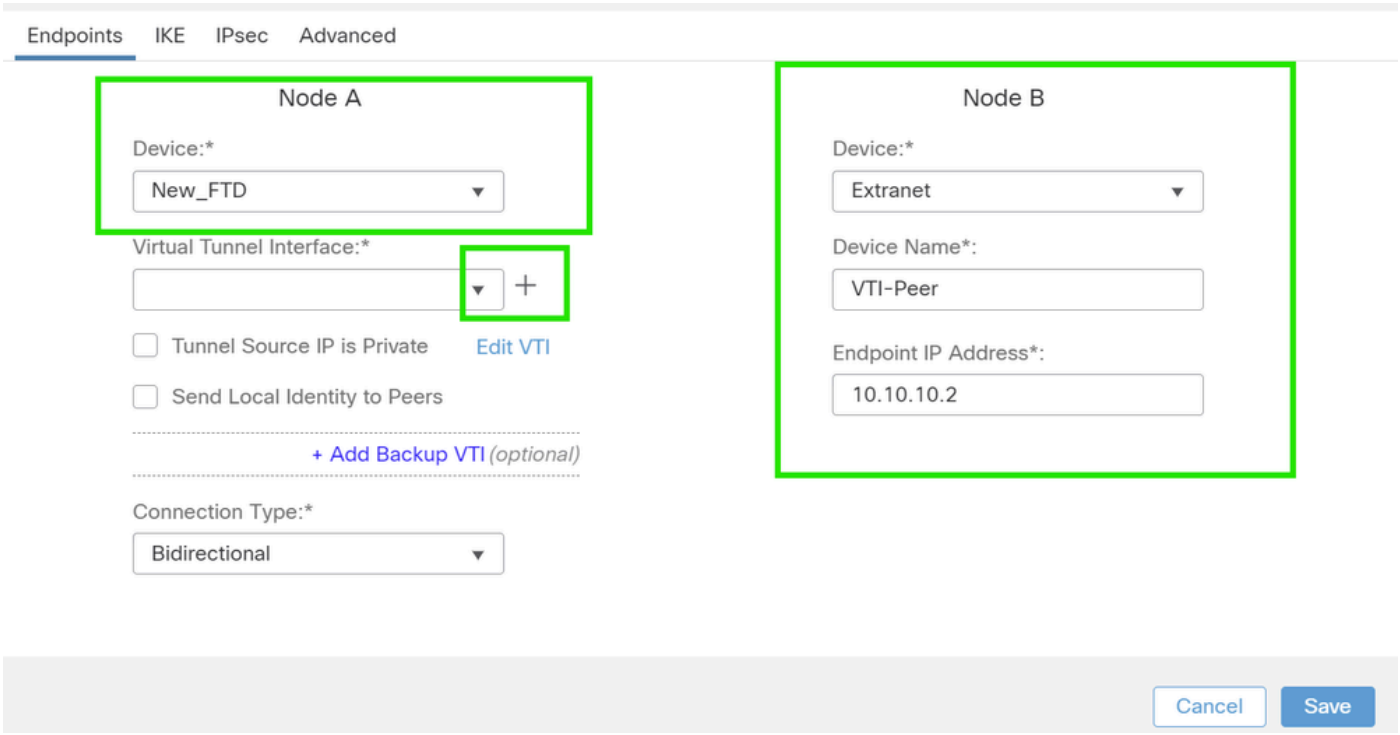
3. Assegnare un nome alla topologia, scegliere VTI e Point-to-Point, quindi selezionare una versione IKE (in questo caso IKEv2).

Configurazione degli endpoint

1. Scegliere il dispositivo su cui configurare il tunnel.

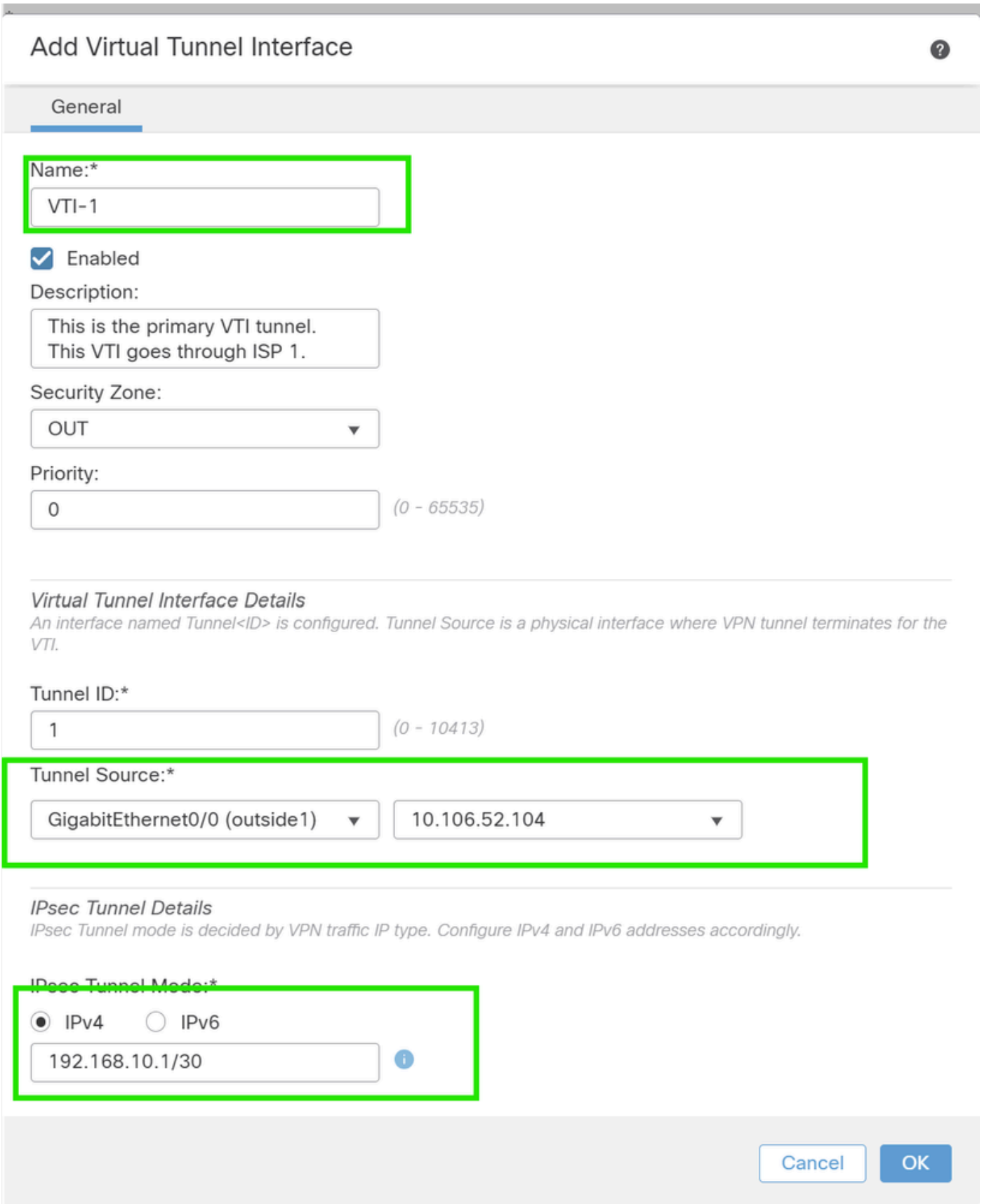
Aggiungere i dettagli del peer remoto.

È possibile aggiungere una nuova interfaccia di modello virtuale facendo clic sull'icona "+" oppure selezionarne una dall'elenco esistente.

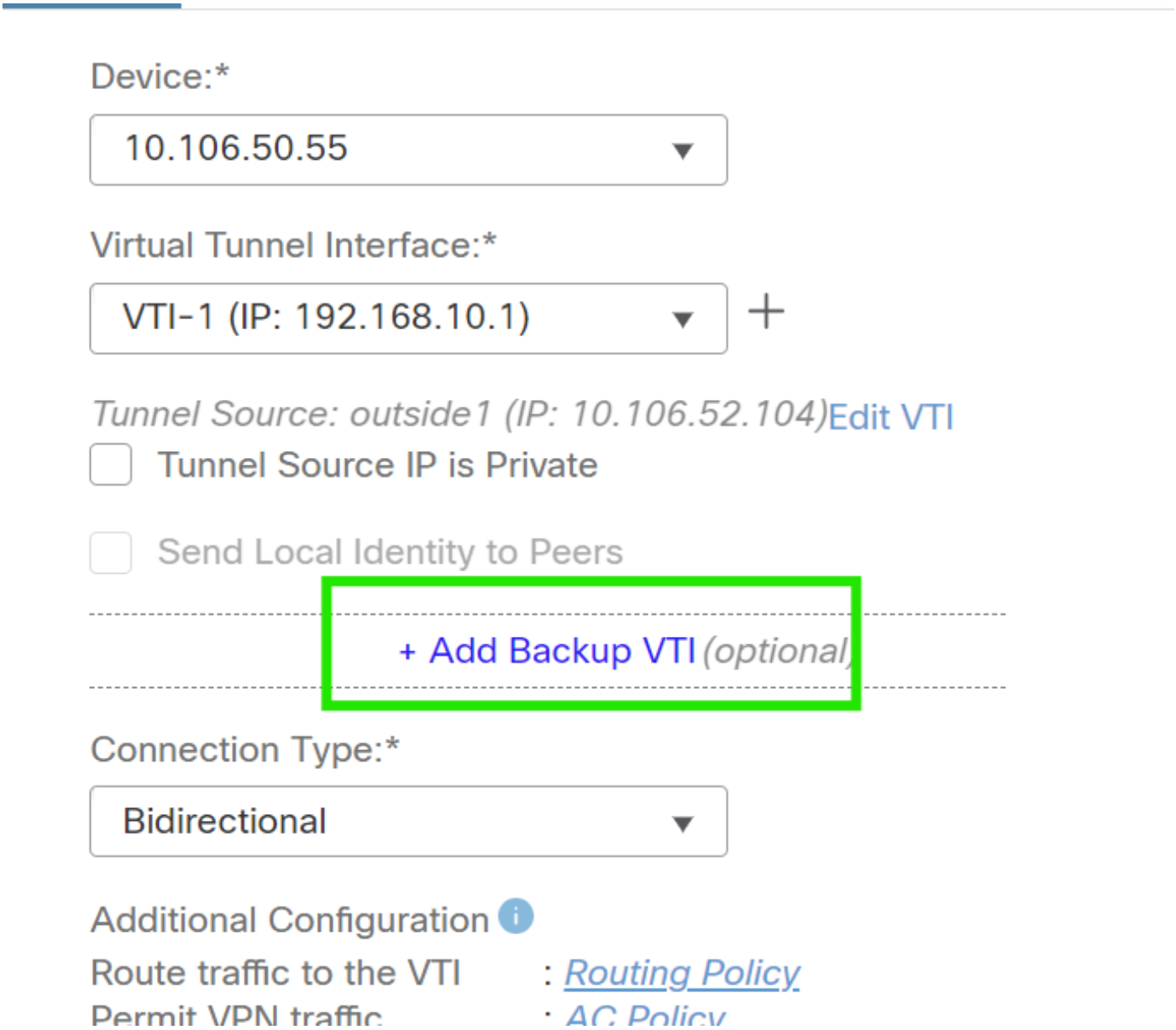


Se si sta creando una nuova interfaccia VTI, aggiungere i parametri corretti, attivarla e fare clic su "OK".

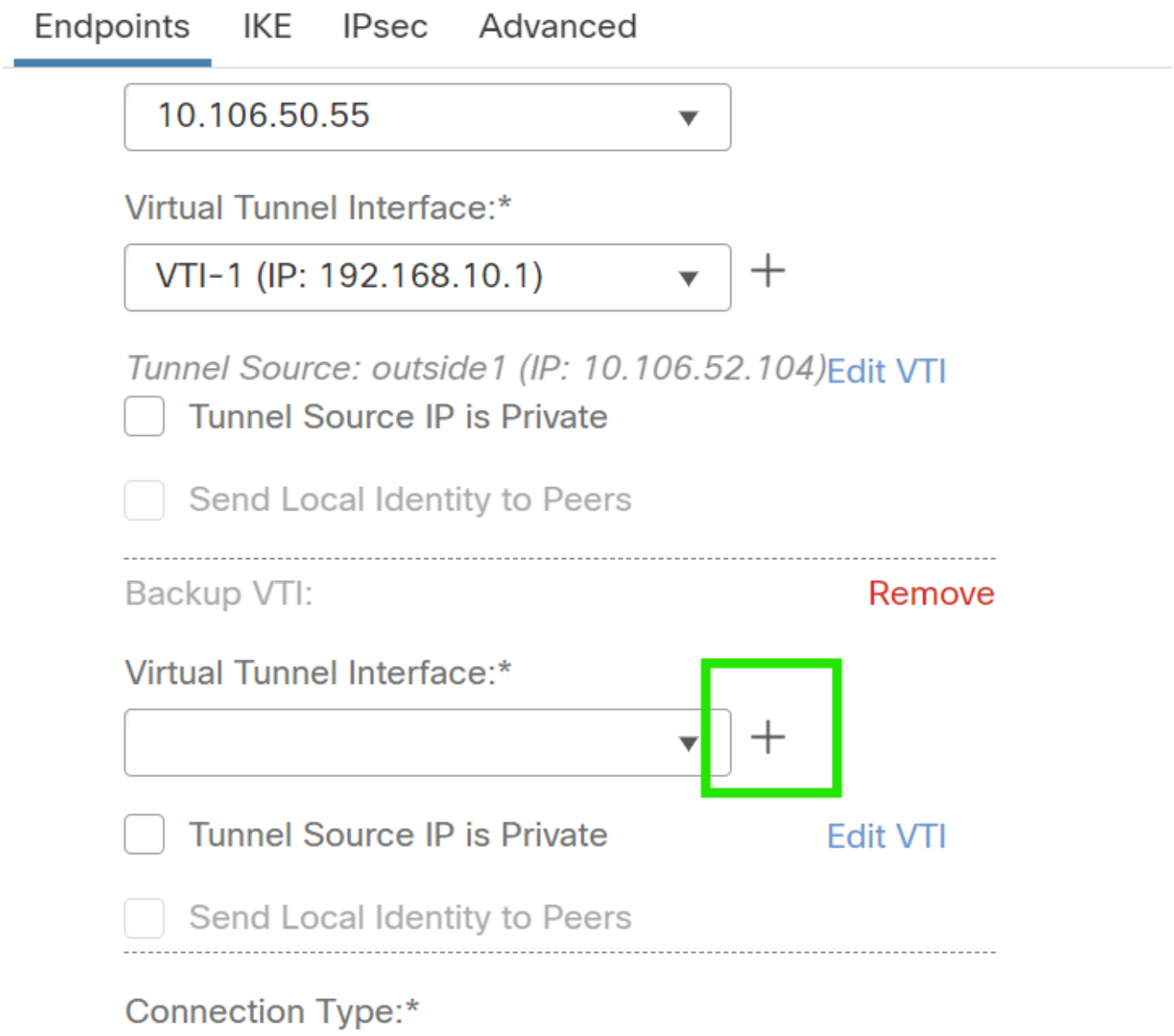
NOTA: questa diventa la VTI principale.



3. Fare clic su "+ ". Add Backup VIT" (Aggiungi VIT di backup) per aggiungere una VIT secondaria.

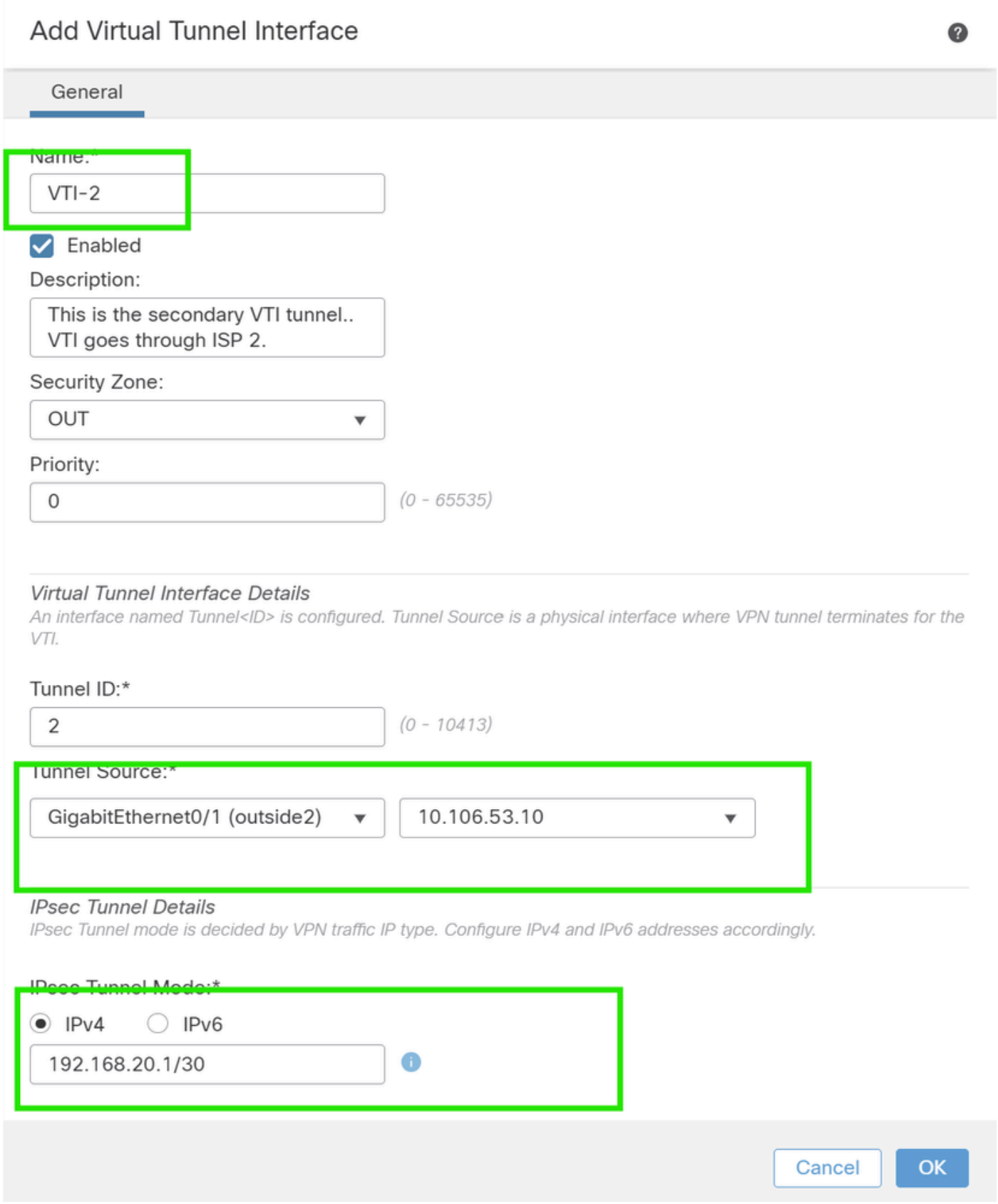


4. Fare clic su "+" per aggiungere il parametro per la VTI secondaria (se non è già stato configurato).



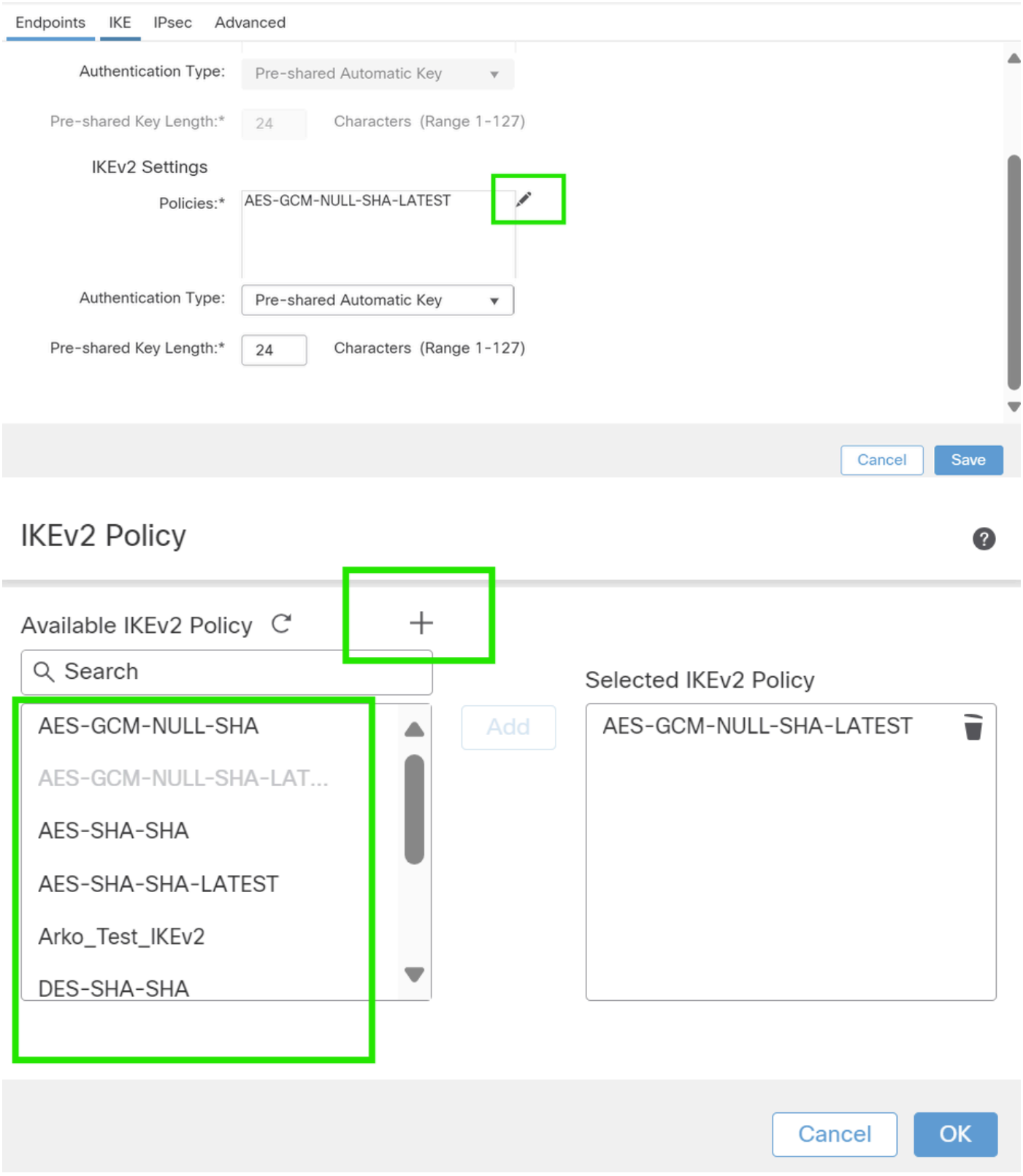
5. Se si sta creando una nuova interfaccia VTI, aggiungere i parametri corretti, abilitarla e fare clic su "OK".

NOTA: questa diventa la VTI secondaria.

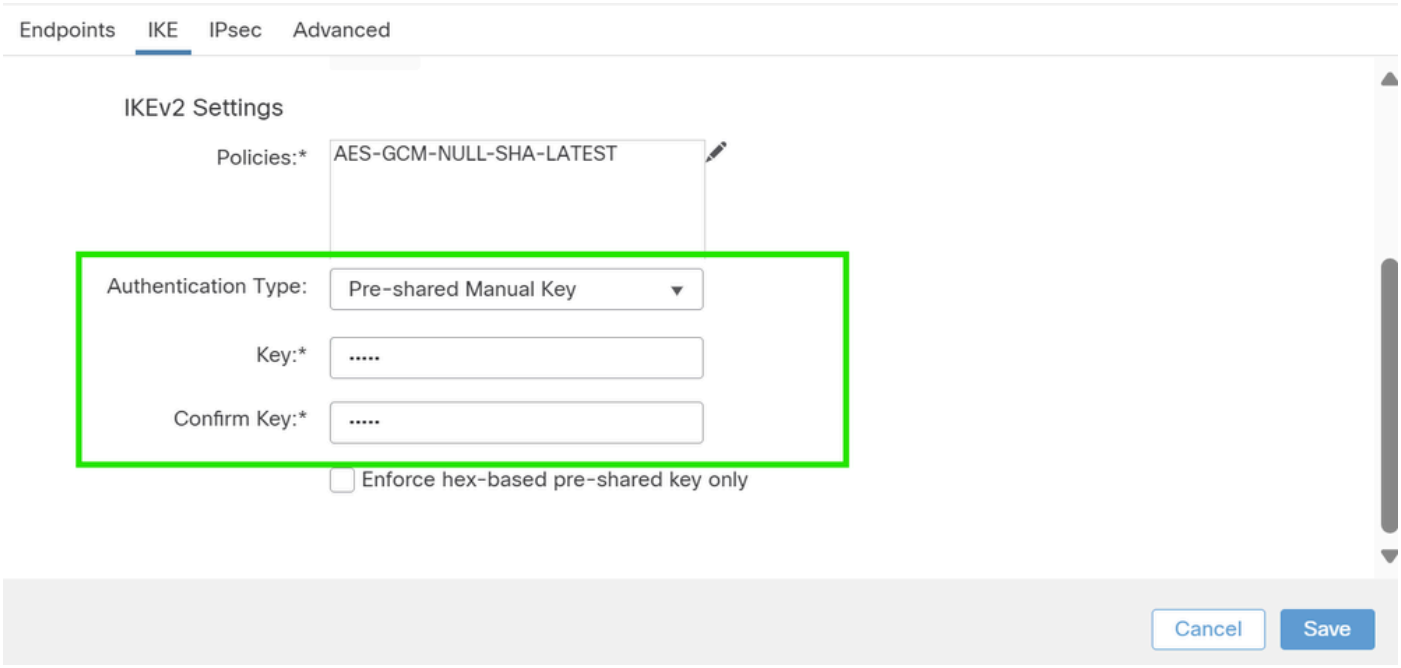


Configurazione IKE

1. Passare alla scheda IKE. È possibile scegliere di utilizzare un criterio predefinito oppure fare clic sul pulsante a forma di matita accanto alla scheda Criterio per crearne uno nuovo oppure selezionare un altro criterio disponibile in base alle proprie esigenze.

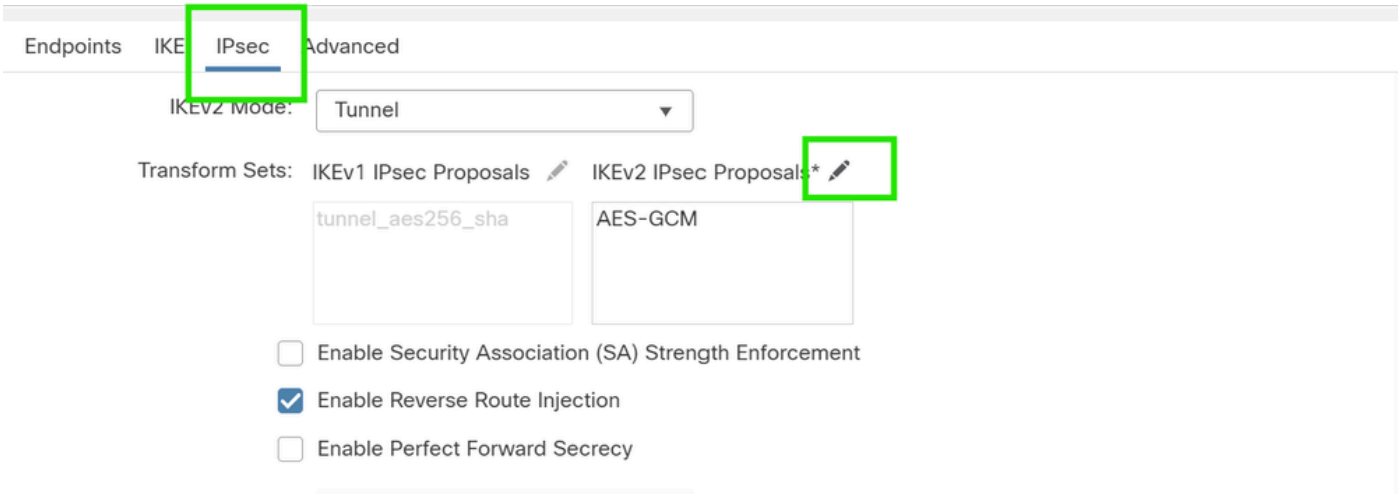


2. Selezionare il tipo di autenticazione. Se viene utilizzata una chiave manuale già condivisa, specificare la chiave nelle caselle Chiave e Conferma chiave.



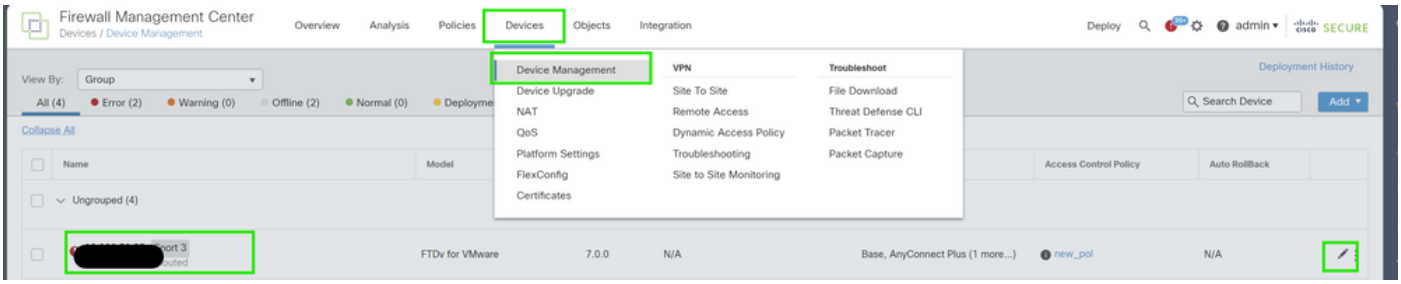
Configurazione IPSec

Passare alla scheda IPSec. È possibile scegliere di utilizzare una proposta predefinita facendo clic sul pulsante a matita accanto alla scheda proposta per crearne una nuova oppure selezionare un'altra proposta disponibile in base alle proprie esigenze.



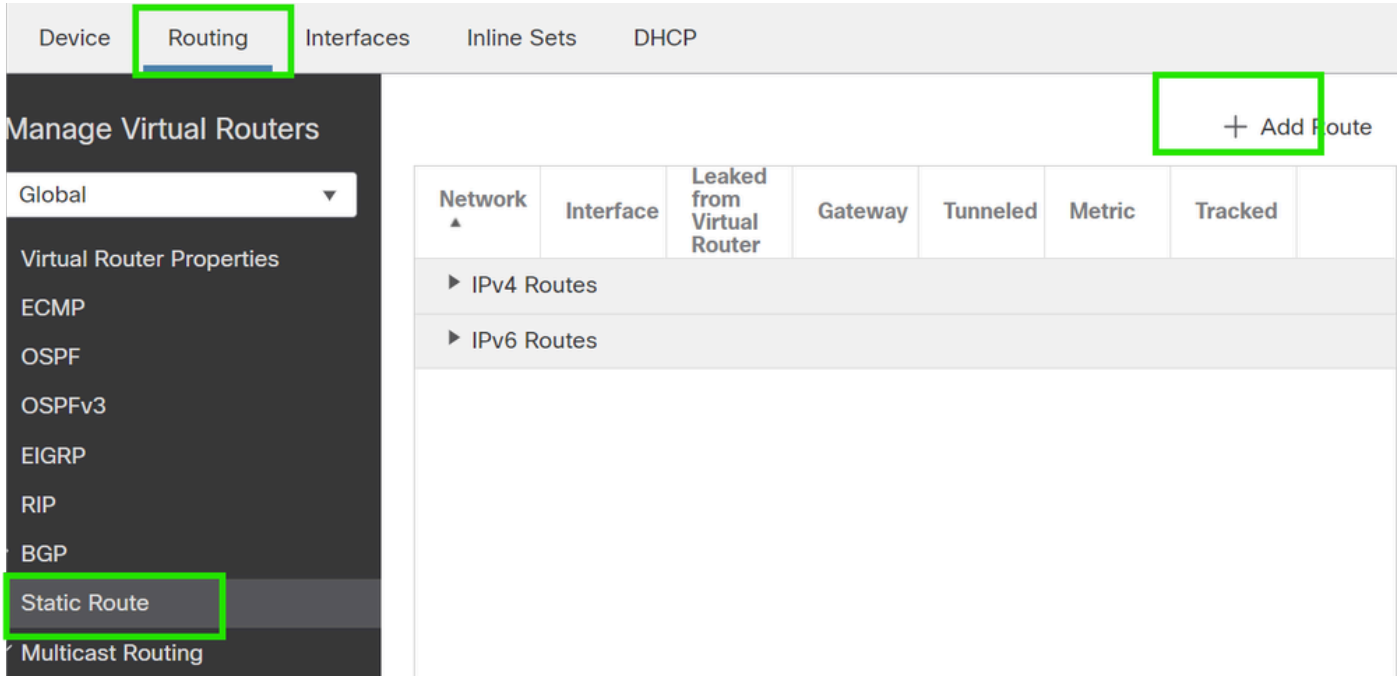
Configurazione del routing

1. Selezionare Device > Device Management e fare clic sull'icona a forma di matita per modificare il dispositivo (FTD).



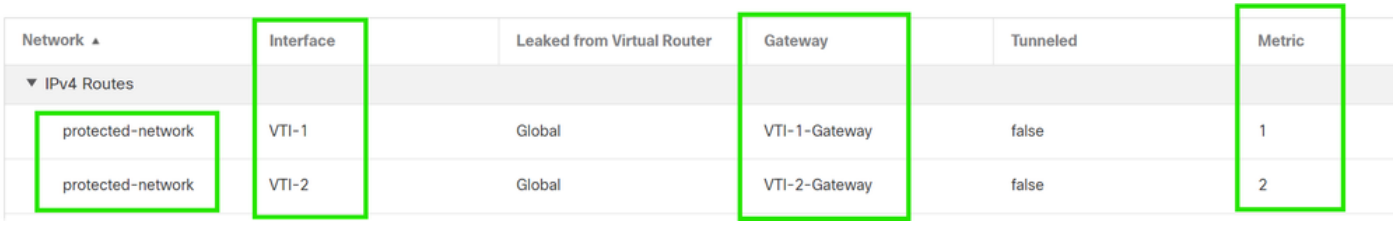
2. Andare a Instradamento > Instradamento statico e fare clic sul pulsante "+" per aggiungere un instradamento alla VTI principale e secondaria.

NOTA: è possibile configurare il metodo di routing appropriato affinché il traffico passi attraverso l'interfaccia del tunnel. In questo caso, sono state utilizzate route statiche.



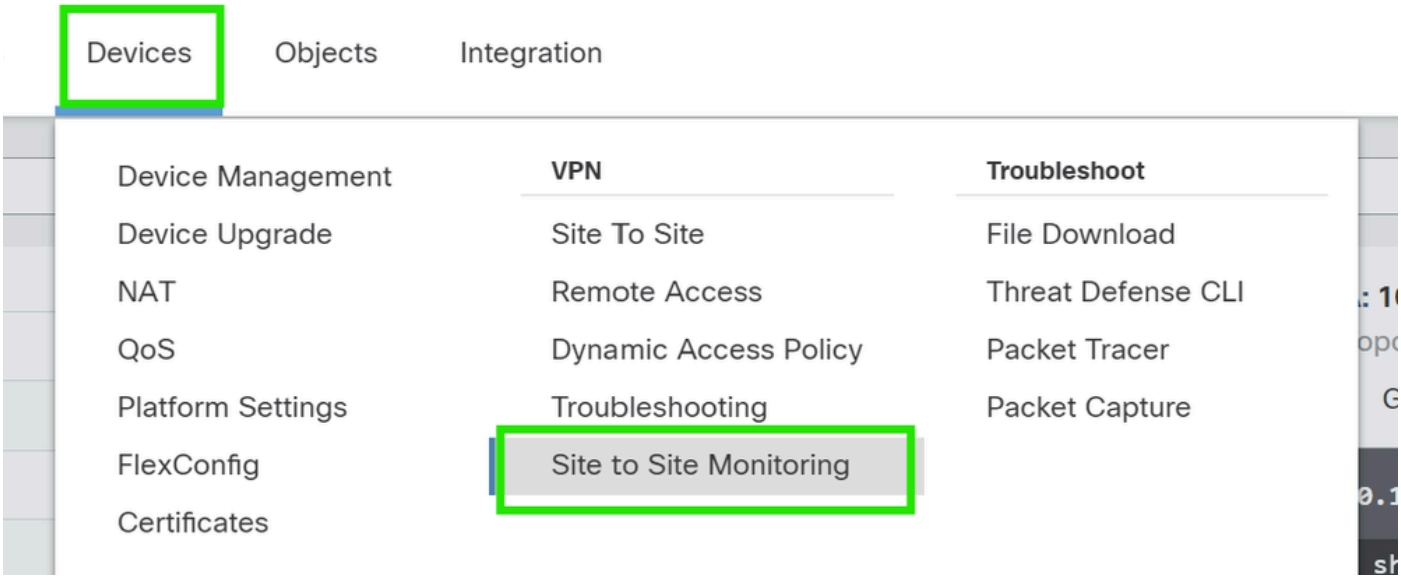
3. Aggiungere due route per la rete protetta e impostare un valore AD superiore (in questo caso 2) per la route secondaria.

La prima route utilizza l'interfaccia VTI-1, la seconda l'interfaccia VTI-2.

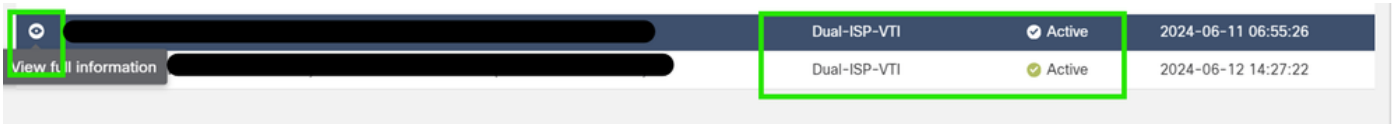


Verifica

1. Accedere a Dispositivi > VPN > Monitoraggio da sito a sito .



2. Fai clic sull'occhio per controllare ulteriori dettagli sullo stato del tunnel.



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).