Configurazione della migrazione VPN tra FTD gestiti da un singolo FMC

Sommario

Introduzione

Prerequisiti

- Requisiti
- Componenti usati

Configurazione

- Procedura

Verifica

Risoluzione dei problemi

- Problemi iniziali di connettività
- Problemi specifici del traffico

Introduzione

Questo documento descrive la migrazione di una VPN da sito a sito da un FTD all'altro, gestita dallo stesso FMC, mantenendo la connessione VPN al router.

Prerequisiti

Requisiti

Per eseguire in modo efficace il processo di migrazione, Cisco consiglia di familiarizzare con gli argomenti forniti:
· Registrazione FTD presso il CCP: Come registrare i dispositivi Firepower Threat Defense (FTD) con Firepower Management Center (FMC).
· Configurazione VPN da sito a sito: Esperienza nella configurazione di VPN da sito a sito su dispositivi FTD gestiti da FMC.

Componenti usati

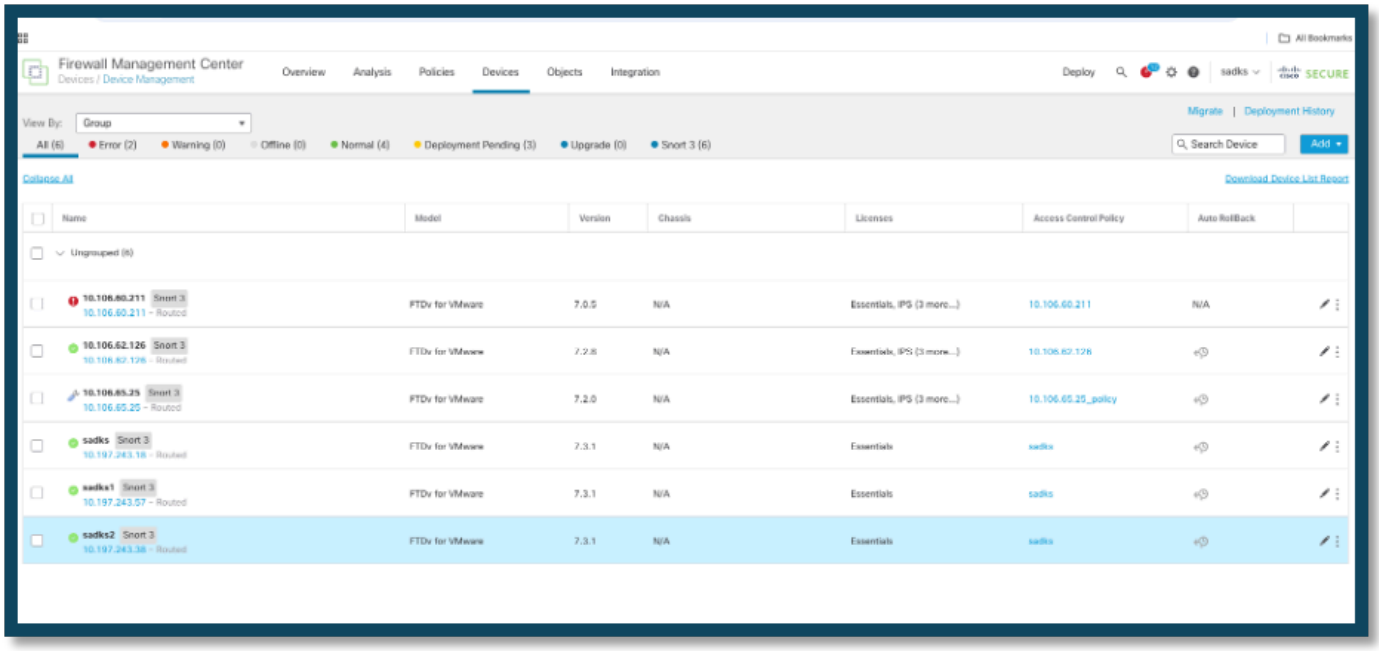
Questo documento si basa sulle versioni software e hardware fornite:
· Firepower Threat Defense Virtual (FTDv): Due istanze che eseguono la versione 7.3.1.
· Firepower Management Center (FMC): Versione 7.4.0.

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.

Configurazione

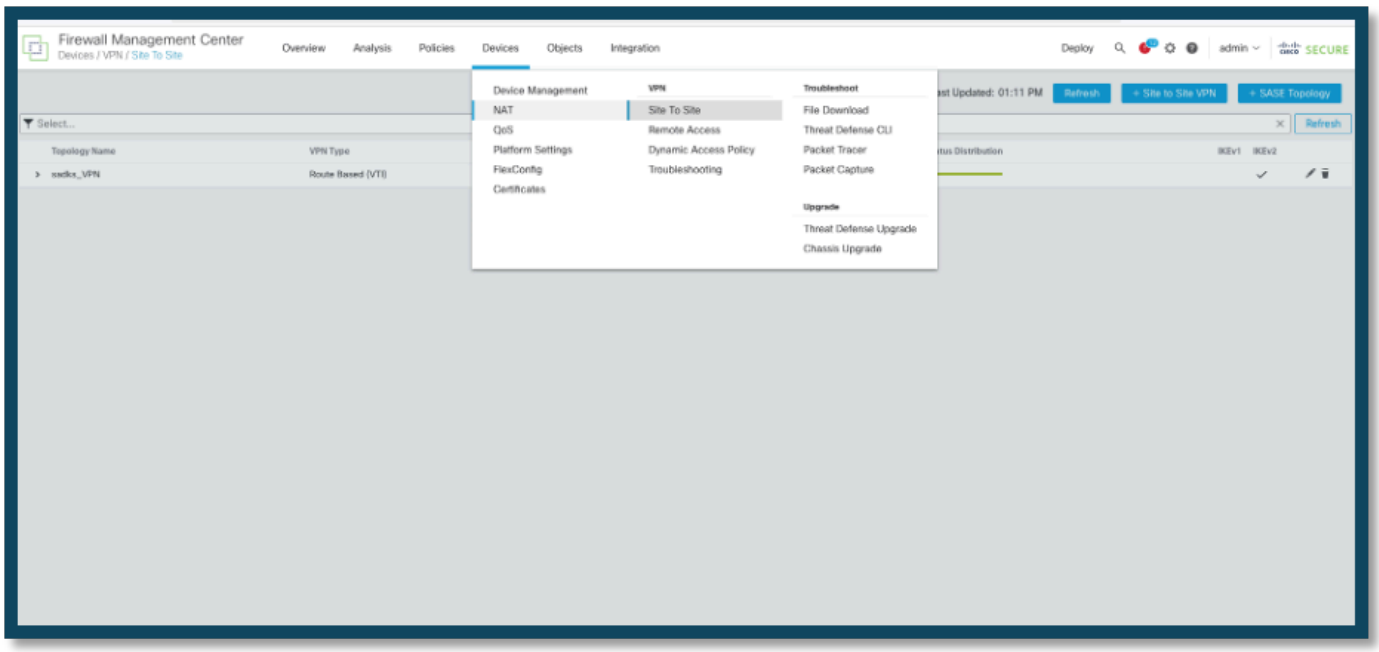
Procedura

1. Registrare il nuovo FTD presso il CCP:
   · Iniziare registrando il nuovo dispositivo Firepower Threat Defense (FTD) in Firepower Management Center (FMC) in Dispositivi > Gestione dispositivi.
   · In questo esempio, il nuovo dispositivo registrato è denominato "sadks2".



Nuovo FTD registrato

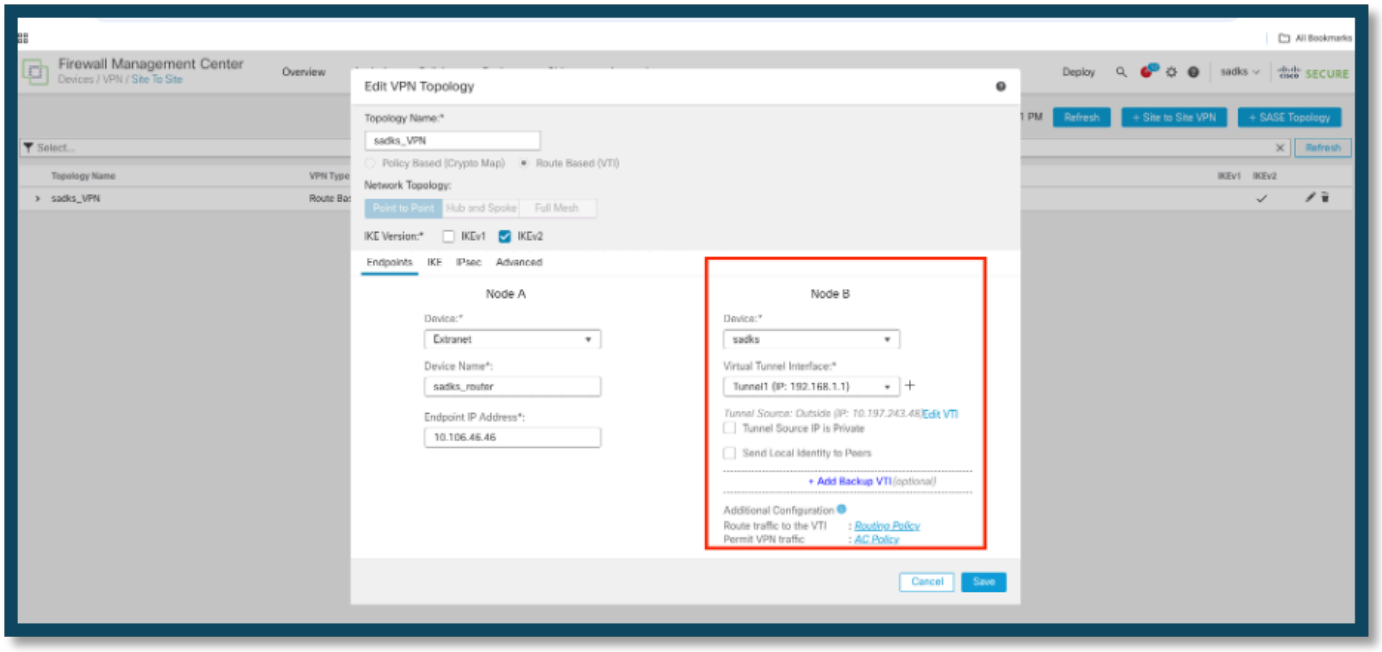
2. Accedere alla configurazione del tunnel da sito a sito:
   · Passare alle impostazioni del tunnel da sito a sito passando a Dispositivi > Da sito a sito nell'interfaccia FMC.



3. Modificare la configurazione VPN:

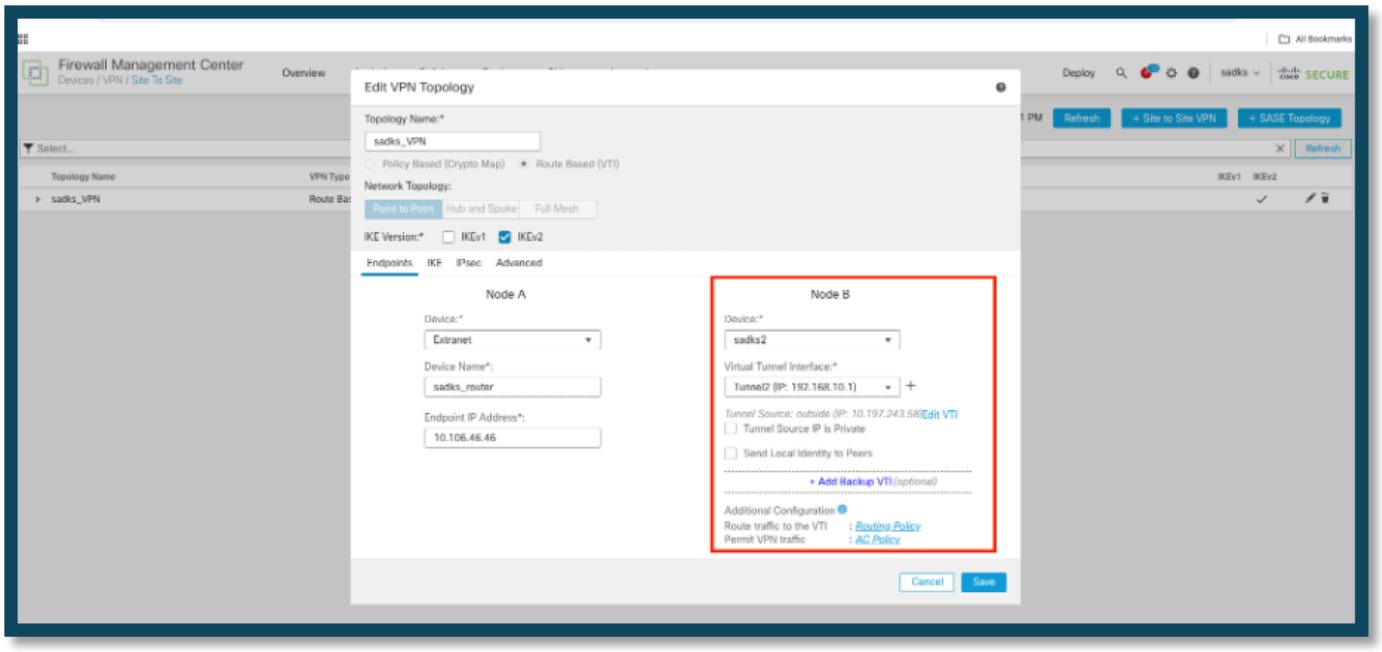
· Selezionare la configurazione VPN da aggiornare.

•Esempio: In questo scenario, la configurazione VPN interessa un dispositivo FTD e un router. Qui, il nodo B rappresenta il dispositivo FTD, e la configurazione è stata aggiornata per modificare l'associazione del dispositivo da "sadks" a "sadks2".



Dispositivo FTD precedente

A



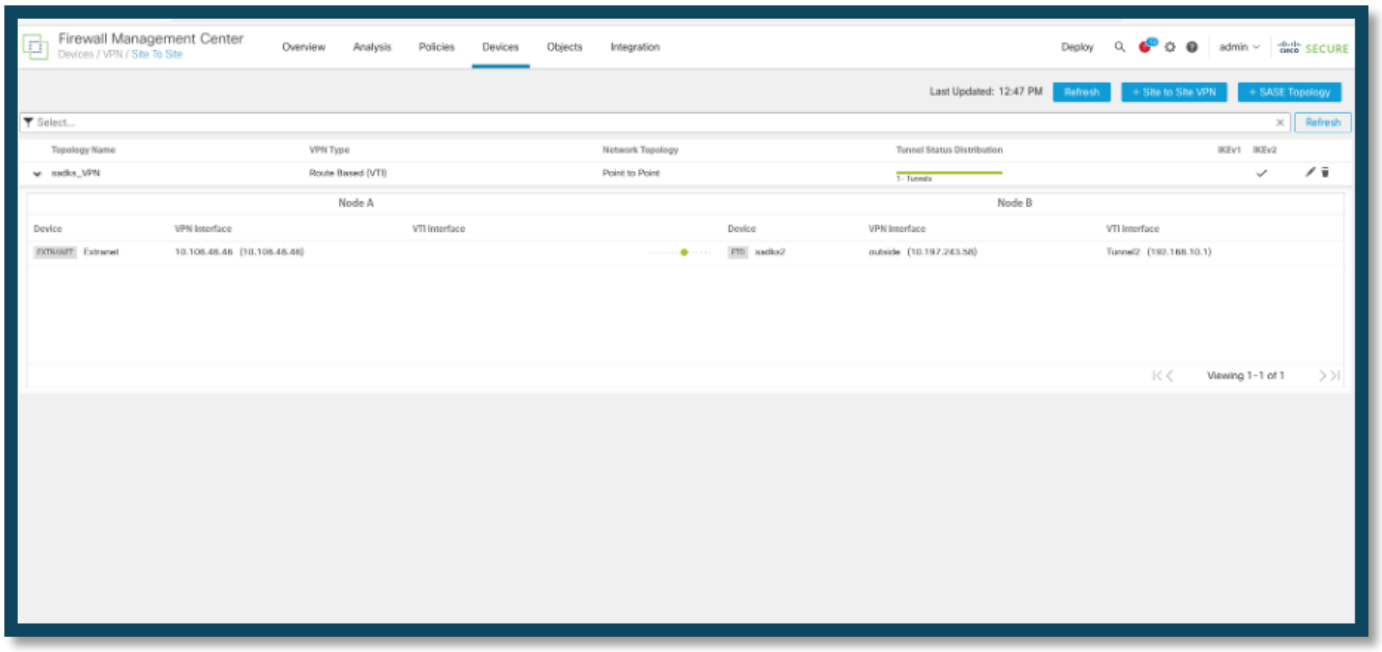
Nuovo dispositivo FTD

4. Salvare e distribuire la configurazione:

· Dopo aver apportato le modifiche necessarie, salvare la configurazione e distribuirla per attivare gli aggiornamenti.

Verifica

Il tunnel viene attivato una volta implementato.



Stato tunnel

Risoluzione dei problemi

Problemi iniziali di connettività

Quando si costruisce una VPN, ci sono due lati che negoziano il tunnel. Pertanto, è meglio ottenere entrambi i lati della conversazione quando si risolvono i problemi relativi a qualsiasi tipo di errore del tunnel. Una guida dettagliata su come eseguire il debug dei tunnel IKEv2 è disponibile qui: Come eseguire il debug delle VPN IKEv2

La causa più comune degli errori del tunnel è un problema di connettività. Il modo migliore per determinare questa condizione è acquisire i pacchetti sul dispositivo. Usare questo comando per acquisire i pacchetti sul dispositivo:

<#root>

```
capture capout interface outside match ip host 10.106.46.46 host 10.197.243.58
```

Una volta eseguita l'acquisizione, provare a inviare il traffico sulla VPN e verificare la presenza di traffico bidirezionale nell'acquisizione dei pacchetti.

Esaminare l'acquisizione dei pacchetti con questo comando:

<#root>

```
show cap capout
```

Problemi specifici del traffico

I problemi più comuni che si possono verificare sono:

- Problemi di routing dietro l'FTD — la rete interna non è in grado di indirizzare i pacchetti agli indirizzi IP e ai client VPN assegnati.
- Access Control List che blocca il traffico.
- Non è possibile ignorare Network Address Translation per il traffico VPN.

Per ulteriori informazioni sulle VPN sull'FTD gestito da FMC, è possibile consultare la guida alla configurazione completa qui: Guida alla configurazione di FTD gestito da FMC

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).