Konfiguration der VPN-Migration zwischen FTDs, die von einem einzigen FMC verwaltet werden

Inhalt

Einleitung

In diesem Dokument wird die Migration eines standortübergreifenden VPN von einem FTD zu einem anderen beschrieben, das vom gleichen FMC verwaltet wird, während die VPN-Verbindung zum Router erhalten bleibt.

Voraussetzungen

Anforderungen

Zur effektiven Durchführung des Migrationsprozesses empfiehlt Cisco, sich mit den folgenden Themen vertraut zu machen:
- FTD-Registrierung beim FMC: Sie wissen, wie Sie Firepower Threat Defense (FTD)-Geräte beim Firepower Management Center (FMC) registrieren können.
- Standortübergreifende VPN-Konfiguration: Erfahrung bei der Konfiguration von Site-to-Site-VPNs auf von FMC verwalteten FTD-Geräten.

Verwendete Komponenten

Dieses Dokument basiert auf den angegebenen Software- und Hardwareversionen:
- Firepower Threat Defense Virtual (FTDv): Zwei Instanzen mit Version 7.3.1.
- FirePOWER Management Center (FMC): Version 7.4.0

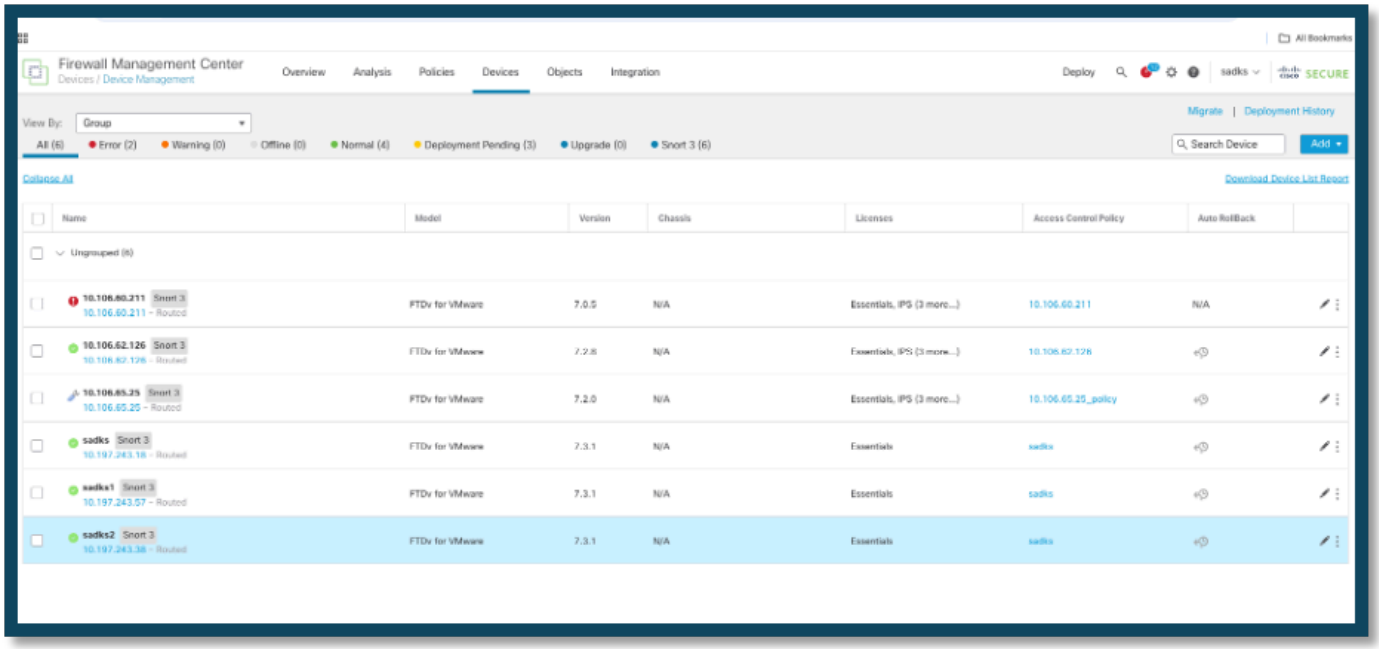
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher,

dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

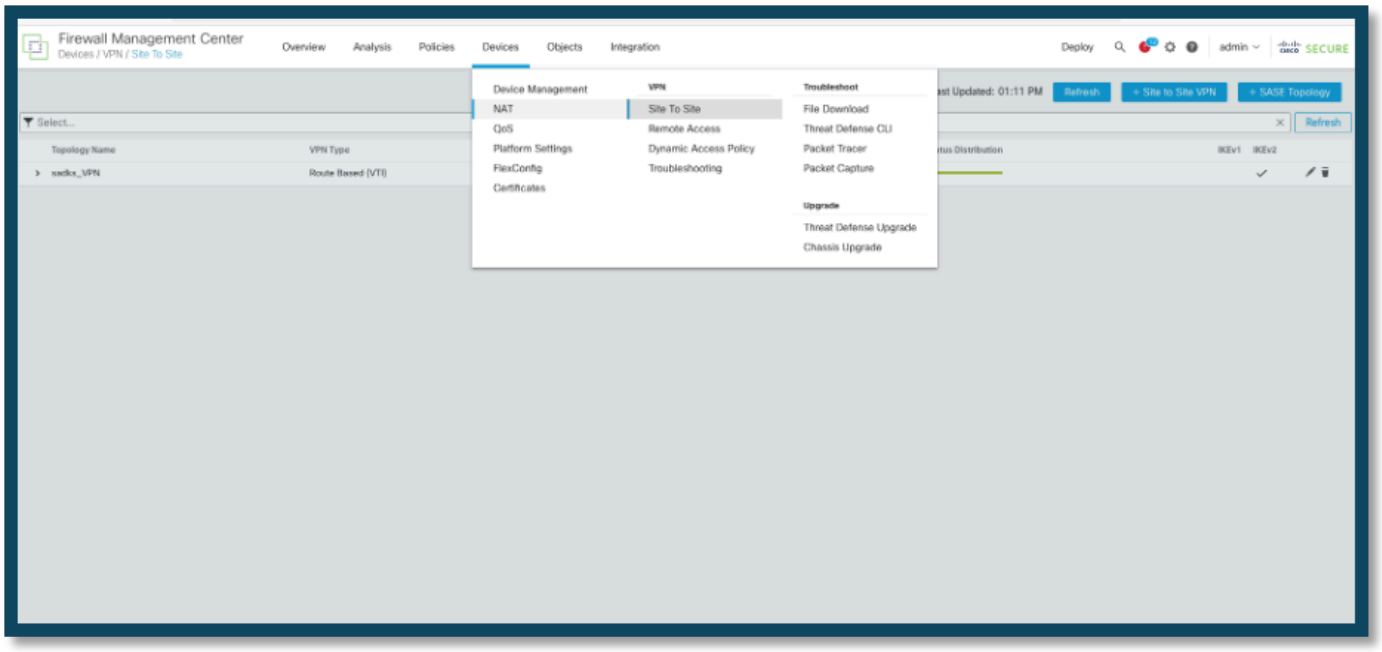
Vorgehensweise

1. Registrieren Sie die neue FTD bei FMC:
   - Registrieren Sie zunächst das neue FirePOWER Threat Defense (FTD)-Gerät im FirePOWER Management Center (FMC) unter Devices (Geräte) > Device Management (Geräteverwaltung).
   - In diesem Beispiel hat das neu registrierte Gerät den Namen "sadks2".



Neue FTD registriert

2. Zugreifen auf die Konfiguration des standortübergreifenden Tunnels:
   - Navigieren Sie zu den Site-to-Site-Tunneleinstellungen, indem Sie Devices > Site-to-Site in der FMC-Schnittstelle auswählen.

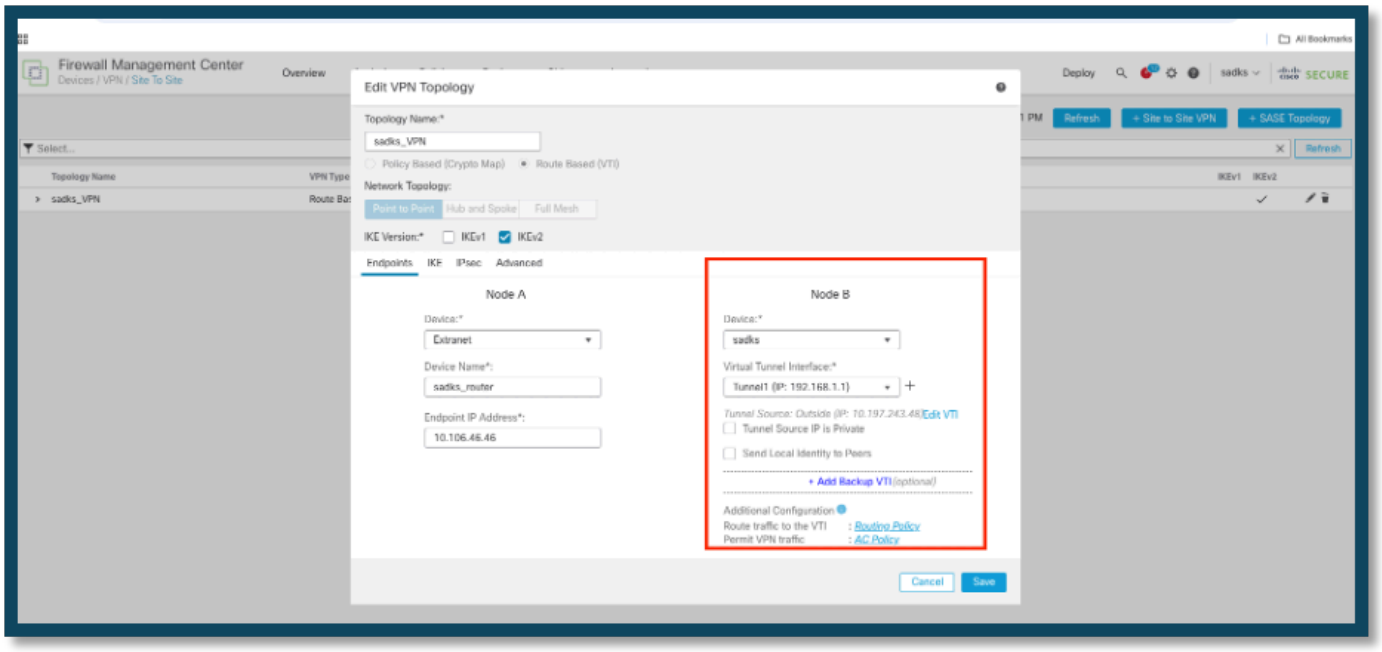


Zur VPN-Konfiguration navigieren

3. Ändern Sie die VPN-Konfiguration:

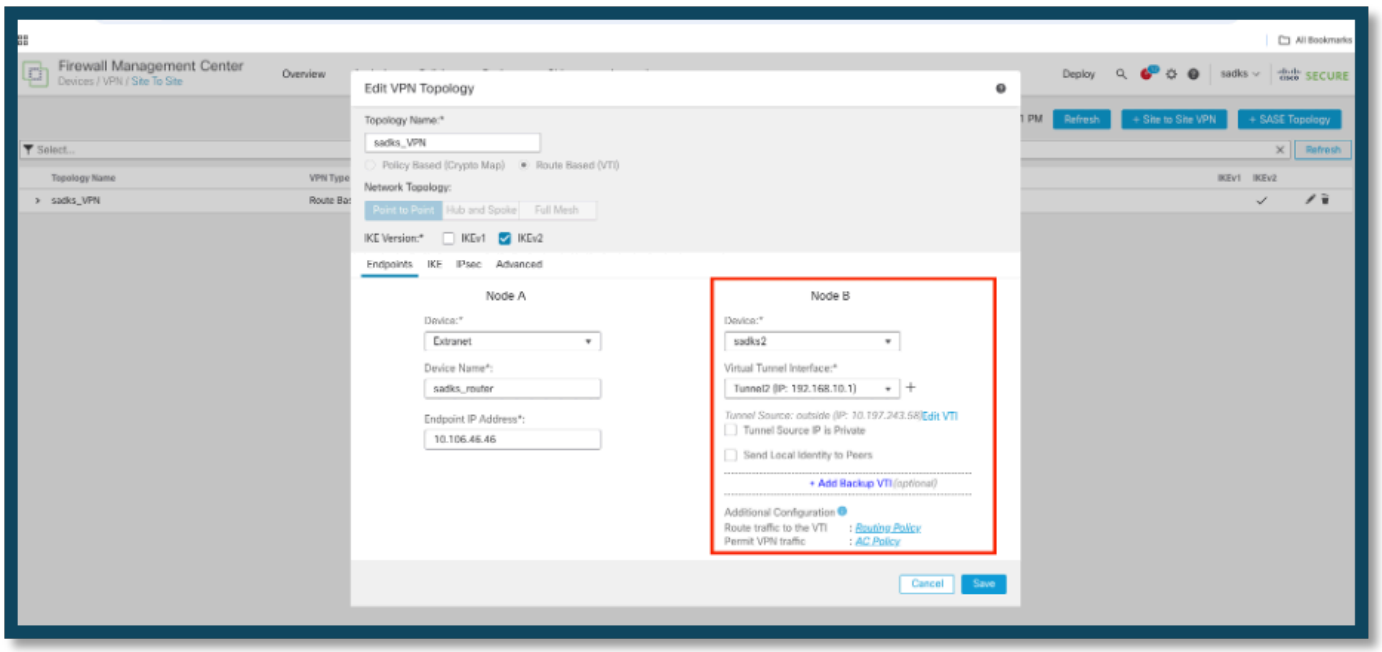
- Wählen Sie die VPN-Konfiguration aus, die Sie aktualisieren möchten.

•Beispiel: In diesem Szenario umfasst die VPN-Konfiguration ein FTD-Gerät und einen Router. Hier repräsentiert Knoten B das FTD-Gerät. Die Konfiguration wurde aktualisiert, um die Gerätezuordnung von "sadks" zu "sadks2" zu ändern.



Altes FTD-Gerät

ZU



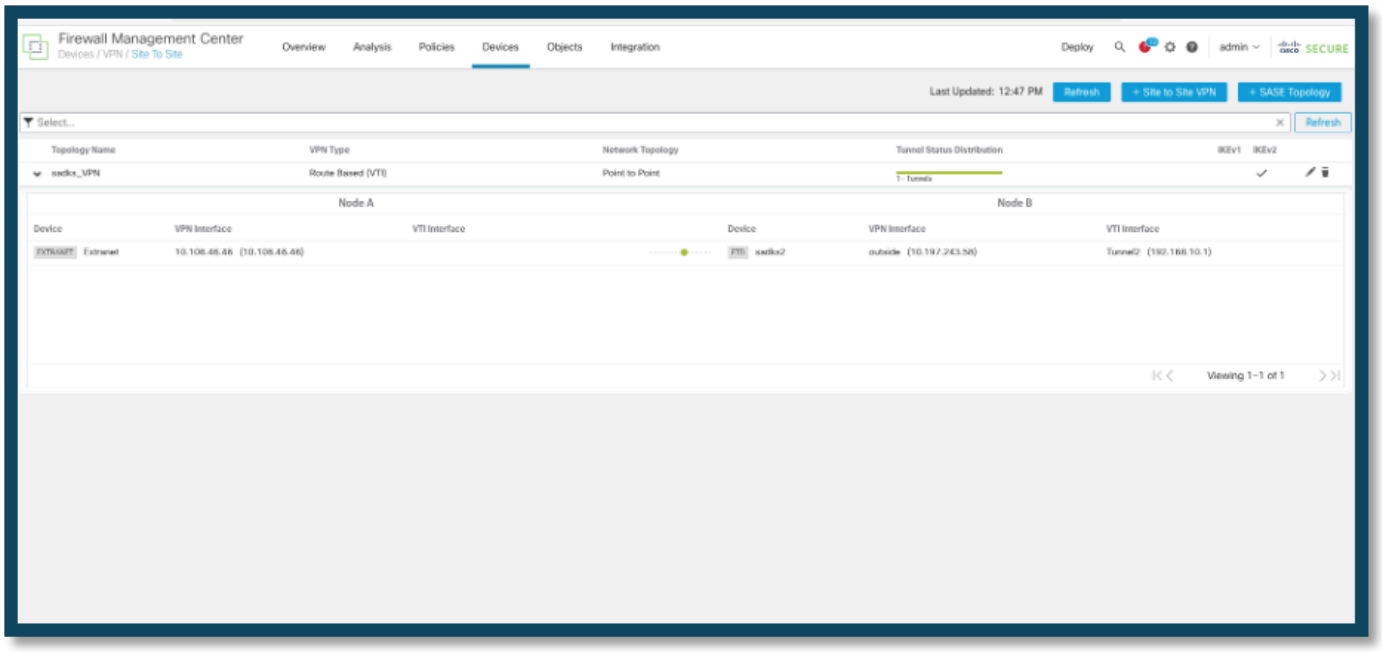
Neues FTD-Gerät

4. Speichern und Bereitstellen der Konfiguration:

- Speichern Sie die Konfiguration, nachdem Sie die erforderlichen Änderungen vorgenommen haben, und stellen Sie sie bereit, um die Updates zu aktivieren.

Überprüfung

Der Tunnel wird nach der Bereitstellung hochgefahren.



Tunnelstatus

Fehlerbehebung

Anfängliche Verbindungsprobleme

Beim Aufbau eines VPN gibt es zwei Seiten, die den Tunnel aushandeln. Daher ist es am besten, bei der Fehlerbehebung bei Tunnelausfällen beide Seiten des Gesprächs zu berücksichtigen. Eine detaillierte Anleitung zum Debuggen von IKEv2-Tunneln finden Sie hier: [So debuggen Sie IKEv2-VPNs]

Die häufigste Ursache von Tunnelausfällen ist ein Verbindungsproblem. Der beste Weg, dies zu bestimmen, besteht darin, die Paketerfassung auf dem Gerät zu übernehmen. Verwenden Sie diesen Befehl, um die Paketerfassung auf dem Gerät zu übernehmen:

<#root>

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

Sobald die Erfassung implementiert ist, versuchen Sie, Datenverkehr über das VPN zu senden, und prüfen Sie, ob bei der Paketerfassung bidirektionaler Datenverkehr vorhanden ist.

Überprüfen Sie die Paketerfassung mit dem folgenden Befehl:

<#root>

```
show cap capout
```

Datenverkehrsspezifische Probleme

Häufige Probleme mit dem Datenverkehr:

- Routingprobleme hinter dem FTD - internes Netzwerk kann Pakete nicht zu den zugewiesenen IP-Adressen und VPN-Clients zurückleiten.
- Zugriffskontrolllisten blockieren den Datenverkehr.
- Die Network Address Translation wird für den VPN-Datenverkehr nicht umgangen.

Weitere Informationen zu VPNs auf dem von FMC verwalteten FTD finden Sie im vollständigen Konfigurationsleitfaden: FTD verwaltet durch FMC-Konfigurationsleitfaden

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.