Fehlerbehebung bei EIGRP auf von FMC verwalteten FTD-Geräten

Inhalt

Einleitung

Voraussetzungen

- Anforderungen
- Verwendete Komponenten

Hintergrundinformationen

- Netzwerkdiagramm

Basiskonfiguration

Validierung

Validierung mit CLI

Fehlerbehebung

- Szenario 1 - IP EIGRP Neighbor debuggen
- Szenario 2 - Authentifizierung
- Szenario 3 - Passive Schnittstellen

Zugehörige Informationen

Einleitung

In diesem Dokument wird beschrieben, wie Sie die EIGRP-Konfiguration auf einem vom FMC verwalteten FTD überprüfen und Fehler auf diesem beheben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- EIGRP (Enhanced Interior Gateway Routing Protocol)
- Cisco Secure Firewall Management Center (FMC)
- Cisco Secure Firewall Threat Defense (FTD)

Verwendete Komponenten

- FTDv in Version 7.4.2.
- FMCv in Version 7.4.2.

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.

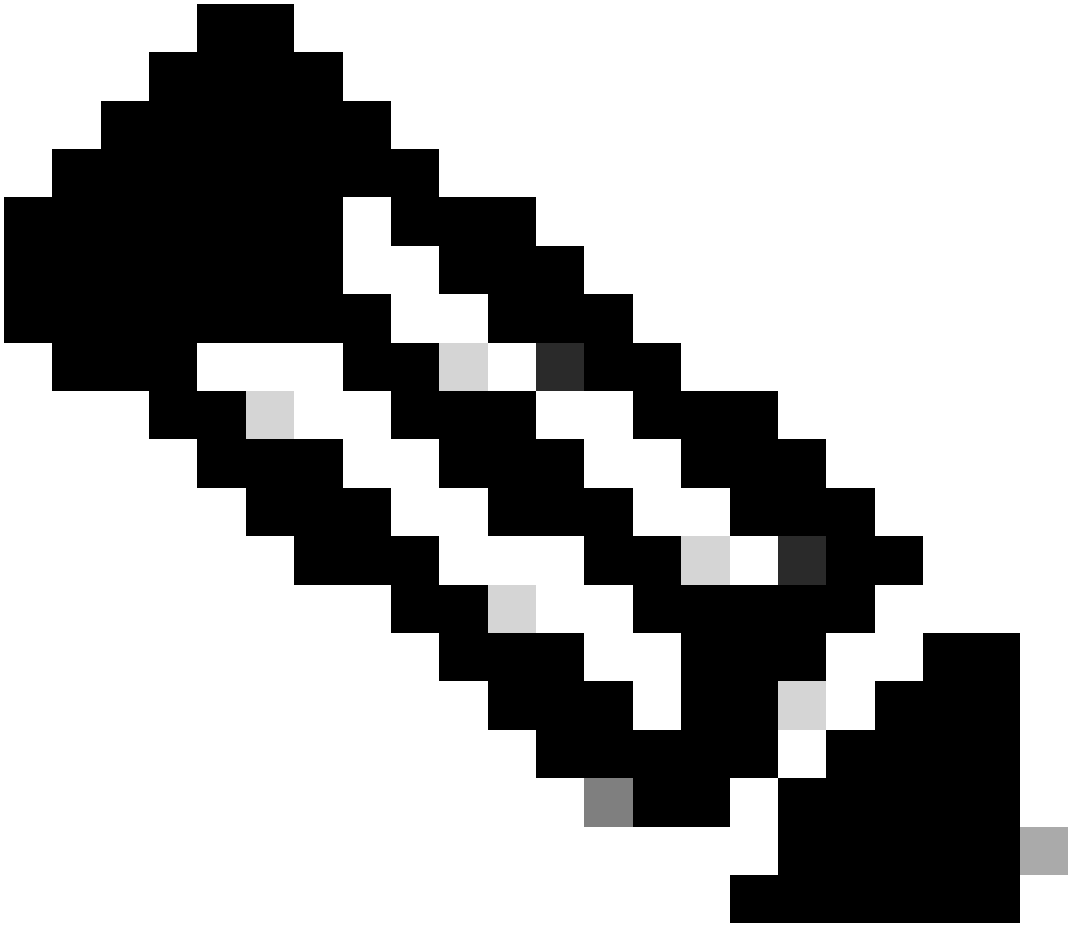
Hintergrundinformationen

EIGRP ist ein fortschrittliches Distanzvektor-Routing-Protokoll, das Funktionen von Distanzvektor- und Link-State-Protokollen kombiniert. Er bietet schnelle Konvergenz durch die Pflege von Routing-Informationen von Nachbarn, sodass eine schnelle Anpassung an alternative Routen möglich ist. EIGRP ist effizient und nutzt partielle, ausgelöste Updates für Routen- oder Metrikänderungen anstelle von regelmäßigen, vollständigen Updates.
Für die Kommunikation arbeitet EIGRP direkt auf der IP-Ebene (Protokoll 88) und nutzt das Reliable Transport Protocol (RTP) für eine garantierte, geordnete Paketübermittlung. Es unterstützt sowohl Multicast als auch Unicast, wobei die Multicast-Adressen 224.0.0.10 oder FF02::A für Hello-Nachrichten verwendet werden.
Der EIGRP-Betrieb basiert im Wesentlichen auf den Informationen, die in drei Tabellen gespeichert sind:

- Nachbartabelle: Diese Tabelle enthält einen Datensatz der direkt verbundenen EIGRP-Geräte, mit denen eine Adjacency erfolgreich eingerichtet wurde.
- Topologietabelle: In dieser Tabelle werden alle erlernten Routen gespeichert, die von Nachbarn angekündigt wurden, einschließlich aller möglichen Pfade zu einem bestimmten Ziel und der zugehörigen Metriken, sodass ihre Qualität und die Anzahl der verfügbaren Pfade evaluiert werden können.
- Routingtabelle: Diese Tabelle enthält den besten Pfad für jedes Ziel, der als 'Successor' bezeichnet wird. Diese Successor-Route wird aktiv für die Weiterleitung von Datenverkehr verwendet und anschließend anderen EIGRP-Nachbarn angekündigt.

EIGRP verwendet bei Routing- und Metrikberechnungen metrische Gewichtungen, die als K-Werte bezeichnet werden, um den optimalen Pfad zu einem Ziel zu bestimmen. Dieser metrische Wert wird von einer Formel abgeleitet, die folgende Parameter verwendet:

- Bandbreite
- Verzögerungszeit
- Zuverlässigkeit
- Wird geladen
- MTU

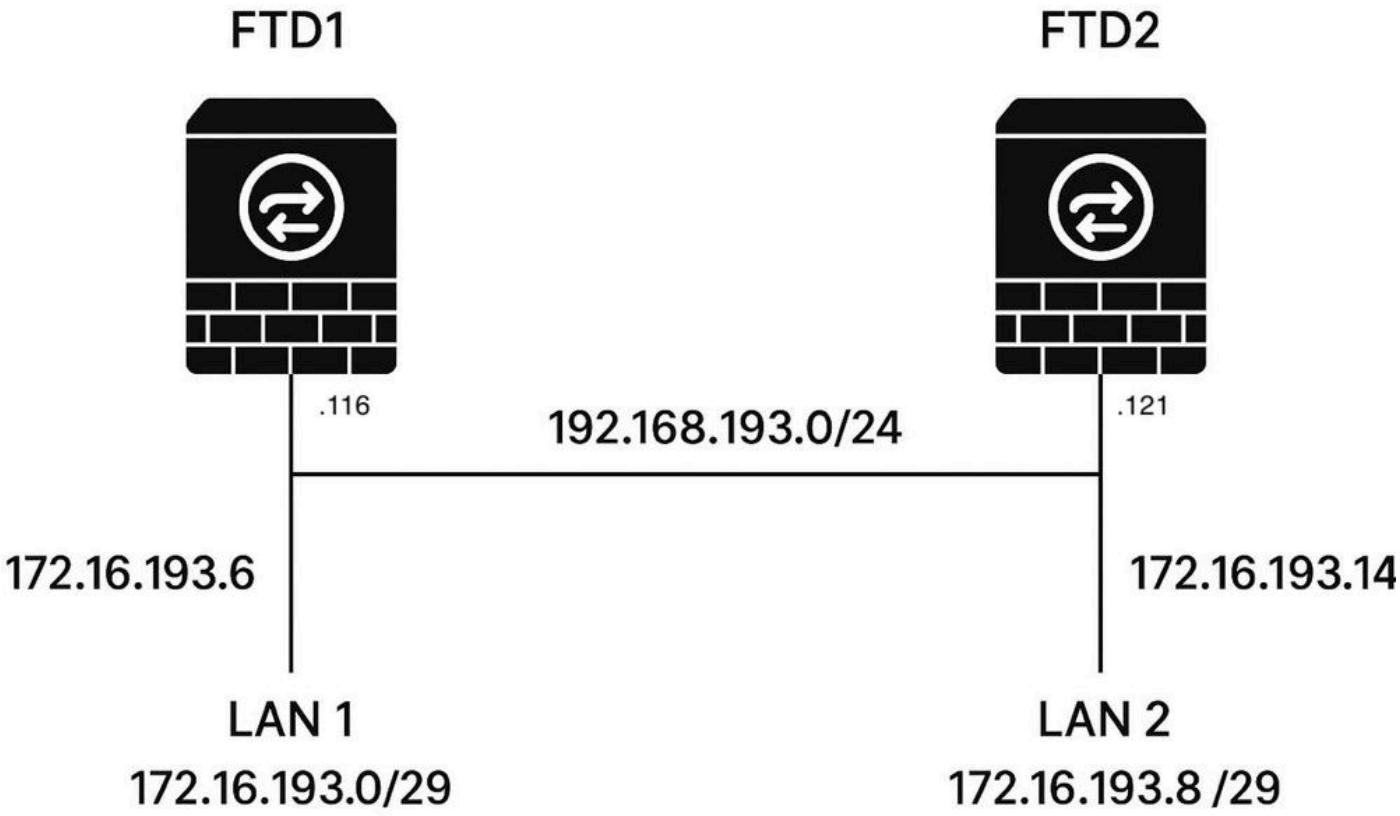


Anmerkung: Im Fall einer metrischen Verknüpfung zwischen mehreren Pfaden wird die Maximum Transmission Unit (MTU) als Verbindungsunterbrecher verwendet, wobei ein höherer MTU-Wert bevorzugt wird.

- Nachfolgeroute: Dies ist der beste Pfad zu einem bestimmten Ziel. Dies ist die Route, die letztendlich in der Routing-Tabelle installiert wird.
- Durchführbare Entfernung (FD): Dies ist die aus Sicht des lokalen Routers am besten berechnete Kennzahl zum Erreichen eines bestimmten Subnetzes.
- Gemeldete Entfernung (RD) / Angekündigte Entfernung (AD): Dies ist die Entfernung (metrisch) zu einem bestimmten Subnetz, die von einem Nachbarn gemeldet wird. Damit ein Pfad als möglicher Nachfolger betrachtet werden kann, muss die gemeldete Entfernung vom Nachbarn kleiner als die tatsächliche Entfernung des lokalen Routers zum gleichen Ziel sein.
- Durchführbarer Nachfolger (FS): Hierbei handelt es sich um einen Backup-Pfad zu einem Ziel, der eine alternative Route bereitstellt, falls die primäre Successor-Route ausfällt. Ein

Pfad gilt als möglicher Nachfolger, wenn seine gemeldete Entfernung (vom Werbenachbarn) strikt kleiner ist als die mögliche Entfernung der aktuellen Nachfolgeroute zum gleichen Ziel.

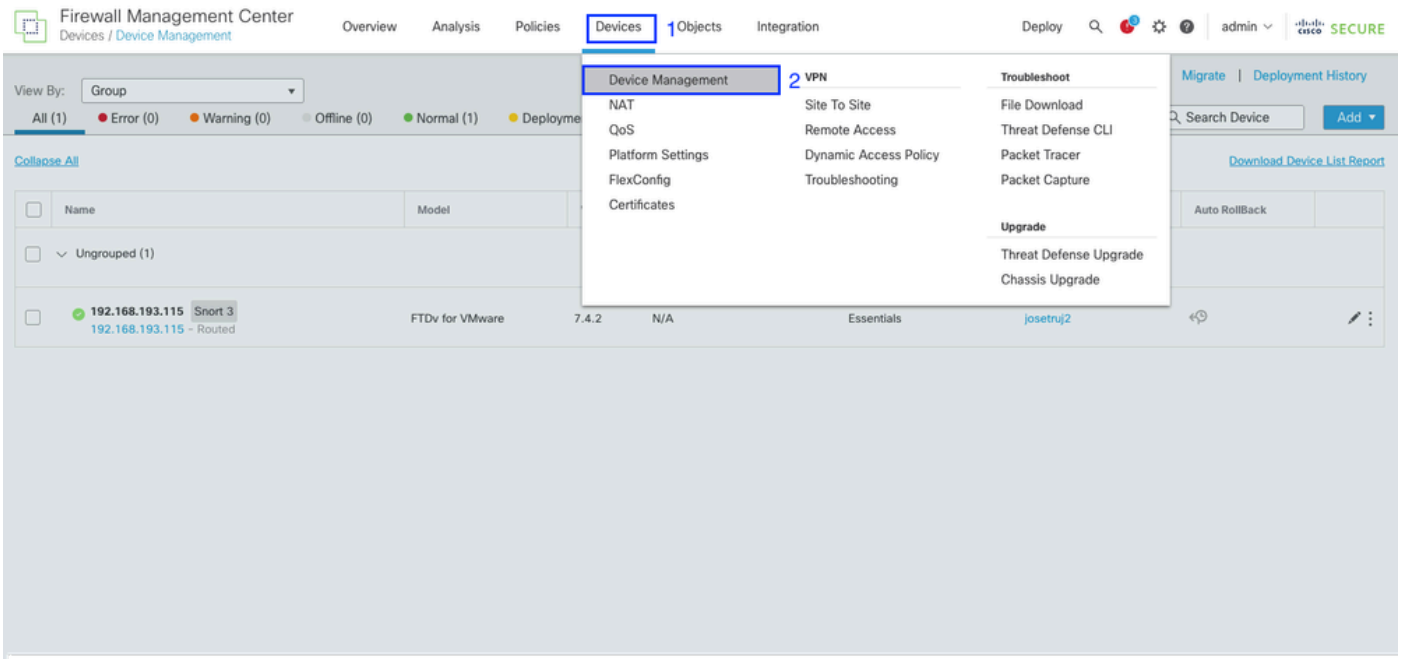
Netzwerkdiagramm



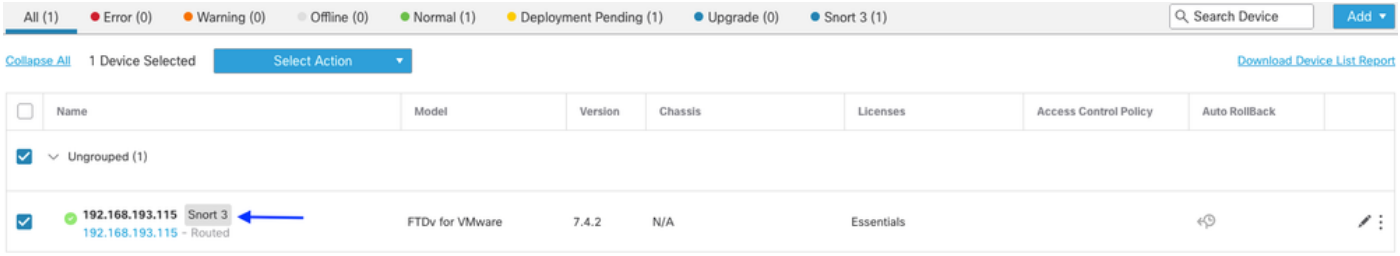
Netzwerkdiagramm

Basiskonfiguration

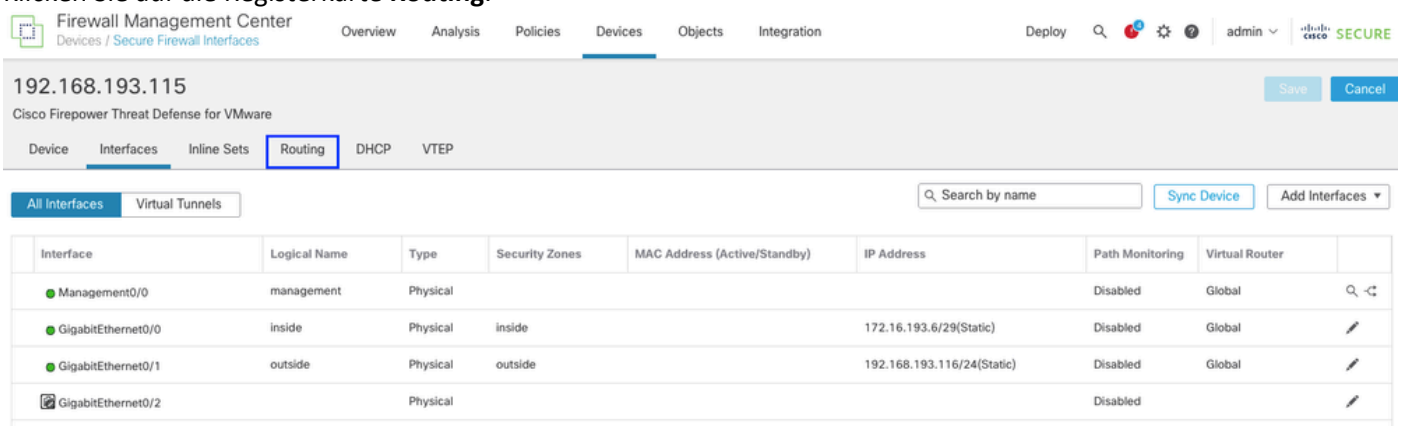
Navigieren Sie zu **Geräte > Geräteverwaltung**:



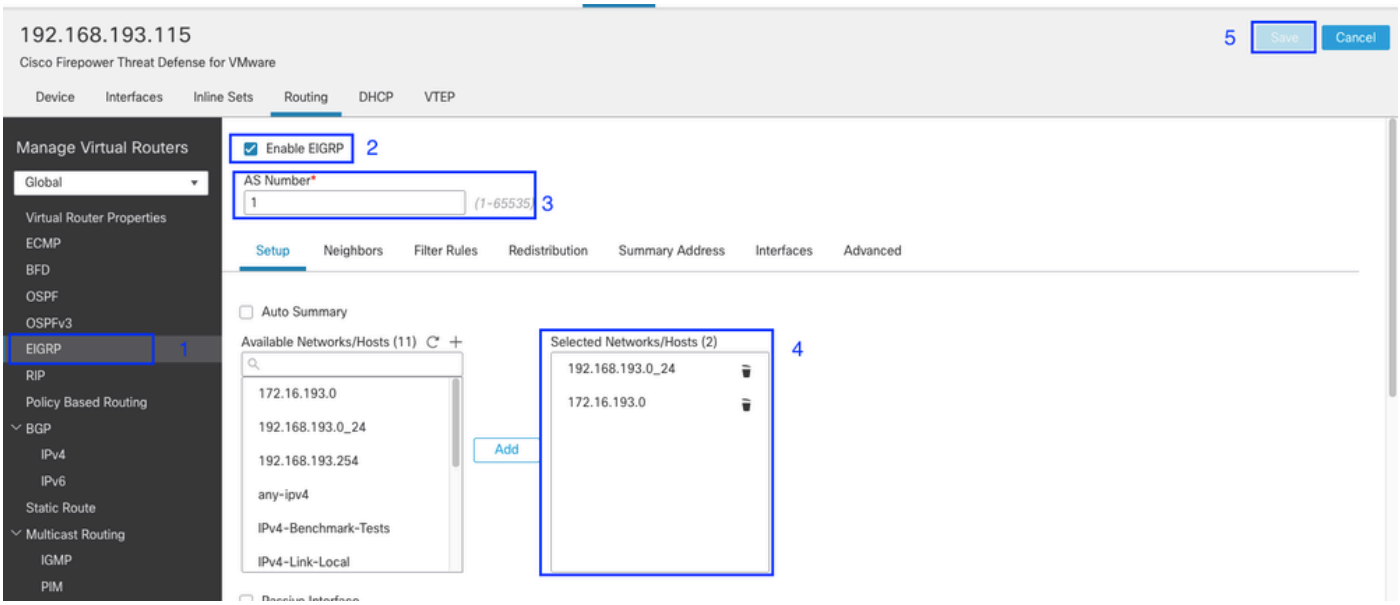
Gerät **auswählen**:



Klicken Sie auf die Registerkarte **Routing**.



Klicken Sie im linken Menü auf **EIGRP**.
Klicken Sie auf **EIGRP aktivieren**.
Weisen Sie die **AS-Nummer** (1-65535) zu.
Wählen Sie ein **Netzwerk/einen Host aus**. Sie können entweder ein zuvor erstelltes Objekt aus der Liste 'Verfügbares Netzwerk/Host' auswählen oder ein neues Objekt erstellen, indem Sie auf die Schaltfläche Plus (**+**) klicken.
Klicken Sie auf **Speichern**.



Validierung

Es folgen die Mindestanforderungen für die EIGRP-Nachbaradjazenz:

- Die AS-Nummer muss übereinstimmen.
- Die Schnittstelle muss aktiv und erreichbar sein.
- Die Hello- und Hold-Timer müssen übereinstimmen.
- K-Werte müssen übereinstimmen.
- Keine Zugriffslisten dürfen EIGRP-Datenverkehr blockieren.

Validierung mit CLI

- show run router eigrp
- eigrp-Nachbarn anzeigen
- EIGRP-Topologie anzeigen
- eigrp-Schnittstellen anzeigen
- Routen-EIGRP anzeigen
- eigrp-Datenverkehr anzeigen
- debug ip eigrp neighbor
- debug eigrp-Pakete

firepower# show run router eigrp

Router EIGRP 1

Keine Standardinformationen in

keine Standardinformationen ausgehend

keine eigrp log-neighbor-Warnungen

Keine Änderungen beim EIGRP-Protokoll-Nachbarn

Netzwerk 192.168.193.0 255.255.255.0

```
 Netzwerk 172.16.193.8 255.255.255.248

Feuerkraft#

firepower# show eigrp neighbors

EIGRP-IPv4-Nachbarn für AS(1)

H Address Interface Hold Uptime SRTT RTO Q Seq

                                    (Sek.) (ms) Cnt Num

0 192.168.193.121 außerhalb 14 21:45:04 40 240 0 30

firepower# eigrp-Topologie anzeigen

EIGRP-IPv4-Topologietabelle für AS(1)/ID(192.168.193.121)

Codes: P - Passiv, A - Aktiv, U - Update, Q - Abfrage, R - Antworten,

       r - reply Status, s - sia Status

P 192.168.193.0 255.255.255.0, 1 Nachfolger, FD ist 512

        über Verbunden, außen

P 172.16.193.0 255.255.255.248, 1 Nachfolger, FD ist 768

        über 192.168.193.116 (768/512), außerhalb

P 172.16.193.8 255.255.255.248, 1 Nachfolger, FD ist 512

        via Verbunden, innen

firepower# show eigrp interfaces

EIGRP-IPv4-Schnittstellen für AS(1)

                        Durchschnittliche XMIT-Warteschlangenpacing-Zeit für Multicast ausstehend

Schnittstelle Peers Unzuverlässige/Zuverlässige Routen von SRTT Un Zuverlässige Flow Timer

Außen 1 0 / 0 10 0 / 1 50 0

innen 0 0 / 0 0 / 1 0

Feuerkraft#


firepower# show route eigrp

Codes: L - lokal, C - verbunden, S - statisch, R - RIP, M - mobil, B - BGP
```

D - EIGRP, EX - EIGRP extern, O - OSPF, IA - OSPF interarea

N1 - OSPF NSSA extern Typ 1, N2 - OSPF NSSA extern Typ 2

E1 - externer OSPF-Typ 1, E2 - externer OSPF-Typ 2, V - VPN

i - IS-IS, su - IS-IS-Zusammenfassung, L1 - IS-IS-Ebene-1, L2 - IS-IS-Ebene-2

ia - IS-IS interarea, * - candidate default, U - per user static route

o - ODR, P - periodische heruntergeladene statische Route, + - replizierte Route

SI = Static InterVRF, BI = BGP InterVRF

Gateway der letzten Instanz ist 192.168.193.254 zum Netzwerk 0.0.0.0

D 172.16.193.0 255.255.255.248

[90/768] 192.168.193.116, 02:32:58, außerhalb

firepower# show route

Codes: L - lokal, C - verbunden, S - statisch, R - RIP, M - mobil, B - BGP

D - EIGRP, EX - EIGRP extern, O - OSPF, IA - OSPF interarea

N1 - OSPF NSSA extern Typ 1, N2 - OSPF NSSA extern Typ 2

E1 - externer OSPF-Typ 1, E2 - externer OSPF-Typ 2, V - VPN

i - IS-IS, su - IS-IS-Zusammenfassung, L1 - IS-IS-Ebene-1, L2 - IS-IS-Ebene-2

ia - IS-IS interarea, * - candidate default, U - per user static route

o - ODR, P - periodische heruntergeladene statische Route, + - replizierte Route

SI = Static InterVRF, BI = BGP InterVRF

Gateway der letzten Instanz ist 192.168.193.254 zum Netzwerk 0.0.0.0

S* 0.0.0.0 0.0.0.0 [1/0] via 192.168.193.254, außerhalb

D 172.16.193.0 255.255.255.248

[90/768] 192.168.193.116, 02:33:41 Uhr, außerhalb

C 172.16.193.8 255.255.255.248 ist direkt angeschlossen, innen

L 172.16.193.14 255.255.255.255 ist direkt angeschlossen, innen

C 192.168.193.0 255.255.255.0 ist direkt angeschlossen, außen

L 192.168.193.121 255.255.255.255 ist direkt angeschlossen, außen

Feuerkraft#

firepower# eigrp-Datenverkehr anzeigen

EIGRP-IPv4-Datenverkehrsstatistik für AS(1)

  Hellos gesendet/empfangen: 4006/4001

  Gesendete/empfangene Updates: 4/4

  Gesendete/empfangene Abfragen: 0/0

  Gesendete/empfangene Antworten: 0/0

  Gesendete/empfangene Nachrichten: 3/2

  SIA-Abfragen gesendet/empfangen: 0/0

  SIA-Antworten gesendet/empfangen: 0/0

  Hallo Prozess-ID: 2503149568

  PDM-Prozess-ID: 2503150496

  Socket-Warteschlange:

  Eingabewarteschlange: 0/2000/2/0 (aktuelle/max/höchste/tropfen)

Feuerkraft#

Fehlerbehebung

Szenario 1 - IP EIGRP Neighbor debuggen

Mithilfe von Debugbefehlen können Änderungen in Nachbarstaaten beobachtet werden.

firepower# debug ip eigrp neighbor

Feuerkraft#

EIGRP: Haltezeit abgelaufen

Absteigend: Peer 192.168.193.121 total=0 stub 0, iidb-stub=0 id-all=0

EIGRP: Fehler beim Aufheben der Zuweisung [0]

EIGRP: Nachbar 192.168.193.121 ging draußen unter

Führen Sie den Befehl show eigrp neighbors aus, um den Nachbarstatus zwischen den FTDs zu überprüfen.

firepower# show eigrp neighbors

EIGRP-IPv4-Nachbarn für AS(1)

Überprüfen Sie den Status der Schnittstellen mit dem Befehl show interface ip brief. Sie können feststellen, dass die GigabitEthernet0/1-Schnittstelle administrativ ausgefallen ist.

firepower# show interface ip brief

Schnittstelle IP-Adresse OK? Methodenstatusprotokoll

GigabitEthernet0/0 172.16.193.14 JA KONFIGURATION HOCH

GigabitEthernet0/1 192.168.193.121 YES KONFIGURATION administrativ nach oben

GigabitEthernet0/2 192.168.194.24 JA, Manuell aktiv

Internal-Control0/0 127.0.1.1 JA nicht eingerichtet

Interne Steuerung0/1 nicht zugewiesen JA nicht eingerichtet

Internal-Data0/0 nicht zugewiesen JA nicht eingerichtet

Internal-Data0/0 nicht zugewiesen JA nicht eingerichtet

Internal-Data0/1 169.254.1.1 JA nicht eingerichtet

Internal-Data0/2 nicht zugewiesen JA nicht eingerichtet

Management0/0 203.0.113.130 JA nicht eingerichtet

Szenario 2 - Authentifizierung

Die FTD unterstützt den MD5-Hash-Algorithmus zur Authentifizierung von EIGRP-Paketen. Diese Authentifizierung ist standardmäßig deaktiviert.

Um den MD5-Hash-Algorithmus zu aktivieren, aktivieren Sie das Kontrollkästchen "MD5 Authentication". Es ist wichtig, dass die Authentifizierungseinstellungen auf beiden Geräten übereinstimmen. Wenn diese Funktion auf einem Gerät, jedoch nicht auf dem anderen aktiviert ist, können sich keine Nachbarumgebungen bilden.

Überprüfen Sie diese Konfiguration mit debug eigrp packages.

firepower# debug eigrp-Pakete

(UPDATE, REQUEST, QUERY, REPLY, HELLO, IPXSAP, PROBE, ACK, STUB, SIAQUERY, SIAREPLY)EIGRP-Paketdebugging ist aktiviert.

Feuerkraft#

EIGRP: Außen: ignoriertes Paket von 192.168.193.121, Opcode = 5 (Authentifizierung deaktiviert

oder Schlüsselbund fehlt)

EIGRP: HELLO außerhalb Nbr 172.16.193.14 erhalten

AS 1, Flags 0x0:(NULL), Seq 0/0 interfaceQ 0/0

EIGRP: HELLO wird nach außen gesendet

AS 1, Flags 0x0:(NULL), Seq 0/0 interfaceQ 0/0 iidbQ un/relay 0/0

EIGRP: HELLO nach innen senden

AS 1, Flags 0x0:(NULL), Seq 0/0 interfaceQ 0/0 iidbQ un/relay 0/0

EIGRP: Außen: ignoriertes Paket von 192.168.193.121, Opcode = 5 (Authentifizierung deaktiviert oder Schlüsselbund fehlt)

EIGRP: HELLO außerhalb Nbr 172.16.193.14 erhalten

AS 1, Flags 0x0:(NULL), Seq 0/0 interfaceQ 0/0

EIGRP: HELLO nach innen senden

AS 1, Flags 0x0:(NULL), Seq 0/0 interfaceQ 0/0 iidbQ un/relay 0/0

EIGRP: HELLO wird nach außen gesendet

AS 1, Flags 0x0:(NULL), Seq 0/0 interfaceQ 0/0 iidbQ un/relay 0/0

EIGRP: Außen: Paket von 192.168.193.121 ignoriert, Opcode = 5 (Authentifizierung deaktiviert oder Schlüsselbund fehlt).

Sie können eine Meldung beobachten, die anzeigt, dass die Authentifizierung deaktiviert ist oder die Schlüsselkette fehlt. In diesem Szenario tritt dies in der Regel dann auf, wenn die Authentifizierung auf einem Peer aktiviert ist, auf dem anderen jedoch nicht.

EIGRP: Außen: Paket von 192.168.193.121 ignoriert, Opcode = 5 (Authentifizierung deaktiviert oder Schlüsselbund fehlt).

Verifizieren mit show run interface <EIGRP-Schnittstelle>.

FirePOWER1# show run interface GigabitEthernet0/1

!

interface GigabitEthernet0/1

nameif extern

Sicherheitsstufe 0

ip address 192.168.193.121 255.255.255.0

Authentifizierungsschlüssel eigrp 1 ***** Schlüssel-ID 10

Authentifizierungsmodus eigrp 1 md5

FirePOWER2# show run interface GigabitEthernet0/1

!

interface GigabitEthernet0/1

nameif extern

Sicherheitsstufe 0

ip address 192.168.193.116 255.255.255.0

Szenario 3 - Passive Schnittstellen

Wenn EIGRP konfiguriert ist, werden EIGRP-Hello-Pakete in der Regel an Schnittstellen gesendet und empfangen, an denen das Netzwerk aktiviert ist.

Wenn eine Schnittstelle jedoch als passiv konfiguriert ist, unterdrückt EIGRP den Austausch von Hello-Paketen zwischen zwei Routern an dieser Schnittstelle, was zum Verlust der Nachbarumgebungen führt. Folglich verhindert diese Aktion nicht nur, dass der Router Routing-Updates von dieser Schnittstelle aus ankündigt, sondern verhindert auch, dass er Routing-Updates von dieser Schnittstelle empfängt.

Führen Sie den Befehl show eigrp neighbors aus, um den Nachbarstatus zwischen den FTDs zu überprüfen.

firepower# show eigrp neighbors

EIGRP-IPv4-Nachbarn für AS(1)

Sie können die gesendeten EIGRP-Pakete und die Schnittstellen, über die sie gesendet werden, mithilfe des Befehls debug eigrp packages überprüfen.

FTD 1

FirePOWER1#

(UPDATE, REQUEST, QUERY, REPLY, HELLO, IPXSAP, PROBE, ACK, STUB, SIAQUERY, SIAREPLY)EIGRP-Paketdebugging ist aktiviert.

Feuerkraft#

EIGRP: HELLO wird nach außen gesendet

AS 1, Flags 0x0:(NULL), Seq 0/0 interfaceQ 0/0 iidbQ un/relay 0/0

EIGRP: HELLO nach innen senden

AS 1, Flags 0x0:(NULL), Seq 0/0 interfaceQ 0/0 iidbQ un/relay 0/0

EIGRP: HELLO wird nach außen gesendet

AS 1, Flags 0x0:(NULL), Seq 0/0 interfaceQ 0/0 iidbQ un/relay 0/0

EIGRP: HELLO nach innen senden

AS 1, Flags 0x0:(NULL), Seq 0/0 interfaceQ 0/0 iidbQ un/relay 0/0

EIGRP: HELLO wird nach außen gesendet

FTD 2

FirePOWER2# debug eigrp packages

(UPDATE, REQUEST, QUERY, REPLY, HELLO, IPXSAP, PROBE, ACK, STUB, SIAQUERY, SIAREPLY)EIGRP-Paketdebugging ist aktiviert.

FirePOWER 2#

In diesem Szenario sendet FTD 2 keine EIGRP-Hello-Nachrichten, da seine internen und externen Schnittstellen als passiv konfiguriert sind. Überprüfen Sie dies mit dem Befehl show run router eigrp.

FirePOWER2# show run router eigrp

Router EIGRP 1

Keine Standardinformationen in

keine Standardinformationen ausgehend

keine eigrp log-neighbor-Warnungen

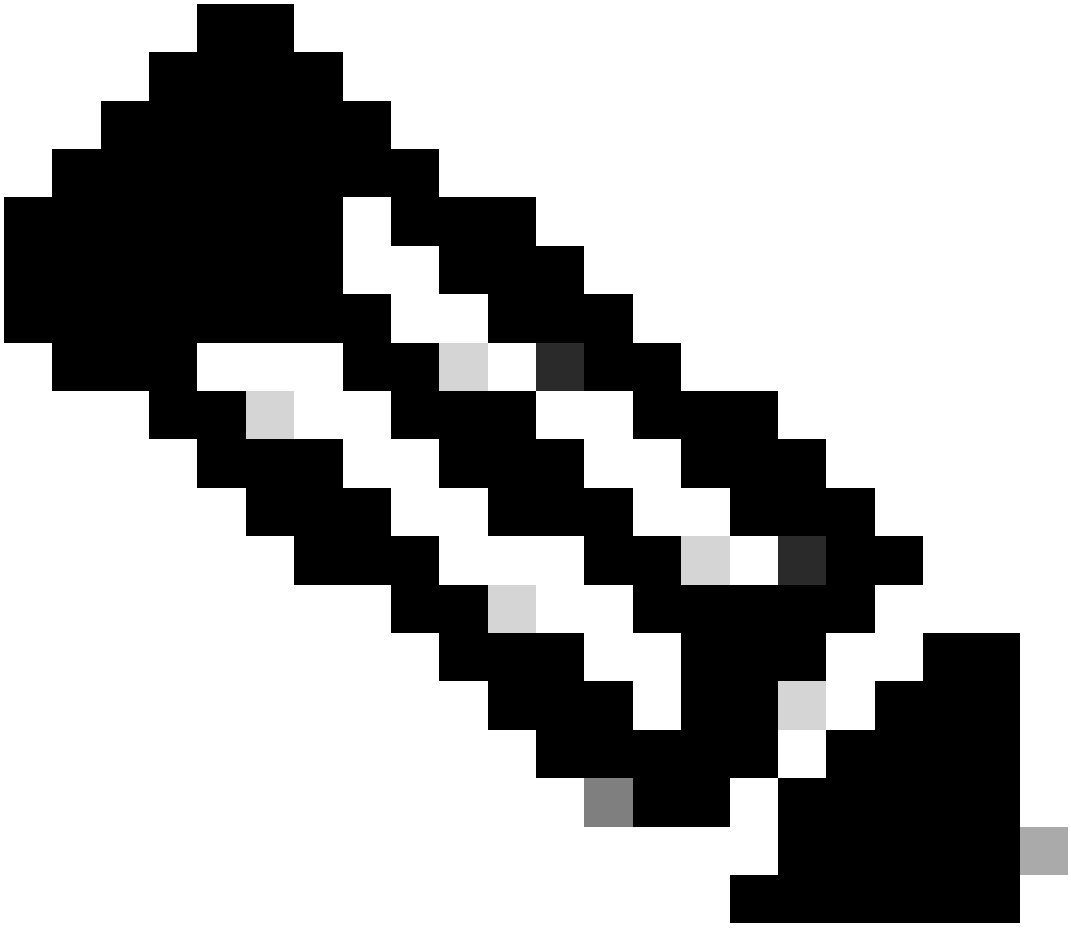
Keine Änderungen beim EIGRP-Protokoll-Nachbarn

Netzwerk 192.168.193.0 255.255.255.0

Netzwerk 172.16.193.8 255.255.255.248

passive Schnittstelle außen

passive Schnittstelle innen



Anmerkung: Um alle konfigurierten Debug-Prozesse zu stoppen, verwenden Sie den Befehl undebug all.

Zugehörige Informationen

- EIGRP auf FTD-Geräten
- Konfigurieren von EIGRP auf FTD
- EIGRP Composite Cost Metrics

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.