

Fehlerbehebung bei EIGRP auf FTD-Geräten

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[EIGRP-Hintergrund](#)

[Basiskonfiguration](#)

[Filterregeln](#)

[Neuverteilung](#)

[Schnittstelle](#)

[Hello- und Hold-Timer](#)

[Authentifizierung](#)

[Befehle zur Fehlerbehebung und Validierung](#)

[Verifizierung](#)

[Basiskonfiguration](#)

[Neuverteilung](#)

[Schnittstellenkonfiguration](#)

[Validierung mithilfe von Befehlen](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie die EIGRP-Konfiguration auf FTD-Geräten mit einem FMC als Manager überprüfen und Fehler bei diesen beheben.

Voraussetzungen

Anforderungen

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

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

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- FTDv für VMware in Version 7.2.8
- FMC für VMWare in Version 7.2.8

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.

EIGRP-Hintergrund

EIGRP kann auf einem FMC konfiguriert werden, um dynamisches Routing zwischen FTD-Geräten und anderen EIGRP-fähigen Geräten zu verwenden.

Das FMC ermöglicht nur die Konfiguration eines EIGRP Autonomous System (AS) im Einzelmodus.

Die nächsten Parameter müssen mit den EIGRP-Nachbarn übereinstimmen, um die EIGRP-Adjacency zu bilden.

- Eine Schnittstelle, die zum gleichen IP-Subnetz gehört.
- EIGRP AS
- Hello- und Hold-Intervalle
- MTU
- Schnittstellenauthentifizierung.

Basiskonfiguration

In diesem Abschnitt werden die erforderlichen Parameter für die EIGRP-Konfiguration beschrieben.

1. Navigieren Sie zu Geräte > Geräteverwaltung > Gerät bearbeiten
2. Klicken Sie auf die Registerkarte Routing.
3. Klicken Sie in der linken Menüleiste auf EIGRP.
4. Aktivieren Sie das Kontrollkästchen Enable EIGRP, um das Protokoll zu aktivieren, und weisen Sie der AS-Nummer einen Wert zwischen 1 und 65535 zu.
5. Beachten Sie, dass die Option Automatische Zusammenfassung standardmäßig deaktiviert ist.
6. Wählen Sie ein Netzwerk/einen Host aus. Sie können ein zuvor erstelltes Objekt verwenden oder ein neues Objekt hinzufügen, indem Sie auf die Schaltfläche zum Hinzufügen klicken (+)
7. (Optional) Aktivieren Sie das Kontrollkästchen Passive Schnittstelle, um die Schnittstellen auszuwählen, die den Datenverkehr nicht weiterverteilen.
8. Klicken Sie auf Speichern, um die Änderungen zu speichern.

Filterregeln

Mit dem FTD kann der Benutzer eine Verteilerliste konfigurieren, um die ein- und ausgehenden Routen zu steuern.

1. Navigieren Sie zu Geräte > Geräteverwaltung > Gerät bearbeiten
2. Klicken Sie auf die Registerkarte Routing.
3. Klicken Sie auf EIGRP.
4. Klicken Sie auf Filterregeln > Hinzufügen.
5. Wählen Sie die entsprechenden Informationen für die Filterfelder aus.

- Filterrichtung
- Schnittstelle auswählen
- Zugriffsliste auswählen

6. Fahren Sie mit den Schritten fort, wenn eine Standard-Zugriffsliste konfiguriert ist.

Wenn der Benutzer eine Standard-Zugriffsliste konfigurieren muss, klicken Sie auf die Schaltfläche mit dem Pluszeichen, oder erstellen Sie sie unter Objekte > Objektverwaltung > Zugriffsliste > Standard > Standard hinzufügen.

7. Zuweisen eines Namens zur Liste

8. Klicken Sie auf die Schaltfläche mit dem Pluszeichen (+).

- Aktion auswählen
- Fügen Sie das Netzwerk oder den Host aus dem verfügbaren Netzwerk zum ausgewählten Netzwerk hinzu.

9. Klicken Sie unten auf Hinzufügen, um den Zugriffslisteneintrag zu speichern.

10. Klicken Sie auf Speichern, um die Standard-Zugriffsliste zu speichern.

11. Klicken Sie auf OK.

12. Klicken Sie auf Speichern, um die Änderungen zu bestätigen.

Neuverteilung

Die FTD kann die von BGP-, RIP- und OSPF-Protokollen oder den statischen und verbundenen Routen generierten Routen auf das EIGRP verteilen.

1. Navigieren Sie zu Geräte > Geräteverwaltung > Gerät bearbeiten
2. Klicken Sie auf die Registerkarte Routing.
3. Klicken Sie auf EIGRP.
4. Klicken Sie auf Weiterverteilung.
5. Geben Sie die Informationen in die Felder für die Neuverteilung ein.

- Protokolle
 - RIP
 - OSPF
 - BGP
 - Verbunden
 - Statisch

Für OSPF muss die Prozess-ID angegeben werden, für BGP die AS-Nummer der hinterlegten Prozess-ID*.

Wenn für die Konfiguration eine Neuverteilung der vom OSPF-Protokoll generierten Informationen erforderlich ist, kann der Benutzer den OSPF-Typ "Neuverteilung" auswählen.

Optionale Kennzahlen beziehen sich auf die EIGRP-Kennzahlen und die Routenübersicht.

Schnittstelle

Hello- und Hold-Timer

Die Hello-Pakete werden für die Ermittlung von Nachbarn und zum Erkennen des verfügbaren Nachbarn verwendet. Diese Pakete werden in Intervallen versendet. Der Standardwert dieses Timers beträgt 5 Sekunden.

Hold-Timer: Diese Eigenschaft bestimmt, wie lange eine Route nach EIGRP erreichbar und funktionsfähig ist. Der Wert für die Haltezeit ist standardmäßig dreimal so groß wie das Hello-Intervall.

Authentifizierung

Die FTD unterstützt den MD5-Hash-Algorithmus zur Authentifizierung der EIGRP-Pakete. Standardmäßig ist die Authentifizierung deaktiviert.

Aktivieren Sie das Kontrollkästchen MD5 Authentication (MD5-Authentifizierung), um den MD5-Hashalgorithmus zu aktivieren.

Wichtigste

Unverschlüsselt - Nur-Text.

Verschlüsselt

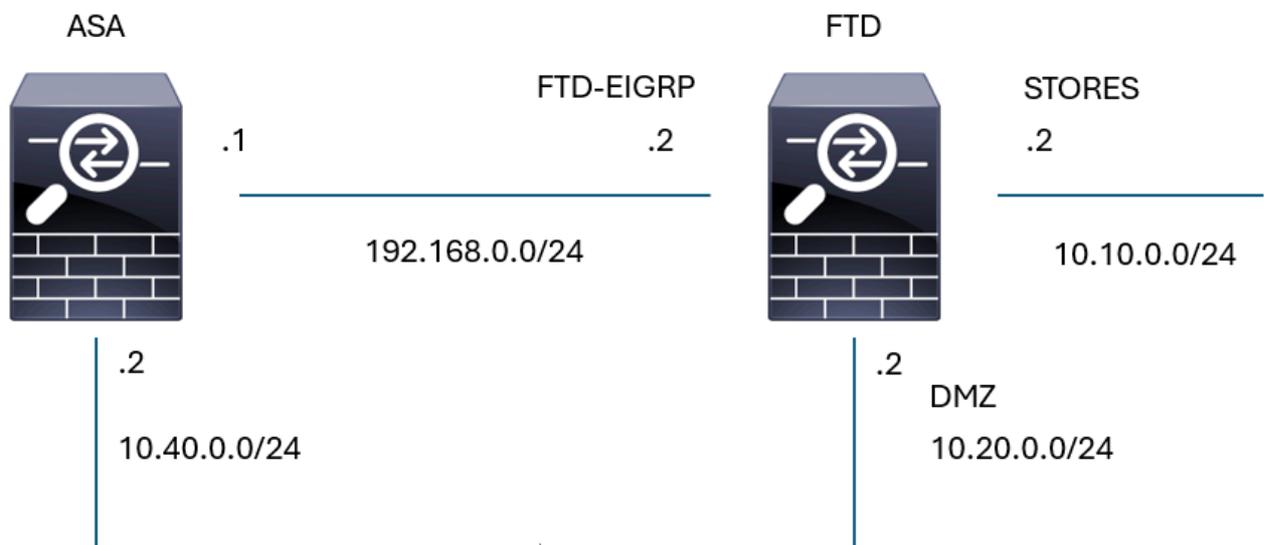
Befehle zur Fehlerbehebung und Validierung

- `show run router eigrp`. Zeigt die EIGRP-Konfiguration an
- `show run interface [Schnittstelle]`. Zeigt die Authentifizierungs- und Timer-Informationen der EIGRP-Schnittstelle an.
- `show eigrp events [{ start end} | type]`. Zeigt das EIGRP-Ereignisprotokoll an.

- show eigrp interfaces [if-name] [detail]. Zeigt die Schnittstellen an, die am EIGRP-Routing teilnehmen.
- show eigrp neighbors [detail | static] [if-name]. Zeigt die EIGRP-Nachbartabelle an.
- show eigrp topology [ip-addr [mask] | active | alle Verbindungen | ausstehend | zusammenfassung | 0-Nachfolger]. Zeigt die EIGRP-Topologietabelle an.
- eigrp-Datenverkehr anzeigen. Zeigt EIGRP-Verkehrsstatistiken an.

Verifizierung

Betrachten Sie die nächste Topologie. In diesem Abschnitt werden die zuvor beschriebenen Befehle verwendet, um die auf das FTD angewendete EIGRP-Konfiguration zu validieren.



EIGRP-Topologie

Basiskonfiguration

FTD02

Cisco Firepower Threat Defense for VMware

Device Routing Interfaces Inline Sets DHCP VTEP

Manage Virtual Routers

Global

Virtual Router Properties

ECMP

OSPF

OSPFv3

EIGRP

RIP

Policy Based Routing

✓ BGP

IPv4

IPv6

Static Route

✓ Multicast Routing

IGMP

PIM

Multicast Routes

Multicast Boundary Filter

General Settings

BGP

Enable EIGRP

AS Number*

100 (1-65535)

Setup

Neighbors

Filter Rules

Redistribution

Summary Address

Interfaces

Advanced

Auto Summary

Available Networks/Hosts (46)

Search

Selected Networks/Hosts (2)

EIGRP-sub	
STORES-sub	

Add

Passive Interface

Selected Interface All Interfaces

Available Interfaces (4)

diagnostic
DMZ
FTD-EIGRP
STORES

Selected Interfaces (2)

OUTSIDE	
INSIDE	

Add

EIGRP-Basiskonfiguration

Neuverteilung

Edit Redistribution ? X

Protocol

Protocol

Process ID

Optional OSPF Redistribution

Internal
 External1
 External2
 Nssa-External1
 Nssa-External2

Optional Metrics

Bandwidth
 (1-4294967295 in kbps)

Delay Time
 (0-4294967295 in 10µs)

Reliability
 (0-255)

Loading
 (1-255)

MTU
 (1-65535 in bytes)

Route Map
 +

EIGRP-Weiterverteilungskonfiguration

Schnittstellenkonfiguration

Edit Interface
ⓘ ×

Interface*

FTD-EIGRP

Hello Interval

10 (1-65535 in secs)

Hold Time

30 (1-65535 in secs)

Split Horizon

Delay Time

(1-16777215 in 10µs)

Authentication

Enable MD5 Authentication

Key Type

Auth Key

Key ID

5 (0-255)

Key

●●●●●●

Confirm Key

●●●●●●

Cancel

OK

EIGRP-Schnittstellenkonfiguration

Validierung mithilfe von Befehlen

```
<#root>
```

```
firepower#
```

```
show run router eigrp
```

```
router eigrp 100
no default-information in
no default-information out
no eigrp log-neighbor-warnings
no eigrp log-neighbor-changes
network 10.10.0.0 255.255.255.0
network 192.168.0.0 255.255.255.0
passive-interface OUTSIDE
passive-interface INSIDE
redistribute static
!
```

```
firepower#
```

```
show run int g 0/2
```

```
!
interface GigabitEthernet0/2
nameif FTD-EIGRP
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
```

```
security-level 0
ip address 192.168.0.2 255.255.255.0
hello-interval eigrp 100 10
hold-time eigrp 100 30
```

```
firepower#
```

```
show eigrp events
```

```
106 04:24:27.980 Conn rt change: 192.168.0.0 255.255.255.0 FTD-EIGRP
107 04:24:27.980 Lost route 1=forceactv: 192.168.0.0 255.255.255.0 0
108 04:24:27.980 Change queue emptied, entries: 1
109 04:24:27.980 Metric set: 192.168.0.0 255.255.255.0 512
110 04:24:27.980 Update reason, delay: new if 4294967295
111 04:24:27.980 Update sent, RD: 192.168.0.0 255.255.255.0 4294967295
112 04:24:27.980 Update reason, delay: metric chg 4294967295
113 04:24:27.980 Update sent, RD: 192.168.0.0 255.255.255.0 4294967295
114 04:24:27.980 Route installed: 192.168.0.0 255.255.255.0 0.0.0.0
115 04:24:27.980 Find FS: 192.168.0.0 255.255.255.0 4294967295
116 04:24:27.980 Rcv update met/succmet: 512 0
117 04:24:27.980 Rcv update dest/orig: 192.168.0.0 255.255.255.0 Connected
118 04:24:27.980 Metric set: 192.168.0.0 255.255.255.0 4294967295
119 04:24:27.980 Conn rt change: 192.168.0.0 255.255.255.0 FTD-EIGRP
```

```
firepower#
```

```
show eigrp interfaces
```

```
EIGRP-IPv4 Interfaces for AS(100)
Interface      Peers    Xmit Queue   Mean    Pacing Time   Multicast    Pending
                Un/Reliable SRTT      Un/Reliable   Flow Timer   Routes
FTD-EIGRP      1         0 / 0        48      0 / 1         193          0
```

```
firepower#
```

```
show eigrp neighbors
```

```
EIGRP-IPv4 Neighbors for AS(100)
H          Address          Interface          Hold    Uptime        SRTT    RTO    Q    Seq
                (sec)                                     (ms)
0          192.168.0.1      FTD-EIGRP          27      09:15:22      48      1458   0    4
```

```
firepower#
```

```
show eigrp topology
```

```
EIGRP-IPv4 Topology Table for AS(100)/ID(192.168.0.2)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
r - reply Status, s - sia Status

P 10.10.0.0 255.255.255.0, 1 successors, FD is 512
via Connected, STORES
P 10.40.0.0 255.255.255.0, 1 successors, FD is 768 ----- Route learn from EIGRP neighbor
via 192.168.0.1 (768/512), FTD-EIGRP
P 192.168.0.0 255.255.255.0, 1 successors, FD is 512
via Connected, FTD-EIGRP
P 0.0.0.0 0.0.0.0, 1 successors, FD is 512
via Rstatic (512/0)
```

```
firepower#
```

```
show eigrp traffic
```

```
EIGRP-IPv4 Traffic Statistics for AS(100)
```

```
Hello sent/received: 16606/6989
```

```
Updates sent/received: 8/4
```

```
Queries sent/received: 2/0
```

```
Replies sent/received: 0/1
```

```
Acks sent/received: 3/5
```

```
SIA-Queries sent/received: 0/0
```

```
SIA-Replies sent/received: 0/0
```

```
Hello Process ID: 4007513056
```

```
PDM Process ID: 4007513984
```

```
Socket Queue:
```

```
Input Queue: 0/2000/2/0 (current/max/highest/drops)
```

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.