

# Resolución de problemas de EIGRP en dispositivos FTD

## Contenido

---

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Fondo EIGRP](#)

[Configuración Básica](#)

[Reglas de filtro](#)

[Redistribución](#)

[Interfaz](#)

[Temporizadores hello y hold](#)

[Autenticación](#)

[Comandos de solución de problemas y validación](#)

[Verificación](#)

[Configuración Básica](#)

[Redistribución](#)

[Configuración de la interfaz](#)

[Validación mediante comandos](#)

---

## Introducción

Este documento describe cómo verificar y resolver problemas de configuración EIGRP en dispositivos FTD usando un FMC como administrador.

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conceptos y funcionalidad del protocolo de routing de gateway interior (EIGRP) mejorado
- Cisco Secure Firewall Management Center (FMC)
- Cisco Secure Firewall Threat Defence (FTD)

### Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- FTDv para VMWare en la versión 7.2.8.
- FMC para VMWare en la versión 7.2.8.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Fondo EIGRP

EIGRP se puede configurar en un FMC para utilizar el routing dinámico entre los dispositivos FTD y otros dispositivos compatibles con EIGRP.

El FMC solo permite configurar un sistema autónomo EIGRP (AS) en modo único.

Los siguientes parámetros deben coincidir con los vecinos EIGRP para formar la adyacencia EIGRP.

- Una interfaz que pertenece a la misma subred IP.
- EIGRP AS
- Intervalos de saludo y espera
- MTU (unidad de transmisión básica)
- Autenticación de la interfaz.

## Configuración Básica

Esta sección describe los parámetros necesarios para configurar EIGRP.

1. Vaya a Dispositivos > Administración de dispositivos > Editar dispositivo
2. Haga clic en la pestaña Routing.
3. Haga clic en EIGRP en la barra de menús izquierda.
4. Marque la casilla de verificación Enable EIGRP, para habilitar el protocolo, y asigne un valor entre 1-65535 a un número AS.
5. Tenga en cuenta que la opción Resumen automático está desactivada de forma predeterminada
6. Seleccione una red/host, puede utilizar un objeto creado anteriormente o agregar uno nuevo haciendo clic en el botón agregar (+)
7. (Opcional) Marque la casilla de verificación Interfaz pasiva, para seleccionar las interfaces que no redistribuyen el tráfico.
8. Haga clic en Save (Guardar) para guardar los cambios.

## Reglas de filtro

El FTD permite al usuario configurar una lista de distribución para controlar las rutas entrantes y salientes.

1. Vaya a Dispositivos > Administración de dispositivos > Editar dispositivo
2. Haga clic en la pestaña Routing.
3. Haga clic en EIGRP.
4. Haga clic en Filtrar reglas > Agregar.
5. Seleccione la información correspondiente para los campos de filtrado.

- Dirección del filtro
- Seleccionar interfaz
- Seleccionar lista de acceso

6. Vaya a los pasos, si hay una lista de acceso estándar configurada.

Si el usuario necesita configurar una lista de acceso estándar, haga clic en el botón más o créela desde Objetos > Administración de objetos > Lista de acceso > Estándar > Agregar lista de acceso estándar.

7. Asigne un nombre a la lista

8. Haga clic en el botón más ( + )

- Seleccione una acción
- Agregue la red o el host de la red disponible a la red seleccionada.

9. Haga clic en Agregar en la parte inferior para guardar la entrada de la lista de acceso.

10. Haga clic en Guardar para guardar la lista de acceso estándar.

11. Haga clic en Aceptar.

12. Haga clic en Guardar para validar los cambios.

## Redistribución

El FTD tiene la capacidad de redistribuir las rutas generadas desde los protocolos BGP, RIP y OSPF, o desde las rutas estáticas y conectadas al EIGRP.

1. Vaya a Dispositivos > Administración de dispositivos > Editar dispositivo
2. Haga clic en la pestaña Routing.
3. Haga clic en EIGRP.
4. Haga clic en Redistribución.
5. Introduzca la información en los campos de redistribución.

- Protocolo

- RIP
- OSPF
- BGP
- Conectado
- Estática

Para OSPF es necesario especificar el ID de proceso, y para BGP el número AS en el ID de proceso\* archivado.

Si la configuración requiere la redistribución de la información generada por el protocolo OSPF, el usuario puede seleccionar el tipo OSPF de Redistribución.

Las métricas opcionales hacen referencia a las métricas EIGRP y al Route Map.

## Interfaz

### Temporizadores hello y hold

Los paquetes de saludo se utilizan para la detección de vecinos y para detectar el vecino disponible. Estos paquetes se envían en intervalos; de forma predeterminada, el valor de este temporizador es de 5 segundos.

Temporizador de espera, determina la cantidad de tiempo que EIGRP considera que una ruta es alcanzable y funcional. De forma predeterminada, el valor del tiempo de espera es 3 veces el intervalo hello.

### Autenticación

El FTD admite el algoritmo hash MD5 para autenticar los paquetes EIGRP. De forma predeterminada, la autenticación está deshabilitada.

Marque la casilla MD5 Authentication (Autenticación MD5) para activar el algoritmo hash MD5.

#### Clave

Sin cifrar: texto sin formato.

Cifrados

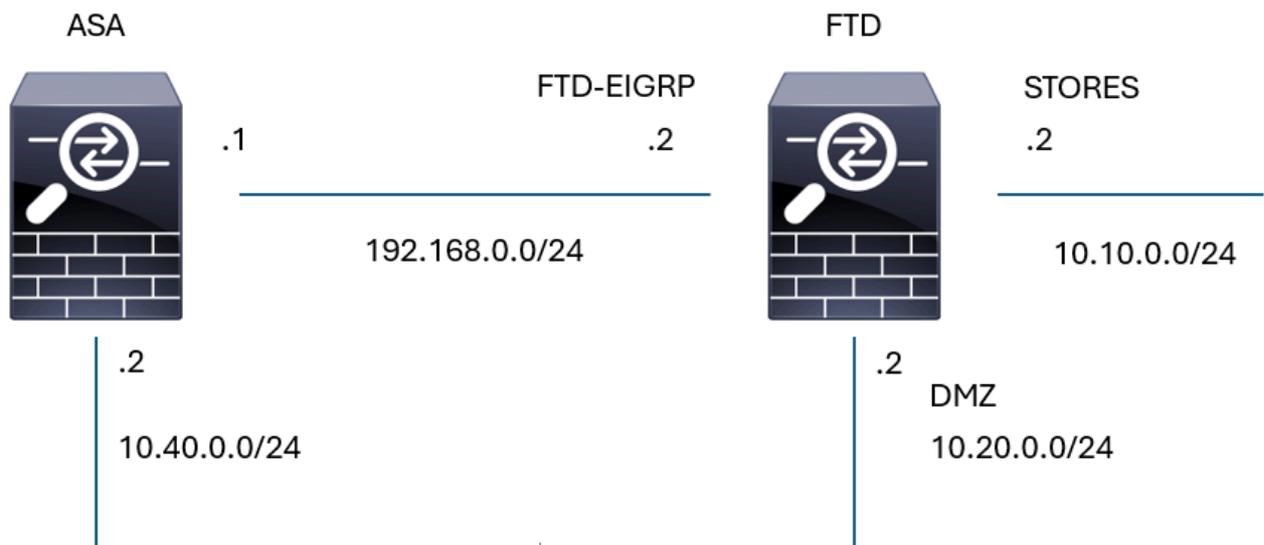
## Comandos de solución de problemas y validación

- show run router eigrp. Muestra la configuración EIGRP
- show run interface [ interface]. Muestra la información de temporizadores y autenticación de la interfaz EIGRP.
- show eigrp events [{ start end} | tipo]. Muestra el registro de eventos EIGRP.
- show eigrp interfaces [ if-name] [ detail]. Muestra las interfaces que participan en el ruteo EIGRP.

- show eigrp neighbors [ detail | static] [ if-name]. Muestra la tabla de vecinos EIGRP.
- show eigrp topology [ ip-addr [ mask] | activo | all-links | pendiente | summary | cero sucesores]. Muestra la tabla de topología EIGRP.
- show eigrp traffic. Muestra estadísticas de tráfico EIGRP.

## Verificación

Piense en la siguiente topología: esta sección utiliza los comandos descritos anteriormente para validar la configuración EIGRP aplicada al FTD.



Topología EIGRP

## Configuración Básica

# 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

Configuración básica de EIGRP

## Redistribución

### Edit Redistribution

---

#### 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  
 +

Configuración de redistribución de EIGRP

## Configuración de la interfaz

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

Configuración de interfaz EIGRP

## Validación mediante comandos

<#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 Un/Reliable	Mean SRTT	Pacing Time Un/Reliable	Multicast Flow Timer	Pending 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 (sec)	Uptime	SRTT (ms)	RTO	Q Cnt	Seq Num
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)
```

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).