Resolución de problemas de EIGRP en dispositivos FTD administrados por FMC

Contenido

Introducción

Este documento describe cómo verificar y resolver problemas de configuración EIGRP en FTD administrado por FMC.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Protocolo de routing de gateway interior mejorado (EIGRP)
- Cisco Secure Firewall Management Center (FMC)
- Cisco Secure Firewall Threat Defence (FTD)

Componentes Utilizados

- FTDv en la versión 7.4.2.
- FMCv en la versión 7.4.2.

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.

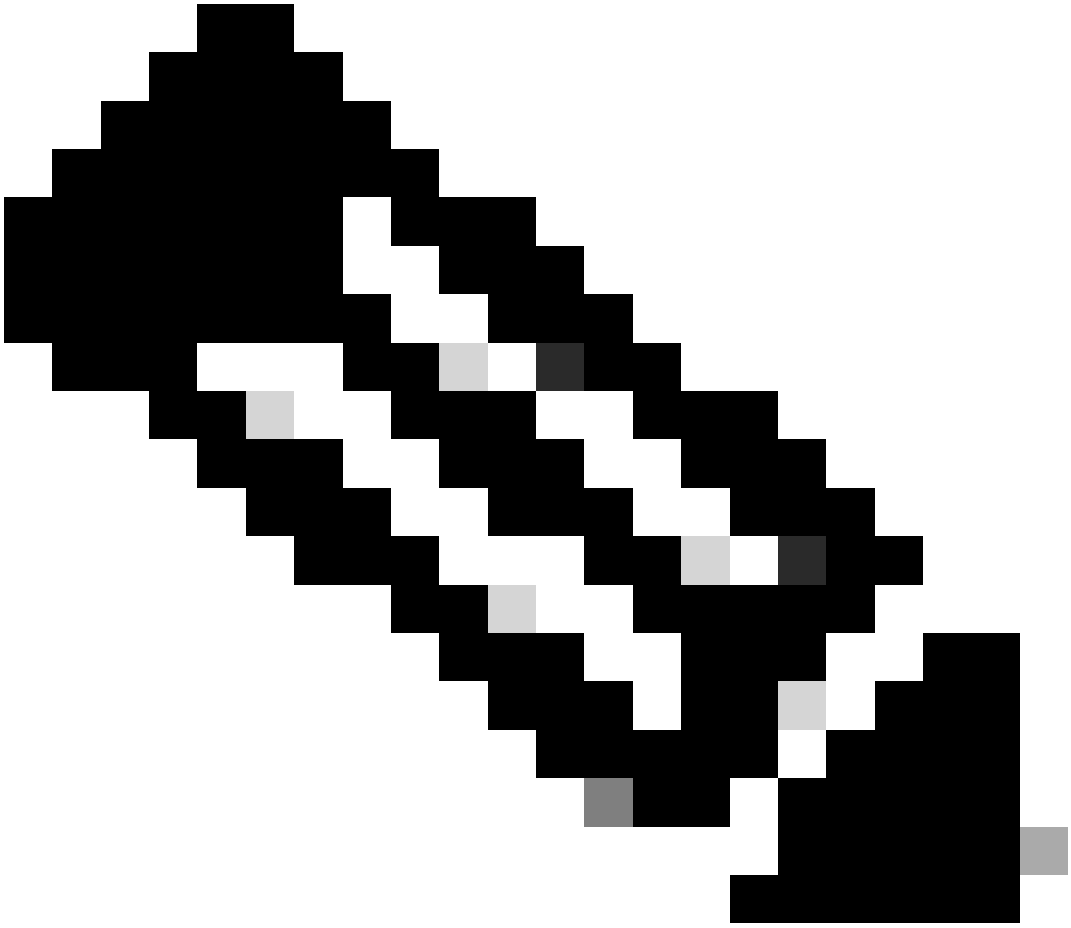
Antecedentes

EIGRP es un protocolo de ruteo de vector de distancia avanzado que combina características de los protocolos de vector de distancia y de estado de link. Ofrece una convergencia rápida al mantener la información de ruteo de los vecinos, lo que permite una adaptación rápida a las rutas alternativas. EIGRP es eficiente, ya que utiliza actualizaciones parciales activadas para cambios de ruta o métrica en lugar de actualizaciones completas periódicas. Para la comunicación, EIGRP opera directamente en la capa IP (protocolo 88) y utiliza el protocolo de transporte confiable (RTP) para garantizar la entrega de paquetes ordenados. Admite tanto multidifusión como unidifusión, con mensajes de saludo que utilizan específicamente las direcciones de multidifusión 224.0.0.10 o FF02::A.
La operación EIGRP se basa fundamentalmente en la información almacenada en tres tablas:

- Tabla de vecino: Esta tabla mantiene un registro de los dispositivos EIGRP conectados directamente con los que se ha establecido correctamente una adyacencia.
- Tabla de topología: Esta tabla almacena todas las rutas aprendidas anunciadas por los vecinos, incluidas todas las rutas factibles a un destino específico y sus métricas asociadas, lo que permite una evaluación de su calidad y el número de rutas disponibles.
- Tabla de ruteo: Esta tabla contiene la mejor ruta para cada destino, conocida como 'Sucesor'. Esta ruta sucesora es la que se utiliza activamente para reenviar tráfico y, posteriormente, se anuncia a otros vecinos EIGRP.

EIGRP utiliza los pesos de métrica, conocidos como valores K, en el ruteo y los cálculos de métrica para determinar la trayectoria óptima a un destino. Este valor de métrica se deriva de una fórmula que utiliza parámetros:

- Ancho de banda
- Tiempo de retraso
- Confiabilidad
- Carga
- MTU (unidad de transmisión básica)



Nota: En el caso de un tiempo de métrica entre varias trayectorias, se utiliza la Unidad de transmisión máxima (MTU) como un desempate, prefiriéndose un valor de MTU más alto.

- Ruta sucesora: Se define como la mejor ruta a un destino específico. Es la ruta que se instala en última instancia en la tabla de ruteo.
- Distancia factible (FD): Representa la métrica mejor calculada para alcanzar una subred determinada desde la perspectiva del router local.
- Distancia notificada (RD)/distancia anunciada (AD): Esta es la distancia (métrica) a una subred específica según lo informado por un vecino. Para que una trayectoria se considere un sucesor factible, la Distancia informada del vecino debe ser menor que la Distancia factible del router local a ese mismo destino.
- Sucesor factible (FS): Esta es una trayectoria de respaldo a un destino, proporcionando una ruta alternativa en caso de que la ruta sucesora principal falle. Una trayectoria se califica

como sucesora factible si su distancia informada (desde el vecino anunciante) es estrictamente menor que la distancia factible de la ruta sucesora actual al mismo destino.

Diagrama de la red

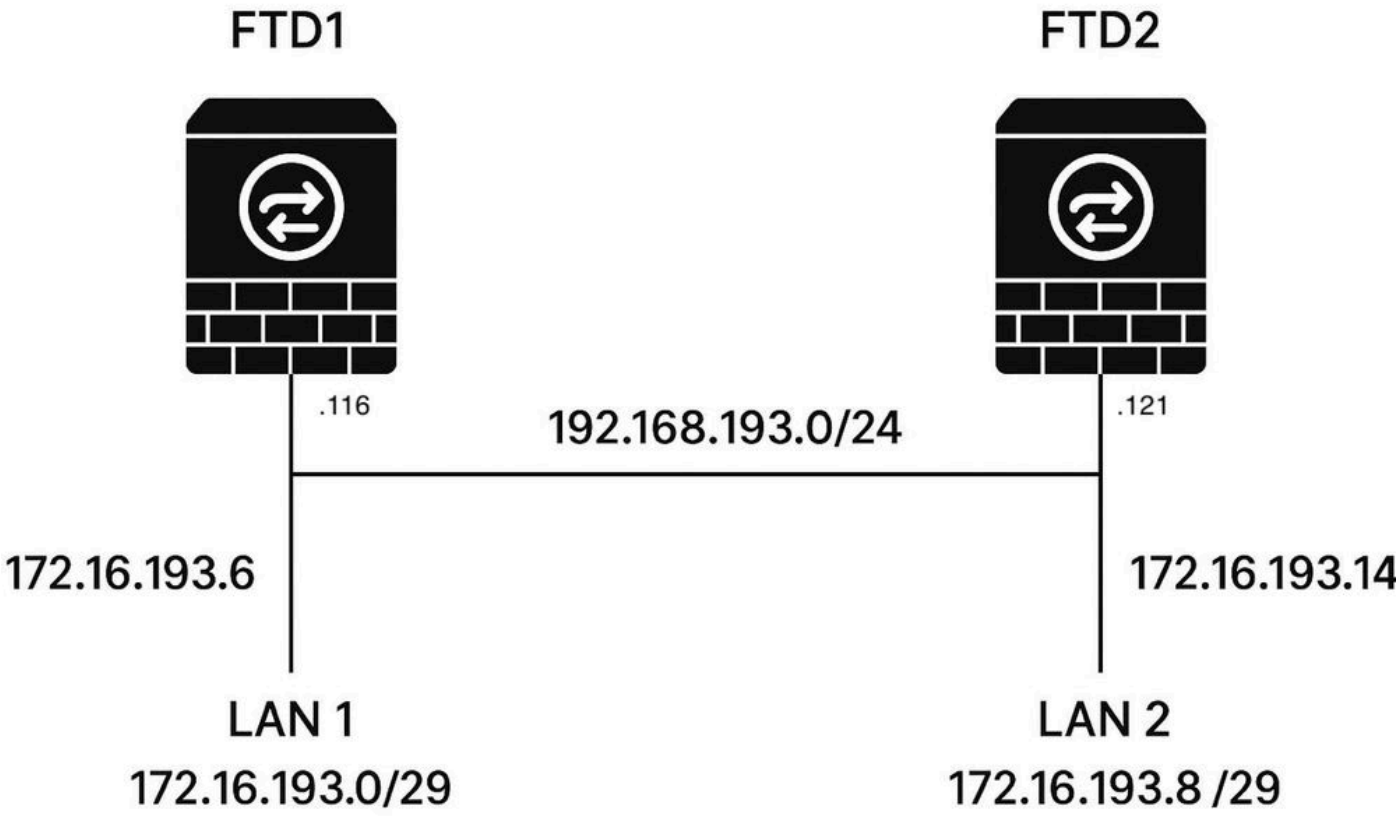
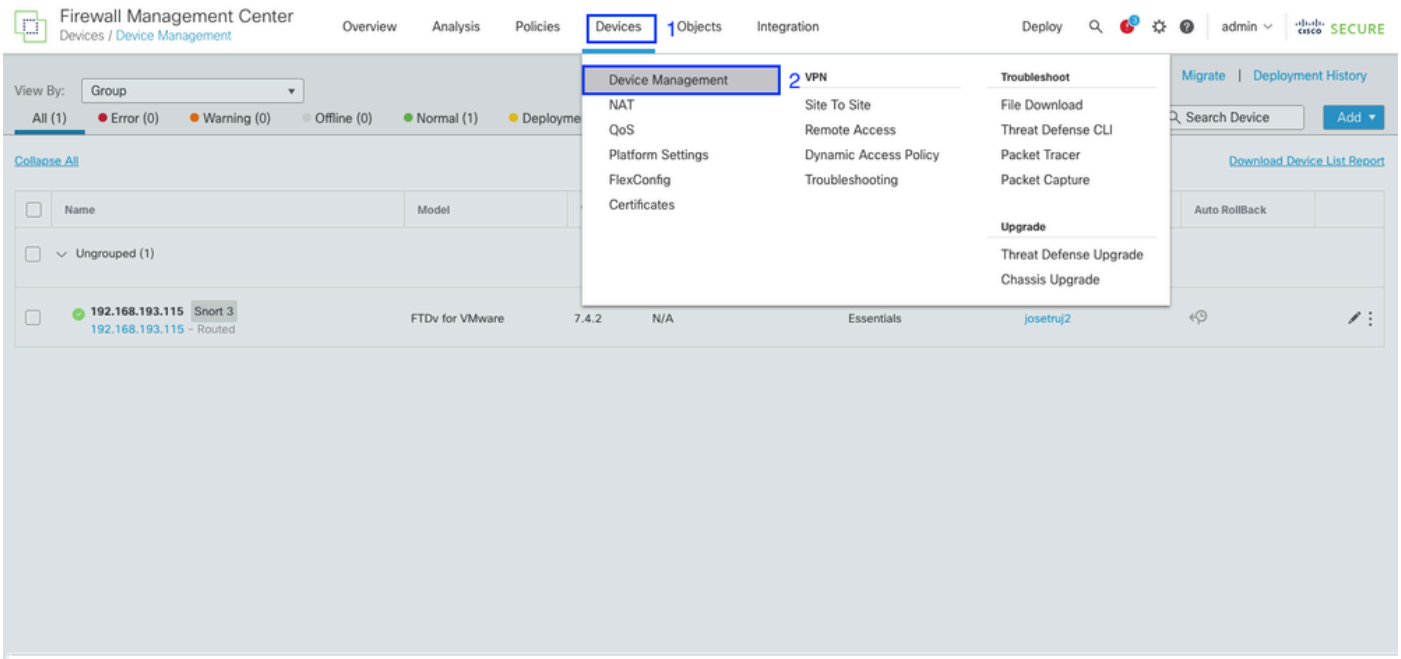


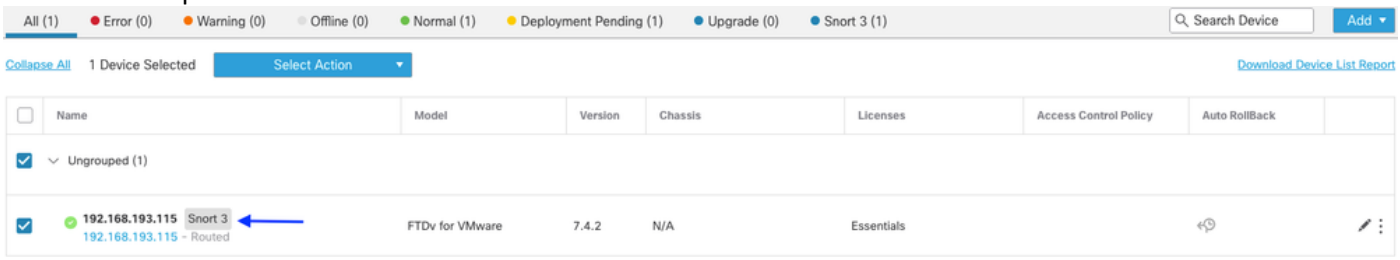
Diagrama de la red

Configuración Básica

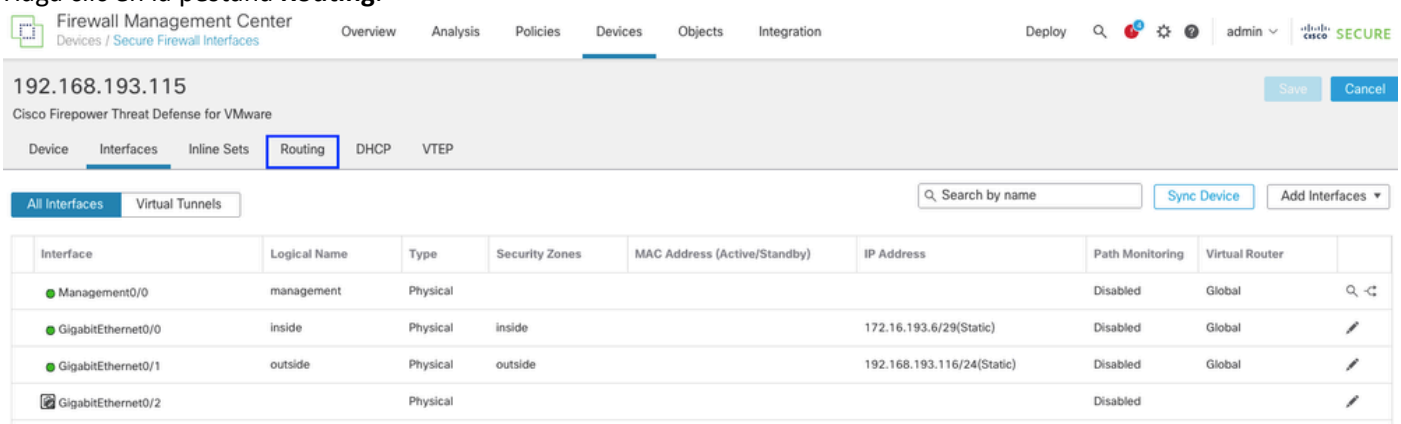
Vaya a **Devices > Device Management**:



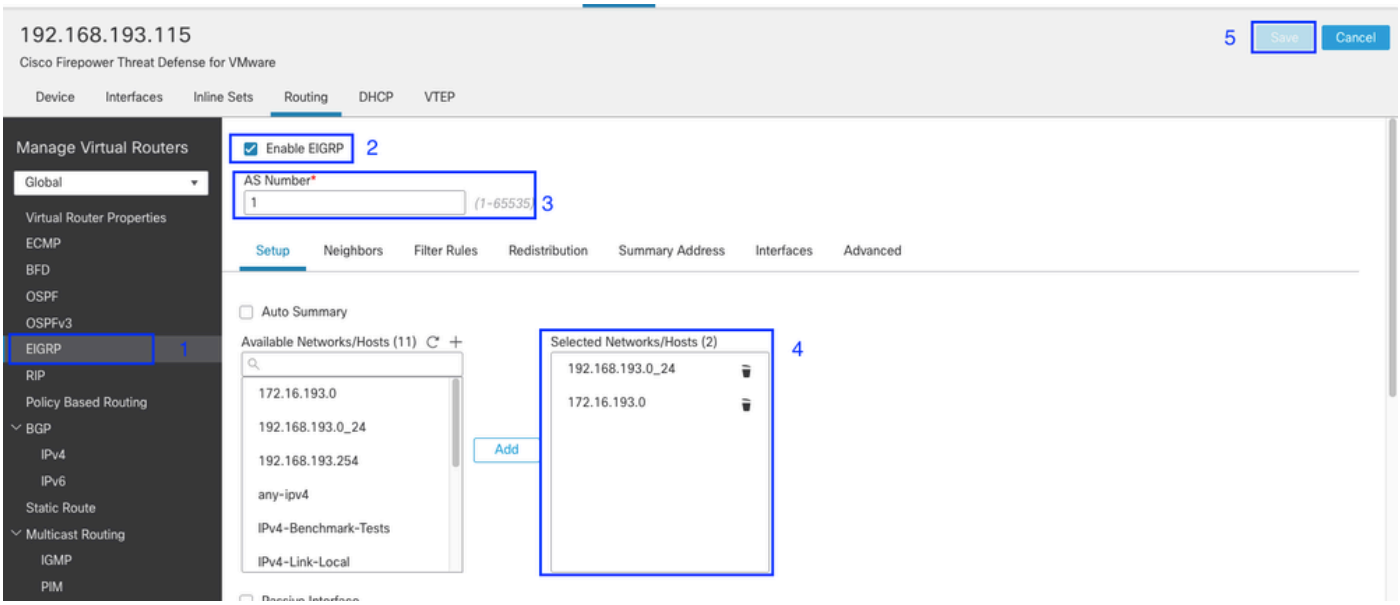
Seleccionar dispositivo:



Haga clic en la pestaña **Routing**.



Haga clic en **EIGRP** en el menú de la izquierda.
Haga clic en **Enable EIGRP**.
Asigne el **número AS** (1-65535).
Seleccione una **red/host**. Puede seleccionar un objeto creado anteriormente de la lista 'Red disponible/Host' o puede crear un nuevo objeto haciendo clic en el botón más (**+**).
Click Save.



Validación

Estos son los requisitos mínimos para la adyacencia de vecino EIGRP:

- El número AS debe coincidir.
- La interfaz debe estar activa y ser accesible.
- Como práctica recomendada, los temporizadores Hello y Hold deben coincidir.
- Los valores K deben coincidir.
- Ninguna lista de acceso debe estar bloqueando el tráfico EIGRP.

Validación con CLI

- show run router eigrp
- show eigrp neighbors
- show eigrp topology
- show eigrp interfaces
- show route eigrp
- show eigrp traffic
- debug ip eigrp neighbor
- debug eigrp packets

firepower# show run router eigrp

router eigrp 1

no default-information in

no default-information out

no eigrp log-neighbor-warnings

no eigrp log-neighbor-changes

network 192.168.193.0 255.255.255.0

```
 network 172.16.193.8 255.255.255.248
firepower#
firepower# show eigrp neighbors
Vecinos EIGRP-IPv4 para AS(1)
H Address Interface Hold Uptime SRTT RTO Q Seq
                                   (s) (ms) núm. cnt
0 192.168.193.121 fuera de 14 21:45:04 40 240 0 30
firepower# show eigrp topology
Tabla de Topología EIGRP-IPv4 para AS(1)/ID(192.168.193.121)
Códigos: P - Pasivo, A - Activo, U - Actualización, Q - Consulta, R - Respuesta,
       r - responder Estado, s - sia Estado
P 192.168.193.0 255.255.255.0, 1 sucesores, FD es 512
        vía Connected, outside
P 172.16.193.0 255.255.255.248, 1 sucesores, FD es 768
        vía 192.168.193.116 (768/512), fuera
P 172.16.193.8 255.255.255.248, 1 sucesores, FD es 512
        vía Connected, inside
firepower# show eigrp interfaces
Interfaces EIGRP-IPv4 para AS(1)
                    Tiempo Medio de Ritmo de Cola de Xmit Multicast Pendiente
Pares de Interfaz No Funcionados/Fiables SRTT No Funcionados/Fiables Flow Timer Routes
outside 1 0 / 0 10 0 / 1 50 0
Inside 0 0 / 0 0 0 / 1 0 0
firepower#

firepower# show route eigrp
Códigos: L - local, C - conectado, S - estático, R - RIP, M - móvil, B - BGP
```

D - EIGRP, EX - EIGRP externo, O - OSPF, IA - OSPF entre áreas

N1 - OSPF NSSA externo tipo 1, N2 - OSPF NSSA externo tipo 2

E1 - OSPF tipo externo 1, E2 - OSPF tipo externo 2, V - VPN

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

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

o - ODR, P - ruta estática descargada periódicamente, + - ruta replicada

SI - InterVRF estático, BI - InterVRF BGP

El gateway de último recurso es 192.168.193.254 a la red 0.0.0.0

D 172.16.193.0 255.255.255.248

[90/768] vía 192.168.193.116, 02:32:58, afuera

firepower# show route

Códigos: L - local, C - conectado, S - estático, R - RIP, M - móvil, B - BGP

D - EIGRP, EX - EIGRP externo, O - OSPF, IA - OSPF entre áreas

N1 - OSPF NSSA externo tipo 1, N2 - OSPF NSSA externo tipo 2

E1 - OSPF tipo externo 1, E2 - OSPF tipo externo 2, V - VPN

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

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

o - ODR, P - ruta estática descargada periódicamente, + - ruta replicada

SI - InterVRF estático, BI - InterVRF BGP

El gateway de último recurso es 192.168.193.254 a la red 0.0.0.0

S* 0.0.0.0 0.0.0.0 [1/0] vía 192.168.193.254, fuera

D 172.16.193.0 255.255.255.248

[90/768] vía 192.168.193.116, 02:33:41, afuera

C 172.16.193.8 255.255.255.248 está conectado directamente, dentro

L 172.16.193.14 255.255.255.255 está conectado directamente, dentro

C 192.168.193.0 255.255.255.0 está conectado directamente, fuera

L 192.168.193.121 255.255.255.255 está conectado directamente, fuera

```
firepower#

firepower# show eigrp traffic

Estadísticas de tráfico EIGRP-IPv4 para AS(1)

  Saludos enviados/recibidos: 4006/4001

  Actualizaciones enviadas/recibidas: 4/4

  Consultas enviadas/recibidas: 0/0

  Respuestas enviadas/recibidas: 0/0

  Acks enviados/recibidos: 3/2

  Consultas SIA enviadas/recibidas: 0/0

  Respuestas SIA enviadas/recibidas: 0/0

  ID de proceso Hello: 2503149568

  ID de proceso de PDM: 2503150496

  Cola de socket:

  Cola de entrada: 0/2000/2/0 (actual/máx./máximo/caídas)

firepower#
```

Troubleshoot

Escenario 1 - Debug IP EIGRP Neighbor

Los comandos de depuración se pueden utilizar para observar cualquier cambio en los estados vecinos.

```
firepower# debug ip eigrp neighbor

firepower#

EIGRP: Tiempo en espera vencido

Bajando: Peer 192.168.193.121 total=0 stub 0, iidb-stub=0 iid-all=0

EIGRP: Controlar error de desasignación [0]

EIGRP: El vecino 192.168.193.121 cayó afuera
```

Ejecute el comando show eigrp neighbors para validar el estado de vecino entre los FTD.

firepower# show eigrp neighbors

Vecinos EIGRP-IPv4 para AS(1)

Verifique el estado de las interfaces mediante el comando show interface ip brief. Puede observar que la interfaz GigabitEthernet0/1 está administrativamente inactiva.

firepower# show interface ip brief

¿Interfaz IP-Address OK? Protocolo de estado de método

GigabitEthernet0/0 172.16.193.14 SÍ CONFIG up up

GigabitEthernet0/1 192.168.193.121 SÍ CONFIG administrativamente inactivo

GigabitEthernet0/2 192.168.194.24 SÍ manual arriba

Internal-Control0/0 127.0.1.1 YES unset up

Internal-Control0/1 unassign YES unset up

Internal-Data0/0 unassign YES unset down up

Internal-Data0/0 unassign YES unset up

Internal-Data0/1 169.254.1.1 SÍ desconfigurado

Internal-Data0/2 unassign YES unset up

Management0/0 203.0.113.130 SÍ desconfigurado

Situación 2: autenticación

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

Para habilitar el algoritmo hash MD5, marque la casilla de verificación 'Autenticación MD5'. Es crucial que la configuración de autenticación coincida en ambos dispositivos; si se habilita en un dispositivo pero no en el otro, no se puede formar adyacencia de vecino entre ellos.

Verifique esta configuración mediante debug eigrp packets.

firepower# debug eigrp packets

(UPDATE, REQUEST, QUERY, REPLY, HELLO, IPXSAP, PROBE, ACK, STUB, SIAQUERY, SIAREPLY)La depuración de paquetes EIGRP está activada

firepower#

EIGRP: fuera: paquete ignorado de 192.168.193.121, opcode = 5 (falta autenticación o key chain)

EIGRP: HELLO recibido en el exterior nbr 172.16.193.14

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

EIGRP: Enviando SALUDO desde fuera

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

EIGRP: Enviando SALUDO desde dentro

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

EIGRP: fuera: paquete ignorado de 192.168.193.121, opcode = 5 (falta autenticación o key chain)

EIGRP: HELLO recibido en el exterior nbr 172.16.193.14

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

EIGRP: Enviando SALUDO desde dentro

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

EIGRP: Enviando SALUDO desde fuera

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

EIGRP: fuera: paquete ignorado de 192.168.193.121, opcode = 5 (falta autenticación o key chain).

Puede observar un mensaje que indica que la autenticación está desactivada o que falta la cadena de claves. En este escenario, esto ocurre típicamente cuando la autenticación está habilitada en un par pero no en el otro.

EIGRP: fuera: paquete ignorado de 192.168.193.121, opcode = 5 (falta autenticación o key chain).

Verifique con show run interface <interfaz EIGRP>.

Firepower1# show run interface GigabitEthernet0/1

!

interface GigabitEthernet0/1

nameif outside

security-level 0

ip address 192.168.193.121 255.255.255.0

authentication key eigrp 1 ***** key-id 10

authentication mode eigrp 1 md5

Firepower2# show run interface GigabitEthernet0/1

!

interface GigabitEthernet0/1

 nameif outside

 security-level 0

 ip address 192.168.193.116 255.255.255.0

Situación 3: interfaces pasivas

Cuando se configura EIGRP, los paquetes hello de EIGRP se envían y reciben generalmente en las interfaces donde la red está habilitada.

Sin embargo, si una interfaz se configura como pasiva, EIGRP suprime el intercambio de paquetes de saludo entre dos routers en esa interfaz, lo que resulta en la pérdida de adyacencia de vecinos. En consecuencia, esta acción no sólo evita que el router anuncie actualizaciones de ruteo fuera de esa interfaz, sino que también impide que reciba actualizaciones de ruteo desde esa interfaz.

Ejecute el comando show eigrp neighbors para validar el estado de vecino entre los FTD.

firepower# show eigrp neighbors

Vecinos EIGRP-IPv4 para AS(1)

Puede verificar los paquetes EIGRP que se envían y las interfaces a través de las cuales se envían mediante el comando debug eigrp packets.

FTD 1

Firepower1#

    (UPDATE, REQUEST, QUERY, REPLY, HELLO, IPXSAP, PROBE, ACK, STUB, SIAQUERY, SIAREPLY)La depuración de paquetes EIGRP está activada

firepower#

EIGRP: Enviando SALUDO desde fuera

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

EIGRP: Enviando SALUDO desde dentro

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

EIGRP: Enviando SALUDO desde fuera

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

EIGRP: Enviando SALUDO desde dentro

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

EIGRP: Enviando SALUDO desde fuera

FTD 2

Firepower2# debug eigrp packets

(UPDATE, REQUEST, QUERY, REPLY, HELLO, IPXSAP, PROBE, ACK, STUB, SIAQUERY, SIAREPLY)La depuración de paquetes EIGRP está activada

Firepower2#

En esta situación, FTD 2 no envía mensajes hello de EIGRP porque sus interfaces interna y externa están configuradas como pasivas. Verifique esto con el comando show run router eigrp.

Firepower2# show run router eigrp

router eigrp 1

no default-information in

no default-information out

no eigrp log-neighbor-warnings

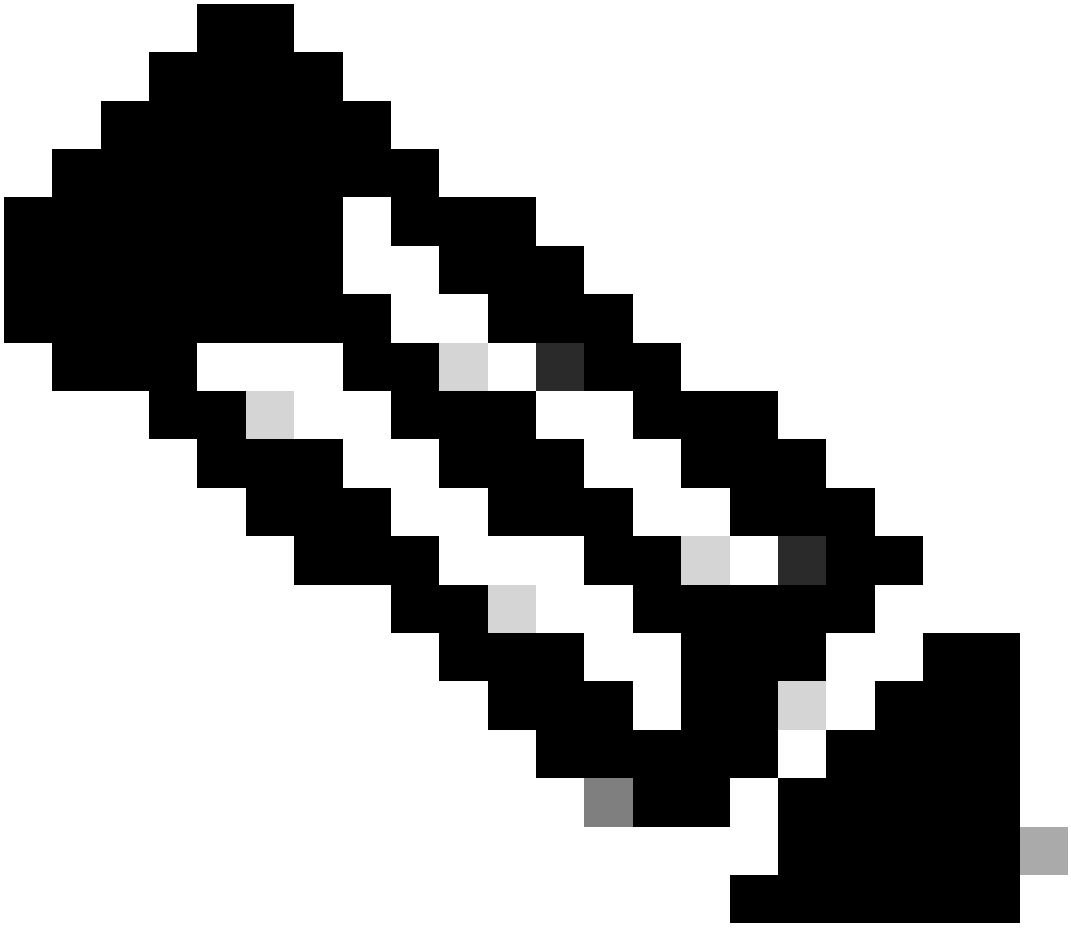
no eigrp log-neighbor-changes

network 192.168.193.0 255.255.255.0

network 172.16.193.8 255.255.255.248

passive-interface outside

passive-interface inside



Nota: Para detener todos los procesos de depuración configurados, utilice el comando undebug all.

Información Relacionada

- EIGRP en dispositivos FTD
- Configuración de EIGRP en FTD
- Métricas de Costes Compuestos EIGRP

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).