Identificar e Solucionar Problemas do EIGRP em Dispositivos FTD Gerenciados pelo FMC

Contents

Introdução

Este documento descreve como verificar e solucionar problemas de configuração do EIGRP no FTD gerenciado pelo FMC.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Enhanced Interior Gateway Routing Protocol (EIGRP)
- Cisco Secure Firewall Management Center (FMC)
- Defesa contra ameaças (FTD) do Cisco Secure Firewall

Componentes Utilizados

- FTDv na versão 7.4.2.
- CVP na versão 7.4.2.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma

configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

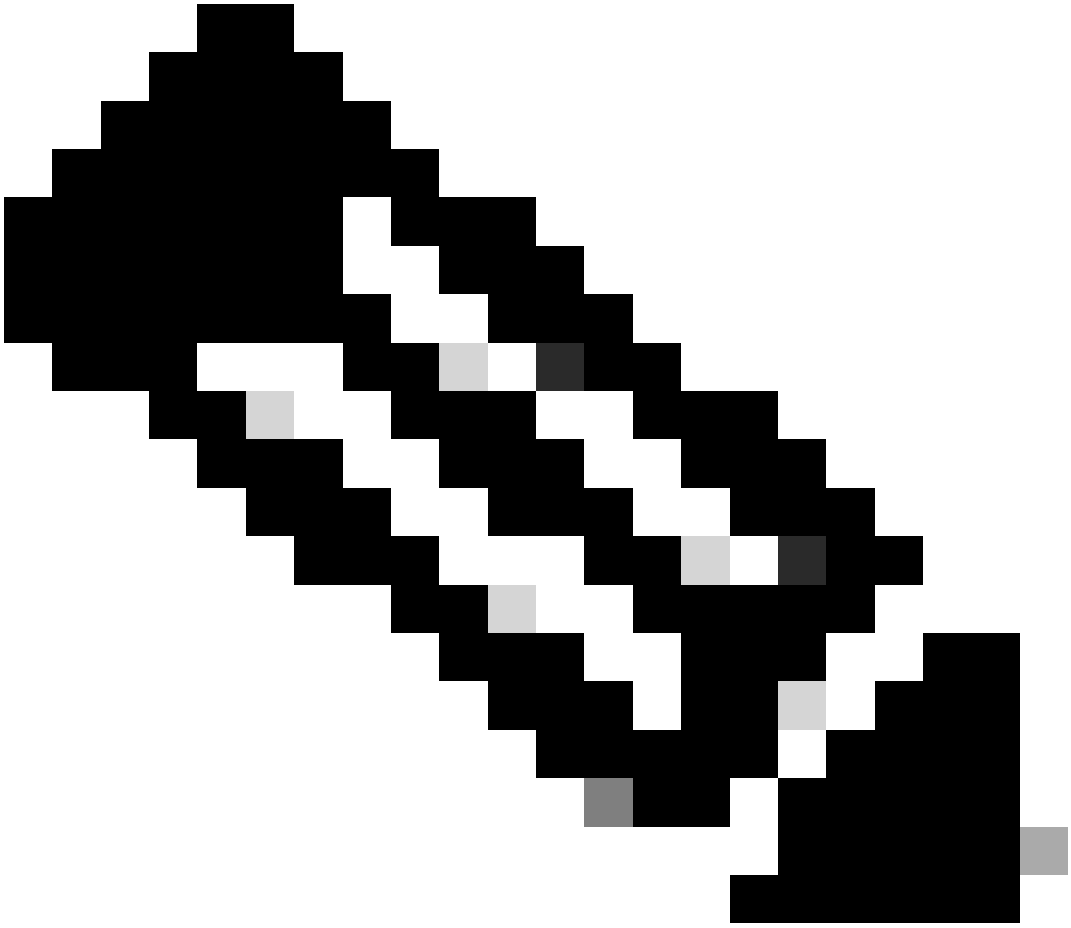
Informações de Apoio

O EIGRP é um protocolo de roteamento de vetor de distância avançado que combina recursos de protocolos de vetor de distância e de link-state. Ele oferece convergência rápida mantendo informações de roteamento dos vizinhos, permitindo uma rápida adaptação a rotas alternativas. O EIGRP é eficiente, utilizando atualizações parciais e acionadas para alterações de rota ou métrica em vez de atualizações completas periódicas.
Para comunicação, o EIGRP opera diretamente na camada IP (Protocolo 88) e usa o Protocolo de Transporte Confiável (RTP) para a entrega garantida e ordenada de pacotes. Ele suporta multicast e unicast, com mensagens hello usando especificamente endereços multicast 224.0.0.10 ou FF02::A.
A operação do EIGRP é fundamentalmente baseada nas informações armazenadas em três tabelas:

- Tabela de vizinhos: Esta tabela mantém um registro dos dispositivos EIGRP diretamente conectados com os quais uma adjacência foi estabelecida com êxito.
- Tabela de topologias: Esta tabela armazena todas as rotas aprendidas anunciadas pelos vizinhos, incluindo todos os caminhos viáveis para um destino específico e suas métricas associadas, permitindo uma avaliação de sua qualidade e o número de caminhos disponíveis.
- Routing Table: Esta tabela contém o melhor caminho para cada destino, conhecido como 'Sucessor'. Essa rota Sucessora é a usada ativamente para encaminhar o tráfego e é anunciada subsequentemente a outros vizinhos EIGRP.

O EIGRP usa pesos de métrica, conhecidos como valores K, em roteamento e cálculos de métrica para determinar o caminho ideal para um destino. Este valor de métrica é derivado de uma fórmula que utiliza parâmetros:

- Largura de banda
- Tempo de atraso
- Confiabilidade
- Carregando
- MTU



Note: No caso de um empate métrico entre vários caminhos, a Unidade Máxima de Transmissão (MTU) é usada como um desempate, com um valor de MTU mais alto sendo preferido.

- Rota sucessora: Isso é definido como o melhor caminho para um destino específico. É a rota que é finalmente instalada na tabela de roteamento.
- Distância Viável (FD): Isso representa a melhor métrica calculada para acessar uma sub-rede específica da perspectiva do roteador local.
- Distância Relatada (RD) / Distância Anunciada (AD): Esta é a distância (métrica) para uma sub-rede específica conforme relatada por um vizinho. Para que um caminho seja considerado um sucessor viável, a distância relatada do vizinho deve ser menor que a distância viável do roteador local para esse mesmo destino.
- Sucessor Viável (FS): Esse é um caminho de backup para um destino, fornecendo uma rota alternativa caso a Rota Sucessora principal falhe. Um caminho se qualifica como Sucessor

Viável se sua Distância Relatada (do vizinho do anúncio) for estritamente menor que a Distância Viável da Rota Sucessora atual para o mesmo destino.

Diagrama de Rede

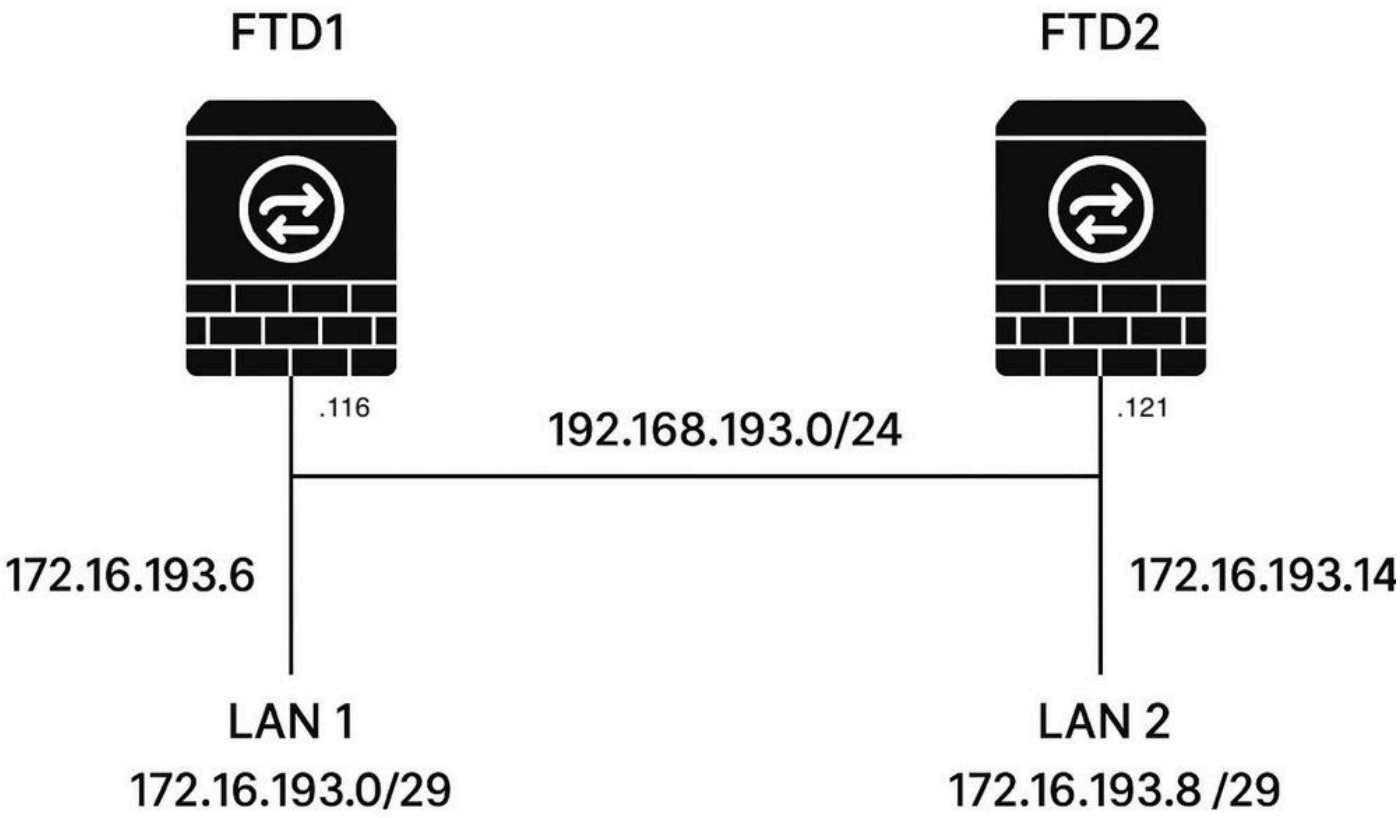
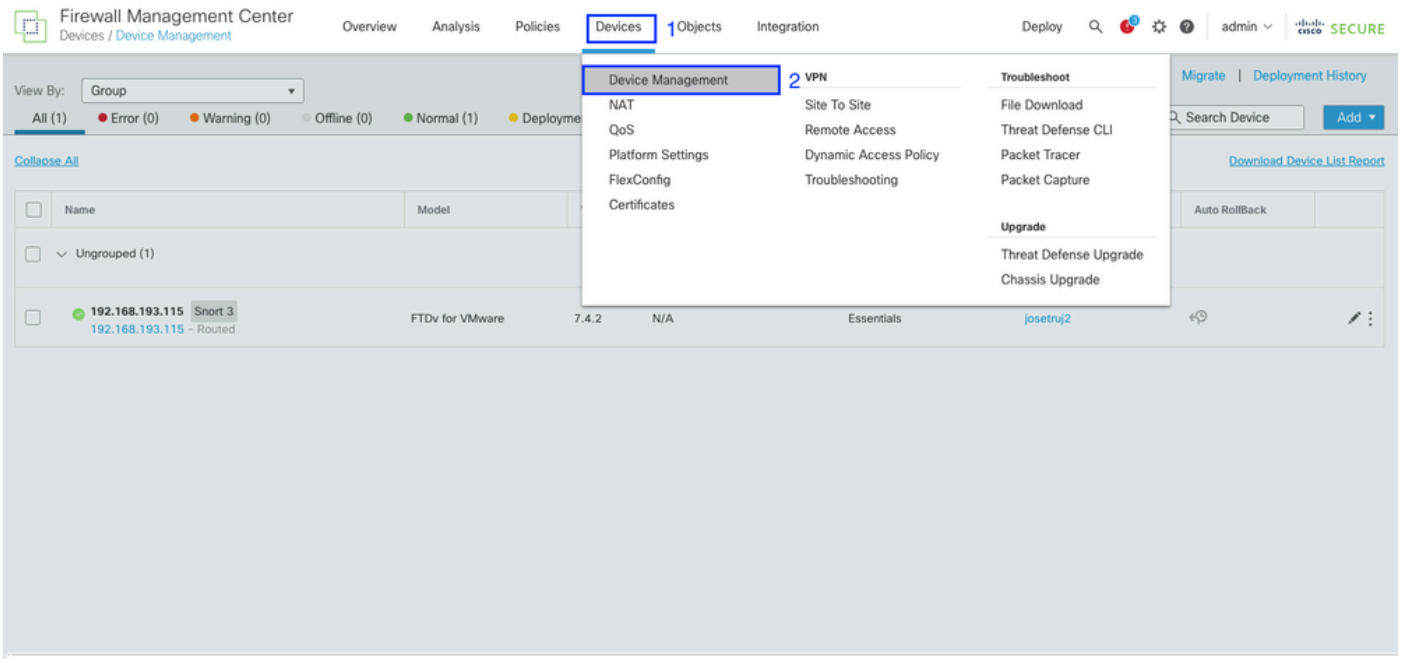


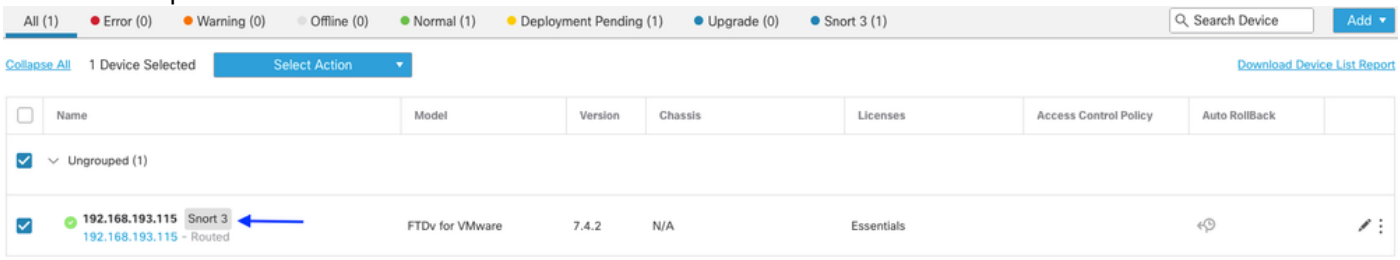
Diagrama de Rede

Configuração básica

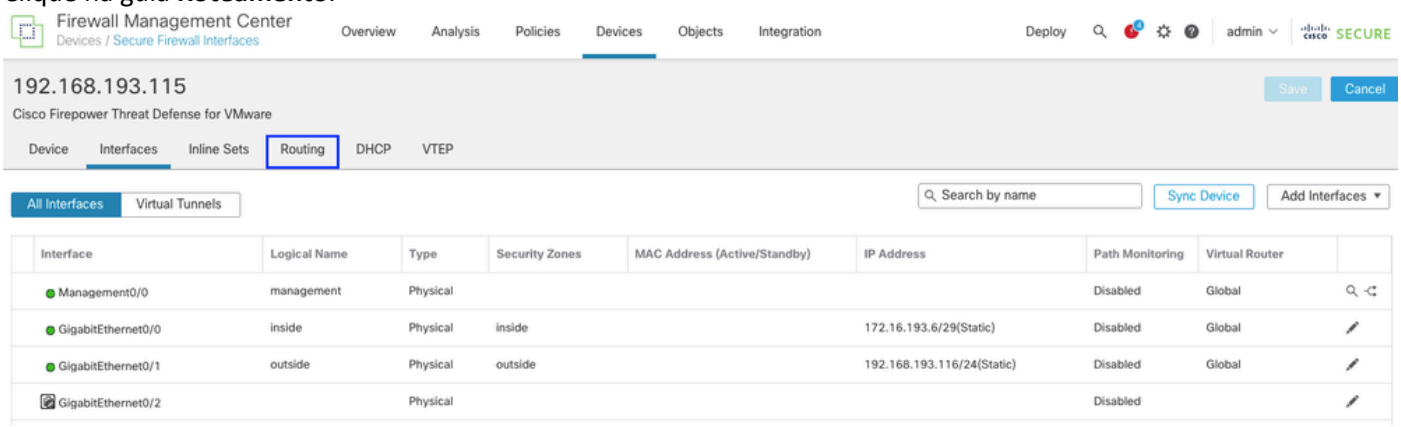
Navegue até **Devices > Device Management**:



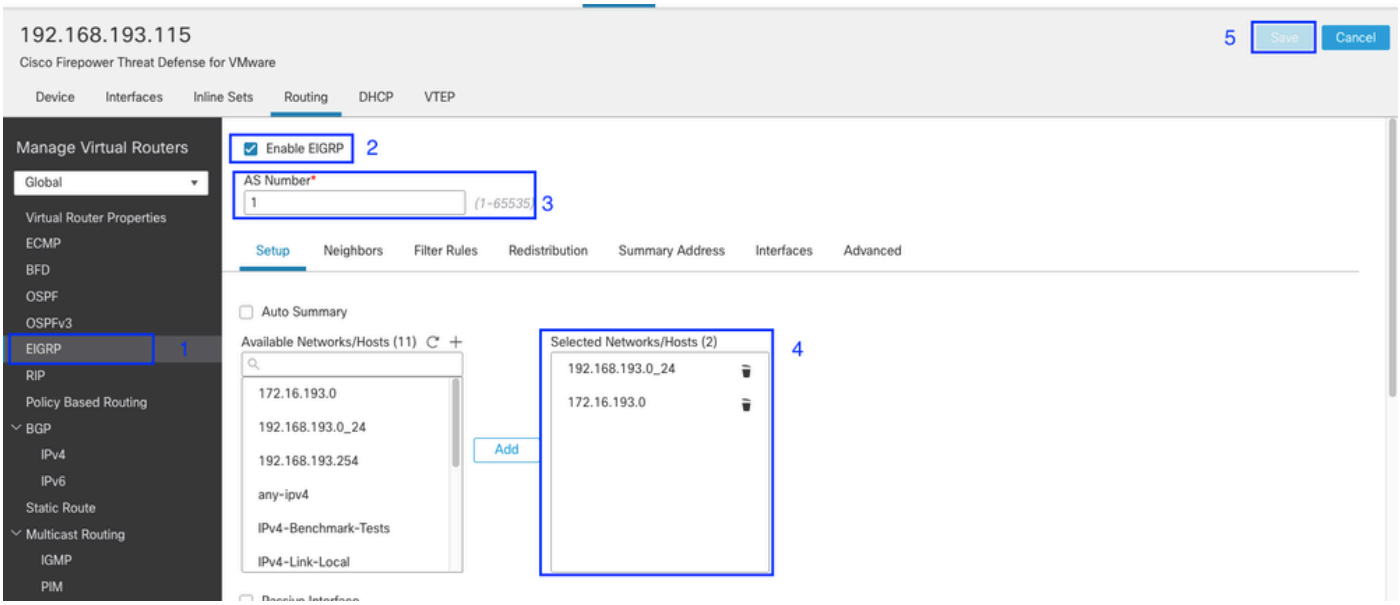
Selecionar dispositivo:



Clique na guia **Roteamento**.



Clique em **EIGRP** no menu esquerdo.
Clique em **Ativar EIGRP**.
Atribua o **número AS** (1-65535).
Selecione uma **rede/host**. Você pode selecionar um objeto criado anteriormente na lista 'Rede disponível/Host' ou pode criar um novo objeto clicando no botão de adição (**+**).
Click Save.



Validação

Estes são os requisitos mínimos para a adjacência de vizinhos EIGRP:

- O número AS deve corresponder.
- A interface deve estar ativa e acessível.
- Como prática recomendada, os temporizadores de Hello e de Hold devem ser correspondentes.
- Os valores K devem corresponder.
- Nenhuma lista de acesso deve bloquear o tráfego do EIGRP.

Validação usando 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

```
 rede 192.168.193.0 255.255.255.0
 rede 172.16.193.8 255.255.255.248
firepower#
firepower#show eigrp neighbors
Vizinhos EIGRP-IPv4 para AS(1)
H Address Interface Hold Uptime SRTT RTO Q Seq
                                   (seg) (ms) Núm. Contagem
0 192.168.193.121 externo 14 21:45:04 40 240 0 30
firepower#show eigrp topology
Tabela de Topologia EIGRP-IPv4 para AS(1)/ID(192.168.193.121)
Códigos: P - Passivo, A - Ativo, U - Atualização, Q - Consulta, R - Resposta,
       r - status da resposta, s - status da sia
P 192.168.193.0 255.255.255.0, 1 sucessor, FD é 512
        via Conectado, externo
P 172.16.193.0 255.255.255.248, 1 sucessor, FD é 768
        via 192.168.193.116 (768/512), fora
P 172.16.193.8 255.255.255.248, 1 sucessor, FD é 512
        via Conectado, interno
firepower#show eigrp interfaces
Interfaces EIGRP-IPv4 para AS(1)
                        Tempo Médio de Ritmo da Fila de Envio Multicast Pendente
Parceiros de interface Un/Confiável SRTT Un/Confiável Rotas de temporizador de fluxo
fora 1 0 / 0 10 0 / 1 50 0
dentro de 0 0 / 0 0 / 1 0 0
firepower#

firepower#show route eigrp
```

Códigos: L - local, C - conectado, S - estático, R - RIP, M - móvel, 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 - resumo IS-IS, L1 - IS-IS nível 1, L2 - IS-IS nível 2

ia - IS-IS inter-área, * - candidato padrão, U - rota estática por usuário

o - ODR, P - rota estática baixada periodicamente, + - rota replicada

SI - InterVRF estático, BI - BGP InterVRF

O gateway de último recurso é 192.168.193.254 para a rede 0.0.0.0

D 172.16.193.0 255.255.255.248

[90/768] via 192.168.193.116, 02:32:58, externo

firepower# show route

Códigos: L - local, C - conectado, S - estático, R - RIP, M - móvel, 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 - resumo IS-IS, L1 - IS-IS nível 1, L2 - IS-IS nível 2

ia - IS-IS inter-área, * - candidato padrão, U - rota estática por usuário

o - ODR, P - rota estática baixada periodicamente, + - rota replicada

SI - InterVRF estático, BI - BGP InterVRF

O gateway de último recurso é 192.168.193.254 para a rede 0.0.0.0

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

D 172.16.193.0 255.255.255.248

[90/768] via 192.168.193.116, 02:33:41, externo

C 172.16.193.8 255.255.255.248 está conectado diretamente, dentro

A L 172.16.193.14 255.255.255.255 está diretamente conectada, dentro

C 192.168.193.0 255.255.255.0 está conectado diretamente, fora

A L 192.168.193.121 255.255.255.255 está diretamente conectada, fora

firepower#

firepower#show eigrp traffic

Estatísticas de Tráfego EIGRP-IPv4 para AS(1)

  Hellos enviados/recebidos: 4006/4001

  Atualizações enviadas/recebidas: 4/4

  Consultas enviadas/recebidas: 0/0

  Respostas enviadas/recebidas: 0/0

  Confirmações enviadas/recebidas: 3/2

  Consultas SIA enviadas/recebidas: 0/0

  Respostas SIA enviadas/recebidas: 0/0

  ID do processo Hello: 2503149568

  ID do processo PDM: 2503150496

  Fila de soquetes:

  Fila de entrada: 0/2000/2/0 (atual/máx/mais alta/quedas)

firepower#

Troubleshooting

Cenário 1 - Depurar Vizinho EIGRP IP

Os comandos debug podem ser utilizados para observar qualquer alteração nos estados dos vizinhos.

firepower#debug ip eigrp neighbor

firepower#

EIGRP: Tempo de espera expirado

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

EIGRP: Falha de desalocação de tratamento [0]

EIGRP: O vizinho 192.168.193.121 foi desativado na parte externa

Execute o comando show eigrp neighbors para validar o status do vizinho entre os FTDs.

firepower#show eigrp neighbors

Vizinhos EIGRP-IPv4 para AS(1)

Verifique o status das interfaces usando o comando show interface ip brief. Você pode observar que a interface GigabitEthernet0/1 está administrativamente inoperante.

firepower#show interface ip brief

Interface IP-Address OK? Method Status Protocol

GigabitEthernet0/0 172.16.193.14 SIM CONFIG up up

GigabitEthernet0/1 192.168.193.121 SIM CONFIG administrativamente desativado

GigabitEthernet0/2 192.168.194.24 SIM manual para cima

Internal-Control0/0 127.0.1.1 YES unset up

Internal-Control0/1 não atribuído SIM não configurado

Internal-Data0/0 não atribuído YES unset up up

Internal-Data0/0 não atribuído SIM não configurado

Internal-Data0/1 169.254.1.1 YES unset up

Internal-Data0/2 não atribuído SIM não configurado

Management0/0 203.0.113.130 YES unset up

Cenário 2 - Autenticação

O FTD suporta o algoritmo de hash MD5 para autenticar pacotes EIGRP. Por padrão, essa autenticação está desabilitada.

Para ativar o algoritmo de hash MD5, marque a caixa de seleção 'MD5 Authentication'. É crucial que as configurações de autenticação correspondam em ambos os dispositivos; se habilitada em um dispositivo, mas não no outro, a adjacência vizinha não pode se formar entre eles.

Verifique essa configuração usando debug eigrp packets.

firepower#debug eigrp packets

(UPDATE, REQUEST, QUERY, REPLY, HELLO, IPXSAP, PROBE, ACK, STUB, SIAQUERY, SIAREPLY)A depuração do pacote EIGRP está ativada

firepower#

EIGRP: externa: pacote ignorado de 192.168.193.121, opcode = 5 (autenticação desativada ou cadeia de chaves ausente)

EIGRP: HELLO recebido no número externo 172.16.193.14

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

EIGRP: Enviando HELLO para fora

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

EIGRP: Enviando HELLO por dentro

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

EIGRP: externa: pacote ignorado de 192.168.193.121, opcode = 5 (autenticação desativada ou cadeia de chaves ausente)

EIGRP: HELLO recebido no número externo 172.16.193.14

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

EIGRP: Enviando HELLO por dentro

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

EIGRP: Enviando HELLO para fora

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

EIGRP: externa: pacote ignorado de 192.168.193.121, opcode = 5 (autenticação desativada ou cadeia de chaves ausente).

Você pode observar uma mensagem indicando que a autenticação está desativada ou que a cadeia de chaves está ausente. Neste cenário, isso geralmente ocorre quando a autenticação é habilitada em um peer, mas não no outro.

EIGRP: externa: pacote ignorado de 192.168.193.121, opcode = 5 (autenticação desativada ou cadeia de chaves ausente).

Verifique com show run interface <EIGRP interface>.

Firepower1#show run interface GigabitEthernet0/1

!

interface GigabitEthernet0/1

nameif externo

nível de segurança 0

ip address 192.168.193.121 255.255.255.0

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

modo de autenticação eigrp 1 md5

Firepower2#show run interface GigabitEthernet0/1

!

interface GigabitEthernet0/1

nameif externo

nível de segurança 0

ip address 192.168.193.116 255.255.255.0

Cenário 3 - Interfaces passivas

Quando o EIGRP é configurado, os pacotes Hello do EIGRP são normalmente enviados e recebidos em interfaces onde a rede está habilitada.

No entanto, se uma interface for configurada como passiva, o EIGRP suprimirá a troca de pacotes hello entre dois roteadores nessa interface, o que resultará na perda de adjacências de vizinhos. Consequentemente, essa ação não apenas impede que o roteador anuncie atualizações de roteamento a partir dessa interface, mas também impede que ele receba atualizações de roteamento dessa interface.

Execute o comando show eigrp neighbors para validar o status do vizinho entre os FTDs.

firepower#show eigrp neighbors

Vizinhos EIGRP-IPv4 para AS(1)

Você pode verificar os pacotes EIGRP que estão sendo enviados e as interfaces pelas quais eles são enviados usando o comando debug eigrp packets.

FTD 1

Firepower1#

(UPDATE, REQUEST, QUERY, REPLY, HELLO, IPXSAP, PROBE, ACK, STUB, SIAQUERY, SIAREPLY)A depuração do pacote EIGRP está ativada

firepower#

EIGRP: Enviando HELLO para fora

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

EIGRP: Enviando HELLO por dentro

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

EIGRP: Enviando HELLO para fora

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

EIGRP: Enviando HELLO por dentro

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

EIGRP: Enviando HELLO para fora

FTD 2

Firepower2# debug eigrp packets

(UPDATE, REQUEST, QUERY, REPLY, HELLO, IPXSAP, PROBE, ACK, STUB, SIAQUERY, SIAREPLY)A depuração do pacote EIGRP está ativada

Firepower2#

Neste cenário, o FTD 2 não está enviando mensagens de saudação do EIGRP porque suas interfaces internas e externas estão configuradas como passivas. Verifique isso com o 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

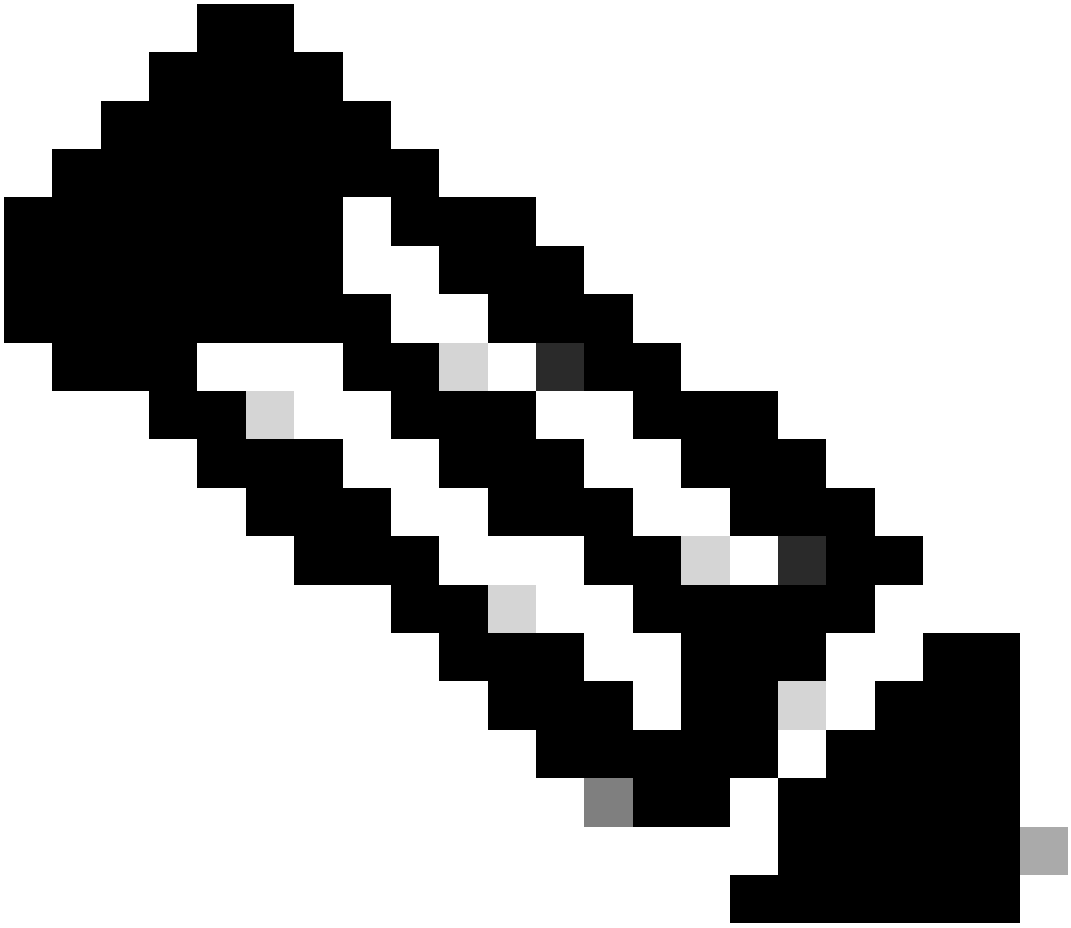
no eigrp log-neighbor-changes

rede 192.168.193.0 255.255.255.0

rede 172.16.193.8 255.255.255.248

passive-interface outside

passive-interface inside



Note: Para parar todos os processos de depuração configurados, use o comando undebug all.

Informações Relacionadas

- EIGRP em Dispositivos FTD
- Configurar o EIGRP no FTD
- Métricas de Custo Composto do EIGRP

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.