排除FMC管理的FTD设备上的EIGRP故障

目录

简介

本文档介绍如何验证由FMC管理的FTD上的EIGRP配置并对其进行故障排除。

先决条件

要求

Cisco 建议您了解以下主题：

- 增强型内部网关路由协议 (EIGRP)
- 思科安全防火墙管理中心(FMC)
- 思科安全防火墙威胁防御(FTD)

使用的组件

- 版本7.4.2中的FTDv。
- 版本7.4.2中的FMCv。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

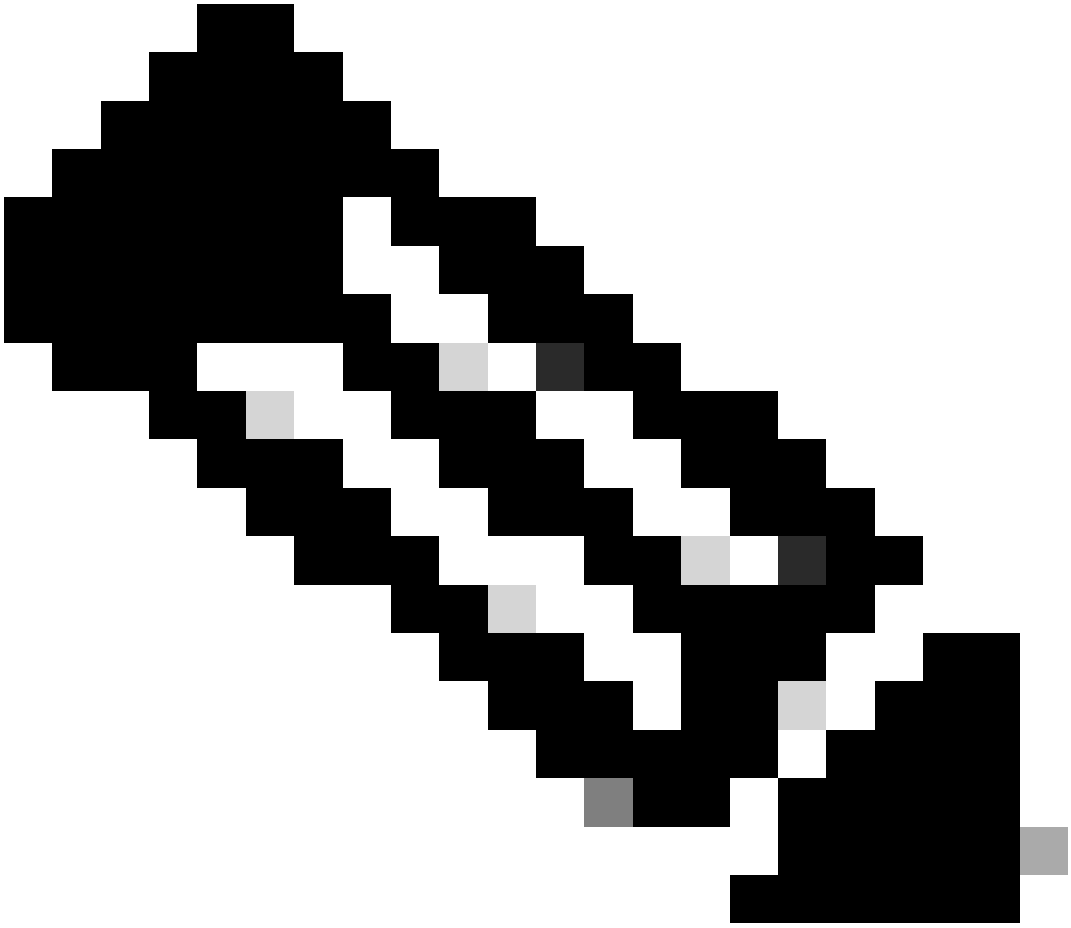
EIGRP是一种高级距离矢量路由协议，结合了距离矢量协议和链路状态协议的功能。它通过维护来自邻居的路

由信息来提供快速收敛，从而允许快速自适应到备用路由。EIGRP非常高效，它利用部分触发更新来更改路由或度量，而不是定期完全更新。
对于通信，EIGRP直接在IP层（协议88）上运行，并使用可靠传输协议(RTP)进行有保证有序的数据包传输。它支持组播和单播，并特别使用组播地址224.0.0.10或FF02::A发送hello消息。
EIGRP的运行基本上基于三个表中存储的信息：

- 邻居表:此表维护已成功建立邻接关系的直连EIGRP设备的记录。
- 拓扑表：此表存储由邻居通告的所有获知的路由，包括到特定目标的所有可行路径及其相关度量，以便评估其质量和可用路径的数量。
- 路由表： 此表包含每个目标的最佳路径，称为“后继路由器”。 此后继路由是主动用于转发流量的路由，随后会通告给其他EIGRP邻居。

EIGRP在路由和度量计算中使用度量权重(称为K值)来确定到达目的地的最佳路径。此度量值源自一个使用以下参数的公式：

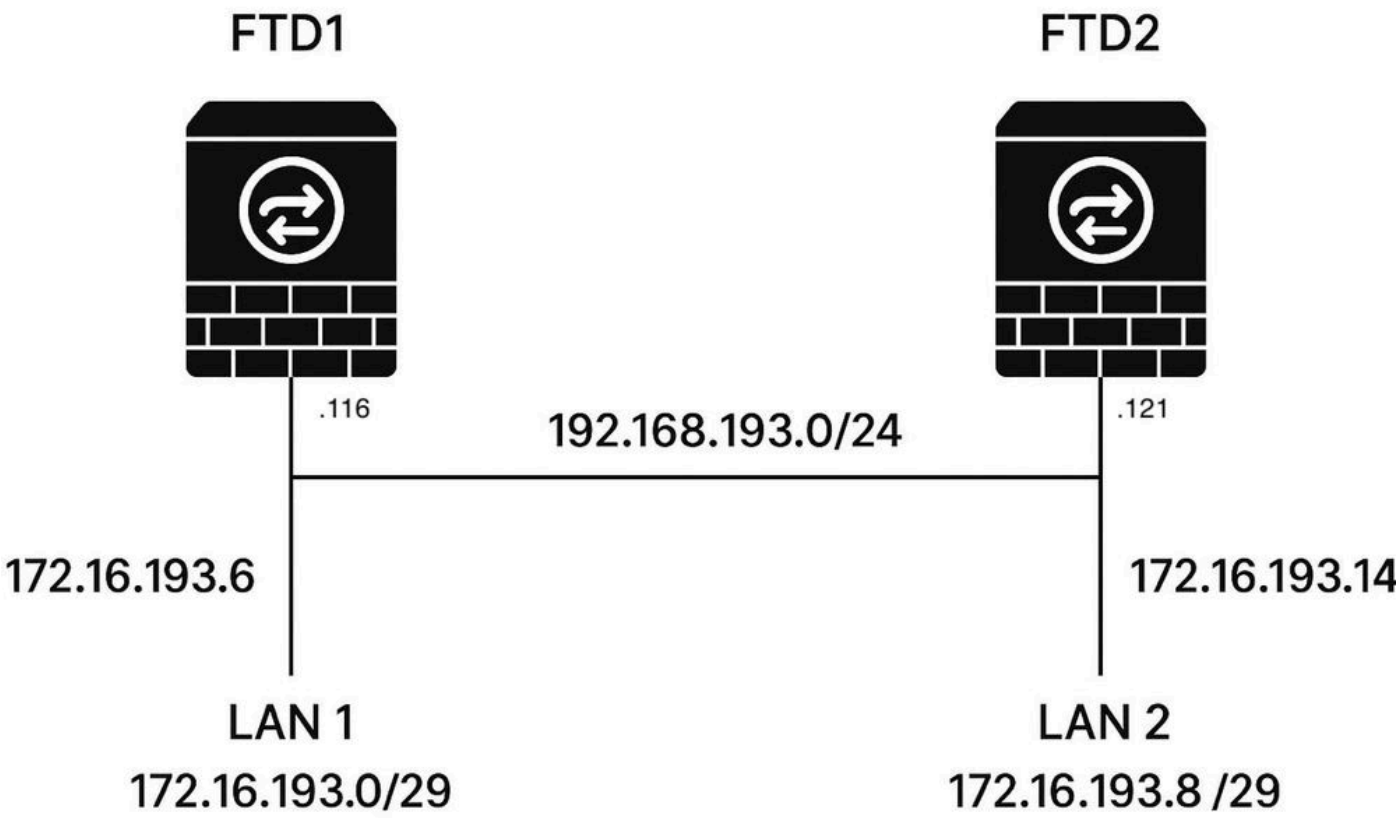
- 带宽
- 延迟时间
- 可靠性
- 正在加载
- MTU



注意：如果多条路径之间存在度量连接，则最大传输单位(MTU)用作断路器，首选较高的MTU值。

- 后继路由:这是通往特定目的地的最佳路径。它是最终安装到路由表中的路由。
- 可行距离 (FD)：从本地路由器的角度来说，这表示到达特定子网的最佳计算度量。
- 报告距离(RD)/通告距离(AD):这是邻居报告的到特定子网的距离（度量）。对于要被视为可行后继路由的路径，从邻居的报告距离必须小于本地路由器到同一目的地的可行距离。
- 可行后继路由器(FS):这是通向目的地的备用路径，在主后继路由发生故障时提供备用路由。如果路径的报告距离（与通告邻居的距离）严格小于当前后继路由到同一目的地的可行距离，则该路径符合可行后继路由的条件。

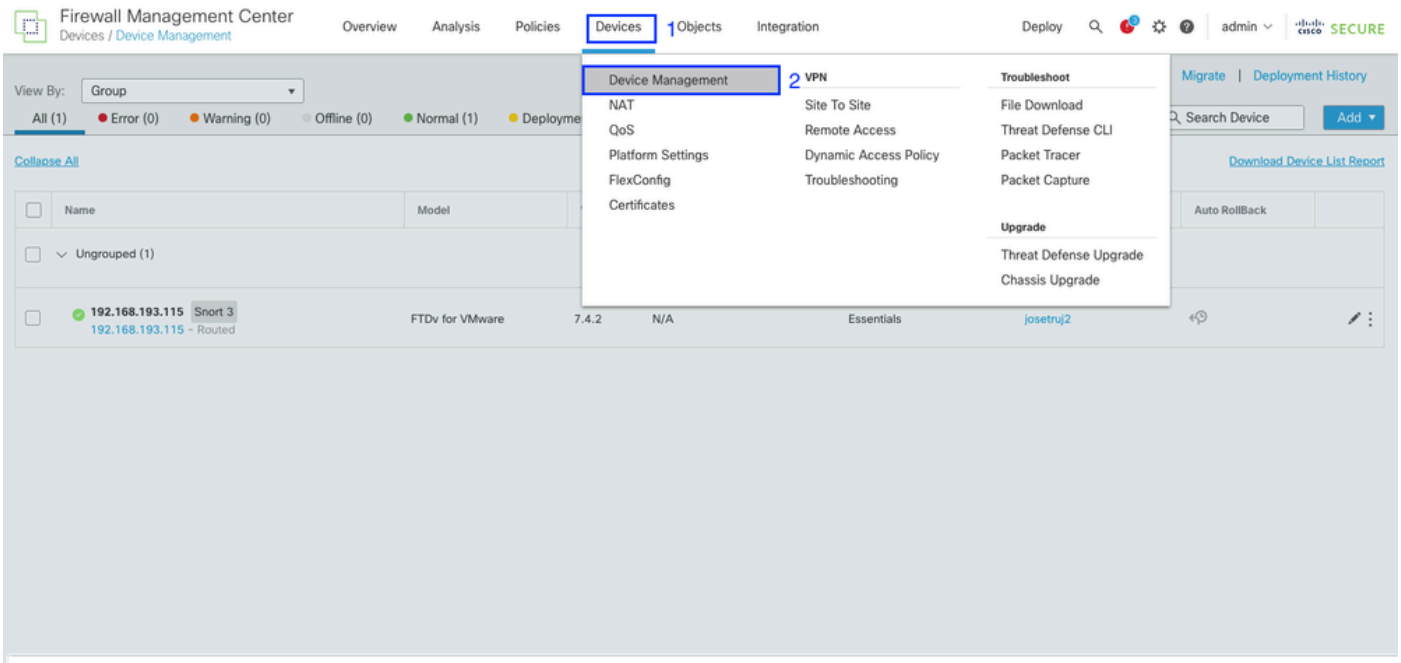
网络图



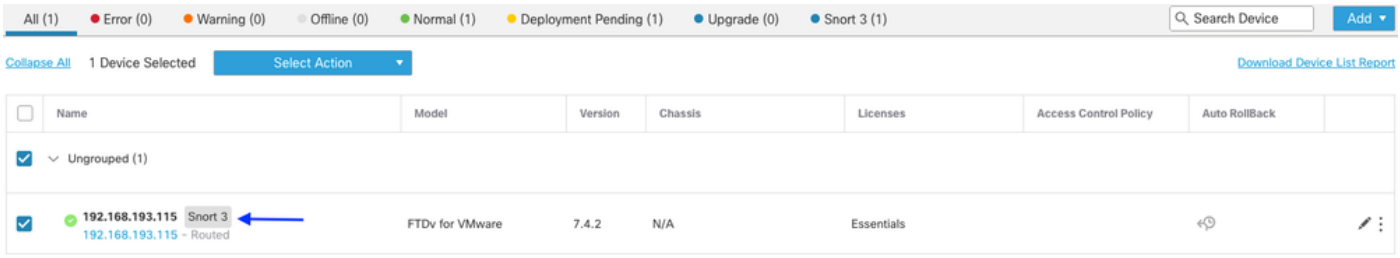
网络图

基本配置

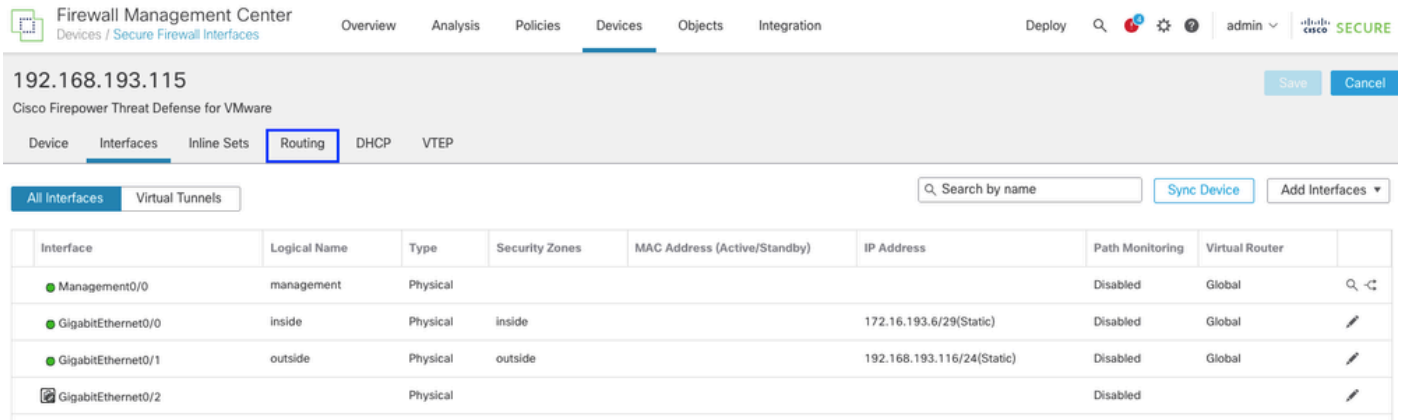
导航到设备>设备管理:



选择设备:



单击**Routing**选项卡。



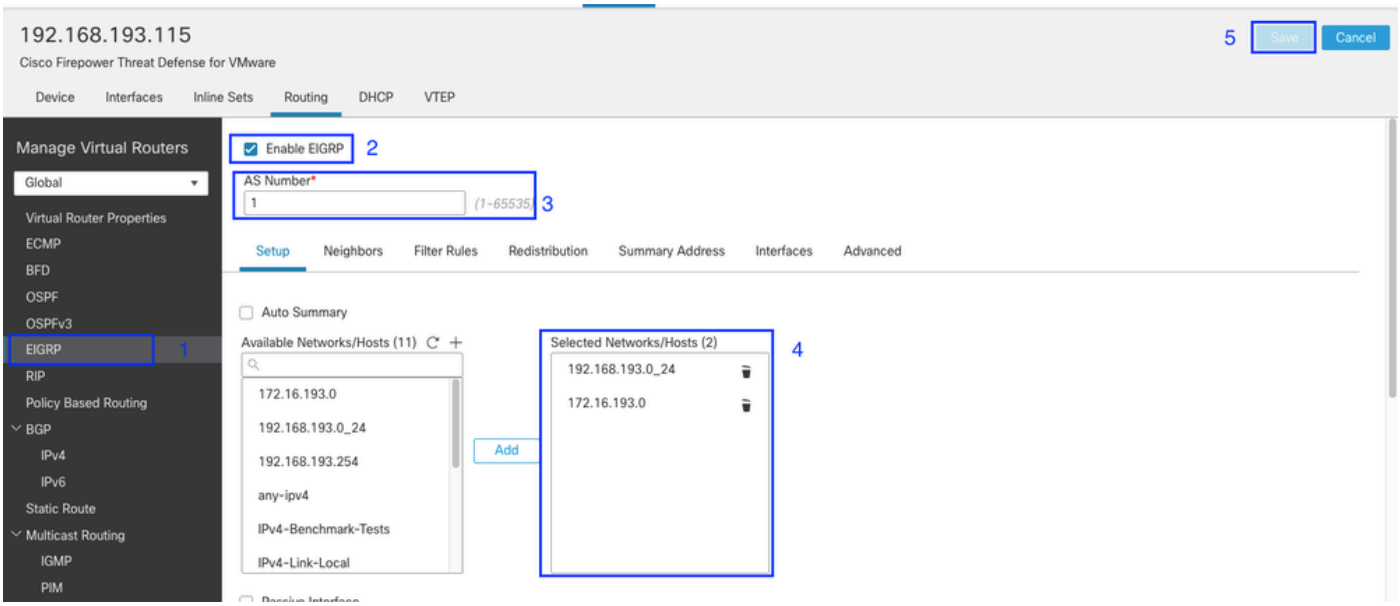
单击左侧菜单中的**EIGRP**。

单击**Enable EIGRP**。

分配**AS**编号(1-65535)。

选择一个网络/主机。您可以从“可用网络/主机”(Available Network/Host)列表中选择以前创建的对象，也可以通过点击加号(+)按钮创建新对象。

Click Save.



验证

以下是EIGRP邻居邻接的最低要求：

- AS编号必须匹配。
- 接口必须处于活动状态且可以访问。
- 作为一种最佳实践，Hello计时器和保持计时器必须匹配。
- K值必须匹配。
- 访问列表不能阻止EIGRP流量。

使用CLI进行验证

- 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

 无默认信息

 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

AS(1)的EIGRP-IPv4邻居

H Address Interface Hold Uptime SRTT RTO Q Seq

                                    (sec) (ms) Cnt Num

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

firepower# show eigrp topology

AS(1)/ID(192.168.193.121)的EIGRP-IPv4拓扑表

代码：P - Passive, A - Active, U - Update, Q - Query, R - Reply,

      r - reply Status, s - sia Status

P 192.168.193.0 255.255.255.0,1个后继路由器，FD为512

       通过已连接，外部
```

P 172.16.193.0 255.255.255.248,1个后继路由器，FD为768

通过192.168.193.116(768/512)，外部

P 172.16.193.8 255.255.255.248,1个后继路由器，FD为512

通过Connected、inside

firepower# show eigrp interfaces

AS(1)的EIGRP-IPv4接口

Xmit Queue Mean Pacing Time Multicast Pending

接口对等体不可靠SRTT不可靠流计时器路由

外部1 0 / 0 10 0 / 1 50 0

内部0 0 / 0 0 / 1 0 0

firepower#

firepower# show route eigrp

代码：L — 本地，C — 连接，S — 静态，R - RIP，M — 移动，B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF外部类型1、E2 - OSPF外部类型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 — 定期下载的静态路由，+ — 复制路由

SI — 静态InterVRF、BI - BGP InterVRF

Gateway of last resort is 192.168.193.254 to network 0.0.0.0

D 172.16.193.0 255.255.255.248

[90/768]通过192.168.193.116,02:32:58，外部

firepower# show route

代码：L — 本地，C — 连接，S — 静态，R - RIP，M — 移动，B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF外部类型1、E2 - OSPF外部类型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 — 定期下载的静态路由，+ — 复制路由

SI — 静态InterVRF、BI - BGP InterVRF

Gateway of last resort is 192.168.193.254 to network 0.0.0.0

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

D 172.16.193.0 255.255.255.248

[90/768]通过192.168.193.116,02:33:41，外部

C 172.16.193.8 255.255.255.248直接连接，在内部

L 172.16.193.14 255.255.255.255直接连接，内部

C 192.168.193.0 255.255.255.0直接连接，外部

L 192.168.193.121 255.255.255.255直接连接，外部

firepower#

firepower# show eigrp traffic

AS(1)的EIGRP-IPv4流量统计信息

Hellos sent/received:4006/4001

Updates sent/received:4/4

Queries sent/received:0/0

Replies sent/received:0/0

Acks sent/received:3/2

SIA-Queries sent/received:0/0

SIA-Replies sent/received:0/0

Hello Process ID:2503149568

PDM Process ID:2503150496

套接字队列：

Input queue:0/2000/2/0（当前/最大/最高/丢弃）

firepower#

故障排除

场景1 — 调试IP EIGRP邻居

可以使用debug命令来观察邻居状态的任何变化。

firepower# debug ip eigrp neighbor

firepower#

EIGRP:保持时间已过期

下降：对等192.168.193.121 total=0 stub 0,iidb-stub=0 iid-all=0

EIGRP:处理取消分配失败[0]

EIGRP:邻居192.168.193.121在外部发生故障

运行show eigrp neighbors命令以验证FTD之间的邻居状态。

firepower# show eigrp neighbors

AS(1)的EIGRP-IPv4邻居

使用show interface ip brief命令检验接口的状态。您可以看到GigabitEthernet0/1接口已管理性关闭。

firepower# show interface ip brief

Interface IP-Address OK?Method Status Protocol

GigabitEthernet0/0 172.16.193.14是启用配置

GigabitEthernet0/1 192.168.193.121 YES CONFIG administratively down（千兆以太网接口0/1 192.168.193.121是，管理性关闭）

GigabitEthernet0/2 192.168.194.24是手动启动

Internal-Control0/0 127.0.1.1是未设置

Internal-Control0/1 unassigned YES unset up

Internal-Data0/0 unassigned YES unset up

Internal-Data0/0 unassigned YES unset up

Internal-Data0/1 169.254.1.1是未设置

Internal-Data0/2 unassigned YES unset up

Management0/0 203.0.113.130是未设置

场景2 — 身份验证

FTD支持MD5散列算法对EIGRP数据包进行身份验证。默认情况下，此身份验证处于禁用状态。

要启用MD5散列算法，请选中“MD5身份验证”复选框。两台设备上的身份验证设置必须匹配；如果一台设备启用了，而另一台设备未启用，则两台设备之间无法形成邻居邻接关系。

使用debug eigrp packets验证此配置。

firepower# debug eigrp packets

（更新、请求、查询、应答、HELLO、IPXSAP、探测、ACK、末节、SIAQUERY、简单）EIGRP数据包调试已打开

firepower#

EIGRP:外部：忽略来自192.168.193.121的数据包，操作码= 5（身份验证关闭或缺少密钥链）

EIGRP:收到外部nbr 172.16.193.14的hello数据包

AS 1，标志0x0：（空），Seq 0/0 interfaceQ 0/0

EIGRP:在外部发送HELLO

AS 1，标志0x0:(NULL),Seq 0/0 interfaceQ 0/0 iidbQ un/lely 0/0

EIGRP:在内部发送HELLO

AS 1，标志0x0:(NULL),Seq 0/0 interfaceQ 0/0 iidbQ un/lely 0/0

EIGRP:外部：忽略来自192.168.193.121的数据包，操作码= 5（身份验证关闭或缺少密钥链）

EIGRP:收到外部nbr 172.16.193.14的hello数据包

AS 1，标志0x0：（空），Seq 0/0 interfaceQ 0/0

EIGRP:在内部发送HELLO

AS 1，标志0x0:(NULL),Seq 0/0 interfaceQ 0/0 iidbQ un/lely 0/0

EIGRP:在外部发送HELLO

AS 1，标志0x0:(NULL),Seq 0/0 interfaceQ 0/0 iidbQ un/lely 0/0

EIGRP:外部：忽略来自192.168.193.121的数据包，操作码= 5（身份验证关闭或缺少密钥链）。

您可以看到一条消息，指示身份验证已关闭或密钥链丢失。在这种情况下，当在一个对等体上启用身份验证而不在另一个对等体上启用身份验证时，通常会发生这种情况。

EIGRP:外部：忽略来自192.168.193.121的数据包，操作码= 5（身份验证关闭或缺少密钥链）。

使用show run interface <EIGRP interface>进行验证。

Firepower1# show run interface GigabitEthernet0/1

!

interface GigabitEthernet0/1

 nameif outside

 安全级别0

 ip address 192.168.193.121 255.255.255.0

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

 身份验证模式eigrp 1 md5

Firepower2# show run interface GigabitEthernet0/1

!

interface GigabitEthernet0/1

 nameif outside

 安全级别0

 ip address 192.168.193.116 255.255.255.0

场景3 — 被动接口

当配置了EIGRP时，EIGRP hello数据包通常在启用网络的接口上发送和接收。

但是，如果接口配置为被动接口，EIGRP会抑制该接口上两台路由器之间的hello数据包交换，从而导致邻居邻接关系丢失。因此，此操作不仅会阻止路由器通告该接口以外的路由更新，还会阻止路由器从该接口接收路由更新。

运行show eigrp neighbors命令以验证FTD之间的邻居状态。

firepower# show eigrp neighbors

AS(1)的EIGRP-IPv4邻居

您可以使用debug eigrp packets命令验证正在发送的EIGRP数据包及其所通过的接口。

FTD 1

Firepower1#

（更新、请求、查询、应答、HELLO、IPXSAP、探测、ACK、末节、SIAQUERY、简单）EIGRP数据包调试已打开

firepower#

EIGRP:在外部发送HELLO

AS 1，标志0x0:(NULL),Seq 0/0 interfaceQ 0/0 iidbQ un/lely 0/0

EIGRP:在内部发送HELLO

AS 1，标志0x0:(NULL),Seq 0/0 interfaceQ 0/0 iidbQ un/lely 0/0

EIGRP:在外部发送HELLO

AS 1，标志0x0:(NULL),Seq 0/0 interfaceQ 0/0 iidbQ un/lely 0/0

EIGRP:在内部发送HELLO

AS 1，标志0x0:(NULL),Seq 0/0 interfaceQ 0/0 iidbQ un/lely 0/0

EIGRP:在外部发送HELLO

FTD 2

Firepower2# debug eigrp packets

（更新、请求、查询、应答、HELLO、IPXSAP、探测、ACK、末节、SIAQUERY、简单）EIGRP数据包调试已打开

Firepower2#

在此场景中，FTD 2不发送EIGRP hello消息，因为其内部和外部接口配置为被动接口。使用show run router eigrp命令验证这一点。

Firepower2# show run router eigrp

router eigrp 1

无默认信息

no default-information out

no eigrp log-neighbor-warnings

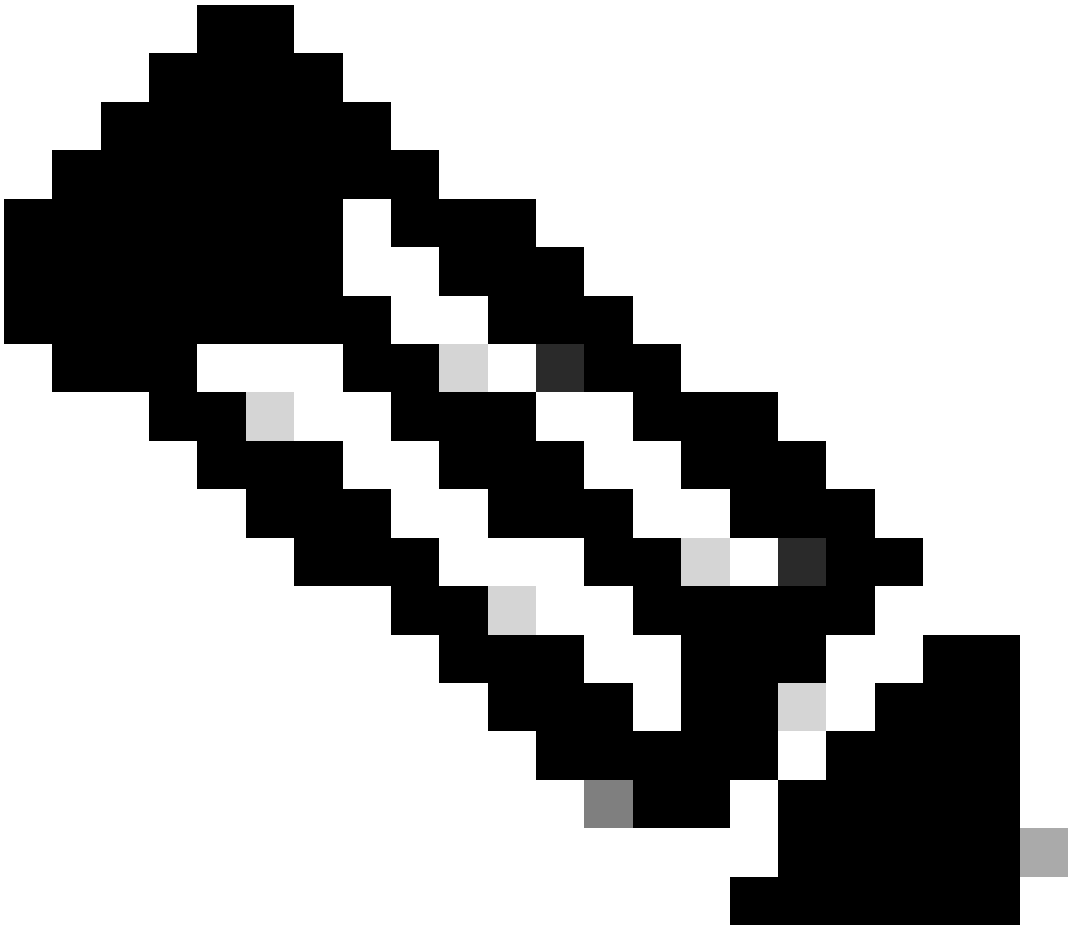
no eigrp log-neighbor-changes

network 192.168.193.0 255.255.255.0

network 172.16.193.8 255.255.255.248

passive-interface out

passive-interface inside



注意：要停止所有已配置的调试进程，请使用undebug all命令。

相关信息

- FTD设备上的EIGRP
- 在FTD上配置EIGRP
- EIGRP复合成本度量

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。