排除FMC管理的FTD裝置上的EIGRP故障

目錄

[簡介](#)

[必要條件](#)

- [需求](#)
- [採用元件](#)

[背景資訊](#)

- [網路圖表](#)

[基本配置](#)

[驗證](#)

[使用CLI進行驗證](#)

[疑難排解](#)

- [場景1 — 調試IP EIGRP鄰居](#)
- [案例2 — 驗證](#)
- [案例3 — 被動介面](#)

[相關資訊](#)

簡介

本檔案介紹如何驗證和疑難排解由FMC管理的FTD上的EIGRP配置。

必要條件

需求

思科建議您瞭解以下主題：

- 增強型內部閘道路由通訊協定(EIGRP)
- 思科安全防火牆管理中心(FMC)
- 思科安全防火牆威脅防禦(FTD)

採用元件

- 7.4.2版中的FTDv。
- 7.4.2版中的FMCv。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

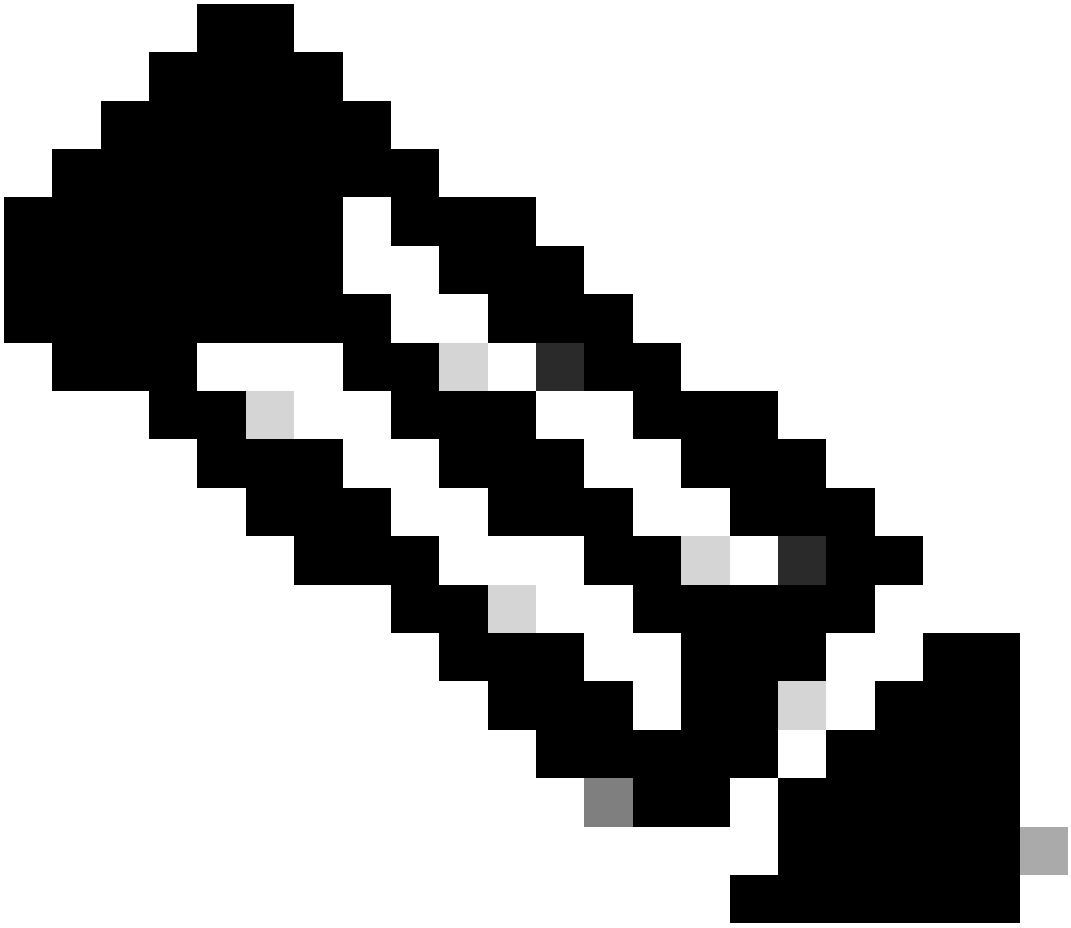
EIGRP是一種高級距離向量路由協定，結合了距離向量協定和鏈路狀態協定的特性。它通過維護來自鄰居的路

由資訊來提供快速收斂，從而允許快速調整到備用路由。EIGRP非常高效，它利用部分觸發更新來更改路由或度量，而不是定期進行完全更新。
對於通訊，EIGRP直接在IP層（協定88）上運行，並使用可靠傳輸協定(RTP)進行有保證有序的資料包傳輸。它支援組播和單播，並專門使用組播地址224.0.0.10或FF02::A傳送問候消息。
EIGRP操作基本上基於儲存在三個表中的資訊：

- 鄰居表：此表維護已成功建立鄰接關係的直連EIGRP裝置的記錄。
- 拓撲表：此表儲存鄰居通告的所有獲知的路由，包括到特定目標的所有可行路徑及其關聯的度量，以便評估它們的品質和可用路徑數。
- 路由表： 此表包含每個目標的最佳路徑，稱為「後繼路由器」。 此後繼路由是主動用於轉發流量的路由，隨後會通告給其他EIGRP鄰居。

EIGRP在路由和度量計算中使用度量權重(稱為K值)來確定到達目的地的最佳路徑。此度量值從使用以下引數的公式匯出：

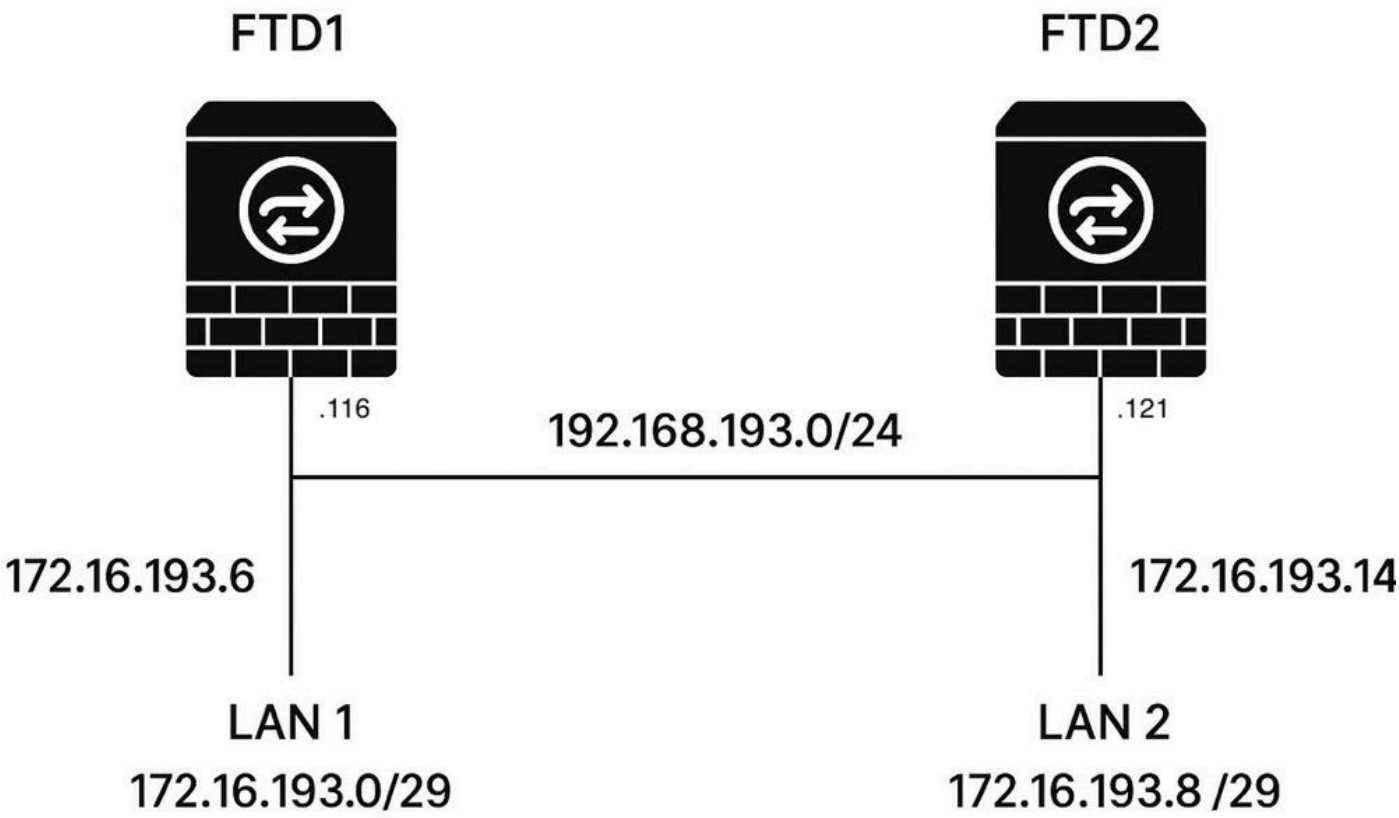
- 頻寬
- 延遲時間
- 可靠性
- 載入中
- MTU



附註：在多個路徑之間出現度量連線的情況下，最大傳輸單元(MTU)用作連線斷路器，最好使用較高的MTU值。

- 後繼路由:這是前往特定目的地的最佳路徑。最終會將該路由安裝到路由表中。
- 可行距離(FD):從本地路由器的角度來看，這表示到達特定子網的最佳計算度量。
- 報告距離(RD)/通告距離(AD):這是鄰居報告的特定子網的距離（度量）。對於要被視為可行後繼路由的路徑，鄰居的報告距離必須小於本地路由器到同一目的地的可行距離。
- 可行後繼路由器(FS):這是通往目的地的備用路徑，在主後繼路由發生故障時提供備用路由。如果某條路徑的報告距離（與通告鄰居的距離）嚴格小於當前後繼路由到同一目的地的可行距離，則該路徑有資格成為可行後繼路由。

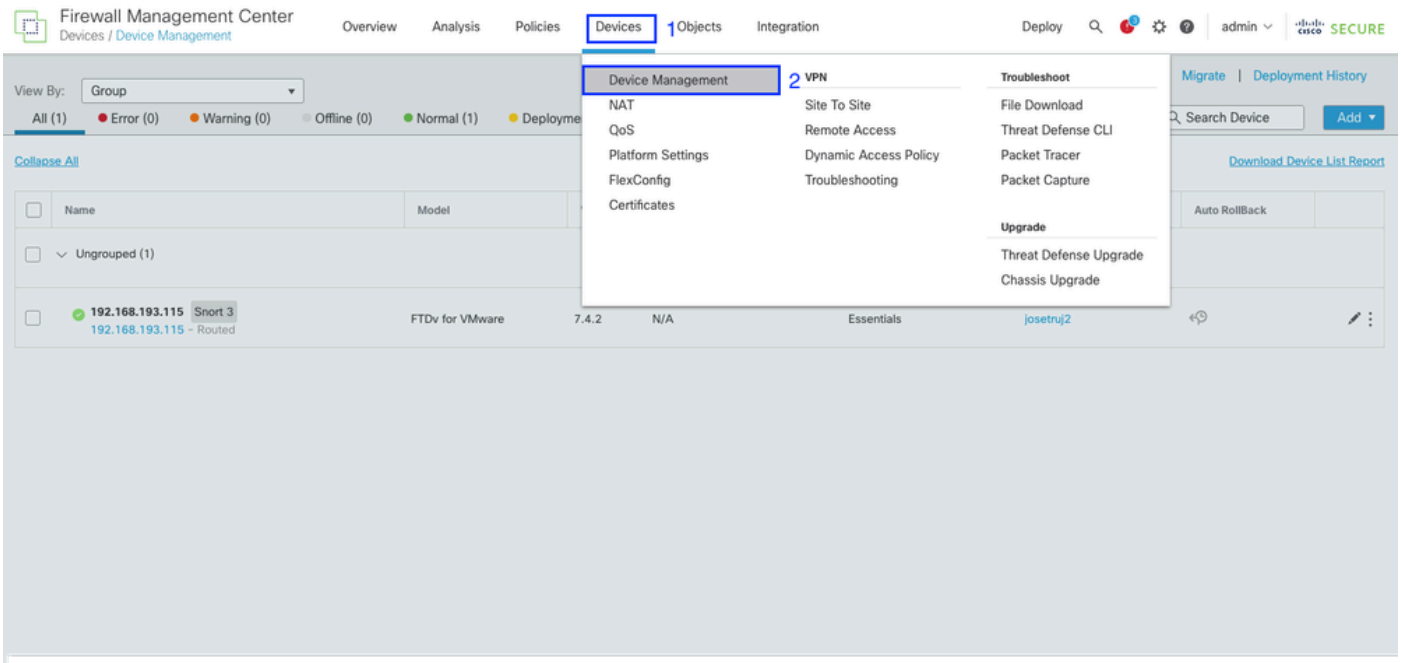
網路圖表



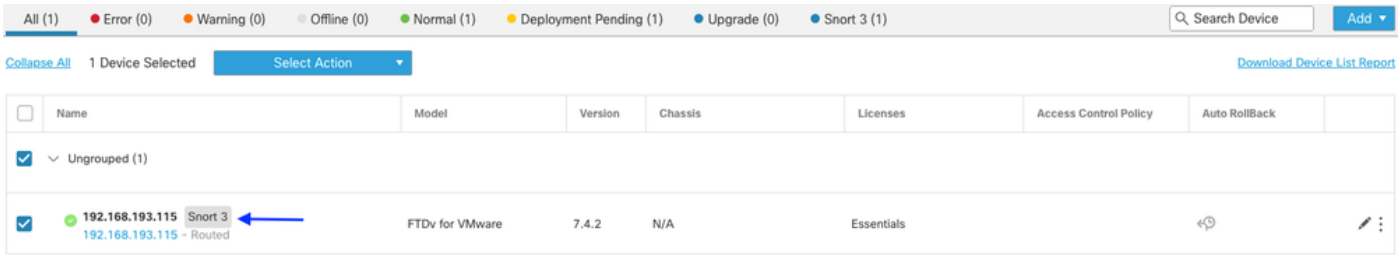
網路圖表

基本配置

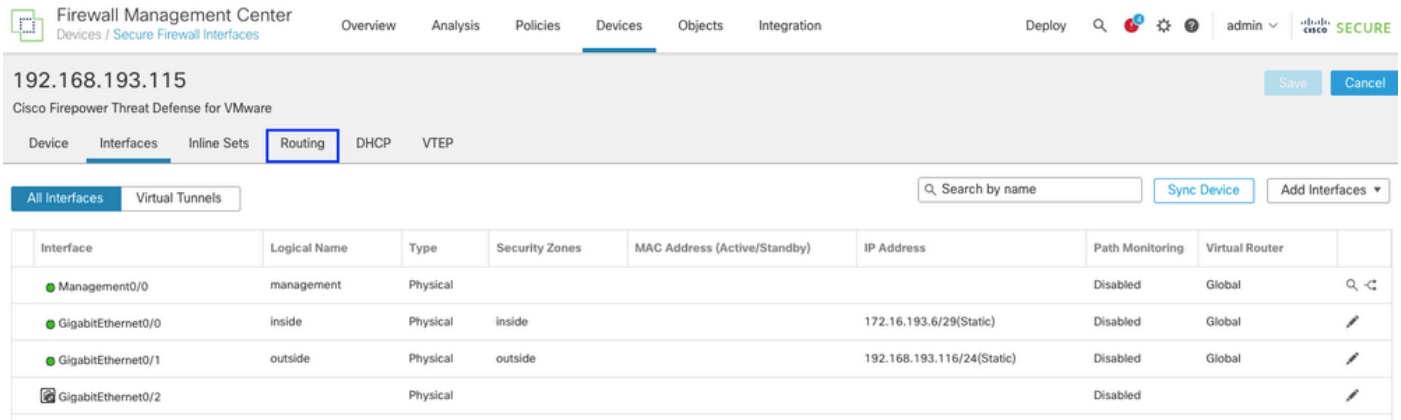
導覽至Devices > Device Management:



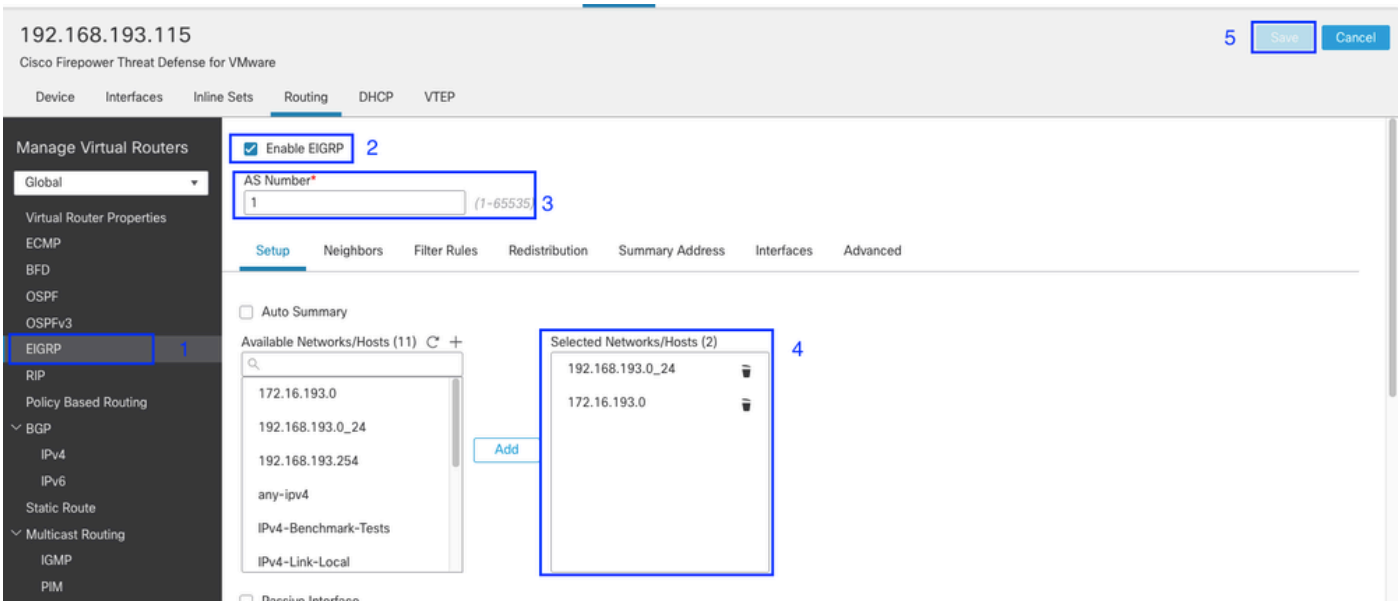
選擇裝置：



按一下**Routing**頁籤。



按一下左側選單中的**EIGRP**。
按一下**Enable EIGRP**。
分配**AS編號**(1-65535)。
選擇一個網路/主機。您可以從「可用網路/主機」清單中選擇以前建立的對象，也可以按一下加號(+)按鈕**創建新對象**。
按一下「**Save**」。



驗證

以下是EIGRP鄰居鄰接的最低要求：

- AS編號必須匹配。
- 介面必須處於作用中且可以連線。
- 作為一種最佳實踐，Hello計時器和Hold計時器必須匹配。
- K值必須匹配。
- 沒有訪問清單必須阻止EIGRP流量。

使用CLI進行驗證

- show run router eigrp
- 顯示eigrp鄰居
- 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

no default-information out

no eigrp log-neighbor-warnings

no eigrp log-neighbor-changes

網路192.168.193.0 255.255.255.0

網路172.16.193.8 255.255.255.248

firepower#

firepower# show eigrp neighbors

AS(1)的EIGRP-IPv4鄰居

H地址介面保持正常運行時間SRTT RTO Q序列

（秒）（毫秒）Cnt數

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拓撲表

代碼：P — 被動，A — 主動，U — 更新，Q — 查詢，R — 回覆，

r — 回覆狀態，s - sia狀態

P 192.168.193.0 255.255.255.0,1個後繼路由器，FD為512

通過已連線，外部

P 172.16.193.0 255.255.255.248,1個後繼路由器，FD為768

通過192.168.193.116(768/512)，外部

P 172.16.193.8 255.255.255.248,1個後繼路由器，FD為512

通過Connected、inside

firepower# show eigrp interfaces

AS(1)的EIGRP-IPv4介面

Xmit隊列平均步調時間多播掛起

介面對等體無/可靠SRTT無/可靠流計時器路由

外部1 0 / 0 10 0 / 1 50 0

內部0 0 / 0 0 / 1 0

firepower#

firepower# show route eigrp

代碼：L — 本地， C — 連線， S — 靜態， R - RIP， M — 移動， B - BGP

D - EIGRP、EX - EIGRP外部、O - OSPF、IA - OSPF內部區域

N1 - OSPF NSSA外部型別1,N2 - OSPF NSSA外部型別2

E1 - OSPF外部型別1,E2 - OSPF外部型別2,V - VPN

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

ia - IS-IS內部區域， * — 候選預設值， U — 每使用者靜態路由

o - ODR， P — 定期下載靜態路由， + — 複製路由

SI — 靜態InterVRF、BI - BGP InterVRF

最後選用網關是192.168.193.254到網路0.0.0.0

D 172.16.193.0 255.255.248

[90/768]通過192.168.193.116,02:32:58，外部

firepower# show route

代碼：L — 本地， C — 連線， S — 靜態， R - RIP， M — 移動， B - BGP

D - EIGRP、EX - EIGRP外部、O - OSPF、IA - OSPF內部區域

N1 - OSPF NSSA外部型別1,N2 - OSPF NSSA外部型別2

E1 - OSPF外部型別1,E2 - OSPF外部型別2,V - VPN

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

ia - IS-IS內部區域， * — 候選預設值， U — 每使用者靜態路由

o - ODR， P — 定期下載靜態路由， + — 複製路由

SI — 靜態InterVRF、BI - BGP InterVRF

最後選用網關是192.168.193.254到網路0.0.0.0

S* 0.0.0.0 0.0.0.0 [1/0]（通過192.168.193.254，外部）

D 172.16.193.0 255.255.248

[90/768]通過192.168.193.116,02:33:41，外部

C 172.16.193.8 255.255.255.248直接連線，在內部

L 172.16.193.14 255.255.255.255直接連線，在內部

C 192.168.193.0 255.255.255.0直接連線，外部

L 192.168.193.121 255.255.255.255直接連線，外部

firepower#

firepower# show eigrp traffic

AS(1)的EIGRP-IPv4流量統計資訊

傳送/接收的Hello:4006/4001

傳送/接收的更新：4/4

傳送/接收的查詢：0/0

已傳送/已接收答覆：0/0

傳送/接收的ACK:3/2

傳送/接收的SIA查詢：0/0

SIA — 已傳送/已接收：0/0

Hello進程ID:2503149568

PDM進程ID:2503150496

套接字隊列：

輸入隊列：0/2000/2/0(current/max/highest/drops)

firepower#

疑難排解

場景1 — 調試IP EIGRP鄰居

Debug命令可用於觀察鄰居狀態的任何變化。

firepower# debug ip eigrp neighbor

firepower#

EIGRP:保持時間已過期

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

EIGRP:處理取消分配失敗[0]

EIGRP:鄰居192.168.193.121在外部斷開

運行show eigrp neighbors命令以驗證FTD之間的鄰居狀態。

firepower# show eigrp neighbors

AS(1)的EIGRP-IPv4鄰居

使用show interface ip brief命令檢驗介面的狀態。您可以看到GigabitEthernet0/1介面處於管理性關閉狀態。

firepower# show interface ip brief

介面IP地址是否正常？方法狀態協定

GigabitEthernet0/0 172.16.193.14 YES CONFIG up

GigabitEthernet0/1 192.168.193.121 YES CONFIG管理性關閉

GigabitEthernet0/2 192.168.194.24是，手動啟動

Internal-Control0/0 127.0.1.1是未設定

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是未設定

Internal-Data0/2 unassigned YES unset up

Management0/0 203.0.113.130是未設定

案例2 — 驗證

FTD支援MD5雜湊演演算法來驗證EIGRP封包。預設情況下，此身份驗證處於禁用狀態。

要啟用MD5雜湊演算法，請選中「MD5身份驗證」覈取方塊。兩台裝置上的身份驗證設定匹配至關重要；如果在一台裝置上啟用，但在另一台裝置上未啟用，則無法在它們之間形成鄰居鄰接關係。

使用debug eigrp packets驗證此配置。

firepower# debug eigrp packets

(UPDATE、REQUEST、QUERY、REPLY、HELLO、IPXSAP、PROBE、ACK、STUB、SIAQUERY、SIAREPLY)EIGRP資料包調試已啟用

firepower#

EIGRP:outside:忽略來自192.168.193.121的資料包，操作碼= 5（身份驗證關閉或缺少金鑰鏈）

EIGRP:在外部nbr 172.16.193.14上收到HELLO

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

EIGRP:在外部傳送HELLO

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

EIGRP:正在內部傳送HELLO

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

EIGRP:outside:忽略來自192.168.193.121的資料包，操作碼= 5（身份驗證關閉或缺少金鑰鏈）

EIGRP:在外部nbr 172.16.193.14上收到HELLO

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

EIGRP:正在內部傳送HELLO

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

EIGRP:在外部傳送HELLO

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

EIGRP:outside:忽略來自192.168.193.121的資料包，操作碼= 5（身份驗證關閉或缺少金鑰鏈）。

您可以看到一條消息，指示身份驗證已關閉或缺少金鑰鏈。在此案例中，通常是在一個對等體啟用身份驗證，而在另一個對等體未啟用身份驗證時發生。

EIGRP:outside:忽略來自192.168.193.121的資料包，操作碼= 5（身份驗證關閉或缺少金鑰鏈）。

使用show run interface <EIGRP interface>進行驗證。

Firepower1# show run interface GigabitEthernet0/1

!

interface GigabitEthernet0/1

 nameif outside

 安全級別0

 ip address 192.168.193.121 255.255.255.0

 身份驗證金鑰eigrp ***** key-id 10

 身份驗證模式eigrp 1 md5

Firepower2# show run interface GigabitEthernet0/1

!

interface GigabitEthernet0/1

 nameif outside

 安全級別0

 ip address 192.168.193.116 255.255.255.0

案例3 — 被動介面

配置EIGRP後，通常會在啟用網路的介面上傳送和接收EIGRP hello資料包。

但是，如果將介面配置為被動介面，EIGRP會抑制該介面上兩台路由器之間的hello資料包交換，從而導致鄰居鄰接關係丟失。因此，此操作不僅阻止路由器通告該介面以外的路由更新，而且阻止路由器從該介面接收路由更新。

運行show eigrp neighbors命令以驗證FTD之間的鄰居狀態。

firepower# show eigrp neighbor

AS(1)的EIGRP-IPv4鄰居

您可以使用debug eigrp packets命令檢驗要傳送的EIGRP資料包以及要通過哪個介面傳送這些資料包。

FTD 1

Firepower1#

(UPDATE、REQUEST、QUERY、REPLY、HELLO、IPXSAP、PROBE、ACK、STUB、SIAQUERY、SIAREPLY)EIGRP資料包調試已啟用

firepower#

EIGRP:在外部傳送HELLO

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

EIGRP:正在內部傳送HELLO

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

EIGRP:在外部傳送HELLO

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

EIGRP:正在內部傳送HELLO

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

EIGRP:在外部傳送HELLO

FTD 2

Firepower2# debug eigrp packets

(UPDATE、REQUEST、QUERY、REPLY、HELLO、IPXSAP、PROBE、ACK、STUB、SIAQUERY、SIAREPLY)EIGRP資料包調試已啟用

Firepower2#

在此案例中，FTD 2不傳送EIGRP hello消息，因為其內部和外部介面配置為被動介面。使用show run router eigrp命令驗證這一點。

Firepower2# show run router eigrp

router eigrp 1

no default-information

no default-information out

no eigrp log-neighbor-warnings

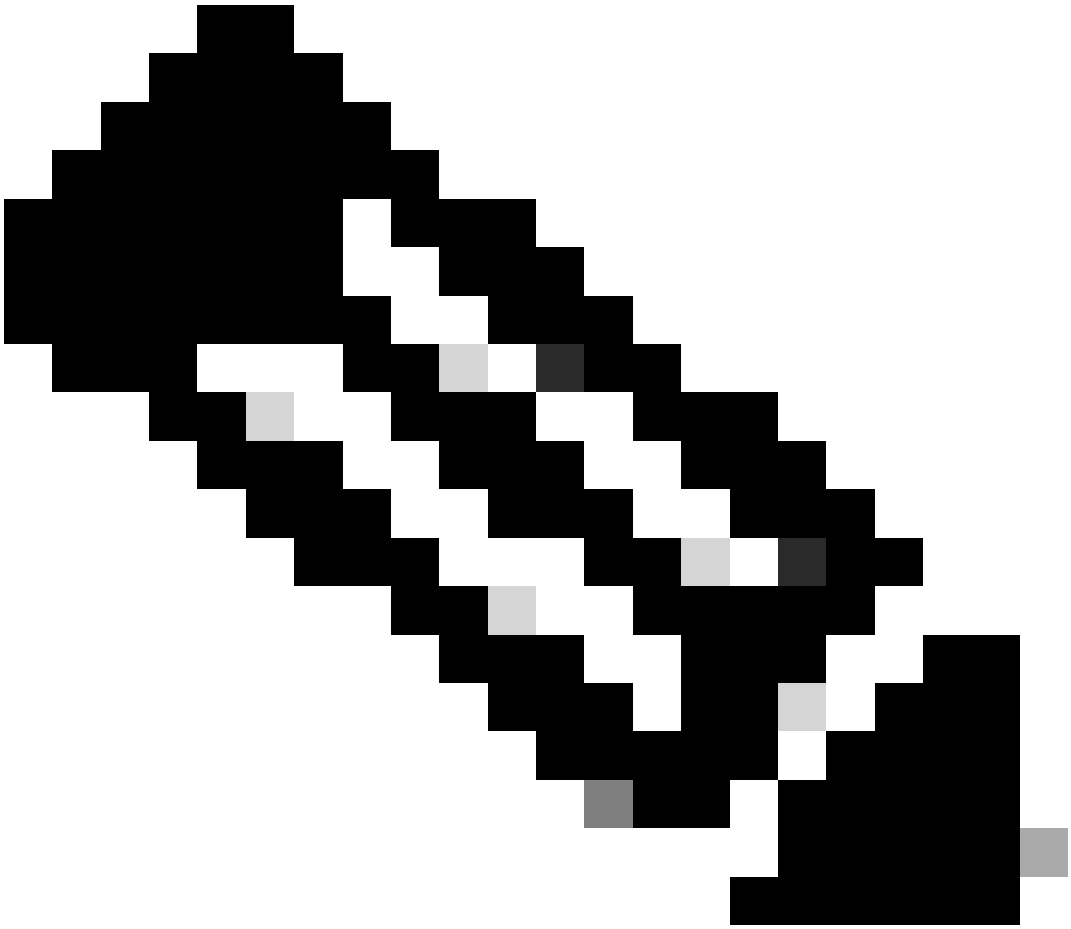
no eigrp log-neighbor-changes

網路192.168.193.0 255.255.255.0

網路172.16.193.8 255.255.255.248

passive-interface out

passive-interface inside



附註：若要停止所有已配置的調試進程，請使用undebug all命令。

相關資訊

- FTD裝置上的EIGRP
- 在FTD上設定EIGRP
- EIGRP複合成本度量

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。