Risoluzione dei problemi relativi a EIGRP su dispositivi FTD gestiti da FMC

Sommario

Introduzione

In questo documento viene descritto come verificare e risolvere i problemi relativi alla configurazione EIGRP su FTD gestito da FMC.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Protocollo EIGRP (Enhanced Interior Gateway Routing Protocol)
- Cisco Secure Firewall Management Center (FMC)
- Cisco Secure Firewall Threat Defense (FTD)

Componenti usati

- FTDv nella versione 7.4.2.
- FMCv nella versione 7.4.2.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata

ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

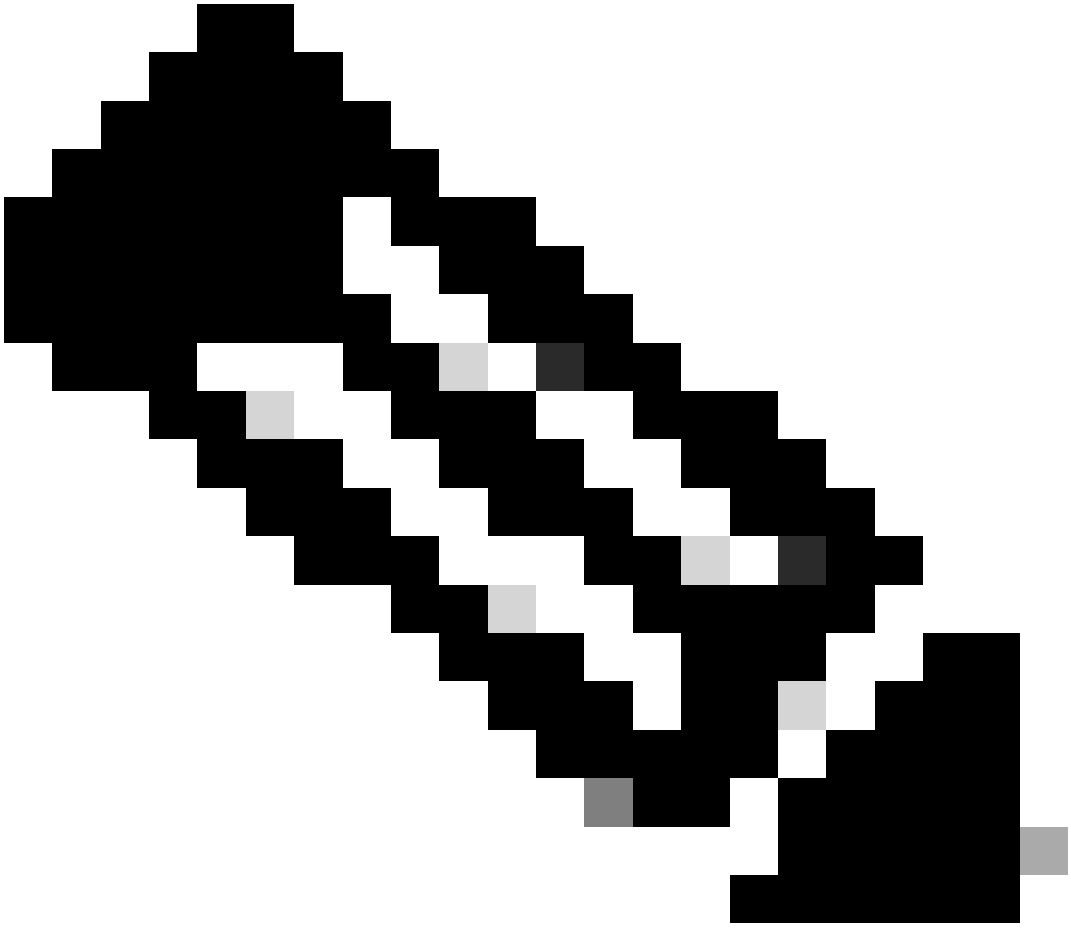
Premesse

EIGRP è un protocollo avanzato di routing dei vettori di distanza che combina le caratteristiche dei protocolli vettore di distanza e stato del collegamento. Offre una rapida convergenza mantenendo le informazioni di routing dai vicini, consentendo un rapido adattamento a percorsi alternativi. Il protocollo EIGRP è efficiente e utilizza aggiornamenti parziali attivati per le modifiche delle route o delle metriche anziché aggiornamenti completi periodici.
Per la comunicazione, EIGRP opera direttamente sul layer IP (protocollo 88) e utilizza il protocollo RTP (Reliable Transport Protocol) per la consegna di pacchetti ordinati e garantiti. Supporta sia multicast che unicast, con messaggi di saluto che utilizzano specificamente indirizzi multicast 24.0.0.10 o FF02::A.
L'operazione EIGRP si basa essenzialmente sulle informazioni memorizzate in tre tabelle:

- Tabella router adiacente: Questa tabella conserva un record di dispositivi EIGRP collegati direttamente con cui è stata stabilita una adiacenza.
- Tabella topologia: In questa tabella vengono memorizzati tutti i percorsi appresi annunciati dai vicini, inclusi tutti i percorsi possibili per una destinazione specifica e le metriche associate, consentendo una valutazione della qualità e del numero di percorsi disponibili.
- Tabella di routing: Questa tabella contiene il percorso migliore per ogni destinazione, noto come 'Successore'. Questa route Successor è quella utilizzata attivamente per l'inoltro del traffico e viene successivamente pubblicizzata ad altri vicini EIGRP.

Il protocollo EIGRP utilizza pesi metrici, noti come valori K, nei calcoli di routing e metrici per determinare il percorso ottimale verso una destinazione. Questo valore della metrica è derivato da una formula che utilizza i parametri riportati di seguito.

- Larghezza di banda
- Tempo di ritardo
- Affidabilità
- Caricamento in corso
- MTU

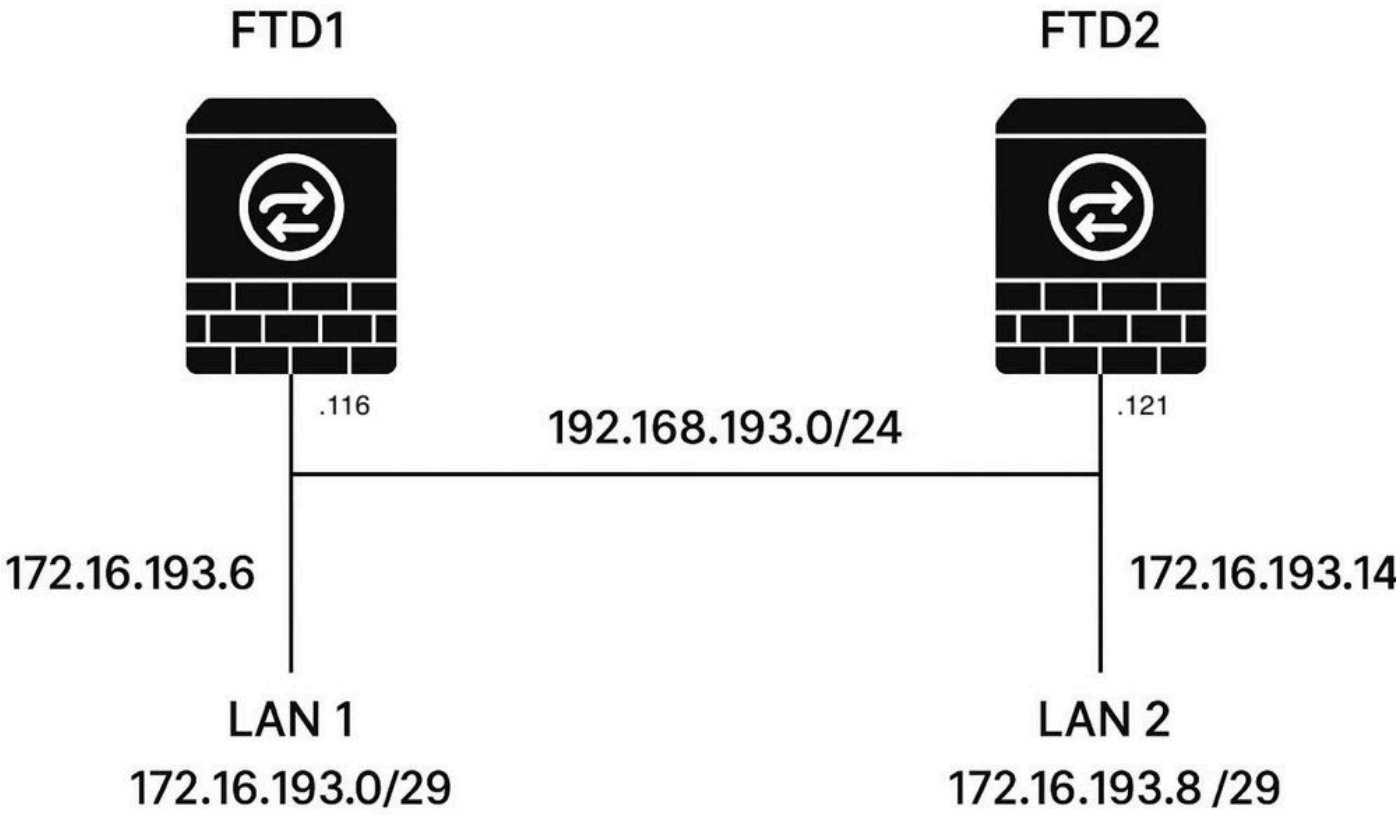


Nota: Nel caso di un legame metrico tra più percorsi, l'MTU (Maximum Transmission Unit) viene usata come interrompente, preferendo un valore MTU più alto.

- Route successore: Questo è definito come il miglior percorso verso una destinazione specifica. È il percorso che viene installato nella tabella di routing.
- Distanza realizzabile (FD): Questa è la metrica meglio calcolata per raggiungere una particolare subnet dal punto di vista del router locale.
- Distanza segnalata (RD) / Distanza annunciata (AD): Distanza (metrica) da una subnet specifica rilevata da un router adiacente. Affinché un percorso sia considerato un successore fattibile, la distanza indicata dal router adiacente deve essere inferiore alla distanza fattibile del router locale verso la stessa destinazione.
- Feasible Successor (FS): Si tratta di un percorso di backup verso una destinazione, che fornisce un percorso alternativo in caso di errore della route successore primaria. Un percorso viene considerato successore realizzabile se la distanza riportata (dal router

adiacente pubblicitario) è strettamente inferiore alla distanza realizzabile del percorso successore corrente verso la stessa destinazione.

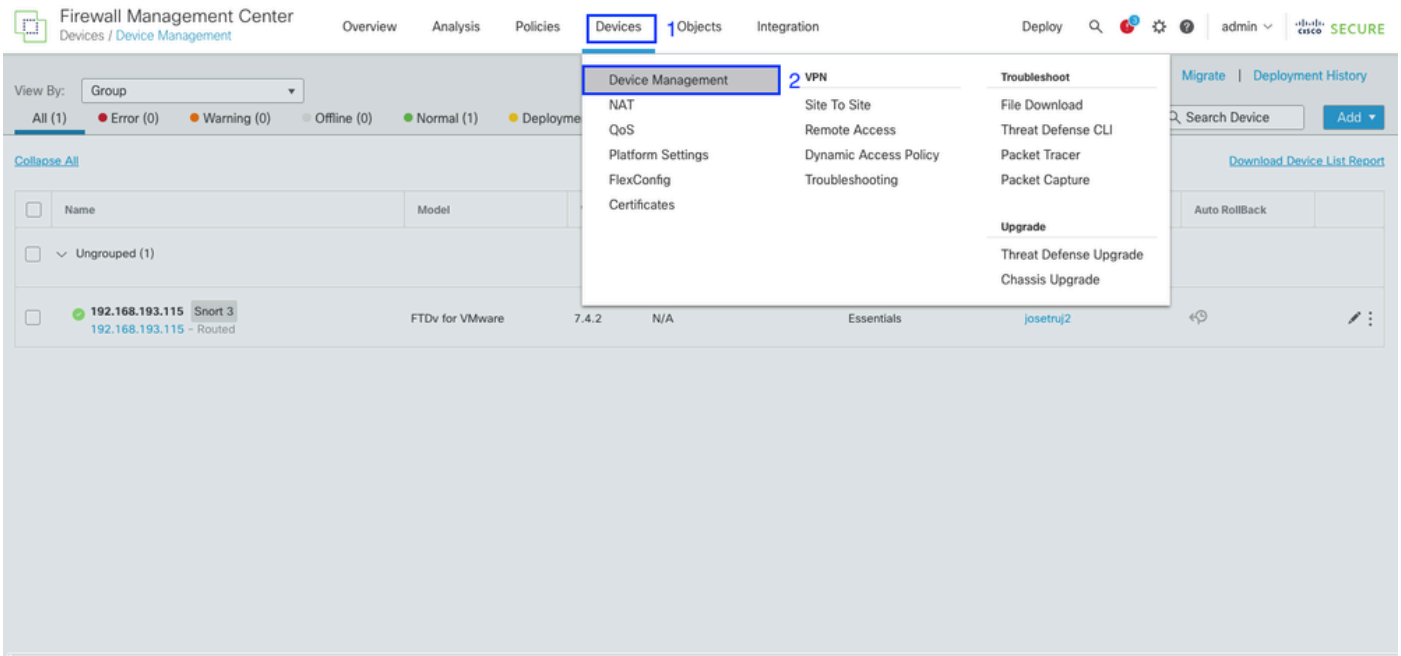
Esempio di rete



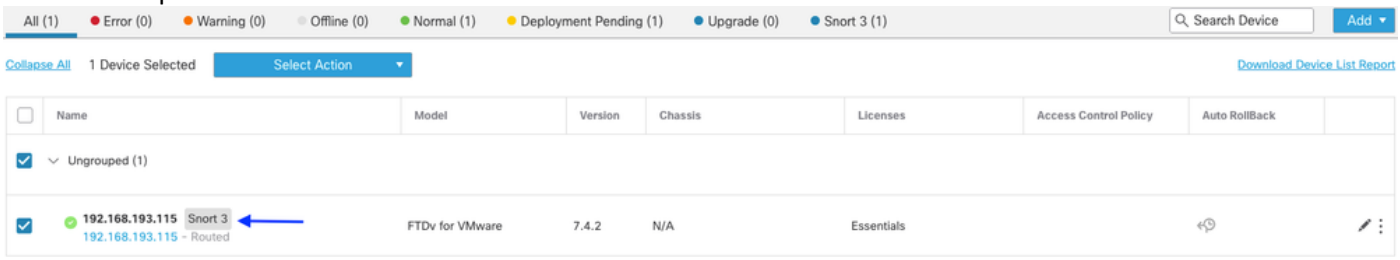
Esempio di rete

Configurazione di base

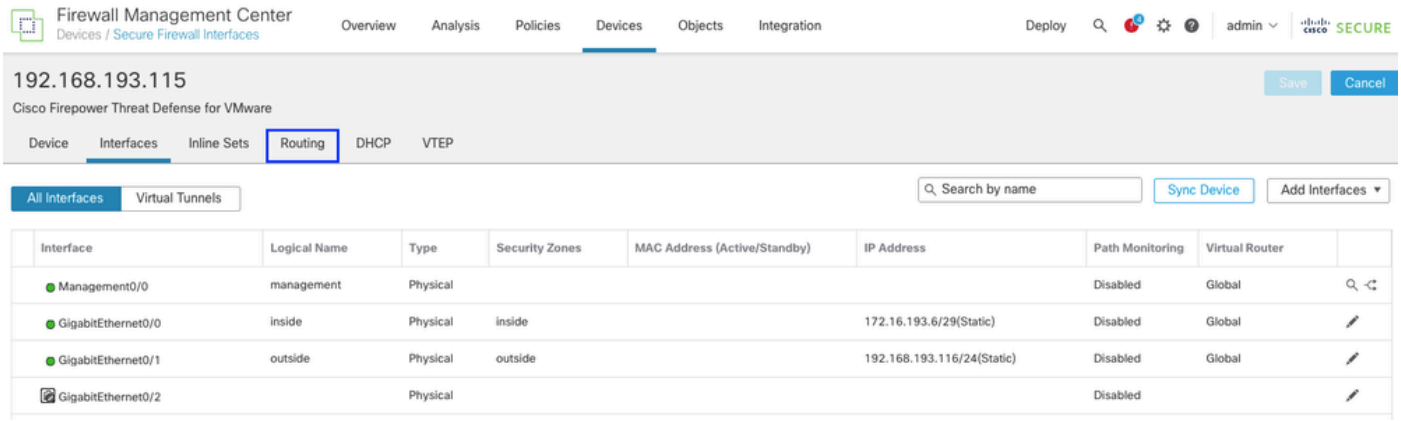
Selezionare **Dispositivi > Gestione dispositivi**:



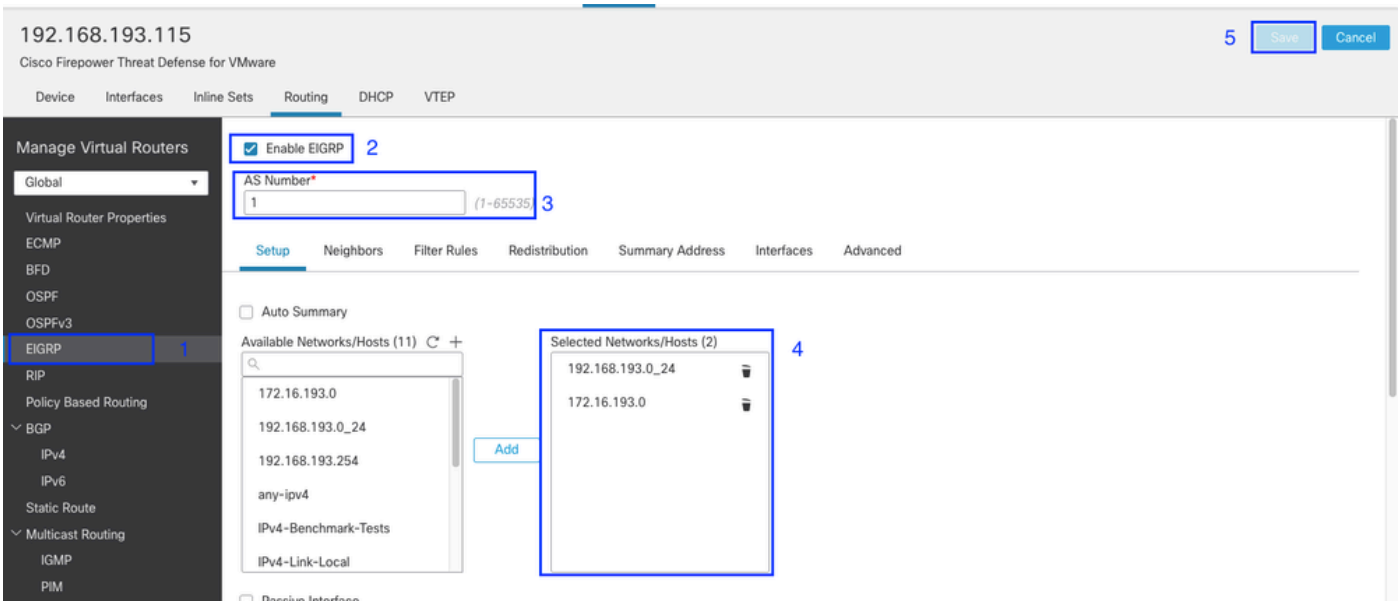
Seleziona dispositivo:



Fare clic sulla scheda **Instradamento**.



Fare clic su **EIGRP** nel menu a sinistra.
Fare clic su **Enable EIGRP**.
Assegnare il **numero AS** (1-65535).
Selezionare una **rete/host**. È possibile selezionare un oggetto creato in precedenza dall'elenco 'Rete/host disponibile' oppure creare un nuovo oggetto facendo clic sul pulsante più (**+**).
Fare clic su Save (Salva).



Convalida

Di seguito sono riportati i requisiti minimi per l'adiacenza del router adiacente EIGRP:

- Il numero AS deve corrispondere.
- L'interfaccia deve essere attiva e raggiungibile.
- È buona norma che i timer Hello e Hold corrispondano.
- I valori K devono corrispondere.
- Nessun elenco degli accessi deve bloccare il traffico EIGRP.

Convalida tramite CLI

- show run router eigrp
- mostra router adiacenti eigrp
- show eigrp topology
- show eigrp interfaces
- show route eigrp
- mostra traffico eigrp
- debug ip eigrp neighbors
- debug eigrp packets

firepower# show run router eigrp

router eigrp 1

nessuna informazione predefinita in

nessuna informazione predefinita in uscita

no eigrp log-neighbor-warnings

no eigrp log-neighbor-changes

rete 192.168.193.0 255.255.255.0

```
 rete 172.16.193.8 255.255.255.248
firepower#
firepower# mostra router adiacenti eigrp
Adiacenti EIGRP-IPv4 per AS(1)
H Interfaccia indirizzo Tempo di attesa Tempo di attesa SRTT Q Seq
                                        (sec) (ms) Cnt Num
0 192.168.193.121 fuori dalle 14 21:45:04 40 240 0 30
firepower# mostra topologia eigrp
Tabella della topologia EIGRP-IPv4 per AS(1)/ID(192.168.193.121)
Codici: P - Passivo, A - Attivo, U - Aggiornamento, Q - Query, R - Risposta,
       r - stato risposta, s - stato sia
P 192.168.193.0 255.255.255.0, 1 successore, DF 512
        tramite Connesso, esterno
P 172.16.193.0 255.255.255.248, 1 successore, DF è 768
        via 192.168.193.116 (768/512), esterno
P 172.16.193.8 255.255.255.248, 1 successore, DF 512
        tramite Connesso, interno
firepower# mostra interfacce eigrp
Interfacce EIGRP-IPv4 per AS(1)
                    Tempo medio coda Xmit per multicast in sospeso
Peer di interfaccia Un/Affidabile SRTT Un/Affidabile Flusso Timer Routing
esterno 1 0 / 0 10 0 / 1 50 0
interno 0 / 0 0 0 / 1 0 0
firepower#

firepower# show route eigrp
Codici: L - locale, connesso tramite C, S - statico, R - RIP, M - mobile, B - BGP
```

D - EIGRP, EX - EIGRP esterno, O - OSPF, IA - OSPF interarea

N1 - Tipo esterno NSSA OSPF 1, N2 - Tipo esterno NSSA OSPF 2

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

i - IS-IS, su - IS-IS riepilogo, L1 - IS-IS livello-1, L2 - IS livello-2

ia - IS-IS inter area, * - valore predefinito candidato, U - route statica per utente

o - ODR, P - route statica scaricata periodicamente, + - route replicata

SI - Static InterVRF, BI - BGP InterVRF

Gateway di ultima istanza è 192.168.193.254 alla rete 0.0.0.0

D 172.16.193.0 255.255.255.248

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

firepower# show route

Codici: L - locale, connesso tramite C, S - statico, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP esterno, O - OSPF, IA - OSPF interarea

N1 - Tipo esterno NSSA OSPF 1, N2 - Tipo esterno NSSA OSPF 2

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

i - IS-IS, su - IS-IS riepilogo, L1 - IS-IS livello-1, L2 - IS livello-2

ia - IS-IS inter area, * - valore predefinito candidato, U - route statica per utente

o - ODR, P - route statica scaricata periodicamente, + - route replicata

SI - Static InterVRF, BI - BGP InterVRF

Gateway di ultima istanza è 192.168.193.254 alla rete 0.0.0.0

S* 0.0.0.0 0.0.0.0 [1/0] tramite 192.168.193.254, all'esterno

D 172.16.193.0 255.255.255.248

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

C 172.16.193.8 255.255.255.248 è collegata direttamente, all'interno

L 172.16.193.14.255.255.255.255 è collegato direttamente, all'interno

C 192.168.193.0 255.255.255.0 è collegato direttamente, all'esterno

L 192.168.193.121 255.255.255.255 è collegato direttamente, all'esterno

```
firepower#

firepower# mostra traffico eigrp

Statistiche del traffico EIGRP-IPv4 per AS(1)

  Hellos inviati/ricevuti: 4006/4001

  Aggiornamenti inviati/ricevuti: 4/4

  Query inviate/ricevute: 0/0

  Risposte inviate/ricevute: 0/0

  Ack inviati/ricevuti: 3/2

  Query SIA inviate/ricevute: 0/0

  Risposte SIA inviate/ricevute: 0/0

  ID processo Hello: 2503149568

  ID processo PDM: 2503150496

  Coda socket:

  Coda di input: 0/2000/2/0 (corrente/max/massima/cadute)

firepower#
```

Risoluzione dei problemi

Scenario 1 - Debug del router adiacente IP EIGRP

I comandi di debug possono essere utilizzati per osservare i cambiamenti degli stati dei router adiacenti.

```
firepower# debug ip eigrp neighbors

firepower#

EIGRP: Tempo di attesa scaduto

Discesa: Peer 192.168.193.121 total=0 stub, iidb-stub=0 id-all=0

EIGRP: Gestisci errore di deallocazione [0]

EIGRP: Il router adiacente 192.168.193.121 è andato giù all'esterno
```

Eseguire il comando show eigrp neighbors per convalidare lo stato dei router adiacenti tra i FTD.

firepower# mostra router adiacenti eigrp

Adiacenti EIGRP-IPv4 per AS(1)

Verificare lo stato delle interfacce con il comando show interface ip brief. Si noti che l'interfaccia Gigabit Ethernet 0/1 è disattivata a livello amministrativo.

firepower# show interface ip brief

Interface IP-Address (Indirizzo IP interfaccia) OK? Protocollo di stato del metodo

Gigabit Ethernet0/0 172.16.193.14 YES CONFIGURAZIONE

Gigabit Ethernet0/1 192.168.193.121 YES CONFIG disattivato a livello amministrativo

Gigabit Ethernet0/2 192.168.194.24 SÌ manuale attivo

Controllo interno0/0 127.0.1.1 SÌ non impostato

Controllo interno0/1 non assegnato SÌ non impostato

Dati interni0/0 non assegnati SÌ non impostato attivo

Dati interni0/0 non assegnati SÌ non impostato

Internal-Data0/1 169.254.1.1 SÌ non impostato

Dati interni0/2 non assegnati SÌ non impostato

Management0/0 203.0.113.130 SÌ disinstallazione

Scenario 2 - Autenticazione

L'FTD supporta l'algoritmo hash MD5 per autenticare i pacchetti EIGRP. Per impostazione predefinita, questa autenticazione è disabilitata.

Per abilitare l'algoritmo hash MD5, selezionare la casella di controllo 'Autenticazione MD5'. È fondamentale che le impostazioni di autenticazione corrispondano su entrambi i dispositivi; se questa opzione è attivata su un dispositivo ma non sull'altro, le adiacenze adiacenti non possono formarsi tra di essi.

Verificare la configurazione utilizzando i pacchetti debug eigrp.

firepower# debug eigrp packets

(UPDATE, REQUEST, QUERY, REPLY, HELLO, IPXSAP, PROBE, ACK, STUB, SIAREPLY)
Debug dei pacchetti EIGRP attivato

firepower#

EIGRP: esterno: pacchetto ignorato da 192.168.193.121, opcode = 5 (autenticazione disattivata o

catena di chiavi mancante)

EIGRP: Ricevuto HELLO su esterno nbr 172.16.193.14

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

EIGRP: Invio di HELLO all'esterno

AS 1, Flag 0x0:(NULL), Seq 0/0 interfaceQ 0/0 idbQ un/relay 0/0

EIGRP: Invio di HELLO all'interno

AS 1, Flag 0x0:(NULL), Seq 0/0 interfaceQ 0/0 idbQ un/relay 0/0

EIGRP: esterno: pacchetto ignorato da 192.168.193.121, opcode = 5 (autenticazione disattivata o catena di chiavi mancante)

EIGRP: Ricevuto HELLO su esterno nbr 172.16.193.14

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

EIGRP: Invio di HELLO all'interno

AS 1, Flag 0x0:(NULL), Seq 0/0 interfaceQ 0/0 idbQ un/relay 0/0

EIGRP: Invio di HELLO all'esterno

AS 1, Flag 0x0:(NULL), Seq 0/0 interfaceQ 0/0 idbQ un/relay 0/0

EIGRP: esterno: pacchetto ignorato da 192.168.193.121, opcode = 5 (autenticazione disattivata o catena di chiavi mancante).

È possibile osservare un messaggio che indica che l'autenticazione è disattivata o che la catena di chiavi è mancante. In questo scenario questo si verifica in genere quando l'autenticazione è abilitata su un peer ma non sull'altro.

EIGRP: esterno: pacchetto ignorato da 192.168.193.121, opcode = 5 (autenticazione disattivata o catena di chiavi mancante).

Verificare con show run interface <interfaccia EIGRP>.

Firepower1# show run interface Gigabit Ethernet0/1

!

interfaccia Gigabit Ethernet0/1

nameif esterno

livello di protezione 0

indirizzo ip 192.168.193.121.255.255.255.0

chiave di autenticazione eigrp 1 ***** key-id 10

modalità di autenticazione eigrp 1 md5

Firepower2# show run interface Gigabit Ethernet0/1

!

interfaccia Gigabit Ethernet0/1

nameif esterno

livello di protezione 0

indirizzo ip 192.168.193.116.255.255.255.0

Scenario 3 - Interfacce passive

Quando si configura il protocollo EIGRP, i pacchetti di saluto EIGRP vengono in genere inviati e ricevuti sulle interfacce in cui è abilitata la rete.

Tuttavia, se un'interfaccia è configurata come passiva, il protocollo EIGRP interrompe lo scambio di pacchetti hello tra due router sull'interfaccia, causando la perdita di adiacenze con i router adiacenti. Di conseguenza, questa azione non solo impedisce al router di annunciare gli aggiornamenti del routing dall'interfaccia, ma impedisce anche al router di ricevere gli aggiornamenti del routing dall'interfaccia.

Eseguire il comando show eigrp neighbors per convalidare lo stato dei router adiacenti tra i FTD.

router adiacenti firepower# show eigrp

Adiacenti EIGRP-IPv4 per AS(1)

Per verificare i pacchetti EIGRP inviati e le interfacce usate, usare il comando debug eigrp packets.

FTD

Firepower1#

(UPDATE, REQUEST, QUERY, REPLY, HELLO, IPXSAP, PROBE, ACK, STUB, SIAREPLY)
Debug dei pacchetti EIGRP attivato

firepower#

EIGRP: Invio di HELLO all'esterno

AS 1, Flag 0x0:(NULL), Seq 0/0 interfaceQ 0/0 idbQ un/relay 0/0

EIGRP: Invio di HELLO all'interno

AS 1, Flag 0x0:(NULL), Seq 0/0 interfaceQ 0/0 idbQ un/relay 0/0

EIGRP: Invio di HELLO all'esterno

AS 1, Flag 0x0:(NULL), Seq 0/0 interfaceQ 0/0 idbQ un/relay 0/0

EIGRP: Invio di HELLO all'interno

AS 1, Flag 0x0:(NULL), Seq 0/0 interfaceQ 0/0 idbQ un/relay 0/0

EIGRP: Invio di HELLO all'esterno

FTD

Firepower2# pacchetti debug eigrp

(UPDATE, REQUEST, QUERY, REPLY, HELLO, IPXSAP, PROBE, ACK, STUB, SIAREPLY)
Debug dei pacchetti EIGRP attivato

Firepower2#

In questo scenario, FTD 2 non invia messaggi di saluto EIGRP perché le relative interfacce interna ed esterna sono configurate come passive. Verificare questa condizione con il comando show run router eigrp.

Firepower2# show run router eigrp

router eigrp 1

nessuna informazione predefinita in

nessuna informazione predefinita in uscita

no eigrp log-neighbor-warnings

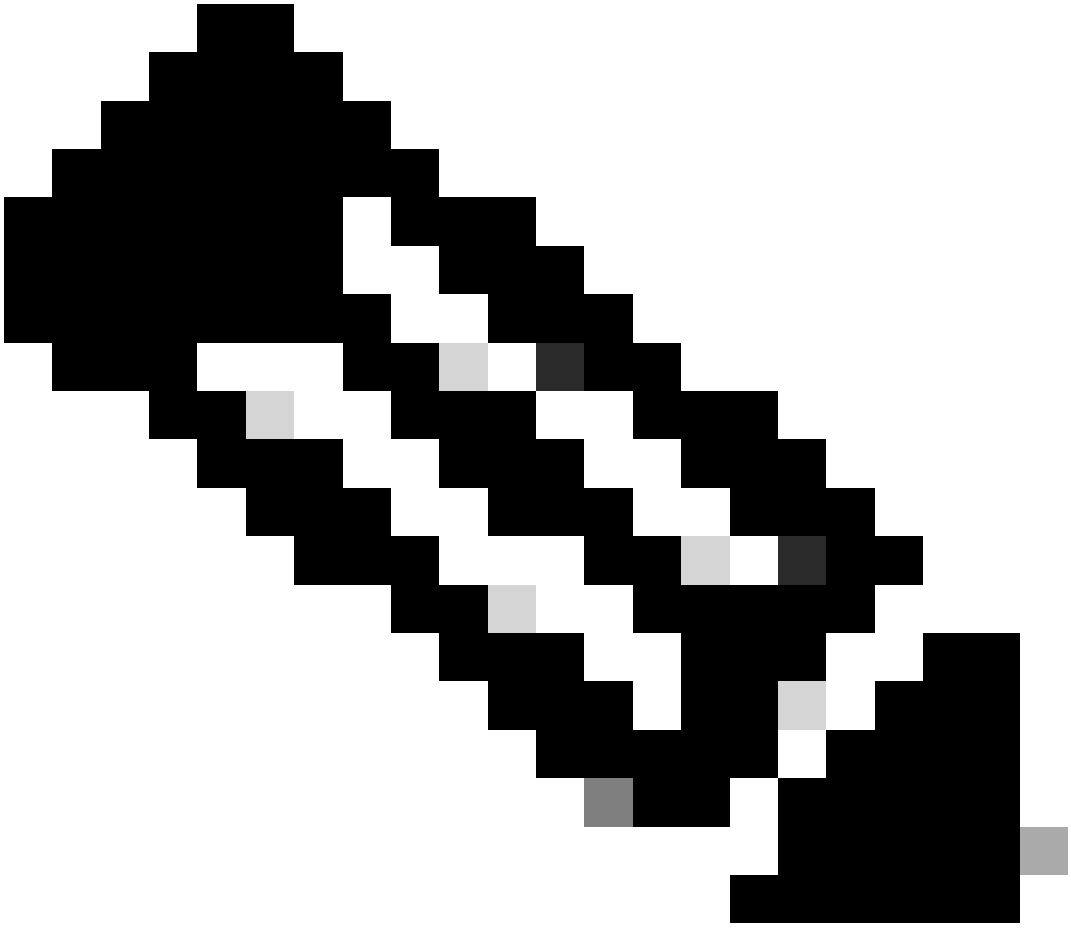
no eigrp log-neighbor-changes

rete 192.168.193.0 255.255.255.0

rete 172.16.193.8 255.255.255.248

interfaccia passiva esterna

interno di interfaccia passiva



Nota: Per arrestare tutti i processi di debug configurati, usare il comando undebug all.

Informazioni correlate

- EIGRP su dispositivi FTD
- Configura EIGRP su FTD
- Metriche dei costi compositi EIGRP

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).