Dépannage du protocole EIGRP sur les périphériques FTD gérés par FMC

Table des matières

Introduction

Ce document décrit comment vérifier et dépanner la configuration EIGRP sur FTD géré par FMC.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

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

Composants utilisés

- FTDv dans la version 7.4.2.
- FMCv dans la version 7.4.2.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

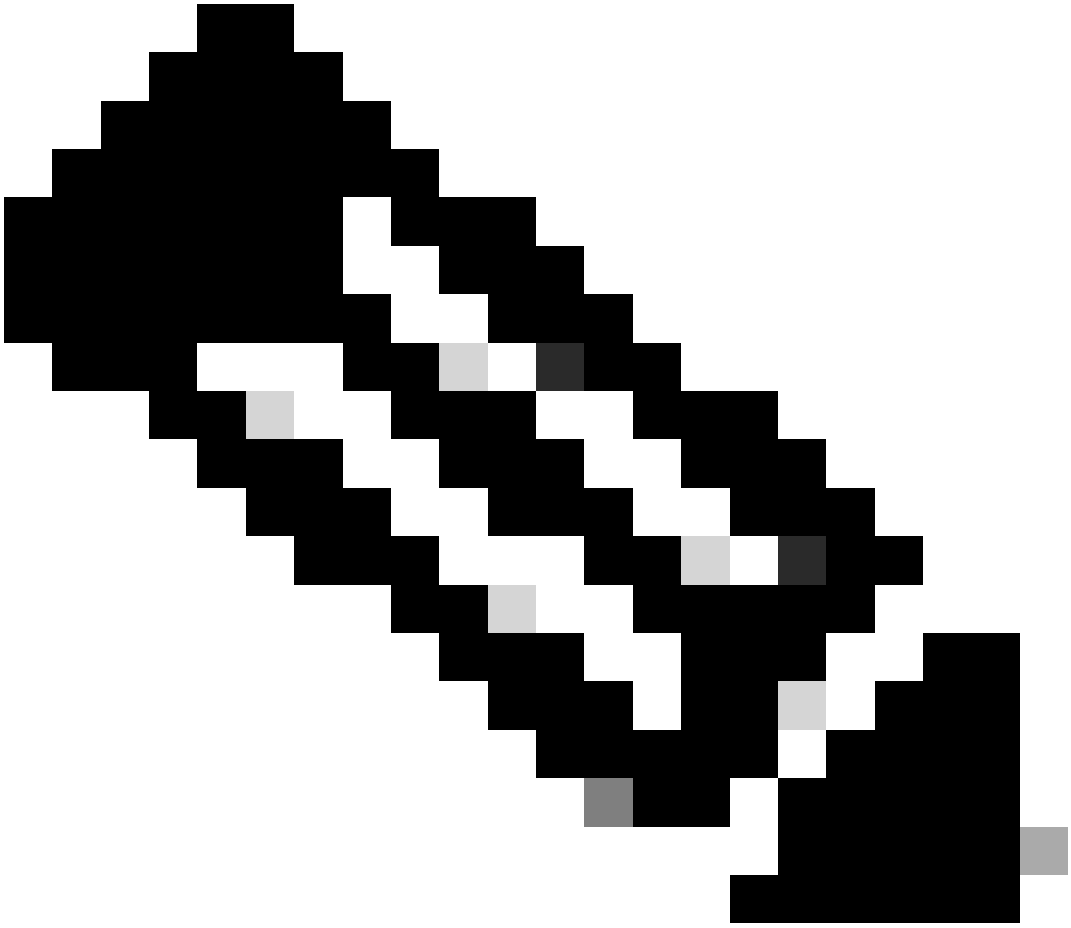
Informations générales

Le protocole EIGRP est un protocole de routage à vecteur de distance avancé qui combine les fonctionnalités des protocoles à vecteur de distance et à état de liens. Il offre une convergence rapide en conservant les informations de routage des voisins, ce qui permet une adaptation rapide aux routes alternatives. Le protocole EIGRP est efficace, car il utilise des mises à jour déclenchées partielles pour les modifications de routage ou de métrique au lieu de mises à jour complètes périodiques.
Pour la communication, le protocole EIGRP fonctionne directement sur la couche IP (protocole 88) et utilise le protocole RTP (Reliable Transport Protocol) pour la livraison de paquets ordonnée et garantie. Il prend en charge la multidiffusion et la monodiffusion, avec des messages Hello utilisant spécifiquement les adresses de multidiffusion 224.0.0.10 ou FF02::A.
Le fonctionnement du protocole EIGRP repose fondamentalement sur les informations stockées dans trois tables :

- Table de voisinage : Cette table tient à jour un enregistrement des périphériques EIGRP connectés directement avec lesquels une contiguïté a été établie avec succès.
- Table topologique : Cette table stocke toutes les routes apprises annoncées par les voisins, y compris tous les chemins possibles vers une destination spécifique et leurs métriques associées, permettant une évaluation de leur qualité et du nombre de chemins disponibles.
- Table de routage : Cette table contient le meilleur chemin pour chaque destination, appelé « successeur ». Cette route successeur est celle qui est activement utilisée pour transférer le trafic et qui est ensuite annoncée aux autres voisins EIGRP.

Le protocole EIGRP utilise des pondérations de métriques, appelées valeurs K, dans les calculs de routage et de métriques afin de déterminer le chemin optimal vers une destination. Cette valeur métrique est dérivée d'une formule qui utilise des paramètres :

- Bande passante
- Délai D'Attente
- Fiabilité
- Chargement
- MTU



Remarque : Dans le cas d'un lien métrique entre plusieurs chemins, l'unité de transmission maximale (MTU) est utilisée comme un point de rupture, une valeur MTU plus élevée étant préférée.

- Route successeur : Il s'agit du meilleur chemin vers une destination spécifique. Il s’agit de la route qui est finalement installée dans la table de routage.
- Distance de faisabilité (FD) : Il s’agit de la mesure la mieux calculée pour atteindre un sous-réseau particulier du point de vue du routeur local.
- Distance annoncée (RD) / Distance annoncée (AD) : Il s’agit de la distance (métrique) vers un sous-réseau spécifique tel que signalé par un voisin. Pour qu’un chemin soit considéré comme un successeur potentiel, la distance annoncée par rapport au voisin doit être inférieure à la distance de faisabilité du routeur local vers cette même destination.
- Successeur potentiel (FS) : Il s’agit d’un chemin de secours vers une destination, fournissant une route alternative en cas de défaillance de la route successeur principale. Un chemin est

considéré comme successeur potentiel si sa distance annoncée (par rapport au voisin annonceur) est strictement inférieure à la distance de faisabilité de la route successeur actuelle vers la même destination.

Diagramme du réseau

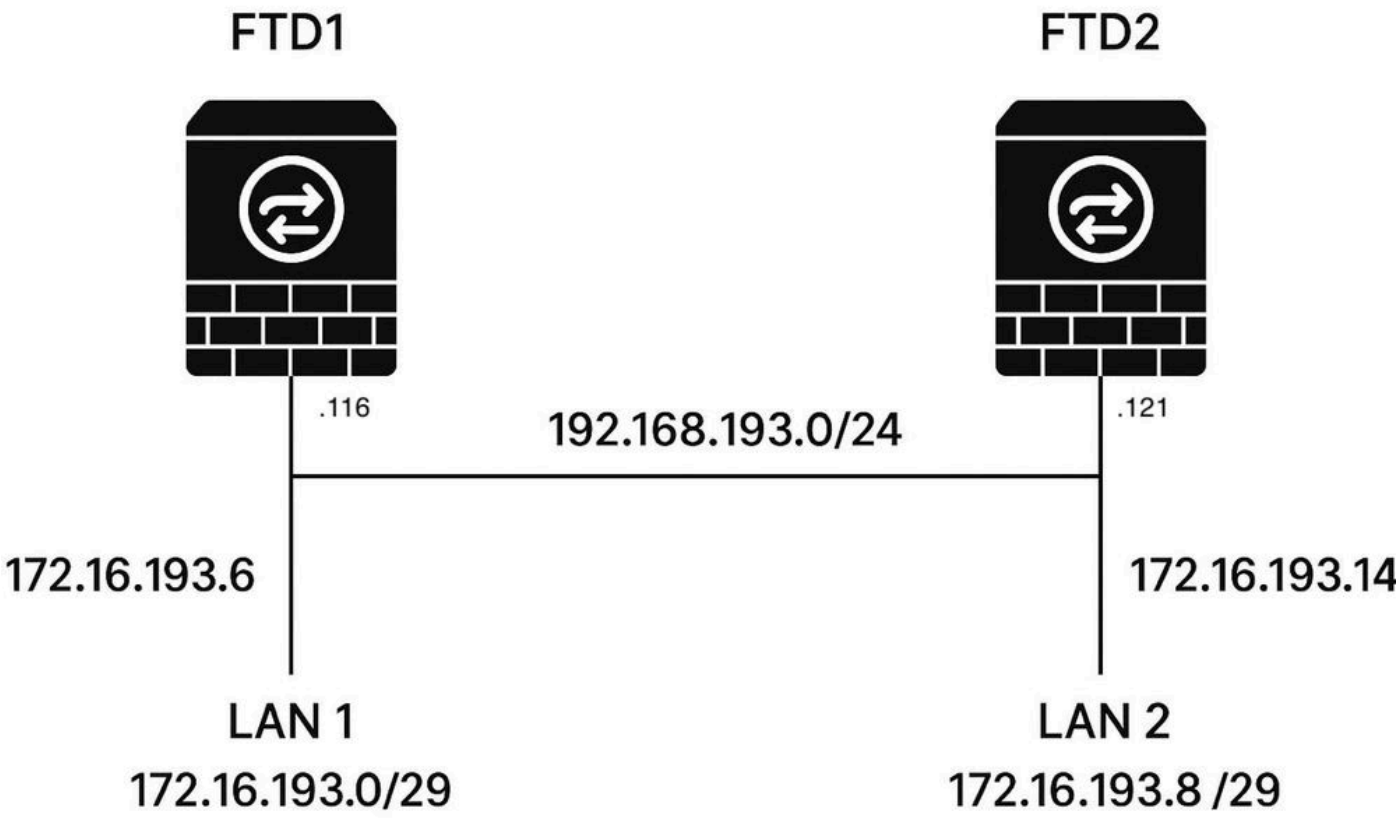
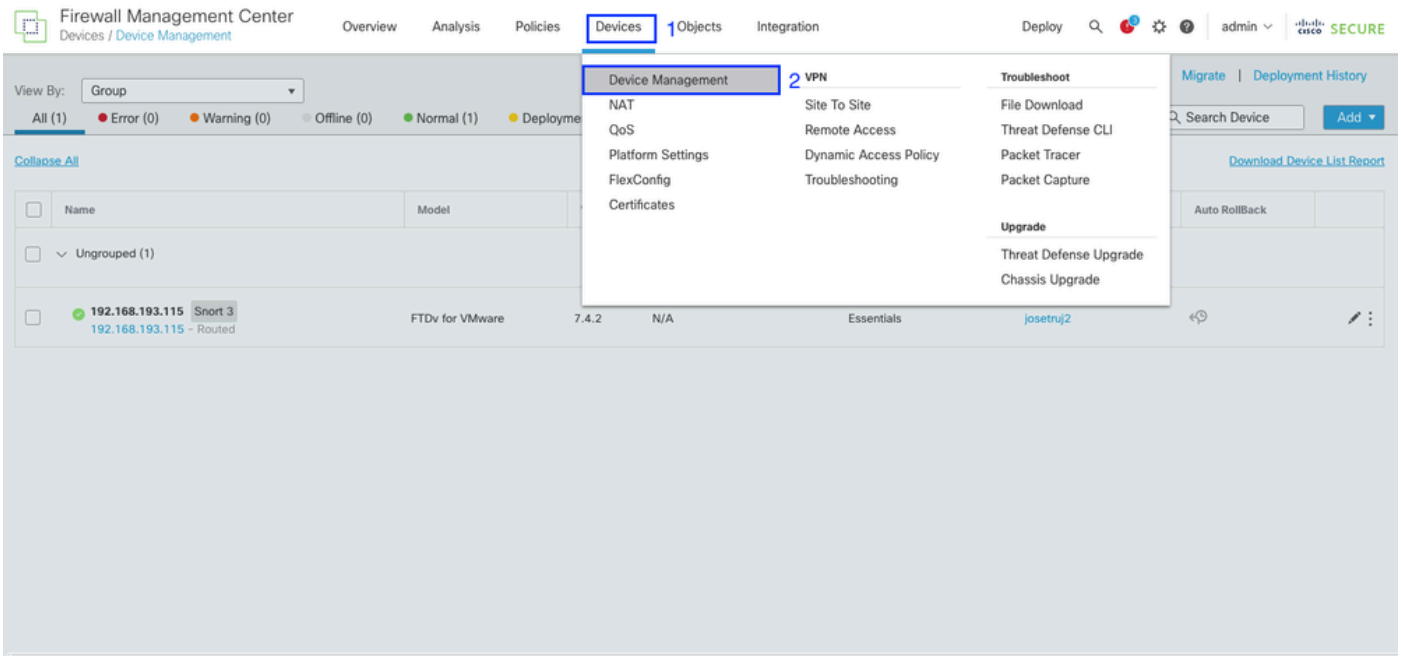


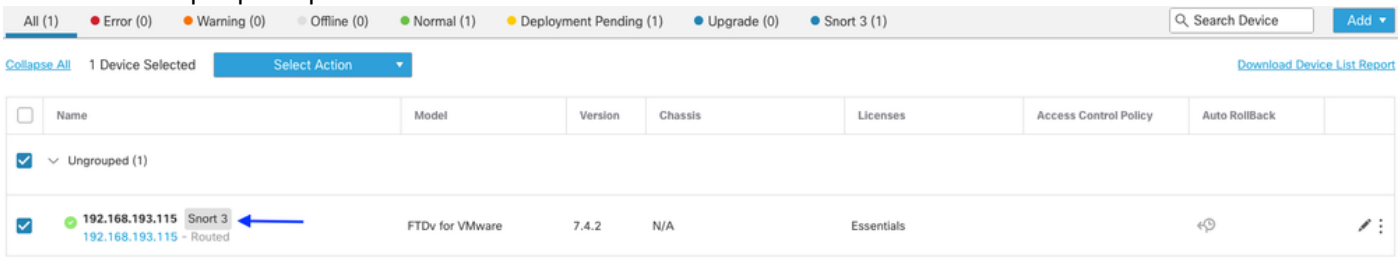
Diagramme du réseau

Configuration de base

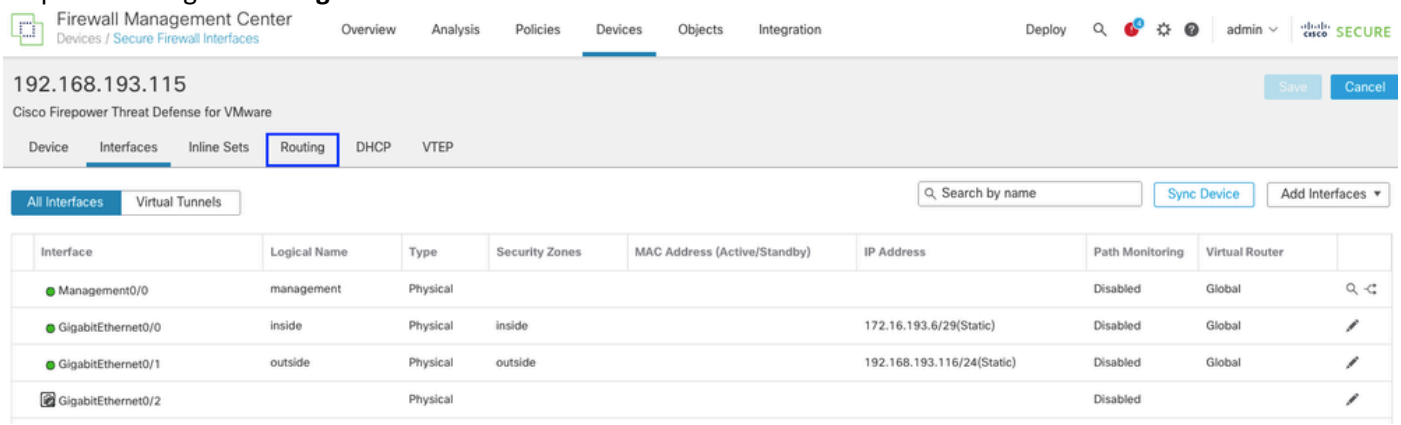
Accédez à **Devices > Device Management** :



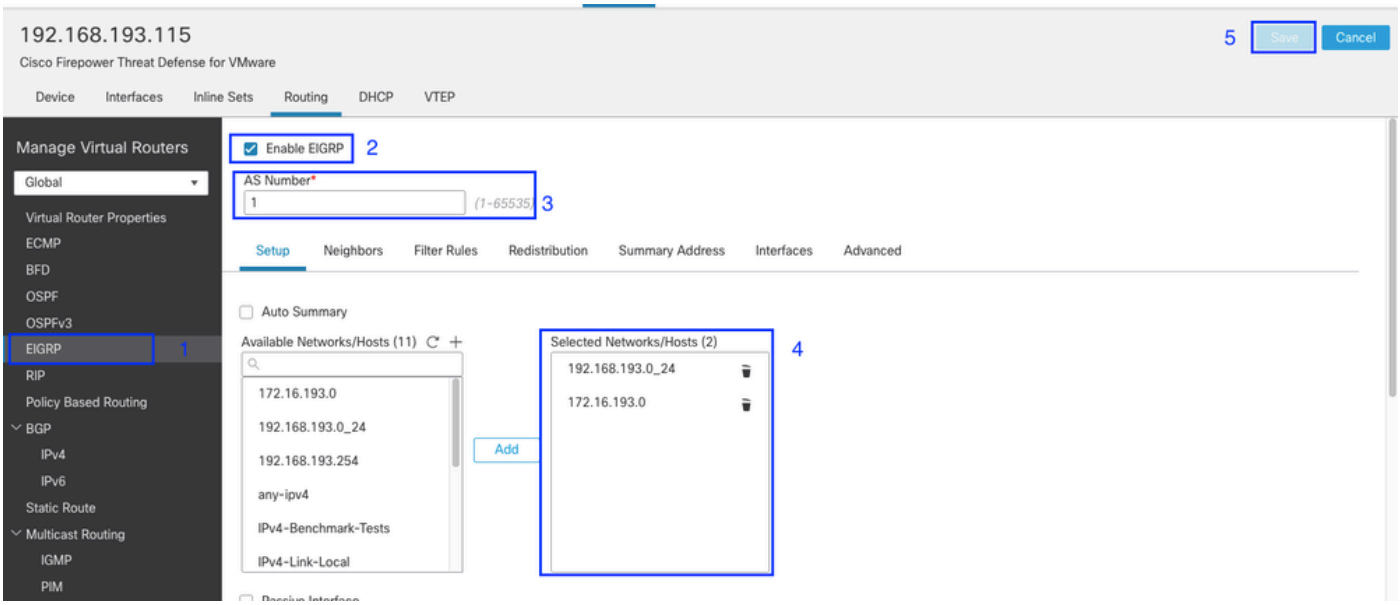
Sélectionner le périphérique :



Cliquez sur l'onglet **Routing**.



Cliquez sur **EIGRP** dans le menu de gauche.
Cliquez sur **Enable** EIGRP.
Attribuez le **numéro AS** (1-65535).
Sélectionnez un **réseau/hôte**. Vous pouvez soit sélectionner un objet précédemment créé dans la liste « Réseau/Hôte disponible », soit créer un nouvel objet en cliquant sur le bouton plus (**+**).
Cliquez sur Save.



Validation

Voici la configuration minimale requise pour la contiguïté de voisinage EIGRP :

- Le numéro de système autonome doit correspondre.
- L'interface doit être active et accessible.
- Il est recommandé de faire correspondre les minuteurs Hello et Hold.
- Les valeurs K doivent correspondre.
- Aucune liste d'accès ne doit bloquer le trafic EIGRP.

Validation via 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

routeur eigrp 1

no default-information in

no default-information out

no eigrp log-neighbor-warnings

no eigrp log-neighbor-changes

réseau 192.168.193.0 255.255.255.0

```
 réseau 172.16.193.8 255.255.255.248

firepower#

firepower# show eigrp neighbors

Voisins EIGRP-IPv4 pour AS(1)

H Address Interface Hold Uptime SRTT RTO Q Seq

                                    (sec) (ms) Num. cit.

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

firepower# show eigrp topology

Table topologique EIGRP-IPv4 pour AS(1)/ID(192.168.193.121)

Codes : P - Passif, A - Actif, U - Mise à jour, Q - Requête, R - Réponse,

       r - reply Status, s - sia Status

P 192.168.193.0 255.255.255.0, 1 successeurs, FD = 512

        via Connecté, extérieur

P 172.16.193.0 255.255.255.248, 1 successeurs, FD = 768

        via 192.168.193.116 (768/512), externe

P 172.16.193.8 255.255.255.248, 1 successeurs, FD = 512

        via Connecté, à l'intérieur

firepower# show eigrp interfaces

Interfaces EIGRP-IPv4 pour AS(1)

                    File d'attente Xmit Durée moyenne de régulation Multicast en attente

Homologues d’interface Routages de temporisateur de flux non fiables SRTT

extérieur 1 0 / 0 10 0 / 1 50 0

intérieur 0 0 / 0 0 / 1 0 0

firepower#

firepower# show route eigrp

Codes : L - local, C - connecté, S - statique, R - RIP, M - mobile, B - BGP
```

D - EIGRP, EX - EIGRP externe, O - OSPF, IA - OSPF inter-zone

N1 - OSPF NSSA de type externe 1, N2 - OSPF NSSA de type externe 2

E1 - OSPF de type externe 1, E2 - OSPF de type externe 2, V - VPN

i - IS-IS, su - Résumé IS-IS, L1 - IS-IS niveau 1, L2 - IS-IS niveau 2

ia - IS-IS inter-zone, * - candidat default, U - route statique par utilisateur

o - ODR, P - route statique téléchargée périodiquement, + - route répliquée

SI - InterVRF statique, BI - BGP InterVRF

La passerelle de dernier recours est 192.168.193.254 vers le réseau 0.0.0.0

D 172.16.193.0 255.255.255.248

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

firepower# show route

Codes : L - local, C - connecté, S - statique, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP externe, O - OSPF, IA - OSPF inter-zone

N1 - OSPF NSSA de type externe 1, N2 - OSPF NSSA de type externe 2

E1 - OSPF de type externe 1, E2 - OSPF de type externe 2, V - VPN

i - IS-IS, su - Résumé IS-IS, L1 - IS-IS niveau 1, L2 - IS-IS niveau 2

ia - IS-IS inter-zone, * - candidat default, U - route statique par utilisateur

o - ODR, P - route statique téléchargée périodiquement, + - route répliquée

SI - InterVRF statique, BI - BGP InterVRF

La passerelle de dernier recours est 192.168.193.254 vers le réseau 0.0.0.0

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

D 172.16.193.0 255.255.255.248

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

C 172.16.193.8 255.255.255.248 est directement connecté, à l'intérieur

L 172.16.193.14 255.255.255.255 est directement connecté, à l'intérieur

C 192.168.193.0 255.255.255.0 est directement connecté, à l'extérieur

L 192.168.193.121 255.255.255.255 est directement connecté, à l'extérieur

```
firepower#

firepower# show eigrp traffic

Statistiques de trafic EIGRP-IPv4 pour AS(1)

  Hello envoyés/reçus : 4006/4001

  Mises à jour envoyées/reçues : 4/4

  Requêtes envoyées/reçues : 0/0

  Réponses envoyées/reçues : 0/0

  Accusés de réception envoyés/reçus : 3/2

  Requêtes SIA envoyées/reçues : 0/0

  Réponses SIA envoyées/reçues : 0/0

  ID du processus Hello : 2503149568

  ID de processus PDM : 2503150496

  File d'attente de socket :

  File d'attente : 0/2000/2/0 (courant/max/maximum/pertes)

firepower#
```

Dépannage

Scénario 1 : débogage du voisin IP EIGRP

Les commandes de débogage peuvent être utilisées pour observer tout changement dans les états de voisinage.

```
firepower# debug ip eigrp neighbor

firepower#

EIGRP : Durée de conservation expirée

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

EIGRP : Gérer l'échec de désaffectation [0]

EIGRP : Le voisin 192.168.193.121 est tombé en panne à l'extérieur
```

Exécutez la commande show eigrp neighbors pour valider l'état du voisin entre les FTD.

firepower# show eigrp neighbors

Voisins EIGRP-IPv4 pour AS(1)

Vérifiez l'état des interfaces en utilisant la commande show interface ip brief. Vous pouvez constater que l'interface GigabitEthernet0/1 est désactivée sur le plan administratif.

firepower# show interface ip brief

Interface IP-Address OK ? protocole d'état de méthode

GigabitEthernet0/0 172.16.193.14 OUI CONFIG up

GigabitEthernet0/1 192.168.193.121 OUI CONFIGURATION administrativement désactivée

GigabitEthernet0/2 192.168.194.24 OUI manuel up up

Internal-Control0/0 127.0.1.1 OUI non configuré

Internal-Control0/1 non affecté OUI non configuré

Internal-Data0/0 non assigné OUI non configuré désactivé

Internal-Data0/0 non affecté OUI non configuré

Internal-Data0/1 169.254.1.1 OUI non configuré

Internal-Data0/2 non affecté OUI non configuré

Management0/0 203.0.113.130 OUI non configuré

Scénario 2 - Authentification

Le FTD prend en charge l’algorithme de hachage MD5 pour authentifier les paquets EIGRP. Par défaut, cette authentification est désactivée.

Pour activer l'algorithme de hachage MD5, cochez la case « Authentification MD5 ». Il est essentiel que les paramètres d'authentification correspondent sur les deux périphériques ; si cette option est activée sur un périphérique mais pas sur l'autre, la contiguïté de voisinage ne peut pas se former entre eux.

Vérifiez cette configuration en utilisant debug eigrp packets.

firepower# debug eigrp packets

(UPDATE, REQUEST, QUERY, REPLY, HELLO, IPXSAP, PROBE, ACK, STUB, SIAQUERY, SIAREPLY)Le débogage des paquets EIGRP est activé

firepower#

EIGRP : extérieur : paquet ignoré de 192.168.193.121, opcode = 5 (authentification désactivée ou

chaîne de clés manquante)

EIGRP : Reçu HELLO sur le numéro externe 172.16.193.14

AS 1, indicateurs 0x0 : (NULL), interface Seq 0/0Q 0/0

EIGRP : Envoi d'HELLO à l'extérieur

AS 1, indicateurs 0x0:(NULL), interface Seq 0/0Q 0/0 iidbQ un/rely 0/0

EIGRP : Envoi de HELLO à l'intérieur

AS 1, indicateurs 0x0:(NULL), interface Seq 0/0Q 0/0 iidbQ un/rely 0/0

EIGRP : extérieur : paquet ignoré de 192.168.193.121, opcode = 5 (authentification désactivée ou chaîne de clés manquante)

EIGRP : Reçu HELLO sur le numéro externe 172.16.193.14

AS 1, indicateurs 0x0 : (NULL), interface Seq 0/0Q 0/0

EIGRP : Envoi de HELLO à l'intérieur

AS 1, indicateurs 0x0:(NULL), interface Seq 0/0Q 0/0 iidbQ un/rely 0/0

EIGRP : Envoi d'HELLO à l'extérieur

AS 1, indicateurs 0x0:(NULL), interface Seq 0/0Q 0/0 iidbQ un/rely 0/0

EIGRP : extérieur : paquet ignoré de 192.168.193.121, opcode = 5 (authentification désactivée ou chaîne de clés manquante).

Vous pouvez observer un message indiquant que l'authentification est désactivée ou que la chaîne de clés est manquante. Dans ce scénario, cela se produit généralement lorsque l'authentification est activée sur un homologue mais pas sur l'autre.

EIGRP : extérieur : paquet ignoré de 192.168.193.121, opcode = 5 (authentification désactivée ou chaîne de clés manquante).

Vérifiez avec show run interface <interface EIGRP>.

Firepower1# show run interface GigabitEthernet0/1

!

interface GigabitEthernet0/1

nameif outside

niveau de sécurité 0

adresse ip 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

niveau de sécurité 0

adresse ip 192.168.193.116 255.255.255.0

Scénario 3 - Interfaces passives

Lorsque le protocole EIGRP est configuré, les paquets Hello EIGRP sont généralement envoyés et reçus sur les interfaces où le réseau est activé.

Cependant, si une interface est configurée comme passive, le protocole EIGRP supprime l'échange de paquets Hello entre deux routeurs sur cette interface, ce qui entraîne la perte de contiguïté de voisinage. Par conséquent, cette action empêche non seulement le routeur d'annoncer les mises à jour de routage à partir de cette interface, mais l'empêche également de recevoir les mises à jour de routage à partir de cette interface.

Exécutez la commande show eigrp neighbors pour valider l'état du voisin entre les FTD.

firepower# show eigrp neighbors

Voisins EIGRP-IPv4 pour AS(1)

Vous pouvez vérifier les paquets EIGRP envoyés et les interfaces par lesquelles ils sont envoyés à l'aide de la commande debug eigrp packets.

Durée de vie 1

Firepower1#

(UPDATE, REQUEST, QUERY, REPLY, HELLO, IPXSAP, PROBE, ACK, STUB, SIAQUERY, SIAREPLY)Le débogage des paquets EIGRP est activé

firepower#

EIGRP : Envoi d'HELLO à l'extérieur

AS 1, indicateurs 0x0:(NULL), interface Seq 0/0Q 0/0 iidbQ un/rely 0/0

EIGRP : Envoi de HELLO à l'intérieur

AS 1, indicateurs 0x0:(NULL), interface Seq 0/0Q 0/0 iidbQ un/rely 0/0

EIGRP : Envoi d'HELLO à l'extérieur

AS 1, indicateurs 0x0:(NULL), interface Seq 0/0Q 0/0 iidbQ un/rely 0/0

EIGRP : Envoi de HELLO à l'intérieur

AS 1, indicateurs 0x0:(NULL), interface Seq 0/0Q 0/0 iidbQ un/rely 0/0

EIGRP : Envoi d'HELLO à l'extérieur

Durée de vie 2

Firepower2# debug eigrp packets

(UPDATE, REQUEST, QUERY, REPLY, HELLO, IPXSAP, PROBE, ACK, STUB, SIAQUERY, SIAREPLY)Le débogage des paquets EIGRP est activé

Firepower2#

Dans ce scénario, FTD 2 n'envoie pas de messages Hello EIGRP car ses interfaces interne et externe sont configurées comme passives. Pour le vérifier, utilisez la commande show run router eigrp.

Firepower2# show run router eigrp

routeur eigrp 1

no default-information in

no default-information out

no eigrp log-neighbor-warnings

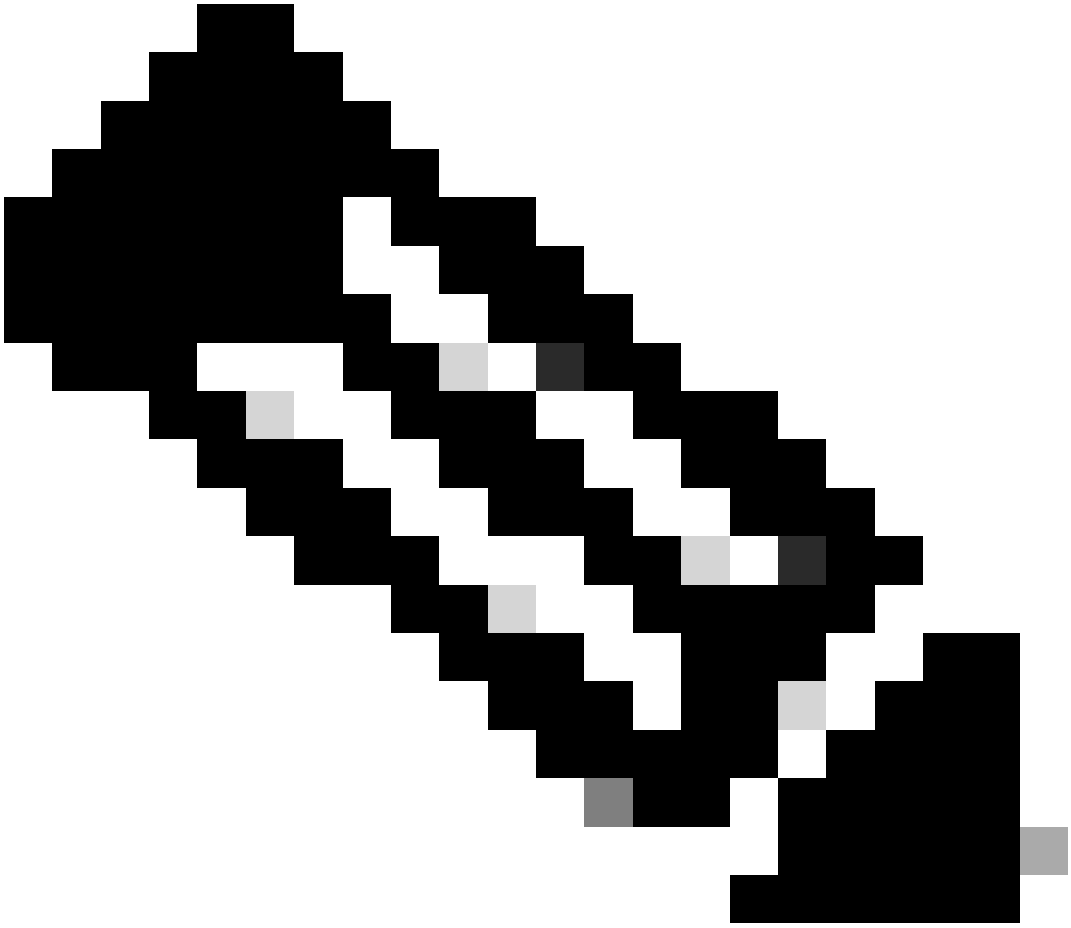
no eigrp log-neighbor-changes

réseau 192.168.193.0 255.255.255.0

réseau 172.16.193.8 255.255.255.248

passive-interface outside

passive-interface inside



Remarque : Afin d'arrêter tous les processus de débogage configurés, veuillez utiliser la commande undebug all.

Informations connexes

- EIGRP sur les périphériques FTD
- Configuration du protocole EIGRP sur FTD
- Mesures de coût composites EIGRP

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.