FMCによって管理されるFTDデバイスでのEIGRPのトラブルシューティング

内容

はじめに

このドキュメントでは、FMCによって管理されるFTDのEIGRP設定を確認し、トラブルシューティングする方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

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

使用するコンポーネント

- バージョン7.4.2のFTDv。
- バージョン7.4.2のFMCv

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始していま

す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

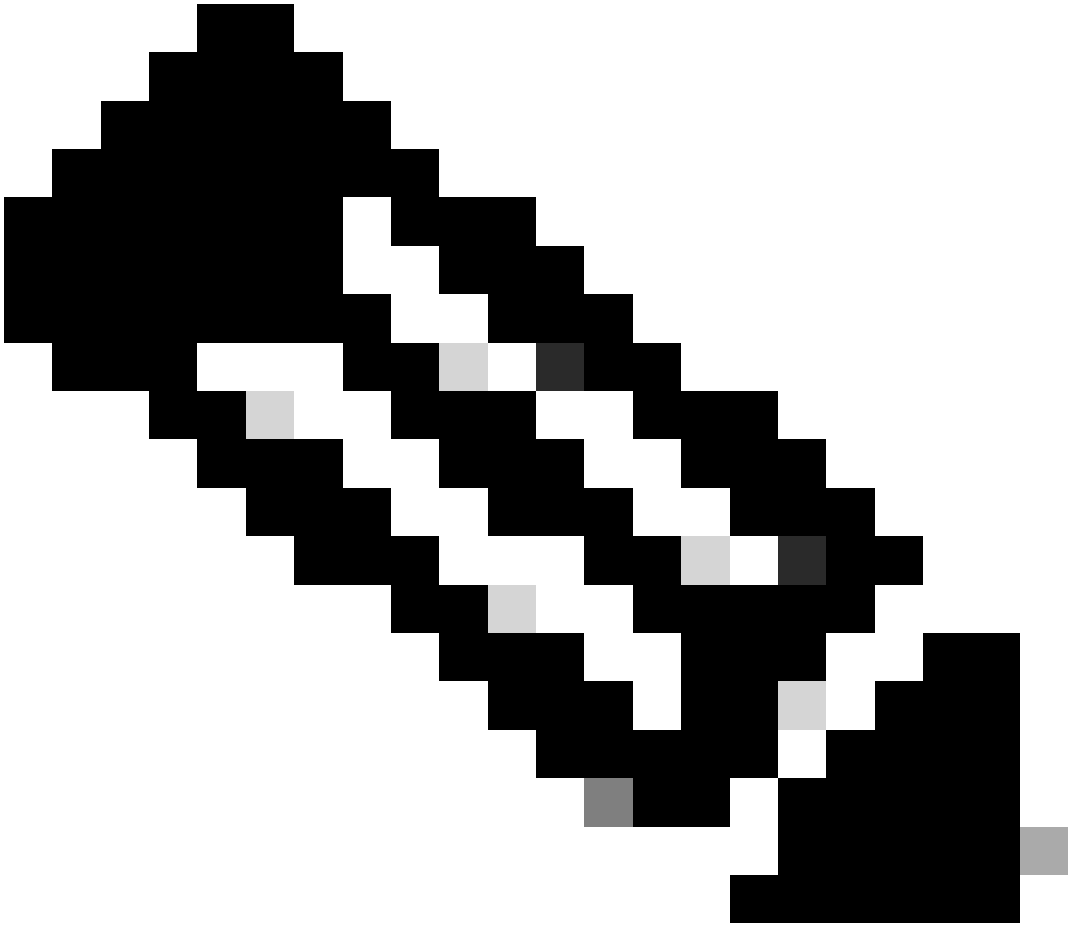
背景説明

EIGRPは、ディスタンスベクタープロトコルとリンクステートプロトコルの両方の機能を組み合わせた高度なディスタンスベクタールーティングプロトコルです。ネイバーからのルーティング情報を維持することで高速コンバージェンスを提供し、代替ルートへすばやく適応できるようにします。EIGRPは、ルートまたはメトリックの変更に、定期的なフルアップデートではなく、部分的なトリガードアップデートを使用する効率的な方法です。
通信用に、EIGRPはIP層（プロトコル88）で直接動作し、保証された順序付けされたパケット配信のためにReliable Transport Protocol(RTP)を使用します。マルチキャストアドレス224.0.0.10またはFF02::Aを使用するhelloメッセージにより、マルチキャストとユニキャストの両方がサポートされます。
EIGRPの動作は、基本的に次の3つの表に格納されている情報に基づいています。

- ネイバーテーブル：このテーブルには、隣接関係が正常に確立された、直接接続されたEIGRPデバイスのレコードが保持されます。
- トポロジテーブル：このテーブルには、特定の宛先への到達可能なパスとそれに関連付けられたメトリックを含め、ネイバーによってアドバタイズされたすべての学習ルートが保存されます。これにより、品質と使用可能なパスの数を評価できます。
- ルーティング テーブル: このテーブルには、「サクセサ」と呼ばれる各宛先のベストパスが含まれます。 このサクセサルートはトラフィックの転送にアクティブに使用され、その後、他のEIGRPネイバーにアドバタイズされます。

EIGRPは、K値と呼ばれるメトリックの重み付けをルーティングおよびメトリックの計算に使用して、宛先への最適なパスを決定します。このメトリック値は、パラメータを使用する式から導出されます。

- 帯域幅
- 遅延時間
- 信頼性
- Loading
- MTU

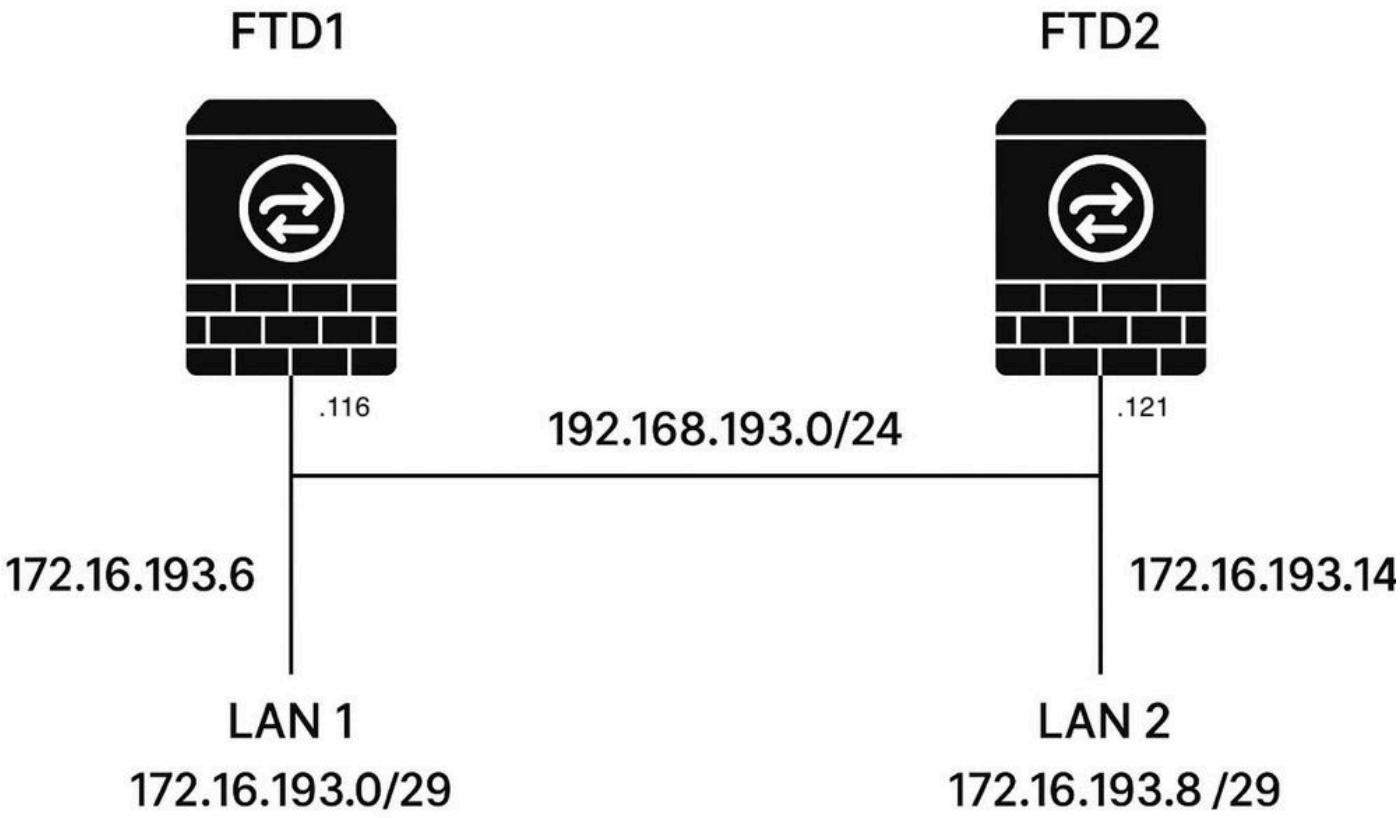


注：複数のパス間でメトリックが一致する場合は、より大きいMTU値が優先される最大伝送ユニット(MTU)が選出され、MTUが選出の基準として使用されます。

- サクセサルート:これは特定の宛先へのベストパスとして定義されます。最終的にルーティングテーブルにインストールされるルートです。
- フィジブルディスタンス(FD)：ローカルルータの観点から特定のサブネットに到達するための最適な計算メトリックを表します。
- レポーテッドディスタンス(RD)/アドバタイズドディスタンス(AD)：これは、ネイバーによって報告された特定のサブネットまでの距離（メトリック）です。パスをフィージブルサクセサと見なすには、ネイバーからのレポーテッドディスタンスが、同じ宛先へのローカルルータのフィージブルディスタンスよりも小さい必要があります。
- フィジブルサクセサ(FS)：これは宛先へのバックアップパスで、プライマリサクセサルートに障害が発生した場合に代替ルートを提供します。（アドバタイジングネイバーからの）レポーテッドディスタンスが、同じ宛先への現在のサクセサルートのフィージブルディスタン

スよりも厳密に小さい場合、そのパスはフィージブルサクセサとして認定されます。

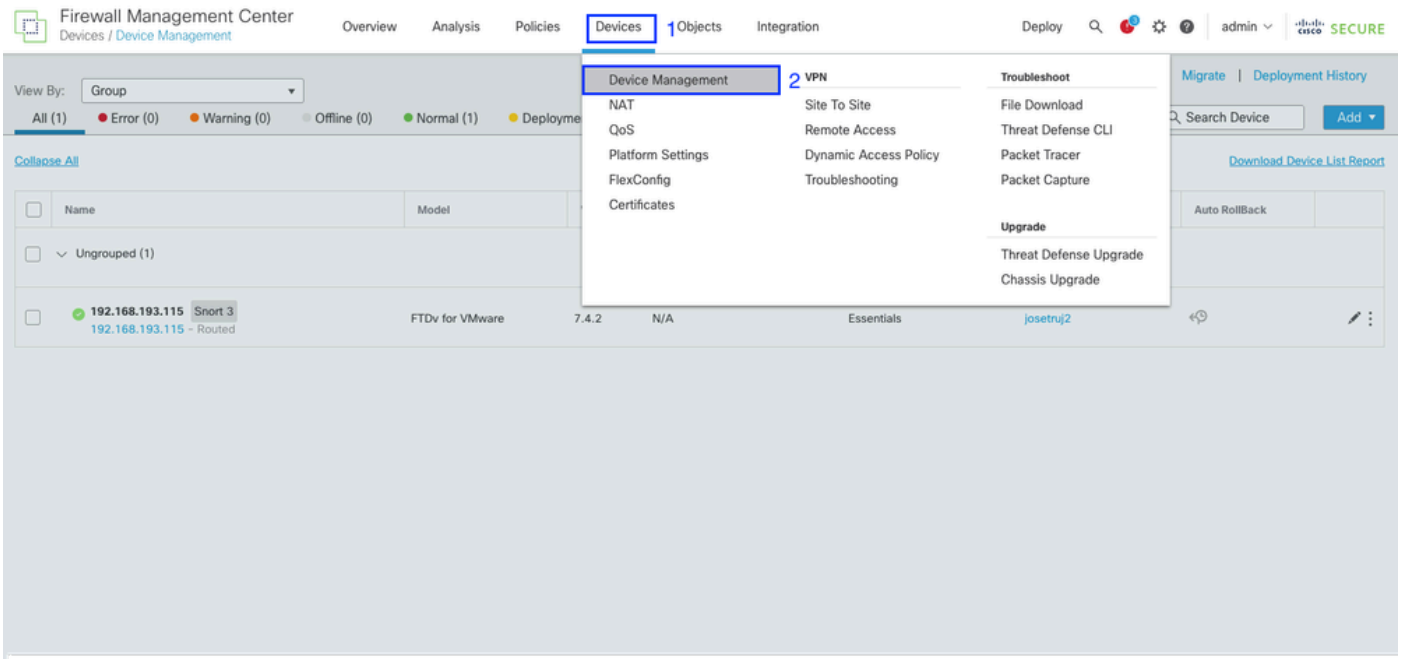
ネットワーク図



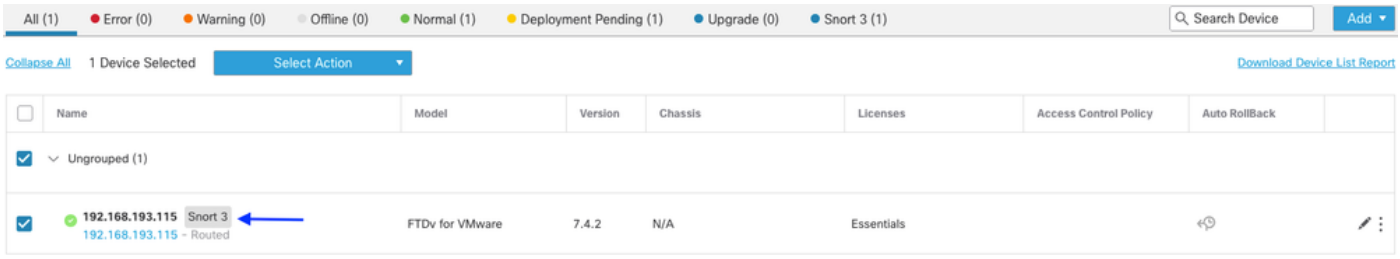
ネットワーク図

基本設定

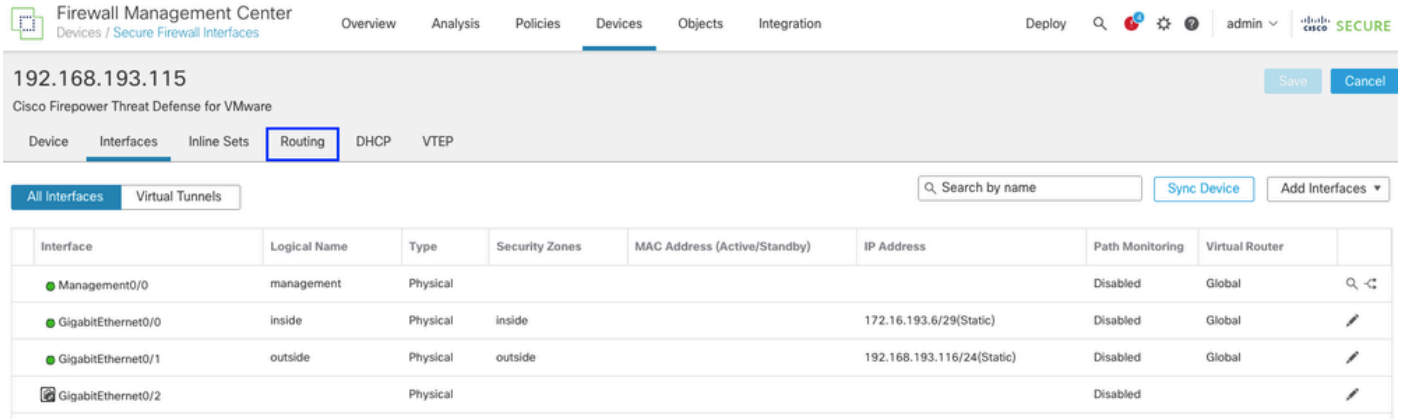
Devices > Device Managementの順に移動します。



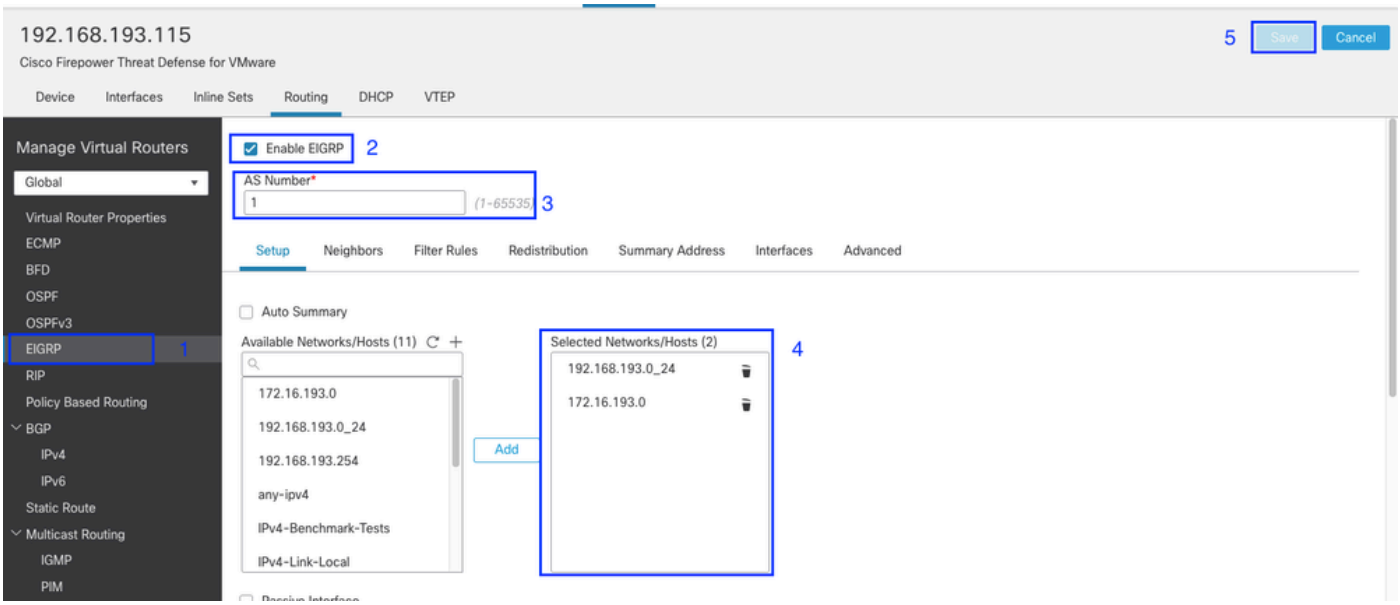
デバイスの選択:



Routingタブをクリックします。



左側のメニューで**EIGRP**をクリックします。
Enable EIGRPをクリックします。
AS番号(1 ~ 65535)を割り当てます。
ネットワーク/ホストを1つ選択します。「Available Network/Host」リストから以前作成したオブジェクトを選択するか、プラス(+)ボタンをクリックして新しいオブジェクトを作成できます。
[Save] をクリックします。



検証

EIGRPネイバー（隣接）関係の最小要件は次のとおりです。

- AS番号が一致している必要があります。
- interfaceがアクティブで到達可能である必要があります。
- ベストプラクティスとして、Helloタイマーとホールドタイマーは一致している必要があります。
- K値は一致する必要があります。
- EIGRPトラフィックをブロックしているアクセスリストがないこと。

CLIを使用した検証

- show run router eigrp（すべてのコマンド）
- show eigrp neighborsコマンド
- show eigrp topologyの出力
- show eigrp interfaces（隠しコマンド）
- show route eigrp（すべてのコマンド）
- show eigrp traffic
- debug ip eigrp neighbor（隠しコマンド）
- eigrpパケットのデバッグ

firepower# show run router eigrp

router eigrp 1

デフォルト情報なし

no default-information out（デフォルト情報なし）

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)のEIGRP-IPv4ネイバー
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)のEIGRP-IPv4トポロジテーブル
コード：P – パッシブ、A – アクティブ、U – アップデート、Q – クエリ、R – 応答、
      r：応答ステータス、s:siaステータス
P 192.168.193.0 255.255.255.0, 1 successors, FD is 512
        接続経由、外部
P 172.16.193.0 255.255.255.248, 1 successors, FD is 768
        192.168.193.116(768/512)経由、外部
P 172.16.193.8 255.255.255.248, 1 successors, FD is 512
        接続経由、内部
firepower# show eigrp interfaces
AS(1)のEIGRP-IPv4インターフェイス
                  Xmit Queue Mean Pacing Time Multicast Pending ( キュー平均ペーシング時間 – 保留中 )
インターフェイスピア無効/信頼できるSRTT無効/信頼できるフロータイマールート
外部1 0 / 0 10 0 / 1 50 0
内側0 0 / 0 0 / 1 0 0
firepower#
```

```
firepower# show route eigrp
コード：L – ローカル、C – 接続、S – スタティック、R - RIP、M – モバイル、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外部タイプ1、E2 - OSPF外部タイプ2、V - VPN
       i - IS-IS、su - IS-ISサマリー、L1 - IS-ISレベル1、L2 - IS-ISレベル2
       ia:IS-ISエリア間、*：候補デフォルト、U：ユーザごとのスタティックルート
       o:ODR、P：定期的にダウンロードされたスタティックルート、+：複製ルート
       SI：スタティックInterVRF、BI:BGP InterVRF
ラストリゾートゲートウェイは192.168.193.254からネットワーク0.0.0.0です。
D 172.16.193.0 255.255.255.248
           [90/768] via 192.168.193.116、02:32:58、外部
firepower# show route
コード：L – ローカル、C – 接続、S – スタティック、R - RIP、M – モバイル、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外部タイプ1、E2 - OSPF外部タイプ2、V - VPN
       i - IS-IS、su - IS-ISサマリー、L1 - IS-ISレベル1、L2 - IS-ISレベル2
       ia:IS-ISエリア間、*：候補デフォルト、U：ユーザごとのスタティックルート
       o:ODR、P：定期的にダウンロードされたスタティックルート、+：複製ルート
       SI：スタティックInterVRF、BI:BGP InterVRF
ラストリゾートゲートウェイは192.168.193.254からネットワーク0.0.0.0です。
S* 0.0.0.0 0.0.0.0 [1/0]経由192.168.193.254、外部
D 172.16.193.0 255.255.255.248
           [90/768] via 192.168.193.116、02:33:41、外部
C 172.16.193.8 255.255.255.248 is directly connected, inside（直接接続されている）
L 172.16.193.14 255.255.255.255 is directly connected, inside（内部）
```

C 192.168.193.0 255.255.255.0は直接接続されています（外部）。

L 192.168.193.121 255.255.255.255 is directly connected, outside（直接接続、外部）

firepower#

firepower# show eigrp traffic

AS(1)のEIGRP-IPv4トラフィック統計情報

  Hello送受信：4006/4001

  送受信アップデート：4/4

  送受信されたクエリ： 0/0

  送信/受信した応答： 0/0

  送信または受信した確認応答： 3/2

  送受信されたSIAクエリ： 0/0

  送信/受信されたSIA応答： 0/0

  HelloプロセスID:2503149568

  PDMプロセスID: 2503150496

  ソケットキュー：

  入力キュー：0/2000/2/0（現在/最大/最大/最大/ドロップ）

firepower#

トラブルシュート

シナリオ1:IP EIGRPネイバーのデバッグ

debugコマンドを使用すると、ネイバーの状態の変化を確認できます。

firepower# debug ip eigrp neighbor

firepower#

EIGRP:Holdtime期限切れ

ダウン状態：ピア192.168.193.121 total=0スタブ0、iidb-stub=0 iid-all=0

EIGRP：割り当て解除の失敗を処理します[0]

EIGRP：ネイバー192.168.193.121がoutsideでダウンした

show eigrp neighborsコマンドを実行して、FTD間のネイバーステータスを確認します。

firepower# show eigrp neighbors

AS(1)のEIGRP-IPv4ネイバー

show interface ip briefコマンドを使用して、インターフェイスのステータスを確認します。GigabitEthernet0/1インターフェイスが管理上ダウンしていることがわかります。

firepower# show interface ip brief

Interface IP-Address OK?Method Status Protocol

GigabitEthernet0/0 172.16.193.14 YES CONFIG UP

GigabitEthernet0/1 192.168.193.121 YES CONFIG administratively down up

GigabitEthernet0/2 192.168.194.24 YES手動アップ

Internal-Control0/0 127.0.1.1 YESセットアップ解除

Internal-Control0/1 unassigned YESセットアップ解除

Internal-Data0/0 unassigned YESセットアップ解除

Internal-Data0/0 unassigned YESセットアップ解除

Internal-Data0/1 169.254.1.1 YESセットアップ解除

Internal-Data0/2 unassigned YESセットアップ解除

Management0/0 203.0.113.130 YESセットアップ解除

シナリオ2：認証

FTDは、EIGRPパケットを認証するMD5ハッシュアルゴリズムをサポートします。デフォルトでは、この認証は無効になっています。

MD5ハッシュアルゴリズムを有効にするには、[MD5認証]チェックボックスをオンにします。両方のデバイスで認証設定が一致していることが重要です。一方のデバイスで認証設定が有効になっていて、もう一方では有効になっていない場合、両方のデバイス間でネイバー/アジャセンシー関係を形成できません。

debug eigrp packetsを使用して、この設定を確認します。

firepower# debug eigrp packets

(UPDATE、REQUEST、QUERY、REPLY、HELLO、IPXSAP、PROBE、ACK、STUB、SIAQUERY、SIAREPLY)EIGRPパケットのデバッグがオン

firepower#

EIGRP:outside:192.168.193.121からのignoredパケット、opcode = 5（認証オフまたはキーチェーンの欠落）

EIGRP:Outside NBR 172.16.193.14でHELLOを受信

AS 1、フラグ0x0:(NULL)、Seq 0/0 interfaceQ 0/0

EIGRP：外部にHELLOを送信

AS 1、フラグ0x0:(NULL)、Seq 0/0 interfaceQ 0/0 iidbQ un/rely 0/0

EIGRP：内部でHELLOを送信

AS 1、フラグ0x0:(NULL)、Seq 0/0 interfaceQ 0/0 iidbQ un/rely 0/0

EIGRP:outside:192.168.193.121からのignoredパケット、opcode = 5（認証オフまたはキーチェーンの欠落）

EIGRP:Outside NBR 172.16.193.14でHELLOを受信

AS 1、フラグ0x0:(NULL)、Seq 0/0 interfaceQ 0/0

EIGRP：内部でHELLOを送信

AS 1、フラグ0x0:(NULL)、Seq 0/0 interfaceQ 0/0 iidbQ un/rely 0/0

EIGRP：外部にHELLOを送信

AS 1、フラグ0x0:(NULL)、Seq 0/0 interfaceQ 0/0 iidbQ un/rely 0/0

EIGRP: outside: ignored packet from 192.168.193.121, opcode = 5（authentication offまたはkey-chain missing）。

認証がオフになっているか、キーチェーンが欠落していることを示すメッセージを確認できます。このシナリオでは、通常、認証が一方のピアでは有効になっていて、他方では有効になっていない場合に、このような状況が発生します。

EIGRP: outside: ignored packet from 192.168.193.121, opcode = 5（authentication offまたはkey-chain missing）。

show run interface <EIGRP interface>を使用して確認します。

Firepower1# show run interface GigabitEthernet0/1

!

interface GigabitEthernet0/1

nameif外部

セキュリティレベル0

ipアドレス192.168.193.121 255.255.255.0

認証キーeigrp 1 *****キーid 10

認証モードeigrp 1 md5

Firepower2# show run interface GigabitEthernet0/1

!

interface GigabitEthernet0/1

nameif外部

セキュリティレベル0

ipアドレス192.168.193.116 255.255.255.0

シナリオ3 – パッシブインターフェイス

EIGRPを設定すると、通常、EIGRP helloパケットは、ネットワークが有効になっているインターフェイスで送受信されます。

ただし、インターフェイスがパッシブとして設定されている場合、EIGRPはそのインターフェイス上の2台のルータ間のhelloパケットの交換を抑制し、その結果、ネイバーとの隣接関係が失われます。その結果、このアクションは、ルータがそのインターフェイスからルーティングアップデートをアドバタイズすることを防止するだけでなく、そのインターフェイスからのルーティングアップデートの受信も停止します。

show eigrp neighborsコマンドを実行して、FTD間のネイバーステータスを確認します。

firepower# show eigrp neighbors

AS(1)のEIGRP-IPv4ネイバー

debug eigrp packetsコマンドを使用すると、送信されているEIGRPパケットと、それらが送信されているインターフェイスを確認できます。

FTD 1

Firepower1#

(UPDATE、REQUEST、QUERY、REPLY、HELLO、IPXSAP、PROBE、ACK、STUB、SIAQUERY、SIAREPLY)EIGRPパケットのデバッグがオン

firepower#

EIGRP：外部にHELLOを送信

AS 1、フラグ0x0:(NULL)、Seq 0/0 interfaceQ 0/0 iidbQ un/rely 0/0

EIGRP：内部でHELLOを送信

AS 1、フラグ0x0:(NULL)、Seq 0/0 interfaceQ 0/0 iidbQ un/rely 0/0

EIGRP：外部にHELLOを送信

AS 1、フラグ0x0:(NULL)、Seq 0/0 interfaceQ 0/0 iidbQ un/rely 0/0

EIGRP：内部でHELLOを送信

AS 1、フラグ0x0:(NULL)、Seq 0/0 interfaceQ 0/0 iidbQ un/rely 0/0

EIGRP：外部にHELLOを送信

FTD 2

Firepower2# debug eigrp packets

(UPDATE、REQUEST、QUERY、REPLY、HELLO、IPXSAP、PROBE、ACK、STUB、SIAQUERY、SIAREPLY)EIGRPパケットのデバッグがオン

Firepower2#

このシナリオでは、FTD 2のinsideインターフェイスとoutsideインターフェイスがパッシブとして設定されているため、EIGRP helloメッセージは送信されていません。show run router eigrpコマンドで、これを確認してください。

Firepower2# show run router eigrp

router eigrp 1

デフォルト情報なし

no default-information out（デフォルト情報なし）

no eigrp log-neighbor-warnings

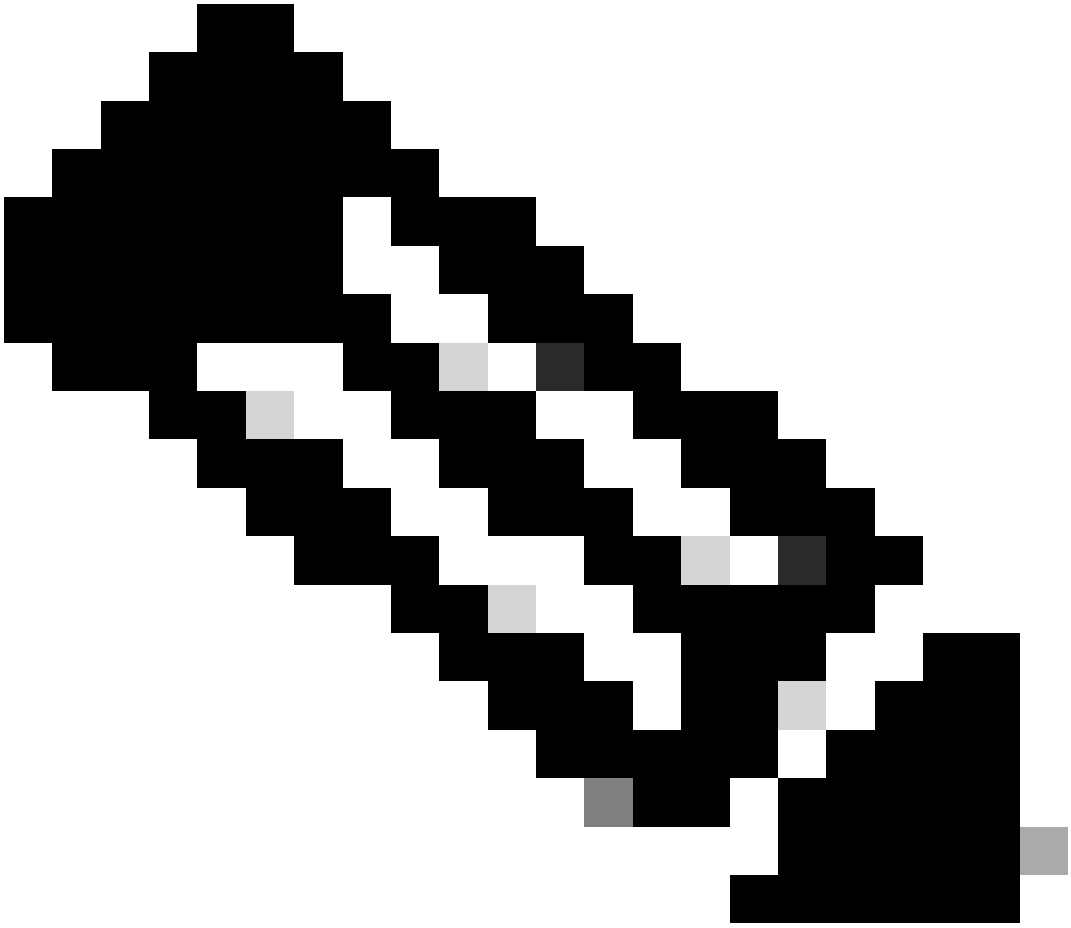
no eigrp log-neighbor-changes

network 192.168.193.0 255.255.255.0

network 172.16.193.8 255.255.255.248

パッシブインターフェイス外部

パッシブインターフェイス内部



注：設定されたすべてのデバッグプロセスを停止するには、undebug allコマンドを使用してください。

関連情報

- FTDデバイスでのEIGRP
- FTDでのEIGRPの設定
- EIGRP複合コストメトリック

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。