EIGRP

このセクションでは、Enhanced Interior Gateway Routing Protocol（EIGRP）を使用してデータをルーティングし、認証を実行し、ルーティング情報を再配布するように Firewall Threat Defense を設定する方法について説明します。

EIGRP ルーティングについて

シスコによって開発された Enhanced Interior Gateway Routing Protocol（EIGRP）は、IGRP の拡張バージョンです。IGRP や RIP と異なり、EIGRP が定期的にルート アップデートを送信することはありません。EIGRP アップデートは、ネットワーク トポロジが変更された場合にだけ送信されます。EIGRP を他のルーティング プロトコルと区別する主な機能には、迅速なコンバージェンス、可変長サブネットマスクのサポート、部分的アップデートのサポート、複数のネットワーク レイヤ プロトコルのサポートなどがあります。

EIGRP を実行するルータでは、すべてのネイバー ルーティング テーブルが格納されているため、代替ルートに迅速に適応できます。適切なルートが存在しない場合、EIGRP はそのネイバーにクエリーを送信して代替のルートを検出します。これらのクエリは、代替ルートが検出されるまで伝搬されます。EIGRP では可変長サブネットマスクがサポートされているため、ルートはネットワークの境界で自動的に集約されます。さらに、任意のインターフェイスの任意のビット境界で集約を行うように EIGRP を設定することもできます。

EIGRP は定期的なアップデートを行いません。その代わり、ルートのメトリックが変更されたときに、部分的なアップデートを送信します。部分的アップデートの伝搬では、その情報を必要とするルータだけがアップデートされるように境界が自動的に設定されます。これらの 2 つの機能により、EIGRP の帯域幅消費量は IGRP に比べて大幅に減少します。

脅威防御では、直接接続されているネットワーク上にある他のルータをダイナミックに把握するために、ネイバー探索が使用されます。EIGRP ルータは、マルチキャスト hello パケットを送信して、ネットワーク上に自分が存在していることを通知します。EIGRP デバイスは、新し

いネイバーから hello パケットを受信すると、トポロジテーブルに初期化ビットを設定してそのネイバーに送信します。ネイバーは、初期化ビットが設定されたトポロジアップデートを受信すると、自分のトポロジテーブルをデバイスに返送します。

hello パケットはマルチキャスト メッセージとして送信されます。hello メッセージへの応答は想定されていません。スタティックに定義されたネイバーは、このルールの例外です。ネイバーを手動で設定すると、hello メッセージ、ルーティングアップデート、および確認応答がユニキャストメッセージとして送信されます。

このネイバー関係が確立した後は、ネットワーク トポロジが変更された場合にだけ、ルーティング アップデートが交換されます。ネイバー関係は、hello パケットによって維持されます。ネイバーから受信した各 hello パケットには、保持時間が含まれています。保持時間は、その間に脅威防御がそのネイバーから hello パケットを受信すると想定できる時間です。デバイスは、保持時間内にそのネイバーからアドバタイズされた hello パケットを受信しない場合、そのネイバーを使用不能と見なします。

EIGRP は、ネイバー探索/回復、Reliable Transport Protocol（RTP）、および Diffusing Update Algorithm（DUAL）をルート計算に使用します。DUAL は、最小コストのルートだけでなく、宛先へのすべてのルートをトポロジテーブルに保存します。最小コストのルートはルーティングテーブルに挿入されます。その他のルートは、トポロジテーブルに残ります。メインのルートに障害が発生したら、フィジブル サクセサから別のルートが選択されます。サクセサとは、宛先への最小コストパスを持ち、パケット転送に使用される隣接ルータです。フィジビリティ計算によって、パスがルーティングループを形成しないことが保証されます。

フィジブルサクセサがトポロジテーブル内にない場合は、ルートが再計算されます。ルートの再計算中、DUAL は EIGRP ネイバーにルートを求めるクエリを送信します。このクエリは、連続するネイバーに伝播されます。フィジブルサクセサが見つからない場合は、到達不能メッセージが返されます。

ルートの再計算中、DUAL は、ルートをアクティブとマークします。デフォルトでは、脅威防御は、ネイバーから応答が返ってくるのを 3 分間待ちます。デバイスがネイバーから応答を受信しないと、そのルートは stuck-in-active とマークされます。トポロジ テーブル内のルートのうち、応答しないネイバーをフィジブル サクセサとして指しているものはすべて削除されます。

EIGRP の要件と前提条件

モデルのサポート

Threat Defense

Firewall Threat Defense Virtual

サポートされるドメイン

任意

ユーザの役割

管理者

ネットワーク管理者

EIGRP ルーティングのガイドラインと制限事項

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードでのみサポートされています。

デバイスのガイドライン

- デバイスごとに許可される EIGRP プロセスは 1 つだけです。
- EIGRP は、Firewall Threat Defense 6.6 以降のバージョンの Management Center の UI を使用して設定できます。

インターフェイスのガイドライン

- EIGRP ルーティングプロセスに関連付けられるのは、論理名と IP アドレスを持つルーテッドインターフェイスだけです。
- グローバル仮想ルータに属するインターフェイスのみ EIGRP の一部にできます。EIGRP は、グローバル仮想ルータのルーティングプロトコル全体でルートを学習、フィルタ処理、および再配布できます。
- 物理、EtherChannel、冗長インターフェイス、サブインターフェイスのみをサポートします。ただし、EtherChannel インターフェイスのメンバーはサポートされていません。
- BVI および VNI は EIGRP の一部にできません。
- パッシブインターフェイスはネイバーインターフェイスとして設定できません。

IP アドレスとネットワークオブジェクトのサポート

- IPv4 アドレスのみサポートされています。
- 範囲、FQDN、およびワイルドカードマスクはサポートされていません。
- 標準アクセスリストオブジェクトのみがサポートされています。

再配布のガイドライン

- グローバル仮想ルータの BGP、OSPF、および RIP は、EIGRP に再配布できます。
- EIGRP では、グローバル仮想ルータ内の BGP、OSPF、RIP、スタティック、および接続済みルートに再配布できます。

- EIGRP が、OSPF ネットワークの一部であるデバイスで設定されている場合、またはその逆の場合は、ルートにタグを付けるように OSPF ルータが設定されていることを確認します（EIGRP はルートタグをサポートしていません）。

  EIGRP を OSPF に再配布し、OSPF を EIGRP に再配布する場合は、いずれかのリンクまたはインターフェイスで障害が発生したときや、ルート発信元がダウンしたときにも、ルーティングループが発生します。あるドメインから同じドメインに再度ルートを再配布することを避けるため、ルータは、再配布する際にドメインに属しているルートにタグ付けすることができます。そして、そのタグに基づいて、リモートルータでそれらのルートをフィルタ処理できます。それらのルートはルーティングテーブルにインストールされないため、再度同じドメインに再配布されることはありません。

展開プロセスのガイドライン

展開された EIGRP 設定の既存の AS 番号を変更する場合は、EIGRP を無効にして展開する必要があります。この手順により、Threat Defense に展開された EIGRP 設定がクリアされます。次に、新しい AS 番号で EIGRP 設定を再作成して展開します。このプロセスにより、Threat Defense に展開されている同じ EIGRP 設定による展開の失敗を阻止できます。

アップグレードのガイドライン

バージョン 7.2 以降にアップグレードし、以前のバージョンに FlexConfig EIGRP ポリシーがある場合、展開中に Management Center に警告メッセージが表示されます。ただし、展開プロセスは停止しません。ただし、展開後、UI（**[デバイスの編集（Device (Edit)）]** > **[ルーティング（Routing）]** > **[EIGRP]**）から EIGRP ポリシーを管理するには、**[デバイスの編集（Device (Edit)）]** > **[ルーティング（Routing）]** > **[EIGRP]**ページで設定をやり直し、FlexConfig から設定を削除する必要があります。を参照してください。UI でのポリシーの作成を自動化するために、Firewall Management Center にはポリシーを FlexConfig から UI に移行するオプションがあります。詳細については、FlexConfig ポリシーの移行、を参照してください。

EIGRP の設定

[ルーティング（Routing）] タブで、ファイアウォールデバイスの EIGRP を有効にして設定することができます。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、Firewall Threat Defense デバイスを編集します。

ステップ 2 [ルーティング（Routing）] タブをクリックします。

ステップ 3 [グローバル（Global）] で、[EIGRP] をクリックします。

ステップ 4 [EIGRPの有効化（Enable EIGRP）] チェックボックスをオンにして EIGRP ルーティングプロセスを有効にします。

ステップ 5 [AS番号（AS Number）] フィールドに、EIGRP プロセスの自律システム（AS）番号を入力します。AS 番号には、複数の自律番号が含まれます。AS 番号は 1 ～ 65535 であり、固有に割り当てられた値であるため、インターネットの各ネットワークが識別されます。

ステップ 6 他の EIGRP プロパティを設定するには、次のトピックを参照してください。

1. EIGRP の設定 （5 ページ）。
2. EIGRP ネイバー設定の設定 （6 ページ）。
3. EIGRP のフィルタルールの設定 （6 ページ）。
4. EIGRP 再配布の設定 （7 ページ）。
5. EIGRP サマリーアドレスの設定 （9 ページ）。
6. EIGRP インターフェイス設定の指定 （9 ページ）。
7. EIGRP の高度な設定の指定 （10 ページ）。

EIGRP の設定

手順

ステップ 1 [EIGRP] ページで [セットアップ（Setup）] タブをクリックします。

ステップ 2 [自動サマリー（Auto Summary）] チェックボックスをオンにして、EIGRP がネットワーク番号境界を集約できるようにします。

（注）
[自動サマリー（Auto Summary）] を有効にすると、不連続ネットワークがある場合にルーティングの問題の原因となることがあります。

ステップ 3 [使用可能なネットワーク/ホスト（Available Networks/Hosts）] ボックスで、EIGRP ルーティングプロセスに参加する必要があるネットワークまたはホストをクリックし、[追加（Add）] をクリックします。新しいネットワークオブジェクトを追加するには、[追加（Add）] (＋) をクリックします。ネットワークを追加する手順については、ネットワークを参照してください。

ステップ 4 パッシブインターフェイスを構成するには、[パッシブインターフェイス（Passive Interface）] チェックボックスをオンにします。EIGRP の場合、受動インターフェイスではルーティングアップデートが送受信されません。

a) 選択したインターフェイスをパッシブとして指定するには、[選択したインターフェイス（Selected Interface）] オプションボタンをクリックします。[使用可能なインターフェイス（Available Interfaces）] ボックスでインターフェイスを選択し、[追加（Add）] をクリックします。

b) すべてのインターフェイスをパッシブとして指定するには、[すべてのインターフェイス（All Interfaces）] オプションボタンをクリックします。

ステップ 5 [OK] をクリックし、[保存（Save）] をクリックして設定を保存します。

EIGRP ネイバー設定の設定

EIGRP プロセスのスタティックネイバーを定義できます。EIGRP ネイバーを定義すると、hello パケットがそのネイバーにユニキャストされます。

手順

ステップ 1 [EIGRP] ページで [ネイバー（Neighbors）] タブをクリックします。

ステップ 2 [Add] をクリックします。

ステップ 3 [インターフェイス（Interface）] ドロップダウンリストから、ネイバーが使用可能になるインターフェイスを選択します。

ステップ 4 [ネイバー（Neighbor）] ドロップダウンから、スタティックネイバーの IP アドレスを選択します。ネットワークオブジェクトを追加するには、[追加（Add）] (+) をクリックします。ネットワークオブジェクトの追加手順については、ネットワークを参照してください。

ステップ 5 [OK] をクリックし、[保存（Save）] をクリックして設定を保存します。

EIGRP のフィルタルールの設定

EIGRP ルーティングプロセスのルートフィルタルールを設定できます。フィルタルールによって、EIGRP ルーティングプロセスで受け入れまたはアドバタイズされるルートを制御できます。

手順

ステップ 1 [EIGRP] ページで、[フィルタルール（Filter Rules）] タブをクリックします。

ステップ 2 [追加（Add）] (+) をクリックします。

ステップ 3 [フィルタルールの追加（Add Filter Rules）] ダイアログボックスで、[フィルタ方向（Filter Direction）] ドロップダウンからルールの方向を選択します。

- [インバウンド（Inbound）]：このルールは、着信 EIGRP ルーティングアップデートからのデフォルトルート情報をフィルタリングします。
- [アウトバウンド（Outbound）]：このルールは、発信 EIGRP ルーティングアップデートからのデフォルトルート情報をフィルタリングします。

ステップ 4 フィルタルールを適用するインターフェイスを選択するには、[インターフェイス（Interface）] オプションボタンをクリックし、ドロップダウンからインターフェイスを選択します。

（注）
VTI インターフェイス上では、EIGRP フィルタリング ルールを適用できません。

ステップ 5 フィルタルールを適用するプロトコルを選択するには、[プロトコル（Protocol）] オプションボタンをクリックし、ドロップダウンからプロトコル（[BGP]、[RIP]、[静的（Static）]、[接続（Connected）]、または [OSPF]）を選択します。BGP および OSPF プロトコルの場合は、関連するプロセス ID を指定できます。

ステップ 6 [Access List] ドロップダウンから、アクセスリストを選択します。このリストは、受信されるネットワークとルーティングアップデートで抑制されるネットワークを定義します。新しい標準アクセスリストオブジェクトを追加するには、[追加（Add）] (+) をクリックし、詳細な手順について 標準 ACL オブジェクトの設定 を参照してください。

ステップ 7 [OK] をクリックし、[保存（Save）] をクリックして設定を保存します。

EIGRP 再配布の設定

他のルーティングプロトコルから EIGRP ルーティングプロセスにルートを再配布するためのルールを定義できます。

手順

ステップ 1 [EIGRP] ページで、[再配布（Redistribution）] タブをクリックします。

ステップ 2 [追加（Add）] (+) をクリックします。

ステップ 3 [再配布の追加（Add Redistribution）] ダイアログボックスの [プロトコル（Protocol）] ドロップダウンから、ルートが再配布されるソースプロトコルを選択します。

- [BGP]：BGP ルーティングプロセスによって検出されたルートを EIGRP に再配布します。
- [RIP]：RIP ルーティングプロセスによって検出されたルートを EIGRP に再配布します。
- [Static]：スタティックルートを EIGRP ルーティングプロセスに再配布します。ネットワーク設定の範囲内にあるスタティックルートは EIGRP に自動的に再配布されるため、それらのルートの再配布ルールを定義する必要はありません。 ただし、EIGRP で VTI インターフェイスを指すスタティック ルートを再配布する場合は、メトリックを指定する必要があります。他のタイプのインターフェイスを指すスタティック ルートの場合、メトリックの指定は必須ではありません。
- [Connected]：接続されたルート（インターフェイス上で IP アドレスをイネーブルにすることによって自動的に確立されるルート）を EIGRP ルーティングプロセスに再配布します。ネットワーク設定の範囲内にある接続済みルートは EIGRP に自動的に再配布されるため、それらのルートの再配布ルールを定義する必要はありません。

- [OSPF]：OSPF ルーティングプロセスで検出されたルートを EIGRP に再配布します。このプロトコルを選択すると、[オプションのOSPF再配布（Optional OSPF Redistribution）] で、このダイアログボックスの [一致（Match）] オプションが表示されます。
  - [Internal]：特定の AS の内部のルート。
  - [External1]：AS の外部にあり、OSPF にタイプ 1 外部ルートとしてインポートされるルート。
  - [External2]：AS の外部にあり、選択したプロセスにタイプ 2 外部ルートとしてインポートされるルート。
  - [Nsaa-External1]：AS の外部にあり、選択したプロセスにタイプ 1 外部ルートとしてインポートされる Not-So-Stubby Area（NSSA）ルート。
  - [Nsaa-External2]：AS の外部にあり、選択したプロセスにタイプ 2 外部ルートとしてインポートされる（NSSA）ルート。

（注）
これらのオプションは、スタティック、接続済み、RIP、または BGP ルートを再配布するときには使用できません。

ステップ 4 [オプションメトリック（Optional Metrics）] で、関連する値を入力します。

- [帯域幅（Bandwidth）]：ルートの最小帯域幅（キロビット/秒）。有効値の範囲は 1 ～ 4294967295 です。
- [遅延時間（Delay Time）]：10 マイクロ秒単位のルート遅延です。有効値の範囲は、0 ～ 4294967295 です。
- [信頼性（Reliability）]：0 ～ 255 の数値で表現した、パケットが正常に伝送される見込み。値 255 は 100 % の信頼性を意味し、0 は信頼性がないことを表します。
- [ローディング（Loading）]：ルートの実効帯域幅。有効値の範囲は、1 ～ 255 です。255 は 100% のロードを意味します。
- [MTU]：パスの最大伝送単位の最小許容値。有効値の範囲は 1 ～ 65535 です。

ステップ 5 [ルートマップ（Route Map）] ドロップダウンから、再配布エントリに適用するルートマップオブジェクトを選択します。新しいルートマップオブジェクトを作成するには、[追加（Add）] (＋) をクリックします。新しいルートマップを追加する手順については、「ルートマップエントリの設定」を参照してください。

ステップ 6 [OK] をクリックし、[保存（Save）] をクリックして設定を保存します。

EIGRP サマリーアドレスの設定

インターフェイスごとにサマリーアドレスを設定できます。ネットワークの境界以外でサマリーアドレスを作成する場合、または自動ルート集約が無効になったThreat Defenseでサマリーアドレスを使用する場合は、手動でサマリーアドレスを定義する必要があります。より具体的なルートがルーティングテーブルにある場合、EIGRPは、より具体的なすべてのルートの最小に等しいメトリックを持つサマリーアドレスをアドバタイズします。

手順

ステップ1 [EIGRP] ページで、[サマリーアドレス（Summary Address）] タブをクリックします。

ステップ2 [Add] をクリックします。

ステップ3 [インターフェイス（Interface]） ドロップダウンで、どのインターフェイスからこのサマリーアドレスをアドバタイズするかを選択します。

ステップ4 [ネットワーク（Network）] ドロップダウンから、集約する特定のIPアドレスとネットワークマスクを持つネットワークオブジェクトを選択します。新しいネットワークを追加するには、[追加（Add）] (+) をクリックします。ネットワークを追加する手順については、ネットワークを参照してください。

ステップ5 [アドミニストレーティブ ディスタンス（Administrative Distance）] フィールドに、サマリールートのアドミニストレーティブ ディスタンスを入力します。有効値の範囲は、1 ～ 255 です。

ステップ6 [OK] をクリックし、[保存（Save）] をクリックして設定を保存します。

EIGRP インターフェイス設定の指定

[インターフェイス（Interfaces）] タブで、インターフェイス固有のEIGRPルーティングプロパティを設定できます。

手順

ステップ1 [EIGRP] ページで、[インターフェイス（Interfaces）] タブをクリックします。

ステップ2 [追加（Add）] (+) をクリックします。

ステップ3 [インターフェイス（Interface）] ドロップダウンから、設定が適用されるインターフェイスの名前を選択します。

ステップ4 [hello間隔（Hello Interval）] フィールドに、インターフェイスで送信されるEIGRP helloパケットの間隔を秒単位で入力します有効値の範囲は1 ～ 65535 です。デフォルト値は5秒です。

ステップ 5 [ホールド時間（Hold Time）] フィールドに、EIGRP hello パケットでデバイスによってアドバタイズされるホールド時間を入力します。有効値の範囲は 3 ～ 65535 です。デフォルト値は 15 秒です。

ステップ 6 インターフェイスで EIGRP スプリットホライズンを有効にするには、[スプリットホライズン（Split Horizon）] チェックボックスをオンにします。

ステップ 7 [遅延時間（Delay Time）] フィールドに、遅延時間を 10 マイクロ秒単位で入力します。有効な値は、1 ～ 16777215 です。このオプションは、マルチコンテキストモードのデバイスではサポートされています。

ステップ 8 認証プロパティの値を指定します。

- [MD5認証の有効化（Enable MD5 Authentication）]：EIGRP パケットの認証に MD5 ハッシュアルゴリズムを使用するには、このチェックボックスをオンにします。
- [キータイプ（Key Type）]：このドロップダウンから、次のいずれかのキータイプを選択します。
  - [なし（None）]：認証が必要ないことを示します。
  - [非暗号化（Unencrypted）]：使用されるキー文字列がクリアテキストの認証用パスワードであることを示します。
  - [暗号化（Encrypted）]：使用されるキー文字列が暗号化された認証用パスワードであることを示します。
  - [認証キー（Auth Key）]：使用されるキー文字列が EIGRP 認証キーであることを示します。
- [キーID（Key ID）]：EIGRP 更新の認証に使用されるキーの ID。数値のキー ID を入力します。有効値の範囲は 0 ～ 255 です。
- [キー（Key）]：最大 17 文字の英数字文字列。暗号化された認証タイプの場合は、このフィールドに 17 文字以上の文字列が必要です。
- [キーの確認（Confirm Key）]：キーを再入力します。

ステップ 9 [OK] をクリックし、[保存（Save）] をクリックして設定を保存します。

EIGRP の高度な設定の指定

ルータ ID、スタブルーティング、隣接関係の変更など、EIGRP の詳細設定を設定します。

手順

ステップ 1 [EIGRP] ページで [詳細（Advanced）] タブをクリックします。

ステップ 2 [デフォルトルート情報（Default Route Information）] で、EIGRP アップデート内のデフォルトルート情報の送受信を指定できます。

- （非クラスタおよびスパンド EtherChannel モードのクラスタの場合に表示）[ルータID（IP アドレス）（Router ID (IP Address)）]：外部ルートの発信元ルータを識別するために使用される ID を入力します。外部ルートがローカルのルータ ID で受信された場合、このルートは廃棄されます。この問題を回避するには、ルータ ID のグローバルアドレスを指定します。各 EIGRP ルータには、一意の値を設定する必要があります。
- （個別インターフェイスモードのクラスタの場合にのみ表示）[IPv4アドレスプール（IPv4 Address Pool）]：関連するクラスタプール値（IPv4 アドレスプールオブジェクト）を選択します。アドレスプールを作成するには、アドレス プール を参照して ください。
- [デフォルトのルート情報を受け入れる（Accept Default Route Info）]：外部のデフォルトルーティング情報を受け入れるように EIGRP を設定するには、このチェックボックスをオンにします。
  - [アクセスリスト（Access List）]：[アクセスリスト（Access List）] ドロップダウンから、デフォルトルート情報の受信時に許可するネットワークと許可しないネットワークを定義する標準アクセスリストを指定します。新しい標準アクセスリストオブジェクトを追加するには、[追加（Add）] (+) をクリックし、詳細な手順について 標準 ACL オブジェクトの設定 を参照してください。
- [デフォルトのルート情報を送信する（Send Default Route Info）]：外部のデフォルトルーティング情報をアドバタイズするように EIGRP を設定するには、このチェックボックスをオンにします。
  - [アクセスリスト（Access List）]：[アクセスリスト（Access List）] ドロップダウンから、デフォルトルート情報の送信時に許可するネットワークと許可しないネットワークを定義する標準アクセスリストを指定します。新しい標準アクセスリストオブジェクトを追加するには、[追加（Add）] (+) をクリックし、詳細な手順について 標準 ACL オブジェクトの設定 を参照してください。

ステップ 3 [アドミニストレーティブ ディスタンス（Administrative Distance）] で、次の項目を指定します。

- [内部ディスタンス（Internal Distance）]：EIGRP 内部ルートのアドミニストレーティブディスタンスです。内部ルートとは、同じ自律システム内の別のエンティティから学習されるルートです。有効値の範囲は、1 ～ 255 です。デフォルトは 90 です。
- [外部ディスタンス（External Distance）]：EIGRP 外部ルートのアドミニストレーティブディスタンスです。外部ルートとは、最適パスを自律システムの外部にあるネイバーから学習するルートです。有効値の範囲は、1 ～ 255 です。デフォルト値は 170 です。

ステップ 4 [隣接関係の変更（Adjacency Changes）] で、次の項目を指定します。

- [ログネイバーの変更（Log Neighbor Changes）]：EIGRP ネイバーの隣接関係の変更に関するロギングを有効にするには、このチェックボックスをオンにします。

- [ログネイバーの警告（Log Neighbor Warnings）]：EIGRP ネイバーの警告メッセージのロギングを有効にするには、このチェックボックスをオンにします。
- （任意）ネイバー警告メッセージの反復時間間隔（秒数）を入力します。有効値の範囲は 1 ～ 65535 です。この間隔内に警告が繰り返し発生した場合、それらの警告はログに記録されません。

ステップ 5 EIGRP スタブルーティングプロセスとしてデバイス有効にするには、[スタブ（Stub）] にある次の EIGRP スタブルーティングプロセスのチェックボックスを 1 つ以上オンにします。

- [受信のみ（Receive only）]：ネイバールータからルート情報を受信しても、そのネイバールータにはルート情報を送信しない EIGRP スタブルーティングプロセスを設定します。このオプションを選択する場合は、他のスタブ ルーティング オプションを選択できません。
- [接続済み（Connected）]：接続済みルートをアドバタイズします。
- [再配布済み（Redistributed）]：再配布済みルートをアドバタイズします。
- [スタティック（Static）]：スタティックルートをアドバタイズします。
- [サマリー（Summary）]：サマリールートをアドバタイズします。

ステップ 6 [デフォルトのメトリック（Default Metrics）] で、EIGRP ルーティングプロセスに再配布されるルートのデフォルトのメトリックを定義します。

- [帯域幅（Bandwidth）]：ルートの最小帯域幅（キロビット/秒）。有効値の範囲は 1 ～ 4294967295 です。
- [遅延時間（Delay Time）]：ルートの遅延（10 マイクロ秒）。有効値の範囲は、0 ～ 4294967295 です。
- [信頼性（Reliability）]：0 ～ 255 の数値で表現した、パケットが正常に伝送される見込み。値 255 は 100 % の信頼性を意味し、0 は信頼性がないことを表します。
- [ローディング（Loading）]：ルートの実効帯域幅。有効値の範囲は 1 ～ 255 で、255 は負荷が 100 % であることを示します。
- [MTU]：パスの最大伝送単位の最小許容値。有効値の範囲は 1 ～ 65535 です。

EIGRP の履歴

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
EIGRP 設定	7.2	任意（Any）	以前のリリースでは、EIGRP は FlexConfig を介してのみ Threat Defense で設定できました。FlexConfig は、EIGRP 設定をサポートしなくなりました。Management Center の UI で Threat Defense 用の EIGRP 設定を構成できるようになりました。 新規/変更された画面：**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[ルーティング（Routing）]** > **[EIGRP]**。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。