Firepower Threat Defense の BGP

この項では、Border Gateway Protocol（BGP）を使用してデータのルーティング、認証の実行、ルーティング情報の再配布を行うように Firepower Threat Defense を設定する方法について説明します。

BGP について

BGP は相互および内部の自律システムのルーティング プロトコルです。自律システムとは、共通の管理下にあり、共通のルーティング ポリシーを使用するネットワークまたはネットワーク グループです。BGP は、インターネットのルーティング情報を交換するために、インターネット サービス プロバイダー（ISP）間で使用されるプロトコルです。

ルーティング テーブルの変更

BGP ネイバーは、ネイバー間で最初に TCP 接続を確立する際に、完全なルーティング情報を交換します。ルーティング テーブルで変更が検出された場合、BGP ルータはネイバーに対し、変更されたルートのみを送信します。BGP ルータは、定期的にルーティング アップデートを送信しません。また BGP ルーティング アップデートは、宛先ネットワークに対する最適パスのアドバタイズのみを行います。

BGP により学習されたルートには、特定の宛先に対して複数のパスが存在する場合、宛先に対する最適なルートを決定するために使用されるプロパティが設定されています。これらのプロパティは BGP 属性と呼ばれ、ルート選択プロセスで使用されます。

- [重要度（Weight）]：これは、シスコ定義の属性で、ルータに対してローカルです。[重要度（Weight）] 属性は、隣接ルータにアドバタイズされません。ルータが同じ宛先への複数のルートがあることを学習すると、[重要度（Weight）] 属性値が最も大きいルートが優先されます。

- [ローカル プリファレンス（Local preference）]：この属性は、ローカル AS からの出力点を選択するために使用されます。[重要度（Weight）] 属性とは異なり、[ローカルプリファレンス（Local preference）] 属性は、ローカル AS 全体に伝搬されます。AS からの出力点が複数ある場合は、[ローカル プリファレンス（Local preference）] 属性値が最も高い出力点が特定のルートの出力点として使用されます。
- [Multi-Exit 識別子（Multi-exit discriminator）]：メトリック属性である Multi-Exit 識別子（MED）は、メトリックをアドバタイズしている AS への優先ルートに関して、外部 AS への提案として使用されます。これが提案と呼ばれるのは、MED を受信している外部 AS がルート選択の際に他の BGP 属性も使用している可能性があるためです。MED メトリックが小さい方のルートが優先されます。
- [発信元（Origin）]：この属性は、BGP が特定のルートについてどのように学習したかを示します。[発信元（Origin）] 属性は、次の 3 つの値のいずれかに設定することができ、ルート選択に使用されます。
  - [IGP]：ルートは発信側 AS の内部にあります。この値は、ネットワーク ルータ コンフィギュレーション コマンドを使用して BGP にルートを挿入する際に設定されます。
  - [EGP]：ルートは Exterior Border Gateway Protocol（EBGP）を使用して学習されます。
  - [未完了（Incomplete）]：ルートの送信元が不明であるか、他の方法で学習されています。未完了の発信元は、ルートが BGP に再配布されるときに発生します。
- [AS_path]：ルート アドバタイズメントが自律システムを通過すると、ルート アドバタイズメントが通過した AS 番号が AS 番号の順序付きリストに追加されます。AS_path リストが最も短いルートのみ、IP ルーティング テーブルにインストールされます。
- [ネクスト ホップ（Next hop）]：EBGP の [ネクスト ホップ（Next hop）] 属性は、アドバタイズしているルータに到達するために使用される IP アドレスです。EBGP ピアの場合、ネクスト ホップ アドレスは、ピア間の接続の IP アドレスです。IBGP の場合、EBGP のネクスト ホップ アドレスがローカル AS に伝送されます。
- [コミュニティ（Community）]：この属性は、ルーティングの決定（承認、優先度、再配布など）を適用できる宛先をグループ化する方法、つまりコミュニティを提供します。ルート マップは、[コミュニティ（Community）] 属性を設定するために使用されます。定義済みの [コミュニティ（Community）] 属性は次のとおりです。
  - [no-export]：EBGP ピアにこのルートをアドバタイズしません。
  - [no-advertise]：このルートをどのピアにもアドバタイズしない。
  - [インターネット（internet）]：インターネット コミュニティにこのルートをアドバタイズします。ネットワーク内のすべてのルートがこのコミュニティに属します。

BGP を使用する状況

大学や企業などの顧客ネットワークでは、そのネットワーク内でルーティング情報を交換するために OSPF などの内部ゲートウェイ プロトコル（IGP）を通常使用しています。顧客は ISP

に接続し、ISP は BGP を使用して顧客のルートと ISP のルートを交換します。自律システム（AS）間で BGP を使用する場合、このプロトコルは外部 BGP（EBGP）と呼ばれます。サービス プロバイダーが BGP を使用して AS 内でルートを交換する場合、このプロトコルは内部 BGP（IBGP）と呼ばれます。

BGP は、IPv6 ネットワーク上で IPv6 プレフィックスのルーティング情報を伝送するために使用することもできます。

BGP パスの選択

BGP は、異なる送信元から同じルートの複数のアドバタイズメントを受信する場合があります。BGP はベスト パスとして 1 つのパスだけを選択します。このパスを選択すると、BGP は IP ルーティング テーブルに選択したパスを格納し、そのネイバーにパスを伝搬します。BGP は次の基準を使用して（示されている順序で）、宛先へのパスを選択します。

- パスで指定されているネクストホップが到達不能な場合、この更新はドロップされます。
- ウェイトが最大のパスが優先されます。
- ウェイトが同じである場合、ローカルの優先順位が最大のパスが優先されます。
- ローカルの優先順位が同じである場合、このルータで動作している BGP により発信されたパスが優先されます。
- ルートが発信されていない場合、AS_path が最短のルートが優先されます。
- すべてのパスの AS_path の長さが同じである場合、起点タイプが最下位のパス（[IGP] は [EGP] よりも低く、[EGP] は [不完全（Incomplete）] よりも低い）が優先されます。
- 起点コードが同じである場合、最も小さい MED 属性を持つパスが優先されます。
- パスの MED が同じである場合、内部パスより外部パスが優先されます。
- それでもパスが同じである場合、最も近い IGP ネイバーを経由するパスが優先されます。
- BGP マルチパス （3 ページ） のルーティング テーブルで、複数のパスのインストールが必要かどうかを判断します。
- 両方のパスが外部の場合、最初に受信したパス（最も古いパス）が優先されます。
- BGP ルータ ID で指定された、IP アドレスが最も小さいパスが優先されます。
- 送信元またはルータ ID が複数のパスで同じである場合、クラスタ リストの長さが最小のパスが優先されます。
- 最も小さいネイバー アドレスから発信されたパスが優先されます。

BGP マルチパス

BGP マルチパスでは、同一の宛先プレフィックスへの複数の等コスト BGP パスを IP ルーティング テーブルに組み込むことができます。その場合、宛先プレフィックスへのトラフィックは、組み込まれたすべてのパス間で共有されます。

これらのパスは、負荷共有のためのベスト パスと共にテーブルに組み込まれます。BGP マルチパスは、ベストパスの選択には影響しません。たとえば、ルータは引き続き、アルゴリズムに従っていずれかのパスをベスト パスとして指定し、このベスト パスをルータの BGP ピアにアドバタイズします。

同一宛先へのパスをマルチパスの候補にするには、これらのパスの次の特性がベストパスと同等である必要があります。

- Weight
- ローカル プリファレンス
- AS-PATH の長さ
- オリジン コード
- Multi Exit Discriminator（MED）
- 次のいずれかです。
  - ネイバー AS またはサブ AS（BGP マルチパスの追加前）
  - AS-PATH（BGP マルチパスの追加後）

一部の BGP マルチパス機能では、マルチパス候補に要件が追加されます。

- パスは外部ネイバーまたは連合外部ネイバー（eBGP）から学習される必要があります。
- BGP ネクスト ホップへの IGP メトリックは、ベストパス IGP メトリックと同等である必要があります。

内部 BGP（iBGP）マルチパス候補の追加要件を次に示します。

- 内部ネイバー（iBGP）からパスが学習される必要があります。
- ルータが不等コスト iBGP マルチ パス用に設定されていない限り、BGP ネクストホップへの IGP メトリックは、ベスト パス IGP メトリックと同等です。

BGP はマルチパス候補から最近受信したパスのうち、最大 *n* 本のパスを IP ルーティング テーブルに挿入します。この *n* は、BGP マルチパスの設定時に指定した、ルーティング テーブルに組み込まれるルートの数です。マルチパスが無効な場合のデフォルト値は 1 です。

不等コスト ロード バランシングの場合、BGP リンク帯域幅も使用できます。

（注） 内部ピアへの転送前に、eBGP マルチパスで選択されたベストパスに対し、同等の next-hop-self が実行されます。

BGP のガイドライン

ファイアウォール モードのガイドライン

トランスペアレント ファイアウォール モードはサポートされません。BGP は、ルータ モードでのみサポートされています。

IPv6 のガイドライン

IPv6 をサポートします。グレースフル リスタートは、IPv6 アドレス ファミリではサポートされません。

BGP の設定

BGP を設定するには、以下のトピックを参照してください。

手順

ステップ 1 BGP 基本設定 （5 ページ）
ステップ 2 BGP 一般設定 （8 ページ）
ステップ 3 BGP ネイバーの設定 （10 ページ）
ステップ 4 BGP 集約アドレス設定 （15 ページ）
ステップ 5 BGPv4 フィルタリング設定 （16 ページ）

（注） フィルタリング セクションは、IPv4 設定にのみ適用されます。

ステップ 6 BGP ネットワーク設定 （17 ページ）
ステップ 7 BGP 再配布設定 （17 ページ）
ステップ 8 BGP ルート注入の設定 （18 ページ）

BGP 基本設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	該当なし	Firepower Threat Defense	任意（Any）	Access Admin Administrator Network Admin

BGP の多くの基本設定が可能です。

手順

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

ステップ 2 [ルーティング（Routing）] タブを選択します。

ステップ 3 [BGP] を選択します。

ステップ 4 [BGP を有効にする（Enable BGP）] チェックボックスを選択して、BGP 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、BGP プロセスの自律システム（AS）番号を入力します。AS 番号内部には、複数の自律番号が含まれます。AS 番号には、1 ～ 4294967295 または 1.0 ～ 65535.65535 を指定できます。AS 番号は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 （オプション）General でさまざまな BGP 設定を編集します。これらの設定のデフォルトはほとんどの場合で適切ですが、ネットワークのニーズに合わせて調整できます。[編集（Edit）]（鉛筆）ボタンをクリックして、グループの設定を編集します。

a) [ルータ ID（Router ID）] ドロップダウンリストで、[自動（Automatic）] または [手動（Manual）] を選択します。自動を選択すると、Firepower Threat Defense デバイス上で最上位の IP アドレスがルータ ID として使用されます。固定ルータ ID を使用するには、[手動（Manual）] を選択して、[IP アドレス（IP Address）] フィールドに IPv4 アドレスを入力します。デフォルト値は [自動（Automatic）] です。

b) [AS_パス属性の AS 番号の数（number of AS numbers in AS_PATH attribute）] を入力します。AS パス属性は、移動パケットの最短ルートになる送信元と宛先のルータ間の中間 AS 番号のシーケンスです。有効な値は、1 ～ 254 です。デフォルト値は None です。

c) [ログ ネイバー変更（Log Neighbor Changes）] チェックボックスをオンにして、BGP ネイバーの変更（アップ状態またはダウン状態）およびリセットのロギングをイネーブルにします。これは、ネットワーク接続の問題をトラブルシューティングしたり、ネットワークの安定性を評価する際に役に立ちます。この設定はデフォルトで有効になっています。

d) [TCP パス MTU ディスカバリ使用（Use TCP path MTU discovery）] チェックボックスをオンにし、パス MTU 手法を使用して 2 つの IP ホスト間のネットワーク パスにおける最大伝送単位（MTU）のサイズを決定します。これにより、IP フラグメンテーションが回避されます。この設定はデフォルトで有効になっています。

e) [フェールオーバー後すぐにセッションをリセット（Reset session upon Failover）] チェックボックスをオンにして、リンク障害の発生時に外部 BGP セッションをただちにリセットします。この設定はデフォルトで有効になっています。

f) [最初の AS を EBGP ルートのピアの AS として実行（Enforce that first AS is peer's AS for EBGP routes）] チェックボックスをオンにして、その AS 番号を AS_path 属性の 1 つ目のセグメントとしてリストしていない外部 BGP ピアから受信した着信アップデートを破棄します。これにより、誤って設定されたピアや許可されていないピアが、別の自律システムから送信されたかのようにルートをアドバイタイズしてトラフィックを誤った宛先に送信することがなくなります。この設定はデフォルトで有効になっています。

g) [AS 番号のドット表記を使用（Use dot notation for AS numbers）] チェックボックスをオンにして、完全なバイナリ 4 バイトの AS 番号を、ドットで区切られた 16 ビットの 2 文字ず

つに分割します。0 ～ 65553 の AS 番号は 10 進数で表され、65535 を超える AS 番号はドット付き表記を使用して表されます。これは、デフォルトでは無効になっています。

h) [OK] をクリックします。

ステップ 7 （オプション）[ベスト パス選択（Best Path Selection）] セクションを編集します。

a) [デフォルト ローカル優先度（Default Local Preference）] で 0 ～ 4294967295 の値を入力します。デフォルト値は 100 です。値が大きいほど、優先度が高いことを示します。この優先度は、ローカル自律システム内のすべてのルータおよびアクセス サーバに送信されます。

b) [異なるネイバーからの MED 比較を許可（Allow comparing MED from different neighbors）] チェックボックスをオンにして、さまざまな自律システムのネイバーからのパスにおいて Multi-exit discriminator（MED）の比較ができるようにします。これは、デフォルトでは無効になっています。

c) [同一 EBGP パスのルータ ID を比較（Compare Router ID for identical EBGP paths）] チェックボックスをオンにして、最適なパスの選択プロセス中に、外部BGP ピアから受信した類似のパスを比較し、最適なパスをルータ IDが最も小さいルートに切り替えます。これは、デフォルトでは無効になっています。

d) [隣接する AS がアドバタイズしたパス間の最適 MED を選別（Pick the best MED path among paths advertised from the neighboring AS）] チェックボックスをオンにして、連合ピアから学習したパス間における MED 比較を有効にします。MED 間の比較は、外部の自律システムがパスに存在しない場合にのみ行われます。これは、デフォルトでは無効になっています。

e) [欠落 MED を最低優先度として処理（Treat missing MED as the least preferred one）] チェックボックスをオンにして、欠落している MED 属性は無限大の値を持つものとみなし、このパスを最も推奨度の低いパスにします。したがって、MED が欠落しているパスが最も優先度が低くなります。これは、デフォルトでは無効になっています。

f) [OK] をクリックします。

ステップ 8 （オプション）[ネイバー タイマー（Neighbor Timers）] セクションを編集します。

a) [キープアライブ インターバル（Keepalive interval）] フィールドでキープアライブ メッセージを送信しなかった場合に、その後 BGP ネイバーがアクティブな状態を維持する時間間隔を入力します。このキープアライブ インターバルが終わると、メッセージが送信されない場合、BGP ピアはデッドとして宣言されます。デフォルト値は 60 秒です。

b) [維持時間（Hold Time）] フィールドで、BGP 接続が開始、設定されている間、BGP ネイバーがアクティブな状態を維持する時間間隔を入力します。デフォルト値は 180 秒です。

c) （オプション）[最小維持時間（Min Hold time）] フィールドで、BGP 接続が開始、設定されている間、BGP ネイバーがアクティブな状態を維持する最小時間間隔を入力します。0 ～ 65535 の値を指定します。

d) [OK] をクリックします。

ステップ 9 （オプション）[グレースフル リスタート（Graceful Restart）] セクションを編集します。

（注） このセクションは、Firepower Threat Defenseデバイスがフェールオーバーまたはスパンド クラスタ モードになっているときにのみ使用できます。フェールオーバー設定のデバイスの 1 つが失敗した場合に、トラフィック フローのパケットでドロップがないように行われるものです。

a) [グレースフル リスタートを有効にする（Enable Graceful Restart）] チェックボックスをオンにして、Firepower Threat Defense ピアがスイッチオーバー後のルート フラップを回避できるようにします。
b) [リスタート時間（Restart Time）] フィールドで BGP オープン メッセージが受信される前に、Firepower Threat Defenseピアが古いルートを削除するまでの待機時間を入力します。デフォルト値は 120 秒です。有効な値は 1 ～ 3600 秒です。
c) [Stalepath 時間（Stalepath Time）] フィールドで、リスタートする Firepower Threat Defense から End Of Record（EOR）メッセージを受信した後、Firepower Threat Defenseが古いルートを削除するまでの待機時間を入力します。デフォルト値は 360 秒です。有効な値は 1 ～ 3600 秒です。
d) [OK] をクリックします。

ステップ 10 [保存（Save）] をクリックします。

BGP 一般設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	該当なし	Firepower Threat Defense	任意（Any）	Access Admin Administrator Network Admin

ルートマップ、アドミニストレーティブルートディスタンス、同期、ネクストホップ、パケット転送を設定します。これらの設定のデフォルトはほとんどの場合で適切ですが、ネットワークのニーズに合わせて調整できます。

手順

ステップ 1 **[ルーティング（Routing）]** > **[BGP]** > **[IPv4]** または **[Ipv6]** に進み、**[一般（General）]** タブを選択します。

ステップ 2 [一般（General）] タブで、次のセクションを更新します。

a) [設定（Settings）] セクションで、[ルート マップ（Route Map）] オブジェクトを入力または選択して、ネクストホップ検証用の BGP ルータの [スキャン インターバル（Scanning Interval）] を入力します。有効な値は 5 ～ 60 秒です。デフォルト値は 60 です。[OK] をクリックします。

（注） [ルート マップ（Route Map）] フィールドは、IPv4 設定にのみ適用されます。

b) [ルートと同期化（Routes and Synchronization）] セクションで、必要に応じて以下を更新し、[OK] をクリックします。

- （オプション）[デフォルト ルートの生成（Generate Default Routes）]：これを選択して、デフォルト ルート（ネットワーク 0.0.0.0）を配布するように BGP ルーティング プロセスを設定します。
- （オプション）[サブネット ルートのネットワーク レベル ルートへの集約（Summarize subnet routes into network-level routes）]：これを選択して、ネットワーク レベルのルートへのサブネット ルートの自動集約を設定します。このチェックボックスを適用できるのは、IPv4 設定だけです。
- （オプション）[非アクティブなルートのアドバタイズ（Advertise inactive routes）]：これを選択して、ルーティング情報ベース（RIB）にインストールされていないルートをアドバタイズします。
- （オプション）[BGP と IGP システム間の同期化（Synchronise between BGP and IGP system）]：これを選択して、BGP と内部ゲートウェイ プロトコル（IGP）システムの間の同期を有効にします。通常、ルートがローカルであるか IGP に存在する場合を除き、BGP スピーカーは外部ネイバーにルートをアドバタイズしません。この機能により、自律システム内のルータおよびアクセス サーバは、BGP が他の自律システムでルートを使用可能にする前にルートを確保できるようになります。
- （オプション）[IBGP の IGP への再配布（Redistribute IBGP into IGP）]：これを選択して、OSPF などの内部ゲートウェイ プロトコル（IGP）への iBGP の再配布を設定します。

c) [アドミニストレーティブ ルート ディスタンス（Administrative Route Distances）] セクションで、必要に応じて以下を更新し、[OK] をクリックします。

- [外部（External）]：外部 BGP 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。外部自律システムから学習されたルートは、外部ルートです。この引数の値の範囲は 1 ～ 255 です。デフォルト値は 20 です。
- [内部（Internal）]：内部 BGP 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。ローカル自律システムのピアから学習されたルートは、内部ルートです。この引数の値の範囲は 1 ～ 255 です。デフォルト値は 200 です。
- [ローカル（Local）]：ローカル BGP 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。ローカル ルートは、別のプロセスから再配布されているルータまたはネットワークの、多くの場合バック ドアとして、ネットワーク ルータ表示コマンドによりリストされるネットワークです。この引数の値の範囲は 1 ～ 255 です。デフォルト値は 200 です。

d) [ネクスト ホップ（Next Hop）] セクションで、必要に応じて BGP ネクストホップ アドレスを有効にする [アドレス追跡を有効にする（Enable address tracking）] チェックボックスを選択し、ルーティング テーブルにインストールされた更新ネクストホップ ルートのチェックの間で [遅延インターバル（Delay Interval）] を入力します。[OK] をクリックします。

（注） [ネクスト ホップ（Next Hop）] セクションは、IPv4 設定にのみ適用されます。

e) [多重パスでパケットを転送（Forward Packets over Multiple Paths）] セクションで、必要に応じて以下を更新し、[OK] をクリックします。

- （オプション）[パスの数（Number of Paths）] : ルーティング テーブルにインストール可能な Border Gateway Protocol ルートの最大数を指定します。値の範囲は 1 ～ 8 です。デフォルト値は 1 です。
- （オプション）[IBGP パスの数（IBGP Number of Paths）] : ルーティング テーブルにインストール可能な並行内部ボーダー ゲートウェイ プロトコル（IBGP）ルートの最大数を指定します。値の範囲は 1 ～ 8 です。デフォルト値は 1 です。

ステップ 3 [保存（Save）] をクリックします。

BGP ネイバーの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	該当なし	Firepower Threat Defense	任意（Any）	Access Admin Administrator Network Admin

BGP ルータは更新を交換する前に、各ピアとの接続を確立する必要があります。これらのピアは BGP ネイバーと呼ばれます。[ネイバー（Neighbor）] タブを使用して、BGP IPv4 または IPv6 ネイバーとネイバーの設定を定義します。

手順

ステップ 1 **[ルーティング（Routing）] > [BGP] > [IPv4]** または [IPv6] を選択し、[ネイバー（Neighbor）] タブをクリックします。

ステップ 2 [追加（Add）] をクリックして、BGP ネイバーとネイバーの設定を定義します。

ステップ 3 BGP ネイバーの **IP アドレス**を入力します。この IP アドレスは、BGP ネイバー テーブルに追加されます。

ステップ 4 BGP ネイバーの**インターフェイス**を入力します。

（注） [インターフェイス（Interface）] フィールドは、IPv6 の設定にのみ適用されます。

ステップ 5 [リモート AS（Remote AS）] フィールドに、BGP ネイバーが属する自律システムを入力します。

ステップ 6 [有効アドレス（Enabled address）] チェックボックスをオンにして、BGP ネイバーとの通信を有効にします。[有効アドレス（Enabled address）] チェックボックスがオンの場合にのみ、追加のネイバー設定が行われます。

ステップ 7 （オプション）[管理シャットダウン（Shutdown administratively）] チェックボックスをオンにして、ネイバーまたはピア グループを無効化します。

ステップ 8 （オプション）[グレースフル リスタートの設定（Configure graceful restart）] チェックボックスをオンにして、このネイバーの BGP グレースフル リスタート機能の設定を有効にします。このオプションを選択した後、[グレースフル リスタート（フェールオーバー/スパンド モード）（Graceful Restart (failover/spanned mode)）] オプションを使用して、このネイバーに対してグレースフル リスタートを有効にするか、または無効にするかを指定する必要があります。

（注） [グレースフル リスタート（graceful restart）] フィールドは、IPv4 の設定にのみ適用されます。

ステップ 9 （オプション）BGP ネイバーの**説明**を入力します。

ステップ 10 （オプション）[ルートのフィルタリング（Filtering Routes）] タブで、必要に応じてアクセス リスト、ルートマップ、プレフィックス リスト、および AS パスのフィルタを使用して、BGP ネイバー情報を配布します。次の各セクションを更新します。

a) 適切な着信または発信**アクセス リスト**を入力または選択して、BGP ネイバー情報を配布します。

（注） アクセス リストは、IPv4 の設定にのみ適用されます。

b) 適切な着信または発信**ルートマップ**を入力または選択して、着信または発信ルートにルート マップを適用します。

c) 適切な着信または発信**プレフィックス リスト**を入力または選択して、BGP ネイバー情報を配布します。

d) 適切な着信または発信 **AS パス フィルタ**を入力または選択して、BGP ネイバー情報を配布します。

e) （オプション）[ネイバーから許可されるプレフィックスの数を制限する（Limit the number of prefixes allowed from the neighbor）] チェックボックスをオンにして、ネイバーから受信できるプレフィックスの数を制御します。

- [最大プレフィックス数（Maximum Prefixes）] フィールドに、特定のネイバーからの許可される最大プレフィックス数を入力します。
- [しきい値レベル（Threshold Level）] フィールドに、ルータが警告メッセージの生成を開始するパーセンテージ（最大数に対する割合）を入力します。有効な値は 1 ～ 100 の整数です。デフォルト値は 75 です。

f) [ピアから受信したプレフィックスを制御する（Control prefixes received from the peer）] チェックボックスをオンにし、ピアから受信したプレフィックスに対する追加の制御を指定します。次のいずれかを実行します。

- プレフィックス数の制限値に到達したときに BGP ネイバーを停止するには、[プレフィックス数の制限値を超えたときにピアリングを停止する（Terminate peering when prefix limit is exceeded）] ラジオ ボタンを選択します。[再起動間隔（Restart interval）] フィールドで、BGP ネイバーが再起動するまでの時間を指定します。

- 最大プレフィックス数の制限値を超えたときにログ メッセージを生成するには、[プレフィックス数の制限値を超えたときに警告メッセージのみを表示する（Give only warning message when prefix limit is exceeded）] ラジオ ボタンを選択します。この場合、BGP ネイバーは終了しません。

g) [OK] をクリックします。

ステップ 11 （オプション）[ルート（Routes）] タブで、その他のネイバー ルート パラメータを指定します。次を更新します。

a) [アドバタイズメントの間隔（Advertisement Interval）] フィールドに、BGP ルーティング アップデートが送信される最小間隔（秒）を入力します。有効な値は、1 ～ 600 です。

b) [発信ルーティング更新からプライベート AS 番号を削除する（Remove private AS numbers from outbound routing updates）] を選択して、プライベート AS 番号を発信ルートにおけるアドバタイズ対象から除外します。

c) [デフォルト ルートの生成（Generate default routes）] チェックボックスをオンにして、ローカル ルータにネイバーへのデフォルト ルート 0.0.0.0 の送信を許可して、このルートがデフォルト ルートとして使用されるようにします。[ルート マップ（Route map）] フィールドで、ルート 0.0.0.0 が条件に応じて注入されるように許可するルート マップを入力または選択します。

d) 条件に応じてアドバタイズされるルートを追加するには、[行を追加（Add Row）]（+）ボタンをクリックします。[アドバタイズ対象ルートの追加（Add Advertised Route）] ダイアログボックスで、次の手順を実行します。

1. [アドバタイズ マップ（Advertise Map）] フィールドで、exist-map または非存在マップの条件が満たされた場合にアドバタイズされるルート マップを追加または選択します。
2. [exist-map（Exist Map）] ラジオ ボタンを選択し、[ルート マップ オブジェクト セレクタ（Route Map Object Selector）] からルート マップを選択します。このルート マップは、advertise-map のルートがアドバタイズされるかどうかを判断するために BGP テーブル内のルートと比較されます。
3. [非存在マップ（Non-Exist Map）] ラジオ ボタンを選択し、[ルート マップ オブジェクト セレクタ（Route Map Object Selector）] からルート マップを選択します。このルート マップは、advertise-map のルートがアドバタイズされるかどうかを判断するために BGP テーブル内のルートと比較されます。
4. [OK] をクリックします。

ステップ 12 [タイマー（Timers）] タブで [BGP ピアの時間を設定する（Set Timers for the BGP Peer）] チェックボックスをオンにし、キープアライブ頻度、保留時間、最小保留時間を設定します。

- [キープアライブ インターバル（Keepalive Interval）]：Firepower Threat Defense デバイスがキープアライブ メッセージをネイバーに送信する頻度（秒）を入力します。有効な値は、0 ～ 65535 です。デフォルト値は 60 秒です。

- [保留時間（Hold time）]：キープアライブ メッセージを受信できない状態が継続して、ピアがデッドであると Firepower Threat Defense デバイスが宣言するまでの時間（秒）を入力します。有効な値は、0 ～ 65535 です。デフォルト値は 180 秒です。
- [最小保留時間（Min hold time）]：（オプション）キープアライブ メッセージを受信できない状態が継続して、ピアがデッドであると Firepower Threat Defense デバイスが宣言するまでの最小時間（秒）を入力します。有効な値は、0 ～ 65535 です。デフォルト値は 0 秒です。

ステップ 13 [詳細（Advanced）] タブで、次を更新します。

a) （オプション）[認証を有効にする（Enable Authentication）] を選択して、2 つの BGP ピア間の TCP 接続で MD5 認証を有効にします。

1. [暗号化を有効にする（Enable Encryption）] ドロップダウン リストから暗号化タイプを選択します。
2. パスワードを [パスワード（Password）] フィールドに入力します。[確認（Confirm）] フィールドにパスワードを再入力します。パスワードは大文字と小文字を区別し、service password-encryption コマンドが有効な場合は最大 25 文字、service password-encryption コマンドが有効でない場合は最大 81 文字を指定できます。最初の文字を数値にはできません。この文字列には、スペースも含め、あらゆる英数字を使用できます。

（注） 数字-スペース-任意の文字の形式でパスワードを指定することはできません。数字の後にスペースを使用すると、認証に失敗する原因となることがあります。

b) （オプション）[このネイバーにコミュニティ属性を送信する（Send Communty attribute to this neighbor）] チェックボックスをオンにして、コミュニティ属性を BGP ネイバーに送信することを指定します。

c) （オプション）[このネイバーのネクスト ホップとして FTD を使用する（Use FTD as next hop for this neighbor）] チェックボックスをオンにし、ルータを BGP スピーキング ネイバーまたはピア グループのネクスト ホップとして設定します。

d) [接続の検証を無効にする（Disable Connection Verification）] チェックボックスをオンにして、シングルホップで到達可能な eBGP ピアリング セッションについての接続の検証プロセスを無効にします。これにより、ループバック インターフェイスで設定されたピアや直接接続されない IP アドレスが設定されたピアとの間でセッションを確立することができます。オフ（デフォルト）にすると、シングルホップ eBGP ピアリング セッション（TTL=254）について、BGP ルーティング プロセスで接続が検証され、eBGP ピアが同じネットワーク セグメントに直接接続されているかどうか確認されます。ピアが同じネットワーク セグメントに直接接続されていない場合、ピアリング セッションは確立されません。

e) [直接接続されていないネイバーとの接続を許可する（Allow connections with neighbor that is not directly connected）] ラジオ ボタンを選択して、直接接続されていないネットワーク上で外部ピアからの BGP 接続を受け入れ、またそのピアへの BGP 接続を試みます。（オプション）[TTL ホップ（TTL hops）] フィールドに存続可能時間を入力します。有効な値は、1 ～ 255 です。または、[ネイバーへの TTL ホップの制限数（Limited number of TTL

hops to neighbor）] ラジオ ボタンを選択して、BGP ピアリング セッションを保護します。[TTL ホップ（TTL hops）] フィールドに、eBGP ピアを区切るホップの最大数を入力します。 有効な値は、1 ～ 254 です。

f) （オプション）[TCP MTU パス検出の使用（Use TCP MTU path discovery）] チェックボックスをオンにして、BGP セッションの TCP トランスポート セッションを有効にします。

g) [TCP トランスポート モード（TCP Transport Mode）] ドロップダウン リストから TCP 接続モードを選択します。オプションは [デフォルト（Default）]、[アクティブ（Active）]、または [パッシブ（Passive）] です。

h) （オプション）BGP ネイバー接続の**ウェイト**を入力します。

i) ドロップダウン リストから Firepower Threat Defense デバイスが受け入れる **BGP バージョン**を選択します。[4 のみ（4-Only）] に設定すると、指定されたネイバーとの間でバージョン 4 だけが使用されます。デフォルトでは、バージョン 4 が使用され、要求された場合は動的にネゴシエートしてバージョン 2 に下がります。

ステップ 14 AS 移行を考慮する場合にのみ [移行（Migration）] タブを更新します。

（注） AS 移行カスタマイズは、遷移の完了後に削除される必要があります。

a) （オプション）[ネイバーから受信したルートの AS 番号をカスタマイズする（Customize the AS number for routes received from the neighbor）] チェックボックスをオンにして、eBGP ネイバーから受信したルートの AS_path 属性をカスタマイズします。

b) [ローカル AS 番号（Local AS number）] フィールドにローカル自律システム番号を入力します。有効な値は、1 ～ 4294967295 または 1.0 ～ 65535.65535 の有効な自律システム番号です。

c) （オプション）[ローカル AS 番号をネイバーから受信したルートの前に付加しない（Do not prepend local AS number to routes received from neighbor）] チェックボックスをオンにして、ローカル AS 番号が eBGP ピアから受信したルートの前に付加されないようにします。

d) （オプション）[実 AS 番号をネイバーから受信したルートのローカル AS 番号に置き換える（Replace real AS number with local AS number in routes received from neighbor）] チェックボックスをオンにして、実自律システム番号を eBGP 更新のローカル自律システム番号に置き換えます。ローカル BGP ルーティング プロセスからの自律システム番号は、追加されません。

e) （オプション）[実 AS 番号またはネイバーから受信したルートのローカル AS 番号を受け入れる（Accept either real AS number or local AS number in routesreceived from neighbor）] チェックボックスをオンにして、実自律システム番号（ローカル BGP ルーティング プロセスより）またはローカル自律システム番号を使用するピアリングセッションを確立するように eBGP ネイバーを設定します。

ステップ 15 [OK] をクリックします。

ステップ 16 [保存（Save）] をクリックします。

BGP 集約アドレス設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	該当なし	Firepower Threat Defense	任意（Any）	Access Admin Administrator Network Admin

BGP ネイバーはルーティング情報を格納し、交換しますが、設定される BGP スピーカーの数が増えるに従って、ルーティング情報の量が増えます。ルート集約は、複数の異なるルートの属性を合成し、1 つのルートだけがアドバタイズされるようにするプロセスです。集約プレフィックスは、クラスレス ドメイン間ルーティング（CIDR）の原則を使用して、複数の隣接するネットワークを、ルーティング テーブルに要約できる IP アドレスのクラスレス セット 1 つに合成します。結果として、アドバタイズの必要なルートは少なくなります。[集約アドレスの追加/編集（Add/Edit Aggregate Address）] ダイアログボックスで、特定のルートの 1 つのルートへの集約を定義します。

手順

ステップ 1 Firepower Threat Defense デバイスを編集する際、**[ルーティング（Routing）]** > **[BGP]** > **[IPv4]** または **[IPv6]** を選択して、**[集約アドレス（Aggregate Address）]** タブを選択します。

ステップ 2 [集約アドレス（Aggregate Addresses）] タブをクリックします。

ステップ 3 [集約タイマー（Aggregate Timer）] フィールドで、集約タイマーの値（秒）を入力します。有効な値は、0 または 6 ～ 60 の値です。デフォルト値は 30 です。

ステップ 4 [追加（Add）] をクリックして、[集約アドレスの追加（Add Aggregate Address）] ダイアログを更新します。

a) [ネットワーク（Network）]：IPv4 アドレスを入力するか、任意のネットワーク/ホスト オブジェクトを選択します。

b) [集約マップ（Attribute Map）]：（オプション）集約ルートの属性の設定に使用されるルート マップを入力または選択します。

c) [アドバタイズマップ（Advertise Map）]：（オプション）AS 設定の元のコミュニティを作成するルートの選択に使用されるルート マップを入力または選択します。

d) [抑制マップ（Suppress Map）]：（オプション）抑制するルートの選択に使用されるルートマップを入力または選択します。

e) [AS 設定パス情報の生成（Generate AS set path Information）]：（オプション）自律システム設定パス情報の生成を有効にするには、チェックボックスを選択します。

f) [更新から全ルートをフィルタ処理（Filter all routes from updates）]：（オプション）更新からのすべての特定のルートをフィルタ処理するには、チェックボックスを選択します。

g) [OK] をクリックします。

次のタスク

- BGPv4 設定については、次に進みます。 BGPv4 フィルタリング設定 （16 ページ）
- BGPv6 設定については、次に進みます。 BGP ネットワーク設定 （17 ページ）

BGPv4 フィルタリング設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	該当なし	Firepower Threat Defense	任意（Any）	Access Admin Administrator Network Admin

フィルタリング設定は、受信される BGP 更新プログラムのフィルタ処理ルートまたはネットワークに使用されます。フィルタリングは、ルータが学習またはアドバタイズするルーティング情報を制限するために使用されます。

始める前に

フィルタリングは、BGP の IPv4 ルーティング ポリシーでのみ適用されます。

手順

ステップ 1 **[ルーティング（Routing）] > [BGP] > [IPv4]** を選択し、**[フィルタリング（Filtering）]** タブを選択します。

ステップ 2 [追加（Add）] をクリックして、[フィルタの追加（Add Filter）] ダイアログを更新します。

a) [アクセス リスト（Access List）]：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するアクセスコントロールリストを選択します。

b) [指示（Direction）]：（オプション）インバウンド更新、アウトバウンド更新のどちらにフィルタを適用するかを指定する指示を選択します。

c) [プロトコル（Protocol）]：（オプション）なし、BGP、接続中、OSPF、RIP または静的のルーティング プロセスのうち、フィルタ処理するものを選択します。

d) [プロセス ID（Process ID）]：（オプション）OSPF ルーティング プロトコルのプロセス ID を入力します。

e) [OK] をクリックします。

ステップ 3 [保存（Save）] をクリックします。

BGP ネットワーク設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	該当なし	Firepower Threat Defense	任意（Any）	Access Admin Administrator Network Admin

ネットワーク設定は、BGP ルーティング プロセスによってアドバタイズされるネットワーク、アドバタイズされるネットワークのフィルタ処理で確認されるルートマップを追加するために使用されます。

手順

ステップ 1 **[ルーティング（Routing）]** > **[BGP]** > **[IPv4]** または **[IPv6]** に進み、[ネットワーク（Networks）] タブを選択します。

ステップ 2 [追加（Add）] をクリックして、[ネットワークの追加（Add Networks）] ダイアログを更新します。

a) [ネットワーク（Network）]：BGP ルーティング プロセスによってアドバタイズされるネットワークを入力します。

b) （オプション）[ルートマップ（Route Map）]：アドバタイズされるネットワークをフィルタ処理するために調べる必要のあるルートマップを入力または選択します。この値を指定しない場合、すべてのネットワークが再配布されます。

c) [OK] をクリックします。

ステップ 3 [保存（Save）] をクリックします。

BGP 再配布設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	該当なし	Firepower Threat Defense	任意（Any）	Access Admin Administrator Network Admin

再配布設定により、別のルーティング ドメインから BGP にルートを再配布する条件を定義できます。

手順

ステップ 1 **[ルーティング（Routing）] > [BGP > IPv4]** または **[IPv6]** に進み、[再配布（Redistribution）] タブを選択します。

ステップ 2 [追加（Add）] をクリックして、[再配布の追加（Add Redistribution）] ダイアログを更新します。

a) [送信元プロトコル（Source Protocol）]：送信元プロトコル ドロップダウンリストから、どのプロトコルからルートを BGP ドメインに再配布するかを選択します。

b) [プロセス ID（Process ID）]：選択されている送信元プロトコルの識別子を入力します。OSPF プロトコルに適用されます。

c) [メトリック（Metric）]：（オプション）再配布されているルートのメトリックを入力します。

d) [ルートマップ（Route Map）]：再配布されるネットワークをフィルタ処理するために調べる必要のあるルートマップを入力または選択します。この値を指定しない場合、すべてのネットワークが再配布されます。

e) [一致（Match）]：1 つのルーティング プロトコルから別のルーティング プロトコルへのルート再配布に使用される条件。ルートが再配布されるには、選択した条件と一致している必要があります。次の一致条件から 1 つ以上を選択できます。これらのオプションは、OSPF が送信元プロトコルとして選択されているときにのみ有効になります。

- 内線
- 外部 1
- 外部 2
- NSSA 外部 1
- NSSA 外部 2

f) [OK] をクリックします。

BGP ルート注入の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	該当なし	Firepower Threat Defense	任意（Any）	Access Admin Administrator Network Admin

ルート注入設定により、条件に応じて BGP ルーティング テーブルに注入されるルートを定義できます。

手順

ステップ 1 **[ルーティング（Routing）]** > **[BGP]** > **[IPv4]** または **[IPv6]** を選択し、[ルート注入（Route Injection）] タブを選択します。

ステップ 2 [追加（Add）] をクリックして、[ルート注入の追加（Add Route Injection）] ダイアログを更新します。

a) [マップ注入（Inject Map）]：ローカル BGP ルーティング テーブルに注入するプレフィックスを指定するルート マップを入力または選択します。

b) [マップ存在（Exist Map）]：BGP スピーカーが追跡するプレフィックスを含むルート マップを入力または選択します。

c) [注入されたルートが集約ルートの属性を継承（Injected routes will inherit the attributes of the aggregate route）]：これを選択し、集約ルートの属性を継承するよう注入されたルートを設定します。

d) [OK] をクリックします。

ステップ 3 [保存（Save）] をクリックします。