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Firewall Threat Defenseを設定する方法について説明します。

- BGPについて （1 ページ）
- BGP の要件と前提条件 （5 ページ）
- BGP のガイドライン （5 ページ）
- BGP の設定 （6 ページ）
- BGP の履歴 （24 ページ）

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のグループです。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。

（注） AS ループの検出は、完全な AS パス（AS_PATH 属性で指定される）をスキャンし、ローカルシステムの AS 番号が AS パスに現れないことを確認することによって実行されます。デフォルトでは、EBGP は学習したルートを同じピアにアドバタイズすることで、ループチェックを実行するときにデバイスで追加の CPU サイクルが発生することを防ぐとともに、既存の発信更新タスクの遅延を防ぎます。

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。次のプロパティはBGP属性と呼ばれ、ルート選択プロセスで使用されます。

- 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。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、[重み（Weight）] 属性値が最も大きいルートが優先されます。
- Local preference: Local preference属性は、ローカルASからの出口点を選択するために使用されます。Weight属性とは異なり、Local preference属性は、ローカルAS全体に伝搬されます。ASからの出口点が複数ある場合は、Local preference属性が最も高い出口点が特定のルートの出口点として使用されます。
- Multi-exit discriminator: メトリック属性であるMulti-exit discriminator (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。
- Origin: Origin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。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場合に設定されます。
  - EGP: ルートはExterior Border Gateway Protocol (EBGP)を使用して学習されます。
  - 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。IncompleteのOrigin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。
- Next hop: EBGPのnext-hop属性は、アドバタイジング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。ただし、ネクストホップが eBGP ピアのピアリングアドレスと同じサブネットにある場合、ネクストホップは変更されません。この動作は、サードパーティのネクストホップと呼ばれます。

  VPN でアドバタイズされたルートを iBGP ピアに再配布する場合は、**next-hop-self** コマンドを使用して、ルートが正しいネクストホップ IP で再配布されるようにします。
- Community: Community属性は、ルーティングの決定(承認、優先順位、再配布など)を適用できる接続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、Community 属性を設定するために使用されます。事前定義済みのCommunity属性は次のとおりです。

- no-export: EBGPピアにアドバタイズしません。
- no-advertise: どのピアにもこのルートをアドバイタイズしません。
- 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

通常、大学や企業などの顧客ネットワークでは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 Interior Gateway Protocol（IGP）を採用しています。カスタマーはISPに接続し、ISPはBGPを使用してカスタマーおよびISP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内の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も使用することができます。

BGP パスの選択

BGPは、異なる送信元から同じルートに対する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。ベストパスを選択すると、BGPは選択したパスをIPルーティングテーブルに格納し、そのネイバーにパスを伝達します。BGP は、次に示す順序で次の条件を使用して、宛先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、更新はドロップされます。
- 重みが最大のパスが優先されます。
- 重みが同じ場合、ローカルプリファレンスが最大のパスが優先されます。
- ローカルプリファレンスが同じ場合、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 の長さが同じ場合、Origin タイプが最下位のパス（IGP は EGP よりも低く、EGP は Incomplete よりも低い）が優先されます。
- Origin コードが同じ場合、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 （4 ページ） 用のルーティングテーブルに複数のパスをインストールする必要があるか判断します。
- 両方のパスが外部のときは、先に受信したパス(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。
- 発信元 ID またはルータ ID が複数のパスで同じ場合は、最小のクラスタ リスト長を持つ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、同じ宛先プレフィックスへの複数の等コスト BGP パスの IP ルーティングテーブルへのインストールが許可されます。その場合、宛先プレフィックスへのトラフィックは、インストールされたすべてのパス間で共有されます。

これらのパスは、ロードシェアリング用にベストパスとともにテーブルにインストールされます。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、ルータではアルゴリズムに従って、ベストパスとしてパスの 1 つが引き続き指定され、そのベストパスが BGP ピアにアドバタイズされます。

マルチパスの候補になるためには、同じ宛先へのパスに、最適パスの特性に等しいこれらの特性が備わっている必要があります。

- 重量
- ローカル プリファレンス
- AS-PATH length
- オリジン コード
- Multi Exit識別子(MED)
- 次のいずれか。
  - ネイバー AS または sub-AS（BGP マルチパス機能が追加される前）
  - AS-PATH（BGP マルチパス機能が追加された後）

一部の BGP マルチパス機能により、マルチパス候補に関する追加要件が加わりました。

- パスは、外部またはコンフェデレーション外部の近接ルータ（eBGP）から学習されます。
- BGP ネクストホップへの IGP メトリックは、最適パスの IGP メトリックと等しくなる必要があります。

内部 BGP（iBGP）マルチパスの候補には次の追加要件があります。

- パスは、内部の近接ルータ（iBGP）から学習されます。
- ルータが不等コスト iBGP マルチパスで設定されない限り、BGP ネクストホップへの IGP メトリックは、最適パスの IGP メトリックと等しくなる必要があります。

BGP は、マルチパス候補から最近受信した最大 *n* 個のパスを IP ルーティングテーブルに挿入します。ここで、*n* は、BGPマルチパスを設定するときに指定した、ルーティングテーブルに

インストールするルートの数です。マルチパスがディセーブルになっている場合のデフォルト値は 1 です。

不等コスト ロード バランシングでは、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

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、ルーテッド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。

その他のガイドライン

- BGP の場合、ルートのネクストホップ IP アドレスはネットワーク IP アドレスであり、0.0.0.0 ではありません。

- システムは、PPPoE 経由で受信した IP アドレスのルートエントリを CP ルートテーブルに追加しません。BGP は常に CP ルートテーブルを調べて TCP セッションを開始するため、BGP は TCP セッションを形成しません。

  つまり、PPPoE 経由の BGP はサポートされません。

- 管理専用または BVI インターフェイスでは、BGP はサポートされません
- ルートアップデートがリンク上の最小 MTU より大きい場合に、ルートアップデートがドロップされることによる隣接フラップを回避するには、リンクの両側のインターフェイスで同じ MTU を設定する必要があります。
- PATH MTU（PMTU）を使用した BGP は、特に ECMP ルーティングで MTU ディスカバリが失敗した場合に、隣接関係（アジャセンシー）フラップを引き起こす可能性があります。したがって、何らかの理由で MTU ディスカバリが失敗した場合にパケットドロップが発生する可能性があるため、BGP、PMTU、および ECMP の使用時には注意が必要です。
- メンバーユニットの BGP テーブルは、制御ユニットテーブルと同期されません。ルーティングテーブルだけが、制御ユニットのルーティングテーブルと同期されます。
- 静的または動的な VTI インターフェイスを使用してルートベースのサイト間 VPN を構成する場合、ルーティングプロトコルとして BGP を使用している場合は、TTL ホップの値が 2 以上であることを確認してください。

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 （7 ページ）
ステップ 2 BGP 一般設定 （10 ページ）
ステップ 3 BGP ネイバーの設定 （12 ページ）
ステップ 4 BGP 集約アドレス設定の設定 （16 ページ）
ステップ 5 BGPv4 フィルタリング設定 （18 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 （18 ページ）
ステップ 7 BGP 再配布設定 （19 ページ）
ステップ 8 BGP ルート注入の設定 （20 ページ）

ステップ 9 BGP ルートのインポート/エクスポート設定の設定 （21 ページ）

BGP 基本設定

BGP の多くの基本設定が可能です。

仮想ルーティングを使用するデバイスの場合、このセクションで説明する基本設定は、[BGP] ページの [一般設定（General Settings）] で設定する必要があります。詳細については、Firewall Management Center Web インターフェイスの変更：[ルーティング（Routing）] ページを参照してください。

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）] を選択します。

ステップ 3 （仮想ルータ対応デバイスの場合）[一般設定（General Settings）] で [BGP] をクリックします。

ステップ 4 [BGP の有効化（Enable BGP）] チェックボックスをオンにして、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 [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）]（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）または [クラスタプール（Cluster Pool）]（個別インターフェイスモードのクラスタの場合に表示）を選択します。自動を選択すると、Firewall 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。[手動（Manual）] を選択した場合は、[IPアドレス（IP Address）] フィールドに IP アドレスを入力します。[クラスタプール（Cluster Pool）] を選択した場合は、[クラスタプール（Cluster Pool）] フィールドにクラスタプール値を入力します。クラスタプールアドレスの作成については、アドレス プールを参照してください。

ステップ 7 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。仮想ルータ対応デバイスの場合は、**[仮想ルータ（Virtual Routers）] > [BGP]** ページでルータ ID の設定をオーバーライドできます。

ステップ 8 （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）]（✎）をクリックして、グループの設定を編集します。

a) ネクストホップの検証用に BGP ルータの**スキャン間隔**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。

b) [AS_PATH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 9 （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 10 （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（Keep alive interval）] フィールドに、BGP ネイバーがキープアライブメッセージを送信しなくなった後アクティブな状態を継続する時間を入力します。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。0 ～ 65535 の値を指定します。

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。3 ～ 65535 の値を指定します。

（注）
ホールドタイムが 20 秒未満の場合、ピアフラッピングの可能性が高くなります。

d) [OK] をクリックします。

ステップ 11 [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追跡を有効にする [アドレス追跡を有効にする（Enable address tracking）] チェックボックスをオンにし、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間隔として [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。

ステップ 12 （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、Firewall 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、Firewall 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、Firewall 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 Firewall Threat Defenseから End Of Record（EOR）メッセージを受信した後、Firewall 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 13 [保存（Save）] をクリックします。

ステップ 14 BGP の基本設定を表示するには、[仮想ルータ（Virtual Routers）] ドロップダウンから目的のルータを選択し、[BGP] をクリックします。

このページには、[設定（Settings）]ページで設定された基本設定が表示されます。このページでルータ ID の設定を編集できます。

ステップ 15 ルータ ID の設定を編集するには、[IPアドレス（IP Address）] フィールドの IP アドレスを変更します。変更された値で、[BGP] ページの [一般設定（General Settings）] で設定されたルータ ID の設定がオーバーライドされます。

BGP 一般設定

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 [デバイス管理（Device Management）] ページで、[ルーティング（Routing）] をクリックします。

ステップ 2 （仮想ルータ対応デバイスの場合）[仮想ルータ（Virtual Routers）] ドロップダウンから、BGP を設定する仮想ルータを選択します。

ステップ 3 **[BGP]** > **[IPv4]** または [IPv6] を選択します。

ステップ 4 [General] をクリックします。

ステップ 5 [一般（General）] で、次のセクションを更新します。

a) [設定（Settings）] セクションの [ルートマップ（Route Map）] でルートマップオブジェクトを入力または選択し、[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) [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。

c) [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）]：デフォルトの情報発信元を設定するには、このオプションのチェックボックスをオンにします。
- （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）]：このオプションのチェックボックスをオンにして、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は、IPv4 設定にのみ適用されます。
- （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）]：このオプションのチェックボックスをオンにして、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（Synchronize between BGP and IGP system）]：このオプションのチェックボックスをオンにして、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）]：このオプションのチェックボックスをオンにして、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。

d) [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 ルートの最大数を入力します。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）ルートの最大数を入力します。値の範囲は 1 ～ 8 です。デフォルト値は 1 です。

ステップ 6 [保存（Save）] をクリックします。

BGP ネイバーの設定

BGP ルータは、更新を交換する前に各ピアと接続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。この手順を実行して、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 [デバイス管理（Device Management）] ページで、[ルーティング（Routing）] をクリックします。

ステップ 2 （仮想ルータ対応デバイスの場合）[仮想ルータ（Virtual Routers）] ドロップダウンリストから、BGP を設定する仮想ルータを選択します。

ステップ 3 **[BGP]** > **[IPv4]** または [IPv6] を選択します。

ステップ 4 [Neighbor] クリックします。

ステップ 5 [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 6 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。静的 VTI で BGP IPv6 を設定する場合は、ネイバーの仮想トンネル IP アドレスを入力します。

ステップ 7 BGP ネイバーのインターフェイスを選択します。

（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 8 [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 9 [有効アドレス（Enabled address）] チェックボックスをオンにして、この 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 10 （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 11 （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））]** チェックボックスを使用して、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、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。

- グレースフルリスタートは、デバイスがHAモードの場合、またはL2クラスタ（同じネットワークのすべてのノード）が設定されている場合にのみ有効になります。

ステップ 12 （オプション）BGP の BFD サポートの設定を有効にするには、[BFDフェールオーバー（BFD Failover）] ドロップダウンリストから BFD タイプ（single-hop、multi-hop、auto-detect-hop）を選択します。この選択により、BFD から転送パス検出失敗メッセージを受信するように BGP ネイバーが登録されます。BFD サポートが必要ない場合は、[なし（None）] を選択します。

ステップ 13 （オプション）BGP ネイバーの**説明**を入力します。

ステップ 14 （オプション）[ルートのフィルタリング（Filtering Routes）] 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) [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の制御（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）] チェックボックスをオンにします。[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）] チェックボックスをオンにします。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 15 （オプション）[ルート（Routes）] 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) [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）] チェックボックスをオンにして、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）]（+）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. [存在マップ（Exist Map）] をクリックし、[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、アドバタイズマップ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）] をクリックし、[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、アドバタイズマップ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 16 [タイマー（Timers）] で [BGP ピアのタイマーを設定する（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（Keep alive interval）]：Firewall Threat Defense 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、ピアがデッドであると Firewall Threat Defense が宣言するまでの間隔（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Firewall Threat Defenseが宣言するまでの最小間隔（秒）を入力します。有効な値は、3 ～ 65535 です。デフォルト値は 3 秒です。

（注）
ホールドタイムが 20 秒未満の場合、ピアフラッピングの可能性が高くなります。

ステップ 17 [詳細（Advanced）] で、次を更新します。

a) （オプション）[認証を有効にする（Enable Authentication）] チェックボックスをオンにして、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。[Confirm Password] 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 文字まで指定できます。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 Community 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）] 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）] を選択して、BGP ピアリングセッションを保護します。[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 Firewall Threat Defense が受け入れる [BGP バージョン（BGP version）] 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 18 AS 移行を考慮する場合にのみ [移行（Migration）] 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タのAS番号をカスタマイズ（Customize the AS number for routes received from the neighbor）] チェックボックスをオンにし、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 19 [OK] をクリックします。

ステップ 20 [保存（Save）] をクリックします。

BGP 集約アドレス設定の設定

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 Firewall Threat Defense デバイスを編集する場合は、[ルーティング（Routing）] をクリックします。

ステップ 2 （仮想ルータ対応デバイスの場合）[仮想ルータ（Virtual Routers）] ドロップダウンから、BGP を設定する仮想ルータを選択します。

ステップ 3 **[BGP]** > **[IPv4]** または [IPv6] を選択します。

ステップ 4 [集約アドレスの追加（Add Aggregate Address）] をクリックします。

ステップ 5 [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 6 （＋）[追加（Add）] をクリックして、[集約アドレスの追加（Add Aggregate Address）] ダイアログボックスを更新します。

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オンにします。

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オンにします。

g) [OK] をクリックします。

次のタスク

- BGPv4 設定については、BGPv4 フィルタリング設定 （18 ページ）に進みます。
- BGPv6 設定については、BGP ネットワーク設定 （18 ページ）に進みます。

BGPv4 フィルタリング設定

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 [デバイス管理（Device Management）] ページで、[ルーティング（Routing）] をクリックします。

ステップ 2 （仮想ルータ対応デバイスの場合）[仮想ルータ（Virtual Routers）] ドロップダウンから、BGP を設定する仮想ルータを選択します。

ステップ 3 **[BGP]** > **[IPv4]** を選択します。

ステップ 4 [Filtering] をクリックします。

（注）
[フィルタリング（Filtering）] フィールドは、IPv4 設定にのみ適用されます。

ステップ 5 （＋）[追加（Add）] をクリックして、[フィルタの追加（Add Filter）] ダイアログボックスを更新します。

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制御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 6 [保存（Save）] をクリックします。

BGP ネットワーク設定

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 [デバイス管理（Device Management）] ページで、[ルーティング（Routing）] をクリックします。

ステップ 2 （仮想ルータ対応デバイスの場合）[仮想ルータ（Virtual Routers）] ドロップダウンから、BGP を設定する仮想ルータを選択します。

ステップ 3 **[BGP]** > **[IPv4]** または [IPv6] を選択します。

ステップ 4 [Networks] をクリックします。

ステップ 5 [追加（Add）] をクリックして、[ネットワークの追加（Add Networks）] ダイアログボックスを更新します。

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選択します。

（注）
ネットワークプレフィックスをアドバタイズするには、デバイスへのルートがルーティングテーブルに存在する必要があります。

新しいネットワークオブジェクトを追加するには、ネットワーク オブジェクトの作成を参照してください。

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。新しいルートマップオブジェクトを追加するには、ルート マップを参照してください。

c) [OK] をクリックします。

ステップ 6 [保存（Save）] をクリックします。

BGP 再配布設定

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 [デバイス管理（Device Management）] ページで、[ルーティング（Routing）] をクリックします。

ステップ 2 （仮想ルータ対応デバイスの場合）[仮想ルータ（Virtual Routers）] ドロップダウンから、BGP を設定する仮想ルータを選択します。

ステップ 3 **[BGP]** > **[IPv4]** または [IPv6] を選択します。

ステップ 4 [Redistribution] をクリックします。

ステップ 5 [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。

（注）
ユーザ定義の仮想ルータは、RIP からのトラフィックの再配布をサポートしていません。

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。仮想ルーティングを使用しているデバイスの場合、このドロップダウンリストには、BGP 設定を設定する仮想ルータに割り当てられたプロセス ID が表示されます。

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。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。

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

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 [デバイス管理（Device Management）] ページで、[ルーティング（Routing）] をクリックします。

ステップ 2 （仮想ルータ対応デバイスの場合）[仮想ルータ（Virtual Routers）] ドロップダウンから、BGP を設定する仮想ルータを選択します。

ステップ 3 **[BGP]** > **[IPv4]** または [IPv6] を選択します。

ステップ 4 [Route Injection] をクリックします。

ステップ 5 [追加（Add）] をクリックして、[ルート注入の追加（Add Route Injection）] ダイアログボックスを更新します。

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。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。

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）]：このチェックボックスをオンにして、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 6 [保存（Save）] をクリックします。

BGP ルートのインポート/エクスポート設定の設定

BGP では、宛先仮想ルータと送信元仮想ルータの各ルートターゲット拡張コミュニティを使用してルートをインポートまたはエクスポートすることで、仮想ルータ間ルートリークを実装できます。ルーティングテーブル全体をリークする代わりに、ルートマップを使用して目的のルートターゲットをフィルタ処理できます。また、グローバル仮想ルータのルートをユーザ定義の仮想ルータにリークすることも、その逆も可能です。

- ルートターゲット拡張コミュニティを使用して、2 つのユーザ定義の仮想ルータ間でルートをリークするように BGP を設定できます。
  - ルートターゲットエクスポートを使用して、送信元仮想ルータからのルートターゲットでルートにタグを付けます。
  - ルートターゲットインポートを使用して、ルートターゲットに一致するルートを宛先仮想ルータにインポートします。
  - オプションで、エクスポートルートマップまたはインポートルートマップをそれぞれ使用して、送信元仮想ルータからのルート、または宛先仮想ルータへのルートをフィ

ルタ処理できます。ルートをフィルタリングするために、一致拡張コミュニティリストを使用してルートマップを設定できます。同様に、拡張コミュニティ ルート ターゲットを設定してルートマップを設定し、ルートターゲット拡張コミュニティにルートをタグ付けできます。

- グローバル仮想ルータからユーザ定義の仮想ルータにルートをインポートするには、[グローバル仮想ルータのインポートルートマップ（Global Virtual Router Import Route Map）] で IPv4/IPv6 ルートマップを指定して、ユーザ定義の仮想ルータにインポートします。
- ユーザ定義の仮想ルータからグローバル仮想ルータにルートをエクスポートするには、ルートターゲットのエクスポートに加えて、[グローバル仮想ルータのエクスポートルートマップ（Global Virtual Router Export Route Map）] を指定して、ユーザ定義の仮想ルータからエクスポートすることもできます。

BGP 仮想ルータ間ルートリークは、IPv4 と IPv6 の両方のプレフィックスをサポートします。

始める前に

- 仮想ルータを作成します。仮想ルータの作成
- 仮想ルータ上で BGP を有効にします。BGP 基本設定 （7 ページ）
- BGP の設定 （6 ページ）。

手順

ステップ 1 [デバイス管理（Device Management）] ページで、[ルーティング（Routing）] をクリックします。

ステップ 2 （仮想ルータ対応デバイスの場合）[仮想ルータ（Virtual Routers）] ドロップダウンから、BGP を設定する仮想ルータを選択します。

ステップ 3 **[BGP]** > **[IPv4]** または [IPv6] を選択します。

ステップ 4 （仮想ルータでのみサポート）[ルートのインポート/エクスポート（Route Import/Export）] をクリックします。

ステップ 5 [ルートターゲットのインポート（Route Targets Import）] フィールドに、インポートするルートに一致するルートターゲット拡張コミュニティを入力します。展開時に、この値に一致する宛先仮想ルータのルートが送信元仮想ルータの BGP テーブルにインポートされます。

（注）
- ルートターゲットは ASN:nn 形式である必要があります。
- 複数のルートターゲットをカンマ区切り値として入力できます。
- この値の範囲は 0:1 ー 65534:65535 です。

ステップ 6 [ルートターゲットのエクスポート（Route Targets Export）] フィールドに、ルートターゲット拡張コミュニティを入力して、送信元仮想ルータのルートにルートターゲット値をタグ付けします。展開時に、送信元仮想ルータのルートはこの値でタグ付けされます。

（注）
- ルートターゲットは ASN:nn 形式である必要があります。
- 複数のルートターゲットをカンマ区切り値として入力できます。
- この値の範囲は 0:1 ー 65534:65535 です。

ステップ 7 ルートマップを使用すると、ルーティングテーブル全体をリークすることなく、共有するルートを絞り込めます。ルートマップフィルタリングは、指定されたルートターゲット値で取得されたルートのリストに適用されます。

a) （オプション）[ユーザ仮想ルータ（User Virtual Router）] で、[インポートルートマップ（Import Route Map）] ドロップダウンリストからルートマップを選択し、宛先仮想ルータでルートをフィルタ処理します。

（注）
ユーザ仮想ルータのインポートルートマップは、ルートターゲットのインポートが設定されている場合にのみ有効です。

b) （オプション）[ユーザー仮想ルータ（User Virtual Router）] で、[エクスポートルートマップ（Export Route Map）] ドロップダウンリストからルートマップを選択し、ルートが他の仮想ルータにエクスポートされる前に、送信元仮想ルータでルートをフィルタ処理します。

（注）
ルートマップの match 句と set 句をルートターゲット拡張コミュニティリストとともに使用して、他の基準に基づいてフィルタリングしたり、ルート ターゲット コミュニティ値でルートにタグ付けしたりできます。詳細については、ルート マップを参照してください。

ステップ 8 ユーザ定義の仮想ルータとグローバル仮想ルータの間でルートを共有するには、[グローバル仮想ルータ（Global Virtual Router）] でルートマップを指定します。

a) グローバル仮想ルータルートをユーザ定義の仮想ルータにリークするには、[インポートルートマップ（Import Route Map）] ドロップダウンリストからルートマップを選択します。IPv4 または IPv6 ルートマップがユーザ定義の仮想ルータにインポートされます。

b) ユーザ定義の仮想ルータルートをグローバル仮想ルータにリークするには、[エクスポートルートマップ（Export Route Map）] ドロップダウンリストからルートマップを選択します。IPv4 または IPv6 ルートマップがグローバル仮想ルータにエクスポートされます。

（注）
ルートマップの指定とは別に、エクスポートのルートターゲットを指定する必要があります。

（注）

ルートマップオブジェクトの match 句を使用して、リークのルートをフィルタ処理できます。詳細については、ルート マップを参照してください。

ステップ 9 手順（ステップ 3 ー 8）に従って、他の仮想ルータの関連する BGP ルートインポートおよびエクスポート設定も設定します。ステップ 3 （22 ページ） ステップ 8 （23 ページ）

ステップ 10 [保存して展開（Save and Deploy）] をクリックします。

パケットが入力仮想ルータに流れると、BGP は一致するルートターゲット値を持つ宛先仮想ルータからルートをインポートします。ルートマップも設定されている場合、ルートはさらにフィルタ処理され、パケットをルーティングするベストパスルートを特定するために使用されます。

BGP の履歴

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
仮想ルータを相互接続するための BGP 設定	7.1	任意（Any）	ユーザー定義の仮想ルータ間、およびグローバル仮想ルータとユーザー定義の仮想ルータ間でルートを動的にリークするように BGP 設定を構成できます。ルートのインポートおよびエクスポート機能が導入され、仮想ルータにルートターゲットのタグを付け、必要に応じて、一致したルートをルートマップでフィルタリングすることにより、仮想ルータ間でルートを交換します。この BGP 機能は、ユーザー定義の仮想ルータを選択した場合にのみ利用できます。 新規/変更された画面：選択したユーザー定義の仮想ルータについて、**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[ルーティング（Routing）]** > **[BGPv4/v6]** > **[ルートのインポート/エクスポート（Route Import/Export）]** タブ。
ユーザー定義の仮想ルータでの BGPv6 サポート	7.1	任意（Any）	Secure Firewall Threat Defense は、ユーザー定義の仮想ルータでの BGPv6 の設定をサポートするようになりました。 新規/変更された画面：選択したユーザー定義の仮想ルータについて、**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[ルーティング（Routing）]** > **[BGPv6]** ページ。

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。