

BGP

この章では、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 ASA を設定する方法について説明します。

- BGP （1 ページ）
- BGP のガイドライン （6 ページ）
- BGP の設定 （7 ページ）
- BGP のモニタリング （30 ページ）
- BGP の履歴 （31 ページ）

BGP

ボーダー ゲートウェイ プロトコル（BGP）は、次のような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（共通のルーティングポリシーを使用する共通の管理下にあるネットワークまたはネットワークグループ）の内部および相互間で動作します。
- インターネットのルーティング情報を交換します。
- 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として機能します。

BGP 使用シナリオ

BGP 使用シナリオは、次のようなネットワーク設定です。

- ISP が外部 BGP（EBGP）を使用して自律システム間でお客様と ISP のルートを交換できるようにします。
- サービスプロバイダーが内部 BGP（IBGP）を使用して自律システム内でルートを交換できるようにします。
- IPv6 ネットワークを介した IPv6 プレフィックスルーティングをサポートします。

BGP 導入コンテキスト

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使用することもできます。



（注） BGPv6 デバイスは、クラスタに参加すると、ロギング レベル 7 が有効の場合ソフト トレースバックを生成します。

ルーティングテーブルの変更

ルーティングテーブルの変更は、次のようなネットワークの更新です。

- BGP ネイバーが最初の TCP 接続確立時に完全なルーティング情報を交換するときに発生します。
- ルーティングテーブルの変更が検出されたときに、変更されたルートのみをネイバーに送信する必要があります。
- 定期的な更新なしで、接続先ネットワークへの最適なパスのみをアドバタイズします。

ルート選択のための BGP 属性

BGPにより学習されたルートには、宛先に対して複数のパスが存在する場合に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。

- [重み（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。[重み（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。
- [ローカルプリファレンス（Local preference）]：この属性により、ローカル AS からの出力点が選択されます。重み属性とは異なり、ローカル AS 全体で共有されます。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用に選択されます。
- [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。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。
- [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。

（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が遅延しないようにします。

BGP パス選択

BGP パス選択は、BGP が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した場合に、ベストパスとして 1 つのパスのみを選択し、選択したパスを IP ルーティングテーブルに配置して、優先順位に従って特定の基準を使用してパスをネイバーに伝達するルーティングプロセスです。

BGP パス選択基準

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。

1. 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。そうでない場合、重みが最大のパスが優先されます。
2. 重みが同じである場合、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。
3. 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。
4. 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。
5. 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。次に、BGP マルチパス （4 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。
6. BGP マルチパス （4 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。
7. 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。
8. 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。
9. 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 マルチパスは、次の特長を持つ BGP 機能です。

- 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。
- 宛先プレフィックスへの通信は、組み込まれたすべてのパス間で共有できます。
- ベストパス選択アルゴリズムには影響しません。

BGP マルチパス要件

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。

- 重み
- 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

コンテキストモードのガイドライン

BGP を導入する場合は、次のコンテキストモードの要件を考慮してください。

- シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。
- すべてのコンテキストでサポートされる自律システム（AS）番号は 1 つだけです。

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。

その他のガイドライン

その他の次の運用要件および制限事項を考慮してください。

- 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。
- 高可用性モードで設定された Firewall Threat Defense デバイスで BGP を使用する場合、グレースフルタイムアウト機能を有効にします。この機能を有効にすると、BGP コンバージェンスに関連する問題が原因で発生するパケットドロップが削減されます。

BGP の設定

ここでは、システムで BGP プロセスをイネーブルにして設定する方法について説明します。

手順

ステップ 1 BGP の有効化 （7 ページ）。
ステップ 2 BGP ルーティング プロセスの最適なパスの定義 （9 ページ）。
ステップ 3 ポリシー リストの設定 （9 ページ）。
ステップ 4 AS パス フィルタの設定 （11 ページ）。
ステップ 5 コミュニティ ルールの設定 （12 ページ）。
ステップ 6 IPv4 アドレス ファミリの設定 （13 ページ）。
ステップ 7 IPv6 アドレス ファミリの設定 （22 ページ）。

BGP の有効化

ここでは、BGP の有効化、BGP ルーティング プロセスの確立、一般的な BGP パラメータの設定に必要な手順について説明します。

手順

ステップ 1 シングル モードの場合、ASDM で **[Configuration]** > **[Device Setup]** > **[Routing]** > **[BGP]** > **[General]** の順に選択します。

（注） マルチ モードの場合、ASDM で [Configuration] > [Context Management] > [BGP] の順に選択します。BGP をイネーブルにした後に、セキュリティ コンテキストに切り替え、[Configuration] > [Device Setup] > [Routing] > [BGP] > [General] の順に選択して BGP をイネーブルにします。

ステップ 2 [Enable BGP Routing] チェックボックスをオンにします。
ステップ 3 [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 ～ XX.YY を指定できます。
ステップ 4 （オプション）[Limit the number of AS numbers in the AS_PATH attribute of received routes] チェックボックスをオンにして、AS_PATH 属性の AS 番号の数を特定数に制限します。有効値は 1 ～ 254 です。

ステップ 5 （オプション）[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。

ステップ 6 （オプション）[Use TCP path MTU discovery] チェックボックスをオンにし、パス MTU ディスカバリ手法を使用して 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。

ステップ 7 （オプション）[Enable fast external 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。

ステップ 8 （オプション）[Enforce that first AS is peer's AS for EBGP routes] チェックボックスをオンにすると、AS_PATH 属性の最初のセグメントとしてその AS 番号をリストしていない外部 BGP ピアから受信される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。

ステップ 9 （オプション）[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。

ステップ 10 [Neighbor timers] 領域でタイマー情報を指定します。

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

c) （オプション）[Min. Hold Time] フィールドに、BGP 接続の開始中/設定中に BGP ネイバーがアクティブな状態を維持する最小時間を入力します。0 ～ 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。

ステップ 11 （オプション）[Non Stop Forwarding] セクションで、次の手順を実行します。

a) [Enable Graceful Restart] チェックボックスをオンにして、ASA 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) [Restart Time] フィールドに、BGP オープン メッセージを受信するまで ASA が古いルートを削除するのを待機する時間を入力します。デフォルト値は 120 秒です。有効な値は 1 ～ 3600 秒です。

c) [Stale Path Time] フィールドに、リスタートする ASA から End Of Record（EOR）メッセージを受信した後、古いルートを削除するまで ASA が待機する時間を入力します。デフォルト値は 360 秒です。有効な値は 1 ～ 3600 秒です。

ステップ 12 [OK] をクリックします。

ステップ 13 [Apply] をクリックします。

BGP ルーティング プロセスの最適なパスの定義

ここでは、BGP の最適なパスを設定するために必要な手順について説明します。最適なパスの詳細については、BGP パス選択 （4 ページ）を参照してください。

手順

ステップ 1 ASDM で、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[BGP]** > **[Best Path]** の順に選択します。

[Best Path configuration] ペインが表示されます。

ステップ 2 [Default Local Preference] フィールドに、0 ～ 4294967295 の値を指定します。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 サーバーに送信されます。

ステップ 3 [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。

ステップ 4 [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。

ステップ 5 [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 比較をイネーブルにし、新しいネットワーク エントリを追加します。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。

ステップ 6 [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。

ステップ 7 [OK] をクリックします。

ステップ 8 [Apply] をクリックします。

ポリシー リストの設定

ルート マップ内でポリシー リストが参照されると、ポリシー リスト内の match 文すべてが評価され、処理されます。1 つのルート マップに 2 つ以上のポリシー リストを設定できます。ポリシー リストは、同じルート マップ内にあるがポリシー リストの外で設定されている他の既存の match および set 文とも共存できます。ここでは、ポリシー リストを設定するために必要な手順について説明します。

手順

ステップ 1 ASDM で、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[BGP]** > **[Policy Lists]** の順に選択します。

ステップ 2 [Add] をクリックします。

[Add Policy List] ダイアログボックスが表示されます。このダイアログボックスでは、ポリシー リスト名、その再配布アクセス（許可または拒否）、一致インターフェイス、一致 IP アドレス、一致 AS パス、一致コミュニティ名リスト、一致メトリック、一致タグ番号を追加することができます。

ステップ 3 [Policy List Name] フィールドに、ポリシー リストの名前を入力します。

ステップ 4 [Permit] または [Deny] オプション ボタンをクリックして再配布アクセスを指定します。

ステップ 5 [Match Interfaces] チェックボックスをオンにして、指定のインターフェイスの 1 つのネクスト ホップを持つルートを配布し、次のいずれかを実行します。

- [Interface] フィールドに、インターフェイス名を入力します。
- [Interface] フィールドで、省略記号をクリックすると、手動でインターフェイスを参照し、指定できます。1 つ以上のインターフェイスを選択し、[Interface] をクリックして [OK] をクリックします。

ステップ 6 [Specify IP] 領域で、次のように設定します。

a) [Match Address] チェックボックスをオンにして、標準アクセス リストまたはプレフィックス リストで許可された宛先ネットワーク番号アドレスを持つルートを再配布し、パケットにポリシー ルーティングを実行します。

アクセス リストまたはプレフィックス リストを指定するか、省略記号をクリックして手動でアクセス リストを参照し、指定します。1 つ以上のアクセス リストを選択し、[Access List] をクリックして [OK] をクリックします。

b) [Match Next Hop] チェックボックスをオンにして、指定したアクセス リストまたはプレフィックス リストの 1 つから渡されたネクスト ホップ ルータ アドレスを持つルートを再配布します。

アクセス リストまたはプレフィックス リストを指定するか、省略記号をクリックして手動でアクセス リストを参照し、指定します。1 つ以上のアクセス リストを選択し、[Access List] をクリックして [OK] をクリックします。

c) [Match Route Source] チェックボックスをオンにして、アクセス リストまたはプレフィックス リストで指定されたアドレスのルータおよびアクセス サーバーによってアドバタイズされたルートを再配布します。

アクセス リストまたはプレフィックス リストを指定するか、省略記号をクリックして手動でアクセス リストを参照し、指定します。1 つ以上のアクセス リストを選択し、[Access List] をクリックして [OK] をクリックします。

ステップ 7 [Match AS Path] チェックボックスをオンにして、BGP 自律システム パスを一致させます。

AS パス フィルタを指定するか、省略記号をクリックして手動で AS パス フィルタを参照し、指定します。1 つ以上の AS パス フィルタを選択し、[AS Path Filter] をクリックして [OK] をクリックします。

ステップ 8 [Match Community Names List] チェックボックスをオンにして、BGP コミュニティを一致させます。

a) コミュニティ ルールを指定するか、省略記号をクリックしてコミュニティ ルールを手動で参照し、指定します。1 つ以上のコミュニティ ルールを選択し、[Community Rules] をクリックして [OK] をクリックします。

b) [Match the specified community exactly] チェックボックスをオンにして、特定の BGP コミュニティを一致させます。

ステップ 9 [Match Metrices] チェックボックスをオンにして、指定したメトリックを持つルートを再配布します。複数のメトリックを指定する場合、ルートはいずれかのメトリックと一致します。

ステップ 10 [Match Tag Numbers] チェックボックスをオンにして、指定したタグと一致するルーティング テーブル内のルートを再配布します。複数のタグ番号を指定した場合、ルートはいずれかのメトリックと一致します。

ステップ 11 [OK] をクリックします。

ステップ 12 [Apply] をクリックします。

AS パス フィルタの設定

AS パス フィルタで、アクセス リストを使用してルーティング アップデート メッセージをフィルタリングし、アップデート メッセージ内の個々のプレフィックスを確認できます。アップデート メッセージ内のプレフィックスがフィルタ基準に一致すると、フィルタ エントリで実行するように設定されているアクションに応じて、個々のプレフィックスは除外されるか受け入れられます。ここでは、AS パス フィルタを設定するために必要な手順について説明します。

（注） AS パス アクセス リストは、通常のファイアウォール ACL とは異なります。

手順

ステップ 1 ASDM で、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[BGP]** > **[AS Path Filters]** の順に選択します。

ステップ 2 [Add] をクリックします。

[Add Filter] ダイアログボックスが表示されます。このダイアログボックスで、フィルタの名前、その再配布アクセス（許可または拒否）、および正規表現を追加できます。

ステップ 3 [Name] フィールドに、AS パス フィルタの名前を入力します。

ステップ 4 [Permit] または [Deny] オプション ボタンをクリックして再配布アクセスを指定します。

ステップ 5 正規表現を指定します。正規表現を作成するには、[Build] をクリックします。

ステップ 6 [Test] をクリックして、正規表現が選択した文字列と一致するかどうかテストします。

ステップ 7 [OK] をクリックします。

ステップ 8 [Apply] をクリックします。

コミュニティ ルールの設定

コミュニティは、共通するいくつかの属性を共有する宛先のグループです。コミュニティ リストを使用すると、ルート マップの match 句で使用されるコミュニティ グループを作成できます。アクセス リストと同様に、一連のコミュニティ リストを作成できます。ステートメントは一致が見つかるまでチェックされ、1 つのステートメントが満たされると、テストは終了します。ここでは、コミュニティ ルールを設定するために必要な手順について説明します。

手順

ステップ 1 ASDM で、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[BGP]** > **[Community Rules]** > の順に選択します。

ステップ 2 [Add] をクリックします。

[Add Community Rule] ダイアログボックスが表示されます。このダイアログボックスで、ルール名、ルール タイプ、その再配布アクセス（許可または拒否）、および特定のコミュニティを追加できます。

ステップ 3 [Rule Name] フィールドに、コミュニティ ルールの名前を入力します。

ステップ 4 [Standard] または [Expanded] オプション ボタンをクリックして、コミュニティ ルール タイプを指定します。

ステップ 5 [Permit] または [Deny] オプション ボタンをクリックして再配布アクセスを指定します。

ステップ 6 標準コミュニティ ルールを追加するには、次の手順を実行します。

a) [Communities] フィールドで、コミュニティ番号を指定します。有効値は 1 ～ 4294967200 です。

b) （オプション）[Internet]（既知のコミュニティ）チェックボックスをオンにして、インターネットコミュニティを指定します。このコミュニティのルートは、すべてのピア（内部および外部）にアドバタイズされます。

c) （オプション）[Do not advertise to any peers]（既知のコミュニティ）チェックボックスをオンにして、no-advertise コミュニティを指定します。このコミュニティのあるルートはピア（内部または外部）にはアドバタイズされません。

d) （オプション）[Do not export to next AS]（既知のコミュニティ）チェック ボックスをオンにして、no-export コミュニティを指定します。このコミュニティのあるルートは、同じ自

律システム内のピアへのみ、または連合内の他のサブ自律システムへのみアドバタイズされます。これらのルートは外部ピアにはアドバタイズされません。

ステップ 7 拡張コミュニティ ルールを追加するには、次の手順を実行します。

a) [Regular Expression] フィールドに、正規表現を入力します。または、[Build] をクリックして正規表現を作成します。

b) [Test] をクリックして、作成した正規表現が選択した文字列と一致するかどうか調べます。

ステップ 8 [OK] をクリックします。

ステップ 9 [Apply] をクリックします。

IPv4 アドレス ファミリの設定

BGP の IPv4 設定は、BGP 設定セットアップ内の IPv4 ファミリ オプションから指定できます。IPv4 ファミリ セクションには、一般設定、集約アドレスの設定、フィルタリング設定、ネイバー 設定のサブセクションが含まれます。これらの各サブセクションを使用して、IPv4 ファミリに固有のパラメータをカスタマイズすることができます。

IPv4 ファミリの一般設定

ここでは、一般的な IPv4 の設定に必要な手順を説明します。

手順

ステップ 1 ASDM で、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[BGP]** > **[IPv4 Family]** の順に選択します。

ステップ 2 [General] をクリックします。

[General IPv4 family BGP parameters] 設定ペインが表示されます。

ステップ 3 [Administrative Distances] 領域で、[External]、[Internal] および [Local] のディスタンスを指定します。

ステップ 4 [Learned Routes Map] ドロップダウン リストからルート マップ名を選択します。[Manage] をクリックして、ルート マップを追加および設定します。

ステップ 5 （オプション）[Generate Default Route] チェックボックスをオンにして、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。

ステップ 6 （オプション）[Summarize subnet routes into network-level routes] 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。

ステップ 7 （オプション）[Advertise inactive routes] 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。

ステップ 8 （オプション）[Redistribute iBGP into an IGP] チェックボックスをオンにして、IS-IS や OSPF などの Interior Gateway Protocol（IGP）への iBGP の再配布を設定します。

ステップ 9 （オプション）[Scanning Interval] フィールドに、ネクスト ホップの検証用に BGP ルータのスキャン間隔（秒）を入力します。有効な値は 5 ～ 60 秒です。

ステップ 10 （オプション）[Enable address tracking] チェックボックスをオンにして、BGP ネクスト ホップ アドレス トラッキングを有効化します。[Delay Interval] フィールドで、ルーティング テーブルにインストールされている更新済みのネクストホップ ルートのチェック間の遅延間隔を指定します。

ステップ 11 （オプション）ルーティング テーブルにインストールできる並列の内部ボーダー ゲートウェイ プロトコル（iBGP）ルートの最大数を [Number of paths] フィールドで指定し、[iBGP multipaths] チェックボックスをオンにします。

ステップ 12 [Apply] をクリックします。

IPv4 ファミリ集約アドレスの設定

ここでは、特定のルートの 1 つのルートへの集約を定義するために必要な手順について説明します。

手順

ステップ 1 ASDM で、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[BGP]** > **[IPv4 Family]** の順に選択します。

ステップ 2 [Aggregate Address] をクリックします。

[Aggregate Address parameters] 設定ペインが表示されます。

ステップ 3 [Add] をクリックします。

[Add Aggregate Address] ペインが表示されます。

ステップ 4 [Network] フィールドでネットワーク オブジェクトを指定します。

ステップ 5 [Generate autonomous system set path information] チェックボックスをオンにして、自律システムの設定パス情報を生成します。

ステップ 6 [Filters all more- specific routes from the updates] チェックボックスをオンにして、アップデートから固有性の強いルートをすべてフィルタリングします。

ステップ 7 [Attribute 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。[Manage] をクリックして、ルート マップを追加または設定します。

ステップ 8 [Advertise 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。[Manage] をクリックして、ルートを追加または設定します。

ステップ 9 [Suppress 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。[Manage] をクリックして、ルートを追加または設定します。

ステップ 10 [OK] をクリックします。

ステップ 11 [Aggregate Timer] フィールドで、集約タイマーの値（秒）を指定します。有効な値は、0 または 6 ～ 60 の値です。

ステップ 12 [Apply] をクリックします。

IPv4 ファミリのフィルタリング設定

ここでは、着信 BGP アップデートで受信したルートまたはネットワークをフィルタリングするために必要な手順について説明します。

手順

ステップ 1 **[Configuration]** > **[Device Setup]** > **[Routing]** > **[BGP]** > **[IPv4 Family]** を選択します。

ステップ 2 [Filtering] をクリックします。

[Define filters for BGP updates] ペインが表示されます。

ステップ 3 [Add] をクリックします。

[Add Filter] ペインが表示されます。

ステップ 4 [Direction] ドロップダウン リストから方向を選択します。方向は、フィルタを着信アップデートに適用するか、または発信アップデートに適用するかを指定します。

ステップ 5 [Access List] ドロップダウン リストから標準アクセス リストを選択します。[Manage] をクリックして、新しい ACL を追加します。

ステップ 6 発信フィルタには、オプションで、配信されるルートのタイプを指定できます。

a) [Protocol] ドロップダウン リストからオプションを選択します。

[BGP]、[EIGRP]、[OSPF]、または [RIP] などのルーティング プロトコルを選択できます。

接続ルートから学習されたピアおよびネットワークをフィルタリングするには、[Connected] を選択します。

スタティック ルートから学習されたピアおよびネットワークをフィルタリングするには、[Static] を選択します。

b) [BGP]、[EIGRP]、または [OSPF] を選択した場合は、そのプロトコルのプロセス ID も [Process ID] で選択します。

ステップ 7 [OK] をクリックします。

ステップ 8 [Apply] をクリックします。

IPv4 ファミリの BGP ネイバーの設定

ここでは、BGP ネイバーおよびネイバー設定を定義するために必要な手順について説明します。

手順

ステップ 1 ASDM で、**[Configuration]** > **[Device Setup]** >**[Routing]** **[BGP]** > **[IPv4 Family]** の順に選択します。

ステップ 2 [Neighbor] クリックします。

ステップ 3 [Add] をクリックします。

ステップ 4 左側のペインで、[General] をクリックします。

ステップ 5 [IP Address] フィールドに 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 6 [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 7 （オプション）[Description] フィールドに BGP ネイバーの説明を入力します。

ステップ 8 （オプション）[Shutdown neighbor 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 9 （オプション）[アドレスファミリを有効化（Enable address family）] 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。

ステップ 10 （オプション）[Global Restart Functionality for this peer] チェックボックスをオンにして、ASA ネイバーまたはピア グループの Border Gateway Protocol（BGP）グレースフル リスタート機能をイネーブルまたはディセーブルにします。

（注） このオプションは、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有効になります。

ステップ 11 （オプション）BGP ネイバーシップの送信元としてインターフェイスを更新するには、[送信元の更新（Update-Source）] ドロップダウンボックスからインターフェイスを選択します。

（注） BGP ネイバーシップの送信元としてループバック インターフェイスを更新すると、ループバック インターフェイスの IP アドレスがネットワーク全体にアドバタイズされます。ループバック インターフェイスは eBGP ピアとして機能し、ルーティングに参加します。ループバック インターフェイスは有効にすると安定し、管理上のシャットダウンまで使用可能な状態になるため、ループバック インターフェイスの IP アドレスで常に ASA に到達できます。

ステップ 12 左側のペインで、[Filtering] をクリックします。

ステップ 13 （オプション）[Filter routes using an access list] 領域で、適切な着信または発信アクセス コントロール リストを選択して BGP ネイバー情報を配布します。必要に応じて、[Manage] をクリックして、ACL と ACE を追加します。

ステップ 14 （オプション）[Filter routes using a route map] 領域で、適切な着信または発信ルート マップを選択して、着信ルートまたは発信ルートにルート マップを適用します。[Manage] をクリックして、ルート マップを設定します。

ステップ 15 （オプション）[Filter routes using a prefix list] 領域で、適切な着信または発信プレフィックス リストを選択して BGP ネイバー情報を配布します。[Manage] をクリックして、プレフィックス リストを設定します。

ステップ 16 （オプション）[Filter routes using AS path filter] 領域で、適切な着信または発信 AS パス フィルタを選択して BGP ネイバー情報を配布します。[Manage] をクリックして、AS パス フィルタを設定します。

ステップ 17 （オプション）[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。

- [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。
- [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。
- （オプション）[Control prefixes received from a 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、[Terminate peering when prefix limit is exceeded] をクリックします。[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、[Give only warning message when prefix limit is exceeded] をクリックします。この場合、BGP ネイバーは終了しません。

ステップ 18 左側のペインで、[Routes] をクリックします。

ステップ 19 [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。

ステップ 20 （オプション）[Generate Default route] 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。

- [Route map] ドロップダウン リストから、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 マップを選択します。[Manage] をクリックして、ルート マップを追加および設定します。

ステップ 21 （オプション）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、次の手順を実行します。

a) [Conditionally Advertised Routes] セクションで [Add] をクリックします。

b) exist-map または non-exist-map の条件に一致した場合にアドバタイズされるルート マップを [Advertise Map] ドロップダウン リストから選択します。

c) 次のいずれかを実行します。

- [Exist Map] をクリックしてルート 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。
- [Non-exist Map] をクリックしてルート 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。

d) [OK] をクリックします。

ステップ 22 （オプション）[Remove private autonomous system (AS) numbers from outbound routing updates] チェックボックスをオンにし、プライベート AS 番号を発信ルートにおけるアドバイタイズ対象から除外します。

ステップ 23 左側のペインで、[Timers] をクリックします。

ステップ 24 （オプション）[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、保持時間、最小保持時間を設定します。

- [Keepalive frequency] フィールドに、ASA 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。
- [Hold time] フィールドに、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 ASA が宣言するまでの時間（秒）を入力します。デフォルト値は 180 秒です。
- （オプション）[Min Hold time] フィールドに、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 ASA が宣言するまでの最小時間（秒）を入力します。

（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。

ステップ 25 左側のペインで、[Advanced] をクリックします。

ステップ 26 （オプション）[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。

- [Encryption Type] ドロップダウン リストから暗号化タイプを選択します。
- パスワードを [Password] フィールドに入力します。[パスワードの確認（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 文字を指定できます。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。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。

ステップ 27 （オプション）[Send Community Attribute to this neighbor**]** チェックボックスをオンにします。

ステップ 28 （オプション）[ネイバーのネクストホップとしてASAを使用（Use ASA as next hop for 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。

ステップ 29 次のいずれかを実行します。

- [Allow connections with neighbor that is not directly connected] をクリックして、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 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。
  - （オプション）[接続確認を無効化（Disable connection verification）] チェックボックスをオンにし、ループバック インターフェイスを使用するシングルホップピアとの eBGP ピアリングセッションを確立するための接続確認を無効にします。
- [Limit number of TTL hops to neighbor] をクリックして、BGP ピアリング セッションを保護できるようにします。
  - [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。

ステップ 30 （オプション）[Weight] フィールドに BGP ネイバー接続の重みを入力します。

ステップ 31 [BGP version] ドロップダウン リストから、ASA が受け入れる BGP バージョンを選択します。

（注） バージョンを 2 に設定すると、指定されたネイバーとの間でバージョン 2 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 32 （オプション）[TCP Path MTU 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 セッションをイネーブルにします。

ステップ 33 [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。

ステップ 34 左側のペインで、[Migration] をクリックします。

ステップ 35 （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。

- [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 ～ 65535 です。

- （オプション）[Do not prepend local AS number for routes received from neighbor] チェックボックスをオンにします。ローカル AS 番号は、eBGP ピアから受信したルートの前に追加されません。
- （オプション）[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ます。ローカル ルーティング プロセスの AS 番号は前に追加されません。
- （オプション）[Accept either real AS number or local AS number in routes received from neighbor] チェックボックスをオンにします。

ステップ 36 [OK] をクリックします。

ステップ 37 [Apply] をクリックします。

IPv4 ネットワークの設定

ここでは、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を定義するために必要な手順について説明します。

手順

ステップ 1 ASDM で、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[BGP]** > **[IPv4 Family]** の順に選択します。

ステップ 2 [Networks] をクリックします。

[Define networks to be advertised by the BGP routing process] 設定ペインが表示されます。

ステップ 3 [Add] をクリックします。

[Add Network] ペインが表示されます。

ステップ 4 [Address] フィールドで BGP がアドバタイズするネットワークを指定します。

（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。

ステップ 5 （オプション）[Netmask] ドロップダウン リストからネットワーク マスクまたはサブネットワーク マスクを選択します。

ステップ 6 [Route Map] ドロップダウン リストから、アドバタイズされるネットワークをフィルタリングするために調べる必要のあるルート マップを選択します。[Manage] をクリックして、ルートマップを設定または追加します。

ステップ 7 [OK] をクリックします。

ステップ 8 [Apply] をクリックします。

IPv4 再配布の設定

ここでは、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するために必要な手順について説明します。

手順

ステップ 1 ASDM で、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[BGP]** > **[IPv4 Family]** > の順に選択します。

ステップ 2 [Redistribution] をクリックします。

[Redistribution] ペインが表示されます。

ステップ 3 [Add] をクリックします。

[Add Redistribution] ペインが表示されます。

ステップ 4 [Source Protocol] 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。

ステップ 5 [Process ID] ドロップダウン リストからソース プロトコルのプロセス ID を選択します。

ステップ 6 （オプション）[Metric] フィールドに、再配布されるルートのメトリックを入力します。

ステップ 7 [Route Map] ドロップダウン リストから、再配布されるネットワークをフィルタリングするために調べる必要のあるルート マップを選択します。[Manage] をクリックして、ルート マップを設定または追加します。

ステップ 8 [Internal]、[External]、および [NSSA External Match] チェックボックスのうち 1 つ以上をオンにして、OSPF ネットワークからルートを再配布します。

この手順は、OSPF ネットワークからの再配布にのみ適用できます。

ステップ 9 [OK] をクリックします。

ステップ 10 [Apply] をクリックします。

IPv4 ルート注入の設定

ここでは、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するために必要な手順について説明します。

手順

ステップ 1 ASDM で、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[BGP]** > **[IPv4 Family]** > の順に選択します。

ステップ 2 [Route Injection] をクリックします。

[Route Injection] ペインが表示されます。

ステップ 3 [Add] をクリックします。

[Add Conditionally injected route] ペインが表示されます。

ステップ 4 [Inject Map] ドロップダウン リストから、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 マップを選択します。

ステップ 5 [Exist Map] ドロップダウン リストから、BGP スピーカーが追跡するプレフィックスを含むルート マップを選択します。

ステップ 6 [Injected routes will inherit the attributes of the aggregate route] チェックボックスをオンにし、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。

ステップ 7 [OK] をクリックします。

ステップ 8 [Apply] をクリックします。

IPv6 アドレス ファミリの設定

BGP の IPv6 設定は、BGP 設定セットアップ内の IPv6 ファミリ オプションから指定できます。IPv6 ファミリ セクションには、一般設定、集約アドレスの設定、ネイバー設定のサブセクションが含まれます。これらの各サブセクションを使用して、IPv6 ファミリに固有のパラメータをカスタマイズすることができます。

ここでは、BGP IPv6 ファミリの設定をカスタマイズする方法について説明します。

IPv6 ファミリの一般設定

ここでは、一般的な IPv6 の設定に必要な手順を説明します。

手順

ステップ 1 ASDM で、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[BGP]** > **[IPv6 Family]** の順に選択します。

ステップ 2 [General] をクリックします。

[General IPv6 family BGP parameters] 設定ペインが表示されます。

ステップ 3 [Administrative Route Distances] 領域で、外部、内部およびローカル ディスタンスを指定します。

ステップ 4 （オプション）[Generate Default Route] チェックボックスをオンにして、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。

ステップ 5 （オプション）[Advertise inactive routes] 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。

ステップ 6 （オプション）[Redistribute iBGP into an IGP] チェックボックスをオンにして、IS-IS や OSPF などの Interior Gateway Protocol（IGP）への iBGP の再配布を設定します。

ステップ 7 （オプション）[Scanning Interval] フィールドに、ネクスト ホップの検証用に BGP ルータのスキャン間隔（秒）を入力します。有効な値は 5 ～ 60 秒です。

ステップ 8 （オプション）[Number of paths**]** フィールドに、Border Gateway Protocol ルートの最大数を指定します。

ステップ 9 （オプション）[IBGP multipaths] チェックボックスをオンにし、[Number of paths] フィールドに、ルーティング テーブルにインストールできる並列の内部ボーダー 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。

ステップ 10 [Apply] をクリックします。

IPv6 ファミリ集約アドレスの設定

ここでは、特定のルートの 1 つのルートへの集約を定義するために必要な手順について説明します。

手順

ステップ 1 ASDM で、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[BGP]** > **[IPv6 Family]** の順に選択します。

ステップ 2 [Aggregate Address] をクリックします。

[Aggregate Address parameters] 設定ペインが表示されます。

ステップ 3 [Add] をクリックします。

[Add Aggregate Address] ペインが表示されます。

ステップ 4 [IPv6/Address Mask] フィールドで IPv6 アドレスを指定します。または、ネットワーク オブジェクトを参照して追加します。

ステップ 5 [Generate autonomous system set path information] チェックボックスをオンにして、自律システムの設定パス情報を生成します。このルートにアドバタイズされるパスは、集約中のすべてのパス内に含まれるすべての要素で構成される AS_SET になります。

（注） このルートは集約されたルート変更に関する自律システムパス到着可能性情報として継続的に削除してアップデートする必要があるため、多くのパスを集約する際に aggregate-address コマンドのこの形式を使用しないでください。

ステップ 6 [Filters all more- specific routes from the updates] チェックボックスをオンにして、アップデートから固有性の強いルートをすべてフィルタリングします。これにより、集約ルートが作成されるだけでなく、すべてのネイバーへの固有性の強いルートのアドバタイズメントが抑制されます。

ステップ 7 [Attribute 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。[Manage] をクリックして、ルートマップを追加または設定します。これにより、集約ルートの属性を変更できます。

ステップ 8 [Advertise 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。[Manage] をクリックして、ルートを追加または設定します。これにより、集約ルートのさまざまなコンポーネントの作成に使用される特定のルートが選択されます。

ステップ 9 [Suppress 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。[Manage] をクリックして、ルートを追加または設定します。これにより、集約ルートが作成されますが、指定したルートのアドバタイズメントは抑制されます。

ステップ 10 [OK] をクリックします。

ステップ 11 [Aggregate Timer] フィールドで、集約タイマーの値（秒）を指定します。有効な値は、0 または 6 ～ 60 の値です。この値で、ルートが集約される間隔を指定します。デフォルト値は 30 秒です。

ステップ 12 [Apply] をクリックします。

IPv6 ファミリの BGP ネイバーの設定

ここでは、BGP ネイバーおよびネイバー設定を定義するために必要な手順について説明します。

手順

ステップ 1 ASDM で、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[BGP]** > **[IPv6 Family]** の順に選択します。

ステップ 2 [Neighbor] をクリックします。

ステップ 3 [Add] をクリックします。

ステップ 4 左側のペインで、[General] をクリックします。

ステップ 5 [IPv6 Address] フィールドに BGP ネイバーの IPv6 アドレスを入力します。この IPv6 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 6 [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 7 （オプション）[Description] フィールドに BGP ネイバーの説明を入力します。

ステップ 8 （オプション）[Shutdown neighbor 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 9 （オプション）[Enable address family] 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。

ステップ 10 （オプション）[Global Restart Functionality for this peer] チェックボックスをオンにして、ASA ネイバーまたはピア グループの Border Gateway Protocol（BGP）グレースフル リスタート機能をイネーブルまたはディセーブルにします。

（注） このオプションは、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有効になります。

ステップ 11 （オプション）BGP ネイバーシップの送信元としてインターフェイスを更新するには、[送信元の更新（Update-Source）] ドロップダウンボックスからインターフェイスを選択します。

（注） BGP ネイバーシップの送信元としてループバック インターフェイスを更新すると、ループバック インターフェイスの IP アドレスがネットワーク全体にアドバタイズされます。ループバック インターフェイスは eBGP ピアとして機能し、ルーティングに参加します。ループバック インターフェイスは有効にすると安定し、管理上のシャットダウンまで使用可能な状態になるため、ループバック インターフェイスの IP アドレスで常に ASA に到達できます。

ステップ 12 左側のペインで、[Filtering] をクリックします。

ステップ 13 （オプション）[Filter routes using a route map] 領域で、適切な着信または発信ルート マップを選択して、着信ルートまたは発信ルートにルート マップを適用します。[Manage] をクリックして、ルート マップを設定します。

ステップ 14 （オプション）[Filter routes using a prefix list] 領域で、適切な着信または発信プレフィックス リストを選択して BGP ネイバー情報を配布します。[Manage] をクリックして、プレフィックス リストを設定します。

ステップ 15 （オプション）[Filter routes using AS path filter] 領域で、適切な着信または発信 AS パス フィルタを選択して BGP ネイバー情報を配布します。[Manage] をクリックして、AS パス フィルタを設定します。

ステップ 16 （オプション）[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。

ステップ 17 [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。

ステップ 18 [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。

ステップ 19 （オプション）[Control prefixes received from a 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、[Terminate peering when prefix limit is exceeded] をクリックします。[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、[Give only warning message when prefix limit is exceeded] をクリックします。この場合、BGP ネイバーは終了しません。

ステップ 20 左側のペインで、[Routes] をクリックします。

ステップ 21 [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。

ステップ 22 （オプション）[Generate Default route] 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。

ステップ 23 [Route map] ドロップダウン リストから、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 マップを選択します。[Manage] をクリックして、ルート マップを追加および設定します。

ステップ 24 （オプション）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、次の手順を実行します。

a) [Conditionally Advertised Routes] セクションで [Add] をクリックします。

b) exist-map または non-exist-map の条件に一致した場合にアドバタイズされるルート マップを [Advertise Map] ドロップダウン リストから選択します。

c) 次のいずれかを実行します。

- [Exist Map] をクリックしてルート 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。
- [Non-exist Map] をクリックしてルート 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。

d) [OK] をクリックします。

ステップ 25 （オプション）[Remove private autonomous system (AS) numbers from outbound routing updates] チェックボックスをオンにし、プライベート AS 番号を発信ルートにおけるアドバイタイズ対象から除外します。

ステップ 26 左側のペインで、[Timers] をクリックします。

ステップ 27 （オプション）[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、保持時間、最小保持時間を設定します。

ステップ 28 [Keepalive frequency] フィールドに ASA 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。

ステップ 29 [Hold time] フィールドに、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 ASA が宣言するまでの時間（秒）を入力します。デフォルト値は 180 秒です。

ステップ 30 （オプション）[Min Hold time] フィールドに、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 ASA が宣言するまでの最小時間（秒）を入力します。

（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。

ステップ 31 左側のペインで、[Advanced] をクリックします。

ステップ 32 （オプション）[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。

ステップ 33 [Encryption Type] ドロップダウン リストから暗号化タイプを選択します。

ステップ 34 パスワードを [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 文字を指定できます。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。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。

ステップ 35 （オプション）[Send Community Attribute to this neighbor] チェックボックスをオンにします。

ステップ 36 （オプション）[Use ASA as next hop for 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。

ステップ 37 次のいずれかを実行します。

- [Allow connections with neighbor that is not directly connected] をクリックして、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。
  - （オプション）[Disable connection verification] チェックボックスをオンにし、ループバック インターフェイスを使用するシングル ホップ ピアと eBGP ピアリング セッションを確立するための接続確認を無効にします。
- [Limit number of TTL hops to neighbor] をクリックして、BGP ピアリング セッションを保護できるようにします。[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。

ステップ 38 （オプション）[Weight] フィールドに BGP ネイバー接続の重みを入力します。

ステップ 39 [BGP version] ドロップダウン リストから、ASA が受け入れる BGP バージョンを選択します。

（注） バージョンを 2 に設定すると、指定されたネイバーとの間でバージョン 2 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 40 （オプション）[TCP Path MTU 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 セッションをイネーブルにします。

ステップ 41 [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。

ステップ 42 左側のペインで、[Migration] をクリックします。

ステップ 43 （オプション）[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。

- [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 ～ 65535 です。
- （オプション）[Do not prepend local AS number for routes received from neighbor] チェックボックスをオンにします。ローカル AS 番号は、eBGP ピアから受信したルートの前に追加されません。
- （オプション）[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ます。ローカル ルーティング プロセスの AS 番号は前に追加されません。
- （オプション）[Accept either real AS number or local AS number in routes received from neighbor] チェックボックスをオンにします。

ステップ 44 [OK] をクリックします。

ステップ 45 [Apply] をクリックします。

IPv6 ネットワークの設定

ここでは、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を定義するために必要な手順について説明します。

手順

ステップ 1 ASDM で、**[設定（Configuration）] > [デバイスの設定（Device Setup）] > [ルーティング（Routing）] > [BGP] > [IPv6ファミリ（IPv6 Family）]** の順に選択します。

ステップ 2 [Networks] をクリックします。

[Define the networks to be advertised by the BGP routing process] 設定ペインが表示されます。

ステップ 3 [Add] をクリックします。

[Add Network] ペインが表示されます。

ステップ 4 （任意）[Prefix Name] フィールドに、DHCPv6 プレフィックス委任クライアントのプレフィックスの名前を指定します（IPv6 プレフィックス委任クライアントの有効化 を参照）。

ステップ 5 [IPv6 Address/mask] フィールドで、BGP がアドバタイズするネットワークを指定します。

[Prefix Name] を指定した場合、サブネット プレフィックスおよびサブネット マスクを入力します。アドバタイズされたネットワークは、委任されたプレフィックスとサブネットプレフィクスで構成されます。

ステップ 6 [Route Map] ドロップダウン リストから、アドバタイズされるネットワークをフィルタリングするために調べる必要のあるルートマップを選択します。任意で、[Manage] をクリックして、ルート マップを設定または追加します。

ステップ 7 [OK] をクリックします。

ステップ 8 [Apply] をクリックします。

IPv6 再配布の設定

ここでは、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するために必要な手順について説明します。

手順

ステップ 1 ASDM で、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[BGP]** > **[IPv6 Family]** の順に選択します。

ステップ 2 [Redistribution] をクリックします。

ステップ 3 [Add] をクリックします。

[Add Redistribution] ペインが表示されます。

ステップ 4 [Source Protocol] ドロップダウン リストで、BGP ドメインにルートを再配布する元となるプロトコルを選択します。

ステップ 5 [Process ID] ドロップダウン リストで、ソース プロトコルのプロセス ID を選択します。これは OSPF ソース プロトコルに対してのみ使用できます。

ステップ 6 （オプション）[Metric] フィールドに、再配布されるルートのメトリックを入力します。

ステップ 7 [Route Map] ドロップダウン リストで、再配布されるネットワークをフィルタリングをするために調べる必要のあるルート マップを選択します。[Manage] をクリックして、ルート マップを設定または追加します。

ステップ 8 [Match] チェックボックス（[Internal]、[External 1]、[External 2]、[NSSA External 1]、[NSSA External 2] チェックボックス）を 1 つ以上オンにして、OSPF ネットワークからルートを再配布します。

この手順は、OSPF ネットワークからの再配布にのみ適用できます。

ステップ 9 [OK] をクリックします。

ステップ 10 [Apply] をクリックします。

IPv6 ルート注入の設定

ここでは、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するために必要な手順について説明します。

手順

ステップ 1 ASDM で、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[BGP]** > **[IPv4 Family]** の順に選択します。

ステップ 2 [Route Injection] をクリックします。

ステップ 3 [Add] をクリックします。

[Add Conditionally injected route] ペインが表示されます。

ステップ 4 [Inject Map] ドロップダウン リストで、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 マップを選択します。

ステップ 5 [Exist Map] ドロップダウン リストで、BGP スピーカーが追跡するプレフィックスを含むルート マップを選択します。

ステップ 6 [Injected routes will inherit the attributes of the aggregate route] チェックボックスをオンにし、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。

ステップ 7 [OK] をクリックします。

ステップ 8 [Apply] をクリックします。

BGP のモニタリング

次のコマンドを使用して、BGP ルーティング プロセスをモニターできます。コマンド出力の例と説明については、コマンド リファレンスを参照してください。また、ネイバー変更メッセージとネイバー警告メッセージのロギングをディセーブルにできます。

さまざまな BGP ルーティング統計情報をモニターするには、次のコマンドの 1 つを入力します。

（注） BGP ログ メッセージを無効にするには、ルータ コンフィギュレーション モードで **no bgp log-neighbor-changes** コマンドを入力します。これにより、ネイバー変更メッセージのロギングが無効になります。BGP ルーティング プロセスのルータ コンフィギュレーション モードでこのコマンドを入力します。デフォルトでは、ネイバー変更はログに記録されます。

- **[Monitoring] > [Routing] > [BGP Neighbors]**

  各行は 1 つの BGP ネイバーを表します。リストには、ネイバーごとに、IP アドレス、AS 番号、ルータ ID、状態（アクティブ、アイドルなど）、稼働時間、グレースフル リスタート機能、再起動時間、stalepath 時間が含まれます。

- **[Monitoring] > [Routing] > [BGP Routes]**

  各行は 1 つの BGP ルートを表します。リストには、ルートごとに、ステータス コード、IP アドレス、ネクスト ホップ アドレス、ルート メトリック、Local preference 値、重み、パスが含まれます。

BGP の履歴

表 *1 : BGP* の各機能の履歴

機能名	プラットフォームリリース	機能情報
BGP のサポート	9.2(1)	Border Gateway Protocol を使用した、データのルーティング、認証の実行、およびルーティング情報の再配布とモニターについて、サポートが追加されました。 次の画面が導入されました。 [Configuration] > [Device Setup] > [Routing] > [BGP Monitoring] > [Routing] > [BGP Neighbors, Monitoring] > [Routing] > [BGP Routes] 次の画面が変更されました。 [Configuration] > [Device Setup] > [Routing] > [Static Routes> Add] > [Add Static Route Configuration] > [Device Setup] > [Routing] > [Route Maps> Add] > [Add Route Map]
ASA クラスタリングに対する BGP のサポート	9.3(1)	L2 および L3 クラスタリングのサポートが追加されました。 次の画面が変更されました。[Configuration] > [Device Setup] > [Routing] > [BGP] > [IPv4 Family] > [General]
ノンストップ フォワーディングに対する BGP のサポート	9.3(1)	ノンストップ フォワーディングのサポートが追加されました。 次の画面が変更されました。[Configuration] > [Device Setup] > [Routing] > [BGP] > [General]、[Configuration] > [Device Setup] > [Routing] > [BGP] > [IPv4 Family] > [Neighbor]、[Monitoring] > [Routing] > [BGP Neighbors]

機能名	プラットフォームリリース	機能情報
アドバタイズされたマップに対する BGP のサポート	9.3(1)	アドバタイズされたマップに対する BGPv4 のサポートが追加されました。 次の画面が変更されました。[Configuration] > [Device Setup] > [Routing] > [BGP] > [IPv4 Family] > [Neighbor] > [Add BGP Neighbor] > [Routes]
IPv6 に対する BGP のサポート	9.3(2)	IPv6 のサポートが追加されました。 次の画面が導入されました。[Configuration] > [Device Setup] > [Routing] > [BGP] > [IPv6 Family]
委任プレフィックスの IPv6 ネットワーク アドバタイズメント	9.6(2)	ASA は DHCPv6 プレフィックスの委任クライアントをサポートするようになりました。ASA は DHCPv6 サーバーから委任プレフィックスを取得します。ASA は、これらのプレフィックスを使用して他の ASA インターフェイスのアドレスを設定し、ステートレスアドレス自動設定（SLAAC）クライアントが同じネットワーク上で IPv6 アドレスを自動設定できるようにします。これらのプレフィックスをアドバタイズするように BGP ルータを設定できます。 次の画面が変更されました。**[Configuration]** > **[Device Setup]** > **[Routing]** > **[BGP]** > **[IPv6 Family]** > **[Networks]**
BGP トラフィックのループバック インターフェイス サポート	9.18(2)	ループバック インターフェイスを追加して、BGP トラフィックに使用できるようになりました。 新規/変更されたコマンド：**interface loopback**、**neighbor update-source** 新規/変更された画面： • [設定（Configuration）] > [デバイスのセットアップ（Device Setup）] > [インターフェイスの設定（Interface Settings）] > [インターフェイス（Interfaces）] > [ループバック インターフェイスの追加（Add Loopback Interface）] • [設定（Configuration）] > [デバイスのセットアップ（Device Setup）] > [ルーティング（Routing）] > [BGP] > [IPv4ファミリ（IPv4 Family）]/[IPv6ファミリ（IPv6 Family）] > [ネイバー（Neighbor）] > [追加（Add）] > [全般（General）] ASDM サポートは 7.19 で追加されました。

機能名	プラットフォームリリース	機能情報
IPv6 のグレースフルリスタート	9.19(1)	IPv6アドレスファミリのグレースフルリスタートサポートを追加しました。

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。

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。

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。