

ASA/PIX および OSPF の設定例

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[関連製品](#)

[表記法](#)

[背景説明](#)

[設定](#)

[ネットワーク図](#)

[設定](#)

[ASDM の設定](#)

[OSPF 認証の設定](#)

[Cisco ASA CLI 設定](#)

[Cisco IOS ルータ \(R2 \) CLI 設定](#)

[Cisco IOS ルータ \(R1 \) CLI 設定](#)

[Cisco IOS ルータ \(R3 \) CLI 設定](#)

[ASA による OSPF への再配布](#)

[確認](#)

[トラブルシューティング](#)

[ポイントツーポイント ネットワーク向けのスタティック ネイバー設定](#)

[トラブルシューティングのためのコマンド](#)

[関連情報](#)

概要

このドキュメントでは、Open Shortest Path First (OSPF) を介してルートを学習し、認証および再配布を実行するように、Cisco ASA を設定する方法について説明します。

EIGRP 設定の詳細については、『[PIX/ASA 8.x : Cisco Adaptive Security Appliance \(ASA \) での EIGRP の設定](#)』を参照してください。

注: 非対称ルーティングは ASA/PIX ではサポートされません。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- Cisco ASA/PIX は、バージョン 7.x 以降を実行する必要があります。
- OSPF は、マルチコンテキスト モードではサポートされていません。これは、シングル モードのみでサポートされます。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- ソフトウェア バージョン 8.0 以降が稼働する Cisco 5500 シリーズ適応型セキュリティ アプライアンス (ASA)
- Cisco Adaptive Security Device Manager (ASDM) ソフトウェア バージョン 6.0 以降

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

関連製品

このドキュメントの情報は、ソフトウェア バージョン 8.0 以降が稼働する Cisco 500 シリーズ PIX ファイアウォールにも適用できます。

表記法

ドキュメント表記の詳細は、『[シスコ テクニカル ティップスの表記法](#)』を参照してください。

背景説明

OSPF は、すべての既知の宛先までの最短パスを構築および計算するために、リンクステート アルゴリズムを使用します。OSPF エリア内の各ルータには、ルータが使用可能なインターフェイスと到達可能なネイバーそれぞれのリストである同一のリンクステート データベースが置かれています。

RIP に比べると OSPF は次の点で有利です。

- OSPF のリンクステート データベースのアップデート送信は RIP ほど頻繁ではありません。また、古くなった情報のタイムアウトで徐々にアップデートされるのではなく、リンクステート データベースは瞬時にアップデートされます。
- ルーティング決定はコストに基づいて行われます。これは、特定のインターフェイスを介してパケットを送信するためにオーバーヘッドが必要であることを示しています。セキュリティ アプライアンスは、インターフェイスのコストをリンク帯域幅に基づいて計算し、宛先までのホップ数は使用しません。コストは優先パスを指定するために設定できます。

最短パス優先アルゴリズムの欠点は、CPU サイクルとメモリが大量に必要なことです。

セキュリティ アプライアンスは、OSPF プロトコルのプロセス 2 つを異なるインターフェイス セット上で同時に実行できます。同じ IP アドレスを使用する複数のインターフェイス (NAT ではこのようなインターフェイスは共存可能ですが、OSPF ではアドレスの重複は許可されません) があるときに、2 つのプロセスを実行する場合があります。あるいは、一方のプロセスを内部で実行しながら別のプロセスを外部で実行し、ルートのサブセットをこの 2 つのプロセス間で再配布する場合があります。同様に、プライベート アドレスをパブリック アドレスから分離する

必要がある場合もあります。

OSPF ルーティング プロセスには、別の OSPF ルーティング プロセスや RIP ルーティング プロセスから、または OSPF 対応インターフェイスに設定されているスタティック ルートおよび接続されているルートから、ルートを再配布できます。

セキュリティ アプライアンスは、次の OSPF 機能をサポートします。

- エリア内ルート、エリア間ルート、および外部ルート (タイプ I とタイプ II) のサポート
- 仮想リンクのサポート
- OSPF の LSA フラッディング
- OSPF パケットの認証 (パスワード認証と MD5 認証の両方)
- セキュリティ アプライアンスの指定ルータまたは指定バックアップ ルータとしての設定のサポート。セキュリティ アプライアンスは、ABR として設定することもできます。ただし、セキュリティ アプライアンスの ASBR としての設定は、デフォルト情報のみに制限されます (たとえば、デフォルト ルートのインジェクトなど)。
- スタブ エリアと not so stubby エリアのサポート
- ABR タイプ 3 LSA フィルタリング

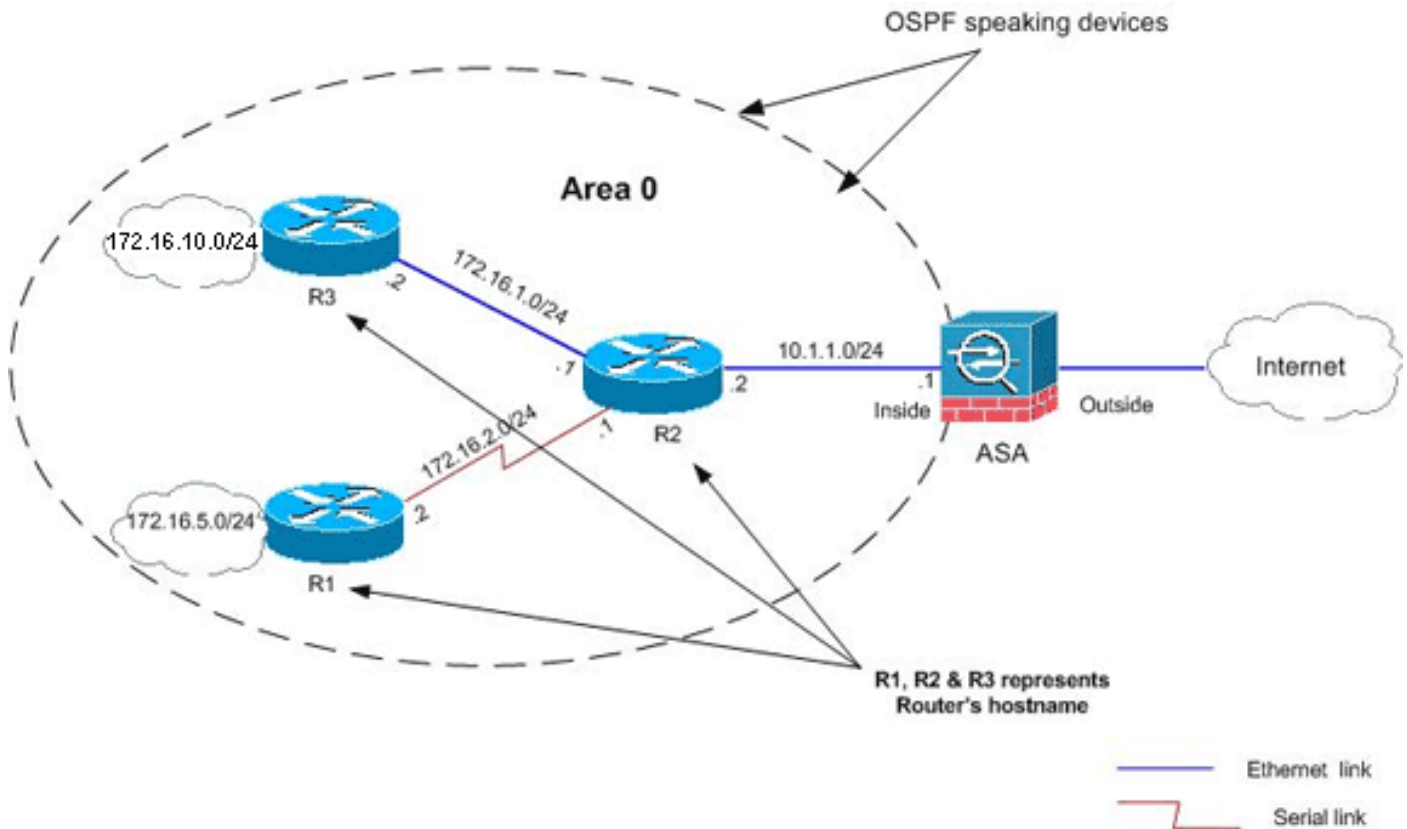
設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このセクションで使用されているコマンドの詳細を調べるには、[Command Lookup Tool](#) ([登録ユーザ専用](#)) を使用してください。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。



このネットワークトポロジでは、Cisco ASA 内部インターフェイス IP アドレスは、10.1.1.1/24 です。ここでは、OSPF を Cisco ASA で設定し、隣接ルータ (R2) を直接介した内部ネットワーク (172.16.1.0/24、172.16.2.0/24、172.16.5.0/24、172.16.10.0/24) へのルートを学習することを目的とします。R2 は、他の 2 つのルータ (R1 と R3) を介したリモート内部ネットワークへのルートを学習します。

設定

このドキュメントでは、次の設定を使用します。

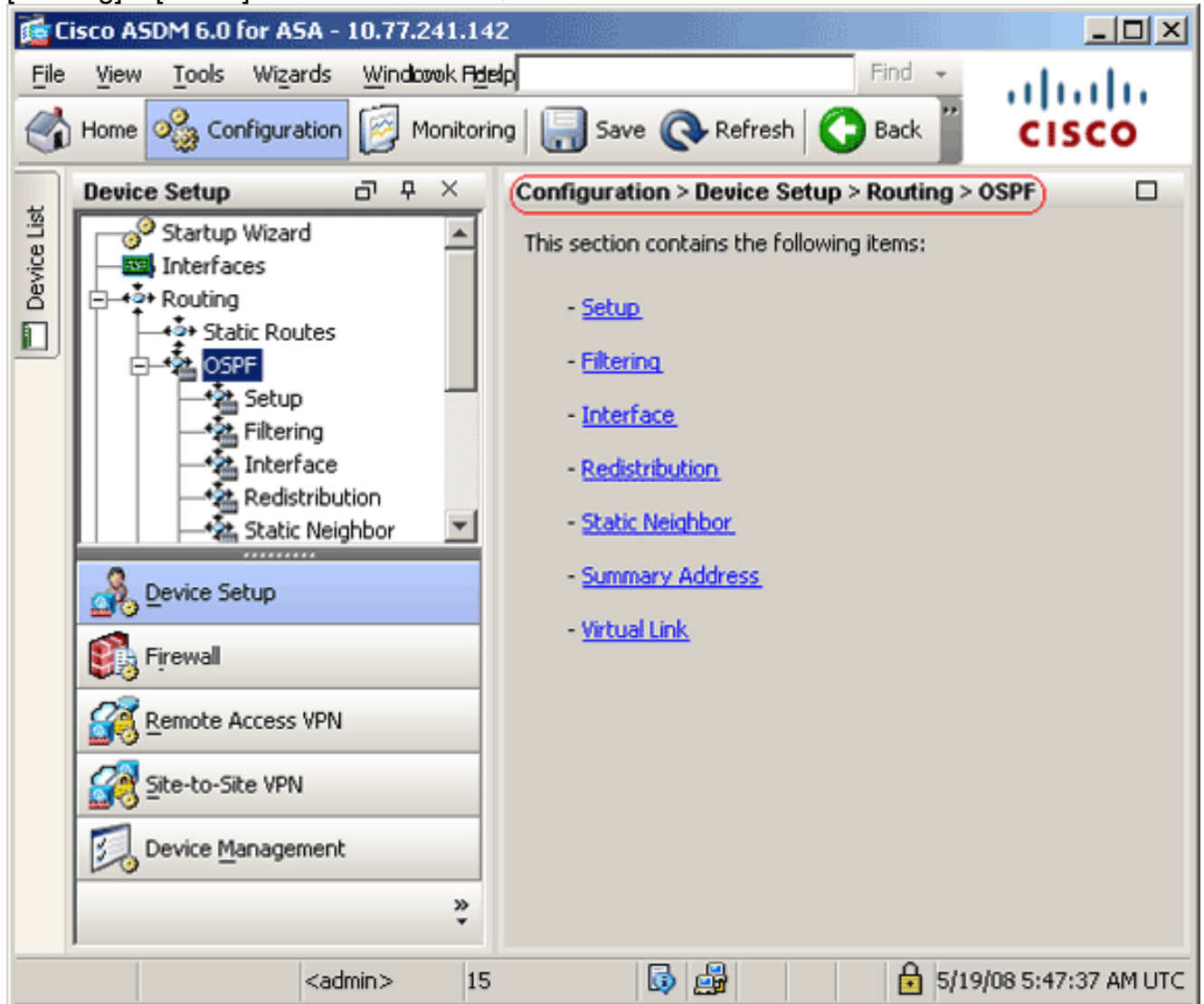
- [ASDM の設定](#)
- [OSPF 認証の設定](#)
- [Cisco ASA CLI 設定](#)
- [Cisco IOS ルータ \(R2 \) CLI 設定](#)
- [Cisco IOS ルータ \(R1 \) CLI 設定](#)
- [Cisco IOS ルータ \(R3 \) CLI 設定](#)
- [ASA による OSPF への再配布](#)

ASDM の設定

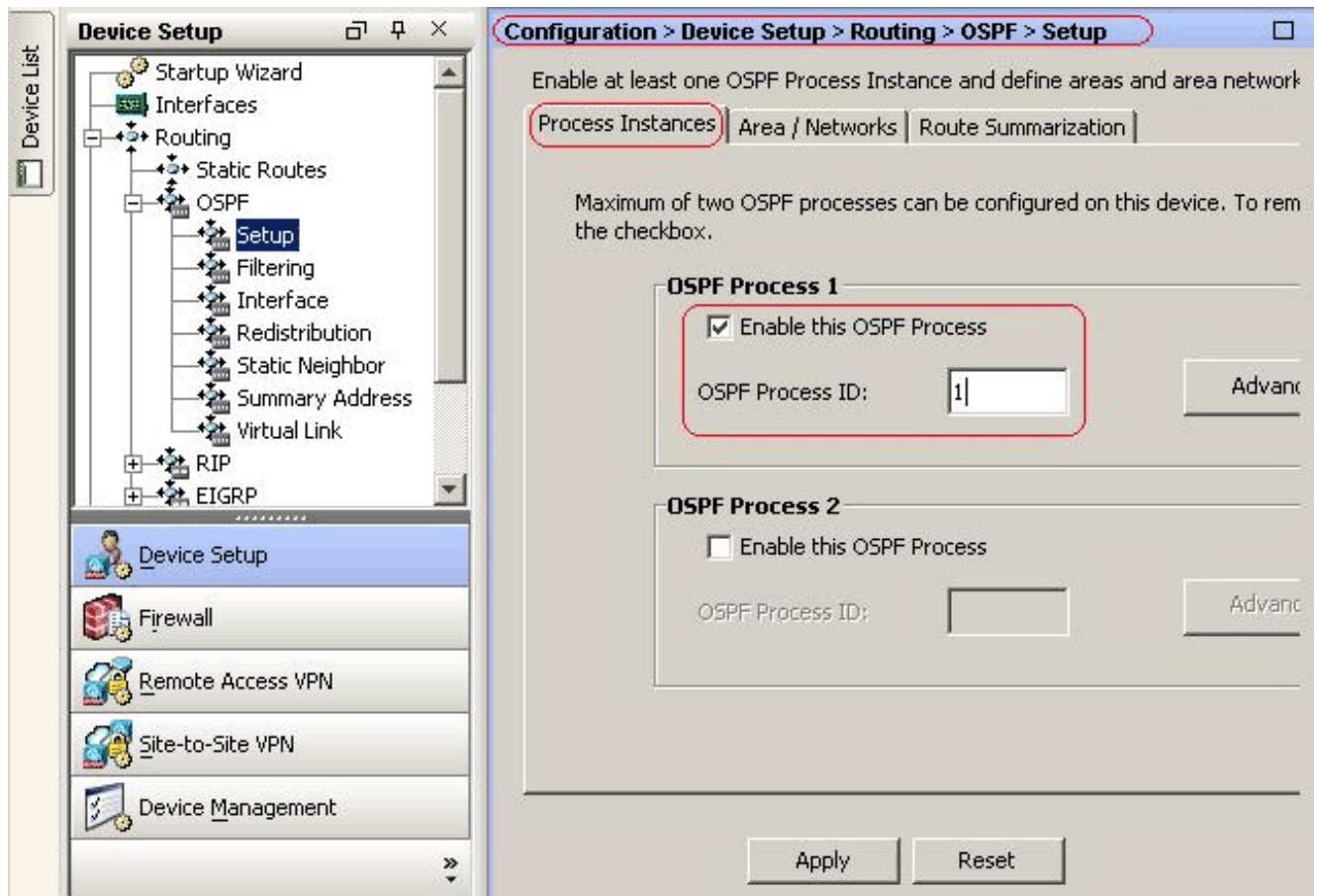
Adaptive Security Device Manager (ASDM) は、セキュリティ アプライアンスのソフトウェアの設定およびモニタに使用されるブラウザベースのアプリケーションです。ASDM は、セキュリティ アプライアンスからロードされ、デバイスの設定、モニタ、管理に使用されます。また、ASDM Launcher (Windows のみ) を使用して、Java アプレットより高速に ASDM アプリケーションを起動することもできます。ここでは、この ASDM のマニュアルで説明する機能を設定する際に必要な情報を説明します。

Cisco ASA で OSPF を設定するには、次の手順を実行してください。

1. Cisco ASA の ASDM にログインします。
2. この図に示すように、ASDM インターフェイスの [Configuration] > [Device Setup] > [Routing] > [OSPF] エリアに移動します。



3. この図に示すように、[Setup] > [Process Instances] タブで OSPF ルーティング プロセスをイネーブルにします。この例では、OSPF ID プロセスは 1 です。



4. [Setup > Process Instances] タブで [Advanced] をクリックして、オプションの高度な OSPF ルーティング プロセス パラメータを設定できます。[Router ID]、[Adjacency Changes]、[Administrative Route Distances]、[Timers] および [Default Information Originate] 設定など、プロセス固有の設定を編集できます。

Edit OSPF Process Advanced Properties

OSPF Process: Router ID:

Ignore LSA MOSPF (suppress the sending of syslog messages when router receives a LSA MOSPF packets) RFC1583 Compatible (calculate summary route costs per RFC 1583)

Adjacency Changes

Enable this for the firewall to send a syslog message when an OSPF neighbor goes up/down. Log Adjacency Changes

Enable this for the firewall to send a syslog for each state change. Log Adjacency Change Details

Administrative Route Distances

Inter Area (distance for all routes from one area to another area)	Intra Area (distance for all routes within an area)	External (distance for all routes from other routing domains, learned by redistribution)
<input type="text" value="110"/>	<input type="text" value="110"/>	<input type="text" value="110"/>

Timers (in seconds)

SPF Delay Time (between when OSPF receives a topology change and when it starts a SPF calculation)	SPF Hold Time (between two consecutive SPF calculations)	LSA Group Pacing (interval at which OSPF LSAs are collected into a group and refreshed)
<input type="text" value="5"/>	<input type="text" value="10"/>	<input type="text" value="240"/>

Default Information Originate

Configure this to generate default external route into an OSPF routing domain.

Enable Default Information Originate Always advertise the default route

Metric Value: Metric Type: Route Map:

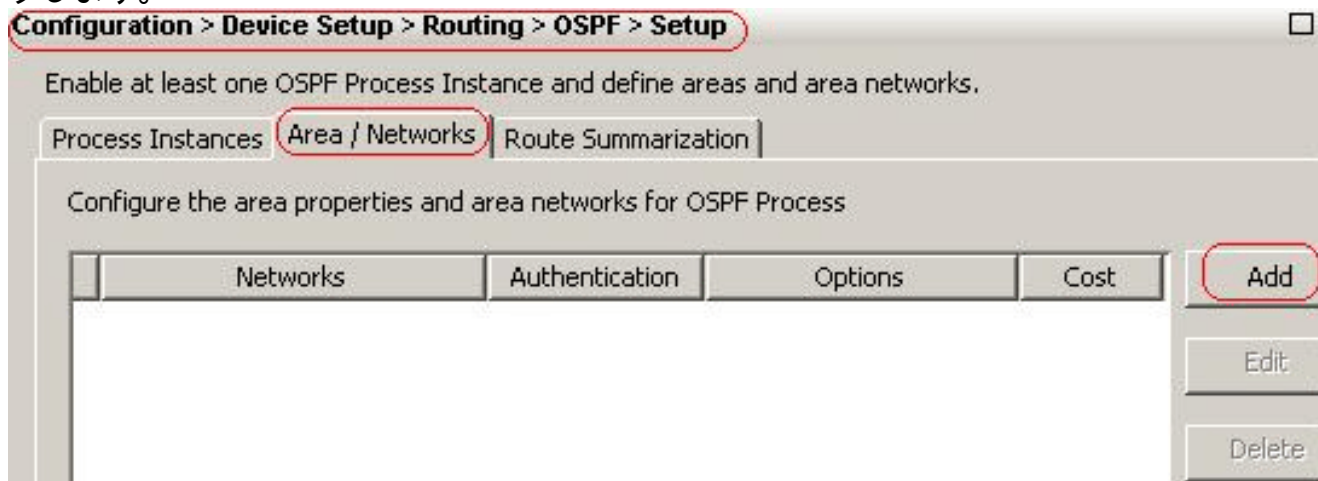
OK Cancel Help

このリストは各フィールドについて説明します。[OSPF Process] : 設定している OSPF プロセスを表示します。この値は変更できません。[Router ID] : 固定のルータ ID を使用するには、[Router ID] フィールドにルータ ID を IP アドレス形式で入力します。この値を空白のままにした場合、セキュリティ アプライアンスで最上位の IP アドレスがルータ ID として使用されます。この例では、[Router ID] は、内部インターフェイス (10.1.1.1) の IP アドレスで静的に設定されます。[Ignore LSA MOSPF] : セキュリティ アプライアンスがタイプ 6 (MOSPF) LSA パケットを受信するときにシステム ログ メッセージの設定を抑制するには、このチェックボックスをオンにします。デフォルトでは、この設定はオフになっています。[RFC 1583 Compatible] : RFC 1583 あたりのサマリー ルート コストを計算するには、このチェックボックスをオンにします。RFC 2328 あたりのサマリー ルート コストを計算するには、このチェックボックスをオフにします。ルーティング ループの可能性を最小限に抑えるには、OSPF ルーティング ドメイン内のすべての OSPF デバイスに同じように RFC 互換性が設定されている必要があります。この設定は、デフォルトでオンになっています。[Adjacency Changes] : 隣接関係の変更を定義する設定が含まれます。隣接関係が変更されると、システム ログ メッセージが送信されます。[Log Adjacency

Changes] : OSPF ネイバーが起動またはダウンしたときだけでなく、セキュリティ アプライアンスがシステム ログ メッセージを送信するようにするには、このチェックボックスをオンにします。この設定は、デフォルトでオンになっています。[Log Adjacency Changes Detail] : ネイバーが起動またはダウンしたときだけでなく、状態の変更が発生するたびにセキュリティ アプライアンスがシステム ログ メッセージを送信するようにするには、このチェックボックスをオンにします。デフォルトでは、この設定はオフになっています。

[Administrative Route Distances] : ルート タイプに基づくルートのアドミニストレーティブ ディスタンスの設定を含みます。[Inter Area] : 1 つのエリアから別のエリアへのすべてのルートのアドミニストレーティブ ディスタンスを設定します。有効な値の範囲は 1 ~ 255 です。デフォルト値は 100 です。[Intra Area] : エリア内のすべてのルートのアドミニストレーティブ ディスタンスを設定します。有効な値の範囲は 1 ~ 255 です。デフォルト値は 100 です。[External] : 再配布を通じて取得される他のルーティング ドメインからのすべてのルートのアドミニストレーティブ ディスタンスを設定します。有効な値の範囲は 1 ~ 255 です。デフォルト値は 100 です。[Timers] : LSA ペーシングおよび SPF 計算タイマーの設定に使用する設定が含まれます。[SPF Delay Time] : OSPF がトポロジの変更を受信してから SPF の計算が開始されるまでの時間を指定します。0 ~ 65535。デフォルト値は 5 です。[SPF Hold Time] : 連続する SPF 計算の間の保持時間を指定します。有効値の範囲は 1 ~ 65534 です。10 [LSA Group Pacing] : LSA がグループに収集され、更新、チェックサム、または時間経過する間隔を指定します。有効な値の範囲は 10 ~ 1800 です。デフォルト値は 240 です。[Default Information Originate] : ASBR がデフォルトの外部ルートを OSPF ルーティング ドメインに生成するとき使用する設定を含みます。[Enable Default Information Originate] : OSPF ルーティング ドメインへのデフォルト ルートの生成をイネーブルにするには、このチェックボックスをオンにします。[Always advertise the default route] : デフォルト ルートを常にアドバタイズするには、このチェックボックスをオンにします。このオプションは、デフォルトではオフになっています。[Metric Value] : OSPF デフォルト メトリックを指定します。0 16777214。デフォルト値は 1 です。[Metric Type] : OSPF ルーティング ドメインにアドバタイズされたデフォルト ルートに関連付けられた外部リンク タイプを指定します。有効値は 1 または 2 です。それぞれタイプ 1 またはタイプ 2 外部ルートを示します。2 [Route Map] : (任意) 適用するルート マップの名前です。ルート マップが一致すると、ルーティング プロセスによってデフォルト ルートが生成されます。

5. これまでの手順を完了したら、[Setup] > [Area/Networks] タブで OSPF ルーティングに参加するネットワークおよびインターフェイスを定義し、この図に示すように、[Add] をクリックします。



[Add OSPF Area] ダイアログ ボックスが表示されます。

Add OSPF Area

OSPF Process: Area ID:

Area Type

Normal

Stub Summary (allows sending LSAs into the stub area)

NSSA Redistribute (imports routes to normal and NSSA areas)

Summary (allows sending LSAs into the NSSA area)

Default Information Originate (generate a Type 7 default)

Metric Value: Metric Type:

Area Networks

Enter IP Address and Mask

IP Address:

Netmask:

IP Address	Netmask
10.1.1.0	255.255.255.0

Authentication

None Password MD5

Default Cost:

この例では、OSPF が内部インターフェイスのみでイネーブルにされているため、追加されるネットワークだけが内部ネットワーク (10.1.1.0/24) です。注: IP アドレスが定義済みネットワークの範囲内にあるインターフェイスだけが、OSPF ルーティング プロセスに参加します。

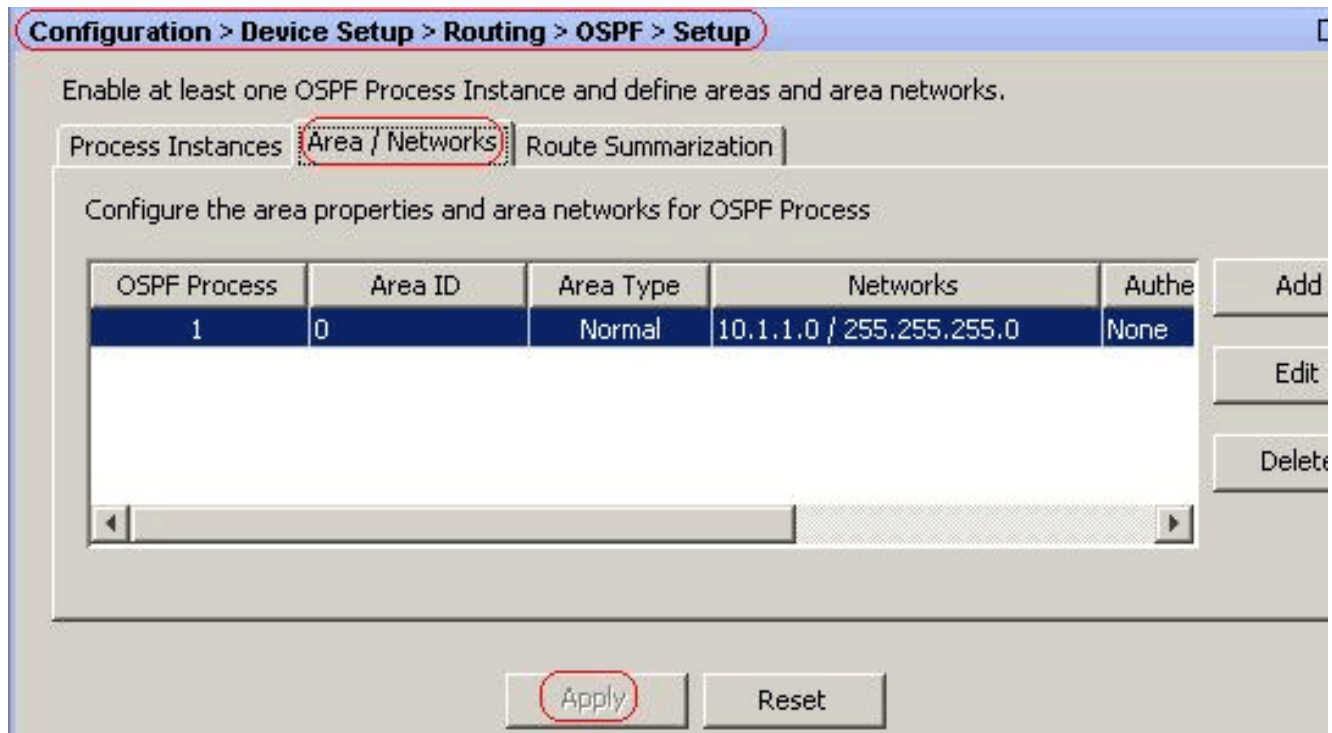
6. [OK] をクリックします。このリストは各フィールドについて説明します。[OSPF Process]: 新しいエリアを追加する場合、OSPF プロセスの ID を選択します。セキュリティ アプライアンスでイネーブルにされている OSPF プロセスが 1 つだけの場合、そのプロセスがデフォルトで選択されます。既存のエリアを編集する場合、OSPF プロセス ID は変更できません。[Area ID]: 新しいエリアを追加する場合、エリア ID を入力します。このエリア ID には、10 進数が IP アドレスを指定できます。有効な 10 進値の範囲は、0 ~ 4294967295 です。既存のエリアを編集する場合、エリア ID は変更できません。この例では、[Area ID] は 0 です。[Area Type]: 設定しているエリアのタイプに対する設定を含みます。[Normal]: このエリアを標準の OSPF エリアにする場合、このオプションを選択します。エリアを最初に作成するときは、このオプションがデフォルトで選択されています。[Stub]: このエリアをスタブ エリアにする場合、このオプションを選択します。スタブ エ

リアには、その向こう側にルータまたはエリアはありません。スタブ エリアでは、AS External LSA (タイプ 5 LSA) がスタブ エリアにフラッディングされないようになっています。スタブ エリアを作成する場合、[Summary] チェックボックスをオフにして、サマリー LSA (タイプ 3 および 4) がエリアにフラッディングされないようにします。

[Summary] : エリアがスタブ エリアとして定義される場合、LSA がスタブ エリアに送信されないようにこのチェックボックスをオフにします。スタブ エリアの場合、このチェックボックスはデフォルトでオンになっています。NSSA — not-so-stubby NSSA はタイプ 7 LSA を受け入れます。NSSA を作成する場合、[Summary] チェックボックスをオフにして、サマリー LSA がエリアにフラッディングされないようにします。また、[Redistribute] チェックボックスをオフにし、[Default Information Originate] をイネーブルにして、ルート再配布をディセーブルにすることもできます。[Redistribute] : ルートが NSSA にインポートされないようにするには、このチェックボックスをオフにします。このチェックボックスは、デフォルトでオンになっています。[Summary] : エリアが NSSA として定義される場合、LSA がスタブ エリアに送信されないようにこのチェックボックスをオフにします。NSSA の場合、このチェックボックスはデフォルトでオンになっています。[Default Information Originate] : タイプ 7 デフォルトを NSSA に生成するには、このチェックボックスをオンにします。このチェックボックスは、デフォルトでオフになっています。[Metric Value] : デフォルト ルートの OSPF メトリック値を指定するには、値を入力します。0 16777214。デフォルト値は 1 です。[Metric Type] : デフォルト ルートの OSPF メトリック タイプを指定するには、値を入力します。選択肢は 1 (タイプ 1) または 2 (タイプ 2) です。2

[Area Networks] : OSPF エリアを定義する設定を含めます。[Enter IP Address and Mask] : そのエリア内のネットワークを定義するのに使用する設定を含みます。[IP Address] : そのエリアに追加するネットワークまたはホストの IP アドレスを入力します。デフォルト エリアを作成するには、0.0.0.0 およびネットマスク 0.0.0.0 を使用します。0.0.0.0 は 1 つのエリア内だけで使用できます。[Netmask] : エリアに追加する IP アドレスまたはホストのネットワーク マスクを選択します。ホストを追加する場合、255.255.255.255 マスクを選択します。この例では、10.1.1.0/24 は、設定されるネットワークです。[Add] : [Enter IP Address and Mask] エリアで定義したネットワークをエリアに追加します。追加されたネットワークは、[Area Networks] テーブルに表示されます。[Delete] : 選択したネットワークを [Area Networks] テーブルから削除します。[Area Networks] : そのエリアに対して定義されたネットワークを表示します。[IP Address] : ネットワークの IP アドレスを表示します。[Netmask] : ネットワークのネットワーク マスクを表示します。[Authentication] : OSPF エリア認証の設定が含まれます。[None] : OSPF エリア認証をディセーブルにするには、このオプションを選択します。これがデフォルト設定です。[Password] : エリア認証用のクリア テキスト パスワードを使用する場合、このオプションを選択します。セキュリティ面が懸念される場合、このオプションは推奨しません。MD5 — MD5 [Default Cost] : エリアのデフォルト コストを指定します。0 ~ 65535。デフォルト値は 1 です。

7. [Apply] をクリックします。



8. オプションで、[Filter Rules] ペインでルート フィルタを定義できます。ルート フィルタにより、OSPF 更新で送受信することを許可されているルートをより細かく制御できます。
9. オプションで、ルート再配布を設定できます。Cisco ASA は、RIP および EIGRP により検出されるルートを OSPF ルーティング プロセスに再配布できます。スタティック ルートおよび接続されているルートも、OSPF ルーティング プロセスに再配布できます。
[Redistribution] ペインでルート再配布を定義します。
10. OSPF hello パケットはマルチキャスト パケットとして送信されます。OSPF ネイバーが、トンネルなど、非ブロードキャスト ネットワークを越えた場所にある場合、そのネイバーを手動で定義する必要があります。手動で OSPF ネイバーを定義すると、hello パケットはユニキャスト メッセージとしてそのネイバーに送信されます。スタティック OSPF ネイバーを定義するには、[Static Neighbor] ペインに移動します。
11. 他のルーティング プロトコルから学習したルートをサマライズできます。サマリーのアドバタイズに使用されるメトリックは、具体的なルートすべての中で最小のメトリックです。サマリー ルートは、ルーティング テーブルのサイズを削減するのに役立ちます。OSPF のサマリー ルートを使用すると、OSPF ASBR は、そのアドレスでカバーされるすべての再配布ルートの集約として、1つの外部ルートをアドバタイズします。OSPF に再配布されている、他のルーティング プロトコルからのルートだけをサマライズできます。
12. [Virtual link] ペインで、エリアを OSPF ネットワークに追加できます。ただし、エリアをバックボーン エリアに直接接続することはできません。この場合、仮想リンクを作成する必要があります。仮想リンクは、通過エリアと呼ばれる共通エリアを持つ2つの OSPF デバイスを接続します。OSPF デバイスのいずれかは、バックボーン エリアに接続されている必要があります。

OSPF 認証の設定

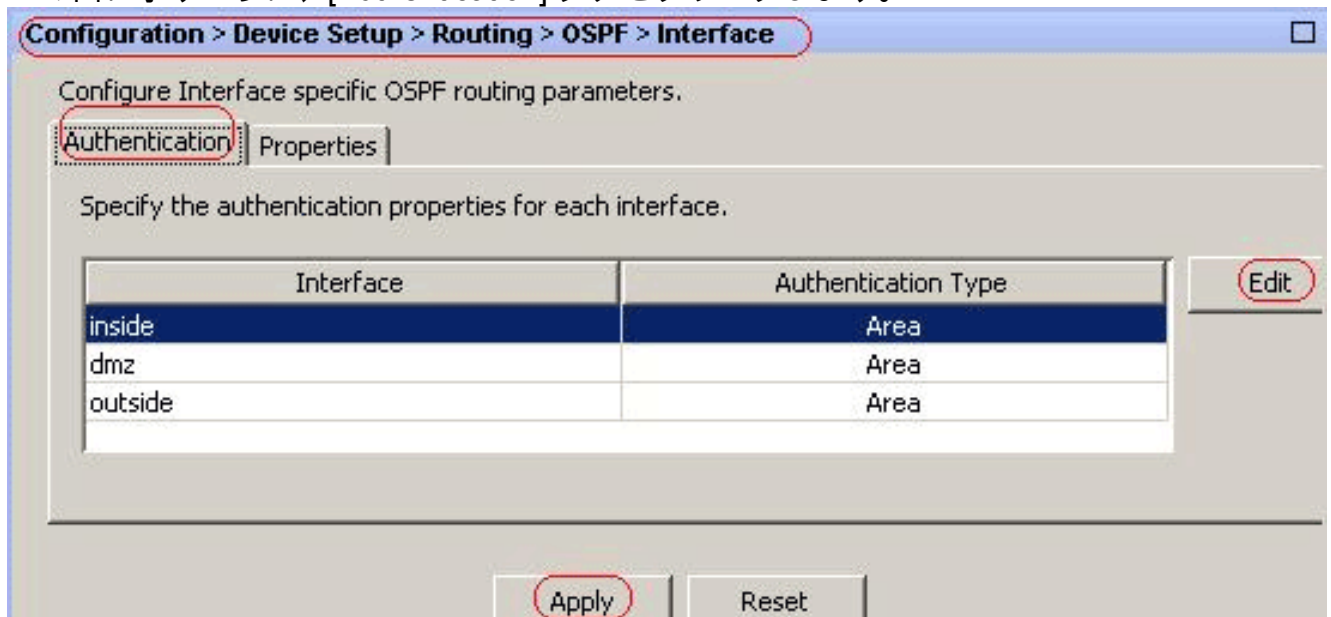
Cisco ASA は、OSPF ルーティング プロトコルからのルーティング アップデートの MD5 認証をサポートします。MD5 キーを使用したダイジェストが各 OSPF パケットに含まれており、承認されていない送信元からの不正なルーティング メッセージや虚偽のルーティング メッセージが取り込まれないように阻止します。認証を OSPF メッセージに追加すると、ルータおよび Cisco ASA のみが、同じ事前共有キーで設定される他のルーティング デバイスからルーティング メッセージを受信します。この認証を設定しない場合、ネットワークへの異なるまたは逆方向のルー

ト情報を持つ別のルーティング デバイスが別のユーザにより導入されると、ルータまたは Cisco ASA のルーティング テーブルが破損し、Denial of Service 攻撃が発生します。ルーティング デバイス (ASA を含む) 間で送信される EIGRP メッセージに認証を追加すると、意図する場合でもしない場合でも別のルータがネットワークに追加されたり、問題が発生したりすることを回避できます。

OSPF ルート認証は、インターフェイスごとに設定します。OSPF メッセージ認証対象として設定されたインターフェイス上にあるすべての OSPF ネイバーには、隣接関係を確立できるように同じ認証モードとキーを設定する必要があります。

Cisco ASA で OSPF MD5 認証をイネーブルにするには、次の手順を実行します。

1. ASDM で、[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Interface] に移動して、この図に示すように、[Authentication] タブをクリックします。



- この場合、OSPF は、内部インターフェイスでイネーブルにされます。
2. [inside] インターフェイスを選択して、[Edit] をクリックします。
3. [Authentication] で、[MD5 authentication] を選択して、認証パラメータに関する情報を追加します。この場合、事前共有キーは [cisco123] で、キー ID は [1] です。

Edit OSPF Interface Authentication

Interface:

Authentication

No authentication
 Area authentication, if defined
 MD5 authentication

Authentication Password

Enter Password: Re-enter Password:

MD5 IDs and Keys

MD5 Key ID:

MD5 Key:

MD5 Key ID	MD5 Key
1	cisco123

4. [OK] をクリックして、[Apply] をクリックします。

Configuration > Device Setup > Routing > OSPF > Interface

Configure Interface specific OSPF routing parameters.

Specify the authentication properties for each interface.

Interface	Authentication Type
inside	MD5
dmz	Area
outside	Area

Cisco ASA CLI 設定

Cisco ASA

```
ciscoasa#show running-config : Saved : ASA Version
8.0(2) ! hostname ciscoasa enable password
8Ry2YjIyt7RRXU24 encrypted names !--- Inside interface
configuration interface Ethernet0/1 nameif inside
security-level 100 ip address 10.1.1.1 255.255.255.0
ospf cost 10 !--- OSPF authentication is configured on
the inside interface ospf message-digest-key 1 md5
<removed> ospf authentication message-digest ! !---
Outside interface configuration interface Ethernet0/2
nameif outside security-level 0 ip address 192.168.1.2
255.255.255.0 ospf cost 10 ! !--- Output Suppressed icmp
unreachable rate-limit 1 burst-size 1 asdm image
disk0:/asdm-602.bin no asdm history enable arp timeout
14400 ! !--- OSPF Configuration router ospf 1 network
10.1.1.0 255.255.255.0 area 0 log-adj-changes ! !---
This is the static default gateway configuration in
order to reach Internet route outside 0.0.0.0 0.0.0.0
192.168.1.1 1 ciscoasa#
```

Cisco IOS ルータ (R2) CLI 設定

Cisco IOS ルータ (R2)

```
!--- Interface that connects to the Cisco ASA. !---
Notice the OSPF authentication parameters interface
Ethernet0 ip address 10.1.1.2 255.255.255.0 ip ospf
authentication message-digest ip ospf message-digest-key
1 md5 cisco123 !--- Output Suppressed !--- OSPF
Configuration router ospf 1 log-adjacency-changes
network 10.1.1.0 0.0.0.255 area 0 network 172.16.1.0
0.0.0.255 area 0 network 172.16.2.0 0.0.0.255 area 0
```

Cisco IOS ルータ (R1) CLI 設定

Cisco IOS ルータ (R1)

```
!--- Output Suppressed !--- OSPF Configuration router
ospf 1 log-adjacency-changes network 172.16.5.0
0.0.0.255 area 0 network 172.16.2.0 0.0.0.255 area 0
```

Cisco IOS ルータ (R3) CLI 設定

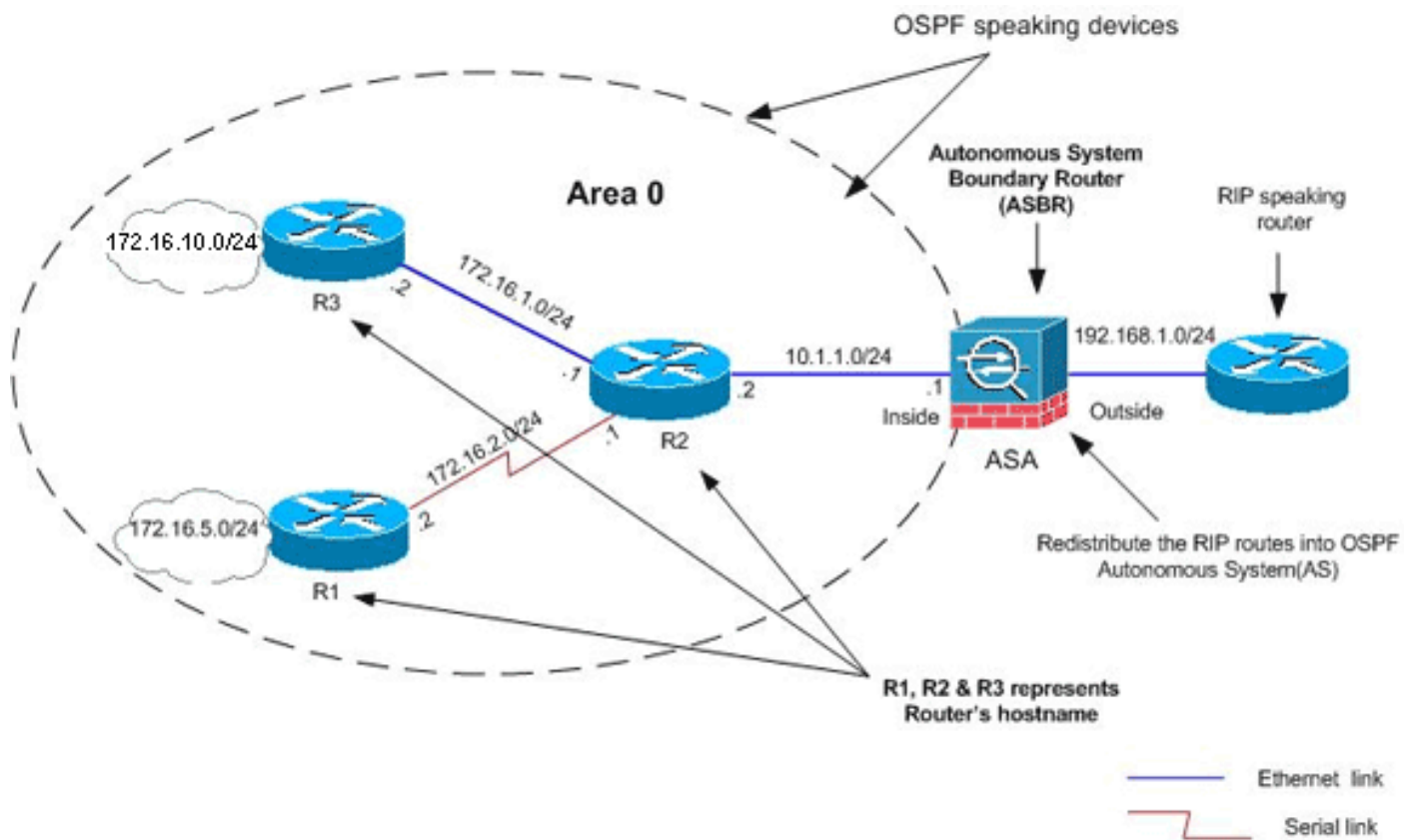
Cisco IOS ルータ (R3)

```
!--- Output Suppressed !--- OSPF Configuration router
ospf 1 log-adjacency-changes network 172.16.1.0
0.0.0.255 area 0 network 172.16.10.0 0.0.0.255 area 0
```

ASA による OSPF への再配布

上記のとおり、OSPF ルーティング プロセスには、別の OSPF ルーティング プロセスや RIP ルーティング プロセスから、または OSPF 対応インターフェイスに設定されているスタティック ルートおよび接続されているルートから、ルートを再配布できます。

この例では、次のようなネットワーク図で、RIP ルートを OSPF に再配布します。



ASDM の設定

1. [Configuration] > [Device Setup] > [Routing] > [RIP] > [Setup] を選択し、RIP をイネーブルにして、次の図に示すように、ネットワーク 192.168.1.0 を追加します。

Configuration > Device Setup > Routing > RIP > Setup

Configure the global Routing Information Protocol (RIP) parameters. You can configure the setting of the RIP routing process.

Enable RIP routing

Enable auto-summarization

Enable RIP version Version 1 Version 2

(If global version in not configured then device sends Version 1 and receives Versions 1 & 2.)

Enable default information originate Route Map:

Networks

IP Network to Add:

192.168.1.0

Passive Interfaces

Global passive: Configure all the interfaces as passive globally. This setting will override the individual

Interface	Passive
inside	<input type="checkbox"/>
dmz	<input type="checkbox"/>

2. [Apply] をクリックします。
3. [Configuration] > [Device Setup] > [Routing] > [OSPF] > [Redistribution] > [Add] を選択して、RIP ルートを OSPF に再配布します。

Configuration > Device Setup > Routing > OSPF > Redistribution

Define the conditions for redistributing routes from one OSPF process to another.

OSPF Process	Protocol	Match	Subnets	Metric Value	Metric Type

4. [OK] をクリックして、[Apply] をクリックします。

Add OSPF Redistribution Entry

OSPF Process: 1

Protocol: Static Connected OSPF **RIP** EIGRP

Optional

Match

Internal External 1 External 2 NSSA External 1 NSSA External 2

Metric Value: Metric Type: 2 Tag Value: **Use subnets**

Route Map:

OK Cancel Help

同等の CLI 設定

RIP を OSPF AS に再配布するための ASA の CLI 設定

```
router ospf 1
 network 10.1.1.0 255.255.255.0 area 0
 log-adj-changes
 redistribute rip subnets router rip network 192.168.1.0
```

RIP ルートを OSPF AS に再配布したら、ネイバー IOS ルータ (R2) のルーティング テーブルを参照できます。

```
R2#show ip route Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D -
EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 -
OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP i - IS-
IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * -
candidate default, U - per-user static route o - ODR, P - periodic downloaded static route
Gateway of last resort is not set 172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks O
172.16.10.1/32 [110/11] via 172.16.1.2, 01:17:29, Ethernet1 O 172.16.5.1/32 [110/65] via
172.16.2.2, 01:17:29, Serial1 C 172.16.1.0/24 is directly connected, Ethernet1 C 172.16.2.0/24
is directly connected, Serial1 10.0.0.0/24 is subnetted, 1 subnets C 10.1.1.0 is directly
connected, Ethernet0 O E2 192.168.1.0/24 [110/20] via 10.1.1.1, 01:17:29, Ethernet0 !---
Redistributed route adversted by Cisco ASA
```

確認

設定を確認するには、次の手順を実行します。

1. ASDM で、[Monitoring] > [Routing] > [OSPF Neighbors] に移動し、各 OSPF ネイバーを確認できます。この図は、アクティブ ネイバーとしての内部ルータ (R2) を示しています。このネイバーが常駐するインターフェイス、ネイバー ルータ ID、状態、デッド タイムも確認できます。

Monitoring > Routing > OSPF Neighbors

OSPF Neighbors

Each row represents one OSPF Neighbor. Please click the help button for a description of the states.

Neighbor	Priority	State	Dead Time	Address	Interface
172.16.2.1	1	FULL/BDR	0:00:34	10.1.1.2	inside

Last Updated: 5/19/08 3:55:10 PM

2. また、[Monitoring] > [Routing] > [Routes] に移動して、ルーティング テーブルを確認できます。この図では、the 172.16.1.0/24、172.16.2.0/24、172.16.5.0/24 および 172.16.10.0/24 ネットワークが、R2 (10.1.1.2) を介して学習されます。

Monitoring > Routing > Routes

Routes

Each row represents one route. AD is the administrative distance.

Protocol	Type	Destination IP	Netmask	Gateway	Int
OSPF	-	172.16.10.1	255.255.255.255	10.1.1.2	inside
OSPF	-	172.16.5.1	255.255.255.255	10.1.1.2	inside
OSPF	-	172.16.1.0	255.255.255.0	10.1.1.2	inside
OSPF	-	172.16.2.0	255.255.255.0	10.1.1.2	inside
CONNECTED	-	10.1.1.0	255.255.255.0	-	inside
CONNECTED	-	10.77.241.128	255.255.255.192	-	dmz
STATIC	-	10.77.0.0	255.255.0.0	10.77.241.129	dmz
CONNECTED	-	192.168.1.0	255.255.255.0	-	outside
STATIC	DEFAULT	0.0.0.0	0.0.0.0	192.168.1.1	outside

3. CLI から、**show route** コマンドを使用して、同じ出力を取得できます。ciscoasa#show route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area * - candidate default, U - per-user static route, o - ODR P - periodic downloaded static route Gateway of last resort is 192.168.1.1 to network 0.0.0.0 O 172.16.10.1 255.255.255.255 [110/21] via 10.1.1.2, 0:00:06, inside O 172.16.5.1 255.255.255.255 [110/75] via 10.1.1.2, 0:00:06, inside O 172.16.1.0 255.255.255.0 [110/20] via 10.1.1.2, 0:00:06, inside O 172.16.2.0 255.255.255.0 [110/74] via 10.1.1.2, 0:00:06, inside C 10.1.1.0 255.255.255.0 is directly connected, inside C 10.77.241.128 255.255.255.192 is directly connected, dmz S 10.77.0.0 255.255.0.0 [1/0] via 10.77.241.129, dmz C 192.168.1.0 255.255.255.0 is directly connected, outside S* 0.0.0.0 0.0.0.0 [1/0] via 192.168.1.1, outside
4. また、**show ospf database** コマンドを使用して、学習したネットワークおよび ospf トポロジに関する情報を取得することもできます。ciscoasa#show ospf database OSPF Router with ID (192.168.1.2) (Process ID 1) Router Link States (Area 0) Link ID ADV Router Age Seq# Checksum Link count 172.16.1.2 172.16.1.2 123 0x80000039 0xfd1d 2 172.16.2.1 172.16.2.1 775 0x8000003c 0x9b42 4 172.16.5.1 172.16.5.1 308 0x80000038 0xb91b 3 192.168.1.2 192.168.1.2 1038 0x80000037 0x29d7 1 Net Link States (Area 0) Link ID ADV Router Age Seq# Checksum 10.1.1.1 192.168.1.2 1038 0x80000034 0x72ee 172.16.1.1 172.16.2.1 282 0x80000036 0x9e68
5. **show ospf neighbors** コマンドは、アクティブ ネイバーおよび対応情報の確認にも役に立ちます。この例では、手順 1 で ASDM から取得した情報と同じ情報を示します。
ciscoasa#show ospf neighbor Neighbor ID Pri State Dead Time Address Interface 172.16.2.1 1 FULL/BDR 0:00:36 10.1.1.2 inside

トラブルシューティング

このセクションでは、OSPF 問題のトラブルシューティングに役に立つ情報を提供します。

ポイントツーポイント ネットワーク向けのスタティック ネイバー設定

ASA で OSPF ネットワークをポイントツーポイント 非ブロードキャストとして設定している場合、スタティック OSPF ネイバーを定義して、ポイントツーポイント非ブロードキャスト ネットワーク上で OSPF ルートをアドバタイズする必要があります。詳細については、『[スタティック OSPF ネイバーの定義](#)』を参照してください。

トラブルシューティングのためのコマンド

[Output Interpreter Tool](#) (OIT) ([登録ユーザ専用](#)) では、特定の **show** コマンドがサポートされています。OIT を使用して、**show** コマンド出力の解析を表示できます。

注: [debug](#) コマンドを使用する前に、『[debug コマンドの重要な情報](#)』を参照してください。

- **debug ospf events** : OSPF イベントのデバッグをイネーブルにします。

```
ciscoasa(config)#debug ospf events OSPF events debugging is on ciscoasa(config)# int e0/1
ciscoasa(config-if)# no shu ciscoasa(config-if)# OSPF: Interface inside going Up OSPF: Send
with youngest Key 1 OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2 OSPF: 2 Way
Communication to 172.16.2.1 on inside, state 2WAY OSPF: Backup seen Event before WAIT timer
on inside OSPF: DR/BDR election on inside OSPF: Elect BDR 172.16.2.1 OSPF: Elect DR
172.16.2.1 DR: 172.16.2.1 (Id) BDR: 172.16.2.1 (Id) OSPF: Send DBD to 172.16.2.1 on inside
seq 0xlabd opt 0x2 flag 0x7 len 32 OSPF: Send with youngest Key 1 OSPF: End of hello
processing OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2 OSPF: End of hello
processing OSPF: Rcv DBD from 172.16.2.1 on inside seq 0x12f3 opt 0x42 flag 0x7 len 32 mtu
1500 state EXSTART OSPF: First DBD and we are not SLAVE OSPF: Rcv DBD from 172.16.2.1 on
inside seq 0xlabd opt 0x42 flag 0x2 len 152 mt u 1500 state EXSTART OSPF: NBR Negotiation
Done. We are the MASTER OSPF: Send DBD to 172.16.2.1 on inside seq 0xlabe opt 0x2 flag 0x3
len 132 OSPF: Send with youngest Key 1 OSPF: Send with youngest Key 1 OSPF: Database request
to 172.16.2.1 OSPF: sent LS REQ packet to 10.1.1.2, length 12 OSPF: Rcv DBD from 172.16.2.1
on inside seq 0xlabe opt 0x42 flag 0x0 len 32 mtu 1500 state EXCHANGE OSPF: Send DBD to
172.16.2.1 on inside seq 0xlabf opt 0x2 flag 0x1 len 32 OSPF: Send with youngest Key 1 OSPF:
Send with youngest Key 1 OSPF: Rcv DBD from 172.16.2.1 on inside seq 0xlabf opt 0x42 flag
0x0 len 32 mtu 1500 state EXCHANGE OSPF: Exchange Done with 172.16.2.1 on inside OSPF:
Synchronized with 172.16.2.1 on inside, state FULL OSPF: Send with youngest Key 1 OSPF: Send
with youngest Key 1 OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2 OSPF:
Neighbor change Event on interface inside OSPF: DR/BDR election on inside OSPF: Elect BDR
192.168.1.2 OSPF: Elect DR 172.16.2.1 OSPF: Elect BDR 192.168.1.2 OSPF: Elect DR 172.16.2.1
DR: 172.16.2.1 (Id) BDR: 192.168.1.2 (Id) OSPF: End of hello processing OSPF: Send with
youngest Key 1 OSPF: Send with youngest Key 1 OSPF: Send with youngest Key 1 OSPF: Send with
youngest Key 1 OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2 OSPF: End of
hello processing OSPF: Send with youngest Key 1 OSPF: Rcv hello from 172.16.2.1 area 0 from
inside 10.1.1.2 OSPF: End of hello processing OSPF: Send with youngest Key 1 OSPF: Rcv hello
from 172.16.2.1 area 0 from inside 10.1.1.2 OSPF: End of hello processing OSPF: Send with
youngest Key 1 OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2 OSPF: End of
hello processing
```

注: 問題のトラブルシューティングに役に立つさまざまなコマンドの詳細については、『Cisco Security Appliance Command Reference, Version 8.0』の [debug ospf](#) に関するセクションを参照してください。

関連情報

- [Cisco 5500 シリーズ 適応型セキュリティ アプライアンスに関するサポート ページ](#)
- [Cisco 500 シリーズ PIX に関するサポート ページ](#)
- [PIX/ASA 8.X : Cisco 適応型セキュリティ アプライアンス \(ASA \) の EIGRP の設定](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)