RIP による ASA/PIX の設定例

目次

概要

このドキュメントでは、Routing Information Protocol（RIP）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: このドキュメントの設定は、RIP バージョン 2 に基づきます。

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。
- RIP 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

RIP は、ホップ カウントをメトリックとして使用するディスタンスベクトル ルーティング プロトコルです。 RIP がインターフェイス上でイネーブルの場合、そのインターフェイスは、ネイバー デバイスと RIP ブロードキャストを交換して、ルートの動的な学習およびアドバタイズを行います。

セキュリティ アプライアンスは、RIP バージョン 1 と RIP バージョン 2 の両方をサポートします。 RIP バージョン 1 は、ルーティング更新でサブネット マスクを送信しません。 RIP バージョン 2 は、ルーティング更新でサブネット マスクを送信し、変数長サブネット マスクをサポートします。 また、RIP バージョン 2 では、ルーティング更新の交換時にネイバー認証がサポートされます。 この認証によって、セキュリティ アプライアンスは信頼できるソースから信頼できるルーティング情報を受信します。

制限事項：

1. セキュリティ アプライアンスは、インターフェイス間で RIP アップデートを渡すことはできません。
2. RIP バージョン 1 では、可変長サブネット マスク（VLSM）がサポートされていません。
3. RIP の最大ホップ カウントは 15 です。 ホップ カウントが 15 を超えるルートは、到達不能と見なされます。
4. RIP の収束は、他のルーティング プロトコルと比べて時間がかかります。
5. セキュリティ アプライアンスでは、RIP プロセスを 1 つだけイネーブルにできます。

注: この情報は、RIP バージョン 2 だけに適用されます。

1. ネイバー認証を使用する場合、認証キーとキー ID は、RIP バージョン 2 アップデートをインターフェイスに提供するすべてのネイバー デバイスで同じである必要があります。
2. RIP バージョン 2 では、セキュリティ アプライアンスは、マルチキャスト アドレス

224.0.0.9 を使用してデフォルト ルート アップデートを送受信します。 パッシブ モードでは、そのアドレスでルート アップデートが受信されます。

3. RIP バージョン 2 がインターフェイスで設定されている場合、マルチキャスト アドレス 224.0.0.9 がそのインターフェイス上に登録されます。 RIP バージョン 2 構成がインターフェイスから削除されると、そのマルチキャスト アドレスは登録解除されます。

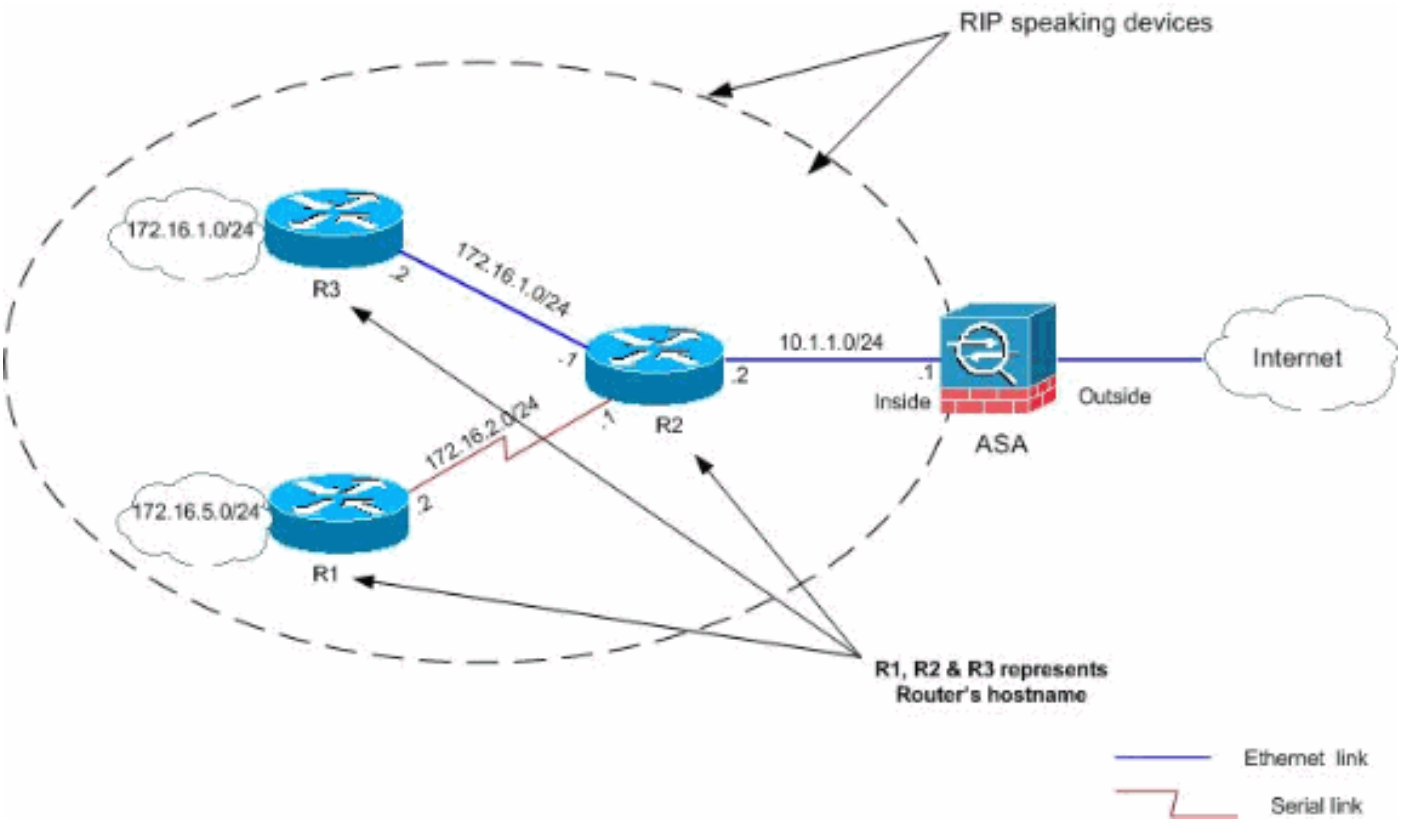
設定

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。



設定

このドキュメントでは、次の設定を使用します。

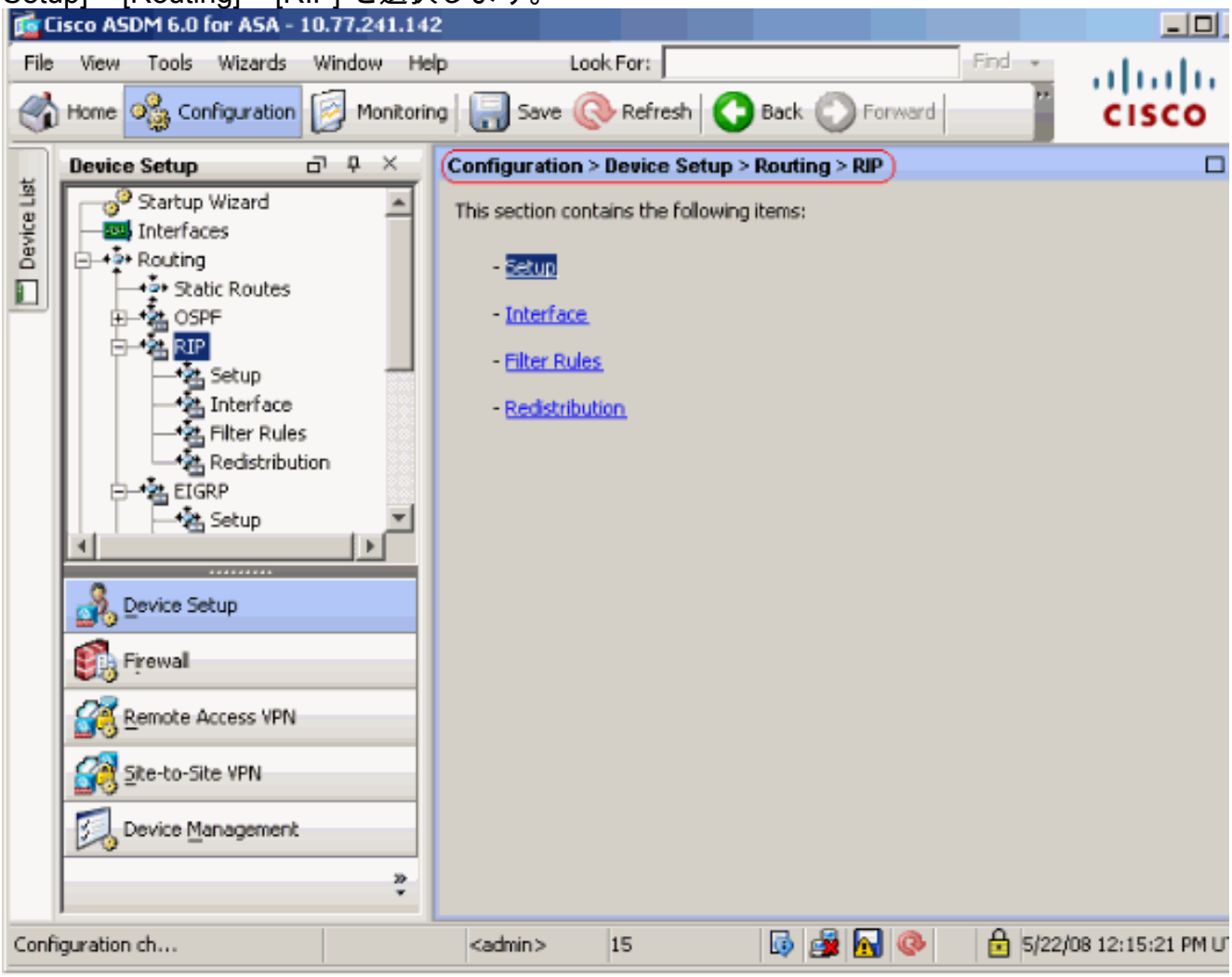
- ASDM の設定
- RIP 認証の設定
- Cisco ASA CLI 設定
- Cisco IOS ルータ（R2）CLI 設定
- Cisco IOS ルータ（R1）CLI 設定
- Cisco IOS ルータ（R3）CLI 設定

ASDM の設定

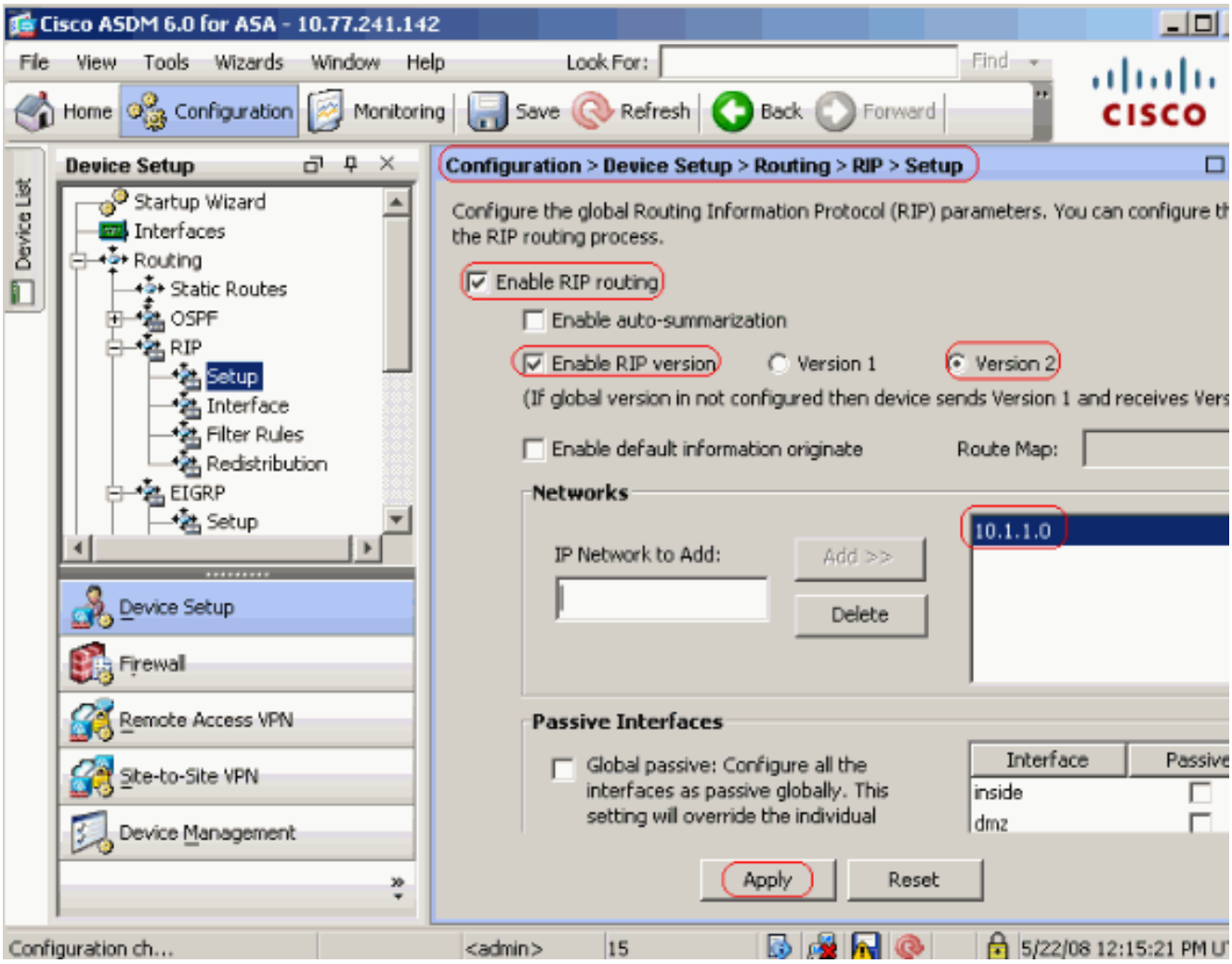
Adaptive Security Device Manager（ASDM）は、セキュリティ アプライアンスのソフトウェアの設定およびモニタに使用されるブラウザベースのアプリケーションです。 ASDM は、セキュリティ アプライアンスからロードされ、デバイスの設定、モニタ、管理に使用されます。 また ASDM アプリケーションを Javaアプレットより速く起動させるために ASDM ランチャー（Windows® だけ）を使用できます。 ここでは、この ASDM のマニュアルで説明する機能を設定する際に必要な情報を説明します。

Cisco ASA で RIP 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. スクリーンショットに示すように、ASDM インターフェイスで [Configuration] > [Device Setup] > [Routing] > [RIP] を選択します。



3. RIP ルーティングをイネーブルにするには、次に示すように、[Configuration] > [Device Setup] > [Routing] > [RIP] > [Setup] を選択します。[Enable RIP routing] チェック ボックスをオンにします。[Enable RIP version] チェック ボックスをオンにして、[Version 2] ラジオ ボタンを選択します。[Networks] タブで、ネットワーク **10.1.1.0** を追加します。[Apply] をクリックします。



フィールド[Enable RIP Routing]：セキュリティ アプライアンスでの RIP ルーティング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。 RIP をイネーブルにすると、すべてのインターフェイス上でイネーブルになります。 また、このチェック ボックスをオンにすると、このペインの他のフィールドもイネーブルになります。 セキュリティ アプライアンスでの RIP ルーティングをディセーブルにするには、このチェック ボックスをオフにします。[Enable Auto-summarization]：自動ルート集約をディセーブルにするには、このチェック ボックスをオフにします。 自動ルート集約を再度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。 RIP バージョン 1 では、常に自動集約が使用されます。 RIP バージョン 1 に対して自動集約をディセーブルにすることはできません。 RIP バージョン 2 を使用している場合は、このチェック ボックスをオフにすれば自動集約をオフにできます。 切断されているサブネット間のルーティングを実行する必要がある場合は、自動サマライズをディセーブルにします。 自動サマライズをディセーブルにすると、サブネットがアドバタイズされます。[Enable RIP version]：セキュリティ アプライアンスが使用する RIP のバージョンを指定するには、このチェック ボックスをオンにします。 このチェック ボックスがオフの場合、セキュリティ アプライアンスは RIP バージョン 1 のアップデートを送信し、RIP バージョン 1 およびバージョン 2 のアップデートを受け入れます。 これよりも優先する設定を、インターフェイスごとに [Interface] ペインで指定できます。[Version 1]：セキュリティ アプライアンスが RIP バージョン 1 のアップデートだけを送信および受信するように指定します。 受信されたバージョン 2 更新はドロップされます。[Version 2]：セキュリティ アプライアンスが RIP バージョン 2 のアップデートだけを送信および受信するように指定します。 受信されたバージョン 1 更新はドロップされます。[Enable default information originate]：RIP ルーティング プロセスにデフォルト ルートを生成するには、このチェック ボックスをオンにします。 デフォルト ルートの生成前に満たす必要のあるルート マップを設定できます。[Route-map]：適用するルート マップの名前を入

力します。 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。[IP Network to Add]：RIP ルーティング プロセスのネットワークを定義します。 指定されたネットワーク番号は、サブネット情報に含めないでください。 セキュリティ アプライアンスの設定に追加できるネットワーク数に制限はありません。 指定されたネットワーク上のインターフェイスのみを経由して、RIP ルーティング アップデートが送受信されます。 また、インターフェイスのネットワークを指定しない場合、インターフェイスは RIP アップデートでアドバタイズされません。[Add]：指定したネットワークをネットワークのリストに追加するには、このボタンをクリックします。[Delete]：選択したネットワークをネットワークのリストから削除するには、このボタンをクリックします。
[Configure interfaces as passive globally]：セキュリティ アプライアンス上のすべてのインターフェイスをパッシブ RIP モードに設定するには、このチェック ボックスをオンにします。 セキュリティ アプライアンスはすべてのインターフェイス上の RIP ルーティング ブロードキャストをリッスンし、その情報を使用してルーティング テーブルを取り込みますが、ルーティング アップデートをブロードキャストすることはありません。 特定のインターフェイスをパッシブ RIP に設定するには、[Passive Interfaces] テーブルを使用します。
[Passive Interface] テーブル：セキュリティ アプライアンスで設定されたインターフェイスの一覧を示します。 パッシブ モードで操作するインターフェイスの [Passive] カラムにあるチェックボックスをオンにします。 他のインターフェイスは、引き続き RIP ブロードキャストを送信および受信します。

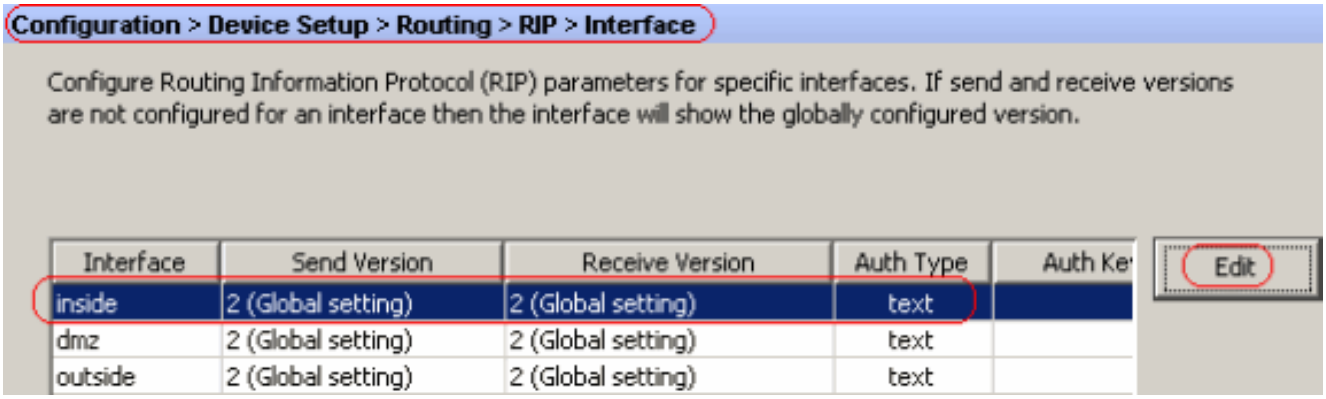
RIP 認証の設定

Cisco ASA は、RIP v2 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 RIP 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 RIP 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、DoS 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 RIP 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。

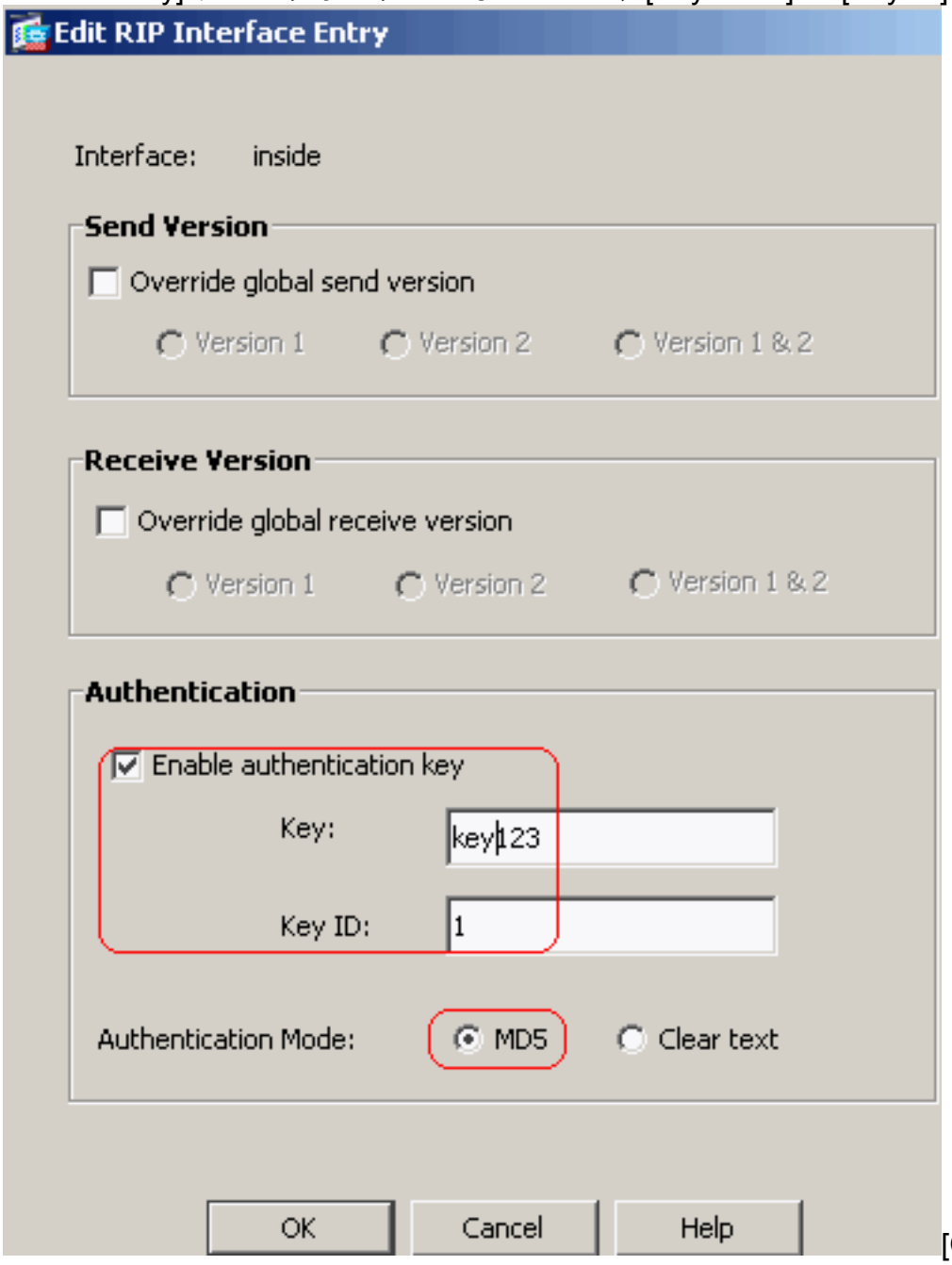
RIP ルート認証は、インターフェイスごとに設定します。 RIP メッセージ認証対象として設定されたインターフェイス上にあるすべての RIP ネイバーには、同じ認証モードとキーを設定する必要があります。

Cisco ASA で RIP 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] > [RIP] > [Interface] を選択し、マウスで内部インターフェイスを選択します。 [Edit] をクリックします。



2. [Enable authentication key] チェックボックスをオンにして、[Key value] と [Key ID] の値を



入力します。[OK] をクリックし、次に [Apply] をクリックします。

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 !--- RIP authentication is configured
on the inside interface. rip authentication mode md5 rip
authentication key <removed> key_id 1 ! !--- Output
Suppressed !--- Outside interface configuration interface
Ethernet0/2 nameif outside security-level 0 ip address
192.168.1.2 255.255.255.0 !--- RIP Configuration router rip
network 10.0.0.0 version 2 !--- This is the static default
gateway configuration in !--- order to reach the Internet.
route outside 0.0.0.0 0.0.0.0 192.168.1.1 1
```

Cisco IOS ルータ (R2) CLI 設定

Cisco IOS ルータ (R2)

```
interface Ethernet0
 ip address 10.1.1.2 255.255.255.0
 ip rip authentication mode md5 ip rip authentication key-
chain 1 ! router rip version 2 network 10.0.0.0 network
172.16.0.0 no auto-summary
```

Cisco IOS ルータ (R1) CLI 設定

Cisco IOS ルータ (R1)

```
router rip version 2 network 172.16.0.0 no auto-summary
```

Cisco IOS ルータ (R3) CLI 設定

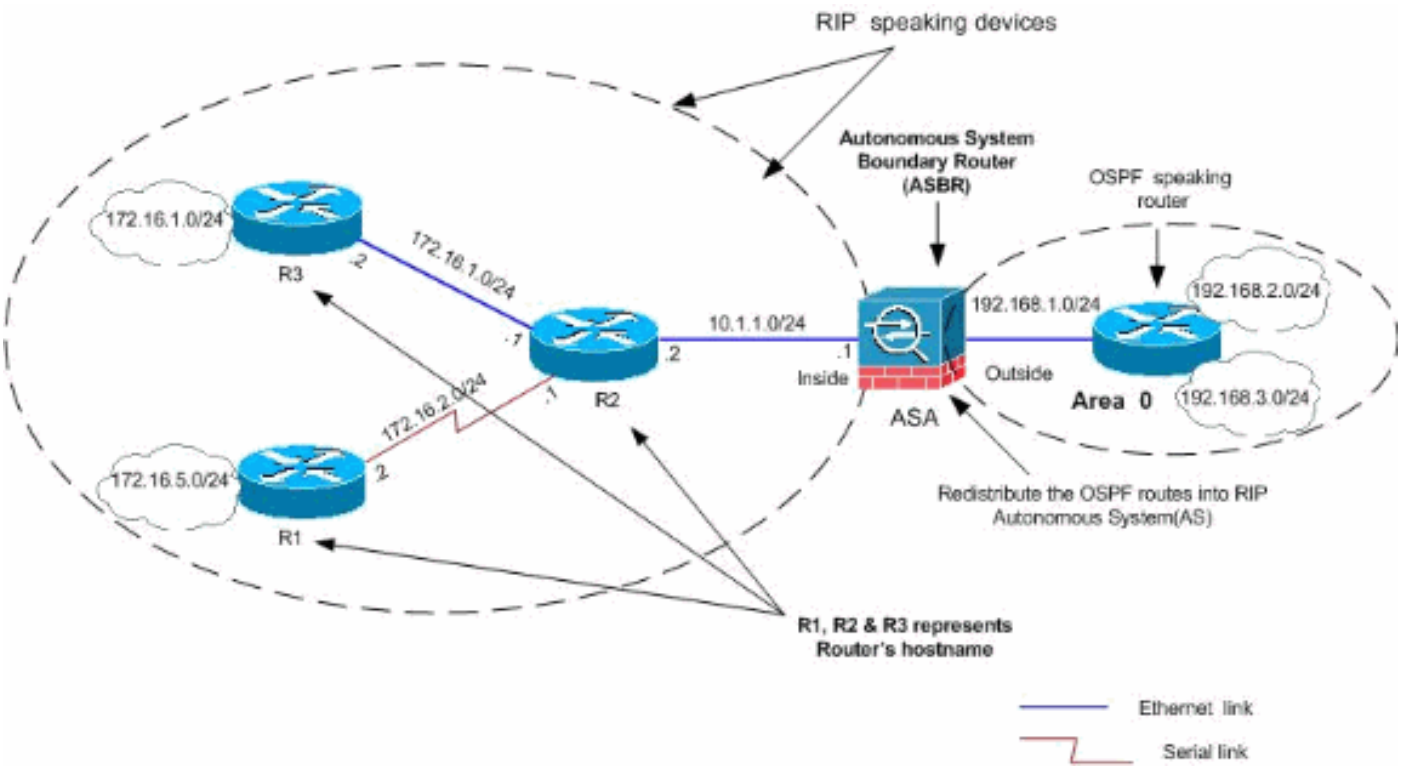
Cisco IOS ルータ (R3)

```
router rip version 2 network 172.16.0.0 no auto-summary
```

ASA を使用した RIP への再配布

OSPF ルーティング プロセス、EIGRP ルーティング プロセス、スタティック ルーティング プロセス、および接続されているルーティング プロセスからルートを RIP ルーティング プロセスに再配布できます。

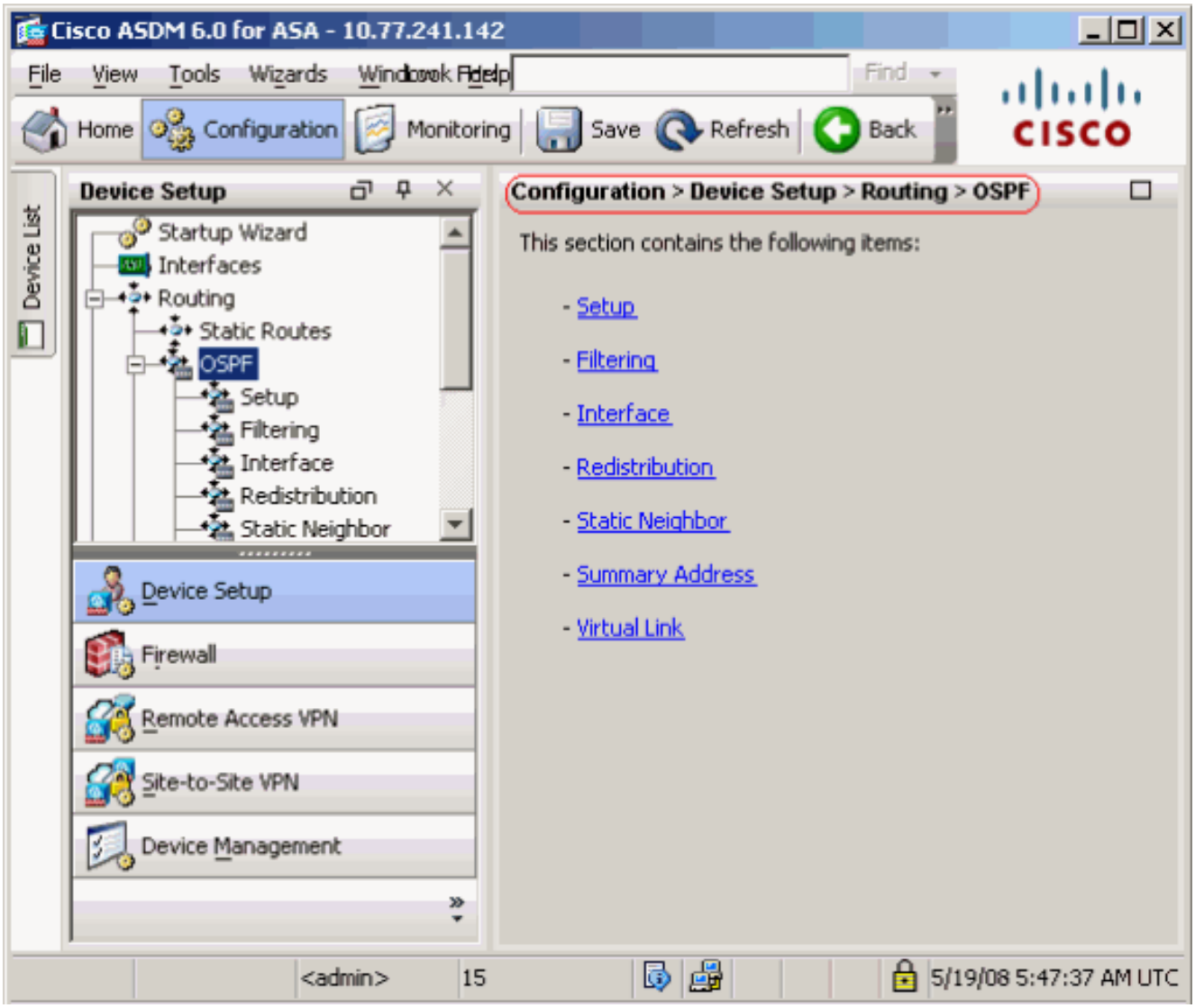
この例では、OSPF ルートの RIP への再配布をネットワーク図で示します。



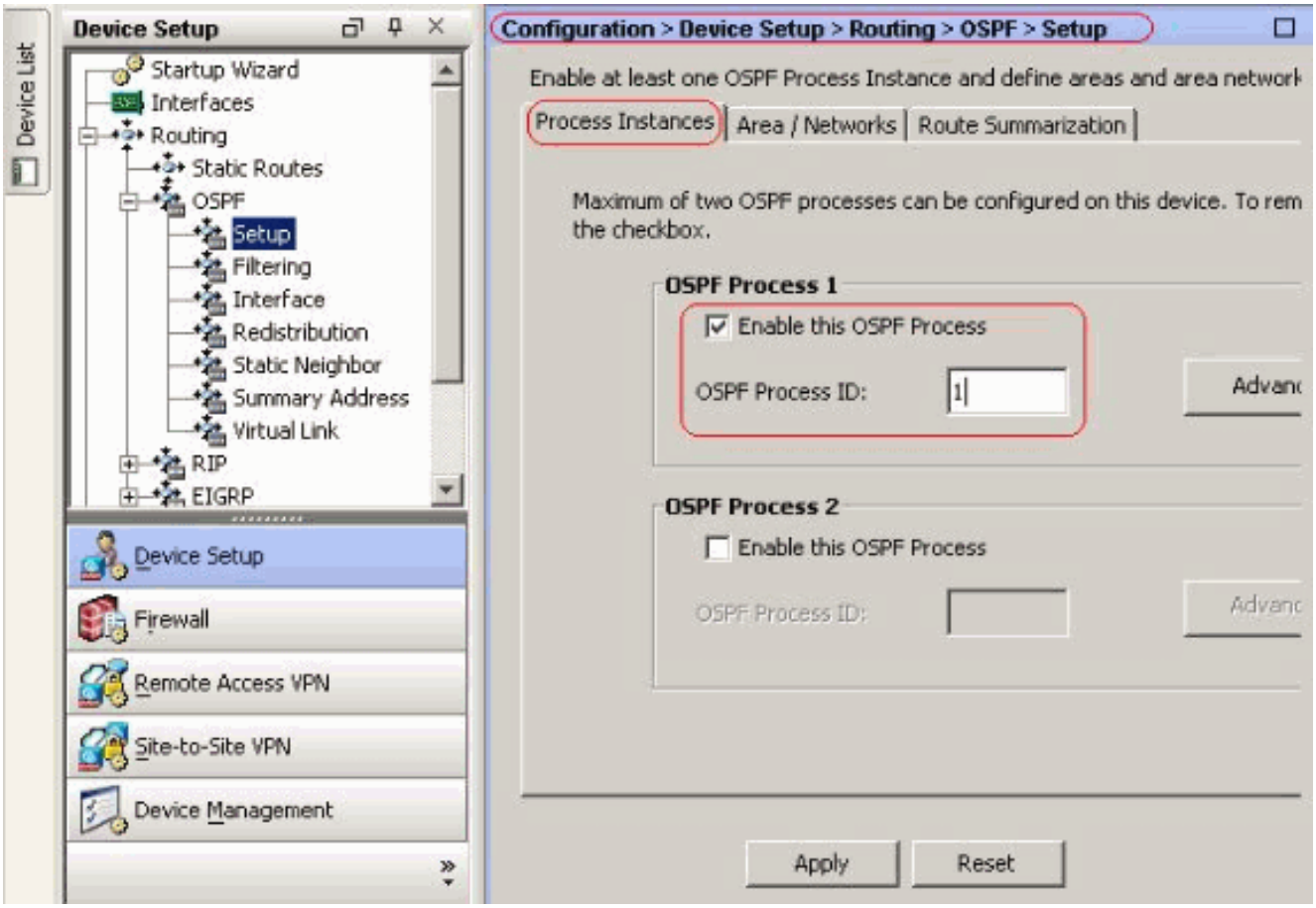
ASDM の設定

次の手順を実行します。

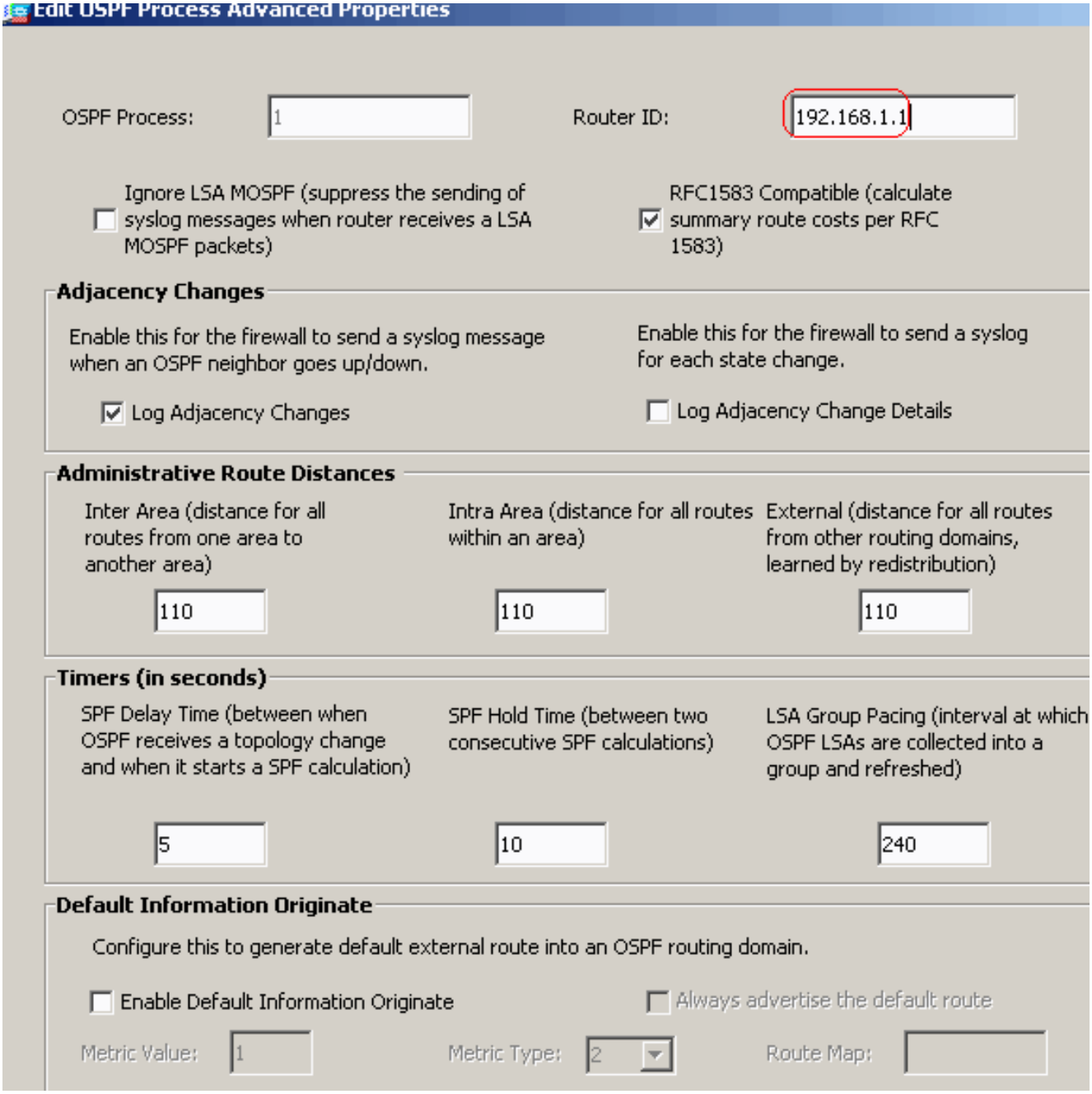
1. **OSPF 設定**スクリーンショットに示すように、ASDM インターフェイスで [Configuration] > [Device Setup] > [Routing] > [OSPF] を選択します。



スクリーンショットに示すように、[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。



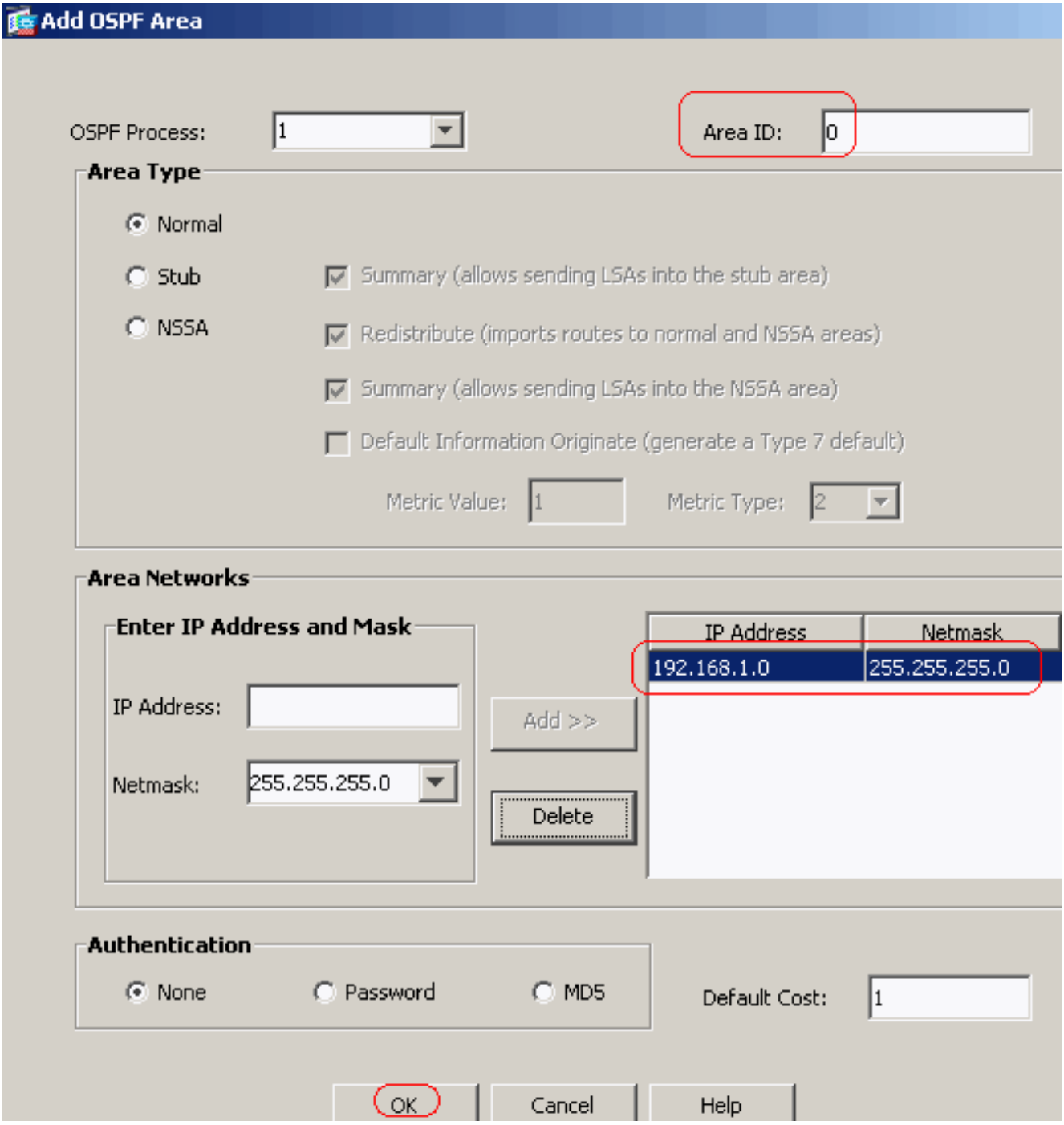
オプションの高度な OSPF ルーティング プロセス パラメータを設定するには、[Setup] > [Process Instances] タブで [Advanced] をクリックします。 [Router ID]、[Adjacency Changes]、[Administrative Route Distances]、[Timers] および [Default Information Originate] 設定など、プロセス固有の設定を編集できます。



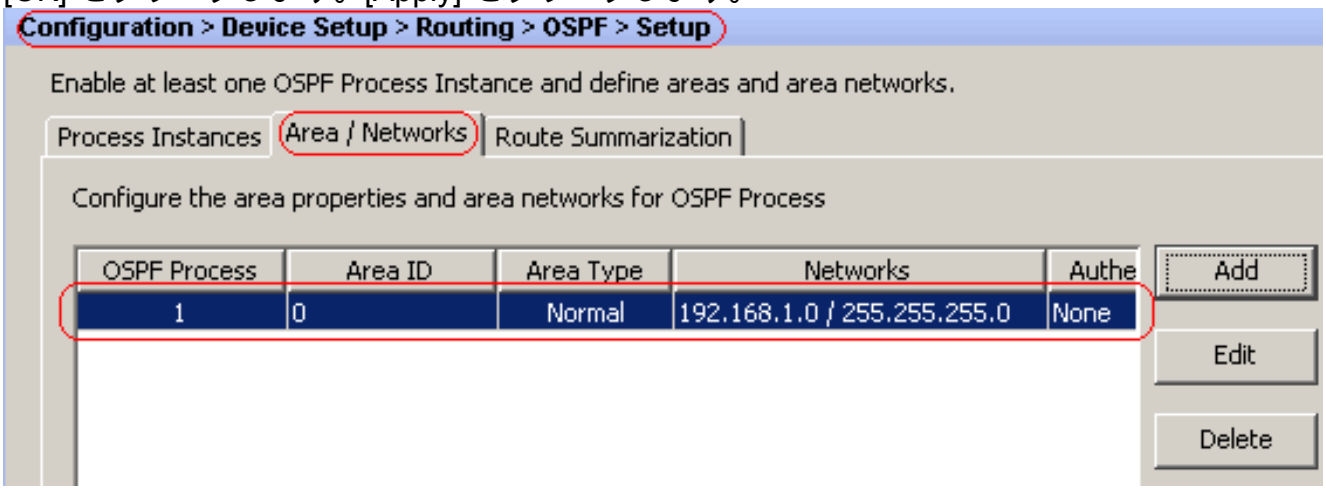
[OK] をクリックします。これまでの手順を完了したら、[Setup] > [Area/Networks] タブで OSPF ルーティングに参加するネットワークおよびインターフェイスを定義します。 このスクリーンショットに示すように、[Add] をクリックします。

次の画面が表示されます。 この例では、OSPF が外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、追加するネットワークは外部ネットワーク（192.168.1.0/24）だけです

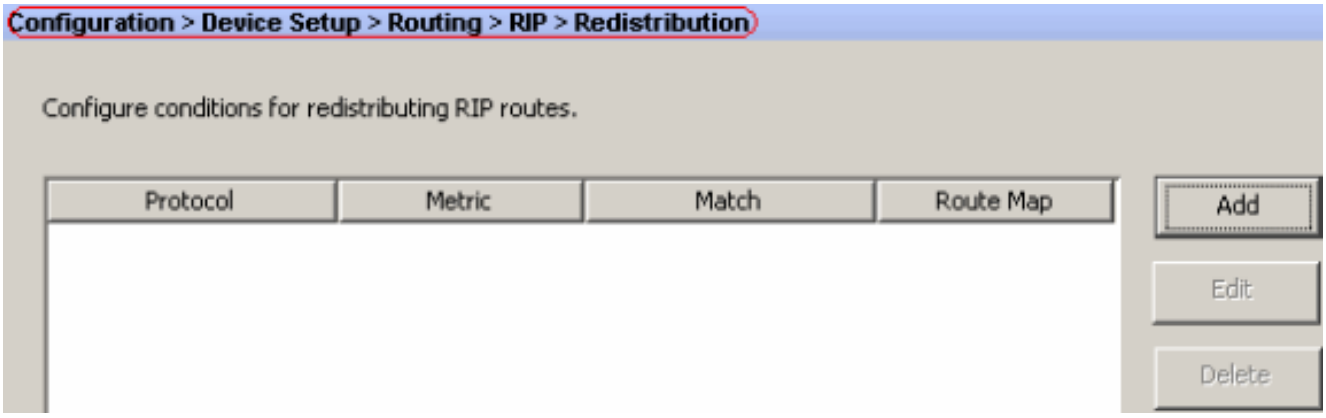
。**注:** IP アドレスが定義済みネットワークの範囲内にあるインターフェイスだけが、OSPF ルーティング プロセスに参加します。



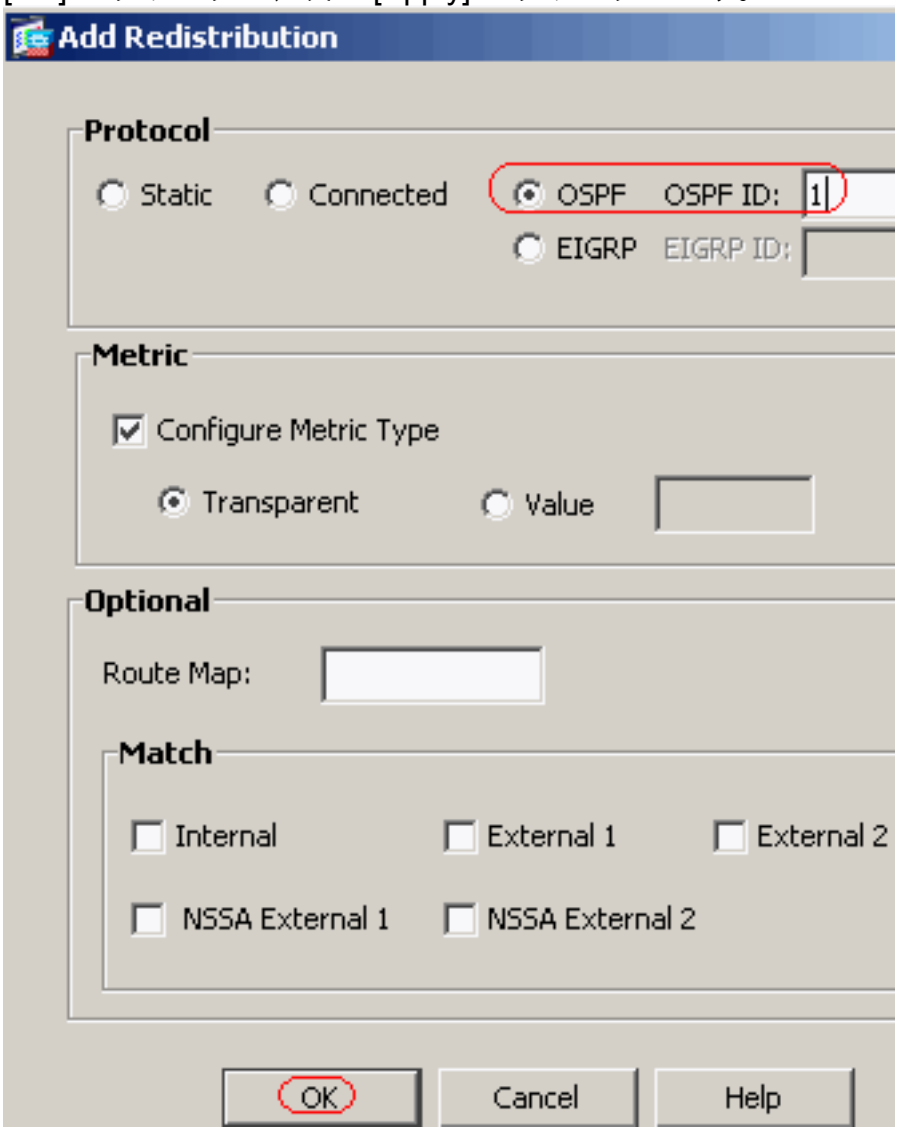
[OK] をクリックします。[Apply] をクリックします。



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



3. [OK] をクリックし、次に [Apply] をクリックします。



同等の CLI 設定

OSPF を RIP AS に再配布するための ASA の CLI 設定
router rip network 10.0.0.0 **redistribute ospf 1 metric transparent** version 2 ! router ospf 1 router-id 192.168.1.1 network 192.168.1.0 255.255.255.0 area 0 area 0 log-adj-changes

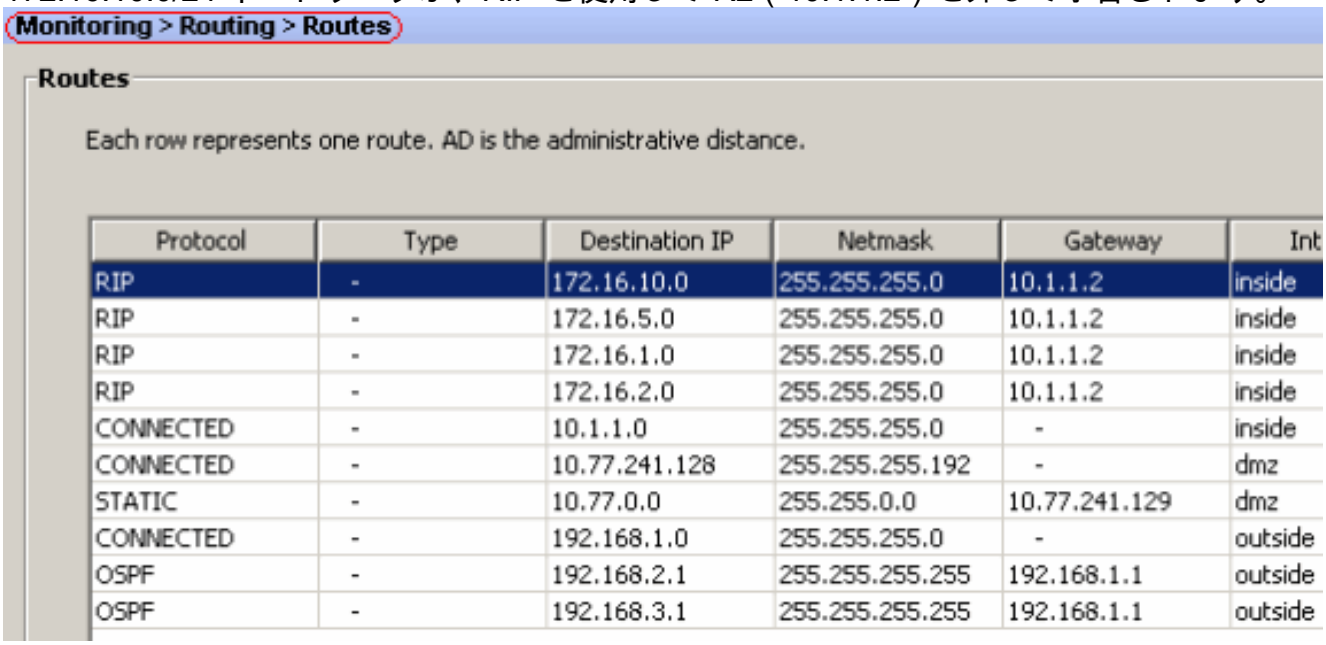
OSPF ルートを RIP AS に再配布したら、ネイバー Cisco IOS ルータ（R2）のルーティング テーブルを参照できます。

```
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 172.16.0.0/24 is subnetted, 4 subnets R 172.16.10.0 [120/1] via 172.16.1.2, 00:00:25, Ethernet1 R 172.16.5.0 [120/1] via 172.16.2.2, 00:00:20, Serial1 C 172.16.1.0 is directly connected, Ethernet1 C 172.16.2.0 is directly connected, Serial1 10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks C 10.1.1.0/24 is directly connected, Ethernet0 R 10.77.241.128/26 [120/1] via 10.1.1.1, 00:00:06, Ethernet0 R 192.168.1.0/24 [120/1] via 10.1.1.1, 00:00:05, Ethernet0 192.168.2.0/32 is subnetted, 1 subnets R 192.168.2.1 [120/12] via 10.1.1.1, 00:00:05, Ethernet0 192.168.3.0/32 is subnetted, 1 subnets R 192.168.3.1 [120/12] via 10.1.1.1, 00:00:05, Ethernet0 !--- Redistributed route advertised 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. [Monitoring] > [Routing] > [Routes] に移動して、ルーティング テーブルを検証できます。 このスクリーンショットでは、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、RIP を使用して R2（10.1.1.2）を介して学習されます。



Protocol	Type	Destination IP	Netmask	Gateway	Int
RIP	-	172.16.10.0	255.255.255.0	10.1.1.2	inside
RIP	-	172.16.5.0	255.255.255.0	10.1.1.2	inside
RIP	-	172.16.1.0	255.255.255.0	10.1.1.2	inside
RIP	-	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
OSPF	-	192.168.2.1	255.255.255.255	192.168.1.1	outside
OSPF	-	192.168.3.1	255.255.255.255	192.168.1.1	outside

2. 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 not set R 172.16.10.0 255.255.255.0 [120/2] via 10.1.1.2, 0:00:10, inside R 172.16.5.0 255.255.255.0 [120/2] via 10.1.1.2, 0:00:10, inside R 172.16.1.0 255.255.255.0 [120/1] via 10.1.1.2, 0:00:10, inside R 172.16.2.0 255.255.255.0 [120/1] via 10.1.1.2, 0:00:10, 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 O 192.168.2.1 255.255.255.255 [110/11] via 192.168.1.1, 0:34:46, outside O 192.168.3.1 255.255.255.255 [110/11] via 192.168.1.1, 0:34:46, outside ciscoasa#
```

トラブルシューティング

ここでは、OSPF の問題のトラブルシューティングに役立つ debug コマンドについて説明します。

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 rip events**：RIP イベントのデバッグをイネーブルにします。
```
ciscoasa#debug rip events
rip_route_adjust for inside coming up RIP: sending request on inside to 224.0.0.9 RIP: received v2
update from 10.1.1.2 on inside 172.16.1.0255.255.255.0 via 0.0.0.0 in 1 hops 172.16.2.0255.255.255.0
via 0.0.0.0 in 1 hops 172.16.5.0255.255.255.0 via 0.0.0.0 in 2 hops 172.16.10.0255.255.255.0 via
0.0.0.0 in 2 hops RIP: Update contains 4 routes RIP: received v2 update from 10.1.1.2 on inside
172.16.1.0255.255.255.0 via 0.0.0.0 in 1 hops 172.16.2.0255.255.255.0 via 0.0.0.0 in 1 hops
172.16.5.0255.255.255.0 via 0.0.0.0 in 2 hops 172.16.10.0255.255.255.0 via 0.0.0.0 in 2 hops RIP:
Update contains 4 routes RIP: sending v2 flash update to 224.0.0.9 via dmz (10.77.241.142) RIP: build
flash update entries 10.1.1.0 255.255.255.0 via 0.0.0.0, metric 1, tag 0 172.16.1.0 255.255.255.0 via
0.0.0.0, metric 2, tag 0 172.16.2.0 255.255.255.0 via 0.0.0.0, metric 2, tag 0 172.16.5.0
255.255.255.0 via 0.0.0.0, metric 3, tag 0 172.16.10.0 255.255.255.0 via 0.0.0.0, metric 3, tag 0
RIP: Update contains 5 routes RIP: Update queued RIP: sending v2 flash update to 224.0.0.9 via inside
(10.1.1.1) RIP: build flash update entries - suppressing null update RIP: Update sent via dmz rip-
len:112 RIP: sending v2 update to 224.0.0.9 via dmz (10.77.241.142) RIP: build update entries
10.1.1.0 255.255.255.0 via 0.0.0.0, metric 1, tag 0 172.16.1.0 255.255.255.0 via 0.0.0.0, metric 2,
tag 0 172.16.2.0 255.255.255.0 via 0.0.0.0, metric 2, tag 0 172.16.5.0 255.255.255.0 via 0.0.0.0,
metric 3, tag 0 172.16.10.0 255.255.255.0 via 0.0.0.0, metric 3, tag 0 192.168.1.0 255.255.255.0 via
0.0.0.0, metric 1, tag 0 192.168.2.1 255.255.255.255 via 0.0.0.0, metric 12, tag 0 192.168.3.1
255.255.255.255 via 0.0.0.0, metric 12, tag 0 RIP: Update contains 8 routes RIP: Update queued RIP:
sending v2 update to 224.0.0.9 via inside (10.1.1.1) RIP: build update entries 10.77.241.128
255.255.255.192 via 0.0.0.0, metric 1, tag 0 192.168.1.0 255.255.255.0 via 0.0.0.0, metric 1, tag 0
192.168.2.1 255.255.255.255 via 0.0.0.0, metric 12, tag 0 192.168.3.1 255.255.255.255 via 0.0.0.0,
metric 12, tag 0 RIP: Update contains 4 routes RIP: Update queued RIP: Update sent via dmz rip-
len:172 RIP: Update sent via inside rip-len:92 RIP: received v2 update from 10.1.1.2 on inside
172.16.1.0255.255.255.0 via 0.0.0.0 in 1 hops 172.16.2.0255.255.255.0 via 0.0.0.0 in 1 hops
172.16.5.0255.255.255.0 via 0.0.0.0 in 2 hops 172.16.10.0255.255.255.0 via 0.0.0.0 in 2 hops RIP:
Update contains 4 routes
```

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