ASA/PIX mit RIP-Konfigurationsbeispiel

Inhalt

Einführung

In diesem Dokument wird erläutert, wie die Cisco ASA so konfiguriert wird, dass Routen über das Routing Information Protocol (RIP) erfasst, authentifiziert und neu verteilt werden.

Weitere Informationen finden Sie unter PIX/ASA 8.X: Konfigurieren von EIGRP auf der Cisco Adaptive Security Appliance (ASA) für weitere Informationen zur EIGRP-Konfiguration

Hinweis: Diese Dokumentkonfiguration basiert auf RIP-Version 2.

Hinweis: Asymmetrisches Routing wird in ASA/PIX nicht unterstützt.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- Cisco ASA/PIX muss Version 7.x oder höher ausführen.
- RIP wird im Multi-Context-Modus nicht unterstützt. Es wird nur im Einzelmodus unterstützt.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Adaptive Security Appliance (ASA) der Serie 5500 mit Softwareversion 8.0 und höher
- Cisco Adaptive Security Device Manager (ASDM)-Software 6.0 und höher

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Zugehörige Produkte

Die Informationen in diesem Dokument gelten auch für die Cisco PIX-Firewall der Serie 500, die die Softwareversion 8.0 und höher ausführt.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

RIP ist ein Distanzvektor-Routing-Protokoll, das die Hop-Anzahl als Metrik für die Pfadauswahl verwendet. Wenn RIP auf einer Schnittstelle aktiviert ist, tauscht die Schnittstelle RIP-Broadcasts mit benachbarten Geräten aus, um dynamisch Informationen zu Routen zu erhalten und diese anzuzeigen.

Die Security Appliance unterstützt sowohl RIP Version 1 als auch RIP Version 2. RIP Version 1 sendet die Subnetzmaske nicht mit dem Routing-Update. RIP Version 2 sendet die Subnetzmaske mit dem Routing-Update und unterstützt Subnetzmasken mit variabler Länge. Darüber hinaus unterstützt RIP Version 2 beim Austausch von Routing-Updates die Nachbar-Authentifizierung. Diese Authentifizierung stellt sicher, dass die Security Appliance zuverlässige Routing-Informationen von einer vertrauenswürdigen Quelle erhält.

Einschränkungen:

1. Die Sicherheits-Appliance kann RIP-Updates nicht zwischen Schnittstellen übergeben.
2. RIP Version 1 unterstützt keine Subnetzmasken mit variabler Länge (VLSM).
3. RIP hat eine maximale Hop-Anzahl von 15. Eine Route mit einer Hop-Anzahl von mehr als 15 gilt als nicht erreichbar.
4. Im Vergleich zu anderen Routing-Protokollen ist die RIP-Konvergenz relativ langsam.

5. Sie können nur einen einzigen RIP-Prozess auf der Security Appliance aktivieren.

Hinweis: Diese Informationen gelten nur für RIP Version 2:

1. Wenn Sie die Nachbarauthentifizierung verwenden, müssen der Authentifizierungsschlüssel und die Schlüssel-ID auf allen Nachbargeräten identisch sein, die RIP-Version-2-Updates für die Schnittstelle bereitstellen.
2. Mit RIP Version 2 überträgt und empfängt die Sicherheits-Appliance Standard-Routen-Updates mithilfe der Multicast-Adresse 224.0.0.9. Im passiven Modus werden Routen-Updates an dieser Adresse empfangen.
3. Wenn RIP Version 2 auf einer Schnittstelle konfiguriert ist, wird die Multicast-Adresse 224.0.0.9 auf dieser Schnittstelle registriert. Wenn eine Konfiguration der RIP-Version 2 von einer Schnittstelle entfernt wird, ist diese Multicast-Adresse nicht registriert.

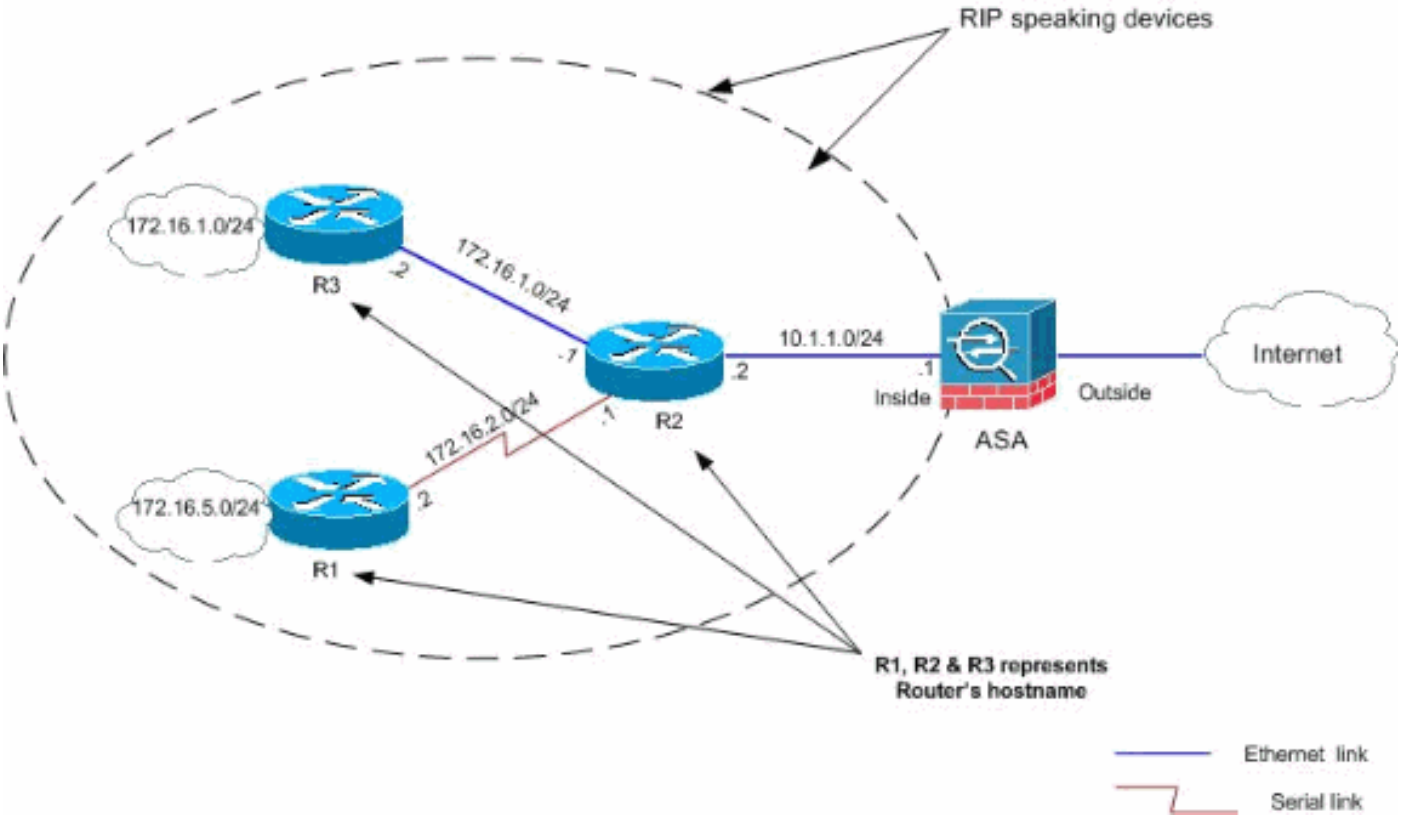
Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Konfigurationen

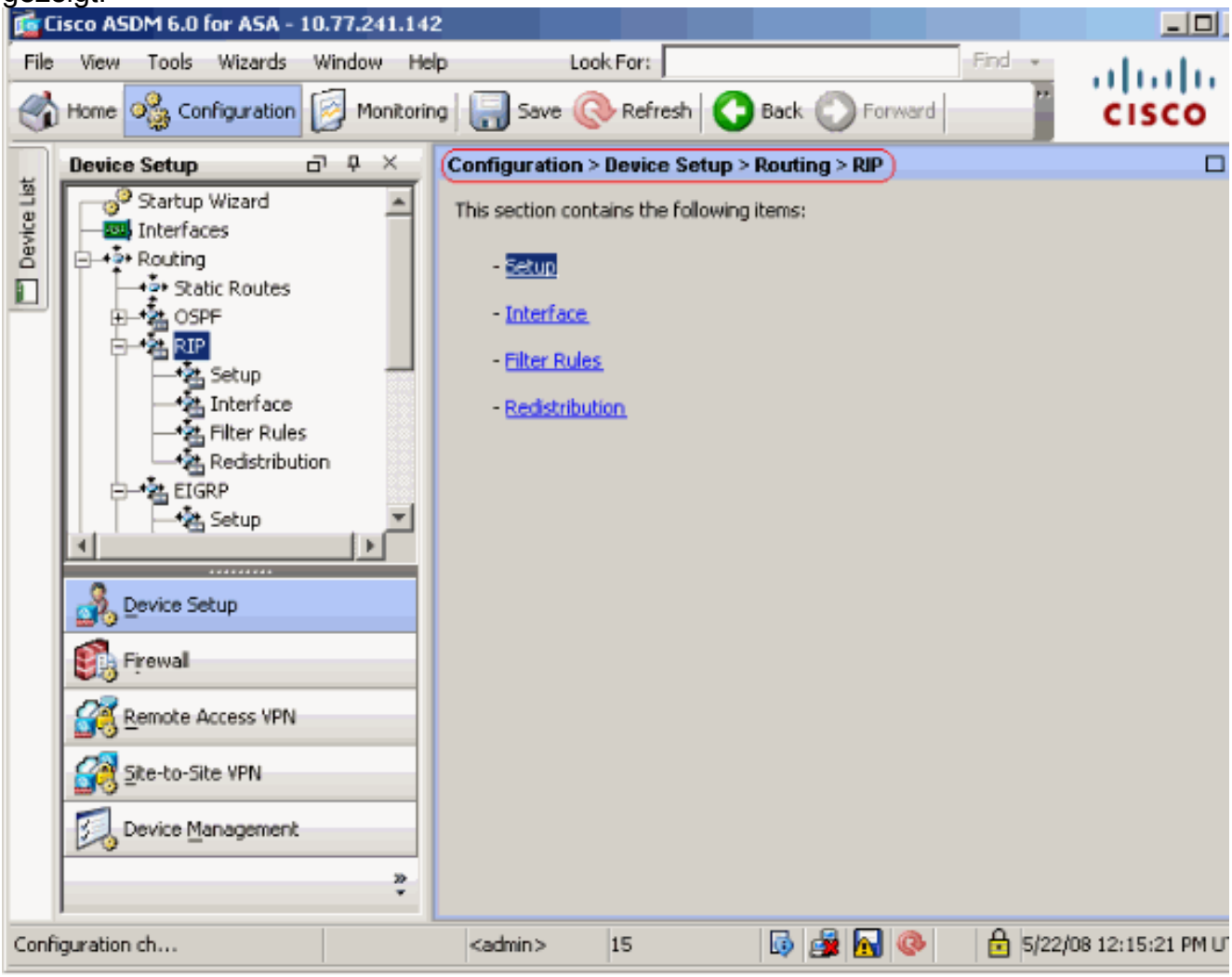
In diesem Dokument werden folgende Konfigurationen verwendet:

ASDM-Konfiguration

Adaptive Security Device Manager (ASDM) ist eine browserbasierte Anwendung zur Konfiguration und Überwachung der Software auf Sicherheitsgeräten. ASDM wird von der Sicherheits-Appliance geladen und anschließend zur Konfiguration, Überwachung und Verwaltung des Geräts verwendet. Sie können auch den ASDM Launcher (nur Windows®) verwenden, um die ASDM-Anwendung schneller als das Java-Applet zu starten. In diesem Abschnitt werden die Informationen beschrieben, die Sie benötigen, um die in diesem Dokument beschriebenen Funktionen mit ASDM zu konfigurieren.

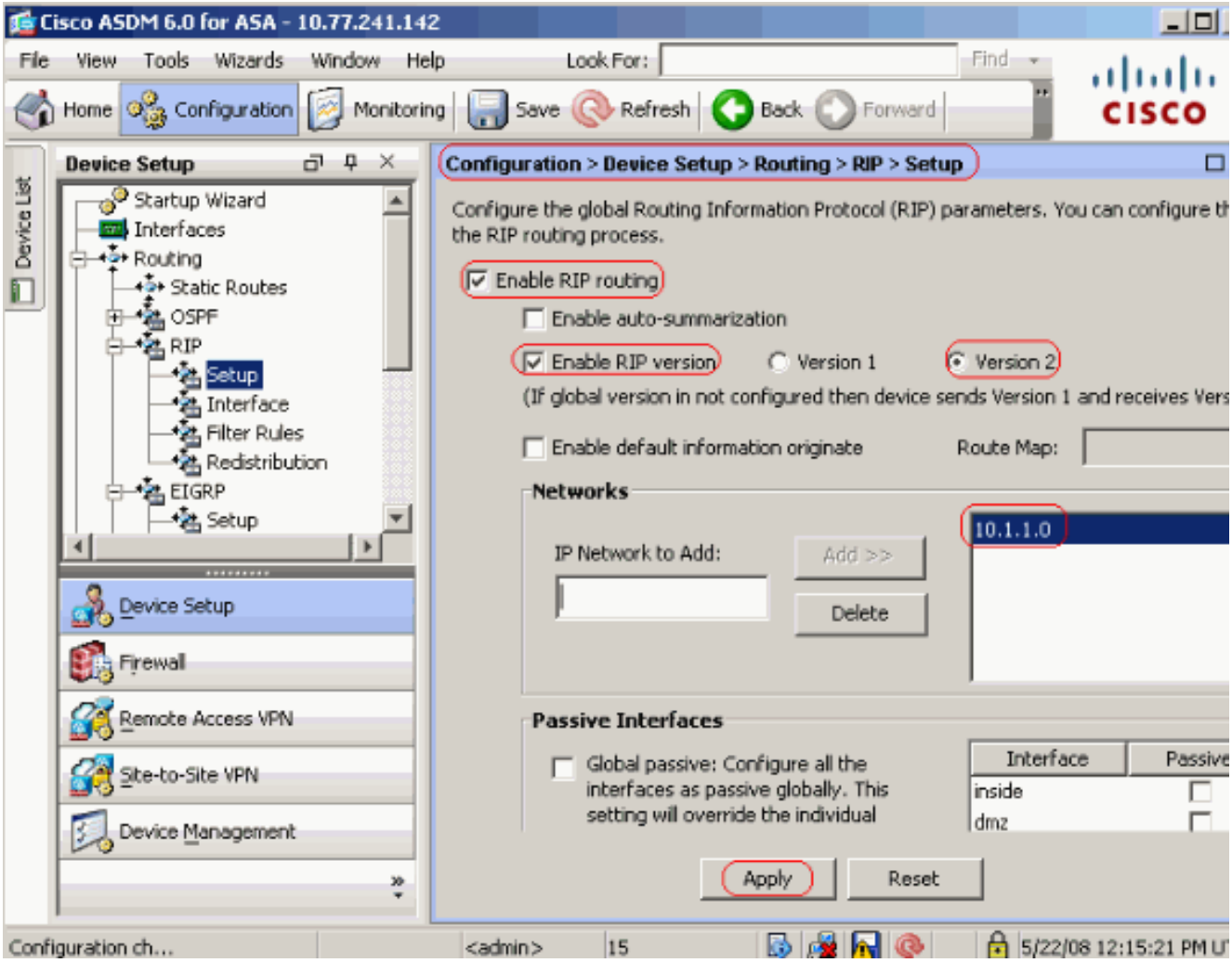
Gehen Sie wie folgt vor, um RIP in der Cisco ASA zu konfigurieren:

1. Melden Sie sich mit ASDM bei der Cisco ASA an.
2. Wählen Sie **Configuration > Device Setup > Routing > RIP** in der ASDM-Schnittstelle aus, wie im Screenshot
   gezeigt.



3. Wählen Sie **Configuration > Device Setup > Routing > RIP > Setup (Konfiguration >**

Geräteinstallation > Routing > RIP > Setup), um das RIP-Routing wie gezeigt zu aktivieren.Aktivieren Sie das Kontrollkästchen **RIP-Routing aktivieren**.Aktivieren Sie das Kontrollkästchen **RIP-Version** mit dem Optionsfeld **Version 2 aktivieren**.Fügen Sie auf der Registerkarte **Netzwerke** das Netzwerk **10.1.1.0 hinzu**.Klicken Sie auf **Übernehmen**.



FelderEnable RIP Routing (RIP-Routing aktivieren) - Aktivieren Sie dieses Kontrollkästchen, um RIP-Routing auf der Security Appliance zu aktivieren. Wenn Sie RIP aktivieren, wird es auf allen Schnittstellen aktiviert. Wenn Sie dieses Kontrollkästchen aktivieren, werden auch die anderen Felder in diesem Bereich aktiviert. Deaktivieren Sie dieses Kontrollkästchen, um RIP-Routing auf der Security Appliance zu deaktivieren.Automatische Zusammenfassung aktivieren - Deaktivieren Sie dieses Kontrollkästchen, um die automatische Routenzusammenfassung zu deaktivieren. Aktivieren Sie dieses Kontrollkästchen, um die automatische Routenzusammenfassung erneut zu aktivieren. RIP Version 1 verwendet immer eine automatische Zusammenfassung. Sie können die automatische Zusammenfassung für RIP Version 1 nicht deaktivieren. Wenn Sie RIP Version 2 verwenden, können Sie die automatische Zusammenfassung deaktivieren, wenn Sie dieses Kontrollkästchen deaktivieren. Deaktivieren Sie die automatische Zusammenfassung, wenn Sie das Routing zwischen nicht verbundenen Subnetzen durchführen müssen. Wenn die automatische Zusammenfassung deaktiviert ist, werden Subnetze angezeigt.Enable RIP version (RIP-Version aktivieren): Aktivieren Sie dieses Kontrollkästchen, um die von der Sicherheits-Appliance verwendete RIP-Version anzugeben. Wenn dieses Kontrollkästchen deaktiviert ist, sendet die Sicherheits-Appliance RIP Version 1-Updates und akzeptiert RIP Version 1- und Version 2-Updates. Diese Einstellung kann im Schnittstellenbereich auf

Schnittstellenbasis überschrieben werden.Version 1 - Gibt an, dass die Sicherheits-Appliance nur RIP Version 1-Updates sendet und empfängt. Alle Updates der Version 2 werden gelöscht.Version 2 - Gibt an, dass die Sicherheits-Appliance nur RIP Version 2-Updates sendet und empfängt. Alle Updates der Version 1 werden gelöscht.Ermöglichen des Generierens von Standardinformationen - Aktivieren Sie dieses Kontrollkästchen, um eine Standardroute im RIP-Routing-Prozess zu generieren. Sie können eine Routenübersicht konfigurieren, die erfüllt werden muss, bevor die Standardroute generiert werden kann.Route-Map (Route-Map) - Geben Sie den Namen der Route-Map ein, um diese anzuwenden. Der Routing-Prozess generiert die Standardroute, wenn die Routenzuordnung eingehalten wird.IP Network to Add (Zu addiertes IP-Netzwerk): Definiert ein Netzwerk für den RIP-Routing-Prozess. Die angegebene Netzwerknummer darf keine Subnetzinformationen enthalten. Die Anzahl der Netzwerke, die Sie der Sicherheitsappliance-Konfiguration hinzufügen können, ist unbegrenzt. RIP-Routing-Updates werden nur über Schnittstellen in den angegebenen Netzwerken gesendet und empfangen. Wenn das Netzwerk einer Schnittstelle nicht angegeben ist, wird die Schnittstelle auch nicht in RIP-Aktualisierungen angekündigt.Add (Hinzufügen): Klicken Sie auf diese Schaltfläche, um das angegebene Netzwerk der Liste der Netzwerke hinzuzufügen.Löschen - Klicken Sie auf diese Schaltfläche, um das ausgewählte Netzwerk aus der Liste der Netzwerke zu entfernen.Globale passive Schnittstellen konfigurieren - Aktivieren Sie dieses Kontrollkästchen, um alle Schnittstellen der Sicherheits-Appliance auf den passiven RIP-Modus festzulegen. Die Sicherheits-Appliance überwacht RIP-Routing-Broadcasts auf allen Schnittstellen und verwendet diese Informationen zum Füllen der Routing-Tabellen, sendet jedoch keine Routing-Updates. Verwenden Sie die Tabelle für passive Schnittstellen, um bestimmte Schnittstellen auf passives RIP festzulegen.Tabelle für passive Schnittstellen: Führt die konfigurierten Schnittstellen auf der Sicherheits-Appliance auf. Aktivieren Sie das Kontrollkästchen in der Spalte Passive (Passiv) für die Schnittstellen, die Sie im passiven Modus betreiben möchten. Die anderen Schnittstellen senden und empfangen weiterhin RIP-Broadcasts.

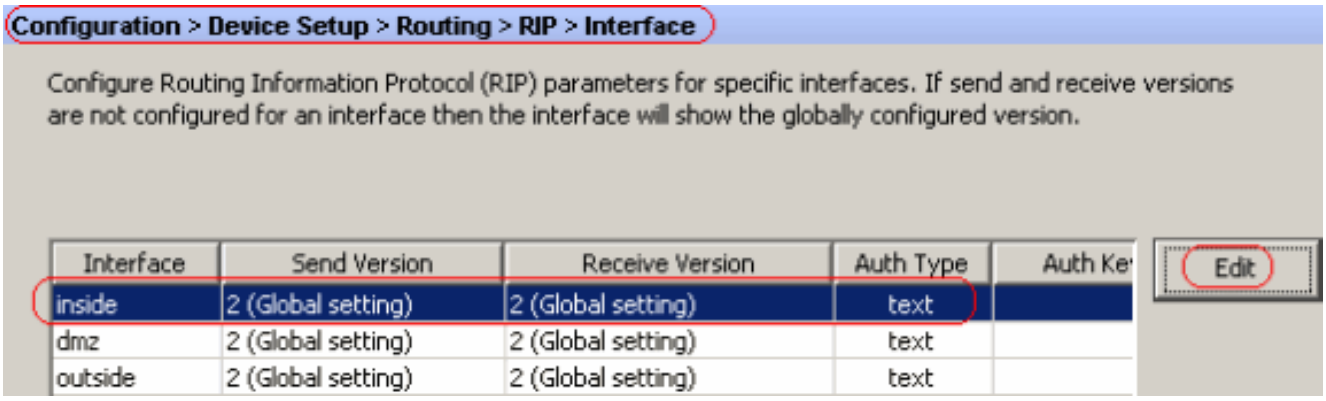
Konfigurieren der RIP-Authentifizierung

Die Cisco ASA unterstützt die MD5-Authentifizierung von Routing-Updates über das RIP v2-Routing-Protokoll. Der MD5-verschlüsselte Digest in jedem RIP-Paket verhindert das Einschleusen nicht autorisierter oder falscher Routing-Nachrichten von nicht genehmigten Quellen. Durch das Hinzufügen einer Authentifizierung zu Ihren RIP-Nachrichten wird sichergestellt, dass Ihre Router und die Cisco ASA nur Routing-Nachrichten von anderen Routing-Geräten akzeptieren, die mit demselben vorinstallierten Schlüssel konfiguriert sind. Wenn Sie ohne die konfigurierte Authentifizierung ein anderes Routing-Gerät mit unterschiedlichen oder gegenteiligen Routing-Informationen in das Netzwerk einführen, können die Routing-Tabellen auf Ihren Routern oder der Cisco ASA beschädigt werden, und es kann zu einem Denial-of-Service-Angriff kommen. Wenn Sie den RIP-Nachrichten, die zwischen den Routing-Geräten gesendet werden, eine Authentifizierung hinzufügen (einschließlich der ASA), verhindert dies die zielgerichtete oder versehentliche Hinzufügung eines anderen Routers zum Netzwerk sowie jegliche Probleme.

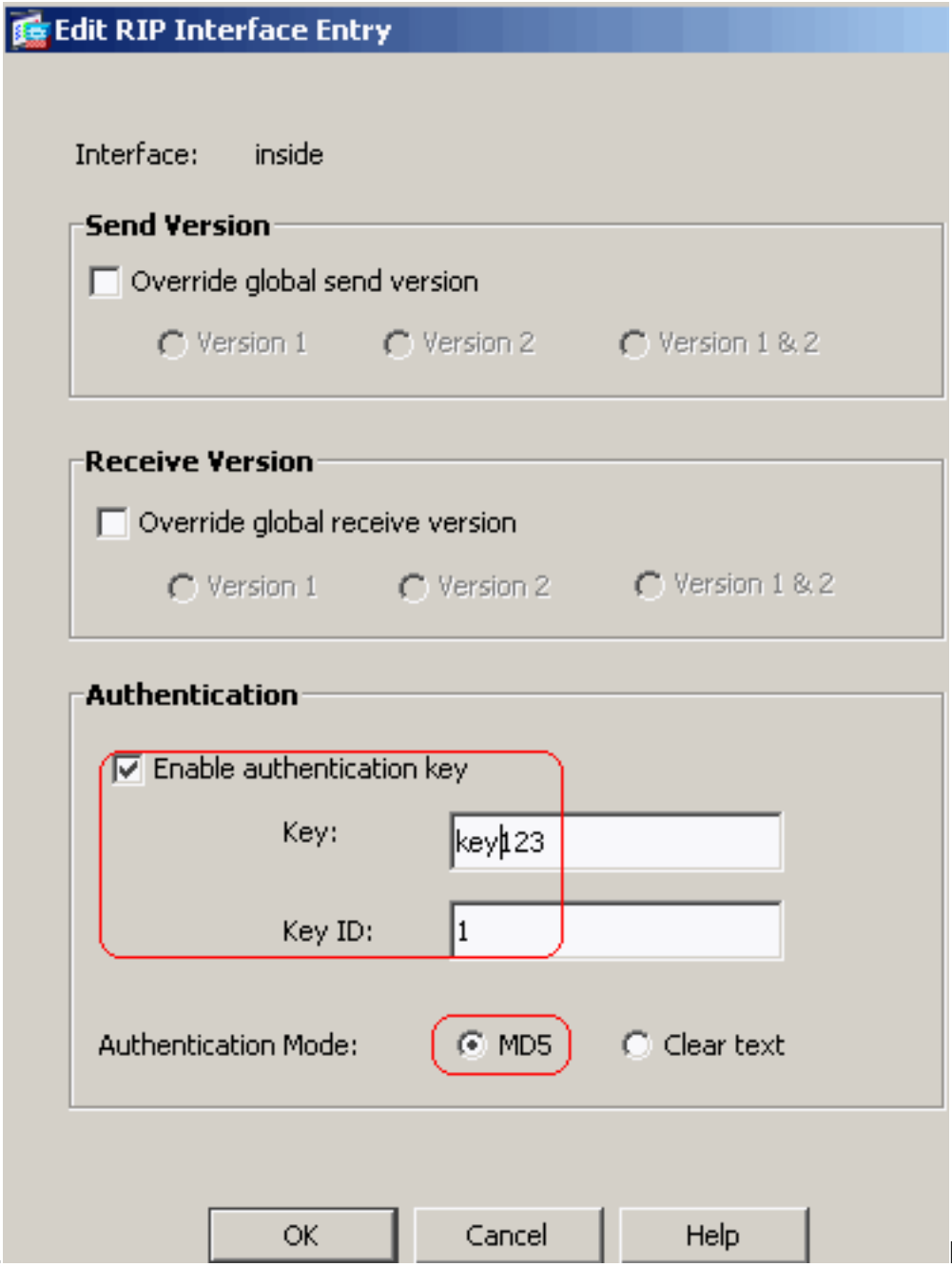
Die RIP-Routenauthentifizierung wird auf Schnittstellenbasis konfiguriert. Alle RIP-Nachbarn auf für die RIP-Nachrichtenauthentifizierung konfigurierten Schnittstellen müssen mit demselben Authentifizierungsmodus und Schlüssel konfiguriert werden.

Gehen Sie wie folgt vor, um die RIP MD5-Authentifizierung auf der Cisco ASA zu aktivieren.

1. Wählen Sie im ASDM **Configuration > Device Setup > Routing > RIP > Interface (Konfiguration > Geräteeinrichtung > Routing > RIP > Schnittstelle) aus,** und wählen Sie die interne Schnittstelle mit der Maus aus. Klicken Sie auf **Bearbeiten**.



2. Aktivieren Sie das Kontrollkästchen **Authentifizierungsschlüssel aktivieren**, und geben Sie dann den **Key-**Wert und den **Key-ID-**Wert

ein. 

Klicken Sie auf **OK** und dann auf **Übernehmen**.

Cisco ASA CLI-Konfiguration

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




!

!--- 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
```

CLI-Konfiguration des Cisco IOS Routers (R2)

Cisco IOS-Router (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
```

CLI-Konfiguration des Cisco IOS Routers (R1)

Cisco IOS-Router (R1)

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

CLI-Konfiguration des Cisco IOS Routers (R3)

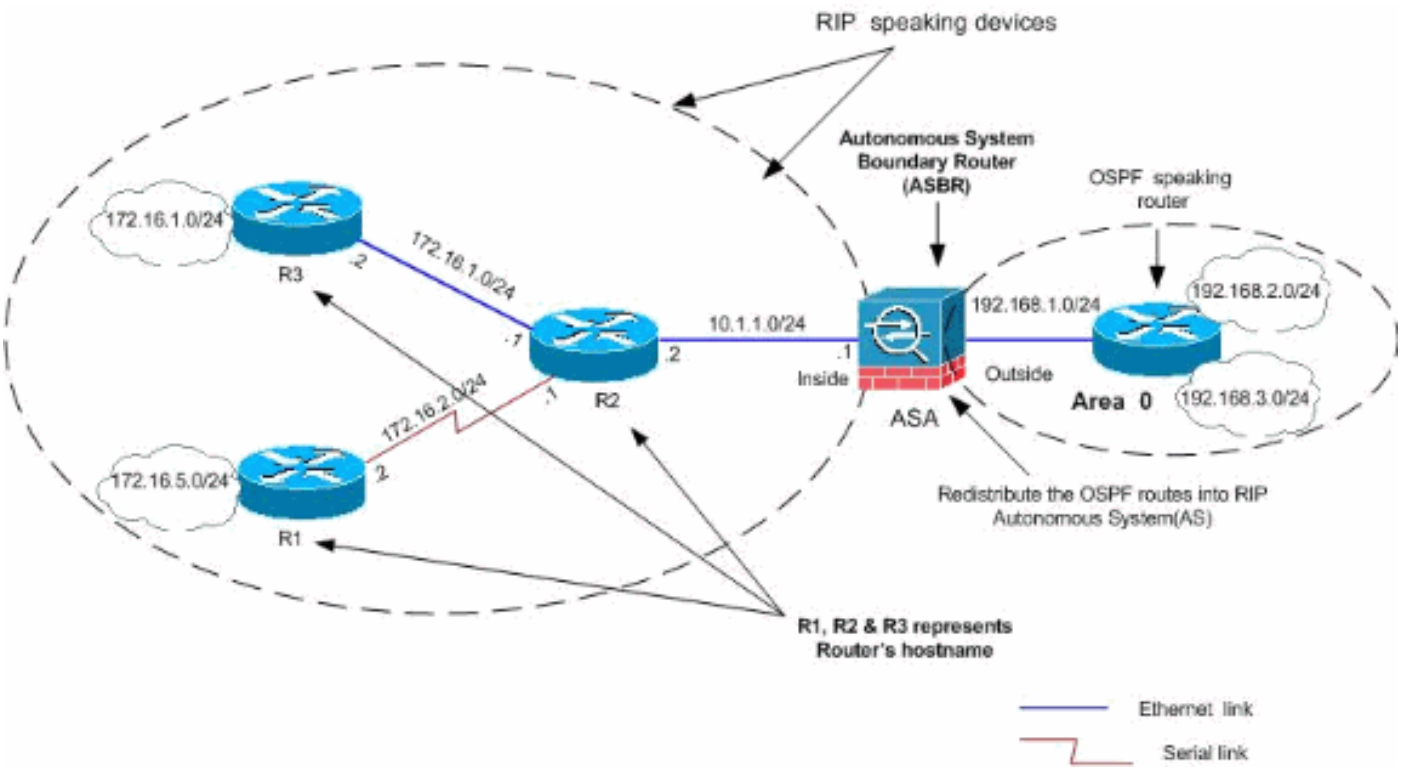
Cisco IOS-Router (R3)

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

Neuverteilung über RIP mit ASA

Routen von OSPF-, EIGRP-, statischen und verbundenen Routing-Prozessen können über den RIP-Routing-Prozess neu verteilt werden.

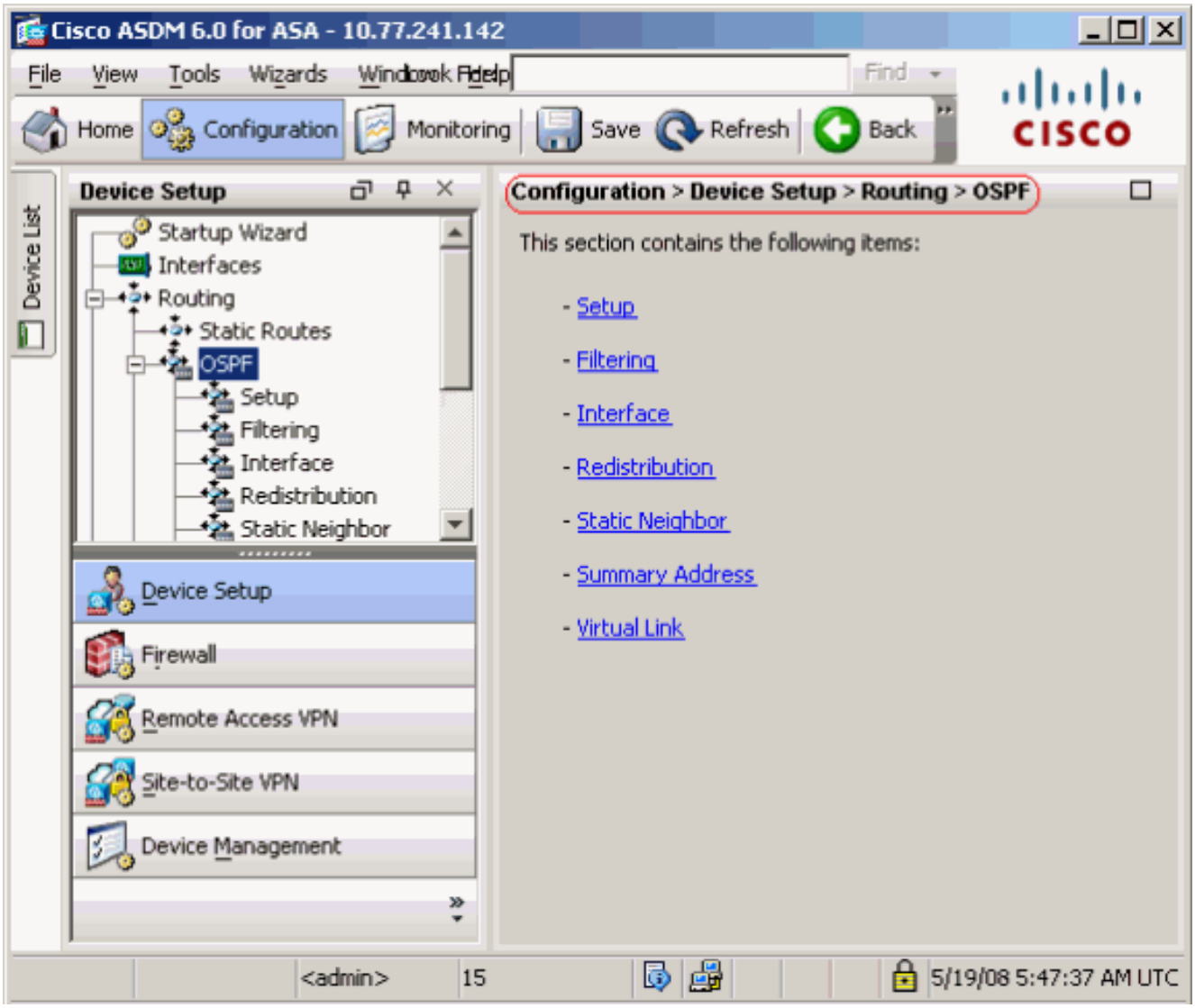
In diesem Beispiel wird die Neuverteilung der OSPF-Routen in RIP mithilfe des Netzwerkdiagramms dargestellt:



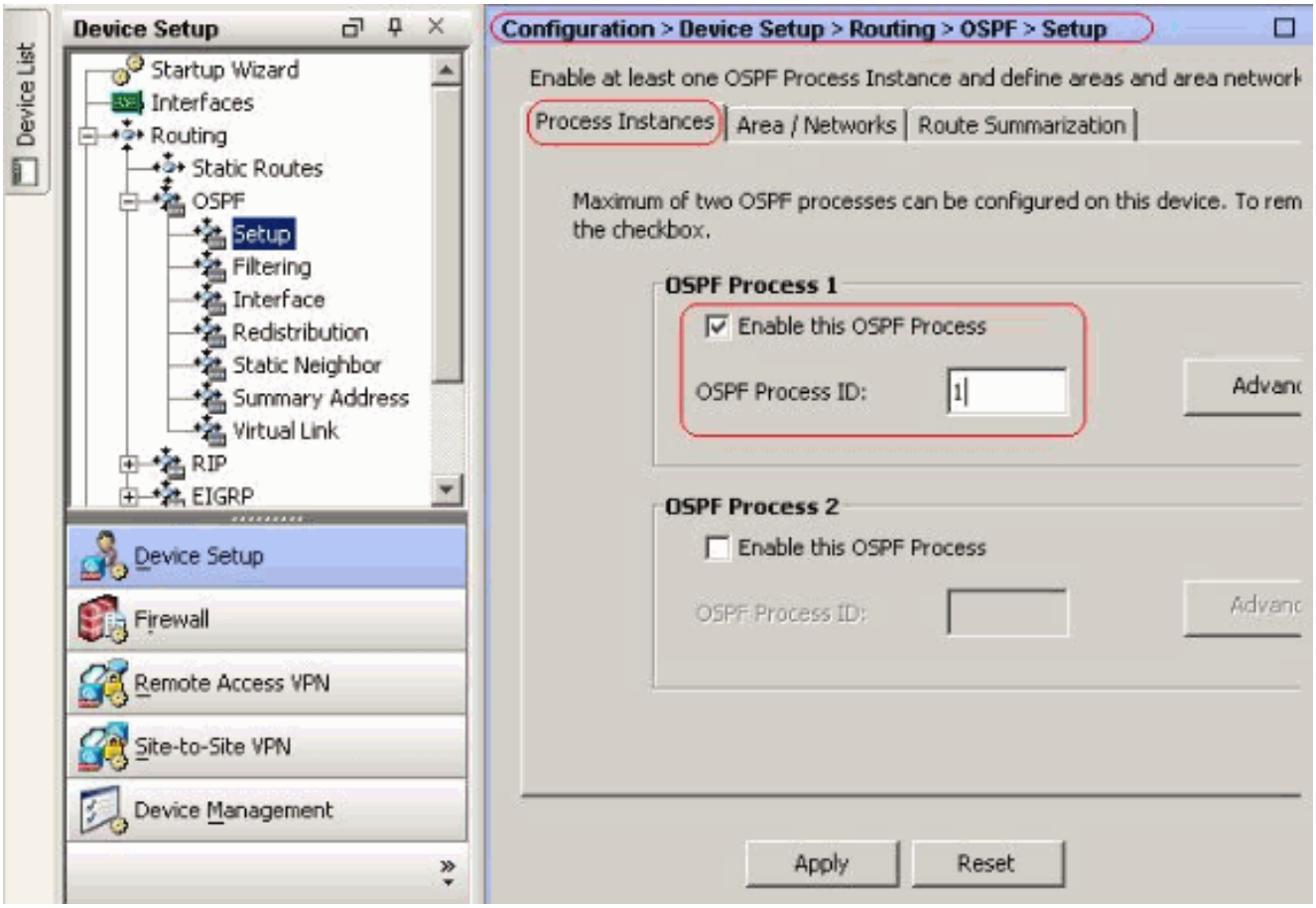
ASDM-Konfiguration

Gehen Sie wie folgt vor:

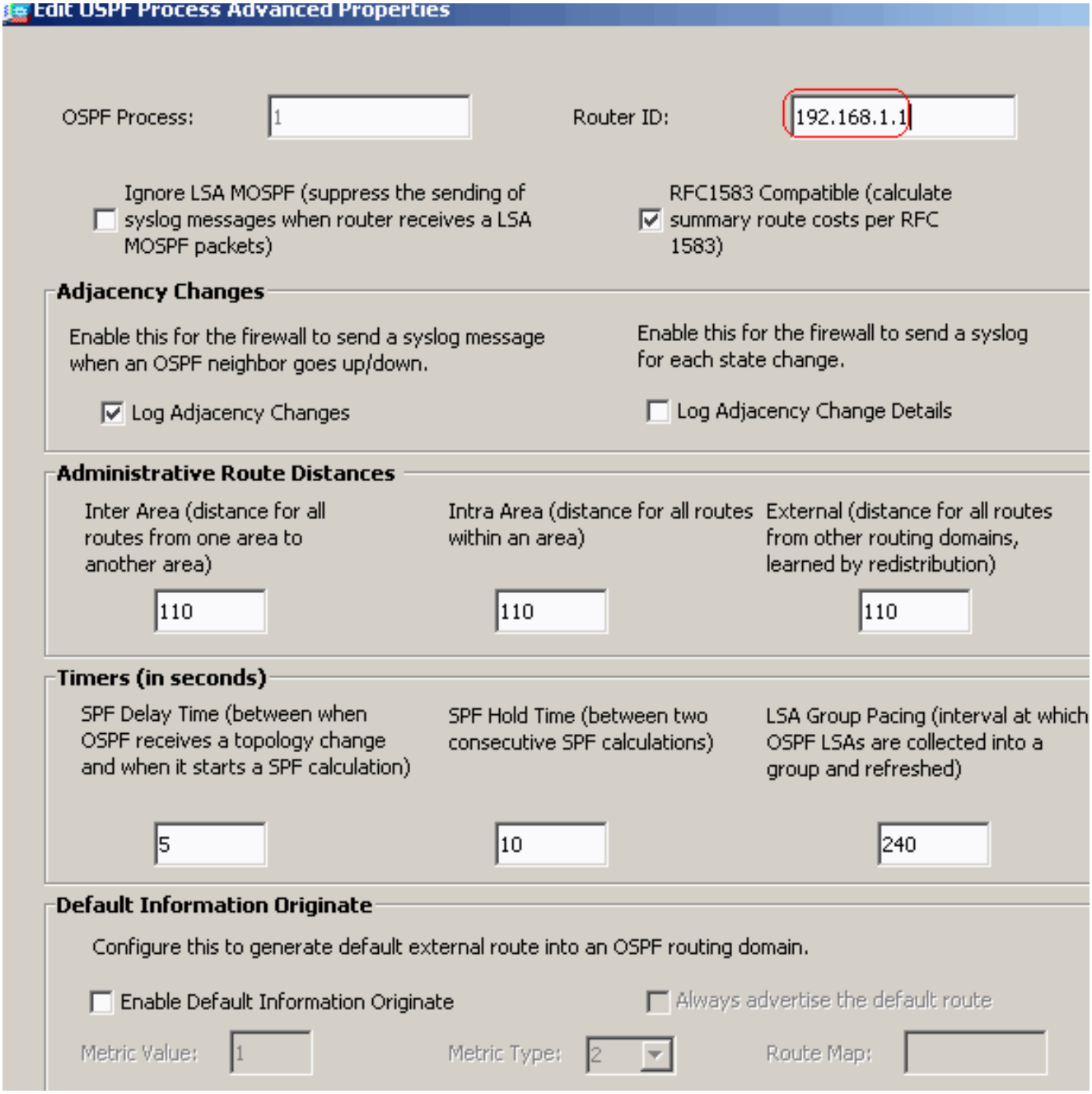
1. **OSPF-Konfiguration**Wählen Sie **Configuration > Device Setup > Routing > OSPF** in der ASDM-Schnittstelle aus, wie im Screenshot gezeigt.



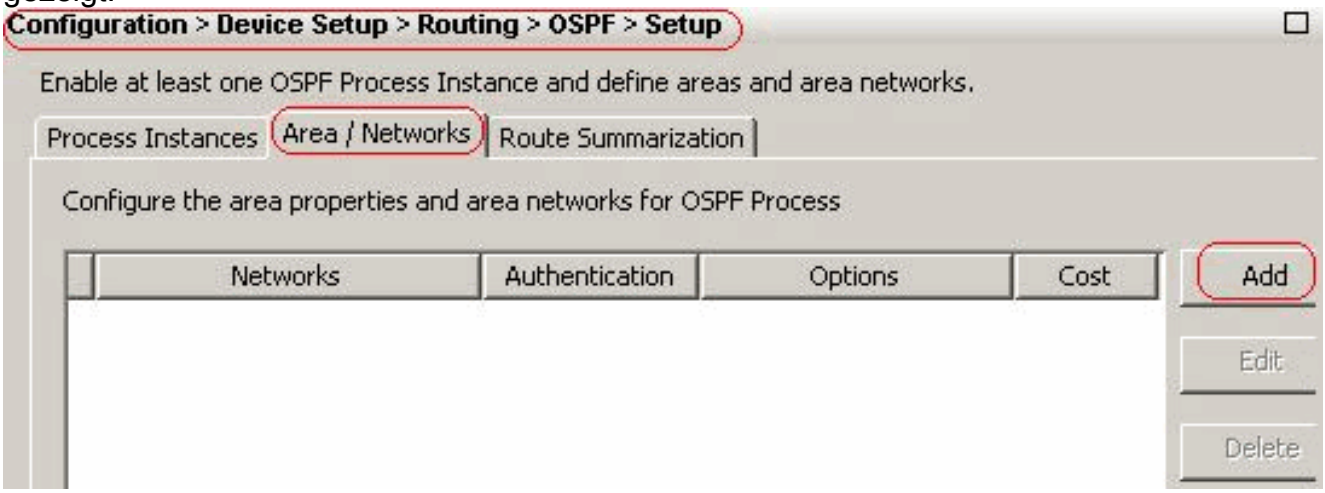
Aktivieren Sie den OSPF-Routing-Prozess auf der Registerkarte **Setup > Process Instances** (**Setup > Process Instanzen**), wie im Screenshot gezeigt. In diesem Beispiel lautet der OSPF-ID-Prozess
1.



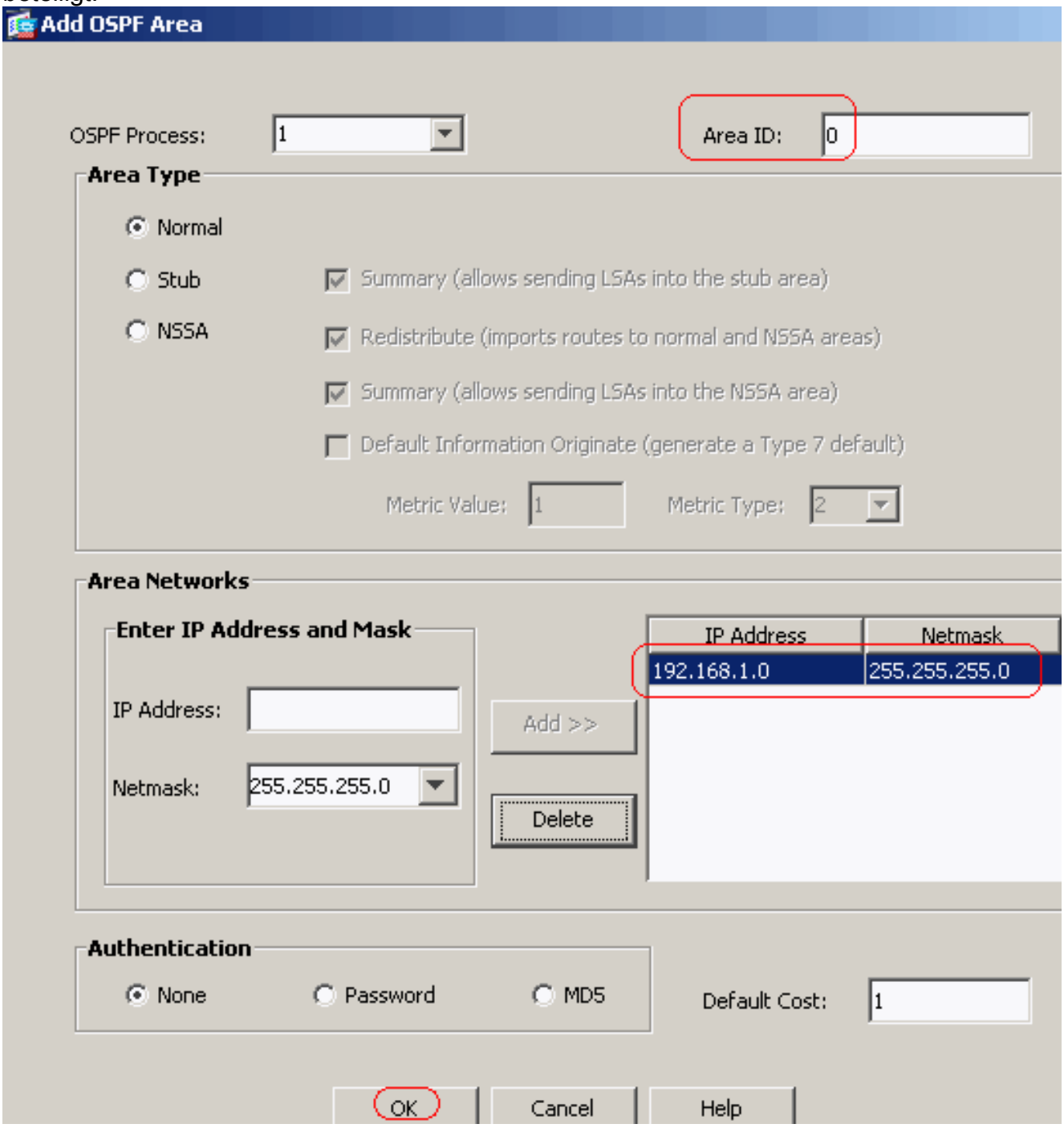
Klicken Sie auf der Registerkarte **Setup > Process Instances** (Setup > Process Instanzen) auf **Advanced**, um optionale erweiterte OSPF-Routingprozessparameter zu konfigurieren. Sie können prozessspezifische Einstellungen bearbeiten, z. B. die Router-ID, Adjacency-Änderungen, Administrative Route Distances, Timer und die Einstellungen für die Standard-Informationsursprungskonfiguration.



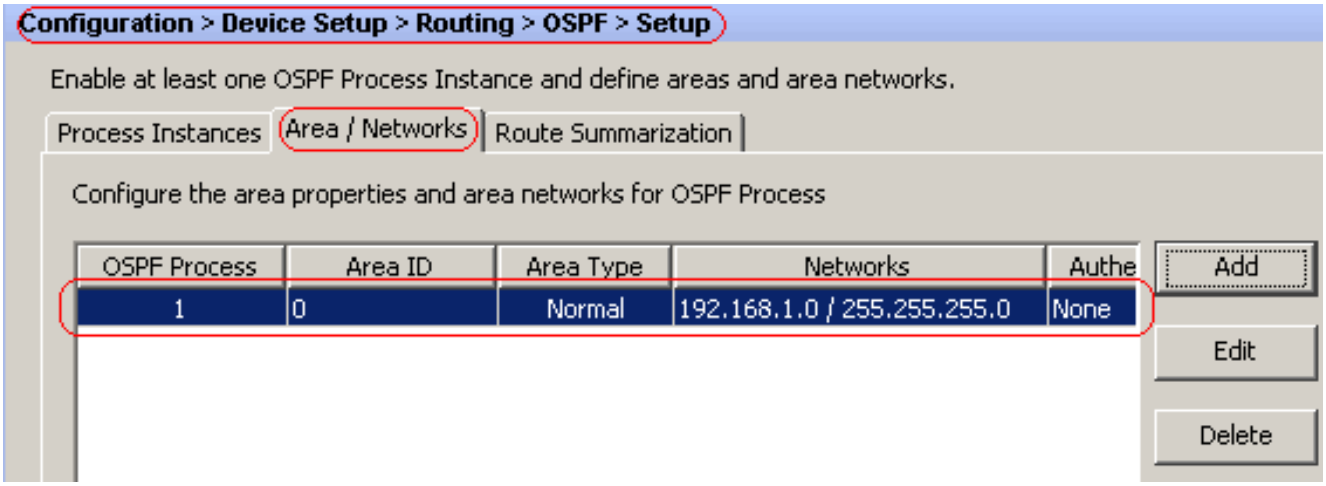
Klicken Sie auf **OK**.Nachdem Sie die vorherigen Schritte ausgeführt haben, definieren Sie die Netzwerke und Schnittstellen, die am OSPF-Routing teilnehmen, auf der Registerkarte **Setup > Area/Networks (Setup > Bereich/Netzwerke)**. Klicken Sie auf **Hinzufügen**, wie in diesem Screenshot
gezeigt.



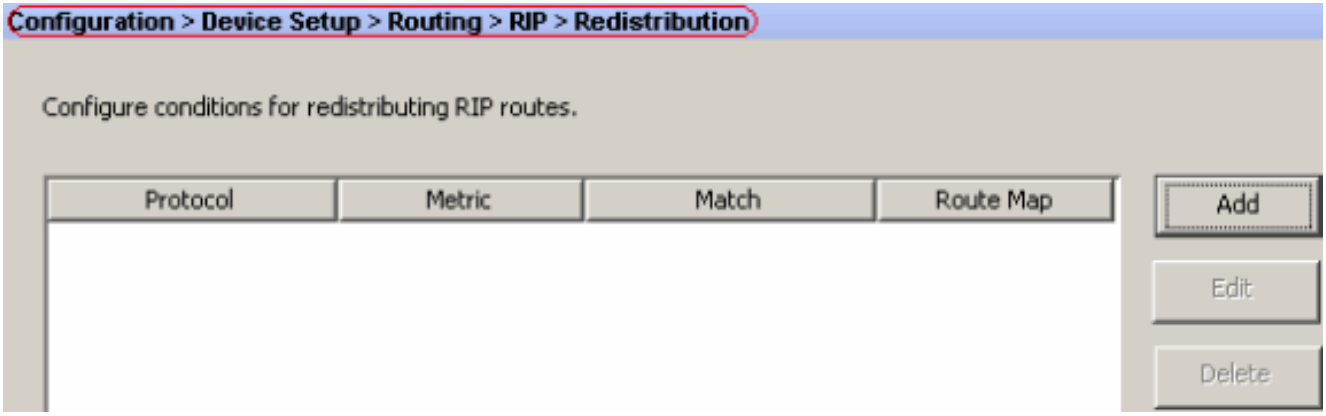
Dieser Bildschirm wird angezeigt. In diesem Beispiel wird nur das externe Netzwerk (192.168.1.0/24) hinzugefügt, da OSPF nur für die externe Schnittstelle aktiviert ist.**Hinweis:** Nur Schnittstellen mit einer IP-Adresse, die zu den definierten Netzwerken gehören, sind am OSPF-Routing-Prozess
beteiligt.



Klicken Sie auf **OK**.Klicken Sie auf **Übernehmen**.

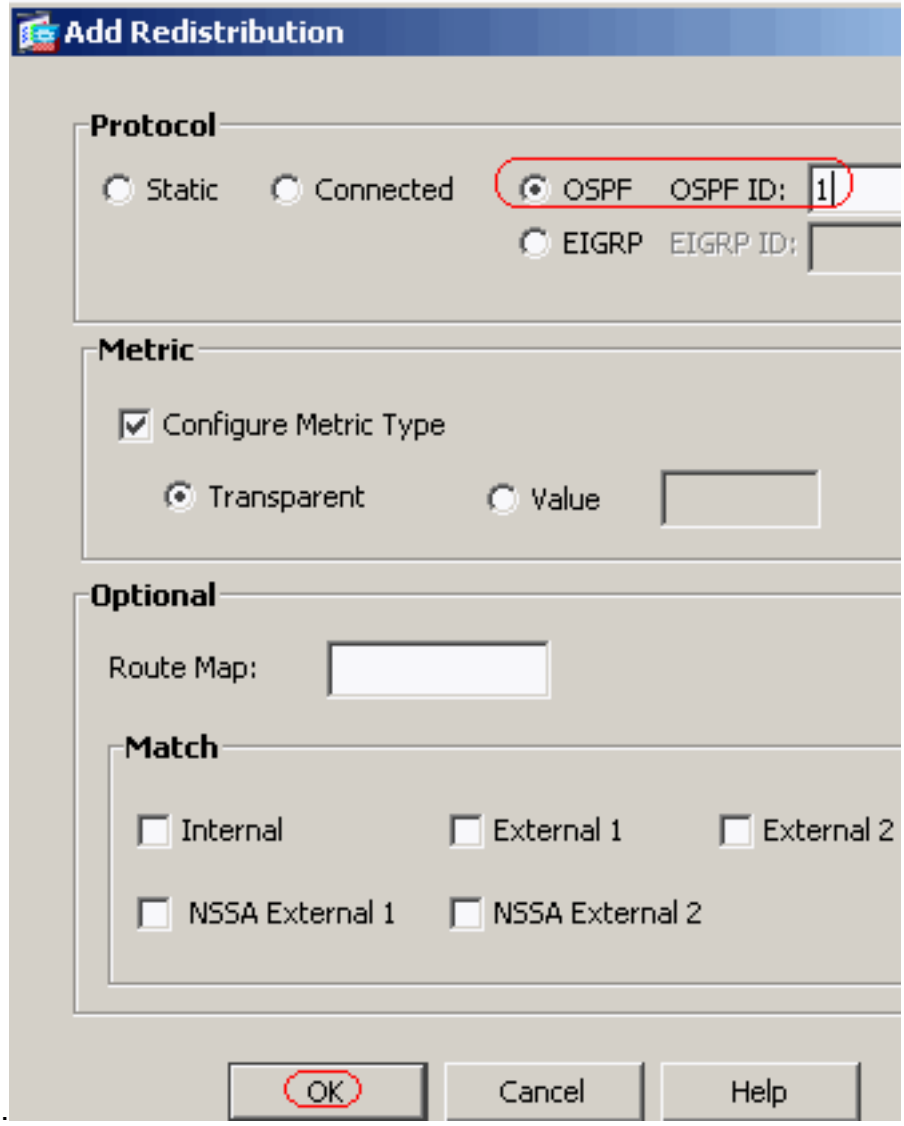


2. Wählen Sie **Configuration > Device Setup > Routing > RIP > Redistribution > Add** aus, um OSPF-Routen in RIP neu zu verteilen.



3. Klicken Sie auf **OK** und dann auf

Übernehmen.



Entsprechende CLI-Konfiguration

CLI-Konfiguration der ASA zur Neuverteilung von OSPF in RIP AS
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

Sie sehen die Routing-Tabelle des benachbarten Cisco IOS-Routers (R2) nach der Neuverteilung von OSPF-Routen in RIP AS.

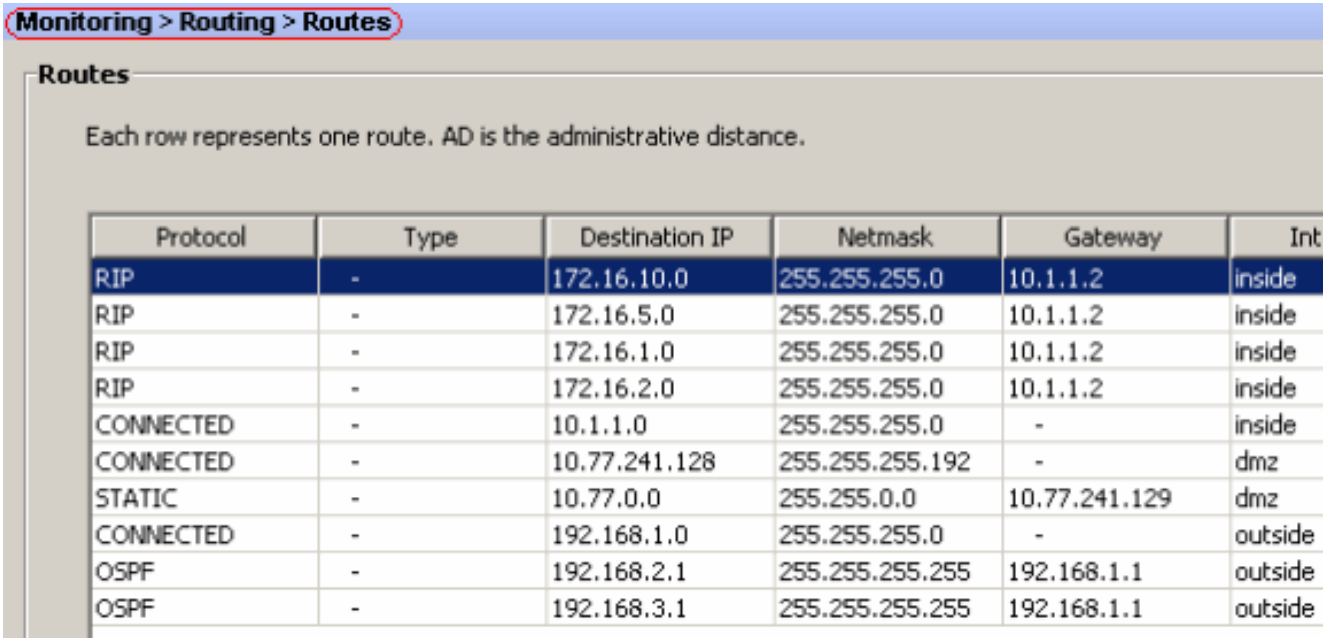
```
R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
        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
```

Überprüfen

Gehen Sie wie folgt vor, um Ihre Konfiguration zu überprüfen:

1. Sie können die Routing-Tabelle überprüfen, wenn Sie zu **Monitoring > Routing > Routes** navigieren. In diesem Screenshot sehen Sie, dass die Netzwerke 172.16.1.0/24, 172.16.2.0/24, 172.16.5.0/24 und 172.16.10.0/24 mit RIP über R2 (10.1.1.2) erfasst werden.



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. In der CLI können Sie den Befehl **show route** verwenden, um dieselbe Ausgabe zu erhalten.

```
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#
```

Fehlerbehebung

Dieser Abschnitt enthält Informationen über Debugbefehle, die zur Behebung von OSPF-Problemen nützlich sein können.

Befehle zur Fehlerbehebung

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

Hinweis: Beachten Sie vor der Verwendung von **Debug-**Befehlen die Informationen zu Debug-Befehlen.

- **debug rip events** - Aktiviert das Debuggen von RIP-Ereignissen

```
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
```

Zugehörige Informationen

- Support-Seite für Cisco Adaptive Security Appliances der Serie 5500
- Support-Seite für Cisco PIX der Serie 500
- PIX/ASA 8.X: Konfigurieren von EIGRP auf der Cisco Adaptive Security Appliance (ASA)
- Technischer Support und Dokumentation - Cisco Systems