Esempio di configurazione di ASA/PIX con RIP

Sommario

Introduzione

Questo documento spiega come configurare Cisco ASA in modo da imparare a usare il protocollo RIP (Routing Information Protocol), eseguire l'autenticazione e la ridistribuzione.

Per ulteriori informazioni, fare riferimento al documento PIX/ASA 8.X: Configurazione di EIGRP su Cisco Adaptive Security Appliance (ASA) per ulteriori informazioni sulla configurazione EIGRP.

Nota: questa configurazione del documento è basata su RIP versione 2.

Nota: il routing asimmetrico non è supportato in ASA/PIX.

Prerequisiti

Requisiti

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- Cisco ASA/PIX deve eseguire la versione 7.x o successive.
- RIP non supportato in modalità contesto multiplo. è supportato solo in modalità singola.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco serie 5500 Adaptive Security Appliance (ASA) con software versione 8.0 e successive.
- Software Cisco Adaptive Security Device Manager (ASDM) versione 6.0 e successive.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Prodotti correlati

Le informazioni discusse in questo documento sono valide anche per il Cisco serie 500 PIX firewall con software versione 8.0 e successive.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Premesse

RIP è un protocollo di routing tra vettori di distanza che utilizza il conteggio hop come metrica per la selezione del percorso. Quando RIP è abilitato su un'interfaccia, l'interfaccia scambia le trasmissioni RIP con i dispositivi adiacenti per conoscere e annunciare dinamicamente le route.

L'appliance di sicurezza supporta RIP versione 1 e RIP versione 2. RIP versione 1 non invia la subnet mask con l'aggiornamento del routing. RIP versione 2 invia la subnet mask con l'aggiornamento del routing e supporta subnet mask a lunghezza variabile. RIP versione 2 supporta inoltre l'autenticazione dei router adiacenti quando vengono scambiati gli aggiornamenti di routing. Questa autenticazione garantisce che l'accessorio di protezione riceva informazioni di routing affidabili da una fonte attendibile.

Limitazioni:

1. L'appliance di sicurezza non è in grado di passare aggiornamenti RIP tra le interfacce.
2. RIP versione 1 non supporta le subnet mask a lunghezza variabile (VLSM).
3. RIP ha un numero massimo di hop pari a 15. Una route con un numero di hop maggiore di 15 è considerata irraggiungibile.
4. La convergenza RIP è relativamente lenta rispetto ad altri protocolli di routing.
5. Èpossibile abilitare un solo processo RIP sull'appliance di sicurezza.

Nota: queste informazioni si applicano solo a RIP versione 2:

1. Se si utilizza l'autenticazione dei router adiacenti, la chiave di autenticazione e l'ID della chiave devono essere gli stessi in tutti i dispositivi adiacenti che forniscono aggiornamenti RIP versione 2 all'interfaccia.
2. Con RIP versione 2, l'accessorio di protezione trasmette e riceve gli aggiornamenti delle route predefinite utilizzando l'indirizzo multicast 224.0.0.9. In modalità passiva, riceve gli aggiornamenti delle route a tale indirizzo.
3. Quando RIP versione 2 è configurato su un'interfaccia, l'indirizzo multicast 224.0.0.9 viene registrato su tale interfaccia. Quando una configurazione RIP versione 2 viene rimossa da un'interfaccia, viene annullata la registrazione dell'indirizzo multicast.

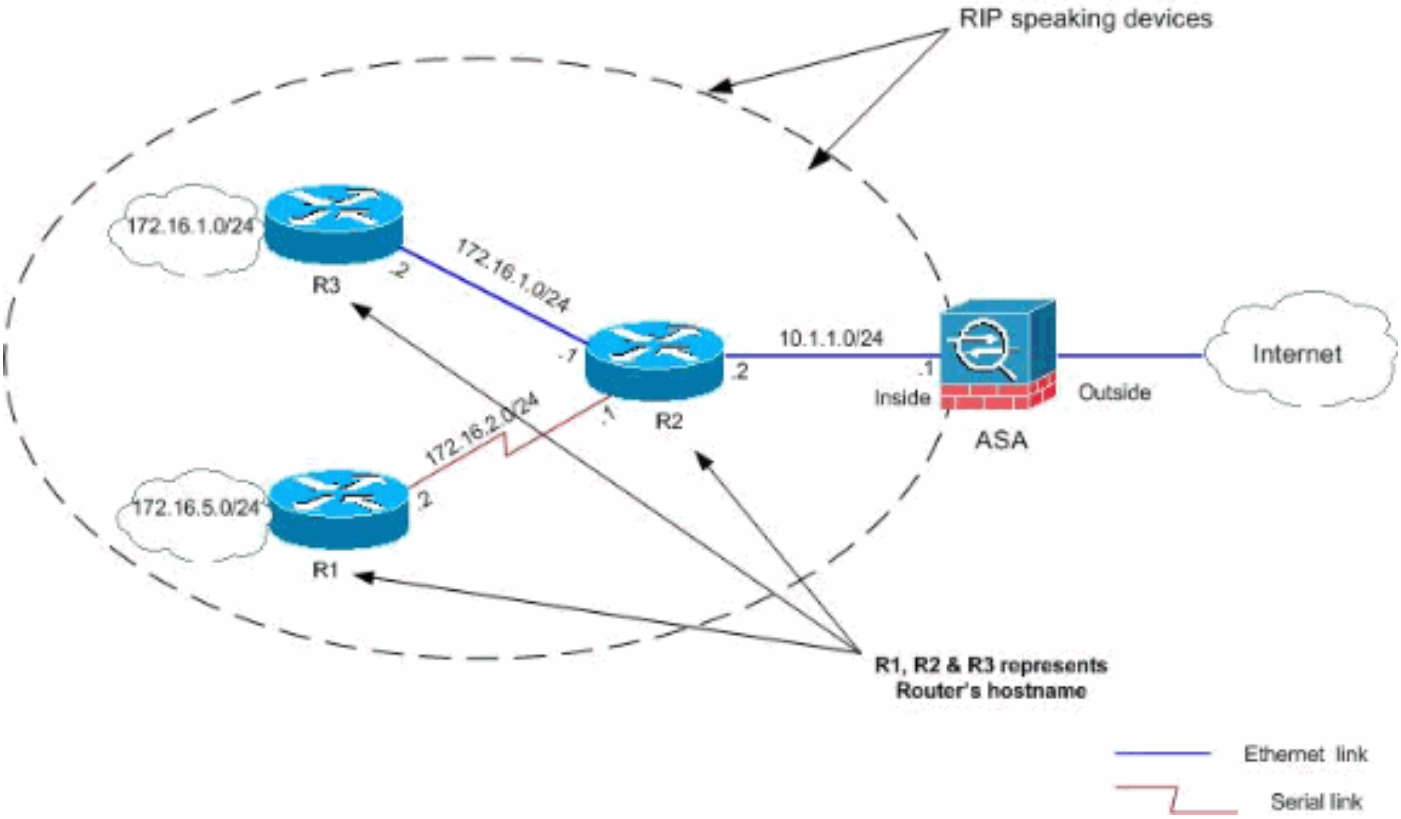
Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Configurazioni

Nel documento vengono usate queste configurazioni:

- Configurazione ASDM
- Configura autenticazione RIP

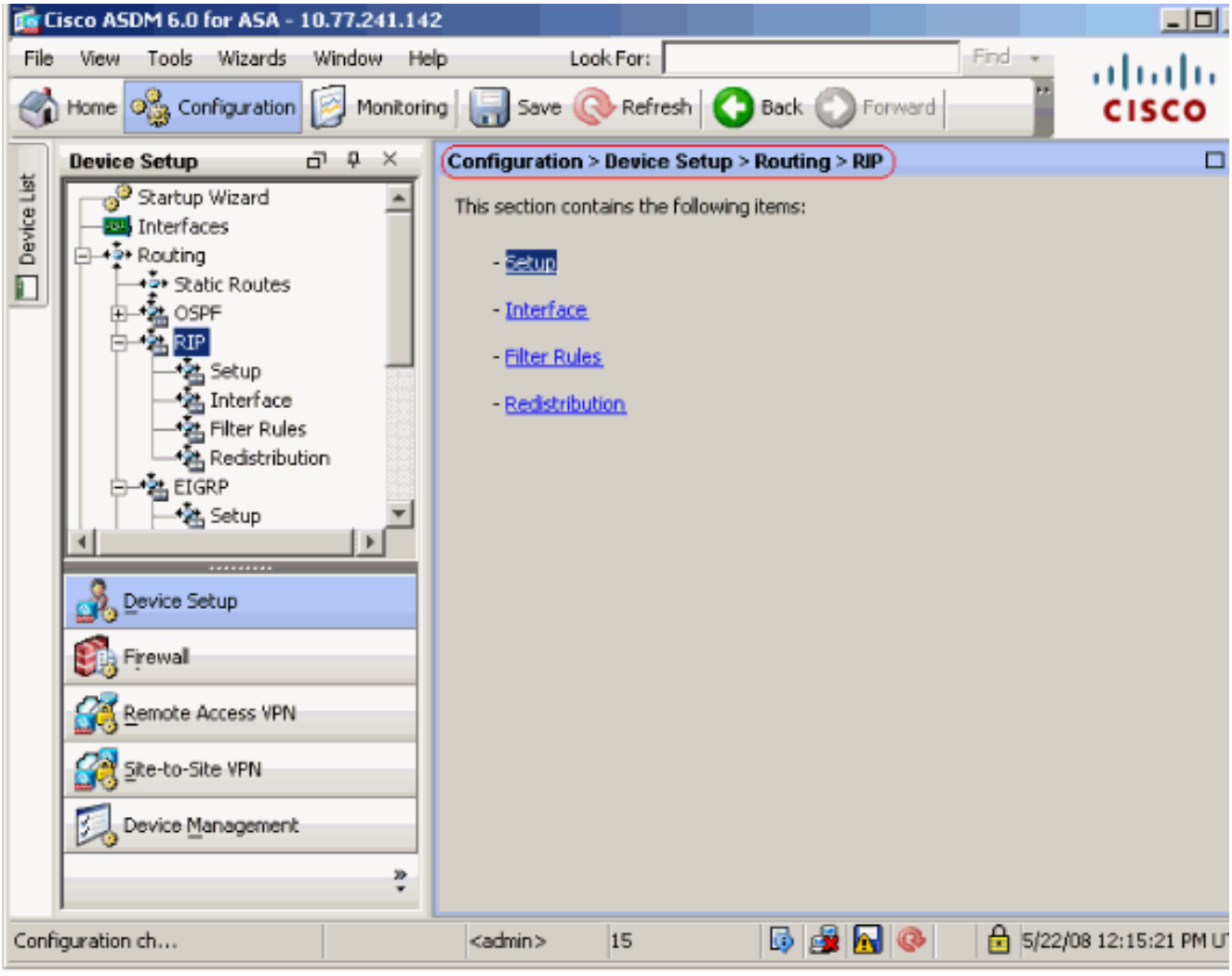
- Configurazione Cisco ASA CLI
- Configurazione CLI del router Cisco IOS (R2)
- Configurazione CLI del router Cisco IOS (R1)
- Configurazione CLI del router Cisco IOS (R3)

Configurazione ASDM

Adaptive Security Device Manager (ASDM) è un'applicazione basata su browser utilizzata per configurare e monitorare il software sui dispositivi di sicurezza. ASDM viene caricato dall'appliance di sicurezza e quindi utilizzato per configurare, monitorare e gestire il dispositivo. È inoltre possibile utilizzare l'utilità di avvio ASDM (solo Windows®) per avviare l'applicazione ASDM più rapidamente dell'applet Java. In questa sezione vengono descritte le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento con ASDM.

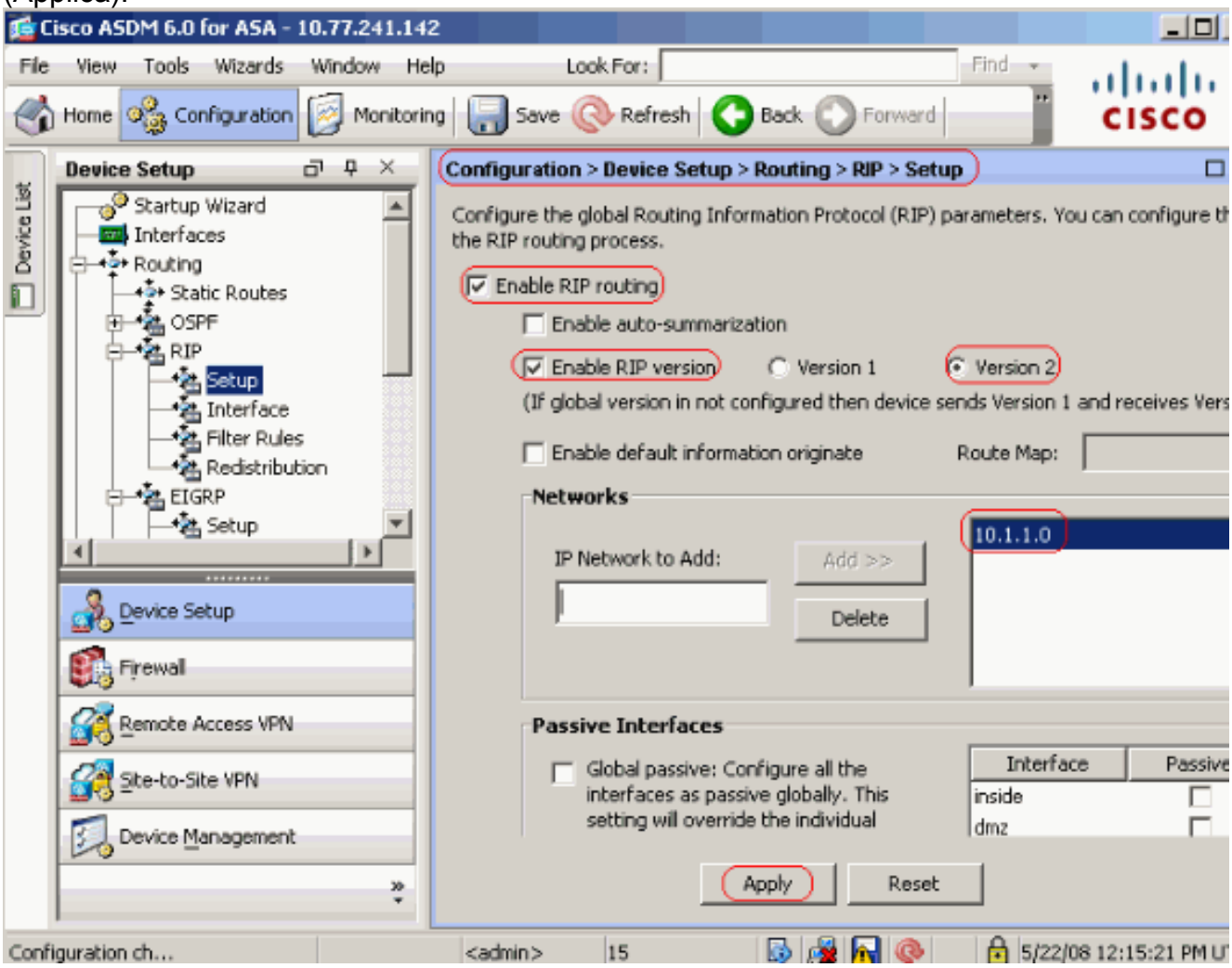
Per configurare il RIP nell'appliance Cisco ASA, completare la procedura seguente:

1. Accedere all'appliance Cisco ASA con ASDM.
2. Scegliere **Configurazione > Impostazione dispositivo > Routing > RIP** nell'interfaccia ASDM, come mostrato nella schermata.



3. Per abilitare il routing RIP, scegliere **Configurazione > Impostazione dispositivo > Routing > RIP > Impostazione**, come mostrato di seguito.Selezionare la casella di controllo **Abilita routing RIP**.Selezionare la casella di controllo **Abilita versione RIP** con il pulsante di opzione **Versione 2**.In **Reti**, aggiungere la rete **10.1.1.0**.Fare clic su **Apply**

(Applica).



CampiAbilita routing RIP: selezionare questa casella di controllo per abilitare il routing RIP sull'accessorio di sicurezza. Quando si abilita RIP, questo viene abilitato su tutte le interfacce. Se si seleziona questa casella di controllo, verranno attivati anche gli altri campi del riquadro. Deselezionare questa casella di controllo per disabilitare il routing RIP sull'accessorio di sicurezza.Abilita riepilogo automatico: deselezionare questa casella di controllo per disabilitare il riepilogo automatico delle route. Selezionare questa casella di controllo per riattivare il riepilogo automatico delle route. RIP versione 1 utilizza sempre il riepilogo automatico. Non è possibile disattivare il riepilogo automatico per RIP versione 1. Se si utilizza RIP versione 2, è possibile disattivare il riepilogo automatico deselezionando questa casella di controllo. Disabilitare la generazione automatica del riepilogo se è necessario eseguire il routing tra subnet disconnesse. Quando la generazione automatica del riepilogo è disattivata, le subnet vengono annunciate.Abilita versione RIP: selezionare questa casella di controllo per specificare la versione di RIP utilizzata dall'accessorio di protezione. Se questa casella di controllo è deselezionata, l'accessorio di protezione invia aggiornamenti RIP versione 1 e accetta gli aggiornamenti RIP versione 1 e versione 2. È possibile ignorare questa impostazione per singola interfaccia nel riquadro Interfaccia.Versione 1: specifica che l'accessorio di protezione invia e riceve solo aggiornamenti RIP versione 1. Tutti gli aggiornamenti della versione 2 ricevuti vengono eliminati.Versione 2: specifica che l'accessorio di protezione invia e riceve solo aggiornamenti RIP versione 2. Tutti gli aggiornamenti della versione 1 ricevuti vengono eliminati.Abilita origine informazioni di default (Enable default information originate) - Selezionate questa casella di controllo per generare una route di default nel processo di

routing RIP. È possibile configurare una mappa dei percorsi che deve essere soddisfatta prima che sia possibile generare il percorso predefinito.Route-map (Route-map) - Consente di immettere il nome della mappa della route da applicare. Il processo di instradamento genera il instradamento predefinito se la mappa del instradamento è soddisfatta.Rete IP da aggiungere: definisce una rete per il processo di routing RIP. Il numero di rete specificato non deve contenere informazioni sulla subnet. Non esistono limiti al numero di reti che è possibile aggiungere alla configurazione dell'appliance di sicurezza. Gli aggiornamenti del routing RIP vengono inviati e ricevuti solo tramite interfacce nelle reti specificate. Inoltre, se non si specifica la rete di un'interfaccia, l'interfaccia non viene annunciata in alcun aggiornamento RIP.Aggiungi: fare clic su questo pulsante per aggiungere la rete specificata all'elenco delle reti.Elimina: fare clic su questo pulsante per rimuovere la rete selezionata dall'elenco delle retiConfigura interfacce come passive a livello globale: selezionare questa casella di controllo per impostare tutte le interfacce sull'appliance di sicurezza sulla modalità RIP passiva. L'appliance di sicurezza resta in ascolto delle trasmissioni di routing RIP su tutte le interfacce e utilizza tali informazioni per popolare le tabelle di routing ma non trasmette gli aggiornamenti di routing. Utilizzare la tabella Interfacce passive per impostare interfacce specifiche su RIP passivo.Tabella Interfacce passive: elenca le interfacce configurate sull'appliance di sicurezza. Selezionare la casella di controllo nella colonna Passivo per le interfacce che si desidera utilizzare in modalità passiva. Le altre interfacce continuano a inviare e ricevere trasmissioni RIP.

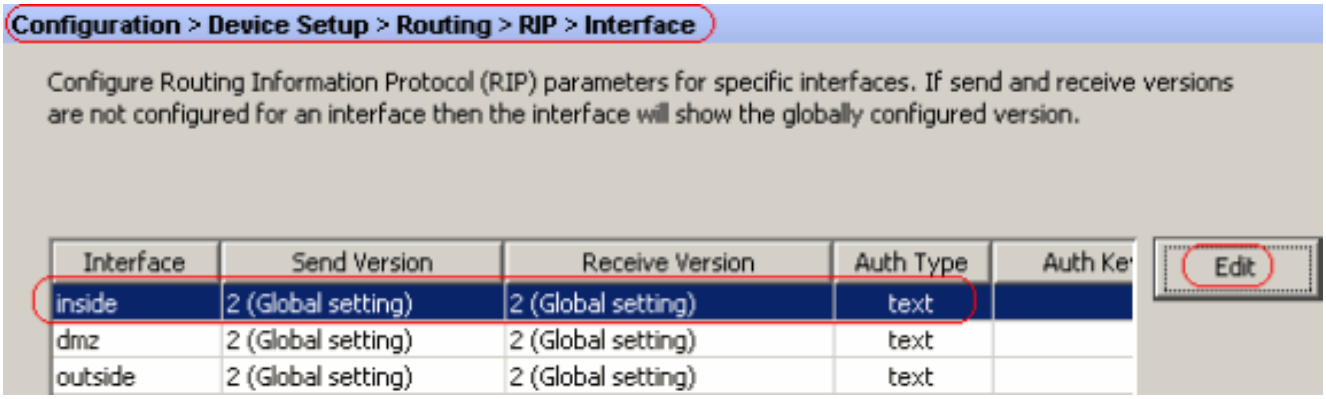
Configura autenticazione RIP

Cisco ASA supporta l'autenticazione MD5 degli aggiornamenti di routing dal protocollo di routing RIP v2. Il digest con chiave MD5 in ciascun pacchetto RIP impedisce l'introduzione di messaggi di routing non autorizzati o falsi provenienti da origini non approvate. L'aggiunta dell'autenticazione ai messaggi RIP garantisce che i router e l'appliance Cisco ASA accettino solo messaggi di routing da altri dispositivi di routing configurati con la stessa chiave precondivisa. Senza questa autenticazione configurata, se si introduce un altro dispositivo di routing con informazioni di routing diverse o diverse sulla rete, le tabelle di routing sui router o su Cisco ASA possono danneggiarsi e può verificarsi un attacco Denial of Service. L'aggiunta dell'autenticazione ai messaggi RIP inviati tra i dispositivi di routing, compresa l'ASA, impedisce l'aggiunta intenzionale o accidentale di un altro router alla rete e qualsiasi problema.

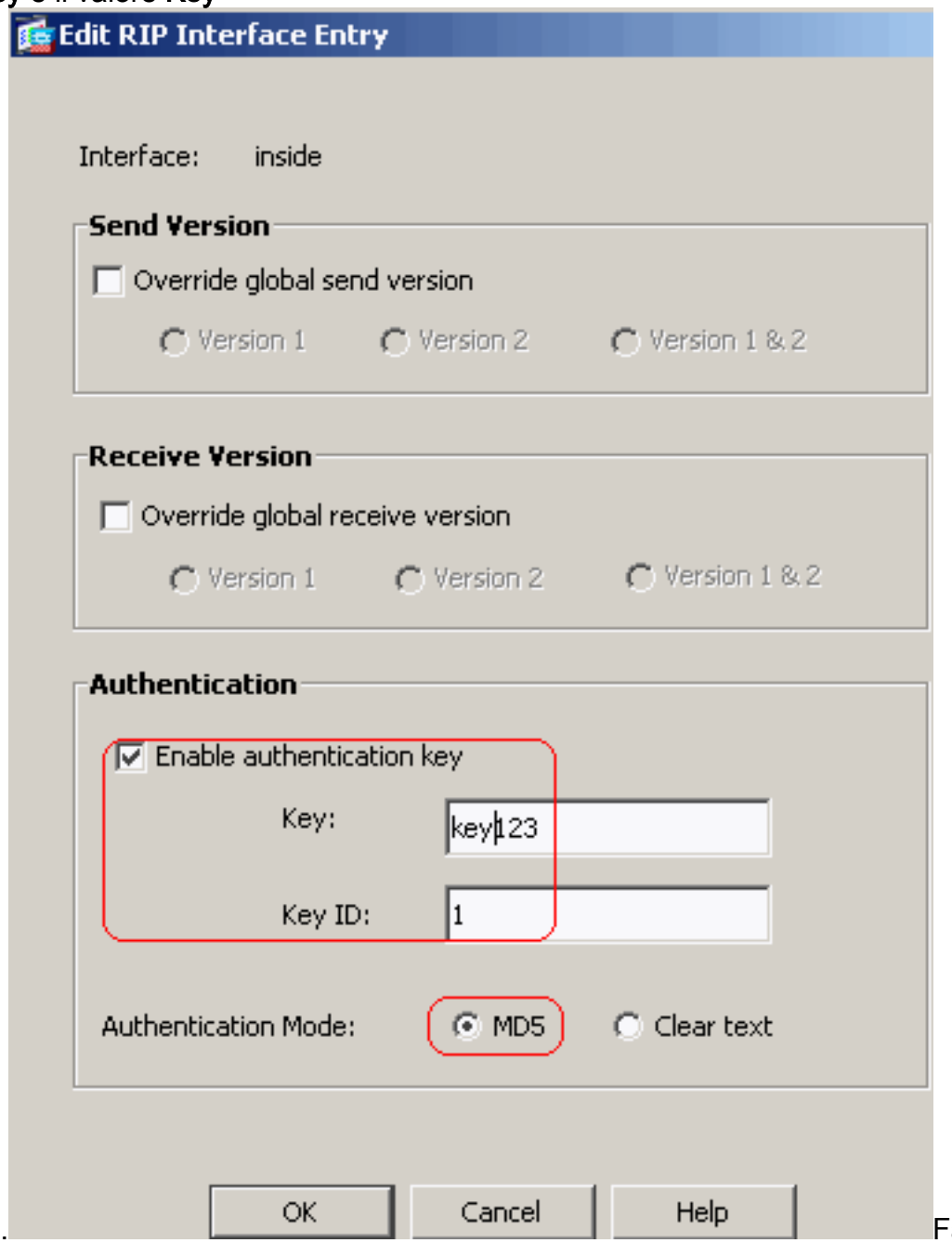
L'autenticazione route RIP è configurata per interfaccia. Tutti i router RIP adiacenti sulle interfacce configurate per l'autenticazione tramite messaggio RIP devono essere configurati con la stessa modalità e chiave di autenticazione.

Completare questa procedura per abilitare l'autenticazione RIP MD5 sull'appliance Cisco ASA.

1. In ASDM, scegliere **Configurazione > Impostazione dispositivo > Routing > RIP > Interfaccia** e scegliere l'interfaccia interna con il mouse. Fare clic su **Modifica**.



2. Selezionare la casella di controllo **Abilita chiave di autenticazione**, quindi immettere il valore **Key** e il valore **Key**



ID. Fare clic su **OK**, quindi su **Applica**.

Configurazione Cisco ASA CLI

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
```

Configurazione CLI del router Cisco IOS (R2)

Router Cisco IOS (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
```

Configurazione CLI del router Cisco IOS (R1)

Router Cisco IOS (R1)

```
router rip
 version 2
 network 172.16.0.0
```

```
no auto-summary
```

Configurazione CLI del router Cisco IOS (R3)

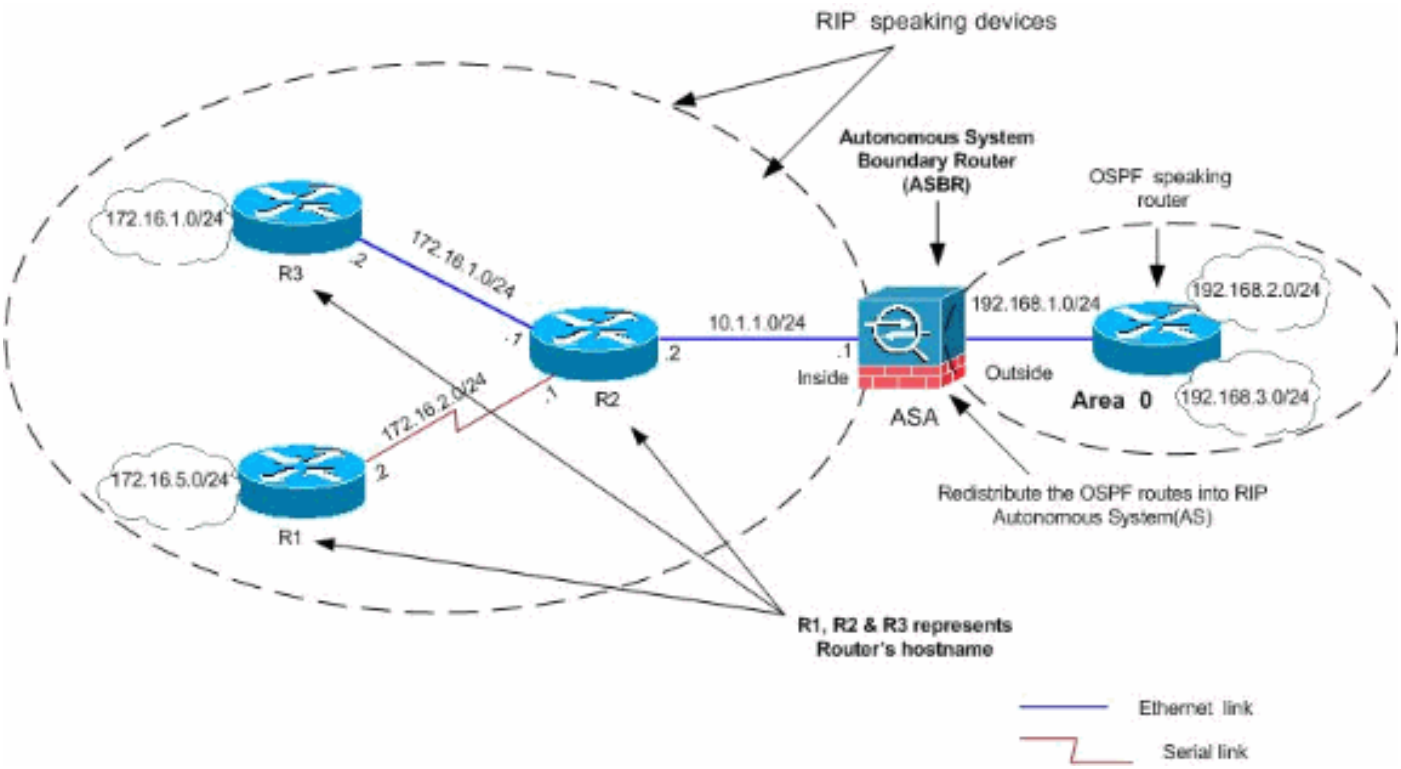
Router Cisco IOS (R3)

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

Ridistribuzione in RIP con ASA

Èpossibile ridistribuire le route dai processi di routing OSPF, EIGRP, statico e connesso nel processo di routing RIP.

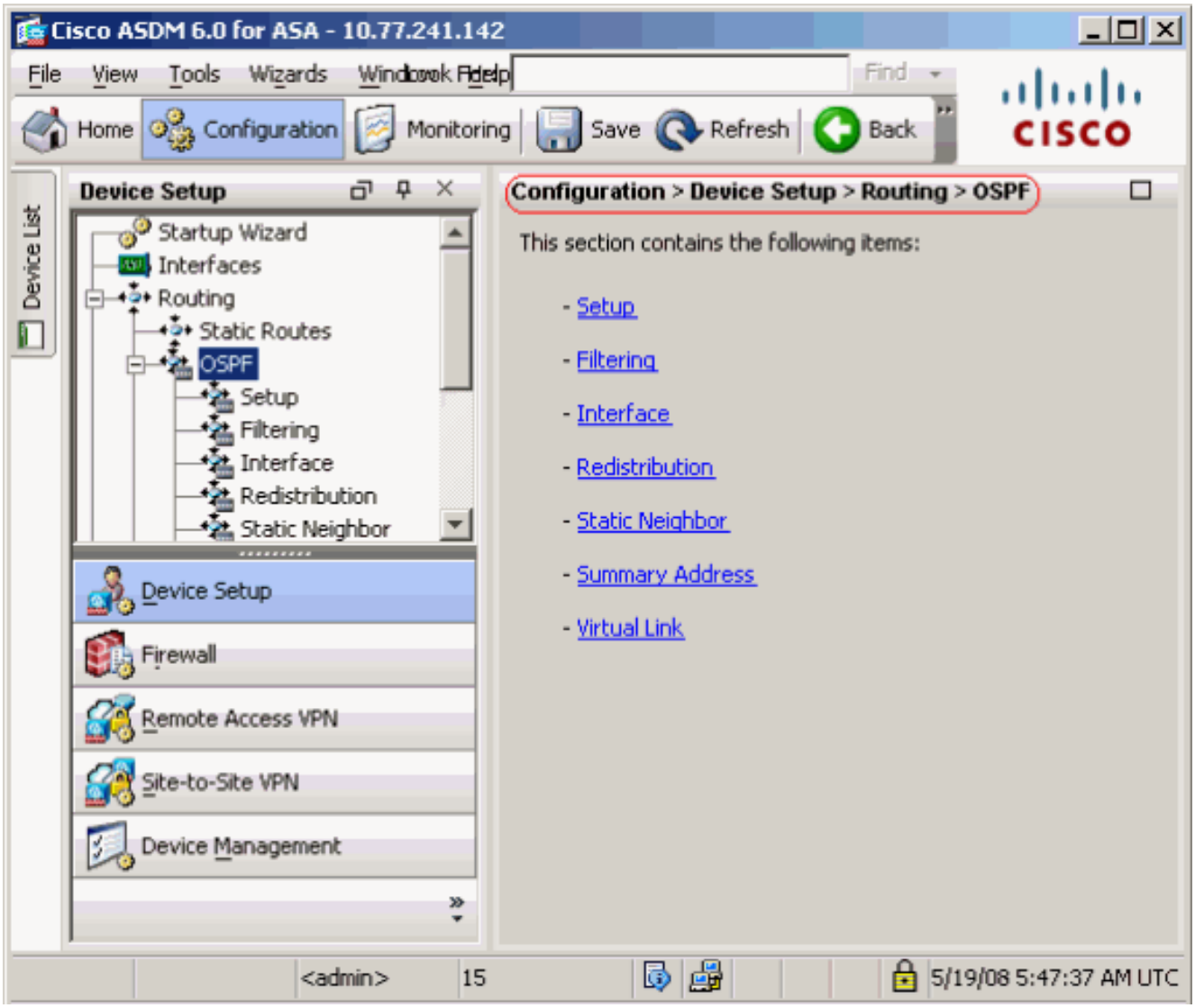
In questo esempio viene mostrata la ridistribuzione delle route OSPF in RIP con il diagramma di rete:



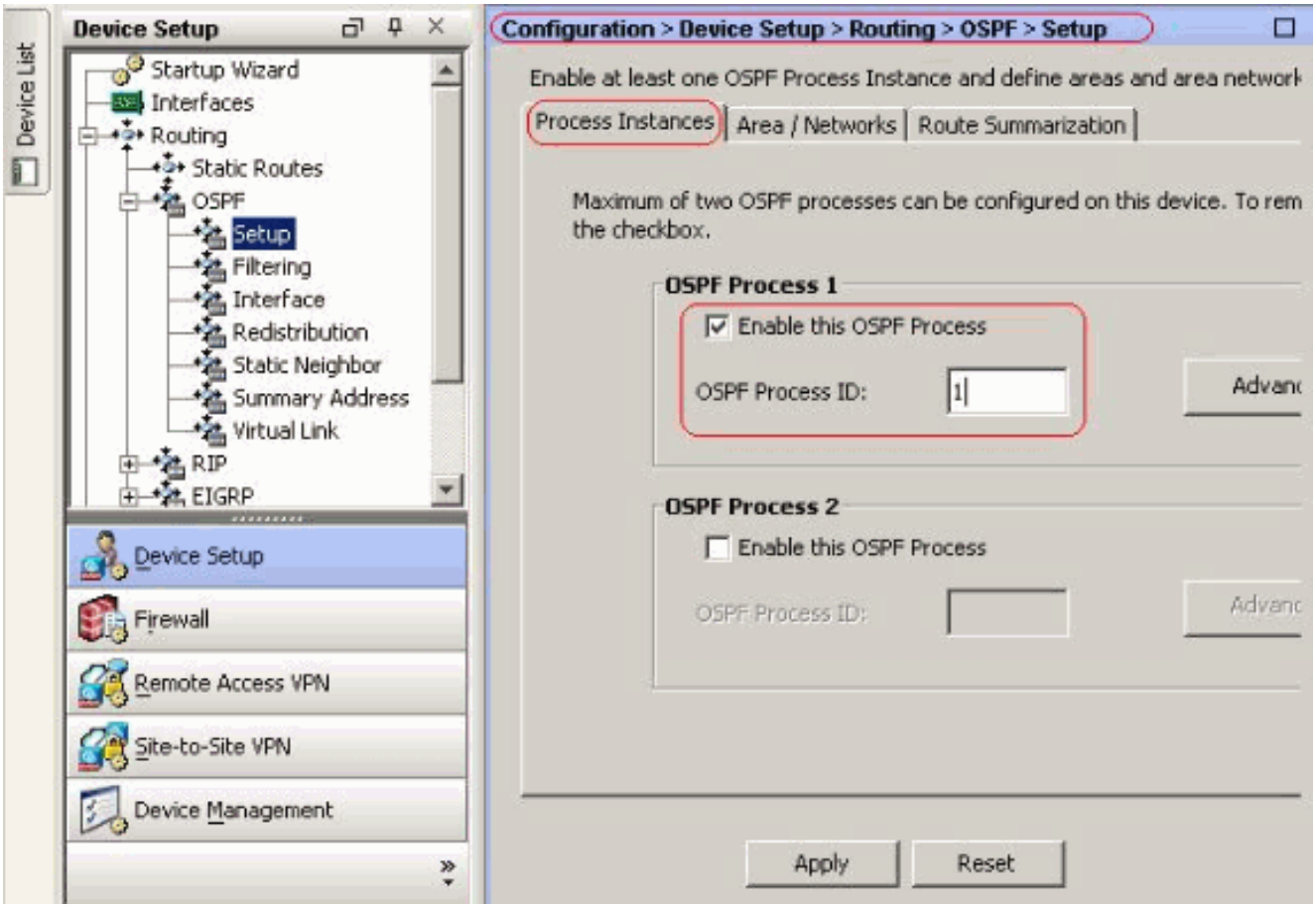
Configurazione ASDM

Attenersi alla seguente procedura:

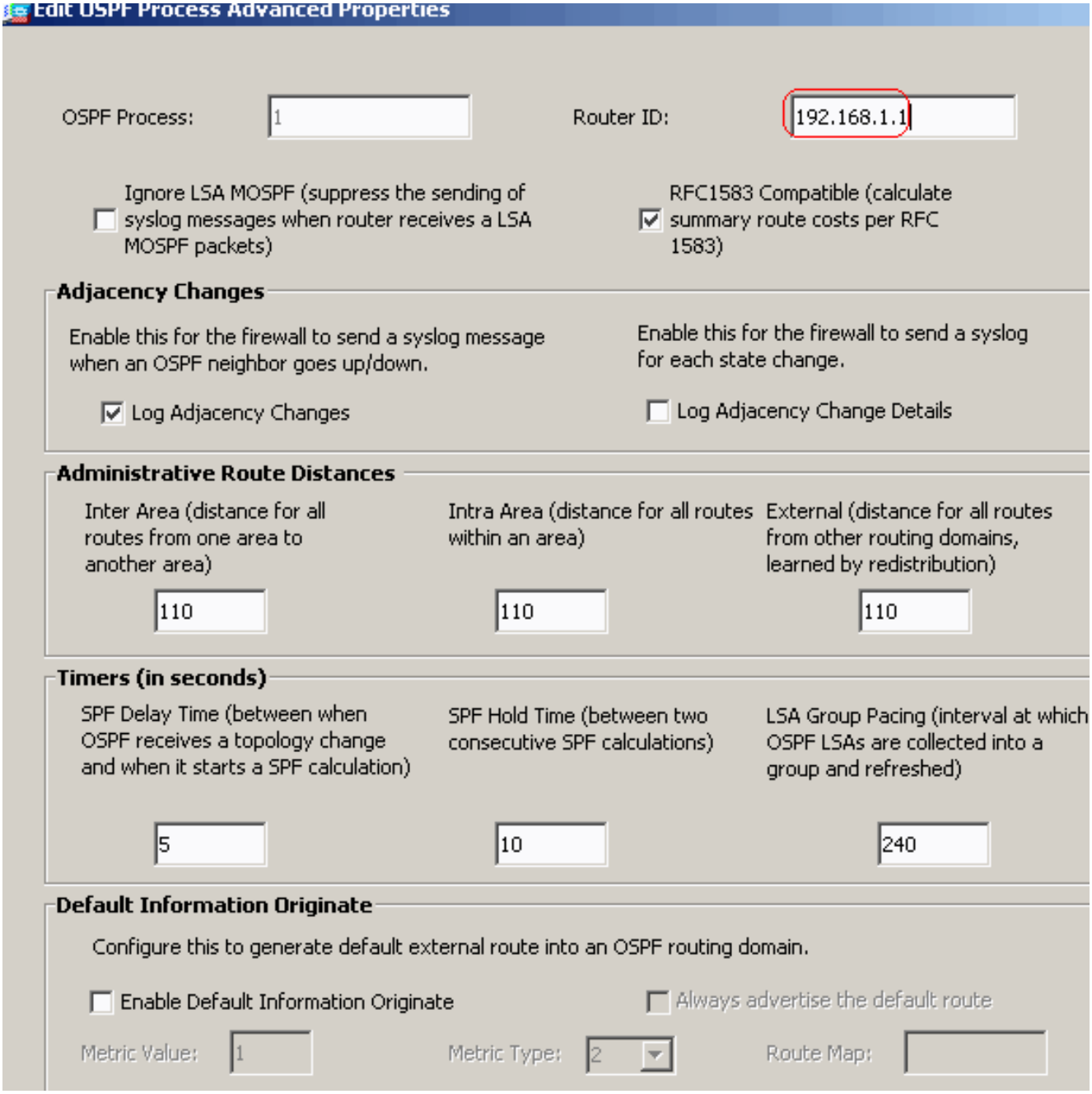
1. **Configurazione OSPF**Scegliere **Configurazione > Configurazione dispositivo > Routing > OSPF** nell'interfaccia ASDM, come mostrato nella schermata.



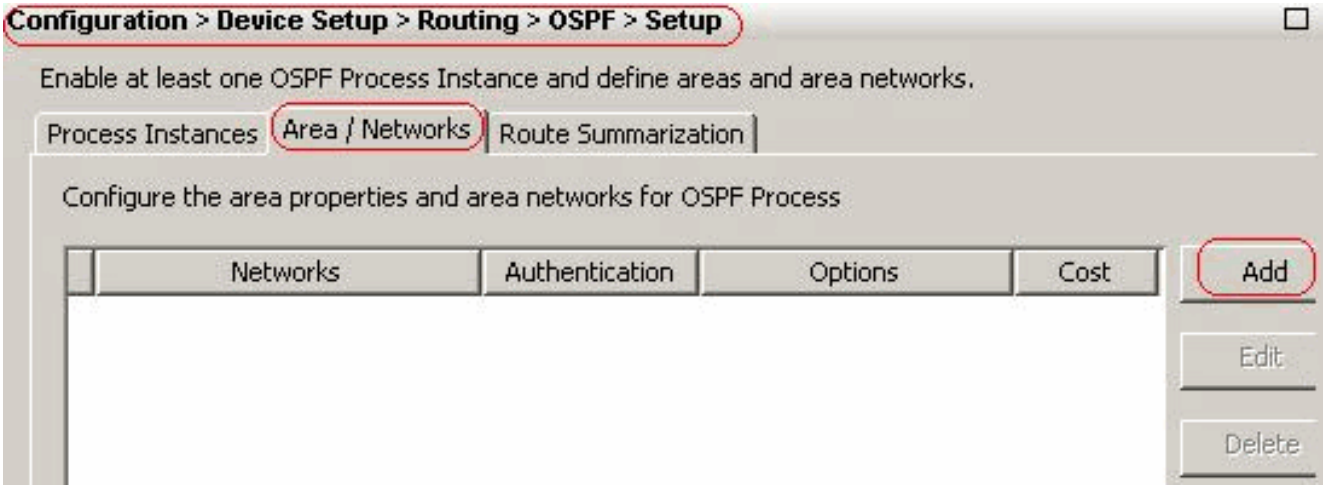
Abilitare il processo di routing OSPF nella scheda **Impostazione > Istanze processo**, come mostrato nella schermata. Nell'esempio, il processo ID OSPF è **1**.



Fare clic su **Avanzate** nella scheda **Impostazione > Istanze di processo** per configurare i parametri opzionali avanzati del processo di routing OSPF. È possibile modificare le impostazioni specifiche del processo, ad esempio l'ID del router, le modifiche alle adiacenze, le distanze di instradamento amministrativo, i timer e le impostazioni di origine delle informazioni
predefinite.

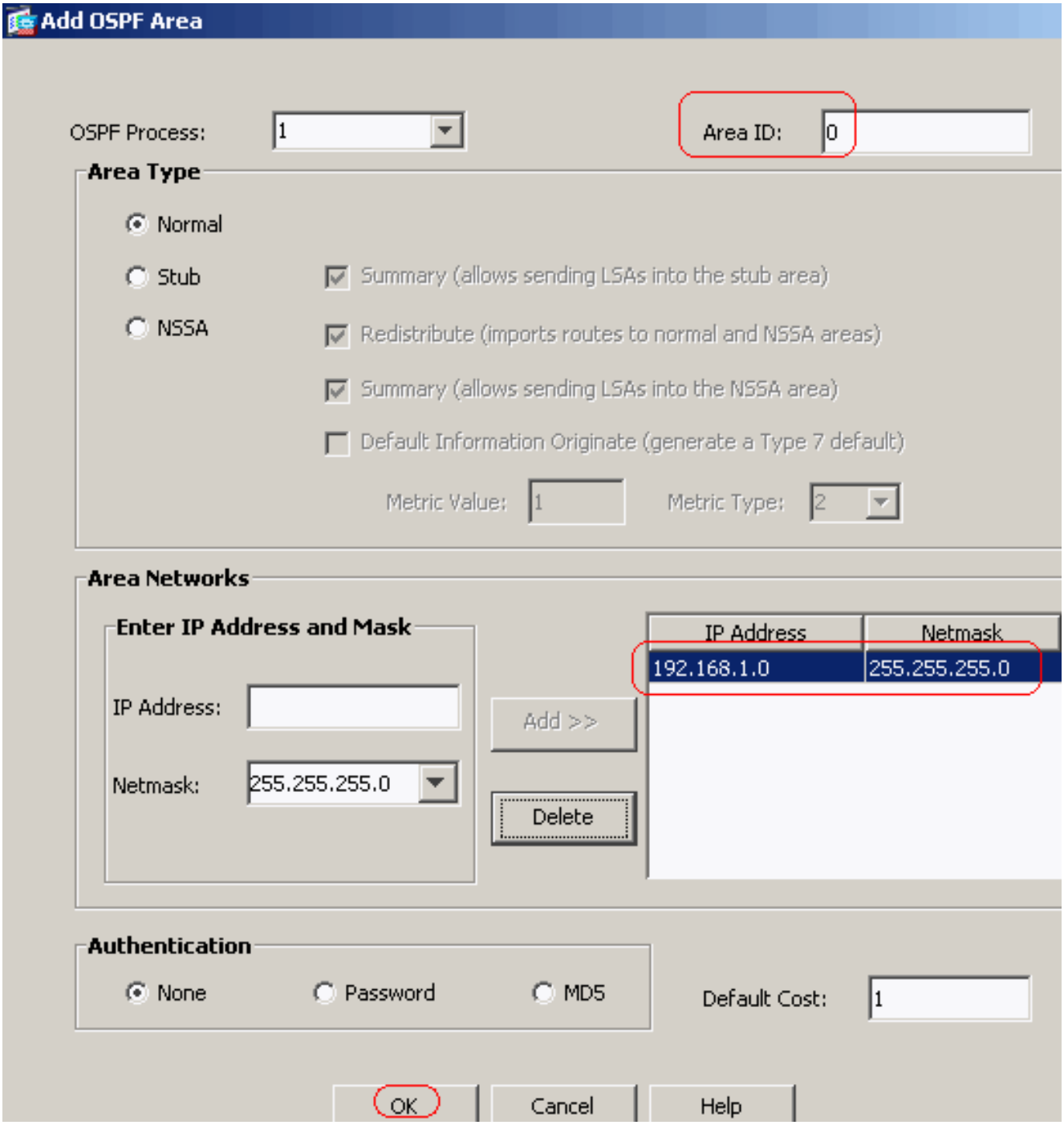


Fare clic su **OK**.Dopo aver completato i passaggi precedenti, definire le reti e le interfacce che partecipano al routing OSPF nella scheda **Imposta > Area/Reti**. Fare clic su **Add** (Aggiungi) come mostrato in questa schermata.

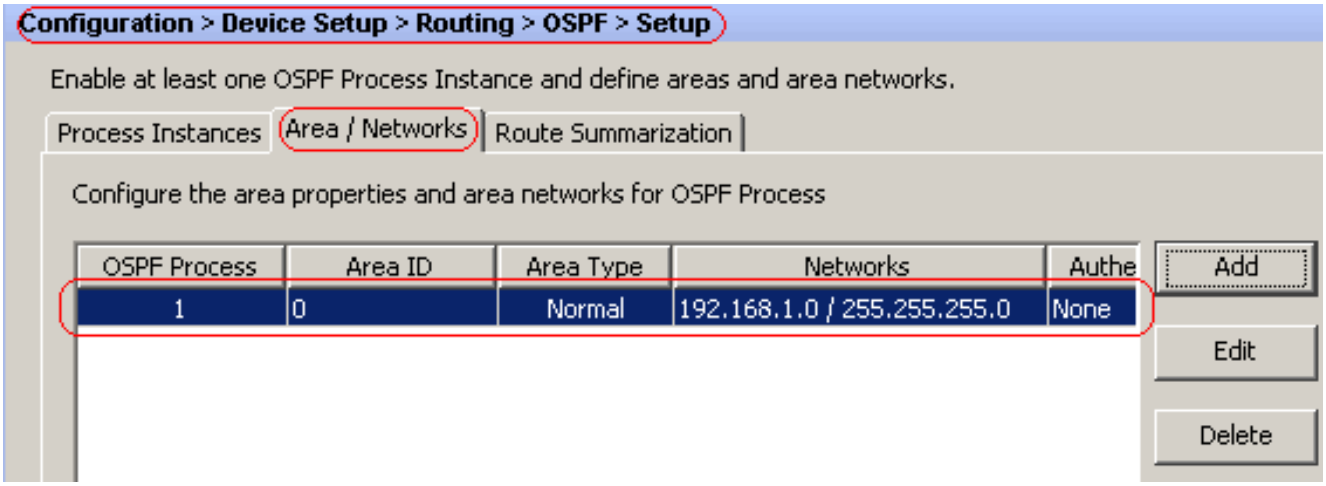


Viene visualizzata questa schermata. Nell'esempio, l'unica rete aggiunta è la rete esterna

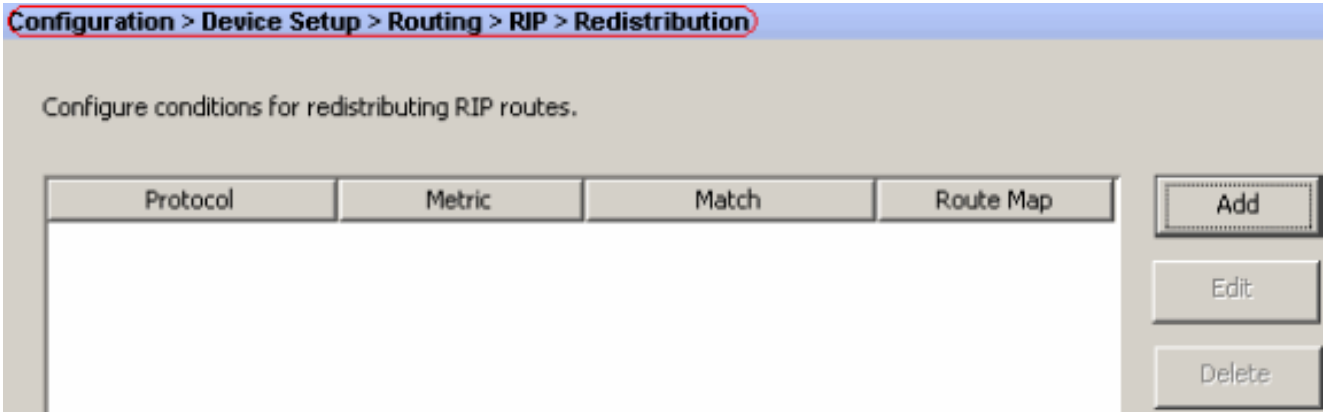
(192.168.1.0/24), in quanto OSPF è abilitato solo sull'interfaccia esterna.**Nota:** solo le interfacce con un indirizzo IP che rientrano nelle reti definite partecipano al processo di routing
OSPF.



Fare clic su **OK**.Fare clic su **Apply** (Applica).

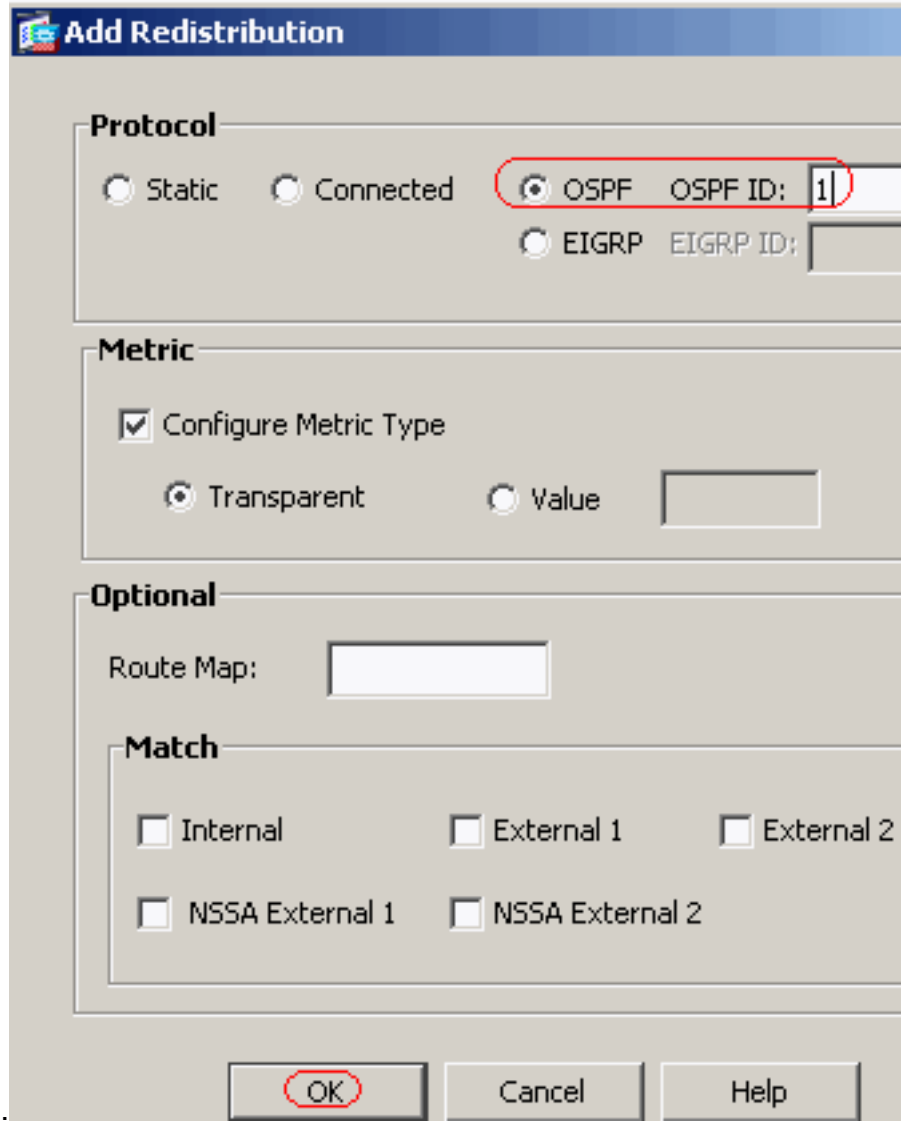


2. Scegliere **Configurazione > Configurazione dispositivo > Routing > RIP > Ridistribuzione > Aggiungi** per ridistribuire le route OSPF in RIP.



3. Fare clic su **OK**, quindi su

Applica.



Configurazione CLI equivalente

Configurazione CLI di ASA per la ridistribuzione di 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

Dopo aver ridistribuito le route OSPF in RIP AS, è possibile visualizzare la tabella di routing del router Cisco IOS (R2) adiacente.

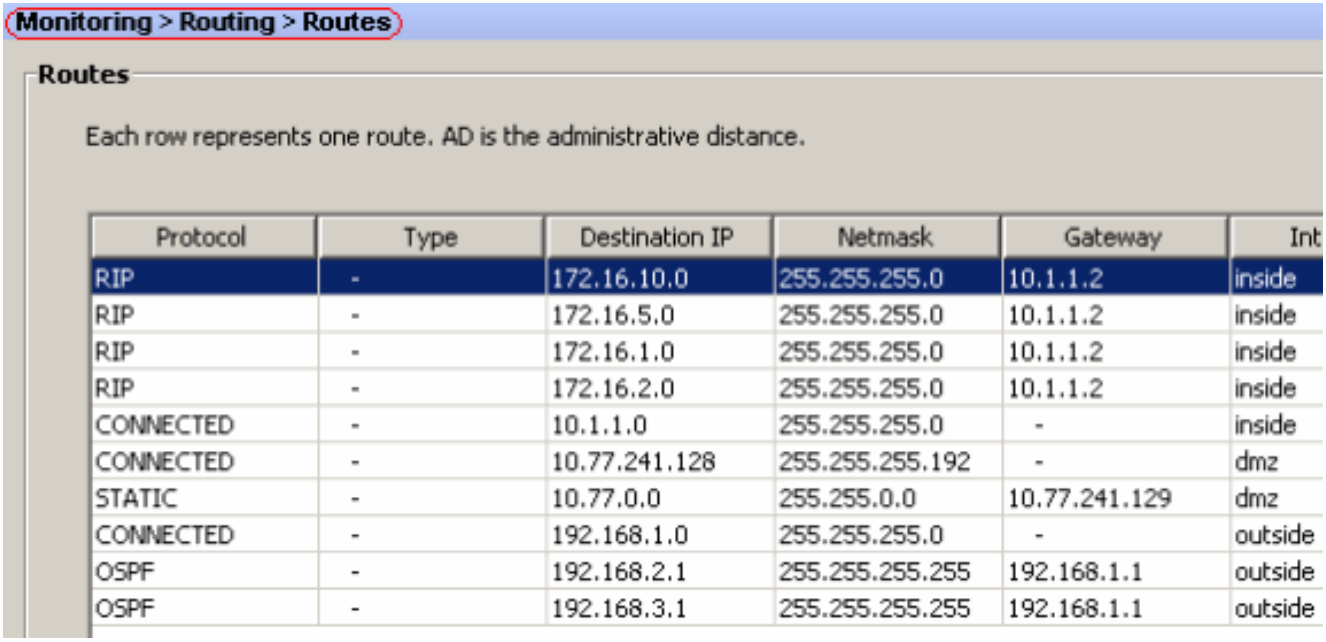
```
R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
        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
```

Verifica

Per verificare la configurazione, effettuare i seguenti passaggi:

1. Èpossibile verificare la tabella di instradamento selezionando **Controllo > Instradamento > Instradamenti**. In questa schermata è possibile vedere che le reti 172.16.1.0/24, 172.16.2.0/24, 172.16.5.0/24 e 172.16.10.0/24 vengono apprese tramite R2 (10.1.1.2) con RIP.



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. Dalla CLI, è possibile usare il comando **show route** per ottenere lo stesso output.

```
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#
```

Risoluzione dei problemi

In questa sezione vengono fornite informazioni sui comandi di debug che possono essere utili per risolvere i problemi relativi a OSPF.

Comandi per la risoluzione dei problemi

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Nota: consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug**.

- **debug rip events**: abilita il debug degli eventi RIP

```
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
```

Informazioni correlate

- Cisco serie 5500 Adaptive Security Appliance - Pagina di supporto
- Cisco serie 500 PIX Support Page
- PIX/ASA 8.X: Configurazione di EIGRP su Cisco Adaptive Security Appliance (ASA)
- Documentazione e supporto tecnico – Cisco Systems