ASA/PIX con el ejemplo de la configuración de RIP

Contenido

Introducción

Este documento explica cómo configurar Cisco ASA para aprender las rutas con el Routing Information Protocol (RIP), realiza la autenticación, y la redistribución.

Refiera al PIX/ASA 8.X: Configurar el EIGRP en el dispositivo de seguridad adaptante de Cisco (ASA) para más información sobre la configuración EIGRP.

Nota: Esta configuración del documento se basa en la versión de RIP 2.

Nota: El Asymmetric Routing no se soporta adentro ASA/PIX.

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Cisco ASA/PIX debe funcionar con la versión 7.x o posterior.
- El RIP no se soporta en el modo del multi-contexto; se soporta solamente en el modo simple.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Seguridad adaptante Appliance(ASA) de las Cisco 5500 Series que funciona con la versión de software 8.0 y posterior.
- Versión de software adaptante 6.0 de Manager(ASDM) del dispositivo de seguridad de Cisco y posterior.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Productos Relacionados

La información en este documento es también aplicable al firewall PIX de las Cisco 500 Series que funciona con la versión de software 8.0 y posterior.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Antecedentes

El RIP es un Distance Vector Routing Protocol que utiliza el conteo saltos como el métrico para la selección de trayecto. Cuando el RIP se habilita en una interfaz, el RIP de los intercambios de la interfaz transmite con los dispositivos de vecindad para aprender dinámicamente alrededor y hacer publicidad de las rutas.

La versión de RIP 1 de la versión de RIP 1 y de la versión de RIP 2. del soporte del dispositivo de seguridad no envía a la máscara de subred con la actualización de ruteo. La versión de RIP 2 envía a la máscara de subred con la actualización de ruteo y apoya a las máscaras de subred de longitud variable. Además, la versión de RIP 2 soporta la autenticación de vecino cuando se intercambian las actualizaciones de ruteo. Esta autenticación se asegura de que el dispositivo de seguridad reciba la información de ruteo confiable de una fuente confiable.

Limitaciones:

1. El dispositivo de seguridad no puede pasar las actualizaciones del RIP entre las interfaces.
2. La versión de RIP 1 no apoya a las máscaras de subred de longitud variable (VLS).

3. El RIP tiene una cuenta del salto máximo de 15. Una ruta con un conteo saltos mayor de 15 se considera inalcanzable.
4. La convergencia del RIP es relativamente lenta comparada a otros Routing Protocol.
5. Usted puede habilitar solamente un solo proceso del RIP en el dispositivo de seguridad.

Nota: Esta información se aplica a la versión de RIP 2 solamente:

1. Si usted utiliza la autenticación de vecino, la clave de autenticación y la clave ID deben ser lo mismo en todos los dispositivos vecinos que proporcionen la versión de RIP 2 actualizaciones a la interfaz.
2. Con la versión de RIP 2, el dispositivo de seguridad transmite y recibe las actualizaciones de la ruta predeterminado con el uso de la dirección Multicast 224.0.0.9. En el modo pasivo, recibe las actualizaciones de la ruta en ese direccionamiento.
3. Cuando la versión de RIP 2 se configura en una interfaz, registran a la dirección Multicast 224.0.0.9 en esa interfaz. Cuando una configuración de la versión de RIP 2 se quita de una interfaz, desregistran a esa dirección Multicast.

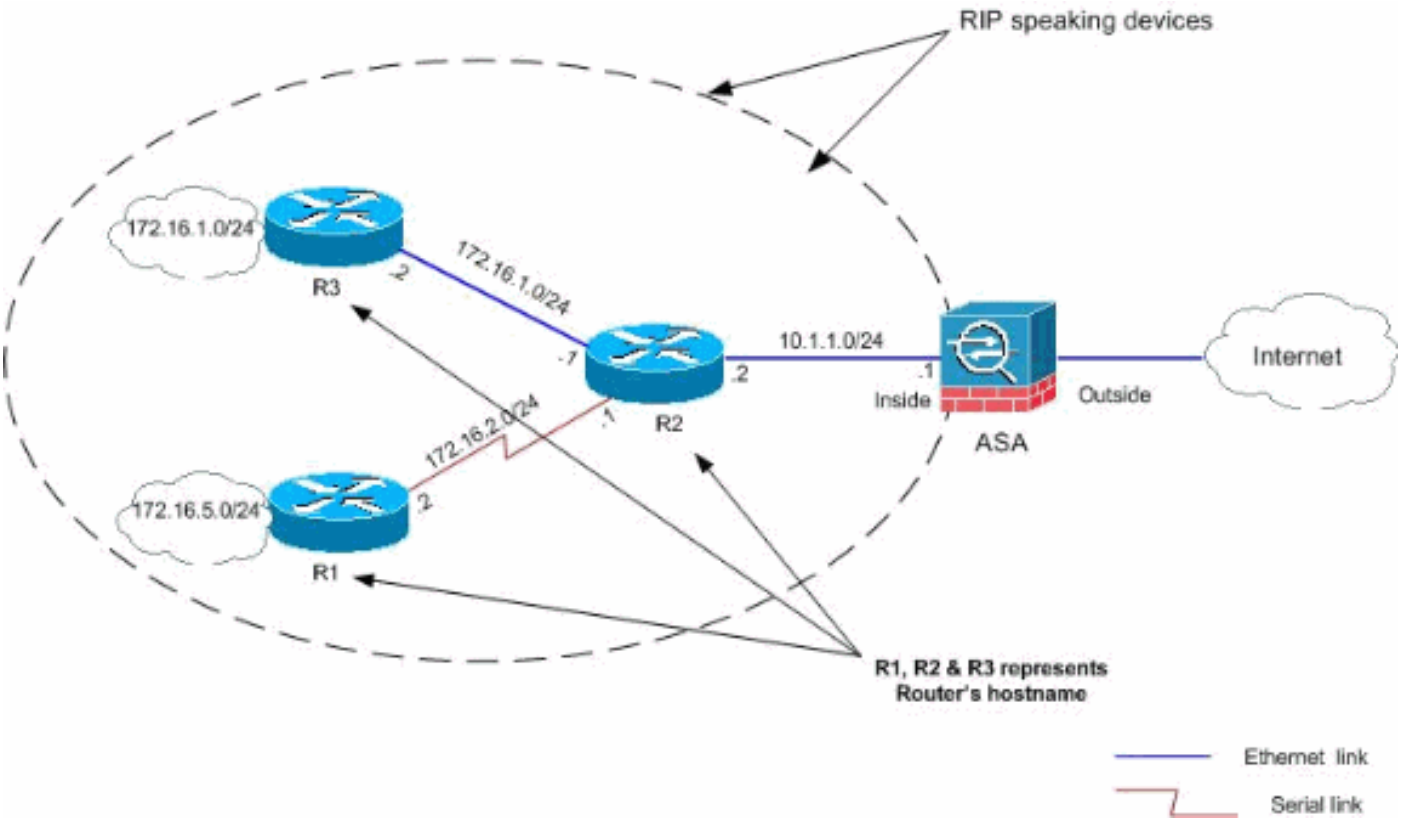
Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Configuraciones

En este documento, se utilizan estas configuraciones:

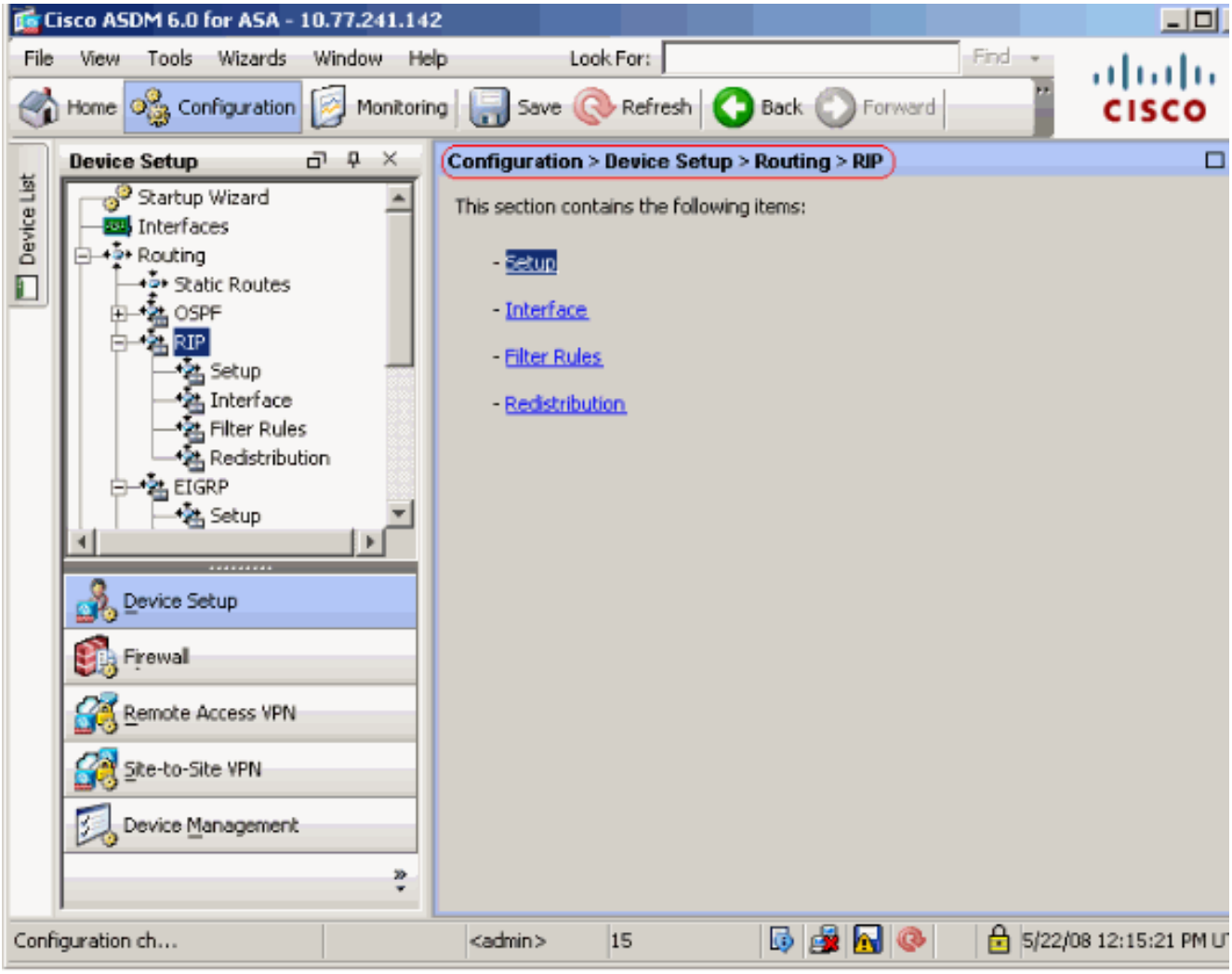
- Configuración de ASDM
- Autenticación del RIP de la configuración
- Configuración CLI de Cisco ASA
- Configuración CLI del router del Cisco IOS (r2)
- Configuración CLI del router del Cisco IOS (r1)
- Configuración CLI del router del Cisco IOS (R3)

Configuración de ASDM

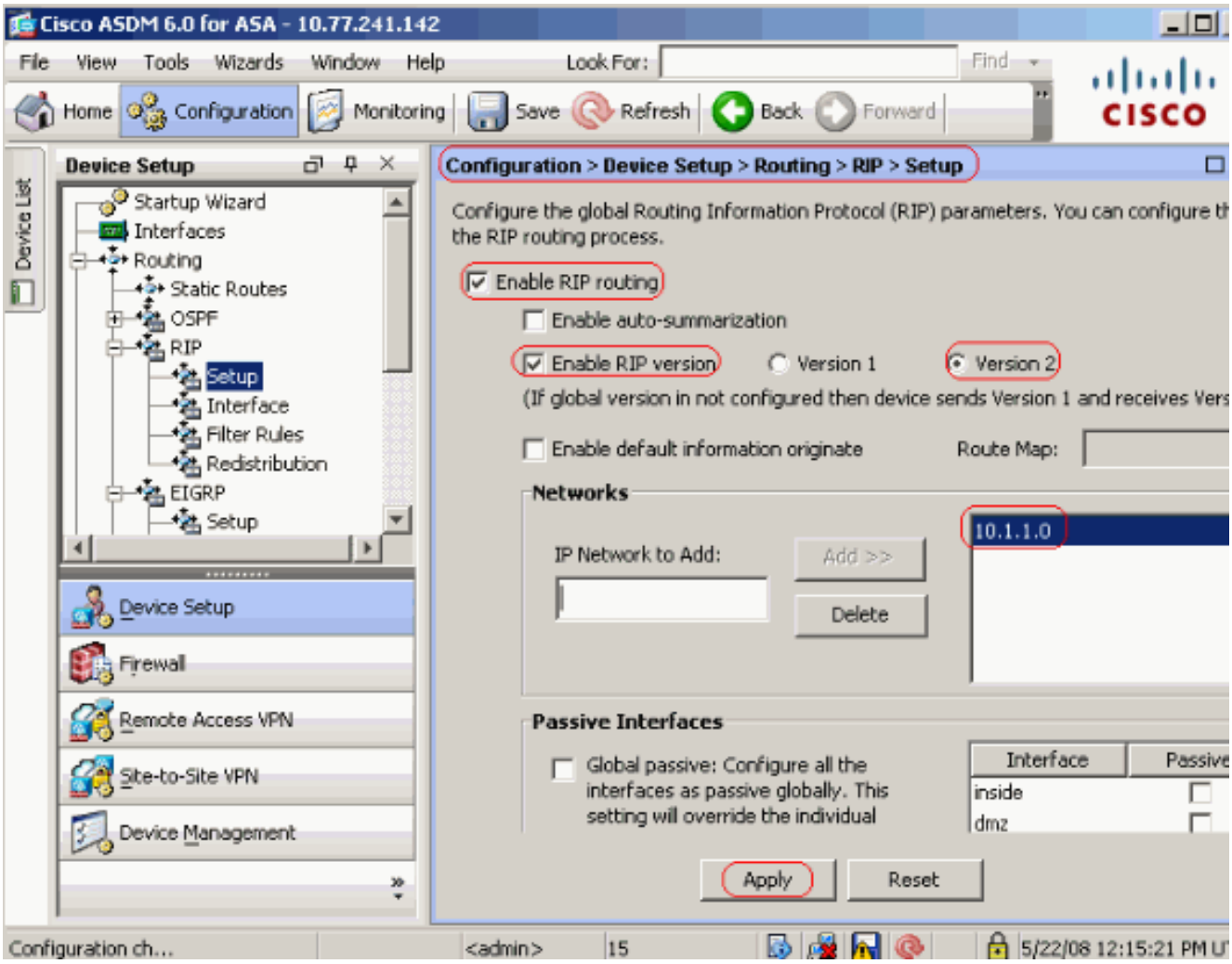
El Administrador de dispositivos de seguridad adaptante (ASDM) es aplicaciones basadas en el buscador usadas para configurar y monitorear el software en los dispositivos de seguridad. El ASDM se carga del dispositivo de seguridad, y después se utiliza para configurar, para monitorear, y para manejar el dispositivo. Usted puede también utilizar el activador de ASDM (Windows® solamente) para poner en marcha la aplicación ASDM más rápidamente que los subprogramas java. Esta sección describe la información que usted necesita configurar las características descritas en este documento con el ASDM.

Complete estos pasos para configurar el RIP en Cisco ASA:

1. Inicie sesión a Cisco ASA con el ASDM.
2. Elija la **configuración > la configuración > la encaminamiento > el RIP de dispositivo** en la interfaz del ASDM, tal y como se muestra en del tiro de pantalla.



3. Elija la **configuración > la configuración > la encaminamiento > el RIP de dispositivo > puesto** para habilitar el RIP que rutea como se muestra.Elija **rutear del RIP del permiso de la** casilla de verificación.Elija la **versión de RIP del permiso de la** casilla de verificación con la **versión 2 del** botón de radio.Bajo **redes** tabule, agregue la red **10.1.1.0**.Haga clic en Apply (Aplicar).



CamposEl rutear del RIP del permiso — Marque esta orden del inb de la casilla de verificación para habilitar el RIP que rutea en el dispositivo de seguridad. Cuando usted habilita el RIP, se habilita en todas las interfaces. Si usted marca esta casilla de verificación, ésta también habilita los otros campos en este cristal. Desmarque esta casilla de verificación para inhabilitar el RIP que rutea en el dispositivo de seguridad.Summarization auto del permiso — Borre esta casilla de verificación para inhabilitar el resumen de Route automático. Marque esta casilla de verificación para volver a permitir el resumen de Route automático. La versión de RIP 1 utiliza siempre el resumen automático. Usted no puede inhabilitar el resumen automático para la versión de RIP 1. Si usted utiliza la versión de RIP 2, usted puede apagar el resumen automático si usted desmarca esta casilla de verificación. Inhabilite el resumen automático si usted debe realizar la encaminamiento entre las subredes disconnected. Cuando se inhabilita el resumen automático, se hacen publicidad las subredes.Versión de RIP del permiso — Marque esta casilla de verificación para especificar la versión del RIP usada por el dispositivo de seguridad. Si se borra esta casilla de verificación, después el dispositivo de seguridad envía la versión de RIP 1 pone al día y valida las actualizaciones de la versión de RIP 1 y de la versión 2. Esta configuración se puede reemplazar sobre una base del por interface en el cristal de la interfaz.Versión 1 — Especifica que el dispositivo de seguridad envía y recibe solamente las actualizaciones de la versión de RIP 1. Cualquier actualización de la versión 2 recibida se cae.Versión 2 — Especifica que el dispositivo de seguridad envía y recibe solamente la versión de RIP 2 actualizaciones. Cualquier actualización de la versión 1 recibida se cae.La información predeterminada del permiso origina — Marque esta casilla de verificación para generar una ruta predeterminado en el proceso de ruteo del RIP. Usted puede configurar un Route Map que deba ser satisfecho antes de que la ruta predeterminado pueda ser generada.Route-

map — Ingrese el nombre del Route Map para aplicarse. El proceso de ruteo genera la ruta predeterminado si se satisface el Route Map.Red del IP a agregar — Define una red para el proceso de ruteo del RIP. El network number especificado no debe contener ninguna información de subred. No hay límite al número de red que usted puede agregar a la configuración del dispositivo de seguridad. Las actualizaciones de RIP Routing se envían y se reciben solamente a través de las interfaces en las redes específicadas. También, si la red de una interfaz no se especifica, la interfaz no se hace publicidad en ninguna actualizaciones del RIP.Agregue — Haga clic este botón para agregar la red específicada a la lista de redes.Cancelación — Haga clic este botón para quitar la red seleccionada de la lista de redesConfigure las interfaces como voz pasiva global — Marque esta casilla de verificación para fijar todas las interfaces en el dispositivo de seguridad al modo pasivo del RIP. El dispositivo de seguridad está atento el RIP que rutea los broadcasts en todas las interfaces y las aplicaciones que la información para poblar las tablas de ruteo pero no transmite las actualizaciones de ruteo. Utilice la tabla de las interfaces pasivas para fijar las interfaces específicas al RIP pasivo.Tabla de las interfaces pasivas — Enumera las interfaces configuradas en el dispositivo de seguridad. Marque la casilla de verificación en la columna pasiva para esas interfaces que usted quiere actuar en el modo pasivo. Las otras interfaces todavía envían y reciben los broadcasts del RIP.

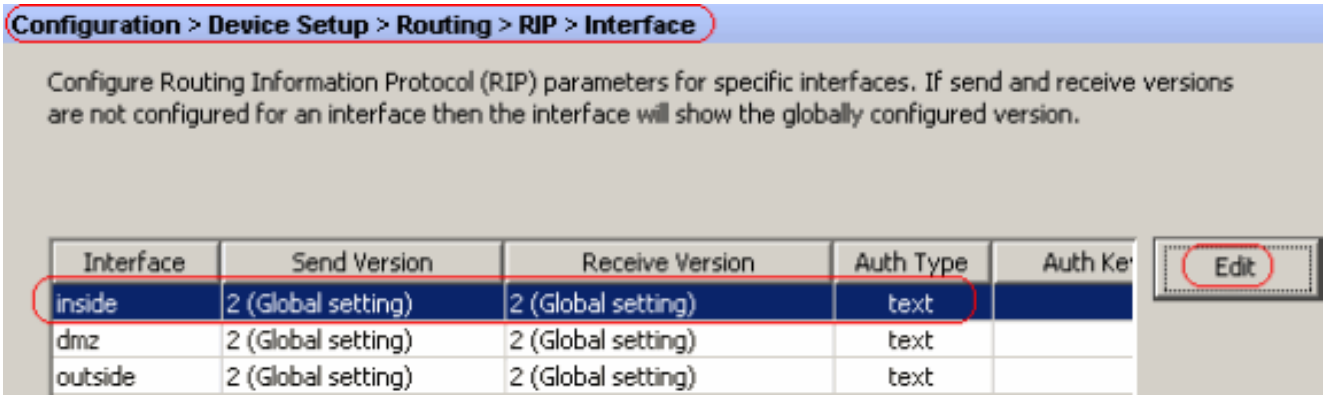
Autenticación del RIP de la configuración

Cisco ASA soporta autenticación de MD5 de las actualizaciones de ruteo del Routing Protocol del RIP v2. La publicación cerrada MD5 en cada paquete RIP previene la introducción de mensajes de ruteo desautorizados o falsos de las fuentes no aprobadas. La adición de autenticación a sus mensajes del RIP se asegura de que su Routers y Cisco ASA validen solamente los mensajes de ruteo de otros dispositivos de ruteo que se configuren con la misma clave previamente compartida. Sin esta autenticación configurada, si usted introduce otro dispositivo de ruteo con información de ruta diversa o contraria encendido a la red, las tablas de ruteo en su Routers o Cisco ASA pueden llegar a ser corruptas, y un establecimiento de rechazo del servicio puede seguir. Cuando usted agrega la autenticación a los mensajes del RIP enviados entre sus dispositivos de ruteo, que incluye el ASA, previene la adición útil o accidental de otro router a la red y a cualquier problema.

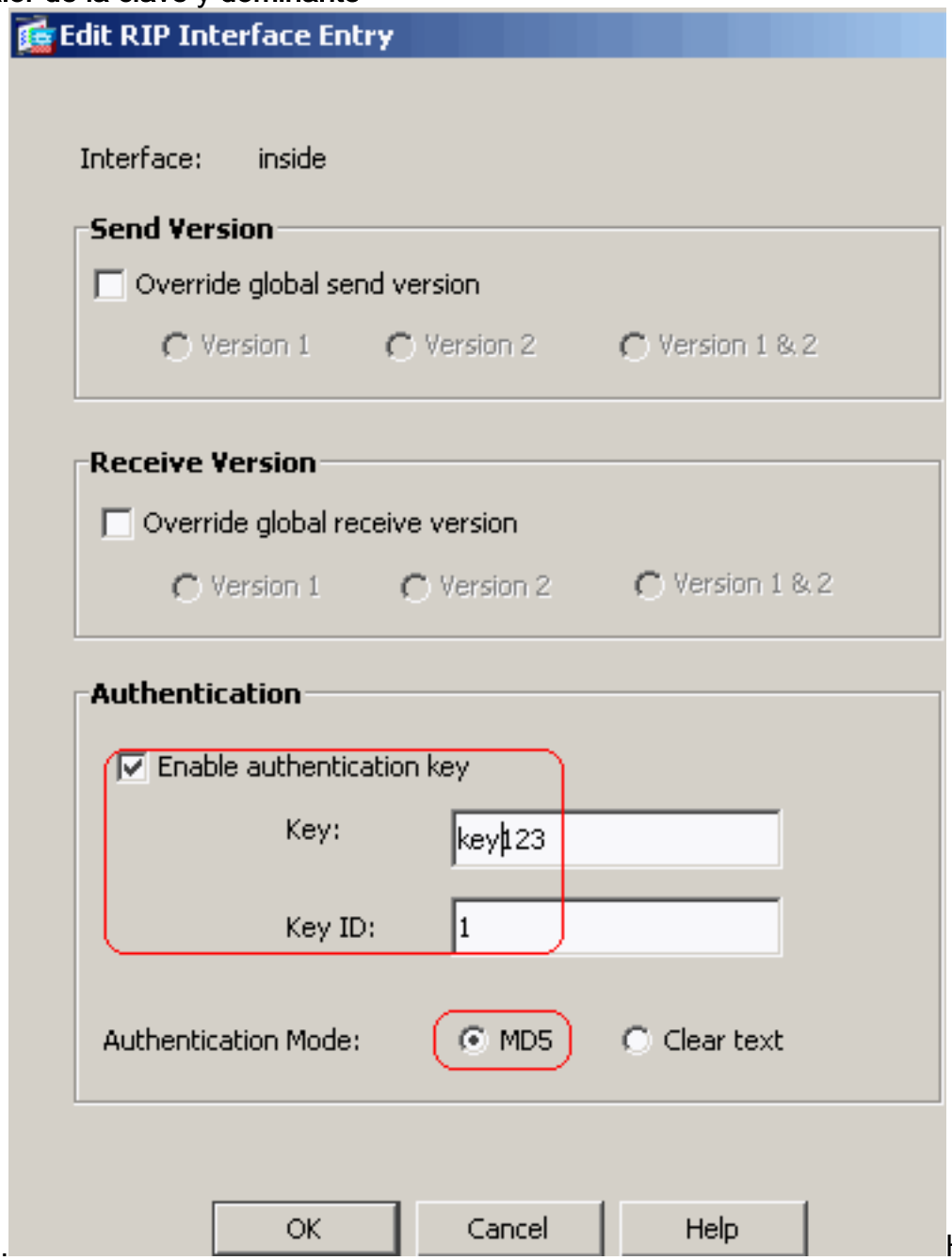
La autenticación del RIP Route se configura sobre una base del por interface. Todos RASGAN a los vecinos en las interfaces configuradas para la autenticación del mensaje del RIP se deben configurar con el mismo modo de autenticación y clave.

Complete estos pasos para habilitar el RIP autenticación de MD5 en Cisco ASA.

1. En el ASDM, elija la **configuración > la configuración > la encaminamiento > el RIP > la interfaz de dispositivo** y elija la interfaz interior con el ratón. Haga clic en **Editar**.



2. Elija el checkbox de la **clave de autenticación del habilitar** y después ingrese el valor del **valor de la clave** y **dominante**



ID. Haga clic en OK y en **Apply**.

Configuración CLI de Cisco ASA

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
```

Configuración CLI del router del Cisco IOS (r2)

Router del 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
```

Configuración CLI del router del Cisco IOS (r1)

Router del Cisco IOS (r1)

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

Configuración CLI del router del Cisco IOS (R3)

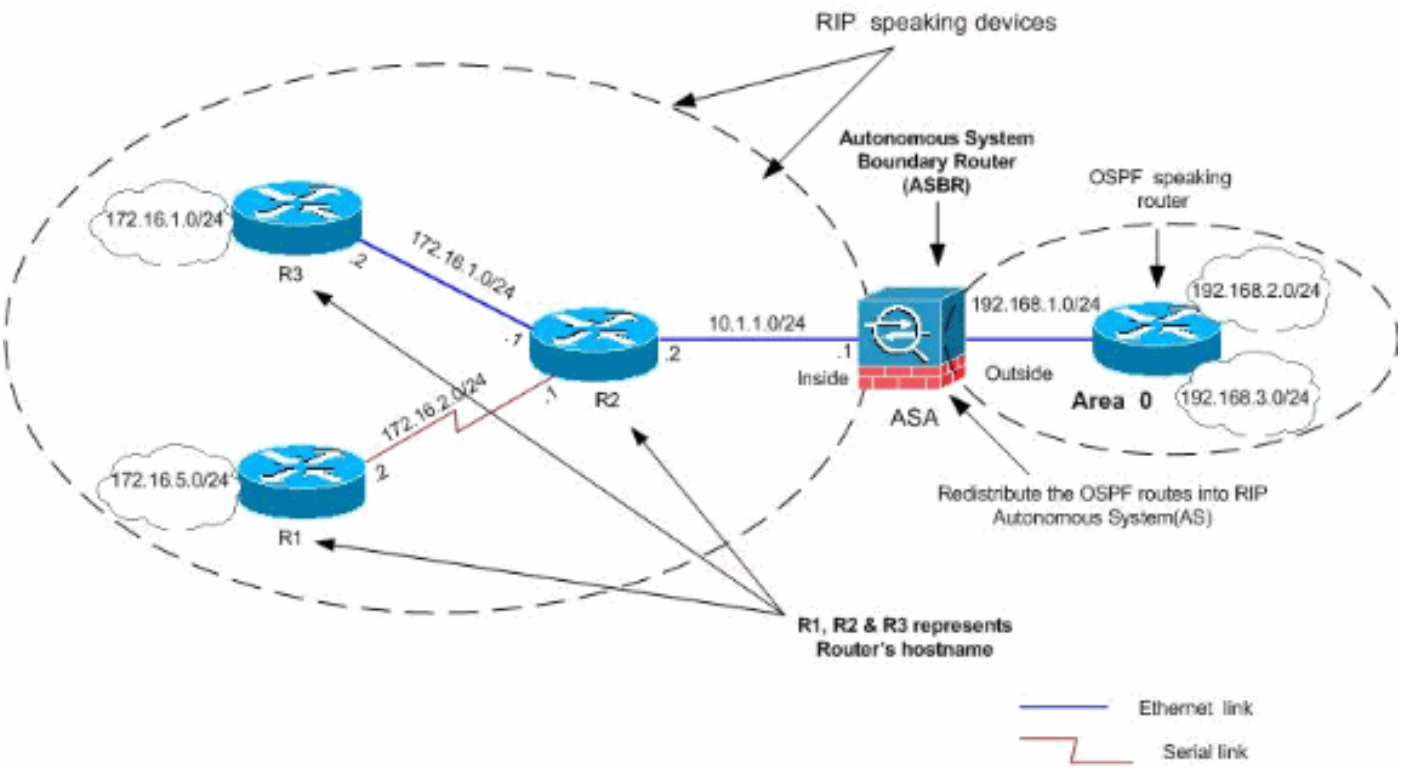
Router del Cisco IOS (R3)

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

Redistribuya en el RIP con el ASA

Usted puede redistribuir las rutas del OSPF, del EIGRP, de los parásitos atmosféricos, y de los procesos de ruteo conectados en el proceso de ruteo del RIP.

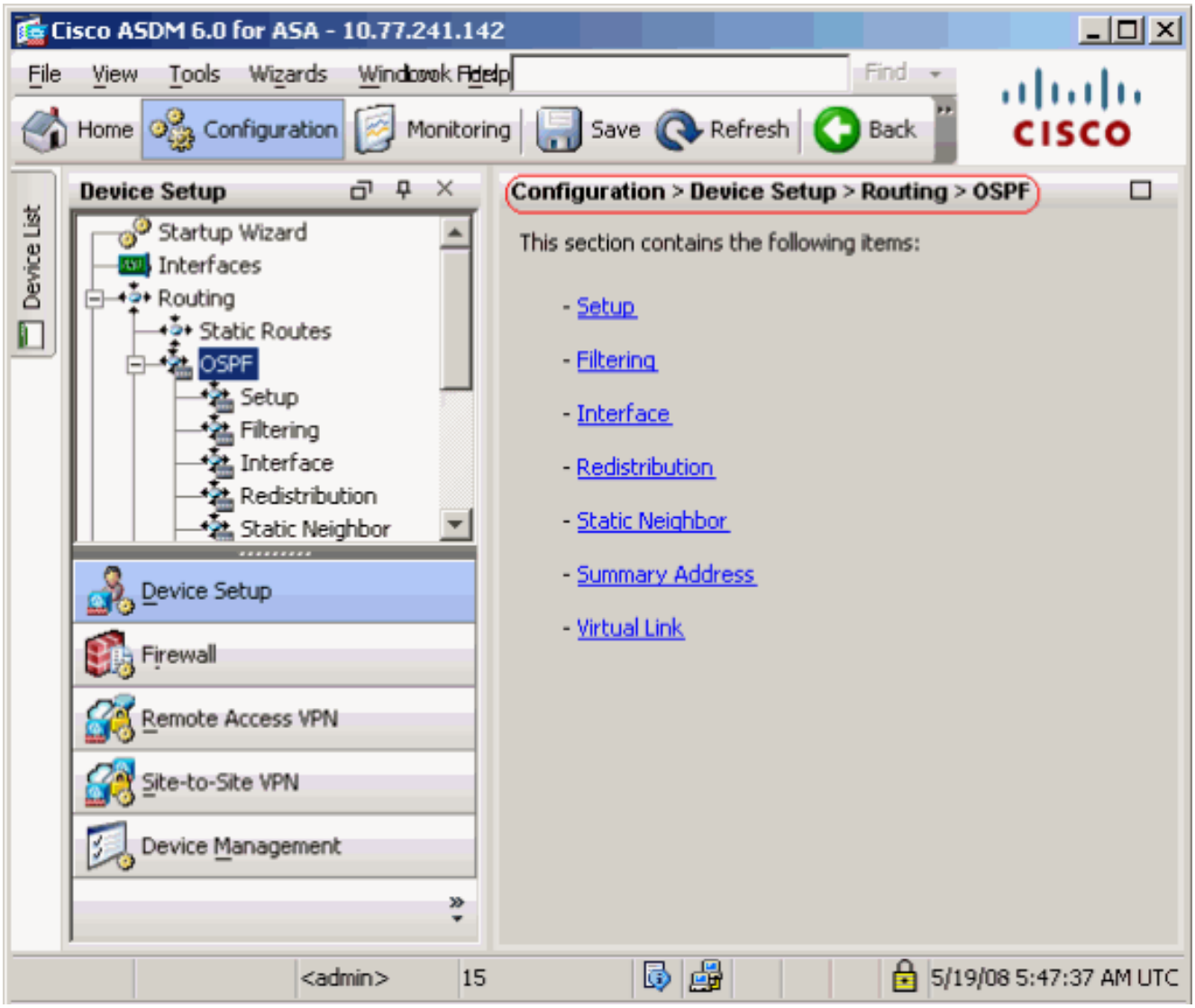
En este ejemplo, la redistribución de las OSPF rutas en el RIP con el diagrama de la red se muestra:



Configuración de ASDM

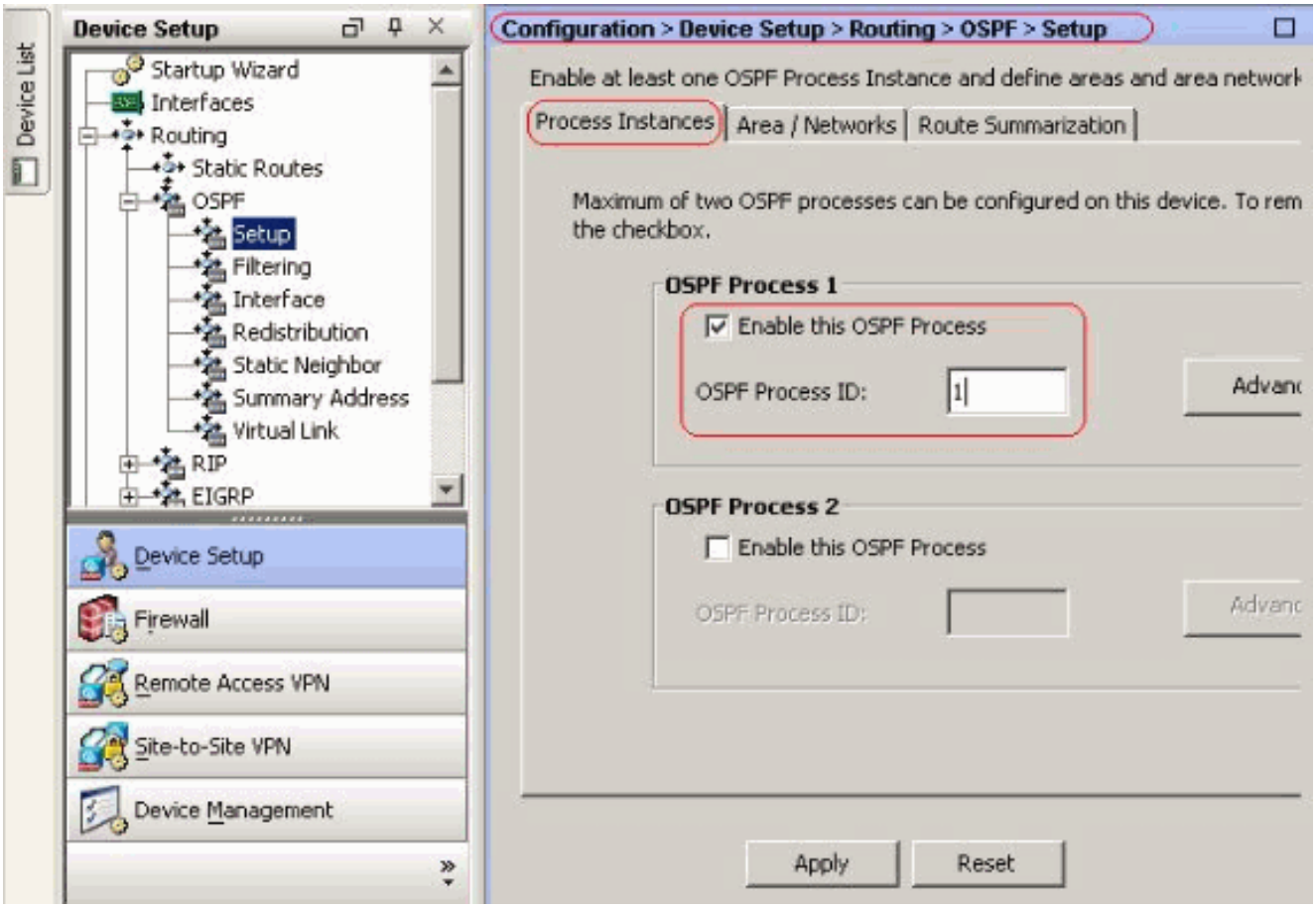
Complete estos pasos:

1. **Configuración de OSPF**Elija la **configuración > la configuración > la encaminamiento > el OSPF de dispositivo** en la interfaz del ASDM, tal y como se muestra en del tiro de pantalla.

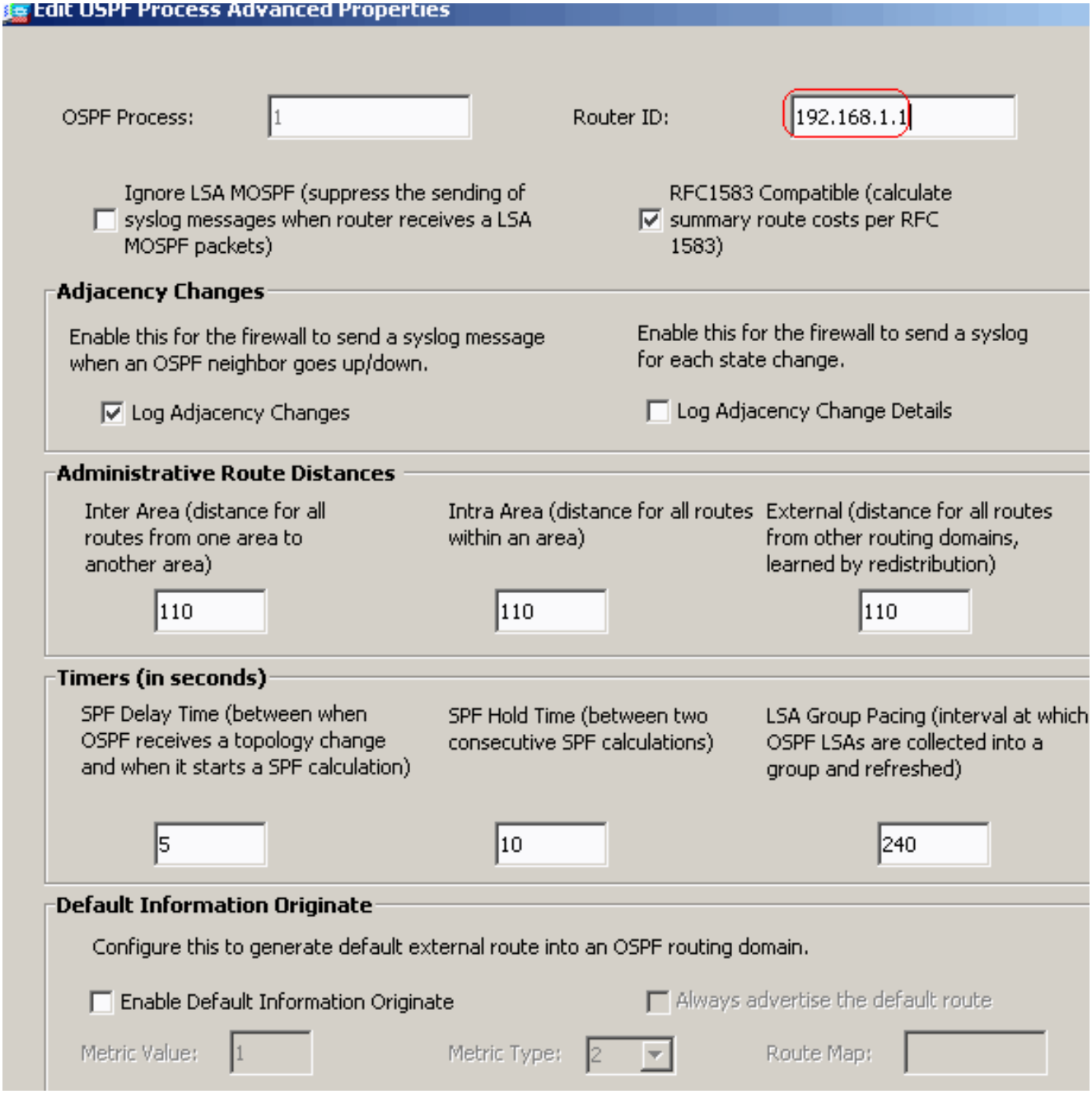


Habilite el proceso de ruteo de OSPF en la lengueta de los **casos de la configuración > del proceso**, tal y como se muestra en del tiro de pantalla. En este ejemplo, el proceso OSPF ID es

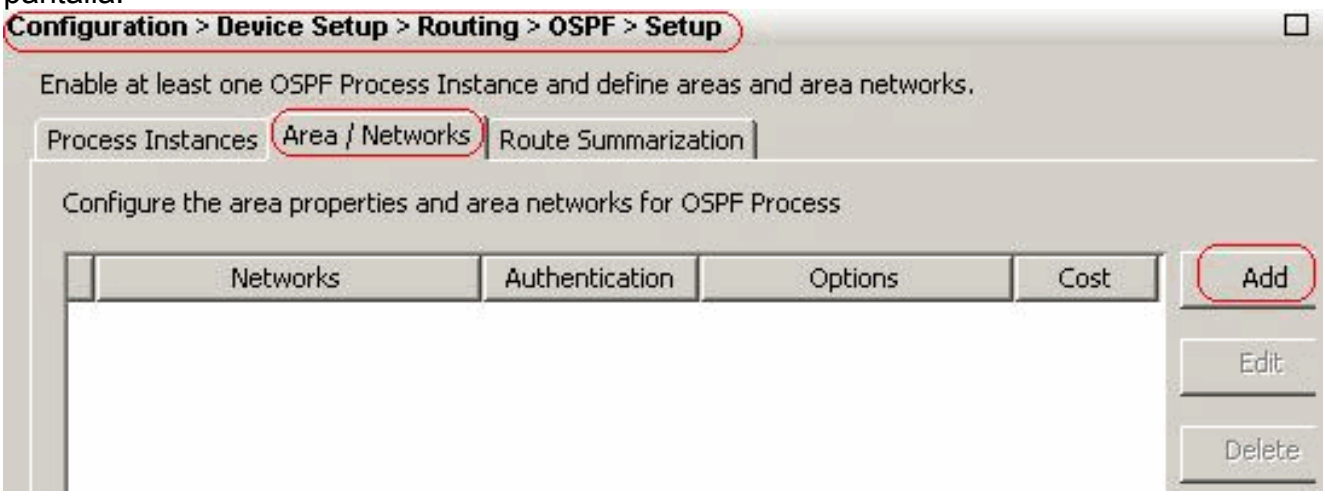
1.



El tecleo **avanzado** en los **casos de la configuración > del proceso** tabula para configurar los parámetros de proceso de ruteo de OSPF avanzados opcionales. Usted puede editar las configuraciones proceso-específicas, tales como el Router ID, los cambios de la adyacencia, las distancias administrativas de la ruta, los temporizadores, y la información predeterminada origina las
configuraciones.

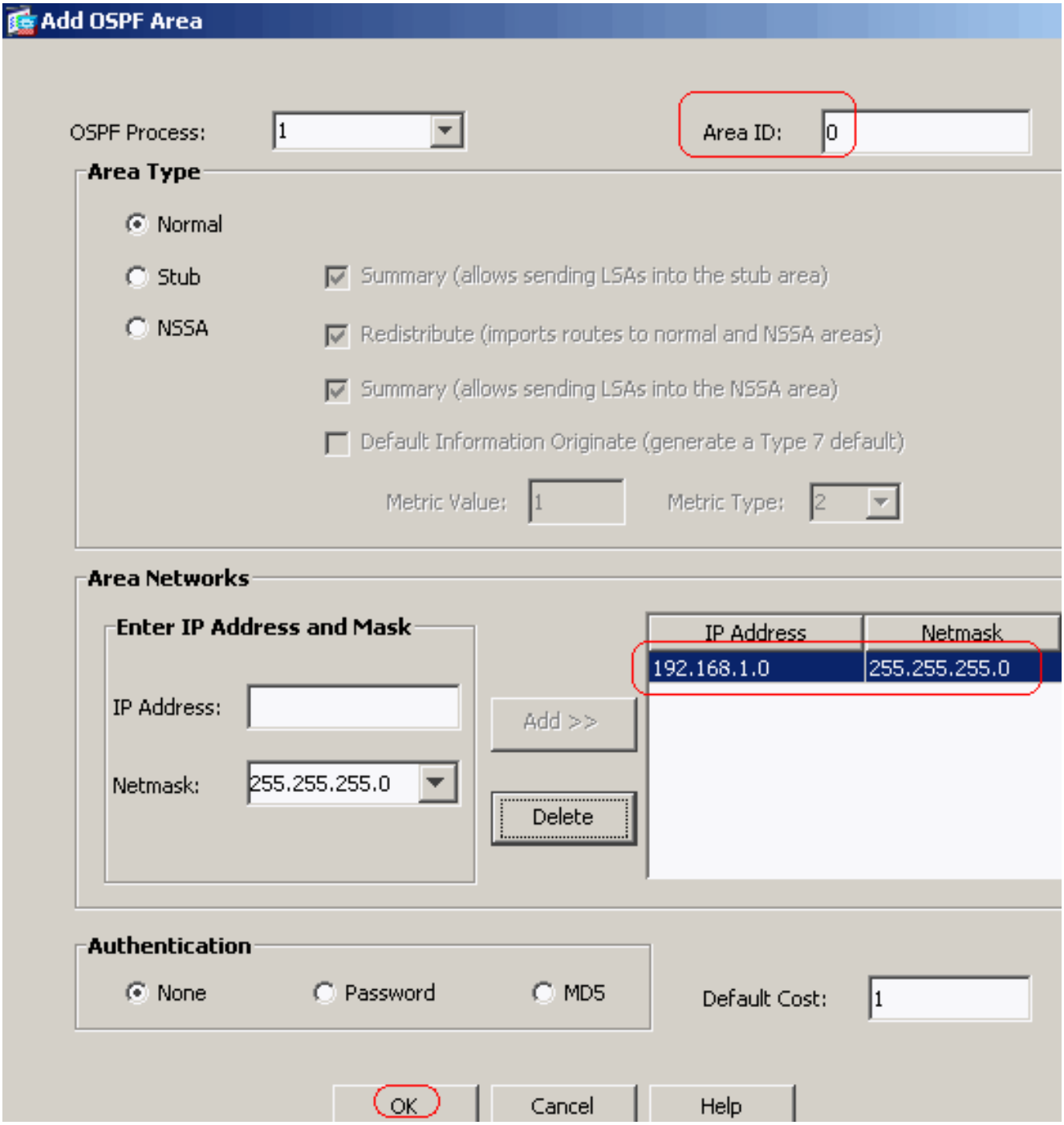


Haga clic en OK.Después de que usted complete los pasos anteriores, defina las redes y las interfaces que participan en el OSPF Routing en tecleo del cuadro de la **configuración > del área/de las redes agregan** tal y como se muestra en de este tiro de pantalla.

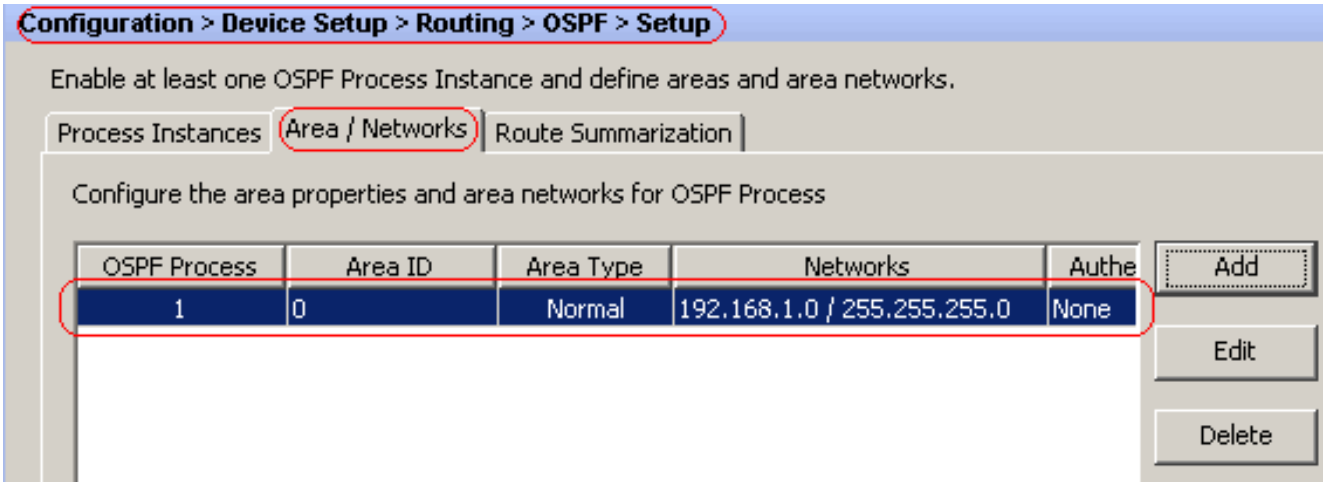


Esta pantalla aparece. En este ejemplo, la única red que agregamos es la red externa

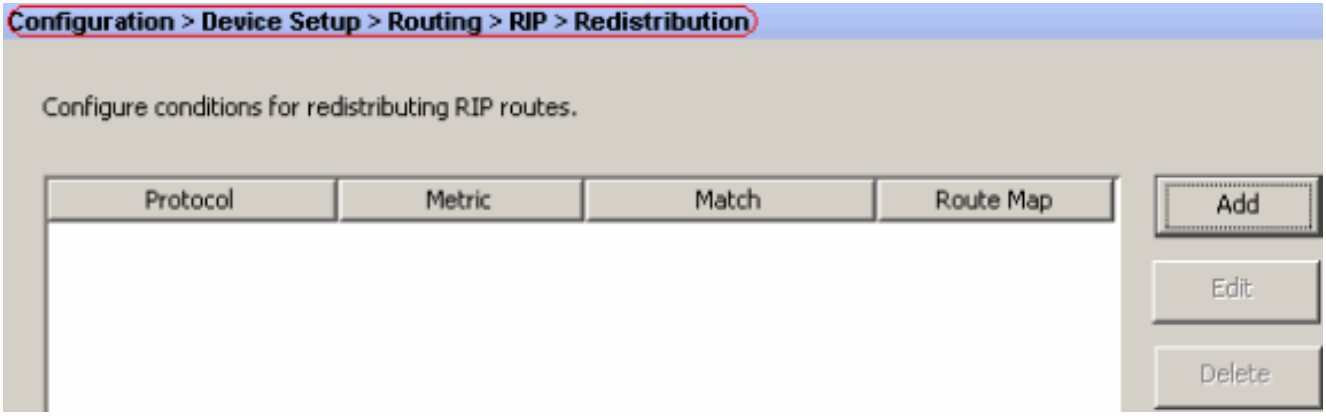
(192.168.1.0/24) puesto que el OSPF se habilita solamente en la interfaz exterior.**Nota:** Interconecta solamente con una dirección IP que baja dentro de las redes definidas participa en el proceso de ruteo de OSPF.



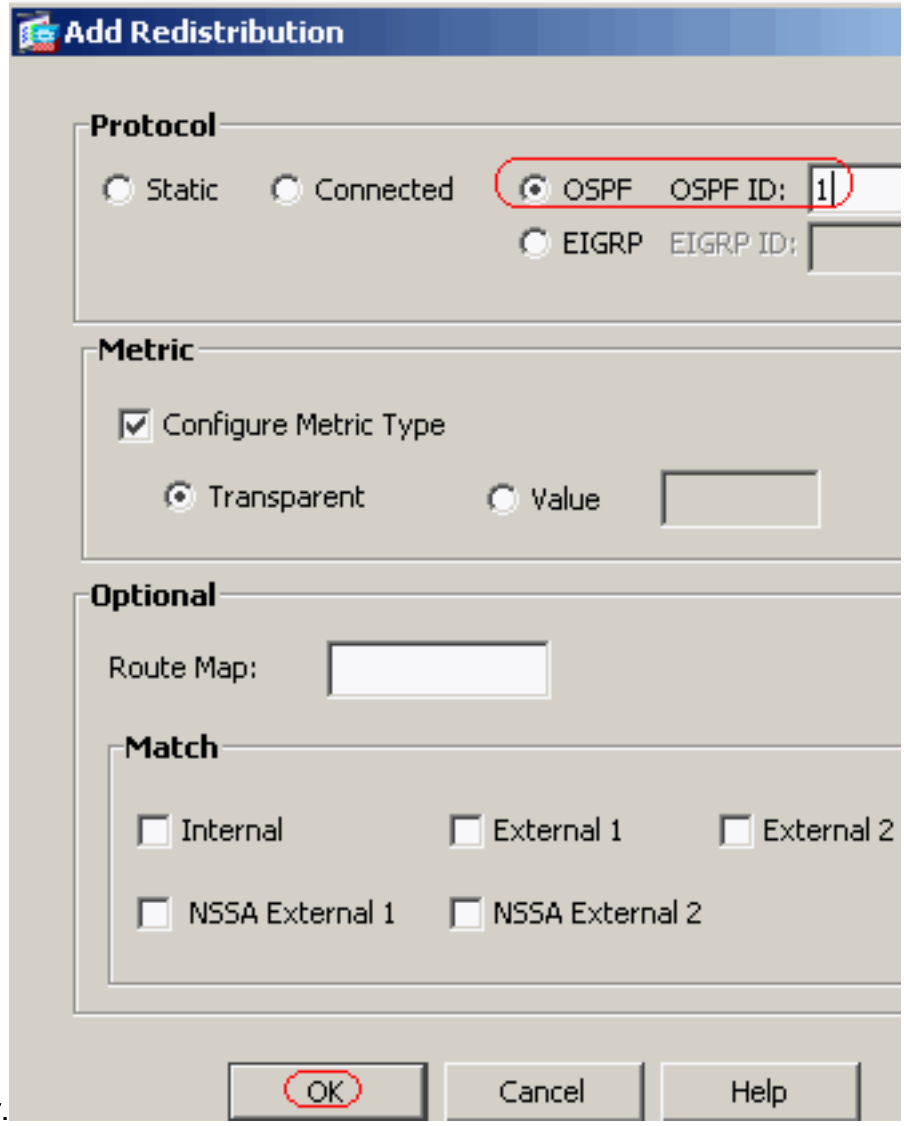
Haga clic en OK.Haga clic en Apply (Aplicar).



2. Elija la **configuración > la configuración > la encaminamiento > el RIP > la redistribución de dispositivo > Add** para redistribuir las OSPF rutas en el RIP.



3. Haga clic en OK y en **Apply**.



Configuración CLI equivalente

La configuración CLI del ASA para redistribuye el OSPF en el RIP COMO
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

Usted puede ver la tabla de ruteo del Cisco IOS vecino Router(R2) después de redistribuir las OSPF rutas en el RIP COMO.

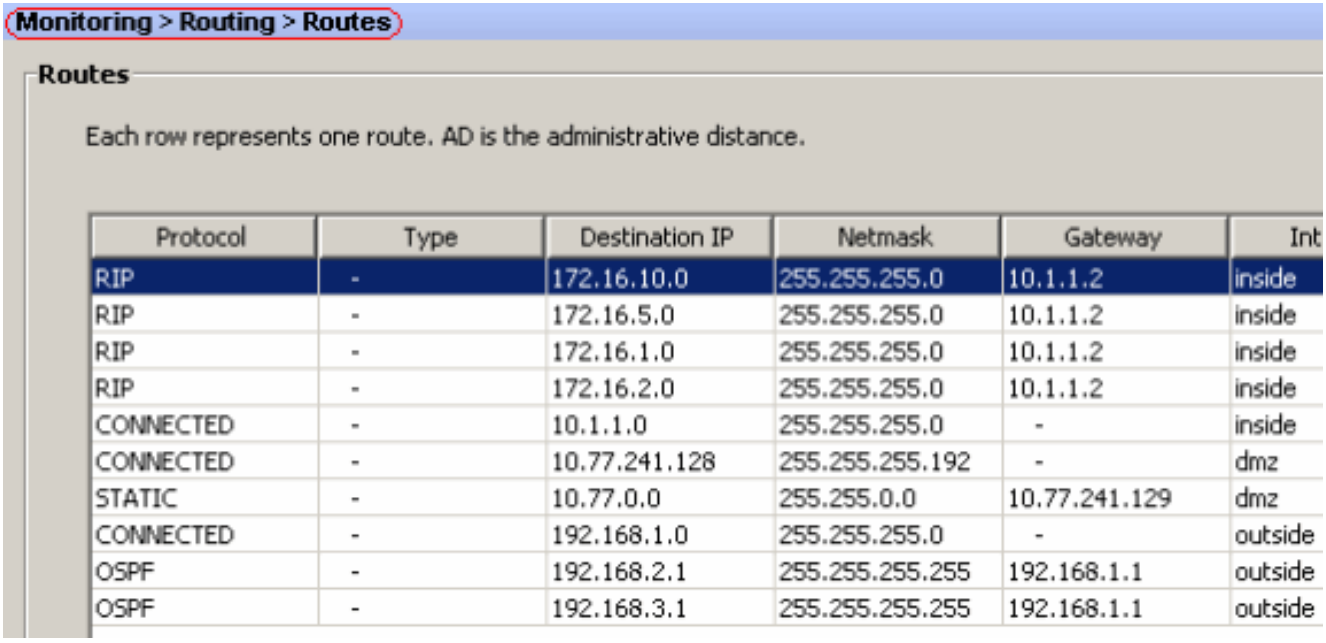
R2#**show ip route** Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP i - IS-IS, su - IS-IS 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
```

Verificación

Complete estos pasos para verificar su configuración:

1. Usted puede verificar la tabla de ruteo si usted navega a **monitorear > encaminamiento > las rutas**. En este tiro de pantalla, usted puede ver que las 172.16.1.0/24, 172.16.2.0/24, 172.16.5.0/24 y 172.16.10.0/24 redes son doctas con el r2 (10.1.1.2) con el 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. Del CLI, usted puede utilizar el **comando show route** para conseguir la misma salida.

```
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#
```

Troubleshooting

Esta sección incluye la información sobre los comandos debug que pueden ser útiles para resolver problemas los problemas OSPF.

Comandos para resolución de problemas

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Nota: Consulte Información Importante sobre Comandos de Debug antes de usar un **comando**

debug.

- **haga el debug de los eventos del RIP** — Habilita el debugging de los eventos del 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
```

Información Relacionada

- Página de Soporte de Cisco 5500 Series Adaptive Security Appliance
- Página del soporte de PIX de las Cisco 500 Series
- PIX/ASA 8.X: Configurando el EIGRP en el dispositivo de seguridad adaptante de Cisco (ASA)
- Soporte Técnico y Documentación - Cisco Systems