

Ejemplo de Configuración de ASA/PIX con OSPF

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Productos Relacionados](#)

[Convenciones](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Configuración de ASDM](#)

[Configuración de la Autenticación OSPF](#)

[Configuración de Cisco ASA CLI](#)

[Configuración CLI del router Cisco IOS \(R2\)](#)

[Configuración CLI del router Cisco IOS \(R1\)](#)

[Configuración CLI del router Cisco IOS \(R3\)](#)

[Redistribución en OSPF con ASA](#)

[Verificación](#)

[Troubleshoot](#)

[Configuración de Vecino Estático para la Red Punto a Punto](#)

[Comandos para resolución de problemas](#)

[Información Relacionada](#)

[Introducción](#)

Este documento describe cómo configurar Cisco ASA para aprender las rutas a través de OSPF (Open Shortest Path First), realizar la autenticación y la redistribución.

Consulte [PIX/ASA 8.X: Configuración de EIGRP en Cisco Adaptive Security Appliance \(ASA\)](#) para obtener más información sobre la configuración de EIGRP.

Nota: El ruteo asimétrico no se soporta en ASA/PIX.

[Prerequisites](#)

[Requirements](#)

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Cisco ASA/PIX debe ejecutar la versión 7.x o posterior.
- OSPF no se soporta en el modo multicontexto; solo se admite en modo único.

Componentes Utilizados

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

- Cisco 5500 Series Adaptive Security Appliance (ASA) que ejecuta la versión de software 8.0 y posteriores
- Software Cisco Adaptive Security Device Manager (ASDM) versión 6.0 y posterior

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Productos Relacionados

La información en este documento también es aplicable al Cisco 500 Series PIX firewall que ejecuta 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

OSPF usa un algoritmo de estado de link para construir y calcular la ruta más corta a todos los destinos conocidos. Cada router en un área OSPF contiene una base de datos de estado de link idéntica, que es una lista de cada una de las interfaces utilizables del router y de los vecinos alcanzables.

Las ventajas de OSPF sobre RIP incluyen:

- Las actualizaciones de la base de datos de estado de link OSPF se envían con menos frecuencia que las actualizaciones RIP, y la base de datos de estado de link se actualiza instantáneamente en lugar de gradualmente a medida que se agota el tiempo de espera de la información obsoleta.
- Las decisiones de ruteo se basan en el costo, lo que indica la sobrecarga necesaria para enviar paquetes a través de una interfaz determinada. El dispositivo de seguridad calcula el costo de una interfaz en función del ancho de banda del link en lugar del número de saltos al destino. El costo se puede configurar para especificar las rutas preferidas.

La desventaja de los algoritmos de ruta más corta primero es que requieren muchos ciclos de CPU y memoria.

El dispositivo de seguridad puede ejecutar dos procesos de protocolo OSPF simultáneamente, en diferentes conjuntos de interfaces. Puede que desee ejecutar dos procesos si tiene interfaces que

utilizan las mismas direcciones IP (NAT permite que estas interfaces coexistan, pero OSPF no permite direcciones superpuestas). O puede que desee ejecutar un proceso en el interior y otro en el exterior, y redistribuir un subconjunto de rutas entre los dos procesos. Del mismo modo, es posible que deba separar las direcciones privadas de las públicas.

Puede redistribuir las rutas en un proceso de ruteo OSPF desde otro proceso de ruteo OSPF, un proceso de ruteo RIP o desde rutas estáticas y conectadas configuradas en interfaces habilitadas para OSPF.

El dispositivo de seguridad soporta estas funciones OSPF:

- Compatibilidad con rutas internas, interzonales y externas (tipo I y tipo II).
- Compatibilidad con un link virtual.
- Inundación OSPF LSA.
- Autenticación a paquetes OSPF (tanto contraseña como autenticación MD5).
- Soporte para configurar el dispositivo de seguridad como un router designado o un router de respaldo designado. El dispositivo de seguridad también se puede configurar como ABR. Sin embargo, la capacidad de configurar el dispositivo de seguridad como ASBR se limita a la información predeterminada solamente (por ejemplo, inyectando una ruta predeterminada).
- Soporte para áreas stub y áreas no tan stubby.
- Filtrado LSA tipo 3 del router de límite de área.

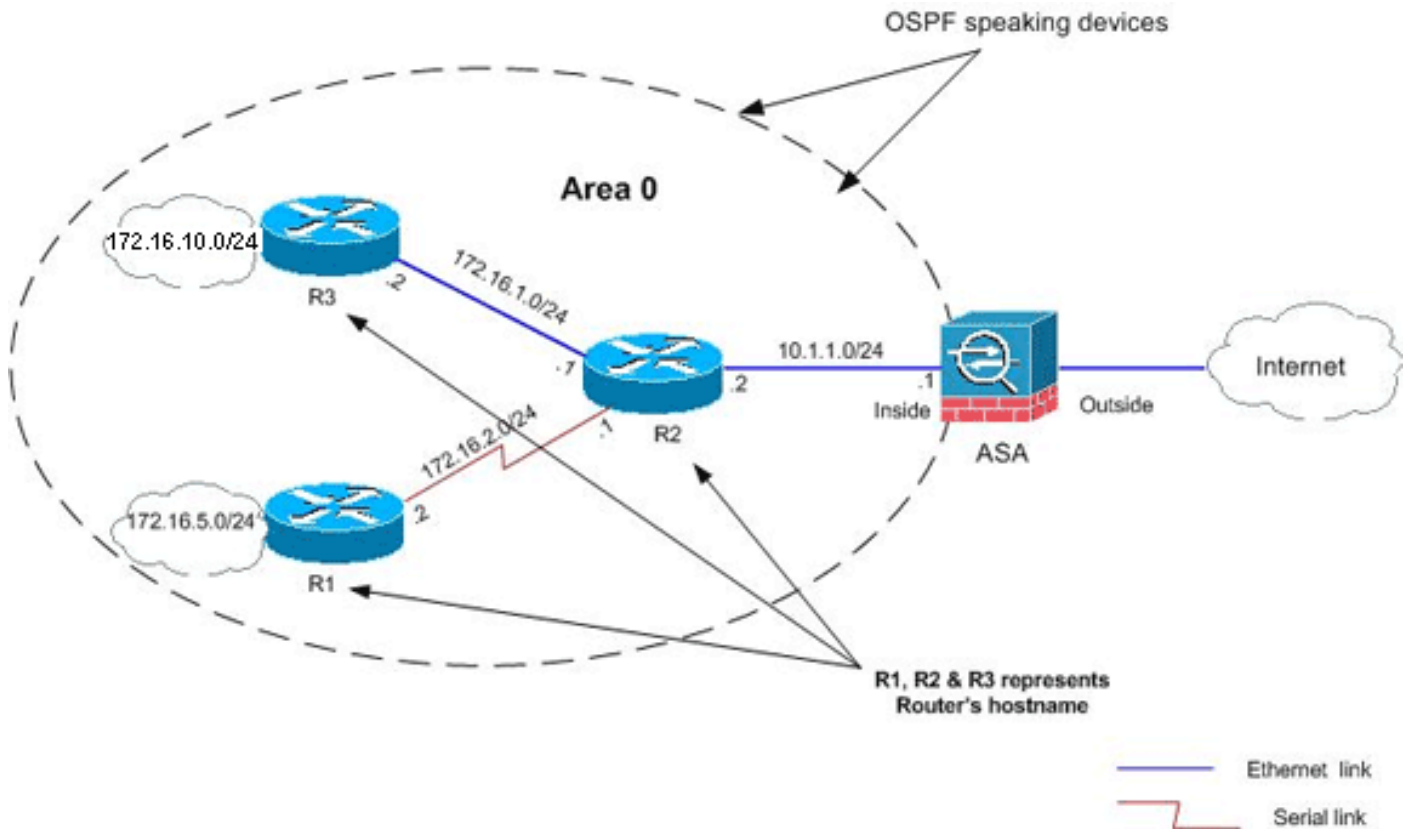
[Configurar](#)

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

[Nota:](#) Use el [Command Lookup Tool](#) (únicamente clientes registrados) para obtener más información sobre los comandos que se utilizan en esta sección.

[Diagrama de la red](#)

En este documento, se utiliza esta configuración de red:



En esta topología de red, la dirección IP de la interfaz interna de Cisco ASA es 10.1.1.1/24. El objetivo es configurar OSPF en Cisco ASA para aprender las rutas a las redes internas (172.16.1.0/24, 172.16.2.0/24, 172.16.5.0/24 y 172.16.10.0/24) dinámicamente a través del router adyacente (R2). R2 aprende las rutas a redes internas remotas a través de los otros dos routers (R1 y R3).

Configuraciones

En este documento, se utilizan estas configuraciones:

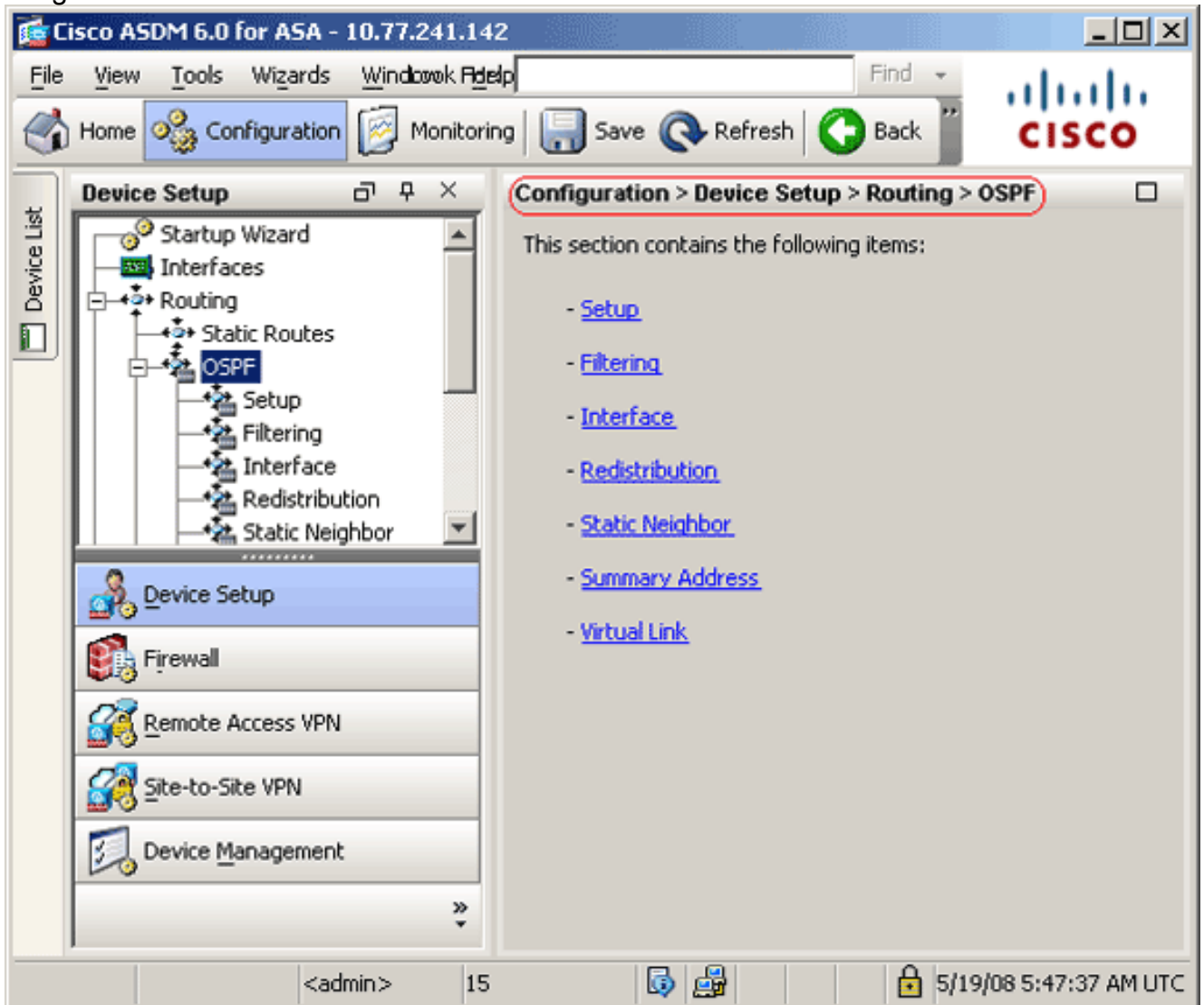
- [Configuración de ASDM](#)
- [Configuración de la Autenticación OSPF](#)
- [Configuración de Cisco ASA CLI](#)
- [Configuración CLI del router Cisco IOS \(R2\)](#)
- [Configuración CLI del router Cisco IOS \(R1\)](#)
- [Configuración CLI del router Cisco IOS \(R3\)](#)
- [Redistribución en OSPF con ASA](#)

Configuración de ASDM

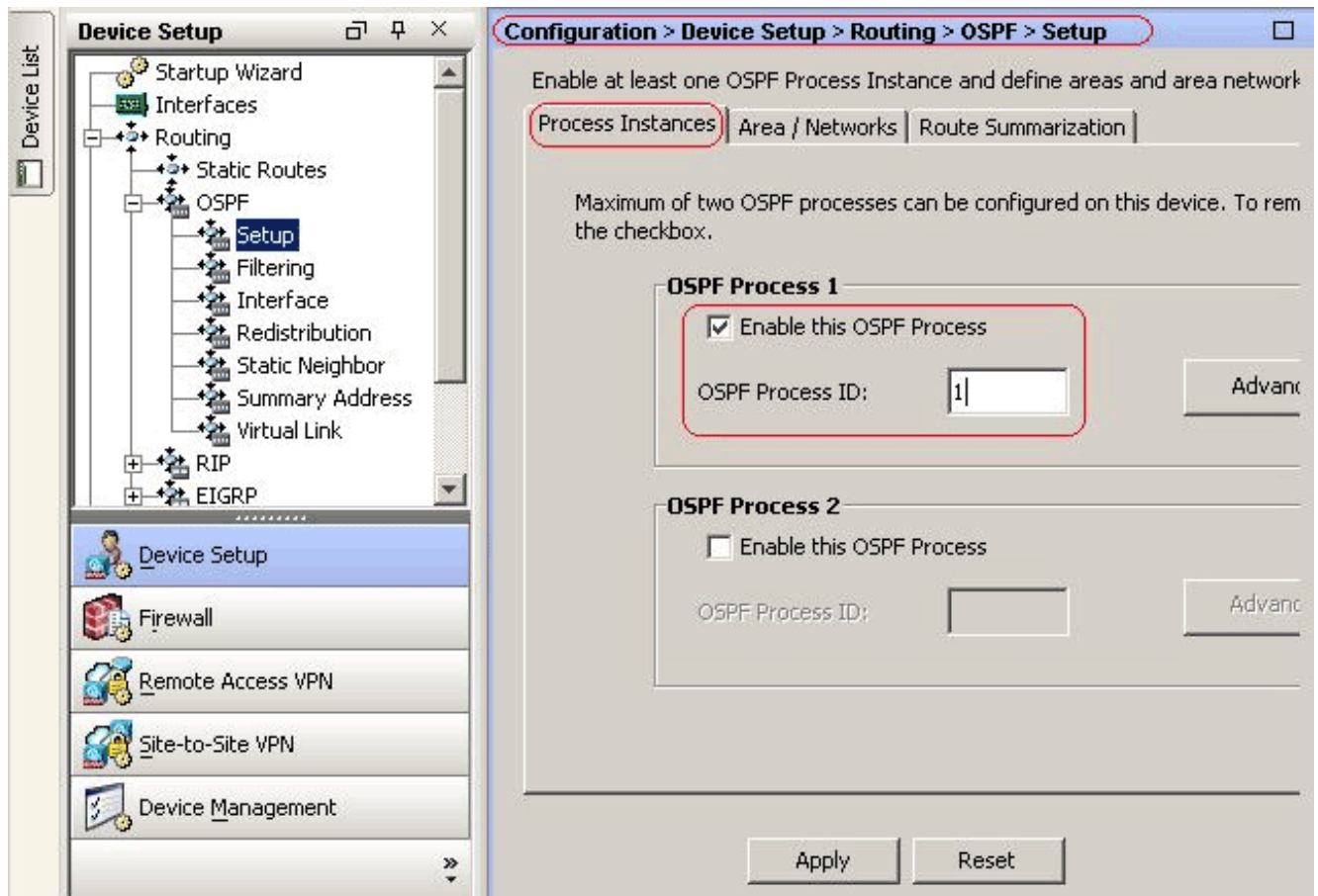
Adaptive Security Device Manager (ASDM) es una aplicación basada en navegador que se utiliza para configurar y supervisar el software en dispositivos de seguridad. El ASDM se carga desde el dispositivo de seguridad y luego se utiliza para configurar, supervisar y administrar el dispositivo. También puede utilizar el iniciador ASDM (sólo Windows) para iniciar la aplicación ASDM más rápido que el applet Java. Esta sección describe la información que necesita para configurar las funciones descritas en este documento con ASDM.

Complete estos pasos para configurar OSPF en el Cisco ASA:

1. Inicie sesión en Cisco ASA con ASDM.
2. Vaya al área **Configuration > Device Setup > Routing > OSPF** de la interfaz ASDM, como se muestra en esta imagen.



3. Habilite el proceso de ruteo OSPF en la pestaña **Setup > Process Instancias**, como se muestra en esta imagen. En este ejemplo, el proceso OSPF ID es 1.



4. Puede hacer clic en **Avanzadas** en la pestaña **Setup > Process Instancias** para configurar los parámetros opcionales del proceso de ruteo OSPF avanzado. Puede editar la configuración específica del proceso, como la ID del router, los cambios de adyacencia, las distancias de ruta administrativas, los temporizadores y la configuración de origen de la información predeterminada.

Edit OSPF Process Advanced Properties

OSPF Process: Router ID:

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

Adjacency Changes

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

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

Administrative Route Distances

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

Timers (in seconds)

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

Default Information Originate

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

Enable Default Information Originate Always advertise the default route

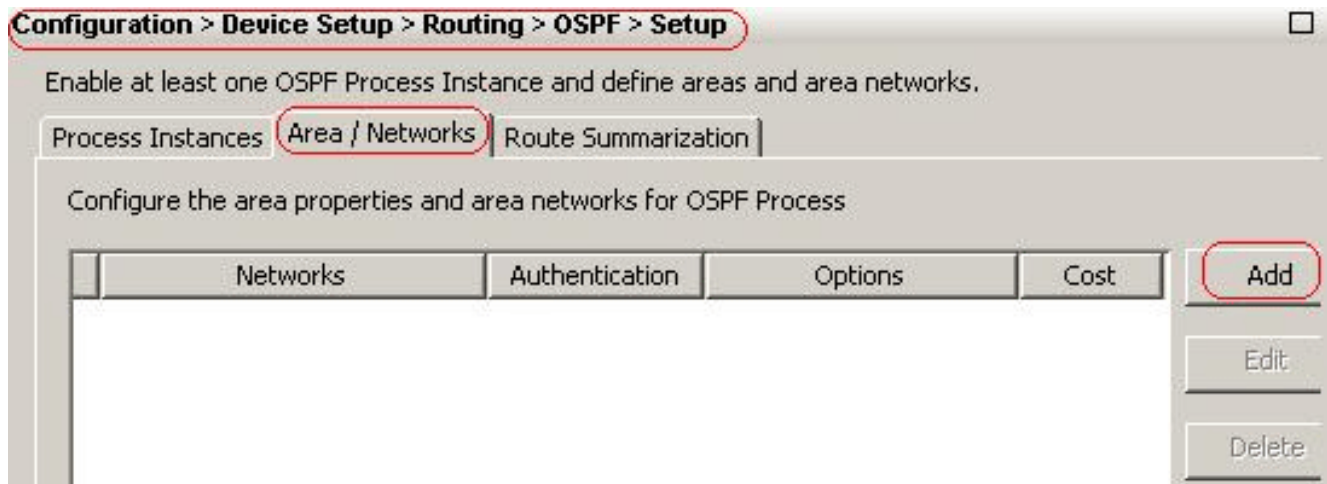
Metric Value: Metric Type: Route Map:

OK Cancel Help

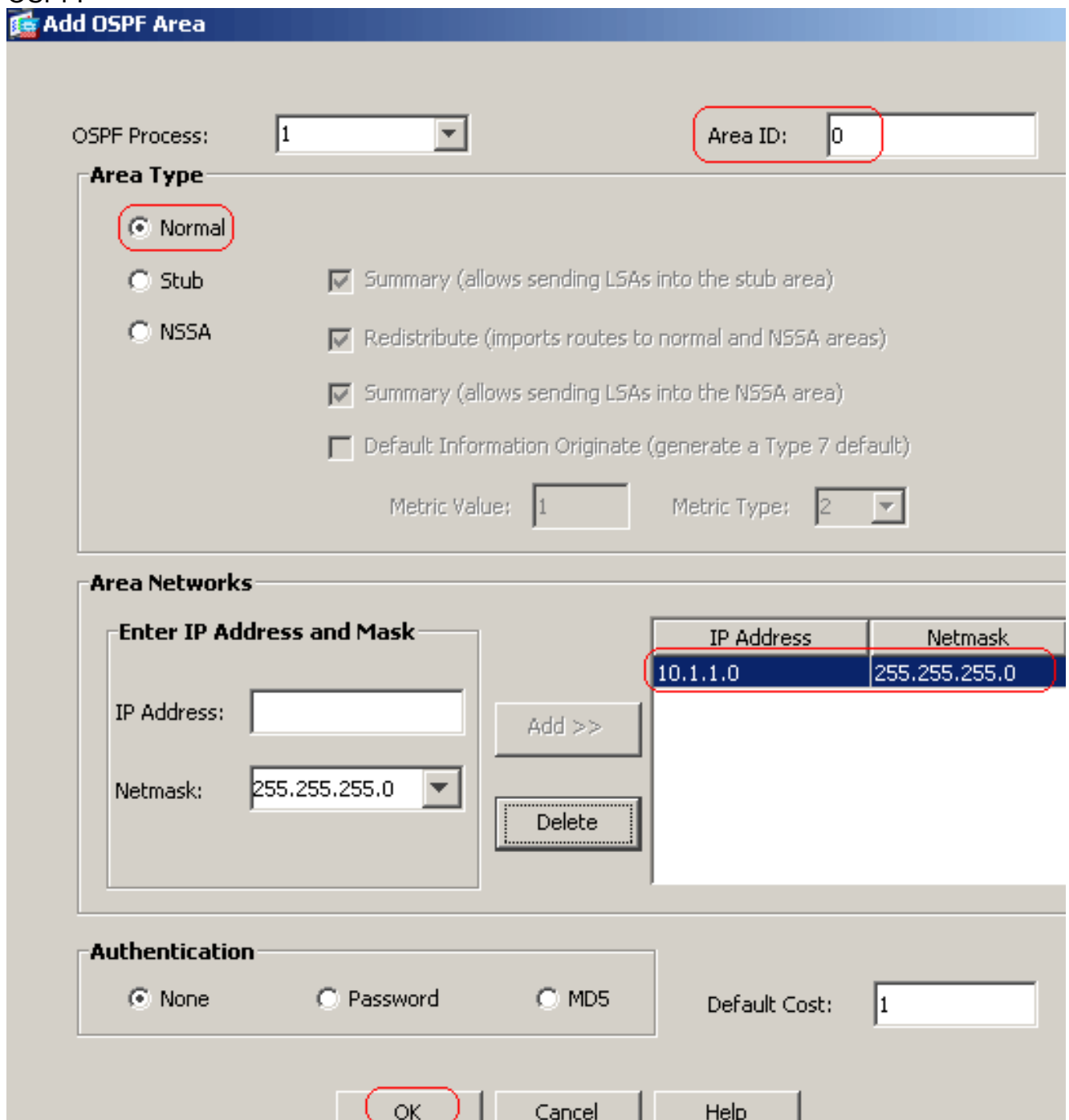
Esta lista describe cada campo:Proceso OSPF: muestra el proceso OSPF que está configurando. No puede cambiar este valor.ID del router: para utilizar una ID de router fija, introduzca una ID de router en formato de dirección IP en el campo ID del router. Si deja este valor en blanco, la dirección IP de nivel más alto del dispositivo de seguridad se utiliza como ID de router.En este ejemplo, el ID de router se configura estáticamente con la dirección IP de la interfaz interna (10.1.1.1).Ignorar LSA MOSPF: active esta casilla de verificación para suprimir el envío de mensajes de registro del sistema cuando el dispositivo de seguridad recibe paquetes LSA de tipo 6 (MOSPF). Esta configuración está desactivada de forma predeterminada.Compatible con RFC 1583: active esta casilla de verificación para calcular los costes de ruta de resumen según RFC 1583. Desmarque esta casilla de verificación para calcular los costos de ruta de resumen según RFC 2328. Para minimizar la posibilidad de bucles de ruteo, todos los dispositivos OSPF en un dominio de ruteo OSPF deben tener la compatibilidad RFC configurada de manera idéntica. Esta configuración está seleccionada de forma predeterminada.Cambios de adyacencia: contiene la configuración que define los cambios de adyacencia que hacen que se envíen los mensajes del registro

del sistema. Cambios de adyacencia de registro: active esta casilla de verificación para que el dispositivo de seguridad envíe un mensaje de registro del sistema cada vez que un vecino OSPF se activa o desactiva. Esta configuración está seleccionada de forma predeterminada. Detalles de cambios de adyacencia de registro: active esta casilla de verificación para que el dispositivo de seguridad envíe un mensaje de registro del sistema cada vez que se produzca algún cambio de estado, no sólo cuando un vecino se active o desactive. Esta configuración está desactivada de forma predeterminada. Distancias de ruta administrativas: contiene la configuración para las distancias administrativas de las rutas basadas en el tipo de ruta. Inter Area: establece la distancia administrativa para todas las rutas de un área a otro. Los valores válidos varían de 1 a 255. El valor predeterminado es 100. Intra Area (Intra Area): establece la distancia administrativa para todas las rutas dentro de un área. Los valores válidos varían de 1 a 255. El valor predeterminado es 100. Externa: establece la distancia administrativa para todas las rutas de otros dominios de ruteo aprendidos a través de la redistribución. Los valores válidos varían de 1 a 255. El valor predeterminado es 100. Timers (Temporizadores): contiene la configuración utilizada para configurar el ritmo de LSA y los temporizadores de cálculo SPF. Tiempo de Retraso SPF: especifica el tiempo entre que OSPF recibe un cambio de topología y cuando se inicia el cálculo SPF. Los valores válidos varían de 0 a 65535. El valor predeterminado es 5. Tiempo en espera de SPF: especifica el tiempo en espera entre los cálculos consecutivos de SPF. Los valores válidos van de 1 a 65534. El valor predeterminado es 10. Rastreo de grupo LSA: especifica el intervalo en el que se recopilan los LSA en un grupo y se actualizan, se suman o envejecen. Los valores válidos varían de 10 a 1800. El valor predeterminado es 240. Default Information Originate (Origen de la información predeterminada): contiene la configuración utilizada por un ASBR para generar una ruta externa predeterminada en un dominio de ruteo OSPF. Enable Default Information Originate (Activar origen de información predeterminada): active esta casilla de verificación para habilitar la generación de la ruta predeterminada en el dominio de ruteo OSPF. Anunciar siempre la ruta predeterminada: active esta casilla de verificación para anunciar siempre la ruta predeterminada. Esta opción está desactivada de forma predeterminada. Valor de métrica: especifica la métrica predeterminada de OSPF. Los valores válidos varían de 0 a 16777214. El valor predeterminado es 1. Tipo de métrica: especifica el tipo de link externo asociado con la ruta predeterminada anunciada en el dominio de ruteo OSPF. Los valores válidos son 1 o 2, lo que indica una ruta externa Tipo 1 o Tipo 2. El valor predeterminado es 2. Route Map: (*Opcional*) Nombre del route map que se aplicará. El proceso de ruteo genera la ruta predeterminada si se satisface el route map.

5. Después de completar los pasos anteriores, defina las redes e interfaces que participan en el ruteo OSPF en la ficha **Setup > Area/Networks**, y luego haga clic en **Add** como se muestra en esta imagen:



Aparece el cuadro de diálogo Agregar área OSPF.



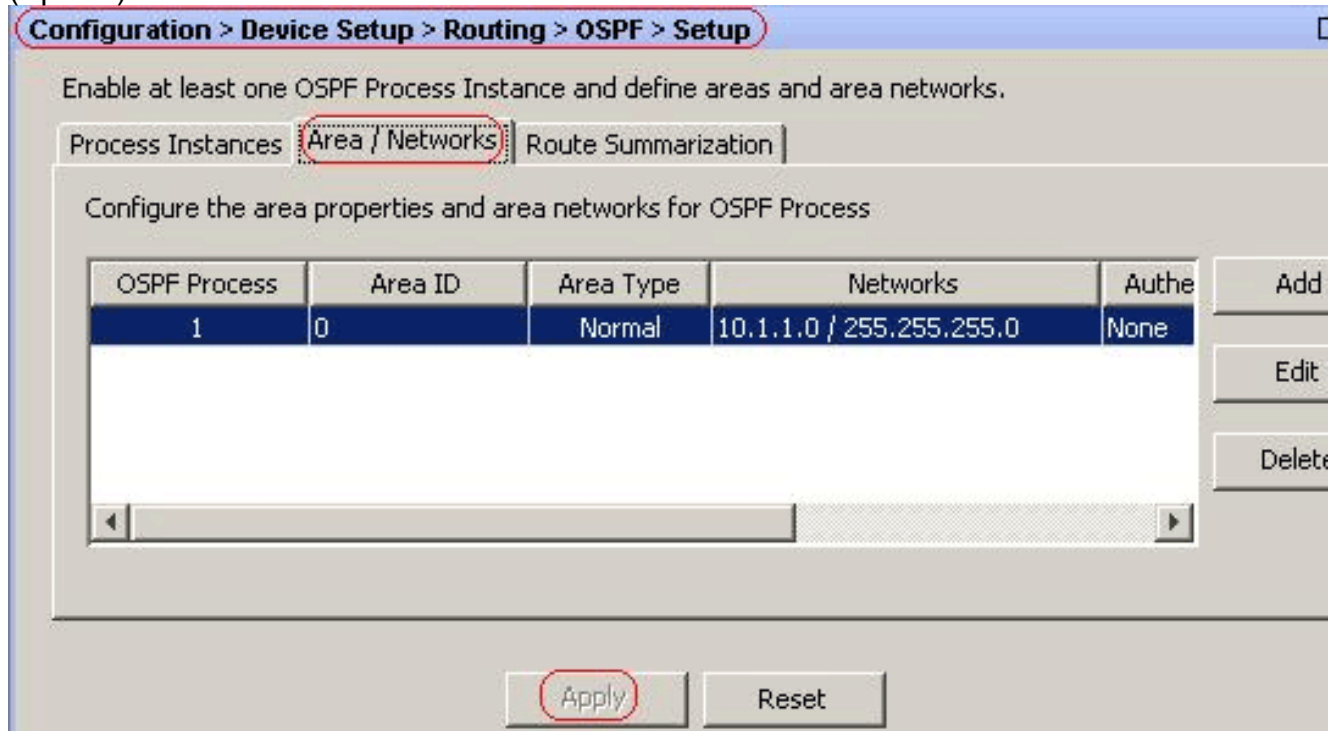
En este ejemplo, la única red que se agrega es la red interna (10.1.1.0/24), ya que OSPF sólo se habilita en la interfaz interna. **Nota:** Sólo las interfaces con una dirección IP que se

encuentren dentro de las redes definidas participan en el proceso de ruteo OSPF.

6. Click OK. Esta lista describe cada campo:
Proceso OSPF: cuando agrega un área nueva, elija el ID para el proceso OSPF. Si sólo hay un proceso OSPF habilitado en el dispositivo de seguridad, ese proceso se selecciona de forma predeterminada. Cuando edita un área existente, no puede cambiar el ID de proceso OSPF.
ID de área: al agregar un área nueva, introduzca la ID de área. Puede especificar el ID de área como un número decimal o una dirección IP. Los valores decimales válidos van de 0 a 4294967295. No puede cambiar el ID de área cuando edita un área existente. En este ejemplo, el ID de área es 0.
Tipo de área: contiene la configuración del tipo de área que se está configurando.
Normal: elija esta opción para convertir el área en un área OSPF estándar. Esta opción se selecciona de forma predeterminada cuando se crea un área por primera vez.
Stub: elija esta opción para convertir el área en un área stub. Las áreas stub no tienen routers ni áreas más allá. Las áreas stub impiden que los LSA externos de AS (LSA de tipo 5) se inunden en el área stub. Al crear un área stub, puede desmarcar la casilla de verificación Summary para evitar que los LSA de resumen (tipo 3 y 4) se inunden en el área.
Resumen: cuando el área que se define es un área stub, desmarque esta casilla de verificación para evitar que los LSA se envíen al área stub. Esta casilla de verificación está activada de forma predeterminada para las áreas stub.
NSSA: elija esta opción para convertir el área en un área no tan fragmentada. Los NSSA aceptan LSA de tipo 7. Cuando crea una NSSA, puede desmarcar la casilla de verificación Resumen para evitar que los LSA de resumen se inunden en el área. Además, puede desmarcar la casilla de verificación Redistribute y habilitar Default Information Originate para inhabilitar la redistribución de rutas.
Redistribute (Redistribuir): desactive esta casilla de verificación para evitar que las rutas se importen a NSSA. Esta casilla de verificación está activada de forma predeterminada.
Resumen: cuando el área que se define es una NSSA, desmarque esta casilla de verificación para evitar que los LSA se envíen al área stub. Esta casilla de verificación está activada de forma predeterminada para NSSA.
Default Information Originate (Origen de la información predeterminada): active esta casilla de verificación para generar un valor predeterminado de tipo 7 en NSSA. Esta casilla de verificación está desactivada de forma predeterminada.
Valor de métrica: introduzca un valor para especificar el valor de métrica OSPF para la ruta predeterminada. Los valores válidos varían de 0 a 16777214. El valor predeterminado es 1.
Tipo de métrica: elija un valor para especificar el tipo de métrica OSPF para la ruta predeterminada. Las opciones son 1 (tipo 1) o 2 (tipo 2). El valor predeterminado es 2.
Redes de área: contiene la configuración que define un área OSPF.
Introducir dirección IP y máscara: contiene la configuración utilizada para definir las redes del área.
IP Address (Dirección IP): introduzca la dirección IP de la red o el host que desea agregar al área. Utilice 0.0.0.0 con una máscara de red de 0.0.0.0 para crear el área predeterminada. Sólo puede utilizar 0.0.0.0 en un área.
Máscara de red: elija la máscara de red para la dirección IP o el host que desea agregar al área. Si agrega un host, elija la máscara 255.255.255.255. En este ejemplo, **10.1.1.0/24** es la red que se va a configurar.
Agregar: agrega la red definida en el área. Introducir dirección IP y máscara al área. La red agregada aparece en la tabla Redes de área.
Eliminar: elimina la red seleccionada de la tabla Redes de área.
Redes de área: muestra las redes definidas para el área.
Dirección IP: muestra la dirección IP de la red.
Máscara de red: muestra la máscara de red para la red.
Autenticación: contiene la configuración para la autenticación de área OSPF.
Ninguno: elija esta opción para inhabilitar la autenticación de área OSPF. Esta es la configuración predeterminada.
Contraseña: elija esta opción para utilizar una contraseña de texto sin cifrar para la autenticación de área. Esta opción no se recomienda cuando la seguridad es un problema.
MD5: elija esta opción para utilizar la autenticación MD5.
Costo

predeterminado: especifique un costo predeterminado para el área. Los valores válidos varían de 0 a 65535. El valor predeterminado es 1.

7. Haga clic en Apply (Aplicar).



8. Opcionalmente, puede definir filtros de ruta en el panel Reglas de filtrado. El filtrado de rutas proporciona más control sobre las rutas que se permiten enviar o recibir en las actualizaciones OSPF.
9. Opcionalmente, puede configurar la redistribución de rutas. Cisco ASA puede redistribuir las rutas detectadas por RIP y EIGRP en el proceso de ruteo OSPF. También puede redistribuir las rutas estáticas y conectadas en el proceso de ruteo OSPF. Defina la redistribución de rutas en el panel de redistribución.
10. Los paquetes hello OSPF se envían como paquetes multicast. Si un vecino OSPF se encuentra a través de una red no broadcast, debe definir manualmente ese vecino. Cuando define manualmente un vecino OSPF, los paquetes hello se envían a ese vecino como mensajes unicast. Para definir vecinos OSPF estáticos, vaya al panel Vecino estático.
11. Las rutas aprendidas de otros protocolos de ruteo se pueden resumir. La métrica utilizada para anunciar el resumen es la métrica más pequeña de todas las rutas más específicas. Las rutas de resumen ayudan a reducir el tamaño de la tabla de ruteo. El uso de rutas de resumen para OSPF hace que un OSPF ASBR anuncie una ruta externa como un agregado para todas las rutas redistribuidas que están cubiertas por la dirección. Sólo se pueden resumir las rutas de otros protocolos de ruteo que se redistribuyen en OSPF.
12. En el panel de link virtual, puede agregar un área a una red OSPF y no es posible conectar el área directamente al área de estructura básica; debe crear un link virtual. Un link virtual conecta dos dispositivos OSPF que tienen un área común, llamada área de tránsito. Uno de los dispositivos OSPF debe estar conectado al área de estructura básica.

[Configuración de la Autenticación OSPF](#)

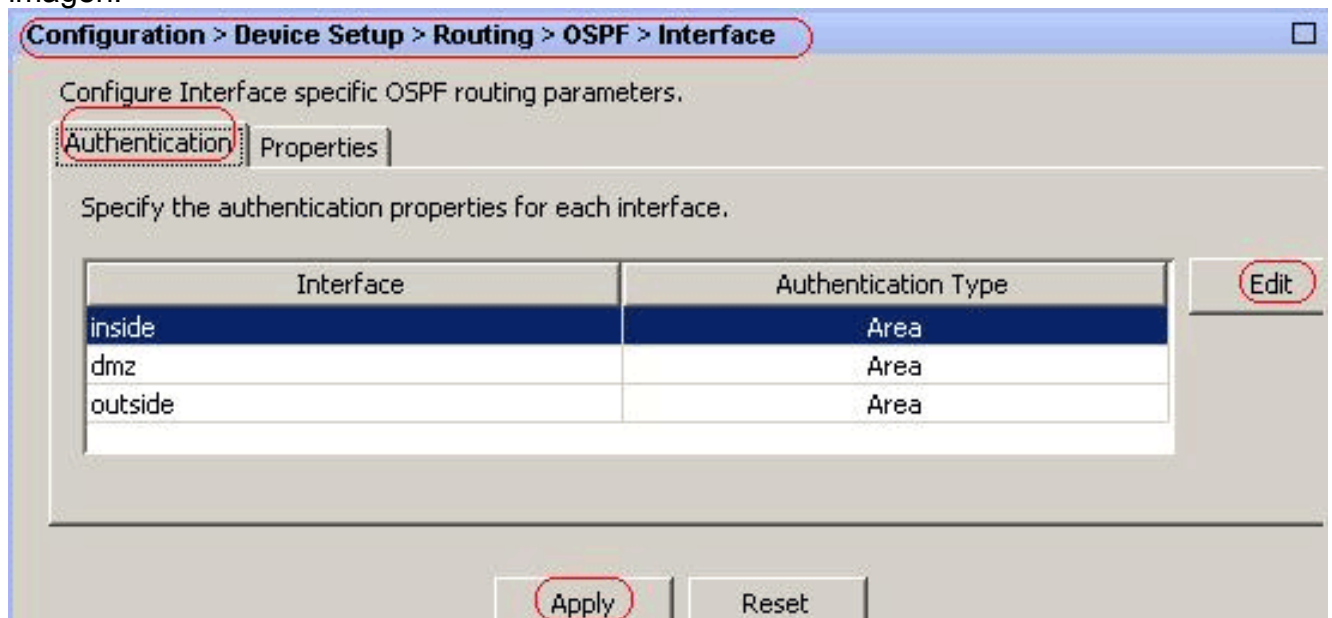
Cisco ASA admite la autenticación MD5 de las actualizaciones de ruteo desde el protocolo de ruteo OSPF. El resumen con llave MD5 en cada paquete OSPF evita la introducción de mensajes

de ruteo no autorizados o falsos de fuentes no aprobadas. La adición de la autenticación a sus mensajes OSPF garantiza que sus routers y Cisco ASA sólo acepten mensajes de ruteo de otros dispositivos de ruteo configurados con la misma clave previamente compartida. Sin esta autenticación configurada, si alguien introduce otro dispositivo de ruteo con información de ruta diferente o contraria en la red, las tablas de ruteo de sus routers o Cisco ASA pueden dañarse y puede producirse un ataque de denegación de servicio. Cuando agrega autenticación a los mensajes EIGRP enviados entre sus dispositivos de ruteo (que incluye el ASA), evita la adición deliberada o accidental de otro router a la red y cualquier problema.

La autenticación de ruta OSPF se configura por interfaz. Todos los vecinos OSPF en las interfaces configuradas para la autenticación de mensajes OSPF deben configurarse con el mismo modo de autenticación y clave para que se establezcan adyacencias.

Complete estos pasos para habilitar la autenticación OSPF MD5 en Cisco ASA:

1. En ASDM, navegue hasta **Configuration > Device Setup > Routing > OSPF > Interface** y luego haga clic en la pestaña **Authentication**, como se muestra en esta imagen.



En este caso, OSPF se habilita en la interfaz interna.

2. Elija la interfaz **interior** y haga clic en **Editar**.
3. En Authentication, elija **MD5 authentication** y agregue más información sobre los parámetros de autenticación aquí. En este caso, la clave previamente compartida es **cisco123**, y el ID de clave es
1.

Edit OSPF Interface Authentication

Interface:

Authentication

No authentication
 Area authentication, if defined
 MD5 authentication

Authentication Password

Enter Password: Re-enter Password:

MD5 IDs and Keys

MD5 Key ID:

MD5 Key:

MD5 Key ID	MD5 Key
1	cisco123

4. Haga clic en **Aceptar** y luego en **Aplicar**.

Configuration > Device Setup > Routing > OSPF > Interface

Configure Interface specific OSPF routing parameters.

Specify the authentication properties for each interface.

Interface	Authentication Type
inside	MD5
dmz	Area
outside	Area

Cisco ASA

```
ciscoasa#show running-config
: Saved
:
ASA Version 8.0(2)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names

!--- Inside interface configuration interface
Ethernet0/1 nameif inside security-level 100 ip address
10.1.1.1 255.255.255.0 ospf cost 10 !--- OSPF
authentication is configured on the inside interface
ospf message-digest-key 1 md5 <removed> ospf
authentication message-digest ! !--- Outside interface
configuration interface Ethernet0/2 nameif outside
security-level 0 ip address 192.168.1.2 255.255.255.0
ospf cost 10 ! !--- Output Suppressed icmp unreachable
rate-limit 1 burst-size 1 asdm image disk0:/asdm-602.bin
no asdm history enable arp timeout 14400 ! !--- OSPF
Configuration router ospf 1
  network 10.1.1.0 255.255.255.0 area 0
  log-adj-changes
!

!--- This is the static default gateway configuration in
order to reach Internet route outside 0.0.0.0 0.0.0.0
192.168.1.1 1 ciscoasa#
```

Configuración CLI del router Cisco IOS (R2)

Router Cisco IOS (R2)

```
!--- Interface that connects to the Cisco ASA. !---
Notice the OSPF authentication parameters interface
Ethernet0
  ip address 10.1.1.2 255.255.255.0
  ip ospf authentication message-digest
  ip ospf message-digest-key 1 md5 cisco123

!--- Output Suppressed !--- OSPF Configuration router
ospf 1
  log-adjacency-changes
  network 10.1.1.0 0.0.0.255 area 0
  network 172.16.1.0 0.0.0.255 area 0
  network 172.16.2.0 0.0.0.255 area 0
```

Configuración CLI del router Cisco IOS (R1)

Router Cisco IOS (R1)

```
!--- Output Suppressed !--- OSPF Configuration router
ospf 1
  log-adjacency-changes
```

```
network 172.16.5.0 0.0.0.255 area 0
network 172.16.2.0 0.0.0.255 area 0
```

Configuración CLI del router Cisco IOS (R3)

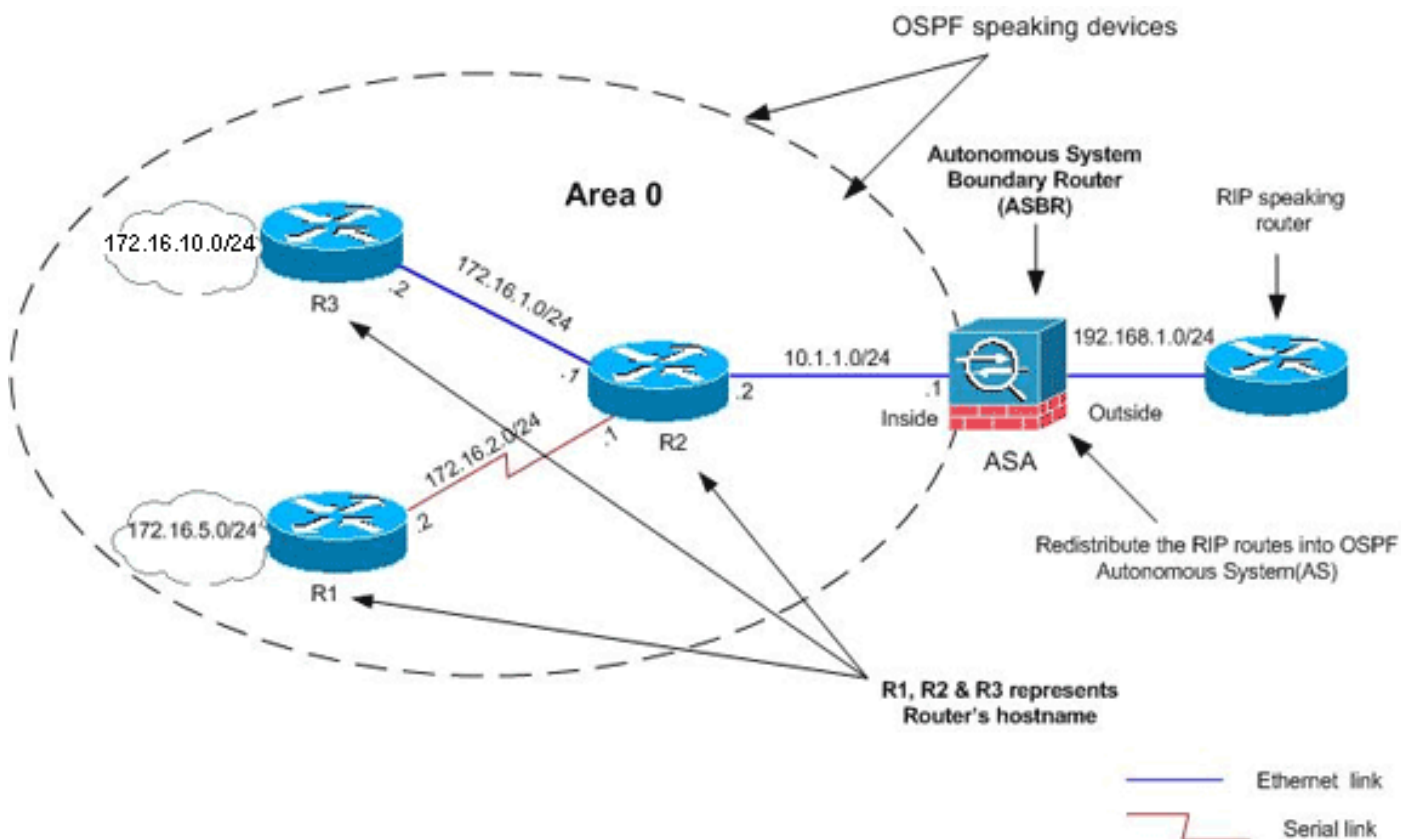
Router Cisco IOS (R3)

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

Redistribución en OSPF con ASA

Como se mencionó anteriormente, puede redistribuir las rutas en un proceso de ruteo OSPF desde otro proceso de ruteo OSPF, un proceso de ruteo RIP o desde rutas estáticas y conectadas configuradas en interfaces habilitadas para OSPF.

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



Configuración de ASDM

1. Elija **Configuration > Device Setup > Routing > RIP > Setup** para habilitar RIP y agregue la red 192.168.1.0 como se muestra en esta imagen.

Configuration > Device Setup > Routing > RIP > Setup

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

Enable RIP routing

Enable auto-summarization

Enable RIP version Version 1 Version 2

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

Enable default information originate Route Map:

Networks

IP Network to Add:

192.168.1.0

Passive Interfaces

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

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

- Haga clic en Apply (Aplicar).
- Elija **Configuration > Device Setup > Routing > OSPF > Redistribution > Add** para redistribuir las rutas RIP en OSPF.

Configuration > Device Setup > Routing > OSPF > Redistribution

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

OSPF Process	Protocol	Match	Subnets	Metric Value	Metric Type

- Haga clic en **Aceptar** y luego en **Aplicar**.

Configuración CLI equivalente

Configuración CLI de ASA para la Redistribución de RIP en OSPF AS

```

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

router rip
 network 192.168.1.0

```

Puede ver la tabla de ruteo del router IOS vecino(R2) después de redistribuir las rutas RIP en OSPF 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

```

172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
O    172.16.10.1/32 [110/11] via 172.16.1.2, 01:17:29, Ethernet1
O    172.16.5.1/32 [110/65] via 172.16.2.2, 01:17:29, Serial1
C    172.16.1.0/24 is directly connected, Ethernet1
C    172.16.2.0/24 is directly connected, Serial1
10.0.0.0/24 is subnetted, 1 subnets

```

```
C 10.1.1.0 is directly connected, Ethernet0
O E2 192.168.1.0/24 [110/20] via 10.1.1.1, 01:17:29, Ethernet0
!--- Redistributed route advertised by Cisco ASA
```

Verificación

Complete estos pasos para verificar su configuración:

1. En ASDM, puede navegar hasta **Monitoring > Routing > OSPF Neighbors** para ver cada uno de los vecinos OSPF. Esta imagen muestra el router interno (R2) como vecino activo. También puede ver la interfaz donde reside este vecino, ID del router vecino, estado y tiempo muerto.

Monitoring > Routing > OSPF Neighbors

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

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

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

2. Además, puede verificar la tabla de ruteo si navega a **Monitoring > Routing > Routes**. En esta imagen, las redes 172.16.1.0/24, 172.16.2.0/24, 172.16.5.0/24 y 172.16.10.0/24 se aprenden a través de R2 (10.1.1.2).

Monitoring > Routing > Routes

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

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

3. Desde la CLI, puede utilizar el comando **show route** para obtener el mismo resultado.

```
ciscoasa#show route
```

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
 * - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is 192.168.1.1 to network 0.0.0.0

```
O 172.16.10.1 255.255.255.255 [110/21] via 10.1.1.2, 0:00:06, inside
O 172.16.5.1 255.255.255.255 [110/75] via 10.1.1.2, 0:00:06, inside
O 172.16.1.0 255.255.255.0 [110/20] via 10.1.1.2, 0:00:06, inside
O 172.16.2.0 255.255.255.0 [110/74] via 10.1.1.2, 0:00:06, inside
C 10.1.1.0 255.255.255.0 is directly connected, inside
C 10.77.241.128 255.255.255.192 is directly connected, dmz
S 10.77.0.0 255.255.0.0 [1/0] via 10.77.241.129, dmz
C 192.168.1.0 255.255.255.0 is directly connected, outside
S* 0.0.0.0 0.0.0.0 [1/0] via 192.168.1.1, outside
```

4. También puede utilizar el comando **show ospf database** para obtener información sobre las redes aprendidas y la topología ospf.

```
ciscoasa#show ospf database
```

OSPF Router with ID (192.168.1.2) (Process ID 1)

Router Link States (Area 0)

Link ID	ADV Router	Age	Seq#	Checksum	Link count
172.16.1.2	172.16.1.2	123	0x80000039	0xfd1d	2
172.16.2.1	172.16.2.1	775	0x8000003c	0x9b42	4
172.16.5.1	172.16.5.1	308	0x80000038	0xb91b	3
192.168.1.2	192.168.1.2	1038	0x80000037	0x29d7	1

Net Link States (Area 0)

Link ID	ADV Router	Age	Seq#	Checksum
10.1.1.1	192.168.1.2	1038	0x80000034	0x72ee
172.16.1.1	172.16.2.1	282	0x80000036	0x9e68

5. El comando **show ospf neighbors** también es útil para verificar los vecinos activos y la información del correspondiente. Este ejemplo muestra la misma información que obtuvo de ASDM en el paso 1.

```
ciscoasa#show ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
172.16.2.1	1	FULL/BDR	0:00:36	10.1.1.2	inside

Troubleshoot

Esta sección proporciona información que podría facilitar la resolución de problemas de OSPF.

Configuración de Vecino Estático para la Red Punto a Punto

Si ha configurado *red OSPF punto a punto sin broadcast* en el ASA, debe definir vecinos OSPF estáticos para anunciar rutas OSPF en una red punto a punto sin broadcast. Consulte [Definición de Vecinos OSPF Estáticos](#) para obtener más información.

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 Debug](#) antes de utilizar los comandos debug.

- **debug ospf events:** habilita la depuración de eventos OSPF.

```
ciscoasa(config)#debug ospf events
OSPF events debugging is on
ciscoasa(config)# int e0/1
ciscoasa(config-if)# no shu
ciscoasa(config-if)#
OSPF: Interface inside going Up
OSPF: Send with youngest Key 1
OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2
OSPF: 2 Way Communication to 172.16.2.1 on inside, state 2WAY
OSPF: Backup seen Event before WAIT timer on inside
OSPF: DR/BDR election on inside
OSPF: Elect BDR 172.16.2.1
OSPF: Elect DR 172.16.2.1
      DR: 172.16.2.1 (Id)   BDR: 172.16.2.1 (Id)
OSPF: Send DBD to 172.16.2.1 on inside seq 0x1abd opt 0x2 flag 0x7 len 32
OSPF: Send with youngest Key 1
OSPF: End of hello processing
OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2
OSPF: End of hello processing
OSPF: Rcv DBD from 172.16.2.1 on inside seq 0x12f3 opt 0x42 flag 0x7 len 32  mtu
 1500 state EXSTART
OSPF: First DBD and we are not SLAVE
OSPF: Rcv DBD from 172.16.2.1 on inside seq 0x1abd opt 0x42 flag 0x2 len 152  mt
u 1500 state EXSTART
OSPF: NBR Negotiation Done. We are the MASTER
OSPF: Send DBD to 172.16.2.1 on inside seq 0x1abe opt 0x2 flag 0x3 len 132
OSPF: Send with youngest Key 1
OSPF: Send with youngest Key 1
OSPF: Database request to 172.16.2.1
OSPF: sent LS REQ packet to 10.1.1.2, length 12
OSPF: Rcv DBD from 172.16.2.1 on inside seq 0x1abe opt 0x42 flag 0x0 len 32  mtu
 1500 state EXCHANGE
OSPF: Send DBD to 172.16.2.1 on inside seq 0x1abf opt 0x2 flag 0x1 len 32
OSPF: Send with youngest Key 1
OSPF: Send with youngest Key 1
OSPF: Rcv DBD from 172.16.2.1 on inside seq 0x1abf opt 0x42 flag 0x0 len 32  mtu
 1500 state EXCHANGE
OSPF: Exchange Done with 172.16.2.1 on inside
OSPF: Synchronized with 172.16.2.1 on inside, state FULL
OSPF: Send with youngest Key 1
OSPF: Send with youngest Key 1
OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2
OSPF: Neighbor change Event on interface inside
OSPF: DR/BDR election on inside
OSPF: Elect BDR 192.168.1.2
OSPF: Elect DR 172.16.2.1
OSPF: Elect BDR 192.168.1.2
OSPF: Elect DR 172.16.2.1
      DR: 172.16.2.1 (Id)   BDR: 192.168.1.2 (Id)
OSPF: End of hello processing
OSPF: Send with youngest Key 1
OSPF: Send with youngest Key 1
OSPF: Send with youngest Key 1
OSPF: Send with youngest Key 1
OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2
OSPF: End of hello processing
OSPF: Send with youngest Key 1
OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2
OSPF: End of hello processing
```

```
OSPF: Send with youngest Key 1
OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2
OSPF: End of hello processing
OSPF: Send with youngest Key 1
OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2
OSPF: End of hello processing
```

Nota: Refiérase a la sección [debug ospf](#) de la Referencia de Comandos de Dispositivos de Seguridad de Cisco, Versión 8.0 para obtener más información sobre varios comandos que son útiles para resolver el problema.

[Información Relacionada](#)

- [Página de Soporte de Cisco 5500 Series Adaptive Security Appliance](#)
- [Página de soporte de PIX de la serie 500 de Cisco](#)
- [PIX/ASA 8.X: Configuración de EIGRP en Cisco Adaptive Security Appliance \(ASA\)](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)