ASA/PIX con el ejemplo de la configuración de OSPF

Contenido

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.

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: 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 OSPF 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.

- El dispositivo de seguridad adaptante de las Cisco 5500 Series (ASA) ese funciona con la versión de software 8.0 y posterior
- Versión de software 6.0 del Cisco Adaptive Security Device Manager (ASDM) 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

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

Las ventajas del OSPF sobre el RIP incluyen:

- Las actualizaciones de la base de datos de estado de links OSPF se envían menos con frecuencia que las actualizaciones, y la base de datos de estado de link se pone al día inmediatamente bastante que gradualmente mientras que la información que ha expirado se mide el tiempo hacia fuera.
- Las decisiones de ruteo se basan en el coste, que es una indicación de los gastos indirectos requeridos para enviar los paquetes a través de una cierta interfaz. El dispositivo de seguridad calcula el coste de una interfaz basada en el ancho de banda de link bastante que el número de saltos al destino. El coste se puede configurar para especificar los trayectos preferidos.

La desventaja de los primeros algoritmos del trayecto más corto es que requieren muchos ciclos

de la CPU y memoria.

El dispositivo de seguridad puede funcionar con dos procesos del protocolo OSPF simultáneamente, en diversos conjuntos de las interfaces. Usted puede ser que quiera funcionar con dos procesos si usted tiene interfaces que utilicen los mismos IP Addresses (el NAT permite que estas interfaces coexistan, pero el OSPF no permite a las direcciones superpuestas). O usted puede ser que quiera ejecutar un proceso en el interior, y otro en el exterior, y redistribuye un subconjunto de rutas entre los dos procesos. Semejantemente, usted puede ser que necesite segregar a las direcciones privadas de las direcciones públicas.

Usted puede redistribuir las rutas en un proceso de ruteo de OSPF de otro proceso de ruteo de OSPF, un proceso de ruteo del RIP, o de los parásitos atmosféricos y de los Routeconectad configurados en las interfaces OSPF-habilitadas.

El dispositivo de seguridad soporta estas características OSPF:

- Soporte del intra-area, del interarea, y del externo (tipo rutas de I y del tipo II).
- Soporte de un link virtual.
- Inundación OSPF LSA.
- Autenticación a los paquetes OSPF (contraseña y autenticación de MD5).
- Soporte para configurar el dispositivo de seguridad como un router designado o router de backup señalado. El dispositivo de seguridad también se puede configurar como ABR. Sin embargo, se limita la capacidad de configurar el dispositivo de seguridad como ASBR de omitir la información solamente (por ejemplo, inyectando una ruta predeterminado).
- Soporte para las zonas fragmentadas y el Not-So-Stubby Areas.
- Filtración del router type-3 LSA del límite de área.

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:

En esta topología de red, la dirección IP de la interfaz interior de Cisco ASA es 10.1.1.1/24. La meta es configurar el 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). El r2 aprende las rutas a las redes internas remotas a través del otro dos Routers (r1 y R3).

Configuraciones

En este documento, se utilizan estas configuraciones:

- Configuración de ASDM

- Autenticación OSPF 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)
- Redistribuya en el OSPF con el ASA

Configuración de ASDM

El Administrador de dispositivos de seguridad adaptante (ASDM) es aplicaciones basadas en el buscador usadas para configurar y para 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 OSPF en Cisco ASA:

1. Inicie sesión a Cisco ASA con el ASDM.
2. Navegue a la **configuración > a la configuración > a la encaminamiento > a la área OSPF de dispositivo de la** interfaz del ASDM, tal y como se muestra en de esta imagen.
3. Habilite el proceso de ruteo de OSPF en la lengueta de los **casos de la configuración > del proceso**, tal y como se muestra en de esta imagen. En este ejemplo, el proceso OSPF ID es **1.**
4. Usted puede hacer clic **avanzado** en la lengueta de los **casos de la configuración > del proceso** 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.Esta lista describe cada campo:Proceso OSPF — Visualiza el proceso OSPF que usted está configurando. Usted no puede cambiar este valor.Router ID — Para utilizar un Router ID fijo, ingrese un Router ID en el formato de IP Address en el campo del Router ID. Si usted deja este espacio en blanco del valor, la dirección IP del más alto nivel en el dispositivo de seguridad se utiliza como el Router ID.En este ejemplo, el Router ID se configura estáticamente con la dirección IP de la interfaz interior (10.1.1.1).Ignore LSA MOSPF — Marque esta casilla de verificación para suprimir el envío de los mensajes del registro del sistema cuando el dispositivo de seguridad recibe los paquetes LSA del tipo 6 (MOSPF). Esta configuración se desmarca por abandono.RFC 1583 compatible — Marque esta casilla de verificación para calcular los costes de la ruta de resumen por el RFC 1583. Desmarque esta casilla de verificación para calcular los costes de la ruta de resumen por el RFC 2328. Para minimizar la ocasión de los loopes de la encaminamiento, todos los dispositivos OSPF en un dominio de ruteo OSPF deben tener compatibilidad RFC fijada idénticamente. Esta configuración se selecciona por abandono.Cambios de la adyacencia — Contiene las configuraciones que definen los cambios de la adyacencia que hacen los mensajes del registro del sistema ser enviados.Cambios de la adyacencia del registro — Marque esta casilla de verificación para hacer el dispositivo de seguridad enviar un mensaje del registro del sistema siempre que vaya un vecino OSPF hacia arriba o hacia abajo. Esta

configuración se selecciona por abandono.La adyacencia del registro cambia el detalle — Marque esta casilla de verificación para hacer el dispositivo de seguridad enviar un mensaje del registro del sistema siempre que ocurra cualquier cambio de estado, no en el momento en que va un vecino hacia arriba o hacia abajo. Esta configuración se desmarca por abandono.Distancias administrativas de la ruta — Contiene las configuraciones para las distancias administrativas de las rutas basadas en el tipo de la ruta.Área inter — Fija la distancia administrativa para todas las rutas a partir de una área a otra. Los valores válidos se extienden a partir de la 1 a 255. El valor predeterminado es 100.Intra área — Fija la distancia administrativa para todas las rutas dentro de un área. Los valores válidos se extienden a partir de la 1 a 255. El valor predeterminado es 100.Externo — Fija la distancia administrativa para todas las rutas de otros dominios de ruteo que sean doctos con la redistribución. Los valores válidos se extienden a partir de la 1 a 255. El valor predeterminado es 100.Temporizadores — Contiene las configuraciones usadas para configurar los temporizadores del establecimiento del paso LSA y del cálculo SPF.Tiempo de retraso SPF — Especifica el tiempo entre cuando el OSPF recibe un cambio de la topología y cuando el cálculo SPF comienza. Los valores válidos se extienden a partir de la 0 a 65535. El valor predeterminado es 5.Tiempo en espera SPF — Especifica el tiempo en espera entre los cálculos consecutivos SPF. Los valores válidos se extienden a partir de la 1 a 65534. El valor predeterminado es 10.Establecimiento del paso del grupo LSA — Especifica el intervalo en el cual los LSA se recogen en un grupo y se restauran, checksummed, o se envejecen. Los valores válidos se extienden a partir del 10 a 1800. El valor predeterminado es 240.La información predeterminada origina — Contiene las configuraciones usadas por un ASBR para generar una ruta externo predeterminada en un dominio de ruteo OSPF.La información predeterminada del permiso origina — Marque esta casilla de verificación para habilitar la generación de la ruta predeterminado en el dominio de ruteo OSPF.Haga publicidad siempre de la ruta predeterminado — Marque esta casilla de verificación para hacer publicidad siempre de la ruta predeterminado. Esta opción se desmarca por abandono.Valor métrico — Especifica el OSPF predeterminado métrico. Los valores válidos se extienden a partir de la 0 a 16777214. El valor predeterminado es 1.Tipo de métrica — Especifica el tipo de link externo asociado a la ruta predeterminado de divulgación en el dominio de ruteo OSPF. Los valores válidos son 1 o 2, indicando un tipo 1 o una ruta externo del Tipo 2. El valor predeterminado es 2.Route Map — (*opcional*) el nombre del Route Map a aplicarse. El proceso de ruteo genera la ruta predeterminado si se satisface el Route Map.

5. Después de que usted complete los pasos anteriores, defina las redes y las interfaces que participan en el OSPF Routing en la lengueta de la **configuración > del área/de las redes**, y después haga clic **agregan** tal y como se muestra en de esta imagen:El cuadro de diálogo de la área OSPF del agregar aparece.En este ejemplo, la única red se agrega que es la red interna (10.1.1.0/24) puesto que el OSPF se habilita solamente en la interfaz interior.**Nota:** Interconecta solamente con una dirección IP que baja dentro de las redes definidas participa en el proceso de ruteo de OSPF.
6. Haga clic en OK.Esta lista describe cada uno coloca:Proceso OSPF — Cuando usted agrega una nueva área, elija el ID para el proceso OSPF. Si hay solamente un proceso OSPF habilitado en el dispositivo de seguridad, después ese proceso se selecciona por abandono. Cuando usted edita un área existente, usted no puede cambiar el proceso OSPF ID.ID de área — Cuando usted agrega una nueva área, ingrese el ID de área. Usted puede especificar el ID de área como un número decimal o dirección IP. Los valores decimales válidos se extienden a partir de la 0 a 4294967295. Usted no puede cambiar el ID de área cuando usted edita un área existente.En este ejemplo, el ID de área es **0**.Tipo de área —

Contiene las configuraciones para el tipo de zona que es configurado.Normal — Elija esta opción para hacer el área a la área OSPF estándar. Esta opción se selecciona por abandono cuando usted primero crea un área.Stub — Elija esta opción para hacer el área a la zona fragmentada. Las zonas fragmentadas no tienen ningún Routers o áreas más allá de ella. Las zonas fragmentadas previenen COMO LSA externo (tipo 5 LSA) de ser inundado en la zona fragmentada. Cuando usted crea una zona fragmentada, usted puede desmarcar la casilla de verificación sumaria para prevenir los LSA de resúmenes (tipo 3 y 4) de ser inundado en el área.Resumen — Cuando el área que es definida es una zona fragmentada, desmarque esta casilla de verificación para evitar que los LSA sean enviados en la zona fragmentada. Esta casilla de verificación se selecciona por abandono para las zonas fragmentadas.NSSA — Elija esta opción para hacer el área un Not-So-Stubby Area. Los NSSA validan el tipo 7 LSA. Cuando usted crea un NSSA, usted puede desmarcar la casilla de verificación sumaria para evitar que los LSA de resúmenes sean inundados en el área. Además, usted puede desmarcar la casilla de verificación de la redistribución y la información de Defautl del permiso origina para inhabilitar la redistribución de ruta.Redistribuya — Desmarque esta casilla de verificación para evitar que las rutas sean importadas en el NSSA. Esta casilla de verificación se selecciona por abandono.Resumen — Cuando el área que es definida es un NSSA, desmarque esta casilla de verificación para evitar que los LSA sean enviados en la zona fragmentada. Esta casilla de verificación se selecciona por abandono para los NSSA.La información predeterminada origina — Marque esta casilla de verificación para generar un valor por defecto del tipo 7 en el NSSA. Esta casilla de verificación se desmarca por abandono.Valor métrico — Ingrese un valor para especificar el valor métrico OSPF para la ruta predeterminado. Los valores válidos se extienden a partir de la 0 a 16777214. El valor predeterminado es 1.Tipo de métrica — Elija un valor para especificar el tipo de métrica OSPF para la ruta predeterminado. Las opciones son 1 (tipo 1) o 2 (tipo-2). El valor predeterminado es 2.Redes de área — Contiene las configuraciones que definen una área OSPF.Ingrese el IP Address y la máscara — Contiene las configuraciones usadas para definir las redes en el área.IP Address — Ingrese el IP Address de la red o recíbalo para ser agregado al área. Utilice 0.0.0.0 con un netmask de 0.0.0.0 para crear el área predeterminada. Usted puede utilizar 0.0.0.0 en solamente una área.Netmask — Elija a la máscara de la red para la dirección IP o recíbala para ser agregada al área. Si usted agrega un host, elija la máscara de 255.255.255.255.En este ejemplo, **10.1.1.0/24** es la red que se configurará.Agregue — Agrega la red definida en el área del IP Address y de la máscara del ingresar al área. La red agregada aparece en la tabla de redes de área.Cancelación — Borra la red seleccionada de la tabla de redes de área.Redes de área — Visualiza las redes definidas para el área.Dirección IP — Visualiza la dirección IP de la red.Netmask — Visualiza a la máscara de la red para la red.Autenticación — Contiene las configuraciones para la autenticación de la área OSPF.Ninguno — Elija esta opción para inhabilitar la autenticación de la área OSPF. Ésta 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 donde está una preocupación la Seguridad.MD5 — Elija esta opción para utilizar autenticación de MD5.Costo predeterminado — Especifique un costo predeterminado para el área. Los valores válidos se extienden a partir de la 0 a 65535. El valor predeterminado es 1.

7. Haga clic en Apply (Aplicar).
8. Opcionalmente, usted puede definir los filtros de la ruta en el cristal de las reglas para filtros. El filtrado de Routes proporciona más control sobre las rutas que se permiten ser enviadas o ser recibidas en las actualizaciones OSPF.

9. Usted puede configurar opcionalmente la redistribución de ruta. Cisco ASA puede redistribuir las rutas descubiertas por el RIP y el EIGRP en el proceso de ruteo de OSPF. Usted puede también redistribuir los parásitos atmosféricos y los Routeconectad en el proceso de ruteo de OSPF. Defina la redistribución de ruta en el cristal de la redistribución.
10. Los paquetes OSPF de saludo se envían como paquetes de multidifusión. Si un vecino OSPF está situado a través de una red del nonbroadcast, usted debe definir manualmente a ese vecino. Cuando usted define manualmente a un vecino OSPF, los paquetes de saludo se envían a ese vecino como mensajes del unicast. Para definir a los vecinos OSPF estáticos, vaya al cristal del vecino estático.
11. Las rutas aprendidas de otros Routing Protocol pueden ser resumidas. El métrico usado para hacer publicidad del resumen es el métrico más pequeño de rutas más específicas. Las rutas de resumen ayudan a reducir el tamaño de la tabla de ruteo.Usando las rutas de resumen para el OSPF hace un OSPF ASBR hacer publicidad de una ruta externo como agregado para todas las rutas redistribuido que sean cubiertas por el direccionamiento. Solamente las rutas de otros Routing Protocol que se estén redistribuyendo en el OSPF pueden ser resumidas.
12. En el cristal del link virtual, usted puede agregar un área a una red OSPF, y no es posible conectar el área directamente con la área de estructura básica; usted debe establecer un link virtual. Un link virtual conecta dos dispositivos OSPF que tengan una área común, llamados la área de tránsito. Uno de los dispositivos OSPF se debe conectar con la área de estructura básica.

Autenticación OSPF de la configuración

Cisco ASA soporta autenticación de MD5 de las actualizaciones de ruteo del OSPF Routing Protocol. La publicación cerrada MD5 en cada paquete OSPF previene la introducción de mensajes de ruteo desautorizados o falsos de las fuentes no aprobadas. La adición de autenticación a sus mensajes OSPF 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 alguien introduce otro dispositivo de ruteo con información de ruta diversa o contraria sobre 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 EIGRP 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 de la OSPF ruta se configura sobre una base del por interface. Todos los vecinos OSPF en las interfaces configuradas para la autenticación del mensaje OSPF deben ser configurados con el mismo modo de autenticación y clave para que las adyacencias sean establecidas.

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

1. En el ASDM, navegue a la **configuración > a la configuración > a la encaminamiento > al OSPF > a la interfaz de dispositivo**, y después haga clic la lengueta de la **autenticación** tal y como se muestra en de esta imagen.En este caso, el OSPF se habilita en la interfaz interior.
2. Elija la **interfaz interior**, y el tecleo **edita**.
3. Bajo autenticación, elija **autenticación de MD5**, y agregue más información sobre los parámetros de autenticación aquí.En este caso, la clave del preshared es **cisco123**, y la

clave ID es **1.**

4. El Haga Click en OK, y entonces hace clic **se aplica**.

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
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 del Cisco IOS (r2)

Router del 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 del Cisco IOS (r1)

Router del 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 del Cisco IOS (R3)

Router del 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
```

Redistribuya en el OSPF con el ASA

Según lo mencionado anterior, usted puede redistribuir las rutas en un proceso de ruteo de OSPF de otro proceso de ruteo de OSPF, un proceso de ruteo del RIP, o de los parásitos atmosféricos y de los Routeconectad configurados en las interfaces OSPF-habilitadas.

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

Configuración de ASDM

1. Elija la **configuración > la configuración > la encaminamiento > el RIP de dispositivo > puesto** para habilitar el RIP, y agregue la red 192.168.1.0 tal y como se muestra en de esta imagen.
2. Haga clic en Apply (Aplicar).
3. Elija la **configuración > la configuración > la encaminamiento > el OSPF > la redistribución de dispositivo > Add** para redistribuir las rutas del RIP en el OSPF.
4. El Haga Click en OK, y entonces hace clic **se aplica**.

Configuración CLI equivalente

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

Usted puede ver la tabla de ruteo del IOS del vecino Router(R2) después de redistribuir las rutas del RIP en el OSPF 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 172.16.0.0/16 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 adverstied by Cisco ASA
```

Verificación

Complete estos pasos para verificar su configuración:

1. En el ASDM, usted puede navegar a **monitorear > encaminamiento > los vecinos OSPF** para ver a cada uno de los vecinos OSPF. Esta imagen muestra al router interno (r2) como vecino activo. Usted puede también ver la interfaz donde reside este vecino, el ID de router de vecino, el estado, y el tiempo muerto.
2. Además, usted puede verificar la tabla de ruteo si usted navega a **monitorear > encaminamiento > las rutas**. En esta imagen, 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).
3. 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 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. Usted puede también utilizar el **comando ospf database de la demostración** para obtener la información sobre las redes doctas 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** es también útil para verificar los vecinos activos y la información correspondiente. Este ejemplo muestra la misma información que usted obtuvo del 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
```

Troubleshooting

Esta sección proporciona la información que pudo facilitar el resolver problemas de los problemas OSPF.

Configuración del vecino estático para el red Point-to-Point

Si usted ha configurado *no-broadcast de punto a punto de la red OSPF* en el ASA, usted debe definir a los vecinos OSPF estáticos para hacer publicidad de las OSPF rutas sobre un Punto a punto, red sin broadcast. Refiera a definir a los vecinos OSPF estáticos para 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 de Debug antes de usar un **comando debug**.

- **haga el debug de los eventos OSPF** — Habilita el debugging de los 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: Refiera a la sección OSPF del debug de la referencia de comandos del dispositivo del Cisco Security, versión 8.0 para más información sobre los diversos comandos que son útiles para resolver problemas el problema.

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