Ejemplo de Configuración de ASA 9.x EIGRP

Contenido

Introducción

Este documento describe cómo configurar Cisco Adaptive Security Appliance (ASA) para aprender las rutas a través del protocolo de routing de gateway interior mejorado (EIGRP), que se admite en la versión 9.x y posteriores del software ASA, y realizar la autenticación.

Prerequisites

Requirements

Cisco requiere que cumpla estas condiciones antes de intentar esta configuración:

- Cisco ASA debe ejecutar la versión 9.x o posterior.

- EIGRP debe estar en modo de contexto único, porque no se soporta en modo de contexto múltiple.

Componentes Utilizados

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

- Cisco ASA Software Version 9.2.1
- Versión 7.2.1 de Cisco Adaptive Security Device Manager (ASDM)
- Cisco IOS® Router que ejecuta la versión 12.4

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.

Antecedentes

Pautas y limitaciones

- Se admite una instancia EIGRP en modo único y por contexto en modo múltiple.
- Se crean dos subprocesos por contexto por instancia de EIGRP en modo múltiple y se pueden ver con el proceso show.
- El resumen automático está desactivado de forma predeterminada.
- No se establece una relación de vecino entre las unidades de clúster en el modo de interfaz individual.
- La información predeterminada de [<acl>] se utiliza para filtrar el bit Exterior en las rutas predeterminadas candidatas entrantes.
- Default-information out [<acl>] se utiliza para filtrar el bit Exterior en las rutas predeterminadas del candidato saliente.

EIGRP y Failover

El código Cisco ASA versión 8.4.4.1 y posterior sincroniza las rutas dinámicas de la unidad ACTIVE a la unidad STANDBY. Además, la eliminación de rutas también se sincroniza con la unidad STANDBY. Sin embargo, el estado de las adyacencias de peer no está sincronizado; sólo el dispositivo ACTIVE mantiene el estado de vecino y participa activamente en el ruteo dinámico. Consulte Preguntas frecuentes sobre ASA: ¿Qué ocurre después de la conmutación por fallas si las rutas dinámicas están sincronizadas? para más información.

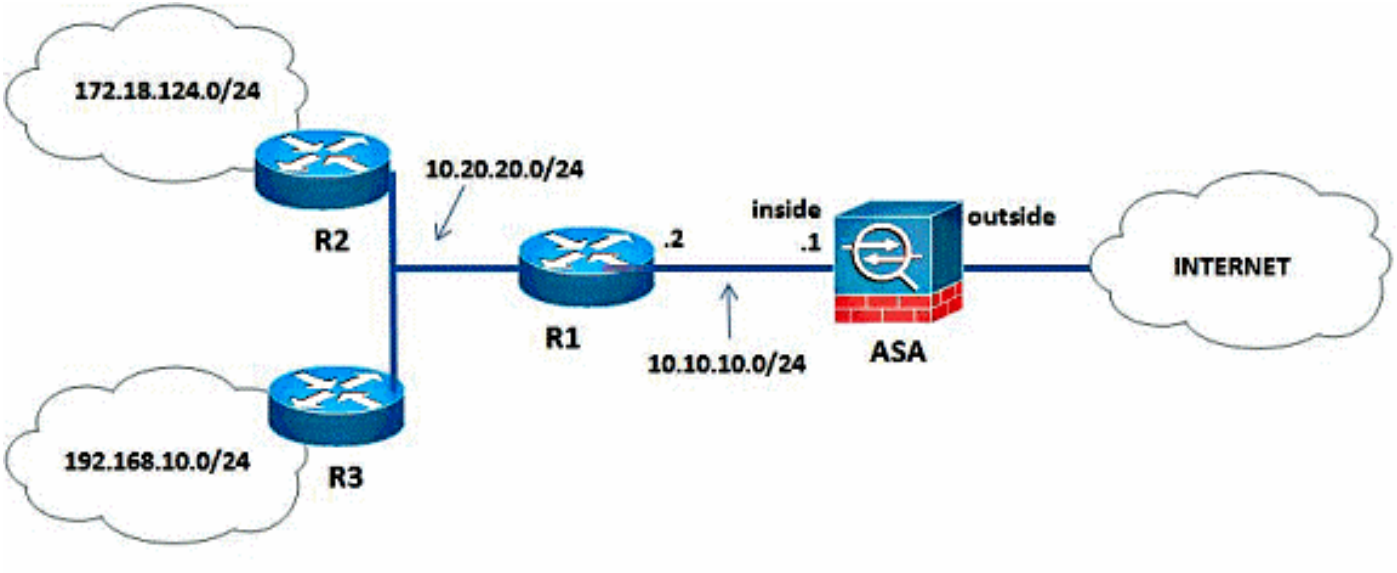
Configurar

Esta sección describe cómo configurar las funciones que se tratan 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 la topología de red que se ilustra, la dirección IP de la interfaz interna de Cisco ASA es 10.10.10.1/24. El objetivo es configurar EIGRP en Cisco ASA para aprender las rutas a las redes internas (10.20.20.0/24, 172.18.124.0/24 y 192.168.10.0/24) dinámicamente a través del router adyacente (R1). R1 aprende las rutas a redes internas remotas a través de los otros dos routers (R2 y R3).

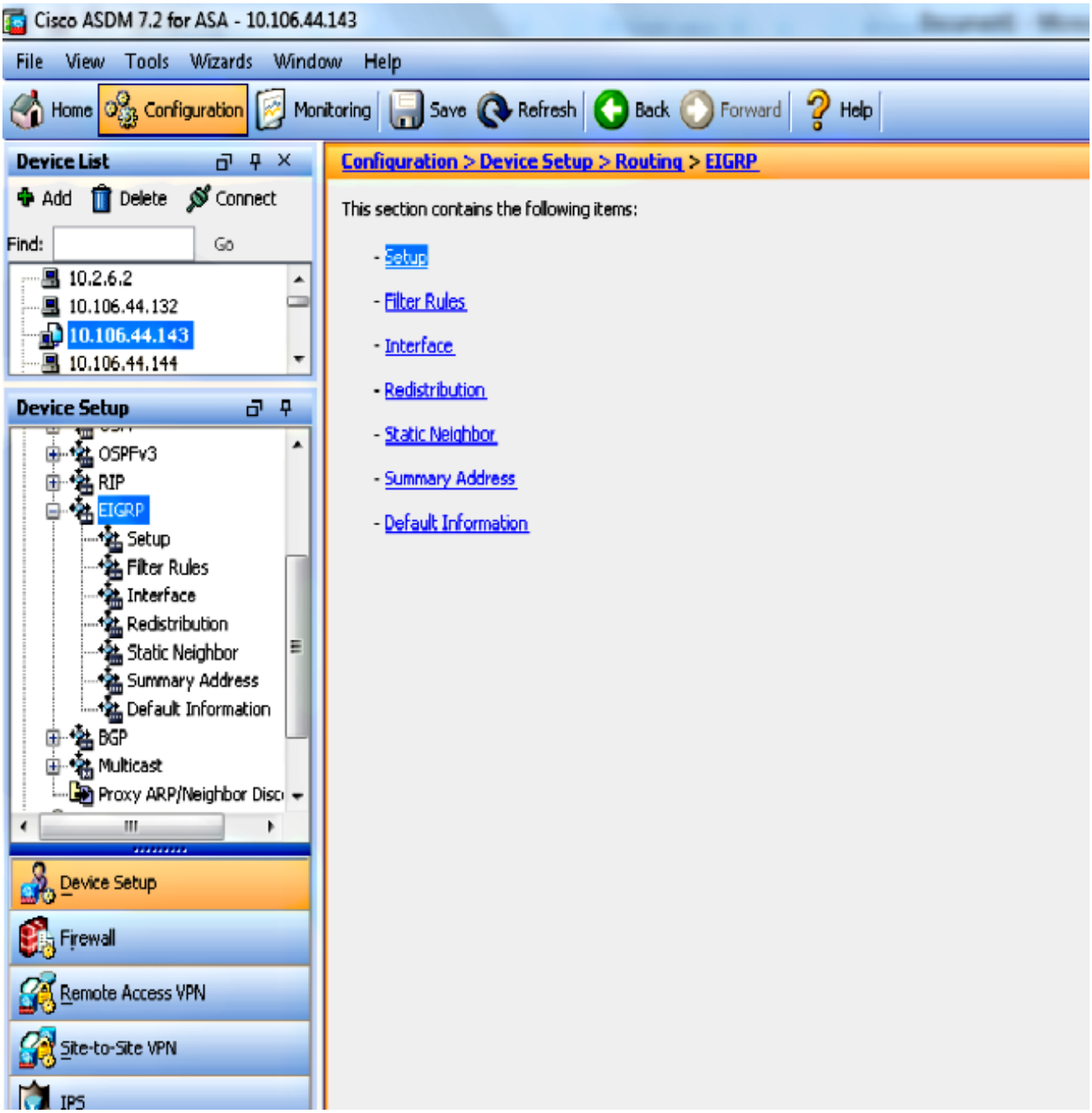
Configuración de ASDM

ASDM es una aplicación basada en navegador que se utiliza para configurar y monitorear el software en dispositivos de seguridad. El ASDM se carga desde el dispositivo de seguridad y luego se utiliza para configurar, monitorear y administrar el dispositivo. También puede utilizar el iniciador ASDM 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.

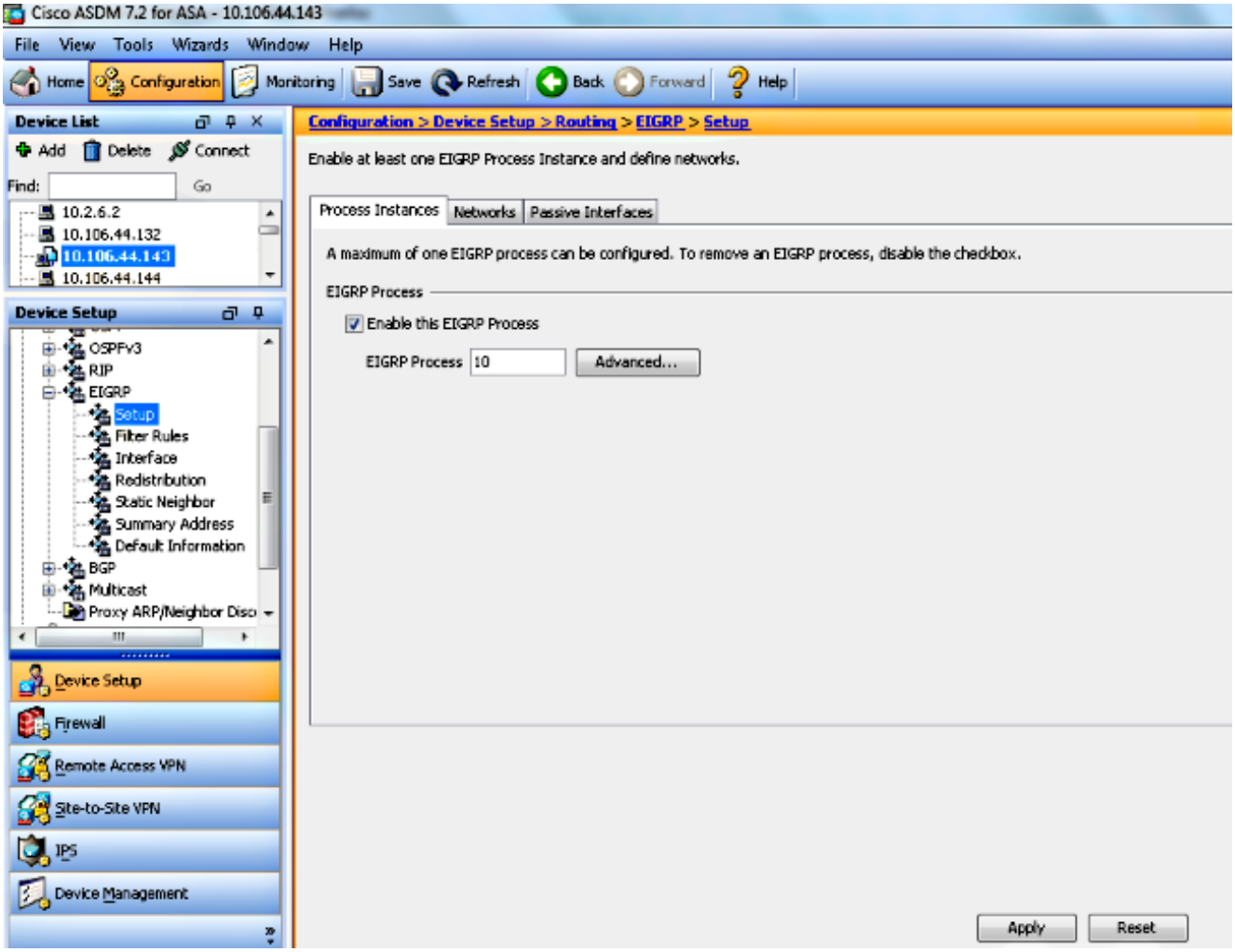
Complete estos pasos para configurar EIGRP en Cisco ASA.

1. Inicie sesión en Cisco ASA con el ASDM.

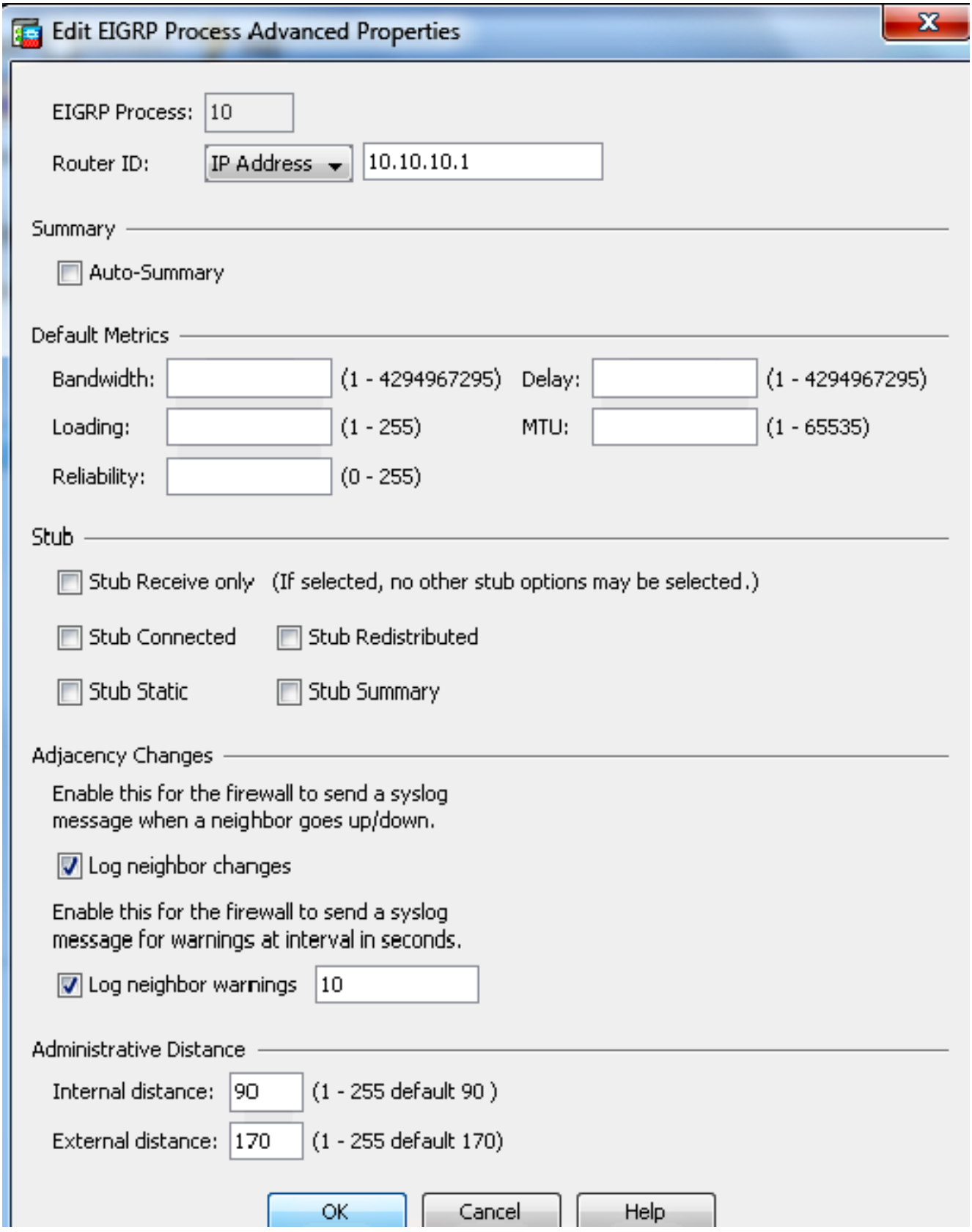
2. Navegue hasta el área **Configuration > Device Setup > Routing > EIGRP** de la interfaz ASDM, como se muestra en esta captura de pantalla.



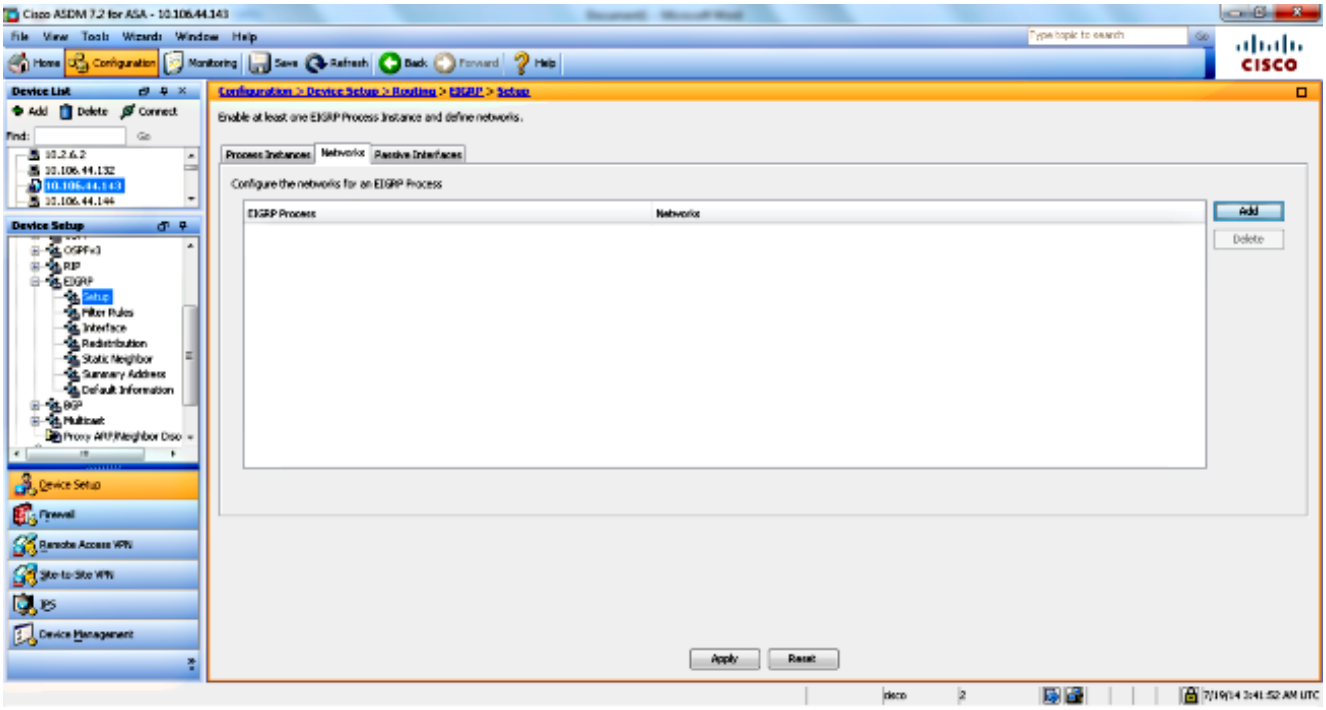
3. Habilite el proceso de ruteo EIGRP en la pestaña **Setup > Process Instases**, como se muestra en esta captura de pantalla. En este ejemplo, el proceso EIGRP es **10**.



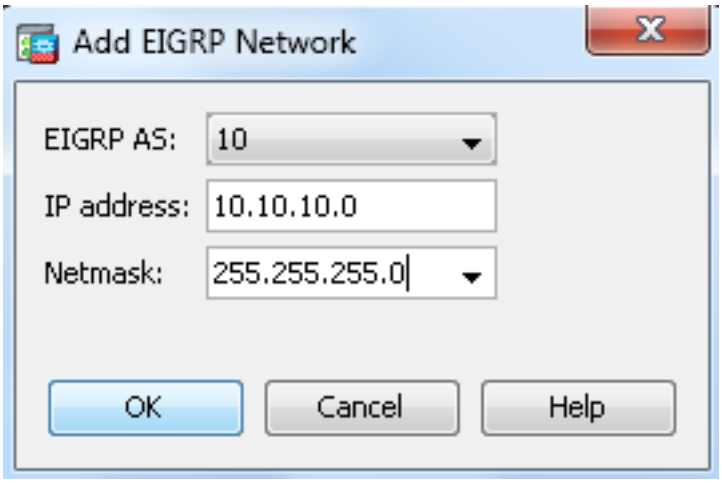
4. Puede configurar parámetros de proceso de ruteo EIGRP avanzado opcionales. Haga clic en **Avanzado** en la pestaña **Setup > Process Instancias**. Puede configurar el proceso de ruteo EIGRP como un proceso de ruteo stub, inhabilitar el resumen automático de ruta, definir las métricas predeterminadas para las rutas redistribuidas, cambiar las distancias administrativas para las rutas EIGRP internas y externas, configurar un ID de router estático y habilitar o inhabilitar el registro de los cambios de adyacencia. En este ejemplo, el ID de router EIGRP se configura estáticamente con la dirección IP de la interfaz interna (10.10.10.1). Además, **Auto-Summary** también está inhabilitado. Todas las demás opciones se configuran con sus valores predeterminados.



5. Después de completar los pasos anteriores, defina las redes e interfaces que participan en el ruteo EIGRP en la pestaña **Setup > Networks**. Haga clic en **Agregar** como se muestra en esta captura de pantalla.



6. Aparece esta pantalla. En este ejemplo, la única red que agrega es la red interna (10.10.10.0/24), ya que EIGRP sólo está habilitado en la interfaz interna.



Sólo las interfaces con una dirección IP que se encuentra dentro de las redes definidas participan en el proceso de ruteo EIGRP. Si tiene una interfaz que no desea participar en el ruteo EIGRP pero que está conectada a una red que desea anunciar, configure una entrada de red en la pestaña **Setup > Networks** que cubre la red a la que está conectada la interfaz, y luego configure esa interfaz como una interfaz pasiva para que la interfaz no pueda enviar ni recibir actualizaciones EIGRP.

Nota: Las interfaces configuradas como pasivas no envían ni reciben actualizaciones EIGRP.

7. 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 EIGRP.

8. Opcionalmente, puede configurar la redistribución de rutas. Cisco ASA puede redistribuir las

rutas detectadas por el protocolo de información de routing (RIP) y Open Shortest Path First (OSPF) en el proceso de routing EIGRP. También puede redistribuir las rutas estáticas y conectadas en el proceso de ruteo EIGRP. No es necesario redistribuir las rutas estáticas o conectadas si se encuentran dentro del rango de una red configurada en la ficha **Setup > Networks**. Defina la redistribución de rutas en el panel de redistribución.

9. Los paquetes Hello EIGRP se envían como paquetes multicast. Si un vecino EIGRP se encuentra a través de una red no broadcast, debe definir manualmente ese vecino. Cuando define manualmente un vecino EIGRP, los paquetes Hello se envían a ese vecino como mensajes unicast. Para definir vecinos EIGRP estáticos, vaya al panel **Vecino estático**.

10. De forma predeterminada, se envían y aceptan las rutas predeterminadas. Para restringir o inhabilitar el envío y recepción de información de ruta predeterminada, abra el **panel Configuration > Device Setup > Routing > EIGRP > Default Information** . El panel Información predeterminada muestra una tabla de reglas para controlar el envío y recepción de información de ruta predeterminada en las actualizaciones de EIGRP.

    Nota: Puede tener una regla *"in"* y una "*out*" para cada proceso de ruteo EIGRP. (Actualmente sólo se admite un proceso.)

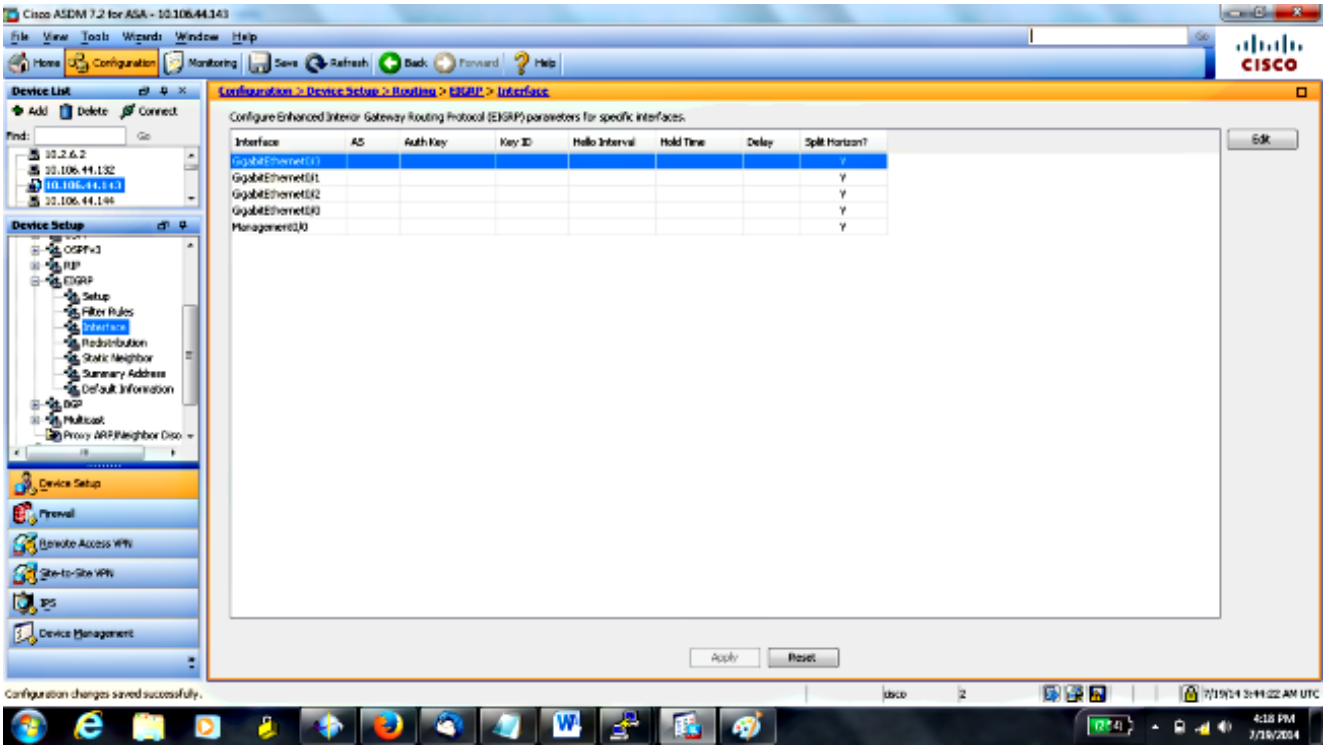
Configuración de la Autenticación EIGRP

Cisco ASA admite la autenticación MD5 de las actualizaciones de ruteo del protocolo de ruteo EIGRP. El resumen con la llave MD5 en cada paquete EIGRP evita la introducción de mensajes de ruteo no autorizados o falsos de fuentes no aprobadas. La adición de la autenticación a sus mensajes EIGRP 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 las adiciones no autorizadas de routers EIGRP en su topología de ruteo.

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

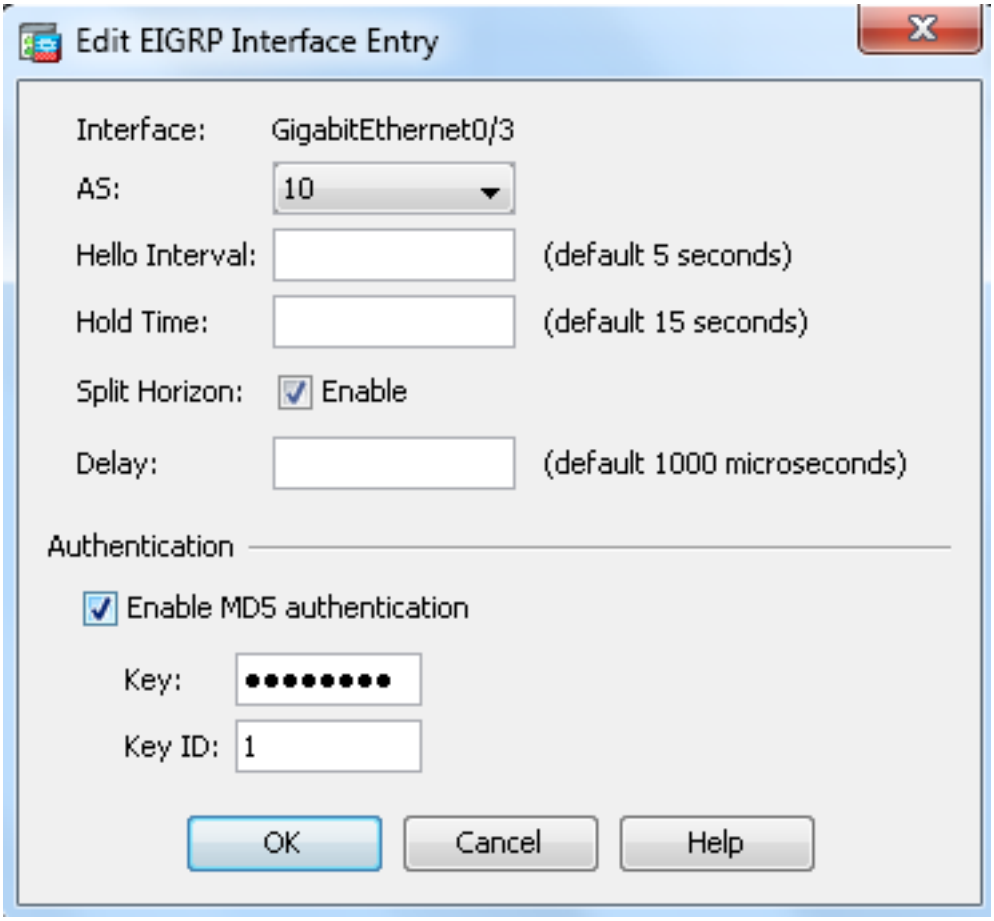
Complete estos pasos para habilitar la autenticación EIGRP MD5 en Cisco ASA.

1. En el ASDM, navegue hasta **Configuration > Device Setup > Routing > EIGRP > Interface** como se muestra.



2. En este caso, EIGRP está habilitado en la interfaz interna (GigabitEthernet 0/1). Elija la interfaz **GigabitEthernet 0/1** y haga clic en **Editar**.

3. En Authentication , elija **Enable MD5 authentication**. Agregue aquí más información sobre los parámetros de autenticación. En este caso, la clave previamente compartida es **cisco123**, y el ID de clave es **1**.



Filtrado de Rutas EIGRP

Con EIGRP, puede controlar las actualizaciones de ruteo que se envían y reciben. En este ejemplo, bloqueará las actualizaciones de ruteo en el ASA para el prefijo de red 192.168.10.0/24, que está detrás de R1. Para el filtrado de rutas, sólo puede utilizar la **ACL ESTÁNDAR**.

```
access-list eigrp standard deny 192.168.10.0 255.255.255.0
access-list eigrp standard permit any

router eigrp 10
distribute-list eigrp in
```

Verificación

```
ASA(config)# show access-list eigrp
access-list eigrp; 2 elements; name hash: 0xd43d3adc
access-list eigrp line 1 standard deny 192.168.10.0 255.255.255.0 (hitcnt=3) 0xeb48ecd0
access-list eigrp line 2 standard permit any4 (hitcnt=12) 0x883fe5ac
```

Configuraciones

Configuración de Cisco ASA CLI

Esta es la configuración de Cisco ASA CLI.

```
!outside interface configuration

interface GigabitEthernet0/0
description outside interface connected to the Internet
nameif outside
security-level 0
ip address 198.51.100.120 255.255.255.0
!

!inside interface configuration

interface GigabitEthernet0/1
description interface connected to the internal network
nameif inside
security-level 100
ip address 10.10.10.1 255.255.255.0
!

!EIGRP authentication is configured on the inside interface

authentication key eigrp 10 cisco123 key-id 1
authentication mode eigrp 10 md5
!

!management interface configuration

interface Management0/0
nameif management
security-level 99
```

```
ip address 10.10.20.1 255.255.255.0 management-only
!
!

!EIGRP Configuration - the CLI configuration is very similar to the
!Cisco IOS router EIGRP configuration.

router eigrp 10
no auto-summary
eigrp router-id 10.10.10.1
network 10.10.10.0 255.255.255.0
!

!This is the static default gateway configuration

route outside 0.0.0.0 0.0.0.0 198.51.100.1 1
```

Configuración CLI del router Cisco IOS (R1)

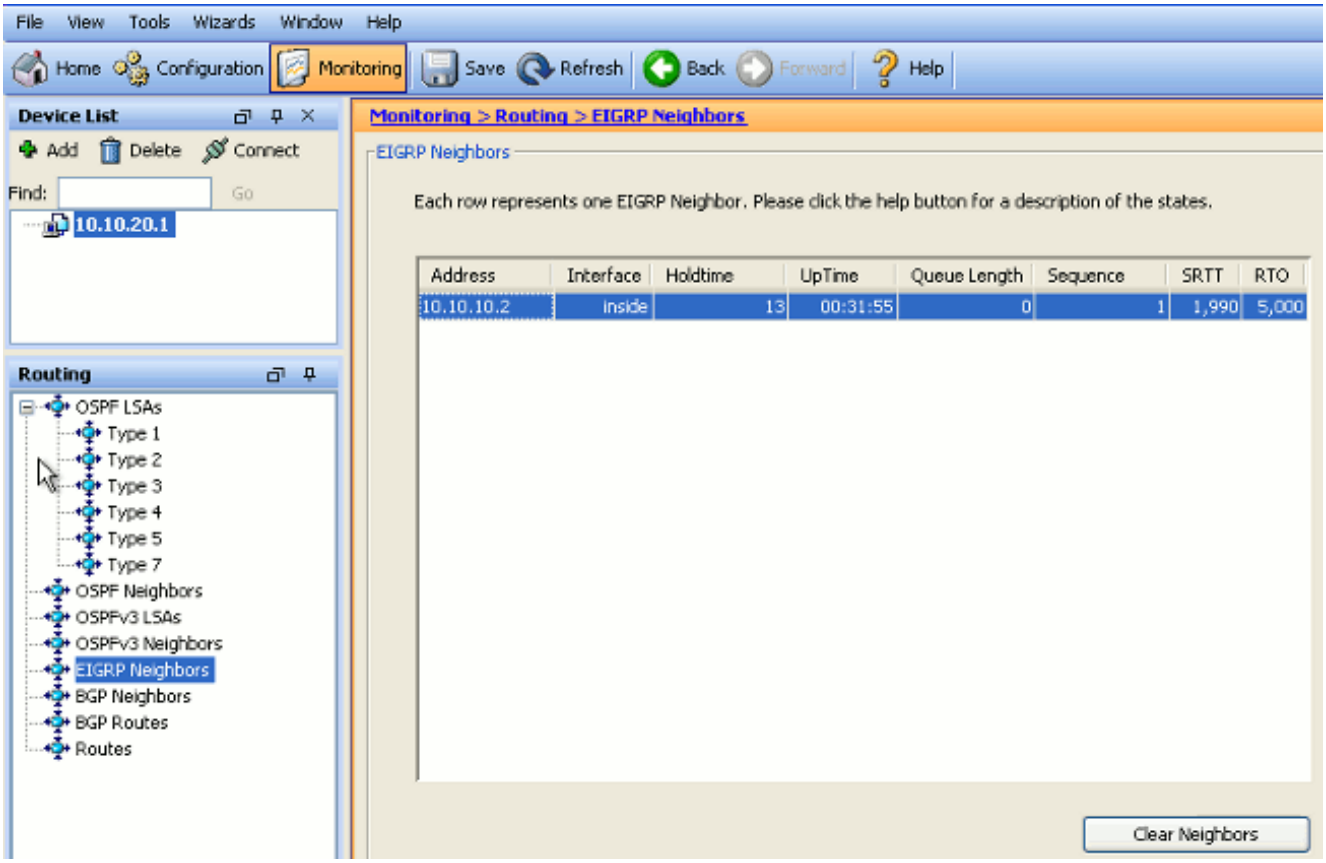
Ésta es la configuración CLI de R1 (router interno).

```
!!Interface that connects to the Cisco ASA. Notice the EIGRP authentication
paramenters.


interface FastEthernet0/0
ip address 10.10.10.2 255.255.255.0
ip authentication mode eigrp 10 md5
ip authentication key-chain eigrp 10 MYCHAIN
!
!

! EIGRP Configuration

router eigrp 10
network 10.10.10.0 0.0.0.255
network 10.20.20.0 0.0.0.255
network 172.18.124.0 0.0.0.255
network 192.168.10.0
no auto-summary
```

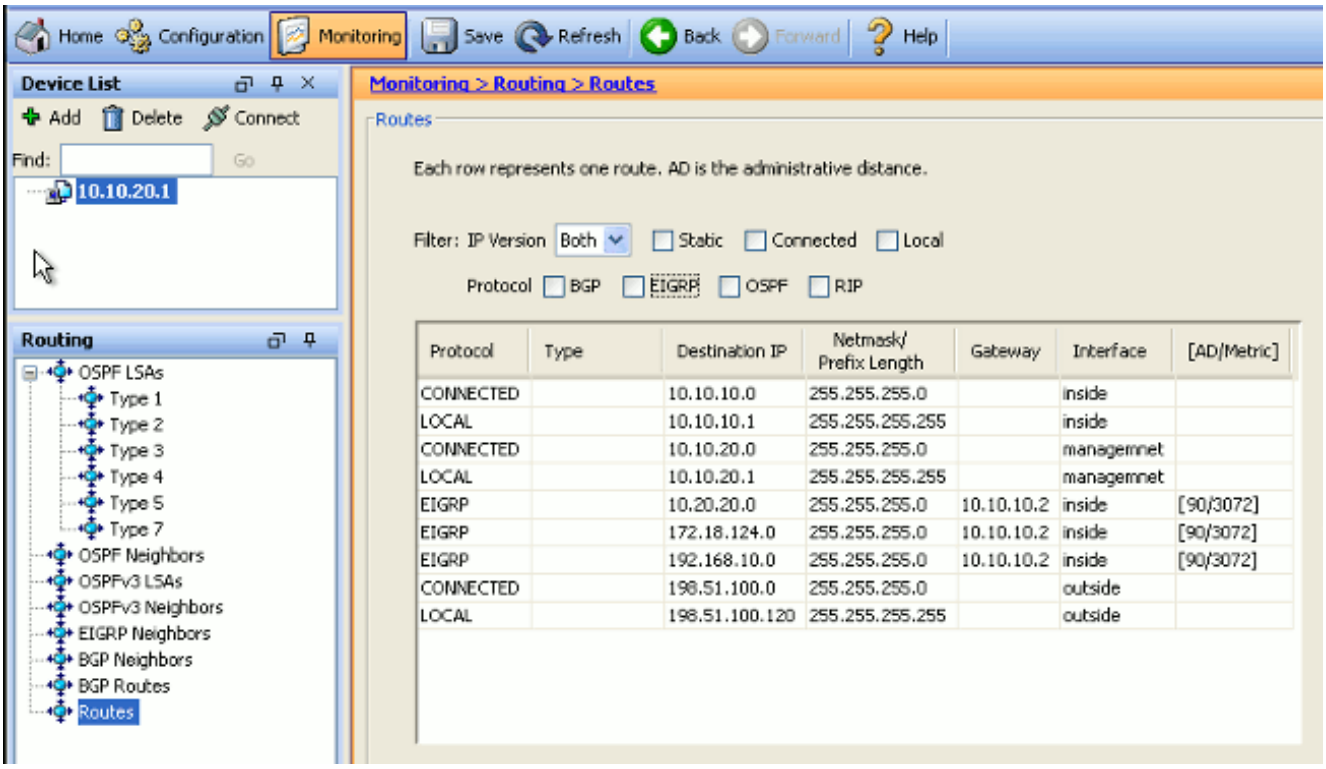
Verificación

Complete estos pasos para verificar su configuración.

1. En el ASDM, puede navegar a **Monitoring > Routing > EIGRP Neighbor** para ver cada uno de los vecinos EIGRP. Esta captura de pantalla muestra el router interno (R1) como vecino activo. También puede ver la interfaz en la que reside este vecino, el tiempo de espera y cuánto tiempo ha estado activa la relación de vecino (UpTime).



2. Además, puede verificar la tabla de ruteo si navega a **Monitoring > Routing > Routes**. En esta captura de pantalla, puede ver que las redes **192.168.10.0/24, 172.18.124.0/24** y **10.20.20.0/24** se aprenden a través de R1 (**10.10.10.2**).



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 100.10.10.2 to network 0.0.0.0
C 198.51.100.0 255.255.255.0 is directly connected, outside
D 192.168.10.0 255.255.255.0 [90/131072] via 10.10.10.2, 0:32:29, inside
D 172.18.124.0 255.255.255.0 [90/131072] via 10.10.10.2, 0:32:29, inside
C 127.0.0.0 255.255.0.0 is directly connected, cplane
D 10.20.20.0 255.255.255.0 [90/28672] via 10.10.10.2, 0:32:29, inside
C 10.10.10.0 255.255.255.0 is directly connected, inside
C 10.10.20.0 255.255.255.0 is directly connected, management
S* 0.0.0.0 0.0.0.0 [1/0] via 198.51.100.1, outside
```

Con ASA versión 9.2.1 y posteriores, puede utilizar el comando **show route eigrp** para mostrar solamente las rutas EIGRP.

```
ciscoasa(config)# show route eigrp

Codes: L - local, C - connected, S - static, 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
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, + - replicated route

Gateway of last resort is not set

D 192.168.10.0 255.255.255.0 [90/131072] via 10.10.10.2, 0:32:29, inside
D 172.18.124.0 255.255.255.0 [90/131072] via 10.10.10.2, 0:32:29, inside
D 10.20.20.0 255.255.255.0 [90/28672] via 10.10.10.2, 0:32:29, inside
```

3. También puede utilizar el comando **show eigrp topology** para obtener información sobre las redes aprendidas y la topología EIGRP.

```
    ciscoasa# show eigrp topology
EIGRP-IPv4 Topology Table for AS(10)/ID(10.10.10.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
r - reply Status, s - sia Status
P 10.20.20.0 255.255.255.0, 1 successors, FD is 28672
via 10.10.10.2 (28672/28416), GigabitEthernet0/1
P 10.10.10.0 255.255.255.0, 1 successors, FD is 2816
via Connected, GigabitEthernet0/1
P 192.168.10.0 255.255.255.0, 1 successors, FD is 131072
via 10.10.10.2 (131072/130816), GigabitEthernet0/1
P 172.18.124.0 255.255.255.0, 1 successors, FD is 131072
via 10.10.10.2 (131072/130816), GigabitEthernet0/1
```

4. El comando **show eigrp neighbors** también es útil para verificar los vecinos activos y la información del corresponsal. Este ejemplo muestra la misma información que obtuvo del ASDM en el Paso 1.

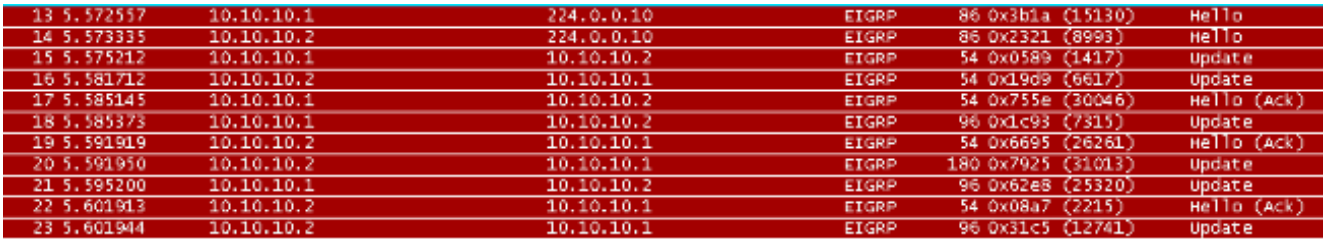
```
ciscoasa# show eigrp neighbors
EIGRP-IPv4 neighbors for process 10
H Address Interface Hold Uptime SRTT RTO Q Seq (sec) (ms)Cnt Num

0 10.10.10.2 Gi0/1 12 00:39:12 107 642 0 1
```

Flujo de paquetes

Aquí está el flujo de paquetes.

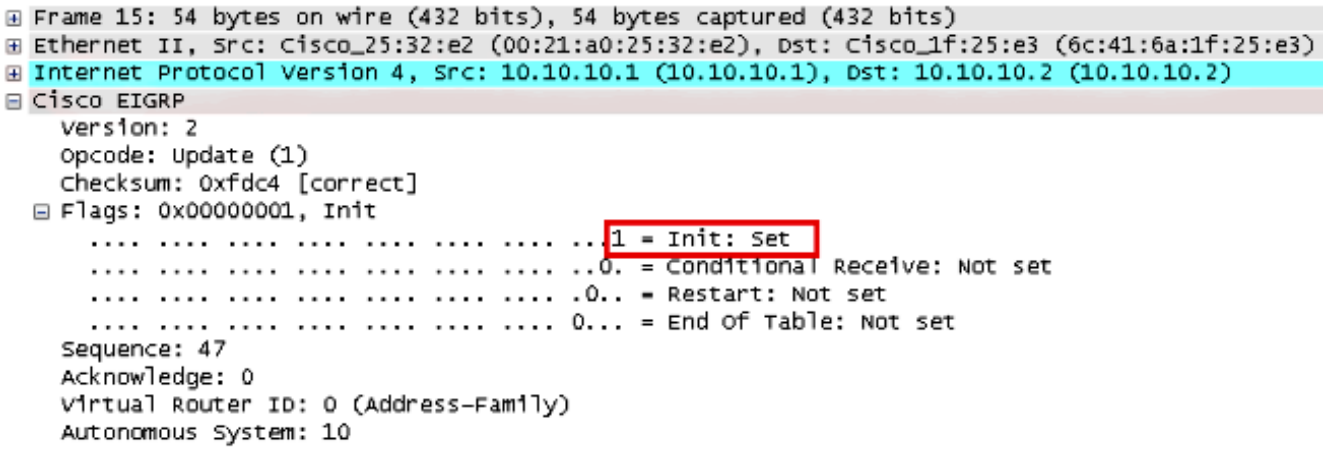
1. El ASA se activa en el link y envía un paquete mCast Hello a través de todas sus interfaces configuradas por EIGRP.

2. R1 recibe un paquete Hello y envía un paquete mCast Hello.



3. El ASA recibe el paquete Hello y envía un paquete Update con un bit inicial configurado, lo que indica que éste es el proceso de inicialización.

4. R1 recibe un paquete Update y envía un paquete Update con un bit inicial configurado, lo que indica que éste es el proceso de inicialización.



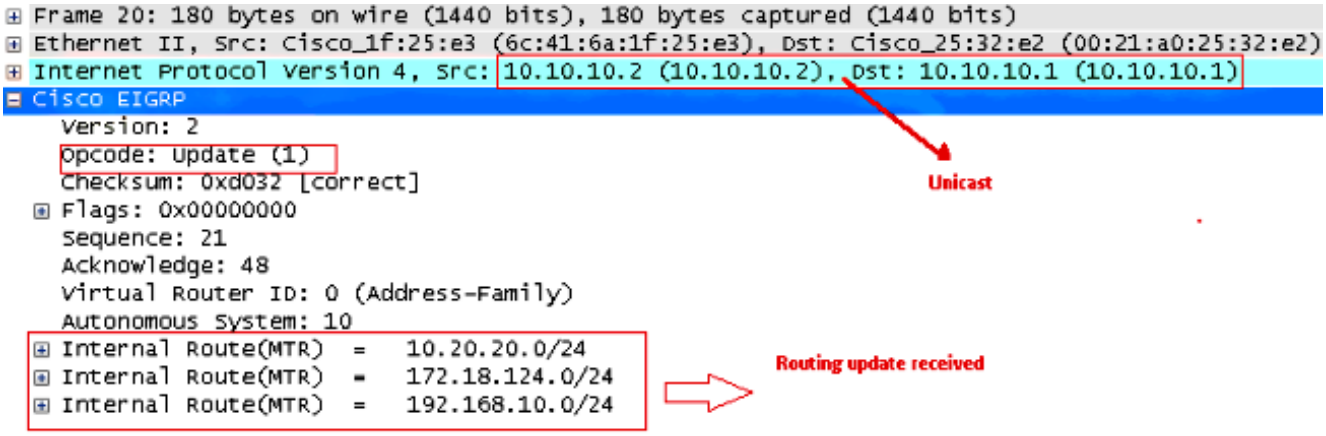
5. Después de que el ASA y el R1 hayan intercambiado saludos y de que se establezca la adyacencia de vecino, tanto el ASA como el R1 responden con un paquete ACK, lo que

indica que se recibió la información de actualización.

6. ASA envía su información de ruteo a R1 en un paquete Update.

7. R1 inserta la información del paquete Update en su tabla de topología. La tabla de topología incluye todos los destinos anunciados por los vecinos. Se organiza de modo que se muestre cada destino, junto con todos los vecinos que pueden viajar al destino y sus métricas asociadas.

8. R1 luego envía un paquete de actualización al ASA.



9. Una vez que recibe el paquete Update, el ASA envía un paquete ACK a R1. Después de que el ASA y R1 reciban correctamente los paquetes Update entre sí, están listos para elegir las rutas sucesoras (mejores) y sucesoras factibles (de respaldo) en la tabla de topología, y ofrecer las rutas sucesoras a la tabla de ruteo.

Troubleshoot

Esta sección incluye información sobre los comandos **debug** y **show** que pueden ser útiles para resolver problemas de EIGRP.

Comandos para resolución de problemas

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilize el OIT para ver una análisis de la salida del comando show.

> **Nota:** Consulte Información Importante sobre Comandos de Debug antes de usar un comando debug. Para mostrar la información de depuración en la máquina de estado finito Diffusing Update Algorithm (DUAL), utilice el comando **debug eigrp fsm** en el modo EXEC privilegiado. Este comando le permite observar la actividad sucesora factible de EIGRP y determinar si las actualizaciones de ruta son instaladas y eliminadas por el proceso de ruteo.

Ésta es la salida del comando **debug** dentro del par exitoso con R1. Puede ver cada una de las diferentes rutas que se instalan correctamente en el sistema.

```
EIGRP-IPv4(Default-IP-Routing-Table:10): Callback: route_adjust GigabitEthernet0/1
DUAL: dest(10.10.10.0 255.255.255.0) not active
DUAL: rcvupdate: 10.10.10.0 255.255.255.0 via Connected metric 2816/0 on topoid 0
DUAL: Find FS for dest 10.10.10.0 255.255.255.0. FD is 4294967295, RD is 4294967
295 on topoid 0 found
DUAL: RT installed 10.10.10.0 255.255.255.0 via 0.0.0.0
DUAL: Send update about 10.10.10.0 255.255.255.0. Reason: metric chg on topoid
0
DUAL: Send update about 10.10.10.0 255.255.255.0. Reason: new if on topoid 0
DUAL: dest(10.20.20.0 255.255.255.0) not active
DUAL: rcvupdate: 10.20.20.0 255.255.255.0 via 10.10.10.2 metric 28672/28416 on t
opoid 0
DUAL: Find FS for dest 10.20.20.0 255.255.255.0. FD is 4294967295, RD is 4294967
295 on topoid 0 found
EIGRP-IPv4(Default-IP-Routing-Table:10): route installed for 10.20.20.0 ()
DUAL: RT installed 10.20.20.0 255.255.255.0 via 10.10.10.2
DUAL: Send update about 10.20.20.0 255.255.255.0. Reason: metric chg on topoid
0
DUAL: Send update about 10.20.20.0 255.255.255.0. Reason: new if on topoid 0
DUAL: dest(172.18.124.0 255.255.255.0) not active
DUAL: rcvupdate: 172.18.124.0 255.255.255.0 via 10.10.10.2 metric 131072/130816
on topoid 0
DUAL: Find FS for dest 172.18.124.0 255.255.255.0. FD is 4294967295, RD is 42949
67295 on topoid 0 found
EIGRP-IPv4(Default-IP-Routing-Table:10): route installed for 172.18.124.0 ()
DUAL: RT installed 172.18.124.0 255.255.255.0 via 10.10.10.2
DUAL: Send update about 172.18.124.0 255.255.255.0. Reason: metric chg on topoi
d 0
DUAL: Send update about 172.18.124.0 255.255.255.0. Reason: new if on topoid 0
DUAL: dest(192.168.10.0 255.255.255.0) not active
DUAL: rcvupdate: 192.168.10.0 255.255.255.0 via 10.10.10.2 metric 131072/130816
on topoid 0
DUAL: Find FS for dest 192.168.10.0 255.255.255.0. FD is 4294967295, RD is 42949
67295 on topoid 0 found
EIGRP-IPv4(Default-IP-Routing-Table:10): route installed for 192.168.10.0 ()
DUAL: RT installed 192.168.10.0 255.255.255.0 via 10.10.10.2
DUAL: Send update about 192.168.10.0 255.255.255.0. Reason: metric chg on topoi
d 0
DUAL: Send update about 192.168.10.0 255.255.255.0. Reason: new if on topoid 0
```

También puede utilizar el comando **debug eigrp neighbor**. Este es el resultado de este comando **debug** cuando Cisco ASA creó con éxito una nueva relación de vecino con R1.

```
ciscoasa# EIGRP-IPv4(Default-IP-Routing-Table:10): Callback: route_adjust Gigabi
tEthernet0/1
EIGRP: New peer 10.10.10.2
EIGRP-IPv4(Default-IP-Routing-Table:10): route installed for 10.20.20.0 ()
EIGRP-IPv4(Default-IP-Routing-Table:10): route installed for 172.18.124.0 ()
EIGRP-IPv4(Default-IP-Routing-Table:10): route installed for 192.168.10.0 ()
```

También puede utilizar los paquetes debug EIGRP para obtener información detallada sobre el intercambio de mensajes EIGRP entre Cisco ASA y sus pares. En este ejemplo, la clave de autenticación se cambió en el router (R1) y el resultado de la depuración muestra que el problema es una falta de coincidencia de autenticación.

```
ciscoasa# EIGRP: Sending HELLO on GigabitEthernet0/1
AS 655362, Flags 0x0, Seq 0/0 interfaceQ 1/1 iidbQ un/rely 0/0
EIGRP: pkt key id = 1, authentication mismatch
EIGRP: GigabitEthernet0/1: ignored packet from 10.10.10.2, opcode = 5
(invalid authentication)
```

El Vecindario EIGRP Va Abajo con Syslogs ASA-5-336010

ASA descarta la vecindad EIGRP cuando se realizan cambios en la lista de distribución EIGRP. Se ve este mensaje de Syslog.

```
EIGRP Nieghborship Resets with syslogs ASA-5-336010: EIGRP-IPv4: PDM(314 10:
Neighbor 10.15.0.30 (GigabitEthernet0/0) is down: route configuration changed
```

Con esta configuración, cada vez que se **agrega una nueva entrada acl** en la ACL, la **lista de red Eigrp** se reinicia la vecindad EIGRP.

```
router eigrp 10
distribute-list Eigrp-network-list in
network 10.10.10.0 255.0.0.0
passive-interface default
no passive-interface inside
redistribute static

access-list Eigrp-network-list standard permit any
```

Puede observar que la relación de vecino está activa con el dispositivo adyacente.

```
ciscoasa(config)# show eigrp neighbors
EIGRP-IPv4 neighbors for process 10
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 10.10.10.2 Gi0/3 10 00:01:22 1 5000 0 5

ciscoasa(config)# show eigrp neighbors
EIGRP-IPv4 neighbors for process 10
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 10.10.10.2 Gi0/3 13 00:01:29 1 5000 0 5
```

Ahora puede agregar **access-list Eigrp-network-list standard deny 172.18.24.0 255.255.255.0**.

```
%ASA-5-111010: User 'enable_15', running 'CLI' from IP 0.0.0.0, executed 'debug
eigrp fsm'
%ASA-7-111009: User 'enable_15' executed cmd: show access-list
%ASA-5-111008: User 'enable_15' executed the 'access-list Eigrp-network-list line
1 permit 172.18.24.0 255.255.255.0' command.
%ASA-5-111010: User 'enable_15', running 'CLI' from IP 0.0.0.0, executed 'access-list
Eigrp-network-list line 1 permit 172.18.24.0 255.255.255.0'
%ASA-7-111009: User 'enable_15' executed cmd: show eigrp neighbors
%ASA-5-336010: EIGRP-IPv4: PDM(599 10: Neighbor 10.10.10.2 (GigabitEthernet0/3) is
down: route configuration changed
%ASA-5-336010: EIGRP-IPv4: PDM(599 10: Neighbor 10.10.10.2 (GigabitEthernet0/3) is
up: new adjacency
```

Estos registros se pueden ver en **debug eigrp fsm**.

```
IGRP2: linkdown: start - 10.10.10.2 via GigabitEthernet0/3
DUAL: Destination 10.10.10.0 255.255.255.0 for topoid 0
DUAL: linkdown: finish
```

Este es el comportamiento esperado en todas las nuevas versiones de ASA de 8.4 y 8.6 a 9.1. Lo mismo se ha observado en los routers que ejecutan los trenes de código 12.4 a 15.1. Sin embargo, este comportamiento no se observa en la versión 8.2 de ASA ni en las versiones

anteriores del software ASA porque los cambios realizados en una ACL no restablecen las adyacencias EIGRP.

Dado que EIGRP envía la tabla de topología completa a un vecino cuando el vecino aparece por primera vez y luego envía solamente los cambios, la configuración de una lista de distribución con la naturaleza de EIGRP basada en eventos dificultaría la aplicación de los cambios sin un reinicio completo de la relación de vecino. Los routers necesitarían realizar un seguimiento de cada ruta enviada y recibida de un vecino para saber qué ruta ha cambiado (es decir, si se enviaría o no se aceptaría) para aplicar los cambios según lo dictado por la lista de distribución actual. Es mucho más fácil simplemente derribar y restablecer la adyacencia entre vecinos.

Cuando una adyacencia se desactiva y se restablece, todas las rutas aprendidas entre vecinos particulares simplemente se olvidan y toda la sincronización entre los vecinos se realiza de nuevo - con la nueva lista de distribución en su lugar.

La mayoría de las técnicas EIGRP que utiliza para resolver problemas de routers Cisco IOS se pueden aplicar en Cisco ASA. Para resolver problemas de EIGRP, utilice el Diagrama de Flujo de Troubleshooting Principal; comience en el cuadro marcado **Main**.