

# Ejemplo de configuración de EIGRP ASA 9.x

## Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Guías de consulta y limitaciones](#)

[EIGRP y Conmutación por falla](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuración de ASDM](#)

[Autenticación del EIGRP de la configuración](#)

[Filtración de la ruta EIGRP](#)

[Verificación](#)

[Configuraciones](#)

[Configuración CLI de Cisco ASA](#)

[Configuración CLI del router del Cisco IOS \(r1\)](#)

[Verificación](#)

[Flujo de paquetes](#)

[Troubleshooting](#)

[Comandos para resolución de problemas](#)

[La vecindad EIGRP va abajo con los Syslog ASA-5-336010](#)

## Introducción

Este documento describe cómo configurar el dispositivo de seguridad adaptante de Cisco (ASA) para aprender las rutas con el Enhanced Interior Gateway Routing Protocol (EIGRP), que se soporta en la versión de software 9.x ASA y posterior, y realizar la autenticación.

## Prerrequisitos

### Requisitos

Cisco requiere que usted cumpla estas condiciones antes de que usted intente esta configuración:

- Cisco ASA debe funcionar con la versión 9.x o posterior.

- El EIGRP debe estar en el modo del solo-contexto, porque no se soporta en el modo del multi-contexto.

## Componentes Utilizados

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

- Versión de software 9.2.1 de Cisco ASA
- Versión 7.2.1 del Cisco Adaptive Security Device Manager (ASDM)
- Router del <sup>®</sup> del Cisco IOS que funciona con la versión 12.4

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.

## Antecedentes

### Guías de consulta y limitaciones

- Un caso del EIGRP se soporta en el modo simple y por el contexto en con varios modos de funcionamiento.
- Dos hilos se crean por el contexto por el caso del EIGRP en con varios modos de funcionamiento y se pueden ver con el proceso de la demostración.
- El automóvil summary se inhabilita por abandono.
- Una relación de vecino no se establece entre las unidades de cluster en el modo de la interfaz individual.
- la Valor por defecto-información en el [<acl>] se utiliza para filtrar el bit exterior en las Default rutas candidato entrantes.
- de la Valor por defecto-información el [<acl>] hacia fuera se utiliza para filtrar el bit exterior en las Default rutas candidato salientes.

### EIGRP y Conmutación por falla

La versión del código 8.4.4.1 de Cisco ASA y posterior sincroniza las rutas dinámico de la unidad activa a la unidad en espera. Además, la cancelación de las rutas también se sincroniza a la unidad en espera. Sin embargo, el estado de las adyacencias del par no se sincroniza; solamente el dispositivo activo mantiene al estado de vecino y participa activamente en el Dynamic Routing. Refiera a [ASA FAQ: ¿Qué sucede después de la Conmutación por falla si se sincronizan las rutas dinámico?](#) para más información.

## Configurar

Esta sección describe cómo configurar las características cubiertas 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 se ilustra que, la dirección IP de la interfaz interior de Cisco ASA es 10.10.10.1/24. La meta es configurar el 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). El r1 aprende las rutas a las redes internas remotas a través del otro dos Routers (r2 y R3).

## Configuración de ASDM

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

Complete estos pasos para configurar el EIGRP en Cisco ASA.

1. Inicie sesión a Cisco ASA con el ASDM.
2. Navegue al área de la **configuración > de la configuración de dispositivo > de la encaminamiento > del EIGRP de la** interfaz del ASDM, tal y como se muestra en de este tiro de pantalla.
3. Habilite el proceso de EIGRP Routing en la lengüeta de los **casos de la configuración > del proceso**, tal y como se muestra en de este tiro de pantalla. En este ejemplo, el proceso EIGRP es 10.
4. Usted puede configurar los parámetros de proceso avanzados opcionales de EIGRP Routing. Teclee **avanzado** en la lengüeta de los **casos de la configuración > del proceso**. Usted puede configurar el proceso de EIGRP Routing como un proceso de ruteo de stub, inhabilita el resumen de Route automático, define la métrica predeterminada para las rutas redistribuido, cambia las distancias administrativas para interno y las rutas EIGRP externas, configura un Router ID estático, y habilita o inhabilita el registro de los cambios de la adyacencia. En este ejemplo, configuran al router EIGRP ID estáticamente con la dirección IP de la interfaz interior (10.10.10.1). Además, el **automóvil summary** también se inhabilita. Todas las otras opciones se configuran con sus valores predeterminados.

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

6. Esta pantalla aparece. En este ejemplo, la única red que usted agrega es la red interna (10.10.10.0/24) puesto que el EIGRP se habilita solamente en la interfaz interior.

Interconecta solamente con una dirección IP que las caídas dentro de las redes definidas participen en el proceso de EIGRP Routing. Si usted tiene una interfaz que usted no quiere participar en el EIGRP Routing pero eso está asociada a una red que usted quiera hecho publicidad, configure una entrada de red en la lengüeta de la **configuración > de las redes** que cubre la red a la cual se asocia la interfaz, y entonces configurar esa interfaz como interfaz pasiva de modo que la interfaz no pueda enviar o recibir las Actualizaciones de EIGRP.

Nota: Las interfaces configuradas como voz pasiva no envían ni reciben las Actualizaciones de EIGRP.

7. Usted puede definir opcionalmente 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 de EIGRP.

8. Usted puede configurar opcionalmente la redistribución de ruta. Cisco ASA puede redistribuir las rutas descubiertas por el Routing Information Protocol (RIP) y el Open Shortest Path First (OSPF) en el proceso de EIGRP Routing. Usted puede también redistribuir los parásitos atmosféricos y los Routeconectad en el proceso de EIGRP Routing. Usted no necesita redistribuir los parásitos atmosféricos o los Routeconectad si caen dentro del rango de una red configurada en la **configuración > las redes** cuadro definen la redistribución de ruta en el cristal de la redistribución.

9. Los paquetes de saludo EIGRP se envían como paquetes de multidifusión. Si un vecino EIGRP está situado a través de una red sin broadcast, usted debe definir manualmente a ese vecino. Cuando usted define manualmente a un vecino EIGRP, los paquetes de saludo se envían a ese vecino como mensajes del unicast. Para definir a los vecinos EIGRP estáticos, vaya al cristal del **vecino estático**.

10. Por abandono, se envían y se validan las rutas predeterminado. Para restringir o inhabilitar el envío y la recepción de la información de Route predeterminado, abra la **configuración > la configuración de dispositivo > la encaminamiento > el EIGRP > el cristal de la información del valor por defecto**. El cristal predeterminado de la información visualiza una tabla de reglas para controlar el envío y la recepción de la información de Route

predeterminado en las Actualizaciones de EIGRP.

Nota: Usted puede hacer que uno “en” y uno “hacia fuera” gobierne para cada proceso de EIGRP Routing. (Solamente un proceso se soporta actualmente.)

## Autenticación del EIGRP de la configuración

Cisco ASA soporta autenticación de MD5 de las actualizaciones de ruteo del EIGRP Routing Protocol. La publicación MD5-keyed en cada paquetes EIGRP previene la introducción de mensajes de ruteo desautorizados o falsos de las fuentes no aprobadas. La adición de autenticación a sus mensajes del EIGRP 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 encendido a la red, las tablas de ruteo en su Routers o Cisco ASA pueden llegar a ser corruptas y un establecimiento de rechazo del servicio puede seguir. Cuando usted agrega la autenticación a los mensajes del EIGRP enviados entre sus dispositivos de ruteo (que incluye el ASA), previene las adiciones desautorizadas de routers EIGRP en su topología de ruteo.

La autenticación de la ruta EIGRP se configura sobre una base del por interface. Todos los vecinos EIGRP en las interfaces configuradas para la autenticación del mensaje del EIGRP deben ser configurados con el mismo modo de autenticación y clave para que las adyacencias sean establecidas.

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

1. En el ASDM, navegue a la **configuración > a la configuración > a la encaminamiento > al EIGRP > a la interfaz de dispositivo** como se muestra.
2. En este caso, el EIGRP se habilita en la interfaz interior (gigabitethernet 0/1). Elija el **gigabitethernet 0/1** interfaz y el tecleo **edita**.
3. Bajo autenticación, elija el **permiso autenticación de MD5**. Agregue más información sobre los parámetros de autenticación aquí. En este caso, la clave del preshared es **cisco123**, y la clave ID es 1.

## Filtración de la ruta EIGRP

Con el EIGRP, usted puede controlar las actualizaciones de ruteo se envían y se reciben que. En este ejemplo, usted 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 Routes, usted puede utilizar solamente el **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 CLI de Cisco ASA

Ésta es la configuración CLI de Cisco ASA.

```
!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 del Cisco IOS (r1)

Ésta es la configuración CLI del r1 (router interno).

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

```
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, usted puede navegar a **monitorear > encaminamiento > vecino EIGRP** para ver a cada uno de los vecinos EIGRP. Este tiro de pantalla muestra al router interno (r1) como vecino activo. Usted puede también ver la interfaz de donde reside este vecino, el holdtime, y encima de cuánto tiempo la relación de vecino ha estado (UpTime).
2. Además, usted puede verificar la tabla de ruteo si usted navega a **monitorear > encaminamiento > las rutas**. En este tiro de pantalla, usted puede ver que las **192.168.10.0/24, 172.18.124.0/24, y 10.20.20.0/24** redes son doctas con el r1 (10.10.10.2).

Del CLI, usted puede utilizar el **comando show route** para conseguir la misma salida.

```
ciscoasa# show route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is 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 la Versión de ASA 9.2.1 y posterior, usted puede utilizar el comando **eigrp** de la ruta de la demostración para visualizar 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. Usted puede también utilizar el comando de la **topología EIGRP** de la demostración para obtener la información sobre las redes doctas 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 **neighbors del eigrp** de la demostración 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 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 sube en el link y envía un paquete de saludo del mcast con todas sus interfaces Eigrp-configuradas.
2. El r1 recibe un paquete de saludo y envía un paquete de saludo del mcast.
3. El ASA recibe el paquete de saludo y envía un paquete de actualización con un conjunto de bits inicial, que indica que éste es el proceso de inicialización.
4. El r1 recibe un paquete de actualización y envía un paquete de actualización con un conjunto de bits inicial, que indica que éste es el proceso de inicialización.
5. Después del ASA y del r1 han intercambiado el hellos y se establece la adyacencia de vecino, el ASA y contestación del r1 con un paquete ACK, que indica que la información de actualización fue recibida.
6. El ASA envía su información de ruteo al r1 en un paquete de actualización.
7. El r1 inserta la información del paquete de actualización en su tabla de topología. La tabla de topología incluye todos los destinos des divulgación por los vecinos. Se ordena de modo que cada destino sea mencionado, junto con todos los vecinos que puedan viajar al destino y a su métrica asociada.
8. El r1 entonces envía un paquete de actualización al ASA.
9. Una vez que recibe el paquete de actualización, el ASA envía un paquete ACK al r1. Después de que el ASA y el r1 reciban con éxito los paquetes de actualización de uno a, están listos eligieron las rutas del sucesor (mejor) y del sucesor factible (respaldo) de la tabla de topología, y ofrecen las rutas del sucesor a la tabla de ruteo.

## Troubleshooting

Esta sección incluye la información sobre los **comandos debug and show** que pueden ser útiles para resolver problemas los problemas del EIGRP.

### Comandos para resolución de problemas

[La herramienta Output Interpreter Tool \(clientes registrados solamente\)](#) (OIT) soporta ciertos comandos show. Utilice 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 visualizar la información del debug la máquina de estados finitos (DUAL) del algoritmo difusor de actualización, utiliza el **comando debug eigrp fsm** en el modo EXEC privilegiado. Este comando le deja observar la actividad del sucesor factible del EIGRP y determinarla si las actualizaciones de la ruta son instaladas y borradas por el proceso de ruteo.

Ésta es la salida del **comando debug** dentro del peering acertado con el r1. Usted puede ver cada uno de las diversas rutas que esté instalada con éxito 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
```

Usted puede también utilizar el **comando neighbor del eigrp del debug**. Ésta es la salida de este **comando debug** cuando Cisco ASA creó con éxito una nueva relación vecina con el 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 ()
```

Usted puede también utilizar los paquetes EIGRP del debug para la información detallada del intercambio del mensaje del EIGRP entre Cisco ASA y sus pares. En este ejemplo, la clave de

autenticación fue cambiada en el router (r1), y la salida de los debugs le muestra que el problema es una discordancia de la 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)
```

## La vecindad EIGRP va abajo con los Syslog ASA-5-336010

El ASA cae la vecindad EIGRP cuando cualquier cambio en la lista de distribución del EIGRP se realiza. Se considera 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, siempre que una nueva entrada acl se agregue en el ACL, se reajusta la vecindad EIGRP de la Eigrp-red-lista.

```
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
```

Usted puede observar que la relación de vecino está para arriba 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 usted puede agregar el estándar de la Eigrp-red-lista de la lista de acceso niega **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 172.18.24.0.0 255.255.255.0'
%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 el **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

Ésta es conducta esperada en todas las nuevas Versiones de ASA a partir del 8.4 y 8.6 a 9.1. Lo mismo se ha observado en el Routers que funciona con los 12.4 a 15.1 trenes del código. Sin embargo, este comportamiento no se observa en la Versión de ASA 8.2 y versiones de software anteriores ASA porque los cambios realizados a un ACL no reajustan las adyacencias del EIGRP.

Puesto que el EIGRP envía la tabla de topología llena a un vecino cuando sube el vecino primero, y entonces él envía solamente los cambios, configurar una lista de la distribución con la naturaleza evento-conducida del EIGRP haría difícil para que los cambios se apliquen sin una restauración completa de la relación de vecino. El Routers necesitaría no perder de vista cada ruta enviada a y recibida de un vecino para saber qué ruta ha cambiado (es decir, o no sería enviado/fue validado) para aplicar los cambios como dictado por la corriente distribuya la lista. Es mucho más fácil derribar y restablecer simplemente la adyacencia entre los vecinos.

Cuando se derriba y se restablece una adyacencia, todas las rutas aprendido entre los vecinos particulares se olvidan simplemente y la sincronización entera entre los vecinos se realiza de nuevo - con el nuevo distribuya la lista en el lugar.

La mayor parte de las técnicas del EIGRP que usted utiliza para resolver problemas al Routers del Cisco IOS se pueden aplicar en Cisco ASA. Para resolver problemas el EIGRP, utilice el [diagrama de flujo de Troubleshooting principal](#); comience en la **tubería** marcada cuadro.