Ejemplo de configuración de la autenticación del mensaje del EIGRP

Contenido

Introducción

Este documento explica cómo agregar autenticación de mensajes a sus routers EIGRP (Enhanced Interior Gateway Routing Protocol) y proteger la tabla de ruteo contra una corrupción voluntaria o accidental.

La adición de autenticación a los mensajes del EIGRP de su Routers se asegura de que su Routers valide solamente los mensajes de ruteo del otro Routers que conoce la misma clave previamente compartida. Sin esta autenticación configurada, si alguien presenta a otro router con información de ruta diversa o en conflicto encendido a la red, las tablas de ruteo en su Routers podrían llegar a ser corruptas y un establecimiento de rechazo del servicio podría seguir. Así, cuando usted agrega la autenticación a los mensajes del EIGRP enviados entre su Routers, previene alguien de adrede o accidentalmente agregando a otro router a la red y causando un problema.

Precaución: Cuando la autenticación del mensaje del EIGRP se agrega a la interfaz de un router, las paradas de ese router que reciben los mensajes de ruteo de sus pares hasta que también lo configuren para la autenticación del mensaje. Esto interrumpe las comunicaciones de la encaminamiento sobre su red. Vea los mensajes cuando solamente Dallas se configura para más

información.

prerrequisitos

Requisitos

- El tiempo se debe configurar correctamente en todo el Routers. Refiera a configurar el NTP para más información.
- Se recomienda una configuración EIGRP de trabajo.

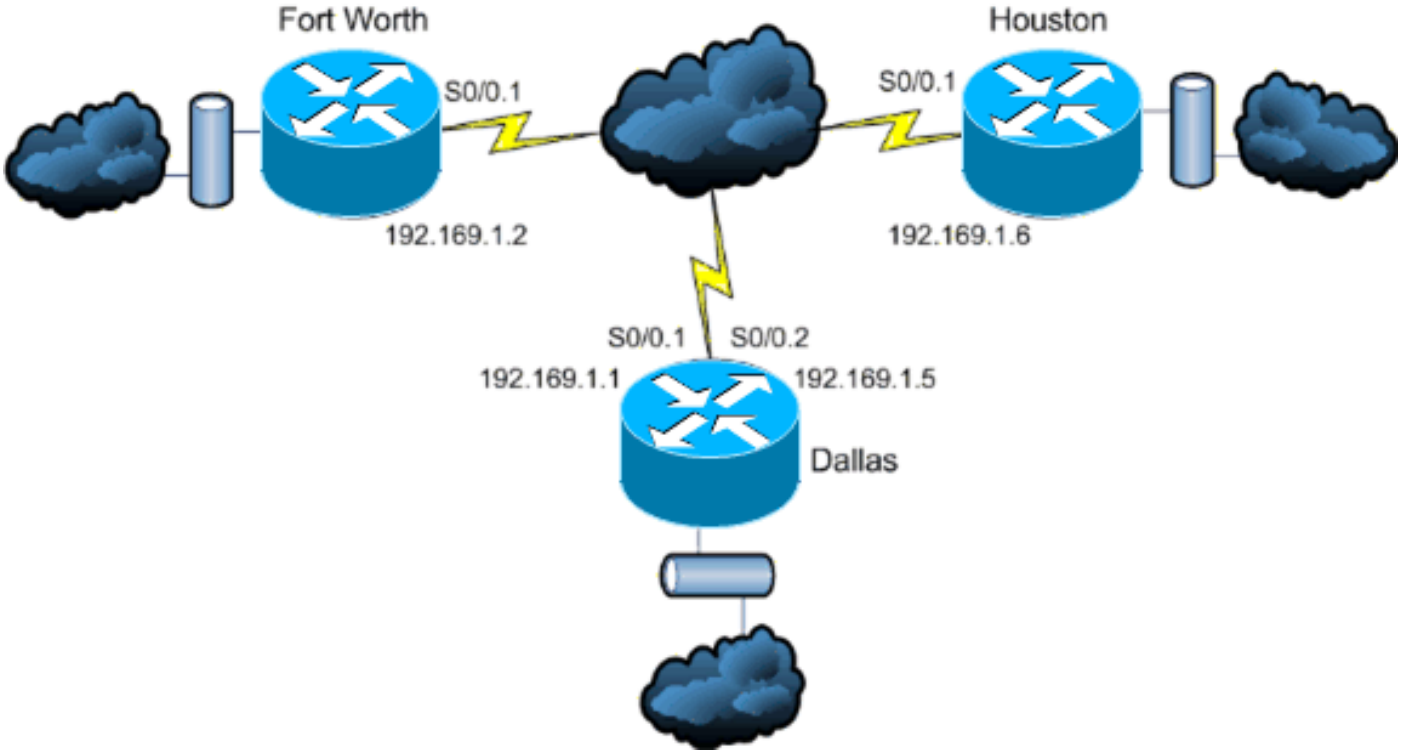
Componentes Utilizados

La información en este documento se basa en el Software Release 11.2 y Posterior de Cisco IOS®.

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.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Convenciones

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

Antecedentes

En este escenario un administrador de la red quiere configurar la autenticación para los mensajes del EIGRP entre el router de eje de conexión en Dallas y los sitios remotos en Fort Worth y Houston. La configuración EIGRP (sin la autenticación) es ya completa en el tres Routers. Esta salida de ejemplo es de Dallas:

```
Dallas#show ip eigrp neighbors IP-EIGRP neighbors for process 10 H Address Interface Hold Uptime
SRTT RTO Q Seq Type (sec) (ms) Cnt Num 1 192.169.1.6 Se0/0.2 11 15:59:57 44 264 0 2 0
192.169.1.2 Se0/0.1 12 16:00:40 38 228 0 3 Dallas#show cdp neigh Capability Codes: R - Router, T
- Trans Bridge, B - Source Route Bridge S - Switch, H - Host, I - IGMP, r - Repeater Device ID
Local Intrfce Holdtme Capability Platform Port ID Houston Ser 0/0.2 146 R 2611 Ser 0/0.1
FortWorth Ser 0/0.1 160 R 2612 Ser 0/0.1
```

Autenticación del mensaje del EIGRP de la configuración

La configuración de la autenticación del mensaje del EIGRP consiste en dos pasos:

1. La creación de un llavero y de una clave.
2. La configuración de la autenticación del EIGRP para utilizar ese llavero y clave.

Esta sección ilustra los pasos para configurar la autenticación del mensaje del EIGRP en el router de Dallas y entonces el Routers de Fort Worth y de Houston.

Cree un llavero en Dallas

La autenticación de ruteo confía en una clave en un llavero para funcionar. Antes de que la autenticación pueda ser habilitada, un llavero y por lo menos una clave debe ser creado.

1. Ingrese al modo de configuración global.`Dallas#`**`configure terminal`**
2. Cree el llavero. **MYCHAIN** se utiliza en este ejemplo.`Dallas(config)#`**`key chain MYCHAIN`**
3. Especifique el número dominante. **1** se utiliza en este ejemplo.**Nota:** Se recomienda que el número dominante sea lo mismo en todo el Routers implicado en la configuración.`Dallas(config-keychain)#`**`key 1`**
4. Especifique la clave-cadena para la clave. **securetraffic** se utiliza en este ejemplo.`Dallas(config-keychain-key)#`**`key-string securetraffic`**
5. Termine la configuración.`Dallas(config-keychain-key)#`**`end`** `Dallas#`

Configure la autenticación en Dallas

Una vez que usted crea un llavero y una clave, usted debe configurar el EIGRP para realizar la autenticación del mensaje con la clave. Esta configuración se completa en las interfaces que el EIGRP está configurado encendido.

Precaución: Cuando la autenticación del mensaje del EIGRP se agrega a las interfaces de Dallas, para el recibir de los mensajes de ruteo de sus pares hasta que también se configuren para la autenticación del mensaje. Esto interrumpe las comunicaciones de la encaminamiento sobre su red. Vea los mensajes cuando solamente Dallas se configura para más información.

1. Ingrese al modo de configuración global.`Dallas#`**`configure terminal`**
2. Del modo de configuración global, especifique la interfaz que usted quiere configurar la

autenticación del mensaje del EIGRP encendido. En este ejemplo la primera interfaz es el **serial 0/0.1**.`Dallas(config)#`**`interface serial 0/0.1`**

3. Autenticación del mensaje del EIGRP del permiso. **Los 10** usados aquí es el número del sistema autónomo de la red. **el md5** indica que el hash del md5 debe ser utilizado para la autenticación.`Dallas(config-subif)#`**`ip authentication mode eigrp 10 md5`**
4. Especifique el llavero que se debe utilizar para la autenticación. **10** es el número del sistema autónomo. **MYCHAIN** es el llavero que fue creado en el crear una sección del llavero.`Dallas(config-subif)#`**`ip authentication key-chain eigrp 10 MYCHAIN`** `Dallas(config-subif)#`**`end`**
5. Complete la misma configuración en el serial 0/0.2 de la interfaz.`Dallas#`**`configure terminal`** `Dallas(config)#`**`interface serial 0/0.2`** `Dallas(config-subif)#`**`ip authentication mode eigrp 10 md5`** `Dallas(config-subif)#`**`ip authentication key-chain eigrp 10 MYCHAIN`** `Dallas(config-subif)#`**`end`** `Dallas#`

Configure Fort Worth

Esta sección muestra los comandos necesarios configurar la autenticación del mensaje del EIGRP en el router de Fort Worth. Para más explicación detallada de los comandos mostrados aquí, vea para crear un llavero en Dallas y para configurar la autenticación en Dallas.

```
FortWorth#configure terminal FortWorth(config)#key chain MYCHAIN FortWorth(config-keychain)#key
1 FortWort(config-keychain-key)#key-string securetraffic FortWort(config-keychain-key)#end
FortWorth# Fort Worth#configure terminal FortWorth(config)#interface serial 0/0.1
FortWorth(config-subif)#ip authentication mode eigrp 10 md5 FortWorth(config-subif)#ip
authentication key-chain eigrp 10 MYCHAIN FortWorth(config-subif)#end FortWorth#
```

Configure Houston

Esta sección muestra los comandos necesarios configurar la autenticación del mensaje del EIGRP en el router de Houston. Para más explicación detallada de los comandos mostrados aquí, vea para crear un llavero en Dallas y para configurar la autenticación en Dallas.

```
Houston#configure terminal Houston(config)#key chain MYCHAIN Houston(config-keychain)#key 1
Houston(config-keychain-key)#key-string securetraffic Houston(config-keychain-key)#end Houston#
Houston#configure terminal Houston(config)#interface serial 0/0.1 Houston(config-subif)#ip
authentication mode eigrp 10 md5 Houston(config-subif)#ip authentication key-chain eigrp 10
MYCHAIN Houston(config-subif)#end Houston#
```

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

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

Mensajes cuando solamente se configura Dallas

Una vez que la autenticación del mensaje del EIGRP se configura en el router de Dallas, ese router comienza a rechazar los mensajes del Routers de Fort Worth y de Houston porque todavía no hacen la autenticación configurar. Esto puede ser verificada publicando un **comando debug eigrp packets** en el router de Dallas:

```
Dallas#debug eigrp packets 17:43:43: EIGRP: ignored packet from 192.169.1.2 (invalid
authentication) 17:43:45: EIGRP: ignored packet from 192.169.1.6 (invalid authentication) !---
```

```
Packets from Fort Worth and Houston are ignored because they are !--- not yet configured for
authentication.
```

Mensajes cuando configuran a todo el Routers

Una vez que la autenticación del mensaje del EIGRP se configura en el tres Routers, él comienza a intercambiar los mensajes del EIGRP otra vez. Esto puede ser verificada publicando un **comando debug eigrp packets** de nuevo. Las salidas de esta vez del Routers de Fort Worth y de Houston se muestran:

```
FortWorth#debug eigrp packets 00:47:04: EIGRP: received packet with MD5 authentication, key id =
1 00:47:04: EIGRP: Received HELLO on Serial0/0.1 nbr 192.169.1.1 !--- Packets from Dallas with
MD5 authentication are received. Houston#debug eigrp packets 00:12:50.751: EIGRP: received
packet with MD5 authentication, key id = 1 00:12:50.751: EIGRP: Received HELLO on Serial0/0.1
nbr 192.169.1.5 !--- Packets from Dallas with MD5 authentication are received.
```

Troubleshooting

link unidireccional

Usted debe configurar el EIGRP los temporizadores hola y del tiempo en espera en los ambos extremos. Si usted configura los temporizadores solamente en un extremo, un link unidireccional ocurre.

Un router en un link unidireccional pudo poder recibir los paquetes de saludo. Sin embargo, los paquetes de saludo enviados no se reciben en el otro extremo. Este link unidireccional es indicado generalmente por los mensajes *excedidos límite de la recomprobación* en un extremo.

Para ver el *límite de la recomprobación excedió los* mensajes, utiliza los **paquetes EIGRP del debug** y **hace el debug de los** comandos de las **notificaciones del eigrp del IP**.

Información Relacionada

- Soporte de tecnología del Enhanced Interior Gateway Routing Protocol (EIGRP)
- Soporte Técnico y Documentación - Cisco Systems