Ejemplo de Configuración de Autenticación de Mensajes 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 EIGRP de sus routers garantiza que éstos sólo acepten mensajes de ruteo de otros routers que conozcan la misma clave previamente compartida. Sin esta autenticación configurada, si alguien introduce otro router con información de ruta diferente o conflictiva en la red, las tablas de ruteo en sus routers podrían dañarse y podría producirse un ataque de denegación de servicio. Por lo tanto, cuando agrega autenticación a los mensajes EIGRP enviados entre sus routers, evita que alguien agregue deliberada o accidentalmente otro router a la red y cause un problema.

Precaución: Cuando se agrega la autenticación de mensajes EIGRP a la interfaz de un router, ese router deja de recibir mensajes de ruteo de sus pares hasta que también se configuran para la autenticación de mensajes. Esto sí interrumpe las comunicaciones de ruteo en su red. Para obtener más información, consulte Mensajes cuando solo Dallas está configurado.

Prerequisites

Requirements

- La hora debe configurarse correctamente en todos los routers. Consulte Configuración de NTP para obtener más información.
- Se recomienda una configuración EIGRP en funcionamiento.

Componentes Utilizados

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

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). If your network is live, make sure that you understand the potential impact of any command.

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 esta situación, un administrador de red desea configurar la autenticación para los mensajes EIGRP entre el router hub en Dallas y los sitios remotos en Fort Worth y Houston. La configuración EIGRP (sin autenticación) ya está completa en los tres routers. Este ejemplo de resultado es de Dallas:

<#root>

```
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
```

Configurar autenticación de mensaje EIGRP

La configuración de la autenticación de mensajes EIGRP consta de dos pasos:

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

Esta sección ilustra los pasos para configurar la autenticación de mensajes EIGRP en el router de Dallas y luego en los routers de Fort Worth y Houston.

Crear un llavero en Dallas

La autenticación de ruteo se basa en una llave en un llavero para funcionar. Antes de que se pueda habilitar la autenticación, se debe crear una cadena de claves y al menos una clave.

1. Ingrese al modo de configuración global.

   <#root>

   ```
   Dallas#
   configure terminal
   ```

2. Cree el key chain. MYCHAIN se utiliza en este ejemplo.

   <#root>

   ```
   Dallas(config)#
   key chain MYCHAIN
   ```

3. Especifique el número de clave. 1 se utiliza en este ejemplo.

   Nota: Se recomienda que el número de clave sea el mismo en todos los routers involucrados en la configuración.

   <#root>

   ```
   Dallas(config-keychain)#
   ```

```
key 1
```

4. Especifique la cadena de clave para la clave. securetraffic se utiliza en este ejemplo.

```
<#root>
Dallas(config-keychain-key)#
key-string securetraffic
```

5. Finalice la configuración.

```
<#root>
Dallas(config-keychain-key)#
end
Dallas#
```

Configurar autenticación en Dallas

Una vez que haya creado una cadena de claves y una clave, debe configurar EIGRP para realizar la autenticación de mensajes con la clave. Esta configuración se completa en las interfaces en las que se configura EIGRP.

Precaución: Cuando se agrega la autenticación de mensajes EIGRP a las interfaces de Dallas, deja de recibir mensajes de ruteo de sus pares hasta que también se configuran para la autenticación de mensajes. Esto sí interrumpe las comunicaciones de ruteo en su red. Para obtener más información, consulte Mensajes cuando solo Dallas está configurado.

1. Ingrese al modo de configuración global.

```
<#root>
Dallas#
configure terminal
```

2. En el modo de configuración global, especifique la interfaz en la que desea configurar la autenticación de mensajes EIGRP. En este ejemplo, la primera interfaz es Serial 0/0.1.

```
<#root>
```

```
Dallas(config)#
interface serial 0/0.1
```

3. Habilitar autenticación de mensajes EIGRP. El 10 que se utiliza aquí es el número del sistema autónomo de la red. md5 indica que el hash md5 se va a utilizar para la autenticación.

```
<#root>
Dallas(config-subif)#
ip authentication mode eigrp 10 md5
```

4. Especifique la cadena de claves que se debe utilizar para la autenticación. 10 es el número del sistema autónomo. MYCHAIN es el llavero que se creó en la sección Create a Keychain (Crear un llavero).

```
<#root>
Dallas(config-subif)#
ip authentication key-chain eigrp 10 MYCHAIN
Dallas(config-subif)#
end
```

5. Complete la misma configuración en la interfaz Serial 0/0.2.

```
<#root>
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#
```

Configurar Fort Worth

Esta sección muestra los comandos necesarios para configurar la autenticación de mensajes EIGRP en el router de Fort Worth. Para obtener una explicación más detallada de los comandos que se muestran aquí, vea Create a Keychain on Dallas y Configure Authentication on Dallas.

<#root>

```
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#
```

Configurar Houston

Esta sección muestra los comandos necesarios para configurar la autenticación de mensajes EIGRP en el router de Houston. Para obtener una explicación más detallada de los comandos que se muestran aquí, vea Create a Keychain on Dallas y Configure Authentication on Dallas.

<#root>

```
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 Debug antes de utilizar los comandos debug.

Mensajes cuando solamente Dallas está configurado

Una vez que se configura la autenticación de mensajes EIGRP en el router de Dallas, ese router comienza a rechazar los mensajes de los routers de Fort Worth y Houston porque aún no tienen la autenticación configurada. Esto se puede verificar mediante la ejecución del comando debug eigrp packets en el router de Dallas:

<#root>

```
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 authe
```

Mensajes cuando se configuran todos los routers

Una vez configurada la autenticación de mensajes EIGRP en los tres routers, comienzan a intercambiar mensajes EIGRP nuevamente. Esto se puede verificar ejecutando una vez más el comando debug eigrp packets. Esta vez se muestran las salidas de los routers de Fort Worth y Houston:

<#root>

```
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.
```

<#root>

```
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.
```

Troubleshoot

link unidireccional

Debe configurar los temporizadores EIGRP Hello y Hold-time en ambos extremos. Si configura los temporizadores solamente en un extremo, se produce un link unidireccional.

Un router en un link unidireccional podría ser capaz de recibir paquetes de saludo. Sin embargo, los paquetes de saludo enviados no se reciben en el otro extremo. Este link unidireccional suele estar indicado por los mensajes de límite de reintentos excedidos en un extremo.

Para ver los mensajes de límite de reintento excedido, utilice los comandos debug eigrp packet y debug ip eigrp notifications.

Información Relacionada

- Compatibilidad mejorada con la tecnología de protocolo de routing de gateway interior (EIGRP)
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).