Exemplo de configuração da autenticação de mensagem EIGRP

Índice

Introdução

Este documento ilustra como adicionar uma autenticação de mensagem a seus roteadores com Enhanced Interior Gateway Routing Protocol (EIGRP) e proteger a tabela de roteamento de corrompimento intencional ou acidental.

A adição de autenticação às mensagens EIGRP do seu Roteadores assegura-se de que seu Roteadores aceite somente mensagens de roteamento do outro Roteadores que conhece a mesma chave pré-compartilhada. Sem esta autenticação configurada, se alguém introduz um outro roteador com informação de rota diferente ou opondo sobre à rede, as tabelas de roteamento em seu Roteadores poderiam tornar-se corrompidas e um ataque de recusa de serviço poderia seguir. Assim, quando você adiciona a autenticação às mensagens EIGRP enviadas entre seu Roteadores, impede alguém de propositadamente ou acidentalmente adicionando um outro roteador à rede e causando um problema.

Caution: Quando a autenticação de mensagem EIGRP for adicionada à relação de um roteador, as paradas desse roteador que recebem mensagens de roteamento de seus pares até que estiverem configurados igualmente para a autenticação de mensagem. Isto interrompe comunicações do roteamento em sua rede. Veja mensagens quando somente Dallas é

configurada para mais informação.

Pré-requisitos

Requisitos

- O tempo deve corretamente ser configurado em todo o Roteadores. Refira configurar o NTP para mais informação.
- Uma configuração de EIGRP de trabalho é recomendada.

Componentes Utilizados

A informação neste documento é baseada no Software Release 11.2 e Mais Recente de Cisco IOS®.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

Nesta encenação um administrador de rede quer configurar a autenticação para mensagens EIGRP entre o roteador de hub em Dallas e os locais remotos em Fort Worth e em Houston. A configuração de EIGRP (sem autenticação) está já completa em todos os três Roteadores. Estas saídas de exemplo são 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
```

Configurar a autenticação de mensagem EIGRP

A configuração da autenticação de mensagem EIGRP consiste em duas etapas:

1. A criação de um keychain e de uma chave.
2. A configuração da autenticação EIGRP para usar esses keychain e chave.

Esta seção ilustra as etapas para configurar a autenticação de mensagem EIGRP no roteador de Dallas e então no Roteadores de Fort Worth e de Houston.

Crie um Keychain em Dallas

A autentificação de roteamento confia em uma chave em um keychain para funcionar. Antes que a autenticação possa ser permitida, um keychain e pelo menos uma chave devem ser criados.

1. Insira o modo de configuração global.
   ```
   Dallas#configure terminal
   ```

2. Crie a porta-chaves. **MYCHAIN** é usado neste exemplo.
   ```
   Dallas(config)#key chain MYCHAIN
   ```

3. Especifique o número chave. **1** é usado neste exemplo.**Note**: Recomenda-se que o número chave seja o mesmo em todo o Roteadores envolvido na configuração.
   ```
   Dallas(config-keychain)#key 1
   ```

4. Especifique a chave-corda para a chave. **securetraffic** é usado neste exemplo.
   ```
   Dallas(config-keychain-key)#key-string securetraffic
   ```

5. Termine a configuração.
   ```
   Dallas(config-keychain-key)#end
   Dallas#
   ```

Configurar a autenticação em Dallas

Uma vez que você cria um keychain e uma chave, você deve configurar o EIGRP para executar a autenticação de mensagem com a chave. Esta configuração é terminada nas relações que o EIGRP está configurado sobre.

Caution: Quando a autenticação de mensagem EIGRP é adicionada às relações de Dallas, para de receber mensagens de roteamento de seus pares até que estejam configurados igualmente para a autenticação de mensagem. Isto interrompe comunicações do roteamento em sua rede. Veja mensagens quando somente Dallas é configurada para mais informação.

1. Insira o modo de configuração global.
   ```
   Dallas#configure terminal
   ```

2. Do modo de configuração global, especifique a relação que você quer configurar sobre a autenticação de mensagem EIGRP. Neste exemplo a primeira relação é a **série 0/0.1**.
   ```
   Dallas(config)#interface serial 0/0.1
   ```

3. Permita a autenticação de mensagem EIGRP. **O 10** usado aqui é o número de sistema

autônomo da rede. **md5** indica que a mistura md5 deve ser usada para a autenticação.

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

4. Especifique o keychain que deve ser usado para a autenticação. **o 10** é o número de sistema autônomo. **MYCHAIN** é o keychain que foi criado na criação uma seção de Keychain.

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

5. Termine a mesma configuração na série 0/0.2 da relação.

```
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 seção mostra os comandos necessários configurar a autenticação de mensagem EIGRP no roteador de Fort Worth. Para mais explicação detalhada dos comandos mostrados aqui, veja para criar um Keychain em Dallas e para configurar a autenticação em 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#
```

Configurar Houston

Esta seção mostra os comandos necessários configurar a autenticação de mensagem EIGRP no roteador de Houston. Para mais explicação detalhada dos comandos mostrados aqui, veja para criar um Keychain em Dallas e para configurar a autenticação em 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#
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Note: Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug**.

Mensagens quando somente Dallas for configurada

Uma vez que a autenticação de mensagem EIGRP é configurada no roteador de Dallas, esse roteador começa a rejeitar mensagens do Roteadores de Fort Worth e de Houston porque não têm ainda a autenticação configurada. Isto pode ser verificado emitindo um **comando debug eigrp packets no** roteador 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.
```

Mensagens quando todo o Roteadores for configurado

Uma vez que a autenticação de mensagem EIGRP é configurada em todos os três Roteadores, começam a trocar outra vez mensagens EIGRP. Isto pode ser verificado emitindo um **comando debug eigrp packets** mais uma vez. As saídas desta vez do Roteadores de Fort Worth e de Houston são mostradas:

```
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 unidirecional

Você deve configurar temporizadores dos hello de EIGRP e do hold-time no ambas as extremidades. Se você configura os temporizadores somente em uma extremidade, um enlace unidirecional ocorre.

Um roteador em um enlace unidirecional pôde poder receber pacotes Hello. Contudo, os pacotes Hello mandados não são recebidos no extremo oposto. Este enlace unidirecional é indicado geralmente por mensagens *excedidas limite da nova tentativa em* uma extremidade.

A fim ver o *limite da nova tentativa excedeu* mensagens, usa o **pacote EIGRP debugar** e **debuga** comandos das **notificações do eigrp IP**.

Informações Relacionadas

- Suporte por tecnologia do Enhanced Interior Gateway Routing Protocol (EIGRP)
- Suporte Técnico e Documentação - Cisco Systems