Exemplo de Configuração de Autenticação de Mensagem do EIGRP

Contents

Introduction

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 do EIGRP dos seus roteadores garante que os roteadores aceitem apenas mensagens de roteamento de outros roteadores que saibam a mesma chave pré-compartilhada. Sem essa autenticação configurada, se alguém introduzir outro roteador com informações de rota diferentes ou conflitantes na rede, as tabelas de roteamento em seus roteadores poderão ficar corrompidas e um ataque de negação de serviço poderá ocorrer. Assim, quando você adiciona autenticação às mensagens do EIGRP enviadas entre seus roteadores, isso impede que alguém adicione outro roteador à rede proposital ou acidentalmente, causando um problema.

Cuidado: quando a autenticação de mensagem do EIGRP é adicionada à interface de um roteador, esse roteador pára de receber mensagens de roteamento de seus pares até que elas também sejam configuradas para autenticação de mensagem. Isso interrompe as comunicações de roteamento na rede. Consulte Mensagens quando apenas Dallas está configurado para obter

mais informações.

Prerequisites

Requirements

- A hora deve ser configurada corretamente em todos os roteadores. Consulte Configurando o NTP para obter mais informações.
- Uma configuração do EIGRP em funcionamento é recomendada.

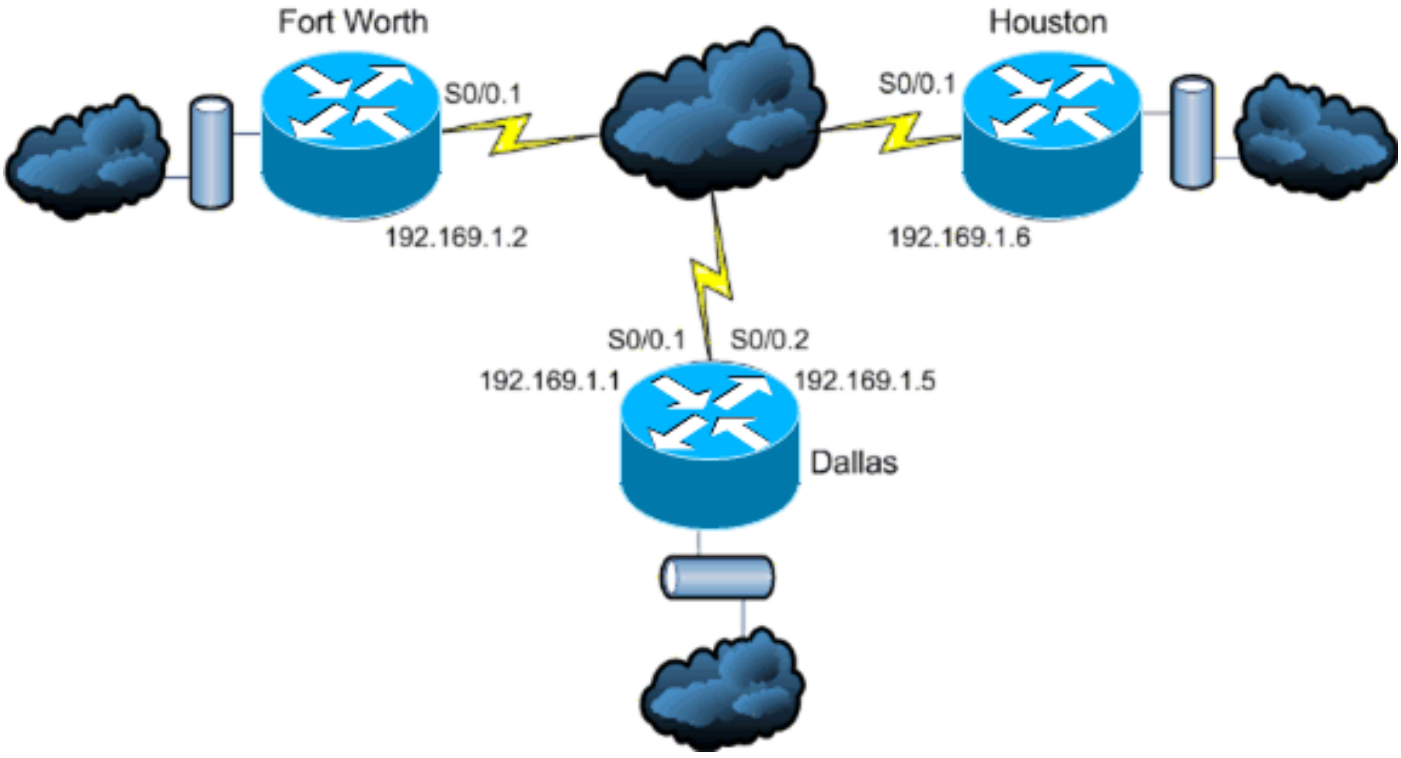
Componentes Utilizados

As informações neste documento são baseadas no software Cisco IOS® versão 11.2 e posterior.

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.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Conventions

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

Informações de Apoio

Neste cenário, um administrador de rede deseja configurar a autenticação para mensagens EIGRP entre o roteador de hub em Dallas e os locais remotos em Fort Worth e Houston. A configuração do EIGRP (sem autenticação) já está concluída nos três roteadores. Este exemplo de saída é 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 do EIGRP

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

1. A criação de um conjunto de chaves e chaves.
2. A configuração da autenticação do EIGRP para usar esse conjunto de chaves e essa chave.

Esta seção ilustra as etapas para configurar a autenticação de mensagens do EIGRP no roteador Dallas e, em seguida, nos roteadores Fort Worth e Houston.

Criar um conjunto de chaves em Dallas

A autenticação de roteamento depende de uma chave em um conjunto de chaves para funcionar. Para que a autenticação possa ser ativada, é necessário criar um conjunto de chaves e pelo menos uma chave.

1. Insira o modo de configuração global.
   ```
   Dallas#configure terminal
   ```
2. Crie a cadeia de chaves. **MYCHAIN** é usado neste exemplo.
   ```
   Dallas(config)#key chain MYCHAIN
   ```
3. Especifique o número da chave. **1** é usado neste exemplo.**Observação:** recomenda-se que o número da chave seja o mesmo em todos os roteadores envolvidos na configuração.
   ```
   Dallas(config-keychain)#key 1
   ```
4. Especifique a sequência de chaves 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

Depois de criar um conjunto de chaves e uma chave, você deve configurar o EIGRP para executar a autenticação de mensagens com a chave. Essa configuração é concluída nas interfaces nas quais o EIGRP está configurado.

Cuidado: quando a autenticação de mensagem do EIGRP é adicionada às interfaces Dallas, ele pára de receber mensagens de roteamento de seus pares até que elas também sejam configuradas para autenticação de mensagem. Isso interrompe as comunicações de roteamento na rede. Consulte Mensagens quando apenas Dallas está configurado para obter mais informações.

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

2. No modo de configuração global, especifique a interface na qual deseja configurar a autenticação de mensagem do EIGRP. Neste exemplo, a primeira interface é **Serial 0/0.1**.
   ```
   Dallas(config)#interface serial 0/0.1
   ```

3. Ative a autenticação de mensagem do EIGRP. O **10** usado aqui é o número do sistema autônomo da rede. **md5** indica que o hash md5 deve ser usado para autenticação.
   ```
   Dallas(config-subif)#ip authentication mode eigrp 10 md5
   ```

4. Especifique o conjunto de chaves que deve ser usado para autenticação. **10** é o número do sistema autônomo. **MYCHAIN** é o conjunto de chaves que foi criado na seção Criar um conjunto de chaves.
   ```
   Dallas(config-subif)#ip authentication key-chain eigrp 10 MYCHAIN
   Dallas(config-subif)#end
   ```

5. Conclua a mesma configuração na interface Serial 0/0.2.
   ```
   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 Forte

Esta seção mostra os comandos necessários para configurar a autenticação de mensagem do EIGRP no roteador Fort Worth. Para obter uma explicação mais detalhada dos comandos mostrados aqui, consulte Criar um conjunto de chaves em Dallas e 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 para configurar a autenticação de mensagem do EIGRP no roteador Houston. Para obter uma explicação mais detalhada dos comandos mostrados aqui, consulte Criar um conjunto de chaves em Dallas e 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.

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

Mensagens quando apenas Dallas está configurado

Quando a autenticação de mensagem do EIGRP é configurada no roteador Dallas, o roteador começa a rejeitar mensagens dos roteadores Fort Worth e Houston porque ainda não têm a autenticação configurada. Isso pode ser verificado emitindo um comando **debug eigrp packets** no roteador 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 todos os roteadores são configurados

Quando a autenticação de mensagem do EIGRP é configurada nos três roteadores, eles começam a trocar mensagens do EIGRP novamente. Isso pode ser verificado emitindo um comando **debug eigrp packets** novamente. Desta vez, as saídas dos roteadores Fort Worth e 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.
```

Troubleshoot

Link unidirecional

Você deve configurar os temporizadores Hello e Hold-time do EIGRP em ambas as extremidades. Se você configurar os temporizadores apenas em uma extremidade, um link unidirecional ocorrerá.

Um roteador em um link unidirecional pode receber pacotes de saudação. No entanto, os pacotes hello enviados não são recebidos na outra extremidade. Esse link unidirecional geralmente é indicado por *limite de repetição excedido* em uma extremidade.

Para visualizar as mensagens *limite de repetição excedido*, use os comandos **debug eigrp packet** e **debug ip eigrp notification**.

Informações Relacionadas

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