EIGRP消息身份驗證配置示例

目錄

簡介

本文說明如何為增強型內部網關路由協定(EIGRP)路由器新增消息身份驗證，並保護路由表免受蓄意或意外損壞。

在路由器的EIGRP消息中新增身份驗證可確保您的路由器只接受來自知道相同預共用金鑰的其他路由器的路由消息。如果沒有配置此身份驗證，如果有人向網路引入另一個具有不同或衝突的路由資訊的路由器，則路由器上的路由表可能會損壞，並可能引發拒絕服務攻擊。因此，當您為路由器之間傳送的EIGRP消息新增身份驗證時，可防止有人故意或意外將另一台路由器新增到網路並造成問題。

注意：將EIGRP消息身份驗證新增到路由器的介面時，該路由器會停止接收來自對等體的路由消息，直到這些消息也配置為進行消息身份驗證。這會**中斷**您網路上的路由通訊。如需詳細資訊，請參閱只設定Dallas時的訊息。

必要條件

需求

- 必須在所有路由器上正確配置時間。有關詳細資訊，請參閱配置NTP。
- 建議使用有效的EIGRP配置。

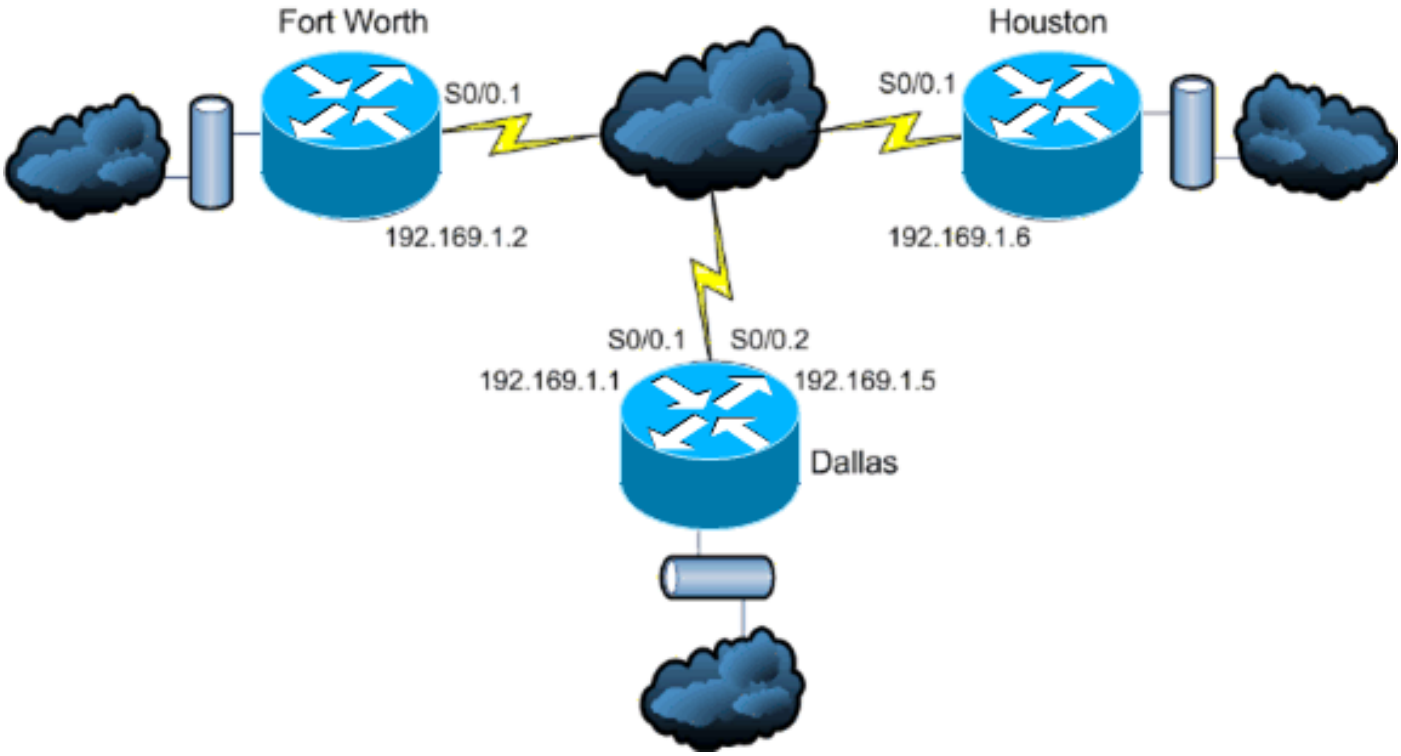
採用元件

本檔案中的資訊是根據Cisco IOS®軟體版本11.2及更新版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

網路圖表

本檔案會使用以下網路設定：



慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

背景資訊

在此場景中，網路管理員希望為達拉斯中心路由器與沃斯堡和休斯頓的遠端站點之間的EIGRP消息配置身份驗證。所有三台路由器上的EIGRP配置（無身份驗證）都已完成。以下示例輸出來自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
```

配置EIGRP消息身份驗證

EIGRP消息身份驗證的配置包括兩個步驟：

1. 建立金鑰鏈和金鑰。
2. 配置EIGRP身份驗證以使用該金鑰鏈和金鑰。

本節說明了在Dallas路由器，然後在Fort Worth和Houston路由器上配置EIGRP消息身份驗證的步驟。

在Dallas上建立金鑰鏈

路由驗證依賴於金鑰鏈上的金鑰才能運行。必須先建立金鑰鏈和至少一個金鑰，然後才能啟用身份驗證。

1. 進入全域性配置模式。
   ```
   Dallas#configure terminal
   ```

2. 建立金鑰鏈。此範例中使用的是MYCHAIN。
   ```
   Dallas(config)#key chain MYCHAIN
   ```

3. 指定金鑰編號。1用於本例中。**注意**：建議在配置涉及的所有路由器上使用相同的金鑰號。
   ```
   Dallas(config-keychain)#key 1
   ```

4. 指定金鑰的key-string。本例中使用的是securetraffic。
   ```
   Dallas(config-keychain-key)#key-string securetraffic
   ```

5. 結束配置。
   ```
   Dallas(config-keychain-key)#end
   Dallas#
   ```

在Dallas上配置身份驗證

建立金鑰鏈和金鑰後，必須配置EIGRP以使用金鑰執行消息身份驗證。在配置EIGRP的介面上完成此配置。

注意：將EIGRP消息身份驗證新增到Dallas介面時，它會停止接收來自對等體的路由消息，直到它們也配置為消息身份驗證。這會**中斷**您網路上的路由通訊。如需詳細資訊，請參閱只設定Dallas時的訊息。

1. 進入全域性配置模式。
   ```
   Dallas#configure terminal
   ```

2. 在全域性配置模式下，指定要在其上配置EIGRP消息身份驗證的介面。在本示例中，第一個介面是Serial 0/0.1。
   ```
   Dallas(config)#interface serial 0/0.1
   ```

3. 啟用EIGRP消息身份驗證。此處使用的10是網路的自治系統編號。md5表示將使用md5雜湊進行身份驗證。
```
Dallas(config-subif)#ip authentication mode eigrp 10 md5
```

4. 指定用於身份驗證的金鑰鏈。10是自治系統編號。MYCHAIN是在「建立金鑰鏈」(Create a Keychain)部分中建立的金鑰鏈。
```
Dallas(config-subif)#ip authentication key-chain eigrp 10 MYCHAIN
Dallas(config-subif)#end
```

5. 在介面Serial 0/0.2上完成相同的配置。
```
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#
```

配置Fort Worth

本節介紹在Fort Worth路由器上配置EIGRP消息身份驗證所需的命令。有關此處顯示的命令的更詳細說明，請參閱在Dallas上建立金鑰鏈和在Dallas上設定驗證。

```
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#
```

配置Houston

本節顯示了在Houston路由器上配置EIGRP消息身份驗證所需的命令。有關此處顯示的命令的更詳細說明，請參閱在Dallas上建立金鑰鏈和在Dallas上設定驗證。

```
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#
```

驗證

使用本節內容，確認您的組態是否正常運作。

附註：使用 **debug** 指令之前，請先參閱有關 Debug 指令的重要資訊。

僅配置Dallas時的消息

在Dallas路由器上配置了EIGRP消息身份驗證後，該路由器開始拒絕來自Fort Worth和Houston路由器的消息，因為它們尚未配置身份驗證。這可以通過在Dallas路由器上發出**debug eigrp packets**命令來驗證：

```
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.
```

配置所有路由器時的消息

一旦在所有三台路由器上配置了EIGRP消息身份驗證，它們就會再次開始交換EIGRP消息。這可以通過再次發出**debug eigrp packets**命令來驗證。這一次，沃思堡路由器和休斯敦路由器的輸出如下所示：

```
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.
```

疑難排解

單向鏈路

您必須在兩端配置EIGRP Hello計時器和保持時間計時器。如果僅在一端設定計時器，則會發生單向連結。

單向鏈路上的路由器可能能夠接收hello資料包。但是，在另一端不會收到發出的hello資料包。此單向連結通常由一個端的*超出重試限*制訊息指示。

若要檢視*retry limit exceeded*消息，請使用**debug eigrp packet**和**debug ip eigrp notifications**命令。

相關資訊

- 增強型內部閘道路由通訊協定(EIGRP)技術支援
- 技術支援與文件 - Cisco Systems