Esempio di configurazione dell'autenticazione dei messaggi EIGRP

Sommario

Introduzione

In questo documento viene spiegato come aggiungere l'autenticazione dei messaggi ai router EIGRP (Enhanced Interior Gateway Routing Protocol) e proteggere la tabella di routing da danneggiamenti intenzionali o accidentali.

L'aggiunta dell'autenticazione ai messaggi EIGRP dei router assicura che i router accettino solo messaggi di routing da altri router che conoscono la stessa chiave precondivisa. Se questa autenticazione non viene configurata, se un utente introduce nella rete un altro router con informazioni di route diverse o in conflitto, le tabelle di routing sui router potrebbero danneggiarsi e potrebbe verificarsi un attacco Denial of Service. Pertanto, quando si aggiunge l'autenticazione ai messaggi EIGRP inviati tra i router, si impedisce a un utente di aggiungere accidentalmente o intenzionalmente un altro router alla rete e si verifica un problema.

Attenzione: quando all'interfaccia di un router viene aggiunta l'autenticazione dei messaggi EIGRP, il router non riceve più messaggi di routing dai peer fino a che non vengono configurati per l'autenticazione dei messaggi. In questo modo **le** comunicazioni di routing sulla rete vengono interrotte. Per ulteriori informazioni, vedere Messaggi in cui è configurata solo la modalità Dallas.

Prerequisiti

Requisiti

- L'ora deve essere configurata correttamente su tutti i router. Per ulteriori informazioni, fare riferimento a Configurazione dell'NTP.
- Si consiglia una configurazione EIGRP funzionante.

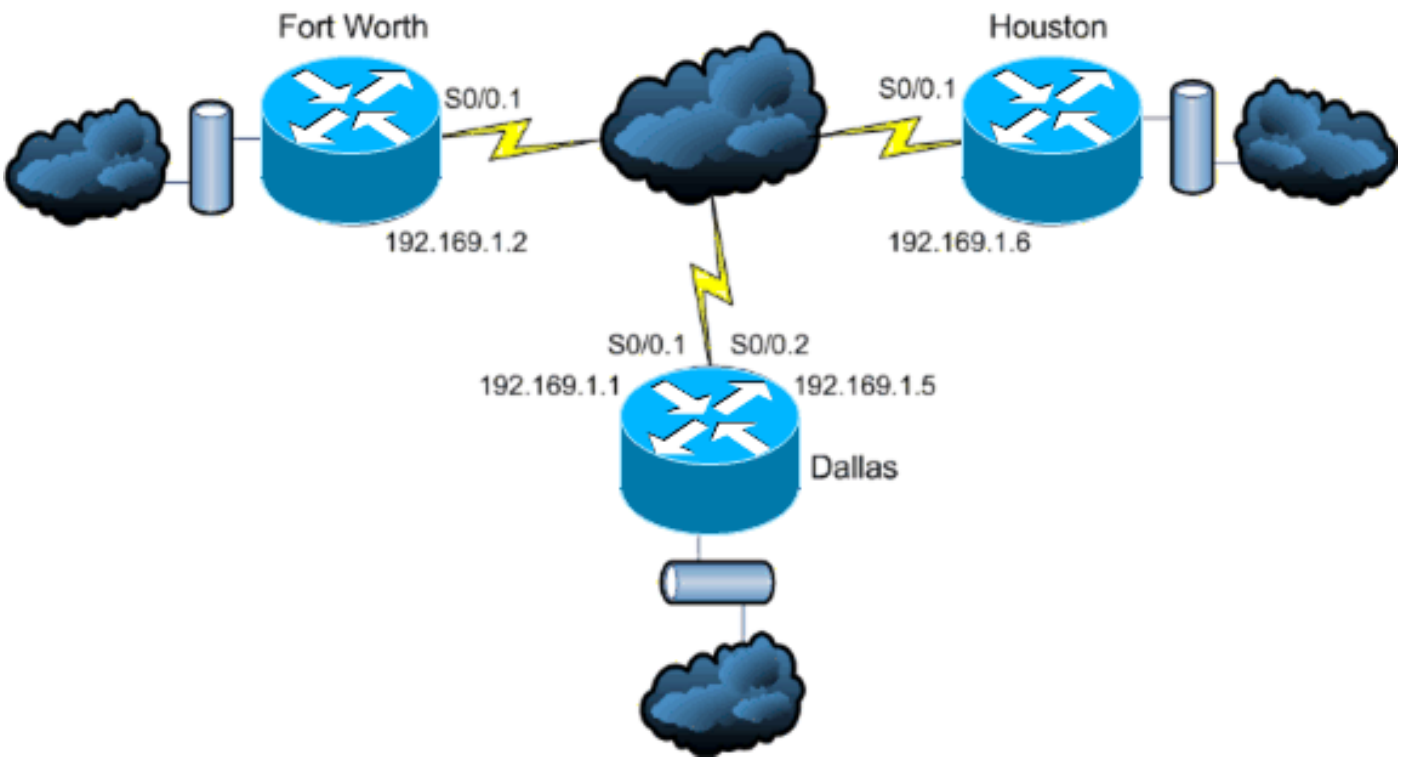
Componenti usati

Per questo documento, è stato usato il software Cisco IOS® versione 11.2 e successive.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Premesse

In questo scenario, un amministratore di rete desidera configurare l'autenticazione per i messaggi

EIGRP tra il router hub di Dallas e i siti remoti di Fort Worth e Houston. La configurazione EIGRP (senza autenticazione) è già stata completata su tutti e tre i router. Questo output di esempio viene generato da 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
```

Configura autenticazione messaggi EIGRP

La configurazione dell'autenticazione dei messaggi EIGRP prevede due passaggi:

1. Creazione di un portachiavi e di una chiave.
2. Configurazione dell'autenticazione EIGRP per l'utilizzo di tale portachiavi e chiave.

In questa sezione viene illustrata la procedura per configurare l'autenticazione dei messaggi EIGRP sul router Dallas e quindi sui router Fort Worth e Houston.

Creare un portachiavi a Dallas

L'autenticazione di routing si basa su una chiave di un portachiavi per funzionare. Prima di abilitare l'autenticazione, è necessario creare un portachiavi e almeno una chiave.

1. Accedere alla modalità di configurazione globale.
   ```
   Dallas#configure terminal
   ```

2. Creare la catena di chiavi. Nell'esempio viene utilizzato **MYCHAIN**.
   ```
   Dallas(config)#key chain MYCHAIN
   ```

3. Specificare il numero della chiave. **nell**'esempio viene utilizzato **1**.**Nota:** si consiglia di usare lo stesso numero di chiave su tutti i router coinvolti nella configurazione.
   ```
   Dallas(config-keychain)#key 1
   ```

4. Specificare la stringa della chiave. nell'esempio viene utilizzato **securetraffic**.
   ```
   Dallas(config-keychain-key)#key-string securetraffic
   ```

5. Terminare la configurazione.
   ```
   Dallas(config-keychain-key)#end
   Dallas#
   ```

Configura autenticazione in Dallas

Una volta creati un portachiavi e una chiave, è necessario configurare EIGRP per eseguire l'autenticazione del messaggio con la chiave. Questa configurazione viene completata sulle

interfacce su cui è configurato EIGRP.

Attenzione: quando si aggiunge l'autenticazione dei messaggi EIGRP alle interfacce Dallas, i messaggi di routing dei peer non vengono più ricevuti finché non vengono configurati per l'autenticazione dei messaggi. In questo modo **le** comunicazioni di routing sulla rete vengono interrotte. Per ulteriori informazioni, vedere Messaggi in cui è configurata solo la modalità Dallas.

1. Accedere alla modalità di configurazione globale.
   ```
   Dallas#configure terminal
   ```

2. In modalità di configurazione globale, specificare l'interfaccia su cui configurare l'autenticazione dei messaggi EIGRP. Nell'esempio, la prima interfaccia è **Serial 0/0.1**.
   ```
   Dallas(config)#interface serial 0/0.1
   ```

3. Abilitare l'autenticazione dei messaggi EIGRP. Il **10** utilizzato qui è il numero di sistema autonomo della rete. **md5** indica che l'hash md5 deve essere utilizzato per l'autenticazione.
   ```
   Dallas(config-subif)#ip authentication mode eigrp 10 md5
   ```

4. Specificare il portachiavi da utilizzare per l'autenticazione. **10** è il numero del sistema autonomo. **MYCHAIN** è il portachiavi creato nella sezione Crea portachiavi.
   ```
   Dallas(config-subif)#ip authentication key-chain eigrp 10 MYCHAIN
   Dallas(config-subif)#end
   ```

5. Completare la stessa configurazione sull'interfaccia 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#
   ```

Configurazione di Fort Worth

Questa sezione illustra i comandi necessari per configurare l'autenticazione dei messaggi EIGRP sul router Fort Worth. Per una spiegazione più dettagliata dei comandi mostrati di seguito, vedere Create a Keychain on Dallas e Configure Authentication on 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#
```

Configurazione Houston

Questa sezione illustra i comandi necessari per configurare l'autenticazione dei messaggi EIGRP sul router Houston. Per una spiegazione più dettagliata dei comandi mostrati di seguito, vedere

Create a Keychain on Dallas e Configure Authentication on 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#
```

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Nota: consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug**.

Messaggi in cui è configurata solo Dallas

Dopo aver configurato l'autenticazione dei messaggi EIGRP sul router Dallas, il router inizia a rifiutare i messaggi provenienti dai router Fort Worth e Houston perché non hanno ancora configurato l'autenticazione. È possibile verificare questa condizione eseguendo un comando **debug eigrp packets** sul router 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.
```

Messaggi quando tutti i router sono configurati

Una volta configurata l'autenticazione dei messaggi EIGRP su tutti e tre i router, questi iniziano a scambiare di nuovo i messaggi EIGRP. È possibile verificare questa condizione eseguendo nuovamente il comando **debug eigrp packets**. Questa volta vengono mostrati gli output dei router Fort Worth e Houston:

```
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.
```

Risoluzione dei problemi

Collegamento unidirezionale

Ènecessario configurare i timer EIGRP Hello e Hold-time su entrambe le estremità. Se si configurano i timer solo su un'estremità, si verifica un collegamento unidirezionale.

Un router su un collegamento unidirezionale potrebbe essere in grado di ricevere pacchetti hello. Tuttavia, i pacchetti hello inviati non vengono ricevuti dall'altra parte. Questo collegamento unidirezionale è in genere indicato dal *superamento del limite di tentativi* nei messaggi su un'estremità.

Per visualizzare i messaggi di *superamento* del *limite di tentativi*, usare i comandi **debug eigrp packet** e **debug ip eigrp notification**.

Informazioni correlate

- Supporto della tecnologia EIGRP (Enhanced Interior Gateway Routing Protocol)
- Documentazione e supporto tecnico – Cisco Systems