Konfigurationsbeispiel für EIGRP-Nachrichtenauthentifizierung

Inhalt

Einführung

In diesem Dokument wird veranschaulicht, wie Sie den EIGRP-Routern (Enhanced Interior Gateway Routing Protocol) eine Nachrichtenauthentifizierung hinzufügen und die Routing-Tabelle vor vorsätzlichen oder versehentlichen Beschädigungen schützen.

Durch das Hinzufügen einer Authentifizierung zu den EIGRP-Nachrichten Ihrer Router wird sichergestellt, dass Ihre Router nur Routing-Nachrichten von anderen Routern akzeptieren, die denselben vorinstallierten Schlüssel kennen. Wenn keine solche Authentifizierung konfiguriert ist und jemand einen anderen Router mit anderen oder in Konflikt stehenden Routeninformationen in das Netzwerk einführt, können die Routing-Tabellen auf Ihren Routern beschädigt werden und ein Denial-of-Service-Angriff stattfinden. Wenn Sie also den EIGRP-Nachrichten, die zwischen Ihren Routern gesendet werden, Authentifizierung hinzufügen, wird verhindert, dass jemand absichtlich oder versehentlich einen anderen Router zum Netzwerk hinzufügt und ein Problem verursacht.

Vorsicht: Wenn der Schnittstelle eines Routers eine EIGRP-Nachrichtenauthentifizierung hinzugefügt wird, hört dieser Router auf, Routing-Meldungen seiner Peers zu empfangen, bis er auch für die Nachrichtenauthentifizierung konfiguriert wurde. Dadurch **wird die** Routing-Kommunikation im Netzwerk unterbrochen. Weitere Informationen finden Sie unter Meldungen,

wenn nur Dallas konfiguriert ist.

Voraussetzungen

Anforderungen

- Die Uhrzeit muss auf allen Routern richtig konfiguriert sein. Weitere Informationen finden Sie unter Konfigurieren von NTP.
- Eine funktionierende EIGRP-Konfiguration wird empfohlen.

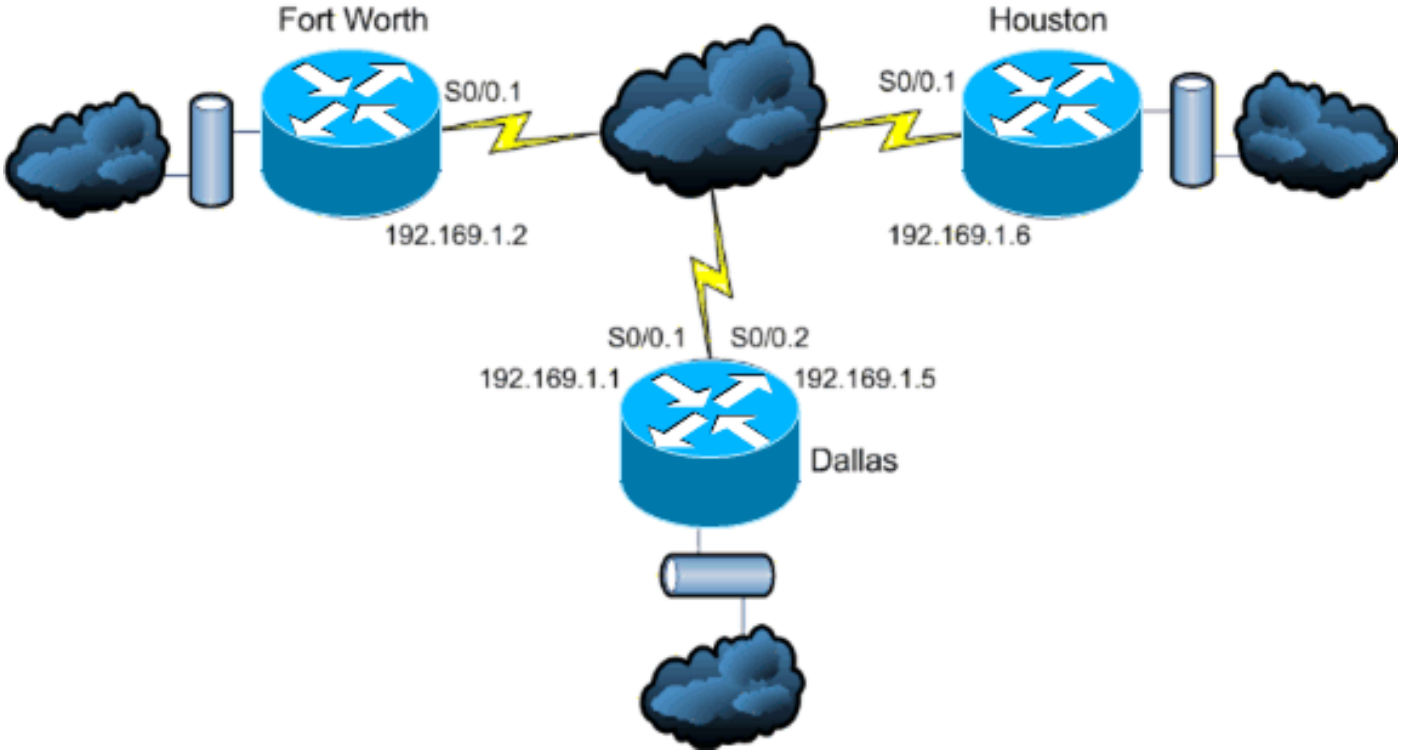
Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Cisco IOS® Software-Version 11.2 und höher.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

In diesem Szenario möchte ein Netzwerkadministrator die Authentifizierung für EIGRP-Nachrichten zwischen dem Hub-Router in Dallas und den Remote-Standorten in Fort Worth und Houston konfigurieren. Die EIGRP-Konfiguration (ohne Authentifizierung) ist auf allen drei Routern bereits abgeschlossen. Diese Beispielausgabe stammt von 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
```

Konfigurieren der EIGRP-Nachrichtenauthentifizierung

Die Konfiguration der EIGRP-Nachrichtenauthentifizierung besteht aus zwei Schritten:

1. Die Erstellung einer Schlüsselkette und eines Schlüssels.
2. Die Konfiguration der EIGRP-Authentifizierung zur Verwendung dieser Schlüsselkette und dieses Schlüssels.

In diesem Abschnitt werden die Schritte zum Konfigurieren der EIGRP-Nachrichtenauthentifizierung auf dem Dallas-Router und dann auf den Routern Fort Worth und Houston veranschaulicht.

Erstellen einer Keychain auf Dallas

Die Routing-Authentifizierung beruht auf einem Schlüssel in einer Schlüsselkette, um zu funktionieren. Bevor die Authentifizierung aktiviert werden kann, muss eine Schlüsselkette und mindestens ein Schlüssel erstellt werden.

1. Wechseln in den globalen Konfigurationsmodus
   ```
   Dallas#configure terminal
   ```

2. Erstellen Sie die Schlüsselkette. **MYCHAIN** wird in diesem Beispiel verwendet.
   ```
   Dallas(config)#key chain MYCHAIN
   ```

3. Geben Sie die Schlüsselnummer an. **1** wird in diesem Beispiel verwendet.**Hinweis:** Es wird empfohlen, dass die Schlüsselnummer auf allen Routern, die an der Konfiguration beteiligt sind, identisch ist.
   ```
   Dallas(config-keychain)#key 1
   ```

4. Geben Sie die Schlüsselzeichenfolge für den Schlüssel an. In diesem Beispiel wird **sicherer Datenverkehr** verwendet.
   ```
   Dallas(config-keychain-key)#key-string securetraffic
   ```

5. Beenden Sie die Konfiguration.
```
Dallas(config-keychain-key)#end
Dallas#
```

Konfigurieren der Authentifizierung in Dallas

Nachdem Sie eine Schlüsselkette und einen Schlüssel erstellt haben, müssen Sie EIGRP so konfigurieren, dass die Nachrichtenauthentifizierung mit dem Schlüssel durchgeführt wird. Diese Konfiguration ist auf den Schnittstellen abgeschlossen, auf denen EIGRP konfiguriert ist.

Vorsicht: Wenn den Dallas-Schnittstellen eine EIGRP-Nachrichtenauthentifizierung hinzugefügt wird, wird der Empfang von Routing-Nachrichten von Peers unterbrochen, bis diese auch für die Nachrichtenauthentifizierung konfiguriert sind. Dadurch **wird die** Routing-Kommunikation im Netzwerk unterbrochen. Weitere Informationen finden Sie unter Meldungen, wenn nur Dallas konfiguriert ist.

1. Wechseln in den globalen Konfigurationsmodus
```
Dallas#configure terminal
```

2. Geben Sie im globalen Konfigurationsmodus die Schnittstelle an, für die Sie die EIGRP-Nachrichtenauthentifizierung konfigurieren möchten. In diesem Beispiel ist die erste Schnittstelle **Serial 0/0.1**.
```
Dallas(config)#interface serial 0/0.1
```

3. Aktivieren Sie die EIGRP-Nachrichtenauthentifizierung. Die **10** wird hier als autonome Systemnummer des Netzwerks verwendet. **md5** gibt an, dass der md5 Hash für die Authentifizierung verwendet werden soll.
```
Dallas(config-subif)#ip authentication mode eigrp 10 md5
```

4. Geben Sie die Schlüsselkette an, die für die Authentifizierung verwendet werden soll. **10** ist die autonome Systemnummer. **MYCHAIN** ist die Schlüsselkette, die im Abschnitt Keychain erstellen erstellt wurde.
```
Dallas(config-subif)#ip authentication key-chain eigrp 10 MYCHAIN
Dallas(config-subif)#end
```

5. Führen Sie die gleiche Konfiguration für die Schnittstelle Serial 0/0.2 aus.
```
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#
```

Konfiguration von Fort Worth

Dieser Abschnitt enthält die Befehle, die zum Konfigurieren der EIGRP-Nachrichtenauthentifizierung auf dem Fort Worth-Router erforderlich sind. Ausführlichere Erläuterungen zu den hier gezeigten Befehlen finden Sie unter Erstellen einer Keychain auf Dallas und Konfigurieren der Authentifizierung auf 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#
```

Konfigurieren von Houston

Dieser Abschnitt enthält die Befehle, die für die Konfiguration der EIGRP-Nachrichtenauthentifizierung auf dem Houston-Router erforderlich sind. Ausführlichere Erläuterungen zu den hier gezeigten Befehlen finden Sie unter Erstellen einer Keychain auf Dallas und Konfigurieren der Authentifizierung auf 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#
```

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Hinweis: Beachten Sie vor der Verwendung von **Debug-**Befehlen die Informationen zu Debug-Befehlen.

Nachrichten, wenn nur Dallas konfiguriert ist

Sobald die EIGRP-Nachrichtenauthentifizierung auf dem Dallas-Router konfiguriert ist, beginnt dieser Router, Nachrichten von den Routern Fort Worth und Houston abzulehnen, da für sie noch keine Authentifizierung konfiguriert ist. Dies kann überprüft werden, indem der Befehl **debug eigrp packages** auf dem Dallas-Router ausgeführt wird:

```
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.
```

Nachrichten bei der Konfiguration aller Router

Sobald die EIGRP-Nachrichtenauthentifizierung auf allen drei Routern konfiguriert ist, beginnen sie erneut, EIGRP-Nachrichten auszutauschen. Dies kann überprüft werden, indem ein Befehl

debug eigrp packages erneut ausgegeben wird. Diese Zeitausgaben der Router Fort Worth und Houston werden angezeigt:

```
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.
```

Fehlerbehebung

Unidirektionale Verbindung

Sie müssen EIGRP Hello- und Hold-Time-Timer auf beiden Seiten konfigurieren. Wenn Sie die Timer nur an einem Ende konfigurieren, wird eine unidirektionale Verbindung hergestellt.

Ein Router auf einer unidirektionalen Verbindung kann möglicherweise Hello-Pakete empfangen. Die versendeten Hello-Pakete werden am anderen Ende jedoch nicht empfangen. Diese unidirektionale Verbindung wird in der Regel durch die *Beschränkung* der *Wiederholungsversuche überschritten* Nachrichten an einem Ende angezeigt.

Um die *Retry-Beschränkung* der *Überschreitung* von Nachrichten anzuzeigen, verwenden Sie die Befehle **debug eigrp-Paket** und **debug ip eigrp-Benachrichtigungen**.

Zugehörige Informationen

- Unterstützung der EIGRP-Technologie (Interior Gateway Routing Protocol)
- Technischer Support und Dokumentation - Cisco Systems