Configuratievoorbeeld van DHCP-berichtverificatie

Inhoud

Inleiding

Dit document illustreert hoe u berichtverificatie aan uw uitgebreide routers van de Binnengateway Routing Protocol (DHCP) kunt toevoegen en de routingtabel kunt beveiligen tegen opzettelijke of accidentele corruptie.

De toevoeging van authenticatie aan de berichten van uw routers EIS waarborgt dat uw routers slechts routeberichten van andere routers accepteren die de zelfde pre-gedeelde sleutel kennen. Zonder deze authenticatie ingesteld, als iemand een andere router met verschillende of tegenstrijdige routeinformatie over het netwerk introduceert, kunnen de routingtabellen op uw routers corrupt worden en kan er een 'denial of service'-aanval optreden. Dus wanneer u authenticatie aan de EHRM berichten toevoegt die tussen uw routers worden verzonden, voorkomt het iemand opzettelijk of per ongeluk een andere router aan het netwerk toe te voegen en veroorzaakt een probleem.

Waarschuwing: wanneer de EIS van het bericht aan de interface van een router wordt toegevoegd, houdt die router op het ontvangen van routingberichten van zijn gelijken tot zij ook voor berichtauthenticatie worden gevormd. Dit **onderbreekt** routingcommunicatie op uw netwerk. Zie Berichten wanneer alleen DSL's zijn ingesteld voor meer informatie.

Voorwaarden

Vereisten

- De tijd moet op alle routers correct worden ingesteld. Zie NTP configureren voor meer informatie.
- Een werkende configuratie wordt geadviseerd.

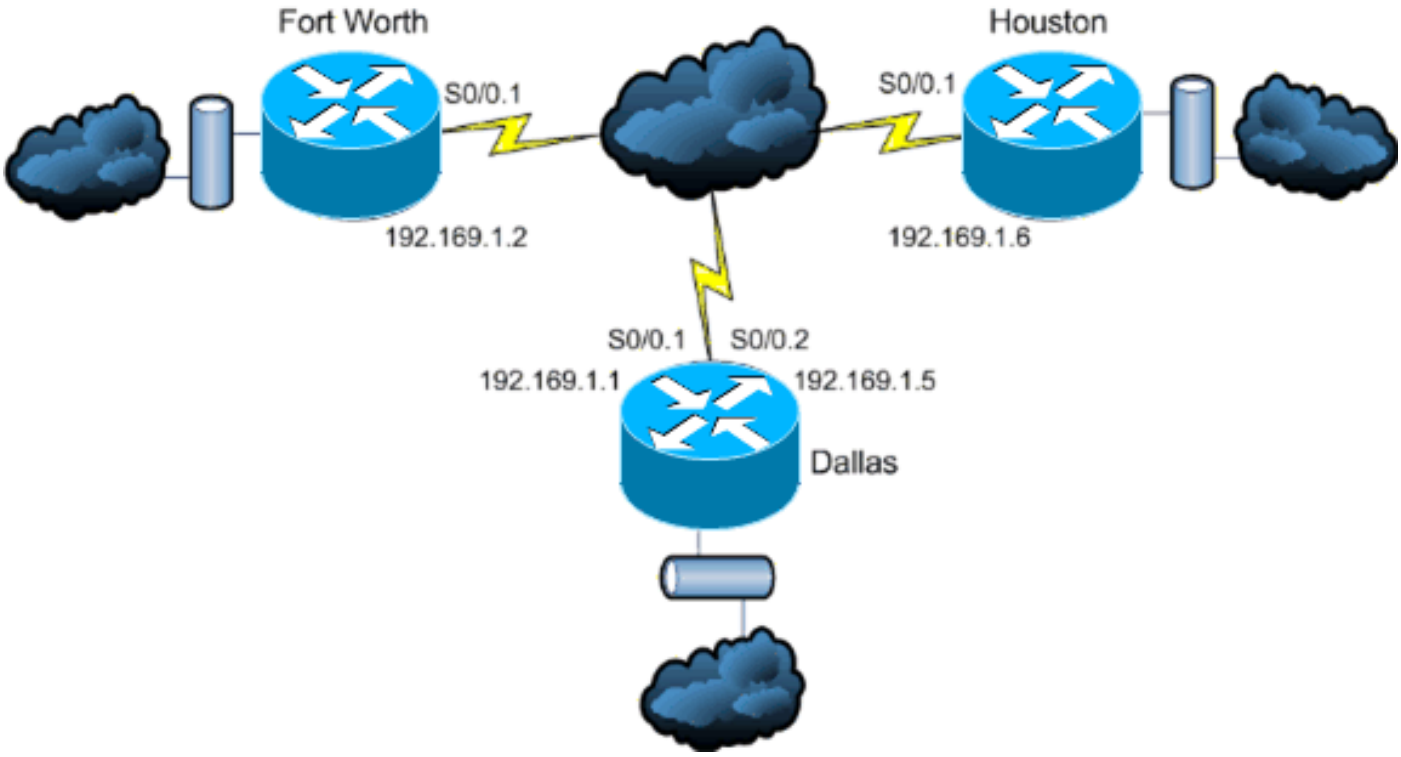
Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco IOS® softwarerelease 11.2 en hoger.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Achtergrondinformatie

In dit scenario wil een netwerkbeheerder authenticatie voor Ecu berichten tussen de router van de hub in Dallas en de verre plaatsen in de Vlek en Houston vormen. De configuratie (zonder

authenticatie) is reeds op alle drie routers voltooid. Deze voorbeelduitvoer komt van 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
```

Configureer RDRBTP-verificatie

De configuratie van de Ecu-berichtverificatie bestaat uit twee stappen:

1. De creatie van een sleutelketting en sleutel.
2. De configuratie van EcpEcu-verificatie om die sleutelketting en sleutel te gebruiken.

Deze sectie illustreert de stappen om EHRM berichtauthenticatie op de router Dallas en dan de routers van de Kort en Houston te configureren.

Een sleutelketting maken op Dallas

Routing Authenticatie is afhankelijk van een sleutel op een sleutelketen om te functioneren. Voordat verificatie kan worden ingeschakeld, moet een sleutelketen en ten minste één sleutel worden gecreëerd.

1. Geef de configuratie van het netwerk op.
   ```
   Dallas#configure terminal
   ```

2. Maak de sleutelketen. **MYCHAIN** wordt in dit voorbeeld gebruikt.
   ```
   Dallas(config)#key chain MYCHAIN
   ```

3. Specificeer het sleutelnummer. **1** wordt in dit voorbeeld gebruikt.**N.B.:** Het is aanbevolen het sleutelnummer op alle routers die bij de configuratie betrokken zijn, gelijk te geven.
   ```
   Dallas(config-keychain)#key 1
   ```

4. Specificeer de string voor de toets. in dit voorbeeld wordt gebruik gemaakt van **beveiligingsverkeer** .
   ```
   Dallas(config-keychain-key)#key-string securetraffic
   ```

5. Einde de configuratie.
   ```
   Dallas(config-keychain-key)#end
   Dallas#
   ```

Verificatie via Dallas configureren

Zodra u een ketting en een sleutel tot stand hebt gebracht, moet u EIS configureren om

berichtauthenticatie met de sleutel uit te voeren. Deze configuratie wordt voltooid op de interfaces waarop de DHCP is ingesteld.

Waarschuwing: Wanneer de EIS van het bericht aan de Dallas interfaces wordt toegevoegd, houdt het op het ontvangen van routingberichten van zijn gelijken tot zij ook voor berichtauthenticatie worden gevormd. Dit **onderbreekt** routingcommunicatie op uw netwerk. Zie Berichten wanneer alleen DSL's zijn ingesteld voor meer informatie.

1. Geef de configuratie van het netwerk op.
   ```
   Dallas#configure terminal
   ```

2. Van globale configuratiewijze, specificeer de interface die u EHRM berichtauthenticatie wilt configureren. In dit voorbeeld is de eerste interface **serieel 0/0.1**.
   ```
   Dallas(config)#interface serial 0/0.1
   ```

3. Schakel Ecp-berichtverificatie in. De **10** die hier wordt gebruikt is het autonome systeemnummer van het netwerk. **md5** geeft aan dat de md5 hash moet worden gebruikt voor echtheidscontrole .
   ```
   Dallas(config-subif)#ip authentication mode eigrp 10 md5
   ```

4. Specificeer de sleutelketen die voor authenticatie moet worden gebruikt. **10** is het autonome systeemnummer. **MYCHAIN** is de sleutelketen die is aangemaakt in het gedeelte Een sleutelketen maken.
   ```
   Dallas(config-subif)#ip authentication key-chain eigrp 10 MYCHAIN
   Dallas(config-subif)#end
   ```

5. Voltooi dezelfde configuratie op interface-seriële 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#
   ```

Fort Worth configureren

Deze sectie toont de opdrachten nodig om de Echtheidscontrole van het EIS-bericht op de router van de Veldwaarde te configureren. Voor een gedetailleerdere uitleg van de hier getoonde opdrachten, zie Een sleutelketen maken op Dallas en Verificatie op Dallas configureren.

```
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#
```

Configure Houston

Deze sectie toont de opdrachten nodig om de EIS-berichtverificatie op de Houston-router te configureren. Voor een gedetailleerdere uitleg van de hier getoonde opdrachten, zie Een sleutelketen maken op Dallas en Verificatie op Dallas configureren.

```
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#
```

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Opmerking: Raadpleeg Belangrijke informatie over debug Commands voordat u **debug**-opdrachten gebruikt.

Berichten waarbij alleen de Dallas is geconfigureerd

Zodra de Echtheidscontrole van het EIS- bericht op de router van Dallas wordt gevormd, begint die router berichten van de routers van de Kort en de Houston te verwerpen omdat zij nog geen authenticatie hebben ingesteld. Dit kan worden geverifieerd door een opdracht **debug** IP-pakketten op de Dallas-router uit te geven:

```
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.
```

Berichten wanneer alle routers zijn ingesteld

Nadat de EHRM berichtauthenticatie op alle drie routers is ingesteld, beginnen ze EHRM berichten opnieuw uit te wisselen. Dit kan worden geverifieerd door de opdracht **debug** IP-**pakketten** opnieuw uit te voeren. Deze keer worden de uitvoer van de routers van Fort Worth en Houston weergegeven:

```
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.
```

Problemen oplossen

Unidirectionele link

U moet de tijden van de deelnemers aan beide eindpunten van de EHRM en van de Tijd van de Wacht van de tijd configureren. Als u de timers slechts op één eind vormt, komt een unidirectionele verbinding voor.

Een router op een unidirectionele verbinding kan hallo pakketten ontvangen. Maar de verschenen hallo-pakketten worden aan het andere eind niet ontvangen. Deze unidirectionele link wordt normaal gesproken aangegeven door een *overschrijdingslimiet* aan één kant.

Om de *reprobeert limiet te* bekijken *overschreden* berichten, gebruikt u het **debug** RTP-**pakket** en **debug ip eigrp-kennisgevingen**.

Gerelateerde informatie

- Verbeterde ondersteuning voor Interior Gateway Routing Protocol (NGEW)
- Technische ondersteuning en documentatie – Cisco Systems