EIGRP 메시지 인증 컨피그레이션 예

목차

소개

이 문서에서는 EIGRP(Enhanced Interior Gateway Routing Protocol) 라우터에 메시지 인증을 추가하고 의도적이거나 우발적인 손상으로부터 라우팅 테이블을 보호하는 방법을 설명합니다.

라우터의 EIGRP 메시지에 인증을 추가하면 라우터가 동일한 사전 공유 키를 알고 있는 다른 라우터의 라우팅 메시지만 수락할 수 있습니다.이 인증을 구성하지 않으면 다른 라우터가 네트워크에 서로 다르거나 충돌하는 경로 정보가 있는 다른 라우터를 소개하면 라우터의 라우팅 테이블이 손상되고 서비스 거부 공격이 발생할 수 있습니다.따라서 라우터 간에 전송되는 EIGRP 메시지에 인증을 추가하면 누군가가 의도적으로 또는 실수로 네트워크에 다른 라우터를 추가하여 문제를 일으키는 것을 방지합니다.

주의: EIGRP 메시지 인증이 라우터의 인터페이스에 추가되면 해당 라우터는 메시지 인증용으로 구성될 때까지 해당 피어로부터 라우팅 메시지 수신을 중지합니다.이렇게 **하면** 네트워크의 라우팅 통신이 중단됩니다.자세한 내용은 Dallas만 구성된 경우 메시지를 참조하십시오.

사전 요구 사항

요구 사항

- 모든 라우터에서 시간을 올바르게 구성해야 합니다.자세한 내용은 NTP 구성을 참조하십시오.
- 작동하는 EIGRP 컨피그레이션이 권장됩니다.

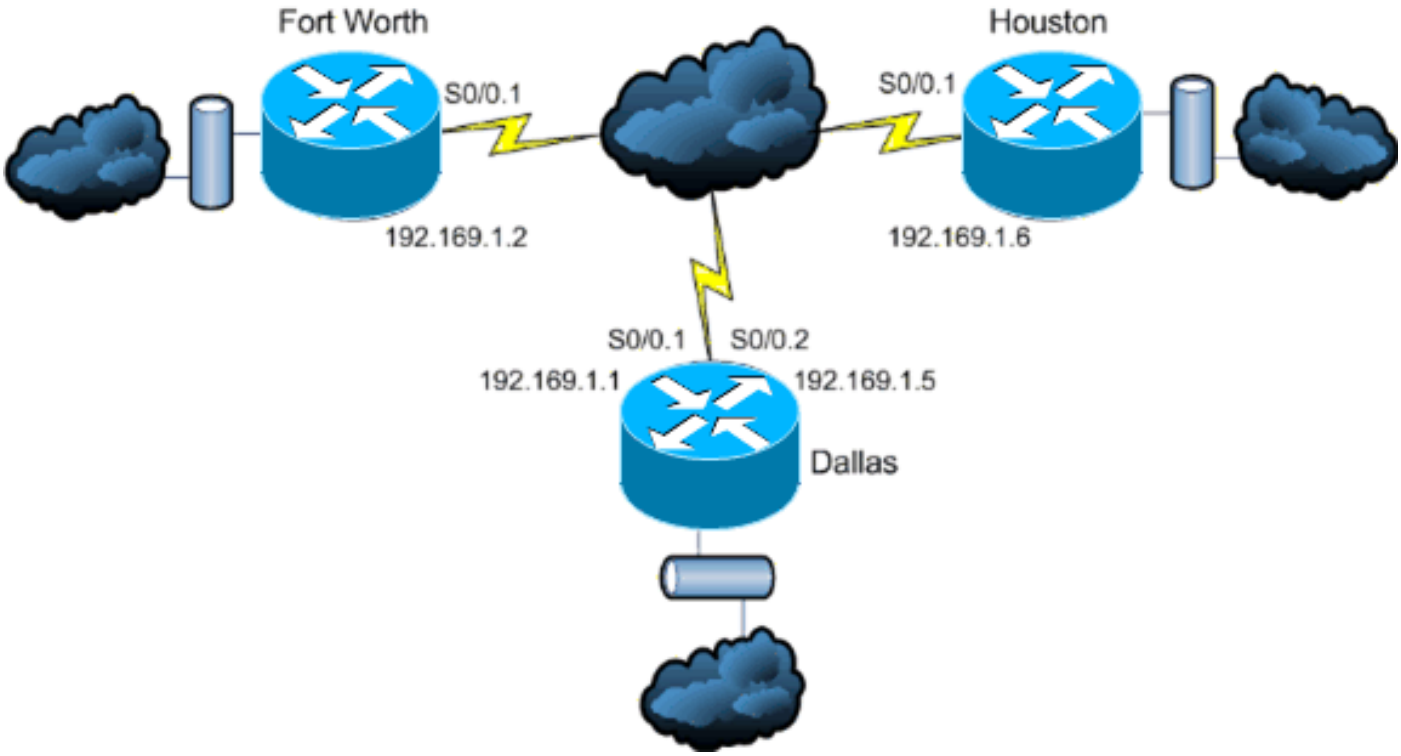
사용되는 구성 요소

이 문서의 정보는 Cisco IOS® 소프트웨어 릴리스 11.2 이상을 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

배경 정보

이 시나리오에서는 네트워크 관리자가 Dallas의 허브 라우터와 Fort Worth와 Houston의 원격 사이트 간에 EIGRP 메시지에 대한 인증을 구성하려고 합니다.EIGRP 컨피그레이션(인증 없음)이 세 라우터 모두에서 이미 완료되었습니다.이 예제 출력은 Dallas에서 가져온 것입니다.

```
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
```

EIGRP 메시지 인증 구성

EIGRP 메시지 인증의 컨피그레이션은 다음 두 단계로 구성됩니다.

1. 키 체인 및 키 생성
2. 해당 키 체인 및 키를 사용하도록 EIGRP 인증의 컨피그레이션입니다.

이 섹션에서는 Dallas 라우터와 Fort Worth 및 Houston 라우터에서 EIGRP 메시지 인증을 구성하는 단계를 설명합니다.

댈러스에서 키 체인 만들기

라우팅 인증은 키 체인의 키를 사용하여 작동합니다.인증을 활성화하려면 먼저 키 체인과 키를 하나 이상 생성해야 합니다.

1. 전역 컨피그레이션 모드로 들어갑니다.
   ```
   Dallas#configure terminal
   ```

2. 키 체인을 생성합니다.**MYCHAIN**은 이 예에서 사용됩니다.
   ```
   Dallas(config)#key chain MYCHAIN
   ```

3. 키 번호를 지정합니다.**1**이 이 예제에 사용됩니다.**참고:** 컨피그레이션과 관련된 모든 라우터에서 키 번호가 동일해야 합니다.
   ```
   Dallas(config-keychain)#key 1
   ```

4. 키의 키 문자열을 지정합니다.**securetraffic**이 이 예에서 사용됩니다.
   ```
   Dallas(config-keychain-key)#key-string securetraffic
   ```

5. 컨피그레이션을 종료합니다.
   ```
   Dallas(config-keychain-key)#end
   Dallas#
   ```

댈러스에서 인증 구성

키 체인과 키를 생성한 후에는 키를 사용하여 메시지 인증을 수행하도록 EIGRP를 구성해야 합니다.이 컨피그레이션은 EIGRP가 구성된 인터페이스에서 완료됩니다.

주의: EIGRP 메시지 인증이 달라스 인터페이스에 추가되면 피어가 메시지 인증용으로 구성될 때까지 라우팅 메시지 수신을 중지합니다.이렇게 **하면** 네트워크의 라우팅 통신이 중단됩니다.자세한 내용은 Dallas만 구성된 경우 메시지를 참조하십시오.

1. 전역 컨피그레이션 모드로 들어갑니다.
   ```
   Dallas#configure terminal
   ```

2. 전역 컨피그레이션 모드에서 EIGRP 메시지 인증을 구성할 인터페이스를 지정합니다.이 예에

서 첫 번째 인터페이스는 **Serial 0/0.1입니다**.

```
Dallas(config)#interface serial 0/0.1
```

3. EIGRP 메시지 인증을 활성화합니다.여기서 사용하는 10은 네트워크의 자동 시스템 번호입니다.**md5**는 md5 해시가 인증에 사용됨을 나타냅니다.

```
Dallas(config-subif)#ip authentication mode eigrp 10 md5
```

4. 인증에 사용할 키 체인을 지정합니다.**10**은 자동 시스템 번호입니다.**MYCHAIN**은 Create a Keychain 섹션에서 생성된 키 체인입니다.

```
Dallas(config-subif)#ip authentication key-chain eigrp 10 MYCHAIN
Dallas(config-subif)#end
```

5. 인터페이스 Serial 0/0.2에서 동일한 구성을 완료합니다.

```
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#
```

포트 워스 구성

이 섹션에서는 Fort Worth 라우터에서 EIGRP 메시지 인증을 구성하는 데 필요한 명령을 보여줍니다.여기에 표시된 명령에 대한 자세한 설명은 Dallas에서 키 체인 만들기 및 Dallas에서 인증 구성을 참조하십시오.

```
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#
```

휴스턴 구성

이 섹션에서는 Houston 라우터에서 EIGRP 메시지 인증을 구성하는 데 필요한 명령을 보여줍니다.여기에 표시된 명령에 대한 자세한 설명은 Dallas에서 키 체인 만들기 및 Dallas에서 인증 구성을 참조하십시오.

```
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#
```

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

참고: debug **명령**을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

달라스만 구성된 경우 메시지

Dallas 라우터에 EIGRP 메시지 인증이 구성되면 Fort Worth 및 Houston 라우터에서 보내는 메시지를 거부하기 시작합니다. 아직 인증이 구성되지 않았기 때문입니다.이는 Dallas 라우터에서 debug eigrp packets 명령**을 실행하여** 확인할 수 있습니다.

```
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.
```

모든 라우터가 구성된 경우의 메시지

세 라우터 모두에 EIGRP 메시지 인증이 구성되면 EIGRP 메시지를 다시 교환하기 시작합니다.이는 debug eigrp packets 명령을 다시 한 번 **실행하여** 확인할 수 있습니다.Fort Worth 및 Houston 라우터의 시간 출력이 표시됩니다.

```
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.
```

문제 해결

단방향 링크

양쪽 끝에서 EIGRP Hello 및 Hold-time 타이머를 구성해야 합니다.타이머를 한 쪽 끝에만 구성하면 단방향 링크가 발생합니다.

단방향 링크의 라우터가 hello 패킷을 수신할 수 있습니다.그러나 전송된 hello 패킷은 다른 끝에서는 수신되지 않습니다.이 단방향 링크는 일반적으로 한 쪽의 *재시도 제한 초과* 메시지로 표시됩니다.

재시도 제한 초과 메시지를 보려면 debug eigrp **packet** 및 debug ip eigrp **notifications** 명령을 사용합니다.

관련 정보

- EIGRP(Enhanced Interior Gateway Routing Protocol) 기술 지원
- 기술 지원 및 문서 – Cisco Systems