RIPv2에서 인증을 위한 샘플 컨피그레이션

목차

소개

이 문서에서는 RIPv2(Routing Information Protocol version 2)에 대한 라우팅 정보 교환 프로세스를 인증하기 위한 샘플 컨피그레이션을 보여 줍니다.

Cisco의 RIPv2 구현은 두 가지 인증 모드를 지원합니다. 일반 텍스트 인증 및 MD5(Message Digest 5) 인증 인증이 활성화된 경우 모든 RIPv2 패킷의 기본 설정은 일반 텍스트 인증 모드입니다. 보안의 경우 암호화되지 않은 인증 비밀번호가 모든 RIPv2 패킷에서 전송되므로 일반 텍스트 인증을 사용할 수 없습니다.

참고: RIP 버전 1(RIPv1)은 인증을 지원하지 않습니다. RIPv2 패킷을 보내고 받는 경우 인터페이스에서 RIP 인증을 활성화할 수 있습니다.

사전 요구 사항

요구 사항

이 문서의 독자는 다음에 대한 기본적인 이해가 있어야 합니다.

- RIPv1 및 RIPv2

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다. Cisco IOS® Software 버전 11.1부터 RIPv2가 지원되므로 컨피그레이션에 지정된 모든 명령이 Cisco IOS® Software 버전 11.1 이상에서 지원됩니다.

문서의 컨피그레이션은 다음 소프트웨어 및 하드웨어 버전을 사용하여 테스트되고 업데이트됩니다 .

- Cisco 2500 Series 라우터
- Cisco IOS Software 버전 12.3(3)

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.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

배경 정보

보안은 오늘날 네트워크 설계자의 주요 관심사 중 하나입니다. 네트워크 보안에는 라우팅 테이블에 입력된 정보가 유효한지, 네트워크 중단을 시도하는 사람이 시작한 것이 아닌지 또는 변조되지 않았는지 확인하는 등 라우터 간 라우팅 정보 교환을 보호하는 것이 포함됩니다. 공격자는 잘못된 업데이트를 도입하여 라우터를 잘못된 대상으로 데이터를 전송하도록 유도하거나 네트워크 성능을 심각하게 떨어뜨릴 수 있습니다. 또한 잘못된 경로 업데이트는 네트워크 경계에서 **패시브 인터페이스** 명령을 사용하지 않는 등의 잘못된 컨피그레이션 또는 잘못된 라우터로 인해 라우팅 테이블에 나타날 수 있습니다. 따라서 라우터에서 실행 중인 라우팅 업데이트 프로세스를 인증하는 것이 중요합니다.

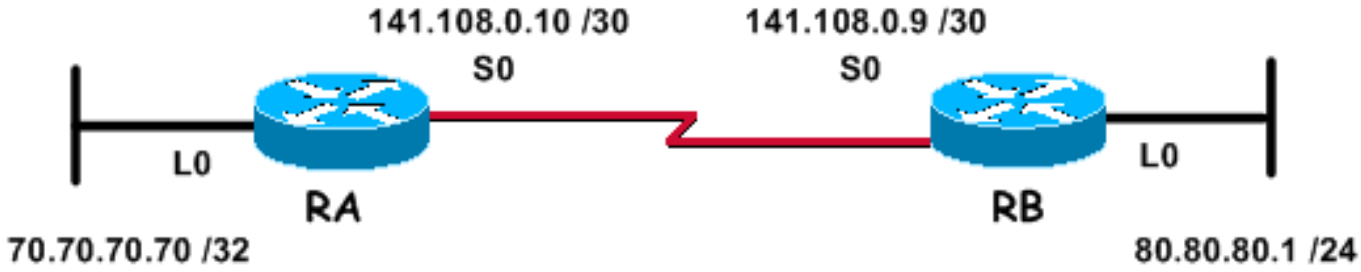
구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: 이 문서에 사용된 명령에 대한 추가 정보를 찾으려면 명령 조회 도구(등록된 고객만 해당)를 사용합니다.

네트워크 다이어그램

이 문서에서는 아래 다이어그램에 표시된 네트워크 설정을 사용합니다.



위의 네트워크는 다음 컨피그레이션 예에 사용되며 두 개의 라우터로 구성됩니다. 라우터 RA 및 라우터 RB - 둘 다 RIP를 실행하고 라우팅 업데이트를 정기적으로 교환합니다. 직렬 링크를 통해 이러한 라우팅 정보 교환을 인증해야 합니다.

구성

RIPv2에서 인증을 구성하려면 다음 단계를 수행합니다.

1. 이름으로 키 체인을 정의합니다.**참고:** 키 체인은 인터페이스에서 사용할 수 있는 키 집합을 결정합니다. 키 체인이 구성되지 않은 경우 해당 인터페이스에서 인증이 수행되지 않습니다.
2. 키 체인의 키 또는 키를 정의합니다.
3. 키에 사용할 암호 또는 키 문자열을 지정합니다.인증 중인 라우팅 프로토콜을 사용하여 패킷에서 보내고 받아야 하는 인증 문자열입니다. 아래 예에서 문자열 값은 234입니다.
4. 인터페이스에서 인증을 활성화하고 사용할 키 체인을 지정합니다.인증은 인터페이스별로 활성화되므로 RIPv2를 실행하는 라우터는 특정 인터페이스에서 인증하도록 구성할 수 있으며 다른 인터페이스에서 어떤 인증도 하지 않고 작동할 수 있습니다.
5. 인터페이스에서 일반 텍스트 또는 MD5 인증을 사용할지 지정합니다.이전 단계에서 인증이 활성화된 경우 RIPv2에 사용되는 기본 인증은 일반 텍스트 인증입니다. 따라서 일반 텍스트 인증을 사용할 경우 이 단계는 필요하지 않습니다.
6. 키 관리를 구성합니다(이 단계는 선택 사항).키 관리는 인증 키를 제어하는 방법입니다. 이는 한 인증 키를 다른 인증 키로 마이그레이션하는 데 사용됩니다. 자세한 내용은 IP 라우팅 프로토콜 독립 기능 구성의 "인증 키 관리" 섹션을 참조하십시오.

일반 텍스트 인증 구성

RIP 업데이트를 인증할 수 있는 두 가지 방법 중 하나는 일반 텍스트 인증을 사용하는 것입니다. 아래 표에 표시된 대로 구성할 수 있습니다.

RA
key chain kal *!--- Name a key chain. A key chain may contain more than one key for added security. !--- It need not be identical on the remote router.* **key 1** *!--- This is the Identification number of an authentication key on a key chain. !--- It need not be identical on the remote router.* **key-string 234** *!--- The actual password or key-string. !--- It needs to be identical to the key-string on the remote router.* ! interface Loopback0 ip address 70.70.70.70 255.255.255.255 ! interface Serial0 ip address

```
141.108.0.10 255.255.255.252 ip rip authentication key-
chain kal
!--- Enables authentication on the interface and
configures !--- the key chain that will be used. !
router rip version 2 network 141.108.0.0 network
70.0.0.0
```

RB

```
key chain kal

key 1
key-string 234


!

interface Loopback0

 ip address 80.80.80.1 255.255.255.0

!

interface Serial0

 ip address 141.108.0.9 255.255.255.252

 ip rip authentication key-chain kal

 clockrate 64000

!

router rip

 version 2

 network 141.108.0.0

 network 80.0.0.0
```

명령에 대한 자세한 내용은 Cisco IOS IP 명령 참조를 참조하십시오.

MD5 인증 구성

MD5 인증은 Cisco가 원래 RFC 1723 정의 일반 텍스트 인증에 추가하는 선택적 인증 모드입니다. 추가 명령 ip rip 인증 모드 md5를 사용하는 경우를 제외하고 일반 텍스트 인증의 컨피그레이션과 동일합니다. 사용자는 MD5 인증 방법을 위해 링크의 양쪽에서 라우터 인터페이스를 구성해야 합니다. 그러면 키 번호와 키 문자열이 양쪽에서 일치하는지 확인해야 합니다.

RA

```
key chain kal

!--- Need not be identical on the remote router. key 1
```

```
!--- Needs to be identical on remote router. key-string
234

!--- Needs to be identical to the key-string on the
remote router. ! interface Loopback0 ip address
70.70.70.70 255.255.255.255 ! interface Serial0 ip
address 141.108.0.10 255.255.255.252 ip rip
authentication mode md5
!--- Specifies the type of authentication used !--- in
RIPv2 packets. !--- Needs to be identical on remote
router. !-- To restore clear text authentication, use
the no form of this command. ip rip authentication key-
chain kal

 !

 router rip

  version 2

  network 141.108.0.0

  network 70.0.0.0
```

RB

```
key chain kal

key 1

key-string 234

!

interface Loopback0

 ip address 80.80.80.1 255.255.255.0

!

interface Serial0

 ip address 141.108.0.9 255.255.255.252

 ip rip authentication mode md5

 ip rip authentication key-chain kal

 clockrate 64000

!

router rip

 version 2

 network 141.108.0.0

 network 80.0.0.0
```

명령에 대한 자세한 내용은 Cisco IOS 명령 참조를 참조하십시오.

다음을 확인합니다.

일반 텍스트 인증 확인

이 섹션에서는 컨피그레이션이 제대로 작동하는지 확인하는 정보를 제공합니다.

위에 표시된 대로 라우터를 구성하면 모든 라우팅 업데이트 교환이 승인되기 전에 인증됩니다. 이는 debug ip rip 및 **show ip route** 명령에서 얻은 출력을 관찰하여 확인할 수 있습니다.

참고: debug 명령을 실행하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

```
RB#debug ip rip

 RIP protocol debugging is on

*Mar  3 02:11:39.207: RIP: received packet with text authentication 234

*Mar  3 02:11:39.211: RIP: received v2 update from 141.108.0.10 on Serial0

*Mar  3 02:11:39.211: RIP: 70.0.0.0/8 via 0.0.0.0 in 1 hops

RB#show ip route

R    70.0.0.0/8 [120/1] via 141.108.0.10, 00:00:25, Serial0

     80.0.0.0/24 is subnetted, 1 subnets

C       80.80.80.0 is directly connected, Loopback0

     141.108.0.0/30 is subnetted, 1 subnets

C       141.108.0.8 is directly connected, Serial0
```

일반 텍스트 인증을 사용하면 로컬 라우팅 교환 프로세스에 참여하지 않으려는 라우터에서 시작된 라우팅 업데이트를 추가할 수 없으므로 네트워크 설계가 향상됩니다. 그러나 이 인증 유형은 안전하지 않습니다. 비밀번호(이 예에서는 234)는 일반 텍스트로 교환됩니다. 그것은 쉽게 포착되고 악용될 수 있다. 앞에서 언급한 것처럼 보안이 문제가 될 경우 일반 텍스트 인증보다 MD5 인증을 선호해야 합니다.

MD5 인증 확인

위에 표시된 대로 RA 및 RB 라우터를 구성하면 모든 라우팅 업데이트 교환이 승인되기 전에 인증됩니다. 이는 debug ip rip 및 **show ip route** 명령에서 얻은 출력을 관찰하여 확인할 수 있습니다.

```
RB#debug ip rip

 RIP protocol debugging is on

*Mar  3 20:48:37.046: RIP: received packet with MD5 authentication

*Mar  3 20:48:37.046: RIP: received v2 update from 141.108.0.10 on Serial0
```

```
*Mar  3 20:48:37.050:  70.0.0.0/8 via 0.0.0.0 in 1 hops
```

```
RB#show ip route
R    70.0.0.0/8 [120/1] via 141.108.0.10, 00:00:03, Serial0
     80.0.0.0/24 is subnetted, 1 subnets
C       80.80.80.0 is directly connected, Loopback0
     141.108.0.0/30 is subnetted, 1 subnets
C       141.108.0.8 is directly connected, Serial0
```

MD5 인증은 강력한 해싱 알고리즘으로 확인된 단방향 MD5 해시 알고리즘을 사용합니다. 이 인증 모드에서 라우팅 업데이트는 인증을 위해 비밀번호를 전달하지 않습니다. 대신, 비밀번호에 MD5 알고리즘을 실행하여 생성되는 128비트 메시지가 인증용으로 함께 전송됩니다. 따라서 일반 텍스트 인증보다 안전하므로 일반 텍스트 인증에서 MD5 인증을 사용하는 것이 좋습니다.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

문제 해결 명령

일부 **show 명령은** 출력 인터프리터 툴 에서 지원되는데(등록된 고객만), 이 툴을 사용하면 **show 명령 출력의 분석 결과를 볼 수 있습니다.**

debug **ip rip** 명령은 RIPv2 인증 관련 문제를 해결하는 데 사용할 수 있습니다.

참고: debug 명령을 실행하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

참고: 다음은 **debug ip rip** 명령 출력의 예입니다. 이 경우 인접 라우터 간에 동일해야 하는 인증 관련 매개변수가 일치하지 않습니다. 따라서 라우터가 하나 또는 둘 다 라우팅 테이블에 수신된 경로를 설치하지 않을 수 있습니다.

```
RA#debug ip rip
   RIP protocol debugging is on

   *Mar 1 06:47:42.422: RIP: received packet with text authentication 234
   *Mar 1 06:47:42.426: RIP: ignored v2 packet from 141.108.0.9 (invalid authentication)

   RB#debug ip rip
   RIP protocol debugging is on

   *Mar 1 06:48:58.478: RIP: received packet with text authentication 235
```

```
*Mar 1 06:48:58.482: RIP: ignored v2 packet from 141.108.0.10 (invalid authentication)
```

show ip route 명령의 다음 출력에서는 **라우터가 RIP를 통해 경로를 학습하고 있지 않음을 보여줍니다.**

```
RB#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

80.0.0.0/24 is subnetted, 1 subnets

   C 80.80.80.0 is directly connected, Loopback0

   141.108.0.0/30 is subnetted, 1 subnets

   C 141.108.0.8 is directly connected, Serial0

   RB#
```

참고 1: 일반 텍스트 인증 모드를 사용할 경우 다음 매개변수가 성공적인 인증을 위해 인접 라우터에서 일치하는지 확인합니다.

- 키 문자열
- 인증 모드

참고 2: MD5 인증 모드를 사용할 때 인증에 성공하려면 다음 매개변수가 인접 라우터에서 일치하는지 확인합니다.

- 키 문자열
- 키 번호
- 인증 모드

관련 정보

- RIP(Routing Information Protocol) 소개
- RIP 구성
- IP 라우팅 프로토콜 독립 기능 구성
- RIP 명령
- Cisco IOS IP 명령 참조, 볼륨 2/4: 라우팅 프로토콜, 릴리스 12.3
- RIP 기술 지원 페이지
- IP 라우팅 프로토콜 기술 지원 페이지
- Technical Support - Cisco Systems