RIPv2 认证示例配置

目录

简介

本文档介绍 Routing Information Protocol 版本 2 (RIPv2) 路由信息交换进程身份验证的配置示例。

Cisco RIPv2 实施支持两种身份验证模式：纯文本身份验证和消息摘要 5 (MD5) 身份验证。启用身份验证时，在每个 RIPv2 数据包中，纯文本身份验证模式都是默认设置。如果考虑安全性，就不应该使用纯文本身份验证，因为在每个 RIPv2 数据包中将发送未加密的身份验证口令。

注意： RIP 版本 1 (RIPv1) 不支持身份验证。如果是发送和接收 RIPv2 数据包，则可在接口上启用 RIP 身份验证。

先决条件

要求

本文档的读者应该对以下主题有一定的基本了解：

- RIPv1 和 RIPv2

使用的组件

本文档不限于特定的软件和硬件版本。自 Cisco IOS® 软件版本 11.1 开始提供了对 RIPv2 的支持，因此 Cisco IOS® 软件版本 11.1 及更高版本支持配置中给出的所有命令。

测试和更新本文档中的配置时使用的是以下版本的软件和硬件：

- Cisco 2500 系列路由器
- Cisco IOS 软件版本 12.3(3)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

如今，安全是网络设计人员的首要关注点之一。保护网络包括保护路由器间的路由信息交换，例如，确保进入路由表的信息有效，而且不会由试图干扰网络的人发起或被其篡改。攻击者可能会尝试引入无效更新，以欺骗路由器发送数据到错误的目标地址或严重降低网络性能。此外，由于配置不良（例如不在网络边界上使用 **passive interface** 命令）或路由器功能不正常，无效的路由更新可能最终就留在路由表中。因此就有必要对路由器上运行的路由更新进程进行身份验证。

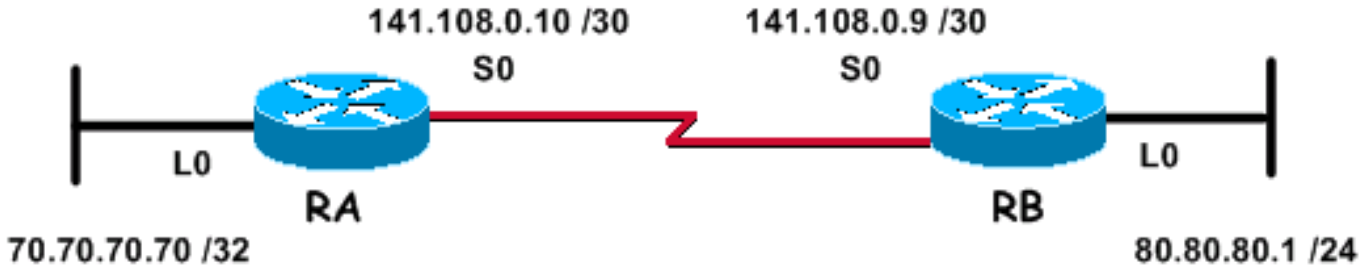
配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 要查找本文档所用命令的其他信息，请使用命令查找工具（仅限注册用户）。

网络图

本文档使用下图所示的网络设置。



以下配置示例中使用的上述网络由两个路由器组成，即路由器 RA 和路由器 RB，它们都运行 RIP 并定期交换路由更新。通过串行链路进行的这种路由信息交换必须经过身份验证。

配置

执行以下步骤，以配置 RIPv2 中的身份验证：

1. 为密钥链定义一个名称。**注意：** 密钥链确定了一组可在接口上使用的密钥。如果没有配置密钥链，在该接口上就不执行身份验证。
2. 定义钥匙链上的密钥。
3. 指定用于密钥的口令或密钥字符串。这是使用所验证的路由协议的数据包中必须发送和接收的身份验证字符串。（在下面给出的示例中，字符串的值是 234。）
4. 启用接口上的身份验证并指定要使用的密钥链。由于身份验证是按接口启用的，因此对于某个运行 RIPv2 的路由器，可以在某些特定接口上进行身份验证配置，而无需其他任何接口也进行身份验证。
5. 指定接口是使用纯文本身份验证还是 MD5 身份验证。在上一步启用身份验证后，RIPv2 中使用的默认身份验证是纯文本身份验证。因此，如果要使用纯文本身份验证，则无需执行此步骤。
6. 配置密钥管理（此步骤为可选）。密钥管理是一种控制身份验证密钥的方法。它用于从一个身份验证密钥迁移到另一个。有关详细信息，请参阅配置独立于 IP 路由协议的功能中的“管理身份验证密钥”部分。

配置纯文本认证

有两种方法可用于对 RIP 更新进行身份验证，其中之一就是使用纯文本身份验证。可按下表所示的方式进行配置。

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

有关命令的详细信息，请参阅 Cisco IOS IP 命令参考。

配置 MD5认证

MD5 身份验证是一种可选的身份验证模式，由 Cisco 在原始的 RFC 1723 定义的纯文本身份验证基础之上添加而来。 除了额外使用 ip rip authentication mode md5 命令之外，其配置与纯文本身份验证的配置相同。对于 MD5 身份验证方法，用户必须对链路两端的路由器接口都进行配置，确保两端的密钥编号和密钥字符串匹配。

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
```

有关命令的详细信息，请参阅 Cisco IOS 命令参考。

验证

验证纯文本认证

本部分提供的信息用于确认您的配置可以正常发挥作用。

如上所示配置路由器之后，交换的所有路由更新在接收之前都将经过身份验证。通过观察 debug ip rip 和 show ip route 命令的输出可以验证这一点。

注意： 在发出 debug 命令之前，请参阅有关 Debug 命令的重要信息。

```
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
```

使用纯文本身份验证可以防止原本不是要参与本地路由交换进程的路由器发起路由更新，从而改进网络设计。然而，这种身份验证不安全。口令（在本示例中为 234）的交换采用了纯文本形式。这样很容易遭到捕获和利用。正如前文所述，考虑到安全性时，相对于纯文本身份验证，更好的方法是选择 MD5 身份验证。

验证 MD5 认证

如上所示配置 RA 和 RB 路由器之后，交换的所有路由更新在接收之前都将经过身份验证。通过观察 debug ip rip 和 show ip route 命令的输出可以验证这一点。

```
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 身份验证使用单向式 MD5 散列算法，这是一种公认的较强的散列算法。在这种身份验证模式下，路由更新不再出于身份验证目的传输口令。相反，将对口令运行 MD5 算法以生成一则 128 位消息，然后将此消息发送出去以进行身份验证。因此，考虑到 MD5 身份验证更安全，推荐使用这种方法而非纯文本身份验证方法。

故障排除

本部分提供的信息可用于对配置进行故障排除。

故障排除命令

命令输出解释程序工具（仅限注册用户）支持某些 **show** 命令，使用此工具可以查看对 show 命令输出的分析。

debug ip rip 命令可用于在遇到 RIPv2 身份验证相关问题时进行故障排除。

注意： 发出 **debug** 命令之前，请参阅关于 Debug 命令的重要信息。

注意： 下面是一个 debug ip rip 命令输出示例，其中说明的问题是相邻路由器之间要求完全相同的身份验证相关参数实际上并未匹配。这可能导致两个路由器中的某一个或全部都无法在各自的路由表中安装接收到的路由。

```
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)
```

下面的 show ip route 命令输出显示路由器未通过 RIP 获知任何路由：

```
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#
```

注释 1：使用纯文本身份验证模式时，为了成功进行身份验证，请确保相邻路由器上的以下参数互相匹配。

- 密钥字符串
- 身份验证模式

注释 2：使用 MD5 身份验证模式时，为了成功进行身份验证，请确保相邻路由器上的以下参数互相匹配。

- 密钥字符串
- 密钥编号
- 身份验证模式

相关信息

- Routing Information Protocol (RIP) 简介
- 配置 RIP
- 配置独立于 IP 路由协议的功能
- RIP 命令
- Cisco IOS IP 命令参考，第 2 卷（共 4 卷）：路由协议，版本 12.3
- RIP 技术支持页
- IP 路由协议技术支持页
- 技术支持 - Cisco Systems