Configuración de ejemplo para la autenticación en RIPv2

Contenido

Introducción

Este documento muestra configuraciones de ejemplo para la autenticación del proceso de intercambio de información de ruteo para el Protocolo de información de ruteo versión 2 (RIPv2).

La implementación de Cisco de RIPv2 admite dos modos de autenticación: autenticación de texto únicamente y autenticación del Digesto de mensaje 5 (MD5) El modo de autenticación de texto sin formato es la configuración predeterminada en cada paquete RIPv2, cuando se habilita la autenticación. La autenticación de texto sin formato no debe utilizarse cuando la seguridad es un problema, porque la contraseña de autenticación sin cifrar se envía en cada paquete RIPv2.

Nota: RIP versión 1 (RIPv1) no admite autenticación. Si está enviando y recibiendo paquetes RIPv2, puede habilitar la autenticación RIP en una interfaz.

Prerequisites

Requirements

Quienes lean este documento deben tener conocimientos básicos sobre lo siguiente:

- RIPv1 y RIPv2

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware. A partir de la versión del software Cisco IOS® 11.1, se admite RIPv2 y, por lo tanto, todos los comandos que se proporcionan en la configuración se admiten en la versión de software Cisco IOS® 11,1 y posteriores.

La configuración ilustrada en este documento fue probada y actualizada mediante las siguientes versiones de software y hardware:

- Router serie 2500 de Cisco
- Versión de software Cisco IOS 12.3(3)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte Convenciones de Consejos Técnicos de Cisco.

Antecedentes

En la actualidad, la seguridad es una de las principales preocupaciones de los diseñadores de redes. Proteger una red incluye asegurar el intercambio de la información de ruteo entre los routers, así como asegurarse de que la información que ingresa a la tabla de ruteo sea válida y no originada o alterada por alguien que intenta interrumpir la red. Es posible que un atacante intente introducir actualizaciones inválidas para engañar al router para que envíe datos a un destino erróneo o para que baje el rendimiento de la red. Además, las actualizaciones de rutas inválidas pueden terminar en la tabla de ruteo debido a una configuración deficiente (como puede ser no utilizar el comando passive interface en el límite de la red) o al funcionamiento incorrecto de un router. Debido a esto, es prudente autenticar el proceso de actualización de enrutamiento que se ejecuta en un router.

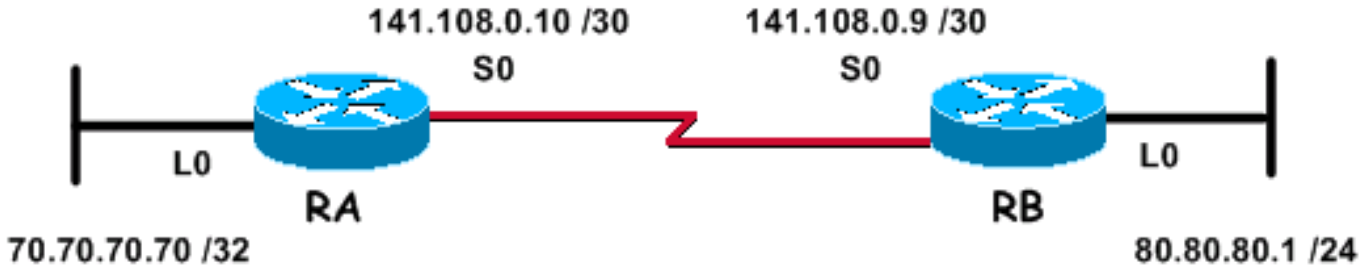
Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Para encontrar información adicional sobre los comandos usados en este documento, utilice la Command Lookup Tool (sólo clientes registrados) .

Diagrama de la red

Este documento utiliza la instalación de red que se muestra en el siguiente diagrama.



La red anterior, que se utiliza para los siguientes ejemplos de configuración, consta de dos routers; el router RA y el RB de router, que ejecutan RIP e intercambian periódicamente las actualizaciones de enrutamiento. Se requiere que este intercambio de información de ruteo sobre un link serial sea autenticada.

Configuraciones

Siga estos pasos para configurar la autenticación en RIPv2:

1. Definir una cadena de claves con un nombre.**Nota:** La cadena de claves determina el conjunto de claves que se pueden utilizar en la interfaz. Si una cadena de claves no está configurada, no se realiza ninguna autenticación en esa interfaz.
2. Defina la clave o las claves en la cadena de claves.
3. Especifique la contraseña o la cadena de clave que se utilizará en la clave.Esta es la cadena de autenticación que se debe enviar y recibir en los paquetes que utilicen el protocolo de enrutamiento que se esta autenticando. (En el ejemplo que se muestra a continuación, el valor de la cadena es 234).
4. Habilite la autenticación en una interfaz y especifique la cadena de claves que se utilizará.Dado que la autenticación se habilita por cada interfaz, se puede configurar un router que ejecute RIPv2 para la autenticación en ciertas interfaces y pueda funcionar sin ninguna autenticación en otras interfaces.
5. Especifique si la interfaz usará texto sin formato o autenticación MD5.La autenticación predeterminada que se utiliza en RIPv2 es la autenticación de texto sin formato cuando la autenticación está habilitada en el paso anterior. Por lo tanto, si utiliza la autenticación de texto sin formato, este paso no es necesario.
6. Configure la administración de claves (este paso es opcional).La administración de claves es un método para controlar las claves de autenticación. Se utiliza para migrar de una clave de autenticación a otra. Para obtener más información, consulte la sección "Administrar claves de autenticación" de Configuración de las funciones independientes del protocolo de enrutamiento IP.

Configuración de autenticación con texto sin formato

Una de las dos maneras en las que se pueden autenticar las actualizaciones de RIP es utilizar la autenticación de texto sin formato. Esto puede configurarse como se indica en las tablas a continuación.

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
```

Para obtener información detallada sobre los comandos, consulte el Material de referencia del comando IP de Cisco IOS.

Configuración de la autenticación MD5

La autenticación MD5 es un modo opcional de autenticación agregado por Cisco a la autenticación de texto sin formato definida por RFC 1723. La configuración es idéntica a la de la autenticación de sólo texto, con excepción del uso del modo md5 de autenticación ip rip del comando adicional. Los usuarios deben configurar las interfaces del router en ambos lados del enlace para el método de autenticación MD5. Para ello, deben asegurarse de que el número de clave y la cadena de clave coincidan en ambos lados.

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
```

Para obtener información detallada sobre los comandos, consulte el Material de referencia del comando IP de Cisco IOS.

Verificación

Verificación de la autenticación de texto únicamente

En esta sección, encontrará información que puede utilizar para confirmar si la configuración funciona adecuadamente.

Al configurar los routers según se indicó anteriormente, todos los intercambios de actualización de ruteo se autenticarán antes de ser aceptados. Esto puede verificarse si observa el resultado de los comandos debug ip rip y **show ip route.**

Nota: Antes de ejecutar un comando **debug**, consulte Información Importante sobre Comandos Debug.

```
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
```

El uso de la autenticación de texto sin formato mejora el diseño de la red, ya que evita que se

agreguen actualizaciones de enrutamiento realizadas por routers que no deben participar del proceso de intercambio de enrutamiento local. Sin embargo, este tipo de autenticación no es segura. La contraseña (234 en este ejemplo) se intercambia en texto sin formato. Se puede capturar fácilmente y luego se pueden obtener las respectivas ventajas. Como se mencionó anteriormente, debe preferirse la autenticación de MD5 en lugar de la autenticación de texto únicamente cuando la seguridad es un problema.

Verificación de la autenticación MD5

Al configurar los routers según se indicó anteriormente, todos los intercambios de actualización de enrutamiento se autenticarán antes de ser aceptados. Esto puede verificarse si observa el resultado de los comandos **debug ip rip y show ip route.**

```
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
```

La autenticación MD5 utiliza el algoritmo de troceo MD5 unidireccional, que es un algoritmo sólido. En este modo de autenticación, la actualización de ruteo no lleva la contraseña para autenticación. En cambio, se envía un mensaje de 128 bits, generado mediante la ejecución del algoritmo MD5 sobre la contraseña, junto con el mensaje para la autenticación. Por lo tanto, se recomienda utilizar la autenticación MD5 en lugar de la autenticación de texto sin formato, ya que es más segura.

Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Comandos para resolución de problemas

La herramienta Output Interpreter (sólo para clientes registrados) permite utilizar algunos comandos “show” y ver un análisis del resultado de estos comandos.

El comando debug ip rip puede utilizarse para solucionar problemas relacionados con la autenticación de RIPv2.

Nota: Antes de ejecutar **comandos debug**, consulte Información Importante sobre Comandos Debug.

Nota: A continuación se muestra un ejemplo de la salida del comando debug ip rip, cuando cualquiera de los parámetros relacionados con la autenticación que necesitan ser idénticos entre los routers vecinos no coincide. Esto puede hacer que uno o ambos routers no instalen las rutas recibidas en su tabla de enrutamiento.

```
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)
```

Este resultado del comando show ip route muestra que el router no está detectando ninguna ruta a través de la RIP:

```
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#
```

Nota 1: Cuando utilice el modo de autenticación de texto sin formato, asegúrese de que los siguientes parámetros coincidan con los routers vecinos para que la autenticación se realice correctamente.

- Cadena de clave
- Modo de autenticación

Nota 2: Al utilizar el modo de autenticación MD5, para que la autenticación tenga éxito, asegúrese de que los siguientes parámetros coincidan con los routers vecinos.

- Cadena de clave
- Número de clave
- Modo de autenticación

Información Relacionada

- Introducción al protocolo de información de enrutamiento (RIP)
- Configuración de RIP
- Configuración de las funciones independientes del protocolo de enrutamiento IP
- Comandos de RIP
- Material de referencia del comando IP de Cisco IOS, Volumen 2 de 4: Protocolos de enrutamiento, versión 12.3
- Página de soporte de la tecnología de RIP
- Página de soporte de la tecnología de protocolos de enrutamiento IP
- Soporte Técnico - Cisco Systems