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 del RIPv2 apoya a dos modos de autenticación: autenticación de texto únicamente y autenticación del Digesto de mensaje 5 (MD5) El modo del autenticación de texto únicamente es la configuración predeterminada en cada paquete del RIPv2, cuando se habilita la autenticación. El autenticación de texto únicamente no debe ser utilizado cuando la Seguridad es un problema, porque la contraseña de autenticación unencrypted se envía en cada paquete del RIPv2.

Nota: La versión de RIP 1 (RIPv1) no soporta la autenticación. Si usted es de envío y de recepción de los paquetes del RIPv2, usted puede habilitar la autenticación del RIP en una interfaz.

prerrequisitos

Requisitos

Los Quien lea este documento deben tener la comprensión básica del 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 de software 11.1 de Cisco IOS®, se soporta el RIPv2 y por lo tanto todos los comandos dados en la configuración se soportan en la versión de software 11.1 de Cisco IOS® y posterior.

La configuración en el documento se prueba y se pone al día usando estas versiones de software y hardware:

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

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 ruteo que se ejecuta en un router.

Configurar

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

Nota: Para obtener información adicional sobre los comandos que se utilizan en este documento, use la Command Lookup Tool (solo para clientes registrados).

Diagrama de la red

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

La red arriba, que se utiliza para los ejemplos de configuración siguientes, consiste en dos Routers; router RA y RB del router, que está ejecutando el RIP y está intercambiando periódicamente las actualizaciones de ruteo. Se requiere que este intercambio de información de ruteo sobre un link serial sea autenticada.

Configuraciones

Realice estos pasos para configurar la autenticación en el RIPv2:

1. Defina un llavero con un nombre.**Nota:** El encadenamiento dominante determina el conjunto de las claves que se pueden utilizar en la interfaz. Si un llavero no se configura, no se realiza ninguna autenticación en esa interfaz.
2. Defina la clave o las claves en el llavero.
3. Especifique la contraseña o la clave-cadena que se utilizarán en la clave.Ésta es la cadena de la autentificación que se debe enviar y recibir en los paquetes usando el Routing Protocol que es autenticado. (En el ejemplo dado abajo, el valor de la cadena es 234.)
4. Habilite la autenticación en una interfaz y especifique el llavero que se utilizará.Puesto que la autenticación se habilita en a por la base de la interfaz, un RIPv2 corriente del router se puede configurar para la autenticación en las ciertas interfaces y puede actuar sin ninguna autenticación en otras interfaces.
5. Especifique si la interfaz utilizará el sólo texto o autenticación de MD5.La autenticación predeterminada usada en el RIPv2 es autenticación de texto únicamente, cuando la autenticación se habilita en el paso anterior. Así pues, si usa el autenticación de texto únicamente, este paso no se requiere.
6. Administración de claves de la configuración (este paso es opcional).La administración de claves es un método de controlar las claves de autenticación. Esto se utiliza para emigrar la clave de autenticación de la forma una a otra. Para más información, refiera a la sección "Administrar claves de autenticación" de configurar las características IP Routing Protocol-Independent.

Configuración de autenticación con texto sin formato

Una de las dos maneras de las cuales el RIP se pone al día se puede autenticar está utilizando el autenticación de texto únicamente. 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 información detallada sobre los comandos, refiera a la referencia del comando ip del 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 a ambos lados del link para autenticación de MD5 el método, aseegurandose la correspondencia de cadenas dominante del número y de la clave en los 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 información detallada sobre los comandos, refiera a la referencia del comando cisco ios.

Verificación

Verificación de la autenticación de texto únicamente

Esta sección proporciona la información para confirmar su configuración está trabajando correctamente.

Al configurar los routers según se indicó anteriormente, todos los intercambios de actualización de ruteo se autenticarán antes de ser aceptados. Esto puede ser verificada observando la salida obtenida del RIP y de los comandos show ip route del IP del debug.

Nota: Antes de ejecutar un comando de depuración, consulte Información importante sobre comandos de depuración.

```
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
```

Usando el autenticación de texto únicamente mejora el diseño de red previniendo la adición de actualizaciones de ruteo originadas por el Routers no significado para participar en el proceso local del intercambio de ruteo. Sin embargo, este tipo de autenticación no es seguro. La contraseña (234 en este ejemplo) se intercambia en el sólo texto. 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

Configurando al Routers RA y del RB como se muestra arriba, todos los intercambios de la actualización de ruteo serán autenticados antes de ser validado. Esto puede ser verificada observando la salida obtenida del RIP y de los comandos show ip route del IP del debug.

```
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. Así, se recomienda para utilizar autenticación de MD5 sobre el autenticación de texto únicamente puesto que es más seguro.

Troubleshooting

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 ser utilizado para resolver problemas los problemas autenticación-relacionados del RIPv2.

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

Nota: Lo que sigue es un ejemplo de la salida del comando debug ip rip, cuando los parámetros autenticación-relacionados uces de los que necesitan ser idénticos entre los routeres de la vencidad no están correspondiendo con. Esto puede dar lugar uno o ambos el Routers que no instala las rutas recibidas en su tabla de ruteo.

```
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)
```

El producto siguiente del comando show ip route muestra que el router no está aprendiendo ninguna rutas vía el 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: Al usar el modo del autenticación de texto únicamente, aseegurese que los parámetros siguientes están correspondiendo con en los routeres de la vencidad para la autenticación satisfactoria.

- Clave-cadena
- Modo de autenticación

Nota 2: Al usar autenticación de MD5 el modo, porque la autenticación satisfactoria aseegurese que los parámetros siguientes están correspondiendo con en los routeres de la vencidad.

- Clave-cadena
- Número dominante
- Modo de autenticación

Información Relacionada

- Introducción al Routing Information Protocol (RIP)
- Configurar el RIP
- Configurar las características de la Protocolo-independiente del Routing IP
- Comandos del RIP
- Referencia del comando ip del Cisco IOS, volumen 2 de 4: Routing Protocol, Release12.3
- Página de soporte de la tecnología del RIP
- Página de soporte de la tecnología de los IP Routing Protocol
- Soporte Técnico - Cisco Systems