Exemplo de configuração para autenticação em RIPv2

Índice

Introdução

Este documento mostra exemplos de configuração para autenticação do processo de troca de informações de roteamento para o RIPv2.

A implementação Cisco do RIPv2 apoia dois modos de autenticação: autenticação de texto simples e autenticação Message Digest 5 (MD5). O modo da autenticação de texto simples é a configuração padrão em cada pacote do RIPv2, quando a autenticação é permitida. A autenticação de texto simples não deve ser usada quando a Segurança é uma edição, porque a senha da autenticação não criptografada está enviada em cada pacote do RIPv2.

Nota: A versão RIP 1 (RIPv1) não apoia a autenticação. Se você é de emissão e de recepção pacotes do RIPv2, você pode permitir a autenticação do RASGO em uma relação.

Pré-requisitos

Requisitos

Os leitores deste documento devem ter a compreensão básica do seguinte:

- RIPv1 e RIPv2

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas. Partindo da versão de software 11.1 de Cisco IOS®, o RIPv2 é apoiado e consequentemente todos os comandos dados na configuração são apoiados na versão de software 11.1 de Cisco IOS® e mais atrasado.

A configuração no documento é testada e utilização actualizada esta versão de software e hardware:

- Cisco 2500 Series Router
- Versão 12.3(3) do Cisco IOS Software

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Informações de Apoio

Atualmente, segurança é uma das principais preocupações dos designers de rede. Proteger uma rede inclui proteger a troca de informações de roteamento entre os roteadores, como garantir que as informações inseridas na tabela de roteamento sejam válidas e não originadas ou violadas por alguém tentando corromper a rede. Um atacante pode tentar introduzir atualizações inválidas para enganar o roteador, fazendo com que ele envie dados para o destino errado, ou degradar gravemente o desempenho da rede. Além disso, atualizações de rota inválida podem acabar na tabela de roteamento devido à configuração insatisfatória (como, por exemplo, sem usar o comando de interface passiva no limite de rede) ou ao mau funcionamento do roteador. Devido a isto é prudente autenticar o processo de atualização de roteamento que é executado em um roteador.

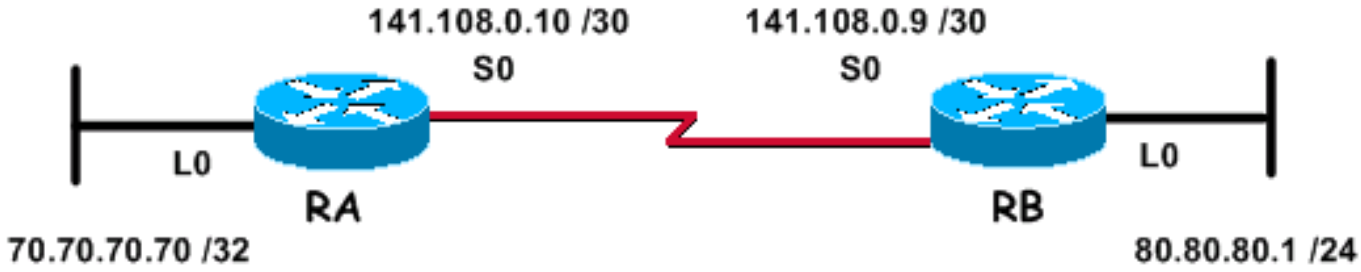
Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Para localizar informações adicionais sobre os comandos usados neste documento, utilize a Ferramenta Command Lookup (somente clientes registrados).

Diagrama de Rede

Este documento utiliza a instalação de rede mostrada no diagrama abaixo.



A rede acima, que é usada para os seguintes exemplos de configuração, consiste em dois Roteadores; RB do roteador em e do roteador, ambo está executando o RASGO e periodicamente as atualizações de roteamento de troca. É necessário que essa troca de informações de roteamento pelo enlace serial seja autenticada.

Configurações

Realize estas etapas para configurar a autenticação no RIPv2:

1. Defina uma porta-chaves com um nome.**Nota:** A porta-chaves determina o grupo de chaves que podem ser usadas na relação. Se uma porta-chaves não é configurada, nenhuma autenticação está executada nessa relação.
2. Defina a chave ou as chaves na porta-chaves.
3. Especifique a senha ou a chave-corda a ser usadas na chave.Este é o string de autenticação que deve ser enviado e recebido nos pacotes usando o protocolo de roteamento que está sendo autenticado. (No exemplo dado abaixo, o valor da corda é 234.)
4. Permita a autenticação em uma relação e especifique a porta-chaves a ser usada.Desde que a autenticação é permitida na pela base da relação, um RIPv2 running do roteador pode ser configurado para a autenticação em determinadas interfaces e pode operar-se sem nenhuma autenticação em outras relações.
5. Especifique se a relação usará o texto simples ou a autenticação md5.A autenticação padrão usada no RIPv2 é autenticação de texto simples, quando a autenticação é permitida na etapa precedente. Assim, se usando a autenticação de texto simples, esta etapa não é exigida.
6. Configurar o gerenciamento chave (esta etapa é opcional).O gerenciamento chave é um método de controlar chaves de autenticação. Isto é usado para migrar a chave de autenticação do formulário um a outro. Para mais informação, refira a seção " chaves de autenticação de gerenciamento " de configurar características independentes do protocolo de IP Routing.

Configurando uma autenticação de texto simples

Uma das duas maneiras em que o RASGO atualiza pode ser autenticado está usando a autenticação de texto simples. Isso pode ser configurado como mostrado nas tabelas abaixo.

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 informações detalhadas sobre dos comandos, refira a referência do comando ip do Cisco IOS.

Configurando a autenticação MD5

A autenticação MD5 é um modo de autenticação opcional adicionado pela autenticação de texto sem formatação definido pelo RFC 1723 original da Cisco. A configuração é idêntica à da autenticação de texto simples, exceto pelo uso do comando adicional ip rip authentication mode md5. Os usuários devem configurar interfaces do roteador em ambos os lados do link para o método de autenticação md5, certificando-se da série de compatibilidade chave do número e da chave em ambos os 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 informações detalhadas sobre dos comandos, refira a referência do comando cisco ios.

Verificar

Verificando a autenticação do texto simples

Esta seção fornece a informação para confirmar sua configuração está trabalhando corretamente.

Ao configurar os roteadores da forma que foi exibido acima, todos os intercâmbios de atualização de roteamento serão autenticados antes de serem aceitos. Isto pode ser verificado observando a saída obtida do rasgo e dos comandos show ip route debugar IP.

Nota: Antes de emitir comandos de depuração, consulte as informações importantes sobre eles.

```
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
```

Usar a autenticação de texto simples melhora o projeto de rede impedindo a adição de atualizações de roteamento originadas pelo Roteadores não significado participar no processo local do intercâmbio de roteamento. Contudo, este tipo de autenticação não é seguro. A senha (234 neste exemplo) é trocada no texto simples. Ela pode ser capturada facilmente e, então, explorada. Como já mencionado, a autenticação MD5 tem preferência sobre a autenticação de texto simples, quando há problemas com a segurança.

Verificando a autenticação MD5

Configurando o Roteadores RA e de RB como mostrado acima, todas as trocas da atualização de roteamento serão autenticadas antes de ser aceitada. Isto pode ser verificado observando a saída obtida do rasgo e dos comandos show ip route debugar IP.

```
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
```

A autenticação MD5 usa o algoritmo de hash MD5 unidirecional, reconhecido como um algoritmo de hash forte. Nesse modo de autenticação, a atualização de roteamento não transporta a senha para fins de autenticação. Em vez disso, uma mensagem de 128 bits, gerada pela execução do algoritmo MD5 na senha, e a mensagem são enviadas juntamente com a autenticação. Assim, recomenda-se usar a autenticação md5 sobre a autenticação de texto simples desde que é mais seguro.

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Comandos para Troubleshooting

A Output Interpreter Tool (somente clientes registrados) oferece suporte a determinados

comandos show, o que permite exibir uma análise da saída do comando show.

O comando debug ip rip pode ser usado para pesquisar defeitos problemas autenticação-relacionados do RIPv2.

Nota: Antes de emitir comandos debug, consulte Informações importantes sobre comandos debug.

Nota: Seguir é um exemplo da saída do comando debug ip rip, quando alguns dos parâmetros autenticação-relacionados que precisam de ser idênticos entre os roteadores vizinho não estão combinando. Isto pode conduzir a um ou ambo o Roteadores que não instala as rotas recebidas em sua tabela de roteamento.

```
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)
```

A seguinte saída do comando show ip route mostra que o roteador não está aprendendo nenhuma rotas através do RASGO:

```
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: Ao usar o modo da autenticação de texto simples, certifique-se de que os seguintes parâmetros estão combinando em roteadores vizinho para a autenticação bem sucedida.

- Chave-corda
- Modo de autenticação

Nota 2: Ao usar o modo da autenticação md5, porque a autenticação bem sucedida certifique-se de que os seguintes parâmetros estão combinando em roteadores vizinho.

- Chave-corda
- Número chave
- Modo de autenticação

Informações Relacionadas

- Introdução ao Routing Information Protocol (RIP)
- Configurando o RASGO
- Configurando características Protocolo-independentes de Roteamento IP
- Comandos do RASGO
- Referência do comando ip do Cisco IOS, volume 2 de 4: Protocolos de roteamento, Versão 12.3
- Página de suporte de tecnologia do RASGO
- Página de suporte de tecnologia dos protocolos de IP Routing
- Suporte Técnico - Cisco Systems