Exemple de configuration de l'authentification en RIPv2

Contenu

Introduction

Ce document affiche des exemples de configurations pour authentifier le processus d'échange des informations de routage pour la version 2 du Protocole d'Information de Routage (RIPv2).

La mise en œuvre de RIPv2 de Cisco prend en charge deux modes d’authentification : l’authentification en texte brut et l’authentification MD5 (Message Digest 5). Le mode d’authentification en texte brut est le paramètre par défaut dans chaque paquet RIPv2, lorsque l’authentification est activée. L’authentification en texte brut ne doit pas être utilisée lorsque la sécurité est importante, car le mot de passe d’authentification non chiffré est envoyé dans chaque paquet RIPv2.

Remarque : RIP version 1 (RIPv1) ne prend pas en charge l'authentification. Si vous envoyez ou recevez des paquets RIPv2, vous pouvez activer l’authentification RIP sur une interface.

Conditions préalables

Conditions requises

Si vous lisez ce document, vous devez avoir des connaissances de base des éléments suivants :

- protocoles RIPv1 et RIPv2

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques. À partir de la version 11.1 du logiciel Cisco IOS®, RIPv2 est pris en charge et, par conséquent, toutes les commandes fournies dans la configuration sont prises en charge sur le logiciel Cisco IOS® de la version 11.1 et des versions ultérieures.

La configuration dans le présent document est testée et mise à jour à l'aide des versions logicielles et matérielles suivantes :

- Routeur de la gamme 2500 de Cisco
- Logiciel Cisco IOS, version 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.

Conventions

Pour plus d'informations sur les conventions des documents, référez-vous aux Conventions utilisées pour les conseils techniques de Cisco.

Informations générales

De nos jours, la sécurité est l'une des préoccupations principales des concepteurs de réseau. La sécurisation d'un réseau consiste à sécuriser l'échange d'information de routage entre les routeurs, par exemple en s'assurant que l'information entrée dans la table de routage est valide et qu'elle ne provient pas, ni n'a été falsifiée par une personne tentant de perturber le réseau. Un agresseur peut essayer d'introduire des mises à jour non valides pour amener le routeur à envoyer des données à une destination incorrecte ou à gravement détériorer la performance du réseau. De plus, des mises à jour de routage non valides peuvent se retrouver dans la table de routage en raison d'une mauvaise configuration (par exemple en n'utilisant pas la commande **passive interface sur la limite du réseau) ou en raison d'un routeur défectueux.** Pour cette raison, il est prudent d'authentifier le processus de mise à jour de routage exécuté sur un routeur.

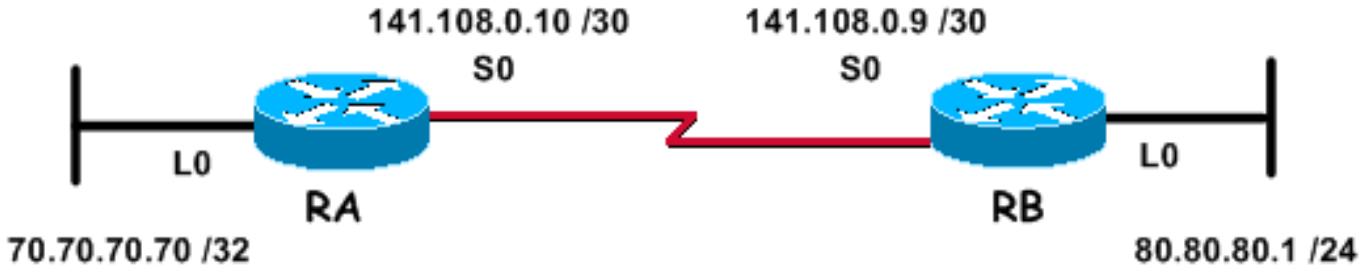
Configuration

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque : Pour en savoir plus sur les commandes utilisées dans le présent document, utilisez l'outil de recherche de commandes (clients inscrits seulement).

Diagramme du réseau

Ce document utilise la configuration réseau indiquée dans le diagramme suivant :



Le réseau ci-dessus, utilisé pour les exemples de configuration qui suivent, est composé de deux routeurs, le routeur RA et le routeur RB qui exécutent tous deux le protocole RIP et qui échangent régulièrement des mises à jour de routage. Il est nécessaire que cet échange d'information de routage sur la liaison série soit authentifié.

Configurations

Suivez ces étapes pour configurer l'authentification dans RIPv2 :

1. Définissez un trousseau de clés avec un nom.**Remarque :** La chaîne de clés détermine le jeu de clés qui peut être utilisé sur l'interface. Si un trousseau de clés n'est pas configuré, aucune authentification n'est effectuée sur cette interface.
2. Définissez la ou les clés du trousseau.
3. Spécifiez le mot de passe ou la chaîne clé à utiliser dans la clé.Celle-ci est la chaîne d'authentification qui doit être envoyée et reçue dans les paquets utilisant le protocole de routage qui sont authentifiés. (Dans l'exemple ci-dessous, la valeur de la chaîne est 234.)
4. Activez l'authentification sur une interface et spécifiez le trousseau de clés à utiliser.Comme l'activation de l'authentification se fait par interface, un routeur exécutant RIPv2 peut être configuré pour l'authentification sur certaines interfaces et peut fonctionner sans authentification sur d'autres.
5. Indiquez si l'interface doit utiliser l'authentification MD5 ou en texte brut.L'authentification par défaut utilisée dans RIPv2 est celle en texte brut quand celle-ci est activée comme à l'étape précédente. Par conséquent, si vous utilisez l'authentification en texte brut, cette étape n'est pas nécessaire.
6. Configurez la gestion des clés (cette étape est facultative).La gestion des clés est une méthode de contrôle des clés d'authentification. Cette méthode permet de passer d'une clé d'authentification à une autre. Pour plus d'information, consultez la section « Gestion des clés d'authentification » du document Configuration des fonctionnalités indépendantes du protocole de routage IP.

Configuration de l'authentification en texte brut

L'authentification en texte brut est l'une des deux façons par lesquelles les mises à jour du protocole RIP peuvent être authentifiées. Elle peut être configurée comme indiqué dans les tableaux ci-dessous.

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
```

Pour obtenir de l'information détaillée sur les commandes, consultez le document Référence des commandes IP de Cisco IOS.

Configuration de l'authentification MD5

L'authentification MD5 est un mode d'authentification facultatif ajouté par Cisco à l'authentification en texte brut définie par le RFC 1723 . La configuration est identique à celle de l'authentification

en texte brut, à l'exception de l'utilisation de la commande supplémentaire **ip rip authentication mode md5**. Les utilisateurs doivent configurer les interfaces de routeur de part et d'autre de la liaison pour la méthode d'authentification MD5, en s'assurant que le numéro de clé et la chaîne clé correspondent de part et d'autre.

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
```

Pour obtenir de l'information détaillée sur les commandes, consultez le document Référence des commandes de Cisco IOS.

Vérification

Vérification de l'authentification en texte brut

Cette section fournit l'information qui vous permet de confirmer que votre configuration fonctionne correctement.

En configurant les routeurs comme indiqué ci-dessus, tous les échanges de mises à jour de routage seront authentifiés avant d'être acceptés. Ceci peut être vérifié en observant la sortie obtenue des commandes debug ip rip et **show ip route**.

Remarque : avant d'émettre des commandes **debug**, reportez-vous à Informations importantes sur les commandes de débogage.

```
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
```

L'authentification en texte brut améliore la conception du réseau en empêchant l'ajout de mises à jour de routage provenant de routeurs qui ne sont pas censés participer au processus d'échange de routage local. Toutefois, ce type d'authentification n'est pas sécurisé. Le mot de passe (234 dans cet exemple) est échangé en texte brut. Il peut facilement être capturé, puis exploité.

Comme mentionné précédemment, l'authentification MD5 doit être préférée à l'authentification en texte brut lorsque la sécurité est une question importante.

Vérification de l'authentification MD5

En configurant les routeurs RA et RB comme indiqué ci-dessus, tous les échanges de mises à jour de routage seront authentifiés avant d'être acceptés. Ceci peut être vérifié en observant la sortie obtenue des commandes debug ip rip et **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
```

L'authentification MD5 utilise l'algorithme de hachage MD5 unidirectionnel qui est reconnu comme un algorithme de hachage puissant. Dans ce mode d'authentification, la mise à jour de routage ne contient pas le mot de passe aux fins d'authentification. Au lieu de cela, un message de 128 bits, généré en exécutant l'algorithme MD5 sur le mot de passe, et le message sont envoyés pour effectuer l'authentification. Par conséquent, il est recommandé d'utiliser l'authentification MD5 plutôt que l'authentification en texte brut, car elle est plus sécurisée.

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Dépannage des commandes

Certaines commandes **show** sont prises en charge par l'Output Interpreter Tool (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

La commande debug ip rip peut être utilisée pour dépanner les problèmes liés à l'authentification RIPv2.

Remarque : avant d'émettre des commandes **debug**, consultez Informations importantes sur les commandes de débogage.

Remarque : Voici un exemple de la sortie de la commande debug ip rip, lorsque aucun des paramètres liés à l'authentification qui doivent être identiques entre les routeurs voisins ne correspond. Dans ce cas, il possible que des routes reçues ne soient pas installées dans la table de routage d'un routeur ou des deux.

```
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)
```

Le résultat suivant de la commande show ip route montre que le routeur n'apprend pas de routes par 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#
```

Remarque 1 : Lorsque vous utilisez le mode d'authentification en texte brut, assurez-vous que les paramètres suivants sont identiques dans les routeurs voisins pour réussir l'authentification.

- Chaîne clé
- Mode d'authentification

Remarque 2 : Lorsque vous utilisez le mode d'authentification MD5, assurez-vous que les

paramètres suivants sont identiques dans les routeurs voisins pour réussir l'authentification.

- Chaîne clé
- Numéro de clé
- Mode d'authentification

Informations connexes

- Présentation du protocole RIP (Routing Information Protocol)
- Configuration du protocole RIP
- Configuration des fonctionnalités indépendantes du protocole de routage IP
- Commandes du protocole RIP
- Référence des commandes IP de Cisco IOS, volume 2 de 4 : Protocoles de routage, version 12.3
- Page d'assistance de la technologie RIP
- Page d'assistance de la technologie des protocoles de routage IP
- Support technique - Cisco Systems