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).

L'implémentation de Cisco de RIPv2 prend en charge deux modes de l'authentification : authentification en texte brut et authentification de Message Digest 5 (MD5). Le mode d'authentification en texte brut est la valeur par défaut en chaque paquet RIPv2, quand l'authentification est activée. L'authentification en texte brut ne devrait pas être utilisée quand la Sécurité est une question, parce que le mot de passe d'authentification décrypté est introduit chaque paquet RIPv2.

Remarque: La version RIP 1 (RIPv1) ne prend en charge pas l'authentification. Si vous êtes envoyant et recevant les paquets RIPv2, vous pouvez activer l'authentification de RIP sur une interface.

Conditions préalables

Conditions requises

Les lecteurs de ce document devraient avoir la compréhension de base de ce qui suit :

- RIPv1 et RIPv2

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques. À partir de la version de logiciel 11.1 de Cisco IOS®, RIPv2 est pris en charge et donc toutes les instructions données dans la configuration sont prises en charge sur la version de logiciel 11.1 de Cisco IOS® et plus tard.

La configuration dans le document est testée et mise à jour utilisant des ces le logiciel et les versions de matériel :

- Routeur de gamme Cisco 2500
- Version de logiciel de Cisco IOS 12.3(3)

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

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

Informations générales

La Sécurité est l'une des principales préoccupations des créateurs de réseau aujourd'hui. Sécurisant un réseau inclut sécuriser l'échange des informations de routage entre les Routeurs, tels que s'assurer que l'information saisie dans la table de routage est valide et non d'origine ou trifouillée par quelqu'un qui essaye de perturber le réseau. Un attaquant pourrait essayer d'introduire les mises à jour non valides pour duper le routeur dans envoyer des données à la destination fausse, ou pour dégrader sérieusement des performances du réseau. En outre, les mises à jour de route non valides pourraient finir par dans la table de routage due à la mauvaise configuration (comme pas utilisant la **commande d'interface passive** sur la limite du réseau), ou due à un routeur de défaut de fonctionnement. Pour cette raison il est prudent d'authentifier le processus exécuté de mise à jour de routage sur un routeur.

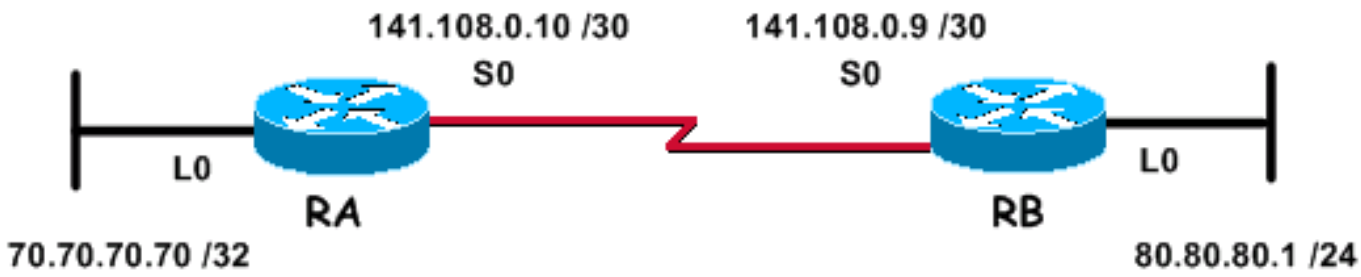
Configurez

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

Remarque: Pour obtenir des informations supplémentaires sur les commandes utilisées dans ce document, utilisez l'Outil de recherche de commande (clients enregistrés seulement).

Diagramme du réseau

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



Le réseau ci-dessus, qui est utilisé pour les exemples suivants de configuration, se compose de deux Routeurs ; RA de routeur et RB de routeur, qui exécutent le RIP et permutent périodiquement des mises à jour de routage. On l'exige que cet échange des informations de routage au-dessus de la liaison série soit authentifié.

Configurations

Effectuez ces étapes pour configurer l'authentification dans RIPv2 :

1. Définissez une chaîne de clés avec un nom.**Remarque:** La chaîne de clés détermine l'ensemble de clés qui peuvent être utilisées sur l'interface. Si une chaîne de clés n'est pas configurée, aucune authentification n'est exécutée sur cette interface.
2. Définissez la clé ou les clés sur la chaîne de clés.
3. Spécifiez le mot de passe ou le key-string à utiliser dans la clé.C'est la chaîne d'authentification qui doit être envoyée et reçue dans les paquets utilisant le protocole de routage étant authentifié. (Dans l'exemple donné ci-dessous, la valeur de la chaîne est 234.)
4. Activez l'authentification sur une interface et spécifiez la chaîne de clés à utiliser.Puisque l'authentification est activée sur a par base d'interface, un routeur exécutant RIPv2 peut être configuré pour l'authentification sur certaines interfaces et peut opérer sans n'importe quelle authentification sur d'autres interfaces.
5. Spécifiez si l'interface utilisera le texte brut ou l'authentification de MD5.L'authentification par défaut utilisée dans RIPv2 est authentification en texte brut, quand l'authentification est activée dans l'étape précédente. Ainsi, si utilisant l'authentification en texte brut, cette étape n'est pas exigée.
6. Configurez la gestion des clés (cette étape est facultative).La gestion des clés est une méthode de contrôler des clés d'authentification. Ceci est utilisé pour migrer la clé d'authentification de la forme une à l'autre. Le pour en savoir plus, se rapportent à la section « gèrent d'authentification clés » de configurer des caractéristiques de Protocol-indépendant de Routage IP.

Configurer l'authentification en texte brut

Une des deux manières dans lesquelles le RIP met à jour peut être authentifiée utilise l'authentification en texte brut. Ceci peut être configuré suivant les indications des tables 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 des informations détaillées sur les commandes, référez-vous à la référence de commandes IP de Cisco IOS.

Configurer l'authentification de MD5

L'authentification de MD5 est une authentication mode facultative ajoutée par Cisco à l'authentification en texte brut RFC 1723-defined d'original. La configuration est identique à celle pour l'authentification en texte brut, excepté l'utilisation du **MD5** supplémentaire d'**ip rip authentication mode de** commande. Les utilisateurs doivent configurer des interfaces de routeur des deux côtés du lien pour la méthode d'authentification de MD5, veillant le nombre et la correspondance principaux de chaîne de clé des deux côtés.

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 des informations détaillées sur les commandes, référez-vous à la référence de commande Cisco IOS.

Vérifiez

Vérifier l'authentification en texte brut

Cette section fournit des informations pour confirmer votre configuration fonctionne correctement.

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

Remarque: Avant d'émettre des commandes de **débogage**, référez-vous aux informations importantes sur des commandes de 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
```

Utilisant l'authentification en texte brut améliore la conception de réseaux en empêchant l'ajout des mises à jour de routage lancées par des Routeurs non censés pour participer au processus d'échange local de routage. Cependant, ce type d'authentification n'est pas sécurisé. Le mot de passe (234 dans cet exemple) est permuté en texte brut. Il peut être capturé facilement et être ainsi exploité. Comme indiqué précédemment, l'authentification de MD5 doit être préférée au-dessus de l'authentification en texte brut quand la Sécurité est une question.

Vérifier l'authentification de MD5

En configurant les Routeurs de RA et de RB comme affichés ci-dessus, tous les échanges de mise à jour de routage seront authentifiés avant d'être reçu. Ceci peut être vérifié en observant la sortie obtenue du **debug ip rip** et des commandes de **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 de MD5 utilise l'one-way, algorithme de hachage de MD5, reconnu pour être un algorithme de hachage fort. En ce mode de l'authentification, la mise à jour de routage ne porte pas le mot de passe afin de l'authentification. En revanche, un message 128-bit, généré en exécutant l'algorithme de MD5 sur le mot de passe, et le message sont envoyés le long pour l'authentification. Ainsi, il est recommandé pour utiliser l'authentification de MD5 au-dessus de l'authentification en texte brut puisqu'il est plus sécurisé.

Dépannez

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 de **debug ip rip** peut être utilisée pour dépannage des problèmes RIPv2 liés à l'authentification.

Remarque: Avant d'émettre des commandes **Debug**, référez-vous à Informations importantes sur les commandes Debug.

Remarque: Être suit un exemple de la sortie de commande de **debug ip rip**, quand les paramètres liés à l'authentification l'uns des qui doivent être identiques entre les routeurs voisins ne s'assortit pas. Ceci peut avoir comme conséquence either one or both les Routeurs n'installant pas les artères reçues dans leur table de routage.

```
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)
```

La sortie suivante de la commande de **show ip route** prouve que le routeur n'apprend aucune artère par l'intermédiaire du 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#
```

Note 1 : En utilisant le mode d'authentification en texte brut, assurez-vous que les paramètres suivants s'assortissent sur des routeurs voisins pour l'authentification réussie.

- Key-string
- Authentication mode

Note 2 : En utilisant l'authentication mode de MD5, parce que l'authentification réussie assurez-vous que les paramètres suivants s'assortissent sur des routeurs voisins.

- Key-string
- Nombre principal
- Authentication mode

Informations connexes

- Introduction au Protocole RIP (Routing Information Protocol)
- Configurer le RIP
- Configurer des caractéristiques de Protocole-indépendant de Routage IP
- Commandes de RIP
- Référence de commandes IP de Cisco IOS, volume 2 de 4 : Protocoles de routage, version 12.3
- Page de support technologique de RIP

- Page de support technologique de protocoles de Routage IP
- Support technique - Cisco Systems