Exemple de configuration de l'authentification des messages EIGRP

Contenu

Introduction

Ce document montre comment ajouter l'authentification de message à vos routeurs d'Enhanced Interior Gateway Routing Protocol (EIGRP) et protéger la table de routage contre la corruption intentionnelle ou accidentelle.

L'ajout de l'authentification aux messages EIGRP de vos routeurs garantit que vos routeurs acceptent uniquement les messages de routage provenant d'autres routeurs qui connaissent la même clé pré-partagée. Sans cette authentification configurée, si quelqu'un introduit un autre routeur avec des informations de route différentes ou conflictuelles sur le réseau, les tables de routage de vos routeurs pourraient devenir corrompues et une attaque par déni de service pourrait s'ensuivre. Ainsi, lorsque vous ajoutez l'authentification aux messages EIGRP envoyés entre vos routeurs, cela empêche quelqu'un d'ajouter volontairement ou accidentellement un autre routeur au réseau et pose un problème.

Attention : lorsque l'authentification des messages EIGRP est ajoutée à l'interface d'un routeur, ce dernier cesse de recevoir des messages de routage de ses homologues jusqu'à ce qu'ils soient également configurés pour l'authentification des messages. Cela **interrompt** les communications de routage sur votre réseau. Reportez-vous à Messages lorsque seule Dallas est configurée pour

plus d'informations.

Conditions préalables

Conditions requises

- L'heure doit être correctement configurée sur tous les routeurs. Référez-vous à Configuration de NTP pour plus d'informations.
- Une configuration EIGRP fonctionnelle est recommandée.

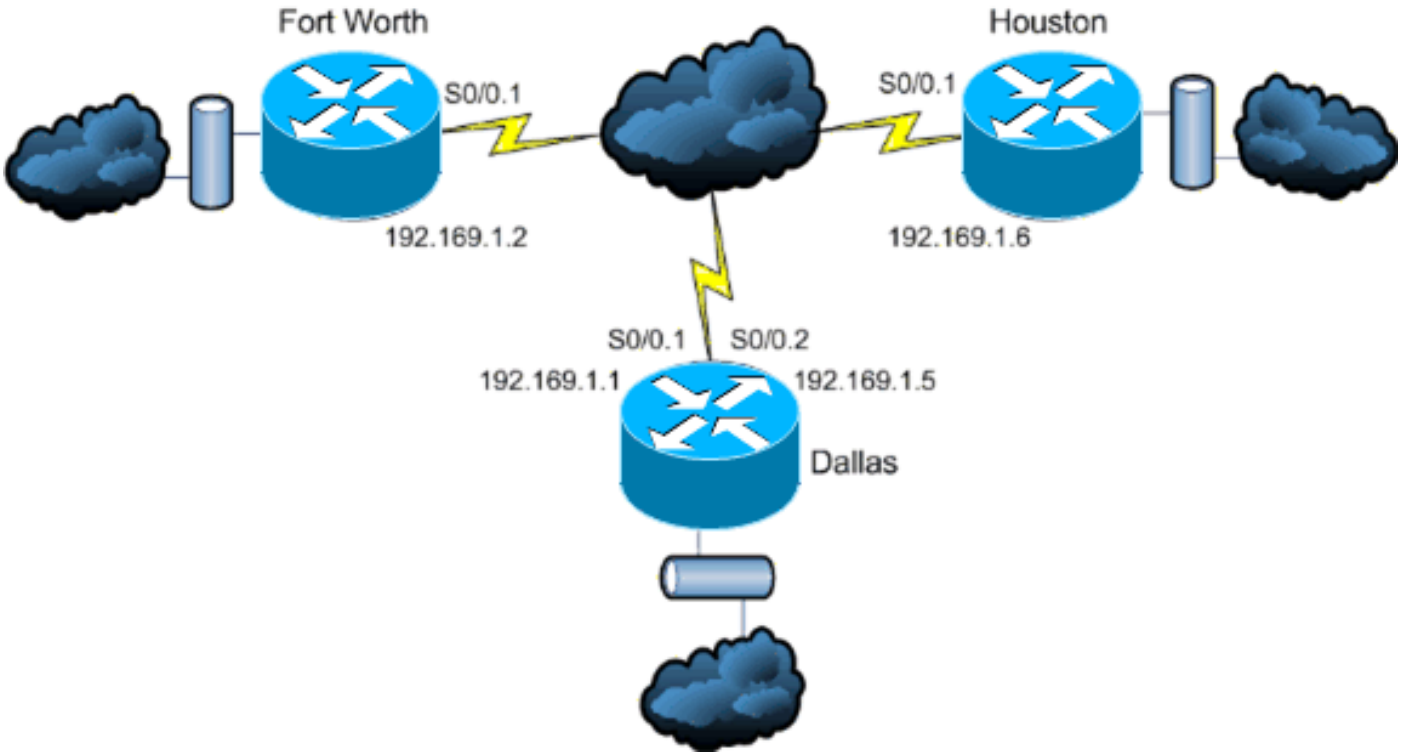
Components Used

Les informations de ce document sont basées sur le logiciel Cisco IOS® Version 11.2 et ultérieure.

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.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

Dans ce scénario, un administrateur réseau souhaite configurer l'authentification des messages EIGRP entre le routeur concentrateur de Dallas et les sites distants de Fort Worth et Houston. La configuration EIGRP (sans authentification) est déjà terminée sur les trois routeurs. Cet exemple de résultat provient de Dallas :

```
Dallas#show ip eigrp neighbors
IP-EIGRP neighbors for process 10
H   Address                 Interface   Hold Uptime   SRTT   RTO  Q  Seq Type
                                        (sec)         (ms)       Cnt Num
1   192.169.1.6             Se0/0.2       11 15:59:57   44   264  0  2
0   192.169.1.2             Se0/0.1       12 16:00:40   38   228  0  3
Dallas#show cdp neigh
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
Houston          Ser 0/0.2          146          R        2611      Ser 0/0.1
FortWorth        Ser 0/0.1          160          R        2612      Ser 0/0.1
```

Configuration de l'authentification des messages EIGRP

La configuration de l'authentification des messages EIGRP se compose de deux étapes :

1. Création d'une chaîne de clés et d'une clé.
2. Configuration de l'authentification EIGRP pour utiliser cette chaîne de clés et cette clé.

Cette section illustre les étapes de configuration de l'authentification des messages EIGRP sur le routeur Dallas, puis sur les routeurs Fort Worth et Houston.

Créer une chaîne de clés sur Dallas

L'authentification de routage repose sur une clé d'une chaîne de clés pour fonctionner. Avant d'activer l'authentification, une chaîne de clés et au moins une clé doivent être créées.

1. Entrez le mode de configuration globale .
   ```
   Dallas#configure terminal
   ```
2. Créez la chaîne de clés. **MYCHAIN** est utilisé dans cet exemple.
   ```
   Dallas(config)#key chain MYCHAIN
   ```
3. Spécifiez le numéro de clé. **1** est utilisé dans cet exemple.**Remarque :** il est recommandé que le numéro de clé soit le même sur tous les routeurs impliqués dans la configuration.
   ```
   Dallas(config-keychain)#key 1
   ```
4. Spécifiez la chaîne de clé de la clé. **securetraffic** est utilisé dans cet exemple.
   ```
   Dallas(config-keychain-key)#key-string securetraffic
   ```
5. Mettre fin à la configuration.
   ```
   Dallas(config-keychain-key)#end
   Dallas#
   ```

Configuration de l'authentification sur Dallas

Une fois que vous avez créé une chaîne de clés et une clé, vous devez configurer le protocole

EIGRP pour effectuer l'authentification des messages avec la clé. Cette configuration est terminée sur les interfaces sur lesquelles le protocole EIGRP est configuré.

Attention : Lorsque l'authentification des messages EIGRP est ajoutée aux interfaces Dallas, elle arrête de recevoir des messages de routage de ses homologues jusqu'à ce qu'ils soient également configurés pour l'authentification des messages. Cela **interrompt** les communications de routage sur votre réseau. Reportez-vous à Messages lorsque seule Dallas est configurée pour plus d'informations.

1. Entrez le mode de configuration globale .
   ```
   Dallas#configure terminal
   ```

2. Àpartir du mode de configuration globale, spécifiez l'interface sur laquelle vous voulez configurer l'authentification des messages EIGRP. Dans cet exemple, la première interface est **Serial 0/0.1**.
   ```
   Dallas(config)#interface serial 0/0.1
   ```

3. Activez l'authentification des messages EIGRP. Le **10** utilisé ici est le numéro de système autonome du réseau. **md5** indique que le hachage md5 doit être utilisé pour l'authentification.
   ```
   Dallas(config-subif)#ip authentication mode eigrp 10 md5
   ```

4. Spécifiez la chaîne de clés à utiliser pour l'authentification. **10** est le numéro de système autonome. **MYCHAIN** est la chaîne de clés créée dans la section Créer une chaîne de clés.
   ```
   Dallas(config-subif)#ip authentication key-chain eigrp 10 MYCHAIN
   Dallas(config-subif)#end
   ```

5. Effectuez la même configuration sur l'interface Serial 0/0.2.
   ```
   Dallas#configure terminal
   Dallas(config)#interface serial 0/0.2
   Dallas(config-subif)#ip authentication mode eigrp 10 md5
   Dallas(config-subif)#ip authentication key-chain eigrp 10 MYCHAIN
   Dallas(config-subif)#end
   Dallas#
   ```

Configurer Fort Worth

Cette section présente les commandes nécessaires à la configuration de l'authentification des messages EIGRP sur le routeur Fort Worth. Pour plus d'informations sur les commandes présentées ici, consultez Créer une chaîne de clés sur Dallas et Configurer l'authentification sur Dallas.

```
FortWorth#configure terminal
FortWorth(config)#key chain MYCHAIN
FortWorth(config-keychain)#key 1
FortWort(config-keychain-key)#key-string securetraffic
FortWort(config-keychain-key)#end
FortWorth#
Fort Worth#configure terminal
FortWorth(config)#interface serial 0/0.1
FortWorth(config-subif)#ip authentication mode eigrp 10 md5
FortWorth(config-subif)#ip authentication key-chain eigrp 10 MYCHAIN
FortWorth(config-subif)#end
FortWorth#
```

Configurer Houston

Cette section présente les commandes nécessaires à la configuration de l'authentification des messages EIGRP sur le routeur Houston. Pour plus d'informations sur les commandes présentées ici, consultez Créer une chaîne de clés sur Dallas et Configurer l'authentification sur Dallas.

```
Houston#configure terminal
Houston(config)#key chain MYCHAIN
Houston(config-keychain)#key 1
Houston(config-keychain-key)#key-string securetraffic
Houston(config-keychain-key)#end
Houston#
Houston#configure terminal
Houston(config)#interface serial 0/0.1
Houston(config-subif)#ip authentication mode eigrp 10 md5
Houston(config-subif)#ip authentication key-chain eigrp 10 MYCHAIN
Houston(config-subif)#end
Houston#
```

Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

Remarque : Consulter les renseignements importants sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

Messages lorsque seule Dallas est configurée

Une fois que l'authentification des messages EIGRP est configurée sur le routeur Dallas, ce routeur commence à rejeter les messages des routeurs Fort Worth et Houston, car ils n'ont pas encore configuré l'authentification. Ceci peut être vérifié en émettant une commande **debug eigrp packets** sur le routeur Dallas :

```
Dallas#debug eigrp packets
17:43:43: EIGRP: ignored packet from 192.169.1.2 (invalid authentication)
17:43:45: EIGRP: ignored packet from 192.169.1.6 (invalid authentication)
!--- Packets from Fort Worth and Houston are ignored because they are !--- not yet configured
for authentication.
```

Messages lors de la configuration de tous les routeurs

Une fois l'authentification des messages EIGRP configurée sur les trois routeurs, ils commencent à échanger à nouveau des messages EIGRP. Ceci peut être vérifié en émettant une nouvelle commande **debug eigrp packets**. Cette fois, les sorties des routeurs Fort Worth et Houston sont affichées :

```
FortWorth#debug eigrp packets
00:47:04: EIGRP: received packet with MD5 authentication, key id = 1
00:47:04: EIGRP: Received HELLO on Serial0/0.1 nbr 192.169.1.1
!--- Packets from Dallas with MD5 authentication are received.

Houston#debug eigrp packets
 00:12:50.751: EIGRP: received packet with MD5 authentication, key id = 1
 00:12:50.751: EIGRP: Received HELLO on Serial0/0.1 nbr 192.169.1.5
!--- Packets from Dallas with MD5 authentication are received.
```

Dépannage

Liaison unidirectionnelle

Vous devez configurer les temporisateurs Hello et de temps d'attente EIGRP aux deux extrémités. Si vous ne configurez les compteurs qu'à une extrémité, une liaison unidirectionnelle se produit.

Un routeur sur une liaison unidirectionnelle peut être en mesure de recevoir des paquets Hello. Cependant, les paquets Hello envoyés ne sont pas reçus à l'autre extrémité. Cette liaison unidirectionnelle est généralement indiquée par des messages *de limite de tentative dépassée* à une extrémité.

Afin d'afficher les messages de *limite de tentative dépassée*, utilisez les commandes **debug eigrp packet** et **debug ip eigrp notifications**.

Informations connexes

- Prise en charge de la technologie EIGRP (Enhanced Interior Gateway Routing Protocol)
- Support et documentation techniques - Cisco Systems