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 s'assure que vos Routeurs reçoivent seulement des messages de routage d'autres Routeurs qui connaissent la même clé pré-partagée. Sans cette authentification configurée, si quelqu'un présente un autre routeur avec les informations différentes ou contradictoires d'artère en fonction au réseau, les tables de routage sur vos Routeurs pourraient devenir corrompues et une attaque par déni de service pourrait s'ensuivre. Ainsi, quand vous ajoutez l'authentification aux messages EIGRP envoyés entre vos Routeurs, il empêche quelqu'un d'exprès ou accidentellement ajoutant un autre routeur au réseau et posant un problème.

Attention : Quand l'authentification de message EIGRP est ajoutée à l'interface d'un routeur, des arrêts de ce routeur recevant des messages de routage de ses pairs jusqu'à ce qu'ils soient également configurés pour l'authentification de message. Ceci interrompt des transmissions de routage sur votre réseau. Voir les messages quand seulement Dallas est pour en savoir plus

configuré.

Conditions préalables

Conditions requises

- Le temps doit être correctement configuré sur tous les Routeurs. Référez-vous à configurer le pour en savoir plus de NTP.
- Une configuration fonctionnante EIGRP est recommandée.

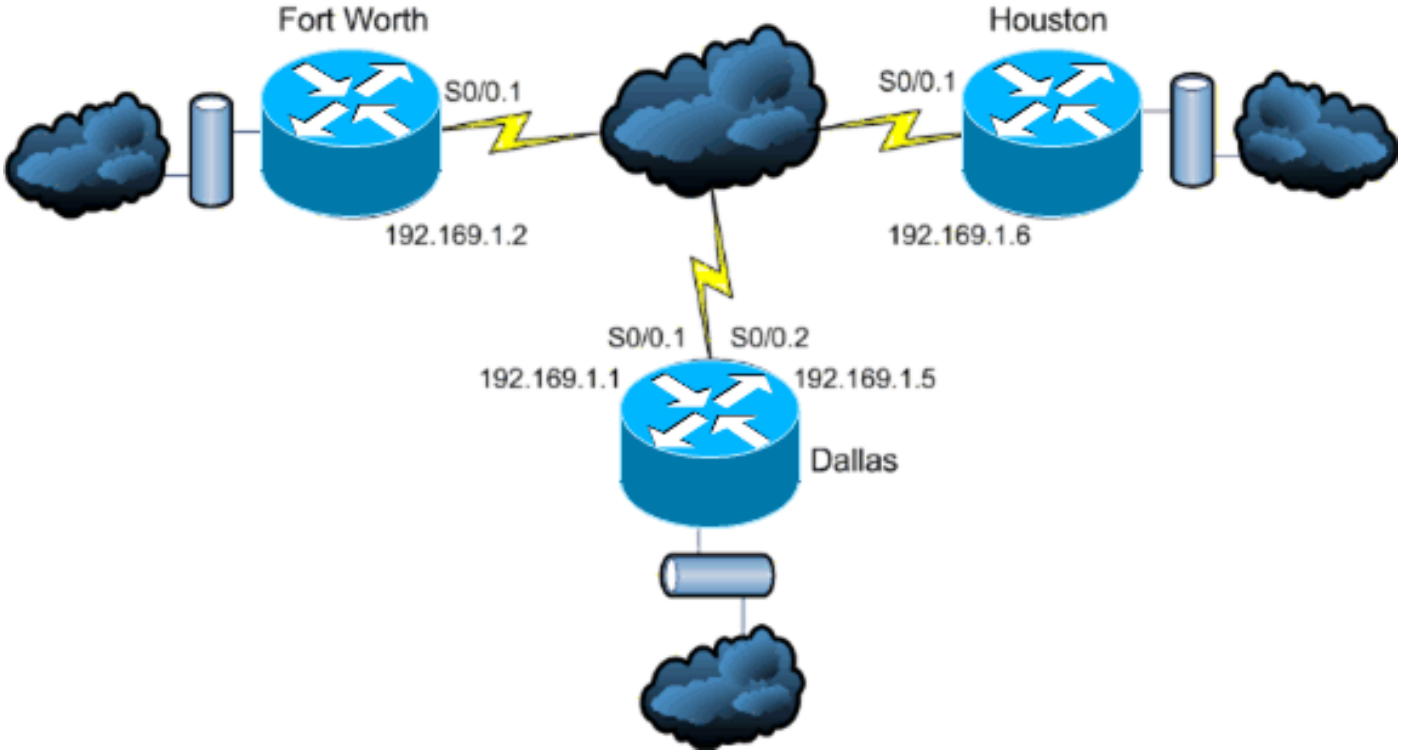
Composants utilisés

Les informations dans ce document sont basées sur la version de logiciel 11.2 et ultérieures de Cisco IOS®.

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.

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 veut configurer l'authentification pour des messages EIGRP entre le routeur concentrateur à Dallas et les sites distants à Fort Worth et à Houston. La configuration EIGRP (sans authentification) est déjà complète sur chacun des trois Routeurs. Cet exemple de sortie est 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
```

Configurez l'authentification de message EIGRP

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

1. La création d'un trousseau de clés et d'une clé.
2. La configuration de l'authentification EIGRP pour utiliser ces trousseau de clés et clé.

Cette section montre les étapes pour configurer l'authentification de message EIGRP sur le routeur de Dallas et puis les Routeurs de Fort Worth et de Houston.

Créez un trousseau de clés sur Dallas

L'acheminement de l'authentification se fonde sur une clé sur un trousseau de clés pour fonctionner. Avant que l'authentification puisse être activée, un trousseau de clés et au moins une clé doivent être créés.

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 nombre principal. **1** est utilisé dans cet exemple.**Note**: L'il est recommandé que le nombre principal soit identiques sur tous les Routeurs impliqués dans la configuration.
   ```
   Dallas(config-keychain)#key 1
   ```
4. Spécifiez le key-string pour la clé. **securetraffic** est utilisé dans cet exemple.
   ```
   Dallas(config-keychain-key)#key-string securetraffic
   ```
5. Finissez la configuration.
   ```
   Dallas(config-keychain-key)#end
   Dallas#
   ```

Configurez l'authentification sur Dallas

Une fois que vous créez un trousseau de clés et une clé, vous devez configurer l'EIGRP pour exécuter l'authentification de message avec la clé. Cette configuration est terminée sur les interfaces que l'EIGRP est configuré en fonction.

Attention : Quand l'authentification de message EIGRP est ajoutée aux interfaces de Dallas, elle cesse de recevoir des messages de routage de ses pairs jusqu'à ce qu'ils soient également configurés pour l'authentification de message. Ceci interrompt des transmissions de routage sur votre réseau. Voir les messages quand seulement Dallas est pour en savoir plus configuré.

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

2. Du mode de configuration globale, spécifiez l'interface que vous voulez configurer l'authentification de message EIGRP en fonction. Dans cet exemple la première interface est l'**interface série 0/0.1**.
   ```
   Dallas(config)#interface serial 0/0.1
   ```

3. Authentification de message de l'enable EIGRP. **Les 10** utilisés ici est le numéro de système autonome du réseau. **le MD5** indique que les informations parasites de MD5 doivent être utilisées pour l'authentification.
   ```
   Dallas(config-subif)#ip authentication mode eigrp 10 md5
   ```

4. Spécifiez le trousseau de clés qui devrait être utilisé pour l'authentification. **10** est le numéro de système autonome. **MYCHAIN** est le trousseau de clés qui a été créé dans la création par section de trousseau de clés.
   ```
   Dallas(config-subif)#ip authentication key-chain eigrp 10 MYCHAIN
   Dallas(config-subif)#end
   ```

5. Terminez-vous la même configuration sur l'interface série 0/0.2 d'interface.
   ```
   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#
   ```

Configurez Fort Worth

Cette section affiche les commandes nécessaires pour configurer l'authentification de message EIGRP sur le routeur de Fort Worth. Pour l'explication plus détaillée des commandes affichées ici, voyez pour créer un trousseau de clés sur Dallas et pour 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#
```

Configurez Houston

Cette section affiche les commandes nécessaires pour configurer l'authentification de message EIGRP sur le routeur de Houston. Pour l'explication plus détaillée des commandes affichées ici, voyez pour créer un trousseau de clés sur Dallas et pour 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#
```

Vérifiez

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

Note: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

Messages quand seulement Dallas est configuré

Une fois que l'authentification de message EIGRP est configurée sur le routeur de Dallas, ce routeur commence à rejeter des messages des Routeurs de Fort Worth et de Houston parce qu'ils ne font pas encore configurer l'authentification. Ceci peut être vérifié en émettant des **debugs eigrp packets** commandent sur le routeur de 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 quand tous les Routeurs sont configurés

Une fois que l'authentification de message EIGRP est configurée sur chacun des trois Routeurs, ils commencent à permuter des messages EIGRP de nouveau. Ceci peut être vérifié en émettant des **debugs eigrp packets** commandent de nouveau. Des sorties de cette fois des Routeurs de Fort Worth et de 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.
```

Dépannez

Liaison unidirectionnelle

Vous devez configurer l'EIGRP des temporisateurs bonjour et de temps de maintien sur les deux extrémités. Si vous configurez les temporisateurs seulement sur une extrémité, un lien unidirectionnel se produit.

Un routeur sur un lien unidirectionnel pourrait pouvoir recevoir bonjour des paquets. Cependant, bonjour les paquets envoyés ne sont pas reçus à l'autre extrémité. Ce lien unidirectionnel est habituellement indiqué par des *messages de dépassement de limite de relance* sur une extrémité.

Afin de visualiser les *messages de dépassement de limite de relance*, utilisez les commandes de **debug eigrp packet** et de **debug ip eigrp notifications**.

Informations connexes

- Support technique de Protocole EIGPR (Enhanced Interior Gateway Routing Protocol)
- Support et documentation techniques - Cisco Systems