EIGRP信息认证配置示例

目录

简介

本文档说明了如何将消息认证添加到增强的内部网关路由选择协议 (EIGRP) 路由器，并保护路由表免受蓄意或意外损坏。

您的路由器的 EIGRP 消息增加了认证内容，确保您的路由器只接受了解同一预共享密钥的其他路由器的路由信息。在未配置此认证的情况下，如果有用户将其他包含不同或冲突的路由信息的路由器引入网络，则可能损坏路由器上的路由表，并可能随之产生拒绝服务攻击。因此，当您将认证添加到在您的路由器之间发送的 EIGRP 消息中时，它可防止有人有意或无意将另一个路由器添加到网络，并引起问题。

警告： 当 EIGRP 消息认证添加到路由器的接口时，该路由器停止接收来自其对等体的路由消息，直到它们也配置消息认证。这**的确**中断了您网络上的路由通信。有关详细信息，请参阅仅配置 Dallas 时的消息。

先决条件

要求

- 必须正确配置所有路由器上的时间。有关详细信息，请参阅配置 NTP。
- 推荐一个工作 EIGRP 配置。

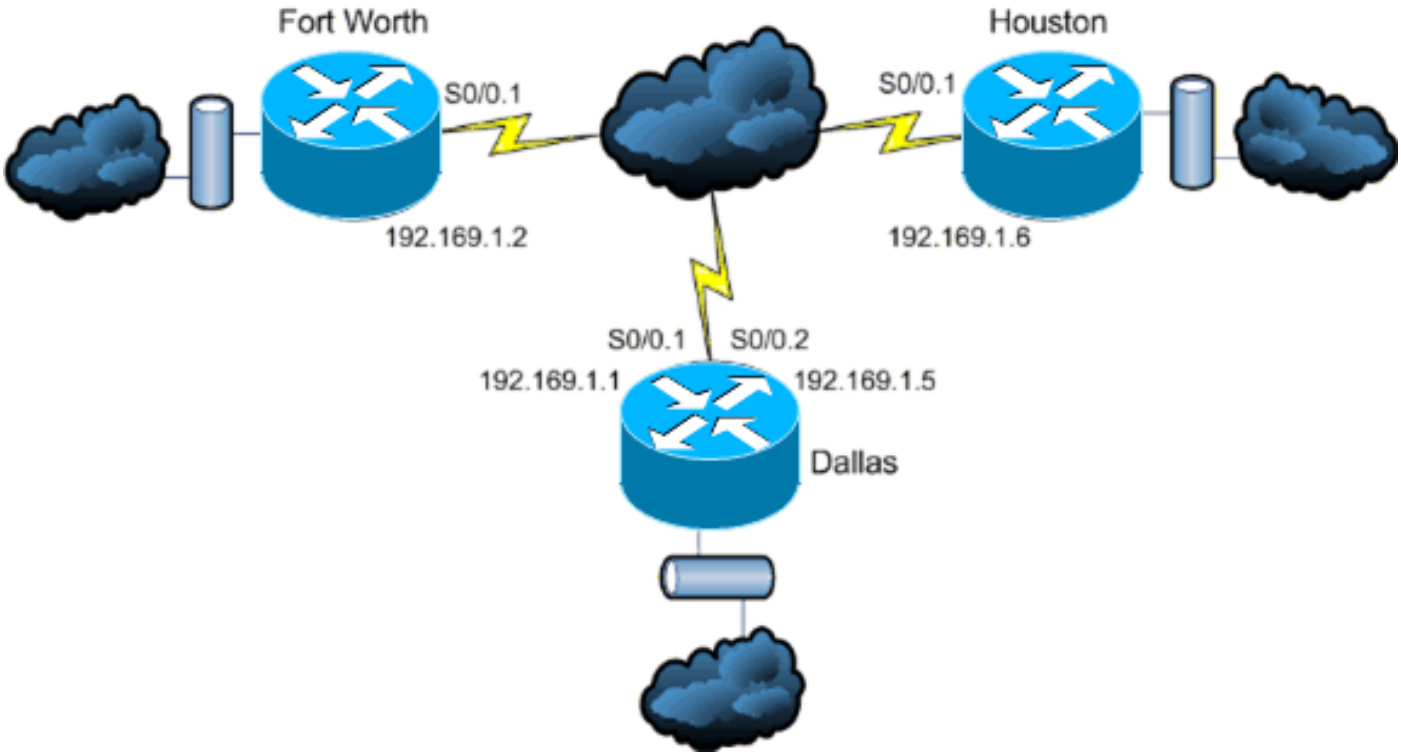
使用的组件

本文档中的信息基于 Cisco IOS® 软件版本 11.2 及以上。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

网络图

本文档使用以下网络设置：



规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

在这种情况下，网络管理员要在 Dallas 的中心路由器与 Fort Worth 和 Houston 的远程站点之间配置 EIGRP 消息认证。EIGRP 配置（无认证）已在所有的三个路由器上完成。此示例输出来自 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
```

配置 EIGRP 消息认证

EIGRP 消息认证的配置包含两个步骤：

1. 密钥链和密钥的创建。
2. 使用该密钥链和密钥的 EIGRP 认证配置。

本部分说明了先在 Dallas 路由器上，然后在 Fort Worth 和 Houston 路由器上配置 EIGRP 消息认证的步骤。

在 Dallas 上创建密钥链

路由认证依靠密钥链上的一个密钥起作用。在可以启用认证之前，必须创建一个密钥链和至少一个密钥。

1. 进入全局配置模式。`Dallas#configure terminal`
2. 创建密钥链。此示例中使用 **MYCHAIN**。`Dallas(config)#key chain MYCHAIN`
3. 指定密钥编号。此示例中使用 **1**。**注意：** 建议密钥编号在配置涉及的所有路由器上相同。`Dallas(config-keychain)#key 1`
4. 指定密钥的密钥字符串。此示例中使用 **securetraffic**。`Dallas(config-keychain-key)#key-string securetraffic`
5. 结束配置。`Dallas(config-keychain-key)#end Dallas#`

在 Dallas 上配置认证

一旦创建密钥链和密钥，您必须配置 EIGRP 以使用密钥进行消息认证。此配置在配置 EIGRP 所在的接口上完成。

警告： 当 EIGRP 消息认证添加到 Dallas 接口时，该路由器停止接收来自其对等体的路由消息，直到它们也配置消息认证。这**的确**中断了您网络上的路由通信。有关详细信息，请参阅仅配置 Dallas 时的消息。

1. 进入全局配置模式。`Dallas#configure terminal`
2. 从全局配置模式指定您要配置 EIGRP 消息认证所在的接口。在本示例中，第一个接口是 **Serial 0/0.1**。`Dallas(config)#interface serial 0/0.1`
3. 启用 EIGRP 消息认证。此处使用的 **10** 是网络的自治系统编号。**md5** 表示 md5 散列要用于认证。`Dallas(config-subif)#ip authentication mode eigrp 10 md5`
4. 指定应该用于认证的密钥链。**10** 是自治系统编号。**MYCHAIN** 是在创建密钥链部分创建的密钥链。`Dallas(config-subif)#ip authentication key-chain eigrp 10 MYCHAIN Dallas(config-subif)#end`
5. 在接口序列 0/0.2 上完成相同的配置。`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#`

配置 Fort Worth

本部分显示了在 Fort Worth 路由器上配置 EIGRP 消息认证所必需的命令。有关此处显示的命令的更多详细说明，请参阅在 Dallas 上创建密钥链和在 Dallas 上配置认证。

```
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#
```

配置 Houston

本部分显示了在 Houston 路由器上配置 EIGRP 消息认证所必需的命令。有关此处显示的命令的更多详细说明，请参阅在 Dallas 上创建密钥链和在 Dallas 上配置认证。

```
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#
```

验证

使用本部分可确认配置能否正常运行。

注意： 使用 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

仅配置 Dallas 时的消息

一旦在 Dallas 路由器上配置 EIGRP 消息认证之后，该路由器开始拒绝来自 Fort Worth 和 Houston 路由器的消息，因为它们尚未配置认证。这可以通过在 Dallas 路由器上发出一个 **debug eigrp packets 命令**进行验证：

```
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.
```

配置所有路由器时的消息

一旦 EIGRP 消息认证在所有的三个路由器上配置之后，它们开始再次交换 EIGRP 消息。这可以通过再次发出一个 **debug eigrp packets 命令**进行验证。显示来自 Fort Worth 和 Houston 路由器的时间输出：

```
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.
```

故障排除

单向链路

您必须在两端配置 EIGRP Hello 和 Hold-time 计时器。如果仅在一端配置计时器，则出现单向链路。

单向链路上的路由器也许能接收 Hello 数据包。然而，在另一端没有接收到发出的 Hello 数据包。此单向链路通常由一端的*已超出重试次数限制*消息表示。

为查看*已超出重试次数限制*消息，请使用 **debug eigrp packet** 和 **debug ip eigrp notifications** 命令。

相关信息

- 增强的内部网关路由选择协议 (EIGRP) 技术支持
- 技术支持和文档 - Cisco Systems