ASA 9.x EIGRP配置示例

目录

简介

本文描述如何配置Cisco可适应安全工具(ASA)为了学习路由通过增强的内部网关路由选择协议(EIGRP)， ASA软件版本9.x支持和以后和执行验证。

先决条件

要求

思科要求您符合这些情况，在您尝试此配置前：

- Cisco ASA必须运行9.x或以后。
- 因为多个上下文模式，不支持EIGRP必须在单一上下文模式。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco ASA软件版本9.2.1
- Cisco Adaptive Security Device Manager (ASDM)版本7.2.1
- 运行版本12.4的Cisco IOS路由器

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。

背景信息

指南和限制

- 一个EIGRP实例支持在单模和每上下文在多模。
- 两个线索每上下文创建每个在多模的EIGRP实例，并且可以查看与show process。
- 默认情况下Auto-summary禁用。
- 邻接关系没有被建立在机群之间在单个接口模式。
- 在[<acl>]的默认信息用于为了过滤流入候选默认路由的外部位。
- 默认信息[<acl>]用于为了过滤流出的候选默认路由的外部位。

EIGRP和故障切换

思科ASA代码版本8.4.4.1和以后同步动态路由从活动装置到备用装置。另外，路由的删除也同步到备用装置。然而，对等体邻接的状态没有同步;仅活动设备保持邻居状态和积极参加动态路由。参考的ASA FAQ ：如果动态路由同步，什么在故障切换以后发生？。

配置

此部分描述如何配置在本文报道的功能。

> **Note**:使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图

本文档使用以下网络设置：

在图示的网络拓扑中，Cisco ASA 内部接口 IP 地址是 10.10.10.1/24。目标是配置在思科ASA的EIGRP为了动态地学习路由到内部网络(10.20.20.0/24， 172.18.124.0/24和192.168.10.0/24)通过邻接路由器(R1)。R1 通过其他两个路由器（R2 和 R3）识别通往远程内部网络的路由。

ASDM 配置

ASDM是用于的一基于浏览器的应用程序为了配置和监控在安全工具的软件。ASDM从安全工具装载，然后用于为了配置，监控和管理设备。您比Java程序能也使用ASDM发射器为了启动ASDM应用程序快速。此部分描述您需要为了配置在与ASDM的本文描述的功能的信息。

完成这些步骤为了配置在思科ASA的EIGRP。

1. 登陆对与ASDM的思科ASA。

2. 如此屏幕画面所显示，导航到ASDM接口的**Configuration>设备设置>路由> EIGRP**地区。

3. 如此屏幕画面所显示，启用在**设置>进程实例**选项卡的EIGRP路由进程。在本示例中，EIGRP进程是 **10。**

4. 您可以配置可选的高级 EIGRP 路由进程参数。单击 **Setup > Process Instances** 选项卡上的 **Advanced**。您可以将 EIGRP 路由进程配置为残域路由进程，禁用自动路由汇总，定义重分配路由的默认度量值，更改内部和外部 EIGRP 路由的管理距离，配置静态路由器 ID，并且启用或禁用邻接更改的日志记录。在本示例中，使用内部接口的 IP 地址 (10.10.10.1) 静态配置 EIGRP 路由器 ID。另外，也禁用了 **Auto-summary**。所有其他选项都使用默认值配置。

5. 完成前述步骤后，在 **Setup > Networks** 选项卡上定义 EIGRP 路由中涉及的网络和接口。单击 **Add**，如屏幕截图所示。

6. 将出现此屏幕。在本例中，您添加的唯一的网络是网络内部(10.10.10.0/24)，因为EIGRP在内部接口仅启用。

   只协调与属于定义的网络参加EIGRP路由进程的IP地址。如果有一个接口您不要参加EIGRP路由，但是那附加对您想要通告的网络，请配置在包括网络接口附加，然后配置该接口作为无源接口的**设置>网络**选项卡的一个网络入口，以便接口不能发送或接收EIGRP更新。

   Note:配置为无源的接口不发送或接收 EIGRP 更新。

7. 还可以选择在 Filter Rules 窗格中定义路由过滤器。路由过滤可对允许在 EIGRP 更新中发送或接收的路由提供更多控制。

8. 您也可以选择配置路由重分配。思科ASA能由路由信息协议(RIP)重新分配路由已发现和开放最短路径优先(OSPF)到EIGRP路由进程。您还可以将静态和连接的路由重分配到 EIGRP 路由进程。如果静态或已连接路由在 **Setup > Networks** 选项卡上配置的网络范围内，则不需要对其重分配。请在 Redistribution 窗格中定义路由重分配。

9. EIGRP hello 数据包作为多播数据包发送。如果EIGRP邻居在间非广播网络查找，您必须手工定义该邻居。手动定义 EIGRP 邻居时，hello 数据包作为单播消息发送到该邻居。为了定义静态 EIGRP 邻居，请转到 **Static Neighbor** 窗格。

10. 默认情况下，会发送并且接受默认路由。为了限制或禁用发送和接收默认路由信息，请打开 **Configuration > Device Setup > Routing > EIGRP > Default Information** 窗格。Default Information 窗格显示控制发送和接收 EIGRP 更新中的默认路由信息的规则表。

    Note:您能安排一"*在*"和一个""为每EIGRP路由进程规定。（当前仅支持一个进程。）

配置 EIGRP 身份验证

Cisco ASA 支持来自 EIGRP 路由协议的更新路由的 MD5 身份验证。在每EIGRP数据包的MD5-keyed摘要防止未授权的或错误路由消息的介绍未经同意的来源。对 EIGRP 消息添加身份验证可确保您的路由器和 Cisco ASA 只接受来自配置了相同预共享密钥的其他路由设备的路由消息。没有配置的此验证，如果某人引入有另外或相反路由信息的另一个路由设备对网络，在您的路由器的路由表或思科ASA能变得损坏，并且拒绝服务攻击能接着而来。当您添加验证到在(之间的EIGRP发送的消息包括ASA)的您的路由设备，防止EIGRP路由器的未授权的新增内容到您的路由结构。

EIGRP 路由身份验证基于每个接口进行配置。对于针对 EIGRP 消息身份验证配置的接口上的所有 EIGRP 邻居，必须为要建立的相邻关系配置相同的身份验证模式和密钥。

完成这些步骤为了启用在思科ASA的EIGRP MD5身份验证。

1. 在ASDM，请导航对**Configuration>设备设置>路由> EIGRP >接口**如显示。

2. 在这种情况下，EIGRP 在内部接口 (GigabitEthernet 0/1) 上启用。选择 **GigabitEthernet 0/1** 接口，然后单击 **Edit**。

3. 在 Authentication 下，选择 **Enable MD5 authentication**。添加关于验证参数的更多信息此处。在本示例中，预共享密钥是 **cisco123**，密钥 ID 是 **1**。

EIGRP路由过滤

使用EIGRP，您能控制被发送并且接收的路由更新。在本例中，您将阻塞在ASA的路由更新网络前缀的192.168.10.0/24，是在R1后。对于路由过滤，您能只使用**标准ACL**。

```
access-list eigrp standard deny 192.168.10.0 255.255.255.0
access-list eigrp standard permit any

router eigrp 10
distribute-list eigrp in
```

验证

```
ASA(config)# show access-list eigrp
access-list eigrp; 2 elements; name hash: 0xd43d3adc
access-list eigrp line 1 standard deny 192.168.10.0 255.255.255.0 (hitcnt=3) 0xeb48ecd0
access-list eigrp line 2 standard permit any4 (hitcnt=12) 0x883fe5ac
```

配置

Cisco ASA CLI 配置

这是思科ASA CLI配置。

```
ASA(config)# show access-list eigrp
access-list eigrp; 2 elements; name hash: 0xd43d3adc
access-list eigrp line 1 standard deny 192.168.10.0 255.255.255.0 (hitcnt=3) 0xeb48ecd0
access-list eigrp line 2 standard permit any4 (hitcnt=12) 0x883fe5ac
```

Cisco IOS 路由器 (R1) CLI 配置

这是 R1（内部路由器）的 CLI 配置。

```
ASA(config)# show access-list eigrp
access-list eigrp; 2 elements; name hash: 0xd43d3adc
access-list eigrp line 1 standard deny 192.168.10.0 255.255.255.0 (hitcnt=3) 0xeb48ecd0
access-list eigrp line 2 standard permit any4 (hitcnt=12) 0x883fe5ac
```

验证

完成这些步骤为了验证您的配置。

1. 在ASDM，您能导航到**路由的Monitoring> > EIGRP邻居**为了看到其中每一EIGRP邻居。此屏幕截图显示了作为活动邻居的内部路由器 (R1)。您还可以看到此邻居驻留的接口、保持时间和邻接关系的正常运行时间 (UpTime)。

2. 此外，如果导航到 **Monitoring > Routing > Routes**，还可以验证路由表。在此屏幕截图中，可以看到 **192.168.10.0/24、172.18.124.0/24** 和 **10.20.20.0/24** 网络是通过 R1 (**10.10.10.2**) 识别的。

   从 CLI 中，可以使用 **show route** 命令获得相同的输出。

   ```
   ciscoasa# show route

   Codes: C - connected, S - static, I - IGRP, 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, E - EGP
i - IS-IS, 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 100.10.10.2 to network 0.0.0.0
C 198.51.100.0 255.255.255.0 is directly connected, outside
D 192.168.10.0 255.255.255.0 [90/131072] via 10.10.10.2, 0:32:29, inside
D 172.18.124.0 255.255.255.0 [90/131072] via 10.10.10.2, 0:32:29, inside
C 127.0.0.0 255.255.0.0 is directly connected, cplane
D 10.20.20.0 255.255.255.0 [90/28672] via 10.10.10.2, 0:32:29, inside
C 10.10.10.0 255.255.255.0 is directly connected, inside
C 10.10.20.0 255.255.255.0 is directly connected, management
S* 0.0.0.0 0.0.0.0 [1/0] via 198.51.100.1, outside
```

使用ASA版本9.2.1和以上，您能使用**show route EIGRP命令**为了显示仅EIGRP路由。

```
ciscoasa(config)# show route eigrp

Codes: L - local, 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, + - replicated route

Gateway of last resort is not set

D 192.168.10.0 255.255.255.0 [90/131072] via 10.10.10.2, 0:32:29, inside
D 172.18.124.0 255.255.255.0 [90/131072] via 10.10.10.2, 0:32:29, inside
D 10.20.20.0 255.255.255.0 [90/28672] via 10.10.10.2, 0:32:29, inside
```

3. 您能也使用**show eigrp topology**命令为了得到关于获知的网络和EIGRP拓扑的信息。

```
    ciscoasa# show eigrp topology
EIGRP-IPv4 Topology Table for AS(10)/ID(10.10.10.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
r - reply Status, s - sia Status
P 10.20.20.0 255.255.255.0, 1 successors, FD is 28672
via 10.10.10.2 (28672/28416), GigabitEthernet0/1
P 10.10.10.0 255.255.255.0, 1 successors, FD is 2816
via Connected, GigabitEthernet0/1
P 192.168.10.0 255.255.255.0, 1 successors, FD is 131072
via 10.10.10.2 (131072/130816), GigabitEthernet0/1
P 172.18.124.0 255.255.255.0, 1 successors, FD is 131072
via 10.10.10.2 (131072/130816), GigabitEthernet0/1
```

4. **显示EIGRP邻居**命令也是有用的为了验证活动邻居和对应的信息。此示例显示您从在Step1的ASDM得到的同一信息。

```
ciscoasa# show eigrp neighbors
EIGRP-IPv4 neighbors for process 10
H Address Interface Hold Uptime SRTT RTO Q Seq (sec) (ms)Cnt Num

0 10.10.10.2 Gi0/1 12 00:39:12 107 642 0 1
```

数据包流

这是数据包流。

1. ASA在链路出现并且通过所有其Eigrp配置的接口发送mcast Hello数据包。
2. R1收到Hello数据包并且发送mcast Hello数据包。
3. ASA收到Hello数据包并且发送有最初的位集的一更新数据包，表明这是初始化进程。
4. R1收到更新数据包并且发送有最初的位集的一更新数据包，表明这是初始化进程。
5. 在ASA和R1以后交换了hello，并且邻接设立，与ACK数据包的ASA和R1回复，表明更新信息接收。
6. ASA发送其路由信息对在更新数据包的R1。
7. R1在其拓扑表里插入更新数据包信息。拓扑表包括邻居通告的所有目的地。它与能到目的地和他们相关的量度传播的所有邻居一起被组织，以便每个目的地是列出的。
8. R1然后发送更新数据包对ASA。
9. 一旦它收到更新数据包， ASA发送ACK数据包对R1。在ASA和R1成功接受从彼此后的更新数据包，他们准备好选择后继路由(最佳)和可行后继者(备份)路由在拓扑表里，并且提供后继路由路由对路由表。

故障排除

此部分包括关于可以是有用的为了排除故障EIGRP问题的**Debug与Show**调试指令的信息。

故障排除命令

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

Note:使用 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。为了显示调试信息 Diffusing Update Algorithm (DUAL)有限状态机，在特权EXEC模式使用**debug eigrp fsm命令**。此命令使您可以观察 EIGRP 可行后继路由活动并确定路由进程是否安装并删除了路由更新。

这是具有 R1 的成功对等体内的 debug 命令输出。您可以看到系统中成功安装的每个不同的路由。

```
ciscoasa# show eigrp neighbors
EIGRP-IPv4 neighbors for process 10
H Address Interface Hold Uptime SRTT RTO Q Seq (sec) (ms)Cnt Num

0 10.10.10.2 Gi0/1 12 00:39:12 107 642 0 1
```

您还可以使用 **debug eigrp neighbor** 命令。这是此 debug 命令在 Cisco ASA 成功创建具有 R1 的新邻居关系时的输出。

```
ciscoasa# EIGRP-IPv4(Default-IP-Routing-Table:10): Callback: route_adjust Gigabi
tEthernet0/1
EIGRP: New peer 10.10.10.2
EIGRP-IPv4(Default-IP-Routing-Table:10): route installed for 10.20.20.0 ()
EIGRP-IPv4(Default-IP-Routing-Table:10): route installed for 172.18.124.0 ()
EIGRP-IPv4(Default-IP-Routing-Table:10): route installed for 192.168.10.0 ()
```

您还可以将 debug eigrp 数据包用于 Cisco ASA 和其对等体之间详细的 EIGRP 消息交换信息。在本示例中，身份验证密钥在路由器 (R1) 上进行了更改，并且 debug 输出显示问题是身份验证不匹配。

```
ciscoasa# EIGRP: Sending HELLO on GigabitEthernet0/1
AS 655362, Flags 0x0, Seq 0/0 interfaceQ 1/1 iidbQ un/rely 0/0
EIGRP: pkt key id = 1, authentication mismatch
EIGRP: GigabitEthernet0/1: ignored packet from 10.10.10.2, opcode = 5
(invalid authentication)
```

EIGRP结邻下来与Syslog ASA-5-336010匹配

当在EIGRP分配表上的所有变化做时， ASA下降EIGRP结邻。此系统消息被看到。

```
ciscoasa# EIGRP: Sending HELLO on GigabitEthernet0/1
AS 655362, Flags 0x0, Seq 0/0 interfaceQ 1/1 iidbQ un/rely 0/0
EIGRP: pkt key id = 1, authentication mismatch
EIGRP: GigabitEthernet0/1: ignored packet from 10.10.10.2, opcode = 5
(invalid authentication)
```

使用此配置，每当**新的ACL条目**在ACL**被添加**， Eigrp网络**列表**EIGRP结邻重置。

```
ciscoasa# EIGRP: Sending HELLO on GigabitEthernet0/1
AS 655362, Flags 0x0, Seq 0/0 interfaceQ 1/1 iidbQ un/rely 0/0
EIGRP: pkt key id = 1, authentication mismatch
EIGRP: GigabitEthernet0/1: ignored packet from 10.10.10.2, opcode = 5
(invalid authentication)
```

您能注意到邻接关系是邻接设备。

```
ciscoasa(config)# show eigrp neighbors
EIGRP-IPv4 neighbors for process 10
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 10.10.10.2 Gi0/3 10 00:01:22 1 5000 0 5

ciscoasa(config)# show eigrp neighbors
EIGRP-IPv4 neighbors for process 10
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 10.10.10.2 Gi0/3 13 00:01:29 1 5000 0 5
```

现在您能添加**access-list Eigrp网络列表标准拒绝172.18.24.0 255.255.255.0**。

```
ciscoasa(config)# show eigrp neighbors
EIGRP-IPv4 neighbors for process 10
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 10.10.10.2 Gi0/3 10 00:01:22 1 5000 0 5

ciscoasa(config)# show eigrp neighbors
EIGRP-IPv4 neighbors for process 10
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 10.10.10.2 Gi0/3 13 00:01:29 1 5000 0 5
```

这些日志在**debug eigrp fsm**能被看到。

```
ciscoasa(config)# show eigrp neighbors
EIGRP-IPv4 neighbors for process 10
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 10.10.10.2 Gi0/3 10 00:01:22 1 5000 0 5

ciscoasa(config)# show eigrp neighbors
EIGRP-IPv4 neighbors for process 10
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 10.10.10.2 Gi0/3 13 00:01:29 1 5000 0 5
```

这是总计的预料之中的行为从8.4的新建的ASA版本和8.6到9.1。同样在运行12.4到15.1代码系列的路由器被观察了。 然而，因为做的变动对ACL不重置EIGRP邻接，此行为在ASA版本8.2和以下ASA软件版本没有被观察。

因为EIGRP发送全双工拓扑表给邻居，当邻居首先出现，然后它时发送仅更改，配置与EIGRP的事件驱动的本质的一分配列表将使困难为了更改能应用，不用邻接关系的全双工重置。路由器会需要记录从邻接发送对和接收的每个路由为了知道哪个路由更改(即会或不会发送/接受)为了应用更改如指明由当前请分配列表。切断和重建在邻居之间的邻接是更加容易的。

当邻接被切断并且被重建时，在特定邻居之间的所有获取的路由被忘记，并且在邻居之间的整个同步重新执行-与新请分配到位列表。

您使用为了排除故障Cisco IOS路由器的大多EIGRP技术在思科ASA可以应用。为了排除故障EIGRP，请使用主要故障排除流程图;从标记 **Main** 的框处开始。