



EIGRP

本部分介绍如何使用增强型内部网关路由协议 (EIGRP) 配置 威胁防御，以路由数据、执行身份验证以及重新分发路由信息。

- [关于 EIGRP 路由，第 1 页](#)
- [EIGRP 的要求和必备条件，第 2 页](#)
- [EIGRP 路由的准则和限制，第 2 页](#)
- [配置 EIGRP，第 3 页](#)

关于 EIGRP 路由

思科开发的增强型内部网关路由协议 (EIGRP) 是 IGRP 的增强版本。与 IGRP 和 RIP 不同，EIGRP 不发送定期路由更新。仅在网络拓扑发生更改时才会发送 EIGRP 更新。将 EIGRP 与其他路由协议区分开来的主要功能包括快速收敛、支持可变长度子网掩码、支持部分更新以及支持多个网络层协议。

运行 EIGRP 的路由器会存储所有邻居路由表，以便可以迅速适应备用路由。如果不存在合适的路由，则 EIGRP 会查询其邻居以发现备用路由。这些查询会被传播直至找到备用路由为止。EIGRP 对可变长度子网掩码功能的支持允许在网络边界自动汇总路由。此外，还可以将 EIGRP 配置为在任何接口的任何位边界汇总。

EIGRP 不会定期更新。相反，它会在路由指标发生更改时发送部分更新。部分更新的传播是自动绑定的，因此只有需要该信息的路由器才会更新。得益于这两项功能，EIGRP 与 IGRP 相比可显著减少占用的带宽。

要动态地了解直接连接网络上的其他路由器，威胁防御会使用邻居发现。EIGRP 路由器发出组播 Hello 数据包，通告其在网络中的存在状态。当 EIGRP 设备收到来自新邻居的 Hello 数据包时，会将其包含初始化位集的拓扑表发送至邻居。当邻居收到包含初始化位集的拓扑更新时，邻居将其拓扑表发回到设备。

Hello 数据包作为组播消息发出。预期不会对 Hello 消息作出响应。静态定义的邻居不在此规则的范围。如果手动配置邻居，则 Hello 消息、路由更新和确认将作为单播消息发送。

一旦邻居关系建立后，除非网络拓扑发生更改，否则便不会交换路由更新。邻居关系通过 Hello 数据包来维护。从邻居收到的每个 Hello 数据包均包括保持时间。保持时间是威胁防御预期收到该邻

居的 Hello 数据包的时间。如果设备在保持时间内未收到由该邻居通告的 Hello 数据包，则设备会将该邻居视为不可用。

EIGRP 会使用邻居发现/恢复、可靠传输协议 (RTP) 和扩散更新算法 (DUAL) 进行路由计算。DUAL 将目标的所有路由都保存在拓扑表中，而不只是保存最低成本路由。最低成本路由会插入到路由表中。其他路由则保留在拓扑表中。如果主路由发生故障，可以从可行后继路由中选择另一个路由。后继路由是指用于进行数据包转发的具有到达目标的最低成本路径的邻居路由器。可行性计算可确保路径不是路由环路的一部分。

如果在拓扑表中找不到可行后继路由，则会重新计算路由。在路由重新计算期间，DUAL 会查询 EIGRP 邻居以获取路由。查询会被传播到连续的邻居。如果找不到可行的后继邻居，则会返回不可达消息。

在路由重新计算期间，DUAL 会将路由标记为活动状态。默认情况下，威胁防御会等待三分钟接收来自其邻居的响应。如果设备未收到来自邻居的响应，则会将路由标记为陷入主动状态。系统会删除拓扑表中作为可行性后继路由指向无响应邻居的所有路由。

EIGRP 的要求和必备条件

型号支持

威胁防御

Threat Defense Virtual

支持的域

任意

用户角色

管理员

网络管理员

EIGRP 路由的准则和限制

防火墙模式指导原则

仅支持路由防火墙模式。

设备准则

- 每台设备仅允许有一个 EIGRP 进程。
- 可以通过 威胁防御 6.6 及更高版本上的管理中心 UI 来配置 EIGRP。

接口指导原则

- 只有具有逻辑名称和 IP 地址的路由接口才能与 EIGRP 路由进程相关联。
- 只有属于全局虚拟路由器的接口才能成为 EIGRP 的一部分。EIGRP 可以在全局虚拟路由器中跨路由协议获知、过滤和重新分发路由。
- 仅支持物理、端口通道、冗余、子接口。
- VTI、BVI、VNI 和 EtherChannel 接口不能作为 EIGRP 的一部分。
- 被动接口不能被配置为邻居接口。

IP 地址和网络对象支持

- 仅支持 IPv4 地址。
- 不支持范围、FQDN 和通配符掩码。
- 仅支持标准访问列表对象。

重新分配准则

- 全局虚拟路由器中的 BGP、OSPF 和 RIP 可以重新分配到 EIGRP。
- EIGRP 可以重新分配到全局虚拟路由器中的 BGP、OSPF、RIP、静态和已连接。

部署流程准则

如果要更改已部署 EIGRP 配置的现有 AS 编号，您必须禁用 EIGRP 并进行部署。此步骤将清除威胁防御上已部署的 EIGRP 配置。接下来使用新的 AS 编号重新创建 EIGRP 配置，然后进行部署。因此，此过程可防止由于在威胁防御上部署相同的 EIGRP 配置而导致任何部署失败。

升级指南

如果您升级到版本 7.2 和更新版本具有任何 FlexConfig EIGRP 策略，则管理中心会在部署期间显示警告消息。但是，它不会停止部署过程。但在部署后，要从 UI（设备（编辑）(Device [Edit]) > 路由 (Routing) > EIGRP）管理 EIGRP 策略，则必须在 设备（编辑）(Device [Edit]) > 路由 (Routing) > EIGRP 页面中重新执行配置，并从 FlexConfig 中删除配置。为了简化该手动过程，引入了命令行迁移工具来将 EIGRP Flex 配置迁移到 EIGRP 路由策略。有关详细信息，请参阅[迁移 FlexConfig 策略](#)。

配置 EIGRP

您可以在路由 (Routing) 选项卡中启用和配置防火墙设备上的 EIGRP。

过程

- 步骤 1** 依次选择设备(Devices) > 设备管理(Device Management), 并且编辑 威胁防御 设备。
- 步骤 2** 点击路由选项卡。
- 步骤 3** 在“全局”(Global)下, 点击 **EIGRP**。
- 步骤 4** 选中启用 **EIGRP (Enable EIGRP)** 复选框以启用 EIGRP 路由进程。
- 步骤 5** 在 **AS 编号** 字段中, 输入 EIGRP 进程的自治系统 (AS) 编号。AS 编号包含多个自主编号。AS 编号可从 1 到 65535, 并且是分配的唯一值, 用于在互联网上标识各个网络。
- 步骤 6** 要配置其他 EIGRP 属性, 请参阅以下主题:
1. [配置 EIGRP 设置, 第 4 页。](#)
 2. [配置 EIGRP 邻居设置, 第 5 页。](#)
 3. [配置 EIGRP 过滤器规则设置, 第 5 页。](#)
 4. [配置 EIGRP 重新分发设置, 第 6 页。](#)
 5. [配置 EIGRP 摘要地址设置, 第 7 页。](#)
 6. [配置 EIGRP 接口设置, 第 7 页。](#)
 7. [配置 EIGRP 高级设置, 第 8 页。](#)
-

配置 EIGRP 设置

过程

- 步骤 1** 在 **EIGRP** 页面上, 点击**设置 (Setup)** 选项卡。
- 步骤 2** 点击**自动汇总 (Auto Summary)** 复选框, 使 EIGRP 能够汇总网络编号边界。
- 注释** 如果存在非连续网络, 启用自动汇总这可能会引起路由问题。
- 步骤 3** 在**可用网络/主机 (Available Networks/Hosts)** 框中, 点击应参与 EIGRP 路由进程的网络或主机, 然后点击**添加 (Add)**。要添加新的网络对象, 请点击 **添加 (+)**。有关添加网络的过程, 请参阅[网络](#)。
- 步骤 4** 要配置被动接口, 请点击**被动接口 (Passive Interface)** 复选框。在 EIGRP 中, 被动接口既不发送也不接收路由更新。
- a) 要将选择性接口指定为被动接口, 请点击**选定接口 (Selected Interface)** 单选按钮。在**可用接口 (Available Interfaces)** 框中, 选择接口, 然后点击**添加 (Add)**。
 - b) 要将所有接口指定为被动, 点击**所有接口 (All Interfaces)** 单选按钮。

步骤 5 点击**确定 (Ok)** 和**保存 (Save)** 以保存这些设置。

配置 EIGRP 邻居设置

您可以为 EIGRP 进程定义静态邻居。在手动定义 EIGRP 邻居时，Hello 数据包会单播至该邻居。

过程

步骤 1 在 **EIGRP** 页面上，点击**邻居 (Neighbors)** 选项卡。

步骤 2 点击**添加 (Add)**。

步骤 3 从**接口 (Interface)** 下拉列表中选择可通过其访问邻居的接口。

步骤 4 从**邻居 (Neighbor)** 下拉列表中选择静态邻居的 IP 地址。要添加网络对象，请点击**添加 (+)**。有关添加网络对象的过程，请参阅[网络](#)。

步骤 5 点击**确定 (Ok)** 和**保存 (Save)** 以保存这些设置。

配置 EIGRP 过滤器规则设置

您可以为 EIGRP 路由进程配置路由过滤规则。过滤规则让您能够控制 EIGRP 路由进程接受或通告的路由。

过程

步骤 1 在 **EIGRP** 页面上，点击**过滤器规则 (Filter Rules)** 选项卡。

步骤 2 请点击**添加 (+)**。

步骤 3 在**添加过滤器规则 (Add Filter Rules)** 对话框中，从**过滤器方向 (Filter Direction)** 下拉列表中选择规则的方向：

- 入站 (Inbound) - 规则过滤来自传入 EIGRP 路由更新的默认路由信息。
- 出站 (Outbound) - 规则过滤来自传出 EIGRP 路由更新的默认路由信息。

步骤 4 要选择应用过滤规则的接口，请点击**接口 (Interface)** 单选按钮，然后从下拉列表中选择接口。

步骤 5 要选择应用过滤规则的协议，请点击**协议 (Protocol)** 单选按钮，然后从下拉列表中选择协议 - BGP、RIP、静态、已连接或 OSPF。对于 BGP 和 OSPF 协议，您可以指定相关的进程 ID。

步骤 6 从**访问列表 (Access List)** 下拉列表中选择访问列表。此列表定义了要在路由更新中接收的网络和要抑制的网络。若要添加新的标准访问列表对象，请点击**添加 (+)** 并参阅[配置标准 ACL 对象](#)了解详细程序。

步骤 7 点击确定 (Ok) 和保存 (Save) 以保存这些设置。

配置 EIGRP 重新分发设置

您可以定义将来自其他路由协议的路由重新分发到 EIGRP 路由进程的规则

过程

步骤 1 在 EIGRP 页面上，点击重新分配 (Redistribution) 选项卡。

步骤 2 请点击添加 (+)。

步骤 3 在添加重新分配 (Add Redistribution) 对话框中，从协议 (Protocol) 下拉列表选择要从其重新分配路由的源协议：

- BGP - 将 BGP 路由进程发现的路由重新分配给 EIGRP。
- RIP - 将 RIP 路由进程发现的路由重新分配给 EIGRP。
- 静态 - 将静态路由重新分布到 EIGRP 路由过程中。位于 network 语句范围内的静态路由会自动重新分发到 EIGRP；不需要为其定义重新分发规则。
- 已连接 - 将已连接路由（通过在接口上启用 IP 地址自动建立的路由）重新分发到 EIGRP 路由进程。位于 network 语句范围内的已连接路由会自动重新分发到 EIGRP；不需要为其定义重新分发规则。
- OSPF - 将由 OSPF 路由进程发现的路由重新分发到 EIGRP。如果选择此协议，则此对话框中的“匹配” (Match) 选项将在可选 OSPF 重新分配 (Optional OSPF Redistribution) 下变得可见：
 - 内部 - 特定 AS 的内部路由。
 - External1 - AS 外部的路由，会作为 1 类外部路由导入 OSPF。
 - External2 - AS 外部的路由，会作为第 2 类外部路由导入所选进程。
 - Nsaa-External1 - AS 外部的路由，会作为第 1 类外部路由导入所选进程的次末节区域 (NSSA)。
 - Nsaa-External2 - AS 外部的路由，会作为第 2 类外部路由导入所选进程的 (NSSA)。

注释 当重新分发静态、已连接、RIP 或 BGP 路由时，这些选项不可用。

步骤 4 在可选指标 (Optional Metrics) 下输入相关值：

- 带宽 (Bandwidth) - 路由的最小带宽（以千比特/秒为单位）。有效值范围为 1 到 4294967295。
- 延迟时间 (Delay Time) - 路由延迟（以十微秒为单位）。有效值范围为 0 到 4294967295。
- 可靠性 (Reliability) - 数据包成功传输的可能性（以 0 到 255 的数字表示）。值 255 表示 100% 可靠；0 表示不可靠。

- **正在加载 (Loading)** - 路由的有效带宽。有效值范围为 1 到 255。255 表示 100% 加载。
- **MTU** - 路径的最大传输单位允许的最小值。有效值范围为 1 到 65535。

步骤 5 从路由地图 (**Route Map**) 下拉列表中选择要应用于重新分配条目的路由映射。要创建新的路由映射对象，请点击 **添加 (+)**。请参阅程序的 [配置路由映射条目](#) 以添加新的路由映射。

步骤 6 点击 **确定 (Ok)** 和 **保存 (Save)** 以保存这些设置。

配置 EIGRP 摘要地址设置

您可以为每个接口配置汇总地址。如果要创建不会出现在网络边界上的汇总地址，或者要在自动路由汇总禁用的情况下在威胁防御上使用汇总地址，则需要手动定义汇总地址。如果路由表中有任何更具体的路由，则 EIGRP 会使用与所有更具体路由的最小值相等的指标来通告汇总地址。

过程

步骤 1 在 **EIGRP** 页面上，点击 **汇总地址 (Summary Address)** 选项卡。

步骤 2 点击 **添加 (Add)**。

步骤 3 从 **接口 (Interface)** 下拉列表中，选择从其通告汇总地址的接口。

步骤 4 从 **网络 (Network)** 下拉列表中，选择具有要汇总的特定 IP 地址和网络掩码的网络对象。要添加新的网络，请点击 **添加 (+)**。有关添加网络的过程，请参阅 [网络](#)。

步骤 5 在“管理距离” (**Administrative Distance**) 字段中，输入汇总路由的管理距离。有效值范围为 1 到 255。

步骤 6 点击 **确定 (Ok)** 和 **保存 (Save)** 以保存这些设置。

配置 EIGRP 接口设置

您可以在“接口” (**Interfaces**) 选项卡中配置接口特定的 EIGRP 路由属性。

过程

步骤 1 在 **EIGRP** 页面上，点击 **接口 (Interfaces)** 选项卡。

步骤 2 请点击 **添加 (+)**。

步骤 3 从 **接口 (Interface)** 下拉列表中，选择要应用配置的接口的名称。

步骤 4 在 **Hello 间隔 (Hello Interval)** 字段中，输入在接口上发送 EIGRP 呼叫数据包的间隔（以秒为单位）。有效值范围为 1 到 65535。默认值为 5 秒。

步骤 5 在 **保持时间 (Hold Time)** 字段中，输入设备在 EIGRP Hello 数据包中进行通告的保持时间。有效值范围为 3 到 65535。默认值为 15 秒。

步骤 6 要在接口上启用 EIGRP 水平分割，请点击**水平分割 (Split Horizon)** 复选框。

步骤 7 在**延迟时间 (Delay Time)** 字段中输入延迟时间，以十微秒为单位。有效值范围为 1 至 16777215。在多情景模式下，设备不支持此选项。

步骤 8 指定身份验证属性的值：

- **启用 MD5 身份验证 (Enable MD5 Authentication)** - 点击此复选框可使用 MD5 散列算法对 EIGRP 数据包进行身份验证。
- **密钥类型 (Key Type)** - 从下拉列表中选择以下任一密钥类型：
 - “无” (None) - 表示无需身份验证。
 - “未加密” (Unencrypted) - 指示要使用的密钥字符串是用于身份验证的明文密码。
 - “已加密” (Encrypted) - 指示要使用的密钥字符串是用于身份验证的加密密码。
 - “身份验证密钥” (Auth Key) - 指示要使用的密钥字符串是 EIGRP 身份验证密钥。
- **密钥 ID (Key ID)** - 用于对 EIGRP 更新进行身份验证的密钥的 ID。输入数字密钥标识符。有效值范围为 0 到 255。
- **密钥 (Key)** - 最多包含 17 个字符的字母数字字符串。对于加密身份验证类型，此字段应至少包含 17 个字符。
- **确认密钥 (Confirm Key)** - 重新输入密钥。

步骤 9 点击**确定 (Ok)** 和**保存 (Save)** 以保存这些设置。

配置 EIGRP 高级设置

您可以配置 EIGRP 高级设置，例如路由器 ID、末节路由和邻接更改。

过程

步骤 1 在 **EIGRP** 页面上，点击**高级 (Advanced)** 选项卡。

步骤 2 在默认路由器信息 (**Default Route Information**) 下，您可以指定 EIGRP 更新中默认路由信息的发送和接收。

- **路由器 ID (IP 地址) (Router ID [IP Address])** - 输入用于标识外部路由的始发路由器的 ID。如果收到的外部路由具有本地路由器 ID，该路由将被丢弃。要防止出现此问题，请为路由器 ID 指定全局地址。应该为每台 EIGRP 路由器配置一个唯一值。
- **接受默认路由信息 (Accept Default Route Info)** - 点击此复选框可将 EIGRP 配置为接受外部默认路由信息。

- **访问列表 (Access List)** - 从访问列表 (**Access List**) 下拉列表中，指定一个标准访问列表，该列表定义接收默认路由信息时允许的网络和不允许的网络。若要添加新的标准访问列表对象，请点击 **添加 (+)** 并参阅 [配置标准 ACL 对象](#) 了解详细程序。
- **发送默认路由信息 (Send Default Route Info)** - 点击此复选框可将 EIGRP 配置为通告外部默认路由信息。
- **访问列表 (Access List)** - 从访问列表 (**Access List**) 下拉列表中，指定一个标准访问列表，该列表定义发送默认路由信息时允许的网络和不允许的网络。若要添加新的标准访问列表对象，请点击 **添加 (+)** 并参阅 [配置标准 ACL 对象](#) 了解详细程序。

步骤 3 在**管理距离 (Administrative Distance)** 下，指定：

- **内部距离 (Internal Distance)** - EIGRP 内部路由的管理距离。内部路由是从同一自主系统中的其他实体学习的路由。有效值范围为 1 到 255。默认值为 90。
- **外部距离 (External Distance)** - EIGRP 外部路由的管理距离。外部路由是为其从自主系统外部的邻居学习最佳路径的路由。有效值范围为 1 到 255。默认值为 170。

步骤 4 在**邻接更改 (Adjacency Changes)** 下，指定：

- **记录邻居更改 (Log Neighbor Changes)** - 点击此复选框可启用 EIGRP 邻居邻接更改的日志记录。
- **记录邻居警告 (Log Neighbor Warnings)** - 点击此复选框可启用 EIGRP 邻居警告消息的日志记录。
- (可选) 输入重复的邻居警告消息之间的时间间隔 (以秒为单位)。有效值范围为 1 到 65535。系统不会记录在此间隔期间重复出现的警告。

步骤 5 在**末节 (Stub)** 下，要启用设备作为 EIGRP 末节路由进程，请选中以下一个或多个 EIGRP 末节路由进程复选框：

- “**仅接收 (Receive only)**” - 将 EIGRP 末节路由进程配置为接收来自相邻路由器的路由信息，但不向邻居发送路由信息。如果选中此选项，则不能选择任何其他末节路由选项。
- “**已连接 (Connected)**” - 通告已连接路由。
- “**已重新分发 (Redistributed)**” - 通告重新分发的路由。
- “**静态 (Static)**” - 通告静态路由。
- “**汇总 (Summary)**” - 通告汇总路由。

步骤 6 在**默认指标 (Default Metrics)** 下，定义重分布到 EIGRP 路由进程中的路由的默认指标：

- “**带宽 (Bandwidth)**” - 路由的最小带宽 (以千比特/秒为单位)。有效值范围为 1 到 4294967295。
- “**延迟时间 (Delay Time)**” - 路由延迟 (以十微秒为单位)。有效值范围为 0 到 4294967295。
- “**可靠性 (Reliability)**” - 数据包成功传输的可能性 (以 0 到 255 的数字表示)。值 255 表示 100% 可靠；0 表示不可靠。

- “正在加载” (Loading) - 路由的有效带宽。有效值范围为 1 到 255；255 表示已 100% 加载。
 - MTU - 路径的最大传输单位允许的最小值，以字节表示。有效值范围为 1 到 65535。
-

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。