



ECMP

本章介绍配置等价多路径 (ECMP) 路由的程序，该路由协议用于网络流量负载均衡。

- [关于 ECMP，第 1 页](#)
- [ECMP 的准则和限制，第 1 页](#)
- [管理 ECMP 页面，第 3 页](#)
- [创建 ECMP 区域，第 3 页](#)
- [配置等价静态路由，第 4 页](#)
- [修改 ECMP 区域，第 5 页](#)
- [删除 ECMP 区域，第 6 页](#)
- [ECMP 的配置示例，第 6 页](#)
- [Cisco Secure Firewall Threat Defense 中的 ECMP 的历史记录，第 10 页](#)

关于 ECMP

Firepower 威胁防御设备支持等价多路径 (ECMP) 路由。您可以将每个虚拟路由器的流量区域配置为包含一组接口。您可以在每个区域中最多跨 8 个接口配置最多 8 个等价静态或动态路由。例如，您可以在区域中跨三个接口配置多个默认路由：

```
route for 0.0.0.0 0.0.0.0 through outside1 to 10.1.1.2
route for 0.0.0.0 0.0.0.0 through outside2 to 10.2.1.2
route for 0.0.0.0 0.0.0.0 through outside3 to 10.3.1.2
```

ECMP 的准则和限制

防火墙模式指导原则

ECMP 区域仅在路由防火墙模式下支持。

设备准则

- 威胁防御 6.5 及更高版本的设备支持在 **管理中心** 中配置 ECMP 流量区域：

- 版本 6.6 及更高版本的 威胁防御 设备支持每个虚拟路由器的 ECMP。
- 威胁防御 6.5 版设备或更早设备不支持虚拟路由，您可以将全局接口与 ECMP 相关联。
- 一台设备最多可以有 256 个 ECMP 区域。

接口指导原则

- 可以在全局虚拟路由器和用户定义的虚拟路由器中创建 ECMP 区域。
- 只有路由接口才能与 ECMP 区域相关联。
- 只有具有逻辑名称的接口才能与 ECMP 区域相关联。
- 接口应属于在上面创建 ECMP 的虚拟路由器。
- 每个 ECMP 区域只能关联 8 个接口。
- 接口只能是一个 ECMP 区域的成员。
- 不能从 ECMP 区域中删除与等价静态路由相关联的接口。
- 如果 ECMP 区域的接口具有与其关联的等价静态路由，则您无法删除该区域。
- 对于 7.1 之前的 威胁防御 版本，sVTI 接口不能用于 ECMP 区域。
- 对于 7.1 之前的 威胁防御 版本，站点间 VPN 或远程访问 IPsec-IKEv2 VPN 中不支持 ECMP 区域成员接口。
- 以下接口不能与 ECMP 区域相关联：
 - BVI 接口。
 - EtherChannel 中的成员接口。
 - 故障转移或状态链路接口。
 - 管理专用接口或管理访问接口。
 - 集群控制链路接口。
 - 冗余接口及其成员。
 - VNI。
 - VLAN 接口。
 - 已启用 SSL 的 RA VPN 配置中的接口。

升级指南

升级自 管理中心 7.0 或更早版本时，现有的 ECMP FlexConfig 不会被部署到设备。因此，要成功部署，您必须在 UI 中将 FlexConfig 流量区域手动迁移到 ECMP。

您可以从管理中心 UI 为所有 6.5 及更高版本的路由设备创建 ECMP。

其他规定

- DHCP 中继 - 不在与 ECMP 区域关联的接口上启用 DHCP 中继。
- 双 ISP/WAN 威胁防御部署 - 为主数据接口和辅助数据接口创建单个 ECMP 区域。此配置允许为具有相同指标值的两个接口创建静态路由。
- 威胁防御不支持在 IPsec 会话中使用 NAT 的 ECMP - 标准 IPsec 虚拟专用网络 (VPN) 隧道不适用于 IPsec 数据包传送路径中的 NAT 点。

管理 ECMP 页面

当您点击“路由”(Routing)窗格中的 **ECMP** 时，系统将显示与虚拟路由器对应的 ECMP 页面。此页面将显示现有 ECMP 区域以及虚拟路由器的关联接口。在此页面中，您可以将 ECMP 区域添加到虚拟路由器。您还可以 **编辑** (✎) 和 **删除** (🗑️) ECMP。

您可以执行以下操作：

- [创建 ECMP 区域，第 3 页](#)
- [配置等价静态路由，第 4 页](#)
- [修改 ECMP 区域，第 5 页](#)
- [删除 ECMP 区域，第 6 页](#)

创建 ECMP 区域

ECMP 区域会按虚拟路由器来创建。因此，只有创建 ECMP 的虚拟路由器的接口才能与 ECMP 相关联。

过程

步骤 1 依次选择 **设备 > 设备管理**，并且编辑 威胁防御设备。

步骤 2 点击 **路由**。

步骤 3 在虚拟路由器下拉列表中，选择要在其中创建 ECMP 区域的虚拟路由器。

您可以在全局虚拟路由器和用户定义的虚拟路由器中创建 ECMP 区域。有关创建虚拟路由器的信息，请参阅 [创建虚拟路由器](#)。

步骤 4 点击 **ECMP**。

步骤 5 点击添加 (**Add**)。

步骤 6 在添加 **ECMP (Add ECMP)** 框中，输入 ECMP 区域的名称。

注释 路由设备的 ECMP 名称必须是唯一的。

步骤 7 要关联接口，请在可用接口 (**Available Interfaces**)框下选择接口，然后点击添加 (**Add**)。

请记住以下几点：

- 只有属于虚拟路由器的接口可供分配。
- 可用接口框下仅列出具有逻辑名称的接口。您可以编辑接口并在接口中提供逻辑名称。请记住保存更改，以使设置生效。

步骤 8 点击确定 (**OK**)。

ECMP 页面现在会显示新创建的 ECMP。

步骤 9 点击保存 (**Save**) 和部署 (**Deploy**) 以部署配置。

通过为其定义相同的目标和指标值但使用不同的网关，您可以将 ECMP 区域接口与等价静态路由相关联。

下一步做什么

- [配置等价静态路由，第 4 页](#)
- [修改 ECMP 区域，第 5 页](#)
- [删除 ECMP 区域，第 6 页](#)

配置等价静态路由

智能许可证	经典许可证	支持的设备	支持的域	访问权限
Any	不适用	威胁防御和threat defense virtual	Any	管理员/网络管理员/安全审批人

您可以将虚拟路由器的接口（全局和用户定义）分配给设备的 ECMP 区域。

开始之前

- 要为接口配置等价静态路由，请确保将其与 ECMP 区域关联。请参阅[创建 ECMP 区域，第 3 页](#)。
- 非 VRF 设备的所有路由配置设置也可用于全局虚拟路由器。
- 如果没有将接口与 ECMP 区域关联，则无法为具有相同目标和指标的接口定义静态路由。

过程

- 步骤 1** 在设备 (Devices) > 设备管理 (Device Management) 页面中，编辑威胁防御设备。点击路由 (Routing) 选项卡。
- 步骤 2** 从下拉列表中，选择其接口与 ECMP 区域相关联的虚拟路由器。
- 步骤 3** 要为接口配置等价静态路由，请点击静态路由 (Static Route)。
- 步骤 4** 点击添加路由 (Add Route) 以添加新路由，或点击现有路由的编辑 (✎)。
- 步骤 5** 从接口 (Interface) 下拉列表中，选择属于虚拟路由器的接口和 ECMP 区域。
- 步骤 6** 从可用网络 (Available Networks) 框中选择目标网络，然后点击添加 (Add)。
- 步骤 7** 输入网络的网关。
- 步骤 8** 输入指标值。它可以是介于 1 和 254 之间的数字。
- 步骤 9** 要保存设置，点击保存 (Save)。
- 步骤 10** 要配置等价静态路由，请重复上述步骤，为同一 ECMP 区域中具有相同目的网络和指标值的另一个接口配置静态路由。请记住提供其他网关。

下一步做什么

- [修改 ECMP 区域，第 5 页](#)
- [删除 ECMP 区域，第 6 页](#)

修改 ECMP 区域

过程

- 步骤 1** 依次选择设备 > 设备管理，然后编辑 FTD 设备。
- 步骤 2** 点击路由。
- 步骤 3** 点击 ECMP。
ECMP 区域及其关联的接口会显示在 ECMP 页面中。
- 步骤 4** 要修改 ECMP，请根据所需的 ECMP 点击编辑 (✎)。在编辑 ECMP (Edit ECMP) 框中，您可以执行以下操作：
 - ECMP 名称 (ECMP Name) - 确保更改的名称对于设备是唯一的。
 - 接口 (Interfaces) - 您可以添加或删除接口。您不能包含已与其他 ECMP 关联的接口。此外，您不能删除与等价静态路由关联的接口。
- 步骤 5** 单击确定 (OK)。

步骤 6 要保存更改，请点击**保存**。

下一步做什么

- [配置等价静态路由，第 4 页](#)
- [删除 ECMP 区域，第 6 页](#)

删除 ECMP 区域

过程

步骤 1 依次选择**设备 > 设备管理**，然后编辑 FTD 设备。

步骤 2 点击**路由**。

步骤 3 点击 **ECMP**。

ECMP 区域及其关联的接口会显示在 **ECMP** 页面中。

步骤 4 要删除 ECMP 区域，请点击 ECMP 区域旁的 **删除** (🗑)。

如果 ECMP 区域的任何接口与等价静态路由关联，则您无法删除该区域。

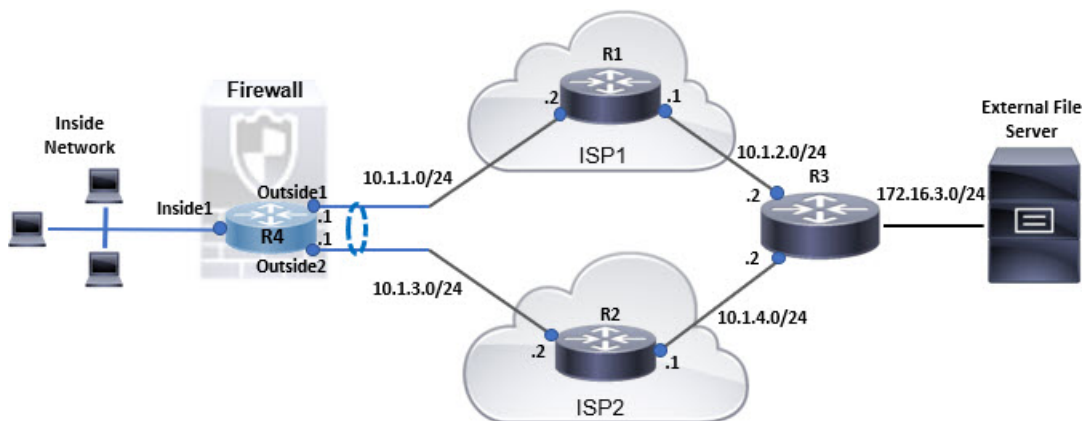
步骤 5 在确认邮件中单击**删除 (Delete)**。

步骤 6 要保存更改，请点击**保存**。

ECMP 的配置示例

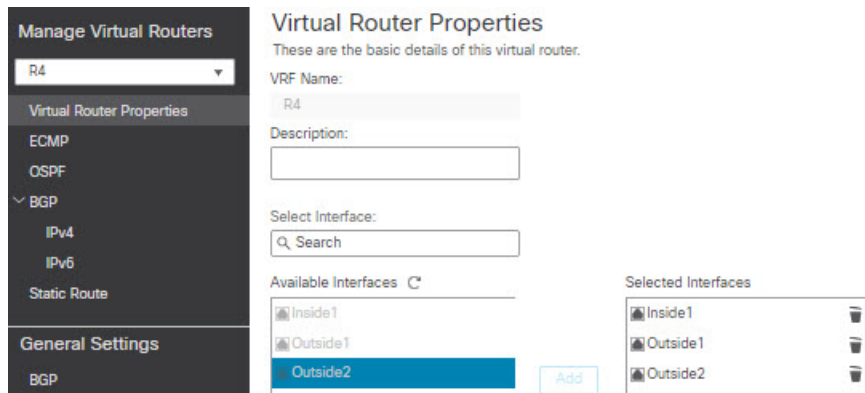
此示例演示了如何使用 **管理中心** 在 **威胁防御** 上配置 ECMP 区域，以便有效地处理流经设备的流量。如果配置了 ECMP，**威胁防御** 会维护每个区域的路由表，因此可以在最佳路由中重新路由数据包。因此，ECMP 支持非对称路由、负载均衡并无缝处理丢失的流量。在本例中，R4 会记录到达外部文件服务器的两个路径。

图 1: ECMP 的配置示例



过程

步骤 1 创建虚拟路由器 (Create virtual router) - 包含 *Inside1*、*Outside1* 和 *Outside2* 接口的 *R4*:

图 2: 配置 *R4* 虚拟路由器

步骤 2 创建 ECMP 区域:

- 在路由 (**Routing**) 选项卡中, 选择 *R4* 用户定义的虚拟路由器, 然后点击 **ECMP**。
- 单击添加。
- 输入 ECMP 名称, 然后从可用接口 (**Available Interfaces**) 列表中选择 *Outside1* 和 *Outside2*:

图 3: 创建 ECMP 区域

Add ECMP

Name
ECMP-R4

Associate Interfaces with ECMP
You can add interfaces to this ECMP by clicking on Add button. ECMP can have up to 8 interfaces associated with it. All the interfaces in the ECMP must have a name and security level as this ECMP.

Available Interfaces
Inside1

Add

Selected Interfaces
Outside1
Outside2

Cancel OK

d) 点击确定 (Ok), 然后点击保存 (Save)。

步骤 3 为区域接口创建静态路由:

- 在路由 (**Routing**) 选项卡中, 点击静态路由 (**Static Route**)。
- 在接口 (**Interface**) 下拉列表中, 选择 Outside1。
- 在可用网络 (**Available Network**) 下, 选择 any-ipv4, 然后点击添加 (**Add**)。
- 在网关 (**Gateway**) 字段 10.1.1.2 中指定下一跳地址:

图 4: 为 *Outside1* 配置静态路由

Add Static Route Configuration

Type: IPv4 IPv6

Interface*
Outside1

(Interface starting with this icon signifies it is available for route leak)

Available Network +
Q Search

- any-ipv4
- IPv4-Benchmark-Tests
- IPv4-Link-Local
- IPv4-Multicast
- IPv4-Private-10.0.0.0-8
- IPv4-Private-172.16.0.0-11

Add

Selected Network
any-ipv4

Gateway*
10.1.1.2 +

Metric:
1
(1 - 254)

Tunneled: (Used only for default Route)

Route Tracking:
+

Cancel OK

e) 为 *Outside2* 配置静态路由，重复步骤 3b 到步骤 3d。

确保为静态路由指定相同的指标，但要使用不同的网关：

图 5: 已配置的 *ECMP* 区域接口静态路由

+ Add Route

Network [▲]	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked
▼ IPv4 Routes						
any-ipv4	Outside1		10.1.1.2	false	1	
any-ipv4	Outside2		10.1.3.2	false	1	
▼ IPv6 Routes						

步骤 4 保存 (Save) 和部署 (Deploy)。

根据 ECMP 算法，到达目的地 R3 的网络数据包会遵循 R4>R1>R3 或 R4>R2>R3。如果 R1>R3 路由丢失，流量将流经 R2，而不会丢弃任何数据包。类似地，虽然数据包是从 *outside1* 发送的，但来自 R3 的响应可被 *outside2* 接收。此外，当网络流量很大时，R4 会在两条路由之间分配流量，从而均衡负载。

Cisco Secure Firewall Threat Defense中的 ECMP 的历史记录

特性	Version	最低 威胁防御	详细信息
ECMP 支持作为路由策略	7.1	任意	<p>Cisco Secure Firewall Threat Defense 通过 FlexConfig 策略支持 ECMP 路由。在此版本中，您可以将接口分组到流量区域，并在 Cisco Secure Firewall Management Center 中配置 ECMP 路由。</p> <p>新增/修改的屏幕：设备 (Devices) > 设备管理 (Device Management) > 路由 (Routing) > ECMP</p>

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。