路由基础知识和静态路由

系统使用路由表来确定进入系统的数据包的传出接口。以下主题介绍路由的基本信息以及如何在设备上配置静态路由。

路由最佳实践

在网络中设计路由进程的过程可能十分复杂。本章假定您将威胁防御设备配置为可在现有网络中工作，并参与已在网络中建立的路由进程。

如果要创建新网络，请花时间阅读从其他位置获取的有关路由协议及如何设计适用于您网络的有效路由计划的信息。本章不介绍关于如何选择协议的建议，也不介绍协议的工作方式。

如果网络非常小，而且您只向上链接到ISP，则可能只需要一些静态路由即可，根本不需要实现路由协议。

但是，如果要建立含许多路由器的大型网络，则可能需要为内部路由至少实现一种路由协议（例如OSPF），为外部路由至少实现一种路由协议（例如BGP）。服务提供商可帮助您了解可能需要的外部路由（如果有）。如果是这种情况，请首先了解使用 威胁防御可以配置的路由协议，然后规划网络，最后根据计划来配置 威胁防御 设备。

路由概述

以下主题介绍路由在威胁防御设备中的运行方式。所谓路由是指通过网络将信息从源发送到目标的活动。在途中通常会经过至少一个中间节点。路由涉及两个基本活动：确定最佳路由路径和通过网络传输数据包。

支持的路由协议

下表介绍可使用 设备管理器在 威胁防御 设备上配置的路由协议和技术，以及完成配置所需的方法。

表 *1:* 支持的路由协议

路由功能	配置方法	说明
BGP	Smart CLI	从**设备 (Device)** > **路由 (Routing)** 页面中配置 BGP Smart CLI 对象。 使用**设备 (Device)** > **高级配置 (Advanced Configuration)**页面中的 Smart CLI 对象配置 BGP 中使用的对象，例如路由映射。
双向转发检测 (BFD)	FlexConfig	从**设备 (Device)** > **高级配置 (Advanced Configuration)**页面中使用 FlexConfig 对象配置 BFD。仅 BGP 支持 BFD。
EIGRP	Smart CLI	在**设备 (Device)** > **路由 (Routing)**页面中配置 EIGRP Smart CLI 对象。 使用**设备 (Device)** > **高级配置 (Advanced Configuration)**页面中的 Smart CLI 对象配置 EIGRP 中使用的对象（例如路由映射）。
IS-IS	FlexConfig	使用**设备 (Device)** > **高级配置 (Advanced Configuration)**页面的 FlexConfig 对象配置 IS-IS。
组播路由	FlexConfig	使用**设备 (Device)** > **高级配置 (Advanced Configuration)** 页面中的 FlexConfig 对象配置组播路由。
OSPFv2	Smart CLI	使用**设备 (Device)** > **路由 (Routing)** 页面中的 Smart CLI 对象配置 OSPFv2。 使用**设备 (Device)** > **高级配置 (Advanced Configuration)** 页面中的 Smart CLI 对象配置 OSPFv2 中使用的对象，例如路由映射。
OSPFv3	—	不支持 OSPFv3 配置。
基于策略的路由 (PBR)	FlexConfig	使用**设备 (Device)** > **高级配置 (Advanced Configuration)** 页面中的 FlexConfig 对象配置基于策略的路由 (PBR)。
RIP	FlexConfig	使用**设备 (Device)** > **高级配置 (Advanced Configuration)**页面中的 FlexConfig 对象配置 RIP。
静态路由	设备管理器	从**设备 (Device)** > **路由 (Routing)** 页面全局地或针对每个虚拟路由器配置静态路由。
虚拟路由器，VRF	设备管理器	从**设备 (Device)** > **路由 (Routing)** 页面配置虚拟路由器。

路由类型

主要有两种类型的路由：静态路由或动态路由。

静态路由是明确定义的路由。它们相对稳定且通常具有高优先级，用于确保将发往路由目标的流量发送到正确的接口。例如，您可以创建一个默认静态路由，用于覆盖尚未被任何其他路由覆盖的所有流量，即 IPv4 的 0.0.0.0/0 或 IPv6 的 ::/0。另一个示例是指向您经常使用的内部系统日志服务器的静态路由。

动态路由是从路由协议（如 OSPF、BGP、EIGRP、IS-IS 或 RIP）的操作中习得的路由协议，您不用直接定义这类路由。相反，您配置路由协议，然后系统与邻居路由器进行通信，传输并接收路由更新。

动态路由协议通过分析收到的路由更新消息调整路由表，使其适应不断变化的网络环境。如果有消息表明网络发生更改，则系统会重新计算路由并发出新的路由更新消息。这些消息会渗入网络，促使路由器重新运行其算法并相应地更改其路由表。

静态路由非常简单，发挥基本路由的作用，在网络流量相对可预测且网络设计相对简单的环境中十分适用。但是，静态路由不能更改（除非您编辑它们），因此它们不能应对网络中的更改。

除非您有一个小型网络，否则您通常会将静态路由和一个或多个动态路由协议搭配使用。您将定义至少一个静态路由，作为不匹配显式路由的流量的默认路由。

注释 可以使用 Smart CLI 配置以下路由协议：OSPF、BGP。使用 FlexConfig 配置 ASA 软件支持的其他路由协议。

路由表和路由选择

如果 NAT 转换 (xlates) 和规则无法确定传出接口，系统将使用路由表来确定数据包的路径。

路由表中的路由包括一个名为“管理距离”的指标，提供相对于既定路由的优先级。如果某个数据包与多个路由条目匹配，则使用距离最短的路由。直连网络（在接口上定义的网络）的距离为 0，因此始终首选使用此网络。静态路由的默认距离为 1，但您可以使用 1-254 之间的任意距离创建默认距离。

标识具体目标的路由优先于默认路由（即目标为 0.0.0.0/0 或 ::/0 的路由）。

路由表的填充方式

威胁防御路由表可以通过静态定义的路由、直连路由以及动态路由协议发现的路由来填充。由于威胁防御 设备除具有路由表中的静态路由和已连接路由外，还可以运行多条路由协议，因此可通过多种方式发现或输入同一路由。当在路由表中放入同一目标的两条路由时，将按如下确定保留在路由表中的路由：

- 如果两个路由具有不同的网络前缀长度（网络掩码），则会将两个路由都视为唯一并输入到路由表中。然后，由数据包转发逻辑确定使用哪一条路由。

  例如，如果 RIP 和 OSPF 进程发现以下路由：

- RIP：192.168.32.0/24
- OSPF：192.168.32.0/19

即使 OSPF 路由具有更好的管理距离，但由于两条路由具有不同的前缀长度（子网掩码），因此均会安装在路由表中。这两条路由被视为不同目标，数据包转发逻辑会确定使用哪条路由。

- 如果 威胁防御 设备从单个路由协议（例如 RIP）获悉通向同一目标的多条路径，则会在路由表中输入具有更佳指标的路由（由路由协议确定）。

  度量是与特定路由关联的值，从最高优先到最低优先进行排序。用于确定度量的参数根据路由协议而异。具有最低指标的路径选择作为最佳路径并安装在路由表中。如果有多个度量相等的通向同一目的地的路径，则会在这些等价路径上进行负载均衡。

- 如果 威胁防御 设备从多个路由协议获悉目标，则会比较路由的管理距离，并在路由表中输入管理距离较短的路由。

路由的管理距离

您可以更改由路由协议发现或重分发到路由协议中的路由的管理距离。如果来自两个不同路由协议的两条路由具有相同的管理距离，则会将具有较短默认管理距离的路由输入到路由表中。对于EIGRP和 OSPF 路由，如果 EIGRP 路由和 OSPF 路由具有相同的管理距离，则默认选择 EIGRP 路由。

管理距离是 威胁防御设备在有两个或多个通向同一目标（来自两个不同路由协议）的路由时，用于选择最佳路径的路由参数。由于路由协议具有基于不同于其他协议的算法的度量，因此并非总能够确定通向由不同路由协议生成的同一目的地的两条路由的最佳路径。

每个路由协议使用管理距离值划分优先级。下表显示 威胁防御设备支持的路由协议的默认管理距离值。

表 *2:* 受支持的路由协议的默认管理距离

路由源	默认管理距离
已连接的接口	0
VPN 路由	1
静态路由	1
EIGRP 汇总路由	5
外部 BGP	20
内部 EIGRP	90
OSPF	110
IS-IS	115
RIP	120

路由源	默认管理距离
EIGRP 外部路由	170
内部和本地 BGP	200
未知	255

管理距离值越小，协议的优先等级越高。例如，如果 威胁防御设备从 OSPF 路由进程（默认管理距离 - 110）和 RIP 路由进程（默认管理距离 - 120）均收到通向特定网络的路由，则 威胁防御设备 会选择 OSPF 路由，因为 OSPF 具有更高的优先级。在这种情况下，路由器会将 OSPF 版本的路由添加到路由表。

VPN 通告路由 (V-Route/RRI)）相当于默认管理距离为 1 的静态路由。但与网络掩码 255.255.255.255 一样，它具有更高的优先级。

在本示例中，如果 OSPF 派生路由的源丢失（例如，由于电源关闭），则 威胁防御设备会使用 RIP 派生路由，直至 OSPF 派生路由再次出现。

管理距离是一项本地设置。例如，如果您更改通过 OSPF 获取的路由的管理距离，那么这种更改只会影响在其上输入该命令的 威胁防御设备的路由表。在路由更新中不会通告管理距离。

管理距离不影响路由进程。路由进程仅通告路由进程已发现或重分发到路由进程中的路由。例如，即使在 路由表中使用 OSPF 路由进程发现的路由，RIP 路由进程也会通告 RIP 路由。

备份动态和浮动静态路由

当由于安装另一条路由而导致初始尝试将路由安装在路由表中失败时，系统会注册备用路由。如果安装在路由表中的路由失败，则路由表维护进程会呼叫已注册备用路由的每个路由协议进程，并请求它们重新在路由表中安装此路由。如果有多个协议为失败路由注册了备用路由，则根据管理距离选择优先路由。

鉴于以上过程，当动态路由协议发现的路由失败时，您可以创建安装在路由表中的浮动静态路由。浮动静态路仅仅是配置有比 威胁防御设备上运行的动态路由协议更大的管理距离的静态路由。当动态路由进程发现的对应路由失败时，会在路由表中安装静态路由。

如何制定转发决策

系统按如下制定转发决策：

- 如果目的不匹配路由表中的条目，则通过为默认路由指定的接口转发数据包。如果尚未配置默认路由，则会丢弃数据包。
- 如果目的匹配路由表中的单个条目，则通过与该路由关联的接口转发数据包。
- 如果目的匹配路由表中的多个条目，则通过与具有较长网络前缀的路由相关联的接口转发数据包。

例如，发往 192.168.32.1 的数据包到达在路由表中拥有以下路由的接口：

- 192.168.32.0/24 网关 10.1.1.2

- 192.168.32.0/19 网关 10.1.1.3

在这种情况下，发往 192.168.32.1 的数据包直接发送到 10.1.1.2，因为 192.168.32.1 属于 192.168.32.0/24 网络。它也属于路由表中的其他路由，但 192.168.32.0/24 在路由表中的前缀最长（24 位对比 19 位）。在转发数据包时，较长前缀始终优先于较短的前缀。

注释 即便新的相似连接将因路由中的变化而导致不同行为，现有连接也将继续使用其已建立的接口。

管理流量的路由表

威胁防御 设备包括用于关联设备管理流量的以下路由表：

- Linux 管理路由表 - 来自管理接口的特殊管理流量（例如 设备管理器 管理会话、 许可通信和数据库更新）始终使用 Linux 管理路由表。
- 数据路由表 - 默认情况下，所有关联设备流量（以及所有通过流量）使用数据路由表。所有常规数据接口都属于此路由表。大多数服务允许您选择特定接口，因此仅使用与该接口关联的路由。
- 管理专用路由表 - 管理接口和您设置为管理专用的所有数据接口都属于此路由表。要从这些接口中的任一接口发送关联设备流量，必须在配置服务时选择特定的管理专用接口。DNS 查找存在一种例外情况：在某些情况下， 威胁防御将使用数据路由表，然后在未找到路由时自动回退到管理路由表。您可以为管理专用接口添加静态路由，但不能为特殊管理接口添加静态路由。威胁防御 设备会自动为管理接口添加一个将流量转发到 Linux 的默认路由，这时将在 Linux 路由表中执行单独的路由查找。您可以使用 威胁防御 CLI **configure network static-routes** 命令将静态路由添加到 Linux 路由表中，供管理接口使用。

注释 使用 **configure network ipv4** 或 **configure network ipv6** 命令设置默认 Linux 路由。

注释 对于尚未合并管理接口和旧诊断接口的设备，请参阅本指南 7.3 版之前的版本。

等价多路径 (ECMP) 路由

威胁防御设备支持等价多路径 (ECMP) 路由。

每个接口最多支持 8 个等价静态或动态路由。例如，您可以在外部接口上配置多个默认路由，指定不同的网关：

```
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.2
```

```
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.3
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.4
```

在这种情况下，流量在外部接口上的 10.1.1.2、10.1.1.3 和 10.1.1.4 之间进行负载均衡。流量基于散列源和目标 IP 地址、传入接口、协议、源与目标端口的算法在 指定网关之间进行分发。

使用流量区域跨多个接口的 ECMP

如果将流量区域配置为包含一组接口，在每个区域中最多可以跨 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
```

同样，动态路由协议可以自动配置等价路由。威胁防御设备使用更稳健的负载均衡机制跨接口对流量进行负载均衡。

当某条路由丢失时，设备会将流量无缝移至其他路由。

静态路由

您可以创建静态路由，以提供网络基本路由。

关于静态路由和默认路由

要将流量路由到非连接的主机或网络，必须使用静态路由或动态路由定义到主机或网络的路由。通常，您必须配置至少一个静态路由：所有流量的默认路由（不是通过其他方式路由到默认网络网关），通常是指下一跳路由器。

默认路由

最简单的方法是配置一个默认静态路由，将所有流量都发送到上游路由器，从而依靠该路由器来为您路由流量。默认路由对网关 IP 地址进行标识，威胁防御设备将所有不具有已获悉或静态路由的数据包发送到该网关地址。默认静态路由是以 0.0.0.0/0 (IPv4) 或 ::/0 (IPv6) 作为目标 IP 地址的静态路由。

应始终定义一个默认路由。

威胁防御 为数据接口和管理专用接口（包括特殊的 Linux 管理接口）提供单独的路由表。只能为数据路由表添加默认路由。 威胁防御 会自动在管理专用路由表中添加一个将流量发送到 Linux 管理接口的默认路由，这时将在 Linux 路由表中执行单独的路由查找。您可以使用 威胁防御 CLI **configure network static-routes** 命令将静态路由添加到 Linux 路由表中，供管理接口使用。

注释 使用 **configure network ipv4** 或 **configure network ipv6** 命令设置默认 Linux 路由。

静态路由

在以下情况下，您可能希望使用静态路由：

- 您的网络使用不受支持的路由器发现协议。
- 网络规模较小，并且可以轻松管理静态路由。
- 不希望流量或 CPU 开销与路由协议相关联。
- 在某些情况下，仅使用默认路由并不足够。默认网关可能无法到达目标网络，因此还必须配置更具体的静态路由。例如，如果默认网关在外部，则默认路由无法将直接流量定向到未直接与威胁防御设备连接的任何内部网络。
- 您使用的是不支持动态路由协议的功能。

备份静态路由和静态路由跟踪

使用静态路由的一个问题是，缺乏用于确定路由处于开启还是关闭状态的内在机制。即使下一跳网关变得不可用，静态路由依然保留在路由表中。只有关联接口关闭时，静态路由才会从路由表中删除。

通过实施路由跟踪，使用服务级别协议 (SLA) 监控，您可以跟踪静态路由的可用性，并在主路由发生故障时，自动安装备用路由。例如，您可以定义一条到 ISP 网关的默认路由和一条到辅助 ISP 的备用默认路由，以防主 ISP 不可用。

在使用路由跟踪时，将目标网络上的目标 IP 地址关联到跟踪的路由。随后，系统会使用 ICMP 回应请求，以定期验证可以访问此地址。如果系统在指定时间内未收到回应，它便会认为此主机不可访问，并从路由表中删除关联的路由。然后，系统会使用具有较高指标的未跟踪备份路由替代已删除的路由。

因此，要对给定目标使用备份静态路由（包括默认路由），您必须执行以下操作：

1. 创建 SLA 监控，以监控目标网络上的可靠 IP 地址，例如网关或始终启用的服务器（例如 web 服务器或系统日志服务器）。对于在目标网络保持正常运行且可被访问时仍可能会离线的系统，不要监控其 IP 地址。请参阅配置 SLA 监控器对象，第 11 页。
2. 创建通往目标的主路由，并选择适用于此路由的 SLA 监控。通常，此路由的指标应为 1。请参阅配置静态路由，第 9 页。
3. 创建备份静态路由，以便在主路由发生故障时使用。此路由的指标应比主路由的大。例如，如果主路由为 1，则备用路由可能是 10。通常，您还会为备份路由选择一个不同的接口。

静态路由准则

网桥组

- 在路由模式下，必须指定 BVI 作为网关；不能指定成员接口。

- 对于源自 威胁防御设备（例如系统日志或 SNMP）且通过网桥组成员接口为非直接连接网络定义的流量，需要配置默认路由或静态路由，以使 威胁防御设备了解通过哪个网桥组成员接口发出流量。如果存在无法通过单个默认路由进行访问的服务器，则必须配置静态路由。
- 静态路由跟踪不支持网桥组成员接口或 BVI。

IPv6

- IPv6 不支持静态路由跟踪（SLA 监控器）。

等价多路径 (ECMP) 流量区域

- 将 ECMP 流量区域的成员接口保留在同一安全区中，以防止对这些接口应用不同的访问规则、SSL 或身份规则。
- 对于给定 ECMP 流量区域中的网络，最多可以有 8 个等价路由。
- 您最多可以创建 256 个 ECMP 流量区域，每个区域最多 8 个接口。
- ECMP 流量区域可以包含已命名的物理接口、子接口和 EtherChannel。它们不能包含以下内容：
  - 网桥组 (BVI) 或其成员
  - EtherChannel 成员接口
  - HA 接口（故障转移或状态链路）
  - 仅限用于管理的接口
  - 用于站点间 VPN 或远程访问 VPN 连接的接口。
  - 虚拟隧道接口 (VTI) 或其源接口。
  - 为 VPN 管理访问配置的接口。
- 不能在区域的接口上启用 DHCP 中继。

配置静态路由

定义静态路由，以告知系统从何处发送的数据包不会绑定至直连到系统接口的网络。

对于网络 0.0.0.0/0，至少需要一个静态路由，即默认路由。如果数据包的传出接口无法由现有 NAT xlate（转换）、静态 NAT 规则或其他静态路由确定，则此路由为所发送的数据包定义目的。

如果无法使用默认网关到达所有网络，则可能需要其他静态路由。例如，默认路由通常是外部接口上的上游路由器。如果还有其他未直连到设备的内部网络，并且通过默认网关无法访问它们，则需要对每个此类内部网络使用静态路由。

对于直连到系统接口的网络，无法定义静态路由。系统自动创建这些路由。

过程

步骤 1 点击**设备**，然后点击**路由**摘要中的链接。

步骤 2 如果已启用虚拟路由器，请点击要在其中配置静态路由的路由器的查看图标 ()。

步骤 3 在**静态路由页**中，执行以下某项操作：

- 要添加新路由，请点击 **+**。
- 点击要编辑的路由的编辑图标 ()。

如果不再需要路由，请点击该路由的垃圾桶图标将其删除。

步骤 4 配置路由属性。

- **名称 (Name)** - 路由的显示名称。
- **说明** - 路由目的的可选说明。
- **接口** - 选择要通过其发送流量的接口。通过此接口需能够访问网关地址。

  对于网桥组，您应为网桥组接口 (BVI) 而不是为成员接口配置路由。

  如果已启用虚拟路由与转发，则可以选择属于其他虚拟路由器的接口。如果在虚拟路由器中创建用于不同虚拟路由器中接口的静态路由，该路由将跨越虚拟路由器边界，且存在来自该虚拟路由器的流量泄漏到另一个虚拟路由器的风险。这可能是期望的结果，但请仔细确定您是否需要此路由泄漏。选择接口时，接口所属的虚拟路由器的名称将显示在接口右侧。
- **协议** - 选择路由是用于 **IPv4** 地址，还是用于 **IPv6** 地址。
- **网络** - 选择标识目标网络或主机（应使用此路由中的网关）的网络对象。

  要定义默认路由，请使用预定义的 any-ipv4 或 any-ipv6 网络对象，或创建一个适用于 0.0.0.0/0 (IPv4) 或 ::/0 (IPv6) 网络的对象。
- **网关** - 选择标识网关 IP 地址的主机网络对象。流量将发送至此地址。您无法将同一个网关用于多个接口上的路由。

  如果要在虚拟路由器中定义路由，且该接口属于不同的虚拟路由器，则必须将该网关留空。系统会将通往这些网络的流量路由至另一个虚拟路由器，然后使用目标虚拟路由器的路由表来确定网关。
- **度量** - 路由的管理距离，该值介于 1 和 254 之间。静态路由的默认值为 1。如果接口和网关之间还有其他路由器，请输入跳数作为管理距离。

  管理距离是用于比较路由的参数。数字越小，为该路由指定的优先级越高。连接的路由（直连到设备接口的网络）始终优先于静态路由。

步骤 5 （可选；仅限 IPv4 路由。）选择应跟踪此路由的生存能力的 **SLA 监控器**。

SLA 监控器可验证目标网络上始终可用的主机是否可访问。如果无法访问，则系统可以安装备份路由。因此，如果配置 SLA 监控器，则还应为此网络配置另一个具有更大度量指标的静态路由。例

如，如果此路由的度量指标为 1，请创建一个指标为 10 的备份路由。有关详细信息，请参阅备份静态路由和静态路由跟踪，第 8 页。

如果 SLA 监控器对象尚不存在，请点击列表底部的**创建 SLA 监控器**链接，立即创建对象。

注释　如果由于无法对受监控的地址进行 ping 操作而删除受监控路由，则会在静态路由表中指示该路由，并显示一条警告，指出该路由无法访问。确定问题是暂时的还是需要重新配置路由。考虑路由可行的概率，但受监控地址不够可靠。

步骤 6　点击**确定 (OK)**。

配置 SLA 监控器对象

配置服务级别协议 (SLA) 监控对象，以与静态路由配合使用。通过使用 SLA 监控，您可以跟踪静态路由的运行状况，并自动使用新路由替换故障路由。有关路由跟踪的详细信息，请参阅备份静态路由和静态路由跟踪，第 8 页。

选择监控目标时，您需要确保它能够响应 ICMP 回应请求。目标可以是主机网络对象中定义的任何 IP 地址，但您应考虑使用以下地址：

- ISP 网关地址（用于支持双 ISP）。
- 下一跳网关地址，如果您关注网关的可用性。
- 目标网络上的服务器，例如系统需要与之进行通信的系统日志服务器。
- 目标网络上的持久性 IP 地址。可能会在夜间关闭的工作站不是一个理想选择。

过程

步骤 1　选择**对象**，然后从目录中选择 **SLA 监控**。

步骤 2　执行以下操作之一：

- 要创建对象，请点击 + 按钮。
- 要编辑某个对象，请点击该对象的编辑图标 ( )。

要删除某个未引用的对象，请点击该对象的垃圾桶图标 ( )。

步骤 3　输入对象的名称和说明（后者为可选项）。

步骤 4　定义 SLA 监控器所需选项：

- **监控地址** - 选择定义目标网络上待监控地址的主机网络对象。如果所需的对象不存在，可以点击**创建新网络 (Create New Network)**。

  仅当将 SLA 监控器附加至静态路由后，才会监控该地址。

- **目标接口** - 选择用于发送回应请求数据包的接口。这通常是您将在其上定义静态路由的接口。接口源地址用作回应请求数据包中的源地址。

步骤 5 （可选。）调整 **IP ICMP 回应选项**。

所有 ICMP 选项均具有适用于大多数情况的默认设置，但可以对其进行调整以满足您的要求。

- **阈值** - 要声明的上升阀值的毫秒数，在 0 到 2147483647 之间。默认值为 5000（5 秒）。该值不应大于为超时设置的值。阈值仅用于指示超出阈值事件，这不会影响可达性。您可以使用阈值事件的发生频率来评估超时设置。
- **超时** - 在收到请求数据包的响应之前，路由监控操作应等待的时间（以毫秒为单位），在 0 到 604800000 毫秒（7 天）之间。默认值为 5000 毫秒（5 秒）。如果在此期间，监控器有至少一个回应请求未得到响应，此过程将会安装备份路由。
- **频率** - SLA 探测之间的毫秒数，从 1000 到 604800000，以 1000 的倍数表示。设置的频率不可小于超时时间。默认值为 60000 毫秒（60 秒）。
- **服务类型** - 定义 ICMP 回应请求数据包 IP 报头中服务类型 (ToS) 的整数，在 0 到 255 之间。默认值为 0。
- **数据包数量** - 每次轮询中要发送的数据包的数量，在 1 到 100 之间。默认为 1 个数据包。
- **数据量** - 回应请求数据包中使用的数据负载的大小，在 0 到 16384 字节之间。默认值为 28。此设置仅指定负载的大小；不指定整个数据包的大小。

步骤 6 点击**确定 (OK)**。

您现在可以在静态路由中使用 SLA 监控对象。

配置 ECMP 流量区域

通常，如果要使用相同的路由度量为特定网络前缀配置多条路由，您需要在同一接口上配置路由。因此，系统使用等价多路径 (ECMP) 路由计算来平衡通过接口发送到网关的流量。

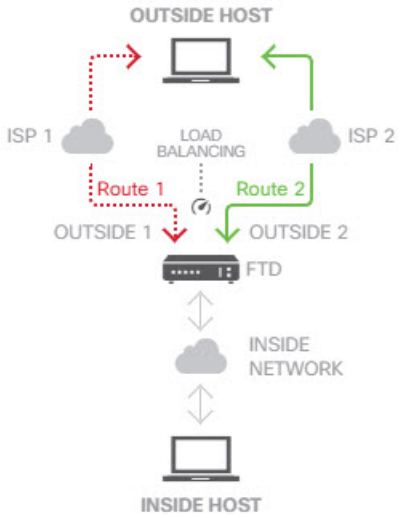
例如，您可以在外部接口上配置多个指定不同网关的默认路由，系统允许这种配置而无需执行其他更改：

```
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.2
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.3
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.4
```

您还可以使用 ECMP 为同一网络前缀和路由度量在多个接口（虚拟路由器内）之间平衡流量。如果可通过单独的接口访问网关，则需要进行此配置。例如，假设您有两个ISP，并且希望在ISP之间平衡负载，但不希望在 ISP 网关之间划分内部地址空间。可通过 outside1 接口访问一个 ISP，通过 outside2 接口访问另一个 ISP。要实现此目的，您需要创建一个包含 outside1 和 outside2 接口的路由流量区域。

```
isp-zone containing outside1 and outside2
```

```
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 10.1.1.3
```



注释 ECMP 路由流量区域与安全区无关。创建包含 outside1 和 outside2 接口的安全区不会实现用于 ECMP 路由的流量区域。

以下程序介绍如何配置 ECMP 区域以利用跨接口的 ECMP 处理。

过程

步骤 1 点击**设备**，然后点击**路由**摘要中的链接。

步骤 2 如果已启用虚拟路由器，请点击要在其中配置静态路由的路由器的查看图标 ( )。

步骤 3 点击 **ECMP 流量区域**选项卡。

步骤 4 在 **ECMP 流量区域 (ECMP Traffic Zones)** 页面上，执行以下一项操作：

- 要添加新区域，请点击 **+** 或**添加 ECMP 流量区域**。
- 点击要编辑的区域的编辑图标 ( )。

如果不再需要某个区域，请点击该区域的垃圾桶图标将其删除。必须先删除依赖于区域的所有静态路由，然后才能删除区域。

步骤 5 为区域输入**名称**和说明（后者为可选项）。

步骤 6 选择最多 8 个**接口**以包含在区域中：

- 点击 **+** 添加接口。
- 点击接口右侧的 **x** 以将其删除。

在选择接口时，请记住以下限制：

- 您可以选择物理接口、子接口和 EtherChannel。
- ECMP 流量区域不能包括以下类型的接口：网桥组 (BVI) 或其成员、EtherChannel 成员接口、HA 接口（故障转移或状态链路）、纯管理接口、虚拟隧道接口 (VTI) 或配置用于 VPN 管理访问的接口。
- 不能包含用于远程访问或站点间 VPN 连接的接口。
- 无论是作为服务器还是代理，都不能选择为 DHCP 中继启用的接口。
- 接口必须分配给同一虚拟路由器。
- 一个接口只能位于一个流量区域中。

步骤 7 点击**确定**。

下一步做什么

现在，您可以转至“静态路由”选项卡，并为同一目的地创建通过这些接口的等价路由。或者，如果通过系统分发等价路由，则动态路由协议可以自动配置等价路由。

监控路由

要对路由进行监控和故障排除，请打开 CLI 控制台或登录设备 CLI 并使用以下命令。您还可以从“路由”(Routing) 页面的**命令 (Commands)** 菜单选择其中一些命令。

- **show route** 显示数据接口的路由表，包括直连网络的路由。
- **show ipv6 route** 显示数据接口的 IPv6 路由表，包括直连网络的路由。
- **show network** 显示管理接口的配置，包括管理网关。通过管理接口的路由不由数据接口路由表处理，除非您指定数据接口作为管理网关。
- **show network-static-routes** 显示使用 **configure network static-routes** 命令为管理接口配置的静态路由。通常不会有任何静态路由，因为在大多数情况下，管理网关足以支持管理路由。这些路由不可用于数据接口上的流量。该命令在 CLI 控制台中不可用。
- **show ospf** 显示有关 OSPF 进程和已获知路由的信息。使用 **show ospf ?** 获取可包含的选项列表，以查看有关 OSPF 的特定信息。
- **show bgp** 显示有关 BGP 进程和已获知路由的信息。使用 **show bgp ?** 获取可包含的选项列表，以查看有关 BGP 的特定信息。
- **show eigrp** 选项显示有关 EIGRP 进程和已获知路由的信息。使用 **show eigrp ?** 获取您可以包含的选项列表；您必须提供一个选项。
- **show isis** 选项显示有关 IS-IS 进程和已获知路由的信息。使用 **show isis ?** 获取您可以包含的选项列表；您必须提供一个选项。

- **show rip database** 显示有关 RIP 进程和已获知路由的信息。
- **show vrf** 显示有关系统上定义的虚拟路由器的信息。
- **show zone** 显示有关 ECMP 流量区域的信息，包括属于每个区域的接口。

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。