静态和默认路由

本章介绍如何在 Firewall Threat Defense上配置静态路由和默认路由。

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，Firewall Threat Defense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。

Firewall Threat Defense 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。 Firewall Threat Defense 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 Firewall Threat Defense 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 Firewall Threat Defense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。
- 虚拟路由器使用静态路由来创建路由泄漏。路由泄漏使流量从虚拟路由器的接口流向另一个虚拟路由器中的另一个接口。有关详细信息，请参阅互联虚拟路由器。

使用到 null0 接口的路由丢弃不必要的流量

通过访问规则，您可以根据其报头中包含的信息过滤数据包。到null0接口的静态路由是访问规则的补充性解决方案。您可以使用 null0 路由转发不必要或不需要的流量，从而丢弃该流量。

静态 null0 路由具有良好的性能配置文件。您还可以使用静态 null0 路由防止产生路由环路。BGP 可以利用静态 null0 路由进行远程触发黑洞路由。

路由优先级

- 标识具体目标的路由优先于默认路由。
- 当存在通向同一目标的多个路由（静态或动态）时，路由的管理距离即可确定优先级。静态路由设置为 1，因此其通常是优先级最高的路由。
- 当您具有多个管理距离相同的通向同一目标的静态路由时，请参阅 等价多路径 (ECMP) 路由，第 13 页。
- 对于来自具有 Tunneled 选项的隧道的新流量，此路由覆盖任何其他已配置或已知悉的默认路由。

透明防火墙模式和网桥组路由

对于源自 Firewall 威胁防御设备并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 Firewall 威胁防御设备了解通过哪个网桥组成员接口发出流量。源自 Firewall 威胁防御设备 的流量可能包括与系统日志服务器或 SNMP 服务器的通信。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。对于透明模式，不能将 BVI 指定为网关接口；只能使用成员接口。 对于路由模式下的网桥组，必须在静态路由中指定 BVI；不能指定成员接口。有关详细信息，请参阅MAC 地址与路由查找。

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，这些路由依然保留在路由表中。只有 Firewall 威胁防御设备 上的关联接口发生故障时，才会从路由表中删除静态路由。

静态路由跟踪功能提供在主路由发生故障的情况下跟踪静态路由的可用性和安装备用路由的方法。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。

Firewall 威胁防御设备 通过将静态路由与 Firewall 威胁防御设备 使用 ICMP 回应请求监控的目标网络上的监控目标主机相关联来实施静态路由跟踪。如果在指定时间内没有收到回应回复，则主机将被视为关闭，并且会从路由表中删除关联路由。使用具有较高指标的未跟踪备用路由替代已删除的路由。

选择监控目标时，您需要确保它能够响应 ICMP 回应请求。该目标可以是您选择的任何网络对象，但是应考虑使用以下对象：

- ISP 网关（用于支持双 ISP）地址
- 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 Firewall 威胁防御设备 需要与之进行通信的系统日志服务器
- 目标网络上的持久网络对象

注释 可能会在夜间关闭的 PC 不是一个理想选择。

您可以为静态定义的路由或通过 DHCP 或 PPPoE 获取的默认路由配置静态路由跟踪。您只能在配置了路由跟踪的多个接口上启用 PPPoE 客户端。

静态路由的要求和前提条件

型号支持

Firewall Threat Defense

支持的域

任意

用户角色

管理员

网络管理员

静态和默认路由准则

防火墙模式和网桥组

- 在透明模式下，静态路由必须使用桥接组成员接口作为网关；不能指定 BVI。
- 在路由模式下，必须指定 BVI 作为网关；不能指定成员接口。
- 静态路由跟踪不支持网桥组成员接口或 BVI。

支持的网络地址

- IPv6 不支持静态路由跟踪。
- Firewall Threat Defense 不支持 E 类路由，因此 E 类网络不能在静态路由中路由。

集群

- 在集群中，仅控制节点上支持静态路由跟踪。

网络对象组

不能在静态路由中使用一系列网络对象或具有一系列 IP 地址的网络对象组。

ASP 和 RIB 路由条目

在 ASP 路由表中捕获设备上安装的所有路由及其距离。这对于所有静态和动态路由协议都是通用的。在 RIB 表中仅捕获最佳距离路由。

添加静态路由

静态路由用于定义为特定目标网络发送流量的位置。至少应定义一个默认路由。默认路由是以0.0.0.0/0作为目标 IP 地址的静态路由。

要为冗余管理器访问数据接口配置路由，请参阅配置冗余管理器访问数据接口。

过程

步骤 1 选择 **设备** > **设备管理**，然后编辑 Firewall Threat Defense 设备。

步骤 2 点击**路由 (Routing)**。

步骤 3 （可能需要）在虚拟路由器下拉列表中，选择要为其配置静态路由的虚拟路由器。

步骤 4 选择 **静态路由**。

步骤 5 点击**添加路由**。

步骤 6 点击 **IPv4** 或 **IPv6**，具体取决于要添加的静态路由的类型。

步骤 7 选择此静态路由应用至的**接口**。

对于透明模式，选择网桥组成员接口名称。对于具有网桥组的路由模式，您可以为 BVI 名称选择网桥组成员接口。要将不必要的流量转发到“黑洞”，请选择 **Null0** 接口。

对于使用虚拟路由的设备，您可以选择属于其他虚拟路由器的接口。如果要将流量从此虚拟路由器泄漏到另一个虚拟路由器，可以创建此类静态路由。有关详细信息，请参阅互联虚拟路由器。

步骤 8 在**可用网络**列表中，选择目标网络。

要定义默认路由，请创建一个具有地址 0.0. 0.0/0 的对象，然后在此处选择它。

注释
虽然可以创建和选择一个包含 IP 地址范围的网络对象组，但 防火墙管理中心 不支持在静态路由中使用范围。

步骤 9 在**网关 (Gateway)**或 **IPv6 网关 (IPv6 Gateway)** 字段中，输入或选择是次路由下一跳的网关路由器。您可以提供 IP 地址或网络/主机对象。

当您为虚拟路由器使用静态路由配置泄漏路由时，请勿指定下一跳网关。

步骤 10 在**指标**字段中，输入到目标网络的跳数。有效值范围为 1 到 255；默认值为 1。

指标是基于到特定主机所在的网络的跳数对路由的“开销”的一种衡量。跳计数是网络数据包在到达最终目标之前必须遍历的网络数，包括目标网络。指标用于比较不同路由协议之间的路由。静态路由的默认管理距离为 1，这使其优先于动态路由协议所发现的路由，但不优先于直连路由。OSPF 所发现路由的默认管理距离为 110。如果静态路由与动态路由的管理距离相同，则静态路由优先。已连接的路由始终优先于静态路由或动态发现的路由。

步骤 11 （可选） 对于默认路由，选中**隧道**复选框可为 VPN 流量定义单独的默认路由。

如果希望 VPN 流量使用与非 VPN 流量不同的默认路由，可以为 VPN 流量定义单独的默认路由。例如，从VPN连接传入的流量可以轻松定向到内部网络，而来自内部网络的流量可以定向到外部。使用“隧道”选项创建默认路由时，来自终止于无法使用已获悉或静态路由进行路由的设备的隧道的所有流量都会发送到该路由。对于每台设备，您只能配置一条默认的隧道网关。不支持隧道流量的 ECMP。

步骤 12 （仅 IPv4 静态路由）要监控路由可用性，请在**路由跟踪**字段中输入或选择定义监控策略的 SLA（服务级别协议）监控对象的名称。

请参阅SLA 监控器。

步骤 13 点击**确定 (OK)**。

路由参考

此部分介绍有关路由如何在 Firewall Threat Defense 内部运行的基本概念。

确定路径

路由协议使用指标来评估传播数据包的最佳路径。指标是一种测量标准，例如供路由算法用于确定目标的最佳路径的路径带宽。为帮助执行确定路径的过程，路由算法会初始化和维护其中包含路由信息的路由表。路由信息根据所使用的路由算法而异。

路由算法使用各种信息来填充路由表。目标或下一跳关联告知路由器，可以通过将数据包发送到特定路由器（表示通往最终目标的下一跳）来以最优路径到达特定目标。当路由器收到传入数据包时，会检查目标地址并尝试将此地址与下一跳关联。

路由表还包含其他信息，例如有关路径可取性的数据。路由器通过比较指标来确定最佳路由，而这些指标根据所使用的路由算法的设计而异。

路由器互相进行通信，并通过传输各种消息来维护其路由表。路由更新消息是通常由路由表的全部或部分内容组成的消息。通过分析来自所有其他路由器的路由更新，路由器可以构建详细的网络拓扑图。链路状态通告（路由器之间发送的另一种消息）用于告知其他路由器发送方链路的状态。链路信息还可用于构建完整网络拓扑图，以使路由器能够确定通向网络目标的最佳路径。

支持的路由类型

路由器可以使用多种路由类型。Firewall 威胁防御设备 使用以下路由类型：

- 静态与动态
- 单路径与多路径
- 平面与分层
- 链路状态与距离矢量

静态与动态

静态路由算法实际上是网络管理员建立的表映射。除非网络管理员修改这些映射，否则映射不会发生更改。使用静态路由的算法设计简单，并且在网络流量相对可预测且网络设计相对简单的环境下适用。

由于静态路由系统无法对网络更改作出反应，因此通常被认为不适合大型且不断变化的网络。大多数主要的路由算法为动态路由算法，这些算法通过分析传入路由更新消息来适应变化的网络环境。如果有消息表明网络发生更改，则路由软件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。

可以酌情使用静态路由对动态路由算法进行补充。例如，可以将必备路由器（所有无法路由的数据包都发送到的路由器的默认路由）指定为所有无法路由的数据包的存储库，从而确保所有消息都至少以某种方式进行处理。

单路径与多路径

某些综合路由协议支持指向同一目标的多个路径。与单路径算法不同，这些多路径算法允许流量在多条线路上多路复用。多路径算法的优势在于显著提高吞吐量和可靠性，通常称为负载共享。

平面与分层

某些路由算法在平面空间中运行，而其他算法则使用路由层次结构。在平面路由系统中，路由器是所有其他路由器的对等体。在分层路由系统中，某些路由器形成实际上的路由主干。来自非主干路由器的数据包会传播到主干路由器，在此数据包通过主干进行发送，直至到达目标的大致区域。此时，数据包通过一个或者多个非主干路由器从最后一个主干路由器传播到最终目标。

路由系统通常会指定一些逻辑节点组，称为域、自治系统或区域。在分层系统中，一个域中的一些路由器可以与其他域中的路由器进行通信，而其他路由器只能与其本域中的路由器进行通信。在超大网络中，还可能存在其他分层级别，其中位于最高分层级别的路由器形成路由主干。

分层路由的主要优点在于，它会模仿大多数公司的组织，从而很好地支持这些公司的流量模式。大多数网络通信发生在小型公司组（域）中。由于域内路由器只需知道其域中的其他路由器即可，因此可以简化这些路由器的路由算法，并根据所使用的路由算法相应地减少路由更新流量。

链路状态与距离矢量

链路状态算法（也称最短路径优先算法）将路由信息以泛洪形式发送给互联网络中的所有节点。但是，每条路由器仅发送用于说明其自身链路状态的路由表部分。在链路状态算法中，每条路由器在其路由表中构建整个网络的情景。距离矢量算法（也称为 Bellman-Ford 算法）要求每条路由器仅向其邻居发送其路由表的全部或部分内容。实质上，链路状态算法会四处发送小的更新，而距离矢量算法只将较大的更新发送给相邻路由器。距离矢量算法仅知道其邻居。通常，链路状态算法与OSPF路由协议结合使用。

支持的互联网路由协议

Firewall 威胁防御设备 支持多种互联网路由协议。本节对每种协议进行简单介绍。

- 增强型内部网关路由协议 (EIGRP)

  EIGRP 是思科专有协议，用于提供与 IGRP 路由器的兼容性和无缝互操作性。通过自动重分发机制，可将 IGRP 路由导入到增强型 IGRP（反之亦然），从而可以将增强型 IGRP 逐渐添加到现有 IGRP 网络。

- 开放最短路径优先 (OSPF)

  OSPF 是由互联网工程任务小组 (IETF) 的内部网关协议 (IGP) 工作小组开发的面向互联网协议 (IP) 网络的路由协议。OSPF 使用链路状态算法构建和计算所有到达已知目标的最短路径。OSPF 区域中的每条路由器包含相同的链路状态数据库，该数据库是由每条路由器可使用的接口和可访问邻居组成的列表。

- 路由信息协议 (RIP)

  RIP 是一种使用跳数作为指标的距离矢量协议。RIP 广泛用于路由全局互联网中的流量，并且是一种内部网关协议 (IGP)，意味着在单个自治系统内执行路由。

- 边界网关协议 (BGP)

  BGP 是一种自治系统间路由协议。BGP 用于交换互联网的路由信息，并且是互联网服务提供商 (ISP) 之间所使用的协议。客户连接到 ISP，然后 ISP 使用 BGP 交换客户路由和 ISP 路由。在自

治系统 (AS) 之间使用 BGP 时，该协议称为外部 BGP (EBGP)。如果运营商使用 BGP 在 AS 内交换路由，则此协议称为内部 BGP (IBGP)。

路由表

Firewall 威胁防御对数据流量（通过设备）和管理流量（来自设备）使用单独的路由表。本部分介绍路由表 的工作原理。有关管理路由表的信息，另请参阅 管理流量的路由表，第 12 页。

路由表的填充方式

Firewall Threat Defense 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 Firewall Threat Defense 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 Firewall Threat Defense 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 Firewall Threat Defense 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 Firewall Threat Defense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 Firewall Threat Defense支持的路由协议的默认管理距离值。

表 *1:* 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
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 Firewall Threat Defense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 Firewall Threat Defense 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 Firewall Threat Defense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 Firewall Threat Defense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 Firewall Threat Defense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。

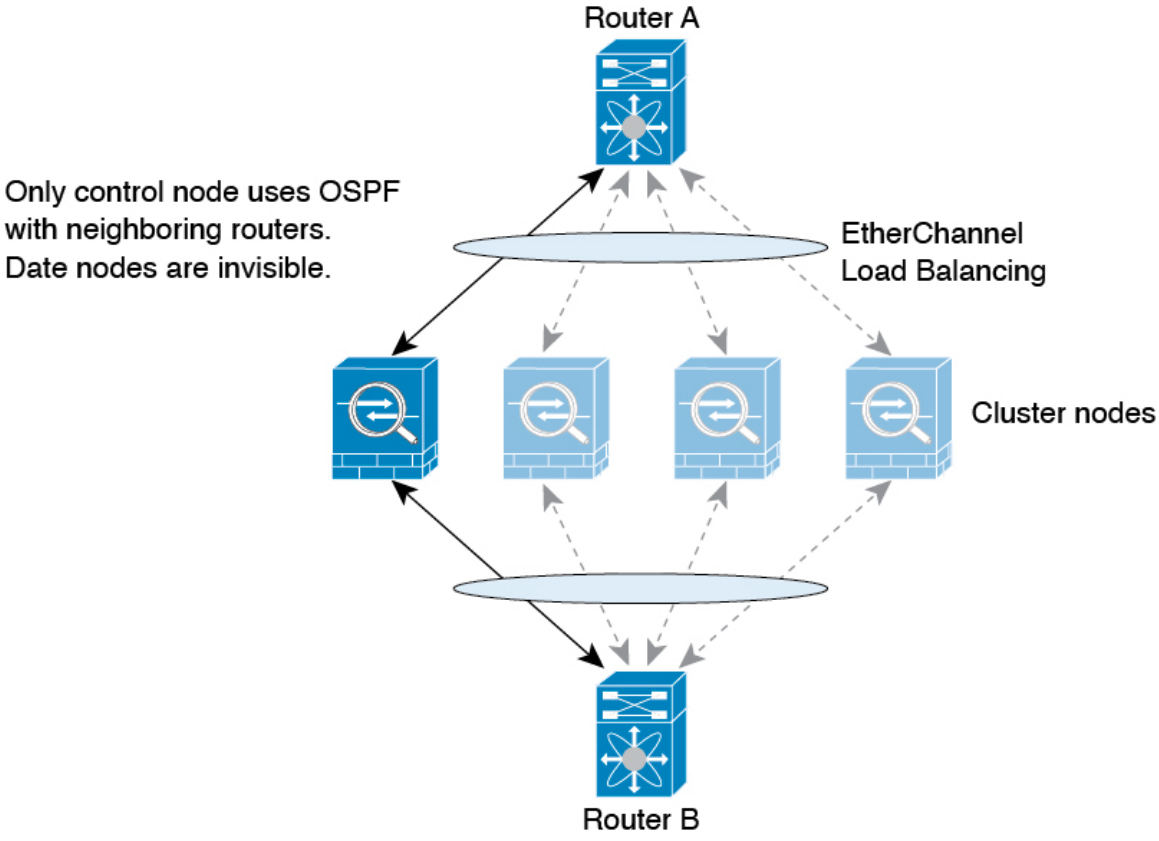
动态路由和

当主用设备上的路由表发生更改时，在备用设备上同步动态路由。这意味着主用设备上的所有添加、删除或更改都将立即传播到备用设备。如果备用设备在主用/备用就绪 对中处于活动状态，则它会有与前一个主用设备相同的路由表，因为路由作为 批量同步和连续复制过程的一部分进行同步。

集群下的动态路由

路由过程仅在控制节点上运行，并且通过控制节点学习路线后复制到数据节点。如果路由数据包到达数据节点，它将重定向到控制节点。

图 *1:* 跨区以太网通道模式下的动态路由



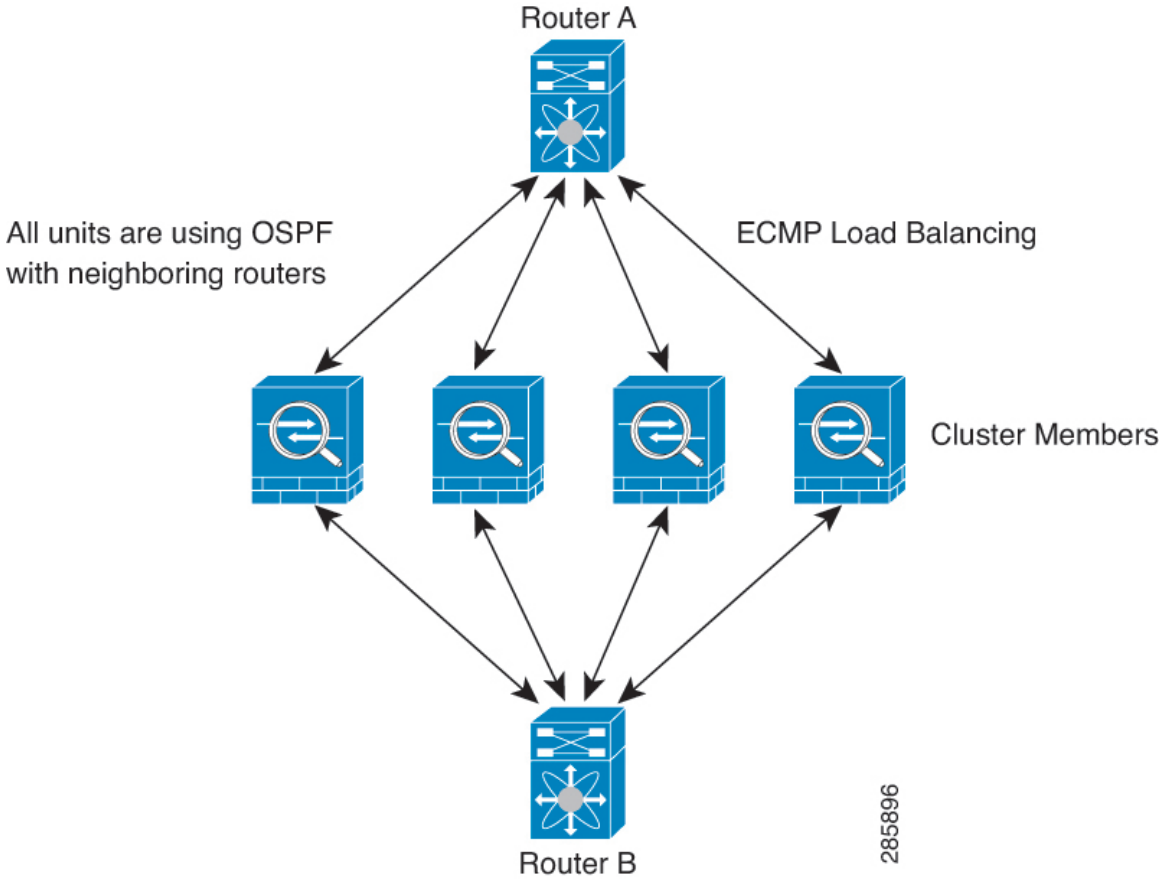
在数据节点向控制节点学习路线后，每个节点将单独做出转发决策。

OSPF LSA 数据库不会从控制节点同步到数据节点。如果切换了控制节点，邻近路由器将检测到重新启动；切换是不透明的。OSPF 进程将挑选一个 IP 地址作为其路由器 ID。您可以分配一个静态路由器 ID，尽管不要求这样做，但这可以确保整个集群中使用的路由器 ID 一致。请参阅 OSPF 无间断转发功能，解决中断问题。

独立接口模式下的动态路由

在独立接口模式下，每个节点作为独立的路由器运行路由协议，且每个节点独立获知路由。

图 *2:* 独立接口模式下的动态路由



在上图中，路由器 A 获知有 4 条等价路径通往路由器 B，每条路径都要经过一个节点。ECMP 用于在这 4 条路径之间对流量执行负载均衡。每个节点在与外部路由器通信时，都会挑选不同的路由器 ID。

您必须为路由器 ID 配置一个集群池，使每个节点都有单独的路由器 ID。

EIGRP 与单个接口模式下的集群对等体不构成邻居关系。

注释 如果该集群为实现冗余有多个设备与同一个路由器相邻，则非对称路由可能会造成不可接受的流量损失。要避免非对称路由，请将所有这些节点接口分组到同一流量区域中。请参阅创建 ECMP 区域。

管理流量的路由表

Firewall Threat Defense 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 防火墙管理中心 通信、 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 和 ICMP （PING 和跟踪路由）存在一种例外情况：在某些情况下， Firewall Threat Defense 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。Firewall Threat Defense 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 Firewall Threat Defense 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

Firewall Threat Defense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。Firewall Threat Defense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。

路由 GRE 流量

在 Firewall 威胁防御 中，使用双向流管理通用路由封装 (GRE) 流量。这意味着每个 GRE 会话都由处理终端之间入站和出站流量的单个流条目表示。对于双向流，仅执行一次路由查找，并将两个方向映射到同一接口。因此，系统无法为每个方向做出独立的路由决策，这在某些情况下可能导致次优路由。

关于路由映射

在将路由重新分发到OSPF、RIP、EIGRP或BGP路由进程时会使用路由映射。在为OSPF路由进程生成默认路由时也会使用路由映射。路由映射定义了允许将来自指定路由协议的哪些路由重新分发到目标路由进程。

路由映射与广为人知的 ACL 具有许多相同功能。以下是两者共有的一些特征：

- 它们都是单独语句的有序序列，各自具有允许或拒绝结果。ACL 或路由映射的评估包括采用预先确定顺序的列表扫描，以及每条语句匹配条件的评估。一旦找到第一个语句匹配即中止列表扫描，并且会执行与语句匹配相关联的操作。
- 它们是通用机制。条件匹配和匹配解释由它们的应用方式和使用它们的功能决定。应用于不同功能的相同路由映射可能以不同方式进行解释。

以下是路由映射与 ACL 之间的一些差异：

- 路由映射比 ACL 更加灵活，可以根据 ACL 无法验证的条件对路由进行验证。例如，路由映射可以验证路由的类型是否为内部路由。
- 每个ACL按照设计约定以隐式拒绝语句结尾。如果在匹配尝试期间到达路由映射的结尾，则结果取决于路由映射的特定应用。应用于重新分发的路由映射与ACL的行为方式相同：如果路由与路由映射中的任何子句不匹配，则会拒绝路由重新分发，就如同路由映射的结尾包含拒绝语句一样。

Permit 和 Deny 子句

路由映射可以具有permit和deny子句。deny子句可拒绝来自重新分发的路由匹配。您可以使用ACL作为路由映射中的匹配标准。由于 ACL 还有 permit 和 deny 子句，因此数据包与 ACL 匹配时会应用以下规则：

- ACL permit + route map permit：重新分发路由。
- ACL permit + route map deny：重新分发路由。
- ACL deny + route map permit or deny：不匹配 route map 子句，并且对下一个 route-map 子句进行评估。

Match 和 Set 子句值

每个路由映射子句均具有两种类型的值：

- match 值用于选择应将此子句应用于的路由。
- set 值用于修改将重新分发到目标协议的信息。

对于要重新分发的每个路由，路由器首先评估路由映射中子句的匹配条件。如果匹配条件成功，则按照 permit 或 deny 子句的指示重新分发或拒绝路由，其某些属性可能会通过 set 命令设置的值修改。如果匹配条件失败，则此子句不适用于路由，软件会根据路由映射中下一个子句继续评估路由。路由映射扫描将继续，直到发现匹配路由的子句或达到路由映射的结尾。

如果存在下列条件中的一个，则每个子句中的 match 值或 set 值可能会缺失或多次重复：

- 如果一个子句中存在多个匹配条目，则对于给定路由而言，所有这些条目必须都符合，该路由才与该子句匹配（也即，为多个 match 命令应用逻辑 AND 算法）。
- 如果一个 match 条目引用了一个条目中的多个对象，那么其中任何一个对象都应匹配（应用逻辑 OR 算法）。
- 如果匹配条目不存在，则所有路由都匹配子句。
- 如果一个 set 条目在 route map permit 子句中不存在，则该路由将被重新分发，而不修改其当前属性。

注释 请勿在 route map deny 子句中配置 set 条目，因为 deny 子句会禁止路由重新分发 - 没有要修改的信息。

没有 match 或 set 条目的 route map 子句需要执行操作。空 permit 子句允许重新分发剩余路由而不进行修改。空 deny 子句不允许重新分发其他路由（如果路由映射在经过完整扫描后，未发现明确的匹配项，此为默认操作）。

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。

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。

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。