静态和默认路由

本章介绍如何在 ASA 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，ASA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。

由于ASA设备使用用于数据流量和管理流量的单独路由表，所以，您可以选择配置数据流量的默认路由和管理流量的另一默认路由。请注意，关联设备流量默认使用管理专用或数据路由表，具体取决于类型，但如果未找到路由，则会退回至其他路由表。默认路由将始终匹配流量，并将阻止退回至其他路由表。在这种情况下，如果接口不在默认路由表中，则必须指定要用于出口流量的接口。

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ASA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。

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。
- 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 ASA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 ASA了解通过哪个网桥组成员接口发出流量。源自 ASA 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ASA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。

ASA 通过将静态路由与 ASA 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 ASA 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。
- ASA 不支持 E 类路由，因此 E 类网络不能在静态路由中路由。

集群和多情景模式

- 在集群中，仅控制节点上支持静态路由跟踪。
- 多情景模式下不支持静态路由跟踪。

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。

配置默认路由和静态路由

您至少应配置一个默认路由。您可能还需要配置静态路由。在本节中，我们将配置默认路由，配置静态路由以及跟踪静态路由。

配置默认路由

默认路由是以 0.0.0.0/0 作为目标 IP 地址的静态路由。您应始终具有默认路由：通过此程序手动配置或者从 DHCP 服务器或其他路由协议派生。

开始之前

请参阅有关 Tunneled 选项的以下准则：

- 请勿在隧道路由的传出接口上启用单播 RPF （**ip verify reverse-path** 命令），因为此设置会导致会话失败。
- 请勿在隧道路由的传出接口上启用 TCP 拦截，因为此设置会导致会话失败。
- 请勿使用带有隧道路由的 VoIP 检测引擎（CTIQBE、H.323、GTP、MGCP、RTSP、SIP、SKINNY)、DNS 检测引擎或 DCE RPC 检测引擎，因为这些检测引擎会忽略隧道路由。
- 不能使用 tunneled 选项定义多个默认路由。
- 不支持隧道流量的 ECMP。
- 桥接组不支持隧道路由，因为不支持直通流量的 VPN 终止。

过程

添加一个默认路由。

IPv4：

route *if_name* **0.0.0.0 0.0.0.0** *gateway_ip* [**distance**] [**tunneled**]

IPv6：

ipv6 route *if_name* **::/0** *gateway_ip* [**distance**] [**tunneled**]

示例：

```
ciscoasa(config)# route outside 0.0.0.0 0.0.0.0 192.168.2.4
ciscoasa(config)# route inside 0.0.0.0 0.0.0.0 10.1.2.3 tunneled
ciscoasa(config)# ipv6 route inside ::/0 3FFE:1100:0:CC00::1
```

if_name 是要通过其发送特定流量的接口。请为透明模式指定网桥组成员接口名称。 对于具有网桥组的路由模式，请指定 BVI 名称。

distance 参数是路由的管理距离，该值介于 1 和 254 之间。如果未指定值，则默认值为 **1**。管理距离是用于比较不同路由协议之间路由的参数。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。

注释
对于通过设备的流量，如果您在具有不同指标的不同接口上同时配置两个默认路由，则从具有更高指标的接口到 ASA 的连接会失败，但是从具有较低指标的接口到 ASA 的连接则会如预期成功。对于设备外流量，如果在具有不同度量的不同接口上配置了两个默认路由，则两个接口可能会用于设备外流量，具体取决于用于传入连接的接口。

如果希望 VPN 流量使用与非 VPN 流量不同的默认路由，可以使用 **tunneled** 关键字定义单独的 VPN 流量。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 tunneled 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 ASA 的隧道的所有流量都会发送到该路由。桥接组不支持此选项。

提示
您可以为目标网络地址和掩码输入 **0 0** 而非 **0.0.0.0 0.0.0.0**，如下例所示：**route outside 0 0 192.168.2.4**

配置静态路由

静态路由用于定义为特定目标网络发送流量的位置。

过程

添加一个静态路由：

IPv4：

route *if_name dest_ip mask gateway_ip* [**distance**]

IPv6：

ipv6 route *if_name dest_ipv6_prefix/prefix_length gateway_ip* [**distance**]

示例：

```
ciscoasa(config)# route outside 10.10.10.0 255.255.255.0 192.168.1.1
ciscoasa(config)# ipv6 route outside 2001:DB8:1::0/32 2001:DB8:0:CC00::1
```

if_name 是要用于发送特定流量的接口。要丢弃不必要的流量，请输入 **null0** 接口。请为透明模式指定网桥组成员接口名称。 对于具有网桥组的路由模式，请指定 BVI 名称。

dest_ip 和 *mask* 或 *dest_ipv6_prefix/prefix_length* 参数指示目标网络的 IP 地址，*gateway_ip* 参数则是下一跳路由器的地址。为静态路由指定的地址是在进入 ASA 并执行 NAT 之前的数据包内的地址。

distance 参数是路由的管理距离。如果未指定值，则默认值为 **1**。管理距离是用于比较不同路由协议之间路由的参数。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。

示例

以下示例显示 3 个通向同一网关的网络和另一个通向不同网关的网络的静态路由。

```
route outside 10.10.10.0 255.255.255.0 192.168.1.1
route outside 10.10.20.0 255.255.255.0 192.168.1.1
route outside 10.10.30.0 255.255.255.0 192.168.1.1
route inside 10.10.40.0 255.255.255.0 10.1.1.1
```

配置静态路由跟踪

要配置静态路由跟踪，请完成以下步骤：

过程

步骤 1 为用于连接网络的接口 (outside 1) 配置静态路由：

```
ciscoasa(config)# route outside1 172.29.139.134 255.255.255.255 10.0.0.1
```

步骤 2 定义监控进程：

sla monitor sla_id

示例：

```
ciscoasa(config)# sla monitor 5
ciscoasa(config-sla-monitor)#
```

步骤 3 指定监控协议、被跟踪网络上的目标主机，以及访问网络所通过的接口。

type echo protocol ipicmpecho target_ip **interface** if_name

示例：

```
ciscoasa(config-sla-monitor)# type echo protocol ipicmpecho 172.29.139.134 interface outside1
ciscoasa(config-sla-monitor-echo)#
```

target_ip 参数是跟踪进程监控其可用性的网络对象的 IP 地址。当该对象可用时，跟踪进程路由会添加到路由表中。当该对象不可用时，跟踪进程删除该路由并改用备用路由进行替代。

步骤 4 （可选）配置监控选项。有关以下命令，请参阅命令参考：**frequency**、**num-packets**、**request-data-size**、**threshold**、**timeout** 和 **tos**。

步骤 5 安排监控进程：

sla monitor schedule sla_id [**life** {**forever** | seconds}] [**start-time** {hh:mm [:ss] [month day | day month] | **pending** | **now** | **after** hh:mm:ss}] [**ageout** seconds] [**recurring**]

示例：

```
ciscoasa(config)# sla monitor schedule 5 life forever start-time now
```

通常情况下，您将使用 **sla monitor schedule** *sla_id***life forever start-timenow** 命令监控计划，并让监控配置确定进行测试的频率。

不过，您可以将监控进程安排在未来开始并仅在指定时间发生。

步骤 6 将被跟踪的静态路由与 SLA 监控进程相关联：

track track_id **rtr** sla_id **reachability**

示例：

```
ciscoasa(config)# track 6 rtr 5 reachability
```

track_id 参数为您使用此命令分配的跟踪编号。*sla_id* 参数为 SLA 进程的 ID 编号。

步骤 7 跟踪以下路由类型之一：

- 静态路由：

  route if_name dest_ip mask gateway_ip [distance] **track** track_id

  示例：

  ```
  ciscoasa(config)# route outside 10.10.10.0 255.255.255.0 192.168.1.1 track 6
  ```

  您不能使用 **tunneled** 选项。

- 通过 DHCP 获取的默认路由：

  ```
  interface interface_id
    dhcp client route track track_id
    ip address dhcp setroute
  ```

- 通过 PPPoE 获取的默认路由：

  ```
  interface interface_id
    pppoe client route track track_id
    ip address pppoe setroute
  ```

步骤 8 创建一个未进行跟踪的备用路由。

备用路由是与被跟踪路由通向同一目标的静态路由，但是通过不同的接口或网关。您必须为此路由分配比被跟踪路由更大的管理距离（指标）。

监控静态路由或默认路由

- **show route**

  显示路由表。

静态路由或默认路由示例

以下示例显示如何创建静态路由，该路由将以 10.1.1.0/24 为目标的所有流量发送到与内部接口连接的路由器 10.1.2.45，定义三个用于将流量定向到 dmz 接口上的三个不同网关的等价静态路由，并为隧道流量和常规流量各添加一个默认路由。

```
route inside 10.1.1.0 255.255.255.0 10.1.2.45
route dmz 10.10.10.0 255.255.255.0 192.168.2.1
route dmz 10.10.10.0 255.255.255.0 192.168.2.2
route dmz 10.10.10.0 255.255.255.0 192.168.2.3
route outside 0 0 209.165.201.1
route inside 0 0 10.1.2.45 tunneled
```

静态和默认的历史记录

表 *1:* 静态和默认路由功能的历史记录

功能名称	平台版本	功能信息
静态路由跟踪	7.2(1)	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。 引入了以下命令：**clear configure sla**、**frequency**、**num-packets**、**request-data-size**、**show sla monitor**、**show running-config sla**、**sla monitor**、**sla monitor schedule**、**threshold**、**timeout**、**tos**、**track rtr**
丢弃流量的静态 null0 路由	9.2(1)	向 null0 接口发送流量会导致丢弃发往指定网络的数据包。此功能有助于为 BGP 配置远程触发黑洞 (RTBH)。 修改了以下命令：**route**。

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。