虚拟路由器

本章介绍了关于虚拟路由器的基本概念以及虚拟路由在 Cisco Secure Firewall Threat Defense 中的表现。

关于虚拟路由器和虚拟路由与转发 (VRF)

可以创建多个虚拟路由器来为接口组维护单独的路由表。由于每个虚拟路由器都有自己的路由表，因此您可以完全分隔流经设备的流量。

因此，您可以通过一组通用的网络设备为两个或多个不同的客户提供支持。您还可以使用虚拟路由器为自身网络的元素提供更多隔离，例如，将开发网络与一般用途的企业网络隔离。

虚拟路由器将实施虚拟路由和转发功能的“轻型”版本（或 VRF Lite），它不支持 BGP 的多协议扩展 (MBGP)。

创建虚拟路由器时，您需要为路由器分配接口。您可以将给定接口分配给一个且仅有一个虚拟路由器。然后即可定义静态路由，并为每个虚拟路由器配置路由协议（例如 OSPF 或 BGP）。还可在整个网络中配置单独的路由进程，以便所有参与设备的路由表都使用每个虚拟路由器相同的路由进程和表。使用虚拟路由器，可在同一物理网络上创建逻辑分隔的网络，以确保流经每个虚拟路由器的流量的隐私。

由于路由表独立存在，因此可以在虚拟路由器上使用相同或重叠的地址空间。例如，可以将 192.168.1.0/24 地址空间用于两个独立的虚拟路由器，分别由两个独立物理接口提供支持。

请注意，每个虚拟路由器有单独的管理和数据路由表。例如，如果将管理专用接口分配给虚拟路由器，则该接口的路由表会与分配给虚拟路由器的数据接口分离开来。

关于虚拟路由器和动态 VTI

虚拟路由器和动态 VTI

您可以创建虚拟路由器，将动态 VTI 与这些虚拟路由器关联，并在网络中扩展动态 VTI 的功能。可以将动态 VTI 与全局或用户定义的虚拟路由器关联。您可以只能将一个动态 VTI 分配给一个虚拟路由器。

与以下项关联的虚拟路由器：

- 动态 VTI 称为室内 VRF (IVRF)。
- 隧道源接口称为 Front Door VRF (FVRF)。

动态 VTI 及其对应的受保护网络接口必须属于同一虚拟路由器。必须将借用 IP 接口和动态 VTI 映射到同一虚拟路由器。隧道源接口可以是多个虚拟路由器的一部分。

要使用动态 VTI 为基于路由的站点间 VPN 配置虚拟路由器，请参阅 如何使用动态 VTI 配置虚拟路由器，第 2 页。

有关配置示例的详细信息，请参阅 如何使用动态 VTI 通过站点间 VPN 保护来自多个虚拟路由器的网络流量，第 33 页

如何使用动态 VTI 配置虚拟路由器

要在管理中心为路由型站点间 VPN 配置具有动态 VTI 的虚拟路由器，请执行以下操作：

步骤	相应操作	更多信息
1	使用中枢上的动态VTI接口和分支上的静态VTI创建基于路由的站点间VPN。	创建基于路由的站点间 VPN
2	创建虚拟路由器。	创建虚拟路由器，第 12 页
3	将接口分配给虚拟路由器。	配置虚拟路由器，第 12 页
4	为中心辐射点配置路由策略。	为中心辐射型拓扑配置终端
5	为中心辐射型配置访问控制策略。	为中心辐射型拓扑配置终端

虚拟路由器的应用

您可以使用虚拟路由器来隔离共享资源上的网络，以及/或者隔离具有通用安全策略的网络。因此，虚拟路由器可以帮助您实现：

- 通过为每个客户或不同部门提供专用路由表来为客户分离流量。

- 不同部门或网络的通用安全策略管理。
- 不同部门或网络的共享互联网接入。

全局和用户定义的虚拟路由器

全局虚拟路由器

对于具有虚拟路由功能的设备，系统会默认创建一个全局虚拟路由器。系统会将网络中的所有接口分配给全局虚拟路由器。路由接口可以属于用户定义的虚拟路由器或全局虚拟路由器。在将威胁防御升级到具有虚拟路由器功能的版本时，其所有现有路由配置将成为全局虚拟路由器的一部分。

用户定义的虚拟路由器

用户定义的虚拟路由器就是您定义的虚拟路由器。您可以在一台设备上创建多个虚拟路由器。但在任何时候，一个接口都只能分配给一个用户定义的虚拟路由器。虽然用户定义的虚拟路由器支持某些设备功能，但只有少数功能仅在全局虚拟路由器上受支持。用户定义的虚拟路由器支持基于路由的站点间 VPN（静态 VTI）（静态和动态 VTI）。

支持的功能和监控策略

您只能在全局虚拟路由器上配置以下功能：

- OSPFv3
- RIP
- EIGRP
- IS-IS
- 组播路由
- 策略型路由 (PBR)

通过管理中心中的 Flex Config 支持 ISIS （请参阅预定义的 FlexConfig 对象）。只为这些功能配置全局虚拟路由器接口。

DHCP 服务器自动配置会使用从接口获知的 WINS/DNS 服务器。此接口只能是全局虚拟路由器接口。

您可以为每个用户定义的虚拟路由器单独配置以下功能：

- 静态路由及其 SLA 监控器
- OSPFv2
- BGPv4/v6
- 集成的路由与桥接 (IRB)
- SNMP

当查询或与远程系统通信时，系统会使用以下功能（传出流量）。这些功能仅使用全局虚拟路由器中的接口。这意味着，如果为该功能配置了接口，则接口必须属于全局虚拟路由器。作为一条规则，系统无论何时出于管理目的必须查找连接外部服务器的路由，它会在全局虚拟路由器中执行路由查找。

- DNS服务器用于解析访问控制规则中使用的完全限定名称，或解析**ping**命令的名称。如果指定**any** 作为 DNS 服务器的接口，则系统仅考虑全局虚拟路由器中的接口。
- 用于 VPN 的 AAA 服务器或身份领域。只能在全局虚拟路由器中的接口上配置 VPN。因此，用于 VPN 的外部 AAA 服务器（如 Active Directory）必须可通过全局虚拟路由器中的接口访问。

配置策略以感知虚拟路由器

创建虚拟路由器时，该虚拟路由器的路由表会自动与全局虚拟路由器或任何其他虚拟路由器分离开来。但是，安全策略不会自动识别虚拟路由器。

例如，如果编写适用于“任何”源或目标安全区的访问控制规则，则该规则将应用于所有虚拟路由器上的所有接口。这实际上可能正是您所希望得到的结果。例如，可能所有客户都想阻止访问相同系列的令人反感的 URL 类别。

但是，如果需要仅向其中一个虚拟路由器应用策略，则需要创建仅包含来自该单一虚拟路由器的接口的安全区。然后，在安全策略的源和目标条件中使用虚拟路由器限制的安全区。

通过使用其成员身份限制为分配给单个虚拟路由器的接口的安全区，您可以在以下策略中编写虚拟路由器感知规则：

- 访问控制策略。
- 入侵和文件策略。
- SSL 解密策略。
- 身份策略和用户到IP地址映射。如果在虚拟路由器中使用重叠地址空间，请确保为每个虚拟路由器创建单独的领域，并在身份策略规则中正确应用。

如果在虚拟路由器中使用重叠地址空间，则应使用安全区确保应用适当的策略。例如，如果在两个单独的虚拟路由器中使用 192.168.1.0/24 地址空间，则指定 192.168.1.0/24 网络的访问控制规则将应用于两个虚拟路由器中的流量。如果这不是期望的结果，您可以通过只为其中一个虚拟路由器指定源/目标安全区来限制该规则的应用。

互联虚拟路由器

静态和动态路由泄漏

您可以配置设备来路由虚拟路由器之间的流量。路由泄漏过程可以通过设置静态路由手动完成，也可以通过 BGP 设置动态完成。

静态路由泄漏

您可以配置静态路由来路由虚拟路由器之间的流量。

例如，如果您在全局虚拟路由器中设有外部接口，则可以在每个其他虚拟路由器中设置静态默认路由，以将流量发送到该外部接口。然后，无法在给定虚拟路由器内路由的任何流量将被发送到全局路由器，以进行后续路由。

虚拟路由器之间的静态路由被称为路由泄漏，这是因为您会将流量泄漏到其他虚拟路由器。泄漏路由（例如，VR1 路由到 VR2）时，可以仅发起从 VR2 到 VR1 的连接。要使流量从 VR1 流向 VR2，必须配置反向路由。当您为另一个虚拟路由器中的接口创建静态路由时，不需要指定网关地址，而只需选择目标接口。

对于虚拟路由器间路由，系统会在源虚拟路由器中查找目标接口。然后，系统会查找目标虚拟路由器中下一跳的MAC地址。因此，目标虚拟路由器必须具有用于目标地址的所选接口的动态（获知）或静态路由。

通过配置将在不同虚拟路由器中使用源接口和目标接口的NAT规则，还允许在虚拟路由器之间路由流量。如果未选择NAT进行路由查找的选项，则每当发生目标转换时，规则就会将流量从目标接口发送到 NATed 地址。但是，目标虚拟路由器应具有一个已转换目标 IP 地址的路由，以便下一跳查找可以取得成功。

虽然NAT规则将流量从一个虚拟路由器泄漏到另一个虚拟路由器，但为了确保正确的路由，建议在这些虚拟路由器之间为转换后的流量配置静态路由泄漏。如果没有路由泄漏，有时该规则可能无法匹配您预期其匹配的流量，并且可能不会应用转换。

虚拟路由不支持级联或路由泄漏链。例如，假设 威胁防御 具有VR1、VR2和VR3虚拟路由器；VR3直接连接到网络 10.1.1.0/24。现在，假设您在 VR1 中通过 VR2 中的接口为网络 10.1.1.0/24 配置了路由泄漏，在 VR2 中通过 VR3 为 10.1.1.0/24 定义了路由泄漏。此路由泄漏链不允许流量从 VR1 跳到 VR2，然后从 VR3 退出。如果存在路由泄漏，路由查找将首先从输入虚拟路由器的路由表确定出口接口，然后查看虚拟路由器的路由表输出，以进行下一跳查找。在上述两次查找中，出口接口应匹配。在本示例中，出口接口不是同一接口，因此流量不会通过。

当目的网络不是上游（传出）VR 的直连子网时，请谨慎使用静态 VRF 间路由。例如，假设有两个 VR - VR1 和 VR2。VR1 处理通过 BGP 或任何动态路由协议从其外部对等体获取默认路由的传出流量，而 VR2 则处理配置了静态 VRF 间默认路由的传入流量，并将 VR1 作为下一跳。当 VR1 丢失来自其对等体的默认路由时，VR2将无法检测到其上游（传出）VR丢失了默认路由，并且仍会向VR1发送流量，该流量最终将被丢弃，而不会发出通知。在这种情况下，我们建议您通过 BGP 为 VR2 配置动态路由泄漏。

使用 BGP 完成的动态路由泄漏

您可以通过使用路由目标扩展社区将路由从源虚拟路由器（比如VR1）导出到源BGP表，然后将相同的路由目标扩展社区从源 BGP 表导入到目的 BGP 表来实现虚拟路由器间路由泄漏，导入的路由目标扩展社区将由目的虚拟路由器（比如 VR2）使用。您可以使用路由映射来过滤路由。全局虚拟路由器的路由也可以泄漏到用户定义的虚拟路由器，反之亦然。BGP 虚拟路由器间路由泄漏支持 IPv4 和 IPv6 前缀。

有关配置 BGP 路由泄漏的详细信息，请参阅配置 BGP 路由导入/导出设置。

BGP 路由泄漏准则

- 确保递归所需的所有路由均已导入并出现在入口虚拟路由器的路由表中。
- 每个虚拟路由器都支持 ECMP。因此，请不要在不同的虚拟路由器之间配置 ECMP。从不同虚拟路由器导入的重叠前缀无法形成 ECMP。也就是说，当您尝试将具有重叠地址的路由从两个不同的虚拟路由器导入到其他虚拟路由器（全局虚拟路由器或用户定义的虚拟路由器）时，只有一条路由（根据 BGP 最佳路径算法，是通告的第一个路由）会导入到相应的虚拟路由表中。例如，如果连接到 VR1 的网络 10.10.0.0/24 先通过 BGP 通告到全局虚拟路由器，之后连接到 VR2 的另一个具有相同地址 10.10.0.0/24 的网络也通过 BGP 通告到全局虚拟路由器，则只有 VR1 网络路由会导入到全局虚拟路由表中。
- 用户定义的虚拟路由器不支持 OSPFv3。因此，请不要将 BGPv6 配置为将 OSPFv3 用户定义的虚拟路由器泄漏到全局虚拟路由器。但是，您可以将 BGPv6 配置为通过重新分发将 OSPFv3 全局虚拟路由器路由泄漏到用户定义的虚拟路由器。
- 建议将 VTI 接口、受保护的内部接口（如果 VTI 支持，则为环回接口）保留为同一虚拟路由器的一部分，以防止需要路由泄漏。

重叠 IP 地址

虚拟路由器会创建多个独立的路由表实例，因此可以使用相同或重叠的 IP 地址，而且不会发生冲突。威胁防御 允许同一网络成为两个或多个虚拟路由器的一部分。这涉及到要在接口或虚拟路由器级别应用的多个策略。

除了少数例外，路由功能以及大多数 NGFW 和 IPS 功能都不会受重叠 IP 地址的影响。以下部分介绍具有重叠 IP 地址限制的功能以及摆脱这些限制的建议。

重叠 IP 地址的限制

在多个虚拟路由器中使用重叠 IP 地址时，为确保正确应用策略，您必须修改某些功能的策略或规则。此类功能要求您拆分现有安全区域或根据需要使用新接口组，以便使用更具体的接口。

在使用重叠 IP 地址时，您需要修改以下功能才能正常运行：

- “网络映射”(Network Map) - 修改网络发现策略以排除一些重叠的 IP 网段，以确保没有映射的重叠 IP 地址。
- “身份策略”(Identity Policy) - 身份源来源无法区分虚拟路由器；要摆脱此限制，请在不同领域映射重叠地址空间或虚拟路由器。

对于以下功能，您需要在特定接口上应用规则，才能确保在重叠的 IP 网段上应用不同的策略：

- 访问策略
- 预过滤器策略
- QoS/速率限制
- SSL 策略

重叠 IP 地址的不支持的功能

- AC 策略中基于 ISE SGT 的规则 - 从思科身份服务引擎 (ISE) 下载的静态安全组标签 (SGT) 到 IP 地址的映射不会感知虚拟路由器。如果需要为每个虚拟路由器创建不同的 SGT 映射，请为每个虚拟路由器设置单独的 ISE 系统。如果打算将相同的 IP 地址映射到各个虚拟路由器中的相同 SGT 编号，则无需执行此操作。
- 不支持跨虚拟路由器使用重叠 DHCP 服务器池。
- 事件和分析 - 很多 管理中心 分析依赖于网络映射和身份映射，如果同一 IP 地址属于两个不同的终端主机，则无法区分。因此，当同一设备中存在重叠的 IP 网段但虚拟路由器不同时，这些分析并不准确。

在用户定义的虚拟路由器上配置 SNMP

除了在管理接口和全局虚拟路由器数据接口上支持 SNMP，Cisco Secure Firewall Threat Defense 现在还允许您在用户定义的虚拟路由器上配置 SNMP 主机。

在用户定义的虚拟路由器上配置 SNMP 主机包括以下过程：

1. 配置设备接口。
2. 创建虚拟路由器
3. 在虚拟路由器接口上配置 SNMP 主机。

注释 SNMP 无法被虚拟路由器感知。因此，在用户定义的虚拟路由器上配置 SNMP 服务器时，请确保网络地址不是重叠 IP 地址。

4. 将配置部署到 Cisco Secure Firewall Threat Defense。在成功部署后，SNMP 轮询和陷阱将通过虚拟路由器接口发送到网络管理站。

按设备型号划分的最大虚拟路由器数量

可以创建的最大虚拟路由器数量取决于设备型号。下表列出了最大限制。您可以通过输入 **show vrf counters** 命令对系统进行复核，该命令显示该平台的用户定义最大虚拟路由器数量（不包括全局虚拟路由器）。下表中的数字包括用户和全局路由器。对于 Firepower 4100/9300，这些数字适用于原生模式。

对于支持多实例功能的平台（例如 Firepower 4100/9300），通过以下方式确定每个容器实例的最大虚拟路由器数：将最大虚拟路由器数除以设备上的核心数，然后乘以分配给该实例的核心数，并四舍五入到最接近的整数。例如，如果平台最多支持 100 个虚拟路由器，并且它有 70 个核心，则每个核心最多支持 1.43 个虚拟路由器（四舍五入为一个）。因此，分配有 6 个核心的实例将支持 8.58 个虚拟路由器（四舍五入为 8 个），分配有 10 个核心的实例将支持 14.3 个虚拟路由器（四舍五入为 14 个）。

设备型号	最大虚拟路由器数量
Firepower 1010	5
Firepower 1120	5
Firepower 1140	10
Firepower 1150	10
Firepower 2110	10
Firepower 2120	20
Firepower 2130	30
Firepower 2140	40
Secure Firewall 3105	10
Secure Firewall 3110	15
Secure Firewall 3120	25
Secure Firewall 3130	50
Secure Firewall 3140	100
Firepower 4112	60
Firepower 4115	80
Firepower 4125	100
Firepower 4145	100
Cisco Secure Firewall 4215	100
Cisco Secure Firewall 4225	100
Cisco Secure Firewall 4245	100
Firepower 9300 设备，所有型号	100
Threat Defense Virtual，所有平台	30
ISA 3000	10

相关主题

容器实例的要求和前提条件

虚拟路由器的要求和必备条件

型号支持

威胁防御

支持的域

任意

用户角色

管理员

网络管理员

安全审批人

虚拟路由器的准则和限制

防火墙模式指导原则

虚拟路由器仅在路由防火墙模式下支持。

接口指导原则

- 您可以只能将一个接口分配给一个虚拟路由器。
- 可以为虚拟路由器分配任意数量的接口。
- 只有具有逻辑名称 和 VTI 的路由接口才能被分配给用户定义的虚拟路由器。
- 如果要将虚拟路由器接口更改为非路由模式，请从虚拟路由器中删除该接口，然后再更改其模式。
- 您可以从全局虚拟路由器或其他用户定义的虚拟路由器将接口分配给虚拟路由器。
- 不能将以下接口分配给用户定义的虚拟路由器：
  - EtherChannel 的成员。
  - 冗余接口的成员。
  - BVI 成员。
- VTI 是基于路由的 VPN。因此，在建立隧道后，必须通过路由控制使用 VTI 进行加密的流量。支持静态路由，以及使用 BGP、OSPFv2/v3, or EIGRP 的动态路由。
- 属于用户定义的虚拟路由器的接口无法用于站点间或 RA VPN。

- 动态 VTI 及其对应的受保护网络接口必须属于同一虚拟路由器。
- 必须将借用 IP 接口和动态 VTI 映射到同一虚拟路由器。
- 用户定义的虚拟路由器仅支持 BGPv4/v6 和 OSPFv2 路由协议。
- 隧道源接口可以位于与动态 VTI 关联的虚拟路由器之外的用户定义的虚拟路由器中。
- 如果使用正在移动的接口或其虚拟路由器被删除的路由存在于源或目的虚拟路由器表中，请在移动接口或删除虚拟路由器之前删除这些路由。
- 由于为每个虚拟路由器维护了单独的路由表，因此当接口从一个虚拟路由器移至另一个虚拟路由器（无论是全局路由器还是用户定义的路由器）时，系统都会临时删除接口上配置的 IP 地址。接口上的所有现有连接都会被终止。因此，在虚拟路由器之间移动接口会对网络流量产生显著影响。因此，请不要在移动接口之前采取预防措施。

全局虚拟路由器准则

- 已命名但不属于其他虚拟路由器的接口是全局虚拟路由器的一部分。
- 您不能从全局虚拟路由器中删除路由接口。
- 您不能修改全局虚拟路由器。
- 通常，在配置接口后，如果取消注册并重新注册到同一或其他 管理中心，则接口配置会从设备导回。使用虚拟路由器支持时存在一个限制 - 只保留全局虚拟路由器接口的 IP 地址。

集群准则

- 当控制设备链路由于其接口故障而发生故障时，该设备会从全局路由表中删除其接口的所有泄漏路由，然后将非活动连接的静态路由传播到集群的其他设备。这样会导致从其他设备的路由表中删除这些泄漏的路由。这些删除发生在另一台设备成为新的控制设备之前，大约需要 500 毫秒。当另一台设备成为新的控制设备时，这些路由将通过BGP融合获知并添加回路由表中。因此，直到融合时间（约一分钟），泄漏的路由才可用于发生路由事件。
- 当集群中发生控制角色更改时，通过BGP获知的泄漏路由将通过最佳ECMP路径进行更新。但是，仅在BGP重新融合计时器过去后（即210秒），才会从集群路由表中删除非最佳ECMP路径。因此，在BGP重新融合计时器到期之前，旧的非最佳ECMP路径将继续作为路由事件的首选路由。

其他规定

- 在为虚拟路由器配置 BGP 时，您可以在同一虚拟路由器内重新分发属于不同协议的路由。例如，无法将 OSPF VR2 路由导入到 BGP VR1 中。您只能将 OSPF VR2 重新分发到 BGP VR2，然后在 BGP VR2 和 BGP VR1 之间配置路由泄漏。
- 您不能使用 IPv6 ACL 来过滤路由地图中的路由。只支持前缀列表。
- 安全智能策略 - 安全智能策略不会感知虚拟路由器。如果将 IP 地址、URL 或 DNS 名称添加到阻止列表，则会被所有虚拟路由器阻止。这一限制适用于具有安全区域的接口。

- NAT 规则 - 不要在 NAT 规则中混用接口。在虚拟路由中，如果指定的源和目的接口对象（接口组或安全区）有属于不同虚拟路由器的接口，那么 NAT 规则会将流量从一个虚拟路由器分流到另一个虚拟路由器。NAT 只会在虚拟路由器表中为入站接口执行路由查找。如有必要，请在源虚拟路由器中为目标接口定义静态路由。如果将接口保留为 **any**，则该规则适用于所有接口，而不考虑虚拟路由器成员关系。
- DHCP 中继 - 不支持为 DHCP 中继互连虚拟路由器。例如，如果在 VR1 接口上启用了 DHCP 中继客户端，而在 VR2 接口上启用了 DHCP 中继服务器，则 DHCP 请求将不会被转发到 VR2 接口之外。
- 重新创建已被删除的虚拟路由器 - 如果您重新创建一个在 10 秒内被删除的虚拟路由器，系统将弹出一条错误消息，指出正在删除该虚拟路由器。如果您要连续重新创建已删除的虚拟路由器，请为新的虚拟路由器使用不同的名称。

管理中心 Web 界面 - 路由页面修改

虚拟路由功能不支持用于 威胁防御 6.6 之前的设备和少数设备型号。对于此类不受支持的设备， 管理中心 Web 界面显示的是 管理中心 6.5 或更早版本的“路由”(Routing) 页面。要了解支持使用虚拟路由功能的设备和平台，请参阅按设备型号划分的最大虚拟路由器数量。

您可以在支持设备的路由页面中配置虚拟路由器：

1. 导航至**设备** > **设备管理**，然后编辑虚拟路由器感知设备。
2. 点击**路由 (Routing)** 以进入虚拟路由器页面。

对于使用虚拟路由功能的设备，“路由”(Routing) 页面的左窗格显示以下选项：

- **管理虚拟路由器** - 允许您创建和管理虚拟路由器。
- 虚拟路由协议列表 - 列出可为虚拟路由器配置的路由协议。
- **常规设置** - 允许您配置适用于所有虚拟路由器的 BGP 常规设置。选中**启用 BGP** 复选框可定义其他 BGP 设置。要为虚拟路由器配置其他 BGP 设置，请导航至虚拟路由协议中的 **BGP**。

管理虚拟路由器

当您点击“虚拟路由器”(Virtual Routers) 窗格上的**管理虚拟路由器 (Manage Virtual Routers)** 时，将出现“管理虚拟路由器”(Manage Virtual Routers) 页面。此页面会显示设备和关联接口上的现有虚拟路由器。在此页面中，您可以**添加虚拟路由器**（+）到设备。您还可以**编辑**（✎）和**删除**（🗑）用户定义的虚拟路由器。您无法编辑或删除全局虚拟路由器。您只能**视图**（👁）全局虚拟路由器的详细信息。

创建虚拟路由器

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 点击**管理虚拟路由器**。

步骤 4 请点击 **添加虚拟路由器** （+）。

步骤 5 在“添加虚拟路由器”框中，输入虚拟路由器的名称和说明。

注释 如果您创建一个在10秒内被删除的虚拟路由器，系统将弹出一条错误消息，指出正在删除该虚拟路由器。如果您要连续创建已删除的虚拟路由器，请为新的虚拟路由器使用不同的名称。

步骤 6 点击**确定 (OK)**。

系统将显示“路由”(Routing) 页面，其中显示新创建的虚拟路由器页面。

下一步做什么

- 配置虚拟路由器。

配置虚拟路由器

您可以为用户定义的虚拟路由器分配接口，并为设备配置路由策略。虽然不能手动为全局虚拟路由器添加或删除接口，但可以为设备接口配置路由策略。

开始之前

- 要为用户定义的虚拟路由器配置路由策略，请添加路由器。请参阅创建虚拟路由器，第 12 页。
- 非虚拟路由设备的所有路由配置设置也可用于全局虚拟路由器。有关设置的信息，请参阅路由设置。
- 用户定义的虚拟路由器只支持有限的路由协议。

过程

步骤 1 在**设备 (Devices)** > **设备管理 (Device Management)** 页面中，编辑虚拟路由器支持的设备。导航至**路由**。有关对路由页面的修改的信息，请参阅 管理中心 Web 界面 - 路由页面修改，第 11 页 。

步骤 2 从下拉列表中，选择所需的虚拟路由器。

步骤 3 在**虚拟路由器属性 (Virtual Router Properties)** 页面中，您可以修改说明。

步骤 4 要添加接口，请在**可用接口**框下选择接口，然后点击**添加**。

请记住以下几点：

- **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。
- 仅全域虚拟路由器可用于分配，**可用接口**框仅列出未分配给任何其他用户定义的虚拟路由器的接口。你可以给虚拟路由器分配物理接口、子接口、冗余接口、网桥组、VTI 和 EtherChannels，但不能分配其成员接口。由于成员接口无法命名，因此无法在虚拟路由中使用。

  您只能将诊断接口 分配给全局虚拟路由器。

步骤 5 要保存设置，点击**保存**。

步骤 6 要为虚拟路由器配置路由策略，请点击各自的名称，打开对应的设置页面：

- **OSPF** - 用户定义的虚拟路由器仅支持 OSPFv2。OSPFv2 的所有其他设置与非虚拟路由器感知接口一样适用，只是**接口**允许您仅选择您正在配置的虚拟路由器的接口。您可以为全局虚拟路由器定义 OSPFv3 和 OSPFv2 路由策略。有关 OSPF 设置的信息，请参阅OSPF。
- **RIP** - 只能为全局虚拟路由器配置 RIP 路由策略。有关 RIP 设置的信息，请参阅RIP。
- **BGP** - 此页面显示您在**设置 (Settings)** 中配置的 BGP 常规设置：
  - 除了路由器 ID 设置外，您无法修改此页面上的任何常规设置。您可以在此页面上进行编辑来覆盖在**设置 (Settings)** 页面中定义的路由器 ID 设置。
  - 要配置其他 BGP IPv4 或 IPv6 设置，必须在**常规设置 (General Settings)** 下的 **BGP** 页面中启用 BGP 选项。
  - 全局路由器和用户定义的虚拟路由器均支持 IPv4 和 IPv6 地址系列的 BGP 配置。

  有关配置 BGP 设置的信息，请参阅BGP。
- **静态路由** - 使用此设置来定义为特定目标网络发送流量的位置。您还可以使用此设置来创建虚拟路由器间静态路由。您可以使用用户定义或全局虚拟路由器的接口创建连接或静态路由的泄漏。**FMC 为接口添加** 前缀，以指示它属于另一个虚拟路由器并可用于路由泄漏。为使路由泄漏成功，请不要指定下一跳网关。

  静态路由表在**已从虚拟路由器泄漏**列中显示其接口用于路由泄漏的虚拟路由器。如果不是路径泄漏，则该列显示 N/A。

  无论静态路由属于哪个虚拟路由器，都会列出 Null0 接口以及与静态路由所属的同一虚拟路由器的接口。

  有关静态路由设置的信息，请参阅静态和默认路由。
- **组播** - 只能为全局虚拟路由器配置组播路由策略。有关组播设置的信息，请参阅组播。

步骤 7 要保存设置，点击**保存**。

下一步做什么

- 修改虚拟路由器。
- 删除虚拟路由器。

修改虚拟路由器

您可以修改虚拟路由器的说明和其他路由策略。

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 点击**管理虚拟路由器**。

所有虚拟路由器以及分配的接口都显示在**虚拟路由器 (Virtual Routers)** 页面中。

步骤 4 要修改虚拟路由器，请点击所需虚拟路由器旁边的 **编辑**（）。

注释 无法修改全局虚拟路由器的常规设置。因此，不能对全局路由器进行编辑； 而是提供 **视图**（） 来查看设置。

步骤 5 要保存更改，请点击**保存 (Save)**。

下一步做什么

- 删除虚拟路由器。

删除虚拟路由器

开始之前

- 不能删除全局虚拟路由器。因此，删除选项不可用于全局虚拟路由器。
- 您可以一次删除多个虚拟路由器。
- 被删除的虚拟路由器的所有路由策略也被删除。
- 被删除的虚拟路由器的所有接口都移动到全局虚拟路由器。
- 如果接口的移动存在任何限制（例如重叠 IP、路由冲突等），则只有在解决冲突后才能删除路由器。

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 点击**管理虚拟路由器**。

所有虚拟路由器以及映射的接口都显示在**虚拟路由器 (Virtual Routers)** 页面中。

步骤 4 要删除虚拟路由器，请点击所需虚拟路由器旁边的 **删除**（ ）。

步骤 5 要删除多个路由器，请按住 CTRL 键，点击要删除的虚拟路由器。右键点击，然后点击**删除**。

步骤 6 要保存更改，请点击**保存**。

监控虚拟路由器

要对虚拟路由器进行监控和故障排除，请登录设备 CLI 并使用以下命令。

- **show vrf**：显示虚拟路由器及其关联接口的详细信息。
- **show route vrf** <*vrf_name*>：显示虚拟路由器的路由详细信息。
- **show run router bgp all**：显示所有虚拟路由器的 BGP 路由详细信息。
- **show run router bgp vrf** <*vrf_name*>：显示虚拟路由器的 BGP 路由详细信息。
- **show crypto ipsec sa/show crypto ikev2 sa**：显示隧道和关联虚拟路由器的详细信息。
- 您可以在站点到站点监控控制面板中监控隧道（**概述 > 站点间 VPN**）。

  在 **隧道状态** 构件中，将鼠标悬停在拓扑上，点击查看 ，然后点击 **数据包跟踪器** 以查看威胁防御 VPN 隧道并进行故障排除。

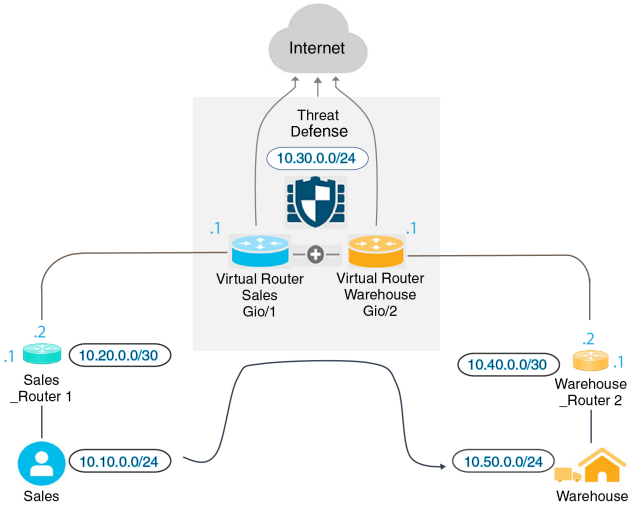
虚拟路由器的配置示例

如何通过虚拟路由器路由到远程服务器

在虚拟路由中，您可以创建多个虚拟路由器来为接口组维护单独的路由表，从而实现网络分离。在某些情况下，您可能需要访问只能通过单独的虚拟路由器访问的服务器。此示例提供了将虚拟路由器互联以访问相距多跳的主机的程序。

例如，假设一家服装公司的销售部成员想要在其工厂单位仓库部门维护的库存中进行查找。在虚拟路由环境中，您需要在目标（仓库部门）与销售部门相距多跳的虚拟路由器之间泄漏路由。路由泄漏是通过添加多跳路由泄漏来完成的，在此过程中，您需要在“销售”虚拟路由器（源）中配置一条通往“仓库”虚拟路由器（目标）中的接口的静态路由。当目标网络相距多跳时，您还需要为“仓库”虚拟路由器配置通往目标网络（即 10.50.0.0/24）的路由。

图 *1:* 互联两个虚拟路由器 - 示例



开始之前

此示例假设您已配置 Sales_Router1，从而将流量从 10.20.0.1/30 接口路由到 10.50.0.5/24。

过程

步骤 1 配置要分给“销售”虚拟路由器的设备的内部接口 (Gi0/1)：

a) 依次选择**设备** > **设备管理** > **接口**。

b) 编辑 Gi0/1 接口：

- **名称** - 本例中为“VR-Sales”。
- 选中**启用**复选框。
- 在 **IPV4** 中，对于 **IP 类型**，请选择**使用静态 IP**。
- **IP 地址** - 输入 10.30.0.1/24。

c) 点击**确定**。

d) 点击**保存 (Save)**。

步骤 2 配置要分配给“仓库”虚拟路由器的设备的内部接口 (Gi0/2)：

a) 依次选择**设备** > **设备管理** > **接口**。

b) 编辑 Gi0/2 接口：

- **名称** - 本例中为“VR-Warehouse”。
- 选中**启用**复选框。
- 在 **IPV4** 中，对于 **IP 类型**，请选择**使用静态 IP**。

- **IP 地址** - 将其留空。该系统不允许您使用相同的 IP 地址 (10.30.0.1/24) 配置接口，因为您尚未创建用户定义的虚拟路由器。

c) 点击**确定**。
d) 点击**保存 (Save)**。

步骤 3 创建“销售”和“仓库”虚拟路由器并分配其接口：

a) 依次选择 **设备** > **设备管理**，并且编辑 威胁防御 设备。
b) 依次选择**路由** > **管理虚拟路由器**。
c) 点击**添加虚拟路由器**并创建“销售”虚拟路由器。
d) 点击**添加虚拟路由器**并创建“仓库”虚拟路由器。
e) 从虚拟路由器下拉列表中选择“销售”，然后在**虚拟路由器属性**中，添加“VR-Sales”作为**选定接口**并保存。
f) 从虚拟路由器下拉列表中选择“仓库”，然后在**虚拟路由器属性**中，添加“VR-Warehouse”作为**选定接口**并保存。

步骤 4 重新访问“VR-Warehouse”接口配置：

a) 依次选择**设备** > **设备管理** > **接口**。
b) 针对“VR-Warehouse”接口点击**编辑**。将 IP 地址指定为 10.30.0.1/24。现在，由于接口分别分配给两个不同的虚拟路由器，因此系统允许您使用“VR-Sales”的同一 IP 地址进行配置。
c) 点击**确定**。
d) 点击**保存 (Save)**。

步骤 5 为仓库服务器 (10.50.0.0/24) 和仓库网关 (10.40.0.2/30) 创建网络对象：

a) 依次选择**对象** > **对象管理**。
b) 依次选择**添加网络** > **添加对象**：

- **名称** - 本例中为“Warehouse-Server”。
- **网络** - 点击“网络”并输入 10.50.0.0/24。

c) 点击**保存 (Save)**。
d) 依次选择**添加网络** > **添加对象**：

- **名称** - 本例中为“Warehouse-Gateway”。
- **网络** - 点击“主机”并输入 10.40.0.2。

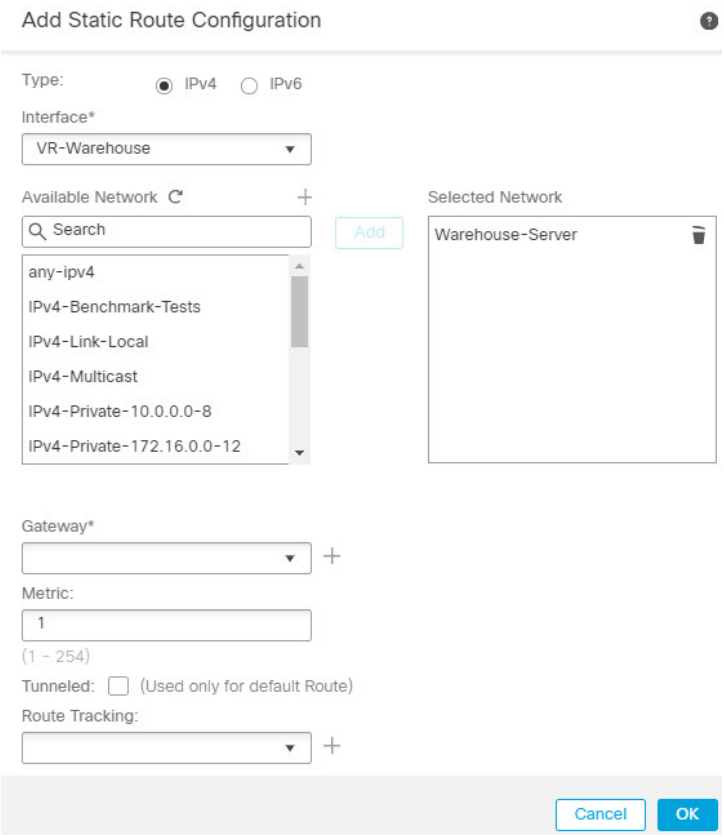
e) 点击**保存 (Save)**。

步骤 6 定义指向“VR-Warehouse”接口的“销售”虚拟路由器中的路由泄漏：

a) 依次选择 **设备** > **设备管理**，并且编辑 威胁防御 设备。
b) 选择**路由**。
c) 从下拉列表中选择“销售”虚拟路由器，然后点击**静态路由**。
d) 点击**添加路由**。在**添加静态路由配置**中，指定以下内容：

- **接口** - 选择“VR-Warehouse”。

- **网络** - 选择 Warehouse-Server 对象。
- **网关** - 将其留空。将路由泄漏到另一个虚拟路由器时，请勿选择网关。



e) 点击**确定**。

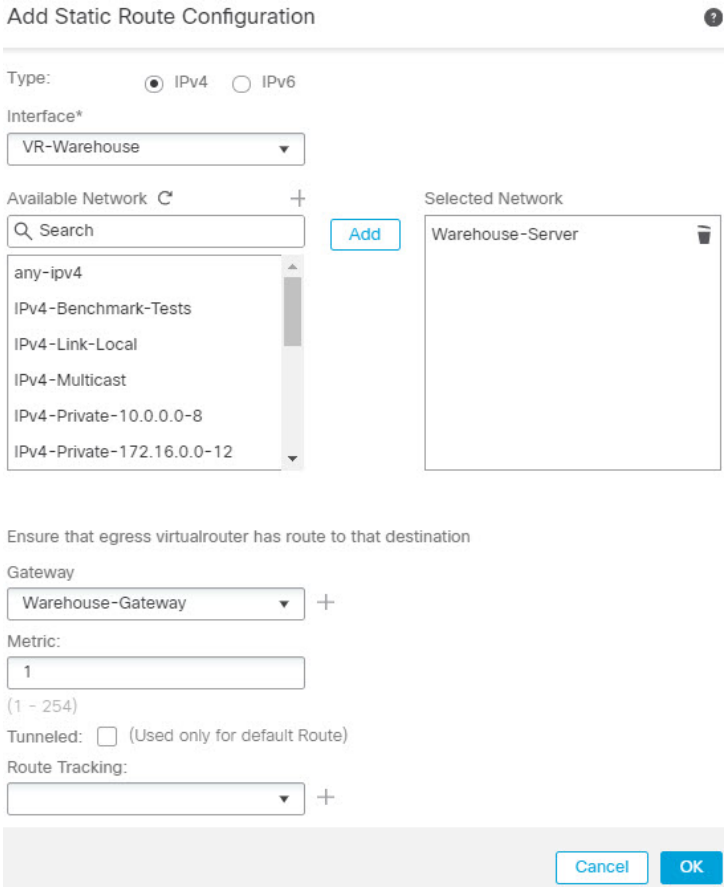
f) 点击**保存 (Save)**。

步骤 7 在“仓库”虚拟路由器中，定义指向仓库路由器 2 网关的路由：

a) 从下拉列表中选择“仓库”虚拟路由器，然后点击**静态路由**。

b) 点击**添加路由**。在**添加静态路由配置**中，指定以下内容：

- **接口** - 选择“VR-Warehouse”。
- **网络** - 选择 Warehouse-Server 对象。
- **网关**-选择 Warehouse-Gateway 对象。



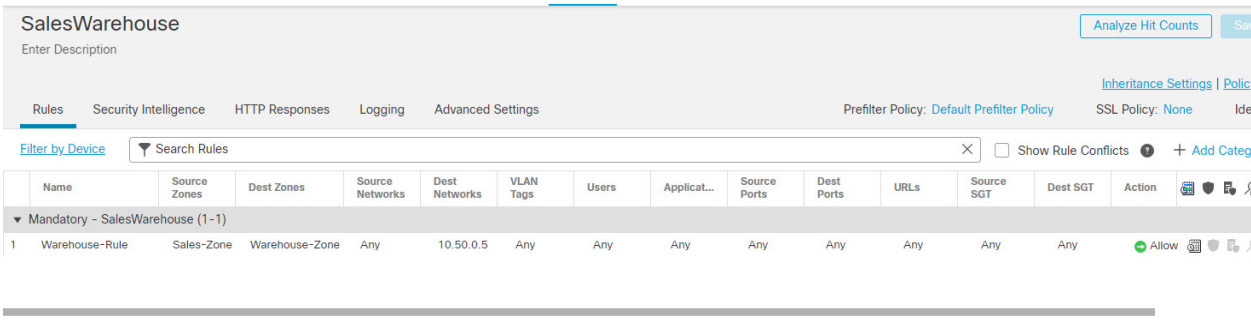
c) 点击**确定**。

d) 点击**保存 (Save)**。

步骤 8 配置允许访问仓库服务器的访问控制规则。要创建访问控制规则，您需要创建安全区域。使用**对象** > **对象管理** > **接口**。依次选择**添加** > **安全区域**并为“VR-Sales”和“VR-Warehouse”创建安全区域；对于Warehouse-Server 网络对象，创建 Warehouse-Server 接口组（依次选择**添加** > **接口组**）。

步骤 9 依次选择**策略** > **访问控制**并配置访问控制规则，以允许流量从“销售”虚拟路由器中的源接口到流向目的 Warehouse-Server 网络对象的“仓库”虚拟路由器中的目的接口。

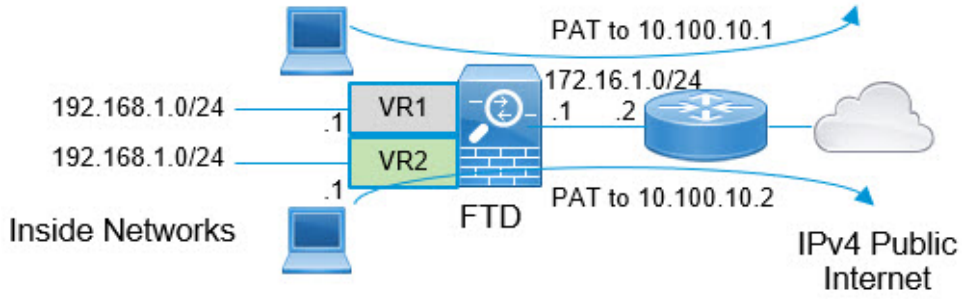
例如，如果“销售”虚拟路由器中的接口位于“销售区域”安全区域中，而“仓库”虚拟路由器中的接口位于“仓库区域”安全区域中，则访问控制规则将如下所述：



如何提供包含重叠地址空间的互联网访问权限

使用虚拟路由器时，您可以为驻留在单独路由器中的多个接口设置相同的网络地址。但是，由于在这些单独的虚拟路由器中路由的 IP 地址相同，因此请使用单独的 NAT/PAT 池为每个接口应用 NAT/PAT 规则，以确保返回流量到达正确的目的地。此示例提供了为管理重叠地址空间而配置虚拟路由器和 NAT/PAT 规则的程序。

例如，FTD 上的接口 vr1-inside 和 vr2-inside 被定义为使用 IP 地址 192.168.1.1/24，从而将终端托管在其在 192.168.1.0/24 网络中的分段上。要允许通过两个使用相同地址空间的虚拟路由器访问互联网，您需要将 NAT 规则分别应用于每个虚拟路由器中的接口，最好使用单独的 NAT 或 PAT 池。可以使用 PAT 将 VR1 中的源地址转换为 10.100.10.1，并将 VR2 中的源地址转换为 10.100.10.2。下图显示了此设置，其中面向互联网的外部接口是全局路由器的一部分。您必须使用明确选择的源接口（vr1-inside 和 vr2-inside）来定义 NAT/PAT 规则 - 使用“任何”作为源接口将使系统无法识别正确源，这是因为两个不同的接口上可能存在相同的 IP 地址。



注释 即使您拥有不使用重叠地址空间的虚拟路由器中的一些接口，也要用源接口定义NAT规则，以便简化故障排除过程，并确保更加清楚地区分来自与互联网绑定的各虚拟路由器之间的流量。

过程

步骤 1 为 VR1 配置设备的内部接口：

a) 依次选择**设备** > **设备管理** > **接口**。

b) 编辑您要分配给 VR1 的接口：

- **名称 (Name)** - 在此示例中为 vr1-inside。
- 选中**启用**复选框。
- 在 **IPV4** 中，对于 **IP 类型**，请选择**使用静态 IP**。
- **IP 地址 (IP Address)** - 输入 192.168.1.1/24。

c) 点击**确定**。

d) 点击**保存 (Save)**。

步骤 2 为 VR2 配置设备的内部接口：

a) 依次选择**设备** > **设备管理** > **接口**。

b) 编辑您要分配给 VR2 的接口：

- **名称 (Name)** - 在此示例中为 vr2-inside。
- 选中**启用**复选框。
- 在 **IPV4** 中，对于 **IP 类型**，请选择**使用静态 IP**。
- **IP 地址** - 将其留空。该系统不允许您使用相同的 IP 地址配置接口，因为您尚未创建用户定义的虚拟路由器。

c) 点击**确定**。

d) 点击**保存 (Save)**。

步骤 3 配置 VR1 和到外部接口的静态默认路由泄漏：

a) 依次选择**设备** > **设备管理**，然后编辑 FTD 设备。

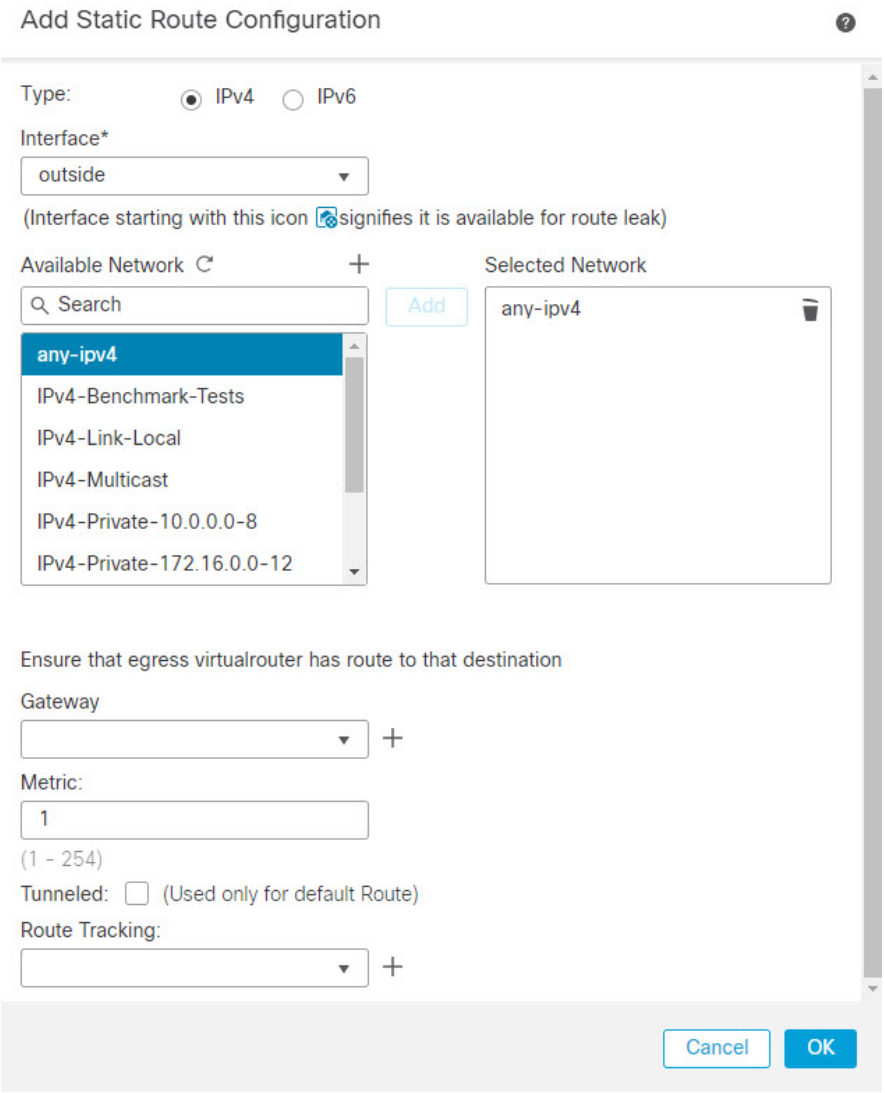
b) 依次选择**路由** > **管理虚拟路由器**。点击**添加虚拟路由器 (Add Virtual Router)**并创建 VR1。

c) 对于 VR1，在**虚拟路由器属性 (Virtual Router Properties)** 中分配 vr1-inside 并保存。

d) 点击**静态路由 (Static Route)**。

e) 点击**添加路由**。在**添加静态路由配置**中，指定以下内容：

- **接口 (Interface)** - 选择全局路由器的外部接口。
- **网络 (Network)** - 选择 any-ipv4 对象。这个网络是无法在 VR1 内路由的任何流量的默认路由。
- **网关** - 将其留空。将路由泄漏到另一个虚拟路由器时，请勿提供网关。



f) 点击**确定**。

g) 点击**保存 (Save)**。

步骤 4 配置 VR2 和到外部接口的静态默认路由泄漏：

a) 依次选择**设备** > **设备管理**，然后编辑 FTD 设备。

b) 依次选择**路由** > **管理虚拟路由器**。点击**添加虚拟路由器 (Add Virtual Router)**并创建 VR2。

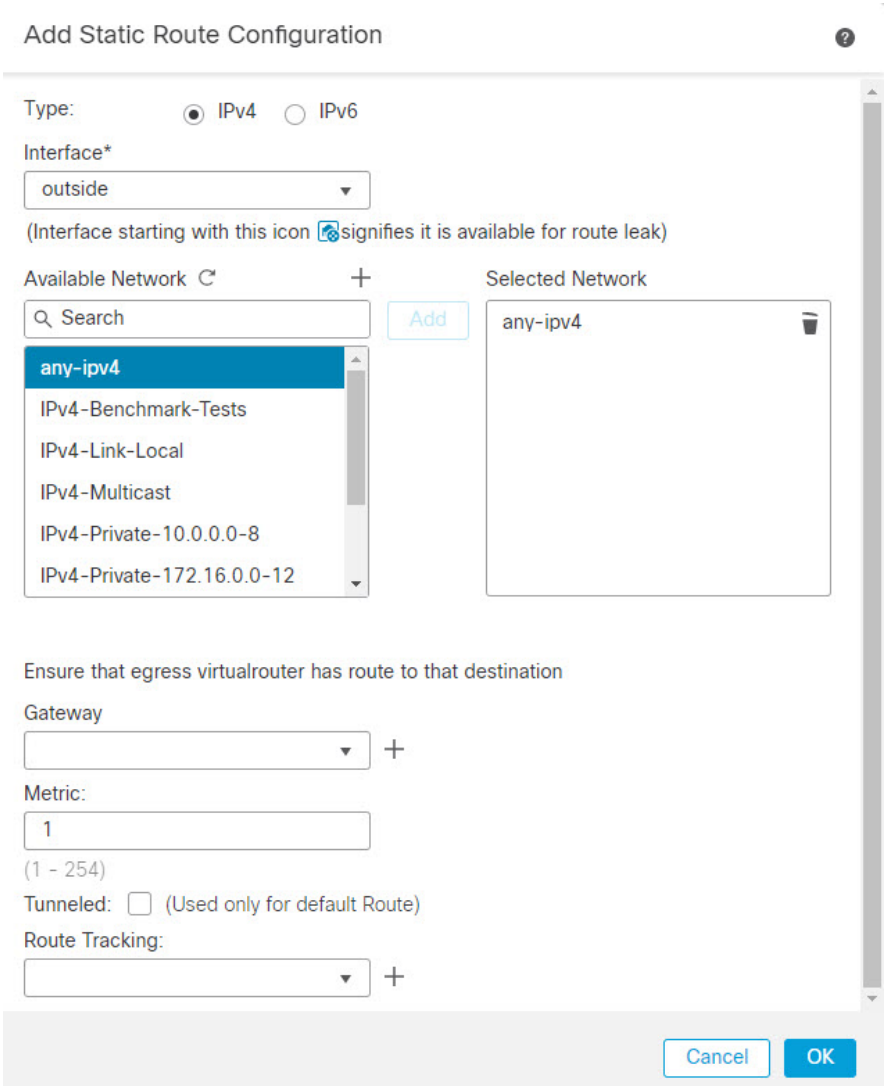
c) 对于 VR2，在**虚拟路由器属性 (Virtual Router Properties)** 中分配 vr2-inside 并保存。

d) 点击**静态路由 (Static Route)**。

e) 点击**添加路由**。在**添加静态路由配置**中，指定以下内容：

- **接口 (Interface)** - 选择全局路由器的外部接口。
- **网络 (Network)** - 选择 any-ipv4 对象。这个网络是无法在 VR2 内路由的任何流量的默认路由。

- **网关** - 将其留空。将路由泄漏到另一个虚拟路由器时，请勿选择网关。



f) 点击**确定**。

g) 点击**保存 (Save)**。

步骤 5 在全局路由器的外部接口上配置 IPv4 静态默认路由，即 172.16.1.2：

a) 依次选择**设备** > **设备管理**，然后编辑 FTD 设备。

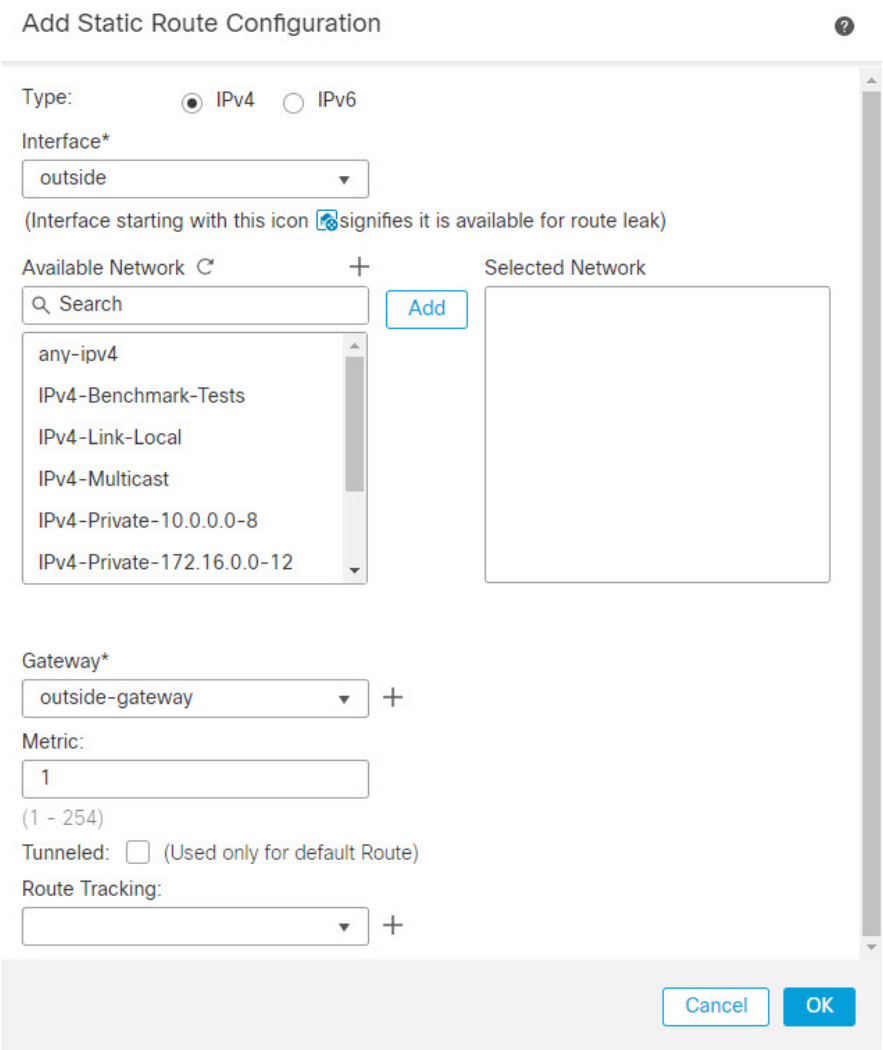
b) 选择**路由 (Routing)** 并编辑全局路由器属性。

c) 点击**静态路由 (Static Route)**。

d) 点击**添加路由**。在**添加静态路由配置**中，指定以下内容：

- **接口 (Interface)** - 选择全局路由器的外部接口。
- **网络 (Network)** - 选择 any-ipv4 对象。这将是用于任何 IPv4 流量的默认路由。

- **网关 (Gateway)** - 如果已创建，请从下拉列表中选择主机名。如果尚未创建对象，请点击**添加 (Add)**，然后为外部接口上网络链路另一端的网关的 IP 地址（在本例中为 172.16.1.2）定义主机对象。创建对象后，在“网关”(Gateway) 字段中选择该对象。



e) 点击**确定**。

f) 点击**保存 (Save)**。

步骤 6 重新访问 vr2-inside 接口配置：

a) 依次选择**设备** > **设备管理** > **接口**。

b) 点击 vr2-inside 接口的**编辑 (Edit)**。将 IP 地址指定为 192.168.1.1/24。现在，由于接口分别分配给两个不同的虚拟路由器，因此系统允许您使用 vr1-inside 的相同 IP 地址进行配置。

c) 点击**确定**。

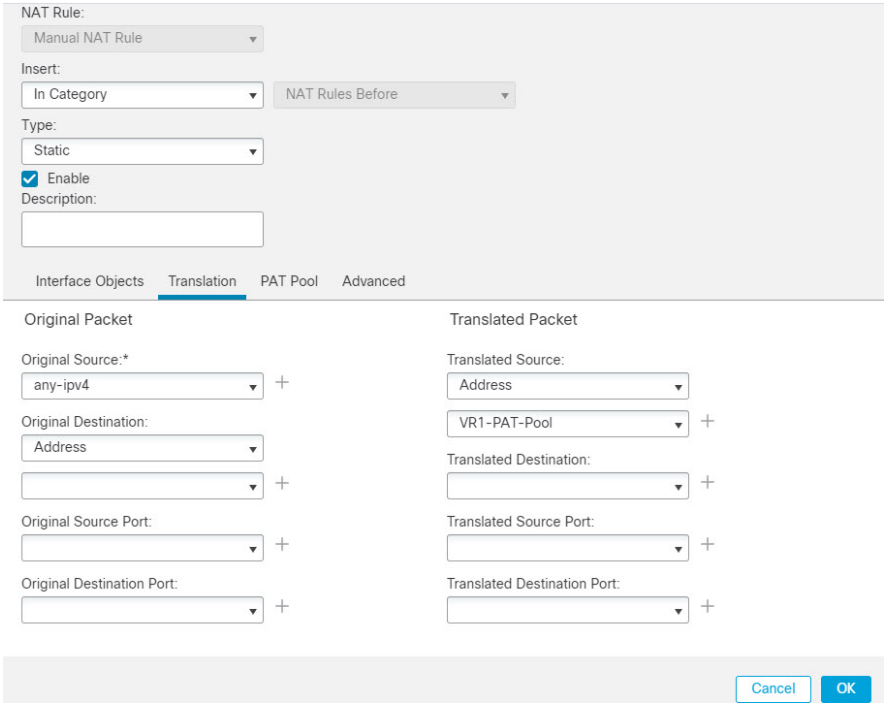
d) 点击**保存 (Save)**。

步骤 7 创建 NAT 规则，以将 VR1 的 PAT 内-外流量传输到 10.100.10.1。

a) 选择**设备** > **NAT**。

b) 点击**新策略 (New Policy)** > **威胁防御 NAT (Threat Defense NAT)**。
c) 输入 InsideOutsideNATRule 作为 NAT 策略名称，然后选择 FTD 设备。单击**保存**。
d) 在 InsideOutsideNATRule 页面中，点击**添加规则 (Add Rule)** 并定义以下内容：

- **NAT 规则 (NAT Rule)** - 选择“手动 NAT 规则”(Manual NAT Rule)。
- **类型 (Type)** - 选择“动态”(Dynamic)。
- **插入 (Insert)** - 如果存在任何动态 NAT 规则，则选择“上方”(Above)。
- 点击 **Enabled**。
- 在**接口对象 (Interface Objects)**中，选择 vr1-interface 对象，然后点击**添加到源 (Add to Source)**（如果对象不可用，请在**对象 (Object)** > **对象管理 (Object Management)** > **接口 (Interface)** 中创建一个对象），然后选择外部作为**添加到目标 (Add to Destination)**。
- 在**转换 (Translation)**中，为**原始源 (Original Source)** 选择 any-ipv4。对于**转换的源 (Translated Source)**，点击**添加 (Add)** 并使用 10.100.10.1 来定义主机对象 VR1-PAT-Pool。选择 VR1-PAT-Pool，如下图所示：



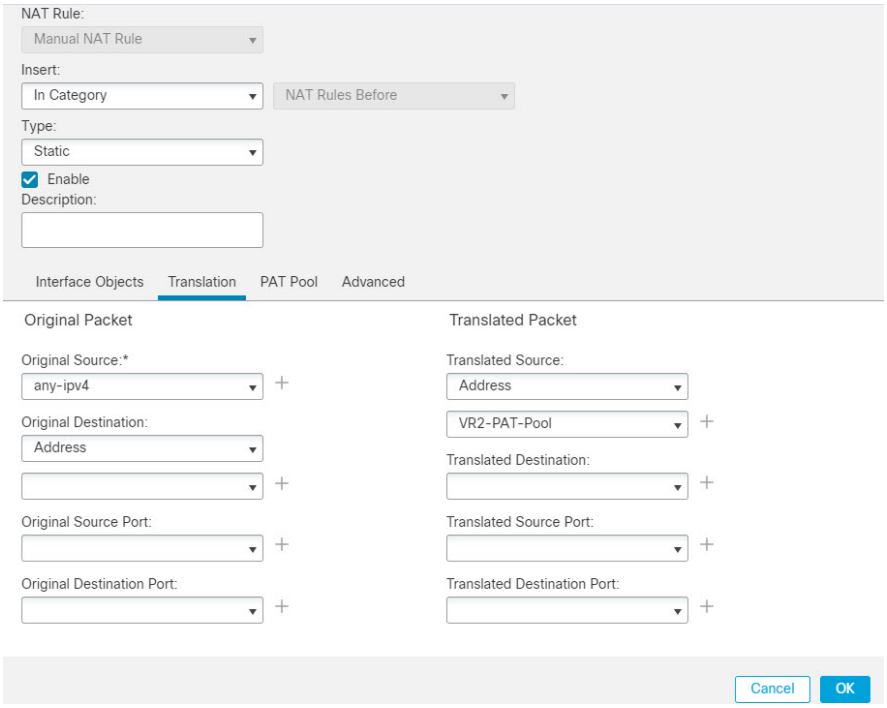
e) 点击**确定**。
f) 点击**保存 (Save)**。

步骤 8 添加 NAT 规则，以将 VR2 的 PAT 内-外流量传输到 10.100.10.2。

a) 选择**设备** > **NAT**。
b) 编辑 InsideOutsideNATRule 以定义 VR2 NAT 规则：

- **NAT 规则 (NAT Rule)** - 选择“手动 NAT 规则”(Manual NAT Rule)。

- **类型 (Type)** - 选择“动态”(Dynamic)。
- **插入 (Insert)** - 如果存在任何动态 NAT 规则，则选择“上方”(Above)。
- 点击 **Enabled**。
- 在**接口对象 (Interface Objects)**中，选择 vr2-interface 对象，然后点击**添加到源 (Add to Source)**（如果对象不可用，请在**对象 (Object)** > **对象管理 (Object Management)** > **接口 (Interface)** 中创建一个对象），然后选择外部作为**添加到目标 (Add to Destination)**。
- 在**转换 (Translation)**中，为**原始源 (Original Source)** 选择 any-ipv4。对于**转换的源 (Translated Source)**，点击**添加 (Add)** 并使用 10.100.10.2 来定义主机对象 VR2-PAT-Pool。选择 VR2-PAT-Pool，如下图所示：



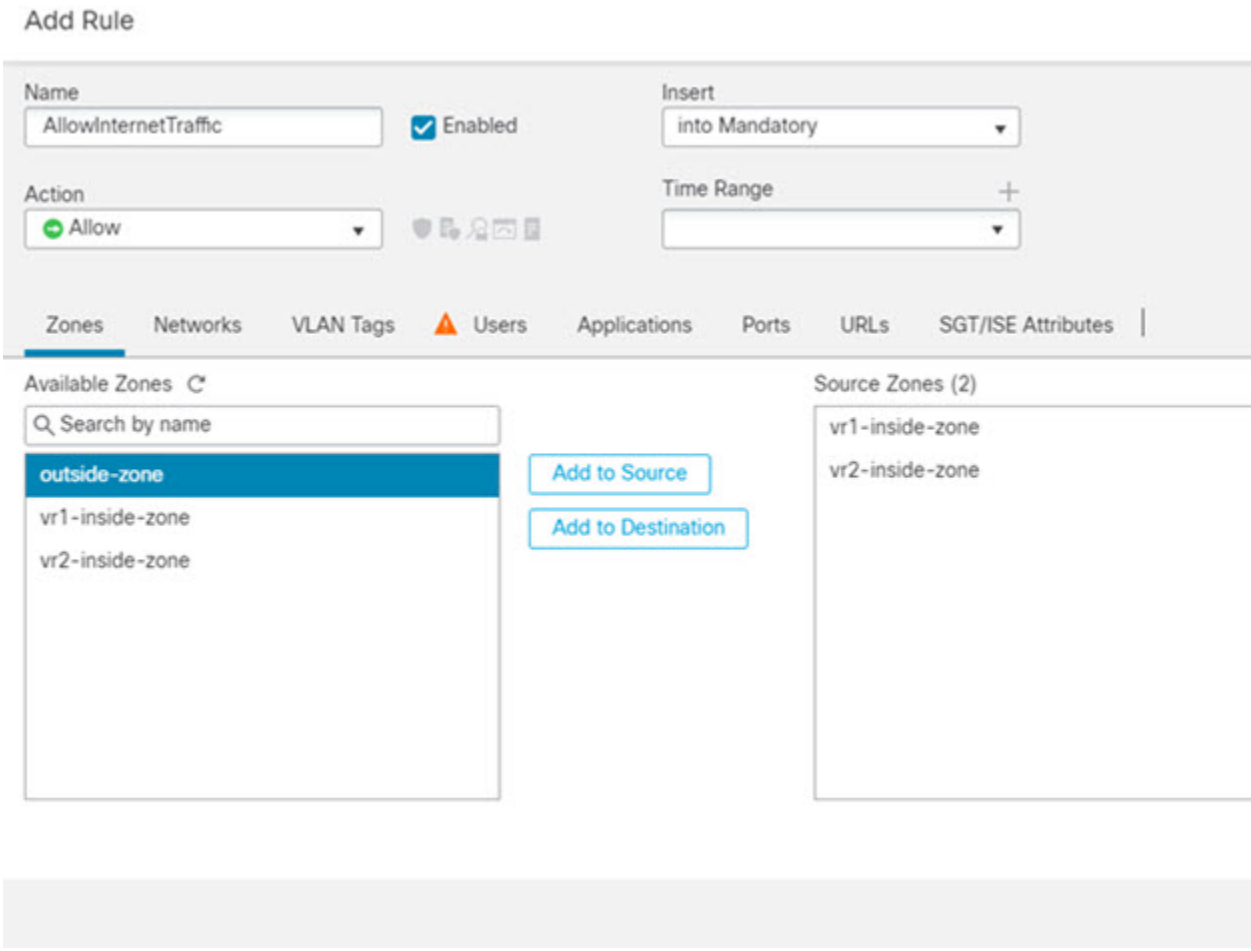
c) 点击**确定**。

d) 点击**保存 (Save)**。

步骤 9 要配置允许流量从 vr1-inside 和 vr2-inside 接口流向外部接口的访问控制策略，您需要创建安全区域。使用**对象** > **对象管理** > **接口**。选择**添加 (Add)** > **安全区域 (Security Zone)** 并为 vr1-inside、vr2-inside 和外部接口创建安全区域。

步骤 10 选择**策略 (Policies)** > **访问控制 (Access Control)**，然后配置访问控制规则以允许将 vr1-inside-zone 和 vr2- inside-zone 中的流量传输到 outside-zone。

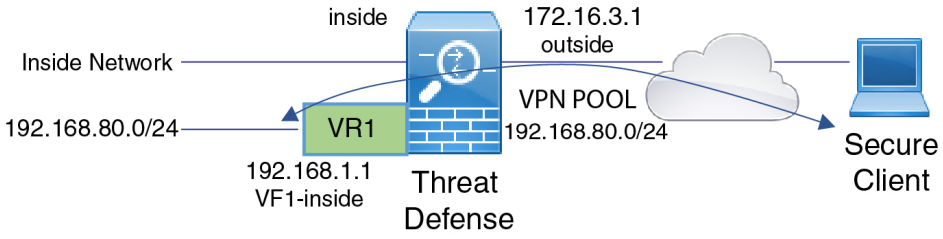
假设您创建了以接口命名的区域，则允许所有流量流向互联网的基本规则将如下所示：您可以将其他参数应用于此访问控制策略：



如何允许对虚拟路由中的内部网络进行 RA VPN 访问

在启用虚拟路由的设备上，只有全局虚拟路由器接口上支持 RA VPN。此示例提供允许 Secure Client 用户连接到用户定义的虚拟路由器网络的程序。

在下面的示例中，RA VPN（Secure Client）用户连接到地址为 172.16.3.1 的 威胁防御 外部接口，并在 192.168.80.0/24 池中获得 IP 地址。该用户只能访问全局虚拟路由器的内部网络。要允许流量通过用户定义的虚拟路由器 VR1 的网络（即 192.168.1.0/24），请通过在全局和 VR1 上配置静态路由来泄漏路由。



开始之前

此示例假设您已配置 RA VPN，定义虚拟路由器，配置接口并将其分配给相应的虚拟路由器。

过程

步骤 1 配置从全局虚拟路由器到用户自定义 VR1 的路由泄漏。

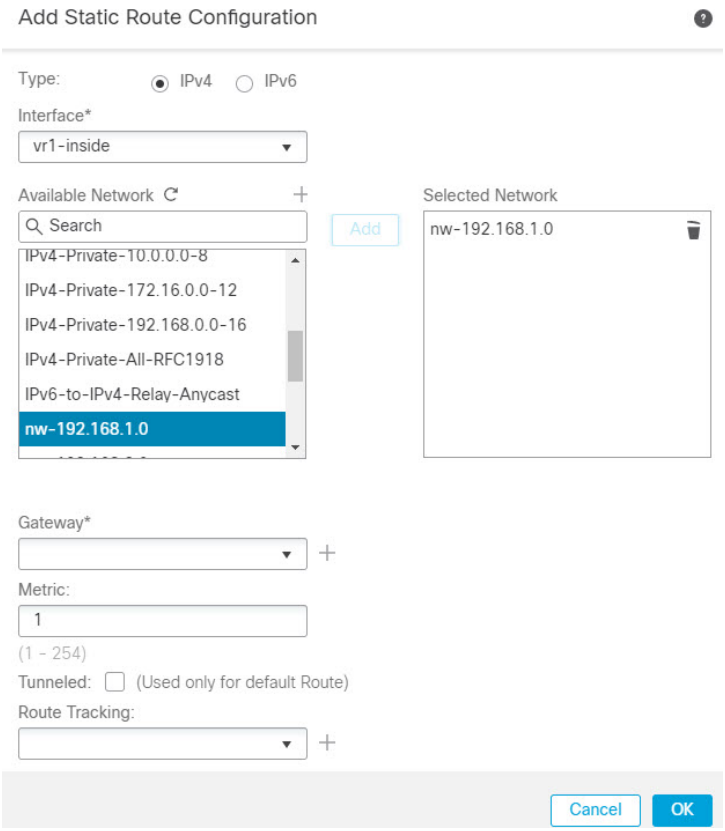
a) 依次选择 **设备** > **设备管理**，并且编辑 威胁防御 设备。

b) 点击**路由**。默认情况下，系统将显示“全局路由属性”(Global routing properties) 页面。

c) 点击**静态路由 (Static Route)**。

d) 点击**添加路由**。在**添加静态路由配置**中，指定以下内容：

- **接口 (Interface)** - 选择 VR1 内部接口。
- **网络 (Network)** - 选择 VR1 虚拟路由器网络对象。您可以使用**添加对象 (Add Object)** 选项创建一个。
- **网关** - 将其留空。将路由泄漏到另一个虚拟路由器时，请勿选择网关。



此路由泄露允许在 VPN 池中分配 IP 地址的 Secure Client 访问 VR1 虚拟路由器中的 192.168.1.0/24 网络。

e) 点击**确定**。

步骤 2 配置从 VR1 到全局虚拟路由器的路由泄漏：

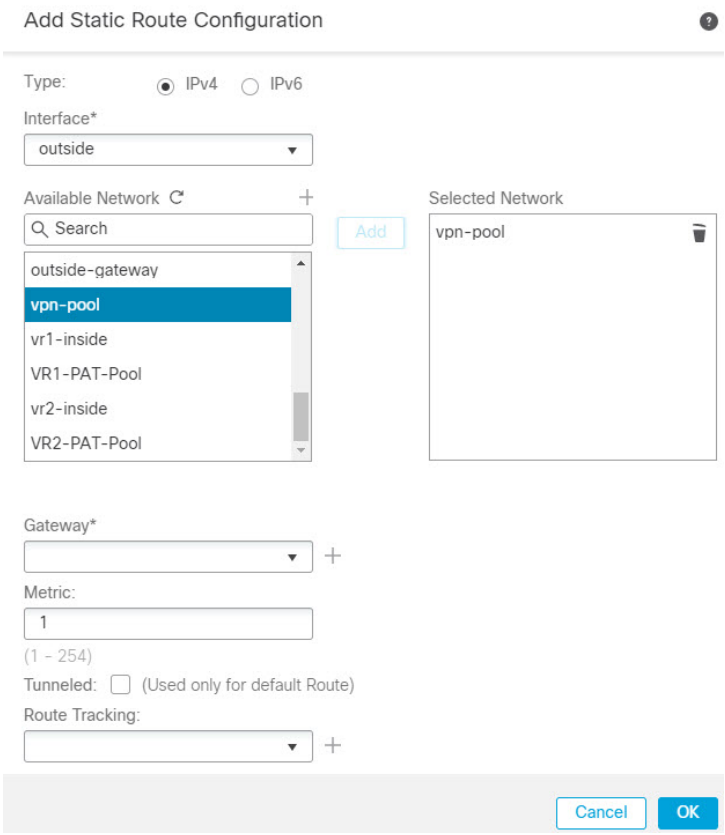
a) 依次选择 **设备** > **设备管理**，并且编辑 威胁防御 设备。

b) 点击**路由 (Routing)**，然后从下拉列表中选择 VR1。

c) 点击**静态路由 (Static Route)**。

d) 点击**添加路由**。在**添加静态路由配置**中，指定以下内容：

- **接口 (Interface)** - 选择全局路由器的外部接口。
- **网络 (Network)** - 选择全局虚拟路由器网络对象。
- **网关** - 将其留空。将路由泄漏到另一个虚拟路由器时，请勿选择网关。



配置的静态路由允许 192.168.1.0/24 网络 (VR1) 上的终端向在 VPN 池中分配 IP 地址的 Secure Client 发起连接。

e) 点击**确定**。

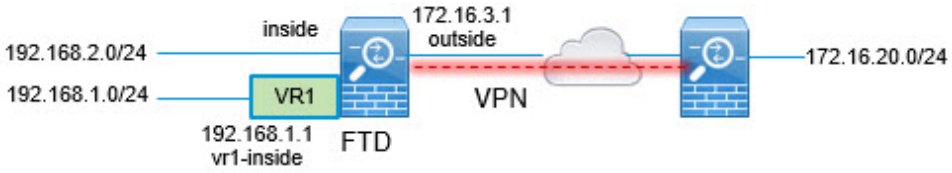
下一步做什么

如果 RA VPN 地址池与用户定义的虚拟路由器中的 IP 地址重叠，则还必须对 IP 地址使用静态 NAT 规则，以启用正确的路由。或者，您可以更改 RA VPN 地址池，以免出现重叠。

如何通过站点间 VPN 保护来自多个虚拟路由器的网络流量

在启用虚拟路由的设备上，只有全局虚拟路由器接口上支持站点间 VPN。您不能在属于用户定义的虚拟路由器的接口上配置它。此示例提供的程序让您能够通过站点间VPN保护来自或到达用户定义的虚拟路由器内的网络的连接。您还需要更新站点间VPN连接，以包括这些用户定义的虚拟路由网络。

我们假设这样一个场景：在分支机构网络和公司总部网络之间配置站点间 VPN；分支机构中的FTD具有虚拟路由器。在这种情况下，站点间 VPN 在 172.16.3.1 的分支机构外部接口上定义。此 VPN 包括内部网络 192.168.2.0/24，而无需进行额外配置，因为内部接口也是全局虚拟路由器的一部分。但是，要为 192.168.1.0/24 网络（其为 VR1 虚拟路由器的一部分）提供站点间 VPN 服务，则必须通过在全局和 VR1 上配置静态路由来泄露路由，并将 VR1 网络加入站点间的 VPN 配置中。



开始之前

此示例假设您已在本地网络 192.168.2.0/24 与外部网络 172.16.20.0/24 之间配置站点间 VPN，定义虚拟路由器，配置接口并将其分配给相应的虚拟路由器。

过程

步骤 1 配置从全局虚拟路由器到用户自定义 VR1 的路由泄漏：

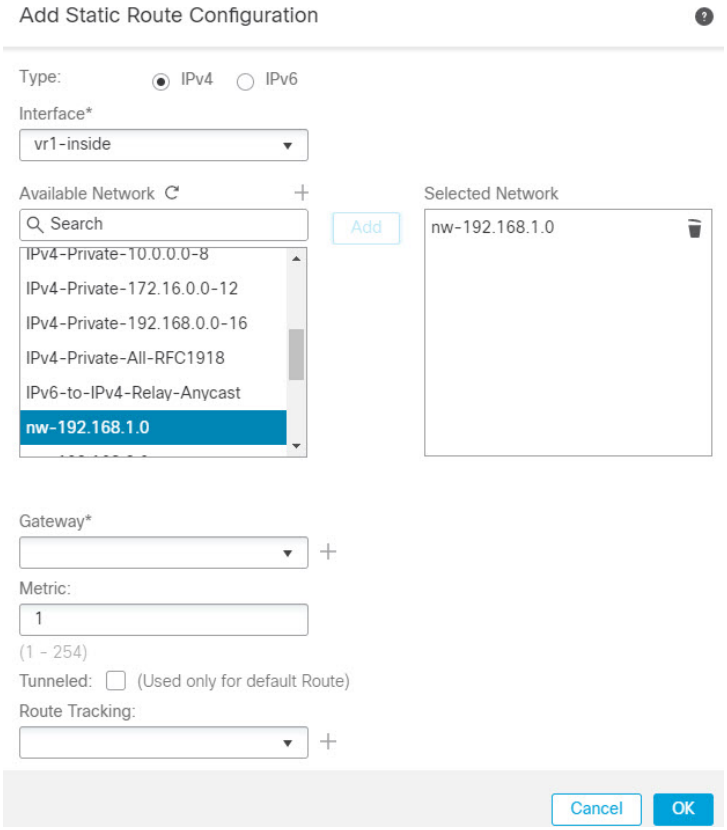
a) 依次选择**设备** > **设备管理**，然后编辑 FTD 设备。

b) 点击**路由**。默认情况下，系统将显示“全局路由属性”(Global routing properties) 页面。

c) 点击**静态路由 (Static Route)**。

d) 点击**添加路由**。在**添加静态路由配置**中，指定以下内容：

- **接口 (Interface)** - 选择 VR1 内部接口。
- **网络 (Network)** - 选择 VR1 虚拟路由器网络对象。您可以使用**添加对象 (Add Object)** 选项创建一个。
- **网关** - 将其留空。将路由泄漏到另一个虚拟路由器时，请勿选择网关。



此路由泄漏允许受站点间 VPN 的外部（远程）终端保护的终端访问 VR1 虚拟路由器中的 192.168.1.0/24 网络。

e) 点击**确定**。

步骤 2 配置从 VR1 到全局虚拟路由器的路由泄漏：

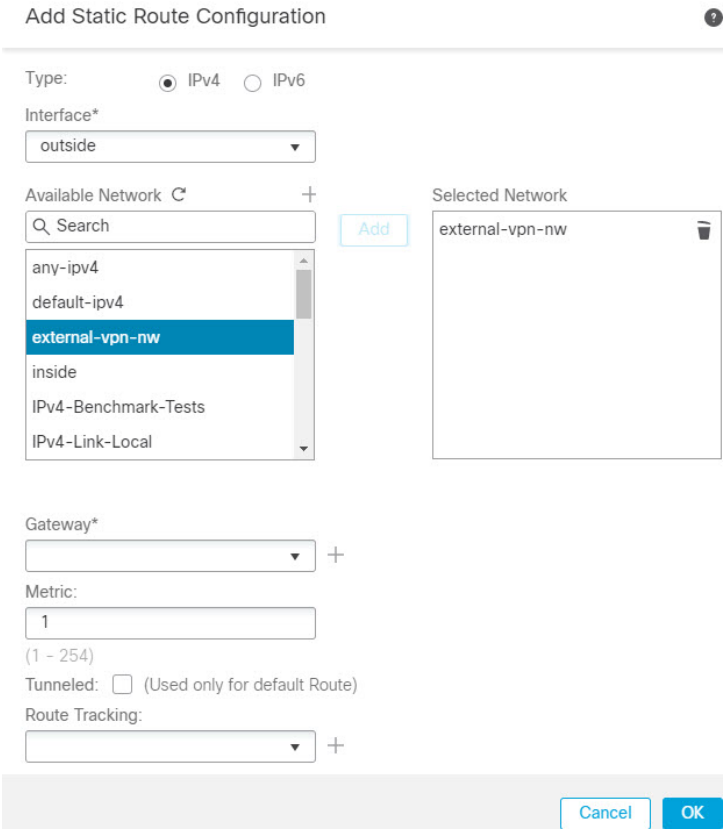
a) 依次选择**设备** > **设备管理**，然后编辑 FTD 设备。

b) 点击**路由 (Routing)**，然后从下拉列表中选择 VR1。

c) 点击**静态路由 (Static Route)**。

d) 点击**添加路由**。在**添加静态路由配置**中，指定以下内容：

- **接口 (Interface)** - 选择全局路由器的外部接口。
- **网络 (Network)** - 选择全局虚拟路由器网络对象。
- **网关** - 将其留空。将路由泄漏到另一个虚拟路由器时，请勿选择网关。



此静态路由允许 192.168.1.0/24 网络 (VR1) 上的终端发起流经站点间 VPN 隧道的连接。在本示例中，远程终端正在保护 172.16.20.0/24 网络。

e) 点击**确定**。

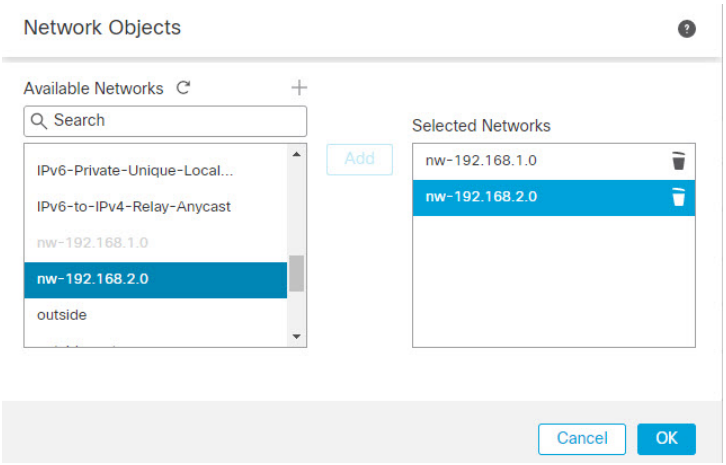
步骤 3 将 192.168.1.0/24 网络添加到站点间 VPN 连接配置文件中：

a) 选择**设备 (Devices)** > **VPN** > **站点间 (Site To Site)**，然后编辑 VPN 拓扑。

b) 在**终端 (Endpoints)** 中，编辑节点 A 终端。

c) 在**编辑终端 (Edit Endpoint)** 的**受保护网络 (Protected Networks)** 字段中，点击**添加新网络对象 (Add New Network Object)**。

d) 添加网络为 192.168.1.0 的 VR1 网络对象：



e) 点击**确定 (Ok)** 并保存配置。

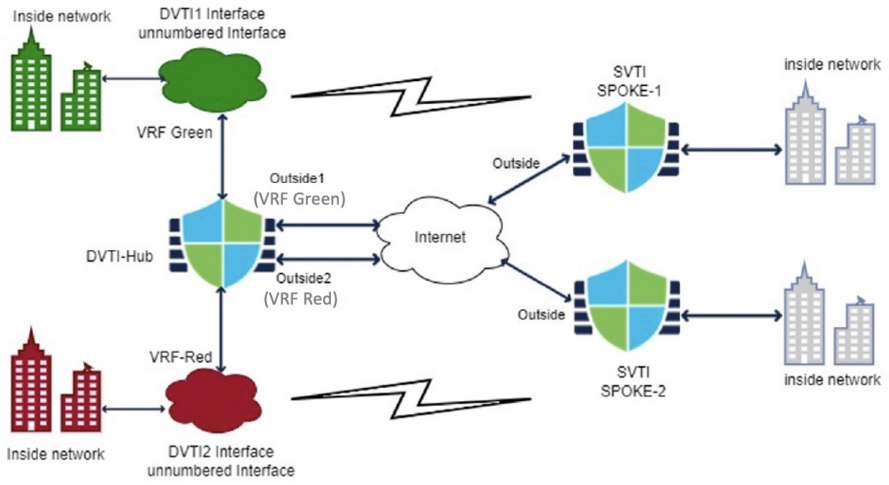
如何使用动态 VTI 通过站点间 VPN 保护来自多个虚拟路由器的网络流量

ISP 为不同的客户提供不同的分段网络。您可以创建虚拟路由器，将动态 VTI 与这些虚拟路由器关联，并在网络中扩展动态 VTI 的功能。可以将动态 VTI 与全局或用户定义的虚拟路由器关联。单个威胁防御设备可以充当具有全局或一个或多个用户定义的虚拟路由器的动态 VTI 中枢。每个用户定义的虚拟路由器都可以是一个客户网络。

让我们考虑在两个公司总部网络与其两个分支机构网络之间配置基于路由的站点到站点 VPN 的示例。ISP 的威胁防御是一个动态 VTI 集线器，它使用两个用户定义的虚拟路由器管理两个公司总部网络：VRF 绿色和 VRF 红色。动态 VTI 集线器在以下对象之间建立站点间 VPN：

- 客户 1（VRF 绿色）和分支机构 1（SVTI 分支 1）
- 客户 2（VRF 红色）和分支机构 2（SVT2 分支 2）

图 *2:* 具有多个虚拟路由器和动态 *VTI* 的站点间 *VPN*



此示例说明如何通过具有动态 VTI 的站点间 VPN 配置具有多个虚拟路由器的网络。

过程

步骤 1 在集线器上配置动态 VTI 接口。

a) 依次选择 **设备 > 设备管理**，并且编辑威胁防御设备。
b) 选择 **添加接口 > 虚拟隧道接口**。
c) 选择 **动态** 作为**隧道类型** 。
d) 将接口名称指定为 DVTI1，并为动态 VTI 配置所有参数。
e) 点击**保存**
f) 重复步骤 1a - e，在集线器 DVTI2 上配置第二个动态 VTI。

步骤 2 在分支 1 上配置静态 VTI。

a) 依次选择 **设备 > 设备管理**，并且编辑威胁防御设备。
b) 选择 **添加接口 > 虚拟隧道接口**。
c) 选择 **隧道类型** 作为 **静态**。
d) 将接口名称指定为 SVTI Spoke-1，并为静态 VTI 配置所有参数。
e) 点击**保存**
f) 重复步骤 2a - e，在分支 2 上配置静态 VTI：SVTI 分支 2。

步骤 3 为中心和 SVTI 1辐射型拓扑配置路由型站点间 VPN。

a) 依次选择 **设备 > 站点间**，然后点击 **+ 站点间 VPN**。
b) 在 **拓扑名称** 字段中，输入 VPN 拓扑的名称。
c) 选择 **基于路由 (VTI)** 并选择 **中心辐射型** 作为网络拓扑。
d) 点击 **终端** 选项卡。
e) 配置中心和分支（DVTI1 和 SVTI 分支 1）及其路由策略。
f) 如果需要，为 VPN 配置 **IKE**、 **IPsec**和 **高级** 选项。

g) 单击**保存**。

h) 重复步骤 3a - g，在中心 (DVTI2) 和 SVTI 分支 2 之间配置第二个基于路由的站点间 VPN 拓扑。

步骤 4 配置两个虚拟路由器。

a) 依次选择 **设备 > 设备管理**，并且编辑威胁防御设备。

b) 点击**路由**。

c) 点击**管理虚拟路由器**。

d) 点击 **Add Virtual Router**。

将名称指定为 VRF 绿色，并提供虚拟路由器的说明。

e) 重复步骤 4a-d，配置 VRF 红色。

步骤 5 将所有接口分配给虚拟路由器。

a) 从下拉列表中，选择虚拟路由器。

b) 在 **虚拟路由器属性** 页面中，选择 **可用接口** 框下列出的接口。

将动态 VTI 接口与其他接口一起分配。

c) 点击**添加 (Add)**。

步骤 6 对 VRF 红色重复步骤 5a-c。

步骤 7 配置虚拟路由器的路由策略。

a) 从下拉列表中，选择虚拟路由器。

b) 点击 **静态路由** 或其中一种动态路由协议。

c) 配置路由参数。

d) 单击**保存**。

下一步做什么

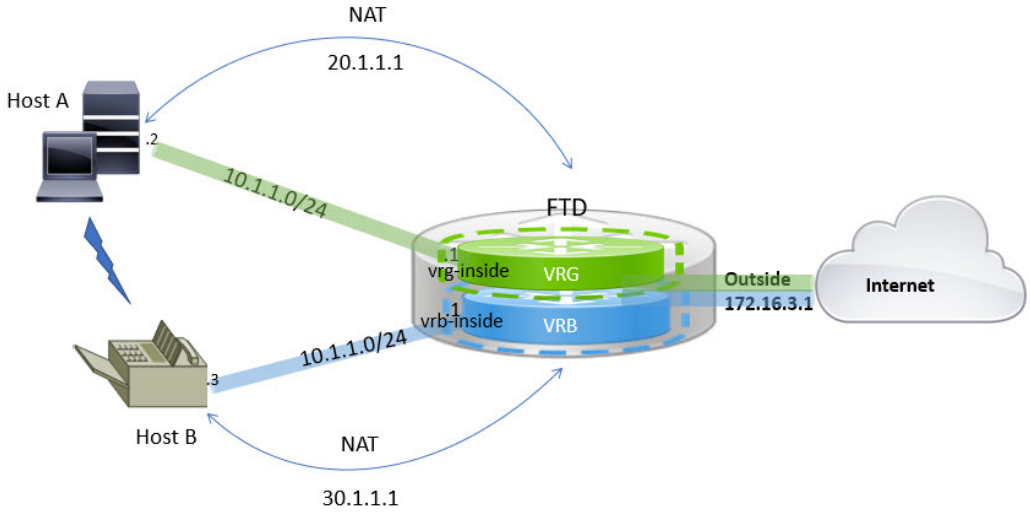
选择中心辐射型设备，然后点击 **部署**。部署后，您可以在站点到站点监控控制面板（**概述 > 站点间 VPN**）中监控 VPN 隧道。

您还可以使用 监控虚拟路由器，第 15 页 中列出的命令查看虚拟路由器并对其进行故障排除。

如何在虚拟路由中的两个重叠网络主机之间路由流量

您可以在具有相同网络地址的虚拟路由器上配置主机。如果主机想要通信，您可以配置两次 NAT。本示例提供了配置 NAT 规则以管理重叠网络主机的程序。

在下面的示例中，两台主机主机 A 和主机 B 属于不同的虚拟路由器：VRG（接口 vrg-inside）和 VRB（接口 vrb-inside），分别具有相同的子网 10.1.1.0/24。要让两台主机通信，请创建一个 NAT 策略，其中 VRG 主机接口对象将使用映射 NAT 地址 - 20.1.1.1，而 VRB 主机接口对象将使用映射 NAT 地址 - 30.1.1.1。因此，主机 A 会使用 30.1.1.1 与主机 B 通信；主机 B 会使用 20.1.1.1 访问主机 A。



开始之前

此示例假定您已：

- vrg-inside 和 vrb-inside 接口分别与虚拟路由器关联：VRG 和 VRB 以及配置了相同子网地址的 vrg-inside 和 vrb-inside 接口（例如 10.1.1.0/24）。
- 分别使用 vrg-inside 和 vrb-inside 接口创建的接口区域 VRG-Inf、VRB-Inf。
- VRG 中的主机 A，默认网关为 vrg-inside；主机 B 位于 VRB 中，vrb-inside 作为默认网关。

过程

步骤 1 创建 NAT 规则以处理从主机 A 到主机 B 的流量。选择**设备 (Devices)** > **NAT**。

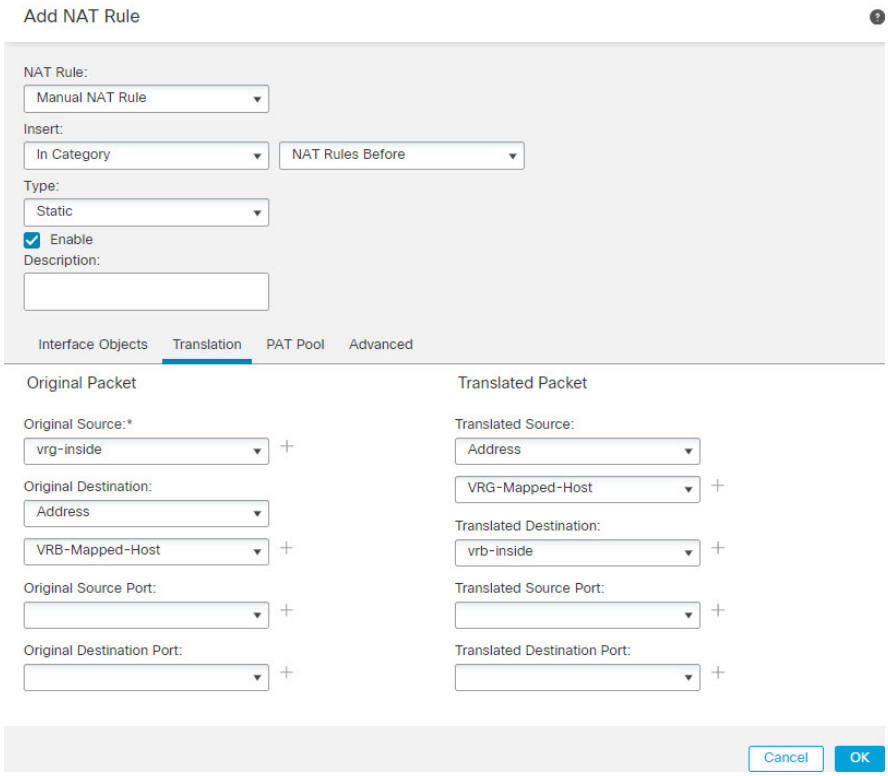
步骤 2 点击**新策略 (New Policy)** > **威胁防御 NAT (Threat Defense NAT)**。

步骤 3 输入 NAT 策略名称，然后选择 威胁防御 设备。单击**保存**。

步骤 4 在 NAT 页面中，点击**添加规则 (Add Rule)** 并定义以下内容：

- **NAT 规则 (NAT Rule)** - 选择“手动 NAT 规则”(Manual NAT Rule)。
- **类型 (Type)** - 选择“静态”(Static)。
- **插入 (Insert)** - 如果存在任何 NAT 规则，则选择“上方”(Above)。
- 点击 **Enabled**。
- 在**接口对象 (Interface Objects)**中，选择 VRG-Inf 对象，然后点击**添加到源 (Add to Source)**（如果对象不可用，请在**对象 (Object)** > **对象管理 (Object Management)** > **接口 (Interface)** 中创建一个对象），然后选择 VRG-Inf 对象并点击**添加到目标 (Add to Destination)**。
- 在**转换 (Translation)** 中选择以下选项：
  - **原始源 (Original Source)**，选择 vrg-inside。

- **原始目标 (Original Destination)**，点击**添加 (Add)** 并使用 30.1.1.1 定义对象 VRB-Mapped-Host。选择 VRB 映射主机。
- **转换后的源 (Translated Source)**，，点击**添加 (Add)** 并使用 20.1.1.1 定义对象 VRG-Mapped-Host。选择 VRG 映射主机。
- **转换后的目标 (Translated Destination)**，选择 vrb-inside，如下图所示：



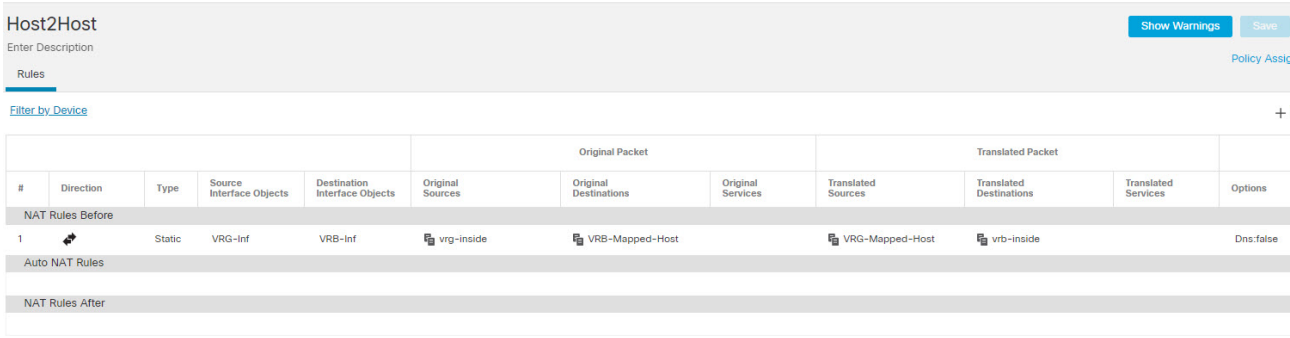
在 威胁防御 设备上运行 **show nat detail** 命令时，您将看到类似于以下内容的输出：

```
firepower(config-service-object-group)# show nat detail
Manual NAT Policies (Section 1)
1 (2001) to (3001) source static vrg-inside VRG-MAPPED-HOST destination static VRB-MAPPED-HOST
 vrb-inside
translate_hits = 0, untranslate_hits = 0
Source - Origin: 10.1.1.1/24, Translated: 20.1.1.1/24
Destination - Origin: 30.1.1.1/24, Translated: 10.1.1.1/24
```

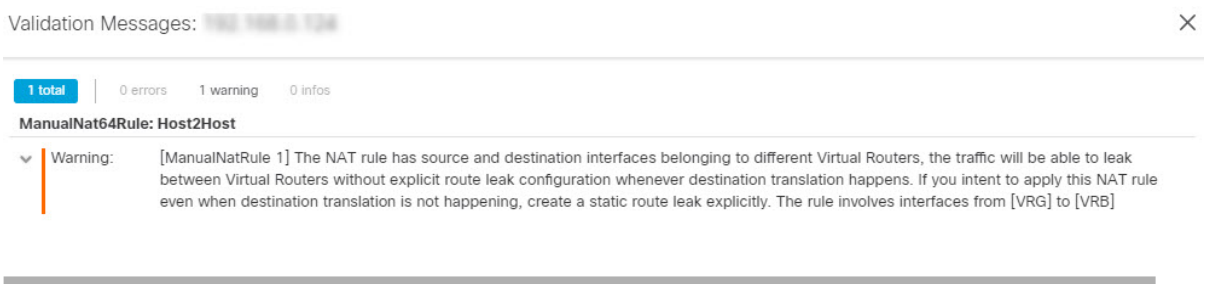
步骤 5 点击**确定**。

步骤 6 点击**保存 (Save)**。

NAT 规则如下所示：



在部署配置时会出现一条警告消息：

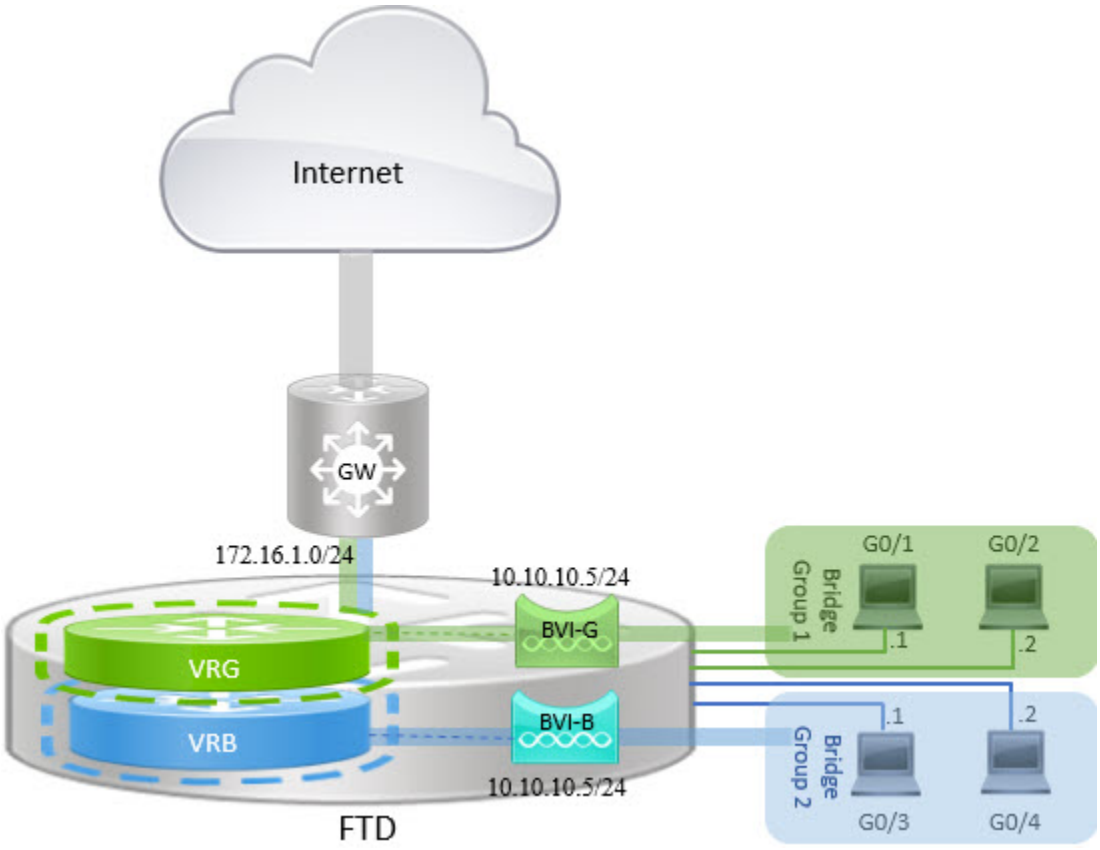


如何使用 BVI 接口在路由防火墙模式下管理重叠网段

您可以在多个重叠网络之间透明地部署单个FTD和/或在同一网络的主机之间部署防火墙。要实现此部署，请按虚拟路由器来配置 BVI。下面介绍了在虚拟路由器中配置 BVI 的程序。

BVI 是路由器内的虚拟接口，其作用类似于普通路由接口。它不支持网桥，但表示路由器内路由接口的可比较网桥组。传入或传出这些桥接接口的所有数据包都会通过 BVI 接口。BVI 的接口编号是虚拟接口所代表的网桥组的编号。

在以下示例中，在 VRG 中配置了 BVI-G，而网桥组 1 是接口 G0/1 和 G0/2 的路由接口。同样，在 VRB 中配置了 BVI-B，网桥组 2 是接口 G0/3 和 G0/4 的路由接口。假设两个 BVI 具有相同的 IP 子网地址，例如 10.10.10.5/24。由于虚拟路由器，网络会在共享资源上被隔离。



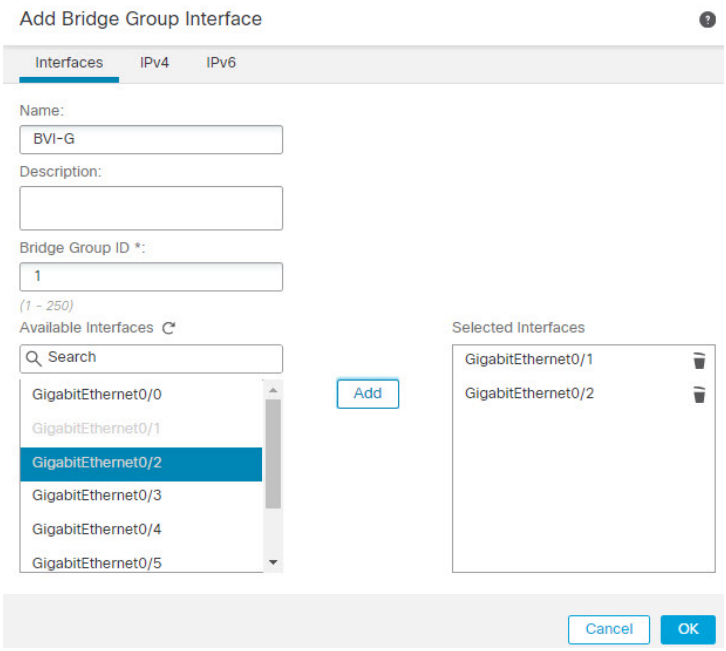
过程

步骤 1 选择**设备** > **设备管理**。编辑所需的设备。

步骤 2 在**接口 (Interfaces)** 中，选择**添加接口 (Add Interfaces)** > **网桥组接口 (Bridge Group Interface)**。

a) 为 BVI-G 输入下列详细信息：

- **名称 (Name)** - 在此示例中，为 BVI-G。
- **网桥组 ID (Bridge Group ID)** - 在本例中为 1。
- **可用接口 (Available Interface)** - 选择接口。
- 在 **IPV4** 中，对于 **IP 类型**，请选择**使用静态 IP**。
- **IP 地址 (IP Address)** - 输入 10.30.0.1/24。

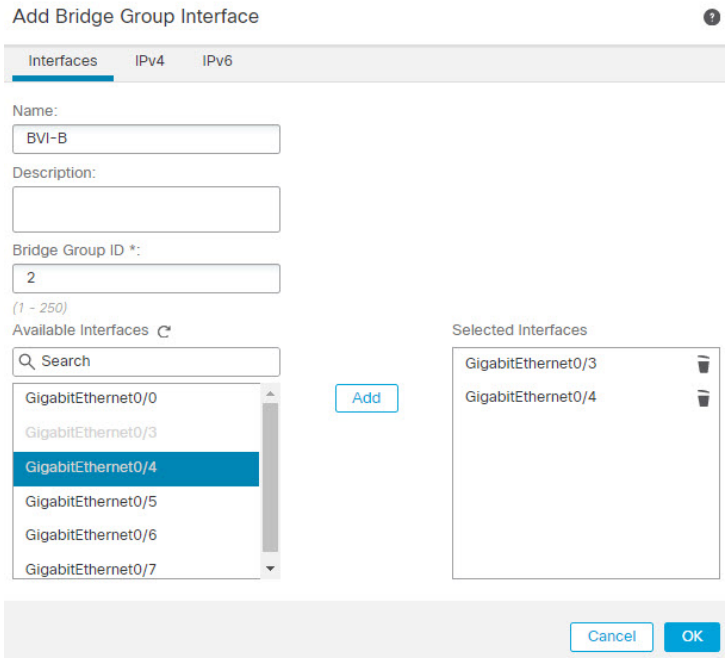


b) 点击**确定**。

c) 点击**保存 (Save)**。

a) 为 BVI-B 输入下列详细信息：

- **名称 (Name)** - 在此示例中，为 BVI-B。
- **网桥组 ID (Bridge Group ID)** - 在本例中为 2。
- **可用接口 (Available Interface)** - 选择子接口。
- 在 **IPV4** 中，对于 **IP 类型**，请选择**使用静态 IP**。
- **IP 地址 (IP Address)** - 将此字段留空，因为系统不允许两个接口具有重叠的 IP 地址。您可以重新访问网桥组并在虚拟路由器下对齐后提供相同的 IP 地址。



b) 点击**确定**。

c) 点击**保存 (Save)**。

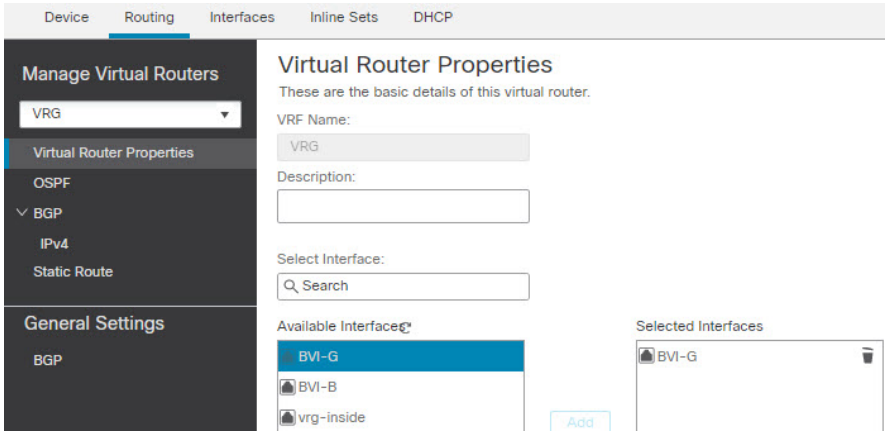
步骤 3 创建虚拟路由器，例如 VRG，然后选择 BVI-G 作为其网络：

a) 选择**设备** > **设备管理**。

b) 编辑设备，然后选择**路由 (Routing)** > **管理虚拟路由器 (Manage Virtual Routers)**。

c) 点击 **Add Virtual Router**。输入虚拟路由器的名称，然后点击**确定 (Ok)**。

d) 在**虚拟路由属性 (Virtual Routing Properties)** 中，选择 **BVI-G**，然后点击**添加 (Add)**。



e) 单击**保存**。

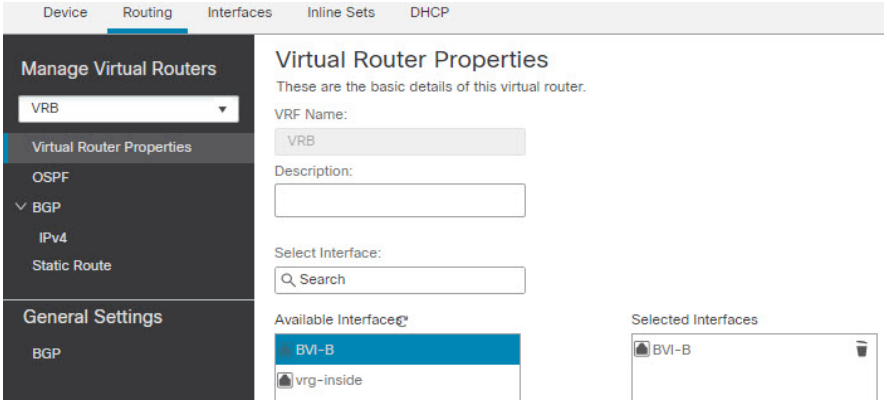
步骤 4 创建虚拟路由器，例如 VRB，然后选择 BVI-B 作为其网络：

a) 选择**设备** > **设备管理**。

b) 编辑设备，然后选择**路由 (Routing)** > **管理虚拟路由器 (Manage Virtual Routers)**。

c) 点击 **Add Virtual Router**。输入虚拟路由器的名称，然后点击**确定 (Ok)**。

d) 在**虚拟路由属性 (Virtual Routing Properties)** 中，选择 **BVI-B**，然后点击**添加 (Add)**。



e) 单击**保存**。

步骤 5 重新访问 BVI-B 配置：

a) 依次选择**设备** > **设备管理** > **接口**。

b) 点击 BVI-B 接口的**编辑 (Edit)**。将 IP 地址指定为 10.10.10.5/24。现在，由于接口分别分配给两个不同的虚拟路由器，因此系统允许您使用 BVI-G 的同一 IP 地址进行配置。

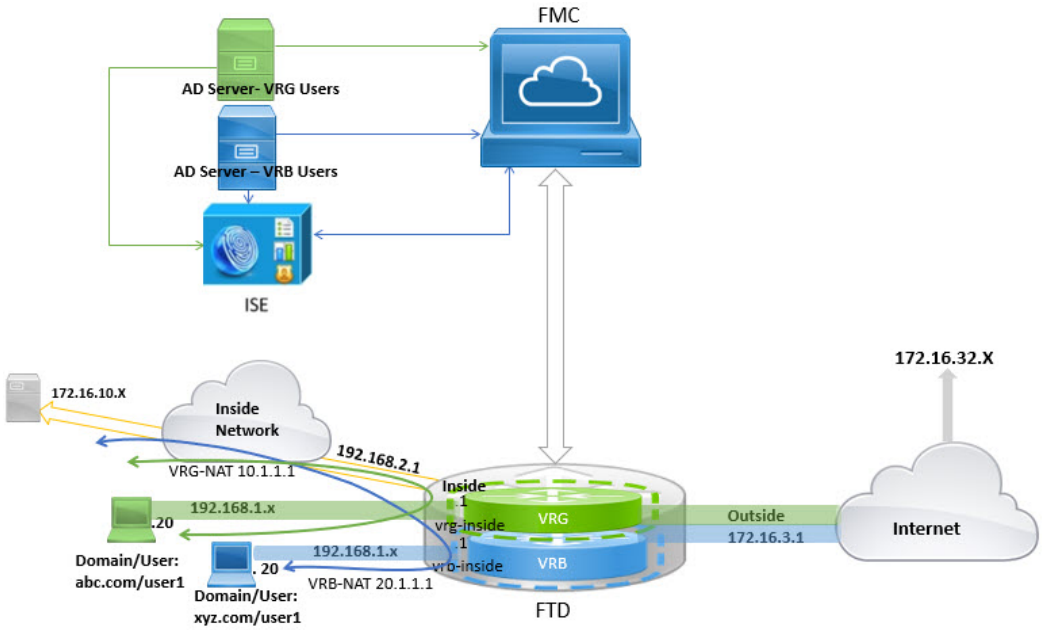
c) 点击**确定**。

d) 点击**保存 (Save)**。

如果要启用 BVI 间通信，请使用外部路由器作为默认网关。在重叠的 BVI 场景中，如本例所示，使用两次 NAT 外部路由器作为网关来建立 BVI 间流量。为网桥组的成员配置 NAT 时，需要指定成员接口。您不能为网桥组接口 (BVI) 本身配置 NAT。在桥接组成员接口之间执行 NAT 时，必须指定实际地址和映射地址。不能指定“任意”作为接口。

如何使用重叠网络来配置用户身份验证

在虚拟路由中，您可以配置多个具有重叠 IP 和重叠用户的虚拟路由器。在本例中，VRG 和 VRB 是具有重叠 IP - 192.168.1.1/24 的虚拟路由器。两个不同域上的用户也同样位于重叠的网络 IP 192.168.1.20 上。为了让 VRG 和 VRB 用户访问共享服务器 172.16.10.X，可将路由泄漏到全局虚拟路由器。使用源 NAT 来处理重叠 IP。要控制来自 VRG 和 VRB 用户的访问，您必须在 FMC 中设置用户身份验证。FMC 会使用领域、Active Directory、身份源以及身份规则和策略来验证用户身份。由于 FTD 在用户身份验证方面并不发挥直接作用，因此仅通过访问控制策略管理用户访问。要控制来自重叠用户的流量，请使用身份策略和规则来创建访问控制策略。



开始之前

此示例假定您已：

- VRG 和 VRB 用户的两台 AD 服务器。
- 添加了包含两台 AD 服务器的 ISE。

过程

步骤 1 为 VRG 配置设备的内部接口：

a) 依次选择**设备** > **设备管理** > **接口**。

b) 编辑您要分配给 VRG 的接口：

- **名称 (Name)** - 在此示例中为 VRG-inside。
- 选中**启用**复选框。
- 在 **IPV4** 中，对于 **IP 类型**，请选择**使用静态 IP**。
- **IP 地址 (IP Address)** - 输入 192.168.1.1/24。

c) 点击**确定**。

d) 点击**保存 (Save)**。

步骤 2 为 VRB 配置设备的内部接口：

a) 依次选择**设备** > **设备管理** > **接口**。

b) 编辑您要分配给 VRB 的接口：

- **名称 (Name)** - 在此示例中为 VRB-inside。
- 选中**启用**复选框。
- 在 **IPV4** 中，对于 **IP 类型**，请选择**使用静态 IP**。
- **IP 地址** - 将其留空。该系统不允许您使用相同的 IP 地址配置接口，因为您尚未创建用户定义的虚拟路由器。

c) 点击**确定**。

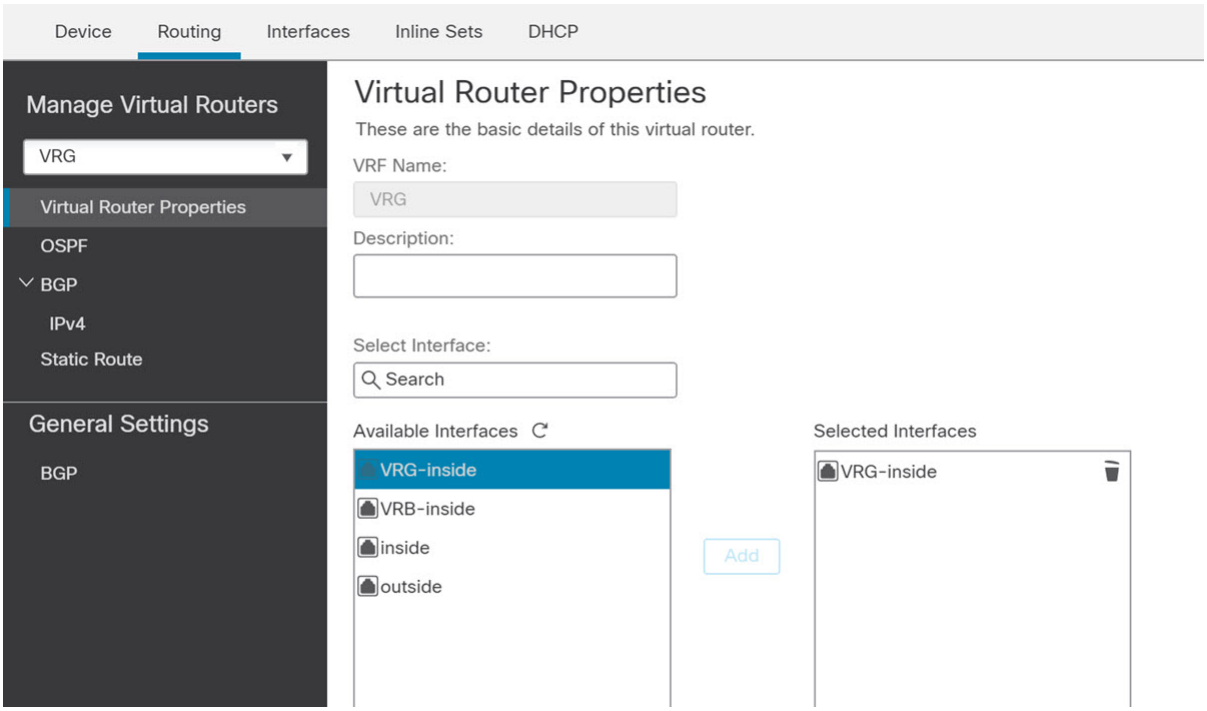
d) 点击**保存 (Save)**。

步骤 3 将 VRG 和静态默认路由泄漏配置到全局路由器的内部接口，以便 VRG 用户访问通用服务器 172.16.10.1：

a) 依次选择**设备** > **设备管理**，然后编辑 FTD 设备。

b) 依次选择**路由** > **管理虚拟路由器**。点击**添加虚拟路由器 (Add Virtual Router)**并创建 VRG。

c) 对于 VRG，在**虚拟路由器属性 (Virtual Router Properties)** 中分配 VRG-inside 并保存。



d) 点击**静态路由 (Static Route)**。

e) 点击**添加路由**。在**添加静态路由配置**中，指定以下内容：

- **接口 (Interface)** - 选择全局路由器的内部接口。
- **网络 (Network)** - 选择 any-ipv4 对象。
- **网关** - 将其留空。将路由泄漏到另一个虚拟路由器时，请勿选择网关。

f) 点击**确定**。

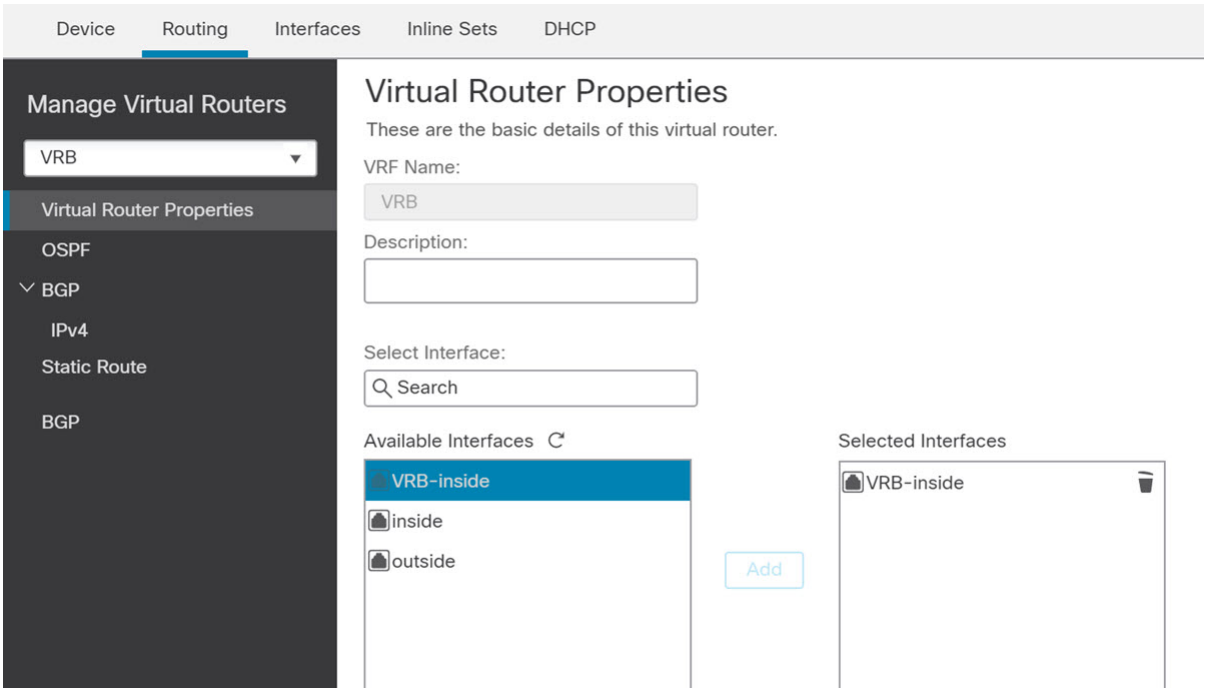
g) 点击**保存 (Save)**。

步骤 4 将 VRB 和静态默认路由泄漏配置到全局路由器的内部接口，以便 VRB 用户访问共享服务器 172.16.10.x：

a) 依次选择**设备** > **设备管理**，然后编辑 FTD 设备。

b) 依次选择**路由** > **管理虚拟路由器**。点击**添加虚拟路由器 (Add Virtual Router)**并创建 VRB。

c) 对于 VRB，在**虚拟路由器属性 (Virtual Router Properties)** 中分配 VRB-inside 并保存。



d) 点击**静态路由 (Static Route)**。

e) 点击**添加路由**。在**添加静态路由配置**中，指定以下内容：

- **接口 (Interface)** - 选择全局路由器的内部接口。
- **网络 (Network)** - 选择 any-ipv4 对象。
- **网关** - 将其留空。将路由泄漏到另一个虚拟路由器时，请勿选择网关。

f) 点击**确定**。

g) 点击**保存 (Save)**。

步骤 5 重新访问 VRB-inside 接口配置：

a) 依次选择**设备** > **设备管理** > **接口**。

b) 点击 VRB-inside 接口的**编辑 (Edit)**。将 IP 地址指定为 192.168.1.1/24。现在，由于接口分别分配给两个不同的虚拟路由器，因此系统允许您使用 VRG-inside 的相同 IP 地址进行配置。

c) 点击**确定**。

d) 点击**保存 (Save)**。

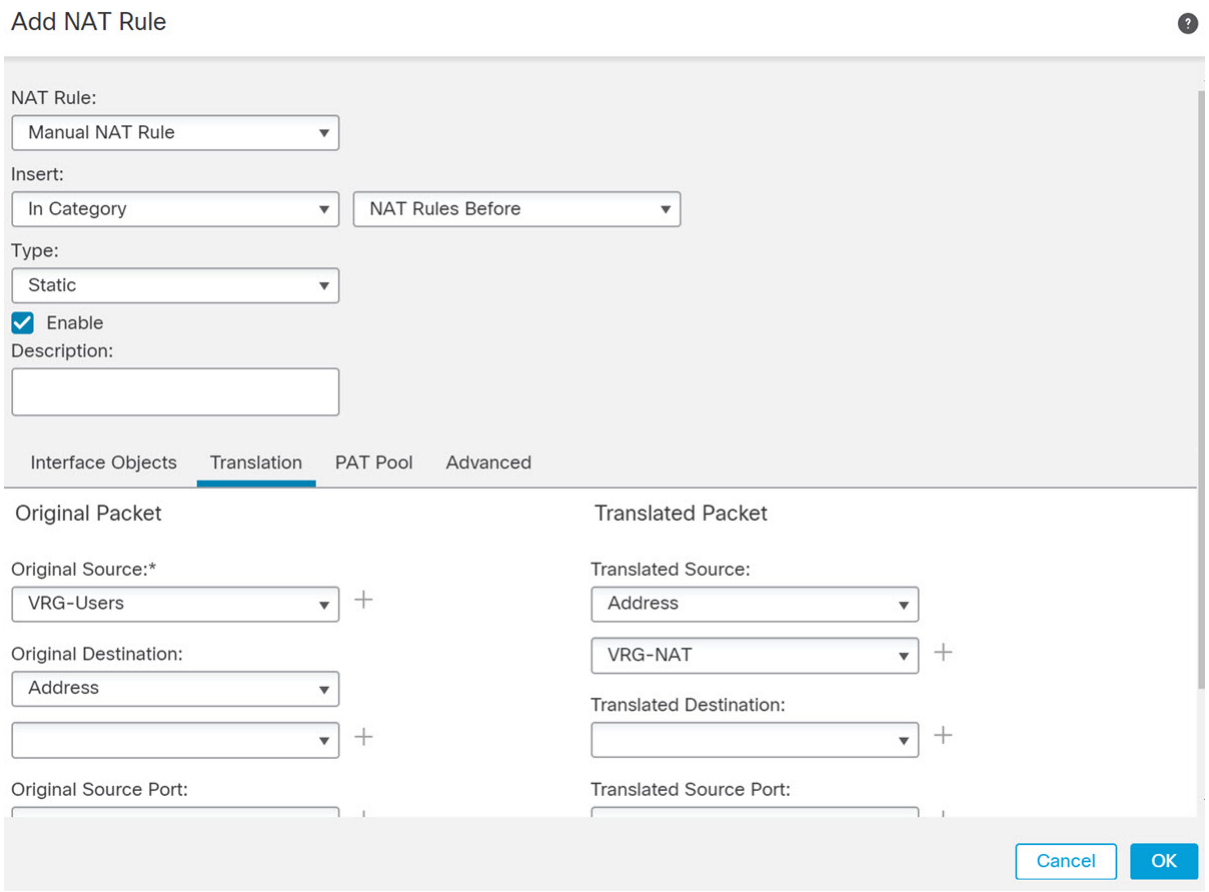
步骤 6 为源对象 VRG 和 VRB 添加 NAT 规则。点击**设备 (Devices)** > **NAT**。

步骤 7 点击**新策略 (New Policy)** > **威胁防御 NAT (Threat Defense NAT)**。

步骤 8 输入 NAT 策略名称，然后选择 FTD 设备。单击**保存**。

步骤 9 在 NAT 页面中，点击**添加规则 (Add Rule)** 并为 VRG 定义以下源 NAT：

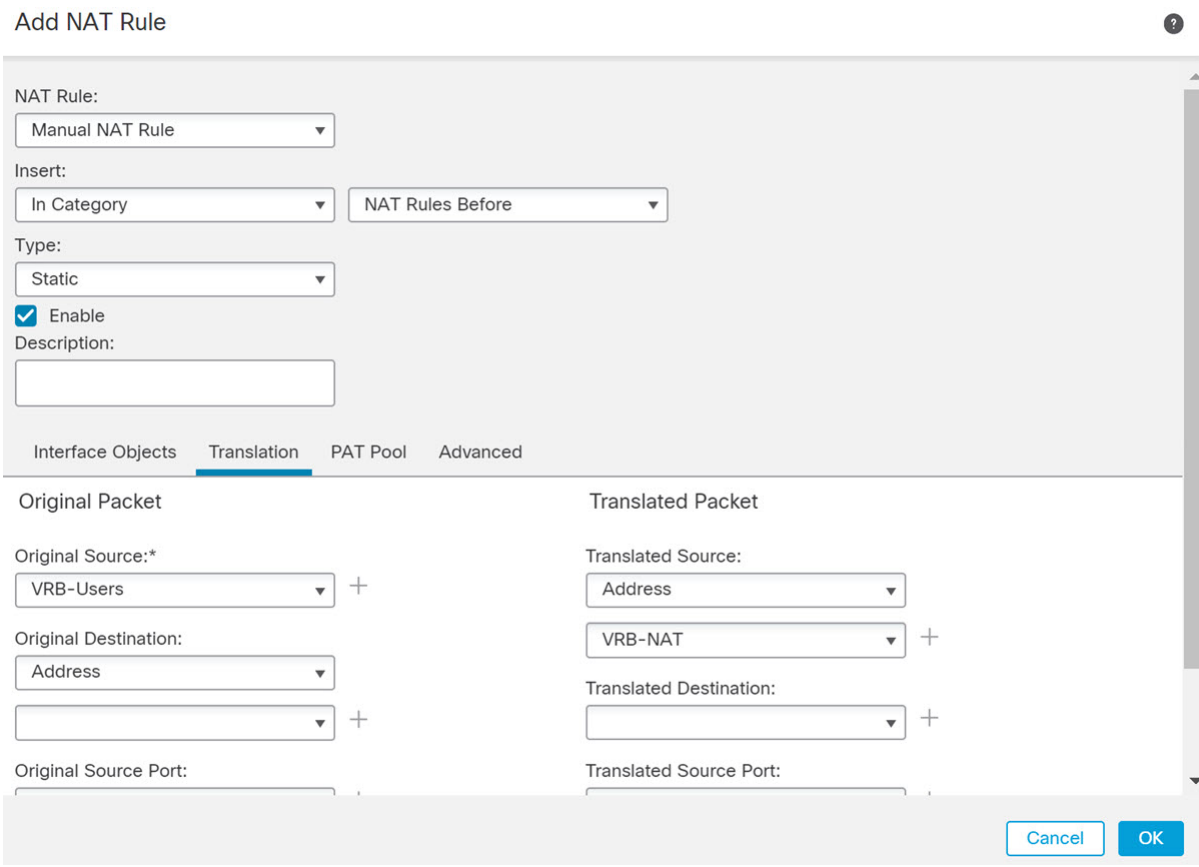
- **NAT 规则 (NAT Rule)** - 选择“手动 NAT 规则”(Manual NAT Rule)。
- **类型 (Type)** - 选择“静态”(Static)。
- **插入 (Insert)** - 如果存在任何 NAT 规则，则选择“上方”(Above)。
- 点击 **Enabled**。
- 在**接口对象 (Interface Objects)**中，选择 VRG-Inside 对象，然后点击**添加到源 (Add to Source)**（如果对象不可用，请在**对象 (Object)** > **对象管理 (Object Management)** > **接口 (Interface)** 中创建一个对象），然后选择 Global-Inside 对象并点击**添加到目标 (Add to Destination)**。
- 在**转换 (Translation)** 中选择以下选项：
  - **原始源 (Original Source)**，选择 VRG-Users。
  - **转换后的源 (Translated Source)**，点击**添加 (Add)**并使用 10.1.1.1 来定义对象 VRG-NAT。选择 VRG-NAT，如下图所示：



步骤 10 点击**确定**。

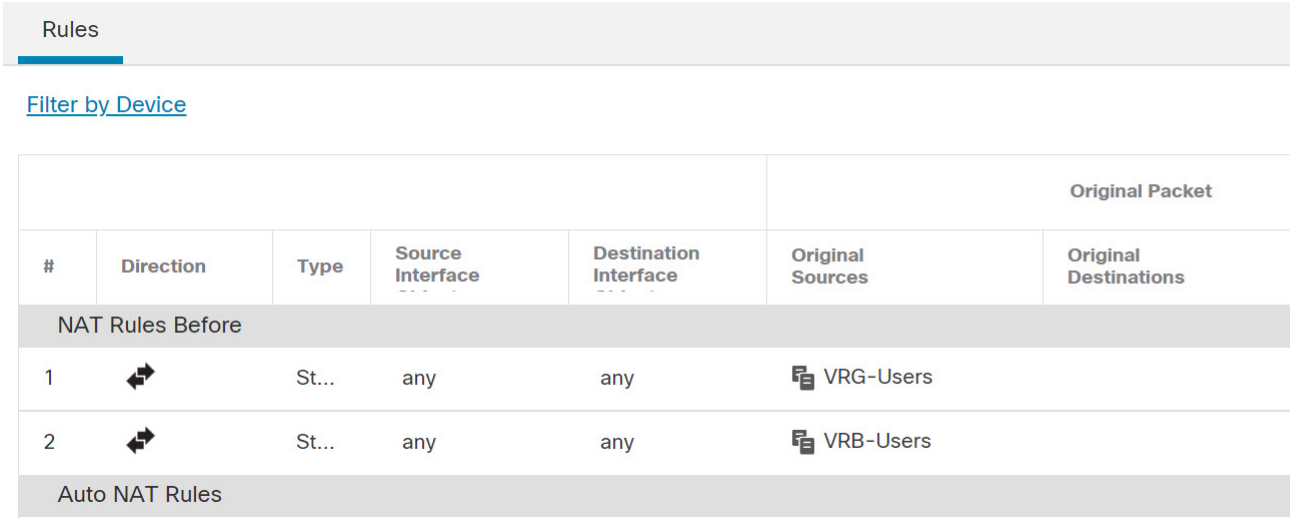
步骤 11 在 NAT 页面中，点击**添加规则 (Add Rule)** 并为 VRB 定义以下源 NAT：

- **NAT 规则 (NAT Rule)** - 选择“手动 NAT 规则”(Manual NAT Rule)。
- **类型 (Type)** - 选择“静态”(Static)。
- **插入 (Insert)** - 如果存在任何 NAT 规则，则选择“上方”(Above)。
- 点击 **Enabled**。
- 在**接口对象 (Interface Objects)**中，选择 VRB-Inside 对象，然后点击**添加到源 (Add to Source)**（如果对象不可用，请在**对象 (Object)** > **对象管理 (Object Management)** > **接口 (Interface)** 中创建一个对象），然后选择 Global-Inside 对象并点击**添加到目标 (Add to Destination)**。
- 在**转换 (Translation)** 中选择以下选项：
  - **原始源 (Original Source)**，选择 VRB-Users。
  - **转换后的源 (Translated Source)**，点击**添加 (Add)**并使用 20.1.1.1 来定义对象 VRB-NAT。选择 VRB-NAT，如下图所示：



步骤 12 单击**保存**。

NAT 规则如下所示：



步骤 13 在 FMC 中为每个 VRG 和 VRB 用户添加两个唯一的 AD 服务器 - 选择**系统 (System)** > **集成 (Integration)** > **领域 (Realms)**。

步骤 14 点击**新建领域 (New Realm)** 并填写字段。有关这些字段的详细信息，请参阅领域字段。

步骤 15 要控制来自 VRG 和 VRB 用户的访问，请定义 2 个 Active Directory，请参阅领域目录和同步字段请参阅创建 LDAP 领域或 Active Directory 领域和领域目录

步骤 16 在 FMC 中添加 ISE - 选择**系统 (System)** > **集成 (Integration)** > **身份源 (Identity Sources)**。

步骤 17 点击**身份服务引擎 (Identity Services Engine)** 并填写字段。有关这些字段的详细信息，请参阅如何为无领域的用户控制配置 ISE/ISE-PIC。

步骤 18 创建身份策略和规则，然后定义访问控制策略，以便控制来自 VRG 和 VRB 的重叠用户的访问。

如何使用 BGP 来互连虚拟路由器

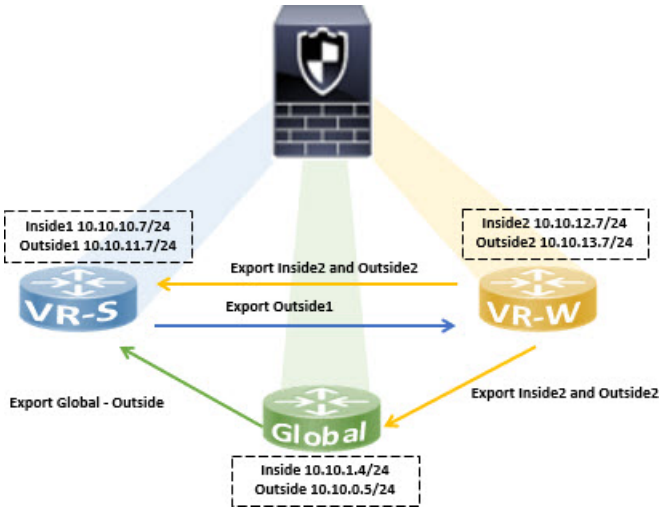
现在，您可以在设备上配置BGP设置，以便在虚拟路由器（全局和用户定义的虚拟路由器）之间泄漏路由。源虚拟路由器的路由目标会被导出到BGP表，而该表又会被导入到目的虚拟路由器。路由地图用于与用户定义的虚拟路由器共享全局虚拟路由，反之亦然。请注意，所有路由到BGP表的导入或导出都在用户定义的虚拟路由器上配置，包括全局虚拟路由。

假设工厂的防火墙设备配置了以下虚拟路由器和接口：

- 全局虚拟路由器配置了内部 (10.10.1.4/24) 和外部 (10.10.0.5/24)
- VR-S（销售）虚拟路由器配置了 Inside1 (10.10.10.7/24) 和 outside1 (10.10.11.7/24)
- VR-W（仓库）虚拟路由器配置了 Inside2 (10.10.12.7/24) 和 outside2 (10.10.13.7/24)

假设您想把仓库 (VR-W) 的路由泄漏给销售 (VR-S) 和全局，并将 VR-S 的外部接口路由到 VR-W。同样，您想把全局路由器的外部接口路由泄漏给销售 (VR-S)。此示例演示了实现路由器互连的 BGP 配置程序：

图 *3:* 使用 *BGP* 设置来互连虚拟路由器



开始之前

- 创建虚拟路由器 - VR-S 和 VR-W。
- 启用 BGP，并为每个虚拟路由器选择配置 BGP 以重新分发连接的路由 (Configure BGP for redistribution of connected routes)。

过程

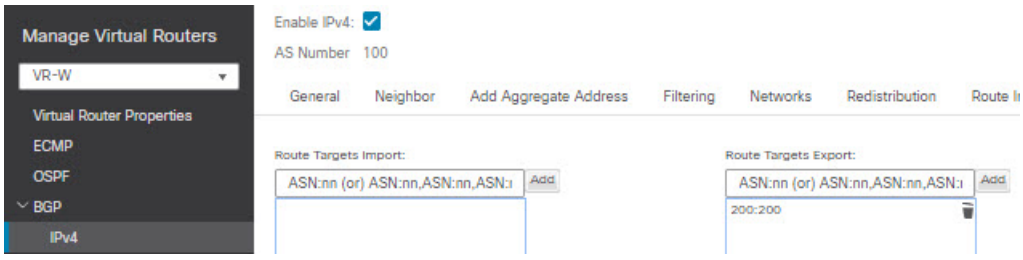
步骤 1 配置 VR-W 以将其带有路由目标的路由导出至 VR-S：

a) 选择**设备 (Devices)** > **设备管理 (Device Management)**，编辑设备，然后点击**路由 (Routing)** 选项卡。

b) 在虚拟路由器下拉列表中选择 VR-W。

c) 点击 **BGP** > **IPv4** > **路由导入/导出 (Route Import/Export)**。

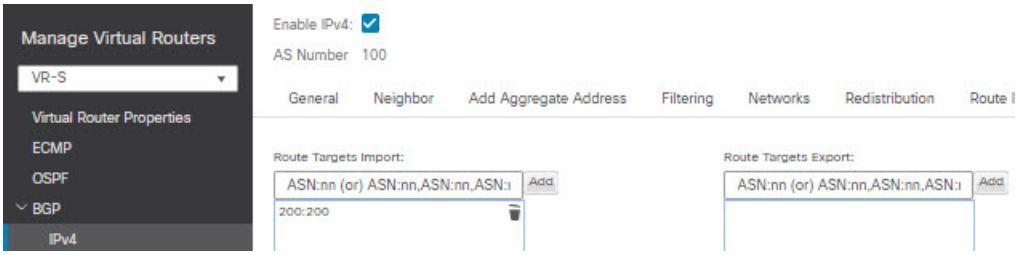
d) 要将 VR-W 路由泄漏到 VR-S，请使用路由目标标记路由，以便将 VR-W 路由导出到其 BGP 表中，并在它上面标记路由目标。在**路由目标导出 (Route Targets Export)** 字段中，输入一个值，例如 *200:200*。点击**添加 (Add)**：



e) 从虚拟路由器下拉列表中选择 VR-S。

f) 点击 **BGP** > **IPv4** > **路由导入/导出 (Route Import/Export)**。

g) 要从 VR-W 接收泄漏的路由，请配置“导入路由目标”(Import Route Target)，以便从（对等体或重新分发的）BGP 表导入标记有路由目标的 VR-W 路由。在**路由目标导入 (Route Targets Import)** 字段中，输入您为 VR-W 配置的相同路由目标值 *200:200*。单击**添加**。



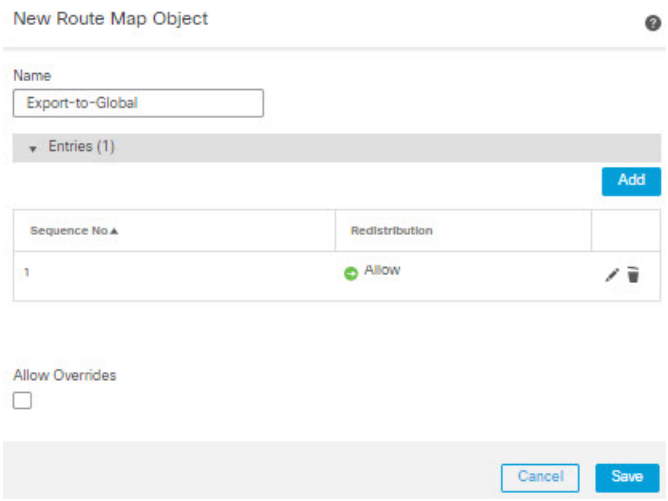
注释 如果要对从 VR-W 泄漏的路由进行条件化，可以在路由映射对象中指定匹配条件，并在**用户虚拟路由器导出路由地图 (User Virtual Router Export Route Map)** 中选择该匹配条件。同样，如果想对要从 BGP 表导入 VR-S 的路由进行条件化，您可以使用**用户虚拟路由器导入路由映射 (User Virtual Router Import Route Map)**。此程序在步骤 3 中进行了介绍。

步骤 2 配置 VR-W 以便将其路由导出到全局虚拟路由器：

a) 您需要创建一个允许将 VR-W 路由导出到全局路由表的路由地图。选择**对象 (Objects)** > **对象管理 (Object Management)** > **路由地图 (Route Map)**。

b) 点击**添加路由地图 (Add Route Map)**，为其命名（如 *Export-to-Global*），然后点击**添加 (Add)**。

c) 指定**序列号 (Sequence Number)**（比如 1），然后从**重新分配 (Redistribution)** 下拉列表选择“运行”(Allow)：

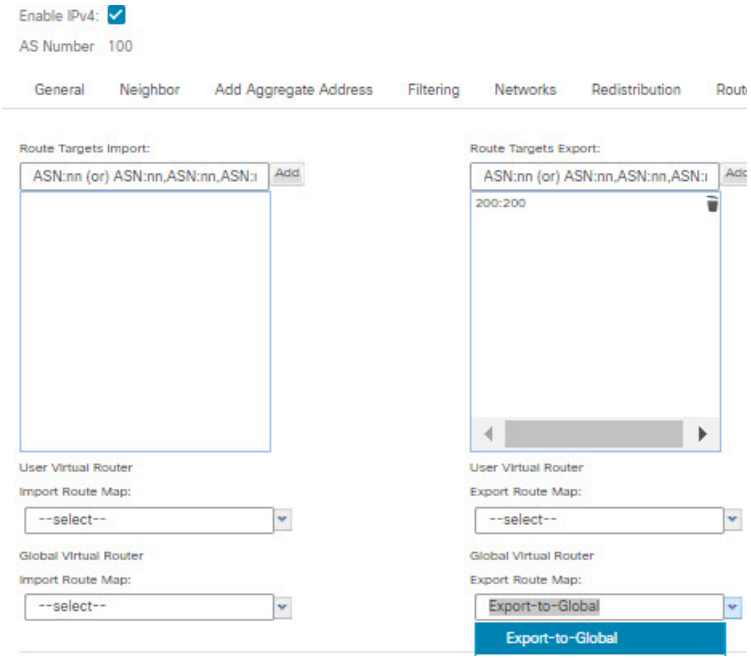


d) 单击**保存**。

在本例中，所有 VR-W 路由都会被泄漏到全局路由表。因此，没有为路由映射配置匹配条件。

e) 导航到设备的**路由 (Routing)** 选项卡，然后选择 VR-W。点击 **BGP** > **IPv4** > **路由导入/导出 (Route Import/Export)**。

f) 从**全局虚拟路由器导出路由地图 (Global Virtual Router Export Route Map)** 下拉列表中，选择 Export-to-Global：



步骤 3 要仅将 VR-S 的外部 1 路由泄漏到 VR-W，请执行以下操作：

a) 从虚拟路由器下拉列表中选择 VR-S。

b) 点击 **BGP** > **IPv4** > **路由导入/导出 (Route Import/Export)**。

c) 要将 VR-S 路由泄漏到 VR-W，请使用路由目标标记路由，以便将 VR-S 路由导出到其 BGP 表中，并在它上面标记路由目标。在**路由目标导出 (Route Targets Export)** 字段中，输入一个值，例如 *100:100*。单击**添加**。

d) 从虚拟路由器下拉列表中，选择 VR-W，然后选择 **BGP** > **IPv4** > **路由导入/导出 (Route Import/Export)**。

e) 要从 VR-S 接收泄漏的路由，请配置“导入路由目标”(Import Route Target)，以便从（对等体或重新分发的）BGP 表导入标记有路由目标的 VR-S 路由。在**路由目标导入 (Route Targets Import)** 字段中，输入 VR-S 路由目标值 *100:100*。单击**添加**。

f) 现在，您需要将 VR-S 的外部 1 路由限制为泄漏到 VR-W。选择**对象 (Objects)** > **对象管理 (Object Management)** > **前缀列表 (Prefix List)** > **IPv4 前缀列表 (IPv4 Prefix List)**。

g) 点击**添加 IPv4 前缀列表 (Add IPv4 Prefix List)**，提供名称（如 *VRS-Outside1-Only*），然后点击**添加 (Add)**。

h) 指定**序列号 (Sequence Number)**（比如 1），然后从**重新分配 (Redistribution)** 下拉列表选择“运行”(Allow)。

i) 输入 VR-S outside1 接口的 IP 地址（前两个八位组）。

j) 单击**保存**。

k) 使用带前缀列表的 match 子句来创建路由地图。点击**路由地图 (Route Map)**。点击**添加路由映射 (Add Route Map)**，指定名称（如 *Import-from-VRS*），然后点击**添加 (Add)**。

l) 指定**序列号 (Sequence Number)**（比如 1），然后从**重新分配 (Redistribution)** 下拉列表选择“运行”(Allow)。

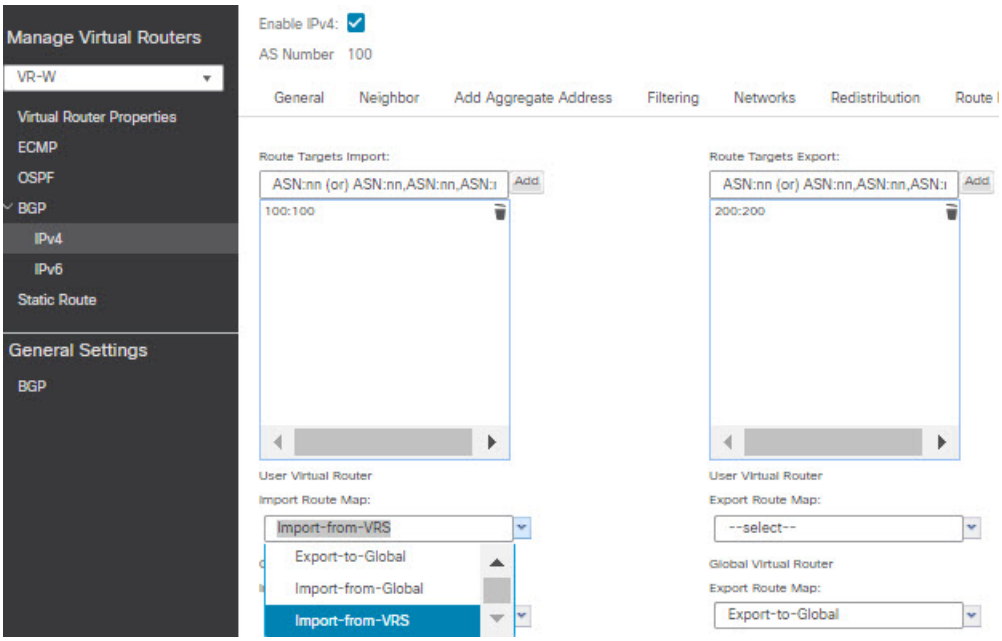
m) 在匹配子句 **(Match Clause)** 选项卡中，点击 **IPv4**。在地址 **(Address)** 选项卡下，点击前缀列表 **(Prefix List)**。

n) 在可用 **IPv4** 前缀列表 **(Available IPv4 Prefix List)** 下，选择 VRS-Outside1-Only，然后点击添加 **(Add)**。

o) 单击保存。

p) 导航到设备的路由 **(Routing)** 选项卡，然后选择 VR-W。点击 **BGP** > **IPv4** > 路由导入/导出 **(Route Import/Export)**。

q) 从全局虚拟路由器导入路由地图 **(Global Virtual Router Import Route Map)** 下拉列表中，选择 Import-from-VRS：



步骤 4 配置 VR-S 以便导入全局虚拟路由器的外部路由：

注释 要从全局虚拟路由器泄漏路由，您必须分别配置源或目标用户定义的虚拟路由器。因此，在本例中，VR-S 是从全局虚拟路由器的外部接口导入路由的目的路由器。

a) 选择对象 **(Objects)** > 对象管理 **(Object Management)** > 前缀列表 **(Prefix List)** > **IPv4** 前缀列表 **(IPv4 Prefix List)**。

b) 点击添加 **IPv4** 前缀列表 **(Add IPv4 Prefix List)**，提供名称（如 *Global-Outside-Only*），然后点击添加 **(Add)**。

c) 指定序列号 **(Sequence Number)**（比如 1），然后从重新分配 **(Redistribution)** 下拉列表选择“运行”(Allow)。

d) 输入 Global Outside 接口的 IP 地址（前两个八位组）：

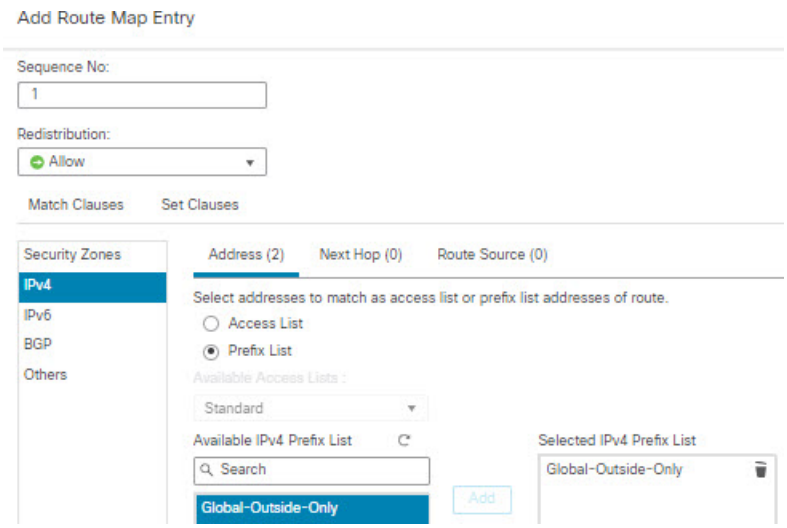
e) 单击**保存**。

f) 点击**路由地图 (Route Map)**。点击**添加路由映射 (Add Route Map)**，指定名称（如 *Import-from-Global*），然后点击**添加 (Add)**。

g) 指定**序列号 (Sequence Number)**（比如 1），然后从**重新分配 (Redistribution)** 下拉列表选择“运行”(Allow)。

h) 在**匹配子句 (Match Clause)** 选项卡中，点击 **IPv4**。在**地址 (Address)** 选项卡下，点击**前缀列表 (Prefix List)**。

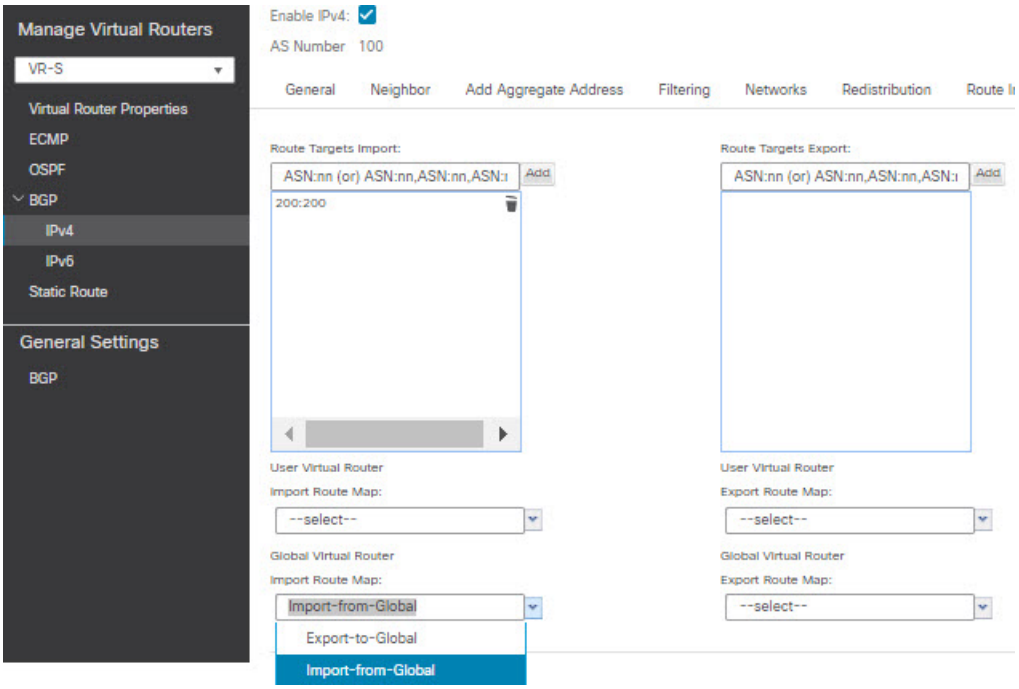
i) 在**可用 IPv4 前缀列表 (Available IPv4 Prefix List)** 下，选择 Global-Outside-Only，然后点击**添加 (Add)**。



j) 单击**保存**。

k) 导航到设备的**路由 (Routing)** 选项卡，然后选择 VR-S。点击 **BGP** > **IPv4** > **路由导入/导出 (Route Import/Export)**。

l) 从**全局虚拟路由器导入路由地图 (Global Virtual Router Import Route Map)** 下拉列表中，选择 Import-from-Global：



步骤 **5** 保存 **(Save)** 和部署 **(Deploy)**。

虚拟路由器的历史记录

特性	最低版本	最低 威胁防御	详细信息
具有动态 VTI 的虚拟路由	管理中心：7.4 威胁防御：7.4	任意	现在，您可以为基于路由的站点间 VPN 配置具有动态 VTI 的虚拟路由器。 新增/修改的屏幕：**设备 (Devices) > 设备管理 (Device Management)** > 编辑设备 (Edit Device) > **路由 (Routing) > 虚拟路由器属性 (Virtual Router Properties)** > **可用接口 (Available Interfaces)** 下的“动态 VTI 接口”(Dynamic VTI interfaces)
对 ISA 3000 的虚拟路由器支持	7.0	任意	您可以在 ISA 3000 设备上最多配置 10 个虚拟路由器。 新增/修改的屏幕：无
已启用 Snort 3 的设备的虚拟路由器	7.0	任意	已启用 Snort3 的设备现在支持虚拟路由器功能。因此，在继续切换到 Snort3 引擎之前，不必从虚拟路由器中删除 Snort 2 设备。 新增/修改的屏幕：无

特性	最低版本	最低 威胁防御	详细信息
在用户定义的虚拟路由器上的 SNMP 支持	7.0	任意	Cisco Secure Firewall Threat Defense 现在支持在用户定义的虚拟路由器上配置 SNMP。 新增/修改的屏幕：无
批量删除虚拟路由器	6.7	任意	您可以从 Cisco Secure Firewall Threat Defense 一次删除多个虚拟路由器。 新增/修改的屏幕：**设备 (Devices)** > **设备管理 (Device Management)** > **路由 (Routing)** > **管理虚拟路由器 (Manage Virtual Routers)** 页面。
Cisco Secure Firewall Threat Defense 的虚拟路由器	6.6	任意	引入了 Cisco Secure Firewall Threat Defense 的虚拟路由器。 新增/修改的屏幕：可以在**设备 (Devices)** > **设备管理 (Device Management)** > **路由 (Routing)** 页面中创建虚拟路由器，并将威胁防御接口分配给虚拟路由器。 支持的平台： Cisco Secure Firewall Threat Defense

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。