虚拟路由器

可以创建虚拟路由器来隔离接口子集之间的流量。

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。

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。

对于不使用安全区的策略（例如 NAT），您可以通过选择分配给单个虚拟路由器的接口作为源接口和目标接口来编写虚拟路由器的特定规则。如果从两个独立的虚拟路由器中选择源接口和目标接口，则必须确保虚拟路由器之间具有适当的路由，以确保规则正常工作。

在虚拟路由器之间路由

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。

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	此型号不支持虚拟路由器。
Firepower 1120	5
Firepower 1140	10
Firepower 1150	10
Cisco Secure Firewall 1210CE	5
Cisco Secure Firewall 1210CP	5
Cisco Secure Firewall 1220CX	10
Cisco Secure Firewall 3105	10
Cisco Secure Firewall 3110	15
Cisco Secure Firewall 3120	25
Cisco Secure Firewall 3130	50
Cisco Secure Firewall 3140	100
Firepower 4112	60
Firepower 4115	80
Firepower 4125	100
Firepower 4145	100

设备型号	最大虚拟路由器数量
Firepower 9300 设备，所有型号	100
Threat Defense Virtual，所有平台	30
ISA 3000	10

虚拟路由器准则

设备型号准则

您可以在所有支持的设备型号上配置虚拟路由器，但以下情况除外：

- Firepower 1010

其他准则

- 您只能在全局虚拟路由器上配置以下功能：
  - OSPFv3
  - RIP
  - EIGRP
  - IS-IS
  - BGPv6
  - 组播路由
  - 基于策略的路由
  - VPN
- 您可以为每个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
- 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。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。一般情况下，无论何时，系统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。您只能在全局虚拟路由器的接口上配置 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。
  - 系统日志服务器。
  - SNMP。

- 在 NAT 中，如果指定将分配给不同虚拟路由器的源接口和目标接口，NAT 规则将通过一个虚拟路由器转移另一个虚拟路由器的流量。确保不会无意中混合NAT规则中的接口。通常将使用源接口和目标接口，并忽略路由表，包括手动 NAT 中的目标转换。但是，如果 NAT 规则确实需要执行路由查找，则仅在VRF表中查找入站接口。如有必要，请在源虚拟路由器中为目标接口定义静态路由。请注意，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。使用虚拟路由器时，请仔细测试NAT规则，以确保实现预期行为。如果您忘记定义所需的路由泄漏，在某些情况下，该规则将不会匹配您预期匹配的所有流量，并且不会应用转换。
- 如果您配置虚拟路由器间路由，例如，将路由从一个虚拟路由器泄漏到另一个虚拟路由器，则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。
- 使用从虚拟路由器 1 到虚拟路由器 2（例如）的虚拟路由器间路由（泄漏路由）时，不需要在虚拟路由器 2 中配置镜像（反向）路由以允许返回流量。但是，如果要允许在两个方向上发起连接，请确保在两个方向上（从虚拟路由器 1 到 2 以及从虚拟路由器 2 到 1）泄漏路由。
- 如果将接口从一个虚拟路由器移至另一个虚拟路由器，则会保留已为该接口配置的所有功能。检查配置，以确保静态路由、IP 地址和其他策略在新虚拟路由器的环境中有意义。
- 如果在多个虚拟路由器中使用重叠地址空间，请注意，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身份领域。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。
- 如果在多个虚拟路由器中使用重叠地址空间，控制面板数据可能具有误导性。与相同IP地址的连接将会汇聚，因此，当两个或多个终端共享给定地址时，系统显示与该地址之间的往来流量更多。如果使用单独的身份领域仔细构建身份策略，则基于用户的统计信息应更准确。
- 不能在单独的虚拟路由器中使用重叠的 DHCP 地址池。
- 只能在全局虚拟路由器中的接口上使用 DHCP 服务器自动配置。为用户定义的虚拟路由器分配的接口不支持自动配置功能。
- 如果在虚拟路由器之间移动接口（包括从全局虚拟路由器移至新路由器），将删除为该接口定义的任何现有连接。
- 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。

管理虚拟路由器

您可以创建多个虚拟路由与转发（VRF）实例（称为虚拟路由器），以便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。

默认情况下，虚拟路由已禁用。整个设备使用一组全局路由表，用于数据（通过）和管理（传入/传出）流量。

启用虚拟路由时，初始路由页面显示系统定义的虚拟路由器的列表。如果不启用虚拟路由器，则初始路由页面显示系统定义的静态路由的列表。

始终有一个全局虚拟路由器。全局路由器保留尚未分配给单个虚拟路由器的所有接口。

过程

步骤 1 点击**设备**，然后点击**路由**摘要中的链接。

步骤 2 如果尚未启用虚拟路由器，请点击**添加多个虚拟路由器**链接，然后点击**创建第一个自定义虚拟路由器**。

创建第一个虚拟路由器在本质上与创建任何附加虚拟路由器的方式基本相同。有关详细信息，请参阅创建虚拟路由器或编辑接口分配，第 7 页。

步骤 3 执行以下任一操作：

- 要配置适用于所有虚拟路由器的全局 BGP 设置，请点击 **BGP 全局设置**按钮。您可以使用 Smart CLI 配置这些设置，如配置 Smart CLI 对象中所述。只有在一个或多个虚拟路由器中配置 BGP 时，才需要配置全局 BGP 设置。
- 要创建新的虚拟路由器，请点击表上方的 + 按钮。
- 要编辑虚拟路由器的路由属性（例如，创建静态路由或定义路由进程），请在虚拟路由器的“操作”单元格中点击查看图标 ( )。
- 要编辑虚拟路由器的名称、说明或接口分配，请在虚拟路由器的“操作”单元格中点击查看图标 ( )，然后选择**虚拟路由器属性**选项卡。
- 要在查看虚拟路由器时进行切换，请点击虚拟路由器名称（位于路由表上方）旁边的向下箭头，然后选择所需的虚拟路由器。点击**返回虚拟路由器 (Go Back to Virtual Routers)** 箭头 ( ) 返回到列表页面。
- 要删除虚拟路由器，请在虚拟路由器的“操作”单元格中点击删除图标 ( )，或在查看虚拟路由器的内容时，点击虚拟路由器名称旁边的删除图标。删除最后一个虚拟路由器（全局路由器除外，因为您无法删除）时，将禁用 VRF。

- 要监控虚拟路由器中的路由，请为该虚拟路由器点击表中的**show**命令之一的链接。点击该命令将打开 CLI 控制台，您可以在其中检查 CLI 命令的输出。显示有关路由、OSPF 和 OSPF 邻居的信息。请注意，命令输出基于已部署的配置；无法查看任何与未部署的编辑相关的内容。

  查看虚拟路由器时，您还可以通过从**命令**下拉列表中选择命令来执行这些命令。

创建虚拟路由器或编辑接口分配

在虚拟路由器上配置静态路由或路由进程之前，您必须先创建路由器并向其分配接口。

开始之前

转至**接口 (Interfaces)**页面，确保要添加到虚拟路由器的每个接口都具有名称。只能将具有名称的接口添加至虚拟路由器。

过程

步骤 1 点击 **设备 (Device)** > **路由 (Routing)**。

步骤 2 执行以下操作之一：

- 如果尚未创建虚拟路由器，请点击**添加多个虚拟路由器 (Add Multiple Virtual Routers)** 链接，然后点击**创建第一个自定义虚拟路由器 (Create First Custom Virtual Router)**
- 点击虚拟路由器列表上方的 + 按钮以新建虚拟路由器。
- 点击虚拟路由器的编辑图标 () 以编辑属性和接口列表。
- 查看虚拟路由器时，点击**虚拟路由器属性 (Virtual Router Properties)** 选项卡，以编辑您正在查看的虚拟路由器的属性。
- 查看虚拟路由器时，点击虚拟路由器名称旁边的向下箭头，然后点击**新建虚拟路由器 (Create New Virtual Router)**。

步骤 3 配置虚拟路由器的属性：

- **名称** - 虚拟路由器名称。
- **说明** - 虚拟路由器的可选说明。
- **接口** - 点击 + 选择应属于虚拟路由器的各个接口。要删除接口，请将鼠标悬停在接口上，然后点击接口卡右侧的 **X** 。您可以将物理接口、子接口和 Etherchannel 分配给虚拟路由器，但不能分配给 VLAN。

  除非您有意将其他接口的路由泄漏到虚拟路由表中，否则路由表将限制为这些接口。

步骤 4 点击**确定 (OK)**或**保存 (Save)**。

您将转到此虚拟路由器的视图，然后在其中配置静态路由或路由进程。

在虚拟路由器中配置静态路由和路由进程

每个虚拟路由器都具有自己的静态路由和路由进程，它们将独立于为任何其他虚拟路由器定义的路由和路由进程运行。

配置静态路由时，可以选择该虚拟路由器以外的目标接口。这会将路由泄漏到包含目标接口的虚拟路由器。确保只泄漏需要泄漏的路由，以确保发送的流量不会超过您想要发往其他虚拟路由器的流量。例如，如果您有一条连接互联网的路径，则有必要将每个虚拟路由器的路由泄漏到面向互联网的虚拟路由器，以便将流量发往互联网。

过程

步骤 1 选择**设备** > **路由**。

步骤 2 在虚拟路由器的“操作”(Action) 单元格中点击查看图标 () 以打开虚拟路由器。

步骤 3 执行以下任一操作：

- 要配置静态路由，请点击**静态路由 (Static Routing)** 选项卡，然后创建或编辑路由。有关详细信息，请参阅配置静态路由。
- 要配置等价多路径 (ECMP) 流量区域，请点击 **ECMP 流量区域 (ECMP Traffic Zones)** 选项卡，然后创建区域。有关详细信息，请参阅配置 ECMP 流量区域。
- 要配置 BGP 路由进程，请点击 **BGP** 选项卡，然后创建定义该进程所需的 Smart CLI 对象。有关详细信息，请参阅边界网关协议 (BGP)。

  还有适用于所有虚拟路由器的 BGP 全局设置。必须返回“虚拟路由器列表”页面，点击 **BGP 全局设置 (BGP Global Settings)** 按钮来配置这些属性。
- 要配置 OSPF 路由进程，请点击 **ospf** 选项卡，然后创建定义最多 2 个进程所需的 Smart CLI 对象及其关联的接口配置。有关详细信息，请参阅开放最短路径优先 (OSPF)。
- （仅限全局虚拟路由器。）要配置 EIGRP 路由进程，请点击 **EIGRP** 选项卡，然后创建定义单个进程所需的 Smart CLI 对象。有关详细信息，请参阅增强型内部网关路由协议 (EIGRP)。

删除虚拟路由器

如果不再需要虚拟路由器，可以将其删除。不能删除全局虚拟路由器。

删除虚拟路由器时，您将删除该虚拟路由器中配置的所有静态路由和路由进程。

分配给虚拟路由器的所有接口都将重新分配给全局路由器。

过程

步骤 1 选择**设备** > **路由**。

步骤 2 执行以下操作之一：

- 在虚拟路由器列表中，请在虚拟路由器的“操作”列中点击删除图标 ()。
- 查看要删除的虚拟路由器时，请点击路由器名称旁边的删除图标 ()。

系统提示您确认要删除虚拟路由器。

步骤 3 点击**确定**，确认删除。

虚拟路由器示例

以下主题提供了一些关于实施虚拟路由器的示例。

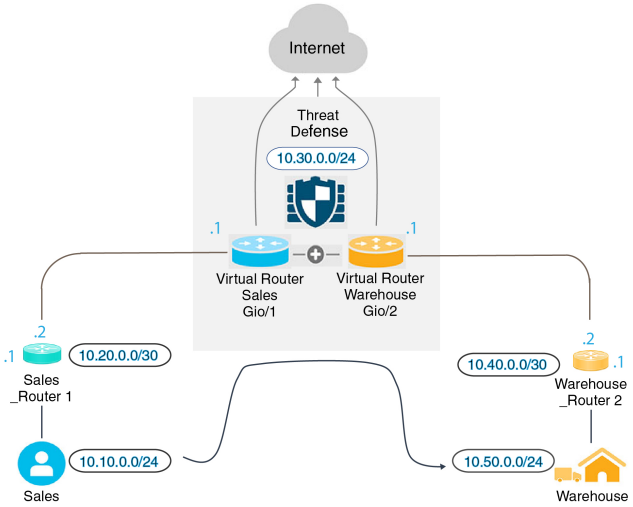
相关主题

如何通过站点间 VPN 保护来自多个虚拟路由器的网络流量
如何对不同虚拟路由器中的内部网络进行 RA VPN 访问

如何通过多个虚拟路由器路由到远程服务器

使用虚拟路由器时，您可能会遇到一种情况，即一个虚拟路由器中的用户需要访问只能通过单独虚拟路由器进行访问的服务器。

以下图为例。销售团队的工作站连接到“销售”虚拟路由器。仓库服务器通过“仓库”虚拟路由器连接。如果销售团队需要在 IP 地址为 10.50.0.5/24 的仓库服务器上查找信息，则需要泄漏从“销售”虚拟路由器到“仓库”虚拟路由器的路由。“仓库”虚拟路由器还必须具有通往仓库服务器的路由，该服务器在仓库路由器 2 之后多跳。



开始之前

此示例假定您已：

- 在 威胁防御 设备上配置“销售”和“仓库”虚拟路由器，其中 GigabitEthernet 0/1 分配给“销售”虚拟路由器，GigabitEthernet 0/2 分配给“仓库”虚拟路由器。
- 销售路由器 1 具有静态或动态路由，用于将流量从 10.20.0.1/30 接口发送到 10.50.0.5/24。

过程

步骤 1 为 10.50.0.5/24 或 10.50.0.0/24 创建网络对象。此外，为网关 10.40.0.2/30 创建对象。

如果要将路由限制为仓库服务器的单个 IP 地址，请使用主机对象来定义 10.50.0.5。或者，如果销售团队应有权访问仓库中的其他系统，则为 10.50.0.0/24 网络创建网络对象。在本例中，我们将为主机 IP 地址创建路由。

a) 选择**对象**，然后从目录中选择**网络**。

b) 点击 **+**，然后填写仓库服务器的对象属性：

c) 点击**确定**。

d) 点击 +，然后填入仓库网络的路由器网关的对象属性：

e) 点击**确定**。

步骤 2 定义指向“仓库”虚拟路由器中 Gi0/2 接口的“销售”虚拟路由器中的路由泄漏。

在本例中，Gi0/1 命名为“inside”，Gi0/2 命名为“inside-2”。

a) 选择**设备**，然后点击**路由**摘要中的**查看配置**。

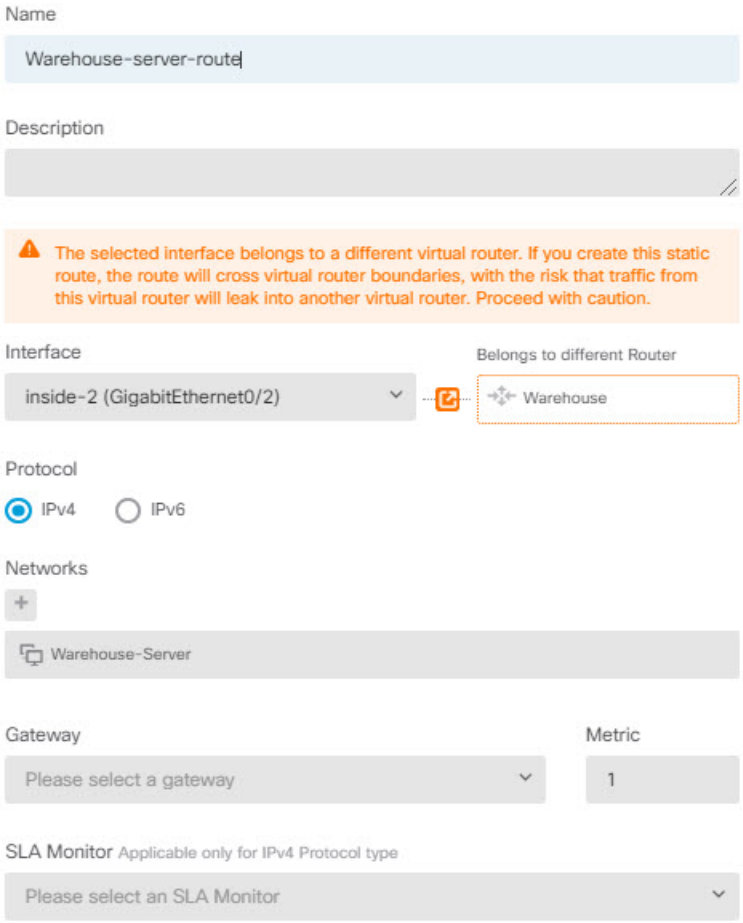
b) 在虚拟路由器列表中，请在“销售”虚拟路由器的操作列中点击查看图标 ( )。

c) 在**静态路由**选项卡上，点击 + 并配置路由：

- **名称** - 任何名称，例如 Warehouse-server-route。
- **接口** - 选择 **inside-2**。您将看到一条警告，指出接口位于不同的路由器中，并且您将创建路由泄漏。这是您需要执行的操作。
- **协议** - 在本例中，使用 **IPv4**。您也可以使用 IPv6 地址来实现此示例。
- **网络** - 选择 Warehouse-Server 对象。

- **网关** - 将此项目留空。将路由泄漏到另一个虚拟路由器时，您不必选择网关地址。

对话框应如下所示：

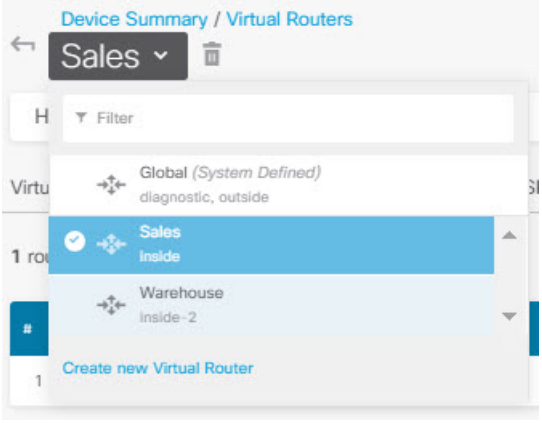


d) 点击**确定**。

步骤 3 在“仓库”虚拟路由器中，定义指向仓库路由器 2 网关的路由。

或者，可以通过配置将动态发现仓库路由器 2 路由的路由协议来完成此操作。在本例中，我们将定义静态路由。

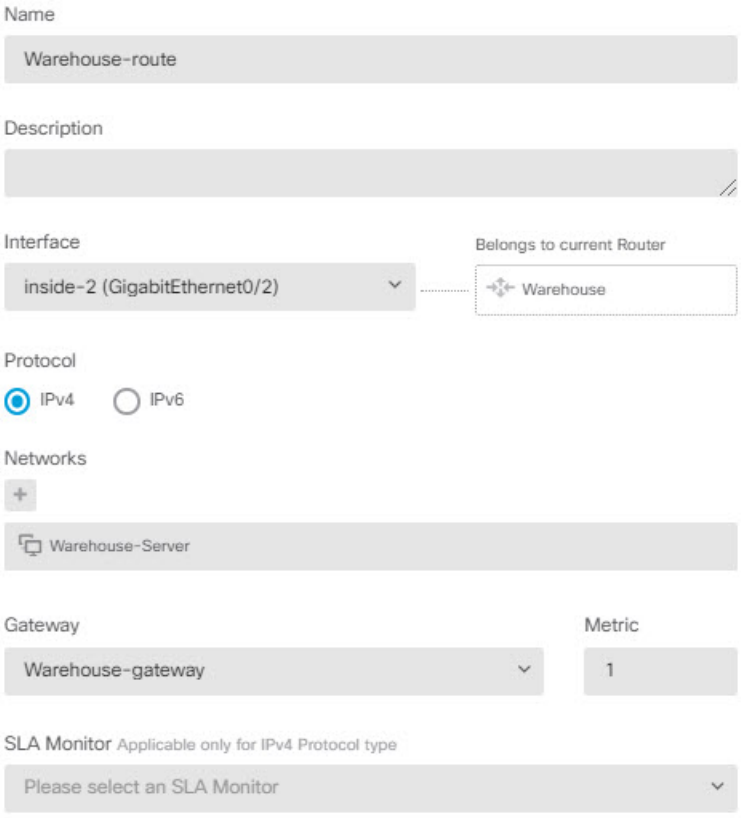
a) 从当前名为“销售”的虚拟路由器下拉列表中，选择“仓库”虚拟路由器以交换路由器。



b) 在**静态路由**选项卡上，点击 + 并配置路由：

- **名称** - 任何名称，例如 Warehouse-route。
- **接口** - 选择 **inside-2**。
- **协议** - 选择 **IPv4**。
- **网络** - 选择 Warehouse-Server 对象。
- **网关** - 选择 Warehouse-gateway 对象。

对话框应如下所示：

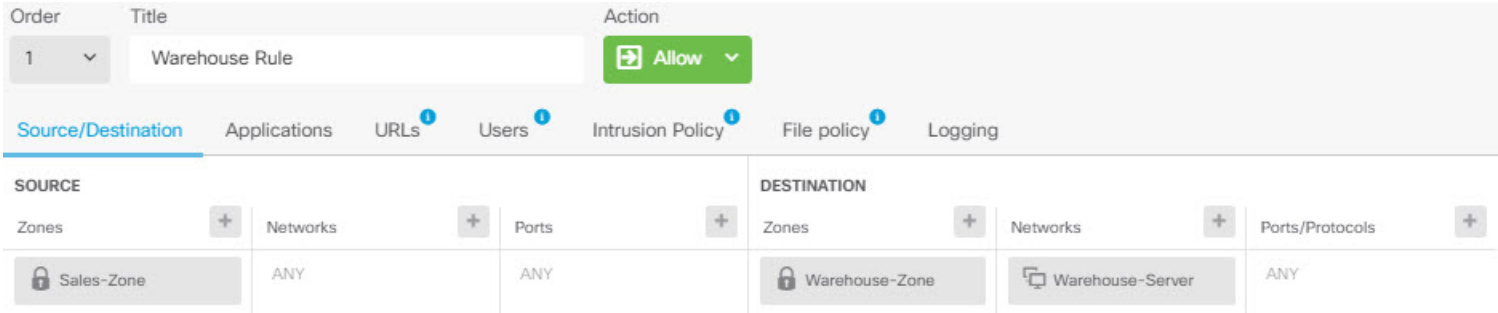


c) 点击**确定**。

步骤 4 确保存在允许访问仓库服务器的访问控制规则。

最简单的规则将允许从“销售”虚拟路由器中的源接口到目标 Warehouse-Server 网络对象的“仓库”虚拟路由器中的目标接口的流量。您可以根据需要对流量应用入侵检测。

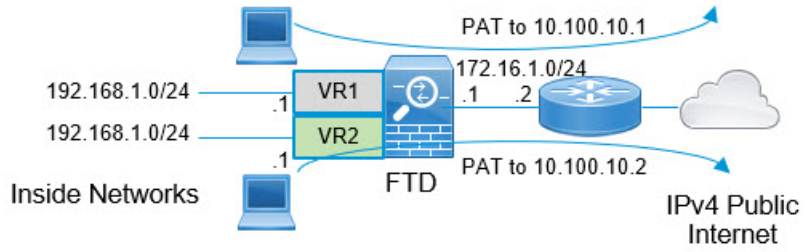
例如，如果“销售”虚拟路由器中的接口位于“销售区域”安全区中，而“仓库”虚拟路由器中的接口位于“仓库区域”安全区中，则访问控制规则将如下所述：



如何提供对包含重叠地址空间的多个虚拟路由器的互联网访问权限

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。例如，可以将 inside 和 inside-2 接口定义为均使用 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。但是，由于在这些单独虚拟路由器中路由的 IP 地址相同，因此您需要认真处理流出虚拟路由器的流量，以确保返回流量流向正确目标地址。

例如，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 将虚拟路由器 1 中的源地址转换为 10.100.10.1，并将虚拟路由器 2 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。请注意，必须使用明确选择的源接口来定义 NAT/PAT 规则，因为使用“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 此示例已简化，其中每个虚拟路由器包含一个接口。如果“内部”虚拟路由器配有多个接口，则需要为每个“内部”接口创建 NAT 规则。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，通过在 NAT 规则中明确标识源接口，也可以简化故障排除过程，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

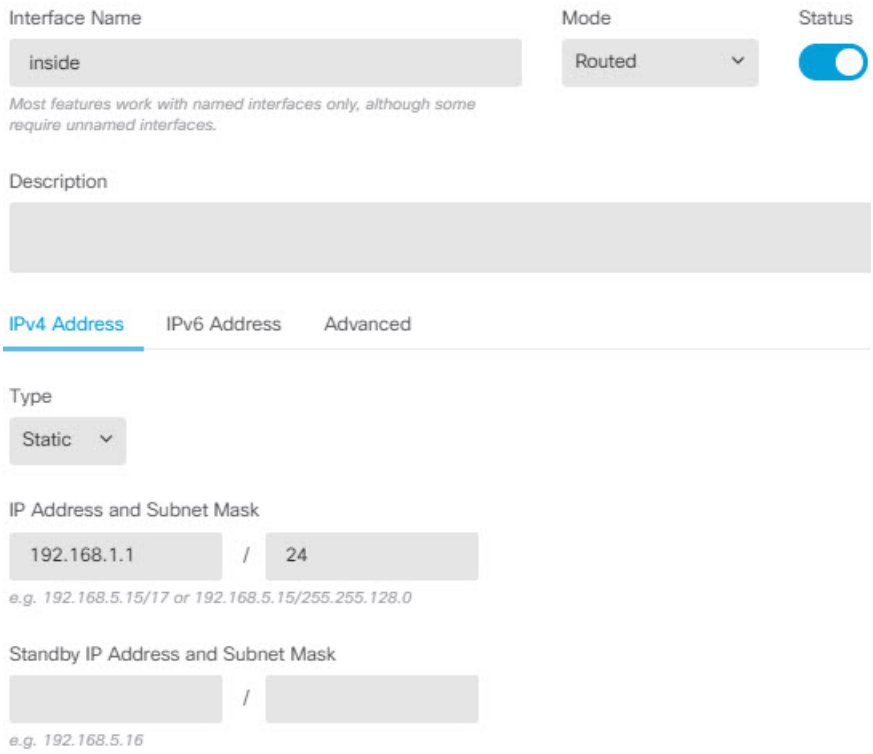
步骤 1 为虚拟路由器 1 (VR1) 配置内部接口。

a) 点击**设备 (Device)**，然后点击**接口 (Interface)** 摘要中的**查看所有接口 (View All Interfaces)**。

b) 对于将分配给 VR1 的接口，在“操作”(Action) 列中点击编辑图标 ( )。

c) 至少配置以下属性：

- **名称** - 在本例中为 **inside**。
- **模式** - 选择**路由**。
- **状态** - 启用接口。
- **IPv4 地址** > **类型** - 选择**静态**。
- **IPv4 地址和子网掩码** - 输入 192.168.1.1/24。



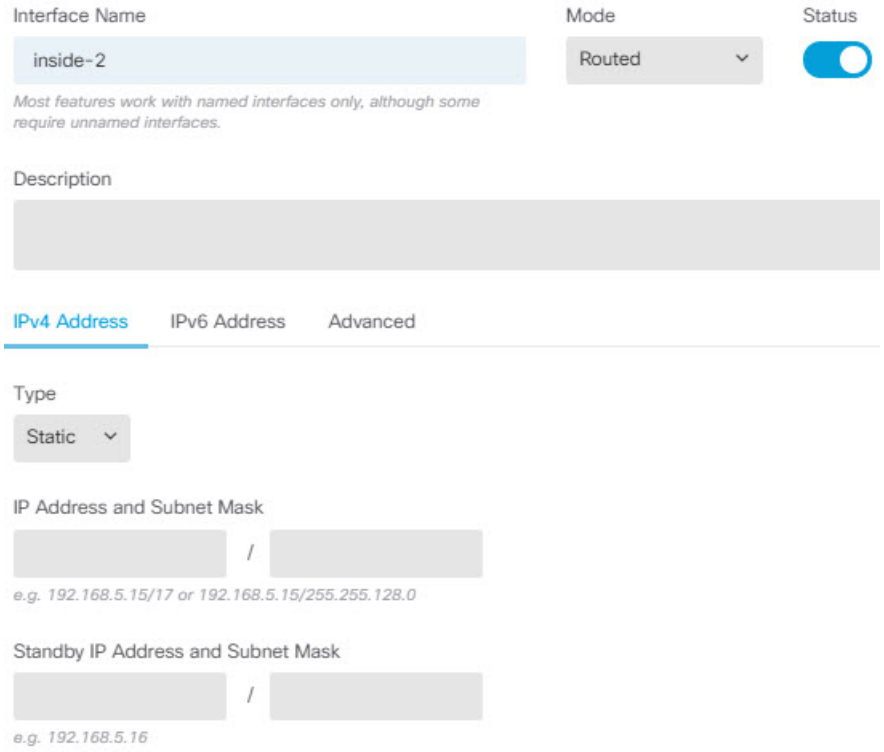
d) 点击**确定 (OK)**。

步骤 2 为虚拟路由器 2 (VR2) 配置 inside-2 接口，但不指定 IP 地址。

a) 在“接口列表”(Interfaces listing) 页面上，点击您将分配给 VR2 的接口的“操作”(Action) 列中的编辑图标 。

b) 至少配置以下属性：

- **名称** - 在本例中为 **inside-2**。
- **模式** - 选择**路由**。
- **状态** - 启用接口。
- **IPv4 地址** > **类型** - 选择**静态**。
- **IPv4 地址和子网掩码** - 将这些字段留空。如果您现在尝试配置与内部接口相同的地址，系统将显示一条错误消息，并阻止您创建非功能性配置。无法通过同一路由器中的不同接口路由到同一地址空间。



c) 点击**确定 (OK)**。

步骤 3 配置虚拟路由器 VR1，其中包括到外部接口的静态默认路由泄漏。

a) 选择**设备 (Device)**，然后点击**路由 (Routing)** 摘要中的**查看配置 (View Configuration)**。

b) 点击“路由”(Routing) 页面顶部的**添加多个虚拟路由器 (Add Multiple Virtual Routers)**。

c) 在说明性面板的右下角，点击**创建第一个自定义虚拟路由器 (Create First Custom Virtual Router)**。

d) 填写虚拟路由器 VR1 的属性。

- **名称** - 输入 VR1 或您选择的其他名称。
- **接口 (Interfaces)** - 点击 **+**，选择 **inside**，然后点击**确定 (OK)**。

e) 点击**确定 (OK)**。

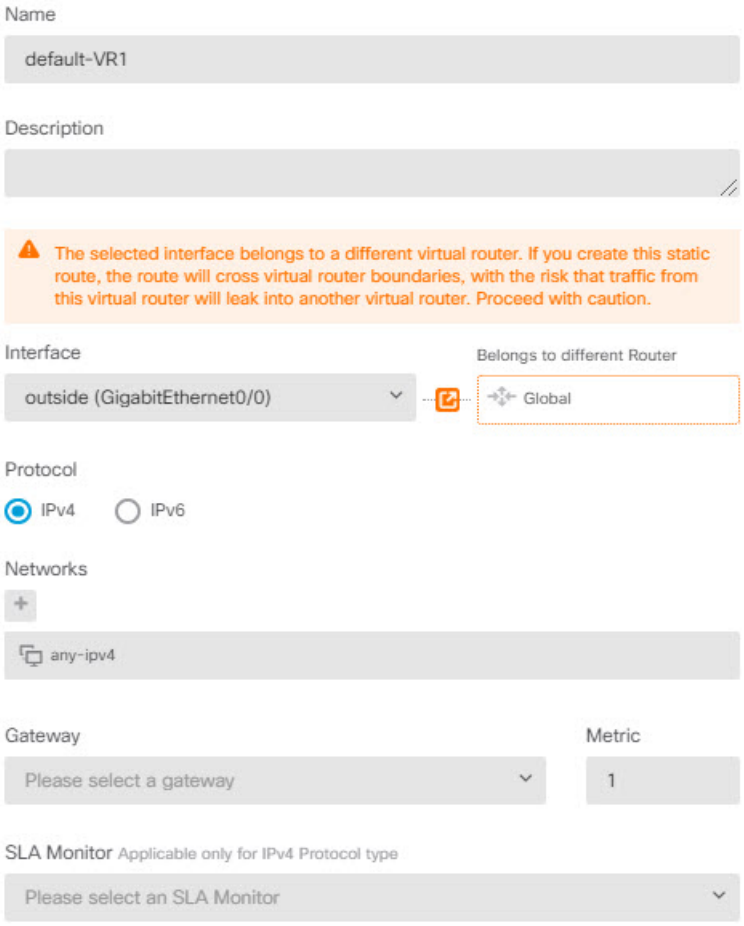
对话框将关闭，并显示虚拟路由器列表。

f) 在虚拟路由器列表中，请在 VR1 虚拟路由器的操作列中点击查看图标 ( )。

g) 在**静态路由 (Static Routing)** 选项卡上，点击 **+** 并配置路由：

- **名称** - 任何名称（例如，**default-VR1**）。
- **接口** - 选择 **outside**。您将看到一条警告，指出接口位于不同的路由器中，并且您将创建路由泄漏。这是您需要执行的操作。
- **协议** - 在本例中，使用 **IPv4**。
- **网络** - 选择 **any-ipv4** 对象。这将是无法在 VR1 内路由的任何流量的默认路由。
- **网关** - 将此项目留空。将路由泄漏到另一个虚拟路由器时，您不必选择网关地址。

对话框应如下所示：



h) 点击**确定 (OK)**。

步骤 4 配置虚拟路由器 VR2，其中包括到外部接口的静态默认路由泄漏。

a) 查看 VR1 时，点击后退按钮（ ）可返回到虚拟路由器列表。

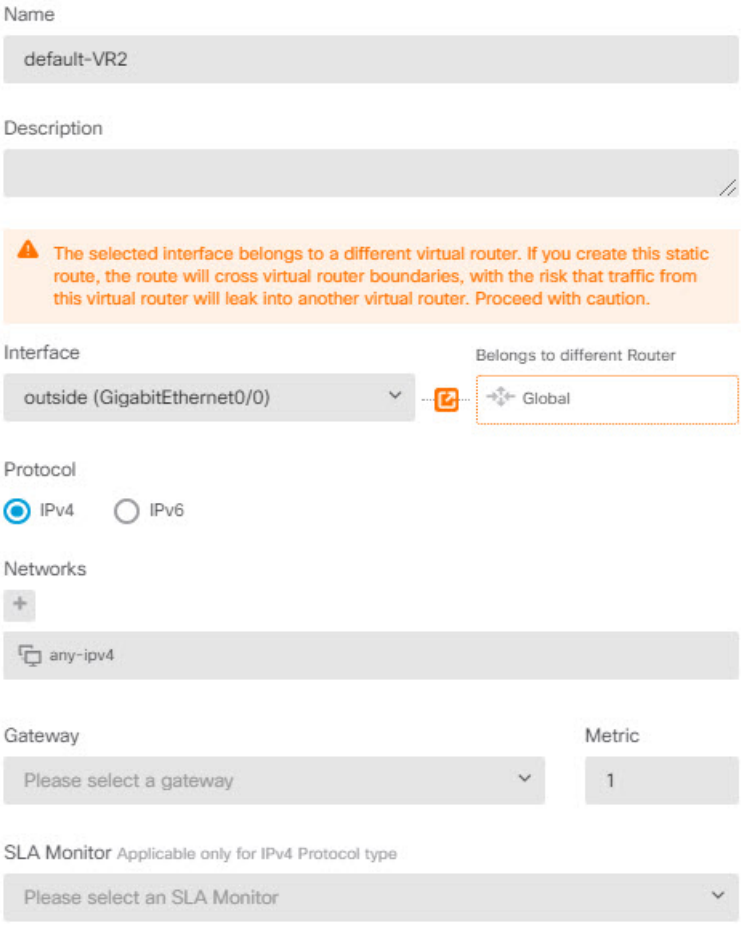
b) 点击列表顶部的 +。
c) 填写虚拟路由器 VR2 的属性。
   - **名称** - 输入 VR2 或您选择的其他名称。
   - **接口 (Interfaces)** - 点击 +，选择 **inside-2**，然后点击**确定 (OK)**。

d) 点击**确定 (OK)**。

   对话框将关闭，并显示虚拟路由器列表。

e) 在虚拟路由器列表中，请在 VR2 虚拟路由器的操作列中点击查看图标 ( )。
f) 在**静态路由 (Static Routing)** 选项卡上，点击 + 并配置路由：
   - **名称** - 任何名称（例如，**default-VR2**）。
   - **接口** - 选择 **outside**。您将看到一条警告，指出接口位于不同的路由器中，并且您将创建路由泄漏。这是您需要执行的操作。
   - **协议** - 在本例中，使用 **IPv4**。
   - **网络** - 选择 **any-ipv4** 对象。这将是用于无法在 VR2 内路由的任何流量的默认路由。
   - **网关** - 将此项目留空。将路由泄漏到另一个虚拟路由器时，您不必选择网关地址。

   对话框应如下所示：

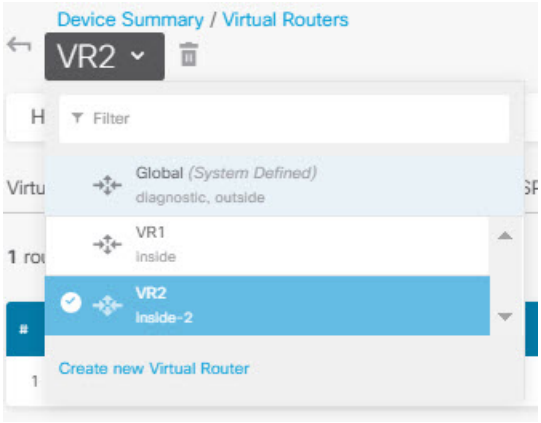


g) 点击**确定 (OK)**。

步骤 5 在全局路由器中创建到外部接口的默认路由。

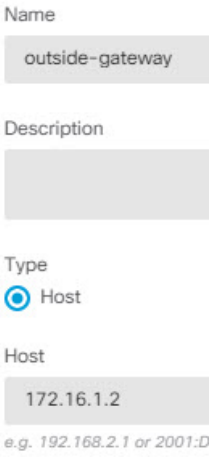
此路由用于为从两个虚拟路由器泄漏到全局路由器的外部接口的流量分配正确的网关。

a) 查看 VR2 时，点击页面顶部的 VR2 名称以打开虚拟路由器列表，然后选择全局路由器。

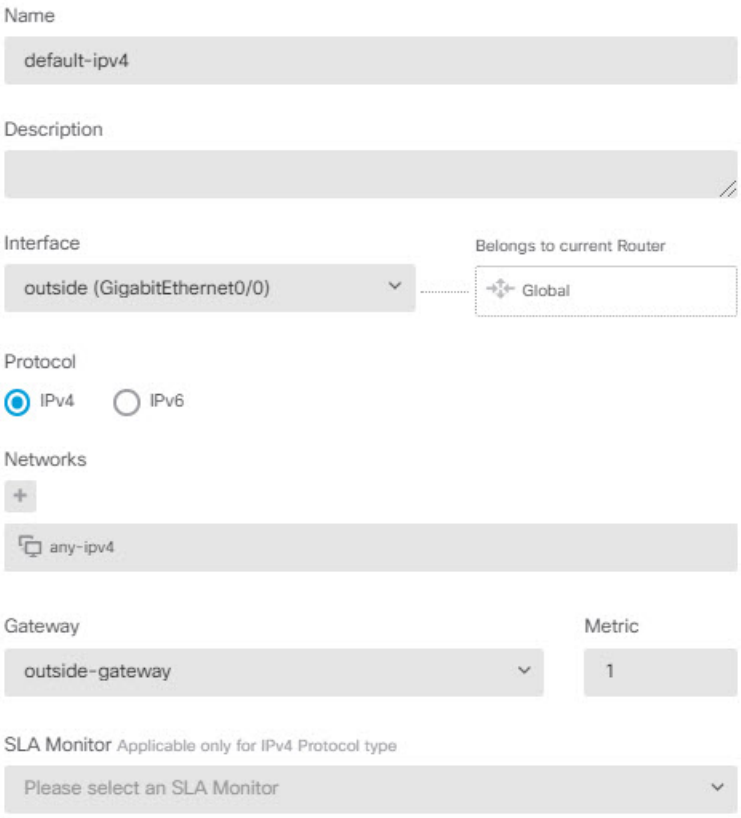


b) 在全局路由器的“静态路由”(Static Routing) 选项卡上，点击 **+** 并配置路由：

- **名称** - 任何名称（例如，default-ipv4）。
- **接口** - 选择 **outside**。
- **协议** - 在本例中，使用 **IPv4**。
- **网络** - 选择 **any-ipv4** 对象。这将是用于任何 IPv4 流量的默认路由。
- **网关 (Gateway)** - 假设对象尚不存在，点击**创建新网络对象 (Create New Network Object)**，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，在静态路由的“网关”字段中选择该对象。



对话框应如下所示：



c) 点击**确定 (OK)**。

步骤 6 返回**接口 (Interfaces)** 页面，并将 IP 地址添加到 inside-2。

a) 点击**设备 (Device)**，然后点击**接口 (Interface)** 摘要中的**查看所有接口 (View All Interfaces)**。

b) 对于将分配给 VR2 的 inside-2 接口，点击“操作”(Action) 列中的编辑图标 ( )。

c) 在 **IPv4 地址**选项卡上，输入 192.168.1.1/24 作为 IP 地址和子网掩码。

d) 点击**确定 (OK)**。

现在将不会出现重复 IP 地址的错误，因为 inside 和 inside-2 接口现在位于不同的虚拟路由器中。

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

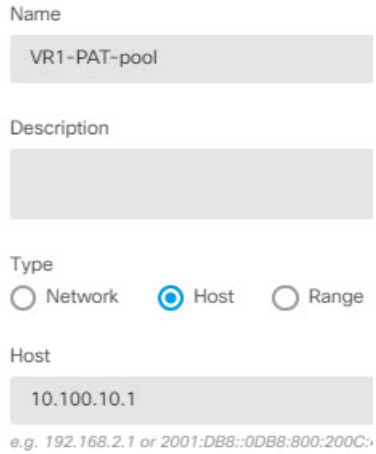
a) 选择**策略 (Policies)**，然后点击 **NAT**。

b) 如果内-外接口已有名为 InsideOutsideNatRule 的手动 NAT 规则来应用接口 PAT，请点击对应于该规则的编辑 ( ) 图标。否则，点击 **+** 创建新规则。

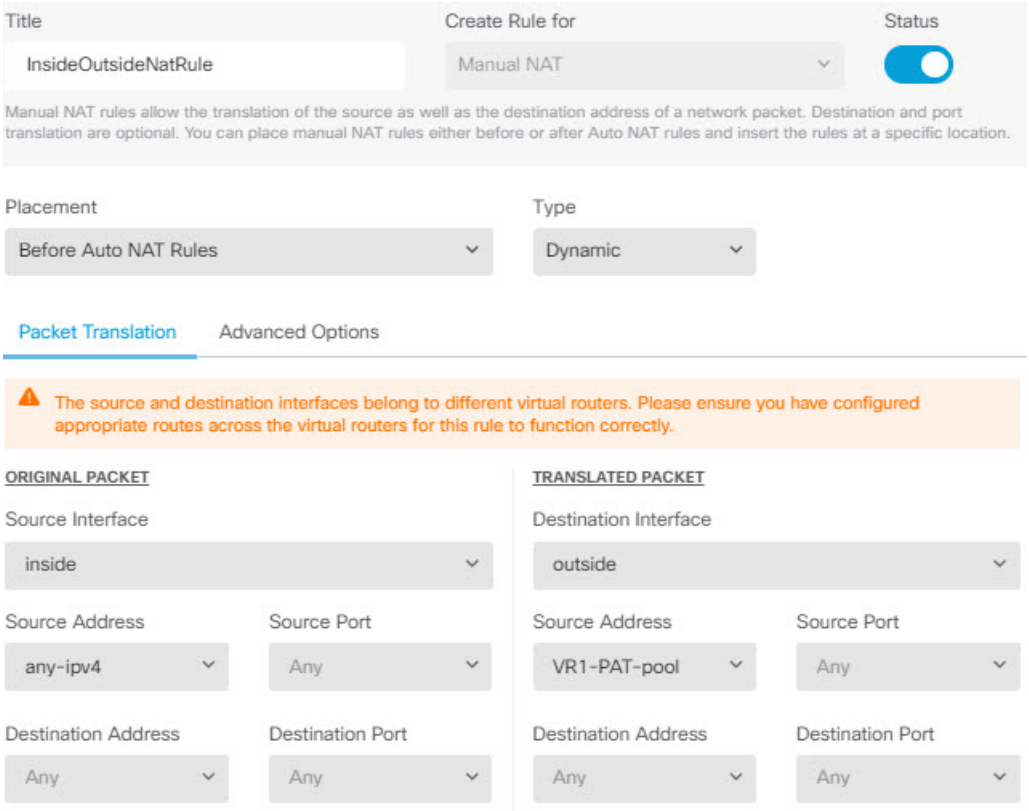
请注意，如果编辑现有规则，现在会出现一条警告，指出源接口和目标接口位于不同的虚拟路由器中，并且您需要定义路由。这是您之前在本程序中执行的操作。

c) 假设要编辑一个现有规则，请点击**转换后的数据包 (Translated Packet)** > **源地址 (Source Address)** 中的下拉箭头，然后点击**创建新网络 (Create New Network)**（假设您没有用于定义 10.100.10.1 的主机对象）。

d) 配置 PAT 地址的主机网络对象。此对象应类似于以下所示：



e) 选择新对象作为**转换后的数据包** > **源地址**。NAT 规则应类似于以下内容：



f) 点击**确定 (OK)**。

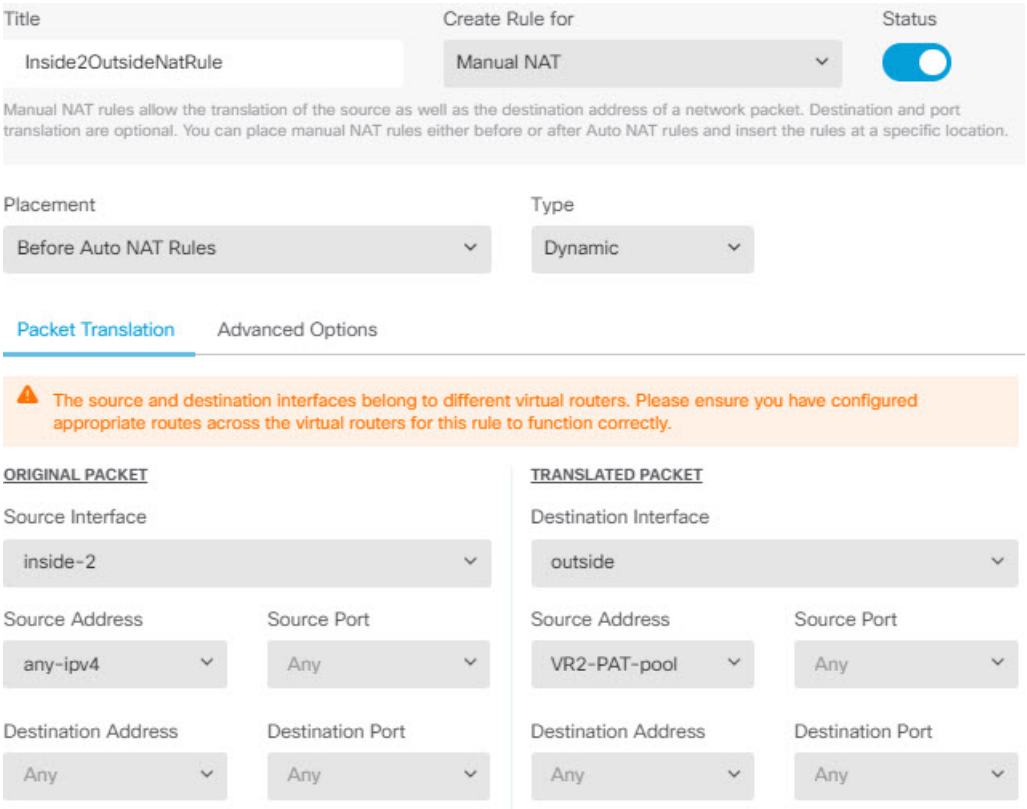
步骤 8 创建 NAT 规则，将从 inside-2 流向外部的流量 PAT 到 10.100.10.2。

此规则与 VR1 的规则完全相同，但以下项除外：

- **名称** - 必须唯一，例如 Inside2OutsideNatRule。
- **原始数据包** > **源接口** - 选择 inside-2。

- **转换后的数据包** > **源地址** - 为 10.100.10.2 创建新的主机网络对象。

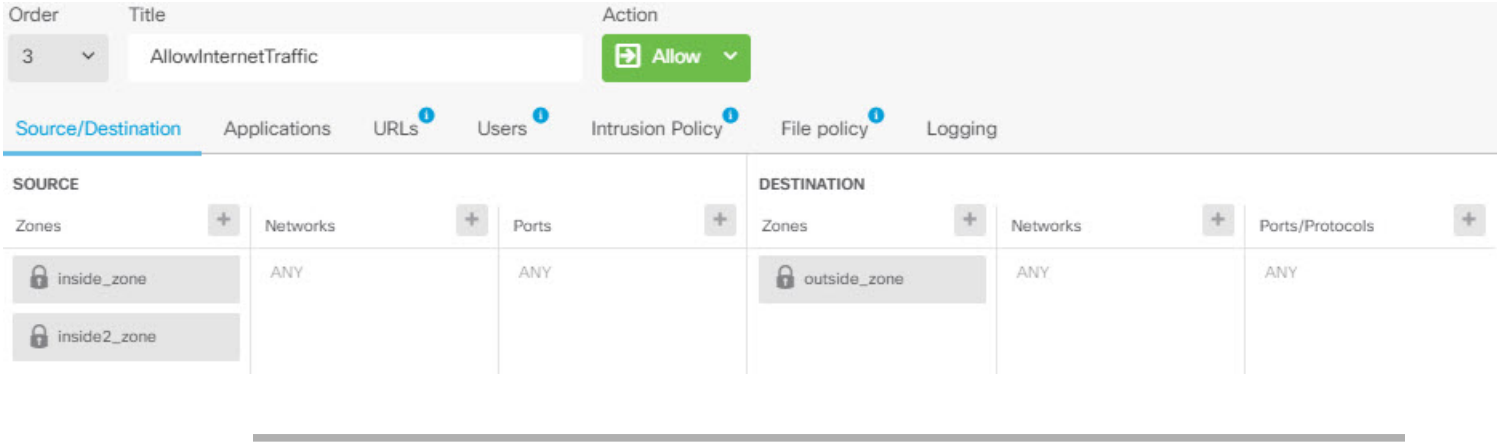
此规则应类似于以下内容：



步骤 9 选择**策略** > **访问控制**，并配置访问控制规则以允许将 inside_zone 和 inside2_zone 中的流量传输到 outside_zone。

最后，您需要配置访问控制策略以允许从 inside 和 inside-2 接口向外部接口传输流量。由于访问控制规则要求使用安全区，因此您需要为每个接口创建区域。或者，可以创建单个区域来同时保存 inside 和 inside-2，但您可能希望在此处或其他策略中创建其他规则，以区分在这些路由器中对流量的处理方式。

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：可以根据需要将入侵策略应用于此规则。可以定义其他规则来阻止不需要的流量，例如，用于实施URL过滤操作。



监控虚拟路由器

要对虚拟路由器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 vrf** 显示有关系统上定义的虚拟路由器的信息。
- **show ospf** ［**vrf** *name* | **all**］

  显示有关虚拟路由器中 OSPF 进程的信息。您可以指定虚拟路由器以仅查看有关该虚拟路由器中进程的信息，或者忽略此选项，以便查看所有虚拟路由器上的 VRF 信息。使用 **show ospf ?** 可查看其他选项。
- **show bgp** ［**vrf** *name* | **all**］

  显示有关虚拟路由器中 BGP 进程的信息。您可以指定虚拟路由器以仅查看有关该虚拟路由器中进程的信息，或者忽略此选项，以便查看所有虚拟路由器上的 VRF 信息。使用 **show bgp ?** 可查看其他选项。
- **show eigrp** 选项

  显示有关 EIGRP 进程的信息。选择 **show eigrp ?** 可查看可用选项。

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。