网络地址转换 (NAT)

以下主题介绍网络地址转换 (NAT) 及其配置方法。

为何使用 NAT？

IP 网络中的每台计算机和设备都分配了标识主机的唯一 IP 地址。因为缺乏公用 IPv4 地址，所以这些 IP 地址中的大多数都是专用地址，在专用公司网络以外的任何地方都不可路由。RFC 1918 定义可以在内部使用但不应通告的专用 IP 地址：

- 10.0.0.0 到 10.255.255.255
- 172.16.0.0 至 172.31.255.255
- 192.168.0.0 到 192.168.255.255

NAT 的主要功能之一是使专用 IP 网络可以连接到互联网。NAT 用公用 IP 地址替换专用 IP 地址，将内部专用网络中的专用地址转换为可在公用互联网上使用的合法可路由地址。NAT 以此方式保存公用地址，因为它可配置为至少仅将整个网络的一个公用地址向外界通告。

NAT 的其他功能包括：

- 安全 - 隐藏内部 IP 地址可以阻止直接攻击。
- IP 路由解决方案 - 使用 NAT 时不会出现重叠 IP 地址。
- 灵活性 - 可以更改内部 IP 寻址方案，而不影响外部的可用公用地址；例如，对于可以访问互联网的服务器，可以维护供互联网使用的固定 IP 地址，但在内部，可以更改服务器地址。

- 在 IPv4 和 IPv6 之间转换（仅路由模式）- 如果想将 IPv6 网络连接到 IPv4 网络，可以利用 NAT 在两种类型的地址之间转换。

注释 不需要 NAT。如果不为一组给定流量配置 NAT，将不转换这些流量，但会正常应用所有安全策略。

NAT 基础知识

以下主题介绍一些 NAT 基础知识。

NAT 术语

本文档使用以下术语：

- 实际地址/主机/网络/接口 - 实际地址是指在主机上定义的转换前地址。在内部网络访问外部网络时，要转换内部网络的典型 NAT 场景中，内部网络会成为“实际”网络。请注意，您可以转换连接到设备的任何网络，而不是只在网络内部转换。因此，如果配置 NAT 以转换外部地址，“实际”可以是指访问内部网络时的外部网络。
- 映射地址/主机/网络/接口 - 映射地址是指实际地址转换而成的地址。在内部网络访问外部网络时，要转换内部网络的典型 NAT 场景中，外部网络会成为“映射”网络。

注释 在地址转换过程中，不会转换为设备接口配置的 IP 地址。

- 双向发起 - 静态 NAT 允许双向发起连接，意味着可发起到主机的连接和从主机发起连接。
- 源 NAT 和目的 NAT - 对于任何给定数据包，将源 IP 地址和目标 IP 地址与 NAT 规则进行比较，转换/不转换一个或两个地址。对于静态 NAT，规则是双向的，因此，请注意，这整个指南中命令和说明中使用的“源”和“目标”，即便是给定的连接，也可能源自“目标”地址。

NAT 类型

可以使用以下方法实施 NAT：

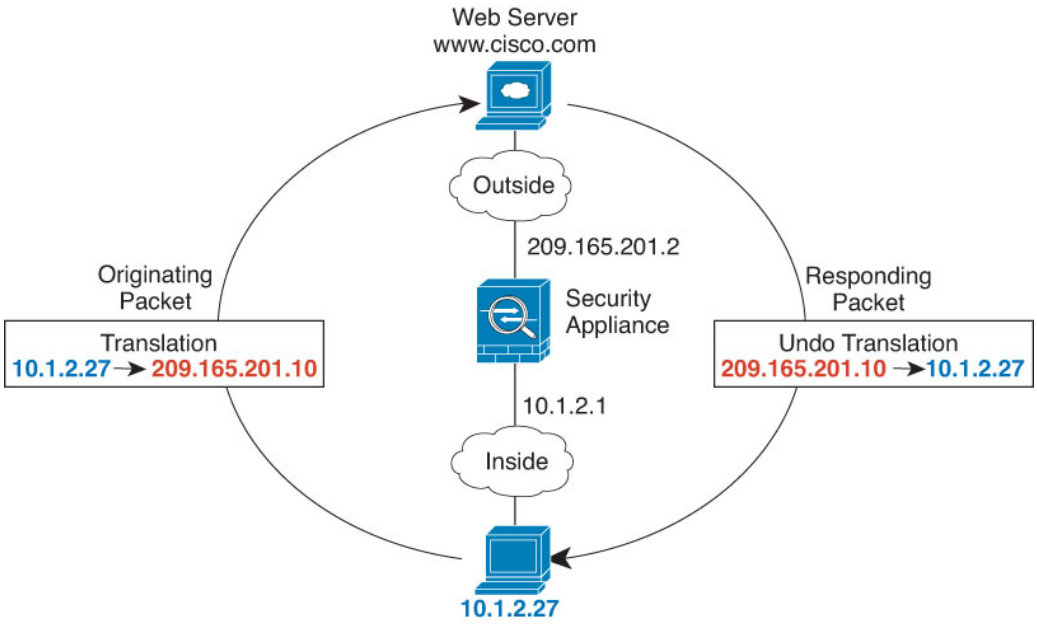
- 动态 NAT - 按先到先得的方式，将一组实际 IP 地址映射到一组映射 IP 地址（通常较小）。仅实际主机可以发起流量。请参阅动态 NAT，第 14 页。
- 动态端口地址转换 (PAT) - 使用 IP 地址的唯一源端口，将一组实际 IP 地址映射到单一 IP 地址。请参阅动态 PAT，第 19 页。
- 静态 NAT - 实际 IP 地址和映射 IP 地址之间的一致映射。允许发起双向流量。请参阅静态 NAT，第 23 页。

- 身份 NAT - 系统将实际地址静态转换为其本身，基本绕过 NAT。当您想转换一大组地址，但又想豁免一小部分地址时，可能就要这样配置 NAT。请参阅身份 NAT，第 31 页。

路由模式下的 NAT

下图显示路由模式下的一个典型 NAT 示例，专用网络位于内部。

图 *1: NAT* 示例：路由模式



1. 当位于 10.1.2.27 的内部主机向 Web 服务器发送数据包时，数据包的实际源地址 10.1.2.27 会转换为映射地址 209.165.201.10。
2. 当服务器响应时，它会将响应发送到映射地址 209.165.201.10，威胁防御设备 接收数据包，因为威胁防御设备 执行代理 ARP 以认领数据包。
3. 接下来，威胁防御设备 变更从映射地址 209.165.201.10 回到实际地址 10.1.2.27 的转换，然后再发送到主机。

自动 NAT 和手动 NAT

可以通过以下两种方法实施地址转换：自动 *NAT* 和手动 *NAT*。

我们建议使用自动 NAT，除非您需要手动 NAT 提供的额外功能。自动 NAT 更容易配置，而且可能对应用（例如 IP 语音 [VoIP]）更加可靠。（对于 VoIP，对不属于规则中使用的任何对象的间接地址进行转换可能会失败。）

自动 NAT

配置为网络对象参数的所有 NAT 规则都被视为自动 *NAT* 规则。这是一种为网络对象配置 NAT 的快捷方法。但是，您无法为对象组创建这些规则。

尽管这些规则配置为对象的一部分，但是您通过对象管理器无法看到对象定义中的 NAT 配置。

当数据包进入接口时，系统会根据自动 NAT 规则来检查源和目标 IP 地址。如果进行独立匹配，可根据独立规则转换数据包中的源地址和目标地址。这些规则互不牵连，可以根据流量使用不同的规则组合。

因为规则从未配对，所以不能指定源 A/目的 A 应当有不同于源 A/目的 B 的转换。手动 NAT 用于实现这样的功能：您可以识别单个规则中的源和目标地址。

手动 NAT

手动 NAT 供您在单个规则中同时标识源和目标地址。同时指定源和目标地址，可以让您指定源 A/目的 A 有不同于源 A/目的 B 的转换。

注释 对于静态 NAT，规则是双向的，因此，请注意，这整个指南中命令和说明中使用的“源”和“目标”，即便是给定的连接，也可能源自“目标”地址。例如，如果配置支持端口地址转换的静态 NAT，然后将源地址指定为某台 Telnet 服务器，并且希望进入该 Telnet 服务器的所有流量都将端口从 2323 转换为 23，那么您就必须指定要转换的源端口（实际端口：23，映射端口：2323）。必须指定源端口是因为您已将 Telnet 服务器地址指定为源地址。

目标地址是可选的。如果指定目标地址，可以将其映射到其本身（身份 NAT），也可以将其映射到不同的地址。目的映射始终是静态映射。

比较自动 NAT 和手动 NAT

这两类 NAT 之间的主要差异是：

- 定义实际地址的方法。
  - 自动 NAT - NAT 规则成为网络对象的参数。网络对象 IP 地址用作原始（实际）地址。
  - 手动 NAT- 标识实际地址和映射地址的网络对象或网络对象组。在这种情况下，NAT 不是网络对象的参数；网络对象或组是NAT配置的参数。能够使用实际地址的网络对象组意味着手动 NAT 更具可扩展性。
- 实施源和目标 NAT 的方法。
  - 自动 NAT- 每个规则都可应用到数据包的源或目标。因此，可能使用两条规则，一条用于源IP地址，一条用于目标IP地址。这两条规则不能绑在一起对源/目的组合进行特定转换。
  - 手动 NAT- 单一规则可以同时转换源和目标。数据包仅匹配一条规则，且不再检查其他规则。即使您不配置可选目标地址，匹配的数据包仍仅匹配一个 手动 NAT 规则。源和目的绑在一起，使您可以根据源/目的组合进行不同的转换。例如，源 A/目的 A 可以有不同于源 A/目的 B 的转换。

- NAT 规则顺序。
  - 自动 NAT- 在 NAT 表中自动排序。
  - 手动 NAT - 在 NAT 表中手动排序（在自动 NAT 规则之前或之后）。

NAT 规则顺序

自动 NAT 和手动 NAT 规则存储在分为三个部分的单个表中。首先应用第一部分规则，其次是第二部分，最后是第三部分，直到找到匹配项为止。例如，如果在第一部分找到匹配项，则不评估第二部分和第三部分。下表显示每个部分的规则顺序。

表 *1: NAT* 规则表

表部分	规则类型	部分中的规则顺序
第 1 部分	手动 NAT	系统按照在配置中出现的顺序应用第一个匹配的规则。因为会应用第一个匹配规则，所以必须确保具体规则位于更加通用的规则前面，否则无法按预期应用特定规则。默认情况下，手动 NAT 规则会添加到第 1 部分。 “具体规则优先”是指： • 静态规则应放在动态规则前面。 • 包含目的地转换的规则应仅放在具有源转换的规则前面。 如果无法消除重叠规则（其中可能有多个规则基于源或目标地址而应用），请特别注意遵循这些建议。
第 2 部分	自动 NAT	如果在第 1 部分未找到匹配项，则会按照以下顺序应用第 2 部分的规则： **1.** 静态规则。 **2.** 动态规则。 **在每个规则类型中，遵循以下排序准则：** **1.** 实际 IP 地址数量 - 从最小到最大。例如，带一个地址的对象将在带 10 个地址的对象之前进行评估。 **2.** 如果数量相同，则按从最低到最高的顺序使用 IP 地址编号。例如，10.1.1.0 在 11.1.1.0 之前进行评估。 **3.** 如果使用同一 IP 地址，则按字母数字顺序使用网络对象名称。例如，abracadabra 在 catwoman 之前进行评估。

表部分	规则类型	部分中的规则顺序
第 3 部分	手动 NAT	如果仍未找到匹配项，则按照在配置中出现的顺序，应用第三部分规则的第一个匹配项。此部分应当包含最通用的规则。还必须确保此部分的特定规则位于通用规则之前，否则会应用通用规则。

例如，对于第二部分规则，在网络对象中定义以下 IP 地址：

- 192.168.1.0/24（静态）
- 192.168.1.0/24（动态）
- 10.1.1.0/24（静态）
- 192.168.1.1/32（静态）
- 172.16.1.0/24（动态）（对象 def）
- 172.16.1.0/24（动态）（对象 abc）

结果排序可能是：

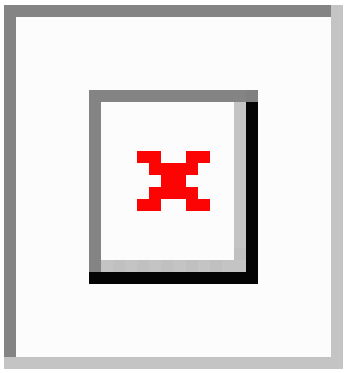
- 192.168.1.1/32（静态）
- 10.1.1.0/24（静态）
- 192.168.1.0/24（静态）
- 172.16.1.0/24（动态）（对象 abc）
- 172.16.1.0/24（动态）（对象 def）
- 192.168.1.0/24（动态）

NAT 接口

除了网桥组成员接口，您可以将NAT规则配置为应用到任何接口（也就是，所有接口），或者也可以标识特定的实际接口和映射接口。还可以为实际地址指定任何接口，为映射地址指定特定接口，反之亦然。

例如，如果在多个接口上使用相同的专用地址，并且在访问外部接口时要将这些地址全部转换到同一全局池，则可能要为实际地址指定任何接口，并且为映射地址指定外部接口。

图 2: 指定任何接口



然而，“任何”接口的概念不适用于网桥组成员接口。当指定“任何”接口时，NAT 将排除所有网桥组成员接口。因此，要将NAT应用于网桥组成员，必须指定成员接口。这样可能导致有许多只有一个接口不同的类似规则。您不能为桥接虚拟接口(BVI)本身配置NAT，只能为成员接口配置NAT。

不能为被动接口配置 NAT。

为 NAT 配置路由

威胁防御 设备需要成为发送到转换（映射）地址的所有数据包的目标。

在发送数据包时，设备使用目标接口（如果指定了接口）或路由表查找（如果未指定接口）来确定出口接口。对于身份 NAT，即使指定了目标接口，您也可以选择使用路由查找。

所需的路由配置类型取决于映射地址的类型，以下主题对此进行了说明。

地址与映射接口在相同的网络中

如果使用与目标（映射）接口在同一网络中的地址，威胁防御设备使用代理ARP应答映射地址的任何 ARP 请求，从而拦截发往映射地址的流量。此解决方案可以简化路由，因为 威胁防御设备 不必成为任何其他网络的网关。如果外部网络包含足够多的空闲地址，并且您正在使用 1:1 转换（例如动态 NAT 或静态 NAT），此解决方案是理想选择。动态 PAT 可显著增加您可以通过少量地址实现的转换数量，因此即使外部网络中的可用地址较少，依然可以使用此方法。对于 PAT，甚至可以使用映射接口的 IP 地址。

唯一网络中的地址

如果需要比目标（映射）接口网络上提供的地址更多的地址，则可以识别其他子网中的地址。上游路由器需要对指向 威胁防御设备 的映射地址进行静态路由。

与实际地址相同的地址（身份 NAT）

身份 NAT 的默认行为已启用代理 ARP，并且与其他静态 NAT 规则匹配。如果需要，可以禁用代理ARP。如果需要，还可以为常规静态NAT禁用代理ARP，在这种情况下，需要确保上游路由器上有适当的路由。

通常，对于身份 NAT，是不需要代理 ARP 的，而且在某些情况下，会造成连接问题。例如，如果为“任何”IP 地址配置一条大体的身份 NAT 规则，则使代理 ARP 保持启用状态会给直接连接到映射接口的网络上的主机造成问题。在这种情况下，当映射网络上的主机要与同一网络上的其他主机通信时，ARP 请求中的地址匹配 NAT 规则（匹配“任何”地址）。然后，威胁防御设备 将代理地址的 ARP，即使数据包实际上不以 威胁防御设备 为目标。（请注意，即便已设置手动 NAT 规则，也会造成此问题；虽然NAT规则必须匹配源地址和目标地址，但仅会根据“源”地址作出代理ARP决定）。如果在实际主机 ARP 响应之前收到 威胁防御设备 ARP 响应，则流量会错误地发送到 威胁防御设备。

NAT 准则

以下主题提供有关实施 NAT 的详细准则。

接口准则

标准路由物理接口或子接口都支持 NAT。

但是，在网桥组成员接口（作为桥接虚拟接口或 BVI 一部分的接口）上配置 NAT 有以下限制：

- 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。
- 在网桥组成员接口之间执行 NAT 时，必须指定源接口和目标接口。不能指定“任何”作为接口。
- 当目标接口为网桥组成员接口时，不能配置接口 PAT，因为没有连接到该接口的 IP 地址。
- 当源接口和目标接口是同一网桥组的成员时，不能在 IPv4 和 IPv6 网络 (NAT64/46) 之间进行转换。静态 NAT/PAT 44/66、动态 NAT44/66 和动态 PAT44 是唯一允许的方法；不支持动态 PAT66。

IPv6 NAT 准则

NAT 支持 IPv6，但有以下准则和限制。

- 对于标准路由模式接口，您还可以在 IPv4 和 IPv6 之间进行转换。
- 对于同一个网桥组的成员接口，不能在 IPv4 和 IPv6 之间进行转换，而只能在两个 IPv6 或两个 IPv4 网络之间进行转换。此限制不适用于一个接口为网桥组成员，另一个为标准路由接口的情况。
- 在同属一个网桥组的接口之间进行转换时，不能将动态 PAT 用于 IPv6 (NAT66)。此限制不适用于一个接口为网桥组成员，另一个为标准路由接口的情况。
- 对于静态 NAT，可以指定一个最大 /64 的 IPv6 子网。不支持更大的子网。
- 将 FTP 和 NAT46 配合使用时，当 IPv4 FTP 客户端连接到 IPv6 FTP 服务器时，客户端必须使用扩展被动模式 (EPSV) 或扩展端口模式 (EPRT)；在使用 IPv6 时，不支持 PASV 和 PORT 命令。

IPv6 NAT 最佳实践

可以使用 NAT 在 IPv6 网络之间转换，以及在 IPv4 和 IPv6 网络之间转换（仅路由模式）。我们推荐以下最佳实践：

- NAT66（IPv6 对 IPv6）- 我们建议使用静态 NAT。尽管可以使用 NAT 或 PAT，但由于 IPv6 地址大量供应，因此不必使用动态 NAT。如果不想允许返回流量，您可以启用单向静态 NAT 规则（仅限于手动 NAT）。
- NAT46（IPv4 对 IPv6）- 我们建议使用静态 NAT。因为 IPv6 地址空间远远大于 IPv4 地址空间，所以可以轻松满足静态转换需求。如果不想允许返回流量，您可以启用单向静态 NAT 规则（仅限于手动 NAT）。转换为 IPv6 子网（/96 或更低）时，默认情况下，生成的映射地址为有嵌入 IPv4 的 IPv6 地址，其中 32 位 IPv4 地址嵌入在 IPv6 前缀后面。例如，如果 IPv6 前缀为 /96 前缀，则 IPv4 地址附在最后的 32 位地址中。例如，如果将 192.168.1.0/24 映射到 201b::0/96，则 192.168.1.4 将被映射到 201b::0.192.168.1.4（通过混合表示法显示）。如果前缀较小（例如 /64），则 IPv4 地址附在前缀的后面，后缀 0 附在 IPv4 地址后面。
- NAT64（IPv6 到 IPv4）- 可能没有足够的 IPv4 地址来容纳大量的 IPv6 地址。我们建议使用动态 PAT 池提供大量的 IPv4 转换。

对检测到的协议的 NAT 支持

检测打开辅助连接或者在数据包中嵌入 IP 地址的一些应用层协议，以提供以下服务：

- 创建小孔 - 一些应用协议在标准端口或协商的端口上打开辅助 TCP 或 UDP 连接。检测会为这些辅助端口打开小孔，使您无需创建访问控制规则予以允许。
- NAT 重写 - 诸如 FTP 等协议会在数据包数据中嵌入用于辅助连接的 IP 地址和端口，作为协议的一部分。如果 NAT 转换涉及到任一终端，则检测引擎会重写数据包数据以反映嵌入式地址和端口的 NAT 转换。在没有 NAT 重写的情况下，辅助连接不起作用。
- 协议实施 - 一些检测会为检测到的协议实施某种程度的 RFC 一致性。

下表列出了应用 NAT 重写及其 NAT 限制的检测到的协议。当编写包括这些协议的 NAT 规则时，请记住这些限制。此处未列出的协议不应用 NAT 重写。这些检测包括 GTP、HTTP、IMAP、POP、SMTP、SSH 和 SSL。

注释 仅列出的端口支持 NAT 重写。如果在非标准端口上使用这些协议，请勿对连接使用 NAT。

表 *2: NAT* 支持的应用检测

应用	检测到的协议、端口	NAT 限制	创建了小孔
DCERPC	TCP/135	无 NAT64。	是

应用	检测到的协议、端口	NAT 限制	创建了小孔
Diameter	TCP/3868 TCP/5868（用于 TCP/TLS） SCTP/3868	无 NAT/PAT。	是
DNS over UDP	UDP/53	无可用于通过 WINS 进行名称解析的 NAT 支持。	否
ESMTP	TCP/25	无 NAT64。	否
FTP	TCP/21	没有限制。	是
GTP	UDP/3386 (GTPv0) UDP/2123 (GTPv1+)	无扩展 PAT。 无 NAT。	—
H.323 H.225（呼叫信令） H.323 RAS	TCP/1720 UDP/1718 对于 RAS， 则为 UDP/1718-1719	无 NAT64。	是
ICMP ICMP 错误	ICMP （从不会对定向到设备接口的 ICMP 流量进行检测。）	没有限制。	否
IP 选项	RSVP	无 NAT64。	否
M3UA	SCTP/2905	无面向嵌入式地址的 NAT 或 PAT。	-
NetBIOS Name Server over IP	UDP/137、138（源端口）	无 NAT64。	否
RSH	TCP/514	无 PAT。 无 NAT64。	是
RTSP	TCP/554 （对于 HTTP 隐藏没有任何处理。）	无 NAT64。	是
SIP	TCP/5060 UDP/5060	无扩展 PAT。 无 NAT64 或 NAT46。	是
Skinny (SCCP)	TCP/2000	无 NAT64、NAT46 或 NAT66。	是

应用	检测到的协议、端口	NAT 限制	创建了小孔
SQL*Net （版本 1、2）	TCP/1521	无 NAT64。	是
SCTP	SCTP	虽然可以对 SCTP 流量执行静态网络对象 NAT（无动态 NAT/PAT），但检测引擎不用于 NAT。	不支持
Sun RPC	TCP/111 UDP/111	无 NAT64。	是
TFTP	UDP/69	无 NAT64。 不转换负载 IP 地址。	是
XDMCP	UDP/177	无 NAT64。	是

FQDN 目的准则

您可以使用完全限定域名 (FQDN) 网络对象而不是 IP 地址在手动 NAT 规则中指定转换（映射）目的。例如，您可以基于发往 www.example.com Web 服务器的流量创建规则。

使用 FQDN 时，系统基于返回的地址获取 DNS 解析并编写 NAT 规则。如果从 DNS 服务器获取多个地址，则使用的地址基于以下条件：

- 如果某个地址与指定接口位于相同的子网上，则使用该地址。如果没有地址位于相同的子网上，则使用返回的第一个地址。
- 转换后的源和转换后的目的的 IP 类型必须匹配。例如，如果转换后的源地址为 IPv6，则 FQDN 对象必须指定 IPv6 作为地址类型。如果转换后的源为 IPv4，则 FQDN 对象可以指定 IPv4 或 IPv4 和 IPv6。在这种情况下，将选择 IPv4 地址。

不能在用于手动 NAT 目的的网络组中包含 FQDN 对象。在 NAT 中，必须单独使用 FQDN 对象，因为只有单个目的主机才适用于此类 NAT 规则。

如果 FQDN 无法解析为 IP 地址，则在获得 DNS 解析之前该规则不起作用。

其他 NAT 准则

- 对于作为网桥组成员的接口，您需要为成员接口编写 NAT 规则。您无法为桥接虚拟接口 (BVI) 本身编写 NAT 规则。
- 您不能为站点间 VPN 中使用的虚拟隧道接口 (VTI) 编写 NAT 规则。为 VTI 的源接口编写规则不会将 NAT 应用于 VPN 隧道。要编写应用于 VTI 上通过隧道传输的 VPN 流量的 NAT 规则，您必须使用“任何”作为接口，而不能明确指定接口名称。

- （仅限于 自动 NAT。）您仅可为给定对象定义单个 NAT 规则，如果要为某个对象配置多个 NAT 规则，则需要创建通过不同名称指定同一 IP 地址的多个对象。
- 如果在接口上定义了 VPN，则接口上的入站 ESP 流量不受 NAT 规则的约束。系统仅允许已建立的 VPN 隧道的 ESP 流量，而丢弃与现有隧道不相关的流量。此限制适用于 ESP 和 UDP 端口 500 和 4500。
- 如果在应用动态 PAT 设备之后的某设备上定义站点间 VPN，以便 UDP 端口 500 和 4500 不是实际使用的端口，必须从 PAT 设备之后的设备发起连接。响应方无法发起安全关联 (SA)，因为不知道正确的端口号。
- 如果更改 NAT 配置，并且不想等待现有转换超时后再使用新 NAT 配置，则可以在设备 CLI 中使用 **clear xlate** 命令清除转换表。然而，清除转换表将断开使用转换的当前所有连接。

  如果创建应应用于现有连接（例如 VPN 隧道）的新 NAT 规则，则需要使用 **clear conn** 来终止连接。然后，尝试重新建立连接应符合 NAT 规则，且连接应正确进行 NAT。

注释 如果删除动态 NAT 或 PAT 规则，然后使用与已删除规则中地址重叠的映射地址添加新规则，则系统将不使用新规则，直至与已删除规则关联的所有连接超时，或已使用 **clear xlate** 或 **clear conn** 命令将这些连接清除。此保护措施确保相同的地址将不分配至多个主机。

- 不能使用同时包含 IPv4 和 IPv6 地址的对象组，对象组只能包括一种类型的地址。
- NAT 中使用的网络对象不能包含超过 131838 个 IP 地址，无论是显式还是隐式包含在地址或子网范围中。将地址空间分成更小的范围，并为较小的对象编写单独的规则。
- （仅限于手动 NAT。）在 NAT 规则中使用 **any** 作为源地址时，“任何”流量（IPv4 与 IPv6）的定义取决于规则。只有数据包为 IPv6 至 IPv6 或 IPv4 至 IPv4，威胁防御设备 才能对数据包执行 NAT；借助此前提条件，威胁防御设备 可确定 NAT 规则中的 **any** 的值。例如，如果配置从“任何”到 IPv6 服务器的规则，且该服务器已从 IPv4 地址映射，则**任何**指“任何 IPv6 流量”。如果配置从“任何”到“任何”的规则，并且将源映射至接口 IPv4 地址，则**任何**指“任何 IPv4 流量”，因为映射的接口地址意味着目标也是 IPv4。
- 可以在多条 NAT 规则中使用同一映射对象或组。
- 映射 IP 地址池不能包括：
  - 映射接口的 IP 地址。如果为该规则指定“任何”接口，则禁止所有接口 IP 地址。对于接口 PAT（仅路由模式），指定接口名称而不是接口地址。
  - 故障转移接口 IP 地址。
  - （动态 NAT。）启用 VPN 时的备用接口 IP 地址。
- 避免在静态和动态 NAT 策略中使用重叠地址。例如，使用重叠地址，如果 PPTP 的辅助连接命中静态而非动态 xlate，将无法建立 PPTP 连接。
- 无法在 NAT 规则的源地址和远程访问 VPN 地址池中使用重叠地址。

- 如果在规则中指定目标接口，则该接口用作出口接口，而不是在路由表中查找路由。但是，对于身份 NAT，您可以选择改为使用路由查找。
- NAT 仅适用于直通流量。系统生成的流量不进行 NAT。
- 请不要使用大写或小写字母的任意组合来命名网络对象或组 pat-pool。
- 不能在协议无关组播 (PIM) 寄存器的内部负载上使用 NAT。
- (手动 NAT) 为双 ISP 接口设置（使用路由配置中的服务级别协议的主接口和备用接口）编写 NAT 规则时，请勿在规则中指定目标条件。确保主接口的规则在备用接口的规则之前。这允许设备在主 ISP 不可用时根据当前路由状态选择正确的 NAT 目的接口。如果指定目标对象，NAT 规则将始终为其他规则选择主接口。
- 如果您收到不应与为接口定义的 NAT 规则匹配的流量的 ASP drop reason nat-no-xlate-to-pat-pool，请为受影响的流量配置身份 NAT 规则，以便流量可以不经转换地通过。
- 如果为 GRE 隧道终端配置 NAT，则您必须在终端上禁用保持连接，否则将无法建立隧道。终端将保持连接发送到原始地址。

配置 NAT

网络地址转换可能非常复杂。我们建议规则应尽可能保持简单，以避免出现转换问题和难以进行故障排除的情况。在实施 NAT 之前仔细规划，这非常重要。以下程序说明了规划的基本方法。

过程

步骤 1 依次选择**策略** > **NAT**。

步骤 2 决定您需要哪些类型的规则。

可以创建动态 NAT、动态 PAT、静态 NAT 和身份 NAT 规则。有关概述，请参阅 NAT 类型，第 2 页。

步骤 3 决定应将哪些规则作为手动或自动 NAT 来实施。

有关这两种实施选项的比较，请参阅自动 NAT 和手动 NAT，第 3 页。

步骤 4 遵循以下部分中的说明创建规则。

- 动态 NAT，第 14 页
- 动态 PAT，第 19 页
- 静态 NAT，第 23 页
- 身份 NAT，第 31 页

步骤 5 管理 NAT 策略和规则。

您可以执行以下操作来管理策略及其规则。

- 要编辑规则，请点击规则的编辑图标 ( )。
- 要删除某条规则，请点击该规则的删除图标 ( )。

动态 NAT

以下主题介绍动态 NAT 以及如何配置动态 NAT。

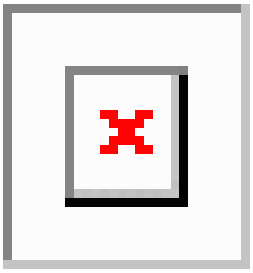
关于动态 NAT

动态NAT将一个实际地址组转换为一个可在目标网络上路由的映射地址池。映射池通常包含少于实际地址组的地址。当您要转换的主机访问目标网络时，NAT会从映射池中为该主机分配IP地址。仅在实际主机发起连接时创建转换。转换仅在连接期间发生，而且转换超时后，给定用户不保持同一IP地址。因此，目标网络上的用户不能向使用动态NAT的主机发起可靠连接，即使访问规则允许该连接。

注释 在转换期间，如果访问规则允许连接转换后主机，远程主机可以发起这种连接。因为地址不可预测，所以与主机的连接不可能发生。然而，在这种情况下，可以依靠访问规则的安全性。

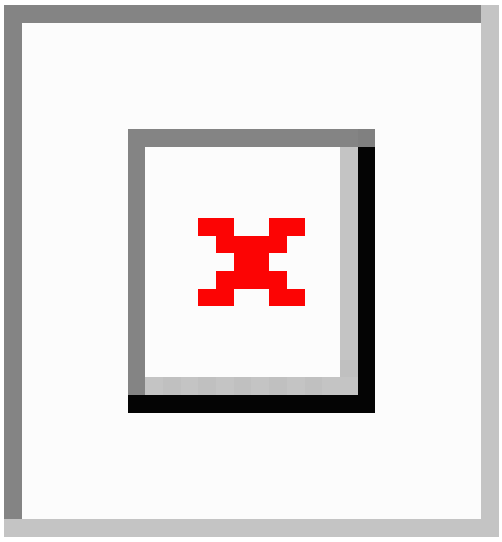
下图显示典型的动态 NAT 场景。仅实际主机可以创建 NAT 会话，允许返回响应流量。

图 *3:* 动态 *NAT*



下图显示一台远程主机尝试发起到映射地址的连接。该地址当前不在转换表中；因此，会丢弃数据包。

图 *4:* 远程主机尝试向映射地址发起连接



动态 NAT 的优缺点

动态 NAT 有以下缺点：

- 如果映射池的地址少于实际组，并且流量数量大于预期，地址可能会用尽。

  如果经常发生这种情况，请使用 PAT 或 PAT 回退方法，因为 PAT 可以使用单一地址的端口提供超过 64,000 次转换。

- 不得不利用映射池中的大量可路由地址，而且可能没有大量的可路由地址可用。

动态 NAT 的优点在于，某些协议不能使用 PAT。PAT 不适用于以下项：

- 没有超载端口的 IP 协议，例如 GRE 0 版本。
- 某些多媒体应用，它们在一个端口上有数据流，在另一个端口上有控制路径，并且不是开放标准。

配置动态自动 NAT

使用动态自动 NAT 规则将地址转换为可在目标网络中路由的其他 IP 地址。

开始之前

选择**对象**并创建规则中所需的网络对象或组。或者，您可以在定义NAT规则时创建对象。对象必须满足以下要求：

- **原始地址** - 该地址必须是网络对象（而非组），而且它可以是主机、范围或子网。
- **转换后的地址** - 该地址可以是网络对象或组，但是它不能包含子网。组不能同时包含 IPv4 和 IPv6 地址，它只能包含一种类型的地址。 如果某个组同时包含范围和主机 IP 地址，则范围将用于动态 NAT，主机 IP 地址将用作 PAT 回退。

过程

步骤 1 依次选择**策略** > **NAT**。

步骤 2 执行以下操作之一：

- 要创建新规则，请点击 + 按钮。
- 要编辑现有规则，请点击规则的编辑图标 ( )。

（要删除不再需要的规则，请点击该规则的垃圾桶图标。）

步骤 3 配置基本规则选项：

- **标题** - 为规则输入名称。
- **创建规则用于** - 选择**自动 NAT**。
- **类型** - 选择**动态**。

步骤 4 配置以下数据包转换选项：

- **源接口**、**目标接口** -（网桥组成员接口的必选项。）应用此 NAT 规则的接口。**源**是实际接口，流量通过该接口进入设备。**目标**是映射接口，流量通过该接口离开设备。默认情况下，此规则应用于除网桥组成员接口之外的所有接口（**任意**）。
- **原始地址** - 包含您要转换的地址的网络对象。
- **转换后的地址** - 包含映射地址的网络对象或组。

步骤 5 （可选。）点击**高级选项**链接并选择所需的选项：

- **转换与此规则匹配的 DNS 回复** - 是否转换 DNS 应答中的 IP 地址。对于从映射接口传输到实际接口的 DNS 回复，地址（IPv4 A 或 IPv6 AAAA）记录会从映射值重写为实际值。相反，对于从实际接口传输到映射接口的DNS回复，该记录会从实际值重写为映射值。此选项用于特定情况，有时 NAT64/46 转换（其中重写也会在 A 和 AAAA 记录之间转换）需要使用此选项。有关详细信息，请参阅使用 NAT 重写 DNS 查询和响应，第 72 页。
- **跳转到接口 PAT（目标接口）** - 当已分配其他映射地址后，是否将目标接口的 IP 地址用作备份方法（接口 PAT 回退）。仅当您选择不是网桥组成员的目的地接口时，此选项才可用。

步骤 6 点击**确定 (OK)**。

配置动态手动 NAT

当自动 NAT 不能满足您的需求时，请使用动态手动 NAT 规则。例如，如果您要根据目标进行不同的转换。动态 NAT 会将地址转换为可在目标网络中路由的其他 IP 地址。

开始之前

选择**对象**并创建规则中所需的网络对象或组。组不能同时包含 IPv4 和 IPv6 地址；只能包含一种类型。或者，您可以在定义 NAT 规则时创建对象。对象还必须满足以下要求：

- **原始源地址** - 地址可以是网络对象或组，而且它可以包含主机、范围或子网。如果要转换所有原始源流量，可以跳过此步骤并在规则中指定**任何**。
- **转换后的源地址** - 此选项可以是网络对象或组，但不能包含在子网中。组不能同时包含 IPv4 和 IPv6 地址，它只能包含一种类型的地址。 如果某个组同时包含范围和主机 IP 地址，则范围将用于动态 NAT，主机 IP 地址将用作 PAT 回退。

如果您要在规则中为**原始目标地址**和**转换后的目标地址**配置静态转换，还可以为这些地址创建网络对象。

对于动态 NAT，您还可以对目标执行端口转换。在对象管理器中，请确保有可用于**原始目标端口**和**转换后的目标端口**的端口对象。系统将忽略您指定的源端口。

过程

步骤 1 依次选择**策略** > **NAT**。

步骤 2 执行以下操作之一：

- 要创建新规则，请点击 + 按钮。
- 要编辑现有规则，请点击规则的编辑图标 ()。

（要删除不再需要的规则，请点击该规则的垃圾桶图标。）

步骤 3 配置基本规则选项：

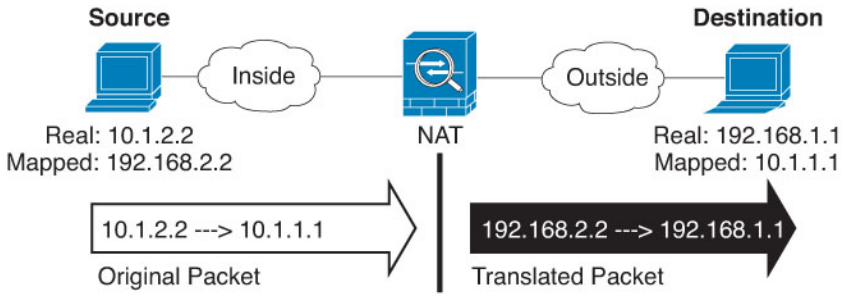
- **标题** - 为规则输入名称。
- **创建规则用于** - 选择**手动 NAT**。
- **规则位置** - 要添加规则的位置。可以将其插入类别中（在自动 NAT 规则之前或之后），或者所选规则的上方或下方。
- **类型** - 选择**动态**。该设置仅应用于源地址。如果为目标地址定义转换，则该转换始终为静态。

步骤 4 配置以下接口选项：

- **源接口**、**目标接口** - （网桥组成员接口的必选项。）应用此 NAT 规则的接口。**源**是实际接口，流量通过该接口进入设备。**目标**是映射接口，流量通过该接口离开设备。默认情况下，此规则应用于除网桥组成员接口之外的所有接口（**任意**）。

步骤 5 确定原始数据包地址（IPv4 或 IPv6 地址）；例如，显示在原始数据包中的数据包地址。

请参阅下图，了解原始数据包与转换后数据包的示例。



- **原始源地址** - 包含将要转换的地址的网络对象或组。
- **原始目标地址** -（可选。）包含目的目标地址的网络对象。如果将此留空，则无论目的目标为何都将应用源地址转换。如果指定目标目的地址，可以为该地址配置静态转换或只是为其使用将身份 NAT 用于该地址。

  可以依次选择**接口**以使原始目标基于源接口（不能为“任意”）。如果选择此选项，则还必须选择一个已转换后的目的目标对象。要为目的目标地址实施带端口转换的静态接口 NAT，请选择此选项，并为目的目标端口选择适当的端口对象。

步骤 6 确定已转换的数据包地址（IPv4 或 IPv6 地址）；例如，显示在目标接口网络中的数据包地址。如果需要，可在 IPv4 与 IPv6 之间进行转换。

- **转换后的源地址** - 包含映射地址的网络对象或组。
- **转换后的目标地址** -（可选。）包含已转换的数据包中使用的目标地址的网络对象或组。如果为**原始目标地址**选择了一个对象，则可以通过选择相同的对象设置身份 NAT（即无转换）。

步骤 7 （可选。）确定用于服务转换的目标服务端口：**原始目标端口**、**转换后的目标端口**。

动态 NAT 不支持端口转换，因此，请将**原始源端口**和**已转换源端口**字段保留为空。然而，由于目标转换始终为静态，因此可为目标端口执行端口转换。

NAT 仅支持 TCP 或 UDP。转换端口时，请确保实际和映射服务对象中的协议相同（同为 TCP 或同为 UDP）。对于身份 NAT，可将相同的服务对象同时用于实际和映射端口。

步骤 8 （可选。）点击**高级选项**链接并选择所需的选项：

- **转换与此规则匹配的 DNS 回复** - 是否转换 DNS 应答中的 IP 地址。对于从映射接口传输到实际接口的 DNS 回复，地址（IPv4 A 或 IPv6 AAAA）记录会从映射值重写为实际值。相反，对于从实际接口传输到映射接口的 DNS 回复，该记录会从实际值重写为映射值。此选项用于特定情况，有时 NAT64/46 转换（其中重写也会在 A 和 AAAA 记录之间转换）需要使用此选项。有关详细信息，请参阅使用 NAT 重写 DNS 查询和响应，第 72 页。
- **跳转到接口 PAT（目标接口）** - 当已分配其他映射地址后，是否将目标接口的 IP 地址用作备份方法（接口 PAT 回退）。仅当您选择不是网桥组成员的目的地接口时，此选项才可用。

步骤 9 点击**确定 (OK)**。

动态 PAT

以下主题介绍动态 PAT。

关于动态 PAT

通过将实际地址和源端口转换为映射地址和唯一端口，动态 PAT 可以将多个实际地址转换为单一映射地址。

每个连接都需要单独的转换会话，因为每个连接的源端口都不同。例如，10.1.1.1:1025 需要来自 10.1.1.1:1026 的单独的转换。

下图显示一个典型的动态 PAT 场景。仅实际主机可以创建 NAT 会话，允许返回响应流量。映射地址对于每次转换都是相同的，但端口需要动态分配。

图 *5:* 动态 *PAT*

对于转换持续时间，如果访问规则允许，目标网络上的远程主机可以发起到转换后主机的连接。因为端口地址（实际和映射）不可预测，所以到该主机的连接不可能发生。然而，在这种情况下，可以依靠访问规则的安全性。

在连接过期后，端口转换也将过期。

注释 建议每个接口使用不同的 PAT 池。如果多个接口使用同一池，尤其是用于“任何”接口时，该池将被快速耗尽，且没有端口可用于新的转换。

动态 PAT 的优缺点

通过动态 PAT，可以使用单一映射地址，从而保存可路由地址。甚至可以将 威胁防御设备 接口 IP 地址用作 PAT 地址。但是，不能将接口 PAT 用于接口上的 IPv6 地址。

在同属一个网桥组的接口之间进行转换时，不能将动态 PAT 用于 IPv6 (NAT66)。此限制不适用于一个接口为网桥组成员，另一个为标准路由接口的情况。

动态 PAT 不适用于某些数据流不同于控制路径的多媒体应用。有关详细信息，请参阅对检测到的协议的 NAT 支持，第 9 页。

动态 PAT 还可以创建大量显示为来自单一 IP 地址的连接，服务器可能将此流量解释为 DoS 攻击。

配置动态自动 PAT

使用动态自动 PAT 规则可将地址转换为唯一的 IP 地址/端口组合，而不是仅转换为多个 IP 地址。可以转换为单个地址，即目标接口的地址或其他地址。

开始之前

选择**对象**并创建规则中所需的网络对象或组。或者，您可以在定义NAT规则时创建对象。对象必须满足以下要求：

- **原始地址** - 该地址必须是网络对象（而非组），而且它可以是主机、范围或子网。
- **转换后的地址** - 可以通过以下选项指定 PAT 地址：
  - **目标接口** - 要使用目标接口 IPv4 地址，不需要网络对象。您不能将接口 PAT 用于 IPv6。
  - **单个 PAT 地址** - 创建包含单个主机的网络对象。

过程

步骤 1 依次选择**策略** > **NAT**。

步骤 2 执行以下操作之一：

- 要创建新规则，请点击 **+** 按钮。
- 要编辑现有规则，请点击规则的编辑图标 ()。

（要删除不再需要的规则，请点击该规则的垃圾桶图标。）

步骤 3 配置基本规则选项：

- **标题** - 为规则输入名称。
- **创建规则用于** - 选择**自动 NAT**。
- **类型** - 选择**动态**。

步骤 4 配置以下数据包转换选项：

- **源接口**、**目标接口** - （网桥组成员接口的必选项。）应用此 NAT 规则的接口。**源**是实际接口，流量通过该接口进入设备。**目标**是映射接口，流量通过该接口离开设备。默认情况下，此规则应用于除网桥组成员接口之外的所有接口（**任意**）。
- **原始地址** - 包含您要转换的地址的网络对象。
- **转换后的地址** - 以下项之一：
  - （接口 PAT。）要使用目标接口的 IPv4 地址，请选择**接口**。您还必须选择具体的目标接口，该接口不能是网桥组成员接口。您不能将接口 PAT 用于 IPv6。
  - 要使用目标接口地址以外的单个地址，请选择为此用途创建的主机网络对象。

步骤 5 （可选。）点击**高级选项**链接并选择所需的选项：

- **跳转到接口 PAT（目标接口）** - 当已分配其他映射地址后，是否将目标接口的 IP 地址用作备份方法（接口 PAT 回退）。仅当您选择不是网桥组成员的目的地接口时，此选项才可用。如果已配置接口 PAT 作为转换后的地址，则不能选择此选项。您也不能将此选项用于 IPv6 网络。

步骤 6 点击**确定 (OK)**。

配置动态手动 PAT

当自动 PAT 不能满足您的需求时，请使用动态手动 PAT 规则。例如，如果您要根据目标进行不同的转换。动态 PAT 可将地址转换为唯一的 IP 地址/端口组合，而不是仅转换为多个 IP 地址。可以转换为单个地址，即目标接口的地址或其他地址。

开始之前

选择**对象**并创建规则中所需的网络对象或组。组不能同时包含 IPv4 和 IPv6 地址；只能包含一种类型。或者，您可以在定义 NAT 规则时创建对象。对象还必须满足以下要求：

- **原始源地址** - 地址可以是网络对象或组，而且它可以包含主机、范围或子网。如果要转换所有原始源流量，可以跳过此步骤并在规则中指定**任何**。
- **转换后的源地址** - 您可通过以下选项指定 PAT 地址：
  - **目标接口** - 要使用目标接口 IPv4 地址，不需要网络对象。您不能将接口 PAT 用于 IPv6。
  - **单个 PAT 地址** - 创建包含单个主机的网络对象。

如果您要在规则中为**原始目标地址**和**转换后的目标地址**配置静态转换，还可以为这些地址创建网络对象。

对于动态 PAT，您还可以对目标执行端口转换。在对象管理器中，请确保有可用于**原始目标端口**和**转换后的目标端口**的端口对象。系统将忽略您指定的源端口。

过程

步骤 1 依次选择**策略** > **NAT**。

步骤 2 执行以下操作之一：

- 要创建新规则，请点击 **+** 按钮。
- 要编辑现有规则，请点击规则的编辑图标 ()。

（要删除不再需要的规则，请点击该规则的垃圾桶图标。）

步骤 3 配置基本规则选项：

- **标题** - 为规则输入名称。
- **创建规则用于** - 选择**手动 NAT**。
- **规则位置** - 要添加规则的位置。可以将其插入类别中（在自动 NAT 规则之前或之后），或者所选规则的上方或下方。

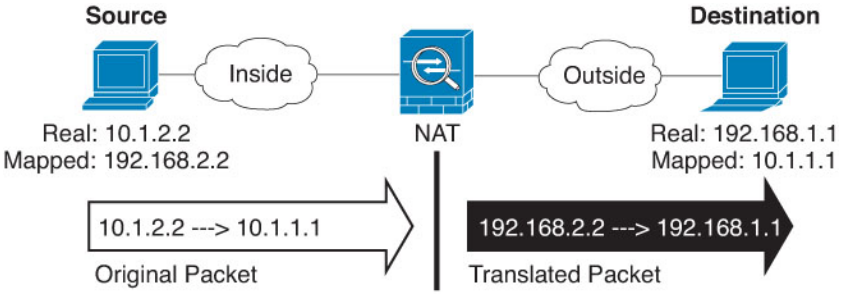
- **类型** - 选择**动态**。该设置仅应用于源地址。如果为目标地址定义转换，则该转换始终为静态。

步骤 4 配置以下接口选项：

- **源接口**、**目标接口** -（网桥组成员接口的必选项。）应用此 NAT 规则的接口。**源**是实际接口，流量通过该接口进入设备。**目标**是映射接口，流量通过该接口离开设备。默认情况下，此规则应用于除网桥组成员接口之外的所有接口（**任意**）。

步骤 5 确定原始数据包地址（IPv4 或 IPv6 地址）；例如，显示在原始数据包中的数据包地址。

请参阅下图，了解原始数据包与转换后数据包的示例。



- **原始源地址** - 包含将要转换的地址的网络对象或组。
- **原始目标地址** -（可选。）包含目的目标地址的网络对象。如果将此留空，则无论目的目标为何都将应用源地址转换。如果指定目标目的地址，可以为该地址配置静态转换或只是为其使用将身份 NAT 用于该地址。

  可以依次选择**接口** 以使原始目标基于源接口（不能为“任意”）。如果选择此选项，则还必须选择一个已转换后的目的目标对象。要为目的目标地址实施带端口转换的静态接口 NAT，请选择此选项，并为目的目标端口选择适当的端口对象。

步骤 6 确定已转换的数据包地址（IPv4 或 IPv6 地址）；例如，显示在目标接口网络中的数据包地址。如果需要，可在 IPv4 与 IPv6 之间进行转换。

- **转换后的源地址** - 以下项之一：
  - （接口 PAT。）要使用目标接口的 IPv4 地址，请选择**接口**。您还必须选择具体的目标接口，该接口不能是网桥组成员接口。您不能将接口 PAT 用于 IPv6。
  - 要使用目标接口地址以外的单个地址，请选择为此用途创建的主机网络对象。
- **转换后的目标地址** -（可选。）包含已转换的数据包中使用的目标地址的网络对象或组。如果为**原始目标**选择了一个对象，则可以通过选择相同的对象确定 NAT（即无转换）。

步骤 7 （可选。）确定用于服务转换的目标服务端口：**原始目标端口**、**转换后的目标端口**。

动态 NAT 不支持端口转换，因此，请将**原始源端口**和**已转换源端口**字段保留为空。然而，由于目标转换始终为静态，因此可为目标端口执行端口转换。

NAT 仅支持 TCP 或 UDP。转换端口时，请确保实际和映射服务对象中的协议相同（同为 TCP 或同为 UDP）。对于身份 NAT，可将相同的服务对象同时用于实际和映射端口。

步骤 8 （可选。）点击**高级选项**链接并选择所需的选项：

- **跳转到接口 PAT（目标接口）**- 当已分配其他映射地址后，是否将目标接口的 IP 地址用作备份方法（接口 PAT 回退）。仅当您选择不是网桥组成员的目的地接口时，此选项才可用。如果已配置接口 PAT 作为转换后的地址，则不能选择此选项。您也不能将此选项用于 IPv6 网络。

步骤 9 点击**确定 (OK)**。

静态 NAT

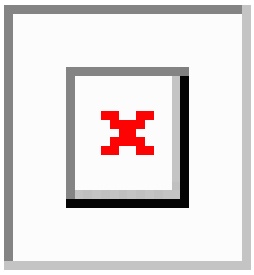
以下主题介绍静态 NAT 以及如何实施静态 NAT。

关于静态 NAT

静态NAT创建实际地址到映射地址的固定转换。因为映射地址对于每个连续连接都是相同的，所以静态NAT允许双向连接发起，即到主机发起和从主机发起（如果有允许这样做的访问规则）。另一方面，通过动态NAT和PAT，每台主机为每次后续转换使用不同的地址或端口，因此，不支持双向发起。

下图显示典型的静态 NAT 场景。转换始终处于活动状态，所以，实际主机和远程主机可以发起连接。

图 *6:* 静态 *NAT*



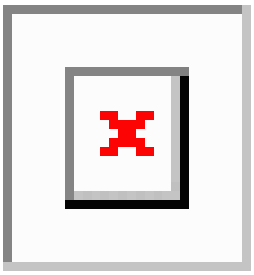
支持端口转换的静态 NAT

支持端口转换的静态 NAT 让您可以指定实际和映射协议及端口。

指定带静态 NAT 的端口时，可以选择将端口和/或 IP 地址映射到同一值或不同值。

下图显示支持端口转换的典型静态NAT场景，其中显示映射到本身的端口和映射到不同值的端口；在这两种情况下，IP 地址映射到不同值。转换始终处于活动状态，所以，转换后主机和远程主机可以发起连接。

图 *7:* 支持端口转换的典型静态 *NAT* 场景



支持端口转换的静态 NAT 规则支持仅访问指定端口的目标 IP 地址。如果您尝试访问其他端口上 NAT 规则未涵盖的的目标 IP 地址，连接将被阻止。此外，对于手动 NAT，如果流量与 NAT 规则的源 IP 地址不匹配，但与目标 IP 地址匹配，流量将被丢弃，不管目标端口为何。因此，您必须为允许发送到目标 IP 地址的所有其他流量添加额外规则。例如，您可以为 IP 地址配置静态 NAT 规则（不含端口规范），并将其放置在端口转换规则后面。

注释 对于需要对辅助信道执行应用检查的应用（例如 FTP 和 VoIP），NAT 会自动转换辅助端口。

下面是使用支持端口转换的静态 NAT 的其他情况。

具有身份端口转换的静态 NAT

可以简化对内部资源的外部访问。例如，如果您有在不同端口上提供服务（例如 FTP、HTTP 和 SMTP）的三个单独的服务器，可以为外部用户提供单个 IP 地址以访问这些服务。然后，可以配置具有身份端口转换的静态NAT，从而根据尝试访问的端口将单个外部IP地址映射到实际服务器的正确 IP 地址。您无需更改端口，因为服务器使用的是标准端口（分别是 21、80 和 25)。

对非标准端口进行端口转换的静态 NAT

还可以利用支持端口转换的静态 NAT 将一个公认端口转换为一个非标准端口，反之亦然。例如，如果内部 Web 服务器使用端口 8080，可以允许外部用户连接到端口 80，然后取消转换到原始端口 8080。同样，要进一步提高安全性，可以告知 Web 用户连接到非标准端口 6785，然后取消转换到端口 80。

具有端口转换的静态接口 NAT

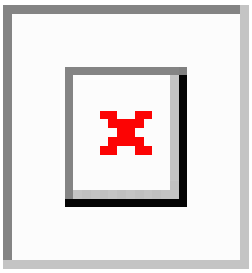
可以配置静态NAT，以将一个实际地址映射到一个接口地址/端口组合。例如，如果要将对设备外部接口的 Telnet 访问重定向至内部主机，则可以将内部主机 IP 地址/端口 23 映射到外部接口地址/端口 23。

一对多静态 NAT

通常，配置带一对一映射的静态 NAT。然而，在某些情况下，可能要将单一实际地址配置到多个映射地址（一对多）。配置一对多静态 NAT 时，当实际主机发起流量时，它始终使用第一个映射地址。然而，对于发起到主机的流量，可以发起到任何映射地址的流量，并且不将它们转换为单一实际地址。

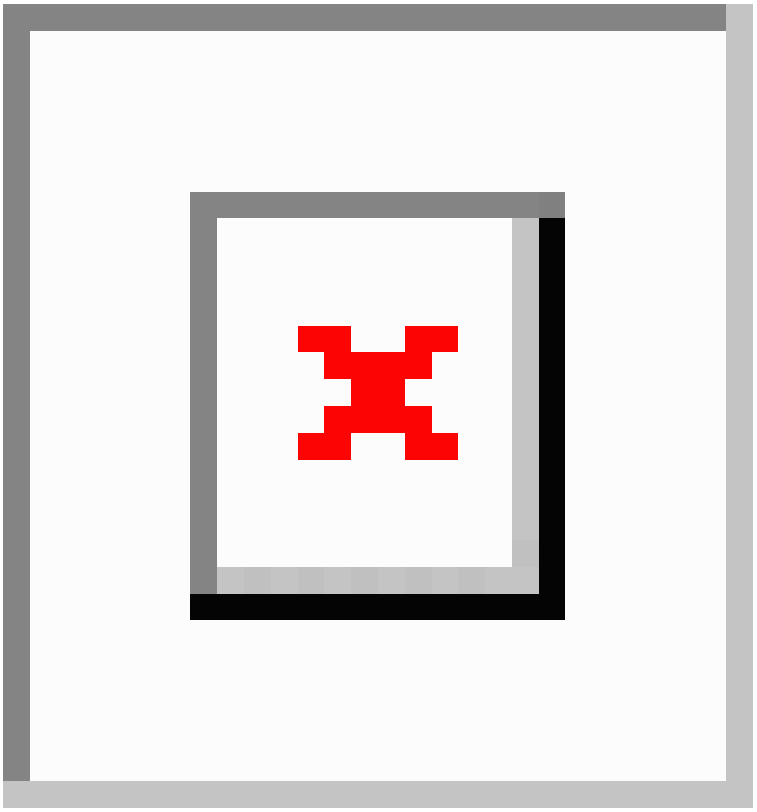
下图显示典型的一对多静态NAT场景。由于实际主机进行的发起的流量始终使用第一个映射地址，因此从技术上说，实际主机 IP/第一个映射 IP 的转换是唯一的双向转换。

图 *8:* 一对多静态 *NAT*



例如，在 10.1.2.27 上有一个负载均衡器。根据请求的 URL，它会将流量重新定向到正确的 Web 服务器。

图 *9:* 一对多静态 *NAT* 示例



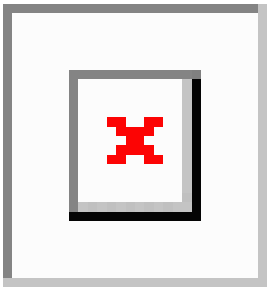
其他映射场景（不推荐）

NAT 具有很高的灵活性，允许任何类型的静态映射场景：不仅包括一对一、一对多，还包括少对多、多对少和多对一映射。我们推荐仅使用一对一或一对多映射。其他映射选项可能会导致意外后果。

在功能上，少对多与一对多相同；但是，因为此配置更加复杂，而且实际映射可能不会一目了然，所以我们建议为每个需要一对多配置的实际地址创建该配置。例如，对于少对多场景，少量的实际地址会按顺序映射到多个映射地址（A 到 1、B 到 2、C 到 3）。当映射所有实际地址时，下一个映射地址会映射到第一个实际地址，依此类推，直到映射了所有映射地址为止（A 到 4、B 到 5、C 到 6）。这将导致每个实际地址有多个映射地址。就像一对多配置一样，仅第一个映射是双向的；后续映射可以将流量发起到实际主机，但所有从实际主机发起的流量仅将第一个映射地址用于源。

下图显示典型的少对多静态 NAT 场景。

图 *10:* 少对多静态 *NAT*

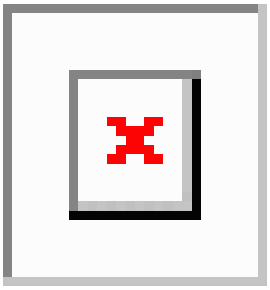


对于实际地址多于映射地址的多对少或多对一配置，映射地址会在实际地址用尽之前先用尽。仅最低实际 IP 地址和映射池之间的映射可以导致双向发起。剩余的更高的实际地址可以发起流量，但不能将流量发起到这些地址（由于五元组 [源 IP、目标 IP、源端口、目标端口、协议] 的唯一性，连接的返回流量会定向到正确的实际地址）。

注释 多对少或多对一 NAT 不是 PAT。如果两台实际主机使用同一源端口号，连接到同一外部服务器和同一 TCP 目标端口，并且两台主机转换到同一 IP 地址，那么由于地址冲突（五元组不唯一），将重置两个连接。

下图显示一个典型的多对少静态 NAT 场景。

图 *11:* 多对少静态 *NAT*



我们建议不要这样使用静态规则，而是为需要双向发起的流量创建一对一规则，为其他地址创建动态规则。

配置静态自动 NAT

使用静态自动 NAT 规则将地址转换为可在目标网络中路由的其他 IP 地址。您还可以通过静态 NAT 规则执行端口转换。

开始之前

选择**对象**并创建规则中所需的网络对象或组。或者，您可以在定义NAT规则时创建对象。对象必须满足以下要求：

- **原始地址** - 该地址必须是网络对象（而非组），而且它可以是主机、范围或子网。
- **转换后的地址** - 您可以通过以下选项指定转换后的地址：
  - **目标接口** - 要使用目标接口 IPv4 地址，不需要网络对象。该选项配置具有端口转换的静态接口NAT：源地址/端口转换为接口的地址和相同的端口号。您不能将接口PAT用于IPv6。
  - **地址** - 创建包含主机、范围或子网的网络对象或组。组不能同时包含 IPv4 和 IPv6 地址；其只能包含一种类型。通常，配置相同数量的映射地址和实际地址，以便进行一对一映射。然而，地址数量可以不匹配。

过程

步骤 1 依次选择**策略** > **NAT**。

步骤 2 执行以下操作之一：

- 要创建新规则，请点击 + 按钮。
- 要编辑现有规则，请点击规则的编辑图标 ( )。

（要删除不再需要的规则，请点击该规则的垃圾桶图标。）

步骤 3 配置基本规则选项：

- **标题** - 为规则输入名称。
- **创建规则用于** - 选择**自动 NAT**。
- **类型** - 选择**静态**。

步骤 4 配置以下数据包转换选项：

- **源接口**、**目标接口** - （网桥组成员接口的必选项。）应用此 NAT 规则的接口。**源**是实际接口，流量通过该接口进入设备。**目标**是映射接口，流量通过该接口离开设备。默认情况下，此规则应用于除网桥组成员接口之外的所有接口（**任意**）。
- **原始地址** - 包含您要转换的地址的网络对象。
- **转换后的地址** - 以下项之一：
  - 要使用一组地址，请选择包含映射地址的网络对象或组。通常，配置相同数量的映射地址和实际地址，以便进行一对一映射。然而，地址数量可以不匹配。

- （具有端口转换的静态接口 NAT。）要使用目标接口的地址，请选择**接口**。您还必须选择具体的目标接口，该接口不能是网桥组成员接口。您不能将接口 PAT 用于 IPv6。该选项配置具有端口转换的静态接口 NAT：源地址/端口转换为接口的地址和相同的端口号。

- （可选。）**原始端口**、**转换后的端口** - 如果需要转换 TCP 或 UDP 端口，请选择定义原始端口和转换后的端口的端口对象。对象必须用于相同的协议。如果对象不存在，请点击**创建新对象**链接。例如，如有必要，可以将 TCP/80 转换为 TCP/8080。

步骤 5 （可选。）点击**高级选项**链接并选择所需的选项：

- **转换与此规则相匹配的 DNS 回复** - 是否转换 DNS 应答中的 IP 地址。对于从映射接口传输到实际接口的 DNS 回复，地址（IPv4 A 或 IPv6 AAAA）记录会从映射值重写为实际值。相反，对于从实际接口传输到映射接口的DNS回复，该记录会从实际值重写为映射值。此选项用于特定情况，有时 NAT64/46 转换（其中重写也会在 A 和 AAAA 记录之间转换）需要使用此选项。有关详细信息，请参阅使用 NAT 重写 DNS 查询和响应，第 72 页。 如果您在进行端口转换，则此选项不可用。
- **不在目标接口上使用代理 ARP** - 为映射 IP 地址的传入数据包禁用代理 ARP。如果使用与映射接口相同的网络中的地址，则系统会使用代理 ARP 来应答映射地址的任何 ARP 请求，从而拦截以映射地址为目的地的流量。此解决方案可以简化路由，因为设备不必是任何其他网络的网关。如果需要，可以禁用代理 ARP，在此情况下需要确保在上游路由器上具有正确的路由。通常，对于身份 NAT，是不需要代理 ARP 的，而且在某些情况下，会造成连接问题。

步骤 6 点击**确定 (OK)**。

配置静态手动 NAT

当自动 NAT 不能满足您的需求时，请使用静态手动 NAT 规则。例如，如果您要根据目标进行不同的转换。静态 NAT 会将地址转换为可在目标网络中路由的其他 IP 地址。您还可以通过静态 NAT 规则执行端口转换。

开始之前

选择**对象**并创建规则中所需的网络对象或组。组不能同时包含 IPv4 和 IPv6 地址；只能包含一种类型。或者，您可以在定义 NAT 规则时创建对象。对象还必须满足以下要求：

- **原始源地址** - 地址可以是网络对象或组，而且它可以包含主机、范围或子网。如果要转换所有原始源流量，可以跳过此步骤并在规则中指定**任何**。

- **转换后的源地址** - 可以通过以下选项指定转换后的地址：

  - **目标接口** - 要使用目标接口 IPv4 地址，不需要网络对象。该选项配置具有端口转换的静态接口 NAT：源地址/端口转换为接口的地址和相同的端口号。您不能将接口 PAT 用于 IPv6。

  - **地址** - 创建包含主机、范围或子网的网络对象或组。组不能同时包含 IPv4 和 IPv6 地址；其只能包含一种类型。通常，配置相同数量的映射地址和实际地址，以便进行一对一映射。然而，地址数量可以不匹配。

如果您要在规则中为**原始目标地址**和**转换后的目标地址**配置静态转换，还可以为这些地址创建网络对象。如果只需要配置支持端口转换的目标静态接口 NAT，则可以跳过为目标映射地址添加对象的过程，并在规则中指定接口。

您还可以对源和/或目标执行端口转换。在对象管理器中，确保有可以用于原始端口和转换后的端口的端口对象。

过程

步骤 1 依次选择**策略** > **NAT**。

步骤 2 执行以下操作之一：

- 要创建新规则，请点击 **+** 按钮。
- 要编辑现有规则，请点击规则的编辑图标 ( )。

（要删除不再需要的规则，请点击该规则的垃圾桶图标。）

步骤 3 配置基本规则选项：

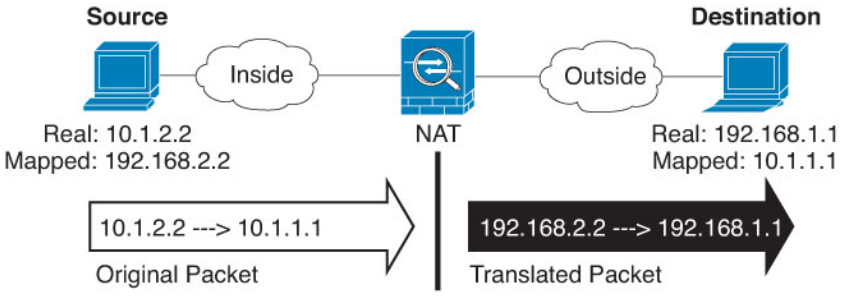
- **标题** - 为规则输入名称。
- **创建规则用于** - 选择**手动 NAT**。
- **规则位置** - 要添加规则的位置。可以将其插入类别中（在自动 NAT 规则之前或之后），或者所选规则的上方或下方。
- **类型** - 选择**静态**。该设置仅应用于源地址。如果为目标地址定义转换，则该转换始终为静态。

步骤 4 配置以下接口选项：

- **源接口**、**目标接口** -（网桥组成员接口的必选项。）应用此 NAT 规则的接口。**源**是实际接口，流量通过该接口进入设备。**目标**是映射接口，流量通过该接口离开设备。默认情况下，此规则应用于除网桥组成员接口之外的所有接口（**任意**）。

步骤 5 确定原始数据包地址（IPv4 或 IPv6 地址）；例如，显示在原始数据包中的数据包地址。

请参阅下图，了解原始数据包与转换后数据包的示例。



- **原始源地址** - 包含将要转换的地址的网络对象或组。
- **原始目标地址** -（可选。）包含目的目标地址的网络对象。如果将此留空，则无论目的目标为何都将应用源地址转换。如果指定目标目的地址，可以为该地址配置静态转换或只是为其使用将身份 NAT 用于该地址。

可以依次选择**接口**以使原始目标基于源接口（不能为“任意”）。如果选择此选项，则还必须选择一个已转换后的目的目标对象。要为目的目标地址实施带端口转换的静态接口 NAT，请选择此选项，并为目的目标端口选择适当的端口对象。

步骤 6 确定已转换的数据包地址（IPv4 或 IPv6 地址）；例如，显示在目标接口网络中的数据包地址。如果需要，可在 IPv4 与 IPv6 之间进行转换。

- **转换后的源地址** - 以下项之一：
  - 要使用一组地址，请选择包含映射地址的网络对象或组。通常，配置相同数量的映射地址和实际地址，以便进行一对一映射。然而，地址数量可以不匹配。
  - （具有端口转换的静态接口 NAT。）要使用目标接口的 IPv4 地址，请选择**接口**。您还必须选择具体的目标接口，该接口不能是网桥组成员接口。该选项配置具有端口转换的静态接口 NAT：源地址/端口转换为接口的地址和相同的端口号。您不能将接口 PAT 用于 IPv6。
- **转换后的目标地址** -（可选。）包含已转换的数据包中使用的目标地址的网络对象或组。如果为**原始目标**选择了一个对象，则可以通过选择相同的对象确定 NAT（即无转换）。

步骤 7 （可选。）为服务转换确定源或目的服务端口。

如果要配置支持端口转换的静态 NAT，可以为源和/或目的转换端口。例如，可以在 TCP/80 和 TCP/8080 之间进行转换。

NAT 仅支持 TCP 或 UDP。转换端口时，请确保实际和映射服务对象中的协议相同（同为 TCP 或同为 UDP）。对于身份 NAT，可将相同的服务对象同时用于实际和映射端口。

- **原始源端口**、**转换后的源端口** - 定义源地址的端口转换。
- **原始目标端口**、**转换后的目标端口** - 定义目标地址的端口转换。

步骤 8 （可选。）点击**高级选项**链接并选择所需的选项：

- **转换与此规则相匹配的 DNS 回复** - 是否转换 DNS 应答中的 IP 地址。对于从映射接口传输到实际接口的 DNS 回复，地址（IPv4 A 或 IPv6 AAAA）记录会从映射值重写为实际值。相反，对于从实际接口传输到映射接口的 DNS 回复，该记录会从实际值重写为映射值。此选项用于特定情况，有时 NAT64/46 转换（其中重写也会在 A 和 AAAA 记录之间转换）需要使用此选项。有关详细信息，请参阅使用 NAT 重写 DNS 查询和响应，第 72 页。 如果您在进行端口转换，则此选项不可用。
- **不在目标接口上使用代理 ARP** - 为映射 IP 地址的传入数据包禁用代理 ARP。如果使用与映射接口相同的网络中的地址，则系统会使用代理 ARP 来应答映射地址的任何 ARP 请求，从而拦截以映射地址为目的地的流量。此解决方案可以简化路由，因为设备不必是任何其他网络的网关。如果需要，可以禁用代理 ARP，在此情况下需要确保在上游路由器上具有正确的路由。通常，对于身份 NAT，是不需要代理 ARP 的，而且在某些情况下，会造成连接问题。

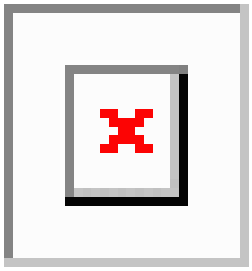
步骤 9 点击**确定 (OK)**。

身份 NAT

可能有一个 NAT 配置，在其中需要将 IP 地址转换为其本身。例如，如果创建一条将 NAT 应用于每个网络的大体的规则，但想使一个网络免于 NAT，则可以创建一条静态 NAT 规则，以将地址转换为其本身。

下图显示典型的身份 NAT 场景。

图 *12: 身份 NAT*



以下主题介绍如何配置身份 NAT。

配置身份自动 NAT

使用静态身份自动 NAT 规则可防止地址转换。即，防止将地址转换为自身。

开始之前

选择**对象**并创建规则中所需的网络对象或组。或者，您可以在定义NAT规则时创建对象。对象必须满足以下要求：

- **原始地址** - 该地址必须是网络对象（而非组），而且它可以是主机、范围或子网。
- **转换后的地址** - 其内容与原始源对象完全相同的网络对象或组。您可以使用相同的对象。

过程

步骤 1 依次选择**策略** > **NAT**。

步骤 2 执行以下操作之一：

- 要创建新规则，请点击 + 按钮。
- 要编辑现有规则，请点击规则的编辑图标 ( )。

（要删除不再需要的规则，请点击该规则的垃圾桶图标。）

步骤 3 配置基本规则选项：

- **标题** - 为规则输入名称。
- **创建规则用于** - 选择**自动 NAT**。
- **类型** - 选择**静态**。

步骤 4 配置以下数据包转换选项：

- **源接口、目标接口** -（网桥组成员接口的必选项。）应用此 NAT 规则的接口。**源**是实际接口，流量通过该接口进入设备。**目标**是映射接口，流量通过该接口离开设备。默认情况下，此规则应用于除网桥组成员接口之外的所有接口（**任意**）。
- **原始地址** - 包含您要转换的地址的网络对象。
- **转换后的地址** - 与原始源相同的对象。或者，您可以选择内容完全相同的其他对象。

不要为身份 NAT 配置**原始端口**和**转换后的端口**选项。

步骤 5 （可选。）点击**高级选项**链接并选择所需的选项：

- **转换与此规则匹配的 DNS 回复** - 请勿为身份 NAT 配置此选项。
- **不在目标接口上使用代理 ARP** - 为映射 IP 地址的传入数据包禁用代理 ARP。如果使用与映射接口相同的网络中的地址，则系统会使用代理 ARP 来应答映射地址的任何 ARP 请求，从而拦截以映射地址为目的地的流量。此解决方案可以简化路由，因为设备不必是任何其他网络的网关。如果需要，可以禁用代理 ARP，在此情况下需要确保在上游路由器上具有正确的路由。通常，对于身份 NAT，是不需要代理 ARP 的，而且在某些情况下，会造成连接问题。
- **对目标接口执行路由查找** - 如果在为原始源地址和已转换源地址选择同一对象时选择源接口和目标接口，则可以选择此选项，以使系统根据路由表而不是使用在NAT规则中配置的目标接口来确定目标接口。

步骤 6 点击**确定 (OK)**。

配置身份手动 NAT

当自动 NAT 不能满足您的需求时，请使用静态身份手动 NAT 规则。例如，如果您要根据目标进行不同的转换。使用静态身份 NAT 规则可防止地址转换。即，防止将地址转换为自身。

开始之前

选择**对象**并创建规则中所需的网络对象或组。组不能同时包含 IPv4 和 IPv6 地址；只能包含一种类型。或者，您可以在定义 NAT 规则时创建对象。对象还必须满足以下要求：

- **原始源地址** - 地址可以是网络对象或组，而且它可以包含主机、范围或子网。如果要转换所有原始源流量，可以跳过此步骤并在规则中指定**任何**。
- **转换后的源地址** - 与原始源相同的对象。或者，您可以选择内容完全相同的其他对象。

如果您要在规则中为**原始目标地址**和**转换后的目标地址**配置静态转换，还可以为这些地址创建网络对象。如果只需要配置支持端口转换的目标静态接口 NAT，则可以跳过为目标映射地址添加对象的过程，并在规则中指定接口。

您还可以对源和/或目标执行端口转换。在对象管理器中，确保有可以用于原始端口和转换后的端口的端口对象。您可以为身份 NAT 使用相同的对象。

过程

步骤 1 依次选择**策略** > **NAT**。

步骤 2 执行以下操作之一：

- 要创建新规则，请点击 + 按钮。
- 要编辑现有规则，请点击规则的编辑图标 ( )。

（要删除不再需要的规则，请点击该规则的垃圾桶图标。）

步骤 3 配置基本规则选项：

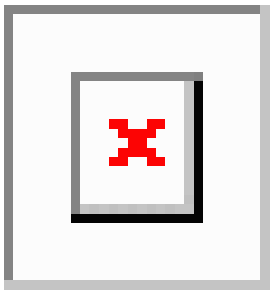
- **标题** - 为规则输入名称。
- **创建规则用于** - 选择**手动 NAT**。
- **规则位置** - 要添加规则的位置。可以将其插入类别中（在自动 NAT 规则之前或之后），或者所选规则的上方或下方。
- **类型** - 选择**静态**。该设置仅应用于源地址。如果为目标地址定义转换，则该转换始终为静态。

步骤 4 配置以下接口选项：

- **源接口**、**目标接口** -（网桥组成员接口的必选项。）应用此 NAT 规则的接口。**源**是实际接口，流量通过该接口进入设备。**目标**是映射接口，流量通过该接口离开设备。默认情况下，此规则应用于除网桥组成员接口之外的所有接口（**任意**）。

步骤 5 确定原始数据包地址（IPv4 或 IPv6 地址）；例如，显示在原始数据包中的数据包地址。

请参阅下图，了解原始数据包与转换后数据包的示例，其中在内部主机上执行身份 NAT，但转换外部主机。



- **原始源地址** - 包含将要转换的地址的网络对象或组。
- **原始目标地址** -（可选。）包含目的目标地址的网络对象。如果将此留空，则无论目的目标为何都将应用源地址转换。如果指定目标目的地址，可以为该地址配置静态转换或只是为其使用将身份 NAT 用于该地址。

  您可以选择**接口**以使原始目标基于源接口（不能为“任何”）。如果选择此选项，则还必须选择一个已转换后的目的目标对象。要为目的目标地址实施带端口转换的静态接口 NAT，请选择此选项，并为目的目标端口选择适当的端口对象。

步骤 6 确定已转换的数据包地址（IPv4 或 IPv6 地址）；例如，显示在目标接口网络中的数据包地址。如果需要，可在 IPv4 与 IPv6 之间进行转换。

- **转换后的源地址** - 与原始源相同的对象。或者，您可以选择内容完全相同的其他对象。
- **转换后的目标地址** -（可选。）包含已转换的数据包中使用的目标地址的网络对象或组。如果为**原始目标地址**选择了一个对象，则可以通过选择相同的对象设置身份 NAT（即无转换）。

步骤 7 （可选。）为服务转换确定源或目的服务端口。

如果要配置支持端口转换的静态 NAT，可以为源和/或目的转换端口。例如，可以在 TCP/80 和 TCP/8080 之间进行转换。

NAT 仅支持 TCP 或 UDP。转换端口时，请确保实际和映射服务对象中的协议相同（同为 TCP 或同为 UDP）。对于身份 NAT，可将相同的服务对象同时用于实际和映射端口。

- **原始源端口、转换后的源端口** - 定义源地址的端口转换。
- **原始目标端口、转换后的目标端口** - 定义目标地址的端口转换。

步骤 8 （可选。）点击**高级选项**链接并选择所需的选项：

- **转换与此规则匹配的 DNS 回复** - 请勿为身份 NAT 配置此选项。
- **不在目标接口上使用代理 ARP** - 为映射 IP 地址的传入数据包禁用代理 ARP。如果使用与映射接口相同的网络中的地址，则系统会使用代理 ARP 来应答映射地址的任何 ARP 请求，从而拦截以映射地址为目的地的流量。此解决方案可以简化路由，因为设备不必是任何其他网络的网关。如果需要，可以禁用代理 ARP，在此情况下需要确保在上游路由器上具有正确的路由。通常，对于身份 NAT，是不需要代理 ARP 的，而且在某些情况下，会造成连接问题。
- **对目标接口执行路由查找** - 如果在为原始源地址和已转换源地址选择同一对象时选择源接口和目标接口，则可以选择此选项，以使系统根据路由表而不是使用在 NAT 规则中配置的目标接口来确定目标接口。

步骤 9 点击**确定 (OK)**。

威胁防御 的 NAT 规则属性

使用网络地址转换 (NAT) 规则将 IP 地址转换为其他 IP 地址。通常使用 NAT 规则将私有地址转换为可公开路由的地址。该转换可以是从一个地址到另一个地址，或者您可以使用端口地址转换 (PAT) 将许多地址转换为一个地址，并且使用端口号区分源地址。

NAT 规则包括以下基本属性。自动 NAT 和手动 NAT 规则的属性相同，除非另行指明。

标题

为规则输入名称。名称不能包含空格。

创建规则用于

转换规则是**自动 NAT** 还是**手动 NAT**。自动 NAT 比手动 NAT 简单，但是手动 NAT 允许根据目标地址为源地址创建单独的转换。

状态

您希望该规则有效还是被禁用。

位置（仅手动 NAT。）

要添加规则的位置。可以将其插入类别中（在自动NAT规则之前或之后），或者所选规则的上方或下方。

类型

转换规则是**动态**还是**静态**。在实施PAT时，动态转换会自动从地址池中选择映射的地址或地址/端口组合。如果要精确定义映射的地址/端口，请使用静态转换。

以下主题介绍了其余的 NAT 规则属性。

自动 NAT 的数据包转换属性

使用**数据包转换**选项定义源地址和映射的转换后地址。以下属性仅适用于自动 NAT。

源接口、目标接口

（网桥组成员接口的必选项。）应用此NAT规则的接口。**源**是实际接口，流量通过该接口进入设备。**目标**是映射接口，流量通过该接口离开设备。默认情况下，此规则应用于除网桥组成员接口之外的所有接口（**任意**）。

原始地址（始终为必填项）。

包含您要转换的源地址的网络对象。该地址必须是网络对象（而非组），而且可以是主机、范围或子网。

转换后的地址（通常为必填项）。

您要转换到的映射地址。您在此处选择的选项取决于定义的转换规则类型。

- **动态 NAT** - 包含映射地址的网络对象或组。该地址可以是网络对象或组，但是它不能包含子网。组不能同时包含 IPv4 和 IPv6 地址，它只能包含一种类型的地址。 如果某个组同时包含范围和主机 IP 地址，则范围将用于动态 NAT，主机 IP 地址将用作 PAT 回退。
- **动态 PAT** - 以下项之一：
  - （接口 PAT。）要使用目标接口的 IPv4 地址，请选择**接口**。您还必须选择具体的目标接口，该接口不能是网桥组成员接口。您不能将接口 PAT 用于 IPv6。
  - 要使用目标接口地址以外的单个地址，请选择为此用途创建的主机网络对象。
- **静态 NAT** - 以下项之一：
  - 要使用一组地址，请选择包含映射地址的网络对象或组。该对象或组可以包含主机、范围或子网。通常，配置相同数量的映射地址和实际地址，以便进行一对一映射。然而，地址数量可以不匹配。
  - （具有端口转换的静态接口 NAT。）要使用目标接口的地址，请选择**接口**。您还必须选择具体的目标接口，该接口不能是网桥组成员接口。该选项配置具有端口转换的静

态接口 NAT：源地址/端口转换为接口的地址和相同的端口号。您不能将接口 PAT 用于 IPv6。

- **身份 NAT** - 与原始源相同的对象。或者，您可以选择内容完全相同的其他对象。

原始端口、转换后的端口（仅静态 NAT）。

如果需要转换 TCP 或 UDP 端口，请选择定义原始端口和转换后的端口的端口对象。对象必须用于相同的协议。例如，如有必要，可以将 TCP/80 转换为 TCP/8080。

手动 NAT 的数据包转换属性

使用**数据包转换**选项定义源地址和映射的转换后地址。以下属性仅适用于手动 NAT。所有选项均为可选，除非另行指明。

源接口、目标接口

（网桥组成员接口的必选项。）应用此NAT规则的接口。**源**是实际接口，流量通过该接口进入设备。**目标**是映射接口，流量通过该接口离开设备。默认情况下，此规则应用于除网桥组成员接口之外的所有接口（**任意**）。

原始源地址（始终为必填项）。

包含您要转换的地址的网络对象或组。该地址可以是网络对象或组，而且它可以包含主机、范围或子网。如果要转换所有原始源流量，可以在规则中指定**任何**。

转换后的源地址（通常为必填项。）

您要转换到的映射地址。您在此处选择的选项取决于定义的转换规则类型。

- **动态 NAT** - 包含映射地址的网络对象或组。该地址可以是网络对象或组，但是它不能包含子网。组不能同时包含 IPv4 和 IPv6 地址，它只能包含一种类型的地址。 如果某个组同时包含范围和主机 IP 地址，则范围将用于动态 NAT，主机 IP 地址将用作 PAT 回退。
- **动态 PAT** - 以下项之一：
  - （接口PAT。）要使用目标接口的地址，请选择**接口**。您还必须选择具体的目标接口，该接口不能是网桥组成员接口。您不能将接口 PAT 用于 IPv6。
  - 要使用目标接口地址以外的单个地址，请选择为此用途创建的主机网络对象。
- **静态 NAT** - 以下项之一：
  - 要使用一组地址，请选择包含映射地址的网络对象或组。该对象或组可以包含主机、范围或子网。通常，配置相同数量的映射地址和实际地址，以便进行一对一映射。然而，地址数量可以不匹配。
  - （具有端口转换的静态接口 NAT。）要使用目标接口的地址，请选择**接口**。您还必须选择具体的目标接口，该接口不能是网桥组成员接口。该选项配置具有端口转换的静态接口 NAT：源地址/端口转换为接口的地址和相同的端口号。您不能将接口 PAT 用于 IPv6。

- **身份 NAT** - 与原始源相同的对象。或者，您可以选择内容完全相同的其他对象。

原始目标地址

包含目的目标地址的网络对象。如果将此留空，则无论目的目标为何都将应用源地址转换。如果指定目标目的地址，可以为该地址配置静态转换或只是为其使用将身份 NAT 用于该地址。

您可以选择**接口**以使原始目标基于源接口（不能为“任何”）。如果选择此选项，则还必须选择一个已转换后的目的目标对象。要为目的目标地址实施带端口转换的静态接口 NAT，请选择此选项，并为目的目标端口选择适当的端口对象。

转换后的目标地址

包含已转换的数据包中使用的目标地址的网络对象或组。如果为**原始目标**选择了一个对象，则可以通过选择相同的对象确定 NAT（即无转换）。

您可以使用指定完全限定域名作为转换目的的网络对象；有关更多信息，请参阅FQDN 目的准则，第 11 页。

原始源端口、转换后的源端口、原始目标端口、转换后的目标端口

为原始和转换后的数据包定义源和目标服务的端口对象。您可以转换端口，或者选择同一对象以便在没有转换端口的情况下使规则敏感察觉到该服务。在配置服务时请记住以下规则：

- （动态 NAT 或 PAT。）不能对**原始源端口**和**转换后的源端口**进行转换。您可以仅对目标端口进行转换。
- NAT 仅支持 TCP 或 UDP。转换端口时，请确保实际和映射服务对象中的协议相同（同为 TCP 或同为 UDP）。对于身份 NAT，您可以将同一对象用于实际端口和映射端口。

高级 NAT 属性

在配置NAT时，可以在**高级**选项中配置提供专业化服务的属性。所有这些属性都是可选的：仅当需要服务时才对其进行配置。

转换与此规则匹配的 DNS 回复

是否转换 DNS 应答中的 IP 地址。对于从映射接口传输到实际接口的 DNS 回复，地址（IPv4 A 或IPv6 AAAA）记录会从映射值重写为实际值。相反，对于从实际接口传输到映射接口的DNS回复，该记录会从实际值重写为映射值。此选项用于特定情况，有时 NAT64/46 转换（其中重写也会在 A 和 AAAA 记录之间转换）需要使用此选项。有关详细信息，请参阅使用 NAT 重写 DNS 查询和响应，第 72 页。 如果在静态 NAT 规则中进行端口转换，则此选项不可用。

贯穿到接口 PAT（目标接口）（仅动态 NAT。）

当已分配其他映射地址后，是否将目标接口的 IP 地址用作备份方法（接口 PAT 回退）。仅当您选择不是网桥组成员的目的地接口时，此选项才可用。如果已配置了接口 PAT 配置作为转换的地址，则不能选择此选项。您不能将此选项用于 IPv6 网络。

不在目标接口上使用代理 ARP（仅静态 NAT。）

为映射IP地址的传入数据包禁用代理ARP。如果使用与映射接口相同的网络中的地址，则系统会使用代理 ARP 来应答映射地址的任何 ARP 请求，从而拦截以映射地址为目的地的流量。此解决方案可以简化路由，因为设备不必是任何其他网络的网关。如果需要，可以禁用代理ARP，

在此情况下需要确保在上游路由器上具有正确的路由。通常，对于身份 NAT，是不需要代理 ARP 的，而且在某些情况下，会造成连接问题。

对目标接口执行路由查找（仅静态身份 NAT。仅路由模式。）

如果在为原始源地址和已转换源地址选择同一对象时选择源接口和目标接口，则可以选择此选项，以使系统根据路由表而不是使用在 NAT 规则中配置的目标接口来确定目标接口。

转换 IPv6 网络

当需要在仅 IPv6 网络和仅 IPv4 网络之间传递流量时，需要使用 NAT 在地址类型之间进行转换。即使两个都是 IPv6 网络，您也可能需要对外部网络隐藏内部地址。

对于 IPv6 网络，您可以使用以下转换类型：

- NAT64、NAT46 - 将 IPv6 数据包转换成 IPv4 数据包，反之亦然。您需要定义两个策略，一个用于 IPv6 向 IPv4 的转换，另一个用于 IPv4 向 IPv6 的转换。虽然您可以使用单一 手动 NAT 规则完成此任务，但如果 DNS 服务器位于外部网络，则可能需要重写 DNS 响应。由于在指定了目标的情况下，无法在手动 NAT 规则中启用 DNS 重写，所以最好创建两个自动 NAT 规则。

注释 NAT46 仅支持静态映射。

- NAT66 - 将 IPv6 数据包转换为不同的 IPv6 地址。我们建议使用静态 NAT。尽管可以使用 NAT 或 PAT，但由于 IPv6 地址大量供应，因此不必使用动态 NAT。

注释 NAT64 和 NAT 46 仅可以在标准路由接口上使用。NAT66 可在路由接口和网桥组成员接口上使用。

NAT64/46：将 IPv6 地址转换为 IPv4 地址

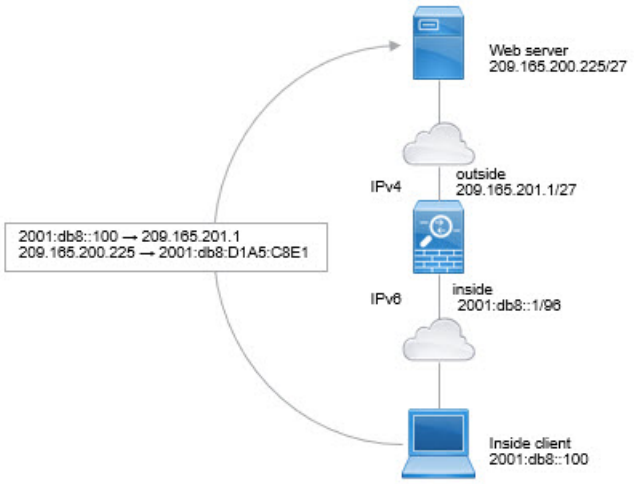
当流量从 IPv6 网络进入仅 IPv4 网络时，您需要将 IPv6 地址转换为 IPv4 地址，并将流量从 Ipv4 返回 IPv6。您需要定义两个地址池，一个 IPv4 地址池用于绑定 IPv4 网络中的 IPv6 地址，另一个 IPv6 地址池用于绑定 IPv6 网络中的 IPv4 地址。

- NAT64 规则的 IPv4 地址池一般较小，通常可能没有足够的地址与 IPv6 客户端地址一对一映射。与动态或静态 NAT 相比，动态 PAT 可以更容易满足可能的大量 IPv6 客户端地址需要。
- NAT46 规则的 IPv6 地址池可以等于或大于要映射的 IPv4 地址数。这允许每个 IPv4 地址映射到不同的 IPv6 地址。NAT46 仅支持静态映射，因此您不能使用动态 PAT。

您需要定义两个策略，一个用于源 IPv6 网络，一个用于目标 IPv4 网络。虽然您可以使用单一 手动 NAT 规则完成此任务，但如果 DNS 服务器位于外部网络，则可能需要重写 DNS 响应。由于在指定了目标的情况下，无法在手动 NAT 规则中启用 DNS 重写，所以最好创建两个自动 NAT 规则。

NAT64/46 示例：内部 IPv6 网络与外部 IPv4 互联网

以下是一个非常简单的示例，假设您具有仅包含 IPv6 的内部网络，且您希望将发送到互联网的流量转换为 IPv4。此示例假定您无需 DNS 转换，以便可以在单个手动 NAT 规则中执行 NAT64 和 NAT46 转换。



在本例中，借助外部接口的 IP 地址，使用动态接口 PAT 将内部 IPv6 网络转换为 IPv4。将外部 IPv4 流量静态转换为 2001:db8::/96 网络中的地址，允许在内部网络中传输。

过程

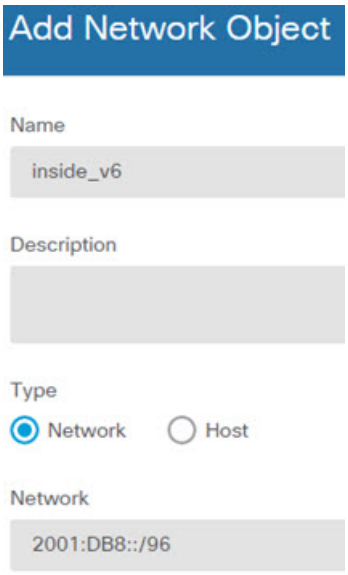
步骤 1 创建用于内部 IPv6 网络的网络对象。

a) 选择**对象**。

b) 从目录中选择**网络**，然后点击 +。

c) 定义内部 IPv6 网络。

为网络对象命名（例如，inside_v6），选择**网络**，然后输入网络地址 2001:db8::/96。



d) 点击**确定**。

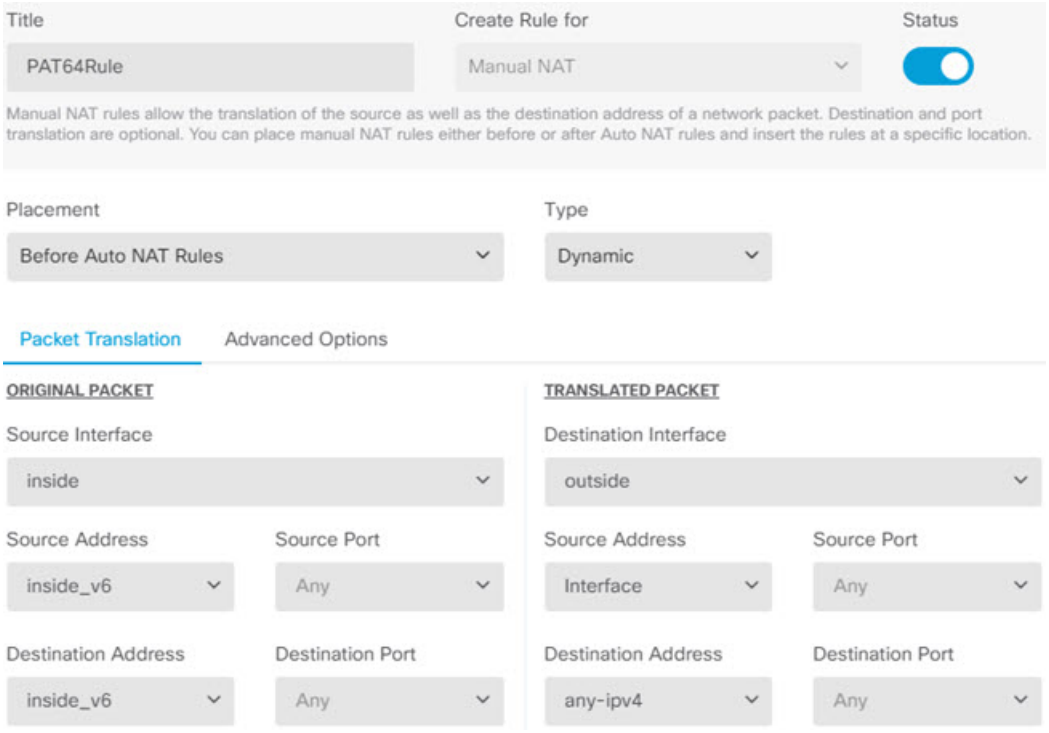
步骤 2 创建手动 NAT 规则以将 IPv6 网络转换为 IPv4 并再次返回。

a) 依次选择**策略** > **NAT**。

b) 点击 + 按钮。

c) 配置以下属性：

- **标题** = PAT64Rule（或您选择的其他名称）。
- **创建规则用于** = **手动 NAT**。
- **位置** = **自动 NAT 规则之前**
- **类型** = **动态**。
- **源接口** = 内部。
- **目标接口** = 外部。
- **原始数据包源地址** = inside_v6 网络对象。
- **转换后数据包源地址** = 接口。此选项使用目标接口的 IPv4 地址作为 PAT 地址。
- **原始数据包目标地址** = inside_v6 网络对象。
- **转换后数据包目标地址** = any-ipv4 网络对象。

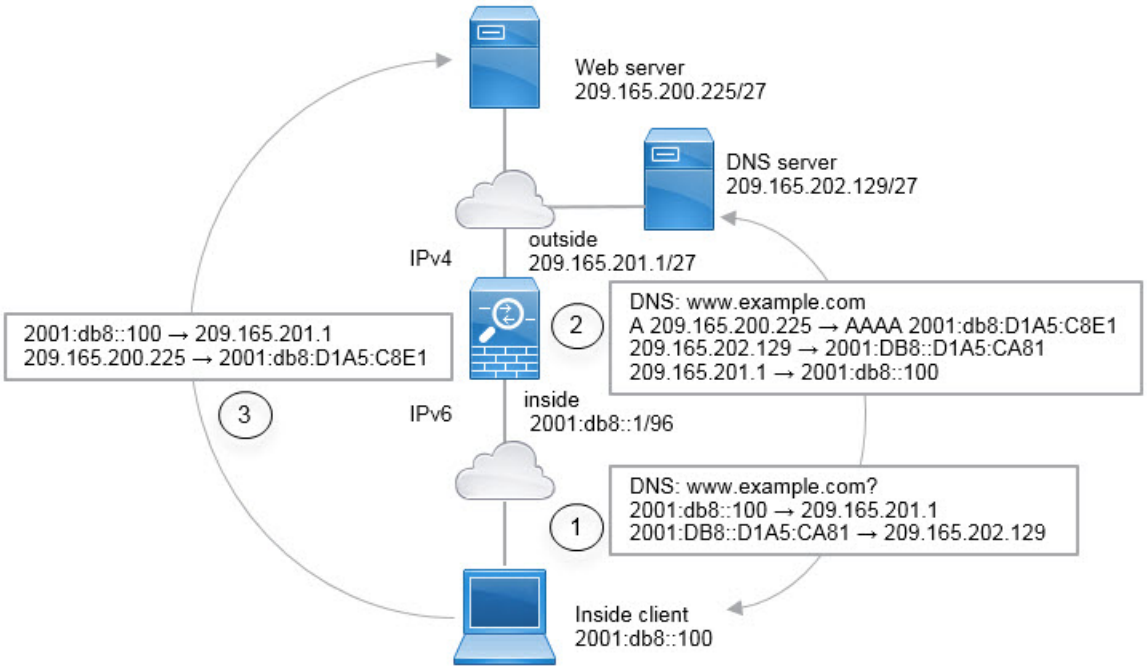


d) 点击**确定**。

使用此规则时，从内部接口上的 2001:db8::/96 子网流向外部接口的任何流量都将接受使用外部接口 IPv4 地址进行的 NAT64 PAT 转换。相反，外部网络中的任何 IPv4 地址到达内部接口，都将使用嵌入式 IPv4 地址方法转换为 2001:db8::/96 网络中的一个地址。

NAT64/46 示例：包含外部 IPv4 互联网和 DNS 转换的内部 IPv6 网络

下面是一个典型的示例：内部网络只支持 IPv6，但外部互联网上有一些内部用户所需的服务只支持 IPv4。



在本例中，借助外部接口的 IP 地址，使用动态接口 PAT 将内部 IPv6 网络转换为 IPv4。将外部 IPv4 流量静态转换为 2001:db8::/96 网络中的地址，允许在内部网络中传输。对 NAT46 规则启用 DNS 重写，使外部 DNS 服务器的回复可以从 A (IPv4) 记录转换为 AAAA (IPv6) 记录，地址也能从 IPv4 地址转换为 IPv6 地址。

当内部 IPv6 网络中地址为 2001:DB8::100 的客户端尝试打开 www.example.com 时，此 Web 请求的典型顺序如下。

1. 客户端的计算机向地址为 2001:DB8::D1A5:CA81 的 DNS 服务器发送 DNS 请求。NAT 规则对 DNS 请求中的源和目的进行以下转换：
   - 2001:DB8::100 转换为 209.165.201.1 上的唯一端口（NAT64 接口 PAT 规则。）
   - 2001:DB8::D1A5:CA81 转换为 209.165.202.129（NAT46 规则。）D1A5:CA81 是 209.165.202.129 的 IPv6 对应物。）
2. DNS 服务器以 A 记录进行响应，指出 www.example.com 位于 209.165.200.225。NAT46 规则（已启用 DNS 重写）将 A 记录转换为 IPv6 对应物 AAAA 记录，并在 AAAA 记录中将 209.165.200.225 转换为 2001:db8:D1A5:C8E1。此外，DNS 响应中的源地址和目标地址未转换：
   - 209.165.202.129 转换为 2001:DB8::D1A5:CA81
   - 209.165.201.1 转换为 2001:db8::100
3. IPv6 客户端现在有 Web 服务器的 IP 地址，于是向位于 2001:db8:D1A5:C8E1 的 www.example.com 发出 HTTP 请求。（D1A5:C8E1 是 209.165.200.225 的 IPv6 对应物。）HTTP 请求中的源和目的进行转换：
   - 2001:DB8::100 转换为 209.156.101.54 上的唯一端口（NAT64 接口 PAT 规则。）

- 2001:db8:D1A5:C8E1 转换为 209.165.200.225（NAT46 规则。）

以下步骤程序介绍了如何配置此示例。

过程

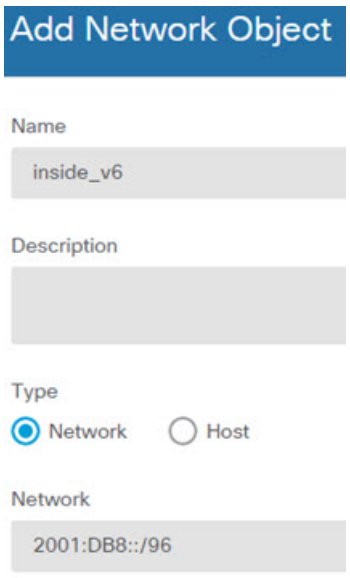
步骤 1 创建定义内部 IPv6 网络和外部 IPv4 网络的网络对象。

a) 选择**对象**。

b) 从目录中选择**网络**，然后点击 +。

c) 定义内部 IPv6 网络。

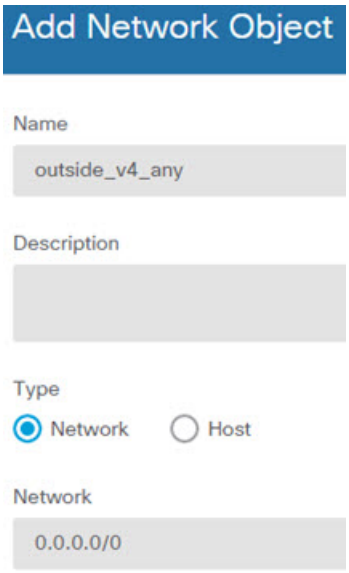
为网络对象命名（例如，inside_v6），选择**网络**，然后输入网络地址 2001:db8::/96。



d) 点击**确定**。

e) 点击 + 并定义外部 IPv4 网络。

为网络对象命名（例如，outside_v4_any），选择**网络**，然后输入网络地址 0.0.0.0/0。



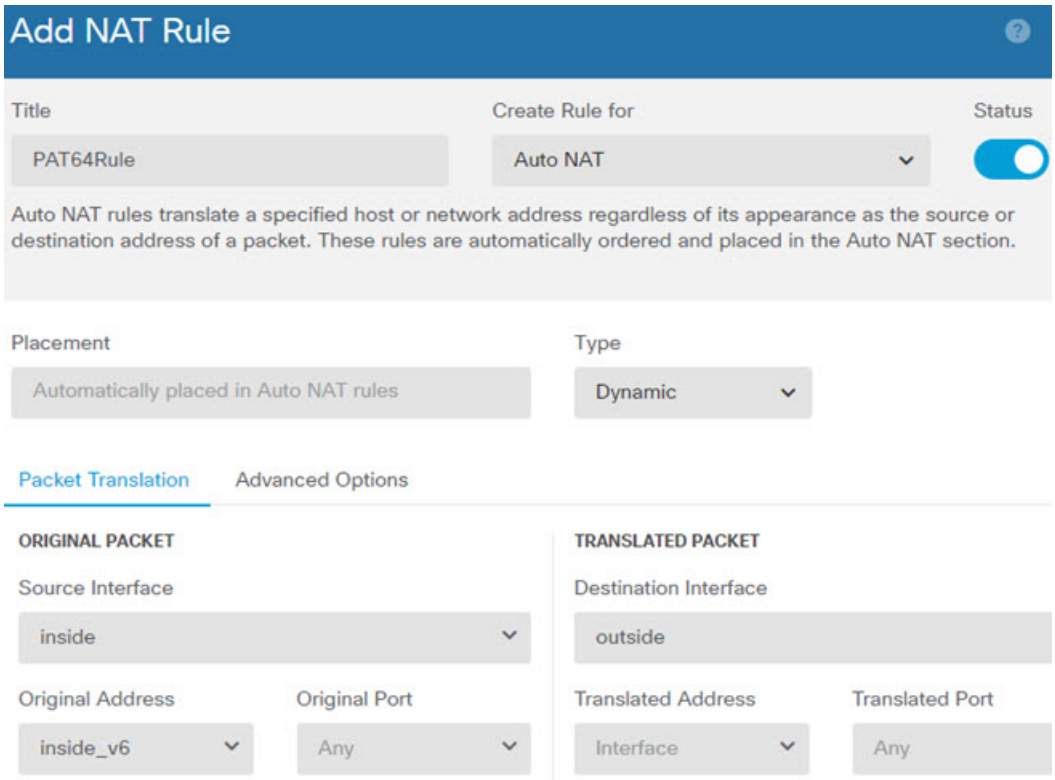
步骤 2 为内部 IPv6 网络配置 NAT64 动态 PAT 规则。

a) 依次选择**策略** > **NAT**。

b) 点击 + 按钮。

c) 配置以下属性：

- **标题** = PAT64Rule（或您选择的其他名称）。
- **创建规则用于** = 自动 NAT。
- **类型** = 动态。
- **源接口** = 内部。
- **目标接口** = 外部。
- **原始地址** = inside_v6 网络对象。
- **转换后的地址** = **接口**。此选项使用目标接口的 IPv4 地址作为 PAT 地址。



d) 点击**确定**。

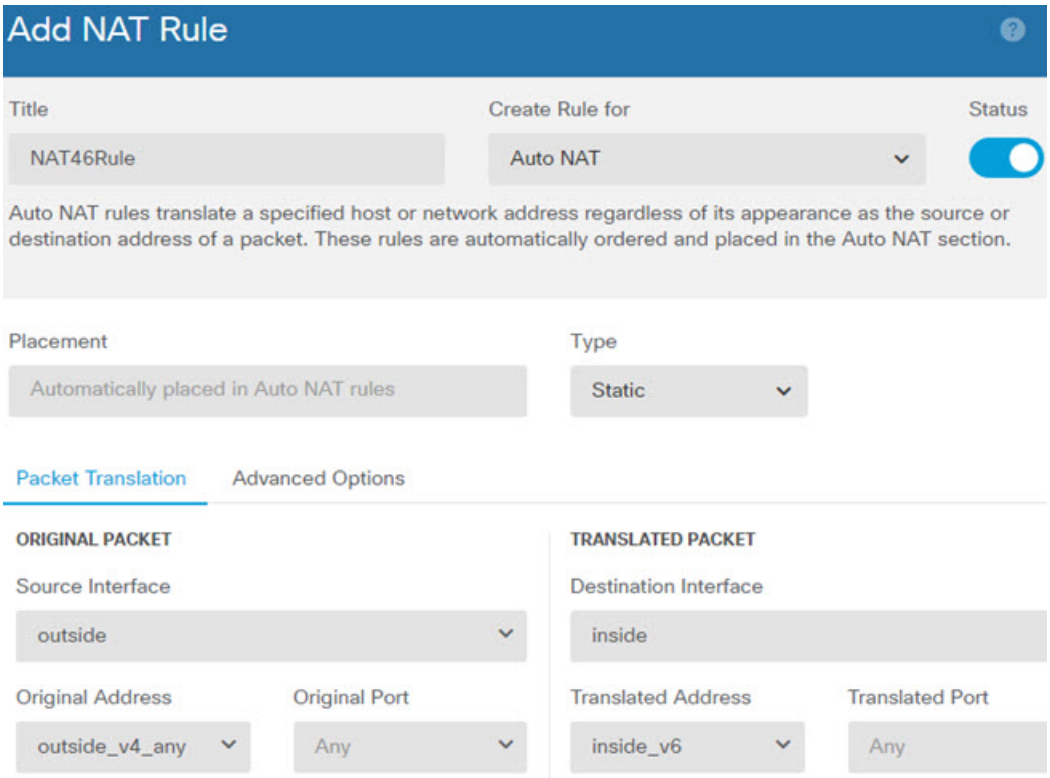
使用此规则时，从内部接口上的 2001:db8::/96 子网流向外部接口的任何流量都将接受使用外部接口 IPv4 地址进行的 NAT64 PAT 转换。

步骤 3 为外部 IPv4 网络配置静态 NAT46 规则。

a) 点击 + 按钮。

b) 配置以下属性：

- **标题** = NAT46Rule（或您选择的其他名称）。
- **创建规则用于** = 自动 NAT。
- **类型** = 静态。
- **源接口** = 外部。
- **目标接口** = 内部。
- **原始地址** = outside_v4_any 网络对象。
- **转换后的地址** = inside_v6 网络对象。
- 在**高级选项**选项卡中，选择**转换与此规则匹配的 DNS 回复**。



c) 点击**确定**。

使用此规则时，外部网络中的任何 IPv4 地址到达内部接口，都将使用嵌入式 IPv4 地址方法转换为 2001:db8::/96 网络中的一个地址。此外，DNS 响应从 A (IPv4) 记录转换为 AAAA (IPv6) 记录，其地址也从 IPv4 地址转换为 IPv6 地址。

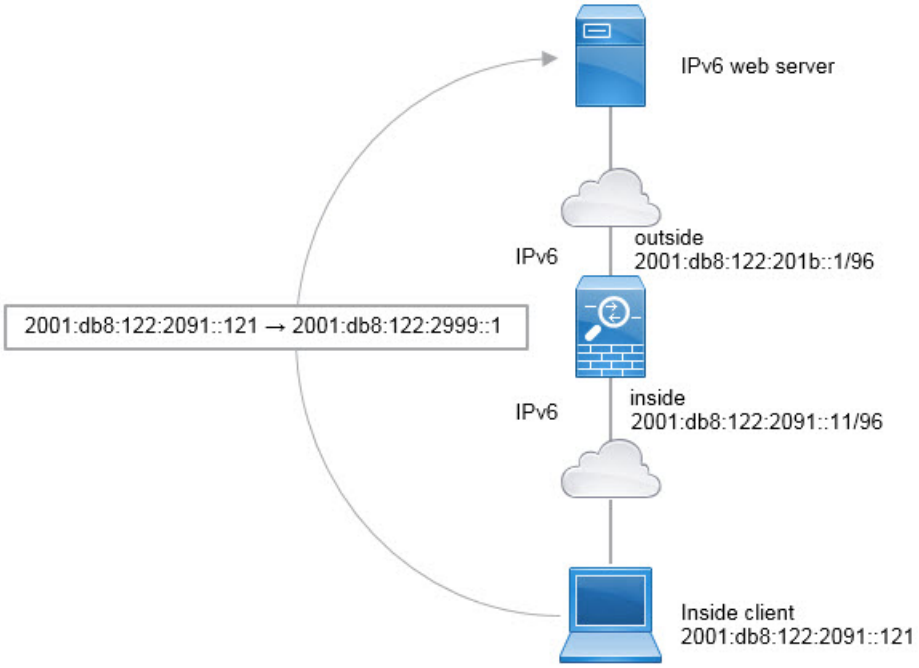
NAT66：将 IPv6 地址转换为不同的 IPv6 地址

当从一个 IPv6 网络进入另一个 IPv6 网络时，您可以将地址转换为外部网络上的不同 IPv6 地址。我们建议使用静态 NAT。尽管可以使用 NAT 或 PAT，但由于 IPv6 地址大量供应，因此不必使用动态 NAT。

因为您不是在不同的地址类型之间转换，所以您需要一个单一的 NAT66 转换规则。使用自动 NAT 可轻松地为这些规则建模。但是，如果不想允许返回流量，您可以仅使用手动 NAT 将静态 NAT 规则设为单向。

NAT66 示例：网络间的静态转换

您可以使用自动 NAT 在 IPv6 地址池之间配置静态转换。以下示例说明如何将 2001:db8:122:2091::/96 网络中的内部地址转换为 2001:db8:122:2999::/96 网络中的外部地址。



注释 此示例假定，内部接口不是网桥组接口 (BVI)，而是标准路由接口。如果内部接口是 BVI，您需要为每个成员接口复制规则。

过程

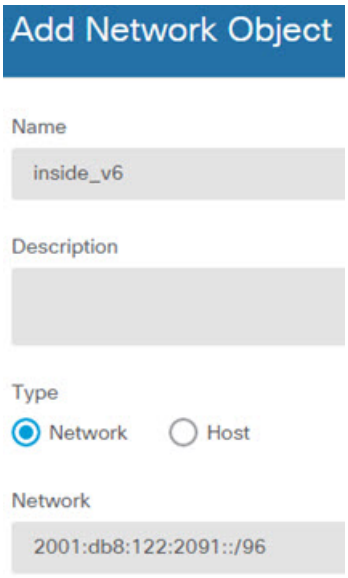
步骤 1 创建定义内部 IPv6 网络和外部 IPv6 NAT 网络的网络对象。

a) 选择**对象**。

b) 从目录中选择**网络**，然后点击 +。

c) 定义内部 IPv6 网络。

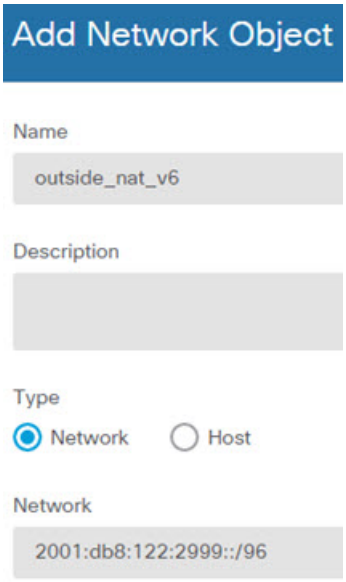
为网络对象命名（例如，inside_v6），选择**网络**，然后输入网络地址 2001:db8:122:2091::/96。



d) 点击**确定**。

e) 点击 + 并定义外部 IPv6 NAT 网络。

为网络对象命名（例如，outside_nat_v6），选择**网络**，然后输入网络地址 2001:db8:122:2999::/96。



步骤 2 为内部 IPv6 网络配置静态 NAT 规则。

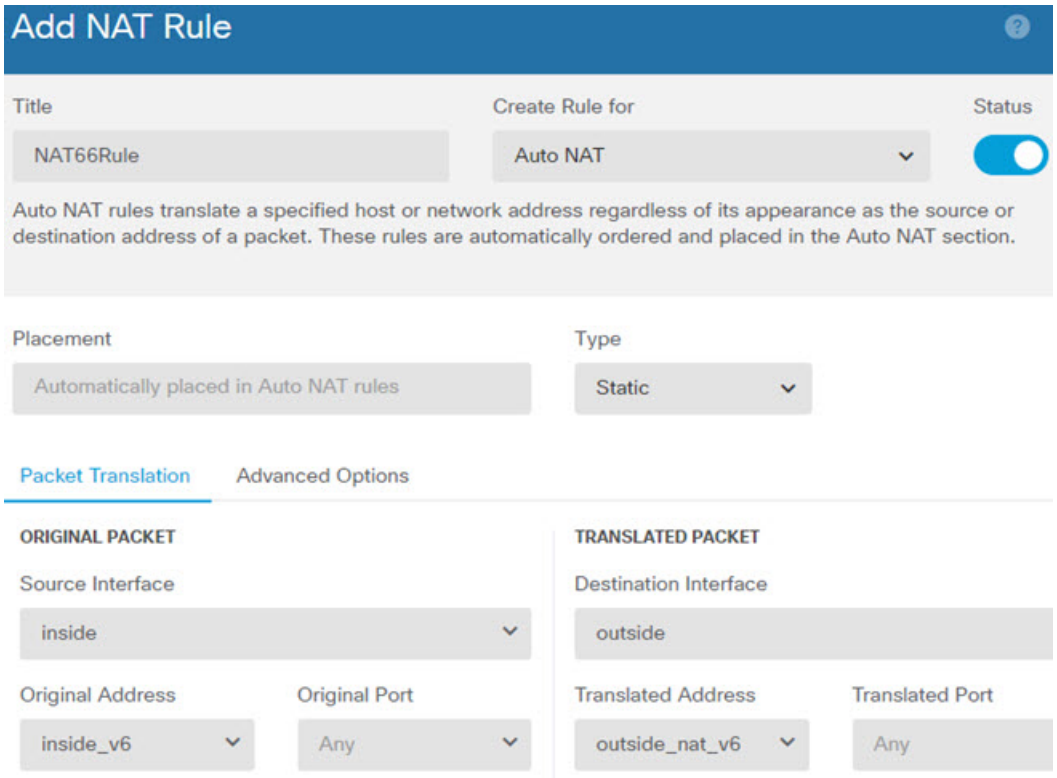
a) 依次选择**策略** > **NAT**。

b) 点击 + 按钮。

c) 配置以下属性：

- **标题** = NAT66Rule（或您选择的其他名称）。
- **创建规则用于** = 自动 NAT。

- **类型** = 静态。
- **源接口** = 内部。
- **目标接口** = 外部。
- **原始地址** = inside_v6 网络对象。
- **转换后的地址** = outside_nat_v6 网络对象。



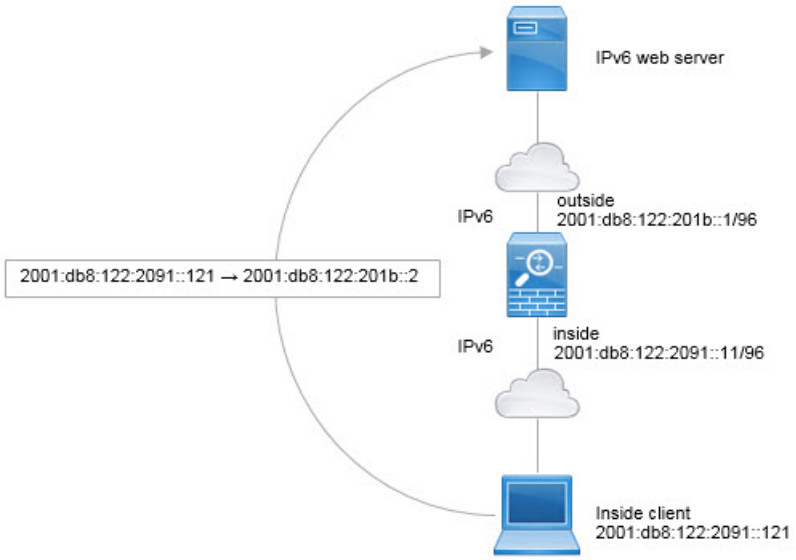
d) 点击**确定**。

使用此规则，从内部接口上的 2001:db8:122:2091::/96 子网到外部接口的任何流量都会经静态 NAT66 转换为 2001:db8:122:2999::/96 网络上的地址。

NAT66 示例：简单 IPv6 接口 PAT

实施 NAT66 的一个简单方法是将内部地址动态分配给外部接口 IPv6 地址上的不同端口。

不过，无法通过 设备管理器使用接口的 IPv6 地址配置接口 PAT。相反，要使用同一网络中的一个空闲地址作为动态 PAT 池。



注释 此示例假定，内部接口不是网桥组接口 (BVI)，而是标准路由接口。如果内部接口是 BVI，您需要为每个成员接口复制规则。

过程

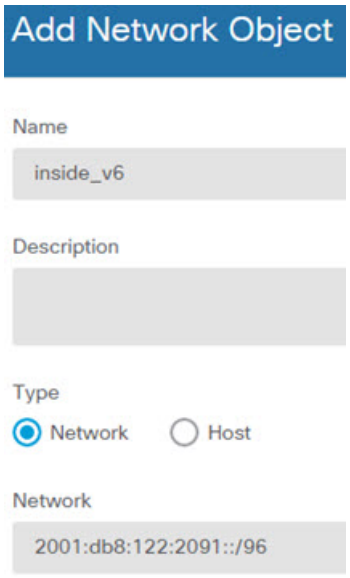
步骤 1 创建定义内部 IPv6 网络和 IPv6 PAT 地址的网络对象。

a) 选择**对象**。

b) 从目录中选择**网络**，然后点击 +。

c) 定义内部 IPv6 网络。

为网络对象命名（例如，inside_v6），选择**网络**，然后输入网络地址 2001:db8:122:2091::/96。



d) 点击**确定**。

e) 点击 + 并定义外部 IPv6 PAT 地址。

为网络对象命名（例如，ipv6_pat），选择**主机**，然后输入主机地址 2001:db8:122:201b::2。

步骤 2 为内部 IPv6 网络配置动态 PAT 规则。

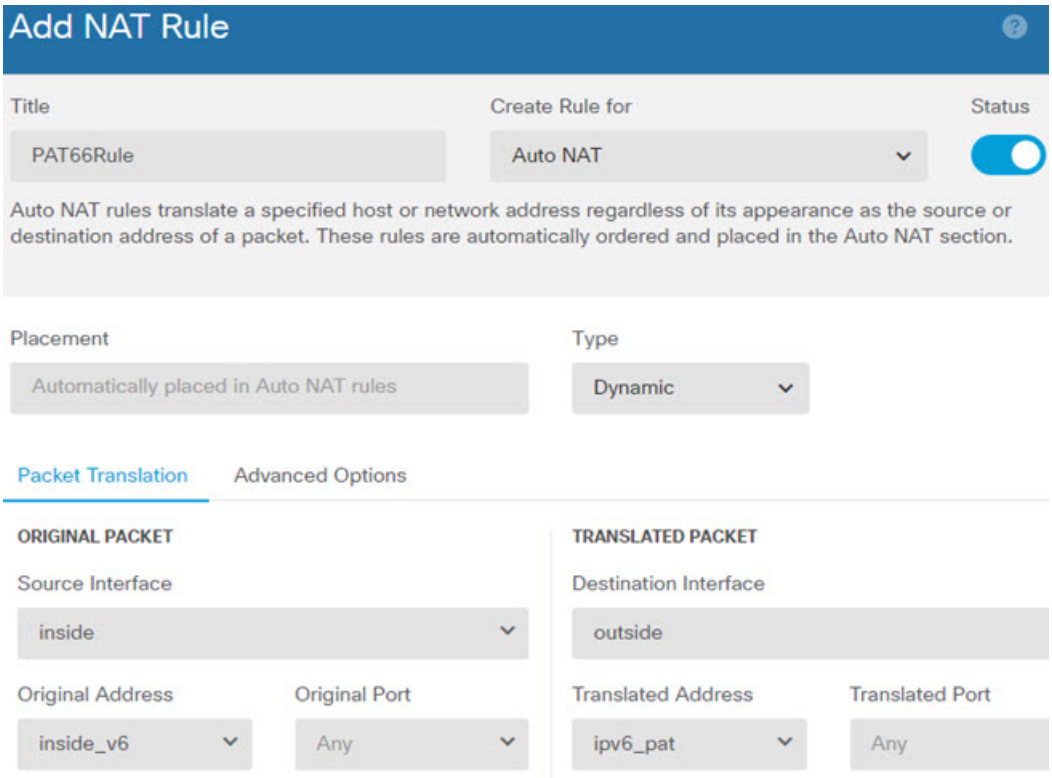
a) 依次选择**策略** > **NAT**。

b) 点击 + 按钮。

c) 配置以下属性：

- **标题** = PAT66Rule（或您选择的其他名称）。
- **创建规则用于** = 自动 NAT。

- **类型** = 动态。
- **源接口** = 内部。
- **目标接口** = 外部。
- **原始地址** = inside_v6 网络对象。
- **转换后的地址** = ipv6_pat 网络对象。



d) 点击**确定**。

使用此规则，从内部接口上的 2001:db8:122:2091::/96 子网到外部接口的任何流量都会经动态 PAT66 转换为 2001:db8:122:201b::2 上的端口。

监控 NAT

要对 NAT 连接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。

- **show nat** 显示 NAT 规则和每个规则的命中计数。还有其他关键字可用于显示 NAT 的其他方面信息。
- **show xlate** 显示当前处于活动状态的实际 NAT 转换。

- **clear xlate** 允许删除处于活动状态的 NAT 转换。如果更改 NAT 规则，您可能需要删除活动的转换，因为现有连接继续使用旧的转换槽，直到连接结束。清除转换允许系统根据您的新规则，在客户端的下一次连接尝试中为客户端构建新的转换。（您无法在CLI控制台中使用此命令。）

NAT 示例

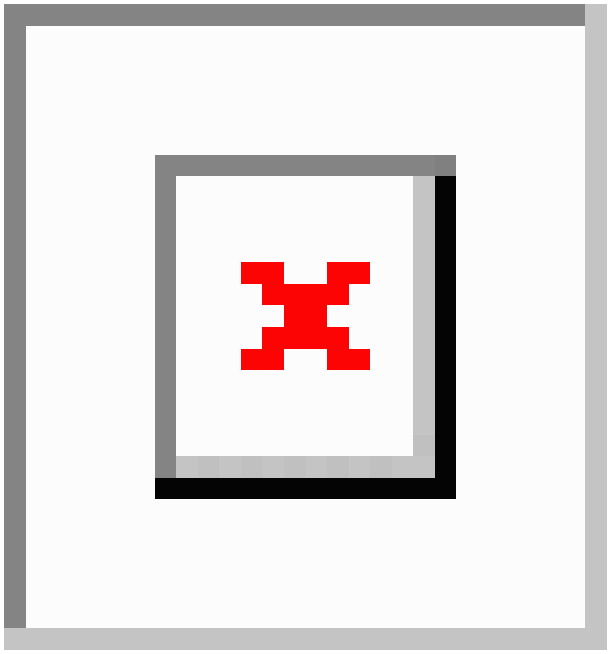
以下主题提供了在威胁防御设备上配置 NAT 的示例。

提供对内部 Web 服务器的访问权限（静态自动 NAT）

以下示例为内部 Web 服务器执行静态 NAT。实际地址位于专用网络上，因此公共地址是必需的。需要静态 NAT，以便主机能够在固定地址发起到 Web 服务器的流量。

注释 此示例假定，内部接口不是网桥组接口 (BVI)，而是标准路由接口。如果内部接口是 BVI，请选择 Web 服务器连接到的具体网桥组成员接口，例如 inside1_3。

图 *13:* 面向内部 *Web* 服务器的静态 *NAT*



过程

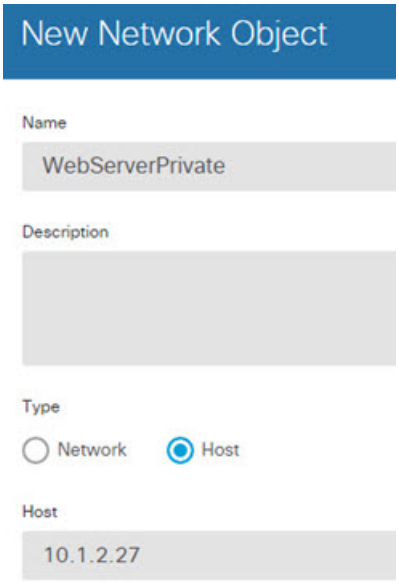
步骤 1 创建定义服务器私有和公共主机地址的网络对象。

a) 选择**对象**。

b) 从目录中选择**网络**，然后点击 +。

c) 定义 Web 服务器的私有地址。

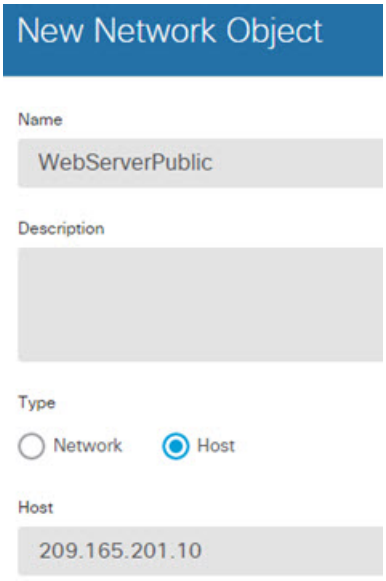
为网络对象命名（例如，WebServerPrivate)，选择**主机**，然后输入实际主机 IP 地址 10.1.2.27。



d) 点击**确定**。

e) 点击 + 并定义公共地址。

为网络对象命名（例如，WebServerPublic)，选择**主机**，然后输入实际主机地址 209.165.201.10。

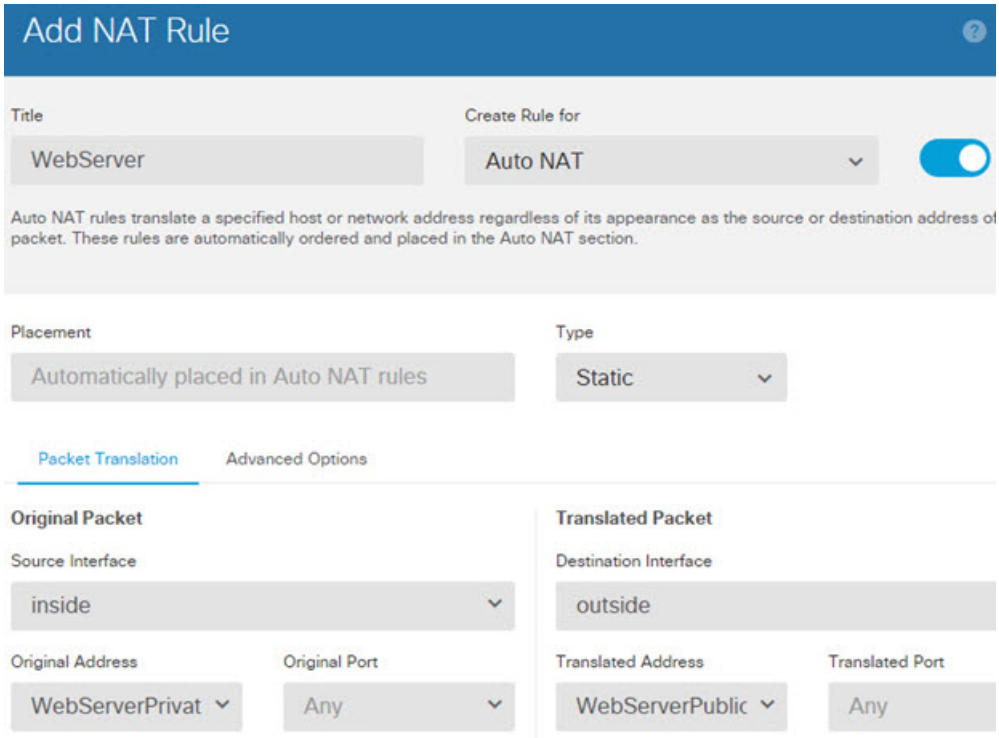


f) 点击**确定**。

步骤 2 配置对象的静态 NAT。

a) 依次选择**策略** > **NAT**。

b) 点击 + 按钮。
c) 配置以下属性：
- **标题** = WebServer（或您选择的其他名称）。
- **创建规则用于** = 自动 NAT。
- **类型** = 静态。
- **源接口** = 内部。
- **目标接口** = 外部。
- **原始地址** = WebServerPrivate 网络对象。
- **转换后的地址** = WebServerPublic 网络对象。



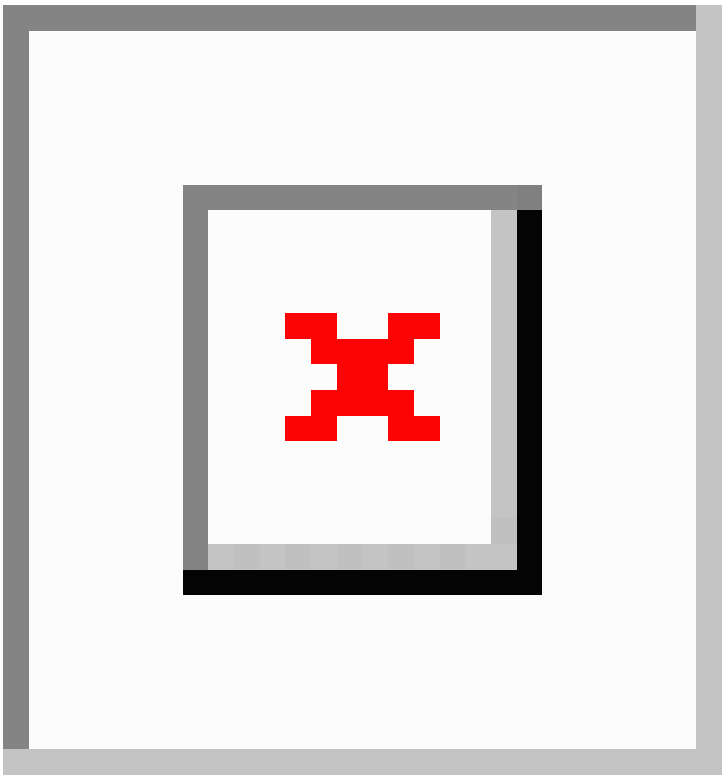
d) 点击**确定 (OK)**。

FTP、HTTP 和 SMTP 的单个地址（具有端口转换的静态自动 NAT）

以下支持端口转换的静态 NAT 示例为远程用户访问 FTP、HTTP 和 SMTP 提供单一地址。实际上，这些服务器是实际网络上的不同设备，但对于每台服务器，可以指定采用端口转换规则的静态NAT，这些规则使用同一映射 IP 地址和不同端口。

注释 此示例假设内部接口是连接到交换机的标准路由接口，其中服务器连接到交换机。如果您的内部接口是网桥组接口 (BVI)，并且服务器连接到单独的网桥组成员接口，请选择对于相应规则，每个服务器连接的特定成员接口。例如，该规则可能以 inside1_2、inside1_3 和 inside1_4 而非 inside 作为源接口。

图 *14:* 支持端口转换的静态 *NAT*



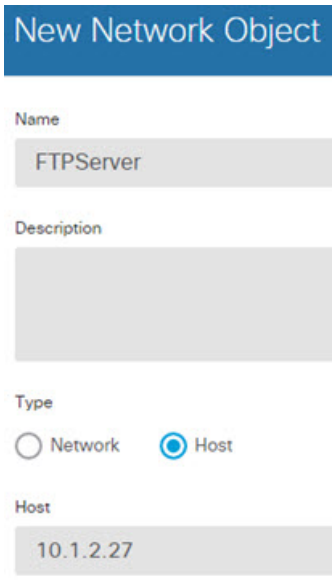
过程

步骤 1 为 FTP 服务器创建网络对象。

a) 选择**对象**。

b) 从目录中选择**网络**，然后点击 +。

c) 为网络对象命名（例如，FTPserver），选择**主机**，然后输入 FTP 服务器的实际 IP 地址 10.1.2.27。

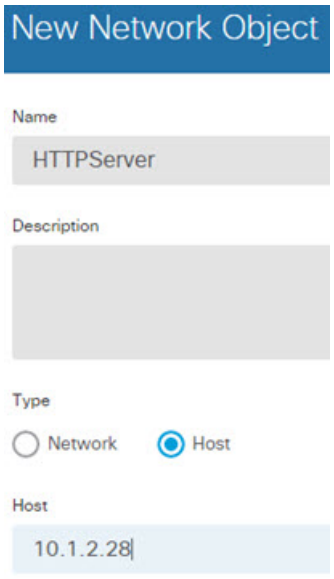


d) 点击**确定**。

步骤 2 为 HTTP 服务器创建网络对象。

a) 点击 +。

b) 为网络对象命名（例如，HTTPserver)，选择**主机**，然后输入实际主机地址 10.1.2.28。

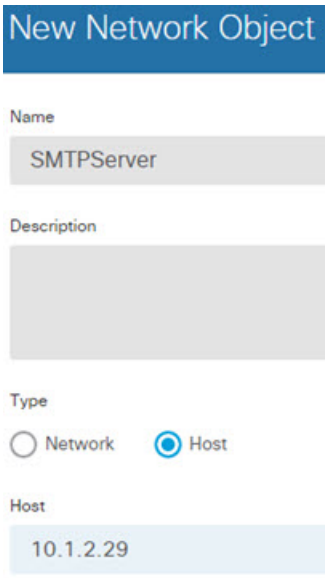


c) 点击**确定**。

步骤 3 为 SMTP 服务器创建网络对象。

a) 点击 +。

b) 为网络对象命名（例如，SMTPserver)，选择**主机**，然后输入实际主机地址 10.1.2.29。

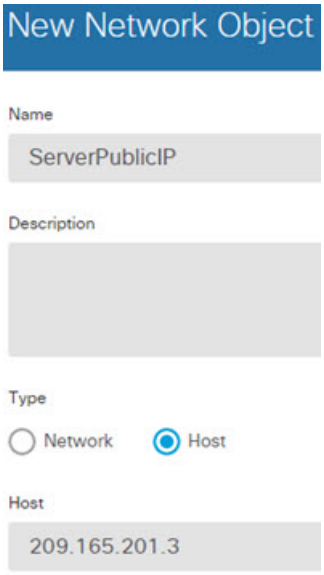


c) 点击**确定**。

步骤 4 为用于三台服务器的公共 IP 地址创建网络对象。

a) 点击 +。

b) 为网络对象命名（例如，ServerPublicIP），选择**主机**，然后输入实际主机地址 209.165.201.3。



c) 点击**确定**。

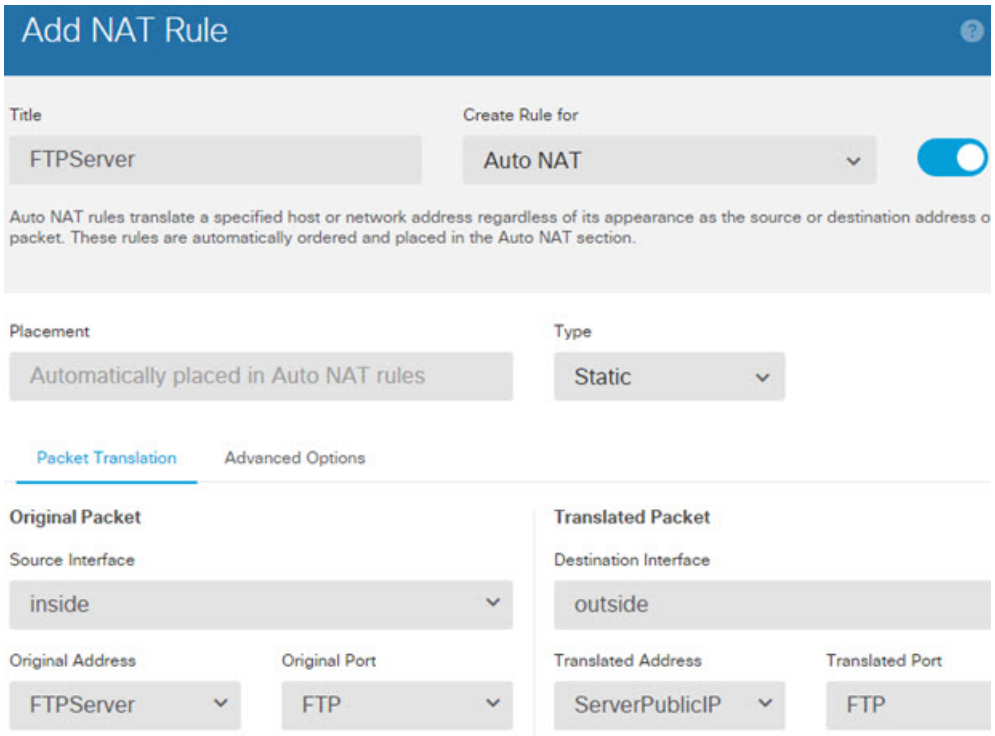
步骤 5 为 FTP 服务器配置具有端口转换的静态 NAT，并将 FTP 端口映射到其自身。

a) 依次选择**策略** > **NAT**。

b) 点击 + 按钮。

c) 配置以下属性：

- **标题** = FTPServer（或您选择的其他名称）。
- **创建规则用于** = 自动 NAT。
- **类型** = 静态。
- **源接口** = 内部。
- **目标接口** = 外部。
- **原始地址** = FTPserver 网络对象。
- **转换后的地址** = ServerPublicIP 网络对象。
- **原始端口** = FTP 端口对象。
- **转换后的端口** = FTP 端口对象。



d) 点击**确定**。

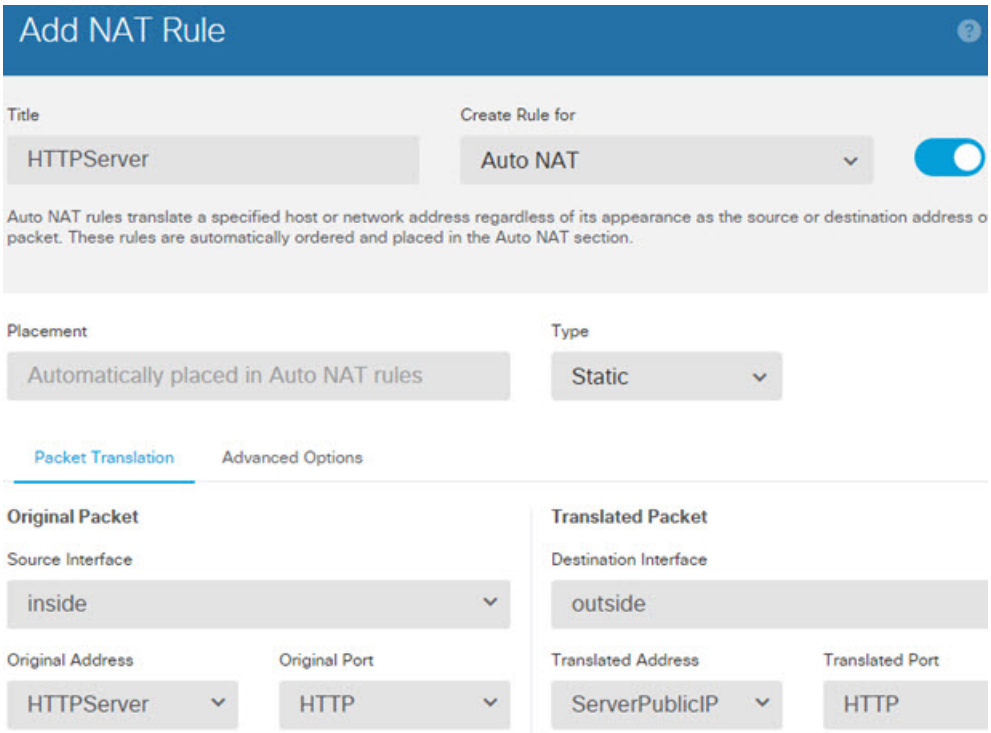
步骤 6 为 HTTP 服务器配置支持端口转换的静态 NAT，并将 HTTP 端口映射到其自身。

a) 点击 + 按钮。

b) 配置以下属性：

- **标题** = HTTPServer（或您选择的其他名称）。
- **创建规则用于** = 自动 NAT。
- **类型** = 静态。

- **源接口** = 内部。
- **目标接口** = 外部。
- **原始地址** = HTTPserver 网络对象。
- **转换后的地址** = ServerPublicIP 网络对象。
- **原始端口** = HTTP 端口对象。
- **转换后的端口** = HTTP 端口对象。



c) 点击**确定**。

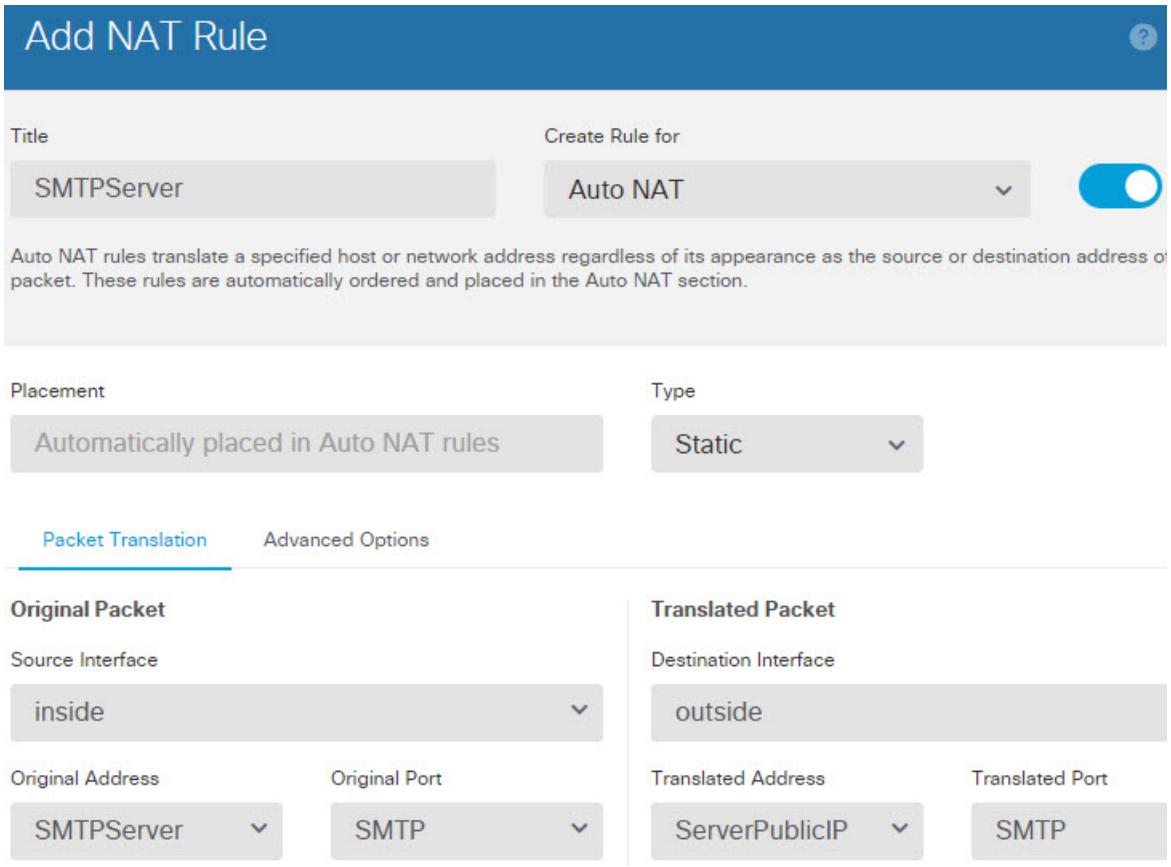
步骤 7 为 SMTP 服务器配置支持端口转换的静态 NAT，并将 SMTP 端口映射到其自身。

a) 点击 + 按钮。

b) 配置以下属性：

- **标题** = SMTPServer（或您选择的其他名称）。
- **创建规则用于** = 自动 NAT。
- **类型** = 静态。
- **源接口** = 内部。
- **目标接口** = 外部。
- **原始地址** = SMTPserver 网络对象。

- **转换后的地址** = ServerPublicIP 网络对象。
- **原始端口** = SMTP 端口对象。
- **转换后的端口** = SMTP 端口对象。



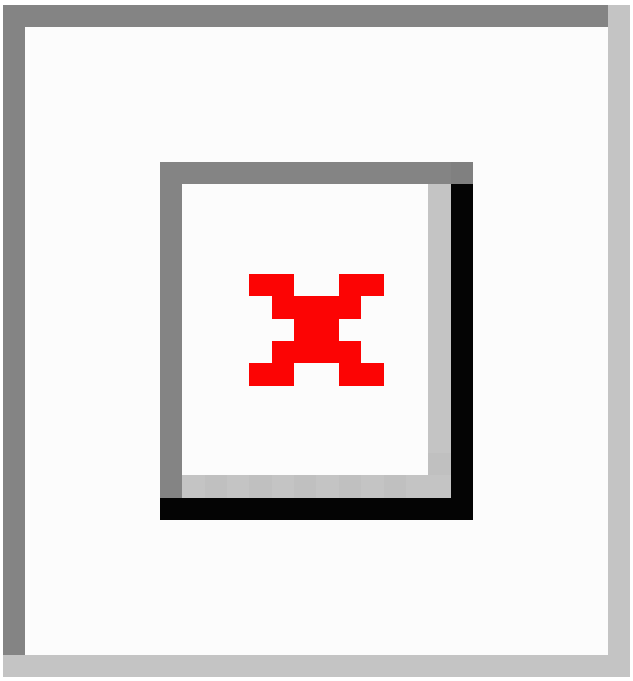
c) 点击**确定 (OK)**。

转换因目标而异（动态手动 PAT）

下图显示 10.1.2.0/24 网络上的一台主机正在访问两台不同的服务器。当主机访问位于 209.165.201.11 的服务器时，实际地址将转换为 209.165.202.129:*port*。当主机访问位于 209.165.200.225 的服务器时，实际地址将转换为 209.165.202.130:*port*。

注释 此示例假设内部接口是连接到交换机的标准路由接口，其中服务器连接到交换机。如果您的内部接口是网桥组接口 (BVI)，并且服务器连接到单独的网桥组成员接口，请选择对于相应规则，每个服务器连接的特定成员接口。例如，该规则可能以 inside1_2 和 inside1_3 而非 inside 作为源接口。

图 *15:* 具有不同目标地址的手动 *NAT*



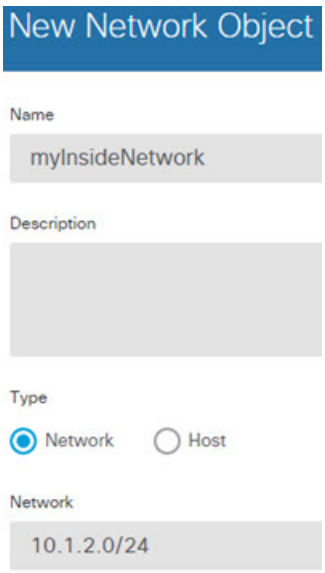
过程

步骤 1 为内部网络创建网络对象。

a) 选择**对象**。

b) 从目录中选择**网络**，然后点击 +。

c) 为网络对象命名（例如，myInsideNetwork），选择**网络**，然后输入实际网络地址 10.1.2.0/24。

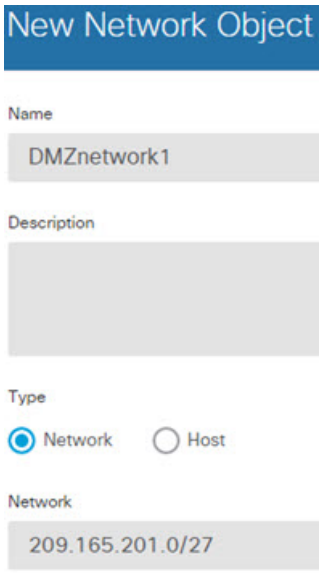


d) 点击**确定**。

步骤 2 为 DMZ 网络 1 创建网络对象。

a) 点击 +。

b) 为网络对象命名（例如，DMZnetwork1），选择**网络**，然后输入网络地址 209.165.201.0/27（子网掩码为 255.255.255.224）。

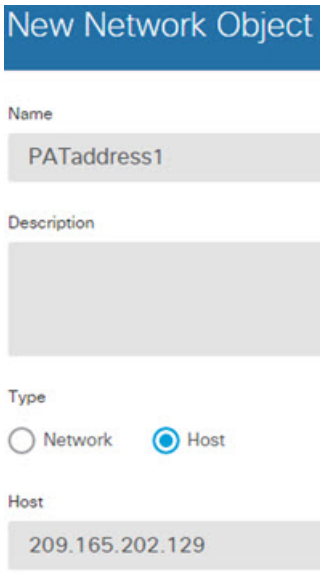


c) 点击**确定**。

步骤 3 为 DMZ 网络 1 的 PAT 地址创建网络对象。

a) 点击 +。

b) 为网络对象命名（例如，PATaddress1），选择**主机**，然后输入主机地址 209.165.202.129。

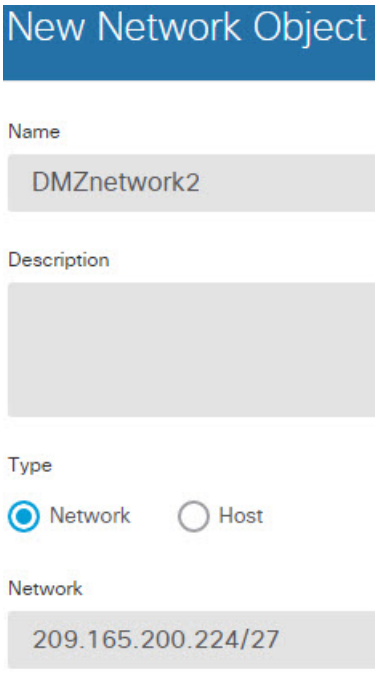


c) 点击**确定**。

步骤 4 为 DMZ 网络 2 创建网络对象。

a) 点击 +。

b) 为网络对象命名（例如，DMZnetwork2），选择**网络**，然后输入网络地址 209.165.200.224/27（子网掩码为 255.255.255.224）。

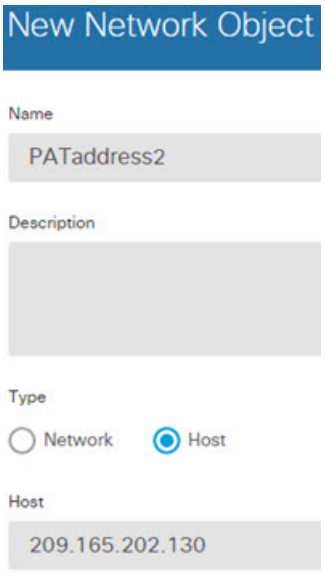


c) 点击**确定**。

步骤 5 为 DMZ 网络 2 的 PAT 地址创建网络对象。

a) 点击 +。

b) 为网络对象命名（例如，PATaddress2），选择**主机**，然后输入主机地址 209.165.202.130。



c) 点击**确定**。

步骤 6 为 DMZ 网络 1 配置动态手动 PAT。

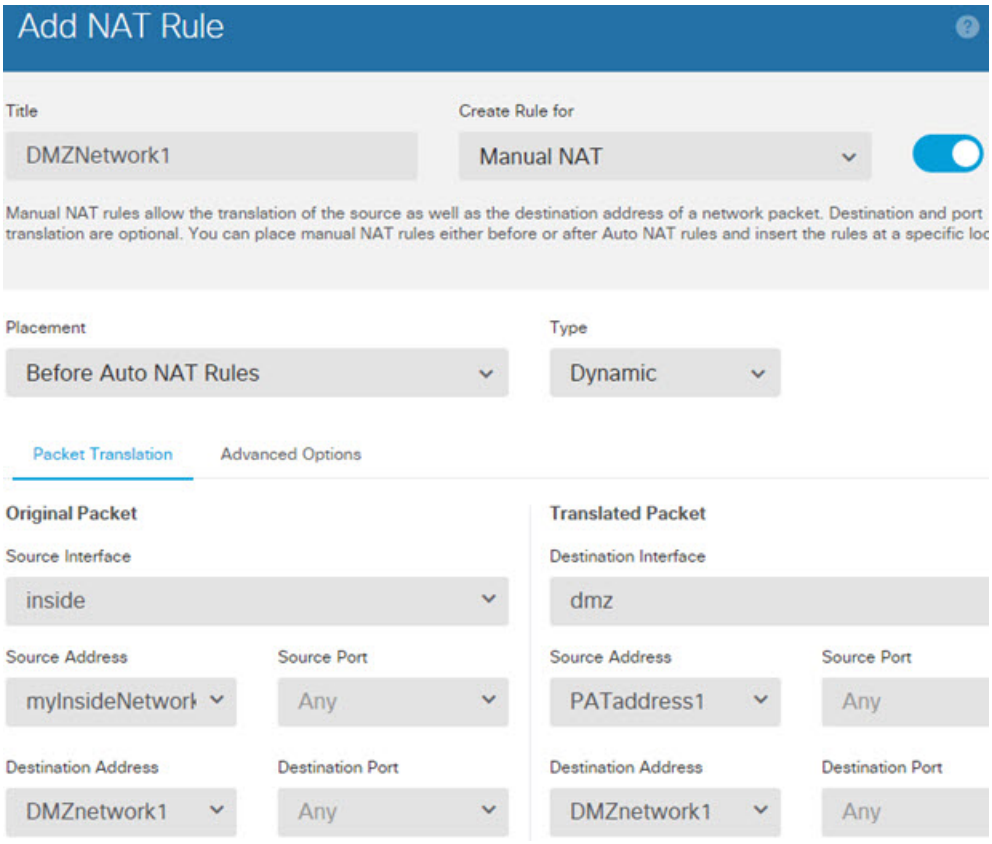
a) 依次选择**策略** > **NAT**。

b) 点击 **+** 按钮。

c) 配置以下属性：

- **标题** = DMZNetwork1（或您选择的其他名称）。
- **创建规则用于** = 手动 NAT。
- **类型** = 动态。
- **源接口** = 内部。
- **目标接口** = dmz。
- **原始源地址** = myInsideNetwork 网络对象。
- **转换后的源地址** = PATaddress1 网络对象。
- **原始目标地址** = DMZnetwork1 网络对象。
- **转换后的目标地址** = DMZnetwork1 网络对象。

  注释 由于您不需要转换目标地址，因此需要通过为原始目标地址和转换后的目标地址指定相同的地址，从而为其配置身份 NAT。将所有端口字段留空。



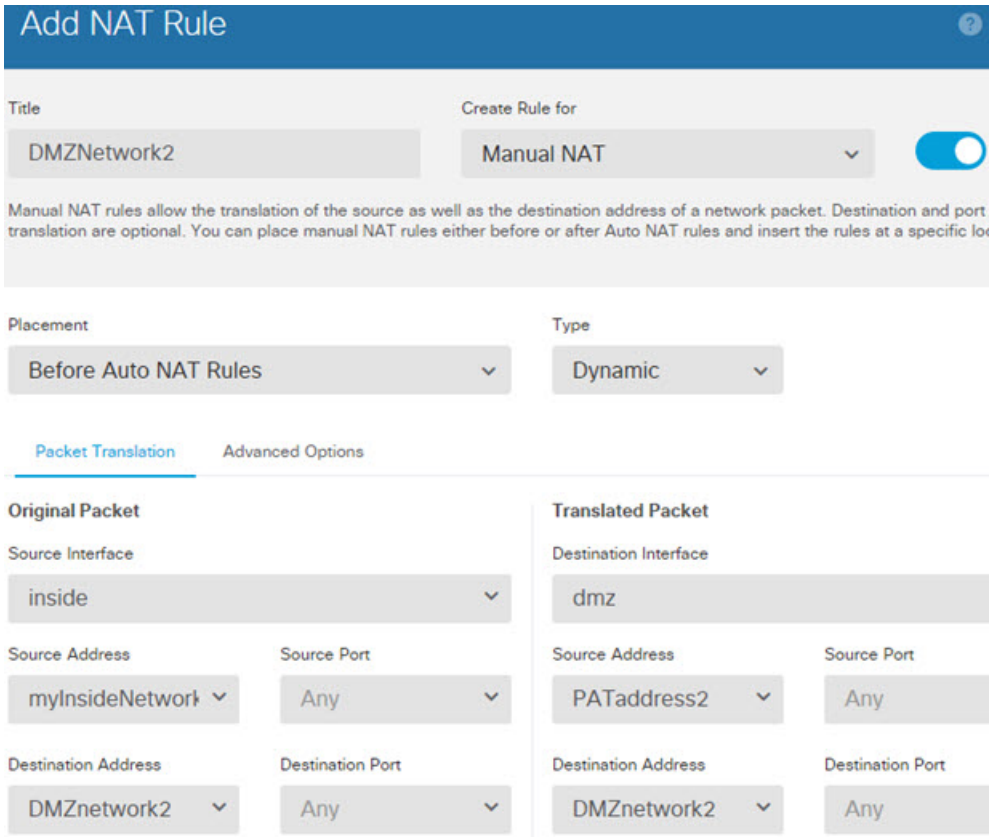
d) 点击**确定**。

步骤 7 为 DMZ 网络 2 配置动态手动 PAT。

a) 点击 + 按钮。

b) 配置以下属性：

- **标题** = DMZNetwork2（或您选择的其他名称）。
- **创建规则用于** = 手动 NAT。
- **类型** = 动态。
- **源接口** = 内部。
- **目标接口** = dmz。
- **原始源地址** = myInsideNetwork 网络对象。
- **转换后的源地址** = PATaddress2 网络对象。
- **原始目标地址** = DMZnetwork2 网络对象。
- **转换后的目标地址** = DMZnetwork2 网络对象。



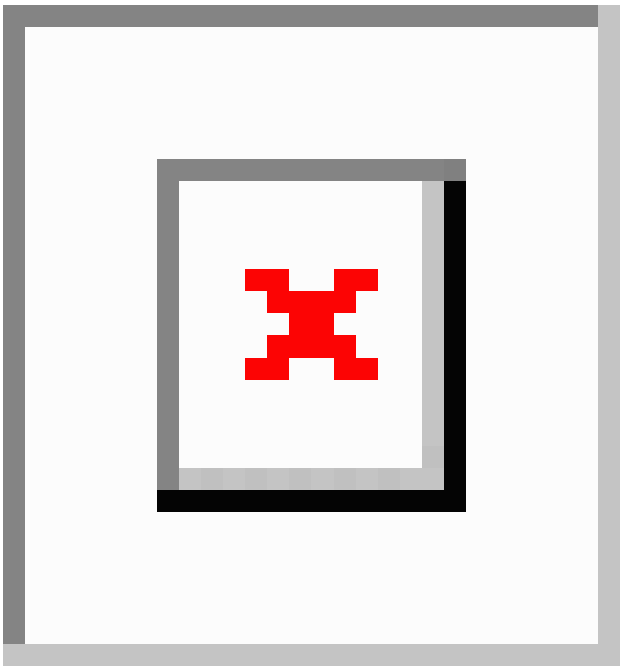
c) 点击**确定 (OK)**。

转换因目标地址和端口而异（动态手动 PAT）

下图显示源端口和目标端口的使用情况。10.1.2.0/24 网络上的主机同时因为网络服务和 Telnet 服务访问单个主机。当主机进行 Telnet 服务访问服务器时，实际地址将转换为 209.165.202.129:*port*。当主机进行网络服务访问相同服务器时，真实地址将转换为 209.165.202.130:*port*。

注释 此示例假设内部接口是连接到交换机的标准路由接口，其中服务器连接到交换机。如果内部接口是网桥组接口 (BVI) 而服务器连接到某个网桥组成员接口，请选择服务器连接到的具体成员接口。例如，该规则可能以 inside1_2 而非 inside 作为源接口。

图 *16:* 具有不同目标端口的手动 *NAT*



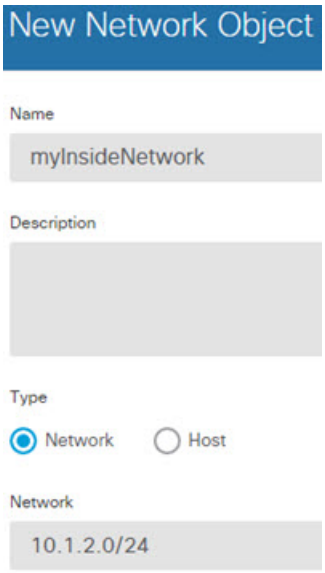
过程

步骤 1 为内部网络创建网络对象。

a) 选择**对象**。

b) 从目录中选择**网络**，然后点击 +。

c) 为网络对象命名（例如，myInsideNetwork)，选择**网络**，然后输入实际网络地址 10.1.2.0/24。

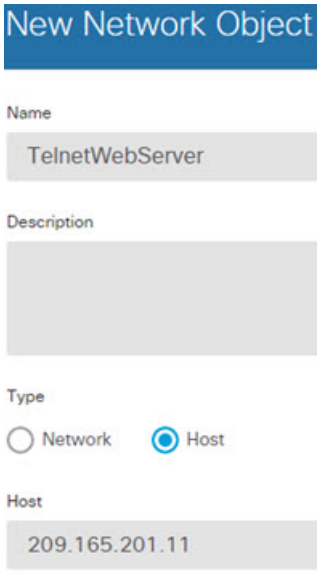


d) 点击**确定**。

步骤 2 为 Telnet/Web 服务器创建网络对象。

a) 点击 +。

b) 为网络对象命名（例如，TelnetWebServer)，选择**主机**，然后输入实际主机地址 209.165.201.11。

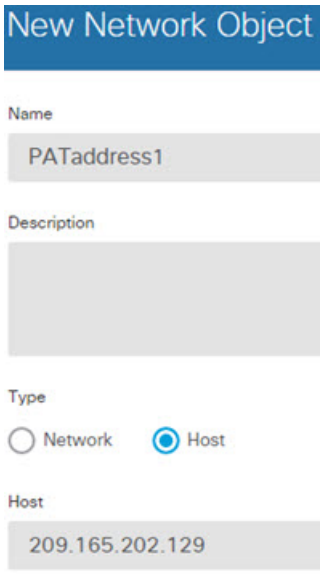


c) 点击**确定**。

步骤 3 使用 Telnet 时为 PAT 地址创建网络对象。

a) 点击 +。

b) 为网络对象命名（例如，PATaddress1)，选择**主机**，然后输入主机地址 209.165.202.129。

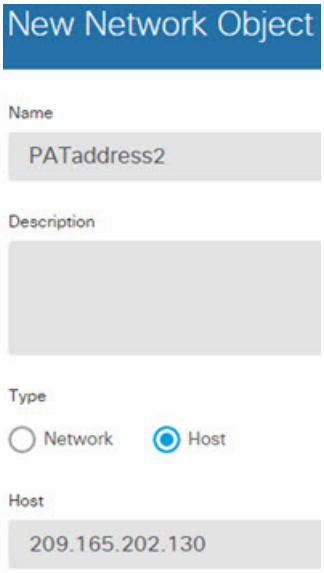


c) 点击**确定**。

步骤 4 使用 HTTP 时为 PAT 地址创建网络对象。

a) 点击 +。

b) 为网络对象命名（例如，PATaddress2），选择**主机**，然后输入主机地址 209.165.202.130。



c) 点击**确定**。

步骤 5 为 Telnet 访问创建动态手动 PAT。

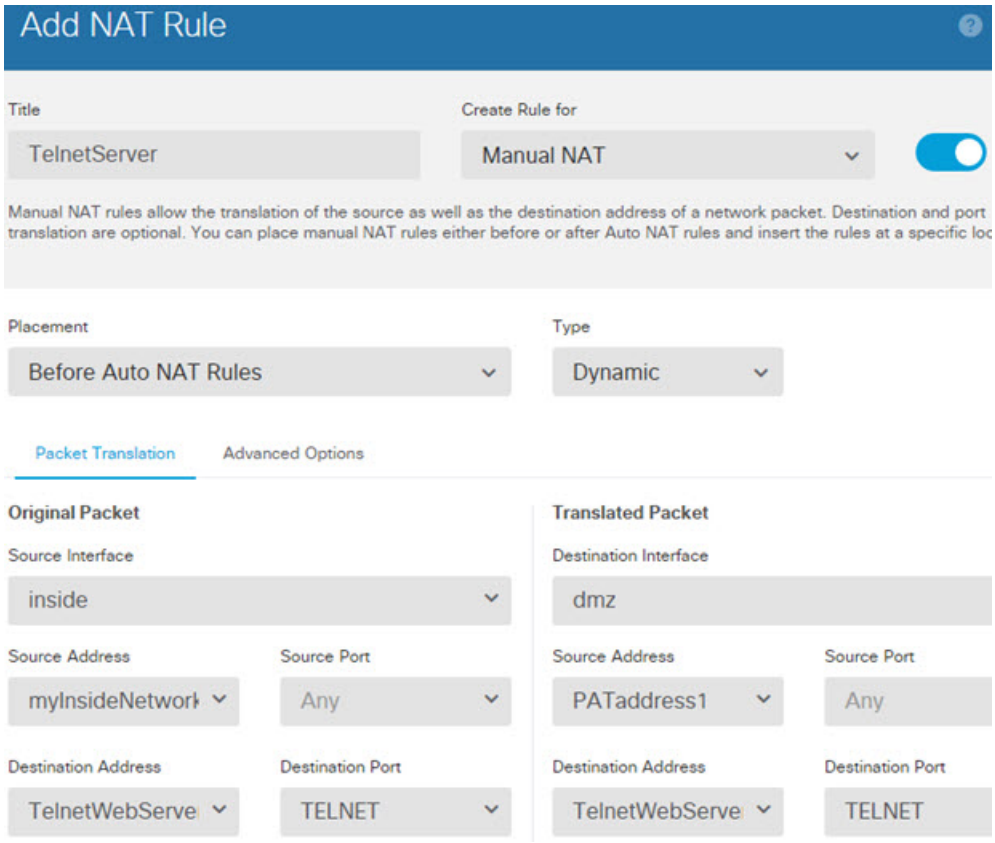
a) 依次选择**策略** > **NAT**。

b) 点击 + 按钮。

c) 配置以下属性：

- **标题** = TelnetServer（或您选择的其他名称）。
- **创建规则用于** = 手动 NAT。
- **类型** = 动态。
- **源接口** = 内部。
- **目标接口** = dmz。
- **原始源地址** = myInsideNetwork 网络对象。
- **转换后的源地址** = PATaddress1 网络对象。
- **原始目标地址** = TelnetWebServer 网络对象。
- **转换后的目标地址** = TelnetWebServer 网络对象。
- **原始目标端口** = TELNET 端口对象。
- **转换后的目标端口** = TELNET 端口对象。

注释　由于您不需要转换目标地址或端口，因此需要通过为原始目标地址和转换后的目标地址指定相同的地址，以及为原始端口和转换后的端口指定相同的端口，从而为它们配置身份 NAT。



d) 点击**确定**。

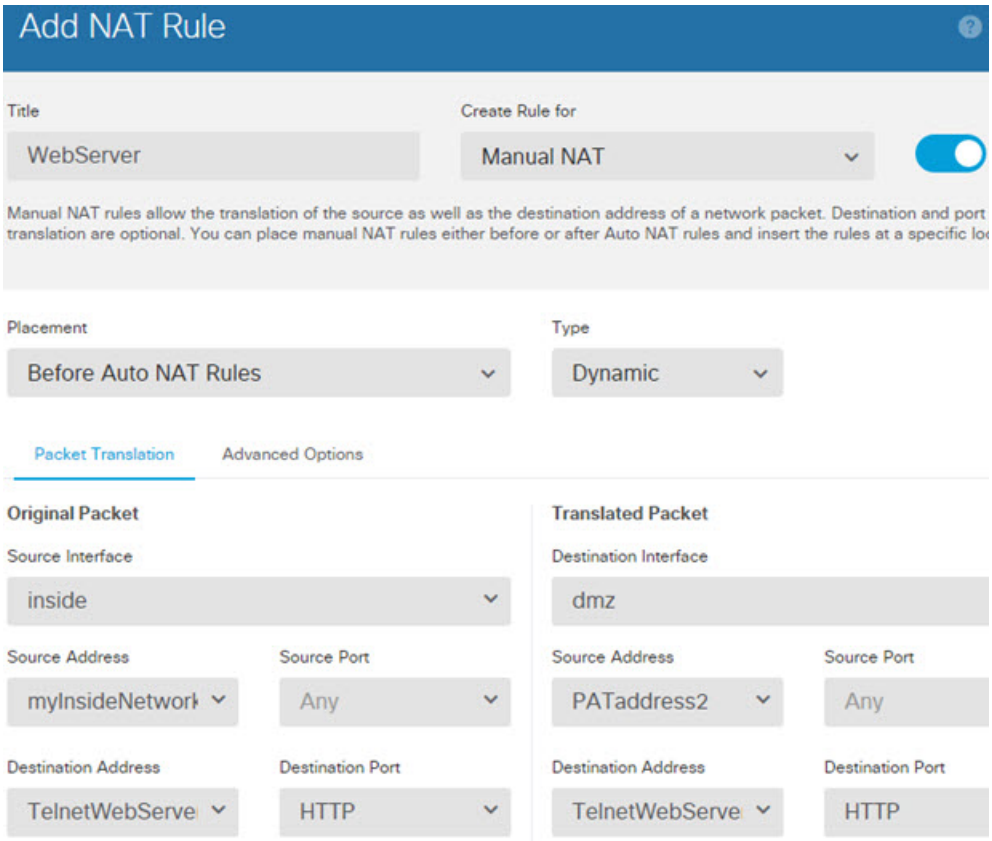
步骤 6　为 Web 访问创建动态手动 PAT。

a) 点击 + 按钮。

b) 配置以下属性：

- **标题** = WebServer（或您选择的其他名称）。
- **创建规则用于** = 手动 NAT。
- **类型** = 动态。
- **源接口** = 内部。
- **目标接口** = dmz。
- **原始源地址** = myInsideNetwork 网络对象。
- **转换后的源地址** = PATaddress2 网络对象。
- **原始目标地址** = TelnetWebServer 网络对象。

- **转换后的目标地址** = TelnetWebServer 网络对象。
- **原始目标端口** = HTTP 端口对象。
- **转换后的目标端口** = HTTP 端口对象。



c) 点击**确定 (OK)**。

使用 NAT 重写 DNS 查询和响应

可能需要配置 威胁防御设备 以修改 DNS 应答，方法是用匹配 NAT 配置的地址替换应答中的地址。配置每条转换规则时，可以配置 DNS 修改。DNS 修改也称为“DNS Doctoring”。

此功能可以重写匹配 NAT 规则的 DNS 查询和应答中的地址（例如，适用于 IPv4 的 A 记录；适用于 IPv6 的 AAAA 记录；或者，适用于逆向 DNS 查询的 PTR 记录）。对于从映射接口穿越到任何其他接口的DNS应答，记录会从映射值被重写为实际值。相反，对于从任何接口穿越到映射接口的DNS应答，记录会从实际值被重写为映射值。此功能适用于 NAT44、NAT 66、NAT46 和 NAT64。

以下是需要在 NAT 规则上配置 DNS 重写的几种主要情况。

- 规则为 NAT64 或 NAT46，并且 DNS 服务器位于外部网络上。您需要进行 DNS 重写以实现 DNS A 记录（适用于 IPv4）和 AAAA 记录（适用于 IPv6）之间的转换。

- DNS 服务器在外部，客户端在内部，并且客户端使用的一些完全限定域名解析到其他内部主机。
- DNS服务器在内部并以专用IP地址进行响应，客户端在外部，并且客户端访问指向内部托管的服务器的完全限定域名。

DNS 重写限制

以下是 DNS 重写的某些限制：

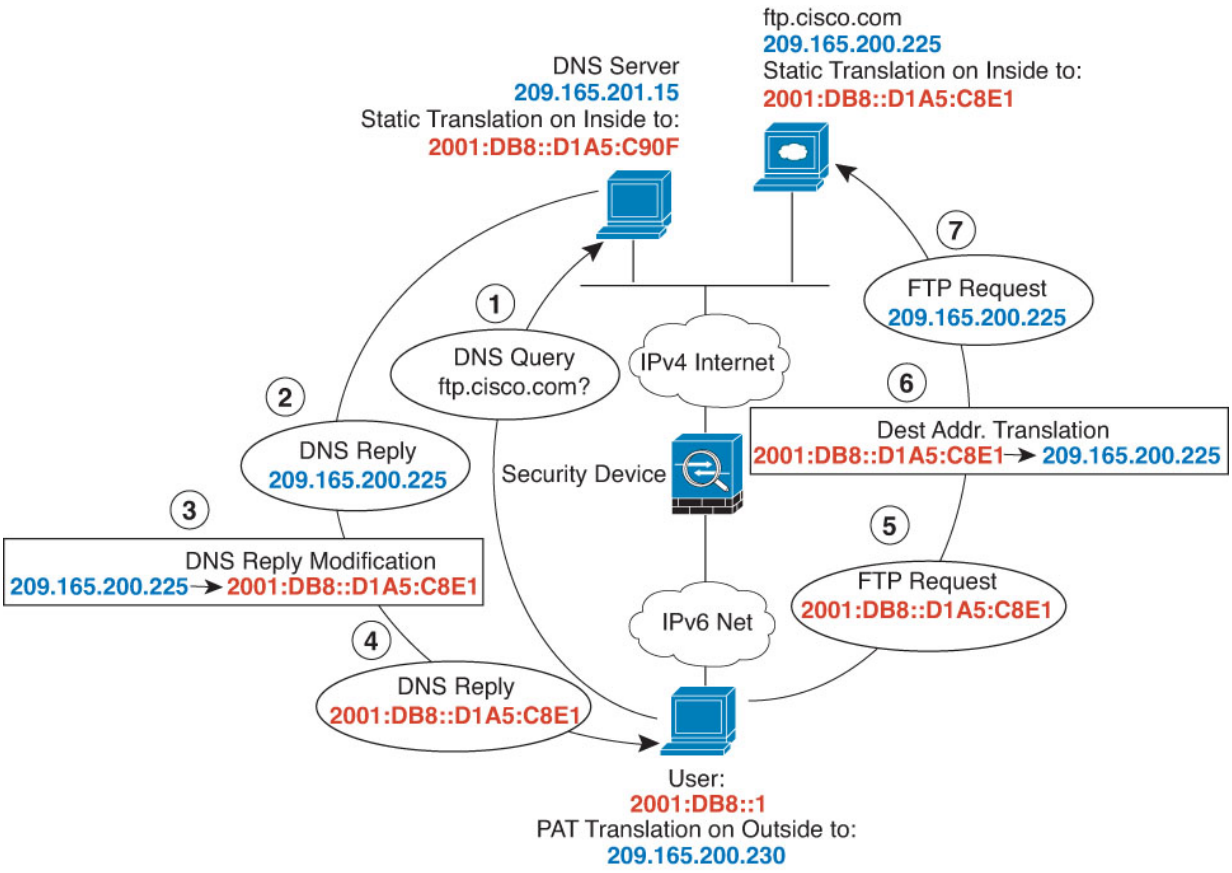
- DNS 重写不适用于 PAT，因为多条 PAT 规则适用于每个 A 或 AAAA 记录，而要使用的 PAT 规则不确定。
- 如果您配置了手动 NAT 规则，当指定了目的地址和源地址时，不能配置 DNS 修改。当流向 A 与 B 时，这类规则可能会有单个地址的不同转换。因此，将精确匹配 DNS 应答中的 IP 地址与正确的两次 NAT 规则相匹配；DNS 应答不包含有关哪个源地址/目标地址组合位于提示 DNS 请求的数据包中的信息。
- 实际上，DNS 重写在 xlate 条目而非 NAT 规则上完成。因此，如果没有面向动态规则的 xlate，则不能正确完成重写。静态 NAT 也会出现相同的问题。
- DNS 重写不会重写 DNS 动态更新消息（操作码为 5）。

以下主题提供了 NAT 规则中 DNS 重写的示例。

DNS 64 回复修改

下图显示外部 IPv4 网络上的 FTP 服务器和 DNS 服务器。系统有面向外部服务器的静态转换。在这种情况下，当内部 IPv6 用户从 DNS 服务器请求 ftp.cisco.com 的地址时，DNS 服务器将以实际地址 209.165.200.225 作为响应。

由于您希望内部用户使用 ftp.cisco.com 的映射地址（2001:DB8::D1A5:C8E1，其中 D1A5:C8E1 是 209.165.200.225 的 IPv6 对应物），因此需要配置 DNS 回复修改以进行静态转换。本示例还包括面向 DNS 服务器的静态 NAT 转换和面向内部 IPv6 主机的 PAT 规则。



注释 此示例假定，内部接口不是网桥组接口 (BVI)，而是标准路由接口。如果内部接口是 BVI，您需要为每个成员接口复制规则。

过程

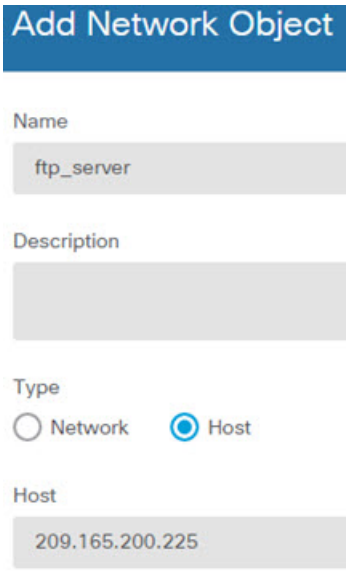
步骤 1 为 FTP 服务器、DNS 服务器、内部网络和 PAT 池创建网络对象。

a) 选择**对象**。

b) 从目录中选择**网络**，然后点击 +。

c) 定义实际 FTP 服务器地址。

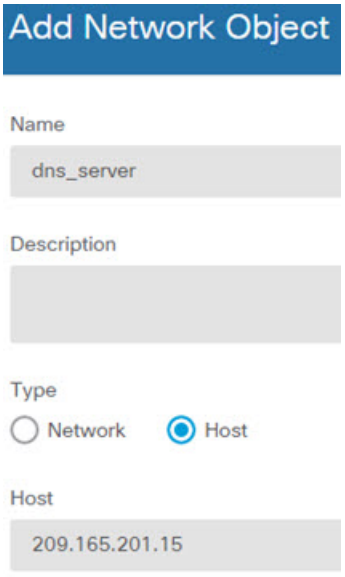
为网络对象命名（例如，ftp_server），选择**主机**，然后输入实际主机 IP 地址 209.165.200.225。



d) 点击**确定**。

e) 点击 + 并定义 DNS 服务器的实际地址。

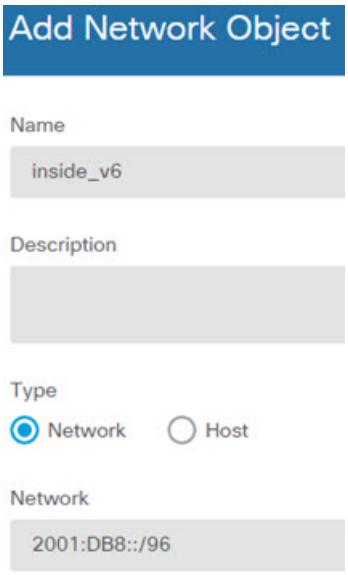
为网络对象命名（例如，dns_server)，选择**主机**，然后输入主机地址 209.165.201.15。



f) 点击**确定**。

g) 点击 + 并定义内部 IPv6 网络。

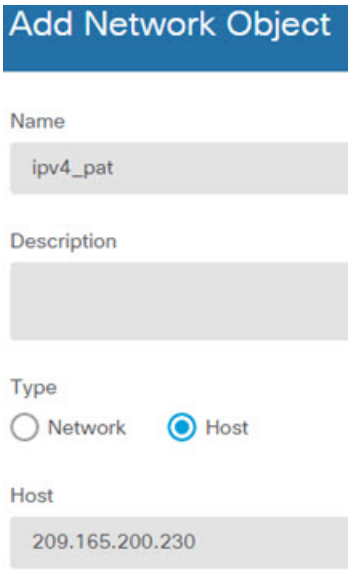
为网络对象命名（例如，inside_v6），选择**网络**，然后输入网络地址 2001:DB8::/96。



h) 点击**确定**。

i) 点击 + 并为内部 IPv6 网络定义 IPv4 PAT 地址。

为网络对象命名（例如，ipv4_pat），选择**主机**，然后输入主机地址 209.165.200.230。



j) 点击**确定**。

步骤 2 为 FTP 服务器配置带 DNS 修改的静态 NAT 规则。

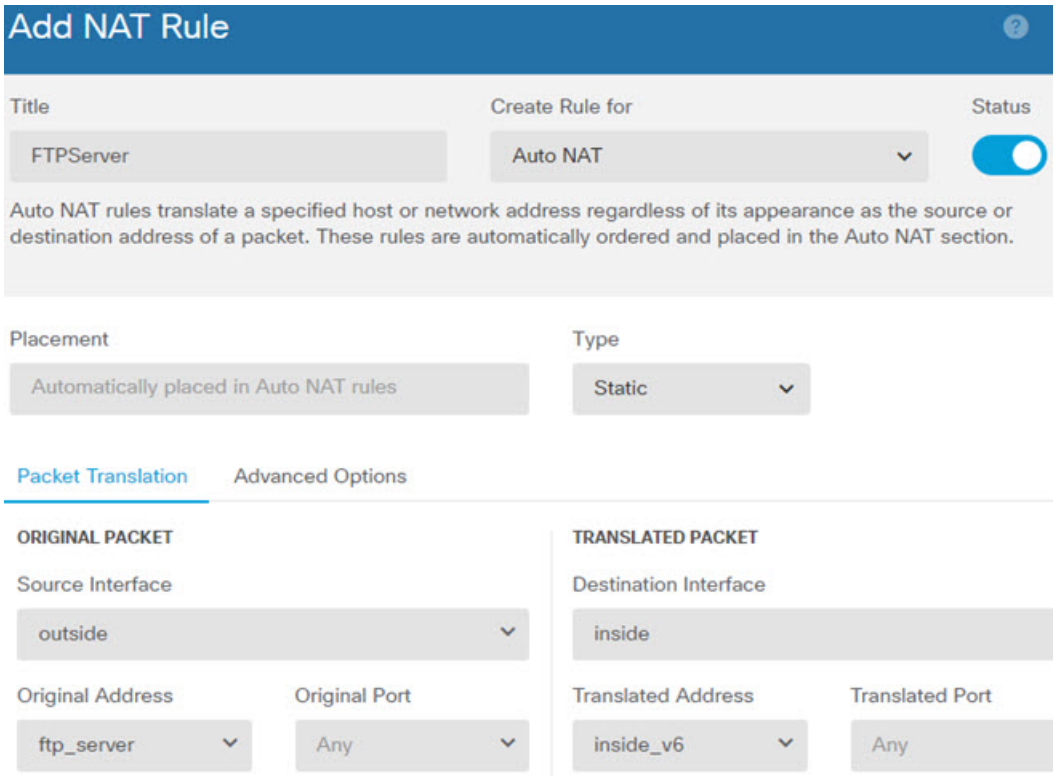
a) 依次选择**策略** > **NAT**。

b) 点击 + 按钮。

c) 配置以下属性：

- **标题** = FTPServer（或您选择的其他名称）。

- **创建规则用于** = 自动 NAT。
- **类型** = 静态。
- **源接口** = 外部。
- **目标接口** = 内部。
- **原始地址** = ftp_server 网络对象。
- **转换后的地址** = inside_v6 网络对象。由于在将 IPv4 转换为 IPv6 地址时使用 IPv4 嵌入地址方法，因此系统将 209.165.200.225 转换为 IPv6 对等的 D1A5:C8E1，并添加网络前缀以获取完整地址 2001:DB8::D1A5:C8E1。
- 在**高级选项**选项卡中，选择**转换与此规则匹配的 DNS 回复**。



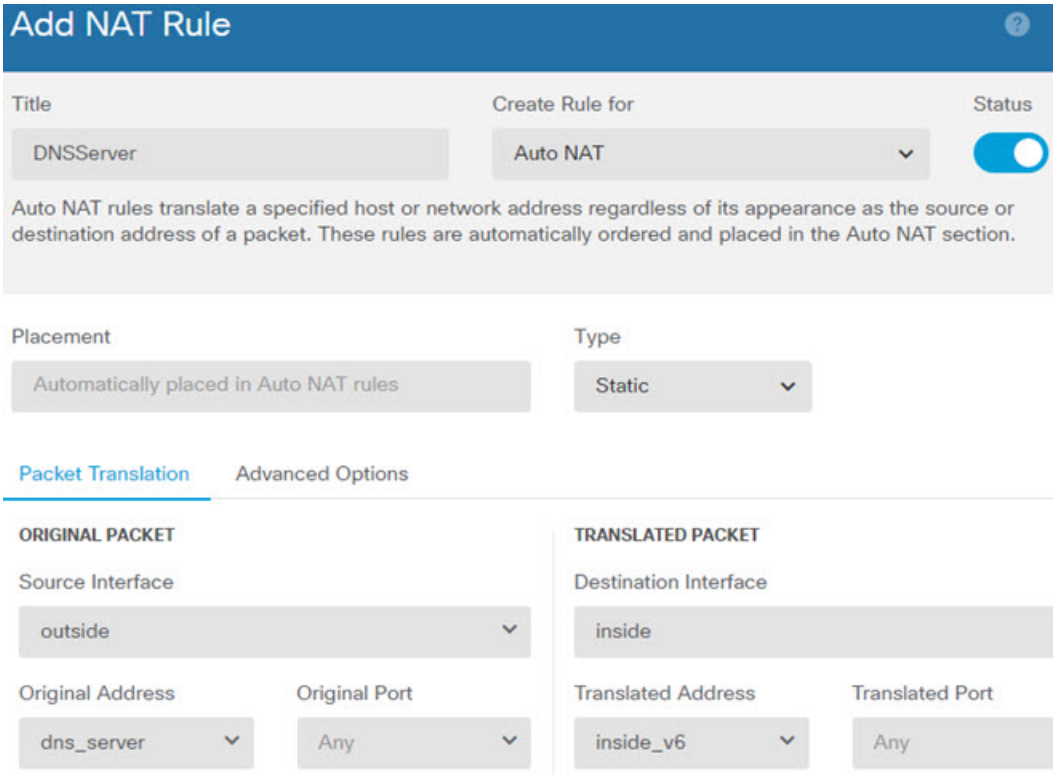
d) 点击**确定**。

步骤 3 为 DNS 服务器配置静态 NAT 规则。

a) 依次选择**策略** > **NAT**。
b) 点击 + 按钮。
c) 配置以下属性：

- **标题** = DNSServer（或您选择的其他名称）。
- **创建规则用于** = 自动 NAT。

- **类型** = 静态。
- **源接口** = 外部。
- **目标接口** = 内部。
- **原始地址** = dns_server 网络对象。
- **转换后的地址** = inside_v6 网络对象。由于在将 IPv4 转换为 IPv6 地址时使用 IPv4 嵌入地址方法，因此系统将 209.165.201.15 转换为 IPv6 对等的 D1A5:C90F，并添加网络前缀以获取完整地址 2001:DB8::D1A5:C90F。



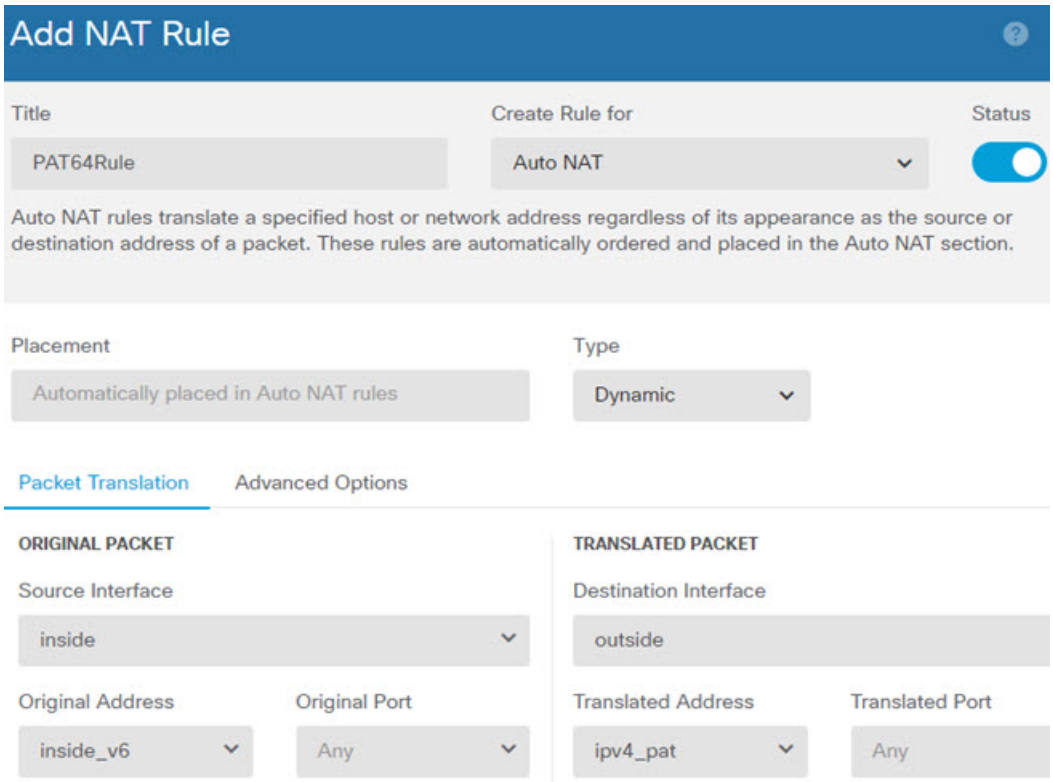
d) 点击**确定**。

步骤 4 为内部 IPv6 网络配置动态 PAT 规则。

a) 依次选择**策略** > **NAT**。
b) 点击 + 按钮。
c) 配置以下属性：

- **标题** = PAT64Rule（或您选择的其他名称）。
- **创建规则用于** = 自动 NAT。
- **类型** = 动态。
- **源接口** = 内部。

- 目标接口 = 外部。
- 原始地址 = inside_v6 网络对象。
- 转换后的地址 = ipv4_pat 网络对象。



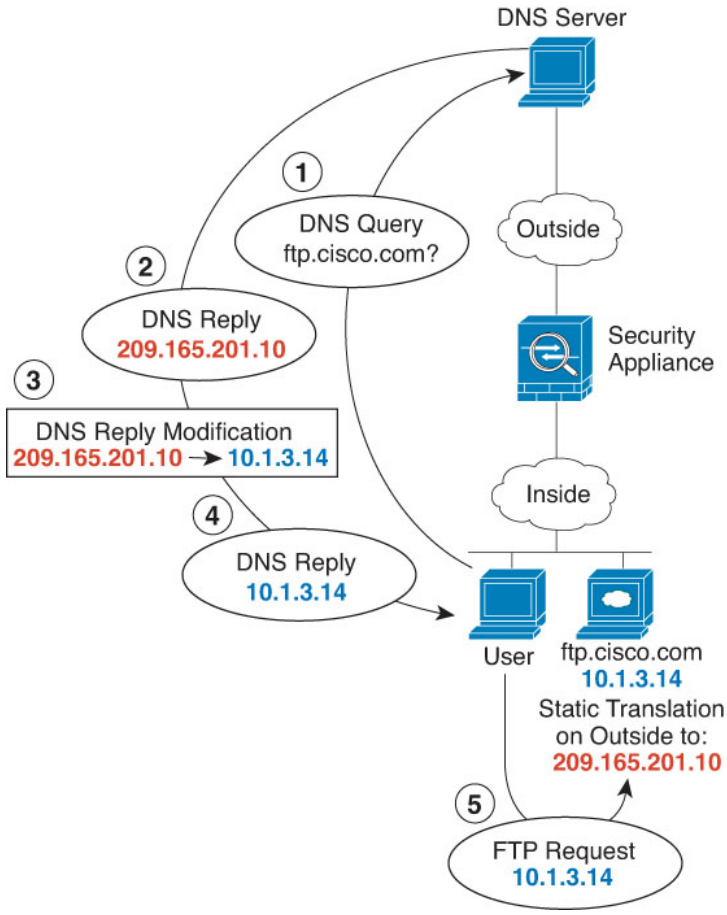
d) 点击确定 (OK)。

DNS 回复修改、外部接口上的 DNS 服务器

下图显示可从外部接口访问的 DNS 服务器。服务器 ftp.cisco.com 在内部接口上。将 NAT 配置为将 ftp.cisco.com 实际地址 (10.1.3.14) 静态转换为在外部网络上可见的映射地址 (209.165.201.10)。

在这种情况下，您要在此静态规则上启用 DNS 回复修改，以便使用实际地址访问 ftp.cisco.com 的内部用户可以接收来自 DNS 服务器的实际地址，而不是映射地址。

当内部主机发送对 ftp.cisco.com 的地址的 DNS 请求时，DNS 服务器将以映射地址 (209.165.201.10) 作为回复。系统引用内部服务器的静态规则，并将 DNS 回复中的地址转换为 10.1.3.14。如果不启用 DNS 回复修改，则内部主机尝试将流量发送到 209.165.201.10，而不是直接访问 ftp.cisco.com。



注释 此示例假定，内部接口不是网桥组接口 (BVI)，而是标准路由接口。如果内部接口是 BVI，您需要为每个成员接口复制规则。

过程

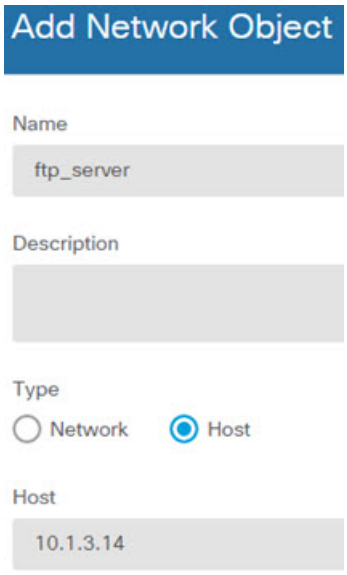
步骤 1 为 FTP 服务器创建网络对象。

a) 选择**对象**。

b) 从目录中选择**网络**，然后点击 +。

c) 定义实际 FTP 服务器地址。

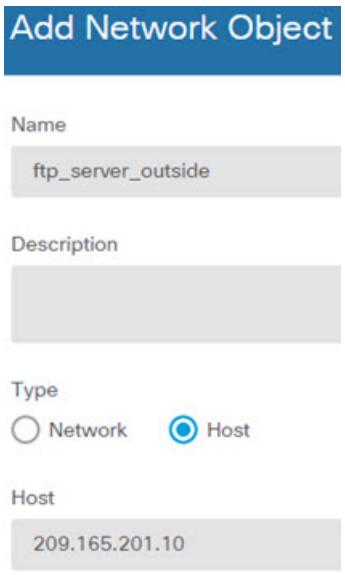
为网络对象命名（例如，ftp_server），选择**主机**，然后输入实际主机 IP 地址 10.1.3.14。



d) 点击**确定**。

e) 点击 +，然后定义 FTP 服务器的转换后的地址。

为网络对象命名（例如，ftp_server_outside），选择**主机**，然后输入主机地址 209.165.201.10。



步骤 2 为 FTP 服务器配置带 DNS 修改的静态 NAT 规则。

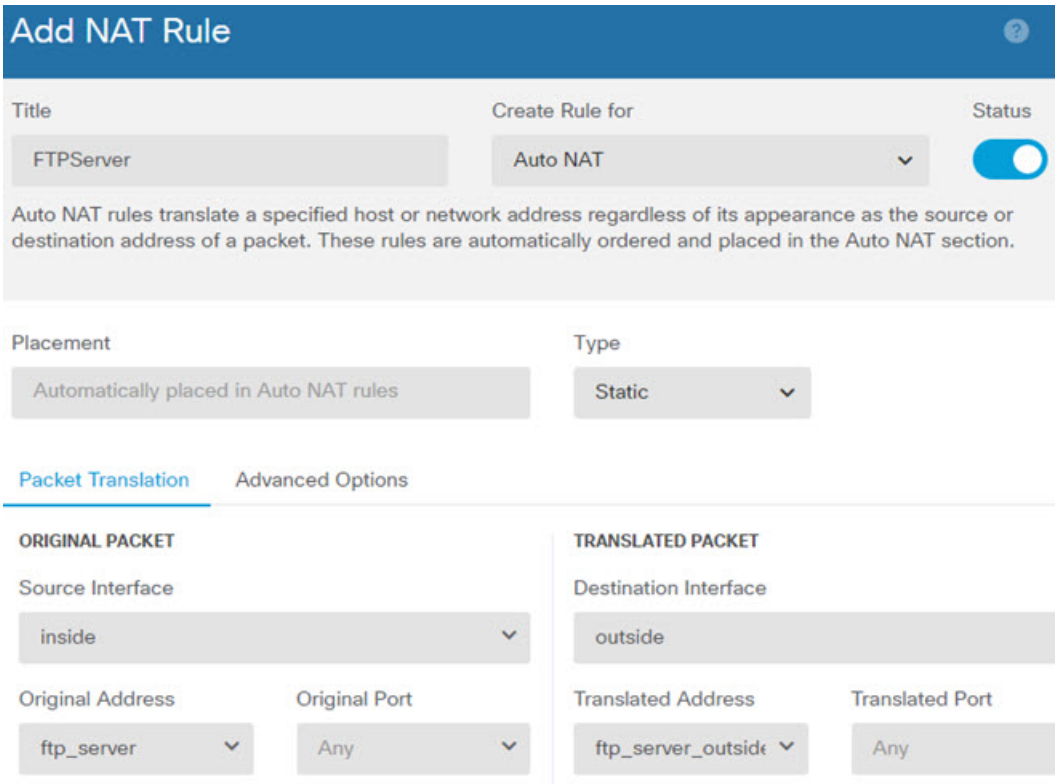
a) 依次选择**策略** > **NAT**。

b) 点击 + 按钮。

c) 配置以下属性：

- **标题** = FTPServer（或您选择的其他名称）。
- **创建规则用于** = 自动 NAT。

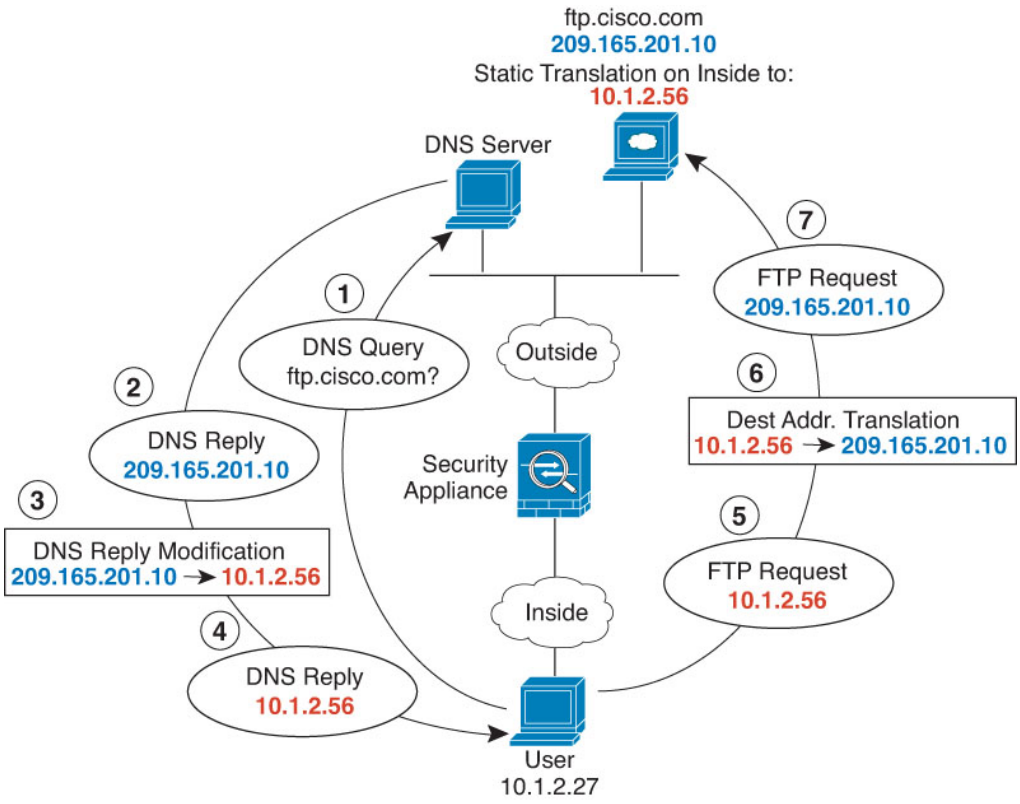
- **类型** = 静态。
- **源接口** = 内部。
- **目标接口** = 外部。
- **原始地址** = ftp_server 网络对象。
- **转换后的地址** = ftp_server_outside 网络对象。
- 在**高级选项**选项卡中，选择**转换与此规则匹配的 DNS 回复**。



d) 点击**确定 (OK)**。

DNS 回复修改、主机网络上的 DNS 服务器

下图显示外部网络上的 FTP 服务器和 DNS 服务器。系统有面向外部服务器的静态转换。在这种情况下，当内部用户从 DNS 服务器请求 ftp.cisco.com 的地址时，DNS 服务器将以实际地址 209.165.20.10 作为响应。由于您希望内部用户使用 ftp.cisco.com 的映射地址 (10.1.2.56)，因此需要配置 DNS 回复修改以进行静态转换。



注释 此示例假定，内部接口不是网桥组接口 (BVI)，而是标准路由接口。如果内部接口是 BVI，您需要为每个成员接口复制规则。

过程

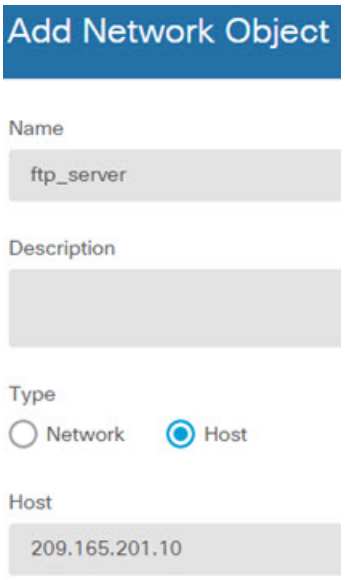
步骤 1 为 FTP 服务器创建网络对象。

a) 选择**对象**。

b) 从目录中选择**网络**，然后点击 +。

c) 定义实际 FTP 服务器地址。

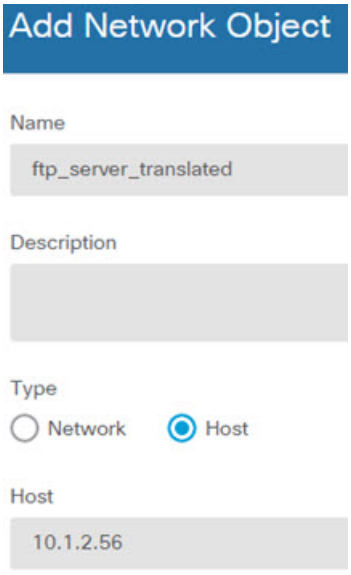
为网络对象命名（例如，ftp_server)，选择**主机**，然后输入实际主机 IP 地址 209.165.201.10.



d) 点击**确定**。

e) 点击 **+**，然后定义 FTP 服务器的转换后的地址。

为网络对象命名（例如，ftp_server_translated），选择**主机**，然后输入主机地址 10.1.2.56.



步骤 2 为 FTP 服务器配置带 DNS 修改的静态 NAT 规则。

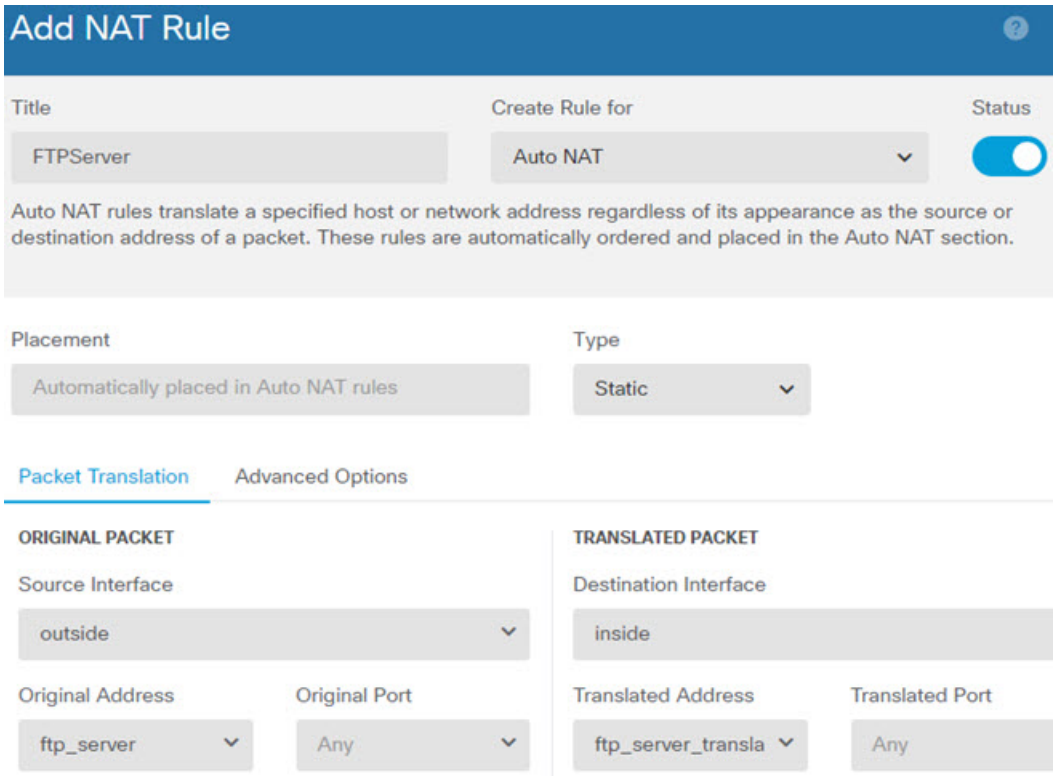
a) 依次选择**策略** > **NAT**。

b) 点击 **+** 按钮。

c) 配置以下属性：

- **标题** = FTPServer（或您选择的其他名称）。
- **创建规则用于** = 自动 NAT。

- **类型** = 静态。
- **源接口** = 外部。
- **目标接口** = 内部。
- **原始地址** = ftp_server 网络对象。
- **转换后的地址** = ftp_server_translated 网络对象。
- 在**高级选项**选项卡中，选择**转换与此规则匹配的 DNS 回复**。



d) 点击**确定 (OK)**。

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。