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 13 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 20 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 31 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 41 页。

网络对象 NAT 和两次 NAT

可以通过以下两种方法实施地址转换：网络对象 *NAT* 和两次 *NAT*。

我们建议使用网络对象 NAT，除非您需要两次 NAT 提供的额外功能。网络对象 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。）

网络对象 NAT

配置为网络对象参数的所有 NAT 规则都被视为网络对象 *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。

配置网络对象之后，可以接着将该对象的映射地址标识为内联地址或者另一个网络对象或网络对象组。

当数据包进入接口时，系统会根据网络对象 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。两次 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。

两次 NAT

两次 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。

比较网络对象 NAT 和两次 NAT

这两类 NAT 之间的主要差异是：

- 定义实际地址的方法。
  - 网络对象 NAT - 将 NAT 定义为网络对象的参数。网络对象命名 IP 主机、范围或子网，以便能在 NAT 配置中使用对象，而不是实际 IP 地址。网络对象 IP 地址用作实际地址。通过此方法，可以轻松将 NAT 添加到可能已在配置的其他部分使用的网络对象。
  - 两次 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两次 NAT 更具可扩展性。
- 实施源和目标 NAT 的方法。
  - 网络对象 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。
  - 两次 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 两次 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。
  - 网络对象 NAT- 在 NAT 表中自动排序。
  - 两次 NAT - 在 NAT 表中手动排序（在网络对象 NAT 规则之前或之后）。

NAT 规则顺序

网络对象 NAT 和两次 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。

注释 还有一个第 0 部分，其中包含系统创建供自己使用的任何 NAT 规则。这些规则优先于所有其他规则。系统会自动创建这些规则并根据需要清除 xlate。您不能在第 0 部分中添加、编辑或修改规则。

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	两次 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，两次 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	网络对象 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。
第 3 部分	两次 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：

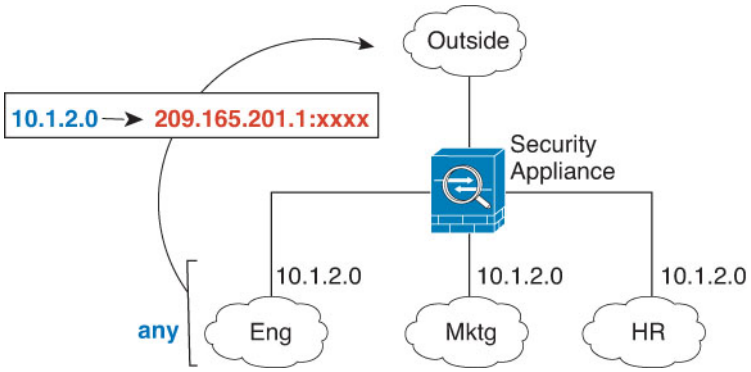
- 192.168.1.1/32（静态）
- 10.1.1.0/24（静态）
- 192.168.1.0/24（静态）
- 172.16.1.0/24（动态）（对象 abc）
- 172.16.1.0/24（动态）（对象 def）
- 192.168.1.0/24（动态）

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 *1:* 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。

NAT 准则

以下主题提供有关实施 NAT 的详细准则。

NAT 防火墙模式准则

在路由和透明防火墙模式下支持 NAT。

不过，在桥接组成员接口（属于桥接组虚拟接口 [BVI] 的接口）上配置 NAT 具有以下局限性：

- 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。
- 当映射地址是桥接组成员接口时，不能配置接口 PAT，因为没有 IP 地址连接到该接口。
- 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。但是，您可以在不同网桥组的成员之间，或在网桥组成员（源接口）和标准路由接口（目标接口）之间执行 NAT64/46。

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。此限制不适用于接口为不同网桥组成员或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)。此限制不适用于接口为不同网桥组成员或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（仅限于两次 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（仅限于两次 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。或者，还能够以网络对网络的方式转换地址，其中第一个 IPv4 地址映射到第一个 IPv6 地址，第二个 IPv4 地址映射到第二个 IPv6，依次类推。

- 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。

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 网络对象 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。例如，**对象网络 obj-10.10.10.1-01**、**对象网络 obj-10.10.10.1-02** 等。
- 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。

- 转换 SCTP 流量时，仅使用静态网络对象 NAT。系统不允许动态 NAT/PAT。虽然您可以配置静态两次 NAT，但不建议这样做，因为 SCTP 关联的目标部分的拓扑未知。
- NAT 中使用的对象和对象组不能是未定义的，它们必须包含 IP 地址。
- 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。

- （仅限于两次 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，ASA 才能对数据包执行 NAT；借助此前提条件，ASA 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。
  - （透明模式。）管理 IP 地址。
  - （动态 NAT。）启用 VPN 时的备用接口 IP 地址。
  - 现有的 VPN 池地址。
- 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。
- 有关 NAT 或 PAT 的应用检测限制，请参阅默认检测和 NAT 限制。
- 用于身份 NAT 的默认行为已启用代理 ARP，匹配其他静态 NAT 规则。如果需要，可以禁用代理 ARP。有关详细信息，请参阅路由 NAT 数据包。
- 启用 **arp permit-nonconnected** 命令时，如果映射地址不是任何已连接子网的一部分，并且没有在 NAT 规则中指定映射接口（即，指定“任何”接口），系统不会响应 ARP 请求。要解决此问题，请指定映射接口。
- 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。
- 如果对用于连接 NFS 服务器的 Sun RPC 流量使用 PAT，请注意，在通过 PAT 方式转换的端口号大于 1024 时，NFS 服务器可能会拒绝连接。NFS 服务器的默认配置是拒绝来自端口号大于 1024 的连接。错误通常为“权限被拒”。如果在较小范围内的端口不可用时选择“扁平范围”选项来使用更高的端口号，则可能会映射编号大于 1024 的端口，尤其是在未选择将较小范围包含在扁平范围内的选项时。 如果不选择将保留端口 (1-1023) 包括在 PAT 池的端口范围内的选项，则系统会映射高于 1024 的端口。您可以通过将 NFS 服务器配置更改为允许所有端口号来避免此问题。
- NAT 仅适用于直通流量。系统生成的流量不进行 NAT。
- 可使用 NAT 的事务提交模式提高系统性能和可靠性。有关详细信息，请参阅常规操作配置指南中的基本设置章节。使用 **asp rule-engine transactional-commit nat** 命令。

- 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。
- 单向选项主要用于测试目的，可能不适用于所有协议。例如，SIP 要求执行协议检查以使用 NAT 转换 SIP 报头，但如果将转换设为单向，则不会发生这种情况。
- 不能在协议无关组播 (PIM) 寄存器的内部负载上使用 NAT。
- (两次 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。
- DHCP 和 BOOTP 共享端口 UDP/67-68。由于 BOOTP 已经过时，如果同时运行 DHCP，为 bootps 端口编写 NAT 规则可能会导致端口分配问题。请考虑使用 DHCP 中继来传输网段之间的 DHCP 请求。

映射地址对象的网络对象 NAT 准则

对于动态 NAT，必须为映射地址使用一个对象或组。对于其他 NAT 类型，可以使用对象或组，或者选择使用内联地址。在使用不连续的 IP 地址范围、多个主机或子网创建映射地址池时，网络对象组特别有用。 使用 **object network** 和 **object-group network** 命令创建对象。

为映射地址创建对象时，请注意以下准则。

- 网络对象组可以包含多个对象或 IPv4 或 IPv6 地址的内联地址。组不能同时包含 IPv4 和 IPv6 地址，它只能包含一种类型的地址。
- 有关不允许的映射 IP 地址的详细信息，请参阅其他 NAT 准则，第 8 页。
- 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。
- 动态 NAT：
  - 不能使用内联地址；必须配置一个网络对象或组。
  - 对象或组不能包含子网；对象必须定义一个范围；组可以包含主机和范围。
  - 如果映射网络对象同时包含范围和主机 IP 地址，则范围可用于动态 NAT，主机 IP 地址可用作 PAT 回退。
- 动态 PAT（隐藏）：
  - 如果不使用对象，可以选择配置内联主机地址或指定接口地址。
  - 如果使用对象，则对象或组不可以包含子网。对象必须定义主机，对于 PAT 池，则必须定义范围。组（对于 PAT 池）可以包含主机和范围。

- 静态 NAT 或支持端口转换的静态 NAT：
  - 如果不使用对象，可以配置内联地址，或者指定接口地址（对于带端口转换的静态NAT）。
  - 如果使用对象，对象或组可以包含主机、范围或子网。
- 身份 NAT
  - 如果不使用对象，可以配置内联地址。
  - 如果使用对象，对象必须匹配要转换的实际地址。

用于实际与映射地址对象的两次 NAT 准则

对于每条 NAT 规则，均可为以下地址配置最多四个网络对象或组：

- 源实际地址
- 源映射地址
- 目标实际地址
- 目标映射地址

除非以内联方式指定 **any** 关键字来代表所有流量，或对于某些类型的 NAT，指定 **interface** 关键字来代表接口地址，否则需要配置对象。在使用不连续的 IP 地址范围、多个主机或子网创建映射地址池时，网络对象组特别有用。 使用 **object network** 和 **object-group network** 命令创建对象。

为两次 NAT 创建对象时，请注意以下准则。

- 网络对象组可以包含多个对象或 IPv4 或 IPv6 地址的内联地址。组不能同时包含 IPv4 和 IPv6 地址，它只能包含一种类型的地址。
- 有关不允许的映射 IP 地址的详细信息，请参阅其他 NAT 准则，第 8 页。
- 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。
- 源动态 NAT：
  - 通常要配置将较大实际地址组映射至较小的组。
  - 映射对象或组不能包含子网；对象必须定义一个范围；组可以包含主机和范围。
  - 如果映射网络对象同时包含范围和主机 IP 地址，则范围可用于动态 NAT，主机 IP 地址可用作 PAT 回退。
- 源动态 PAT（隐藏）：
  - 如果使用对象，则对象或组不可以包含子网。对象必须定义主机，对于 PAT 池，则必须定义范围。组（对于 PAT 池）可以包含主机和范围。
- 源静态 NAT 或支持端口转换的静态 NAT：

- 映射对象或组可能包含主机、范围或子网。
- 静态映射通常为一对一，因此实际地址的数量与映射地址相同。然而，如果需要，可拥有不同的数量。

- 源身份 NAT
  - 实际对象和映射对象必须匹配。可以为这二者使用相同对象，也可以单独创建包含相同 IP 地址的对象。

- 目标静态 NAT 或支持端口转换的静态 NAT（目标转换始终为静态）：
  - 尽管两次 NAT 的主要功能是纳入目标 IP 地址，但目标地址是可选的。如果确实指定目标地址，则可为该地址配置静态转换，或只将身份 NAT 用于该地址。可能需要配置没有目标地址的两次 NAT，以利用两次 NAT 的一些其他特性，包括使用实际地址的网络对象组或对规则手动排序。有关详细信息，请参阅比较网络对象 NAT 和两次 NAT，第 3 页。
  - 对于身份 NAT，实际对象和映射对象必须匹配。可以为这二者使用相同对象，也可以单独创建包含相同 IP 地址的对象。
  - 静态映射通常为一对一，因此实际地址的数量与映射地址相同。然而，如果需要，可拥有不同的数量。
  - 对于支持端口转换的静态接口 NAT（仅路由模式），可指定 **interface** 关键字，而不是映射地址的网络对象/组。
  - 您可以使用完全限定域名作为转换（映射）目标，例如 www.example.com。有关详细信息，请参阅FQDN 目的准则，第 12 页。

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 地址在两次 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。 如果使用多个 DNS 服务器组，则系统会使用过滤器域，并根据过滤器从相应的组请求地址。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 对象必须指定 IPv4 作为地址类型。

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。

实际和映射端口服务对象的两次 NAT 准则

可以选择为以下端口配置服务对象：

- **源实际端口（仅静态）或目标实际端口**
- **源映射端口（仅静态）或目标映射端口**

使用 **object service** 命令创建对象。

为两次 NAT 创建对象时，请注意以下准则。

- NAT 仅支持 TCP、UDP 和 SCTP。在转换端口时，请确保实际服务对象与映射服务对象中的协议完全相同（例如，同为 TCP）。虽然可以使用 SCTP 端口说明配置静态两次 NAT 规则，但建议不要这样操作，因为 SCTP 关联的目标端口的拓扑未知。请使用静态对象 NAT 代替 SCTP。
- 不支持“不等于”(**neq**) 运算符。
- 对于身份端口转换，可将相同的服务对象同时用于实际和映射端口。
- 源动态 NAT - 源动态 NAT 不支持端口转换。
- 源动态 PAT（隐藏）- 源动态 PAT 不支持端口转换。
- 源静态 NAT、支持端口转换的静态 NAT，或身份 NAT - 服务对象可能同时包含源和目标端口；然而，应为两个服务对象指定源或目标端口。如果应用使用固定的源端口（如某些 DNS 服务器），则您只能同时指定源和目标端口；然而，很少使用固定源端口。例如，如果要转换源主机的端口，则请配置源服务。
- 目标静态 NAT 或支持端口转换的静态 NAT（目标转换始终为静态）- 对于非静态源 NAT，只能对目标执行端口转换。服务对象可能同时包含源和目标端口，但在此情况下，将仅使用目标端口。系统将忽略您指定的源端口。

动态 NAT

以下主题介绍动态 NAT 以及如何配置动态 NAT。

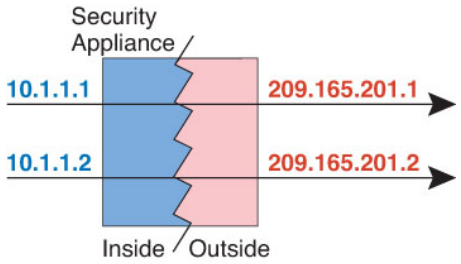
关于动态 NAT

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。远程主机的成功连接可重置连接的空闲计时器。

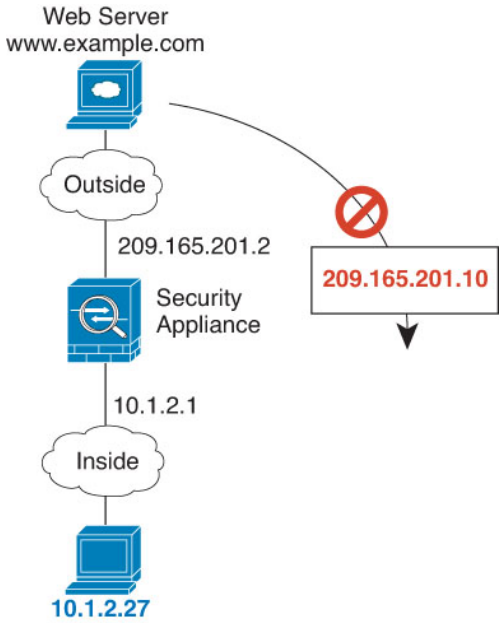
下图显示典型的动态 NAT 场景。仅实际主机可以创建 NAT 会话，允许返回响应流量。

图 *2:* 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 *3:* 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。

配置动态网络对象 NAT

本节介绍如何为动态 NAT 配置网络对象 NAT。

过程

步骤 1 为映射地址创建主机或范围网络对象（使用 **object network** 命令）或网络对象组（使用 **object-group network** 命令）。

- 对象或组不能包含子网；对象必须定义一个范围；组可以包含主机和范围。
- 如果映射网络对象同时包含范围和主机 IP 地址，则范围可用于动态 NAT，主机 IP 地址可用作 PAT 回退。

步骤 2 创建或编辑要为其配置 NAT 的网络对象：**object network** *obj_name*

示例：

```
hostname(config)# object network my-host-obj1
```

步骤 3 （编辑具有正确地址的对象时，请跳过此步骤。）定义要转换的实际 IPv4 或 IPv6 地址。

- **host** {*IPv4_address* | *IPv6_address*} - 单台主机的 IPv4 或 IPv6 地址。例如，10.1.1.1 或 2001:DB8::0DB8:800:200C:417A。
- **subnet** {*IPv4_address IPv4_mask* | *IPv6_address/IPv6_prefix*} - 网络地址。对于 IPv4 子网，请在空格后添加掩码，例如，10.0.0.0 255.0.0.0。对于 IPv6，请将地址和前缀作为一个整体（不带空格），例如 2001:DB8:0:CD30::/60。
- **range** *start_address end_address* - 地址的范围。可以指定 IPv4 或 IPv6 范围。请勿包含掩码或前缀。

示例：

```
hostname(config-network-object)# host 10.2.2.2
```

步骤 4 为对象 IP 地址配置**动态 NAT**。只能为给定对象定义单一 NAT 规则。

nat [**(***real_ifc***,***mapped_ifc***)**] **dynamic** *mapped_obj* [**interface** [**ipv6**]] [**dns**]

其中：

- Interfaces -（对于桥接组成员接口需要填入。）指定实际 (*real_ifc*) 接口和映射 (*mapped_ifc*) 接口。确保包含圆括号。在路由模式下，如果没有指定实际接口和映射接口，则将使用所有接口。您也可以为一个或两个接口指定关键字 **any**（例如 any,outside），但 **any** 不适用于桥接组成员接口。
- Mapped IP address - 指定包括映射的 IP 地址的网络对象或网络对象组。
- Interface PAT fallback -（可选）**interface** 关键字启用接口 PAT 回退。在用尽映射 IP 地址后，使用映射接口的 IP 地址。如果指定 **ipv6**，则将使用接口的 IPv6 地址。对于此选项，必须为 *mapped_ifc* 配置特定接口。（当映射接口为桥接组成员时，无法指定 **interface**。）
- DNS -（可选）**dns** 关键字可以转换 DNS 应答。确保启用 DNS 检测（默认情况下启用）。有关详细信息，请参阅使用 NAT 重写 DNS 查询和响应。

示例：

```
hostname(config-network-object)# nat (inside,outside) dynamic MAPPED_IPS interface
```

示例

以下示例配置动态 NAT，将 192.168.2.0 网络隐藏在外部地址 10.2.2.1 到 10.2.2.10 的范围后面：

```
hostname(config)# object network my-range-obj
hostname(config-network-object)# range 10.2.2.1 10.2.2.10
hostname(config)# object network my-inside-net
hostname(config-network-object)# subnet 192.168.2.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) dynamic my-range-obj
```

以下示例使用动态 PAT 备份配置 动态 NAT。内部网络 10.76.11.0 中的主机首先映射到 nat-range 1 池 (10.10.10.10-10.10.10.20)。分配 nat-range1 池中的所有地址之后，使用 pat-ip1 地址 (10.10.10.21) 执行动态 PAT。PAT 转换也用尽的可能性不大，即使发生这种情况，也可以使用外部接口地址执行动态 PAT。

```
hostname(config)# object network nat-range1
hostname(config-network-object)# range 10.10.10.10 10.10.10.20

hostname(config-network-object)# object network pat-ip1
hostname(config-network-object)# host 10.10.10.21

hostname(config-network-object)# object-group network nat-pat-grp
hostname(config-network-object)# network-object object nat-range1
hostname(config-network-object)# network-object object pat-ip1
```

```
hostname(config-network-object)# object network my_net_obj5
hostname(config-network-object)# subnet 10.76.11.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) dynamic nat-pat-grp interface
```

以下示例使用动态 PAT 备份配置动态 NAT，将 IPv6 主机转换为 IPv4 主机。内部网络 2001:DB8::/96 上的主机首先映射到 IPv4_NAT_RANGE 池（209.165.201.1 到 209.165.201.30）。分配 IPv4_NAT_RANGE 池中的所有地址之后，使用 IPv4_PAT 地址 (209.165.201.31) 执行动态 PAT。在 PAT 转换也被用完的情况下， 使用外部接口地址执行动态 PAT。

```
hostname(config)# object network IPv4_NAT_RANGE
hostname(config-network-object)# range 209.165.201.1 209.165.201.30

hostname(config-network-object)# object network IPv4_PAT
hostname(config-network-object)# host 209.165.201.31

hostname(config-network-object)# object-group network IPv4_GROUP
hostname(config-network-object)# network-object object IPv4_NAT_RANGE
hostname(config-network-object)# network-object object IPv4_PAT

hostname(config-network-object)# object network my_net_obj5
hostname(config-network-object)# subnet 2001:DB8::/96
hostname(config-network-object)# nat (inside,outside) dynamic IPv4_GROUP interface
```

配置静态两次 NAT

本节介绍如何为动态 NAT 配置两次 NAT。

过程

步骤 1 为源实际地址、源映射地址、目标实际地址和目标映射地址创建主机或范围网络对象（使用 **object network** 命令）或网络对象组（使用 **object-group network** 命令）。还可以将 FQDN 网络对象用于目标映射地址。

- 如果要转换所有源流量，则跳过为源实际地址添加对象，转而在 **nat** 命令中指定 **any** 关键字。
- 如果要配置仅支持端口转换的静态接口 NAT，则可跳过为目标映射地址添加对象，转而在 **nat** 命令中指定 **interface** 关键字。

如果创建对象，请注意以下准则：

- 通常要配置将较大实际地址组映射至较小的组。
- 对象或组不能包含子网；对象必须定义一个范围；组可以包含主机和范围。
- 如果映射网络对象同时包含范围和主机 IP 地址，则范围可用于动态 NAT，主机 IP 地址可用作 PAT 回退。

步骤 2 （可选。）为目标实际端口和目标映射端口创建服务对象。

对于动态 NAT，只能对目标执行端口转换。服务对象可能同时包含源和目标端口，但在此情况下，将仅使用目标端口。系统将忽略您指定的源端口。

步骤 3 配置**动态 NAT**。

nat [**(***real_ifc***,***mapped_ifc***)**] [*line* | {**after-auto** [*line*]}] **source dynamic** {*real_obj* | **any**} {*mapped_obj* [**interface** [**ipv6**]]} [**destination static** {*mapped_obj* | **interface** [**ipv6**]} *real_obj*] [**service** *mapped_dest_svc_obj real_dest_svc_obj*] [**dns**] [**unidirectional**] [**inactive**] [**description** *desc*]

其中：

- Interfaces -（对于桥接组成员接口需要填入。）指定实际 (*real_ifc*) 接口和映射 (*mapped_ifc*) 接口。确保包含圆括号。在路由模式下，如果没有指定实际接口和映射接口，则将使用所有接口。您也可以为一个或两个接口指定关键字 **any**（例如 any、outside），但 **any** 不适用于桥接组成员接口。
- Section and Line -（可选。）默认情况下，NAT 规则将添加至 NAT 表的第 1 部分的末尾（请参阅 NAT 规则顺序，第 4 页）。如果要转而将规则添加至第 3 部分（位于网络对象 NAT 规则之后），则可使用 **after-auto** 关键字。可以使用 *line* 参数在适用部分的任意位置插入规则。
- 源地址：
  - Real - 指定网络对象、组或 **any** 关键字。
  - Mapped - 指定不同的网络对象或组。或者您可以选择配置以下回退方法：
    - Interface PAT fallback -（可选。）**interface** 关键字启用接口 PAT 回退。在用尽映射 IP 地址后，使用映射接口的 IP 地址。如果指定 **ipv6**，则将使用接口的 IPv6 地址。对于此选项，必须为 *mapped_ifc* 配置特定接口。（当映射接口为桥接组成员时，无法指定 **interface**）。
- 目标地址（可选）：
  - Mapped - 指定网络对象或组，或对于仅支持端口转换的静态接口 NAT，指定 **interface** 关键字。如果指定 **ipv6**，则将使用接口的 IPv6 地址。如指定 **interface**，请务必也配置 **service** 关键字。对于此选项，必须为 *real_ifc* 配置特定接口。有关详细信息，请参阅支持端口转换的静态 NAT，第 32 页。
  - Real - 指定网络对象或组。对于身份 NAT，只需将相同的对象或组同时用于实际和映射地址。
- Destination port -（可选。）指定 **service** 关键字以及映射和实际服务对象。对于身份端口转换，只需相同的服务对象同时用于实际和映射端口。
- DNS -（可选；适用于源专用规则。）**dns** 关键字转换 DNS 应答。确保启用 DNS 检测（默认情况下启用）。如配置 **destination** 地址，则无法配置 **dns** 关键字。有关详细信息，请参阅 使用 NAT 重写 DNS 查询和响应。
- Unidirectional -（可选。）指定 **unidirectional**，以使目标地址无法发起流向源地址的流量。
- Inactive -（可选。）要使此规则变为非活动状态而不必删除命令，请使用 **inactive** 关键字。要将其重新激活，请重新输入没有 **inactive** 关键字的整个命令。

- Description -（可选。）使用 **description** 关键字可提供最多 200 个字符的说明。

示例：

```
hostname(config)# nat (inside,outside) source dynamic MyInsNet NAT_POOL
destination static Server1_mapped Server1 service MAPPED_SVC REAL_SVC
```

示例

以下示例在访问 209.165.201.1/27 网络上的服务器以及 203.0.113.0/24 网络上的服务器时为内部网络 10.1.1.0/24 配置动态 NAT。

```
hostname(config)# object network INSIDE_NW
hostname(config-network-object)# subnet 10.1.1.0 255.255.255.0

hostname(config)# object network MAPPED_1
hostname(config-network-object)# range 209.165.200.225 209.165.200.254

hostname(config)# object network MAPPED_2
hostname(config-network-object)# range 209.165.202.129 209.165.200.158

hostname(config)# object network SERVERS_1
hostname(config-network-object)# subnet 209.165.201.0 255.255.255.224

hostname(config)# object network SERVERS_2
hostname(config-network-object)# subnet 203.0.113.0 255.255.255.0

hostname(config)# nat (inside,outside) source dynamic INSIDE_NW MAPPED_1
destination static SERVERS_1 SERVERS_1
hostname(config)# nat (inside,outside) source dynamic INSIDE_NW MAPPED_2
destination static SERVERS_2 SERVERS_2
```

以下示例在访问 IPv4 209.165.201.1/27 网络上的服务器以及 203.0.113.0/24 网络上的服务器时为 IPv6 内部网络 2001:DB8:AAAA::/96 配置动态 NAT：

```
hostname(config)# object network INSIDE_NW
hostname(config-network-object)# subnet 2001:DB8:AAAA::/96

hostname(config)# object network MAPPED_1
hostname(config-network-object)# range 209.165.200.225 209.165.200.254

hostname(config)# object network MAPPED_2
hostname(config-network-object)# range 209.165.202.129 209.165.200.158

hostname(config)# object network SERVERS_1
hostname(config-network-object)# subnet 209.165.201.0 255.255.255.224

hostname(config)# object network SERVERS_2
hostname(config-network-object)# subnet 203.0.113.0 255.255.255.0

hostname(config)# nat (inside,outside) source dynamic INSIDE_NW MAPPED_1
destination static SERVERS_1 SERVERS_1
hostname(config)# nat (inside,outside) source dynamic INSIDE_NW MAPPED_2
```

```
destination static SERVERS_2 SERVERS_2
```

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 *4:* 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。对于多会话 PAT，使用 PAT 超时，默认情况下为 30 秒。对于每会话 PAT，会立即删除 xlate。

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 ASA 接口 IP 地址用作 PAT 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)。此限制不适用于接口为不同网桥组成员或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。

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。可以配置一个 PAT 地址池，使用 PAT 地址轮询分配来避免出现这种情况。

PAT 池对象准则

当为 PAT 池创建网络对象时，请遵守以下准则。

对于 PAT 池

- 端口会映射到 1024 到 65535 范围内的可用端口。您可以选择包含保留的端口，即 1024 以下的端口，以便让整个端口范围可用于转换。

  在集群中运行时，每个地址的512个端口块会被分配给集群成员，并在这些端口块内进行映射。如果还启用块分配，则会根据块分配大小（其默认值也是 512）来分配端口。

- 如果对 PAT 池启用块分配，则仅在 1024-65535 范围内分配端口块。因此，如果应用需要较低的端口号 (1-1023)，它可能不起作用。例如，请求端口 22 (SSH) 的应用会获得 1024-65535 范围内和分配到主机的块范围内的映射端口。
- 如在两个不同的规则中使用相同的 PAT 池对象，则请确保为每条规则指定相同的选项。例如，如果一条规则指定扩展 PAT，则另一条规则也必须指定扩展 PAT。
- 如果主机拥有现有连接，则来自该主机的后续连接会使用相同的 PAT IP 地址。如果没有可用的端口，这可能会阻止连接。使用轮询选项可避免此问题。
- 为获得最佳性能，请将 PAT 池中的 IP 地址数量限制为 10,000。

对于 PAT 池的扩展 PAT

- 许多应用检测不支持扩展 PAT。
- 如为动态 PAT 规则启用扩展 PAT，则不能在支持端口转换规则的另一静态 NAT 中使用 PAT 池中的地址作为 PAT 地址。例如，如果 PAT 池包括 10.1.1.1，则无法将 10.1.1.1 作为 PAT 地址创建带端口转换规则的静态 NAT。
- 如使用 PAT 池，并为回退指定接口，则无法指定扩展 PAT。
- 对于使用 ICE 或 TURN 的 VoIP 部署，请勿使用扩展 PAT。ICE 和 TURN 依赖于 PAT 绑定才能对所有目标均保持相同。
- 您不能在集群中的设备上使用扩展 PAT。
- 扩展 PAT 会增加设备上的内存使用率。

对于 PAT 池的轮询

- 如果主机拥有现有连接，并且端口可用，则来自该主机的后续连接将使用相同的 PAT IP 地址。不过，这种“粘性”不能超越故障转移。如果该设备执行故障转移，来自主机的后续连接可能会使用初始 IP 地址。

- 如果在同一接口上混合使用 PAT 池/轮询规则和接口 PAT 规则，IP 地址"粘性"也会受到影响。对于任何给定接口，请选择 PAT 池或接口 PAT；请勿创建竞争 PAT 规则。
- 轮询可能会消耗大量的内存，在与扩展 PAT 组合使用时尤其如此。由于将为每一个映射协议/IP 地址/端口范围创建 NAT 池，因此，轮询会导致大量并发 NAT 池，从而消耗内存。扩展 PAT 甚至将导致更多数量的并发 NAT 池。

配置动态网络对象 PAT

本节介绍如何为动态 PAT 配置网络对象 NAT。

过程

步骤 1 （可选。）为映射地址创建一个主机或范围网络对象（**object network** 命令）或网络对象组（**object-group network** 命令）。

- 如果不使用对象，可以选择配置内联主机地址或指定接口地址。
- 如果使用对象，对象或组不能包含子网；对象必须定义主机，或者对于 PAT 池，必须定义范围；组（对于 PAT 池）可以包含主机和范围。

步骤 2 创建或编辑要为其配置 NAT 的网络对象：**object network** *obj_name*

示例：

```
hostname(config)# object network my-host-obj1
```

步骤 3 （编辑具有正确地址的对象时，请跳过此步骤。）定义要转换的实际 IPv4 或 IPv6 地址。

- **host**{*IPv4_address* | *IPv6_address*} - 单一主机的 IPv4 或 IPv6 地址。例如，10.1.1.1 或 2001:DB8::0DB8:800:200C:417A。
- **subnet** {*IPv4_address IPv4_mask* | *IPv6_address*/*IPv6_prefix*} - 网络地址。对于 IPv4 子网，请在空格后添加掩码，例如，10.0.0.0 255.0.0.0。对于 IPv6，请将地址和前缀作为一个整体（不带空格），例如 2001:DB8:0:CD30::/60。
- **range***start_address end_address* - 地址的范围。可以指定 IPv4 或 IPv6 范围。请勿包含掩码或前缀。

示例：

```
hostname(config-network-object)# range 10.1.1.1 10.1.1.90
```

步骤 4 为对象 IP 地址配置 **dynamic PAT**。只能为给定对象定义单一 NAT 规则。

nat [(*real_ifc*,*mapped_ifc*)] **dynamic** {*mapped_inline_host_ip* | *mapped_obj* | **pat-pool** *mapped-obj* [**round-robin**] [**extended**] [**include-reserve**] [**block-allocation**] | **interface** [**ipv6**]} [**interface** [**ipv6**]]

其中：

- Interfaces -（对于桥接组成员接口需要填入。）指定实际 (*real_ifc*) 接口和映射 (*mapped_ifc*) 接口。确保包含圆括号。在路由模式下，如果没有指定实际接口和映射接口，则将使用所有接口。您也可以为一个或两个接口指定关键字 **any**（例如 any,outside），但 **any** 不适用于桥接组成员接口。
- Mapped IP address - 可以将映射 IP 地址指定为：
  - *mapped_inline_host_ip* - 内联主机地址。
  - *mapped_obj* - 定义为主机地址的网络对象。
  - **pat-pool** *mapped-obj* - 包含多个地址的网络对象或组。
  - **interface** [**ipv6**] - 使用映射接口的 IP 地址作为映射地址。如果指定**ipv6**，则稍后使用该接口的 IPv6 地址。对于此选项，必须为 *mapped_ifc* 配置一个特定接口。（当映射接口为桥接组成员时，无法指定 **interface**。）要使用接口 IP 地址时，必须使用此关键字；不能内联输入或作为对象输入。
- 对于 PAT 池，可以指定以下一个或多个选项：
  - **round-robin**- 为 PAT 池启用轮询地址分配。不使用轮询时，默认情况下，在使用下一个 PAT 地址前，将分配 PAT 地址的所有端口。轮询方法分配来自池中每个 PAT 地址的地址/端口，然后才返回再次使用第一个地址，接着是第二个地址，以此类推。
  - **extended**- 启用扩展 PAT。通过将目的地地址和端口纳入转换信息，相对于按 IP 地址，扩展 PAT 将按服务使用 65535 个端口。通常，创建 PAT 转换时，不考虑目的地端口和地址，因此限制为每个 PAT 地址 65535 个端口。例如，通过扩展 PAT，您可以创建在访问 192.168.1.7:23 时转到 10.1.1.1:1027 的转换，以及在访问 192.168.1.7:80 时转到 10.1.1.1:1027 的转换。
  - **include-reserve** - 包括保留的端口 1-1023，属于可用于地址转换的端口范围。如果不指定此选项，地址将仅被转换为 1024-65535 范围内的端口。
  - **block-allocation**- 启用端口块分配。对于运营商级或大规模 PAT，可以为每个主机分配一个端口块，而非由 NAT 每次分配一个端口转换。如果分配端口块，来自该主机的后续连接将使用该块中随机选定的新端口。如果主机将所有端口的活动连接置于基元块中，可根据需要分配更多块。只能在 1024-65535 范围内分配端口块。端口块分配与 **round-robin** 兼容，但无法使用 **extended** 选项。也无法使用接口 PAT 回退。
- Interface PAT fallback -（可选。）在主 PAT 地址后输入了 **interface** [**ipv6**] 关键字时，该关键字将启用接口 PAT 回退。主要 PAT 地址用尽后，接着将使用映射接口的 IP 地址。如果指定**ipv6**，则稍后使用该接口的 IPv6 地址。对于此选项，必须为 *mapped_ifc* 配置一个特定接口。（当映射接口为桥接组成员时，无法指定 **interface**。）

示例：

```
hostname(config-network-object)# nat (any,outside) dynamic interface
```

示例

以下示例配置动态 PAT，将 192.168.2.0 网络隐藏在地址 10.2.2.2 后面：

```
hostname(config)# object network my-inside-net
hostname(config-network-object)# subnet 192.168.2.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) dynamic 10.2.2.2
```

以下示例配置动态 PAT，将 192.168.2.0 网络隐藏在外部接口地址后面：

```
hostname(config)# object network my-inside-net
hostname(config-network-object)# subnet 192.168.2.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) dynamic interface
```

以下示例配置动态 PAT，使用 PAT 池将内部 IPv6 网络转换为外部 IPv4 网络：

```
hostname(config)# object network IPv4_POOL
hostname(config-network-object)# range 203.0.113.1 203.0.113.254
hostname(config)# object network IPv6_INSIDE
hostname(config-network-object)# subnet 2001:DB8::/96
hostname(config-network-object)# nat (inside,outside) dynamic pat-pool IPv4_POOL
```

配置动态两次 NAT

本节介绍如何为动态 PAT 配置两次 NAT。

过程

步骤 1 为源实际地址、源映射地址、目的实际地址和目的映射地址创建主机或范围网络对象（**object network** 命令）或网络对象组（**object-group network** 命令）。还可以将 FQDN 网络对象用于目标映射地址。

- 如果要转换所有源流量，可以跳过为源实际地址添加对象，转而在 **nat** 命令中指定 **any** 关键字。
- 如果要使用接口地址作为映射地址，可以跳过为源映射地址添加对象，转而在 **nat** 命令中指定 **interface** 关键字。
- 如果要配置仅支持端口转换的静态接口 NAT，则可跳过为目的映射地址添加对象，转而在 **nat** 命令中指定 **interface** 关键字。

如果使用对象，则对象或组不可以包含子网。对象必须定义主机，对于 PAT 池，则必须定义范围。组（对于 PAT 池）可以包含主机和范围。

步骤 2 （可选。）为目标实际端口和目标映射端口创建服务对象。

对于动态 NAT，只能对目标执行端口转换。服务对象可能同时包含源和目标端口，但在此情况下，将仅使用目标端口。系统将忽略您指定的源端口。

步骤 3 配置**动态 PAT**。

nat [(*real_ifc*,*mapped_ifc*)] [*line* | **after-auto** [*line*]] **source dynamic** {*real-obj* | **any**} {*mapped_obj* [**interface** [**ipv6**]] | **pat-pool** *mapped-obj* [**round-robin**] [**extended**] [**include-reserve**] [**block-allocation**] [**interface** [**ipv6**]] | **interface** [**ipv6**]} [**destination static** {*mapped_obj* | **interface** [**ipv6**]} *real_obj*] [**service** *mapped_dest_svc_obj real_dest_svc_obj*] [**unidirectional**] [**inactive**] [**description** *description*]

其中：

- Interfaces -（对于桥接组成员接口需要填入。）指定实际 (*real_ifc*) 接口和映射 (*mapped_ifc*) 接口。确保包含圆括号。在路由模式下，如果没有指定实际接口和映射接口，则将使用所有接口。您也可以为一个或两个接口指定关键字 **any** （例如 any,outside），但 **any** 不适用于桥接组成员接口。
- Section and Line -（可选。）默认情况下，NAT 规则将添加至 NAT 表的第 1 部分的末尾（请参阅 NAT 规则顺序，第 4 页）。如果要转而将规则添加至第 3 部分（位于网络对象 NAT 规则之后），则可使用 **after-auto** 关键字。可以使用 *line* 参数在适用部分的任意位置插入规则。
- 源地址：
  - Real - 网络对象、组或 **any** 关键字。如果要转换从实际接口流向映射接口的所有流量，请使用 **any** 关键字。
  - Mapped - 配置以下其中一项：
    - Network object - 包含主机地址的网络对象。
    - **pat-pool** *mapped-obj* - 包含多个地址的网络对象或组。
    - **interface** [**ipv6**] -（仅路由模式。）使用映射接口的 IP 地址作为映射地址（接口 PAT）。如果指定**ipv6**，则稍后使用该接口的 IPv6 地址。对于此选项，必须为 *mapped_ifc* 配置一个特定接口。（当映射接口为桥接组成员时，无法指定 **interface**。）如果使用 PAT 池或网络对象指定此关键字，则会启用接口 PAT 回退。PAT IP 地址用尽后，接着将使用映射接口的 IP 地址。

  对于 PAT 池，可以指定以下一个或多个选项：
    - **round-robin**- 为 PAT 池启用轮询地址分配。不使用轮询时，默认情况下，在使用下一个 PAT 地址前，将分配 PAT 地址的所有端口。轮询方法分配来自池中每个 PAT 地址的地址/端口，然后才返回再次使用第一个地址，接着是第二个地址，以此类推。
    - **extended**- 启用扩展 PAT。通过将目的地地址和端口纳入转换信息，相对于按 IP 地址，扩展 PAT 将按服务使用 65535 个端口。通常，创建 PAT 转换时，不考虑目的地端口和地址，因此限制为每个 PAT 地址 65535 个端口。例如，通过扩展 PAT，您可以创建在访问 192.168.1.7:23 时转到 10.1.1.1:1027 的转换，以及在访问 192.168.1.7:80 时转到 10.1.1.1:1027 的转换。

- **include-reserve** - 包括保留的端口 1-1023，属于可用于地址转换的端口范围。如果不指定此选项，地址将仅被转换为 1024-65535 范围内的端口。
- **block-allocation**- 启用端口块分配。对于运营商级或大规模 PAT，可以为每个主机分配一个端口块，而非由 NAT 每次分配一个端口转换。如果分配端口块，来自该主机的后续连接将使用该块中随机选定的新端口。如果主机将所有端口的活动连接置于基元块中，可根据需要分配更多块。只能在 1024-65535 范围内分配端口块。端口块分配与 **round-robin** 兼容，但无法使用 **extended** 选项。也无法使用接口 PAT 回退。

- 目标地址（可选）：
  - Mapped - 指定网络对象或组，或对于仅支持端口转换的静态接口 NAT（仅限非桥接组成员接口），指定 **interface** 关键字。如果指定**ipv6**，则稍后使用该接口的 IPv6 地址。如指定 **interface**，请务必也配置 **service** 关键字。对于此选项，必须为 *real_ifc* 配置特定接口。有关详细信息，请参阅支持端口转换的静态 NAT，第 32 页。
  - Real - 指定网络对象或组。对于身份 NAT，只需将相同的对象或组同时用于实际和映射地址。
- Destination port -（可选。）指定 **service** 关键字以及映射和实际服务对象。对于身份端口转换，只需相同的服务对象同时用于实际和映射端口。
- Unidirectional -（可选。）指定 **unidirectional**，以使目标地址无法发起流向源地址的流量。
- Inactive -（可选。）要使此规则变为非活动状态而不必删除命令，请使用 **inactive** 关键字。要将其重新激活，请重新输入没有 **inactive** 关键字的整个命令。
- Description -（可选。）使用 **description** 关键字可提供最多 200 个字符的说明。

示例：

```
hostname(config)# nat (inside,outside) source dynamic MyInsNet interface
destination static Server1 Server1
description Interface PAT for inside addresses when going to server 1
```

示例

以下示例为内部网络 192.168.1.0/24 配置访问外部 Telnet 服务器 209.165.201.23 时的接口 PAT，以及访问 203.0.113.0/24 网络上任何服务器时使用 PAT 池的动态 PAT。

```
hostname(config)# object network INSIDE_NW
hostname(config-network-object)# subnet 192.168.1.0 255.255.255.0

hostname(config)# object network PAT_POOL
hostname(config-network-object)# range 209.165.200.225 209.165.200.254

hostname(config)# object network TELNET_SVR
hostname(config-network-object)# host 209.165.201.23
```

```
hostname(config)# object service TELNET
hostname(config-service-object)# service tcp destination eq 23

hostname(config)# object network SERVERS
hostname(config-network-object)# subnet 203.0.113.0 255.255.255.0

hostname(config)# nat (inside,outside) source dynamic INSIDE_NW interface
destination static TELNET_SVR TELNET_SVR service TELNET TELNET
hostname(config)# nat (inside,outside) source dynamic INSIDE_NW pat-pool PAT_POOL
destination static SERVERS SERVERS
```

以下示例为内部网络 192.168.1.0/24 配置访问外部 IPv6 Telnet 服务器 2001:DB8::23 时的接口 PAT，以及访问 2001:DB8:AAAA::/96 网络上任何服务器时使用 PAT 池的动态 PAT。

```
hostname(config)# object network INSIDE_NW
hostname(config-network-object)# subnet 192.168.1.0 255.255.255.0

hostname(config)# object network PAT_POOL
hostname(config-network-object)# range 2001:DB8:AAAA::1 2001:DB8:AAAA::200

hostname(config)# object network TELNET_SVR
hostname(config-network-object)# host 2001:DB8::23

hostname(config)# object service TELNET
hostname(config-service-object)# service tcp destination eq 23

hostname(config)# object network SERVERS
hostname(config-network-object)# subnet 2001:DB8:AAAA::/96

hostname(config)# nat (inside,outside) source dynamic INSIDE_NW interface ipv6
destination static TELNET_SVR TELNET_SVR service TELNET TELNET
hostname(config)# nat (inside,outside) source dynamic INSIDE_NW pat-pool PAT_POOL
destination static SERVERS SERVERS
```

使用端口块分配配置 PAT

对于运营商级或大规模 PAT，您可以为每台主机分配端口块，而无需通过 NAT 一次分配一个端口转换（请参阅 RFC 6888）。如果分配端口块，来自该主机的后续连接将使用该块中随机选定的新端口。如果主机将所有端口的活动连接置于基元块中，可根据需要分配更多块。当使用块中端口的最后一个转换被删除时，系统将释放该块。

分配端口块的主要原因是为了减少日志记录。记录端口块分配，记录连接，但不会记录在端口块中创建的转换。另一方面，这样会使日志分析变得更加复杂。

只能在 1024-65535 范围内分配端口块。因此，如果应用需要较低的端口号 (1-1023)，它可能不起作用。例如，请求端口 22 (SSH) 的应用会获得 1024-65535 范围内和分配到主机的块范围内的映射端口。您可以创建一个单独的 NAT 规则，对于使用低端口号的应用不应用块分配；对于两次 NAT，请确保该规则位于块分配规则之前。

开始之前

NAT 规则的使用说明：

- 可以包括 **round-robin** 关键字，但不能包括 **extended**、**include-reserve** 或 **interface**（用于接口 PAT 回退）。此外，还允许其他源/目标地址和端口信息。
- 同所有NAT变更一样，如果要替换现有的规则，必须清除与被替换规则相关的转换，新规则才会生效。可以显式清除它们，也可以静待它们超时。在集群中运行时，您必须在整个集群中全局清除 xlate。

注释 如果要在常规 PAT 和块分配 PAT 规则之间切换，您必须先删除规则，然后再清除转换。然后，您可以创建新的对象 NAT 规则。否则，您将在 **show asp drop** 输出中看到 pat-port-block-state-mismatch 丢弃。

- 对于特定 PAT 池，必须为使用该池的所有规则指定（或不指定）块分配。不能在一个规则中分配块，而在另一个规则中不分配块。重叠的 PAT 池也不能混合块分配设置。此外，该池的静态 NAT 不能与端口转换规则重叠。

过程

步骤 1 （可选。）配置块分配大小，即每个块中的端口数。

xlate block-allocation size *value*

范围为 32-4096。默认值为 512。使用“no”形式可恢复默认值。

如果不使用默认值，请确保 64,512 能被您所选的大小整除（1024-65535 范围中的端口数)。否则，会出现无法使用的端口。例如，如果指定 100，会有 12 个未使用端口。

步骤 2 （可选。）配置每个主机可分配的最大块数。

xlate block-allocation maximum-per-host *number*

限制是针对每个协议，因此限制为 4 表示每个主机最多 4 个 UDP 块、4个 TCP 块和 4 个 ICMP 块。范围为 1-8，默认值为 4。使用“no”形式可恢复默认值。

步骤 3 （可选。）启用临时系统日志生成。

xlate block-allocation pba-interim-logging *seconds*

默认情况下，系统会在端口块创建和删除操作发生时生成系统日志消息。如果启用临时日志记录，系统会按您指定的时间间隔生成以下消息。这些消息会报告消息生成时所有已分配的活动端口块，包括协议（ICMP、TCP、UDP、源和目标接口与 IP 地址，以及端口块。可以指定 21600 至 604800 秒（6 小时至 7 天）的时间间隔。

%ASA-6-305017: Pba-interim-logging: Active *protocol* block of ports for translation from *real_interface*:*real_host_ip* to *mapped_interface*:*mapped_ip_address*/*start_port_num-end_port_num*

示例：

```
ciscoasa(config)# xlate block-allocation pba-interim-logging 21600
```

步骤 4 添加使用 PAT 池块分配的 NAT 规则。

- **对象 PAT**。

  nat [(*real_ifc*,*mapped_ifc*)] **dynamic pat-pool** *mapped-obj* **block-allocation**

  示例：

```
object network mapped-pat-pool
   range 10.100.10.1 10.100.10.2
object network src_host
   host 10.111.10.15
object network src_host
   nat (inside,outside) dynamic
pat-pool mapped-pat-pool block-allocation
```

- **两次 PAT**。

  nat [(*real_ifc*,*mapped_ifc*)] [*line* | **after-auto** [*line*]] **source dynamic** *real_obj* **pat-pool***mapped-obj* **block-allocation**

  示例：

```
object network mapped-pat-pool
   range 10.100.10.1 10.100.10.2
object network src_network
   subnet 10.100.10.0 255.255.255.0
nat (inside,outside) 1 source dynamic src_network
pat-pool mapped-pat-pool block-allocation
```

配置每会话 PAT 或多会话 PAT

默认情况下，所有 TCP PAT 流量和所有 UDP DNS 流量均使用每会话 PAT。要将多会话 PAT 用于流量，可配置每会话 PAT 规则：一条允许规则使用每会话 PAT，一条拒绝规则使用多会话 PAT。

每会话 PAT 可以提高 PAT 的可扩展性，对于集群，允许每个成员单元拥有自己的 PAT 连接；多会话 PAT 连接必须转发到主单元并且归控制单元所有。在每会话 PAT 会话结束时，ASA 将发送一条重置消息并立即删除转换。此重置会使结束节点立即释放连接，避免 TIME_WAIT 状态。另一方面，多会话 PAT 使用 PAT 超时，默认为 30 秒。

对于“命中并运行”流量，例如 HTTP 或 HTTPS，每会话 PAT 可以显著增加一个地址支持的连接速率。不使用每会话 PAT，IP 协议的一个地址的最大连接速率大约为每秒 2000。使用每会话 PAT，IP 协议的一个地址的连接速率为 65535/平均生命周期。

对于可受益于多会话 PAT 的流量（例如 H.323、SIP 或 Skinny），可以创建每会话拒绝规则来禁用每会话 PAT。但是，如果还想将每会话 PAT 用于这些协议所用的 UDP 端口，您必须为这些端口创建允许规则。

开始之前

默认情况下，已安装以下规则：

```
xlate per-session permit tcp any4 any4
xlate per-session permit tcp any4 any6
xlate per-session permit tcp any6 any4
xlate per-session permit tcp any6 any6
xlate per-session permit udp any4 any4 eq domain
xlate per-session permit udp any4 any6 eq domain
xlate per-session permit udp any6 any4 eq domain
xlate per-session permit udp any6 any6 eq domain
```

这些规则无法删除，无论手动创建什么规则，它们始终存在。因为会按顺序评估规则，所以可以忽略默认规则。例如，要完全忽略这些规则，可以添加以下规则：

```
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain
```

过程

创建允许或拒绝每会话 PAT 规则。此规则置于默认规则上方，但在任何其他手动创建的规则下方。确保按照所需的应用顺序创建规则。

xlate per-session {**permit** | **deny**} {**tcp** | **udp**} *source_ip* [*operator src_port*] *destination_ip* [*operator dest_port*]

对于源 IP 地址和目标 IP 地址，可以配置以下选项：

- **host** *ip_address* - 指定 IPv4 或 IPv6 主机地址。
- *ip_address mask* - 指定 IPv4 网络地址和子网掩码。
- *ipv6-address/prefix-length* - 指定 IPv6 网络地址和前缀。
- **any4** 和 **any6** - **any4** 指定纯 IPv4 流量；**any6** 则指定 any6 流量。

运算符与源或目标使用的端口号相匹配。默认为所有端口。允许的运算符如下所示：

- **lt** - 小于
- **gt** - 大于
- **eq** - 等于
- **neq** - 不等于

- **range** - 值的范围（包括边界值）。使用该操作符时，请指定两个端口编号，例如，**range 100 200**。

示例

以下示例为 H.323 流量创建拒绝规则，以便它使用多会话 PAT：

```
hostname(config)# xlate per-session deny tcp any4 209.165.201.7 eq 1720
hostname(config)# xlate per-session deny udp any4 209.165.201.7 range 1718 1719
```

以下示例通过允许将每会话 PAT 用于 SIP UDP 端口，启用了跨集群成员分配 SIP。每会话 PAT 是 SIP TCP 端口的默认值，因此除非您更改了默认规则，否则无需 TCP 规则。

```
hostname(config)# xlate per-session permit udp any4 any4 eq sip
```

静态 NAT

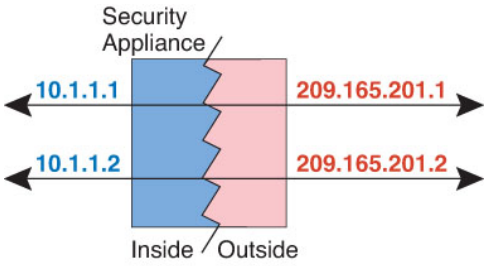
以下主题介绍静态 NAT 以及如何实施静态 NAT。

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 *5:* 静态 *NAT*



注释 如果需要，可以禁用双向性。

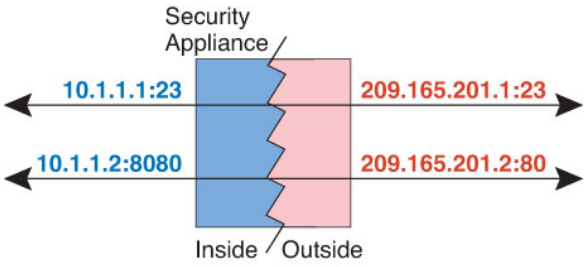
支持端口转换的静态 NAT

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 *6:* 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，对于两次 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)。有关如何配置此示例的详细信息，请参阅用于 FTP、HTTP 和 SMTP（支持端口转换的静态 NAT）的单一地址。

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

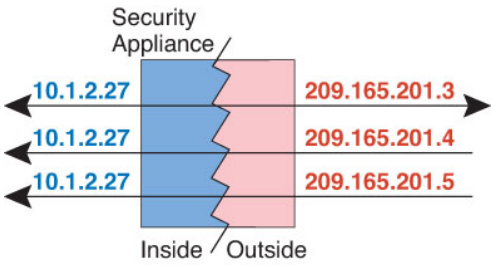
可以配置静态NAT，以将一个实际地址映射到一个接口地址/端口组合。例如，如果要将对设备外部接口的 Telnet 访问重定向至内部主机，则可以将内部主机 IP 地址/端口 23 映射到外部接口地址/端口 23。

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。

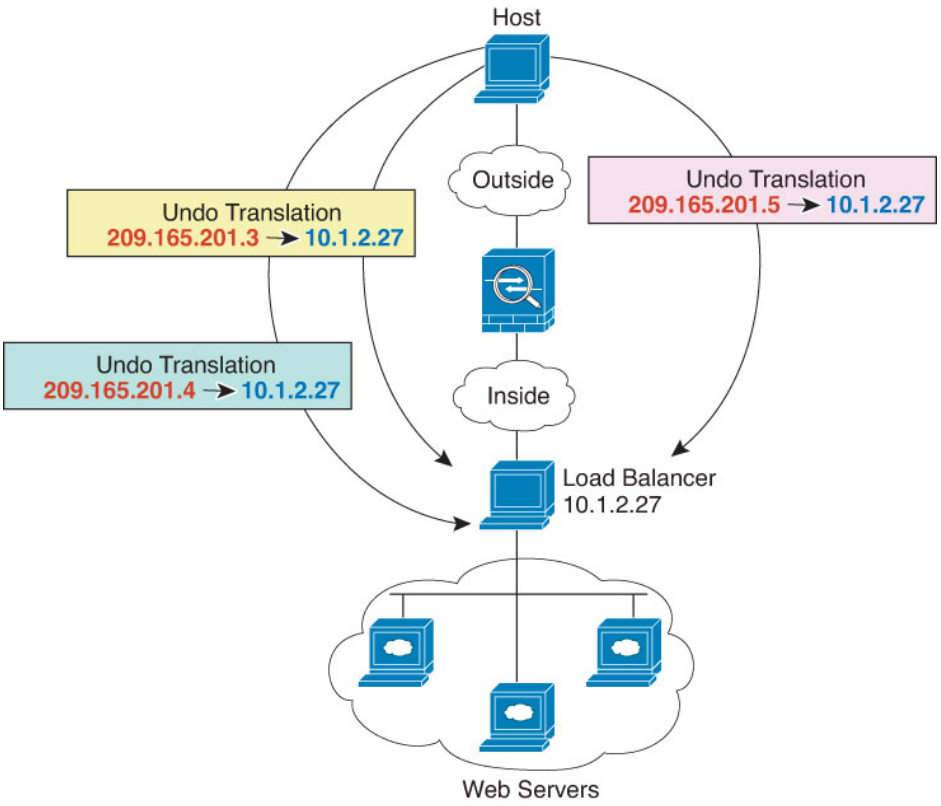
下图显示典型的一对多静态NAT场景。由于实际主机进行的发起的流量始终使用第一个映射地址，因此从技术上说，实际主机 IP/第一个映射 IP 的转换是唯一的双向转换。

图 *7:* 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。有关如何配置此示例的详细信息，请参阅具有多个映射地址的内部负载均衡器（静态 NAT，一对多）。

图 *8:* 一对多静态 *NAT* 示例



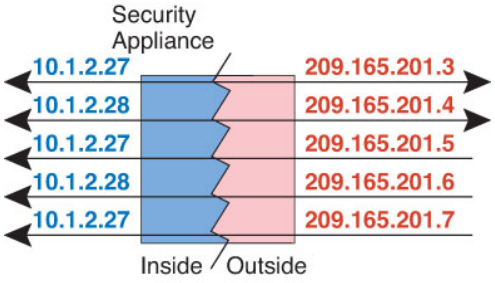
其他映射场景（不推荐）

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 *9:* 少对多静态 *NAT*

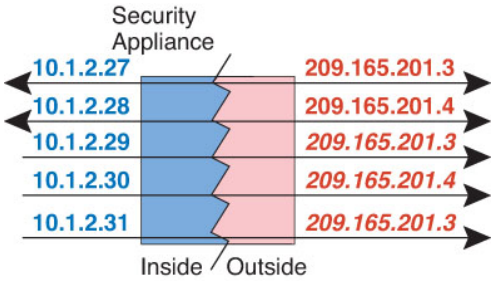


对于实际地址多于映射地址的多对少或多对一配置，映射地址会在实际地址用尽之前先用尽。仅最低实际 IP 地址和映射池之间的映射可以导致双向发起。剩余的更高的实际地址可以发起流量，但不能将流量发起到这些地址（由于五元组 [源 IP、目标 IP、源端口、目标端口、协议] 的唯一性，连接的返回流量会定向到正确的实际地址）。

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 *10:* 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。

配置静态网络对象 NAT 或支持端口转换的静态 NAT

本节介绍如何使用网络对象 NAT 配置静态 NAT 规则。

过程

步骤 1 （可选。）为映射地址创建网络对象（使用 **object network** 命令）或网络对象组（使用 **object-group network** 命令）。

- 如果不使用对象，可以配置内联地址，或者指定接口地址（对于带端口转换的静态 NAT）。
- 如果使用对象，对象或组可以包含主机、范围或子网。

步骤 2 创建或编辑要为其配置 NAT 的网络对象：**object network** *obj_name*

示例：

```
hostname(config)# object network my-host-obj1
```

步骤 3 （编辑具有正确地址的对象时，请跳过此步骤。）定义要转换的实际 IPv4 或 IPv6 地址。

- **host** {*IPv4_address* | *IPv6_address*} - 单台主机的 IPv4 或 IPv6 地址。例如，10.1.1.1 或 2001:DB8::0DB8:800:200C:417A。
- **subnet** {*IPv4_address IPv4_mask* | *IPv6_address/IPv6_prefix*} - 网络地址。对于 IPv4 子网，请在空格后添加掩码，例如，10.0.0.0 255.0.0.0。对于 IPv6，请将地址和前缀作为一个整体（不带空格），例如 2001:DB8:0:CD30::/60。
- **range** *start_address end_address* - 地址的范围。可以指定 IPv4 或 IPv6 范围。请勿包含掩码或前缀。

示例：

```
hostname(config-network-object)# subnet 10.2.1.0 255.255.255.0
```

步骤 4 为对象 IP 地址配置**静态 NAT**。只能为给定对象定义单一 NAT 规则。

nat [**(***real_ifc***,***mapped_ifc***)**] **static** {*mapped_inline_host_ip* | *mapped_obj* | **interface** [**ipv6**]} [**net-to-net**] [**dns** | **service** {**tcp** | **udp** | **sctp**} *real_port mapped_port*] [**no-proxy-arp**]

其中：

- Interfaces -（对于桥接组成员接口需要填入。）指定实际 (*real_ifc*) 接口和映射 (*mapped_ifc*) 接口。确保包含圆括号。在路由模式下，如果没有指定实际接口和映射接口，则将使用所有接口。您也可以为一个或两个接口指定关键字 **any**（例如 any,outside），但 **any** 不适用于桥接组成员接口。
- Mapped IP address - 可以将映射 IP 地址指定为以下任一地址：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。请参阅静态 NAT，第 31 页。
  - *mapped_inline_host_ip* - 内联主机 IP 地址。此项为主机对象提供一对一映射。对于子网对象，内联主机地址使用的是相同的掩码，而映射的内联主机子网中的地址则是一一对应的。对于范围对象，映射地址包括范围对象中相同数量的主机，从映射主机地址开始。例如，如果实际地址定义为 10.1.1.1 到 10.1.1.6 的范围，并且将 172.20.1.1 指定为映射地址，则映射范围将包括 172.20.1.1 到 172.20.1.6。对于 NAT46 或 NAT66 转换，此项可以是 IPv6 网络地址。
  - *mapped_obj* - 现有网络对象或组。要为一系列 IP 地址执行一对一映射，请选择包含具有相同地址数量的范围的对象。

- **interface** -（仅限支持端口转换的静态 NAT。) 映射接口的 IP 地址用作映射地址。如果指定 **ipv6**，则将使用接口的 IPv6 地址。对于此选项，必须为 *mapped_ifc* 配置特定接口。（当映射接口为桥接组成员时，无法指定 **interface**。）要使用接口 IP 地址时，必须使用此关键字；不能内联输入或作为对象输入。另请确保配置 **service** 关键字。

- Net-to-net -（可选。）对于 NAT 46，指定 **net-to-net** 以将第一个 IPv4 地址转换为第一个 IPv6 地址，第二个 IPv4 地址转换为第二个 IPv6 地址，以此类推。如不使用此选项，则将使用 IPv4 嵌入式方法。对于一对一转换，必须使用此关键字。
- DNS -（可选）。**dns** 关键字转换 DNS 应答。确保启用 DNS 检测（默认情况下启用）。有关详细信息，请参阅使用 NAT 重写 DNS 查询和响应。
- Port translation -（仅带端口转换的静态 NAT。）指定具有所需端口关键字的 **service** 以及实际与映射端口。可以输入端口号或已知的端口名称（例如 **http**）。
- No Proxy ARP -（可选。）指定 **no-proxy-arp**，为映射 IP 地址的传入数据包禁用代理 ARP。有关可能需要禁用代理 ARP 的情况的信息，请参阅映射地址和路由。

示例：

```
hostname(config-network-object)#
nat (inside,outside) static MAPPED_IPS service tcp 80 8080
```

示例

以下示例为内部的实际主机 10.1.1.1 到外部的 10.2.2.2 配置静态 NAT，启用 DNS 重写。

```
hostname(config)# object network my-host-obj1
hostname(config-network-object)# host 10.1.1.1
hostname(config-network-object)# nat (inside,outside) static 10.2.2.2 dns
```

以下示例为内部的实际主机 10.1.1.1 到外部的 10.2.2.2 配置使用映射对象的静态 NAT。

```
hostname(config)# object network my-mapped-obj
hostname(config-network-object)# host 10.2.2.2

hostname(config-network-object)# object network my-host-obj1
hostname(config-network-object)# host 10.1.1.1
hostname(config-network-object)# nat (inside,outside) static my-mapped-obj
```

以下示例为 TCP 端口 21 上的 10.1.1.1 到端口 2121 上的外部接口配置支持端口转换的静态 NAT。

```
hostname(config)# object network my-ftp-server
hostname(config-network-object)# host 10.1.1.1
hostname(config-network-object)# nat (inside,outside) static interface service tcp 21 2121
```

以下示例将内部 IPv4 网络映射到外部 IPv6 网络。

```
hostname(config)# object network inside_v4_v6
hostname(config-network-object)# subnet 10.1.1.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) static 2001:DB8::/96
```

以下示例将内部 IPv6 网络映射到外部 IPv6 网络。

```
hostname(config)# object network inside_v6
hostname(config-network-object)# subnet 2001:DB8:AAAA::/96
hostname(config-network-object)# nat (inside,outside) static 2001:DB8:BBBB::/96
```

配置静态两次 NAT 或支持端口转换的静态 NAT

本节介绍如何使用两次 NAT 配置静态 NAT 规则。

过程

步骤 1 为源实际地址、源映射地址、目标实际地址和目标映射地址创建主机或范围网络对象（使用 **object network** 命令）或网络对象组（使用 **object-group network** 命令）。还可以将 FQDN 网络对象用于目标映射地址。

- 如果仅要配置支持端口转换的源静态接口 NAT，则可跳过为源映射地址添加对象，转而在 **nat** 命令中指定 **interface** 关键字。
- 如果要配置仅支持端口转换的静态接口 NAT，则可跳过为目标映射地址添加对象，转而在 **nat** 命令中指定 **interface** 关键字。

如果创建对象，请注意以下准则：

- 映射对象或组可能包含主机、范围或子网。
- 静态映射通常为一对一，因此实际地址的数量与映射地址相同。然而，如果需要，可拥有不同的数量。有关详细信息，请参阅静态 NAT，第 31 页。

步骤 2 （可选。）为以下端口创建服务对象：

- 源或目标实际端口
- 源或目标映射端口

服务对象可同时包含源和目标端口；然而，应为两个服务对象指定源或目标端口。如果应用使用固定的源端口（如某些 DNS 服务器），则您只能同时指定源和目标端口；然而，很少使用固定源端口。例如，如果要转换源主机的端口，则请配置源服务。

步骤 3 配置**静态 NAT**。

nat [**(***real_ifc*,*mapped_ifc***)**] [*line* | {**after-object** [*line*]}] **source static** *real_ob* [*mapped_obj* | **interface** [**ipv6**]] [**destination static** {*mapped_obj* | **interface** [**ipv6**]} *real_obj*] [**service** *real_src_mapped_dest_svc_obj mapped_src_real_dest_svc_obj*] [**net-to-net**] [**dns**] [**unidirectional** | **no-proxy-arp**] [**inactive**] [**description** *desc*]

其中：

- Interfaces -（对于桥接组成员接口需要填入。）指定实际 (*real_ifc*) 接口和映射 (*mapped_ifc*) 接口。确保包含圆括号。在路由模式下，如果没有指定实际接口和映射接口，则将使用所有接口。您也可以为一个或两个接口指定关键字 **any**（例如 any、outside），但 **any** 不适用于桥接组成员接口。
- Section and Line -（可选。）默认情况下，NAT 规则将添加至 NAT 表的第 1 部分的末尾（请参阅 NAT 规则顺序，第 4 页）。如果要转而将规则添加至第 3 部分（位于网络对象 NAT 规则之后），则可使用 **after-auto** 关键字。可以使用 *line* 参数在适用部分的任意位置插入规则。
- 源地址：
  - Real - 指定网络对象或组。请勿使用 **any** 关键字，此关键字用于身份 NAT。
  - Mapped - 指定不同的网络对象或组。仅可为支持端口转换的静态接口 NAT 指定 **interface** 关键字。如果指定 **ipv6**，则将使用接口的 IPv6 地址。如果指定 **interface**，请务必也配置 **service** 关键字（在此情况下，服务对象应仅包括源端口）。对于此选项，必须为 *mapped_ifc* 配置特定接口。（当映射接口为桥接组成员时，无法指定 **interface**。）有关详细信息，请参阅支持端口转换的静态 NAT，第 32 页。
- 目标地址（可选）：
  - Mapped - 指定网络对象或组，或对于仅支持端口转换的静态接口 NAT，指定 **interface** 关键字。如果指定 **ipv6**，则将使用接口的 IPv6 地址。如果指定 **interface**，请务必也配置 **service** 关键字（在此情况下，服务对象应仅包括目标端口）。对于此选项，必须为 *real_ifc* 配置特定接口。（当映射接口为桥接组成员时，无法指定 **interface**。）
  - Real - 指定网络对象或组。对于身份 NAT，只需将相同的对象或组同时用于实际和映射地址。
- Ports -（可选。）指定 **service** 关键字以及实际和映射服务对象。对于源端口转换，对象必须指定源服务。对于源端口转换，命令中服务对象的顺序为 **service** *real_obj mapped_obj*。对于目标端口转换，对象必须指定目标服务。对于目标端口转换，服务对象的顺序为 **service** *mapped_obj real_obj*。在极少数的情况下，会在对象中同时指定源和目标端口，第一个服务对象包含实际源端口/映射目标端口；第二个服务对象包含映射源端口/实际目标端口。对于身份端口转换，只需将相同的服务对象同时用于实际和映射端口（源和/或目标端口，具体取决于配置）。
- Net-to-net -（可选。）对于 NAT 46，指定 **net-to-net** 以将第一个 IPv4 地址转换为第一个 IPv6 地址，第二个 IPv4 地址转换为第二个 IPv6 地址，以此类推。如不使用此选项，则将使用 IPv4 嵌入式方法。对于一对一转换，必须使用此关键字。
- DNS -（可选；适用于源专用规则。）**dns** 关键字转换 DNS 应答。确保启用 DNS 检测（默认情况下启用）。如配置 **destination** 地址，则无法配置 **dns** 关键字。有关详细信息，请参阅 使用 NAT 重写 DNS 查询和响应。

- Unidirectional -（可选。）指定 **unidirectional**，以使目标地址无法发起流向源地址的流量。
- No Proxy ARP -（可选。）指定 **no-proxy-arp**，为映射 IP 地址的传入数据包禁用代理 ARP。有关详细信息，请参阅映射地址和路由。
- Inactive -（可选。）要使此规则变为非活动状态而不必删除命令，请使用 **inactive** 关键字。要将其重新激活，请重新输入没有 **inactive** 关键字的整个命令。
- Description -（可选。）使用 **description** 关键字可提供最多 200 个字符的说明。

示例：

```
hostname(config)# nat (inside,dmz) source static MyInsNet MyInsNet_mapped
destination static Server1 Server1 service REAL_SRC_SVC MAPPED_SRC_SVC
```

示例

以下示例展示支持端口转换的静态接口 NAT 的用途。外部主机通过目标端口 65000 至 65004 连接至外部接口 IP 地址，从而访问内部 FTP 服务器。流量通过 65004 未经转换地发送至位于 192.168.10.100:6500 的内部 FTP 服务器。请注意，应在服务对象中指定源端口范围（而不是指定目标端口），因为要在命令中将源地址和端口转换为已标识状态；目标端口为“any”。由于静态 NAT 是双向的，“源”和“目标”主要指命令关键字；数据包中的实际源和目标地址与端口取决于发送数据包的主机。在此示例中，连接源自外部，通向内部，因此，FTP 服务器的“源”地址和端口实际是源数据包中的目标地址和端口。

```
hostname(config)# object service FTP_PASV_PORT_RANGE
hostname(config-service-object)# service tcp source range 65000 65004

hostname(config)# object network HOST_FTP_SERVER
hostname(config-network-object)# host 192.168.10.100

hostname(config)# nat (inside,outside) source static HOST_FTP_SERVER interface
service FTP_PASV_PORT_RANGE FTP_PASV_PORT_RANGE
```

以下示例显示访问 IPv6 网络时从一个 IPv6 网络 到另一个 IPv6 的静态转换，以及 访问 IPv4 网络时到 IPv4 PAT 池的动态 PAT 转换：

```
hostname(config)# object network INSIDE_NW
hostname(config-network-object)# subnet 2001:DB8:AAAA::/96

hostname(config)# object network MAPPED_IPv6_NW
hostname(config-network-object)# subnet 2001:DB8:BBBB::/96

hostname(config)# object network OUTSIDE_IPv6_NW
hostname(config-network-object)# subnet 2001:DB8:CCCC::/96

hostname(config)# object network OUTSIDE_IPv4_NW
hostname(config-network-object)# subnet 10.1.1.0 255.255.255.0

hostname(config)# object network MAPPED_IPv4_POOL
hostname(config-network-object)# range 10.1.2.1 10.1.2.254
```

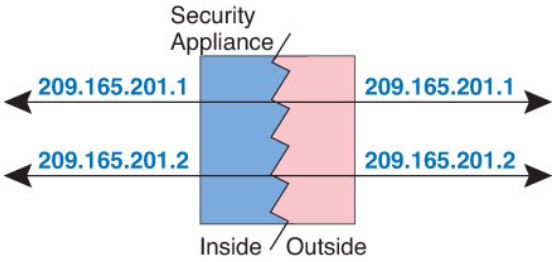
```
hostname(config)# nat (inside,outside) source static INSIDE_NW MAPPED_IPv6_NW
destination static OUTSIDE_IPv6_NW OUTSIDE_IPv6_NW
hostname(config)# nat (inside,outside) source dynamic INSIDE_NW pat-pool MAPPED_IPv4_POOL
destination static OUTSIDE_IPv4_NW OUTSIDE_IPv4_NW
```

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。身份 NAT 是远程访问访问 VPN 所必需的，需要使客户端流量免于 NAT。

下图显示典型的身份 NAT 场景。

图 *11: 身份 NAT*



以下主题介绍如何配置身份 NAT。

配置身份网络对象 PAT

本节介绍如何使用网络对象 NAT 配置身份 NAT 规则。

过程

步骤 1 （可选。）为映射地址创建网络对象（使用 **object network** 命令）或网络对象组（使用 **object-group network** 命令）。

- 如果不使用对象，可以配置内联地址。
- 如果使用对象，对象必须匹配要转换的实际地址。

步骤 2 创建或编辑要为其配置 NAT 的网络对象：**object network** *obj_name*

对象必须不同于用于映射地址的对象，虽然每个对象中的内容必须相同。

示例：

```
hostname(config)# object network my-host-obj1
```

步骤 3 （编辑具有正确地址的对象时，请跳过此步骤。）定义要转换的实际 IPv4 或 IPv6 地址。

- **host** {*IPv4_address* | *IPv6_address*} - 单台主机的 IPv4 或 IPv6 地址。例如，10.1.1.1 或 2001:DB8::0DB8:800:200C:417A。
- **subnet** {*IPv4_address IPv4_mask* | *IPv6_address/IPv6_prefix*} - 网络地址。对于 IPv4 子网，请在空格后添加掩码，例如，10.0.0.0 255.0.0.0。对于 IPv6，请将地址和前缀作为一个整体（不带空格），例如 2001:DB8:0:CD30::/60。
- **range** *start_address end_address* - 地址的范围。可以指定 IPv4 或 IPv6 范围。请勿包含掩码或前缀。

示例：

```
hostname(config-network-object)# subnet 10.2.1.0 255.255.255.0
```

步骤 4 为对象 IP 地址配置**身份 NAT**。只能为给定对象定义单一 NAT 规则。

nat [**(***real_ifc***,***mapped_ifc***)**] **static** {*mapped_inline_host_ip* | *mapped_obj*} [**no-proxy-arp**] [**route-lookup**]

其中：

- Interfaces -（对于桥接组成员接口需要填入。）指定实际 (*real_ifc*) 接口和映射 (*mapped_ifc*) 接口。确保包含圆括号。在路由模式下，如果没有指定实际接口和映射接口，则将使用所有接口。您也可以为一个或两个接口指定关键字 **any**（例如 any、outside），但 **any** 不适用于桥接组成员接口。
- Mapped IP addresses - 确保为映射地址和实际地址配置相同的 IP 地址。使用以下选项之一：
  - *mapped_inline_host_ip* - 内联主机 IP 地址。对于主机对象，请指定相同的地址。对于范围对象，请指定实际范围中的第一个地址（将使用范围中的相同地址数量）。对于子网对象，请指定实际子网中的任何地址（将使用子网中的所有地址）。
  - *mapped_obj* - 包含与实际对象相同地址的网络对象或组。
- No Proxy ARP -（可选。）指定 **no-proxy-arp**，为映射 IP 地址的传入数据包禁用代理 ARP。有关可能需要禁用代理 ARP 的情况的信息，请参阅映射地址和路由。
- Route lookup -（仅路由模式；已指定接口。）指定 **route-lookup** 以使用路由查找而不使用 NAT 命令中指定的接口确定出口接口。有关详细信息，请参阅确定出口接口。

示例：

```
hostname(config-network-object)# nat (inside,outside) static MAPPED_IPS
```

示例

以下示例使用内联映射地址将主机地址映射到它本身：

```
hostname(config)# object network my-host-obj1
hostname(config-network-object)# host 10.1.1.1
hostname(config-network-object)# nat (inside,outside) static 10.1.1.1
```

以下示例使用网络对象 将主机地址映射到它本身：

```
hostname(config)# object network my-host-obj1-identity
hostname(config-network-object)# host 10.1.1.1

hostname(config-network-object)# object network my-host-obj1
hostname(config-network-object)# host 10.1.1.1
hostname(config-network-object)# nat (inside,outside) static my-host-obj1-identity
```

配置身份两次 NAT

本节介绍如何使用两次 NAT 配置身份 NAT 规则。

过程

步骤 1 为源实际地址（通常应为源映射地址使用相同对象）、目标实际地址和目标映射地址创建主机或范围网络对象（使用 **object network** 命令）或网络对象组（使用 **object-group network** 命令）。还可以将 FQDN 网络对象用于目标映射地址。

- 如果要为所有地址执行身份 NAT，则可跳过为源实际地址创建对象，转而在 **nat** 命令中使用关键字 **any any**。
- 如果要配置仅支持端口转换的静态接口 NAT，则可跳过为目标映射地址添加对象，转而在 **nat** 命令中指定 **interface** 关键字。

如果创建对象，请注意以下准则：

- 映射对象或组可能包含主机、范围或子网。
- 实际源对象和映射源对象必须匹配。可以为这二者使用相同对象，也可以单独创建包含相同 IP 地址的对象。

步骤 2 （可选。）为以下端口创建服务对象：

- 源或目标实际端口
- 源或目标映射端口

服务对象可同时包含源和目标端口；然而，应为两个服务对象指定源或目标端口。如果应用使用固定的源端口（如某些 DNS 服务器），则您只能同时指定源和目标端口；然而，很少使用固定源端口。例如，如果要转换源主机的端口，则请配置源服务。

步骤 3 配置**身份 NAT**。

nat [(*real_ifc*,*mapped_ifc*)] [*line* | {**after-object** [*line*]}] **source static** {*nw_obj nw_obj* | **any any**} [**destination static** {*mapped_obj* | **interface** [**ipv6**]} *real_obj*] [**service** *real_src_mapped_dest_svc_obj mapped_src_real_dest_svc_obj*] [**no-proxy-arp**] [**route-lookup**] [**inactive**] [**description** *desc*]

其中：

- Interfaces -（对于桥接组成员接口需要填入。）指定实际 (*real_ifc*) 接口和映射 (*mapped_ifc*) 接口。确保包含圆括号。在路由模式下，如果没有指定实际接口和映射接口，则将使用所有接口。您也可以为一个或两个接口指定关键字 **any**（例如 any、outside），但 **any** 不适用于桥接组成员接口。
- Section and Line -（可选。）默认情况下，NAT 规则将添加至 NAT 表的第 1 部分的末尾（请参阅 NAT 规则顺序，第 4 页）。如果要转而将规则添加至第 3 部分（位于网络对象 NAT 规则之后），则可使用 **after-auto** 关键字。可以使用 *line* 参数在适用部分的任意位置插入规则。
- Source addresses - 同时为实际和映射地址指定网络对象、组或 **any** 关键字。
- 目标地址（可选）：
  - Mapped - 指定网络对象或组，或对于仅支持端口转换的静态接口 NAT，指定 **interface** 关键字。如果指定 **ipv6**，则将使用接口的 IPv6 地址。如果指定 **interface**，请务必也配置 **service** 关键字（在此情况下，服务对象应仅包括目标端口）。对于此选项，必须为 *real_ifc* 配置特定接口。（当实际接口为桥接组成员时，无法指定 **interface**。）
  - Real - 指定网络对象或组。对于身份 NAT，只需将相同的对象或组同时用于实际和映射地址。
- Ports -（可选。）指定 **service** 关键字以及实际和映射服务对象。对于源端口转换，对象必须指定源服务。对于源端口转换，命令中服务对象的顺序为 **service** *real_obj mapped_obj*。对于目标端口转换，对象必须指定目标服务。对于目标端口转换，服务对象的顺序为 **service** *mapped_obj real_obj*。在极少数的情况下，会在对象中同时指定源和目标端口，第一个服务对象包含实际源端口/映射目标端口；第二个服务对象包含映射源端口/实际目标端口。对于身份端口转换，只需将相同的服务对象同时用于实际和映射端口（源和/或目标端口，具体取决于配置）。
- No Proxy ARP -（可选。）指定 **no-proxy-arp**，为映射 IP 地址的传入数据包禁用代理 ARP。有关详细信息，请参阅映射地址和路由。
- Route lookup -（可选、仅路由模式、已指定接口。）指定 **route-lookup** 以使用路由查找而不使用 NAT 命令中指定的接口确定出口接口。有关详细信息，请参阅确定出口接口。
- Inactive -（可选。）要使此规则变为非活动状态而不必删除命令，请使用 **inactive** 关键字。要将其重新激活，请重新输入没有 **inactive** 关键字的整个命令。
- Description -（可选。）使用 **description** 关键字可提供最多 200 个字符的说明。

示例：

```
hostname(config)# nat (inside,outside) source static MyInsNet MyInsNet
destination static Server1 Server1
```

监控 NAT

要监控 NAT，请使用以下命令：

- **show nat**

  显示 NAT 统计信息，包括每条 NAT 规则的命中信息。

- **show nat pool**

  显示 NAT 池统计信息，包括已分配的地址和端口，及其分配次数。

- **show running-config nat**

  显示 NAT 配置。不能使用 **show running-config object** 查看对象 NAT 规则。当使用无修饰符的 show running-config 命令时，包含 NAT 规则的对象会显示两次，第一次随基本地址配置一起显示，然后在使用 NAT 规则的对象配置中显示一次。完整的对象不与地址和 NAT 规则作为整体一起显示。

- **show xlate**

  显示当前 NAT 会话信息。

NAT 的历史记录

功能名称	平台版本	说明
网络对象 NAT	8.3(1)	为网络对象 IP 地址配置 NAT。 引入或修改了以下命令：**nat**（对象网络配置模式）、**show nat**、**show xlate**、**show nat pool**。
两次 NAT	8.3(1)	两次 NAT 可供您在单一规则中同时标识源和目标地址。 修改或引入了以下命令：**nat**、**show nat**、**show xlate**、**show nat pool**。

功能名称	平台版本	说明
身份 NAT 可配置代理 ARP 和路由查找	8.4(2)/8.5(1)	在身份 NAT 的更早版本中，代理 ARP 被禁用，始终使用路由查找确定出口接口。无法配置这些设置。在 8.4(2) 及更高版本中，身份 NAT 的默认行为已更改为匹配其他静态 NAT 配置的行为：在默认情况下，代理 ARP 已启用，并且 NAT 配置确定出口接口（如已指定）。您可以原样保留这些设置，或者单独启用或禁用这些设置。请注意，现在您也可以为常规静态 NAT 禁用代理 ARP。 对于 8.3 之前版本的配置，NAT 免除规则（**nat 0 access-list** 命令）至 8.4(2) 及更高版本的迁移现包含以下关键字，以禁用代理 ARP 并使用路由查找：**no-proxy-arp** 和 **route-lookup**。用于迁移至 8.3(2) 和 8.4(1) 的 **unidirectional** 关键字不再用于迁移。从 8.3(1)、8.3(2) 和 8.4(1) 升级至 8.4(2) 时，所有身份 NAT 配置现包含 **no-proxy-arp** 和 **route-lookup** 关键字，以便维持现有功能。**unidirectional** 关键字已删除。 修改了以下命令：**nat static** [**no-proxy-arp**] [**route-lookup**]。
PAT 池和轮询地址分配	8.4(2)/8.5(1)	现在，您可以指定 PAT 地址池，而不是单一地址。或者还可以启用 PAT 地址的轮询分配，而不是先使用 PAT 地址上的所有端口，然后再使用池中的下一个地址。这些功能有助于防止来自单一 PAT 地址的大量连接显示为 DoS 攻击的一部分，并使大量 PAT 地址的配置过程更轻松。 修改了以下命令：**nat dynamic** [**pat-pool** *mapped_object* [**round-robin**]] 和 **nat source dynamic** [**pat-pool** *mapped_object* [**round-robin**]]。
轮询 PAT 池分配技术使用现有主机的相同 IP 地址	8.4(3)	组合使用 PAT 池与轮询分配时，如果主机拥有现有连接，且有端口可用，则来自该主机的后续连接将使用相同的 PAT IP 地址。 未修改任何命令。 此功能在 *8.5(1)* 或 *8.6(1)* 中不可用。

功能名称	平台版本	说明
用于 PAT 池的不分段 PAT 端口范围	8.4(3)	如果可用，实际源端口号将用于映射端口。然而，如果实际端口不可用，将默认从与实际端口号相同的端口范围选择映射端口：0 至 511、512 至 1023 以及 1024 至 65535。因此，1024 以下的端口只有一个小 PAT 池。 如果大量流量使用较小的端口范围，在使用 PAT 池时，现可指定使用以下不分段端口范围，代替三个分段大小不等的端口范围：1024 至 65535，或 1 至 65535。 修改了以下命令：**nat dynamic** [**pat-pool** *mapped_object* [**flat** [**include-reserve**]]] 和 **nat source dynamic** [**pat-pool** *mapped_object* [**flat** [**include-reserve**]]]。 此功能在 *8.5(1)* 或 *8.6(1)* 中不可用。
用于 PAT 池的扩展 PAT	8.4(3)	每个 PAT IP 地址允许最多 65535 个端口。如果 65535 个端口不能提供足够的转换，则现可启用适合 PAT 池的扩展 PAT。通过将目标地址和端口纳入转换信息，相对于按 IP 地址，扩展 PAT 将按服务使用 65535 个端口。 修改了以下命令：**nat dynamic** [**pat-pool** *mapped_object* [**extended**]] 和 **nat source dynamic** [**pat-pool** *mapped_object* [**extended**]]。 此功能在 *8.5(1)* 或 *8.6(1)* 中不可用。

功能名称	平台版本	说明
自动 NAT 规则，可将 VPN 对等体的本地 IP 地址转换回对等体的实际 IP 地址	8.4(3)	在极少数情况下，您可能要在内部网络上使用 VPN 对等体的实际 IP 地址，而非已分配的本地 IP 地址。通常在使用 VPN 的情况下，对等体会获得分配的本地 IP 地址以访问内部网络。但是，例如在内部服务器和网络安全基于对等体的实际 IP 地址情况下，可能要将本地 IP 地址重新转换为对等体的实际公有 IP 地址。 可以在每个隧道组一个接口的基础上启用此功能。当VPN会话已建立或断开连接时，动态添加或删除对象 NAT 规则。可使用 **show nat** 命令查看这些规则。 由于路由问题，我们不建议使用此功能，除非您知道自己需要此功能；请联系思科 TAC 确认网络的功能兼容性。请参阅以下限制： • 仅支持 Cisco IPsec 和 Secure Client。 • 流向公共 IP 地址的返回流量必须路由回 ASA，以便应用 NAT 策略和 VPN 策略。 • 不支持负载均衡（由于路由问题）。 • 不支持漫游（公共 IP 更改）。 引入了以下命令：**nat-assigned-to-public-ip** *interface*（tunnel-group general-attributes 配置模式）。
NAT 支持 IPv6	9.0(1)	NAT 现在支持 IPv6 流量，以及 IPv4 和 IPv6 之间的转换。在透明模式下，不支持 IPv4 和 IPv6 之间的转换。 修改了以下命令：**nat**（全局和对象网络配置模式）、**show nat**、**show nat pool**、**show xlate**。
NAT 支持反向 DNS 查找	9.0(1)	在为 NAT 规则启用了 DNS 检测的情况下使用 IPv4 NAT、IPv6 NAT 和 NAT64 时，NAT 现支持为反向 DNS 查找转换 DNS PTR 记录。

功能名称	平台版本	说明
每会话 PAT	9.0(1)	每会话 PAT 功能可以提高 PAT 的可扩展性，对于集群，允许每个成员单元拥有自己的 PAT 连接；多会话 PAT 连接必须转发到主单元并且归控制单元所有。在每会话 PAT 会话结束时，ASA 将发送一条重置消息并立即删除转换。此重置会使结束节点立即释放连接，避免 TIME_WAIT 状态。另一方面，多会话 PAT 使用 PAT 超时，默认为 30 秒。对于“命中并运行”的数据流，例如 HTTP 或 HTTPS，每会话功能可以显著提高一个地址支持的连接速度。不使用每会话功能时，一个用于 IP 协议的地址的最大连接速率约为每秒 2000。在使用每会话功能的情况下，对于 IP 协议，一个地址的连接速率为 65535/*average-lifetime*。 默认情况下，所有 TCP 流量和 UDP DNS 流量都使用每会话 PAT xlate。对于需要多会话 PAT 的流量，如 H.323、SIP 或 Skinny，可通过创建每会话拒绝规则来禁用每会话 PAT。 引入了以下命令：**xlate per-session**、**show nat pool**。
NAT 规则引擎上的事务提交模式	9.3(1)	启用时，NAT 规则更新将在规则编译完成后应用，而不影响规则匹配性能。 我们已将 **nat** 关键字添加至以下命令：**asp rule-engine transactional-commit**、**show running-config asp rule-engine transactional-commit**、**clear configure asp rule-engine transactional-commit**。 我们向以下屏幕中添加了 NAT：Configuration > Device Management > Advanced > Rule Engine。
对运营商级 NAT 的改进	9.5(1)	对于运营商级或大规模 PAT，您可以为每台主机分配端口块，而无需通过 NAT 一次分配一个端口转换（请参阅 RFC 6888）。 添加了以下命令：**xlate block-allocation size**、**xlate block-allocation maximum-per-host**。向 **nat** 命令中添加了 **block-allocation** 关键词。
SCTP 的 NAT 支持	9.5(2)	现在，可以在静态网络对象 NAT 规则中指定 SCTP 端口。建议不要在静态两次 NAT 中使用 SCTP。动态 NAT/PAT 不支持 SCTP。 修改了以下命令：**nat static** (object)。

功能名称	平台版本	说明
NAT 端口块分配的临时日志。	9.12(1)	当对 NAT 启用端口块分配功能后，系统会在端口块创建和删除操作发生时生成系统日志消息。如果启用临时日志，系统会按您指定的时间间隔生成消息 305017。这些消息会报告消息生成时所有已分配的活动端口块，包括协议（ICMP、TCP、UDP、源和目标接口与 IP 地址，以及端口块。 添加了以下命令：**xlate block-allocation pba-interim-logging** *seconds*。
集群中对PAT地址分配的更改。PAT 池 **flat** 选项现在已默认启用，并且不可配置。	9.15(1)	更改PAT地址分配给集群成员的方式。以前，地址是分配给集群成员的，因此您的PAT池每个集群成员至少需要一个地址。现在，控制设备改为将每个PAT池地址划分为大小相等的端口块，并在集群成员之间分配它们。每个成员都有相同 PAT 地址的端口块。因此，您可以根据通常需要 PAT 的连接数量，将 PAT 池的大小减小到一个 IP 地址。能在 1024-65535 范围内，在 512 端口块中分配端口块。配置 PAT 池规则时，可以选择在此块分配中包含保留端口 1-1023。例如，在4节点集群中，每个节点获得32个数据块，与每个PAT池IP地址处理65535个连接的单个节点相比，它能够处理每个PAT池IP地址16384个连接。 作为此更改的一部分，所有系统的PAT池（无论是独立系统还是在集群中运行）现在都使用1023-65535的平面端口范围。以前，您可以通过在 PAT 池 **flat** 规则中包含关键字，选择性地使用平面范围。不再支持 **flat** 关键字：PAT 池现在始终为平面。**include-reserve** 关键字以前是 **flat** 的子关键字，现在则是 PAT 池配置中的独立关键字。使用此选项，您可以在 PAT 池中包括 1-1023 端口范围。 请注意，如果配置端口块分配（**block-allocation** PAT 池选项），则会使用块分配大小，而不是默认的 512 端口块。此外，不能为集群中的系统的PAT池配置扩展PAT。 新增/修改的命令： **nat**、**show nat pool**
新增的系统定义的 NAT 规则的第 0 部分。	9.16（1）	向 NAT 规则表添加了新的第 0 部分。此部分专门供系统使用。系统正常运行所需的任何 NAT 规则都添加到此部分，这些规则优先于您创建的任何规则。以前，系统定义的规则添加到第 1 部分，用户定义的规则可能会干扰系统的正常运行。您无法添加、编辑或删除第 0 部分中的规则，但您会在 **show nat detail** 命令输出中看到这些规则。
两次 NAT 支持完全限定域名 (FQDN) 对象作为转换（映像）目的。	9.17(1)	您可以使用 FQDN 网络对象（例如指定 www.example.com 的网络对象）作为二次 NAT 规则中的转换（映射）目标地址。系统根据 DNS 服务器返回的 IP 地址配置规则。

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。