NAT 示例和参考

以下主题介绍有关配置 NAT 的示例，以及有关高级配置和故障排除的信息。

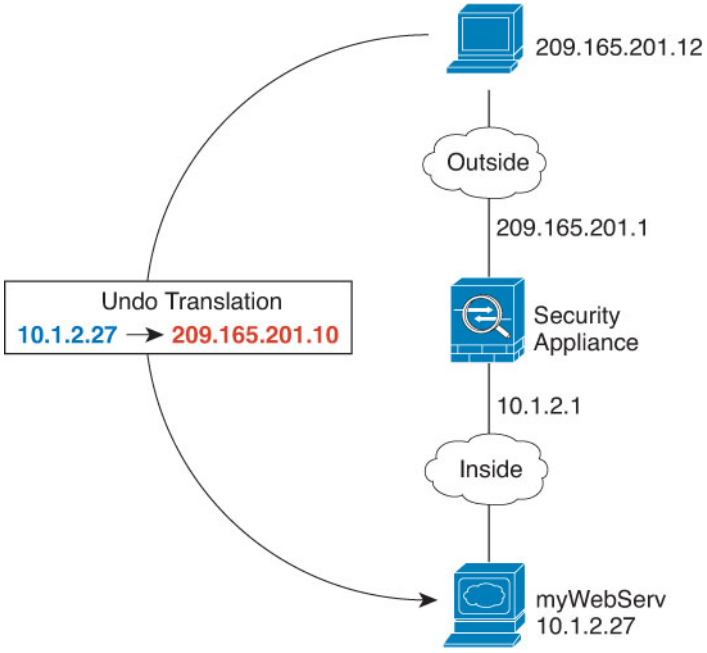
网络对象 NAT 示例

以下是网络对象 NAT 的一些配置示例。

为内部 Web 服务器提供访问（静态 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。

图 *1:* 面向内部 *Web* 服务器的静态 *NAT*



过程

步骤 1 为内部 Web 服务器创建网络对象。

```
hostname(config)# object network myWebServ
hostname(config-network-object)# host 10.1.2.27
```

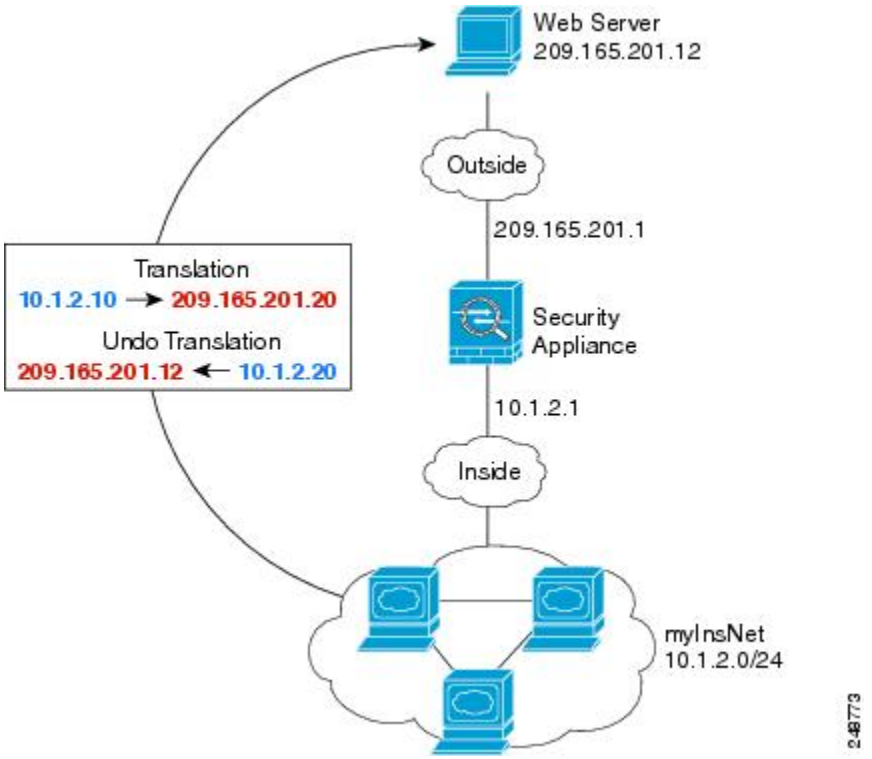
步骤 2 配置对象的静态 NAT：

```
hostname(config-network-object)# nat (inside,outside) static 209.165.201.10
```

面向内部主机的 NAT（动态 NAT）和面向外部 Web 服务器的 NAT（静态 NAT）

当专用网络上的内部用户访问外部 Web 服务器时，以下示例为这些用户配置动态 NAT。此外，当内部用户连接到外部 Web 服务器时，该 Web 服务器地址被转换为显示在内部网络上的地址。

图 *2:* 面向内部 *Web* 服务器的动态 *NAT*，面向外部 *Web* 服务器的静态 *NAT*



过程

步骤 1 为要向其转换内部地址的动态 NAT 池创建一个网络对象。

```
hostname(config)# object network myNatPool
hostname(config-network-object)# range 209.165.201.20 209.165.201.30
```

步骤 2 为内部网络创建网络对象。

```
hostname(config)# object network myInsNet
hostname(config-network-object)# subnet 10.1.2.0 255.255.255.0
```

步骤 3 使用动态 NAT 池对象为内部网络启用动态 NAT。

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

步骤 4 为外部 Web 服务器创建网络对象。

```
hostname(config)# object network myWebServ
hostname(config-network-object)# host 209.165.201.12
```

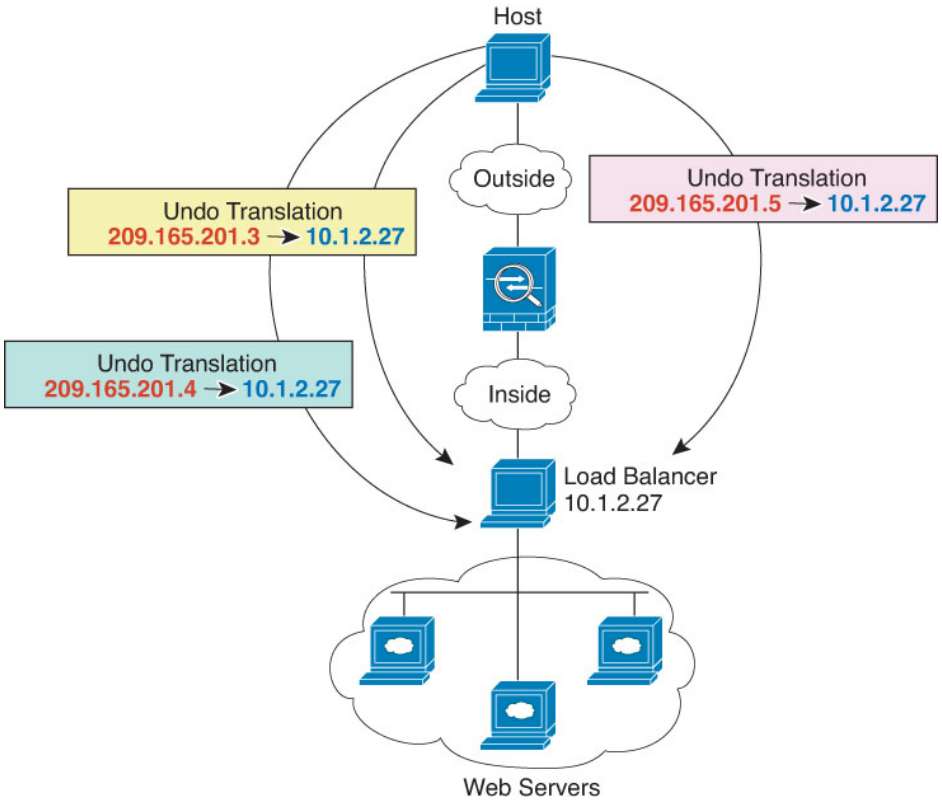
步骤 5 为 Web 服务器配置静态 NAT。

```
hostname(config-network-object)# nat (outside,inside) static 10.1.2.20
```

具有多个映射地址的内部负载均衡器（静态 NAT，一对多）

以下示例显示转换为多个 IP 地址的内部负载均衡器。当外部主机访问其中一个映射 IP 地址时，将该地址反向转换为单一负载均衡器地址。根据请求的URL，它会将流量重新定向到正确的Web服务器。

图 *3:* 内部负载均衡器的一对多静态 *NAT*



过程

步骤 1 为要向其映射负载均衡器的地址创建网络对象。

```
hostname(config)# object network myPublicIPs
hostname(config-network-object)# range 209.165.201.3 209.265.201.8
```

步骤 2 为负载均衡器创建网络对象。

```
hostname(config)# object network myLBHost
hostname(config-network-object)# host 10.1.2.27
```

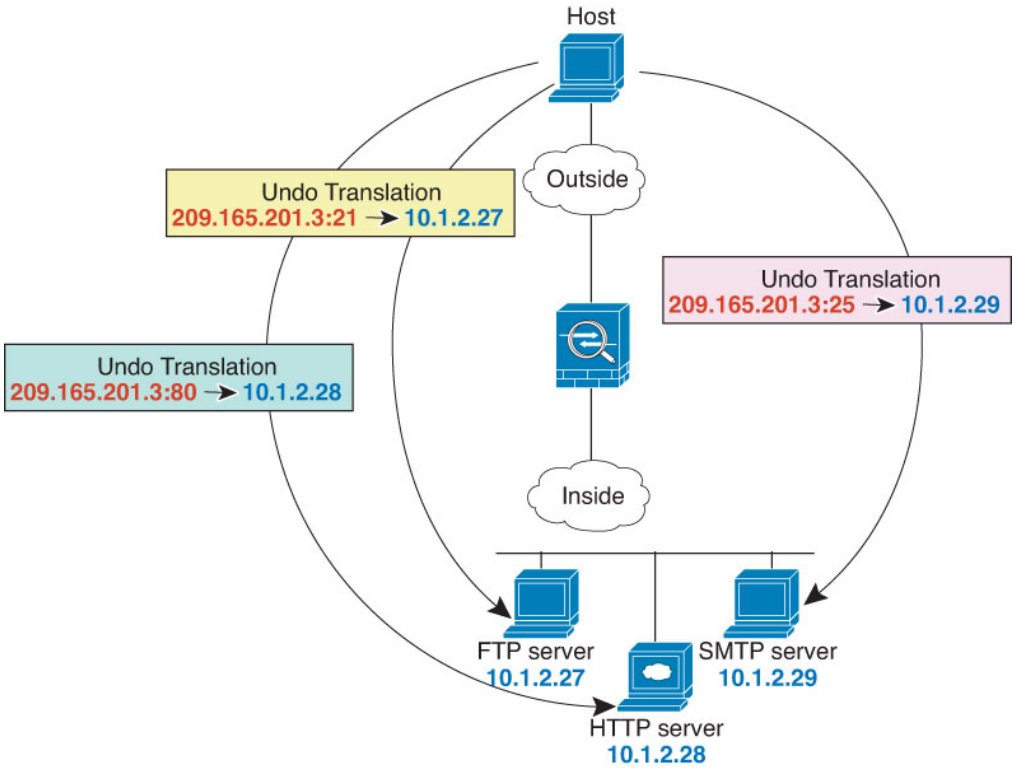
步骤 3 为应用范围对象的负载均衡器配置静态 NAT。

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

用于 FTP、HTTP 和 SMTP（支持端口转换的静态 NAT）的单一地址

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。

图 *4:* 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，并配置支持端口转换的静态 NAT，将 FTP 端口映射到其本身。

```
hostname(config)# object network FTP_SERVER
hostname(config-network-object)# host 10.1.2.27
hostname(config-network-object)# nat (inside,outside) static 209.165.201.3 service tcp ftp
 ftp
```

步骤 2 为 HTTP 服务器创建网络对象，并配置支持端口转换的静态 NAT，将 HTTP 端口映射到其本身。

```
hostname(config)# object network HTTP_SERVER
hostname(config-network-object)# host 10.1.2.28
hostname(config-network-object)# nat (inside,outside) static 209.165.201.3 service tcp http
 http
```

步骤 3 为 SMTP 服务器创建网络对象，并配置支持端口转换的静态 NAT，将 SMTP 端口映射到其本身。

```
hostname(config)# object network SMTP_SERVER
hostname(config-network-object)# host 10.1.2.29
hostname(config-network-object)# nat (inside,outside) static 209.165.201.3 service tcp smtp
 smtp
```

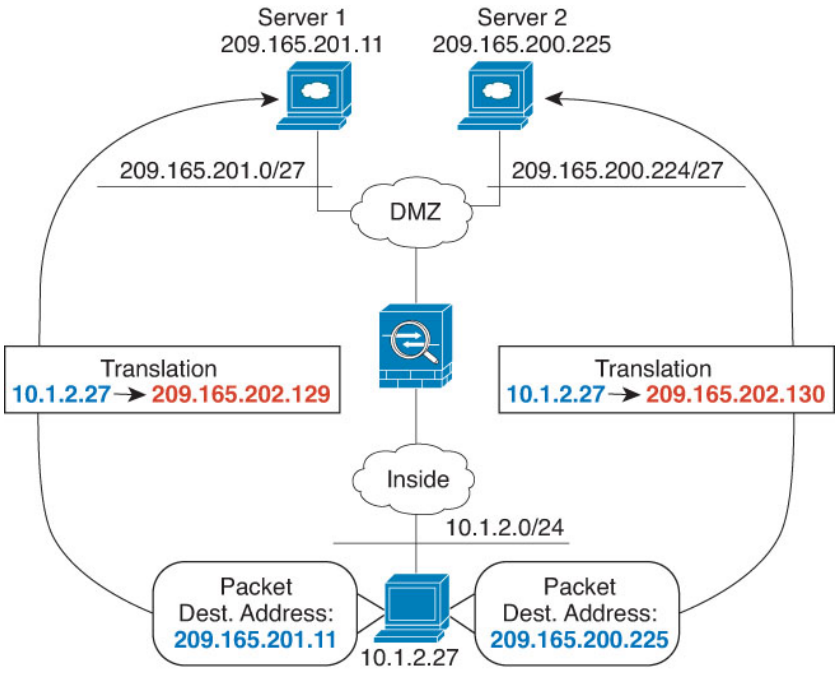
两次 NAT 的示例

本节包括以下配置示例：

根据目标进行不同的转换（动态两次 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*。

图 *5:* 使用不同目标地址的两次 *NAT*



过程

步骤 1 为内部网络添加网络对象：

```
hostname(config)# object network myInsideNetwork
hostname(config-network-object)# subnet 10.1.2.0 255.255.255.0
```

步骤 2 为 DMZ 网络 1 添加网络对象：

```
hostname(config)# object network DMZnetwork1
hostname(config-network-object)# subnet 209.165.201.0 255.255.255.224
```

步骤 3 为 PAT 地址添加网络对象：

```
hostname(config)# object network PATaddress1
hostname(config-network-object)# host 209.165.202.129
```

步骤 4 配置第一条两次 NAT 规则：

```
hostname(config)# nat (inside,dmz) source dynamic myInsideNetwork PATaddress1
destination static DMZnetwork1 DMZnetwork1
```

由于不希望转换目标地址，所以需要通过为实际和映射目标地址指定同一地址来为其配置身份NAT。

步骤 5 为 DMZ 网络 2 添加网络对象：

```
hostname(config)# object network DMZnetwork2
hostname(config-network-object)# subnet 209.165.200.224 255.255.255.224
```

步骤 6 为 PAT 地址添加网络对象：

```
hostname(config)# object network PATaddress2
hostname(config-network-object)# host 209.165.202.130
```

步骤 7 配置第二条两次 NAT 规则：

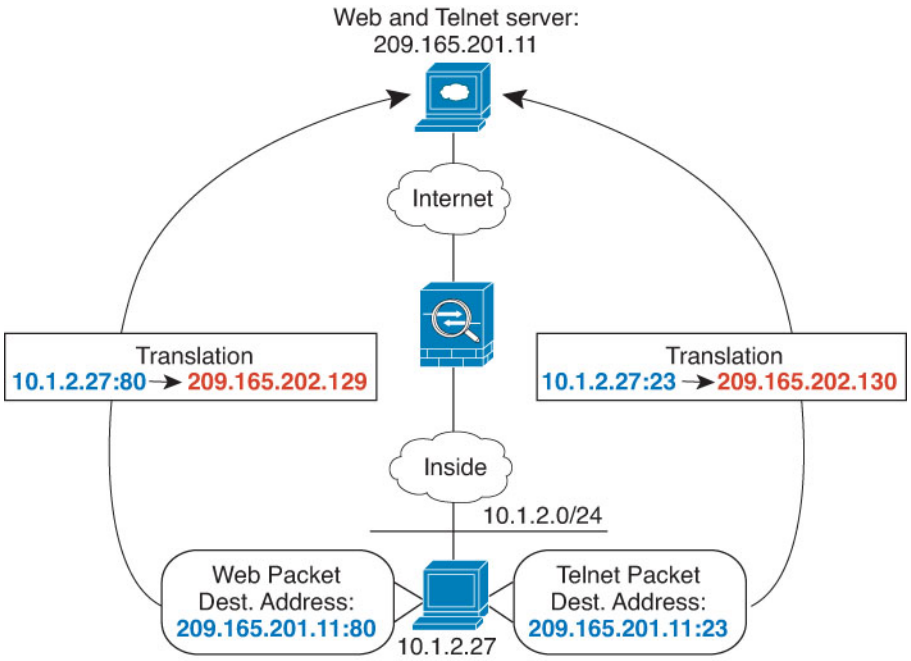
示例：

```
hostname(config)# nat (inside,dmz) source dynamic myInsideNetwork PATaddress2
destination static DMZnetwork2 DMZnetwork2
```

根据目标地址和端口进行不同的转换（动态 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*。

图 *6:* 使用不同目标端口的两次 *NAT*



过程

步骤 1 为内部网络添加网络对象：

```
hostname(config)# object network myInsideNetwork
hostname(config-network-object)# subnet 10.1.2.0 255.255.255.0
```

步骤 2 为 Telnet/Web 服务器添加网络对象：

```
hostname(config)# object network TelnetWebServer
hostname(config-network-object)# host 209.165.201.11
```

步骤 3 使用 Telnet 时为 PAT 地址添加网络对象：

```
hostname(config)# object network PATaddress1
hostname(config-network-object)# host 209.165.202.129
```

步骤 4 为 Telnet 添加服务对象：

```
hostname(config)# object service TelnetObj
hostname(config-network-object)# service tcp destination eq telnet
```

步骤 5 配置第一条两次 NAT 规则：

```
hostname(config)# nat (inside,outside) source dynamic myInsideNetwork PATaddress1
destination static TelnetWebServer TelnetWebServer service TelnetObj TelnetObj
```

由于不希望转换目标地址或端口，所以需要通过为实际和映射目标地址指定同一地址并为实际和映射服务指定同一端口来为它们配置身份 NAT。

步骤 6 使用 HTTP 时为 PAT 地址添加网络对象：

```
hostname(config)# object network PATaddress2
hostname(config-network-object)# host 209.165.202.130
```

步骤 7 为 HTTP 添加服务对象：

```
hostname(config)# object service HTTPObj
hostname(config-network-object)# service tcp destination eq http
```

步骤 8 配置第二条两次 NAT 规则：

```
hostname(config)# nat (inside,outside) source dynamic myInsideNetwork PATaddress2
```

```
destination static TelnetWebServer TelnetWebServer service HTTPObj HTTPObj
```

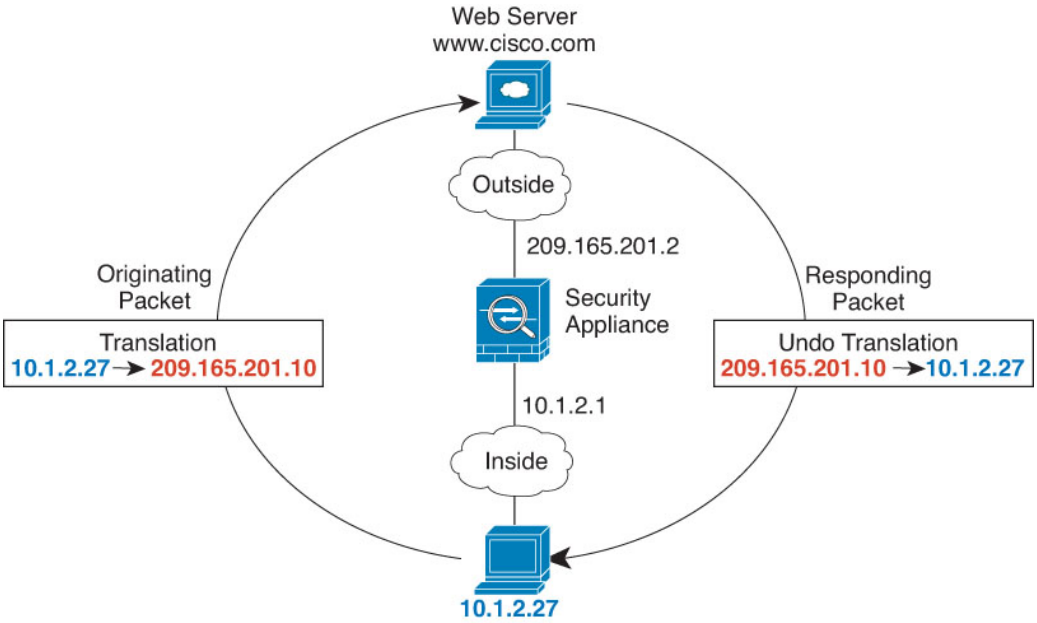
路由和透明防火墙模式下的 NAT

可以在路由和透明防火墙模式下配置 NAT。以下部分介绍每种防火墙模式的典型用法。

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 *7: 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，ASA 接收数据包，因为 ASA 执行代理 ARP 以认领数据包。
3. 接下来，ASA 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。

透明模式下或桥接组内的 NAT

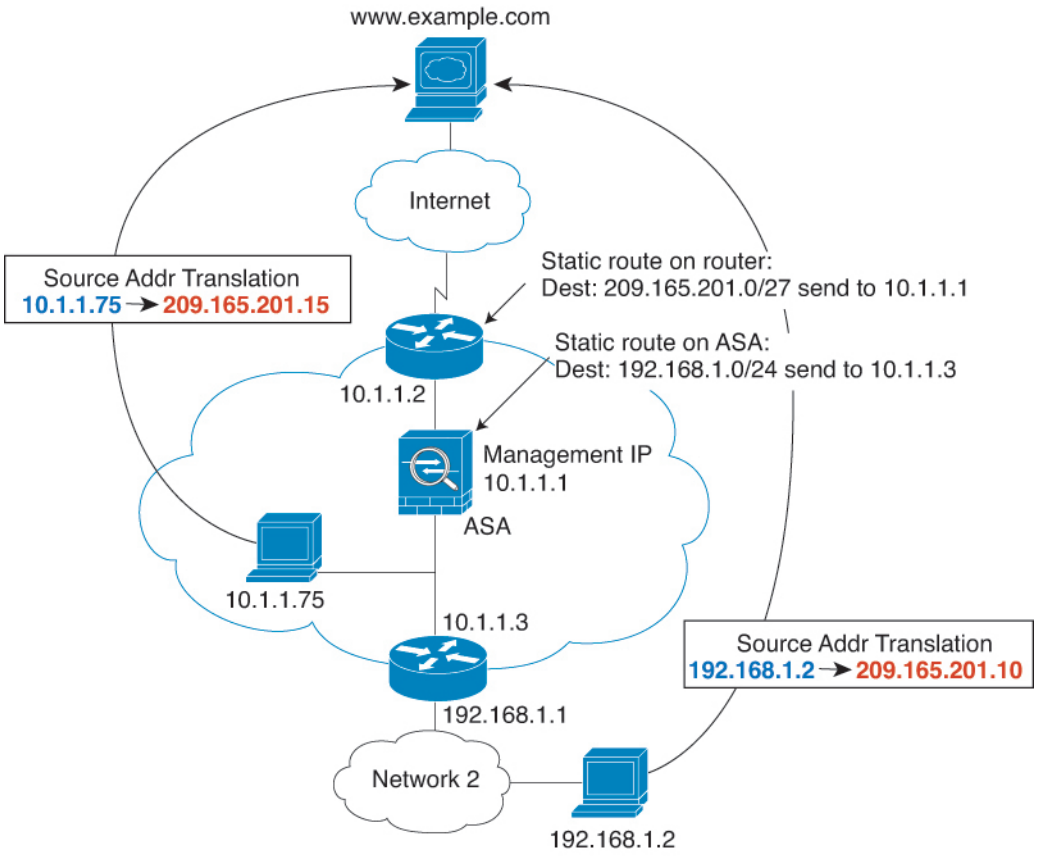
在透明模式下使用NAT可以消除上游或下游路由器为其网络执行NAT的需求。在路由模式下，NAT可以执行与桥接组内类似的功能。

透明模式下的 NAT或在路由模式下同一桥接组的成员之间具有以下要求和局限性：

- 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。
- 不支持 ARP 检测。此外，如果由于某种原因，ASA 一端的主机向 ASA 另一端的主机发送 ARP 请求，而且发起主机实际地址被映射到同一子网的不同地址，则实际地址在 ARP 请求中依然可见。
- 不支持在 IPv4 和 IPv6 网络之间进行转换。支持在两个 IPv6 网络之间或两个 IPv4 网络之间进行转换。

下图显示透明模式下的典型NAT场景，内部接口和外部接口上的网络相同。在此场景中，透明防火墙执行 NAT 服务，因此上游路由器不必执行 NAT。

图 *8: NAT* 示例：透明模式



1. 当位于 10.1.1.75 的内部主机将数据包发送到 Web 服务器时，数据包的实际源地址 10.1.1.75 被更改为映射地址 209.165.201.15。
2. 当服务器响应时，它将响应发送到映射地址 209.165.201.15，ASA 接收数据包，因为上游路由器将此映射网络包含在定向到 ASA 管理 IP 地址的静态路由中。
3. 然后，ASA 取消映射地址 209.165.201.15 回到实际地址 10.1.1.1.75 的转换。因为实际地址是直接连接的，所以 ASA 将实际地址直接发送到主机。

4. 对于主机 192.168.1.2，发生相同流程，但返回流量除外，ASA 在其路由表中查询路由，根据 192.168.1.0/24 的 ASA 静态路由，将数据包发送到位于 10.1.1.3 的下游路由器。

路由 NAT 数据包

ASA需要是发送到映射地址的任何数据包的目标。此外，ASA还需要为它收到的以映射地址为目标的数据包确定出口接口。本节介绍 ASA 如何处理通过 NAT 接受和交付数据包。

映射地址和路由

将实际地址转换为映射地址时，如果需要，您选择的映射地址将确定如何为映射地址配置路由。

请参阅其他 NAT 准则，了解有关映射 IP 地址的其他准则。

以下主题介绍映射地址类型。

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，ASA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ASA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。

注释 如果将映射接口配置为任何接口，而且在与其中一个映射接口相同的网络中指定映射地址，那么如果从其他接口传入对此映射地址的 ARP 请求，则需要在入口接口上为该网络手动配置 ARP 条目，并指定其 MAC 地址。通常，如果该映射接口指定任何接口，则将唯一网络用于此映射地址，避免此类情况发生。使用 **arp** 命令配置 ARP。

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 ASA 的映射地址进行静态路由。

或者，对于路由模式，可以将目标网络上的任何 IP 地址用作网关，为映射地址配置 ASA 上的静态路由，然后使用路由协议重新分配路由。例如，如果您将 NAT 用于内部网络 (10.1.1.0/24)，并且使用映射 IP 地址 209.165.201.5，则可以为 10.1.1.99 网关配置 209.165.201.5 255.255.255.255（主机地址）的可重新分发静态路由。

```
route inside 209.165.201.5 255.255.255.255 10.1.1.99
```

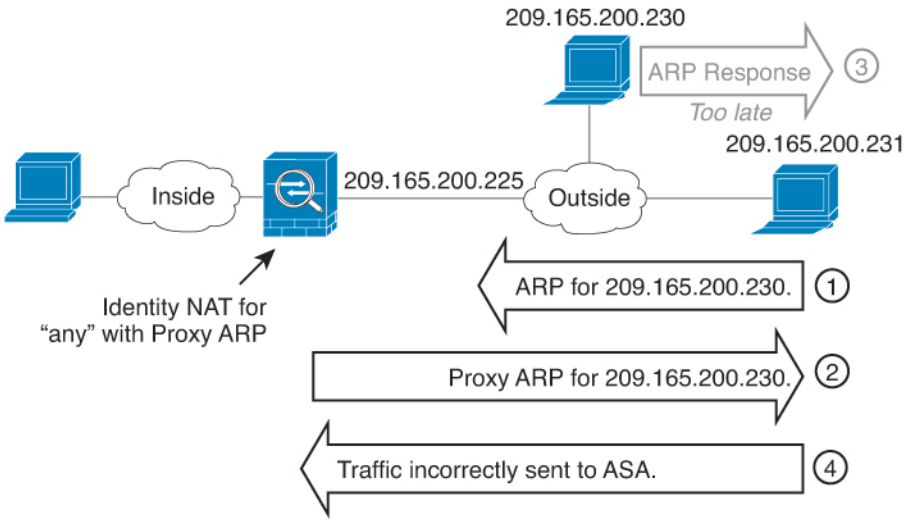
对于透明模式，如果直接连接实际主机，则将上游路由器的静态路由配置为指向 ASA：，指定桥接组 IP 地址。对于透明模式下的远程主机，在上游路由器上的静态路由中，您也可以指定下游路由器 IP 地址。

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。

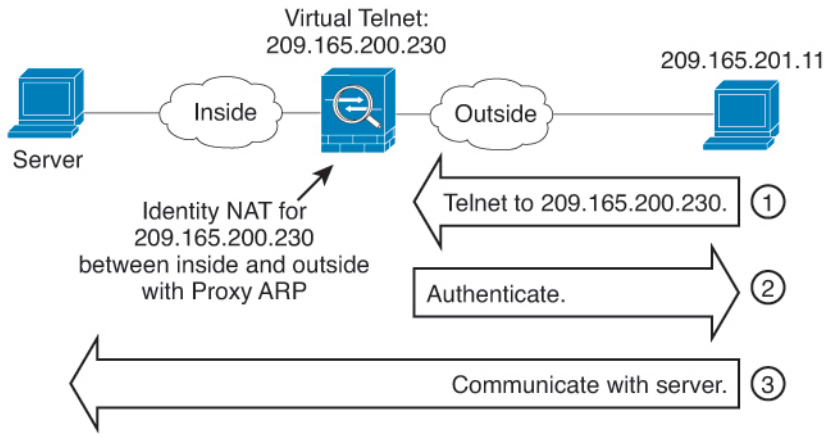
通常，对于身份 NAT，是不需要代理 ARP 的，而且在某些情况下，会造成连接问题。例如，如果为“任何”IP 地址配置一条大体的身份 NAT 规则，则使代理 ARP 保持启用状态会给直接连接到映射接口的网络上的主机造成问题。在这种情况下，当映射网络上的主机要与同一网络上的其他主机通信时，ARP 请求中的地址匹配NAT规则（匹配“任何”地址）。然后，ASA 将代理地址的ARP，即使数据包实际上不以 ASA 为目标。（请注意，即便已设置两次 NAT 规则，也会造成此问题；虽然 NAT 规则必须匹配源地址和目标地址，但仅会根据“源”地址作出代理 ARP 决定）。如果在实际主机 ARP 响应之前收到 ASA ARP 响应，则流量会错误地发送到 ASA。

图 *9:* 身份 *NAT* 的代理 *ARP* 问题



在极少数情况下，需要面向身份 NAT 的代理 ARP；例如，对于虚拟 Telnet。将 AAA 用于网络访问时，主机需要先利用 Telnet 等服务对 ASA 进行身份验证，然后才能让任何其他流量通过。您可以在 ASA 上配置虚拟 Telnet 服务器，以提供必需的登录。从外部访问虚拟 Telnet 地址时，必需为此地址配置身份 NAT 规则，尤其是对于代理 ARP 功能而言。由于虚拟 Telnet 的内部流程，代理 ARP 允许 ASA 保留以虚拟 Telnet 地址为目的的流量，而不是根据 NAT 规则将流量发送到源接口外部。（请见下图。）

图 *10:* 代理 *ARP* 和虚拟 *Telnet*



远程网络的透明模式路由要求

在透明模式下使用NAT时，某些类型的流量要求静态路由。有关更多信息，请参阅一般操作配置指南。

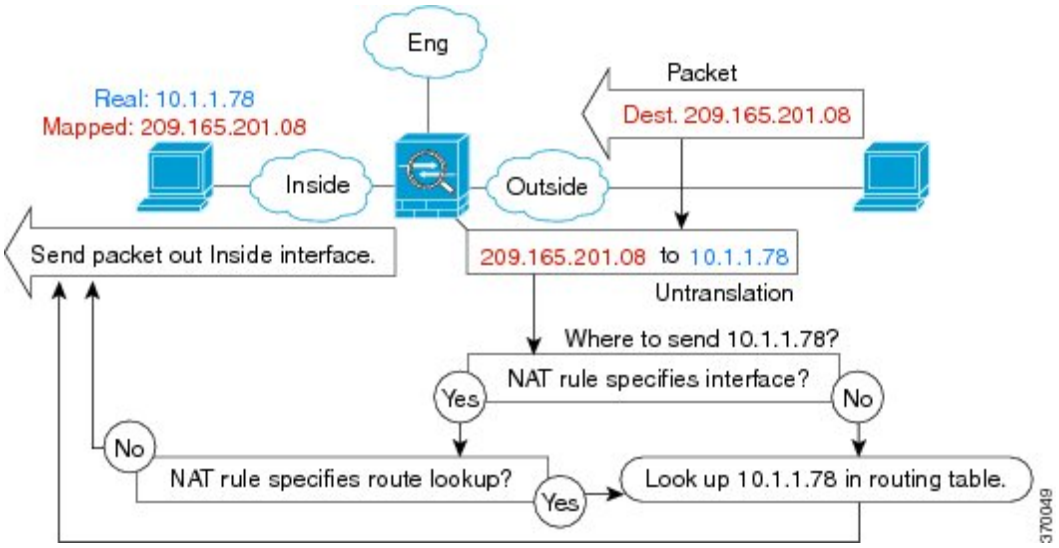
确定出口接口

当使用 NAT 且 ASA 接收映射地址的流量时，ASA 根据 NAT 规则取消转换目标地址，然后将数据包发送到实际地址。ASA 按照以下方式为数据包确定出口接口：

- 透明模式或路由模式下的网桥组接口 - ASA 使用 NAT 规则，为实际地址确定出口接口；您必须在 NAT 规则中指定源和目标网桥组成员接口。
- 路由模式下的常规接口 - ASA 按照以下其中一种方式确定出口接口：
  - 在 NAT 规则中配置接口 - ASA 使用 NAT 规则确定出口接口。然而，您可以选择始终使用路由查询。在某些情景下，必须使用路由查找覆盖。
  - 不在 NAT 规则中配置接口 - ASA 使用路由查询确定出口接口。

下图显示路由模式下的出口接口选择方法。几乎在所有情况下，路由查询都等同于NAT规则接口，但在某些配置中，这两种方法可能不同。

图 *11:* 含 *NAT* 的路由模式出口接口选择



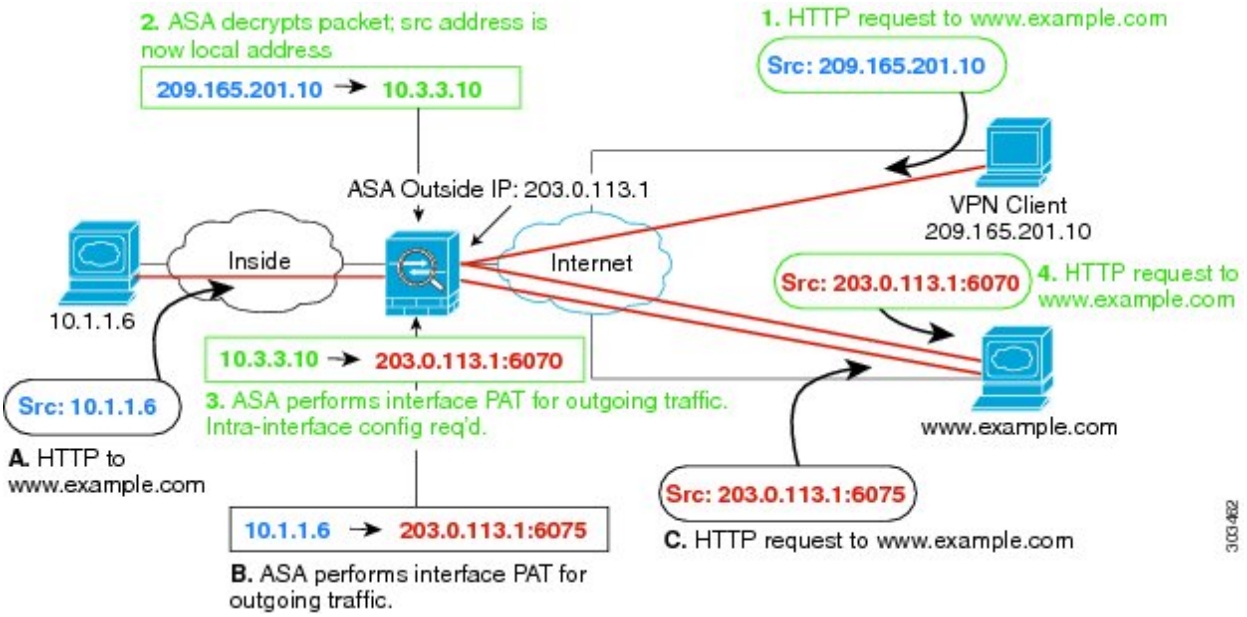
用于 VPN 的 NAT

以下主题借助各种类型的 VPN 来介绍 NAT 用途。

NAT 和远程访问 VPN

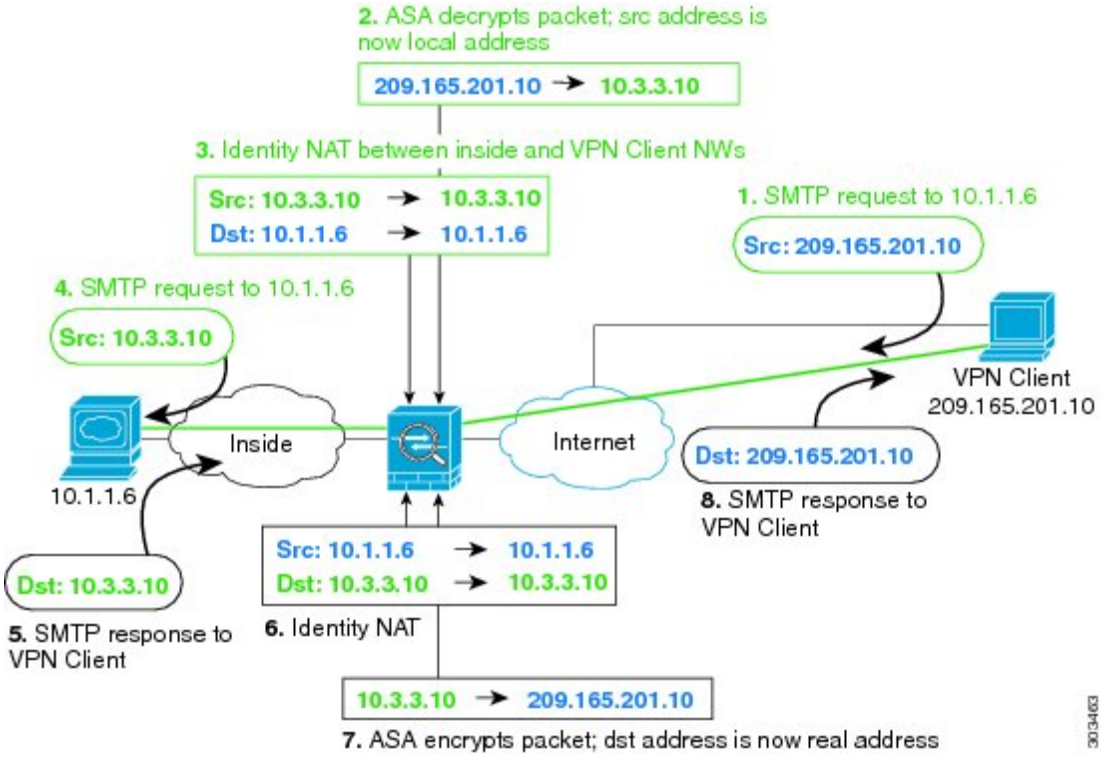
下图显示访问互联网的内部服务器 (10.1.1.6) 和 VPN 客户端 (209.165.201.10)。除非为 VPN 客户端配置拆分隧道（只有指定流量会流经 VPN 隧道），否则互联网绑定的 VPN 流量还必须流经 ASA。当 VPN 流量传入 ASA 时，ASA 会解密数据包；生成的数据包会将 VPN 客户端本地地址 (10.3.3.10) 作为源。对于内部和 VPN 客户端本地网络，需要使用 NAT 提供的公用 IP 地址访问互联网。以下示例使用接口 PAT 规则。为使 VPN 流量可以退出其已进入的相同接口，还需要启用接口内通信（也称为“发夹”网络）。

图 *12:* 面向互联网绑定 ***VPN*** 流量的接口 ***PAT***（接口内）



下图显示要访问内部邮件服务器的 VPN 客户端。由于 ASA 预计内部网络与任何外部网络之间的流量与您为互联网访问设置的 PAT 规则匹配，所以从 VPN 客户端 (10.3.3.10) 流向 SMTP 服务器 (10.1.1.6) 的流量会由于反向路径失败而被丢弃：从 10.3.3.10 流向 10.1.1.6 的流量与 NAT 规则不匹配，但从 10.1.1.6 返回 10.3.3.10 的流量应与外发流量的接口 PAT 规则匹配。由于转发流和反向流不匹配，ASA 在收到数据包时会将其丢弃。为避免这种故障，需要在那些网络之间使用身份 NAT 规则，使内部到 VPN 客户端流量免于应用接口 PAT 规则。身份 NAT 只能将地址转换为其相同的地址。

图 *13:* 面向 *VPN* 客户端的身份 *NAT*



请参阅以下用于上述网络的 NAT 配置示例：

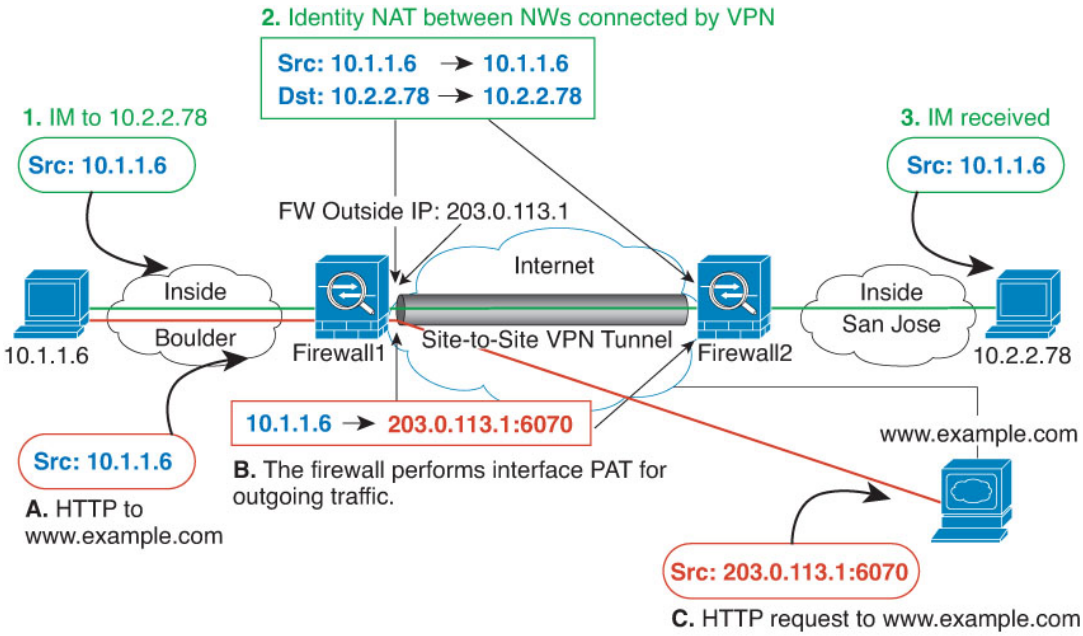
```
! Enable hairpin for non-split-tunneled VPN client traffic:
same-security-traffic permit intra-interface

! Identify local VPN network, & perform object interface PAT when going to Internet:
object network vpn_local
subnet 10.3.3.0 255.255.255.0
nat (outside,outside) dynamic interface

! Identify inside network, & perform object interface PAT when going to Internet:
object network inside_nw
subnet 10.1.1.0 255.255.255.0
nat (inside,outside) dynamic interface

! Use twice NAT to pass traffic between the inside network and the VPN client without
! address translation (identity NAT):
nat (inside,outside) source static inside_nw inside_nw destination static vpn_local vpn_local
```

NAT 和站点间 VPN

下图显示连接博尔德办公室和圣荷西办公室的站点间隧道。对于要发送到互联网的流量（例如，从博尔德办公室中的 10.1.1.6 到 www.example.com），需要利用 NAT 提供的公用 IP 地址访问互联网。以下示例使用接口 PAT 规则。然而，对于要穿过 VPN 隧道的流量（例如，从博尔德办公室中的

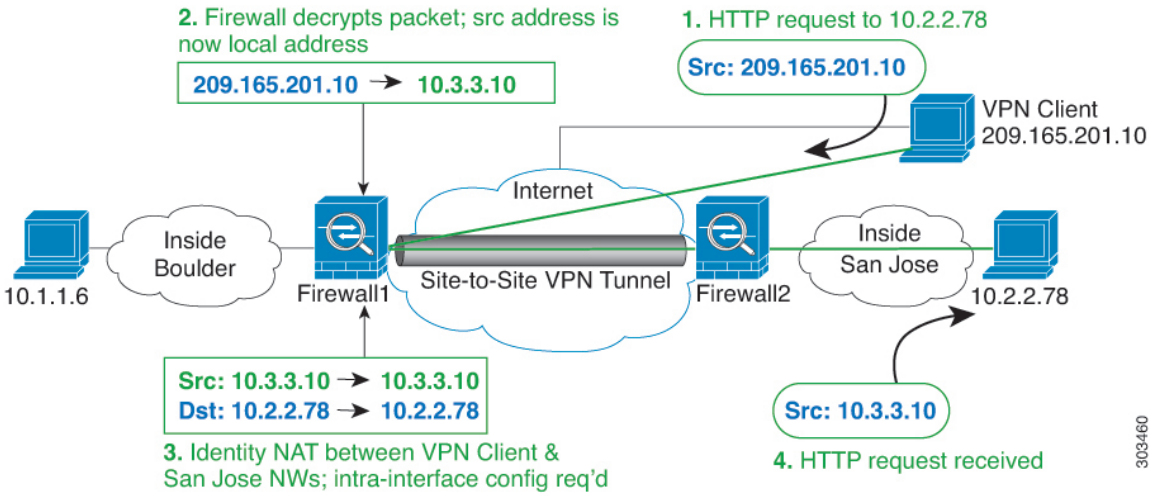
10.1.1.6 到圣荷西办公室中的 10.2.2.78），您不想执行 NAT；您需要通过创建身份 NAT 规则来豁免此流量。身份 NAT 只能将地址转换为其相同的地址。

图 *14:* 用于站点间 ***VPN*** 的接口 ***PAT*** 和身份 ***NAT***



下图显示连接到 Firewall1（博尔德）的 VPN 客户端以及对通过 Firewall1 与 Firewall2（圣荷西）之间的站点间隧道可访问的服务器 (10.2.2.78) 的 Telnet 请求。因为这是一种发夹连接，所以您需要启用接口内通信，这也是来自 VPN 客户端的非拆分隧道互联网绑定流量所必需的。还需要在 VPN 客户端以及博尔德和圣荷西网络之间配置身份 NAT，就像在 VPN 连接的任何网络之间一样配置，使此流量免于应用出站 NAT 规则。

图 *15:* ***VPN*** 客户端访问站点间 ***VPN***



对于第二个示例，请参阅以下针对 Firewall1（博尔德）的 NAT 配置示例：

```
! Enable hairpin for VPN client traffic:
same-security-traffic permit intra-interface

! Identify local VPN network, & perform object interface PAT when going to Internet:
object network vpn_local
subnet 10.3.3.0 255.255.255.0
nat (outside,outside) dynamic interface

! Identify inside Boulder network, & perform object interface PAT when going to Internet:
object network boulder_inside
subnet 10.1.1.0 255.255.255.0
nat (inside,outside) dynamic interface

! Identify inside San Jose network for use in twice NAT rule:
object network sanjose_inside
subnet 10.2.2.0 255.255.255.0

! Use twice NAT to pass traffic between the Boulder network and the VPN client without
! address translation (identity NAT):
nat (inside,outside) source static boulder_inside boulder_inside
destination static vpn_local vpn_local

! Use twice NAT to pass traffic between the Boulder network and San Jose without
! address translation (identity NAT):
nat (inside,outside) source static boulder_inside boulder_inside
destination static sanjose_inside sanjose_inside

! Use twice NAT to pass traffic between the VPN client and San Jose without
! address translation (identity NAT):
nat (outside,outside) source static vpn_local vpn_local
destination static sanjose_inside sanjose_inside
```

请参阅以下针对 Firewall2（圣荷西）的 NAT 配置示例：

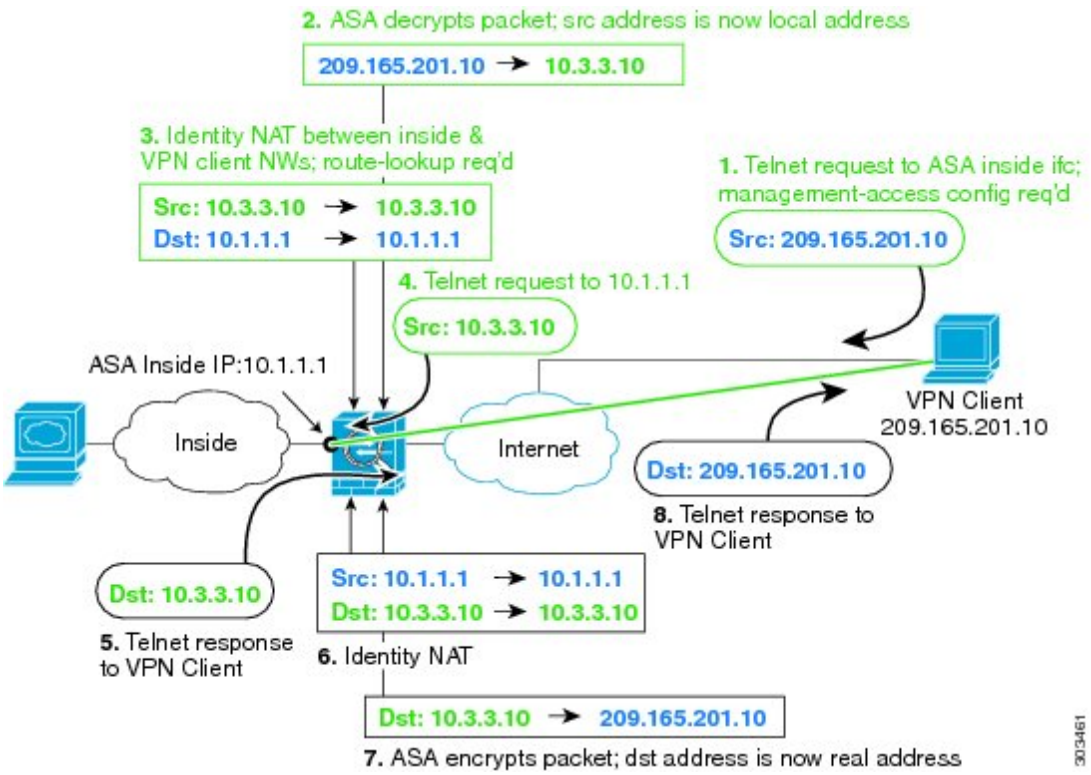
```
! Identify inside San Jose network, & perform object interface PAT when going to Internet:
object network sanjose_inside
subnet 10.2.2.0 255.255.255.0
nat (inside,outside) dynamic interface

! Identify inside Boulder network for use in twice NAT rule:
object network boulder_inside
subnet 10.1.1.0 255.255.255.0

! Identify local VPN network for use in twice NAT rule:
object network vpn_local
subnet 10.3.3.0 255.255.255.0

! Use twice NAT to pass traffic between the San Jose network and Boulder without
! address translation (identity NAT):
nat (inside,outside) source static sanjose_inside sanjose_inside
destination static boulder_inside boulder_inside

! Use twice NAT to pass traffic between the San Jose network and the VPN client without
! address translation (identity NAT):
nat (inside,outside) source static sanjose_inside sanjose_inside
destination static vpn_local vpn_local
```

NAT 和 VPN 管理访问

使用VPN时，可允许管理访问连接到与您进入ASA所用接口不同的接口（请参阅**management-access**命令）。例如，如果您从外部接口进入 ASA，则管理访问功能允许您使用 ASDM、SSH、Telnet 或 SNMP 连接到内部接口；或者可以 ping 连接内部接口。

下图显示使用 Telnet 连接到 ASA 内部接口的 VPN 客户端。当使用管理访问接口，并且根据 NAT 和远程访问 VPN，第 15 页或 NAT 和站点间 VPN，第 17 页配置身份 NAT 时，必须为 NAT 配置路由查询选项。如果未配置路由查询，ASA 会将流量传出 NAT 命令中指定的接口，不考虑路由表规则；在以下示例中，出口接口为内部接口。您不希望ASA将管理流量发送到内部网络，否则它们将再不会回到内部接口 IP 地址。路由查询选项允许 ASA 将流量直接发送到内部接口 IP 地址，而不是流入内部网络。对于从VPN客户端到内部网络上的主机的流量，路由查询选项仍将导致正确的出口接口（内部），因此，正常业务流不会受到影响。有关路由查询选项的详细信息，请参阅确定出口接口，第 14 页。

图 *16: VPN* 管理访问



请参阅以下用于上述网络的 NAT 配置示例：

```
! Enable hairpin for non-split-tunneled VPN client traffic:
same-security-traffic permit intra-interface

! Enable management access on inside ifc:
management-access inside

! Identify local VPN network, & perform object interface PAT when going to Internet:
object network vpn_local
```

```
subnet 10.3.3.0 255.255.255.0
nat (outside,outside) dynamic interface

! Identify inside network, & perform object interface PAT when going to Internet:
object network inside_nw
subnet 10.1.1.0 255.255.255.0
nat (inside,outside) dynamic interface

! Use twice NAT to pass traffic between the inside network and the VPN client without
! address translation (identity NAT), w/route-lookup:
nat (outside,inside) source static vpn_local vpn_local
destination static inside_nw inside_nw route-lookup
```

NAT 和 VPN 故障排除

请参阅以下用于排除 VPN 中 NAT 问题的监控工具：

- 数据包跟踪器 - 正确使用时，数据包跟踪器显示数据包命中了哪些 NAT 规则。
- **show nat detail** - 显示给定 NAT 规则的命中数和未转换流量。
- **show conn all** - 让您查看活动连接，包括流向设备的流量和通过设备的流量。

要让自己熟悉非工作配置和工作配置，可以执行以下步骤：

1. 配置无身份 NAT 的 VPN。
2. 输入 **show nat detail** 和 **show conn all**。
3. 添加身份 NAT 配置。
4. 重复 **show nat detail** 和 **show conn all**。

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 两次 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，无法在两次 NAT 规则中启用 DNS 重写，所以最好创建两个网络对象 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

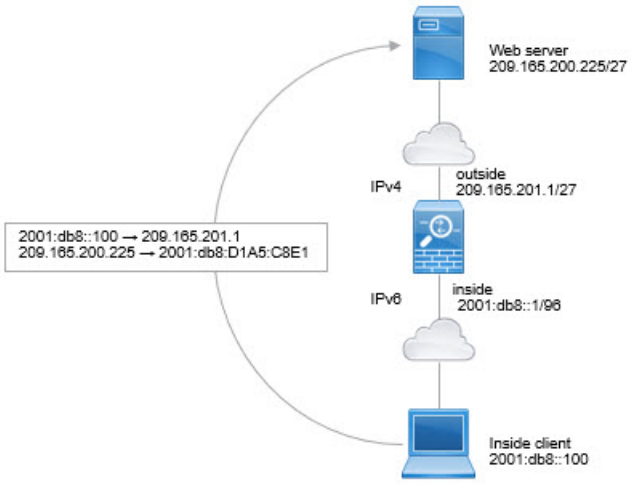
当流量从 IPv6 网络进入仅 IPv4 网络时，您需要将 IPv6 地址转换为 IPv4 地址，并将流量从 Ipv4 返回 IPv6。您需要定义两个地址池，一个 IPv4 地址池用于绑定 IPv4 网络中的 IPv6 地址，另一个 IPv6 地址池用于绑定 IPv6 网络中的 IPv4 地址。

- 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 两次 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，无法在两次 NAT 规则中启用 DNS 重写，所以最好创建两个网络对象 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，以便可以在单个两次 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。

```
hostname(config)# object network inside_v6
hostname(config-network-object)# subnet 2001:db8::/96
```

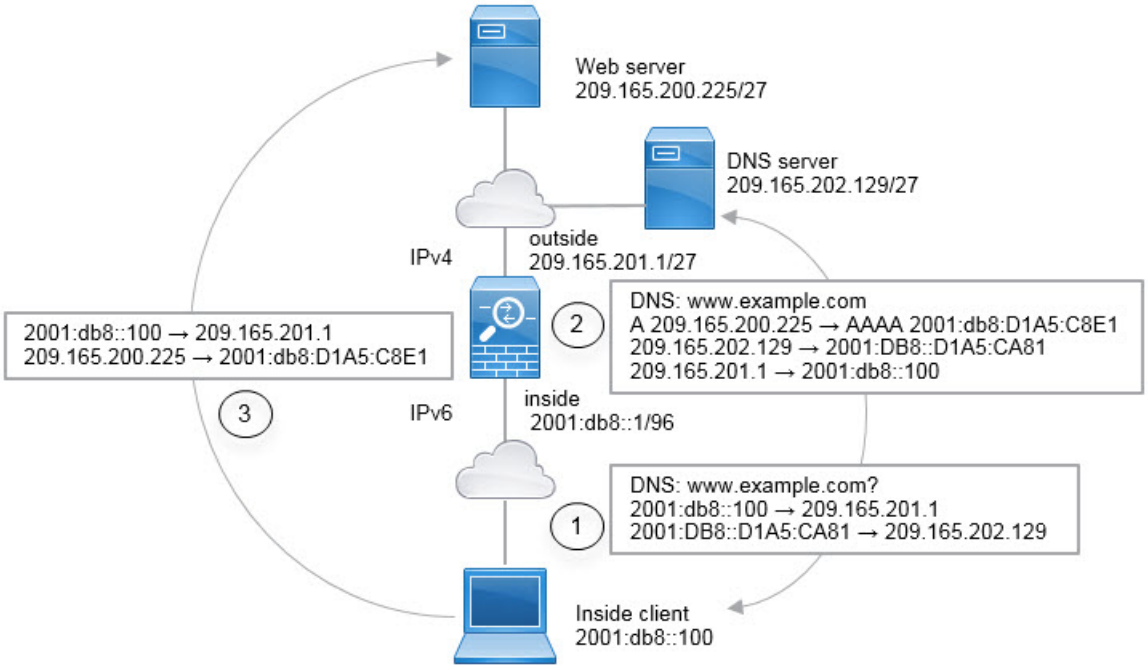
步骤 2 创建两次 NAT 规则以将 IPv6 网络转换为 IPv4 并再次返回。

```
hostname(config)# nat (inside,outside) source dynamic inside_v6 interface
destination static inside_v6 any
```

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 为内部 IPv6 网络创建一个网络对象，并添加 NAT64 规则。

```
hostname(config)# object network inside_v6
hostname(config-network-object)# subnet 2001:db8::/96
hostname(config-network-object)# nat(inside,outside) dynamic interface
```

使用此规则， 从内部接口的 2001:db8::/96 子网到 外部接口的任何流量均会使用外部接口的 IPv4 地址 获得 NAT64 PAT 转换。

步骤 2 为外部 IPv4 网络转换的 IPv6 网络创建一个网络对象，并添加 NAT46 规则。

```
hostname(config)# object network outside_v4_any
hostname(config-network-object)# subnet 0.0.0.0 0.0.0.0
hostname(config-network-object)# nat(outside,inside) static 2001:db8::/96 dns
```

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。

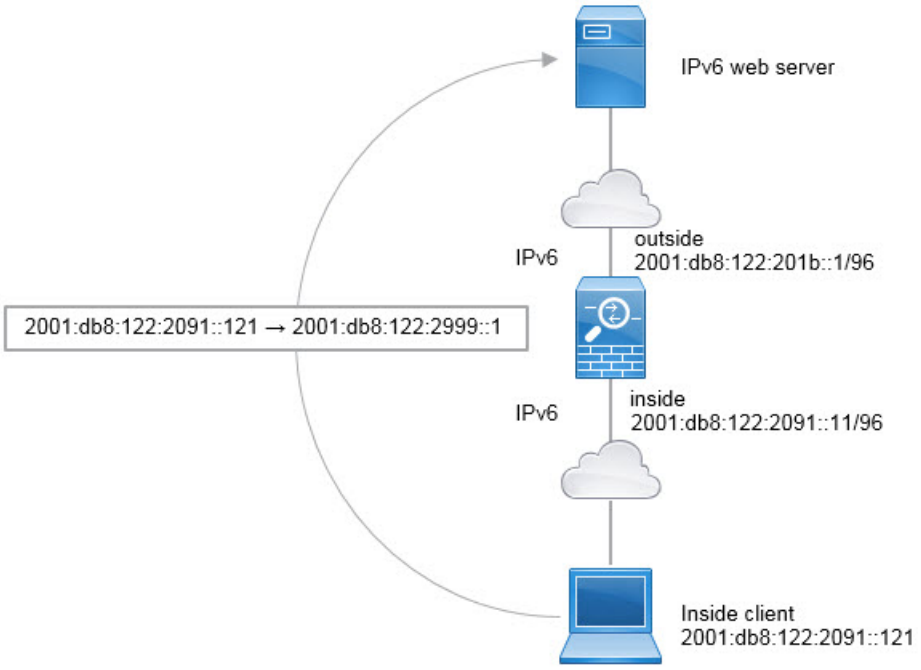
NAT66：将 IPv6 地址转换为不同的 IPv6 地址

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。使用网络对象 NAT 可轻松地为这些规则建模。但是，如果不想允许返回流量，您可以仅使用两次 NAT 将静态 NAT 规则设为单向。

NAT66 示例：网络间的静态转换

您可以使用网络对象 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。



过程

为内部 IPv6 网络创建网络对象并添加静态 NAT 规则。

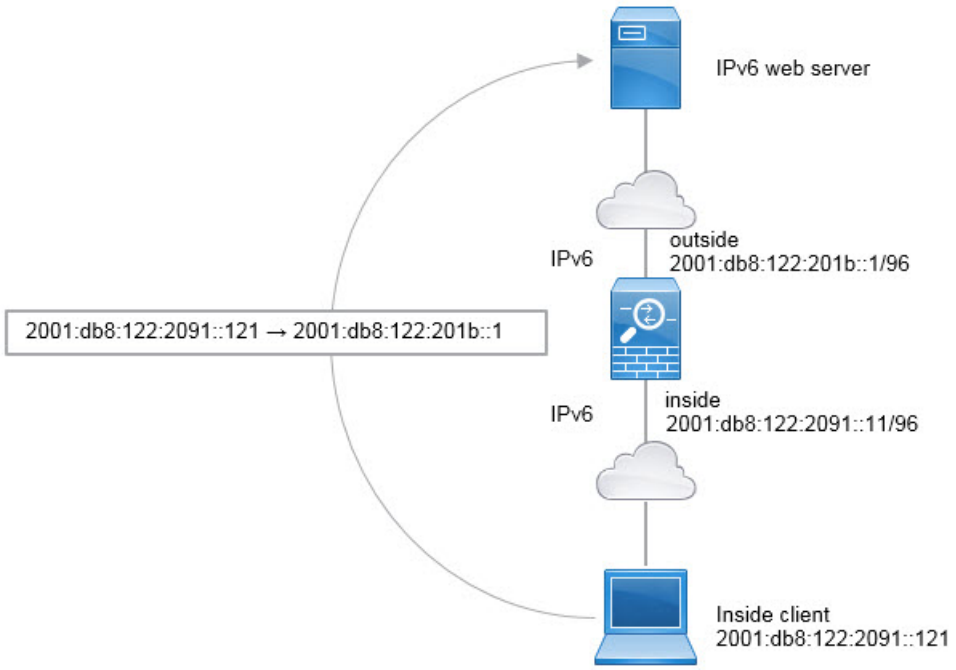
```
hostname(config)# object network inside_v6
hostname(config-network-object)# subnet 2001:db8:122:2091::/96
hostname(config-network-object)# nat(inside,outside) static 2001:db8:122:2999::/96
```

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均会通过静态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。

为 NAT66 配置接口 PAT 规则时，该接口上配置的所有全局地址均用于 PAT 映射。该接口的链路本地地址或站点本地地址不用于 PAT。



过程

为内部 IPv6 网络创建网络对象并添加动态 PAT 规则。

```
hostname(config)# object network inside_v6
hostname(config-network-object)# subnet 2001:db8:122:2091::/96
hostname(config-network-object)# nat(inside,outside) dynamic interface ipv6
```

使用此规则，从内部接口的 2001:db8:122:2091::/96 子网到外部接口的任何流量均会通过 NAT66 PAT 转换为为外部接口配置的 IPv6 全局地址之一。

使用 NAT 重写 DNS 查询和响应

可能需要配置 ASA 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。
- 如果您配置了两次 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。
- 要重写 DNS 查询和响应，您必须启用针对 NAT 规则启用了 DNS NAT 重写的 DNS 应用检查。默认情况下，启用了 DNS NAT 重写的 DNS 检查会全局应用，因此可能无需更改检查配置。
- 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）。

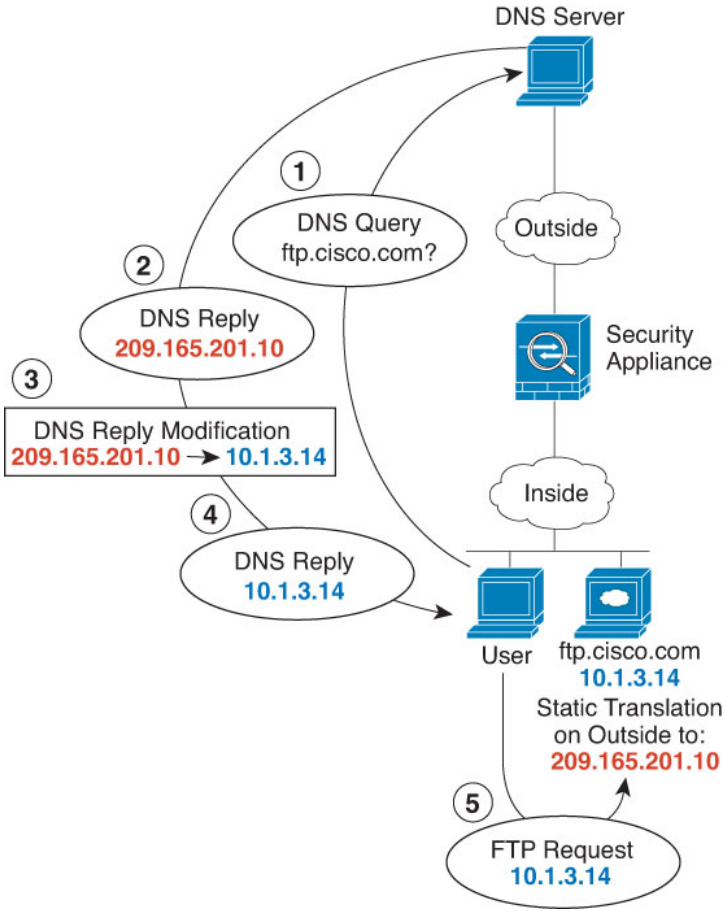
以下主题提供了 NAT 规则中 DNS 重写的示例。

DNS 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。



过程

步骤 1 为 FTP 服务器创建网络对象。

```
hostname(config)# object network FTP_SERVER
hostname(config-network-object)# host 10.1.3.14
```

步骤 2 配置支持 DNS 修改的静态 NAT。

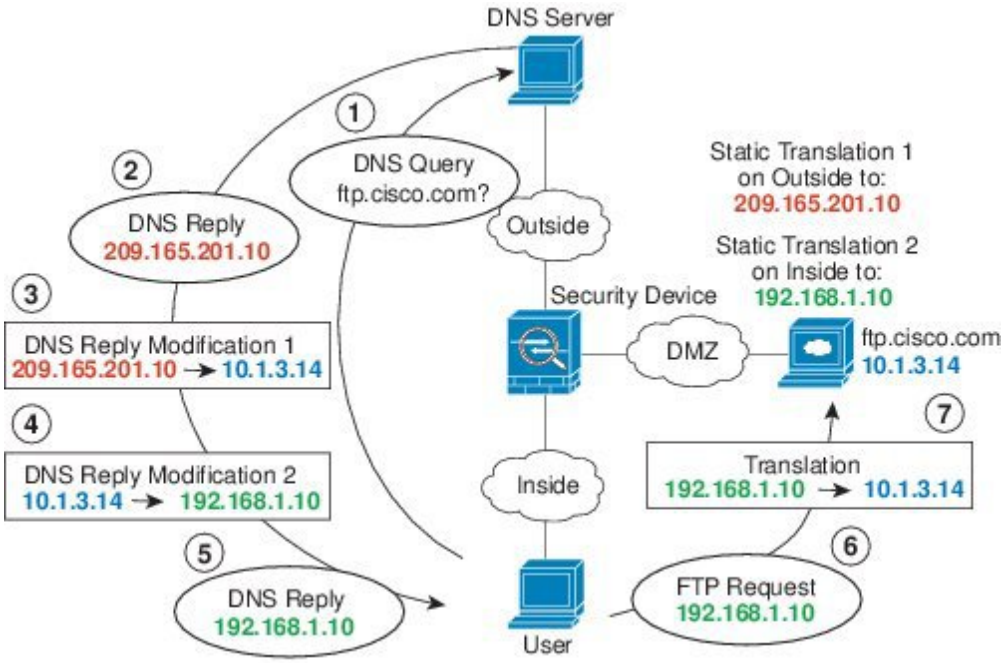
```
hostname(config-network-object)# nat (inside,outside) static 209.165.201.10 dns
```

独立网络上的 DNS 应答修改、DNS 服务器、主机和服务器

下图显示一个内部网络的用户正在从外部 DNS 服务器请求 DMZ 网络上的 ftp.cisco.com 的 IP 地址。DNS 服务器根据外部网络和 DMZ 网络之间的静态规则，以映射地址 (209.165.201.10) 作为应答，即使该用户不在 DMZ 网络中。ASA 将 DNS 应答内的地址转换为 10.1.3.14。

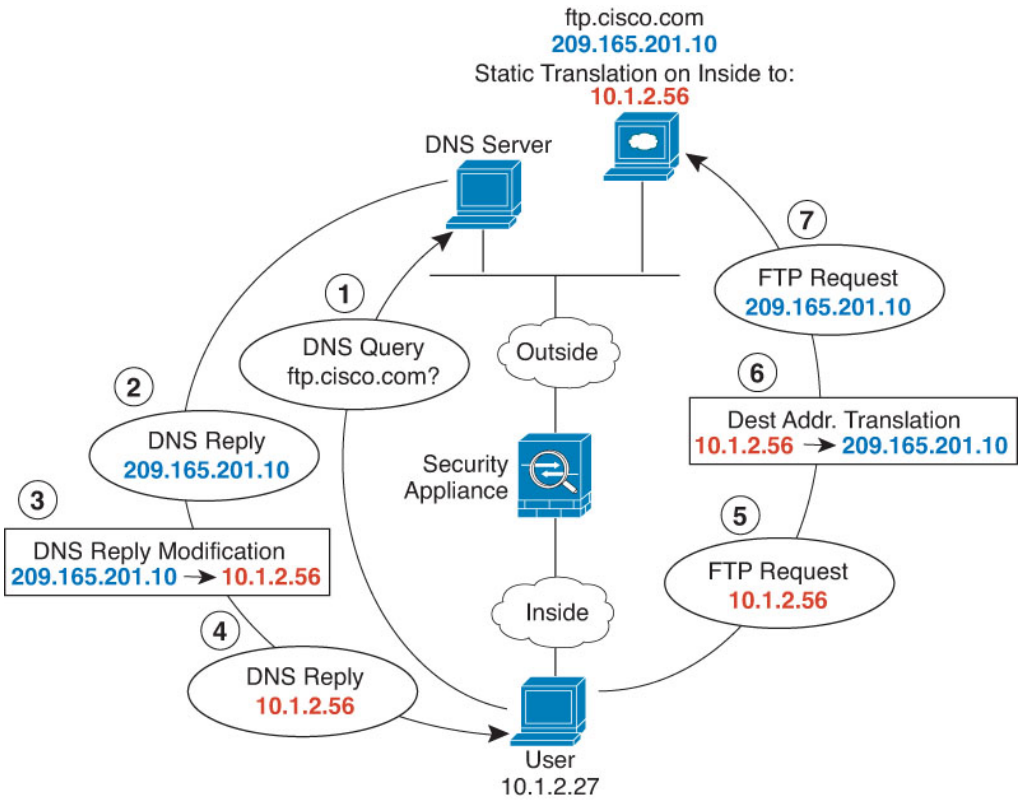
如果用户需要使用实际地址访问 ftp.cisco.com，则无需更多配置。如果内部网络和 DMZ 网络之间也有静态规则，还需要在此规则上启用 DNS 应答修改。然后，修改 DNS 应答两次。这种情况下，ASA 会根据内部和 DMZ 之间的静态规则将 DNS 应答内的地址重新转换为 192.168.1.10。

图 *17:* 独立网络上的 *DNS* 应答修改、*DNS* 服务器、主机和服务器



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。



过程

步骤 1 为 FTP 服务器创建网络对象。

```
hostname(config)# object network FTP_SERVER
hostname(config-network-object)# host 209.165.201.10
```

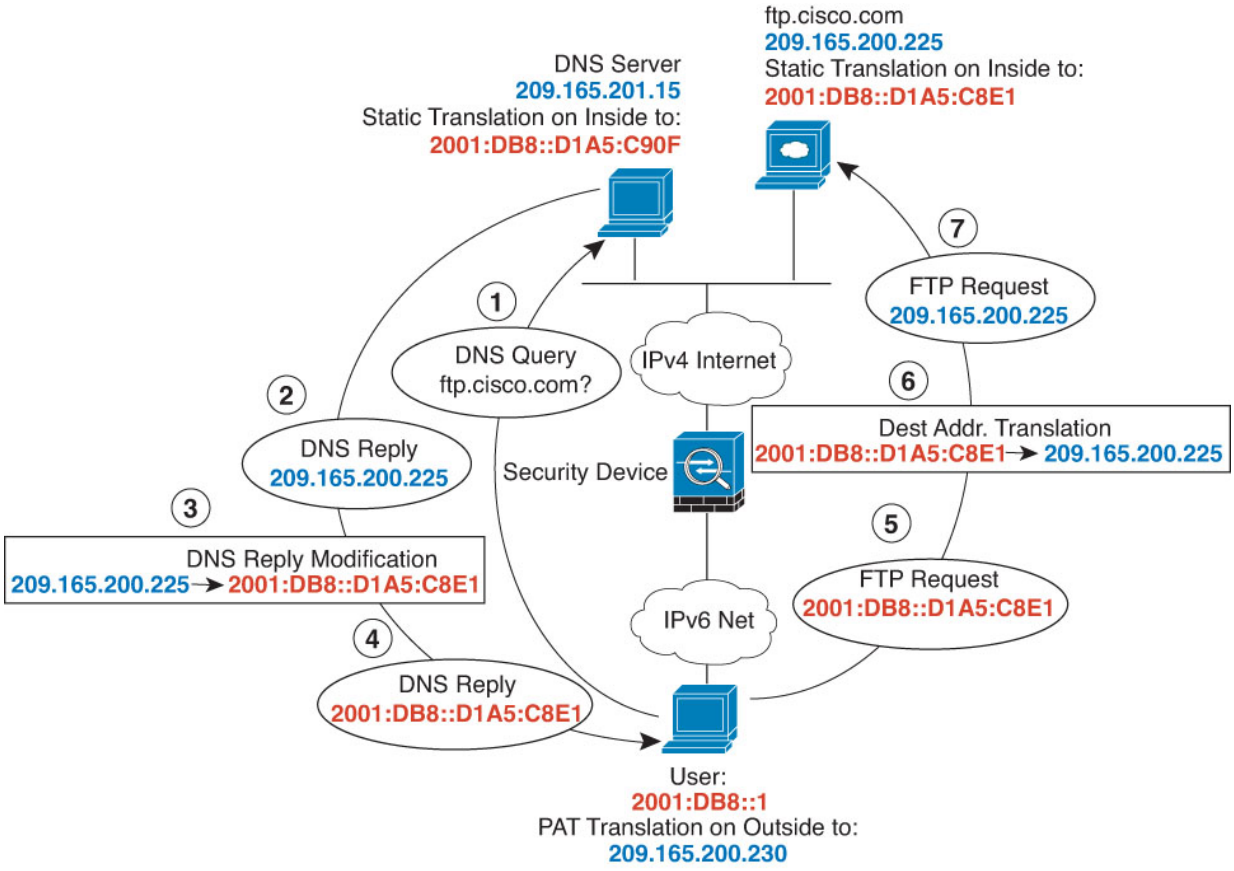
步骤 2 配置支持 DNS 修改的静态 NAT。

```
hostname(config-network-object)# nat (outside,inside) static 10.1.2.56 dns
```

DNS64 应答修改

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。



过程

步骤 1 为 FTP 服务器创建网络对象并配置支持 DNS 修改的静态 NAT 由于这是一对一的转换，请为 NAT46 包含 **net-to-net** 选项。

```
hostname(config)# object network FTP_SERVER
hostname(config-network-object)# host 209.165.200.225
hostname(config-network-object)# nat (outside,inside) static 2001:DB8::D1A5:C8E1/128
net-to-net dns
```

步骤 2 为 DNS 服务器创建网络对象并配置静态 NAT。为 NAT46 包含 **net-to-net** 选项。

```
hostname(config)# object network DNS_SERVER
hostname(config-network-object)# host 209.165.201.15
hostname(config-network-object)# nat (outside,inside) static 2001:DB8::D1A5:C90F/128
net-to-net
```

步骤 3 配置 IPv4 PAT 池，以转换内部 IPv6 网络。

示例：

```
hostname(config)# object network IPv4_POOL
hostname(config-network-object)# range 209.165.200.230 209.165.200.235
```

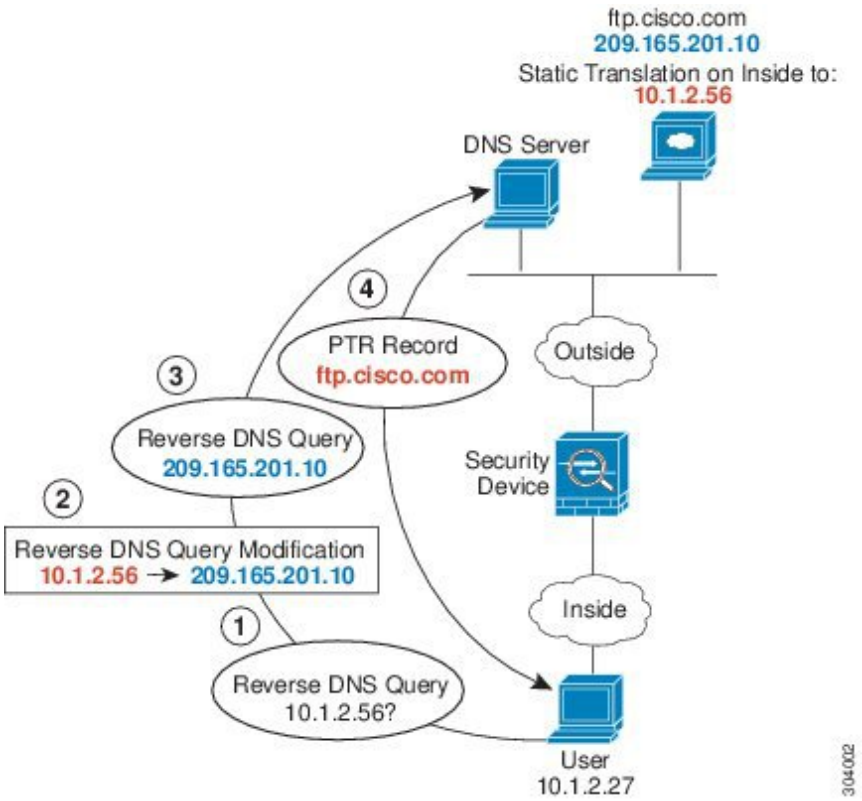
步骤 4 为内部 IPv6 网络创建网络对象，并配置带 PAT 池的动态 NAT。

```
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
```

PTR 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。ASA 包含用于外部服务器的静态转换。在这种情况下，当内部用户为 10.1.2.56 执行逆向 DNS 查询时，ASA 将使用实际地址修改逆向 DNS 查询，而 DNS 服务器将使用服务器名称 ftp.cisco.com 提供响应。

图 *18: PTR* 修改，主机网络上的 *DNS* 服务器



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。