

PIX/ASA 7.x和FWSM : NAT和PAT语句

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[nat-control 命令](#)

[使用 NAT 0 的多条 NAT 语句](#)

[多个全局池](#)

[网络图](#)

[混合 NAT 和 PAT 全局语句](#)

[网络图](#)

[使用 NAT 0 Access-List 的多条 NAT 语句](#)

[网络图](#)

[使用策略 NAT](#)

[网络图](#)

[静态NAT](#)

[网络图](#)

[如何绕过 NAT](#)

[配置身份 NAT](#)

[配置静态身份 NAT](#)

[配置 NAT 免除](#)

[验证](#)

[故障排除](#)

[为端口443添加静态PAT时收到的错误消息](#)

[错误：映射地址与现有静态地址冲突](#)

[相关信息](#)

简介

本文档提供了 Cisco PIX/ASA 安全设备上基本网络地址转换 (NAT) 和端口地址转换 (PAT) 配置的示例。并提供了简化的网络图。有关详细信息，请参阅有关您的 PIX/ASA 软件版本的 PIX/ASA 文档。

要了解有关PIX 5.x及更高版本上的**nat**、**global**、**static**、**conduit**和**access-list**命令以及端口重定向（转发）的详细信息，请参阅在PIX上使用**nat**、**global**、**static**、**conduit**和**access-list**命令和端口重定向（转发）。

要了解有关 Cisco 安全 PIX 防火墙上基本 NAT 和 PAT 配置示例的详细信息，请参阅[在 Cisco 安全 PIX 防火墙上使用 NAT 和 PAT 语句](#)。

有关ASA 8.3版及更高版本中NAT配置的详细信息，请参阅[有关NAT的信息](#)。

注意：PIX/ASA版本8.x支持透明模式下的NAT。有关详细信息，[请参阅透明模式下的NAT](#)。

[先决条件](#)

[要求](#)

本文档的读者应具备 Cisco PIX/ASA 安全设备的相关知识。

[使用的组件](#)

本文档中的信息基于 Cisco PIX 500 系列安全设备软件版本 7.0 及更高版本。

注意： 本文档已经过 PIX/ASA 版本 8.x 再认证。

注意： 本文档中使用的命令适用于防火墙服务模块(FWSM)。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

[规则](#)

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

[nat-control 命令](#)

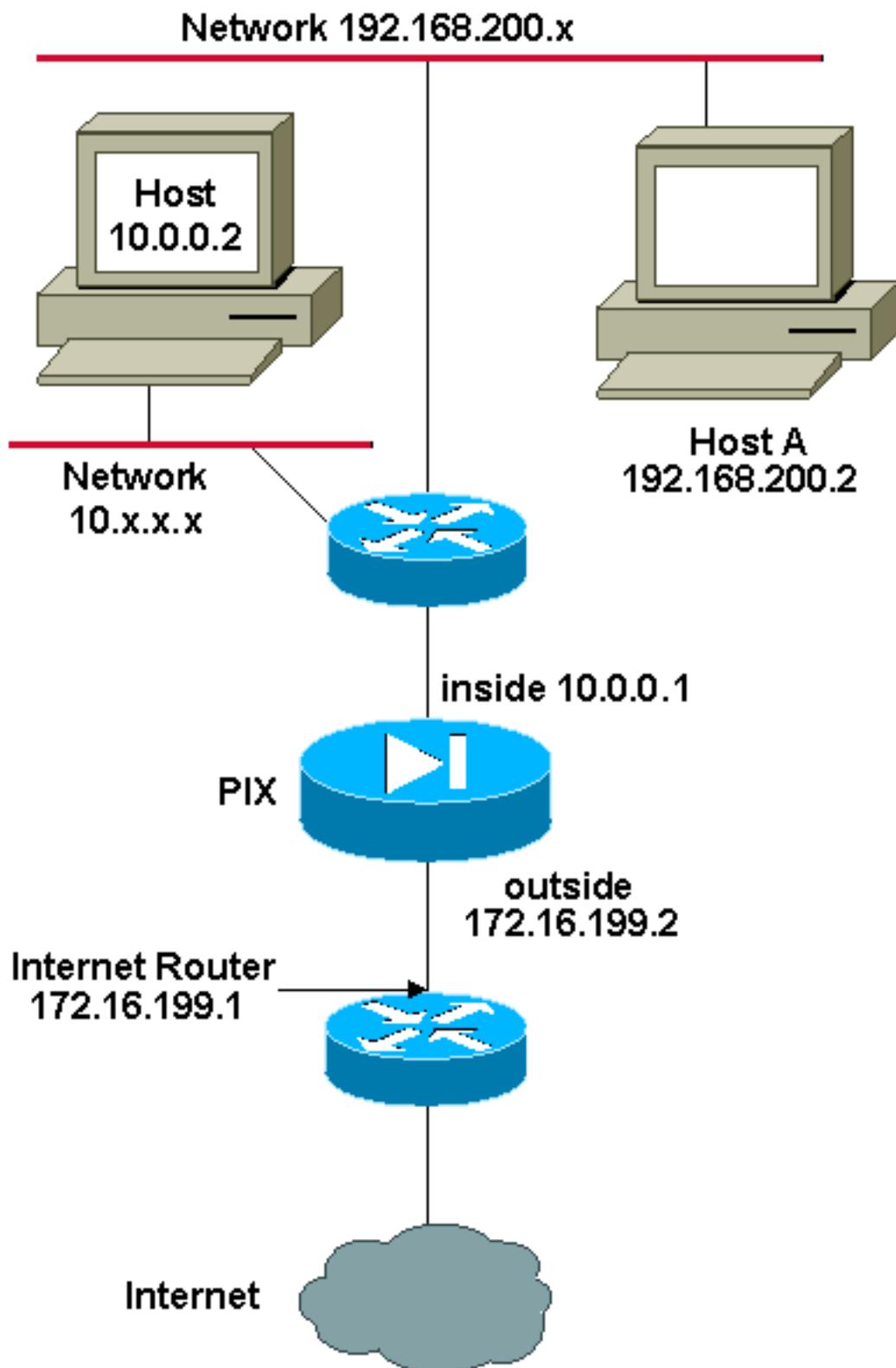
PIX/ASA 上的 `nat-control` 命令指定，通过防火墙的所有数据流都必须具有具体的转换条目（具有匹配的 `global` 或 `static` 语句的 `nat` 语句）才能通过防火墙。`nat-control` 命令可确保转换行为与7.0之前的PIX防火墙版本相同。PIX/ASA 7.0及更高版本的默认配置是`no nat-control`命令的规范。对于PIX/ASA 版本 7.0 及更高版本，可以在发出 `nat-control` 命令时更改此行为。

在禁用 `nat-control` 的情况下，PIX/ASA 将数据包从安全性较高的接口转发到安全性较低的接口，而不在配置中设置具体的转换条目。要将数据流从安全性较低的接口传递到安全性较高的接口，请使用访问列表以允许该数据流。然后，PIX/ASA 会转发该数据流。本文档重点介绍已启用 `nat-control` 时的 PIX/ASA 安全设备行为。

注意： 如果要在PIX/ASA中删除或禁用`nat-control`语句，则需要从安全设备中删除所有NAT语句。一般来说，需要在关闭 NAT 控制之前删除 NAT。必须在 PIX/ASA 中重新配置 NAT 语句才能按预期工作。

[使用 NAT 0 的多条 NAT 语句](#)

网络图



注意：此配置中使用的IP编址方案在Internet上无法合法路由。这些地址是在实验室环境中使用的 [RFC 1918 地址](#)。

在本示例中，ISP为网络管理器提供从172.16.199.1到172.16.199.63的地址范围。网络管理器决定将172.16.199.1分配给Internet路由器的内部接口，将172.16.199.2分配给PIX/ASA的外部接口。

网络管理员已有一个分配给网络的C类地址192.168.200.0/24，并有一些使用这些地址访问Internet的工作站。系统不会对这些工作站进行地址转换。但是，新工作站将被分配10.0.0.0/8网络中的地址，这些地址需要进行转换。

为了适应此网络设计，网络管理员必须在 PIX/ASA 配置中使用两条 NAT 语句和一个全局池，如以下输出所示：

```
global (outside) 1 172.16.199.3-172.16.199.62 netmask 255.255.255.192

nat (inside) 0 192.168.200.0 255.255.255.0 0 0

nat (inside) 1 10.0.0.0 255.0.0.0 0 0
```

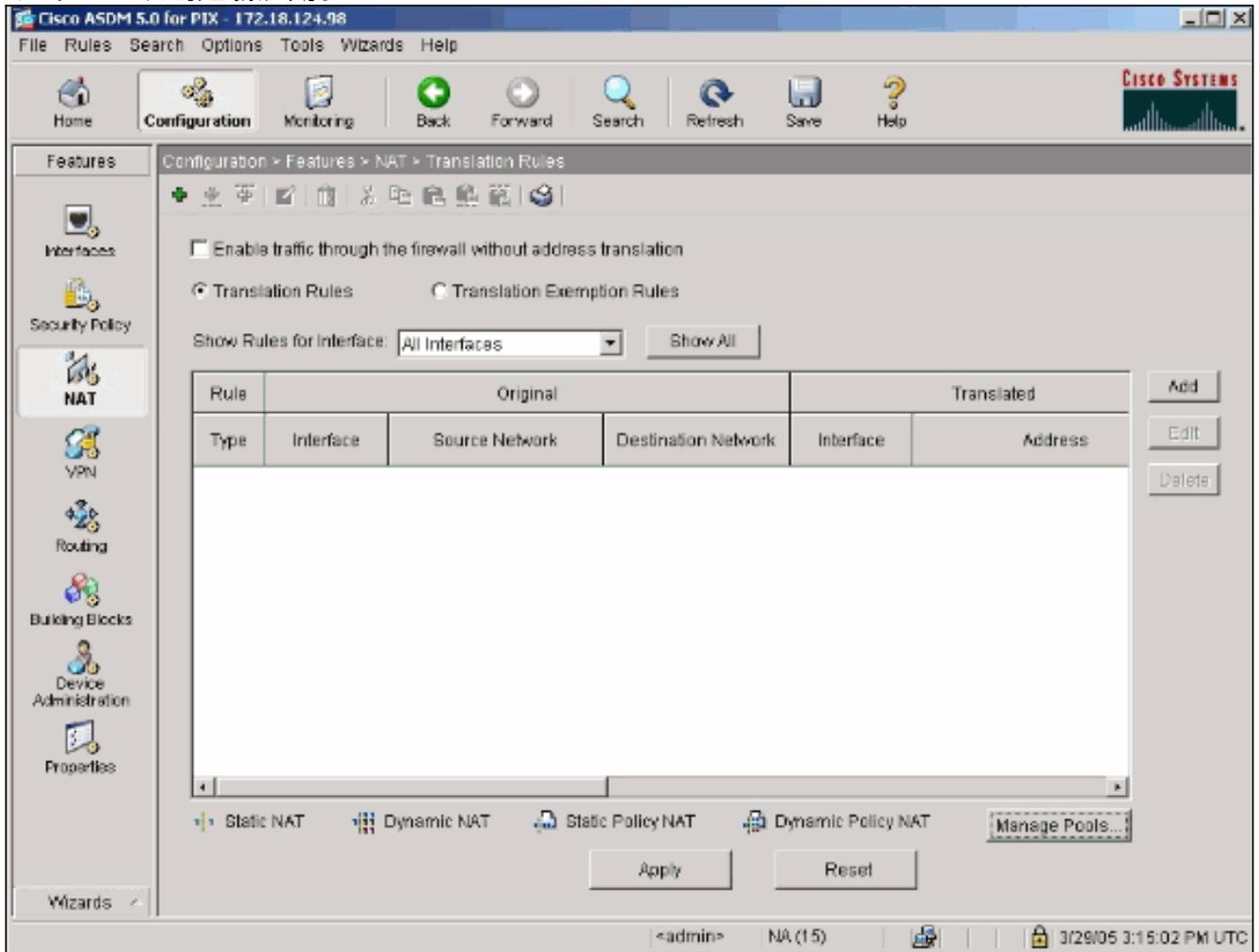
此配置不会转换来自 192.168.200.0/24 网络的任何出站数据流的源地址。它会将 10.0.0.0/8 网络中的源地址转换为一个范围从 172.16.199.3 到 172.16.199.62 的地址。

以下步骤提供如何使用自适应安全设备管理器 (ASDM) 应用此相同配置的说明。

注意：通过CLI或ASDM执行所有配置更改。同时使用 CLI 和 ASDM 进行配置更改会导致配置发挥作用的方式非常不稳定（具体取决于通过 ASDM 应用了哪些配置）。这不是 Bug，而是由于 ASDM 的工作方式引起的。

注意：打开ASDM时，它会从PIX/ASA导入当前配置，并在您进行和应用更改时从该配置中工作。如果在 ASDM 会话处于打开状态时对 PIX/ASA 进行了更改，则 ASDM 将不再使用它“认为”是 PIX/ASA 的当前配置的配置工作。如果通过 CLI 进行配置更改，请务必关闭所有 ASDM 会话。当您希望通过 GUI 工作时，请再次打开 ASDM。

1. 启动 ASDM，浏览到 Configuration 选项卡，然后单击 NAT。
2. 单击 Add 以创建新规则。



此时将显示一个新窗口，允许用户更改此 NAT 条目的 NAT 选项。对于本示例，请对到达内部接口且源自特定 10.0.0.0/24 网络的数据包执行 NAT。PIX/ASA 会将这些数据包转换为外部接

口上的动态 IP 池。在输入描述要对什么数据流执行 NAT 的信息后，请为转换的数据流定义 IP 地址池。

3. 单击 **Manage Pools** 以添加新的 IP 池。

Add Address Translation Rule

Use NAT Use Policy NAT

Source Host/Network

Interface: inside

IP Address: 10.0.0.0

Mask: 255.255.255.0

Browse ...

NAT Options...

Translate Address on Interface: outside

Translate Address To

Static IP Address: []

Redirect port

TCP Original port: [] Translated port: []

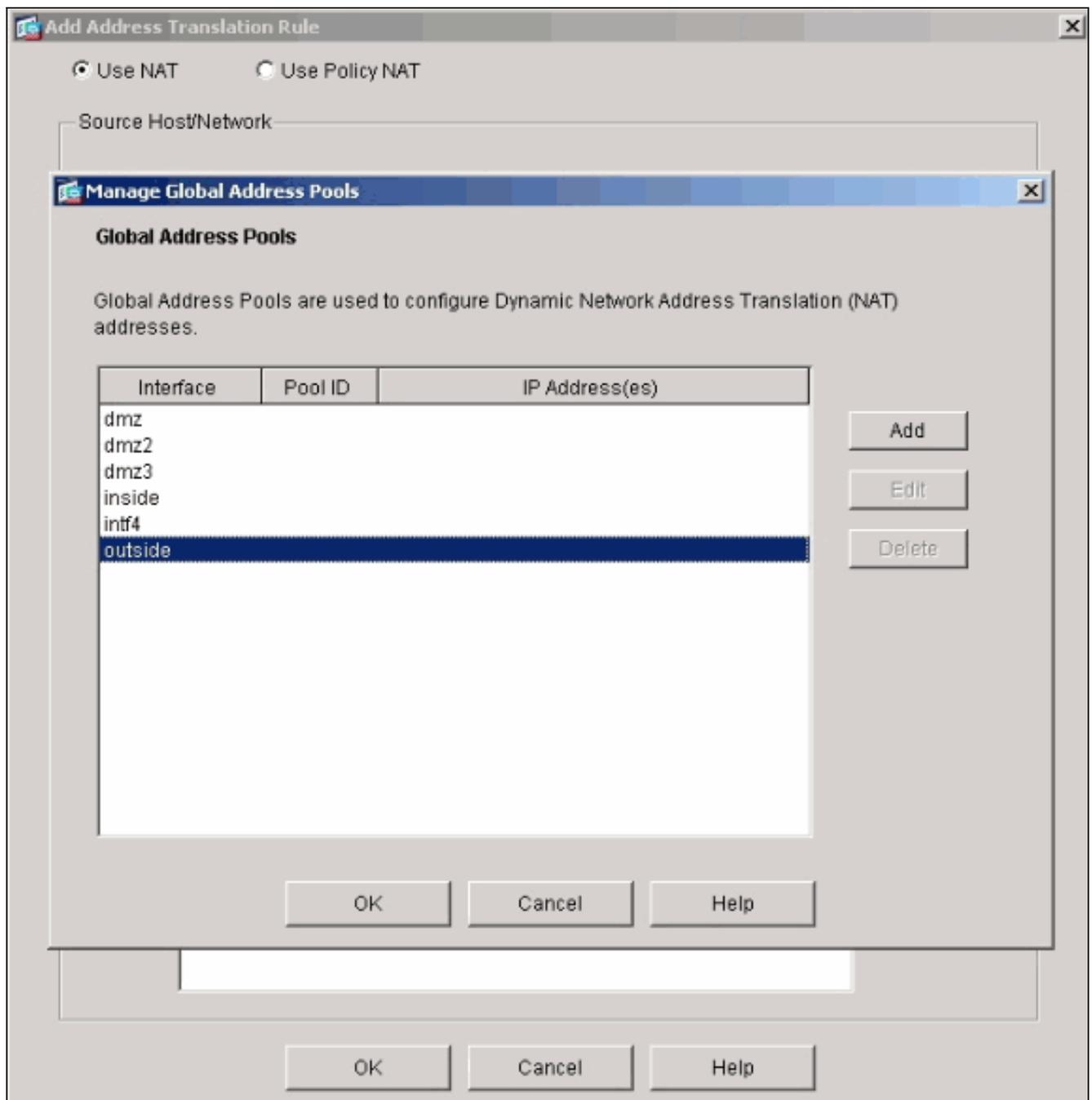
UDP

Dynamic Address Pool: same address Manage Pools...

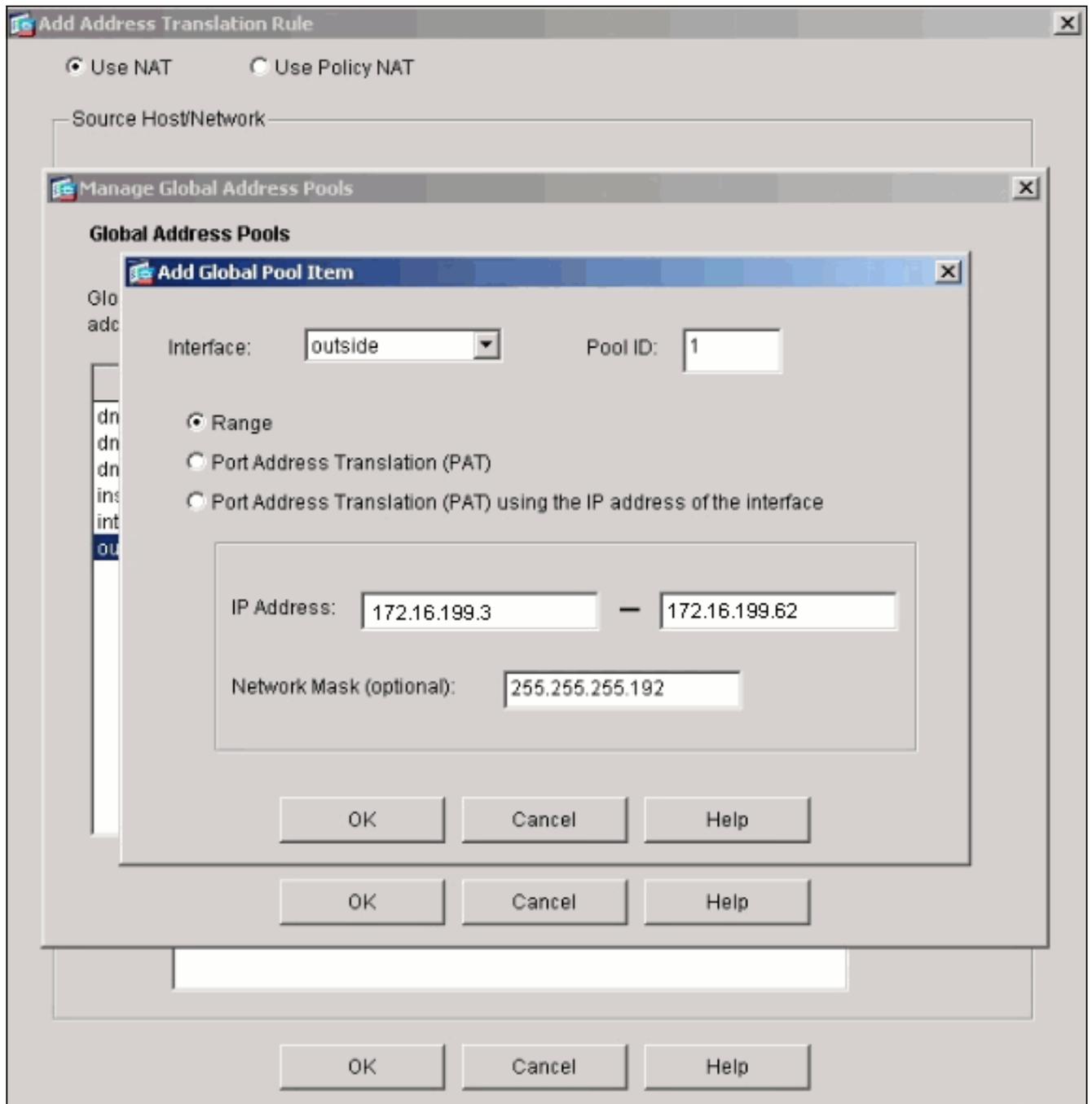
Pool ID	Address
N/A	No address pool defined

OK Cancel Help

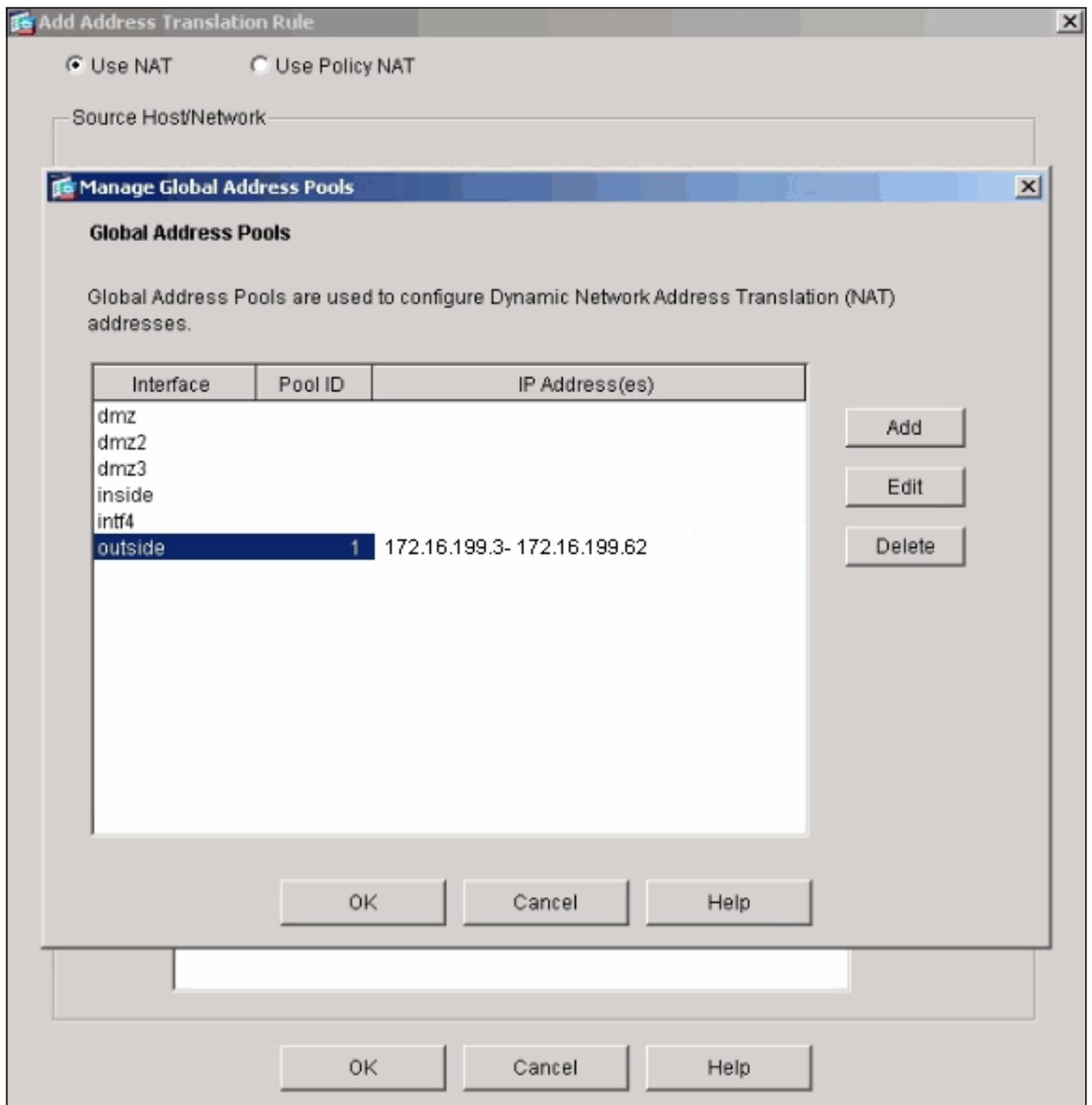
4. 选择 **outside**，然后单击 **Add**。



5. 指定池的 IP 范围，并为池提供一个唯一的整数 ID 编号。



6. 输入适当的值，然后单击 **OK**。这便为外部接口定义了新池。



7. 在定义池之后，单击 **OK** 以返回到 NAT 规则配置窗口。请确保在 Address Pool 下拉列表下选择刚创建的正确池。

Add Address Translation Rule

Use NAT Use Policy NAT

Source Host/Network

Interface:

IP Address:

Mask:

Translate Address on Interface:

Translate Address To

Static IP Address:

Redirect port

TCP Original port: Translated port:

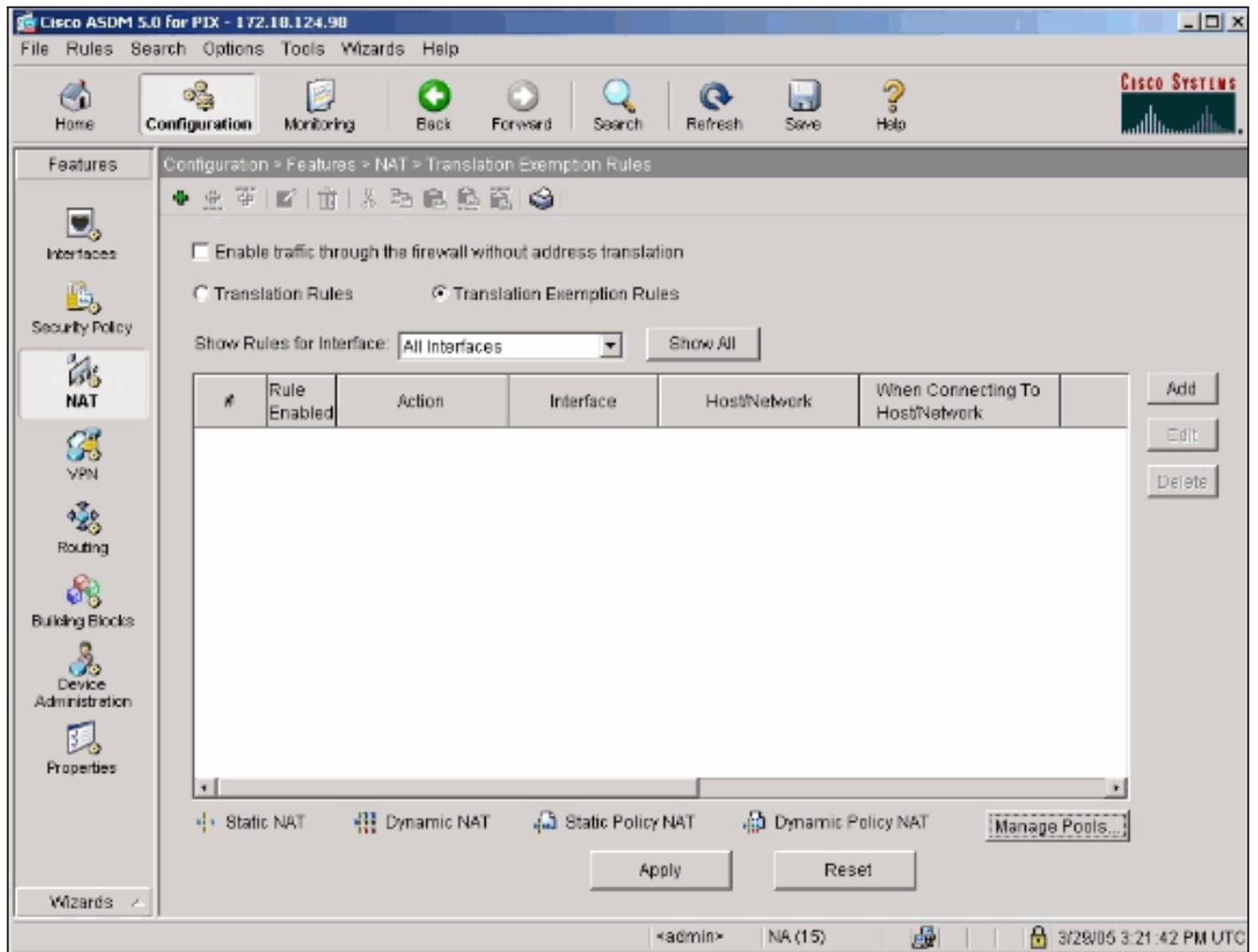
UDP

Dynamic Address Pool:

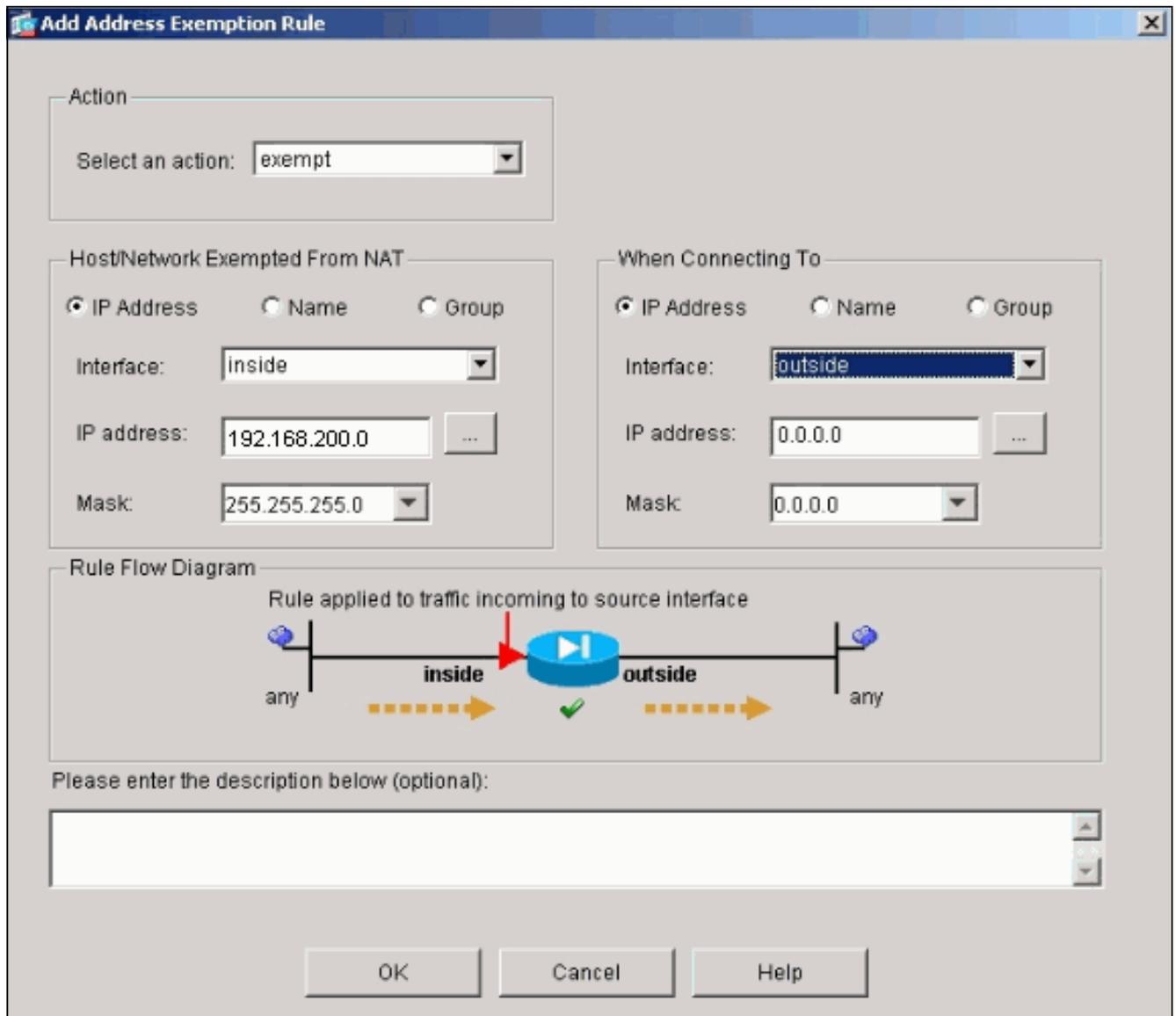
Pool ID	Address
1	172.16.199.3- 172.16.199.62

现在，您已创建了一个通过安全设备的 NAT 转换。但是，您仍然需要创建指定不对什么数据流执行 NAT 的 NAT 条目。

- 单击位于窗口顶部的 **Translation Exemption Rules**，然后单击 **Add** 以创建新规则。



9. 选择 *inside interface* 作为源，并指定 *192.168.200.0/24* 子网。保留“*When connecting*”值为默认值。



现在已定义了 NAT 规则。

10. 单击 **Apply** 以将更改应用于安全设备的当前运行配置。此输出显示已应用于 PIX/ASA 配置的实际增加内容。这与通过手动方法输入的命令稍有不同，但它们的作用是相同的。

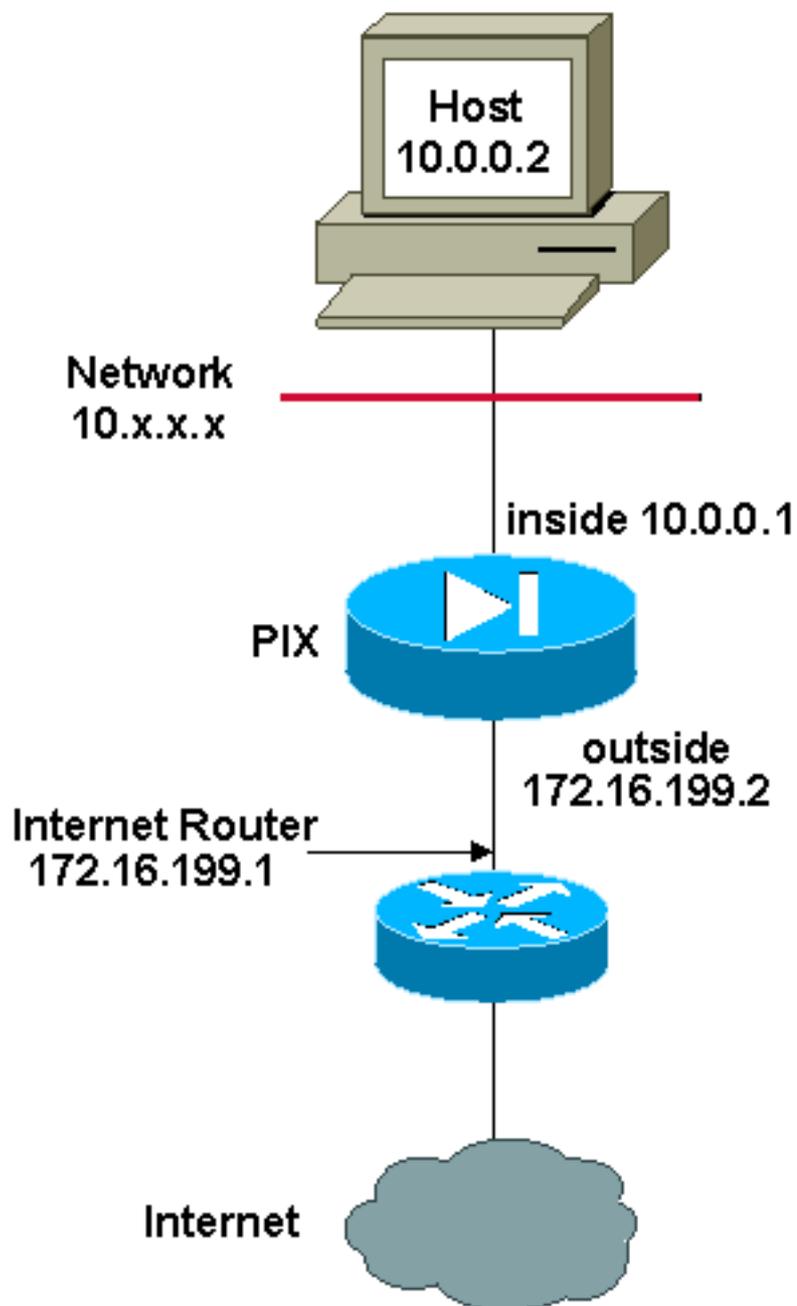
```
access-list inside_nat0_outbound extended permit
ip 192.168.200.0 255.255.255.0 any
```

```
global (outside) 1 172.16.199.3-172.16.199.62 netmask 255.255.255.192
```

```
nat (inside) 0 access-list inside_nat0_outbound
nat (inside) 1 10.0.0.0 255.255.255.0
```

[多个全局池](#)

[网络图](#)



注意：此配置中使用的IP编址方案在Internet上无法合法路由。这些地址是在实验室环境中使用的[RFC 1918 地址](#)。

在本示例中，网络管理员有在 Internet 上注册的两个 IP 地址范围。网络管理员必须将所有内部地址（位于 10.0.0.0/8 范围中）转换为注册地址。网络管理器必须使用的IP地址范围是172.16.199.1到172.16.199.62和192.168.150.1到192.168.150.254。网络管理器可以通过以下方式实现：

```
global (outside) 1 172.16.199.3-172.16.199.62 netmask 255.255.255.192
global (outside) 1 192.168.150.1-192.168.150.254 netmask 255.255.255.0
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
```

在动态 NAT 中，更具体的语句是当您在全局使用同一个接口时优先的那条语句。

```
nat (inside) 1 10.0.0.0 255.0.0.0
nat (inside) 2 10.1.0.0 255.255.0.0
global (outside) 1 172.16.1.1
```

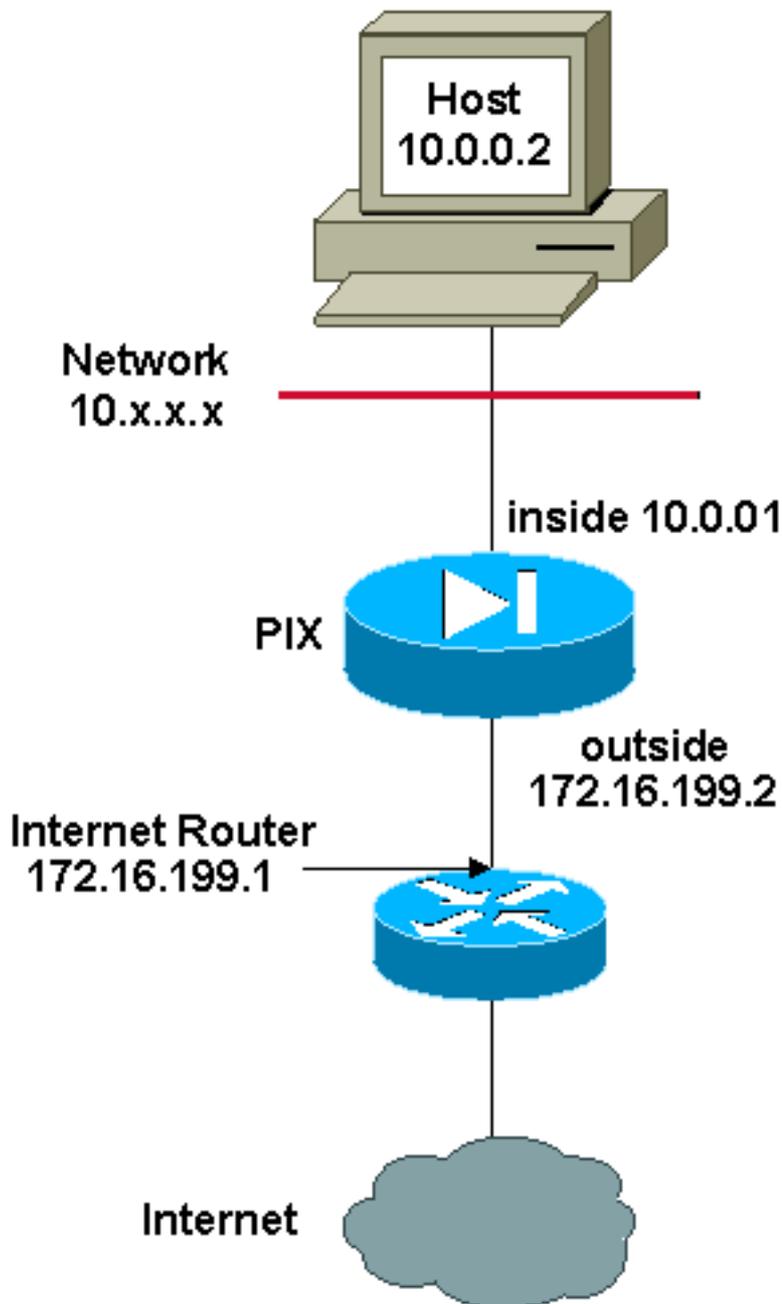
```
global (outside) 2 192.168.1.1
```

如果有内部网络 10.1.0.0，NAT global 2 优先于 1，因为它对于转换更具体。

注意：NAT语句中使用通配符编址方案。此语句告诉 PIX/ASA 在任何内部源地址访问 Internet 时都对该地址进行转换。如果需要，此命令中的地址可以更具体。

混合 NAT 和 PAT 全局语句

网络图



注意：此配置中使用的IP编址方案在Internet上无法合法路由。这些地址是在实验室环境中使用的 [RFC 1918 地址](#)。

在本示例中，ISP 为网络管理员提供了从 172.16.199.1 到 172.16.199.63 的地址范围，供公司使用。网络管理员决定将 172.16.199.1 用于 Internet 路由器上的内部接口，将 172.16.199.2 用于 PIX/ASA 上的外部接口。剩下的从 172.16.199.3 到 172.16.199.62 的地址可用于 NAT 池。但是

，网络管理员知道，随时可能有 60 个以上的用户尝试访问 PIX/ASA 外部。因此，网络管理员决定拿出 172.16.199.62 并将其设为 PAT 地址，以便多个用户可以同时共享一个地址。

```
global (outside) 1 172.16.199.3-172.16.199.61 netmask 255.255.255.192
```

```
global (outside) 1 172.16.199.62 netmask 255.255.255.192
```

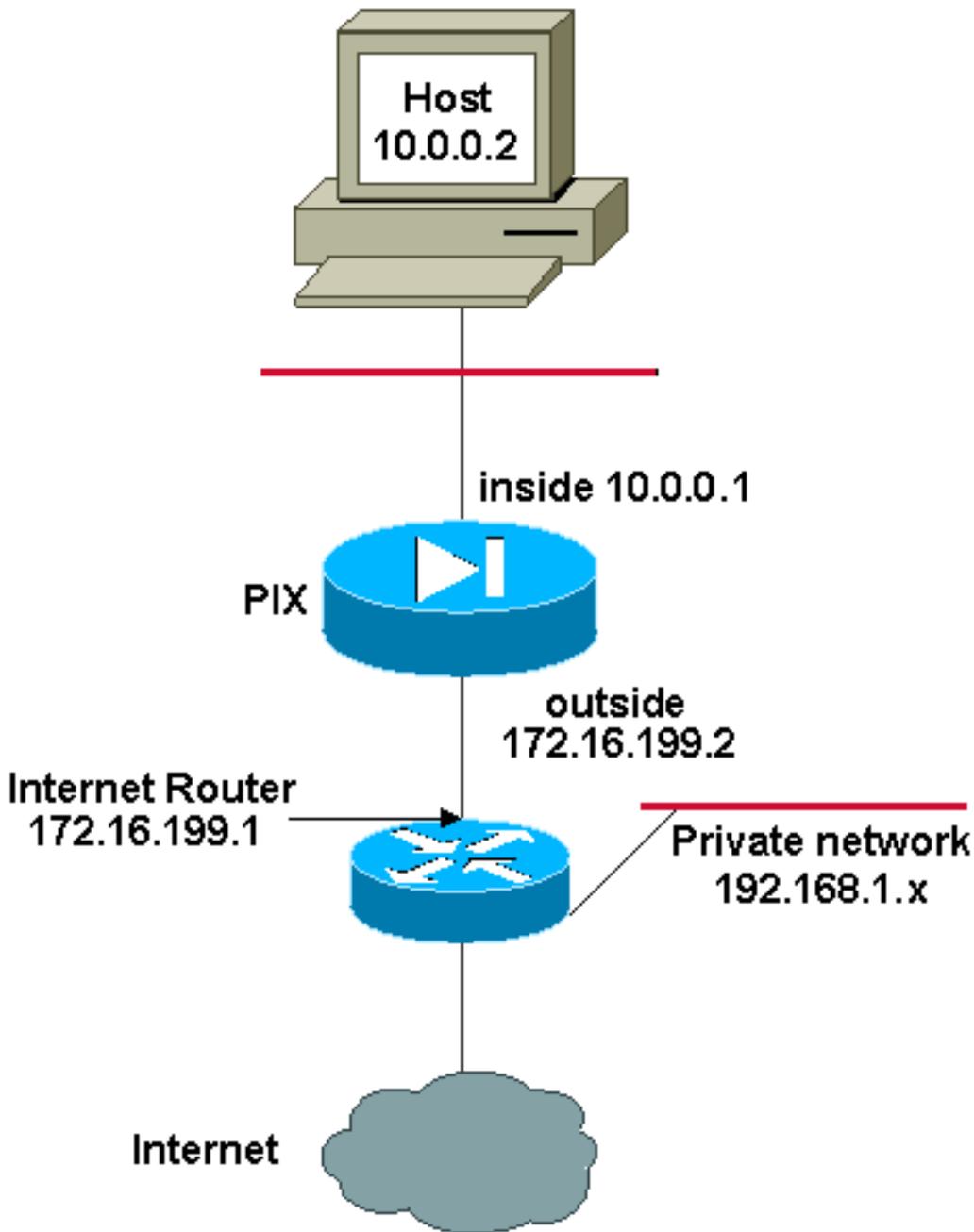
```
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
```

这些命令指示 PIX/ASA 将前 59 个要通过 PIX/ASA 的内部用户的源地址转换成从 172.16.199.3 到 172.16.199.61 的地址。在用完这些地址后，PIX 将所有后续源地址转换为 172.16.199.62，直到 NAT 池中的一个地址处于空闲状态为止。

注意：NAT语句中使用通配符编址方案。此语句告诉 PIX/ASA 在任何内部源地址访问 Internet 时都对该地址进行转换。如果需要，此命令中的地址可以更具具体。

[使用 NAT 0 Access-List 的多条 NAT 语句](#)

[网络图](#)



注意：此配置中使用的IP编址方案在Internet上无法合法路由。这些地址是在实验室环境中使用的[RFC 1918 地址](#)。

在本示例中，ISP为网络管理器提供从172.16.199.1到172.16.199.63的地址范围。网络管理器决定将172.16.199.1分配给Internet路由器的内部接口，将172.16.199.2分配给PIX/ASA的外部接口。

但是，在此方案中，有另一个专用 LAN 分段位于 Internet 路由器之外。当这两个网络中的主机相互通信时，网络管理器不愿意浪费全局池中的地址。网络管理器仍然需要在所有内部用户 (10.0.0.0/8) 访问 Internet 时转换这些用户的源地址。

```
access-list 101 permit ip 10.0.0.0 255.0.0.0 192.168.1.0 255.255.255.0
```

```
global (outside) 1 172.16.199.3-172.16.199.62 netmask 255.255.255.192
```

```
nat (inside) 0 access-list 101
```

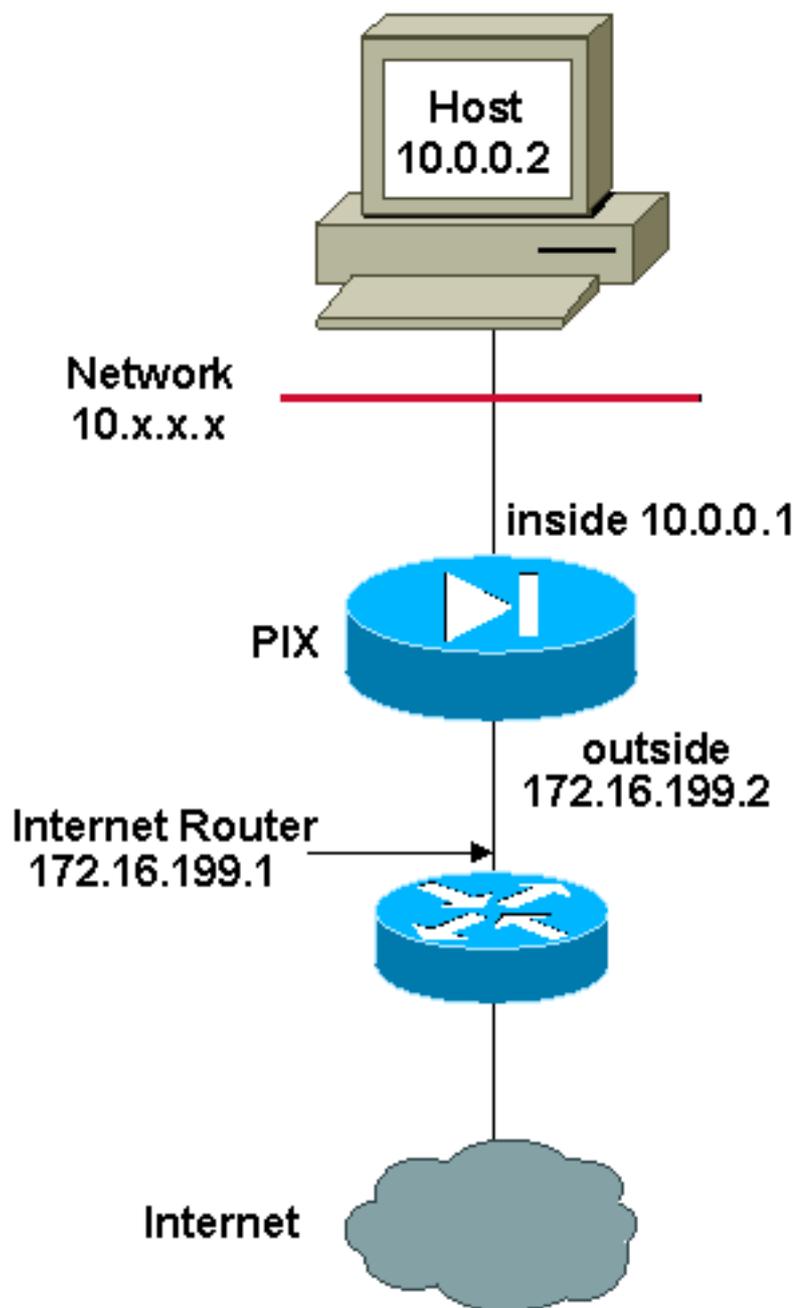
```
nat (inside) 1 10.0.0.0 255.0.0.0 0 0
```

此配置不会将源地址为10.0.0.0/8且目标地址为192.168.1.0/24的地址转换为地址，它会将源地址从10.0.0.0/8网络内发起并发往192.168.1.0/24以外任何位置的任何流量转换为地址范围从172.16.199.3到172.16.199.62。

如果您有来自 Cisco 设备的 `write terminal` 命令的输出，则可以使用[命令输出解释程序工具 \(仅限注册用户\)](#)。

使用策略 NAT

网络图



注意：此配置中使用的IP编址方案在Internet上无法合法路由。这些地址是在实验室环境中使用的[RFC 1918 地址](#)。

当您对 0 以外的任何 NAT ID 配合使用访问列表和 `nat` 命令时，您便启用了策略 NAT。

注意：6.3.2版中引入了策略NAT。

策略 NAT 允许您在访问列表中指定源地址和目标地址（或端口）时标识要进行地址转换的本地数据流。常规 NAT 仅使用源地址/端口，而策略 NAT 同时使用源和目标地址/端口。

注意：除NAT免除(nat 0 access-list)外，所有类型的NAT都支持策略NAT。“NAT 免除”使用访问控制表标识本地地址，但与策略 NAT 不同的是它不考虑端口。

使用策略 NAT，可以创建多条标识同一本地地址的 NAT 或 static 语句（只要源/端口和目标/端口组合对于每条语句是唯一的）。然后，您可以将不同的全局地址匹配到每个源/端口和目标/端口对。

在本示例中，网络管理员为端口 80 (Web) 和端口 23 (Telnet) 提供了对目标 IP 地址 192.168.201.11 的访问权限，但必须使用两个不同的 IP 地址作为源地址。IP 地址 172.16.199.3 用作 Web 的源地址。IP 地址 172.16.199.4 用于 Telnet，并且必须转换位于 10.0.0.0/8 范围中的所有内部地址。网络管理员可使用以下命令执行此操作：

```
access-list WEB permit tcp 10.0.0.0 255.0.0.0 192.168.201.11  
255.255.255.255 eq 80
```

```
access-list TELNET permit tcp 10.0.0.0 255.0.0.0 192.168.201.11  
255.255.255.255 eq 23
```

```
nat (inside) 1 access-list WEB
```

```
nat (inside) 2 access-list TELNET
```

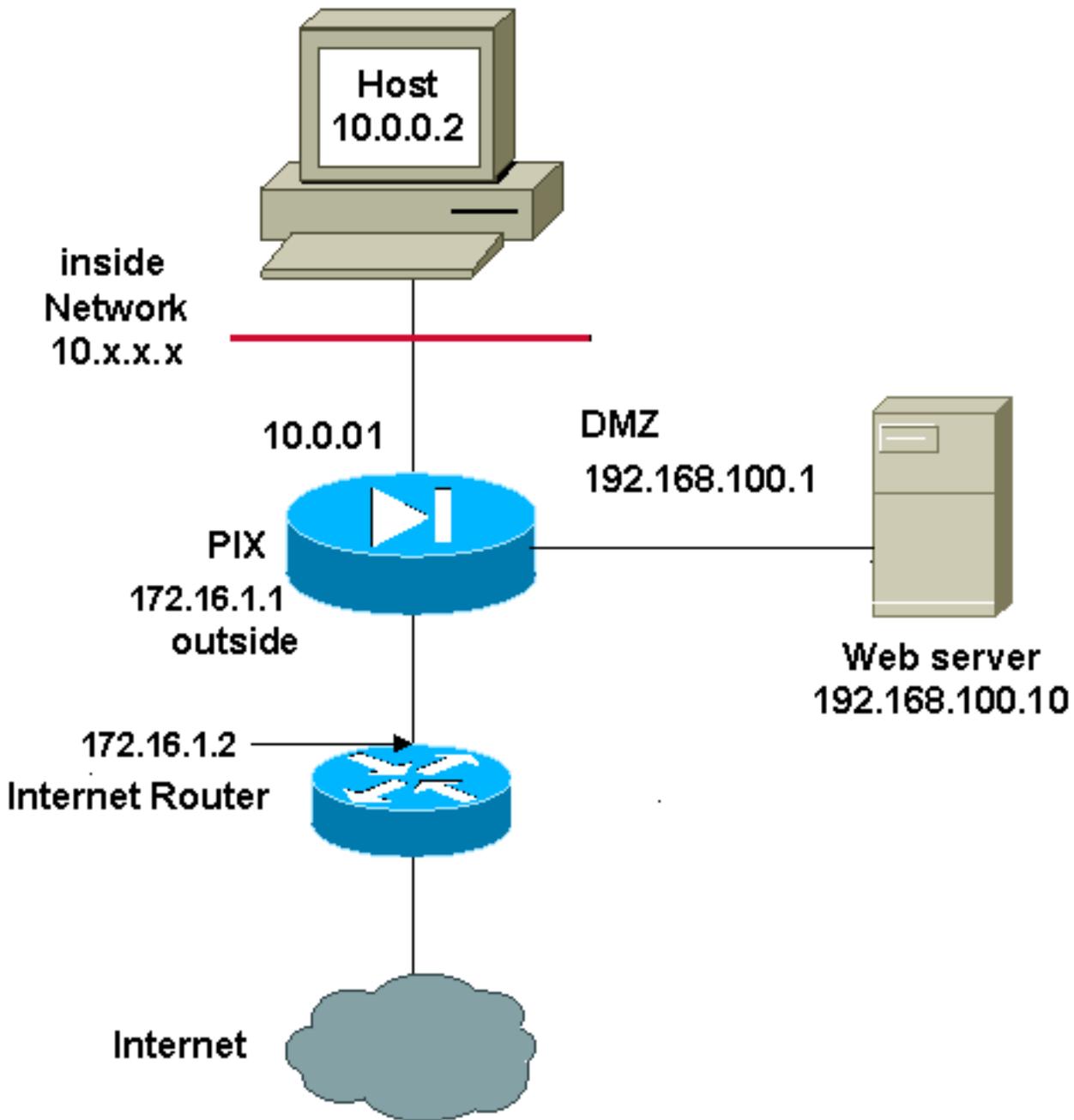
```
global (outside) 1 172.16.199.3 netmask 255.255.255.192
```

```
global (outside) 2 172.16.199.4 netmask 255.255.255.192
```

您可以使用[命令输出解释程序工具（仅限注册用户）](#)显示潜在问题和解决方法。

静态NAT

网络图



注意：此配置中使用的IP编址方案在Internet上无法合法路由。这些地址是在实验室环境中使用的 [RFC 1918 地址](#)。

一个静态 NAT 配置创建一个一对一的映射，并将某个具体地址转换为另一个地址。只要此类配置存在且使内部和外部主机都能够建立连接，此类配置就可在 NAT 表中创建永久性条目。这对于提供应用程序服务（如邮件、Web、FTP 等）的主机最有用。在本示例中，配置了静态 NAT 语句以允许内部用户和外部用户访问 DMZ 上的 Web 服务器。

此输出显示如何构建静态语句。请注意映射的 IP 地址和实际 IP 地址的顺序。

```
static (real_interface,mapped_interface) mapped_ip real_ip netmask mask
```

创建以下静态转换可授予内部接口上的用户对 DMZ 上服务器的访问权限。它在内部地址和 DMZ 上的服务器地址之间创建一个映射。内部用户便可以通过内部地址访问 DMZ 上的服务器。

```
static (DMZ,inside) 10.0.0.10 192.168.100.10 netmask 255.255.255.255
```

创建以下静态转换可授予外部接口上的用户对 DMZ 上服务器的访问权限。它在外部地址和 DMZ 上的服务器地址之间创建一个映射。外部用户便可以通过外部地址访问 DMZ 上的服务器。

```
static (DMZ,outside) 172.16.1.5 192.168.100.10 netmask 255.255.255.255
```

注意：由于外部接口的安全级别低于DMZ，因此还必须创建访问列表以允许外部用户访问DMZ上的服务器。访问列表必须授予用户对静态转换中映射的地址的访问权限。建议将此访问列表设置得尽可能具体。在本例中，任何主机都只被允许访问 Web 服务器上的端口 80 (www/http) 和 443 (https)。

```
access-list OUTSIDE extended permit tcp any host 172.16.1.5 eq www
access-list OUTSIDE extended permit tcp any host 172.16.1.5 eq https
```

然后必须将访问列表应用于外部接口。

```
access-group OUTSIDE in interface outside
```

有关 **access-list** 和 **access-group** 命令的详细信息，请参阅 [access-list extended](#) 和 [access-group](#)。

[如何绕过 NAT](#)

本部分介绍如何绕过 NAT。当您启用 NAT 控制时，您可能希望绕过 NAT。您可以使用身份 NAT、静态身份 NAT 或 NAT 免除来绕过 NAT。

[配置身份 NAT](#)

身份 NAT 将实际 IP 地址转换为相同的 IP 地址。只有“转换的”主机可以创建 NAT 转换，并且允许发送回响应数据流。

注意：如果更改 NAT 配置，并且不希望等待现有转换超时后再使用新的 NAT 信息，则可以使用 **clear xlate** 命令以清除转换表。但是，当您清除转换表时，使用转换的所有当前连接都将断开。

要配置身份 NAT，请输入以下命令：

```
hostname(config)#nat (real_interface) 0 real_ip
[mask [dns] [outside] [norandomseq] [tcp] tcp_max_conns [emb_limit]] [udp
udp_max_conns]
```

例如，要对内部 10.1.1.0/24 网络使用身份 NAT，请输入以下命令：

```
hostname(config)#nat (inside) 0 10.1.1.0
255.255.255.0
```

有关 **nat** 命令的详细信息，请参阅 [Cisco 安全设备命令参考，版本 7.2。](#)

[配置静态身份 NAT](#)

静态身份 NAT 将实际 IP 地址转换为相同的 IP 地址。转换始终处于活动状态，并且“转换的”主机和远程主机都可以发起连接。静态身份 NAT 允许您使用常规 NAT 或策略 NAT。策略 NAT 允许您在

确定要转换的实际地址时标识实际和目标地址（有关策略 NAT 的详细信息，请参阅[使用策略 NAT 部分](#)）。例如，您可以在内部地址访问外部接口且目标为服务器 A 时对内部地址使用策略静态身份 NAT，但在其访问外部服务器 B 时使用普通转换。

注意：如果删除 static 命令，使用该转换的当前连接不受影响。要删除这些连接，请输入 [clear local-host 命令](#)。使用 [clear xlate 命令](#) 不能从转换表中清除静态转换；您必须删除 static 命令。使用 [clear xlate 命令](#) 只能删除由 nat 和 global 命令创建的动态转换。

要配置策略静态身份 NAT，请输入以下命令：

```
hostname(config)#static
(real_interface,mapped_interface) real_ip access-list acl_id [dns]
[norandomseq] [[tcp] tcp_max_conns [emb_limit]] [udp udp_max_conns]
```

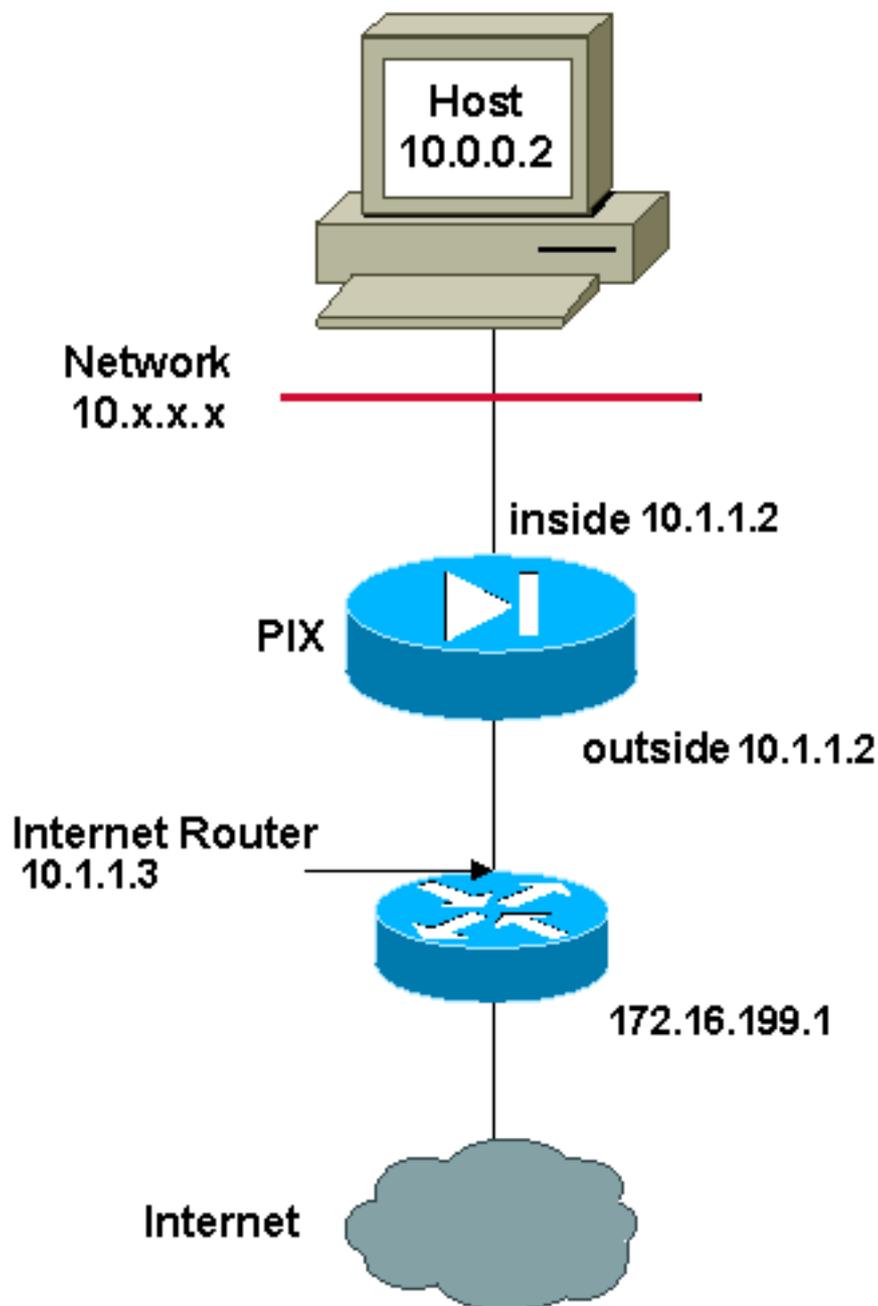
请使用 [access-list extended 命令](#) 创建[扩展访问列表](#)。此访问列表应该只包括允许 ACE。请确保访问列表中的源地址与此命令中的 real_ip 匹配。策略 NAT 不考虑 inactive 或 time-range 关键字；对于策略 NAT 配置，所有 ACE 都被认为处于活动状态。有关详细信息，[使用策略 NAT 部分](#)。

要配置常规静态身份 NAT，请输入以下命令：

```
hostname(config)#static
(real_interface,mapped_interface) real_ip real_ip [netmask mask] [dns]
[norandomseq] [[tcp] tcp_max_conns [emb_limit]] [udp
udp_max_conns]
```

为两个 real_ip 参数指定相同的 IP 地址。

网络图



注意：此配置中使用的IP编址方案在Internet上无法合法路由。这些地址是在实验室环境中使用的[RFC 1918 地址](#)。

例如，当内部 IP 地址 (10.1.1.2) 被外部地址访问时，此命令对该内部地址使用静态身份 NAT：

```
hostname(config)#static (inside,outside) 10.1.1.2  
10.1.1.2 netmask 255.255.255.255
```

有关 static 命令的详细信息，请参阅 [Cisco 安全设备命令参考，版本 7.2](#)。

当外部地址 (172.16.199.1) 被内部地址访问时，此命令对该外部地址使用静态身份 NAT：

```
hostname(config)#static (outside,inside) 172.16.199.1  
172.16.199.1 netmask 255.255.255.255
```

此命令静态地映射整个子网：

```
hostname(config)#static (inside,dmz) 10.1.1.2 10.1.1.2
netmask 255.255.255.0
```

此静态身份策略 NAT 示例显示在访问一个目标地址时使用身份 NAT，在访问另一个目标地址时使用转换的单个实际地址：

```
hostname(config)#access-list NET1 permit ip host
10.1.1.3 172.16.199.0 255.255.255.224
```

```
hostname(config)#access-list NET2 permit ip host
10.1.1.3 172.16.199.224 255.255.255.224
```

```
hostname(config)#static (inside,outside) 10.1.1.3
access-list NET1
```

```
hostname(config)#static (inside,outside) 172.16.199.1
access-list NET2
```

注意： 有关 `static` 命令的详细信息，请参阅 [Cisco ASA 5580 自适应安全设备命令参考，版本 8.1。](#)

注意： 有关访问列表的详细信息，请参阅 [Cisco ASA 5580 自适应安全设备命令行配置指南，版本 8.1。](#)

[配置 NAT 免除](#)

“NAT 免除”使一些地址免于转换，并同时允许实际主机和远程主机发起连接。“NAT 免除”允许您在确定要免除的实际数据流时指定实际和目标地址（类似于策略 NAT），因此使用“NAT 免除”比使用身份 NAT 拥有更大的控制权。但是与策略 NAT 不同，“NAT 免除”不考虑访问列表中的端口。使用静态身份 NAT 可考虑访问列表中的端口。

注意： 如果删除“NAT 免除”配置，使用“NAT 免除”的现有连接不受影响。要删除这些连接，请输入 [clear local-host 命令](#)。

要配置“NAT 免除”，请输入以下命令：

```
hostname(config)#nat (real_interface) 0 access-list
acl_name [outside]
```

使用 [access-list extended 命令创建扩展访问列表](#)。此访问列表可以同时包括允许 ACE 和拒绝 ACE。请勿在访问列表中指定实际和目标端口；“NAT 免除”不考虑端口。“NAT 免除”也不考虑 `inactive` 或 `time-range` 关键字；对于“NAT 免除”配置，所有 ACE 都被认为处于活动状态。

默认情况下，此命令将免除从内部到外部的数据流。如果希望从外部到内部的数据流绕过 NAT，请另外添加一个 `nat` 命令并输入 `outside` 以将 NAT 实例标识为外部 NAT。如果为外部接口配置动态 NAT 并且希望免除其他数据流，您可能需要使用外部 NAT 免除。

例如，要在内部网络访问任何目标地址时免除内部网络，请输入以下命令：

```
hostname(config)#access-list EXEMPT permit ip 10.1.1.0
255.255.255.0 any
```

```
hostname(config)# nat (inside) 0 access-list
EXEMPT
```

要对 DMZ 网络使用动态外部 NAT 并免除另一个 DMZ 网络，请输入以下命令：

```
hostname(config)#nat (dmz) 1 10.1.1.0 255.255.255.0
outside dns
```

```
hostname(config)#global (inside) 1
10.1.1.2
```

```
hostname(config)#access-list EXEMPT permit ip 10.1.1.0
255.255.255.0 any
```

```
hostname(config)#nat (dmz) 0 access-list
EXEMPT
```

要在内部地址访问两个不同的目标地址时免除内部地址，请输入以下命令：

```
hostname(config)#access-list NET1 permit ip 10.1.1.0
255.255.255.0 172.16.199.0 255.255.255.224
```

```
hostname(config)#access-list NET1 permit ip 10.1.1.0
255.255.255.0 172.16.199.224 255.255.255.224
```

```
hostname(config)#nat (inside) 0 access-list NET1
```

验证

流经安全设备的数据流很可能经过 NAT。请参阅 [PIX/ASA：监控和排除性能问题](#)。

show xlate count 命令显示通过 PIX 的当前转换数和最大转换数。转换是内部地址到外部地址的映射，可能是一对一的映射（如 NAT），也可能是多对一的映射（如 PAT）。此命令是 **show xlate** 命令的子集，它输出通过 PIX 的每个转换。命令输出显示了“in use”转换，这是指发出该命令时 PIX 中的活动转换数；“most used”是指自 PIX 通电后，在其上看到的最大转换数。

故障排除

[为端口443添加静态PAT时收到的错误消息](#)

问题

为端口443添加静态PAT时，您会收到以下错误消息：

```
[ERROR] static(INSIDE,OUTSIDE)tcp interface 443 192.168.1.87 443 netmask 255.255.255.255 tcp 0 0  
udp 0
```

PAT443

解决方案

当ASDM或WEBVPN在443端口上运行时，会出现此错误消息。要解决此问题，请登录防火墙并完成以下步骤之一：

- 要将ASDM端口更改为除443以外的任何端口，请运行以下命令：

```
ASA(config)#no http server enable  
ASA(config)#http server enable 8080
```

- 要将WEBVPN端口更改为除443以外的任何端口，请运行以下命令：

```
ASA(config)#webvpn  
ASA(config-webvpn)#enable outside  
ASA(config-webvpn)#port 65010
```

运行这些命令后，您应该能够将端口443上的NAT/PAT添加到另一台服务器。当您尝试将来使用ASDM管理ASA时，请将新端口指定为8080。

[错误：映射地址与现有静态地址冲突](#)

问题

在ASA上添加静态语句时，您会收到以下错误：

解决方案

验证要添加的静态源的条目是否尚不存在。

[相关信息](#)

- [PIX 支持页](#)
- [PIX 命令参考](#)
- [ASA 支持页](#)
- [ASA 命令参考](#)
- [请求注解 \(RFC\)](#)
- [技术支持和文档 - Cisco Systems](#)