PIX/ASA 7.x：使用 nat、global、static 和 access-list 命令进行端口重定向（转发）

目录

简介

为了在实施 Cisco PIX 安全设备版本 7.0 时最大程度地提高安全性，在使用 **nat-control**、nat、global、static、access-list 和 access-group 命令时，必须了解数据包在安全性较高的接口和安全性较低的接口之间的传递方式。本文档说明这些命令之间的差异，以及如何使用命令行界面或自适应安全设备管理器 (ASDM) 在 PIX 软件版本 7.x 中配置端口重定向（转发）和外部网络地址转换 (NAT) 功能。

注意： ASDM 5.2 及更高版本中的一些选项与 ASDM 5.1 中的选项看上去可能会有所不同。有关详细信息，请参阅 ASDM 文档。

先决条件

要求

为了允许使用 ASDM 配置设备，请参阅允许对 ASDM 进行 HTTPS 访问。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco PIX 500 系列安全设备软件版本 7.0 及更高版本
- ASDM 版本 5.x 及更高版本

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。

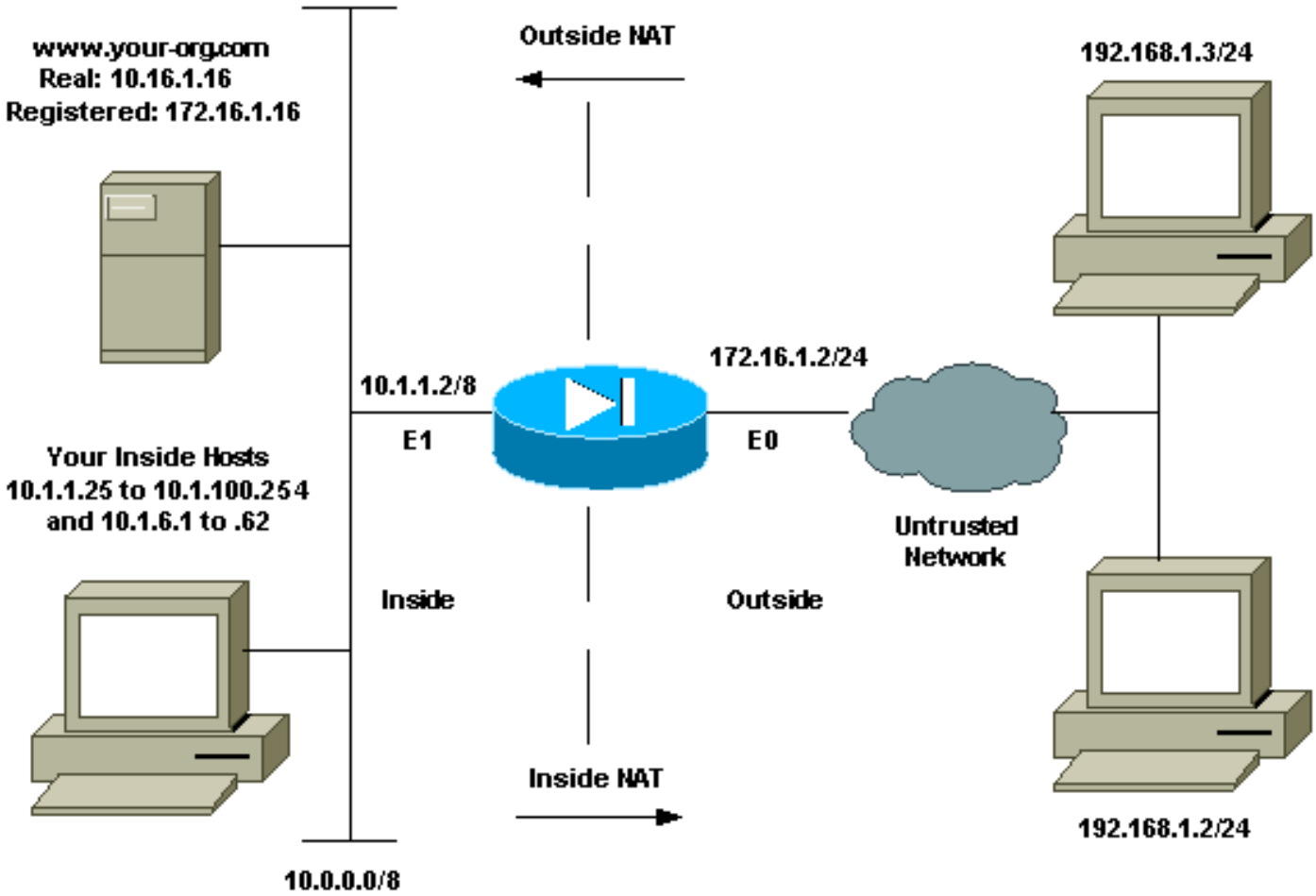
相关产品

您也可以将此配置用于 Cisco ASA 安全设备版本 7.x 及更高版本。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

网络图



此配置中使用的 IP 编址方案在 Internet 上不可合法路由。这些地址是在实验室环境中使用的 RFC

1918 地址。

初始配置

接口名称如下：

- **interface ethernet 0** - 外部名称
- **interface ethernet 1** - 内部名称

注意： 要查找有关本文档中所使用的命令的详细信息，请使用命令查找工具（仅限注册用户）。

允许出站访问

出站访问描述从较高安全级别的接口到较低安全级别的接口的连接。这包括从内部到外部的连接、从内部到隔离区 (DMZ) 的连接和从 DMZ 到外部的连接。只要连接源接口的安全级别高于目标接口的安全级别，这还可能包括从一个 DMZ 到另一个 DMZ 的连接。请查看 PIX 接口上的“security-level”配置进行确认。

本示例显示安全级别和接口名称配置：

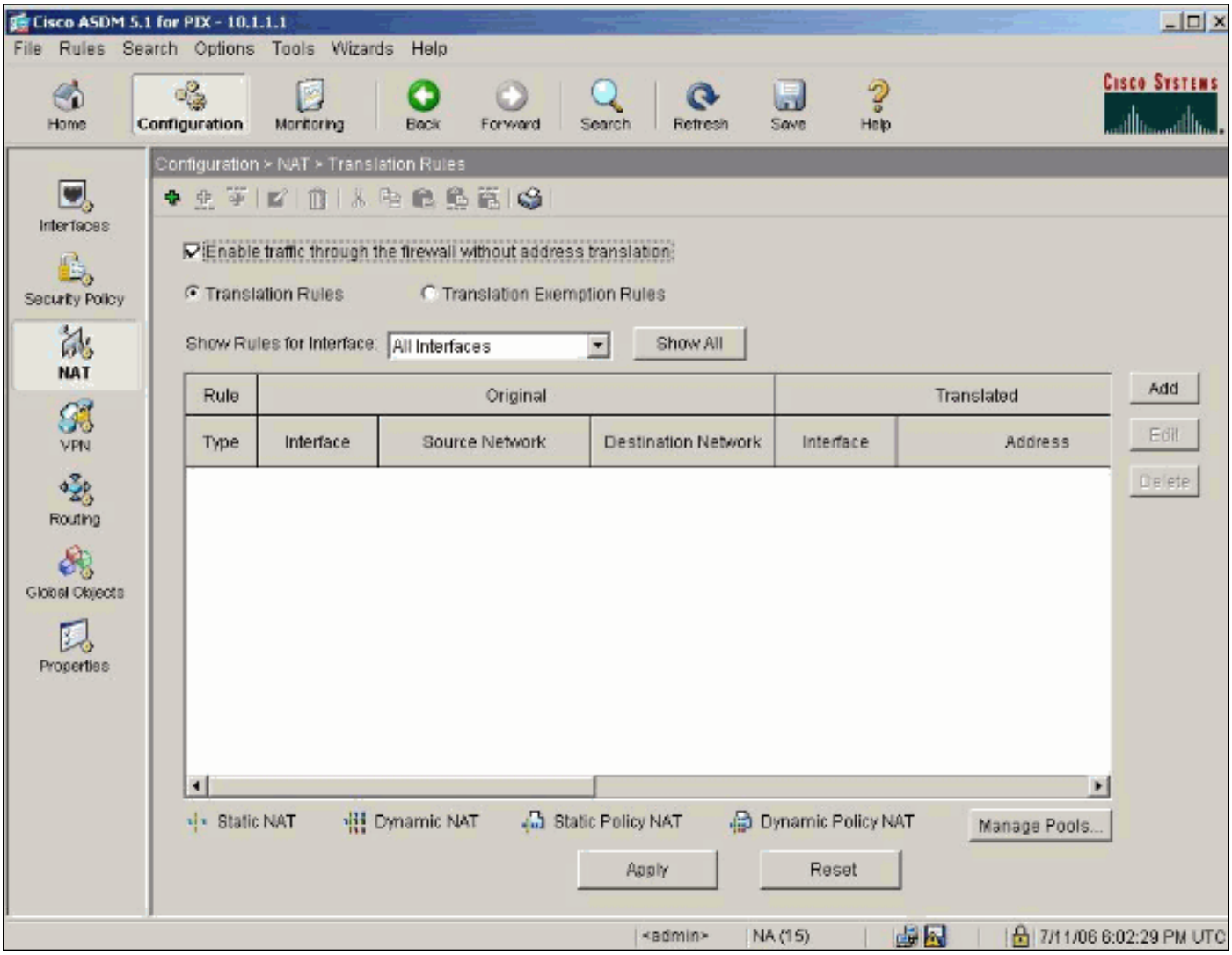
```
pix(config)#interface ethernet 0 pix(config-if)#security-level 0 pix(config-if)#nameif outside
pix(config-if)#exit
```

PIX 7.0 中引入了 **nat-control** 命令。您可以在配置模式下使用 **nat-control** 命令以指定 NAT 对于外部通信是否是必需的。启用 NAT 控制后，必须配置 NAT 规则才能允许出站数据流，这与以前版本的 PIX 软件一样。如果禁用 NAT 控制 (**no nat-control**)，则内部主机可以在不配置 NAT 规则的情况下与外部网络通信。但是，如果有些内部主机不具有公共地址，则仍然需要为这些主机配置 NAT。

为了使用 ASDM 配置 NAT 控制，请从 ASDM Home 窗口中选择 Configuration 选项卡，然后从功能菜单中选择 **NAT**。

Enable traffic through the firewall without translation：此选项在 PIX 版本 7.0(1) 中引入。选中此选项时，将在配置中发出 **no nat-control** 命令。此命令意味着不需要进行任何转换便可通过防火墙。通常只有当内部主机具有公用 IP 地址或网络拓扑不要求将内部主机转换为任何 IP 地址时，才选中此选项。

如果内部主机具有专用 IP 地址，则必须取消选中此选项，以便内部主机可以被转换为公用 IP 地址并访问 Internet。



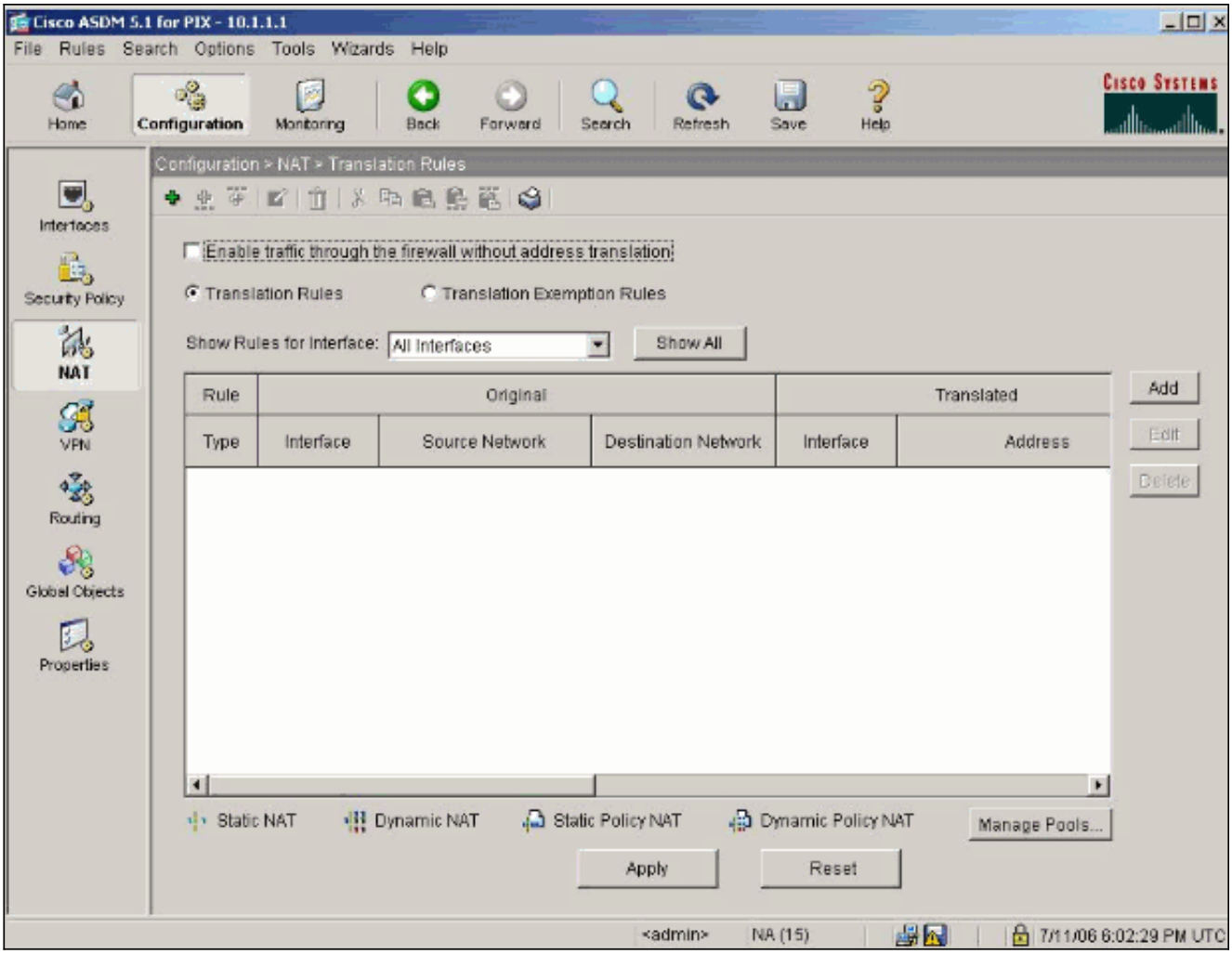
为了允许带有 NAT 控制的出站访问，需要使用两个策略。第一个是转换方法。这可以是使用 **static** 命令的静态转换，也可以是使用 nat/global 规则的动态转换。如果已禁用 NAT 控制并且内部主机具有公共地址，则不需要此策略。

出站访问的另一个要求（不管启用还是禁用 NAT 控制，此要求都适用）是是否存在访问控制列表 (ACL)。如果存在 ACL，则它必须允许源主机使用特定协议和端口访问目标主机。默认情况下，对于通过 PIX 的出站连接没有任何访问限制。这意味着如果没有为源接口配置 ACL，则在默认情况下，只要配置了转换方法便允许出站连接。

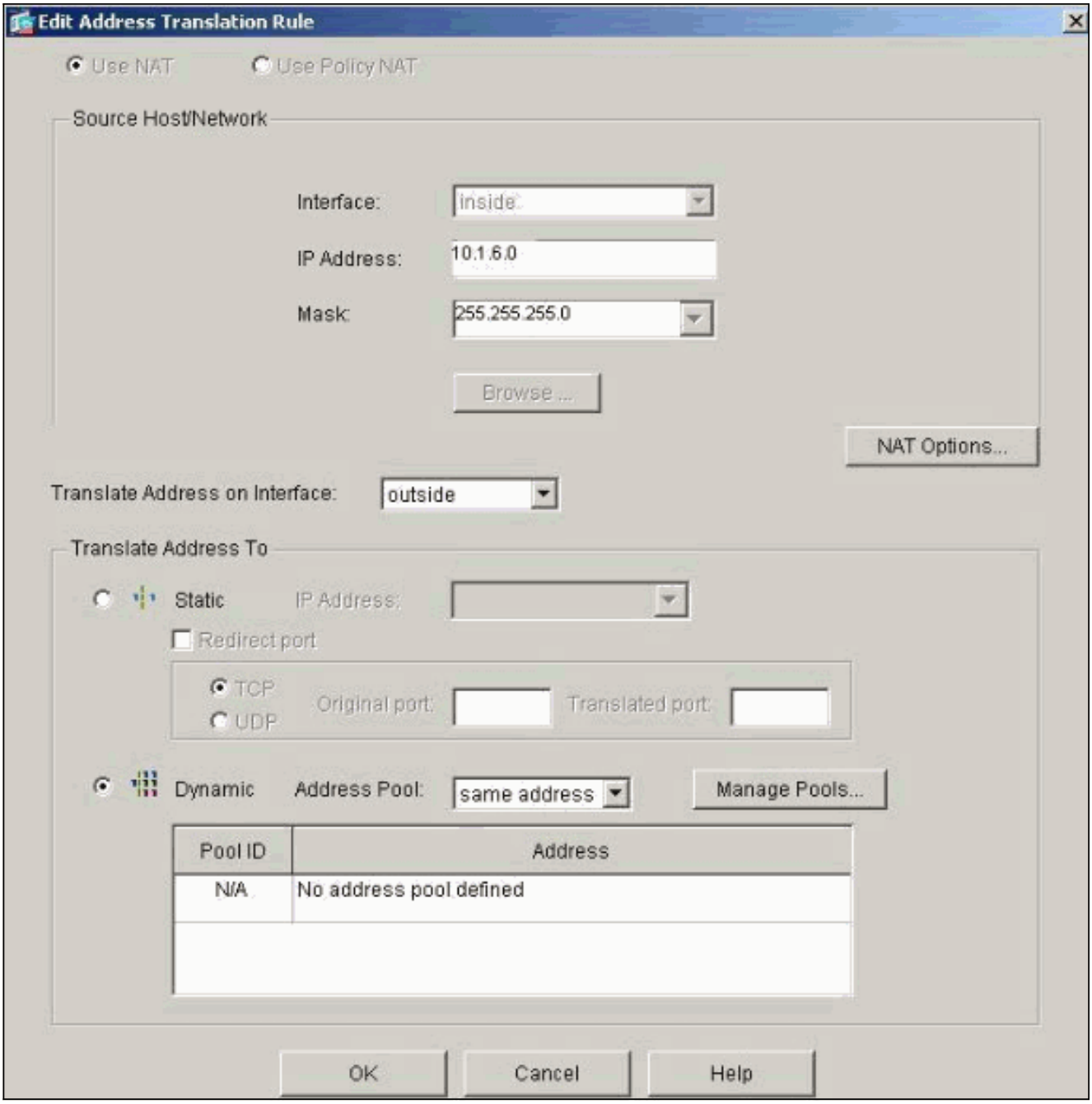
允许内部主机使用 NAT 访问外部网络

此配置授予子网 10.1.6.0/24 上的所有主机对外部的访问权限。为了实现此目的，请使用 **nat** 和 global 命令，如以下过程所示。

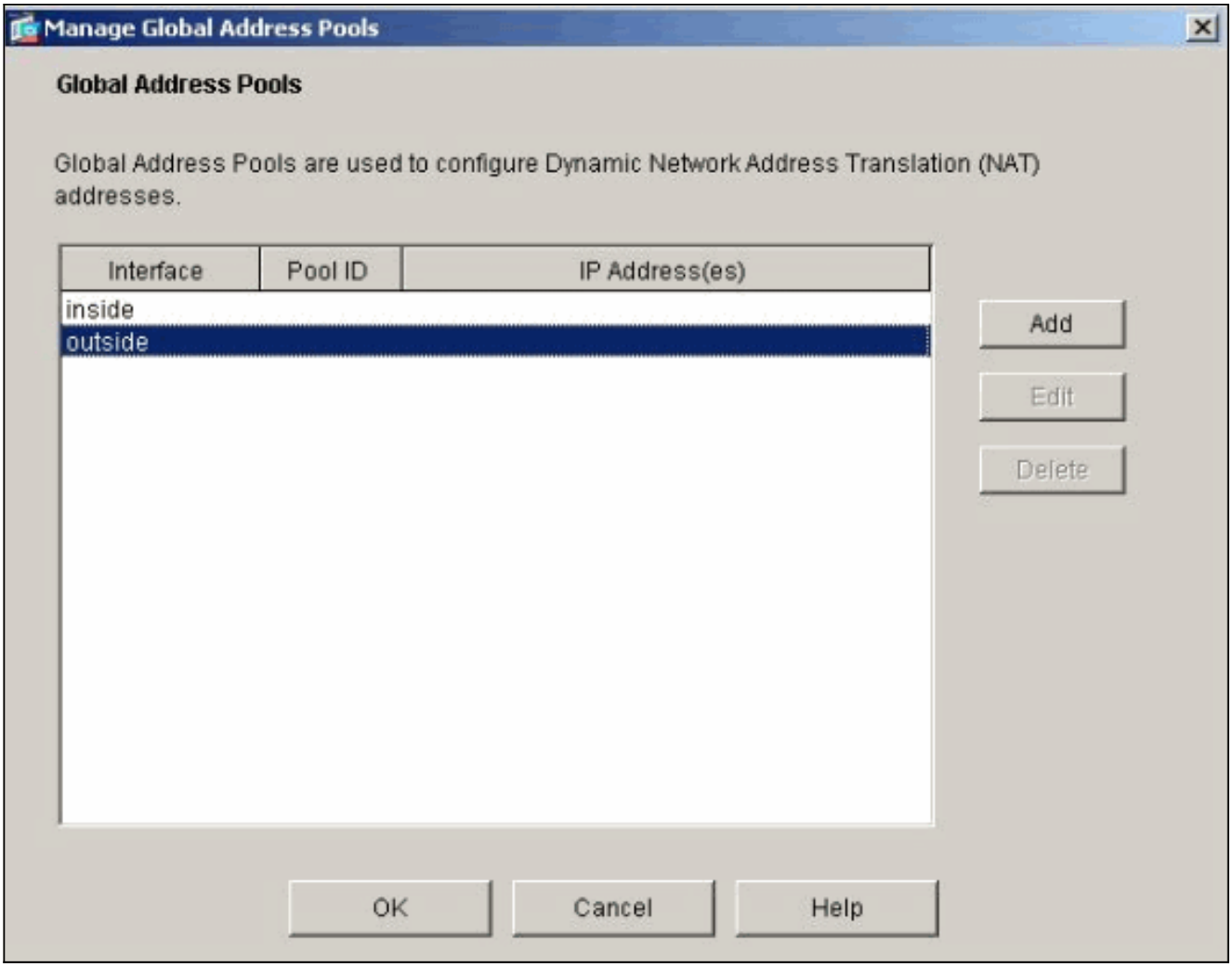
1. 定义要为 NAT 包括的内部组。
   ```
   nat (inside) 1 10.1.6.0 255.255.255.0
   ```
2. 在外部接口上指定 NAT 语句中定义的主机将被转换到的地址池。
   ```
   global (outside) 1 172.16.1.5-172.16.1.10 netmask 255.255.255.0
   ```
3. 使用 ASDM 来创建全局地址池。选择 **Configuration > Features > NAT** 并取消选中 Enable traffic through the firewall without address translation。然后单击 **Add** 以配置 NAT 规则。



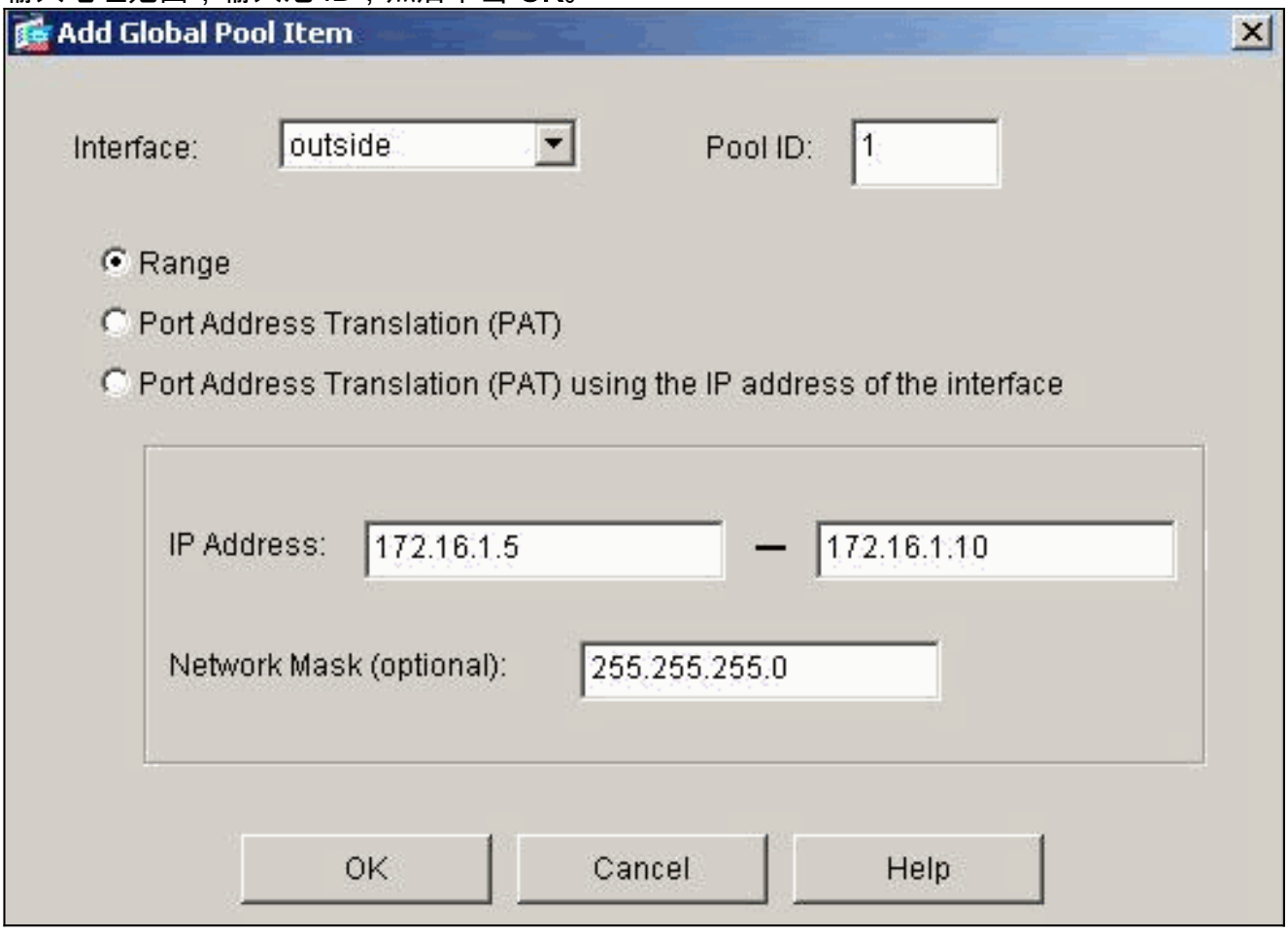
4. 单击 **Manage Pools** 以定义 NAT 池地址。



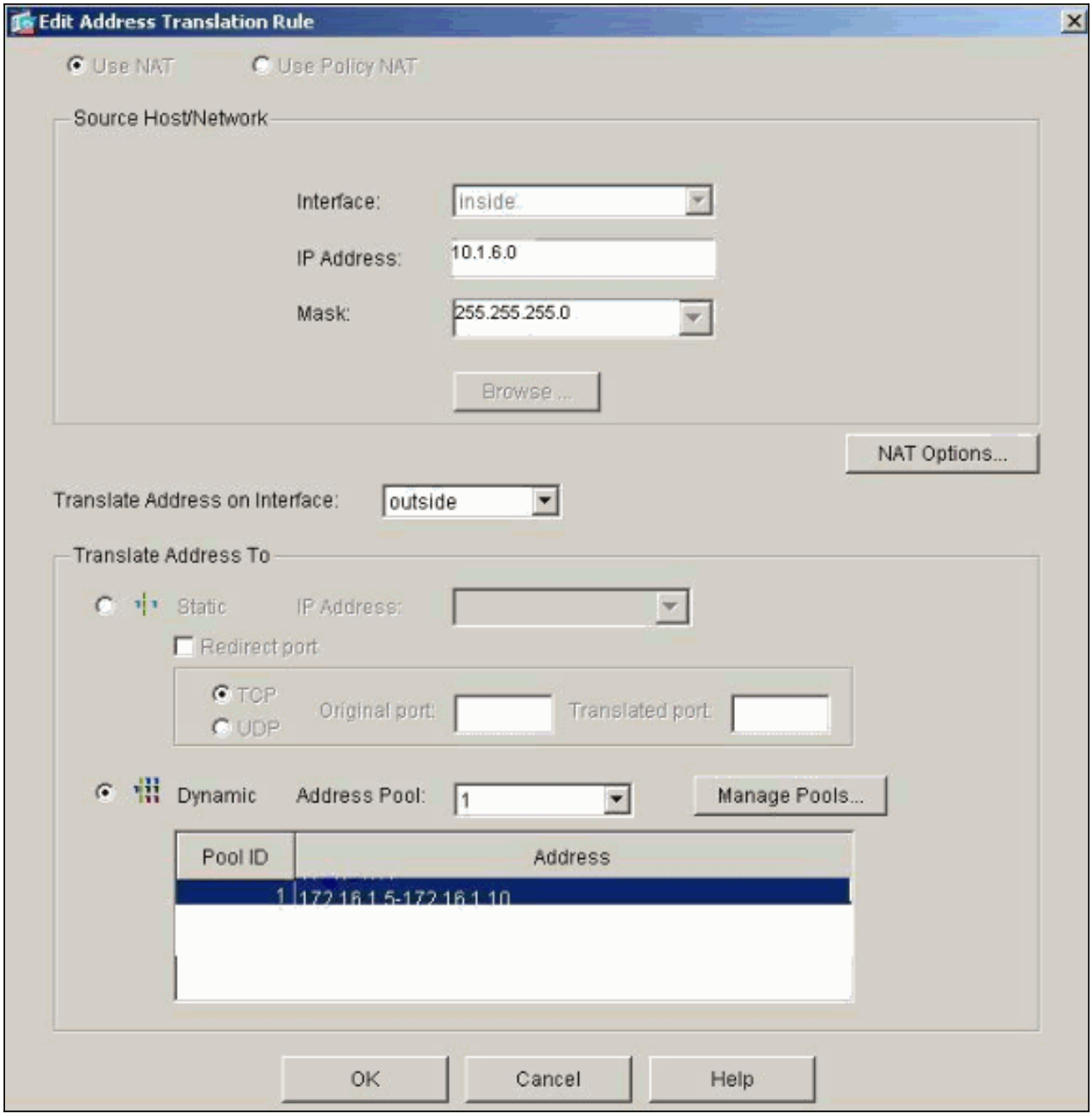
5. 选择 **Outside > Add**，并选择一个范围以指定地址池。



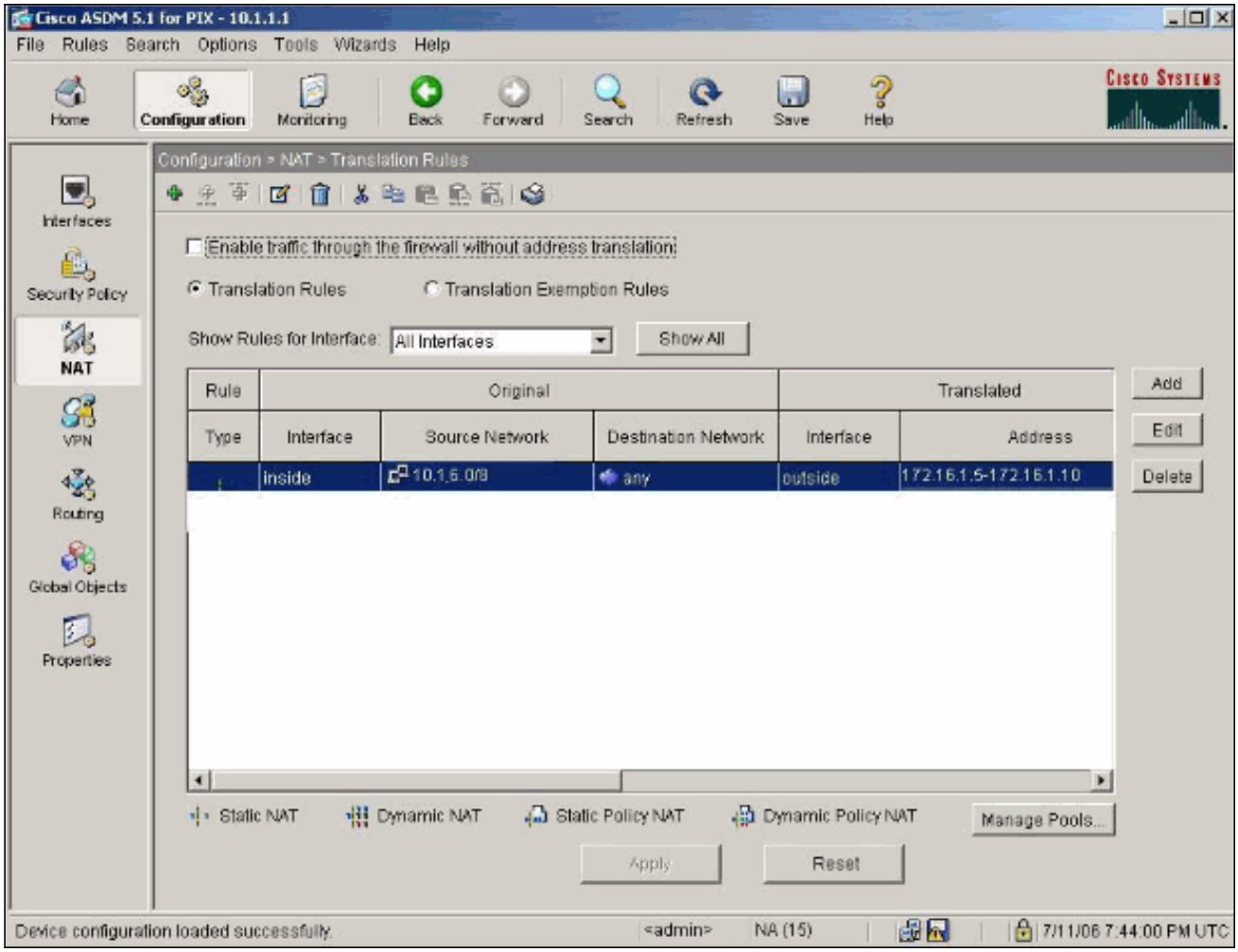
6. 输入地址范围，输入池 ID，然后单击 **OK**。



7. 选择 **Configuration > Features > NAT > Translation Rules** 以创建转换规则。
8. 选择 **Inside** 作为源接口，然后输入要进行 NAT 转换的地址。
9. 对于 Translate Address on Interface，选择 **Outside**，选择 Dynamic，然后选择您刚配置的地址池。
10. 单击 **Ok**。



11. 当您选择 **Configuration > Features > NAT > Translation Rules** 时，转换将显示在 Translation Rules 中。

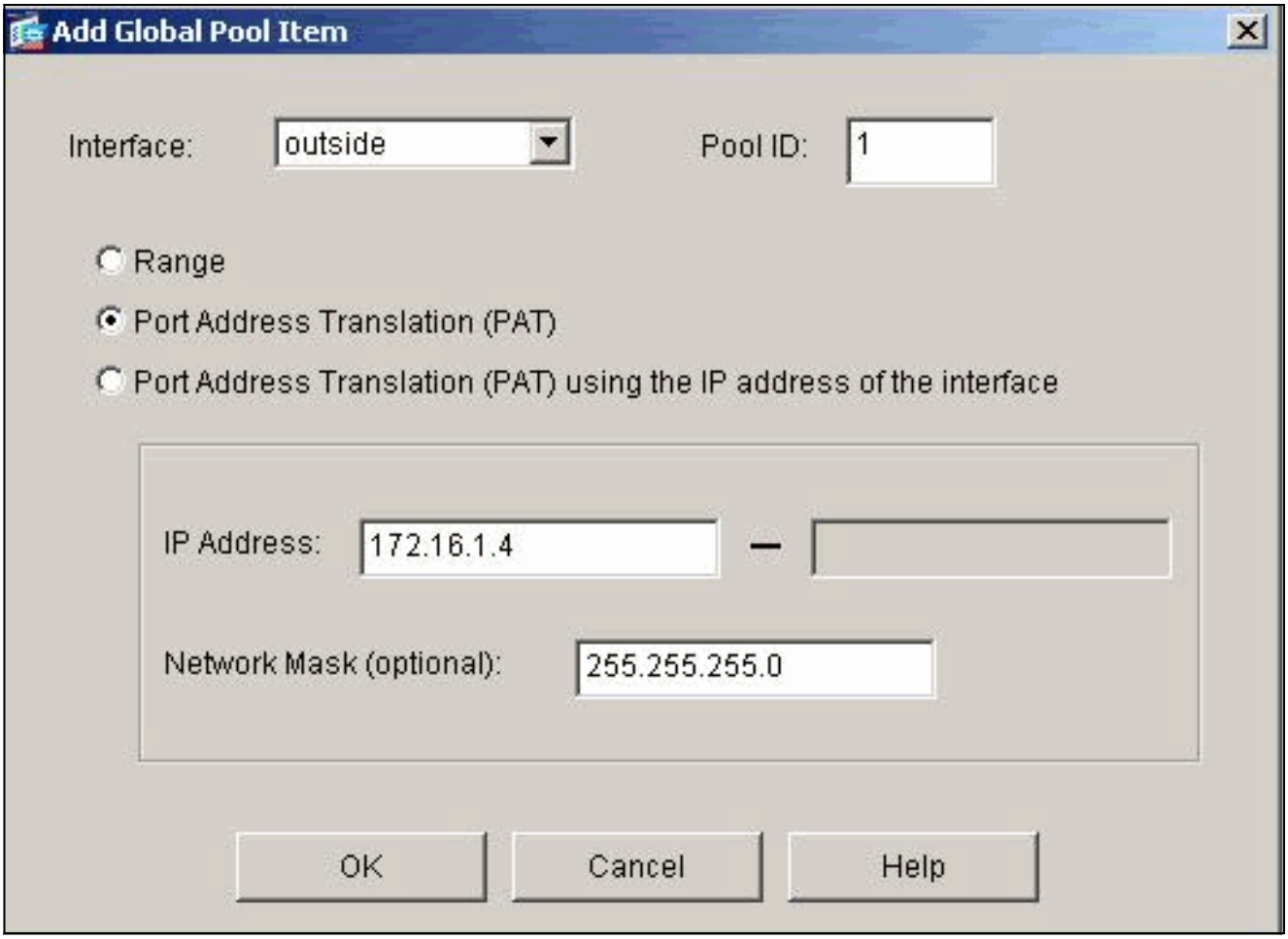


现在，内部的主机可以访问外部网络。当内部主机启动与外部的连接时，它们将被转换为全局池中的某个地址。全局池中的地址按照先到先转换的原则分配，并且从池中的最小地址开始分配。例如，如果主机 10.1.6.25 第一个启动与外部的连接，则它会得到地址 172.16.1.5。下一台与外部连接的主机将得到地址 172.16.1.6，等等。这不是静态转换，并且该转换在超过以下命令定义的不活动时段后将超时：**timeout xlate hh:mm:ss**。如果内部主机的数量多于池中地址的数量，则池中的最后一个地址将用于端口地址转换 (PAT)。

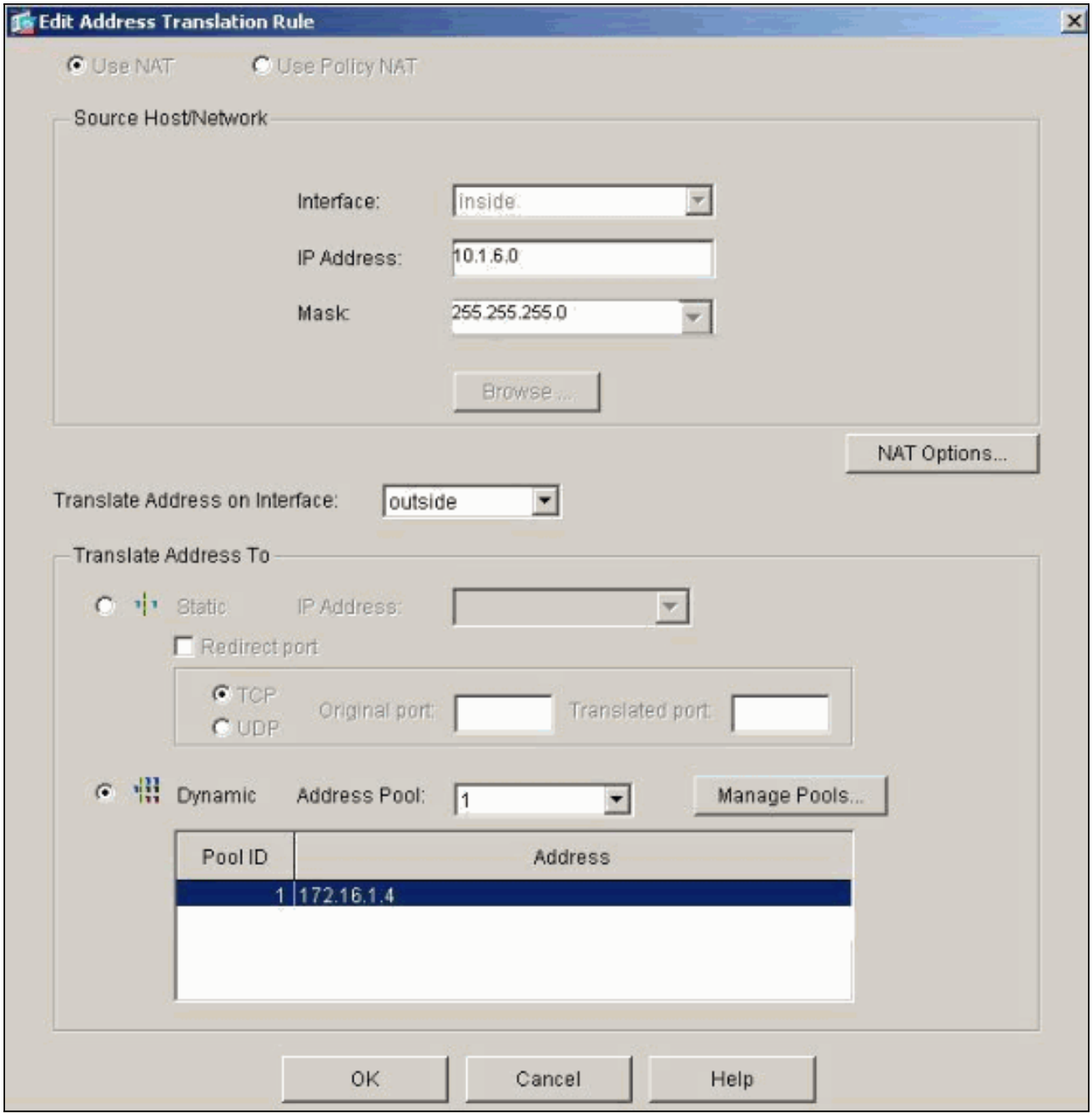
允许内部主机使用 PAT 访问外部网络

如果希望内部主机共享一个公共地址进行转换，请使用 PAT。如果 **global 语句**指定一个地址，则该地址是端口转换地址。PIX 允许每个接口一个端口转换，该转换支持最多 65,535 个活动 xlate 对象到一个全局地址的转换。完成以下步骤，以允许内部主机使用 PAT 访问外部网络。

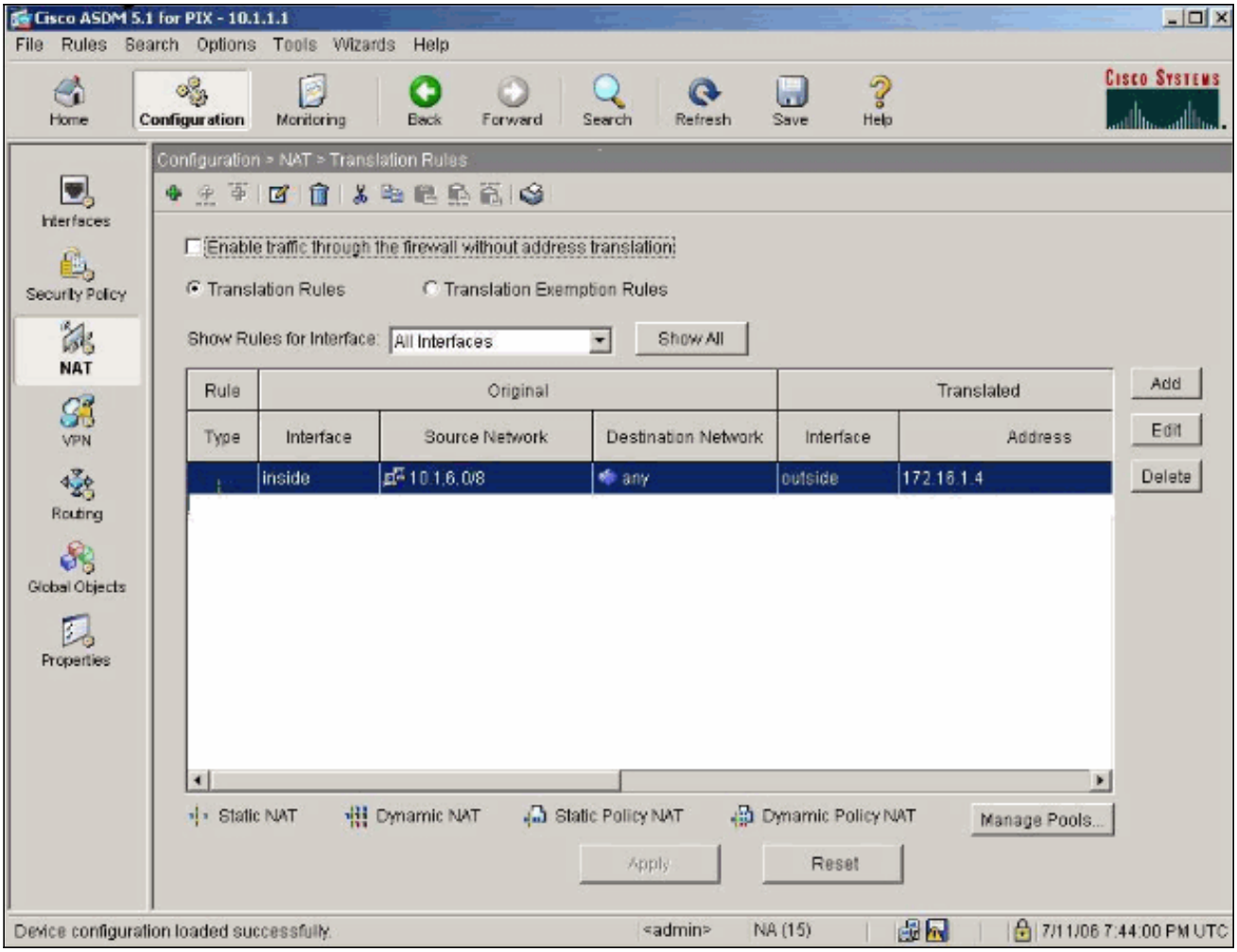
1. 定义要为 PAT 包括的内部组（使用 0 0 时，表示选择所有内部主机。）
   nat (inside) 1 10.1.6.0 255.255.255.0
2. 指定要用于 PAT 的全局地址。这可以是接口地址。
   global (outside) 1 172.16.1.4 netmask 255.255.255.0
3. 在 ASDM 中，选择 **Configuration > Features > NAT** 并取消选中 Enable traffic through the firewall without address translation。
4. 单击 **Add** 以配置 NAT 规则。
5. 选择 **Manage Pools** 以配置 PAT 地址。
6. 选择 **Outside > Add** 并单击 Port Address Translation (PAT) 以配置用于 PAT 的单个地址。
7. 输入地址、池 ID，然后单击 **OK**。



8. 选择 **Configuration > Features > NAT > Translation Rules** 以创建转换规则。
9. 选择 **Inside** 作为源接口，然后输入要进行 NAT 转换的地址。
10. 对于 Translate Address on Interface，选择 **outside**，选择 Dynamic，然后选择您刚配置的地址池。单击 **Ok**。



11. 当您选择 **Configuration > Features > NAT > Translation Rules** 时，转换将显示在 Translation Rules 中。



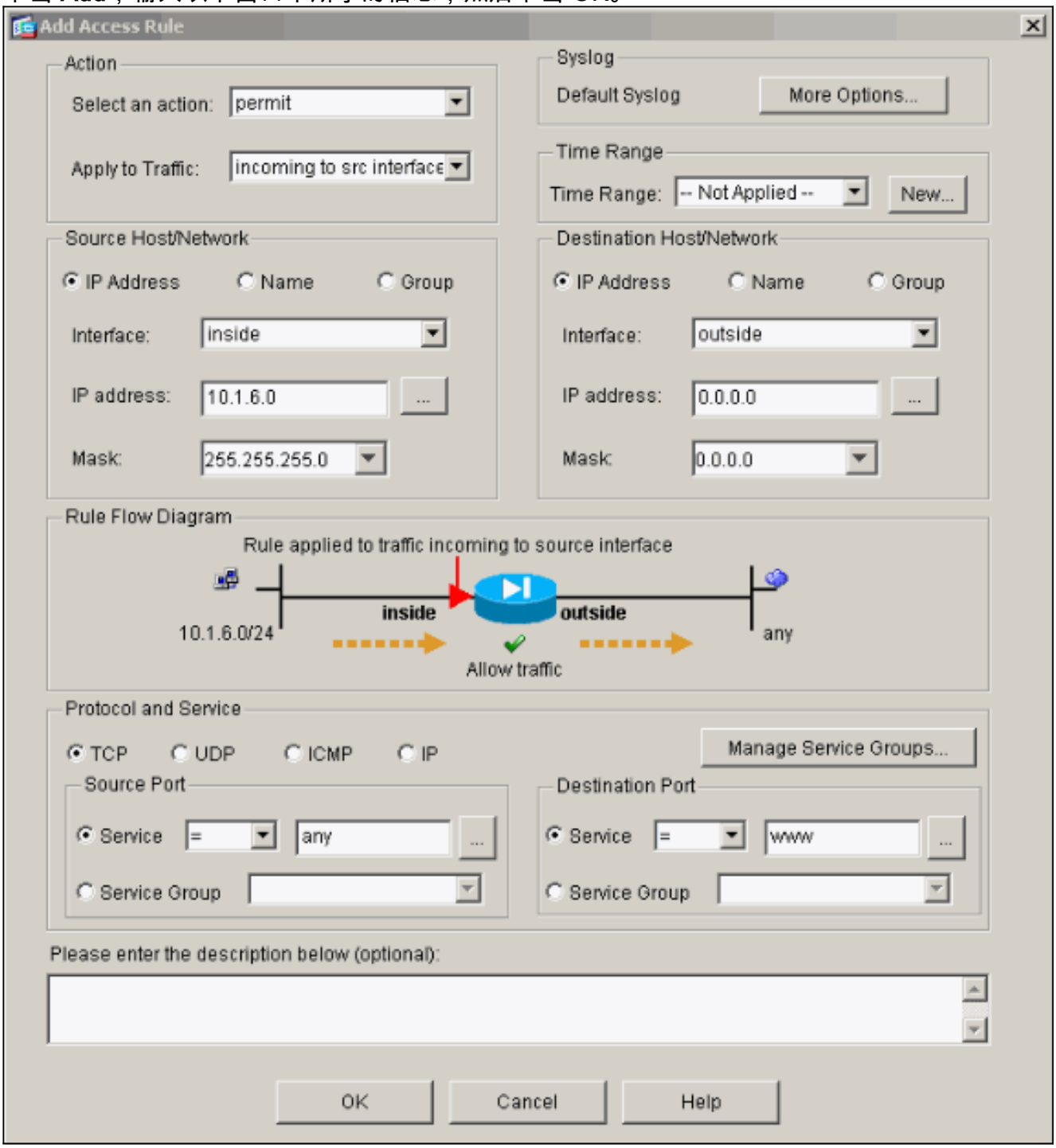
在使用 PAT 时，有几个注意事项。

- 为 PAT 指定的 IP 地址不能位于另一个全局地址池中。
- PAT 不能与 H.323 应用程序、缓存名称服务器和点对点隧道协议 (PPTP) 一起使用。PAT 可与域名服务 (DNS)、FTP 和被动 FTP、HTTP、邮件、远程过程调用 (RPC)、rshell、Telnet、URL 过滤和出站 traceroute 一起使用。
- 当您需要通过防火墙运行多媒体应用程序时，请勿使用 PAT。多媒体应用程序可能与 PAT 提供的端口映射发生冲突。
- 在 PIX 软件版本 4.2(2) 中，PAT 功能对以相反的顺序到达的 IP 数据包不起作用。PIX 软件版本 4.2(3) 更正了此问题。
- 使用 **global 命令**指定的全局地址池中的 IP 地址需要反向 DNS 条目以确保所有外部网络地址都可以通过 PIX 访问。为了创建反向 DNS 映射，请在地址到名称映射文件中为每个全局地址使用一个 DNS 指针 (PTR) 记录。没有 PTR 条目，站点会出现 Internet 连接速度缓慢或连接间歇中断的情况，并且 FTP 请求会一直失败。例如，如果全局 IP 地址是 192.168.1.3，PIX 安全设备的域名是 pix.caguana.com，则 PTR 记录为：`3.1.1.175.in-addr.arpa. IN PTR pix3.caguana.com`
  `4.1.1.175.in-addr.arpa. IN PTR pix4.caguana.com & so on.`

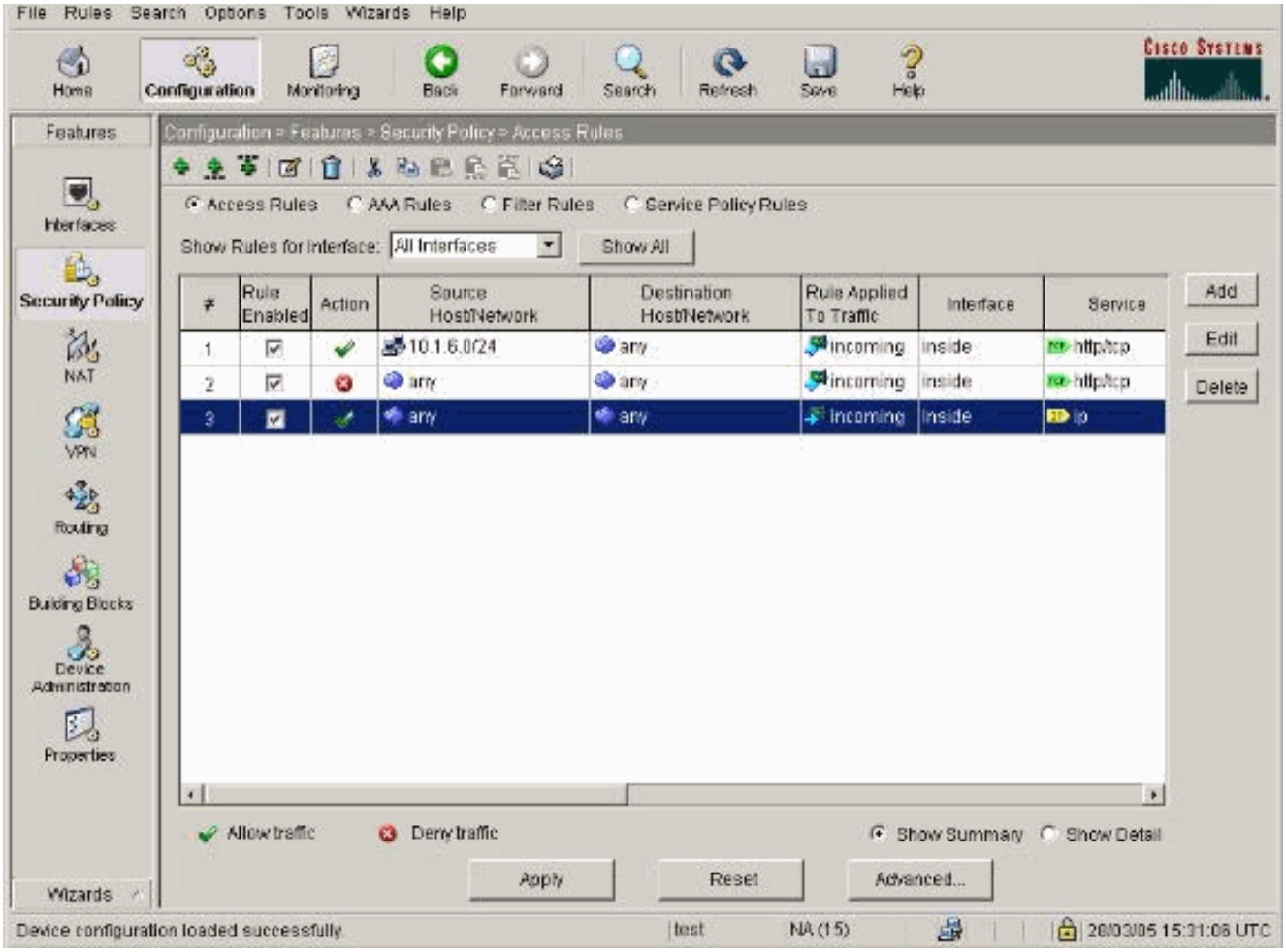
限制内部主机对外部网络的访问

如果为源主机定义了有效的转换方法，并且没有为源 PIX 接口定义 ACL，则默认情况下将允许出站连接。但是，在某些情况下有必要根据源、目标、协议和/或端口限制出站访问。为了实现此目的，请使用 **access-list** 命令配置 ACL 并使用 access-group 命令将其应用于连接源 PIX 接口。入站和出站方向都可以应用 PIX 7.0 ACL。此过程是一个示例，它允许一个子网的出站 HTTP 访问，但拒绝所有其他主机对外部的 HTTP 访问，同时允许每个用户的所有其他 IP 数据流。

1. 定义 ACL。
   access-list acl_outbound permit tcp 10.1.6.0 255.255.255.0 any eq www access-list acl_outbound deny tcp any any eq www access-list acl_outbound permit ip any any **注意：** PIX ACL 不同于 Cisco IOS® 路由器上的 ACL 之处在于，PIX ACL 不像 Cisco IOS 一样使用通配符掩码。它在 ACL 定义中使用常规子网掩码。与 Cisco IOS 路由器一样，PIX ACL 在 ACL 结尾处有一条隐式“deny all”语句。**注意：** 新的访问列表条目将被添附对现有ACE的结尾。如果需要首先处理的特定ACE，您在能使用`line`access-list。这是一example命令摘要：`access-list acl_outbound line 1 extended permit tcp host 10.1.10.225 any`
2. 将 ACL 应用于内部接口。
   access-group acl_outbound in interface inside
3. 使用 ASDM 在步骤 1 中配置第一个访问列表条目以允许来自 10.1.6.0/24 的 HTTP 数据流。选择 **Configuration > Features > Security Policy > Access Rules**。
4. 单击 **Add**，输入以下窗口中所示的信息，然后单击 OK。



5. 输入三个访问列表条目后，选择 **Configuration > Feature > Security Policy > Access Rules** 以显示这些规则。



允许不受信任的主机访问受信任的网络中的主机

大多数组织需要允许不受信任的主机访问它们的受信任网络中的资源。内部 Web 服务器便是一个常见的示例。默认情况下，PIX 拒绝从外部主机到内部主机的连接。为了在 NAT 控制模式下允许此连接，请将 **static** 命令和 access-list、access-group 命令一起使用。如果已禁用 NAT 控制，则在不执行任何转换的情况下，只需要 **access-list** 和 access-group 命令。

使用 **access-group** 命令将 ACL 应用于接口。此命令将 ACL 与接口关联起来，以检查向特定方向流动的数据流。

与允许内部主机访问外部的 **nat** 和 global 命令相比，如果添加适当的 ACL/组，static 命令将创建一个允许内部主机访问外部和外部主机访问内部的双向转换。

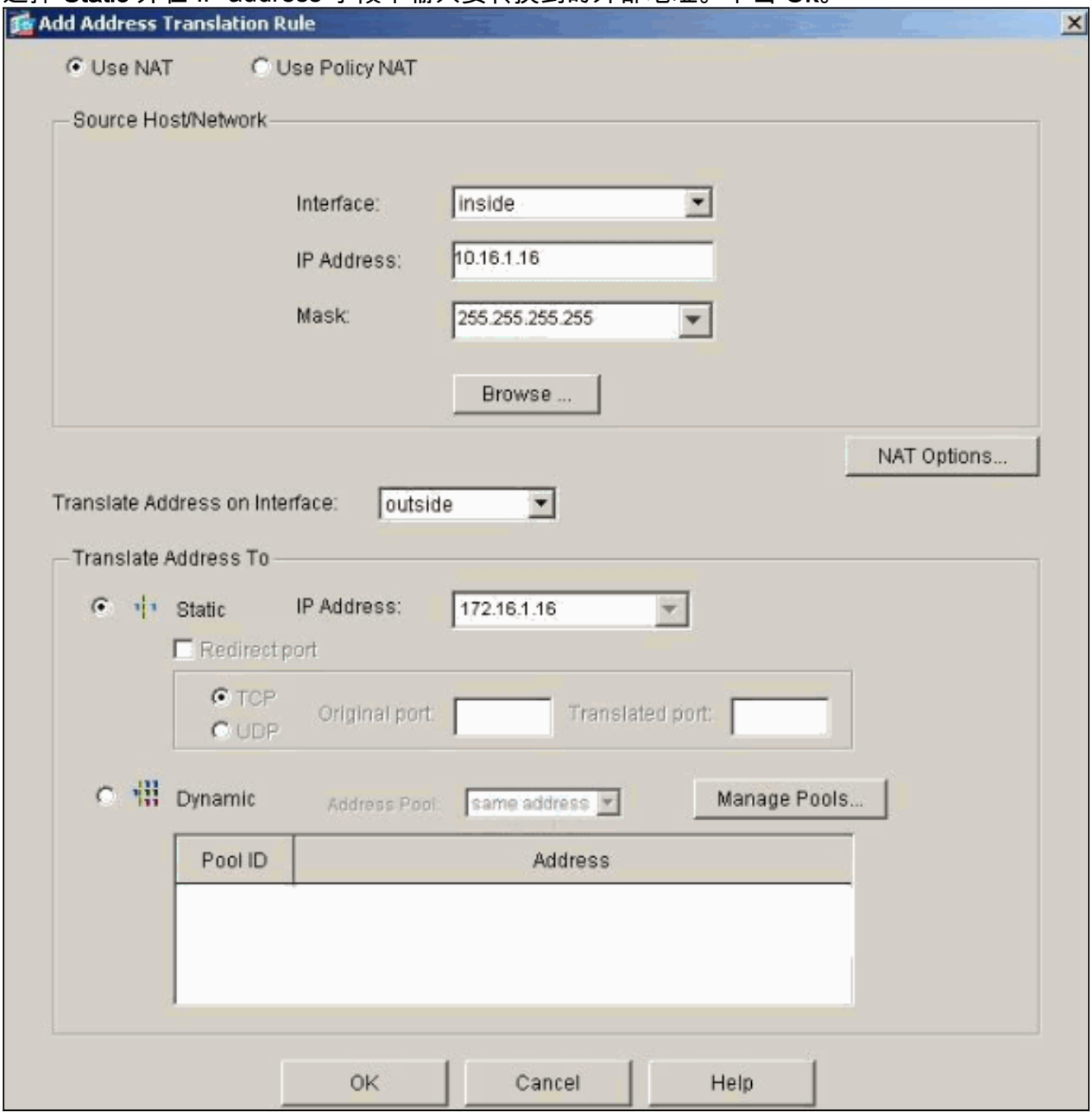
在本文档中显示的 PAT 配置示例中，如果外部主机尝试连接到全局地址，则它可以供数千个内部主机使用。**static** 命令创建一个一对一的映射。**access-list** 命令定义允许与内部主机之间建立的连接类型，当安全性较低的主机连接到安全性较高的主机时总是需要该命令。**access-list** 命令基于端口和协议，根据系统管理员想要实现的目标，可以非常宽松也可以非常严格。

本文档中的网络图说明了如何使用这些命令配置 PIX 以允许所有不受信任的主机连接到内部 Web 服务器，并允许不受信任的主机 192.168.1.1 访问同一台计算机上的 FTP 服务。

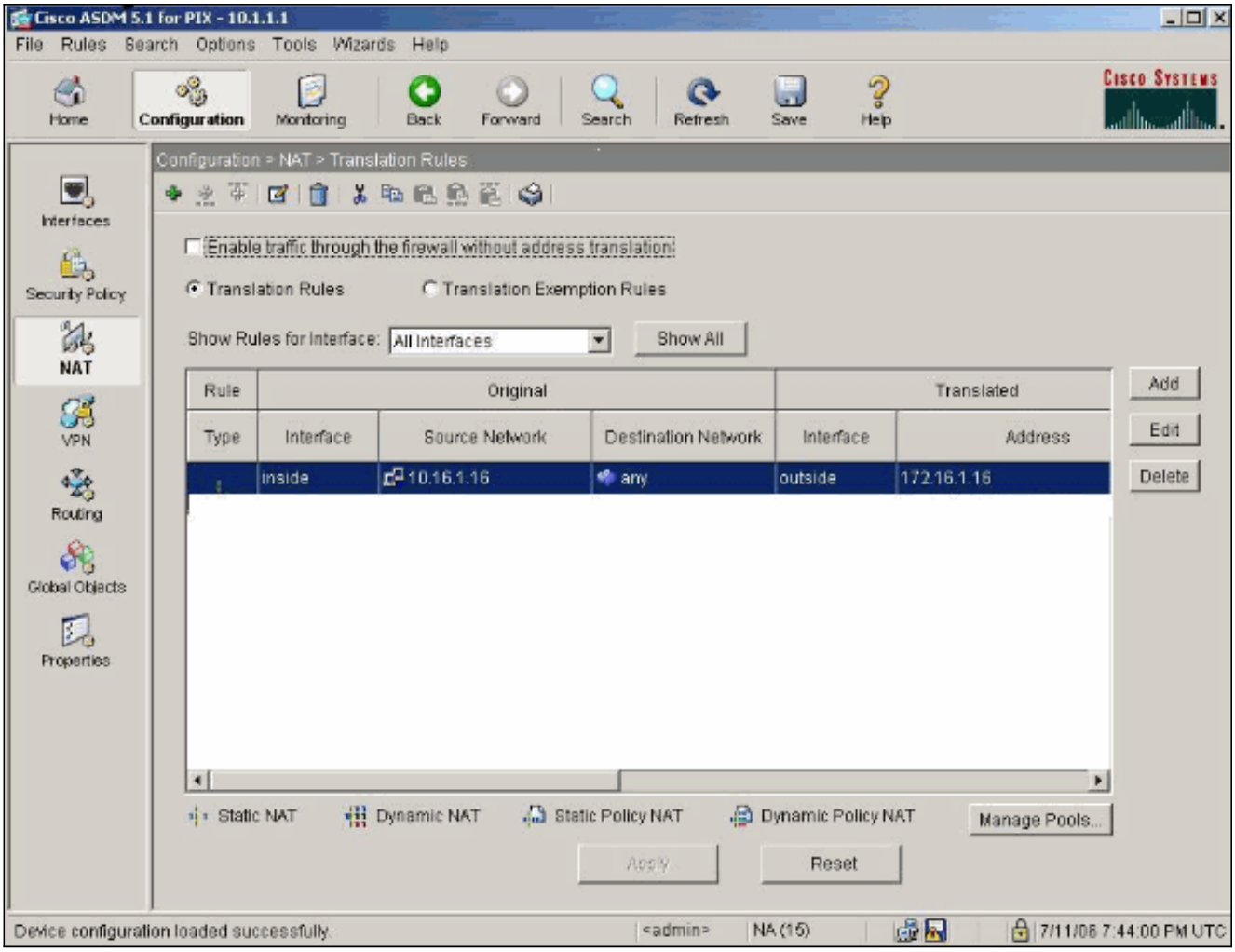
在 PIX 版本 7.0 及更高版本上使用 ACL

完成以下步骤，以在 PIX 软件版本 7.0 及更高版本上使用 ACL。

1. 如果已启用 NAT 控制，请为内部 Web 服务器定义一个到外部/全局地址的静态地址转换。
   static (inside, outside) 172.16.1.16 10.16.1.16
2. 定义哪些主机可在哪些端口上连接到 Web/FTP 服务器。
   access-list 101 permit tcp any host 172.16.1.16 eq www access-list 101 permit tcp host 192.168.1.1 host 172.16.1.16 eq ftp
3. 将 ACL 应用于外部接口。
   access-group 101 in interface outside
4. 选择 **Configuration > Features > NAT** 并单击 Add 以使用 ASDM 创建此静态转换。
5. 选择 **inside** 作为源接口，并输入要为其创建静态转换的内部地址。
6. 选择 **Static** 并在 IP address 字段中输入要转换到的外部地址。单击 **Ok**。



7. 当您选择 **Configuration > Features > NAT > Translation Rules** 时，转换将显示在 Translation Rules 中。



8. 请使用限制内部主机对外部网络的访问过程以输入 **access-list** 条目。**注意：** 在执行这些命令时，请小心。如果执行 **access-list 101 permit ip any any** 命令，则只要存在活动转换，不受信任网络上的任何主机都可以使用 IP 访问受信任网络上的任何主机。

对特定主机/网络禁用 NAT

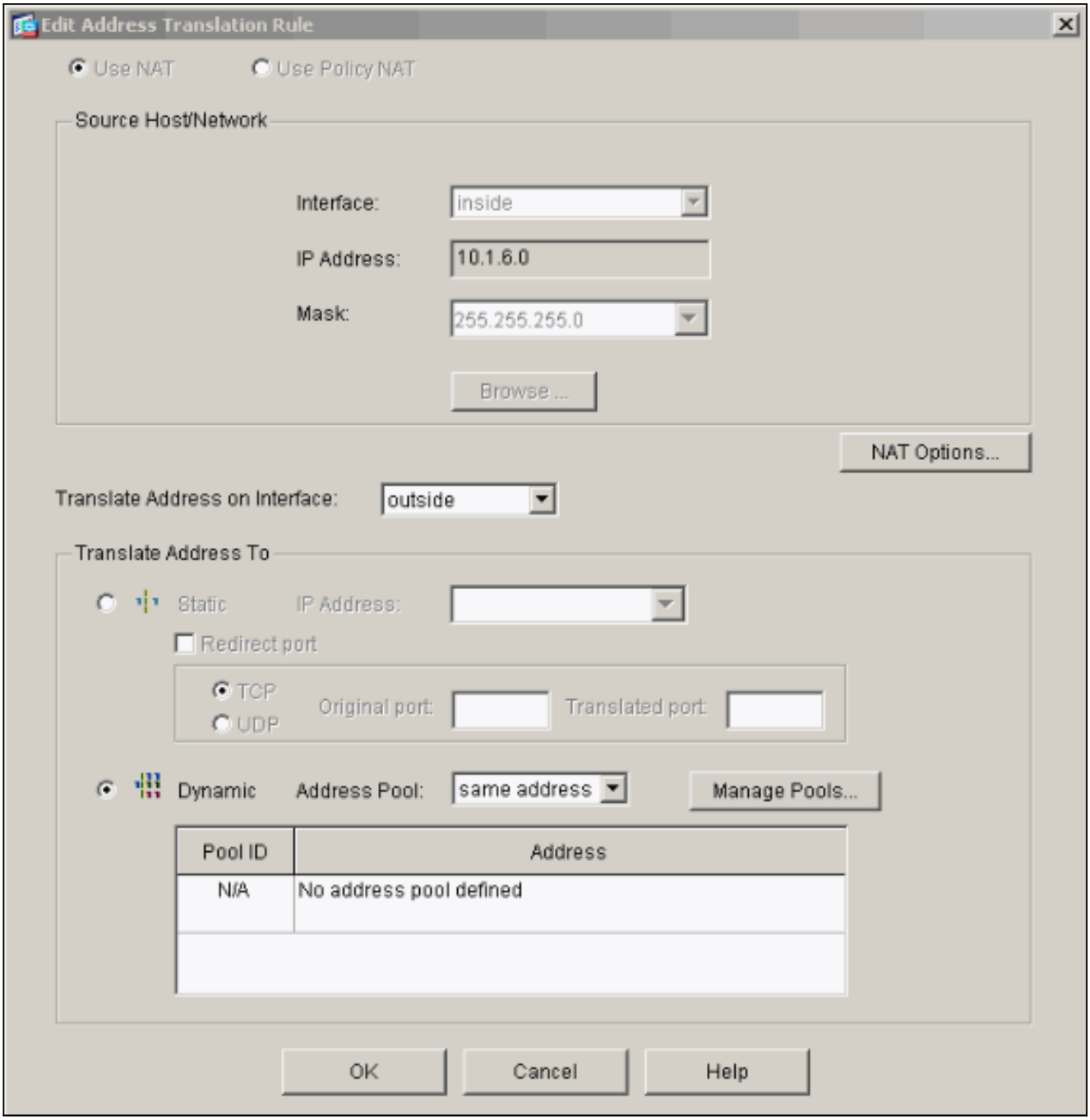
如果使用 NAT 控制并具有内部网络上的一些公共地址，并且希望这些特定内部主机可以在不经转换的情况下访问外部，可以使用 **nat 0** 或 static 命令对这些主机禁用 NAT。

以下是 **nat** 命令的示例：

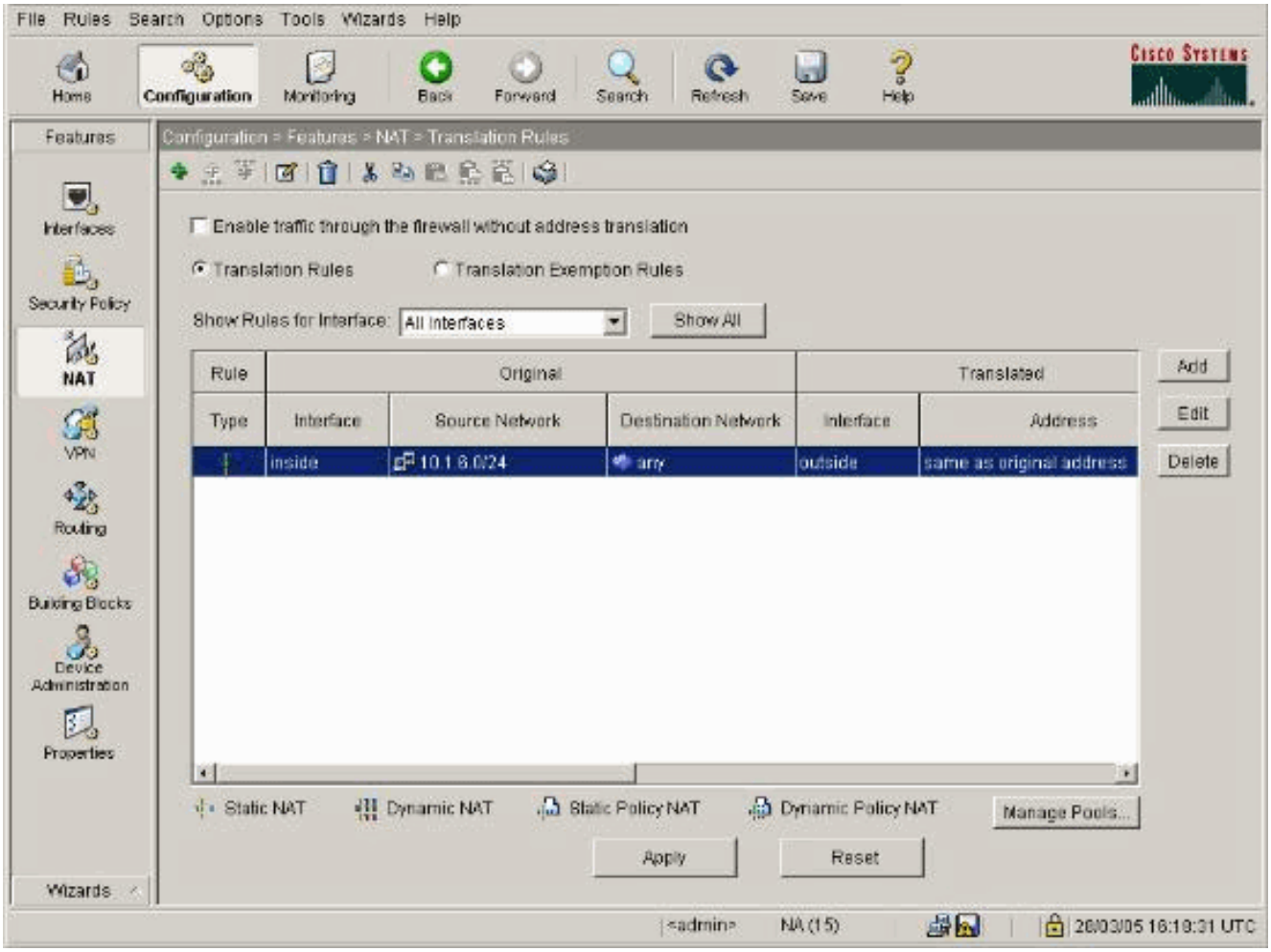
```
nat (inside) 0 10.1.6.0 255.255.255.0
```

完成以下步骤，以使用 ASDM 对特定主机/网络禁用 NAT。

1. 选择 **Configuration > Features > NAT** 并单击 Add。
2. 选择 **inside** 作为源接口，并输入要为其创建静态转换的内部地址/网络。
3. 选择 **Dynamic** 并为 Address Pool 选择 same address。单击 **Ok**。



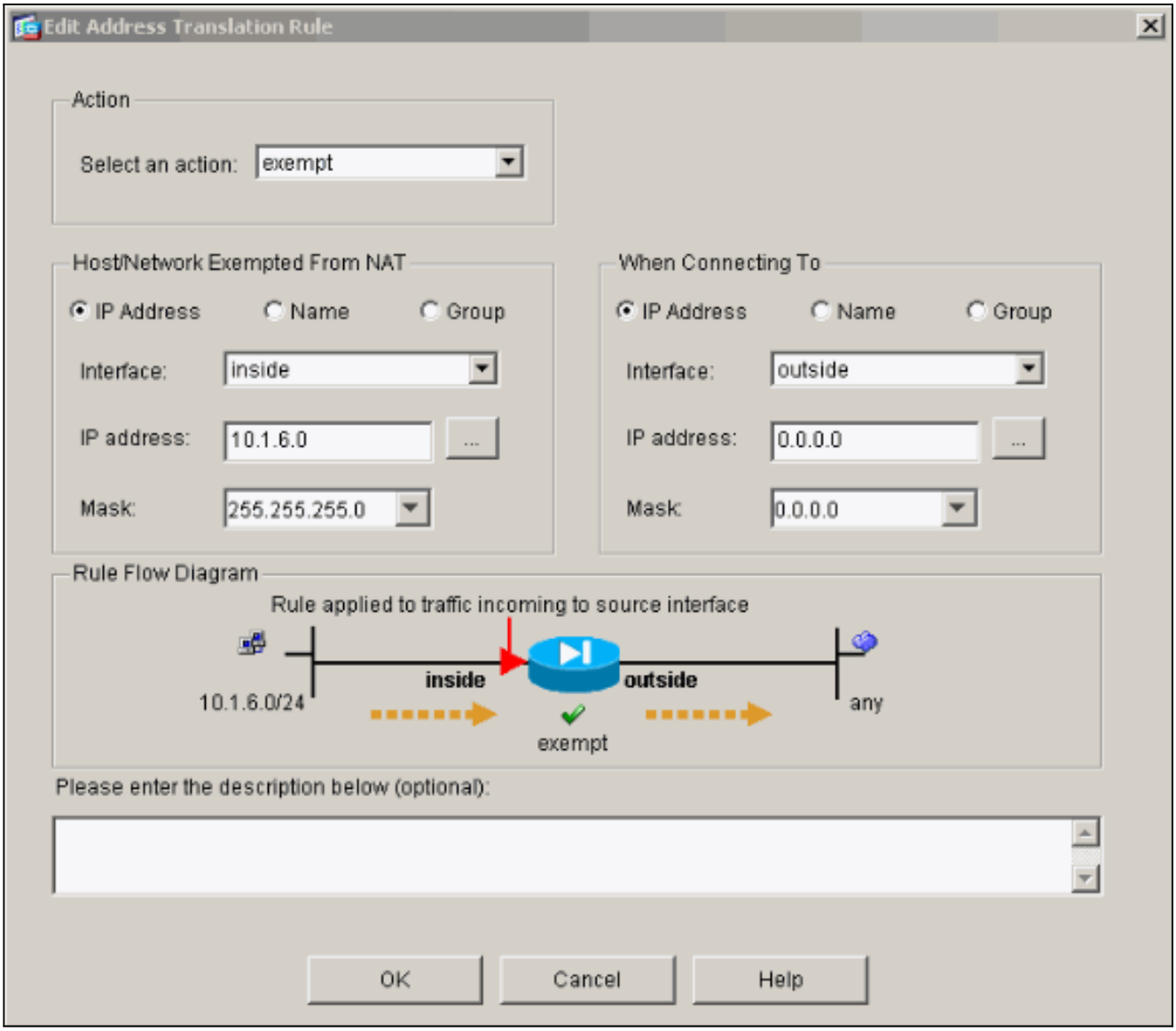
4. 当您选择 **Configuration > Features > NAT > Translation Rules** 时，新规则将显示在 Translation Rules 中。



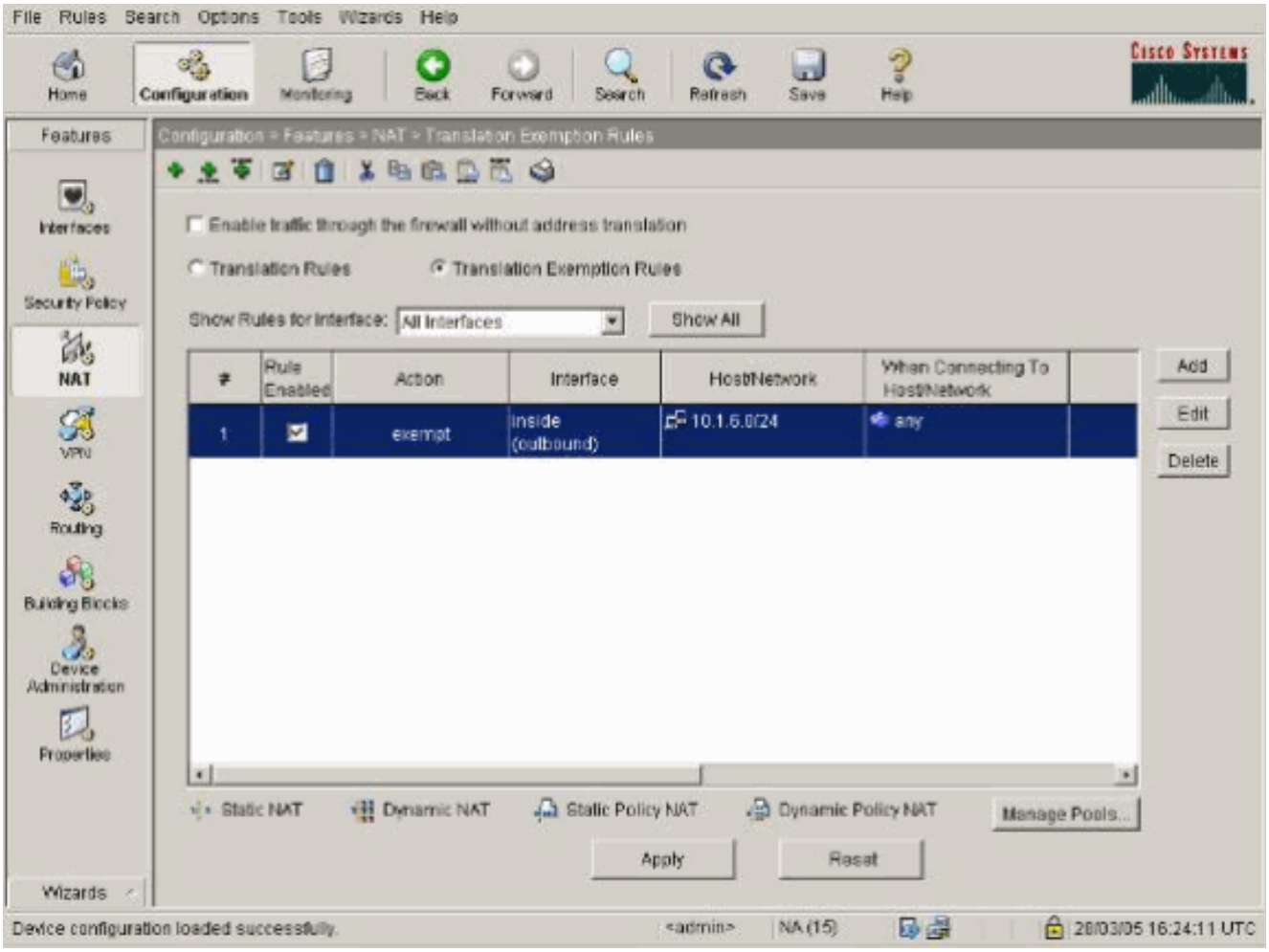
5. 如果使用 ACL 以允许对不应转换（基于源/目标）的数据流进行更精确的控制，请使用以下命令。

```
access-list 103 permit ip 10.1.6.0 255.255.255.0 any nat (inside) 0 access-list 103
```

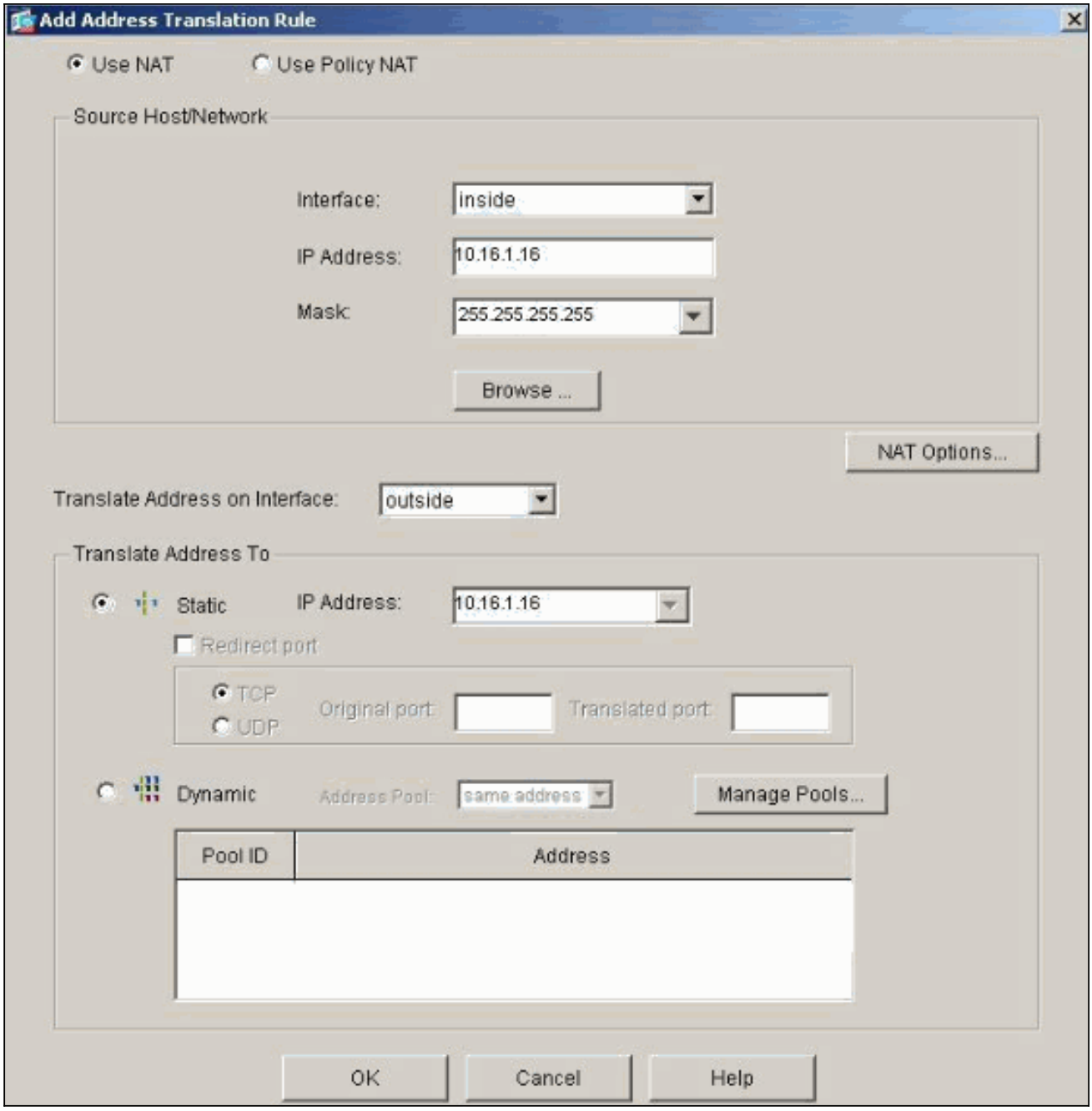
6. 使用 ASDM 并选择 **Configuration > Features > NAT > Translation Rules**。
7. 选择 **Translation Exemption Rules** 并单击 Add。此示例显示如何使从 10.1.6.0/24 网络到任意位置的数据流被免于转换。



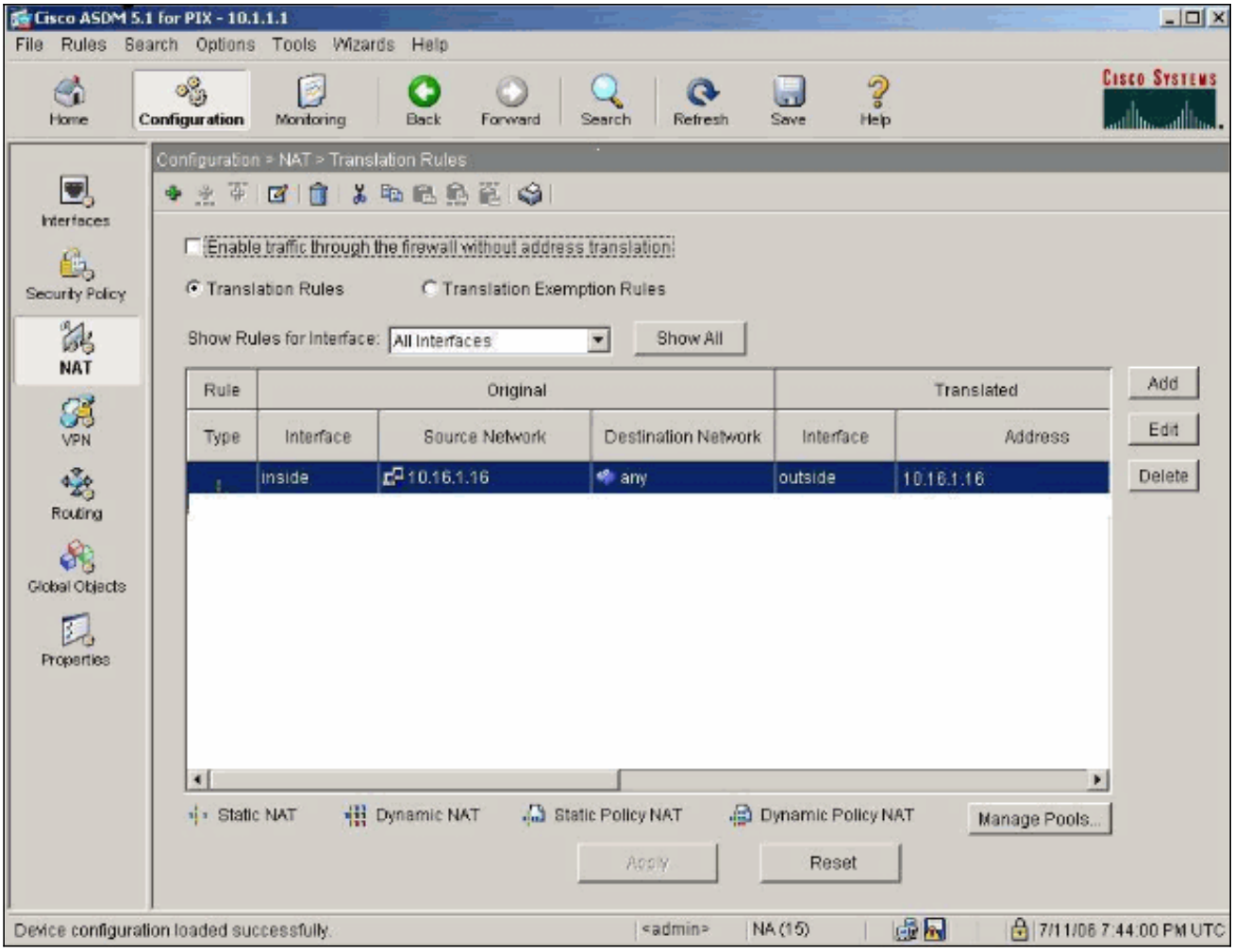
8. 选择 **Configuration > Features > NAT > Translation Exemption Rules** 以显示新的规则。



9. 用于 Web 服务器的 **static** 命令有一些更改，如以下示例所示。
   ```
   static (inside, outside) 10.16.1.16 10.16.1.16
   ```
10. 从 ASDM 中选择 **Configuration > Features > NAT > Translation Rules**。
11. 选择 **Translation Rules** 并单击 Add。输入源地址信息，然后选择 **Static**。在 IP Address 字段中输入同一地址。



12. 当您选择 **Configuration > Features > NAT > Translation Rules** 时，转换将显示在 Translation Rules 中。



13. 如果使用 ACL，请使用以下命令。
access-list 102 permit tcp any host 10.16.1.16 eq www access-group 102 in interface outside 有关在 ASDM 中配置 ACL 的详细信息，请参阅本文档的限制内部主机对外部网络的访问部分。请注意以下两种情况之间的差异：您使用 **nat 0** 指定网络/掩码；您使用一个使用网络/掩码的 ACL，用于仅允许从内部启动连接。将 ACL 与 **nat 0** 一起使用允许由入站或出站数据流启动连接。PIX 接口需要位于不同的子网中以避免出现可达性问题。

使用 Static 命令进行端口重定向（转发）

在 PIX 6.0 中，添加了端口重定向（转发）功能以允许外部用户连接到特定 IP 地址/端口，并让 PIX 将数据流重定向到适当的内部服务器/端口。**static** 命令已被修改。共享地址可以是唯一地址、共享出站 PAT 地址或与外部接口共享的地址。此功能在 PIX 7.0 中可用。

注意： 由于空间限制，命令显示为两行。

static *[(internal_if_name, external_if_name)] {global_ip|interface}local_ip [netmask mask] [max_conns [emb_limit [norandomseq]]]* **static** *[(internal_if_name, external_if_name)] {tcp|udp} {global_ip|interface} global_port local_ip local_port [netmask mask] [max_conns [emb_limit [norandomseq]]]*

注意： 如果静态 NAT 使用外部 IP (global_IP) 地址进行转换，则这可能导致转换。因此，在静态转换中请使用关键字 **interface** 代替 IP 地址。

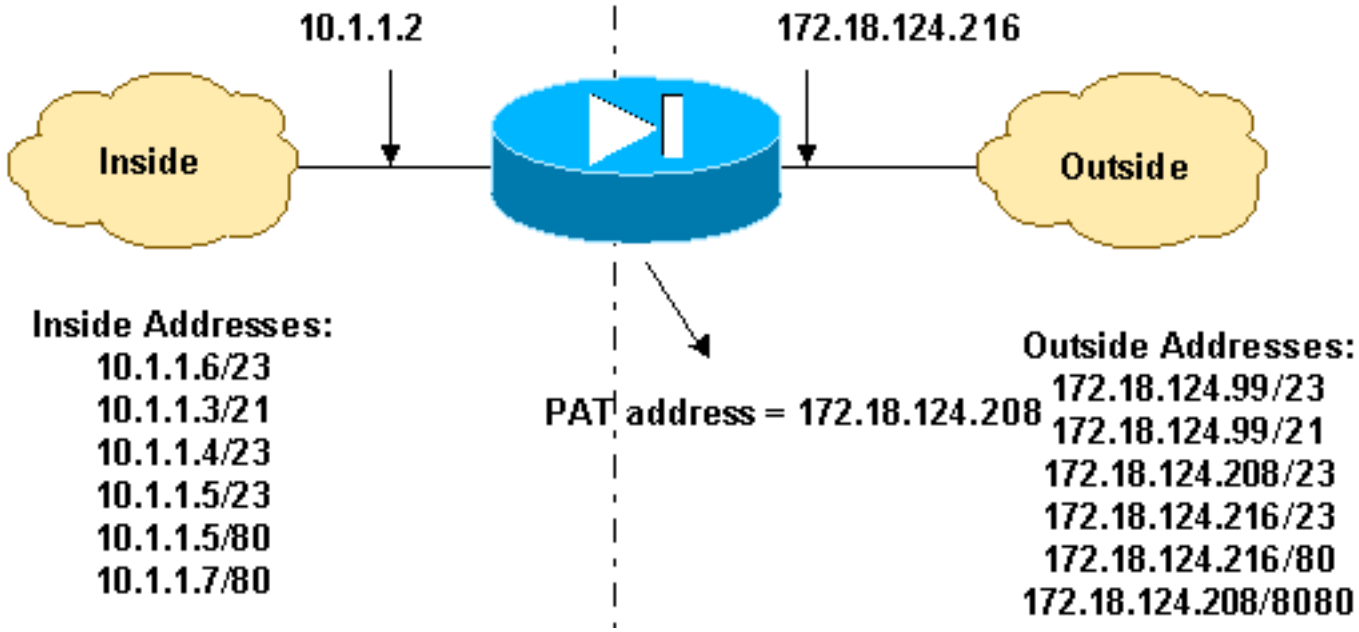
本网络示例中包含以下端口重定向（转发）：

- 外部用户将 Telnet 请求定向到唯一 IP 地址 172.18.124.99，PIX 将其重定向到 10.1.1.6。

- 外部用户将 FTP 请求定向到唯一 IP 地址 172.18.124.99，PIX 将其重定向到 10.1.1.3。
- 外部用户将 Telnet 请求定向到 PAT 地址 172.18.124.208，PIX 将其重定向到 10.1.1.4。
- 外部用户将 Telnet 请求定向到 PIX 外部 IP 地址 172.18.124.216，PIX 将其重定向到 10.1.1.5。
- 外部用户将 HTTP 请求定向到 PIX 外部 IP 地址 172.18.124.216，PIX 将其重定向到 10.1.1.5。
- 外部用户将 HTTP 端口 8080 请求定向到 PAT 地址 172.18.124.208，PIX 将其重定向到 10.1.1.7 端口 80。

此示例还使用 ACL 100 阻止部分用户从内部访问外部。此步骤是可选的。在没有适当的 ACL 的情况下，允许所有数据流出站。

网络图 - 端口重定向（转发）



部分 PIX 配置 - 端口重定向

此部分配置说明如何使用静态端口重定向（转发）。请参阅端口重定向（转发）网络图。

部分 PIX 7.x 配置 - 端口重定向（转发）

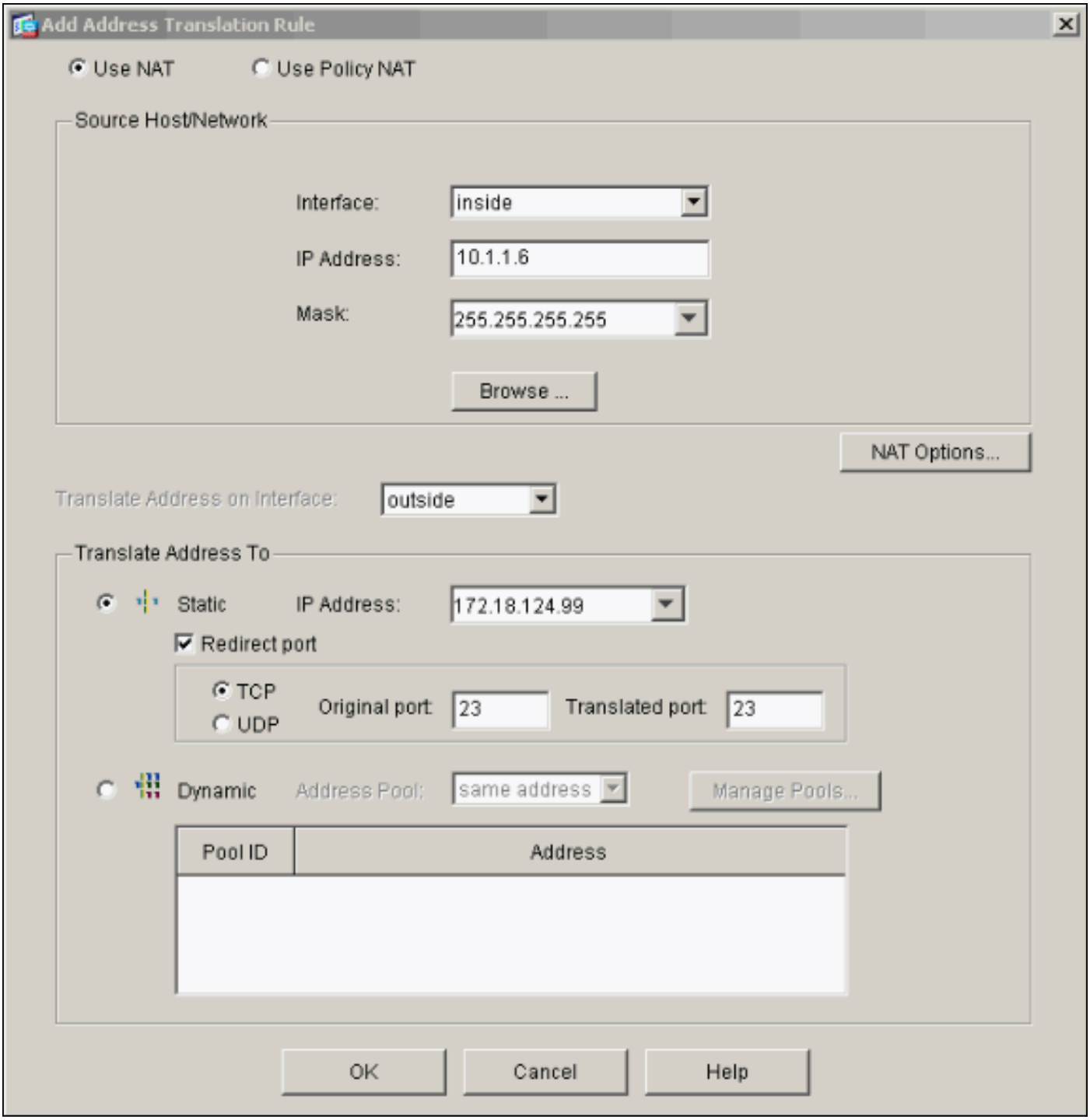
```
fixup protocol ftp 21
!--- Use of an outbound ACL is optional. access-list 100
permit tcp 10.1.1.0 255.255.255.128 any eq www access-
list 100 deny tcp any any eq www access-list 100 permit
tcp 10.0.0.0 255.0.0.0 any access-list 100 permit udp
10.0.0.0 255.0.0.0 host 172.18.124.100 eq domain access-
list 101 permit tcp any host 172.18.124.99 eq telnet
access-list 101 permit tcp any host 172.18.124.99 eq ftp
access-list 101 permit tcp any host 172.18.124.208 eq
telnet access-list 101 permit tcp any host
172.18.124.216 eq telnet access-list 101 permit tcp any
host 172.18.124.216 eq www access-list 101 permit tcp
any host 172.18.124.208 eq 8080 interface Ethernet0
nameif outside security-level 0 ip address
172.18.124.216 255.255.255.0 ! interface Ethernet1
nameif inside security-level 100 ip address 10.1.1.2
255.255.255.0 ! global (outside) 1 172.18.124.208 nat
(inside) 1 0.0.0.0 0.0.0.0 0 0 static (inside,outside)
```

```
tcp 172.18.124.99 telnet 10.1.1.6 telnet netmask
255.255.255.255 0 0 static (inside,outside) tcp
172.18.124.99 ftp 10.1.1.3 ftp netmask 255.255.255.255 0
0 static (inside,outside) tcp 172.18.124.208 telnet
10.1.1.4 telnet netmask 255.255.255.255 0 0 static
(inside,outside) tcp interface telnet 10.1.1.5 telnet
netmask 255.255.255.255 0 0 static (inside,outside) tcp
interface www 10.1.1.5 www netmask 255.255.255.255 0 0
static (inside,outside) tcp 172.18.124.208 8080 10.1.1.7
www netmask 255.255.255.255 0 0 !--- Use of an outbound
ACL is optional. access-group 100 in interface inside
access-group 101 in interface outside
```

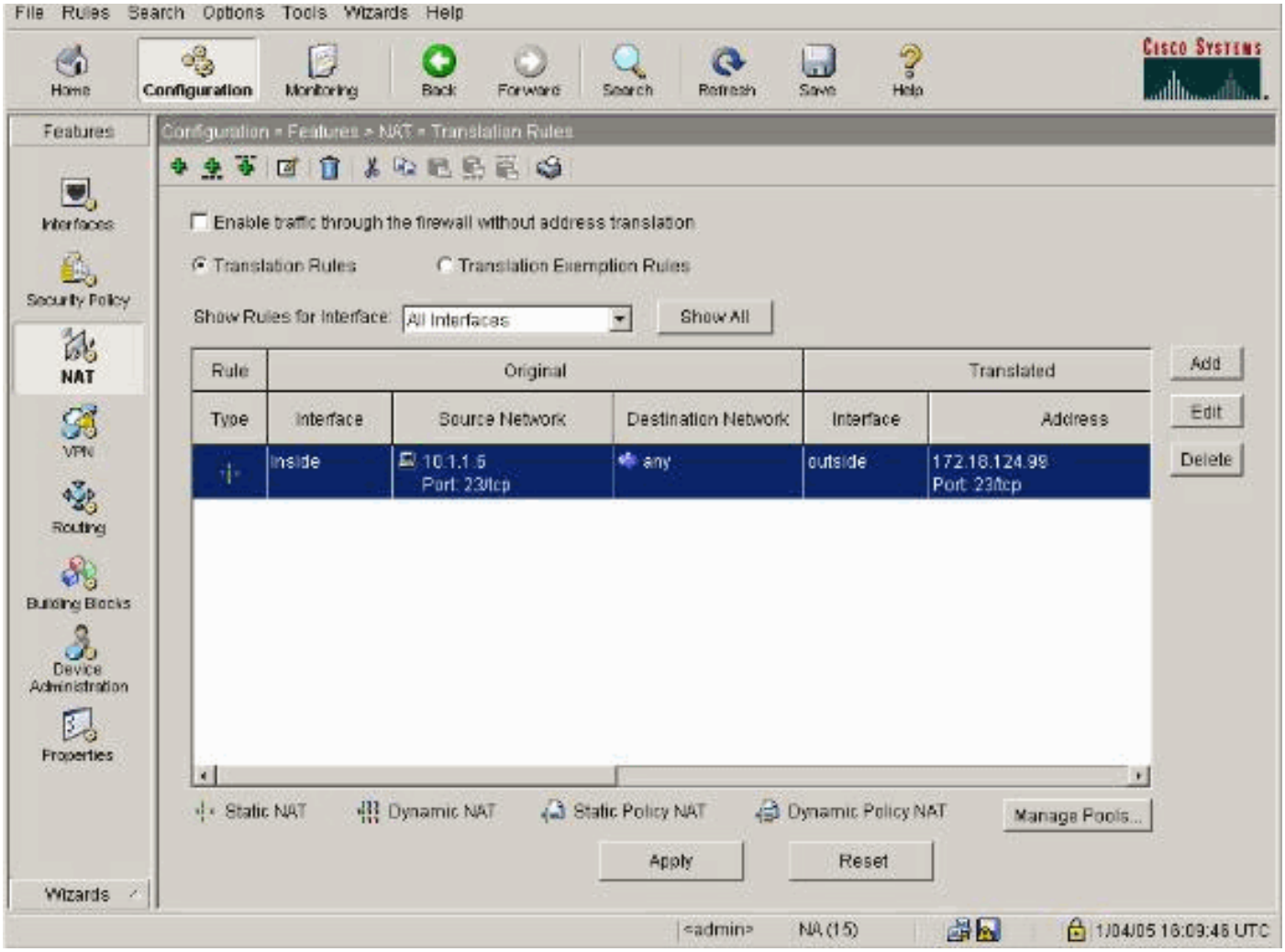
注意： 如果使用 **sysopt noproxyarp outside** 命令配置了 PIX/ASA，则它不允许防火墙在 PIX/ASA 中执行 proxyarp 和静态 NAT 转换。为了解决此问题，请在 PIX/ASA 中删除 **sysopt noproxyarp outside** 命令，然后通过使用无故 ARP 更新 ARP 条目。这使得静态 NAT 条目可以正常工作。

此过程是如何配置允许外部用户将 Telnet 请求定向到唯一 IP 地址 172.18.124.99（PIX 将其重定向到 10.1.1.6）的端口重定向（转发）的示例。

1. 使用 ASDM 并选择 **Configuration > Features > NAT > Translation Rules**。
2. 选择 **Translation Rules** 并单击 Add。
3. 对于 Source Host/Network，输入内部 IP 地址的信息。
4. 对于 Translate Address To，选择 **Static**，输入外部 IP 地址并选中 Redirect port。
5. 输入转换前和转换后端口信息（本示例使端口 23 保持不变）。单击 **Ok**。



当您选择 **Configuration > Features > NAT > Translation Rules** 时，转换将显示在 Translation Rules 中。



使用 Static 命令限制 TCP/UDP 会话

如果要限制到位于 PIX/ASA 中的内部服务器的 TCP 或 UDP 会话，请使用 **static** 命令。

指定整个子网的并发 TCP 和 UDP 连接的最大数量。默认值为 0，这意味着无限的连接（空闲连接在 **timeout conn** 命令指定的空闲超时后被关闭）。此选项不适用于外部 NAT。安全设备只跟踪从安全性较高的接口到安全性较低的接口的连接。

限制初期连接的数量可保护您免受 DoS 攻击。安全设备使用初期限制触发 TCP 拦截，TCP 拦截可防止内部系统受到通过使用 TCP SYN 数据包淹没接口进行的 DoS 攻击。初期连接是源和目标之间尚未完成必要的握手的连接请求。此选项不适用于外部 NAT。TCP 拦截功能仅适用于较高安全级别上的主机或服务器。如果为外部 NAT 设置初期限制，初期限制将被忽略。

例如：

```
ASA(config)#static (inside,outside) tcp 10.1.1.1 www 10.2.2.2 www tcp 500 100 !--- The maximum
number of simultaneous tcp connections the local IP !--- hosts are to allow is 500, default is 0
which means unlimited !--- connections. Idle connections are closed after the time specified !--
- by the timeout conn command !--- The maximum number of embryonic connections per host is 100.
```

%PIX-3-201002 ：Too many connections on {static|xlate} global_address!econns nconns

这是一条与连接相关的消息。当超出到指定静态地址的最大连接数时，将记录此消息。econns 变量是最大初期连接数，nconns 是 static 或 xlate 允许的最大连接数。

建议的操作是使用 **show static** 命令以检查对与静态地址的连接强加的限制。该限制是可配置的。

%ASA-3-201011 ：连接限制从外部超过了1000/1000从10.1.26.51/2393的入站数据包的到10.0.86.155/135在接口

此错误消息归结于Cisco Bug ID CSCsg52106 (仅限注册用户)。有关详细信息，请参阅此 Bug。

基于时间的访问列表

时间范围的创建不限制对设备的访问。**time-range** 命令仅定义时间范围。在定义时间范围之后，您可以将其附加到数据流规则或某个操作。

为了实施基于时间的 ACL，请使用 **time-range** 命令定义一天和一周中的特定时间。然后使用 **with the access-list extended time-range** 命令将时间范围绑定到 ACL。

时间范围依赖于安全设备的系统时钟。但是，此功能与 NTP 同步一起使用时效果最佳。

在创建时间范围并进入时间范围配置模式之后，可以使用 **absolute** 和 periodic 命令定义时间范围参数。为了恢复 **time-range** 命令 absolute 和 periodic 关键字的默认设置，请在时间范围配置模式下使用 default 命令。

为了实施基于时间的 ACL，请使用 **time-range** 命令定义一天和一周中的特定时间。然后使用 **with the access-list extended** 命令将时间范围绑定到 ACL。下一个示例将名为“Sales”的 ACL 绑定到名为“New York Minute”的时间范围：

此示例创建一个名为“New York Minute”的时间范围，并进入时间范围配置模式：

```
hostname(config)#time-range New_York_Minute hostname(config-time-range)#periodic weekdays 07:00 to 19:00 hostname(config)#access-list Sales line 1 extended deny ip any any time-range New_York_Minute hostname(config)#access-group Sales in interface inside
```

建立技术支持请求时应收集的信息

如果仍需要帮助并希望建立一个 Cisco 技术支持请求，请务必包括此信息以用于排除您的 PIX 安全设备的故障。
• 问题说明和相关拓扑详细信息。 • 在建立请求之前用来进行故障排除的步骤。 • 来自 **show tech-support** 命令的输出。 • 运行 logging buffered debugging 命令后来自 **show log** 命令的输出，或用于展示问题的控制台捕获信息（如果有）。 请以非压缩的纯文本格式 (.txt) 将收集的数据附加到请求中。您可以在 TAC 服务请求工具（仅限注册用户）中将信息附加到您的请求。如果不能访问 TAC 服务请求工具（仅限注册用户），则可以通过电子邮件附件的形式将您的信息发送到 attach@cisco.com（请在邮件标题行中注明请求编号）。

相关信息

- **PIX 安全设备支持页**
- **PIX 命令参考**

- Cisco 自适应安全设备管理器 (ASDM) 故障排除和警报
- 请求注解 (RFC)
- 技术支持和文档 - Cisco Systems