ASA 8.2 ：端口重定向(转发)与nat，全局，静态和访问列表命令使用ASDM

目录

简介

本文描述端口重定向如何在思科可适应安全工具(ASA)工作使用ASDM。它处理流量的访问控制通过ASA，并且翻译规则如何工作。

先决条件

要求

Cisco 建议您了解以下主题：

- NAT 概述
- PIX/ASA 7.X：端口重定向

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco 5500系列ASA版本8.2
- Cisco ASDM版本6.3

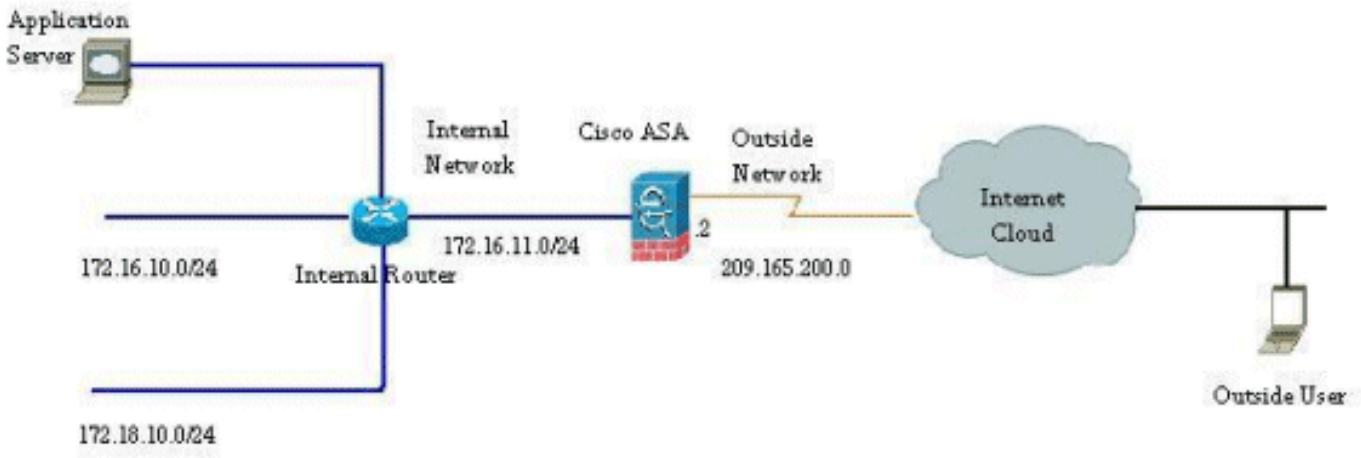
注意： 因为没有在NAT功能的重大更改此配置从Cisco ASA软件版本8.0到8.2仅良好工作。

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。

网络图

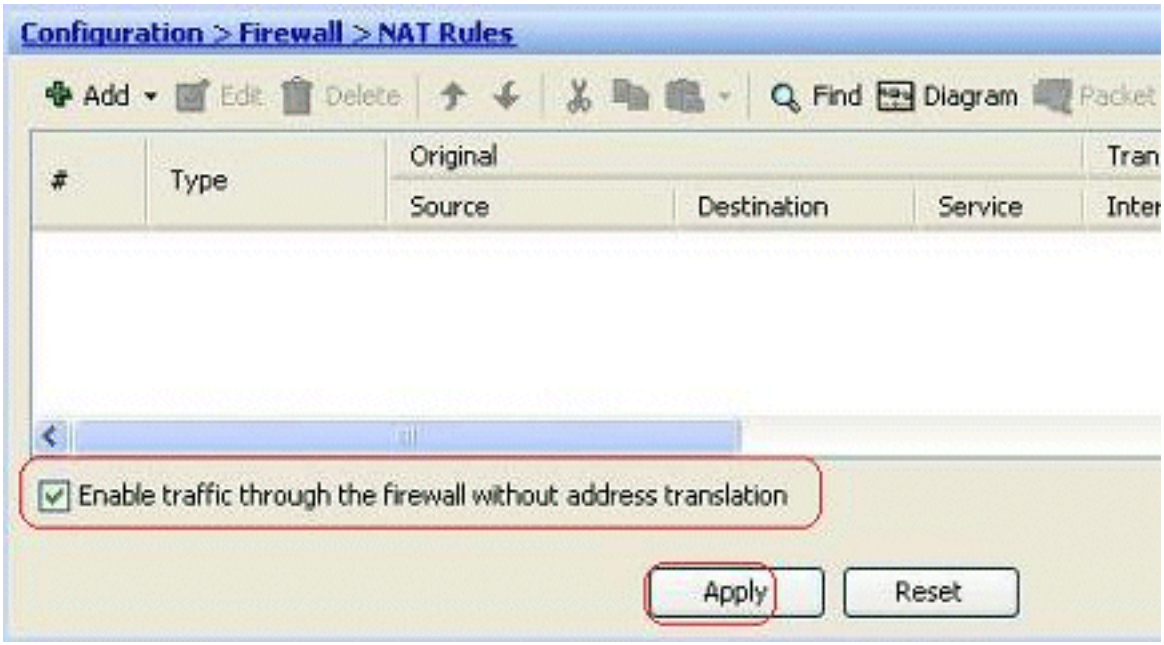


此配置中使用的 IP 编址方案在 Internet 上不可合法路由。这些地址是在实验室环境中使用的 RFC 1918 地址。

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。

连接不能穿过安全工具没有配置的转换规则。此功能呼叫nat-control。此处此处显示的图像表示如何通过ASDM禁用此为了通过ASA允许连接，不用任何地址转换。然而，如果安排任何转换规则配置，然后禁用此功能不保持有效为所有流量，并且您将需要明确地豁免从地址转换的网络。

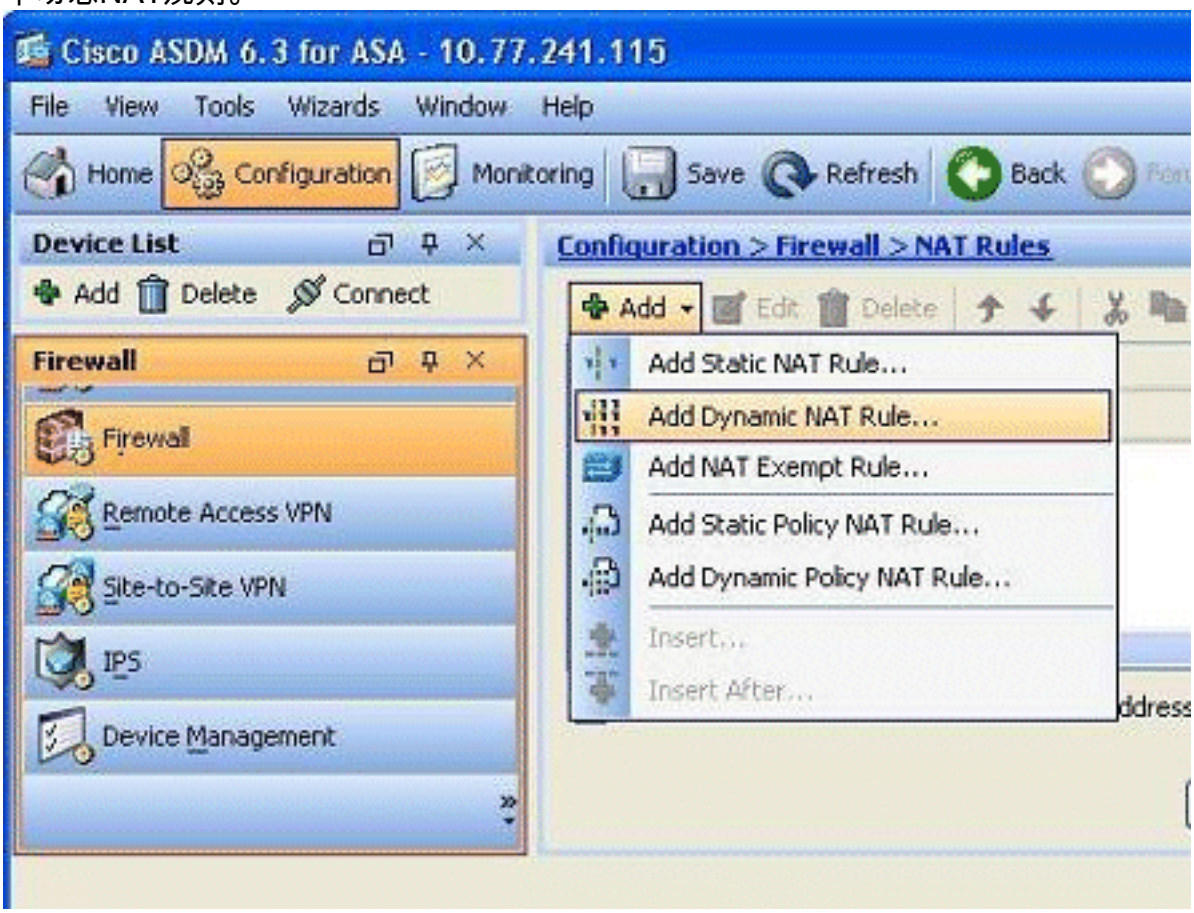


允许内部主机使用 NAT 访问外部网络

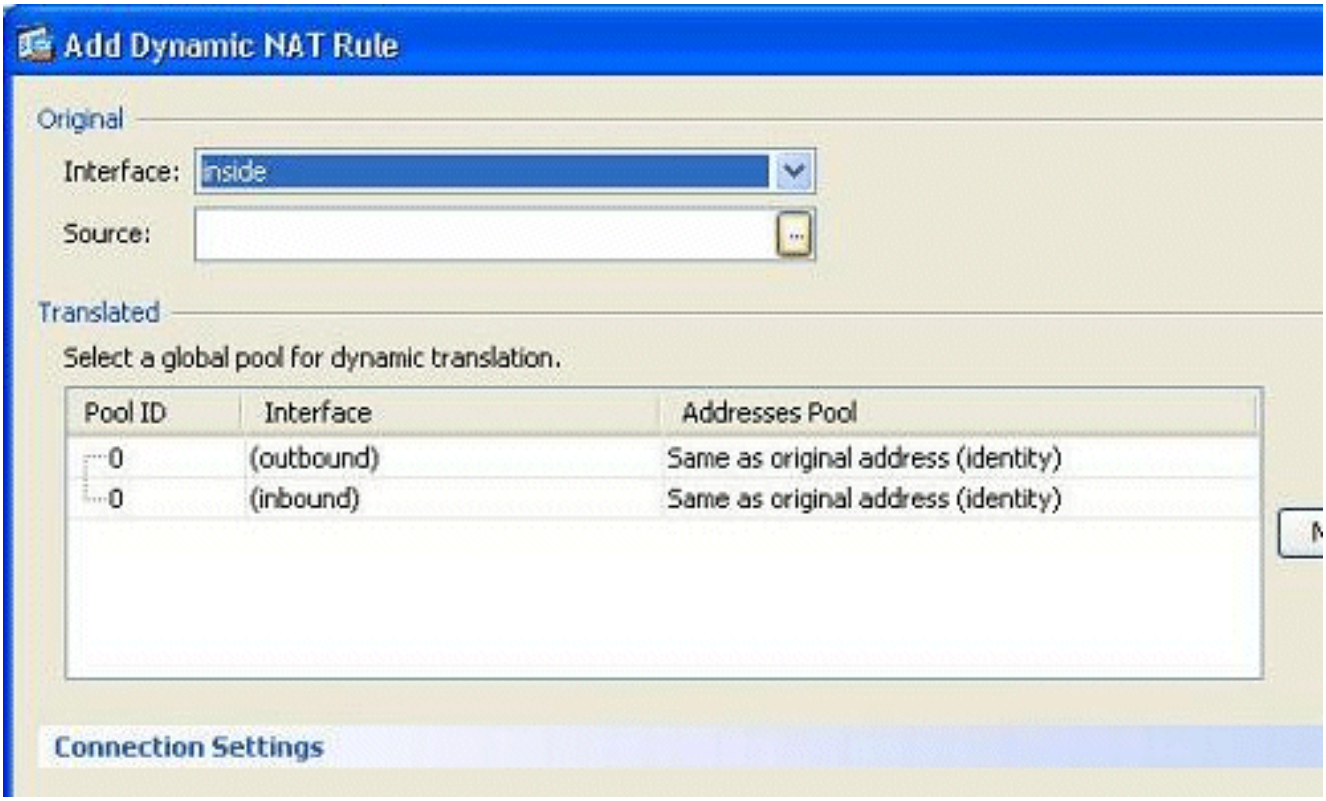
您可能允许内部主机/网络的一组通过配置动态NAT规则访问外界。为了完成此，您需要选择将给的主机/网络的实际地址访问，并且他们必须然后被映射对翻译的IP地址的池。

完成这些步骤为了允许内部主机对外部网络的访问与NAT:

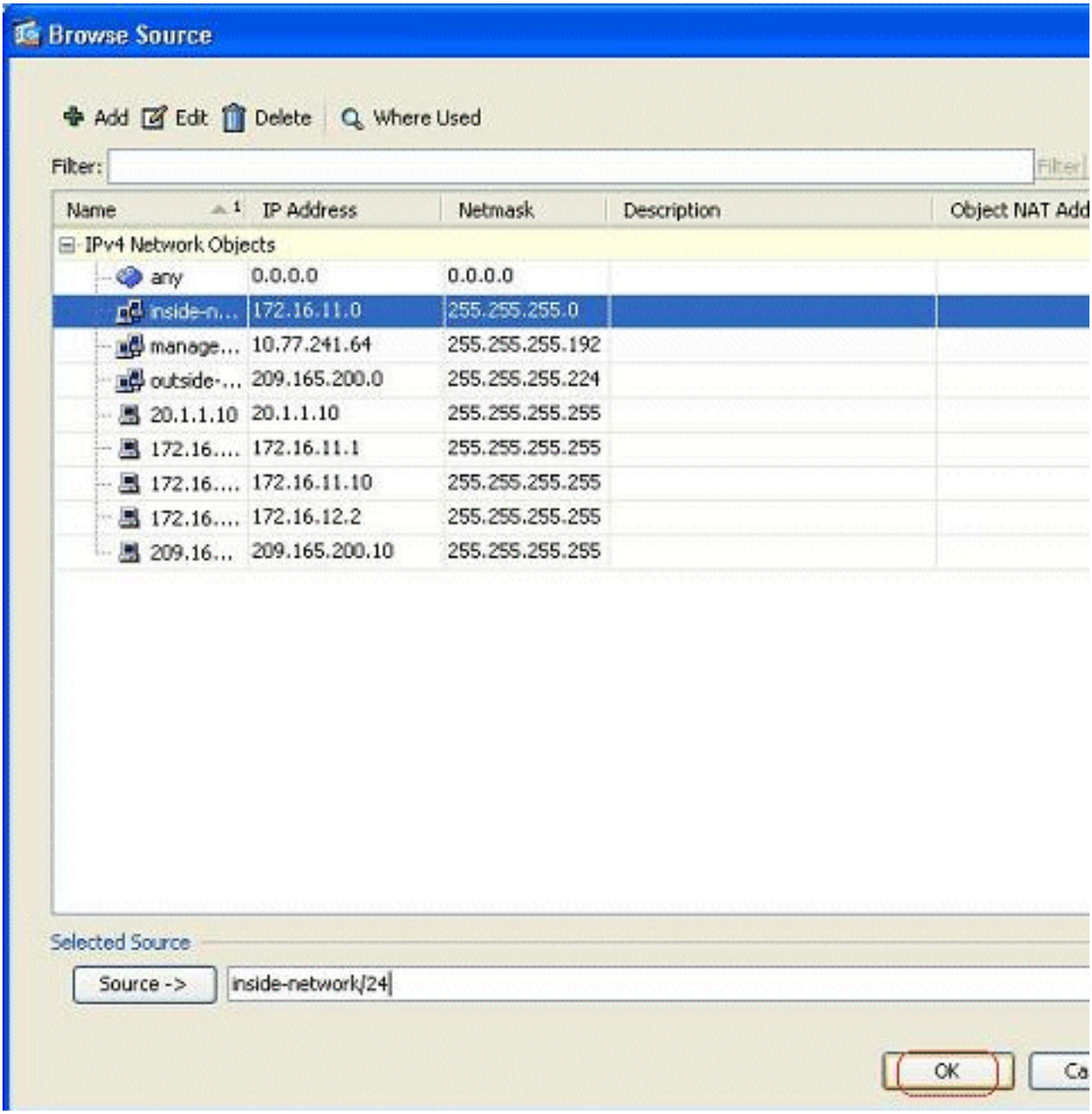
1. 去**Configuration>防火墙> NAT规则**，单击**添加**，然后选择**添加动态NAT规则**选项为了配置一个动态NAT规则。



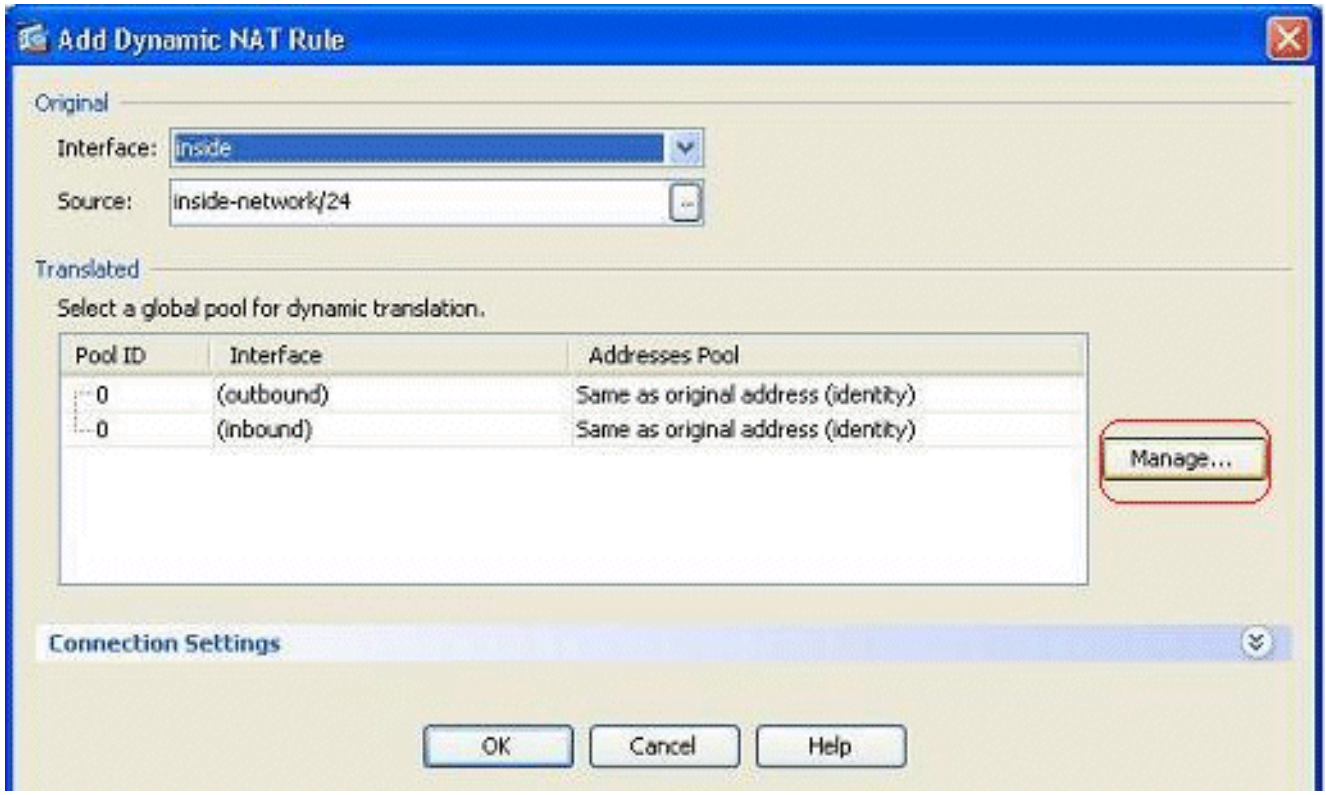
2. 选择实时主机连接接口的名称。使用在**Source字段的详细信息按钮**选择主机/网络的实际IP地址。



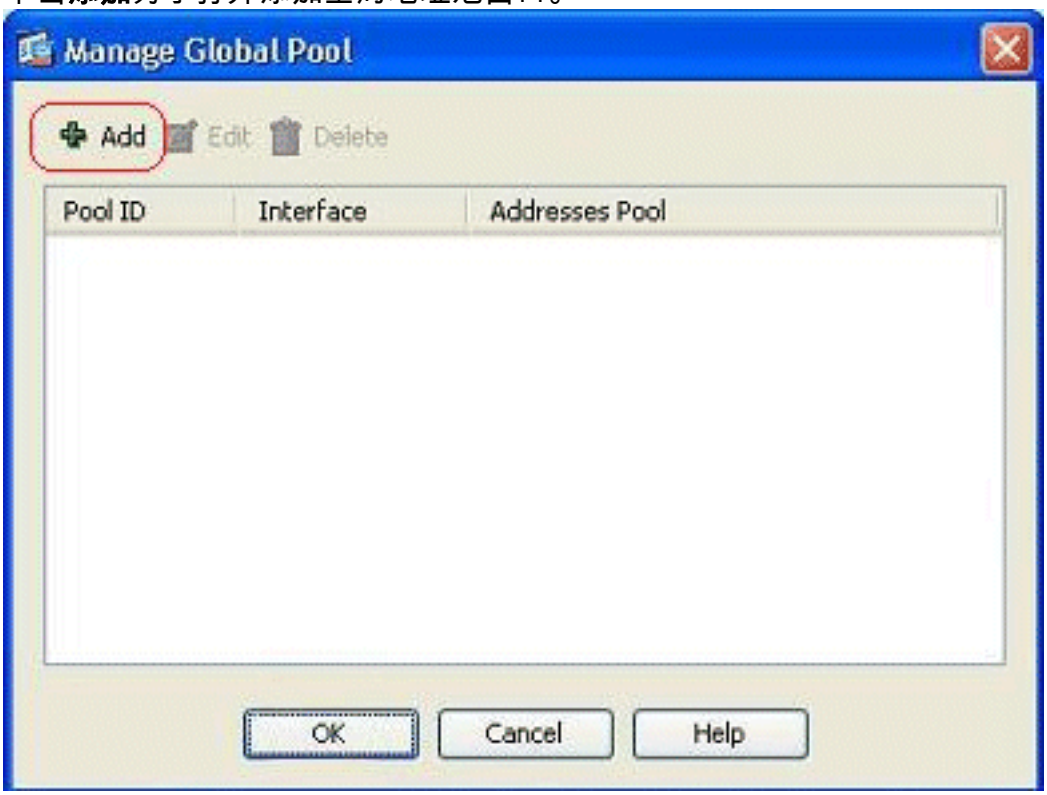
3. 在本例中，整个*网络内部*选择。点击OK键为了完成选择。



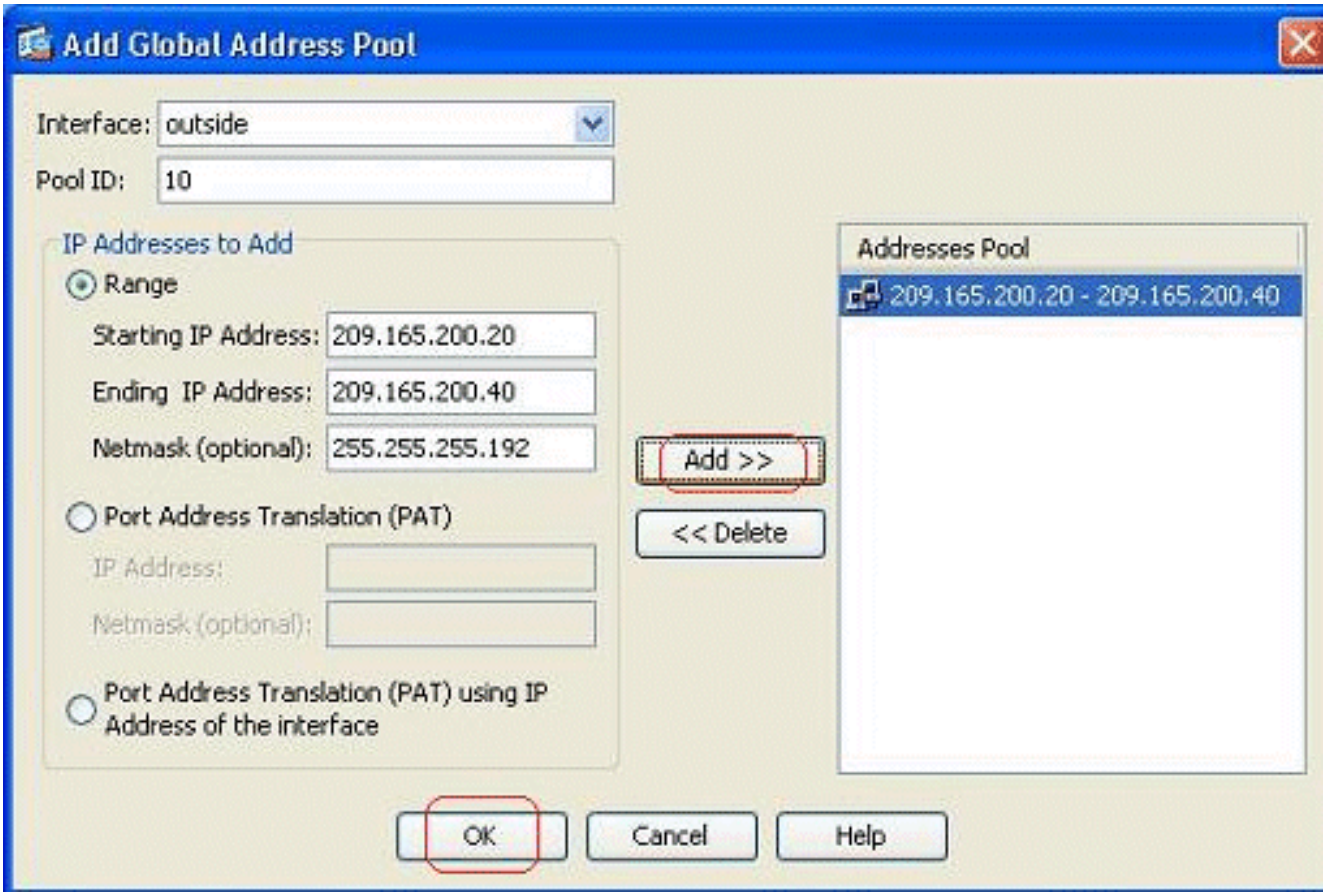
4. 单击**设法**为了选择实际网络将被映射IP地址的池。



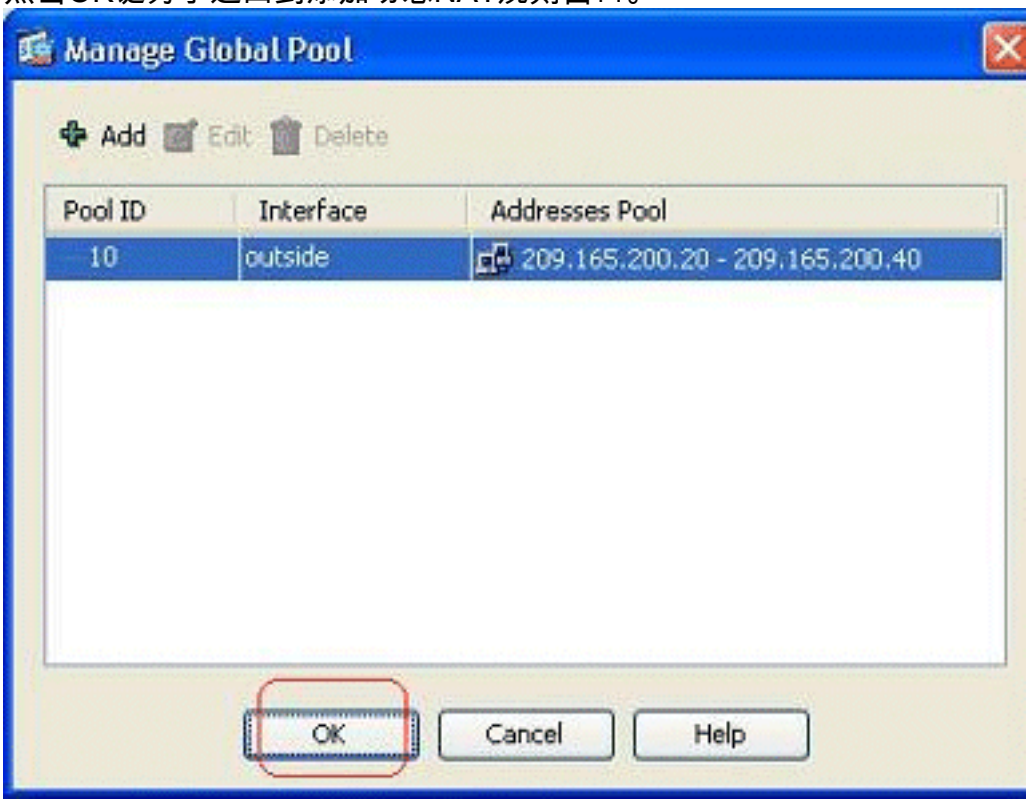
5. 单击**添加**为了打开添加全局地址池窗口。



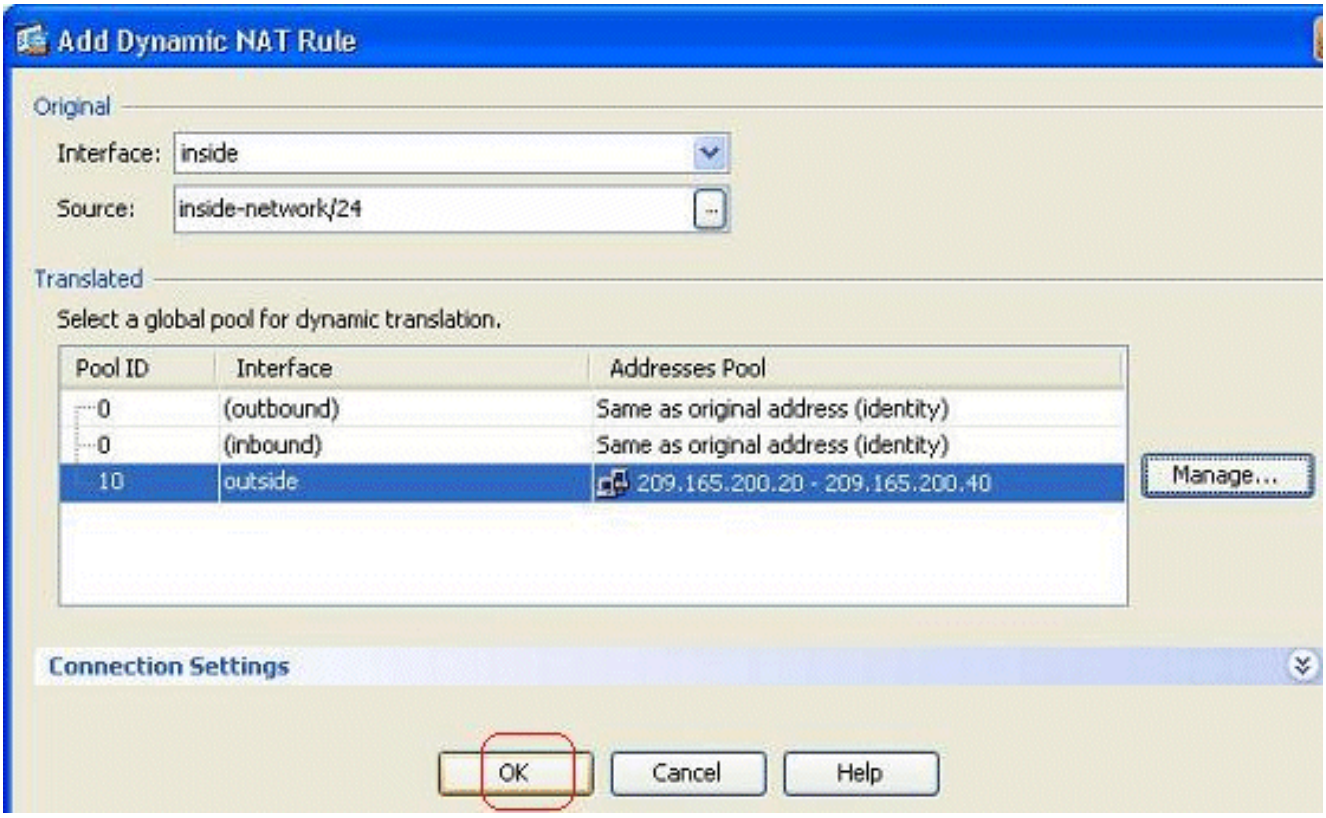
6. 选择**范围**选项并且与出口接口一起指定开始的和结束的IP地址。并且，请指定唯一池ID并且单击**添加**为了添加这些到地址池。点击OK键为了返回到管理全局池窗口。



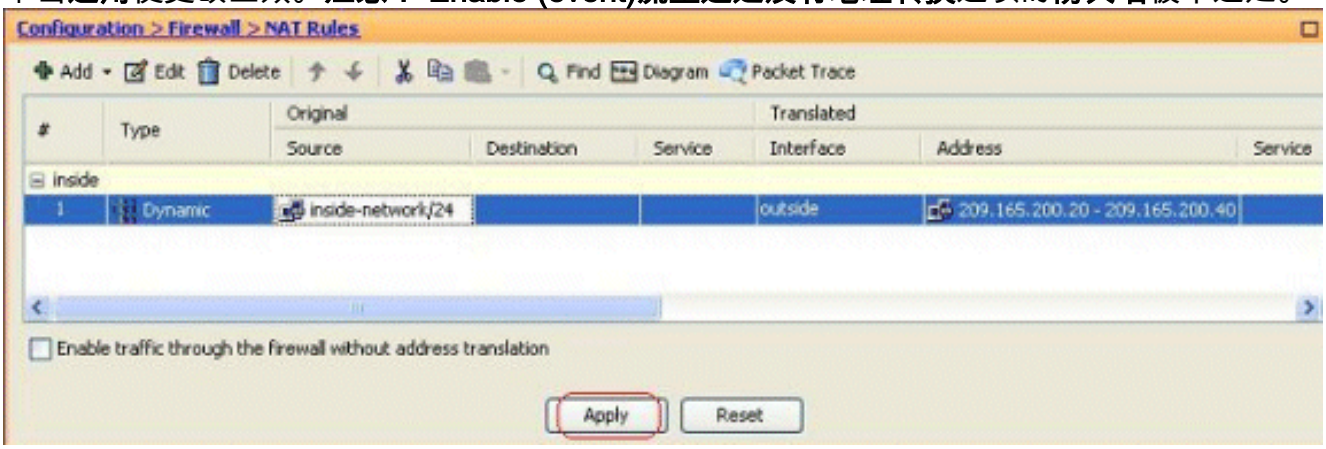
7. 点击OK键为了返回到添加动态NAT规则窗口。



8. 点击OK键为了完成动态NAT规则配置。



9. 单击**运用**使更改生效。**注意： Enable (event)流量通过没有地址转换**选项的**防火墙**被不选定。



这是为此ASDM配置输出的等同CLI ：

```
nat-control global (outside) 10 209.165.200.20-209.165.200.40 netmask 255.255.255.192 nat
(inside) 10 172.16.11.0 255.255.255.0
```

根据此配置，在172.16.11.0网络的主机将被转换对从NAT池的所有IP地址， 209.165.200.20-209.165.200.40。这里， NAT池ID是非常重要。您可能分配同一个NAT池到另一内部/dmz网络。如果被映射的池比实时组有少量地址，您可能用尽地址，如果流量总量更比预计是。结果，您可能尝试实现PAT或您可能设法编辑现有地址池延伸它。

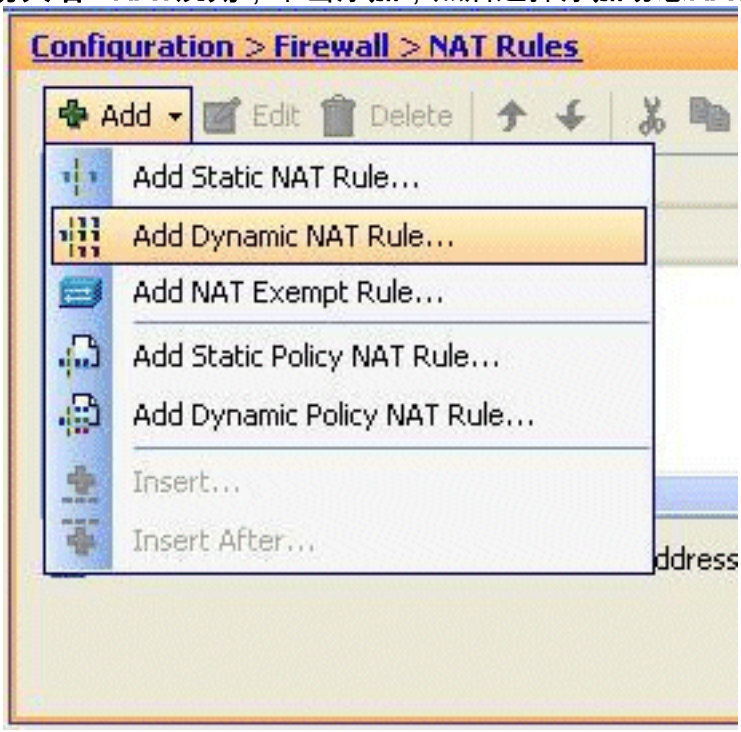
注意： 当进行时对现有转换规则的所有修改，注意到，您需要使用clear xlate命令那些修改生效。否则，上一个现有连接在连接表里将依然是那里，直到他们暂停。请是谨慎的，当曾经**clear xlate命令时**，因为立即终止现有连接。

允许内部主机对外部网络的访问与PAT

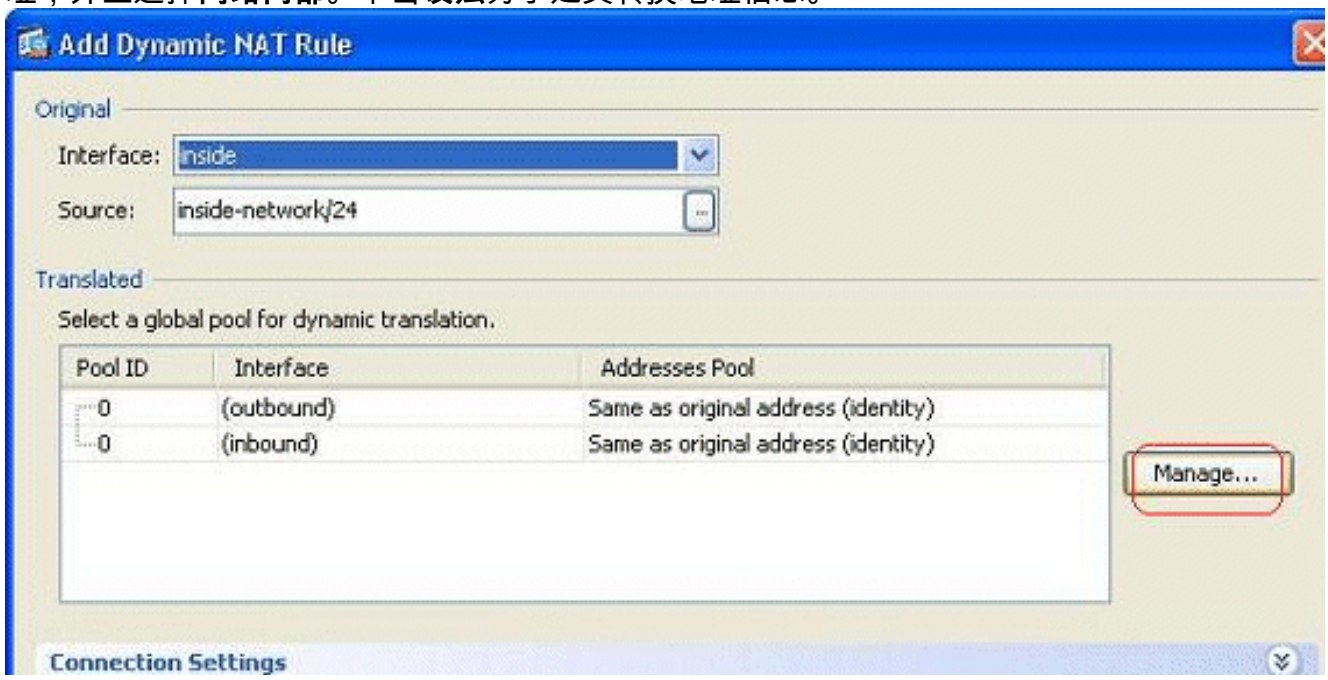
如果希望内部主机共享一个公共地址进行转换，请使用 PAT。如果 **global 语句**指定一个地址，则该地址是端口转换地址。ASA允许每接口和该转换支持的一次端口转换至对单个全局地址的65,535个有效转换对象。

完成这些步骤为了允许内部主机对外部网络的访问与PAT ：

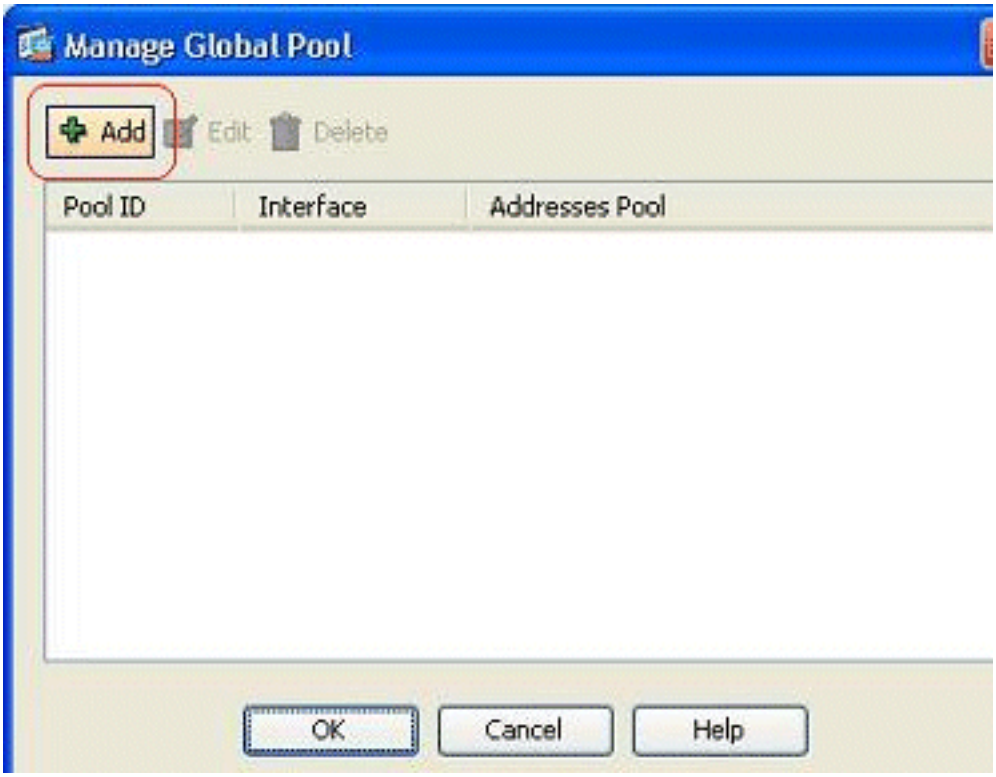
1. 去**Configuration>防火墙> NAT规则**，单击**添加**，然后选择**添加动态NAT规则**选项为了配置一个动态NAT规则。



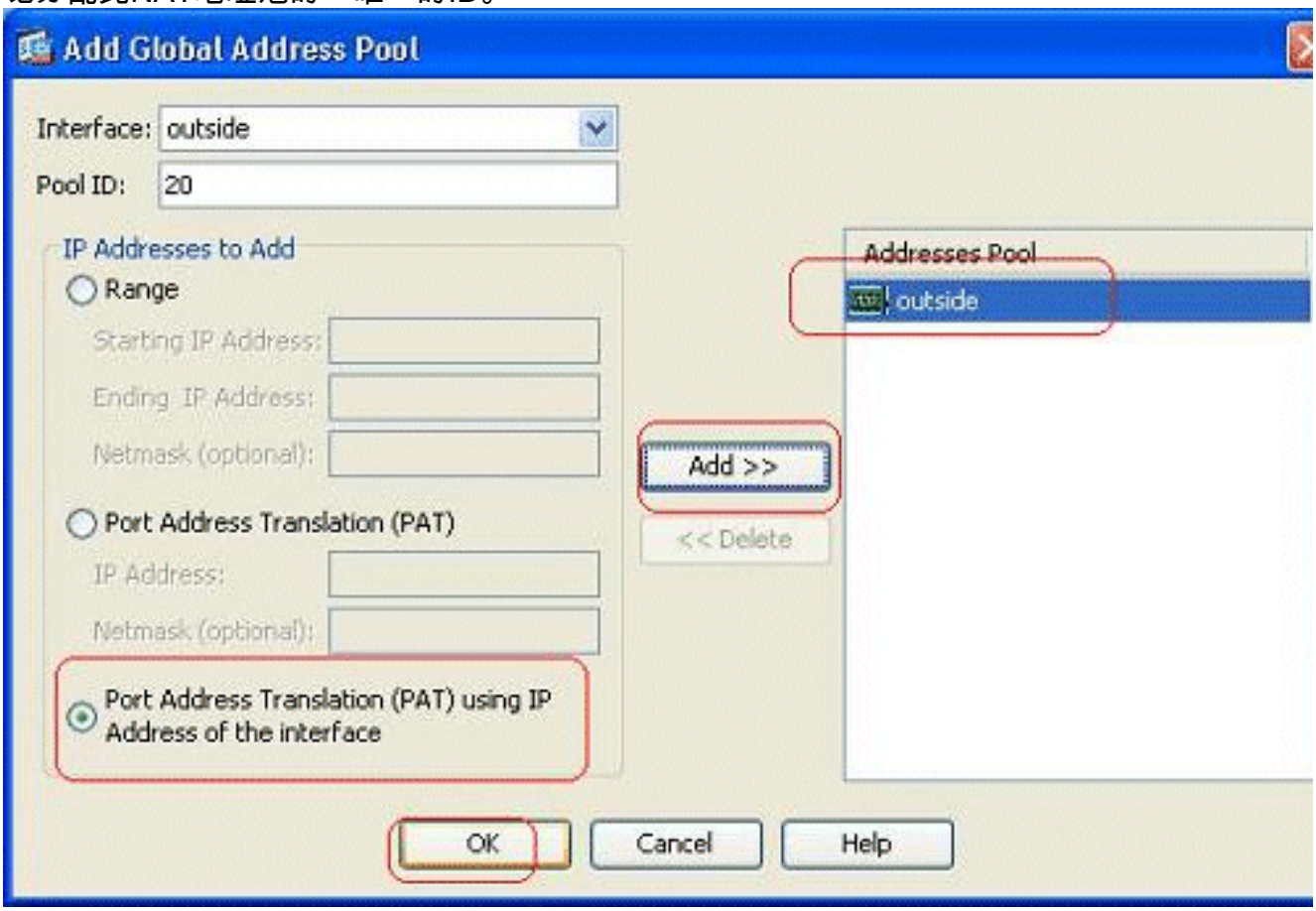
2. 选择实时主机连接接口的名称。使用在**Source字段的详细信息按钮**选择主机/网络的实际IP地址，并且选择**网络内部**。单击**设法**为了定义转换地址信息。



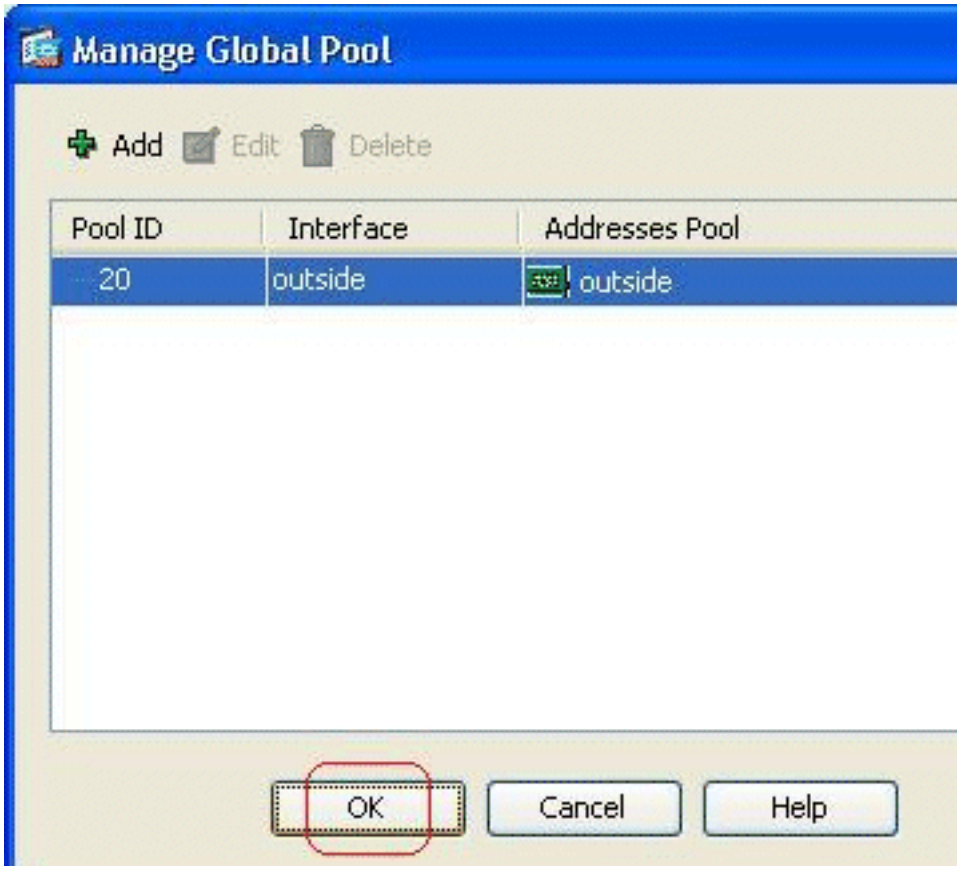
3. 单击 **Add**。



4. **使用接口选择的IP地址**选择**端口地址转换(PAT)**，并且单击**添加**为了添加它到地址池。请勿忘记分配此NAT地址池的一唯一的ID。

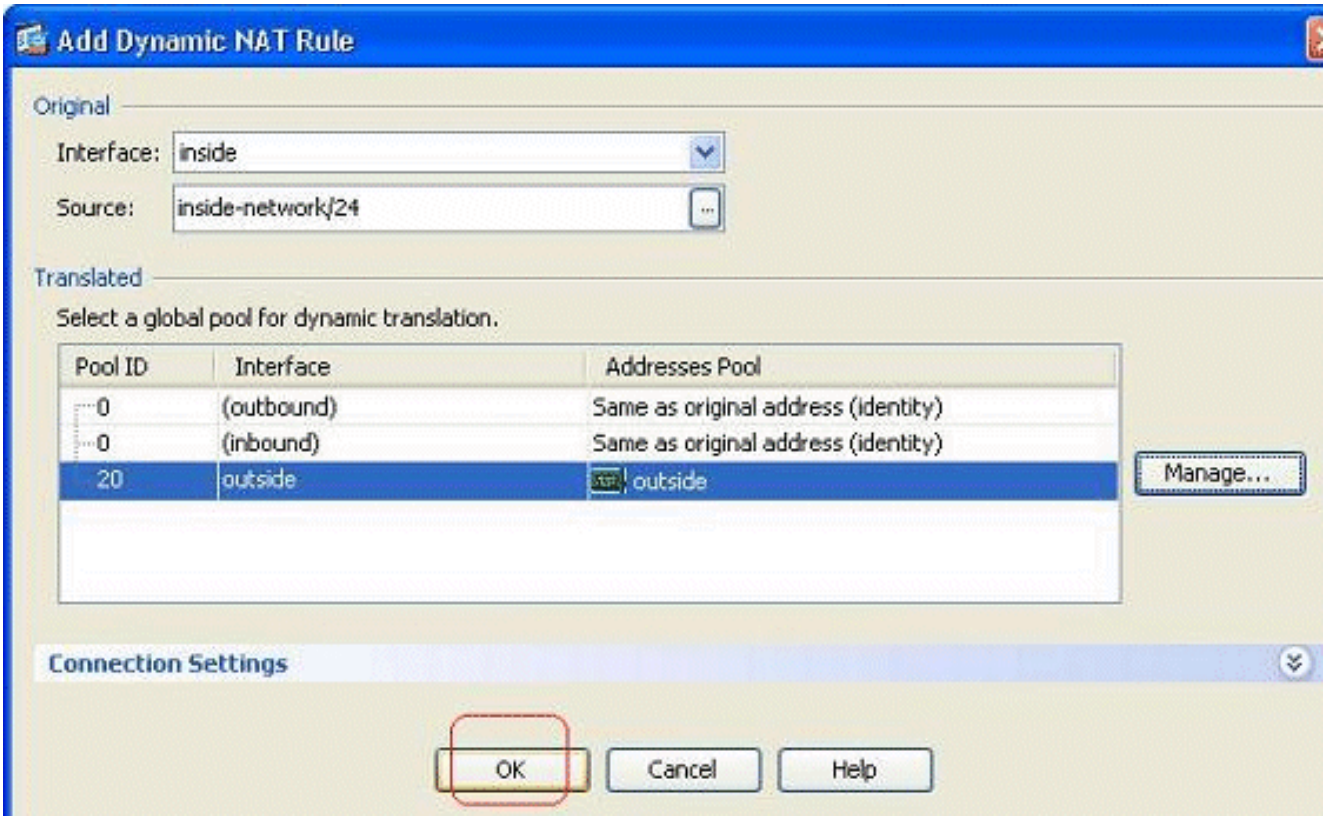


5. 显示此处有外部接口的配置的地址池作为在该池的唯一的可用地址。点击OK键为了返回到添

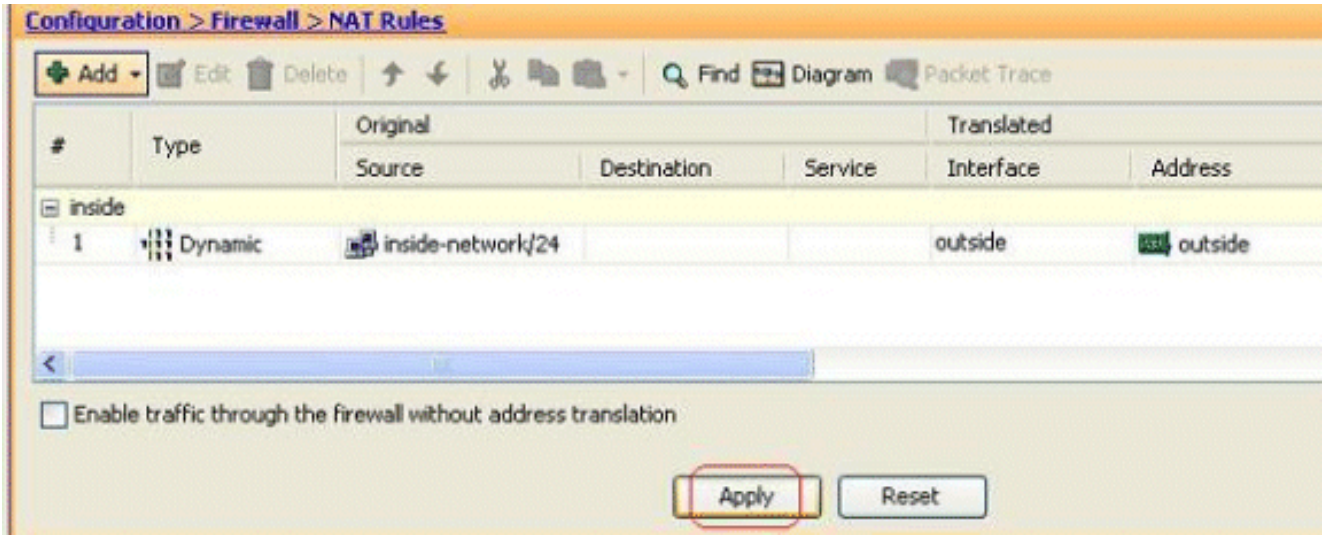


加动态NAT规则窗口。

6. 单击 **Ok**。



7. 已配置的动态NAT规则在Configuration>防火墙> NAT规则窗格显示此处。



这是为此PAT配置输出的等同CLI ：

```
global (outside) 20 interface nat (inside) 20 172.16.11.0 255.255.255.0
```

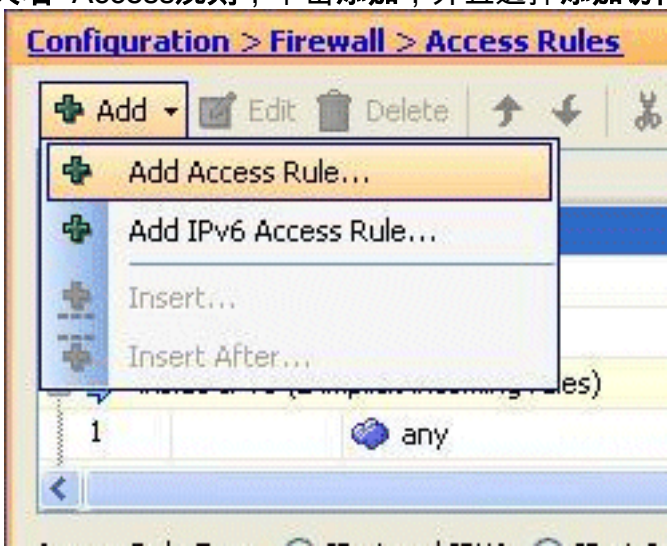
限制内部主机对外部网络的访问

当访问规则没有定义时，从更高安全性接口的用户能访问所有资源关联与较低安全性接口。要限制从访问某些资源的某些用户，请使用访问规则在ASDM。此示例描述如何允许单个用户访问外部资源(与FTP、SMTP、POP3、HTTPS和WWW)和从访问外部资源限制其他。

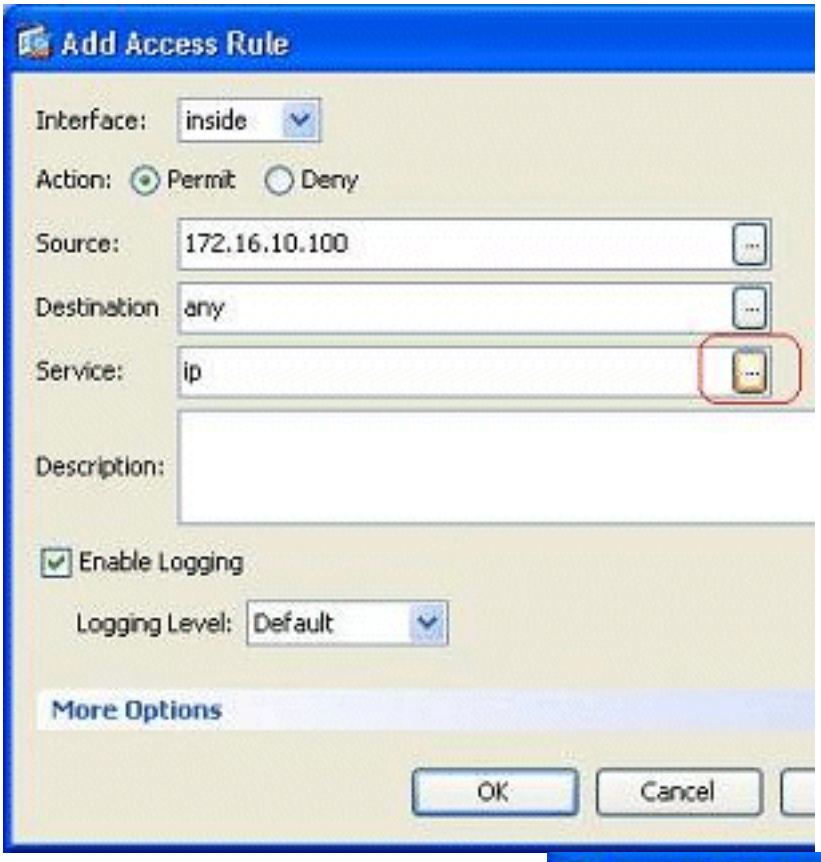
注意： “隐式拒绝”规则在每结束时access-list。

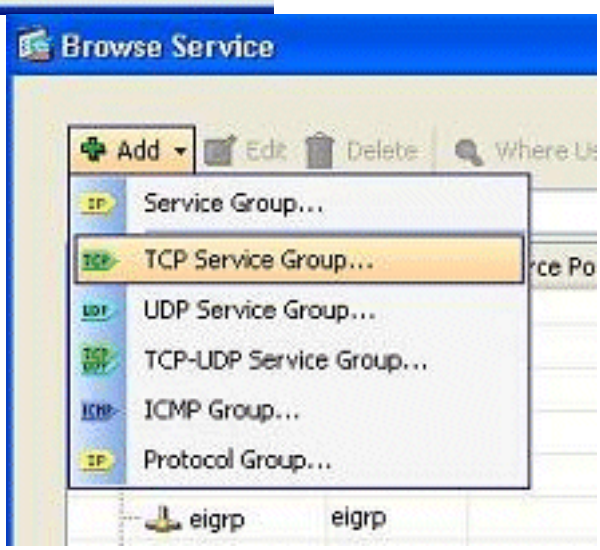
完成这些步骤：

1. 去**Configuration>防火墙**>Access**规则**，单击**添加**，并且选择**添加访问规则**选项为了创建一个新的访问列表条目。

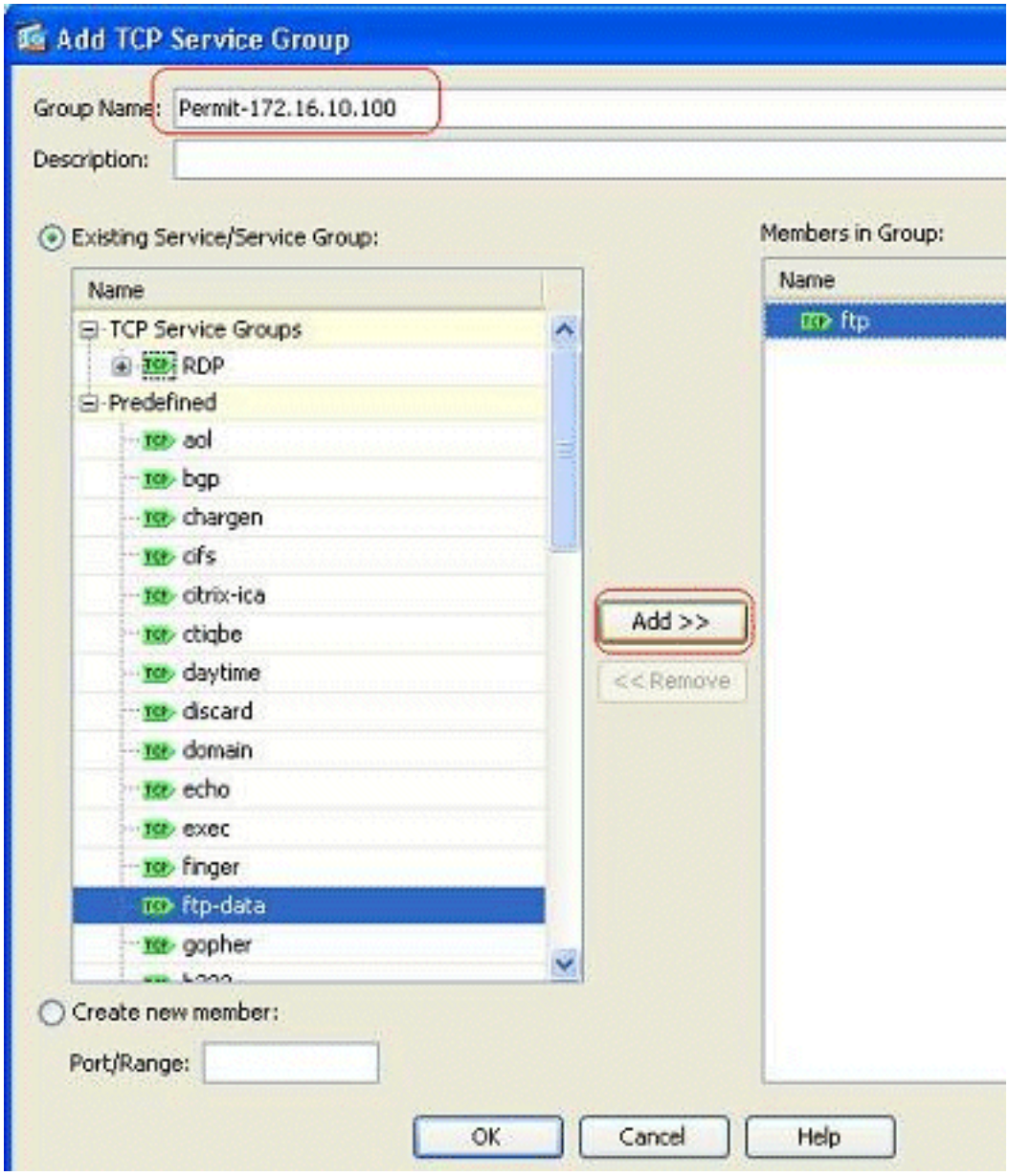


2. 选择将允许在**Source字段的**源IP地址。选择其中**任一**作为目的地，**在**作为接口里面，并且**允许**作为操作。最后，请在服务字段点击**详细信息按钮**为了创建需要的端口的一TCP服务组。



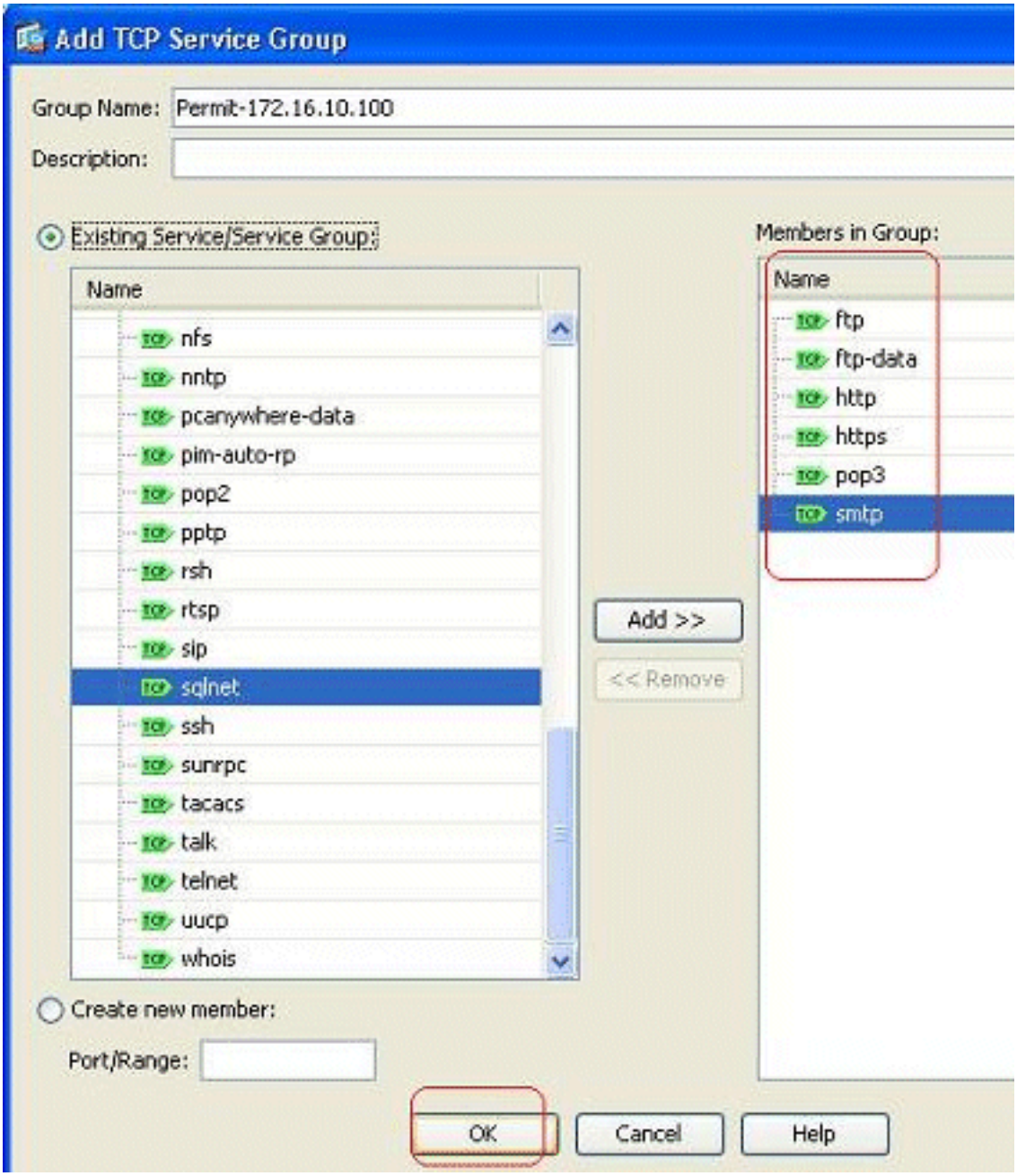


3. 单击**添加**，然后选择**TCP服务组**选项。
4. 输入此组的名称。选择其中每一个需要的端口，并且单击**添加**为了移动他们向Group字段的成

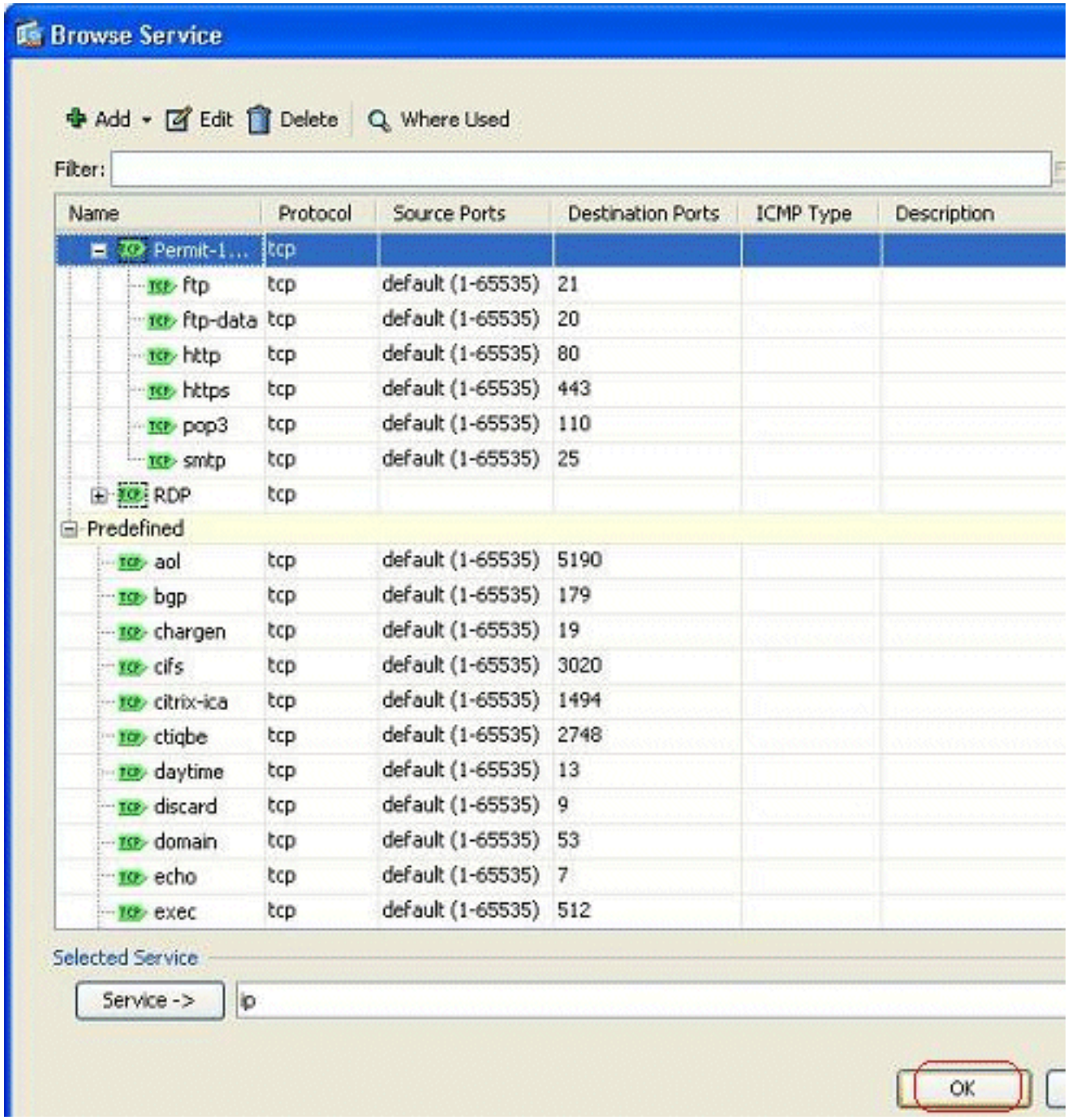


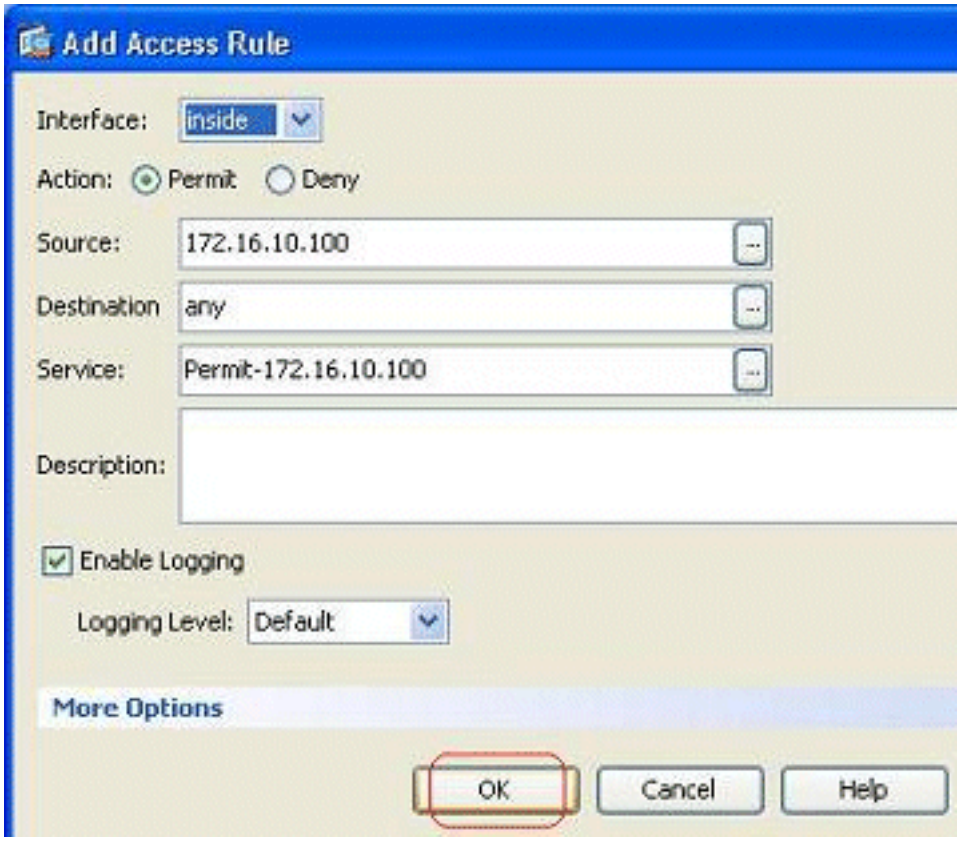
员。

5. 您应该看到所有所选的端口在右边的字段。点击OK键为了完成选择进程的服务端口。

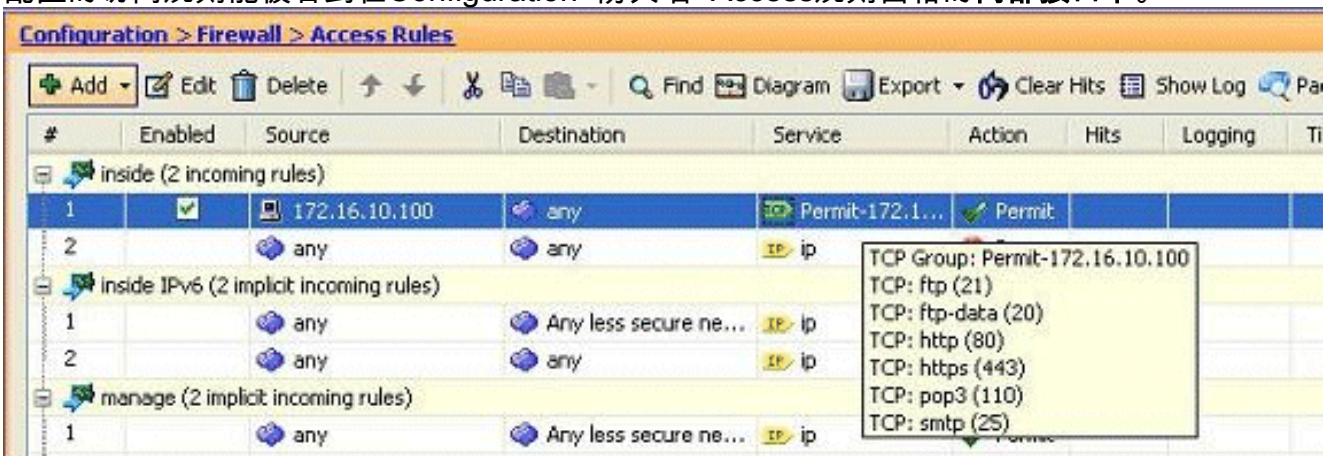


6. 您能看到已配置的TCP服务组此处。单击 **Ok**。

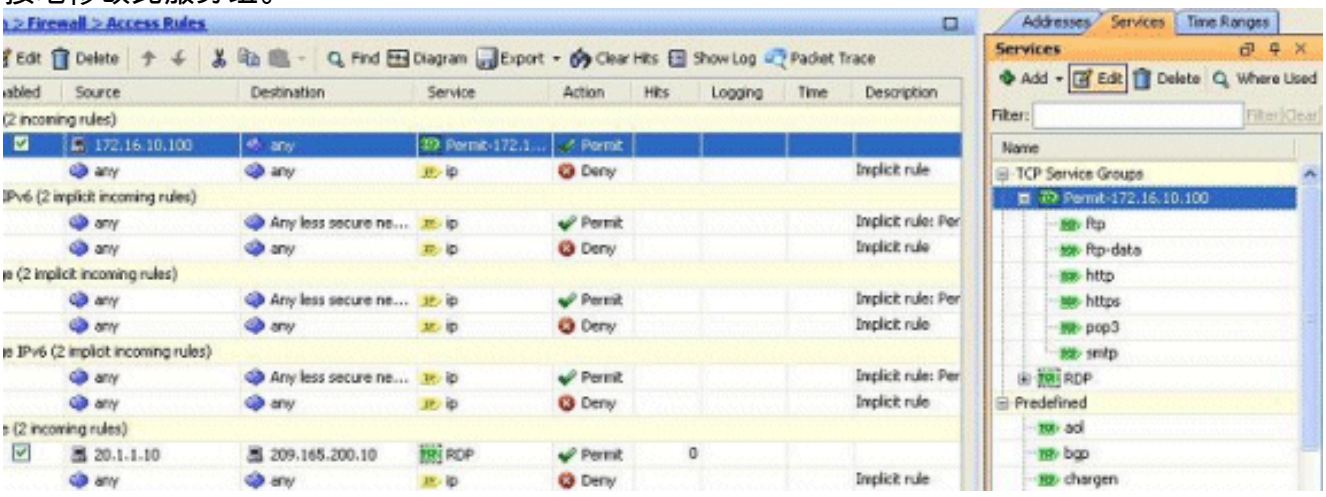

Browse Service
Add
Edit
Delete
Where Used
Filter:
Name
Protocol
Source Ports
Destination Ports
ICMP Type
Description
Permit-1...
tcp
ftp
tcp
default (1-65535)
21
ftp-data
tcp
default (1-65535)
20
http
tcp
default (1-65535)
80
https
tcp
default (1-65535)
443
pop3
tcp
default (1-65535)
110
smtp
tcp
default (1-65535)
25
RDP
tcp
Predefined
aol
tcp
default (1-65535)
5190
bgp
tcp
default (1-65535)
179
chargen
tcp
default (1-65535)
19
cifs
tcp
default (1-65535)
3020
citrix-ica
tcp
default (1-65535)
1494
ctiqbe
tcp
default (1-65535)
2748
daytime
tcp
default (1-65535)
13
discard
tcp
default (1-65535)
9
domain
tcp
default (1-65535)
53
echo
tcp
default (1-65535)
7
exec
tcp
default (1-65535)
512
Selected Service
Service ->
ip
OK



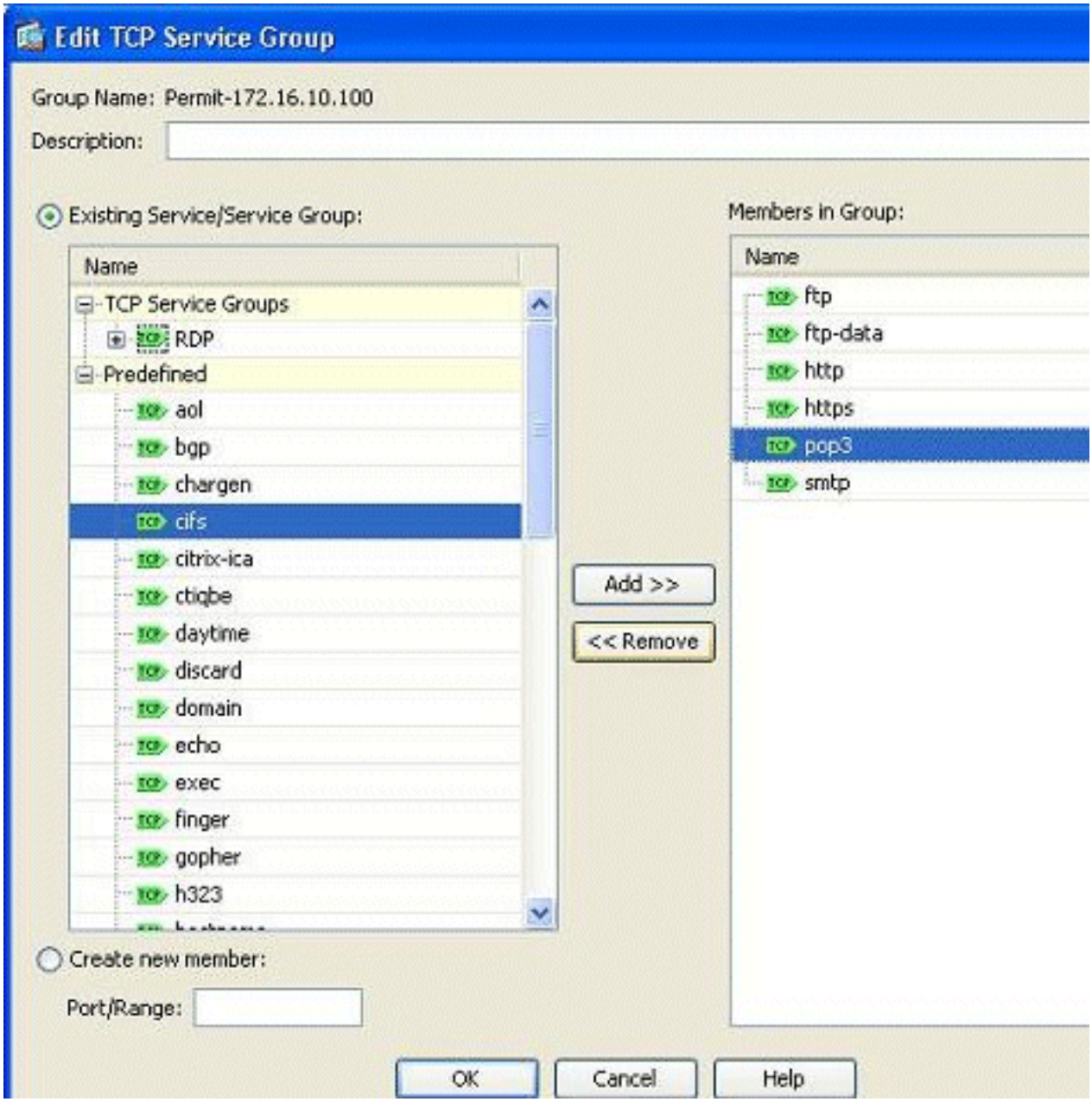
7. 单击 **OK** 以完成配置。
8. 配置的访问规则能被看到在Configuration>防火墙>Access规则窗格的**内部接口下**。



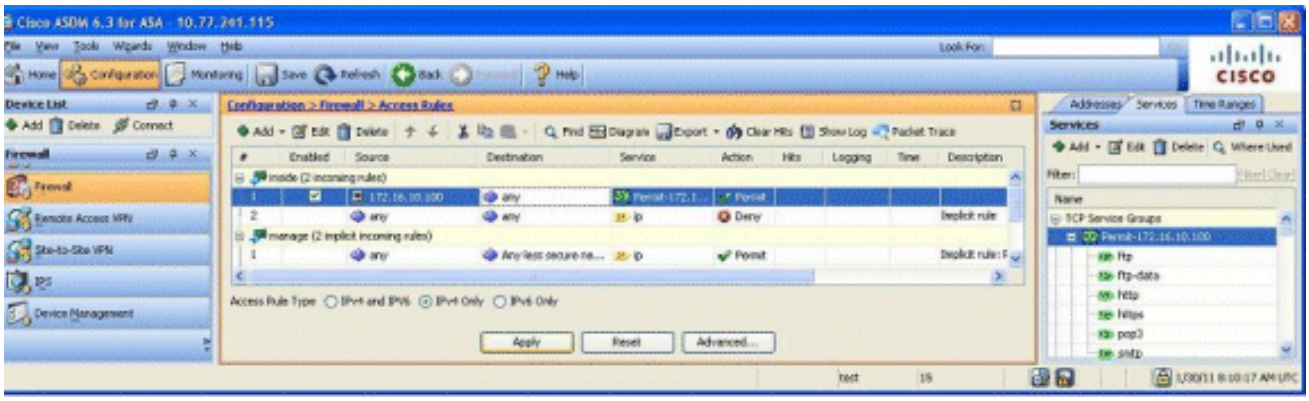
9. 对于易用，您可能也编辑TCP服务组直接地在**Services选项的**右边的窗格的。单击**编辑**为了直接地修改此服务组。



10. 它再重定向对编辑TCP服务组联式窗。进行根据您的需求的修改，并且点击OK键为了保存更改。



11. 显示此处ASDM的一张完整视图
：



这是等同CLI配置：

```
object-group service Permit-172.16.10.100 TCP port-object eq ftp port-object eq ftp-data port-
object eq www port-object eq https port-object eq pop3 port-object eq smtp ! access-list
inside_access_in extended permit TCP host 172.16.10.100 any object-group Permit-172.16.10.100 !
access-group inside_access_in in interface inside !
```

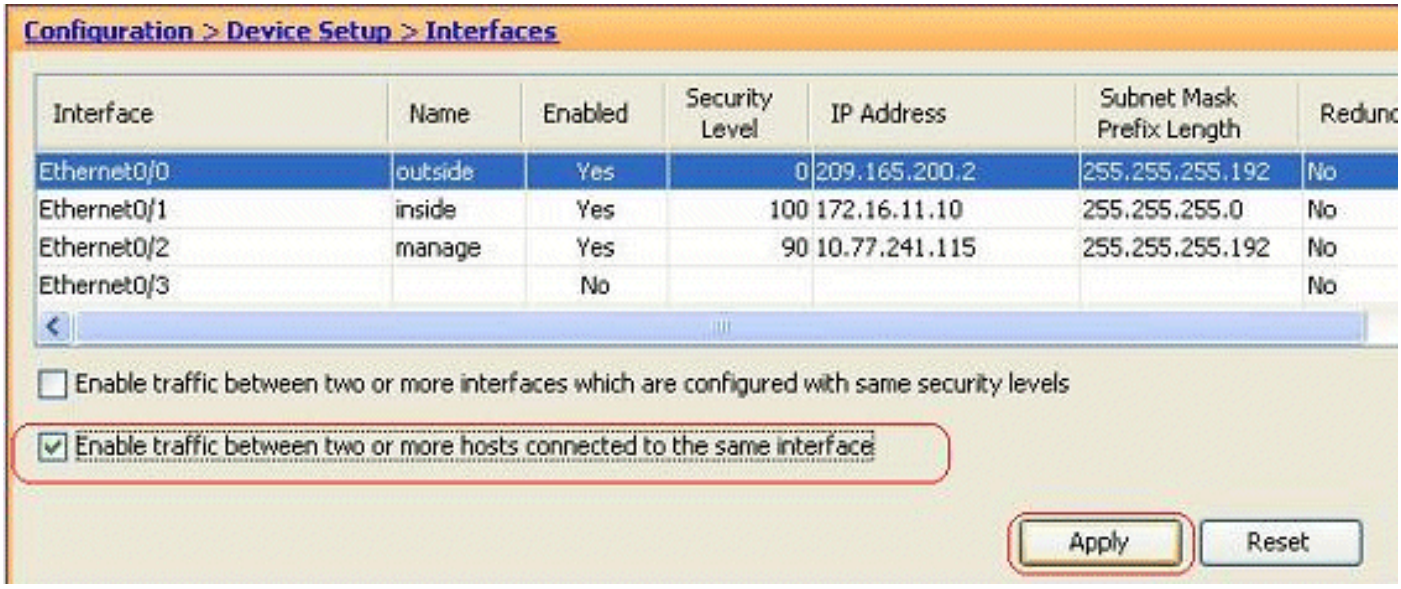
关于实现访问控制的全部信息，参考通过ASDM GUI添加或修改访问列表。

允许接口之间的流量与同样安全等级

此部分描述如何启用在有同样安全等级的接口内的流量。

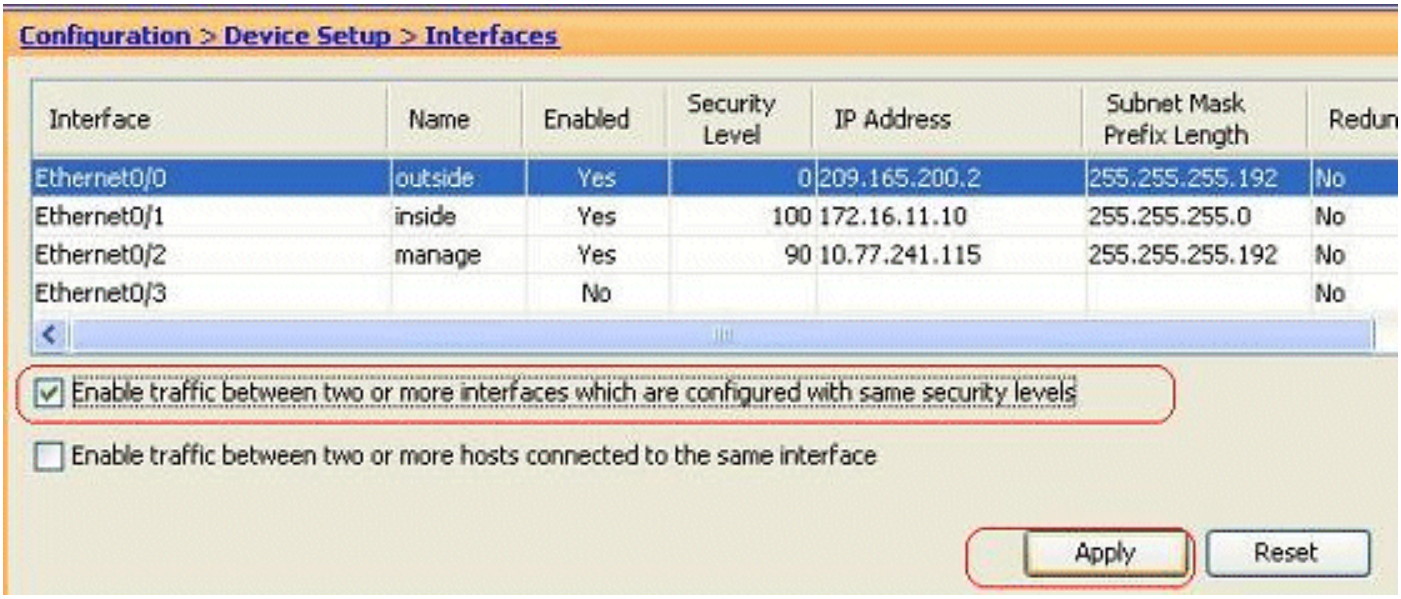
这些说明描述如何启用接口内通信。

进入接口的这为VPN流量将是有用，但是然后路由同一个接口。VPN流量也许在这种情况下未加密，或者也许为另一VPN连接被再加密。去**Configuration>设备设置>接口**，并且选择**两个或多个主机之间的Enable (event)流量连接对同一个接口选择**。



这些说明描述如何启用接口之间通信。

这是有用的允许接口之间的通信与相等的安全等级。去**Configuration>设备设置>接口**，并且选择**配置与同样安全等级**选项的**两个或多个接口之间的Enable (event)流量**。



这是这两设置的等同CLI ：

```
same-security-traffic permit intra-interface
same-security-traffic permit inter-interface
```

允许不受信任的主机访问受信任的网络中的主机

这可以通过应用静态NAT转换和访问规则达到允许那些主机。您需要配置此，每当外部用户希望访问在您的内部网络坐的所有服务器。在不是可路由的在互联网的内部网络的服务器将有一个专用IP地址。结果，您需要翻译该专用IP地址到公网IP地址通过一个静态NAT规则。假设您有一个内部服务器(172.16.11.5)。为了做此工作，您需要翻译此私有服务器IP到公有IP。此示例描述如何实现双向静态NAT翻译172.16.11.5到209.165.200.5。

关于允许外部用户的部分通过实现访问规则访问此Web服务器没有显示此处。摘要CLI片断为您的了解显示此处：

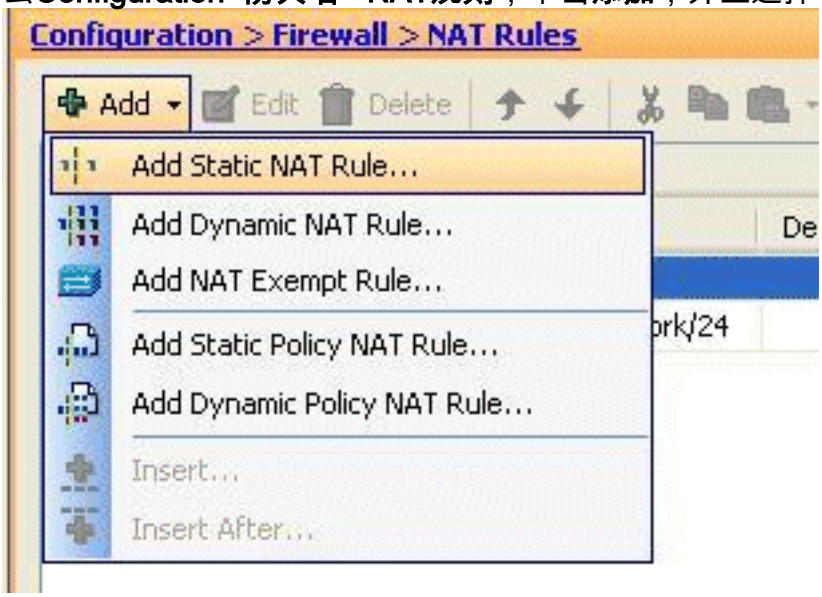
```
access-list 101 permit TCP any host 209.165.200.5
```

欲知更多信息，参考通过ASDM GUI添加或修改访问列表。

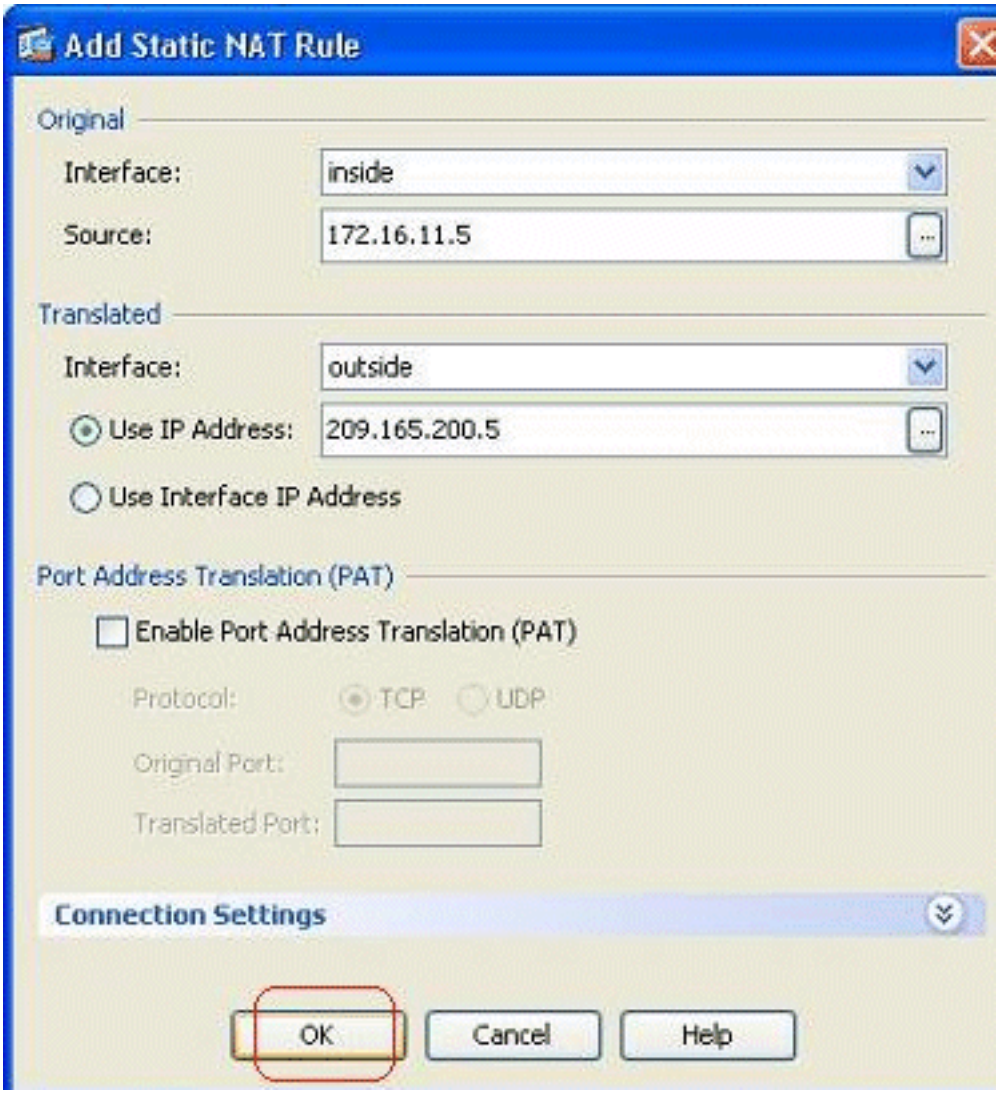
注意： 指定关键字“其中任一”允许从外界的所有用户访问此服务器。并且，如果没有为任何服务端口指定，服务器在所有服务端口可以访问，当那些开放的逗留。请当心，当您实现时，并且您建议限制权限对单个外部用户并且对在服务器的所需端口。

完成这些步骤为了配置静态NAT ：

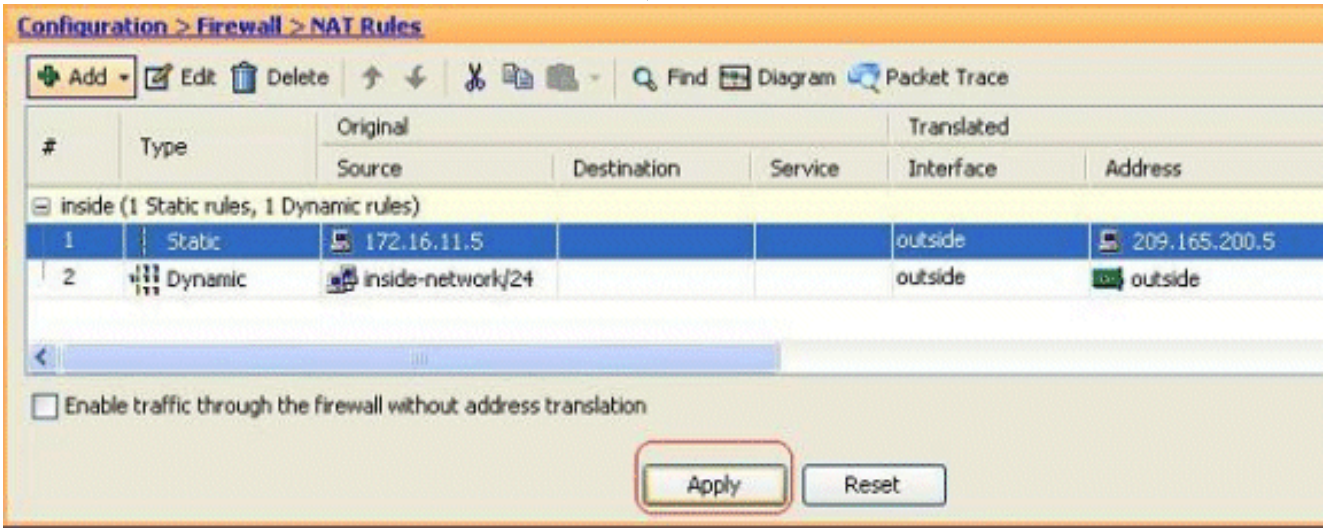
1. 去**Configuration>防火墙> NAT规则**，单击**添加**，并且选择**增加静态NAT规则**。



2. 与他们相关的接口一起指定原始IP地址和转换后的IP地址，并且点击OK键。



3. 您能看到已配置的静态NAT条目此处。单击**应用**为了发送此到ASA。



这是此ASDM配置的一摘要CLI示例：

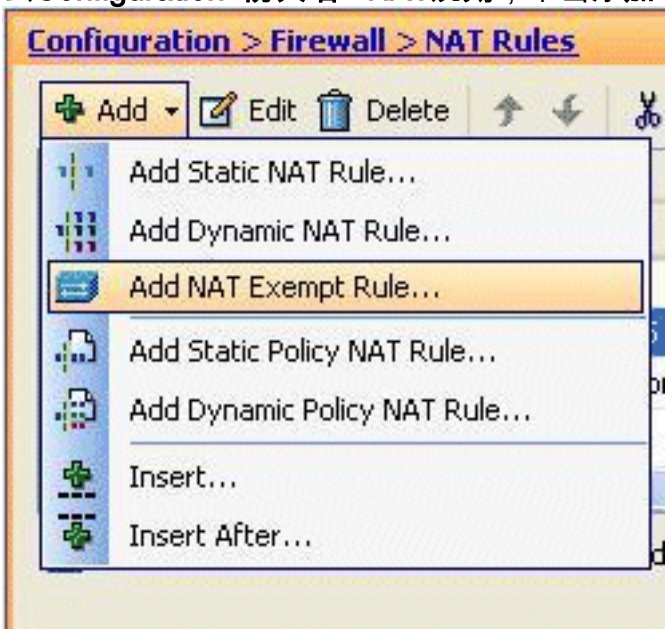
```
! static (inside,outside) 209.165.200.5 172.16.11.5 netmask 255.255.255.255 !
```

对特定主机/网络禁用 NAT

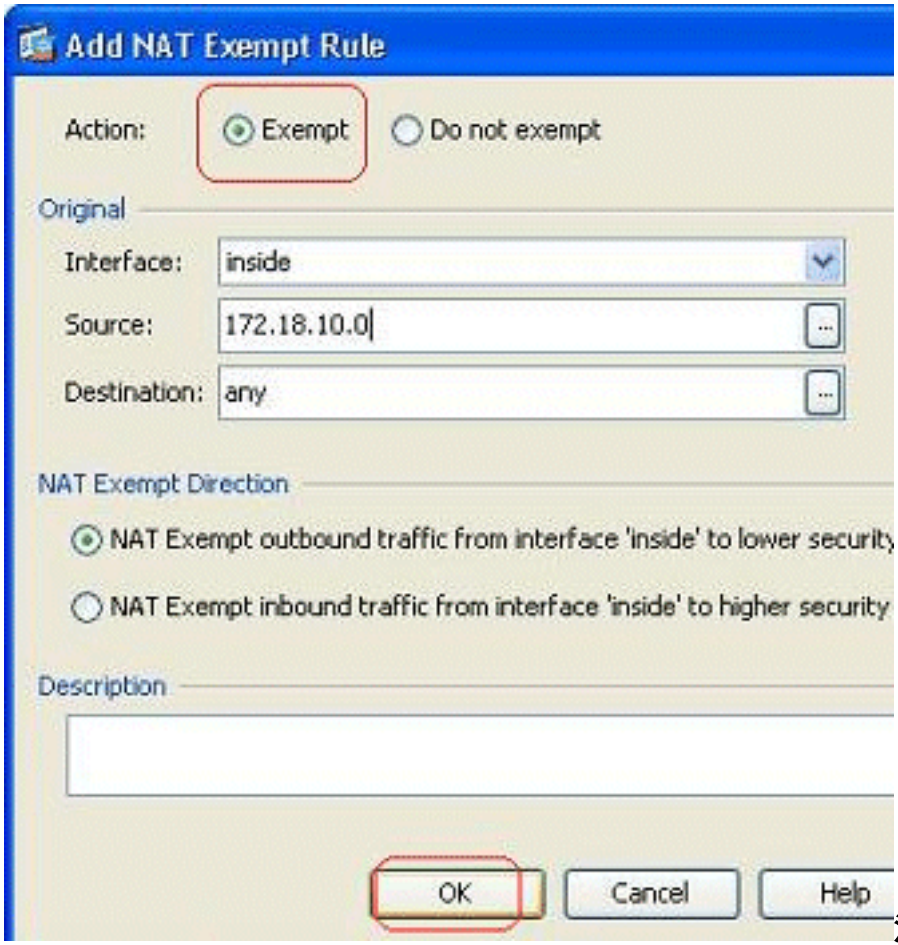
当您需要豁免特定主机或网络从NAT时，请增加一个NAT豁免规则禁用地址转换。这准许翻译和远程主机首次连接。

完成这些步骤：

1. 去**Configuration>防火墙> NAT规则**，单击**添加**，并且选择**增加NAT豁免规则**。

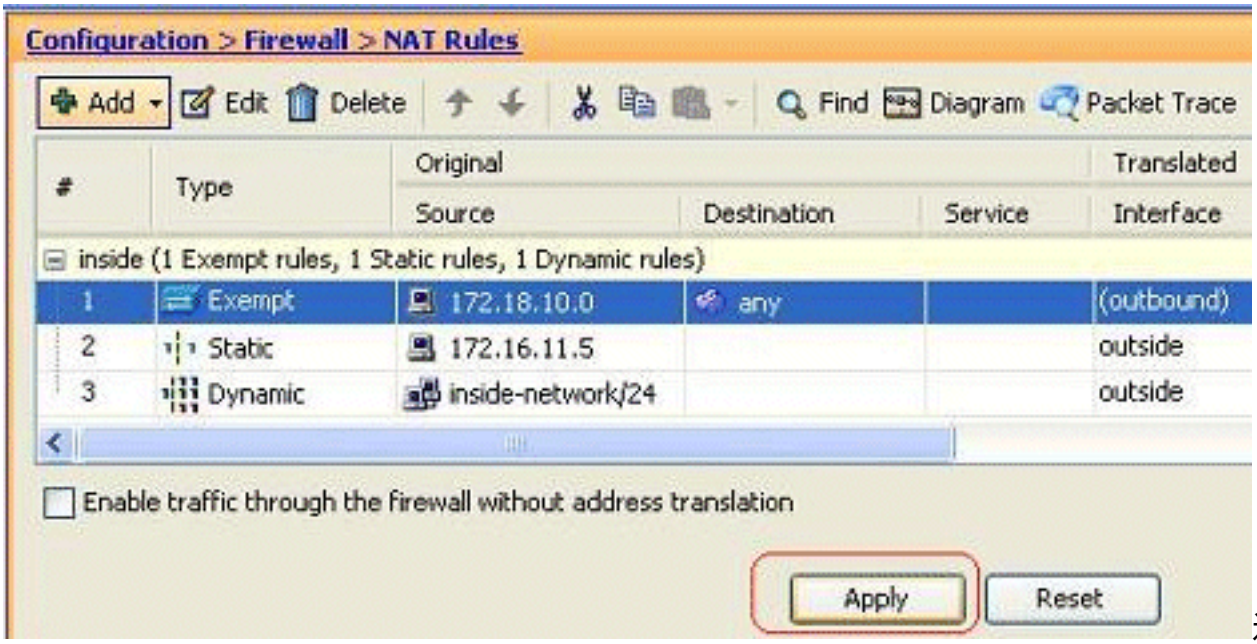


2. 这里，网络内部172.18.10.0从地址转换被豁免了。确保**豁免**选项选择。NAT豁免方向有两个选项：对较低安全性接口的出站流量对更高安全性接口的入站数据流默认选项是为出站流量。



点击OK键为了完成步骤。**注意**：当您选择时请勿**豁免**选项，该特定主机不会从NAT被豁免，并且一个分开的访问规则将增加与“拒绝”关键字。这是有用在避免从NAT的特定主机豁免，虽然完整子网，不包括这些主机，被豁免的NAT。

3. 您能为出站方向看到NAT豁免规则此处。单击**应用**为了发送配置到ASA。

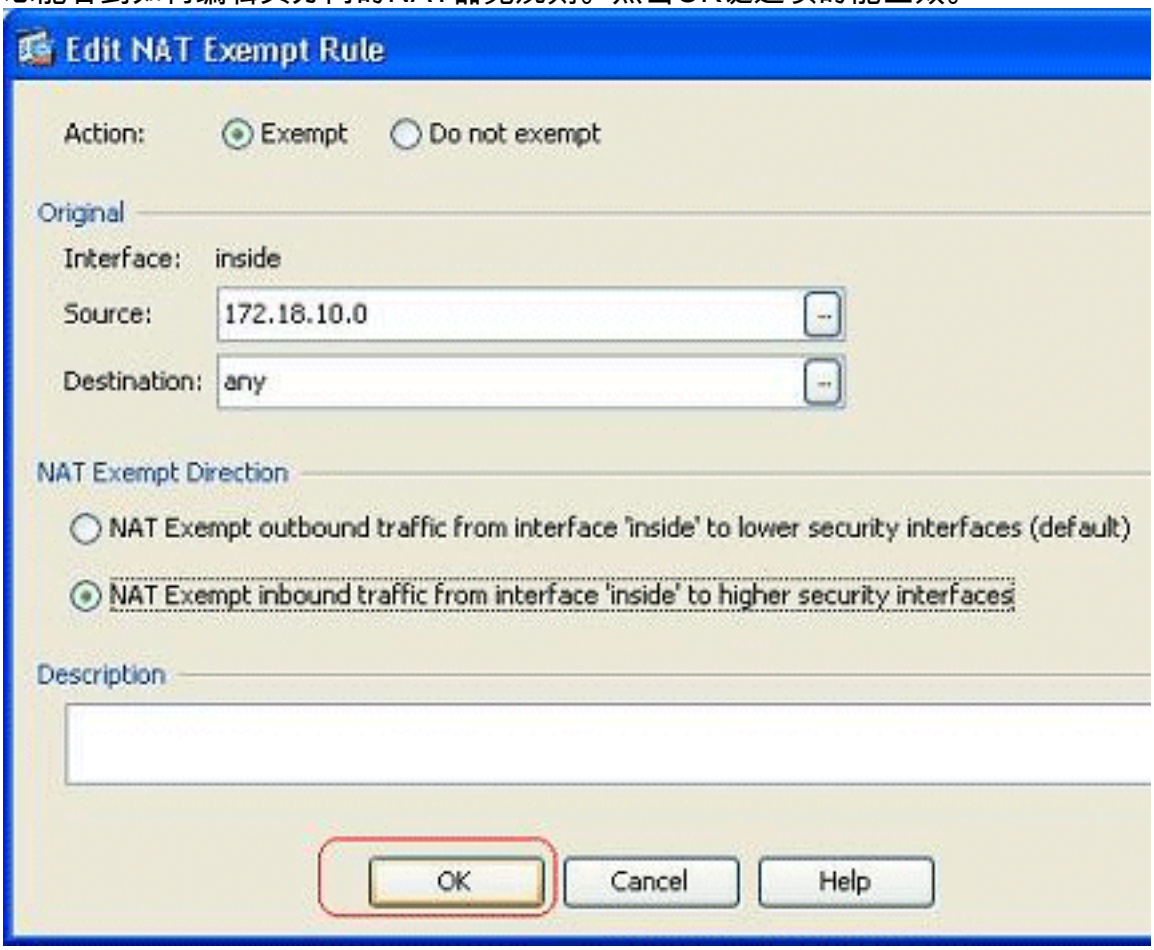


这是

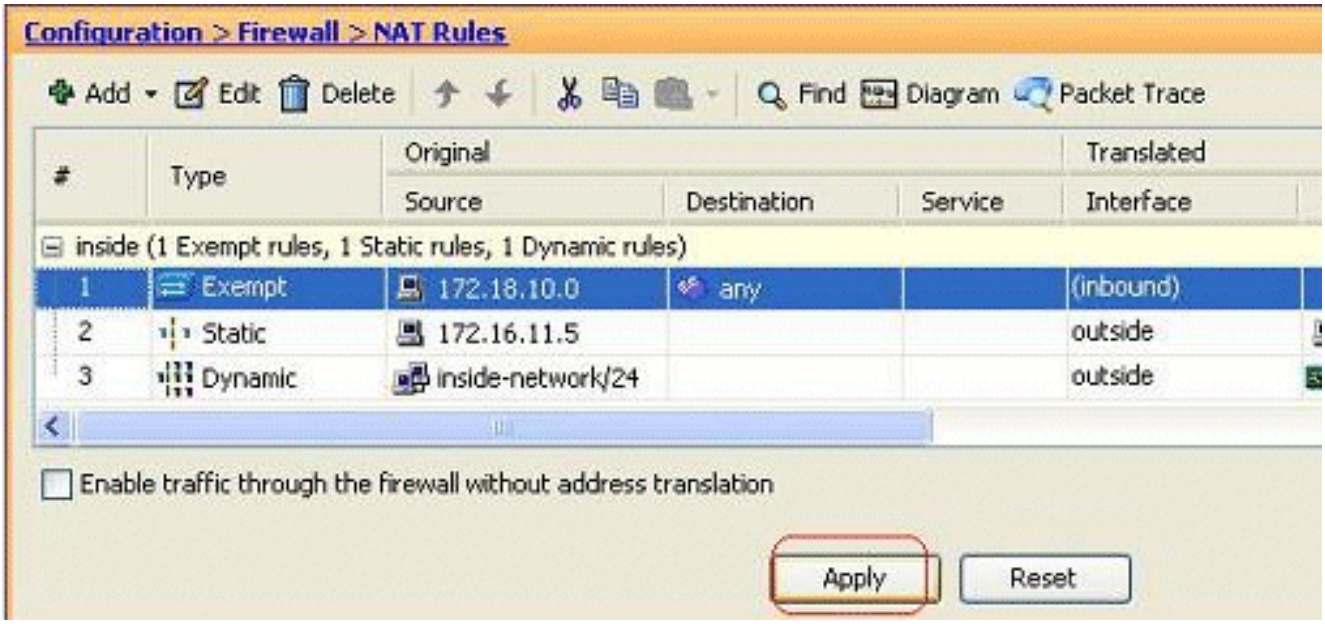
等同CLI输出供您的参考：

```
access-list inside_nat0_outbound extended permit ip host
172.18.10.0 any
!
nat (inside) 0 access-list inside_nat0_outbound
```

4. 您能看到如何编辑其方向的NAT豁免规则。点击OK键选项的能生效。



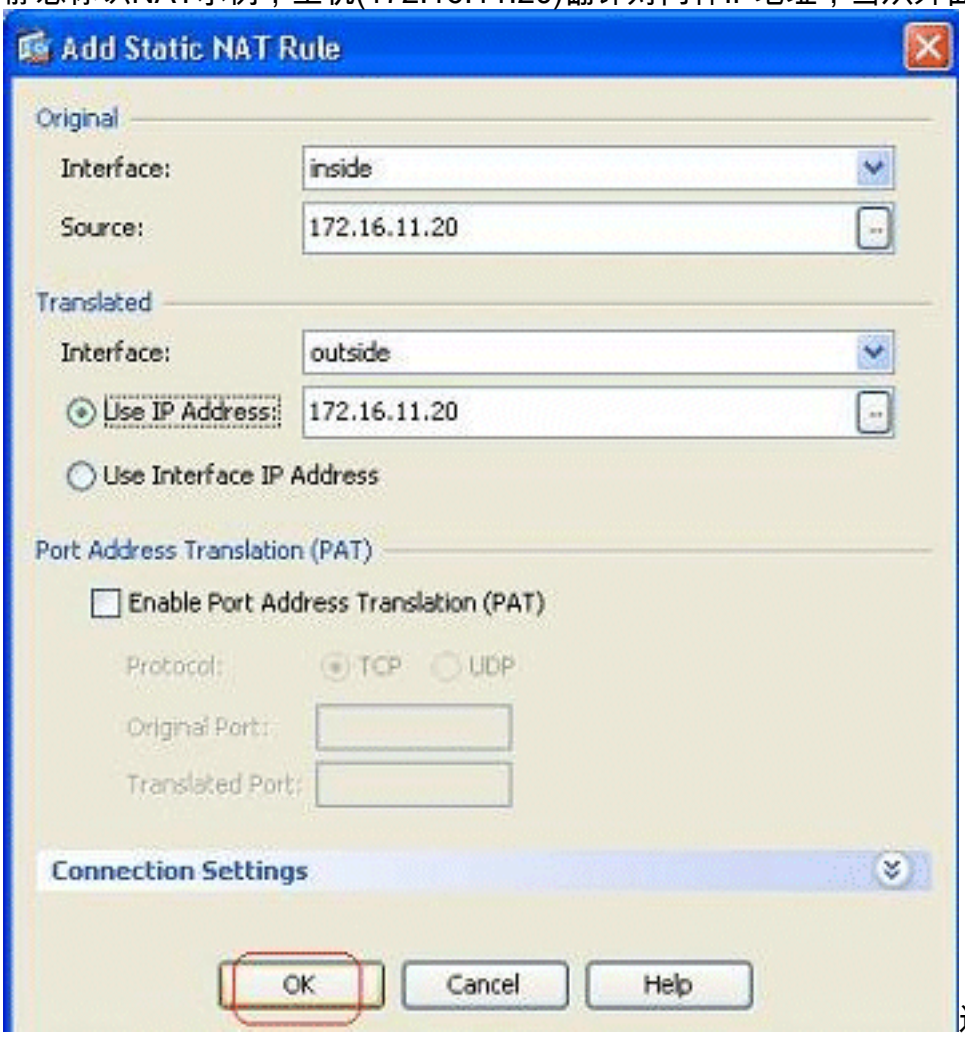
5. 您能当前看到方向更改对*入站*。



单击**应用**为了发送输出的此CLI到ASA ：`access-list inside_nat0_outbound extended permit ip host 172.18.10.0 any`
`!`

`nat (inside) 0 access-list inside_nat0_outbound` **`outside`** **注意：** 从此，您能看到一个新的关键字(从外部)被添加结束**nat 0命令**。此功能呼叫**外部NAT**。

6. 对禁用NAT的另一个方式是通过标识NAT的实施。标识NAT翻译主机对同样IP地址。这是正常静态标识NAT示例，主机(172.16.11.20)翻译对同样IP地址，当从外面时访问。



这是输出的等同CLI ：

```
! static (inside,outside) 172.16.11.20 172.16.11.20 netmask 255.255.255.255 !
```

使用 Static 命令进行端口重定向（转发）

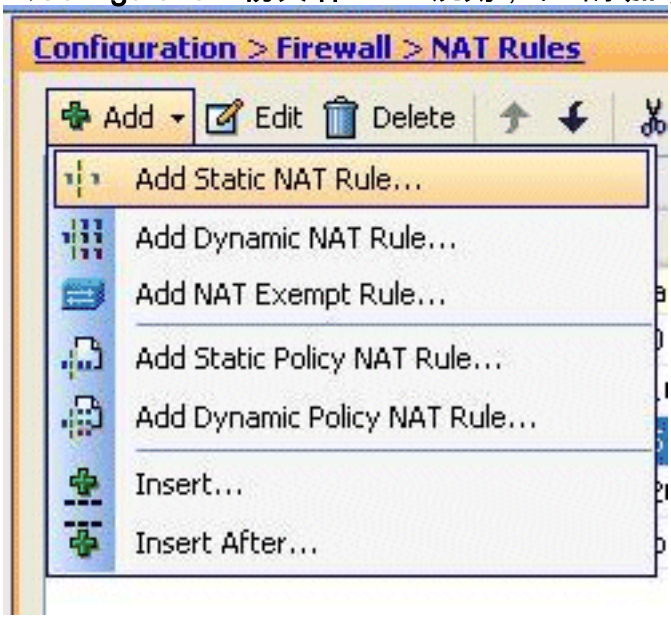
波尔特转发或端口重定向是外部用户设法访问在一个特定端口的一个内部服务器的有用的功能。为了达到此，内部服务器，有一个专用IP地址，将翻译对为特定端口反过来允许访问的公网IP地址。

在本例中，外部用户要在端口25访问SMTP服务器， 209.165.200.15。这在两个步骤完成：

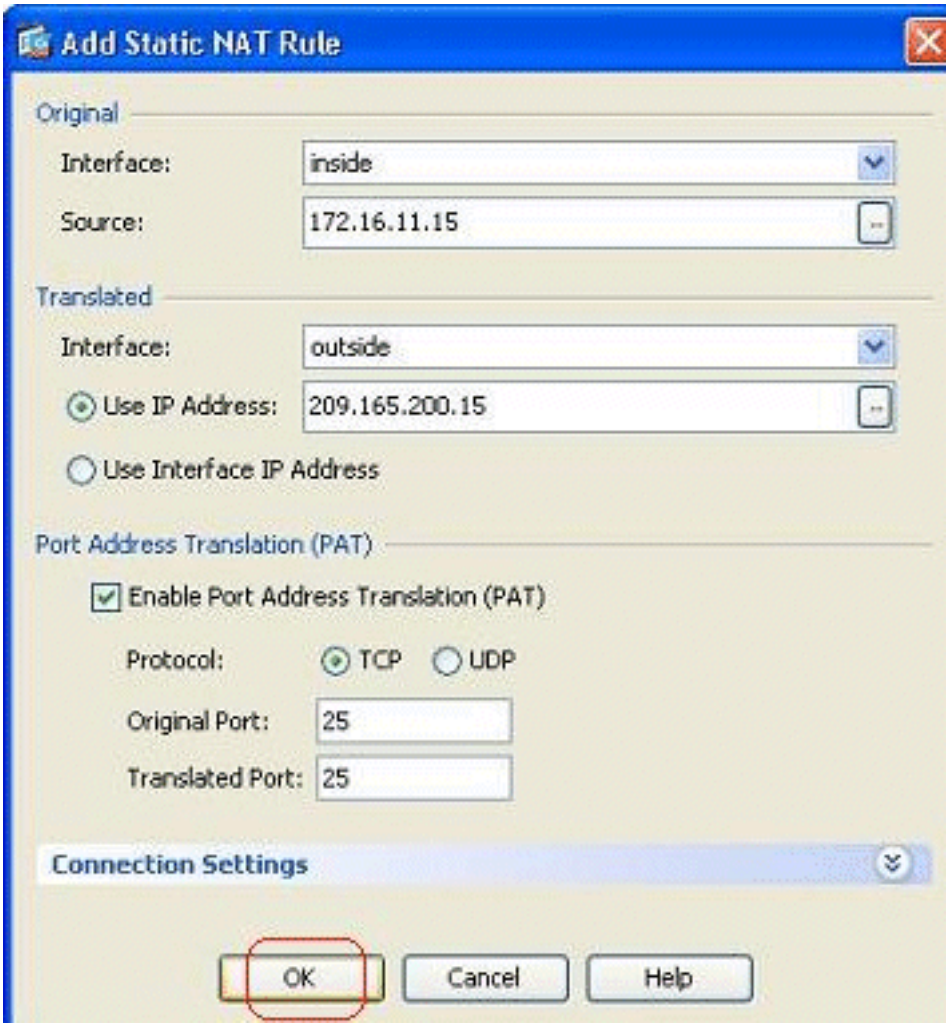
1. 翻译内部邮件服务器，在端口25的172.16.11.15，对公网IP地址， 209.165.200.15在端口25。
2. 对公共邮件服务器的允许，在端口25的209.165.200.15。

当外部用户设法访问服务器，在端口25的209.165.200.15，此流量将重定向到内部邮件服务器，172.16.11 15在端口25。

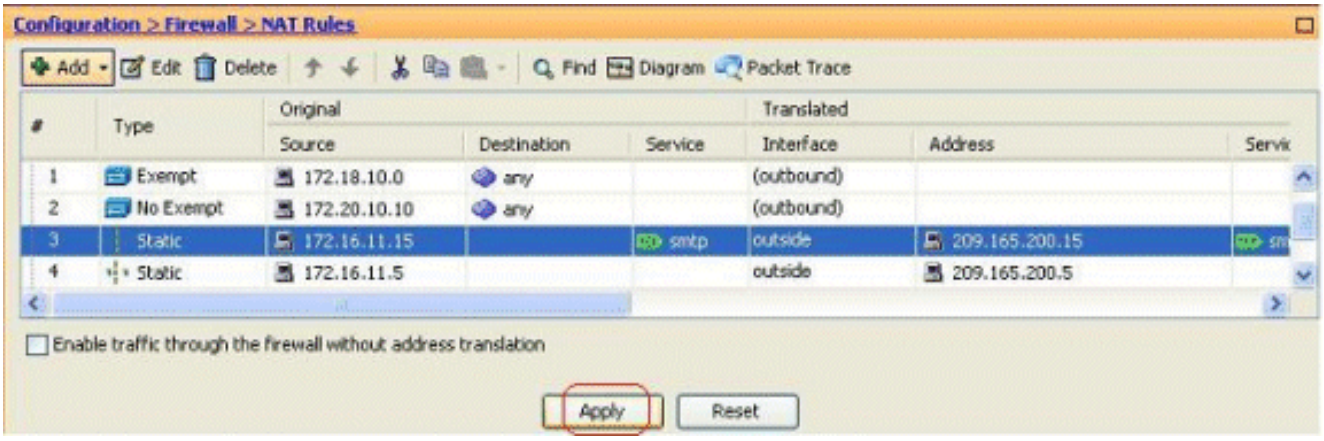
1. 去**Configuration>防火墙> NAT规则**，单击**添加**，并且选择**增加静态NAT规则**。



2. 与他们相关的接口一起指定初始源和转换后的IP地址。选择**Enable (event)端口地址转换(PAT)**，指定将重定向的端口，并且点击OK键。



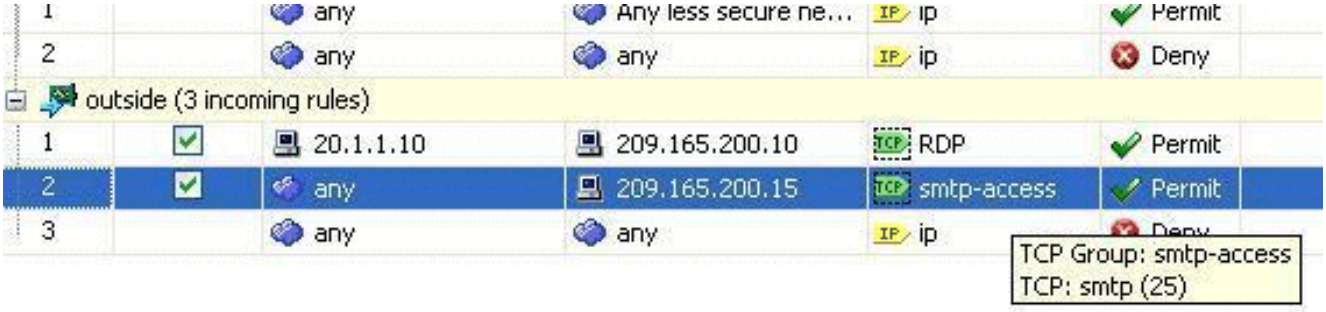
3. 已配置的静态PAT规则被看到此处
   ：



这是输出的等同CLI ：

```
! static (inside,outside) TCP 209.165.200.15 smtp 172.16.11.15 smtp netmask 255.255.255.255
!
```

4. 这是允许外部用户访问公共SMTP服务器在209.165.200.15的访问规则
   ：



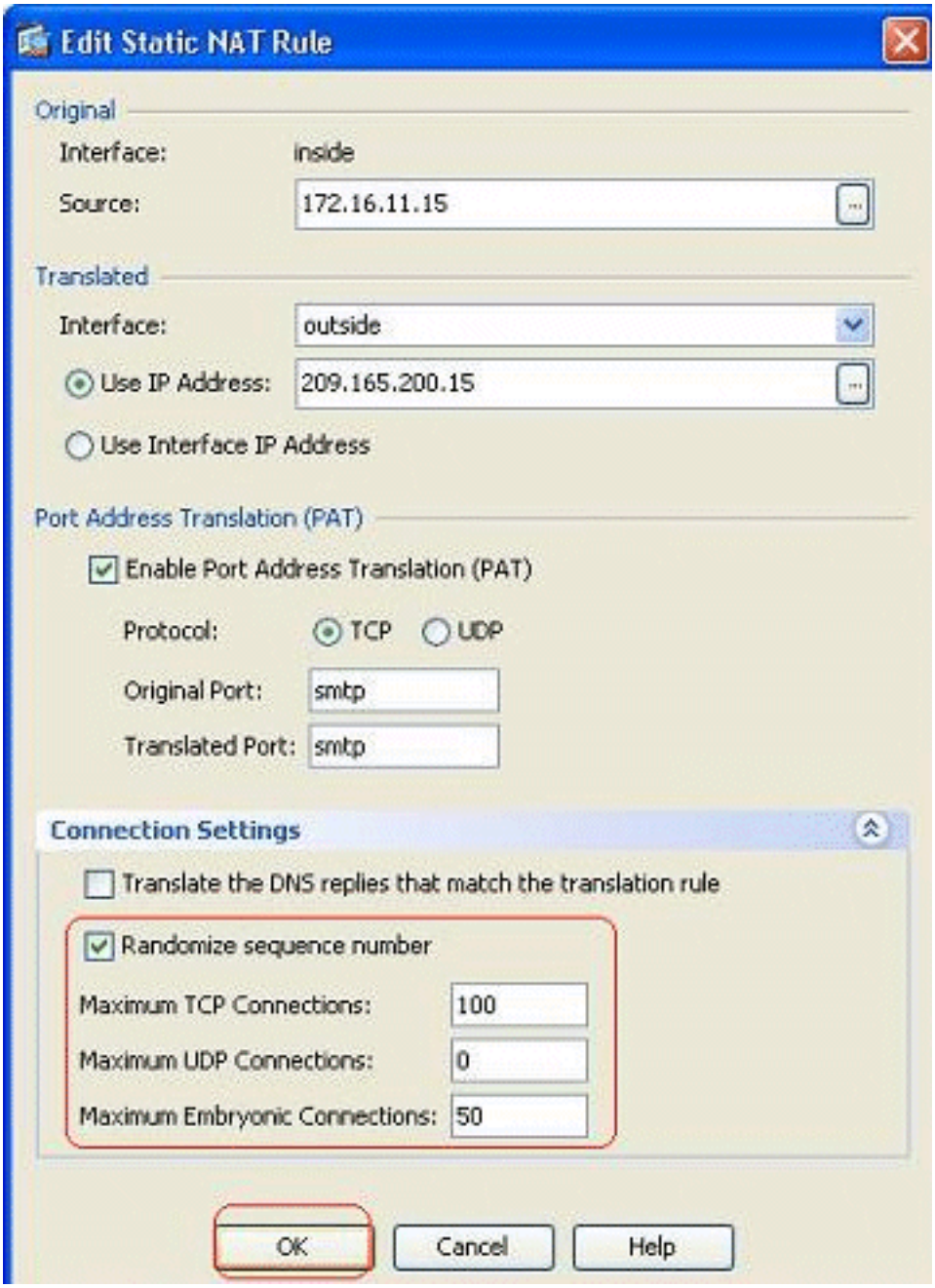
注意： 确保使用特定主机而不是使用**所有**关键字在访问规则的来源。

使用 Static 命令限制 TCP/UDP 会话

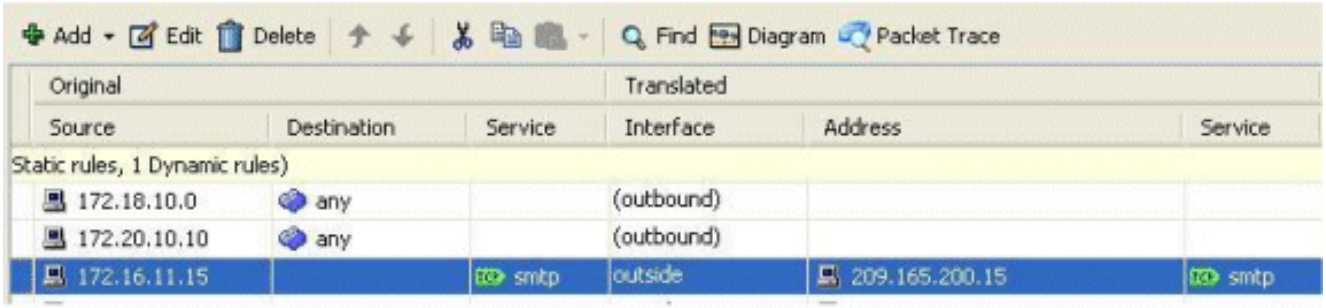
通过使用静态规则，您能指定TCP/UDP连接最大。您能也指定初期连接最大。初期连接是一半打开状态的连接。这些的大数将影响ASA的性能。限制这些连接将在某种程度上防止某些攻击类似DoS和SYN。对于完整缓解，您需要定义在MPF框架的策略，是超出本文的范围之外。关于此主题的更多信息，参考减轻网络攻击。

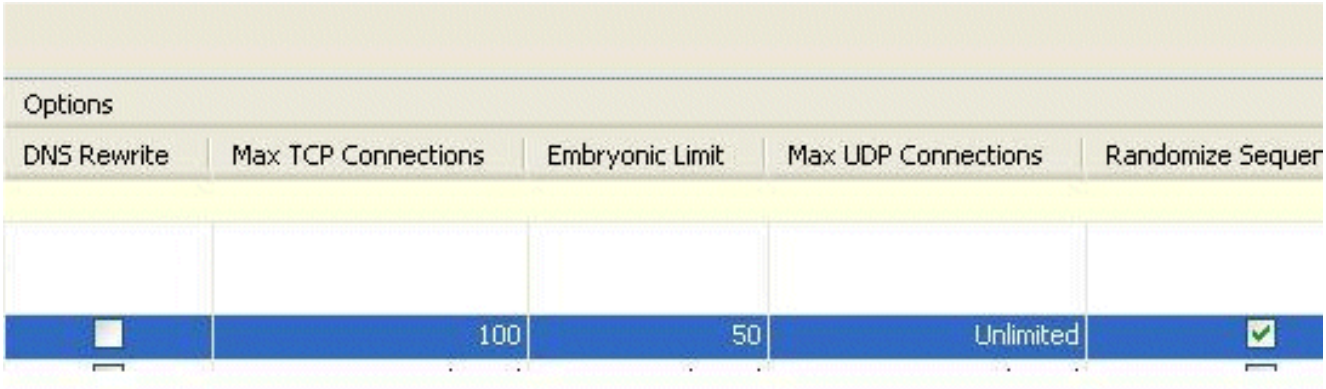
完成这些步骤：

1. 点击**连接设置**选项卡，并且指定最大连接的值此静态转换的。



2. 这些镜像显示此特定静态转换的连接限额
   :





这是输出的等同CLI ：！

```
static (inside,outside) TCP 209.165.200.15 smtp 172.16.11.15 smtp netmask 255.255.255.255
TCP 100 50 !
```

基于时间的访问列表

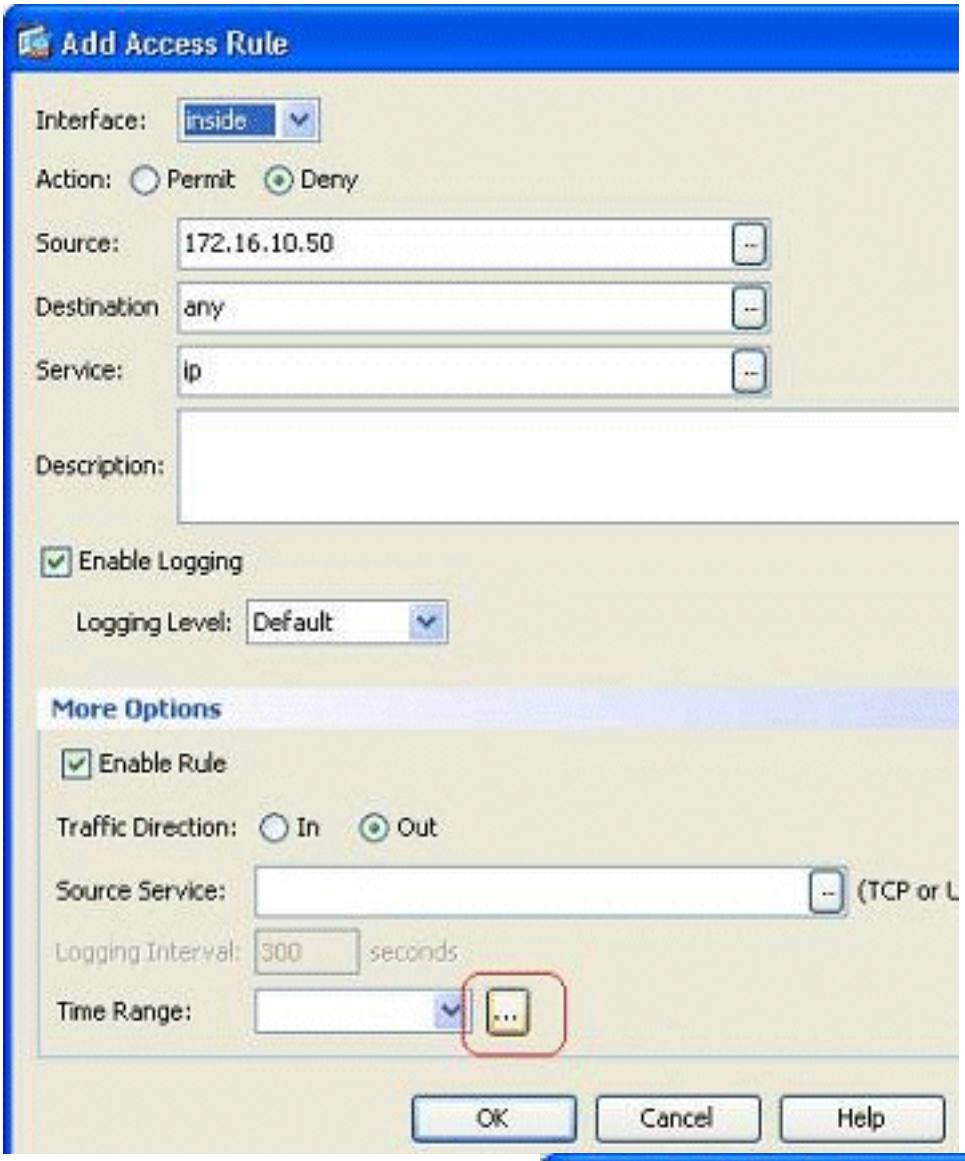
通过使用ASDM，此部分处理实现基于时间的访问列表。访问规则可以应用准时根据。为了实现此，在天/周/月/年之前指定定时的您需要定义time-range。然后，您需要绑定此time-range到需要的访问规则。Time-range可以定义用两种方式：

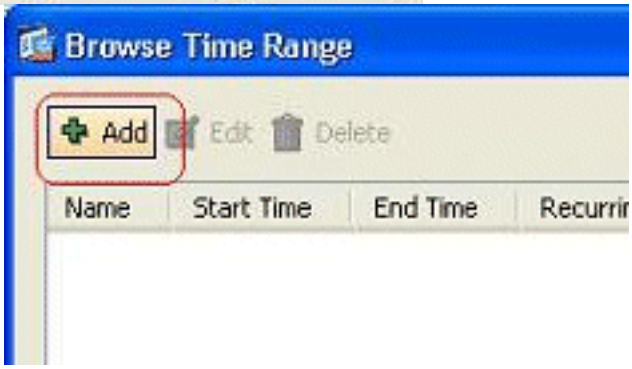
1. 绝对-定义了与开始时间和结束时间的一个时间。
2. 定期-亦称复发。定义了发生在指定的时间间隔的时间。

注意： 在您配置time-range前，请确保ASA配置与正确日期/时间设置，当此功能使用系统时钟设置实现。有与Ntp server同步的ASA将产生好结果。

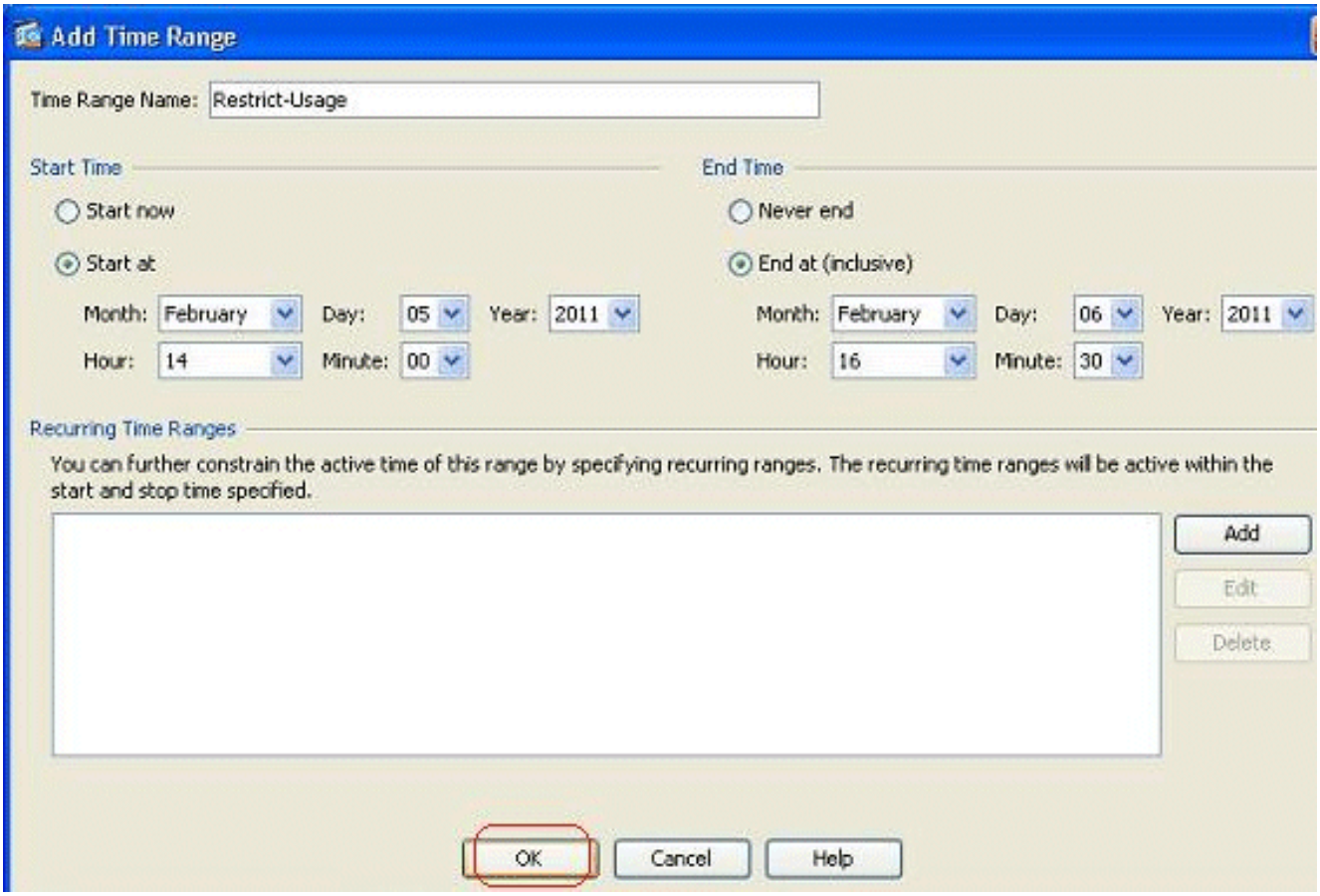
完成这些步骤为了通过ASDM配置此功能：

1. 当定义访问规则时，请在时间范围字段点击**详细信息按钮**。

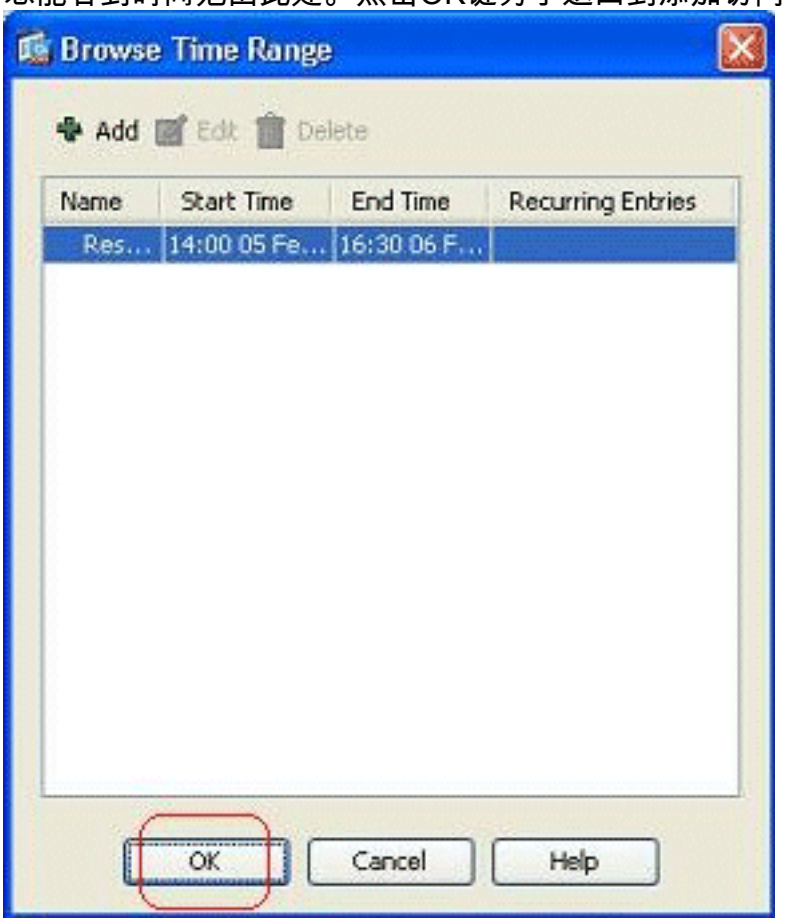




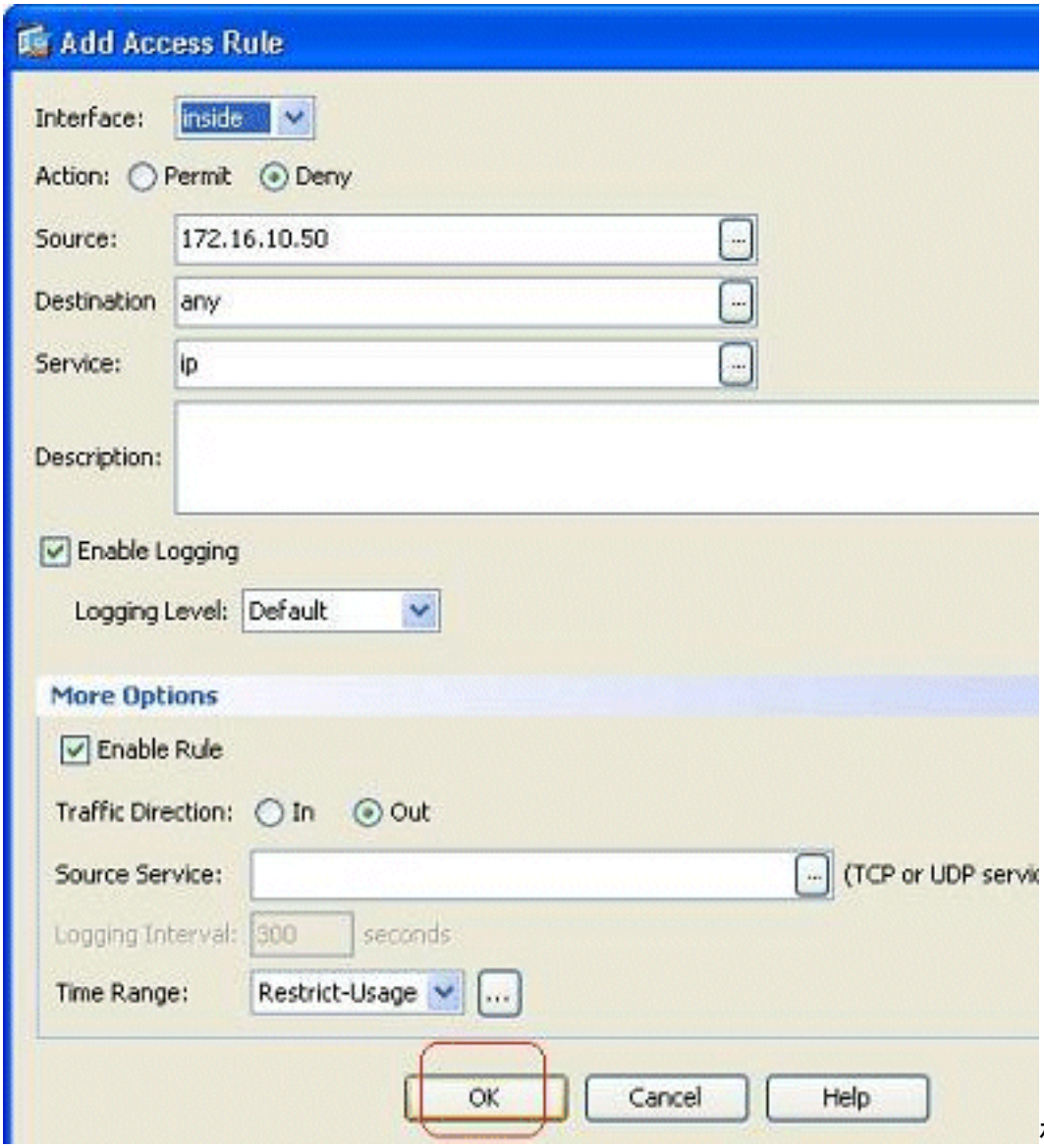
2. 单击**添加**为了创建一新的time-range。
3. 定义时间范围的名称，并且指定开始时间和结束时间。单击 **Ok**。



4. 您能看到时间范围此处。点击OK键为了返回到添加访问规则窗口。



5. 您能当前看到限制使用情况时间范围一定对此访问规则。

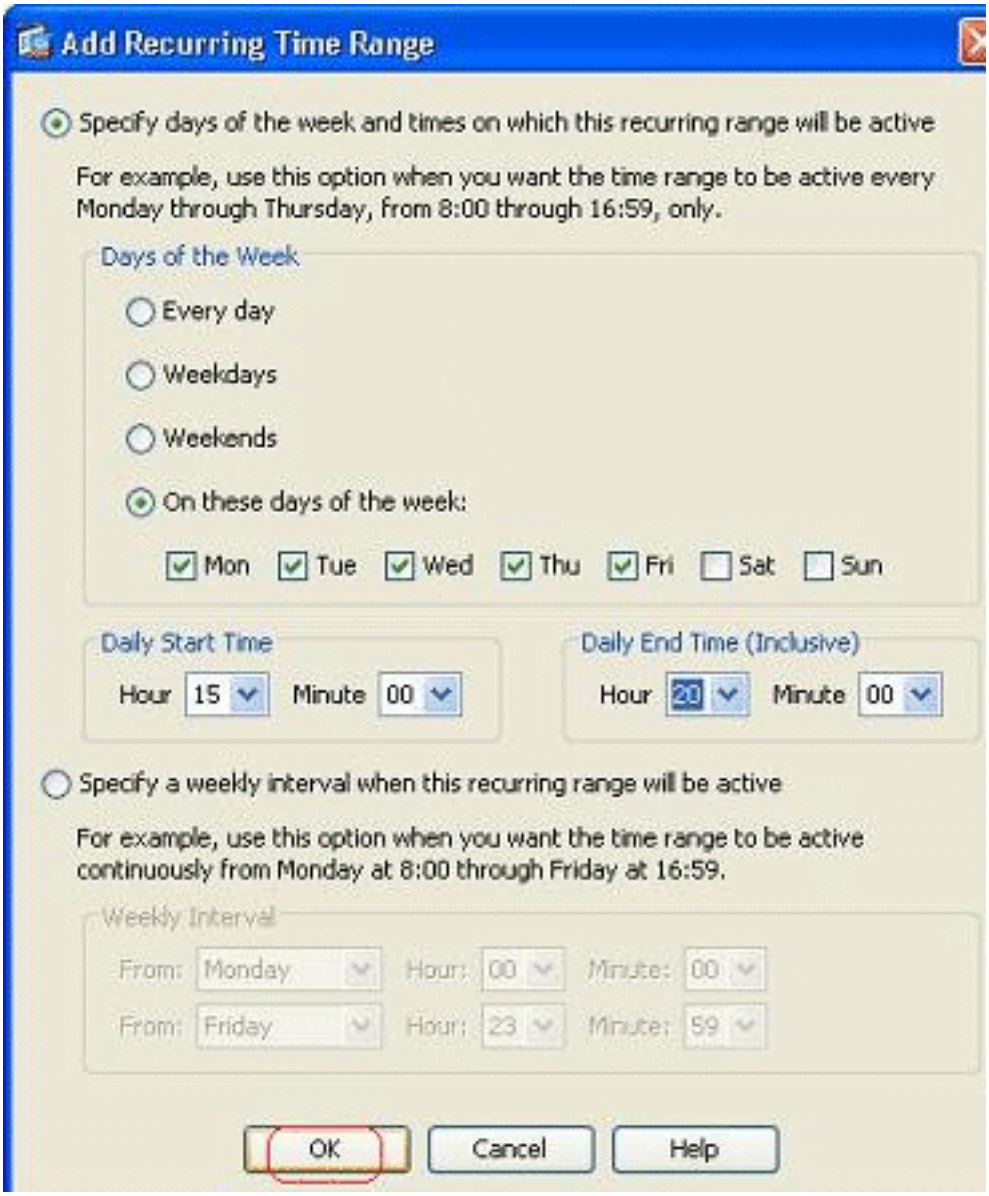


根据此访问规则配置，172.16.10.50的用户从使用所有资源限制从05/Feb/2011下午2点到06/Feb/2011 4.30 PM。这是输出的等同CLI ：

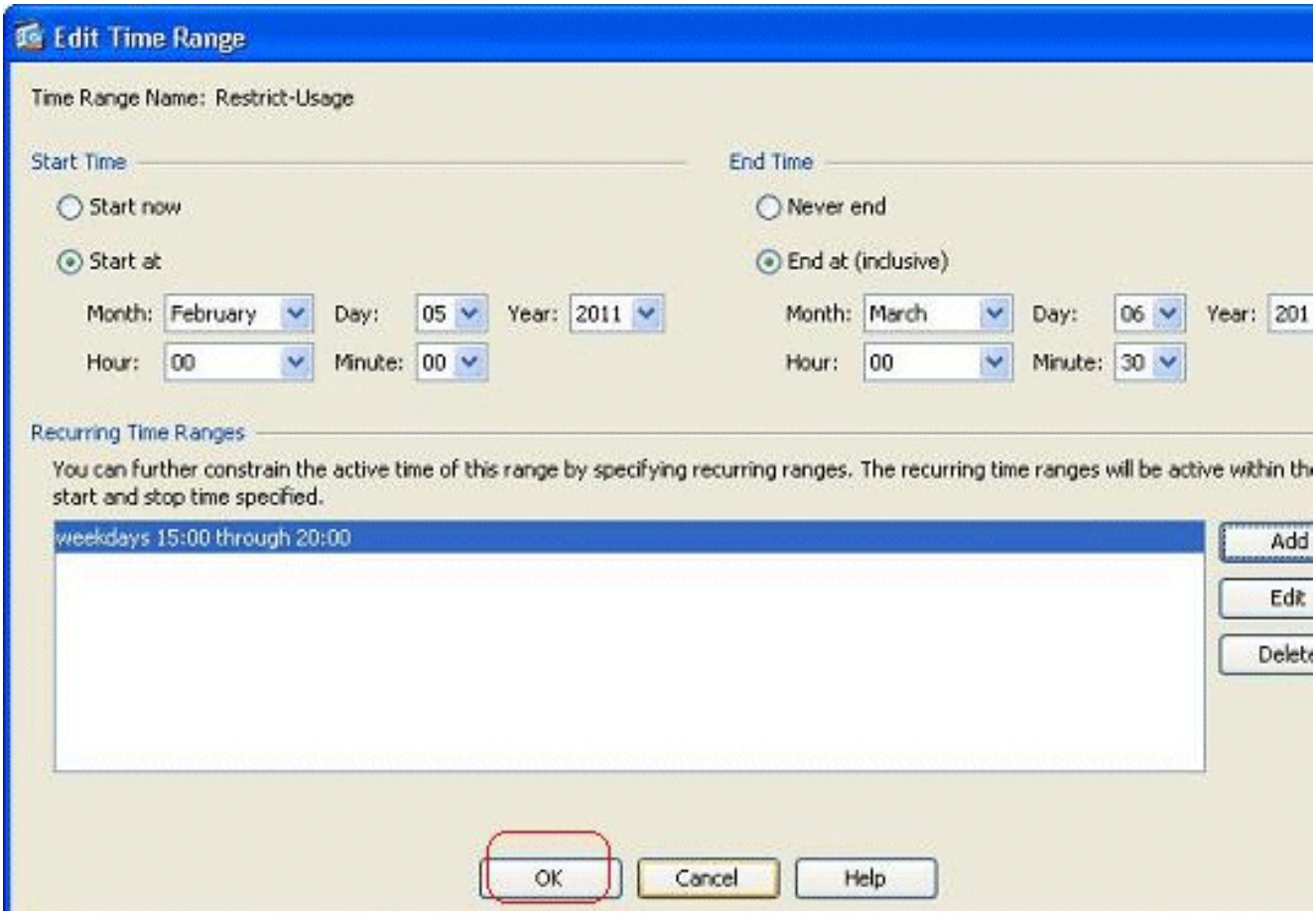
```
time-range Restrict-Usage absolute start 14:00 05 February 2011 end 16:30 06 February 2011
! access-list inside_access_out extended deny ip host 172.16.10.50 any time-range Restrict-
Usage ! access-group inside_access_out in interface inside
```

6. 这是关于怎样的一示例指定循环时间范围。单击**添加**为了定义循环时间范围。

7. 指定根据您的需求的设置，并且点击OK键为了完成。



8. 点击OK键为了返回返回时间范围窗口。



根据此配置， 172.16.10.50的用户是拒绝访问对从下午3点的所有资源到在所有工作日的下午8点除了星期六和星期日。

```
! time-range Restrict-Usage absolute start 00:00 05 February 2011 end 00:30 06 March 2011
periodic weekdays 15:00 to 20:00 ! access-list inside_access_out extended deny ip host
172.16.10.50 any time-range Restrict-Usage ! access-group inside_access_out in interface
inside
```

注意： 如果**time-range命令**有指定的绝对和定期值，则**定期**命令被评估，在绝对开始时间被到达之后，并且不进一步已评估，在绝对结束时间被到达后。

相关信息

- 思科ASA文档页
- 技术支持和文档 - Cisco Systems