ASA 7.x/PIX 6.x 及更高版本：打开或阻拦端口配置示例

目录

简介

本文档提供了一个示例配置，说明如何在安全设备中打开或阻塞各种类型的数据流（如 http 或 ftp）的端口。

注意：术语“打开端口”和“允许端口”具有相同含义。同样，“阻塞端口”和“限制端口”意思也相同。

先决条件

要求

本文档假设 PIX/ASA 已经过配置，且正常运行。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行版本8.2(1)的思科5500系列自适应安全设备(ASA)
- Cisco 自适应安全设备管理器 (ASDM) 版本 6.3(5)

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

此配置也可用于安装有软件版本 6.x 及更高版本的 Cisco 500 系列 PIX 防火墙设备。

规则

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

配置

每个接口必须具有从 0（最低）到 100（最高）的安全等级。 例如，您必须将最安全的网络（如内部主机网络）分配到100级。虽然连接到Internet的外部网络可以是0级，但其他网络（如DMZ）可以位于两者之间。您可以将多个接口分配到同一安全等级。

默认情况下，将阻塞外部接口（安全等级为 0）上的所有端口，并打开安全设备内部接口（安全等级为 100）上的所有端口。这样，所有出站数据流都可以在不需要任何配置的情况下通过安全设备，但入站数据流可以通过配置访问列表和安全设备中的 static 命令允许。

注：通常，所有端口都会从低安全区阻塞到高安全区，并且所有端口都会从高安全区打开到低安全区，前提是已为入站和出站流量启用状态检测。

本部分包含如下所示的子部分：

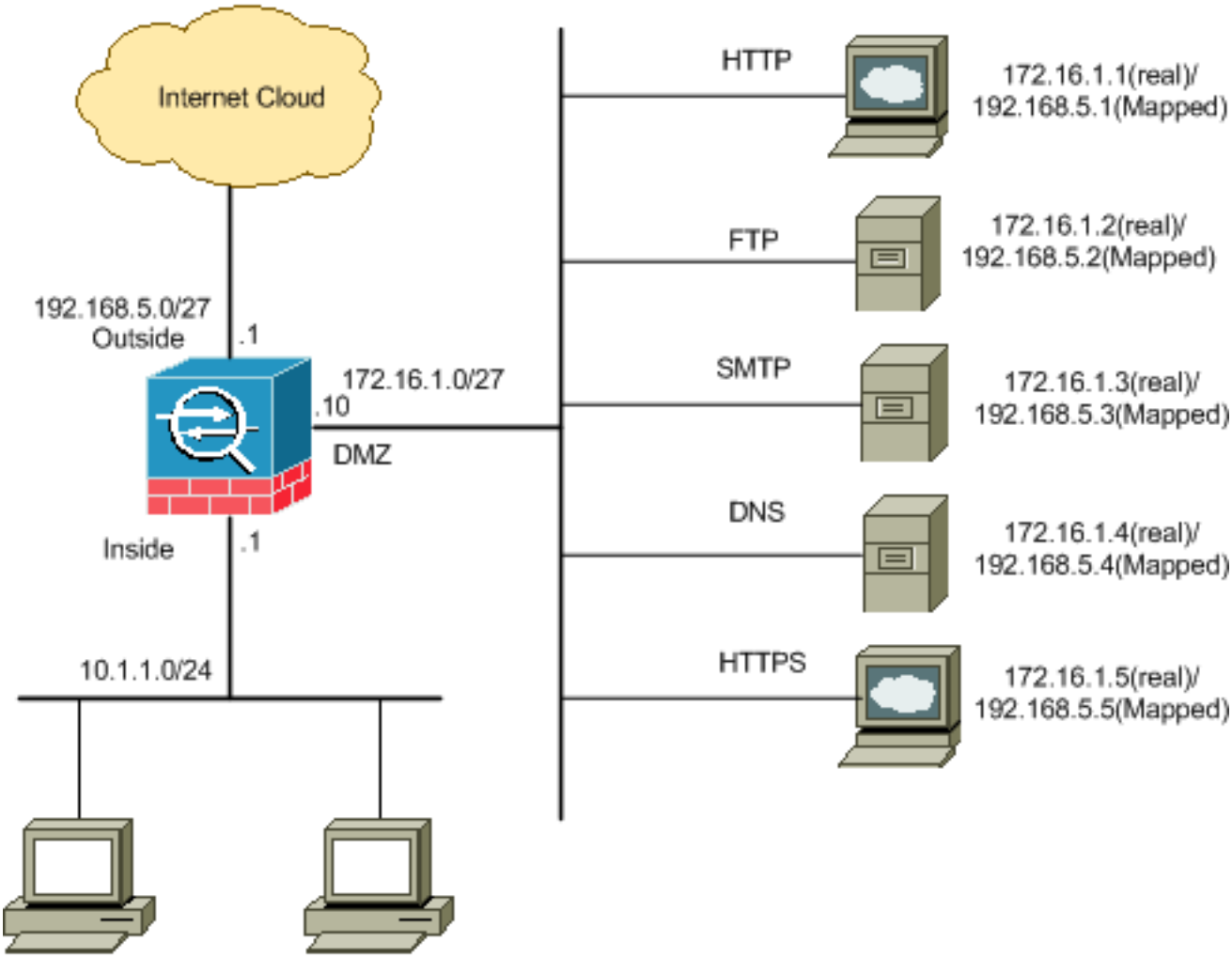
- 网络图
- 阻塞端口配置
- 打开端口配置

本部分提供有关如何配置本文档所述功能的信息。

注意：使用命令查找工具(仅限注册客户)可获取有关本节中使用的命令的详细信息。

网络图

本文档使用以下网络设置：



阻塞端口配置

除非扩展访问列表已明确阻塞，否则安全设备将允许任何出站数据流。

访问列表由一个或多个访问控制条目构成。根据访问列表类型，您可以指定源和目标地址、协议、端口（对于 TCP 或 UDP）、ICMP 类型（对于 ICMP）或 EtherType。

注：对于无连接协议（如ICMP），安全设备会建立单向会话，因此，您需要访问列表以允许双向 ICMP（通过将访问列表应用到源接口和目标接口），或者需要启用ICMP检测引擎。ICMP 检测引擎将 ICMP 会话视为双向连接。

要阻塞端口，请完成以下步骤，这通常适用于从内部（安全性较高的区域）到 DMZ（安全性较低的区域）或从 DMZ 到外部的数据流。

1. 创建一个用于阻塞指定端口数据流的访问控制列表。

   ```
   access-list
   ```

2. 然后使用 access-group **命令绑定该访问列表以激活它。**

   ```
   access-group
   ```

示例：

1. **阻塞 HTTP 端口数据流：**要阻止内部网络 10.1.1.0 访问 DMZ 网络中具有 IP 172.16.1.1 的 http（Web 服务器），请创建如下所示的 ACL：

```
ciscoasa(config)#access-list 100 extended deny tcp 10.1.1.0 255.255.255.0
   host 172.16.1.1  eq 80
ciscoasa(config)#access-list 100 extended permit ip any any
ciscoasa(config)#access-group 100 in interface inside
```

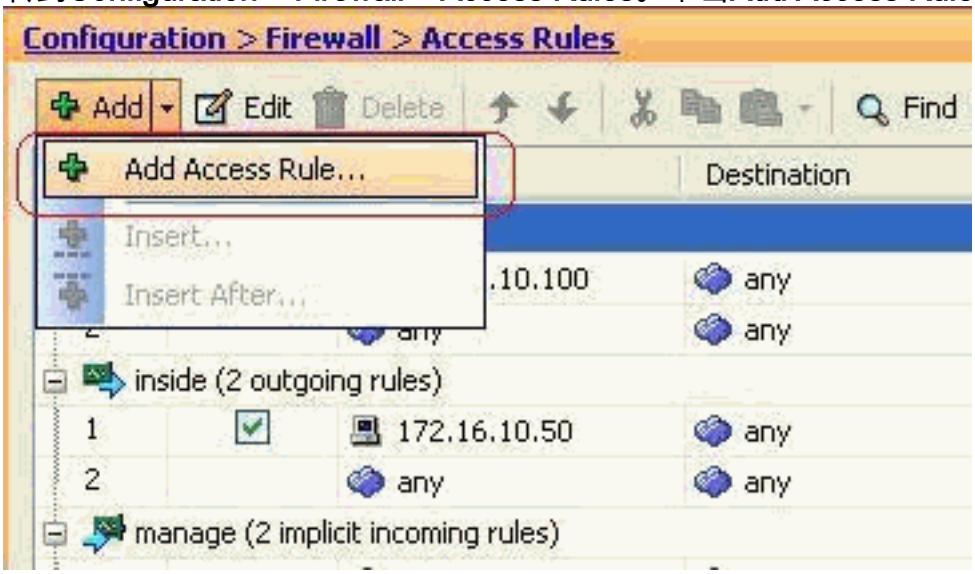
   注意：使用no后跟access list命令以删除端口阻塞。
2. **阻塞 FTP 端口数据流：**要阻止内部网络 10.1.1.0 访问 DMZ 网络中具有 IP 172.16.1.2 的 FTP（文件服务器），请创建如下所示的 ACL：

```
ciscoasa(config)#access-list 100 extended deny tcp 10.1.1.0 255.255.255.0
   host 172.16.1.2  eq 21
ciscoasa(config)#access-list 100 extended permit ip any any
ciscoasa(config)#access-group 100 in interface inside
```

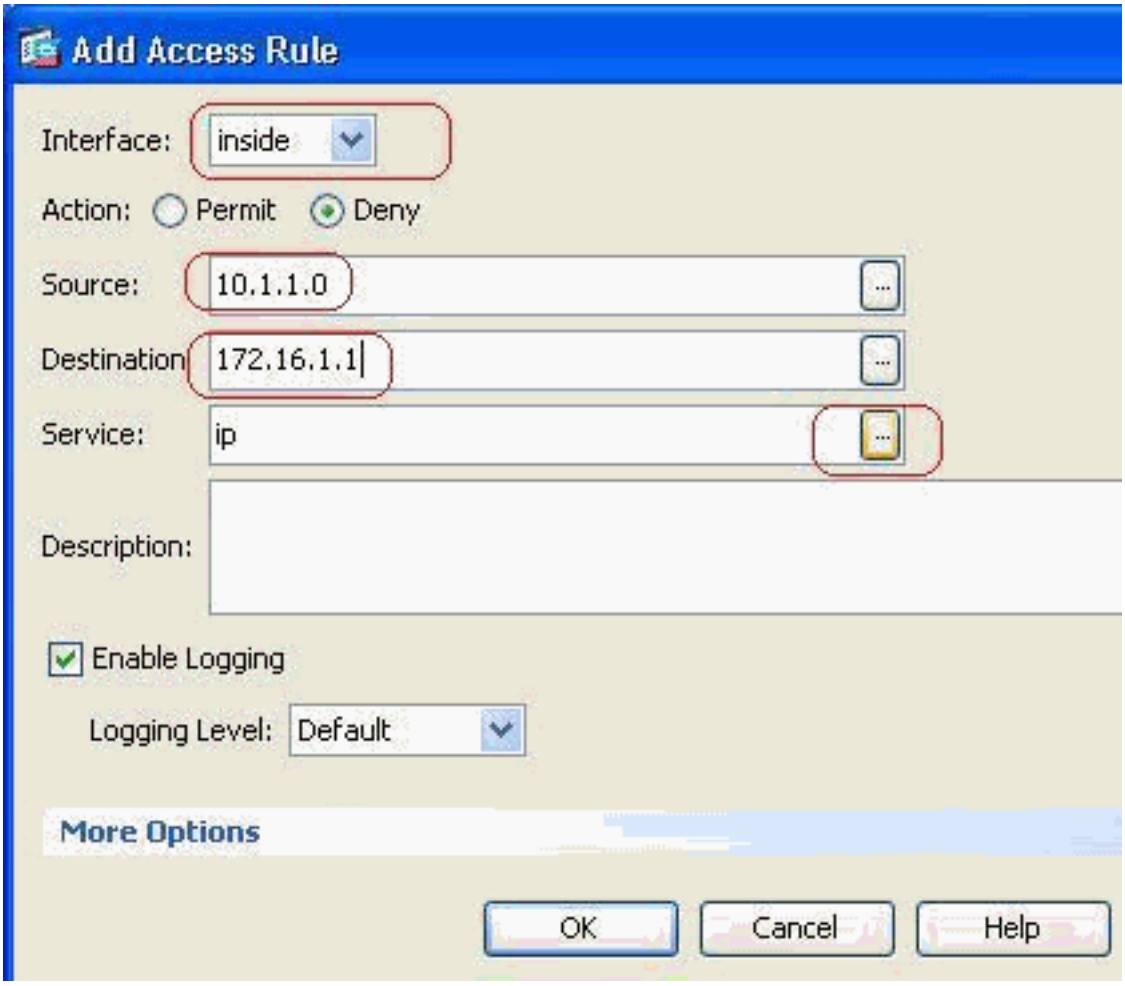
注意：要了解有关端口分配的详细信息，请参阅IANA端口。

本部分显示了通过ASDM执行此操作的分步配置。

1. 转到Configuration > Firewall > Access Rules。单击Add Access Rule以创建访问列表。

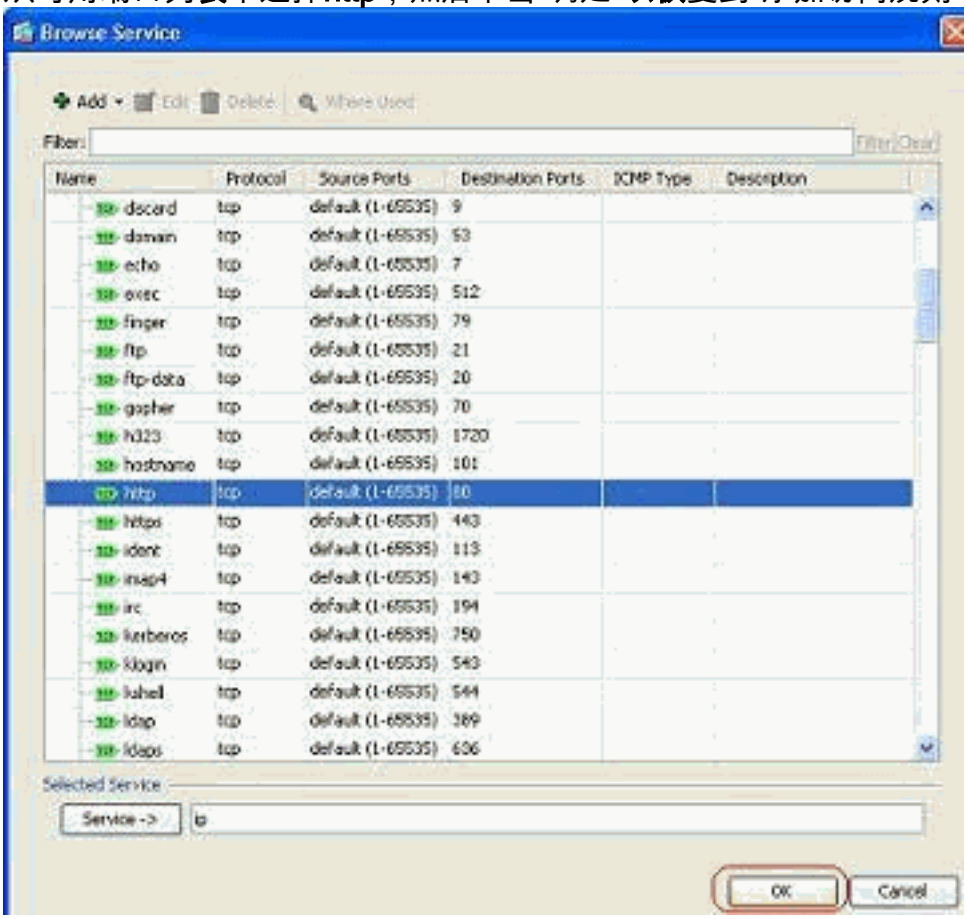


2. 定义源和目标以及访问规则的操作以及此访问规则将关联的接口。选择详细信息以选择要阻止

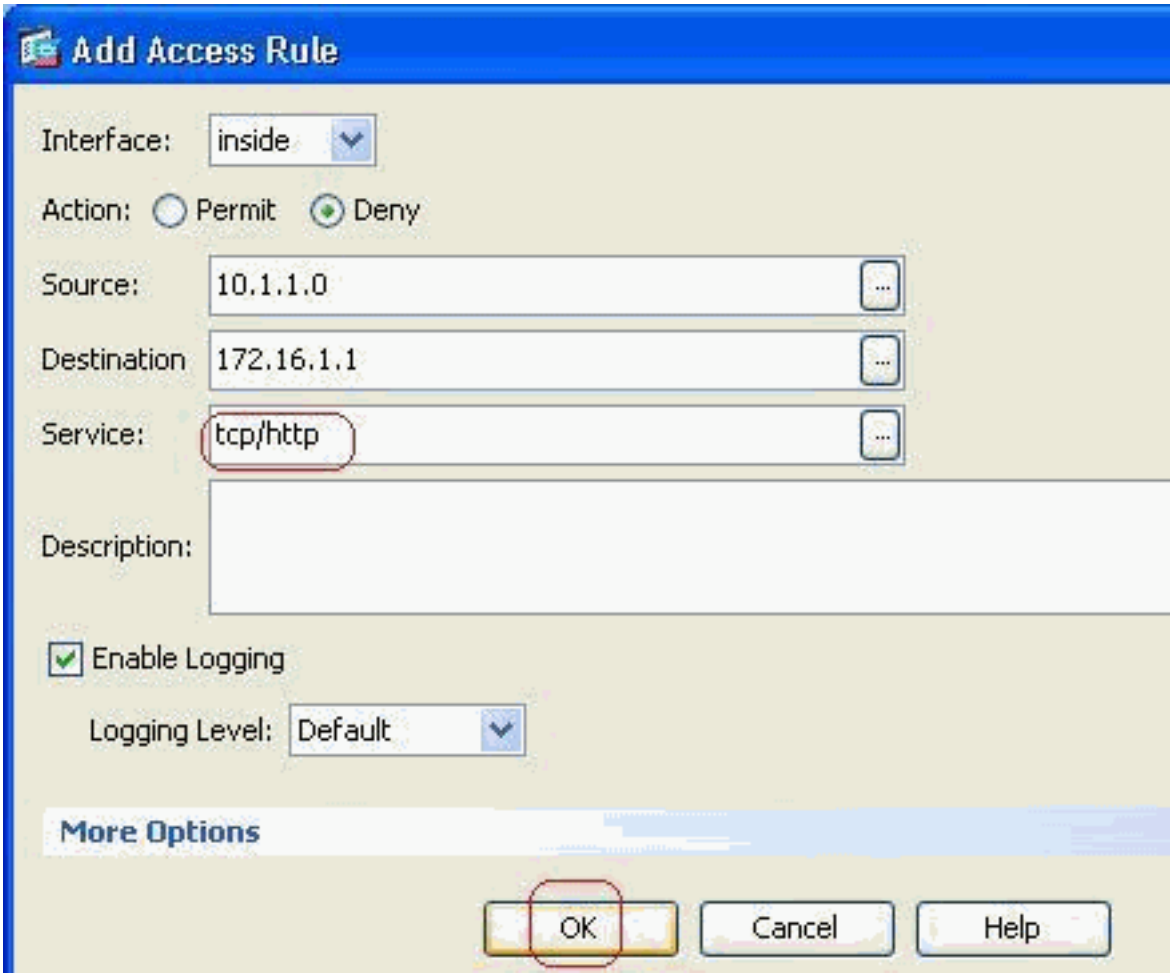


的特定端口。

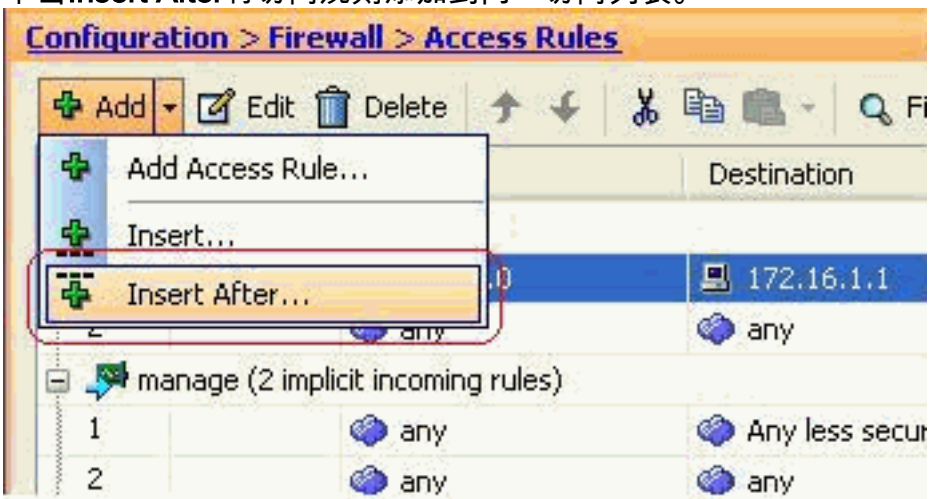
3. 从可用端口列表中选择http，然后单击“确定”以恢复到“添加访问规则”窗口。



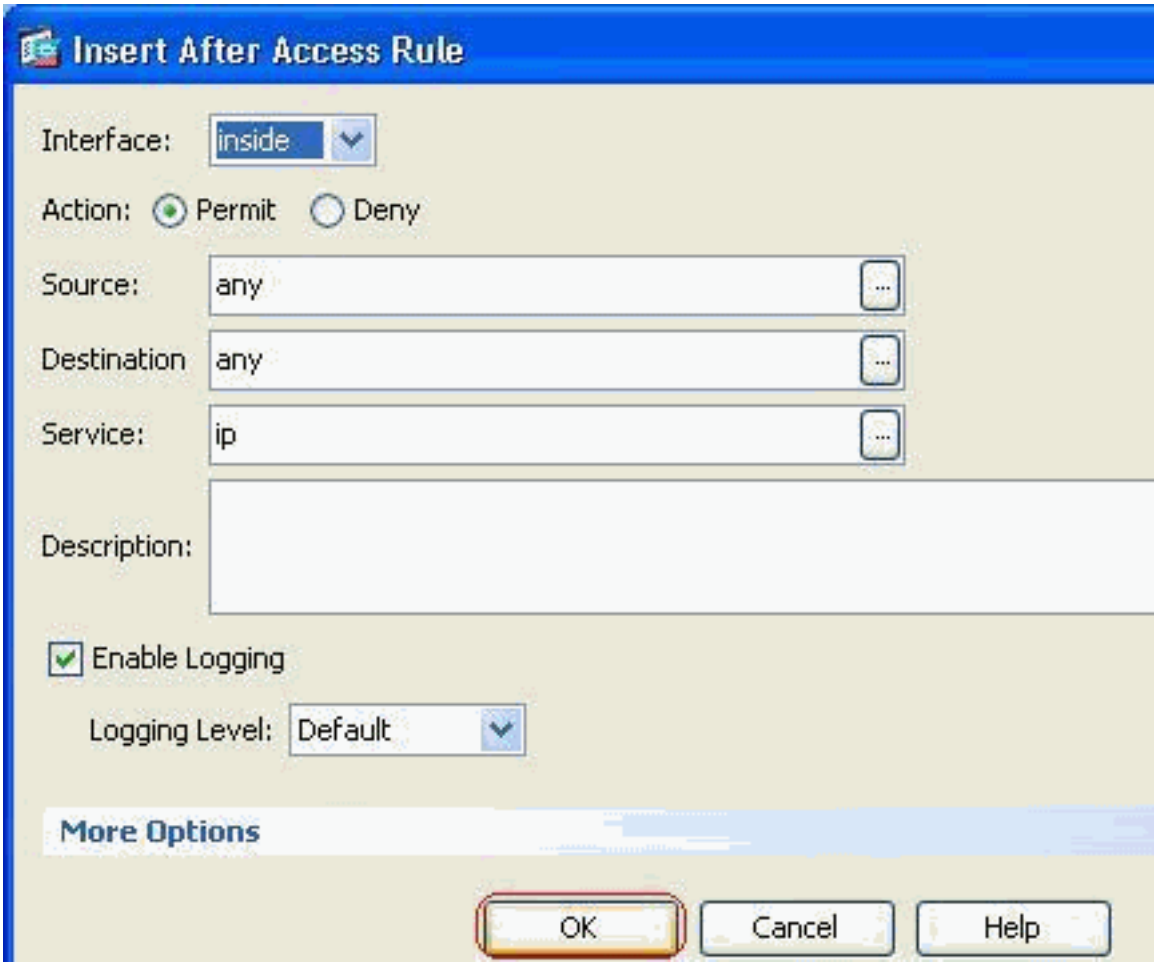
4. 单击OK完成访问规则的配置。



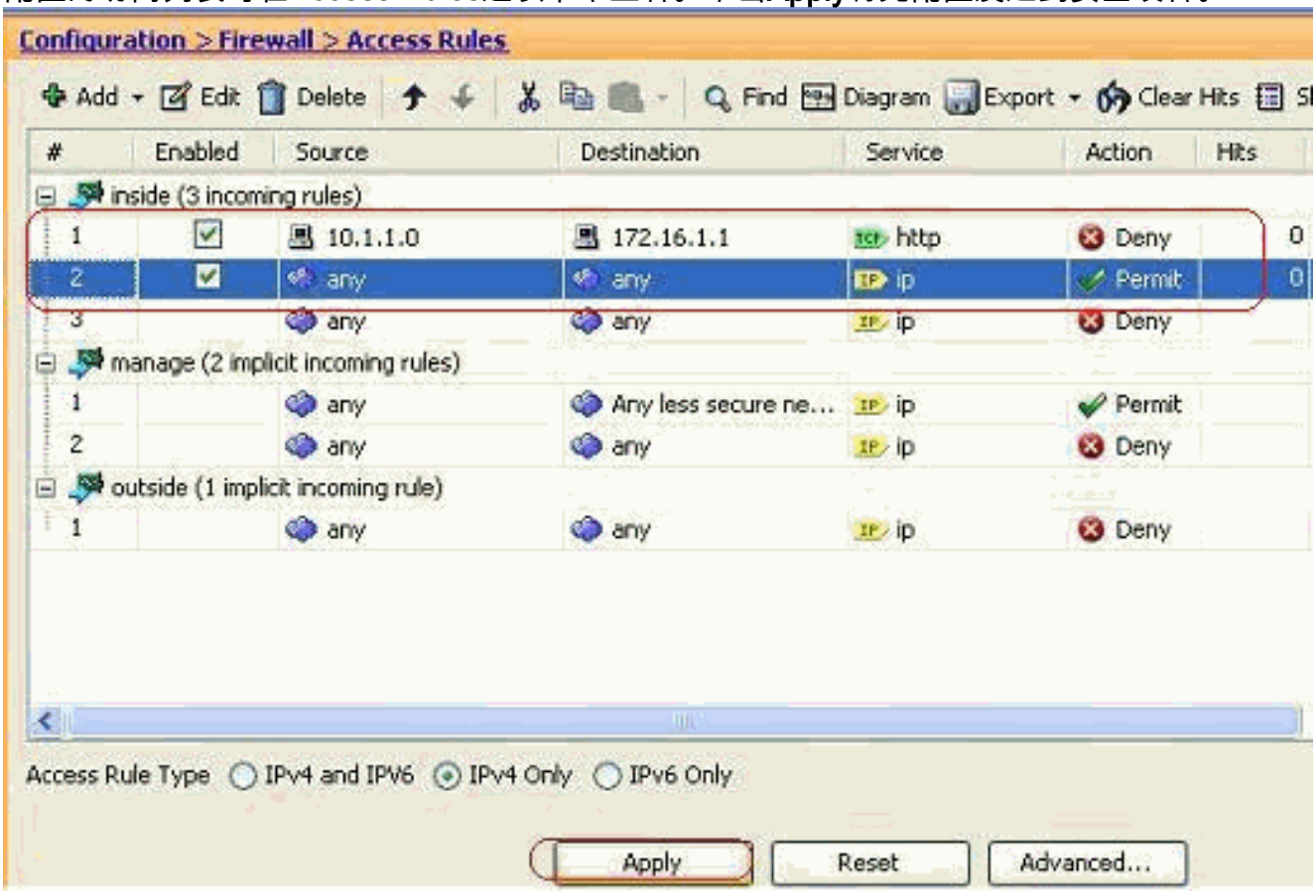
5. 单击**Insert After**将访问规则添加到同一访问列表。



6. 允许流量从“any”到“any”，以防止“隐式拒绝”。 然后，单击**OK**完成添加此访问规则。



7. 配置的访问列表可在Access Rules选项卡中查看。单击**Apply**将此配置发送到安全设备。



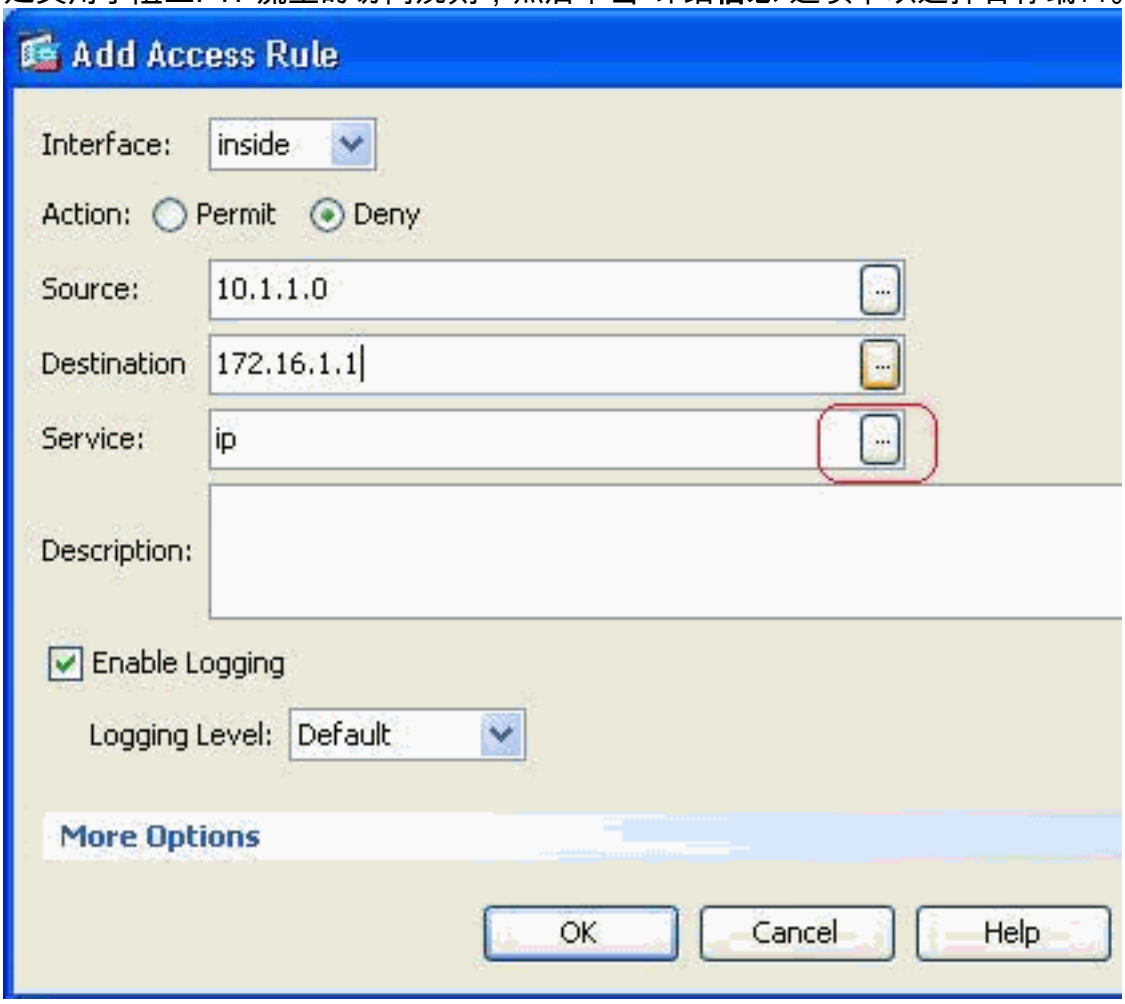
从ASDM发送的配置会在ASA的命令行界面(CLI)上生成这组命令。

```
access-list inside_access_in extended deny tcp host 10.1.1.0 host 172.16.1.1 eq www
access-list inside_access_in extended permit ip any any
access-group inside_access_in in interface inside
```

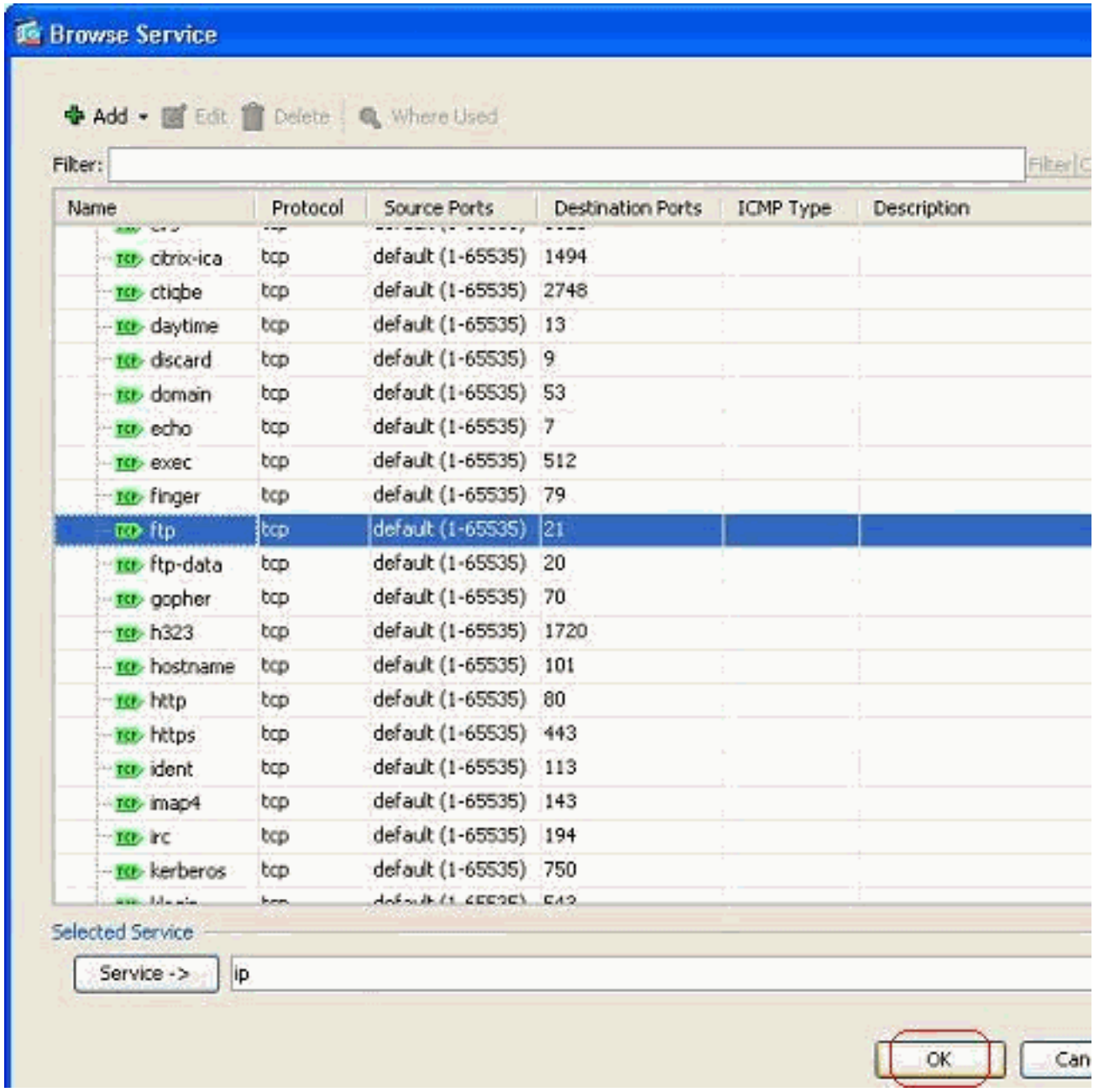
通过这些步骤，示例1通过ASDM阻止10.1.1.0网络访问Web服务器172.16.1.1。示例2也可以以同样的方式阻止整个10.1.1.0网络访问FTP服务器172.16.1.2。唯一的区别是在选择端口时。

注意：此访问规则配置（例如2）假设为新配置。

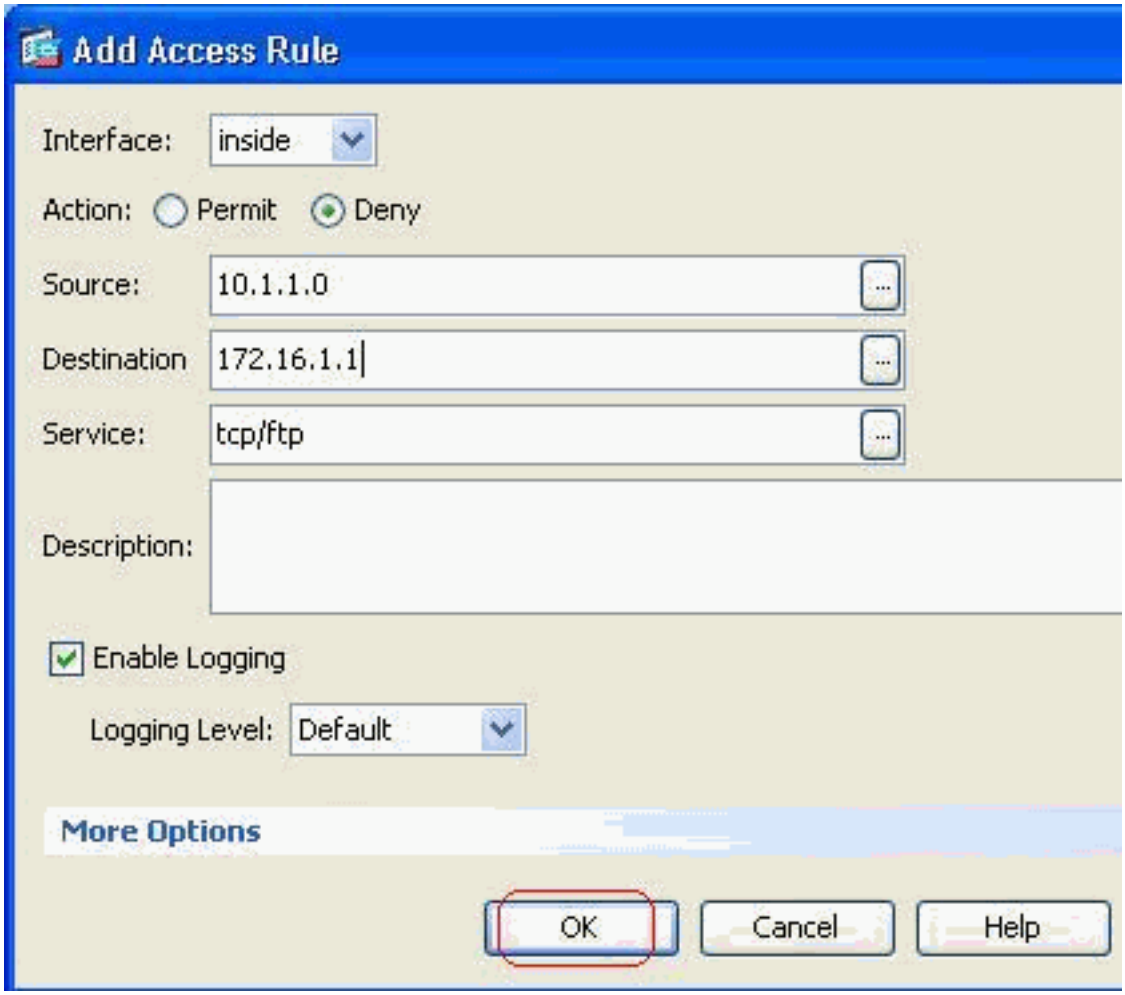
8. 定义用于阻止FTP流量的访问规则，然后单击“详细**信息**”选项卡以选择目标端口。



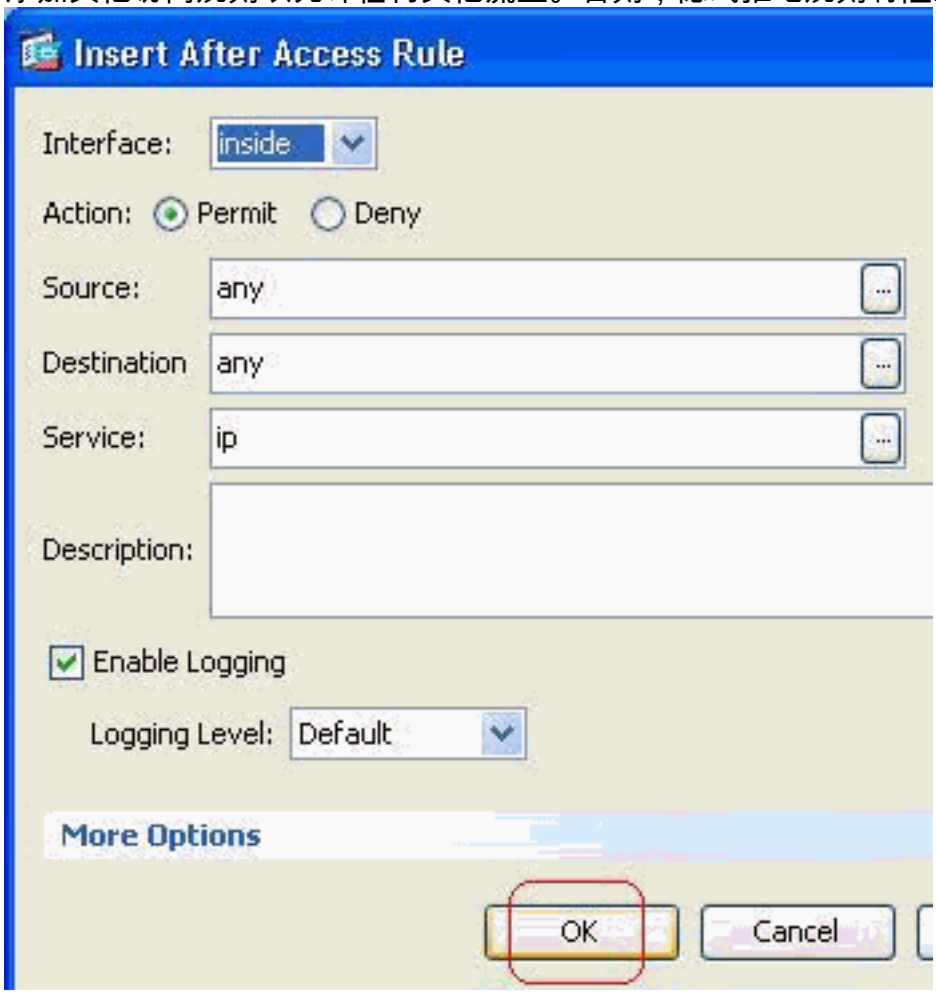
9. 选择ftp**端**口并单击**OK**以恢复到Add Access Rule窗口。



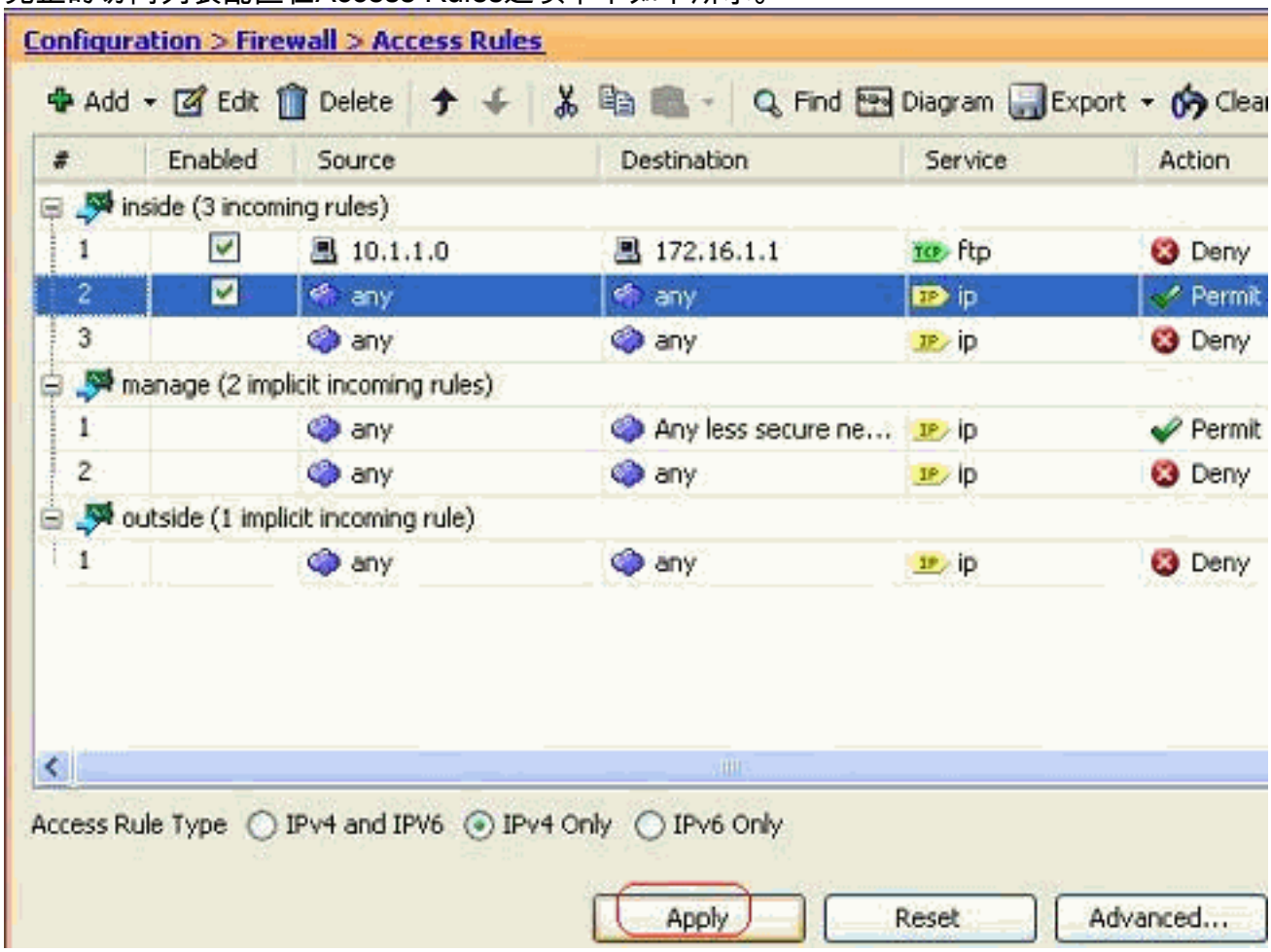
10. 单击**OK**完成访问规则的配置。



11. 添加其他访问规则以允许任何其他流量。否则，隐式拒绝规则将阻止此接口上的所有流量。



12. 完整的访问列表配置在Access Rules选项卡下如下所示。



13. 单击Apply将配置发送到ASA。等效的CLI配置如下所示：

```
access-list inside_access_in extended deny tcp host 10.1.1.0 host 172.16.1.1 eq ftp
access-list inside_access_in extended permit ip any any
access-group inside_access_in in interface inside
```

打开端口配置

除非扩展访问列表明确允许，否则安全设备不允许任何入站数据流。

如果希望允许外部主机访问内部主机，您可以在外部接口上应用一个入站访问列表。您需要在访问列表中指定内部主机的转换地址，因为转换地址是可在外部网络上使用的地址。要打开从安全性较低的区域到安全性较高的区域的端口，请完成以下步骤。例如，允许从外部（安全性较低的区域）到内部接口（安全性较高的区域）或从 DMZ 到内部接口的数据流。

1. 静态 NAT 会创建从实际地址到映射地址的固定转换。此映射地址是位于 Internet 上且在无需知道 DMZ 上的应用程序服务器的实际地址的情况下可用来访问该服务器的地址。

```
static (real_ifc,mapped_ifc) mapped_ip {real_ip [netmask mask] |
   access-list access_list_name | interface}
```

   要了解详细信息，请参阅 PIX/ASA 命令参考的 Static NAT 部分。
2. 创建一个 ACL 以允许特定端口数据流。

```
access-list
```

3. 使用 access-group 命令绑定该访问列表以激活它。

```
access-group
```

示例：

1. **打开 SMTP 端口数据流：**打开端口 tcp 25 以允许外部 (Internet) 主机访问位于 DMZ 网络中的邮件服务器。Static 命令将外部地址 192.168.5.3 映射到实际 DMZ 地址 172.16.1.3。

```
ciscoasa(config)#static (DMZ,Outside) 192.168.5.3 172.16.1.3
 netmask 255.255.255.255
ciscoasa(config)#access-list 100 extended permit tcp
 any host 192.168.5.3 eq 25
ciscoasa(config)#access-group 100 in interface outside
```

2. **打开 HTTPS 端口数据流：**打开端口 tcp 443 以允许外部 (Internet) 主机访问位于 DMZ 网络中的 Web 服务器（安全）。

```
ciscoasa(config)#static (DMZ,Outside) 192.168.5.5 172.16.1.5
 netmask 255.255.255.255
ciscoasa(config)#access-list 100 extended permit tcp
 any host 192.168.5.5  eq 443
ciscoasa(config)#access-group 100 in interface outside
```

3. **允许 DNS 数据流：**打开端口 udp 53 以允许外部 (Internet) 主机访问位于 DMZ 网络中的 DNS 服务器（安全）。

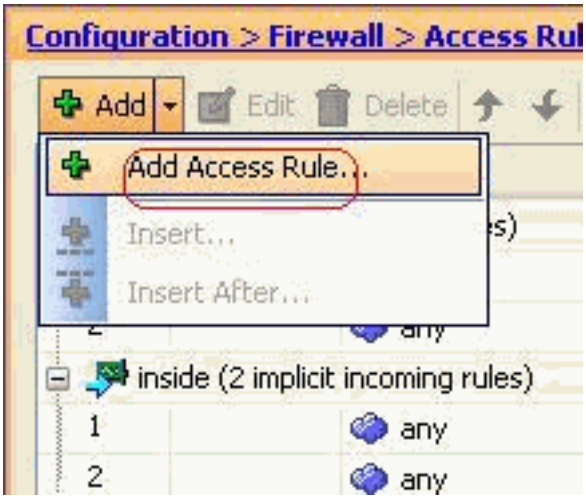
```
ciscoasa(config)#static (DMZ,Outside) 192.168.5.4 172.16.1.4
 netmask 255.255.255.255
ciscoasa(config)#access-list 100 extended permit udp
 any host 192.168.5.4  eq 53
ciscoasa(config)#access-group 100 in interface outside
```

注意：要了解有关端口分配的详细信息，请参阅IANA端口。

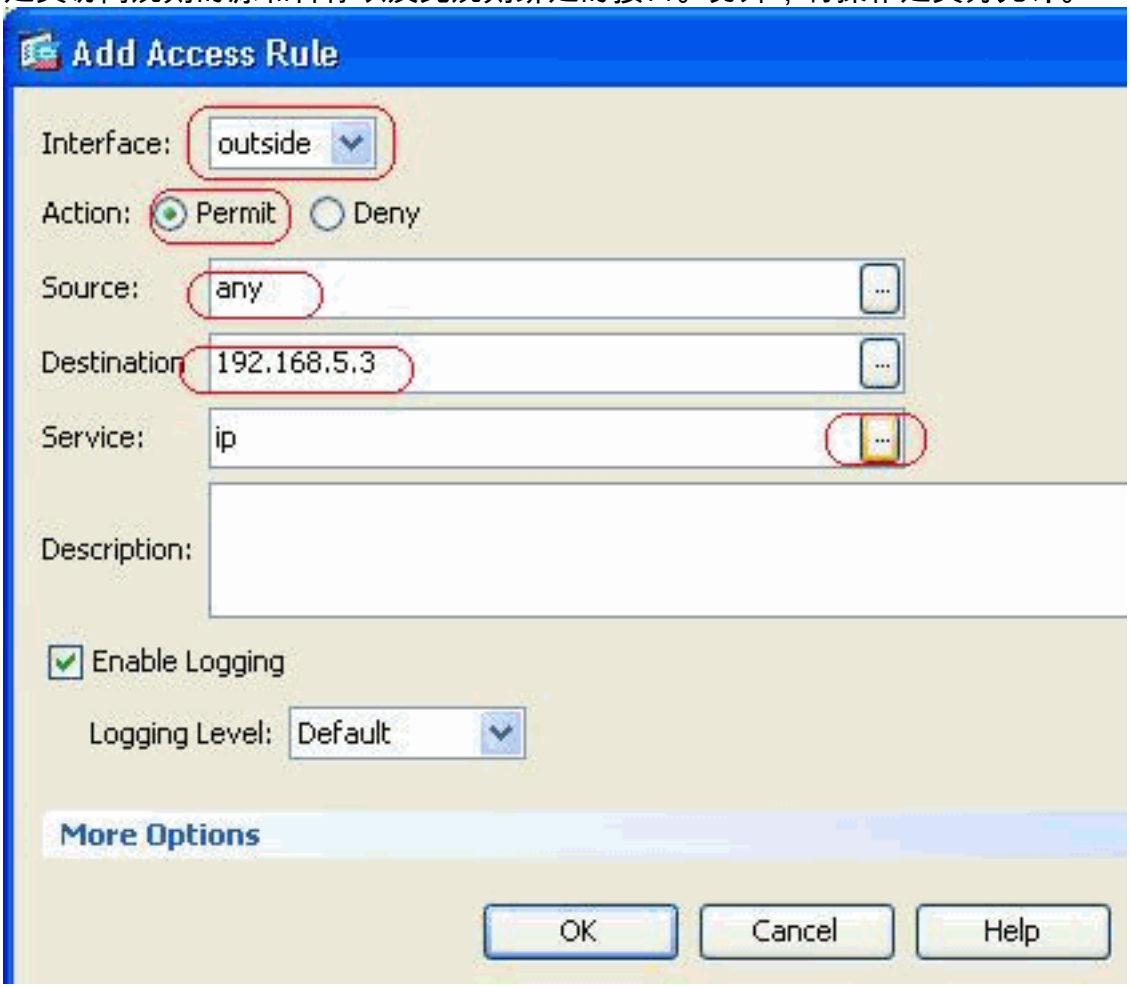
通过ASDM进行配置

本部分显示了通过ASDM执行上述任务的分步方法。

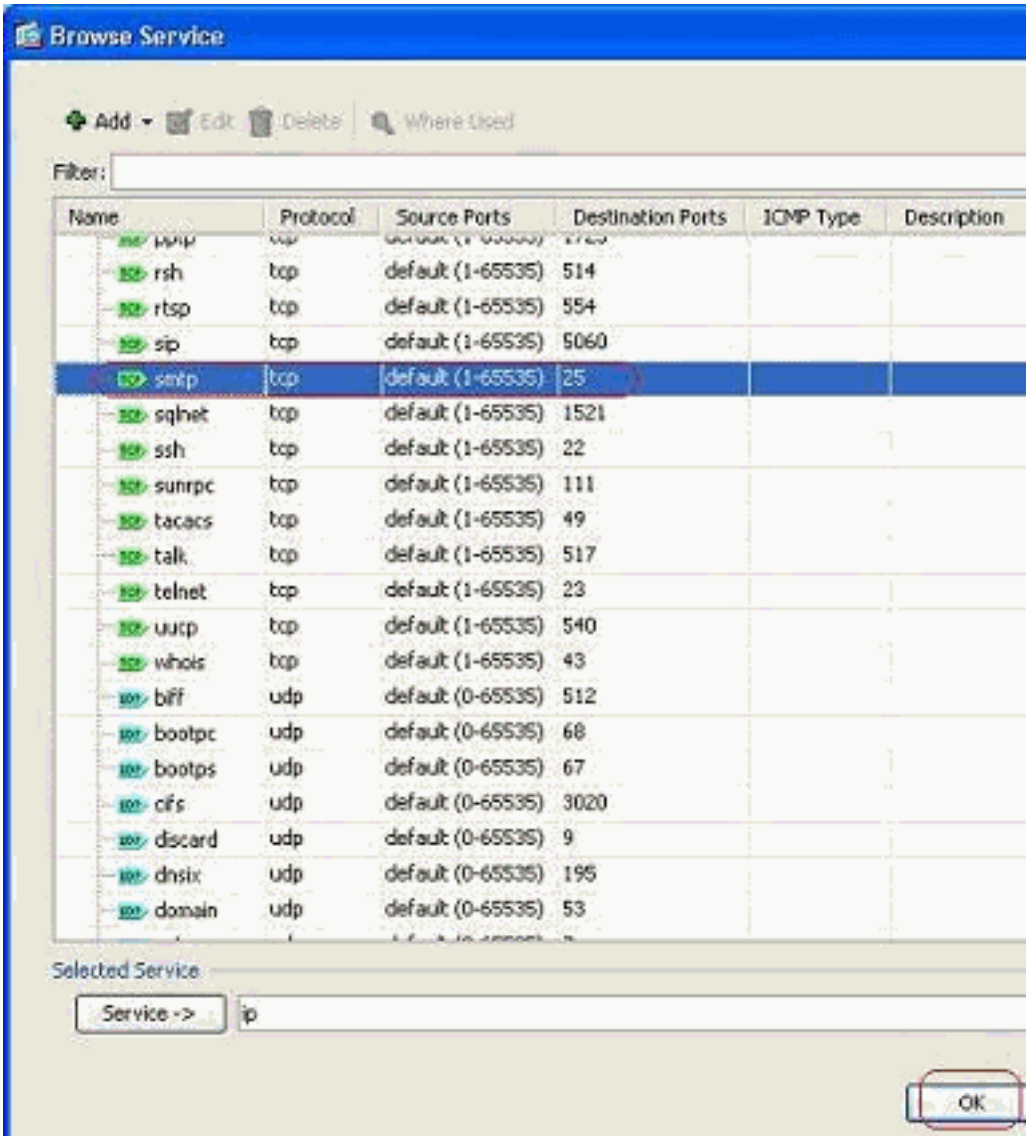
1. 创建访问规则以允许smtp流量到192.168.5.3服务器。



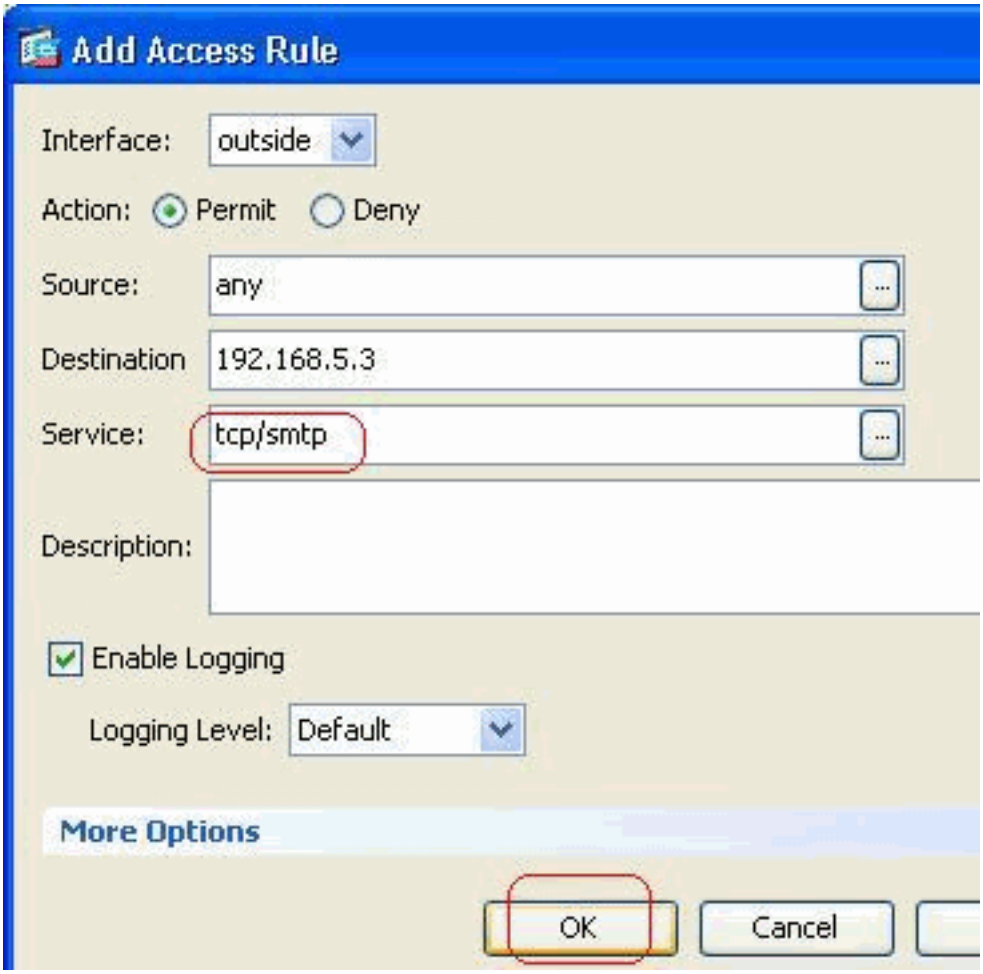
2. 定义访问规则的源和目标以及此规则绑定的接口。另外，将操作定义为**允许**。



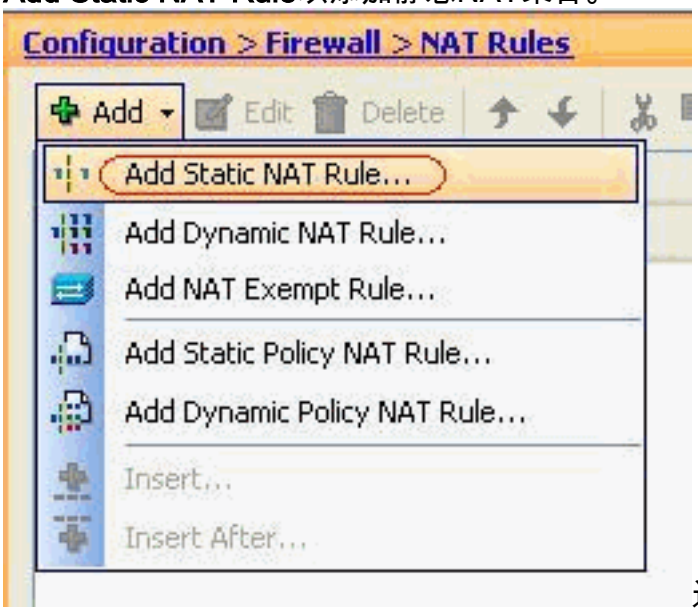
3. 选择SMTP作为端口，然后单击OK。



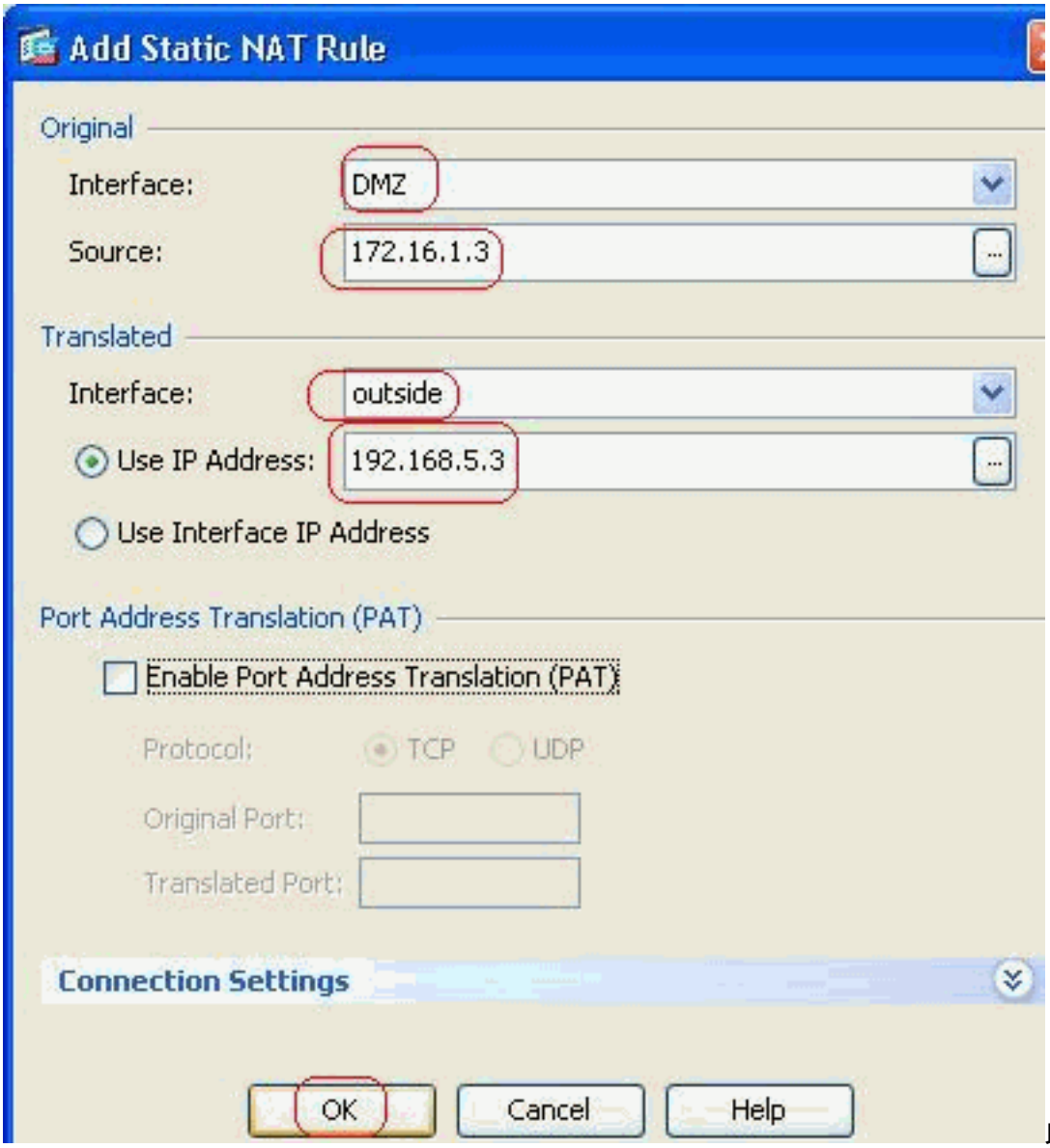
4. 单击OK完成访问规则的配置。



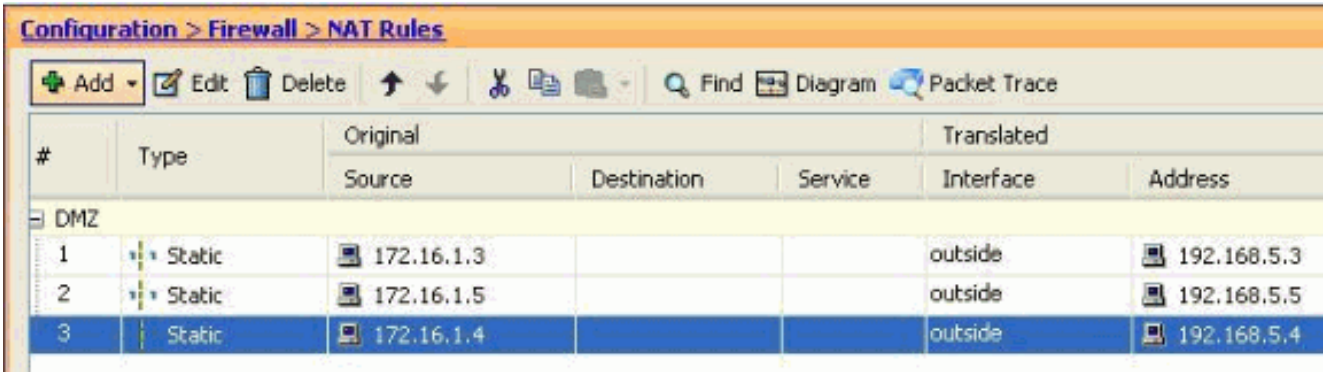
5. 配置静态NAT以将172.16.1.3转换为192.168.5.3转至**Configuration > Firewall > NAT Rules > Add Static NAT Rule**以添加静态NAT条目。



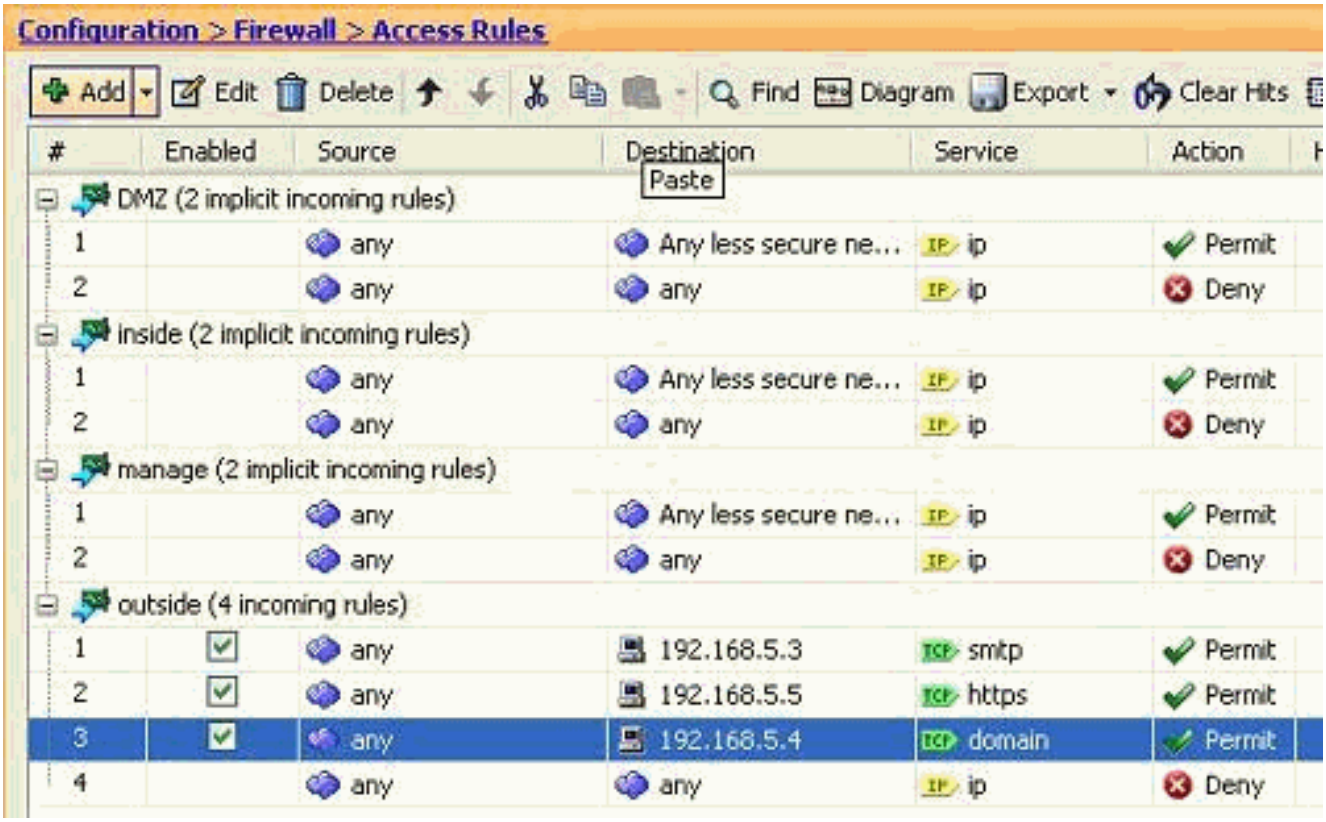
选择Original Source（原始源）和Translated IP地址及其关联接口，然后单击**OK**完成静态NAT规则的配置。



此图显示了“示例”部分列出的所有三个静态规则：



此图显示了“示例”部分列出的所有三个访问规则：



验证

您可以使用某些 **show 命令进行验证，如下所示：**

- **show xlate - 显示当前转换信息**
- **show access-list** - 显示访问策略的命中计数器
- **show logging - 显示缓冲区中的日志。**

命令输出解释程序（仅限注册用户）(OIT) 支持某些 show 命令。使用 OIT 可查看对 show 命令输出的分析。

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- PIX/ASA 7.x：启用/禁用接口之间的通信
- PIX 7.0 和使用 nat、global、static、conduit 和 access-list 命令进行自适应安全设备端口重定向（转发）
- 在 PIX 上使用 nat、global、static、conduit 和 access-list 命令和端口重定向（转发）
- PIX/ASA 7.x：启用 FTP/TFTP 服务配置示例
- PIX/ASA 7.x：启用 VoIP (SIP、MGCP、H323 和 SCCP) 服务配置示例
- PIX/ASA 7.x：DMZ 上的邮件服务器访问配置示例
- 技术支持和文档 - Cisco Systems