ASA 8.X和以后：通过ASDM GUI配置示例添加或修改一访问列表

目录

简介

本文解释如何使用Cisco Adaptive Security Device Manager (ASDM)为了与访问控制列表一起使用。这包括一新的访问列表的创建，如何编辑一个现有的访问列表和其他功能与访问列表。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco可适应安全工具(ASA)有版本8.2.X的
- Cisco Adaptive Security Device Manager (ASDM)有版本6.3.X的

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。

背景信息

访问列表主要用于控制流量流经防火墙。您能允许或否决与访问列表的特定流量类型。每访问列表包含一定数量的访问列表条目(ACE)该控制从一特定来源的通信流到一个特定目的地。通常，此访问列表一定对接口通知应该查找流的方向。访问列表主要分类到两个清楚的类型。

1. 进入访问控制列表
2. 出局访问列表

进入访问控制列表适用于进入该接口的流量，并且出局访问列表适用于退出接口的流量。呼入/呼出的符号是指流量方向根据该接口，但是不对流量的移动更加高和较低安全性接口之间的。

对于TCP和UDP连接，因为安全工具允许所有返回的流量已建立双向连接，您不需要访问列表允许返回流量。对于无连接协议例如ICMP，安全工具建立单向的会话，因此您或者需要访问列表运用访问列表到源和目的接口为了允许在两个方向的ICMP，或者您需要启用ICMP检测引擎。ICMP 检测引擎将 ICMP 会话视为双向连接。

从ASDM版本6.3.X，有您能配置访问列表的两种类型。

1. 接口访问规则
2. 全球访问规则

注意： 访问规则是指单个访问列表项(ACE)。

接口访问规则一定对所有接口在他们的创建时。没有约束他们对接口，您不能创建他们。这与Line命令示例有所不同。使用CLI，您首先建立访问列表用**访问列表命令**，然后绑定此访问列表对一个接口用**access-group命令**。ASDM 6.3及以后，访问列表创建并且一定对接口作为单个任务。这适用于流经仅该特定接口的流量。

全球访问规则没有一定对任何接口。他们可以通过在ASDM的ACL Manager选项卡配置和应用对全局入口流量。当有根据来源、目的地和协议类型时的匹配他们实现。这些规则在每个接口没有复制，因此他们节省存储器空间。

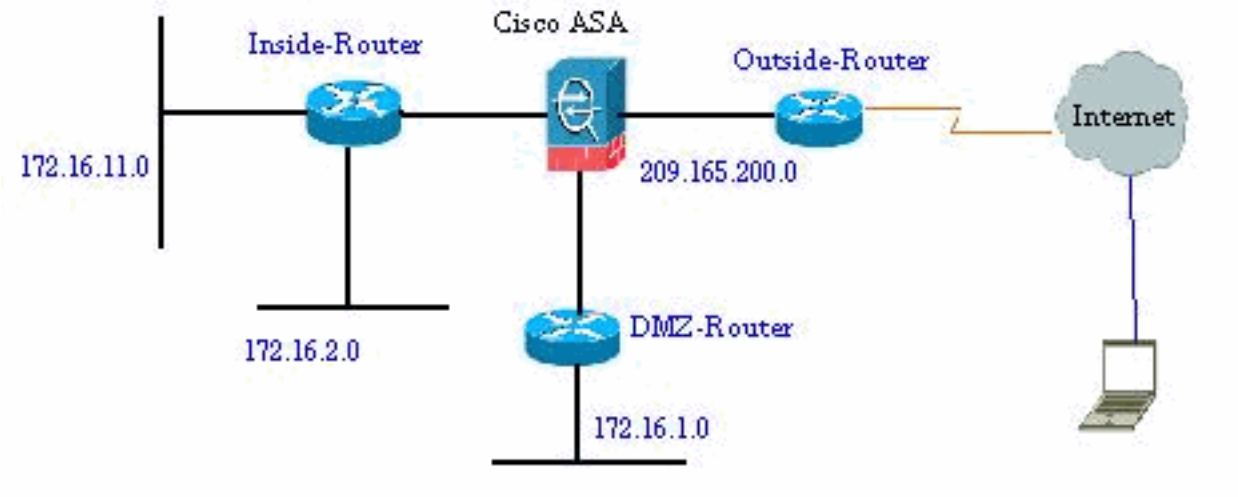
当这两个规则将实现时，接口访问规则通常比全球访问规则优先。

配置

本部分提供有关如何配置本文档所述功能的信息。

网络图

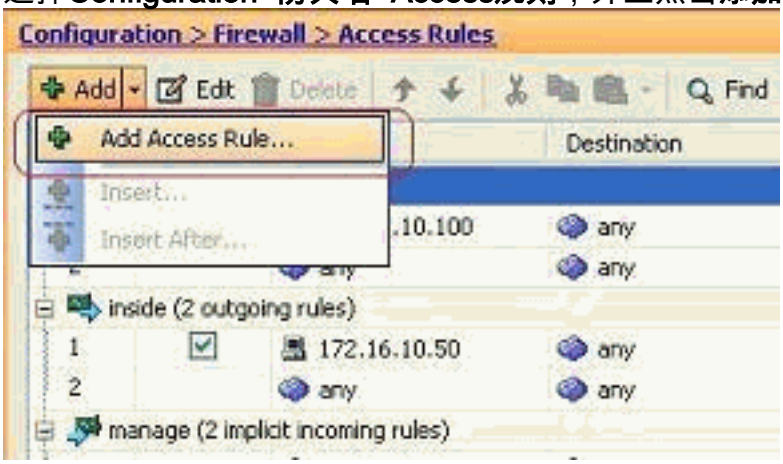
本文档使用以下网络设置：



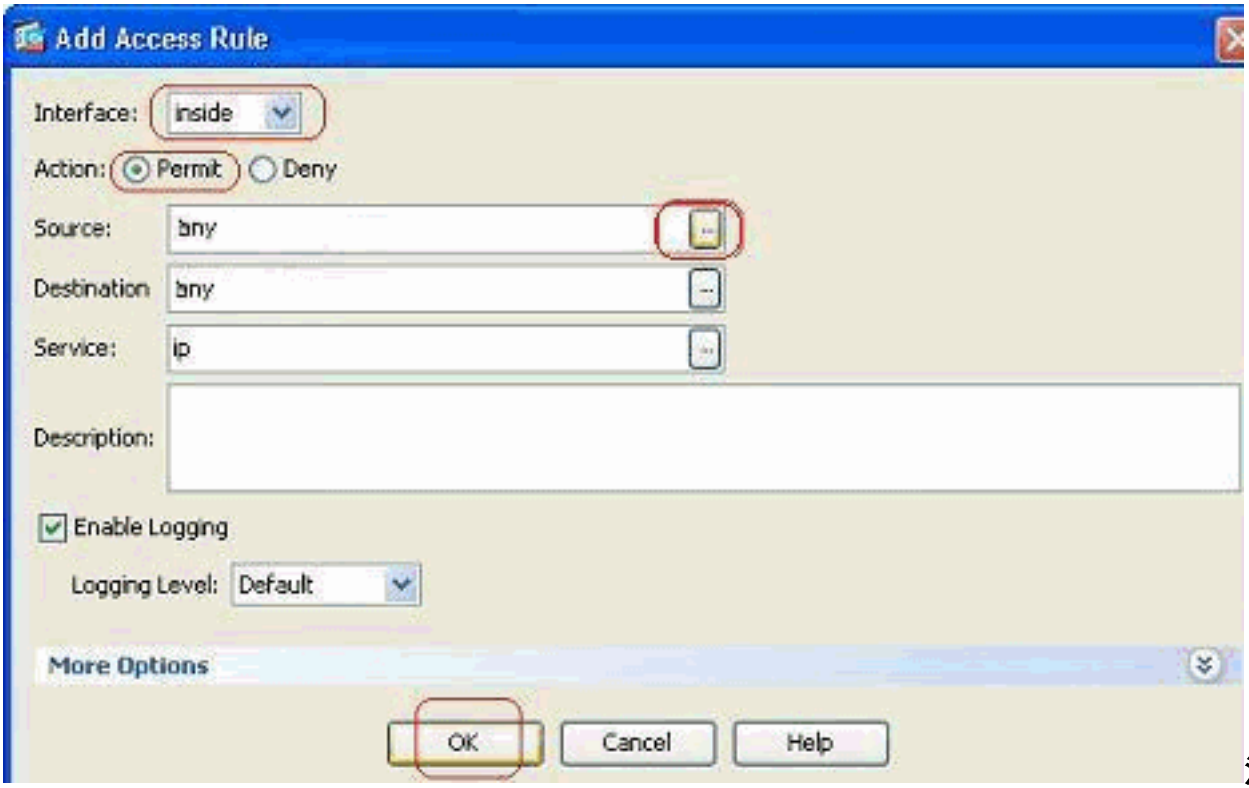
添加新的访问列表

完成这些步骤为了建立与ASDM的一新的访问列表：

1. 选择**Configuration>防火墙>Access规则**，并且点击**添加访问规则**按钮。

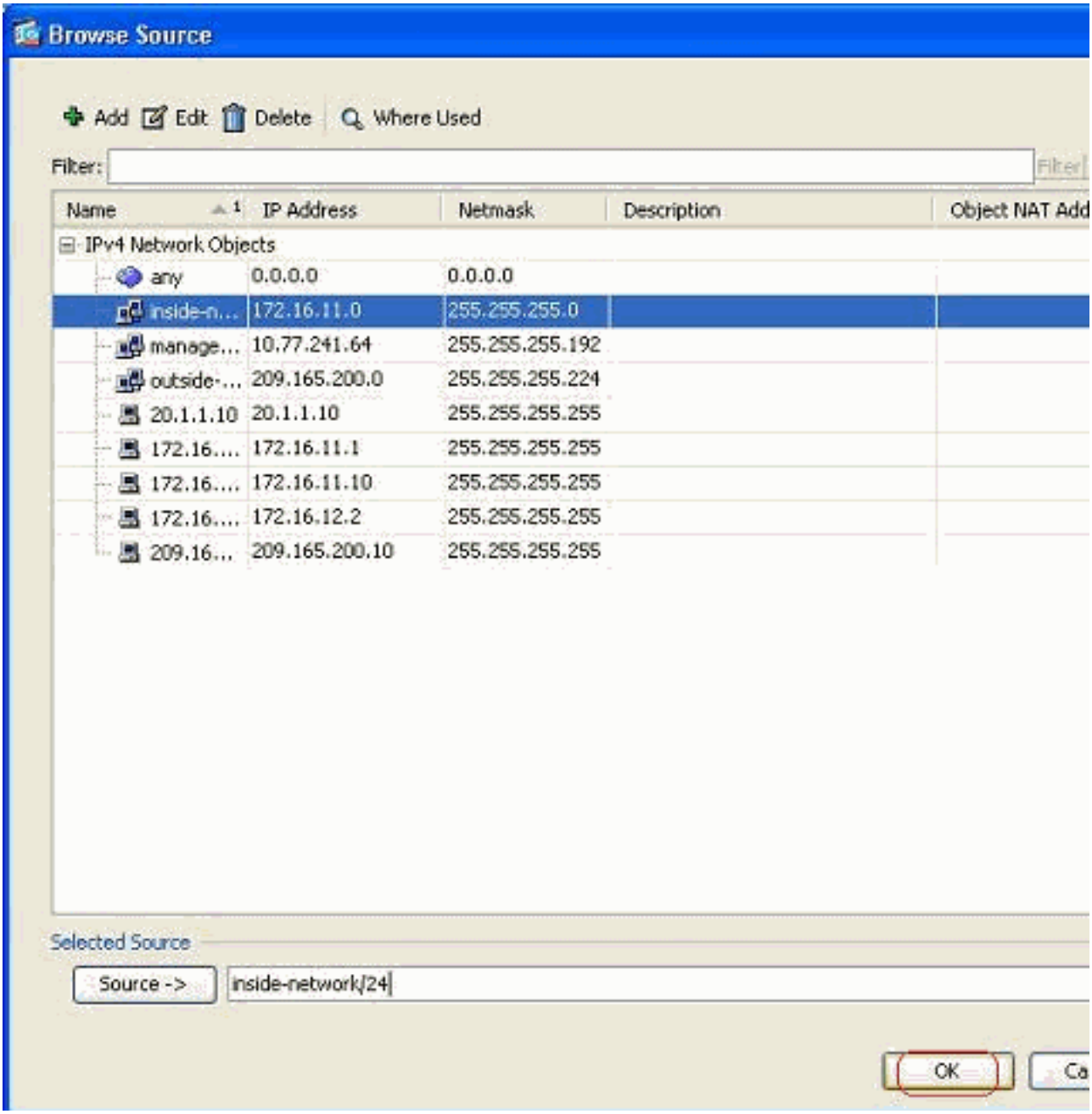


2. 与操作执行一起即选择此访问列表必须跳起的接口，在流量， permit/拒绝。然后请单击Detailsbutton为了选择源网络。

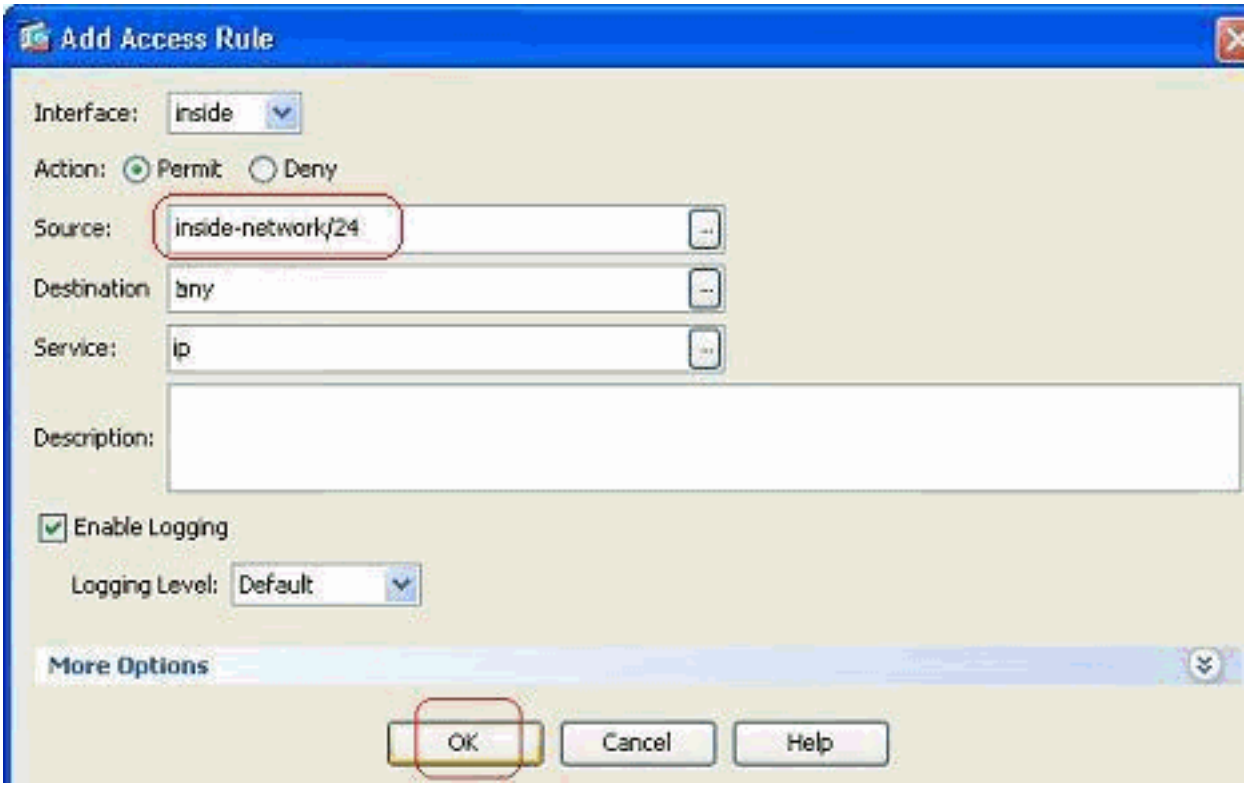


注意：这是在此窗口显示不同的字段的简要说明：**接口**—确定此访问列表一定的接口。**操作**—确定新规则的操作类型。两个选项是可用的。**允许**允许所有流量相匹配并且**否决**块所有流量相匹配。**来源**—此字段指定流量的来源。这可以是任何在单个IP地址、网络、防火墙的接口IP地址或网络对象组中。这些可以选择与**详细信息按钮**。**目的地**—此字段指定流量的来源。这可以是任何在单个IP地址、网络、防火墙的接口IP地址或网络对象组中。这些可以选择与**详细信息按钮**。**服务**—此字段确定此访问列表应用流量的协议或服务。您能也定义包含一套不同的协议的服务组。

3. 在您点击**详细信息按钮后**，包含现有的网络对象的新窗口显示。选择**网络内部**，并且点击OK键。



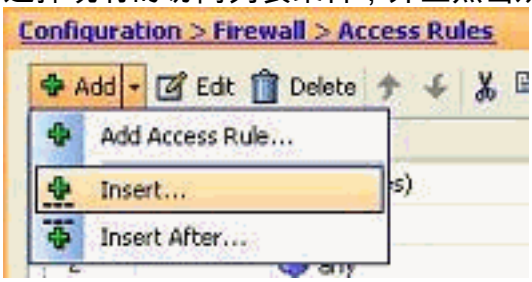
4. 您返回对**添加访问规则**窗口。输入其中**任一**目的区域。并且请点击OK键为了完成访问规则的配置。



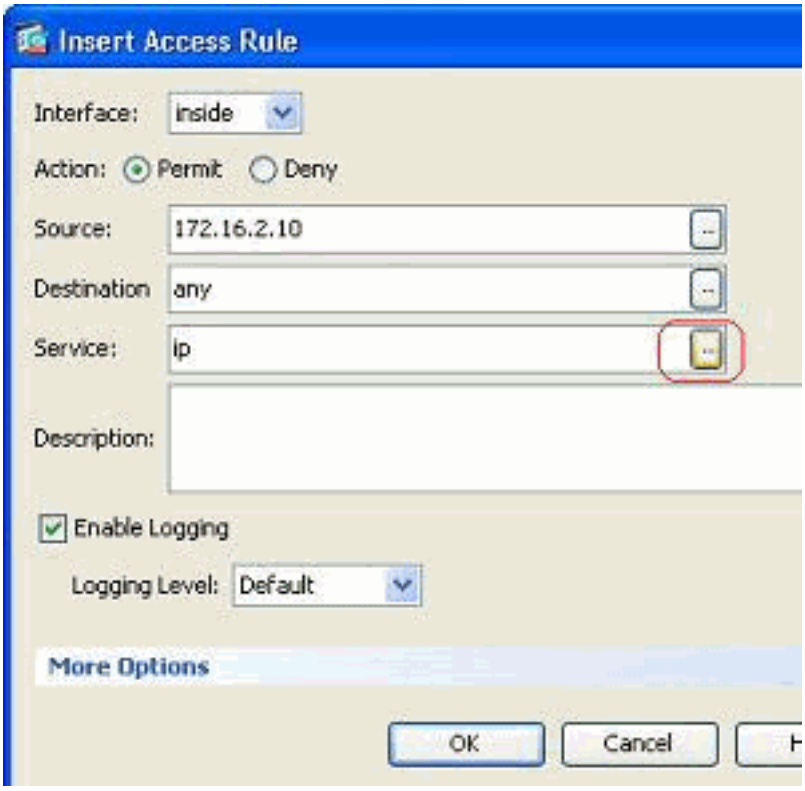
在一存在的一个前增加一个访问规则：

请完成这些步骤为了增加访问规则，在一个已经现有访问规则之前：

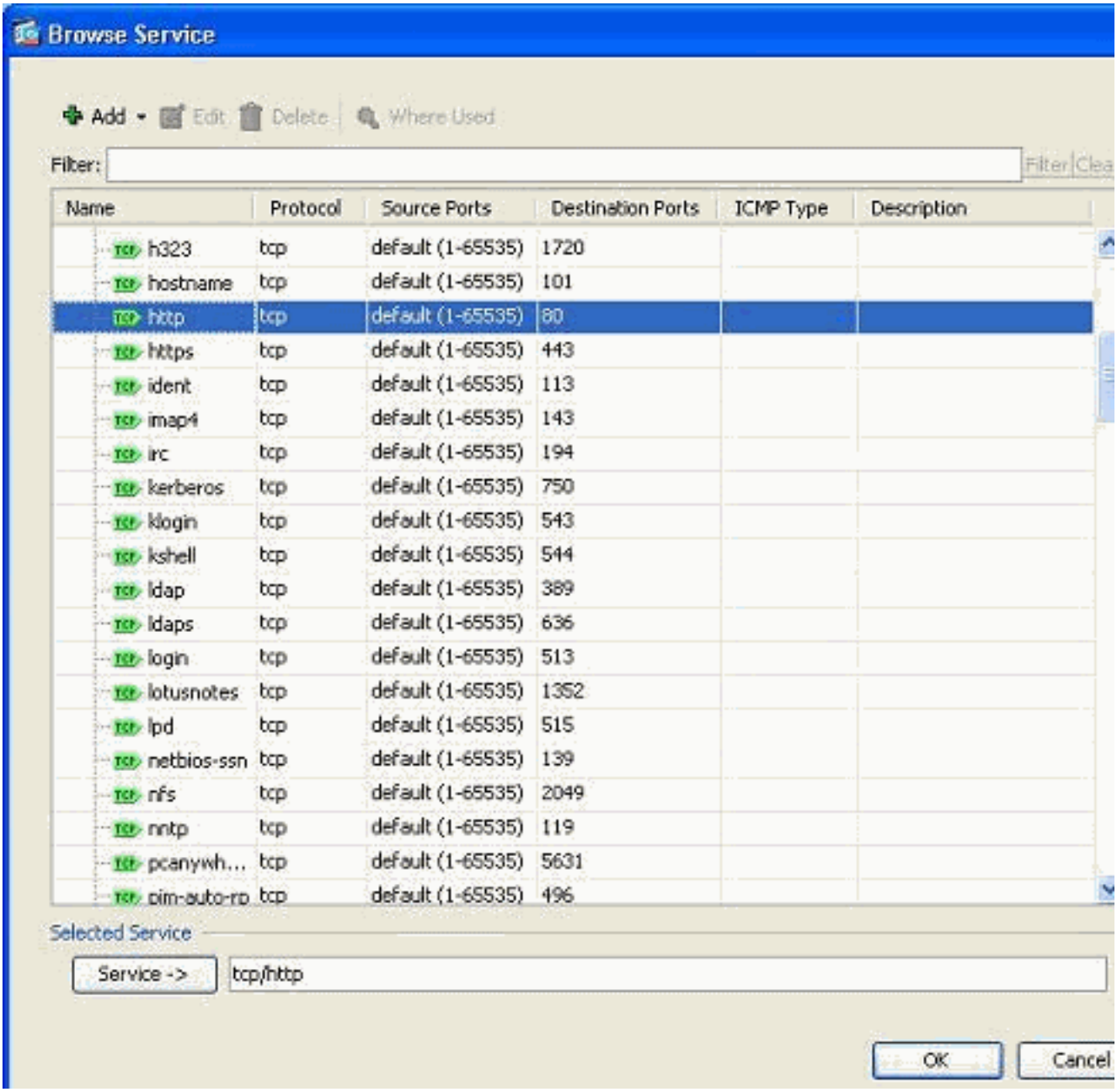
1. 选择现有的访问列表条目，并且点击从**添加**下拉菜单的**插入键**



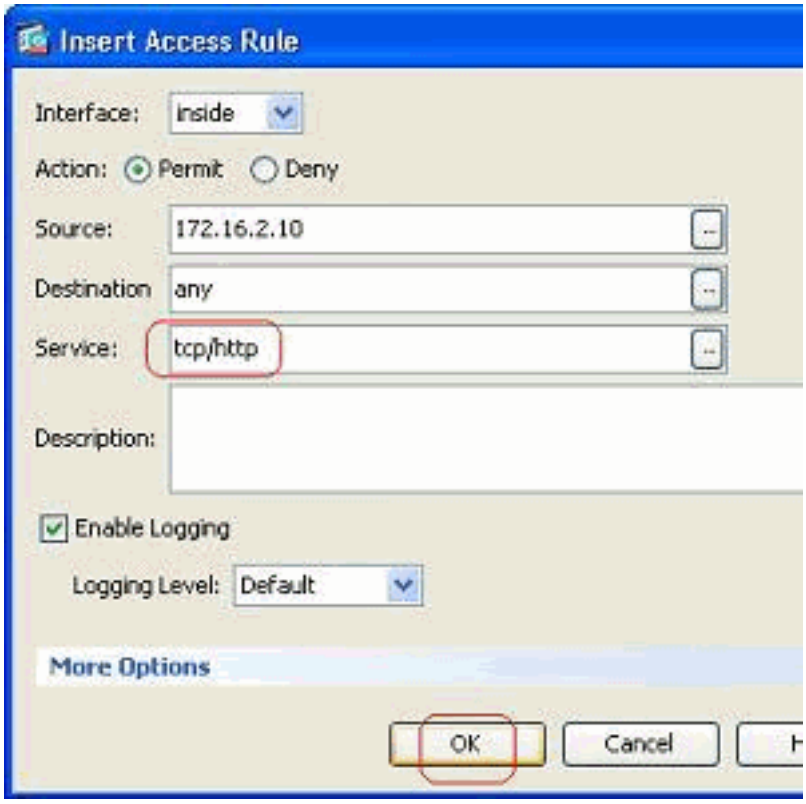
2. 选择源和目的，并且点击服务字段的**详细信息按钮**选择协议。



3. 选择HTTP协议，并且点击OK键。

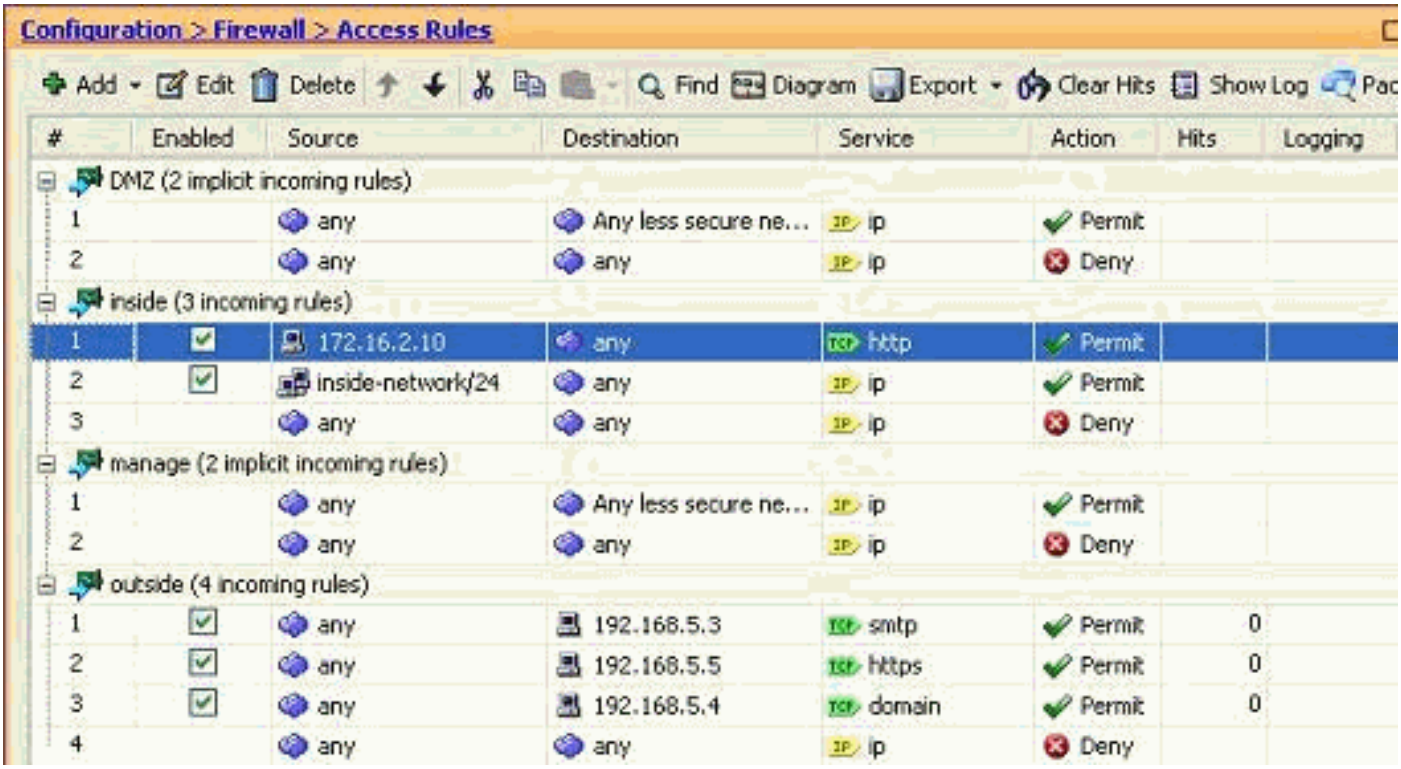


4. 您返回对插入访问规则窗口。服务字段充满**tcp/http**作为选定协议。点击OK键为了完成新的访



问列表条目的配置。

您能对网络内部现在遵守在现有项之前已经显示的新的访问规则。



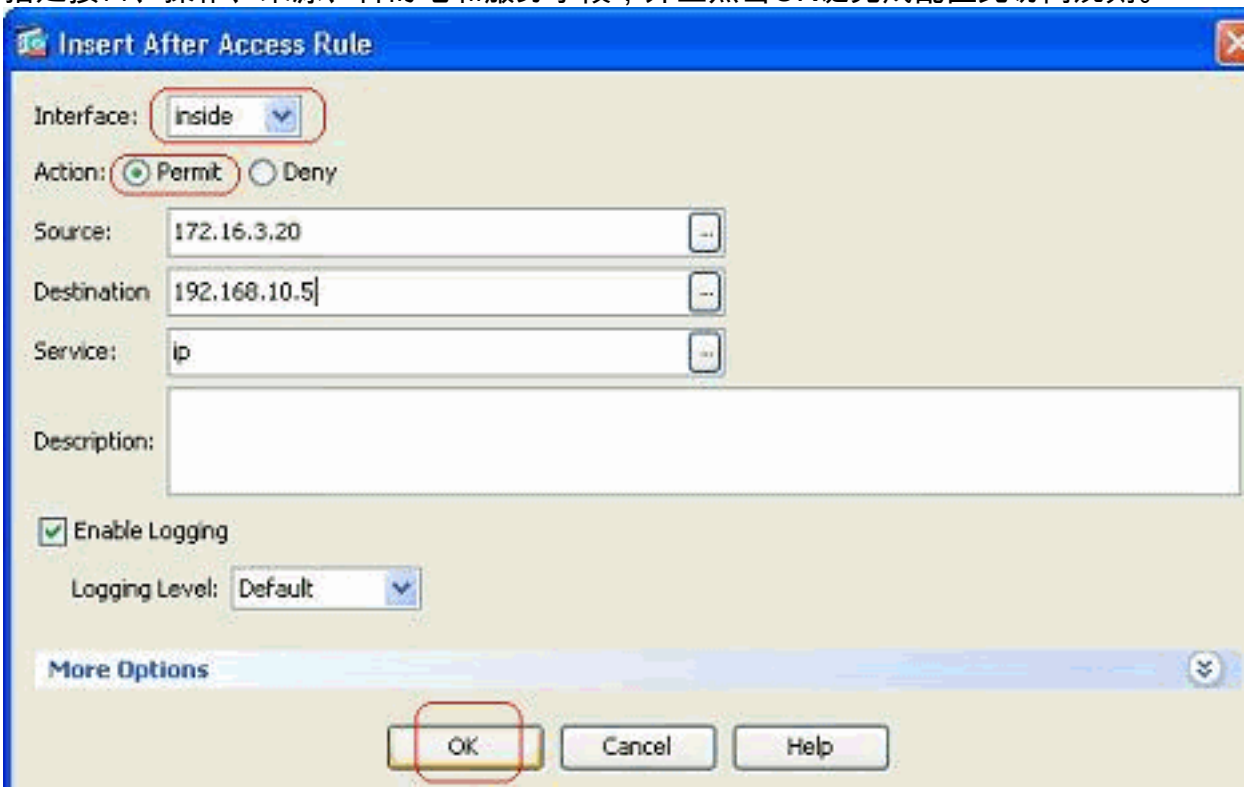
注意： 访问规则的命令是非常重要。当处理每数据包过滤， ASA检查，如果数据包匹配其中任一个在顺序时的访问规则标准，并且，如果匹配发生，实现该访问规则的操作。当访问规则匹配时，不继续对更加进一步的访问规则并且再验证他们。

在一存在的一个以后增加一个访问规则：

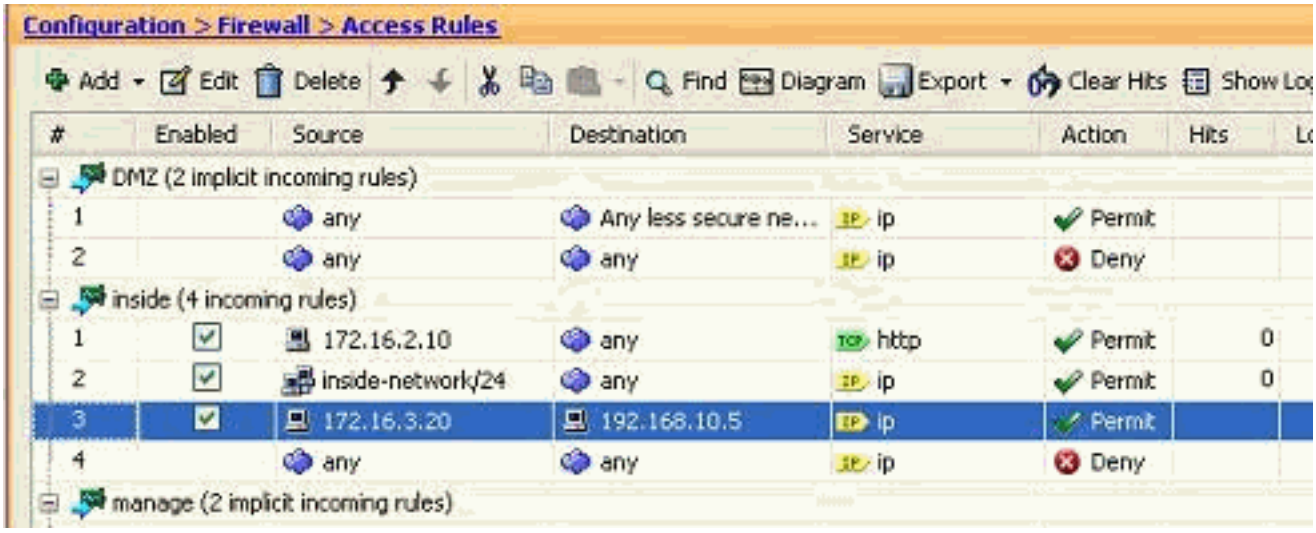
完成这些步骤为了创建访问规则，在一个已经现有访问规则之后。

1. 选择访问规则，在后您需要有一个新的访问规则，并且**以后**从添加下拉菜单选择**插入**。

2. 指定接口、操作、来源、目的地和服务字段，并且点击OK键完成配置此访问规则。



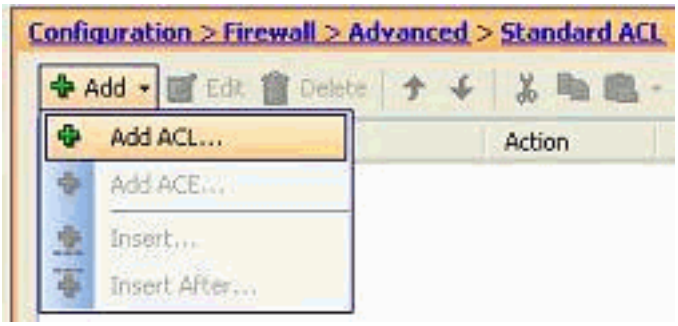
您能查看配置的访问规则在已经已配置的一个之后最近坐。



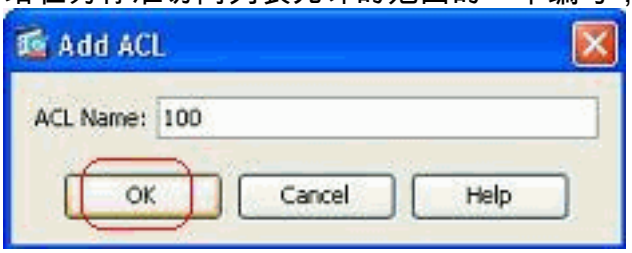
建立标准访问列表

完成这些步骤为了建立与ASDM GUI的一标准访问列表。

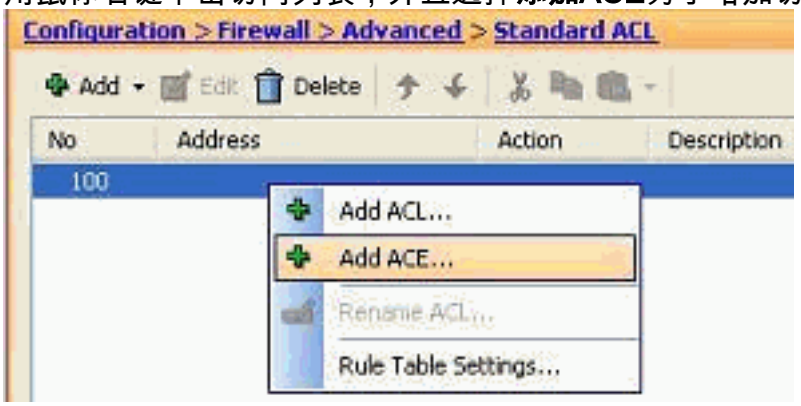
1. 选择**Configuration>防火墙>Advanced >标准ACL >Add**，并且单击**添加ACL**。



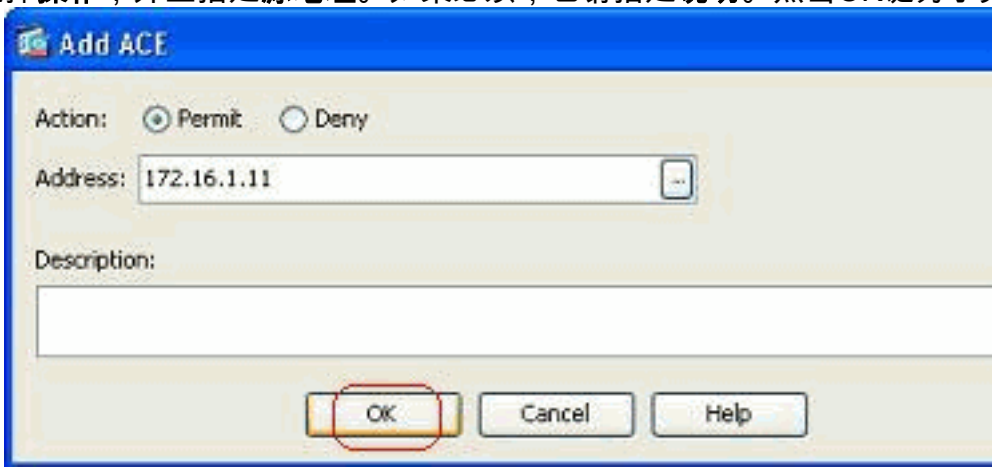
2. 给在为标准访问列表允许的范围的一个编号，并且点击OK键。



3. 用鼠标右键单击访问列表，并且选择**添加ACE**为了增加访问规则到此访问列表。



4. 选择**操作**，并且指定**源地址**。如果必须，也请指定**说明**。点击OK键为了完成访问规则的配置

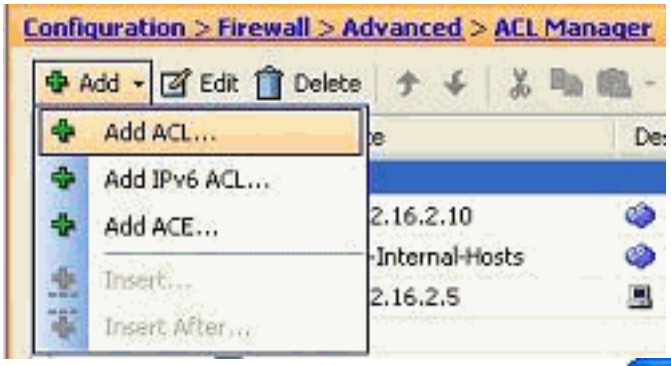


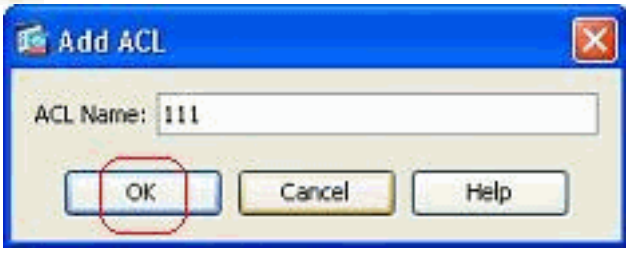
。

创建全球访问规则

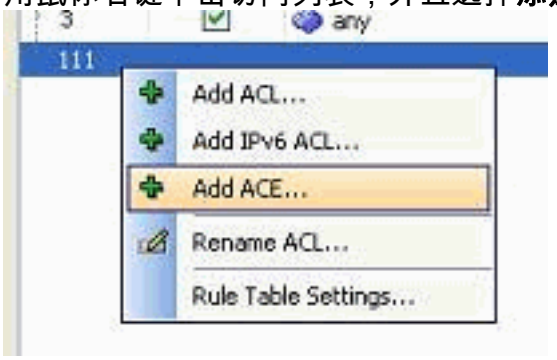
完成这些步骤为了建立包含全球访问规则的扩展访问列表。

1. 选择**Configuration>防火墙>Advanced > ACL Manager >Add**，并且单击**添加ACL**按钮。

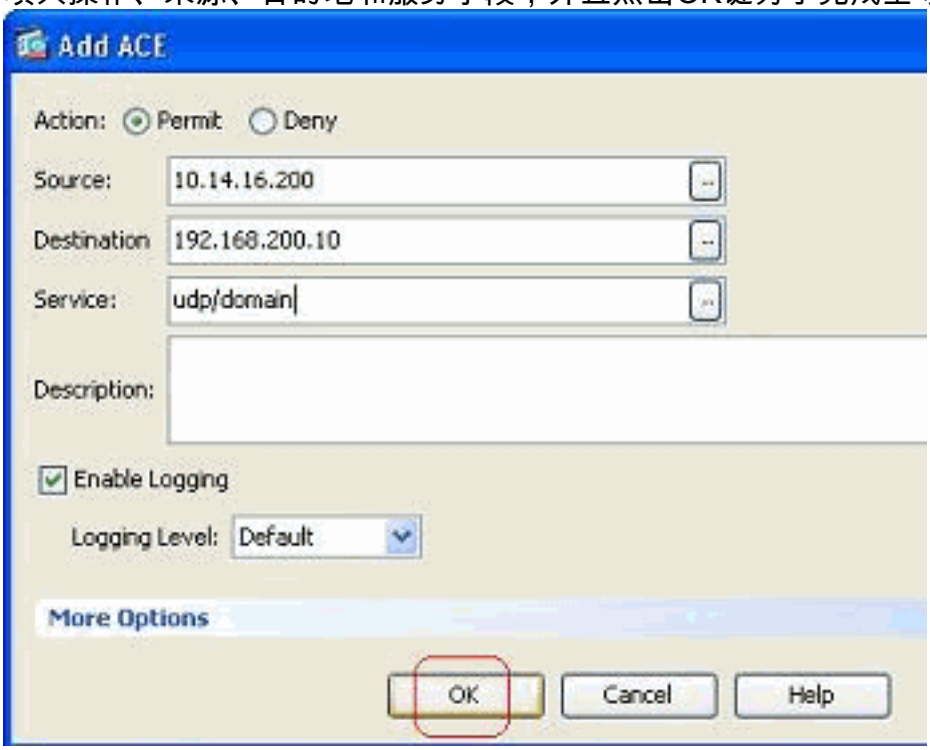




2. 指定一名称对于访问列表，并且点击OK键。
3. 用鼠标右键单击访问列表，并且选择**添加ACE**为了增加访问规则到此访问列表。



4. 填入操作、来源、目的地和服务字段，并且点击OK键为了完成全球访问规则的配置。



您能当前观看全球访问规则，如显示。

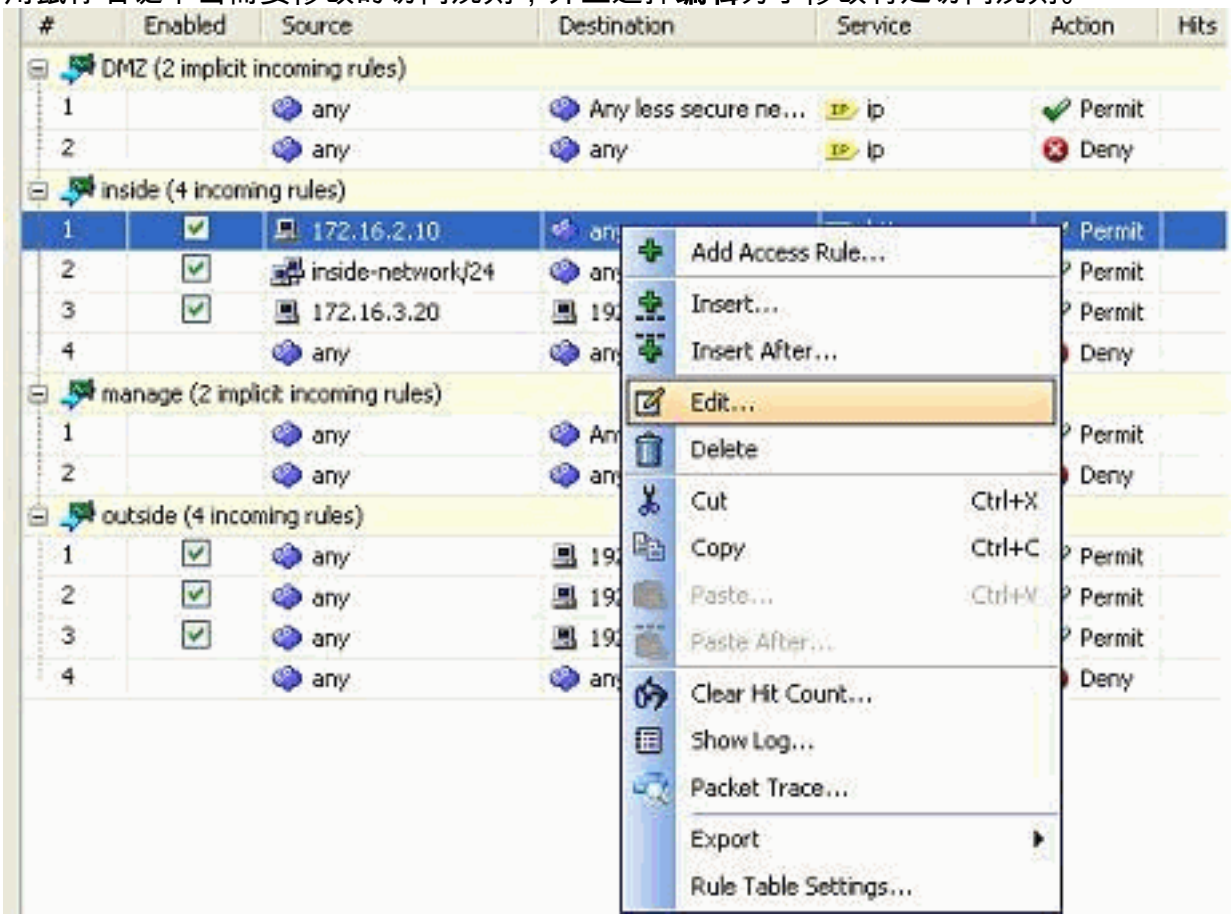
编辑现有的访问列表

此部分讨论如何编辑一现有访问。

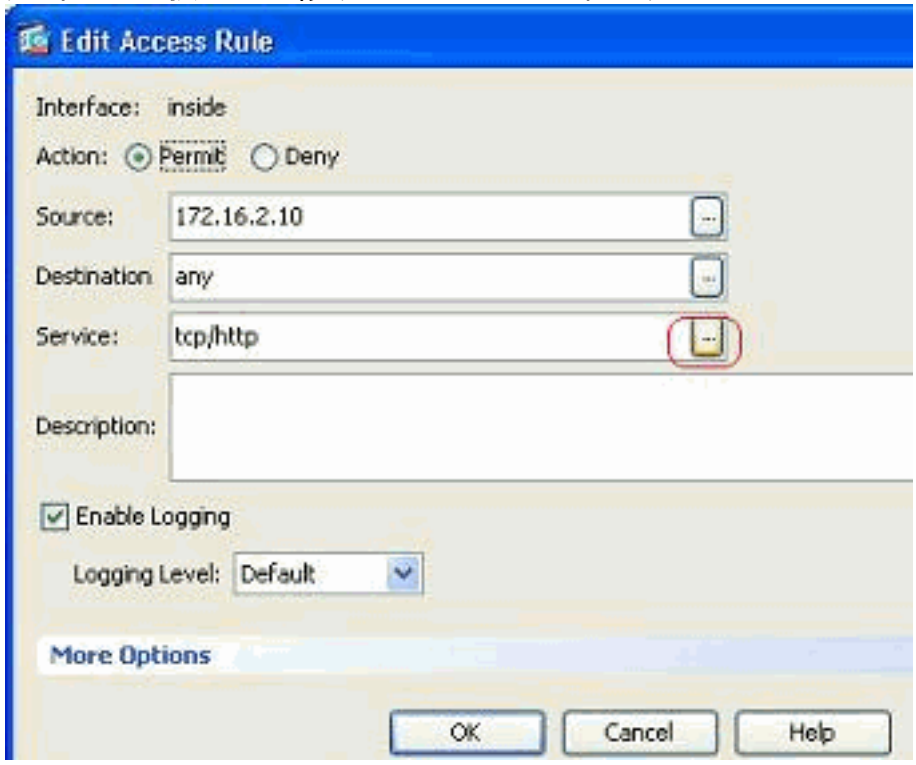
编辑Protocol字段创建服务组：

完成这些步骤为了创建一新的服务组。

1. 用鼠标右键单击需要修改的访问规则，并且选择**编辑**为了修改特定访问规则。

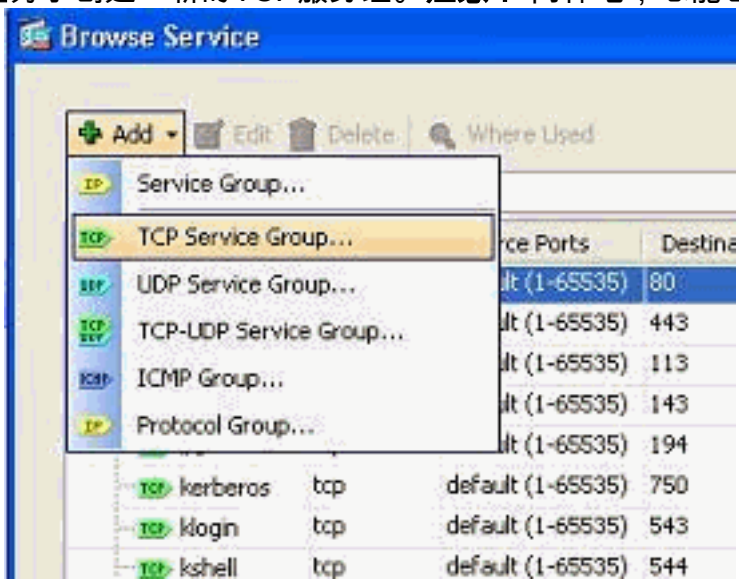


2. 点击**Details按钮**为了修改协议关联与此访问规则。

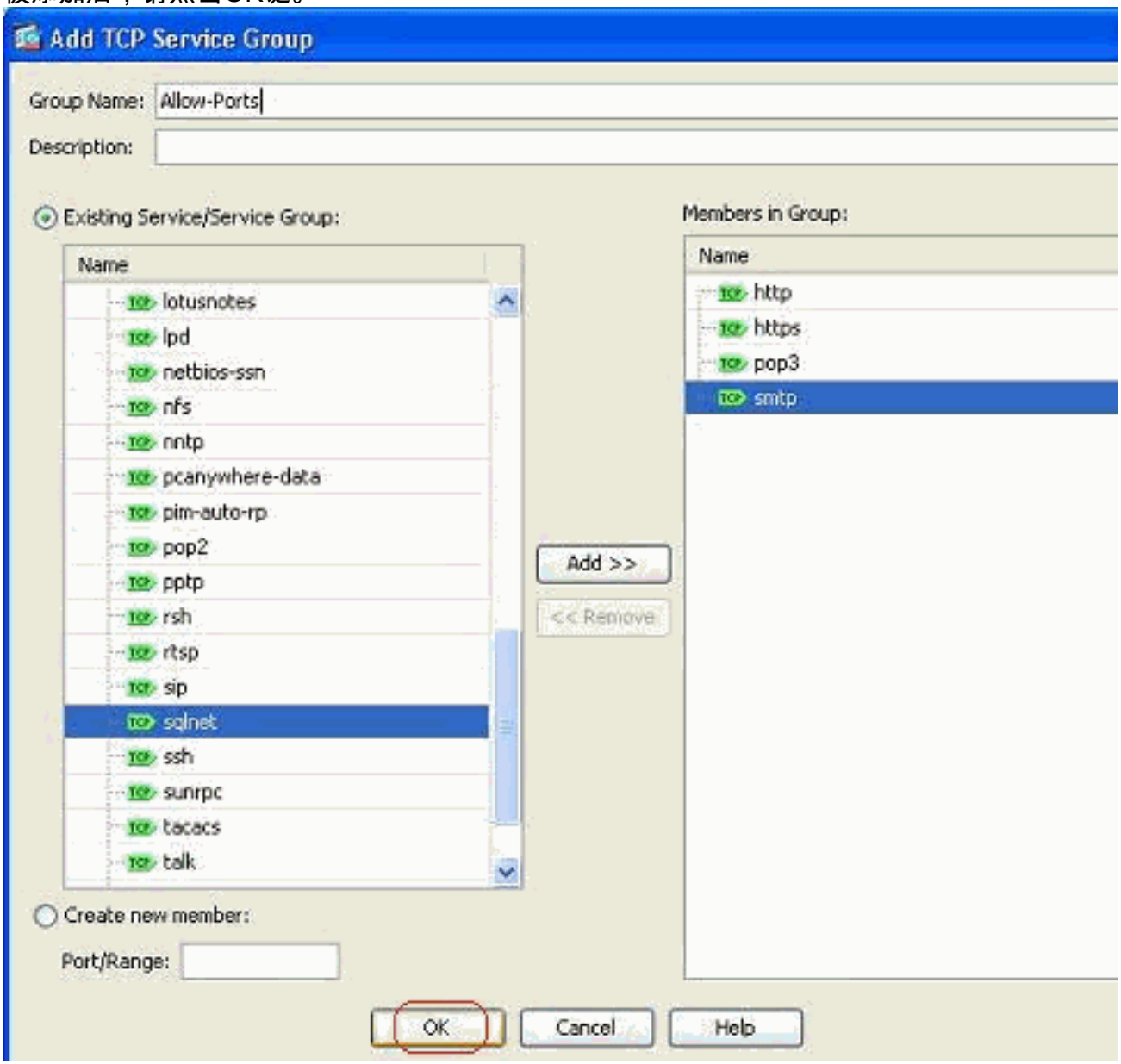


3. 您能如果必须选择所有协议除HTTP之外。如果有将选择的仅单个协议，则没有需要创建服务

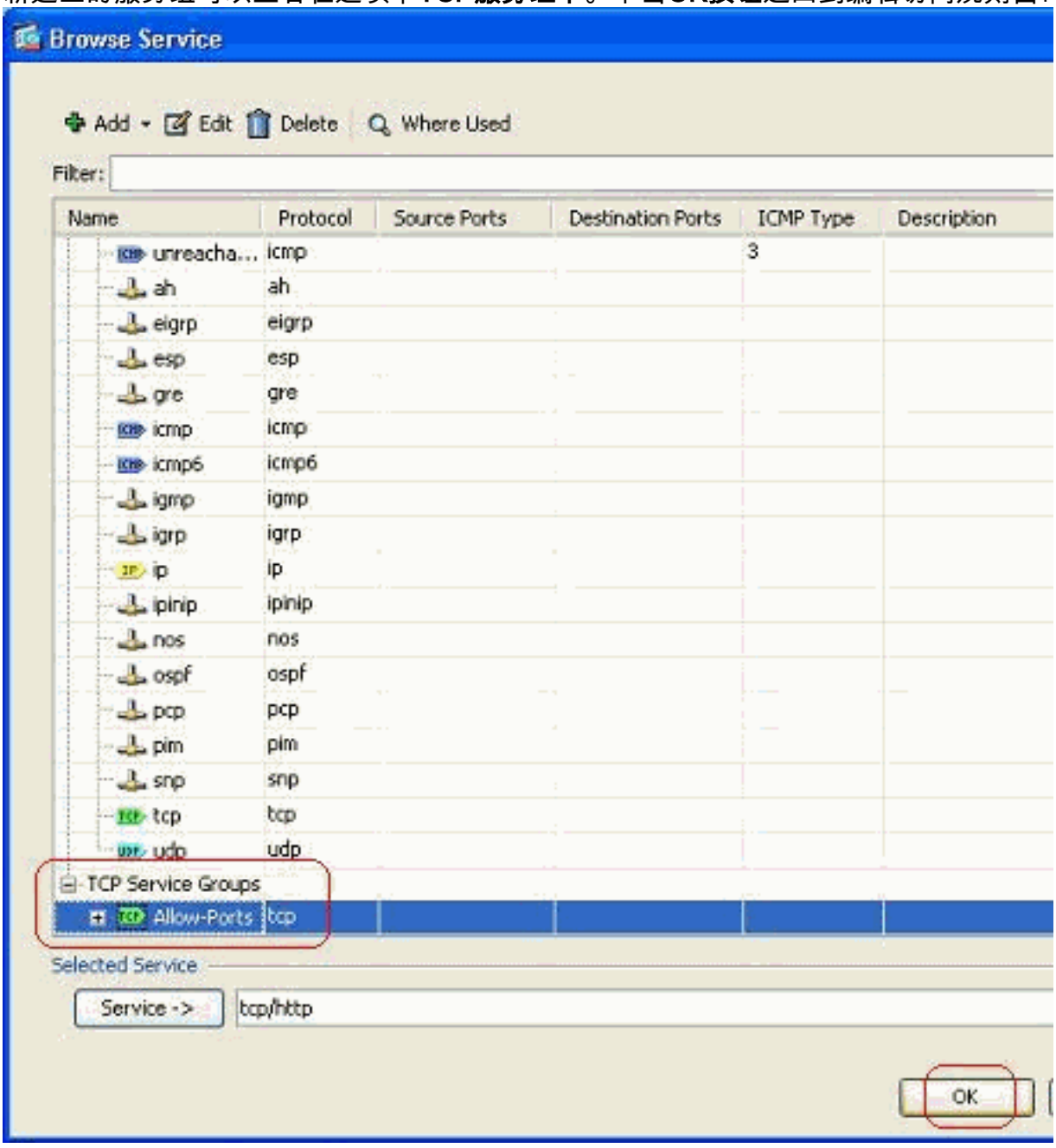
组。当有需求识别此访问规则时，将匹配的许多不邻近的协议创建服务组是有用的。选择**Add> TCP服务组**为了创建一新的TCP服务组。**注意：** 同样地，您能也创建一新的UDP服务组或ICMP组和等。



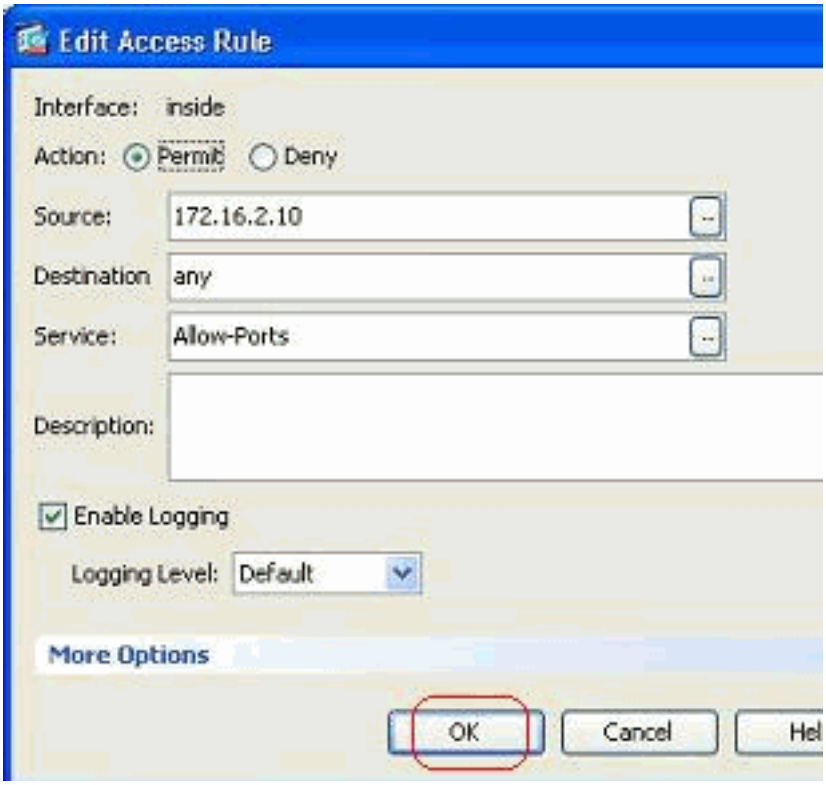
4. 指定一名称对于此服务组，选择在左侧菜单的协议，并且单击**添加**为了移动他们向组菜单的成员在右侧。许多协议可以被添加作为根据需求的服务组的组员。协议逐个被添加。在所有成员被添加后，请点击OK键。



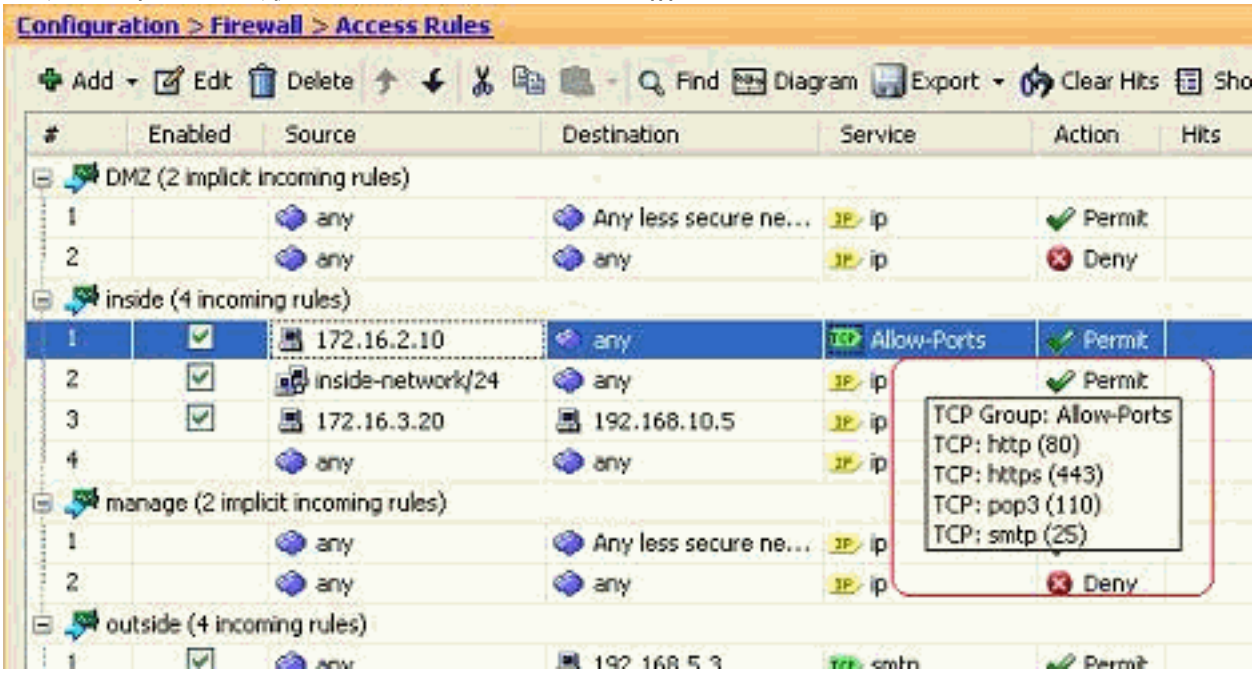
5. 新建立的服务组可以查看在选项卡**TCP服务组下**。单击**OK按钮**返回到编辑访问规则窗口。



6. 您能看到服务字段带有新建立的服务组。点击OK键为了完成编辑。



7. 盘旋您的在该特定服务组的鼠标为了查看所有相关的协议。

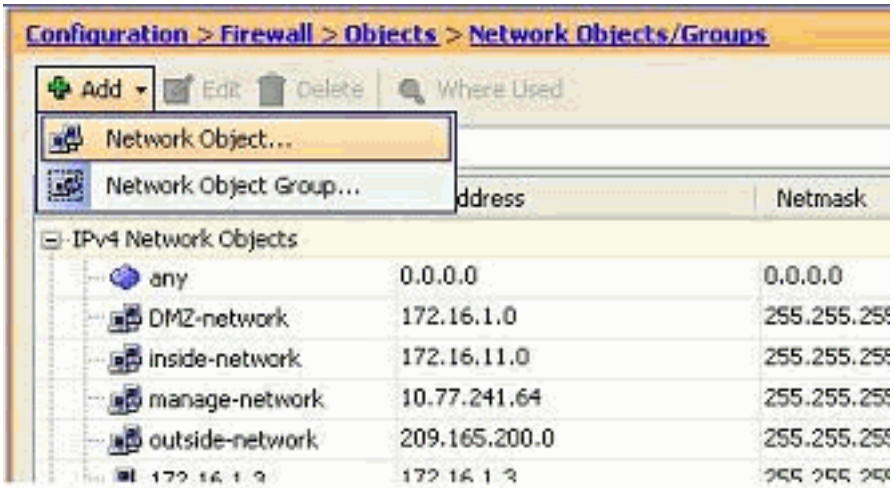


编辑来源/目的区域创建网络对象组：

对象组用于简化访问列表创建和维护。当您组合类似对象时，您在单个ACE能使用对象组而不是必须分开输入每个对象的ACE。在您创建对象组前，您需要创建对象。用ASDM术语，对象呼叫网络对象，并且对象组呼叫网络对象组。

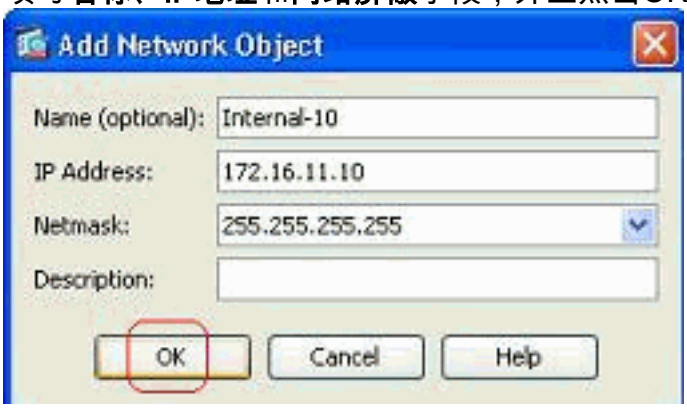
完成这些步骤：

1. 选择**Configuration>防火墙>对象>网络对象/Groups>添加**，并且点击**网络对象**为了创建一个新

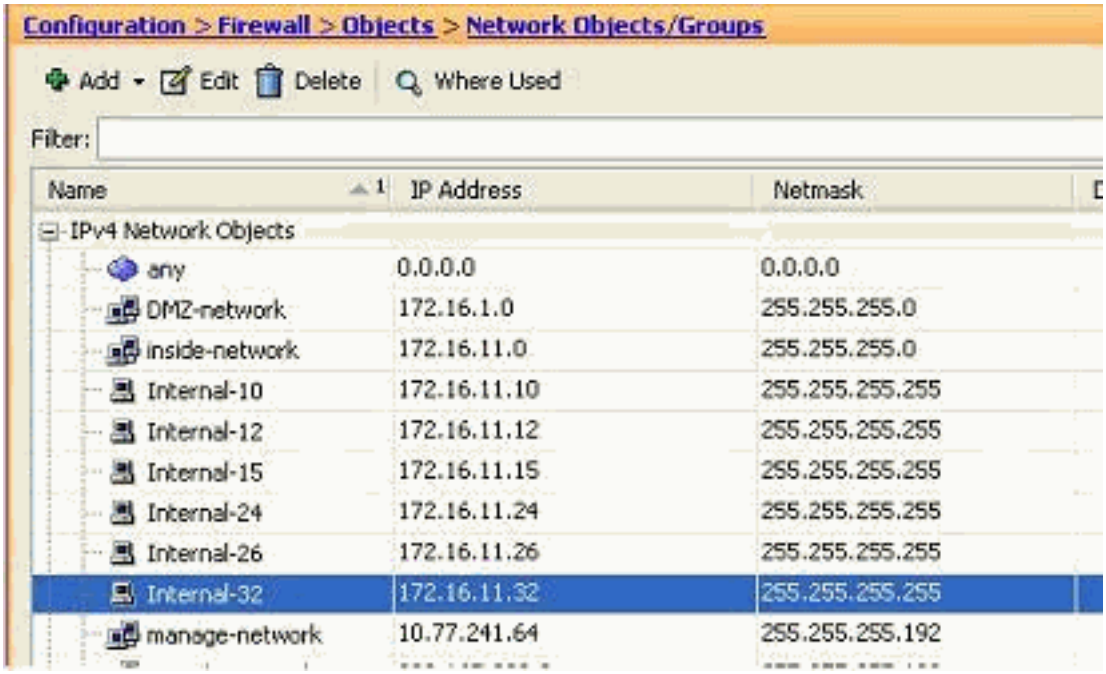


的网络对象。

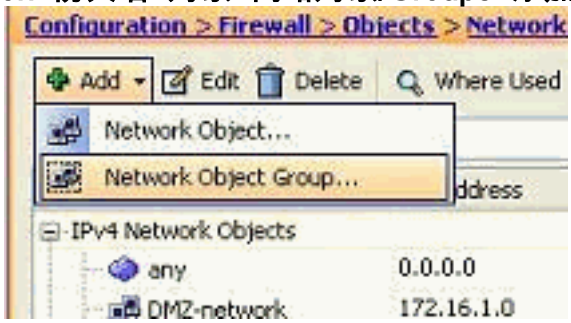
2. 填写**名称、IP地址**和**网络屏蔽**字段，并且点击OK键。



3. 新建立的网络对象在对象的列表能被看到。单击 **Ok**。

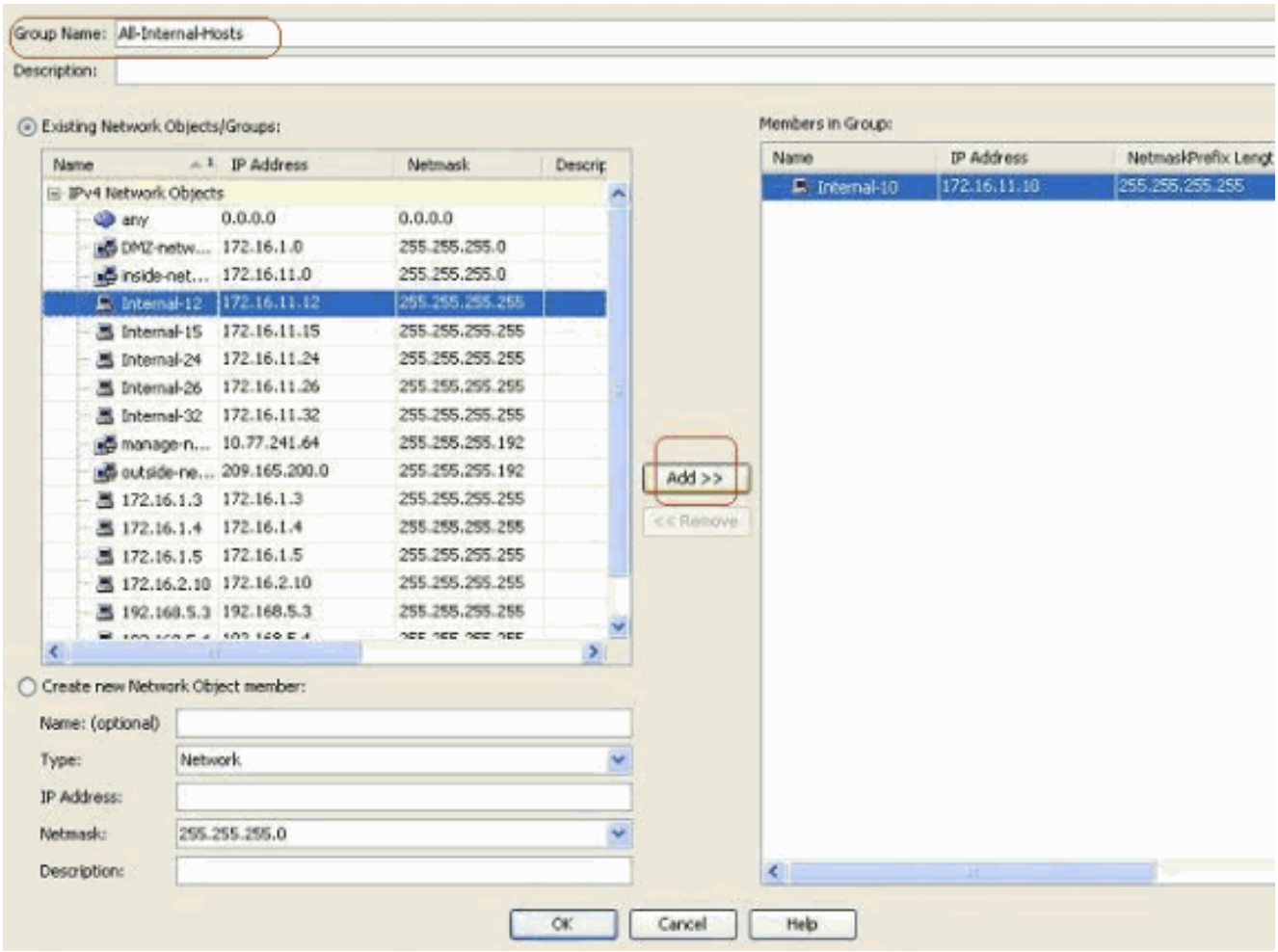


4. 选择**Configuration>防火墙>对象>网络对象/Groups>添加**，并且点击**网络对象组**为了创建一新

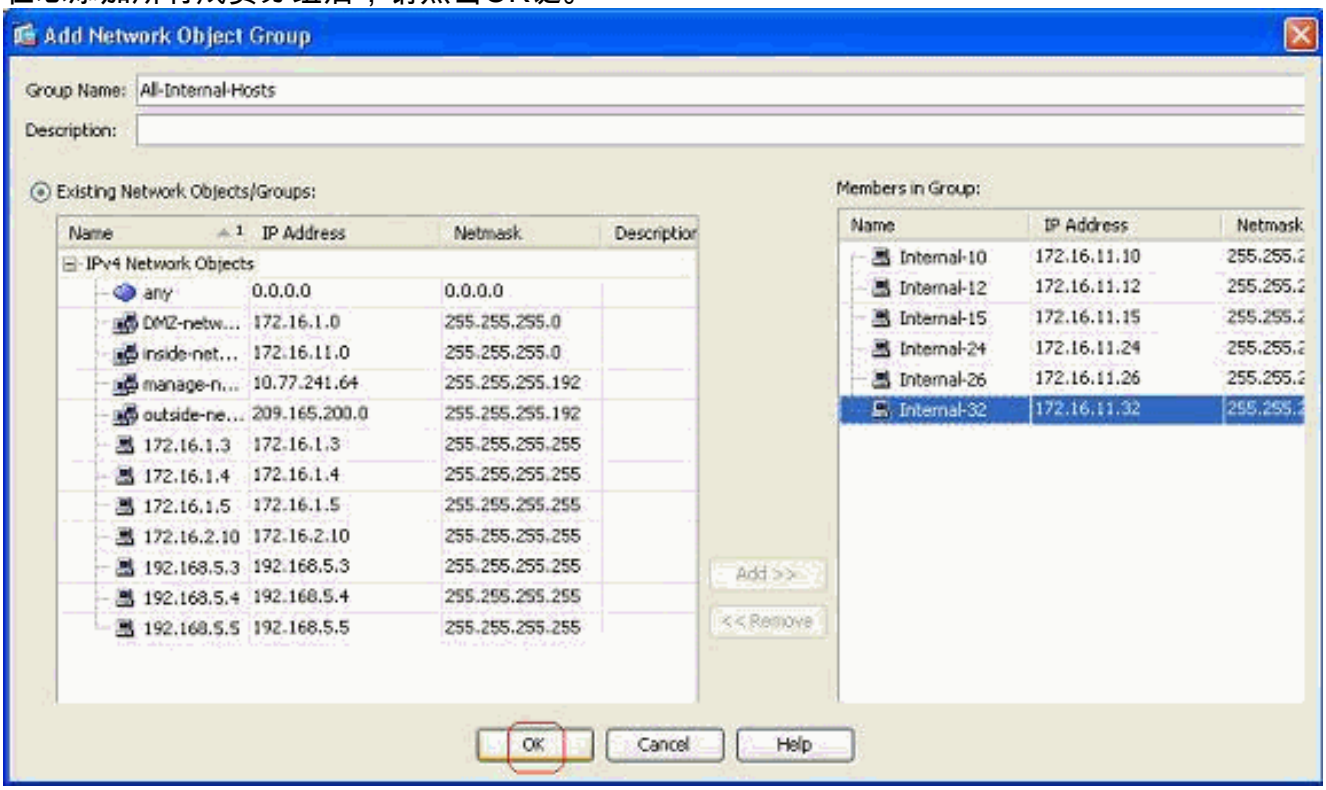


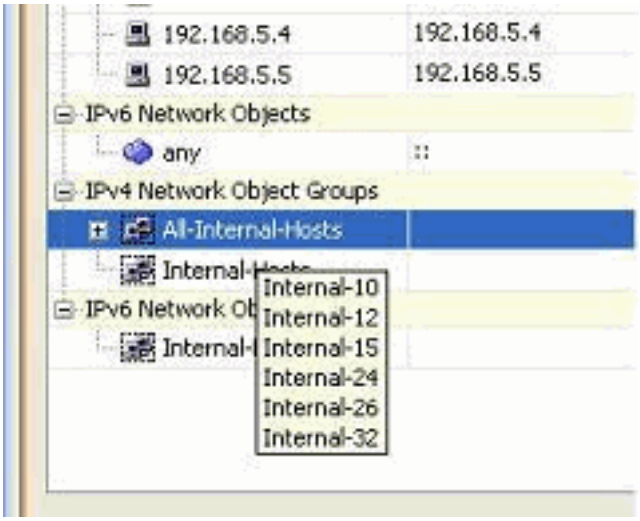
的网络对象组。

5. 所有网络对象可用的列表可以在窗口的左窗格找到。挑选独立网络对象，和点击**Add按钮**为了做他们成员新建立的网络对象组。在为它分配的字段必须指定组名。



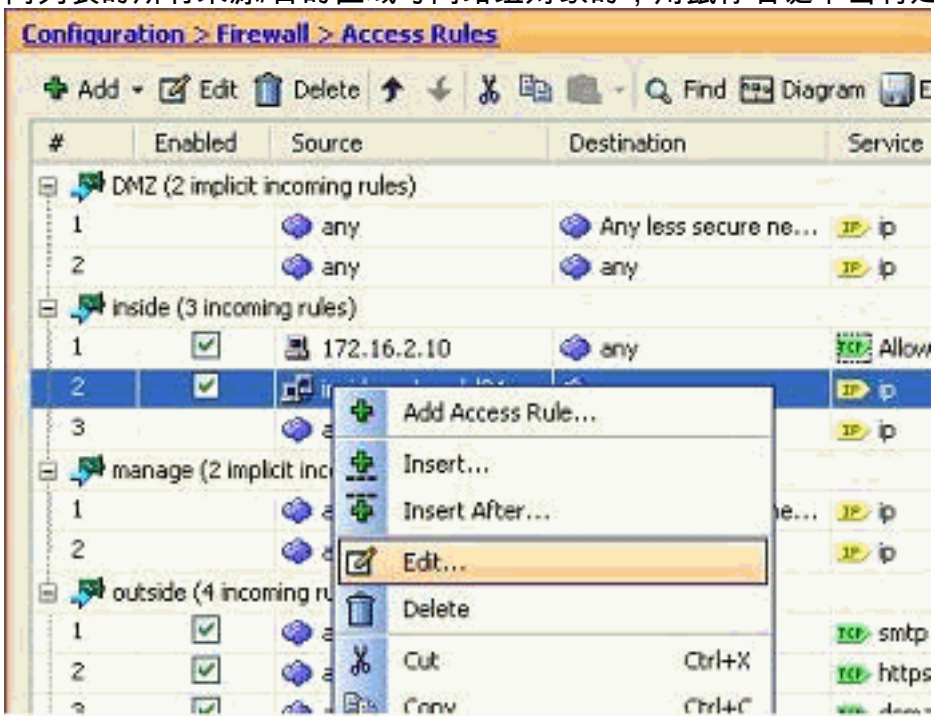
6. 在您添加所有成员分组后，请点击OK键。



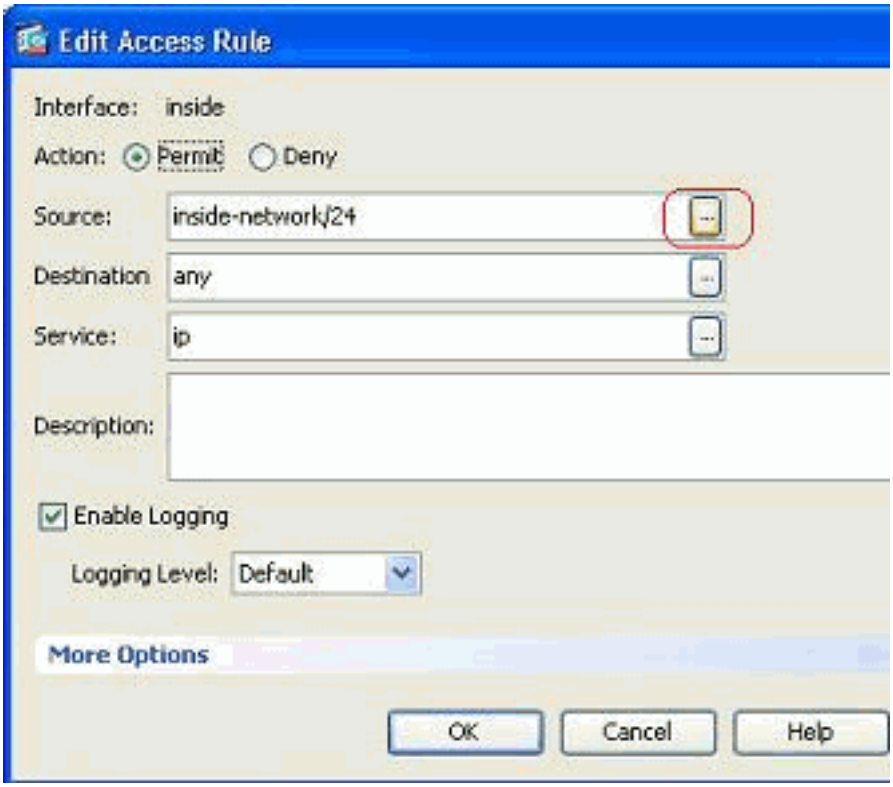


您能当前查看网络对象组。

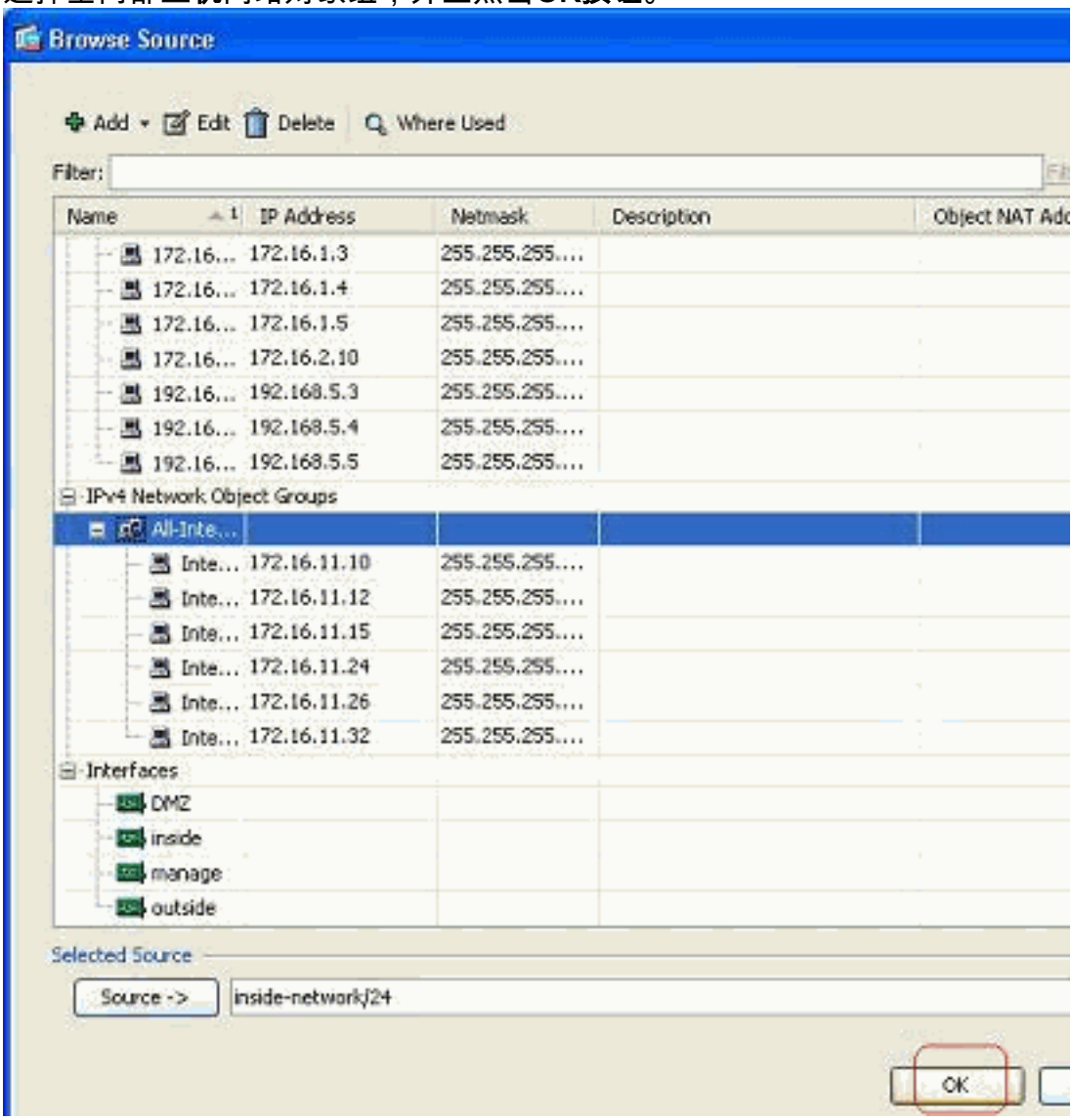
7. 为了修改一个现有的访问列表的所有来源/目的区域与网络组对象的，用鼠标右键单击特定访问规则和选择请**编辑**。



8. 编辑访问规则窗口出现。点击Source字段的**详细信息按钮**为了修改它。

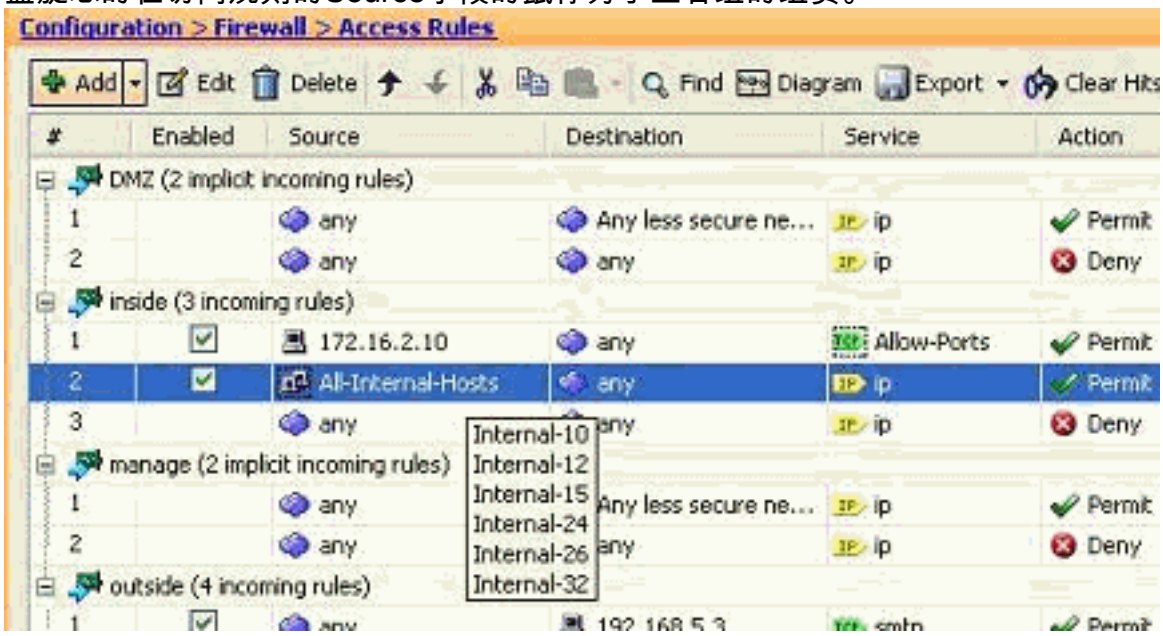


9. 选择全内部**主机**网络对象组，并且点击**OK按钮**。



10. 单击 **Ok**。

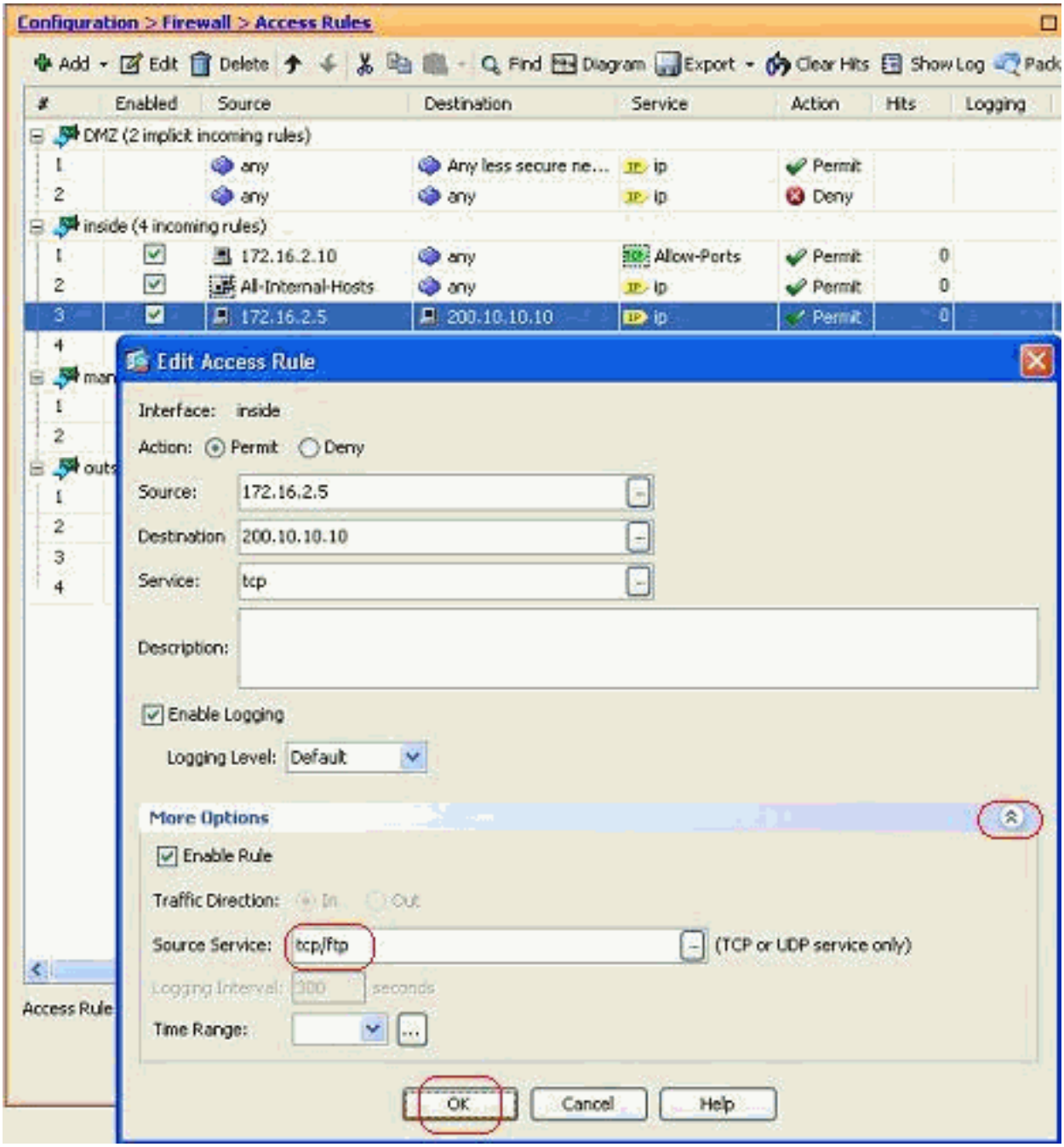
11. 盘旋您的在访问规则的Source字段的鼠标为了查看组的组员。



编辑源端口：

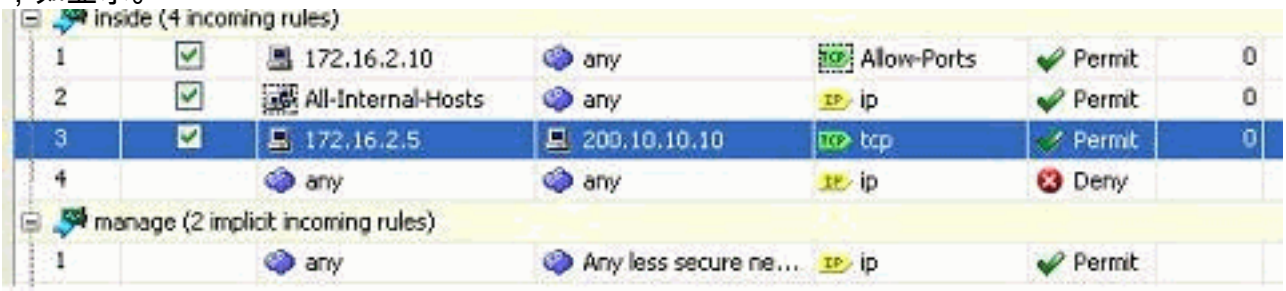
完成这些步骤为了修改访问规则的源端口。

1. 为了修改一个现有访问规则的源端口，用鼠标右键单击它和选择请**编辑**。编辑访问规则窗口出



现。

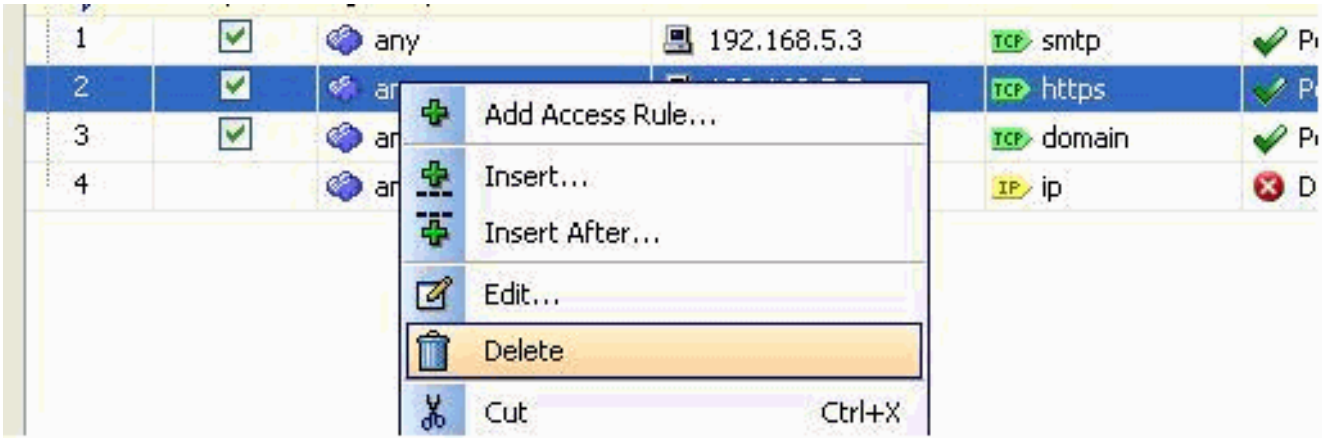
2. 点击**更多选项**下拉式按钮为了修改来源服务字段，并且点击OK键。您能观看已修改访问规则，如显示。



删除访问列表

完成这些步骤为了删除访问列表：

1. 在您删除现有的访问列表前，您需要删除访问列表条目(访问规则)。除非首先删除所有访问规则，删除访问列表是不可能的。用鼠标右键单击访问规则删除，并且选择**删除**。



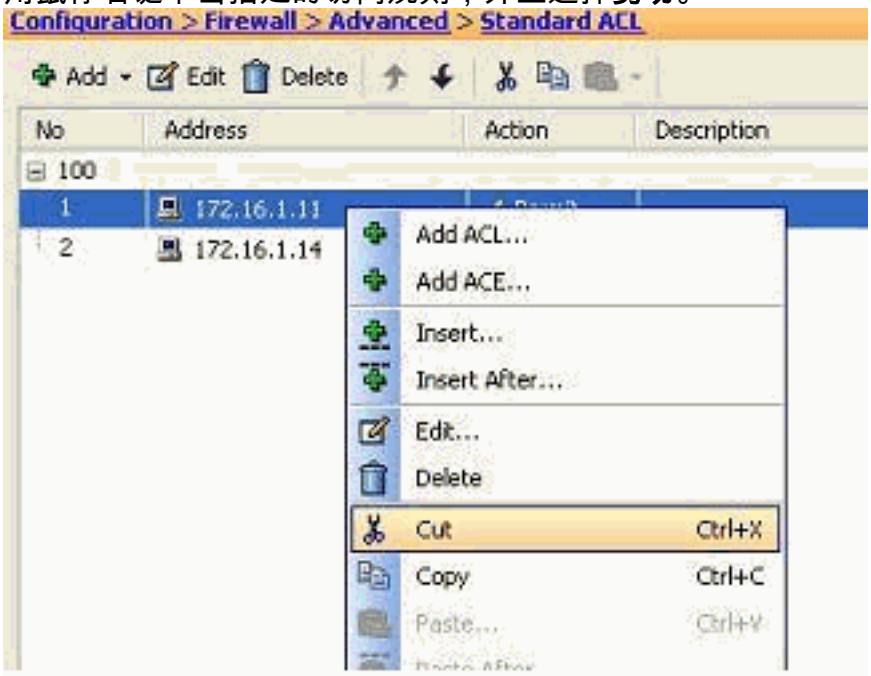
2. 完成在所有现有访问规则的同一删除操作，然后选择访问列表并且选择**删除**为了删除它。

导出访问规则

当ACL Manager跟踪所有扩展访问列表时， ASDM访问规则绑定与各自的接口的访问列表。用ACL Manager创建的访问规则不绑定对任何接口。这些访问列表为NAT-exempt， Vpn过滤器和类似的目的通常使用其他功能没有有接口的地方关联。ACL Manager包含您有在**Configuration>防火墙>Access规则**部分的所有条目。另外， **ACL Manager**也包含没有关联对任何接口的全球访问规则。ASDM被组织，在这种情况下您能容易地导出从所有访问列表的一个访问规则到另一个。

例如，如果需要已经是全球访问规则部分关联与接口的访问规则，您不需要再配置那。反而，您能执行**剪切&粘贴**操作达到此。

1. 用鼠标右键单击指定的访问规则，并且选择**剪切**。



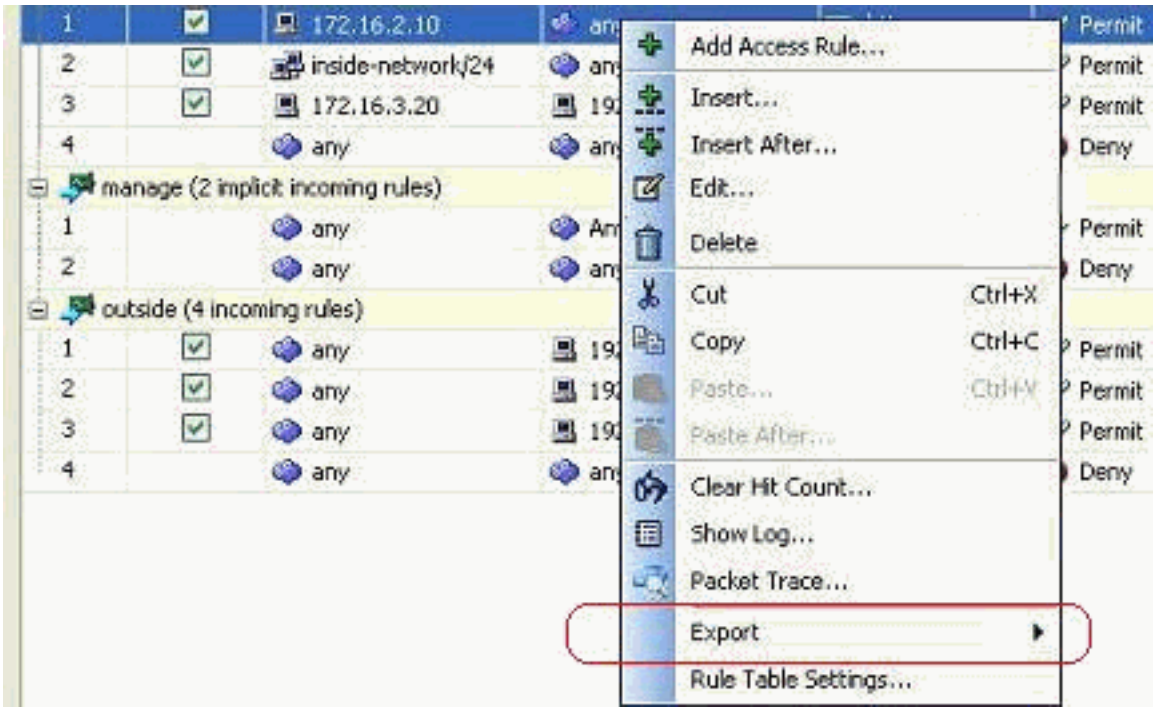
2. 选择您需要插入此访问规则的需要的访问列表。您能使用在工具栏**粘贴**插入访问规则。

导出访问列表信息

您能导出访问列表信息到另一个文件。支持两个格式导出此信息。

1. 逗号分隔的值(CSV)格式
2. HTML格式

用鼠标右键单击其中任一个访问规则，并且选择**出口**为了发送访问列表信息到文件。



这是在HTML格式显示的访问列表信息。

#	Enabled	Source	Destination	Service	Action	Hits	Logging	Time	Description
DMZ (2 incoming rules)									
1	True	172.16.1.10	any	ip	Permit		Default		
2		any	any	ip	Deny		Default		Implicit rule
inside (3 incoming rules)									
1	True	172.16.2.10	any	Allow-Ports	Permit	0	Default		
2	True	All-Internal-Hosts	any	ip	Permit	0	Default		
3		any	any	ip	Deny		Default		Implicit rule
manage (2 implicit incoming rules)									
1		any	Any less secure networks	ip	Permit		Default		Implicit rule: Permit all traffic to less secure networks
2		any	any	ip	Deny		Default		Implicit rule
outside (4 incoming rules)									
1	True	any	192.168.5.3	tcp/smtp	Permit	0	Default		
2	True	any	192.168.5.5	tcp/https	Permit	0	Default		
3	True	any	192.168.5.4	tcp/domain	Permit	0	Default		
4		any	any	ip	Deny		Default		Implicit rule

验证

当前没有可用于此配置的验证过程。

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- ASDM配置示例和TechNotes

- ASA配置示例和Technotes
- 技术支持和文档 - Cisco Systems