ASA 8.X und höher: Konfigurationsbeispiel für die ASDM GUI zum Hinzufügen oder Ändern einer Zugriffsliste

Inhalt

Einführung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Konventionen
Hintergrundinformationen
Konfigurieren
Netzwerkdiagramm
Neue Zugriffsliste hinzufügen
Erstellen einer Standard-Zugriffsliste
Erstellen einer globalen Zugriffsregel
Bearbeiten einer vorhandenen Zugriffsliste
Löschen einer Zugriffsliste
Exportieren der Zugriffsregel
Exportieren der Informationen zur Zugriffsliste
Überprüfen
Fehlerbehebung
Zugehörige Informationen

Einführung

In diesem Dokument wird erläutert, wie Sie den Cisco Adaptive Security Device Manager (ASDM) für die Arbeit mit Zugriffskontrolllisten verwenden können. Dazu gehören die Erstellung einer neuen Zugriffsliste, das Bearbeiten einer vorhandenen Zugriffsliste und anderer Funktionen mit den Zugriffslisten.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Adaptive Security Appliance (ASA) mit Version 8.2.X
- Cisco Adaptive Security Device Manager (ASDM) mit Version 6.3.X

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

Zugriffslisten werden hauptsächlich zur Kontrolle des Datenverkehrsflusses durch die Firewall verwendet. Sie können bestimmte Arten von Datenverkehr mithilfe von Zugriffslisten zulassen oder verweigern. Jede Zugriffsliste enthält eine Reihe von Zugriffslisteneinträgen (ACEs), die den Datenverkehrsfluss von einer bestimmten Quelle zu einem bestimmten Ziel steuern. Normalerweise ist diese Zugriffsliste an eine Schnittstelle gebunden, um die Richtung des Datenflusses zu benachrichtigen, in den sie einsehen soll. Zugriffslisten werden hauptsächlich in zwei große Typen eingeteilt.

1. Eingehende Zugriffslisten
2. Ausgehende Zugriffslisten

Eingehende Zugriffslisten gelten für den Datenverkehr, der in diese Schnittstelle eingeht, und ausgehende Zugriffslisten gelten für den Datenverkehr, der die Schnittstelle verlässt. Die Inbound/Outbound-Notation bezieht sich auf die Richtung des Datenverkehrs in Bezug auf diese Schnittstelle, nicht jedoch auf die Verschiebung des Datenverkehrs zwischen den oberen und unteren Sicherheitsschnittstellen.

Für TCP- und UDP-Verbindungen benötigen Sie keine Zugriffsliste, um zurückkehrenden Verkehr zuzulassen, da die Sicherheits-Appliance den gesamten zurückkehrenden Verkehr für etablierte bidirektionale Verbindungen zulässt. Für verbindungslose Protokolle wie ICMP erstellt die Security Appliance unidirektionale Sitzungen. Sie benötigen daher entweder Zugriffslisten, um Zugriffslisten auf die Quell- und Zielschnittstellen anzuwenden, um ICMP in beide Richtungen zuzulassen, oder Sie müssen die ICMP-Prüfungs-Engine aktivieren. Die ICMP Inspection Engine behandelt ICMP-Sitzungen als bidirektionale Verbindungen.

Von der ASDM-Version 6.3.X gibt es zwei Arten von Zugriffslisten, die Sie konfigurieren können.

1. Schnittstellenzugriffsregeln
2. Globale Zugriffsregeln

Hinweis: Die Zugriffsregel bezieht sich auf einen einzelnen Eintrag in der Zugriffsliste (ACE).

Schnittstellenzugriffsregeln sind zum Zeitpunkt ihrer Erstellung an jede Schnittstelle gebunden. Ohne sie an eine Schnittstelle zu binden, können Sie sie nicht erstellen. Dies unterscheidet sich vom Beispiel für die Befehlszeile. Mit der CLI erstellen Sie zunächst die Zugriffsliste mit dem

Befehl **access list** und binden diese Zugriffsliste dann an eine Schnittstelle mit dem Befehl **access-group**. ASDM 6.3 und höher wird die Zugriffsliste erstellt und als einzelne Aufgabe an eine Schnittstelle gebunden. Dies gilt nur für den Datenverkehr, der durch diese spezifische Schnittstelle fließt.

Globale Zugriffsregeln sind nicht an eine Schnittstelle gebunden. Sie können über die Registerkarte "ACL Manager" (ACL-Manager) im ASDM konfiguriert und auf den globalen eingehenden Datenverkehr angewendet werden. Sie werden implementiert, wenn eine Übereinstimmung basierend auf der Quelle, dem Ziel und dem Protokolltyp vorliegt. Diese Regeln werden nicht auf jeder Schnittstelle repliziert, sodass Speicherplatz eingespart wird.

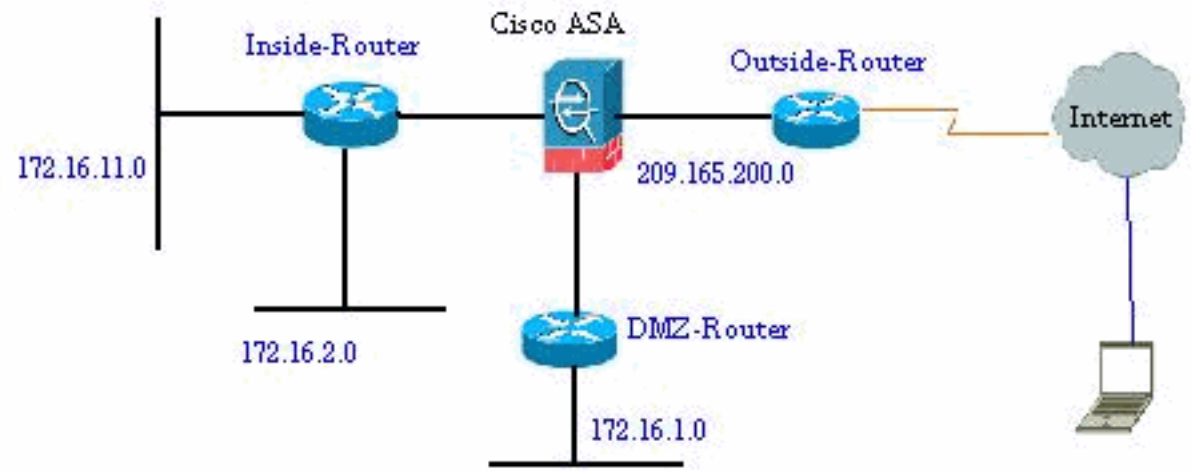
Wenn beide Regeln implementiert werden sollen, haben Schnittstellenzugriffsregeln in der Regel Vorrang vor den globalen Zugriffsregeln.

Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Netzwerkdiagramm

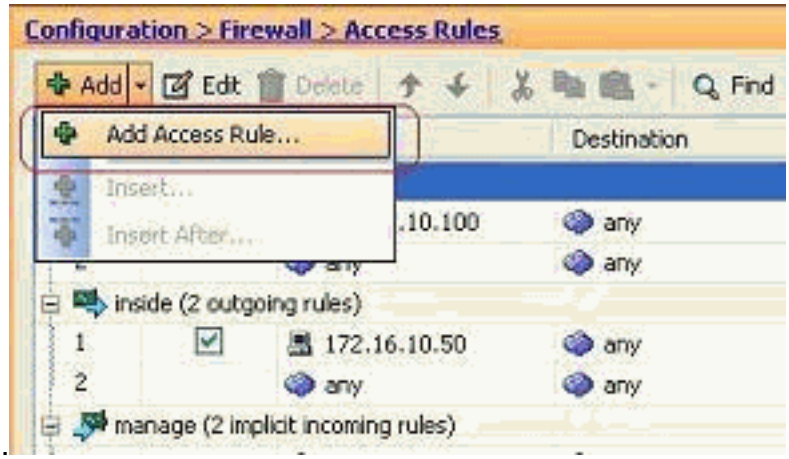
In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Neue Zugriffsliste hinzufügen

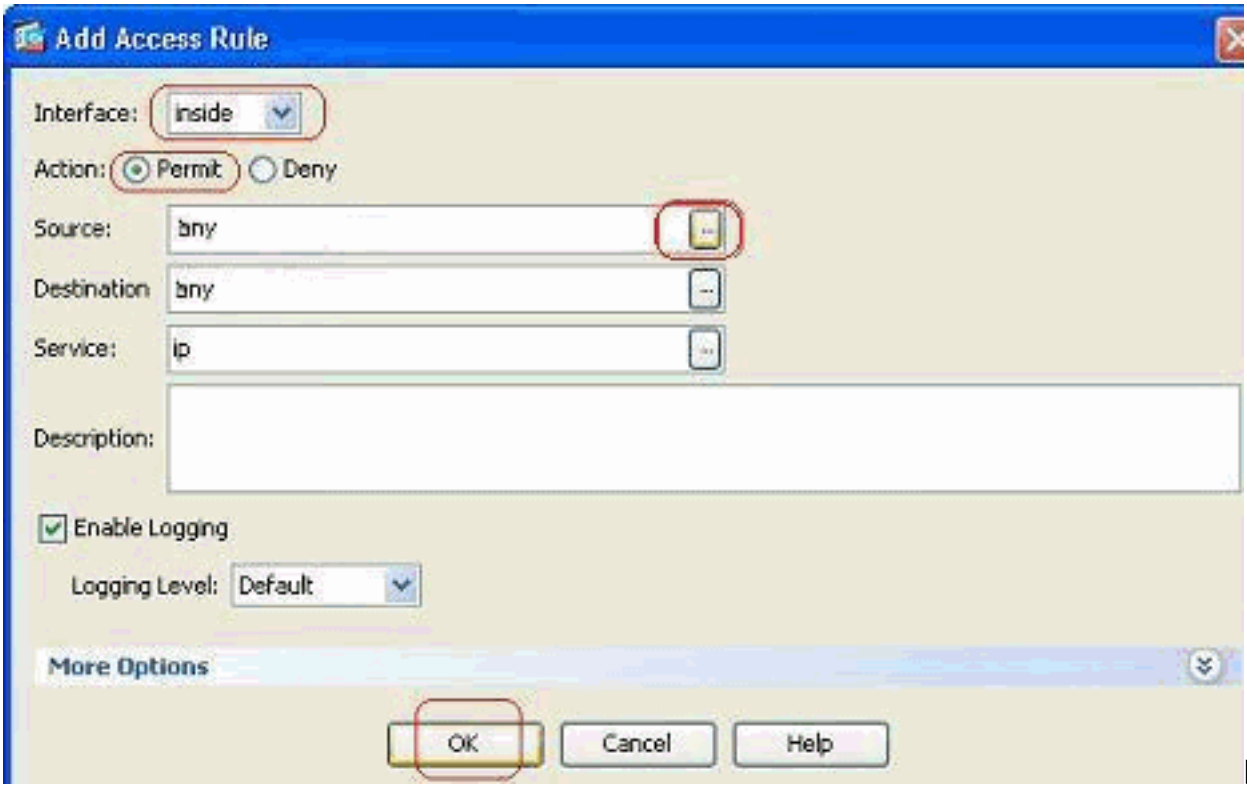
Gehen Sie wie folgt vor, um eine neue Zugriffsliste mit ASDM zu erstellen:

1. Wählen Sie **Konfiguration > Firewall > Zugriffsregeln**, und klicken Sie auf die Schaltfläche



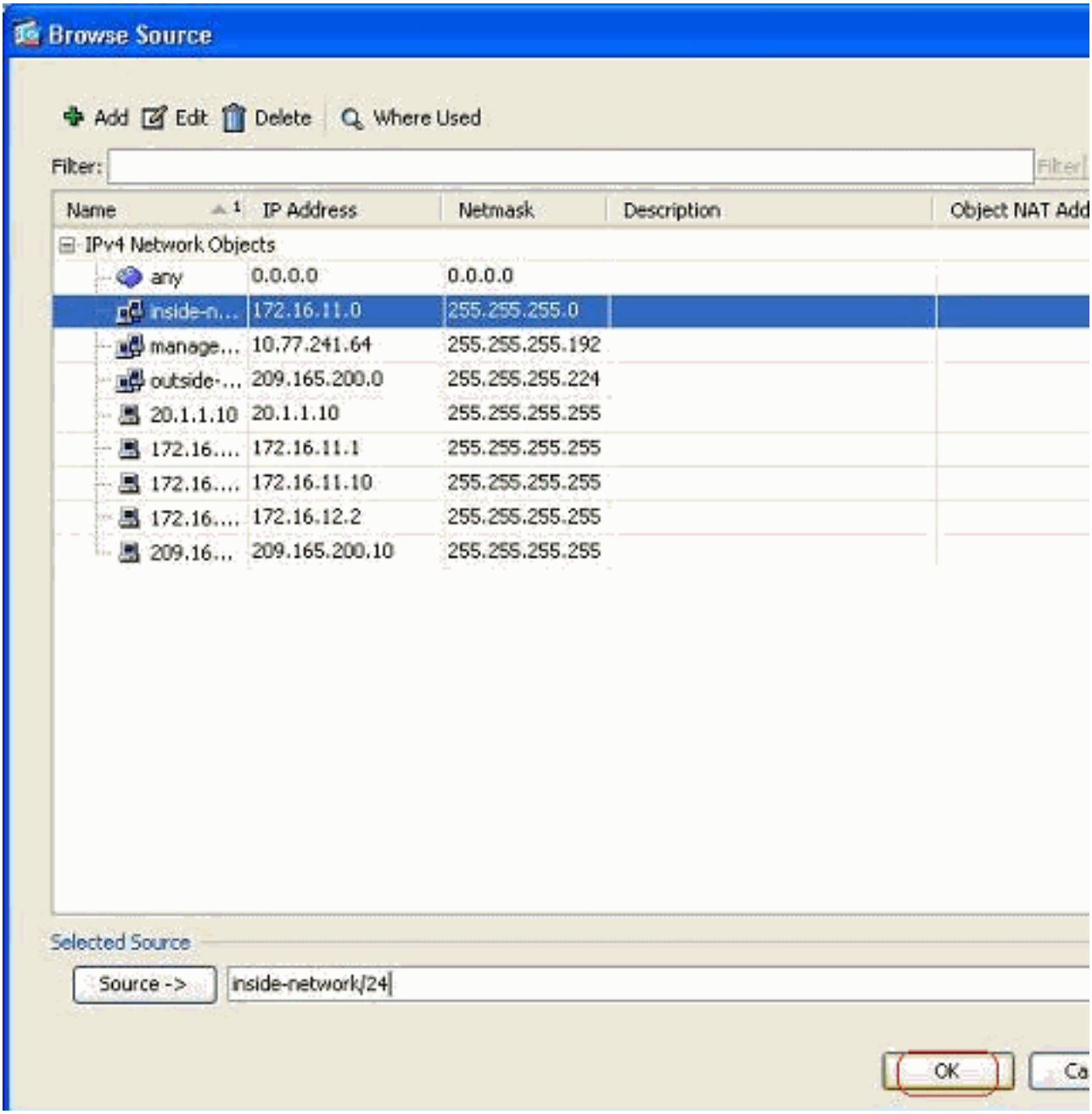
Zugriffsregel hinzufügen.

2. Wählen Sie die Schnittstelle aus, an die diese Zugriffsliste gebunden werden soll, zusammen mit der Aktion, die für den Datenverkehr ausgeführt werden soll, d. h. Zulassen/Verweigern. Klicken Sie dann auf die Schaltfläche **Details**, um das Quellnetzwerk auszuwählen.

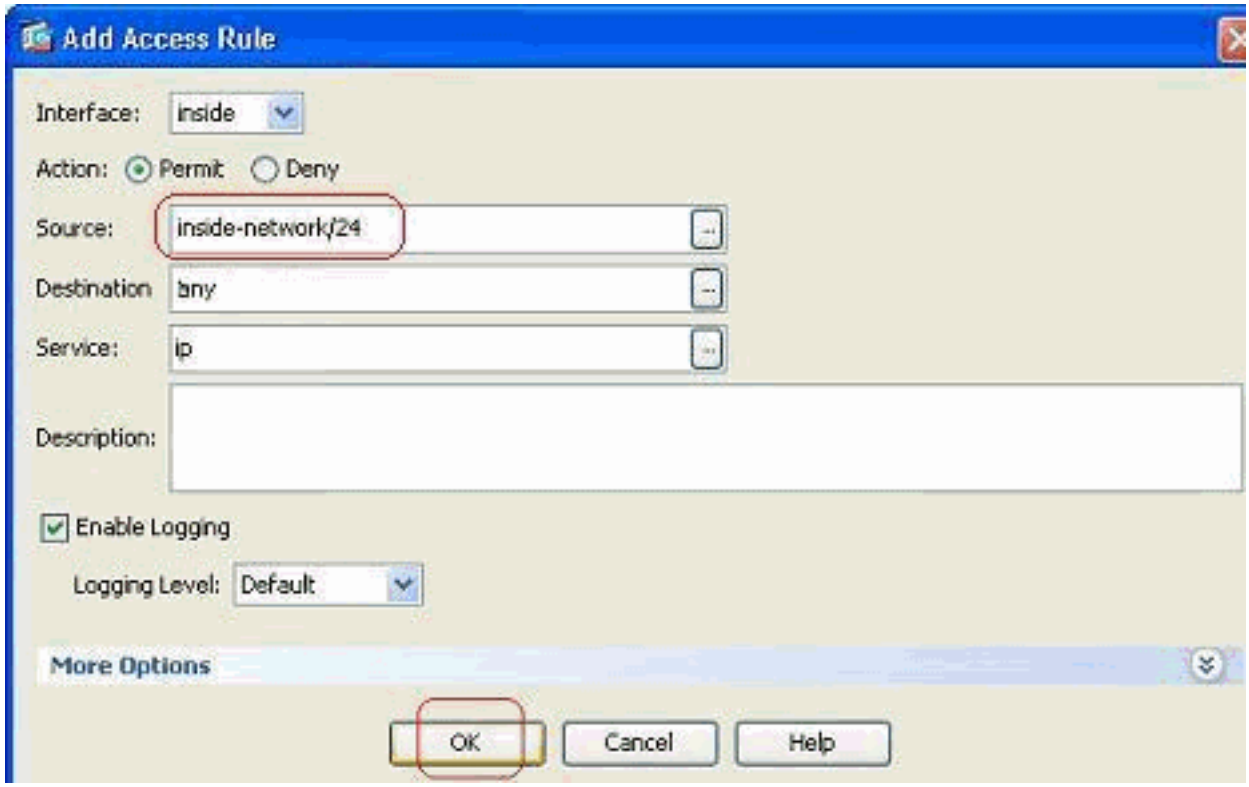


Hinweis: Im Folgenden werden die verschiedenen Felder, die in diesem Fenster angezeigt werden, kurz erläutert:**Interface** (Schnittstelle): Bestimmt die Schnittstelle, an die diese Zugriffsliste gebunden ist.**Action** (Aktion): Bestimmt den Aktionstyp der neuen Regel. Es stehen zwei Optionen zur Verfügung. **Zulassen** erlaubt den gesamten übereinstimmenden Datenverkehr und **Verweigern** blockiert den gesamten übereinstimmenden Datenverkehr.**Source (Quelle)**: Dieses Feld gibt die Quelle des Datenverkehrs an. Dabei kann es sich um alles unter einer einzigen IP-Adresse, einem Netzwerk, einer IP-Adresse der Schnittstelle der Firewall oder einer Netzwerkobjektgruppe handeln. Diese können mit der Schaltfläche **Details** ausgewählt werden.**Destination** (Ziel): Dieses Feld gibt die Quelle des Datenverkehrs an. Dabei kann es sich um alles unter einer einzigen IP-Adresse, einem Netzwerk, einer IP-Adresse der Schnittstelle der Firewall oder einer Netzwerkobjektgruppe handeln. Diese können mit der Schaltfläche **Details** ausgewählt werden.**Service**: Dieses Feld bestimmt das Protokoll oder den Service des Datenverkehrs, auf den diese Zugriffsliste angewendet wird. Sie können auch eine Dienstgruppe definieren, die verschiedene Protokolle enthält.

3. Nachdem Sie auf die Schaltfläche **Details** geklickt haben, wird ein neues Fenster mit den vorhandenen Netzwerkobjekten angezeigt. Wählen Sie das **interne Netzwerk aus**, und klicken Sie auf **OK**.

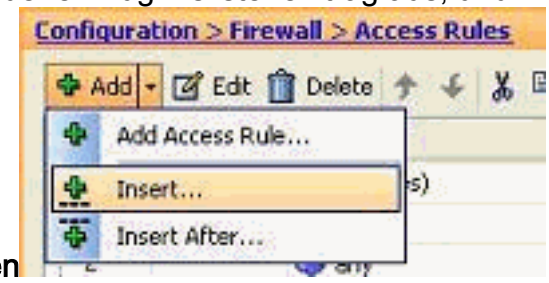


4. Sie kehren zum Fenster **Zugriffsregel hinzufügen zurück**. Geben Sie **any** im Feld Ziel ein. und klicken Sie auf **OK**, um die Konfiguration der Zugriffsregel abzuschließen.

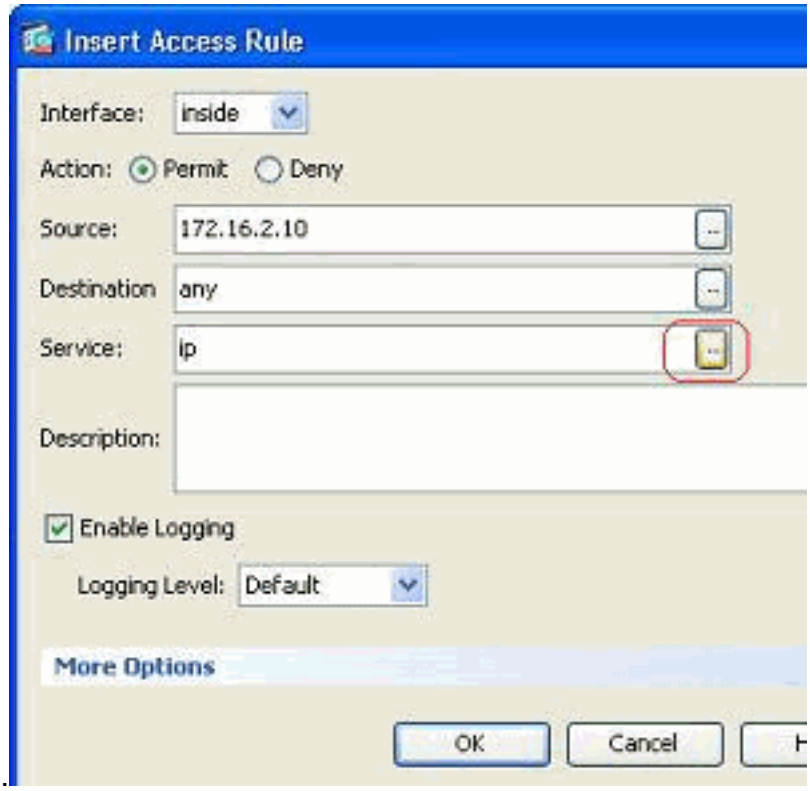


Hinzufügen einer Zugriffsregel vor einer vorhandenen:

Gehen Sie wie folgt vor, um kurz vor einer bereits bestehenden Zugriffsregel eine Zugriffsregel hinzuzufügen:

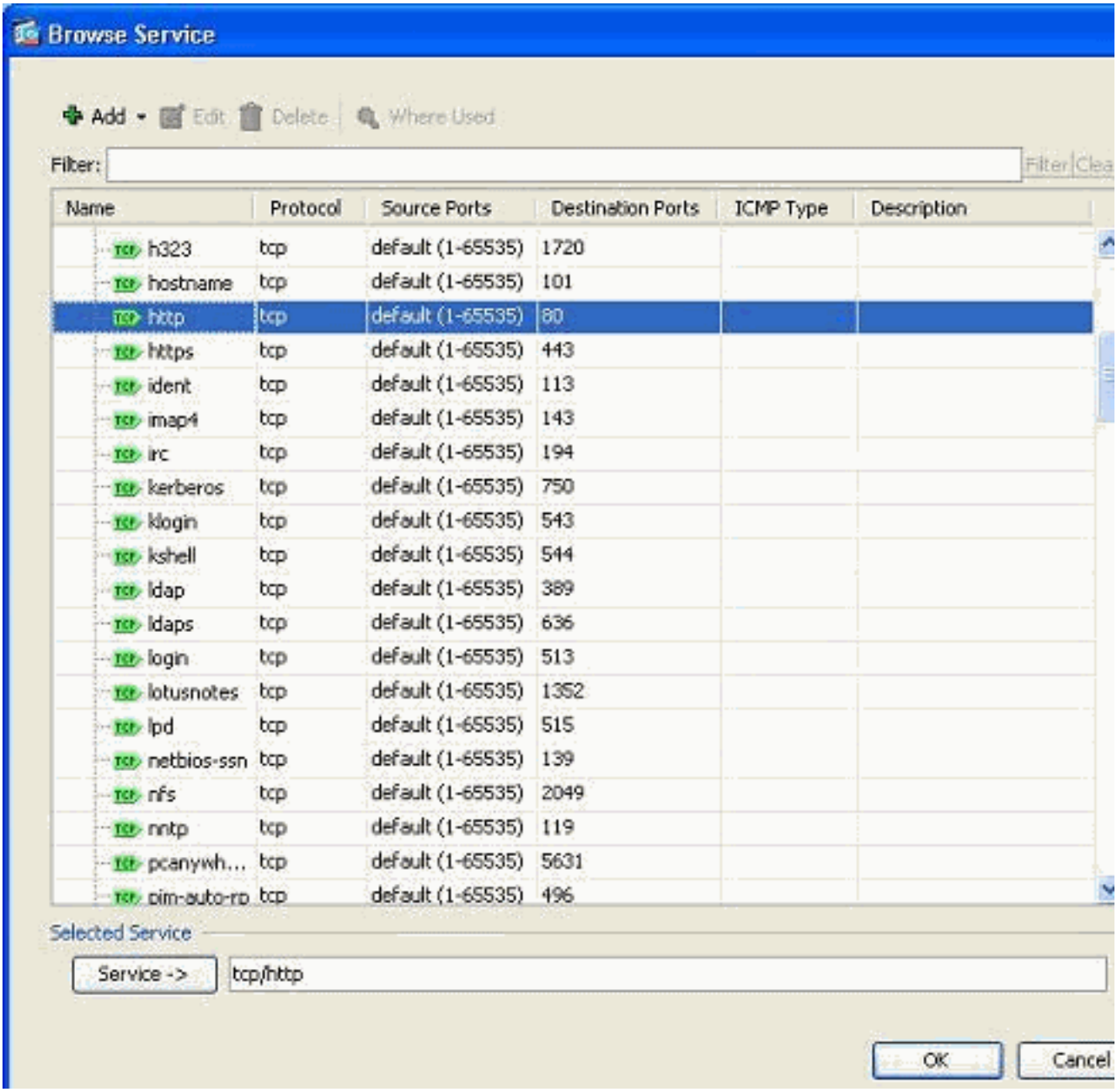
1. Wählen Sie den vorhandenen Zugriffslisteneintrag aus, und klicken Sie im Dropdown-Menü 

Hinzufügen auf **Einfügen**
2. Wählen Sie Quelle und Ziel aus, und klicken Sie auf die Schaltfläche **Details** im Feld Service,



um das Protokoll auszuwählen.

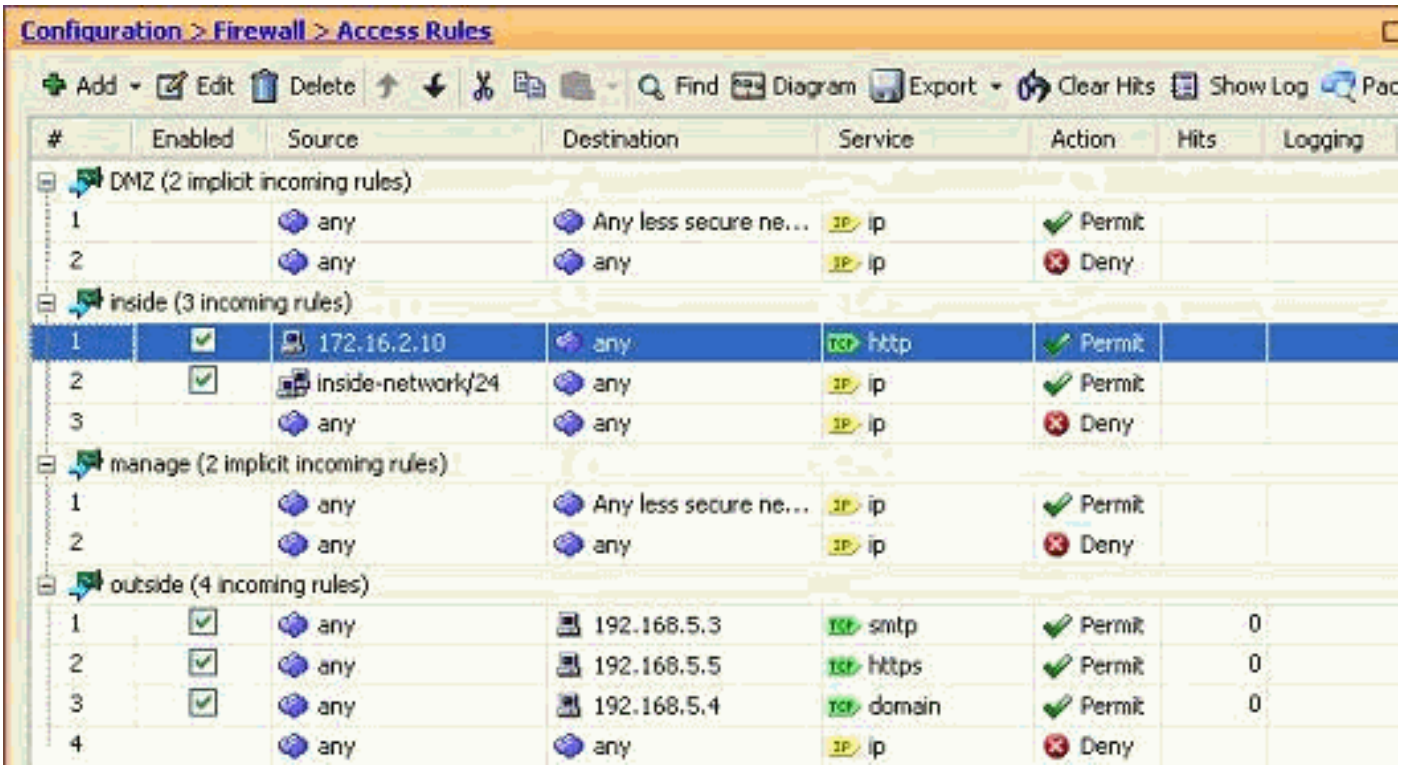
3. Wählen Sie HTTP als Protokoll aus, und klicken Sie auf **OK**.



4. Sie kehren zum Fenster Zugriffsregel einfügen zurück. Das Feld Service wird mit **tcp/http** als ausgewähltem Protokoll gefüllt. Klicken Sie auf **OK**, um die Konfiguration des neuen

Zugriffslisteneintrags abzuschließen.

Sie können jetzt die neue Zugriffsregel beobachten, die kurz vor dem bereits vorhandenen Eintrag für das Inside-Netzwerk angezeigt wird.

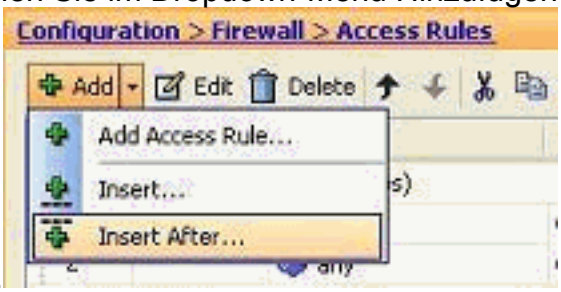


Hinweis: Die Reihenfolge der Zugriffsregeln ist sehr wichtig. Bei der Verarbeitung jedes Pakets zum Filtern prüft die ASA, ob das Paket einem der Kriterien für Zugriffsregeln in sequenzieller Reihenfolge entspricht und ob eine Übereinstimmung vorliegt, die Aktion dieser Zugriffsregel implementiert wird. Wenn eine Zugriffsregel zugeordnet wird, werden keine weiteren Zugriffsregeln angewendet und erneut überprüft.

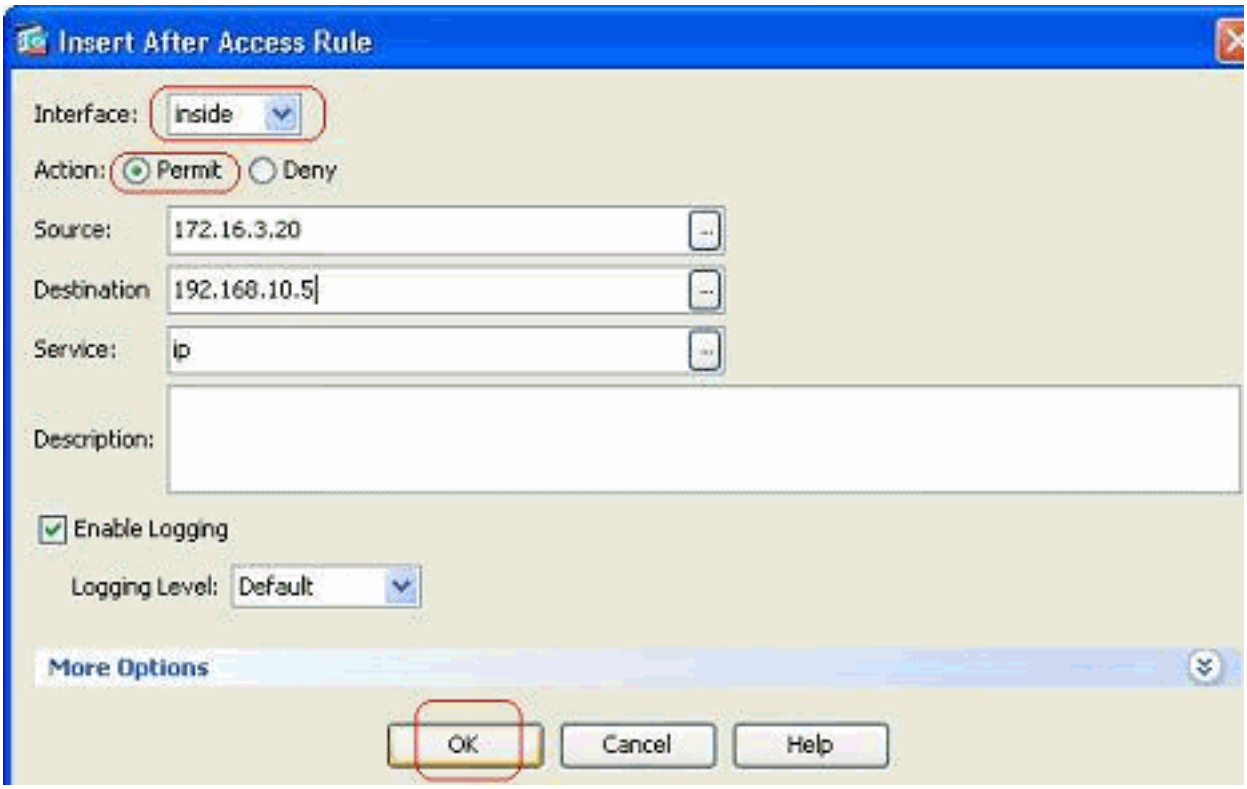
Hinzufügen einer Zugriffsregel nach einer vorhandenen:

Führen Sie diese Schritte aus, um unmittelbar nach einer bereits bestehenden Zugriffsregel eine Zugriffsregel zu erstellen.

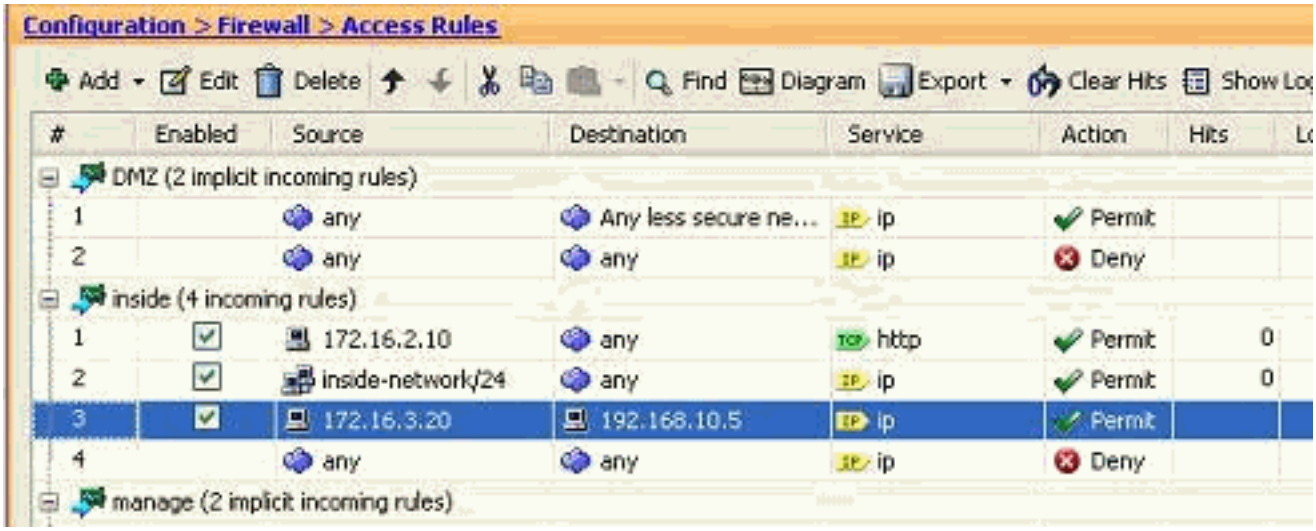
1. Wählen Sie die Zugriffsregel aus, nach der Sie eine neue Zugriffsregel benötigen, und wählen Sie im Dropdown-Menü Hinzufügen die Option **Einfügen** aus.



2. Geben Sie die Felder Interface (Schnittstelle), Action (Aktion), Source (Quelle), Destination (Ziel) und Service (Dienst) an, und klicken Sie auf **OK**, um die Konfiguration dieser Zugriffsregel abzuschließen.

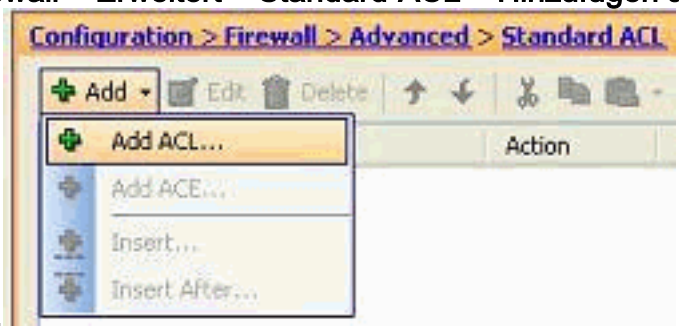


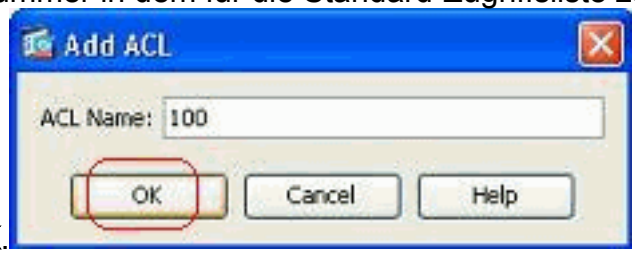
Sie können sehen, dass die neu konfigurierte Zugriffsregel direkt nach der bereits konfigurierten Zugriffsregel angeordnet ist.

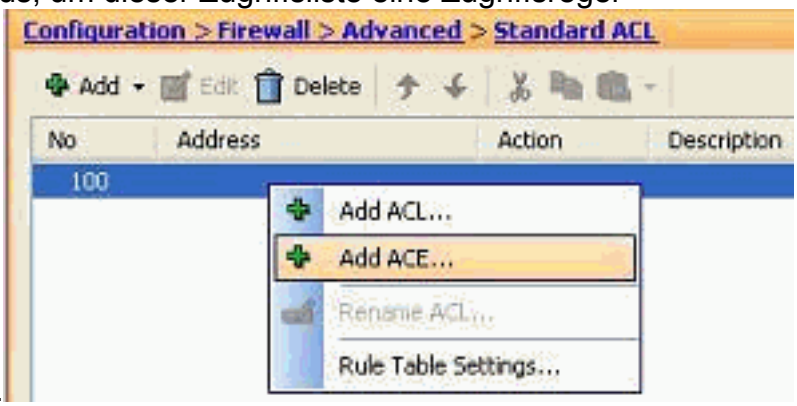


Erstellen einer Standard-Zugriffsliste

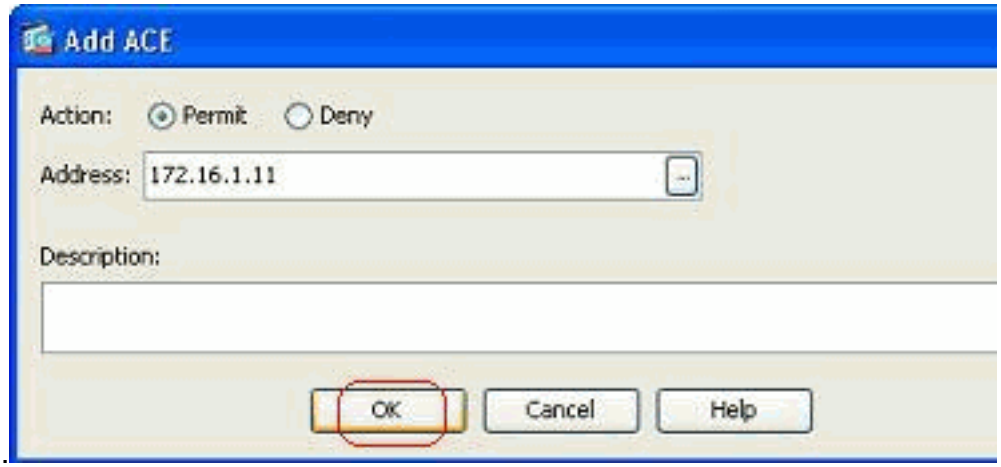
Führen Sie diese Schritte aus, um eine Standard-Zugriffsliste mit der ASDM-GUI zu erstellen.

1. Wählen Sie **Konfiguration > Firewall > Erweitert > Standard-ACL > Hinzufügen aus**, und klicken Sie auf **ACL hinzufügen**.


2. Geben Sie eine Nummer in dem für die Standard-Zugriffsliste zulässigen Bereich an, und klicken Sie auf **OK**.


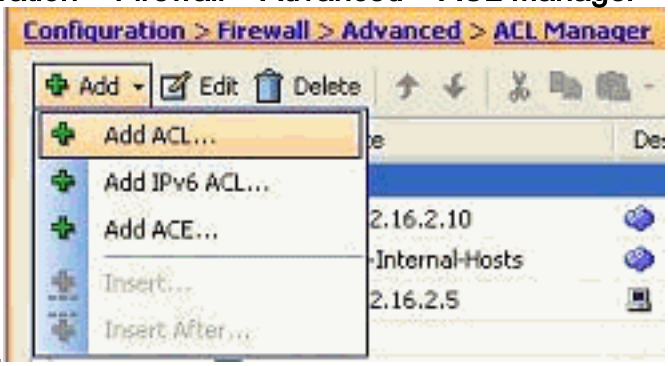
3. Klicken Sie mit der rechten Maustaste auf die Zugriffsliste, und wählen Sie **Add ACE (ACE hinzufügen)** aus, um dieser Zugriffsliste eine Zugriffsregel hinzuzufügen.


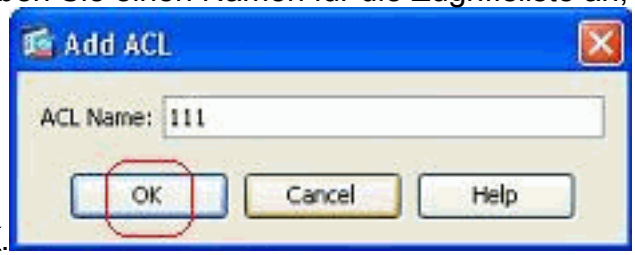
4. Wählen Sie die **Aktion aus**, und geben Sie die **Quelladresse an**. Geben Sie bei Bedarf auch die **Beschreibung an**. Klicken Sie auf **OK**, um die Konfiguration der Zugriffsregel

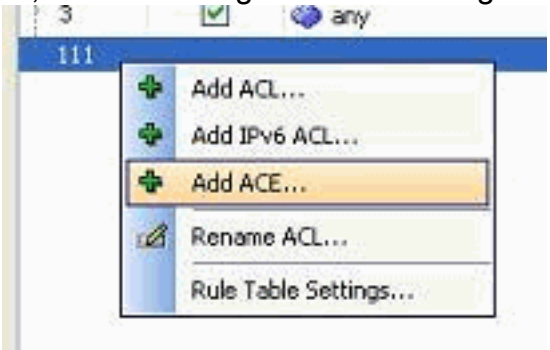
abzuschließen. 

Erstellen einer globalen Zugriffsregel

Führen Sie diese Schritte aus, um eine erweiterte Zugriffsliste mit globalen Zugriffsregeln zu erstellen.

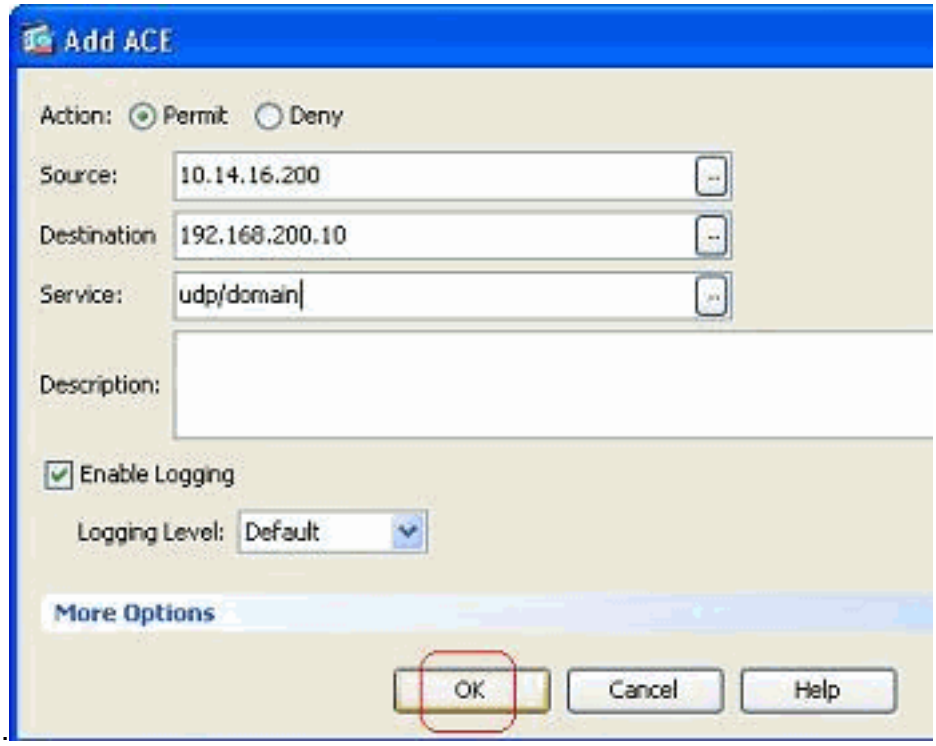
1. Wählen Sie **Configuration > Firewall > Advanced > ACL Manager > Add** aus, und klicken Sie auf **Add ACL** button. 

2. Geben Sie einen Namen für die Zugriffsliste an, und klicken Sie auf **OK**. 

3. Klicken Sie mit der rechten Maustaste auf die Zugriffsliste, und wählen Sie **Add ACE (ACE hinzufügen**) aus, um dieser Zugriffsliste eine Zugriffsregel hinzuzufügen. 

4. Füllen Sie die Felder Aktion, Quelle, Ziel und Service aus, und klicken Sie auf **OK**, um die Konfiguration der globalen Zugriffsregel

abzuschließen.



Sie können jetzt, wie gezeigt, die globale Zugriffsregel anzeigen.

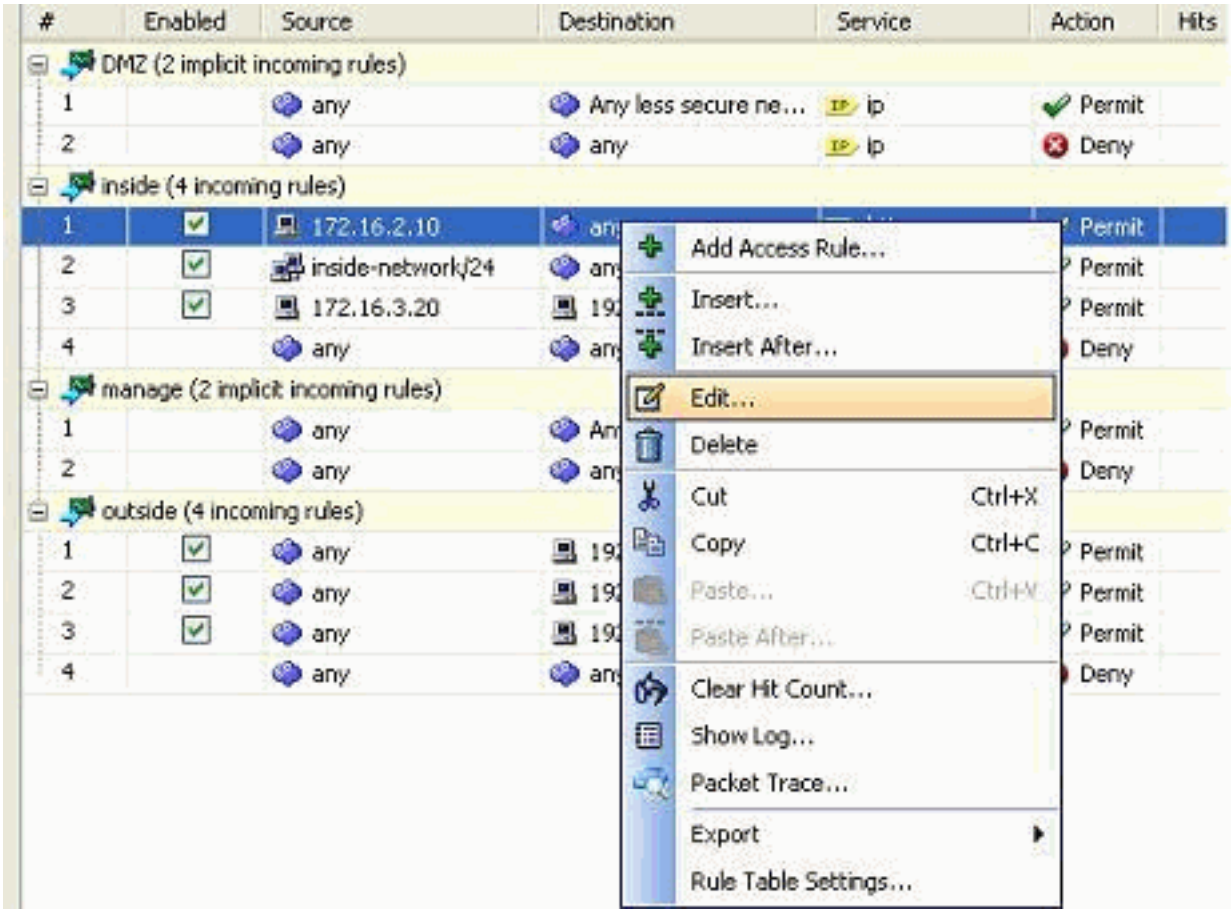
Bearbeiten einer vorhandenen Zugriffsliste

In diesem Abschnitt wird erläutert, wie ein vorhandener Zugriff bearbeitet wird.

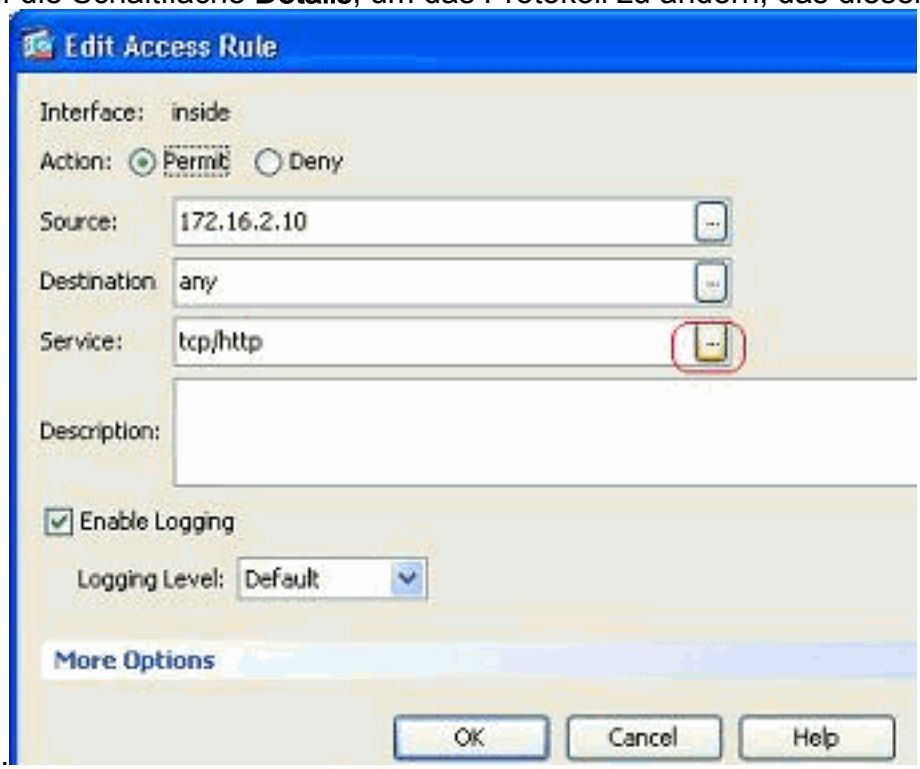
Bearbeiten Sie das Feld Protokoll, um eine Servicegruppe zu erstellen:

Führen Sie diese Schritte aus, um eine neue Servicegruppe zu erstellen.

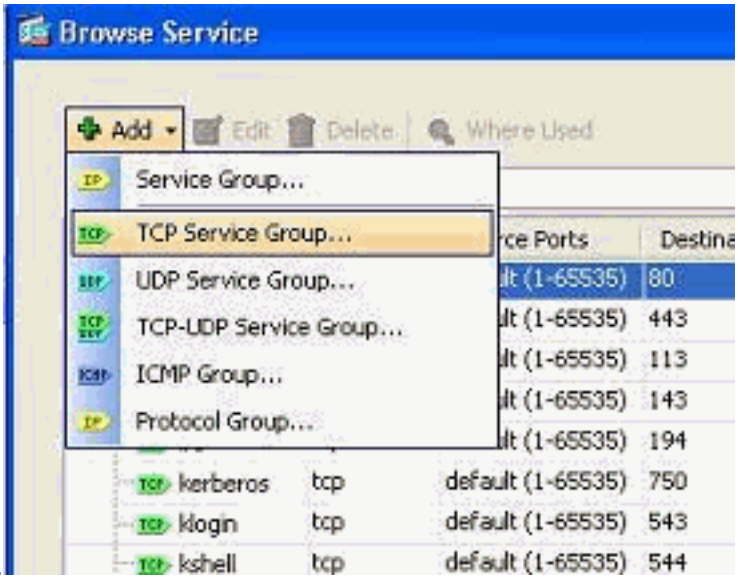
1. Klicken Sie mit der rechten Maustaste auf die Zugriffsregel, die geändert werden muss, und wählen Sie **Bearbeiten** aus, um diese Zugriffsregel zu ändern.



2. Klicken Sie auf die Schaltfläche **Details**, um das Protokoll zu ändern, das dieser Zugriffsregel zugeordnet ist.

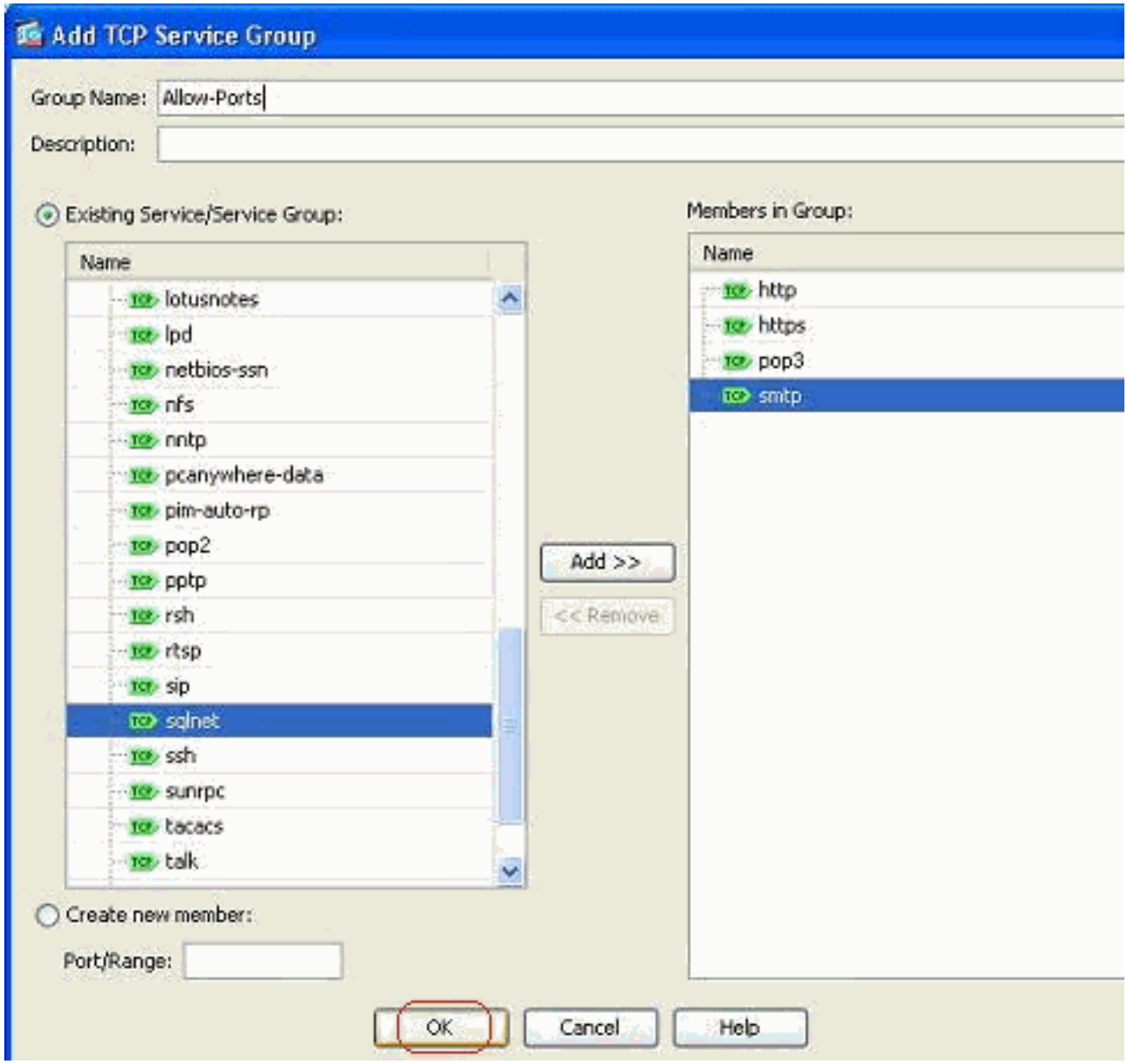


3. Sie können bei Bedarf ein anderes Protokoll als HTTP auswählen. Wenn nur ein Protokoll ausgewählt werden soll, muss die Servicegruppe nicht erstellt werden. Es empfiehlt sich, eine Servicegruppe zu erstellen, wenn eine Anforderung besteht, zahlreiche nicht benachbarte Protokolle zu identifizieren, die dieser Zugriffsregel zugeordnet werden sollen.Wählen Sie **Add > TCP service group**, um eine neue TCP service group zu erstellen.**Hinweis:** Auf dieselbe Weise können Sie auch eine neue UDP-Servicegruppe oder

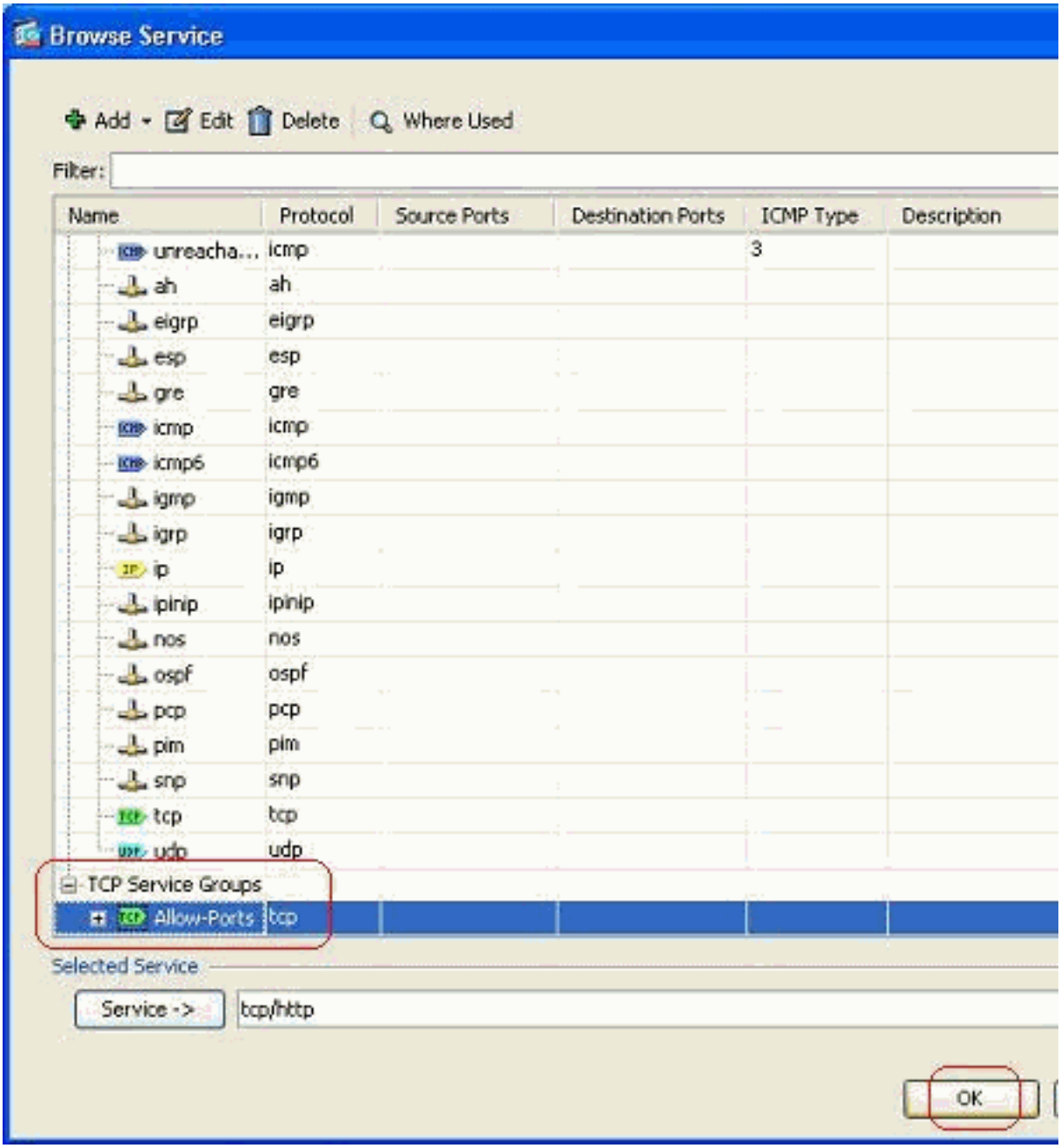


eine ICMP-Gruppe usw. erstellen.

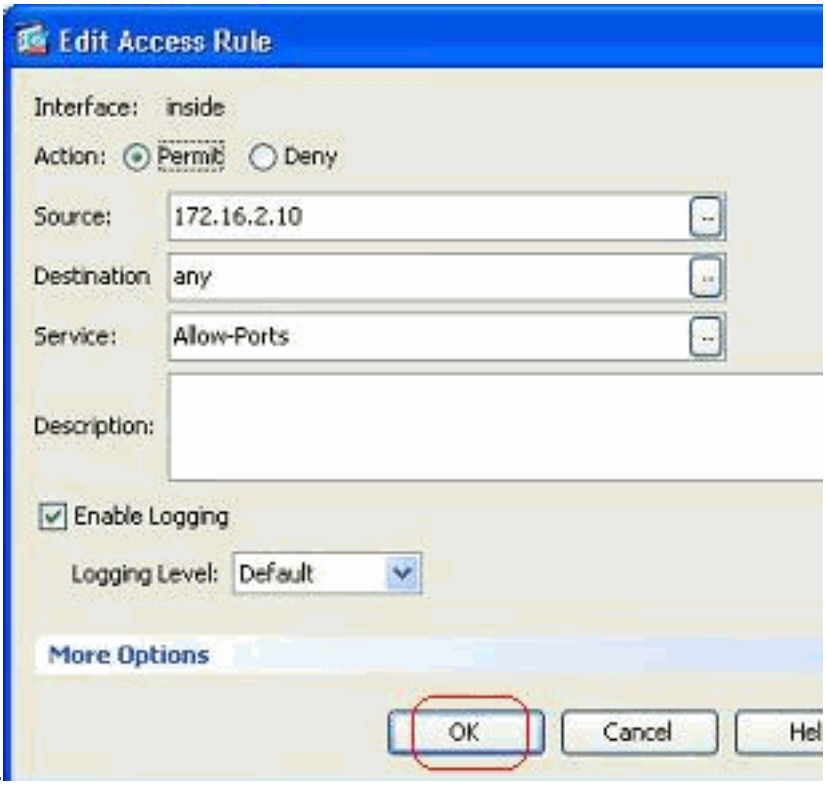
4. Geben Sie einen Namen für diese Servicegruppe an, wählen Sie das Protokoll auf der linken Seite aus, und klicken Sie auf **Hinzufügen**, um sie im Menü Gruppe auf der rechten Seite in das Menü Mitglieder zu verschieben. Je nach Anforderung können mehrere Protokolle als Mitglieder einer Servicegruppe hinzugefügt werden. Die Protokolle werden einzeln hinzugefügt. Nachdem alle Mitglieder hinzugefügt wurden, klicken Sie auf **OK**.



5. Die neu erstellte Servicegruppe kann unter der Registerkarte **TCP-Servicegruppen** angezeigt werden. Klicken Sie auf **OK**, um zum Fenster Zugriffsregel bearbeiten zurückzukehren.

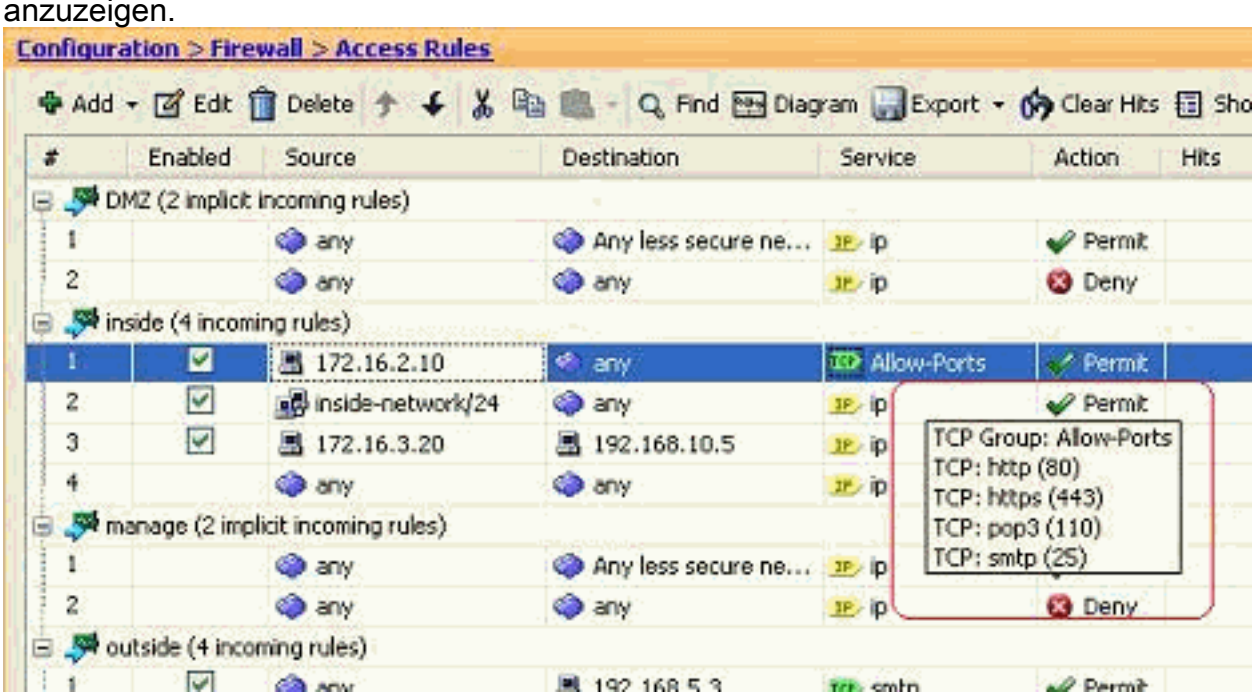


6. Sie sehen, dass das Feld "Service" mit der neu erstellten Servicegruppe ausgefüllt wird. Klicken Sie auf **OK**, um die Bearbeitung



abzuschließen.

7. Bewegen Sie den Mauszeiger über diese Servicegruppe, um alle zugehörigen Protokolle anzuzeigen.

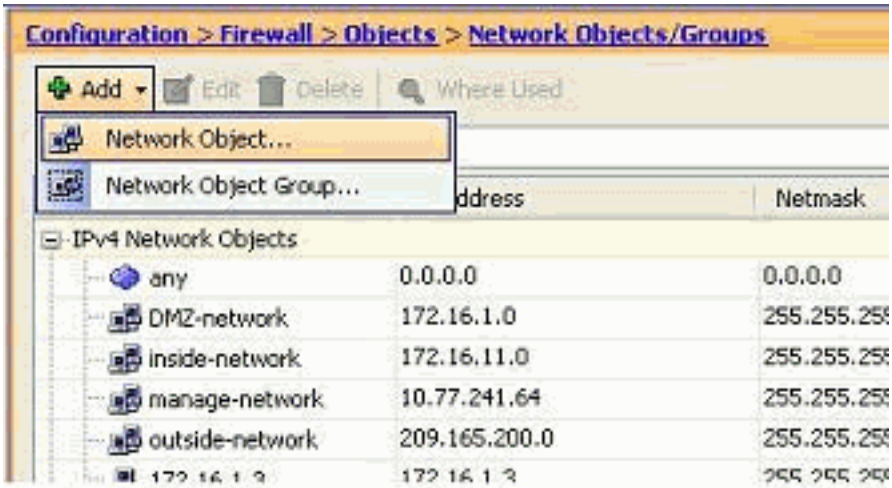


Bearbeiten Sie die Felder Quelle/Ziel, um eine Netzwerkobjektgruppe zu erstellen:

Objektgruppen werden verwendet, um die Erstellung und Pflege von Zugriffslisten zu vereinfachen. Wenn Sie Objekte wie Objekte gruppieren, können Sie die Objektgruppe in einem einzigen ACE verwenden, anstatt einen ACE für jedes Objekt einzeln eingeben zu müssen. Bevor Sie die Objektgruppe erstellen, müssen Sie die Objekte erstellen. In der ASDM-Terminologie wird das Objekt als Netzwerkobjekt und die Objektgruppe als Netzwerkobjektgruppe bezeichnet.

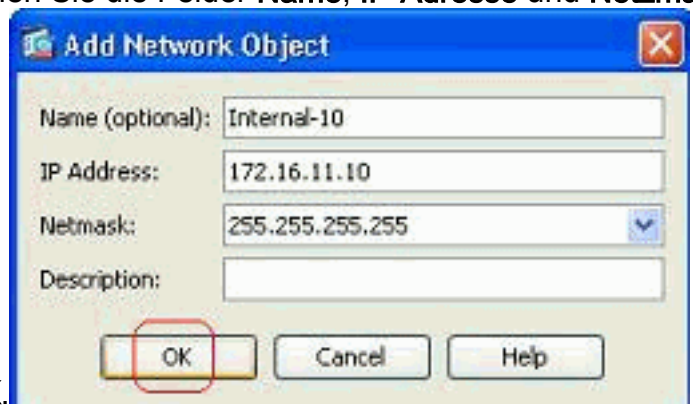
Gehen Sie wie folgt vor:

1. Wählen Sie **Konfiguration > Firewall > Objekte > Netzwerkobjekte/Gruppen > Hinzufügen aus**, und klicken Sie auf **Netzwerkobjekt**, um ein neues Netzwerkobjekt zu

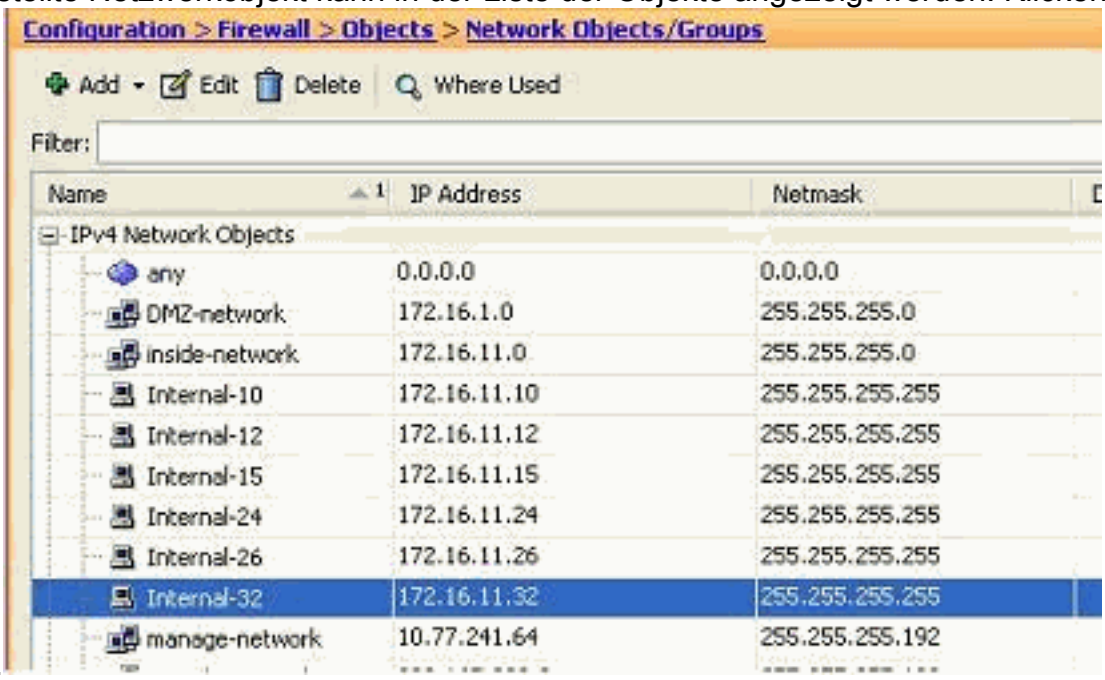


erstellen.

2. Füllen Sie die Felder **Name**, **IP-Adresse** und **Netzmaske aus**, und klicken Sie auf **OK**.



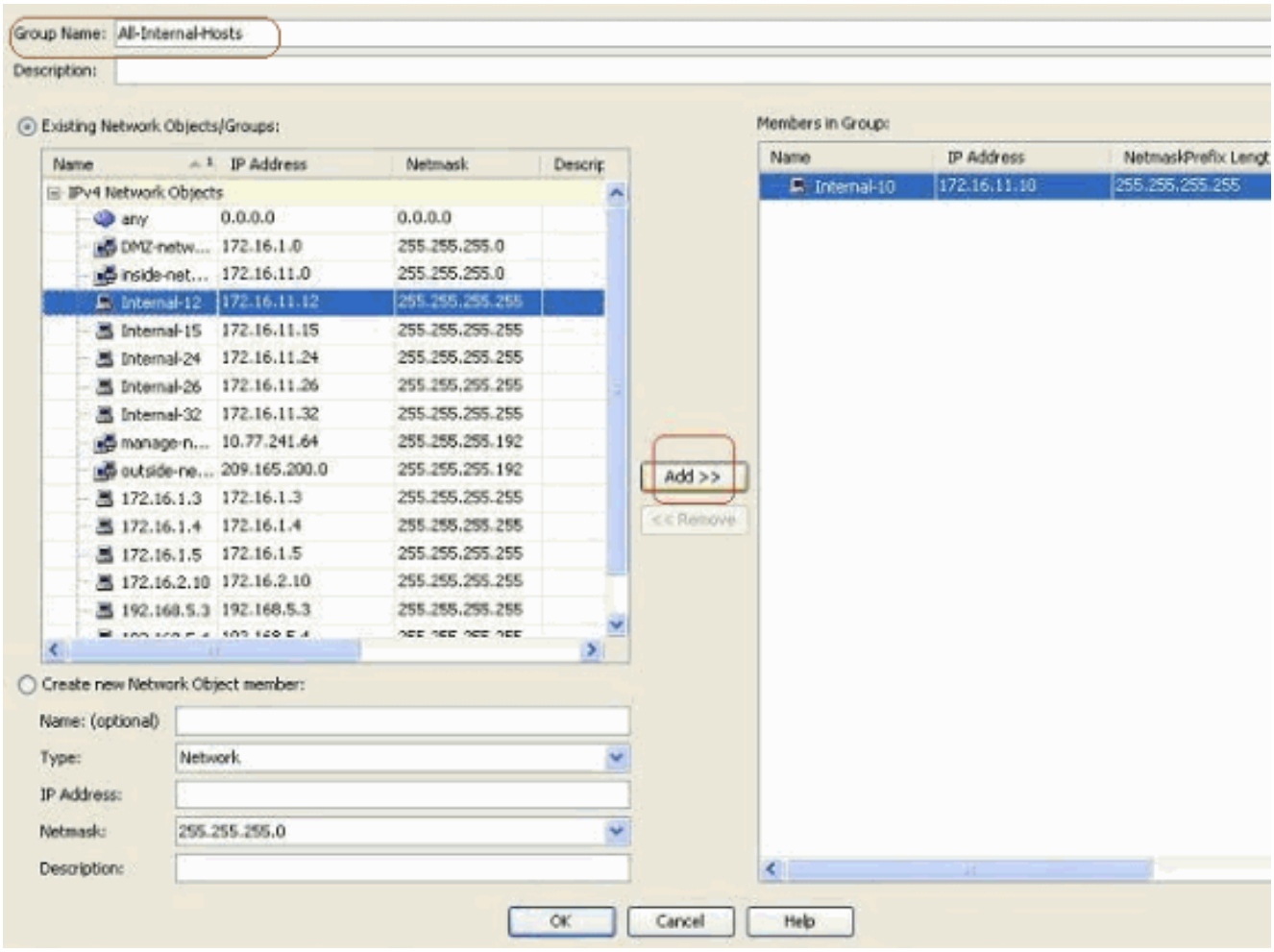
3. Das neu erstellte Netzwerkobjekt kann in der Liste der Objekte angezeigt werden. Klicken Sie auf **OK**.



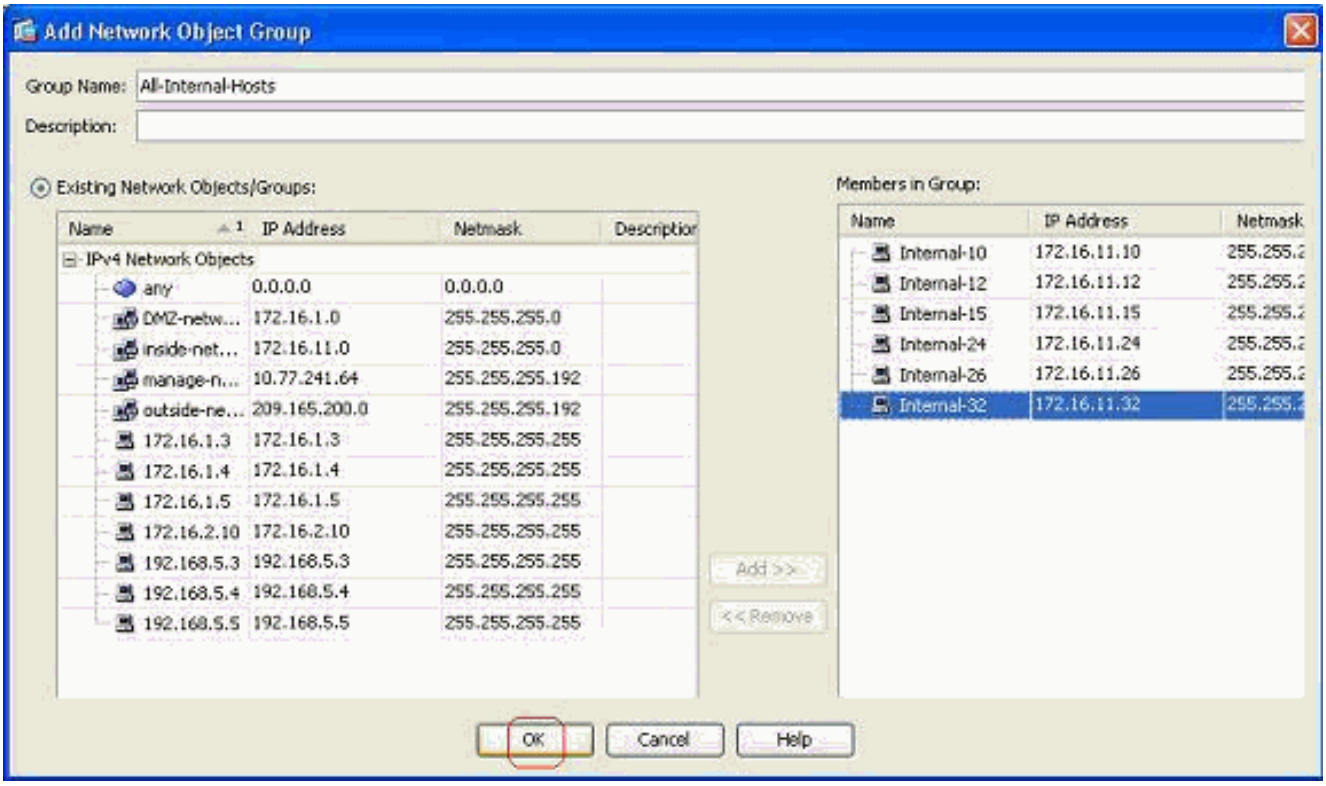
4. Wählen Sie **Konfiguration > Firewall > Objekte > Netzwerkobjekte/Gruppen > Hinzufügen**, und klicken Sie auf **Netzwerkobjektgruppe**, um eine neue Netzwerkobjektgruppe zu

erstellen.

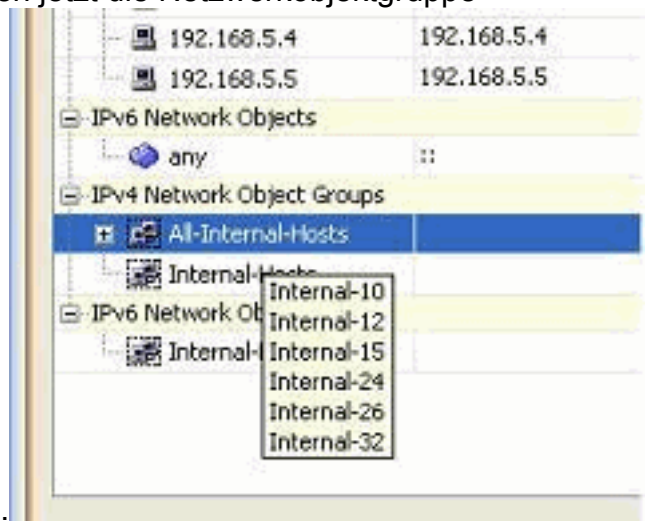
5. Die verfügbare Liste aller Netzwerkobjekte befindet sich im linken Fensterbereich. Wählen Sie einzelne Netzwerkobjekte aus, und klicken Sie auf die Schaltfläche **Hinzufügen**, um sie zu Membern der neu erstellten Netzwerkobjektgruppe zu machen. Der Gruppenname muss in dem ihm zugewiesenen Feld angegeben
werden.



6. Klicken Sie auf **OK**, nachdem Sie alle Mitglieder zur Gruppe hinzugefügt haben.

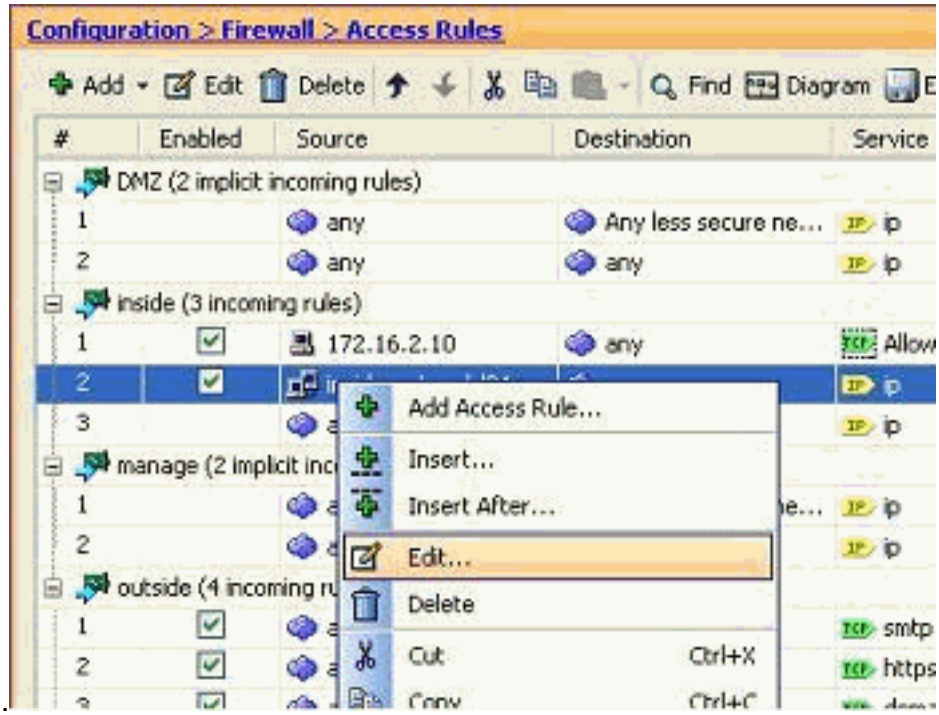


Sie können jetzt die Netzwerkobjektgruppe



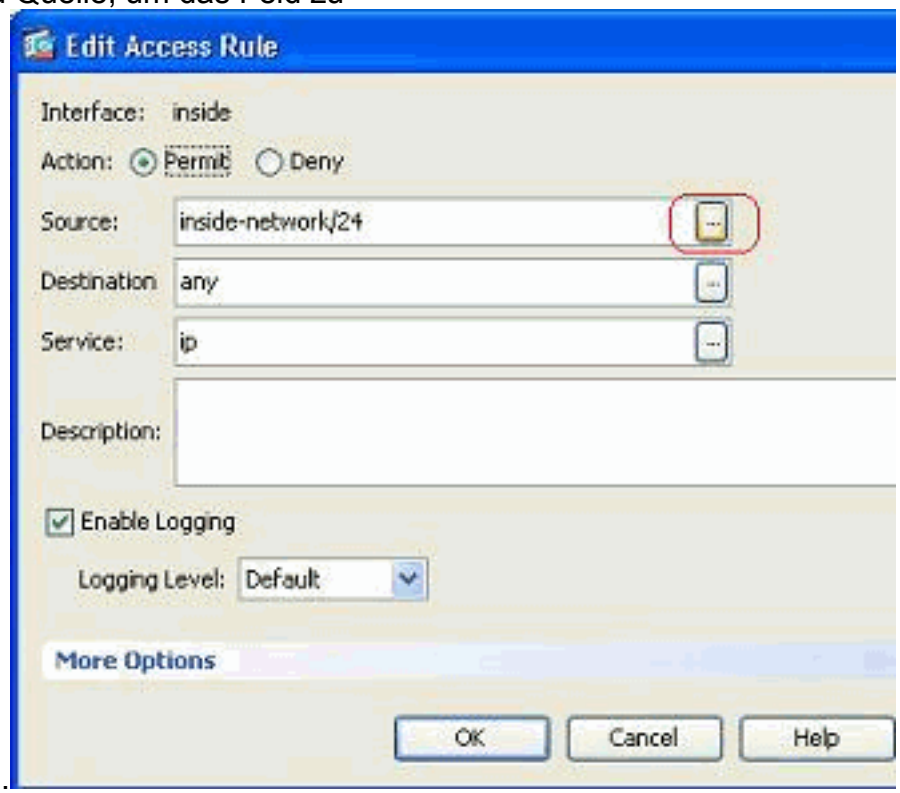
anzeigen.

7. Um ein Quell-/Zielfeld einer vorhandenen Zugriffsliste mit einem Netzwerkgruppenobjekt zu ändern, klicken Sie mit der rechten Maustaste auf die jeweilige Zugriffsregel, und wählen Sie



Bearbeiten aus.

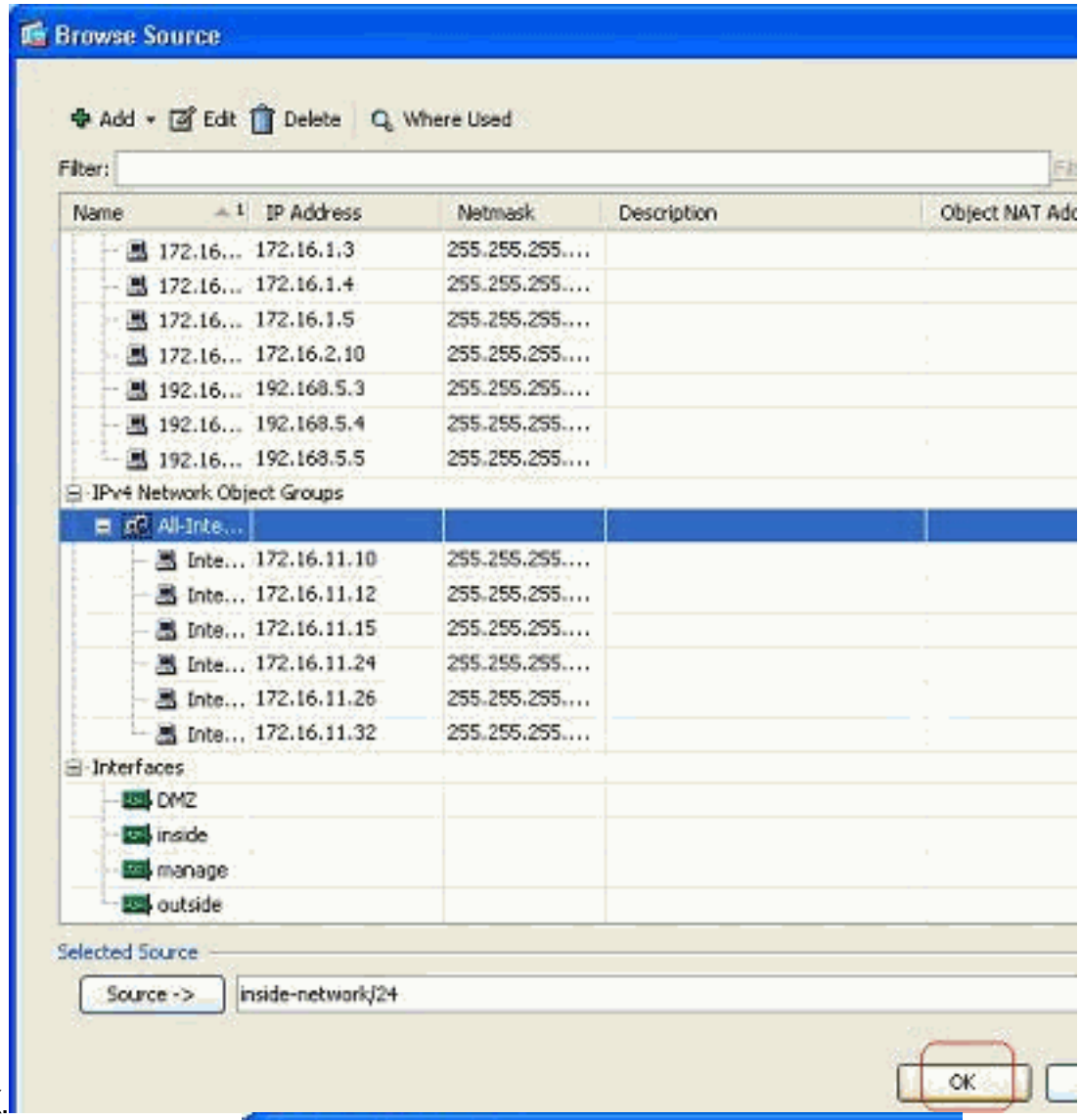
8. Das Fenster Zugriffsregel bearbeiten wird angezeigt. Klicken Sie auf die Schaltfläche **Details** im Feld Quelle, um das Feld zu



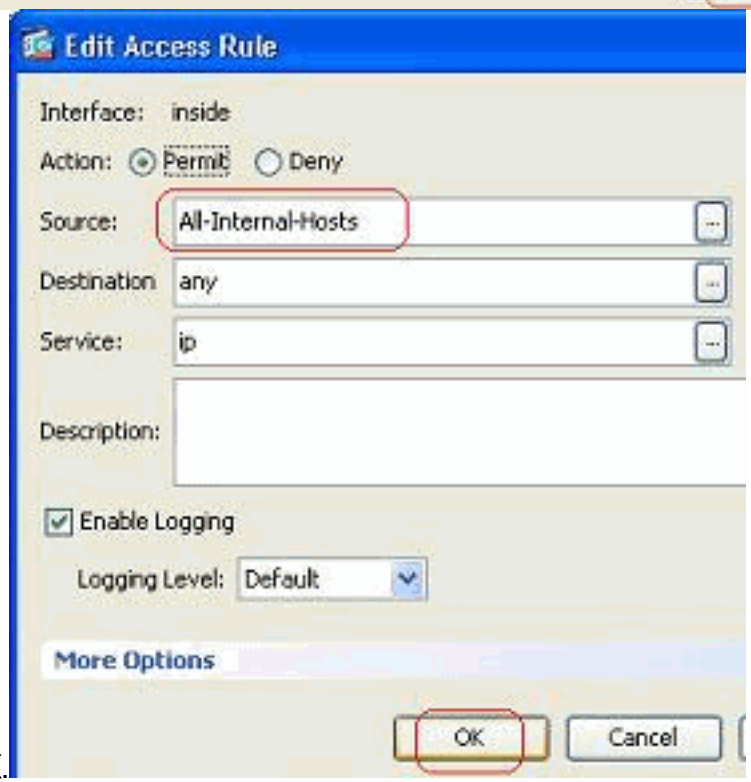
ändern.

9. Wählen Sie die Netzwerkobjektgruppe **All-Internal-Hosts** aus, und klicken Sie auf

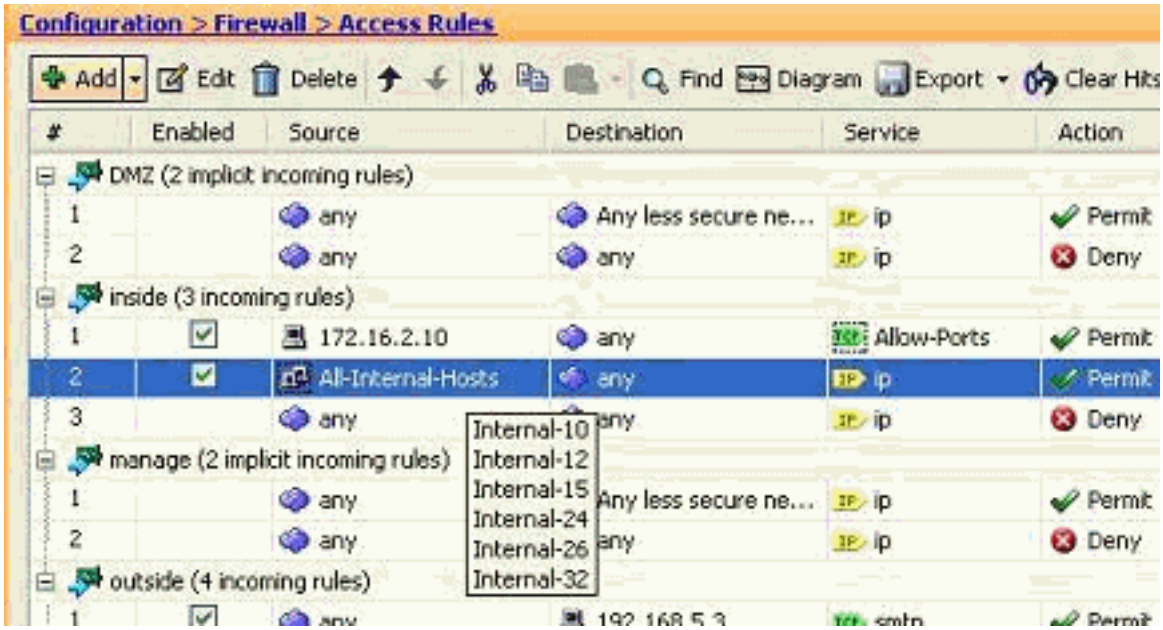
OK.



10. Klicken Sie auf **OK**.



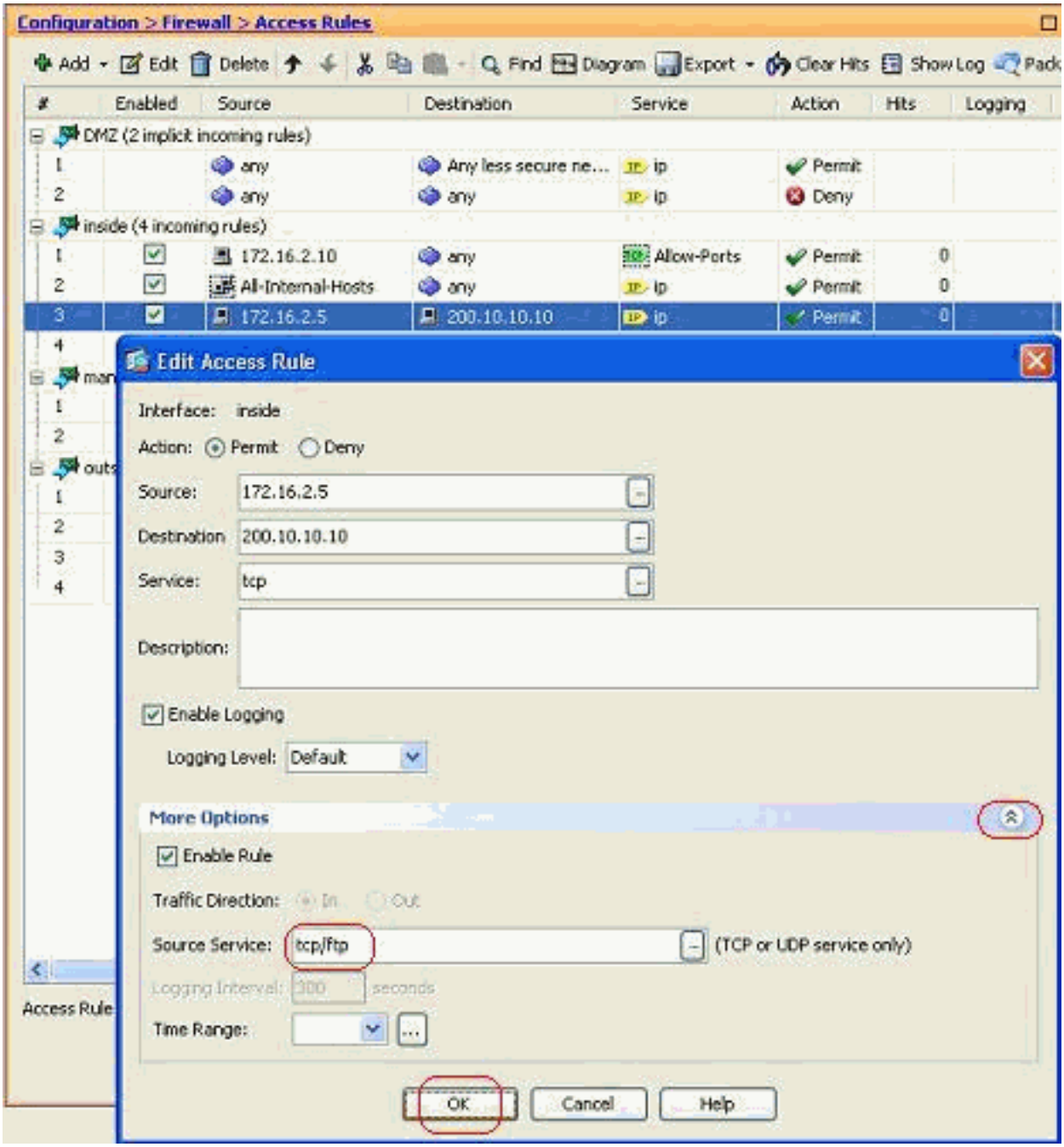
11. Bewegen Sie den Mauszeiger über das Feld Quelle der Zugriffsregel, um die Mitglieder der Gruppe
anzuzeigen.



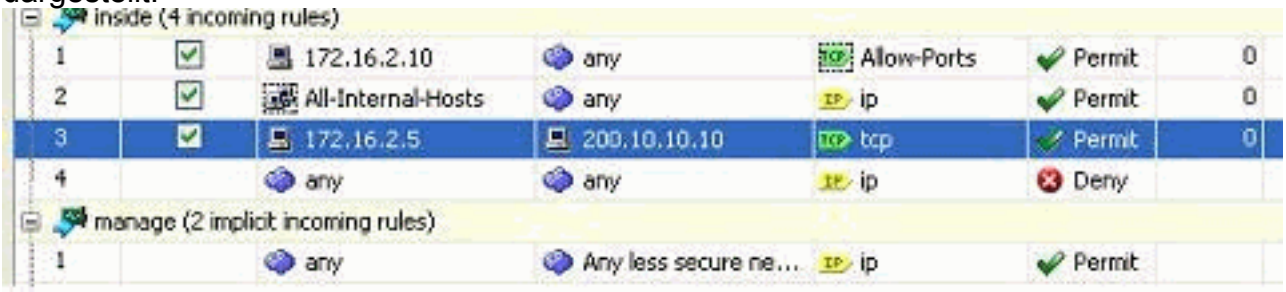
Quellport bearbeiten:

Gehen Sie wie folgt vor, um den Quellport einer Zugriffsregel zu ändern.

1. Um den Quellport einer bestehenden Zugriffsregel zu ändern, klicken Sie mit der rechten Maustaste darauf, und wählen Sie **Bearbeiten** aus.Das Fenster Zugriffsregel bearbeiten wird angezeigt.



2. Klicken Sie auf die Dropdown-Schaltfläche **Weitere Optionen**, um das Feld Quelldienst zu ändern, und klicken Sie auf **OK**.Sie können die geänderte Zugriffsregel anzeigen, wie dargestellt.

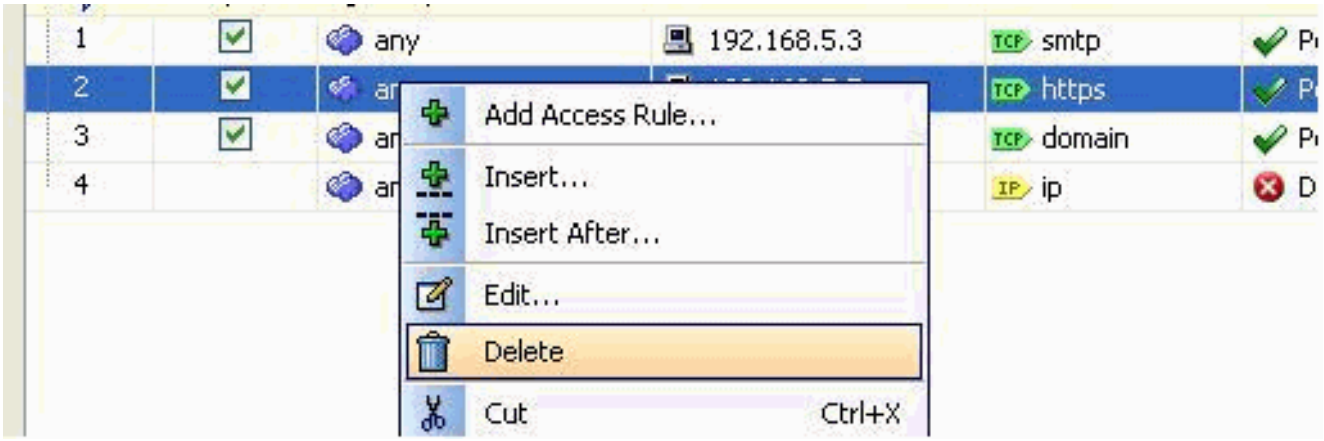


Löschen einer Zugriffsliste

Gehen Sie wie folgt vor, um eine Zugriffsliste zu löschen:

1. Bevor Sie eine vorhandene Zugriffsliste löschen, müssen Sie die Einträge in der Zugriffsliste (die Zugriffsregeln) löschen. Die Zugriffsliste kann nur gelöscht werden, wenn Sie zuerst alle

Zugriffsregeln löschen.Klicken Sie mit der rechten Maustaste auf die zu löschende Zugriffsregel, und wählen Sie **Löschen aus**.



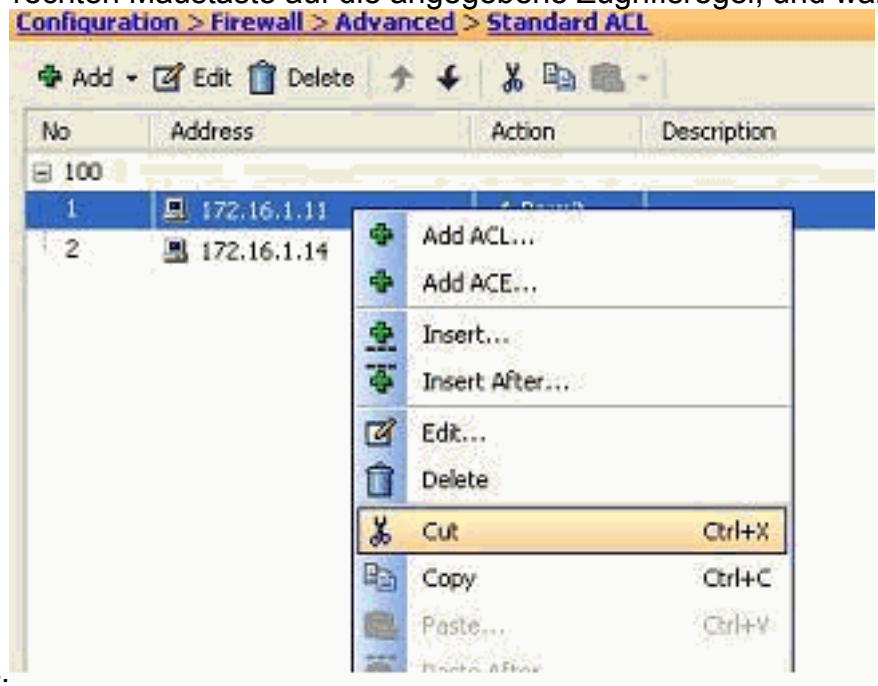
2. Führen Sie denselben Löschvorgang für alle vorhandenen Zugriffsregeln aus, wählen Sie dann die Zugriffsliste aus, und wählen Sie **Löschen aus**, um sie zu löschen.

Exportieren der Zugriffsregel

ASDM-Zugriffsregeln binden die Zugriffsliste an die entsprechende Schnittstelle, während der ACL Manager alle erweiterten Zugriffslisten verfolgt. Die mit dem ACL Manager erstellten Zugriffsregeln sind an keine Schnittstelle gebunden. Diese Zugriffslisten werden in der Regel für NAT-Exempt-, VPN-Filter- und ähnliche andere Funktionen verwendet, wenn keine Verknüpfung mit der Schnittstelle besteht. Der ACL Manager enthält alle Einträge im Abschnitt **"Konfiguration > Firewall > Zugriffsregeln"**. Darüber hinaus enthält der **ACL Manager** auch die globalen Zugriffsregeln, die keiner Schnittstelle zugeordnet sind. ASDM ist so organisiert, dass Sie problemlos eine Zugriffsregel aus einer beliebigen Zugriffsliste in eine andere exportieren können.

Wenn Sie beispielsweise eine Zugriffsregel benötigen, die bereits Teil einer globalen Zugriffsregel ist, um einer Schnittstelle zugeordnet zu werden, müssen Sie diese nicht erneut konfigurieren. Stattdessen können Sie einen **Cut & Paste-**Vorgang ausführen, um dies zu erreichen.

1. Klicken Sie mit der rechten Maustaste auf die angegebene Zugriffsregel, und wählen Sie **Ausschneiden aus**.



2. Wählen Sie die erforderliche Zugriffsliste aus, in die Sie diese Zugriffsregel einfügen

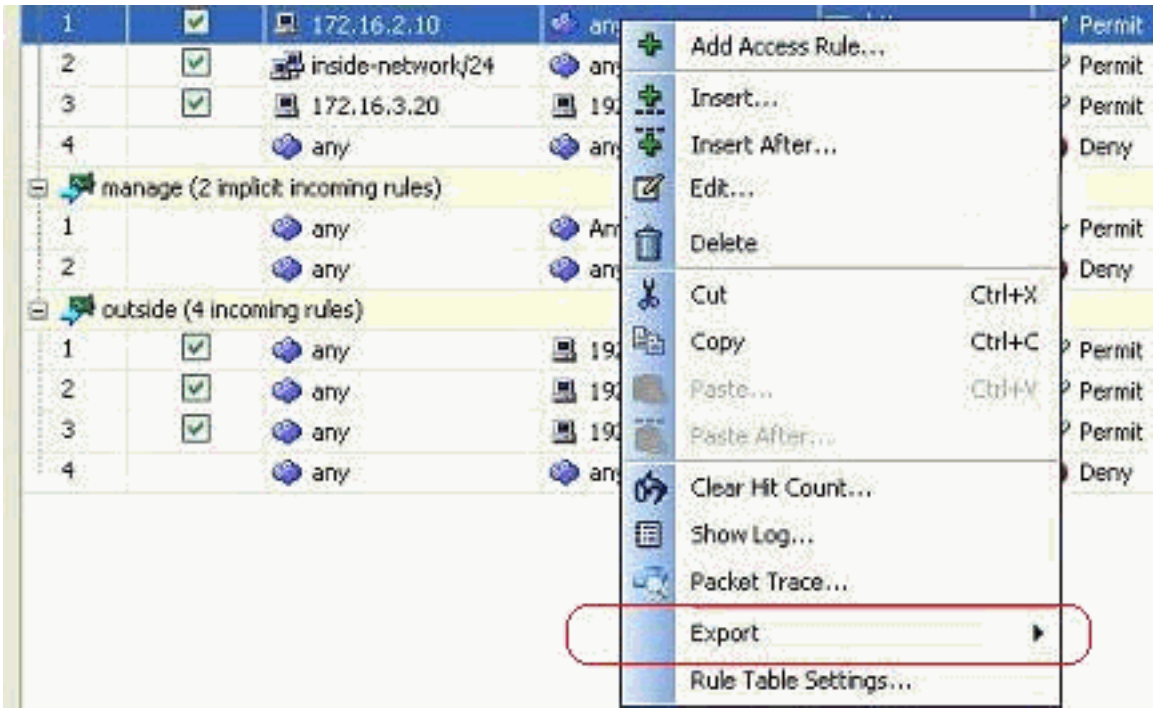
möchten. Sie können **Einfügen** in die Symbolleiste verwenden, um die Zugriffsregel einzufügen.

Exportieren der Informationen zur Zugriffsliste

Sie können die Informationen der Zugriffsliste in eine andere Datei exportieren. Für den Export dieser Informationen werden zwei Formate unterstützt.

1. CSV-Format (Comma Separated Value)
2. HTML-Format

Klicken Sie mit der rechten Maustaste auf eine der Zugriffsregeln, und wählen Sie **Exportieren** aus, um die Zugriffslisteninformationen an eine Datei zu senden.



Hier sind die Zugriffslisteninformationen im HTML-Format.

#	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

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- ASDM-Konfigurationsbeispiele und technische Hinweise
- ASA-Konfigurationsbeispiele und -technische Hinweise
- Technischer Support und Dokumentation - Cisco Systems