ASA 7.x/PIX 6.x und höher: Beispiel für die Port-Konfiguration öffnen/blockieren

Inhalt

Einführung

Dieses Dokument enthält eine Beispielkonfiguration zum Öffnen oder Blockieren der Ports für die verschiedenen Datenverkehrstypen, z. B. http oder ftp, in der Sicherheits-Appliance.

Hinweis: Die Begriffe "Öffnen des Ports" und "Zulassen des Ports" haben dieselbe Bedeutung. Ebenso bieten "Blockieren des Ports" und "Einschränken des Ports" dieselbe Bedeutung.

Voraussetzungen

Anforderungen

In diesem Dokument wird davon ausgegangen, dass PIX/ASA konfiguriert ist und ordnungsgemäß funktioniert.

Verwendete Komponenten

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

- Cisco Adaptive Security Appliance (ASA) der Serie 5500 mit Version 8.2(1)
- Cisco Adaptive Security Device Manager (ASDM) Version 6.3(5)

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.

Zugehörige Produkte

Diese Konfiguration kann auch mit der Cisco PIX Firewall Appliance der Serie 500 mit der Software 6.x und höher verwendet werden.

Konventionen

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

Konfigurieren

Jede Schnittstelle muss eine Sicherheitsstufe zwischen 0 (niedrigste Stufe) und 100 (höchste Stufe) aufweisen. Beispielsweise müssen Sie Ihr sicherstes Netzwerk, z. B. das interne Hostnetzwerk, Ebene 100 zuweisen. Das mit dem Internet verbundene externe Netzwerk kann die Ebene 0 sein, während andere Netzwerke, z. B. DMZs, dazwischen positioniert werden können. Sie können derselben Sicherheitsstufe mehrere Schnittstellen zuweisen.

Standardmäßig sind alle Ports an der externen Schnittstelle (Sicherheitsstufe 0) blockiert, und alle Ports sind an der internen Schnittstelle (Sicherheitsstufe 100) der Sicherheits-Appliance offen. Auf diese Weise kann der gesamte ausgehende Datenverkehr ohne Konfiguration durch die Security Appliance geleitet werden. Eingehender Datenverkehr kann jedoch durch die Konfiguration der Zugriffsliste und der statischen Befehle in der Security Appliance zugelassen werden.

Hinweis: Im Allgemeinen werden alle Ports von der unteren Sicherheitszone zur oberen Sicherheitszone blockiert, und alle Ports sind von der oberen Sicherheitszone zur unteren Sicherheitszone geöffnet, sofern die Stateful Inspection sowohl für eingehenden als auch für ausgehenden Datenverkehr aktiviert ist.

Dieser Abschnitt besteht aus den folgenden Unterabschnitten:

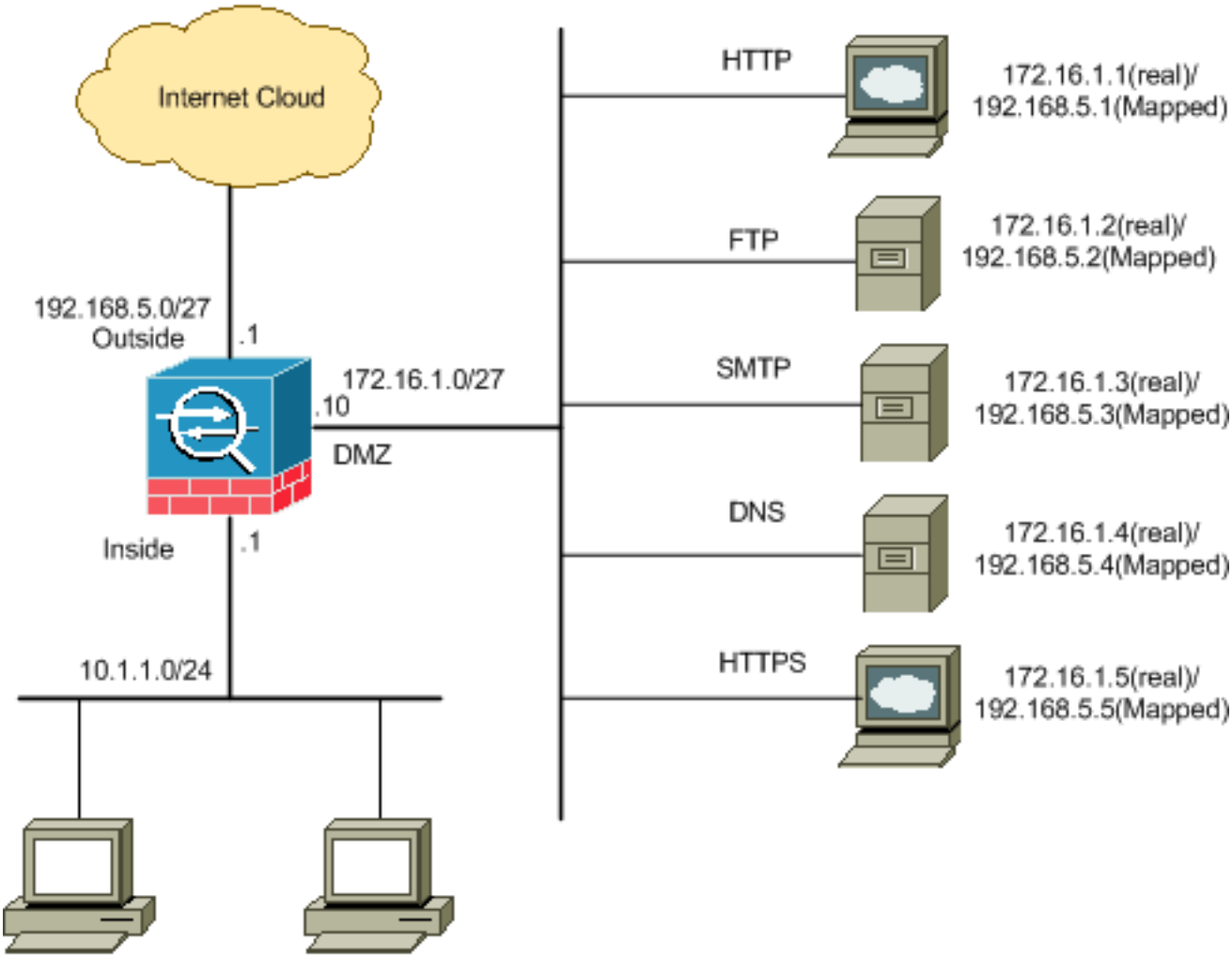
- Netzwerkdiagramm
- Blockieren der Port-Konfiguration
- Öffnen der Port-Konfiguration

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

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Blockieren der Port-Konfiguration

Die Sicherheits-Appliance erlaubt jeglichen ausgehenden Datenverkehr, es sei denn, er wird explizit von einer erweiterten Zugriffsliste blockiert.

Eine Zugriffsliste besteht aus einem oder mehreren Zugriffskontrolleinträgen. Abhängig vom Zugriffslistentyp können Sie Quell- und Zieladressen, Protokolle, Ports (für TCP oder UDP), ICMP-Typ (für ICMP) oder EtherType angeben.

Hinweis: Für verbindungslose Protokolle wie ICMP erstellt die Sicherheitsappliance unidirektionale Sitzungen. Sie benötigen daher entweder Zugriffslisten, um ICMP in beide Richtungen zuzulassen (durch die Anwendung von Zugriffslisten auf die Quell- und Zielschnittstellen), oder Sie müssen die ICMP-Prüfungs-Engine aktivieren. Die ICMP Inspection Engine behandelt ICMP-Sitzungen als bidirektionale Verbindungen.

Führen Sie diese Schritte aus, um die Ports zu blockieren, die normalerweise für Datenverkehr gelten, der von der Innenseite (der höheren Sicherheitszone) zur DMZ (der unteren Sicherheitszone) oder zur DMZ zur Außenseite stammt.

1. Erstellen Sie eine Zugriffssteuerungsliste, sodass der angegebene Port-Datenverkehr blockiert wird.

   ```
   access-list
   ```

2. Binden Sie dann die Zugriffsliste mit dem Befehl **access-group**, um aktiv zu sein.

```
access-group
```

Beispiele:

1. **HTTP-Port-Datenverkehr blockieren:** Um den Zugriff des internen Netzwerks 10.1.1.0 auf das http (Webserver) zu blockieren, wobei IP 172.16.1.1 im DMZ-Netzwerk platziert wird, erstellen Sie eine ACL wie folgt:

```
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
```

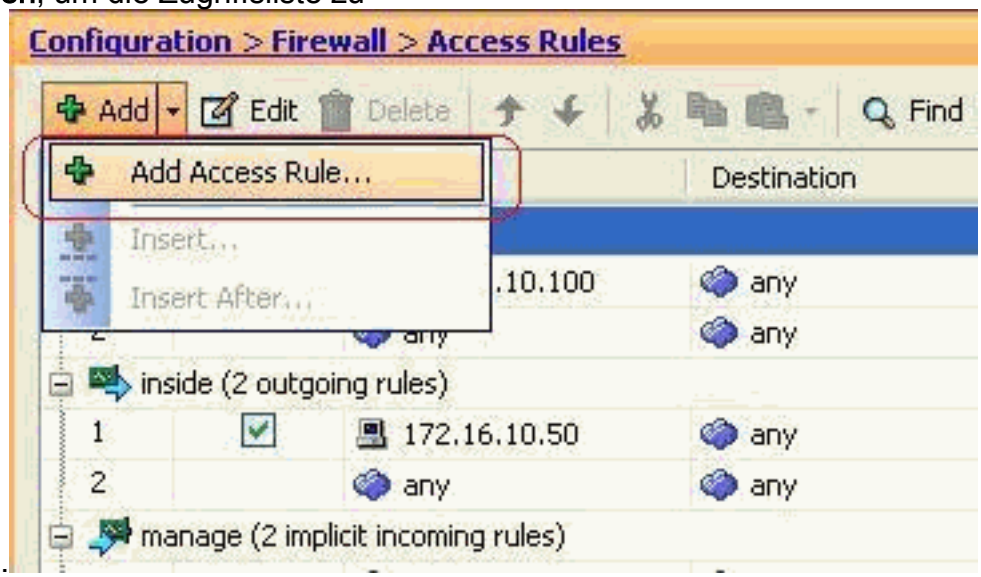
   Hinweis: Verwenden Sie **no** gefolgt von den Befehlen der Zugriffsliste, um die Port-Blockierung zu entfernen.
2. **Blockieren des FTP-Port-Datenverkehrs:** Um den Zugriff des internen Netzwerks 10.1.1.0 auf den FTP (Dateiserver) zu blockieren, in dem IP 172.16.1.2 im DMZ-Netzwerk platziert wird, erstellen Sie eine ACL wie folgt:

```
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
```

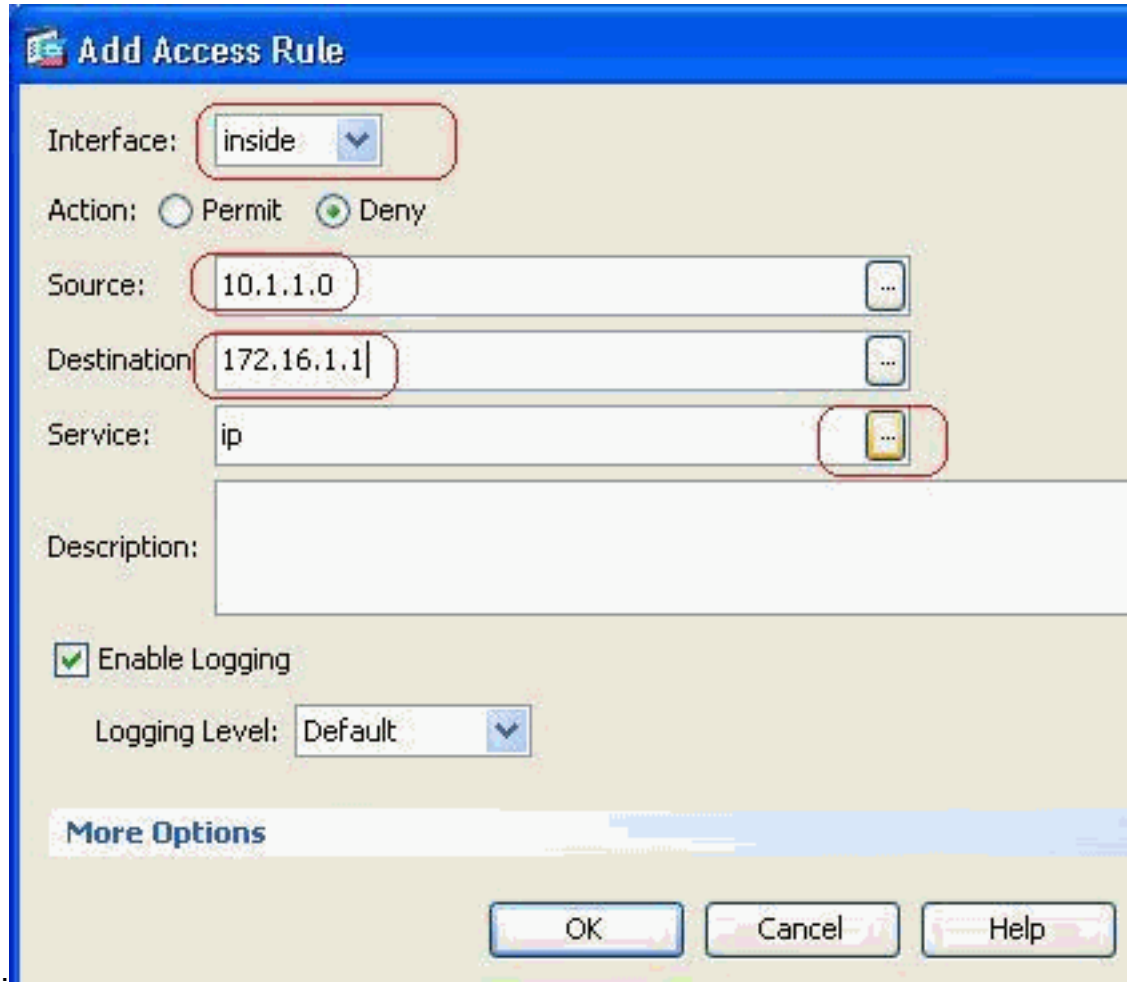
Hinweis: IANA-Ports bieten weitere Informationen zu Portzuweisungen.

In diesem Abschnitt wird die schrittweise Konfiguration zur Durchführung dieser Aufgabe über das ASDM dargestellt.

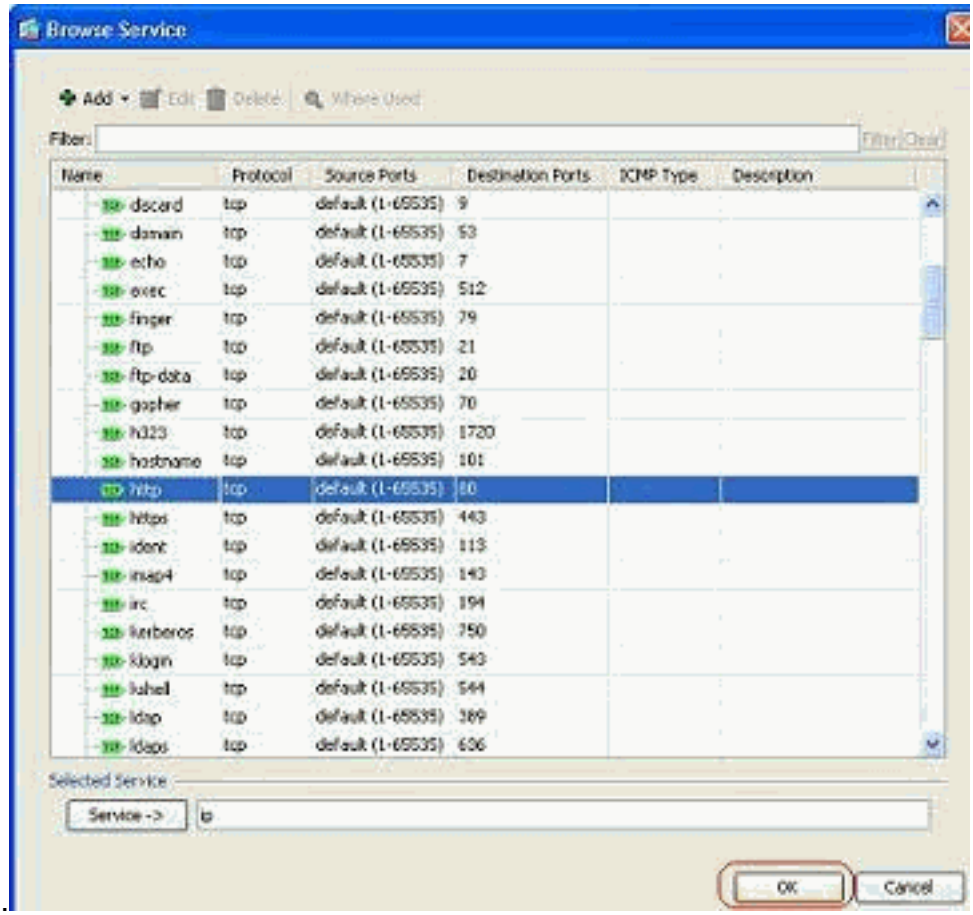
1. Gehen Sie zu **Konfiguration > Firewall > Zugriffsregeln**. Klicken Sie auf **Zugriffsregel hinzufügen**, um die Zugriffsliste zu erstellen.



2. Definieren Sie Quelle und Ziel sowie die Aktion der Zugriffsregel zusammen mit der Schnittstelle, der diese Zugriffsregel zugeordnet wird. Wählen Sie die Details aus, um den zu blockierenden Port auszuwählen.

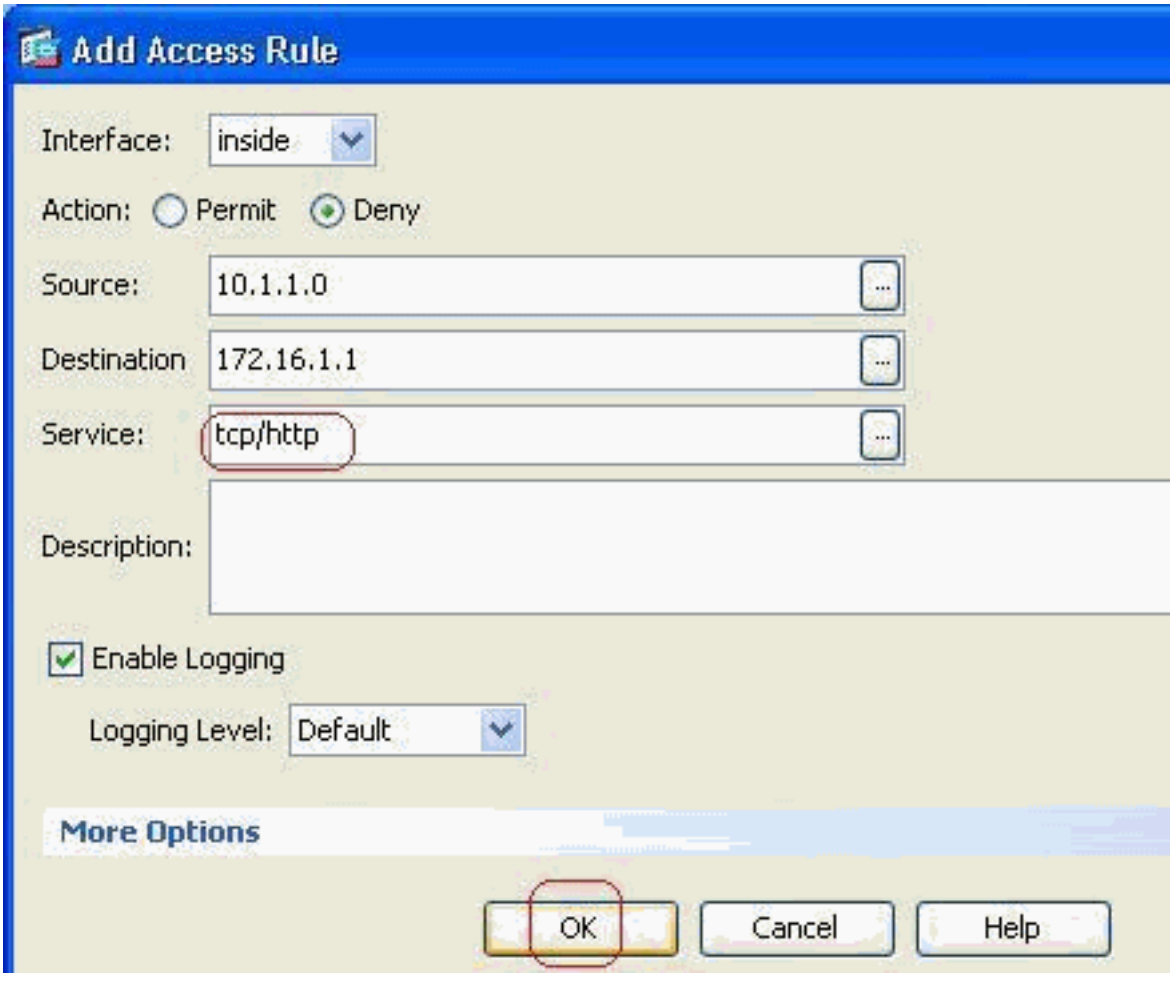


3. Wählen Sie **http** aus der Liste der verfügbaren Ports aus, und klicken Sie dann auf **OK**, um zum Fenster Zugriffsregel hinzufügen



zurückzukehren.

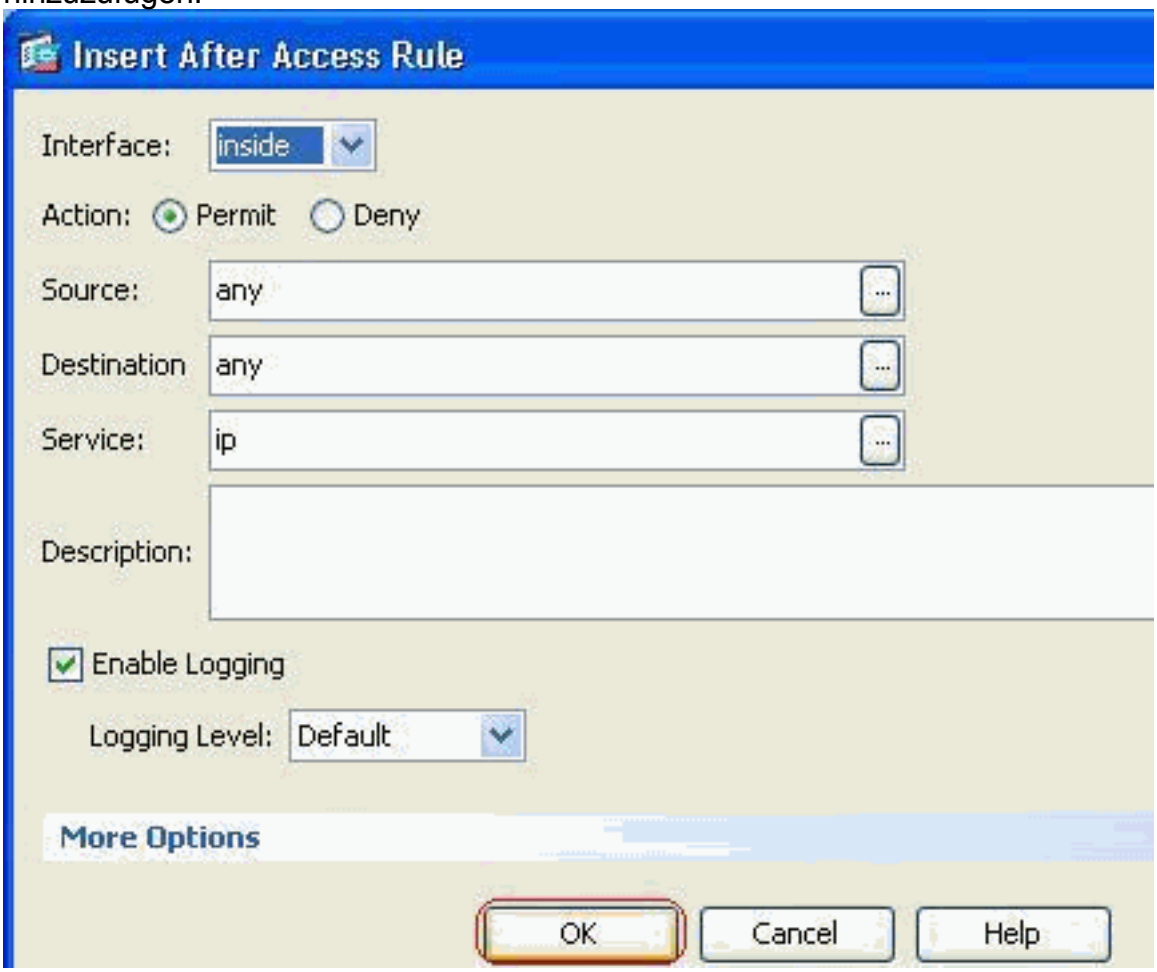
4. Klicken Sie auf **OK**, um die Konfiguration der Zugriffsregel abzuschließen.



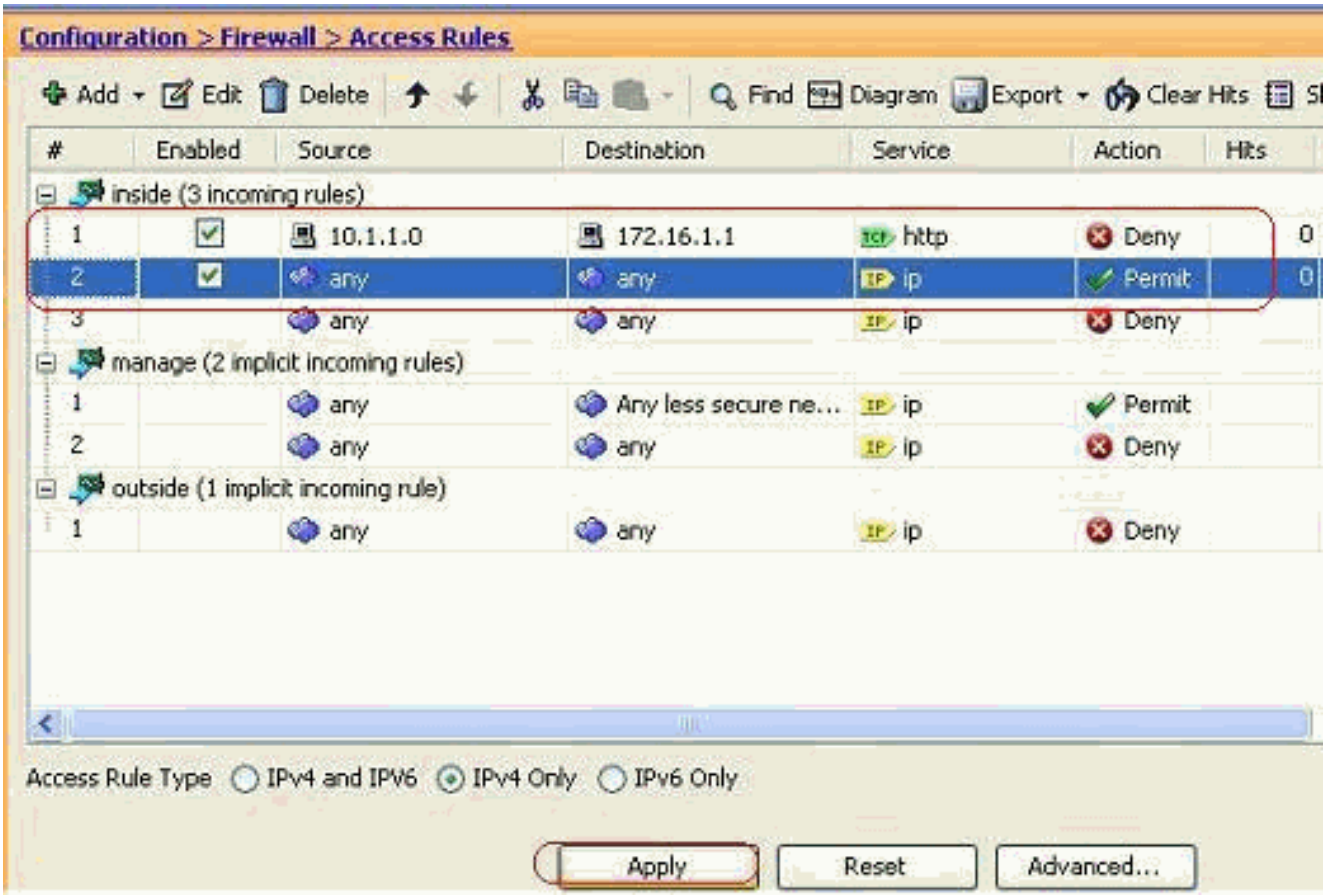
5. Klicken Sie auf **Nach einfügen**, um derselben Zugriffsliste eine Zugriffsregel

hinzuzufügen.

6. Zulassen des Datenverkehrs von "any" zu "any", um die "implizite Verweigerung" zu verhindern. Klicken Sie anschließend auf **OK**, um diese Zugriffsregel hinzuzufügen.



7. Die konfigurierte Zugriffsliste wird auf der Registerkarte "Zugriffsregeln" angezeigt. Klicken Sie auf **Apply**, um diese Konfiguration an die Sicherheits-Appliance zu senden.

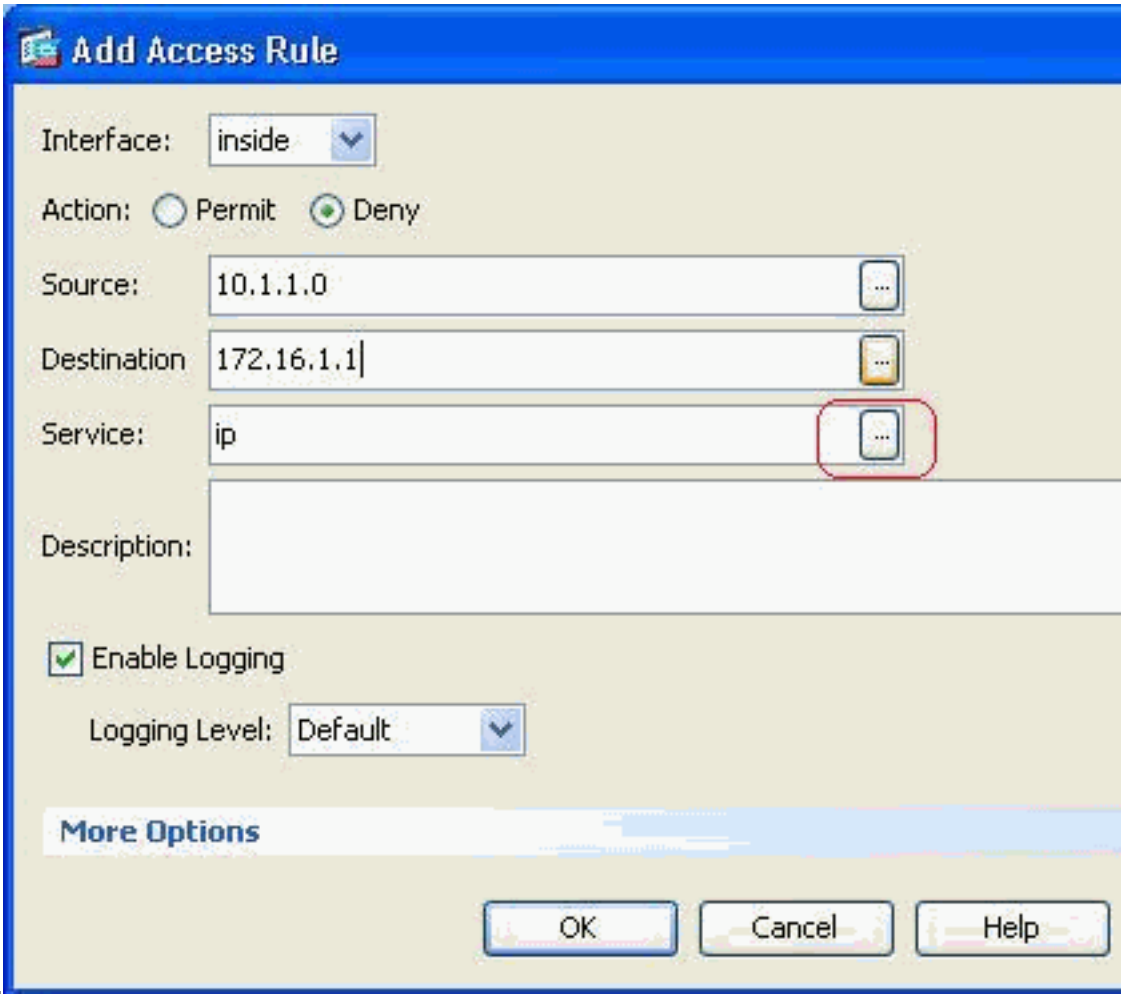


Die vom ASDM gesendete Konfiguration führt zu dieser Gruppe von Befehlen in der Befehlszeilenschnittstelle (CLI) der ASA.

```
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
```

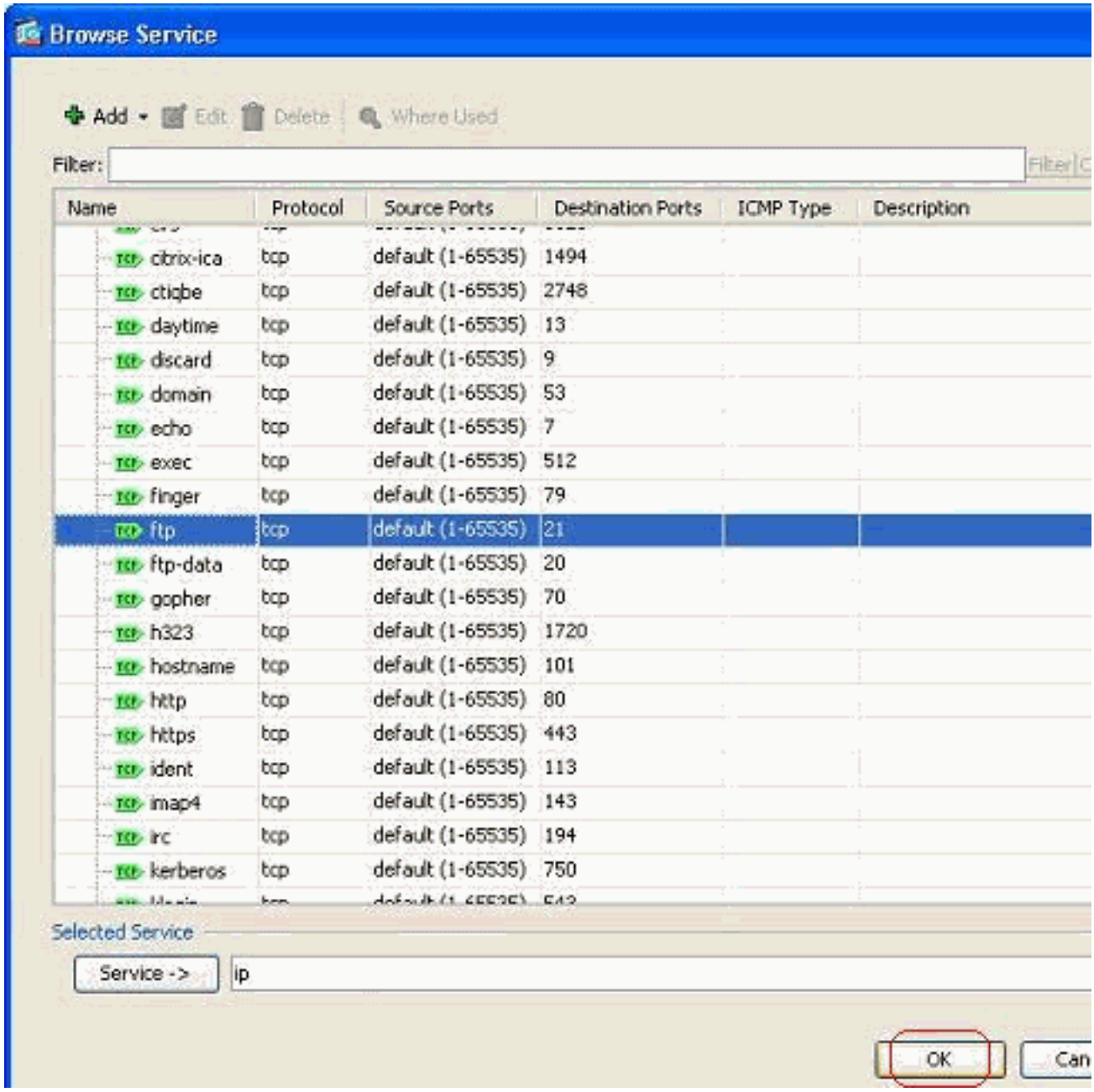
In diesen Schritten wurde Beispiel 1 über ASDM durchgeführt, um den Zugriff des Netzwerks 10.1.1.0 auf den Webserver zu blockieren (172.16.1.1). Beispiel 2 kann auch auf die gleiche Weise erreicht werden, um den Zugriff des gesamten 10.1.1.0-Netzwerks auf den FTP-Server 172.16.1.2 zu blockieren. Der einzige Unterschied besteht darin, dass der Port ausgewählt wird.**Hinweis:** Bei dieser Zugriffsregelkonfiguration für Beispiel 2 wird von einer neuen Konfiguration ausgegangen.

8. Definieren Sie die Zugriffsregel für die Blockierung von FTP-Datenverkehr, und klicken Sie dann auf die Registerkarte **Details**, um den Zielport

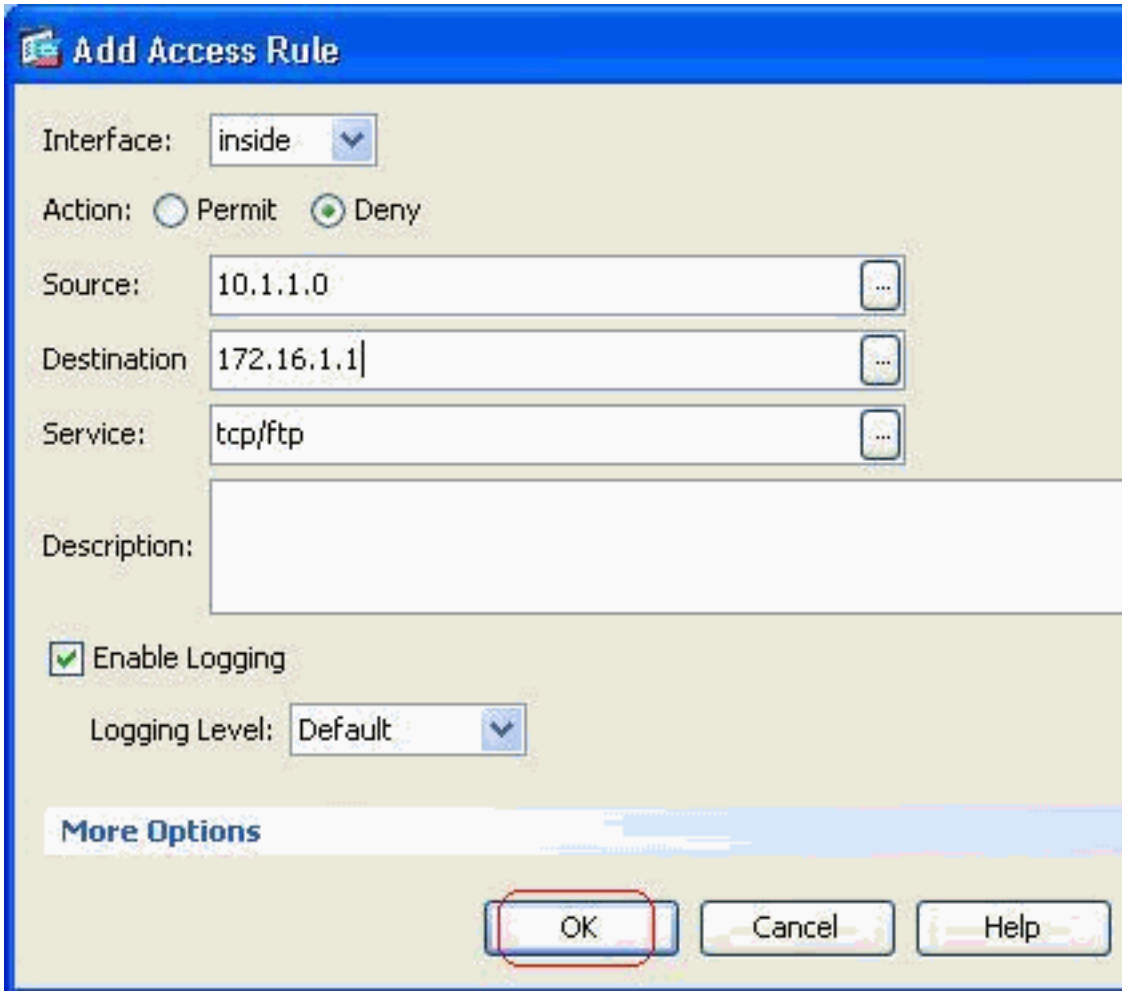


auszuwählen.

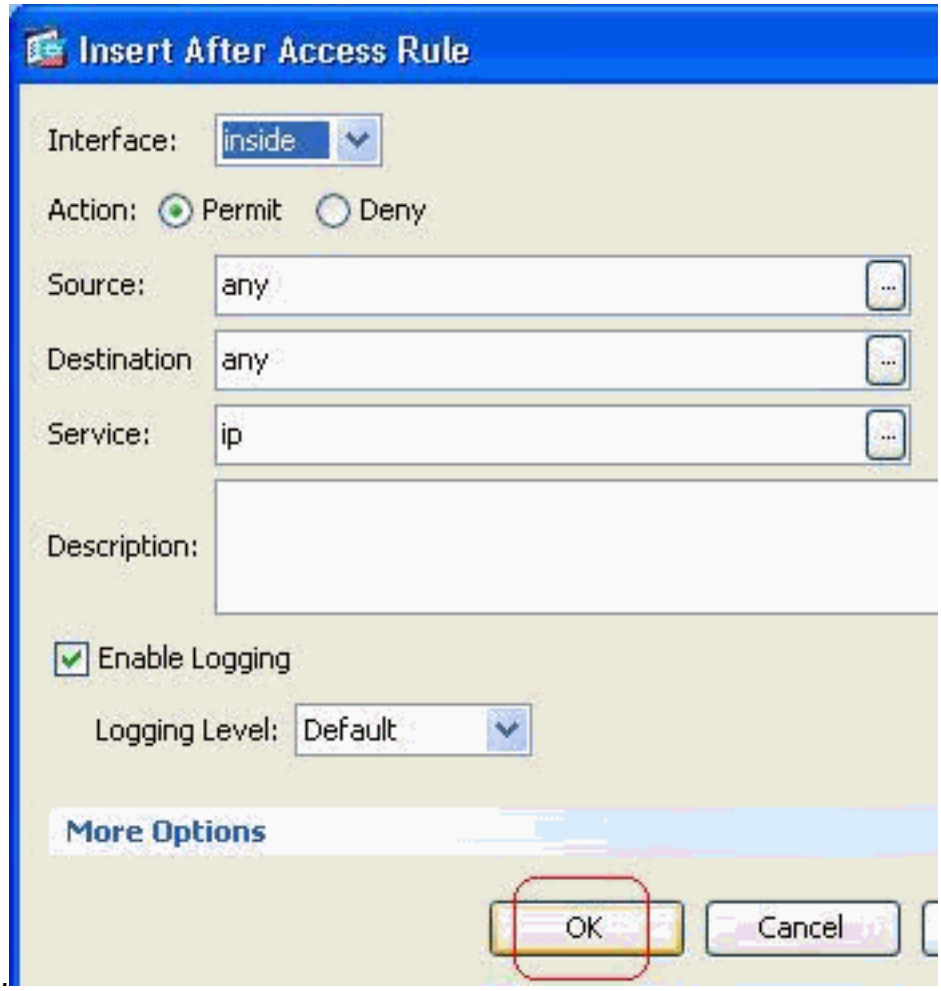
9. Wählen Sie den **FTP-**Port aus, und klicken Sie auf **OK**, um zum Fenster Zugriffsregel hinzufügen
zurückzukehren.



10. Klicken Sie auf **OK**, um die Konfiguration der Zugriffsregel abzuschließen.

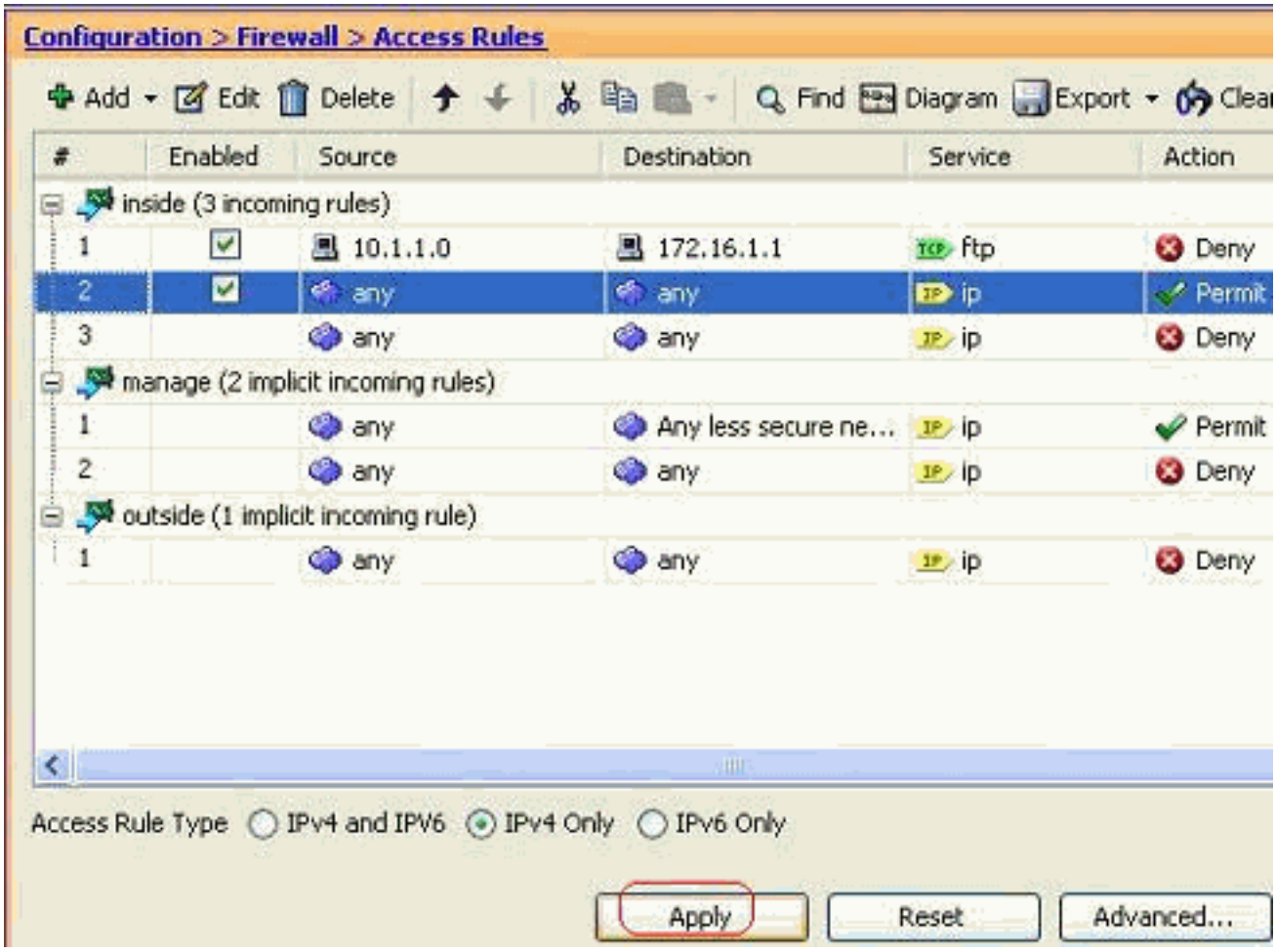


11. Fügen Sie eine andere Zugriffsregel hinzu, um anderen Datenverkehr zuzulassen. Andernfalls wird der gesamte Datenverkehr auf dieser Schnittstelle durch die Regel "Implicit



Deny" blockiert.

12. Die vollständige Konfiguration der Zugriffslisten sieht auf der Registerkarte "Zugriffsregeln" wie folgt
    aus.



13. Klicken Sie auf **Apply**, um die Konfiguration an die ASA zu senden. Die entsprechende CLI-Konfiguration sieht wie folgt aus:

```
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
```

Öffnen der Port-Konfiguration

Die Sicherheits-Appliance erlaubt keinen eingehenden Datenverkehr, es sei denn, dieser wird ausdrücklich von einer erweiterten Zugriffsliste zugelassen.

Wenn Sie einem externen Host den Zugriff auf einen internen Host gestatten möchten, können Sie eine Liste eingehender Zugriffe auf die externe Schnittstelle anwenden. Sie müssen die übersetzte Adresse des internen Hosts in der Zugriffsliste angeben, da die übersetzte Adresse die Adresse ist, die im externen Netzwerk verwendet werden kann. Führen Sie diese Schritte aus, um die Ports von der unteren Sicherheitszone zur höheren Sicherheitszone zu öffnen. Zulassen des Datenverkehrs von außen (untere Sicherheitszone) zur internen Schnittstelle (obere Sicherheitszone) oder der DMZ zur internen Schnittstelle.

1. Static NAT erstellt eine feste Übersetzung einer echten Adresse in eine zugeordnete Adresse. Diese zugeordnete Adresse ist eine Adresse, die im Internet gehostet wird und für den Zugriff auf den Anwendungsserver der DMZ verwendet werden kann, ohne dass die tatsächliche Adresse des Servers bekannt sein muss.

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

Weitere Informationen finden Sie im Abschnitt Static NAT der Befehlsreferenz für PIX/ASA.

2. Erstellen Sie eine ACL, um den spezifischen Port-Datenverkehr zuzulassen.

```
access-list
```

3. Binden Sie die Zugriffsliste mit dem Befehl **access-group**, um aktiv zu sein.

```
access-group
```

Beispiele:

1. **Öffnen Sie den SMTP-Port-Datenverkehr:** Öffnen Sie den Port **tcp 25**, damit die Hosts von außen (Internet) auf den im DMZ-Netzwerk angeordneten Mailserver zugreifen können.Der **statische** Befehl ordnet die externe Adresse 192.168.5.3 der echten DMZ-Adresse 172.16.1.3 zu.

```
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. **Öffnen Sie den HTTPS-Port-Datenverkehr:** Öffnen Sie den Port **tcp 443**, damit die Hosts von außen (Internet) auf den im DMZ-Netzwerk (sicher) eingerichteten Webserver zugreifen können.

```
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. **DNS-Datenverkehr zulassen:** Öffnen Sie den Port **udp 53**, um den Hosts von außen (Internet) den Zugriff auf den DNS-Server (sicher) im DMZ-Netzwerk zu ermöglichen.

```
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
```

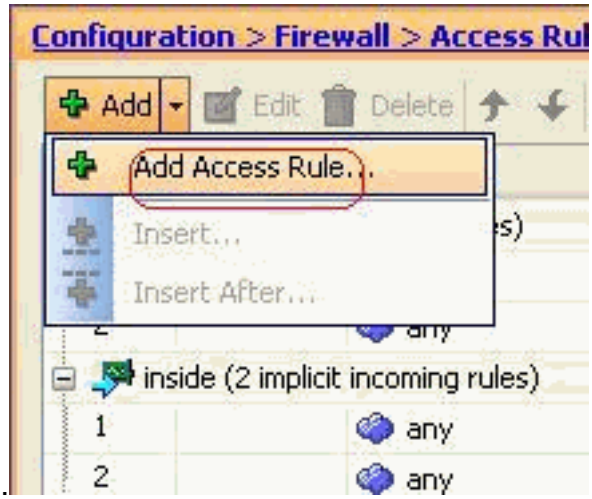
Hinweis: IANA-Ports bieten weitere Informationen zu Portzuweisungen.

Konfiguration über ASDM

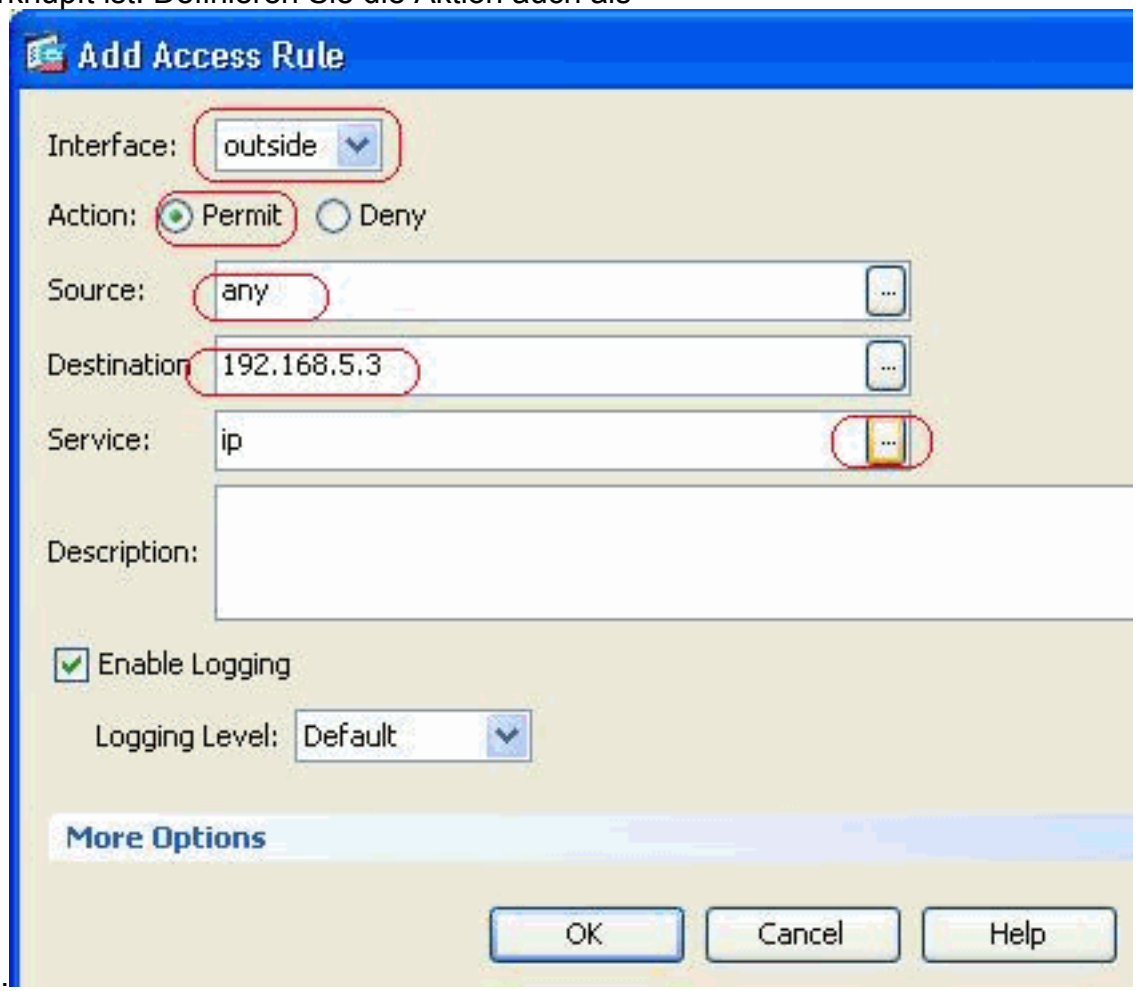
In diesem Abschnitt wird ein schrittweiser Ansatz zur Durchführung der oben genannten Aufgaben über ASDM dargestellt.

1. Erstellen Sie die Zugriffsregel, um den SMTP-Datenverkehr zum Server 192.168.5.3

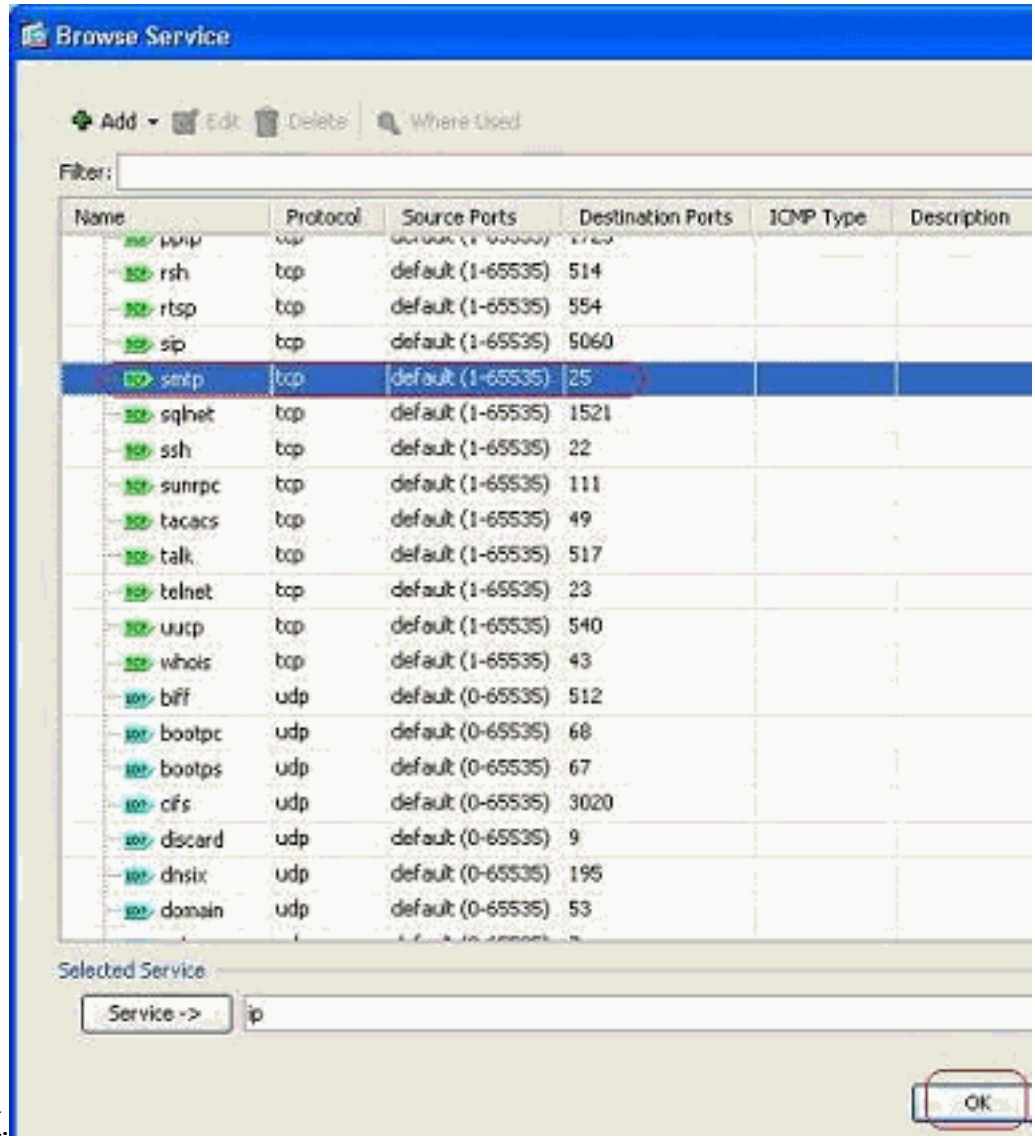
zuzulassen.



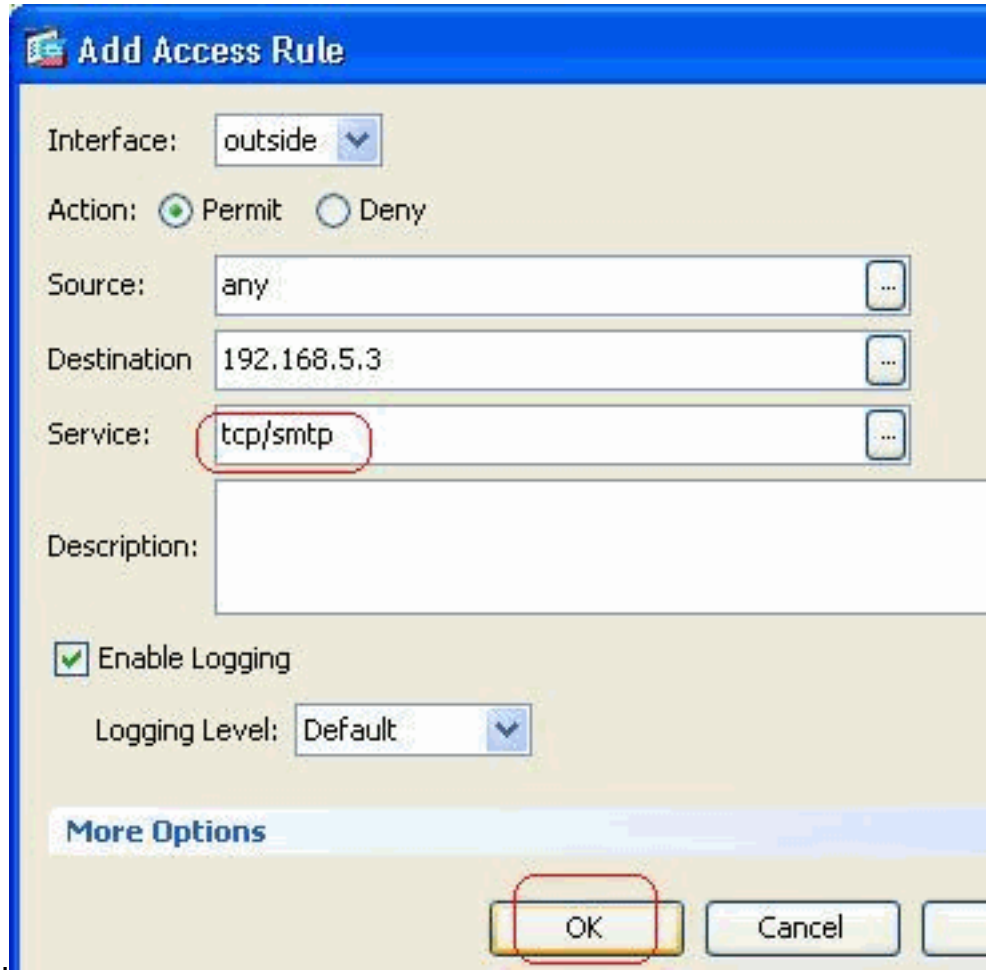
2. Definieren Sie die Quelle und das Ziel der Zugriffsregel und die Schnittstelle, mit der diese Regel verknüpft ist. Definieren Sie die Aktion auch als **Zulassen**.



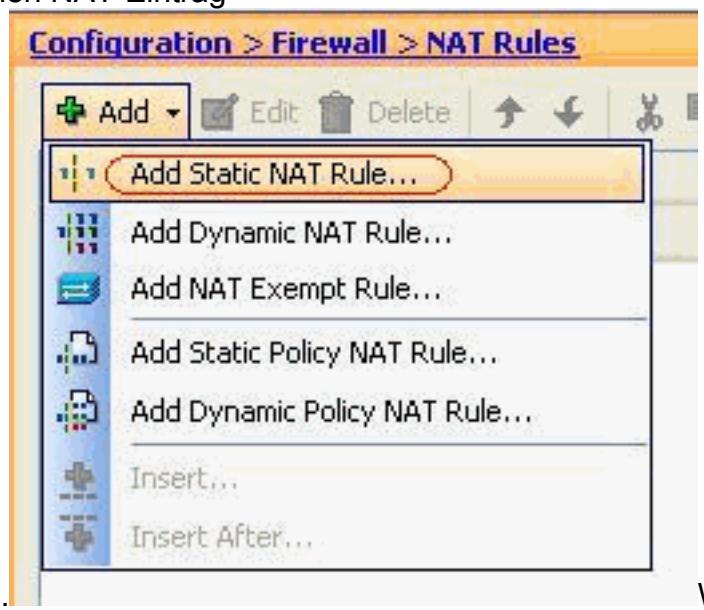
3. Wählen Sie **SMTP** als Port aus, und klicken Sie dann auf



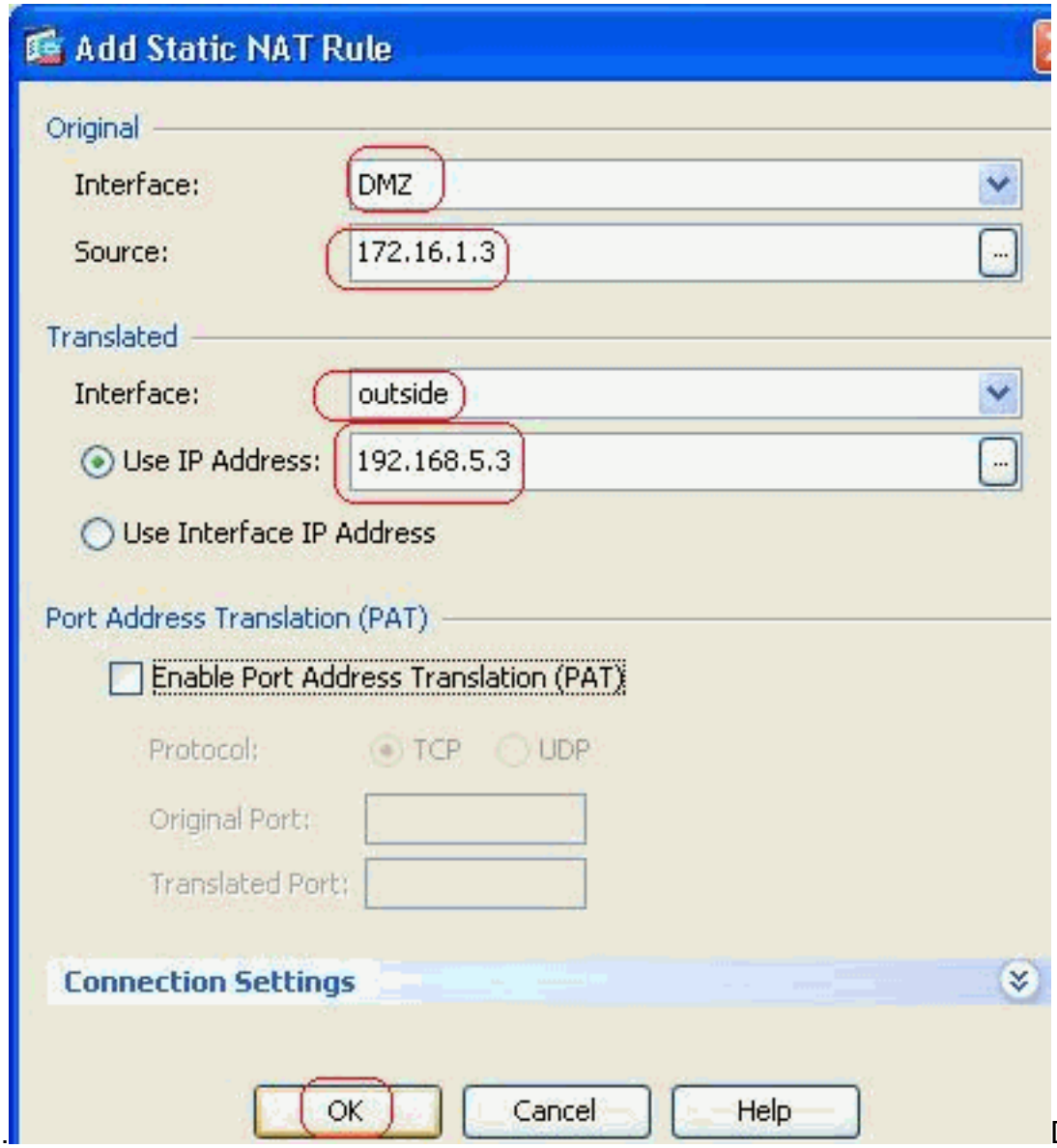
4. Klicken Sie auf **OK**, um die Konfiguration der Zugriffsregel **OK**.

abzuschließen. 

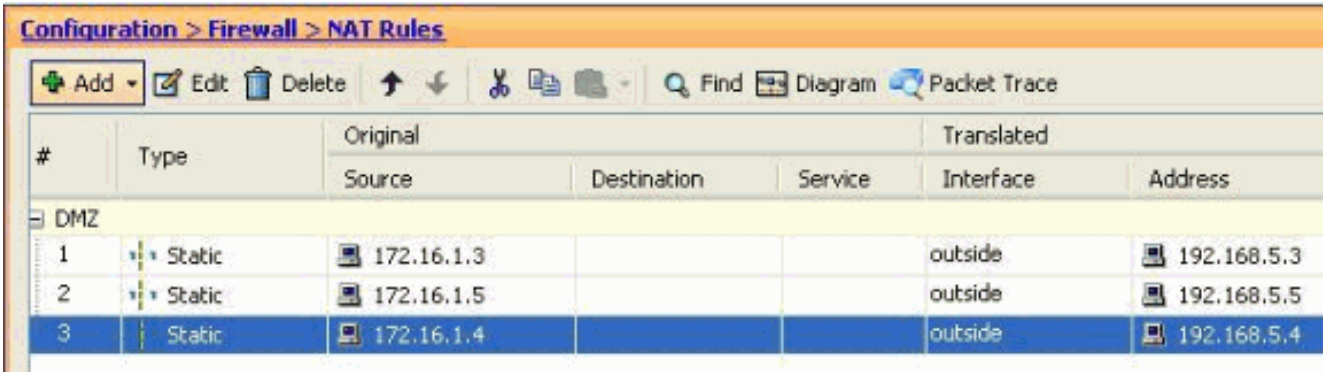
5. Konfigurieren Sie die statische NAT für die Übersetzung von 172.16.1.3 in 192.168.5.3.Gehen Sie zu **Konfiguration > Firewall > NAT Rules > Add Static NAT Rule**, um einen statischen NAT-Eintrag



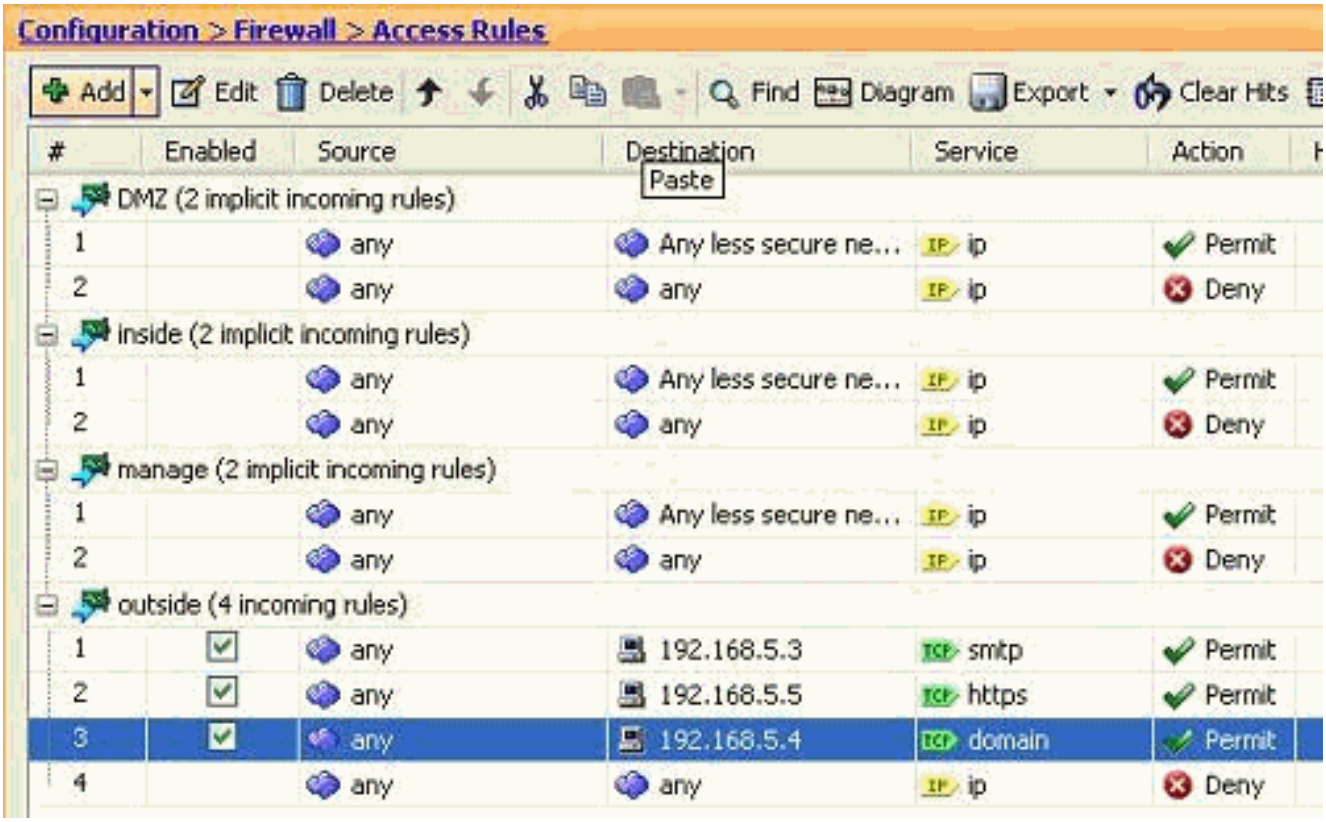
hinzuzufügen. Wählen Sie die ursprüngliche und die umgewandelte IP-Adresse zusammen mit den zugehörigen Schnittstellen aus, und klicken Sie dann auf **OK**, um die Konfiguration der statischen NAT-Regel



abzuschließen. Dieses Bild zeigt alle drei statischen Regeln, die im Abschnitt Beispiele aufgeführt sind:



Dieses Bild zeigt alle drei Zugriffsregeln, die im Abschnitt Beispiele aufgeführt sind:



Überprüfen

Sie können die Überprüfung mit bestimmten **show**-Befehlen wie folgt durchführen:

- **Exlate anzeigen -** aktuelle Übersetzungsinformationen anzeigen
- **show access-list** - Anzeige von Trefferzählern für Zugriffsrichtlinien
- **show logging**: Zeigt die Protokolle im Puffer an.

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

Fehlerbehebung

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

Zugehörige Informationen

- PIX/ASA 7.x: Aktivieren/Deaktivieren der Kommunikation zwischen Schnittstellen
- PIX 7.0 und Adaptive Security Appliance Port Redirection (Forwarding) mit nat-, global, statisch, rohr- und Zugriffslisten-Befehlen
- Verwendung von NAT-, globalen, statischen, Kanal- und Zugriffslisten-Befehlen und Port Redirection (Forwarding) auf PIX
- PIX/ASA 7.x: Beispiel für die Konfiguration von FTP- und TFTP-Services aktivieren
- PIX/ASA 7.x: Konfigurationsbeispiel für VoIP-Services (SIP, MGCP, H323, SCCP) aktivieren
- PIX/ASA 7.x: Mailserver-Zugriff auf das DMZ-Konfigurationsbeispiel
- Technischer Support und Dokumentation - Cisco Systems