PIX/ASA 7.x und höher: Anschließen mehrerer interner Netzwerke mit dem Beispiel einer Internetkonfiguration

Inhalt

Einführung

Dieses Dokument enthält eine Beispielkonfiguration für die PIX/ASA Security Appliance Version 7.x und höher mit mehreren internen Netzwerken, die über die Befehlszeilenschnittstelle (CLI) oder den Adaptive Security Device Manager (ASDM) 5.x oder höher mit dem Internet (oder einem externen Netzwerk) verbunden sind.

Weitere Informationen zum Herstellen und Beheben von Verbindungen über die Cisco Security Appliance finden Sie unter Herstellen und Beheben von Verbindungsproblemen über PIX/ASA.

Weitere Informationen zu gängigen PIX-Befehlen finden Sie unter Using nat, global, static, rohr and access-list Commands and Port Redirection (Forwarding) on PIX.

Hinweis: Einige Optionen in anderen ASDM-Versionen können sich von den Optionen in ASDM 5.1 unterscheiden. Weitere Informationen finden Sie in der ASDM-Dokumentation.

Voraussetzungen

Anforderungen

Wenn Sie hinter einer PIX-Firewall mehrere interne Netzwerke hinzufügen, sollten Sie folgende Punkte berücksichtigen:

- Das PIX unterstützt keine sekundäre Adressierung.
- Hinter dem PIX muss ein Router verwendet werden, um das Routing zwischen dem vorhandenen Netzwerk und dem neu hinzugefügten Netzwerk zu ermöglichen.
- Das Standard-Gateway aller Hosts muss auf den internen Router zeigen.
- Fügen Sie dem internen Router eine Standardroute hinzu, die auf das PIX zeigt.
- Löschen Sie den ARP-Cache (Address Resolution Protocol) auf dem internen Router.

Informationen zur Konfiguration des Geräts durch den ASDM finden Sie unter Zulassen von HTTPS-Zugriff für ASDM.

Verwendete Komponenten

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

- PIX Security Appliance 515E mit Softwareversion 7.1
- ASDM 5.1
- Cisco Router mit Cisco IOS® Software, Version 12.3(7)T

Hinweis: Dieses Dokument wurde mit der PIX/ASA-Softwareversion 8.x und der Cisco IOS-Softwareversion 12.4 neu zertifiziert.

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 Cisco ASA Security Appliance Version 7.x oder höher verwendet werden.

Konventionen

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

Konfigurieren

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.

Die in dieser Konfiguration verwendeten IP-Adressierungsschemata sind im Internet nicht rechtlich routbar. Es handelt sich um RFC 1918-Adressen, die in einer Laborumgebung verwendet wurden.

Hintergrundinformationen

In diesem Szenario sind drei interne Netzwerke (10.1.1.0/24, 10.2.1.0/24 und 10.3.1.0/24) über PIX mit dem Internet (oder einem externen Netzwerk) verbunden. Die internen Netzwerke sind mit der internen Schnittstelle von PIX verbunden. Die Internetverbindung erfolgt über einen Router, der mit der externen Schnittstelle des PIX verbunden ist. Das PIX hat die IP-Adresse 172.16.1.1/24.

Die statischen Routen werden verwendet, um die Pakete von den internen Netzwerken zum Internet und umgekehrt weiterzuleiten. Anstatt die statischen Routen zu verwenden, können Sie auch ein dynamisches Routing-Protokoll wie Routing Information Protocol (RIP) oder Open Shortest Path First (OSPF) verwenden.

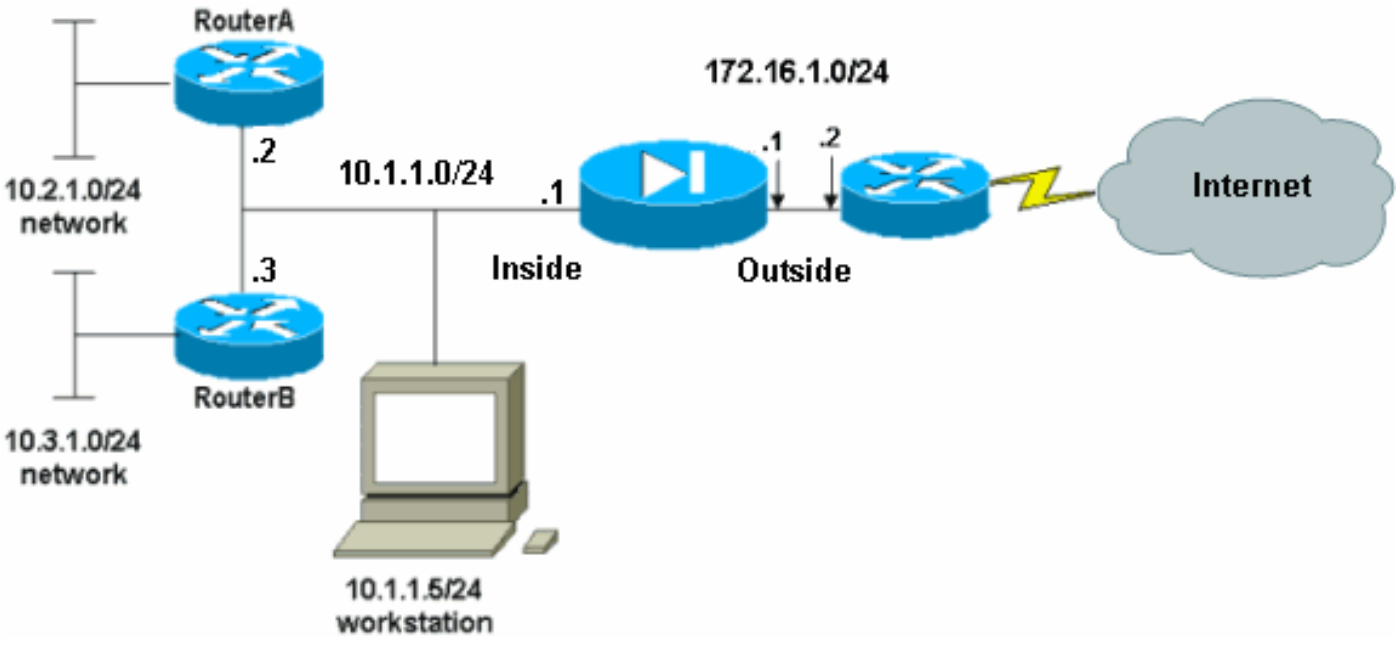
Die internen Hosts kommunizieren mit dem Internet, indem sie die internen Netzwerke auf PIX mithilfe dynamischer NAT übersetzen (Pool von IP-Adressen - 172.16.1.5 bis 172.16.1.10). Wenn der Pool der IP-Adressen ausgeschöpft ist, wird die PIX-Route PAT (unter Verwendung der IP-Adresse 172.16.1.4) an die internen Hosts weiterleiten, um ins Internet zu gelangen.

Weitere Informationen zu NAT/PAT finden Sie in den PIX/ASA 7.x NAT- und PAT-Anweisungen.

Hinweis: Wenn die statische NAT die externe IP-Adresse (global_IP) für die Übersetzung verwendet, kann dies zu einer Übersetzung führen. Verwenden Sie daher in der statischen Übersetzung das Schlüsselwort interface anstelle der IP-Adresse.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Das Standard-Gateway der Hosts im Netzwerk 10.1.1.0 verweist auf RouterA. Eine Standardroute auf RouterB wird hinzugefügt, die auf RouterA zeigt. RouterA verfügt über eine Standardroute, die

auf die PIX-interne Schnittstelle zeigt.

Konfigurationen

In diesem Dokument werden folgende Konfigurationen verwendet:

- RouterA-Konfiguration
- RouterB-Konfiguration
- Konfiguration der PIX Security Appliance 7.1PIX-Konfiguration mit ASDMCLI-Konfiguration der PIX Security Appliance

RouterA-Konfiguration

```
RouterA#show running-config
Building configuration...

Current configuration : 1151 bytes
!
version 12.4
service config
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RouterA
!

interface Ethernet2/0
 ip address 10.2.1.1 255.255.255.0
 half-duplex
!

interface Ethernet2/1
 ip address 10.1.1.2 255.255.255.0
 half-duplex
!
ip classless

ip route 0.0.0.0 0.0.0.0 10.1.1.1
ip route 10.3.1.0 255.255.255.0 10.1.1.3
!
!
line con 0
line aux 0
line vty 0 4
!
end
RouterA#
```

RouterB-Konfiguration

```
RouterB#show running-config
Building configuration...
Current configuration : 1132 bytes
!
version 12.4
service config
service timestamps debug datetime msec
service timestamps log datetime msec
```

```
no service password-encryption
!
hostname RouterB
!

interface FastEthernet0/0
 ip address 10.1.1.3 255.255.255.0
 speed auto
!

interface Ethernet1/0
 ip address 10.3.1.1 255.255.255.0
 half-duplex
!
ip classless

ip route 0.0.0.0 0.0.0.0 10.1.1.2
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
!
end
RouterB#
```

Wenn Sie das ASDM für die Konfiguration der PIX Security Appliance verwenden möchten, das Gerät aber nicht neu gestartet haben, führen Sie die folgenden Schritte aus:

1. In den PIX einstecken.
2. Verwenden Sie aus einer gelöschten Konfiguration die interaktiven Aufforderungen, um ASDM für die Verwaltung des PIX von der Workstation 10.1.1.5 zu aktivieren.

Konfiguration der PIX Security Appliance 7.1

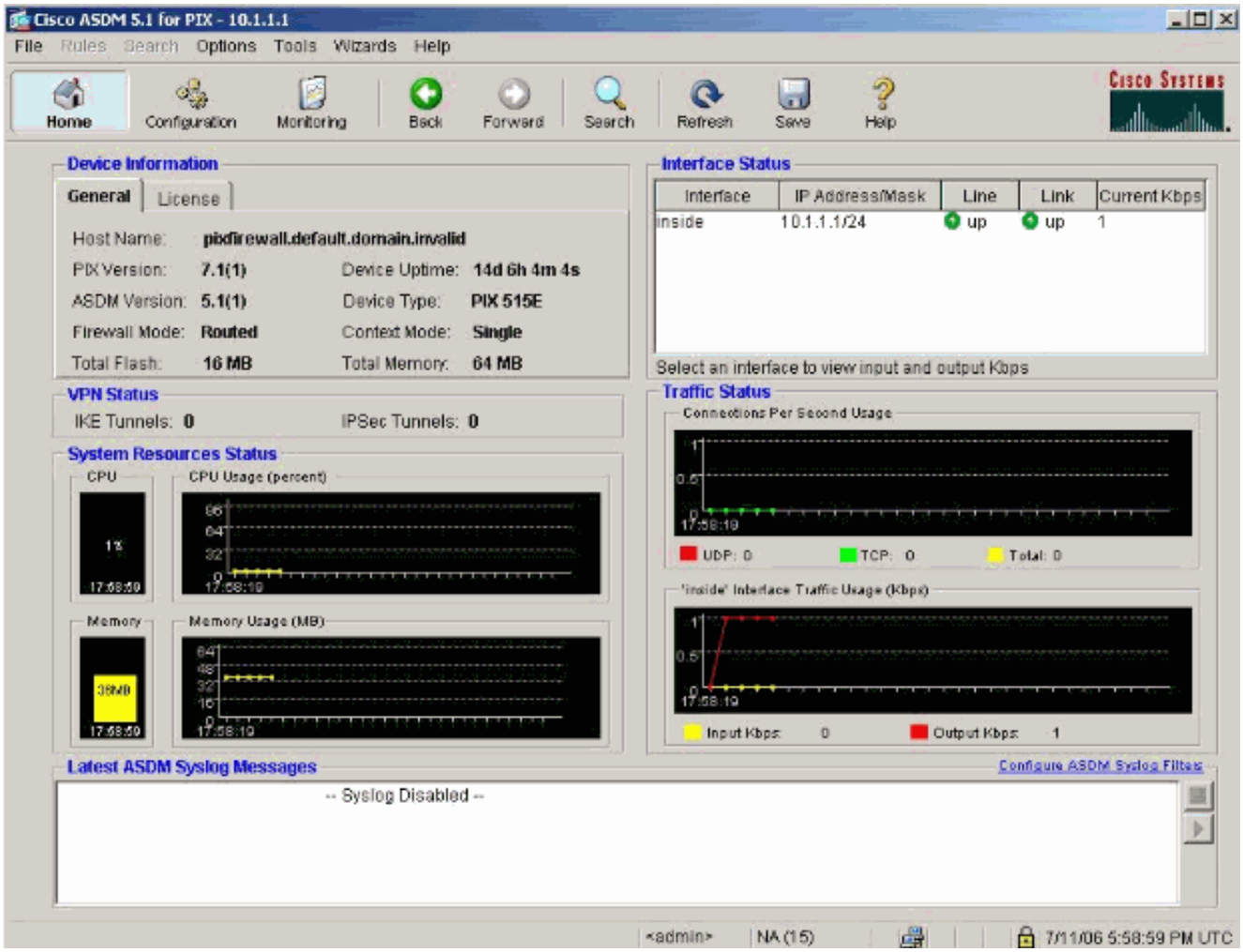
```
Pre-configure Firewall now through interactive prompts
[yes]? yes
Firewall Mode [Routed]:
Enable password [<use current password>]: cisco
Allow password recovery [yes]?
Clock (UTC):
  Year [2005]:
  Month [Mar]:
  Day [15]:
  Time [05:40:35]: 14:45:00
Inside IP address: 10.1.1.1
Inside network mask: 255.255.255.0
Host name: OZ-PIX
Domain name: cisco.com
IP address of host running Device Manager: 10.1.1.5

The following configuration will be used:
         Enable password: cisco
         Allow password recovery: yes
         Clock (UTC): 14:45:00 Mar 15 2005
         Firewall Mode: Routed
         Inside IP address: 10.1.1.1
         Inside network mask: 255.255.255.0
         Host name: OZ-PIX
```

```
         Domain name: cisco.com
         IP address of host running Device Manager:
10.1.1.5

Use this configuration and write to flash? yes
         INFO: Security level for "inside" set to 100 by
default.
         Cryptochecksum: a0bff9bb aa3d815f c9fd269a
3f67fef5

965 bytes copied in 0.880 secs
         INFO: converting 'fixup protocol dns maximum-
length 512' to MPF commands
         INFO: converting 'fixup protocol ftp 21' to MPF
commands
         INFO: converting 'fixup protocol h323_h225
1720' to MPF commands
         INFO: converting 'fixup protocol h323_ras 1718-
1719' to MPF commands
         INFO: converting 'fixup protocol netbios 137-
138' to MPF commands
         INFO: converting 'fixup protocol rsh 514' to
MPF commands
         INFO: converting 'fixup protocol rtsp 554' to
MPF commands
         INFO: converting 'fixup protocol sip 5060' to
MPF commands
         INFO: converting 'fixup protocol skinny 2000'
to MPF commands
         INFO: converting 'fixup protocol smtp 25' to
MPF commands
         INFO: converting 'fixup protocol sqlnet 1521'
to MPF commands
         INFO: converting 'fixup protocol sunrpc_udp
111' to MPF commands
         INFO: converting 'fixup protocol tftp 69' to
MPF commands
         INFO: converting 'fixup protocol sip udp 5060'
to MPF commands
         INFO: converting 'fixup protocol xdmcp 177' to
MPF commands

Type help or '?' for a list of available commands.
         OZ-PIX>
```

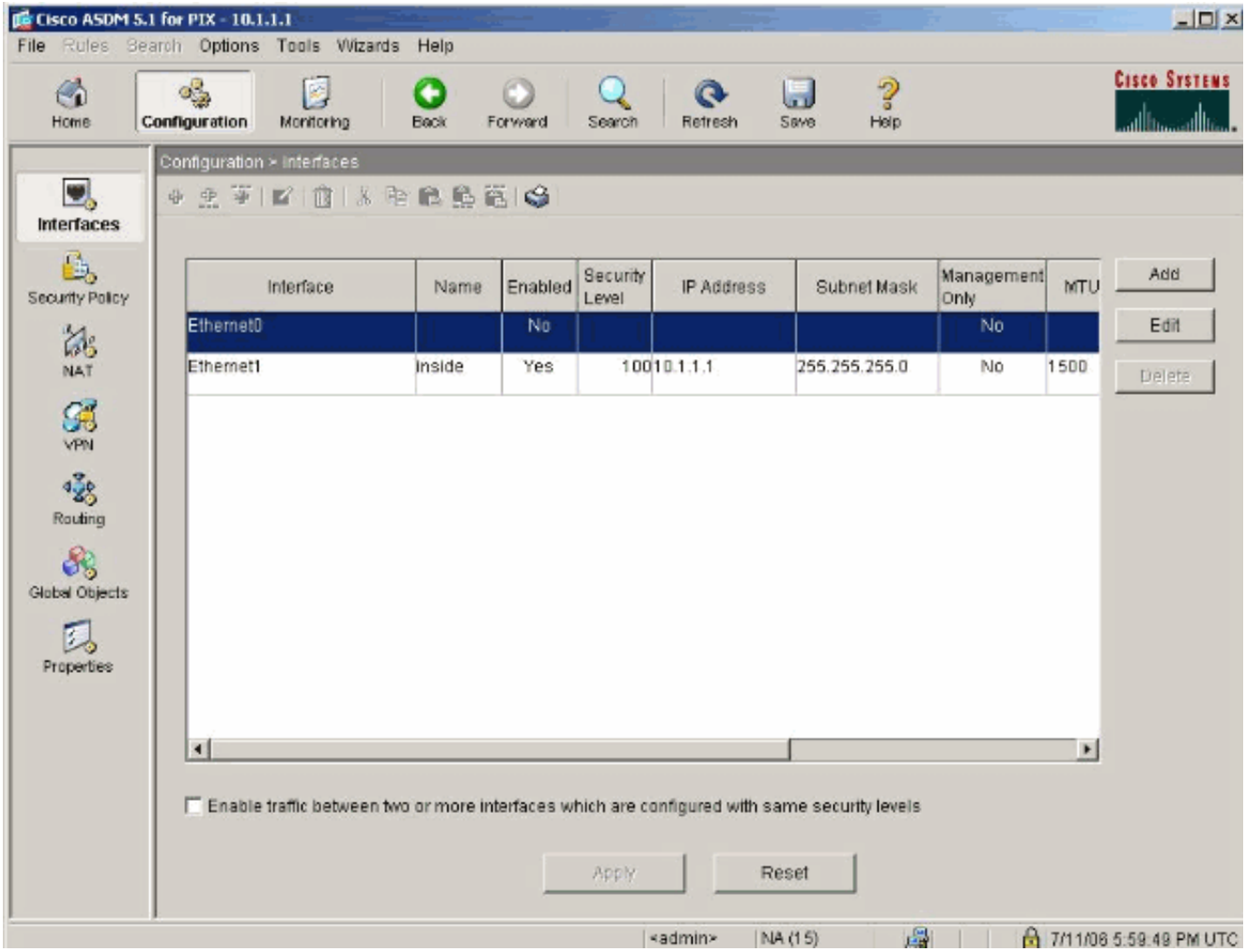
PIX-Konfiguration mit ASDM

Führen Sie die folgenden Schritte aus, um die Konfiguration über die ASDM-GUI durchzuführen:

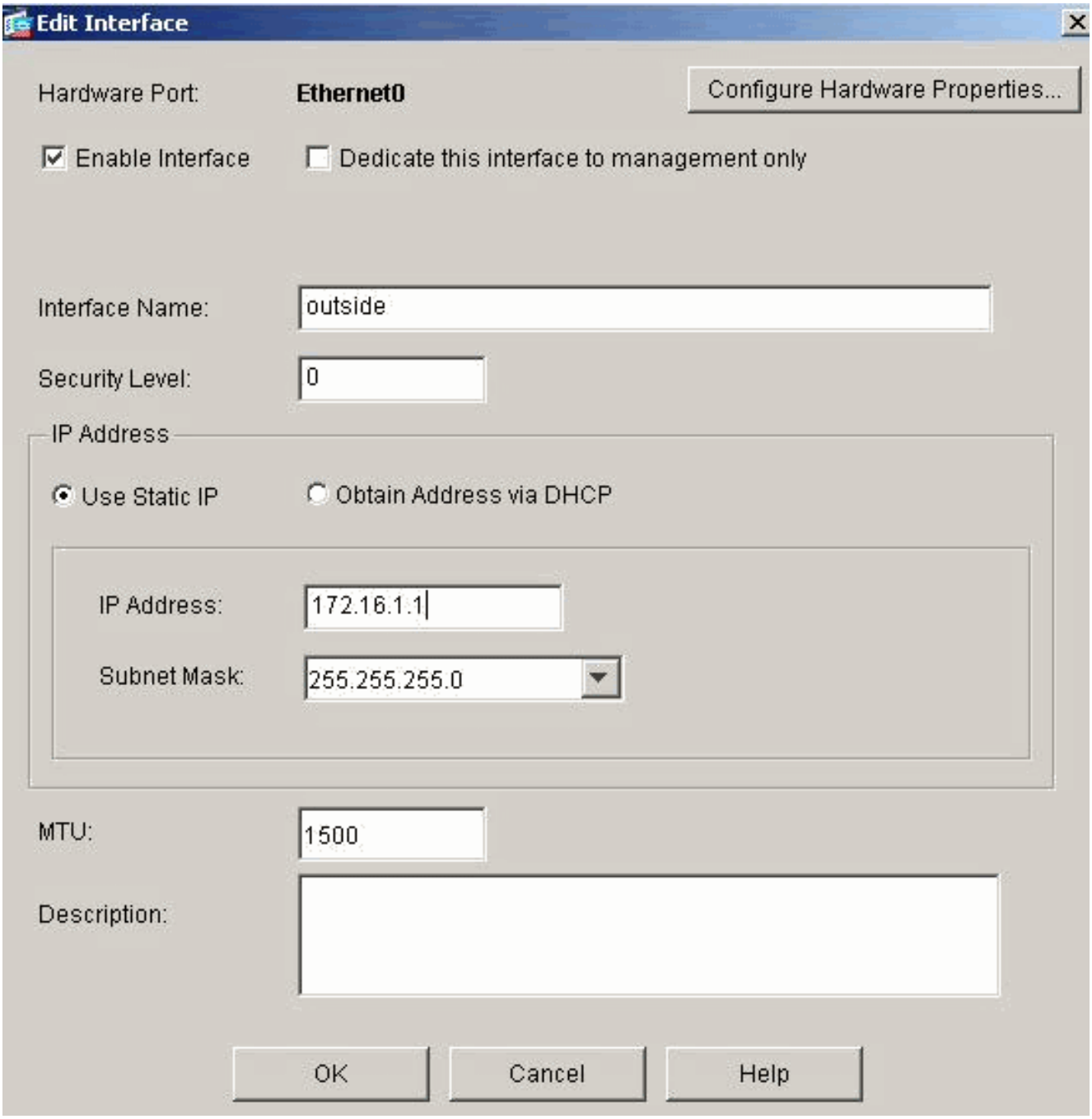
1. Öffnen Sie auf der Workstation 10.1.1.5 einen Webbrowser, um ADSM zu verwenden (in diesem Beispiel https://10.1.1.1).
2. Klicken Sie auf den Zertifikatsaufforderungen auf Ja.
3. Melden Sie sich wie zuvor konfiguriert mit dem enable-Kennwort an.
4. Wenn ASDM zum ersten Mal auf dem PC ausgeführt wird, werden Sie aufgefordert, ASDM Launcher oder ASDM als Java-Anwendung zu verwenden. In diesem Beispiel wird der ASDM Launcher ausgewählt und installiert.
5. Rufen Sie das ASDM Home-Fenster auf, und klicken Sie auf **Configuration**.



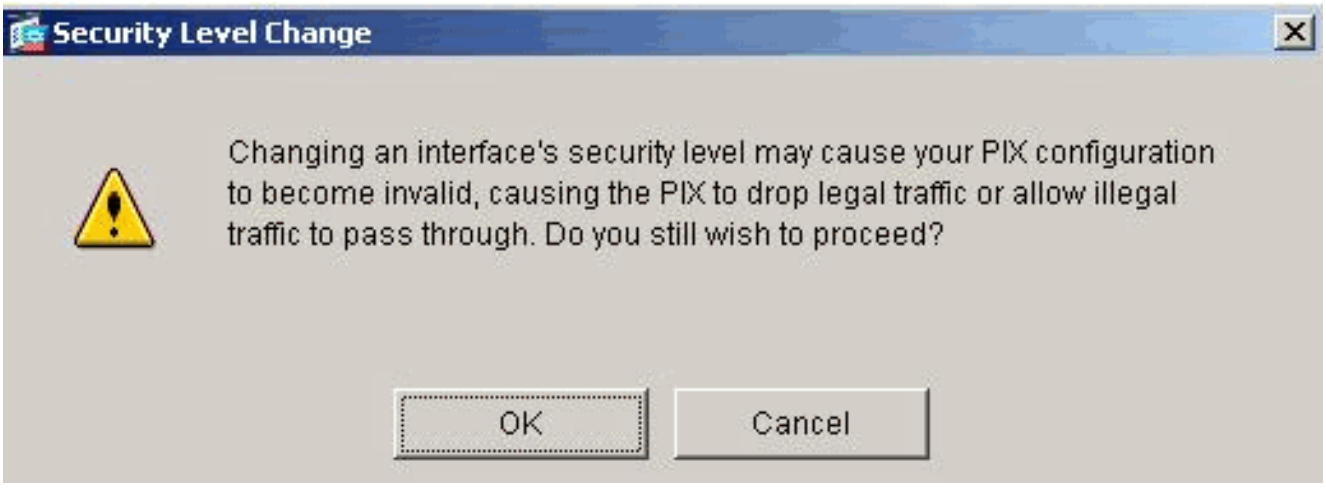
6. Wählen Sie **Interface > Edit**, um die externe Schnittstelle zu konfigurieren.



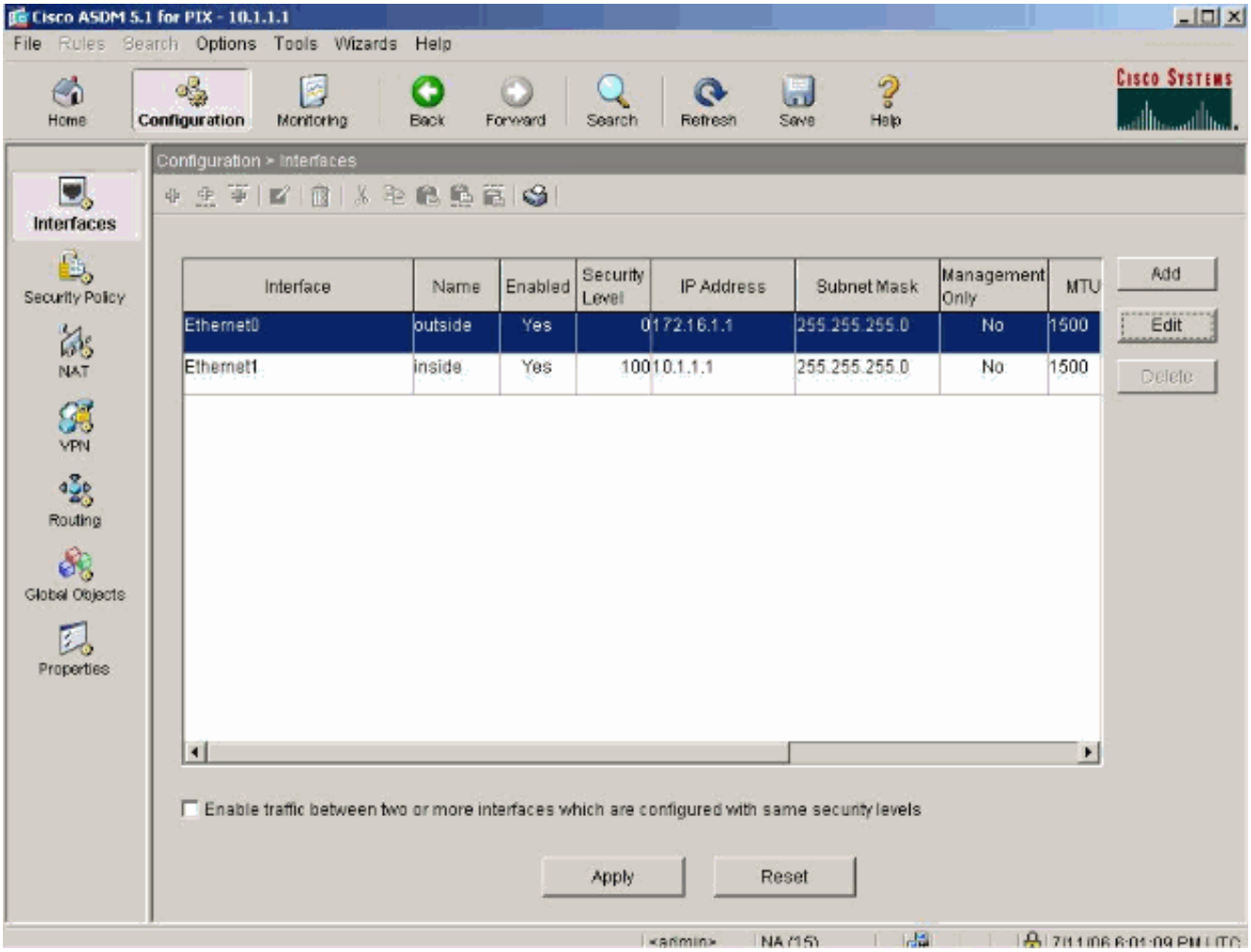
7. Geben Sie die Schnittstellendetails ein, und klicken Sie abschließend auf **OK**.



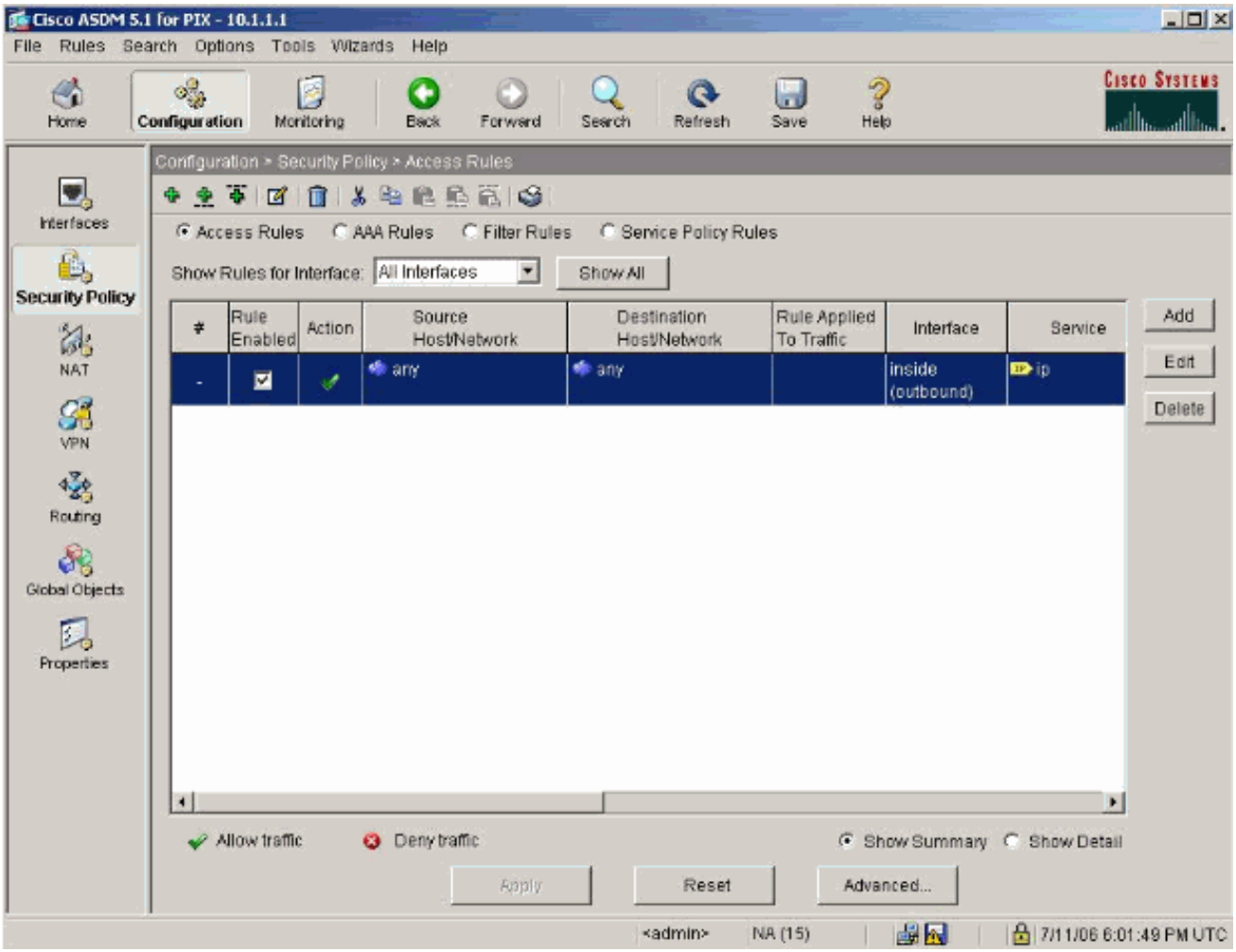
8. Klicken Sie im Dialogfeld zum Ändern der Sicherheitsstufe auf **OK**.



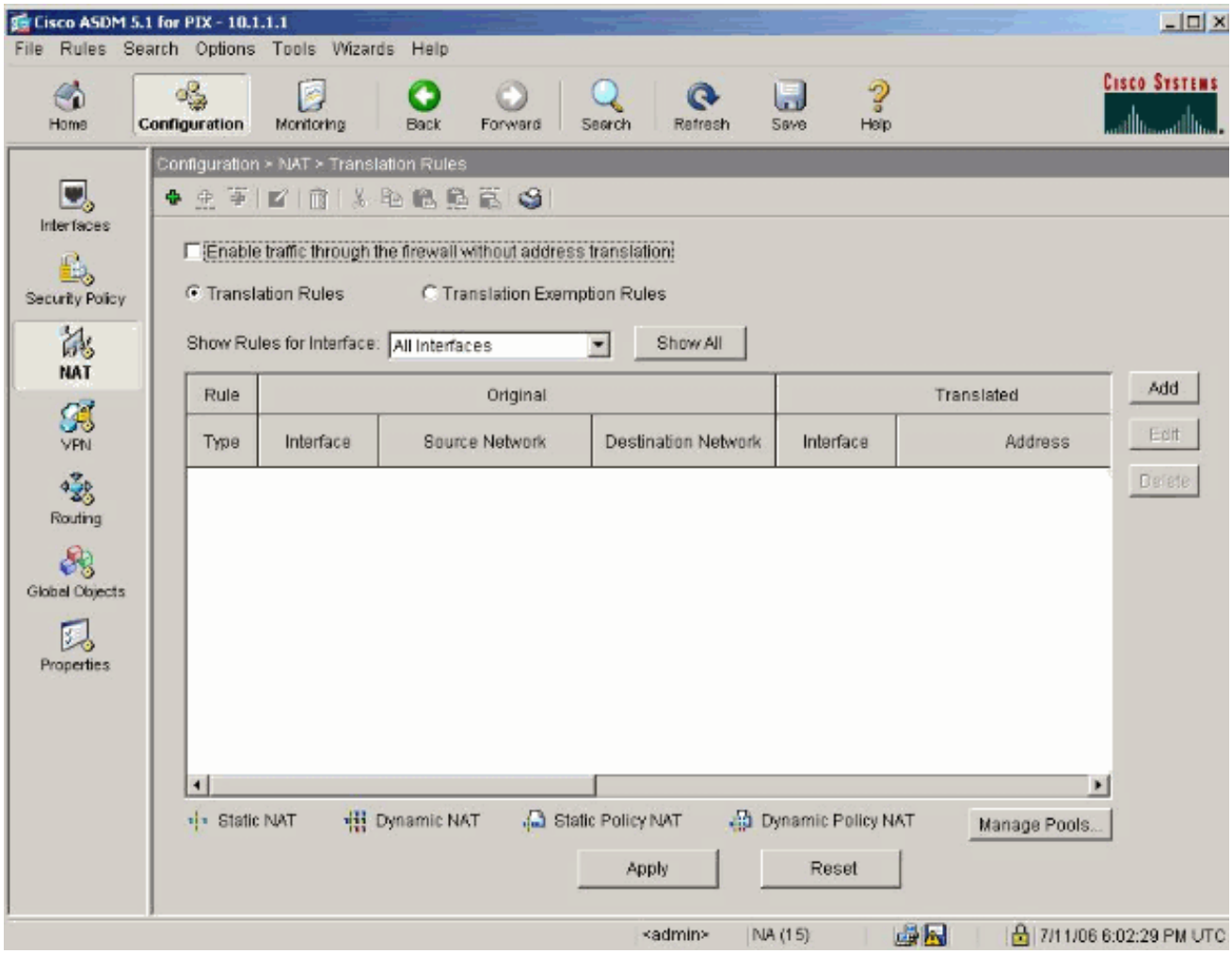
9. Klicken Sie auf **Apply**, um die Schnittstellenkonfiguration zu akzeptieren. Die Konfiguration wird auch auf den PIX übertragen.



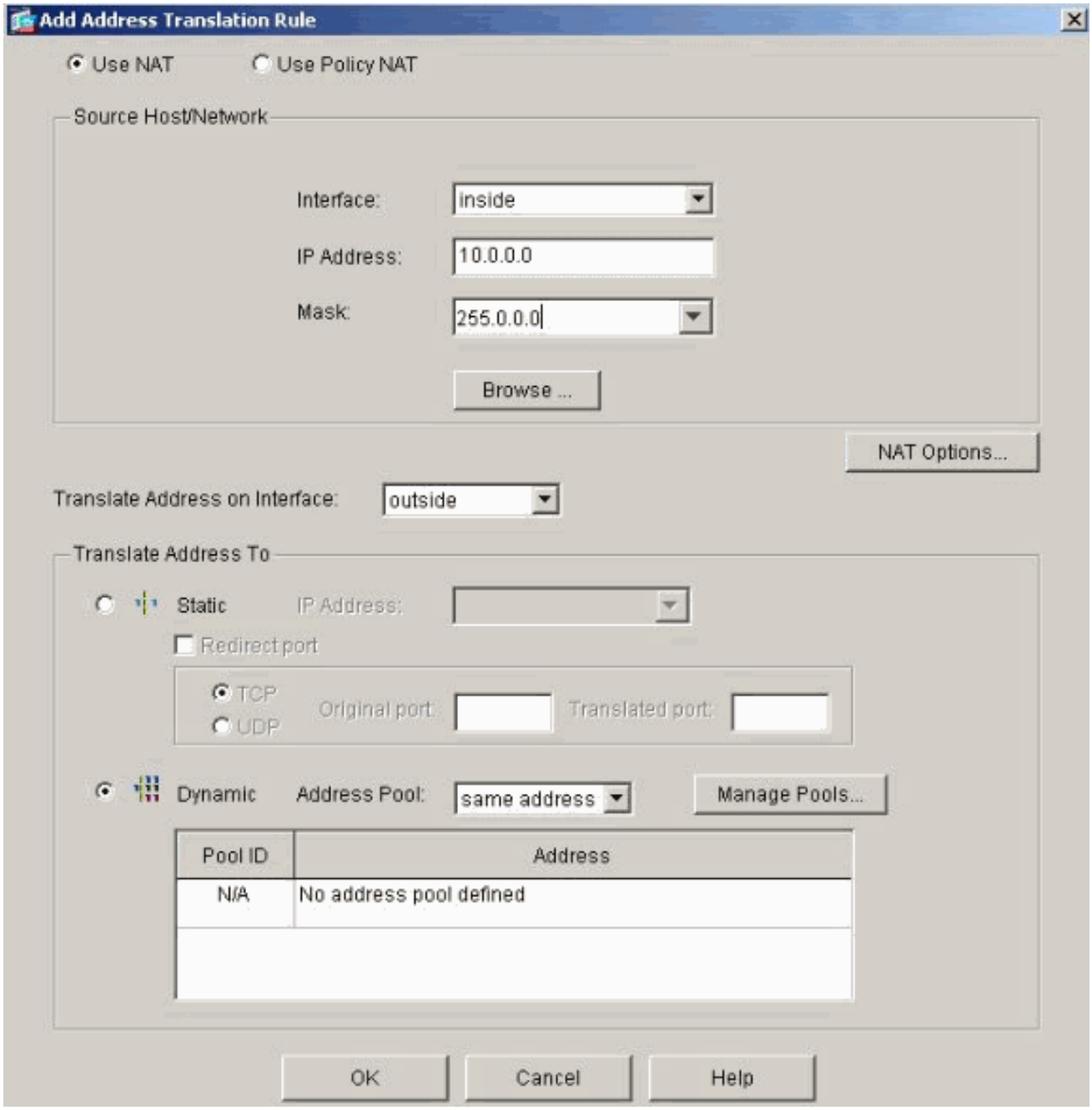
10. Wählen Sie auf der Registerkarte Funktionen **Sicherheitsrichtlinie** aus, um die verwendete Sicherheitsrichtlinienregel zu überprüfen. In diesem Beispiel wird die Standardinterne Regel verwendet.



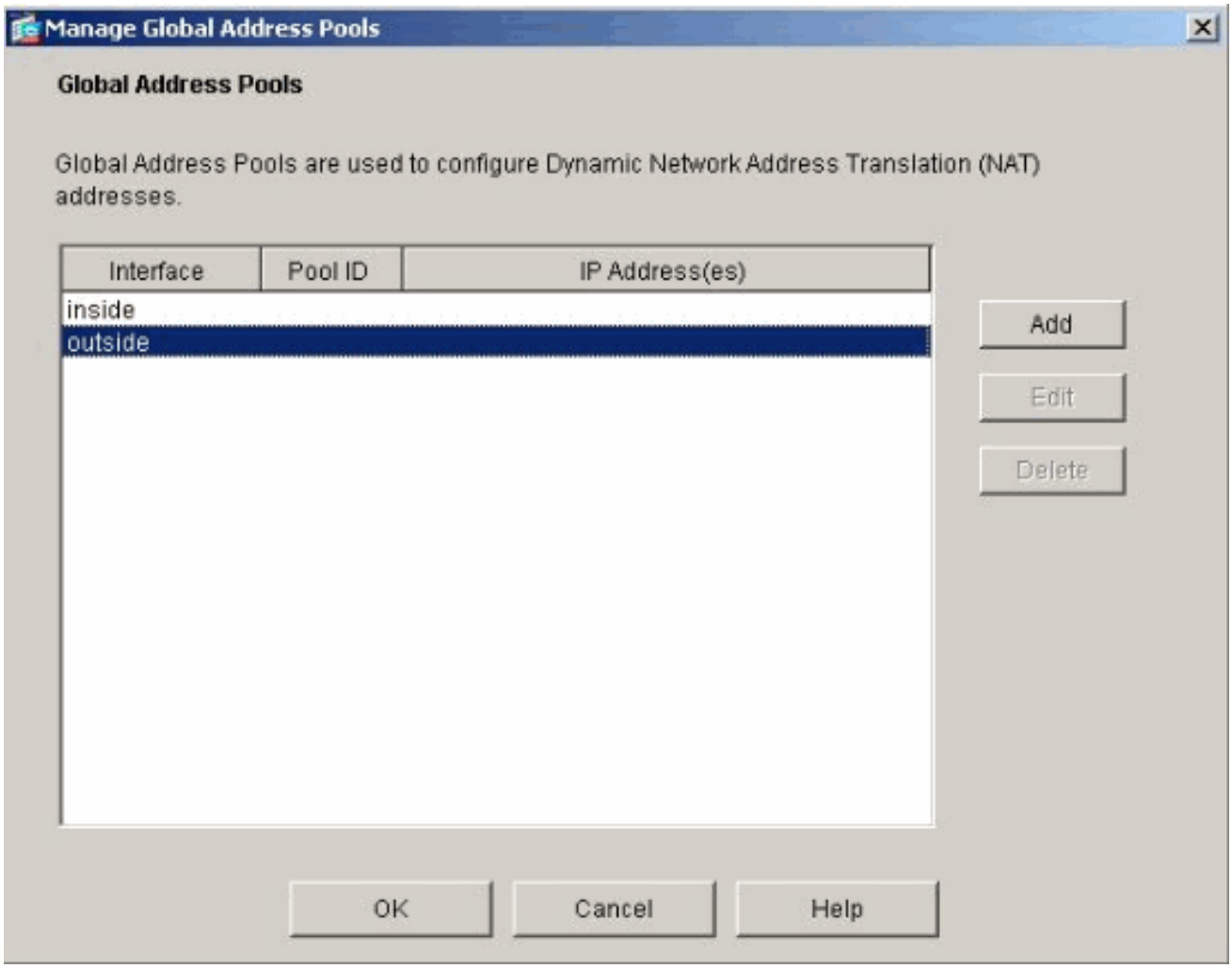
11. In diesem Beispiel wird NAT verwendet. Deaktivieren Sie das Kontrollkästchen **Datenverkehr durch die Firewall ohne Adressumwandlung aktivieren**, und klicken Sie auf **Hinzufügen**, um die NAT-Regel zu konfigurieren.



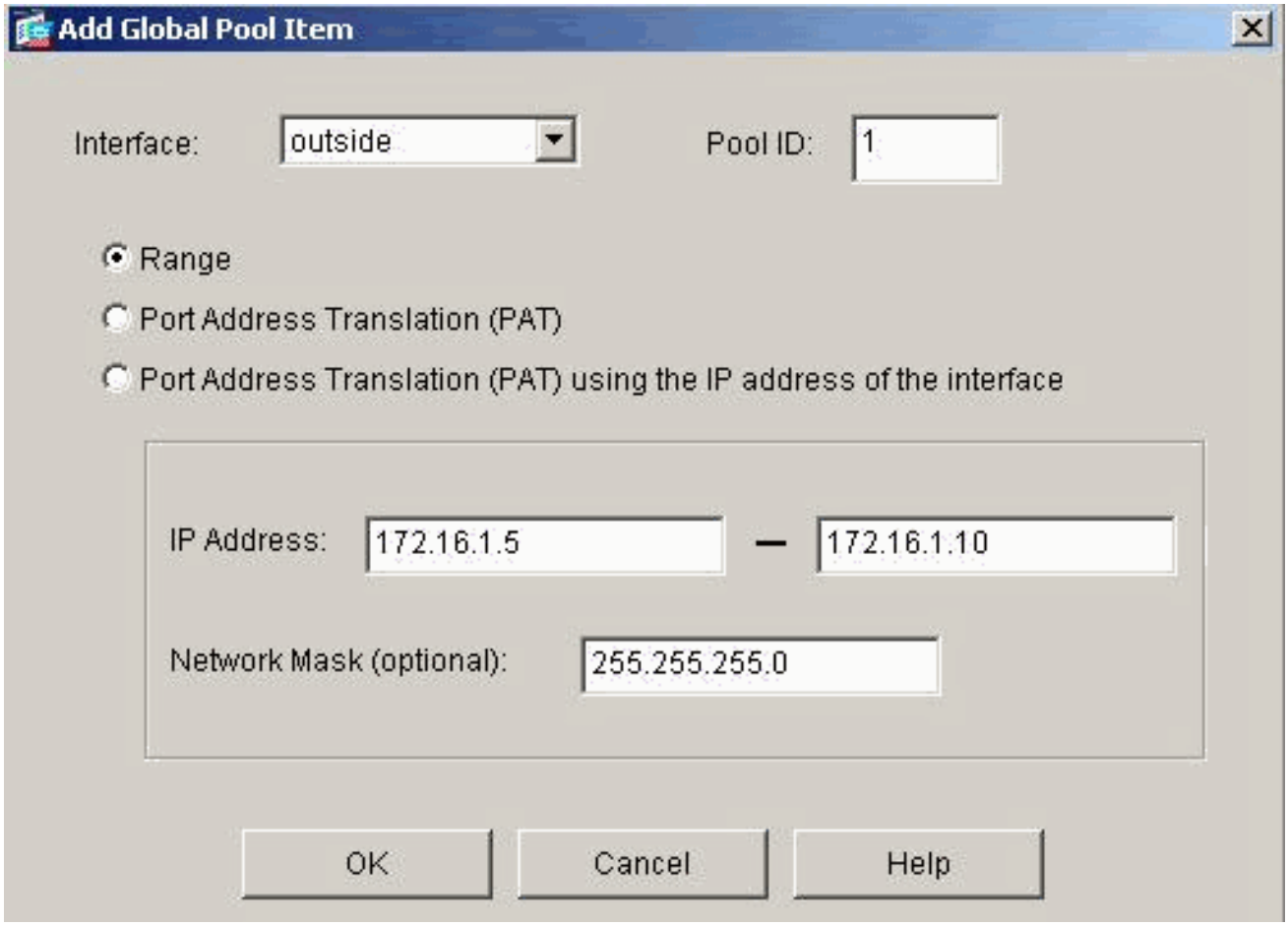
12. Konfigurieren Sie das Quellnetzwerk. In diesem Beispiel wird für die IP-Adresse 10.0.0.0 und für die Maske 255.0.0.0 verwendet.Klicken Sie auf **Pools verwalten**, um die NAT-Pooladressen zu
definieren.



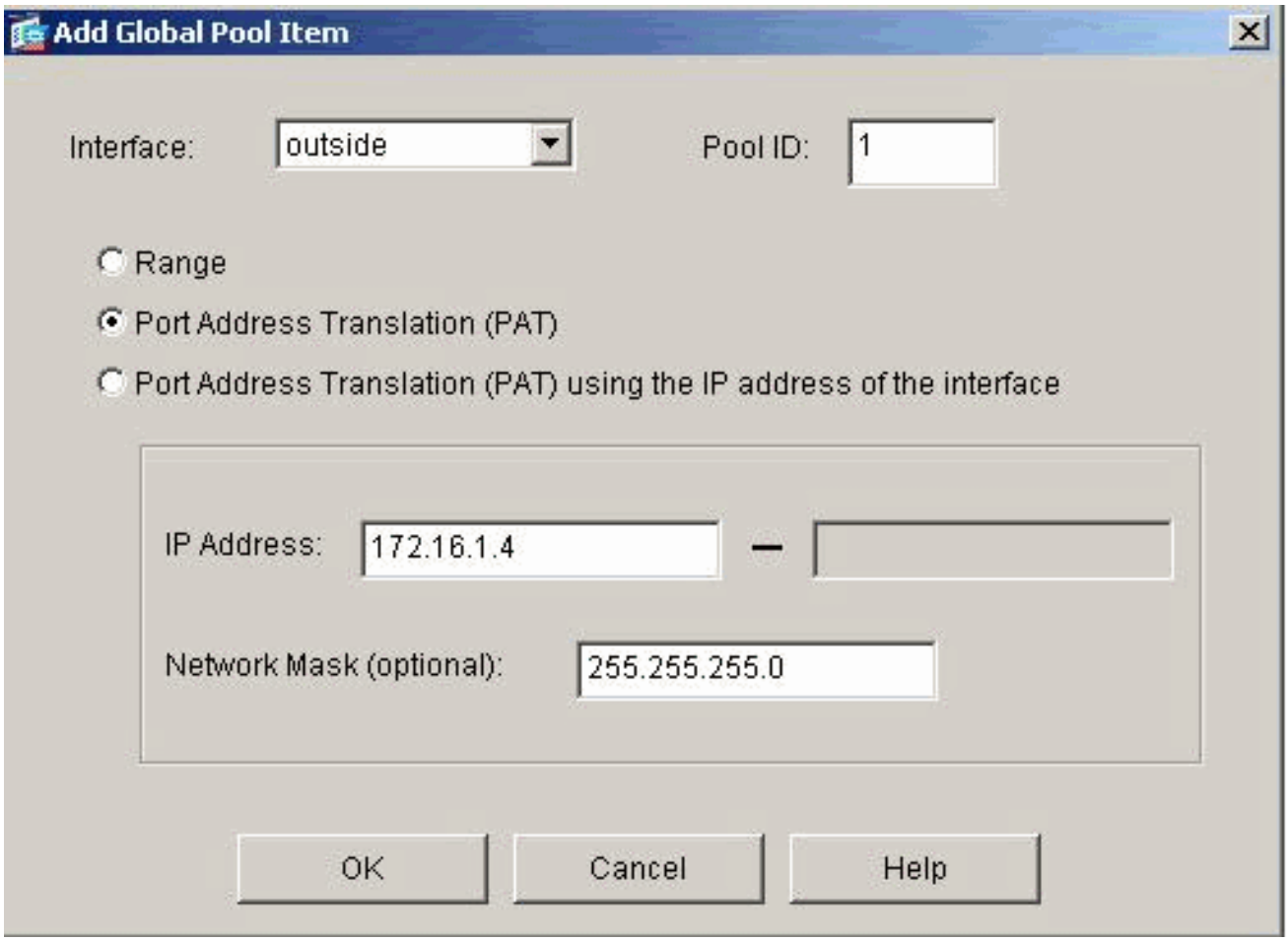
13. Wählen Sie die externe Schnittstelle aus, und klicken Sie auf **Hinzufügen**.



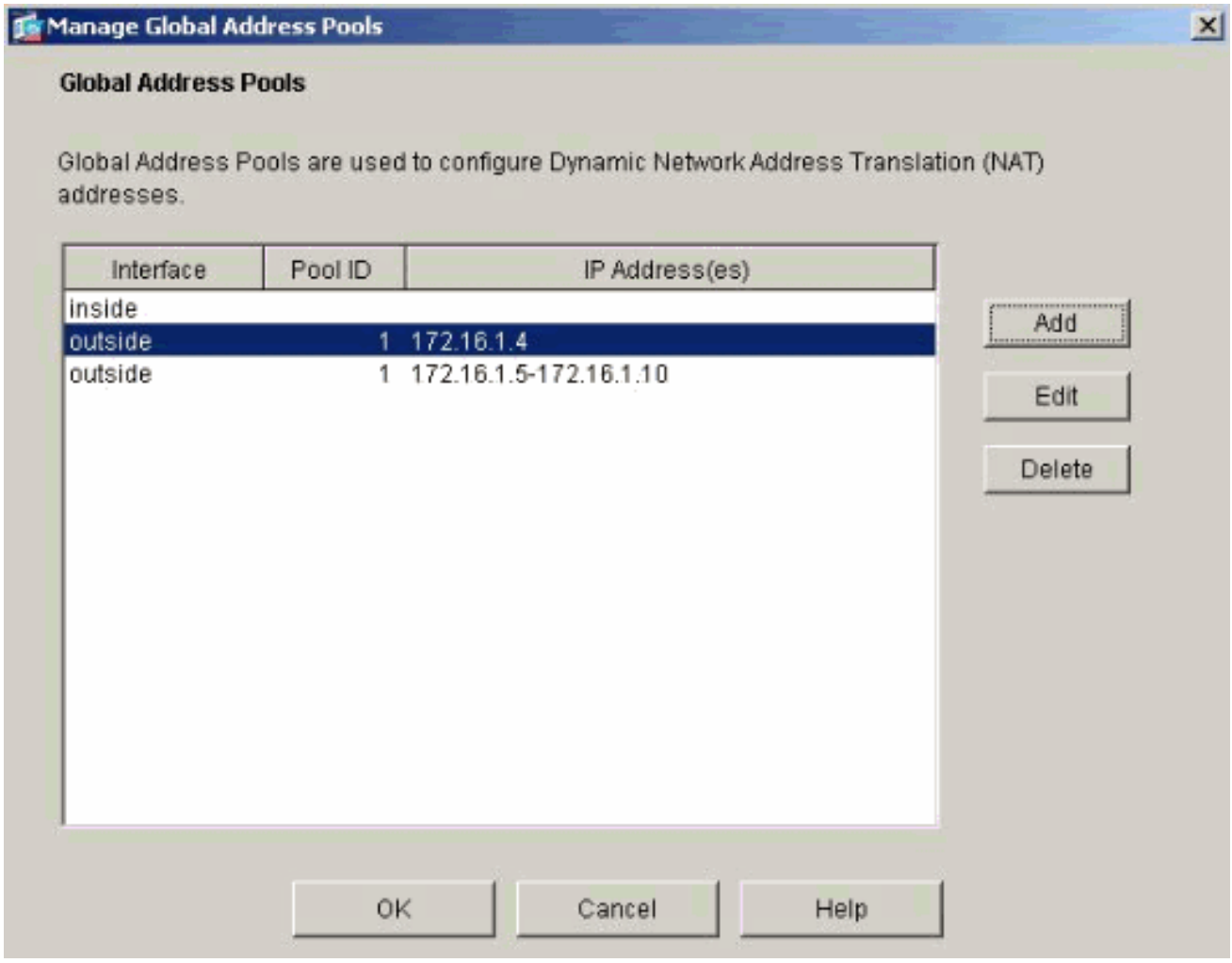
14. In diesem Beispiel werden ein Range-Adresspool und ein PAT-Adresspool konfiguriert. Konfigurieren Sie den Bereich für die NAT-Pooladresse, und klicken Sie auf **OK**.



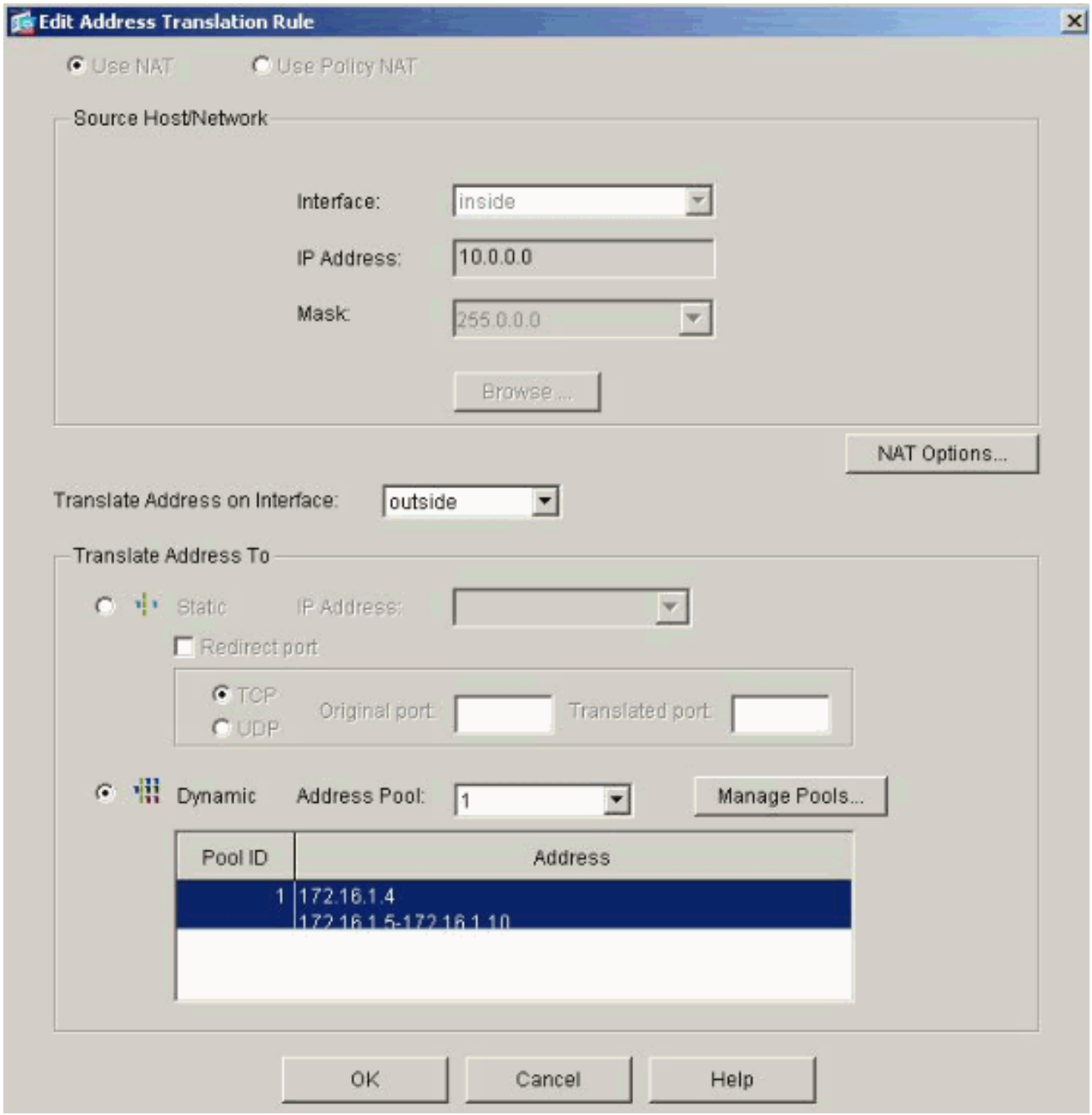
15. Wählen Sie in Schritt 13 die externe Schnittstelle aus, um die PAT-Adresse zu konfigurieren. Klicken Sie auf
OK



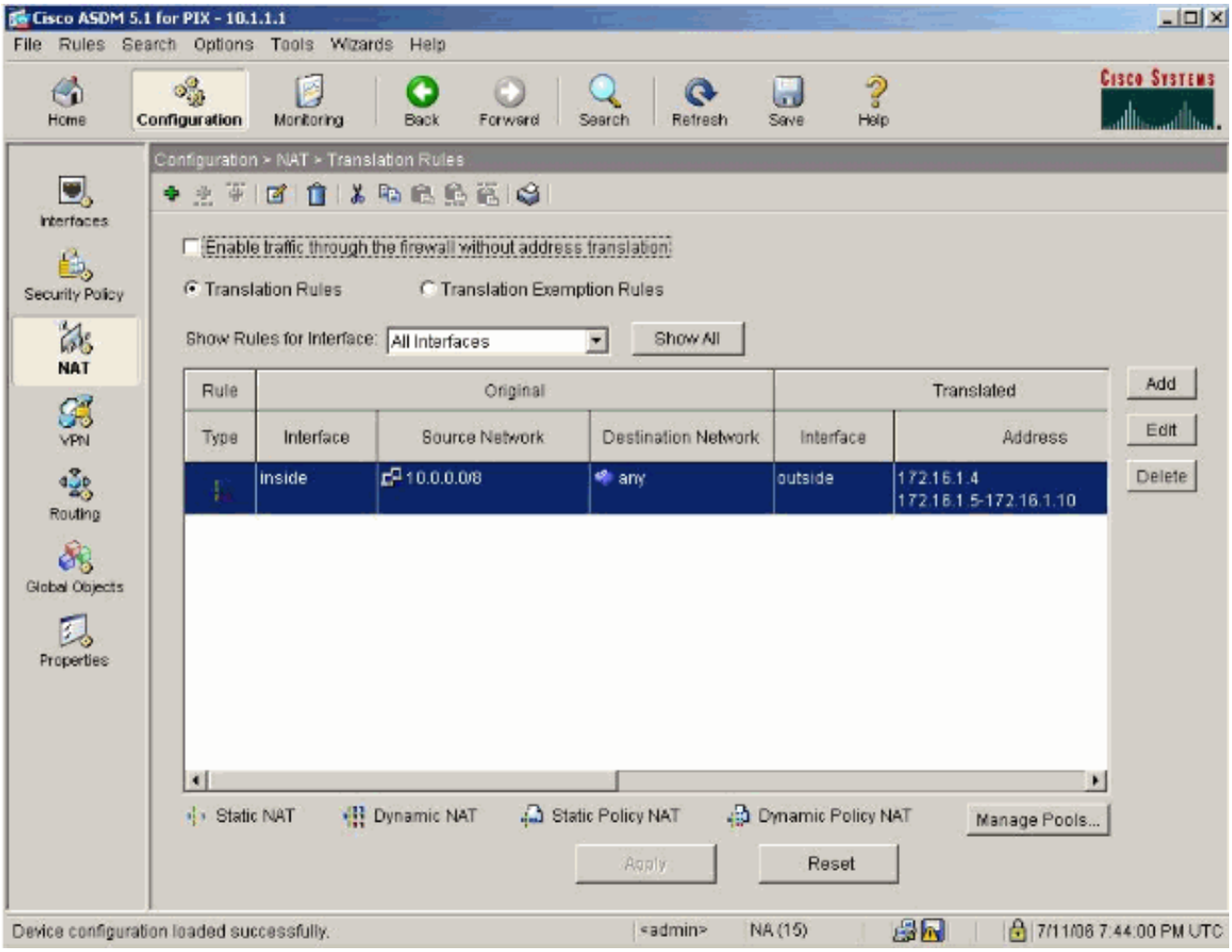
Klicken Sie auf **OK**, um fortzufahren.



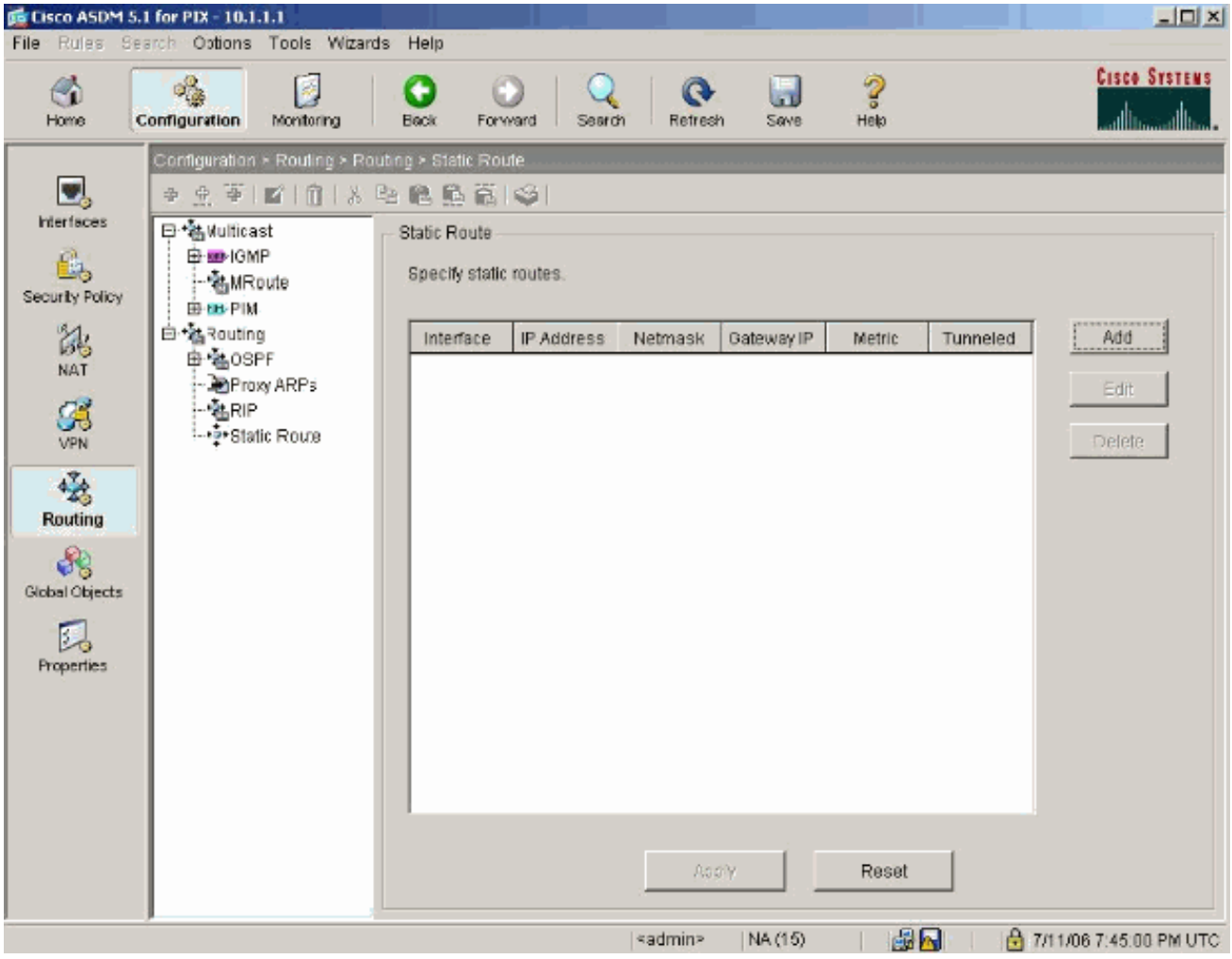
16. Wählen Sie im Fenster Edit Address Translation Rule (Adressenumwandlungsregel bearbeiten) die Pool-ID aus, die vom konfigurierten Quellnetzwerk verwendet werden soll. Klicken Sie auf **OK**.



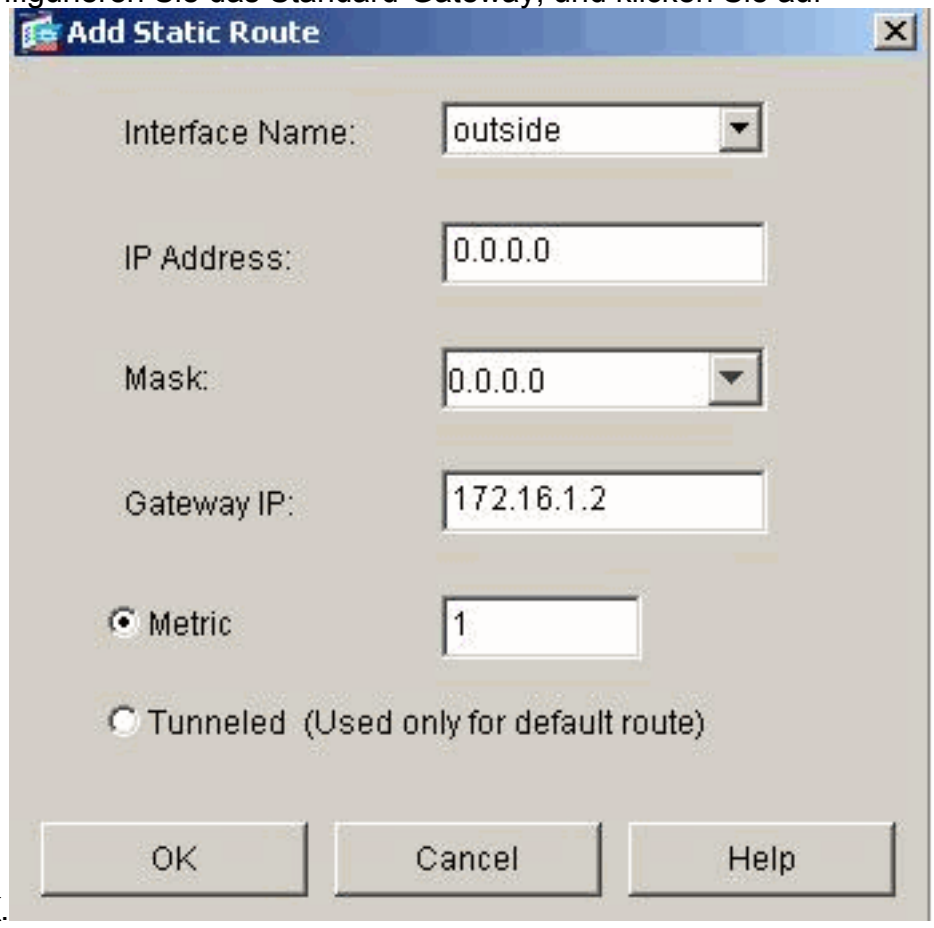
17. Klicken Sie auf **Apply**, um die konfigurierte NAT-Regel auf den PIX zu übertragen.



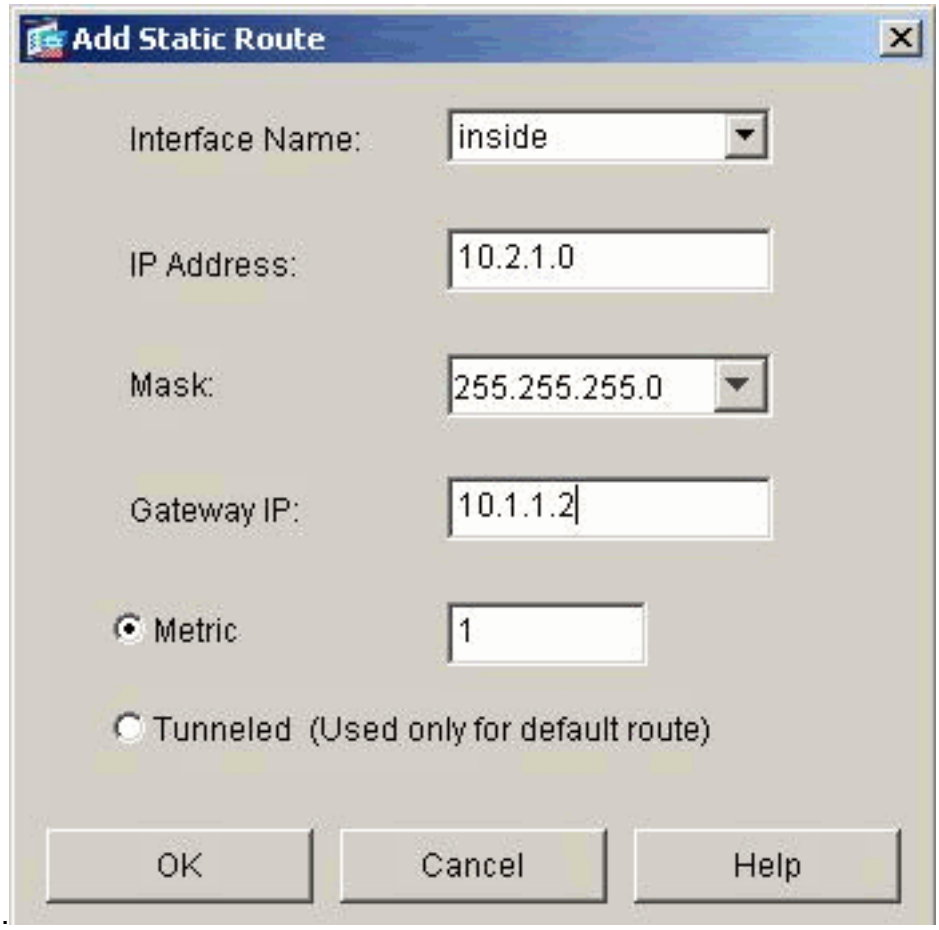
18. In diesem Beispiel werden statische Routen verwendet. Klicken Sie auf **Routing**, wählen Sie **Statische Route aus**, und klicken Sie auf **Hinzufügen**.



19. Konfigurieren Sie das Standard-Gateway, und klicken Sie auf **OK**.

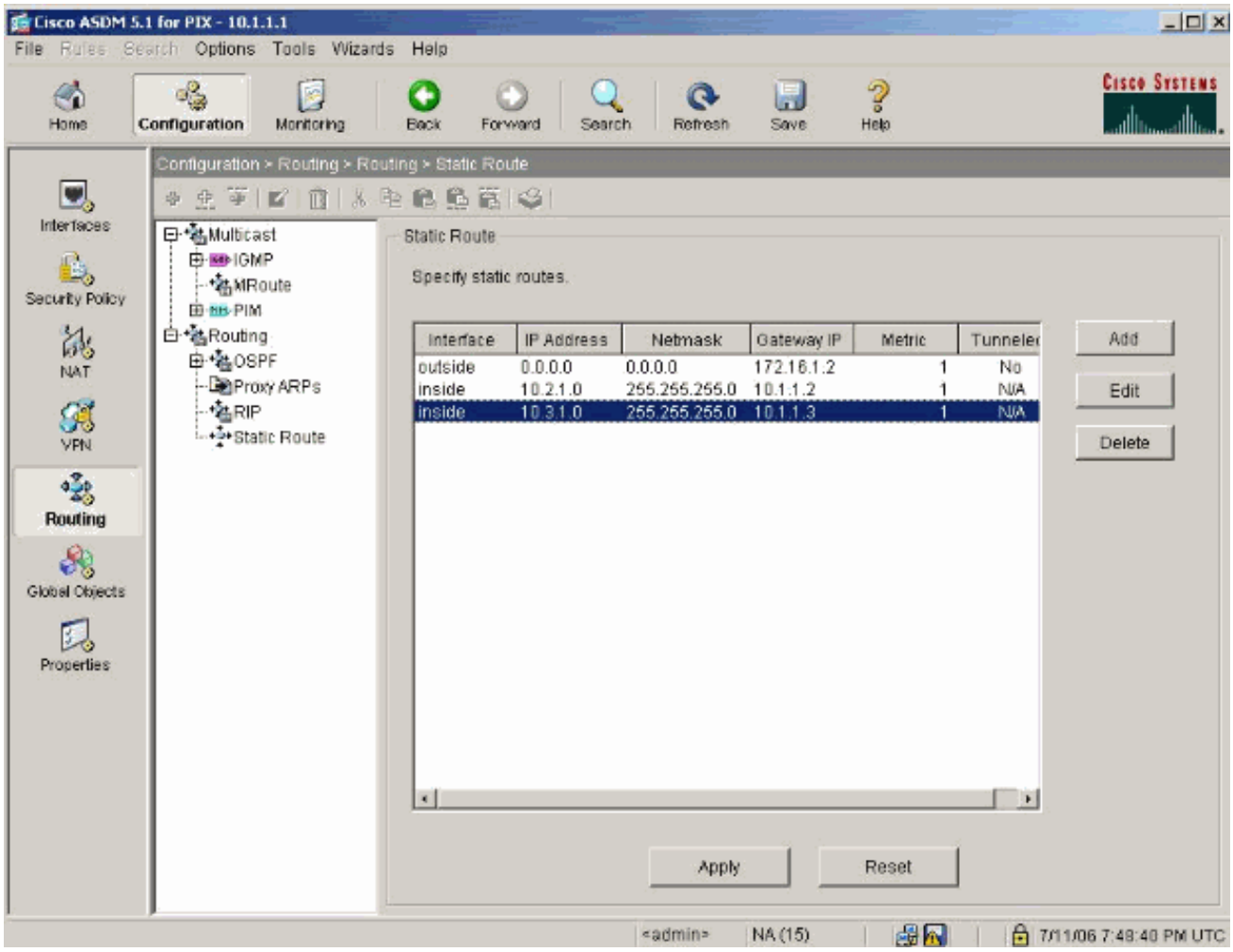


20. Klicken Sie auf **Hinzufügen**, und fügen Sie die Routen zu den internen Netzwerken



hinzu.

21. Bestätigen Sie, dass die richtigen Routen konfiguriert sind, und klicken Sie auf **Übernehmen**.



PIX-Konfiguration mit CLI

Die Konfiguration über die ASDM-GUI ist nun abgeschlossen.

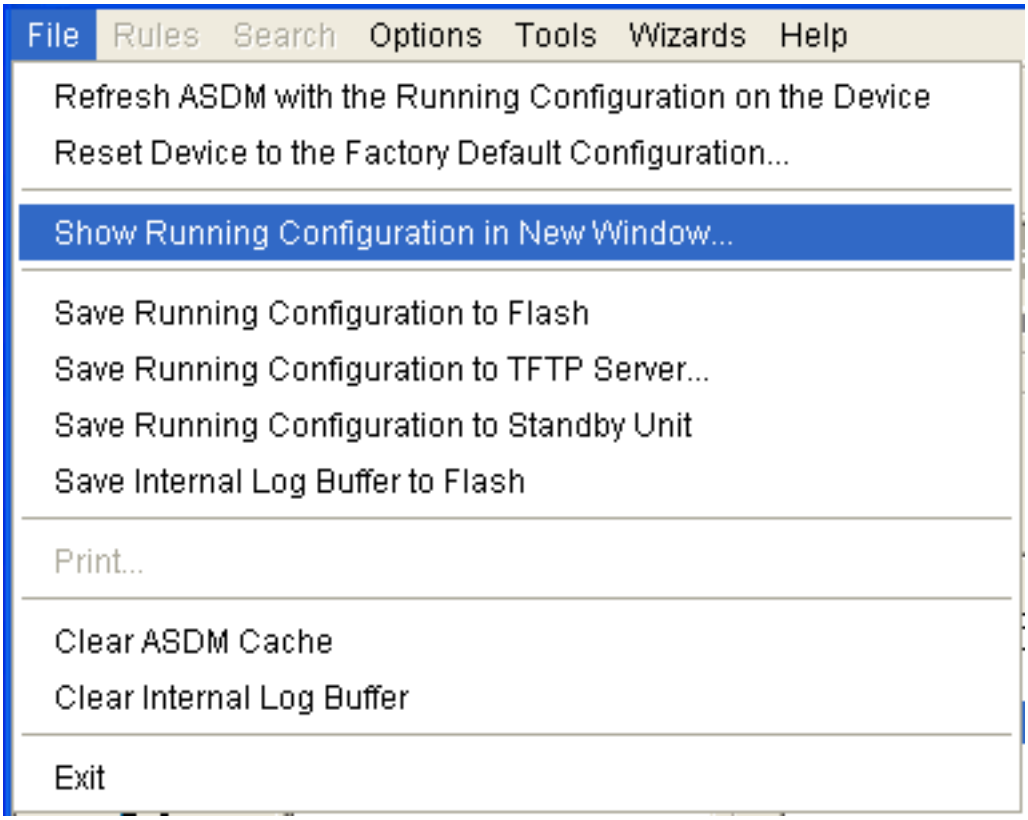
Diese Konfiguration wird über die CLI angezeigt:

CLI der PIX Security Appliance

```
pixfirewall(config)#write terminal
PIX Version 7.0(0)102
names
!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 172.16.1.1 255.255.255.0
!

interface Ethernet1
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0
!--- Assign name and IP address to the interfaces enable
password 2KFQnbNIdI.2KYOU encrypted passwd
2KFQnbNIdI.2KYOU encrypted asdm image
flash:/asdmfile.50073 no asdm history enable arp timeout
14400 nat-control
!--- Enforce a strict NAT for all the traffic through
the Security appliance global (outside) 1 172.16.1.5-
```

```
172.16.1.10 netmask 255.255.255.0
!--- Define a pool of global addresses 172.16.1.5 to
172.16.1.10 with !--- NAT ID 1 to be used for NAT global
(outside) 1 172.16.1.4 netmask 255.255.255.0
!--- Define a single IP address 172.16.1.4 with NAT ID 1
to be used for PAT nat (inside) 1 10.0.0.0 255.0.0.0
!--- Define the inside networks with same NAT ID 1 used
in the global command for NAT route inside 10.3.1.0
255.255.255.0 10.1.1.3 1
route inside 10.2.1.0 255.255.255.0 10.1.1.2 1
!--- Configure static routes for routing the packets
towards the internal network route outside 0.0.0.0
0.0.0.0 172.16.1.2 1
!--- Configure static route for routing the packets
towards the Internet (or External network) timeout xlate
3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp
0:02:00 icmp 0:00:02 sunrpc 0:10:00 h323 0:05:00 h225
1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 sip 0:30:00
sip_media 0:02:00 timeout uauth 0:05:00 absolute http
server enable
!--- Enable the HTTP server on PIX for ASDM access http
10.1.1.5 255.255.255.255 inside
!--- Enable HTTP access from host 10.1.1.5 to configure
PIX using ASDM (GUI) ! !--- Output suppressed ! !
Cryptochecksum:a0bff9bbaa3d815fc9fd269a3f67fef5 : end
```

Wählen Sie **File (Datei) > Show Running Configuration (Konfiguration anzeigen) in New Window**, um die CLI-Konfiguration im ASDM anzuzeigen.



Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Befehle zur Fehlerbehebung

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**.

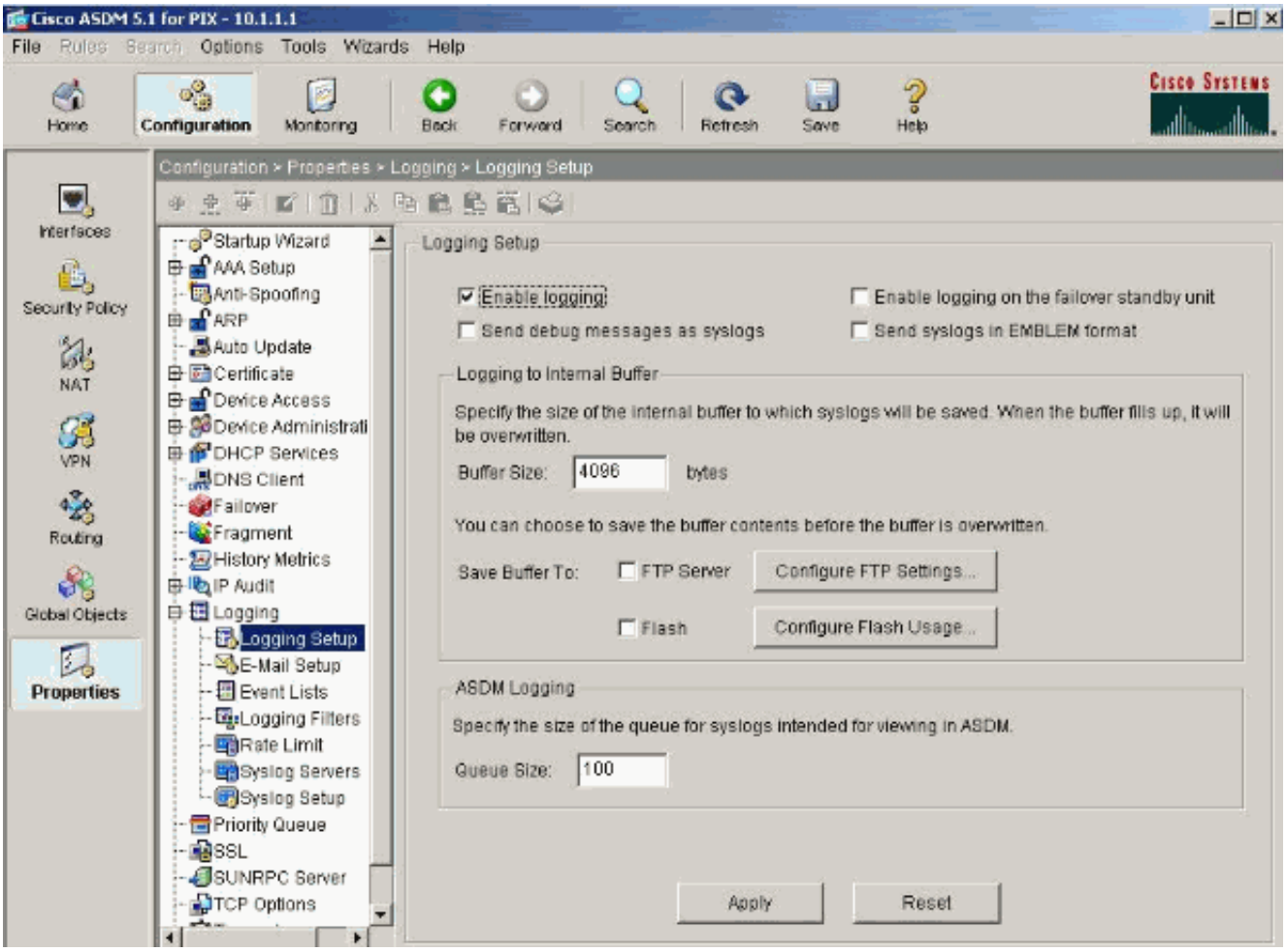
Hinweis: Beachten Sie vor der Verwendung von **Debug-**Befehlen die Informationen zu Debug-Befehlen.

- **debug icmp trace** - Zeigt, ob ICMP-Anfragen von den Hosts den PIX erreichen. Um dieses Debuggen auszuführen, müssen Sie den Befehl **access-list** hinzufügen, um ICMP in der Konfiguration zuzulassen.
- **logging buffer debugging** - Zeigt Verbindungen an, die für Hosts erstellt und abgelehnt werden, die den PIX durchlaufen. Die Informationen werden im PIX-Protokollpuffer gespeichert, und die Ausgabe wird mit dem Befehl **show log** angezeigt.

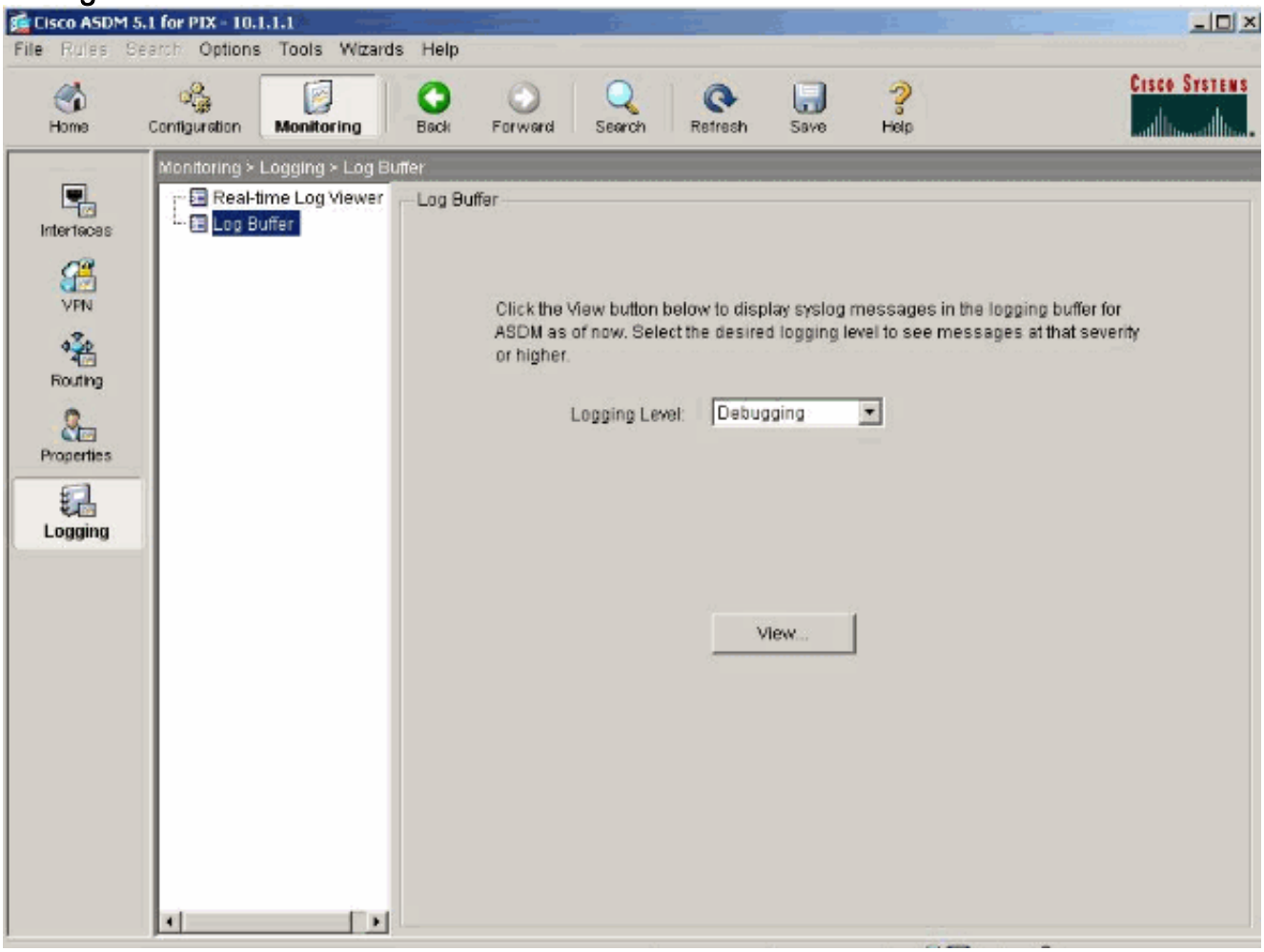
Fehlerbehebungsverfahren

ASDM kann zum Aktivieren der Protokollierung und zum Anzeigen der Protokolle verwendet werden:

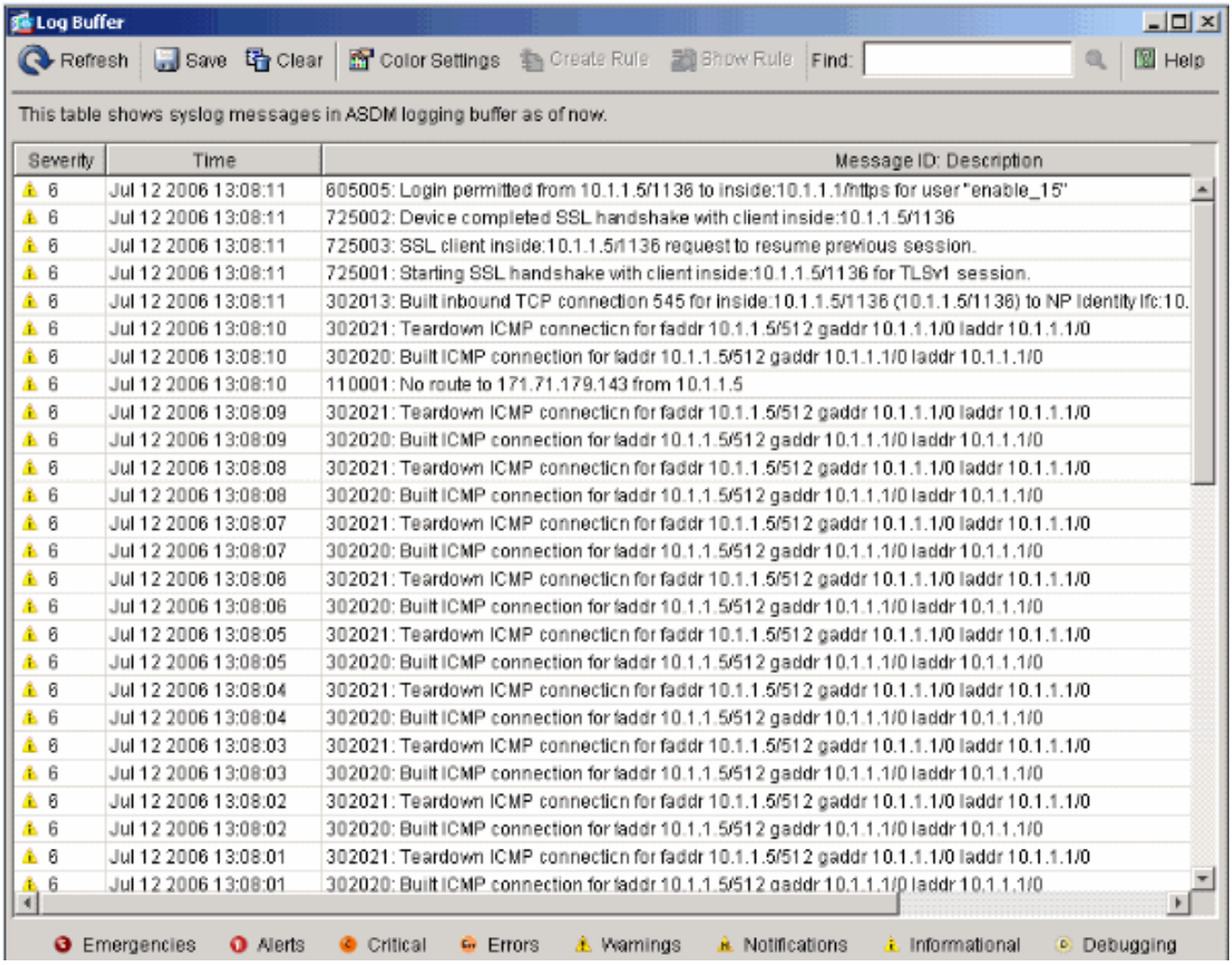
1. Wählen Sie **Konfiguration > Eigenschaften > Protokollierung > Protokollierung Setup**, aktivieren Sie **Protokollierung aktivieren**, und klicken Sie auf **Anwenden**.



2. Wählen Sie **Monitoring > Logging > Log Buffer > Logging Level** und wählen Sie **Logging Buffer** aus der Dropdown-Liste aus. Klicken Sie auf **Anzeigen**.



3. Hier ein Beispiel für den Log-Puffer:



Zugriff auf Websites nach Namen nicht möglich

In bestimmten Szenarien können die internen Netzwerke im Webbrowser nicht mit dem Namen (in Verbindung mit der IP-Adresse) auf die Internetseiten zugreifen. Dieses Problem tritt häufig auf und tritt in der Regel dann auf, wenn der DNS-Server nicht definiert ist, insbesondere dann, wenn PIX/ASA der DHCP-Server ist. Dies kann auch auftreten, wenn die PIX/ASA den DNS-Server nicht übertragen kann oder der DNS-Server nicht erreichbar ist.

Zugehörige Informationen

- Cisco Security Appliances der Serie PIX 500
- Cisco Adaptive Security Appliances der Serie ASA 5500
- Cisco Secure PIX Firewall - Befehlsreferenzen
- Cisco Adaptive Security Device Manager
- Fehlerbehebung und Warnmeldungen mit dem Cisco Adaptive Security Device Manager (ASDM)
- Anforderungen für Kommentare (RFCs)
- Technischer Support und Dokumentation - Cisco Systems