

PIX/ASA (Version 7.x und höher) IPsec-VPN-Tunnel mit Network Address Translation - Konfigurationsbeispiel

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Zugehörige Produkte](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Konfigurationen](#)

[Konfiguration der PIX Security Appliance und Zugriffslisten](#)

[PIX Security Appliance- und MPF-Konfiguration \(Modular Policy Framework\)](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Befehle zur Fehlerbehebung für Router IPsec](#)

[Löschen von Sicherheitszuordnungen](#)

[Befehle zur Fehlerbehebung für PIX](#)

[Zugehörige Informationen](#)

Einführung

Diese Beispielkonfiguration veranschaulicht einen IPsec-VPN-Tunnel durch eine Firewall, die die Network Address Translation (NAT) durchführt. **Diese Konfiguration funktioniert nicht mit Port Address Translation (PAT), wenn Sie Cisco IOS® Software Releases vor und ohne 12.2(13)T verwenden.** Dieser Konfigurationstyp kann zum Tunnel von IP-Datenverkehr verwendet werden. Diese Konfiguration kann nicht zum Verschlüsseln von Datenverkehr verwendet werden, der nicht über eine Firewall geleitet wird, z. B. IPX oder Routing-Updates. Generic Routing Encapsulation (GRE)-Tunneling ist eine geeignetere Option. In diesem Beispiel sind die Cisco 2621- und 3660-Router die IPsec-Tunnel-Endpunkte, die zwei private Netzwerke miteinander verbinden, wobei dazwischen Leitungen oder Zugriffskontrolllisten (ACLs) auf dem PIX angeordnet sind, um den IPsec-Datenverkehr zuzulassen.

Hinweis: NAT ist eine Eins-zu-Eins-Adressenumwandlung, die nicht mit PAT verwechselt werden darf. Hierbei handelt es sich um eine viele (innerhalb der Firewall)-zu-Eins-Übersetzung. Weitere Informationen zum NAT-Betrieb und zur NAT-Konfiguration finden Sie unter [Verifying NAT Operation and Basic NAT Troubleshooting \(NAT-Betrieb und grundlegende NAT-Fehlerbehebung\)](#) oder [How NAT Works \(Funktionsweise von NAT\)](#).

Hinweis: IPsec mit PAT funktioniert möglicherweise nicht ordnungsgemäß, da das Endgerät des externen Tunnels nicht mehrere Tunnel von einer IP-Adresse aus verarbeiten kann. Wenden Sie sich an Ihren Anbieter, um festzustellen, ob die Tunnel-Endgeräte mit PAT kompatibel sind. Darüber hinaus kann in der Cisco IOS-Softwareversion 12.2(13)T und höher die NAT-Transparenzfunktion für PAT verwendet werden. Weitere Informationen finden Sie unter [IPSec NAT Transparency](#). Unter [Support für IPSec ESP Through NAT](#) finden Sie weitere Informationen zu diesen Funktionen in Cisco IOS Software Release 12.2(13)T und höher.

Hinweis: Bevor Sie ein Ticket beim technischen Support von Cisco eröffnen, lesen Sie die [FAT-Fragen](#), die viele Antworten auf häufige Fragen enthält.

Unter [Konfigurieren eines IPSec-Tunnels durch eine Firewall mit NAT](#) finden Sie weitere Informationen zur Konfiguration eines IPsec-Tunnels durch Firewall mit NAT auf PIX, Version 6.x oder früher.

[Voraussetzungen](#)

[Anforderungen](#)

Für dieses Dokument bestehen keine speziellen Anforderungen.

[Verwendete Komponenten](#)

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

- Cisco IOS Software Release 12.0.7.T (bis zu, aber nicht einschließlich Cisco IOS Software Release 12.2(13)T) Neuere Versionen finden Sie unter [IPSec NAT Transparency](#).
- Cisco 2621-Router
- Cisco Router 3660
- Cisco Security Appliance der Serie PIX 500 mit 7.x und höher

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).

[Zugehörige Produkte](#)

Dieses Dokument kann auch mit der Cisco Adaptive Security Appliance (ASA) der Serie 5500 mit der Softwareversion 7.x und höher verwendet werden.

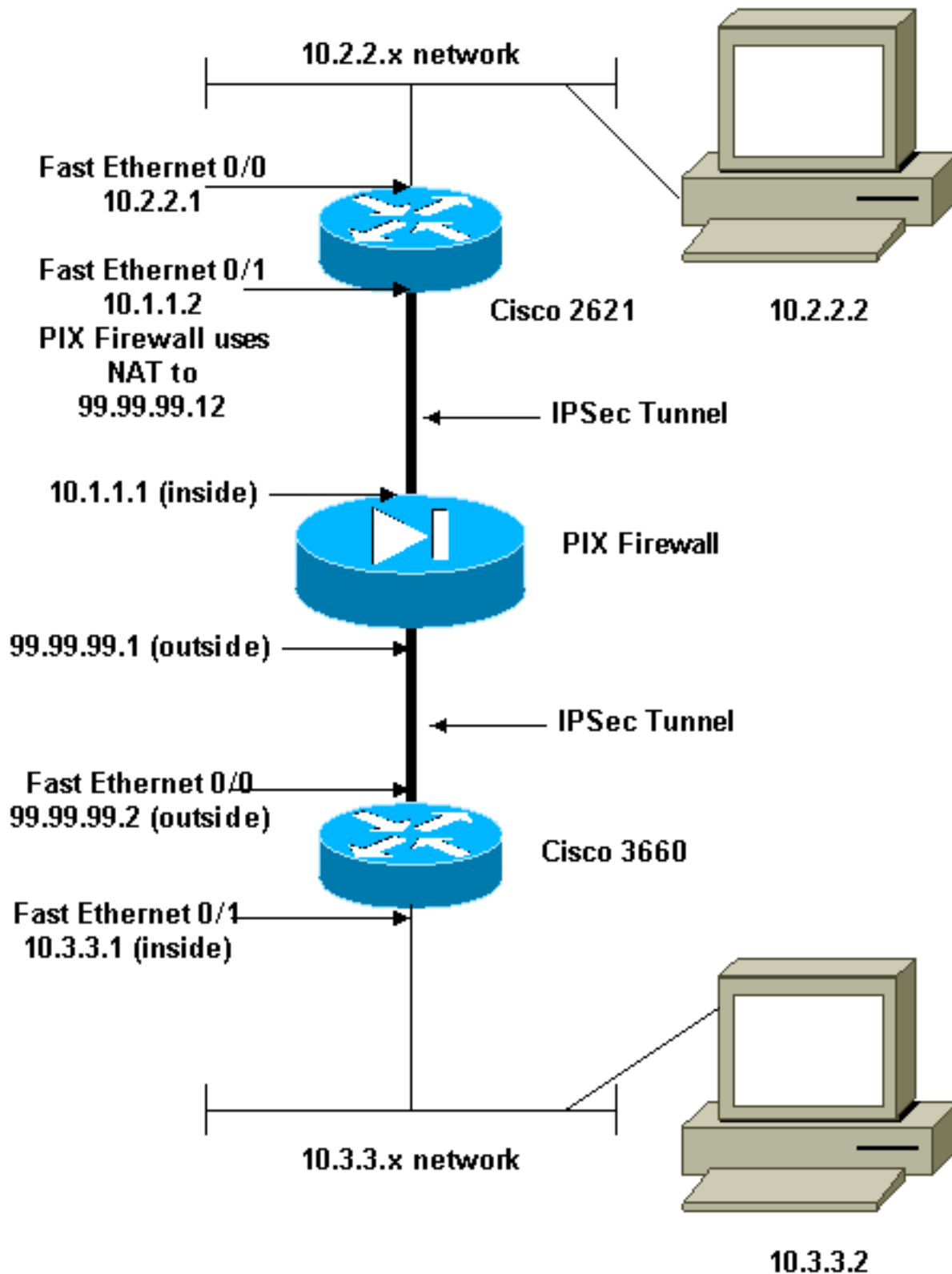
[Konfigurieren](#)

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

Hinweis: Um weitere Informationen zu den Befehlen zu erhalten, die dieses Dokument verwendet, verwenden Sie das [Command Lookup Tool](#) ([nur registrierte Kunden](#)).

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Konfigurationen

In diesem Dokument werden folgende Konfigurationen verwendet:

- [Konfiguration des Cisco 2621](#)
- [Konfiguration des Cisco 3660](#)
- [Konfiguration der PIX Security Appliance und ZugriffslistenKonfiguration der Advanced Security Device Manager GUI \(ASDM\)CLI-Konfiguration \(Command Line Interface\)](#)
- [PIX Security Appliance- und MPF-Konfiguration \(Modular Policy Framework\)](#)

Cisco 2621

```
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname goss-2621
!
ip subnet-zero
!
ip audit notify log
ip audit po max-events 100
isdn voice-call-failure 0
cns event-service server
!
!--- The IKE policy. crypto isakmp policy 10
  hash md5
  authentication pre-share
crypto isakmp key cisco123 address 99.99.99.2
!
crypto ipsec transform-set myset esp-des esp-md5-hmac
!
crypto map mymap local-address FastEthernet0/1

!--- IPsec policy. crypto map mymap 10 ipsec-isakmp
  set peer 99.99.99.2
  set transform-set myset

!--- Include the private-network-to-private-network
traffic !--- in the encryption process. match address
101
!
controller T1 1/0
!
interface FastEthernet0/0
 ip address 10.2.2.1 255.255.255.0
 no ip directed-broadcast
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 10.1.1.2 255.255.255.0
 no ip directed-broadcast
 duplex auto
 speed auto

!--- Apply to the interface. crypto map mymap
```

```

!
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.1
no ip http server

!--- Include the private-network-to-private-network
traffic !--- in the encryption process. access-list 101
permit ip 10.2.2.0 0.0.0.255 10.3.3.0 0.0.0.255
line con 0
  transport input none
line aux 0
line vty 0 4
!
no scheduler allocate
end

```

Cisco 3660

```

version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname goss-3660
!
ip subnet-zero
!
cns event-service server
!

!--- The IKE policy. crypto isakmp policy 10
  hash md5
  authentication pre-share
crypto isakmp key cisco123 address 99.99.99.12
!
crypto ipsec transform-set myset esp-des esp-md5-hmac
!
crypto map mymap local-address FastEthernet0/0

!--- The IPsec policy. crypto map mymap 10 ipsec-isakmp
  set peer 99.99.99.12
  set transform-set myset

!--- Include the private-network-to-private-network
traffic !--- in the encryption process. match address
101
!
interface FastEthernet0/0
  ip address 99.99.99.2 255.255.255.0
  no ip directed-broadcast
  ip nat outside
  duplex auto
  speed auto

!--- Apply to the interface. crypto map mymap
!
interface FastEthernet0/1
  ip address 10.3.3.1 255.255.255.0
  no ip directed-broadcast
  ip nat inside
  duplex auto
  speed auto
!

```

```

interface Ethernet3/0
  no ip address
  no ip directed-broadcast
  shutdown
!
interface Serial3/0
  no ip address
  no ip directed-broadcast
  no ip mroute-cache
  shutdown
!
interface Ethernet3/1
  no ip address
  no ip directed-broadcast
interface Ethernet4/0
  no ip address
  no ip directed-broadcast
  shutdown
!
interface TokenRing4/0
  no ip address
  no ip directed-broadcast
  shutdown
  ring-speed 16
!

!--- The pool from which inside hosts translate to !---
the globally unique 99.99.99.0/24 network. ip nat pool
OUTSIDE 99.99.99.70 99.99.99.80 netmask 255.255.255.0

!--- Except the private network from the NAT process. ip
nat inside source route-map nonat pool OUTSIDE
ip classless
ip route 0.0.0.0 0.0.0.0 99.99.99.1
no ip http server
!

!--- Include the private-network-to-private-network
traffic !--- in the encryption process. access-list 101
permit ip 10.3.3.0 0.0.0.255 10.2.2.0 0.0.0.255
access-list 101 deny ip 10.3.3.0 0.0.0.255 any

!--- Except the private network from the NAT process.
access-list 110 deny ip 10.3.3.0 0.0.0.255 10.2.2.0
0.0.0.255
access-list 110 permit ip 10.3.3.0 0.0.0.255 any
route-map nonat permit 10
  match ip address 110
!
line con 0
  transport input none
line aux 0
line vty 0 4
!
end

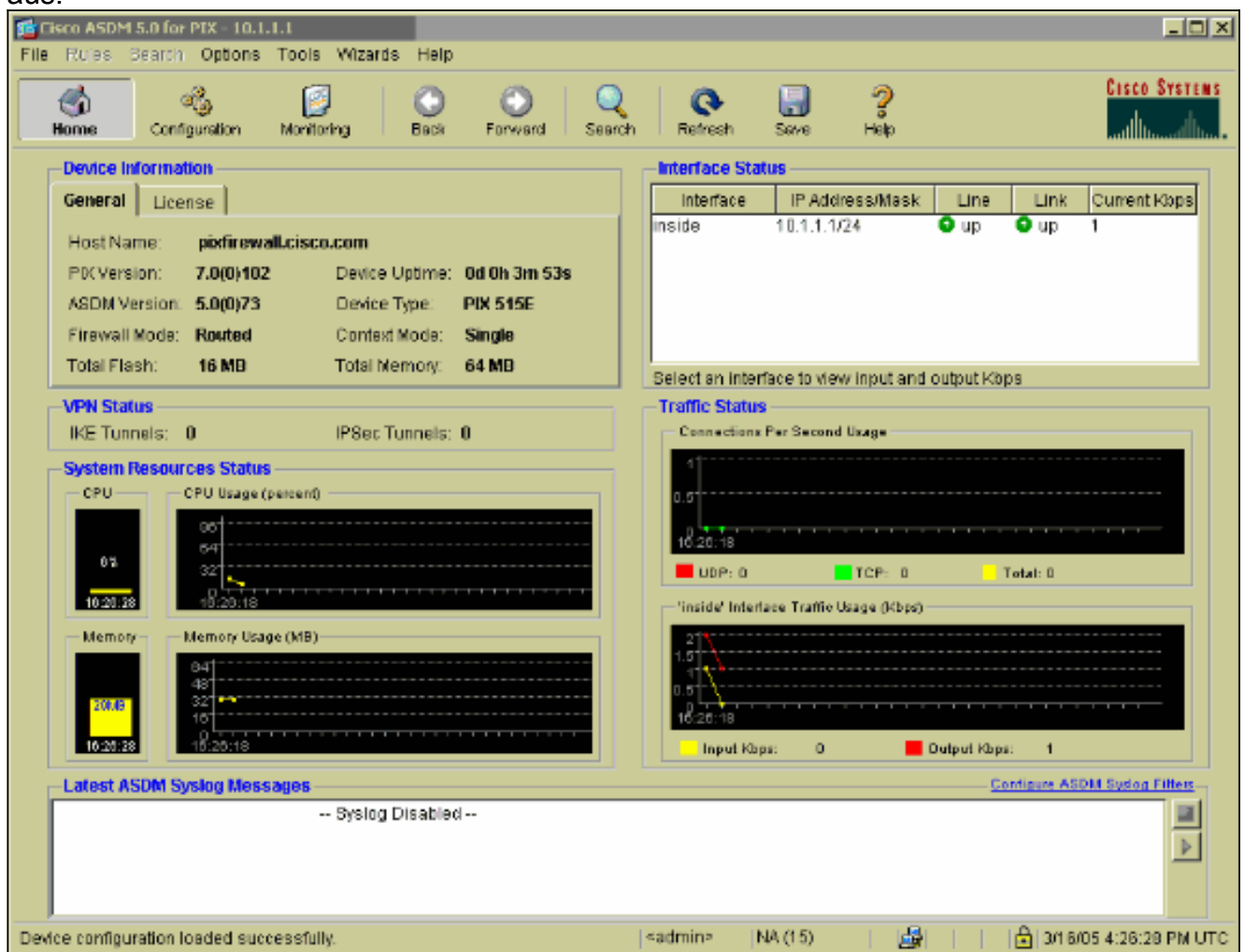
```

[Konfiguration der PIX Security Appliance und Zugriffslisten](#)

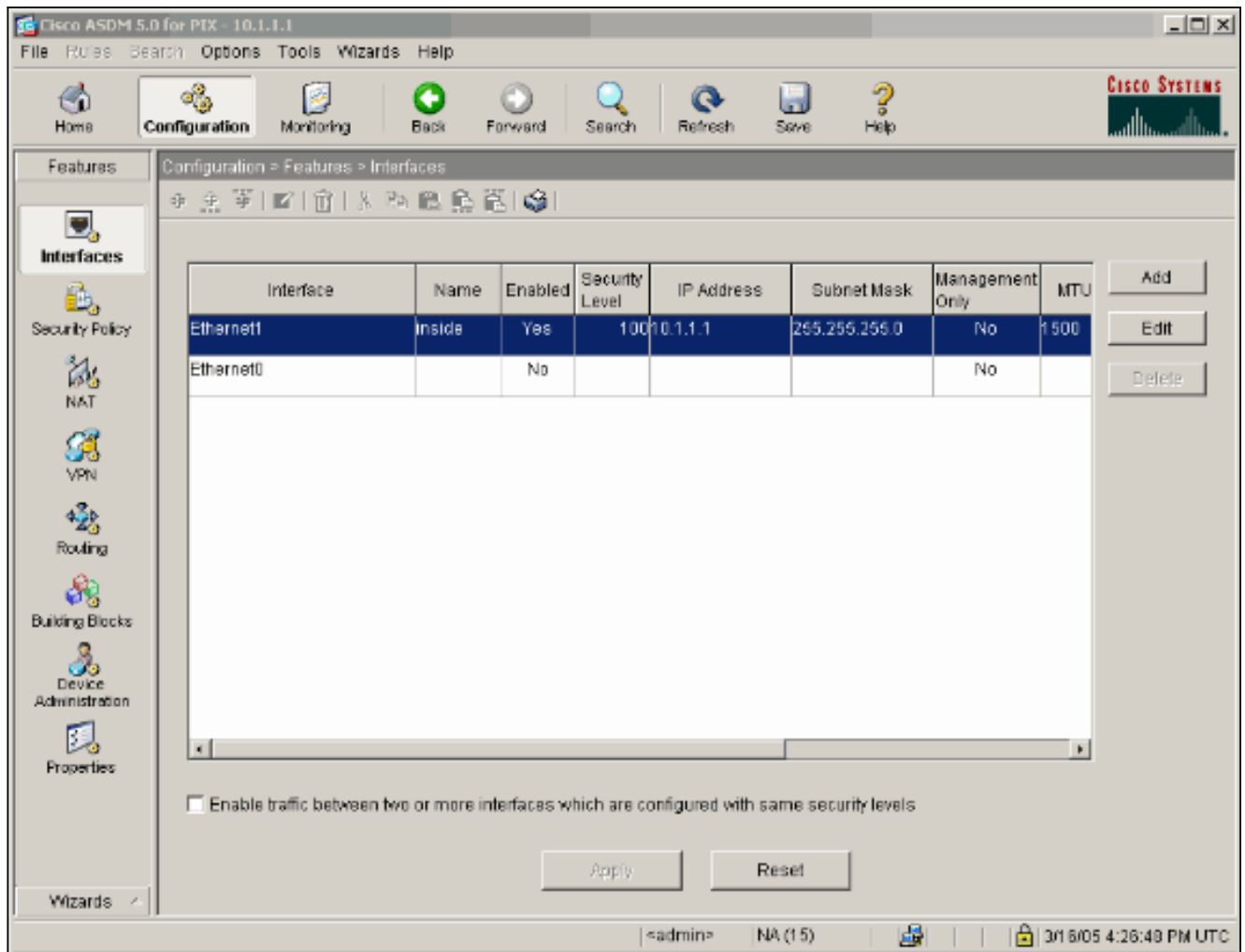
[ASDM 5.0-Konfiguration](#)

Führen Sie diese Schritte aus, um PIX Firewall Version 7.0 mit ASDM zu konfigurieren.

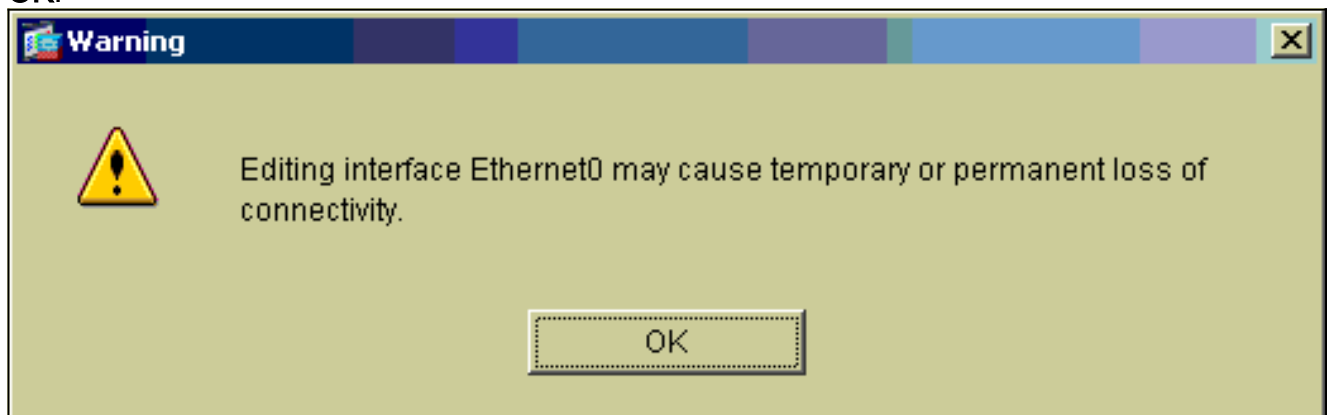
1. In den PIX einstecken. Verwenden Sie nach einer gelöschten Konfiguration die interaktiven Aufforderungen, um die **Advanced Security Device Manager GUI (ASDM)** für die Verwaltung des PIX von der Workstation 10.1.1.3 zu aktivieren.
2. Öffnen Sie auf Workstation 10.1.1.3 einen Webbrowser, und verwenden Sie ASDM (in diesem Beispiel <https://10.1.1.1>).
3. Wählen Sie **Yes (Ja)** auf den Zertifikatsaufforderungen aus, und melden Sie sich mit dem aktivierten Kennwort an, wie in der [ASDM-Bootstrap-Konfiguration der PIX-Firewall](#) konfiguriert.
4. Wenn ASDM zum ersten Mal auf dem PC ausgeführt wird, werden Sie aufgefordert, ASDM Launcher zu verwenden oder ASDM als Java-Anwendung zu verwenden. In diesem Beispiel wird der ASDM Launcher ausgewählt und installiert.
5. Fahren Sie mit dem ASDM Home-Fenster fort, und wählen Sie die Registerkarte Configuration (Konfiguration) aus.



6. Markieren Sie die **Ethernet 0-Schnittstelle**, und klicken Sie auf **Bearbeiten**, um die externe Schnittstelle zu konfigurieren.



7. Klicken Sie an der Eingabeaufforderung Bearbeiten auf OK.



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

Edit Interface

Hardware Port: **Ethernet0** Configure Hardware Properties...

Enable Interface Dedicate this interface to management only

Interface Name:

Security Level:

IP Address

Use Static IP Obtain Address via DHCP

IP Address:


Subnet Mask:

MTU:

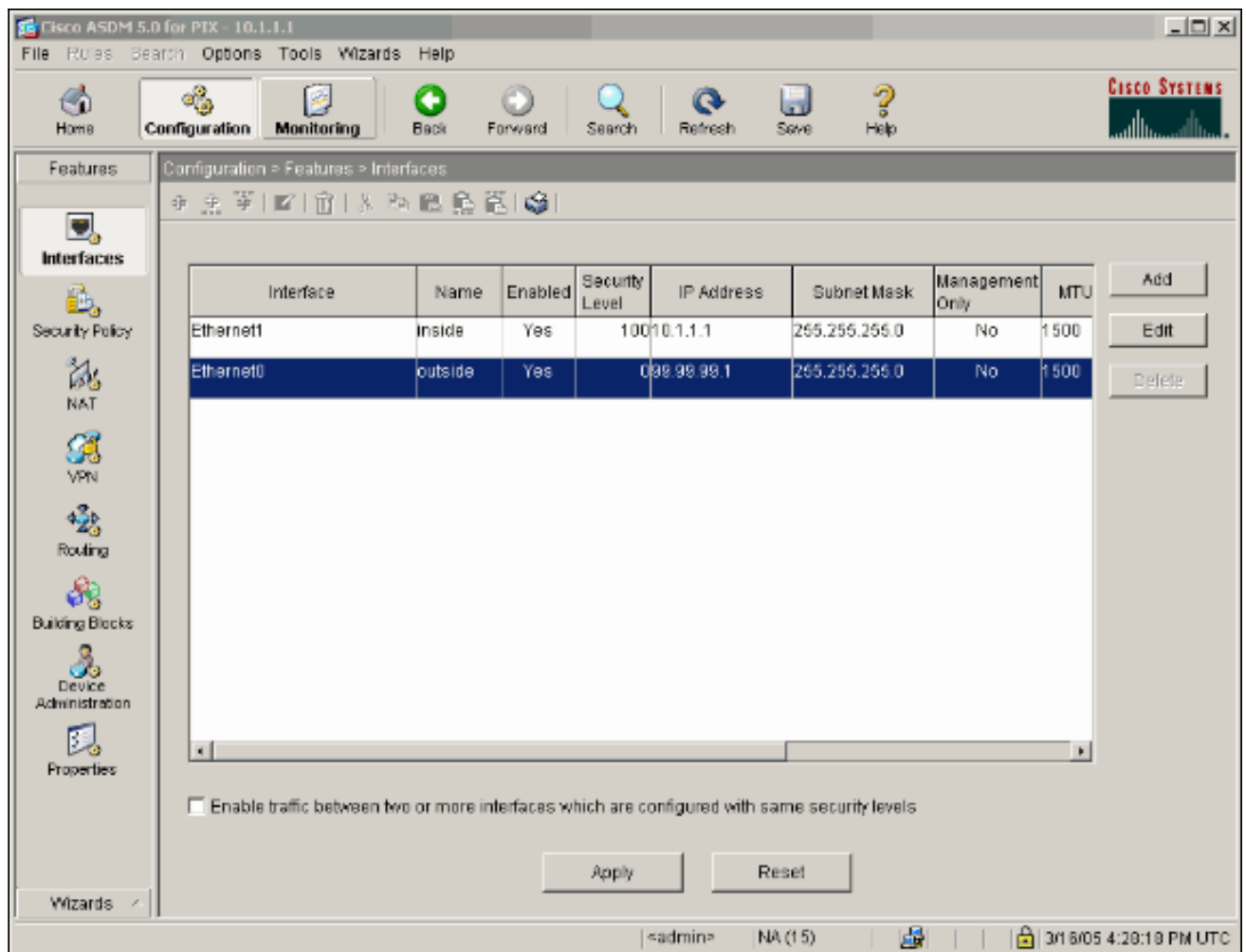
Description:

9. Klicken Sie an der Eingabeaufforderung Schnittstellenänderung auf **OK**.

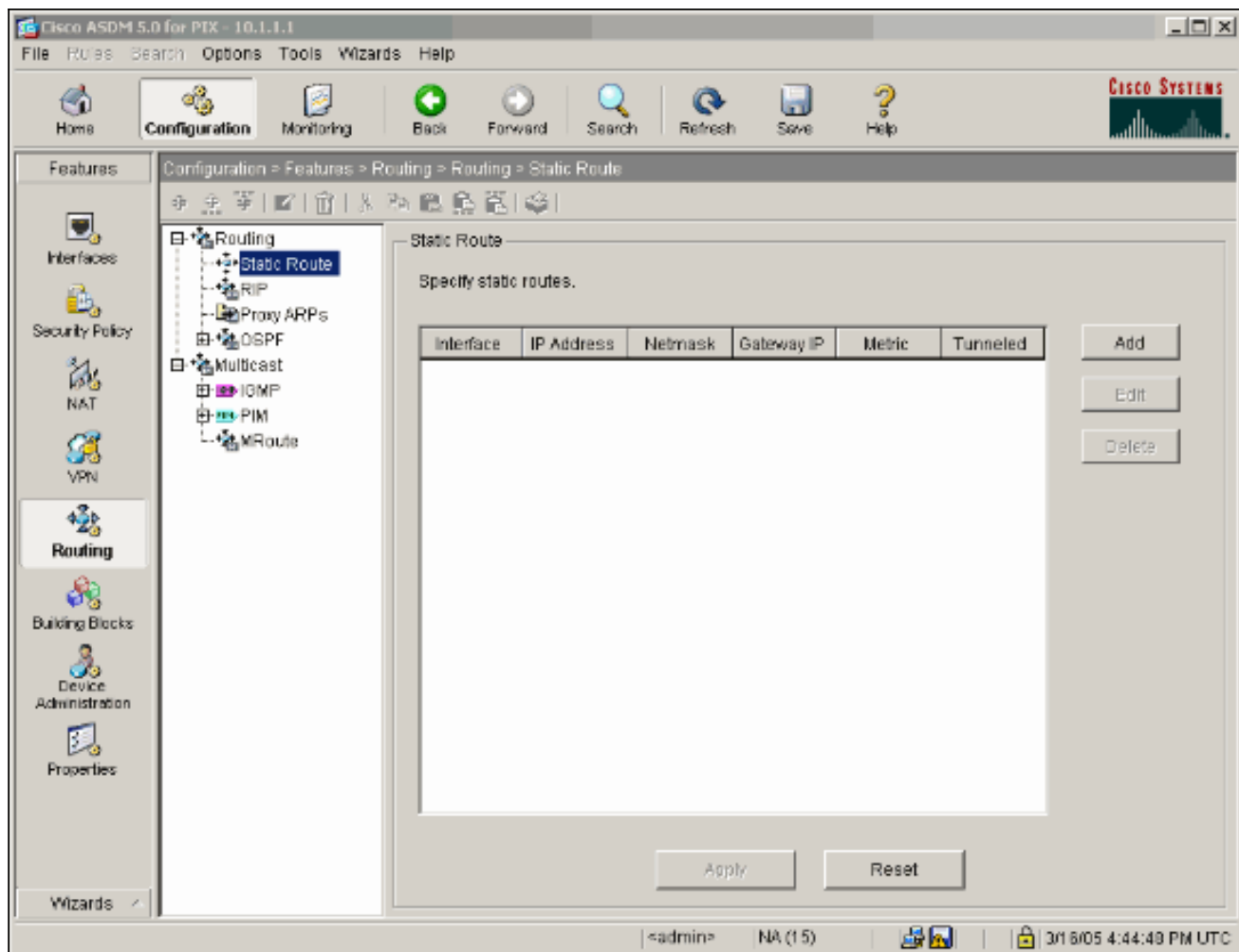
Security Level Change

 Changing an interface's security level may cause your PIX configuration to become invalid, causing the PIX to drop legal traffic or allow illegal traffic to pass through. Do you still wish to proceed?

10. Klicken Sie auf **Apply**, um die Schnittstellenkonfiguration zu akzeptieren. Die Konfiguration wird auch auf den PIX übertragen. In diesem Beispiel werden statische Routen verwendet.



11. Klicken Sie unter der Registerkarte Funktionen auf **Routing**, markieren Sie **Statische Route**, und klicken Sie auf **Hinzufügen**.



12. Konfigurieren Sie das Standard-Gateway, und klicken Sie auf

OK.

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

Add Static Route

Interface Name:

IP Address:

Mask:

Gateway IP:

Metric

Tunneled (Used only for default route)

OK Cancel Help

hinzu.

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

Cisco ASDM 5.0 for PIX - 10.1.1.1

File Rules Search Options Tools Wizards Help

Home Configuration Monitoring Back Forward Search Refresh Save Help

Features

Configuration = Features > Routing > Routing > Static Route

Routing

- Static Route
- RIP
- Proxy ARP's
- OSPF
- Multicast
- IGMP
- PIM
- MRRoute

Static Route

Specify static routes.

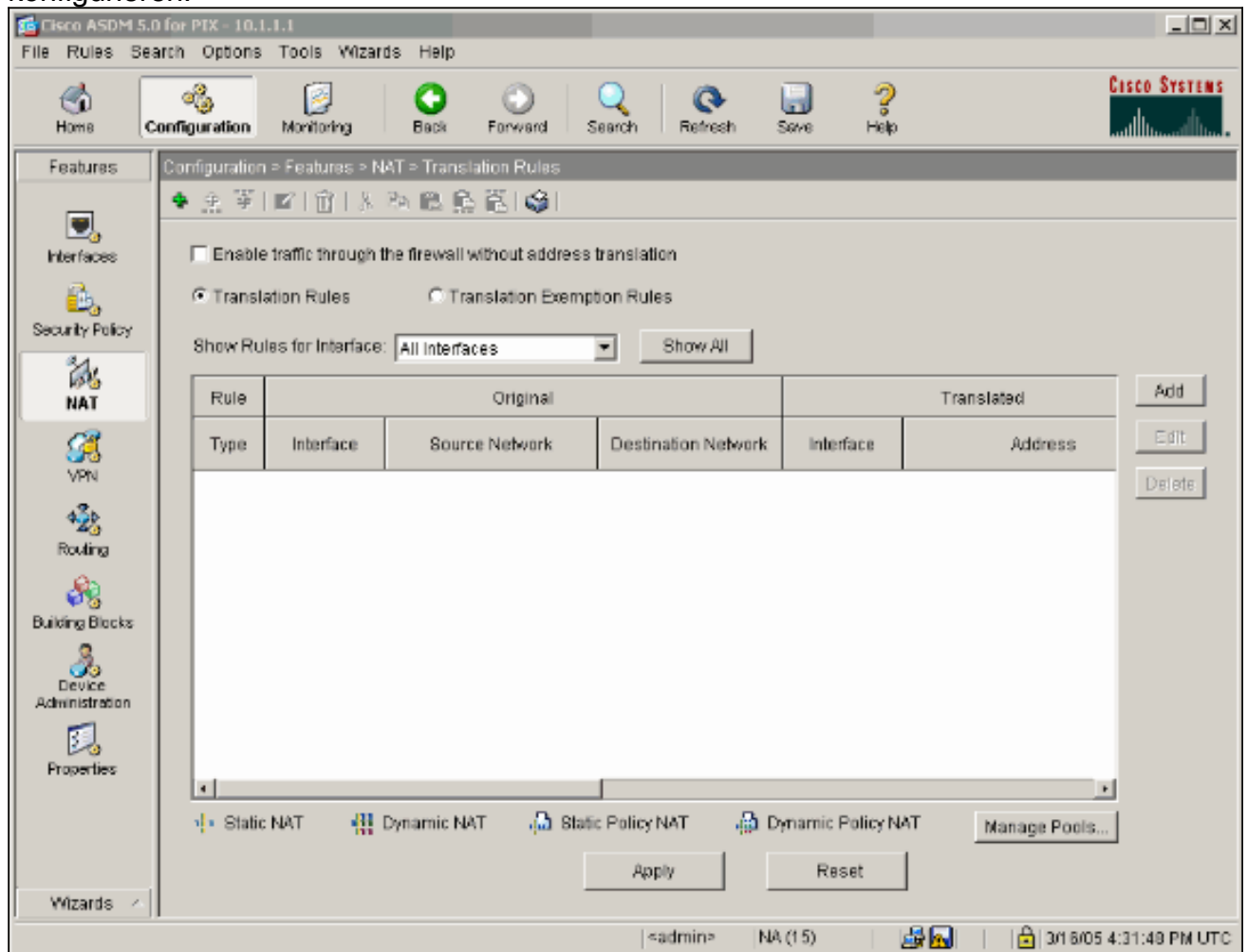
Interface	IP Address	Netmask	Gateway IP	Metric	Tunneled
outside	0.0.0.0	0.0.0.0	99.99.99.2	1	No
inside	10.2.2.0	255.255.2...	10.1.1.2	1	N/A

Add Edit Delete

Apply Reset

<admin> NA (15) 3/1 6/05 4:46:49 PM UTC

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



16. Konfigurieren Sie das Quellnetzwerk (in diesem Beispiel verwenden Sie alle). Klicken Sie anschließend auf **Pools verwalten**, um die PAT zu definieren.

Add Address Translation Rule

Use NAT
 Use Policy NAT

Source Host/Network


Interface:

IP Address:

Mask:


Translate Address on Interface:

Translate Address To

 **Static**
 IP Address:

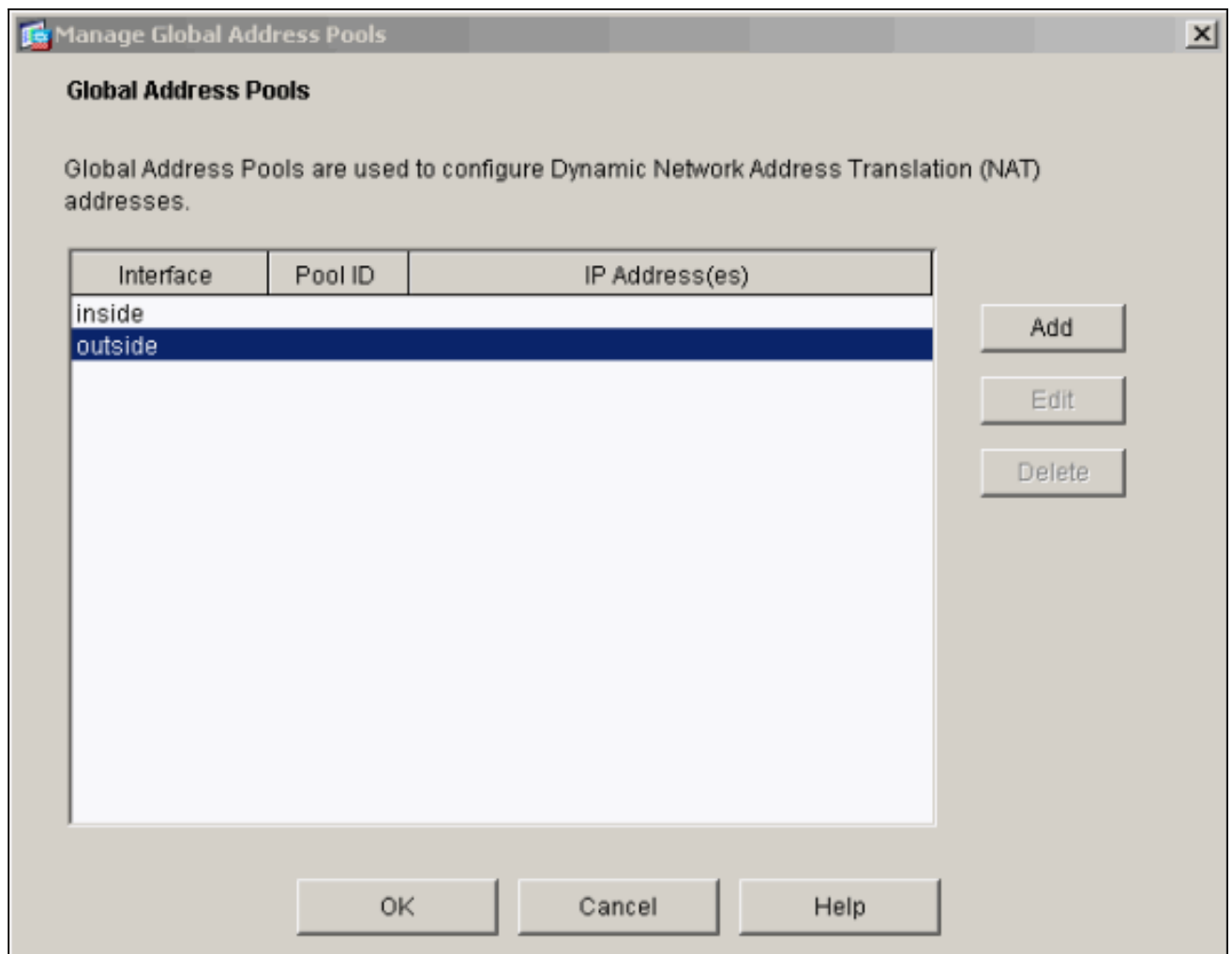
Redirect port

TCP
 UDP
Original port:
Translated port:

 **Dynamic**
Address Pool:

Pool ID	Address
N/A	No address pool defined

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



In diesem Beispiel wird eine PAT verwendet, die die IP-Adresse der Schnittstelle verwendet.

Add Global Pool Item

Interface: Pool ID:

Range

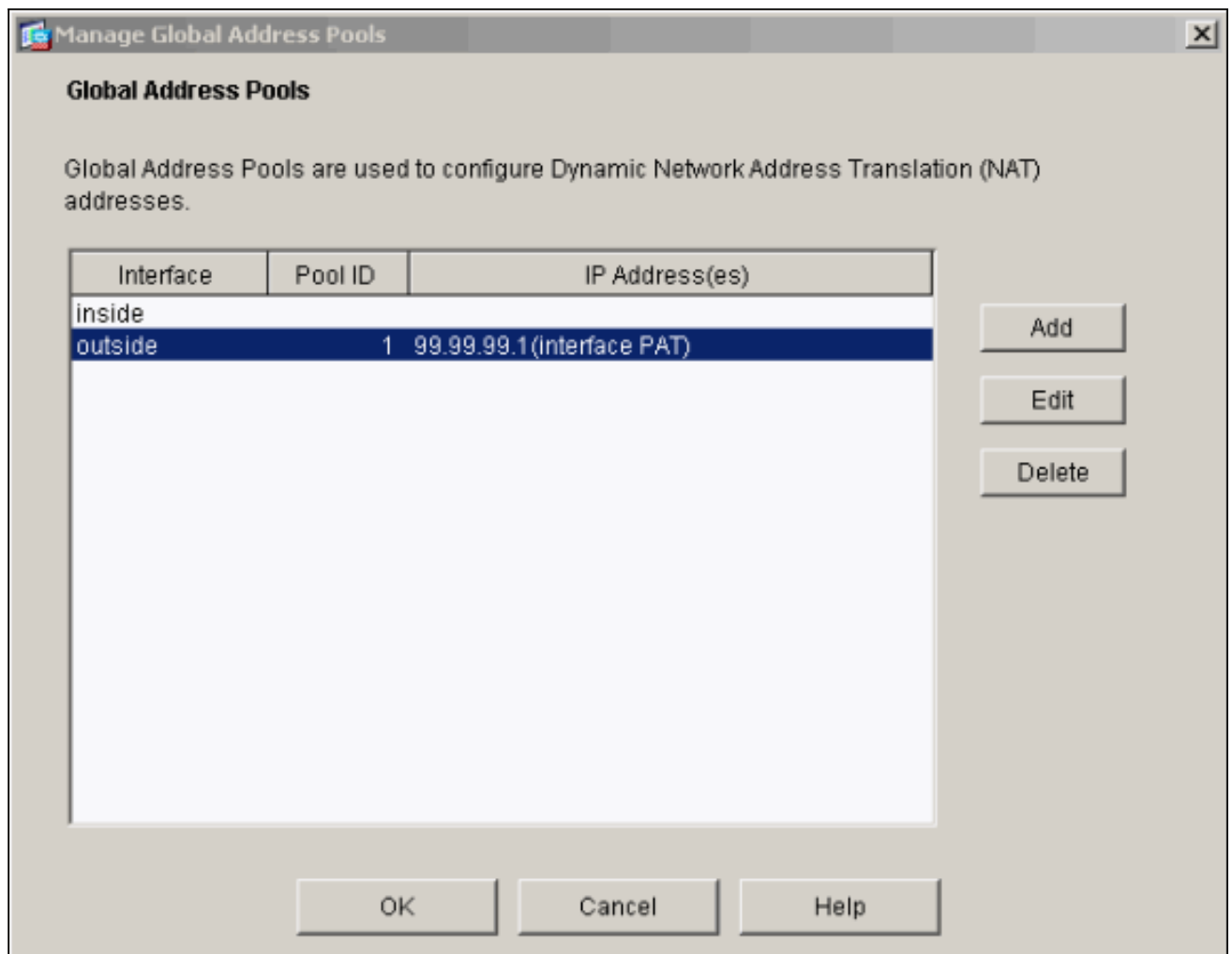
Port Address Translation (PAT)

Port Address Translation (PAT) using the IP address of the interface

IP Address: -

Network Mask (optional):

18. Klicken Sie bei der Konfiguration der PAT auf **OK**.



19. Klicken Sie auf **Hinzufügen**, um die statische Übersetzung zu konfigurieren.

Add Address Translation Rule

Use NAT
 Use Policy NAT

Source Host/Network


Interface:

IP Address:

Mask:

Translate Address on Interface:


Translate Address To

 **Static**
 IP Address:

Redirect port

TCP
 Original port:
 Translated port:

UDP

 **Dynamic**
 Address Pool:

Pool ID	Address
1	99.99.99.1 (interface PAT)

20. Wählen Sie **drinnen** im Dropdown-Menü Interface (Schnittstelle) aus, und geben Sie dann die IP-Adresse **10.1.1.2**, Subnetzmaske **255.255.255**, wählen Sie **Statisch** und den IP-Adresstyp außerhalb der Adresse **99.99.12 ein**. Klicken Sie abschließend auf **OK**.

Add Address Translation Rule

Use NAT Use Policy NAT

Source Host/Network


Interface:

IP Address:

Mask:

Translate Address on Interface:


Translate Address To

 Static IP Address:

Redirect port

TCP Original port: Translated port:

UDP

 Dynamic Address Pool:

Pool ID	Address

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

Configuration > Features > NAT > Translation Rules

Enable traffic through the firewall without address translation

Translation Rules Translation Exemption Rules

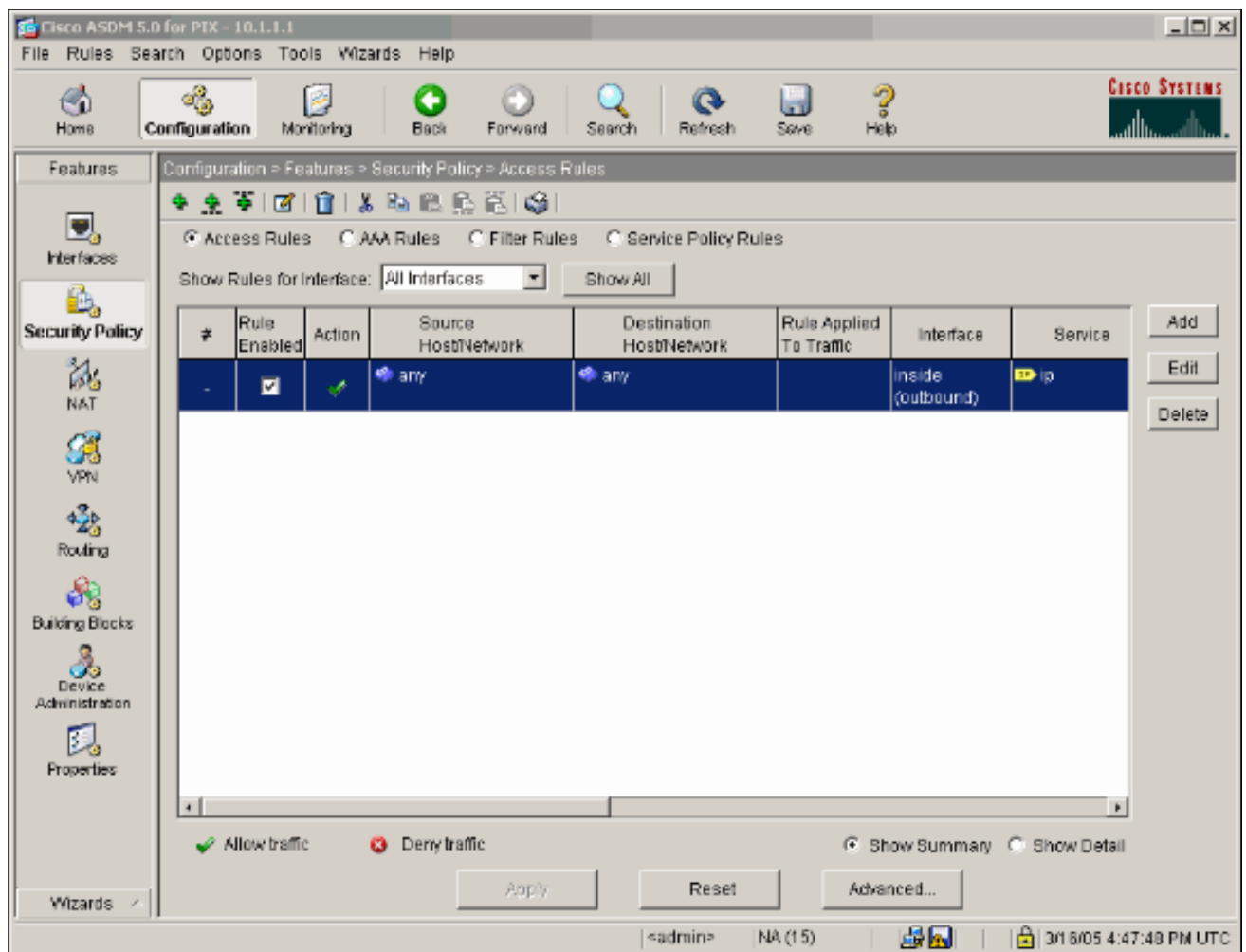
Show Rules for Interface:

Rule	Original			Translated		
Type	Interface	Source Network	Destination Network	Interface	Address	
	inside	10.1.1.2	any	outside	99.99.99.12	<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>
	inside	inside any/0	any	outside	same as original address	

Static NAT
 Dynamic NAT
 Static Policy NAT
 Dynamic Policy NAT

<admin> | NA (15) | 3/1 6/05 4:43:28 PM UTC

22. Wählen Sie auf der Registerkarte Funktionen **Sicherheitsrichtlinie** aus, um die Sicherheitsrichtlinienregel zu konfigurieren.



23. Klicken Sie auf **Hinzufügen**, um Datenverkehr zuzulassen, und klicken Sie auf **OK**, um fortzufahren.

Add Access Rule


Action
 Select an action:
 Apply to Traffic:

Source Host/Network
 IP Address Name Group
 Interface:
 IP address: ...
 Mask:

Destination Host/Network
 IP Address Name Group
 Interface:
 IP address: ...
 Mask:

Syslog
 Default Syslog

Time Range
 Time Range:

Rule Flow Diagram
 Rule applied to traffic incoming to source interface

 99.99.99.2 outside inside 99.99.99.12
 Allow traffic

Protocol and Service
 TCP UDP ICMP IP
 IP Protocol
 IP protocol: ...

Please enter the description below (optional):

24. Klicken Sie auf **Hinzufügen**, um ISAKMP-Datenverkehr zuzulassen, und klicken Sie auf **OK**, um fortzufahren.

Edit Access Rule


Action
 Select an action:
 Apply to Traffic:

Source Host/Network
 IP Address Name Group
 Interface:
 IP address: ...
 Mask:

Destination Host/Network
 IP Address Name Group
 Interface:
 IP address: ...
 Mask:

Syslog
 Default Syslog

Time Range
 Time Range:

Rule Flow Diagram
 Rule applied to traffic incoming to source interface

 99.99.99.2 outside inside 99.99.99.12
 Allow traffic

Protocol and Service
 TCP UDP ICMP IP

Source Port
 Service = ...
 Service Group

Destination Port
 Service = ...
 Service Group

Please enter the description below (optional):

25. Klicken Sie auf **Hinzufügen**, um den UDP-Port 4500-Verkehr für NAT-T zuzulassen, und klicken Sie auf **OK**, um fortzufahren.

Edit Access Rule


Action
 Select an action:
 Apply to Traffic:

Source Host/Network
 IP Address Name Group
 Interface:
 IP address: ...
 Mask:

Destination Host/Network
 IP Address Name Group
 Interface:
 IP address: ...
 Mask:

Syslog
 Default Syslog

Time Range
 Time Range:

Rule Flow Diagram
 Rule applied to traffic incoming to source interface

 99.99.99.2 outside inside 99.99.99.12
 Allow traffic

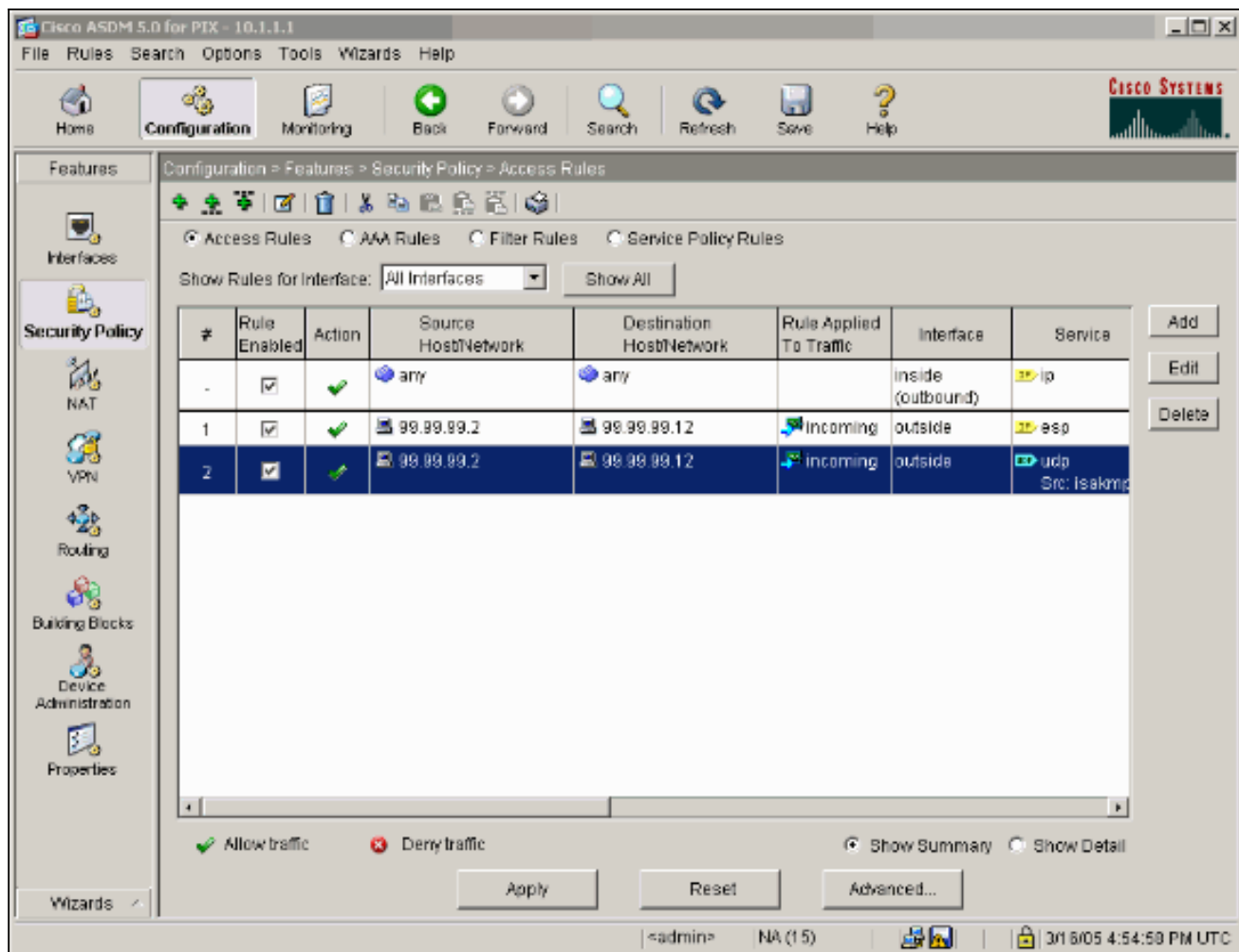
Protocol and Service
 TCP UDP ICMP IP

Source Port
 Service = ...
 Service Group

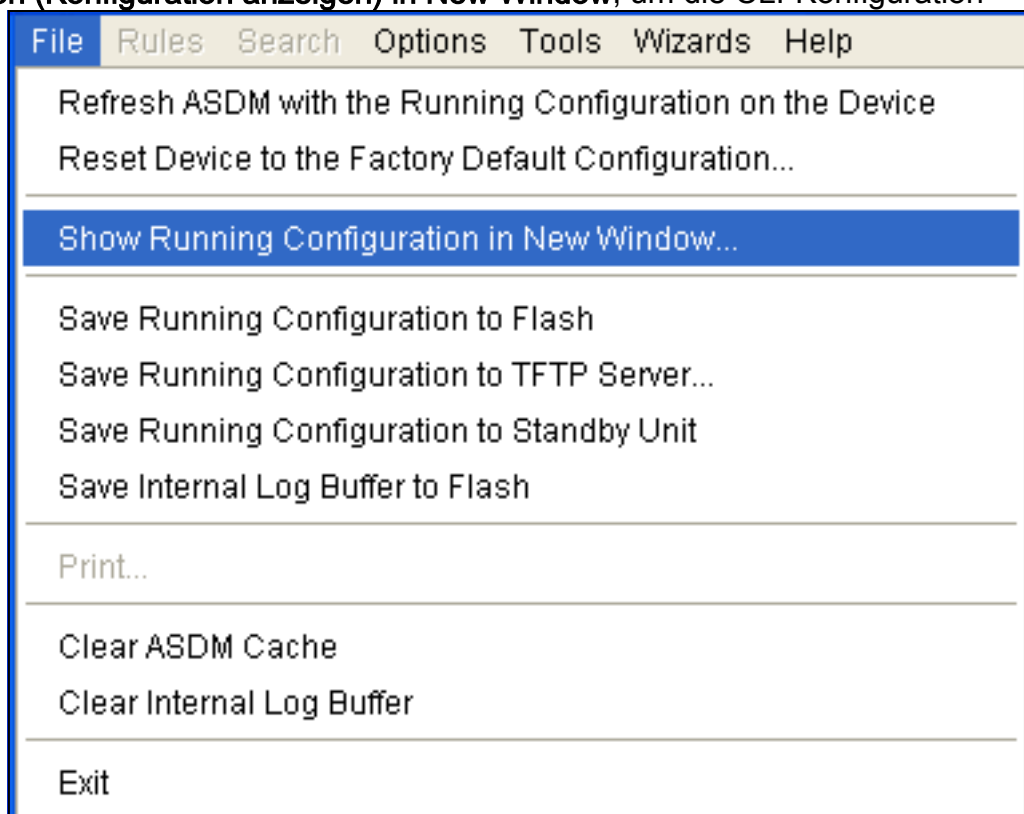
Destination Port
 Service = ...
 Service Group

Please enter the description below (optional):

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



27. Die Konfiguration ist nun abgeschlossen. Wählen Sie **File (Datei) > Show Running Configuration (Konfiguration anzeigen) in New Window**, um die CLI-Konfiguration



anzuzeigen.

PIX-Firewall

```
pixfirewall# show run
: Saved
:
PIX Version 7.0(0)102
names
!
interface Ethernet0
  nameif outside
  security-level 0
  ip address 99.99.99.1 255.255.255.0
!
interface Ethernet1
  nameif inside
  security-level 100
  ip address 10.1.1.1 255.255.255.0
!
enable password 2KFQnbNIdI.2KYOU encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
domain-name cisco.com
ftp mode passive

access-list outside_access_in remark Access Rule to
Allow ESP traffic
access-list outside_access_in
  extended permit esp host 99.99.99.2 host
99.99.99.12

access-list outside_access_in
  remark Access Rule to allow ISAKMP to host
99.99.99.12
access-list outside_access_in
  extended permit udp host 99.99.99.2 eq
isakmp host 99.99.99.12

access-list outside_access_in
  remark Access Rule to allow port 4500 (NAT-
T) to host 99.99.99.12
access-list outside_access_in
  extended permit udp host 99.99.99.2
eq 4500 host 99.99.99.12
pager lines 24
mtu inside 1500
mtu outside 1500
no failover
monitor-interface inside
monitor-interface outside
asdm image flash:/asdmfile.50073
no asdm history enable
arp timeout 14400
nat-control
global (outside) 1 interface
nat (inside) 0 0.0.0.0 0.0.0.0
static (inside,outside) 99.99.99.12 10.1.1.2 netmask
255.255.255.255
access-group outside_access_in in interface outside
route inside 10.2.2.0 255.255.255.0 10.1.1.2 1
route outside 0.0.0.0 0.0.0.0 99.99.99.2 1
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
http 10.1.1.3 255.255.255.255 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
  match default-inspection-traffic
!
!
policy-map asa_global_fw_policy
  class inspection_default
    inspect dns maximum-length 512
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect netbios
    inspect rsh
    inspect rtsp
    inspect skinny
    inspect esmtp
    inspect sqlnet
    inspect sunrpc
    inspect tftp
    inspect sip
    inspect xdmcp
!
service-policy asa_global_fw_policy global
Cryptochecksum:0a12956036ce4e7a97f351cde61fba7e
: end

```

[PIX Security Appliance- und MPF-Konfiguration \(Modular Policy Framework\)](#)

Verwenden Sie anstelle der Zugriffsliste den Befehl **inspect ipsec-pass-thru** in MPF (Modular Policy Framework), um den IPsec-Datenverkehr über die PIX/ASA Security Appliances weiterzuleiten.

Diese Prüfung ist so konfiguriert, dass sie Pinholes für ESP-Datenverkehr öffnet. Alle ESP-Datenflüsse sind zulässig, wenn ein Weiterleitungsfluss vorhanden ist, und es gibt keine Beschränkung für die maximale Anzahl an Verbindungen, die zulässig sein können. AH ist nicht zulässig. Das Timeout für Leerlaufzeiten für ESP-Datenflüsse ist standardmäßig auf 10 Minuten festgelegt. Diese Überprüfung kann an allen Standorten angewendet werden, an denen andere Überprüfungen durchgeführt werden können. Dazu gehören Befehlsmodi für Klassen und Übereinstimmung. Die IPsec-Passthrough-Anwendungsinspektion ermöglicht eine einfache Überbrückung des ESP-Datenverkehrs (IP Protocol 50), der mit einer Verbindung des IKE-UDP-Ports 500 verbunden ist. Sie vermeidet langwierige Zugriffslistenkonfigurationen, um ESP-Datenverkehr zuzulassen, und bietet außerdem Sicherheit mit Timeout und max. Verbindungen. Befehle für **Klassenzuordnung**, **Richtlinienzuordnung** und **Dienstrichtlinien** zum Definieren einer Datenverkehrsklasse, zum Anwenden des Befehls inspect auf die Klasse und zum Anwenden der Richtlinie auf eine oder mehrere Schnittstellen verwenden. Wenn der Befehl **inspect IPsec-pass-thru** aktiviert ist, kann unbegrenzter ESP-Datenverkehr mit einer Zeitüberschreitung von 10

Minuten zugelassen werden, die nicht konfigurierbar ist. NAT- und Nicht-NAT-Datenverkehr ist zulässig.

```
hostname(config)#access-list test-udp-acl extended permit udp any any eq 500
hostname(config)#class-map test-udp-class
hostname(config-cmap)#match access-list test-udp-acl
hostname(config)#policy-map test-udp-policy
hostname(config-pmap)#class test-udp-class
hostname(config-pmap-c)#inspect ipsec-pass-thru
hostname(config)#service-policy test-udp-policy interface outside
```

Überprüfen

Dieser Abschnitt enthält Informationen zur Bestätigung, dass Ihre Konfiguration ordnungsgemäß funktioniert.

Bestimmte **show**-Befehle werden vom [Output Interpreter Tool](#) unterstützt (nur [registrierte](#) Kunden), mit dem Sie eine Analyse der **show**-Befehlsausgabe anzeigen können.

- **show crypto ipsec sa** - Zeigt die Sicherheitszuordnungen für Phase 2 an.
- **show crypto isakmp sa** - Zeigt die Sicherheitszuordnungen für Phase 1 an.
- **show crypto engine connections active** - Zeigt die verschlüsselten und entschlüsselten Pakete an.

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Befehle zur Fehlerbehebung für Router IPsec

Hinweis: Lesen Sie [vor dem](#) Ausgabe von **Debug**-Befehlen unter [Wichtige Informationen zu Debug-Befehlen nach](#).

- **debug crypto engine**: Zeigt den verschlüsselten Datenverkehr an.
- **debug crypto ipsec**: Zeigt die IPsec-Aushandlungen für Phase 2 an.
- **debug crypto isakmp**: Zeigt die Aushandlungen der Internet Security Association und des Key Management Protocol (ISAKMP) für Phase 1 an.

Löschen von Sicherheitszuordnungen

- **clear crypto isakmp** - Löscht die Sicherheitszuordnungen von Internet Key Exchange (IKE).
- **clear crypto ipsec sa**: Löscht IPsec-Sicherheitszuordnungen.

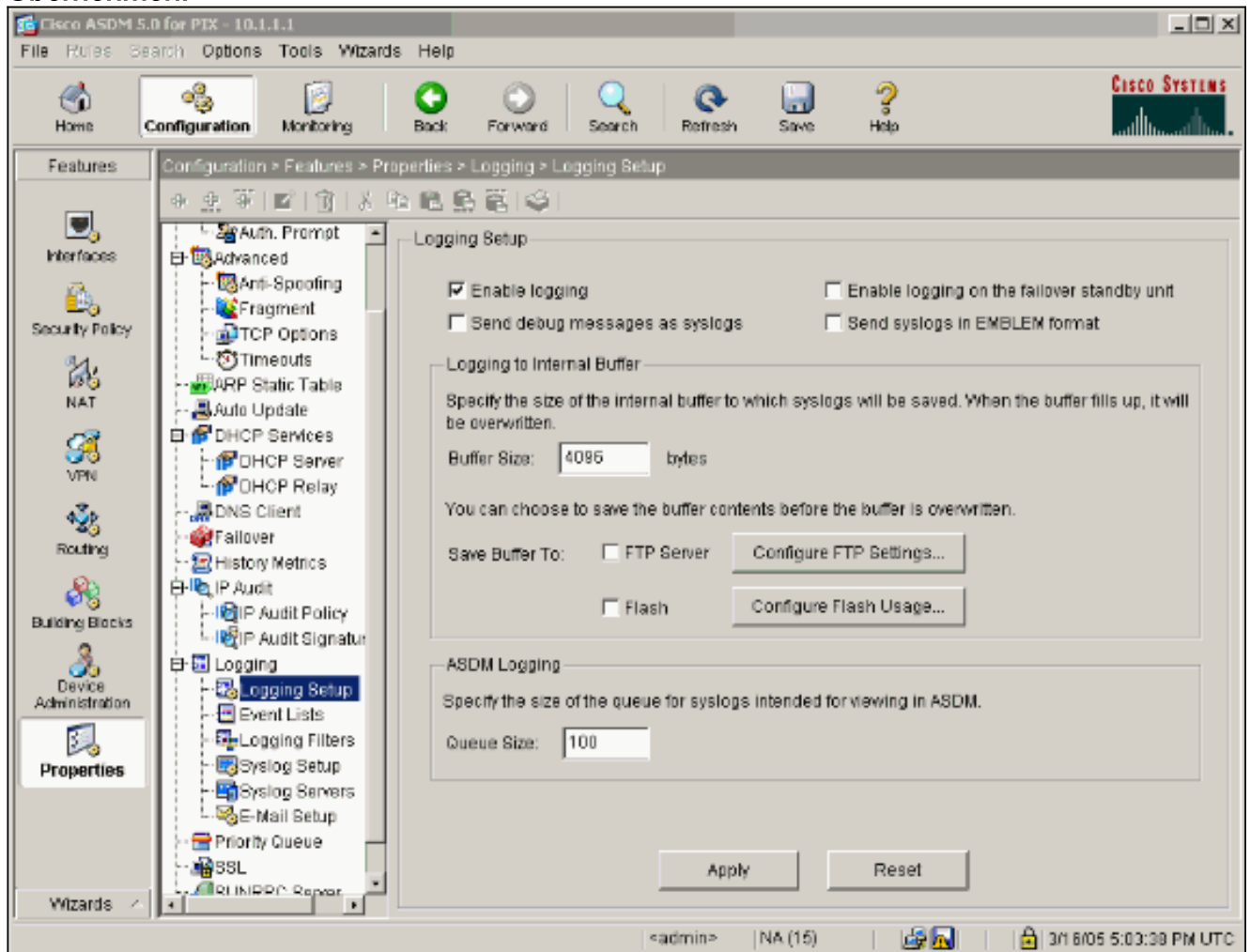
Befehle zur Fehlerbehebung für PIX

Bestimmte **show**-Befehle werden vom [Output Interpreter Tool](#) unterstützt (nur [registrierte](#) Kunden), mit dem Sie eine Analyse der **show**-Befehlsausgabe anzeigen können.

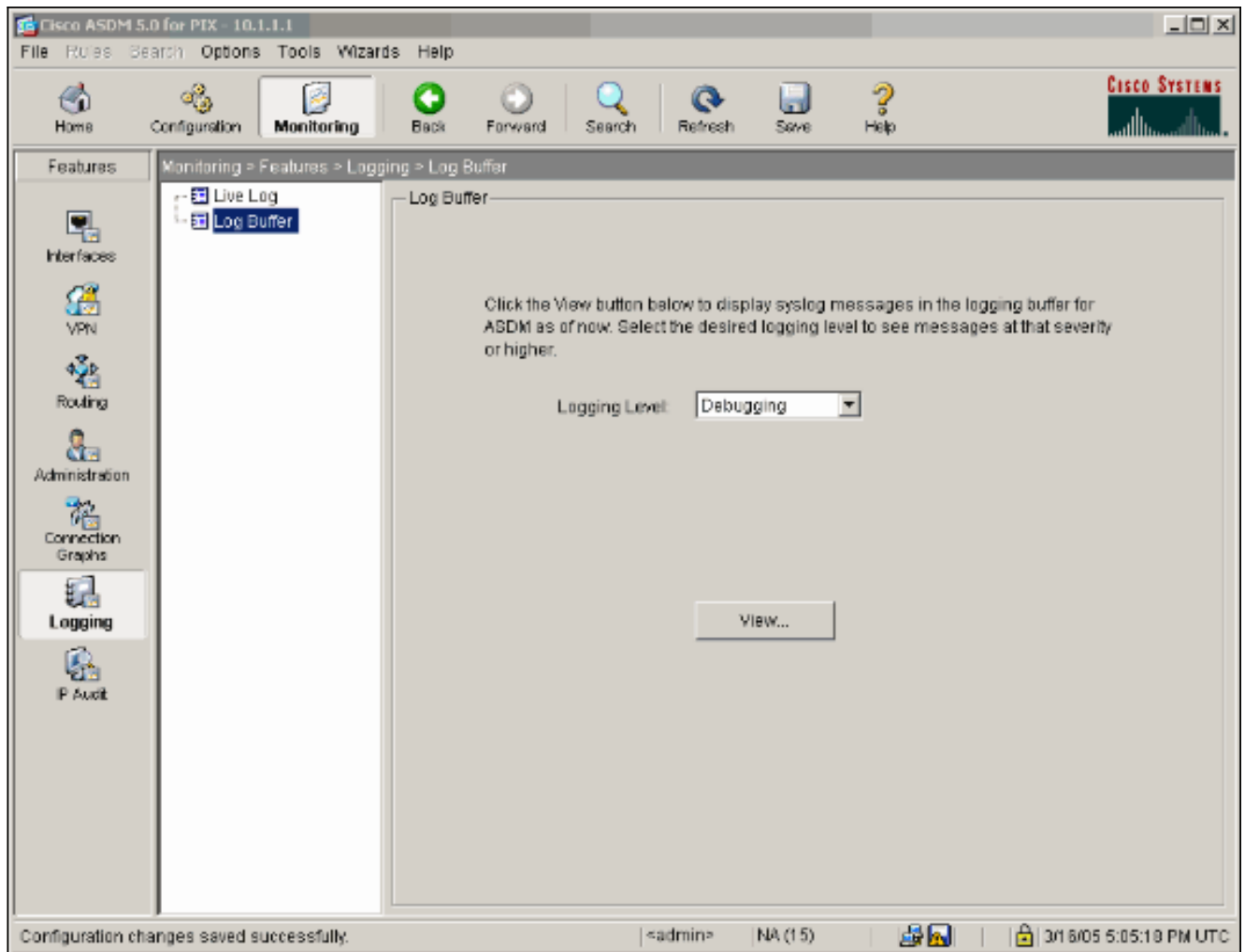
Hinweis: Lesen Sie [vor dem](#) Ausgabe von **Debug**-Befehlen unter [Wichtige Informationen zu Debug-Befehlen nach](#).

- **logging buffer debugging** - Zeigt Verbindungen an, die hergestellt und Hosts verweigert werden, die den PIX durchlaufen. Die Informationen werden im PIX-Protokollpuffer gespeichert, und die Ausgabe kann mit dem Befehl **show log** angezeigt werden.
- ASDM kann verwendet werden, um die Protokollierung zu aktivieren und die Protokolle anzuzeigen, wie in diesen Schritten gezeigt.

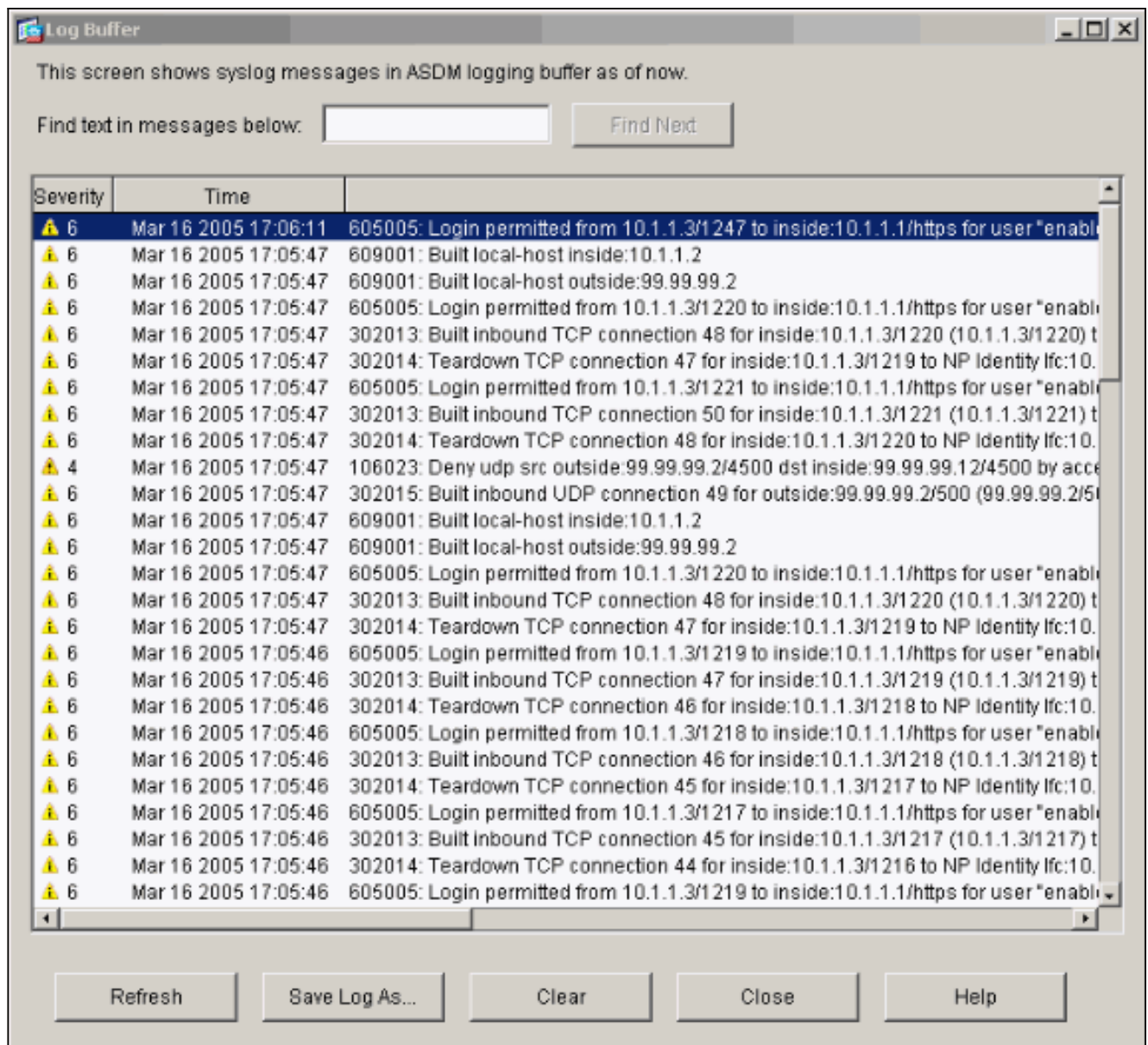
1. Wählen Sie **Konfiguration > Eigenschaften > Protokollierung > Protokollierung > Setup > Protokollierung aktivieren aus**, und klicken Sie dann auf **Übernehmen**.



2. Wählen Sie **Monitoring > Logging > Log Buffer > On Logging Level > Logging Buffer aus**, und klicken Sie dann auf **View (Anzeigen)**.



Dies ist ein Beispiel für den Log-Puffer.



Zugehörige Informationen

- [Support-Seite für IPsec-Aushandlung/IKE-Protokolle](#)
- [PIX-Support-Seite](#)
- [PIX-Befehlsreferenzen](#)
- [NAT-Support-Seite](#)
- [Anforderungen für Kommentare \(RFCs\)](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)