

PIX/ASA 7.x en hoger: Configuratievoorbeeld van meerdere interne netwerken met internet aansluiten

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Verwante producten](#)

[Conventies](#)

[Configureren](#)

[Achtergrondinformatie](#)

[Netwerkdigram](#)

[Configuraties](#)

[PIX-configuratie met ASDM](#)

[PIX-configuratie met CLI](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Opdrachten voor probleemoplossing](#)

[Procedure voor probleemoplossing](#)

[Kan geen toegang tot websites onder naam](#)

[Gerelateerde informatie](#)

Inleiding

Dit document biedt een voorbeeldconfiguratie voor PIX/ASA security applicatie versie 7.x en hoger met meerdere interne netwerken die verbinding maken met het internet (of een extern netwerk) door gebruik van de opdrachtregel interface (CLI) of Adaptieve security apparaat Manager (ASDM) 5.x en hoger.

Raadpleeg [Connectiviteit met Cisco security applicatie voor het opzetten en oplossen van problemen via PIX/ASA](#) voor informatie over het instellen en oplossen van problemen via PIX/ASA.

Raadpleeg [Infrl-, globale, statische, geleider- en toegangslijst Opdrachten en PIX-omleiding \(doorsturen\) op PIX](#) voor informatie over [de](#) gebruikelijke PIX-opdrachten.

Opmerking: Sommige opties in andere ASDM-versies kunnen verschillen van de opties in ASDM 5.1. Raadpleeg de [ASDM-documentatie](#) voor meer informatie.

Voorwaarden

Vereisten

Wanneer u meer dan één intern netwerk achter een PIX-firewall toevoegt, houd dan deze punten in gedachten:

- De PIX ondersteunt secundaire adressering niet.
- Er moet een router achter de PIX worden gebruikt om een routing tussen het bestaande netwerk en het nieuwe toegevoegde netwerk te realiseren.
- De standaardgateway van alle gasteren moet aan de binnenrouter wijzen.
- Voeg een standaardroute op de binnenrouter toe die aan PIX wijst.
- Schakel het arr-geheugen (Adretion Protocol) op de binnenrouter uit.

Raadpleeg [HTTPS-toegang voor ASDM toestaan](#) om het apparaat door de ASDM te laten configureren.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- PIX security applicatie 5150E met softwareversie 7.1
- ASDM 5.1
- Cisco-routers met Cisco IOS® softwarerelease 12.3(7)T

N.B.: Dit document is gecertificeerd met PIX/ASA-softwareversie 8.x en Cisco IOS-softwarerelease 12.4.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Verwante producten

Deze configuratie kan ook worden gebruikt met Cisco ASA security applicatie versie 7.x en hoger.

Conventies

Raadpleeg de [Cisco Technical Tips Convention](#) voor meer informatie over documentconventies.

Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Opmerking: Gebruik het [Opname Gereedschap](#) ([alleen geregistreerde](#) klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

De IP-adresseringsschema's die in deze configuratie worden gebruikt, zijn niet wettelijk

routeerbaar op het internet. Het zijn RFC 1918 adressen die in een labomgeving gebruikt zijn.

Achtergrondinformatie

In dit scenario zijn er drie interne netwerken (10.1.1.0/24, 10.2.1.0/24 en 10.3.1.0/24) die via PIX op het internet (of een extern netwerk) moeten worden aangesloten. De interne netwerken worden aangesloten op de interne interface van PIX. De internetconnectiviteit is door een router die op de buiteninterface van de PIX is aangesloten. De PIX heeft het IP-adres 172.16.1.1/24.

De statische routes worden gebruikt om de pakketten van de interne netwerken naar het Internet te leiden en vice versa. In plaats van het gebruiken van de statische routes, kunt u ook een dynamisch Routing Protocol gebruiken zoals Routing Information Protocol (RIP) of Open Shortest Path First (OSPF).

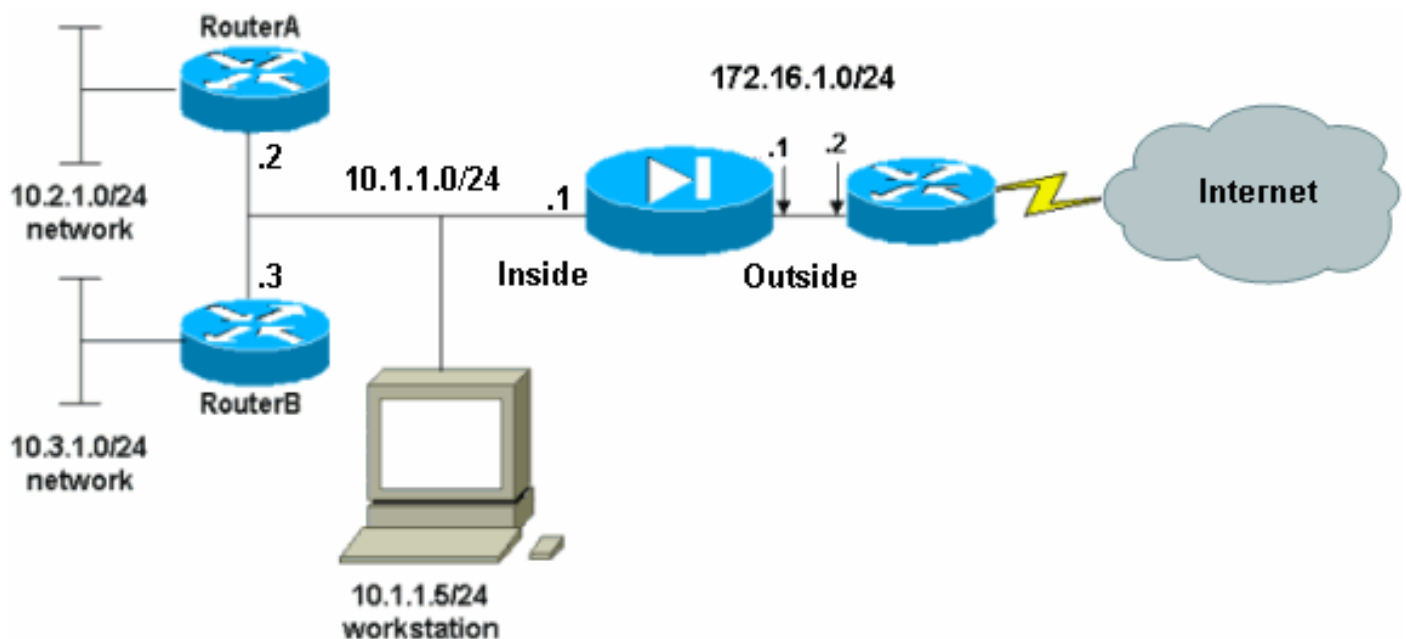
De interne hosts communiceren met het internet door de interne netwerken op PIX te vertalen met behulp van dynamisch NAT (pool van IP-adressen - 172.16.1.5 t/m 172.16.1.10). Als de pool van IP-adressen is uitgeput, zal PIX (met IP-adres 172.16.1.4) de interne hosts toegang tot het internet bieden.

Raadpleeg [PIX/ASA 7.x NAT- en PAT-verklaringen](#) voor meer informatie over NAT/PAT.

Opmerking: Als de statische NAT het externe IP (global_IP)-adres gebruikt om te vertalen, kan dit een vertaling veroorzaken. Gebruik daarom de sleutelwoordeninterface in plaats van het IP-adres in de statische vertaling.

Netwerkdigram

Het netwerk in dit document is als volgt opgebouwd:



De standaardgateway van de hosts op het 10.1.1.0-netwerk wijst op RouterA. Een standaardroute op RouterB wordt toegevoegd die aan RouterA wijst. RouterA heeft een standaardroute die naar de PIX binneninterface wijst.

Configuraties

Dit document gebruikt deze configuraties:

- [Configuratie van routerA](#)
- [Routerconfiguratie](#)
- [Configuratie PIX security applicatie 7.1PIX-configuratie met ASDMPIX security applicatie CLI-configuratie](#)

Configuratie van routerA

```
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#
```

Routerconfiguratie

```
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#

```

Als u de ASDM voor de configuratie van de PIX security applicatie wilt gebruiken maar het apparaat niet op zijn plaats hebt, moet u deze stappen uitvoeren:

1. console in de PIX.
2. Gebruik vanuit een geklaard configuratie de interactieve aanwijzingen om ASDM voor het beheer van de PIX van werkstation 10.1.1.5 mogelijk te maken.

Configuratie PIX security applicatie 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-configuratie met ASDM](#)

Voltooi deze stappen om ze te configureren via de ASDM GUI:

1. Open vanaf werkstation 10.1.1.5 een webbrowser om ASDM te gebruiken (in dit voorbeeld <https://10.1.1.1>).
2. Klik op **Ja** in de reacties op het certificaat.
3. Meld u aan met het wachtwoord voor het inschakelen, zoals eerder ingesteld.
4. Als dit de eerste keer is dat ASDM op de PC wordt uitgevoerd, wordt u gevraagd om ASDM Launcher of ASDM als een Java-app te gebruiken. In dit voorbeeld wordt ASDM Launcher geselecteerd en geïnstalleerd.
5. Ga naar het ASDM Home-venster en klik op **Configuration**.

Cisco ASDM 5.1 for PIX - 10.1.1.1

File Rules Search Options Tools Wizards Help

Home Configuration Monitoring Back Forward Search Refresh Save Help

Device Information

General License

Host Name: **pixfirewall.default.domain.invalid**

PIX Version: **7.1(1)** Device Uptime: **14d 6h 4m 4s**

ASDM Version: **5.1(1)** Device Type: **PIX 515E**

Firewall Mode: **Routed** Context Mode: **Single**

Total Flash: **16 MB** Total Memory: **64 MB**

VPN Status

IKE Tunnels: **0** IPsec Tunnels: **0**

System Resources Status

CPU

CPU Usage (percent)

1% 17:58:19

Memory

Memory Usage (MB)

39MB 17:58:19

Interface Status

Interface	IP Address/Mask	Line	Link	Current Kbps
inside	10.1.1.1/24	up	up	1

Select an interface to view input and output Kbps

Traffic Status

Connections Per Second Usage

UDP: 0 TCP: 0 Total: 0

'inside' Interface Traffic Usage (Kbps)

Input Kbps: 0 Output Kbps: 1

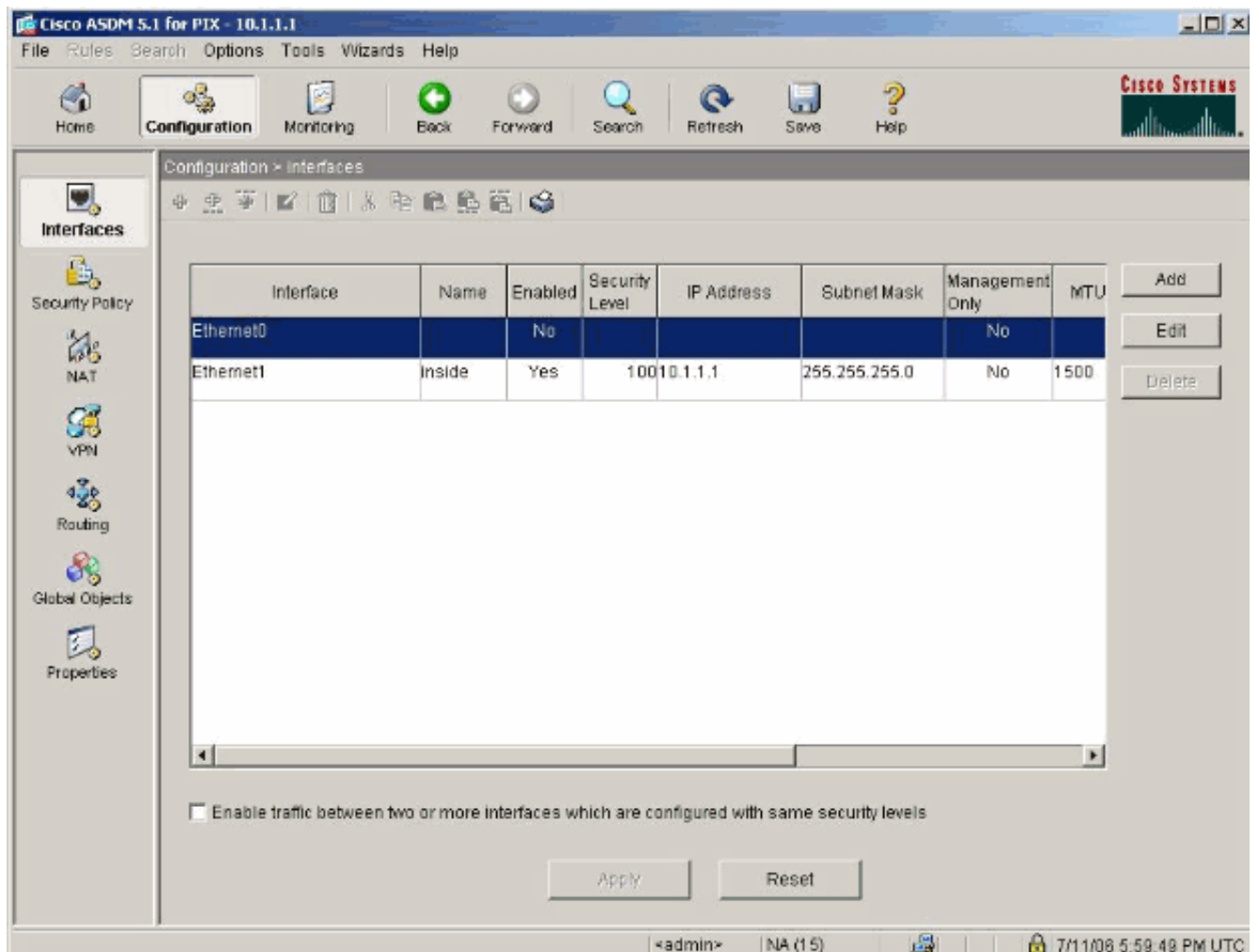
Latest ASDM Syslog Messages

-- Syslog Disabled --

Configure ASDM Syslog Filter

<admin> NA (15) 7/11/06 5:58:59 PM UTC

6. Kies **Interface > Bewerken** om de externe interface te configureren.



7. Voer de interfacedetails in en klik op **OK** wanneer u klaar bent.

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:

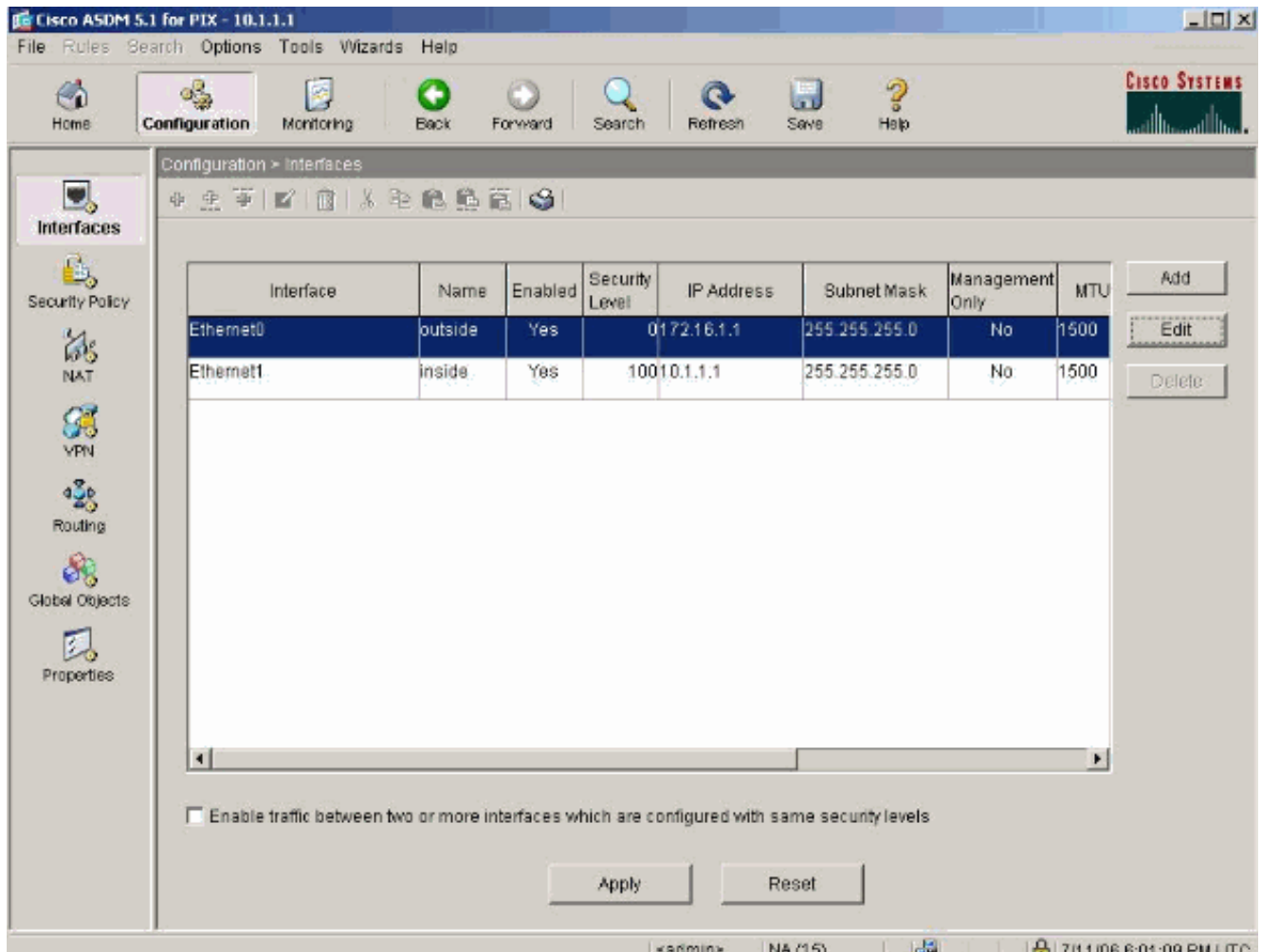
Description:

8. Klik op **OK** in het dialoogvenster Beveiligingsniveau wijzigen.

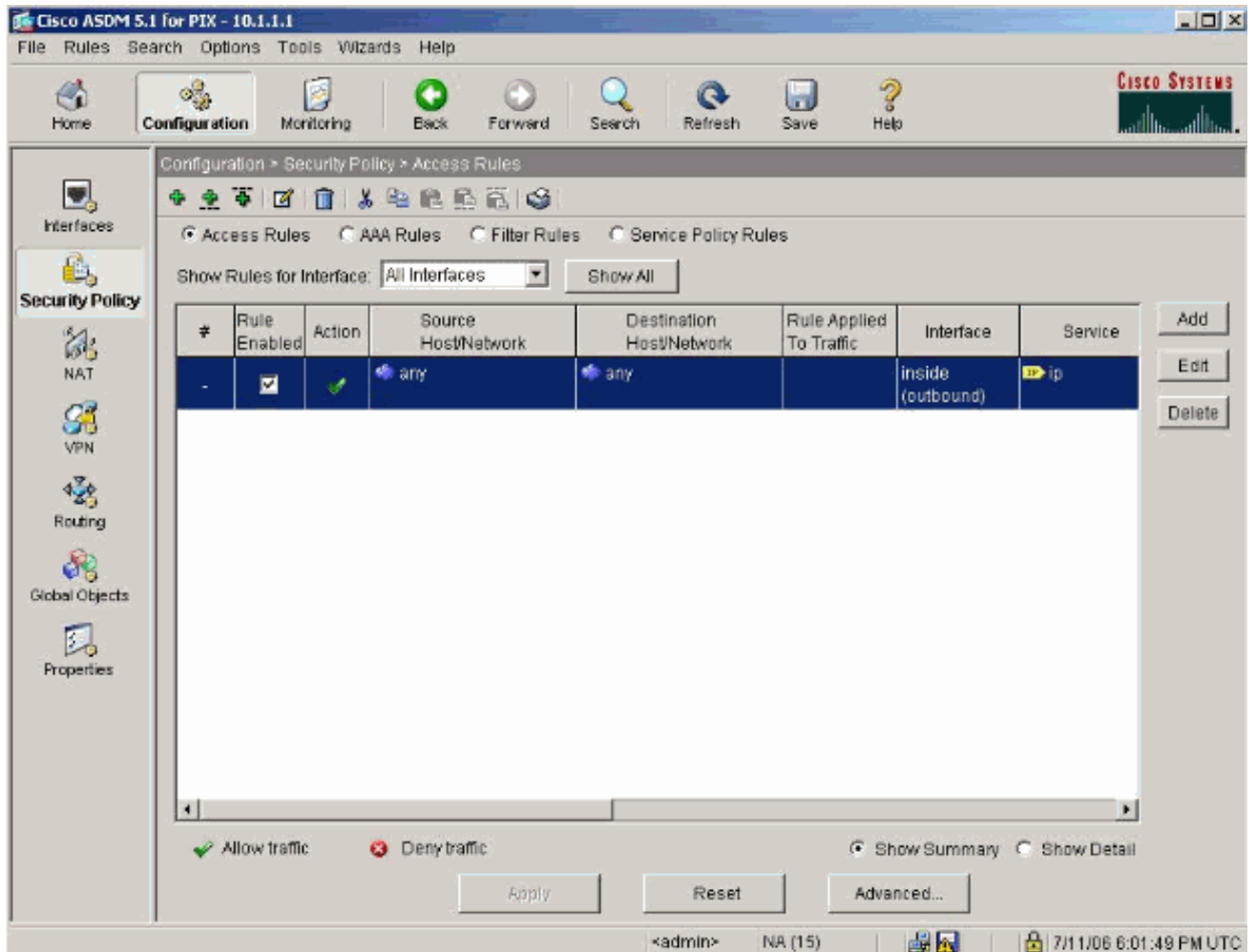
Security Level Change

 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?

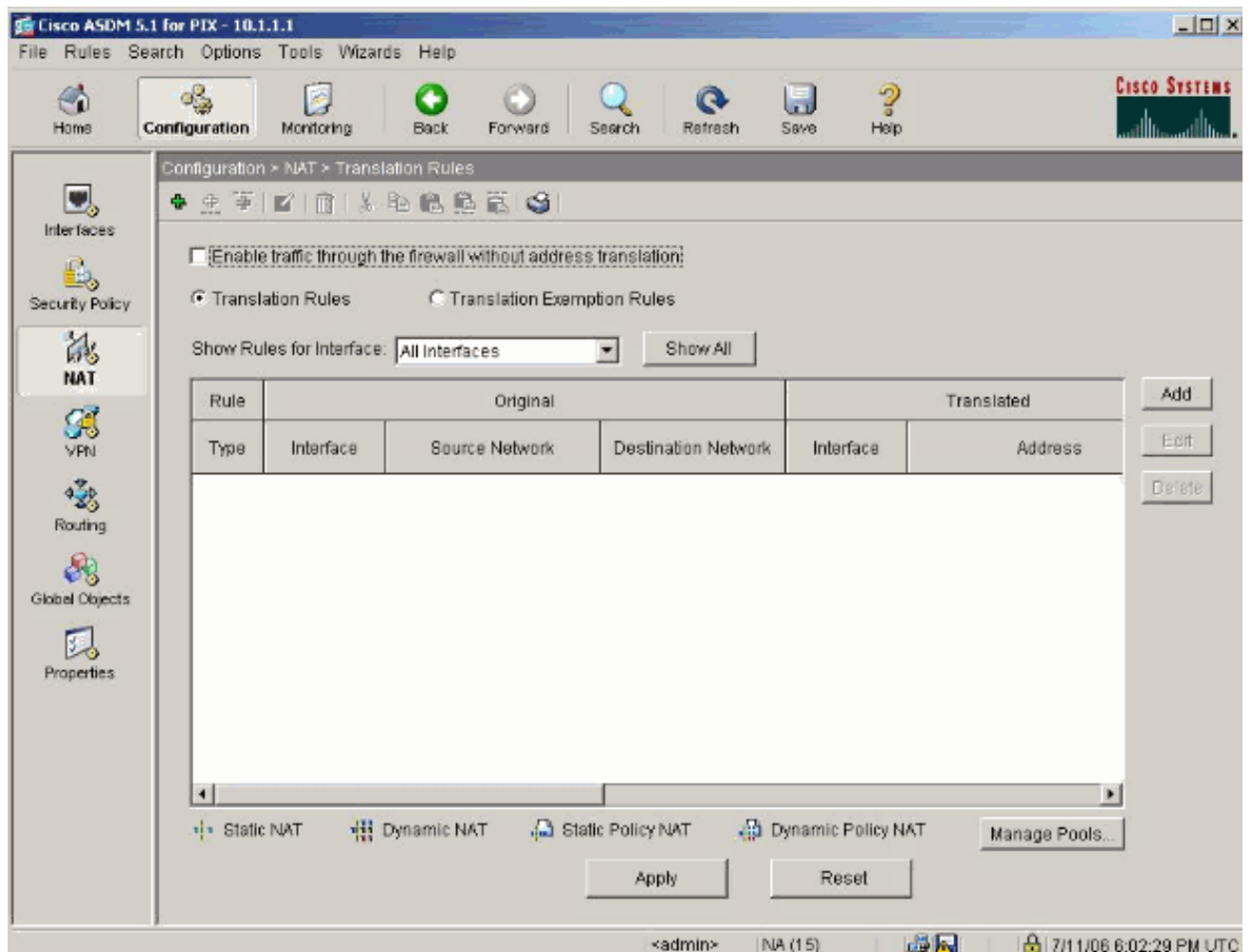
9. Klik op **Toepassen** om de interfaceconfiguratie te aanvaarden. De configuratie wordt ook op de PIX geduwd.



10. Kies **Veiligheidsbeleid** op het tabblad Opties om de gebruikte beveiligingsregels te bekijken. In dit voorbeeld wordt de standaard binnenregel gebruikt.



11. In dit voorbeeld wordt NAT gebruikt. Schakel het aankruispunt **via de firewall** uit **zonder het aankruisvakje voor adresomzetting** en klik op **Toevoegen** om de NAT-regel te configureren.



12. Configureer het bronnetwerk. In dit voorbeeld, wordt 10.0.0.0 gebruikt voor het IP adres, en 255.0.0.0 wordt gebruikt voor het masker. Klik op **Pools beheren** om de NAT-pooladressen te definiëren.

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

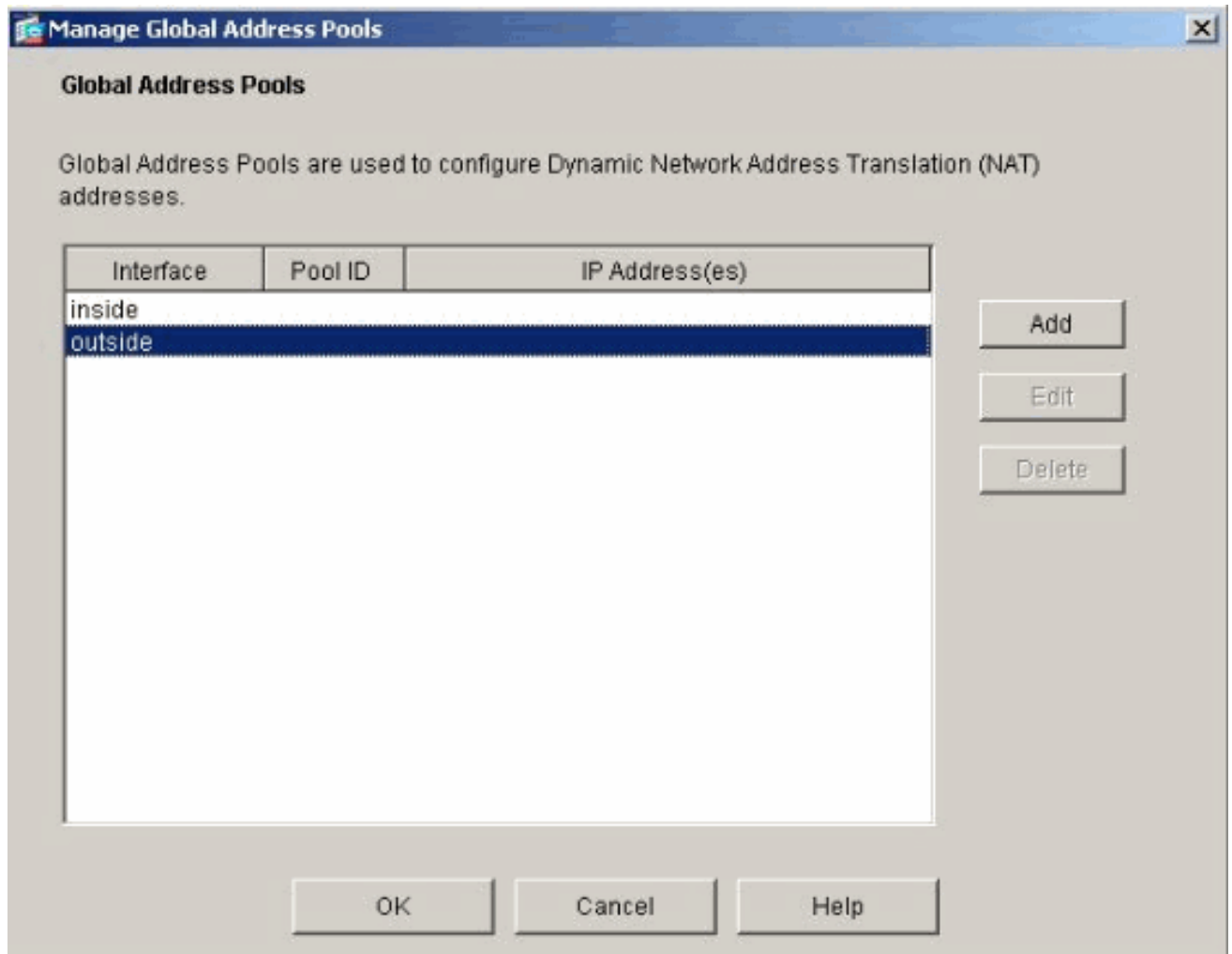
TCP Original port: Translated port:

UDP

Dynamic Address Pool:

Pool ID	Address
N/A	No address pool defined

13. Selecteer de externe interface en klik op **Toevoegen**.



14. In dit voorbeeld, worden een Bereik en PAT adrespool gevormd. Configureer het bereik van NAT en klik op **OK**.

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):

15. Selecteer de externe interface in stap 13 om het PAT-adres te configureren. Klik op **OK**

Add Global Pool Item

Interface: Pool ID:

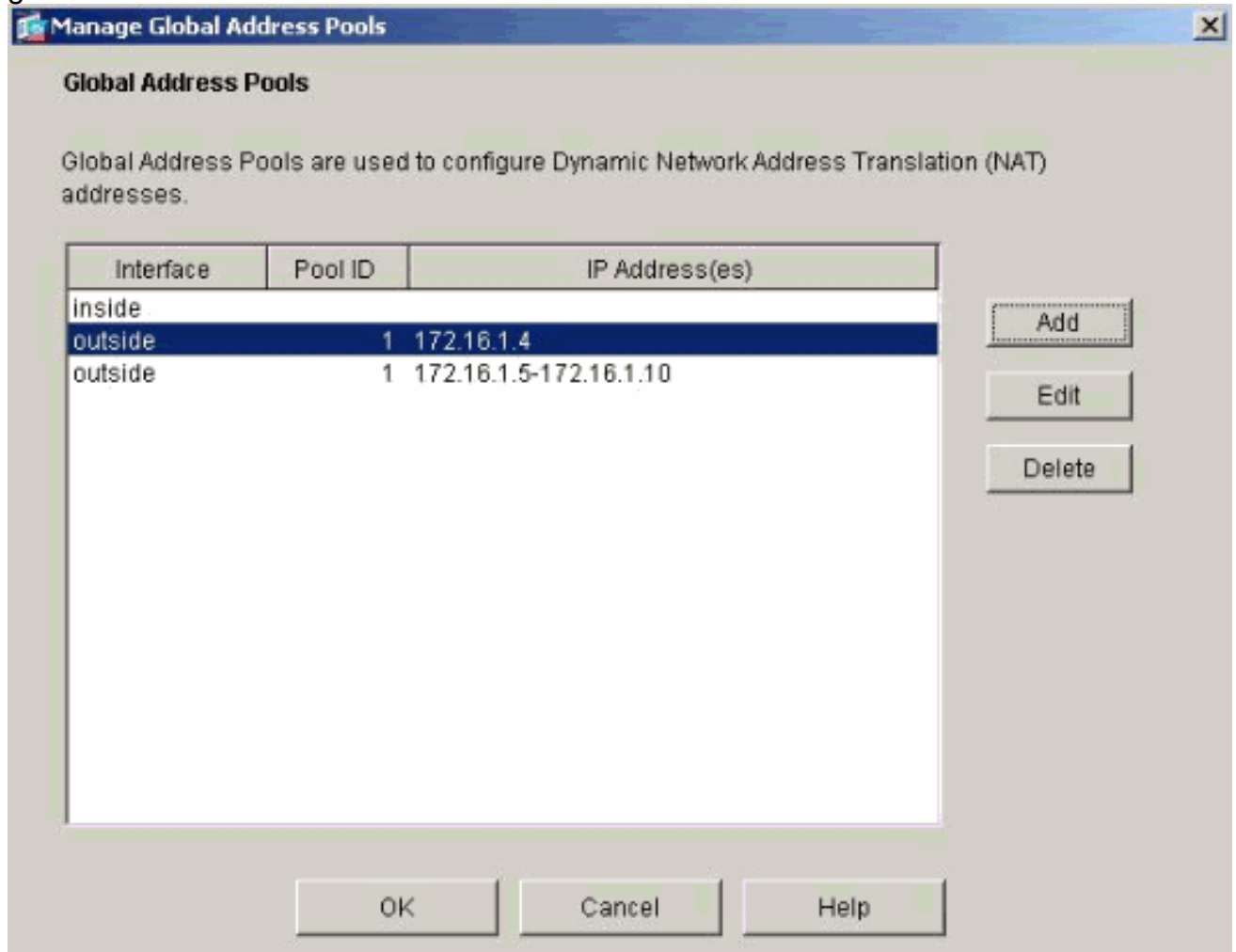
Range
 Port Address Translation (PAT)
 Port Address Translation (PAT) using the IP address of the interface

IP Address: —

Network Mask (optional):

Klik op **OK** om verder te

gaan.



16. Selecteer in het venster Adres Translation Rule de optie Pool ID die door het bronnetwerk zal worden gebruikt. Klik op **OK**.

Edit 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	172.16.1.4 172.16.1.5-172.16.1.10

17. Klik op **Toepassen** om de geconfigureerde NAT-regel op de PIX te drukken.

Cisco ASDM 5.1 for PIX - 10.1.1.1

File Rules Search Options Tools Wizards Help

Home Configuration Monitoring Back Forward Search Refresh Save Help

Configuration > NAT > Translation Rules

Enable traffic through the firewall without address translation

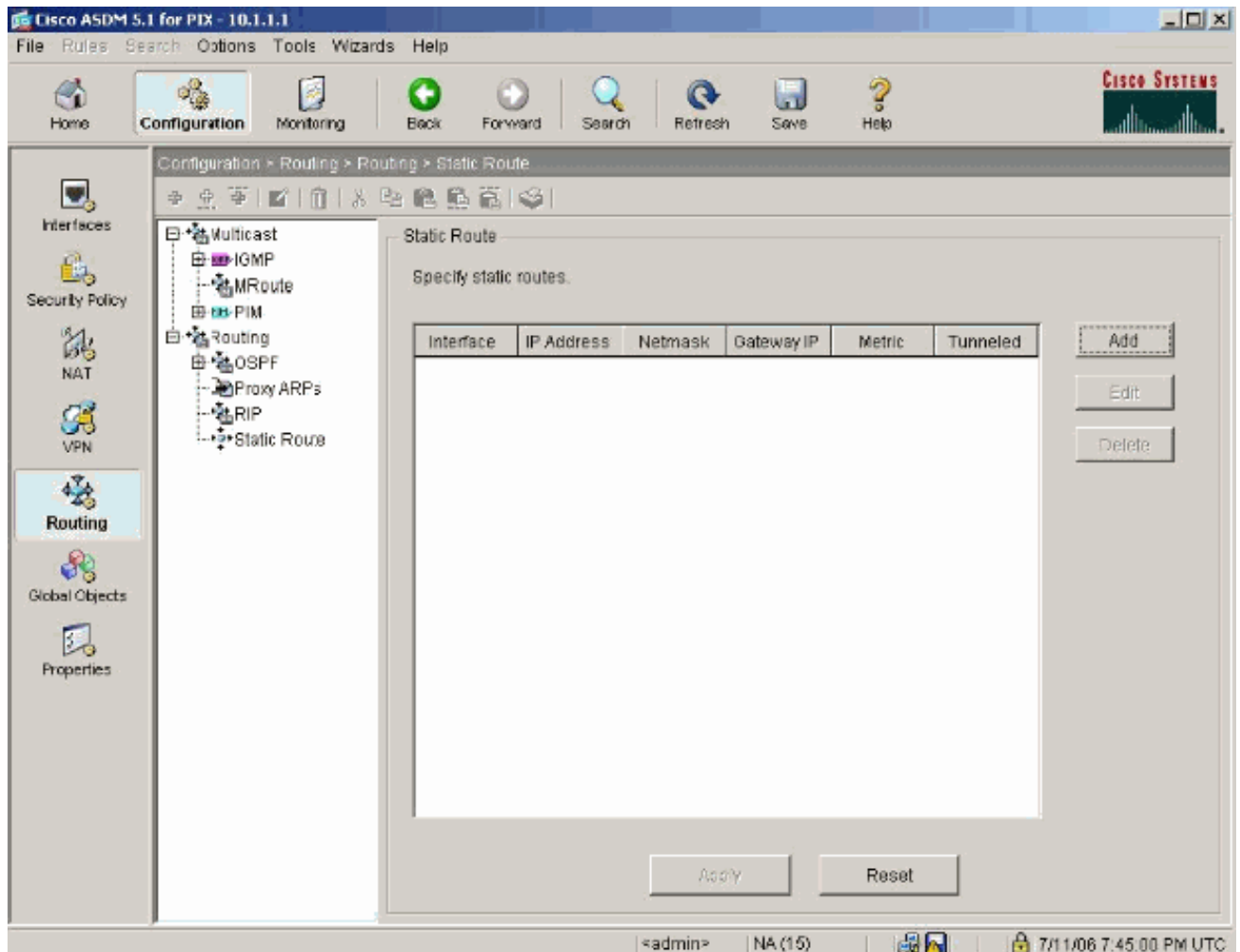
Translation Rules Translation Exemption Rules

Show Rules for Interface: All Interfaces

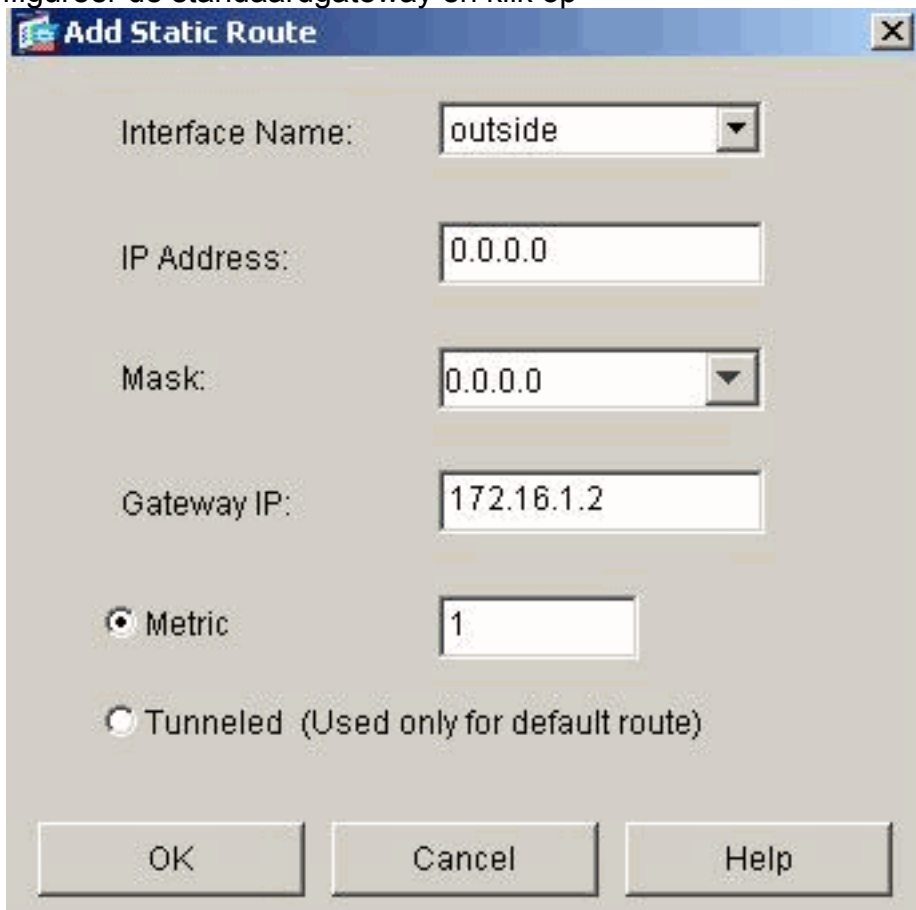
Rule	Original			Translated		Add	Edit	Delete
	Type	Interface	Source Network	Destination Network	Interface			
		inside	10.0.0.0/8	any	outside	172.16.1.4 172.16.1.5-172.16.1.10		

Device configuration loaded successfully. <admin> NA (15) 7/11/08 7:44:00 PM UTC

18. In dit voorbeeld worden statische routes gebruikt. Klik op **Routing**, kies **Statische route** en klik op **Toevoegen**.



19. Configureer de standaardgateway en klik op



OK.

20. Klik op **Add** en voeg de routes aan de binnennetwerken

Add Static Route

Interface Name:

IP Address:

Mask:

Gateway IP:

Metric

Tunneled (Used only for default route)

toe.

Add Static Route

Interface Name:

IP Address:

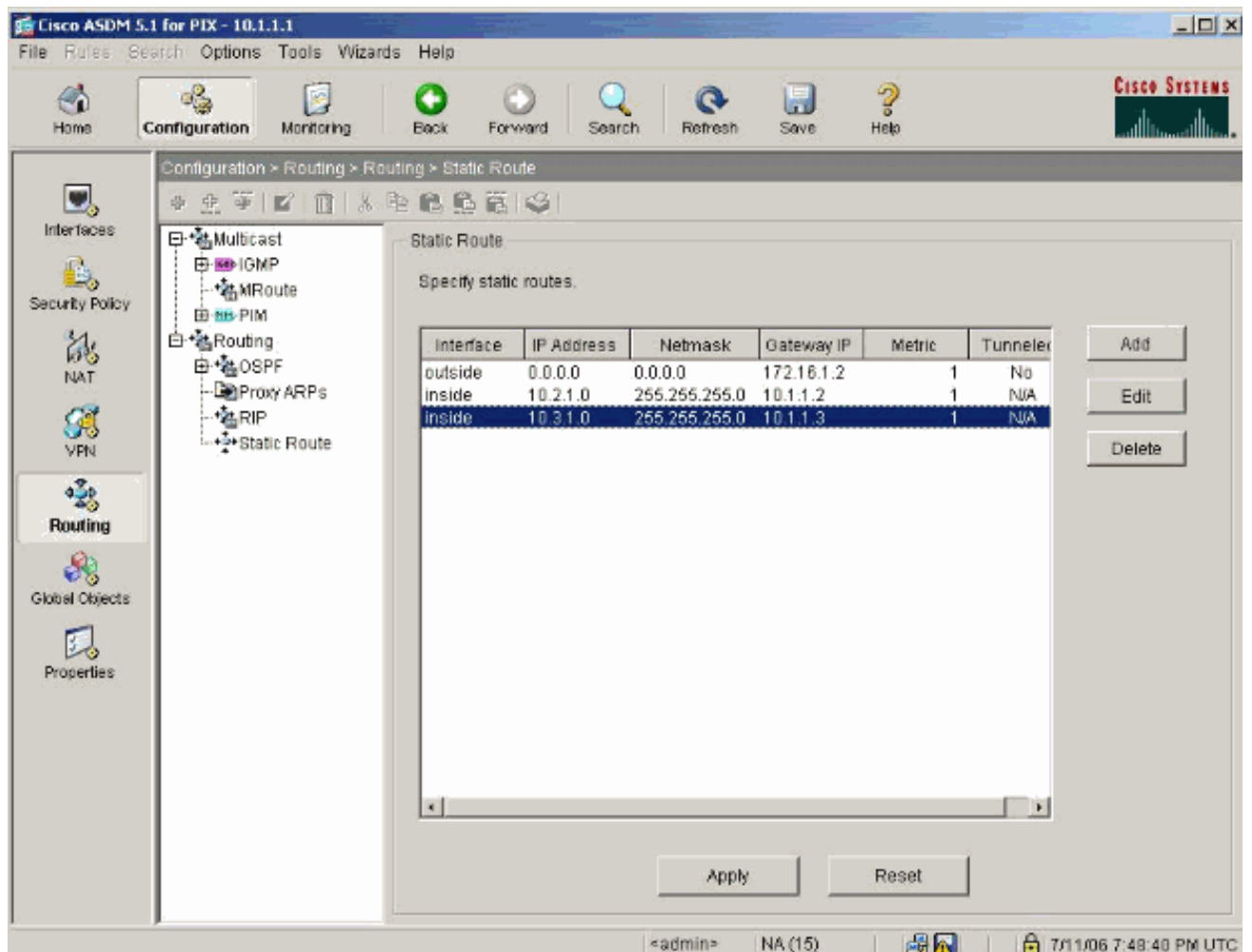
Mask:

Gateway IP:

Metric

Tunneled (Used only for default route)

21. Bevestig dat de juiste routes zijn geconfigureerd en klik op **Toepassen**.



PIX-configuratie met CLI

De configuratie via de ASDM GUI is nu voltooid.

U kunt deze configuratie zien via de CLI:

PIX security applicatie CLI

```

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
!

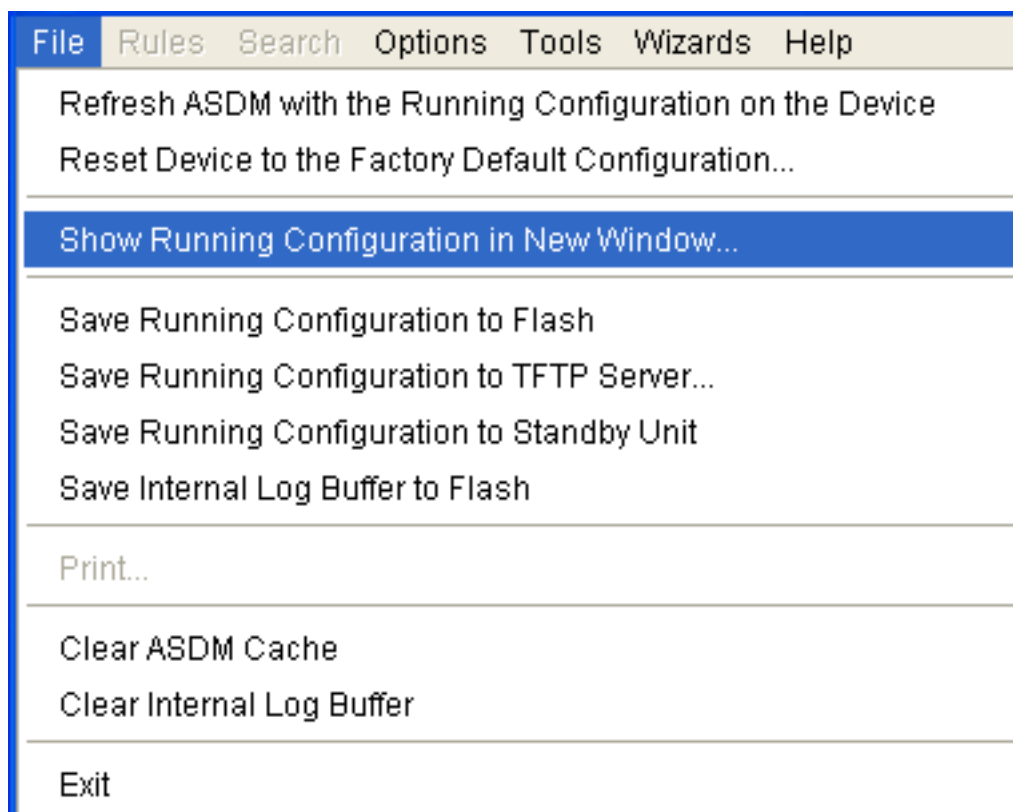
interface Ethernet1
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0
!--- Assign name and IP address to the interfaces enable
password 2KFQnbNIdI.2KYOU encrypted passwd
2KFQnbNIdI.2KYOU encrypted asdm image
flash:/asdmfile.50073 no asdm history enable arp timeout
14400 nat-control
!--- 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

```

Kies **Bestand > Running Configuration in New Window** tonen om de CLI-configuratie in ASDM te bekijken.



Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Opdrachten voor probleemoplossing

Het [Uitvoer Tolk](#) ([uitsluitend geregistreeerde](#) klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

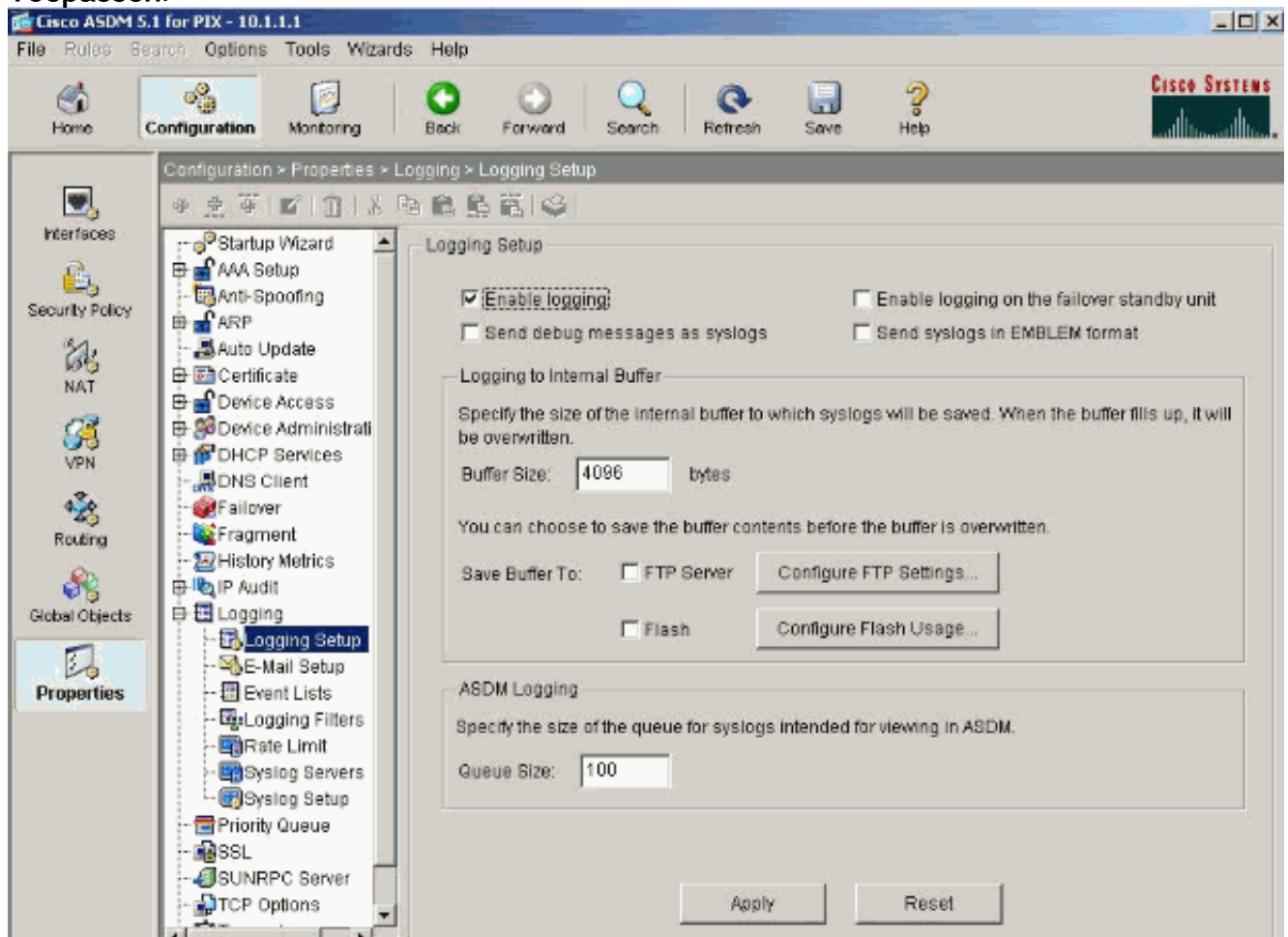
Opmerking: Raadpleeg [Belangrijke informatie over debug Commands](#) voordat u **debug**-opdrachten gebruikt.

- **bug**-overtrekken: toont aan of de verzoeken van ICMP van de hosts de PIX bereiken. Om dit debug te kunnen uitvoeren, moet u de opdracht **toegangslijsten** toevoegen om ICMP in uw configuratie toe te staan.
- **het zuiveren** van de **buffer**-toont verbindingen die gevestigd en ontkend worden aan hosts die door de PIX gaan. De informatie wordt opgeslagen in de PIX-logbuffer en u kunt de uitvoer zien met de opdracht **Logboek weergeven**.

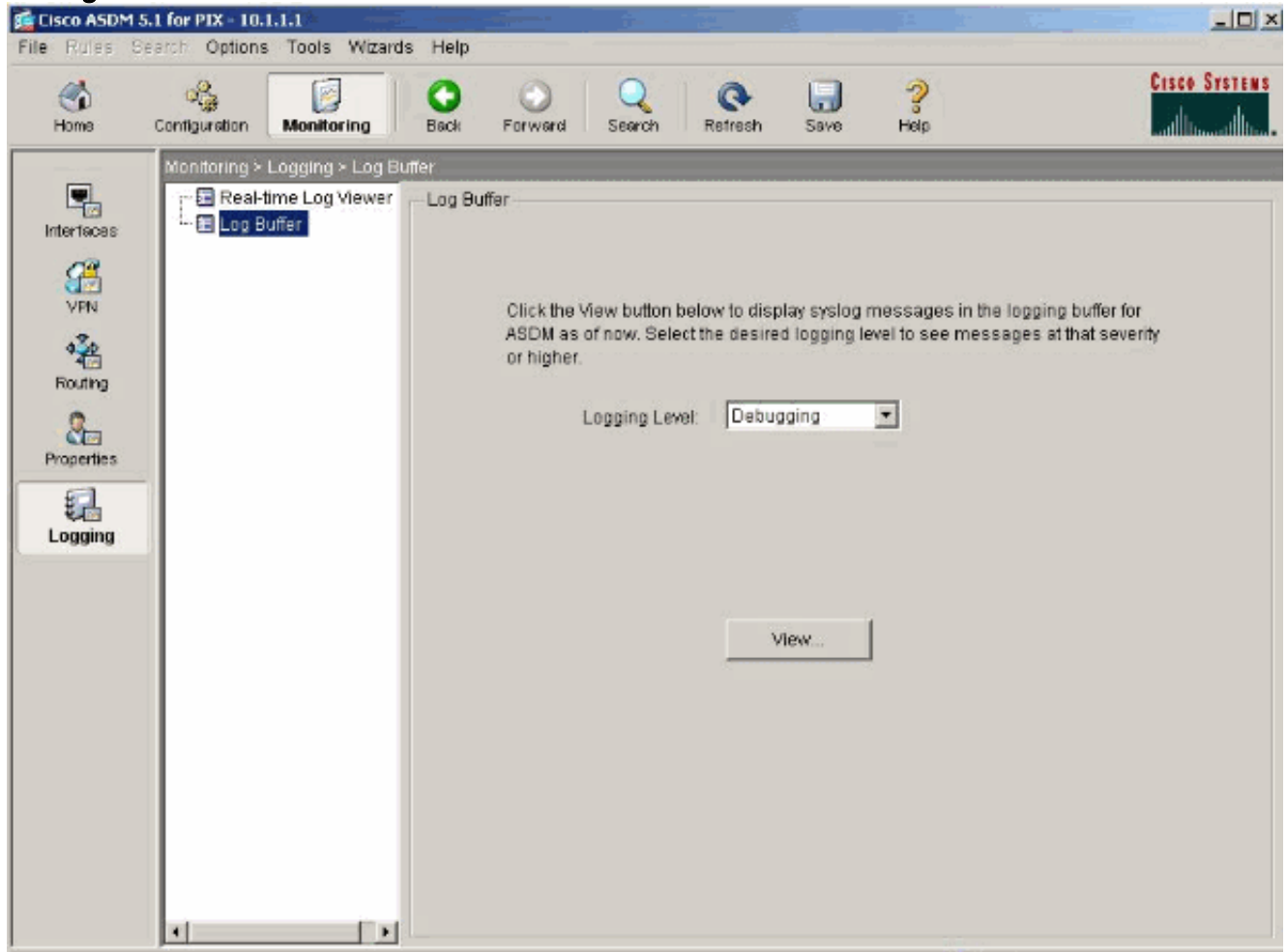
Procedure voor probleemoplossing

ASDM kan worden gebruikt om houtkap mogelijk te maken en ook om de logbestanden te bekijken:

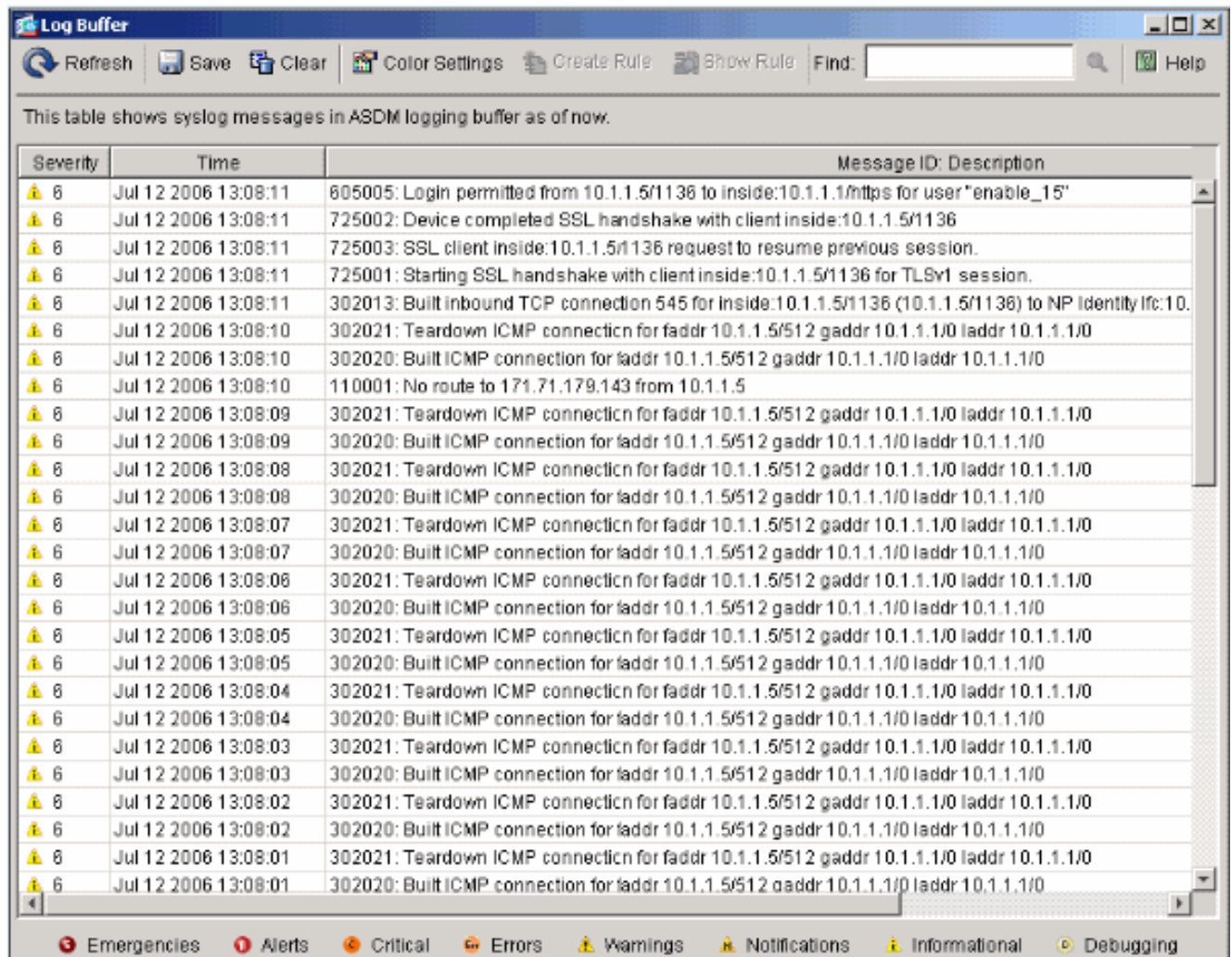
1. Kies **Configuratie > Eigenschappen > Vastlegging > Instellen vastlegging**, controleer **Vastlegging inschakelen** en klik op **Toepassen**.



2. Kies **Controle > Vastlegging > Buffer > Logging Level** en kies **Logging Buffer** uit de vervolgkeuzelijst. Klik op **Weergeven**.



3. Hier is een voorbeeld van de Log Buffer:



Severity	Time	Message ID: Description
6	Jul 12 2006 13:08:11	805005: Login permitted from 10.1.1.5/1136 to inside:10.1.1.1/https for user "enable_15"
6	Jul 12 2006 13:08:11	725002: Device completed SSL handshake with client inside:10.1.1.5/1136
6	Jul 12 2006 13:08:11	725003: SSL client inside:10.1.1.5/1136 request to resume previous session.
6	Jul 12 2006 13:08:11	725001: Starting SSL handshake with client inside:10.1.1.5/1136 for TLSv1 session.
6	Jul 12 2006 13:08:11	302013: Built inbound TCP connection 545 for inside:10.1.1.5/1136 (10.1.1.5/1136) to NP Identity Ifc:10.
6	Jul 12 2006 13:08:10	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:10	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:10	110001: No route to 171.71.179.143 from 10.1.1.5
6	Jul 12 2006 13:08:09	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:09	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:08	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:08	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:07	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:07	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:06	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:06	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:05	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:05	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:04	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:04	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:03	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:03	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:02	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:02	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:01	302021: Teardown ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0
6	Jul 12 2006 13:08:01	302020: Built ICMP connection for faddr 10.1.1.5/512 gaddr 10.1.1.1/0 laddr 10.1.1.1/0

[Kan geen toegang tot websites onder naam](#)

In bepaalde scenario's hebben de interne netwerken geen toegang tot de internetwebsites door in de webbrowser de naam (werkt met IP-adres) te gebruiken. Dit probleem is gebruikelijk en doet zich meestal voor als de DNS-server niet is gedefinieerd, vooral in gevallen waarin PIX/ASA de DHCP-server is. Dit kan ook voorkomen in gevallen als PIX/ASA niet in staat is om de DNS server te drukken of als de DNS server niet bereikbaar is.

[Gerelateerde informatie](#)

- [Cisco PIX 500 Series security applicaties](#)
- [Cisco ASA 5500 Series adaptieve security applicaties](#)
- [Opdrachtreferenties van Cisco Secure PIX-firewall](#)
- [Cisco adaptieve security apparaatbeheer](#)
- [Probleemoplossing en meldingen voor Cisco Adaptieve Security apparaat Manager \(ASDM\)](#)
- [Verzoeken om opmerkingen \(RFC's\)](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)