

PIX/ASA 7.x y posteriores: Conexión de las redes internas múltiples con el ejemplo de configuración de Internet

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Productos Relacionados](#)

[Convenciones](#)

[Configurar](#)

[Antecedentes](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Configuración PIX usando el ASDM](#)

[Configuración PIX usando el CLI](#)

[Verificación](#)

[Troubleshooting](#)

[Comandos para resolución de problemas](#)

[Procedimiento de Troubleshooting](#)

[Incapaz de acceder los sitios web por nombre](#)

[Información Relacionada](#)

Introducción

Este documento proporciona una configuración de muestra para la versión 7.x y posterior del Dispositivo de Seguridad PIX/ASA con varias redes internas que se conectan a Internet (o a una red externa) usando la interfaz de línea de comandos (CLI) o Adaptive Security Device Manager (ASDM) 5.x y posterior.

Refiérase [establecen y resuelven problemas la Conectividad a través del dispositivo del Cisco Security](#) para la información sobre cómo establecer y resolver problemas la Conectividad con el PIX/ASA.

Refiérase [usando nacional, global, estático, conducto, y los comandos access-list y el puerto Redirection\(Forwarding\) en el PIX](#) para la información sobre los comandos pix comunes.

Nota: Algunas opciones en otras versiones del ASDM pueden aparecer diferentes de las opciones en el ASDM 5.1. Consulte la [documentación ASDM](#) para obtener más información.

prerrequisitos

Requisitos

Cuando usted agrega más de una red interna detrás de un firewall PIX, tenga estas puntas presente:

- El PIX no soporta el direccionamiento secundario.
- Un router tiene que ser utilizado detrás del PIX para alcanzar la encaminamiento entre la red existente y la red nuevamente agregada.
- El default gateway de todos los host necesita señalar al router interno.
- Agregue una ruta predeterminado en el router interno esas puntas al PIX.
- Borre el caché del Address Resolution Protocol (ARP) en el router interno.

Consulte [Cómo Permitir Acceso HTTPS para ASDM](#) para permitir que el dispositivo sea configurado por el ASDM.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Dispositivo de seguridad 515E PIX con la versión de software 7.1
- ASDM 5.1
- Routeres Cisco con el Software Release 12.3(7)T de Cisco IOS®

Nota: Este documento recertified con la versión de software 8.x del PIX/ASA y el Cisco IOS Software Release 12.4.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Productos Relacionados

Esta configuración se puede también utilizar con la versión 7.x y posterior del dispositivo de seguridad de Cisco ASA.

Convenciones

Consulte [Convenciones de Consejos Técnicos de Cisco](#) para obtener más información sobre las convenciones sobre documentos.

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Utilice la herramienta [Command Lookup Tool](#) ([clientes registrados solamente](#)) para obtener

más información sobre los comandos utilizados en esta sección.

Los esquemas de direccionamiento IP usados en esta configuración no son legalmente enrutables en Internet. Son las direcciones RFC1918 que se han utilizado en un entorno de laboratorio.

Antecedentes

En este escenario, hay tres redes internas (10.1.1.0/24, 10.2.1.0/24 y 10.3.1.0/24) que se conectarán con Internet (o una red externa) con el PIX. Las redes internas están conectadas con la interfaz interior del PIX. La conectividad a Internet está a través de un router que esté conectado con la interfaz exterior del PIX. El PIX tiene la dirección IP 172.16.1.1/24.

Las Static rutas se utilizan para rutear los paquetes de las redes internas a Internet y vice versa. En vez de usar las Static rutas, usted puede también utilizar un Dynamic Routing Protocol tal como Routing Information Protocol (RIP) o Open Shortest Path First (OSPF).

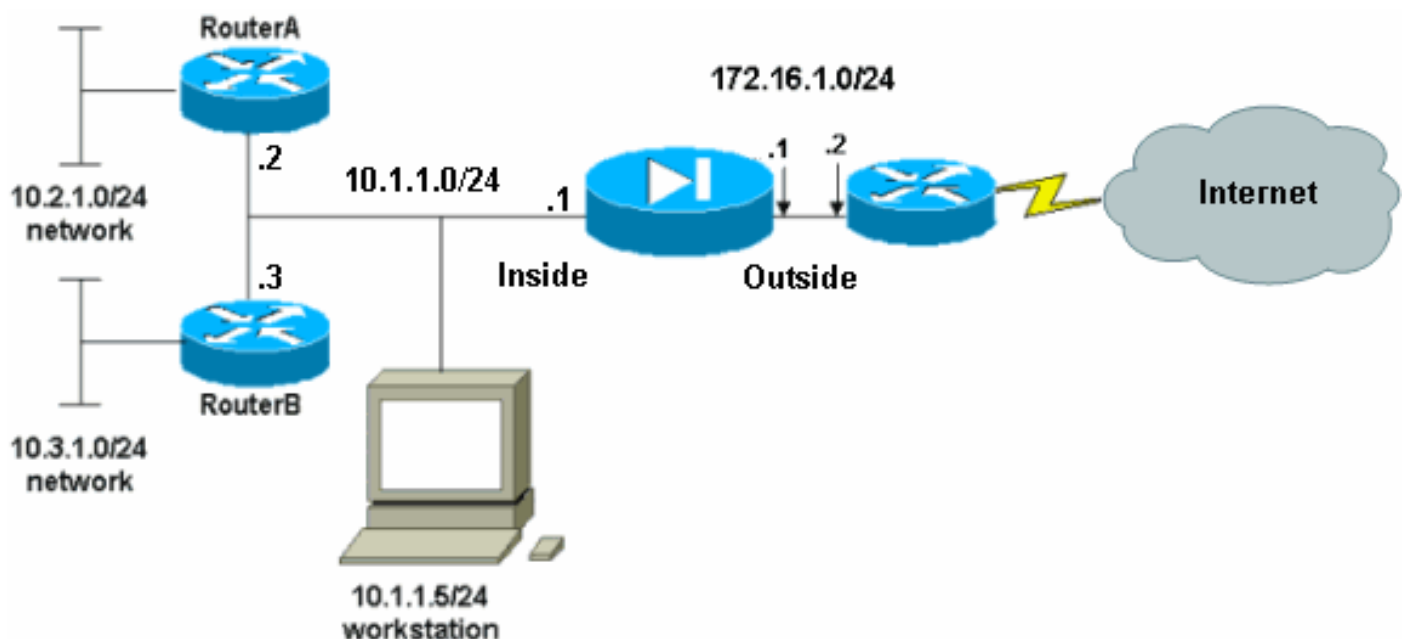
Los host internos comunican con Internet traduciendo las redes internas en el PIX usando NAT dinámico (pool de los IP Addresses - 172.16.1.5 a 172.16.1.10). Si el pool de los IP Addresses se agota, el PIX ACARICIARÁ (usando la dirección IP 172.16.1.4) a los host internos para alcanzar Internet.

Refiera a las [declaraciones del PIX/ASA 7.x NAT y de la PALMADITA](#) para más información sobre el NAT/PAT.

Nota: Si el NAT estático utiliza la dirección exterior del IP (global_IP) para traducir, ésta pudo causar una traducción. Por lo tanto, use la **interfaz de la** palabra clave en vez de la dirección IP en la traducción estática.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



La gateway predeterminada de los hosts en la red 10.1.1.0 apunta hacia el RouterA. Una ruta predeterminado en el routerB se agrega que señala al routerA. RouterA tiene una ruta

predeterminada que señala a la interfaz interior de PIX.

Configuraciones

En este documento, se utilizan estas configuraciones:

- [Configuración del router A](#)
- [Configuración del RouterB](#)
- [Configuración del dispositivo de seguridad 7.1 PIX Configuración PIX usando el ASDM Configuración CLI del dispositivo de seguridad PIX](#)

Configuración del router A

```
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#
```

Configuración del RouterB

```
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#

```

Si usted quiere utilizar el ASDM para la configuración del dispositivo de seguridad PIX, pero no ha atado el dispositivo con correa, complete estos pasos:

1. Consola en el PIX.
2. De una configuración despejada, utilice los prompts interactivos para habilitar el ASDM para la Administración del PIX del puesto de trabajo 10.1.1.5.

Configuración del dispositivo de seguridad 7.1 PIX

```

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>
```

[Configuración PIX usando el ASDM](#)

Complete estos pasos para configurar vía el ASDM GUI:

1. Del puesto de trabajo 10.1.1.5, abra a un buscador Web para utilizar el ADSM (en este ejemplo, <https://10.1.1.1>).
2. Haga clic **sí** en los prompts del certificado.
3. Inicie sesión con la contraseña habilitada, según lo configurado previamente.
4. Si esto está la primera vez el ASDM se ejecuta en el PC, a le indican que utilice el activador de ASDM o el ASDM como subprograma Java. En este ejemplo, se selecciona y está instalado el activador de ASDM.
5. Vaya a la ventana de inicio de ASDM y haga clic la **configuración**.

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)

38MB 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

17:58:19

UDP: 0 TCP: 0 Total: 0

'inside' Interface Traffic Usage (Kbps)

17:58:19

Input Kbps: 0 Output Kbps: 1

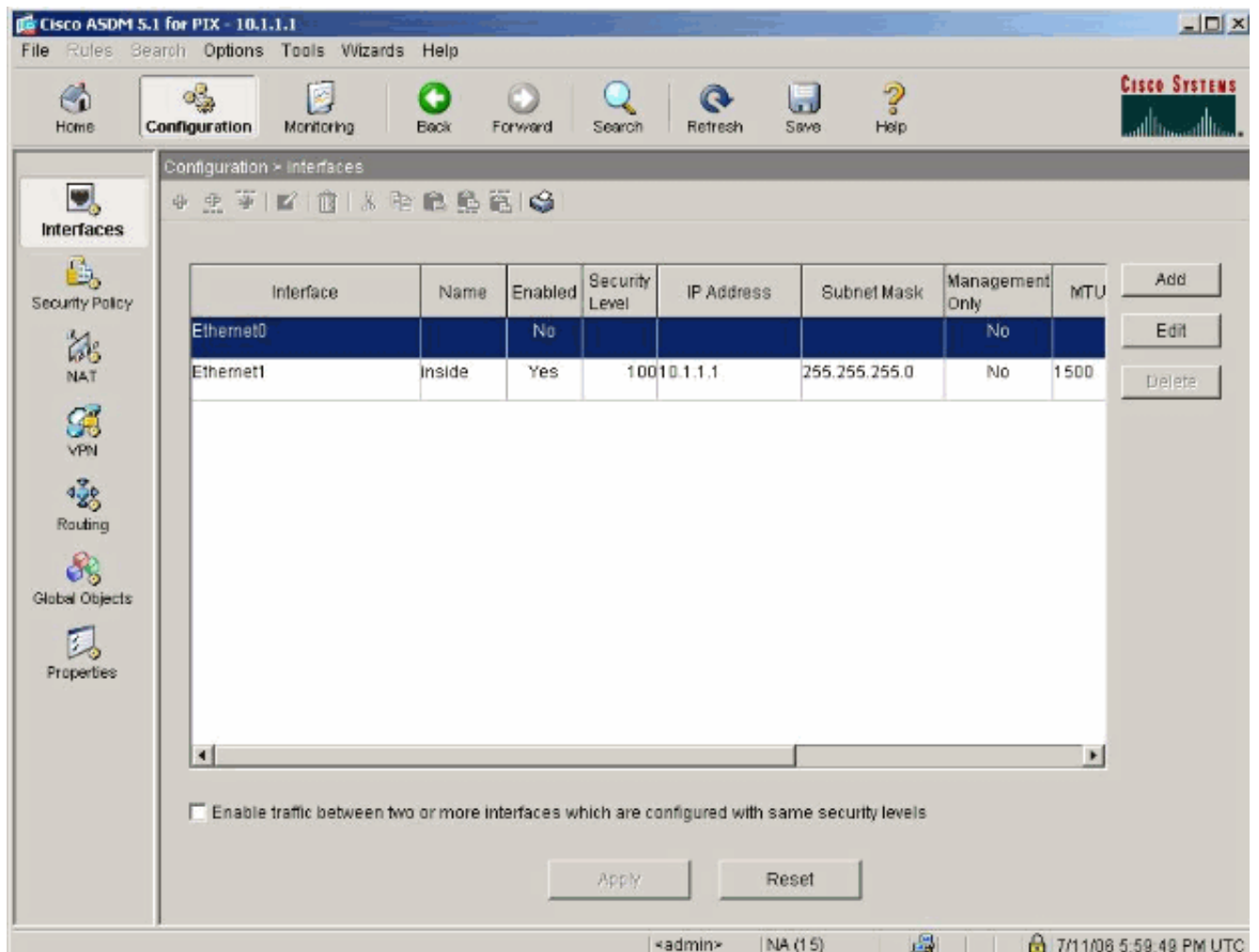
Latest ASDM Syslog Messages

-- Syslog Disabled --

Configure ASDM Syslog Filter

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

6. Elija la **interfaz** > **editan** para configurar la interfaz exterior.



7. Ingrese los detalles de la interfaz y haga clic la **AUTORIZACIÓN** cuando le hacen.

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:

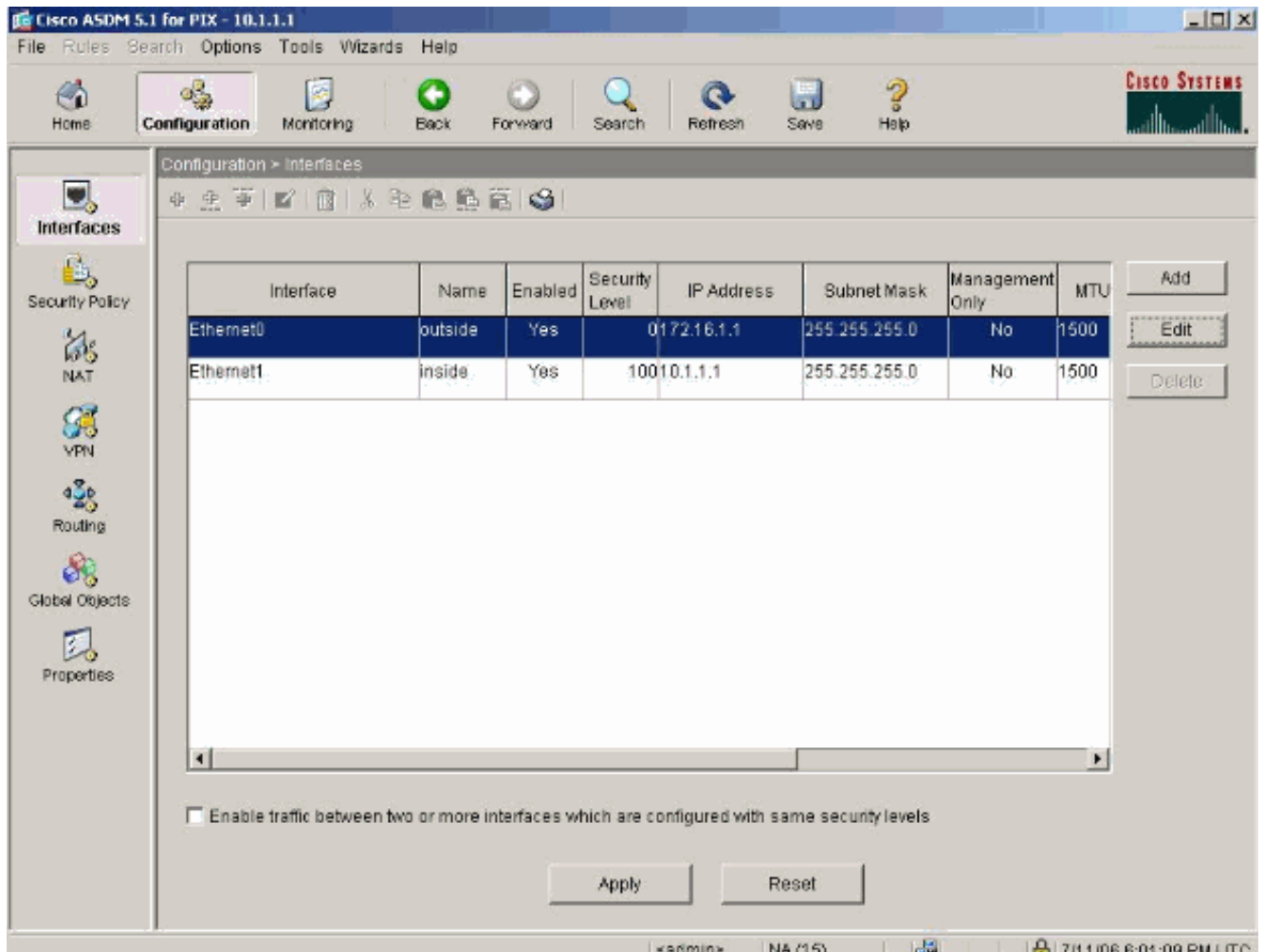
OK Cancel Help

8. Haga Click en OK en el cuadro de diálogo del cambio del nivel de seguridad.

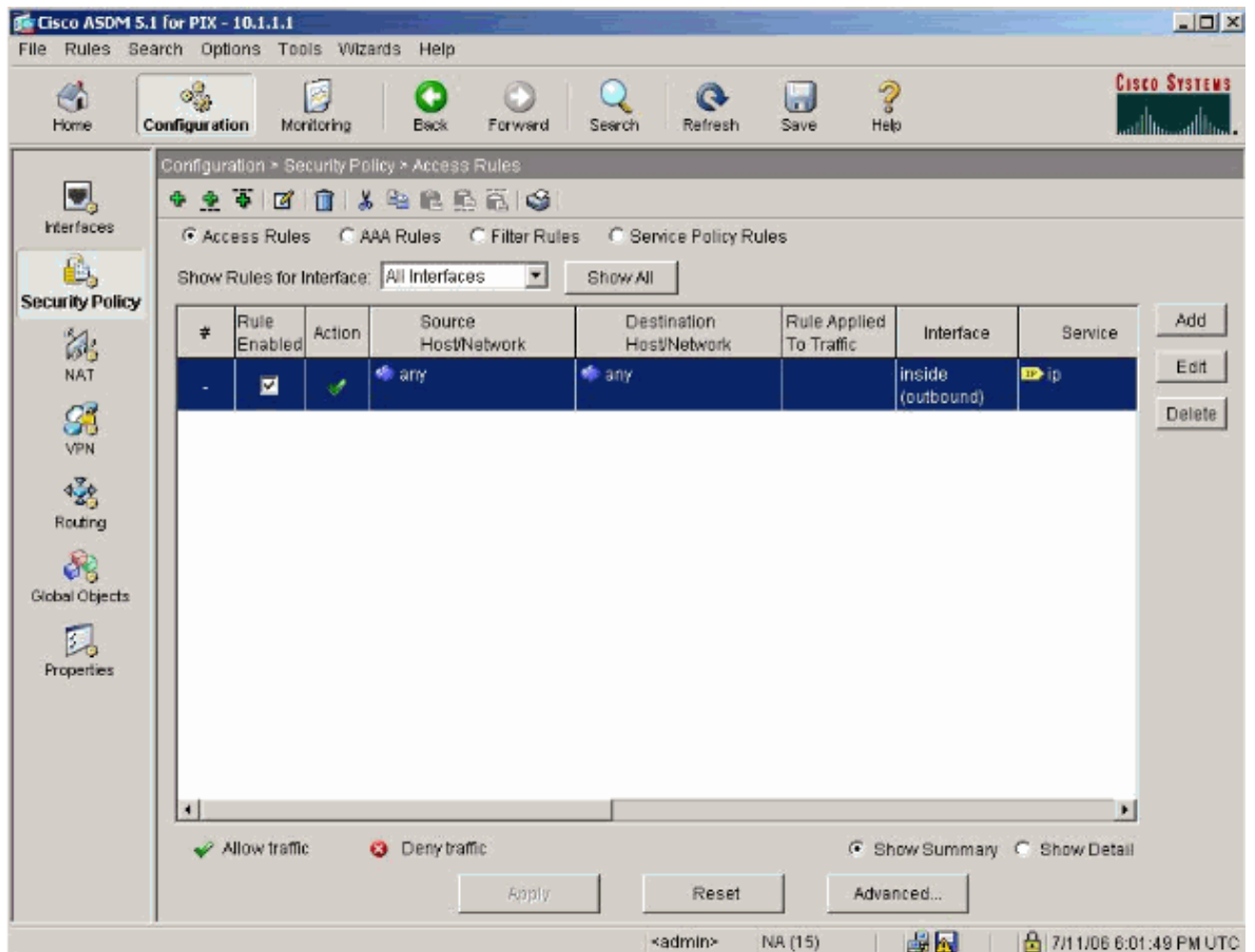
 Changing an interface's security level may cause your PIX configuration to become invalid, causing the PIX to drop legal traffic or allow illegal traffic to pass through. Do you still wish to proceed?

OK Cancel

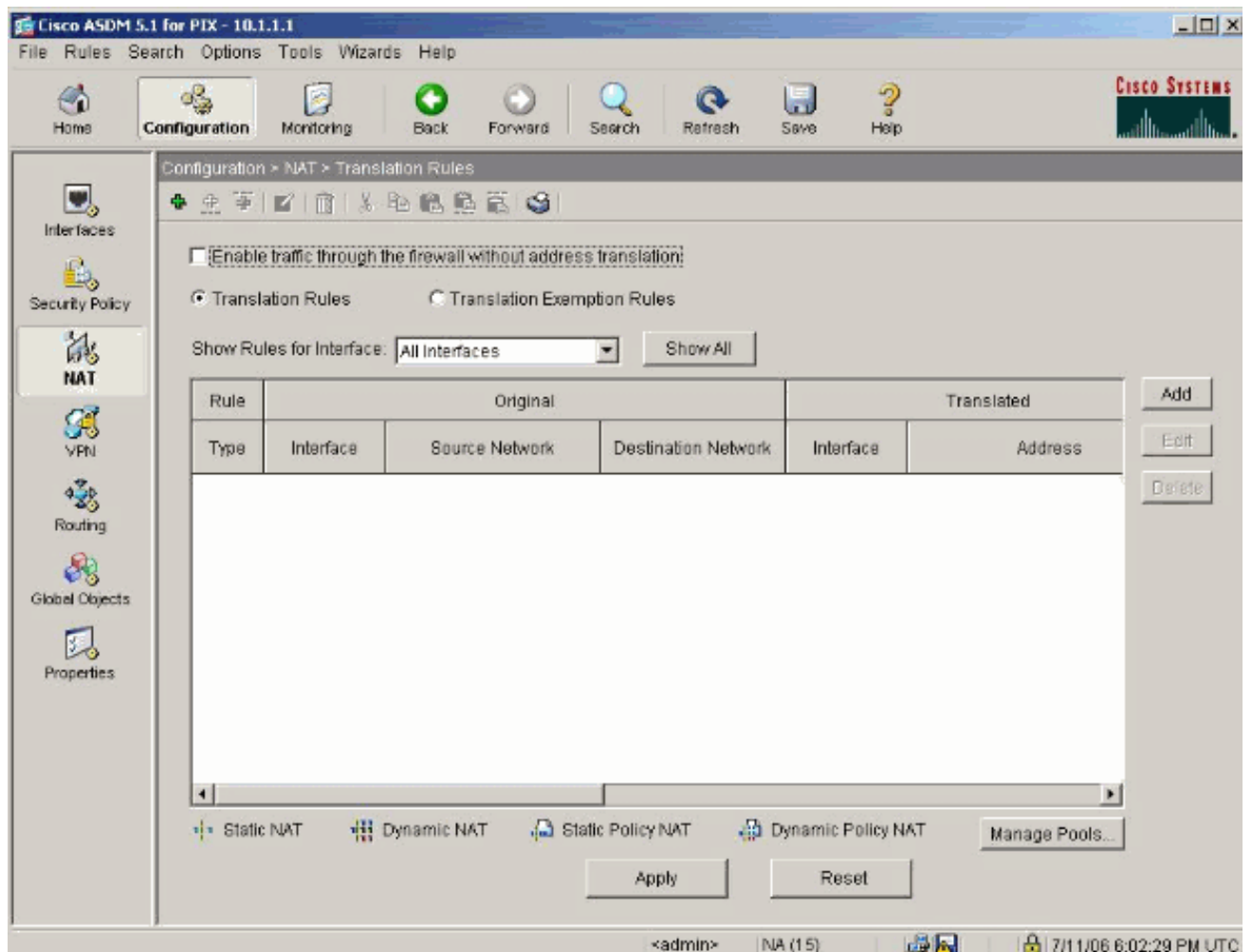
9. El teclado **se aplica** para validar la configuración de la interfaz. La configuración también consigue avanzada sobre el PIX.



10. Elija la política de seguridad en la lengüeta de las características para revisar la regla de la política de seguridad usada. En este ejemplo, se utiliza la regla interior del valor por defecto.



11. En este ejemplo, se utiliza el NAT. Desmarque el tráfico del permiso con el Firewall sin la casilla de verificación de la traducción de la dirección y el tecleo agrega para configurar la regla NAT.



12. Configure la red de origen. En este ejemplo, 10.0.0.0 se utiliza para la dirección IP, y 255.0.0.0 se utiliza para la máscara. Haga clic en **Administrar Pools** para definir las direcciones del pool NAT.

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

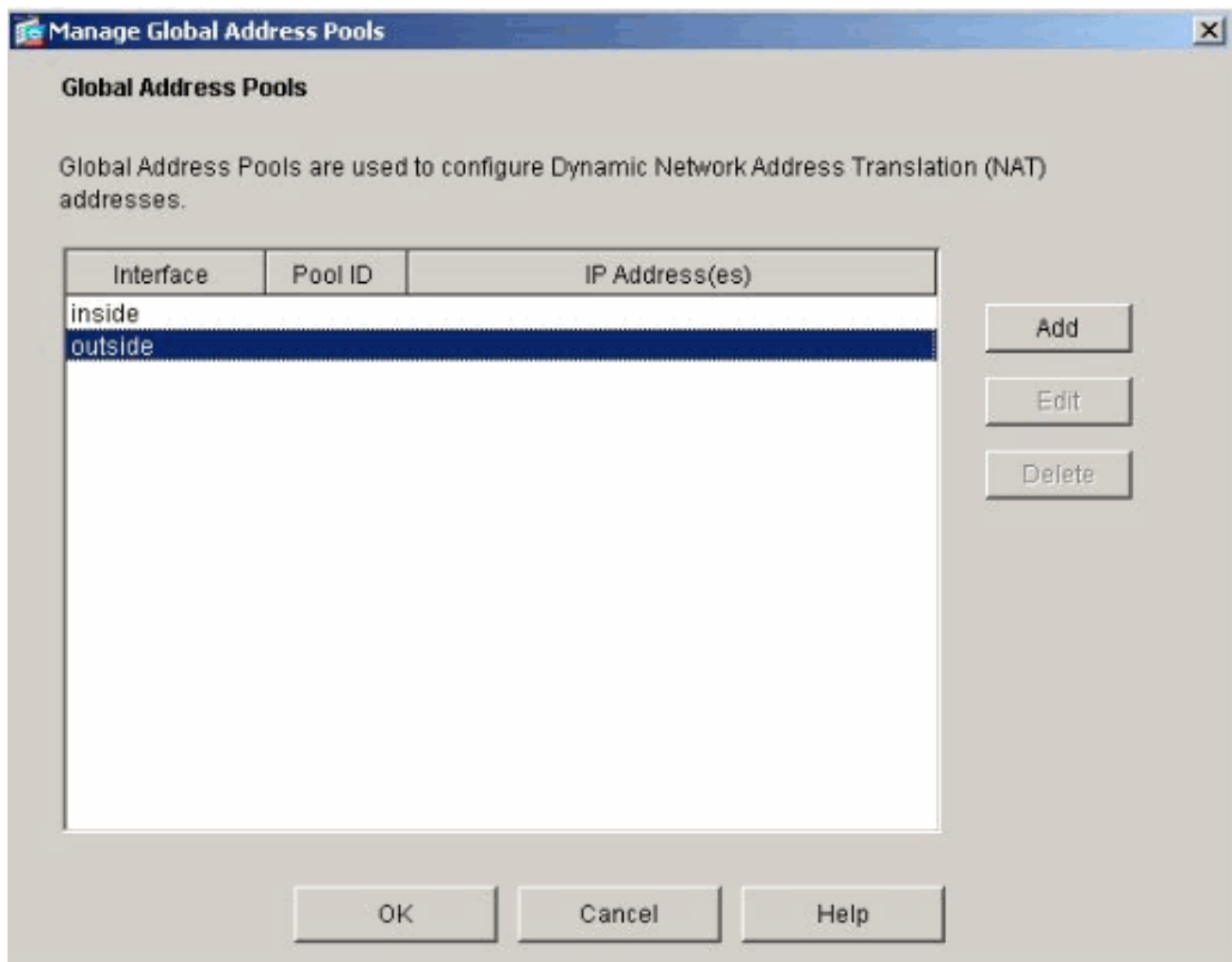
TCP Original port: Translated port:

UDP

Dynamic Address Pool:

Pool ID	Address
N/A	No address pool defined

13. Seleccione la interfaz exterior y el haga click en Add



14. En este ejemplo, se configura el pool de un rango y del PAT Address. Configure el direccionamiento del agrupamiento NAT del rango y haga clic la **AUTORIZACIÓN**.

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. Seleccione la interfaz exterior en el paso 13 para configurar el PAT Address. Haga clic en OK (Aceptar).

Add Global Pool Item

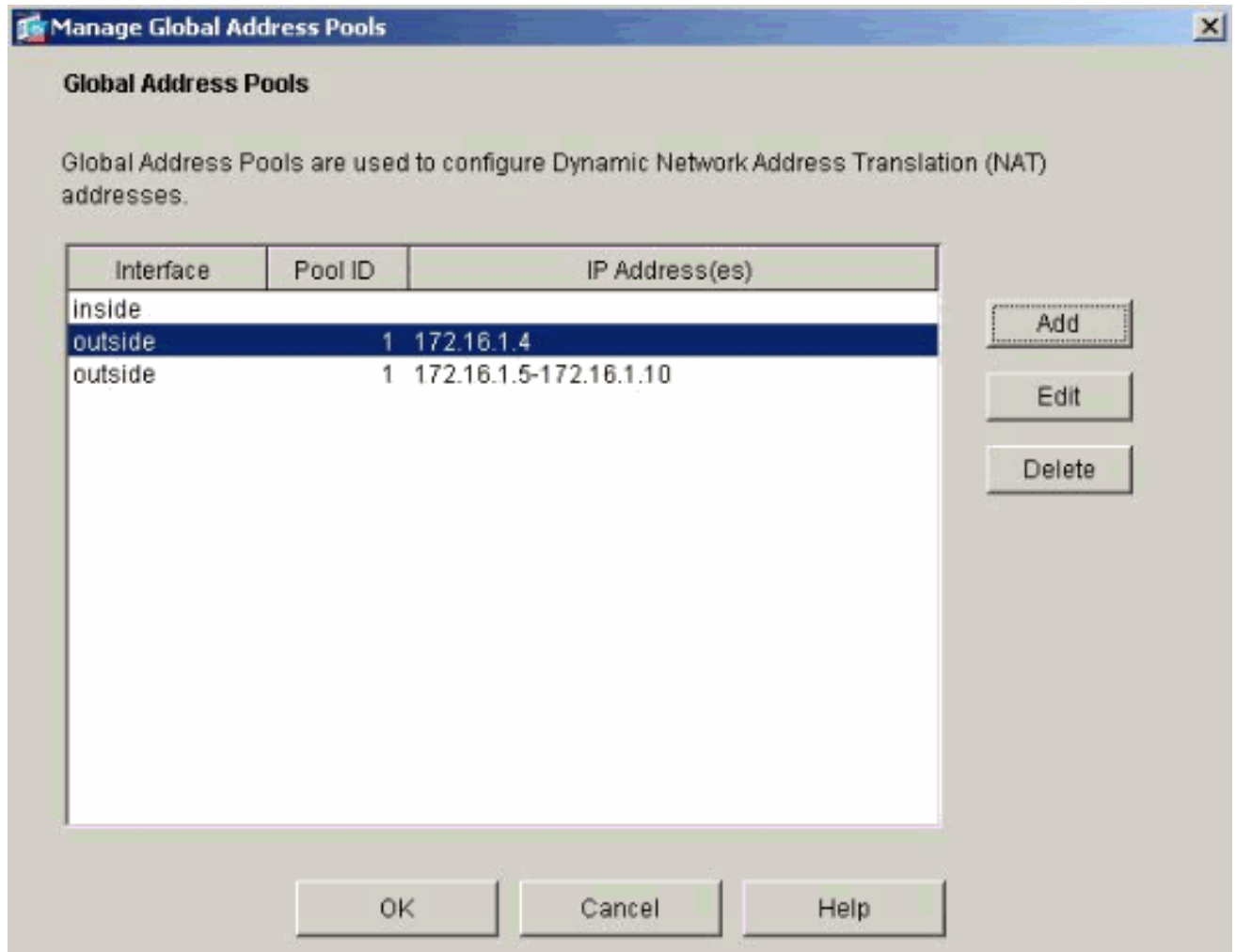
Interface: Pool ID:

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

IP Address: —

Network Mask (optional):

Haga Click en OK para continuar.



16. En la ventana de la regla de traducción de la dirección del editar, seleccione el pool ID para ser utilizado por la red de origen configurada. Haga clic en 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. El tecleo **se aplica** para avanzar la regla configurada NAT al PIX.

Configuration > NAT > Translation Rules

Enable traffic through the firewall without address translation.

Translation Rules Translation Exemption Rules

Show Rules for Interface: All Interfaces Show All

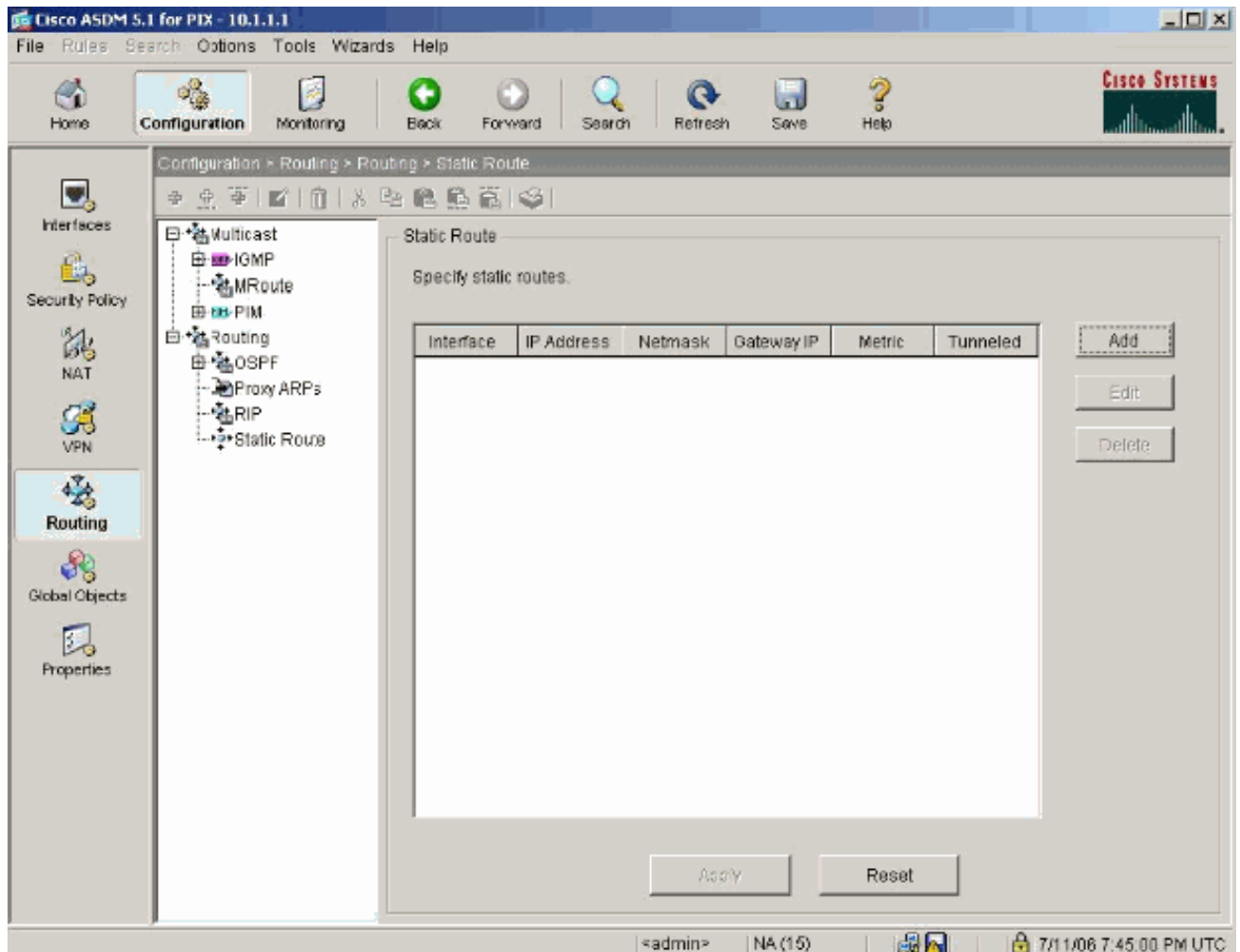
Rule	Original			Translated		Add	Edit	Delete
	Type	Interface	Source Network	Destination Network	Interface			
		inside	10.0.0.0/8	any	outside	172.16.1.4 172.16.1.5-172.16.1.10		

Static NAT Dynamic NAT Static Policy NAT Dynamic Policy NAT Manage Pools...

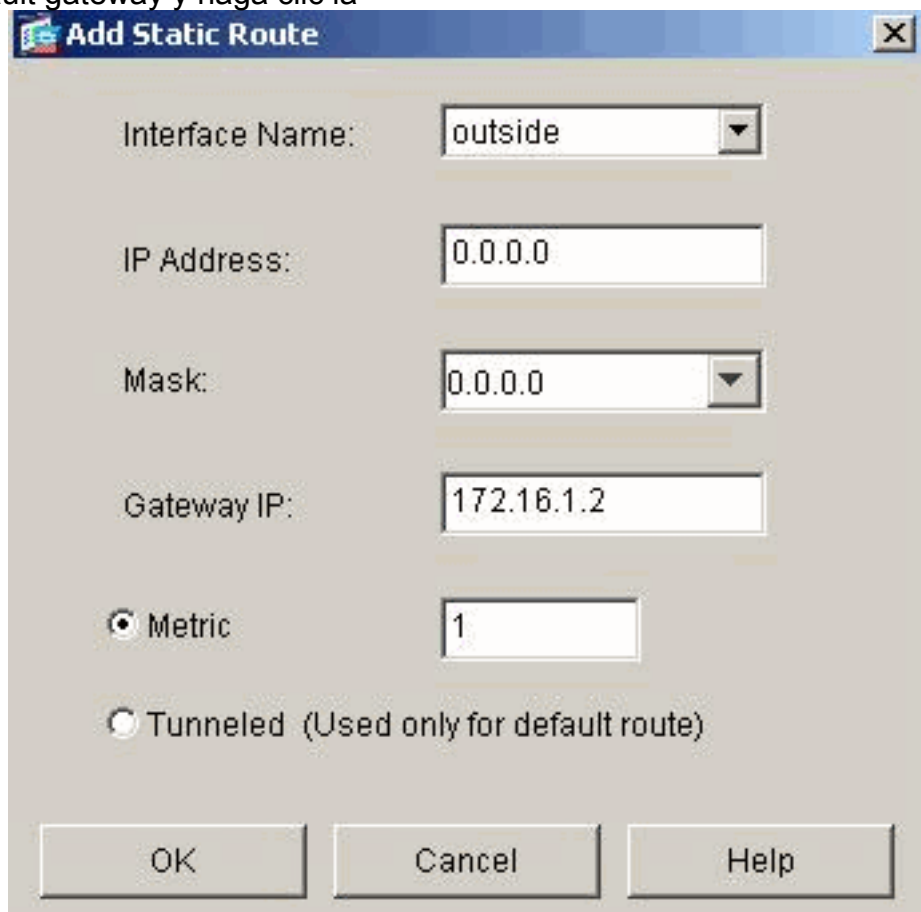
Apply Reset

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

18. En este ejemplo, se utilizan las Static rutas. La encaminamiento del tecleo, elige la **Static ruta** y el haga click en **Add**



19. Configure el default gateway y haga clic la



AUTORIZACIÓN.

20. El tecleo **agrega** y agrega las rutas a las redes

Add Static Route

Interface Name:

IP Address:

Mask:

Gateway IP:

Metric

Tunneled (Used only for default route)

OK Cancel Help

internas.

Add Static Route

Interface Name:

IP Address:

Mask:

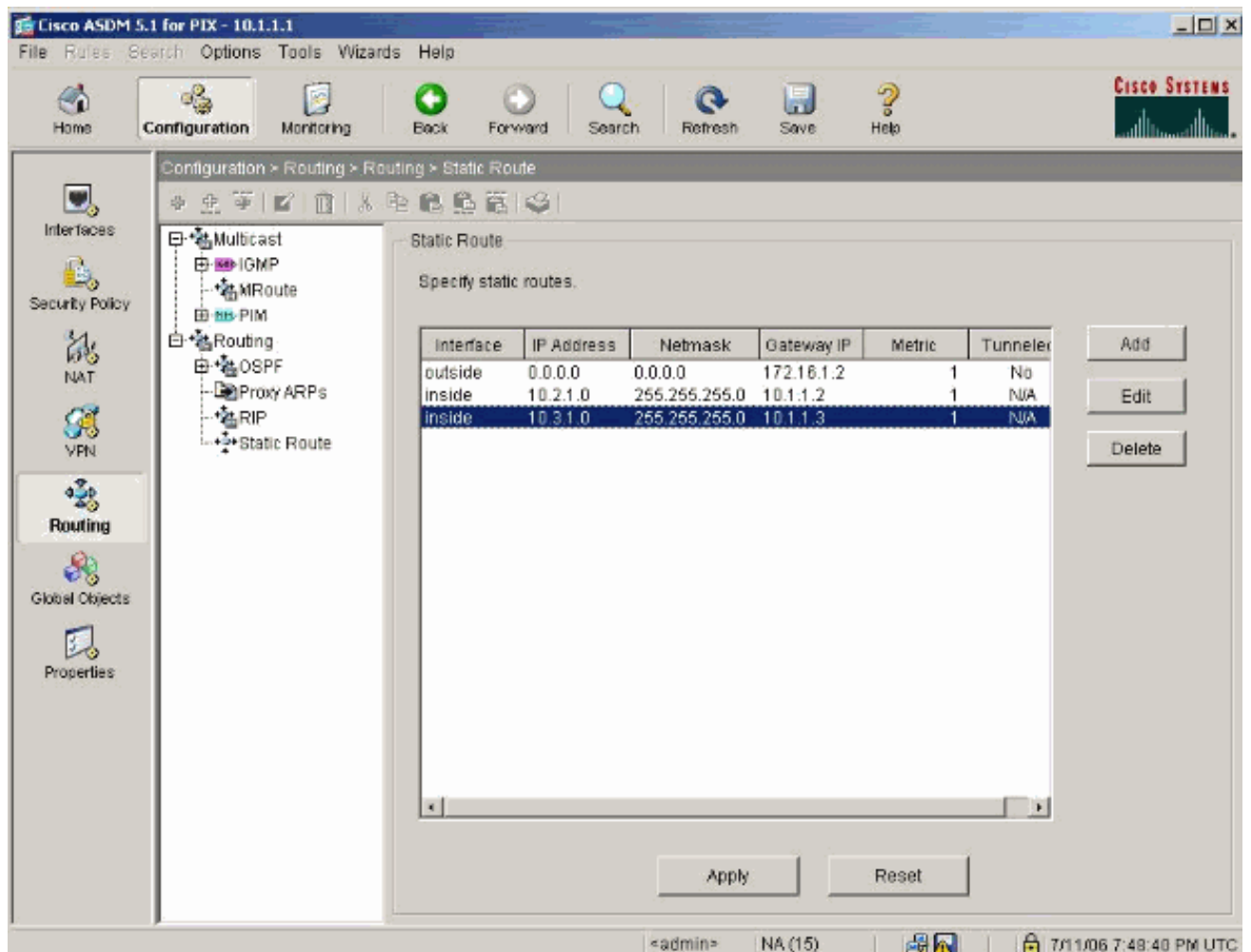
Gateway IP:

Metric

Tunneled (Used only for default route)

OK Cancel Help

21. Confirme que las rutas correctas están configuradas y el tecleo se aplica.



Configuración PIX usando el CLI

La configuración vía el ASDM GUI es completa ahora.

Usted puede ver esta configuración vía el CLI:

```

Dispositivo de seguridad CLI PIX

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
!

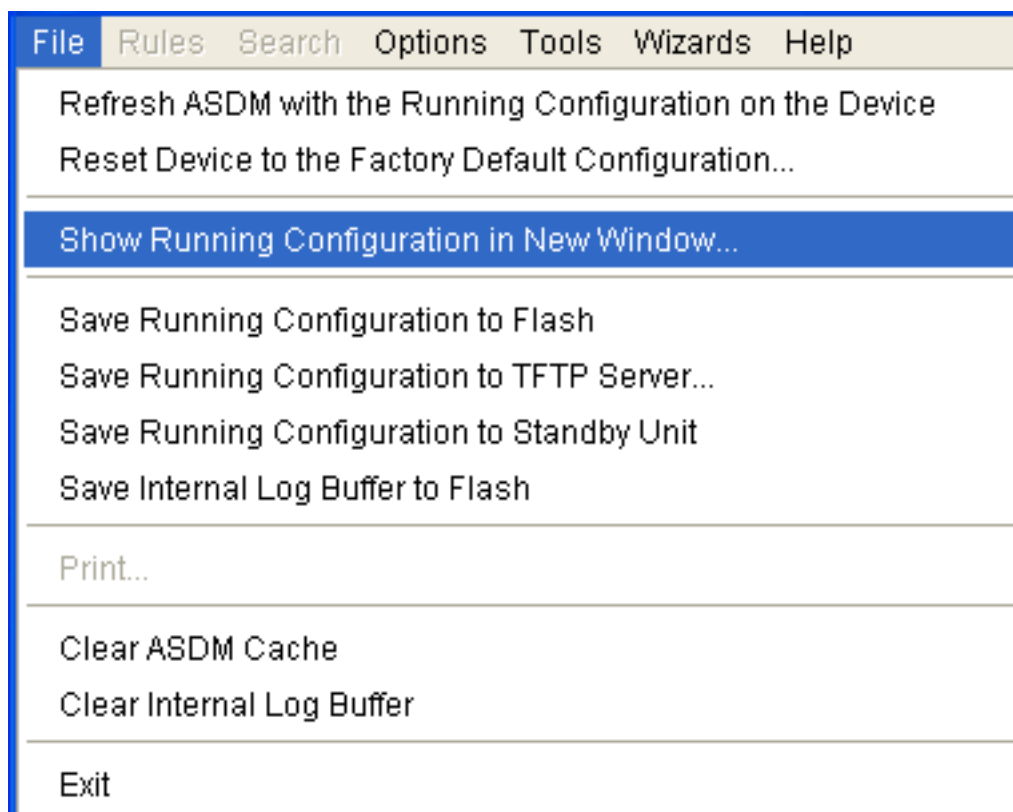
interface Ethernet1
  nameif inside
  security-level 100
  ip address 10.1.1.1 255.255.255.0
!--- Assign name and IP address to the interfaces enable
password 2KFQnbNIdI.2KYOU encrypted passwd
2KFQnbNIdI.2KYOU encrypted asdm image
flash:/asdmfile.50073 no asdm history enable arp timeout
14400 nat-control
!--- 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:a0bfff9bbaa3d815fc9fd269a3f67fef5 : end

```

Elija la configuración corriente del archivo > de la demostración en la nueva ventana para ver la configuración CLI en el ASDM.



Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshooting

Comandos para resolución de problemas

La herramienta [Output Interpreter Tool](#) (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

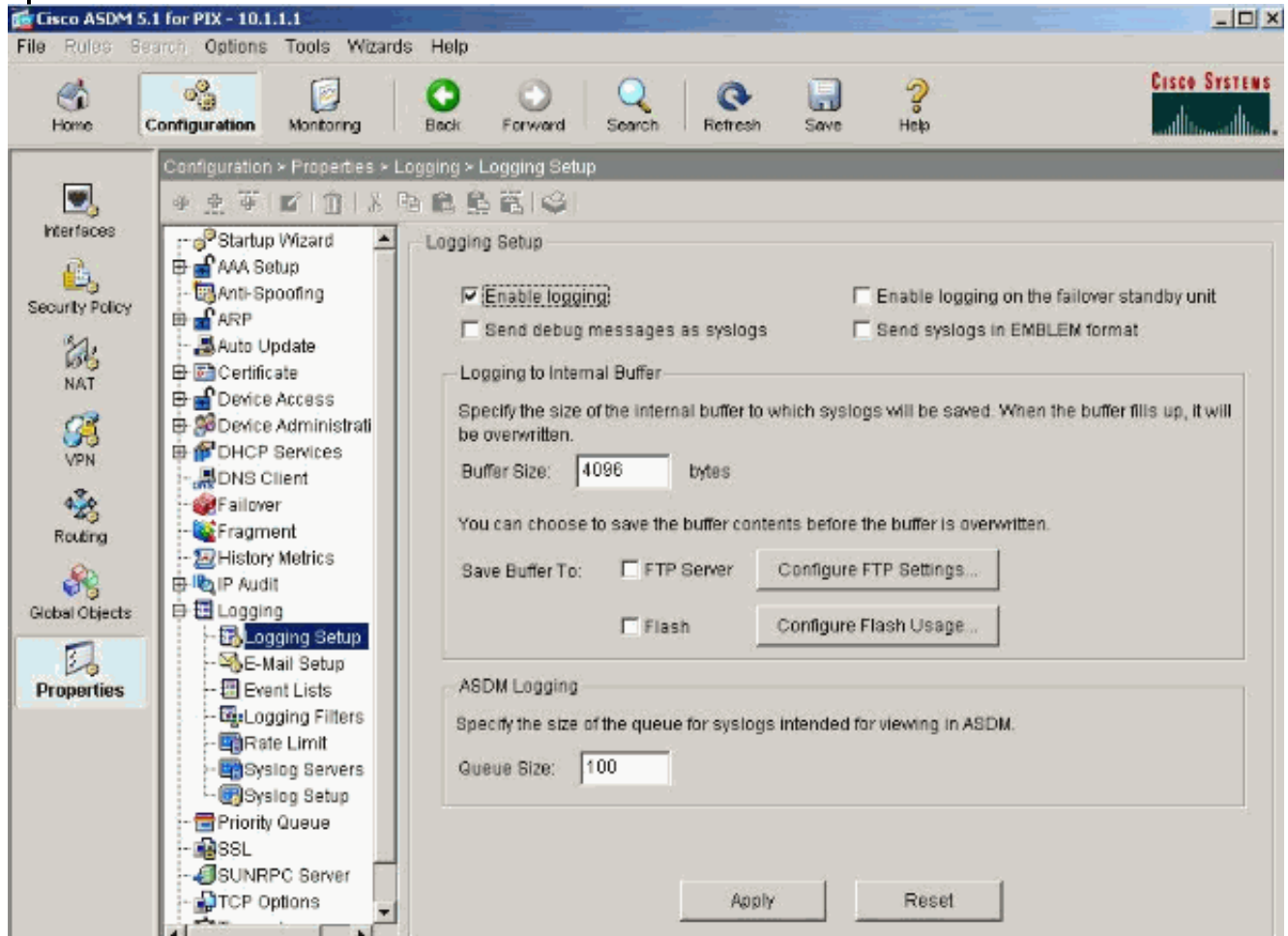
Nota: Consulte [Información Importante sobre Comandos de Debug](#) antes de usar un **comando debug**.

- debug icmp trace – Muestra si las solicitudes ICMP desde los hosts alcanzan al PIX. Para ejecutar este debug, usted necesita agregar el **comando access-list** de permitir el ICMP en su configuración.
- **debugging de memoria intermedia de registro** — Muestra las conexiones que se establecen y se niegan a los host que pasan con el PIX. La información se salva en el búfer del registro PIX y usted puede ver la salida con el **comando show log**.

Procedimiento de Troubleshooting

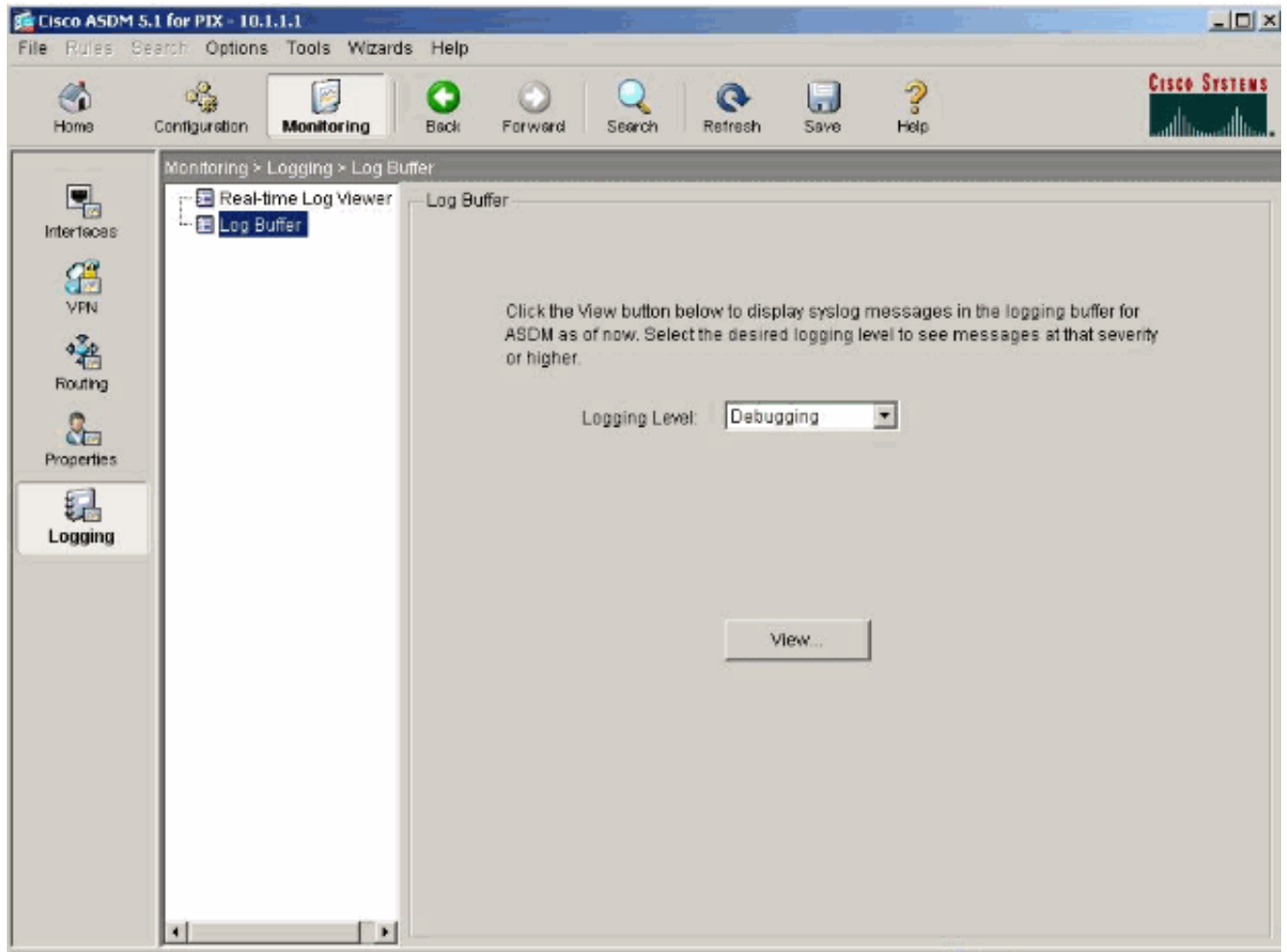
El ASDM se puede utilizar para habilitar el registro, y también para ver los registros:

1. Elija la **configuración > las propiedades > el registro > la configuración del registro**, marque el **registro del permiso**, y el tecleo se aplica.



2. Elija la **supervisión > el registro > el búfer del registro > el nivel de registro** y elija memoria

intermedia de registro de la lista desplegable. Haga clic la visión.



3. Aquí está un ejemplo del búfer del registro:

This table shows syslog messages in ASDM logging buffer as of now.

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./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

Emergencies Alerts Critical Errors Warnings Notifications Informational Debugging

[Incapaz de acceder los sitios web por nombre](#)

En ciertos escenarios, las redes internas no pueden acceder los sitios web de Internet usando el nombre (trabajos con la dirección IP) en el buscador Web. Este problema es común y ocurre generalmente si no definen al servidor DNS, especialmente en caso de que el PIX/ASA es el servidor DHCP. También, esto puede ocurrir en los casos si el PIX/ASA no puede avanzar al servidor DNS o si el servidor DNS no es accesible.

[Información Relacionada](#)

- [Dispositivos de seguridad Cisco PIX de la serie 500](#)
- [Cisco ASA 5500 Series Adaptive Security Appliances](#)
- [Referencias de Comandos de Cisco Secure PIX Firewall](#)
- [Cisco Adaptive Security Device Manager](#)
- [Alertas y Troubleshooting de Cisco Adaptive Security Device Manager \(ASDM\)](#)
- [Solicitudes de Comentarios \(RFC\)](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)