Exemplo de configuração de PIX/ASA como servidor DHCP e cliente

Contents

Introdução

O PIX 500 Series Security Appliance e o Cisco Adaptive Security Appliance (ASA) suportam a operação como servidores de Dynamic Host Configuration Protocol (DHCP) e clientes DHCP. O DHCP é um protocolo que fornece aos hosts parâmetros de configuração automática, como um endereço IP com uma máscara de sub-rede, gateway padrão, servidor DNS e endereço IP do servidor WINS.

O Security Appliance pode atuar como um servidor DHCP ou um cliente DHCP. Quando ele opera como um servidor, o Security Appliance fornece parâmetros de configuração de rede diretamente aos clientes DHCP. Quando ele opera como um cliente DHCP, o Security Appliance solicita esses parâmetros de configuração de um servidor DHCP.

Este documento concentra-se em como configurar o servidor DHCP e o cliente DHCP usando o Cisco Adaptive Security Device Manager (ASDM) no Security Appliance.

Pré-requisitos

Requisitos

Este documento pressupõe que o PIX Security Appliance ou ASA esteja totalmente operacional e configurado para permitir que o Cisco ASDM faça alterações de configuração.

Observação: consulte Permitindo o Acesso HTTPS para o ASDM para permitir que o dispositivo seja configurado pelo ASDM.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- PIX 500 Series Security Appliance 7.x

  Observação: a configuração do PIX CLI usada na versão 7.x também se aplica ao PIX 6.x. A única diferença é que em versões anteriores ao PIX 6.3, o servidor DHCP só pode ser ativado na interface interna. No PIX 6.3 e posterior, o servidor DHCP pode ser ativado em qualquer uma das interfaces disponíveis. Nessa configuração, a interface externa é usada para o recurso do servidor DHCP.

- ASDM 5.x

  Observação: o ASDM suporta apenas o PIX 7.0 e posterior. O PIX Device Manager (PDM) está disponível para configurar o PIX versão 6.x. Consulte Compatibilidade de Hardware e Software do Cisco ASA 5500 Series e do PIX 500 Series Security Appliance para obter mais informações.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Produtos Relacionados

Essa configuração também pode ser usada com o Cisco ASA 7.x.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Configurar

Nesta configuração, há dois PIX Security Appliances que executam a versão 7.x. Um funciona como um servidor DHCP que fornece parâmetros de configuração para outro PIX Security Appliance 7.x que funciona como um cliente DHCP. Quando funciona como um servidor DHCP, o PIX atribui dinamicamente endereços IP a clientes DHCP a partir de um pool de endereços IP designados.

Você pode configurar um servidor DHCP em cada interface do Security Appliance. Cada interface

pode ter seu próprio pool de endereços a partir do qual desenhar. No entanto, as outras configurações de DHCP, como servidores DNS, nome de domínio, opções, tempo limite de ping e servidores WINS, são configuradas globalmente e usadas pelo servidor DHCP em todas as interfaces.

Você não pode configurar um cliente DHCP ou serviços de retransmissão DHCP em uma interface na qual o servidor está habilitado. Além disso, os clientes DHCP devem ser conectados diretamente à interface na qual o servidor está habilitado.

Finalmente, enquanto o servidor DHCP estiver habilitado em uma interface, você não poderá alterar o endereço IP dessa interface.

Observação: Basicamente, não há opção de configuração para definir o endereço de gateway padrão na resposta DHCP enviada do servidor DHCP (PIX/ASA). O servidor DHCP sempre envia seu próprio endereço como gateway para o cliente DHCP. No entanto, definir uma rota padrão que aponte para o roteador de Internet permite que o usuário acesse a Internet.

Observação: o número de endereços de pool de DHCP que podem ser atribuídos depende da licença usada no Security Appliance (PIX/ASA). Se você usar a licença Base/Security Plus, esses limites se aplicarão ao pool DHCP. Se o limite de hosts for 10 hosts, você limitará o pool DHCP a 32 endereços. Se o limite de hosts for 50 hosts, você limitará o pool DHCP a 128 endereços. Se o limite de hosts for ilimitado, você limitará o pool DHCP a 256 endereços. Assim, o pool de endereços é limitado com base no número de Hosts.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

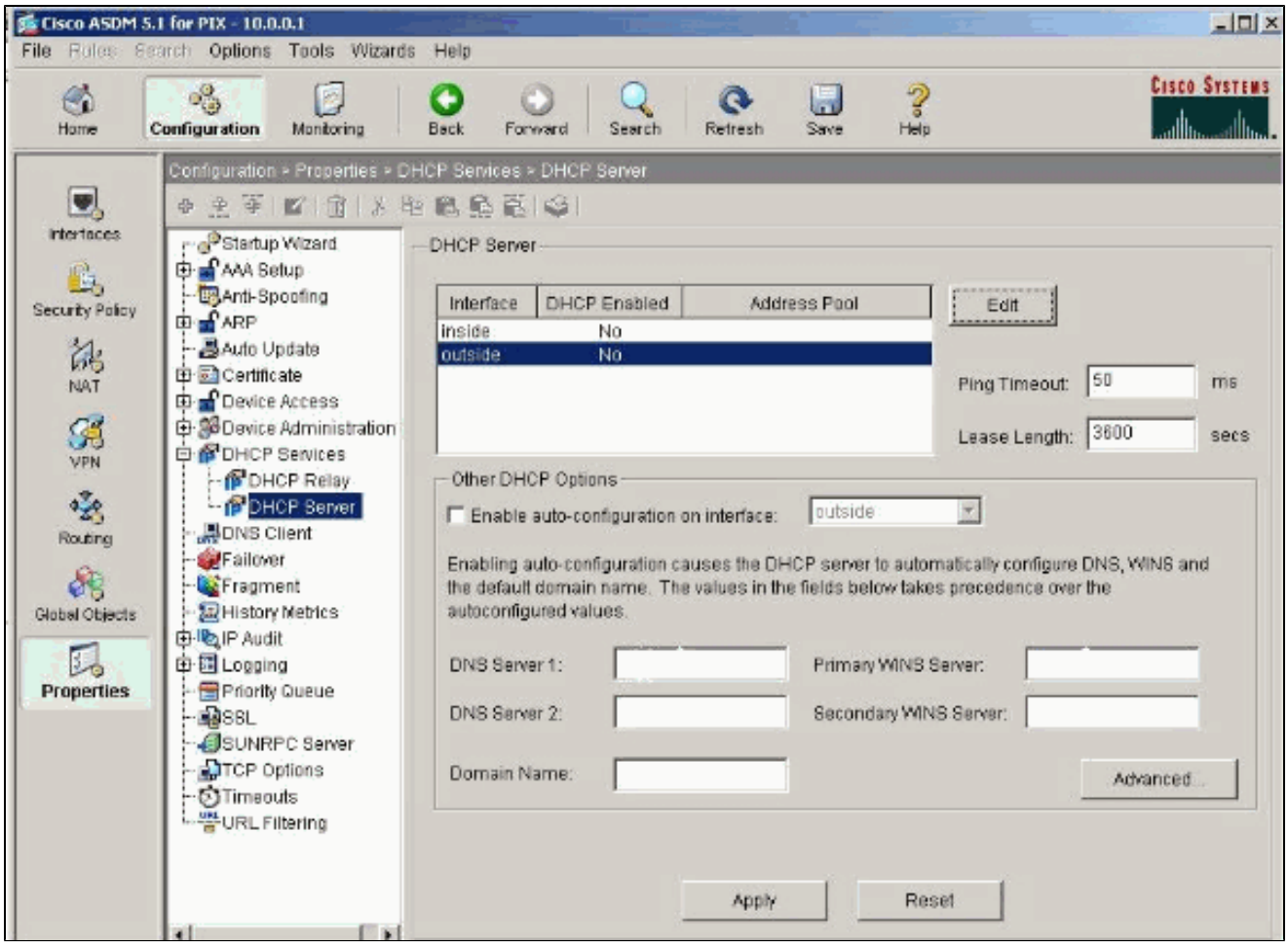
Este documento utiliza as seguintes configurações:

Configuração do servidor DHCP usando ASDM

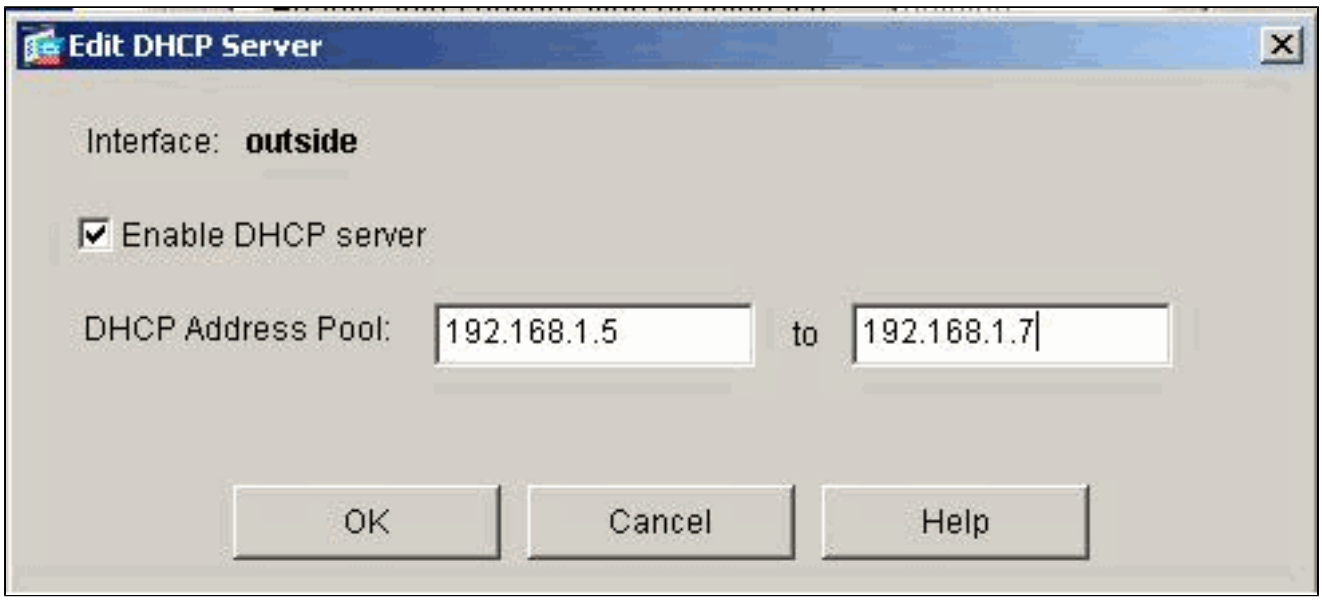
Conclua estas etapas para configurar o PIX Security Appliance ou ASA como um servidor DHCP usando o ASDM.

1. Escolha Configuration > Properties > DHCP Services > DHCP Server na janela Home. Selecione uma interface e clique em Edit para ativar o servidor DHCP e criar um pool de endereços DHCP.

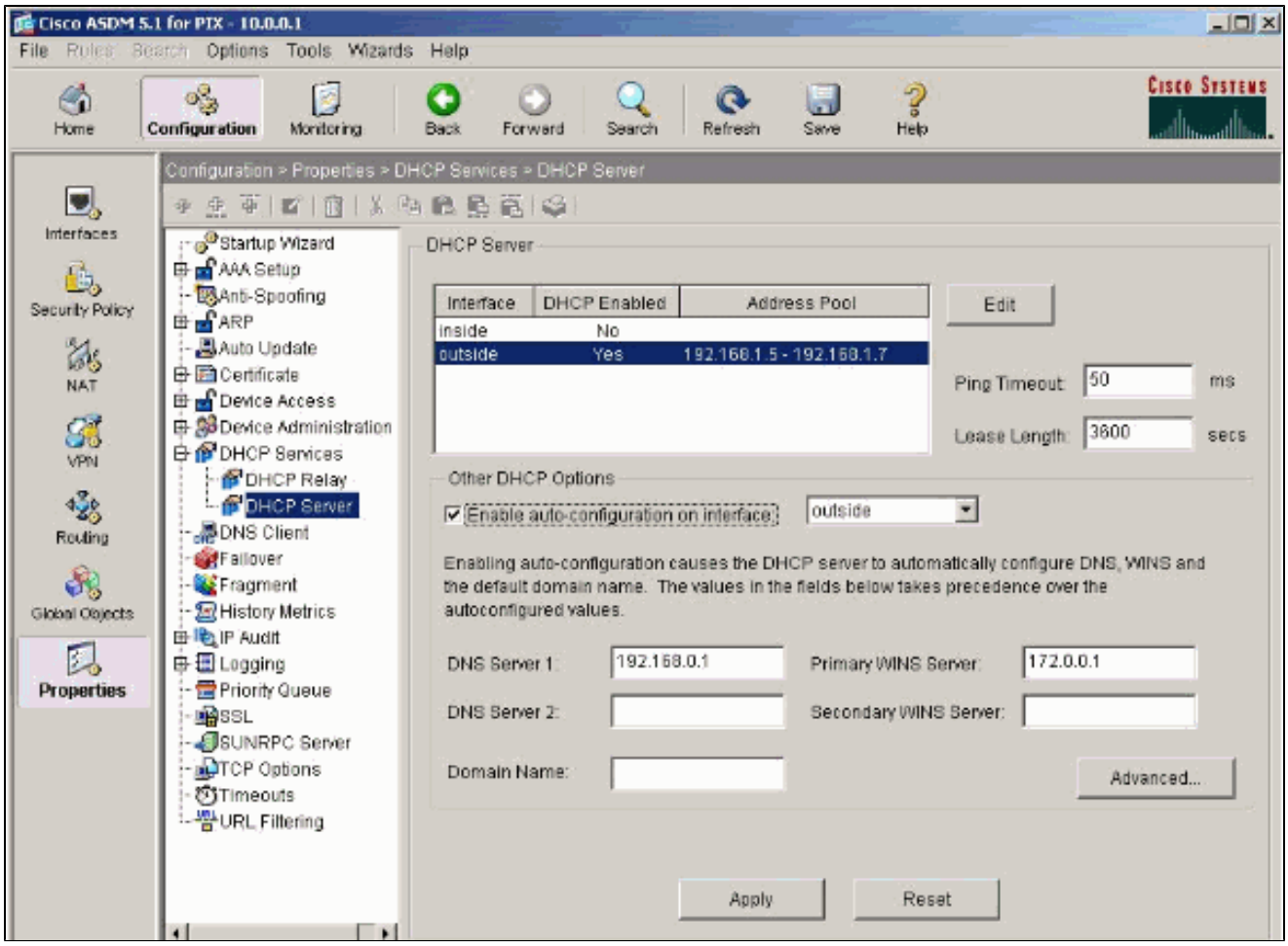
   O pool de endereços deve estar na mesma sub-rede da interface do Security Appliance. Neste exemplo, o servidor DHCP é configurado na interface externa do PIX Security Appliance.



2. Marque Enable DHCP server na interface externa para ouvir as solicitações dos clientes DHCP. Forneça o pool de endereços a serem emitidos para o cliente DHCP e clique em OK para retornar à janela principal.



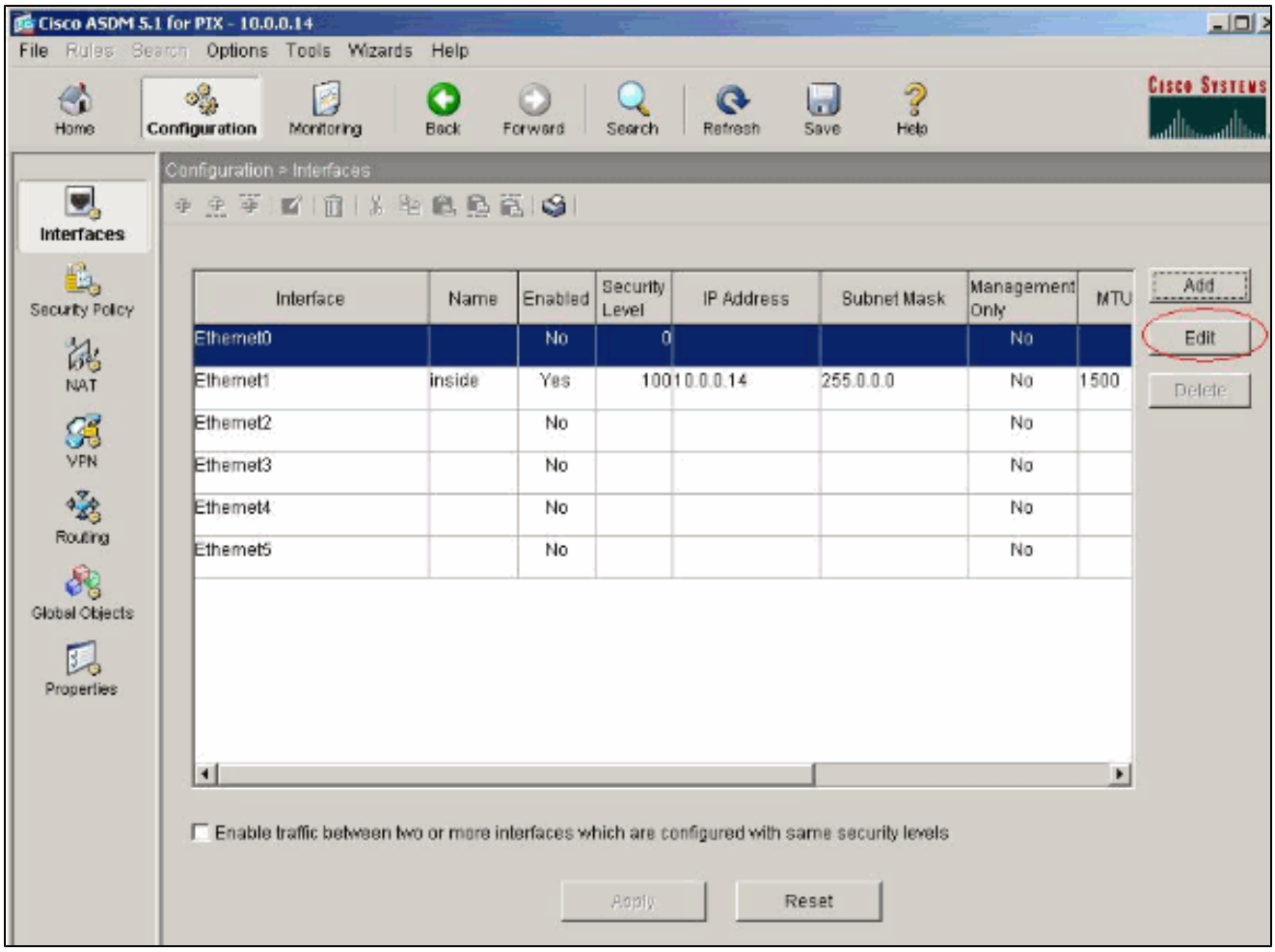
3. Marque Enable autoconfiguration na interface para fazer com que o servidor DHCP configure automaticamente o DNS, o WINS e o Domain Name padrão para o cliente DHCP. Clique em Aplicar para atualizar a configuração atual do Security Appliance.



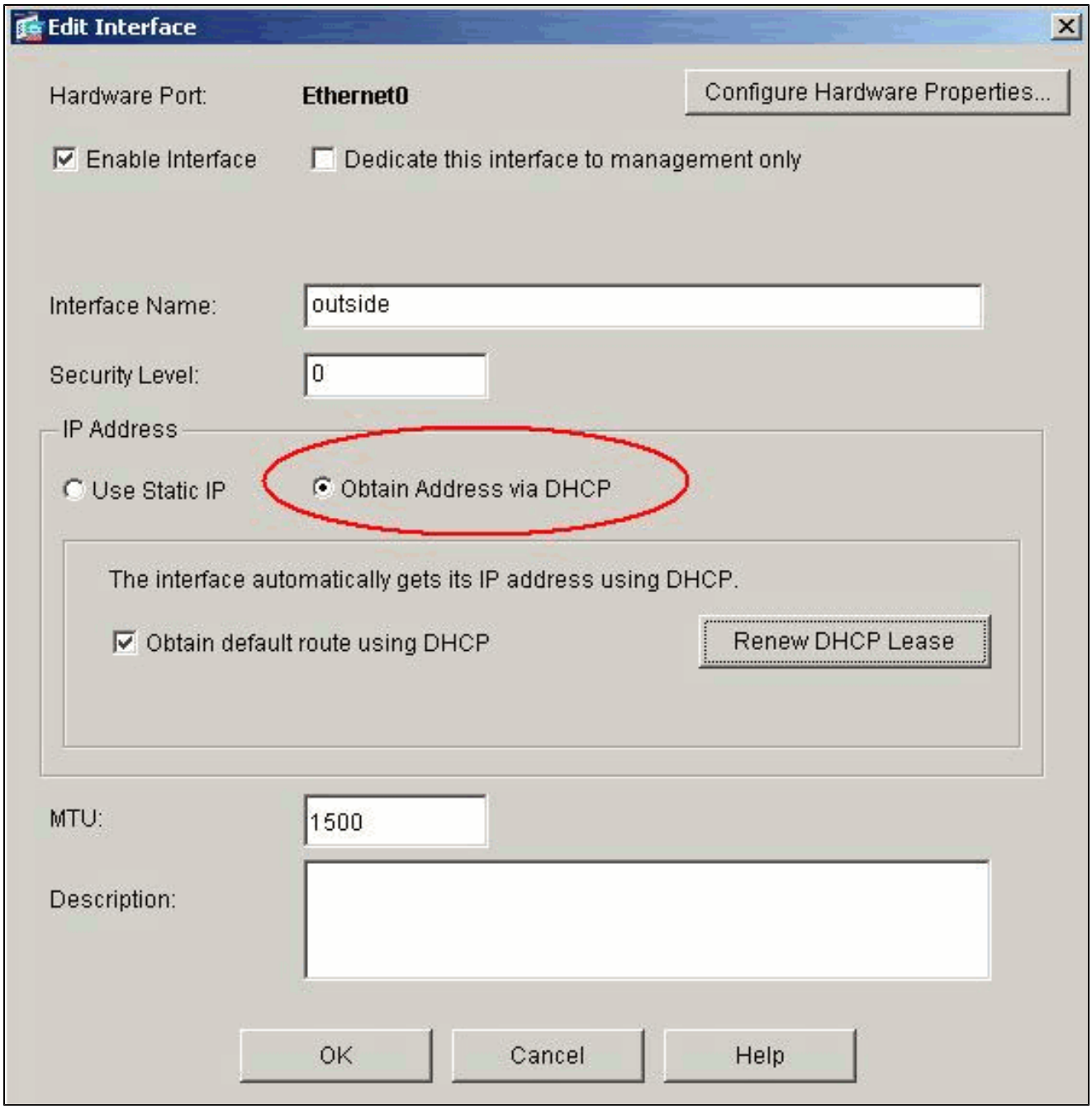
Configuração do cliente DHCP usando ASDM

Conclua estas etapas para configurar o PIX Security Appliance como um cliente DHCP usando o ASDM.

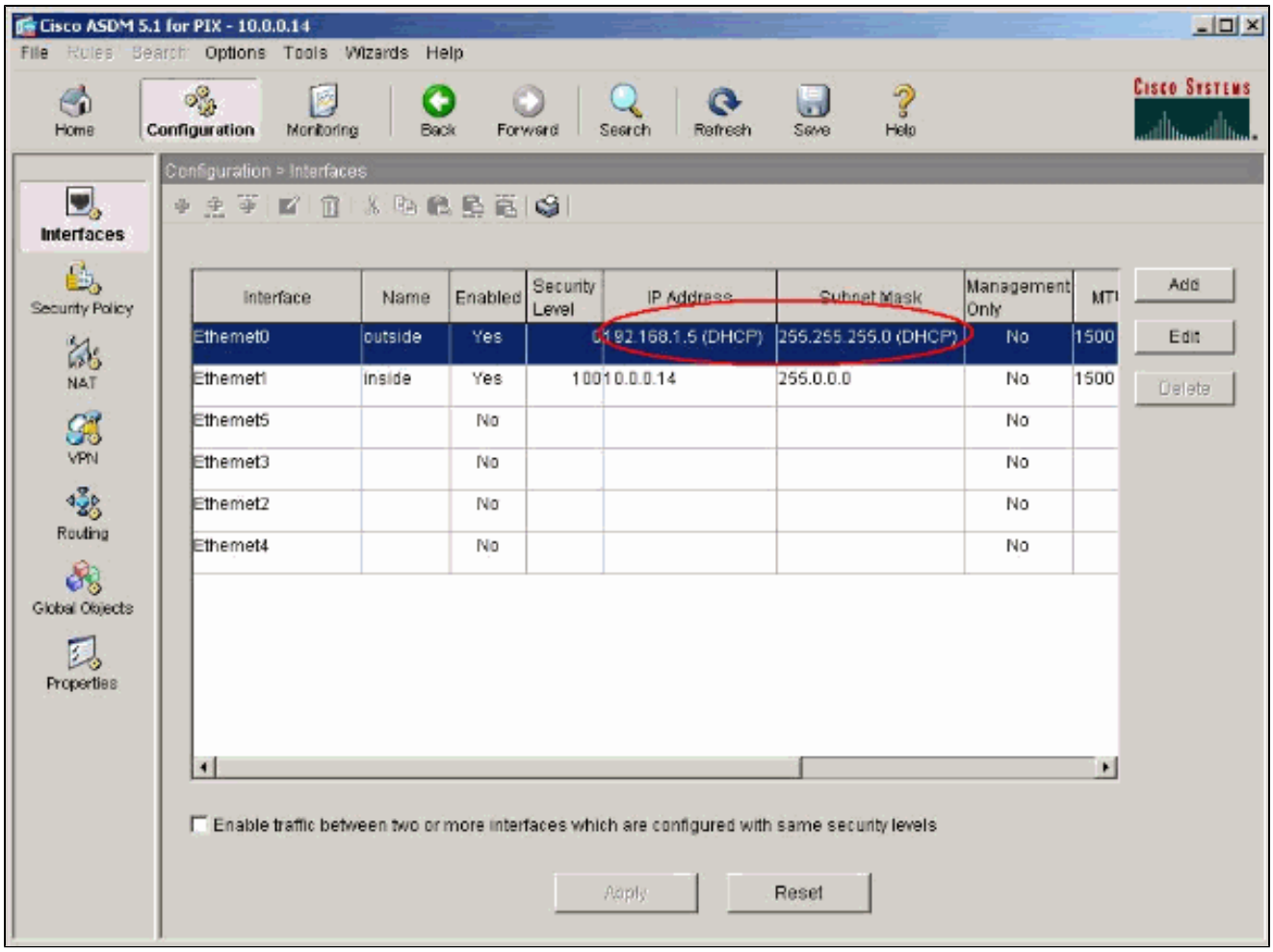
1. Escolha Configuration > Interfaces e clique em Edit para permitir que a interface Ethernet0 obtenha os parâmetros de configuração como um endereço IP com uma máscara de sub-rede, gateway padrão, servidor DNS e endereço IP do servidor WINS do servidor DHCP.



2. Marque Enable Interface e insira o nome da interface e o nível de segurança da interface. Escolha Obtain address via DHCP para o endereço IP e Obtain default route using DHCP para o gateway padrão e, em seguida, clique em OK para ir para a janela Main.



3. Clique em Apply para ver o endereço IP obtido para a interface Ethernet0 do servidor DHCP.



Configuração do servidor DHCP

Esta configuração é criada pelo ASDM:

```
<#root>

pixfirewall#

show running-config


PIX Version 7.1(1)
!
hostname pixfirewall
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 192.168.1.1 255.255.255.0
!
interface Ethernet1
 nameif inside
```

```
 security-level 100
 ip address 10.0.0.1 255.0.0.0
!

!--- Output is suppressed.



logging enable
logging asdm informational
mtu inside 1500
mtu outside 1500
no failover

asdm image flash:/asdm-511.bin

http server enable
http 10.0.0.0 255.0.0.0 inside

no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
telnet timeout 5
ssh timeout 5
console timeout 0


!--- Specifies a DHCP address pool and the interface for the client to connect.


dhcpd address 192.168.1.5-192.168.1.7 outside



!--- Specifies the IP address(es) of the DNS and WINS server !--- that the client uses.


dhcpd dns 192.168.0.1
dhcpd wins 172.0.0.1



!--- Specifies the lease length to be granted to the client. !--- This lease equals the amount of time


dhcpd lease 3600

dhcpd ping_timeout 50
dhcpd auto_config outside


!--- Enables the DHCP daemon within the Security Appliance to listen for !--- DHCP client requests on


dhcpd enable outside

dhcprelay timeout 60
!

!--- Output is suppressed.
```

```
service-policy global_policy global
Cryptochecksum:7a8cd028ee1c56083b64237c832fb5ab
: end
```

Configuração do cliente DHCP

Esta configuração é criada pelo ASDM:

Cliente DHCP

```
<#root>

pixfirewall#

show running-config


PIX Version 7.1(1)
!
hostname pixfirewall
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0
 nameif outside
 security-level 0


!--- Configures the Security Appliance interface as a DHCP client. !--- The

setroute

 keyword causes the Security Appliance to set the default !--- route using the default gateway the DHCI




ip address dhcp setroute


!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 10.0.0.14 255.0.0.0


!--- Output is suppressed.



!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name default.domain.invalid
pager lines 24
```

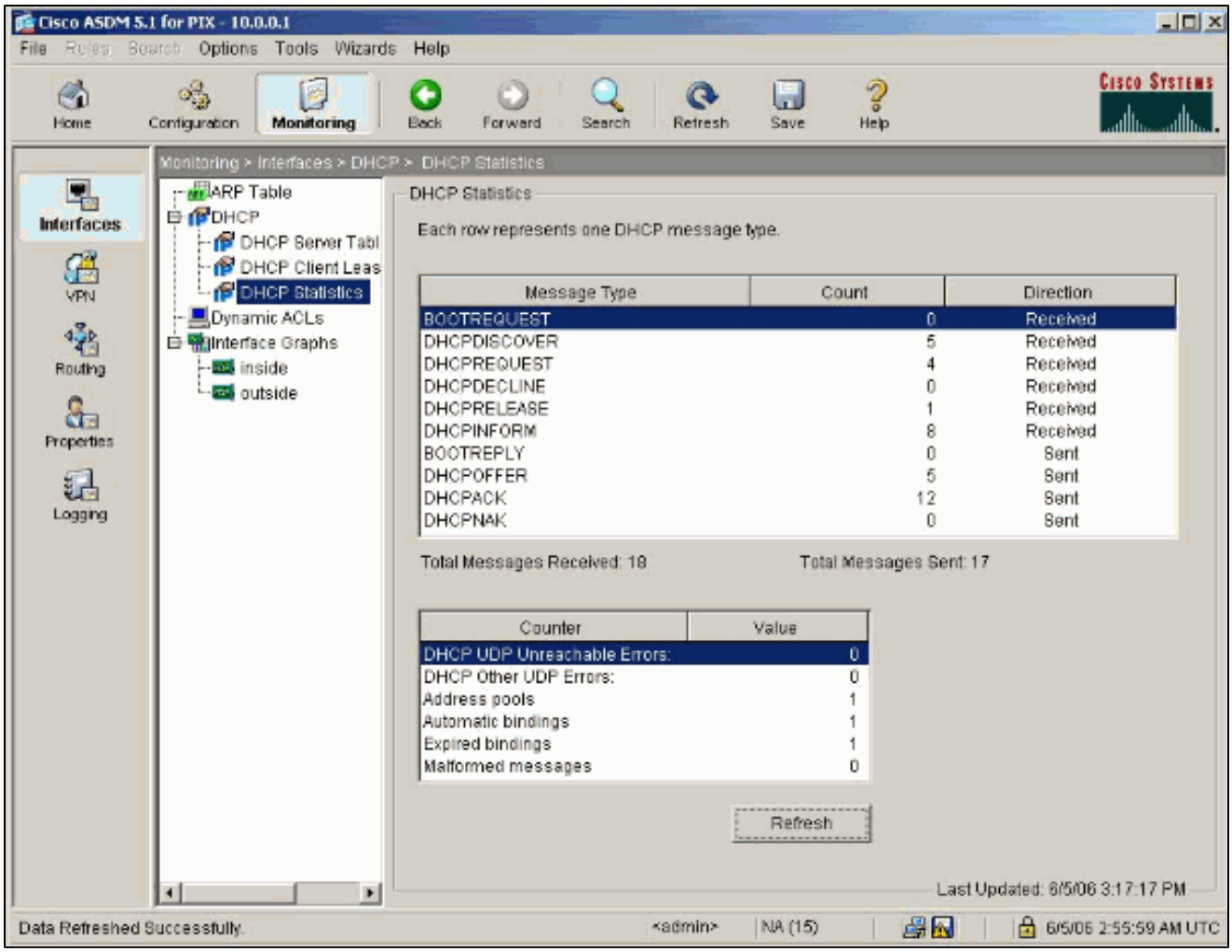
```
logging enable
logging console debugging
logging asdm informational
mtu outside 1500
mtu inside 1500
no failover

asdm image flash:/asdm-511.bin

no asdm history enable
arp timeout 14400
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
http server enable
http 10.0.0.0 255.0.0.0 inside


!--- Output is suppressed.


!
service-policy global_policy global
Cryptochecksum:86dd1153e8f14214524359a5148a4989
: end
```

Verificar

Conclua estas etapas para verificar as estatísticas do DHCP e as informações de vinculação do servidor DHCP e do cliente DHCP usando o ASDM.

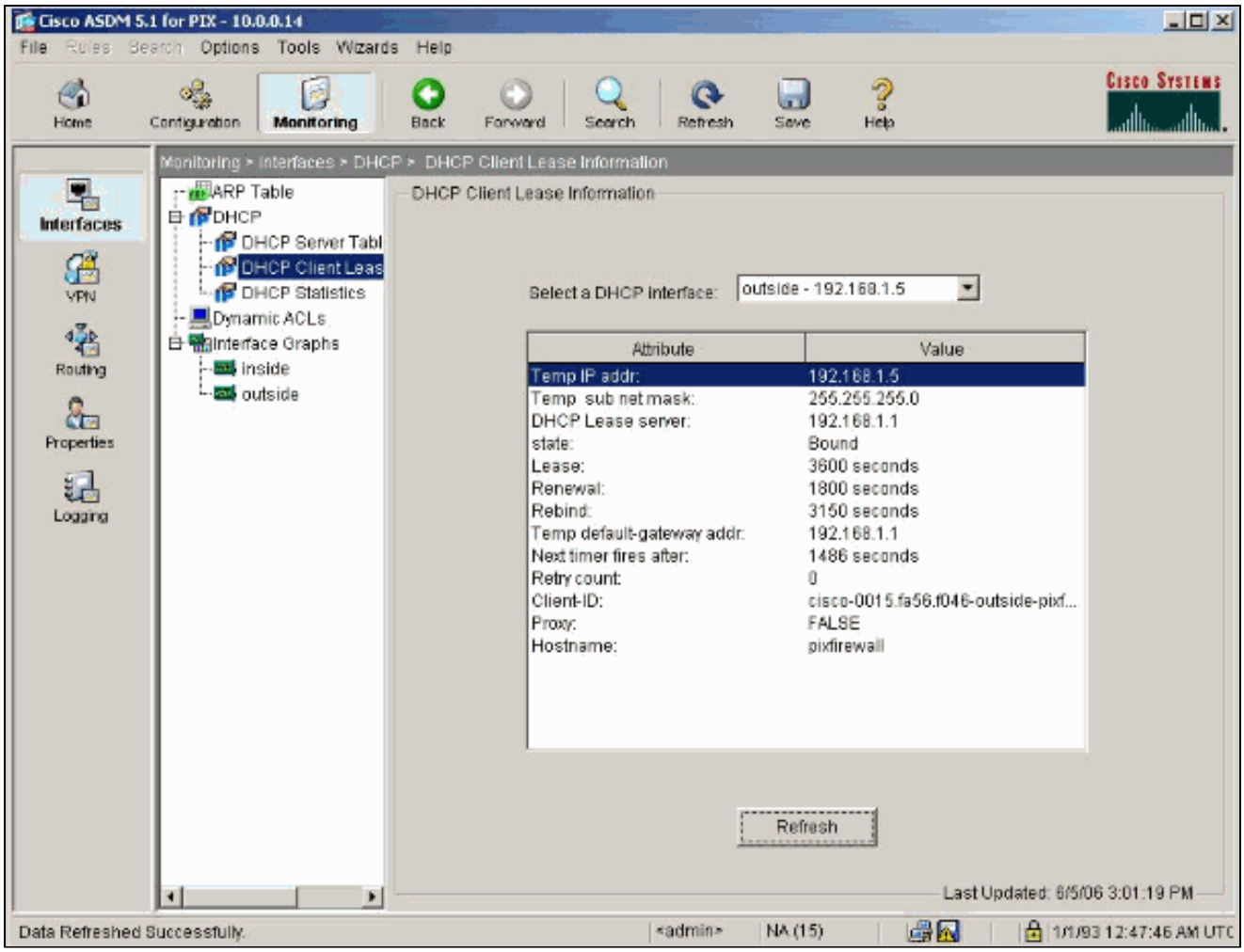
1. Escolha Monitoring > Interfaces > DHCP > DHCP Statistics no servidor DHCP para verificar as estatísticas do DHCP, como DHCPDISCOVER, DHCPREQUEST, DHCPOFFER e DHCPACK.

   Insira o comando show dhcpd statistics na CLI para exibir as estatísticas do DHCP.

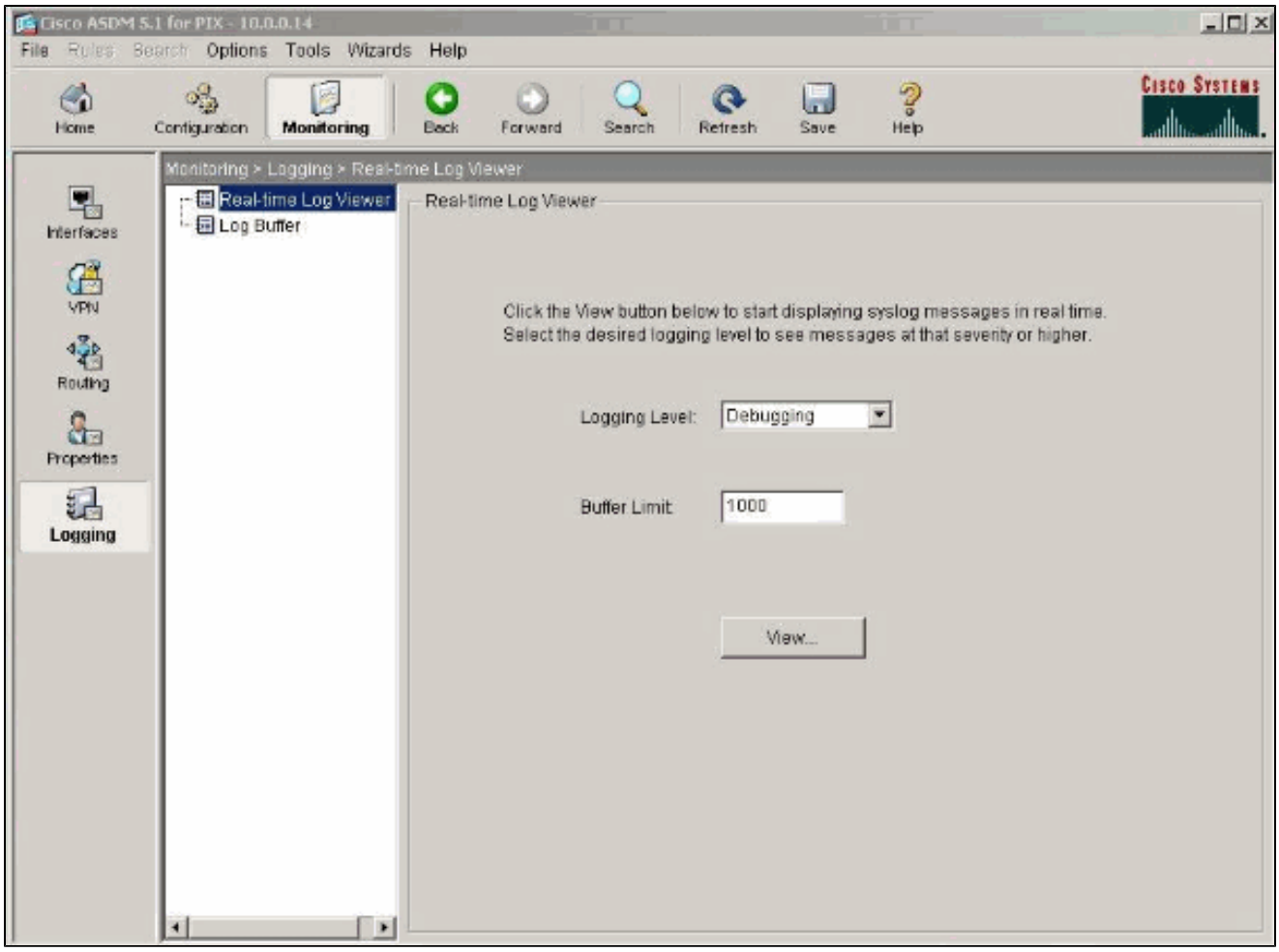


2. Escolha Monitoring > Interfaces > DHCP > DHCP Client Lease Information no cliente DHCP para exibir as informações de associação DHCP.

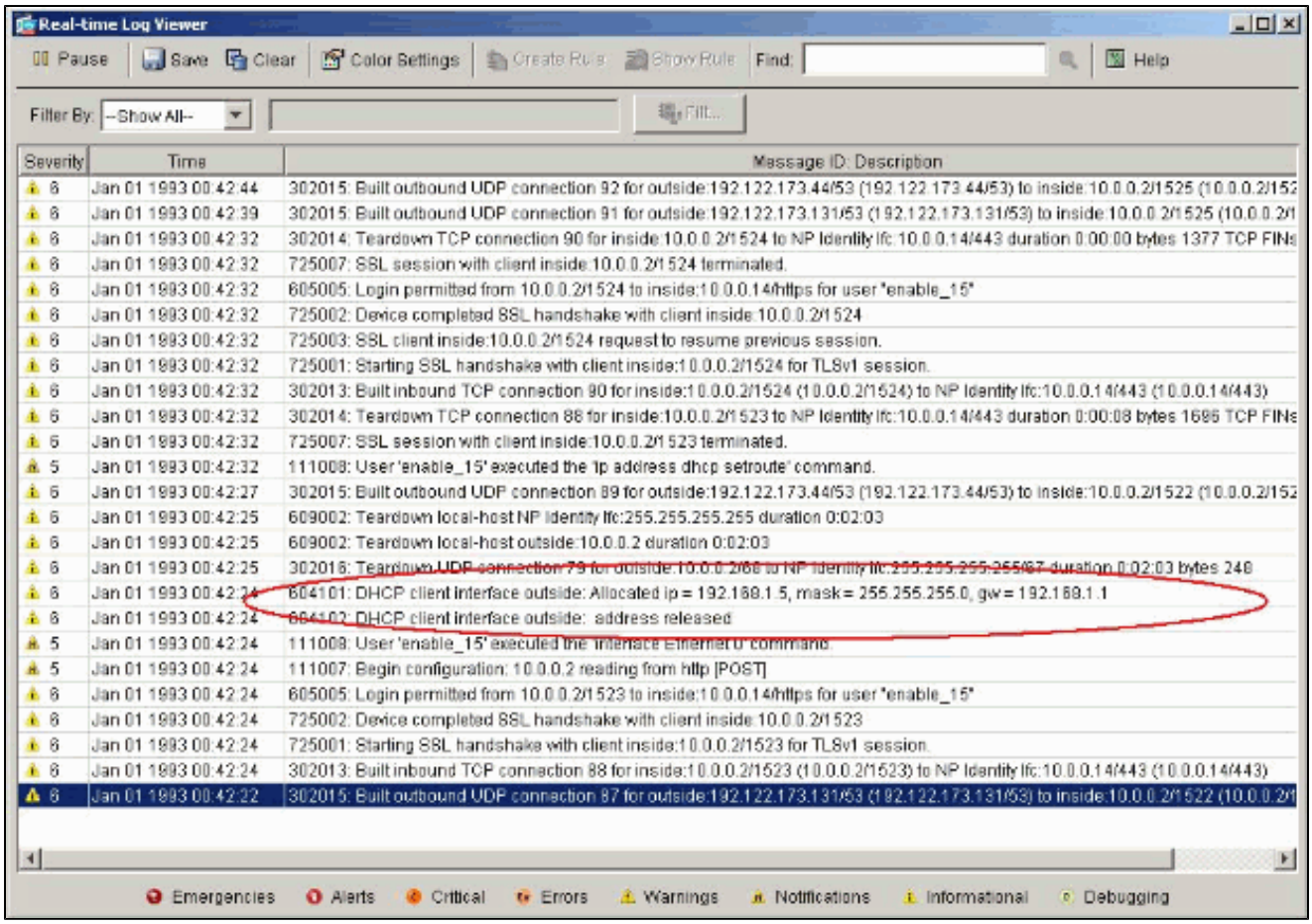
   Insira o comando show dhcpd binding para exibir as informações de vinculação DHCP da CLI.



3. Escolha Monitoring > Logging > Real-time Log Viewer para selecionar o Nível de Log e o limite de buffer para exibir as mensagens de Log em Tempo Real.



4. Exibir os eventos de log em tempo real do cliente DHCP. O endereço IP é alocado para a interface externa do cliente DHCP.



Troubleshooting

Comandos para Troubleshooting

Use esta seção para confirmar se a sua configuração funciona corretamente.

A Output Interpreter Tool (somente clientes registrados) (OIT) oferece suporte a determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Nota:Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos debug.

- debug dhcpd event — Exibe informações sobre eventos associados ao servidor DHCP.
- debug dhcpd packet — Exibe informações sobre o pacote associado ao servidor DHCP.

Mensagens de erro

<#root>

```
CiscoASA(config)#
```

dhcpd address 10.1.1.10-10.3.1.150 inside
Warning, DHCP pool range is limited to 256 addresses, set address range as:
10.1.1.10-10.3.1.150

Explicação: o tamanho do pool de endereços é limitado a 256 endereços por pool no Security Appliance. Isso não pode ser alterado e é uma limitação de software. O total pode ser apenas 256. Se o intervalo do pool de endereços for maior que 253 endereços (por exemplo, 254, 255, 256), a máscara de rede da interface do Security Appliance não poderá ser um endereço de Classe C (por exemplo, 255.255.255.0). Ele precisa ser algo maior, por exemplo, 255.255.254.0.

Consulte o Guia de Configuração de Linha de Comando do Cisco Security Appliance para obter informações sobre como implementar o recurso de servidor DHCP no Security Appliance.

FAQ: Atribuição de endereço

Pergunta — É possível atribuir um endereço IP estático/permanente ao computador que usa o ASA como o servidor DHCP?

Resposta — Não é possível usar o PIX/ASA.

Pergunta — É possível vincular endereços DHCP a endereços MAC específicos no ASA?

Resposta — Não, não é possível .

Informações Relacionadas

- Página de Suporte do PIX Security Appliance
- Referências do comando Cisco Secure PIX Firewall
- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.