PIX/ASA作为DHCP服务器和客户端配置示例

目录

简介

PIX 500 系列安全设备和 Cisco 自适应安全设备 (ASA) 可作为动态主机配置协议 (DHCP) 服务器和 DHCP 客户端运行。DHCP 协议为主机提供自动配置参数，例如带子网掩码的 IP 地址、默认网关、DNS 服务器和 WINS 服务器 IP 地址等。

安全设备可作为 DHCP 服务器或 DHCP 客户端。作为服务器运行时，安全设备可直接为 DHCP 客户端提供网络配置参数。作为 DHCP 客户端运行时，安全设备会向 DHCP 服务器请求这些配置参数。

本文档重点介绍如何在安全设备上使用 Cisco 自适应安全设备管理器 (ASDM) 配置 DHCP 服务器和 DHCP 客户端。

先决条件

要求

本文档假设 PIX 安全设备或 ASA 运行完全正常，并配置为允许 Cisco ASDM 更改配置。

注意： 要允许 ASDM 对设备进行配置，请参阅允许对 ASDM 进行 HTTPS 访问。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- PIX 500 系列安全设备 7.x**注意：** 版本 7.x 使用的 PIX CLI 配置也适用于 PIX 6.x。唯一的差别是，在早于 PIX 6.3 的版本中，只能在内部接口上启用 DHCP 服务器。在 PIX 6.3 及以上版本，可在任何可用接口上启用 DHCP 服务器。在该配置中，外部接口用于 DHCP 服务器功能。
- ASDM 5.x**注意：** ASDM 仅支持 PIX 7.0 及以上版本。PIX 设备管理器 (PDM) 可用于配置 PIX 版本 6.x。有关详细信息，请参阅 Cisco ASA 5500 系列和 PIX 500 系列安全设备硬件和软件兼容性。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

相关产品

此配置也适用于 Cisco ASA 7.x。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

配置

在此配置中，有两个运行版本 7.x 的 PIX 安全设备。一个作为 DHCP 服务器，为作为 DHCP 客户端的另一个 PIX 安全设备 7.x 提供配置参数。作为 DHCP 服务器时，PIX 会动态地将指定的 IP 地址池中的 IP 地址分配给 DHCP 客户端。

您可在安全设备的每个接口上配置 DHCP 服务器。每个接口都有属于其自己的可从中得到地址的地址池。但是，其他 DHCP 设置（例如 DNS 服务器、域名、选项、ping 超时和 WINS 服务器）都是由所有接口上的 DHCP 服务器全局配置和使用。

您不能在启用了服务器的接口上配置 DHCP 客户端或 DHCP 中继服务。另外，DHCP 客户端必须直接连接到启用了服务器的接口。

最后，当在接口上启用 DHCP 服务器时，您无法更改该接口的 IP 地址。

注意： 基本上，没有配置选项可用来设置 DHCP 服务器 (PIX/ASA) 发送的 DHCP 回复的默认网关地址。DHCP 服务器总是将其自己的地址作为网关地址发送给 DHCP 客户端。但是，对指向 Internet 路由器的默认路由进行定义将允许用户到达 Internet。

注意： 可分配的 DHCP 池地址的数量取决于在安全设备 (PIX/ASA) 中使用的许可证。如果使用 Base/Security Plus 许可证，则这些限制适用于 DHCP 池。如果主机限制是 10 台主机，则 DHCP 池的限制为 32 个地址。如果主机限制是 50 台主机，则 DHCP 池的限制为 128 个地址。如果主机没有限制，则 DHCP 池的限制为 256 个地址。因此，地址池的限制是以主机数量为基础的。

注意： 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

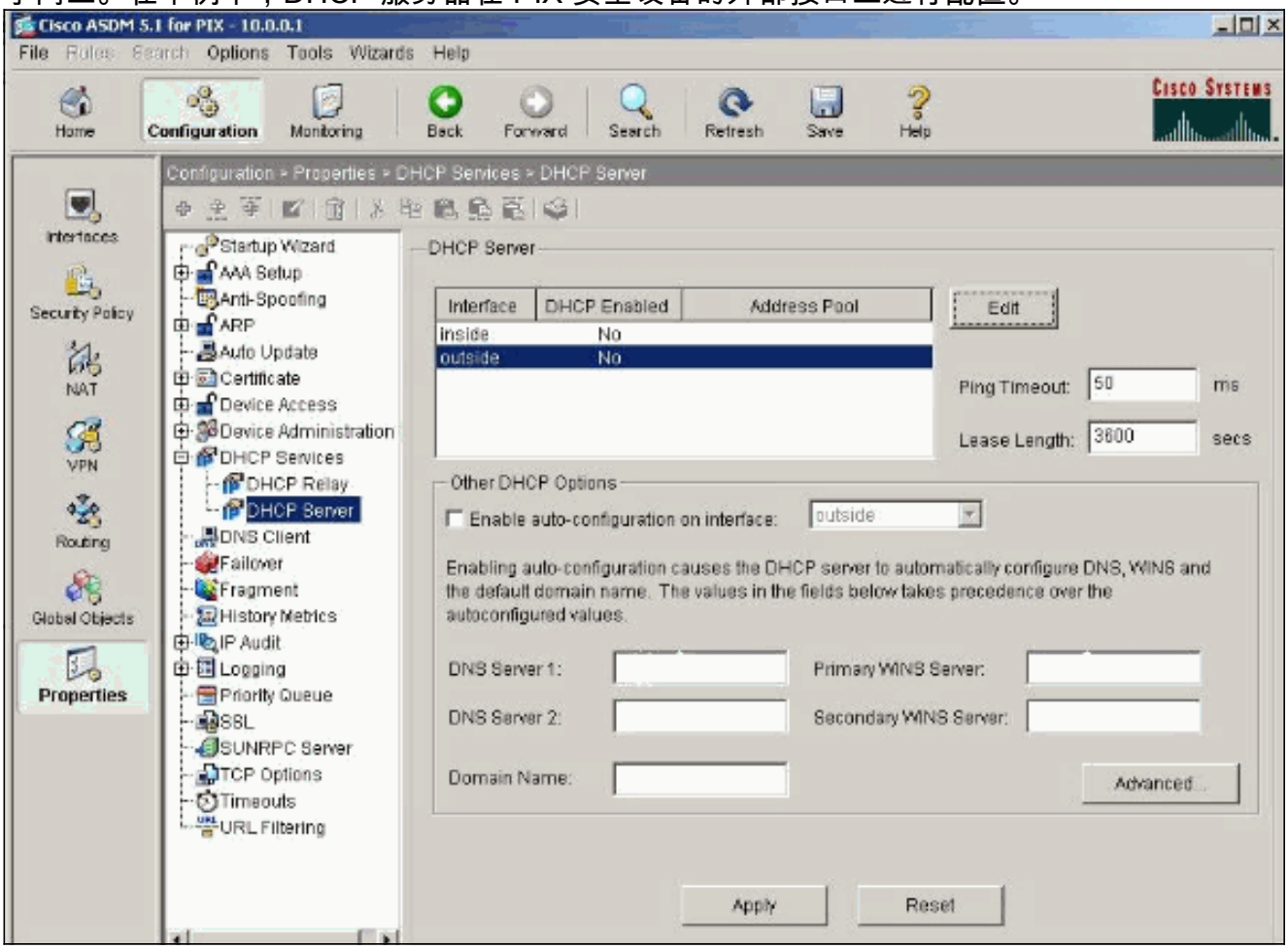
本文档使用以下配置：

- 使用 ASDM 配置 DHCP 服务器

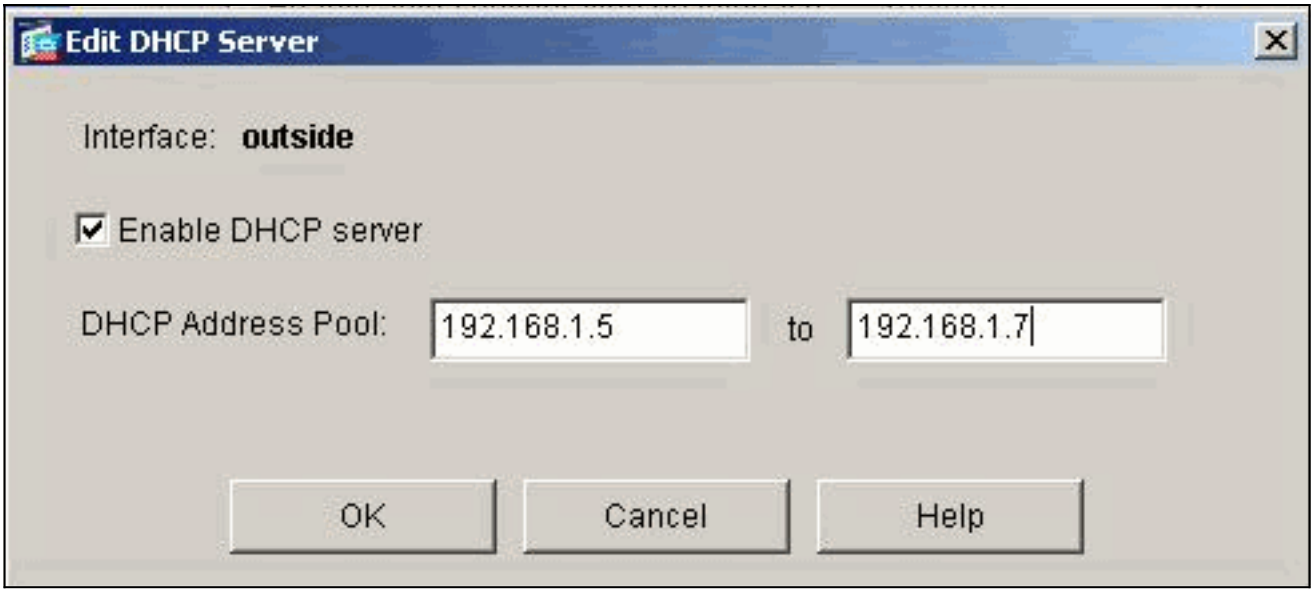
使用 ASDM 配置 DHCP 服务器

使用 ASDM 完成以下步骤以将 PIX 安全设备或 ASA 配置为 DHCP 服务器。

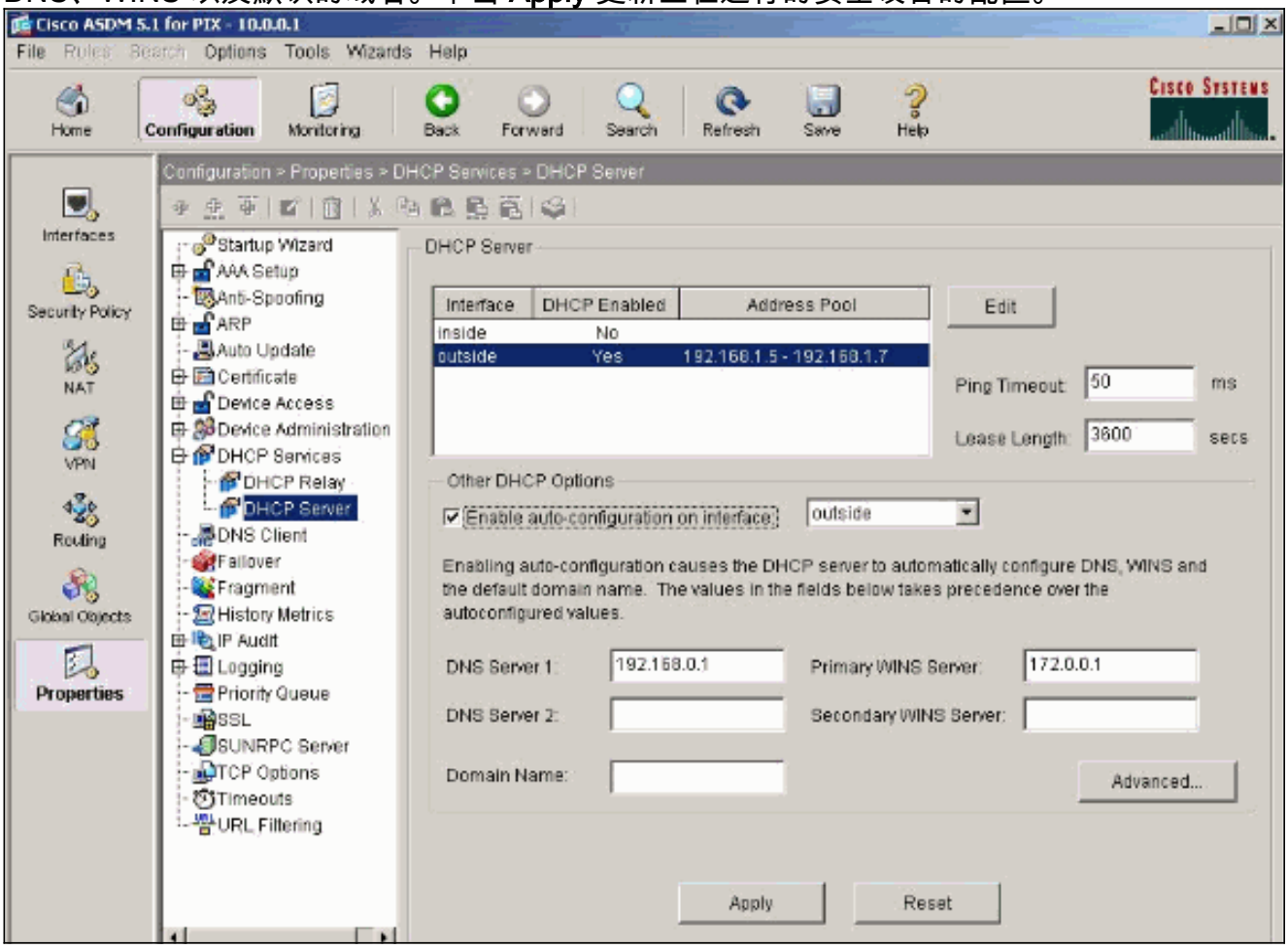
1. 从 Home 窗口选择 **Configuration > Properties > DHCP Services > DHCP Server** 。选择接口并单击 **Edit** 以启用 DHCP 服务器并创建 DHCP 地址池。地址池必须在与安全设备接口相同的子网上。在本例中，DHCP 服务器在 PIX 安全设备的外部接口上进行配置。



2. 在外部接口上选中 **Enable DHCP server** 以侦听 DHCP 客户端的请求。向 DHCP 客户端提供要发出的地址池并单击 **OK** 返回到主窗口。



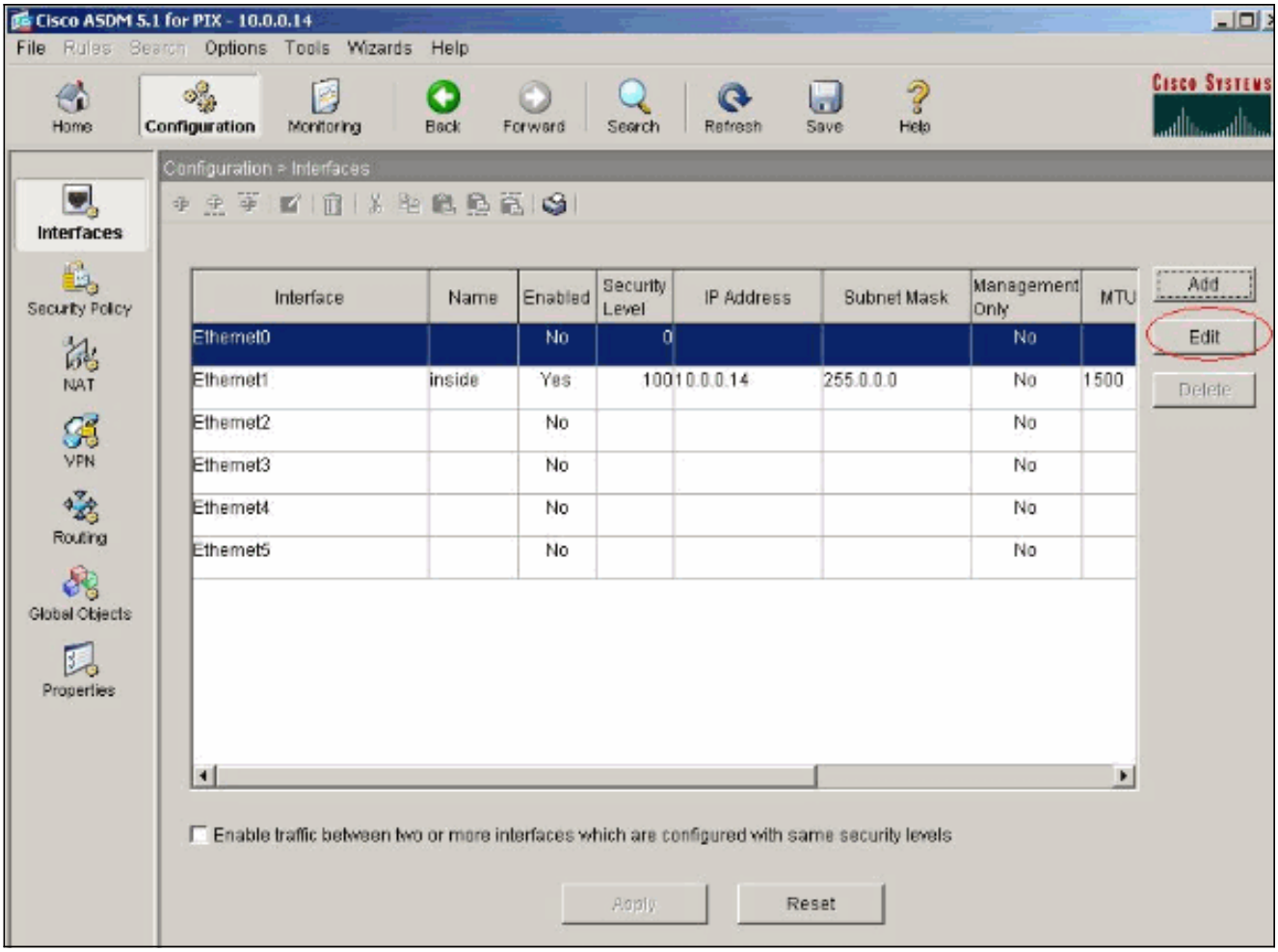
3. 选中 **Enable auto-configuration on the interface** 使 DHCP 服务器自动为 DHCP 客户端配置 DNS、WINS 以及默认的域名。单击 **Apply** 更新正在运行的安全设备的配置。



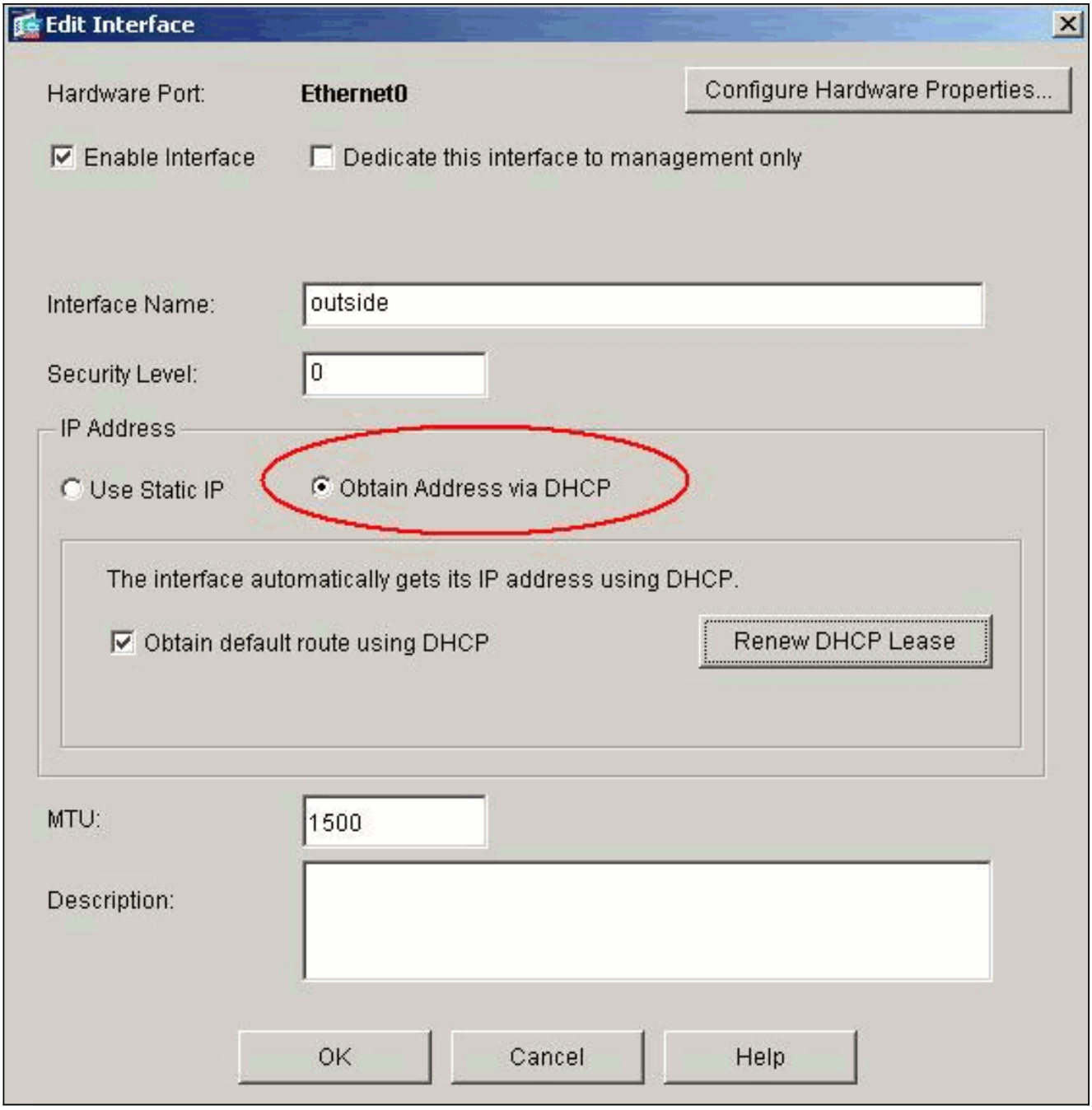
使用 ASDM 配置 DHCP 客户端

使用 ASDM 完成以下步骤将 PIX 安全设备配置为 DHCP 客户端。

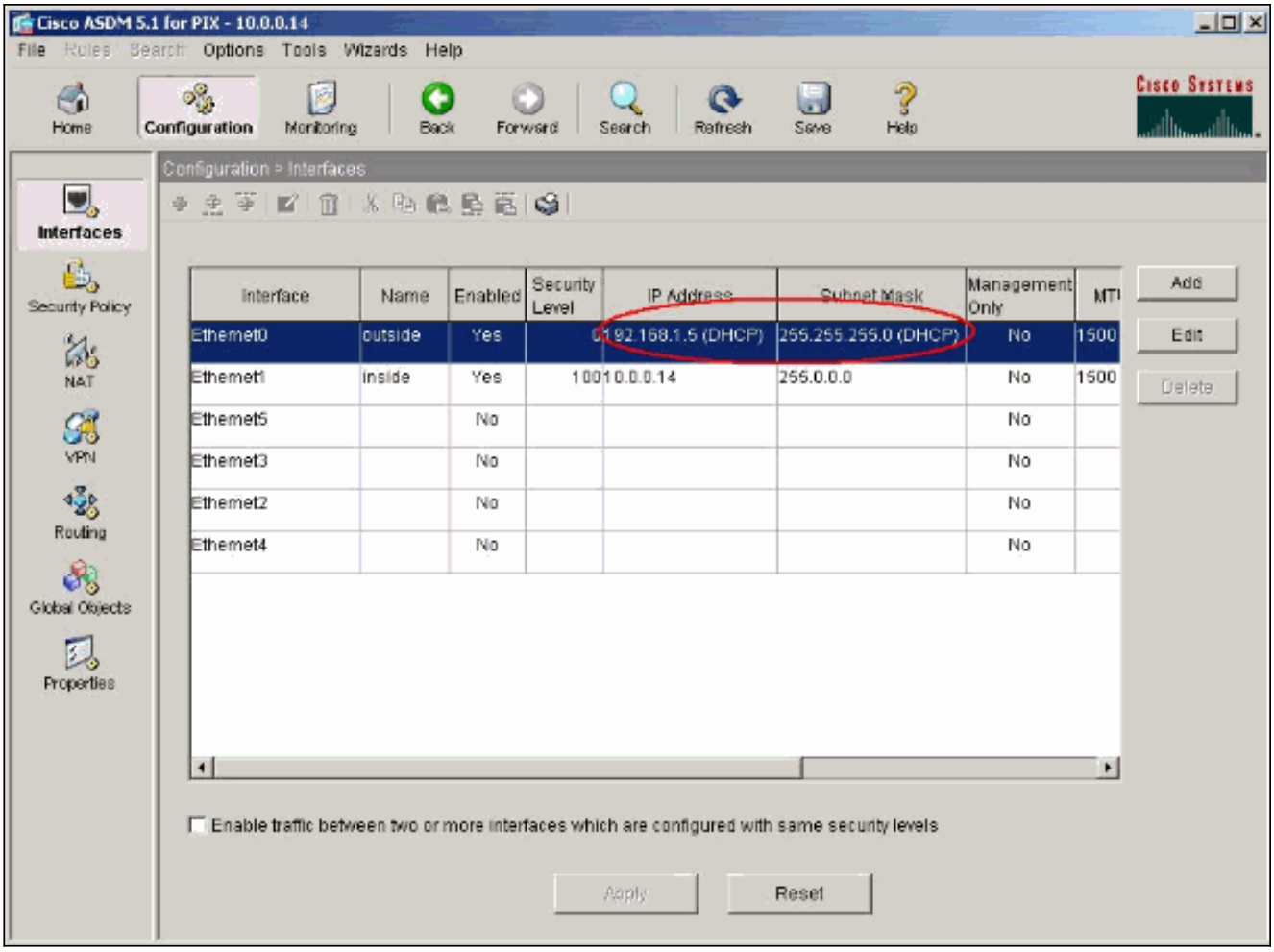
1. 选择 **Configuration > Interfaces** ，然后单击 **Edit** 以启用 Ethernet0 接口，从 DHCP 服务器获取配置参数，如带子网掩码的 IP 地址、默认网关、DNS 服务器以及 WINS 服务器 IP 地址。



2. 选中 **Enable Interface**，然后输入接口名称以及接口的安全级别。选择 **Obtain address via DHCP** 以获得 IP 地址，并选择 **Obtain default route using DHCP** 以获得默认网关，然后单击 **OK** 转到主窗口。



3. 单击 **Apply** 查看从 DHCP 服务器为 Ethernet0 接口获取的 IP 地址。



DHCP 服务器配置

以下配置由 ASDM 创建：

DHCP 服务器

```
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 (in seconds) the client
!--- can use its allocated IP address before the lease
expires. !--- Enter a value between 0 to 1,048,575. The
default value is 3600 seconds. 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 the enabled interface.
dhcpd enable outside dhcprelay timeout 60 ! !--- Output
is suppressed. service-policy global_policy global
Cryptochecksum:7a8cd028ee1c56083b64237c832fb5ab : end
```

DHCP 客户端配置

以下配置由 ASDM 创建：

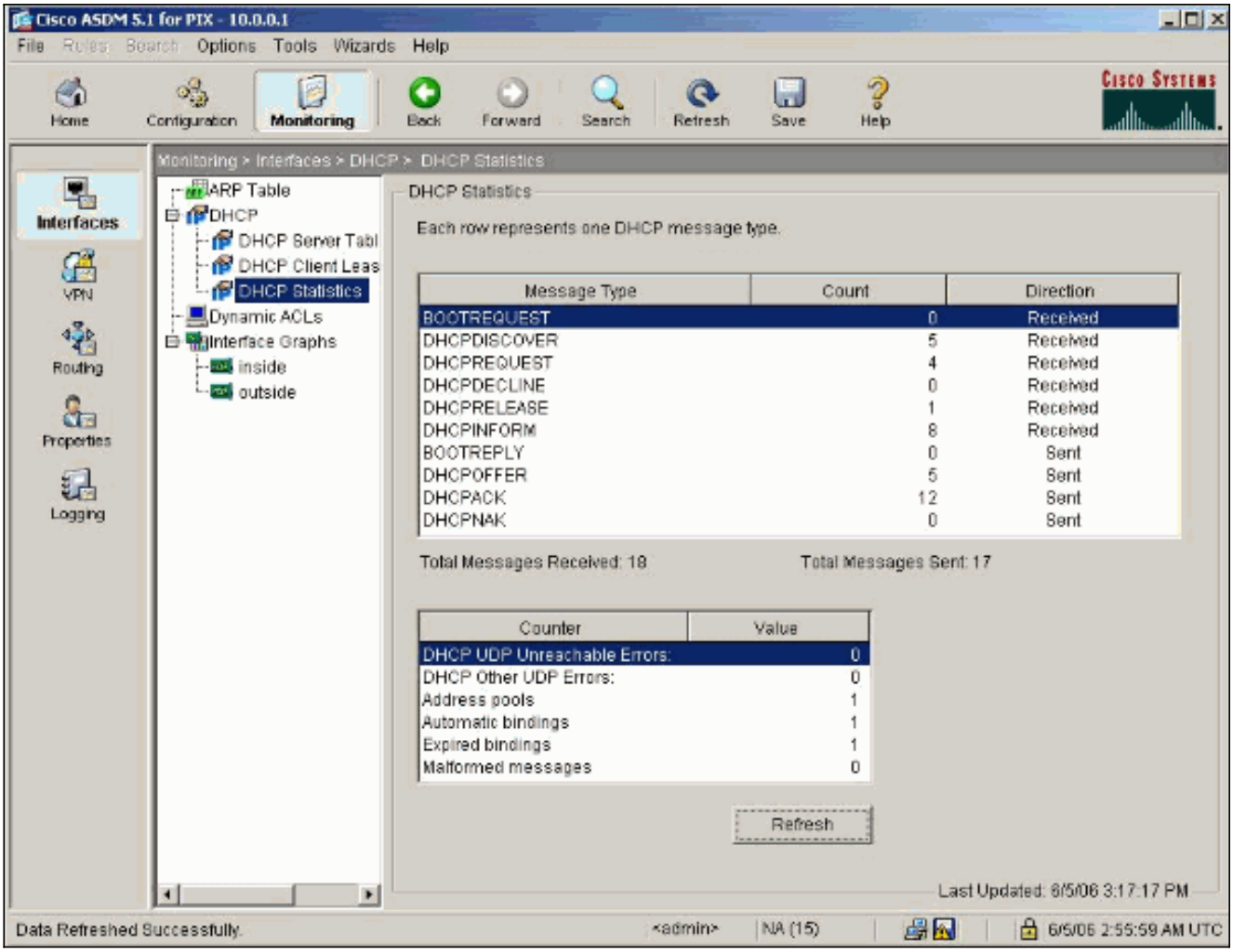
Dhcp 客户机

```
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 DHCP server returns. 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
```

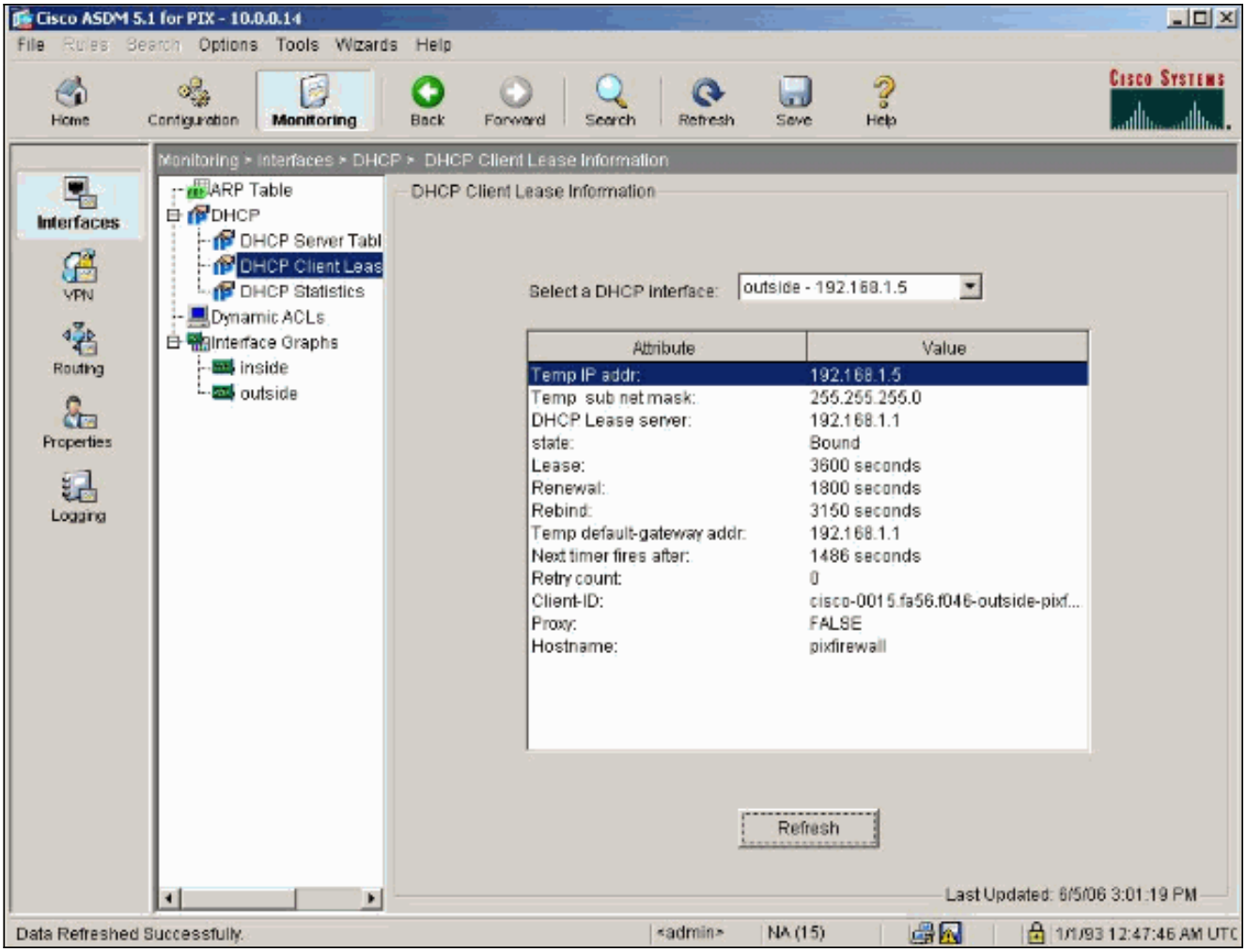
验证

使用 ASDM 完成以下步骤，以验证来自 DHCP 服务器和 DHCP 客户端的 DHCP 统计和绑定信息。

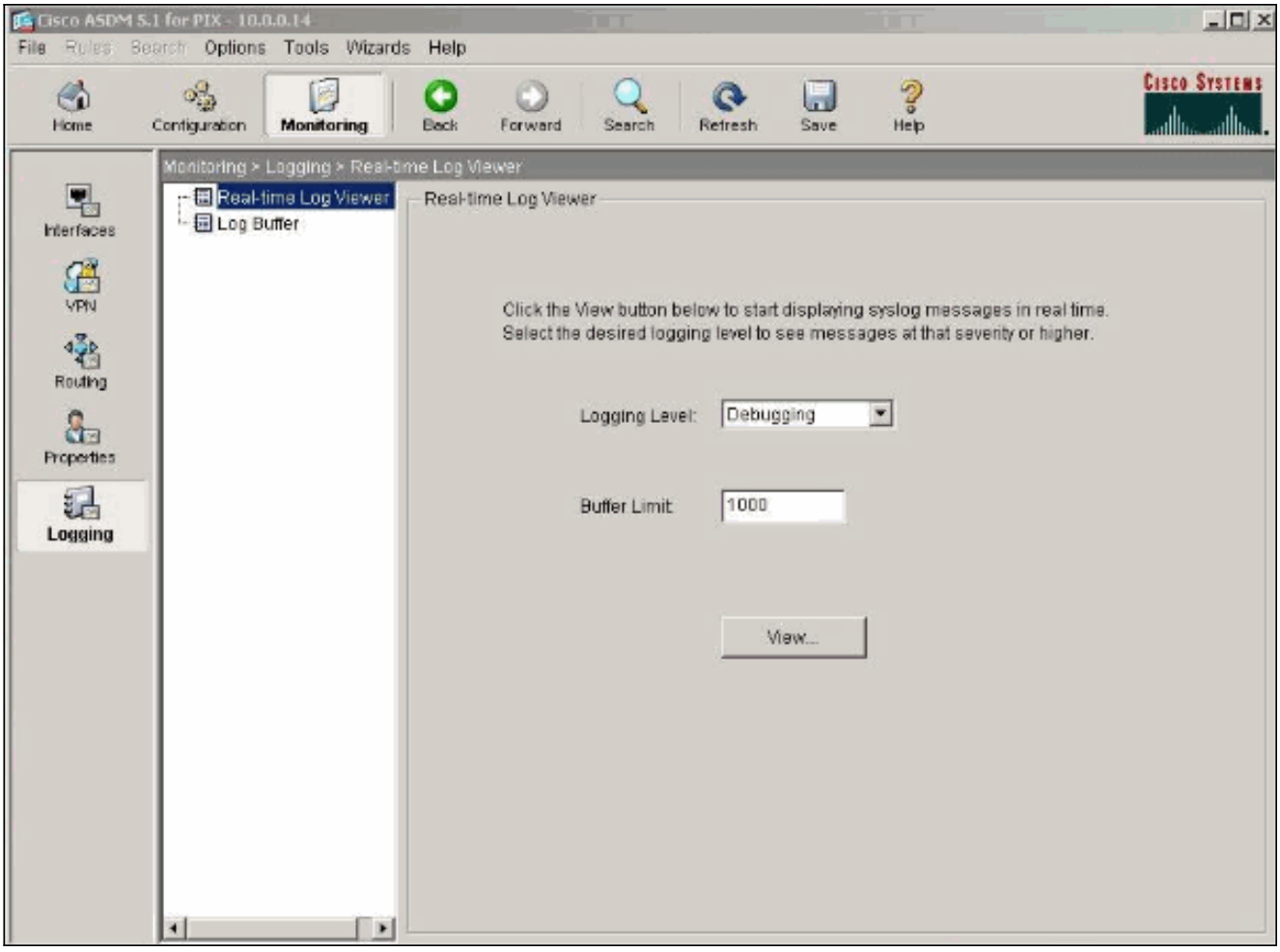
1. 从 DHCP 服务器选择 **Monitoring > Interfaces > DHCP > DHCP Statistics** ，以验证 DHCP 统计数据，如 DHCPDISCOVER、DHCPREQUEST、DHCPOFFER 和 DHCPACK。从 CLI 输入 **show dhcpd statistics** 命令，查看 DHCP 统计数据。



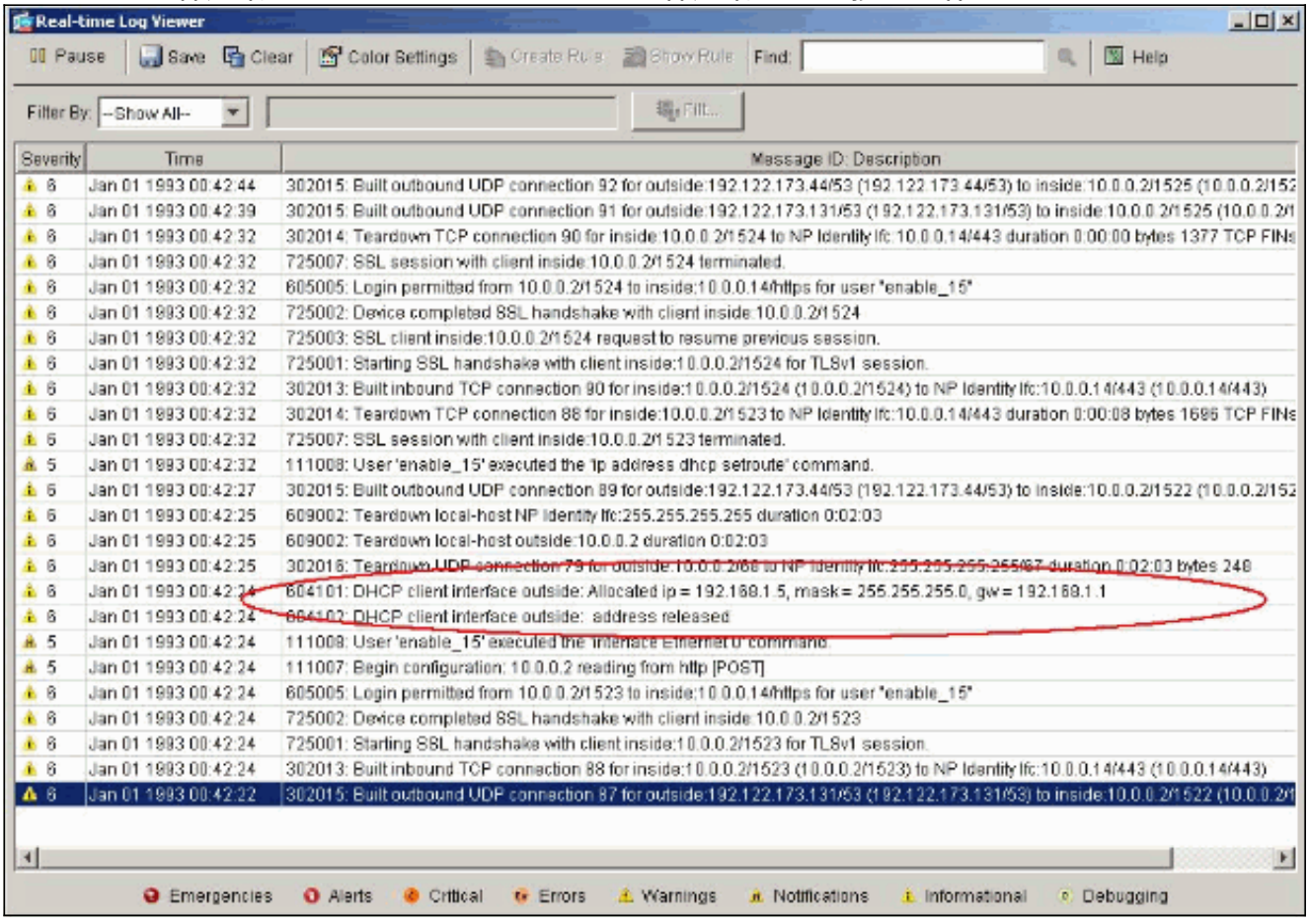
2. 从 DHCP 客户端选择 **Monitoring > Interfaces > DHCP > DHCP Client Lease Information** ，查看 DHCP 绑定信息。从 CLI 输入 **show dhcpd binding** 命令，查看 DHCP 绑定信息。



3. 选择 **Monitoring > Logging > Real-time Log Viewer** 以选择日志级别和缓冲限制，查看实时日志消息。



4. 查看 DHCP 客户端的实时日志事件。为 DHCP 客户端的外部接口分配 IP 地址。



故障排除

故障排除命令

使用本部分可确认配置能否正常运行。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

注意： 使用 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

- **debug dhcpd event** - 显示与 DHCP 服务器关联的事件信息。
- **debug dhcpd packet** - 显示与 DHCP 服务器关联的数据包信息。

错误消息

```
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
```

说明：安全设备上地址池的大小限制为每个池 256 个地址。这一限制无法更改并且是软件限制。总数只能为 256。如果地址池范围大于 253 个地址（例如，254、255、256），则安全设备接口的网络掩码不能为 C 类地址（例如，255.255.255.0）。有时候需要更大的地址，例如，255.255.254.0。

有关如何将 DHCP 服务器功能在安全设备中实施的详细信息，请参阅 Cisco 安全设备命令行配置指南。

FAQ ：地址分配

问题 - 是否有可能向将 ASA 用作 DHCP 服务器的计算机分配静态/永久 IP 地址？

回答 - 如果使用 PIX/ASA，则这是不可能的。

问题 - 是否有可能将 DHCP 地址与特定 MAC 地址连接起来？

答案 - 不，这不是可能的。

相关信息

- PIX 安全设备支持页
- Cisco Secure PIX 防火墙命令参考
- 技术支持和文档 - Cisco Systems