PIX/ASA as a DHCP Server and Client Configuration Example

Document ID: 70391

Contents

Introduction

The PIX 500 Series Security Appliance and Cisco Adaptive Security Appliance (ASA) support operating as both Dynamic Host Configuration Protocol (DHCP) servers and DHCP clients. DHCP is a protocol that supplies automatic configuration parameters such as an IP address with a subnet mask, default gateway, DNS server, and WINS server IP address to hosts.

The Security Appliance can act as a DHCP server or a DHCP client. When it operates as a server, the Security Appliance provides network configuration parameters directly to DHCP clients. When it operates as a DHCP client, the Security Appliance requests such configuration parameters from a DHCP server.

This document focuses on how to configure the DHCP server and DHCP client using the Cisco Adaptive Security Device Manager (ASDM) on the Security Appliance.

Prerequisites

Requirements

This document assumes that the PIX Security Appliance or ASA is fully operational and configured to allow the Cisco ASDM to make configuration changes.

Note: Refer to Allowing HTTPS Access for ASDM to allow the device to be configured by the ASDM.

Components Used

The information in this document is based on these software and hardware versions:

- PIX 500 Series Security Appliance 7.x

  Note: The PIX CLI configuration used in version 7.x is also applicable to PIX 6.x. The only difference is that in versions earlier than PIX 6.3, the DHCP server can only be enabled on the inside interface. In PIX 6.3 and later the DHCP server can be enabled on any of the available interfaces. In this configuration the outside interface is used for the DHCP server feature.
- ASDM 5.x

  Note: ASDM only supports PIX 7.0 and later. The PIX Device Manager (PDM) is available to configure PIX version 6.x .Refer to Cisco ASA 5500 Series and PIX 500 Series Security Appliance Hardware and Software Compatibility for more information.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Related Products

This configuration can also be used with Cisco ASA 7.x.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Configure

In this configuration, there are two PIX Security Appliances that run version 7.x. One functions as a DHCP server that provides configuration parameters to another PIX Security Appliance 7.x which functions as a DHCP client. When it functions as a DHCP server, the PIX dynamically assigns IP addresses to DHCP clients from a pool of designated IP addresses.

You can configure a DHCP server on each interface of the Security Appliance. Each interface can have its own pool of addresses to draw from. However the other DHCP settings, such as DNS servers, domain name, options, ping timeout, and WINS servers are configured globally and used by the DHCP server on all interfaces.

You cannot configure a DHCP client or DHCP relay services on an interface on which the server is enabled. Additionally, DHCP clients must be directly connected to the interface on which the server is enabled.

Finally, while the DHCP server is enabled on an interface, you are unable to change the IP address of that interface.

Note: Basically, there is no configuration option to set the default gateway address in the DHCP reply sent from the DHCP server (PIX/ASA). The DHCP server always sends its own address as the gateway for the DHCP client. However, defining a default route that points to the Internet router allows the user to reach the Internet.

Note: The number of DHCP pool addresses that can be assigned depends upon the licence used in the Security Appliance (PIX/ASA). If you use the Base/Security Plus license then these limits apply to the DHCP

pool. If the Host limit is 10 hosts, you limit the DHCP pool to 32 addresses. If the Host limit is 50 hosts, you limit the DHCP pool to 128 addresses. If the Host limit is unlimited, you limit the DHCP pool to 256 addresses. Thus the address pool is limited based on the number of Hosts.

Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

This document uses these configurations:

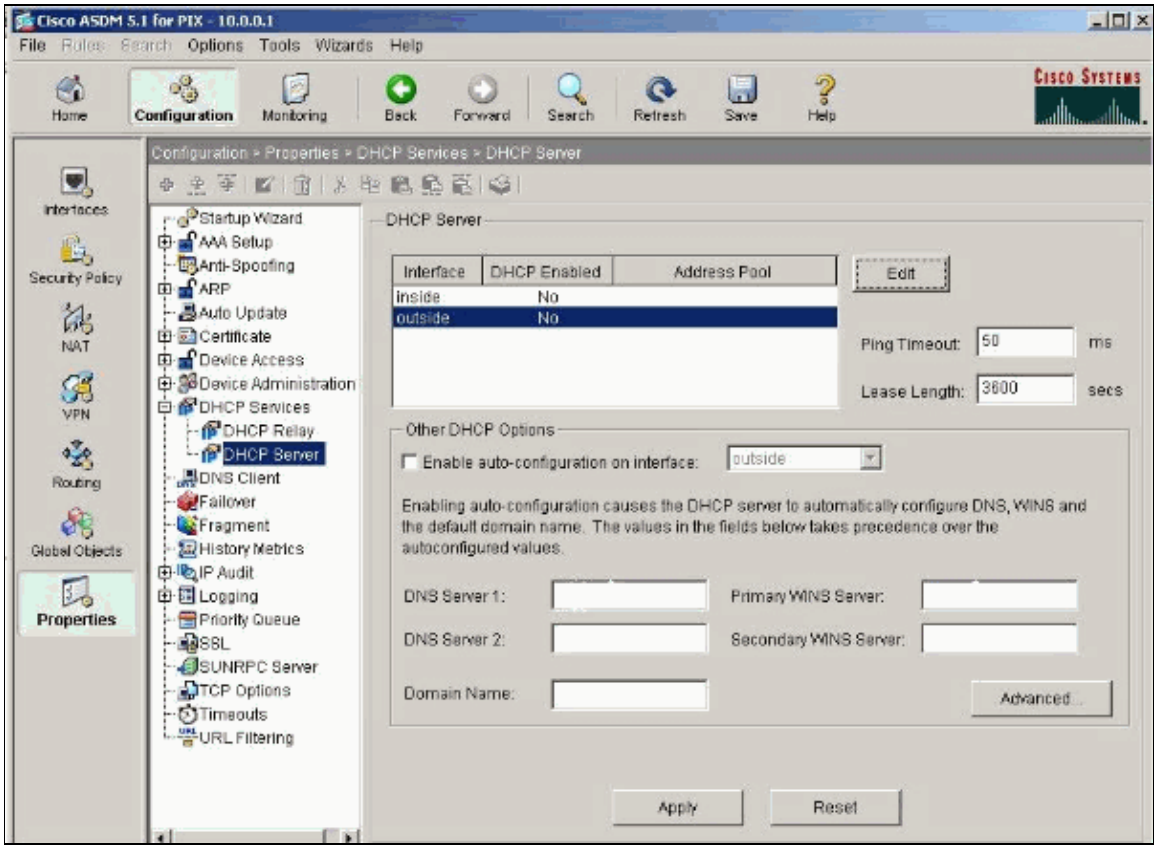
- DHCP Server Configuration using ASDM
- DHCP Client Configuration using ASDM
- DHCP Server Configuration
- DHCP Client Configuration

DHCP Server Configuration using ASDM

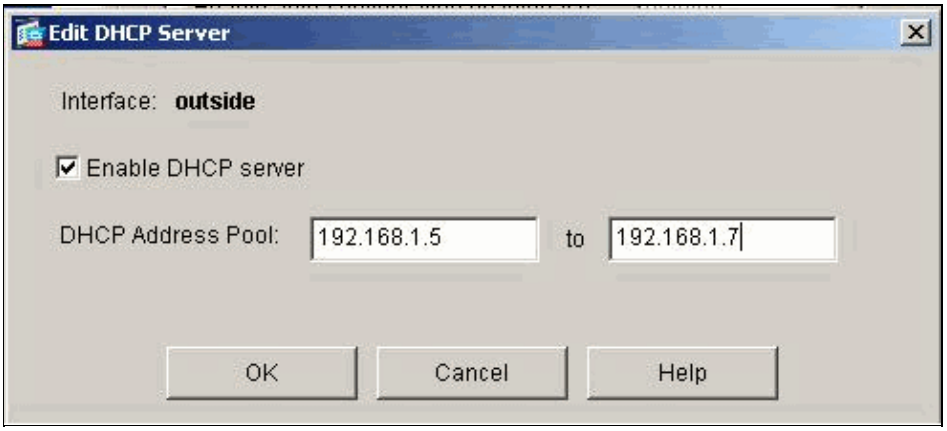
Complete these steps to configure the PIX Security Appliance or ASA as a DHCP server using ASDM.

1. Choose **Configuration > Properties > DHCP Services > DHCP Server** from the Home window. Select an interface and click **Edit** to enable the DHCP server and to create a DHCP address pool.

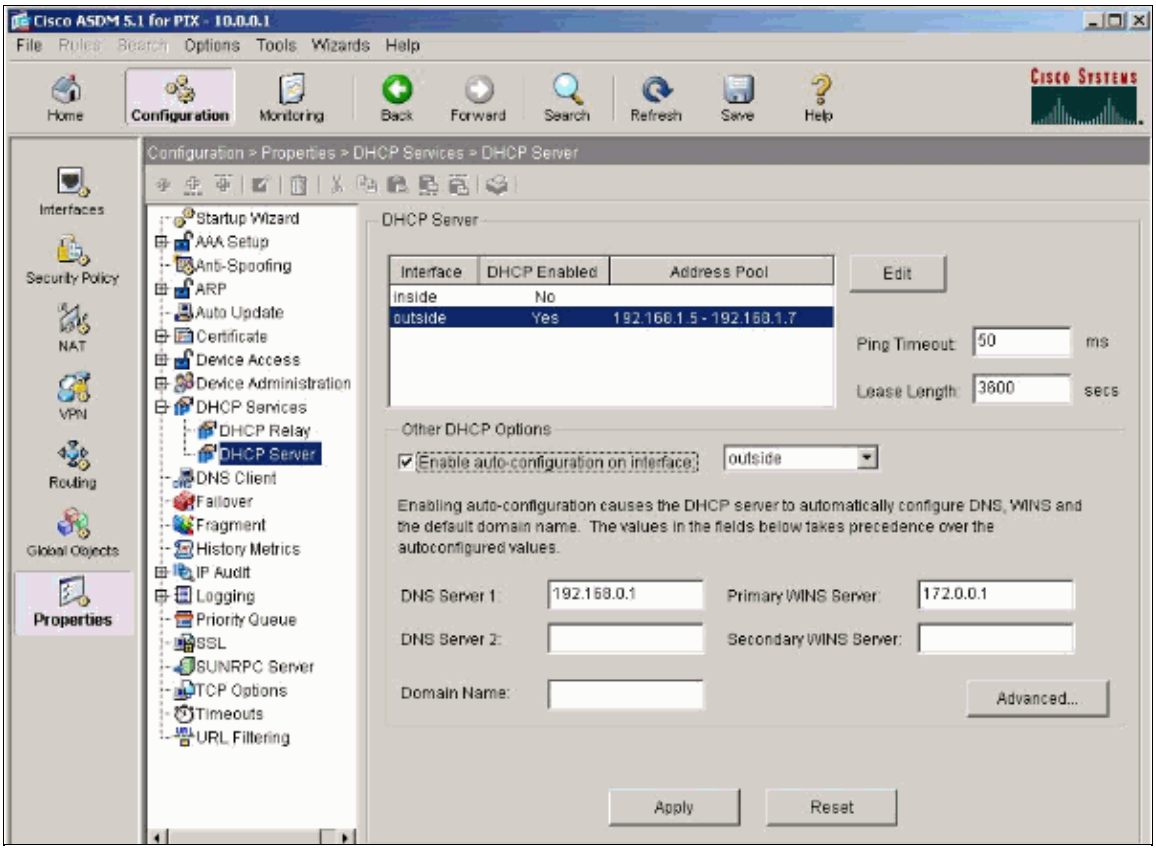
   The address pool must be on the same subnet as the Security Appliance interface. In this example, the DHCP server is configured on the outside interface of the PIX Security Appliance.



2. Check **Enable DHCP server** on the outside interface to listen for the requests of the DHCP clients. Provide the pool of addresses to be issued to the DHCP client and click **OK** to return to the Main window.



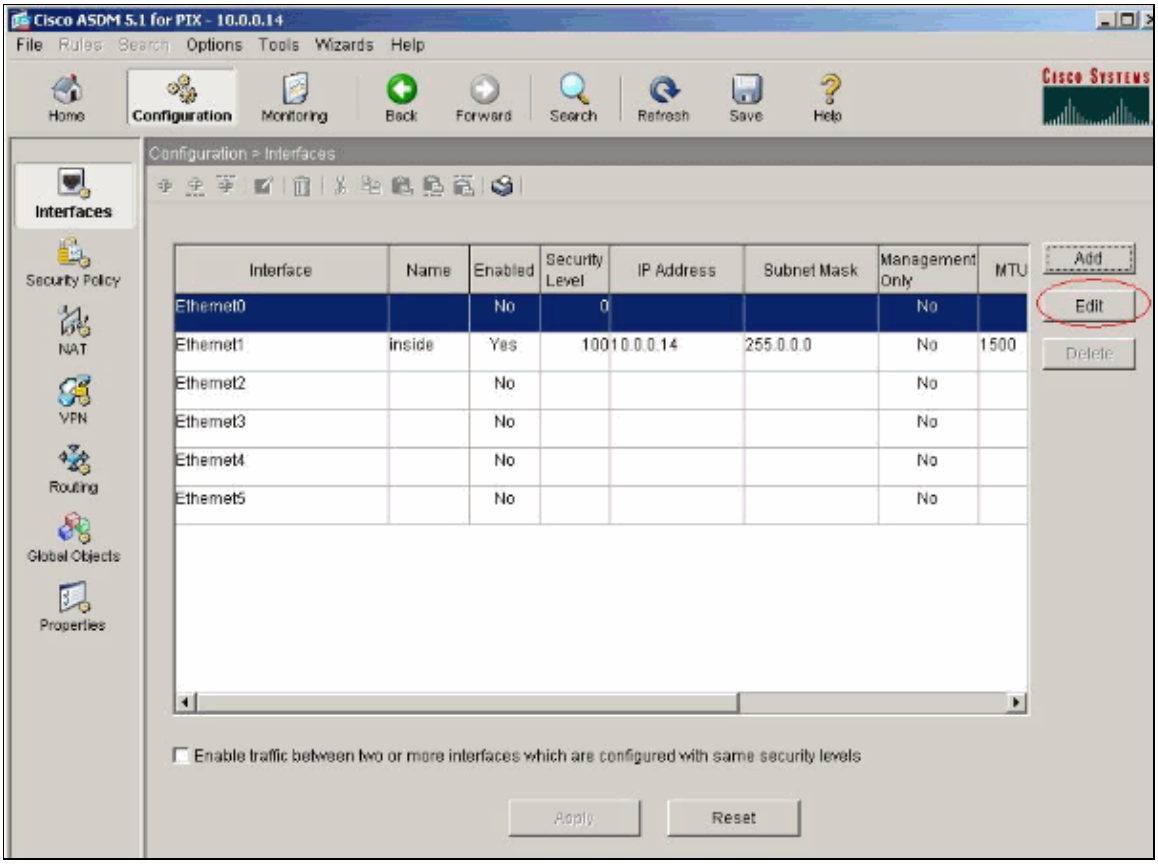
3. Check **Enable auto−configuration on the interface** to cause the DHCP server to automatically configure the DNS, WINS and default Domain Name for the DHCP client. Click **Apply** to update the running configuration of the Security Appliance.



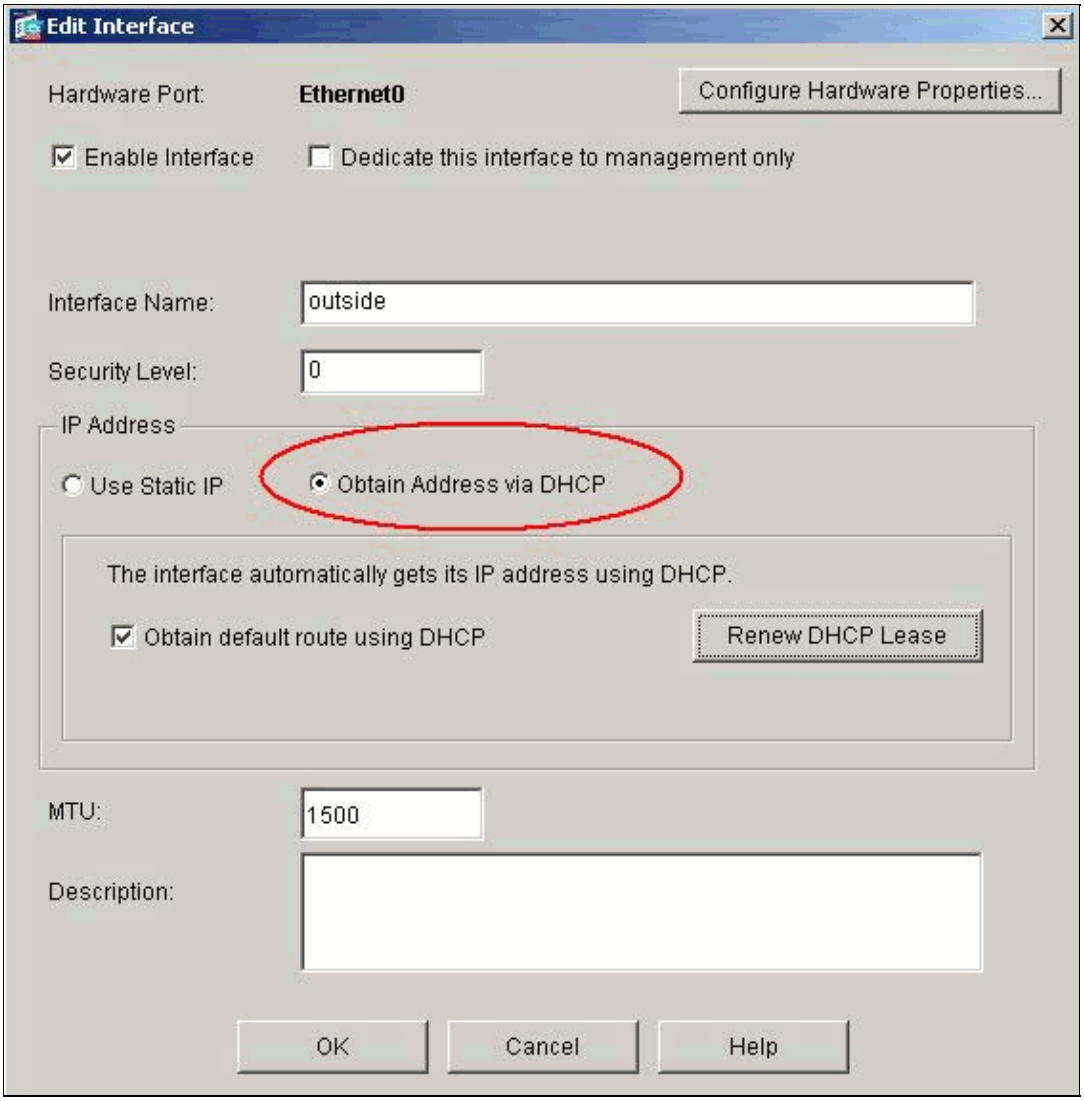
DHCP Client Configuration using ASDM

Complete these steps to configure the PIX Security Appliance as a DHCP client using ASDM.

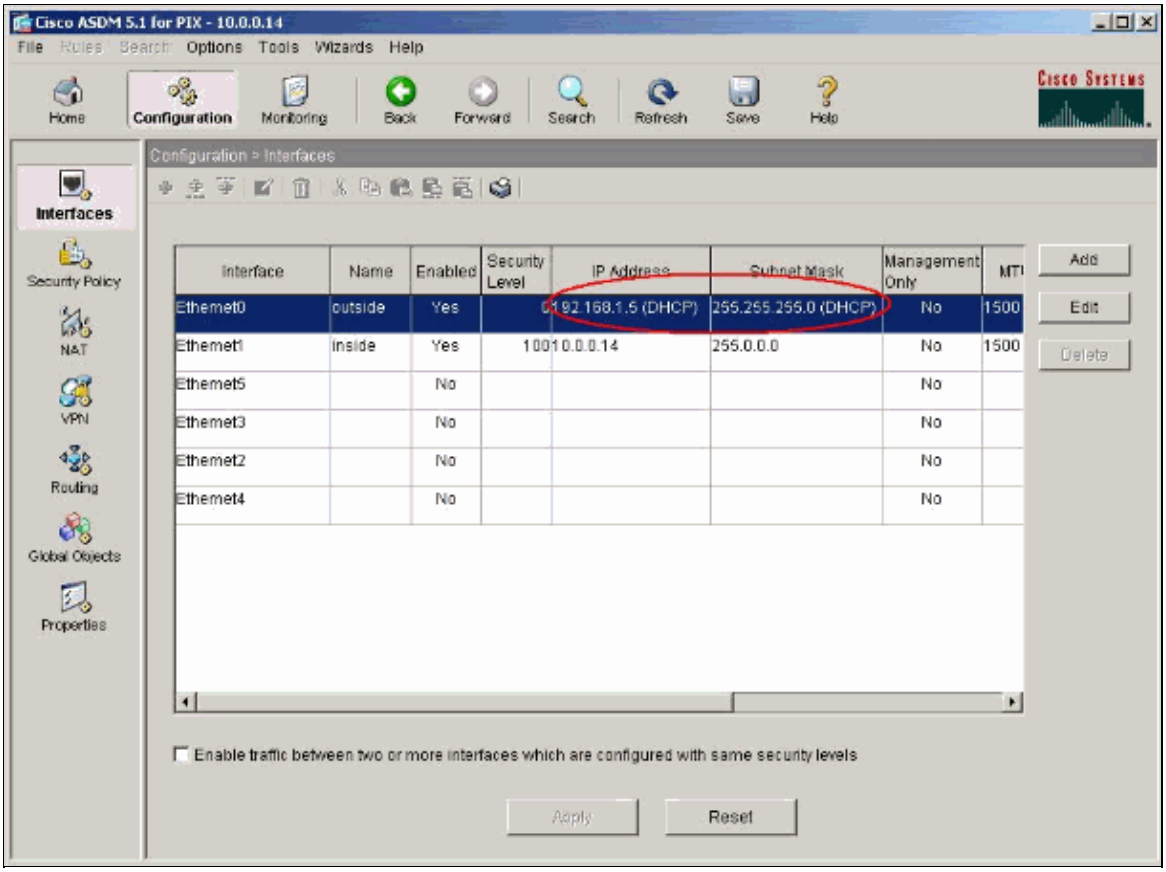
1. Choose **Configuration > Interfaces** and click **Edit** to enable the Ethernet0 interface to obtain the configuration parameters such as an IP address with a subnet mask, default gateway, DNS server and WINS server IP address from the DHCP server.



2. Check **Enable Interface** and enter the Interface Name and Security Level for the interface. Choose **Obtain address via DHCP** for the IP address and **Obtain default route using DHCP** for the default gateway and then click **OK** to go to the Main window.



3. Click **Apply** to see the IP address obtained for the Ethernet0 interface from the DHCP server.



DHCP Server Configuration

This configuration is created by the ASDM:

DHCP Server

```
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 Client Configuration

This configuration is created by the ASDM:

DHCP Client

```
pixfirewall#show running-config
PIX Version 7.1(1)
!
hostname pixfirewall
domain-name default.domain.invalid
```

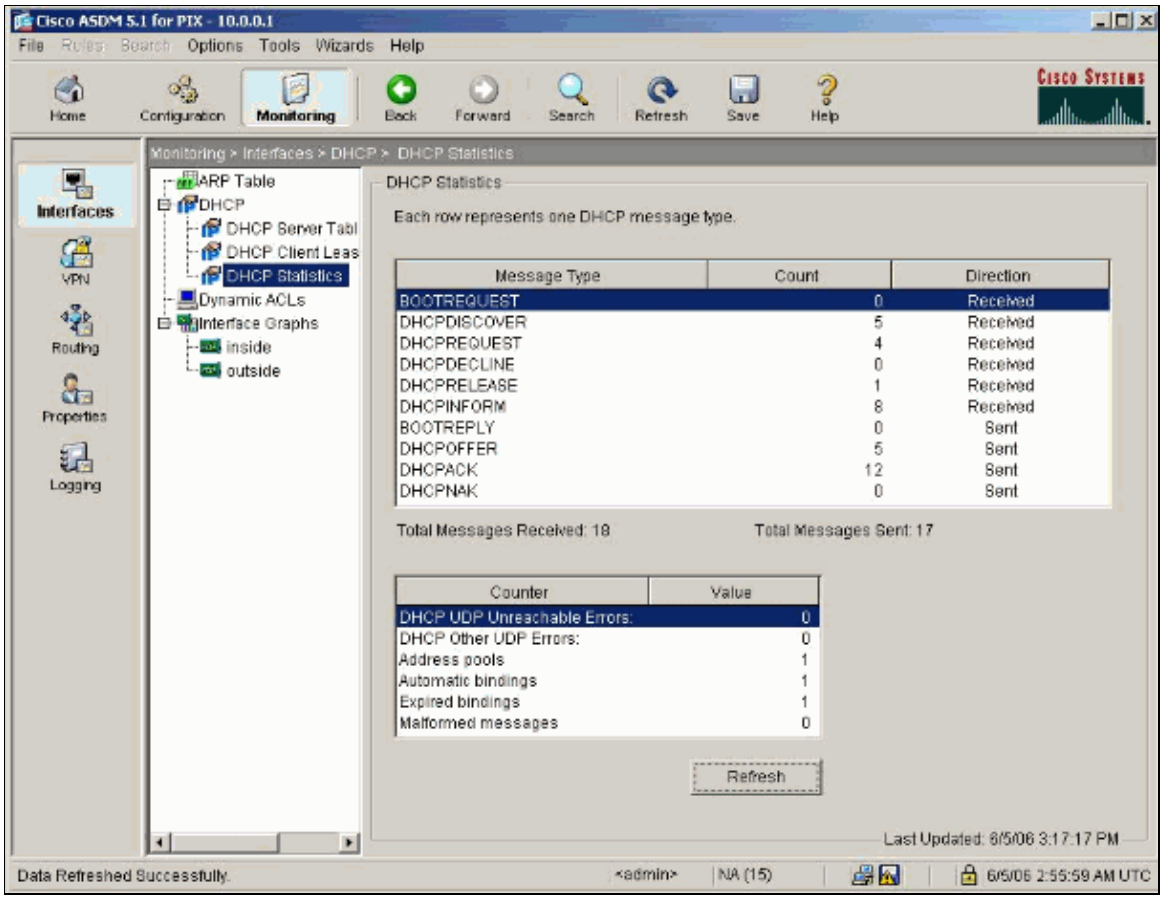
```
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0
 nameif outside
 security-level 0


!--- 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
```

Verify

Complete these steps to verify the DHCP statistics and the binding information from the DHCP server and DHCP client using ASDM.

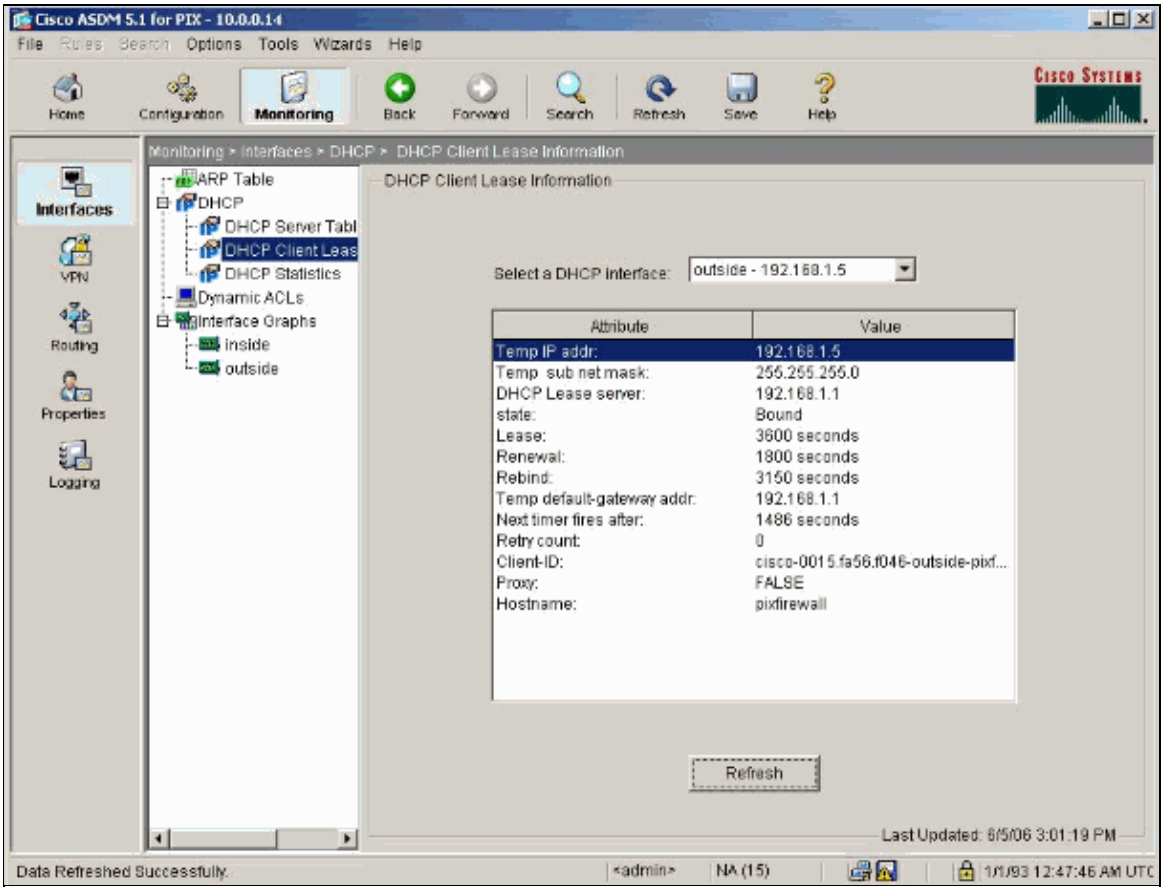
1. Choose **Monitoring > Interfaces > DHCP > DHCP Statistics** from the DHCP server to verify the DHCP statistics, such as DHCPDISCOVER, DHCPREQUEST, DHCPOFFER, and DHCPACK.

   Enter the **show dhcpd statistics** command from the CLI to view the DHCP statistics.

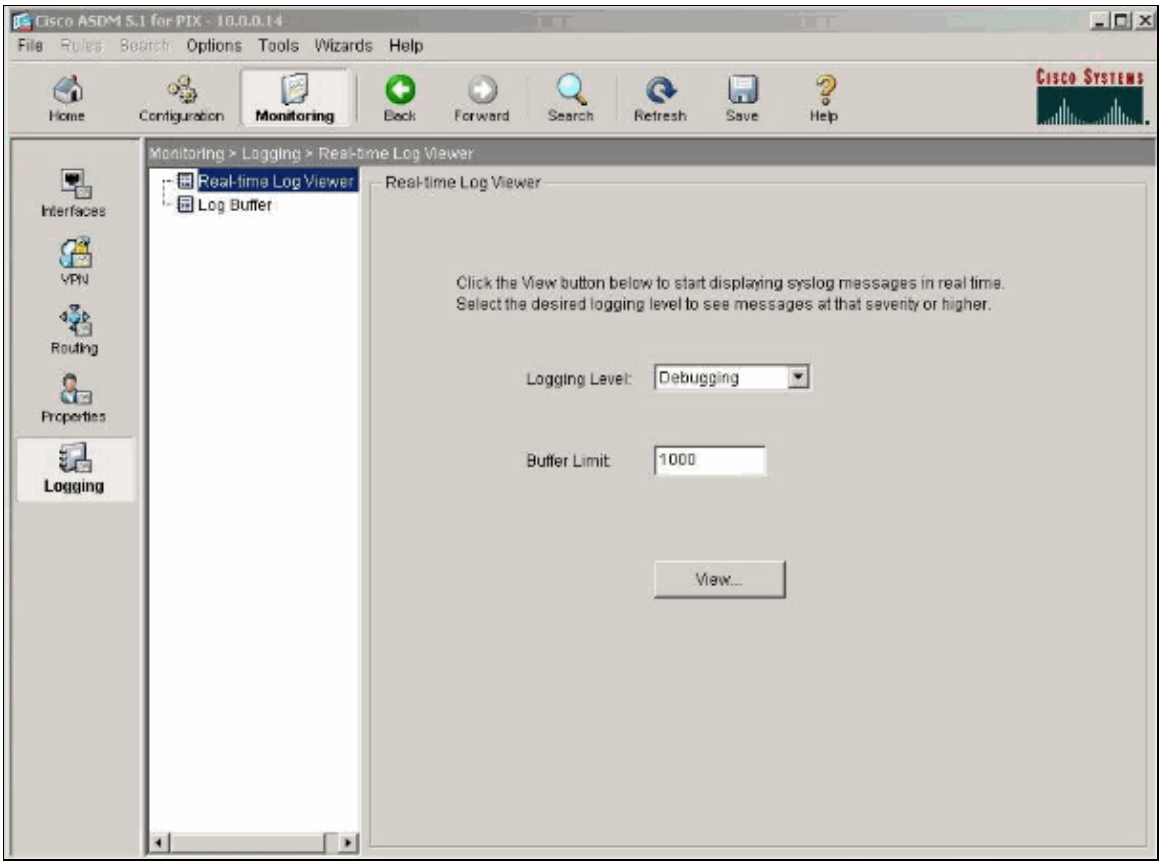


2. Choose **Monitoring > Interfaces > DHCP > DHCP Client Lease Information** from the DHCP client to view the DHCP binding information.

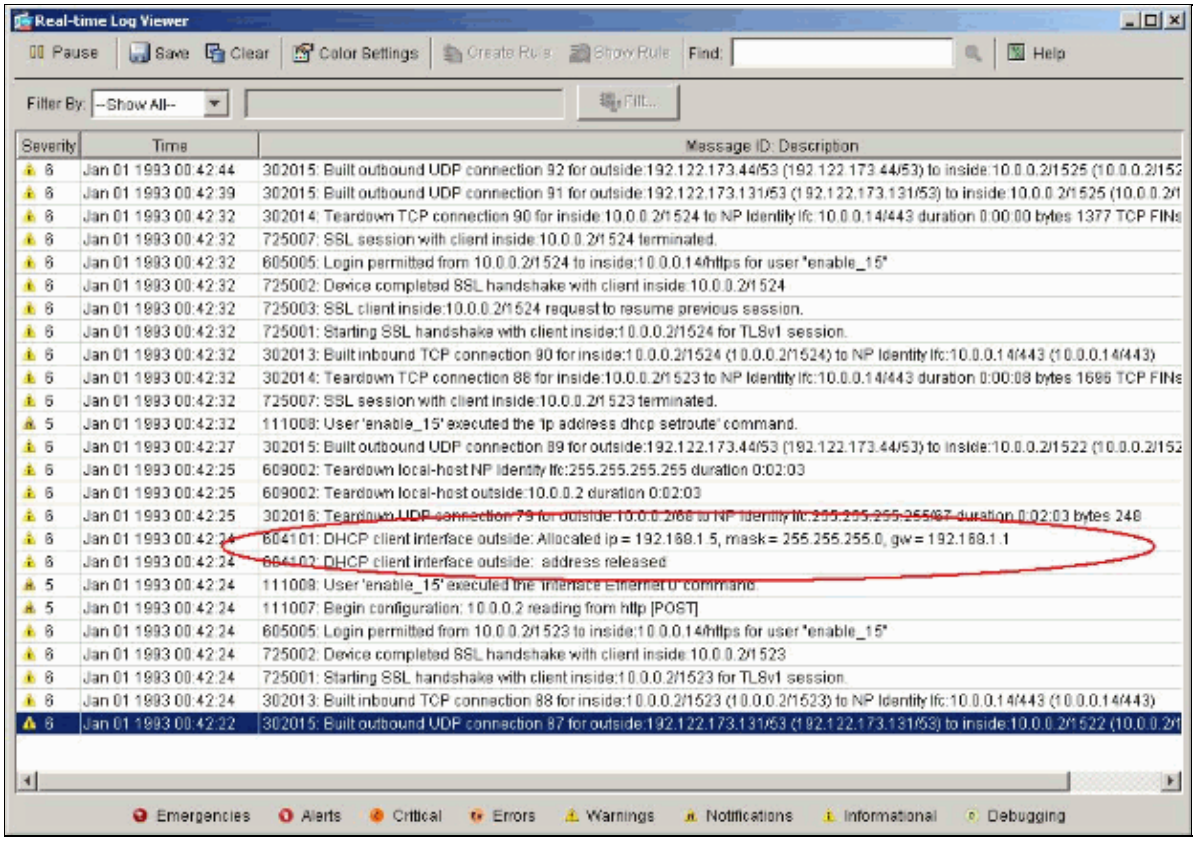
   Enter the **show dhcpd binding** command to view the DHCP binding information from the CLI.



3. Choose **Monitoring > Logging > Real−time Log Viewer** to select the Logging Level and the buffer limit to view the Real Time Log messages.



4. View the real time log events from the DHCP client. The IP address is allocated for the outside interface of the DHCP client.



Troubleshoot

Troubleshooting Commands

Use this section to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

Note: Refer to Important Information on Debug Commands before you use **debug** commands.

- **debug dhcpd event** Displays event information that is associated with the DHCP server.
- **debug dhcpd packet** Displays packet information that is associated with the DHCP server.

Error Messages

```
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
```

Explanation: The size of the address pool is limited to 256 addresses per pool on the security appliance. This cannot be changed and is a software limitation. The total can only be 256. If the address pool range is larger than 253 addresses (for example 254, 255, 256), the netmask of the security appliance interface cannot be a Class C address (for example, 255.255.255.0). It needs to be something larger, for example, 255.255.254.0.

Refer to the Cisco Security Appliance Command Line Configuration Guide for information on how to implement the DHCP server feature into the security appliance.

FAQ: Address Assignment

Question Is it possible to assign a static/permanent IP address to the computer that uses ASA as the DHCP server?

Answer It is not possible using PIX/ASA.

Question Is it possible to tie DHCP addresses to specific MAC addresses on ASA?

Answer No, it is not possible .

Related Information

- **PIX Security Appliance Support Page**
- **Cisco Secure PIX Firewall Command References**
- **Documentation for PIX Firewall**
- **Technical Support & Documentation − Cisco Systems**

Updated: Oct 13, 2008 Document ID: 70391