PIX/ASA as a DHCP Server 및 Client Configuration 예

목차

소개
사전 요구 사항
요구 사항
사용되는 구성 요소
관련 제품
표기 규칙
구성
ASDM을 사용하는 DHCP 서버 구성
ASDM을 사용하는 DHCP 클라이언트 구성
DHCP 서버 구성
DHCP 클라이언트 구성
다음을 확인합니다.
문제 해결
문제 해결 명령
오류 메시지
FAQ:주소 할당
관련 정보

소개

PIX 500 Series Security Appliance 및 Cisco ASA(Adaptive Security Appliance)는 DHCP(Dynamic Host Configuration Protocol) 서버 및 DHCP 클라이언트 둘 다로 작동합니다.DHCP는 IP 주소와 서브넷 마스크, 기본 게이트웨이, DNS 서버, WINS 서버 IP 주소 등의 자동 구성 매개변수를 호스트에 제공하는 프로토콜입니다.

보안 어플라이언스는 DHCP 서버 또는 DHCP 클라이언트 역할을 할 수 있습니다.서버로 작동할 때 보안 어플라이언스는 DHCP 클라이언트에 직접 네트워크 구성 매개변수를 제공합니다.DHCP 클라이언트로 작동하는 경우 보안 어플라이언스는 DHCP 서버에서 이러한 컨피그레이션 매개변수를 요청합니다.

이 문서에서는 보안 어플라이언스에서 Cisco ASDM(Adaptive Security Device Manager)을 사용하여 DHCP 서버 및 DHCP 클라이언트를 구성하는 방법에 대해 중점적으로 설명합니다.

사전 요구 사항

요구 사항

이 문서에서는 PIX Security Appliance 또는 ASA가 완전히 작동 중이고 Cisco ASDM이 컨피그레이션을 변경할 수 있도록 구성되어 있다고 가정합니다.

참고: ASDM에 의해 디바이스를 구성할 수 있도록 ASDM에 대한 HTTPS 액세스 허용을 참조하십시오.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- PIX 500 Series Security Appliance 7.x**참고:** 버전 7.x에서 사용되는 PIX CLI 구성은 PIX 6.x에도 적용됩니다.유일한 차이점은 PIX 6.3 이전 버전에서는 내부 인터페이스에서만 DHCP 서버를 활성화할 수 있다는 것입니다.PIX 6.3 이상에서는 사용 가능한 인터페이스에서 DHCP 서버를 활성화할 수 있습니다.이 컨피그레이션에서는 외부 인터페이스가 DHCP 서버 기능에 사용됩니다.
- ASDM 5.x**참고:** ASDM은 PIX 7.0 이상만 지원합니다.PDM(PIX Device Manager)을 사용하여 PIX 버전 6.x를 구성할 수 있습니다. 자세한 내용은 Cisco ASA 5500 Series 및 PIX 500 Series Security Appliance 하드웨어 및 소프트웨어 호환성을 참조하십시오.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

관련 제품

이 컨피그레이션은 Cisco ASA 7.x에서도 사용할 수 있습니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

구성

이 컨피그레이션에는 버전 7.x를 실행하는 두 개의 PIX Security Appliance가 있습니다.하나는 DHCP 클라이언트로 작동하는 다른 PIX Security Appliance 7.x에 구성 매개변수를 제공하는 DHCP 서버 역할을 합니다.DHCP 서버로 작동할 때 PIX는 지정된 IP 주소 풀의 DHCP 클라이언트에 IP 주소를 동적으로 할당합니다.

보안 어플라이언스의 각 인터페이스에서 DHCP 서버를 구성할 수 있습니다.각 인터페이스에는 가져올 고유한 주소 풀이 있을 수 있습니다.그러나 DNS 서버, 도메인 이름, 옵션, ping 시간 초과 및 WINS 서버와 같은 다른 DHCP 설정은 전역으로 구성되며 모든 인터페이스에서 DHCP 서버에서 사용됩니다.

서버가 활성화된 인터페이스에서는 DHCP 클라이언트 또는 DHCP 릴레이 서비스를 구성할 수 없습니다.또한 DHCP 클라이언트는 서버가 활성화된 인터페이스에 직접 연결되어야 합니다.

마지막으로, DHCP 서버가 인터페이스에서 활성화된 동안에는 해당 인터페이스의 IP 주소를 변경할 수 없습니다.

참고: 기본적으로 DHCP 서버(PIX/ASA)에서 보낸 DHCP 회신에 기본 게이트웨이 주소를 설정하는

구성 옵션은 없습니다. DHCP 서버는 항상 자신의 주소를 DHCP 클라이언트의 게이트웨이로 전송합니다.그러나 인터넷 라우터를 가리키는 기본 경로를 정의하면 사용자가 인터넷에 연결할 수 있습니다.

참고: 할당할 수 있는 DHCP 풀 주소의 수는 Security Appliance(PIX/ASA)에 사용된 라이센스에 따라 달라집니다. Base/Security Plus 라이센스를 사용하는 경우 이러한 제한은 DHCP 풀에 적용됩니다.호스트 제한이 10개 호스트인 경우 DHCP 풀을 32개 주소로 제한합니다.호스트 제한이 50개 호스트인 경우 DHCP 풀을 128개 주소로 제한합니다.호스트 제한이 무제한인 경우 DHCP 풀을 256개의 주소로 제한합니다.따라서 주소 풀은 호스트 수에 따라 제한됩니다.

참고: 명령 조회 도구(등록된 고객만 해당)를 사용하여 이 섹션에 사용된 명령에 대한 자세한 내용을 확인하십시오.

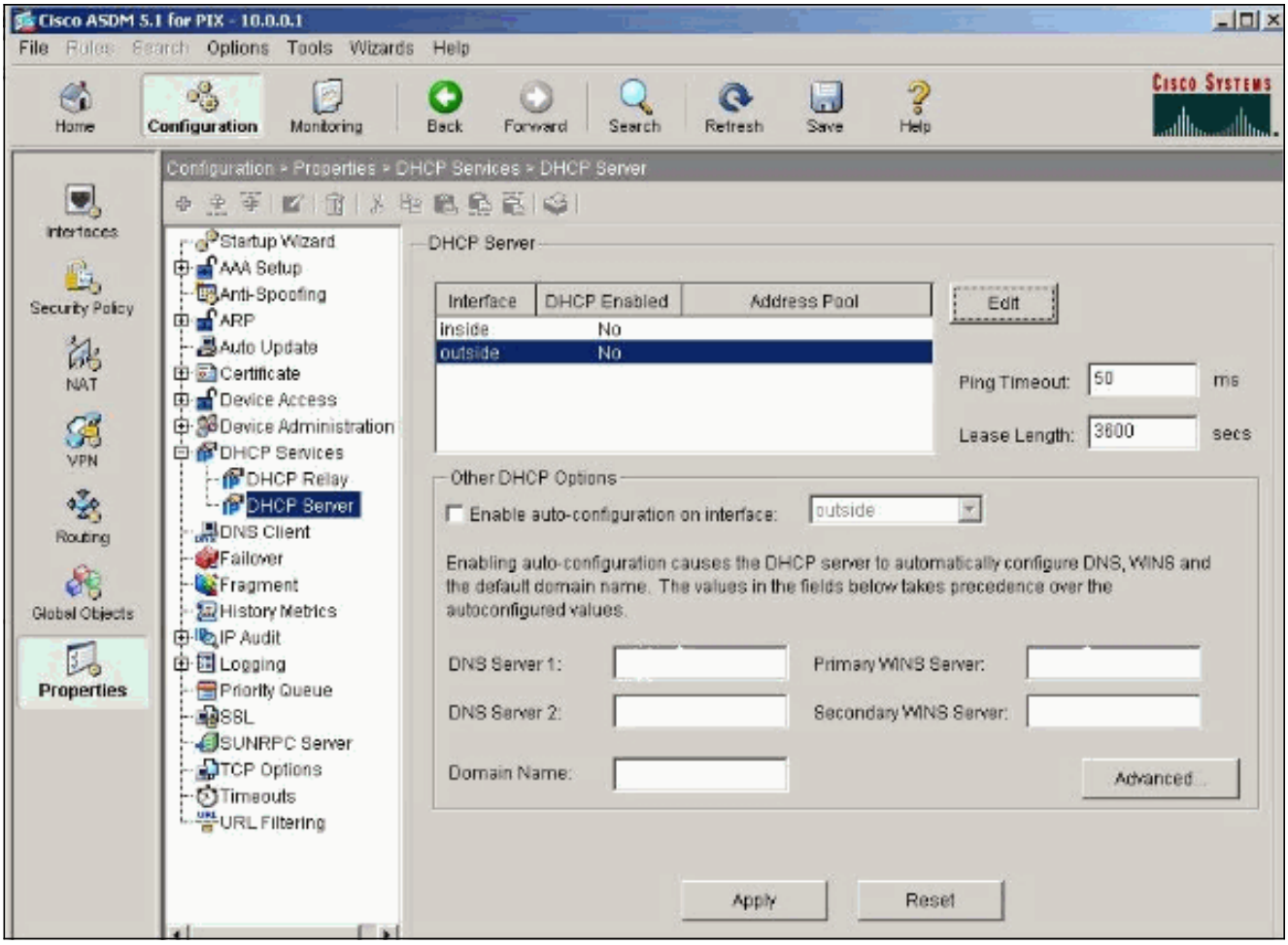
이 문서에서는 다음 구성을 사용합니다.

- ASDM을 사용하는 DHCP 서버 구성
- ASDM을 사용하는 DHCP 클라이언트 구성
- DHCP 서버 구성
- DHCP 클라이언트 구성

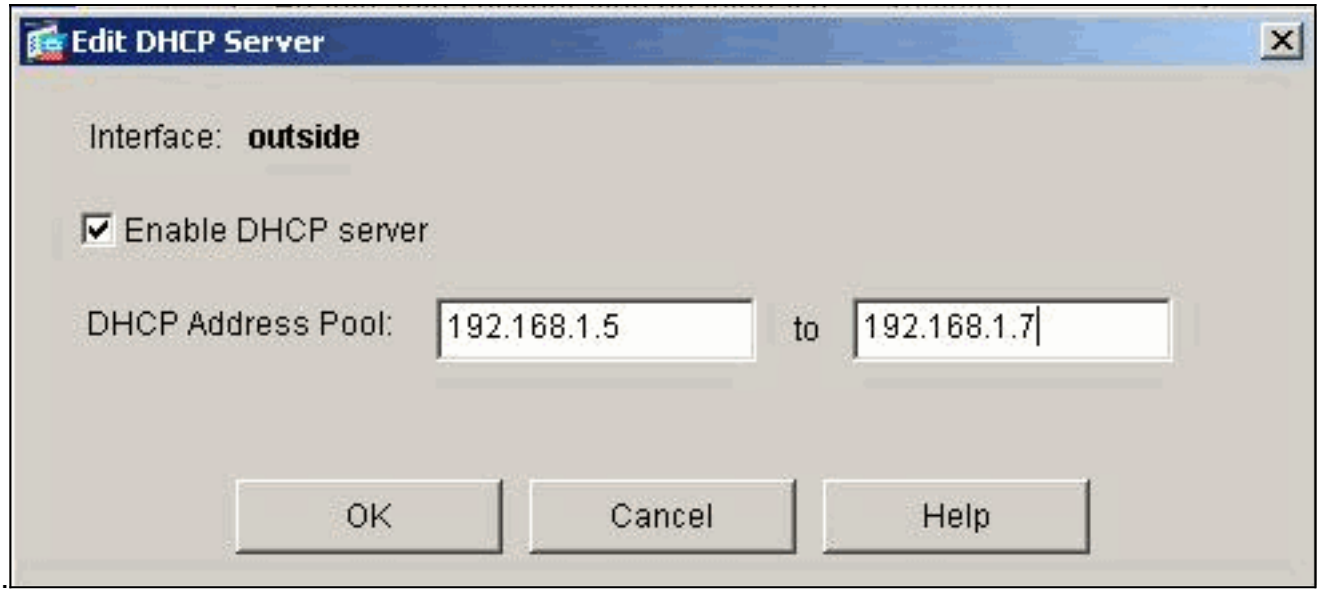
ASDM을 사용하는 DHCP 서버 구성

ASDM을 사용하여 PIX Security Appliance 또는 ASA를 DHCP 서버로 구성하려면 다음 단계를 완료합니다.

1. 홈 창에서 **Configuration > Properties > DHCP Services > DHCP Server**를 선택합니다.인터페이스를 선택하고 **Edit(편집)**를 클릭하여 DHCP 서버를 활성화하고 DHCP 주소 풀을 생성합니다.주소 풀은 보안 어플라이언스 인터페이스와 동일한 서브넷에 있어야 합니다.이 예에서는 DHCP 서버가 PIX Security Appliance의 외부 인터페이스에 구성됩니다
   .



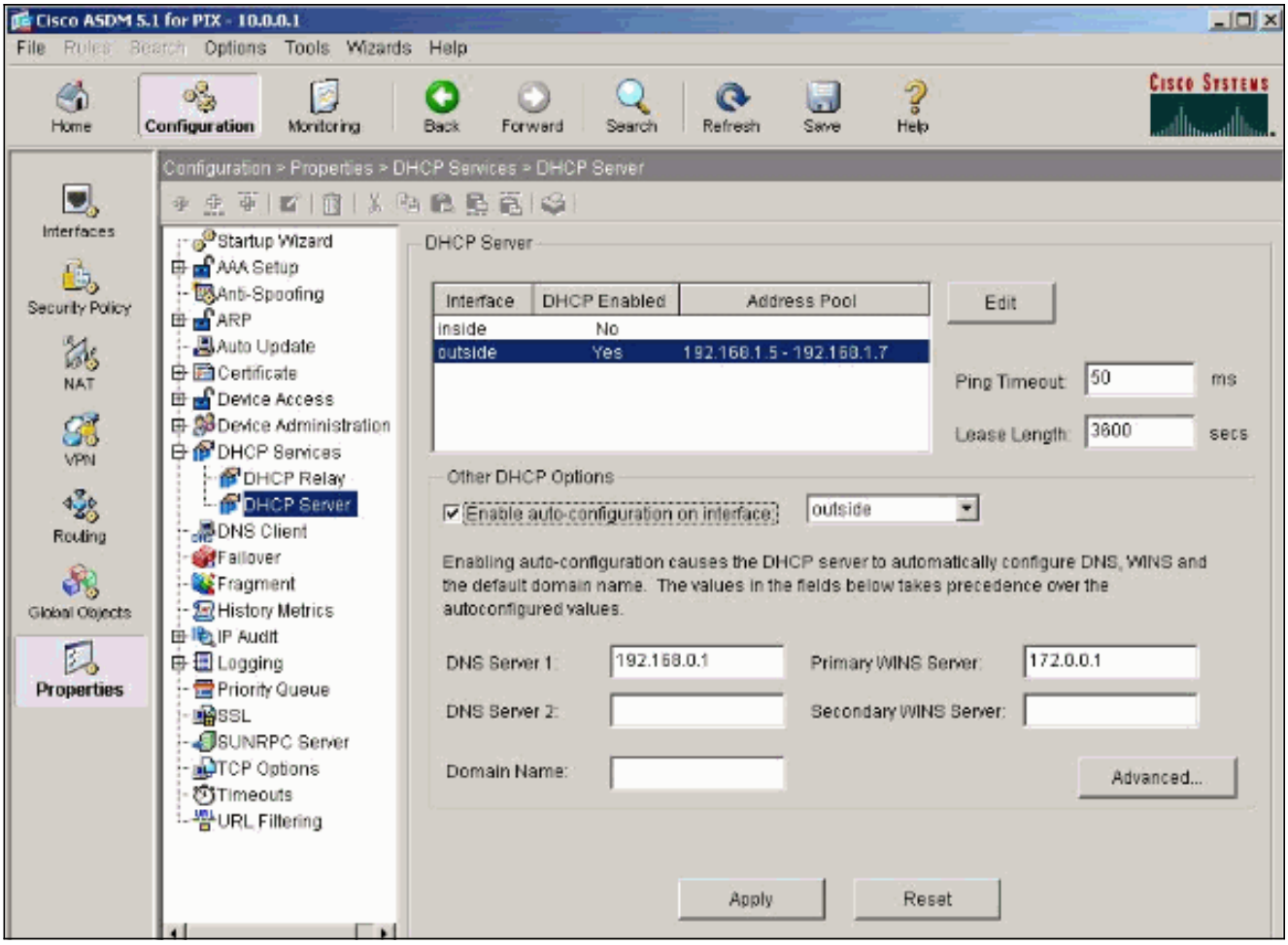
2. Enable **DHCP server** on the outside interface를 선택하여 DHCP 클라이언트의 요청을 수신합니다.DHCP 클라이언트에 발급될 주소 풀을 제공하고 **OK**를 클릭하여 Main 창으로 돌아갑니다



.

3. Enable auto-**configuration on the interface(인터페이스에서 자동 컨피그레이션 활성화)**를 선택하여 DHCP 서버가 DHCP 클라이언트의 DNS, WINS 및 기본 도메인 이름을 자동으로 구성합니다.Apply(**적용**)를 클릭하여 Security Appliance의 실행 중인 컨피그레이션을 업데이트합니다

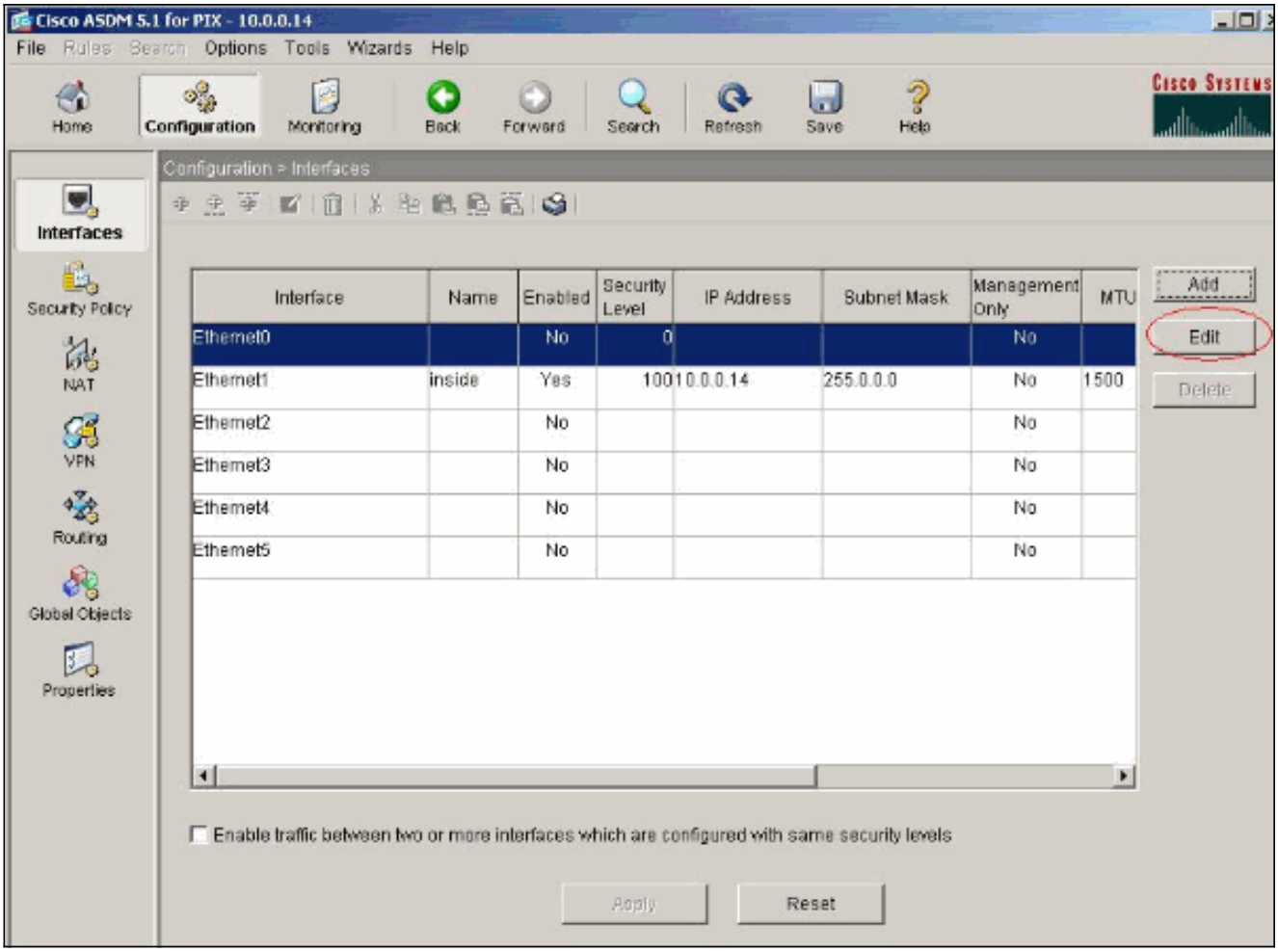
.



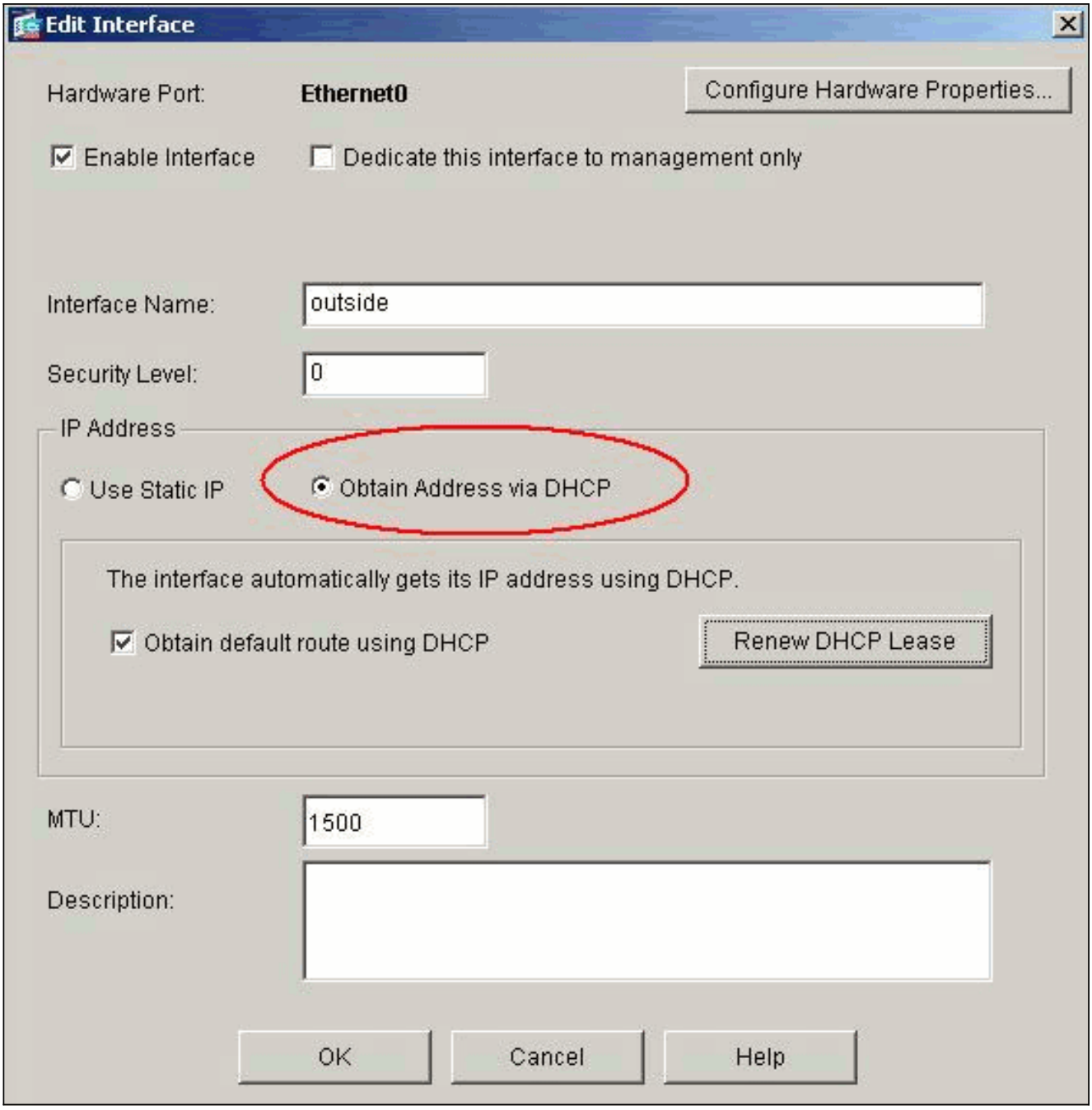
ASDM을 사용하는 DHCP 클라이언트 구성

ASDM을 사용하여 PIX Security Appliance를 DHCP 클라이언트로 구성하려면 다음 단계를 완료합니다.

1. Configuration **> Interfaces**를 선택하고 **Edit**를 클릭하여 Ethernet0 인터페이스가 DHCP 서버에서 서브넷 마스크, 기본 게이트웨이, DNS 서버 및 WINS 서버 IP 주소가 있는 IP 주소와 같은 컨피그레이션 매개변수를 얻도록 활성화합니다
   .

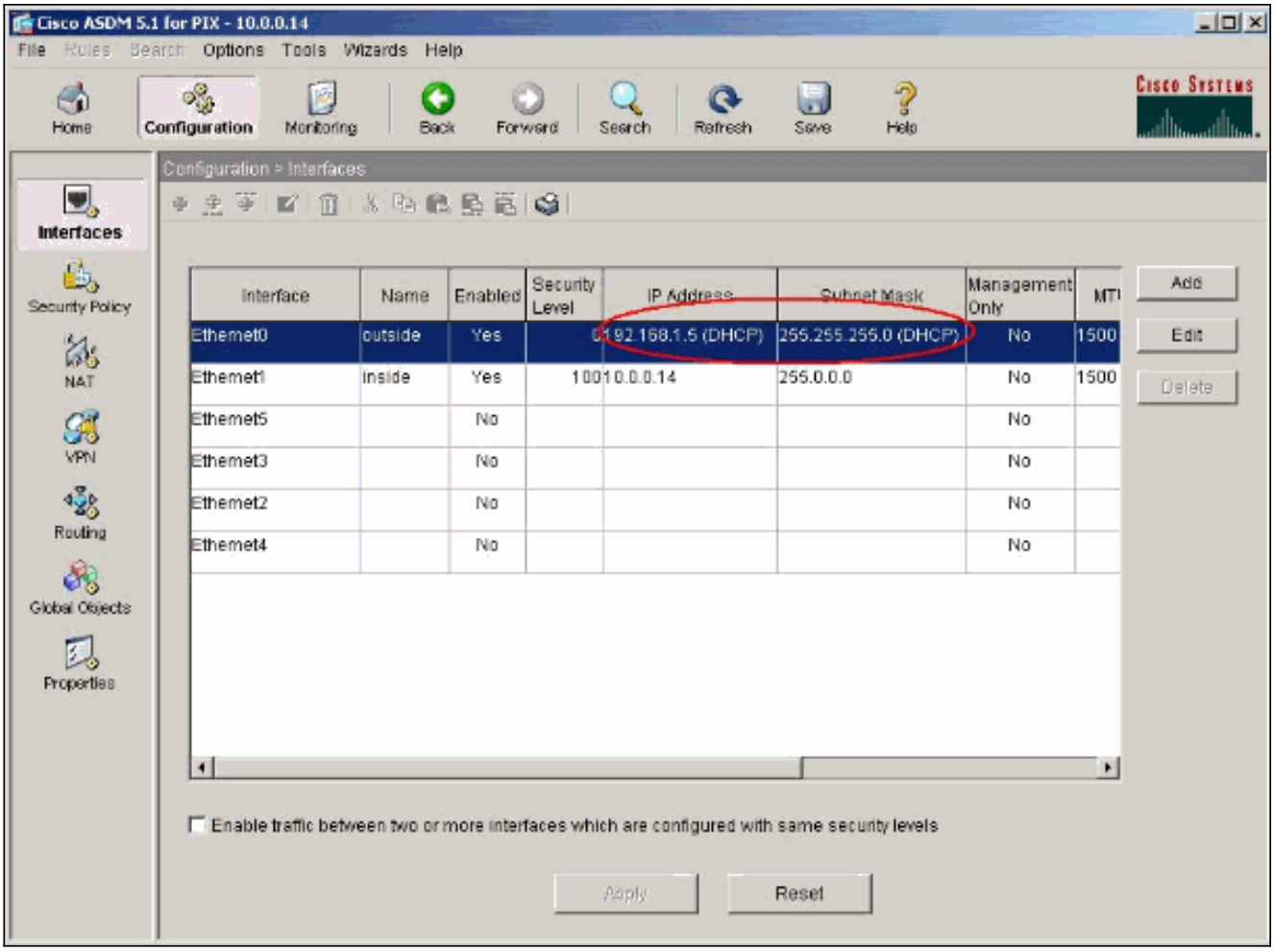


2. Enable **Interface**를 선택하고 인터페이스에 대한 Interface Name 및 Security Level을 입력합니다.Obtain **address via DHCP for the** IP address(IP 주소에 대해 DHCP를 통해 **주소 가져오기)** 및 **Obtain default gateway for the default gateway(기본 게이트웨이**에 DHCP를 사용하여 기본 경로 가져오기)를 선택한 다음 **OK(확인)를** 클릭하여 Main(기본) 창으로 이동합니다
.



3. Apply(**적용**)를 클릭하여 DHCP 서버에서 Ethernet0 인터페이스에 대해 얻은 IP 주소를 확인합니다

.



DHCP 서버 구성

이 컨피그레이션은 ASDM에서 생성합니다.

DHCP 서버

```
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 클라이언트 구성

이 컨피그레이션은 ASDM에서 생성합니다.

DHCP 클라이언트

```
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
```

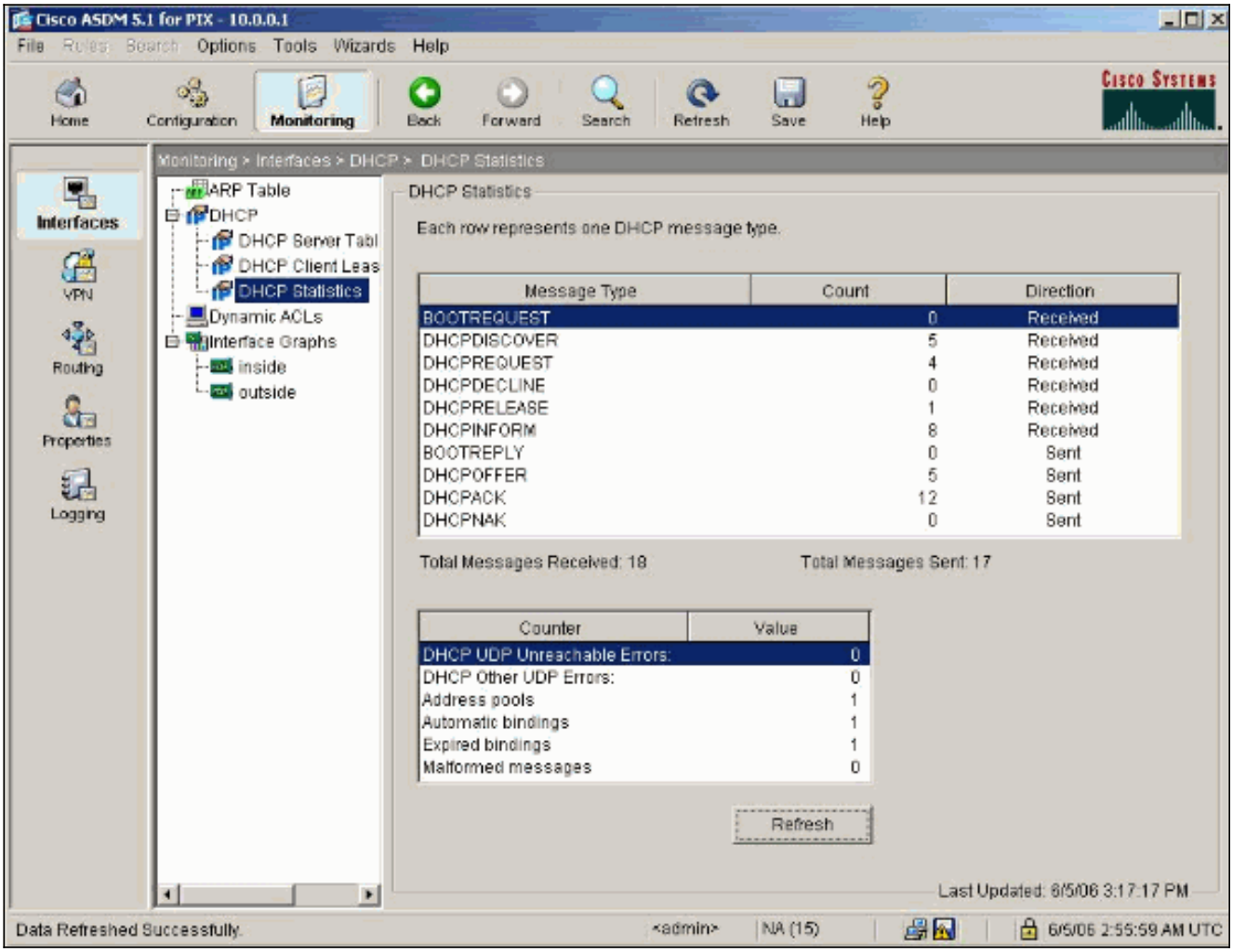
```
logging enable logging console debugging logging asdm
informational mtu outside 1500 mtu inside 1500 no
failover asdm image flash:/asdm-511.bin no asdm history
enable arp timeout 14400 timeout xlate 3:00:00 timeout
conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp
0:00:02 timeout sunrpc 0:10:00 h323 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
```

다음을 확인합니다.

ASDM을 사용하여 DHCP 서버 및 DHCP 클라이언트에서 DHCP 통계 및 바인딩 정보를 확인하려면 다음 단계를 완료하십시오.

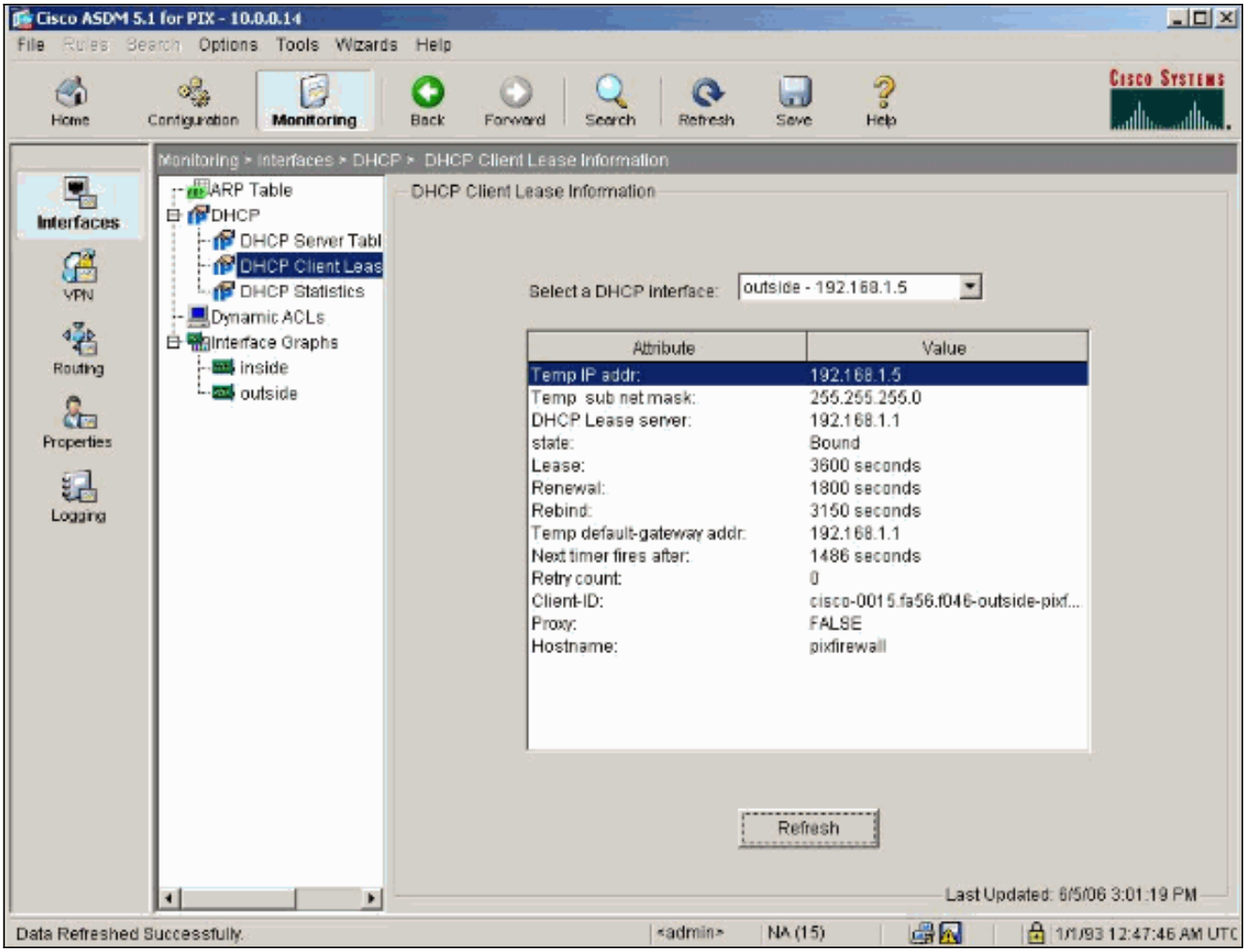
1. DHCP 서버에서 **Monitoring > Interfaces > DHCP > DHCP Statistics**를 선택하여 DHCP 통계를 확인합니다(예: DHCPDISCOVER, DHCPREQUEST, DHCPOFFER, DHCPACK).CLI에서 **show dhcpd statistics** 명령을 입력하여 DHCP 통계를 확인합니다

   .



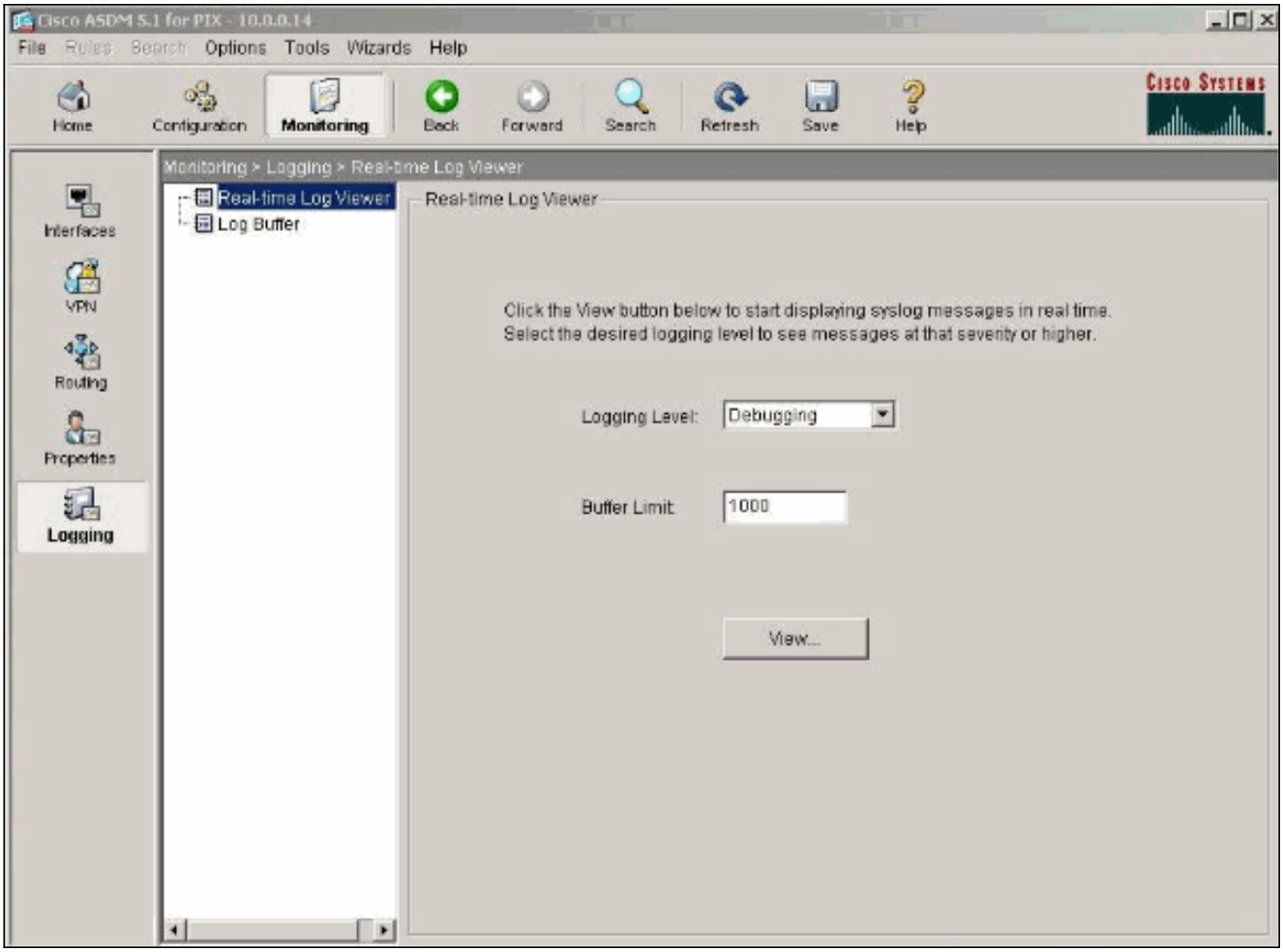
2. DHCP **바인딩** 정보를 보려면 DHCP 클라이언트에서 Monitoring > Interfaces > DHCP > DHCP Client Lease Information을 선택합니다.CLI에서 **DHCP 바인딩** 정보를 보려면 show dhcpd binding 명령을 입력합니다

   .



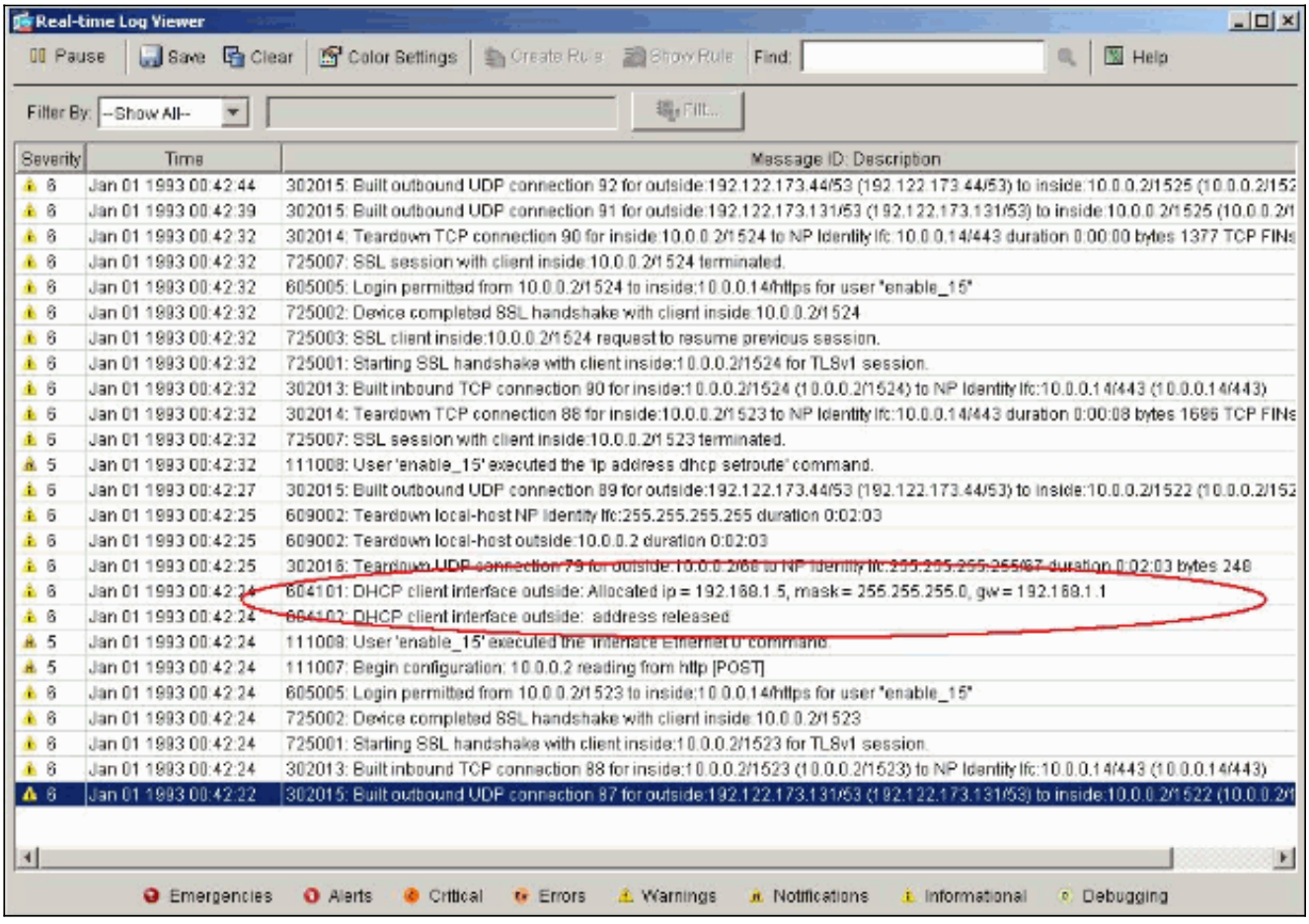
3. Monitoring(**모니터링) > Logging(로깅) > Real-time Log Viewer(실시간 로그 뷰어)**를 선택하여 Logging Level(로깅 레벨)과 버퍼 제한을 선택하여 Real Time Log 메시지를 확인합니다

.



4. DHCP 클라이언트에서 실시간 로그 이벤트를 봅니다.IP 주소는 DHCP 클라이언트의 외부 인터페이스에 할당됩니다

.



문제 해결

문제 해결 명령

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다.OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

참고: debug **명령**을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

- **debug dhcpd event** - DHCP 서버와 연결된 이벤트 정보를 표시합니다.
- **debug dhcpd packet** - DHCP 서버와 연결된 패킷 정보를 표시합니다.

오류 메시지

```
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
```

설명:주소 풀의 크기는 보안 어플라이언스의 풀당 256개의 주소로 제한됩니다.이는 변경할 수 없으며 소프트웨어 제한입니다.합계는 256만 가능합니다. 주소 풀 범위가 253개 주소(예: 254, 255, 256)보다 큰 경우 보안 어플라이언스 인터페이스의 넷마스크는 클래스 C 주소(예: 255.255.255.0)이 될 수 없습니다. 예를 들어 255.255.254.0과 같이 좀 더 큰 것이 필요합니다.

보안 어플라이언스에 DHCP 서버 기능을 구현하는 방법에 대한 자세한 내용은 Cisco Security Appliance 명령줄 컨피그레이션 가이드를 참조하십시오.

FAQ:주소 할당

질문 - ASA를 DHCP 서버로 사용하는 컴퓨터에 고정/영구 IP 주소를 할당할 수 있습니까?

대답 - PIX/ASA를 사용할 수 없습니다.

질문 - DHCP 주소를 ASA의 특정 MAC 주소와 연결할 수 있습니까?

응답 - 아니요, 불가능합니다.

관련 정보

- PIX Security Appliance 지원 페이지
- Cisco Secure PIX Firewall 명령 참조
- 기술 지원 및 문서 – Cisco Systems