Konfigurationsbeispiel für einen DHCP-Server und einen Client mit PIX/ASA

Inhalt

Einführung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Zugehörige Produkte
Konventionen
Konfigurieren
DHCP-Serverkonfiguration mit ASDM
DHCP-Client-Konfiguration mit ASDM
DHCP-Serverkonfiguration
DHCP-Client-Konfiguration
Überprüfen
Fehlerbehebung
Befehle zur Fehlerbehebung
Fehlermeldungen
Häufig gestellte Fragen: Adressenzuweisung
Zugehörige Informationen

Einführung

Die Sicherheitslösung der Serie PIX 500 und die Cisco Adaptive Security Appliance (ASA) unterstützen sowohl als DHCP-Server (Dynamic Host Configuration Protocol) als auch als DHCP-Clients. DHCP ist ein Protokoll, das automatisch Konfigurationsparameter wie eine IP-Adresse mit einer Subnetzmaske, einem Standard-Gateway, einem DNS-Server und einer IP-Adresse des WINS-Servers für Hosts bereitstellt.

Die Sicherheits-Appliance kann als DHCP-Server oder DHCP-Client fungieren. Wenn die Sicherheits-Appliance als Server fungiert, stellt sie Netzwerkkonfigurationsparameter direkt für DHCP-Clients bereit. Wenn die Sicherheits-Appliance als DHCP-Client betrieben wird, werden diese Konfigurationsparameter von einem DHCP-Server angefordert.

In diesem Dokument wird erläutert, wie der DHCP-Server und der DHCP-Client mithilfe des Cisco Adaptive Security Device Manager (ASDM) auf der Security Appliance konfiguriert werden.

Voraussetzungen

Anforderungen

In diesem Dokument wird davon ausgegangen, dass die PIX Security Appliance oder ASA voll betriebsbereit und konfiguriert ist, damit der Cisco ASDM Konfigurationsänderungen vornehmen kann.

Hinweis: Unter Zulassen von HTTPS-Zugriff für ASDM wird die Konfiguration des Geräts durch den ASDM beschrieben.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Security Appliance der Serie PIX 500 7.x**Hinweis:** Die in Version 7.x verwendete PIX-CLI-Konfiguration gilt auch für PIX 6.x. Der einzige Unterschied besteht darin, dass der DHCP-Server in Versionen vor PIX 6.3 nur auf der internen Schnittstelle aktiviert werden kann. In PIX 6.3 und höher kann der DHCP-Server auf allen verfügbaren Schnittstellen aktiviert werden. In dieser Konfiguration wird die externe Schnittstelle für die DHCP-Serverfunktion verwendet.
- ASDM 5.x**Hinweis:** ASDM unterstützt nur PIX 7.0 und höher. Der PIX Device Manager (PDM) ist für die Konfiguration der PIX-Version 6.x verfügbar. Weitere Informationen zur Hardware- und Softwarekompatibilität von Sicherheitsgeräten der Serien Cisco ASA 5500 und PIX 500 finden Sie.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Zugehörige Produkte

Diese Konfiguration kann auch mit Cisco ASA 7.x verwendet werden.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Konfigurieren

In dieser Konfiguration gibt es zwei PIX Security Appliances, die Version 7.x ausführen. Ein Server fungiert als DHCP-Server, der Konfigurationsparameter für eine andere PIX Security Appliance 7.x bereitstellt, die als DHCP-Client fungiert. Wenn es als DHCP-Server fungiert, weist das PIX DHCP-Clients aus einem Pool von zugewiesenen IP-Adressen dynamisch IP-Adressen zu.

Sie können auf jeder Schnittstelle der Sicherheits-Appliance einen DHCP-Server konfigurieren. Jede Schnittstelle kann über einen eigenen Adresspool verfügen, aus dem Sie schöpfen können. Die anderen DHCP-Einstellungen wie DNS-Server, Domänenname, Optionen, Ping-Timeout und WINS-Server werden jedoch global konfiguriert und vom DHCP-Server auf allen Schnittstellen verwendet.

Sie können einen DHCP-Client oder DHCP-Relay-Dienste nicht auf einer Schnittstelle

konfigurieren, auf der der Server aktiviert ist. Zusätzlich müssen DHCP-Clients direkt mit der Schnittstelle verbunden werden, auf der der Server aktiviert ist.

Während der DHCP-Server auf einer Schnittstelle aktiviert ist, können Sie die IP-Adresse dieser Schnittstelle nicht ändern.

Hinweis: Grundsätzlich gibt es keine Konfigurationsoption, um die Standard-Gateway-Adresse in der DHCP-Antwort festzulegen, die vom DHCP-Server (PIX/ASA) gesendet wird. Der DHCP-Server sendet immer seine eigene Adresse als Gateway für den DHCP-Client. Durch die Definition einer Standardroute, die auf den Internet-Router verweist, kann der Benutzer jedoch auf das Internet zugreifen.

Hinweis: Die Anzahl der DHCP-Pool-Adressen, die zugewiesen werden können, hängt von der in der Security Appliance (PIX/ASA) verwendeten Lizenz ab. Wenn Sie die Base/Security Plus-Lizenz verwenden, gelten diese Beschränkungen für den DHCP-Pool. Wenn der Host-Grenzwert 10 Hosts beträgt, beschränken Sie den DHCP-Pool auf 32 Adressen. Wenn der Host-Grenzwert 50 Hosts beträgt, beschränken Sie den DHCP-Pool auf 128 Adressen. Wenn das Hostlimit unbegrenzt ist, beschränken Sie den DHCP-Pool auf 256 Adressen. Daher ist der Adresspool abhängig von der Anzahl der Hosts begrenzt.

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

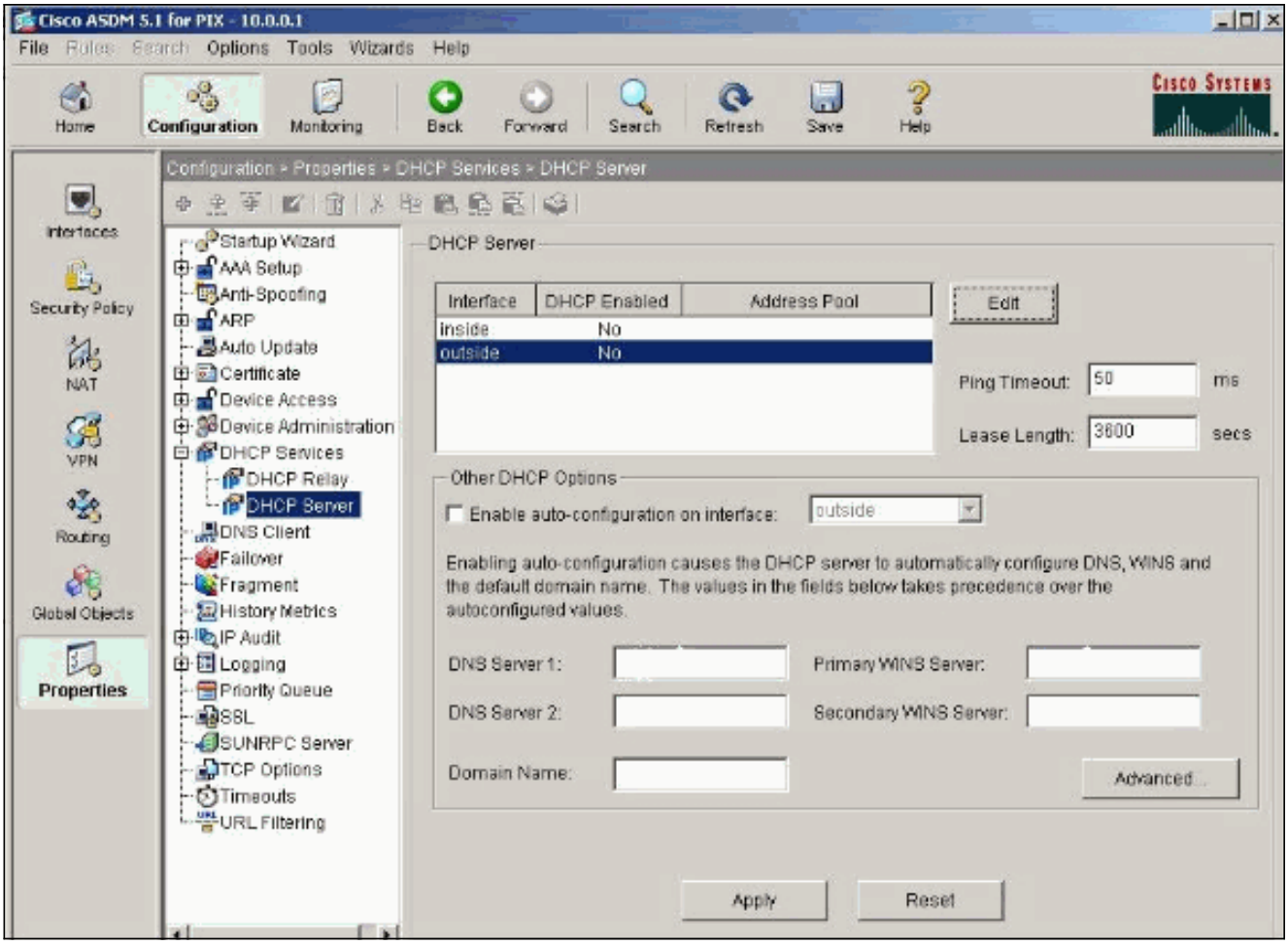
In diesem Dokument werden folgende Konfigurationen verwendet:

- DHCP-Serverkonfiguration mit ASDM
- DHCP-Client-Konfiguration mit ASDM
- DHCP-Serverkonfiguration
- DHCP-Client-Konfiguration

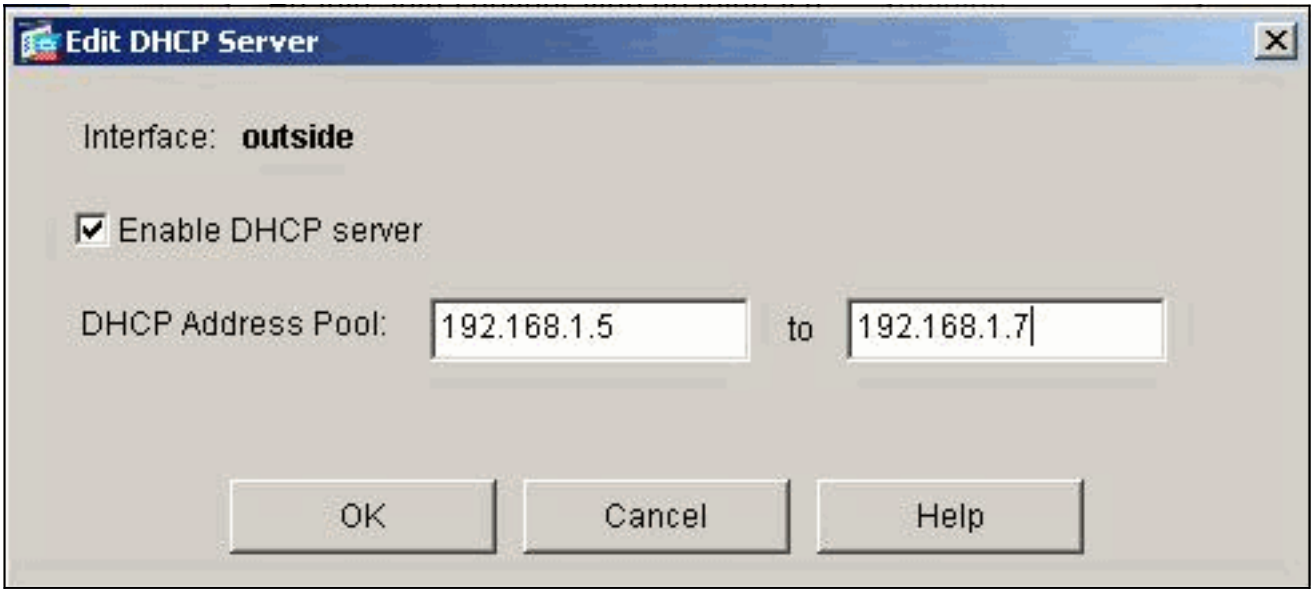
DHCP-Serverkonfiguration mit ASDM

Führen Sie diese Schritte aus, um die PIX Security Appliance oder ASA als DHCP-Server mithilfe von ASDM zu konfigurieren.

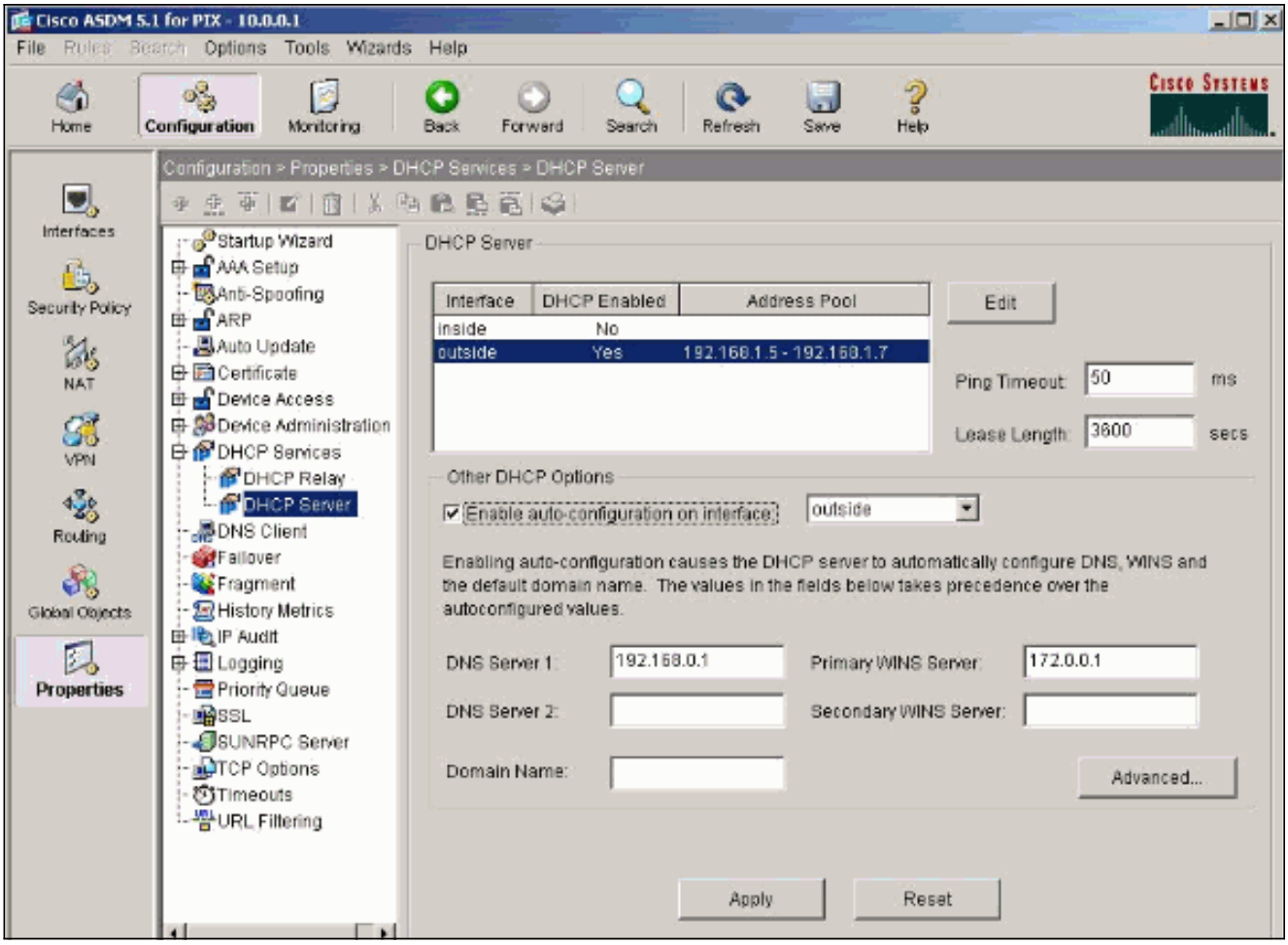
1. Wählen Sie im Hauptfenster **Konfiguration > Eigenschaften > DHCP-Dienste > DHCP-Server** aus. Wählen Sie eine Schnittstelle aus, und klicken Sie auf **Bearbeiten**, um den DHCP-Server zu aktivieren und einen DHCP-Adresspool zu erstellen.Der Adresspool muss sich im gleichen Subnetz wie die Security Appliance-Schnittstelle befinden. In diesem Beispiel wird der DHCP-Server auf der externen Schnittstelle der PIX Security Appliance konfiguriert.



2. Aktivieren Sie **DHCP-Server** auf der externen Schnittstelle **aktivieren**, um die Anfragen der DHCP-Clients zu überwachen. Geben Sie den Adresspool an, der dem DHCP-Client zugewiesen werden soll, und klicken Sie auf **OK**, um zum Hauptfenster zurückzukehren.



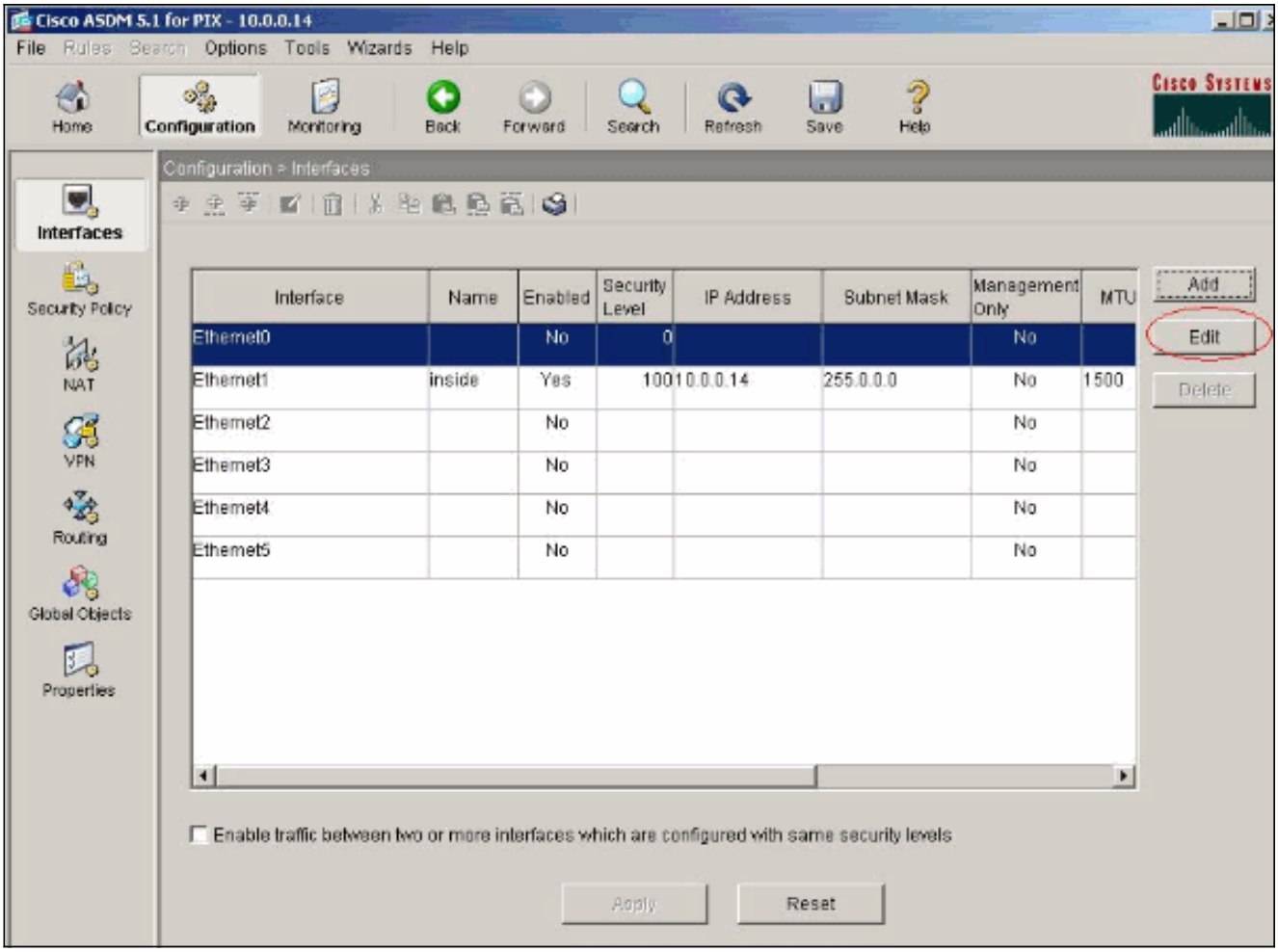
3. Aktivieren Sie **die Option Autokonfiguration auf der Schnittstelle aktivieren**, damit der DHCP-Server den DNS, WINS und den Standard-Domänennamen für den DHCP-Client automatisch konfiguriert. Klicken Sie auf **Apply**, um die aktuelle Konfiguration der Sicherheits-Appliance zu aktualisieren.



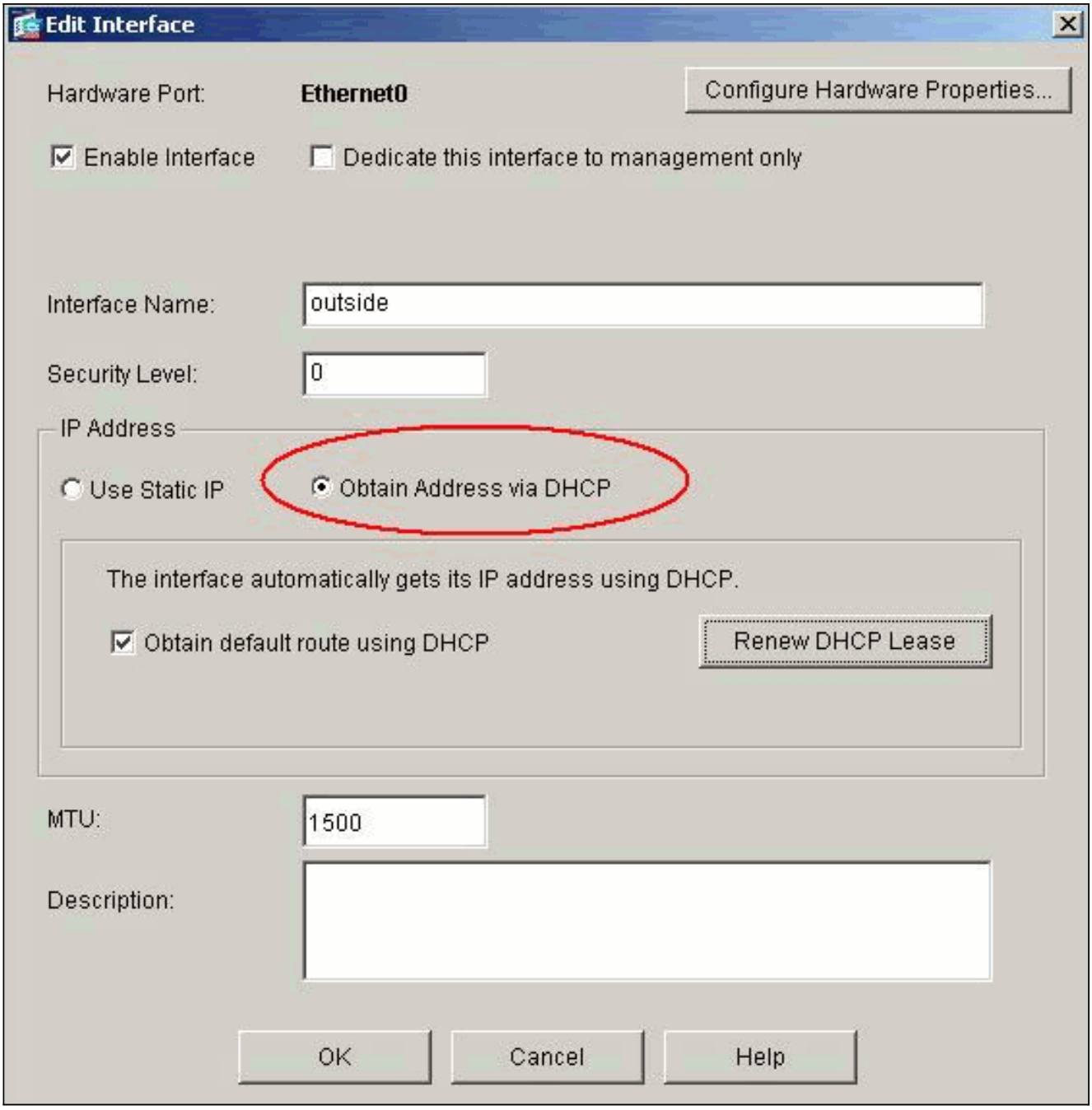
DHCP-Client-Konfiguration mit ASDM

Führen Sie diese Schritte aus, um die PIX Security Appliance als DHCP-Client mithilfe von ASDM zu konfigurieren.

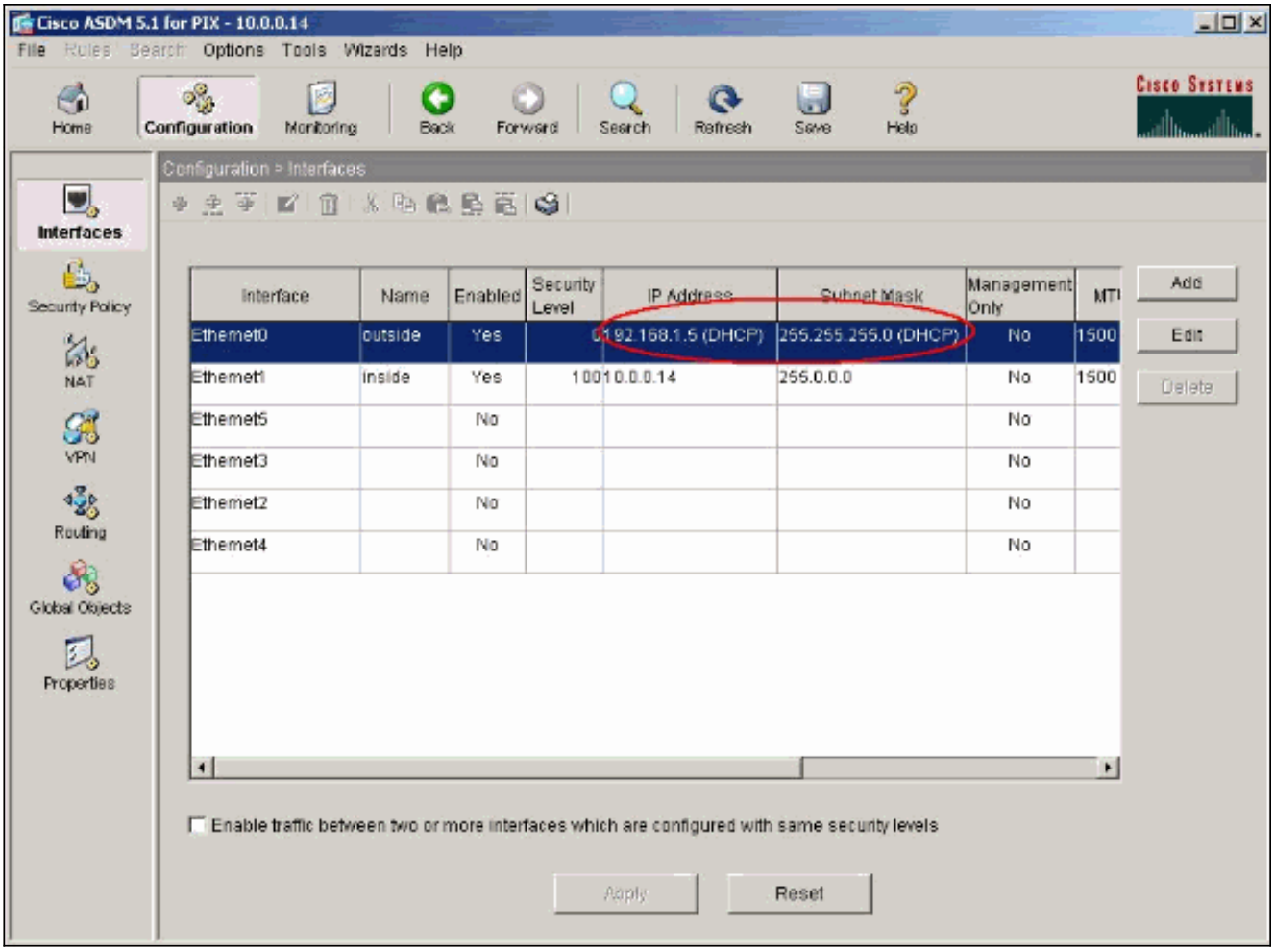
1. Wählen Sie **Configuration > Interfaces (Konfiguration > Schnittstellen) aus,** und klicken Sie auf **Edit**, um die Ethernet0-Schnittstelle so zu aktivieren, dass sie die Konfigurationsparameter wie eine IP-Adresse mit Subnetzmaske, Standard-Gateway, DNS-Server- und WINS-Server-IP-Adresse vom DHCP-Server abruft.



2. Aktivieren Sie **Enable Interface (Schnittstelle aktivieren)**, und geben Sie den Schnittstellennamen und die Sicherheitsstufe für die Schnittstelle ein. Wählen Sie **Adresse über DHCP** für die IP-Adresse **beziehen** und **Standardroute über DHCP** für das Standard-Gateway **beziehen** und klicken Sie dann auf **OK**, um zum Hauptfenster zu gelangen.



3. Klicken Sie auf **Apply**, um die IP-Adresse anzuzeigen, die vom DHCP-Server für die Ethernet0-Schnittstelle abgerufen
wurde.



DHCP-Serverkonfiguration

Diese Konfiguration wird vom ASDM erstellt:

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-Konfiguration

Diese Konfiguration wird vom ASDM erstellt:

DHCP-Client

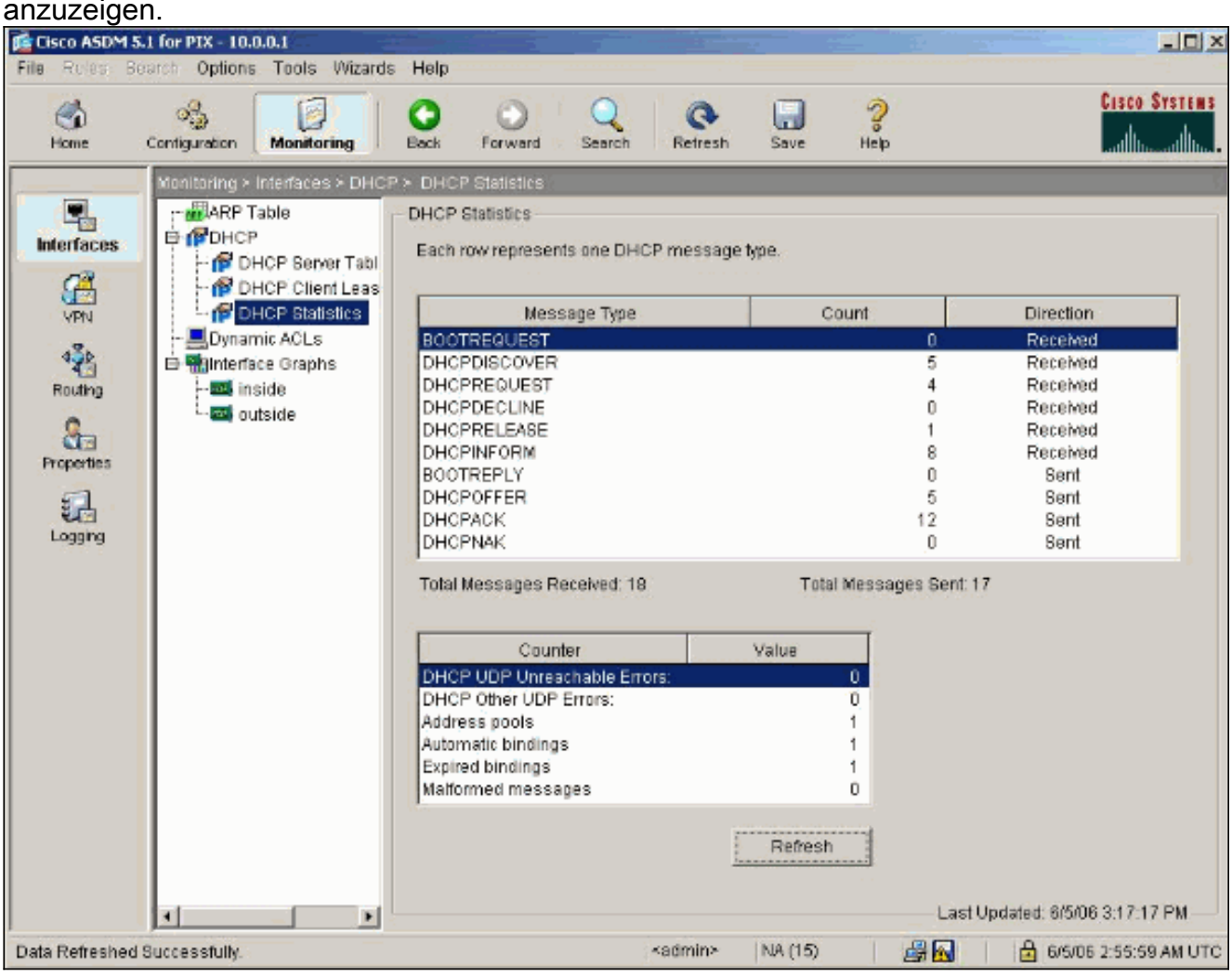
```
pixfirewall#show running-config
PIX Version 7.1(1)
!
hostname pixfirewall
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0
 nameif outside
 security-level 0

!--- 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
```

Überprüfen

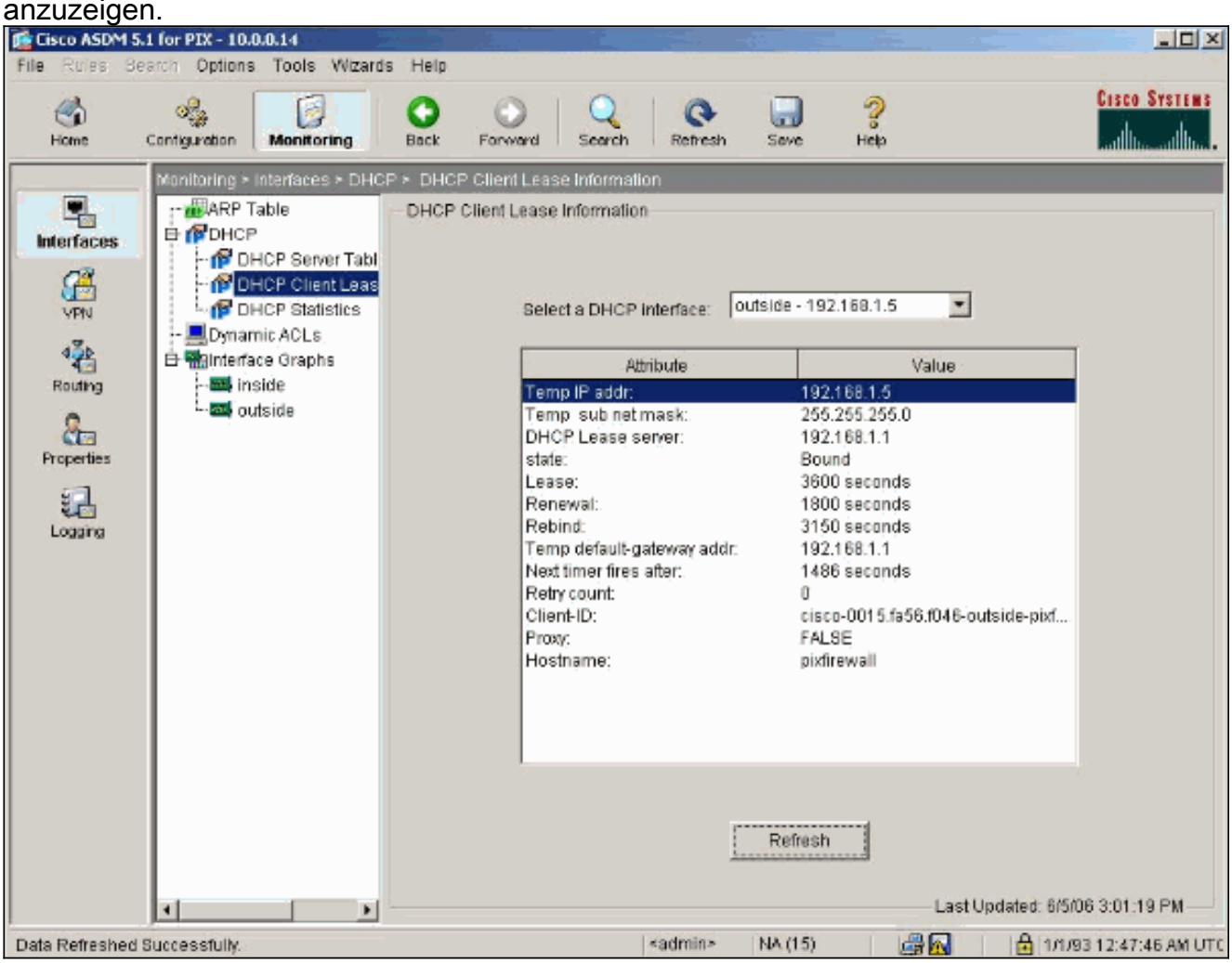
Führen Sie diese Schritte aus, um die DHCP-Statistiken und die Bindungsinformationen vom DHCP-Server und DHCP-Client mithilfe von ASDM zu überprüfen.

1. Wählen Sie **Monitoring > Interfaces > DHCP > DHCP Statistics** vom DHCP-Server aus, um die DHCP-Statistiken wie DHCPDISCOVER, DHCPREQUEST, DHCPOFFER und DHCPACK zu überprüfen.Geben Sie den Befehl **show dhcpd statistics** aus der CLI ein, um die DHCP-Statistiken
anzuzeigen.

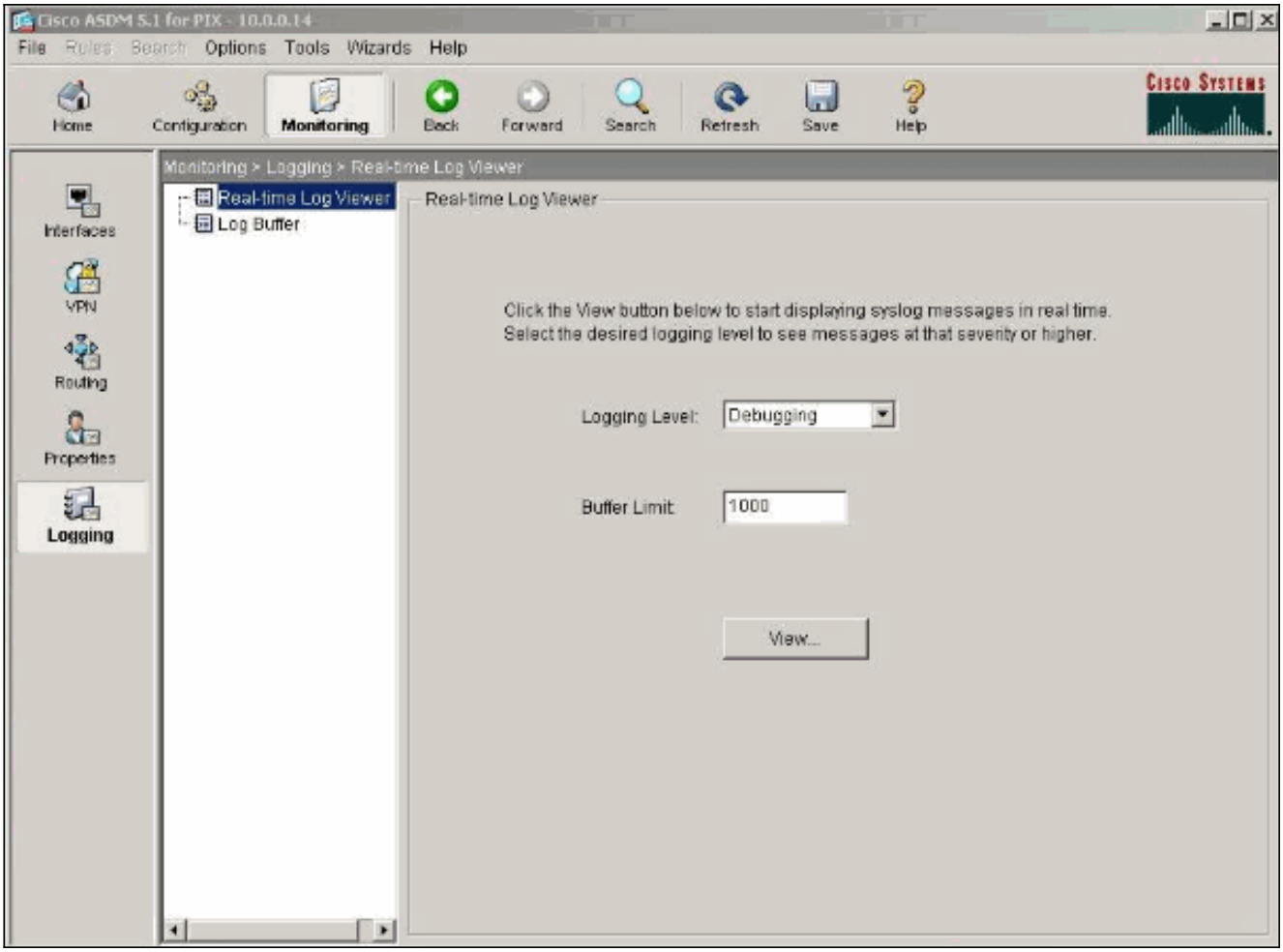


2. Wählen Sie **Monitoring > Interfaces > DHCP > DHCP Client Lease Information** (**Überwachung > Schnittstellen > DHCP > DHCP Client Lease Information**) vom DHCP-Client aus, um die DHCP-Bindungsinformationen anzuzeigen.Geben Sie den Befehl **show dhcpd binding** ein, um die DHCP-Bindungsinformationen aus der CLI

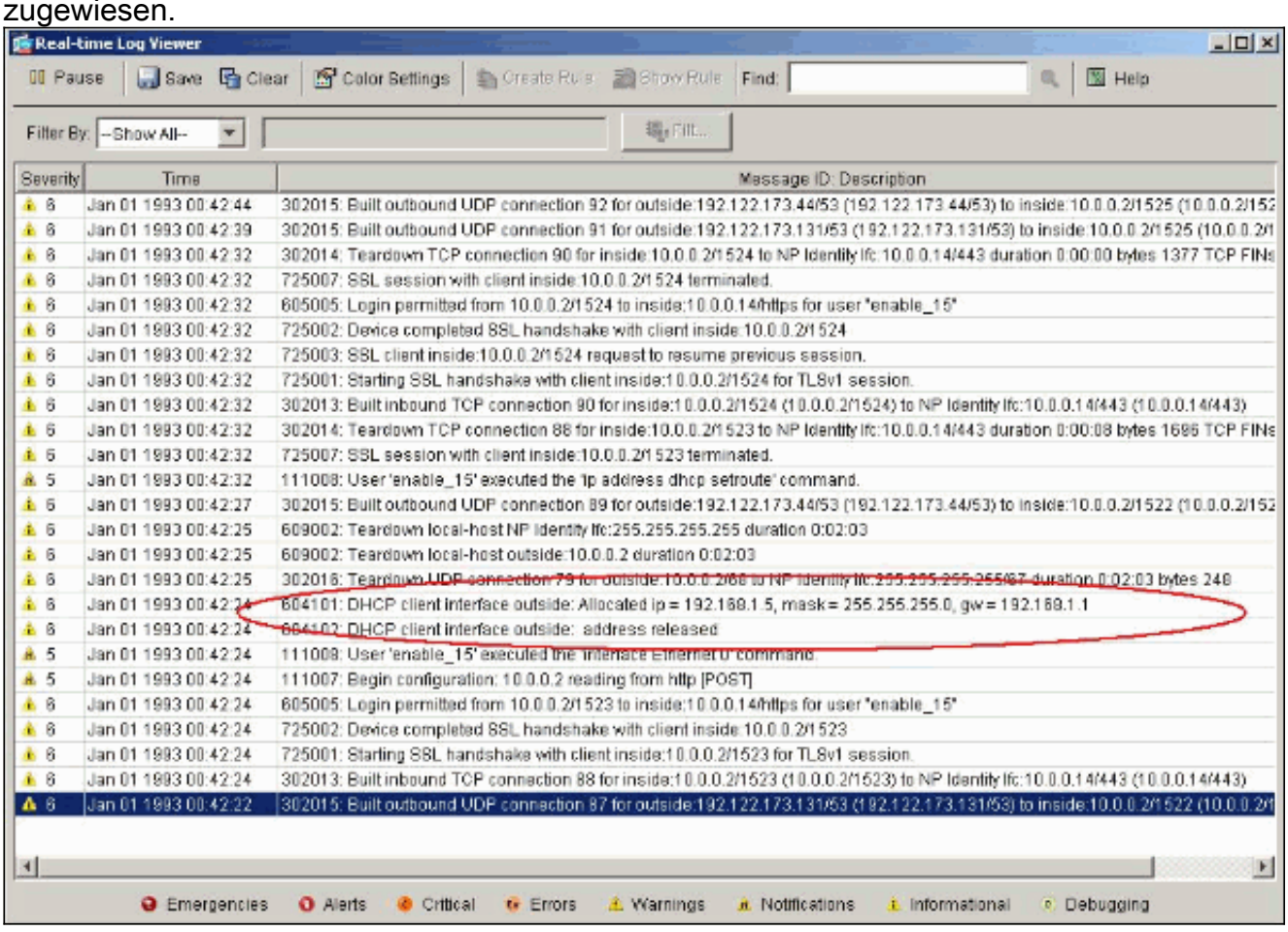
anzuzeigen.



3. Wählen Sie **Monitoring > Logging > Real-time Log Viewer** aus, um die Protokollierungsebene und die Puffergrenze für die Anzeige der Real-Time Log-Meldungen auszuwählen.



4. Zeigen Sie die Echtzeit-Protokollereignisse vom DHCP-Client aus an. Die IP-Adresse ist der externen Schnittstelle des DHCP-Clients zugewiesen.



Fehlerbehebung

Befehle zur Fehlerbehebung

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

Hinweis: Beachten Sie vor der Verwendung von **Debug-**Befehlen die Informationen zu Debug-Befehlen.

- **debug dhcpd event** (**dhcpd-Ereignis debug**): Zeigt Ereignisinformationen an, die dem DHCP-Server zugeordnet sind.
- **debug dhcpd packet**: Zeigt Paketinformationen an, die dem DHCP-Server zugeordnet sind.

Fehlermeldungen

```
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
```

Erläuterung: Die Größe des Adresspools ist auf 256 Adressen pro Pool auf der Sicherheits-Appliance beschränkt. Dies kann nicht geändert werden und ist eine Softwarebeschränkung. Die Gesamtzahl kann nur 256 betragen. Wenn der Adresspoolbereich größer als 253 Adressen ist (z. B. 254, 255, 256), darf die Netzmaske der Security Appliance-Schnittstelle keine Class C-Adresse sein (z. B. 255.255.255.0). Es muss etwas Größeres sein, zum Beispiel 255.255.254.0.

Weitere Informationen zur Implementierung der DHCP-Serverfunktion in die Sicherheits-Appliance finden Sie im Cisco Security Appliance Command Line Configuration Guide.

Häufig gestellte Fragen: Adressenzuweisung

Frage - Ist es möglich, dem Computer, der ASA als DHCP-Server verwendet, eine statische/permanente IP-Adresse zuzuweisen?

Antwort: PIX/ASA ist nicht möglich.

Frage - Ist es möglich, DHCP-Adressen mit bestimmten MAC-Adressen auf ASA zu verknüpfen?

Antwort: Nein, es ist nicht möglich.

Zugehörige Informationen

- Support-Seite für PIX Security Appliance
- Cisco Secure PIX Firewall - Befehlsreferenzen
- Technischer Support und Dokumentation - Cisco Systems