PIX/ASA als voorbeeld van een DHCP-server en clientconfiguratie

Inhoud

Inleiding
Voorwaarden
Vereisten
Gebruikte componenten
Verwante producten
Conventies
Configureren
DHCP-serverconfiguratie met ASDM
DHCP-clientconfiguratie met ASDM
DHCP-serverconfiguratie
DHCP-clientconfiguratie
Verifiëren
Problemen oplossen
Opdrachten voor probleemoplossing
Foutberichten
FAQ: Toewijzing van adres
Gerelateerde informatie

Inleiding

De PIX 500 Series security applicatie en Cisco adaptieve security applicatie (ASA) ondersteunen die werken als Dynamic Host Configuration Protocol (DHCP)-servers en DHCP-clients. DHCP is een protocol dat automatische configuratieparameters zoals een IP-adres met een subnetmasker, standaardgateway, DNS-server en WINS server IP-adres aan hosts levert.

De security applicatie kan fungeren als een DHCP-server of een DHCP-client. Wanneer het als een server werkt, verstrekt de Security applicatie netwerkconfiguratieparameters direct aan DHCP-clients. Wanneer het als een DHCP-client werkt, vraagt de Security applicatie dergelijke configuratieparameters vanaf een DHCP-server.

Dit document concentreert zich op de manier waarop u de DHCP-server en DHCP-client kunt configureren met behulp van Cisco Adaptieve Security Devices Manager (ASDM) op de Security applicatie.

Voorwaarden

Vereisten

Dit document gaat ervan uit dat de PIX security applicatie of ASA volledig gebruiksklaar is en geconfigureerd om Cisco ASDM in staat te stellen om configuratiewijzigingen door te voeren.

Opmerking: Raadpleeg HTTPS Access voor ASDM om het apparaat door ASDM te laten configureren.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- PIX 500 Series security applicatie 7.x**Opmerking:** De PIX CLI-configuratie gebruikt in versie 7.x is ook van toepassing op PIX 6.x. Het enige verschil is dat in versies eerder dan PIX 6.3 de DHCP-server alleen op de interne interface ingeschakeld kan worden. In PIX 6.3 en later kan de DHCP-server worden ingeschakeld op een van de beschikbare interfaces. In deze configuratie wordt de externe interface gebruikt voor de DHCP-serverfunctie.
- ASDM 5.x**Opmerking:** ASDM ondersteunt PIX 7.0 en hoger. PIX Apparaat Manager (PDM) is beschikbaar om PIX versie 6.x te configureren. Raadpleeg Cisco ASA 5500 Series en PIX 500 Series security applicatie, hardware en software-compatibiliteit voor meer informatie.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Verwante producten

Deze configuratie kan ook worden gebruikt met Cisco ASA 7.x.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Configureren

In deze configuratie zijn er twee PIX security applicaties die versie 7.x uitvoeren. Een functioneert als een DHCP-server die configuratieparameters biedt voor een andere PIX security applicatie 7.x die werkt als een DHCP-client. Wanneer het als een DHCP-server functioneert, kent PIX dynamisch IP-adressen toe aan DHCP-clients vanuit een pool van aangewezen IP-adressen.

U kunt een DHCP-server configureren op elke interface van de security applicatie. Elke interface kan een eigen pool van adressen hebben om uit te tekenen. Maar de andere DHCP-instellingen, zoals DNS-servers, domeinnaam, opties, ping-out en WINS-servers worden mondiaal geconfigureerd en op alle interfaces gebruikt door de DHCP-server.

U kunt geen DHCP-client of DHCP-relais instellen op een interface waarop de server is ingeschakeld. Daarnaast moeten DHCP-clients rechtstreeks worden aangesloten op de interface waarop de server is ingeschakeld.

Tenslotte, terwijl de DHCP-server op een interface is ingeschakeld, kunt u het IP-adres van die interface niet wijzigen.

Opmerking: Er is eigenlijk geen configuratieoptie om het standaardgateway-adres in het DHCP-antwoord in te stellen dat vanuit de DHCP-server (PIX/ASA) wordt verzonden. De DHCP-server stuurt altijd zijn eigen adres als gateway voor de DHCP-client. Echter, het bepalen van een standaardroute die aan de router van Internet wijst staat de gebruiker toe om het internet te bereiken.

Opmerking: Het aantal DHCP-pooladressen dat kan worden toegewezen, is afhankelijk van de licentie die wordt gebruikt in de Security Appliance (PIX/ASA). Als u de Base/Security Plus-licentie gebruikt, gelden deze limieten voor de DHCP-pool. Als de Host Limiet 10 hosts is, beperkt u de DHCP-pool tot 32 adressen. Als de Host Limiet 50 hosts is, beperkt u de DHCP-pool tot 128 adressen. Als de Host Limiet onbeperkt is, beperkt u de DHCP-pool tot 256 adressen. De adrespool is dus beperkt op basis van het aantal hosts.

Opmerking: Gebruik het Opname Gereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

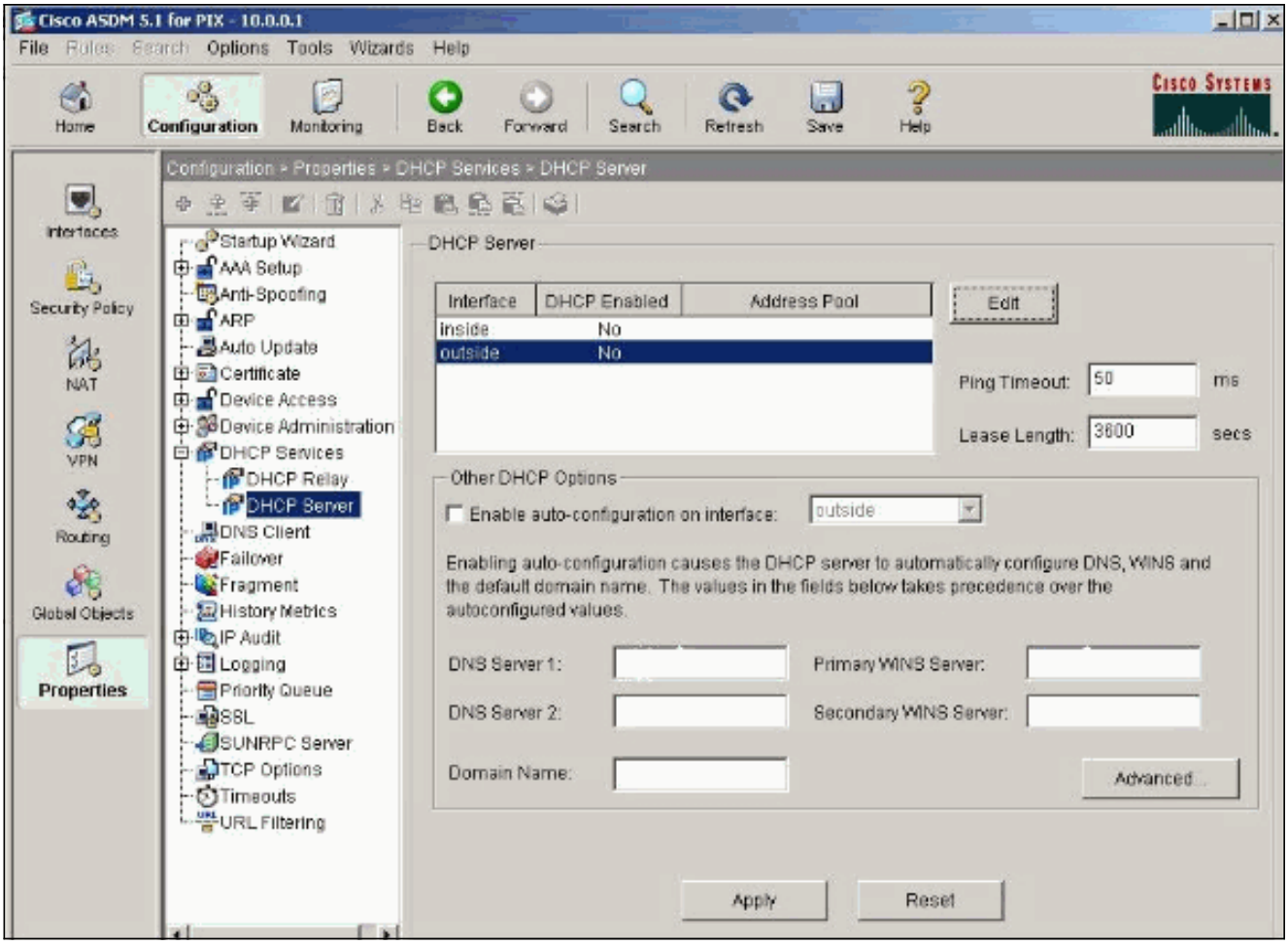
Dit document gebruikt deze configuraties:

- DHCP-serverconfiguratie met ASDM
- DHCP-clientconfiguratie met ASDM
- DHCP-serverconfiguratie
- DHCP-clientconfiguratie

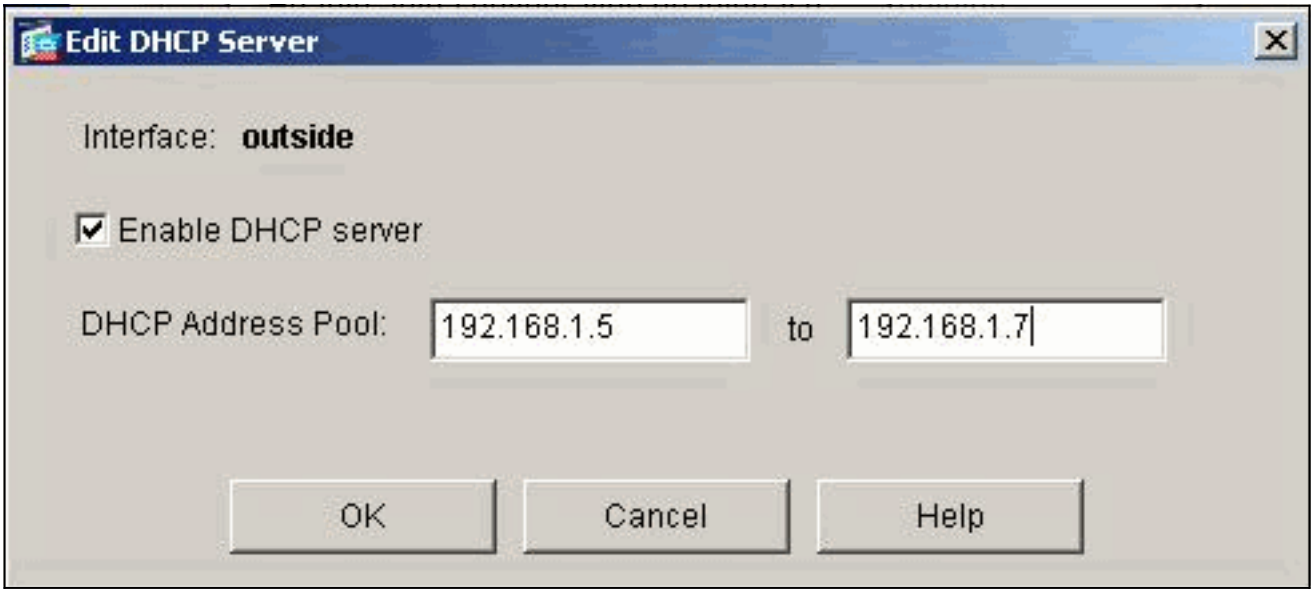
DHCP-serverconfiguratie met ASDM

Voltooi deze stappen om de PIX security applicatie of ASA te configureren als een DHCP-server met ASDM.

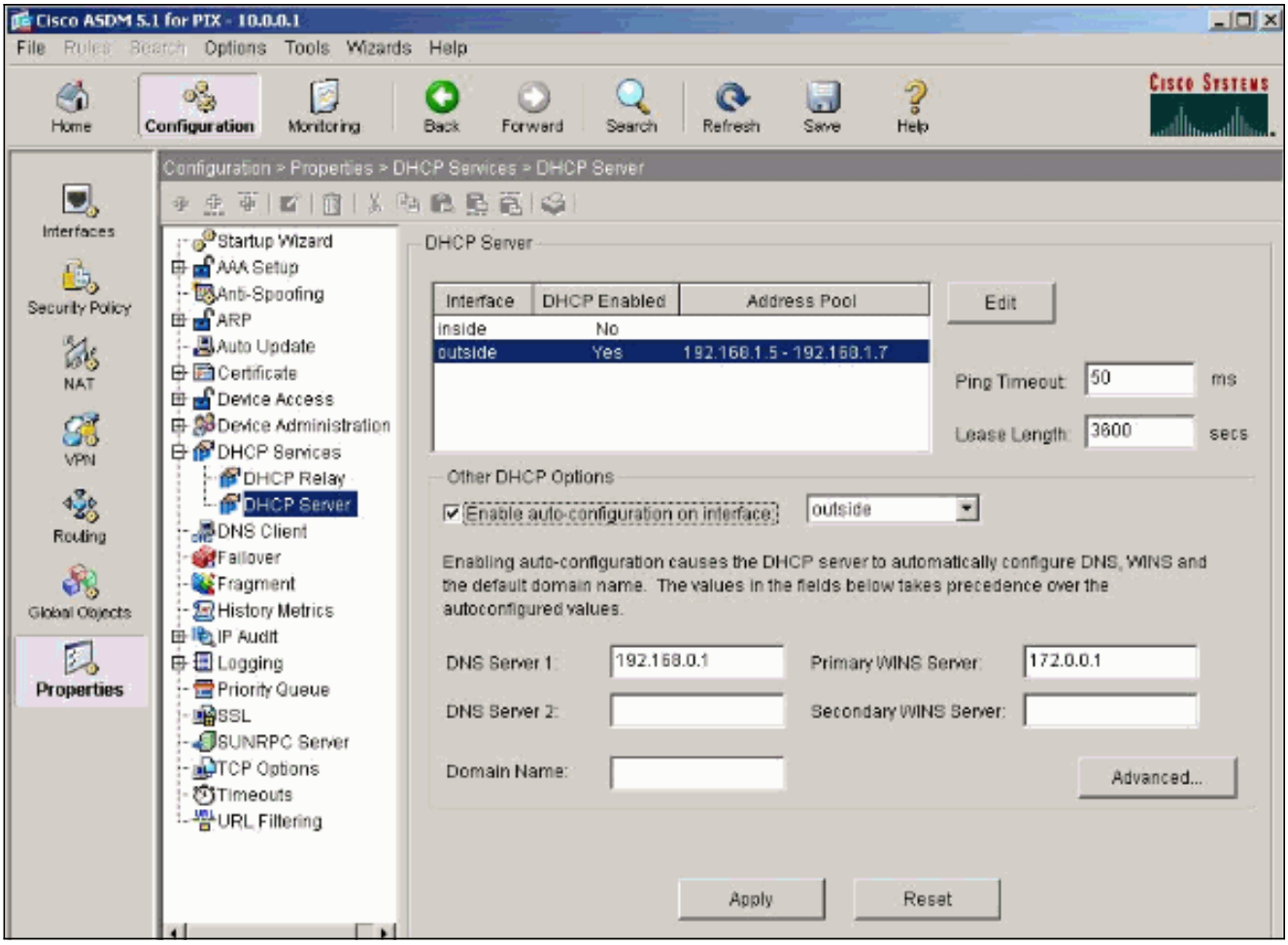
1. Kies **Configuration > Properties > DHCP-services > DHCP-server** vanuit het Home venster. Selecteer een interface en klik op **Bewerken** om de DHCP-server in te schakelen en om een DHCP-adrespool te maken.Het adrestoewijzing moet op hetzelfde net zijn als de interface voor security applicatie. In dit voorbeeld wordt de DHCP-server ingesteld op de externe interface van de PIX security
   applicatie.



2. Controleer **DHCP-server** op de buiteninterface inschakelen om naar de verzoeken van de DHCP-clients te luisteren. Geef het pool van adressen op die aan de DHCP-client moeten worden verstrekt en klik op **OK** om naar het hoofdvenster terug te keren.



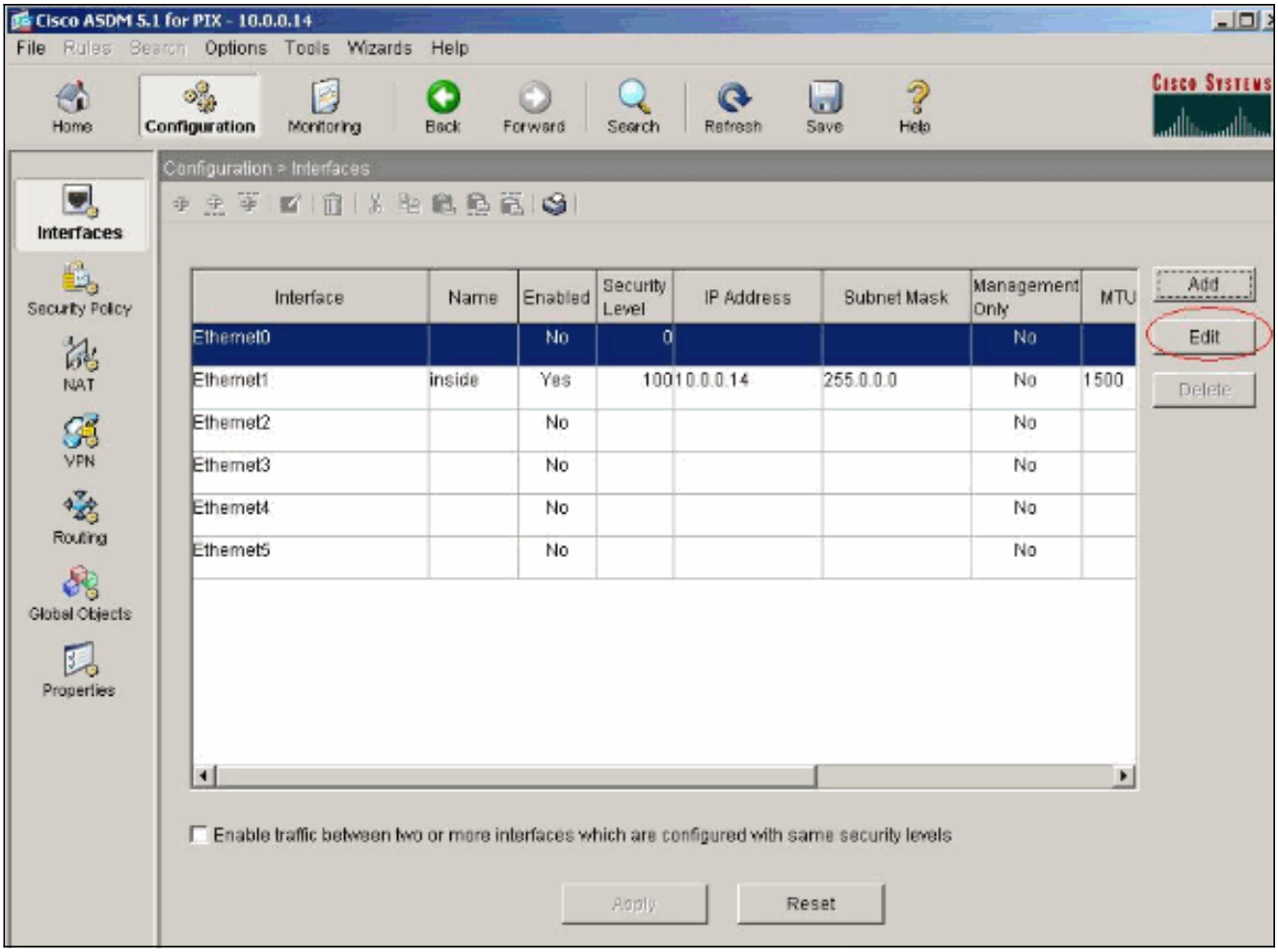
3. Controleer de **automatische configuratie van de interface** in **staat** om de DHCP-server ertoe te brengen automatisch de DNS, WINS en de standaard Domain Name te configureren voor de DHCP-client. Klik op **Toepassen** om de actieve configuratie van het apparaat bij te werken.



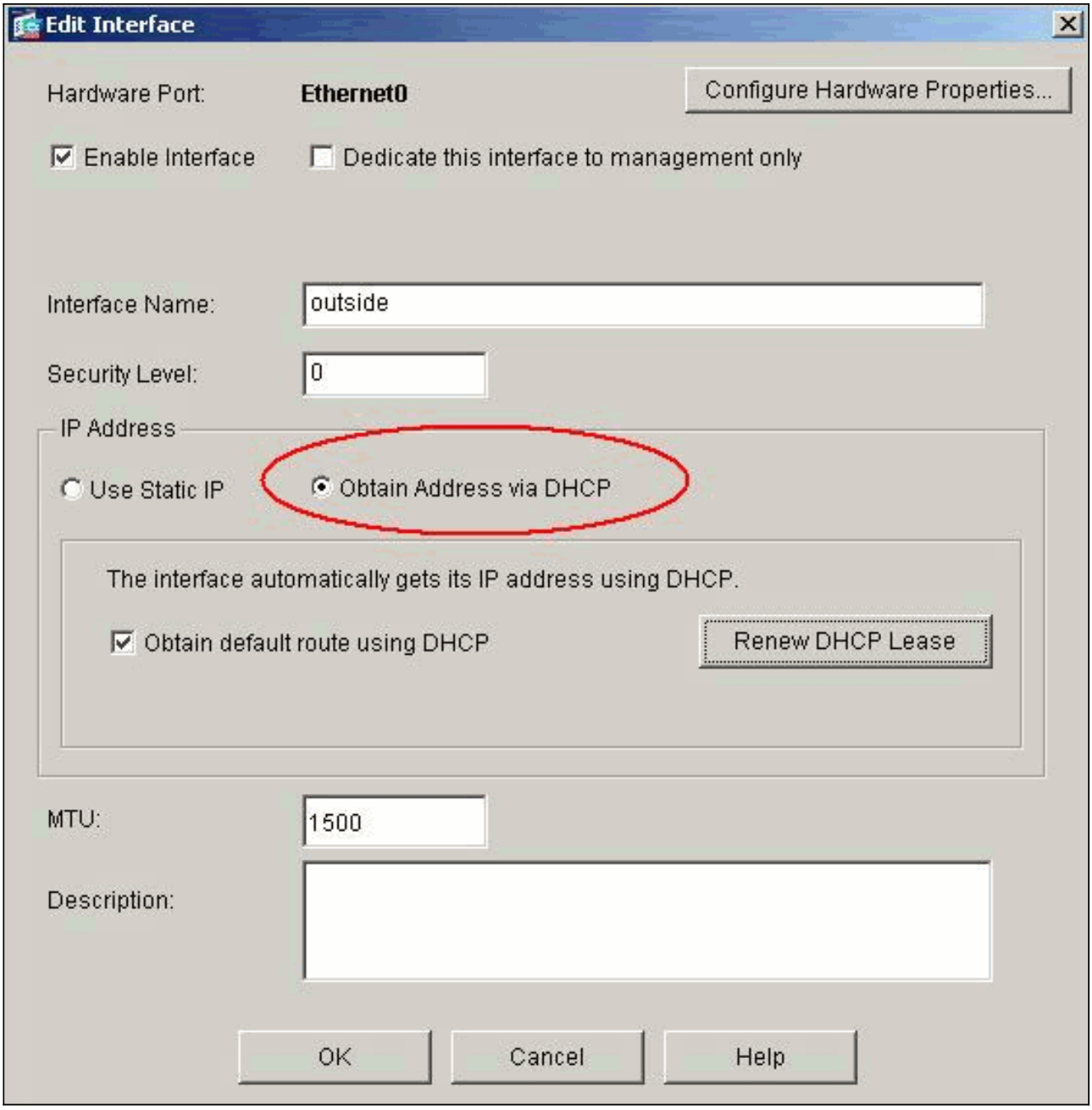
DHCP-clientconfiguratie met ASDM

Voltooi deze stappen om de PIX security applicatie als een DHCP-client te configureren met ASDM.

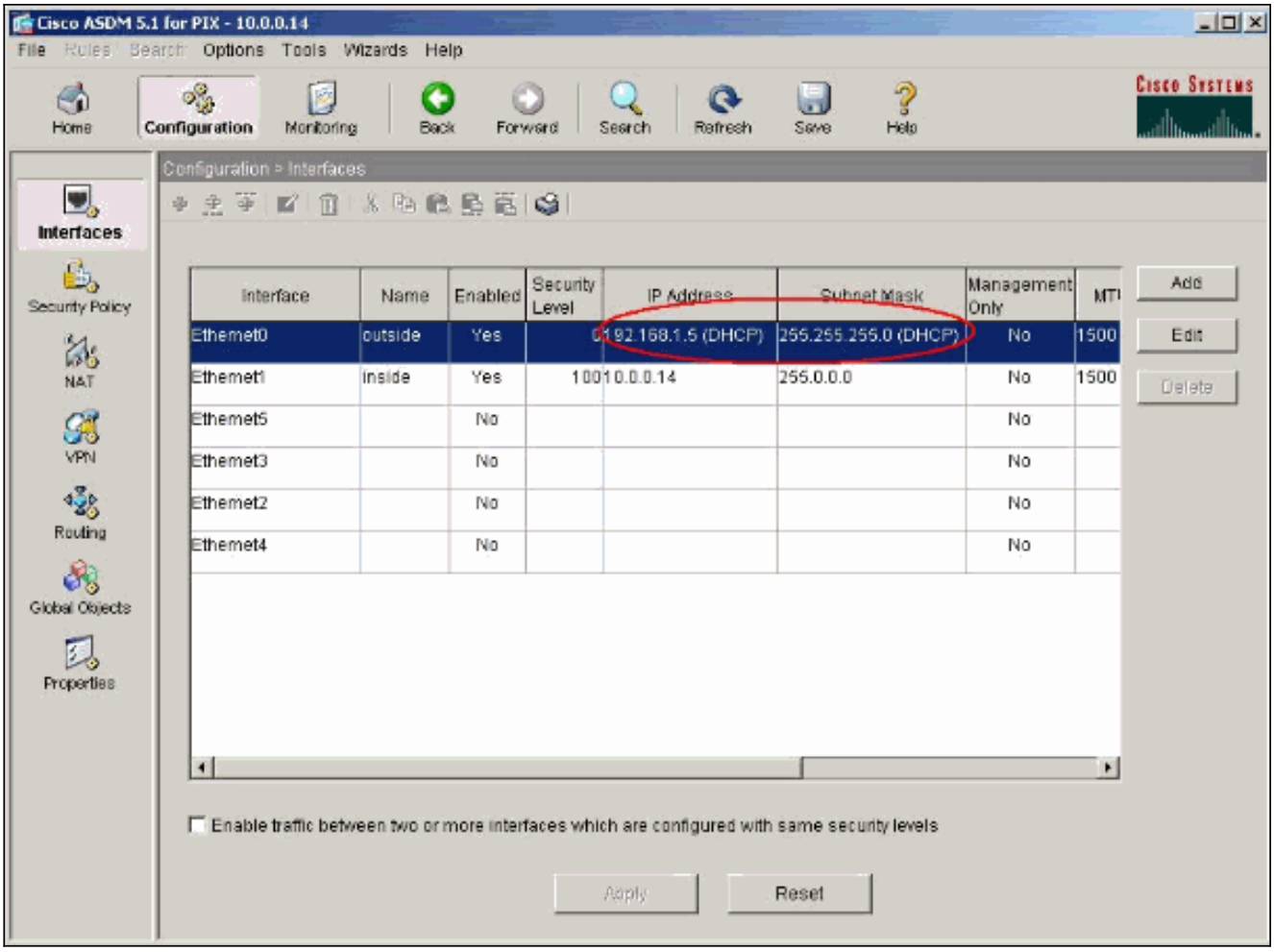
1. Kies **Configuratie > Interfaces** en klik op **Bewerken** om de Ethernet0 interface in staat te stellen om de configuratieparameters zoals een IP-adres te verkrijgen met een subnetmasker, standaardgateway, DNS-server en IP-adres van WINS-server van de DHCP-server.



2. Controleer **Interface inschakelen** en voer het niveau Interface Name en Security in voor de interface. Kies **Adres via DHCP** voor het IP-adres en **verkrijg de standaardroute met DHCP** voor de standaardgateway en klik vervolgens op **OK** om naar het hoofdvenster te gaan.



3. Klik op **Toepassen** om het IP-adres voor de Ethernet0-interface te bekijken op de DHCP-server.



DHCP-serverconfiguratie

Deze configuratie wordt gemaakt door de 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-clientconfiguratie

Deze configuratie wordt gemaakt door de ASDM:

DHCP-client

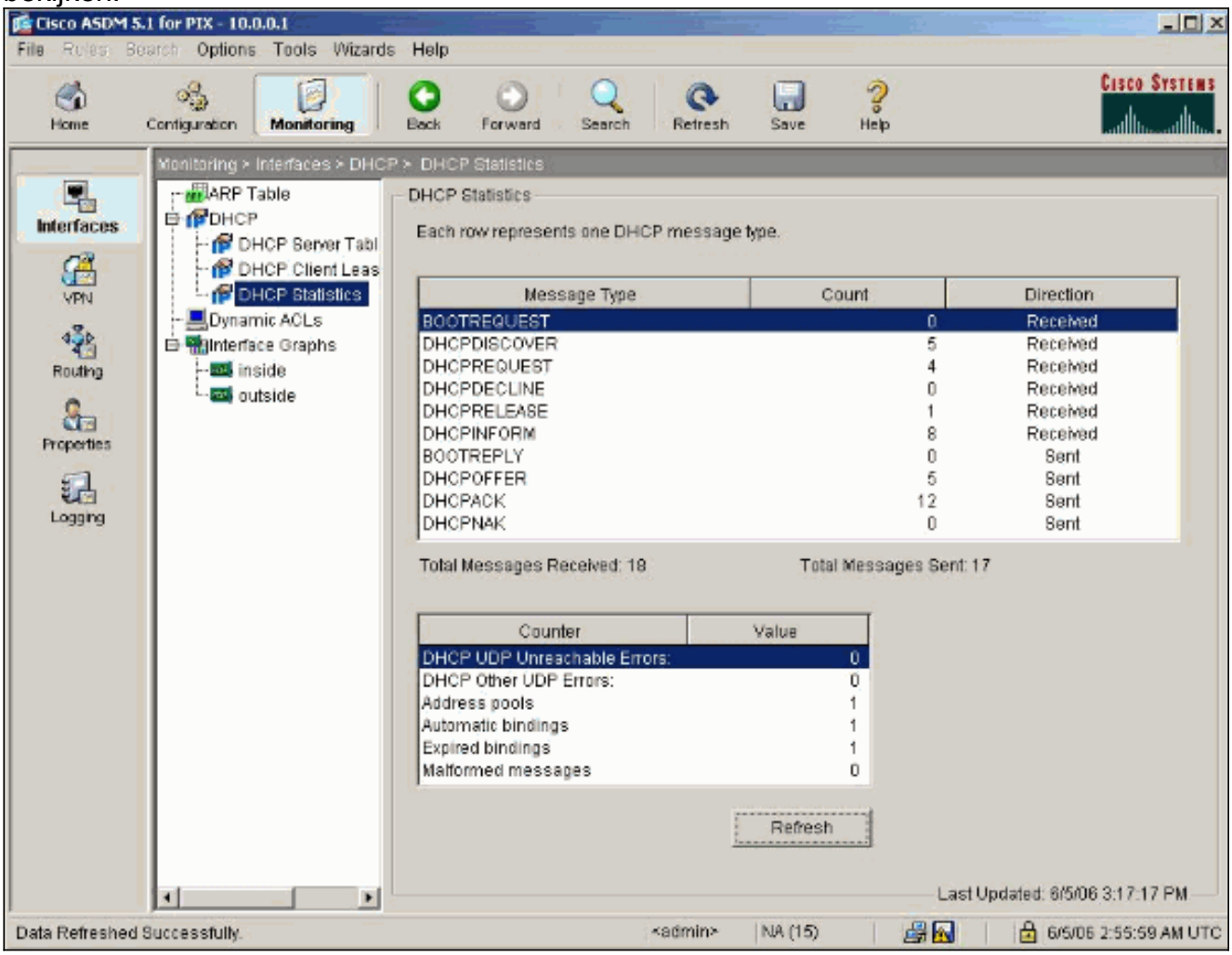
```
pixfirewall#show running-config
PIX Version 7.1(1)
!
hostname pixfirewall
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0
 nameif outside
 security-level 0

!--- 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
```

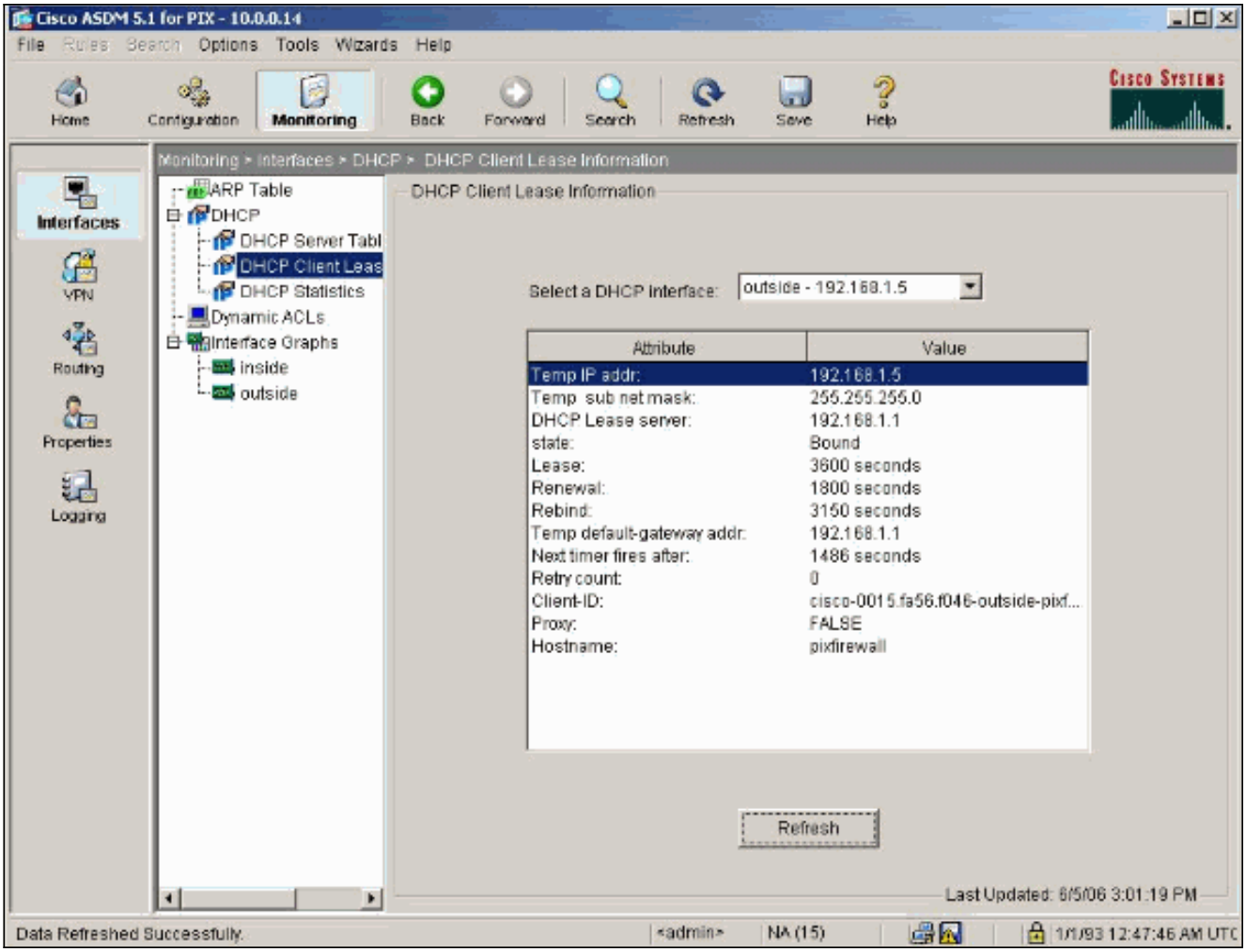
Verifiëren

Voltooi deze stappen om de DHCP-statistieken en de bindende informatie van de DHCP-server en DHCP-client te controleren met behulp van ASDM.

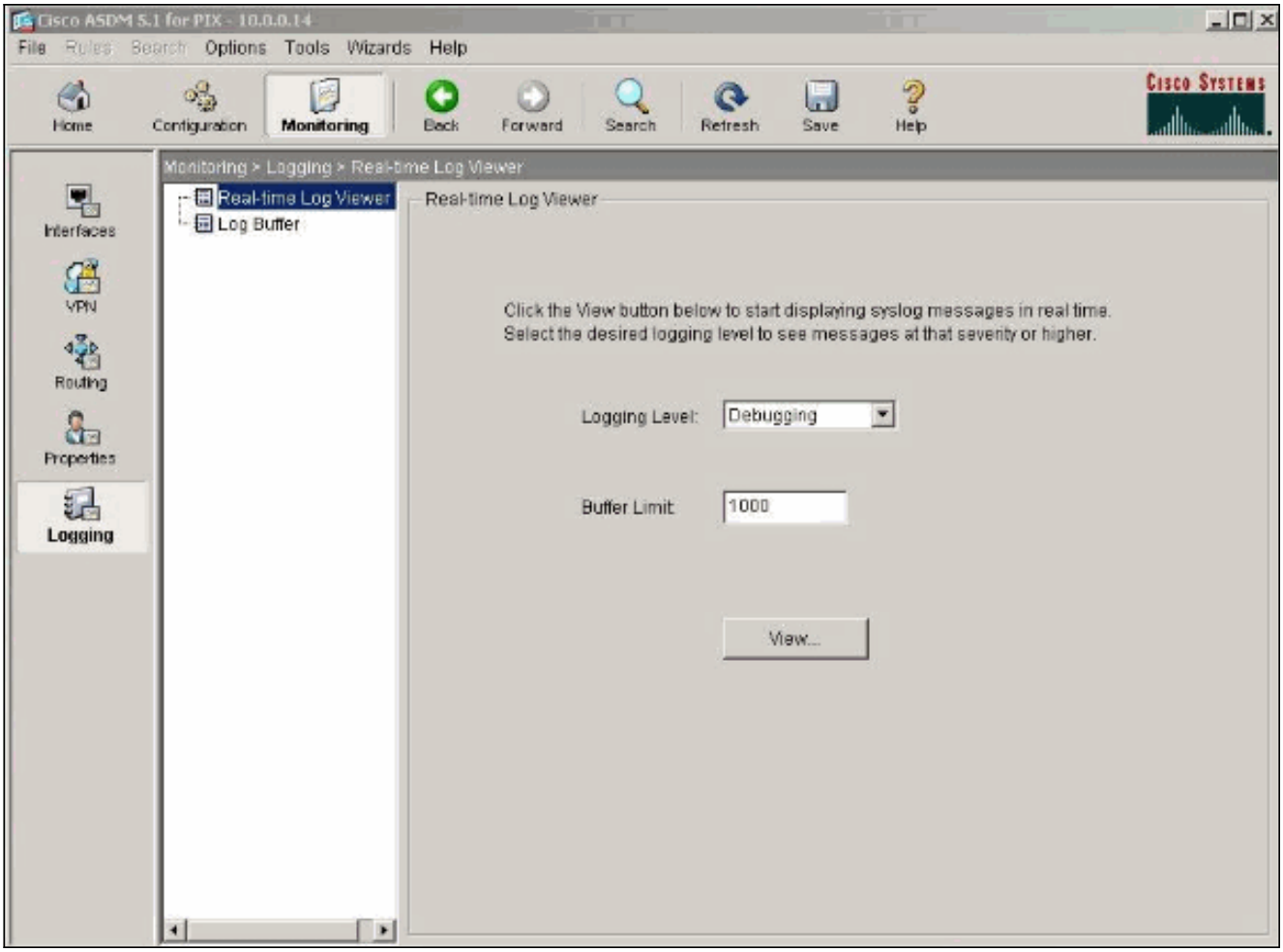
1. Kies **Controle > Interfaces > DHCP > Statistieken** van DHCP van de server van DHCP om de statistieken van DHCP te verifiëren, zoals DHCPCPDISCOVER, DHCPREQUEST, DHCPOFFER, en DHCPACK.Voer de opdracht Statistieken **van** de **show dhcpd in** van de CLI om de DHCP-statistieken te bekijken.



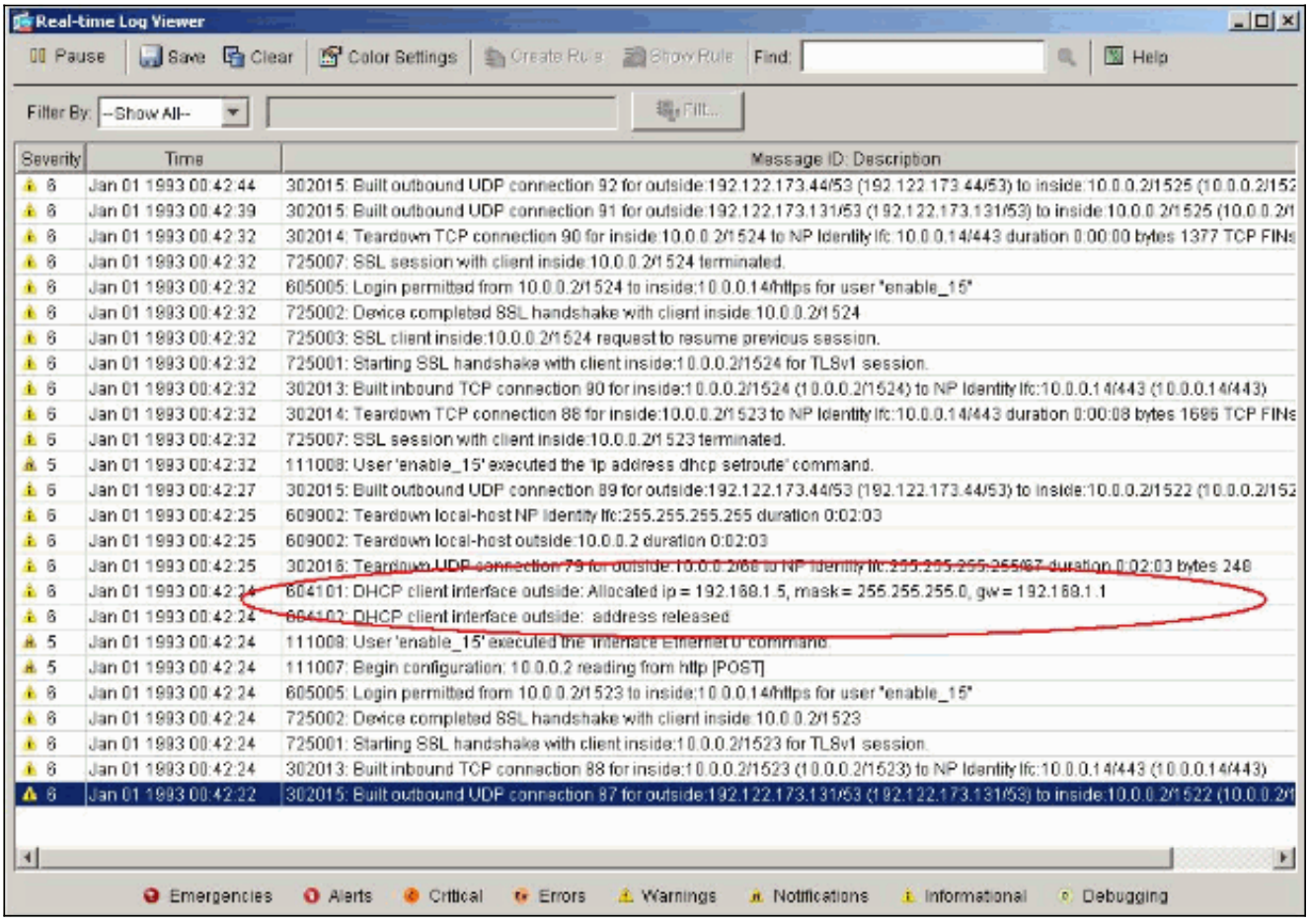
2. Kies **Monitoring > Interfaces > DHCP > DHCP-clientleaseinformatie** van de DHCP-client om de DHCP-bindende informatie te bekijken.Voer de **opdracht** dhcpd-**binding** in om de DHCP-bindingsinformatie uit de CLI te bekijken.



3. Kies **Monitoring > Vastlegging > Realtime logvenster** om het Logging Level en de bufferlimiet te selecteren voor het weergeven van de realtime logberichten.



4. Bekijk de real-time loggebeurtenissen van de DHCP-client. Het IP-adres wordt toegewezen voor de externe interface van de DHCP-client.



Problemen oplossen

Opdrachten voor probleemoplossing

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

Opmerking: Raadpleeg Belangrijke informatie over debug Commands voordat u **debug-**opdrachten gebruikt.

- **debug dhcpd gebeurtenis**-displays die wordt gekoppeld aan de DHCP-server.
- **debug HD-pakket**—Hier wordt pakketinformatie weergegeven die met de DHCP-server is gekoppeld.

Foutberichten

```
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
```

Uitleg: De omvang van de adrespool is beperkt tot 256 adressen per pool op het beveiligingsapparaat. Dit kan niet worden gewijzigd en is een softwarebeperking. Het totaal kan slechts 256 zijn. Als het bereik van de adrespool groter is dan 253 adressen (bijvoorbeeld 254, 255, 256), kan het netmasker van de interface van het veiligheidsapparaat geen Klasse C adres zijn (bijvoorbeeld 255.255.255.0). Het moet iets groters zijn, bijvoorbeeld 255.255.254.0.

Raadpleeg de Cisco Security Opdracht Line Configuration voor Cisco-applicatie voor informatie over het implementeren van de DHCP-serverfunctie in het beveiligingsapparaat.

FAQ: Toewijzing van adres

Vraag-Is het mogelijk om een statisch/permanent IP adres aan de computer toe te wijzen die ASA als DHCP-server gebruikt?

Antwoord: Het is niet mogelijk om PIX/ASA te gebruiken.

Vraag-Is het mogelijk om DHCP-adressen aan specifieke MAC-adressen op ASA te verbinden?

Antwoord: Nee, het is niet mogelijk.

Gerelateerde informatie

- Ondersteuning van PIX-security applicatie
- Opdrachtreferenties van Cisco Secure PIX-firewall
- Technische ondersteuning en documentatie – Cisco Systems