Esempio di configurazione di PIX/ASA come server DHCP e client

Sommario

Introduzione

I modelli PIX serie 500 Security Appliance e Cisco Adaptive Security Appliance (ASA) supportano il funzionamento sia come server DHCP (Dynamic Host Configuration Protocol) sia come client DHCP. DHCP è un protocollo che fornisce agli host parametri di configurazione automatica, ad esempio un indirizzo IP con subnet mask, gateway predefinito, server DNS e indirizzo IP del server WINS.

Appliance di sicurezza può funzionare come server DHCP o client DHCP. Quando funziona come server, Security Appliance fornisce i parametri di configurazione della rete direttamente ai client DHCP. Quando funziona come client DHCP, Appliance di sicurezza richiede tali parametri di configurazione a un server DHCP.

Nel documento viene spiegato come configurare il server DHCP e il client DHCP usando Cisco Adaptive Security Device Manager (ASDM) sull'appliance di sicurezza.

Prerequisiti

Requisiti

In questo documento si presume che l'appliance di sicurezza PIX o l'ASA sia completamente operativa e configurata per consentire a Cisco ASDM di apportare modifiche alla configurazione.

Nota: per consentire al dispositivo di essere configurato da ASDM, consultare il documento sull'autorizzazione dell'accesso HTTPS per ASDM.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- PIX serie 500 Security Appliance 7.x**Nota:** la configurazione PIX CLI utilizzata nella versione 7.x è applicabile anche a PIX 6.x. L'unica differenza è che nelle versioni precedenti a PIX 6.3, il server DHCP può essere abilitato solo sull'interfaccia interna. In PIX 6.3 e versioni successive, il server DHCP può essere abilitato su qualsiasi interfaccia disponibile. In questa configurazione, viene usata l'interfaccia esterna per la funzionalità del server DHCP.
- ASDM 5.x**Nota:** ASDM supporta solo PIX 7.0 e versioni successive. PIX Device Manager (PDM) è disponibile per la configurazione della versione 6.x di PIX. Per ulteriori informazioni, fare riferimento alla compatibilità hardware e software delle appliance di sicurezza Cisco ASA serie 5500 e PIX serie 500.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Prodotti correlati

Questa configurazione può essere utilizzata anche con Cisco ASA 7.x.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Configurazione

In questa configurazione sono presenti due appliance di sicurezza PIX con versione 7.x. Una funziona come server DHCP che fornisce i parametri di configurazione a un altro PIX Security Appliance 7.x che funziona come client DHCP. Quando funziona come server DHCP, il PIX assegna dinamicamente indirizzi IP ai client DHCP da un pool di indirizzi IP designati.

Èpossibile configurare un server DHCP su ciascuna interfaccia dell'appliance di sicurezza. Ogni interfaccia può disporre di un proprio pool di indirizzi da cui estrarre. Tuttavia, le altre impostazioni DHCP, ad esempio i server DNS, il nome di dominio, le opzioni, il timeout del ping e i server WINS, sono configurate globalmente e utilizzate dal server DHCP su tutte le interfacce.

Non è possibile configurare un client DHCP o i servizi di inoltro DHCP su un'interfaccia su cui è abilitato il server. Inoltre, i client DHCP devono essere connessi direttamente all'interfaccia su cui è abilitato il server.

Infine, quando il server DHCP è abilitato su un'interfaccia, non è possibile modificare l'indirizzo IP di tale interfaccia.

Nota: fondamentalmente, non è disponibile un'opzione di configurazione per impostare l'indirizzo del gateway predefinito nella risposta DHCP inviata dal server DHCP (PIX/ASA). Il server DHCP invia sempre il proprio indirizzo come gateway per il client DHCP. Tuttavia, la definizione di un percorso predefinito che punti al router Internet consente all'utente di raggiungere Internet.

Nota: il numero di indirizzi del pool DHCP che possono essere assegnati dipende dalla licenza utilizzata nell'appliance di sicurezza (PIX/ASA). Se si usa la licenza Base/Security Plus, questi limiti sono validi per il pool DHCP. Se il limite per gli host è 10, il pool DHCP può essere limitato a 32 indirizzi. Se il limite per gli host è 50, il pool DHCP può essere limitato a 128 indirizzi. Se il limite dell'host è illimitato, il pool DHCP può essere limitato a 256 indirizzi. Pertanto, il pool di indirizzi è limitato in base al numero di host.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

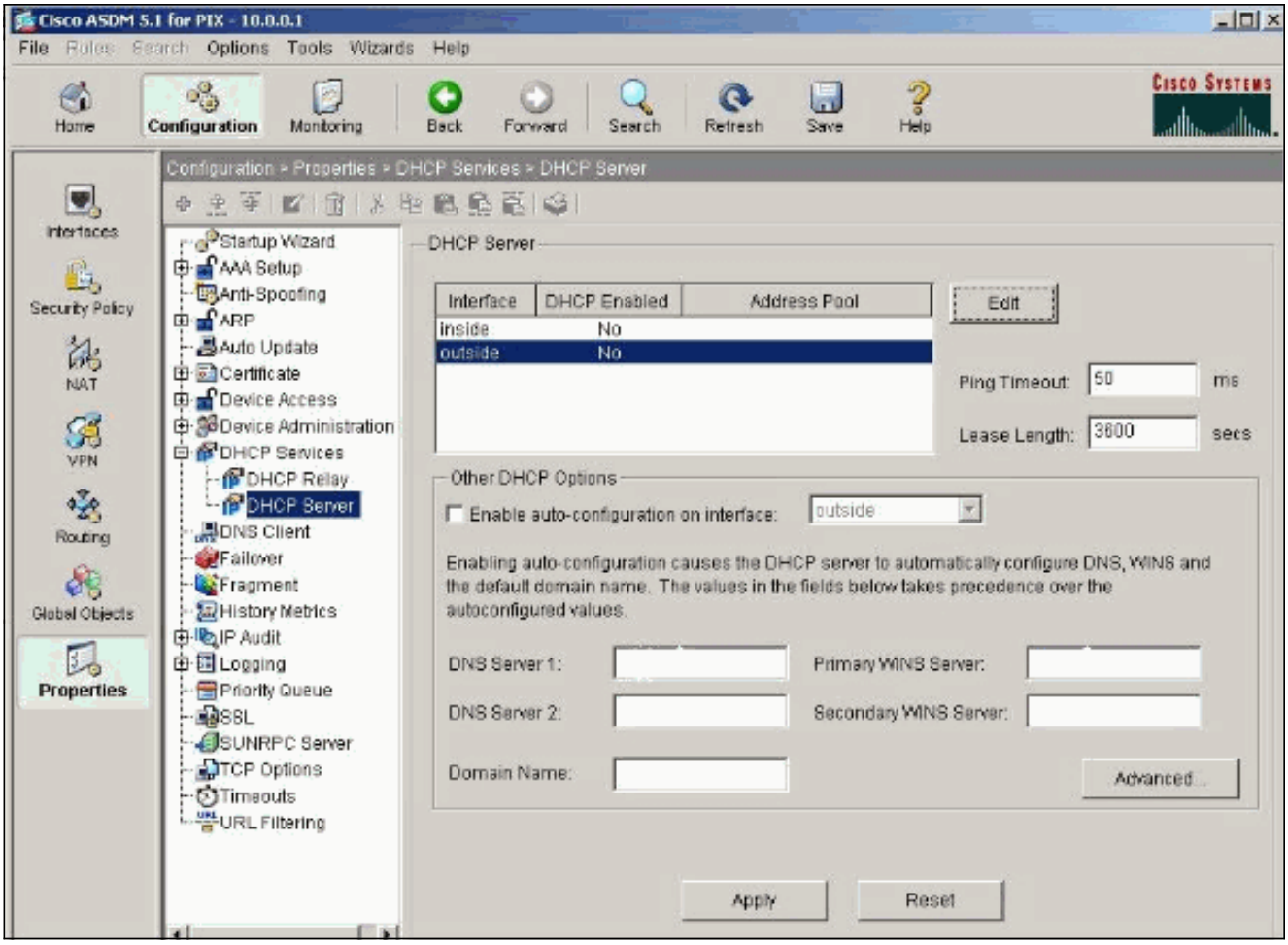
Nel documento vengono usate queste configurazioni:

- Configurazione del server DHCP con ASDM
- Configurazione del client DHCP con ASDM
- Configurazione server DHCP
- Configurazione client DHCP

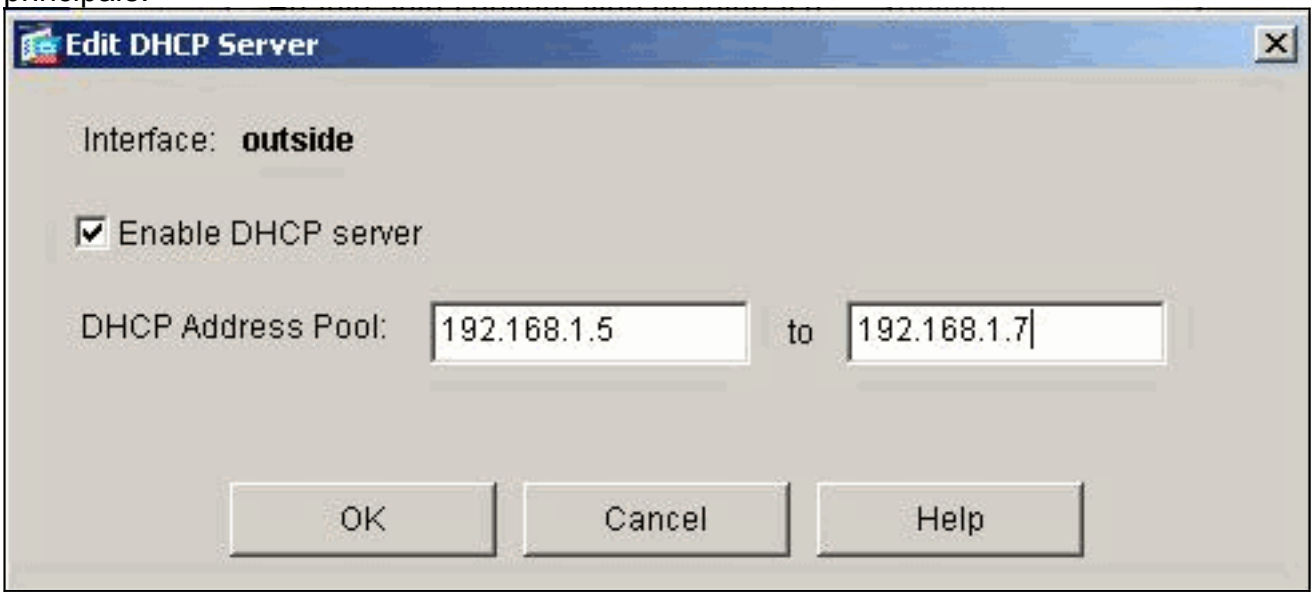
Configurazione del server DHCP con ASDM

Completare la procedura descritta di seguito per configurare l'appliance di sicurezza PIX o l'ASA come server DHCP con ASDM.

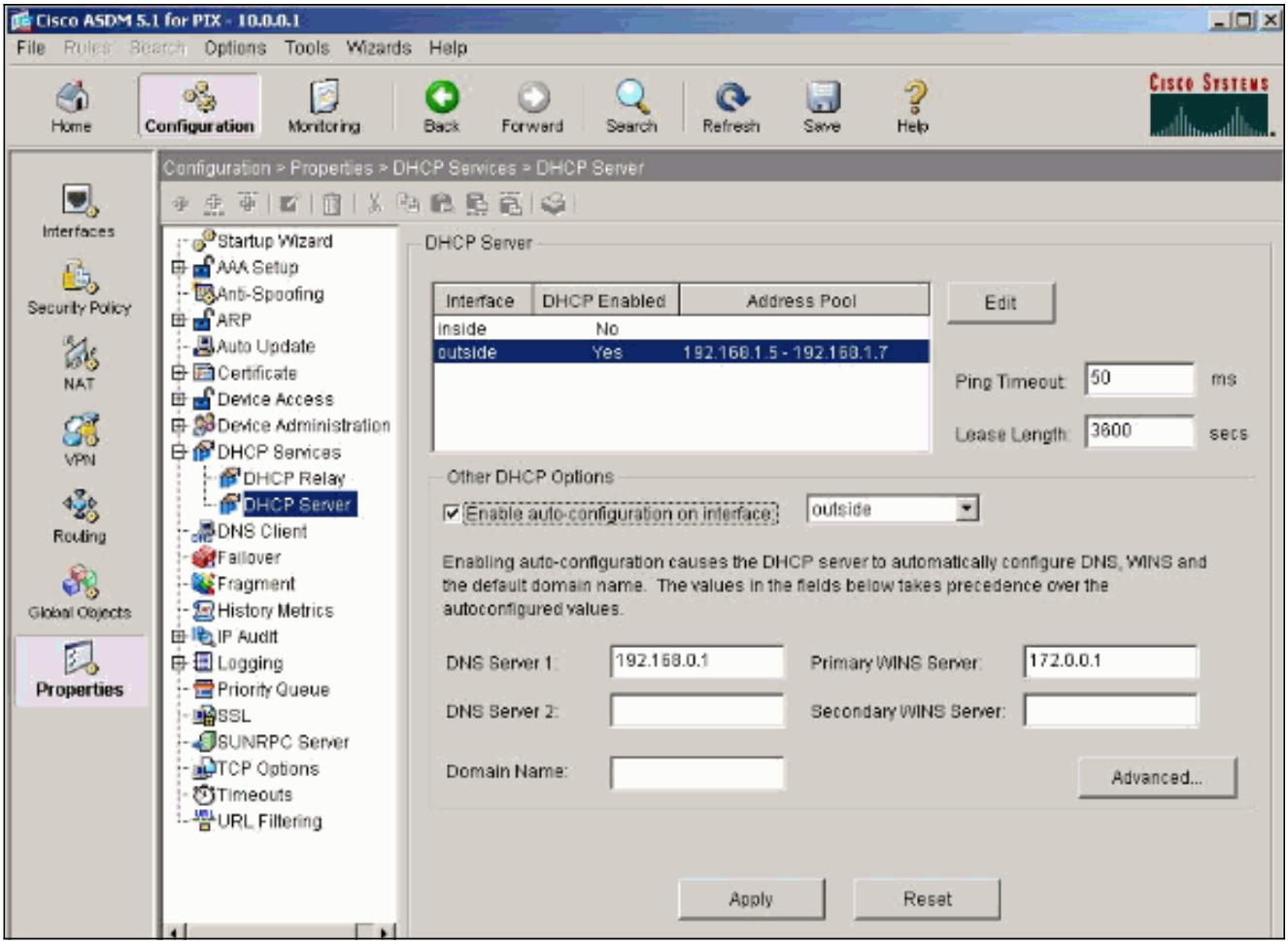
1. Scegliere **Configurazione > Proprietà > Servizi DHCP > Server DHCP** dalla finestra Home. Selezionare un'interfaccia e fare clic su **Modifica** per abilitare il server DHCP e creare un pool di indirizzi DHCP.Il pool di indirizzi deve trovarsi nella stessa subnet dell'interfaccia di Security Appliance. Nell'esempio, il server DHCP è configurato sull'interfaccia esterna di PIX Security
   Appliance.



2. Selezionare **Abilita server DHCP** sull'interfaccia esterna per l'ascolto delle richieste dei client DHCP. Specificare il pool di indirizzi da inviare al client DHCP e fare clic su **OK** per tornare alla finestra
principale.



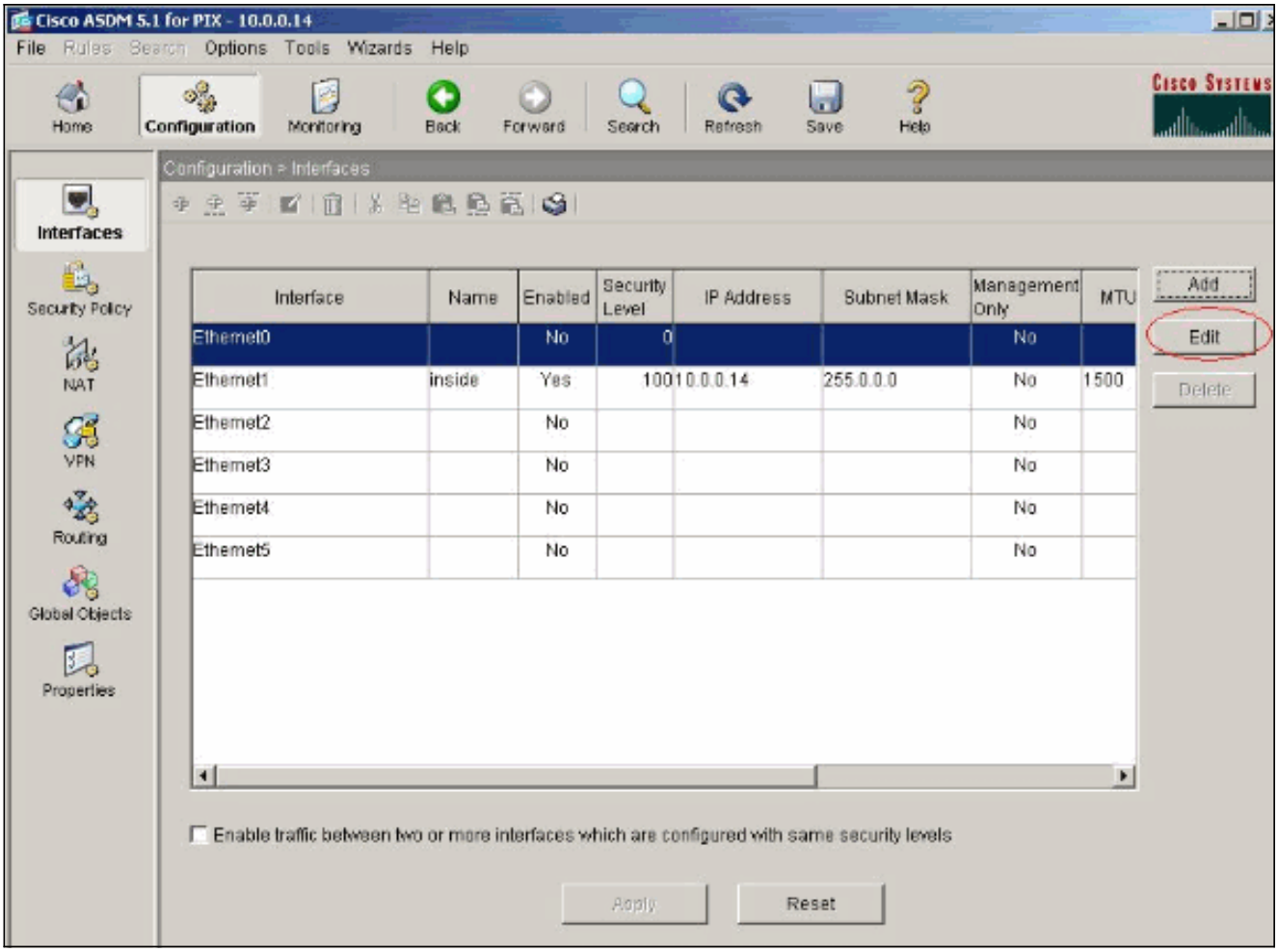
3. Selezionare **Abilita configurazione automatica sull'interfaccia** per fare in modo che il server DHCP configuri automaticamente il DNS, il WINS e il nome di dominio predefinito per il client DHCP. Fare clic su **Applica** per aggiornare la configurazione in esecuzione dell'appliance di sicurezza.



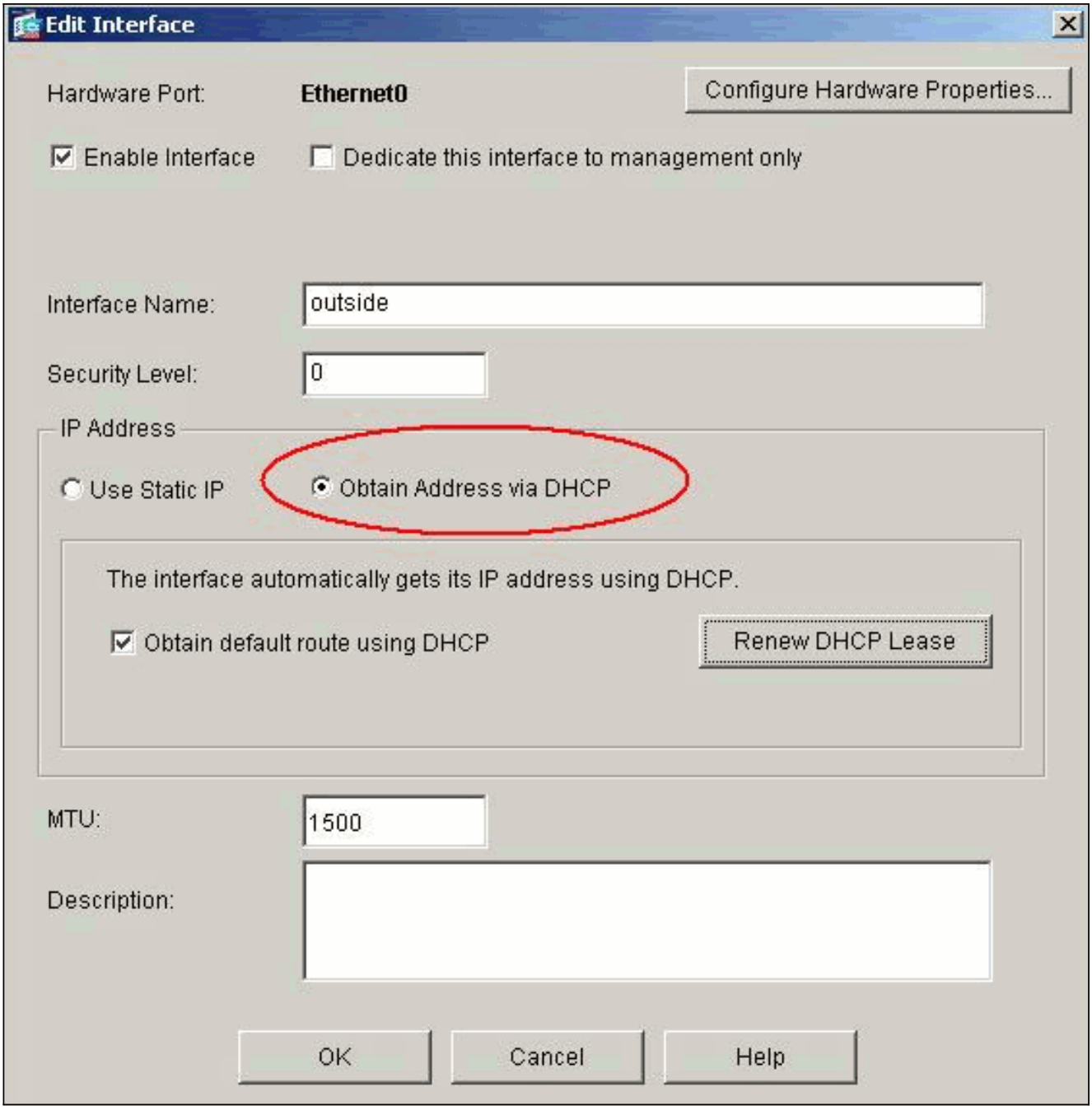
Configurazione del client DHCP con ASDM

Completare la procedura seguente per configurare PIX Security Appliance come client DHCP utilizzando ASDM.

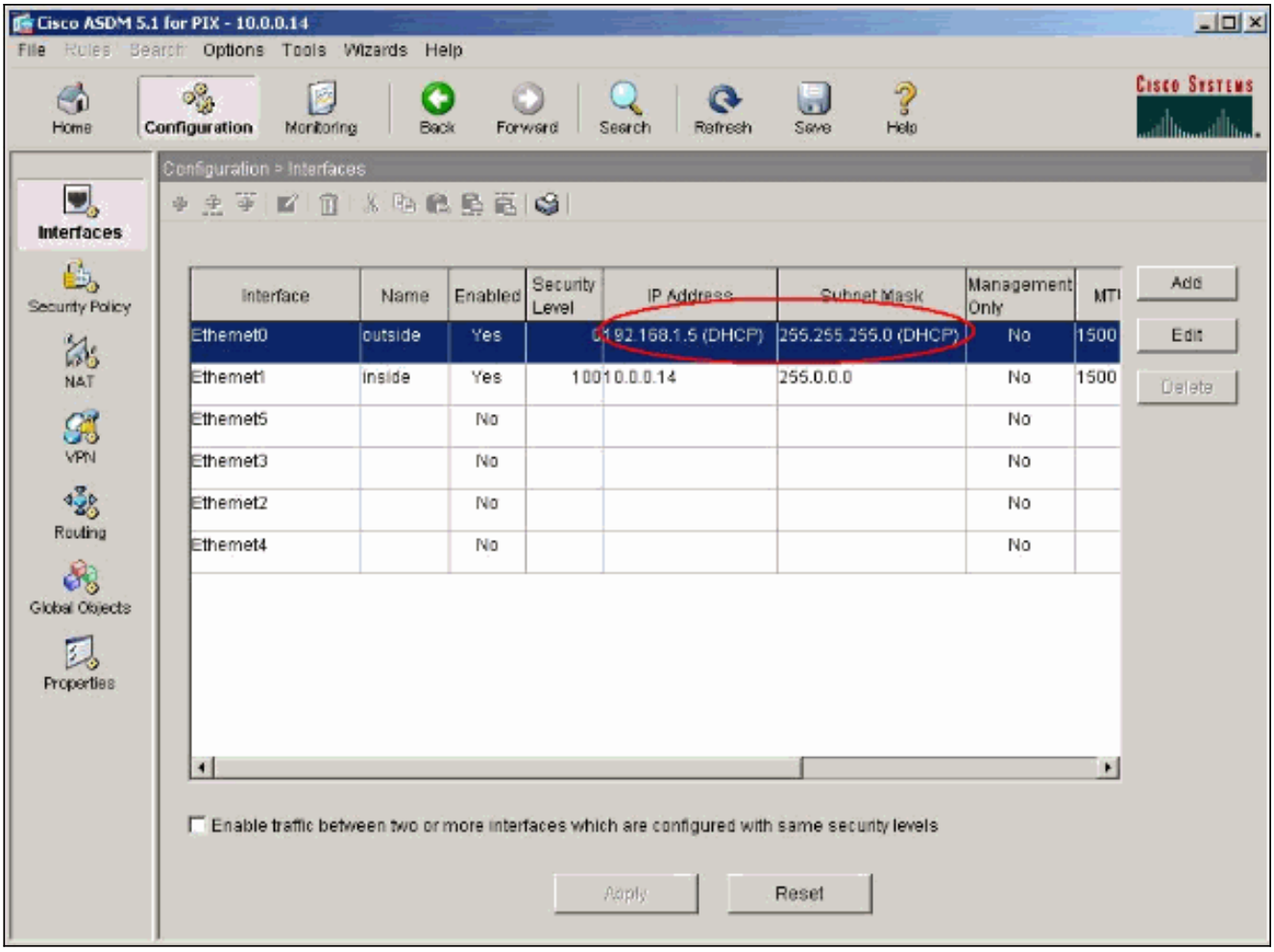
1. Scegliere **Configurazione > Interfacce** e fare clic su **Modifica** per abilitare l'interfaccia Ethernet0 e ottenere dal server DHCP i parametri di configurazione, ad esempio un indirizzo IP con subnet mask, gateway predefinito, server DNS e indirizzo IP del server WINS.



2. Selezionare **Abilita interfaccia** e immettere il nome e il livello di sicurezza dell'interfaccia. Selezionare **Obtain address via DHCP** (Ottieni indirizzo via DHCP) per l'indirizzo IP e **Obtain default route using DHCP (Ottieni percorso predefinito tramite DHCP** per il gateway predefinito), quindi fare clic su **OK** per andare alla finestra principale.



3. Fare clic su **Apply** (Applica) per visualizzare l'indirizzo IP ottenuto per l'interfaccia Ethernet0 dal server
DHCP.



Configurazione server DHCP

Questa configurazione viene creata da ASDM:

Server DHCP

```
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
```

Configurazione client DHCP

Questa configurazione viene creata da ASDM:

Client DHCP

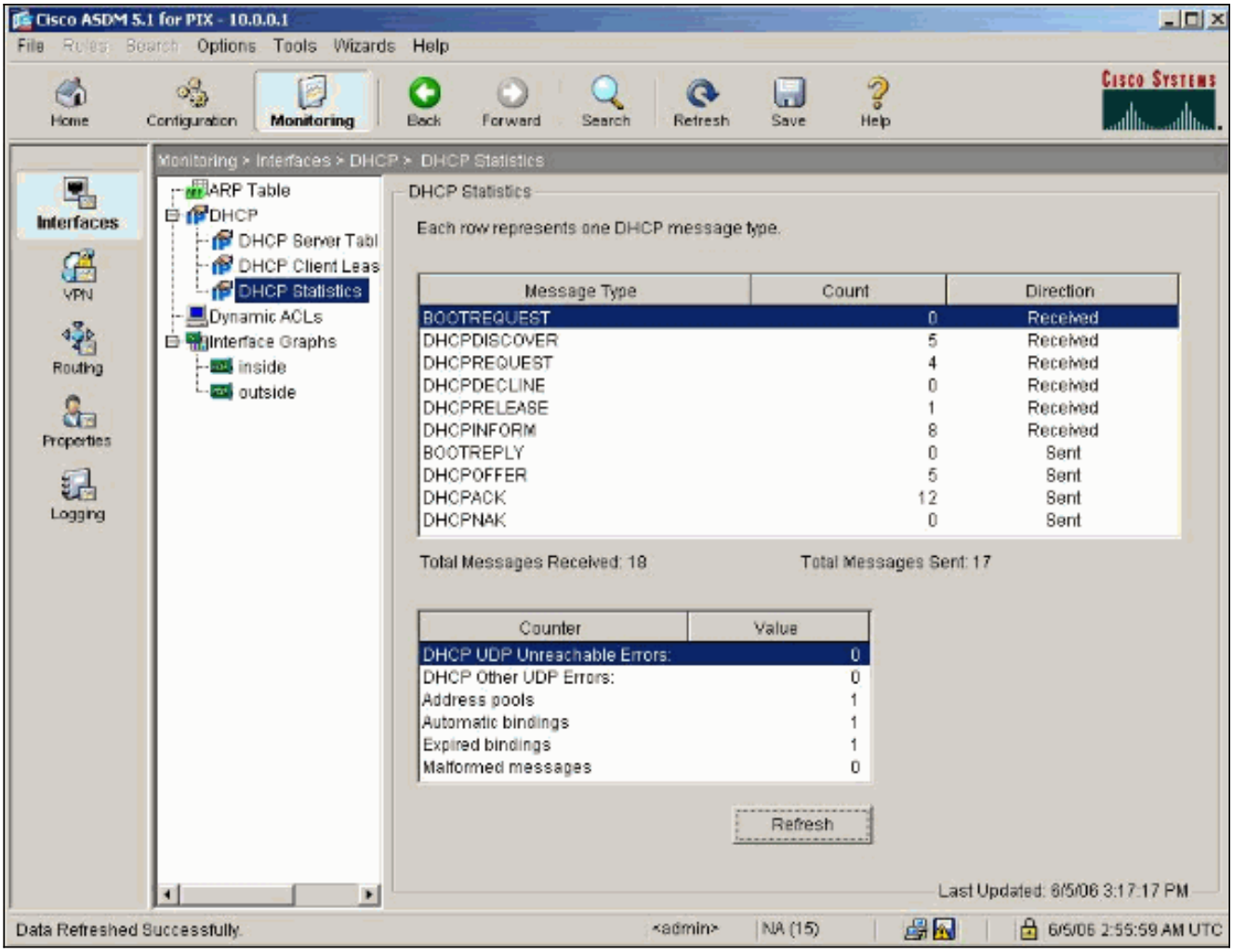
```
pixfirewall#show running-config
PIX Version 7.1(1)
!
hostname pixfirewall
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0
 nameif outside
 security-level 0

!--- 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
```

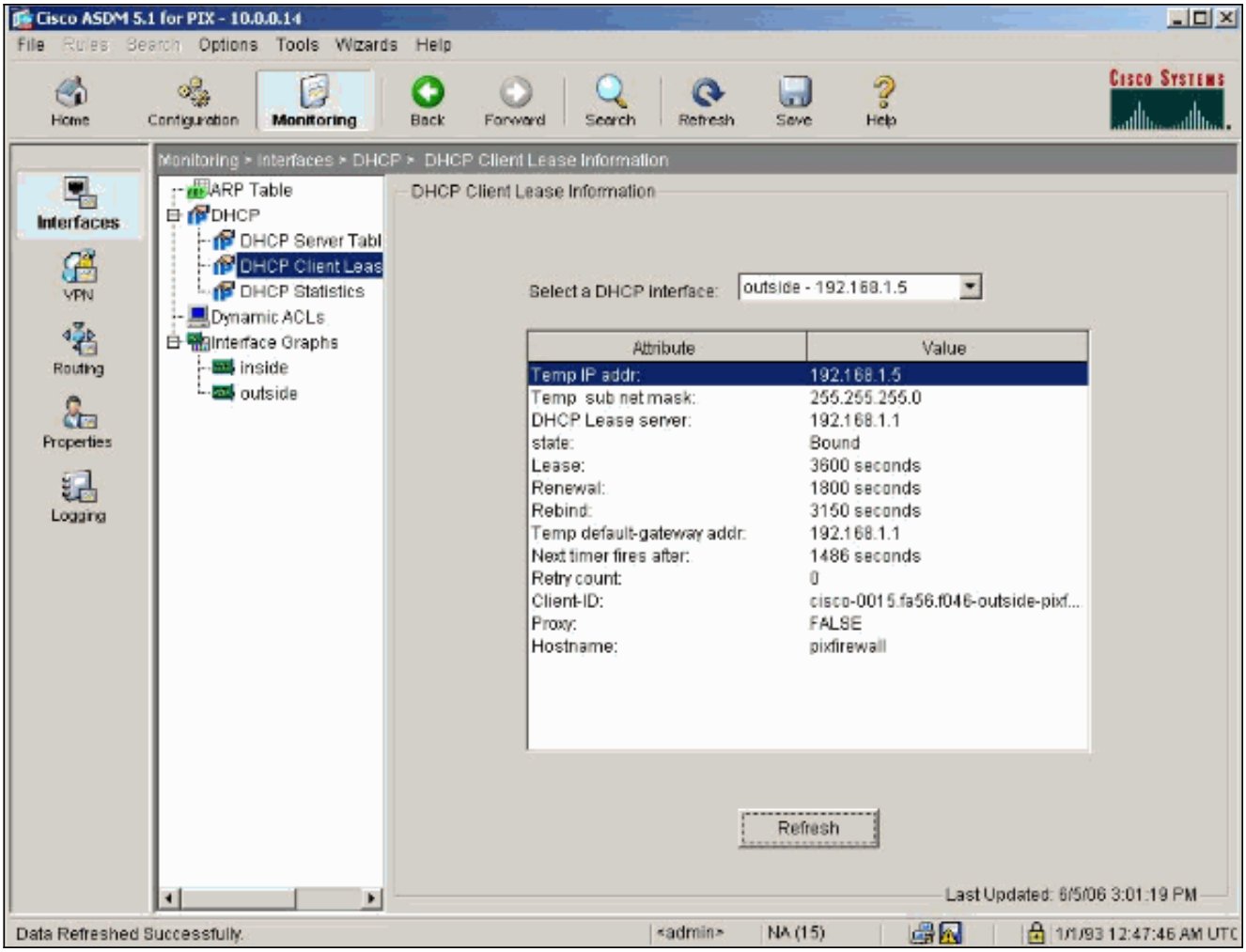
Verifica

Completare la procedura seguente per verificare le statistiche DHCP e le informazioni di binding dal server DHCP e dal client DHCP tramite ASDM.

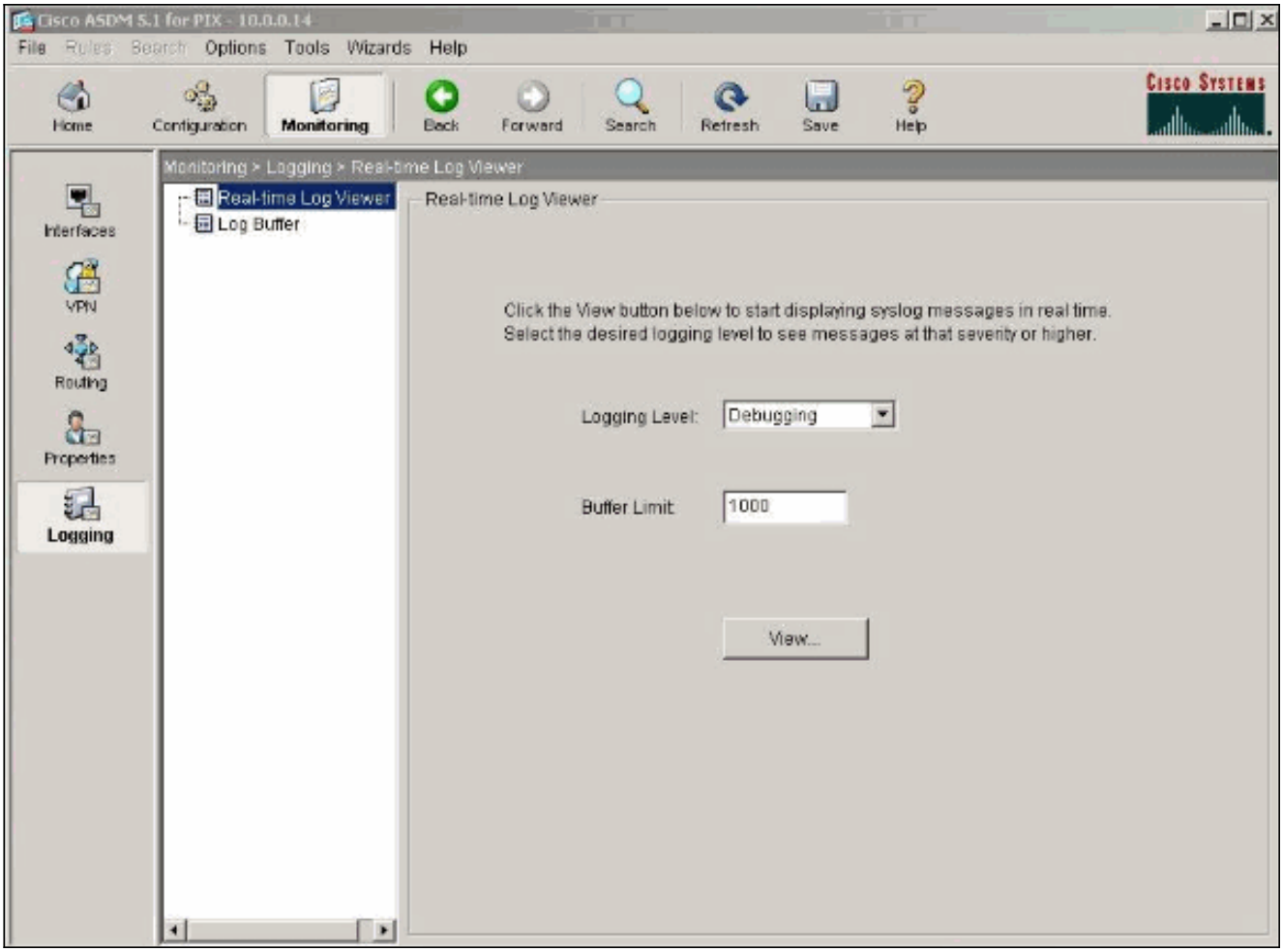
1. Scegliere **Monitoraggio > Interfacce > DHCP > Statistiche DHCP** dal server DHCP per verificare le statistiche DHCP, ad esempio DHCPDISCOVER, DHCPREQUEST, DHCPOFFER e DHCPACK.Immettere il comando **show dhcpd statistics** dalla CLI per visualizzare le statistiche DHCP.



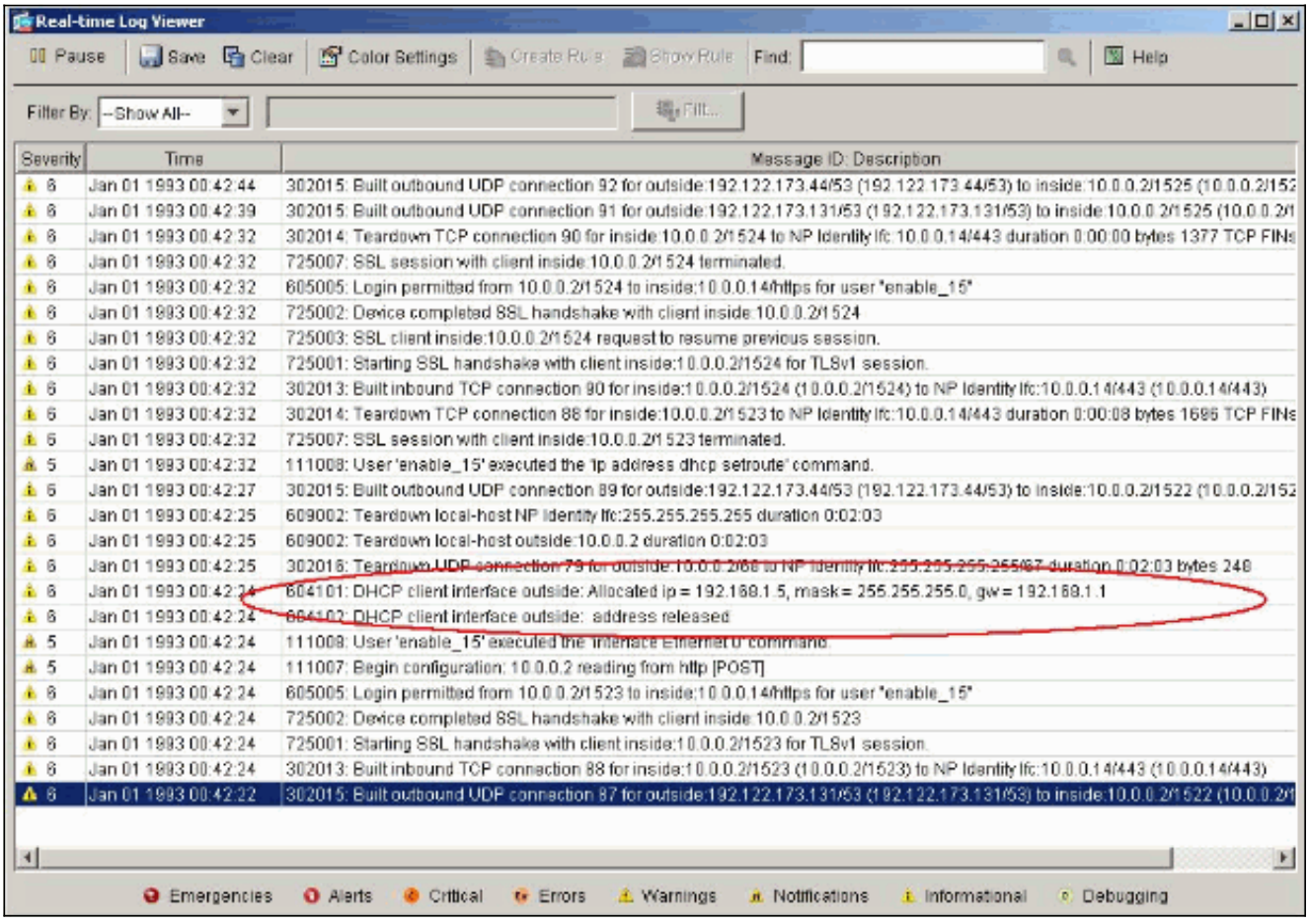
2. Scegliere **Monitoraggio > Interfacce > DHCP > Informazioni sul lease del client DHCP** dal client DHCP per visualizzare le informazioni sul binding DHCP.Immettere il comando **show dhcpd binding** per visualizzare le informazioni sul binding DHCP dalla CLI.



3. Scegliere **Monitoraggio > Log > Visualizzatore log in tempo reale** per selezionare il livello di log e il limite del buffer per visualizzare i messaggi di log in tempo reale.



4. Visualizzare gli eventi del registro in tempo reale dal client DHCP. L'indirizzo IP viene allocato per l'interfaccia esterna del client DHCP.



Risoluzione dei problemi

Comandi per la risoluzione dei problemi

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Nota: consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug**.

- **debug dhcpd event**: visualizza le informazioni sull'evento associate al server DHCP.
- **debug dhcpd packet**: visualizza le informazioni sul pacchetto associate al server DHCP.

Messaggi di errore

```
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
```

Spiegazione: La dimensione del pool di indirizzi è limitata a 256 indirizzi per pool sull'appliance di sicurezza. Non è possibile modificare questa impostazione e si tratta di una limitazione del software. Il totale può essere solo 256. Se l'intervallo dell'insieme di indirizzi è maggiore di 253 indirizzi (ad esempio 254, 255, 256), la maschera di rete dell'interfaccia dell'appliance di sicurezza non può essere un indirizzo di classe C (ad esempio 255.255.255.0). Deve essere qualcosa di più grande, ad esempio 255.255.254.0.

Per informazioni su come implementare la funzionalità server DHCP nell'appliance di sicurezza, consultare la guida alla configurazione della riga di comando di Cisco Security Appliance.

Domande frequenti: Assegnazione indirizzo

Domanda: è possibile assegnare un indirizzo IP statico/permanente al computer che usa ASA come server DHCP?

Risposta - Non è possibile utilizzare PIX/ASA.

Domanda: è possibile associare gli indirizzi DHCP a indirizzi MAC specifici sull'appliance ASA?

Risposta—No, non è possibile .

Informazioni correlate

- Pagina di supporto per PIX Security Appliance
- Riferimenti per i comandi di Cisco Secure PIX Firewall
- Documentazione e supporto tecnico – Cisco Systems