作為DHCP伺服器和客戶端的PIX/ASA配置示例

目錄

簡介

PIX 500系列安全裝置和思科自適應安全裝置(ASA)支援作為動態主機配置協定(DHCP)伺服器和DHCP客戶端運行。DHCP是一種協定，可為主機提供自動配置引數，如帶有子網掩碼的IP地址、預設網關、DNS伺服器和WINS伺服器IP地址。

安全裝置可以充當DHCP伺服器或DHCP客戶端。當作為伺服器運行時，安全裝置將直接向DHCP客戶端提供網路配置引數。當它作為DHCP客戶端運行時，安全裝置從DHCP伺服器請求此類配置引數。

本文檔重點介紹如何使用安全裝置上的思科自適應安全裝置管理器(ASDM)配置DHCP伺服器和DHCP客戶端。

必要條件

需求

本文檔假定PIX安全裝置或ASA完全正常運行並且配置為允許Cisco ASDM更改配置。

註：請參閱允許ASDM進行HTTPS訪問，以允許ASDM配置裝置。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- PIX 500系列安全裝置7.x**註**：7.x版中使用的PIX CLI配置也適用於PIX 6.x。唯一的區別是，在低於PIX 6.3的版本中，只能在內部介面上啟用DHCP伺服器。在PIX 6.3及更高版本中，可以在任何可用介面上啟用DHCP伺服器。在此配置中，外部介面用於DHCP伺服器功能。
- ASDM 5.x**注意**：ASDM僅支援PIX 7.0及更高版本。PIX裝置管理器(PDM)可用於配置PIX版本6.x。有關詳細資訊，請參閱Cisco ASA 5500系列和PIX 500系列安全裝置硬體和軟體相容性。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

相關產品

此配置也可與Cisco ASA 7.x一起使用。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

設定

在此配置中，有兩個運行7.x版的PIX安全裝置。其中一個充當一個DHCP伺服器，為另一個充當DHCP客戶端的PIX安全裝置7.x提供配置引數。當它充當DHCP伺服器時，PIX從指定IP地址池中動態地將IP地址分配給DHCP客戶端。

您可以在安全裝置的每個介面上配置DHCP伺服器。每個介面可以有自己的地址池可供使用。但是，其他DHCP設定（如DNS伺服器、域名、選項、ping超時和WINS伺服器）是全域性配置的，由DHCP伺服器在所有介面上使用。

不能在啟用伺服器的介面上配置DHCP客戶端或DHCP中繼服務。此外，DHCP客戶端必須直接連線到啟用伺服器的介面。

最後，當介面上啟用DHCP伺服器時，您無法更改該介面的IP地址。

注意：基本上，沒有配置選項來設定從DHCP伺服器(PIX/ASA)傳送的DHCP應答中的預設網關地址。 DHCP伺服器始終將自己的地址作為DHCP客戶端的網關傳送。但是，定義指向Internet路由器的預設路由使使用者可以訪問Internet。

注意：可分配的DHCP池地址數量取決於安全裝置(PIX/ASA)中使用的許可證。 如果您使用Base/Security Plus許可證，則這些限制適用於DHCP池。如果主機限製為10台主機，則將DHCP地址池限製為32個地址。如果主機限製為50台主機，則將DHCP地址池限製為128個地址。如果主機限製為無限制，則將DHCP地址池限製為256個地址。因此，地址池根據主機數量受到限制。

註：**使**用Command Lookup Tool(僅供已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

本檔案會使用以下設定：

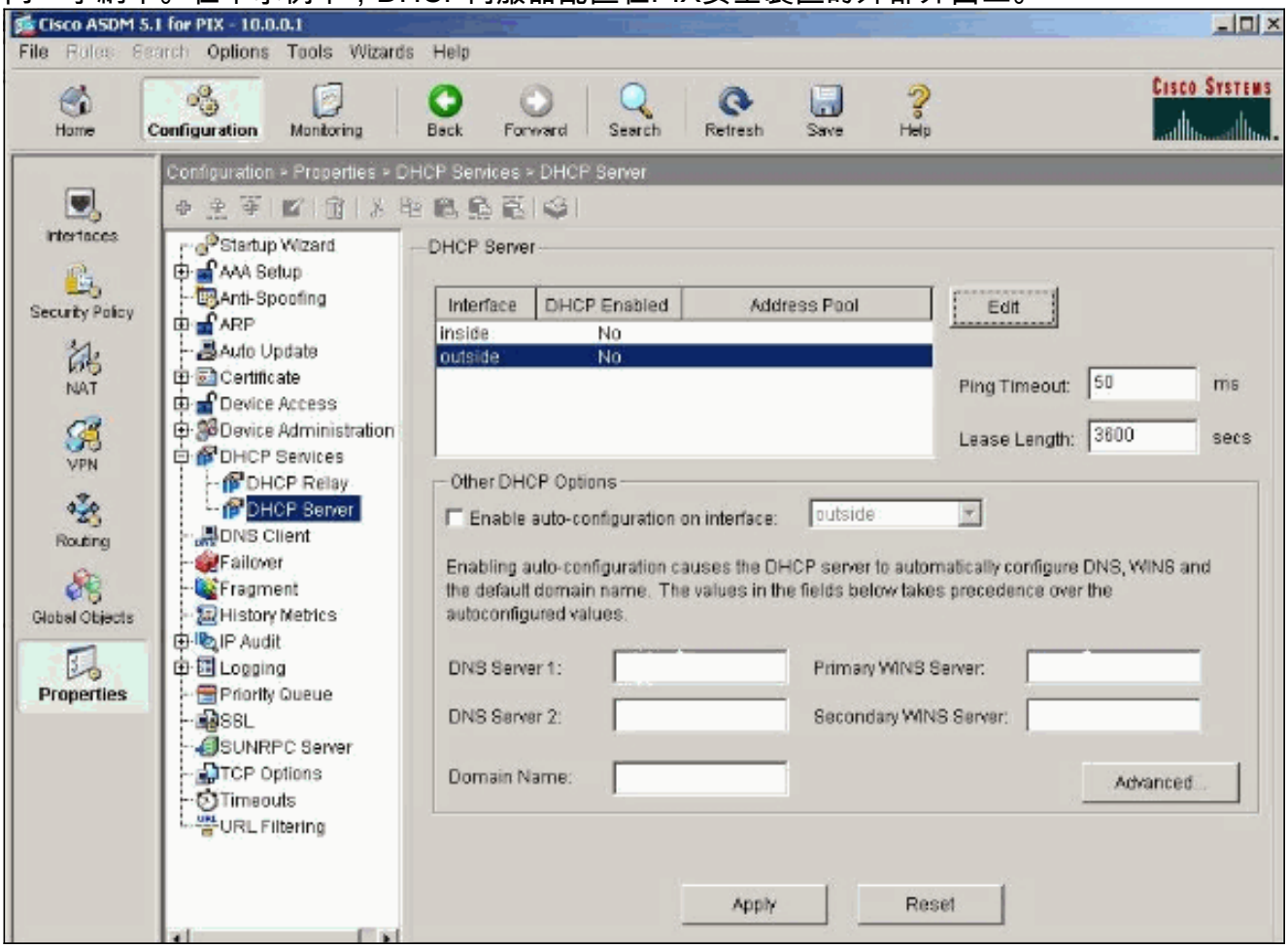
- 使用ASDM配置DHCP伺服器
- 使用ASDM配置DHCP客戶端

- DHCP伺服器組態
- DHCP使用者端組態

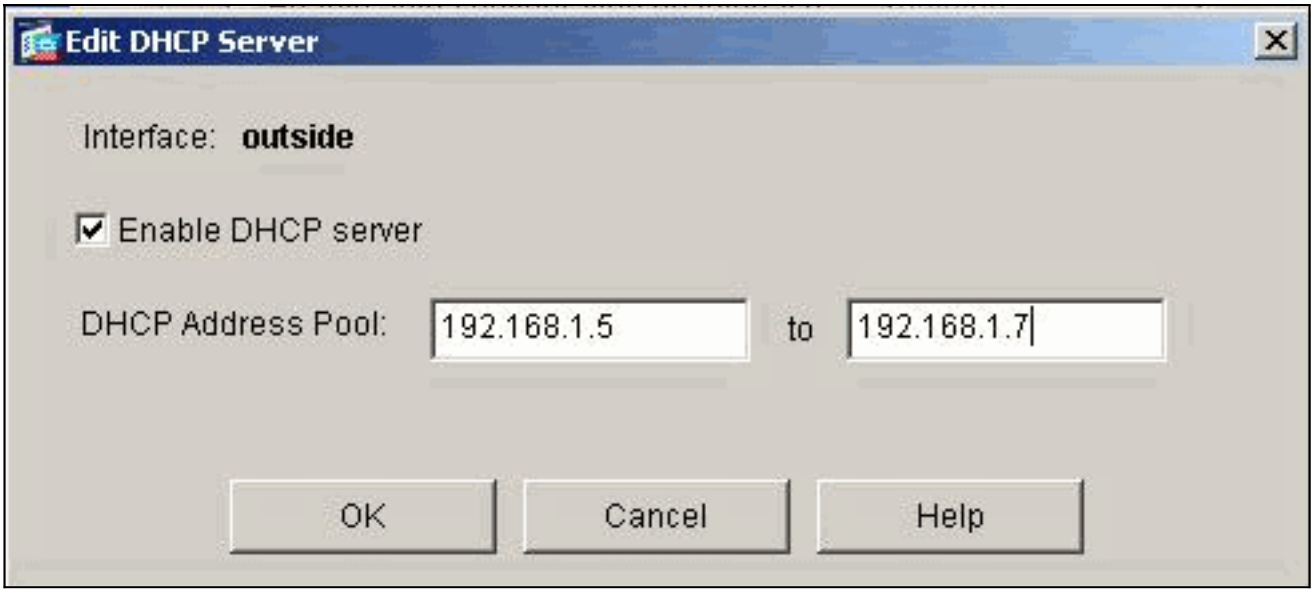
使用ASDM配置DHCP伺服器

完成以下步驟，使用ASDM將PIX安全裝置或ASA配置為DHCP伺服器。

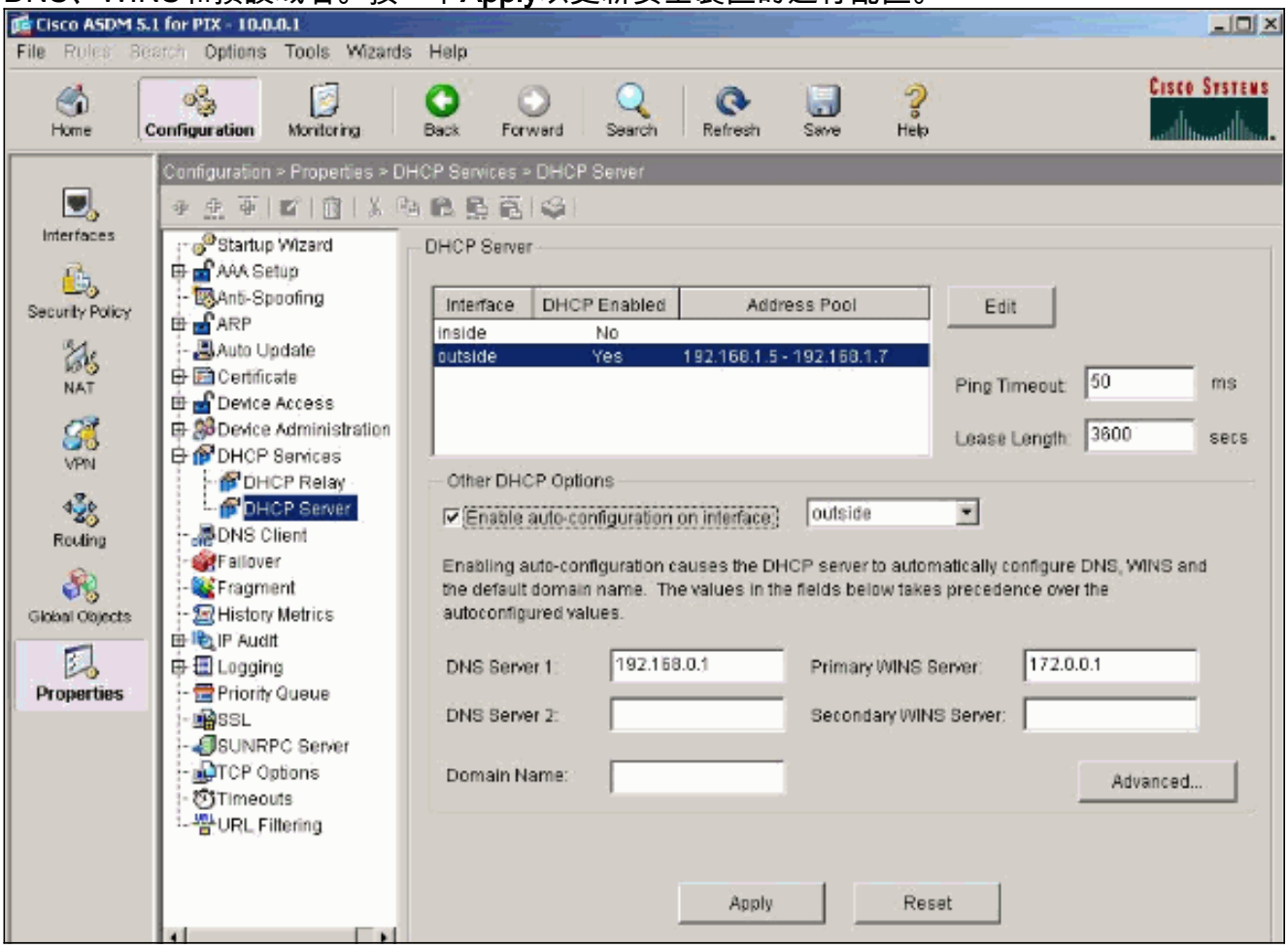
1. 從主視窗中選擇**Configuration > Properties > DHCP Services > DHCP Server**。選擇一個介面，然後按一下**Edit**以啟用DHCP伺服器並建立DHCP地址池。地址池必須與安全裝置介面位於同一子網中。在本示例中，DHCP伺服器配置在PIX安全裝置的外部介面上。



2. 選中**Enable DHCP server** on the outside interface以偵聽DHCP客戶端的請求。提供要傳送到DHCP客戶端的地址池，然後按一下**OK**以返回主視窗。



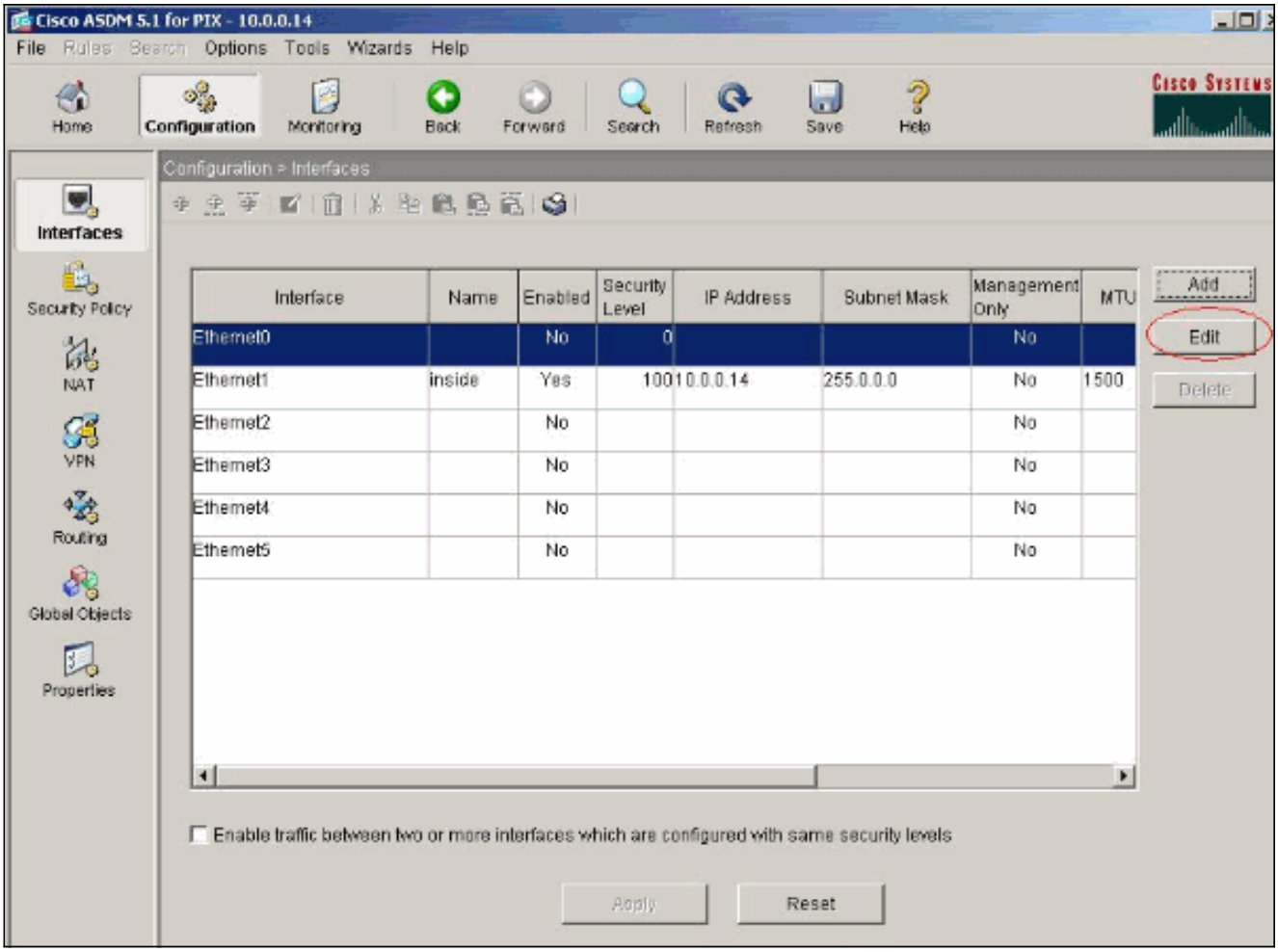
3. 選中**Enable auto-configuration on the interface**，以使DHCP伺服器自動配置DHCP客戶端的DNS、WINS和預設域名。按一下**Apply**以更新安全裝置的運行配置。



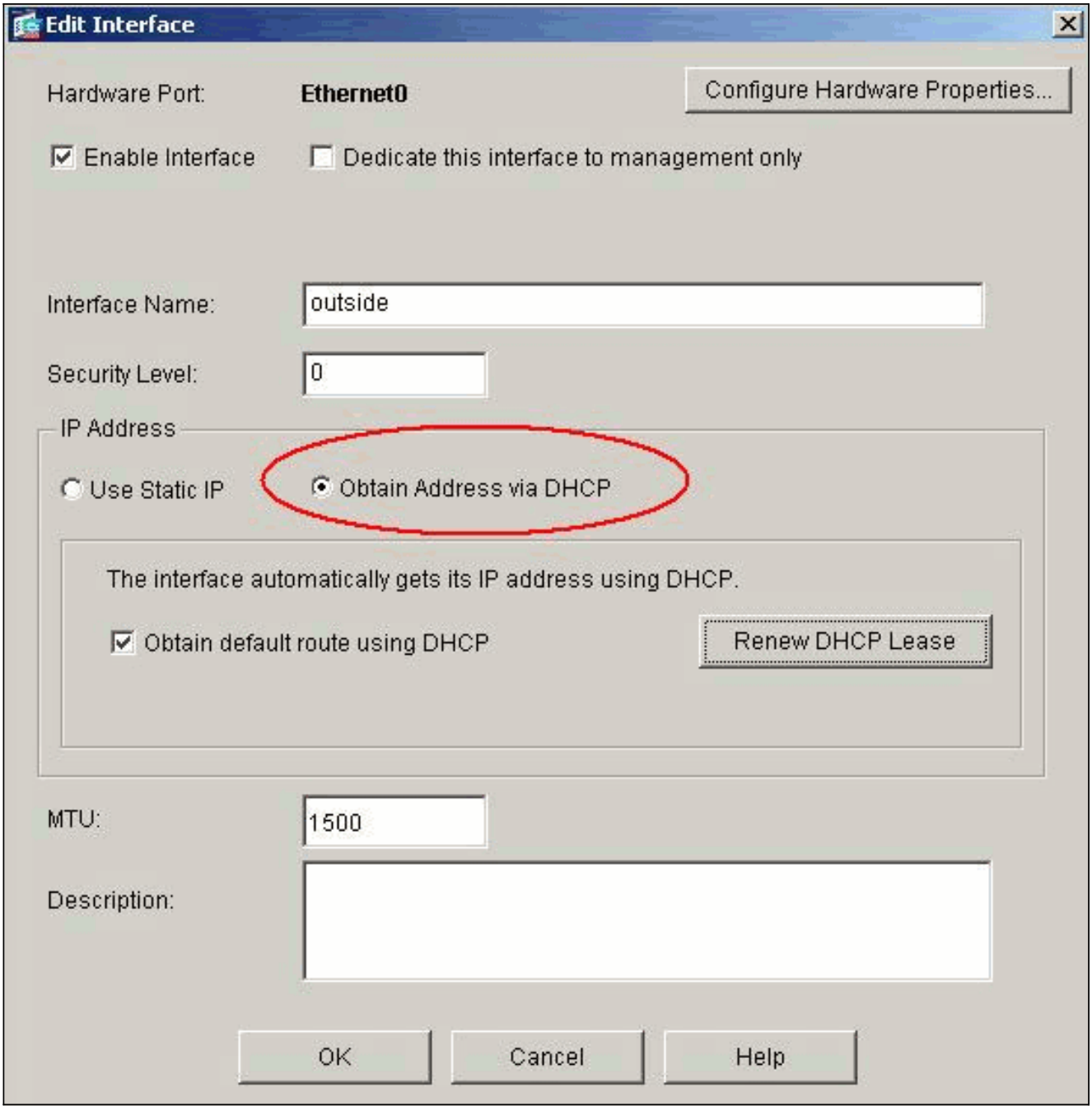
使用ASDM配置DHCP客戶端

完成以下步驟，使用ASDM將PIX安全裝置配置為DHCP客戶端。

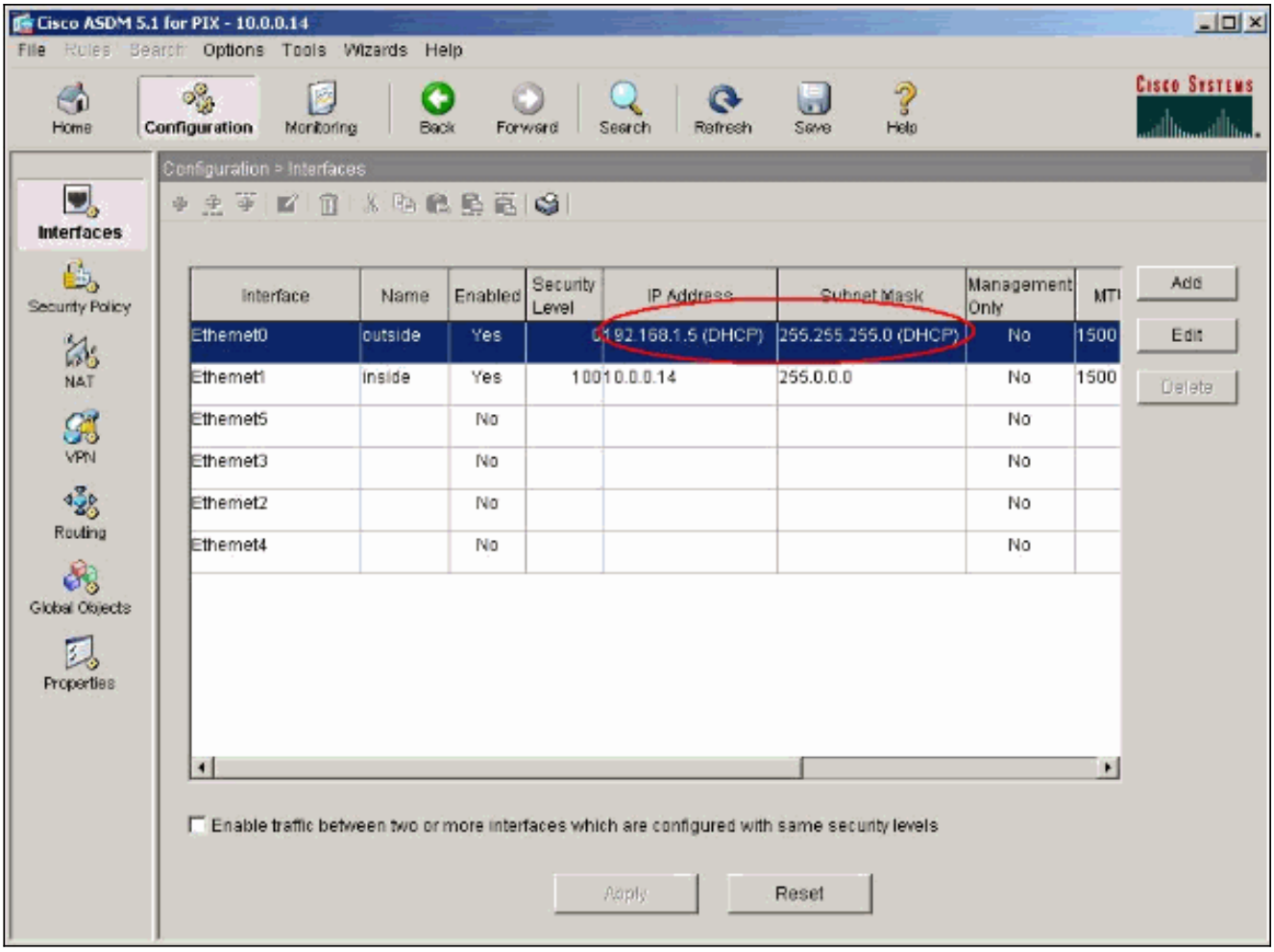
1. 選擇**Configuration > Interfaces**，然後按一下**Edit**以啟用Ethernet0介面從DHCP伺服器獲取配置引數，例如帶有子網掩碼的IP地址、預設網關、DNS伺服器和WINS伺服器IP地址。



2. 選中**Enable Interface**並輸入介面的介面名稱和安全級別。對於IP地址，選擇**Obtain address via DHCP**，對於預設網關，選擇**Obtain default route using DHCP**，然後按一下**OK**以轉至主視窗。



3. 按一下**Apply**檢視從DHCP伺服器為Ethernet0介面獲取的IP地址。



DHCP伺服器組態

此配置由ASDM建立：

DHCP伺服器

```
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使用者端組態

此配置由ASDM建立：

DHCP使用者端

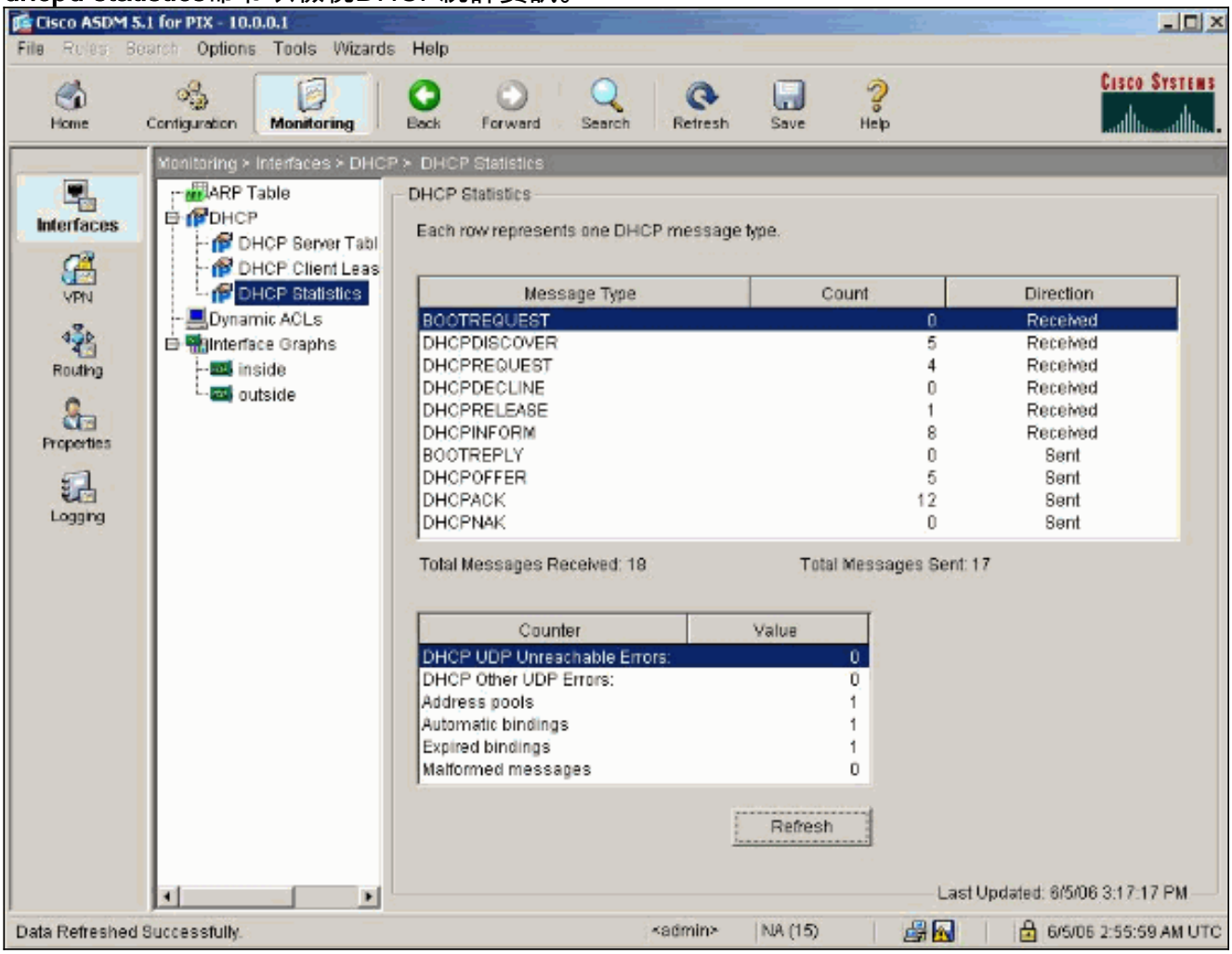
```
pixfirewall#show running-config
PIX Version 7.1(1)
!
hostname pixfirewall
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0
 nameif outside
 security-level 0

!--- 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
```

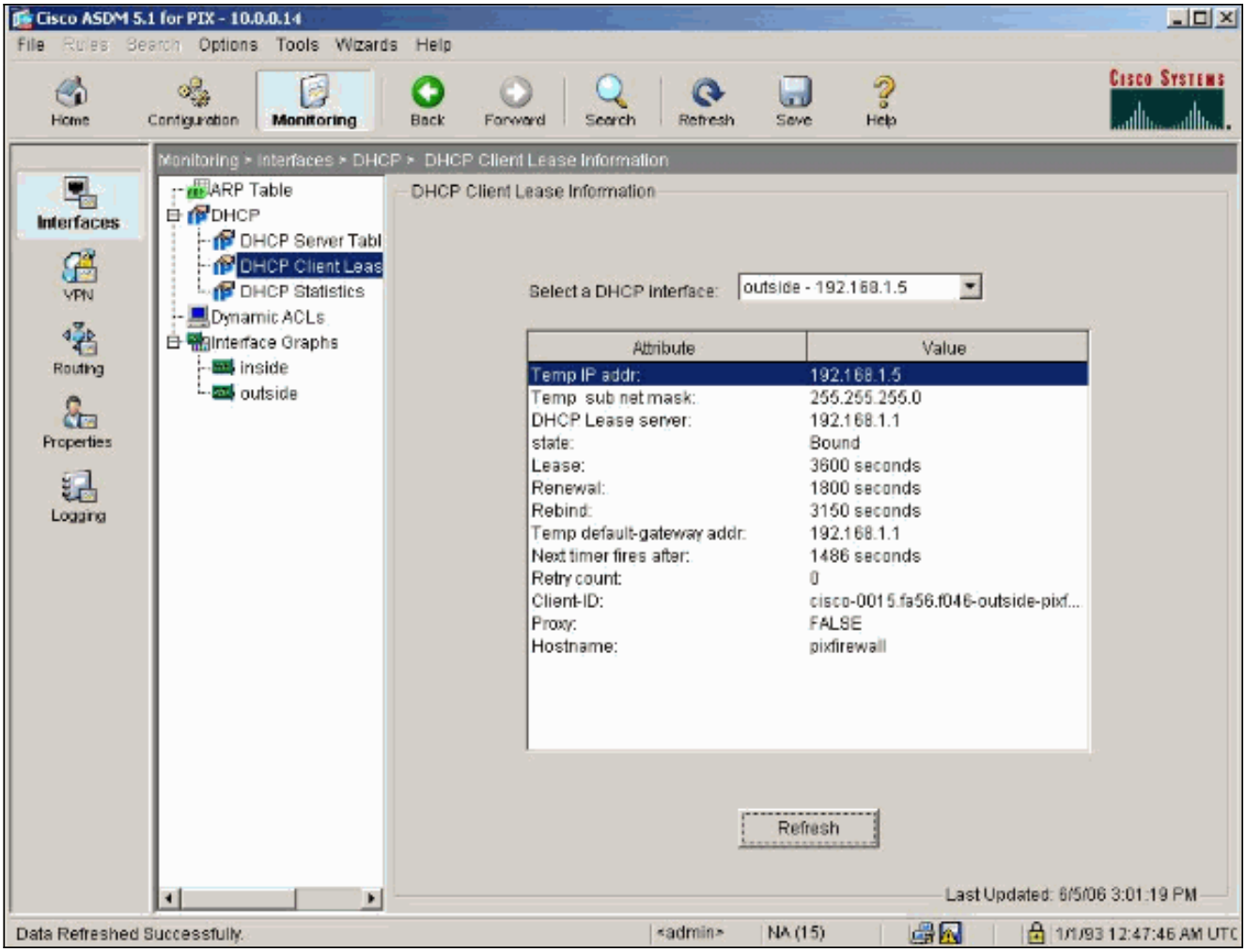
驗證

完成以下步驟，使用ASDM驗證DHCP統計資訊以及來自DHCP伺服器和DHCP客戶端的繫結資訊。

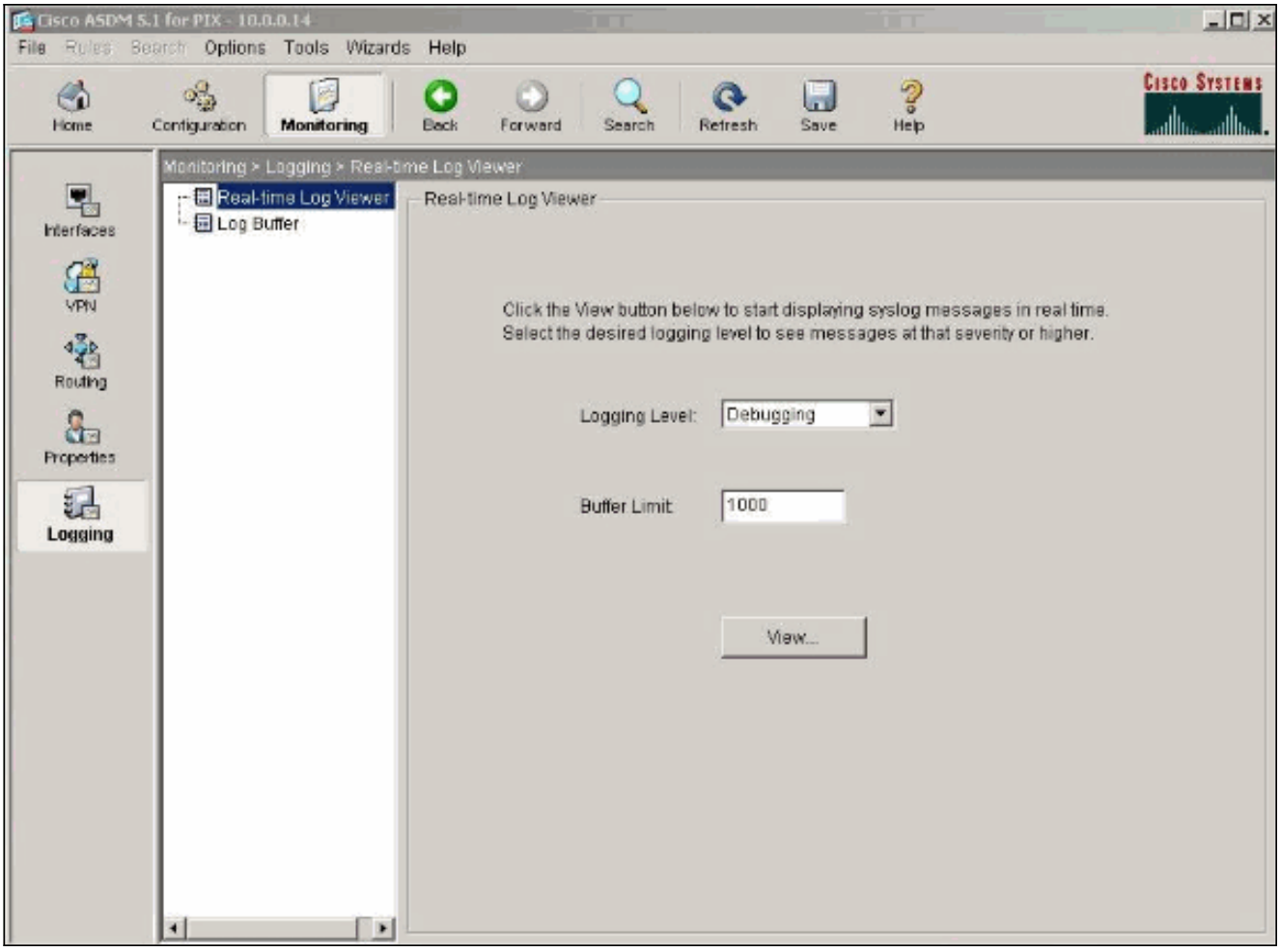
1. 從DHCP伺服器選擇**Monitoring > Interfaces > DHCP > DHCP Statistics**以驗證DHCP統計資訊，例如DHCPDISCOVER、DHCPREQUEST、DHCPOFFER和DHCPACK。從CLI輸入**show dhcpd statistics**命令以檢視DHCP統計資訊。



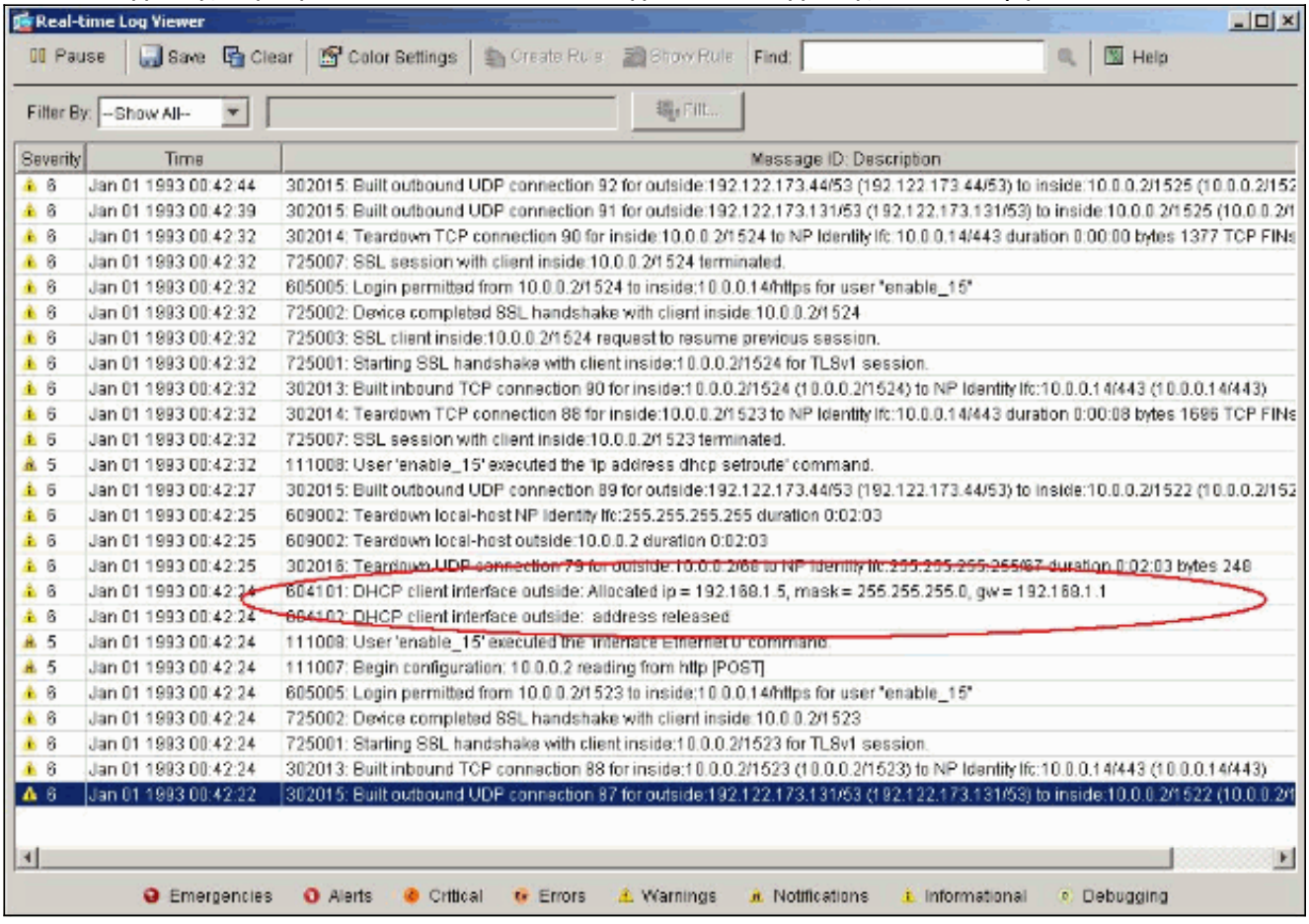
2. 從DHCP客戶端選擇**Monitoring > Interfaces > DHCP > DHCP Client Lease Information**以檢視DHCP繫結資訊。輸入**show dhcpd binding**命令以從CLI檢視DHCP繫結資訊。



3. 選擇**Monitoring > Logging > Real-time Log Viewer**以選擇Logging Level和緩衝區限制以檢視即時日誌消息。



4. 從DHCP客戶端檢視即時日誌事件。IP地址分配給DHCP客戶端的外部介面。



疑難排解

疑難排解指令

使用本節內容，確認您的組態是否正常運作。

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**show**命令輸出的分析。

附註：使用 **debug** 指令之前，請先參閱有關 Debug 指令的重要資訊。

- **debug dhcpd event** — 顯示與DHCP伺服器關聯的事件資訊。
- **debug dhcpd packet** — 顯示與DHCP伺服器關聯的資料包資訊。

錯誤消息

```
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
```

說明:在安全裝置上，地址池的大小限製為每池256個地址。不能更改，這是軟體限制。總數只能為256。如果地址池範圍大於253個地址（例如254、255、256），則安全裝置介面的網路掩碼不能是C類地址（例如255.255.255.0）。 它必須是更大的值，例如255.255.254.0。

有關如何將DHCP伺服器功能實施到安全裝置的資訊，請參閱思科安全裝置命令列配置指南。

常見問題：地址分配

問題 — 能否為使用ASA作為DHCP伺服器的電腦分配靜態/永久IP地址？

答案 — 無法使用PIX/ASA。

問題 — 是否有可能將DHCP地址與ASA上的特定MAC地址關聯？

答案 — 不，不可能。

相關資訊

- PIX安全裝置支援頁
- Cisco Secure PIX防火牆命令參考
- 技術支援與文件 - Cisco Systems