Exemple de configuration de PIX/ASA en tant que serveur et client DHCP

Table des matières

Introduction

Le dispositif de sécurité de la gamme PIX 500 et le Dispositif de sécurité adaptatif Cisco (ASA) fonctionnent à la fois comme serveurs de Protocole de configuration dynamique d'hôte (DHCP) et clients DHCP. DHCP est un protocole qui fournit des paramètres de configuration automatique tels qu'une adresse IP avec un masque de sous-réseau, une passerelle par défaut, un serveur DNS et une adresse IP de serveur WINS aux hôtes.

Le dispositif de sécurité peut agir comme serveur DHCP ou client DHCP. Quand il fonctionne en tant que serveur, le dispositif de sécurité fournit des paramètres de configuration réseau directement aux clients DHCP. Quand il fonctionne en tant que client DHCP, le dispositif de sécurité réclame de tels paramètres de configuration d'un serveur DHCP.

Ce document fait le point sur la façon de configurer le serveur DHCP et le client DHCP à l'aide de Cisco Adaptive Security Device Manager (ASDM) sur le dispositif de sécurité.

Conditions préalables

Exigences

Ce document suppose que le dispositif de sécurité PIX ou ASA est entièrement opérationnel et configuré pour permettre à Cisco ASDM d'apporter des modifications de configuration.

Remarque : référez-vous à Autoriser l'accès HTTPS pour ASDM pour permettre au périphérique d'être configuré par l'ASDM.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Dispositif de sécurité de la gamme PIX 500 7.x

  Remarque : la configuration CLI PIX utilisée dans la version 7.x s'applique également à PIX 6.x. La seule différence est que dans les versions plus récentes que PIX 6.3, le serveur DHCP peut seulement être activé sur l'interface interne. Dans PIX 6.3 et les versions ultérieures, le serveur DHCP peut être activé sur n'importe laquelle des interfaces disponibles. Dans cette configuration, l'interface externe est utilisée pour la fonctionnalité serveur DHCP.

- ASDM 5.x

  Remarque : ASDM ne prend en charge que PIX 7.0 et versions ultérieures. Le PIX Device Manager (PDM) est disponible pour configurer PIX version 6.x. Référez-vous à Compatibilité matérielle et logicielle des dispositifs de sécurité des gammes Cisco ASA 5500 et PIX 500 pour plus d'informations.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Produits connexes

Cette configuration peut également être utilisée avec Cisco ASA 7.x.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous aux Conventions relatives aux conseils techniques Cisco.

Configurer

Dans cette configuration, il y a deux dispositifs de sécurité PIX qui exécutent la version 7.x. Un fonctionne comme serveur DHCP qui fournit des paramètres de configuration à un autre dispositif de sécurité PIX 7.x qui fonctionne comme client DHCP. Lorsqu'il fonctionne comme serveur DHCP, le PIX affecte dynamiquement des adresses IP aux clients DHCP d'un pool d'adresses IP désignées.

Vous pouvez configurer un serveur DHCP sur chaque interface du dispositif de sécurité. Chaque interface peut avoir son propre pool d'adresses à exploiter. Cependant, les autres paramètres DHCP, tels que serveurs DNS, nom de domaine, options, timeout ping et serveurs WINS, sont configurés globalement et utilisés par le serveur DHCP sur toutes les interfaces.

Vous ne pouvez pas configurer des services client DHCP ou relais DHCP sur une interface sur laquelle le serveur est activé. Par ailleurs, des clients DHCP doivent être directement connectés à l'interface sur laquelle le serveur est activé.

Finalement, alors que le serveur DHCP est activé sur une interface, vous ne pouvez pas modifier l'adresse IP de cette interface.

Remarque : il n'existe aucune option de configuration permettant de définir l'adresse de passerelle par défaut dans la réponse DHCP envoyée depuis le serveur DHCP (PIX/ASA). Le serveur DHCP envoie toujours sa propre adresse comme passerelle pour le client DHCP. Toutefois, la définition d'une route par défaut qui indique le routeur Internet permet à l'utilisateur d'atteindre Internet.

Remarque : le nombre d'adresses de pool DHCP pouvant être attribuées dépend de la licence utilisée dans l'appliance de sécurité (PIX/ASA). Si vous utilisez la licence de base/Sécurité Plus, alors ces limites s'appliquent au pool DHCP. Si la limite est de 10 hôtes, vous limitez le pool DHCP à 32 adresses. Si la limite est de 50 hôtes, vous limitez le pool DHCP à 128 adresses. Si la limite est illimitée, vous limitez le pool DHCP à 256 adresses. Ainsi le pool d'adresses est limité selon le nombre d'hôtes.

Remarque : utilisez l'outil de recherche de commandes (clients enregistrés uniquement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Ce document utilise les configurations suivantes :

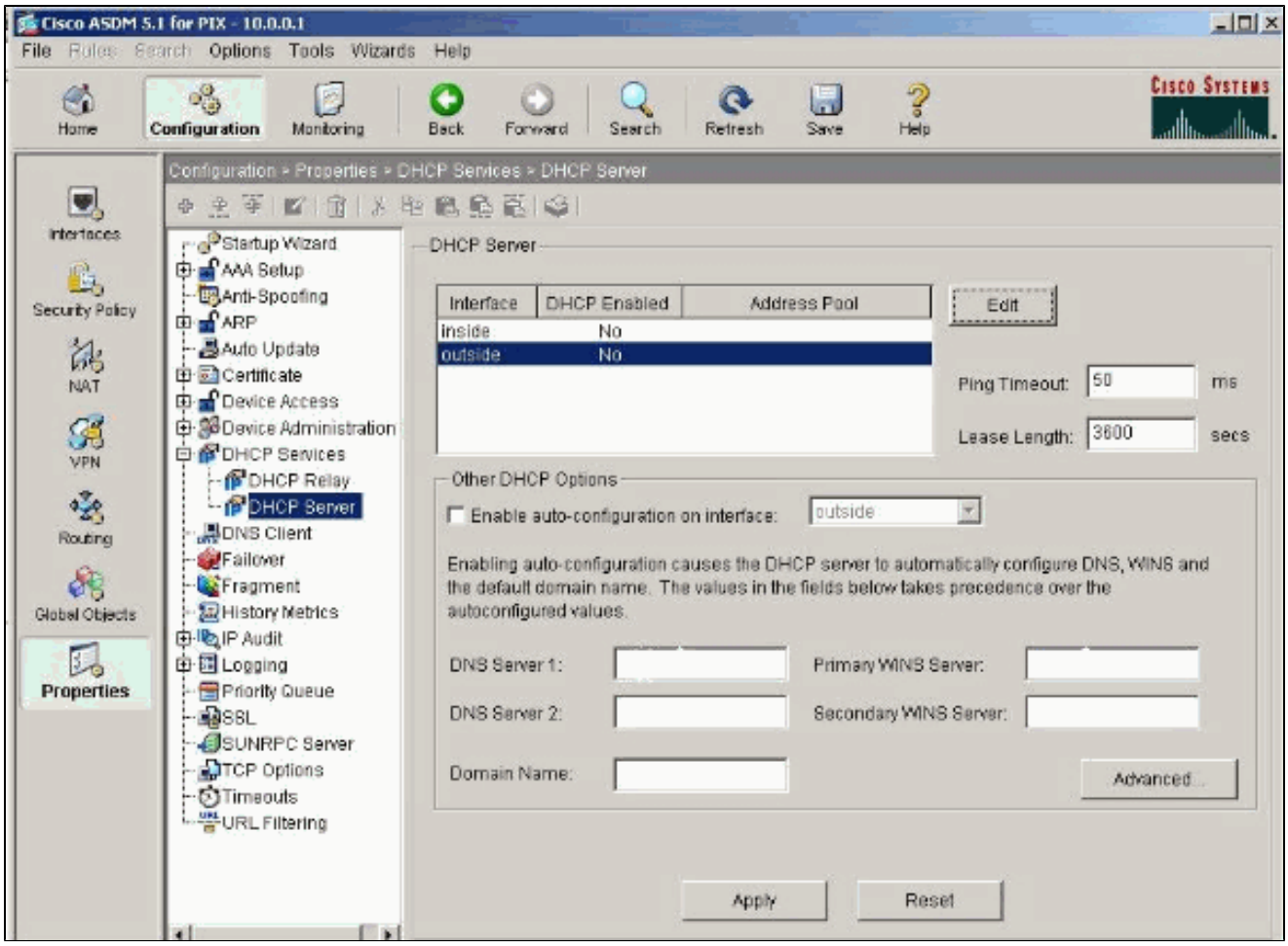
- Configuration du serveur DHCP à l'aide de ASDM
- Configuration du client DHCP à l'aide de ASDM
- Configuration du serveur DHCP
- Configuration du client DHCP

Configuration du serveur DHCP à l'aide de ASDM

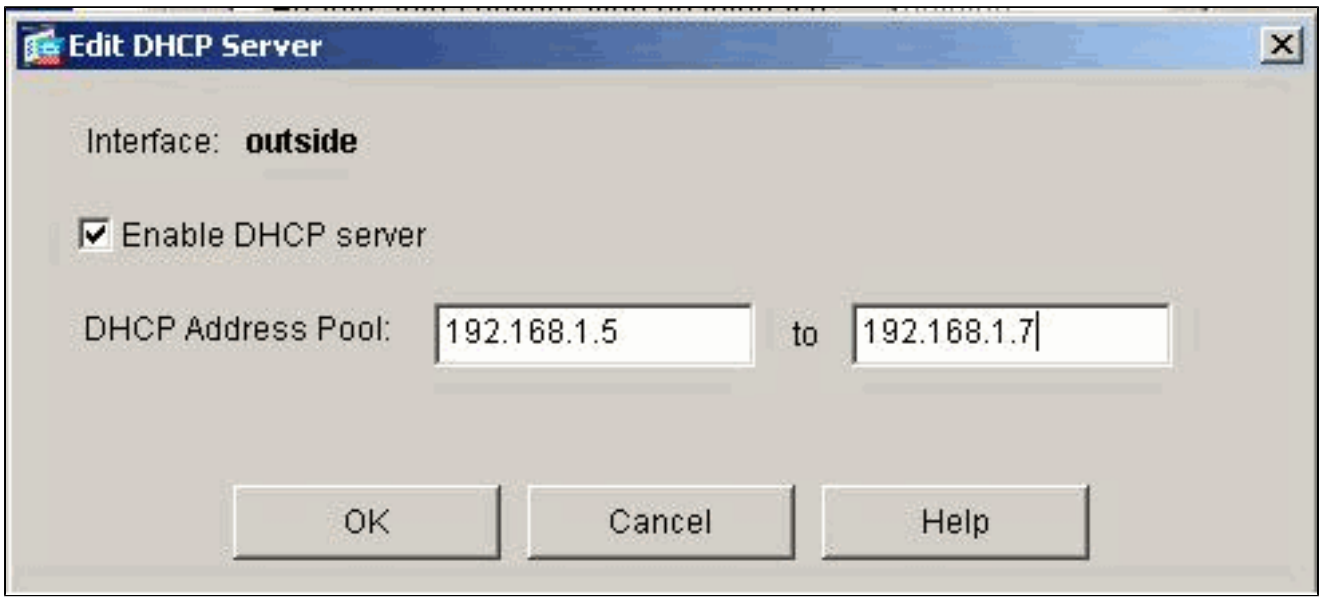
Complétez ces étapes pour configurer le dispositif de sécurité PIX ou ASA comme serveur DHCP à l'aide de ASDM.

1. Choisissez Configuration > Properties > DHCP Services > DHCP Server dans la fenêtre d'accueil. Sélectionnez une interface et cliquez sur Edit pour activer le serveur DHCP et créer un pool d'adresses DHCP.

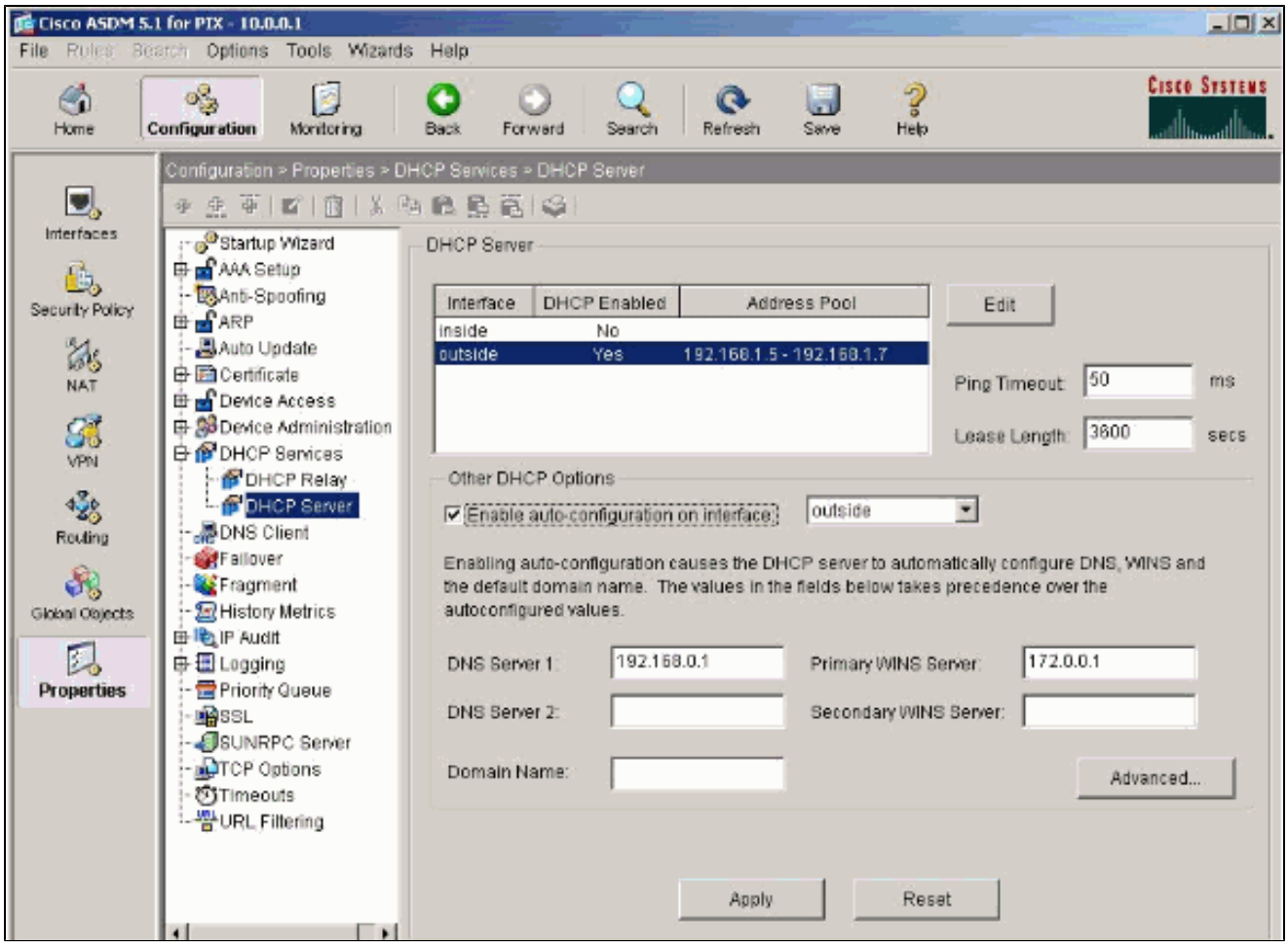
   Le pool d'adresses doit être sur le même sous-réseau que l'interface du dispositif de sécurité. Dans cet exemple, le serveur DHCP est configuré sur l'interface externe du dispositif de sécurité PIX.



2. Vérifiez l'option Enable DHCP server sur l'interface externe pour écouter les requêtes des clients DHCP. Fournissez le pool d'adresses pour le client DHCP et cliquez sur OK pour revenir à la fenêtre principale.



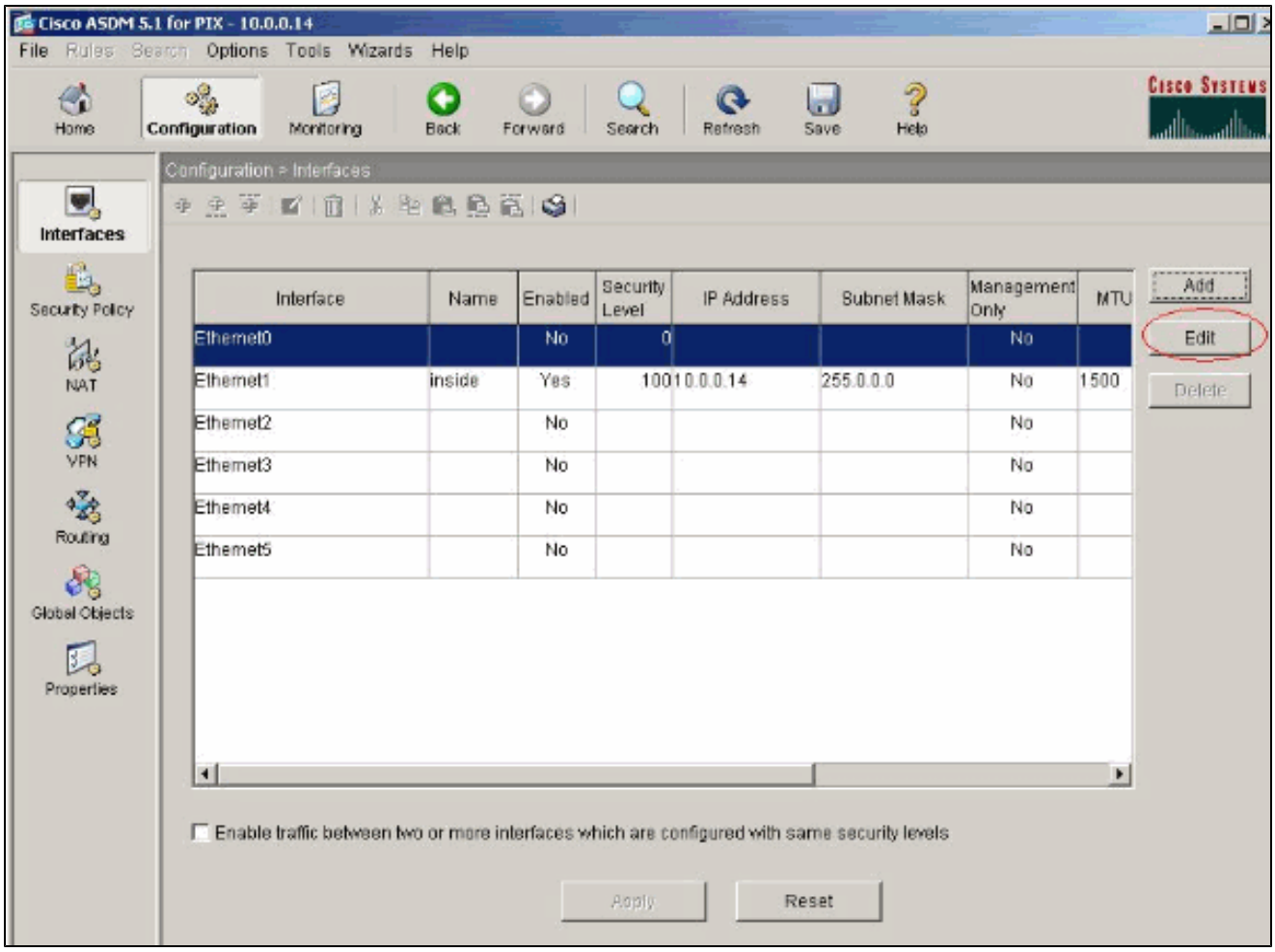
3. Cochez Enable auto-configuration on the interface pour que le serveur DHCP configure automatiquement le DNS, le WINS et le nom de domaine par défaut pour le client DHCP. Cliquez sur Apply pour mettre à jour la configuration en cours du dispositif de sécurité.



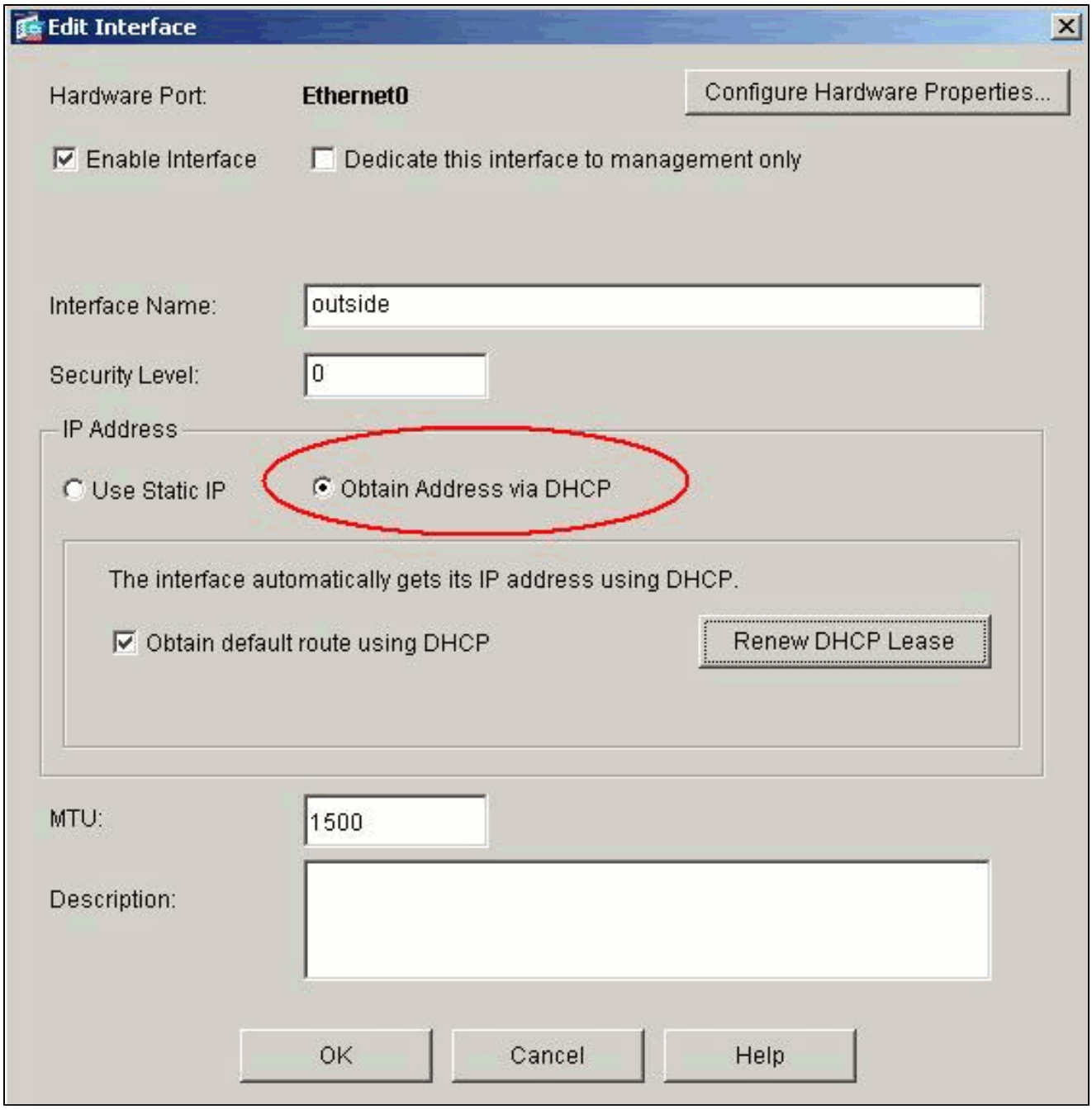
Configuration du client DHCP à l'aide de ASDM

Complétez ces étapes pour configurer le dispositif de sécurité PIX en tant que client DHCP à l'aide de ASDM.

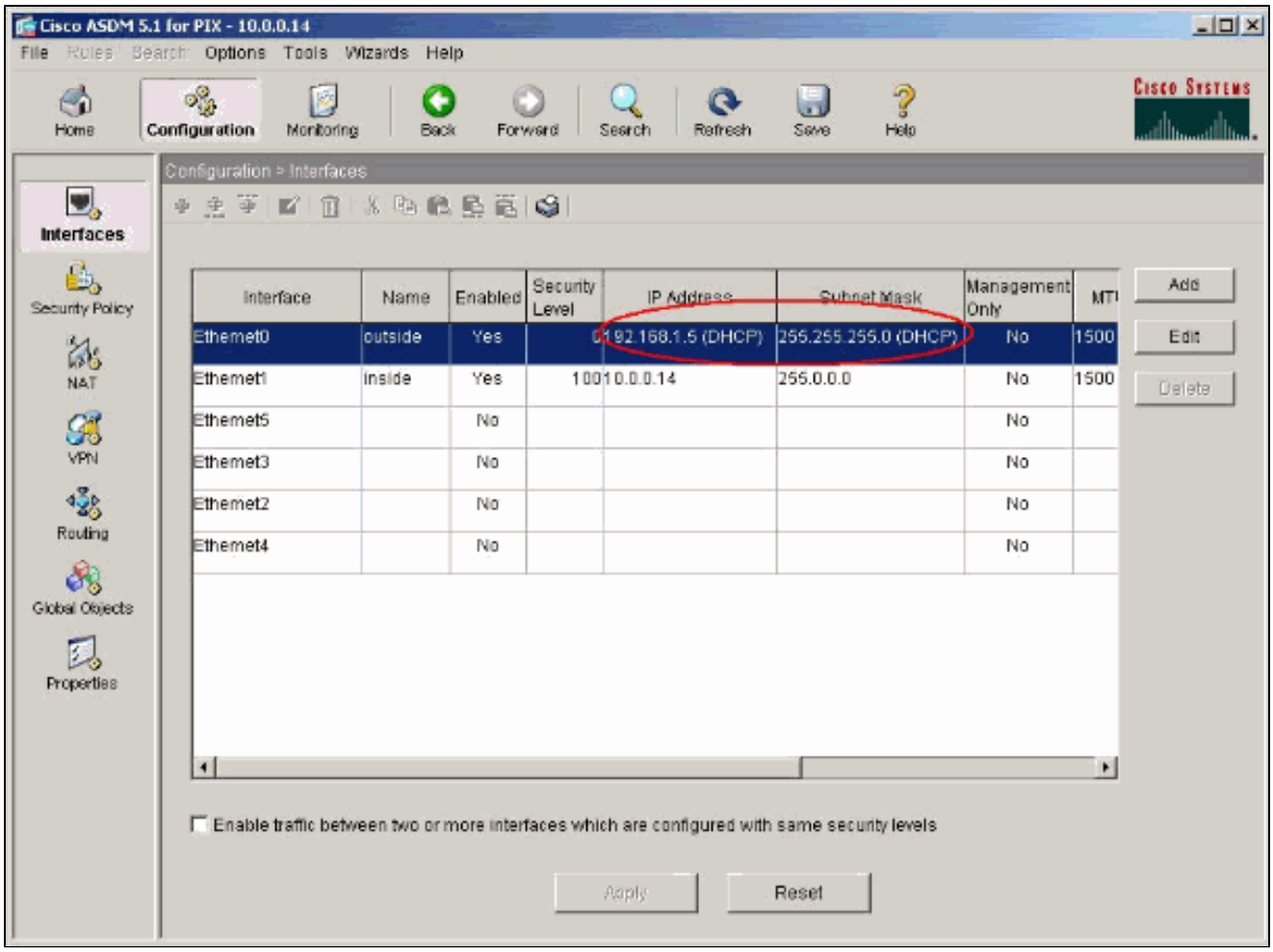
1. Choisissez Configuration > Interfaces et cliquez sur Edit pour permettre à l'interface Ethernet0 d'obtenir les paramètres de configuration tels qu'une adresse IP avec un masque de sous-réseau, une passerelle par défaut, un serveur DNS et un serveur WINS du serveur DHCP.



2. Cochez Enable Interface et saisissez le nom d'interface et le niveau de sécurité pour l'interface. Choisissez Obtain address via DHCP pour l'adresse IP et Obtain default route using DHCP pour la passerelle par défaut, puis cliquez sur OK pour revenir à la fenêtre principale.



3. Cliquez sur Apply pour voir l'adresse IP obtenue pour l'interface Ethernet0 du serveur DHCP.



Configuration du serveur DHCP

Cette configuration est créée par l'ASDM :

```
<#root>

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


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


dhcpd enable outside

dhcprelay timeout 60
!

!--- Output is suppressed.
```

```
service-policy global_policy global
Cryptochecksum:7a8cd028ee1c56083b64237c832fb5ab
: end
```

Configuration du client DHCP

Cette configuration est créée par l'ASDM :

Client DHCP

```
<#root>

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 DHCI




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
```

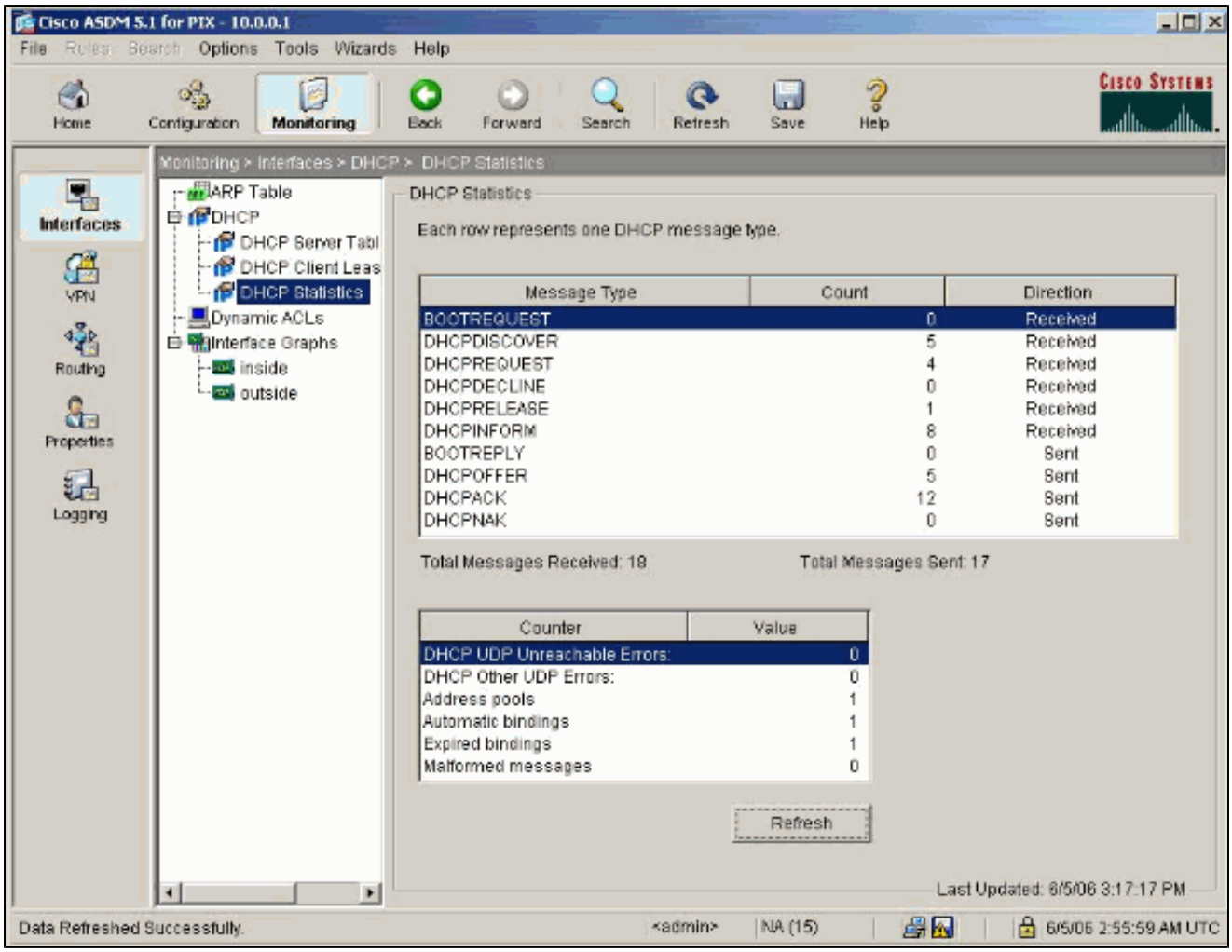
```
logging enable
logging console debugging
logging asdm informational
mtu outside 1500
mtu inside 1500
no failover

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
```

Vérifier

Complétez ces étapes pour vérifier les statistiques DHCP et les informations obligatoires du serveur DHCP et du client DHCP à l'aide de l'ASDM.

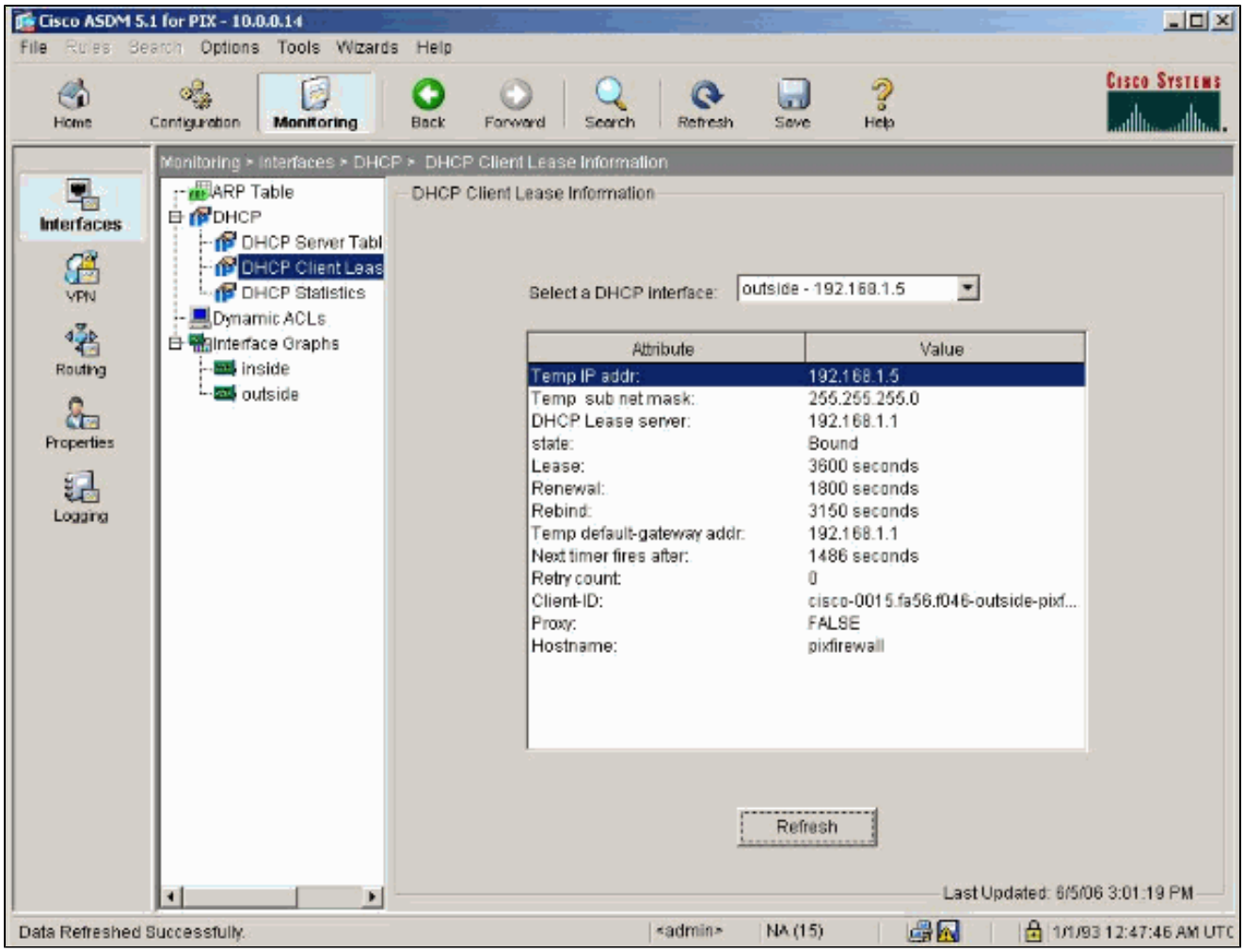
1. Choisissez Monitoring > Interfaces > DHCP > DHCP Statistics dans le serveur DHCP pour vérifier les statistiques DHCP, telles que DHCPDISCOVER, DHCPREQUEST, DHCPOFFER et DHCPACK.

   Saisissez la commande show dhcpd statistics dans le CLI pour afficher les statistiques DHCP.

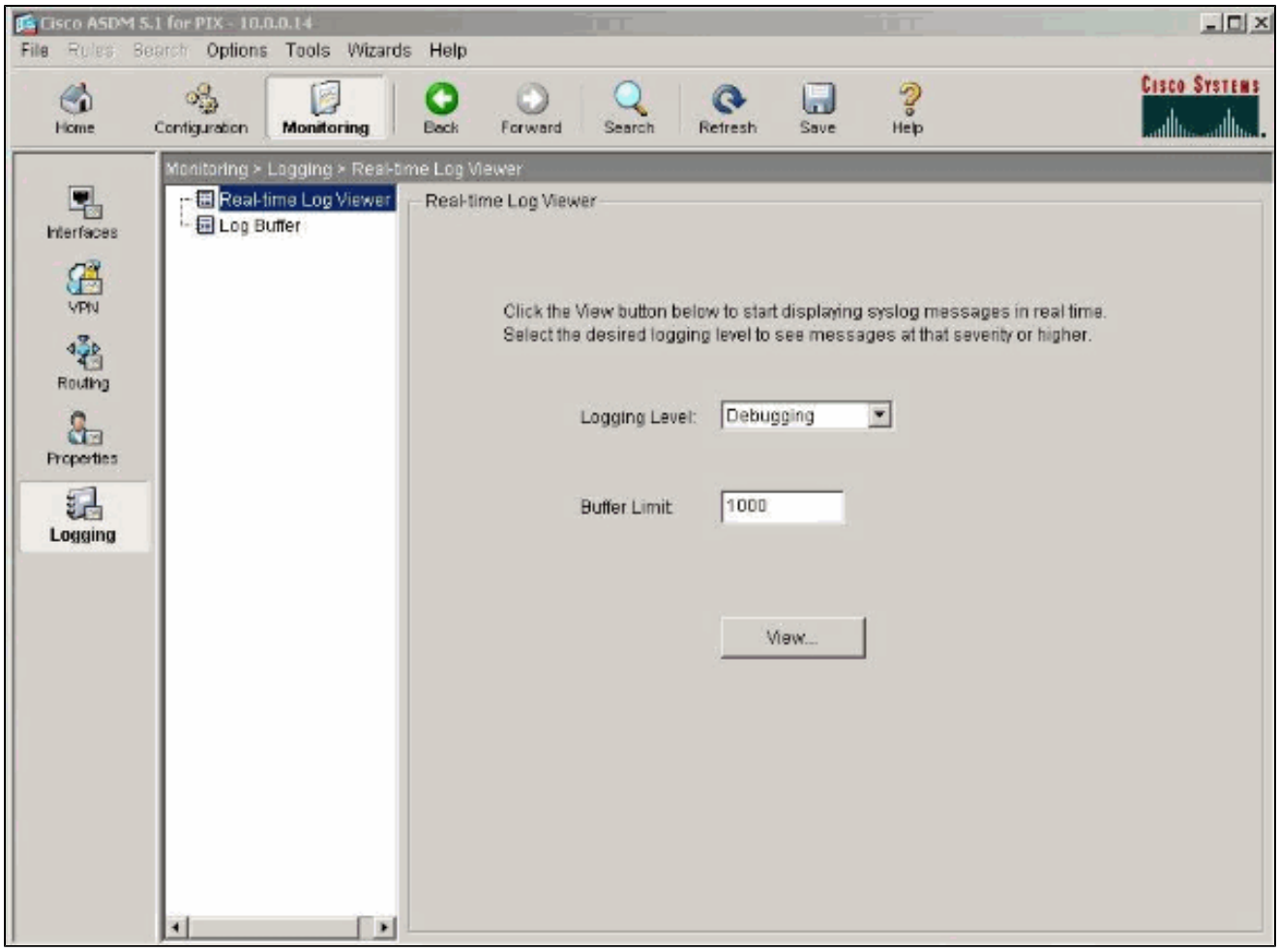


2. Choisissez Monitoring > Interfaces > DHCP > DHCP Client Lease Information dans le client DHCP pour afficher les informations obligatoires DHCP.

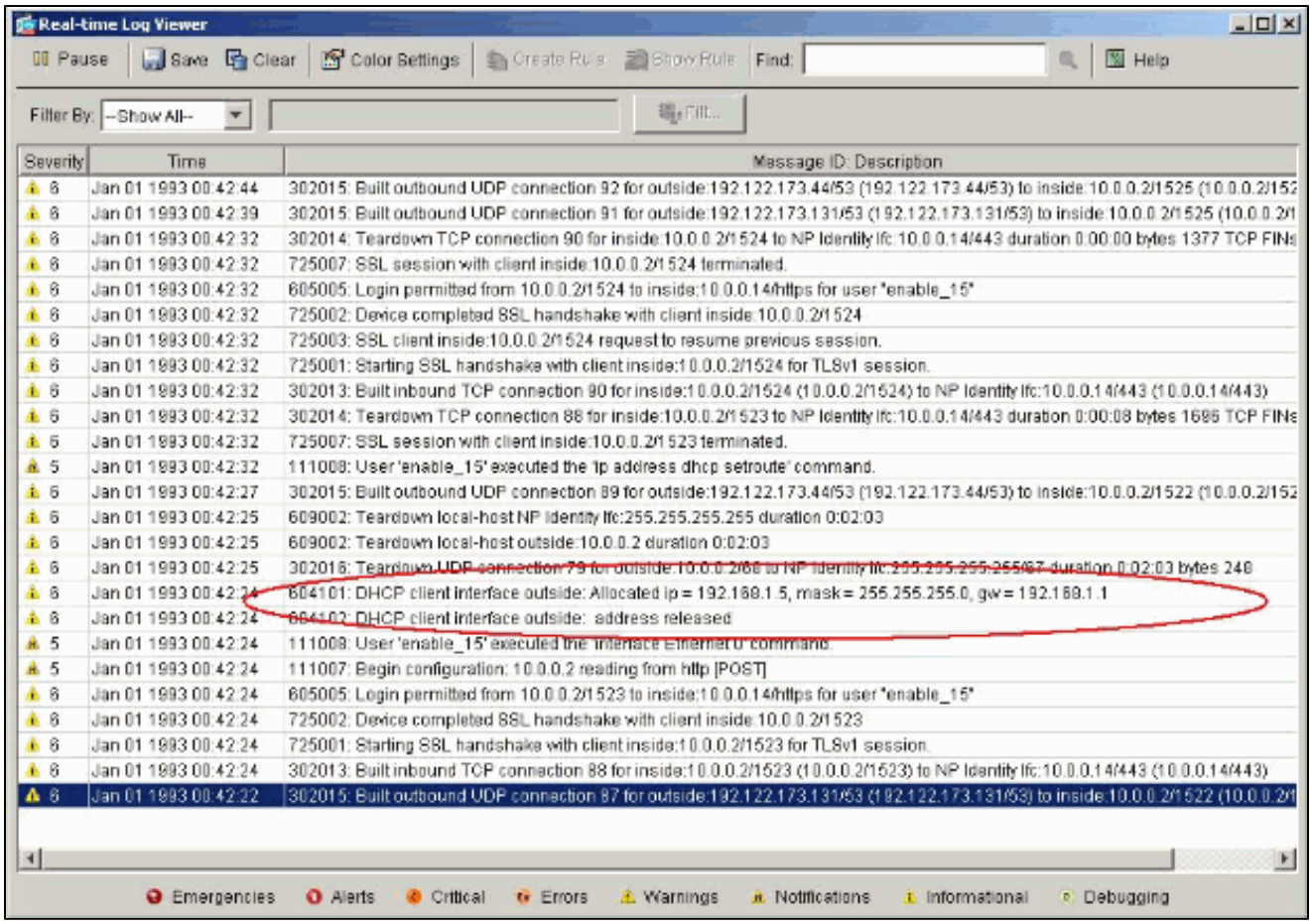
   Sélectionnez la commande show dhcpd binding pour afficher les informations obligatoires DHCP du CLI.



3. Choisissez Monitoring > Logging > Real-time Log Viewer pour sélectionner le niveau de journalisation et la limite de mémoire tampon pour afficher les messages du journal en temps réel.



4. Affichez les événements en temps réel du journal du client DHCP. L'adresse IP est affectée à l'interface externe du client DHCP.



Dépannage

Dépannage des commandes

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes show. Utilisez l'OIT pour afficher une analyse de la sortie de la commande show .

Remarque : Consulter les renseignements importants sur les commandes de débogage avant d'utiliser les commandes de débogage.

- debug dhcpd event — affiche les informations sur l'événement qui sont associées au serveur DHCP.
- debug dhcpd packet — affiche les informations de paquet qui sont associées au serveur DHCP.

Messages d'erreur

<#root>

```
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
```

Explication : la taille du pool d'adresses est limitée à 256 adresses par pool sur l'appliance de sécurité. Cette option ne peut pas être modifiée et est une limitation logicielle. Le total peut être seulement 256. Si la portée du pool d'adresses est plus étendue que 253 adresses (par exemple 254, 255, 256), le masque de réseau de l'interface du dispositif de sécurité ne peut pas être une adresse de classe C (par exemple, 255.255.255.0). Cela doit être plus important, par exemple, 255.255.254.0.

Consultez Guide de configuration de la ligne de commande des dispositifs de sécurité de Cisco pour obtenir des informations sur la façon d'implémenter la fonctionnalité du serveur DHCP dans le dispositif de sécurité.

FAQ : Attribution d'adresse

Question — Est-il possible d'affecter une adresse IP statique/permanente à l'ordinateur qui utilise ASA comme le serveur DHCP ?

Réponse — Cela n'est pas possible avec PIX/ASA.

Question — Est-il possible d'attacher des adresses DHCP aux adresses MAC spécifiques sur ASA ?

Réponse — Non, ce n'est pas possible.

Informations connexes

- Page d'assistance pour les dispositifs de sécurité PIX
- Références des commandes du pare-feu Cisco Secure PIX
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.