Configuración del relé DHCP del dispositivo de seguridad adaptable (ASA)

Contenido

Introducción

Este documento describe la retransmisión DHCP en Cisco ASA con la ayuda de las capturas y depuraciones de paquetes, y proporciona un ejemplo de configuración.

Prerequisites

Un agente de retransmisión de protocolo de configuración dinámica de host (DHCP) permite al dispositivo de seguridad reenviar solicitudes DHCP de clientes a un router u otro servidor DHCP conectado a una interfaz diferente.

Estas restricciones sólo se aplican al uso del agente de retransmisión DHCP:

- El agente de retransmisión no se puede activar si la función de servidor DHCP también está activada.
- Debe estar conectado directamente al dispositivo de seguridad y no puede enviar solicitudes a través de otro agente de retransmisión o un router.
- Para el modo de contexto múltiple, no puede habilitar la retransmisión DHCP, o configurar un servidor de retransmisión DHCP, en una interfaz que es utilizada por más de un contexto.

Los servicios de retransmisión DHCP no están disponibles en el modo de firewall transparente. Un dispositivo de seguridad en modo de firewall transparente solo permite el paso del tráfico del protocolo de resolución de direcciones (ARP). El resto del tráfico requiere una lista de control de acceso (ACL). Para permitir las solicitudes y respuestas DHCP a través del dispositivo de seguridad en modo transparente, debe configurar dos ACL:

- Una ACL que permite las solicitudes DHCP desde la interfaz interna hacia el exterior.
- Una ACL que permite las respuestas del servidor en la otra dirección.

Requirements

Cisco recomienda tener conocimientos básicos de ASA CLI y Cisco IOS® CLI.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Dispositivo de seguridad ASA serie 5500-x, versión 9.x o posterior
- Cisco 1800 series routers

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

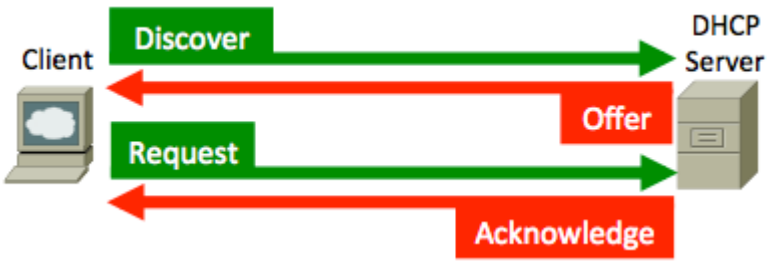
Antecedentes

El protocolo DHCP proporciona parámetros de configuración automática, como una dirección IP con una máscara de subred, una puerta de enlace predeterminada, una dirección de servidor DNS y una dirección WINS (del inglés Windows Internet Name Service, Servicio de nombres de Internet de Windows) a los hosts. Inicialmente, los clientes DHCP no tienen ninguno de estos parámetros de configuración. Para obtener esta información, envían una solicitud de difusión. Cuando un servidor DHCP ve esta solicitud, el servidor DHCP proporciona la información necesaria. Debido a la naturaleza de estas solicitudes de difusión, el cliente y el servidor DHCP deben estar en la misma subred. Los dispositivos de capa 3, como routers y firewalls, no suelen reenviar estas solicitudes de difusión de forma predeterminada.

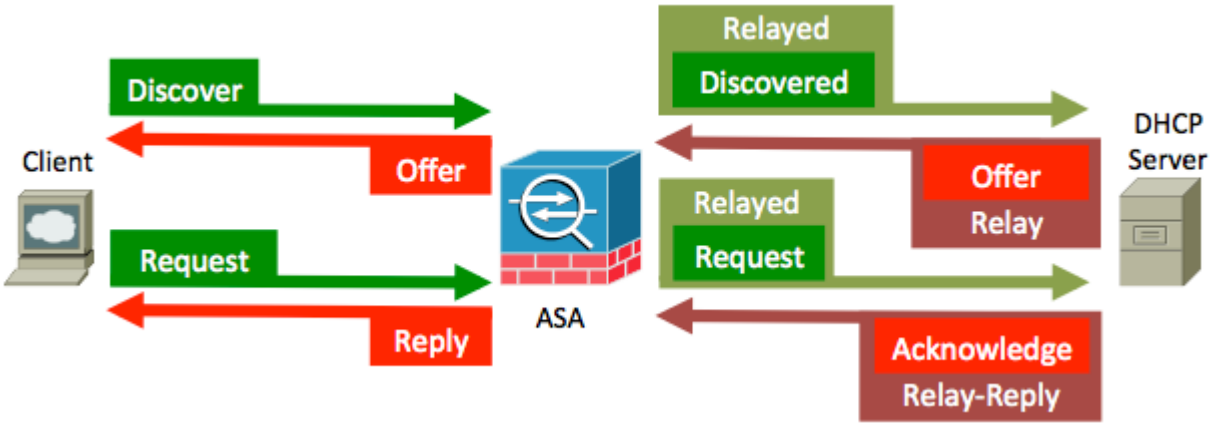
No siempre es conveniente intentar localizar clientes DHCP y un servidor DHCP en la misma subred. En tal situación, puede utilizar la retransmisión DHCP. Cuando el agente de retransmisión DHCP del dispositivo de seguridad recibe una solicitud DHCP de un host en una interfaz interna, reenvía la solicitud a uno de los servidores DHCP especificados en una interfaz externa. Cuando el servidor DHCP responde al cliente, el dispositivo de seguridad reenvía esa respuesta. Por lo tanto, el agente de retransmisión DHCP actúa como un proxy para el cliente DHCP en su conversación con el servidor DHCP.

Flujo de paquetes

Esta imagen ilustra el flujo de paquetes DHCP cuando no se utiliza un agente de retransmisión DHCP:



El ASA intercepta estos paquetes y los envuelve en el formato de retransmisión DHCP:



Retransmisión DHCP con captura de paquetes en la interfaz interna y externa de ASA

Tome nota del contenido resaltado en ROJO, porque así es como ASA modifica varios campos.

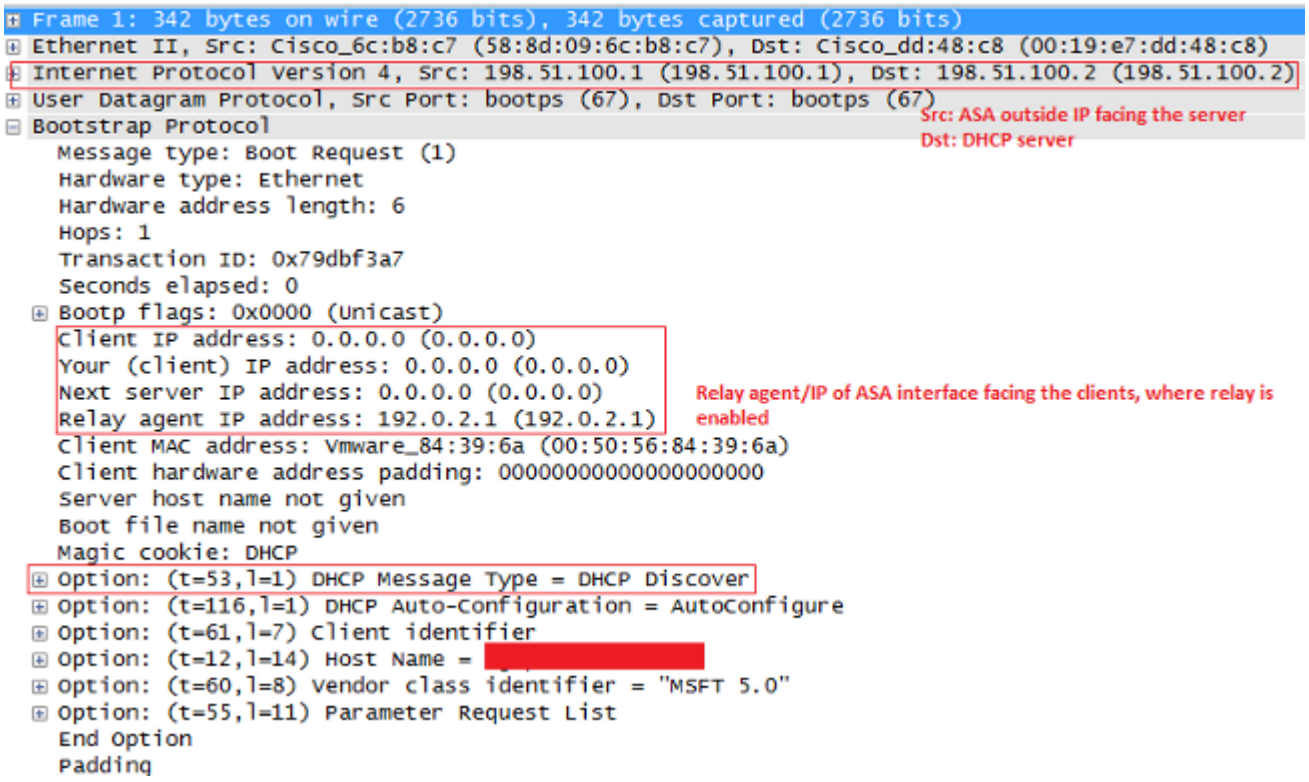
1. Para iniciar el proceso DHCP, inicie el sistema y envíe un mensaje de difusión (DHCPDISCOVER) a la dirección de destino 255.255.255.255 - puerto UDP 67.

```
⊞ Frame 1: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
⊞ Ethernet II, Src: Vmware_84:39:6a (00:50:56:84:39:6a), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
⊞ User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
⊟ Bootstrap Protocol                                   Src IP: No ip on client
                                                       Dst: L3 Broadcast
    Message type: Boot Request (1)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x79dbf3a7     Transcation id should be same for Discover, Offer, Request and Ack (DORA)
    Seconds elapsed: 0
  ⊞ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: Vmware_84:39:6a (00:50:56:84:39:6a)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ⊞ Option: (t=53,l=1) DHCP Message Type = DHCP Discover     DHCP Discover sent by client
  ⊞ Option: (t=116,l=1) DHCP Auto-Configuration = AutoConfigure
  ⊞ Option: (t=61,l=7) Client identifier
  ⊞ Option: (t=12,l=14) Host Name = [redacted]
  ⊞ Option: (t=60,l=8) Vendor class identifier = "MSFT 5.0"
  ⊞ Option: (t=55,l=11) Parameter Request List
    End Option
    Padding
```

Nota: Si un cliente VPN solicita una dirección IP, la dirección IP del agente de retransmisión es la primera dirección IP utilizable definida por el comando dhcp-network-scope, bajo la política de grupo.

---

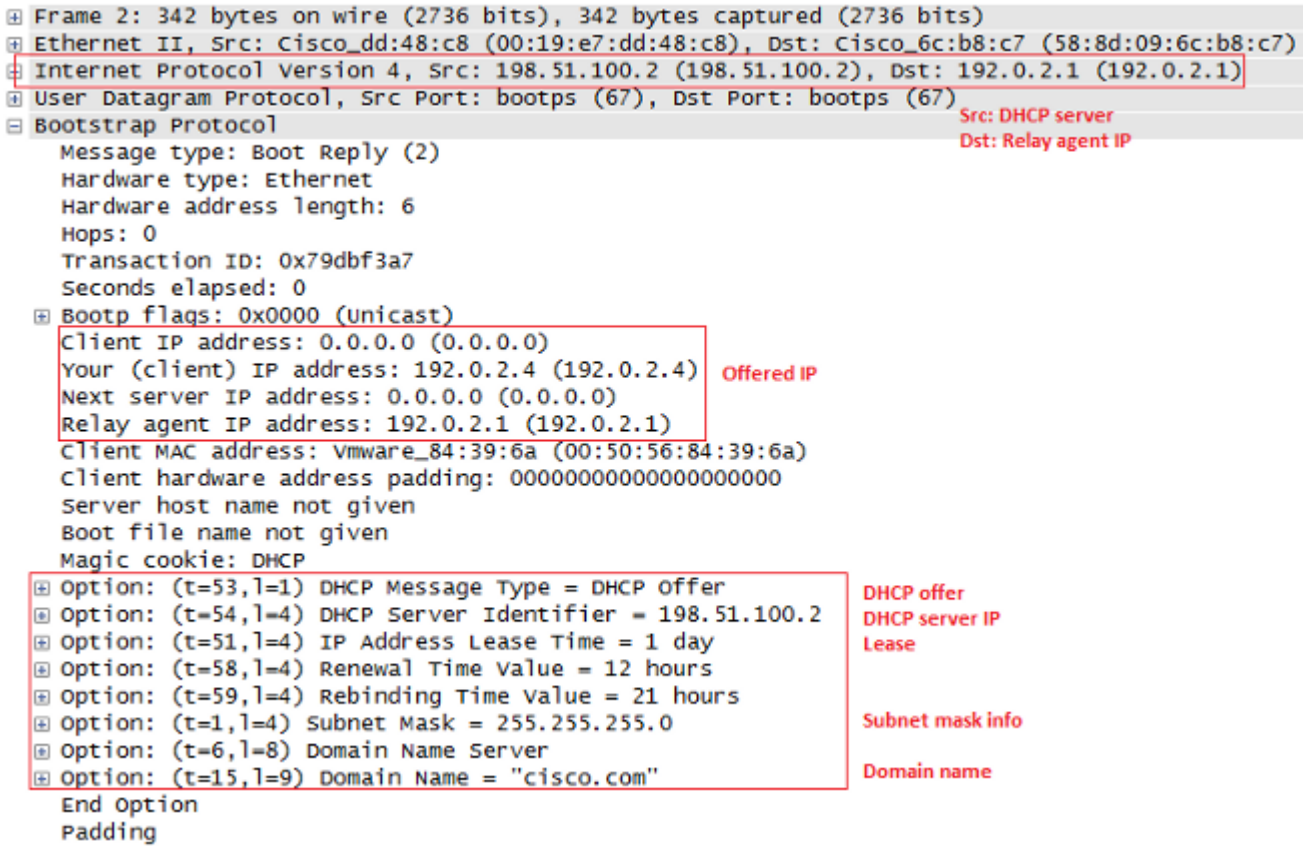
2. Normalmente, ASA descartaría la difusión, pero como está configurado para actuar como un relay DHCP, reenvía el mensaje DHCPDISCOVER como un paquete de unidifusión al IP de abastecimiento del servidor DHCP desde la IP de interfaz que se enfrenta al servidor. En este caso, es la dirección IP de la interfaz externa. Observe el cambio en el encabezado IP y el campo Relay Agent:



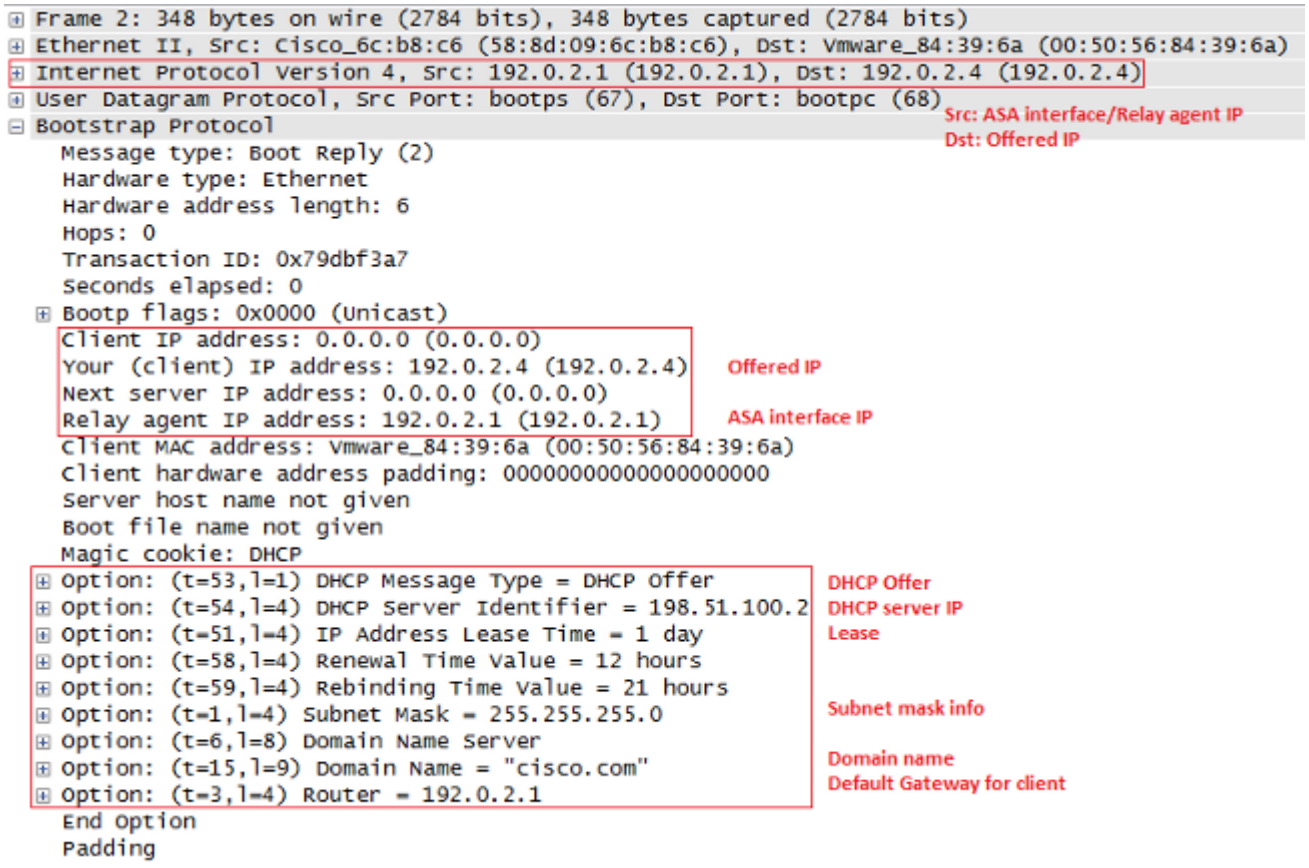
> **Nota**: debido a la corrección incorporada en el ID de bug Cisco CSCuo8924, ASA en las versiones 9.1(5.7), 9.3(1), y posteriores pueden reenviar los paquetes unicast al IP de abastecimiento del servidor DHCP desde la dirección IP de la interfaz que está frente al cliente (giaddr) donde está habilitado dhcprelay. En este caso, puede ser la dirección IP de la interfaz interna.

---

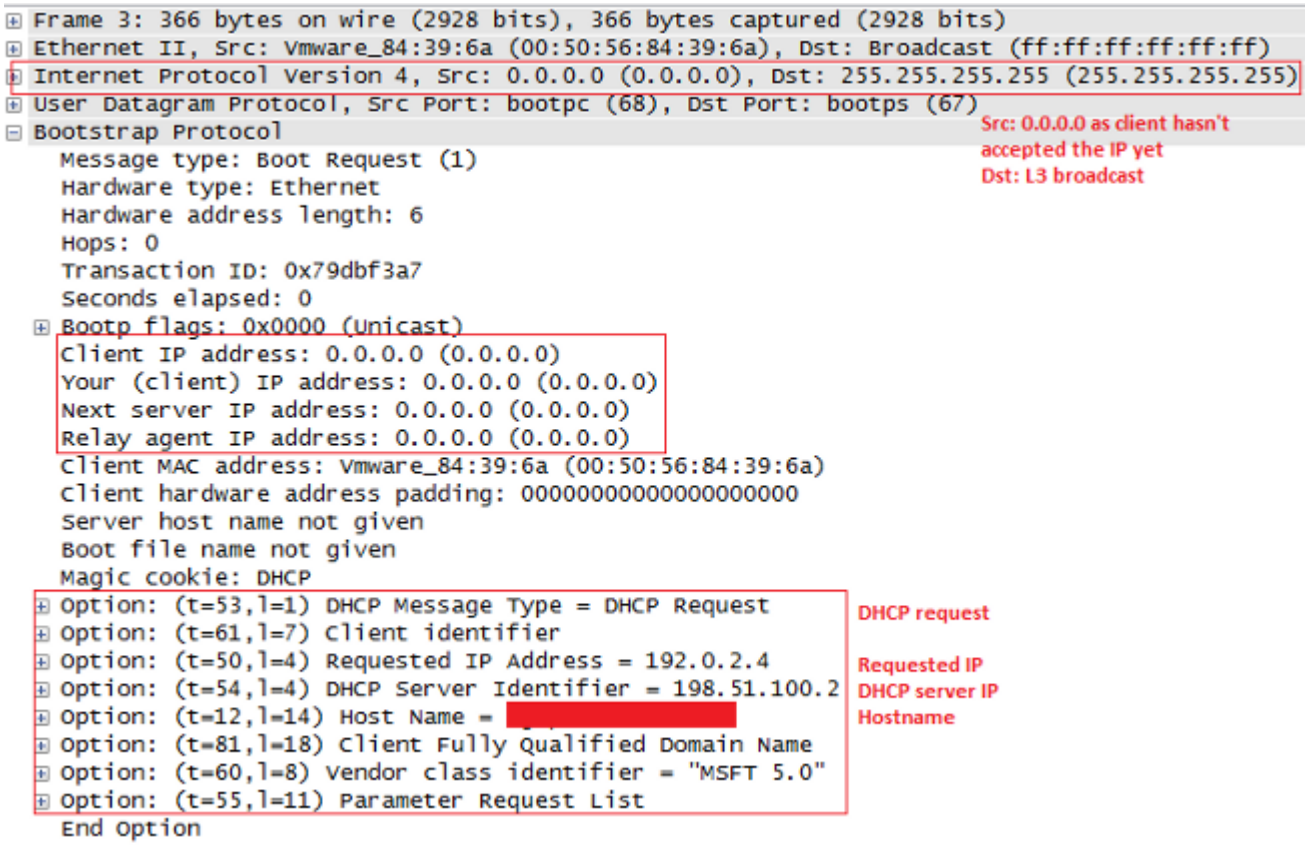
3. El servidor devuelve un mensaje DHCPOFFER como paquete de unidifusión al ASA, destinado a la IP del agente de retransmisión configurada en DHCPDISCOVER- puerto UDP 67. En este caso, es la dirección IP de la interfaz interior (giaddr), donde dhcprelay está habilitado. Observe la IP de destino en el encabezado de capa 3:



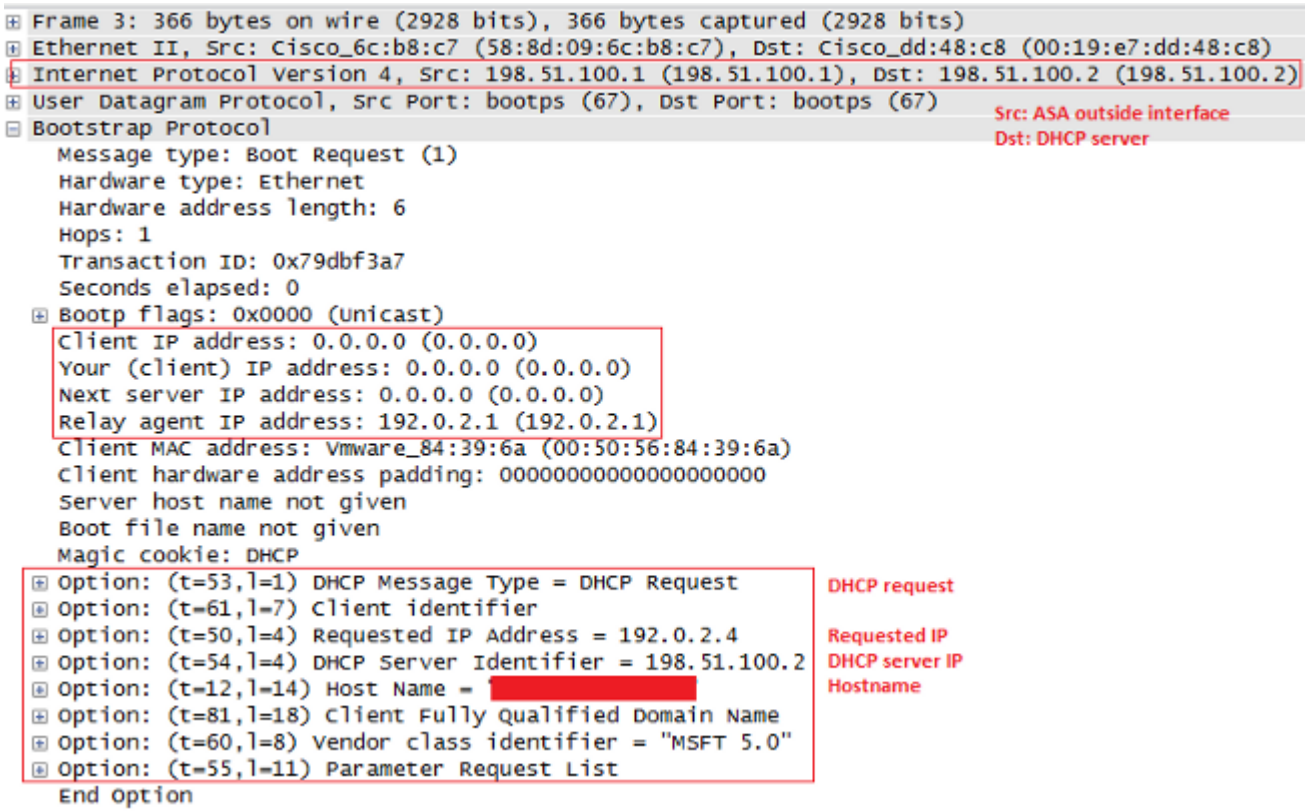
4. ASA envía este paquete fuera de la interfaz interna - puerto UDP 68. Observe el cambio en el encabezado IP mientras el paquete sale de la interfaz interna:



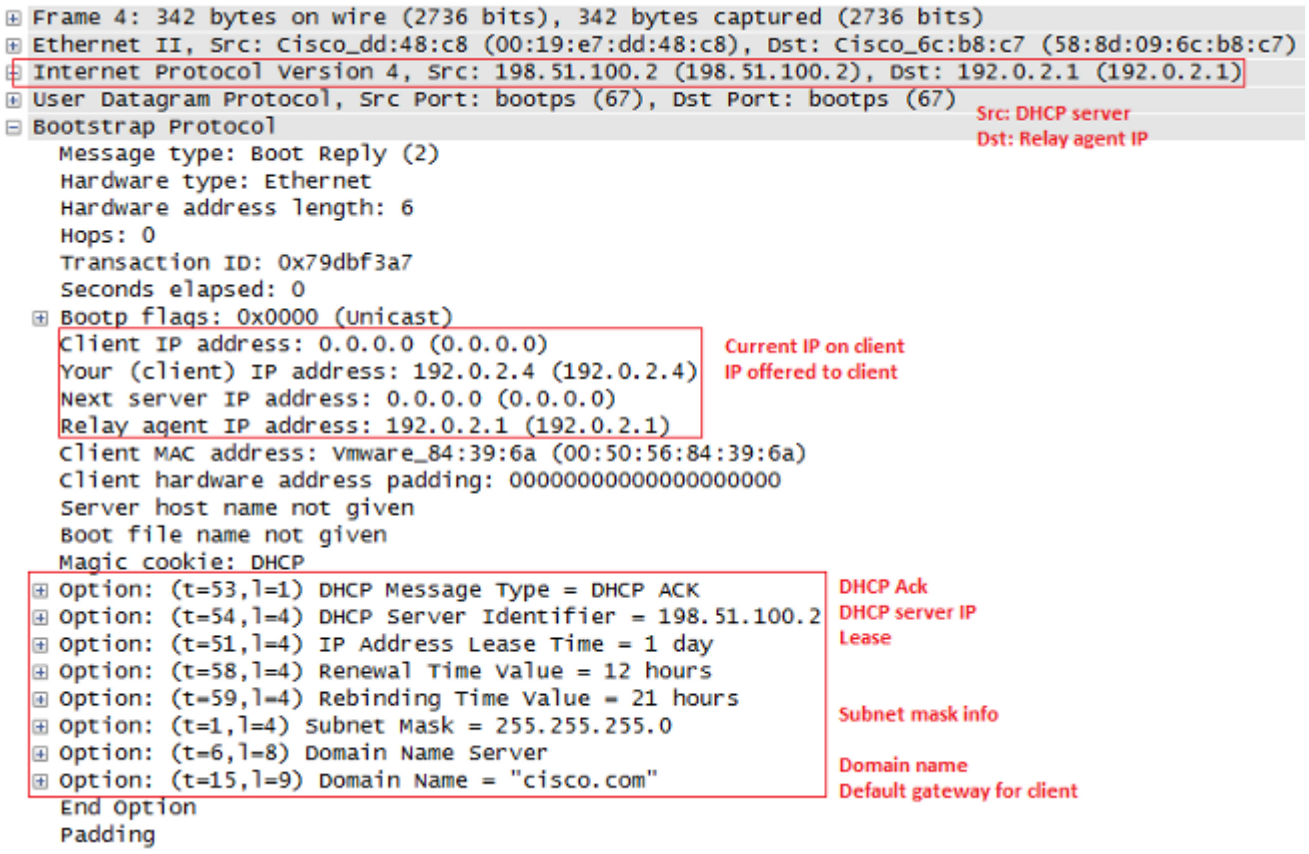
5. Una vez que reciba el mensaje DHCPOFFER, envíe un mensaje DHCPREQUEST para indicar que acepta la oferta.



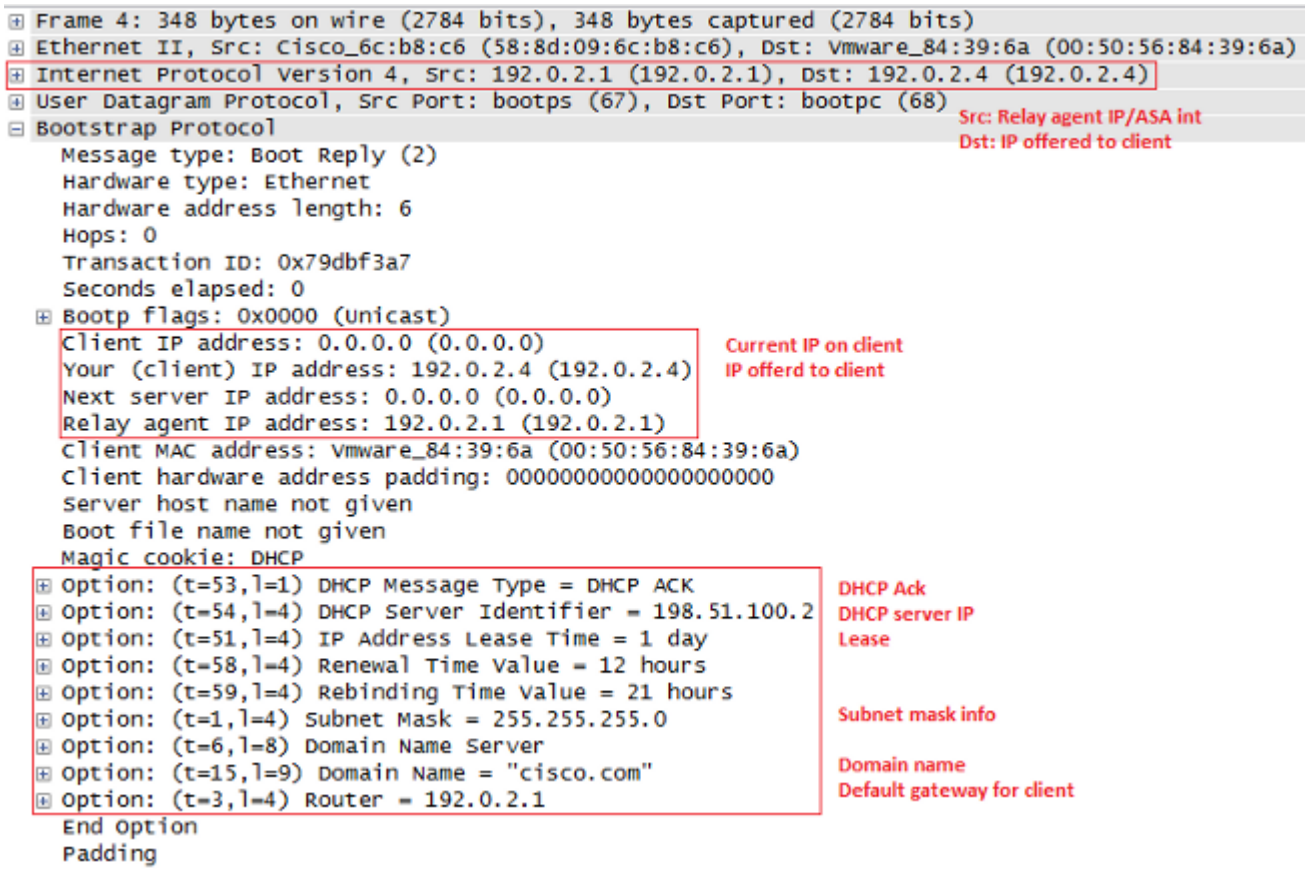
6. ASA pasa el DHCPREQUEST al servidor DHCP.



7. Una vez que el servidor obtiene el DHCPREQUEST, envía el DHCPACK de vuelta para confirmar la IP ofrecida.



8. ASA le pasa el DHCPACK del servidor DHCP y eso completa la transacción.



Depuraciones y registros del sistema para transacciones de retransmisión DHCP

Esta es una solicitud DHCP reenviada a la interfaz del servidor DHCP 198.51.100.2:

```
DHCPRA: relay binding created for client 0050.5684.396a.DHCPD:
 setting giaddr to 192.0.2.1.

dhcpd_forward_request: request from 0050.5684.396a forwarded to 198.51.100.2.
DHCPD/RA: Punt 198.51.100.2/17152 --> 192.0.2.1/17152 to CP
DHCPRA: Received a BOOTREPLY from interface 2
DHCPRA: relay binding found for client 0050.5684.396a.
DHCPRA: Adding rule to allow client to respond using offered address 192.0.2.4
```

Una vez recibida la respuesta del servidor DHCP, el dispositivo de seguridad la reenvía al cliente DHCP con la dirección MAC 0050.5684.396a y cambia la dirección del gateway a su propia interfaz interna.

```
DHCPRA: forwarding reply to client 0050.5684.396a.
DHCPRA: relay binding found for client 0050.5684.396a.
DHCPD: setting giaddr to 192.0.2.1.
dhcpd_forward_request: request from 0050.5684.396a forwarded to 198.51.100.2.
DHCPD/RA: Punt 198.51.100.2/17152 --> 192.0.2.1/17152 to CP
```

```
DHCPRA: Received a BOOTREPLY from interface 2
DHCPRA: relay binding found for client 0050.5684.396a.
DHCPRA: exchange complete - relay binding deleted for client 0050.5684.396a.
DHCPD: returned relay binding 192.0.2.1/0050.5684.396a to address pool.
dhcpd_destroy_binding() removing NP rule for client 192.0.2.1
DHCPRA: forwarding reply to client 0050.5684.396a.
```

La misma transacción aparece también en los syslogs:

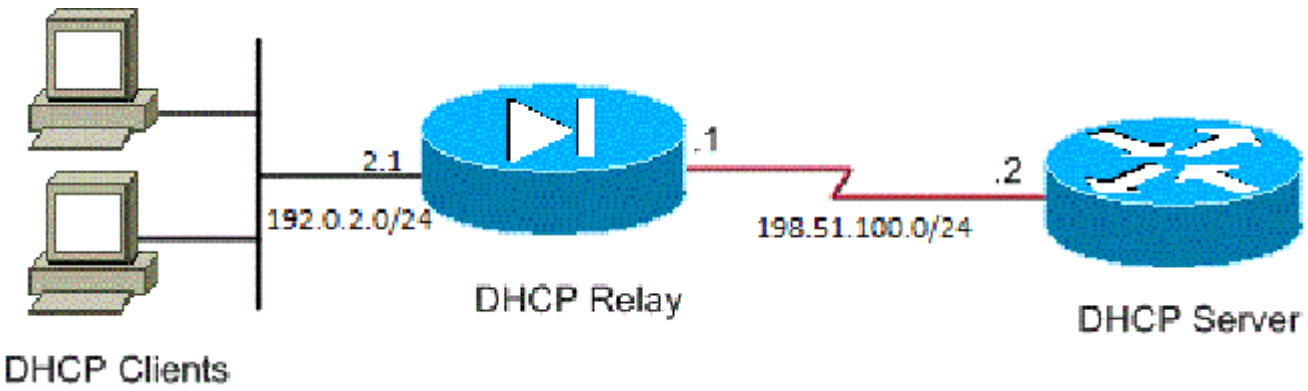
```
%ASA-7-609001: Built local-host inside:0.0.0.0
%ASA-7-609001: Built local-host identity:255.255.255.255
%ASA-6-302015: Built inbound UDP connection 13 for inside:
 0.0.0.0/68 (0.0.0.0/68) to identity:255.255.255.255/67 (255.255.255.255/67)
%ASA-7-609001: Built local-host identity:198.51.100.1
%ASA-7-609001: Built local-host outside:198.51.100.2
%ASA-6-302015: Built outbound UDP connection 14 for outside:
 198.51.100.2/67 (198.51.100.2/67) to identity:198.51.100.1/67 (198.51.100.1/67)

%ASA-7-609001: Built local-host inside:192.0.2.4
%ASA-6-302020: Built outbound ICMP connection for
 faddr 192.0.2.4/0 gaddr 198.51.100.2/1 laddr 198.51.100.2/1
%ASA-7-609001: Built local-host identity:192.0.2.1
%ASA-6-302015: Built inbound UDP connection 16 for outside:
 198.51.100.2/67 (198.51.100.2/67) to identity:192.0.2.1/67 (192.0.2.1/67)
%ASA-6-302015: Built outbound UDP connection 17 for inside:
 192.0.2.4/68 (192.0.2.4/68) to identity:192.0.2.1/67 (192.0.2.1/67)
%ASA-6-302021: Teardown ICMP connection for
 faddr 192.0.2.4/0 gaddr 198.51.100.2/1 laddr 198.51.100.2/1
```

Configurar

En esta sección, se presenta la información utilizada para configurar las funciones descritas en este documento.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Configuraciones

En este documento, se utilizan estas configuraciones:

- Configuración de retransmisión DHCP con el uso de la CLI
- Configuración final de retransmisión DHCP
- Configuración del Servidor DHCP

Configuración de retransmisión DHCP con el uso de la CLI

```
dhcprelay server 198.51.100.2 outside
dhcprelay enable inside
dhcprelay setroute inside
dhcprelay timeout 60
```

Configuración final de retransmisión DHCP

```
show run
!
hostname ASA
names
!
interface Ethernet0/0
 nameif inside
 security-level 0
 ip address 192.0.2.1 255.255.255.0
!
interface Ethernet0/1
 nameif outside
 security-level 100
 ip address 198.51.100.1 255.255.255.0
!
interface Ethernet0/2
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/3
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
ftp mode passive
no pager
logging enable
logging buffer-size 40960
logging buffered debugging
mtu inside 1500
mtu outside 1500
no failover
```

```
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
timeout xlate 0:30:00
timeout pat-xlate 0:00:30
timeout conn 3:00:00 half-closed 0:30:00 udp 0:15:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 0:30:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 0.0.0.0 0.0.0.0 inside
no snmp-server location
no snmp-server contact
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
telnet timeout 5
ssh timeout 5
console timeout 0

dhcprelay server 198.51.100.2 Outside
dhcprelay enable inside
dhcprelay setroute inside

//Defining DHCP server IP and interface//
//Enables DHCP relay on inside/client facing interface//
//Sets ASA inside as DG for clients in DHCP reply packets//

dhcprelay timeout 60
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
webvpn
!
!
prompt hostname context
no call-home reporting anonymous
call-home
 profile CiscoTAC-1
  no active
  destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
  destination address email callhome@cisco.com
  destination transport-method http
  subscribe-to-alert-group diagnostic
  subscribe-to-alert-group environment
  subscribe-to-alert-group inventory periodic monthly
  subscribe-to-alert-group configuration periodic monthly
  subscribe-to-alert-group telemetry periodic daily
Cryptochecksum:7ae5f655ffe399c8a88b61cb13425972
: end
```

Configuración del Servidor DHCP

```
show run
Building configuration...
```

```
Current configuration : 1911 bytes
!
! Last configuration change at 18:36:05 UTC Tue May 28 2013
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
logging buffered 4096
!
no aaa new-model
!
crypto pki token default removal timeout 0
!
!
dot11 syslog
ip source-route
!
ip dhcp excluded-address 192.0.2.1 192.0.2.2
ip dhcp excluded-address 192.0.2.10 192.0.2.254

//IP addresses exluded from DHCP scope//
!
ip dhcp pool pool1
 import all   network 192.0.2.0 255.255.255.0
   dns-server 192.0.2.10 192.0.2.11  domain-name cisco.com

//DHCP pool configuration and various parameters//
!
!
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
license udi pid CISCO1811W-AG-A/K9 sn FCTxxxx
!
!
!
interface Dot11Radio0
 no ip address
 shutdown
 speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
 station-role root
!
interface Dot11Radio1
 no ip address
 shutdown
 speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0
 station-role root
!
interface FastEthernet0
 ip address 198.51.100.2 255.255.255.0
```

```
 duplex auto
 speed auto
!
interface FastEthernet1
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet2
 no ip address
!
interface FastEthernet3
 no ip address
!
interface FastEthernet4
 no ip address
!
interface FastEthernet5
 no ip address
!
interface FastEthernet6
 no ip address
!
interface FastEthernet7
 no ip address
!
interface FastEthernet8
 no ip address
!
interface FastEthernet9
 no ip address
!
interface Vlan1
 no ip address
!
interface Async1
 no ip address
 encapsulation slip
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
ip route 192.0.2.0 255.255.255.0 198.51.100.1

//Static route to ensure replies are routed to relay agent IP//
!
!
!
control-plane
!
!
line con 0
line 1
 modem InOut
 stopbits 1
 speed 115200
 flowcontrol hardware
line aux 0
line vty 0 4
 login
```

```
 transport input all
!
end
```

Retransmisión DHCP con varios servidores DHCP

Puede definir hasta diez servidores DHCP. Cuando un cliente envía un paquete DHCP *Discover*, se reenvía a todos los servidores DHCP.

Aquí tiene un ejemplo:

```
dhcprelay server 198.51.100.2 outside
dhcprelay server 198.51.100.3 outside
dhcprelay server 198.51.100.4 outside
dhcprelay enable inside
dhcprelay setroute inside
```

Depuraciones con varios servidores DHCP

A continuación se muestran algunos ejemplos de depuración cuando se utilizan varios servidores DHCP:

```
DHCP: Received a BOOTREQUEST from interface 2 (size = 300)
DHCPRA: relay binding found for client 000c.291c.34b5.
DHCPRA: setting giaddr to 192.0.2.1.
dhcpd_forward_request: request from 000c.291c.34b5 forwarded to 198.51.100.2.
dhcpd_forward_request: request from 000c.291c.34b5 forwarded to 198.51.100.3.
dhcpd_forward_request: request from 000c.291c.34b5 forwarded to 198.51.100.4.
```

Capturas con varios servidores DHCP

A continuación se muestra un ejemplo de captura de paquetes cuando se utilizan varios servidores DHCP:

```
ASA# show cap out

3 packets captured

 1: 18:48:41.211628       192.0.2.1.67 > 198.51.100.2.67:  udp 300
 2: 18:48:41.211689       192.0.2.1.67 > 198.51.100.3.67:  udp 300
 3: 18:48:41.211704       192.0.2.1.67 > 198.51.100.4.67:  udp 300
```

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

Para ver la información estadística sobre los servicios de retransmisión DHCP, ingrese el comando **show dhcprelay statistics** en la CLI ASA:

```
ASA# show dhcprelay statistics

DHCP UDP Unreachable Errors: 1
DHCP Other UDP Errors: 0

Packets Relayed
BOOTREQUEST          0
DHCPDISCOVER         1
DHCPREQUEST          1
DHCPDECLINE          0
DHCPRELEASE          0
DHCPINFORM           0

BOOTREPLY            0
DHCPOFFER            1
DHCPACK              1
DHCPNAK              0
```

Este resultado proporciona información sobre varios tipos de mensajes DHCP, como DHCPDISCOVER, DHCP REQUEST, DHCP OFER, DHCP RELEASE y DHCP ACK.

- show dhcprelay state on ASA CLI
- show ip dhcp server statistics on router CLI

Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

```
Router#show ip dhcp server statistics

Memory usage         56637
Address pools        1
Database agents      0
Automatic bindings   1
Manual bindings      0
Expired bindings     0
Malformed messages   0
Secure arp entries   0

Message              Received
BOOTREQUEST          0
DHCPDISCOVER         1
DHCPREQUEST          1
DHCPDECLINE          0
DHCPRELEASE          0
DHCPINFORM           0

Message              Sent
BOOTREPLY            0
DHCPOFFER            1
```

```
DHCPACK             1
DHCPNAK             0

ASA# show dhcprelay state
Context  Configured as DHCP Relay
Interface inside, Configured for DHCP RELAY SERVER
Interface outside, Configured for DHCP RELAY
```

También puede utilizar estos comandos debug:

- **debug dhcprelay packet**
- **debug dhcprelay event**
- **Capturas**
- **Registros del sistema**

Nota: Consulte Información Importante sobre Comandos Debug antes de utilizar los comandos debug.

Información Relacionada

- **Capturas en ASA**
- **Soporte Técnico y Documentación - Cisco Systems**

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).