Configurar o relé DHCP do ASA (Adaptive Security Appliance)

Contents

Introdução

Este documento descreve a retransmissão DHCP no Cisco ASA com a ajuda de capturas e depurações de pacotes e fornece um exemplo de configuração.

Pré-requisitos

Um agente relay do protocolo DHCP permite que o Security Appliance encaminhe solicitações DHCP de clientes para um roteador ou outro servidor DHCP conectado a uma interface diferente.

Essas restrições aplicam-se somente ao uso do agente de retransmissão DHCP:

- O agente de retransmissão não poderá ser habilitado se o recurso de servidor DHCP também estiver habilitado.
- Você deve estar diretamente conectado ao Security Appliance e não pode enviar solicitações através de outro agente de retransmissão ou de um roteador.
- Para o modo de contexto múltiplo, você não pode ativar a retransmissão de DHCP ou configurar um servidor de retransmissão de DHCP em uma interface usada por mais de um contexto.

Os serviços de retransmissão DHCP não estão disponíveis no modo de firewall transparente. Um dispositivo de segurança no modo de firewall transparente permite somente o tráfego do Address Resolution Protocol (ARP). Todo o tráfego restante requer uma lista de controle de acesso (ACL). Para permitir solicitações e respostas DHCP através do Security Appliance no modo transparente, você deve configurar duas ACLs:

- Uma ACL que permite solicitações DHCP da interface interna para a externa.
- Uma ACL que permite as respostas do servidor na outra direção.

Requisitos

A Cisco recomenda que você tenha um conhecimento básico do ASA CLI e do Cisco IOS® CLI.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- ASA 5500-x Series Security Appliance versão 9.x ou posterior
- Cisco 1800 Series Routers

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

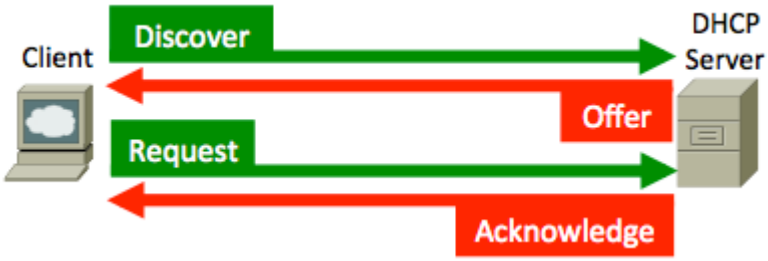
Informações de Apoio

O protocolo DHCP fornece parâmetros de configuração automáticos, como um endereço IP com uma máscara de sub-rede, gateway padrão, endereço do servidor DNS e endereço WINS (Windows Internet Name Service) para os hosts. Inicialmente, os clientes DHCP não têm nenhum desses parâmetros de configuração. Para obter essas informações, eles enviam uma solicitação de broadcast para elas. Quando um servidor DHCP vê essa solicitação, ele fornece as informações necessárias. Devido à natureza dessas solicitações de broadcast, o cliente e o servidor DHCP devem estar na mesma sub-rede. Os dispositivos da camada 3, como roteadores e firewalls, geralmente não encaminham essas solicitações de broadcast por padrão.

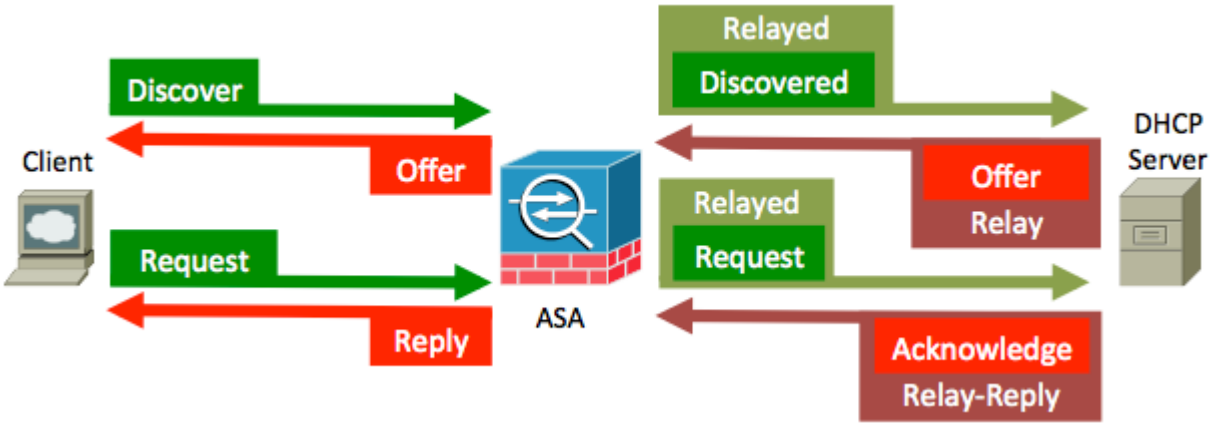
Nem sempre é conveniente tentar localizar clientes DHCP e um servidor DHCP na mesma sub-rede. Nessa situação, você pode usar o DHCP relay. Quando o agente de retransmissão de DHCP no Security Appliance recebe uma solicitação de DHCP de um host em uma interface interna, ele encaminha a solicitação a um dos servidores DHCP especificados em uma interface externa. Quando o servidor DHCP responde ao cliente, o Security Appliance encaminha essa resposta de volta. Assim, o agente de retransmissão DHCP atua como um proxy para o cliente DHCP em sua conversação com o servidor DHCP.

Fluxo de pacote

Esta imagem ilustra o fluxo de pacotes DHCP quando um agente de retransmissão DHCP não é usado:



O ASA intercepta esses pacotes e os encapsula no formato de retransmissão DHCP:



Retransmissão DHCP com capturas de pacotes na interface interna e externa do ASA

Anote o conteúdo destacado em VERMELHO, pois é assim que o ASA modifica vários campos.

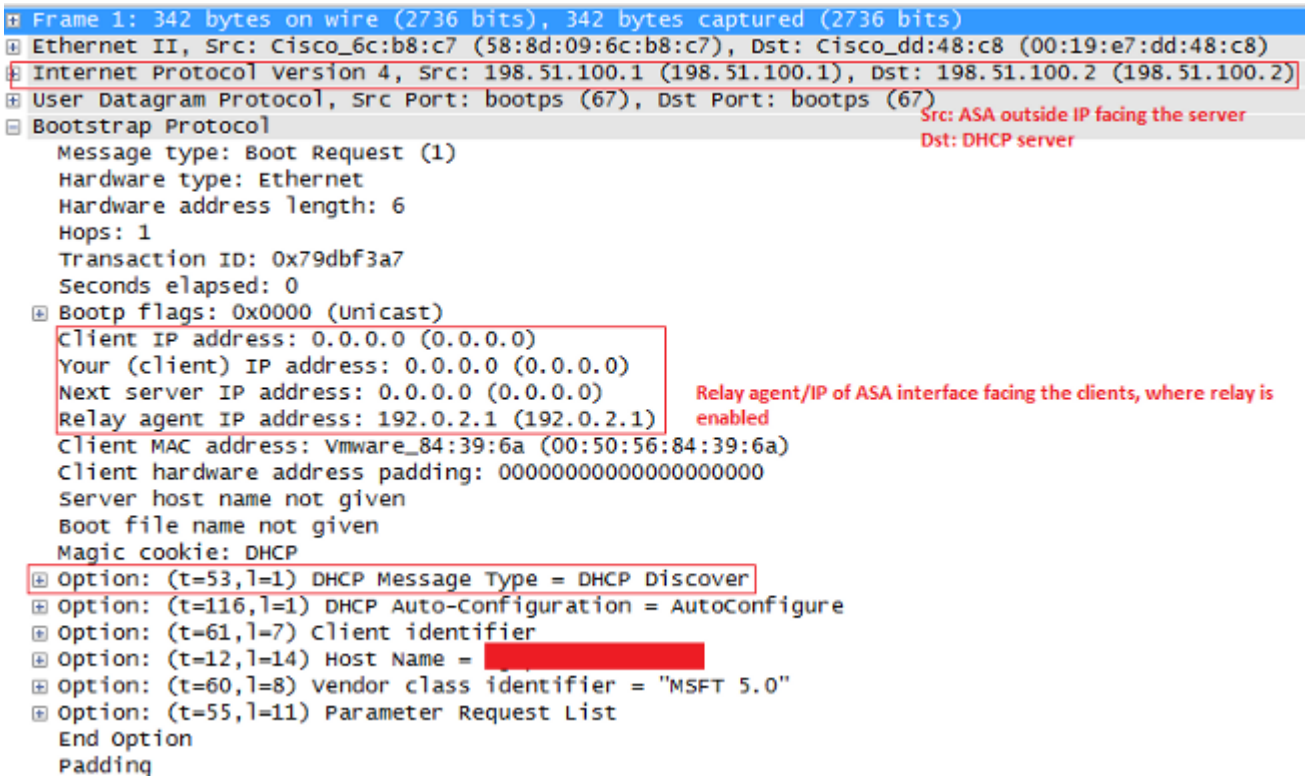
1. Para iniciar o processo DHCP, inicialize o sistema e envie uma mensagem de broadcast (DHCPDISCOVER) para o endereço destino 255.255.255.255 - porta UDP 67.

```
⊞ 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
```

Observação: se um cliente VPN solicita um endereço IP, o endereço IP do agente de retransmissão é o primeiro endereço IP utilizável definido pelo comando dhcp-network-scope, sob a política de grupo.

---

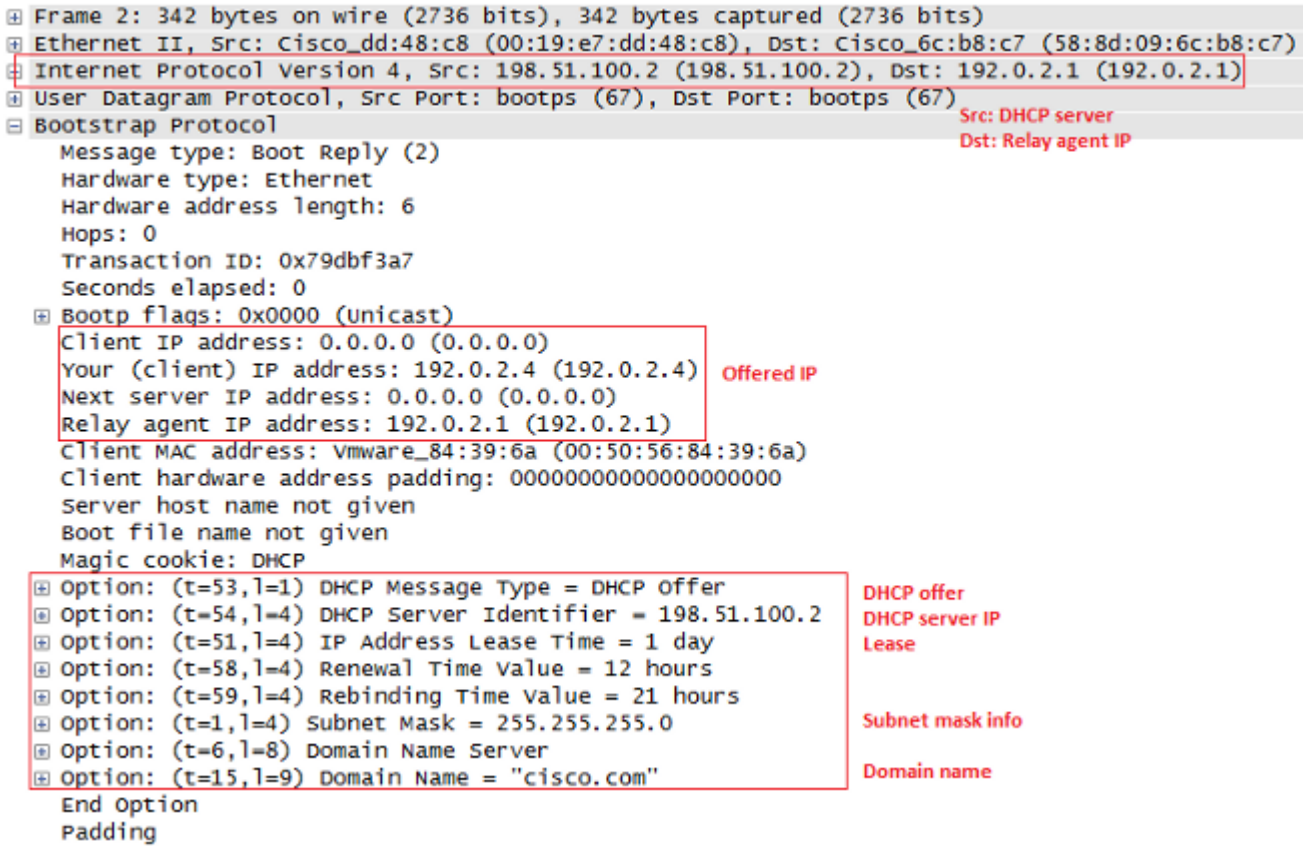
2. Normalmente, o ASA descartaria o broadcast, mas como está configurado para atuar como um relé DHCP, ele encaminha a mensagem DHCPDISCOVER como um pacote unicast para a origem IP do servidor DHCP a partir do IP da interface que encara o servidor. Nesse caso, é o endereço IP da interface externa. Observe a alteração no cabeçalho IP e no campo do agente de retransmissão:



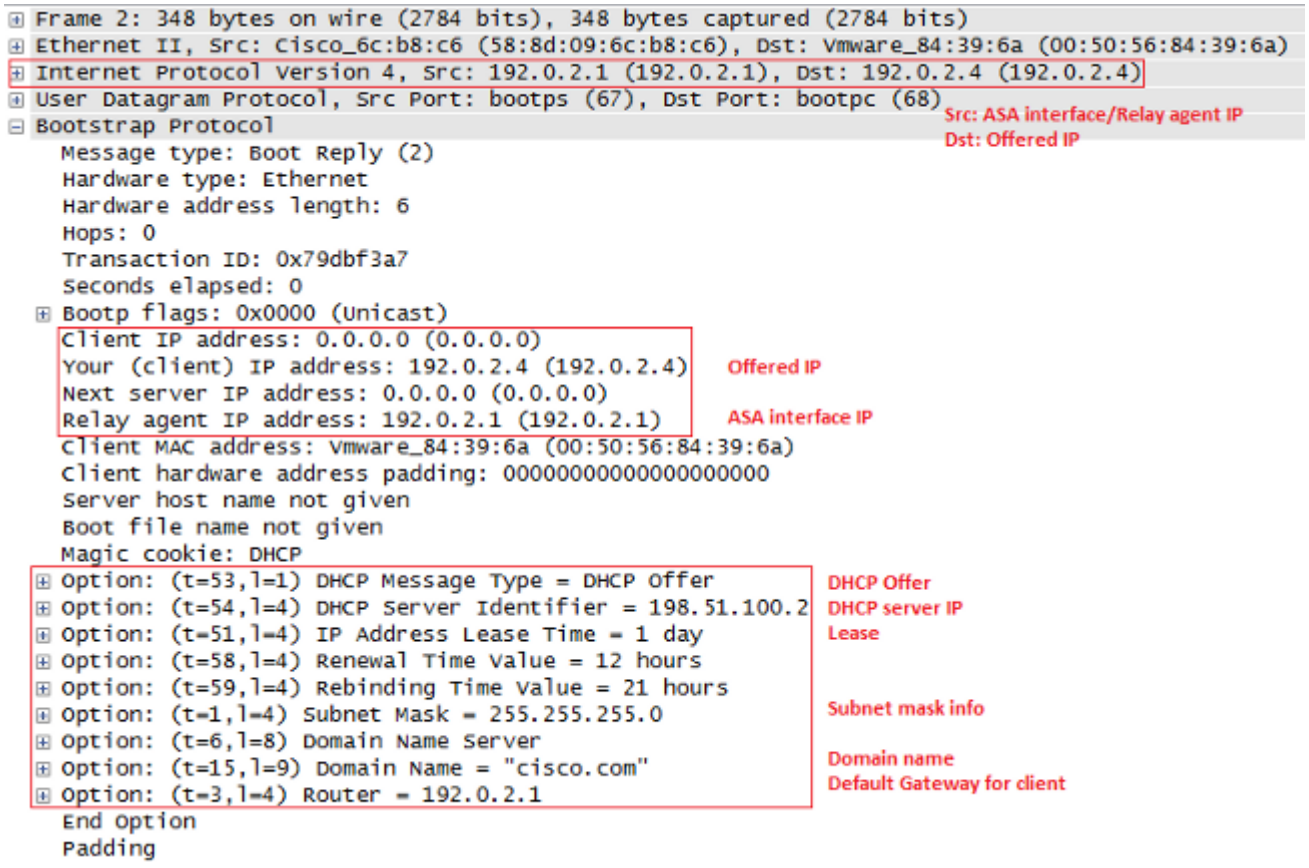
Observação: devido à correção incorporada no bug da Cisco ID CSCuo8924, o ASA nas versões 9.1(5.7), 9.3(1) e posteriores pode encaminhar os pacotes unicast para a origem IP do servidor DHCP a partir do endereço IP da interface que está voltado para o cliente (giaddr) onde o dhcprelay está habilitado. Nesse caso, pode ser o endereço IP da interface interna.

---

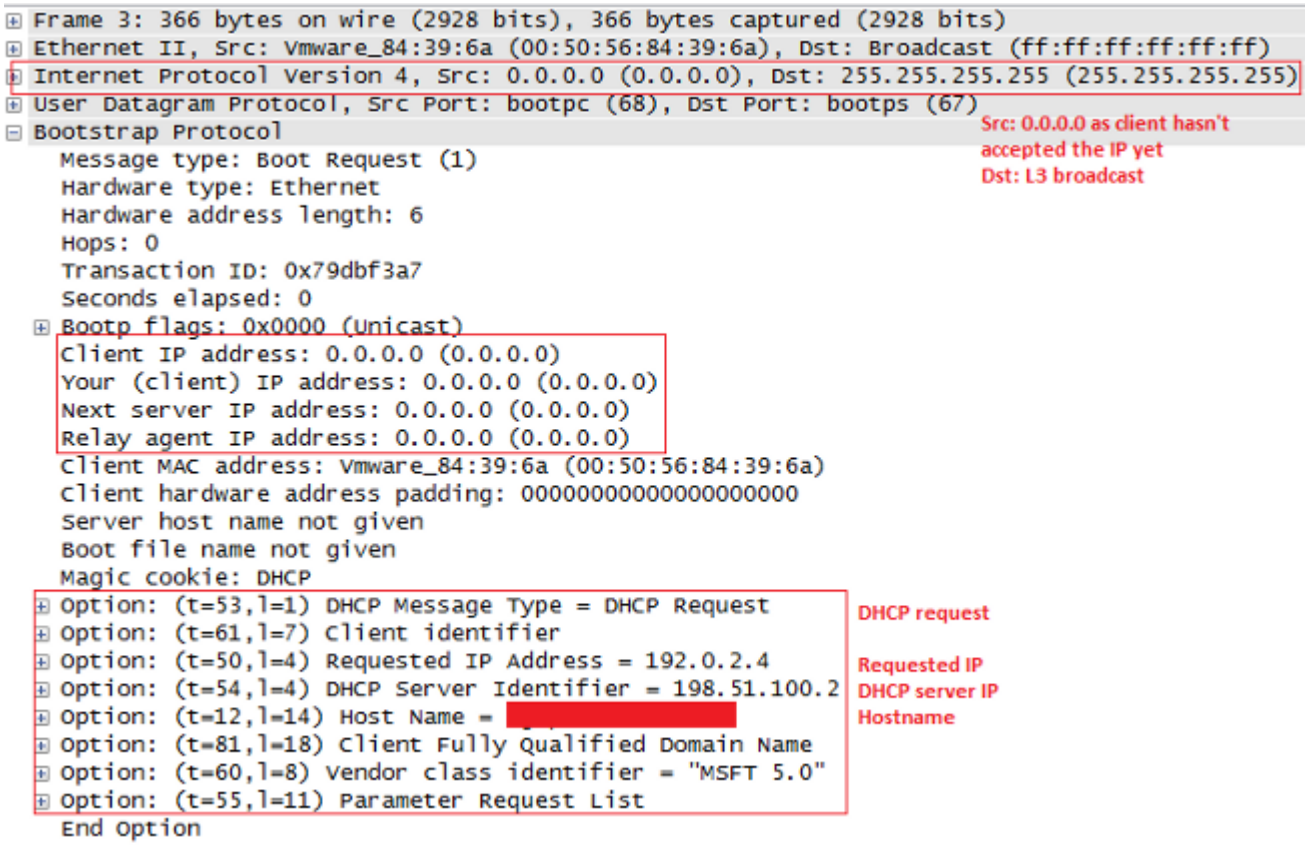
3. O servidor retorna uma mensagem DHCPOFFER como um pacote unicast para o ASA, destinado ao IP do agente de retransmissão configurado na porta 67 DHCPDISCOVER- UDP. Nesse caso, é o endereço IP da interface interna (giaddr), onde dhcprelay está habilitado. Observe o IP de destino no cabeçalho da camada 3:



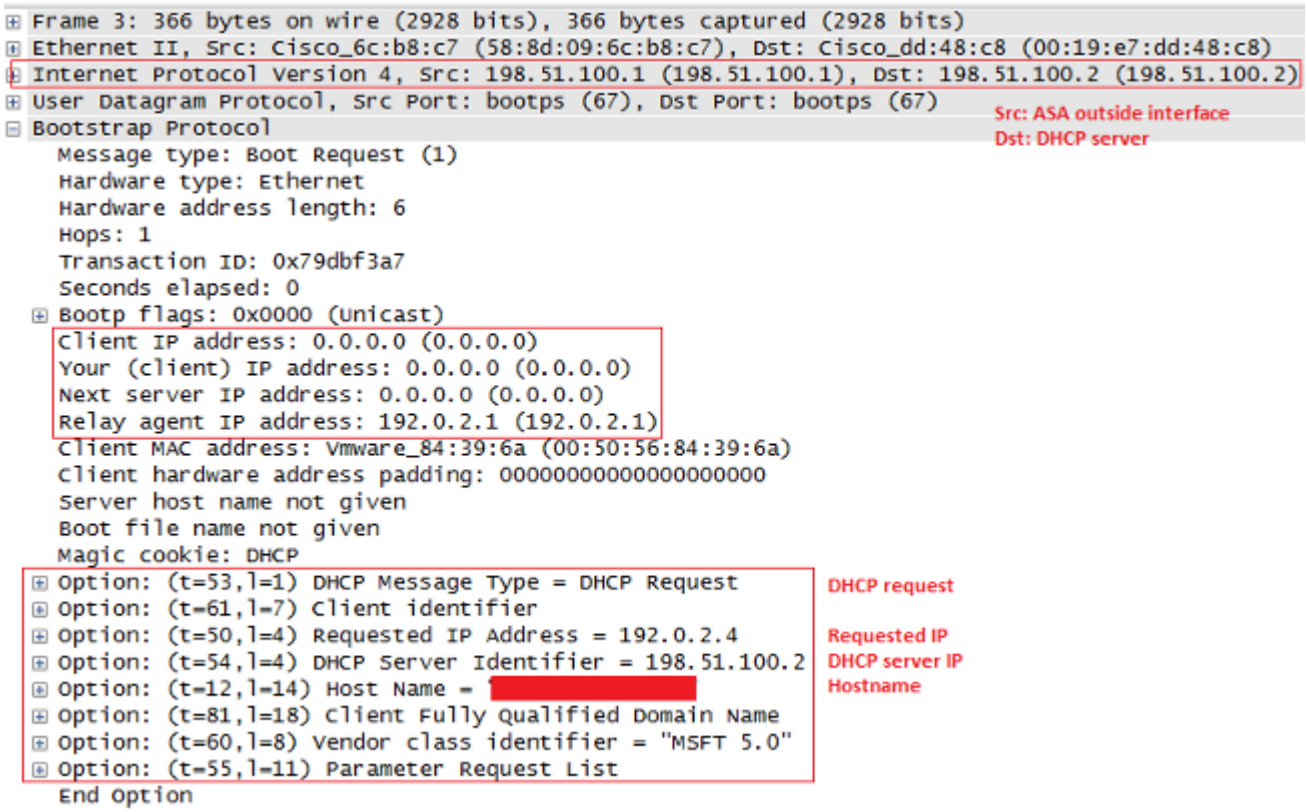
4. O ASA envia esse pacote para fora da interface interna - porta UDP 68. Observe a alteração no cabeçalho IP enquanto o pacote sai da interface interna:



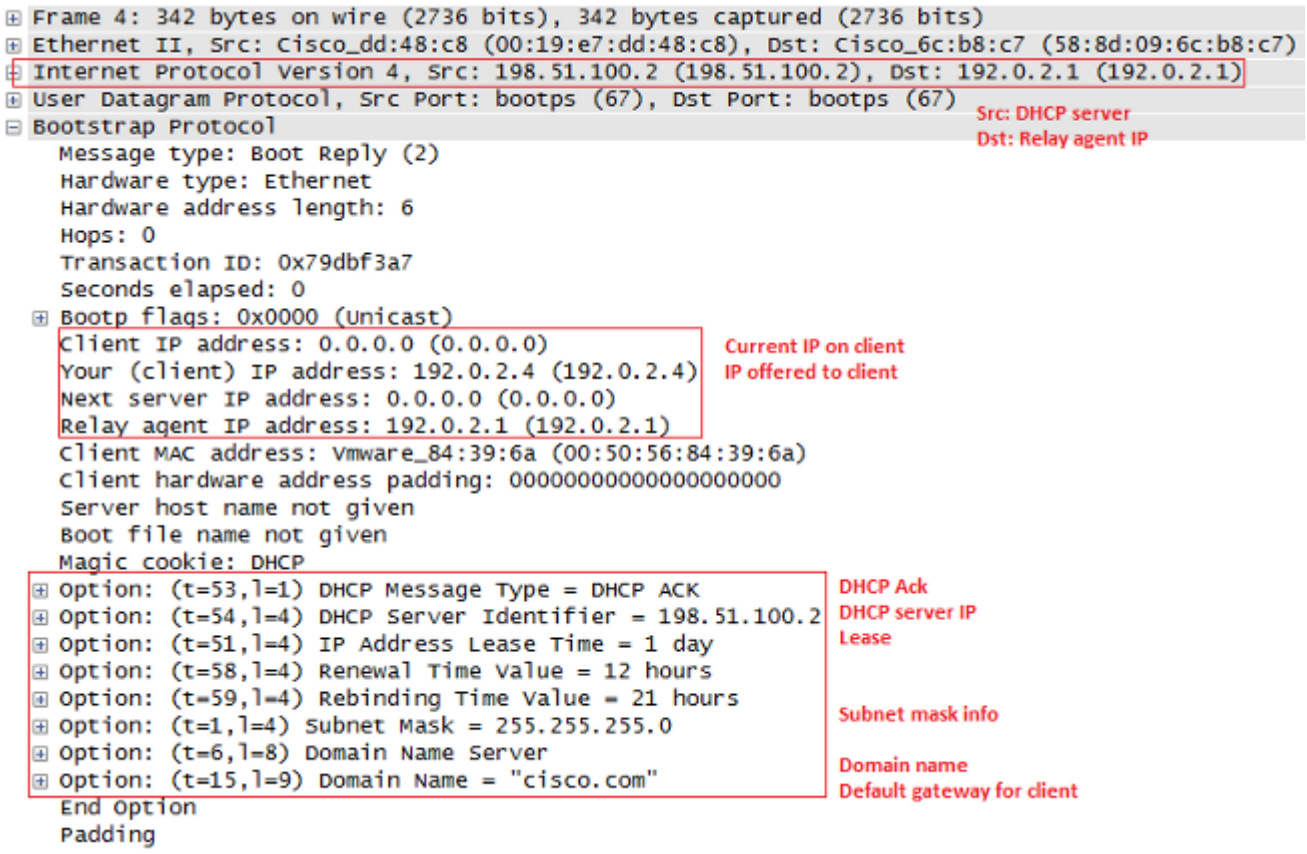
5. Depois de receber a mensagem DHCPOFFER, envie uma mensagem DHCPREQUEST para indicar que você aceitou a oferta.



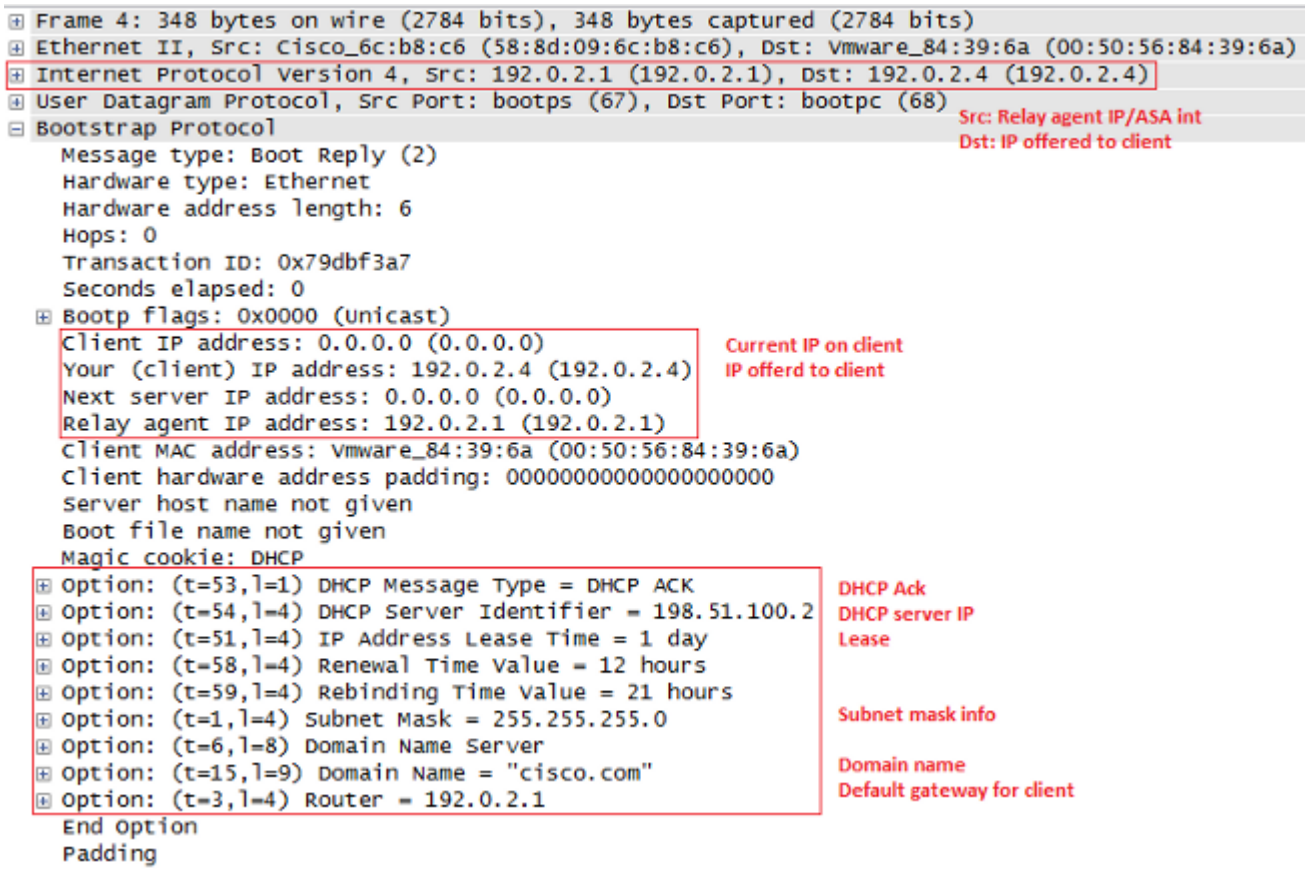
6. O ASA passa o DHCPREQUEST para o servidor DHCP.



7. Quando o servidor obtém o DHCPREQUEST, ele envia o DHCPACK de volta para confirmar o IP oferecido.



8. O ASA passa o DHCPACK do servidor DHCP para você, e isso conclui a transação.



Depurações e Syslogs para Transações de Retransmissão DHCP

Esta é uma solicitação DHCP encaminhada à interface do 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
```

Depois que a resposta é recebida do servidor DHCP, o Security Appliance a encaminha para o cliente DHCP com o endereço MAC 0050.5684.396a e altera o endereço do gateway para sua própria interface 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.
```

A mesma transação também aparece nos syslogs:

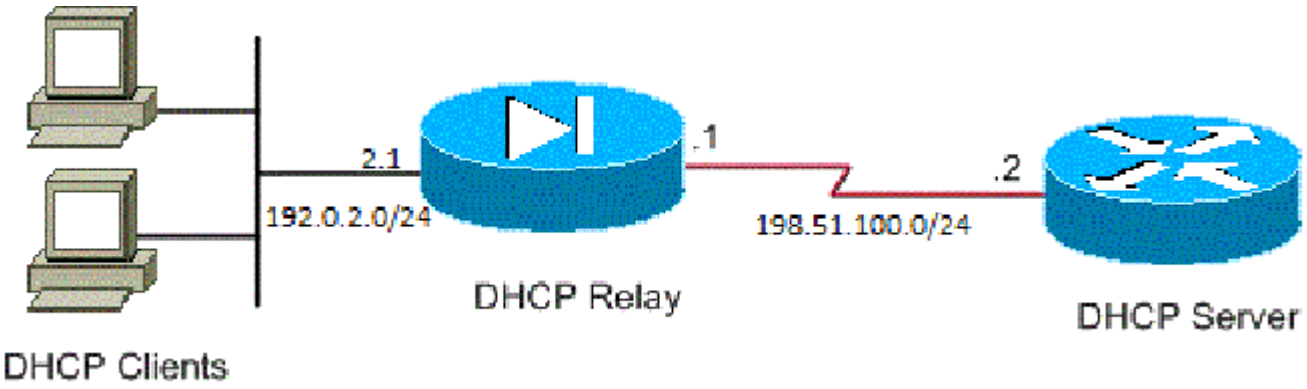
```
%ASA-7-609001: Built local-host inside:0.0.0.0
%ASA-7-609001: Built local-host identity:255.255.255.255
%ASA-6-302015: Built inbound UDP connection 13 for inside:
 0.0.0.0/68 (0.0.0.0/68) to identity:255.255.255.255/67 (255.255.255.255/67)
%ASA-7-609001: Built local-host identity:198.51.100.1
%ASA-7-609001: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

Nesta seção, você verá as informações usadas para configurar os recursos descritos neste documento.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Configurações

Este documento utiliza as seguintes configurações:

- Configuração de Relé DHCP com Uso da CLI
- Configuração final do relé DHCP
- Configuração do servidor DHCP

Configuração de Relé DHCP com Uso da CLI

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

Configuração final do relé 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
```

Configuração do 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
```

Retransmissão DHCP com vários servidores DHCP

Você pode definir até dez servidores DHCP. Quando um cliente envia um pacote DHCP *Discover*, ele é encaminhado a todos os servidores DHCP.

Aqui está um exemplo:

```
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
```

Depurações com vários servidores DHCP

Aqui estão alguns exemplos de depurações quando vários servidores DHCP são usados:

```
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 com Vários Servidores DHCP

Aqui está um exemplo de captura de pacotes quando vários servidores DHCP são usados:

```
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
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Para visualizar as informações estatísticas sobre os serviços de retransmissão de DHCP, insira o comando **show dhcprelay statistics** na CLI do 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
```

Esta saída fornece informações sobre vários tipos de mensagem DHCP, como DHCPDISCOVER, DHCP REQUEST, DHCP OFER, DHCP RELEASE e DHCP ACK.

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

Troubleshooting

Esta seção disponibiliza informações para a solução de problemas de configuração.

```
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
```

Você também pode usar estes comandos de depuração:

- **debug dhcprelay packet**
- **debug dhcprelay event**
- **Capturas**
- **Syslogs**

Nota:Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos debug.

Informações Relacionadas

- **Capturas no ASA**
- **Suporte Técnico e Documentação - Cisco Systems**

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.