DHCP-relay configureren van adaptieve security applicatie (ASA)

Inhoud

Inleiding

Dit document beschrijft DHCP-relay op Cisco ASA met behulp van pakketopnamen en -debugs en biedt een configuratievoorbeeld.

Voorwaarden

Een Dynamic Host Configuration Protocol (DHCP) relay Agent stelt het security apparaat in staat DHCP-verzoeken van clients door te sturen naar een router of andere DHCP-server die is aangesloten op een andere interface.

Deze beperkingen zijn alleen van toepassing op het gebruik van de DHCP Relay Agent:

- De relay agent kan niet worden ingeschakeld als de DHCP-serverfunctie ook is ingeschakeld.
- U moet rechtstreeks worden aangesloten op het security apparaat en kunt geen verzoeken verzenden via een andere relay-agent of een router.
- Voor meerdere contextmodi kunt u DHCP Relay niet inschakelen of een DHCP Relay-server configureren op een interface die door meer dan één context wordt gebruikt.

DHCP-relay services zijn niet beschikbaar in transparante firewallmodus. Een security applicatie in transparante firewallmodus staat alleen verkeer via Address Resolution Protocol (ARP) toe. Al het andere verkeer vereist een toegangscontrolelijst (ACL). U moet twee ACLâ€™s configureren om DHCP-verzoeken en -antwoorden via het security applicatie in transparante modus toe te staan:

- Eén ACL die DHCP-verzoeken van de binnenkant van de interface naar buiten toestaat.
- Eén ACL die de antwoorden van de server in de andere richting toestaat.

Vereisten

Cisco raadt u aan een basiskennis te hebben van ASA CLI en Cisco IOS® CLI.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- ASA 5500-x Series security applicatie release 9.x of hoger
- Cisco 1800 Series routers

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

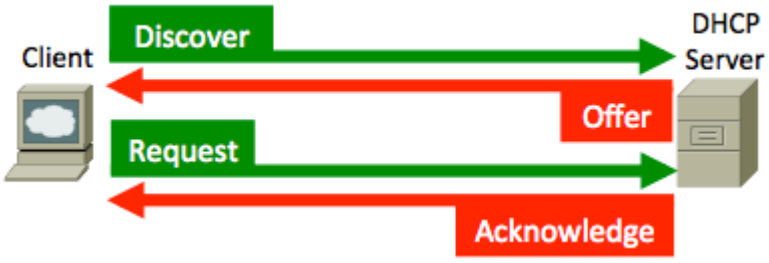
Achtergrondinformatie

Het DHCP-protocol levert automatische configuratieparameters, zoals een IP-adres met een subnetmasker, standaardgateway, DNS-serveradres en Windows Internet Name Service (WINS)-adres aan hosts. Aanvankelijk hebben DHCP-clients geen van deze configuratieparameters. Om deze informatie te verkrijgen, sturen zij een uitzendverzoek om deze informatie. Wanneer een DHCP-server dit verzoek ziet, levert de DHCP-server de benodigde informatie. Wegens de aard van deze uitzendingsverzoeken, moeten de cliënt en de server van DHCP op zelfde Subnet zijn. Layer 3-apparaten zoals routers en firewalls sturen deze uitzendverzoeken doorgaans niet standaard door.

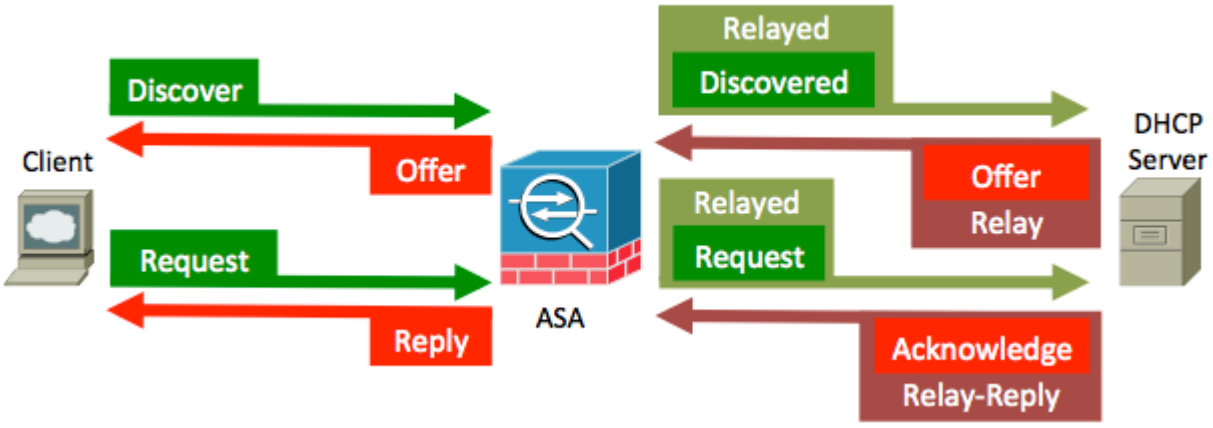
Een poging om DHCP-clients en een DHCP-server te vinden in hetzelfde subnetje is niet altijd handig. In zo een situatie, kunt u DHCP relay gebruiken. Wanneer de DHCP Relay Agent op het security apparaat een DHCP-verzoek van een host ontvangt op een interne interface, stuurt het het verzoek door naar een van de gespecificeerde DHCP-servers op een externe interface. Wanneer de DHCP-server op de client reageert, stuurt het security apparaat dat antwoord terug. Aldus, handelt de DHCP relay agent als volmacht voor de DHCP client in zijn gesprek met de DHCP server.

Pakketstroom

Dit beeld illustreert de DHCP-pakketstroom wanneer een DHCP-relay-agent niet wordt gebruikt:



ASA onderschept deze pakketten en verpakt ze in DHCP-relay-indeling:



DHCP Relay met Packet Captures op de ASA Inside en Outside Interface

Maak een notitie van de inhoud die in rood wordt gemarkeerd, omdat dat is hoe de ASA verschillende velden wijzigt.

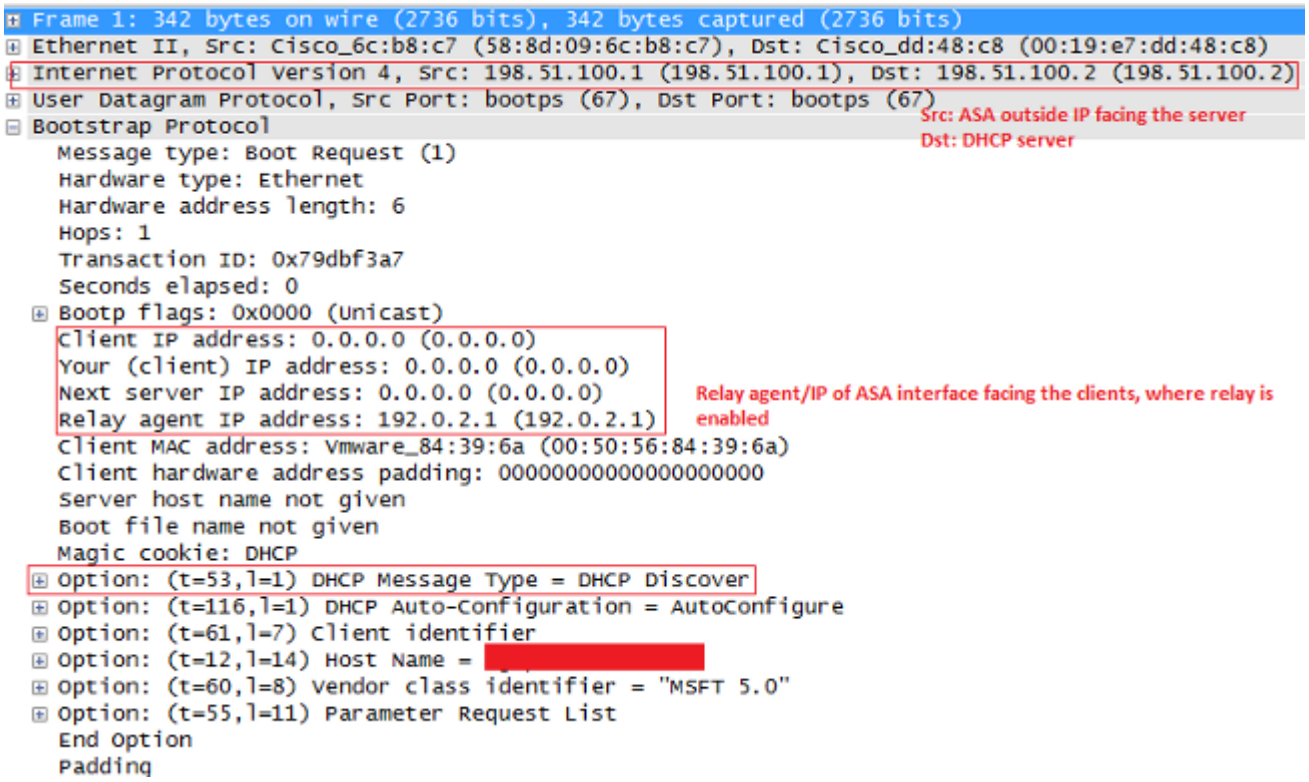
1. Om het DHCP-proces te starten, start u het systeem op en verstuur een uitzendingsbericht (DHCPDiscover) naar het doeladres 255.255.255.255 - UDP-poort 67.

```
⊞ 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
```

Opmerking: Als een VPN-client een IP-adres opvraagt, is het IP-adres van de relay-agent het eerste bruikbare IP-adres dat wordt gedefinieerd door de opdracht DHCP-netwerk-scope onder het groepsbeleid.

---

2. Normaal gesproken zou ASA de uitzending laten vallen, maar omdat deze is geconfigureerd om als DHCP-relay te fungeren, wordt het DHCPDiscover-bericht doorgestuurd als unicastpakket naar de IP-bronning van de DHCP-server vanuit de interface-IP die naar de server kijkt. In dit geval, is het het buiteninterfaceIP adres. Let op de wijziging in het veld IP-header en relay-agent:



Opmerking: vanwege de oplossing die is opgenomen in Cisco bug-id CSCuo8924, ASA in versies 9.1(5.7) en 9.3(1), en kan later de unicast-pakketten doorsturen naar de IP-bron van de DHCP-server vanuit het interface-IP-adres dat naar de client (addr) kijkt waar de dhcprelay is ingeschakeld. In dit geval, kan het het binnen interfaceIP adres zijn.

---

3. De server stuurt een DHCPOFFER-bericht als unicastpakket terug naar de ASA, bestemd voor de relay agent IP die is ingesteld in DHCPDiscover- UDP-poort 67. In dit geval is het het IP-adres van de interface (giaddr), waar Dhcprelay is ingeschakeld. Merk de bestemming IP in laag 3 kopbal op:

```
⊞ Frame 2: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
⊞ Ethernet II, Src: Cisco_dd:48:c8 (00:19:e7:dd:48:c8), Dst: Cisco_6c:b8:c7 (58:8d:09:6c:b8:c7)
⊞ Internet Protocol Version 4, Src: 198.51.100.2 (198.51.100.2), Dst: 192.0.2.1 (192.0.2.1)
⊞ User Datagram Protocol, Src Port: bootps (67), Dst Port: bootps (67)
⊟ Bootstrap Protocol
    Message type: Boot Reply (2)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x79dbf3a7
    Seconds elapsed: 0
  ⊞ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 192.0.2.4 (192.0.2.4)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 192.0.2.1 (192.0.2.1)
    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 Offer
  ⊞ Option: (t=54,l=4) DHCP Server Identifier = 198.51.100.2
  ⊞ Option: (t=51,l=4) IP Address Lease Time = 1 day
  ⊞ Option: (t=58,l=4) Renewal Time Value = 12 hours
  ⊞ Option: (t=59,l=4) Rebinding Time Value = 21 hours
  ⊞ Option: (t=1,l=4) Subnet Mask = 255.255.255.0
  ⊞ Option: (t=6,l=8) Domain Name Server
  ⊞ Option: (t=15,l=9) Domain Name = "cisco.com"
    End Option
    Padding
```

Src: DHCP server
Dst: Relay agent IP

Offered IP

DHCP offer
DHCP server IP
Lease

Subnet mask info

Domain name

4. ASA verstuurt dit pakket vanuit de interface - UDP-poort 68. Merk de verandering in de IP kopbal op terwijl het pakket de binneninterface verlaat:

```
⊞ Frame 2: 348 bytes on wire (2784 bits), 348 bytes captured (2784 bits)
⊞ Ethernet II, Src: Cisco_6c:b8:c6 (58:8d:09:6c:b8:c6), Dst: Vmware_84:39:6a (00:50:56:84:39:6a)
⊞ Internet Protocol Version 4, Src: 192.0.2.1 (192.0.2.1), Dst: 192.0.2.4 (192.0.2.4)
⊞ User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
⊟ Bootstrap Protocol
    Message type: Boot Reply (2)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x79dbf3a7
    Seconds elapsed: 0
  ⊞ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 192.0.2.4 (192.0.2.4)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 192.0.2.1 (192.0.2.1)
    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 Offer
  ⊞ Option: (t=54,l=4) DHCP Server Identifier = 198.51.100.2
  ⊞ Option: (t=51,l=4) IP Address Lease Time = 1 day
  ⊞ Option: (t=58,l=4) Renewal Time Value = 12 hours
  ⊞ Option: (t=59,l=4) Rebinding Time Value = 21 hours
  ⊞ Option: (t=1,l=4) Subnet Mask = 255.255.255.0
  ⊞ Option: (t=6,l=8) Domain Name Server
  ⊞ Option: (t=15,l=9) Domain Name = "cisco.com"
  ⊞ Option: (t=3,l=4) Router = 192.0.2.1
    End Option
    Padding
```

Src: ASA interface/Relay agent IP
Dst: Offered IP

Offered IP

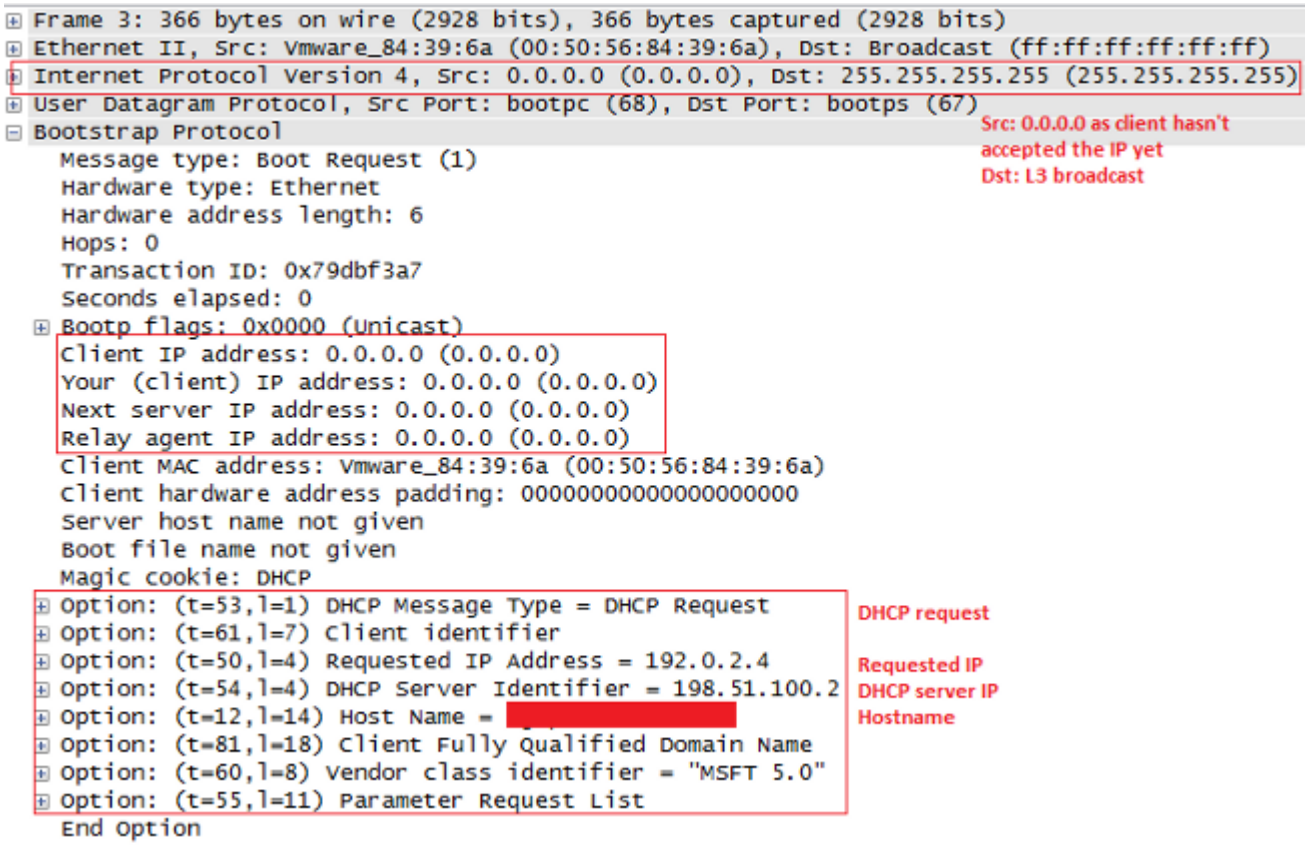
ASA interface IP

DHCP Offer
DHCP server IP
Lease

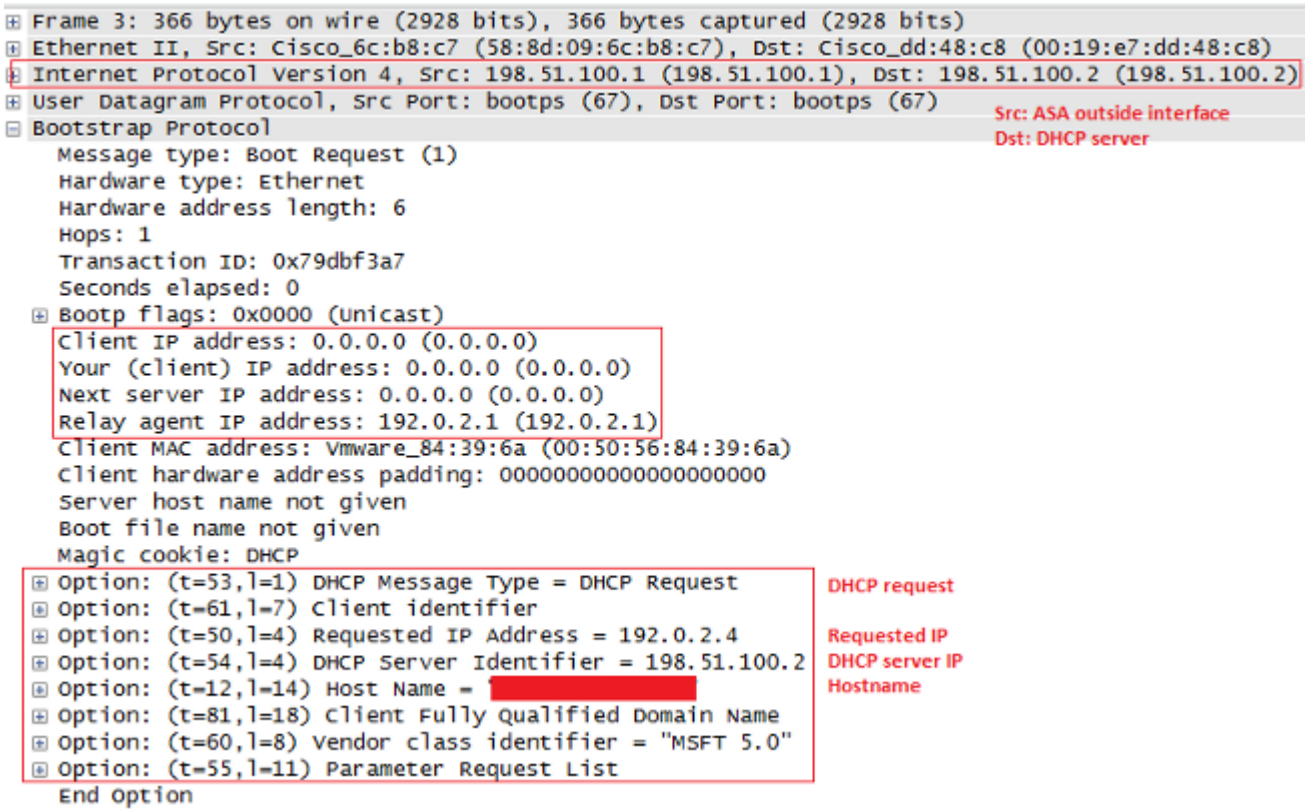
Subnet mask info

Domain name
Default Gateway for client

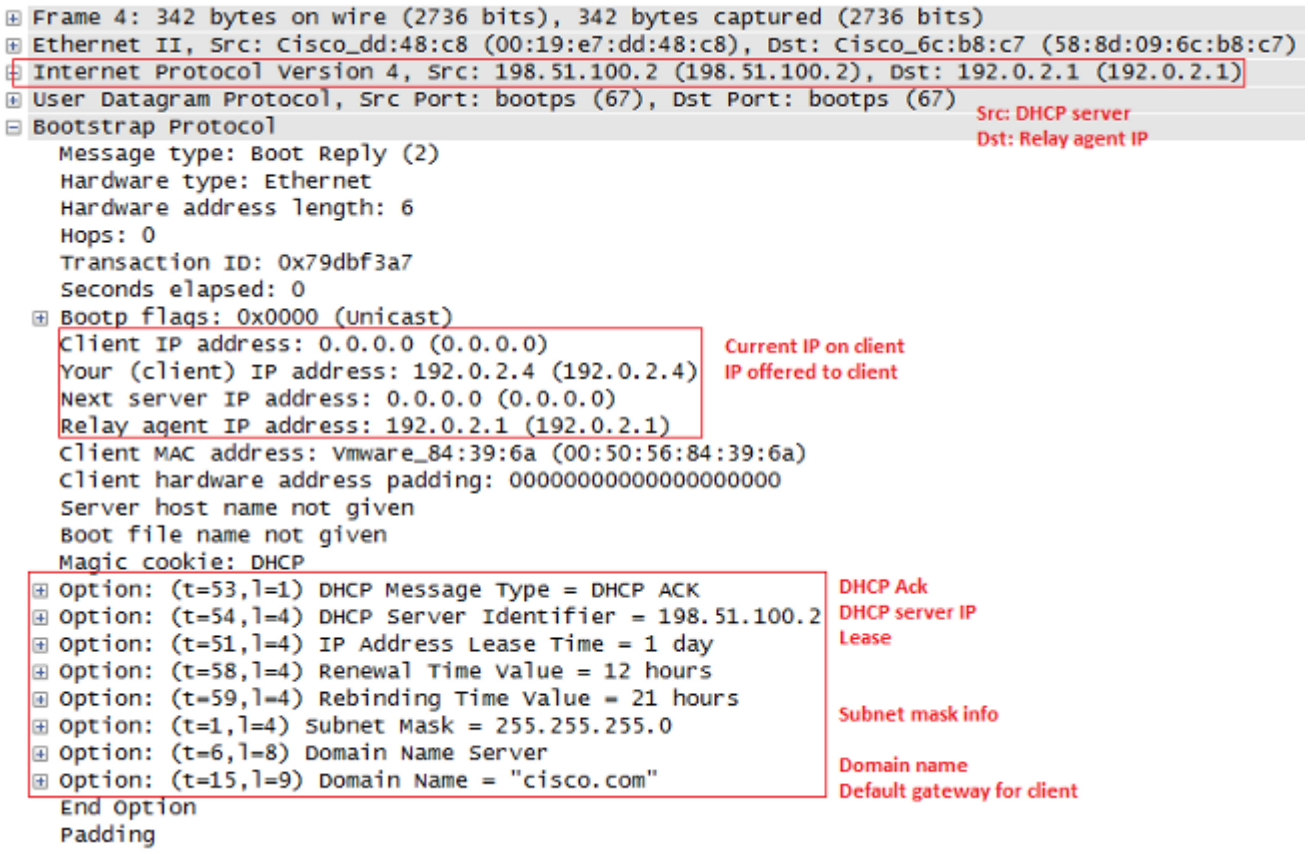
5. Zodra u het DHCPOFFER bericht ontvangt, stuur dan een DHCPREQUEST bericht om aan te geven dat u het aanbod accepteert.



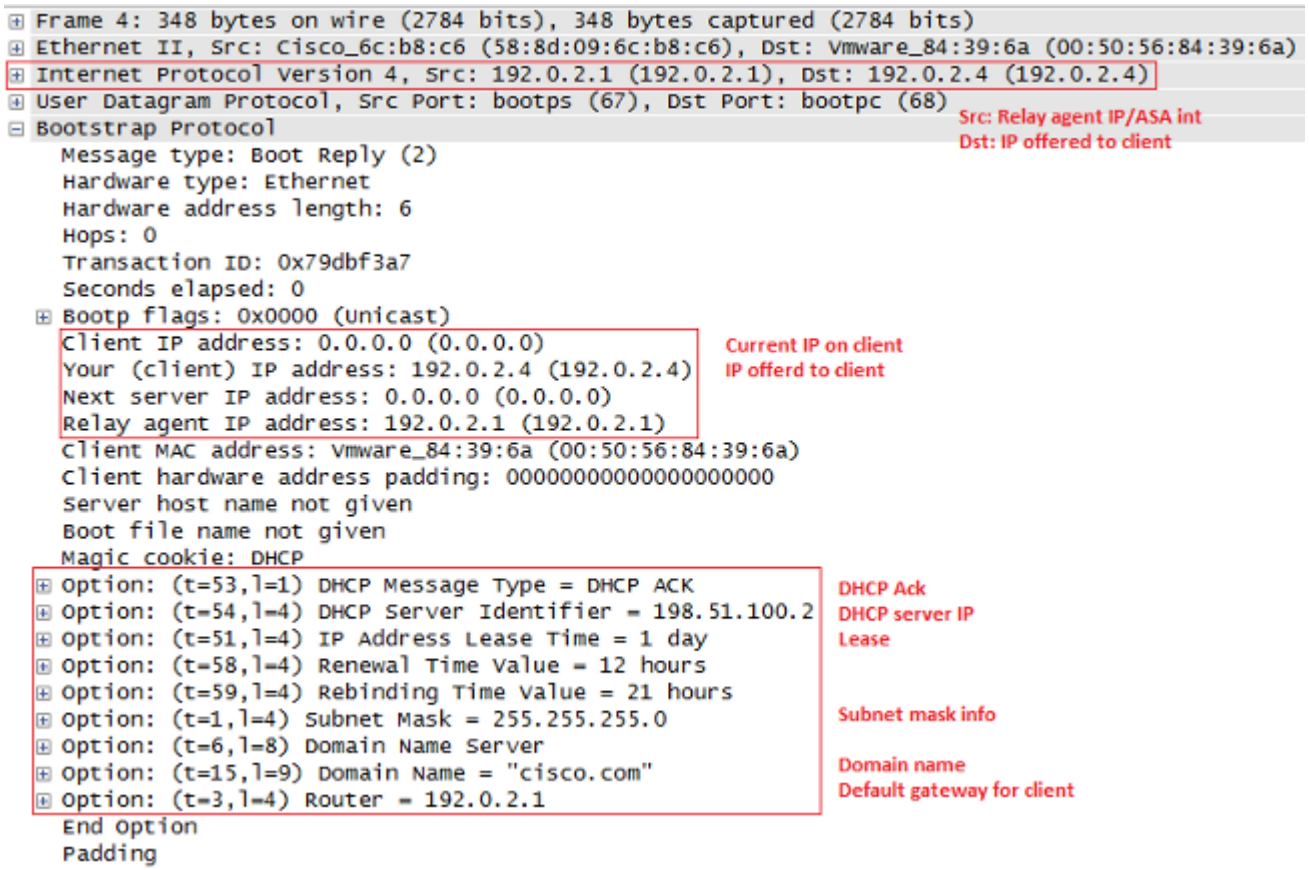
6. ASA geeft de DHCP CPREQUEST door aan de DHCP-server.



7. Zodra de server de DHCPREQUEST krijgt, stuurt het de DHCPACK terug om de aangeboden IP te bevestigen.



8. ASA geeft de DHCPACK van de DHCP server aan u door, en dat voltooit de transactie.



Debugs en syslogs voor DHCP Relay-transacties

Dit is een DHCP-verzoek doorgestuurd naar DHCP-serverinterface 198.51.10.2:

```
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
```

Nadat het antwoord van de server van DHCP wordt ontvangen, door het veiligheidstoestel het aan de cliënt van DHCP met adres 0050.5684.396a van MAC door:sturen, en verandert het gatewayadres in zijn eigen binneninterface.

```
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.
```

Dezelfde transactie verschijnt ook in de syslogs:

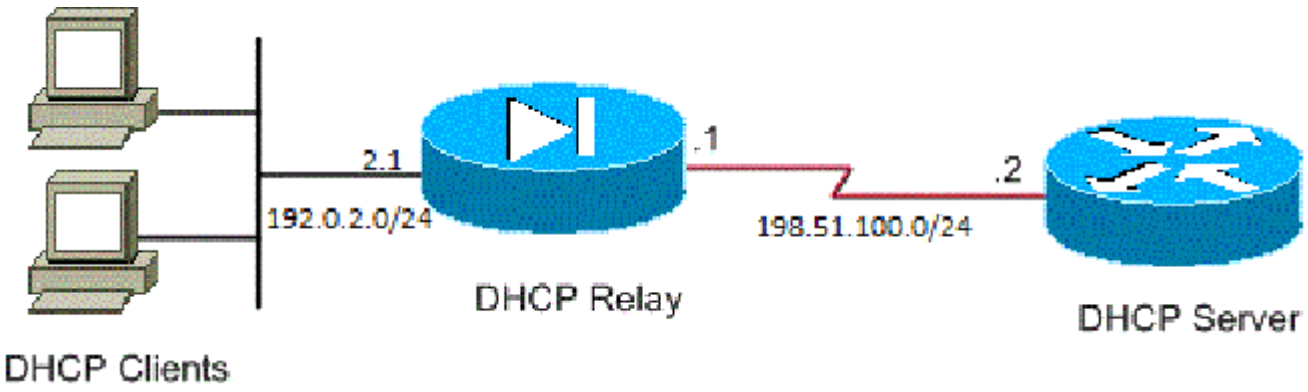
```
%ASA-7-609001: Built local-host inside:0.0.0.0
%ASA-7-609001: Built local-host identity:255.255.255.255
%ASA-6-302015: Built inbound UDP connection 13 for inside:
 0.0.0.0/68 (0.0.0.0/68) to identity:255.255.255.255/67 (255.255.255.255/67)
%ASA-7-609001: Built local-host identity:198.51.100.1
%ASA-7-609001: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

Configureren

In deze sectie vindt u de informatie die wordt gebruikt om de functies te configureren die in dit document worden beschreven.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Configuraties

Dit document gebruikt de volgende configuraties:

- DHCP Relay-configuratie met gebruik van de CLI
- Definitieve configuratie van DHCP Relay
- DHCP-serverconfiguratie

DHCP Relay-configuratie met gebruik van de CLI

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

Definitieve configuratie van DHCP Relay

```
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
```

DHCP-serverconfiguratie

```
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
```

DHCP-relay met meerdere DHCP-servers

U kunt maximaal tien DHCP-servers definiëren. Wanneer een client een DHCP *Discover*-pakket verstuurt, wordt dit doorgestuurd naar alle DHCP-servers.

Hierna volgt een voorbeeld:

```
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
```

Debugs met meerdere DHCP-servers

Hier zijn enkele voorbeelden van debugs wanneer meerdere DHCP servers worden gebruikt:

```
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.
```

Opname met meerdere DHCP-servers

Hier is een voorbeeldpakketopname wanneer meerdere DHCP-servers worden gebruikt:

```
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
```

Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

Om de statistische informatie over de DHCP-relay-services te bekijken, voert u de opdracht **show dhcprelay statistics** op de ASA CLI in:

```
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
```

Deze uitvoer biedt informatie over verschillende DHCP-berichttypes, zoals DHCPDiscover, DHCP-VERZOEK, DHCP-SOFTWARE, DHCP-RELEASE en DHCP-ACK.

- dhcprelay state tonen op ASA CLI
- toon ip DHCP serverstatistieken op router CLI

Problemen oplossen

Deze sectie bevat informatie die u kunt gebruiken om problemen met de configuratie te troubleshooten.

```
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
```

U kunt deze debug-opdrachten ook gebruiken:

- **debug DHCPprelay pakket**
- **debug dhcprelay-gebeurtenis**
- **Opname**
- **Syslogs**

Opmerking: Raadpleeg Belangrijke informatie over debug commando's voordat u **debug** commando's gebruikt.

Gerelateerde informatie

- **Opname op ASA**
- **Technische ondersteuning en documentatie â€“ Cisco Systems**

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.