Konfigurieren des DHCP-Relays der Adaptive Security Appliance (ASA)

Inhalt

Einleitung

In diesem Dokument wird das DHCP-Relay auf der Cisco ASA mithilfe der Paketerfassung und -debuggung beschrieben, und es wird ein Konfigurationsbeispiel bereitgestellt.

Voraussetzungen

Ein DHCP-Relay-Agent (Dynamic Host Configuration Protocol) ermöglicht der Security Appliance die Weiterleitung von DHCP-Anfragen von Clients an einen Router oder einen anderen DHCP-Server, der mit einer anderen Schnittstelle verbunden ist.

Diese Einschränkungen gelten nur für die Verwendung des DHCP-Relay-Agenten:

- Der Relay-Agent kann nicht aktiviert werden, wenn die DHCP-Serverfunktion ebenfalls aktiviert ist.
- Sie müssen direkt mit der Sicherheits-Appliance verbunden sein und können keine Anfragen über einen anderen Relay-Agenten oder einen Router senden.
- Im Modus mit mehreren Kontexten können Sie kein DHCP-Relay aktivieren oder einen DHCP-Relay-Server auf einer Schnittstelle konfigurieren, die von mehreren Kontexten verwendet wird.

DHCP-Relay-Services sind im transparenten Firewall-Modus nicht verfügbar. Eine Sicherheits-Appliance im transparenten Firewall-Modus lässt nur ARP-Datenverkehr (Address Resolution Protocol) zu. Für den übrigen Datenverkehr ist eine Zugriffskontrollliste (Access Control List, ACL) erforderlich. Damit DHCP-Anfragen und -Antworten über die Security Appliance im transparenten Modus ausgeführt werden können, müssen Sie zwei ACLs konfigurieren:

- Eine ACL, die DHCP-Anfragen von der internen Schnittstelle an die Außenseite ermöglicht.
- Eine ACL, die Antworten vom Server in die andere Richtung zulässt.

Anforderungen

Cisco empfiehlt, dass Sie über Grundkenntnisse der ASA CLI und der Cisco IOS® CLI verfügen.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Security Appliance der Serie ASA 5500-x Version 9.x oder höher
- Router der Cisco 1800 Serie

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

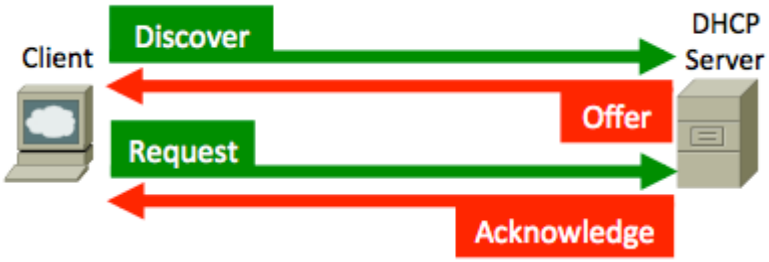
Hintergrundinformationen

Das DHCP-Protokoll stellt Hosts automatische Konfigurationsparameter wie eine IP-Adresse mit einer Subnetzmaske, ein Standard-Gateway, eine DNS-Serveradresse und eine WINS-Adresse (Windows Internet Name Service) zur Verfügung. Zu Beginn verfügen DHCP-Clients nicht über diese Konfigurationsparameter. Um diese Informationen zu erhalten, senden sie eine Broadcast-Anfrage. Wenn diese Anforderung von einem DHCP-Server empfangen wird, stellt der DHCP-Server die erforderlichen Informationen bereit. Aufgrund der Art dieser Broadcast-Anfragen müssen sich der DHCP-Client und -Server im gleichen Subnetz befinden. Layer-3-Geräte wie Router und Firewalls leiten diese Broadcast-Anfragen in der Regel nicht standardmäßig weiter.

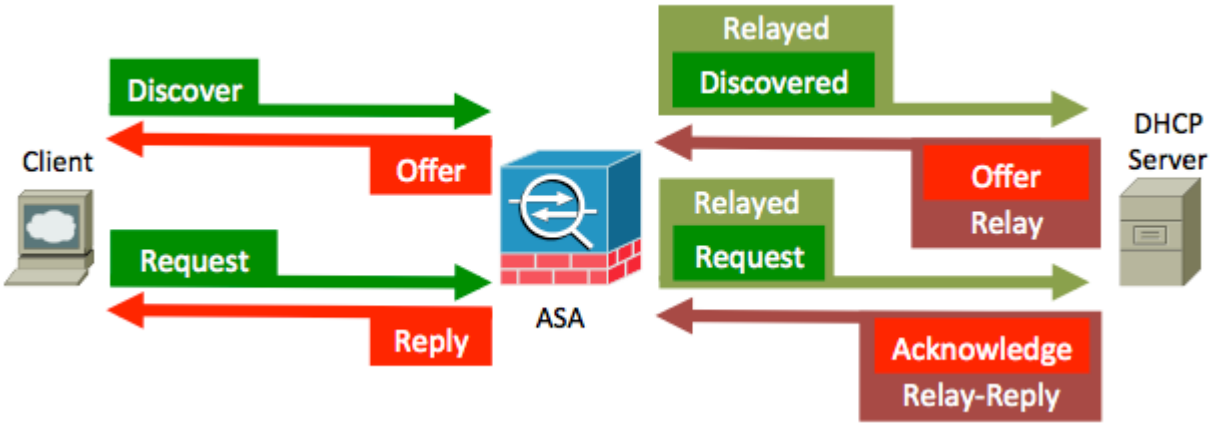
Ein Versuch, DHCP-Clients und einen DHCP-Server im gleichen Subnetz zu finden, ist nicht immer praktisch. In diesem Fall können Sie ein DHCP-Relay verwenden. Wenn der DHCP-Relay-Agent auf der Sicherheits-Appliance eine DHCP-Anfrage von einem Host an einer internen Schnittstelle empfängt, leitet er die Anfrage an einen der angegebenen DHCP-Server an einer externen Schnittstelle weiter. Wenn der DHCP-Server auf den Client antwortet, leitet die Sicherheits-Appliance diese Antwort weiter. Somit fungiert der DHCP Relay Agent als Proxy für den DHCP-Client bei der Kommunikation mit dem DHCP-Server.

Paketfluss

Dieses Bild zeigt den DHCP-Paketfluss, wenn kein DHCP-Relay-Agent verwendet wird:



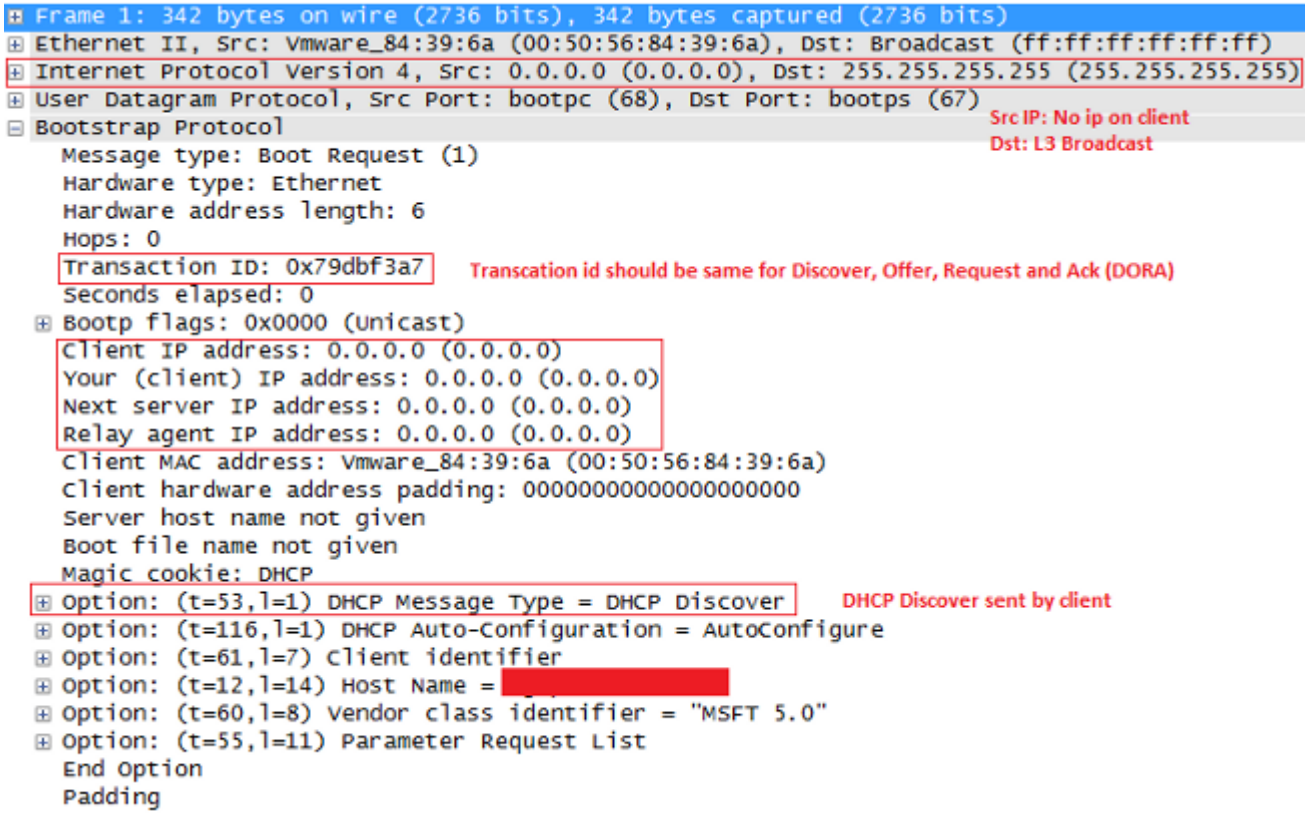
Die ASA fängt diese Pakete ab und bindet sie in das DHCP-Relay-Format ein:



DHCP-Relay mit Paketerfassung auf der internen und externen ASA-Schnittstelle

Notieren Sie sich ROT hervorgehobene Inhalte, da die ASA auf diese Weise verschiedene Felder ändert.

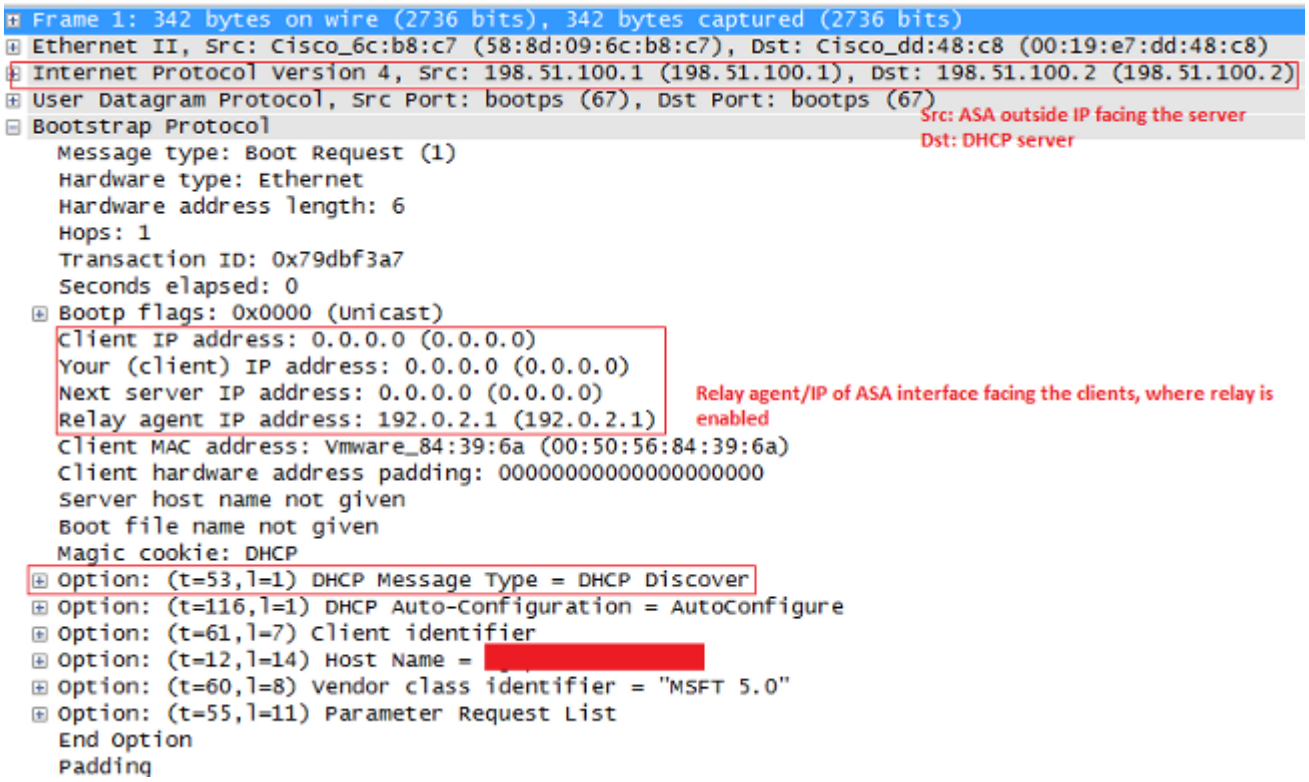
1. Um den DHCP-Prozess zu starten, starten Sie das System, und senden Sie eine Broadcast-Nachricht (DHCPDISCOVER) an die Zieladresse 255.255.255.255 - UDP-Port 67.



Hinweis: Wenn ein VPN-Client eine IP-Adresse anfordert, ist die IP-Adresse des Relay-Agents die erste verwendbare IP-Adresse, die durch den Befehl dhcp-network-scope unter der Gruppenrichtlinie definiert wird.

---

2. Normalerweise würde ASA den Broadcast verwerfen, aber da sie als DHCP-Relay konfiguriert ist, leitet sie die DHCPDISCOVER-Nachricht als Unicast-Paket von der zum Server gerichteten Schnittstellen-IP-Adresse an die IP-Quelle des DHCP-Servers weiter. In diesem Fall handelt es sich um die IP-Adresse der externen Schnittstelle. Beachten Sie die Änderung im Feld "IP-Header und Relay-Agent":



Hinweis: Aufgrund der in Cisco Bug-ID CSCuo89924 integrierten Fehlerbehebung kann ASA in Version 9.1(5.7), 9.3(1) und höher die Unicast-Pakete von der IP-Adresse der Schnittstelle, die dem Client (giaddr) gegenüberliegt, auf dem dhcprelay aktiviert ist, an die IP-Adresse des DHCP-Servers weiterleiten. In diesem Fall kann es sich um die IP-Adresse der internen Schnittstelle handeln.

---

3. Der Server sendet eine DHCPOFFER-Nachricht als Unicast-Paket zurück an die ASA, die an die IP-Adresse des Relay-Agenten gerichtet ist, die im DHCPDISCOVER- UDP-Port 67 eingerichtet ist. In diesem Fall ist es die IP-Adresse der inneren Schnittstelle (giaddr), in der dhcprelay aktiviert ist. Beachten Sie die Ziel-IP im Layer-3-Header:

```
⊞ 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 sendet dieses Paket von der internen Schnittstelle aus - UDP-Port 68. Beachten Sie die Änderung im IP-Header, während das Paket die interne Schnittstelle verlässt:

```
⊞ 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

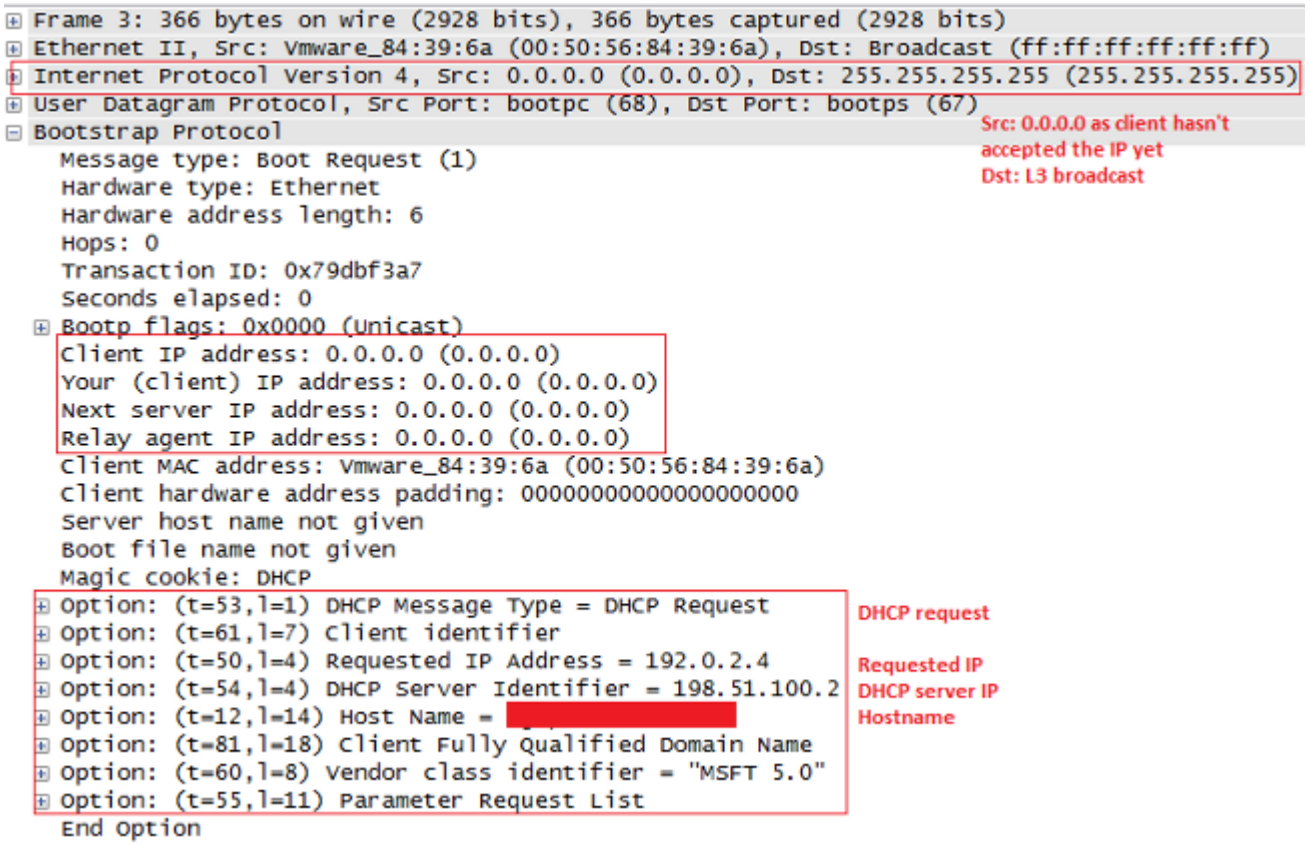
ASA interface IP

DHCP Offer
DHCP server IP
Lease

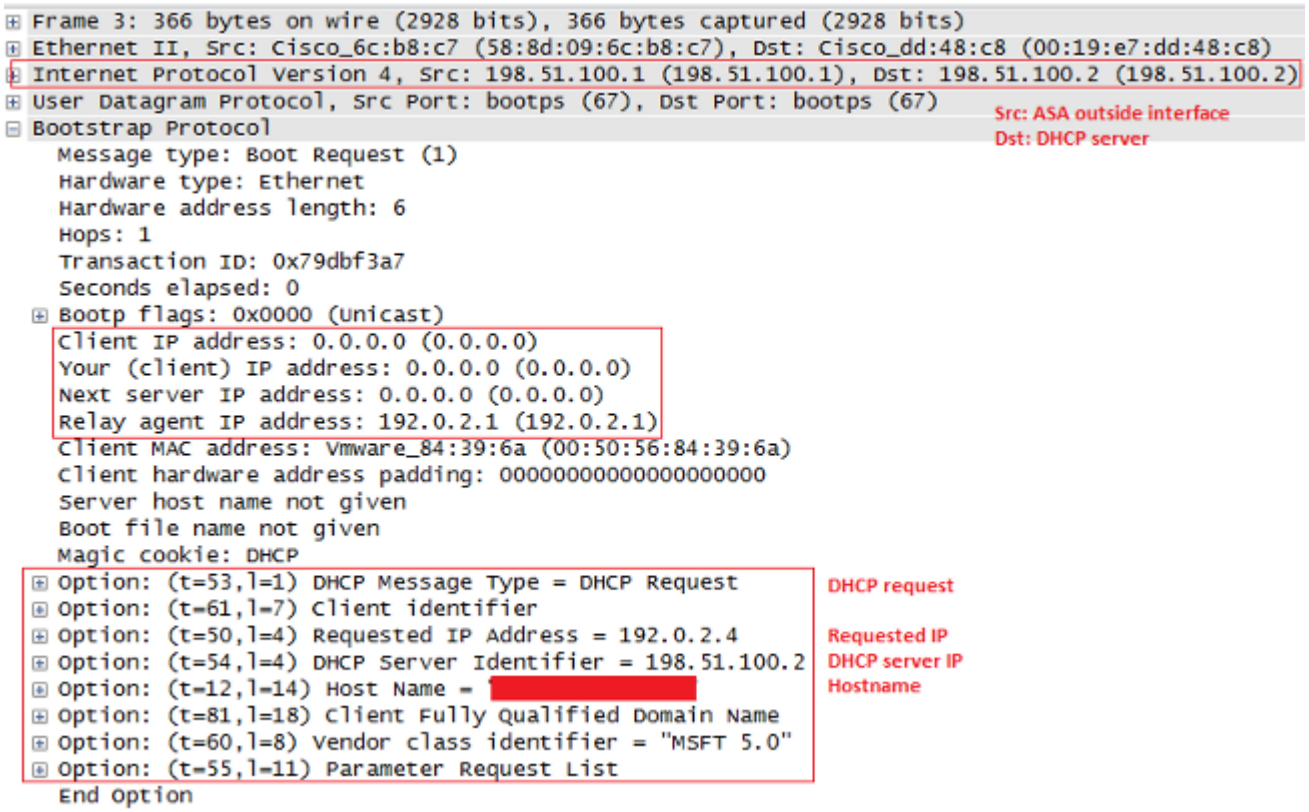
Subnet mask info

Domain name
Default Gateway for client

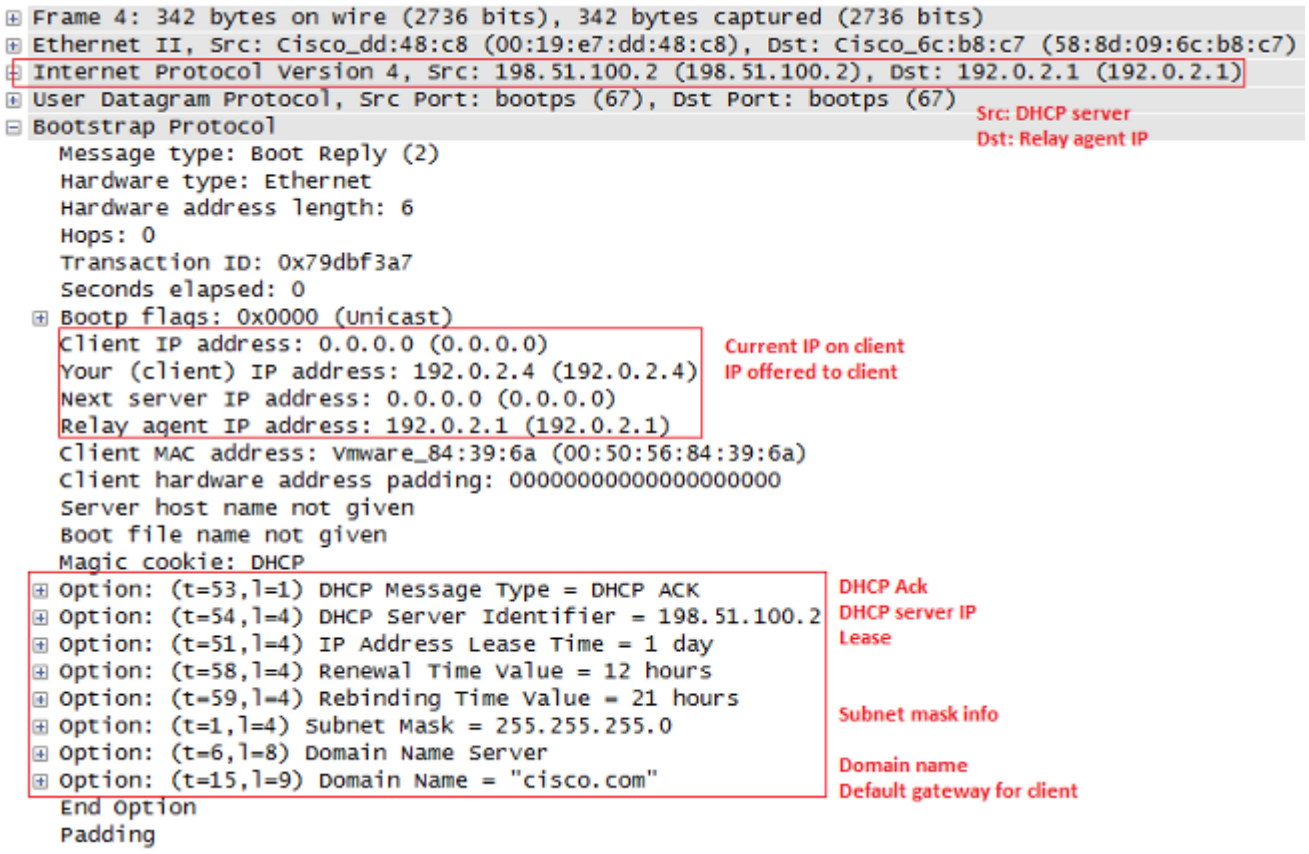
5. Sobald Sie die DHCPOFFER-Nachricht erhalten haben, senden Sie eine DHCPREQUEST-Nachricht, um anzuzeigen, dass Sie das Angebot annehmen.



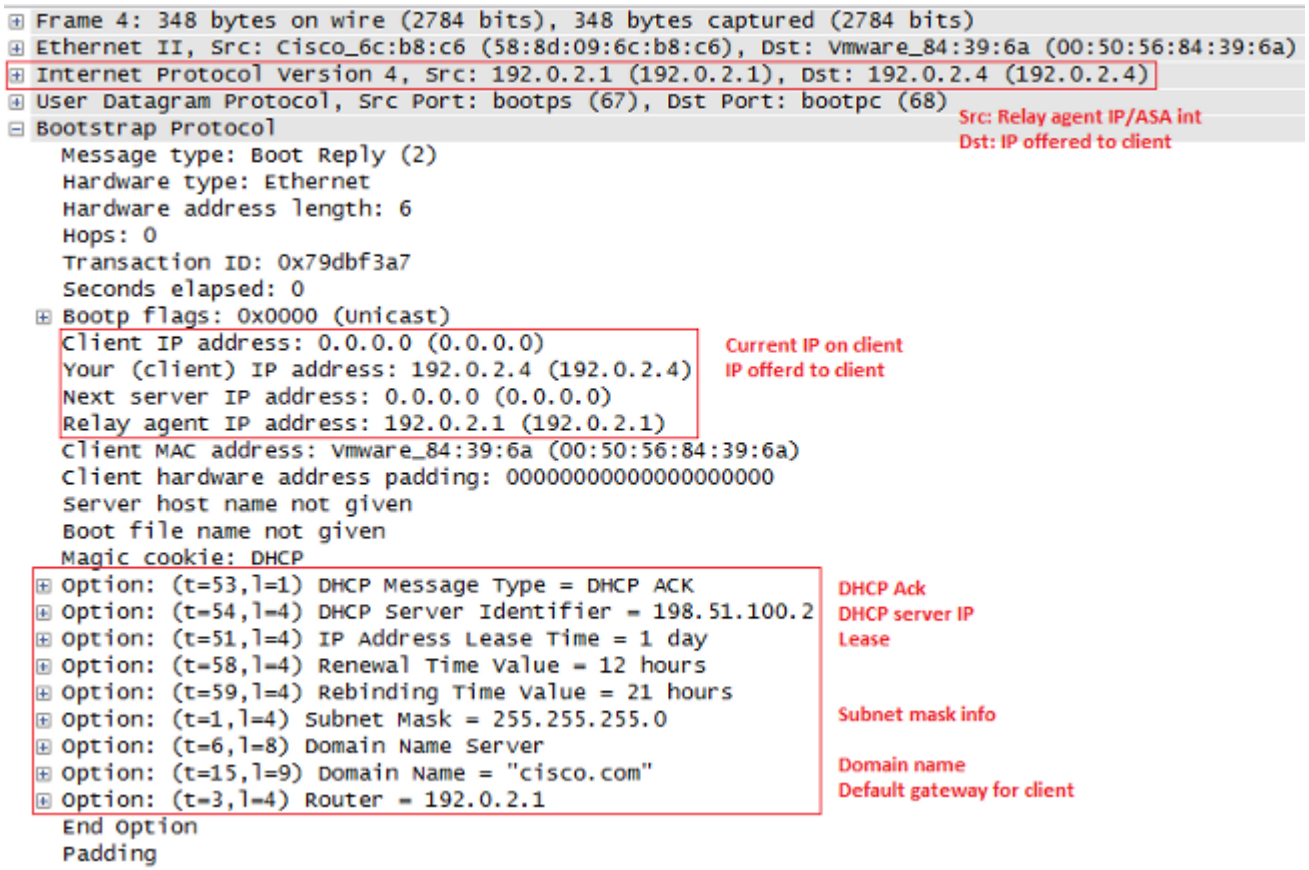
6. ASA leitet DHCPREQUEST an den DHCP-Server weiter



7. Sobald der Server DHCPREQUEST erhält, sendet er das DHCPACK zurück, um die angebotene IP zu bestätigen.



8. ASA leitet das DHCPACK vom DHCP-Server an Sie weiter und schließt die Transaktion ab.



Debugger und Syslogs für DHCP-Relay-Transaktionen

Dies ist eine DHCP-Anfrage, die an die DHCP-Serverschnittstelle 198.51.100.2 weitergeleitet wird:

```
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
```

Nachdem die Antwort vom DHCP-Server empfangen wurde, leitet die Sicherheits-Appliance sie an den DHCP-Client mit der MAC-Adresse 0050.5684.396a weiter und ändert die Gateway-Adresse in eine eigene interne Schnittstelle.

```
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.
```

Dieselbe Transaktion wird auch in den Syslogs angezeigt:

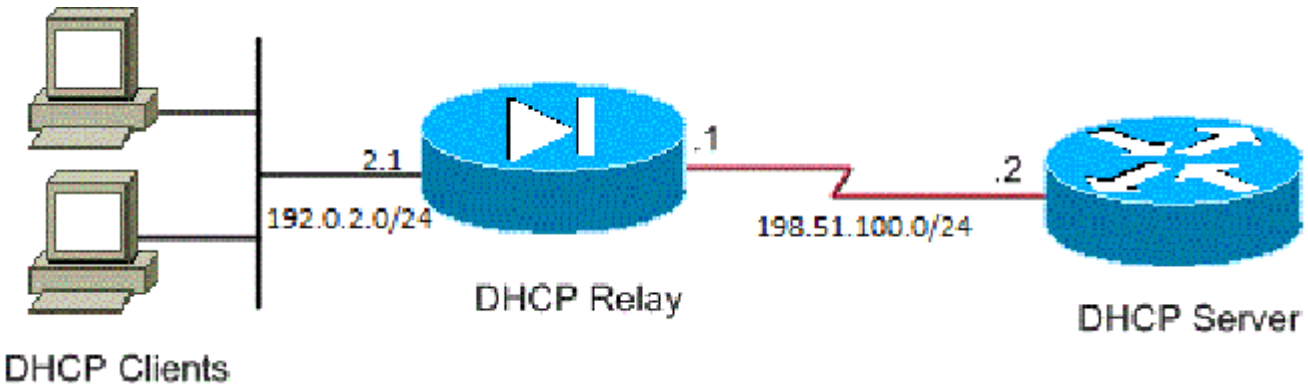
```
%ASA-7-609001: Built local-host inside:0.0.0.0
%ASA-7-609001: Built local-host identity:255.255.255.255
%ASA-6-302015: Built inbound UDP connection 13 for inside:
 0.0.0.0/68 (0.0.0.0/68) to identity:255.255.255.255/67 (255.255.255.255/67)
%ASA-7-609001: Built local-host identity:198.51.100.1
%ASA-7-609001: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

Konfigurieren

In diesem Abschnitt werden die Informationen angezeigt, die zum Konfigurieren der in diesem Dokument beschriebenen Funktionen verwendet werden.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Konfigurationen

In diesem Dokument werden folgende Konfigurationen verwendet:

- DHCP-Relay-Konfiguration mit Verwendung der CLI
- Endkonfiguration des DHCP-Relays
- DHCP-Serverkonfiguration

DHCP-Relay-Konfiguration mit Verwendung der CLI

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

Endkonfiguration des DHCP-Relays

```
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-Serverkonfiguration

```
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 mit mehreren DHCP-Servern

Sie können bis zu zehn DHCP-Server definieren. Wenn ein Client ein DHCP *Discover*-Paket sendet, wird es an alle DHCP-Server weitergeleitet.

Hier ein Beispiel:

```
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
```

Debuggen mit mehreren DHCP-Servern

Nachfolgend finden Sie einige Beispiele für Debugging-Vorgänge bei Verwendung mehrerer DHCP-Server:

```
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.
```

Erfassung mit mehreren DHCP-Servern

Im Folgenden finden Sie ein Beispiel für die Paketerfassung bei Verwendung mehrerer DHCP-Server:

```
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
```

Überprüfung

Verwenden Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Um die statistischen Informationen zu den DHCP-Relay-Services anzuzeigen, geben Sie den Befehl **show dhcprelay statistics** in der ASA CLI ein:

```
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
```

Diese Ausgabe enthält Informationen zu verschiedenen DHCP-Nachrichtentypen, z. B. DHCPDISCOVER, DHCP REQUEST, DHCP OFER, DHCP RELEASE und DHCP ACK.

- Zeigt den DHCP-Prelay-Status auf der ASA-CLI an
- Zeigt IP-DHCP-Serverstatistiken auf Router-CLI an

Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

```
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
```

Sie können auch die folgenden Debug-Befehle verwenden:

- **debug dhcprelay-Paket**
- **debug dhcprelay-Ereignis**
- **Aufnahmen**
- **Syslogs**

Hinweis: Lesen Sie Wichtige Informationen zu Debug-Befehlen, bevor Sie **Debug**-Befehle verwenden.

Zugehörige Informationen

- **Erfassung auf ASA**
- **Technischer Support und Dokumentation für Cisco Systeme**

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.